NIST Special Publication 800-82
Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Victoria Pillitteri
Suzanne Lightman
Marshall Abrams
Adam Hahn

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

National Institute of Standards and Technology
U.S. Department of Commerce

邦訳：
一般社団法人 JPCERT コーディネーションセンター

NIST SP800-82
第 2 版

産業用制御システム（ICS）セキュリティガイド

SCADA、DCS、PLC その他の制御システム設定

Keith Stouffer
Victoria Pillitteri
Suzanne Lightman
Marshall Abrams
Adam Hahn

本出版物は次のサイトから無料で入手可能：
http://dx.doi.org/10.6028/NIST.SP.800-82r2

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-82

Revision 2

Guide to Industrial Control Systems (ICS) Security

Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)

Keith Stouffer
Intelligent Systems Division
Engineering Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Marshall Abrams
The MITRE Corporation

Adam Hahn
Washington State University

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-82r2

May 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

NISTSP800-82
第 2 版

産業用制御システム(ICS)セキュリティガイド

SCADA、DCS、PLC、その他の制御システムの設定

Keith Stouffer
エンジニアリング研究所(EL)
インテリジェントシステム ディビジョン

Victoria Pillitteri
Suzanne Lightman
情報技術研究所(ITL)
コンピュータセキュリティディビジョン

Marshall Abrams
MITRE 社

Adam Hahn
ワシントン州立大学

本出版物は次のサイトから無料で入手可能：
http://dx.doi.org/10.6028/NIST.SP.800-82r2

2015 年 5 月

米国商務省
長官 Penny Pritzker

商務省標準技術担当次官
米国国立標準技術研究所　所長
Willie May

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-82, Revision 2 Natl. Inst. Stand. Technol. Spec. Publ. 800-82, Rev. 2, 247 pages (May 2015)
This publication is available free of charge from
:http://dx.doi.org/10.6028/NIST.SP.800-82r2
CODEN: NSPUE2

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic Mail: nist800-82rev2comments@nist.gov

本文書について

本出版物は、2014 年連邦情報セキュリティ近代化法（FISMA）44 U.S.C. § 3541 及び一般法（P.L.）113-283 に基づき、米国国立標準技術研究所（NIST）がその法的責務を遂行するために作成した。
NIST は、連邦情報システムの最低限の要件事項を含んだ情報セキュリティ標準及びガイドラインを作成する責務があるが、このような標準及びガイドラインは、国家安全保障に係わるシステムにおいては、連邦当局による当該システムに対するポリシー権限を行使する明示的承認がなければ適用されない。本ガイドラインは、行政管理予算局（OMB）通達 A-130、8b(3)条、「政府機関情報システムの保全」（通達 A-130 付録 IV「主要条文の分析」に記載）の要件に一致する。補足情報は、通達 A-130 付録 III「連邦自動化情報リソースのセキュリティ」に記載されている。

本出版物のいかなる記述も、商務長官の法的権限により連邦政府機関に適用される標準及びガイドラインを否定するものではない。またガイドラインは、商務長官、行政管理予算局長官、またはその他連邦当局の既存の権限に変更を加えたり、代替するものと解釈してはならない。
本出版物は、政府以外の組織が任意に使用することができ、米国における著作権の対象とならないが、NIST は著作権の帰属を明記することに感謝する。

米国国立標準技術研究所（NIST）SP800-82 第 2 版、
Natl. Inst. Stand. Technol. Spec. Publ. 800-82, Rev. 2, 247 **ページ**（2015 **年 5 月**）
本出版物は次のサイトから入手可能(無料)
：http://dx.doi.org/10.6028/NIST.SP.800-82r2
CODEN:NSPUE2

本文書では、特定される営利団体名、装置又は資料は、実験的な手順又は概念を適切に説明するためのものである。したがって、NIST による推奨や保証するものではなく、当該営利団体、装置又は資料が、その目的に関して得られる最良のものであることを意味するものでもない。

本出版物では、NIST がその負託された法的責務に従って現在作成中の他の出版物を参照する場合がある。本出版物の概念や方法論を含む情報は、前述の関連出版物の完成前であっても、連邦政府機関が使用する場合がある。よって、各出版物が完成するまでは、現在の必須要件、ガイドライン及び手順が存在する場合、それらは引き続き有効である。連邦政府機関は計画作成と移行の目的として、NIST によるこれら新規出版物の作成状況を確認されたい。
各組織は、パブリックコメントの公募期間中に、全ての公開ドラフト文書を閲覧し、コメントを NIST に提示されたい。全ての NIST コンピュータセキュリティディビジョンの出版物は、上記のものを除き、http://csrc.nist.gov/publications　から入手できる。

本出版物に関する意見は、以下の宛先に提出されたい。

Attn：Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
電子メール：nist800-82rev2comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

Keywords

Computer security; distributed control systems (DCS); industrial control systems (ICS); information security; network security; programmable logic controllers (PLC); risk management; security controls; supervisory control and data acquisition (SCADA) systems

コンピュータシステム技術に関するレポート

米国国立標準技術研究所（NIST）の情報技術研究所（ITL）は、国の計測及び基準インフラに関する技術的統率を図ることにより、米国の経済・公共福祉を促進している。ITL は試験、試験法、基準データ、概念の実証及び技術解析の開発を進め、情報技術の開発と生産的利用を促進している。ITL の責務には、連邦情報システムにおける国のセキュリティ関連情報以外の、費用効果の高いセキュリティ及びプライバシーに関する運営、管理、技術及び物理的基準・ガイドラインの作成が含まれる。SP800 シリーズは、ITL の研究、ガイドライン及び情報システムセキュリティにおける公共福祉に向けた取組並びに産官学との連携に関する報告書である。

抄録

本文書は、SCADA、DCS、PLC その他の制御システム設定を含む産業用制御システム（ICS）の保全方法に関するガイダンスであり、その独特な性能・信頼性・安全性要件について取り上げる。ICS の概要と典型的なシステムトポロジーを述べ、これらシステムへの一般的な脅威と脆弱性を明らかにし、関係するリスクを減らすためのセキュリティ対策について提言する。

キーワード

コンピュータセキュリティ、DCS、ICS、情報セキュリティ、ネットワークセキュリティ、PLC、リスク管理、セキュリティ対策、SCADA

Acknowledgments for Revision 2

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication. A special acknowledgement to Lisa Kaiser, Department of Homeland Security, the Department of Homeland Security Industrial Control System Joint Working Group (ICSJWG), and Office of the Deputy Undersecretary of Defense for Installations and Environment, Business Enterprise Integration Directorate staff, Daryl Haegley and Michael Chipley, for their exceptional contributions to this publication.

Acknowledgments for Previous Versions

The original authors, Keith Stouffer, Joe Falco, and Karen Scarfone of NIST, wish to thank their colleagues who reviewed drafts of the original version of the document and contributed to its technical content. The authors would particularly like to acknowledge Tim Grance, Ron Ross, Stu Katzke, and Freemon Johnson of NIST for their keen and insightful assistance throughout the development of the document. The authors also gratefully acknowledge and appreciate the many contributions from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of the publication. The authors would particularly like to thank the members of ISA99. The authors would also like to thank the UK National Centre for the Protection of National Infrastructure (CPNI)) for allowing portions of the *Good Practice Guide on Firewall Deployment for SCADA and Process Control Network* to be used in the document as well as ISA for allowing portions of the ISA-62443 Standards to be used in the document.

Note to Readers

This document is the second revision to NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security. Updates in this revision include:

- Updates to ICS threats and vulnerabilities.
- Updates to ICS risk management, recommended practices, and architectures.
- Updates to current activities in ICS security.
- Updates to security capabilities and tools for ICS.
- Additional alignment with other ICS security standards and guidelines.
- New tailoring guidance for NIST SP 800-53, Revision 4 security controls including the introduction of overlays.
- An ICS overlay for NIST SP 800-53, Revision 4 security controls that provides tailored security control baselines for Low, Moderate, and High impact ICS.

第 2 版に関する謝辞

本文書の著者らは、官民の個人及び組織から多大の貢献があったことを認め、ここに謝意を表する。その示唆に富み建設的な意見により、本出版物の全体的な質、包括性及び有用性が向上した。特に Lisa Kaiser（国土安全保障省）、国土安全保障省の Industrial Control System Joint Working Group (ICSJWG)及び Office of the Deputy Undersecretary of Defense for Installations and Environment、Business Enterprise Integration Directorate の職員、Daryl Haegley 及び Michael Chipley に対して、それぞれの特別な貢献に謝辞を表するものである。

旧版に関する謝辞

旧版の著者である NIST の Keith Stouffer、Joe Falco 及び Karen Scarfone は、本文書の原案を精査し、その技術的内容に寄与した同僚諸氏に謝意を表する。著者は特に、NIST の Tim Grance、Ron Ross、Stu Katzke 及び Freemon Johnson に対し、文書の作成全般にわたり鋭い洞察を与えてくれたことに謝意を表する。また、官民から多大の貢献があり、示唆に富み建設的な意見により出版物の質と有用性が向上したことにも謝意を表する。とりわけ ISA99 のメンバーには感謝している。また「SCADA 及びプロセス制御ネットワークのファイアウォールに係る適正規範ガイド」の一部を本文書で利用させてくれた英国インフラストラクチャ防護センター（CPNI）及び ISA-62443 規格を同様に利用させてくれた ISA に対しても、謝意を表する。

読者への注記

本文書は NIST SP 800-82「Guide to Industrial Control Systems (ICS) Security（産業用制御システムセキュリティガイド」の第 2 版である。更新内容は以下のとおり。

ICS の脅威と脆弱性に関する改訂
ICS リスク管理、推奨規範およびアーキテクチャに関する改訂
ICS セキュリティにおける現在の活動に関する改訂
ICS のセキュリティ性能とツールに関する改訂
他の ICS セキュリティ基準およびガイドラインとの補足調整
オーバーレイの紹介を含む NIST SP 800-53 の新ガイダンス第 4 版セキュリティ対策
低・中・高インパクト ICS に合ったセキュリティ管理策のベースラインを与えている NIST SP 800-53 第 4 版のセキュリティ管理策に対応した ICS オーバーレイ

Table of Contents

List of Apendix

List of Figure

List of Tables

Executive Summary

This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) are often found in the industrial control sectors. ICS are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods.) SCADA systems are generally used to control dispersed assets using centralized data acquisition and supervisory control. DCS are generally used to control production systems within a local area such as a factory using supervisory and regulatory control. PLCs are generally used for discrete control for specific applications and generally provide regulatory control. These control systems are vital to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems. It is important to note that approximately 90 percent of the nation's critical infrastructures are privately owned and operated. Federal agencies also operate many of the ICS mentioned above; other examples include air traffic control and materials handling (e.g., Postal Service mail handling.) This document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

Initially, ICS had little resemblance to traditional information technology (IT) systems in that ICS were isolated systems running proprietary control protocols using specialized hardware and software. Many ICS components were in physically secured areas and the components were not connected to IT networks or systems. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cybersecurity vulnerabilities and incidents. As ICS are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems. The increasing use of wireless networking places ICS implementations at greater risk from adversaries who are in relatively close physical proximity but do not have direct physical access to the equipment. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new security solutions are needed that are tailored to the ICS environment.

Although some characteristics are similar, ICS also have characteristics that differ from traditional information processing systems. Many of these differences stem from the fact that logic executing in ICS has a direct effect on the physical world. Some of these characteristics include significant risk to the health and safety of human lives and serious damage to the environment, as well as serious financial issues such as production losses, negative impact to a nation’s economy, and compromise of proprietary information. ICS have unique performance and reliability requirements and often use operating systems and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of control systems.

ICS cybersecurity programs should always be part of broader ICS safety and reliability programs at both industrial sites and enterprise cybersecurity programs, because cybersecurity is essential to the safe and reliable operation of modern industrial processes. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious or accidental actions by insiders. ICS security objectives typically follow the priority of availability and integrity, followed by confidentiality.

エグゼクティブサマリー

本文書は、セキュアな産業用制御システム（ICS）を構築するためのガイダンスとなる。SCADA、DCS、PLC その他の制御システム設定を含んだこれら ICS は、産業用制御業界によく見られる。ICS は一般的に電気、上下水、石油・ガス、輸送、化学、医薬品、パルプ・製紙、食品・飲料及び組立製造（自動車、航空宇宙、耐久消費財等）業界で利用されている。SCADA は、集中データ取得監視制御により、分散化された資産を制御するために、通常使用する。DCS は、ローカルエリア内にある工場等の生産システムを、監視・規制制御により制御するために、通常使用する。PLC は、特殊用途での離散制御に通常使用し、規制制御を通常行う。このような制御システムは、高度に連携・相互依存したシステムとなる、米国の重要インフラの運営に緊要な役割を果たしている。国の重要インフラのおよそ 90%は、私企業が保有し運営している点に注意すべきである。連邦政府機関も前述の ICS の多くを運営しているが、そのほかにも航空交通管制や物流処理（郵便物の取扱等）などがある。本文書ではこのような ICS の概要及び一般的なシステムトポロジーについて示し、システムにとっての一般的な脅威と脆弱性を特定し、関連リスクを低減するための推奨セキュリティ対策を提示する。

初期の ICS は、特殊なハードウエアとソフトウエアを使用して専用制御プロトコルを実行する隔絶されたシステムだったため、従来の情報技術（IT）システムとは類似点がほとんどなかった。ICS コンポーネントの多くは物理的に安全なエリア内に置かれ、IT ネットワークやシステムに接続されていなかった。昨今、広く利用可能な低コストのインターネットプロトコル（IP）デバイスが専用ソリューションに取って代わりつつあることから、サイバーセキュリティの脆弱性やインシデントが生じる蓋然性が高まっている。ICS は IT ソリューションを採用して、企業ビジネスシステムへの接続性やリモートアクセス能力を高め、また、業界標準コンピュータ、オペレーティングシステム（OS）及びネットワークプロトコルを使用して設計・実装されるようになっている。このため ICS は次第に IT システムと類似性を持つようになってきた。このような統合化は新たな IT 能力をサポートするが、それ以前のシステムに比べると、外界からの隔絶性が格段に劣るため、セキュリティの必要性が増す。ワイヤレスネットワークの利用度が高まるにつれて、物理的に近い場所にいるが、装備品への直接的な物理的アクセスはできない外敵による ICS 実装リスクが増大する。セキュリティソリューションは、一般的な IT システムにおけるセキュリティ問題を扱うようにできているので、ICS 環境に持ち込む場合には特別な注意が欠かせない。場合によっては、その ICS 環境に特化した新しいセキュリティソリューションが必要となる。

いくつかの特徴は似ていても、ICS には従来の情報処理システムとは異なる特徴もある。そうした違いの多くは、ICS で実行される論理が実世界に直接的な影響を及ぼすという事実から生じたものである。そうした特性の中には、人の健康や安全に対する深刻なリスク、重大な環境破壊のほか、生産量低減、国家経済への悪影響、秘密情報の漏洩といった重大な財務問題も含まれている。ICS の性能及び信頼性要件は独特で、普通の IT 関係者には奇異に見える OS やアプリケーションを使用することが多い。更に安全性と効率性の目標は、制御システムの設計・運用上、セキュリティと競合する場合がある。

サイバーセキュリティは、現代の産業工程を安全かつ高い信頼性をもって運用する上で不可欠であることから、ICS サイバーセキュリティプログラムは、産業現場においても企業サイバーセキュリティプログラムにおいても、常により広範な ICS の安全性・信頼性プログラムの一部となるべきである。制御システムに対する脅威の源は多岐にわたり、敵意を持つ政府、テロリストグループ、不満を抱いた従業員、悪意を持つ侵入者、複雑性、事故、自然災害、内部関係者の意図的又は偶発的行為等がある。ICS セキュリティの目的は、一般的に可用性と完全性を優先事項とし、機密性がそれに続く。

Possible incidents an ICS may face include the following:

- Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation.
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.
- Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects.
- ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects.
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.
- Interference with the operation of safety systems, which could endanger human life.

Major security objectives for an ICS implementation should include the following:

- **Restricting logical access to the ICS network and network activity.** This may include using unidirectional gateways, a demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate and ICS networks, and having separate authentication mechanisms and credentials for users of the corporate and ICS networks. The ICS should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- **Restricting physical access to the ICS network and devices.** Unauthorized physical access to components could cause serious disruption of the ICS's functionality. A combination of physical access controls should be used, such as locks, card readers, and/or guards.
- **Protecting individual ICS components from exploitation.** This includes deploying security patches in as expeditious a manner as possible, after testing them under field conditions; disabling all unused ports and services and assuring that they remain disabled; restricting ICS user privileges to only those that are required for each person's role; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware.
- **Restricting unauthorized modification of data.** This includes data that is in transit (at least across the network boundaries) and at rest.
- **Detecting security events and incidents.** Detecting security events, which have not yet escalated into incidents, can help defenders break the attack chain before attackers attain their objectives. This includes the capability to detect failed ICS components, unavailable services, and exhausted resources that are important to provide proper and safe functioning of the ICS.
- **Maintaining functionality during adverse conditions.** This involves designing the ICS so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, or does not cause another problem elsewhere, such as a cascading event. The ICS should also allow for graceful degradation such as moving from "normal operation" with full automation to "emergency operation" with operators more involved and less automation to "manual operation" with no automation.

ICS が直面し得るインシデントには次のようなものがある。

- ICS ネットワーク経由情報の遮断又は遅延。ICS の運用中断に至りかねない。
- 命令、コマンド又はアラーム閾値の無断変更。装備品の障害、故障若しくは遮断、環境への影響又は人命への危険を生じかねない。
- 無断変更の隠蔽又は操作員に誤操作を行わせることを目的とした、システムオペレータへの誤情報送達。様々な悪影響を生じかねない。
- ICS ソフトウエア若しくは設定の変更又は ICS ソフトウエアのマルウエア感染。様々な悪影響を生じかねない。
- 装備品保護装置との干渉。高額で換装困難な装備品を危険状態に置きかねない。
- 安全装置の運用に対する干渉。人命を危険にさらしかねない。

ICS 実装の主なセキュリティ上の達成目標には以下を含めるべきだ。

- **ICS ネットワークへの論理的なアクセスとネットワーク上の活動の制限。**これには企業ネットワークと ICS ネットワーク間の直接的なネットワークトラフィックを防止し、企業ネットワーク及び ICS ネットワークユーザ向けに、独立した認証メカニズムと認証情報を持つ一方向性ゲートウェイ、非武装地帯（DMZ）のファイアウォール付きネットワークアーキテクチャの利用が含まれる。また ICS は、最もセキュアで信頼性の高いレイヤーで最重要通信を行う、マルチレイヤーネットワークトポロジーを利用すべきである。
- **ICS ネットワーク及びデバイスへの物理的アクセス制限。**コンポーネントへの不正な物理アクセスは、ICS の機能に重大な中断をもたらしかねない。施錠、カードリーダー、警備員等の物理アクセス制御を併用すべきである。
- **個々の ICS コンポーネントの悪用防止。**これには次の内容が含まれる。セキュリティパッチをフィールド条件下で試験後、できるだけ迅速に展開する。使用していないポート及びサービスを全て使用不能にし、使用不能状態が保たれるようにする。ICS ユーザ権限の付与を、役割上必要とする人員に限定する。監査証跡の追跡及び監視。技術的に実行可能な場合、アンチウイルスソフトウエアやファイル整合性確認ソフトウエア等のセキュリティ管理を利用し、マルウエアを予防・抑止・検出・緩和する。
- **データの無断変更制限。**これには送信中のデータ（少なくともネットワーク境界を越えたもの）及び静止データが含まれる。
- **セキュリティ上のイベント及びインシデントの検出。**まだインシデントには至らないセキュリティイベントを検出できれば、防御側は、攻撃側の目的達成前に攻撃連鎖を断ち切ることができる。これには ICS が適正かつ安全な機能を発揮する上で重要な、ICS コンポーネントの障害、使用不能のサービス及び枯渇したリソースを検出する能力が含まれる。
- **悪条件下での機能保持。**これには各重要コンポーネントに冗長性を持たせる ICS 設計が関係してくる。また、あるコンポーネントに障害が出た場合でも、ICS その他のネットワークに不要のトラフィックを生じさせず、連鎖イベントなど別の問題を派生させてはならない。また ICS は、機能が低下する場合であっても、全自動の「正常運転」から操作員も加わった半自動の「緊急運転」へ、次いで完全な「手動運転」へと機能が徐々に低下するグレースフルデグラデーションになっているべきである。

- **Restoring the system after an incident.** Incidents are inevitable and an incident response plan is essential. A major characteristic of a good security program is how quickly the system can be recovered after an incident has occurred.

To properly address security in an ICS, it is essential for a cross-functional cybersecurity team to share their varied domain knowledge and experience to evaluate and mitigate risk to the ICS. The cybersecurity team should consist of a member of the organization's IT staff, control engineer, control system operator, network and system security expert, a member of the management staff, and a member of the physical security department at a minimum. For continuity and completeness, the cybersecurity team should consult with the control system vendor and/or system integrator as well. The cybersecurity team should coordinate closely with site management (e.g., facility superintendent) and the company's Chief Information Officer (CIO) or Chief Security Officer (CSO), who in turn, accepts complete responsibility and accountability for the cybersecurity of the ICS, and for any safety incidents, reliability incidents, or equipment damage caused directly or indirectly by cyber incidents. An effective cybersecurity program for an ICS should apply a strategy known as "defense-in-depth," layering security mechanisms such that the impact of a failure in any one mechanism is minimized. Organizations should not rely on "security by obscurity."

In a typical ICS this means a defense-in-depth strategy that includes:

- Developing security policies, procedures, training and educational material that applies specifically to the ICS.
- Considering ICS security policies and procedures based on the Homeland Security Advisory System Threat Level, deploying increasingly heightened security postures as the Threat Level increases.
- Addressing security throughout the lifecycle of the ICS from architecture design to procurement to installation to maintenance to decommissioning.
- Implementing a network topology for the ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
- Providing logical separation between the corporate and ICS networks (e.g., stateful inspection firewall(s) between the networks, unidirectional gateways).
- Employing a DMZ network architecture (i.e., prevent direct traffic between the corporate and ICS networks).
- Ensuring that critical components are redundant and are on redundant networks.
- Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events.
- Disabling unused ports and services on ICS devices after testing to assure this will not impact ICS operation.
- Restricting physical access to the ICS network and devices.
- Restricting ICS user privileges to only those that are required to perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege).
- Using separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts).

- **インシデント後のシステム復旧。**インシデントは避けられないので、インシデント対処計画が不可欠となる。優れたセキュリティプログラムの主要な特徴は、インシデント発生後、システムをどれだけ迅速に復旧できるかという点にある。

ICS においてセキュリティを適正に確保するには、機能横断型サイバーセキュリティチームが多様な分野の知識・経験を共有し合い、ICS のリスクを評価・緩和することが不可欠となる。サイバーセキュリティチームの構成は、最低でも組織の IT 要員、制御エンジニア、制御システムオペレータ、ネットワーク及びシステムセキュリティ専門員、経営に関わる要員及び物理的セキュリティ部門要員とすべきである。継続性と完全性を確保するため、サイバーセキュリティチームは、制御システムのベンダーやシステムインテグレータとも協議すべきである。また現場管理者（施設責任者等）のほか、ICS のサイバーセキュリティ、安全上のインシデント、信頼性上のインシデント又はサイバーインシデントにより直接・間接に生じた装備品の損害に全責任を負う企業の最高情報責任者（CIO）又は最高セキュリティ責任者（CSO）とも密接に連携を取るべきである。ICS の効果的なサイバーセキュリティプログラムは「多層防御（defense-in-depth）」として知られる戦略、つまり、あるメカニズムの障害の影響が最小限に食い止められる、レイヤリングセキュリティメカニズムを適用すべきである。組織は「曖昧なセキュリティ」に依存すべきでない。

このことは、一般的な ICS では以下の内容を含んだ多層防御戦略を意味する。

- ICS に特化して適用されるセキュリティポリシー、手順及び教育訓練資料の作成
- 国土安全保障アドバイザリーシステム脅威レベルに基づく ICS セキュリティポリシー及び手順の検討、脅威レベルの上昇に追随して段階的に高まるセキュリティ態勢の保持
- アーキテクチャ設計から調達、設置、保守、廃棄まで、ICS の全ライフサイクルを通じたセキュリティの考慮
- 最もセキュアで信頼性の高いレイヤーで最重要通信を行う、マルチレイヤーICS ネットワークトポロジーの実装
- 企業ネットワークと ICS ネットワーク間の論理的分割（ネットワーク間や一方向性ゲートウェイ間のステートフルインスペクションファイアウォールなど）
- DMZ ネットワークアーキテクチャの採用（企業ネットワークと ICS ネットワーク間の直接トラフィックを防止）
- 重要コンポーネントの冗長化と冗長性ネットワーク上での使用
- 壊滅的な連鎖イベントを防ぐグレースフルデグラデーション（フォールトトレラント）を備えた重要システムの設計
- ICS の運用に影響がないことを検証した上で、ICS デバイス上の不使用ポート及びサービスを使用不能にすること
- ICS ネットワーク及びデバイスへの物理的アクセス制限。
- 各人の業務を行うために必要な ICS ユーザ権限に限定した、権限の付与（役割に基づくアクセス制御と最小権限原則に基づく役割構成）
- ICS ネットワーク及び企業ネットワークユーザ向けの独立した認証メカニズムと認証情報の使用（ICS ネットワークアカウントに企業ネットワークユーザのアカウントを使用しない）

- Using modern technology, such as smart cards for Personal Identity Verification (PIV).
- Implementing security controls such as intrusion detection software, antivirus software and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS.
- Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications where determined appropriate.
- Expeditiously deploying security patches after testing all patches under field conditions on a test system if possible, before installation on the ICS.
- Tracking and monitoring audit trails on critical areas of the ICS.
- Employing reliable and secure network protocols and services where feasible.

The National Institute of Standards and Technology (NIST), in cooperation with the public and private sector ICS community, has developed specific guidance on the application of the security controls in NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [22], to ICS.
While many controls in Appendix F of NIST SP 800-53 are applicable to ICS as written, many controls require ICS-specific interpretation and/or augmentation by adding one or more of the following to the control:

- ICS Supplemental Guidance provides organizations with additional information on the application of the security controls and control enhancements in Appendix F of NIST SP 800-53 to ICS and the environments in which these specialized systems operate. The Supplemental Guidance also provides information as to why a particular security control or control enhancement may not be applicable in some ICS environments and may be a candidate for tailoring (i.e., the application of scoping guidance and/or compensating controls). ICS Supplemental Guidance does not replace the original Supplemental Guidance in Appendix F of NIST SP 800-53.
- ICS Enhancements (one or more) that provide enhancement augmentations to the original control that may be required for some ICS.
- ICS Enhancement Supplemental Guidance that provides guidance on how the control enhancement applies, or does not apply, in ICS environments.

The most successful method for securing an ICS is to gather industry recommended practices and engage in a proactive, collaborative effort between management, the controls engineer and operator, the IT organization, and a trusted automation advisor. This team should draw upon the wealth of information available from ongoing federal government, industry groups, vendor and standards organizational activities listed in Appendix D—.

- 身分証明（PIV）用スマートカードなど最新技術の使用
- 技術的に実行可能な場合、ICS に入る、ICS から出る、および ICS 内にあるマルウエアの導入・曝露・伝播を予防・抑止・検出・緩和するための侵入検知ソフトウエア、アンチウイルスソフトウエア、ファイル整合性確認ソフトウエア等によるセキュリティ管理
- 適当であれば、ICS データストレージ及び通信への暗号化又は暗号学的ハッシュ等セキュリティ技術の適用
- ICS へのインストール前に可能であれば、フィールド条件下で試験装置により検証したセキュリティパッチの迅速な展開
- ICS 重要領域での監査証跡の追跡及び監視
- 実行可能なら信頼性の高いセキュアなネットワークプロトコル及びサービスの採用

米国標準技術局（NIST）は官民 ICS 共同体の協力を得て、NISTSP（SP）800-53 第 4 版『連邦情報システム・組織のセキュリティ・プライバシー管理』[22]に記載される ICS へのセキュリティ管理の適用に関して、具体的なガイダンスを作成した。

NIST SP 800-53 の付録 F に記載される制御の多くは、記述どおり ICS に適用可能ではあるが、大抵は ICS 特有の解釈が必要で、以下に示すものを少なくとも 1 つ追加する必要がある。

- ICS 補足ガイダンス。NIST SP 800-53 の付録 F に記載されるセキュリティ管理及び管理拡張を、ICS 及びこれら専用システムの実行環境に適用するための補足情報を示す。また、ICS 環境によっては特定のセキュリティ管理や管理拡張が適用できず、調整が必要となる理由についても示す（スコーピングガイダンス又は補完制御の適用）。ICS 補足ガイダンスは、NIST SP 800-53 の付録 F にあるオリジナルの補足ガイダンスに代わるものではない。
- ICS 拡張（1 つ又は複数）。ICS によっては必要となる元々の制御に拡張を加える。
- ICS 拡張補足ガイダンス。ICS 環境において管理拡張適用の可否について示す。

ICS のセキュリティ確保に最も成果の上がる方法は、業界の推奨規範を蓄積し、幹部、制御エンジニア及び操作員、IT 組織並びに信用のおけるオートメーションアドバイザー間で、積極的に協調して取り組むことである。このチームは、連邦政府、業界グループ、ベンダー及び付録 D に掲載されている規格団体からの豊富な情報を利用すべきである。

1. Introduction

1.1 Purpose and Scope

The purpose of this document is to provide guidance for securing industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems performing control functions. The document provides a notional overview of ICS, reviews typical system topologies and architectures, identifies known threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. Additionally, it presents an ICS-tailored security control overlay, based on NIST SP 800-53 Rev. 4 [22], to provide a customization of controls as they apply to the unique characteristics of the ICS domain. The body of the document provides context for the overlay, but the overlay is intended to stand alone.

ICS are found in many industries such as electric, water and wastewater, oil and natural gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods). Because there are many different types of ICS with varying levels of potential risk and impact, the document provides a list of many different methods and techniques for securing ICS. The document should not be used purely as a checklist to secure a specific system. Readers are encouraged to perform a risk-based assessment on their systems and to tailor the recommended guidelines and solutions to meet their specific security, business and operational requirements. The range of applicability of the basic concepts for securing control systems presented in this document continues to expand.

1.2 Audience

This document covers details specific to ICS. Readers of this document should be acquainted with general computer security concepts, and communication protocols such as those used in networking. The document is technical in nature; however, it provides the necessary background to understand the topics that are discussed.

Relationship to Executive Order 13636 "Improving Critical Infrastructure Cybersecurity"

Recognizing that the national and economic security of the United States depends on the reliable functionality of critical infrastructure, the President under the Executive Order "Improving Critical Infrastructure Cybersecurity" [82] directed NIST to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. The Cybersecurity Framework (CSF) [83] consists of standards, guidelines, and best practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, performance-based, and cost-effective approach of the Framework will help owners and operators of critical infrastructure to manage cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties. The initial CSF, published in February 2014, resulted in a national-level framework that is flexible enough to apply across multiple sectors and for different operational environments. The CSF was developed based on stakeholder input to help ensure that existing work within the various sectors can be utilized within the Framework. Industrial control system cybersecurity standards, guidelines, and practices can be leveraged to address the CSF functions in the context of an organization's risk management program.

1. はじめに

1.1 目的及び適用範囲

本文書の目的は、産業用制御システム（ICS）のセキュリティを確保するためのガイダンスを示すことにあり、ICS には SCADA、DCS、その他の制御システムが含まれる。本文書ではこのような ICS の概念について概要を示し、一般的なシステムトポロジーとアーキテクチャについて考察し、システムに対する既知の脅威と脆弱性を特定し、関連リスクを低減するための推奨セキュリティ対策を提示する。また、NIST SP 800-53 改訂 4 [22]に従い、ICS 向けに調整されたセキュリティ管理オーバーレイを提示し、管理を ICS 領域の独特な特徴に適用する際のカスタマイズについて示す。
文書はオーバーレイの内容を提示するが、オーバーレイはそれ自体が独立したものである。

ICS は電気、上下水、石油・ガス、化学、医薬品、パルプ・製紙、食品・飲料及び組立製造（自動車、航空宇宙、耐久消費財等）業界で利用されている。リスクレベルやその影響が一様でない種々の ICS があるため、本文書では ICS セキュリティの方法と技術のリストを示す。本文書は、特定のシステムセキュリティを確保するための単なるチェックリストとして使用すべきでない。
読者は、使用しているシステムに関して、リスクに立脚した評価を行い、推奨されているガイドライン及びソリューションを固有のセキュリティ、業務および運用上の要件に合うように調整すべきである。本文書に示される制御システムのセキュリティ確保に関する基本概念の適用範囲は、今後も引き続き拡大する。

1.2 対象者

本文書には ICS に特有の詳細な事項が網羅されている。読者は、一般的なコンピュータセキュリティ概念およびネットワークで使用される通信プロトコルに通じているべきである。本文書の内容は、その性質上技術的ではあるが、記述されている論題を理解するために必要な背景をも提示する。

大統領命令 13636「重要インフラストラクチャのサイバーセキュリティ改善」との関係

米国の国家及び経済安全保障は、高い信頼性をもって重要インフラが機能することにかかっており、大統領命令 13636「重要インフラストラクチャのサイバーセキュリティ改善」[82]は NIST に対して、関係者と協働し、重要インフラへのサイバーリスクを減らすための自発的枠組み（フレームワーク）を構築するよう命じている。サイバーセキュリティフレームワーク（CSF）[83]は規格、ガイドライン及び最良規範からなり、重要インフラの保護を促進する。このフレームワークは、優先的で柔軟性があり、反復可能でパフォーマンス本位の、費用効果の高い取組により、重要インフラの所有者及び運用者が企業秘密、個人情報及び人権を保護しつつ、サイバーセキュリティ関連リスクを管理できるように支援する。最初の CSF は 2014 年 2 月に発表され、多様な部門や種々の運用環境に適用できるだけの柔軟性を備えた、国家レベルのフレームワークとなった。この CSF は、関係者からの情報を基に作成され、多種多様な部門における既存業務が、このフレームワーク内で利用できるようにした。
産業用制御システムのサイバーセキュリティ規格、ガイドライン及び規範を活用して、組織のリスク管理プログラムとの関係で CSF の機能を検討することができる。

The intended audience is varied and includes the following:

- Control engineers, integrators, and architects who design or implement secure ICS.
- System administrators, engineers, and other information technology (IT) professionals who administer, patch, or secure ICS.
- Security consultants who perform security assessments and penetration testing of ICS.
- Managers who are responsible for ICS.
- Senior management who are trying to understand implications and consequences as they justify and apply an ICS cybersecurity program to help mitigate impacts to business functionality.
- Researchers and analysts who are trying to understand the unique security needs of ICS.
- Vendors that are developing products that will be deployed as part of an ICS.

1.3 Document Structure

The remainder of this guide is divided into the following major sections:

- Section 2 provides an overview of ICS including a comparison between ICS and IT systems.
- Section 3 provides a discussion of ICS risk management and assessment.
- Section 4 provides an overview of the development and deployment of an ICS security program to mitigate the risk of the vulnerabilities identified in Appendix C.
- Section 5 provides recommendations for integrating security into network architectures typically found in ICS, with an emphasis on network segregation practices.
- Section 6 provides a summary of the management, operational, and technical controls identified in NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, and provides initial guidance on how these security controls apply to ICS.

The guide also contains several appendices with supporting material, as follows:

- Appendix A— provides a list of acronyms and abbreviations used in this document.
- Appendix B— provides a glossary of terms used in this document.
- Appendix C— provides a list of ICS threats, vulnerabilities and incidents.
- Appendix D— provides a list of ICS security activities.
- Appendix E— provides a list of ICS security capabilities and tools
- Appendix F— provides a list of references used in the development of this document.
- Appendix G— provides an ICS overlay, listing security controls, enhancements, and supplemental guidance that apply specifically to ICS.

所期の対象は多岐にわたるが、以下を含む。

- セキュアな ICS の設計又は実装に関わる制御エンジニア、インテグレータ及び設計者
- ICS の管理、パッチまたはセキュリティに携わるシステム管理者、エンジニアその他 IT 専門員
- ICS のセキュリティ評価及びペネトレーション・テストを行うセキュリティコンサルタント
- ICS 担当幹部
- 事業機能への影響を緩和する ICS サイバーセキュリティプログラムの承認・適用を行う際に、その意味と結果の理解に努める上級管理職
- ICS 独特のセキュリティニーズの理解に努める研究者及びアナリスト
- ICS の一部として展開される製品の開発に当たるベンダー

1.3 文書の構成

本ガイドのこれ以降の部分は、以下のセクションに大別される。

- セクション 2：ICS システムと IT システムの比較等、ICS の概要を示す。
- セクション 3：ICS のリスク管理とリスク評価について説明する。
- セクション 4：付録 C で明らかにされている脆弱性リスクを緩和する、ICS セキュリティプログラムの開発・展開について概要を示す。
- セクション 5：ICS の一般的なネットワークアーキテクチャにセキュリティを組み込む上での推奨事項を示す。特にネットワーク隔離規範について特筆する。
- セクション 6：NISTSP800-53『連邦情報システム・組織のセキュリティ・プライバシー管理』に定める管理・運用・技術制御をとりまとめ、このようなセキュリティ管理を ICS に適用する方法について初期のガイダンスを示す。

また本ガイドには、補足資料を提供する以下の付録も含まれる。

- 付録 A−本書で使用する頭字語及び略語のリスト
- 付録 B−本書で使用する用語集
- 付録 C−ICS の脅威、脆弱性及びインシデントリスト
- 付録 D−ICS セキュリティ活動リスト
- 付録 E−ICS セキュリティ能力・ツールリスト
- 付録 F−本書の作成時に使用した参考文献リスト
- 付録 G−ICS に特化して適用されるセキュリティ管理、拡張及び補足ガイダンスリストを掲載した ICS オーバーレイ

2. Overview of Industrial Control Systems

Industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy). The part of the system primarily concerned with producing the output is referred to as the process. The control part of the system includes the specification of the desired output or performance. Control can be fully automated or may include a human in the loop. Systems can be configured to operate open-loop, closed-loop, and manual mode. In open-loop control systems the output is controlled by established settings. In closed-loop control systems, the output has an effect on the input in such a way as to maintain the desired objective. In manual mode the system is controlled completely by humans. The part of the system primarily concerned with maintaining conformance with specifications is referred to as the controller (or control). A typical ICS may contain numerous control loops, Human Machine Interfaces (HMIs), and remote diagnostics and maintenance tools built using an array of network protocols. ICS control industrial processes are typically used in electrical, water and wastewater, oil and natural gas, chemical, transportation, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods) industries.

ICS are critical to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems. It is important to note that approximately 85 percent of the nation's critical infrastructures are privately owned and operated[1]. Federal agencies also operate many of the industrial processes mentioned above as well as air traffic control. This section provides an overview of SCADA, DCS, and PLC systems, including typical topologies and components. Several diagrams are presented to depict the network topology, connections, components, and protocols typically found on each system to facilitate the understanding of these systems. These examples only attempt to identify notional topology concepts. Actual implementations of ICS may be hybrids that blur the line between DCS and SCADA systems. Note that the diagrams in this section do not focus on securing ICS. Security architecture and security controls are discussed in Section 5 and Section 6 of this document respectively.

2.1 Evolution of Industrial Control Systems

Many of today's ICS evolved from the insertion of IT capabilities into existing physical systems, often replacing or supplementing physical control mechanisms. For example, embedded digital controls replaced analog mechanical controls in rotating machines and engines. Improvements in cost-and performance have encouraged this evolution, resulting in many of today's "smart" technologies such as the smart electric grid, smart transportation, smart buildings, and smart manufacturing. While this increases the connectivity and criticality of these systems, it also creates a greater need for their adaptability, resilience, safety, and security.

Engineering of ICS continues to evolve to provide new capabilities while maintaining the typical long lifecycles of these systems. The introduction of IT capabilities into physical systems presents emergent behavior that has security implications. Engineering models and analysis are evolving to address these emergent properties including safety, security, privacy, and environmental impact interdependencies.

[1] http://www.dhs.gov/critical-infrastructure-sector-partnerships (last updated April 2014)

2. 産業用制御システムの概要

産業用制御システム（ICS）とは、数種の制御システムを包括した汎用的な用語で、これには各種産業部門や重要インフラで使用されている SCADA、DCS、PLC、その他の制御システムの設定が含まれる。ICS は産業上の目的（物品やエネルギーの生産・輸送等）を達成するために併用される制御用コンポーネント（電気・機械・油圧・空気等）が組み合わさって構成されている。特に出力を産み出すシステムの一部をプロセスと呼ぶ。システムの制御部分には、所期の出力又はパフォーマンスの仕様が含まれる。制御は完全自動化が可能で、ループ中に人間が含まれる場合もある。システムはオープンループ、クローズドループ及び手動モードのいずれにも設定可能である。オープンループ制御システムでは、出力は設定した内容に従って制御される。クローズドループ制御システムでは、所期の目的を維持するように、出力が入力に影響を及ぼす。手動モードでは、人間が全面的にシステムを制御する。特に仕様を維持しようとするシステムの一部をコントローラ（又は制御）と呼ぶ。一般的な ICS には、多様なネットワークプロトコルを使用して構築された種々の制御ループ、マンマシンインタフェース（HMI）及びリモート診断保守ツールが含まれる。ICS の制御用産業プロセスは、一般に電気、上下水、石油、天然ガス、化学、輸送、医薬品、パルプ・製紙、食品・飲料及び組立製造（自動車、航空宇宙、耐久消費財等）業界で利用されている。

ICS は、高度に連携・相互依存したシステムとなる場合が多い、米国の重要インフラの運営に緊要な役割を果たしている。国の重要インフラのおよそ 85%は、私企業が保有し運営している点に注意すべきである。[2]連邦政府機関は、上記の産業用プロセスのほか航空交通管制でも多くの産業用プロセスを運用している。このセクションでは、一般的なトポロジーやコンポーネントを含め、SCADA、DCS 及び PLC システムについて概要を示す。これらシステムに対する理解を容易にするため、各システムの一般的なネットワークトポロジー、接続、コンポーネント及びプロトコルを図示する。このような例は、単に抽象的なトポロジー概念を明らかにするためのものである。ICS の実際の実装はハイブリッドで、DCS と SCADA の境界が曖昧である。本セクションの図は、ICS のセキュリティに特化したものではない。セキュリティアーキテクチャ及びセキュリティ管理については、セクション 5 とセクション 6 で取り上げる。

2.1 産業用制御システムの進化

今日の ICS の多くは、IT 能力を既存の物理システムに挿入したところから進化しており、物理制御メカニズムに代わるものや補完するものが多い。例えば、組込デジタル制御は、回転式機械やエンジンのアナログ式機械制御に取って代わった。コストパフォーマンスの改善がこの進化を促し、スマート配電網、スマート輸送、スマート建設、スパート製造等、今日の「スマート」テクノロジーをもたらした。これにより、これらシステムの接続性や重要性が増しただけでなく、その適応性、回復力、安全性及びセキュリティに対する多大な需要をも創出した。

ICS のエンジニアリングは引き続き進化しており、新たな能力を付与する一方、これらシステムの概して長いライフサイクルを維持している。IT 能力を物理システムに導入することは、セキュリティ上の意味を持つ新たな行動となっている。エンジニアリングモデル及び分析は進化の途上にあり、安全性、セキュリティ、プライバシー、環境影響といった相互依存性のある新たな属性を取り上げるようになっている。

[2] http://www.dhs.gov/critical-infrastructure-sector-partnerships（最終更新 2014 年 4 月）

2.2 ICS Industrial Sectors and Their Interdependencies

Control systems are used in many different industrial sectors and critical infrastructures, including manufacturing, distribution, and transportation.

2.2.1 Manufacturing Industries

Manufacturing presents a large and diverse industrial sector with many different processes, which can be categorized into *process-based* and *discrete-based* manufacturing.

The *process-based* manufacturing industries typically utilize two main processes [1]:

- **Continuous Manufacturing Processes.** These processes run continuously, often with transitions to make different grades of a product. Typical continuous manufacturing processes include fuel or steam flow in a power plant, petroleum in a refinery, and distillation in a chemical plant.
- **Batch Manufacturing Processes.** These processes have distinct processing steps, conducted on a quantity of material. There is a distinct start and end step to a batch process with the possibility of brief steady state operations during intermediate steps. Typical batch manufacturing processes include food manufacturing.

The *discrete-based* manufacturing industries typically conduct a series of steps on a single device to create the end product. Electronic and mechanical parts assembly and parts machining are typical examples of this type of industry.
Both process-based and discrete-based industries utilize the same types of control systems, sensors, and networks. Some facilities are a hybrid of discrete and process-based manufacturing.

2.2.2 Distribution Industries

ICS are used to control geographically dispersed assets, often scattered over thousands of square kilometers, including distribution systems such as water distribution and wastewater collection systems, agricultural irrigation systems, oil and natural gas pipelines, electrical power grids, and railway transportation systems.

2.2.3 Differences between Manufacturing and Distribution ICS

While control systems used in manufacturing and distribution industries are very similar in operation, they are different in some aspects. Manufacturing industries are usually located within a confined factory or plant-centric area, when compared to geographically dispersed distribution industries. Communications in manufacturing industries are usually performed using local area network (LAN) technologies that are typically more reliable and high speed as compared to the long-distance communication wide-area networks (WAN) and wireless/RF (radio frequency) technologies used by distribution industries. The ICS used in distribution industries are designed to handle long-distance communication challenges such as delays and data loss posed by the various communication media used. The security controls may differ among network types.

2.2.4 ICS and Critical Infrastructure Interdependencies

The U.S. critical infrastructure is often referred to as a “system of systems” because of the interdependencies that exist between its various industrial sectors as well as interconnections between business partners [8] [9]. Critical infrastructures are highly interconnected and mutually dependent in

2.2 ICS の産業部門とその相互依存性

制御システムは製造、物流、輸送等、種々の産業部門で使用され、重要なインフラとなっている。

2.2.1 製造業界

一口に製造といっても、多種多様な部門に様々なプロセスがあり、プロセス主体の製造と組立主体の製造に大別される。

プロセス主体の製造業界は、一般的に次の 2 つの主要プロセスを利用する[1]。

- **継続製造プロセス。**継続的に実施されるプロセスで、グレードが異なる単一の製品に移行することが多い。一般的な継続製造プロセスには、発電所の燃料や蒸気の流れ、製油所の石油、化学プラントの蒸留液が含まれる。
- **バッチ製造プロセス。**大量の資材に対して、明確に分かれたステップからなる。バッチプロセスには明確な開始ステップと終了ステップがあり、その中間においては短い定常状態の業務が行われる場合がある。一般的なバッチ製造プロセスには食品製造が含まれる。

組立主体の製造業界は、一般に単一のデバイスで一連のステップを実行し、最終製品を生み出す。

電子部品・機械部品の組立や部品の工作などはその典型である。

プロセス主体の業界も組立主体の業界も、同種の制御システム、センサ及びネットワークを使用する。施設によっては、両方の製造を同時に行う所もある。

2.2.2 配送業界

ICS は地理的に分散した資産の管理に使用され、ときには範囲が数千キロ平米にもなることがある。例えば上下水道、灌漑、石油・天然ガスパイプライン、送電網、鉄道等である。

2.2.3 製造 ICS と配送 ICS の相違

製造業界と配送業界の制御システムの業務はとてもよく似ているが、異なる面もいくつかある。製造業界は、通常閉鎖された工場やプラント中心の領域内にあるのに対し、配送業界は地理的に分散している。製造業界の通信は LAN を利用して通常行われる。これは配送業界が利用する長距離の WAN 及び無線 RF 技術に比べて、一般に信頼性も速度にも優れる。配送業界の ICS は、利用する種々の通信メディアに起因する遅延やデータ喪失といった長距離通信の諸問題に対処できるように設計される。セキュリティ管理は、ネットワークの種類に応じて異なる。

2.2.4 ICS と重要インフラの相互依存性

米国の重要インフラは、よく「複数のシステムからなるシステム」と呼ばれるが、理由は多種多様な業界・部門が相互に依存し合い、ビジネスパートナー同士が相互に関わり合っているからである[8] [9]。重要インフラは、物理的にも多数の情報・通信技術面でも、高度に相互連携し、複雑に相互依存し合っている。

complex ways, both physically and through a host of information and communications technologies. An incident in one infrastructure can directly and indirectly affect other infrastructures through cascading and escalating failures.

Both the electrical power transmission and distribution grid industries use geographically distributed SCADA control technology to operate highly interconnected and dynamic systems consisting of thousands of public and private utilities and rural cooperatives for supplying electricity to end users. Some SCADA systems monitor and control electricity distribution by collecting data from and issuing commands to geographically remote field control stations from a centralized location. SCADA systems are also used to monitor and control water, oil and natural gas distribution, including pipelines, ships, trucks, and rail systems, as well as wastewater collection systems.

SCADA systems and DCS are often networked together. This is the case for electric power control centers and electric power generation facilities. Although the electric power generation facility operation is controlled by a DCS, the DCS must communicate with the SCADA system to coordinate production output with transmission and distribution demands.

Electric power is often thought to be one of the most prevalent sources of disruptions of interdependent critical infrastructures. As an example, a cascading failure can be initiated by a disruption of the microwave communications network used for an electric power transmission SCADA system. The lack of monitoring and control capabilities could cause a large generating unit to be taken offline, an event that would lead to loss of power at a transmission substation. This loss could cause a major imbalance, triggering a cascading failure across the power grid. This could result in large area blackouts that could potentially affect oil and natural gas production, refinery operations, water treatment systems, wastewater collection systems, and pipeline transport systems that rely on the grid for electric power.

2.3 ICS Operation and Components

The basic operation of an ICS is shown in Figure 2-1 [2]. Some critical processes may also include safety systems. Key components include the following:

A typical ICS contains numerous control loops, human interfaces, and remote diagnostics and maintenance tools built using an array of network protocols on layered network architectures. A control loop utilizes sensors, actuators, and controllers (e.g., PLCs) to manipulate some controlled process. A sensor is a device that produces a measurement of some physical property and then sends this information as controlled variables to the controller. The controller interprets the signals and generates corresponding manipulated variables, based on a control algorithm and target set points, which it transmits to the actuators. Actuators such as control valves, breakers, switches, and motors are used to directly manipulate the controlled process based on commands from the controller.

Operators and engineers use human interfaces to monitor and configure set points, control algorithms, and to adjust and establish parameters in the controller. The human interface also displays process status information and historical information. Diagnostics and maintenance utilities are used to prevent, identify, and recover from abnormal operation or failures.

Sometimes these control loops are nested and/or cascading –whereby the set point for one loop is based on the process variable determined by another loop. Supervisory-level loops and lower-level loops operate continuously over the duration of a process with cycle times ranging on the order of milliseconds to minutes.

あるインフラのインシデントは、連鎖や障害のエスカレーションを通じて、他のインフラにも直接・間接に影響を及ぼす。

送電・配電業界では、いずれも地理的分散 SCADA 制御技術を使用して、エンドユーザに電気を供給するために、数千もの官民公共事業者及び地方協同組合からなる、高度に相互連携した動的システムを運用している。遠隔制御ステーションに対して一か所からコマンドを発行してデータを収集し、配電を監視・制御している SCADA もある。またパイプライン、船舶、トラック、鉄道、下水道等、水・石油・天然ガスの配送を監視・制御する SCADA もある。

SCADA と DCS はネットワーク化されていることが多い。電力制御センターと発電施設がその一例である。発電施設は DCS で制御されるが、DCS は SCADA と通信を行い、送電・配電需要に応じて生産出力を調整しなければならない。

電力は、相互依存し合った重要インフラの崩壊をもたらす、最も普及したソースの一つと考えられている。一例として、送電 SCADA 用のマイクロ波通信網が崩壊すれば、連鎖障害の引き金となり得る。監視・制御能力の欠如は、大型発電装置をオフラインにし、変電所の電力喪失に至りかねない。こうした喪失により大きな不均衡が生じ、電力網全体の連鎖障害の引き金となる。その結果広域停電が生じ、電力網に依存する石油・天然ガス生産、製油所業務、水処理システム、下水道及びパイプライン搬送システムにも影響が出よう。

2.3 ICS の操作及びコンポーネント

ICS の基本操作を図 2-1 に示す[2]。重要プロセスによっては、安全システムを含めるものもある。キーコンポーネントは以下のとおり。

一般的な ICS には数多くの制御ループ、ヒューマンインタフェースのほか、レイヤードネットワークアーキテクチャーの多様なネットワークプロトコルを利用して作成したリモート診断・保守ツールが含まれる。制御ループはセンサ、アクチュエータ及びコントローラ（PLC 等）を使用して、制御プロセスのいくつかを操作する。センサは特定の物理特性を計測し、その情報を制御変数としてコントローラに送信するデバイスである。コントローラは信号を解釈し、制御アルゴリズムと目標設定点を基に対応する操作変数を生成し、アクチュエータに送信する。アクチュエータはバルブ、ブレーカ、スイッチ、モータ等のことで、コントローラからのコマンドに従って制御プロセスを直接操作する。

操作員及びエンジニアはヒューマンインタフェースを利用し、設定点、制御アルゴリズムを監視・設定し、コントローラのパラメータを調整・設定する。

またヒューマンインタフェースはプロセスのステータス情報及び履歴情報を表示する。診断・保守ユーティリティは、異常操作や障害の防止、特定及び回復に利用される。

このような制御ループはネストやカスケードになっていることがあり、その場合、あるループの設定点は別のループにより決まるプロセス変数に依存する。監視レベルのループと低レベルループは 1 つのプロセス中継続的に機能し、サイクル時間はミリ秒から分単位までとなる。

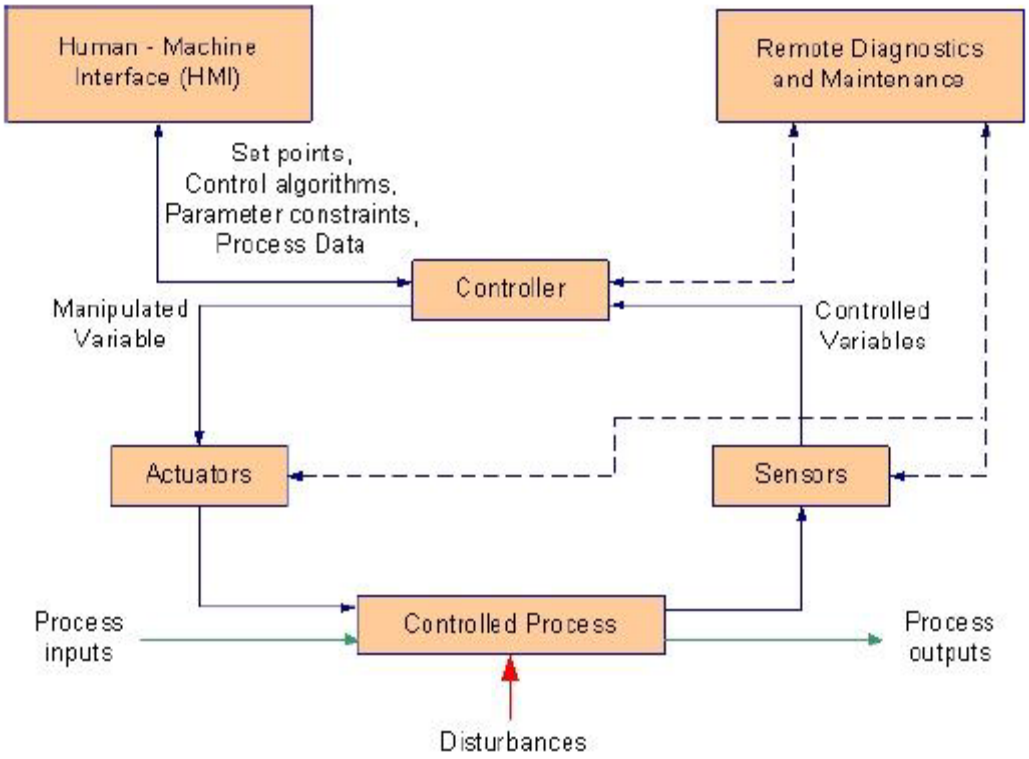

Figure 2-1. ICS Operation

To support subsequent discussions, this section defines key ICS components that are used in control and networking. Some of these components can be described generically for use in SCADA systems, DCS and PLCs, while others are unique to one. The Glossary of Terms in Appendix B— contains a more detailed listing of control and networking components. Additionally, Figure 2-5 and Figure 2-6 show SCADA implementation examples; Figure 2-7 shows a DCS implementation example and Figure 2-8 shows a PLC implementation example that incorporates these components.

2.3.1 ICS System Design Considerations

While Section 2.3 introduced the basic components of an ICS, the design of an ICS, including whether a SCADA, DCS, or PLC-based topologies are used depends on many factors. This section identifies key factors that drive design decisions regarding the control, communication, reliability, and redundancy properties of the ICS. Because these factors heavily influence the design of the ICS, they will also help determine the security needs of the system.

- **Control Timing Requirements.** ICS processes have a wide range of time-related requirements, including very high speed, consistency, regularity, and synchronization. Humans may not be able to reliably and consistently meet these requirements; automated controllers may be necessary. Some systems may require the computation to be performed as close to the sensor and actuators as possible to reduce communication latency and perform necessary control actions on time.

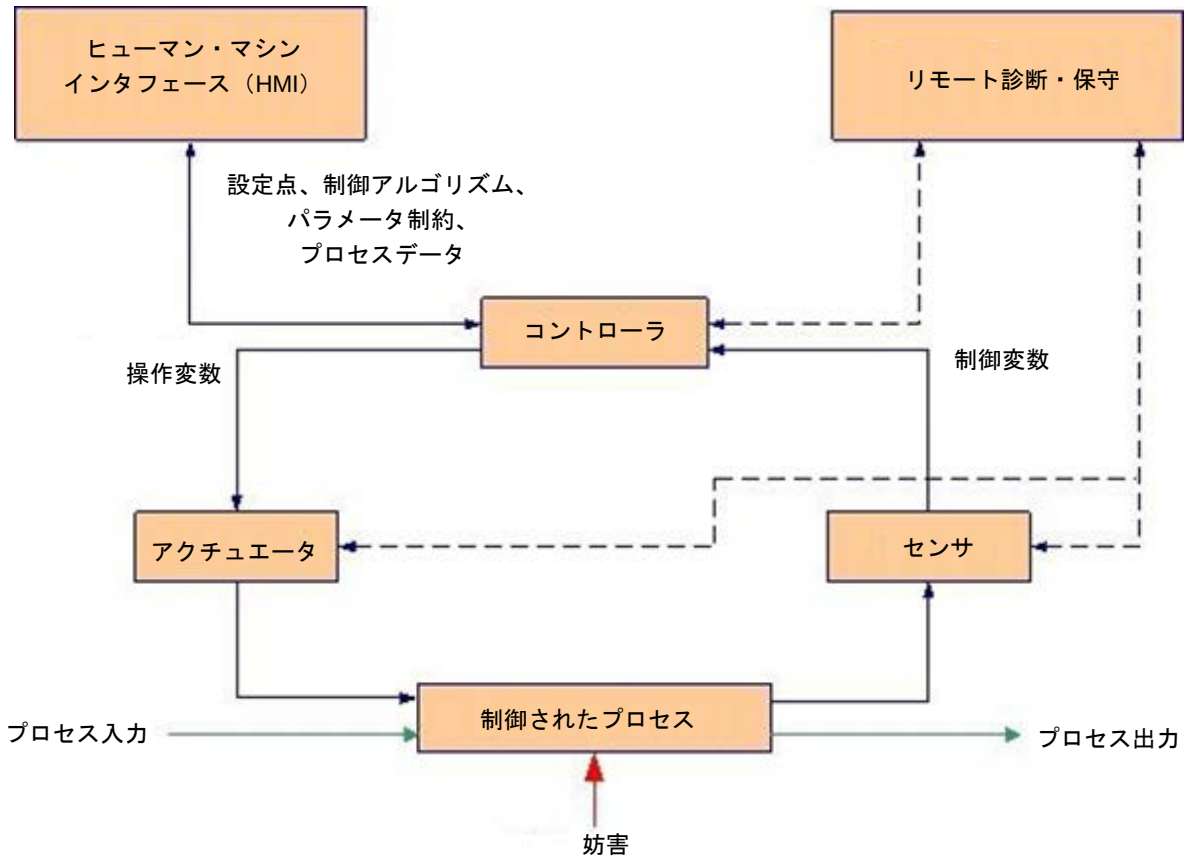

図 2-1.ICS の動作

以後の説明の便宜上、このセクションでは制御及びネットワークで使用する ICS のキーコンポーネントについて明らかにする。SCADA、DCS 及び PLC で汎用的に用いるものもあれば、どれか 1 つに特化しているものもある。付録 B の用語集には、制御コンポーネント及びネットワークコンポーネントの詳細なリストがある。また図 2-5 と図 2-6 には SCADA、図 2-7 には DCS、図 2-8 には PLC の実装例がそれぞれ示され、これらコンポーネントが組み込まれている。

2.3.1 ICS のシステム設計上の考慮事項

セクション 2.3 には ICS の基本コンポーネント、ICS の設計が紹介されており、SCADA、DCS、PLC のいずれに基づくトポロジーを使用すべきかは、多くの要因に依存する点も説明されている。このセクションでは、ICS の制御、通信、信頼性及び冗長特性に関する設計上の重要要因を明らかにする。そうした要因は ICS の設計に大きく影響するため、システムのセキュリティ需要を判定する上でも役立つ。

- **制御のタイミング要件。**ICS のプロセスには、高速性、一貫性、規則性、同期性等、広範な時間関連の要件がある。人間はこうした要件に対して、高い信頼性と一貫性をもって応えることはできないため、自動コントローラが必要となる。システムによっては、通信の待ち時間を短縮し、必要な制御動作を時間どおりに行うため、センサとアクチュエータをできるだけ近づけて計算を行う必要が生じる。

- **Geographic Distribution.** Systems have varying degrees of distribution, ranging from a small system (e.g., local PLC-controlled process) to large, distributed systems (e.g., oil pipelines, electric power grid). Greater distribution typically implies a need for wide area (e.g., leased lines, circuit switching, and packet switching) and mobile communication.
- **Hierarchy.** Supervisory control is used to provide a central location that can aggregate data from multiple locations to support control decisions based on the current state of the system. Often a hierarchical/centralized control is used to provide human operators with a comprehensive view of the entire system.
- **Control Complexity.** Often control functions can be performed by simple controllers and preset algorithms. However, more complex systems (e.g., air traffic control) require human operators to ensure that all control actions are appropriate to meet the larger objectives of the system.
- **Availability.** The system's availability (i.e., reliability) requirements are also an important factor in design. Systems with strong availability/up-time requirements may require more redundancy or alternate implementations across all communication and control.
- **Impact of Failures.** The failure of a control function could incur substantially different impacts across domains. Systems with greater impacts often require the ability to continue operations through redundant controls, or the ability to operate in a degraded state. The design needs to address these requirements.
- **Safety.** The system's safety requirements area also an important factor in design. Systems must be able to detect unsafe conditions and trigger actions to reduce unsafe conditions to safe ones. In most safety-critical operations, human oversight and control of a potentially dangerous process is an essential part of the safety system.

2.3.2 SCADA Systems

SCADA systems are used to control dispersed assets where centralized data acquisition is as important as control [3] [4]. These systems are used in distribution systems such as water distribution and wastewater collection systems, oil and natural gas pipelines, electrical utility transmission and distribution systems, and rail and other public transportation systems. SCADA systems integrate data acquisition systems with data transmission systems and HMI software to provide a centralized monitoring and control system for numerous process inputs and outputs. SCADA systems are designed to collect field information, transfer it to a central computer facility, and display the information to the operator graphically or textually, thereby allowing the operator to monitor or control an entire system from a central location in near real time. Based on the sophistication and setup of the individual system, control of any individual system, operation, or task can be automatic, or it can be performed by operator commands.

Typical hardware includes a control server placed at a control center, communications equipment (e.g., radio, telephone line, cable, or satellite), and one or more geographically distributed field sites consisting of Remote Terminal Units (RTUs) and/or PLCs, which controls actuators and/or monitors sensors. The control server stores and processes the information from RTU inputs and outputs, while the RTU or PLC controls the local process. The communications hardware allows the transfer of information and data back and forth between the control server and the RTUs or PLCs. The software is programmed to tell the system what and when to monitor, what parameter ranges are acceptable, and what response to initiate when parameters change outside acceptable values. An Intelligent Electronic Device (IED), such as a protective relay, may communicate directly to the control server, or a local RTU may poll the IEDs to collect the data and pass it to the control server. IEDs provide a direct interface to control and monitor equipment and sensors. IEDs may be directly polled and controlled by the control server and in most

- **地理的な分散。**システムの分散の程度は、小規模なシステム（ローカル PLC 制御プロセス等）から大規模な分散システム（石油パイプライン、電力網等）まで多岐にわたる。分散の程度が大きくなれば、通常広域になり（回線リース、回路切替、パケット切替等）、移動通信が必要となる。
- **階層。**監視制御を利用して、複数所在地のデータを一か所から収集し、システムの現状に基づいて制御の決定に役立てることができる。階層・集中管理を利用して、システム全体を包括的に見ながら人間が操作を行うことが多い。
- **制御の複雑性。**制御は単純なコントローラとプリセットアルゴリズムで行われることが多い。しかし、より複雑なシステム（航空交通管制等）では、全ての制御行為が適正で、より大きなシステム目標に合致させるため、操作員が必要となる。
- **可用性。**システムの可用性（すなわち信頼性）要件も、設計における重要要因となる。高い可用性/アップタイム要件を持ったシステムには、通信及び制御全般を通じていっそうの冗長性や代替実装が必要となる。
- **障害の影響。**制御機能の障害は、かなり多様な影響を全領域にもたらしかねない。影響度の大きいシステムには、冗長制御や退化状態での運用能力を通じて、運用を継続する能力が求められることが多い。設計ではそうした要件を考慮に入れる必要がある。
- **安全性。**システムの安全性要件も設計の重要要素となる。不安全状態を検知して、安全状態に近づけることが求められる。最も安全性が求められる運用では、潜在的に危険なプロセスに対する人間の監視・制御が安全性システムの不可欠部分となる。

2.3.2 SCADA

SCADA は、集中データ取得が制御と同様に重要な場合に、分散化された資産を制御するために使用する[3] [4]。上下水道、石油・天然ガスパイプライン、送電・配電システム、鉄道その他の公共輸送といった配送システムに使用されている。SCADA は、データ取得システムをデータ送信システムおよび HMI ソフトウエアと統合し、多数のプロセスのインプットとアウトプットのための集中的監視・制御システムとなる。SCADA は、現場の情報を収集して中央コンピュータ施設へ転送し、情報を図形やテキスト形式で操作員に表示し、システム全体をほとんどリアルタイムに一か所から監視・制御できるようにする。個々のシステムを洗練化して設定することにより、個々のシステム、動作又はタスクを自動化したり、オペレータのコマンドで実行したりすることができる。

一般的なハードウエアとしては、コントロールセンターに設置されたコントロールサーバ、通信装置（無線、電話回線、ケーブル、サテライト等）のほか、遠隔端末装置（RTU）又は PLC で構成された 1 か所又は複数の地理的に分散された現場が含まれ、アクチュエータやセンサを監視する。コントロールサーバは、RTU の入出力情報を保存・処理し、RTU 又は PLC はローカルプロセスを制御する。通信ハードウエアは、コントロールサーバと RTU 又は PLC 間の情報転送とデータの送受信を実現する。ソフトウエアはプログラム可能で、監視対象と時期、受入れられるパラメータの範囲、パラメータが範囲を逸脱した場合に取るべき対処を決定する。保護リレー等のインテリジェント電子デバイス（IED）が直接コントロールサーバと通信を行うか、ローカル RTU が IED にポーリングしてデータを収集し、それをコントロールサーバに渡す。IED は、装備品及びセンサの制御・監視の直接的なインタフェースとなる。またコントロールサーバから直接ポーリングと制御を受け、ほとんどの場合、コントロールセンターから直接指示を受けずに IED を操作するローカルプログラミングを有する。

cases have local programming that allows for the IED to act without direct instructions from the control center. SCADA systems are usually designed to be fault-tolerant systems with significant redundancy built into the system. Redundancy may not be a sufficient countermeasure in the face of malicious attack.

Figure 2-2 shows the components and general configuration of a SCADA system. The control center houses a control server and the communications routers. Other control center components include the HMI, engineering workstations, and the data historian, which are all connected by a LAN. The control center collects and logs information gathered by the field sites, displays information to the HMI, and may generate actions based upon detected events. The control center is also responsible for centralized alarming, trend analyses, and reporting. The field site performs local control of actuators and monitors sensors (Note that sensors and actuators are only shown in Figure 2-5). Field sites are often equipped with a remote access capability to allow operators to perform remote diagnostics and repairs usually over a separate dial up modem or WAN connection. Standard and proprietary communication protocols running over serial and network communications are used to transport information between the control center and field sites using telemetry techniques such as telephone line, cable, fiber, and radio frequency such as broadcast, microwave and satellite.

SCADA communication topologies vary among implementations. The various topologies used, including point-to-point, series, series-star, and multi-drop [5], are shown in Figure 2-3.

Point-to-point is functionally the simplest type; however, it is expensive because of the individual channels needed for each connection. In a series configuration, the number of channels used is reduced; however, channel sharing has an impact on the efficiency and complexity of SCADA operations. Similarly, the series-star and multi-drop configurations' use of one channel per device results in decreased efficiency and increased system complexity.

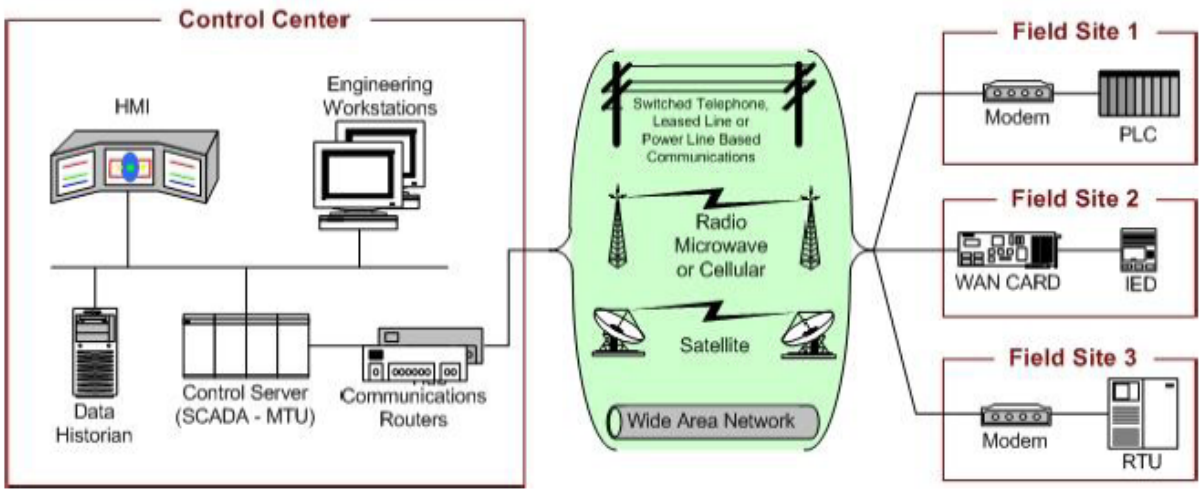

Figure 2-2. SCADA System General Layout

通常、SCADA は、フォールトトレラントシステムで、相当の冗長性が組込まれている。冗長性は、悪意ある攻撃に対しては十分な対策になり得ないことがある。

図 2-2 は SCADA のコンポーネントと全体構成を示す。コントロールセンターには、コントロールサーバと通信ルータが設置される。コントロールセンターのその他のコンポーネントには HMI、エンジニアリングワークステーション及びデータヒストリアンが含まれ、みな LAN で繋がっている。コントロールセンターは、現場サイトが収集した情報を収集・記録し、HMI に表示し、検知したイベントに応じてアクションを生成する。また集中アラーム、トレンド分析及び報告も担当する。現場サイトはアクチュエータのローカル制御を行い、センサを監視する（センサ及びアクチュエータは図 2-5 にのみ示される）。現場サイトは、操作員がリモート診断や修理を行えるようにリモートアクセス能力を備えたものが多く、通常は独立したダイアルアップモデムや WAN 接続を利用している。シリアル通信及びネットワーク通信で使用する標準プロトコル及び専用プロトコルは、コントロールセンターと現場サイト間での情報通信に利用され、この通信は、電話回線、ケーブル、ファイバー、無線周波数（ブロードキャスト、マイクロ波、サテライト等）といったテレメトリ技術を利用して行う。

SCADA 通信トポロジーは、実装によって様々に異なっている。2 地点間、シリーズ、シリーズスター、マルチドロップ[5]等の、利用される様々なトポロジーを図 2-3 に示す。

2 地点間は機能的に最も単純であるが、接続ごとにそれぞれのチャンネルが必要であることからコスト高になる。シリーズ構成では、チャンネル数が少なくてすむが、チャンネルを共有するため、SCADA の動作の効率と複雑さに影響する。
同様にシリーズスター及びマルチドロップ構成では、デバイスごとに 1 チャンネルを使用するため、効率が低下し、システムが複雑になる。

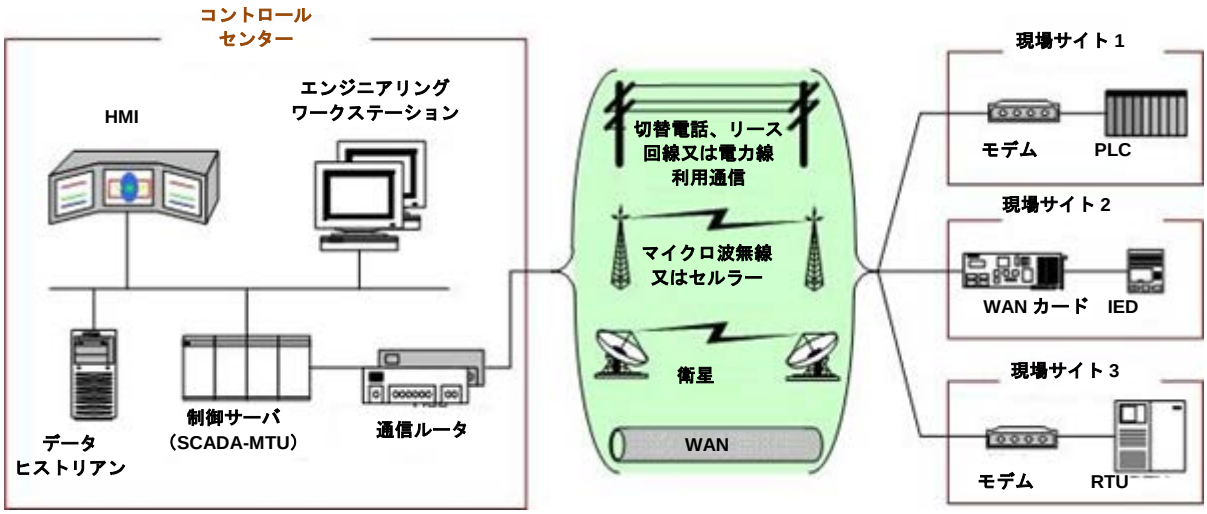

図 2-2.SCADA の全般レイアウト

The four basic topologies Figure 2-3 can be further augmented using dedicated devices to manage communication exchanges as well as message switching and buffering. Large SCADA systems containing hundreds of RTUs often employee a sub-control server to alleviate the burden on the primary server. This type of topology is shown in Figure 2-4.

Figure 2-5 shows an example of a SCADA system implementation. This particular SCADA system consists of a primary control center and three field sites. A second backup control center provides redundancy in the event of a primary control center malfunction. Point-to-point connections are used for all control center to field site communications, with two connections using radio telemetry. The third field site is local to the control center and uses the WAN for communications. A regional control center resides above the primary control center for a higher level of supervisory control. The corporate network has access to all control centers through the WAN, and field sites can be accessed remotely for troubleshooting and maintenance operations. The primary control center polls field devices for data at defined intervals (e.g., 5 seconds, 60 seconds) and can send new set points to a field device as required. In addition to polling and issuing high-level commands, the control server also watches for priority interrupts coming from field site alarm systems.

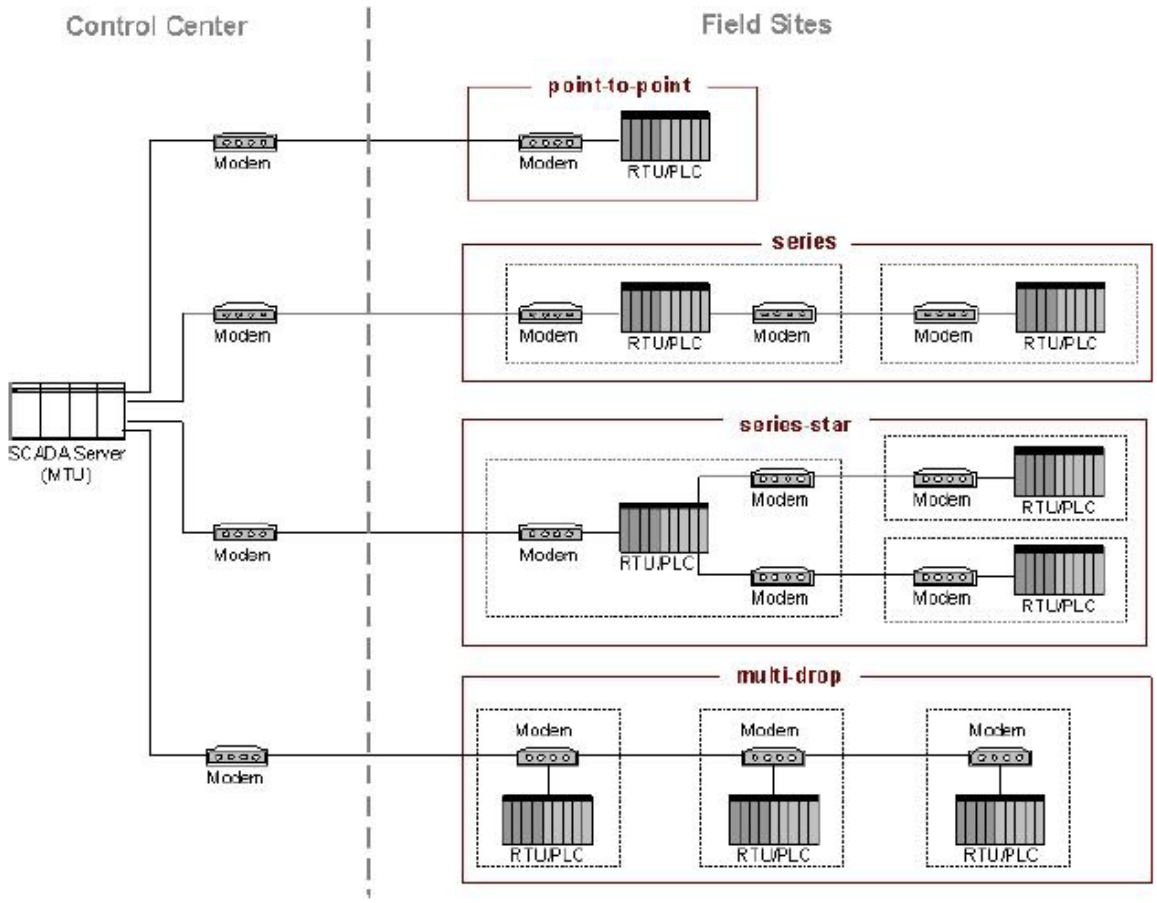

Figure 2-3. Basic SCADA Communication Topologies

図 2-3 の 4 つの基本トポロジーは、専用デバイスを使用して更に増やし、通信交換、メッセージ切替、バッファリングを管理することができる。数百の RTU を持つ大規模 SCADA は、サブコントロールサーバを採用し、プライマリサーバの負荷を軽減していることが多い。この種のトポロジーは図 2-4 に示す。

図 2-5 は SCADA の実装例である。この特殊な SCADA は、プライマリコントロールセンターと 3 つの現場サイトで構成される。2 番目のバックアップコントロールセンターは、プライマリコントロールセンターが不具合を起こしている場合に冗長性を発揮する。2 地点間接続は、全てのコントロールセンターと現場サイト間の通信に使用し、無線テレメトリによる接続が 2 つになっている。3 番目の現場サイトはコントロールセンターに対してローカルで、WAN 接続を利用する。地域コントロールセンターはプライマリコントロールセンターの上位にあり、より高位の監視制御を行う。企業ネットワークは WAN 経由でコントロールセンターにアクセスし、現場サイトは、リモートアクセスによりトラブルシューティングと保守作業を行えるようになっている。プライマリコントロールセンターは、指定された間隔（5 秒、60 秒等）で現場のデバイスにデータのポーリングを行い、必要に応じて新たな設定点を現場のデバイスに送信する。ポーリングとハイレベルコマンドの発行に加えて、コントロールサーバは、現場サイトのアラームシステムから送られる優先中断の監視も行う。

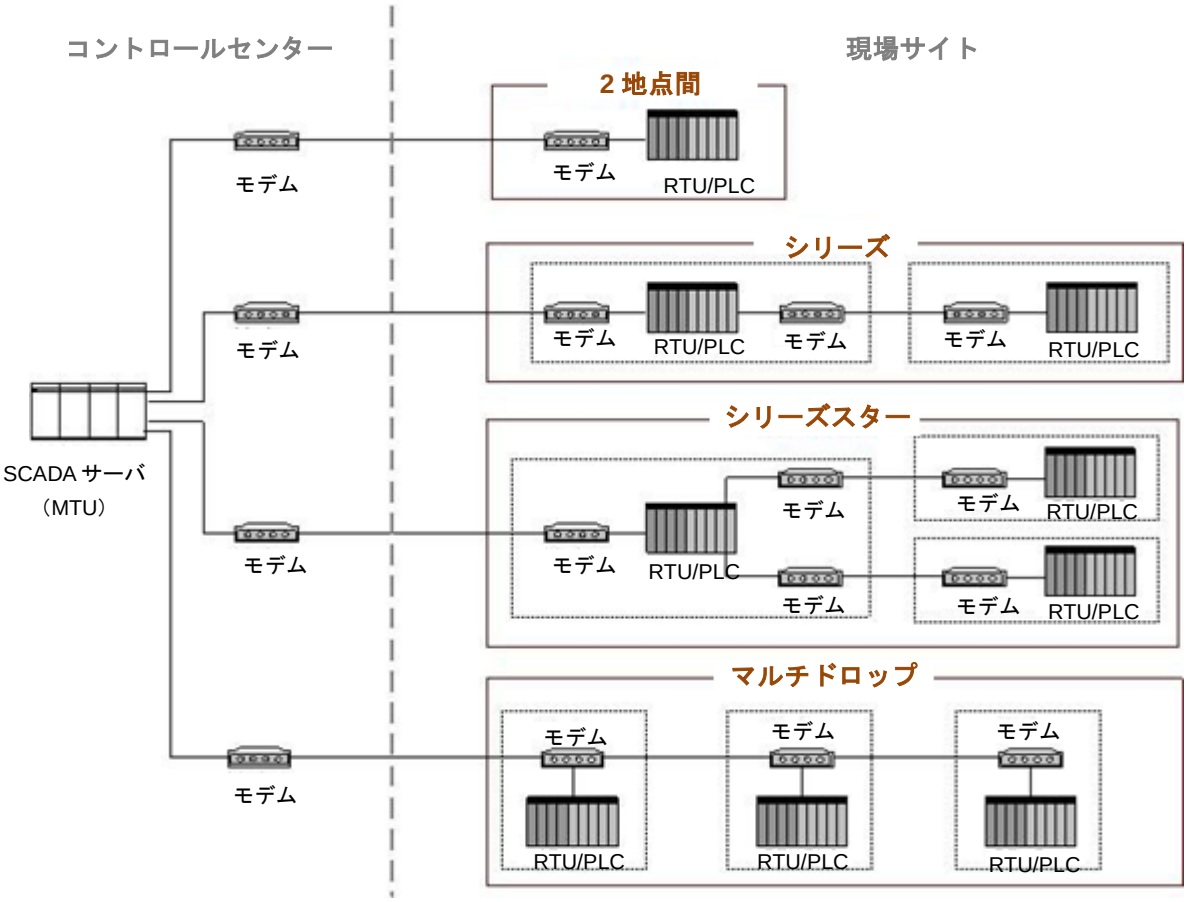

図 2-3.　基本的 SCADA 通信トポロジー

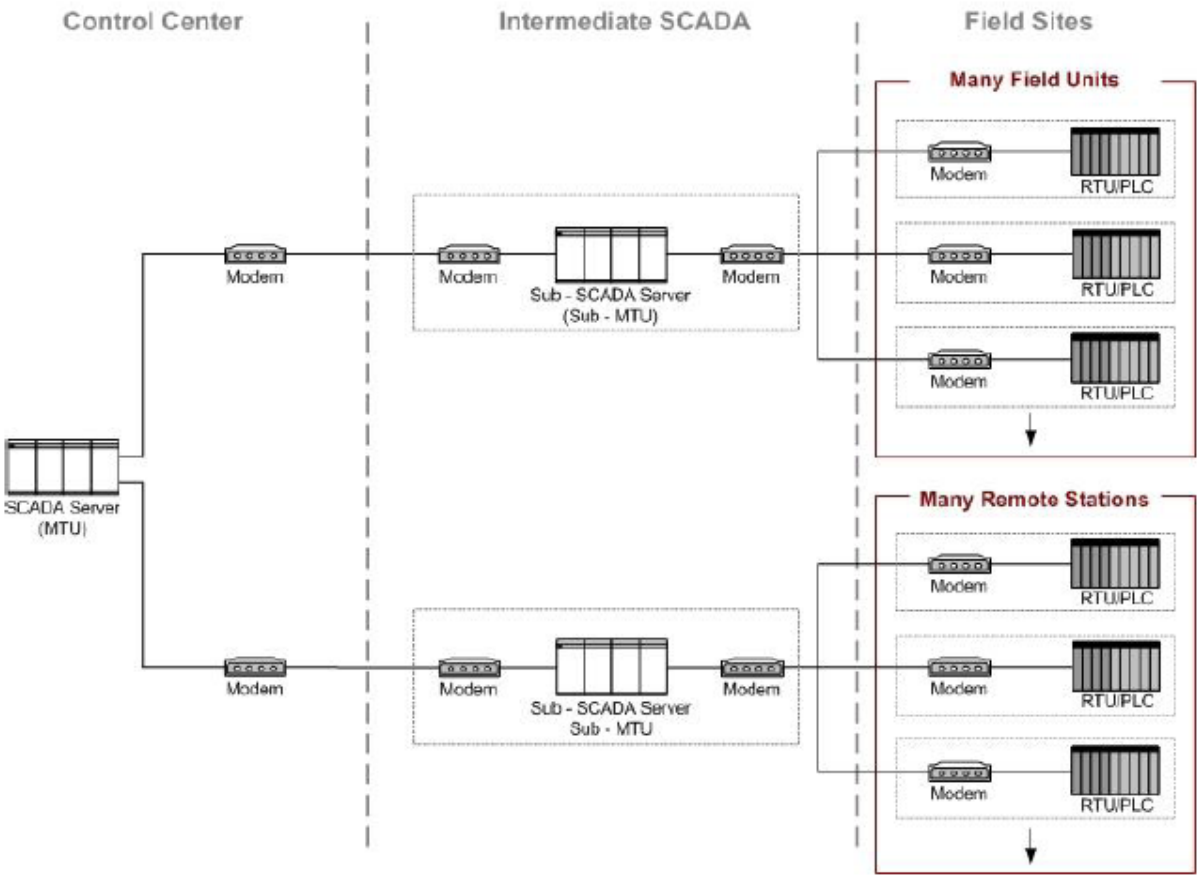

Figure 2-4. Large SCADA Communication Topology

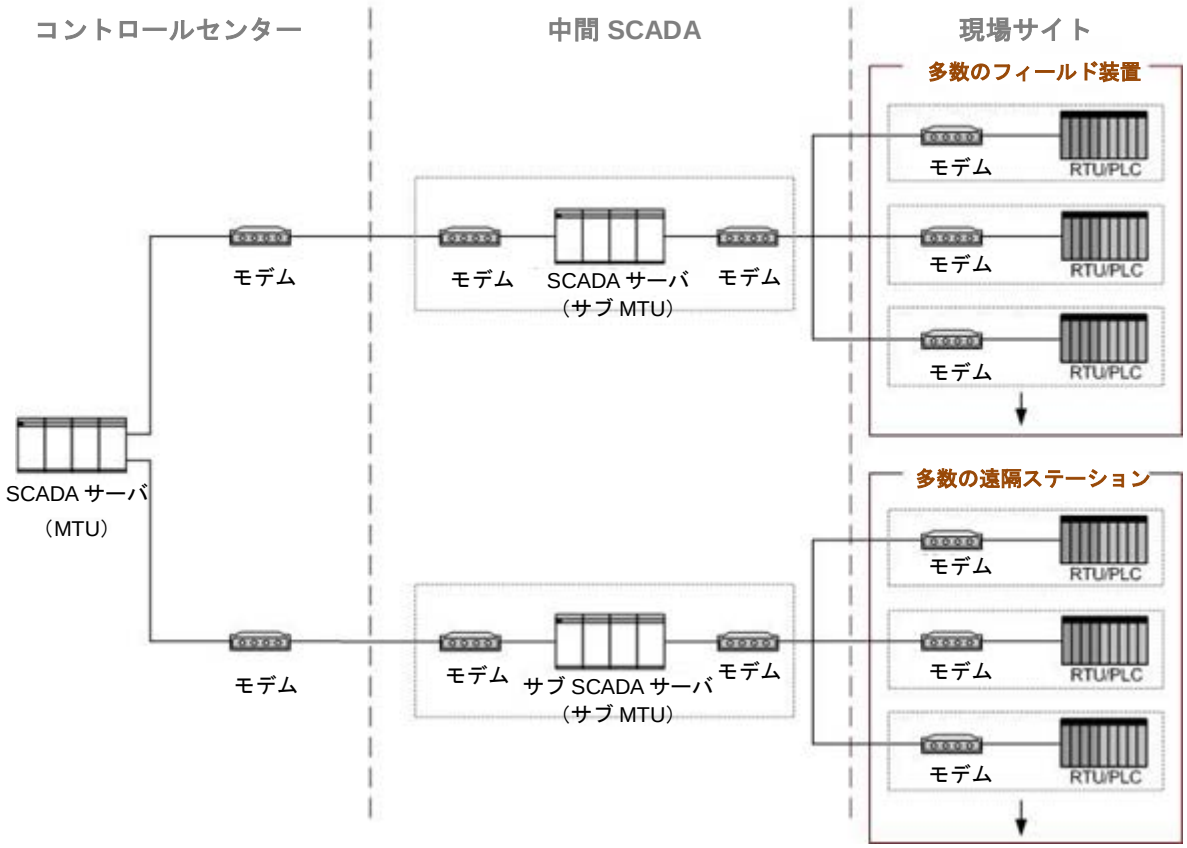

図 2-4. 大規模 SCADA 通信トポロジー

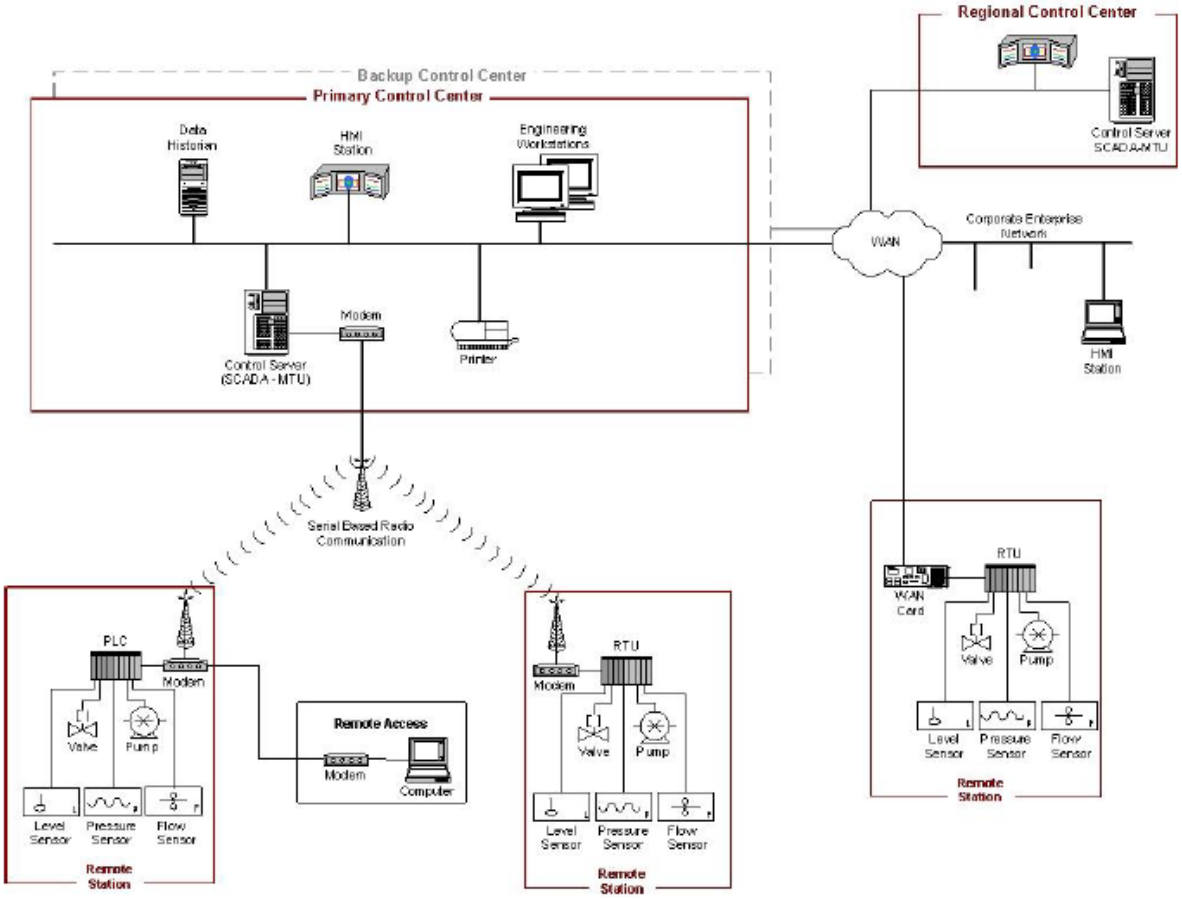

Figure 2-5. SCADA System Implementation Example (Distribution Monitoring and Control)

Figure 2-6 shows an example implementation for rail monitoring and control. This example includes a rail control center that houses the SCADA system and three sections of a rail system. The SCADA system polls the rail sections for information such as the status of the trains, signal systems, traction electrification systems, and ticket vending machines. This information is also fed to operator consoles at the HMI station within the rail control center. The SCADA system also monitors operator inputs at the rail control center and disperses high-level operator commands to the rail section components. In addition, the SCADA system monitors conditions at the individual rail sections and issues commands based on these conditions (e.g., stopping a train to prevent it from entering an area that has been determined to be flooded or occupied by another train based on condition monitoring).

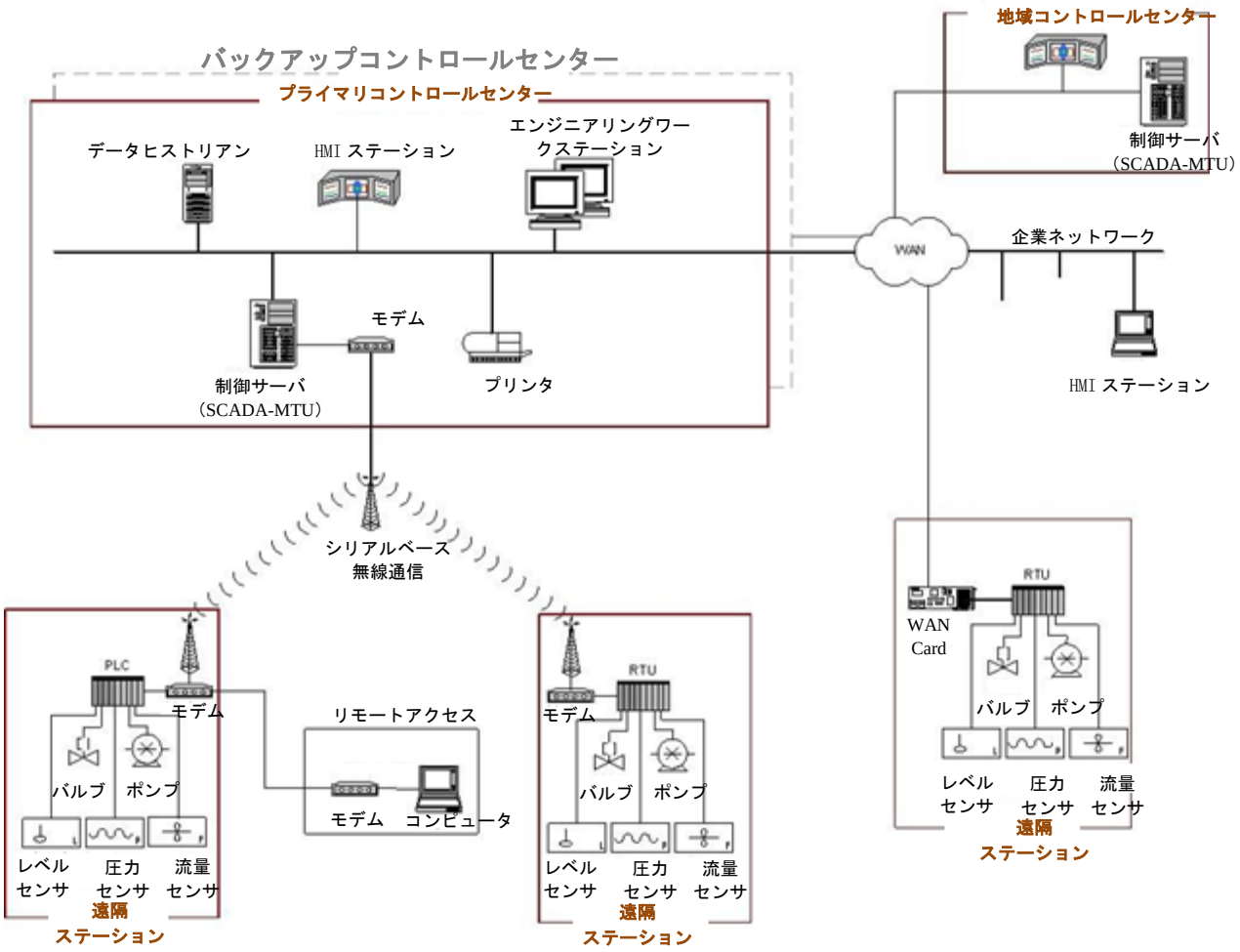

図 2-5.　SCADA の実装例（分散監視・制御）

図 2-6 は、鉄道監視・制御の実装例である。この例では、SCADA と鉄道システムの 3 セクションを有する鉄道制御センターが含まれる。SCADA は鉄道のセクションに対し、列車の状態、信号装置、牽引帯電装置、乗車券販売機等の情報のポーリングを行う。この情報は、鉄道制御センター内にある HMI ステーションの操作員コンソールにも供給される。また SCADA は、鉄道制御センターにおける操作員の入力情報も監視し、上位の操作員コマンドを鉄道セクションコンポーネントに発行する。加えて、個々の鉄道セクションにおける状態を監視し、それに応じてコマンドを発行する（状態監視に基づき、洪水と判定される地区やほかの列車がいる地区に進入しないように列車を停止させるなど）。

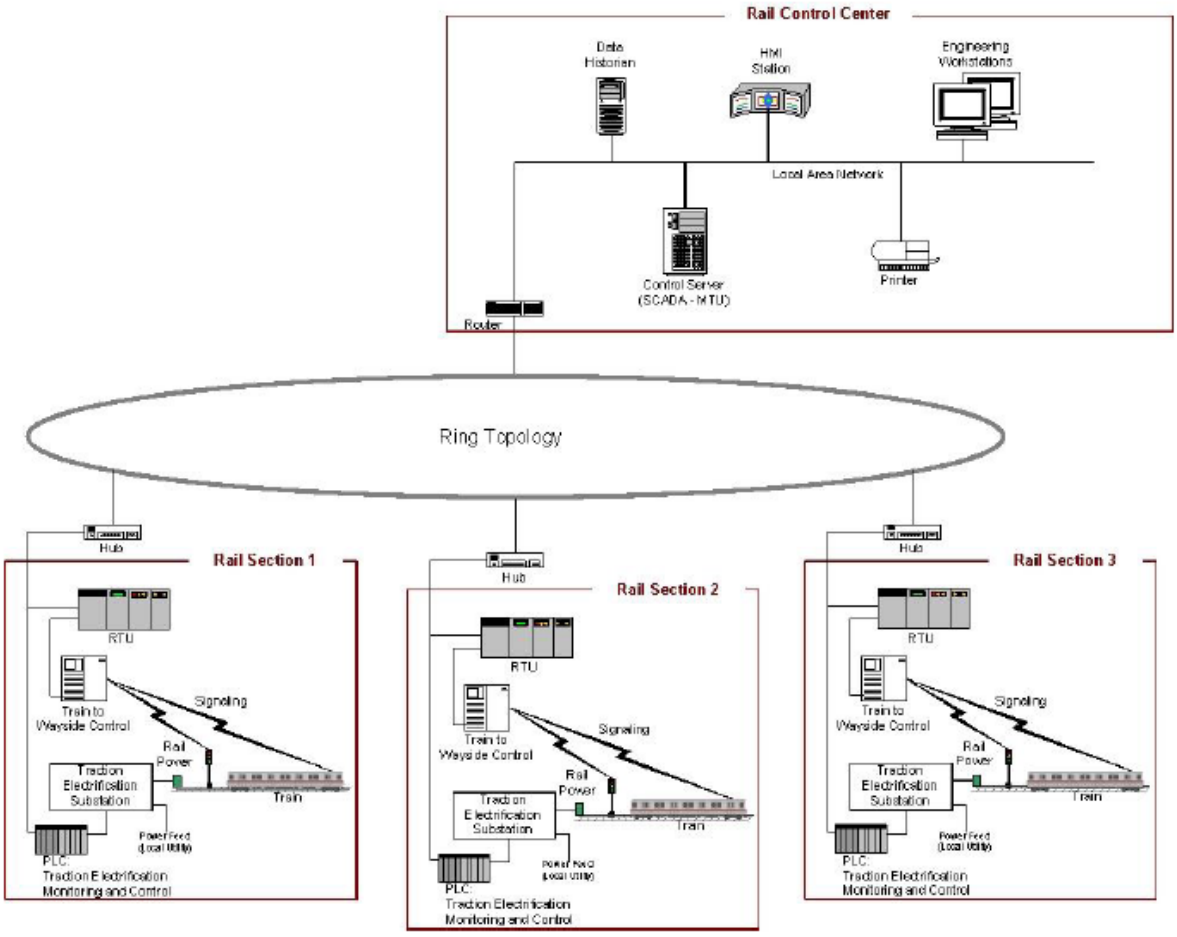

Figure 2-6. SCADA System Implementation Example (Rail Monitoring and Control)

2.3.3 Distributed Control Systems

DCS are used to control production systems within the same geographic location for industries such as oil refineries, water and wastewater treatment, electric power generation plants, chemical manufacturing plants, automotive production, and pharmaceutical processing facilities. These systems are usually process control or discrete part control systems.

DCS are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated sub-systems that are responsible for controlling the details of a localized process. A DCS uses a centralized supervisory control loop to mediate a group of localized controllers that share the overall tasks of carrying out an entire production process [6]. Product and process control are usually achieved by deploying feedback or feedforward control loops whereby key product and/or process conditions are automatically maintained around a desired set point. To accomplish the desired product and/or process tolerance around a specified set point, specific process controllers, or more capable PLCs, are employed in the field and are tuned to provide the desired tolerance as well as the rate of self-correction during process upsets. By modularizing the production system, a DCS reduces the impact of a single fault on the

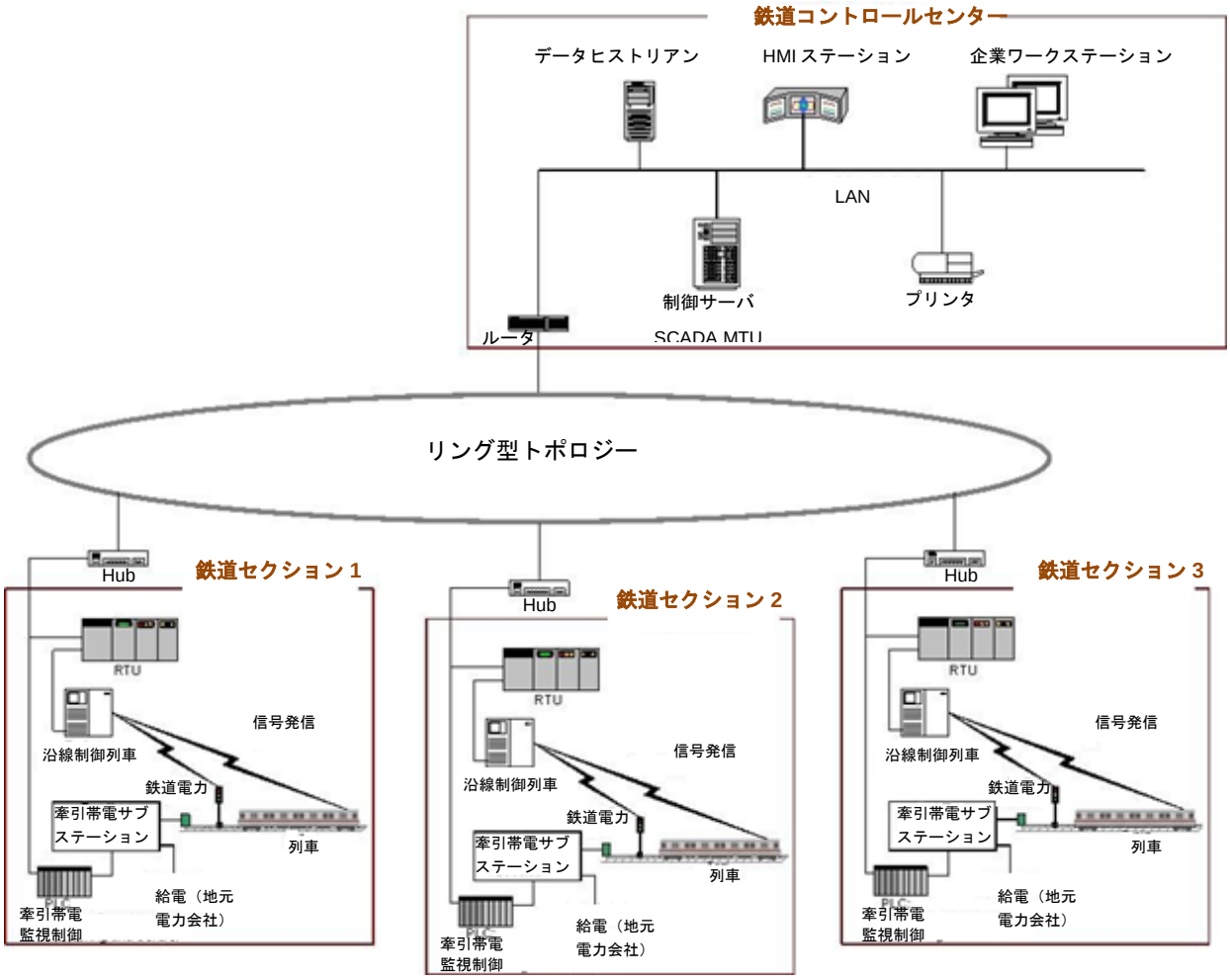

図 2-6. SCADA の実装例（列車監視・制御）

2.3.3　分散制御システム

DCS は地理的に同じ場所にある生産システムの制御に使用され、石油精製、上下水道処理、発電所、化学プラント、自動車生産、医薬品処理施設等が含まれる。このようなシステムは、通常プロセス制御システムや個別部品制御システムである。

DCS は、局在プロセスの細部を制御する複数の統合サブシステムに対する、監視レベルでの制御を含めた制御アーキテクチャとして統合される。DCS は集中監視・制御ループを利用して、生産プロセス全体の実行に関わる全タスクを共有する局在コントローラの 1 グループを仲介する[6]。製品・プロセス制御は、通常フィードバック/フィードフォワード制御ループを展開して行い、重要な製品やプロセスの状態は、所望の設定点付近に自動的に保たれる。所望の製品やプロセスの許容誤差を指定された設定点付近に保つため、特殊プロセスコントローラ又はより高性能の PLC を現場に採用して調整し、プロセス不調時に所望の許容誤差内に収まるようにしたり、自己補正率を設定したりしている。生産システムをモジュール化することで、DCS は、単一の障害がシステム全体に与える影響を減らす。

overall system. In many modern systems, the DCS is interfaced with the corporate network to give business operations a view of production.

An example implementation showing the components and general configuration of a DCS is depicted in Figure 2-7. This DCS encompasses an entire facility from the bottom-level production processes up to the corporate or enterprise layer. In this example, a supervisory controller (control server) communicates to its subordinates via a control network. The supervisor sends set points to and requests data from the distributed field controllers. The distributed controllers control their process actuators based on control server commands and sensor feedback from process sensors.

Figure 2-7 gives examples of low-level controllers found on a DCS system. The field control devices shown include a PLC, a process controller, a single loop controller, and a machine controller. The single loop controller interfaces sensors and actuators using point-to-point wiring, while the other three field devices incorporate fieldbus networks to interface with process sensors and actuators. Fieldbus networks eliminate the need for point-to-point wiring between a controller and individual field sensors and actuators. Additionally, a fieldbus allows greater functionality beyond control, including field device diagnostics, and can accomplish control algorithms within the fieldbus, thereby avoiding signal routing back to the PLC for every control operation. Standard industrial communication protocols designed by industry groups such as Modbus and Fieldbus [7] are often used on control networks and fieldbus networks.

In addition to the supervisory-level and field-level control loops, intermediate levels of control may also exist. For example, in the case of a DCS controlling a discrete part manufacturing facility, there could be an intermediate level supervisor for each cell within the plant. This supervisor would encompass a manufacturing cell containing a machine controller that processes a part and a robot controller that handles raw stock and final products. There could be several of these cells that manage field-level controllers under the main DCS supervisory control loop.

最近のシステムには、DCS と企業ネットワークのインタフェースを確保して、事業業務に生産的な観点を付与しているものが少なくない。

図 2-7 は、コンポーネントと DCS の一般的な構成の例を示す。この DCS では、生産プロセスの底辺から企業層に至る全ての施設が収められている。この例では、監視コントローラ（制御サーバ）が制御ネットワークを介して、従属層と通信を行うようになっている。スーパーバイザは、分散フィールドコントローラへの設定点とそこからの要求を送信する。分散コントローラは、制御サーバのコマンド及びプロセスセンサからのセンサフィードバックを基に、プロセスアクチュエータを制御する。

図 2-7 は、DCS システムに見られる低レベルコントローラの例である。フィールドコントローラデバイスには、PLC、プロセスコントローラ、単一ループコントローラ及びマシンコントローラが配置されている。単一ループコントローラは、2 地点間配線によりセンサとアクチュエータのインタフェースとなり、それ以外の 3 種類のデバイスは、フィールドバスネットワークを使用して、プロセスセンサとアクチュエータのインタフェースを確保している。フィールドバスネットワークには、コントローラと個々のフィールドセンサやアクチュエータ間の 2 地点間配線が不要である。またフィールドバスは、フィールドデバイスの診断など、制御以上の機能を発揮するほか、フィールドバス内で制御アルゴリズムを実現し、制御操作のたびに信号を PLC に返す必要がない。制御ネットワークやフィールドバスネットワークでは、Modbus and Fieldbus [7]等の業界グループが設計した標準的な通信プロトコルが多用される。

監視レベル及びフィールドレベルでの制御ループのほかに、中間レベルの制御もある。例えば、部品組立製造施設を制御する DCS の場合、プラント内のセルごとに中間レベルのスーパーバイザを配置することがある。このスーパーバイザは製造セルを包含し、製造セルには（部品を処理する）マシンコントローラと（原料在庫と最終製品を扱う）ロボットコントローラが含まれる。このようなセルがいくつかあるものもあり、各セルはメイン DCS 監視制御ループの下で、フィールドレベルのコントローラを管理する。

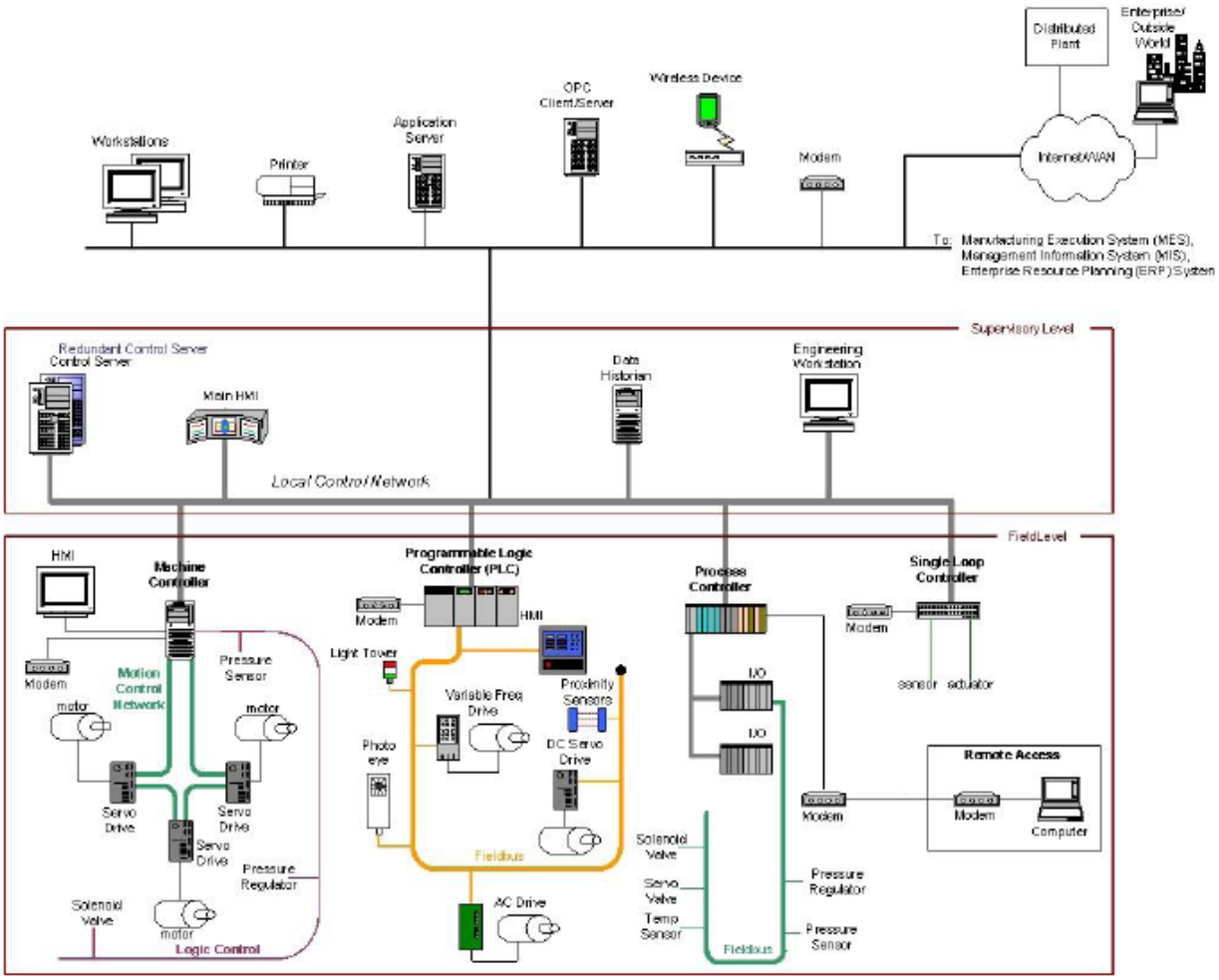

Figure 2-7. DCS Implementation Example

2.3.4 Programmable Logic Controller Based Topologies

PLCs are used in both SCADA and DCS systems as the control components of an overall hierarchical system to provide local management of processes through feedback control as described in the sections above. In the case of SCADA systems, they may provide the same functionality of RTUs. When used in DCS, PLCs are implemented as local controllers within a supervisory control scheme.

In addition to PLC usage in SCADA and DCS, PLCs are also implemented as the primary controller in smaller control system configurations to provide operational control of discrete processes such as automobile assembly lines and power plant soot blower controls These topologies differ from SCADA and DCS in that they generally lack a central control server and HMI and, therefore, primarily provide closed-loop control without direct human involvement. PLCs have a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode proportional-integral-derivative (PID) control, communication, arithmetic, and data and file processing.

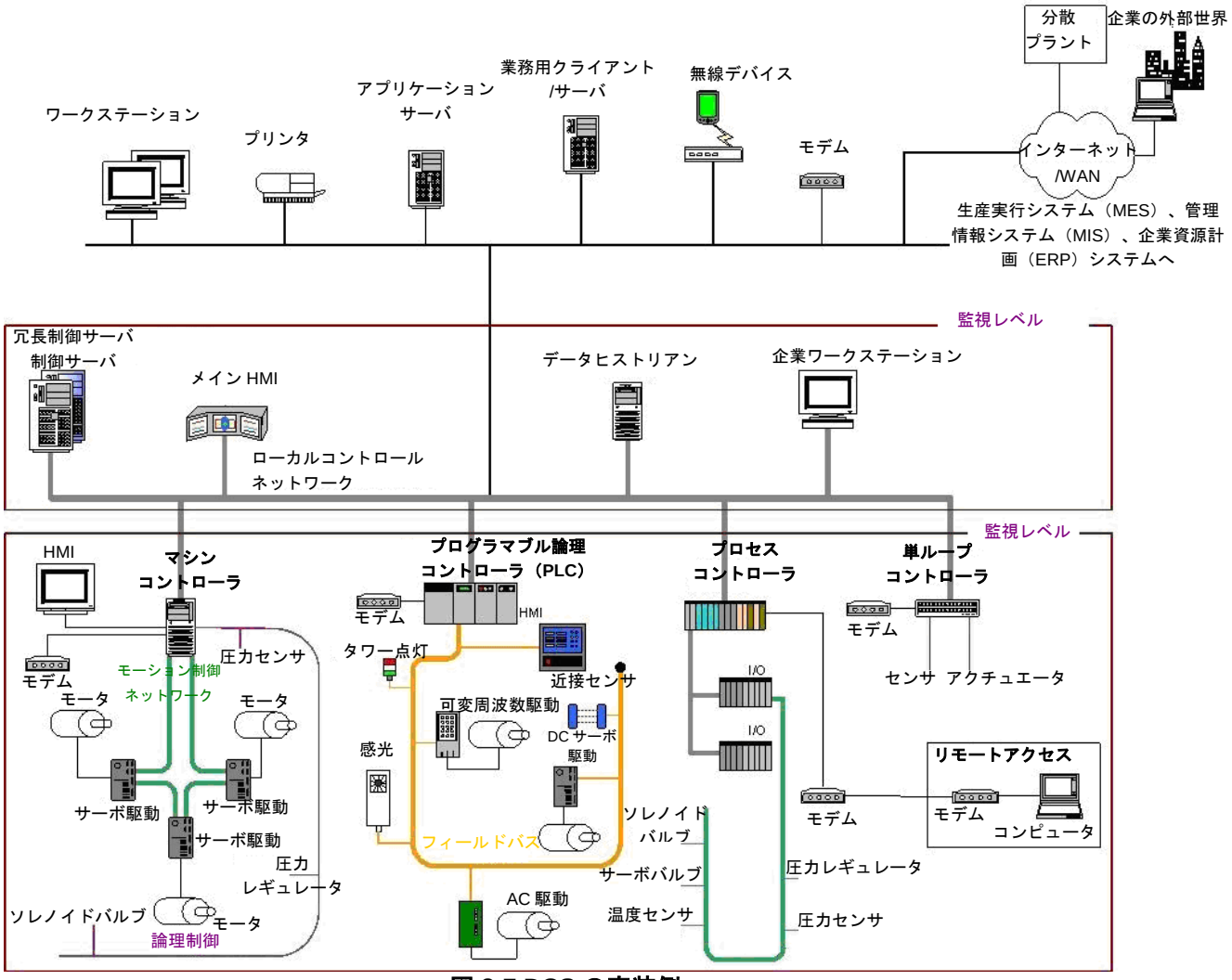

図 2-7.DCS の実装例

2.3.4　プログラム可能論理コントローラベースのトポロジー

PLC は SCADA と DCS の両システムにおいて、階層システム全体の制御コンポーネントとして使用され、前述のとおり、フィードバック制御を通じてプロセスのローカル管理を行う。SCADA の場合、RTU と同様の機能を発揮する。DCS で使用される場合、PLC は監視・制御におけるローカルコントローラとして実装される。

SCADA と DCS で使用されるほか、PLC はより小規模の制御システム構成におけるプライマリコントローラとしても利用され、自動車組立ライン等の組立プロセスや発電所の煤煙ブロアーの制御など、操作を制御する。SCADA や DCS とのトポロジーの違いは、一般に中央制御サーバと HMI がないことで、そのため人間の直接的な介在なしに、主にクローズドループ制御を行っている。PLC にはユーザがプログラム可能なメモリがあり、I/O 制御、論理、タイミング、カウント、比例・積分・微分（PID）3 モード制御、通信、演算、データやファイルの処理等の具体的な機能を実装するための命令を格納する。

Figure 2-8 shows control of a manufacturing process being performed by a PLC over a fieldbus network. The PLC is accessible via a programming interface located on an engineering workstation, and data is stored in a data historian, all connected on a LAN.

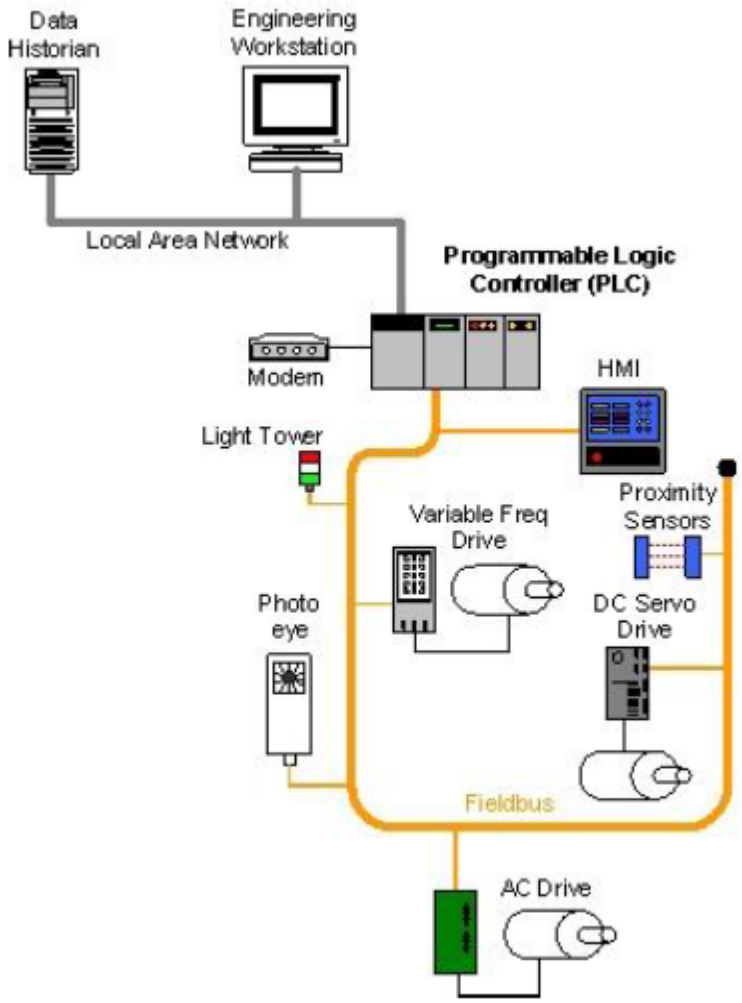

Figure 2-8. PLC Control System Implementation Example

図 2-8 は、フィールドバスネットワーク経由で PLC が実施する製造プロセス制御を示す。

PLC にはエンジニアリングワークステーション上のプログラミングインタフェースを介してアクセスでき、データはヒストリアンに保管され、全て LAN で接続されている。

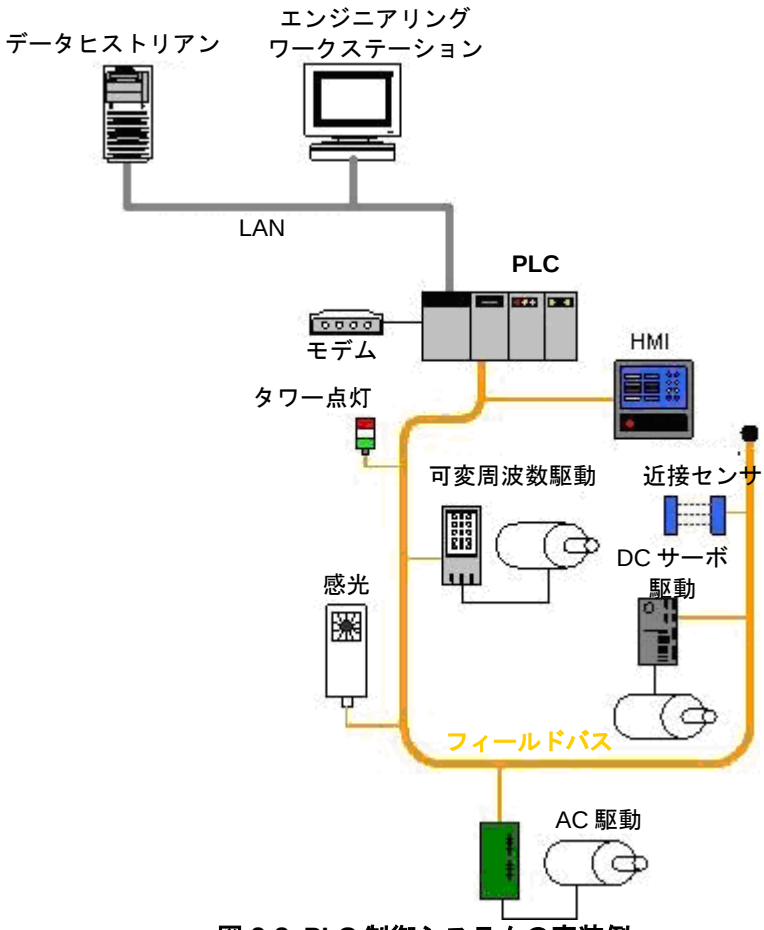

図 2-8. PLC 制御システムの実装例

2.4 Comparing ICS and IT Systems Security

ICS control the physical world and IT systems manage data. ICS have many characteristics that differ from traditional IT systems, including different risks and priorities. Some of these include significant risk to the health and safety of human lives, serious damage to the environment, and financial issues such as production losses, and negative impact to a nation's economy. ICS have different performance and reliability requirements, and also use operating systems and applications that may be considered unconventional in a typical IT network environment. Security protections must be implemented in a way that maintains system integrity during normal operations as well as during times of cyber attack [17].

Initially, ICS had little resemblance to IT systems in that ICS were isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low-cost Ethernet and Internet Protocol (IP) devices are now replacing the older proprietary technologies, which increases the possibility of cybersecurity vulnerabilities and incidents. As ICS are adopting IT solutions to promote corporate connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are starting to resemble IT systems. This integration supports new IT capabilities, but it provides significantly less isolation for ICS from the outside world than predecessor systems, creating a greater need to secure these systems. While security solutions have been designed to deal with these security issues in typical IT systems, special precautions must be taken when introducing these same solutions to ICS environments. In some cases, new security solutions are needed that are tailored to the ICS environment.

The environments in which ICS and IT systems operate are constantly changing. The environments of operation include, but are not limited to: the threat space; vulnerabilities; missions/business functions; mission/business processes; enterprise and information security architectures; information technologies; personnel; facilities; supply chain relationships; organizational governance/culture; procurement/acquisition processes; organizational policies/procedures; organizational assumptions, constraints, risk tolerance, and priorities/trade-offs).

The following lists some special considerations when considering security for ICS:

- **Timeliness and Performance Requirements.** ICS are generally time-critical, with the criterion for acceptable levels of delay and jitter dictated by the individual installation. Some systems require reliable, deterministic responses. High throughput is typically not essential to ICS. In contrast, IT systems typically require high throughput, and they can typically withstand some level of delay and jitter. For some ICS, automated response time or system response to human interaction is very critical. Some ICS are built on real-time operating systems (RTOS), where real-time refers to timeliness requirements. The units of real-time are very application dependent and must be explicitly stated.
- **Availability Requirements.** Many ICS processes are continuous in nature. Unexpected outages of systems that control industrial processes are not acceptable. Outages often must be planned and scheduled days or weeks in advance. Exhaustive pre-deployment testing is essential to ensure high availability (i.e., reliability) for the ICS. Control systems often cannot be easily stopped and started without affecting production. In some cases, the products being produced or equipment being used is more important than the information being relayed. Therefore, the use of typical IT strategies such as rebooting a component, are usually not acceptable solutions due to the adverse impact on the requirements for high availability, reliability and maintainability of the ICS. Some ICS employ redundant components, often running in parallel, to provide continuity when primary components are unavailable.

2.4 ICS システムと IT システムのセキュリティ比較

ICS は物理的世界を制御し、IT システムはデータを管理する。ICS は従来の IT システムとは異なる特徴が多く、リスクも優先度も異なる。中には人の健康や安全に大きなリスクとなり、環境を損ない、生産喪失等の財政問題となり、国家経済に悪影響を及ぼすものもある。ICS の性能及び信頼性要件は異なっており、普通の IT ネットワーク環境では奇異に見える OS やアプリケーションを使用する。セキュリティの保護は、正常運用時にもサイバー攻撃の際にもシステム保全を維持できるように実装しなければならない。[17]

当初 ICS は、特殊なハードウエアとソフトウエアを使用して専用制御プロトコルを実行する隔絶されたシステムだったため、IT システムとは類似点がほとんどなかった。昨今、広く利用可能な低コストのイーサネットやインターネットプロトコル（IP）デバイスが旧式の専用技術に取って代わりつつあることから、サイバーセキュリティの脆弱性やインシデントが生じる蓋然性が高まっている。ICS は IT ソリューションを採用して、企業の接続性やリモートアクセス能力を促進しており、また、業界標準コンピュータ、オペレーティングシステム（OS）及びネットワークプロトコルを使用するように設計・実装されるようになっている。このため ICS は次第に IT システムと類似性を持つようになってきた。このような統合化は新たな IT 能力をサポートするが、それ以前のシステムに比べると、外界からの隔絶性が格段に劣るため、セキュリティの必要性が増す。
セキュリティソリューションは、一般的な IT システムにおけるセキュリティ問題を扱うようにできているが、こうした同じソリューションを ICS 環境に持ち込む場合には特別な注意が欠かせない。場合によっては、その ICS 環境に特化した新しいセキュリティソリューションが必要となる。

ICS システムと IT システムの動作環境は絶えず変化している。例えば、脅威空間、脆弱性、任務・ビジネス機能、任務・ビジネスプロセス、企業・情報セキュリティアーキテクチャ、情報技術、人事、施設、サプライチェーンの関係、組織のガバナンス/カルチャー、調達・取得プロセス、組織の方針・手順、組織の前提事項、制約、リスク許容度、優先度/トレードオフ等がある。

ICS のセキュリティを検討する際の特別な考慮事項を以下に列挙する。

- **適時性要件と性能要件。**ICS は緊急を要するものが多く、遅延やジッターの許容度基準が個々の装置に応じて定められている。信頼性の高い決定論的応答を求めるシステムもある。高いスループットは一般に ICS には必須でない。反対に IT システムでは通常、高いスループットが求められ、ある程度の遅延やジッターは許容される。ある種の ICS では、人の相互作用に対する自動応答時間やシステム応答は非常に重要となる。リアルタイムオペレーティングシステム（RTOS）上に構築される ICS もあり、ここでいうリアルタイムが適時性要件となる。リアルタイムの単位はアプリケーションに依存し、明示的に示す必要がある。
- **可用性要件。**ICS プロセスの多くは、その性質上継続的である。産業プロセスを制御しているシステムの予定外の停止は受け入れられるものではない。停止の多くは、数日又は数週間前にあらかじめ計画・予定されたものでなければならない。ICS の高い可用性（すなわち信頼性）を確保するには、徹底的な展開前試験の実施が不可欠となる。生産に影響を及ぼすことなく、制御システムの停止・開始を容易に実行できることは少ない。生産中の製品や使用中の装備品の方が、伝達する情報よりも重要というケースもある。したがって、コンポーネントのリブートといった一般的な IT 戦略の利用は、ICS の高い可用性・信頼性・保守性要件に悪影響を及ぼすため、通常受け入れられる解決策とはならない。ICS では冗長コンポーネントを採用して同時運用することが多く、プライマリコンポーネントが利用できない場合の継続性を確保している。

- **Risk Management Requirements.** In a typical IT system, data confidentiality and integrity are typically the primary concerns. For an ICS, human safety and fault tolerance to prevent loss of life or endangerment of public health or confidence, regulatory compliance, loss of equipment, loss of intellectual property, or lost or damaged products are the primary concerns. The personnel responsible for operating, securing, and maintaining ICS must understand the important link between safety and security. Any security measure that impairs safety is unacceptable.
- **Physical Effects.** ICS field devices (e.g., PLC, operator station, DCS controller) are directly responsible for controlling physical processes. ICS can have very complex interactions with physical processes and consequences in the ICS domain that can manifest in physical events. Understanding these potential physical effects often requires communication between experts in control systems and in the particular physical domain.
- **System Operation.** ICS operating systems (OS) and control networks are often quite different from IT counterparts, requiring different skill sets, experience, and levels of expertise. Control networks are typically managed by control engineers, not IT personnel. Assumptions that differences are not significant can have disastrous consequences on system operations.
- **Resource Constraints.** ICS and their real time OSs are often resource-constrained systems that do not include typical contemporary IT security capabilities. Legacy systems are often lacking resources common on modern IT systems. Many systems may not have desired features including encryption capabilities, error logging, and password protection. Indiscriminate use of IT security practices in ICS may cause availability and timing disruptions. There may not be computing resources available on ICS components to retrofit these systems with current security capabilities. Adding resources or features may not be possible.
- **Communications.** Communication protocols and media used by ICS environments for field device control and intra-processor communication are typically different from most IT environments, and may be proprietary.
- **Change Management.** Change management is paramount to maintaining the integrity of both IT and control systems. Unpatched software represents one of the greatest vulnerabilities to a system. Software updates on IT systems, including security patches, are typically applied in a timely fashion based on appropriate security policy and procedures. In addition, these procedures are often automated using server-based tools. Software updates on ICS cannot always be implemented on a timely basis. These updates need to be thoroughly tested by both the vendor of the industrial control application and the end user of the application before being implemented. Additionally, the ICS owner must plan and schedule ICS outages days/weeks in advance. The ICS may also require revalidation as part of the update process. Another issue is that many ICS utilize older versions of operating systems that are no longer supported by the vendor. Consequently, available patches may not be applicable. Change management is also applicable to hardware and firmware. The change management process, when applied to ICS, requires careful assessment by ICS experts (e.g., control engineers) working in conjunction with security and IT personnel.
- **Managed Support.** Typical IT systems allow for diversified support styles, perhaps supporting disparate but interconnected technology architectures. For ICS, service support is sometimes via a single vendor, which may not have a diversified and interoperable support solution from another vendor. In some instances, third-party security solutions are not allowed due to ICS vendor license and service agreements, and loss of service support can occur if third party applications are installed without vendor acknowledgement or approval.

- **リスク管理要件。**一般的な IT システムでは、通常データの機密性と保全が主要関心事となる。ICS では、人命の喪失、公衆衛生・国民の信頼の危機、遵法、装備品の損失、知的財産の損失、製品の損害を防止するための人的安全性とフォールトトレランスが主要関心事である。ICS の運用・セキュリティ・保守担当者は、安全性とセキュリティの重要な関係を理解しなければならない。いかなるセキュリティ対策も、安全性を阻害するのであれば受け入れられない。
- **物理的影響。**ICS のフィールドデバイス（PLC、オペレータステーション、DCS コントローラ等）は、物理的プロセスを直接制御している。ICS と物理的プロセスとの相互作用は極めて複雑で、ICS 領域における結果は物理的イベントとして明らかになる。このような物理的影響を理解するには、制御システムの専門員と特定の物理的領域の専門員同士のコミュニケーションが必要となる場合が多い。
- **システム運用。**ICS の OS と制御ネットワークは、IT の場合と全く異なることが多く、求められるスキル、経験、専門知識レベルも異なる。制御ネットワークは、通常、IT 職員ではなく制御エンジニアが管理している。大きな違いはないという認識でいると、システム運用に悲惨な結果を招きかねない。
- **リソースの制約。**ICS とそのリアルタイム OS はリソース制約のあるシステムであることが多く、これには最近の一般的なセキュリティ機能は含まれない。レガシーシステムには、最近の IT システムと共通のリソースがない。暗号化機能、エラーログ、パスワード保護といった望ましい機能が付いていないシステムも多い。ICS における IT セキュリティの規範を見境なく使用すると、可用性やタイミングに問題が起きかねない。このようなシステムに現行のセキュリティ機能を付与し、ICS コンポーネントに利用できるコンピューティングリソースはないであろう。リソースや機能の追加はできない。
- **通信。**フィールドデバイスの制御やプロセッサ内通信用に ICS 環境で使用される通信プロトコル及びメディアは、大抵の IT 環境とは異なり専用のものが多い。
- **管理変更。**管理変更は IT システムと制御システムの保全に肝要である。パッチを当てていないソフトウエアは、システムにとって最も脆弱な点の 1 つとなる。IT システムにおけるセキュリティパッチ等のソフトウエア更新は、適正なセキュリティポリシーと手順に従って、タイムリーに行われる。またこうした手順は、サーバベースのツールを使用して自動化されている場合が多い。ICS でのソフトウエア更新は、必ずしもタイムリーに行われるわけではない。更新の実行前に、産業用制御アプリケーションベンダーとアプリケーションのエンドユーザ双方による徹底的な試験が必要となる。また ICS 所有者は数日から数週間前に、あらかじめ停止の計画・予定を立てなければならない。また更新プロセスの一環として、再検証も必要となる。別の問題として、ベンダーがサポートを打ち切った OS の旧バージョンを使用する ICS が多いことが挙げられる。その結果、入手可能なパッチが適用できないことになる。管理変更は、ハードウエアやファームウエアにも当てはまる。変更管理のプロセスを ICS に適用する場合は、ICS 専門員（制御エンジニア等）がセキュリティ職員や IT 職員と連携して、慎重に評価を行う必要がある。
- **管理サポート。**一般的な IT システムでは種々のサポートスタイルが認められ、異なってはいても相互連接した技術アーキテクチャをサポートしている。ICS では、サービスサポートをベンダー1 社が担当し、ほかのベンダーからの多様で相互運用性のあるサポートソリューションが得られないことがある。また ICS ベンダーのライセンス・サービス契約により、サードパーティのセキュリティソリューションが認められない場合もあり、ベンダーの許可を得ずにサードパーティのアプリケーションをインストールすると、サービスサポートが解約になることもあり得る。

- **Component Lifetime.** Typical IT components have a lifetime on the order of 3 to 5 years, with brevity due to the quick evolution of technology. For ICS where technology has been developed in many cases for very specific use and implementation, the lifetime of the deployed technology is often in the order of 10 to 15 years and sometimes longer.
- **Component Location.** Most IT components and some ICS are located in business and commercial facilities physically accessible by local transportation. Remote locations may be utilized for backup facilities. Distributed ICS components may be isolated, remote, and require extensive transportation effort to reach. Component location also needs to consider necessary physical and environmental security measures.

Table 2-1 summarizes some of the typical differences between IT systems and ICS.

Table 2-1. Summary of IT System and ICS Differences

Category	Information Technology System	Industrial Control System
Performance Requirements	Non-real-time Response must be consistent High throughput is demanded High delay and jitter may be acceptable Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary for security	Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is not acceptable Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction
Availability (Reliability) Requirements	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated, depending on the system's operational requirements	Responses such as rebooting may not be acceptable because of process availability requirements Availability requirements may necessitate redundant systems Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing
Risk Management Requirements	Manage data Data confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Major risk impact is delay of business operations	Control physical world Human safety is paramount, followed by protection of the process Fault tolerance is essential, even momentary downtime may not be acceptable Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production
System Operation	Systems are designed for use with typical operating systems Upgrades are straightforward with the availability of automated deployment tools	Differing and possibly proprietary operating systems, often without security capabilities built in Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved
Resource Constraints	Systems are specified with enough resources to support the addition of third-party applications such as security solutions	Systems are designed to support the intended industrial process and may not have enough memory and computing resources to support the addition of security capabilities

- **コンポーネントの寿命。**一般に IT コンポーネントの寿命は 3～5 年で、技術進歩の速さから短命である。多くの場合、極めて特殊な使用と実装を目指して技術開発された ICS では、寿命は 10～15 年で、場合によってはそれ以上になる。
- **コンポーネントの所在場所。**ほとんどの IT コンポーネント及びある種の ICS コンポーネントは、地元の交通機関を利用して物理的に立入可能な事業・商用施設に置かれている。遠隔地はバックアップ施設として使用される。分散 ICS コンポーネントは隔絶され、離れているため、交通にかなりの労力が必要となる。またコンポーネントの所在場所は、物理的・環境的セキュリティ対策も考慮する必要がある。

表 2-1 は、IT システムと ICS との一般的な相違を取りまとめたものである。

表 2-1.IT システムと ICS の相違点

カテゴリ	情報（IT）システム	産業用制御システム（ICS）
性能要件	リアルタイム不要 応答は一貫していること ハイスループット必須 大きな遅延とジッターは許容 重要な緊急相互作用が少ないこと セキュリティに必要な程度に厳格なアクセス制限を実装できること	リアルタイム 応答は緊急を要する 中程度のスループットで可 大きな遅延やジッターは不可 人その他の緊急相互作用への応答が重要 ICS へのアクセスは厳重に制限されるが、マンマシンインタフェースを阻害・干渉しない
可用性（信頼性）用件	リブート等の応答は可 可用性の欠点はシステムの運用要件に応じて許容されることが多い	プロセスの可用性要件によりリブート等の応答は不可 可用性要件から冗長システムが必要となる場合あり 停止は数日又は数週間前にあらかじめ計画・予定 高可用性要件により徹底的な展開前試験が必要
リスク管理要件	データを管理 データの機密性と保全が肝要 フォールトトレランスはさほど重要でない（瞬時のダウンタイムは重大リスクでない） 重大なリスク影響は業務の遅延	物理世界の制御 人の安全が肝要、プロセスの保護はその次 フォールトトレランスが不可欠、瞬時のダウンタイムも不可 重大なリスク影響は法令不履行、環境への影響、人命・装備品・生産喪失
システム運用	システムは一般的 OS 上で使用 アップグレードは自動展開ツールを利用するので容易	まちまちで専用の OS を使用する場合あり、セキュリティ機能はないことが多い 専用制御アルゴリズムと修正済みハードウエア/ソフトウエアが関係するため、ソフトウエア変更は慎重を要し、通常ベンダーが担当
リソースの制約	システムはセキュリティソリューション等の追加サードパーティアプリケーションに対応する十分なリソースを適用	システムは所期の産業プロセスに対応するようにできており、追加セキュリティ機能に対応する十分なメモリや演算リソースはない

Category	Information Technology System	Industrial Control System
Communications	Standard communications protocols	Many proprietary and standard communication protocols
	Primarily wired networks with some localized wireless capabilities	Several types of communications media used including dedicated wire and wireless (radio and satellite)
	Typical IT networking practices	Networks are complex and sometimes require the expertise of control engineers
Change Management	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance. ICS may use OSs that are no longer supported
Managed Support	Allow for diversified support styles	Service support is usually via a single vendor
Component Lifetime	Lifetime on the order of 3 to 5 years	Lifetime on the order of 10 to 15 years
Components Location	Components are usually local and easy to access	Components can be isolated, remote, and require extensive physical effort to gain access to them

In summary, the operational and risk differences between ICS and IT systems create the need for increased sophistication in applying cybersecurity and operational strategies. A cross-functional team of control engineers, control system operators and IT security professionals needs to work closely to understand the possible implications of the installation, operation, and maintenance of security solutions in conjunction with control system operation. IT professionals working with ICS need to understand the reliability impacts of information security technologies before deployment. Some of the OSs and applications running on ICS may not operate correctly with commercial-off-the-shelf (COTS) IT cybersecurity solutions because of specialized ICS environment architectures.

2.5 Other Types of Control Systems

Although this guide provides guidance for securing ICS, other types of control systems share similar characteristics and many of the recommendations from this guide are applicable and could be used as a reference to protect such systems against cybersecurity threats. For example, although many building, transportation, medical, security and logistics systems use different protocols, ports and services, and are configured and operate in different modes than ICS, they share similar characteristics to traditional ICS [18]. Examples of some of these systems and protocols include:

Other Types of Control Systems

- Advanced Metering Infrastructure.
- Building Automation Systems.
- Building Management Control Systems.
- Closed-Circuit Television (CCTV) Surveillance Systems.
- CO2 Monitoring.
- Digital Signage Systems.
- Digital Video Management Systems.
- Electronic Security Systems.
- Emergency Management Systems.

カテゴリ	情報（IT）システム	産業用制御システム（ICS）
通信	標準通信プロトコル プライマリ有線ネットワークで局所的に無線機能あり 一般的 IT ネットワーク規範	多数の専用・標準通信プロトコル 専用有線・無線（無線及びサテライト）を含む数種の通信メディアを利用 ネットワークは複雑で、制御エンジニアの専門知識を必要とすることあり
管理変更	ソフトウエア変更は良好なセキュリティポリシー・手順に従いタイムリーに実施。手順は自動化されていることが多い。	ソフトウエア変更は、システム全体を通じて徹底的に試験・展開し、制御システムが保全されるようにする。ICS 停止の多くは、数日又は数週間前にあらかじめ計画・予定が必要。サポートが終了した OS を使用している場合あり
管理サポート	多様なサポートスタイルあり	サービスサポートは通常 1 業者のみ
コンポーネントの寿命	3 年～5 年	10 年～15 年
コンポーネントの所在場所	通常ローカル所在で、アクセスが容易	コンポーネントは隔絶された遠隔地にあり、アクセスにはかなりの物理的労力が必要

要約すると、ICS システムと IT システム間には、運用及びリスクの違いがあることから、洗練されたサイバーセキュリティと運用戦略を適用する必要が生じる。制御エンジニア、制御システム操作員及び IT セキュリティ専門員からなる機能横断チームは、緊密に連携して、セキュリティソリューションの導入、運用及び保守がもたらし得る意味を、制御システムの運用との兼ね合いで理解する必要がある。ICS で作業を行う IT 専門員は展開前に、情報セキュリティ技術の信頼性影響について理解しておく必要がある。ICS 上で実行する OS やアプリケーションの中には、特殊な ICS 環境アーキテクチャに起因して、民生（COTS）IT サイバーセキュリティソリューションの正常な動作ができないものもある。

2.5 別種の制御システム

本書では ICS のセキュリティを確保するためのガイダンスを示すが、別種の制御システムでも共通の特徴があり、本書の推奨事項の多くは適用可能で、サイバーセキュリティ脅威からそうしたシステムを保護する際の参考書として活用可能である。例えば、ビル、輸送、医療、セキュリティ、ロジスティック等のシステムの多くは使用するプロトコル、ポート及びサービスが異なり、ICS とは異なるモードで設定され運用されているが、伝統的な ICS と共通の特徴を持っている[18]。そうしたシステムやプロトコルの例を以下に示す。

別種の制御システム

- 最新計量インフラストラクチャ
- ビルオートメーションシステム
- ビル管理制御システム
- CCTV サーベイランスシステム
- CO2 監視
- デジタル標識システム
- デジタルビデオ管理システム
- 電子セキュリティシステム
- 緊急管理システム

- Energy Management Systems.
- Exterior Lighting Control Systems.
- Fire Alarm Systems.
- Fire Sprinkler Systems.
- Interior Lighting Control Systems.
- Intrusion Detection Systems.
- Physical Access Control Systems.
- Public Safety/Land Mobile Radios.
- Renewable Energy Geothermal Systems.
- Renewable Energy Photo Voltaic Systems.
- Shade Control Systems.
- Smoke and Purge Systems.
- Vertical Transport System (Elevators and Escalators).
- Laboratory Instrument Control Systems.
- Laboratory Information Management Systems (LIMS).

Protocols/Ports and Services

- Modbus: Master/Slave - Port 502.
- BACnet[3]: Master/Slave - Port 47808.
- LonWorks/LonTalk[4]: Peer to Peer - Port 1679.
- DNP3: Master/Slave – Port 19999 when using Transport Layer Security (TLS), Port 20000 when not using TLS.
- IEEE 802.x - Peer to Peer.
- ZigBee - Peer to Peer.
- Bluetooth – Master/Slave.

The security controls provided in Appendix G— of this guide are general and flexible enough be used to evaluate other types of control systems, but subject matter experts should review the controls and tailor them as appropriate to address the uniqueness of other types of control systems. There is no “one size fits all,” and the risks may not be the same, even within a particular group. For example, a building has many different sub-systems such as building automation, fire alarm, physical access control, digital signage, CCTV, etc. Critical life safety systems such as the fire alarm and physical access control systems may drive the impact level to be a “High,” while the other systems will usually be “Low.” An organization might decide to evaluate each sub-system individually, or decide to use an aggregated approach. The control systems evaluation should be coupled to the Business Impact, Contingency Plan, and Incident Response Plan to ensure organizational critical functions and operations can be recovered and restored as defined by the organizations Recovery Time Objectives.

[3] http://www.bacnet.org/

[4] http://en.wikipedia.org/wiki/LonWorks

- エネルギー管理システム
- 街灯制御システム
- 火災報知システム
- 消火用スプリンクラーシステム
- 屋内灯制御システム
- 侵入検知システム
- 物理的立入管理システム
- 公衆安全/陸上移動無線
- 再生エネルギー地熱システム
- 再生エネルギー太陽光発電システム
- シェード制御システム
- 排煙システム
- 鉛直輸送システム（エレベータ/エスカレータ）
- 実験室計器制御システム
- 実験室情報管理システム（LIMS）

プロトコル/ポート及びサービス

- Modbus:マスター/スレーブ - ポート 502
- BACnet[5]:マスター/スレーブ - ポート 47808
- LonWorks/LonTalk[6]ピアツーピア - ポート 1679
- DNP3:トランスポート層セキュリティ（TLS）使用時マスター/スレーブ - ポート 19999 TLS 不使用時ポート 20000
- IEEE 802.x - ピアツーピア
- ZigBee - ピアツーピア.
- Bluetooth - マスター/スレーブ

本書の付録 G に記載されるセキュリティ管理は、一般的で柔軟性があるため、別種の制御システムの評価にも利用できるが、それぞれの主題の専門家はその制御を精査し、要すれば調整を加えて、別種システムの独自性を検討すべきである。特定のグループ内であっても、全てに適合する「フリーサイズ」のようなものは存在せず、リスクも同じではない。例えば、ビルにはビルオートメーション、火災報知器、物理的立入管理、デジタル標識、CCTV 等の多種多様なサブシステムが存在する。火災報知器や物理的立入管理システムのような重要な生命安全システムは、影響レベルを「高」とすべきで、その他のシステムは通常「低」となろう。組織はそれぞれのサブシステムの個別評価を行うよう決定し、あるいは集約的なアプローチを取ることを決定できよう。制御システムの評価は、事業影響不測事態計画やインシデント対応計画の一部に含めて、組織の重要機能を確保すれば、組織の目標復旧時間どおりに業務を回復・復旧することができる。

5 http://www.bacnet.org/
6 http://en.wikipedia.org/wiki/LonWorks

3. ICS Risk Management and Assessment

3.1 Risk Management

Organizations manage risk every day in meeting their business objectives. These risks may include financial risk, risk of equipment failure, and personnel safety risk, to name just a few. Organizations must develop processes to evaluate the risks associated with their business and to decide how to deal with those risks based on organizational priorities and both internal and external constraints. This management of risk is conducted as an interactive, ongoing process as part of normal operations. Organizations that use ICS have historically managed risk through good practices in safety and engineering. Safety assessments are well established in most sectors and are often incorporated into regulatory requirements. Information security risk management is an added dimension that can be complementary. The risk management process and framework outlined in this section can be applied to any risk assessment including both safety and information security.

A risk management process should be employed throughout an organization, using a three-tiered approach to address risk at the (i) organization level; (ii) mission/business process level; and (iii) information system level (IT and ICS). The risk management process is carried out seamlessly across the three tiers with the overall objective of continuous improvement in the organization's risk-related activities and effective inter-tier and intra-tier communication among all stakeholders having a shared interest in the mission/business success of the organization.

This section focuses primarily on ICS considerations at the information system level, however, it is important to note that the risk management activities, information, and artifacts at each tier impact and inform the other tiers. Section 6 extends the concepts presented here to the control family level and provides ICS-specific recommendations to augment security control families. Throughout the following discussion of risk management, ICS considerations will be highlighted and the impact that these considerations have on the risk management process will be discussed.

For more information on multi-tiered risk management and the risk management process, refer to NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission and Information System View* [20]. NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* [21], provides guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization,[7] security control selection and implementation, security control assessment, information system authorization,[8] and security control monitoring. NIST Special Publication 800-30, *Guide for Conducting Risk Assessments*, provides a step-by-step process for organizations on: (i) how to prepare for risk assessments; (ii) how to conduct risk assessments; (iii) how to communicate risk assessment results to key organizational personnel; and (iv) how to maintain the risk assessments over time [79].

7 FIPS 199 provides security categorization guidance for non-national security systems [15]. CNSS Instruction 1253 provides similar guidance for national security systems.

8 Security authorization is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

3. ICS のリスク管理とリスク評価

3.1 リスク管理

組織は、その事業目的を達成するため、日々リスクを管理している。そうしたリスクには財政上のリスク、装備品障害によるリスク、人の安全に関するリスクなどがある。組織はプロセスを策定して、事業に関係するリスクを評価し、組織の優先事項や組織内外の制約事項を基に、リスクへの対処法を決定しなければならない。このリスク管理は、正規業務の一環として、相互作用的な現行プロセスとして実施される。ICS を使用する組織は歴史的に、安全性とエンジニアリングにおける優良規範を通じて、リスクを管理してきた。安全性評価はほとんどの部門で確立されており、規制上の要件に盛り込まれていることが多い。情報セキュリティのリスク管理は、補足的な付加的次元のものである。このセクションで略述するリスク管理のプロセスと枠組みは、安全性及び情報セキュリティを含むあらゆるリスク評価に応用できる。

リスク管理のプロセスは、組織全体を通じて、(1)組織レベル、(2)任務/事業プロセスレベル、(3)情報システムレベル（IT 及び ICS）、という 3 段構えのアプローチで採用すべきである。リスク管理プロセスは、組織の任務/事業に共通の関心を抱く関係者間において、組織のリスク関連活動及び各段階間・各段階内の効果的な通信を絶えず改善するという全体的な目的を持って、3 つの段階にわたってシームレスに行われる。

このセクションでは主に、情報システムレベルでの ICS の考慮事項に注目するが、各段階におけるリスク管理活動、情報及び所産が、他の段階に影響と情報をもたらすことに注意すべきである。セクション 6 では、ここで紹介する概念を更に制御系列レベルに拡張し、セキュリティ対策系列を増やすための ICS 特有の推奨事項を提示する。これ以降のリスク管理に関する論議を通じて、ICS の考慮事項について特筆し、そうした考慮事項がリスク管理プロセスに及ぼす影響について考察する。

多段階リスク管理とリスク管理プロセスの詳細については、NISTSP800-39『情報セキュリティリスクの管理：組織、任務及び情報システム概説』[20]を参照のこと。NISTSP800-37 改訂 1『連邦情報システムへのリスク管理体系適用ガイド：セキュリティライフサイクルアプローチ』[21]は、リスク管理体系を連邦情報システムに適用する際のガイドラインとなるもので、セキュリティ区分 [9]、セキュリティ管理の選択・実装、セキュリティ管理の評価、情報システムの認可 [10]及びセキュリティ管理の監視といった諸活動の実施要領が盛り込まれている。NISTSP800-30『リスク評価ガイド』は、(1)リスク評価の準備要領、(2) リスク評価の実施要領、(3)組織要人へのリスク評価結果の伝達要領、(4) リスク評価の経時的維持要領について、組織のプロセスを段階別に説明している[79]。

9 FIPS 199 は、国以外のセキュリティシステムに関するセキュリティ区分のガイダンスとなる[15]。CNSS 命令 1253 は、国のセキュリティシステムに関する同種のガイダンス。

10 セキュリティ認可は、組織の高官による公的な管理決定で、情報システムの運用を認可し、組織の運営・資産、個人、他の組織及び国家に対するリスクを、合意されたセキュリティ対策の実装に基づいて、明示的に許容するものである。

3.2 Introduction to the Risk Management Process

As shown in Figure 3-1, the risk management process has four components: *framing*, *assessing*, *responding* and *monitoring*. These activities are interdependent and often occur simultaneously within an organization. For example, the results of the monitoring component will feed into the framing component. As the environment in which organizations operate is always changing, risk management must be a continuous process where all components have on-going activities. It is important to remember that these components apply to the management of any risk whether information security, physical security, safety or financial.

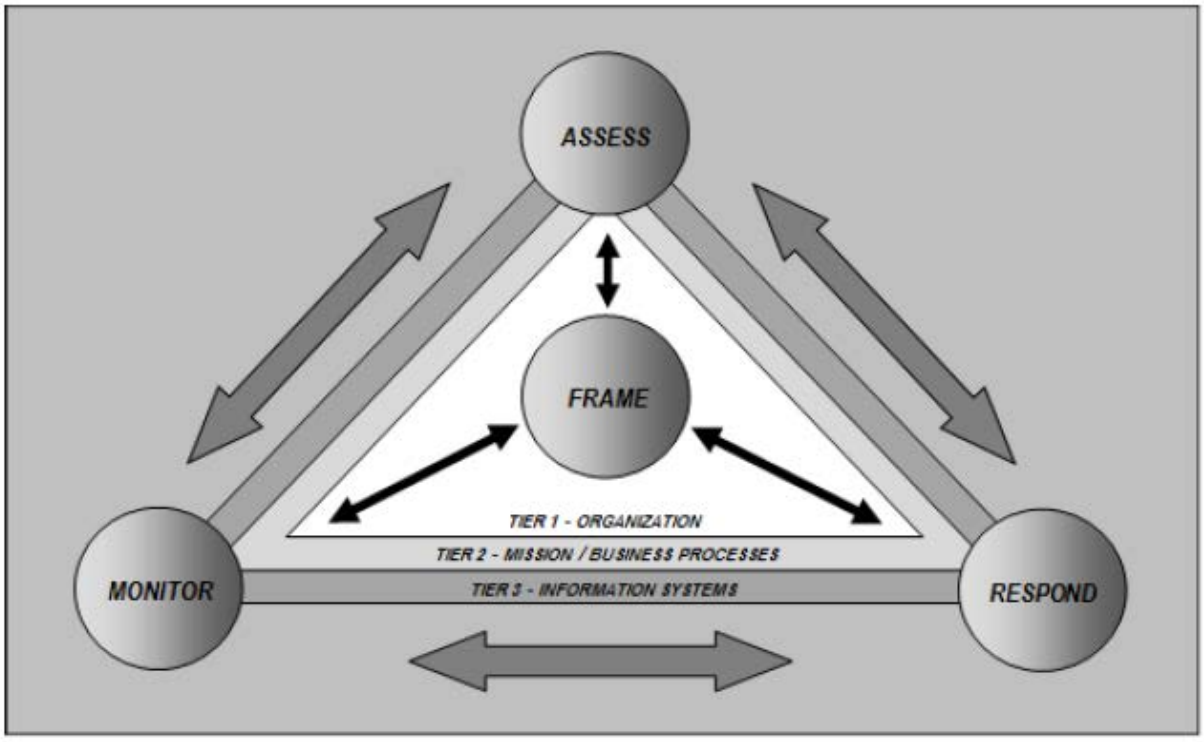

Figure 3-1. Risk Management Process Applied Across the Tiers

The *framing component* in the risk management process consists of developing a framework for the risk management decisions to be made. The level of risk that an organization is willing to accept is its *risk tolerance* [21, p.6].

The framing component should include review of existing documentation, such as prior risk assessments. There may be related activities; such as community wide disaster management planning that also should be considered since they impact the requirements that a risk assessment must consider.

3.2 リスク管理プロセスの紹介

図 3-1 に示すように、リスク管理プロセスには、構想、評価、対応、監視の 4 つの要素がある。これら諸活動は相互依存しており、同じ組織内で同時に生じることが多い。例えば、監視の結果が構想に反映される。組織が置かれた環境は絶えず変化しているため、リスク管理は継続的なプロセスで、4 つの要素がどれも進行中でなければならない。各要素は、情報セキュリティ、物理的セキュリティ、安全、財政の別を問わず、あらゆるリスクの管理に当てはまることを銘記するのは肝要である。

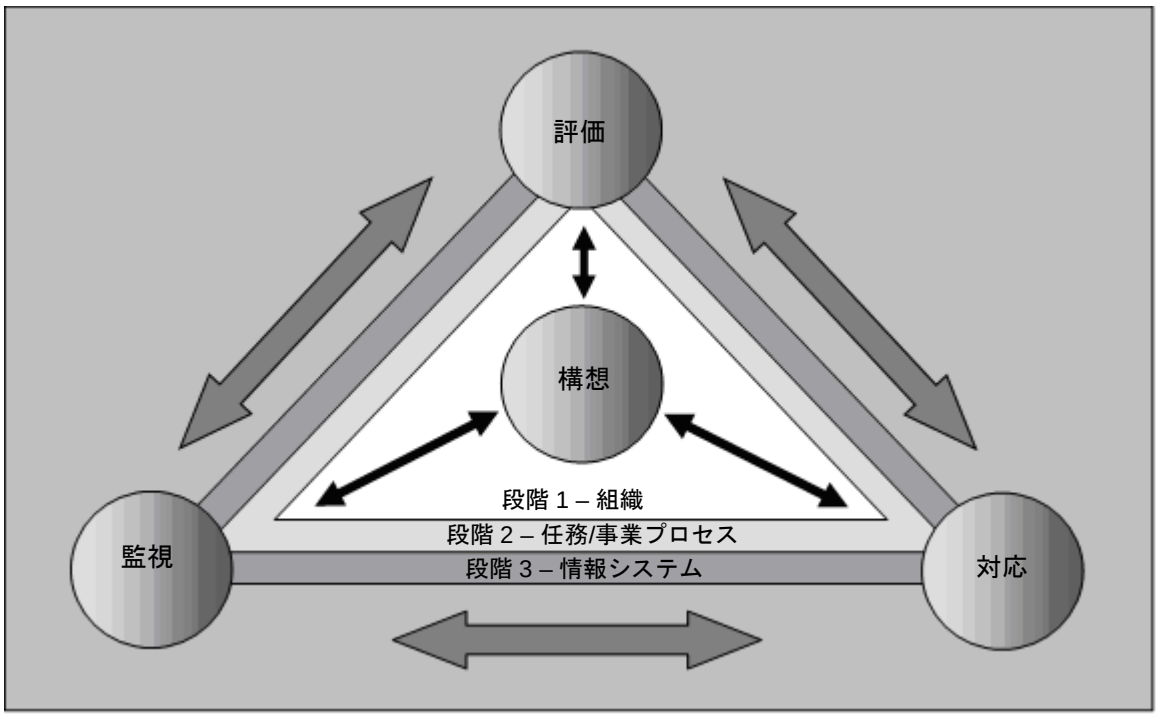

図 3-1.全段階にまたがるリスク管理プロセス

リスク管理プロセスにおける**構想**は、下すべきリスク管理上の決定に関する体系を策定することにある。組織が受け入れられるリスクレベルがリスクトレランスである[21, p. 6]。

この構想には、以前のリスク評価書など既存文書の精査を含めるべきである。関連活動もあり得よう。例えば、共同体内の災害管理計画なども、リスク評価で検討を要する諸要件に影響するため、考慮に含めるべきである。

ICS-specific Recommendations and Guidance

For operators of ICS, safety is the major consideration that directly affects decisions on how systems are engineered and operated. Safety can be defined as "freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment."[11]6 Part of the framing component for an ICS organization is determining how these requirements interact with information security. For example, if safety requirements conflict with good security practice, how will the organization decide between the two priorities? Most ICS operators would answer that safety is the main consideration – the framing component makes such assumptions explicit so that there is agreement throughout the process and the organization.

Another major concern for ICS operators is the availability of services provided by the ICS. The ICS may be part of critical infrastructure (for example, water or power systems), where there is a significant need for continuous and reliable operations. As a result, ICS may have strict requirements for availability or for recovery. Such assumptions should be developed and stated in the framing component. Otherwise, the organization may make risk decisions that result in unintended consequences on those who depend on the services provided.

The physical operating environment is another aspect of risk framing that organizations should consider when working with ICS. ICS often have specific environmental requirements (e.g., a manufacturing process may require precise temperature), or they may be tied to their physical environment for operations. Such requirements and constraints should be explicitly stated in the framing component so that the risks arising from these constraints can be identified and considered.

Assessing risk requires that organizations identify their threats and vulnerabilities, the harm that such threats and vulnerabilities may cause the organization and the likelihood that adverse events arising from those threats and vulnerabilities may actually occur.

ICS-specific Recommendations and Guidance

The DHS National Cybersecurity & Communications Integration Center (NCCIC)[12] serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[13] collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. ICS-CERT works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors.

When assessing the potential impact to an organization's mission from a potential ICS incident, it is important to incorporate the effect on the physical process/system, impact on dependent systems/processes, and impact on the physical environment among other possibilities. In addition, the potential impact on safety should always be considered.

11 MIL-STD-882E, *Standard Practice - System Safety*, Department of Defense (DoD), May 11, 2012, https://acc.dau.mil/CommunityBrowser.aspx?id=683694

12 http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

13 https://ics-cert.us-cert.gov/

ICS 固有の推奨事項及びガイダンス

ICS 操作員にとって安全は、システムの計画・実行要領の決定に直接影響する重大考慮事項である。安全は「死亡、負傷、職業病、装備品・資産の損害・喪失、環境破壊を生じる状態から免れていること」と定義できる[14]。ICS 組織の構想部分は、このような要件と情報セキュリティとの相互作用要領を判定することにある。例えば、安全要件がセキュリティの適正規範と相容れない場合、組織は 2 つの優先課題の間でどのような決定を行うのか。大方の ICS 操作員は、安全が主要な考慮事項だと答えよう。構想は、このような前提事項を明確にして、プロセスと組織全体を通じて合意を形成する。
ICS 操作員にとって、もう 1 つの重大関心事項は、ICS が提供するサービスの可用性である。ICS は重要インフラの一部であることがあり（例えば水道や電気システム）、その場合、継続的で信頼性の高い運用に対する需要は極めて大きい。その結果、ICS は可用性と回復に対する要件が厳格になる。こうした前提事項を策定し、構想に記載すべきである。そうしないと、組織はリスクのある決定を下し、それが元で、提供されるサービスに依存している人々に思わぬ結果をもたらすことになる。

物理的動作環境は、ICS を使用する場合に組織が考慮すべき、もう 1 つの面である。ICS には特殊な環境要件が多く（製造プロセスでの正確な温度要件など）、物理的な動作環境に拘束されていることもある。こうした要件や制約事項も構想に明記し、制約事項から生じるリスクを特定し、配慮できるようにすべきである。

リスクを**評価**する際には、組織の脅威と脆弱性、それによって組織が被る損害、そうした脅威と脆弱性によりもたらされる有害事象が実際に生じる公算を明らかにすることが必要となる。

ICS 固有の推奨事項及びガイダンス

DHS 国家サイバーセキュリティ通信統合センター(NCCIC)[15]は集中所在地として機能し、サイバーセキュリティと通信の信頼性に関わる運用要素はそこで調整され、統合化されている。産業用制御システムサイバー緊急対応チーム(ICS-CERT)[16]は、海外及び民間のコンピュータ緊急対応チーム(CERT)と連携して、制御システム関連のセキュリティインシデントと緩和対策を共有している。ICS-CERT は行政当局や情報組織との連携、連邦・州・地方・諸部族自治体のほか制御システム所有者やベンダーとの協働を通じて、あらゆる重要インフラ部門に関わるリスク削減に努めている。

ICS インシデントが生じた場合に組織の任務に及ぶ影響度を評価する際、とりわけ物理的プロセス/システムへの影響、従属システム/プロセスへの影響及び物理的環境への影響を含めることが肝要である。加えて、安全性に与え得る影響を常に考慮に入れるべきである。

14 MIL-STD-882E, *Standard Practice - System Safety*, 国防総省 (DoD), May 11, 2012, https://acc.dau.mil/CommunityBrowser.aspx?id=683694

15 http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

16 https://ics-cert.us-cert.gov/

The *responding component* is based on the concept of a consistent organization-wide response to the *identification* of risk. Response to identification of risk (as opposed to the response to an incident) requires that organizations first identify possible courses of actions to address risk, evaluate those possibilities in light of the organization's risk tolerance and other considerations determined during the framing step, and choose the best alternative for the organization. The response component includes the implementation of the chosen course of action to address the identified risk: *acceptance, avoidance, mitigation, sharing, transfer,* or any combination of those options[17].

ICS-specific Recommendations and Guidance
For ICS, available risk responses may be constrained by system requirements, potential adverse impact on operations, or even regulatory compliance regimes. An example of risk sharing is when utilities enter into agreements to "loan" line workers in an emergency, which reduces the duration of the effect of an incident to acceptable levels.

Monitoring is the fourth component of the risk management activities. Organizations must monitor risk on an on-going basis including: the implementation of chosen risk management strategies; the changes in the environment that may affect the risk calculation; and, the effectiveness and efficiency of risk reduction activities. The activities in the monitoring component impact all the other components.

3.3 Special Considerations for Doing an ICS Risk Assessment

The nature of ICS means that when an organization does a risk assessment, there may be additional considerations that do not exist when doing a risk assessment of a traditional IT system. Because the impact of a cyber incident in an ICS may include both physical and digital effects, risk assessments need to incorporate those potential effects. This section will provide a more in-depth examination of the following:

- Impacts on safety and use of safety assessments.
- Physical impact of a cyber incident on an ICS, including the larger physical environment; effect on the process controlled, and the physical effect on the ICS itself.
- The consequences for risk assessments of non-digital control components within an ICS.

3.3.1 Safety within an ICS Information Security Risk Assessment

The culture of safety and safety assessments is well established within the majority of the ICS user community. Information security risk assessments should be seen as complementary to such assessments though the assessments may use different approaches and cover different areas. Safety assessments are concerned primarily with the physical world. Information security risk assessments primarily look at the digital world. However, in an ICS environment, the physical and the digital are intertwined and significant overlap may occur.
It is important that organizations consider all aspects of risk management for safety (e.g., risk framing, risk tolerances), as well as the safety assessment results, when carrying out risk assessments for information security. The personnel responsible for the information security risk assessment must be able

[17] For additional information on accepting, avoiding, mitigating, sharing, or transferring risk, refer to NIST Special Publication 800-39 [20].

対応は、組織全体を通じて首尾一貫した形でリスクの特定に取り組むという考え方に基づいている。リスクの**特定**への**対応**は（インシデントへの対応とは異なり）、まずリスクに対して組織が取り得る行動方針を見極め、構想ステップで判定された組織のリスクトレランスその他の考慮事項に照らして、取り得る各行動方針を評価し、最善策を選択することが求められる。対応には、選定した行動方針を実行して、特定済みのリスクに対処することが含まれ、それには**受容、回避、緩和、共有、転嫁**又はこれらの組合せがある [18]。

ICS 固有の推奨事項及びガイダンス

ICS では、利用できるリスク対応はシステム要件、運用に悪影響が出る可能性又は規制へのコンプライアンス形態により制約される場合がある。リスク共有の一例として、緊急時に公共企業が労働者を「出向させる」契約を締結し、それによってインシデントの影響期間が受容レベルまで短縮されるケースが挙げられる。

監視はリスク管理の 4 番目の要素となる。組織はリスクを継続的に監視しなければならないが、それには選定したリスク管理戦略の実行、リスク算定に影響する環境の変化及びリスク削減活動の効果・効率が含まれる。監視における諸活動は他の全ての要素に影響する。

3.3 ICS リスク評価の実施に際しての特別な考慮事項

ICS の性質上、組織がリスク評価を行う際には、在来の IT システムのリスク評価実施時には存在しない補足的な考慮事項があり得ることである。ICS におけるサイバーインシデントの影響には、物理的影響とデジタル効果の両方があるため、リスク評価にはこのような影響の可能性を含める必要がある。このセクションでは、以下について更に深く考察する。

- 安全性への影響及び安全性評価の使用
- サイバーインシデントが ICS に与える影響。これにはより大規模な物理環境、管理されるプロセスへの影響及び ICS そのものへの物理的影響が含まれる。
- ICS 内の非デジタル制御コンポーネントリスク評価結果

3.3.1 ICS 情報セキュリティリスク評価における安全性

大部分の ICS ユーザ共同社会では、安全性や安全性評価の文化が定着している。情報セキュリティリスク評価は、種々のアプローチを利用し様々な分野を対象としてはいるが、あくまでも安全性評価の補完と見なすべきである。安全性評価は、主に物理的な世界を対象にしている。情報セキュリティリスク評価では、主にデジタル世界が関心の対象となる。しかし ICS 環境では、物理世界もデジタル世界も互いに入り組んで、かなり重なり合っている場合もある。

情報セキュリティのリスク評価を行う場合、組織は、安全に関するリスク管理のあらゆる面（リスクの構想、リスクトレランス等）のほか、安全性評価の結果を考慮に入れることが肝要である。情報セキュリティリスク評価担当者は、

[18] リスクの受容、回避、緩和、共有又は転嫁の詳細は NIST 特別出版物 800-39［20］を参照のこと。

to identify and communicate identified risks that could have safety implications. Conversely, the personnel charged with safety assessments must be familiar with the potential physical impacts and their likelihood developed by the information security risk assessment process.

3.3.2 Potential Physical Impacts of an ICS Incident

Evaluating the potential physical damage from a cyber incident should incorporate: i) how an incident could manipulate the operation of sensors and actuators to impact the physical environment; ii) what redundant controls exist in the ICS to prevent an impact; and iii) how a physical incident could emerge based on these conditions. A physical impact could negatively impact the surrounding world through multiple means, including the release of hazardous materials (e.g., pollution, crude oil), damaging kinetic forces (e.g., explosions), and exposure to energy sources (e.g., electricity, steam). The physical incident could negatively impact the ICS and supporting infrastructure, the various processes performed by the ICS, or the larger physical environment. An evaluation of the potential physical impacts should include all parts of an ICS, beginning with evaluating the potential impacts on the set of sensor and actuators. Each of these domains will be further explored below.

Evaluating the impact of a cyber incident on the physical environment should focus on potential damage to human safety, the natural environment, and other critical infrastructures. Human safety impacts should be evaluated based on whether injury, disease, or death is possible from a malfunction of the ICS. This should incorporate any previously performed safety impact assessments performed by the organization regarding both employees and the general public. Environmental impacts also may need to be addressed. This analysis should incorporate any available environmental impact assessments performed by the organization to determine how an incident could impact natural resources and wildlife over the short or long term. In addition, it should be noted that ICS may not be located within a single, controlled location and can be distributed over a wide physical area and exposed to uncontrolled environments. Finally, the impact on the physical environment should explore the extent to which an incident could damage infrastructures external to the ICS (e.g., electric generation/delivery, transportation infrastructures, and water services).

3.3.3 Impact of Physical Disruption of an ICS Process

In addition to the impact on the physical environment, the risk assessment should also evaluate potential effects to the physical process performed by the ICS under consideration, as well as other systems. An incident that impacts the ICS and disrupts the dependent process may cause cascading impacts into other related ICS processes and the general public's dependence on the resulting products and services. Impact to related ICS processes could include both systems and processes within the organization (e.g., a manufacturing process that depends on the process controlled by the system under consideration) or systems and processes external to the organization (e.g., a utility selling generated energy to a nearby plant).

A cyber incident can also negatively impact the physical ICS under consideration. This type of impact primarily includes the physical infrastructure of the plant (e.g., tanks, valves, motors), along with both the digital and non-digital control mechanisms (e.g., cables, PLCs, pressure gauge). Damage to the ICS or physical plant may cause either short or long term outages depending on the degree of the incident. An example of a cyber incident impacting the ICS is the Stuxnet malware, which caused physical damage to the centrifuges as well as disrupting dependent processes.

特定されたリスクで安全上の意味があるものを明らかにして、伝達できなければならない。反対に安全性評価担当者は、情報セキュリティリスク評価プロセスにより発生する可能性のある物理的影響とその公算について精通していなければならない。

3.3.2 ICS インシデントによる物理的影響の可能性

サイバーインシデントにより生じ得る物理的損害の評価には次のものが含まれる。(1)インシデントがセンサ及びアクチュエータの動作をどのように操作して物理的環境に影響を及ぼすか。(2)影響を防ぐためのどのような冗長制御が ICS にあるか。(3)このような条件下で物理的インシデントはどのように生じるか。物理的影響は周囲の世界に様々な手段で悪影響を及ぼしかねないが、それには危険物の放出（汚染、原油等）、運動力による損傷（爆発等）、エネルギー源への曝露（電気、蒸気等）などがある。物理的インシデントは、ICS 及び支援インフラ、ICS が実施する多様なプロセス又はより大規模の物理環境に悪影響を与えかねない。可能性のある物理的影響の評価には ICS のあらゆる部分を含め、まずセンサ・アクチュエータセットへの影響の可能性から開始すべきである。これら領域の各部分については詳しく後述する。

物理環境に与えるサイバーインシデントの影響評価は、人的安全、自然環境その他重要インフラに与え得る損害を重視すべきである。人的安全への影響は、ICS の障害から負傷・疾病・死亡が生じるか否かを基に評価すべきである。これには以前組織が従業員と一般国民に関して実施した安全性影響評価も含めるべきである。環境影響も取り上げる必要があろう。この分析には、インシデントが短期的・長期的に天然資源や野生生物に与える影響を判定するために組織が実施した環境影響評価も、利用できれば含めるべきである。加えて、ICS は管理された一か所に配置されておらず、広範な地域に分散し、管理されていない環境に曝されている場合があることにも留意すべきである。最後に、物理環境への影響は、インシデントが ICS の外部にあるインフラにどの程度の損害を与えるかを調査すべきである（発電・送電、輸送インフラ、水道事業等）。

3.3.3 ICS プロセスの物理的中断による影響

物理環境への影響に加えて、リスク評価では ICS が実行する考慮対象の物理プロセスと他のシステムへの影響も評価すべきである。
ICS に影響を与え従属プロセスを中断させるインシデントは、他の ICS 関連プロセスやそこから生じる製品・サービスに依存している国民にも連鎖的な影響を及ぼしかねない。関連 ICS プロセスへの影響には、組織内のシステム及びプロセス（考慮中のシステムに制御されるプロセスに依存している製造プロセス等）又は組織外のシステム及びプロセス（生産したエネルギーを近隣のプラントに売る公共事業体等）が含まれ得る。

サイバーインシデントは、考慮中の物理的 ICS にも悪影響を与える。この種の影響には主としてプラントの物理的インフラ（タンク、バルブ、モータ等）やデジタル/非デジタル制御メカニズム（ケーブル、PLC、圧力ゲージ等）が含まれる。ICS や物理的プラントへの損害は、インシデントの程度に応じて短期又は長期の停止に至りかねない。ICS に影響するサイバーインシデントの一例として Stuxnet マルウエアがあり、遠心分離機を物理的に損傷し、従属プロセスを中断させる。

3.3.4 Incorporating Non-digital Aspects of ICS into Impact Evaluations

The impacts on the ICS cannot be adequately determined by focusing only on the digital aspects of the system, as there are often non-digital mechanisms available that provide fault tolerance and prevent the ICS from acting outside of acceptable parameters. Therefore, these mechanisms may help reduce any negative impact that a digital incident on the ICS might have and must be incorporated into the risk assessment process. For example, ICS often have non-digital control mechanisms that can prevent the ICS from operating outside of a safe boundary, and thereby limit the impact of an attack (e.g., a mechanical relief pressure valve). In addition, analog mechanisms (e.g., meters, alarms) can be used to observe the physical system state to provide operators with reliable data if digital readings are unavailable or corrupted. Table 3-1 provides a categorization of non-digital control mechanisms that could be available to reduce the impact of an ICS incident.

Table 3-1. Categories of Non-Digital ICS Control Components

System Type	Description
Analog Displays or Alarms	Non-digital mechanisms that measure and display the state of the physical system (e.g., temperature, pressure, voltage, current) and can provide the operator with accurate information in situations when digital displays are unavailable or corrupted. The information may be provided to the operator on some non-digital display (e.g., thermometers, pressure gauges) and through audible alarms.
Manual Control Mechanisms	Manual control mechanisms (e.g., manual valve controls, physical breaker switches) provide operators with the ability to manually control an actuator without relying on the digital control system. This ensures that an actuator can be controlled even if the control system is unavailable or compromised.
Analog Control Systems	Analog control systems use non-digital sensors and actuators to monitor and control a physical process. These may be able to prevent the physical process from entering an undesired state in situations when the digital control system is unavailable or corrupted. Analog controls include devices such as regulators, governors, and electromechanical relays.

Determination of the potential impact that a cyber incident may have on the ICS should incorporate analysis of all non-digital control mechanisms and the extent to which they can mitigate potential negative impacts to the ICS. There are multiple considerations when considering the possible mitigation effects of non-digital control mechanisms, such as:

- Non-digital control mechanisms may require additional time and human involvement to perform necessary monitoring or control functions and these efforts may be substantial. For example, such mechanisms may require operators to travel to a remote site to perform certain control functions. Such mechanisms may also depend on human response times, which may be slower than automated controls.
- Manual and analog systems may not provide monitoring or control capabilities with the same degree of accuracy and reliability as the digital control system. This may present risk if the primary control system is unavailable or corrupted due to reduced quality, safety, or efficiency of the system. For example, a digital/numeric protection relay provides more accuracy and reliable detection of faults than analog/static relays, therefore, the system maybe more likely to exhibit a spurious relay tripping if the digital relays are not available.

3.3.4 ICS の非デジタル面を影響評価に含める

フォールトトレランスを発揮し、ICS が許容パラメータを逸脱しないように防止できる非デジタルメカニズムも利用できるので、システムのデジタル面にのみ注目していると、ICS への影響を適正に判定することができない。したがって、このようなメカニズムは、ICS 上のデジタルインシデントに起因する悪影響を減らすため、リスク評価プロセスに組み込む必要がある。例えば、ICS には非デジタル制御メカニズムを持つものが多く、ICS が安全限界を超えないようにして、攻撃の影響を制限している（機械式の圧力リリーフバルブ等）。またアナログメカニズム（メータ、アラーム等）を使用して、システムの物理的な状態を観察し、デジタル表示の利用不能・中断時に、信頼できるデータを操作員に提示することができる。表 3-1 は、ICS インシデントの影響を減らせる非デジタル制御メカニズムの区分である。

表 3-1. 非デジタル ICS 制御コンポーネントのカテゴリー

システムの種類	内容
アナログディスプレイ又はアラーム	物理的システムの状態（温度、圧力、電圧、電流等）を計測・表示し、デジタルディスプレイの利用不能・中断時に正確な状況情報を操作員に提供できる非デジタルメカニズム。情報は非デジタルディスプレイ（温度計、圧力計等）や音声アラームにより操作員に提供する。
手動制御メカニズム	手動制御メカニズム（手動バルブ制御、物理的ブレーカスイッチ等）があれば、操作員はデジタル制御システムに依存することなくアクチュエータを手で操作できる。このため制御システムが利用不能・不調でもアクチュエータを制御できる。
アナログ制御システム	アナログ制御システムは非デジタルセンサとアクチュエータを使用して、物理プロセスを監視・制御する。このためデジタル制御システムが利用不能・中断時でも、物理プロセスが好ましくない状態に陥らないですむ。アナログ制御にはレギュレータ、ガバナー、電子機械式リレー等のデバイスがある。

サイバーインシデントが ICS に与え得る影響度の判定には、全ての非デジタル制御メカニズムの分析と、それらが ICS への悪影響を緩和できる程度も盛り込むべきである。非デジタル制御メカニズムによるこのような緩和効果を検討する際には、次のような考慮事項がある。

- 非デジタル制御メカニズムが必要な監視又は制御機能を発揮するには、余分の時間と人の関与が不可欠で、それがかなりの程度になることもある。例えば、操作員が遠方の現場まで出向いて、ある種の制御を行わなければならない場合がある。また人による対応時間もかかるため、自動制御に比べると遅くなる。
- 手動及びアナログシステムの監視又は制御能力は、デジタル制御システムほどの精度や信頼性には及ばないことがある。システムの品質、安全性又は効率が低下して、プライマリ制御システムが利用不能や中断になった場合に、これはリスクとなり得る。例えば、デジタル/数値保護リレーは、アナログ/スタティックリレーよりも障害検知精度や信頼性が高いので、デジタルリレーが利用できないと、システムはリレーの疑似トリップが生じやすくなる。

3.3.5 Incorporating the Impact of Safety Systems

Safety systems may also reduce the impact of a cyber incident to the ICS. Safety systems are often deployed to perform specific monitoring and control functions to ensure the safety of people, the environment, process, and ICS. While these systems are traditionally implemented to be fully redundant with respect to the primary ICS, they may not provide complete redundancy from cyber incidents, specifically from a sophisticated attacker. The impact of the implemented security controls on the safety system should be evaluated to determine that they do not negatively impact the system.

3.3.6 Considering the Propagation of Impact to Connected Systems

Evaluating the impact of an incident must also incorporate how the impact from the ICS could *propagate* to a connected ICS or physical system. An ICS may be interconnected with other systems, such that failures in one system or process can easily cascade to other systems either within or external to the organization. Impact propagation could occur due to both physical and logical dependencies. Proper communication of the results of risk assessments to the operators of connected or interdependent systems and processes is one way to mitigate such impacts.

Logical damage to an interconnected ICS could occur if the cyber incident propagated to the connected control systems. An example could be if a virus or worm propagated to a connected ICS and then impacted that system. Physical damage could also propagate to other interconnected ICS. If an incident impacts the physical environment of an ICS, it may also impact other related physical domains. For example, the impact could result in a physical hazard which degrades nearby physical environments. Additionally, the impact could also degrade the common shared dependencies (e.g., power supply), or result in a shortage of material needed for a later stage in an industrial process.

3.3.5 安全システムの影響を含める

安全システムでは、ICS に与えるサイバーインシデントの影響も減る。安全システムは人・環境・プロセス・ICS の安全を確保するために、特殊な監視・制御機能用に展開されることが多い。そうしたシステムでは、プライマリ ICS に関しては従来完全な冗長性が確保されている一方、特に巧妙な攻撃者からのサイバーインシデントに関しては完全な冗長性がない。実装されたセキュリティ管理が安全システムに与える影響の評価は、システムへの悪影響の有無を判定すべきである。

3.3.6 接続システムへの影響波及に対する考慮

インシデントの影響を評価する際には、ICS からの影響が、接続された別の ICS や物理的システムにどの程度波及するかという点も含めなければならない。1 つの ICS は、いくつかのシステムと連接されている場合があり、あるシステム又はプロセスの障害が組織内外の他のシステムに容易に連鎖することがある。影響の波及は、物理的従属関係と論理的従属関係の双方に起因して生じ得る。こうした影響を緩和する 1 つの方法は、リスク評価の結果を連接又は相互依存するシステム及びプロセスの操作員に適切に伝えることである。

連接 ICS の論理的損害は、サイバーインシデントが連接制御システムに波及した場合に生じ得る。ウイルスやワームが連接 ICS に波及し、次いでシステムに影響を与える場合がその一例である。物理的損害も別の連接 ICS に波及し得る。あるインシデントが ICS の物理環境に影響する場合、他の関連物理領域にも影響を及ぼし得る。例えば、影響により物理的危害が生じ、それが隣接の物理環境を劣化させる場合がその一例である。
また影響は共通的な共有従属関係（電源等）をも劣化させ、産業プロセスの後続段階で必要となる資材に不足をきたす事態にもなり得る。

4. ICS Security Program Development and Deployment

Section 2 addresses critical operational differences between ICS and IT systems, and Section 3 addresses risk management. This section combines these two concerns by addressing how organizations should develop and deploy an ICS security program. ICS security plans and programs should be consistent and integrated with existing IT security experience, programs, and practices, but must account for the specific requirements and characteristics of ICS technologies and environments. Organizations should review and update their ICS security plans and programs regularly to reflect changes in technologies, operations, standards, and regulations, as well as the security needs of specific facilities.

This section provides an overview of the development and deployment of an ICS security program. Section 4.1 describes how to establish a business case for an ICS security program, including suggested content for the business case. Sections 4.2 through 4.5 discuss the development of a comprehensive ICS security program and provide information on several major steps in deploying the program. Information on specific security controls that might be implemented as part of the security program is provided in Section 6.

Effectively integrating security into an ICS requires defining and executing a comprehensive program that addresses all aspects of security, ranging from identifying objectives to day-to-day operation and ongoing auditing for compliance and improvement. An ICS information security manager with appropriate scope, responsibility, and authority must be identified. This section describes the basic process for developing a security program, including the following:

- Develop a business case for security.
- Build and train a cross-functional team.
- Define charter and scope.
- Define specific ICS policies and procedures.
- Implement an ICS Security Risk Management Framework.
    - Define and inventory ICS assets.
    - Develop security plan for ICS Systems.
    - Perform a risk assessment.
    - Define the mitigation controls.
- Provide training and raise security awareness for ICS staff.

More detailed information on the various steps is provided in ISA-62443-2-1 *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program* [34].

The commitment to a security program begins at the top. Senior management must demonstrate a clear commitment to information security. Information security is a business responsibility shared by all members of the enterprise and especially by leading members of the business, process, and management teams. Information security programs with adequate funding and visible, top-level support from organization leaders are more likely to achieve compliance, function more smoothly, and have greater success than programs that lack that support.

4. ICS セキュリティプログラムの開発及び展開

セクション 2 では ICS システムと IT システムの運用上の大きな違いを、セクション 3 ではリスク管理について取り上げた。このセクションでは、組織はいかに ICS セキュリティプログラムを策定して展開すべきかについて考察し、これら 2 つの関心事を関連づける。ICS セキュリティの計画及びプログラムは首尾一貫し、既存の IT セキュリティ経験・プログラム・規範と一体化しているべきであるが、ICS 技術・環境の特殊要件及び特性を取り上げていなければならない。組織は、ICS セキュリティの計画及びプログラムを定期的に見直して更新し、技術・運用・規格・規則の変更点のほか、特殊施設のセキュリティ需要を反映すべきである。

このセクションでは、ICS セキュリティプログラムの開発及び展開について概説する。セクション 4.1 では、ICS セキュリティプログラムに関する事業の、内容案も含めた構築例について示す。4.2～4.5 では、包括的な ICS セキュリティプログラムの開発について取上げ、それを展開するための大まかな手順をいくつか示す。セキュリティプログラムの一環として実装される特定のセキュリティ管理については、セクション 6 で取り上げる。

ICS にセキュリティを効果的に組み込むには、日常業務の目的からコンプライアンス・改善に関する監査まで、多岐にわたるセキュリティのあらゆる面を網羅した包括的なプログラムを設計して実行することが必要となる。適正な範囲、責任及び権限を有する ICS 情報セキュリティ管理者を明確にしなければならない。このセクションでは、以下を含むセキュリティプログラム開発に関する基本プロセスについて説明する。

- セキュリティのビジネス事例作成
- 機能横断チームの組成・教育訓練
- 憲章及び適用範囲の明確化
- 具体的な ICS の方針及び手順の明確化
- ICS セキュリティリスク管理体制の実行
    - ICS 資産の特定及び明細化
    - ICS システムセキュリティ計画策定
    - リスク評価実施
    - 緩和対策の明確化
- ICS スタッフの訓練及びセキュリティ意識の強化

種々の手順に関する詳細は、ISA-62443-2-1『工業オートメーション制御システムのセキュリティ：工業オートメーション制御システムセキュリティプログラムの構築』[34]に記載されている。

セキュリティプログラムへの対応は組織のトップから始まる。上級管理者は、情報セキュリティへの明確な対応を明らかにしなければならない。情報セキュリティは企業の全社員が共有している仕事上の責務であるが、特に事業、プロセス及び管理チームの指導者はそう言える。十分な資金があてがわれ、組織のトップレベルの可視化された支援を受けた情報セキュリティプログラムは、それが得られないプログラムに比べて、コンプライアンスを達成し、よりスムーズに機能し、より大きな成功となる公算が高くなる。

Whenever a new system is being designed and installed, it is imperative to take the time to address security throughout the lifecycle, from architecture to procurement to installation to maintenance to decommissioning. There are serious risks in deploying systems to production based on the assumption that they will be secured later. If there is insufficient time and resources to secure the system properly before deployment, it is unlikely that there will be sufficient time and resources later to address security. Designing and implementing a new system is quite rare. It is much more common to improve, expand, or update an existing system. Everything in this section, indeed in this document, applies to managing the risk of existing ICS. Building an ICS Security Program and applying it to existing systems is much more complex and challenging.

4.1 Business Case for Security

The first step in implementing an information security program for ICS is to develop a compelling business case for the unique needs of the organization. The business case should capture the business concerns of senior management while being founded in the experience of those who are already dealing with many of the same risks. The business case provides the business impact and financial justification for creating an integrated information security program. It should include detailed information about the following:

- Benefits, including improved control system reliability and availability, of creating an integrated security program.
- Prioritized potential costs and damage scenarios if an information security program for the ICS is not implemented.
- High-level overview of the process required to implement, operate, monitor, review, maintain, and improve the information security program.
- Costs and resources required to develop, implement and maintain the security program.

Before presenting the business case to management, there should be a well-thought-out and developed security implementation and cost plan. For example, simply requesting a firewall is insufficient.

4.1.1 Benefits

Responsible risk management policy mandates that the threat to the ICS should be measured and monitored to protect the interests of employees, the public, shareholders, customers, vendors, society, and the nation. Risk analysis enables costs and benefits to be weighed so that informed decisions can be made on protective actions. In addition to reducing risks, exercising due-diligence and displaying responsibility also helps organizations by:

- Improving control system safety, reliability and availability.
- Improving employee morale, loyalty, and retention.
- Reducing community concerns.
- Increasing investor confidence.
- Reducing legal liabilities.
- Meeting regulatory requirements.
- Enhancing the corporate image and reputation.
- Helping with insurance coverage and cost.
- Improving investor and banking relations.

新しいシステムを設計・導入する場合は常に、アーキテクチャから調達、導入、保守、廃棄に至るまで、ライフサイクル全体を見通したセキュリティについて考察する時間を取り分けることが肝要である。セキュリティは後で考えるといった想定に基づいて、システムを生産現場に展開することには重大なリスクがある。展開前にシステムセキュリティをしっかり確保するための時間とリソースがなければ、展開後にそれを見いだすことなどおぼつかない。

新規にシステムを設計して実装することはまれである。既存のシステムを改良、拡張又は更新する場合がはるかに多い。このセクションの全て、というよりも本書の全ての部分が、既存 ICS のリスク管理に該当する。ICS セキュリティプログラムを構築して、既存システムに適用するのははるかに複雑で課題が多い。

4.1 セキュリティの事業事例

ICS の情報セキュリティプログラムを実装する第 1 ステップは、組織特有のニーズに対応した強力な事業事例を作成することである。事業事例は、同様のリスクを多分に扱ったことがある者の過去の経験に根ざしつつも、上級管理者の事業への関心事をとらえているべきである。事業事例は、統合情報セキュリティプログラムを作成する上で、事業への影響を与え、資金拠出の理由となる。以下に関する詳細な情報を網羅すべきである。

- 制御システムの信頼性・可用性の向上など、統合セキュリティプログラムを作成することにより得られる便益
- ICS の情報セキュリティプログラムを実装しない場合に生じ得る優先経費及び損害
- 情報セキュリティプログラムの実装・運用・監視・見直し・保守・改善に要するプロセスの、高レベルの概要
- セキュリティプログラムの開発・実装・保守に要する経費及びリソース

事業事例を経営陣に提示する前に、セキュリティの実装・経費計画を慎重に練り上げて作成すべきである。例えば、単にファイアウォールを要求するだけでは不十分である。

4.1.1 便益

しっかりしたリスク管理方針は、ICS に対する脅威を計測・監視して、従業員・国民・株主・顧客・ベンダー・社会・国の利益を守ることを義務づけている。リスク分析によりコスト/便益の比較考量を行うことができ、情報を基に保護対策に関する決定を下すことができる。リスク削減に加え、以下に対する当然の努力及び責任を示すことが組織の益となる。

- 制御システムの安全性・信頼性・可用性の向上
- 従業員の士気・忠誠心・勤続意欲の向上
- 共同体懸念事項の緩和
- 投資家の信頼感の増強
- 法的責任の軽減
- 法的要件の遵守
- 企業イメージ・名声の拡大
- 保険金・経費による救済
- 投資家・銀行との関係改善

A strong safety and information security management program is fundamental to a sustainable business model.

Improved control systems security and control system specific security policies can potentially enhance control system reliability and availability. This also includes minimizing unintentional control system information security impacts from inappropriate testing, policies, and misconfigured systems.

4.1.2 Potential Consequences

The importance of secure systems should be further emphasized as business reliance on interconnectivity increases. Denial of Service (DoS) attacks and malware (e.g., worms, viruses) have become all too common and have already impacted ICS. Cyber attacks can have significant physical and consequential impacts. Risk management is addressed in Section 3. The major categories of impacts are as follows:

- **Physical Impacts.** Physical impacts encompass the set of direct consequences of ICS failure. The potential effects of paramount importance include personal injury and loss of life. Other effects include the loss of property (including data) and potential damage to the environment.
- **Economic Impacts.** Economic impacts are a second-order effect from physical impacts ensuing from an ICS incident. Physical impacts could result in repercussions to system operations, which in turn inflict a greater economic loss on the facility, organization, or others dependent on the ICS. Unavailability of critical infrastructure (e.g., electrical power, transportation) can have economic impact far beyond the systems sustaining direct and physical damage These effects could negatively impact the local, regional, national, or possibly global economy.
- **Social Impacts.** Another second-order effect, the consequence from the loss of national or public confidence in an organization, is many times overlooked. It is, however, a very real consequence that could result from an ICS incident.

The program to control such risks is addressed in Section 3. Note that items in this list are not independent. In fact, one can lead to another. For example, release of hazardous material can lead to injury or death. Examples of potential consequences of an ICS incident are listed below:

- Impact on national security—facilitate an act of terrorism.
- Reduction or loss of production at one site or multiple sites simultaneously.
- Injury or death of employees.
- Injury or death of persons in the community.
- Damage to equipment.
- Release, diversion, or theft of hazardous materials.
- Environmental damage.
- Violation of regulatory requirements.
- Product contamination.
- Criminal or civil legal liabilities.
- Loss of proprietary or confidential information.
- Loss of brand image or customer confidence.

Undesirable incidents of any sort detract from the value of an organization, but safety and security incidents can have longer-term negative impacts than other types of incidents on all stakeholders—employees, shareholders, customers, and the communities in which an organization operates.

The list of potential business consequences needs to be prioritized to focus on the particular business consequences that senior management will find the most compelling. The highest priority items shown in

ビジネスモデルを持続させるには、しっかりした安全性・情報セキュリティ管理プログラムが不可欠である。

制御システムのセキュリティ及び制御システム特有のセキュリティ方針を改善すれば、制御システムの信頼性・可用性を向上させ得る。これには不適切な試験、方針及び誤設定されたシステムから生じる、制御システム情報セキュリティへの想定外の影響を極力抑えることが含まれる。

4.1.2 生じ得る結果

セキュアなシステムが重要なことは、事業が相互接続にますます依存するようになっていることからも明らかである。サービス妨害（DoS）攻撃やマルウエア（ワーム、ウイルス等）の存在は常態になっており、ICS にも影響が及んでいる。サイバー攻撃は物理的な影響や波及的な影響が大きい。リスク管理についてはセクション 3 で取り上げる。影響は以下のように大別される。

- **物理的影響。**これには ICS 障害による直接の結果が含まれる。最悪の結果として人の負傷や死亡が生じ得る。そのほか資産の喪失（データ等）や環境破壊等がある。
- **経済的影響。**これは ICS インシデントに起因する物理的影響から派生する二次的影響で、システム運用に影響を及ぼし、その結果施設、組織その他 ICS に依存するものに対し、更に大きな経済的損失をもたらす。重要インフラ（電力、輸送等）が利用不能になると、システムの直接の物理的損害をはるかに越えた経済的影響が生じる。その結果、地元、地域、国家、さらには世界経済に悪影響が及びかねない。
- **社会的影響。**これは別の二次的影響で、組織に対する国民の信頼感が失われる結果生じるが、見過ごしにされがちである。しかし、ICS インシデントから生じる実に現実的な結果である。

このようなリスクを管理するためのプログラムについてはセクション 3 で取り上げる。このリスト中の項目はそれぞれが独立しているのではない。むしろ、あるものが別のものを導くことがある。例えば、危険物の放出は負傷や死亡事故につながる。ICS インシデントから生じ得る結果を以下に例示する。

- 国家安全保障への影響–テロ行為を助長する
- 1 か所又は複数同時サイトにおける生産の減少・喪失
- 従業員の負傷・死亡
- 共同体構成員の負傷・死亡
- 装備品の損害
- 危険物の放出・流用・盗難
- 環境破壊
- 法的要件の侵害
- 製品の汚染
- 刑法又は民法上の責任
- 専有・秘密情報の喪失
- ブランドイメージ・顧客の信用の喪失

どのような種類のものであれ、望ましくないインシデントは組織の価値を減じるが、安全やセキュリティが関係するインシデントは、それ以外のインシデントに比べて、より長期的な悪影響を従業員、株主、顧客及び組織が属する共同体を含めた全ての関係者に投げかける。

可能性のある事業結果のリストから、事業結果の優先度を検討し、上級管理者が特に影響度が大きいと思えるものに注力する必要がある。優先的な事業結果リストの最優先項目を

the list of prioritized business consequences should be evaluated to obtain an estimate of the annual business impact, preferably but not necessarily in financial terms.

The Sarbanes-Oxley Act requires corporate leaders to sign off on compliance with information accuracy and protection of corporate information.[19] Also, the demonstration of due diligence is required by most internal and external audit firms to satisfy shareholders and other organization stakeholders. By implementing a comprehensive information security program, management is exercising due diligence.

4.1.3 Resources for Building Business Case

Significant resources for information to help form a business case can be found in external resources in other organizations in similar lines of business–either individually or in information sharing exchanges, trade and standards organizations, consulting firms–and internal resources in related risk management programs or engineering and operations. External organizations can often provide useful tips as to what factors most strongly influenced management to support their efforts and what resources within their organizations proved most helpful. For different industries, these factors may be different, but there may be similarities in the roles that other risk management specialists can play. Appendix D— provides a list and short description of some of the current activities in ICS security.
Internal resources in related risk management efforts (e.g., information security, health, safety and environmental risk, physical security, business continuity) can provide tremendous assistance based on their experience with related incidents in the organization. This information is helpful from the standpoint of prioritizing threats and estimating business impact. These resources can also provide insight into which managers are focused on dealing with which risks and, thus, which managers might be the most appropriate or receptive to serving as a champion. Internal resources in control systems engineering and operations can provide insight into the details of how control systems are deployed within the organization, such as the following:

- How networks are typically partitioned and segregated.
- What remote access connections are generally employed.
- How high-risk control systems or safety instrumented systems are typically designed.
- What security countermeasures are commonly used.

4.1.4 Presenting the Business Case to Leadership

Section 3 describes a three-tiered approach that addresses risk at the: (i) *organization* level; (ii) *mission/business process* level; and (iii) *information system* level. The risk management process is carried out seamlessly across the three tiers with the overall objective of continuous improvement in the organization's risk-related activities and effective inter-tier and intra-tier communication among all stakeholders having a shared interest in the mission/business success of the organization.

It is critical for the success of the ICS security program that organization level management buy into and participate in the ICS security program. Tier 1 organization level management that encompasses both IT and ICS operations has the perspective and authority to understand and take responsibility for the risks.

The Tier 1 business leadership will be responsible for approving and driving information security policies, assigning security roles and responsibilities, and implementing the information security program across the organization. Funding for the entire program can usually be done in phases. While some

[19] More information on the Sarbanes-Oxley Act, and a copy of the act itself, can be found at http://www.sec.gov/about/laws.shtml.

評価して、年間事業影響見積を作成すべきである。見積は財務的な観点から行うのが望ましいが、義務ではない。

Sarbanes-Oxley 法は、情報の正確性と企業情報[20]の保護遵守に関して、企業責任者に署名を義務づけている。またほとんどの内外監査法人に対して、然るべき努力を傾注して株主その他組織関係者を満足させるよう求めている。包括的情報セキュリティプログラムを施行することで、経営陣はしかるべき努力を傾注していることになる。

4.1.3 事業事例作成のためのリソース

事業事例の構築に役立つかなりのリソースが外部同業組織のリソースにある。例えば個々の企業、又は情報共有交換、取引組織及び規格組織、コンサルタント企業などのほか、関連リスク管理プログラムやエンジニアリング、業務といった内部リソースからも利用できる。外部組織は、経営陣の取組に最も大きな影響を与える要因について、また組織内のどのリソースが最も役立ったかといった点に関して、有用なヒントを与えてくれることが多い。業界が異なればそうした要因も異なるが、他のリスク管理担当者が果たす役割には共通点もある。付録 D には、ICS セキュリティにおける現在の活動のいくつかを簡単に紹介したリストがある。

関係するリスク管理の取組（情報セキュリティ、衛生、安全・環境リスク、物理的セキュリティ、事業継続等）における内部リソースは、組織の関連インシデントでの経験を基に、大きな助けとなる。この情報は、脅威の優先付けと事業影響の見積の観点から役立つ。こうしたリソースを活用すれば、どの管理者がどのリスクに対応しているか、またどの管理者が推進者として相応しいか、対応力があるかを判断することができよう。制御システムエンジニアリング業務の内部リソースを活用すれば、以下のような、組織への制御システムの詳細な展開方法を判断することができる。
電子メール
- ネットワークの一般的な区画・分割方法
- 一般的に採用するリモートアクセス接続
- 高リスク制御システム又は安全計装システムの一般的設計
- 共通的に使用するセキュリティ対策

4.1.4 事業事例を組織の長に提示する

セクション 3 では次の 3 レベルでのリスクに対応する 3 段階の取組について説明した。（1）組織レベル、（2）任務・事業プロセスレベル、(3)情報システムレベル。リスク管理プロセスは、組織の任務・事業の成功に共通の関心を抱く関係者間において、組織のリスク関連活動及び各段階間・各段階内の効果的なコミュニケーションを絶えず改善するという全体的な目的を持って、3 つの段階にわたってシームレスに行われる。

ICS セキュリティプログラムを成功させるには組織レベルで経営陣が同プログラムに納得して、参加することが肝要である。IT 及び ICS 業務双方を包含する第 1 段階の組織レベル経営陣には、リスクを理解し責任を引き受ける見通しと権限がある。

第 1 段階の事業のリーダーは、情報セキュリティポリシーを承認・推進し、セキュリティの役割と責任を付与し、情報セキュリティプログラムを組織全体にわたって実行する責務を負う。プログラム全体への資金拠出は、通常フェーズごとに行う。

[20] Sarbanes-Oxley 法の詳細及び入手は次の URL を参照のこと。http://www.sec.gov/about/laws.shtml.

funding may be required to start the information security activity, additional funding can be obtained later as the security vulnerabilities and needs of the program are better understood and additional strategies are developed. Additionally, the costs (both direct and indirect) should be considered for retrofitting the ICS for security vs. addressing security to begin with.

Often, a good approach to obtain management buy-in to address the problem is to ground the business case in a successful actual third-party example. The business case should present to management that the other organization had the same problem and then present that they found a solution and how they solved it. This will often prompt management to ask what the solution is and how it might be applicable to their organization.

4.2 Build and Train a Cross-Functional Team

It is essential for a cross-functional information security team to share their varied domain knowledge and experience to evaluate and mitigate risk in the ICS. At a minimum, the information security team should consist of a member of the organization's IT staff, a control engineer, a control system operator, security subject matter experts, and a member of the enterprise risk management staff. Security knowledge and skills should include network architecture and design, security processes and practices, and secure infrastructure design and operation. Contemporary thinking that both safety and security are emergent properties of connected systems with digital control suggests including a safety expert. For continuity and completeness, the information security team should also include the control system vendor and/or system integrator.

The information security team should report directly to the information security manager at the mission/business process or organization tier, who in turn reports to the mission/business process manager (e.g., facility superintendent) or enterprise information security manager (e.g., the company's CIO/CSO), respectively. Ultimate authority and responsibility rests in the Tier 1 risk executive function that provides a comprehensive, organization-wide approach to risk management. The risk executive function works with the top management to accept a level of residual risk and accountability for the information security of the ICS. Management level accountability will help ensure an ongoing commitment to information security efforts.

While the control engineers will play a large role in securing the ICS, they will not be able to do so without collaboration and support from both the IT department and management. IT often has years of security experience, much of which is applicable to ICS. As the cultures of control engineering and IT are often significantly different, their integration will be essential for the development of a collaborative security design and operation.

4.3 Define Charter and Scope

The information security manager should establish policy that defines the guiding charter of the information security organization and the roles, responsibilities, and accountabilities of system owners, mission/business process managers, and users. The information security manager should decide upon and document the objective of the security program, the business organizations affected, all the computer systems and networks involved, the budget and resources required, and the division of responsibilities. The scope can also address business, training, audit, legal, and regulatory requirements, as well as timetables and responsibilities. The guiding charter of the information security organization is a constituent of the information security architecture which is part of the enterprise architecture, as discussed in Section 3.

情報セキュリティ活動を開始するときにある程度の資金がいるが、追加資金は、セキュリティの脆弱性とプログラムの必要性がより明確になり、追加戦略を策定した後で得ることができる。またコスト（直接費・間接費）は、ICS へのセキュリティ実装と開始時のセキュリティとを考慮して決めるべきである。

経営陣が問題に関わるようにするための取組として、事業事例を成功した第三者の実例に倣うと上手く行くことが多い。事業事例は経営陣に対し、他の組織でも同じ問題を抱えたこと、解決策を見いだし、いかに解決したかを示すべきである。そうすることで経営陣は、その解決策は何か、自分たちの組織にどう応用できるのか、問うことができるようになる。

4.2 機能横断チームの組成・教育訓練

機能横断型情報セキュリティチームが多様な分野の知識・経験を共有し合い、ICS のリスクを評価・緩和することが不可欠となる。情報セキュリティチームの構成は、少なくとも組織の IT 職員、制御エンジニア、制御システム操作員、セキュリティ問題担当者及び企業のリスク管理職員を含めるべきである。セキュリティの知識・スキルには、ネットワークアーキテクチャ・設計、セキュリティプロセス・規範及びセキュアなインフラ・業務を含めるべきである。安全とセキュリティはデジタル制御を備えた接続システムの新しい特徴であるという最近の考え方には、安全のエキスパートを含めることが示唆されている。継続性と完全性を確保するため、情報セキュリティチームには、制御システムのベンダーやシステムインテグレータをも含めるべきである。

情報セキュリティチームには、任務・事業プロセス又は組織レベルの情報セキュリティ管理者に直接報告を上げるべきで、次いで同管理者はそれぞれ、任務・事業プロセス管理者（施設監督等）又は企業情報セキュリティ管理者（CIO/CSO 等）に報告する。最終的な権限と責任は、リスク管理に対して全体的、組織全体にわたる取組を行う、第 1 段階におけるリスク担当役員にある。リスク担当役員は、経営のトップと連携して、ICS の情報セキュリティに関する残りのリスクレベルと説明責任を受け入れる。経営陣レベルの説明責任は、情報セキュリティへの取組に対して行われている姿勢を確固たるものにするのに役立つ。

制御エンジニアは ICS のセキュリティ確保に大きな役割を果たすが、IT 部門と経営陣からの協力・支援がなければ務まらない。IT におけるセキュリティの経験は数年に及ぶことが多いが、その大部分は ICS にも応用できる。制御エンジニアと IT の文化はそれぞれ大きく異なるが、協力的なセキュリティの設計・実施を完成するには両者の一体化が不可欠となる。

4.3 憲章及び適用範囲の明確化

情報セキュリティ管理者は、情報セキュリティの組織、システム所有者、任務・事業プロセス管理者及びユーザの役割・責任・説明責任を明確にした、指針となる憲章を定めるべきである。情報セキュリティ管理者は、セキュリティプログラムの目的、影響を受ける事業組織、関係する全てのコンピュータシステムとネットワーク、必要な予算とリソース及び責任の分担を明らかにして、文書化すべきである。
またこれには事業、訓練、監査、法的要件及び予定表と責任も含まれる。情報セキュリティ組織の指針となる憲章は、セクション 3 で説明した企業アーキテクチャの一部をなす情報セキュリティアーキテクチャを構成する要素となる。

There may already be an information security program in place or being developed for the organization's IT business systems. The ICS information security manager should identify which existing practices to leverage and which practices are specific to the control system. In the long run, it will be easier to get positive results if the team can share resources with others in the organization that have similar objectives.

4.4 Define ICS-specific Security Policies and Procedures

Policies and procedures are at the root of every successful security program. Wherever possible, ICS-specific security policies and procedures should be integrated with existing operational/management policies and procedures. Policies and procedures help to ensure that security protection is both consistent and current to protect against evolving threats. Appendix C cites a lack of security policy as an important vulnerability. Appendix G—, the ICS overlay, contains many ICS information security policy recommendations. After an information security risk analysis has been performed, the information security manager should examine existing security policies to see if they adequately address the risks to the ICS. If needed, existing policies should be revised or new policies created.

As discussed in Section 3, Tier 1 management is responsible for developing and communicating the risk tolerance of the organization–the level of risk the organization is willing to accept–which allows the information security manager to determine the level of risk mitigation that should be taken to reduce residual risk to acceptable levels. The development of the security policies should be based on a risk assessment that will set the security priorities and goals for the organization so that the risks posed by the threats are mitigated sufficiently. Procedures that support the policies need to be developed so that the policies are implemented fully and properly for the ICS. Security procedures should be documented, tested, and updated periodically in response to policy, technology, and threat changes.

4.5 Implement an ICS Security Risk Management Framework

From an abstract viewpoint, the management of ICS risks is another risk added to the list of risks confronting an organization (e.g., financial, safety, IT, environmental). In each case, managers with responsibility for the mission or business process establish and conduct a risk management program in coordination with top management's risk executive function. NIST Special Publication 800-39, *Managing Information Security Risk–Organization, Mission, and Information System View* [20], is the foundation of such a risk management program. Just like the other mission/business process areas, the personnel concerned with ICS apply their specialized subject matter knowledge to establishing and conducting ICS security risk management and to communicating with enterprise management to support effective risk management across all the enterprise. NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems* [21], introduces the risk management framework which addresses the process of implementing the framework. The following sections summarize this process and apply the RMF to an ICS environment.

The RMF process includes a set of well-defined risk-related tasks that are to be carried out by selected individuals or groups within well-defined organizational roles (e.g., risk executive [function], authorizing official, authorizing official designated representative, chief information officer, senior information security officer, enterprise architect, information security architect, information owner/steward, information system owner, common control provider, information system security officer, and security control assessor). Many risk management roles have counterpart roles defined in the routine system development life cycle processes. RMF tasks are executed concurrently with or as part of system development life cycle processes, taking into account appropriate dependencies.

既に組織の IT 事業システムに関する情報セキュリティプログラムが施行されているか、作成中という場合もある。ICS 情報セキュリティ管理者は、既存の規範で活用できるものと、制御システムに固有の規範とを特定すべきである。長い目で見れば、組織で同様の目的を持ったチーム同士がリソースを共有し合うことで、よい結果が得やすくなる。

4.4 ICS 固有のセキュリティポリシー及び手順の明確化

ポリシーと手順は、あらゆるセキュリティプログラムを成功に導く要である。可能であれば、ICS 固有のセキュリティポリシーと手順を既存の業務/管理ポリシー及び手順と一体化すべきである。ポリシーと手順は、進化する脅威に対して、セキュリティ保護を一貫性と最新性を備えたものにする上で役立つ。付録 C には、セキュリティポリシーの欠如を重大な脆弱性として言及している。付録 G の ICS オーバーレイには、数々の ICS 情報セキュリティポリシーに関する推奨事項が含まれている。情報セキュリティのリスク分析を実施後、情報セキュリティ管理者は既存のセキュリティポリシーを検証し、ICS へのリスクがしっかり取り上げられているか確認すべきである。必要であれば、既存のセキュリティポリシーを改正するか、作り直すべきである。

セクション 3 で述べたとおり、第 1 段階の経営陣は組織のリスクトレランスを策定して伝達する責任を有する。リスクトレランスとは組織が受け入れ可能なレベルのリスクをいい、これを基に情報セキュリティ管理者は、残りのリスクを受容レベルにまで緩和するためのリスクレベル緩和策を決めることができる。セキュリティポリシーの策定は、リスク評価に基づくが、リスク評価は組織のセキュリティ優先度と目標を設定し、脅威がもたらすリスクを十分緩和できるようにする。ポリシーを支える手順は、ポリシーが ICS に対して十分かつ適正に実施できるように策定する必要がある。セキュリティ手順はポリシー、技術及び脅威の変化に対応して、文書化し、検証し、定期的に更新すべきである。

4.5 ICS セキュリティリスク管理体制の実行

抽象的なとらえ方をすれば、ICS リスクの管理は、組織が直面するリスクリスト（財政、安全、IT、環境等）に追加された付加的リスクといえる。いずれの場合も、任務や事業プロセスに責任を有する管理者は、経営トップのリスク担当役員と協調して、リスク管理プログラムを策定し実行する。NIST 特別出版物 800-39『情報セキュリティリスクの管理－組織、任務および情報システムの精査』[20]は、このようなリスク管理プログラムの基本である。他の任務・事業プロセス分野と同様、ICS に関わる人員はそれぞれの専門知識を、ICS セキュリティリスク管理の策定や、企業経営陣と連携して全社的かつ効果的なリスク管理の支援に適用する。NIST 特別出版物 800-37『連邦情報システムにリスク管理体制を適用するためのガイド』［21]は、リスク管理体制について説明し、体制構築プロセスを取り上げている。続くセクションでは、このプロセスを要約し、ICS 環境へのリスク管理体制（RMF）の適用を説明する。

RMF プロセスには、明確化された組織的役割（リスク担当役員、許可権者、許可権者が指名した代表者、最高情報責任者、情報セキュリティ主任、企業設計者、情報セキュリティ設計者、情報所有者/執事、情報システム所有者、共通制御プロバイダ、情報システムセキュリティ担当者、セキュリティ管理査定者等）の範囲内で選ばれた個人やグループが遂行すべき、明確化されたリスク関連作業が含まれている。リスク管理上の役割の多くには、恒常的なシステム開発ライフサイクルプロセスで明らかにされているものに相当する役割が含まれる。RMF 作業は、適正な相互依存を考慮に入れた上で、システム開発ライフサイクルプロセスと同時に、又はその一部として実施する。

Organizations may also wish to consult ISA-62443-2-1, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*, which describes another view of the elements contained in a cybersecurity management system for use in the industrial automation and control systems environment [34]. It provides guidance on how to meet the requirements described for each element. Sections 4 through 6 correspond most closely to NIST SP 800-39; other sections correspond to other NIST Special Publications and to the ICS overlay in Appendix G— of this document. All of these guidance documents recognize that one size does not fit all; rather, domain knowledge should be applied in tailoring or adapting the guidance to the specific organization.

4.5.1 Categorize ICS Systems and Networks Assets

The information security team should define, inventory, and categorize the applications and computer systems within the ICS, as well as the networks within and interfacing to the ICS. The focus should be on systems rather than just devices, and should include PLCs, DCS, SCADA, and instrument-based systems that use a monitoring device such as an HMI. Assets that use a routable protocol or are dial-up accessible should be documented. The team should review and update the ICS asset list annually and after each asset addition or removal.

There are several commercial enterprise IT inventory tools that can identify and document all hardware and software resident on a network. Care must be taken before using these tools to identify ICS assets; teams should first conduct an assessment of how these tools work and what impact they might have on the connected control equipment. Tool evaluation may include testing in similar, non-production control system environments to ensure that the tools do not adversely impact the production systems. Impact could be due to the nature of the information or the volume of network traffic. While this impact may be acceptable in IT systems, it may not be acceptable in an ICS.

An automated management system for inventory (e.g., Computerized Maintenance Management System (CMMS), Computer Aided Facility Management System (CAFM), Building Information Model (BIM), Geospatial Information System (GIS), Construction-Operations Building information exchange data (COBie, Building Automation Management information exchange (BAMie), Sustainment Management Systems (SMS) Builder) allows an organization to keep an accurate account of what is on the system for security reasons and budgetary reasons as well.

4.5.2 Select ICS Security Controls

The security controls selected based on the security categorization of the ICS are documented in the security plan to provide an overview of the security requirements for the ICS information security program and describes the security controls in place or planned for meeting those requirements. The development of security plans is addressed in NIST Special Publication 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems* [19]. The security plan can be one document, or it can be the set of all documents addressing the security concerns for a system and the plans for countering these concerns. In addition to security controls, NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [20], provides a set of information security program management (PM) controls that are typically implemented at the organization level and not directed at individual organizational information systems. This section addresses how an organization establishes and carries out these program management controls.

The successful implementation of security controls for organizational information systems depends on the successful implementation of organization-wide program management controls. The manner in which organizations implement the program management controls depends on specific organizational characteristics including, for example, the size, complexity, and mission/business requirements of the

ISA-62443-2-1『産業オートメーション及び制御システムのセキュリティ：産業オートメーション及び制御システムのセキュリティプログラムの構築』[34]は、産業オートメーション及び制御システム環境用のサイバーセキュリティ管理システムに対する別の見方を紹介しており、参考にすることができよう。要素ごとに要件を満足するための方法について、指針が記載されている。セクション 4～6 は NIST SP 800-39 にほぼ対応しており、他のセクションはそれ以外の NIST 特別出版物及び本書付録 G の ICS オーバーレイに対応している。これらガイダンス文書はどれもみな、一つのサイズで全てにフィットするようなものはないと述べている。むしろ、ある分野の知見を応用して、ガイダンスを特定の組織に適応させるべきである。

4.5.1 ICS システムとネットワーク資産の分類

情報セキュリティチームは、ICS 内のアプリケーション及びコンピュータシステム並びに ICS 内及び ICS と連接するネットワークを定義し、目録を作成し、分類すべきである。デバイスのみならずシステムに配慮し、PLCs、DCS、SCADA、その他 HMI 等の監視デバイスを使用する計器主体のシステムも含めるべきである。ルーティングプロトコルを使用する資産やダイアルアップでアクセスする資産は文書化すべきである。チームは ICS 資産リストを年に一度、また追加や削除があるたびに見直して更新すべきである。

ネットワークに常駐している全てのハードウエア/ソフトウエアを識別して記録できる、市販の企業 IT インベントリーツールがいくつかある。そうしたツールを使用して ICS 資産を識別する前に注意が必要となる。チームはまずツールの働きと、接続された制御装備品に及ぶ影響を調べるべきである。ツールを評価するには、類似の非生産環境における試験を行い、生産システムには悪影響がないことを確認するとよい。影響は、情報の性質やネットワークトラフィック量に起因することがある。そうした影響は IT システムでは許容できても、ICS では受け入れられないことがある。

インベントリー用自動管理システム（コンピュータ保守管理システム[CMMS]、コンピュータ援用施設管理システム[CAFM]、ビル情報モデル[BIM]、地理空間情報システム[GIS]、建設作業ビル情報交換データ[COBie]、ビルオートメーション管理情報交換[BAMie]、持続管理システム[SMS]ビルダー等）はセキュリティ目的と予算目的でシステム上にあるものを正確に把握することができる。

4.5.2 ICS セキュリティ管理の選択

ICS のセキュリティ分類に従って選択したセキュリティ管理は、セキュリティ計画書に記録され、ICS 情報セキュリティプログラムのセキュリティ要件の概要を示し、要件を遵守するために施行中又は計画中のセキュリティ管理について説明を与える。セキュリティ計画書の作成については、NIST 特別出版物 800-18 改訂第 1 版『連邦情報システム用セキュリティ計画書の作成ガイド』[19]で取り上げられている。セキュリティ計画書は一冊の文書でもよく、システムのセキュリティ上の課題とその対処計画を収めた全文書の一部であってもよい。セキュリティ管理に加えて、NIST 特別出版物 800-53 改訂第 4 版『連邦情報システム・組織用セキュリティ・プライバシー管理』[20]には、一般に組織レベルで実装され、個々の組織情報システムにはない情報セキュリティプログラム管理（PM）制御について取り上げられている。このセクションでは、プログラム管理制御の構築及び実施要領について取り上げる。

組織の情報システム用セキュリティ管理を首尾よく実装できるかどうかは、組織全体にわたるプログラム管理制御を首尾よく実装できるかどうかにかかっている。プログラム管理制御の実装方法は、それぞれの企業の規模、複雑性、任務・事業要件といった企業の性格に左右される。

respective organizations. The program management controls complement the security controls and focus on the programmatic, organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. Organizations document program management controls in the *information security program plan*. The organization-wide information security program plan supplements the individual security plans developed for each organizational information system. Together, the security plans for the individual information systems and the information security program cover the totality of security controls employed by the organization.

4.5.3 Perform Risk Assessment

Because every organization has a limited set of resources, organizations should assess the impacts to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation (e.g., using FIPS 199 [15] or a more granular approach). As discussed in Section 3, organizations can experience the consequences/impact of adverse events at the individual ICS system level (e.g., failing to perform as required), at the mission/business process level (e.g., failing to fully meet mission/business objectives), and at the organizational level (e.g., failing to comply with legal or regulatory requirements, damaging reputation or relationships, or undermining long-term viability). An adverse event can have multiple consequences and different types of impact, at different levels, and in different time frames. NIST SP 800-53 [22] and the ICS overlay in Appendix G— incorporate baseline security controls that derive from this determination of impact.

The organization may perform a detailed risk assessment for the highest impact systems and assessments for lower impact systems as deemed prudent and as resources allow. The risk assessment will help identify any weaknesses that contribute to information security risks and mitigation approaches to reduce the risks. Risk assessments are conducted multiple times during a system's life cycle. The focus and level of detail varies according to the system's maturity.

4.5.4 Implement the Security Controls

Organizations should analyze the detailed risk assessment and the impacts to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, and prioritize selection of mitigation controls. Organizations should focus on mitigating risk with the greatest potential impact. Security control implementation is consistent with the organization's enterprise architecture and information security architecture.

The controls to mitigate a specific risk may vary among types of systems. For example, user authentication controls might be different for ICS than for corporate payroll systems and e-commerce systems. The ICS information security manager should document and communicate the selected controls, along with the procedures for using the controls. Some risks may be identified that can be mitigated by "quick fix" solutions—low-cost, high-value practices that can significantly reduce risk. Examples of these solutions are restricting Internet access and eliminating email access on operator control stations or consoles. Organizations should identify, evaluate, and implement suitable quick fix solutions as soon as possible to reduce security risks and achieve rapid benefits. The Department of Energy (DOE) has a "21 Steps to Improve Cyber Security of SCADA Networks" [33] document that could be used as a starting point to outline specific actions to increase the security of SCADA systems and other ICS.

プログラム管理制御はセキュリティ管理を補完するもので、特定の情報システムから独立した、情報セキュリティプログラムの管理に不可欠な、プログラムに従った全組織的情報セキュリティ要件に焦点を当てている。
組織は、プログラム管理制御を情報セキュリティプログラム計画書の中に記載する。全組織的情報セキュリティプログラム計画書は、各組織の情報システム用個別セキュリティ計画書を補完する。同時に個々の情報システム用セキュリティ計画書と情報セキュリティプログラムは、組織が採用するセキュリティ管理を全体的に網羅する。

4.5.3 リスク評価実施

どの組織にもある程度のリソースがあるため、組織は組織業務への影響（任務、機能、イメージ、評判等）、組織の資産、個人、他の組織や国に対する影響を評価すべきである（FIPS199[15]その他のアプローチを使用）。セクション 3 で説明したように、組織は個々の ICS システムレベルで（要件不履行等）、任務・事業プロセスレベルで（任務・事業目的の不完全な遂行等）、組織レベルで（法的要件の不履行、評判・関係の毀損、長期的実現性の阻害等）、有害事象の結果・影響を被ることがある。有害事象がもたらす結果は種々あり、多様な影響が様々なレベルや時間帯で生じることがある。NIST SP 800-53[22]及び付録 G の ICS オーバーレイには、この影響判定から得た基本となるセキュリティ管理が取り上げられている。

組織は適切と考えられる場合、リソースの許す範囲で、最大の影響を受けるシステムには詳細なリスク評価を行い、比較的影響の少ないシステムにも評価を行うことができる。リスク評価は、情報セキュリティのリスクに寄与する弱点と、リスク緩和策を見極めるのに役立つ。リスク評価はシステムのライフサイクル期間中、何度も行う。重点と詳細レベルはシステムの完成度に応じて異なる。

4.5.4 セキュリティ管理の実装

組織は詳細なリスク評価と、組織業務（任務、機能、イメージ、評判等）、組織資産、個人、他の組織や国に対する影響を分析し、緩和策の選定を優先付けすべきである。また最大の影響がありそうなリスクの緩和に注力すべきである。セキュリティ管理の実装は、組織の企業アーキテクチャ及び情報セキュリティアーキテクチャと整合する。

特定のリスクの緩和策は、システムの種類に応じて異なる。例えば、ICS でのユーザ認証管理は、企業の給与支払システムや e コマースシステムとは異なる。ICS 情報セキュリティ管理者は、選んだ対策とその使用手順について記録し、伝達すべきである。「迅速補修」ソリューション、つまりリスクを大幅に減らせる低コストで高価値な規範により緩和可能なリスクが明らかになることがある。こうしたソリューションの例として、操作員制御ステーションやコンソールへのインターネットアクセスの制限、電子メールアクセスの排除などがある。組織はセキュリティリスクを減らし、すぐに便益が得られるように、適正な迅速補修策の識別・評価・実装を可及的速やかに行うべきである。エネルギー省（DOE）には『SCADA ネットワークのサイバーセキュリティを改善する 21 のステップ』[33]があり、SCADA システムその他 ICS の具体的セキュリティ向上策を考えるスターティングポイントとして使用することができる。

5. ICS Security Architecture

When designing a network architecture for an ICS deployment, it is usually recommended to separate the ICS network from the corporate network. The nature of network traffic on these two networks is different: Internet access, FTP, email, and remote access will typically be permitted on the corporate network but should not be allowed on the ICS network. Rigorous change control procedures for network equipment, configuration, and software changes may not be in place on the corporate network. If ICS network traffic is carried on the corporate network, it could be intercepted or be subjected to DoS or Man-in-the-Middle attacks [5.14]. By having separate networks, security and performance problems on the corporate network should not be able to affect the ICS network.
Practical considerations, such as cost of ICS installation or maintaining a homogenous network infrastructure, often mean that a connection is required between the ICS and corporate networks. This connection is a significant security risk and should be protected by boundary protection devices. If the networks must be connected, it is strongly recommended that only minimal (single if possible) connections be allowed and that the connection is through a firewall and a DMZ. A DMZ is a separate network segment that connects directly to the firewall. Servers containing the data from the ICS that needs to be accessed from the corporate network are put on this network segment. Only these systems should be accessible from the corporate network. With any external connections, the minimum access should be permitted through the firewall, including opening only the ports required for specific communication. The following sections elaborate on these architectural considerations. The ICS-CERT recommended practices working group provides additional guidance as recommended practices[21].

5.1 Network Segmentation and Segregation

This section addresses partitioning the ICS into security domains and separating the ICS from other networks, such as the corporate network, and presents illustrative security architecture. Operational risk analysis should be performed to determine critical parts of each ICS network and operation and help define what parts of the ICS need to be segmented. Network segmentation involves partitioning the network into smaller networks. For example, one large ICS network is partitioned into multiple ICS networks, where the partitioning is based on factors such as management authority, uniform policy and level of trust, functional criticality, and amount of communications traffic that crosses the domain boundary. Network segmentation and segregation is one of the most effective architectural concepts that an organization can implement to protect its ICS. Segmentation establishes security domains, or enclaves, that are typically defined as being managed by the same authority, enforcing the same policy, and having a uniform level of trust. Segmentation can minimize the method and level of access to sensitive information, ICS communication and equipment configuration, and can make it significantly more difficult for a malicious cyber adversary and can contain the effects of non-malicious errors and accidents. A practical consideration in defining a security domain is the amount of communications traffic that crosses the domain boundary, because domain protection typically involves examining boundary traffic and determining whether it is permitted.

The aim of network segmentation and segregation is to minimize access to sensitive information for those systems and people who don’t need it, while ensuring that the organization can continue to operate effectively. This can be achieved using a number of techniques and technologies depending on the network’s architecture and configuration.

[21] ICS-CERT recommended practices may be found at http://ics-cert.us-cert.gov/Recommended-Practices.

5. ICS セキュリティアーキテクチャ

ICS 展開のネットワークアーキテクチャを設計する際には、ICS ネットワークを企業ネットワークから切り離すことが常に推奨される。両者におけるネットワークトラフィックの性質は異なる。企業ネットワークではインターネットアクセス、FTP、電子メール及びリモートアクセスが通常許可されているが、ICS ネットワークでは許可すべきでない。ネットワーク装備品、構成及びソフトウエア変更に関する厳格な変更管理手順は、企業ネットワークでは実施されない。ICS ネットワークを企業ネットワークと一緒にすると、傍受されたり DoS や人が介在する攻撃にさらされかねない[5.14]。ネットワークを切り離すことで、企業ネットワークの性能や問題が生じても、ICS ネットワークには影響が及ばない。

ICS の設置コストや均質なネットワークインフラの保守コストといった現実的な考慮の結果、ICS ネットワークと企業ネットワークを接続することがよくある。このような接続には大きなセキュリティリスクがあり、境界保護デバイスで保護すべきである。両ネットワークを接続する場合、接続を最小限（可能ならシングル）にとどめ、ファイアウォールと DMZ を設けることが強く推奨される。DMZ は別個のネットワークセグメントで、ファイアウォールに直接接続される。ICS からのデータを持っているサーバで、企業ネットワークから接続するものについては、このネットワークセグメントに置く。企業ネットワークから接続可能なのは、このようなシステムのみとすべきである。どのような外部接続であれ、最小限のアクセスのみファイアウォール経由で許可し、特定の接続に必要なポートのみ開放すべきである。続くセクションでは、このようなアーキテクチャ上の考慮事項を詳しく取り上げる。ICS-CERT 推奨規範作業グループは、推奨規範として付加的なガイダンスを提供している。[22]

5.1 ネットワークの分割と分離

このセクションでは、ICS のセキュリティ領域への区画化と、企業ネットワーク等他のネットワークからの ICS の分離について説明し、セキュリティアーキテクチャの例を示す。業務上のリスク分析を実施し、各 ICS ネットワーク及び業務の重要部分を判別し、分割すべき ICS 部位の明確化を支援する。ネットワークの分割には、ネットワークをより小さいネットワークに区画することが含まれる。例えば、大きな ICS ネットワークを複数の ICS ネットワークに区画化するが、区画は経営陣の権限、統一的なポリシー及び信頼レベル、機能上の重要度、領域境界を越える通信トラフィック量といった要因を基にする。ネットワークの分割と分離は、組織がその ICS 防護のために実装できる最も効果的なアーキテクチャ概念の 1 つである。分割によってセキュリティアーキテクチャ領域、つまり飛び地ができるが、これは同じポリシーを施行し、統一された信頼レベルを持つ同一の権限により管理されるものと、一般に定義されている。分割により要注意情報、ICS 通信、及び装備品設定へのアクセス方法やレベルを最小限に抑え、悪意あるサイバー攻撃を著しく困難にし、悪意によらない過誤や事故の影響を封じ込めることができる。セキュリティ領域を明確にする際の現実的な考慮事項として、領域境界を越える通信トラフィック量がある。というのは、領域の保護には、通常境界トラフィックの検証と許可の有無に対する判定が関係しているからである。

ネットワーク分割・分離の主眼は、必要としていないシステムや人が要注意情報にアクセスするのを最小限に抑える一方で、組織の円滑な業務遂行を確保することにある。これは、ネットワークアーキテクチャ及び構成に応じて、種々の技法や技術を駆使することで達成される。

[22] ICS-CERT 推奨の規範については、右記のページを参照のこと。http://ics-cert.us-cert.gov/Recommended-Practices.

Traditionally, network segmentation and segregation is implemented at the gateway between domains. ICS environments often have multiple well-defined domains, such as operational LANs, control LANs, and operational DMZs, as well as gateways to non-ICS and less trustworthy domains such as the Internet and the corporate LANs. When insider attacks, social engineering, mobile devices, and other vulnerabilities and predisposing conditions discussed in Appendix C— are considered, protecting domain gateways is prudent and worth considering.

Network segregation involves developing and enforcing a ruleset controlling which communications are permitted through the boundary. Rules typically are based on source and destination identity and the type or content of the data being transferred.

When implementing network segmentation and segregation correctly you are minimizing the method and level of access to sensitive information. This can be achieved using a variety of technologies and methods. Depending on the architecture and configuration of your network, some of the common technologies and methods used include:

- Logical network separation enforced by encryption or network device-enforced partitioning.
  - Virtual Local Area Networks (VLANS).
  - Encrypted Virtual Private Networks (VPNs) use cryptographic mechanisms to separate traffic combined on one network.
  - Unidirectional gateways restrict communications between connections to a single direction, therefore, segmenting the network.
- Physical network separation to completely prevent any interconnectivity of traffic between domains.
- Network traffic filtering which can utilize a variety of technologies at various network layers to enforce security requirements and domains.
  - Network layer filtering that restricts which systems are able to communicate with others on the network based on IP and route information.
  - State‐based filtering that restricts which systems are able to communicate with others on the network based on their intended function or current state of operation.
  - Port and/or protocol level filtering that restricts the number and type of services that each system can use to communicate with others on the network.
  - Application filtering that commonly filters the content of communications between systems at the application layer. This includes application-level firewalls, proxies, and content-based filter.

Some vendors are making products to filter ICS protocols at the application level which they market as ICS firewalls.

Regardless of the technology chosen to implement network segmentation and segregation, there are four common themes that implement the concept of defense-in-depth by providing for good network segmentation and segregation:

- Apply technologies at more than just the network layer. Each system and network should be segmented and segregated, where possible, from the data link layer up to and including the application layer.
- Use the principles of least privilege and need‐to‐know. If a system doesn’t need to communicate with another system, it should not be allowed to. If a system needs to talk only to another system on a specific port or protocol and nothing else–or it needs to transfer a limited set of labeled or fixed-format data, it should be restricted as such.

従来ネットワークの分割・分離は、領域間のゲートウェイに実装される。ICS 環境は、業務用 LAN、管理用 LAN、業務用 DMZ、非 ICS へのゲートウェイ、インターネット、企業 LAN 等信頼性の低い領域へのゲートウェイといった、明確に定義された複数の領域を持つものが多い。付録 C で取り上げられているインサイダー攻撃、ソーシャルエンジニアリング、モバイルデバイスその他の脆弱性及び弱点となる状態について検討する場合、領域ゲートウェイを防護することは堅実であり、検討に値する。

ネットワークの分割には、境界を越えてもよい通信を管理する規則を策定し、実行することが含まれる。規則は、送信データの発信元・着信先 ID、種類又は内容を基にする。

ネットワークの分割・分離を適正に実装すれば、要注意情報へのアクセス方法やレベルを最小限に抑えることになる。これは多様な技術や方法を用いることで実現する。ネットワークのアーキテクチャ及び構成に応じて、共通に用いられる技術・方法として次のようなものがある。

- 暗号化又はネットワークデバイスによる区画化により実行される論理ネットワーク分離
  - 仮想 LAN（VLANS）
  - 暗号化仮想プライベートネットワーク（VPNs）は暗号メカニズムを使用して、あるネットワーク上のトラフィックの結合を分離する
  - 単方向ゲートウェイは接続点間の通信を一方向に制限して、ネットワークを分割する
- 物理的ネットワーク分離は領域間のトラフィックの相互連接を全て防止する
- ネットワークトラフィックフィルタリングは多様な技術を種々のネットワーク層で使用し、セキュリティ要件及び領域を施行する
  - ネットワーク層フィルタリングは、IP 及びルート情報を基に、ネットワーク上の他のシステムと交信可能なシステムを制限する
  - 状態ベースフィルタリングは、目的とする機能や動作の現状を基に、ネットワーク上の他のシステムと交信可能なシステムを制限する
  - ポート又はプロトコルレベルフィルタリングは、ネットワーク上の他のシステムと交信するためにシステムが使用できるサービスの数と種類を制限する
  - アプリケーションフィルタリングは通常、システム間の交信内容をアプリケーション層でフィルタリングする。アプリケーションレベルのファイアウォール、プロキシ及びコンテンツベースのフィルターが含まれる。

ベンダーによっては、製品が ICS プロトコルをアプリケーションレベルでフィルタリングするようになっており、これを ICS ファイアウォールとして販売している。

ネットワーク分割・分離のために選んだ技術とはかかわりなく、良好なネットワーク分割・分離を具備することで、多層防御概念を実装する次の 4 つの共通的なテーマがある。

- ネットワーク層以外にも技術を適用する。可能であれば、データリンク層からアプリケーション層までシステムごとにネットワークごとに分割・分離すべきである。
- 最小権限の原則と知る必要の原則を適用する。他のシステムとの通信が不要であれば、不許可とすべきである。他のシステムと特定のポートやプロトコルでのみ交信する場合、又は限定されたラベルのデータセットや固定様式のデータのみを送信する場合、そのように制限すべきである。

- Separate information and infrastructure based on security requirements. This may include using different hardware or platforms based on different threat and risk environments in which each system or network segment operates. The most critical components require more strict isolation from other components. In addition to network separation, the use of virtualization could be employed to accomplish the required isolation.
- Implement whitelisting[23] instead of blacklisting; that is, grant access to the known good, rather than denying access to the known bad. The set of applications that run in ICS is essentially static, making whitelisting more practical. This will also improve an organization's capacity to analyze log files.

5.2 Boundary Protection

Boundary protection devices control the flow of information between interconnected security domains to protect the ICS against malicious cyber adversaries and non-malicious errors and accidents. Transferring information between systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. Boundary protection devices are key components of specific architectural solutions that enforce specific security policies. Organizations can isolate ICS and business system components performing different missions and/or business functions. Such isolation limits unauthorized information flows among system components and also provides the opportunity to deploy greater levels of protection for selected components. Separating system components with boundary protection mechanisms provides the capability for increased protection of individual components and more effective control of information flows between those components.

Boundary protection controls include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, intrusion detection systems (networked and host-based), encrypted tunnels, managed interfaces, mail gateways, and unidirectional gateways (e.g., data diodes). Boundary protection devices determine whether data transfer is permitted, often by examining the data or associated metadata.

Network and ICS security architects must decide which domains are to be permitted direct communication, the policies governing permitted communication, the devices to be used to enforce the policy, and the topology for provisioning and implementing these decisions, which are typically based on the trust relationship between domains. Trust involves the degree of control that the organization has over the external domain (e.g., another domain in the same organization, a contracted service provider, the Internet).

Boundary protection devices are arranged in accordance with organizational security architecture. A common architectural construct is the demilitarized zones (DMZ), a host or network segment inserted as a "neutral zone" between security domains. Its purpose is to enforce the ICS domain's information security policy for external information exchange and to provide external domains with restricted access while shielding the ICS domain from outside threats.

Additional architectural considerations and functions that can be performed by boundary protection devices for inter-domain communications include:

[23] A **whitelist** is a list or register of those that are being provided a particular privilege, service, mobility, access or recognition. Only those on the list will be accepted, approved or recognized (i.e., permitted). Whitelisting is the reverse of blacklisting, the practice of identifying those that are denied, unrecognized, or ostracized (i.e., prohibited).

- セキュリティ要件に基づき、情報とインフラを分離する。これには、種々の脅威や各システム又はネットワークセグメントが動作するリスク環境に従って、異なるハードウエアやプラットホームを使用することが含まれる。最重要コンポーネントは、他のコンポーネントからより厳格に分離する必要がある。ネットワークの分離に加えて、必要な分離を実現するために仮想化を用いることができる。
- ブラックリストではなくホワイトリスト [24]を実行する。つまり、既知の悪にアクセスを拒否するのではなく、既知の良にアクセスを許可する。ICS で実行するアプリケーションセットは基本的に静的であるため、ホワイトリストがより現実的である。これにより組織のログファイル分析能力も向上する。

5.2 境界の保護

境界の保護デバイスは、連接されたセキュリティ領域間の情報の流れを制御し、ICS を悪意あるサイバー攻撃や悪意のない過誤・事故から保護する。別のセキュリティポリシーを持ったセキュリティ領域の異なるシステム間で情報送信することは、領域のセキュリティポリシーを少なくとも一つは犯すというリスクが持ち込まれる。境界保護デバイスは、特定のセキュリティポリシーを施行する特定のアーキテクチャソリューションの重要コンポーネントである。
組織は ICS と、別の任務や事業機能を果たしている事業システムコンポーネントを分離することができる。分離することで、システムコンポーネント間の未許可情報の流れを制限し、選定したコンポーネントにより高レベルの保護を与える。境界保護メカニズムを備えたシステムコンポーネントを分離することで、個々のコンポーネントの保護能力が向上し、これらコンポーネント間の情報の流れをより効果的に制御することができる。

境界保護制御には、ゲートウェイ、ルータ、ファイアウォール、ガード、ネットワークベースの悪意あるコード解析・仮想化システム、侵入検知システム（ネットワーク及びホストベース）、暗号化トンネル、管理インタフェース、メールゲートウェイ及び単方向ゲートウェイ（データダイオード等）が含まれる。境界保護デバイスは、データ又は関連メタデータを検証することで、データ送信が許可されているかどうかを判定する。

ネットワーク及び ICS セキュリティの設計者は、直接交信を許可すべき領域、許可された交信を統制するポリシー、ポリシーの実行用デバイスを決定し、通常、ドメイン間の信頼関係を基にした、このような決定の準備・実装トポロジーも決定しなければならない。信頼には、組織が外部領域（同じ組織内の別領域、委託サービスプロバイダ、インターネット等）に対して有する制御の程度が関係する。

境界保護デバイスは、組織のセキュリティアーキテクチャに従って配置する。共通的なアーキテクチャ構成は、非武装地帯（DMZ）、ホスト又はセキュリティ領域間に「中立地帯」として挿入されたネットワークセグメントとなる。目的は、外部との情報交換用 ICS 領域情報セキュリティポリシーを施行し、ICS 領域を外部脅威からシールドしつつ、外部領域にアクセス制限を課することにある。

領域間交信用境界保護デバイスにより実施可能な付加的なアーキテクチャの考慮事項及び機能には次のものがある。

[24] ホワイトリストとは、特定の権限、サービス、移動、アクセス又は認識を付与された人員の登録リストをいう。リストに掲載されている者のみが受容、承認又は認識（許可）される。ホワイトリストはブラックリストの反対で、後者は拒否、非認識又は追放（禁止）された者を識別することをいう。

- Denying communications traffic by default and allowing communications traffic by exception (i.e., deny all, permit by exception). A deny-all, permit-by-exception communications traffic policy ensures that only those connections which are approved are allowed. This is known as a white-listing policy.
- Implementing proxy servers that act as an intermediary for external domains' requesting information system resources (e.g., files, connections, or services) from the ICS domain. External requests established through an initial connection to the proxy server are evaluated to manage complexity and to provide additional protection by limiting direct connectivity.
- Preventing the unauthorized exfiltration of information. Techniques include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to protocol formats and specification at the application layer and serve to identify vulnerabilities that cannot be detected by devices operating at the network or transport layers. The limited number of formats, especially the prohibition of free form text in email, eases the use of such techniques at ICS boundaries.
- Only allowing communication between authorized and authenticated source and destinations address pairs by one or more of the organization, system, application, and individual.
- Extending the DMZ concept to other separate subnetworks is useful, for example, in isolating ICS to prevent adversaries from discovering the analysis and forensics techniques of organizations.
- Enforcing physical access control to limit authorized access to ICS components.
- Concealing network addresses of ICS components from discovery (e.g., network address not published or entered in domain name systems), requiring prior knowledge for access.
- Disabling control and troubleshooting services and protocols, especially those employing broadcast messaging, which can facilitate network exploration.
- Configuring boundary protection devices to fail in a predetermined state. Preferred failure states for ICS involve balancing multiple factors including safety and security.
- Configuring security domains with separate network addresses (i.e., as disjoint subnets).
- Disabling feedback (e.g., non-verbose mode) to senders when there is a failure in protocol validation format to prevent adversaries from obtaining information.
- Implementing one-way data flow, especially between different security domains.
- Establishing passive monitoring of ICS networks to actively detect anomalous communications and provide alerts.

5.3 Firewalls

Network firewalls are devices or systems that control the flow of network traffic between networks employing differing security postures. In most modern applications, firewalls and firewall environments are discussed in the context of Internet connectivity and the UDP/IP protocol suite. However, firewalls have applicability in network environments that do not include or require Internet connectivity. For example, many corporate networks employ firewalls to restrict connectivity to and from internal networks servicing more sensitive functions, such as the accounting or human resource departments. Firewalls can

- デフォルトで通信トラフィックを拒絶し、例外的に通信トラフィックを許可する（全て拒絶し、例外のみ許可）。全て拒絶、例外のみ許可の通信トラフィックポリシーは、承認済みの接続だけが許可されるようにする。これはホワイトリストポリシーとして知られている。
- プロキシサーバを実装し、外部領域から ICS 領域への情報システムリソース（ファイル、接続、サービス等）要求を仲介させる。プロキシサーバへの最初の接続を通じて確立される外部要求は、複雑性を管理し、直接接続を制限することで付加的な保護を与えるために評価を受ける。
- 許可されていない情報がすり抜けることを防止する。例えば、ディープパケットインスペクションファイアウォール、XML、ゲートウェイ等の技術がある。これらデバイスは、プロトコル形式と仕様の整合性をアプリケーション層で検証し、ネットワーク層やトランスポート層で動作するデバイスには検出できない脆弱性を特定する。形式の数が限定されており、特に電子メールにおける自由フォーマットは禁じられているため、このような技術を ICS 境界で使用するのは容易である。
- 組織、システム、アプリケーション及び個人の 1 つ又は複数の承認・認証済みソースと宛先アドレスのペア間でのみ交信を許可する。
- DMZ の概念をほかの分離サブネットワークに拡張するのは有用で、例えば、ICS を隔離する際に、攻撃側が組織の分析や捜査技術を見いだせないようにできる。
- 物理的アクセス制御を実施して、ICS コンポーネントへのアクセス許可を制限する。
- ICS コンポーネントのネットワークアドレスが分からないように隠蔽し（公開しない、ドメイン名システムに入れないなど）、事前の知識がなければアクセスできないようにする。
- 管理サービス、トラブルシューティングサービス及びプロトコルを使用不能にする。特にネットワーク探査が容易にできるブロードキャストメッセージを使用しているものについて言える。
- 境界保護デバイスが決められた状態で機能しなくなるように設定する。ICS に対する故意の機能不能状態は、安全性とセキュリティ等種々の要因間でバランスを取ることが関係する。
- セキュリティ領域に独立したネットワークアドレスを設定する（全く別のサブネット等）。
- プロトコルの妥当性検証形式に不備がある場合、送信側にフィードバックを送らない（非冗長モード等）ようにして、攻撃側が情報を得られなくする。
- 単方向のデータフローを特に別々のセキュリティ領域間に実装する。
- ICS ネットワークをパッシブ監視して、異常交信を積極的に検出し、アラートを発する。

5.3 ファイアウォール

ファイアウォールは、別々のセキュリティ状態にあるネットワーク間で、ネットワークトラフィックの流れを制御するデバイス又はシステムのことである。ほとんどの新しいアプリケーションでは、ファイアウォール及びファイアウォール環境は、インターネット接続や UDP/IP プロトコルスイーツとの関係で言及される。ただしファイアウォールは、インターネット接続を含まない、又は必要としないネットワーク環境にも適用可能である。例えば、多くの企業ネットワークではファイアウォールを使用して、会計や人事部門等、秘匿を要する機能を果たす社内ネットワークへの接続を制限している。更にファイアウォールは、

further restrict ICS inter-subnetwork communications between functional security subnets and devices. By employing firewalls to control connectivity to these areas, an organization can prevent unauthorized access to the respective systems and resources within the more sensitive areas. There are three general classes of firewalls:

- **Packet Filtering Firewalls.** The most basic type of firewall is called a packet filter. Packet filter firewalls are essentially routing devices that include access control functionality for system addresses and communication sessions. The access control is governed by a set of directives collectively referred to as a rule set. In their most basic form, packet filters operate at layer 3 (network) of the Open Systems Interconnection (OSI), ISO/IEC 7498 model. This type of firewall checks basic information in each packet, such as IP addresses, against a set of criteria before forwarding the packet. Depending on the packet and the criteria, the firewall can drop the packet, forward it, or send a message to the originator. This type of firewall can offer a high level of security, but could result in overhead and delay impacts on network performance.
- **Stateful Inspection Firewalls.** Stateful inspection firewalls are packet filters that incorporate added awareness of the OSI model data at layer 4 (transport). Stateful inspection firewalls filter packets at the network layer, determine whether session packets are legitimate, and evaluate the contents of packets at the transport layer (e.g., TCP, UDP) as well. Stateful inspection keeps track of active sessions and uses that information to determine if packets should be forwarded or blocked. It offers a high level of security and good performance, but it may be more expensive and complex to administer. Additional rule sets for ICS applications may be required.
- **Application-Proxy Gateway Firewalls.** This class of firewalls examines packets at the application layer and filters traffic based on specific application rules, such as specified applications (e.g., browsers) or protocols (e.g., FTP). Firewalls of this type can be very effective in preventing attacks on the remote access and configuration services provided by ICS components. They offer a high level of security, but could have overhead and delay impacts on network performance, which can be unacceptable in an ICS environment. NIST SP 800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy* [85], provides general guidance for the selection of firewalls and the firewall policies.

In an ICS environment, firewalls are most often deployed between the ICS network and the corporate network [34]. Properly configured, they can greatly restrict undesired access to and from control system host computers and controllers, thereby improving security. They can also potentially improve a control network's responsiveness by removing non-essential traffic from the network. When properly designed, configured, and maintained, dedicated hardware firewalls can contribute significantly to increasing the security of today's ICS environments.
Firewalls provide several tools to enforce a security policy that cannot be accomplished locally on the current set of process control devices available in the market, including the ability to:

- Block all communications with the exception of specifically enabled communications between devices on the unprotected LAN and protected ICS networks. Blocking can be based on, for example, source and destination IP address pairs, services, ports, state of the connection, and specified applications or protocols supported by the firewall. Blocking can occur on both inbound and outbound packets, which is helpful in limiting high-risk communications such as email.
- Enforce secure authentication of all users seeking to gain access to the ICS network. There is flexibility to employ varying protection levels of authentication methods including simple passwords, complex passwords, multi-factor authentication technologies, tokens, biometrics and smart cards. Select the particular method based upon the vulnerability of the ICS network to be protected, rather than using the method that is available at the device level.

機能的なセキュリティサブネットとデバイス間の ICS サブネット間交信を制限する。ファイアウォールを採用してこうしたエリアへの接続を管理すれば、組織はより機密度の高いエリア内のシステムやリソースへの不正アクセスを防止できる。ファイアウォールは次の 3 つに大別できる。

- **パケットフィルタリングファイアウォール。**最もベーシックなタイプのファイアウォールがパケットフィルタと呼ばれる。パケットフィルタファイアウォールは、基本的にルーティングデバイスで、システムアドレスと交信セッションのアクセス制御機能を持つ。アクセス制御は、ルールセットと総称される一式の指令により制御される。最もベーシックな形態では、パケットフィルタは ISO/IEC 7498 モデル、オープンシステム連接（OSI）のレイヤー3（ネットワーク）で動作する。このタイプのファイアウォールは、パケットを転送する前に、各パケット中の IP アドレス等の基本情報を基準に照らしてチェックする。パケットと基準に応じて、ファイアウォールはパケットのドロップや転送を行うほか、メッセージを発信者に送る。このタイプのファイアウォールは、セキュリティのレベルは高いが、オーバーヘッドや遅延を生じ、ネットワークパフォーマンスに影響を与えることがある。
- **ステートフルインスペクションファイアウォール。**これは OSI モデルデータの追加注意事項をレイヤー4（トランスポート）に組み込んだパケットフィルタである。パケットをネットワークレイヤーでフィルタリングし、セッションパケットの適格性を判定し、パケット内容をトランスポートレイヤー（TCP、UDP 等）でも評価する。ステートフルインスペクションはアクティブセッションを追跡し、その情報を基にパケットの転送又はブロックを判定する。セキュリティのレベルは高くパフォーマンスも良好であるが、高価で管理者にとって複雑となる。ICS アプリケーションの付加的なルールセットが必要になることもある。
- **アプリケーション・プロキシゲートウェイファイアウォール。**このクラスのファイアウォールは、パケットをアプリケーション層で検証し、特定のアプリケーション（ブラウザー等）やプロトコル（FTP 等）といった特定アプリケーションルールに従ってトラフィックをフィルタリングする。このタイプのファイアウォールは、リモートアクセスや ICS コンポーネントが提供する設定サービスに対する攻撃の予防に極めて効果がある。セキュリティのレベルは高いが、オーバーヘッドや遅延を生じ、ネットワークパフォーマンスに影響を与えることがあるため、ICS 環境では受け入れられない場合がある。NIST SP800-41 改訂第 1 版『ファイアウォール及びファイアウォールポリシーガイドライン』[85]には、ファイアウォール及びファイアウォールポリシーを選定するための一般的ガイダンスがある。

ICS 環境では、ファイアウォールは ICS ネットワークと企業ネットワーク間に多用されている[34]。正しく設定すれば、制御システムのホストコンピュータとコントローラ間の不正アクセスを著しく制限し、セキュリティを改善する。また不要なトラフィックをネットワークから除去するため、制御ネットワークの応答感度を改善することもある。設計・設定・保守が適正であれば、専用のハードウエアファイアウォールは、今日の ICS 環境のセキュリティ向上に大きく貢献する。

ファイアウォールはいくつかツールを提供してセキュリティポリシーを施行するが、そのようなセキュリティポリシーは、現在入手可能な市販のプロセス制御デバイスに対してローカルで実現できないものであり、次のような機能を有する。

- 保護されていない LAN 上のデバイスと保護された ICS ネットワーク上のデバイス間で特に許可されたものを除き、全ての交信をブロックする。ブロックはソース及び宛先の IP アドレスペア、サービス、ポート、接続状態、ファイアウォールが許可する特定のアプリケーション又はプロトコルに従って行う。ブロックは着信パケットでも送信パケットでも生じるが、これは e メール等の高リスク通信を制限する上で役立つ。

- ICS ネットワークにアクセスしようとする全てのユーザ認証をセキュアにする。認証方法には単純なパスワード、複雑なパスワード、複合要素認証技術、トークン、生物計測学、スマートカード等があり、種々の保護レベルを柔軟に採用できる。デバイスレベルで利用できる方法を使用するのではなく、保護すべき ICS ネットワークの脆弱性を基に、特定の方法を選定する。

- Enforce destination authorization. Users can be restricted and allowed to reach only the nodes on the control network necessary for their job function. This reduces the potential of users intentionally or accidentally gaining access to and control of devices for which they are not authorized, but adds to the complexity for on-the-job-training or cross-training employees.
- Record information flow for traffic monitoring, analysis, and intrusion detection.
- Permit the ICS to implement operational policies appropriate to the ICS but that might not be appropriate in an IT network, such as prohibition of less secure communications like email, and permitted use of easy-to-remember usernames and group passwords.
- Be designed with documented and minimal (single if possible) connections that permit the ICS network to be severed from the corporate network, should that decision be made, in times of serious cyber incidents.

Other possible deployments include using either host-based firewalls or small standalone hardware firewalls in front of, or running on, individual control devices. Using firewalls on an individual device basis can create significant management overhead, especially in change management of firewall configurations, however this practice will also simplify individual configuration rulesets.
There are several issues that must be addressed when deploying firewalls in ICS environments, particularly the following:

- The possible addition of delay to control system communications.
- The lack of experience in the design of rule sets suitable for industrial applications. Firewalls used to protect control systems should be configured so they do not permit either incoming or outgoing traffic by default. The default configuration should be modified only when it is necessary to permit connections to or from trusted systems to perform authorized ICS functions.

Firewalls require ongoing support, maintenance, and backup. Rule sets need to be reviewed to make sure that they are providing adequate protection in light of ever-changing security threats. System capabilities (e.g., storage space for firewall logs) should be monitored to make sure that the firewall is performing its data collection tasks and can be depended upon in the event of a security violation. Real-time monitoring of firewalls and other security sensors is required to rapidly detect and initiate response to cyber incidents.

5.4 Logically Separated Control Network

The ICS network should, at a minimum, be logically separated from the corporate network on physically separate network devices. Based on the ICS network configuration, additional separation needs to be considered for Safety Instrumented Systems and Security Systems (e.g., physical monitoring and access controls, doors, gates, cameras, VoIP, access card readers) that are often either part of the ICS network or utilize the same communications infrastructure for remote sites. When enterprise connectivity is required:

- There should be documented and minimal (single if possible) access points between the ICS network and the corporate network. Redundant (i.e., backup) access points, if present, must be documented.
- A stateful firewall between the ICS network and corporate network should be configured to deny all traffic except that which is explicitly authorized.
- The firewall rules should at a minimum provide source and destination filtering (i.e., filter on media access control [MAC] address), in addition to TCP and User Datagram Protocol (UDP) port filtering and Internet Control Message Protocol (ICMP) type and code filtering.

- 宛先の許可。ユーザは、自分の業務に必要な制御ネットワーク上のノードにしか到達できないように制限を受ける。これによりユーザが、許可されていないデバイスに、故意又は偶然にアクセスして制御を行う可能性は減るが、OJT や交差訓練中の従業員には複雑さが増す。
- トラフィック監視、解析及び侵入検知のための情報の流れの記録。
- IT ネットワークには適合しないが、ICS には適合する業務ポリシーを ICS が実施することを許可する。例えば電子メール等のセキュリティの低い通信、覚えやすいユーザ名やグループパスワードの使用を禁止するなど。
- 深刻なサイバーインシデントの際に決定があれば、ICS ネットワークを企業ネットワークから切断できる、文書化された最低限の（できれば 1 つのみ）接続にする。

その他可能な展開としては、ホストベースのファイアウォールや、小型のスタンドアローンハードウエアファイアウォールを個々の制御デバイスの前面に又はそうしたデバイス上に配置して使用する案もある。個々のデバイスにファイアウォールを使用すると、特にファイアウォール設定の交換管理に、かなりの管理オーバーヘッドが生じるが、個々の設定ルールセットを簡素化することにもなる。
ICS 環境にファイアウォールを展開する際には、特に次のような考慮すべき問題がいくつかある。

- 制御システムの通信に遅延が加わる可能性
- 産業用途に合ったルールセットの考案における経験の欠如。制御システムの保護に使用するファイアウォールの設定は、着信トラフィックも送信トラフィックもデフォルトで許可しないようにすべきである。デフォルト設定の変更は、信頼されているシステムとの接続を許可して、許可された ICS 機能を実施する必要がある場合のみにすべきである。

ファイアウォールは、絶えずサポート・保守・バックアップを必要とする。絶えず変化する脅威という観点から、しっかり保護を確保できるように、ルールセットを見直す必要がある。システムの能力（ファイアウォールログのストレージ容量等）を監視して、ファイアウォールがデータ収集作業を続行できるようにし、セキュリティ違反事態が生じても信頼性が保たれるようにすべきである。ファイアウォールその他のセキュリティセンサは、リアルタイムで監視し、サイバーインシデントを検知して即応できるようにしなければならない。

5.4 論理的に分離された制御ネットワーク

少なくとも ICS ネットワークは、物理的に分離されたネットワークデバイス上の企業ネットワークから、論理的に分離されているべきである。ICS ネットワーク設定を基に、付加的な分離を安全計装システムとセキュリティシステム（物理的監視アクセス制御、ドア、ゲート、カメラ、VoIP、立入カードリーダー等）向けに検討する必要がある。これらシステムは、ICS ネットワークの一部をなすか、同じ通信インフラを遠隔サイト用に使用していることが多い。企業の接続が必要な場合、

- 文書化された最低限の（できれば 1 つのみ）アクセスポイントが ICS ネットワークと企業ネットワーク間にあるべきである。冗長（バックアップ）アクセスポイントがあれば、文書化しなければならない。
- ICS ネットワークと企業ネットワーク間のステートフルファイアウォールは、明示的に許可されたもの以外、一切のトラフィックを拒絶するように設定する。
- TCP 及びユーザデータグラムプロトコル（UDP）ポートフィルタリング、インターネット制御メッセージプロトコル（ICMP）タイプ・コードフィルタリングに加えて、ファイアウォールルールは少なくともソース及び宛先フィルタリング（メディアアクセス制御[MAC]アドレスでのフィルタリング）を行うべきである。

An acceptable approach to enabling communication between an ICS network and a corporate network is to implement an intermediate DMZ network. The DMZ should be connected to the firewall such that specific (restricted) communication may occur between only the corporate network and the DMZ, and the ICS network and the DMZ. The corporate network and the ICS network should not communicate directly with each other. This approach is described in Sections 5.5.4 and 5.5.5. Additional security may be obtained by implementing a Virtual Private Network (VPN) between the ICS and external networks.

5.5 Network Segregation

ICS networks and corporate networks can be segregated to enhance cybersecurity using different architectures. This section describes several possible architectures and explains the advantages and disadvantages of each. Please note that the intent of the diagrams in Section 5.5 is to show the placement of firewalls to segregate the network. Not all devices that would be typically found on the control network or corporate network are shown. Section 5.6 provides guidance on a recommended defense-in-depth architecture.

5.5.1 Dual-Homed Computer/Dual Network Interface Cards (NIC)

Dual-homed computers can pass network traffic from one network to another. A computer without proper security controls could pose additional threats. To prevent this, no systems other than firewalls should be configured as dual-homed to span both the control and corporate networks. All connections between the control network and the corporate network should be through a firewall. This configuration provides no security improvement and should not be used to bridge networks (e.g., ICS and corporate networks).

5.5.2 Firewall between Corporate Network and Control Network

By introducing a simple two-port firewall between the corporate and control networks, as shown in Figure 5-1, a significant security improvement can be achieved. Properly configured, a firewall significantly reduces the chance of a successful external attack on the control network.
Unfortunately, two issues still remain with this design. First, if the data historian resides on the corporate network, the firewall must allow the data historian to communicate with the control devices on the control network. A packet originating from a malicious or incorrectly configured host on the corporate network (appearing to be the data historian) would be forwarded to individual PLCs/DCS.

ICS ネットワークと企業ネットワーク間の交信を可能にする受け入れられるアプローチは、中間 DMZ ネットワークを実装することである。DMZ はファイアウォールに接続され、企業ネットワークと DMZ 間及び ICS ネットワークと DMZ 間でのみ特定の（制限された）交信が生じるようにする。企業ネットワークと ICS ネットワーク間では直接交信が生じないようにすべきである。このアプローチはセクション 5.5.4 及び 5.5.5 で説明する。VPN を ICS ネットワークと外部ネットワーク間に実装すれば、更にセキュリティが高まる。

5.5 ネットワークの分離

ICS ネットワークと企業ネットワークを分離し、別々のアーキテクチャを使用してサイバーセキュリティを高めることができる。このセクションでは、いくつか可能なアーキテクチャについて取り上げ、それぞれの利点・欠点を説明する。セクション 5.5 の図の意図は、ファイアウォールの配置によるネットワークの分離を示すことにある点に留意されたい。制御ネットワークや企業ネットワーク上に通常あるデバイスが、必ずしも全て示されていない。セクション 5.6 では、推奨される多層防御アーキテクチャのガイダンスを示す。

5.5.1 デュアルホームﾄﾞコンピュータ/デュアルネットワークインタフェースカード（NIC）

デュアルホームﾄﾞコンピュータは、ネットワークトラフィックをあるネットワークから別のネットワークへ通過させる。しっかりしたセキュリティ対策のないコンピュータでは、脅威が増加する。これを防ぐには、制御ネットワークでも企業ネットワークでも、ファイアウォール以外のシステムをデュアルホームﾄﾞに設定することである。制御ネットワークと企業ネットワーク間の全ての接続は、ファイアウォール経由とすべきである。この設定でセキュリティが向上することはなく、ネットワーク間のブリッジに使用すべきでない（ICS ネットワークと企業ネットワーク等）。

5.5.2 企業ネットワークと制御ネットワーク間のファイアウォール

図 5-1 のように、両ネットワーク間に単純な 2 ポートファイアウォールを設置することで、かなりセキュリティが向上する。適正に設定すればファイアウォールは、制御ネットワークに対する外部攻撃が成功する可能性を大幅に減らす。

残念ながらこの設計には 2 つの問題がある。まず、データヒストリアンが企業ネットワークに常駐している場合、ファイアウォールは、データヒストリアンが制御ネットワーク上の制御デバイスと交信するのを許可しなければならない。悪意あるホストや企業ネットワーク上の設定に不備がある（データヒストリアンのように見える）ホストからのパケットは、個々の PLCs/DCS に転送される。

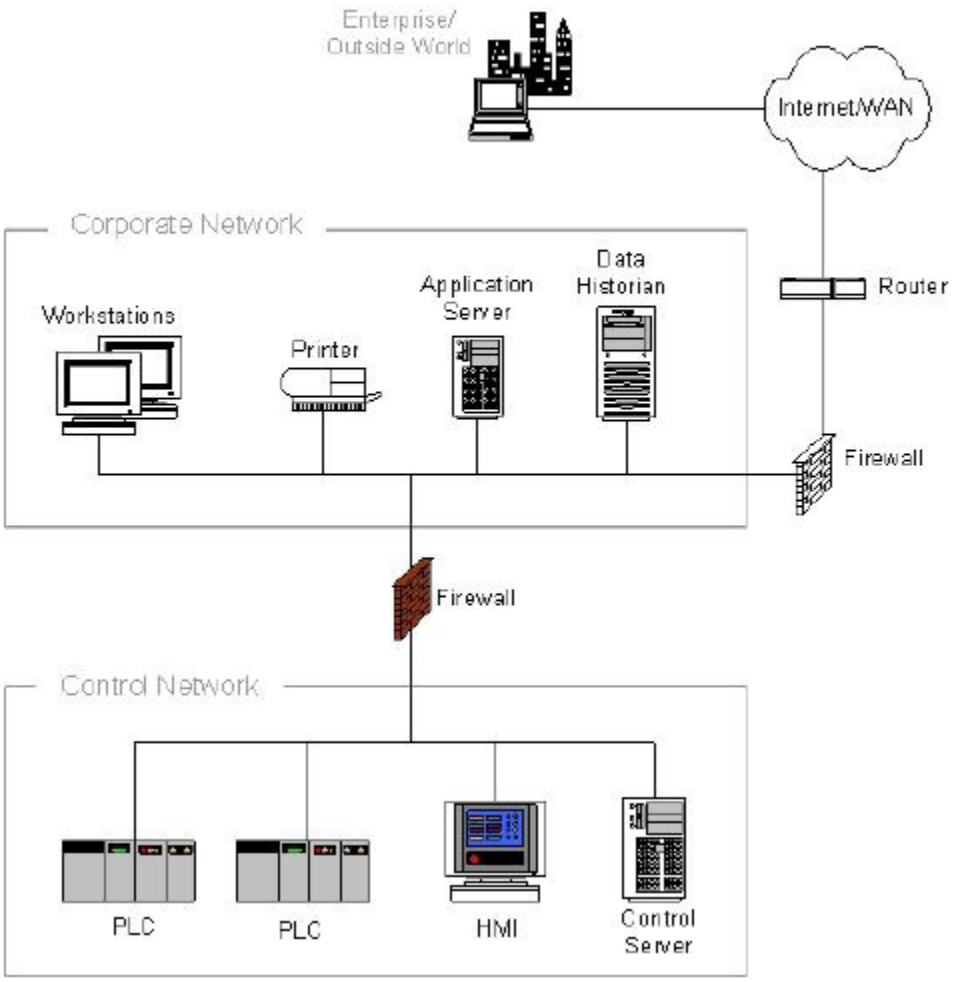

Figure 5-1. Firewall between Corporate Network and Control Network

If the data historian resides on the control network, a firewall rule must exist that allows all hosts from the enterprise to communicate with the historian. Typically, this communication occurs at the application layer as Structured Query Language (SQL) or Hypertext Transfer Protocol (HTTP) requests. Flaws in the historian's application layer code could result in a compromised historian. Once the historian is compromised, the remaining nodes on the control network are vulnerable to a worm propagating or an interactive attack.

Another issue with having a simple firewall between the networks is that spoofed packets can be constructed that can affect the control network, potentially permitting covert data to be tunneled in allowed protocols. For example, if HTTP packets are allowed through the firewall, then Trojan horse software accidentally introduced on an HMI or control network laptop could be controlled by a remote entity and send data (such as captured passwords) to that entity, disguised as legitimate traffic.

In summary, while this architecture is a significant improvement over a non-segregated network, it requires the use of firewall rules that allow direct communications between the corporate network and control network devices. This can result in possible security breaches if not very carefully designed and monitored [35].

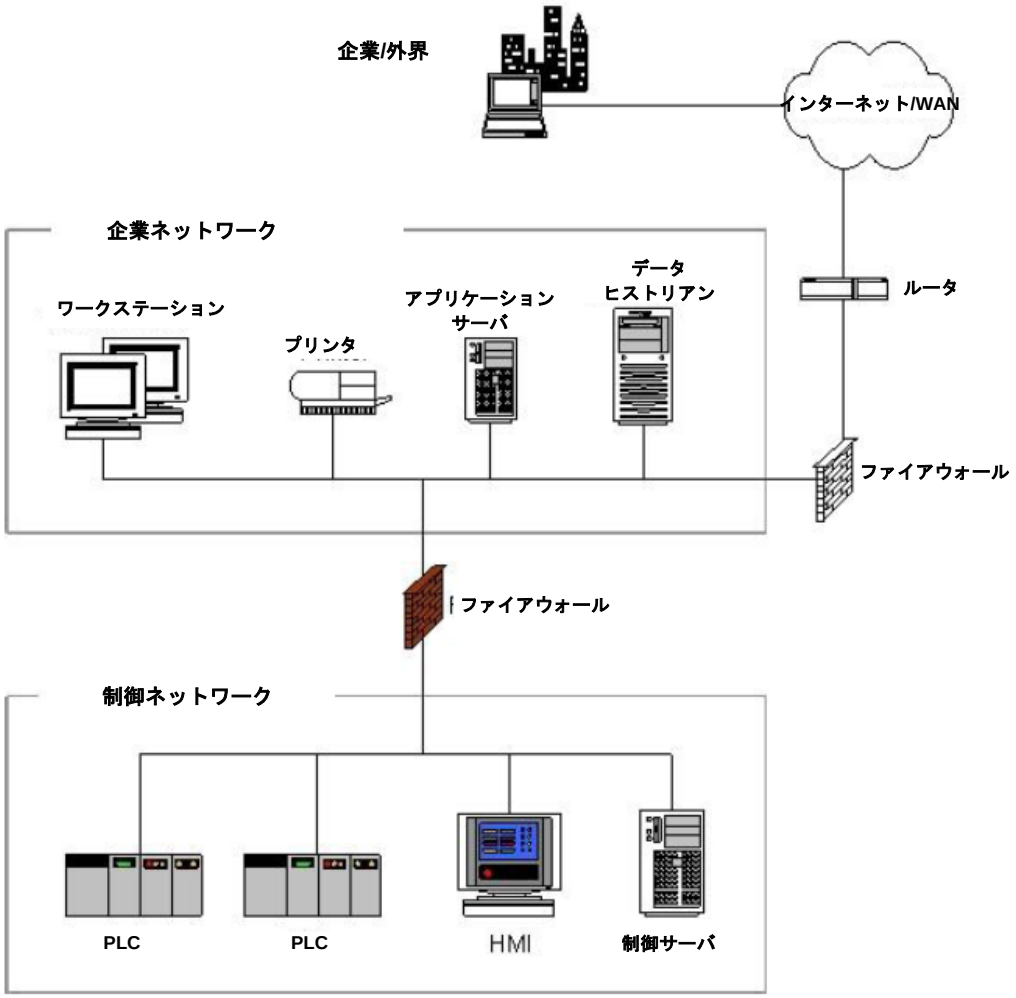

図 5-1.企業ネットワークと制御ネットワーク間のファイアウォール

データヒストリアンが制御ネットワーク上に常駐している場合、全てのホストが企業側からヒストリアンに通信できるファイアウォール規則がなければならない。一般にこの通信は、SQL 又は HTTP 要求としてアプリケーション層で生じる。ヒストリアンのアプリケーション層コードに不備があると、ヒストリアンの機能が低下する。そうなると、制御ネットワークの残りのノードがワームの伝播やインタラクティブ攻撃に対して脆弱になる。

ネットワーク間に単純ファイアウォールを設置するもう一つの問題点は、なりすましパケットが生成され、制御ネットワークに影響を及ぼし、秘密データが許可されたプロトコルでトンネルされる可能性がある。例えば HTTP パケットの通過がファイアウォールから許可されると、HMI や制御ネットワークラップトップに偶然入り込んだトロイの木馬が外部団体に遠隔操作され、正常なトラフィックを装って、データ（捕捉したパスワード等）が当該団体に送信されることになる。

まとめとして、このアーキテクチャは非分離ネットワークをかなり改善する一方で、企業ネットワークデバイスと制御ネットワークデバイス間の直接交信を許可するというファイアウォール規則を使用しなければならない。その結果、設計と監視をかなり慎重に行わないと、セキュリティ侵害が生じることになる。

5.5.3 Firewall and Router between Corporate Network and Control Network

A slightly more sophisticated design, shown in Figure 5-2, is the use of a router/firewall combination. The router sits in front of the firewall and offers basic packet filtering services, while the firewall handles the more complex issues using either stateful inspection or proxy techniques. This type of design is very popular in Internet-facing firewalls because it allows the faster router to handle the bulk of the incoming packets, especially in the case of DoS attacks, and reduces the load on the firewall. It also offers improved defense-in-depth because there are two different devices an adversary must bypass [35].

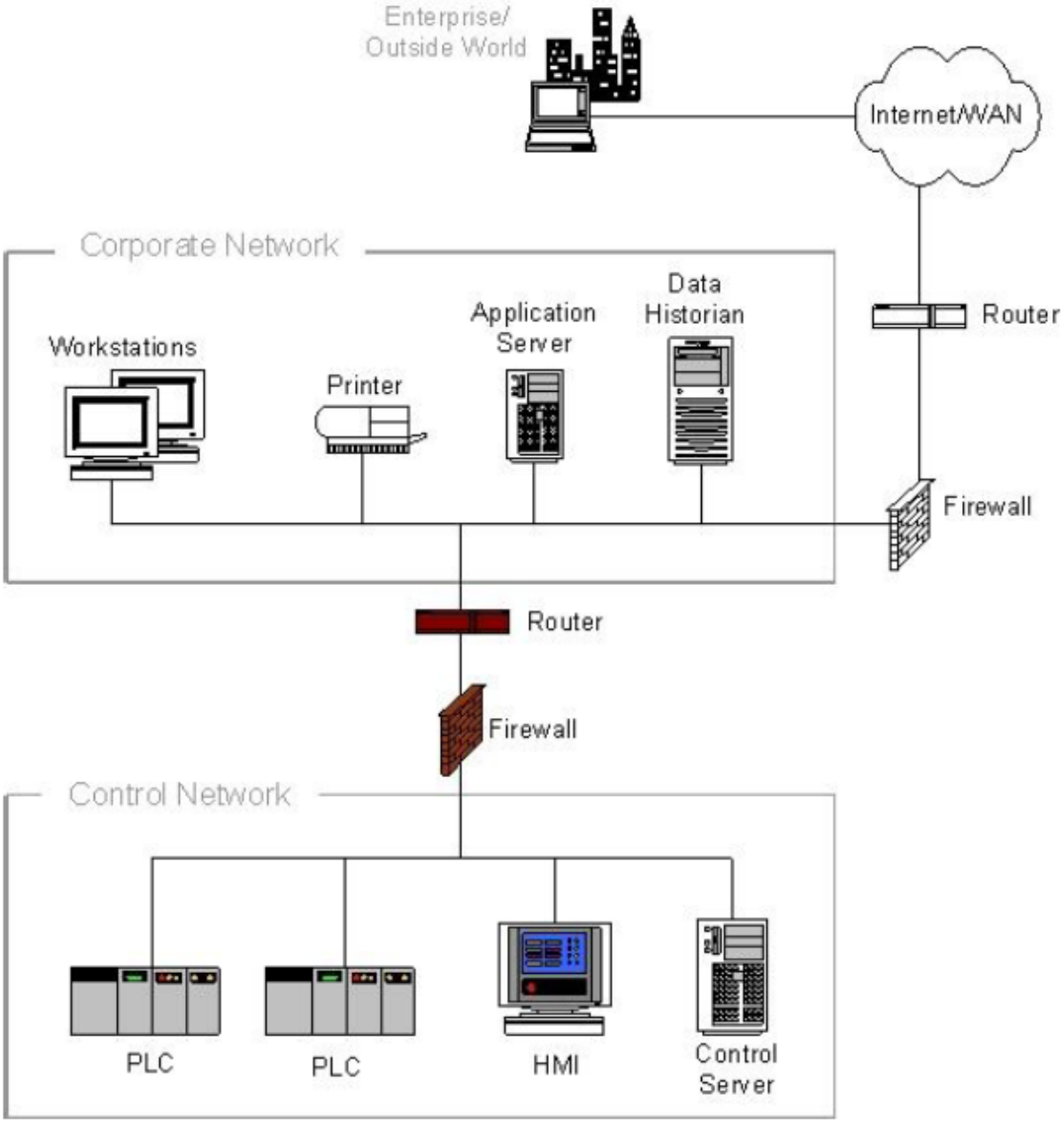

Figure 5-2. Firewall and Router between Corporate Network and Control Network

5.5.3 企業ネットワークと制御ネットワーク間のファイアウォールとルータ

図 5-2 はやや洗練された設計で、ルータとファイアウォールを併用している。ルータをファイアウォールの前面に据え、パケットの基本的フィルタリングを行わせ、ファイアウォールはステートフルインスペクション又はプロキシ技術を用いてより複雑な問題の処理に当たらせる。この種の設計はインターネットに面したファイアウォールではごく一般的であるが、より高速なルータに大量の着信パケットを処理させて、特に DoS 攻撃の場合に備え、ファイアウォールへの負荷を減らすためである。また攻撃側は 2 種のデバイスを通過しなければならないため、多層防御も改善される[35]。

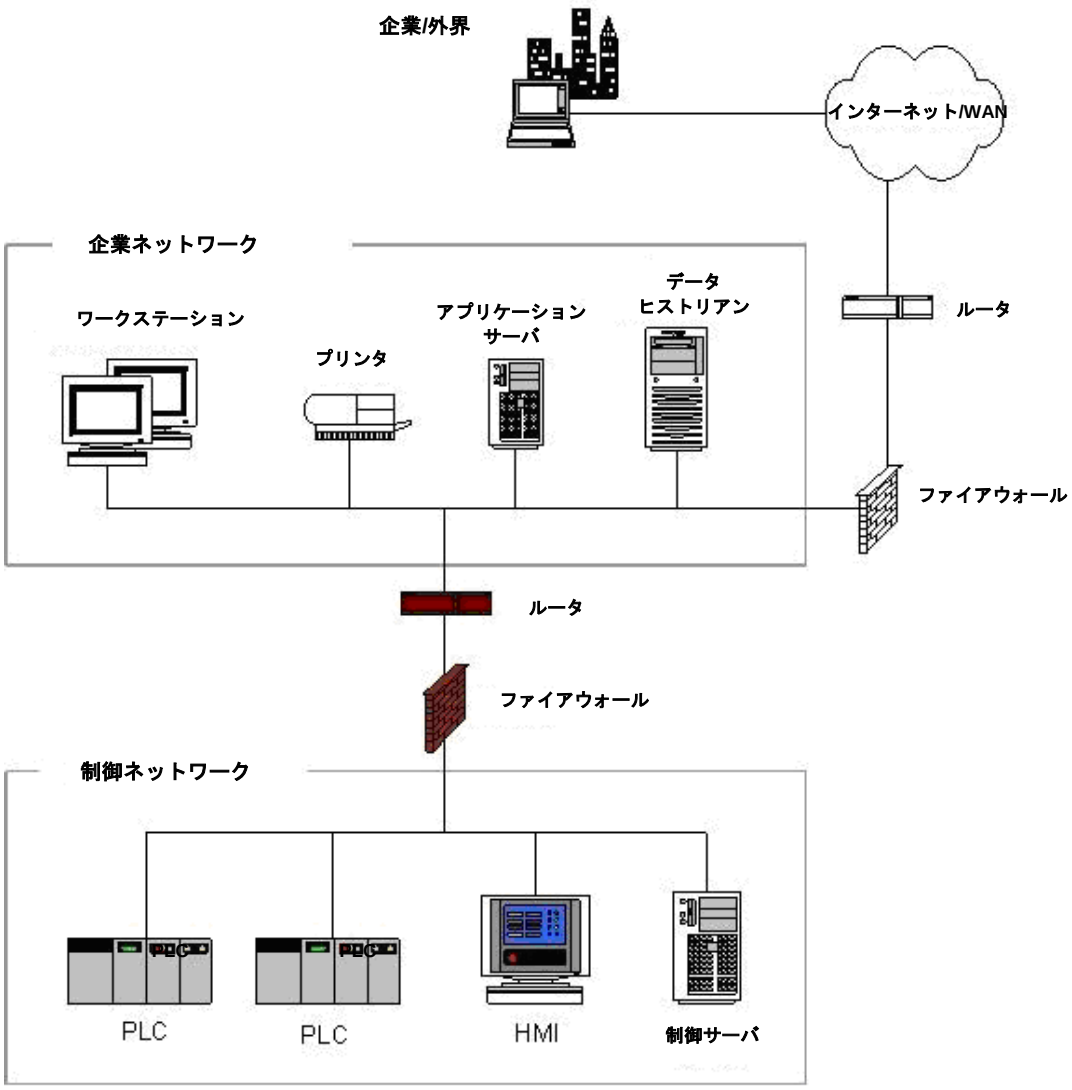

図 5-2.企業ネットワークと制御ネットワーク間のファイアウォールとルータ

5.5.4 Firewall with DMZ between Corporate Network and Control Network

A significant improvement is the use of firewalls with the ability to establish a DMZ between the corporate and control networks. Each DMZ holds one or more critical components, such as the data historian, the wireless access point, or remote and third party access systems. In effect, the use of a DMZ-capable firewall allows the creation of an intermediate network.

Creating a DMZ requires that the firewall offer three or more interfaces, rather than the typical public and private interfaces. One of the interfaces is connected to the corporate network, the second to the control network, and the remaining interfaces to the shared or insecure devices such as the data historian server or wireless access points on the DMZ network. Implementing continuous ingress and egress traffic monitoring on the DMZ is recommended. Additionally, firewall rulesets that only permit connections between the control network and DMZ that are initiated by control network devices are recommended. Figure 5-3 provides an example of this architecture.

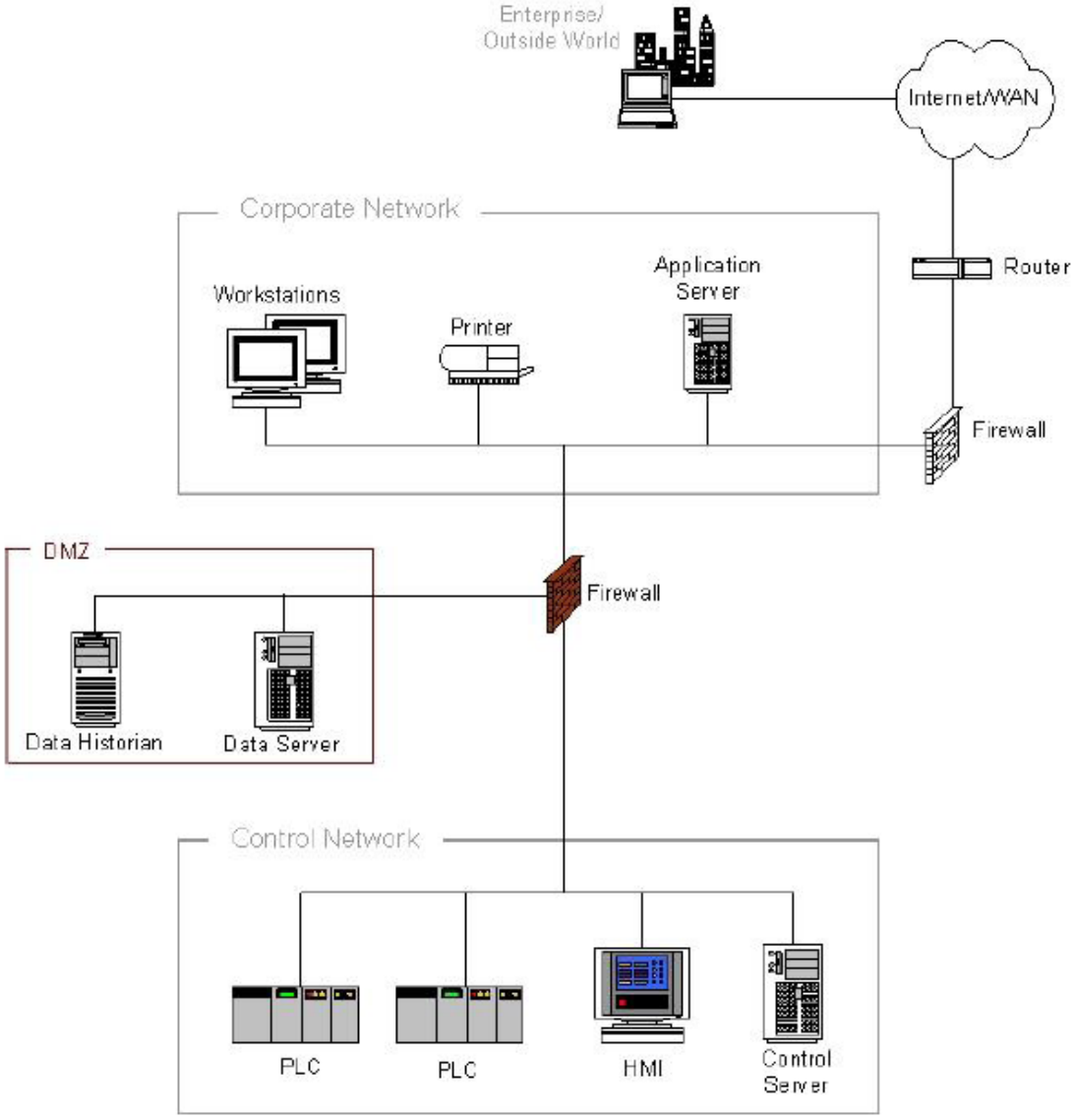

Figure 5-3. Firewall with DMZ between Corporate Network and Control Network

5.5.4 企業ネットワークと制御ネットワーク間の DMZ 付きファイアウォール

企業ネットワークと制御ネットワーク間に DMZ を設置できるファイアウォールを使用すれば、かなりの改善となる。各 DMZ はデータヒストリアン、ワイアレスアクセスポイント、リモートアクセスシステム、サードパーティアクセスシステム等、1 個又は複数の重要コンポーネントを有する。実際に DMZ 能力のあるファイアウォールを使用すれば、中間ネットワークが構築できる。

DMZ を設置するには、ファイアウォールが通常のパブリック・プライベートインタフェースではなく、3 つ以上のインタフェースを備えていることが必須となる。その 1 つは企業ネットワークに接続され、2 つ目は制御ネットワークに、それ以外のインタフェースはデータヒストリアンサーバや DMZ ネットワーク上のワイアレスアクセスポイント等、共有又はセキュリティの低いデバイスに接続される。DMZ の着信・送信トラフィックを連続的に監視できるように実装することが薦められる。またファイアウォールルールセットは、制御ネットワークデバイスが開始した、制御ネットワークと DMZ 間の接続を許可するものが推奨される。
図 5-3 にこのアーキテクチャの例を示す。

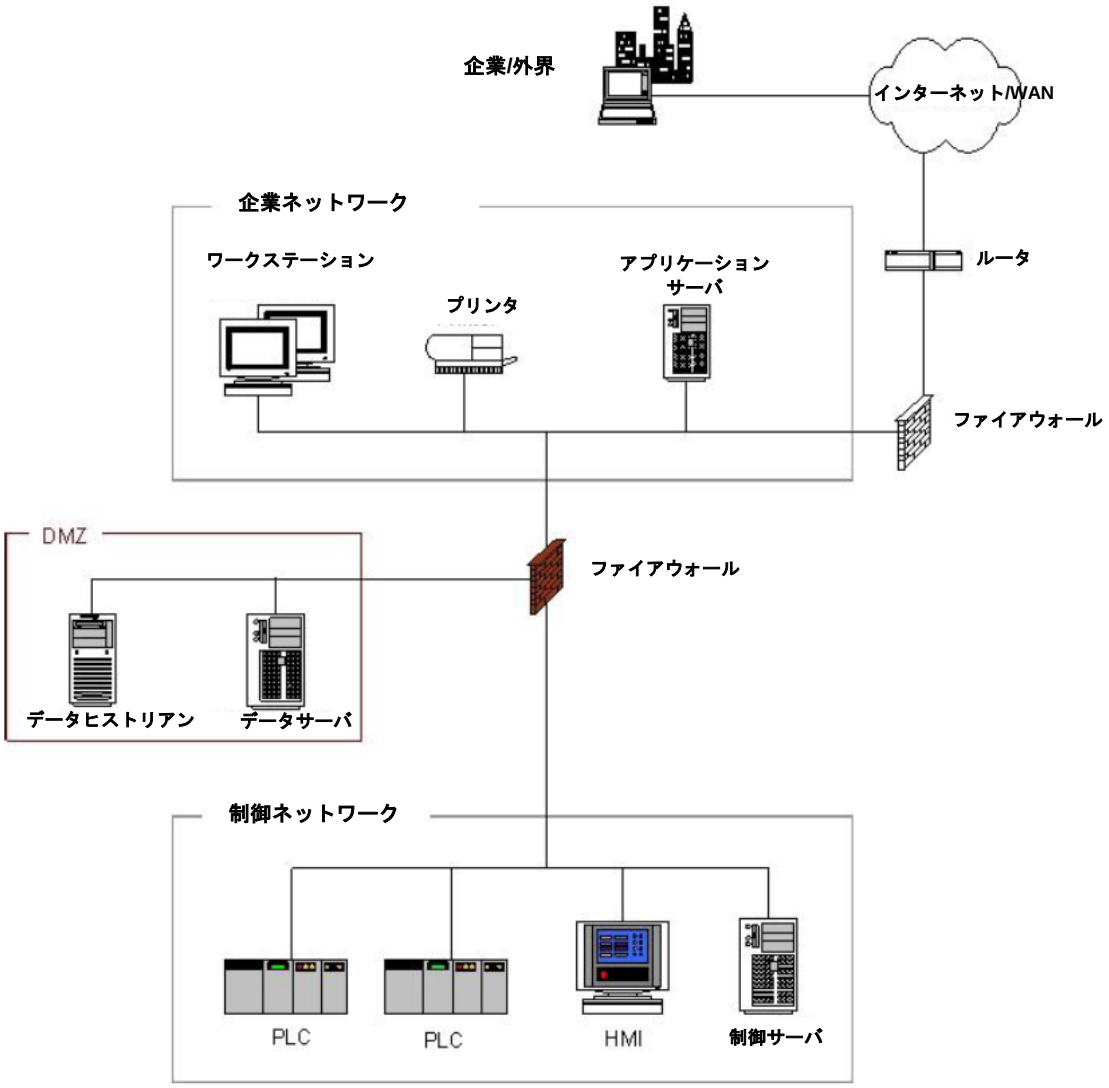

図 5-3.企業ネットワークと制御ネットワーク間の DMZ 付きファイアウォール

By placing corporate-accessible components in the DMZ, no direct communication paths are required from the corporate network to the control network; each path effectively ends in the DMZ. Most firewalls can allow for multiple DMZs, and can specify what type of traffic may be forwarded between zones. As Figure 5-3 shows, the firewall can block arbitrary packets from the corporate network from entering the control network, and can also regulate traffic from the other network zones including the control network. With well-planned rule sets, a clear separation can be maintained between the control network and other networks, with little or no traffic passing directly between the corporate and control networks.

If a patch management server, an antivirus server, or other security server is to be used for the control network, it should be located directly on the DMZ. Both functions could reside on a single server. Having patch management and antivirus management dedicated to the control network allows for controlled and secure updates that can be tailored for the unique needs of the ICS environment. It may also be helpful if the antivirus product chosen for ICS protection is not the same as the antivirus product used for the corporate network. For example, if a malware incident occurs and one antivirus product cannot detect or stop the malware, it is somewhat likely that another product may have that capability.

The primary security risk in this type of architecture is that if a computer in the DMZ is compromised, then it can be used to launch an attack against the control network via application traffic permitted from the DMZ to the control network. This risk can be greatly reduced if a concerted effort is made to harden and actively patch the servers in the DMZ and if the firewall ruleset permits only connections between the control network and DMZ that are initiated by control network devices. Other concerns with this architecture are the added complexity and the potential increased cost of firewalls with several ports. For more critical systems, however, the improved security should more than offset these disadvantages [35].

企業側からアクセス可能なコンポーネントを DMZ 内に配置することで、企業ネットワークから制御ネットワークへの直接的な通信経路は不要となり、各経路は DMZ ですっきり完結する。複数の DMZ を備えたファイアウォールも多く、ゾーン間で転送が許されるトラフィックの種類を指定できるようになっている。図 5-3 に示されるように、ファイアウォールは、企業ネットワークから来た不定のパケットが制御ネットワークに進入するのをブロックし、制御ネットワークも含めた他のネットワークゾーンから来たトラフィックの規制も行う。よく計画されたルールセットを持つことで、制御ネットワークと他のネットワーク間の明確な分離が可能になり、企業ネットワークと制御ネットワーク間にはほとんど又は全くトラフィックが往来しないようになる。

制御ネットワークにパッチ管理サーバ、アンチウイルスサーバその他のセキュリティ サーバを使用する場合、直接 DMZ に配置すべきである。いずれの機能も 1 つのサーバに常駐できる。制御ネットワーク専用のパッチ管理及びアンチウイルス管理を持てば、ICS 環境特有のニーズにフィットする制御されたセキュアな更新が可能になる。また、ICS の保護用に選定したアンチウイルス製品と企業ネットワーク用の製品が違っていれば、これも役立つ。例えば、マルウエアインシデントが起きて、あるアンチウイルス製品では検知・停止不能だったとしても、別の製品にその能力がある場合もある。

この種のアーキテクチャにおける主なセキュリティリスクは、DMZ であるコンピュータの性能が低下した場合に、それを利用して、DMZ から制御ネットワークへ許可されているアプリケーショントラフィック経由で、制御ネットワークへの攻撃を発動することである。DMZ 内のサーバの抗耐性を高め積極的にパッチを当てる取組をし、ファイアウォールのルールセットが、制御ネットワークデバイスが開始した、制御ネットワークと DMZ 間の接続だけを許可するようにすれば、このリスクは著しく減る。このアーキテクチャに関するその他の懸念材料としては、複雑さが増すことと、複数のポートを持つファイアウォールがコスト高になることである。しかし、より重要なシステムでは、セキュリティの向上はこうした欠点を補って余りある[35]。

5.5.5 Paired Firewalls between Corporate Network and Control Network

A variation on the firewall with a DMZ solution is to use a pair of firewalls positioned between the corporate and ICS networks, as shown in Figure 5-4. Common servers such as the data historian are situated between the firewalls in a DMZ-like network zone sometimes referred to as a Manufacturing Execution System (MES) layer. As in the architectures described previously, the first firewall blocks arbitrary packets from proceeding to the control network or the shared historians. The second firewall can prevent unwanted traffic from a compromised server from entering the control network, and prevent control network traffic from impacting the shared servers.

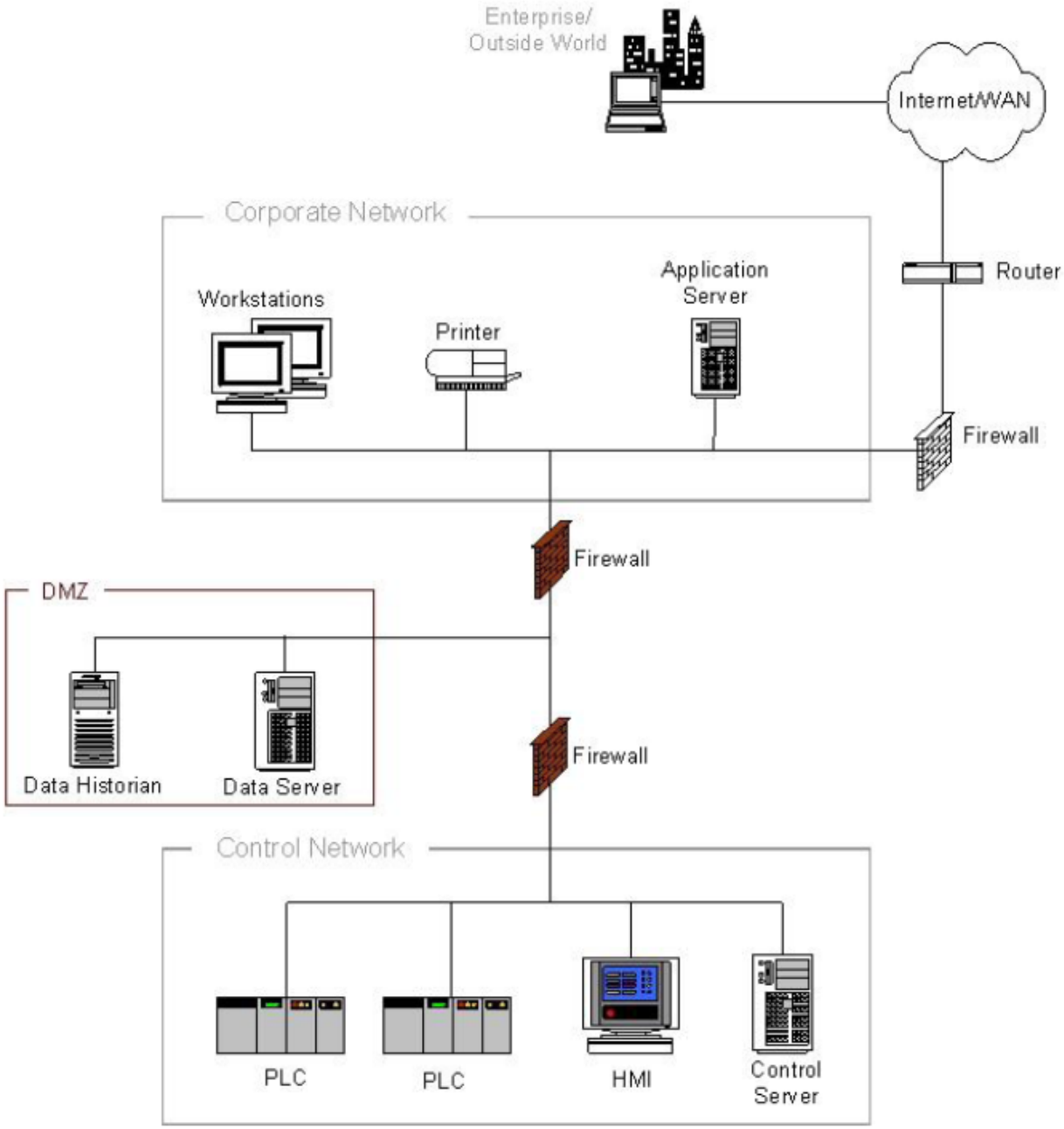

Figure 5-4. Paired Firewalls between Corporate Network and Control Network

5.5.5 企業ネットワークと制御ネットワーク間のペアードファイアウォール

DMZ 付きファイアウォールソリューションのバリエーションとして、図 5-4 に示すように、ファイアウォールをペアにして企業ネットワークと ICS ネットワーク間に配置する方法がある。データヒストリアンのような共通サーバは、生産実施システム（MES）レイヤーと呼ばれる DMZ に似たネットワークゾーン内のファイアウォールとファイアウォールの間に配置される。前述のアーキテクチャと同様、最初のファイアウォールは、不定のパケットが制御ネットワークや共有ヒストリアンへ行かないようにブロックする。2 番目のファイアウォールは、性能が低下したサーバからの不要のトラフィックが制御ネットワークへ進入しないようにし、制御ネットワークトラフィックが共有サーバに影響しないようにする。

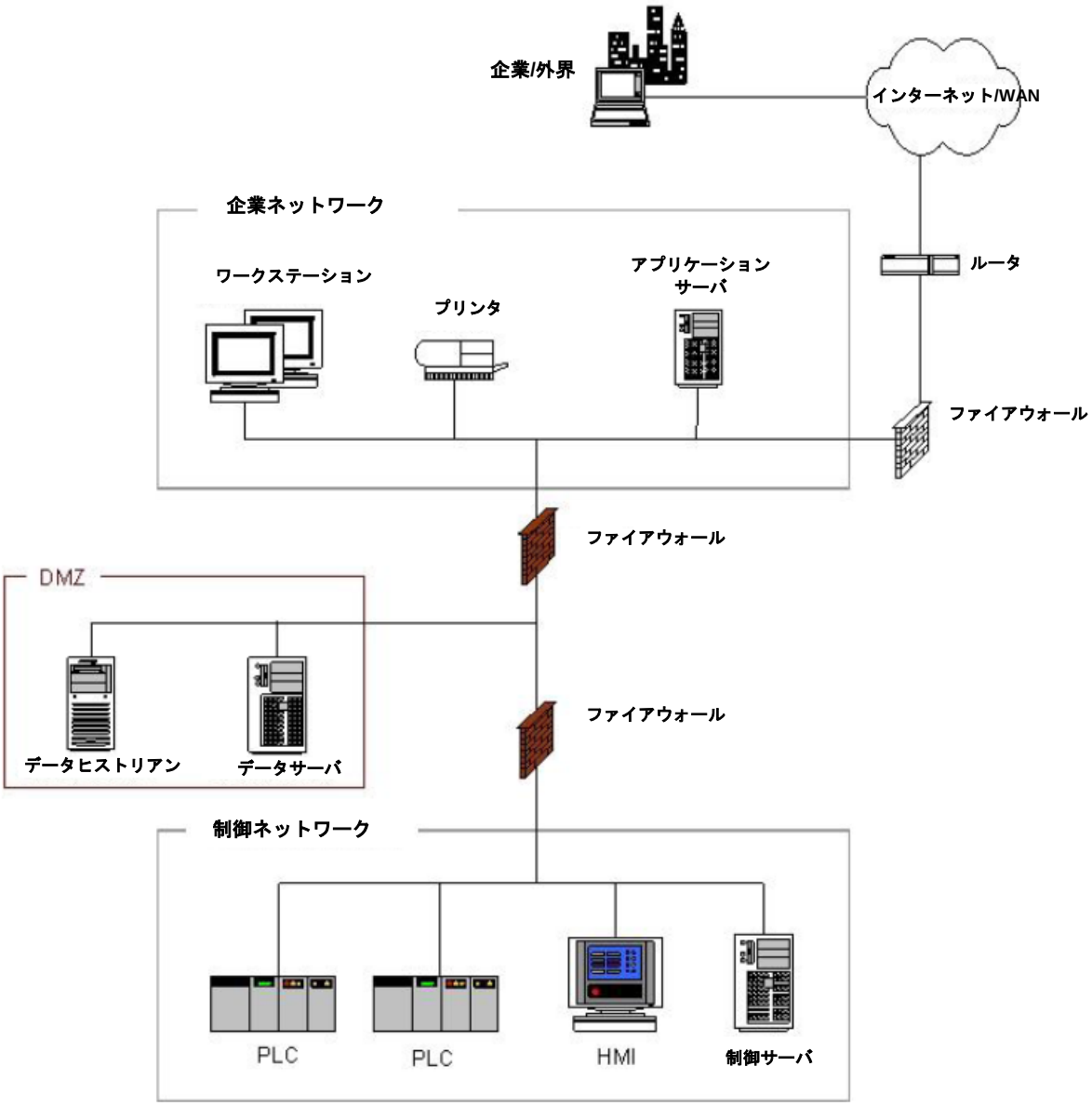

図 5-4.企業ネットワークと制御ネットワーク間のペアードファイアウォール

If firewalls from two different manufacturers are used, then this solution may offer an advantage. It also allows the control group and the IT group to have clearly separated device responsibility because each can manage a firewall on its own, if the decision is made within the organization to do so. The primary disadvantage with two-firewall architectures is the increased cost and management complexity. For environments with stringent security requirements or the need for clear management separation, this architecture has some strong advantages.

5.5.6 Network Segregation Summary

In summary, dual-homed computers generally not provide suitable isolation between control networks and corporate networks. The two-zone solutions (no DMZ) are not recommended because they provide only weak protection. If used, they should only be deployed with extreme care. The most secure, manageable, and scalable control network and corporate network segregation architectures are typically based on a system with at least three zones, incorporating one or more DMZs.

5.6 Recommended Defense-in-Depth Architecture

A single security product, technology or solution cannot adequately protect an ICS by itself. A multiple layer strategy involving two (or more) different overlapping security mechanisms, a technique also known as defense-in-depth, is desired so that the impact of a failure in any one mechanism is minimized. A defense-in-depth architecture strategy includes the use of firewalls, the creation of demilitarized zones, intrusion detection capabilities along with effective security policies, training programs, incident response mechanisms and physical security. In addition, an effective defense-in-depth strategy requires a thorough understanding of possible attack vectors on an ICS. These include:

- Backdoors and holes in network perimeter.
- Vulnerabilities in common protocols.
- Attacks on field devices.
- Database attacks.
- Communications hijacking and ‘man-in-the-middle’ attacks.
- Spoofing attacks.
- Attacks on privileged and/or shared accounts.

Figure 5-5 shows an ICS defense-in-depth architecture strategy that has been developed by the DHS Control Systems Security Program (CSSP) NCCIC/ICS-CERT Recommended Practices committee[25] as described in the *Control Systems Cyber Security: Defense in Depth Strategies* [36] document. Additional supporting documents that cover specific issues and associated mitigations are also included on the site.

The *Control Systems Cyber Security: Defense in Depth Strategies* document provides guidance and direction for developing defense-in-depth architecture strategies for organizations that use control system networks while maintaining a multi-tiered information architecture that requires:

- Maintenance of various field devices, telemetry collection, and/or industrial-level process systems.
- Access to facilities via remote data link or modem.
- Public facing services for customer or corporate operations.

[25] Information on the CSSP Recommended Practices is located at http://ics-cert.us-cert.gov/Recommended-Practices

異なる二つのメーカーのファイアウォールを併用すると、このソリューションには利点がある。また制御グループ及び IT グループのデバイス担当区分を明確にできる。理由は、組織の決定が下されれば、それぞれが自分のファイアウォールを管理できるからである。二重ファイアウォールアーキテクチャの主な欠点は、コスト高になり管理が複雑になることである。厳格なセキュリティ要件のある環境や明確な管理の分離が求められる状況では、このアーキテクチャは大きな利点がある。

5.5.6 ネットワーク分離のまとめ

まとめとして、総じて二重ホームコンピュータは、制御ネットワークと企業ネットワーク間の分離をしっかり行えるものではない。2 ゾーンソリューション（DMZ なし）は、保護に弱点があるため推奨できない。使用する場合は、細心の注意を払って展開すべきである。制御ネットワークと企業ネットワークを分離するための最もセキュアで、管理しやすいスケーラブルな分離アーキテクチャは、通常 1 つ又は複数の DMZ を持った最低 3 つのゾーンを有するシステムを基調とする。

5.6 推奨多層防御アーキテクチャ

単一のセキュリティ製品、技術又はソリューションのみで ICS をしっかり保護することは不可能である。多層防御技術としても知られている 2 つ以上の異種重畳セキュリティメカニズムを用いるマルチレイヤー戦略は、1 つのメカニズムに障害が出ても、その影響を最小に食い止められるため望ましい。多層防御アーキテクチャ戦略には、ファイアウォールの使用、非武装地帯、侵入検知機能、効果的なセキュリティポリシー、訓練計画、インシデント対応メカニズム及び物理的セキュリティの構築が含まれる。加えて、効果的な多層防御戦略を講じるには、ICS に対して攻撃可能なベクターを十分に理解することが求められる。これには以下が含まれる。

- ネットワーク周辺のバックドア及びホール
- 共通プロトコルの脆弱性
- フィールドデバイスに対する攻撃
- データベースに対する攻撃
- 通信ハイジャック及び「人が介在する」攻撃
- なりすまし攻撃
- 権限アカウント又は共通アカウントに対する攻撃

図 5-5 は、『制御システムのサイバーセキュリティ：多層防御戦略』[36]に記述されている DHS 制御システムセキュリティプログラム（CSSP) /ICS-CERT 推奨規範委員会 [26]により開発された、ICS の多層防御アーキテクチャ戦略を示す。具体的な問題点や関連緩和策に関する付加的な根拠文書もサイトにある。

『制御システムのサイバーセキュリティ：多層防御戦略』には、制御システムネットワークを使用し、以下を必要とする多段階情報アーキテクチャを維持している組織向けに、多層防御アーキテクチャ戦略を策定するための指針と指示が記載されている。

- 種々のフィールドデバイス、テレメトリ収集又は産業レベルプロセスシステムの保守
- 遠隔データリンクやモデム経由による施設へのアクセス
- 顧客・企業業務用公共サービス

[26] CSSP 推奨規範に関する情報は次の URL から入手できる。http://ics-cert.us-cert.gov/Recommended-Practices

This strategy includes firewalls, the use of demilitarized zones and intrusion detection capabilities throughout the ICS architecture. The use of several demilitarized zones in Figure 5-5 provides the added capability to separate functionalities and access privileges and has proved to be very effective in protecting large architectures comprised of networks with different operational mandates. Intrusion detection deployments apply different rule-sets and signatures unique to each domain being monitored.

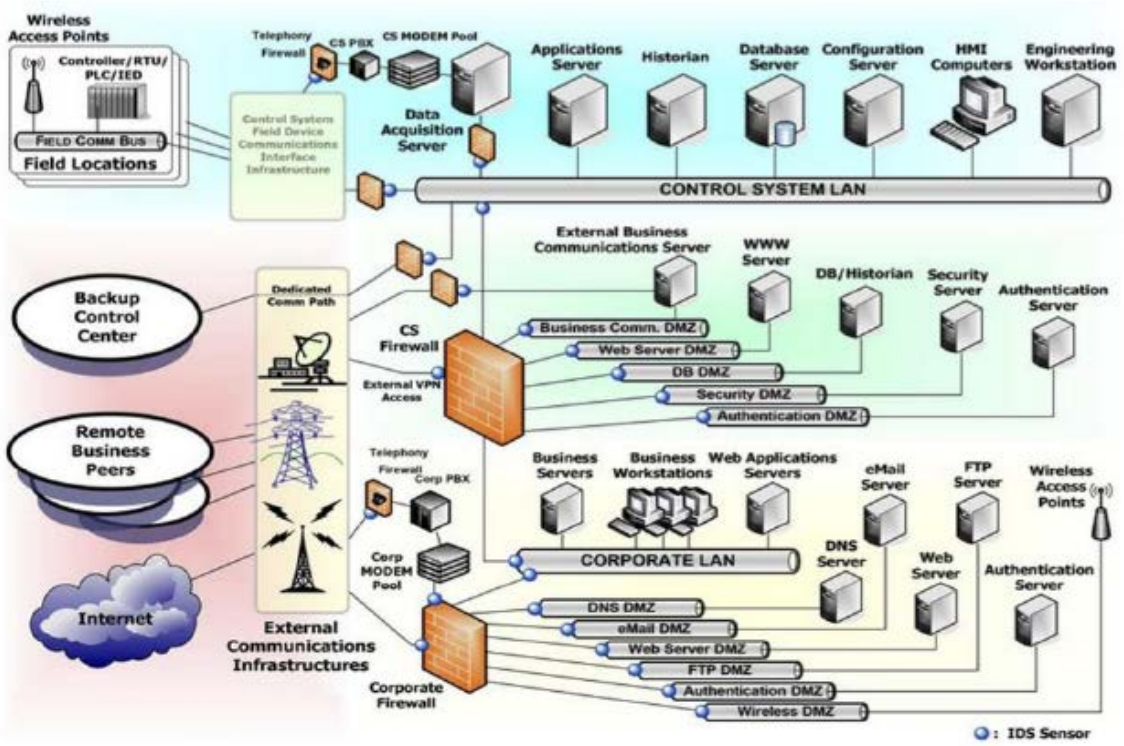

Figure 5-5. CSSP Recommended Defense-In-Depth Architecture

5.7 General Firewall Policies for ICS

Once the defense-in-depth architecture is in place, the work of determining exactly what traffic should be allowed through the firewalls begins. Configuring the firewalls to deny all except for the traffic absolutely required for business needs is every organization's basic premise, but the reality is much more difficult. Exactly what does "absolutely required for business" mean and what are the security impacts of allowing that traffic through? For example, many organizations considered allowing SQL traffic through the firewall as required for business for many data historian servers. Unfortunately, the SQL vulnerability was also the target for the Slammer worm [Table C-8. Example Adversarial Incidents]. Many important protocols used in the industrial world, such as HTTP, FTP, OPC/DCOM, EtherNet/IP, and Modbus/TCP, have significant security vulnerabilities.

The remaining material in this section summarizes some of the key points from the Centre for the Protection of National Infrastructure's (CPNI) *Firewall Deployment for SCADA and Process Control Networks: Good Practice Guide* [35].

When installing a single two-port firewall without a DMZ for shared servers (i.e., the architecture described in Section 5.5.2), particular care needs to be taken with the rule design. At a minimum, all rules

この戦略には、ICS アーキテクチャ全体を通して、ファイアウォール、非武装地帯及び侵入検知機能の使用が含まれる。図 5-5 の複数非武装地帯の使用は、機能とアクセス権限を分けるための付加的な対策で、種々の業務を担う複数ネットワークからなる大規模アーキテクチャの保護に非常に効果のあることが分かっている。侵入検知の展開は、別々のルールセットと監視する領域ごとに一意の署名を適用する。

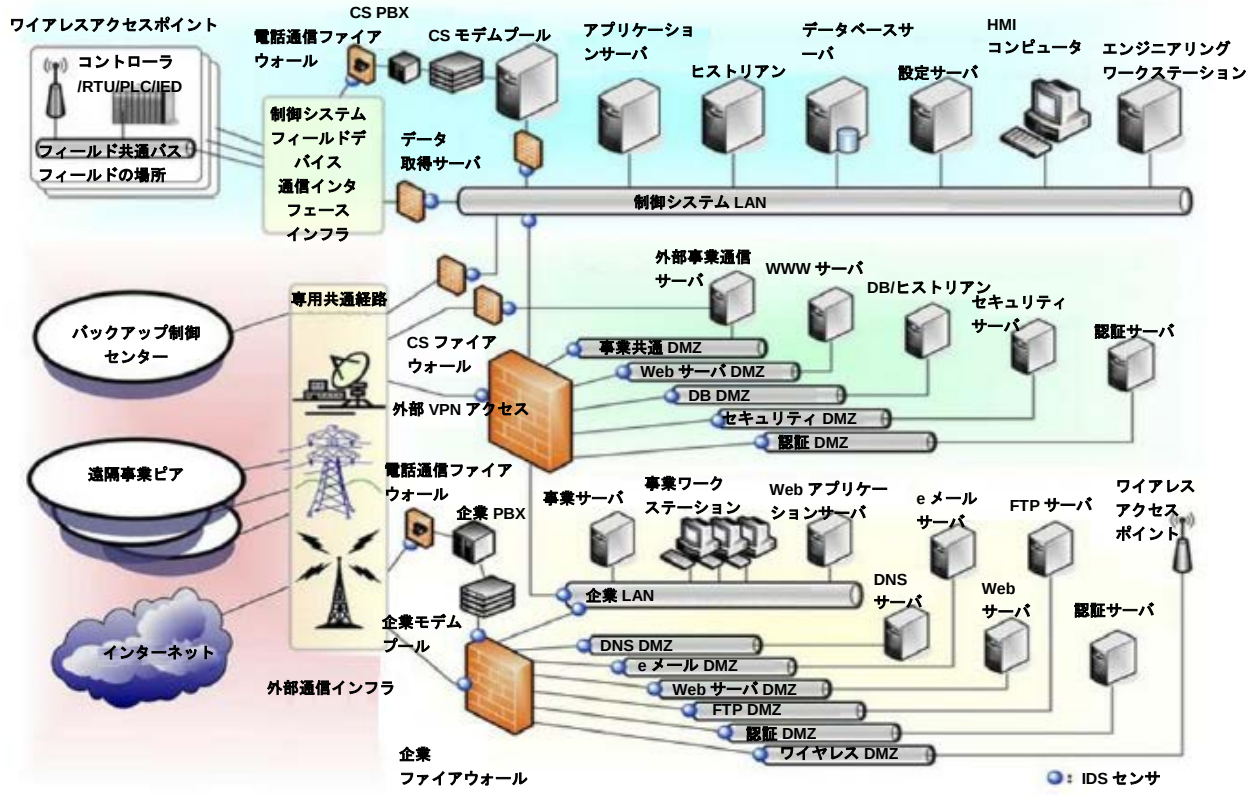

図 5-5.CSSP の推奨多層防御アーキテクチャ

5.7　ICS の全般的ファイアウォールポリシー

多層防御アーキテクチャを施行したなら、次にファイアウォールで許可するトラフィックを明確に決める作業が始まる。事業に絶対必要なトラフィック以外は全て拒絶するようにファイアウォールを設定することは、どの企業でも基本であるが、現実ははるかに難しい。
「事業に絶対必要」とは何を意味するのか、そのトラフィックを通過させるとどんなセキュリティ上の影響が出るのか。例えば、多くの組織では、事業上多数のデータヒストリアンサーバに必要なことから、SQL トラフィックのファイアウォール通過を検討した。残念ながら、SQL の脆弱性もスラマーワームの標的だった[表 C-8.攻撃インシデントの例]。HTTP、FTP、OPC/DCOM、EtherNet/IP、Modbus/TCP 等、産業界で使用されている重要プロトコルの多くには、大きなセキュリティ上の脆弱性がある。

このセクションの残りの部分では、国家インフラ保護センター（CPNI）の『SCADA 及びプロセス制御ネットワーク用ファイアウォール展開：適正規範ガイド』[35]から重要ポイントをいくつか要約する。

共有サーバ（セクション 5.5.2 のアーキテクチャ等）用に DMZ なしの単一 2 ポートファイアウォールを設置する場合、ルールの検討には特に注意を要する。少なくともどのルールも

should be stateful rules that are both IP address and port (application) specific. The address portion of the rules should restrict incoming traffic to a very small set of shared devices (e.g., the data historian) on the control network from a controlled set of addresses on the corporate network. Allowing any IP addresses on the corporate network to access servers inside the control network is not recommended. In addition, the allowed ports should be carefully restricted to relatively secure protocols such as Hypertext Transfer Protocol Secure (HTTPS). Allowing HTTP, FTP, or other unsecured protocols to cross the firewall is a security risk due to the potential for traffic sniffing and modification. Rules should be added to deny hosts outside the control network from initiating connections with hosts on the control network. Rules should only allow devices internal to the control network the ability to establish connections outside the control network.

On the other hand, if the DMZ architecture is being used, then it is possible to configure the system so that no traffic will go directly between the corporate network and the control network. With a few special exceptions (noted below), all traffic from either side can terminate at the servers in the DMZ. This allows more flexibility in the protocols allowed through the firewall. For example, Modbus/TCP might be used to communicate from the PLCs to the data historian, while HTTP might be used for communication between the historian and enterprise clients. Both protocols are inherently insecure, yet in this case they can be used safely because neither actually crosses between the two networks. An extension to this concept is the idea of using “disjoint” protocols in all control network to corporate network communications. That is, if a protocol is allowed between the control network and DMZ, then it is explicitly **not** allowed between the DMZ and corporate network. This design greatly reduces the chance of a worm such as Slammer actually making its way into the control network, because the worm would have to use two different exploits over two different protocols.

One area of considerable variation in practice is the control of outbound traffic from the control network, which could represent a significant risk if unmanaged. One example is Trojan horse software that uses HTTP tunneling to exploit poorly defined outbound rules. Thus, it is important that outbound rules be as stringent as inbound rules.

Example outbound rules include:

- Outbound traffic through the control network firewall should be limited to essential communications only and should be limited to authorized traffic originating from DMZ servers.
- All outbound traffic from the control network to the corporate network should be source and destination-restricted by service and port.

In addition to these rules, the firewall should be configured with outbound filtering to stop forged IP packets from leaving the control network or the DMZ. In practice this is achieved by checking the source IP addresses of outgoing packets against the firewall’s respective network interface address. The intent is to prevent the control network from being the source of spoofed (i.e., forged) communications, which are often used in DoS attacks. Thus, the firewalls should be configured to forward IP packets only if those packets have a correct source IP address for the control network or DMZ networks. Finally, Internet access by devices on the control network should be strongly discouraged.

IP アドレスとポート（アプリケーション）に固有のステートフルルールにすべきである。ルールのアドレス部位は、企業ネットワークの管理されたアドレスセットから来たトラフィックを、制御ネットワーク上のごく小セットの共有デバイス（データヒストリアン等）に限定する。企業ネットワーク上の IP アドレスが制御ネットワーク内のサーバにアクセスできるようにするのは薦められない。また、許可したポートは用心のため、HTTPS 等の比較的セキュアなプロトコルに限定すべきである。HTTP、FTP その他セキュアでないプロトコルがファイアウォールを越えるのは、トラフィックのスニッフィングや変更のおそれがあるため、セキュリティリスクとなる。制御ネットワーク外のホストが制御ネットワーク上のホストに接続できないようにルールを追加すべきである。制御ネットワーク内のデバイスだけが制御ネットワークの外に接続できるルールにすべきである。

反対に、DMZ アーキテクチャを使用している場合は、トラフィックが企業ネットワークと制御ネットワーク間で直接往来しないようにシステム設定することができる。特別な場合を除いて（下記参照）、いずれの側からのトラフィックも DMZ 内のサーバで終了することはできない。これによりファイアウォールを通過可能なプロトコルの柔軟性が向上する。例えば、PLCs からデータヒストリアンへの通信に Modbus/TCP を使用し、HTTP はヒストリアンと企業クライアント間の通信に使用できる。どちらのプロトコルも本来セキュアではないが、この場合は 2 つのネットワークを越えることがないため、安全に使用できる。この概念を敷衍したものが「別種」プロトコルを全ての制御ネットワークと企業ネットワーク通信に使用するという考え方である。つまり、あるプロトコルを制御ネットワークと DMZ 間で許可するが、DMZ と企業ネットワーク間では明示的に許可**しない**というものである。この設計はスラマーのようなワームが制御ネットワークに侵入する機会を著しく減じるが、それはこのワームが 2 種類のプロトコルを利用しなければならないからである。

かなりのバリエーションがあるのが制御ネットワークからの送信トラフィックの制御で、管理が行き届かないと大きなリスクとなる。その一例がトロイの木馬で、HTTP トンネリングを使い、定義に不備がある送信ルールを欺く。したがって、送信ルールは着信ルール同様に厳格でなければならない。

以下は送信ルールの例である。

- 制御ネットワークファイアウォールを越える送信トラフィックは、不可欠な送信のみに限定し、また DMZ サーバからの許可されたトラフィックのみに限定すべきである。
- 制御ネットワークから企業ネックワークへの全ての送信トラフィックは、サービスとポートによりソース及び宛先制限を設けるべきである。

これらのルールに加えて、ファイアウォールの設定は送信フィルタをかけて、偽の IP パケットが制御ネットワークや DMZ から外に出ないようにすべきである。実際には、送信パケットのソース IP アドレスを、ファイアウォールの各ネットワークインタフェースアドレスに照らしてチェックすることでこれを行っている。目的は、制御ネットワークが欺瞞（擬似）通信のソースにならないようにすることである。これは DoS 攻撃で多用される。このようにファイアウォールは、制御ネットワークや DMZ ネットワークの IP アドレスが正しい場合にのみ、IP パケットを転送するように設定すべきである。最後に、制御ネットワーク上のデバイスによるインターネットアクセスは、是非ともやめるべきである。

In summary, the following should be considered as recommended practice for general firewall rule sets:

- The base rule set should be deny all, permit none.
- Ports and services between the control network environment and the corporate network should be enabled and permissions granted on a specific case-by-case basis. There should be a documented business justification with risk analysis and a responsible person for each permitted incoming or outgoing data flow.
- All "permit" rules should be both IP address and TCP/UDP port specific, and stateful if appropriate.
- All rules should restrict traffic to a specific IP address or range of addresses.
- Traffic should be prevented from transiting directly from the control network to the corporate network. All traffic should terminate in the DMZ.
- Any protocol allowed between the control network and DMZ should explicitly NOT be allowed between the DMZ and corporate networks (and vice-versa).
- All outbound traffic from the control network to the corporate network should be source and destination-restricted by service and port.
- Outbound packets from the control network or DMZ should be allowed only if those packets have a correct source IP address that is assigned to the control network or DMZ devices.
- Control network devices should not be allowed to access the Internet.
- Control networks should not be directly connected to the Internet, even if protected via a firewall.
- All firewall management traffic should be carried on either a separate, secured management network (e.g., out of band) or over an encrypted network with multi-factor authentication. Traffic should also be restricted by IP address to specific management stations.
- All firewall policies should be tested periodically.
- All firewalls should be backed up immediately prior to commissioning.

These should be considered only as guidelines. A careful assessment of each control environment is required before implementing any firewall rule sets.

5.8 Recommended Firewall Rules for Specific Services

Beside the general rules described above, it is difficult to outline all-purpose rules for specific protocols. The needs and recommended practices vary significantly between industries for any given protocol and should be analyzed on an organization-by-organization basis. The Industrial Automation Open Networking Association (IAONA) offers a template for conducting such an analysis [37], assessing each of the protocols commonly found in industrial environments in terms of function, security risk, worst case impact, and suggested measures. Some of the key points from the IAONA document are summarized in this section. The reader is advised to consult this document directly when developing rule sets.

まとめとして、全般的なファイアウォールのルールセット用推奨規範として、次の点を考慮すべきである。

- ルールセットの基本は全て拒絶、何も許可しないである。
- 制御ネットワーク環境と企業ネットワーク間のポート及びサービスを使用可能にし、許可はケースバイケースで与えるべきである。これらを事業理由書として文書化し、リスク分析及び許可した着信・送信データフローの責任者とともに記録する。
- 全て「許可」ルールは、IP アドレス及び TCP/UDP ポート固有にし、必要ならステートフルとする。
- 全てのルールは、トラフィックを特定の IP アドレス又はアドレス範囲に限定すべきである。
- トラフィックは、制御ネットワークから企業ネットワークへ直接送信されないようにすべきである。全てのトラフィックは DMZ で終了すべきである。
- 制御ネットワークと DMZ 間で許可されたプロトコルは、DMZ と企業ネットワーク間（その逆方向も）では明示的に許可**しない**ようにすべきである。
- 制御ネットワークから企業ネックワークへの全ての送信トラフィックは、サービスとポートによりソース及び宛先制限を設けるべきである。
- 制御ネットワーク又は DMZ からの送信パケットは、制御ネットワーク又は DMZ デバイスに割り当てられたソース IP アドレスが正しい場合にのみ許可すべきである。
- 制御ネットワークデバイスのインターネットアクセスは許可すべきでない。
- 制御ネットワークは、ファイアウォールで保護されていても、直接インターネットに接続すべきでない。
- 全てのファイアウォール管理トラフィックは、別個の、セキュア管理ネットワーク（バンド外等）又は多要素認証を備えた暗号化ネットワークへ続くべきである。またトラフィックは、IP アドレスにより特定の管理ステーションに限定すべきである。
- 全てのファイアウォールポリシーは、定期的に検証すべきである。
- 全てのファイアウォールは、試運転を行う直前にバックアップすべきである。

以上はあくまでも指針として検討すべきものである。ファイアウォールルールセットを実施する前に、各制御環境を慎重に評価する必要がある。

5.8 特定サービスの推奨ファイアウォールルール

上記の全般ルールに加えて、特定のプロトコル用に汎用的なルールを決めるのは難しい。特定のプロトコルに関するニーズと推奨規範は、業界によってまちまちで、組織ごとに分析すべきである。産業オートメーションオープンネットワーキング協会（IAONA）は、このような分析を行うためのひな形を提供しており[37]、産業環境で使用する一般的なプロトコルを機能、セキュリティリスク、最悪事態の影響及び対策の観点から個別に評価している。IAONA 文書の重要点のいくつかを要約したものをこのセクションで取り上げる。読者は、ルールセットを策定する際に直接この文書を調べるよう推奨する。

5.8.1 Domain Name System (DNS)

Domain Name System (DNS) is primarily used to translate between domain names and IP addresses. For example, a DNS could map a domain name such as *control.com* to an IP address such as *192.168.1.1*. Most Internet services rely heavily on DNS, but its use on the control network is relatively rare at this time. In most cases there is little reason to allow DNS requests out of the control network to the corporate network and no reason to allow DNS requests into the control network. DNS requests from the control network to DMZ should be addressed on a case-by-case basis. Local DNS or the use of host files is recommended.

5.8.2 Hypertext Transfer Protocol (HTTP)

HTTP is the protocol underlying Web browsing services on the Internet. Like DNS, it is critical to most Internet services. It is seeing increasing use on the plant floor as well as an all-purpose query tool. Unfortunately, it has little inherent security, and many HTTP applications have vulnerabilities that can be exploited. HTTP can be a transport mechanism for many manually performed attacks and automated worms.
In general, HTTP should not be allowed to cross from the public/corporate to the control network.
If web-based technologies are absolutely required, the following best practices should be applied:

- Control access to web-based services on the physical or network layer using white-listing;
- Apply access control to both source and destination;
- Implement authorization to access the service on the application layer (instead of physical or network-layer checks);
- Implement service using only the necessary technologies (e.g., scripts are used only if they are required);
- Check service according to known application security practices;
- Log all attempts of service usage ; and
- Use HTTPS rather than HTTP, and only for specific authorized devices.

5.8.3 FTP and Trivial File Transfer Protocol (TFTP)

FTP and Trivial File Transfer Protocol (TFTP) are used for transferring files between devices. They are implemented on almost every platform including many SCADA systems, DCS, PLCs, and RTUs, because they are very well known and use minimum processing power. Unfortunately, neither protocol was created with security in mind; for FTP, the login password is not encrypted, and for TFTP, no login is required at all. Furthermore, some FTP implementations have a history of buffer overflow vulnerabilities. As a result, all TFTP communications should be blocked, while FTP communications should be allowed for outbound sessions only or if secured with additional token-based multi-factor authentication and an encrypted tunnel. More secure protocols, such as Secure FTP (SFTP) or Secure Copy (SCP), should be employed whenever possible.

5.8.4 Telnet

The telnet protocol defines an interactive, text-based communications session between a client and a host. It is used mainly for remote login and simple control services to systems with limited resources or to systems with limited needs for security. It is a severe security risk because all telnet traffic, including passwords, is unencrypted, and it can allow a remote individual considerable control over a device. It is recommended to use the Secure Shell (SSH) protocol [5.8.6] for remote administration. Inbound telnet

5.8.1 領域名システム（DNS）

領域名システム（DNS）は、主として領域名と IP アドレス間の翻訳に使用する。例えば、DNS は *control.com* という領域名を *192.168.1.1* という IP アドレスとしてマップする。
大抵のインターネットサービスは DNS に大きく依存しているが、制御ネットワークでの使用は今のところ比較的少ない。ほとんどの場合、制御ネットワークから企業ネットワークへの DNS 要求を許可する理由はなく、制御ネットワークへの DNS 要求を許可する理由もない。制御ネットワークから DMZ への DNS 要求は、ケースバイケースで扱うべきである。ローカル DNS やホストファイルの使用が推奨される。

5.8.2 ハイパーテキスト転送プロトコル（HTTP）

HTTP はインターネット上の Web 閲覧サービスプロトコルである。DNS と同様、ほとんどのインターネットサービスにとって重要である。プラントの現場や汎用クエリツールでの使用が増えている。
残念ながらセキュリティがしっかりしておらず、HTTP アプリケーションの多くには悪用される脆弱性がある。HTTP は、手動攻撃や自動ワームの多くで送信メカニズムになる。

総じて HTTP は、公開/企業ネットワークから制御ネットワークへ入れるべきでない。ウェブベース技術がどうしても必要となる場合、次のような最良規範を適用すべきである。

- ホワイトリストを使用する物理的又はネットワークレイヤー上のウェブベースサービスへの制御アクセス
- ソース及び宛先の双方にアクセス制御を適用
- アプリケーション層のサービスへのアクセスを許可（物理的又はネットワークレイヤーチェックでなく）
- 必須技術のみを使用してサービスを実装（スクリプトは必要な場合のみ使用）
- 既知のアプリケーションセキュリティ規範に従ってサービスをチェック
- サービスを利用しようとする試みを全て記録
- HTTP の代わりに HTTPS を使用し、許可された特定デバイスのみとする

5.8.3 FTP 及びトリビアルファイル転送プロトコル（TFTP）

FTP と TFTP はデバイス間でのファイルのやり取りに使われる。知名度が高く、処理パワーが最小で済むため、SCADA システム、DCS、PLCs、RTUs 等ほとんど全てのプラットホームに実装されている。残念ながら、どれもセキュリティを考えて作られてはいない。FTP のログインパスワードは暗号化されておらず、TFTP ではログインの必要さえない。更に実装された FTP によっては、バッファがオーバーフローするという脆弱性もあった。その結果、TFTP 通信は全てブロックすべきで、FTP 通信については送信セッションのみ、又は付加的なトークンベースの多要素認証及び暗号化トンネルでセキュリティを確保したもののみ許可すべきである。可能であれば常に、セキュア FTP（SFTP）やセキュアコピーといったよりセキュリティの高いプロトコルを採用すべきである。

5.8.4 テルネット（Telnet）

テルネットプロトコルは、クライアントとホスト間のインタラクティブなテキストベースの通信セッションを定義する。主にリソースの限られたシステムやセキュリティ需要の低いシステムへの遠隔ログイン及び単純な管理サービス用に使用される。全てのテルネットトラフィックはパスワードも含めて暗号化されていないため、セキュリティリスクは重大で、遠隔地にいる個人がデバイスをかなりの程度制御できてしまう。

sessions from the corporate to the control network should be prohibited unless secured with token-based multi-factor authentication and an encrypted tunnel. Outbound telnet sessions should be allowed only over encrypted tunnels (e.g., VPN) to specific authorized devices.

5.8.5 Dynamic Host Configuration Protocol (DHCP)

DHCP is used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. The base DHCP includes no mechanism for authenticating servers and clients. Rogue DHCP servers can provide incorrect information to clients. Unauthorized clients can gain access to server and cause exhaustion of available resources (e.g., IP addresses). To prevent this, it is recommended to use static configuration instead of dynamic address allocation, which should be the typical configuration for ICS devices. If dynamic allocation is necessary, it is recommended to enable DHCP snooping to defend against rogue DHCP servers, Address Resolution Protocol (ARP) and IP spoofing. The DHCP servers should be placed in the same network segment as configured equipment (e.g., on the router). DHCP relaying is not recommended.

5.8.6 Secure Shell (SSH)

SSH allows remote access to a device. It provides secure authentication and authorization based on cryptography. If remote access is required to the control network, SSH is recommended as the alternative to telnet, rlogin, rsh, rcp and other insecure remote access tools.

5.8.7 Simple Object Access Protocol (SOAP)

SOAP is an XML-based format syntax to exchange messages. Traffic flows related to SOAP-based services should be controlled at the firewall between corporate and ICS network segments. If these services are necessary, deep-packet inspection and/or application layer firewalls should be used to restrict the contents of messages.

5.8.8 Simple Mail Transfer Protocol (SMTP)

SMTP is the primary email transfer protocol on the Internet. Email messages often contain malware, so inbound email should not be allowed to any control network device. Outbound SMTP mail messages from the control network to the corporate network are acceptable to send alert messages.

5.8.9 Simple Network Management Protocol (SNMP)

SNMP is used to provide network management services between a central management console and network devices such as routers, printers, and PLCs. Although SNMP is an extremely useful service for maintaining a network, it is very weak in security. Versions 1 and 2 of SNMP use unencrypted passwords to both read and configure devices (including devices such as PLCs), and in many cases the passwords are well known and cannot be changed. Version 3 is considerably more secure but is still limited in use. SNMP V1 & V2 commands both to and from the control network should be prohibited unless they are over a separate, secured management network, whereas SNMP V3 commands may be able to be sent to the ICS using the security features inherent to V3.

遠隔管理にはセキュアシェル（SSH）プロトコル[5.8.6]を使用するよう推奨する。企業ネットワークから制御ネットワークへの着信テルネットセッションは、トークンベースの多要素認証及び暗号化トンネルでセキュリティが確保されていなければ、禁止すべきである。送信テルネットは、許可された特定のデバイスに対して、暗号化トンネル（VPN 等）でのみ許可すべきである。

5.8.5 動的ホスト構成プロトコル（DHCP）

DHCP は、例えば IP アドレスをインタフェースやサービスへ割り当てるなど、IP ネットワーク上でネットワーク構成パラメータを動的に割り当てるときに使用する。基本的な DHCP にはサーバとクライアントの認証メカニズムがない。ローグ DHCP サーバは不正確な情報をクライアントに提供する。未許可のクライアントがサーバにアクセスして、利用可能なリソース（IP アドレス等）を枯渇させることがある。これを防ぐには、動的なアドレス割当ではなく静的構成にすることが推奨され、ICS デバイスではこれが一般的な構成となるべきである。動的割当が必要な場合、DHCP スヌーピングを使用可能にし、ローグ DHCP、アドレス解決プロトコル（ARP）及び IP 詐称を防止することが推奨される。DHCP サーバは、構成装備品と同じネットワークセグメント（ルータ上等）内に配置すべきである。DHCP リレーは推奨できない。

5.8.6 セキュアシェル（SSH)

SSH はデバイスへのリモートアクセスを可能にする。セキュアな認証を行い、暗号法に基づいて許可を与える。制御ネットワークへのリモートアクセスが必要な場合、テルネット、r ログイン、rsh、rcp その他のセキュアでないリモートアクセスツールに代えて SSH の使用が推奨される。

5.8.7 シンプルオブジェクトアクセスプロトコル（SOAP）

SOAP は、メッセージ交換用の XML ベース形式のシンタックスである。SOAP ベースサービスに関連したトラフィックフローは、企業及び ICS ネットワークセグメント間のファイアウォールで制御すべきである。このようなサービスが必要な場合、ディープパケットインスペクション又はアプリケーション層ファイアウォールを使用して、メッセージ内容を制限すべきである。

5.8.8 シンプルメール転送プロトコル（SMTP）

SMTP はインターネットでの主要な電子メール転送プロトコルである。電子メールメッセージにはマルウエアが含まれていることが多いため、着信電子メールは、いかなる制御ネットワークデバイスにも達するべきでない。制御ネットワークから企業ネットワークへの送信 SMTP メールメッセージは、アラートメッセージの送信時に許可される。

5.8.9 シンプルネットワーク管理プロトコル（SNMP）

SNMP は、中央管理コンソールとネットワークデバイス（ルータ、プリンタ、PLCs 等）間のネットワーク管理サービスを提供するために使用する。SNMP はネットワークの保守には極めて便利なサービスであるが、セキュリティが極めて弱い。SNMP のバージョン 1 と 2 では、読取りもデバイス（PLCs 等）設定も暗号化されていないパスワードを使用しており、多くの場合パスワードがよく知られており、変更ができない。バージョン 3 ではかなりセキュアになっているが、使用されている数は少ない。
制御ネットワークとの SNMP バージョン 1 と 2 のコマンドは、別個のセキュアな管理ネットワーク以外では禁止とすべきで、バージョン 3 のコマンドは固有のセキュリティ機能を使用して ICS に送信できる。

5.8.10 Distributed Component Object Model (DCOM)

DCOM is the underlying protocol for OLE for Process Control (OPC). It utilizes Microsoft's Remote Procedure Call (RPC) service which, when not patched, has many vulnerabilities. These vulnerabilities were the basis for the Blaster worm[27] exploits. In addition, OPC, which utilizes DCOM, dynamically opens a wide range of ports (1024 to 65535) that can be extremely difficult to filter at the firewall. This protocol should only be allowed between control network and DMZ networks and explicitly blocked between the DMZ and corporate network. Also, users are advised to restrict the port ranges used by making registry modifications on devices using DCOM.

5.8.11 SCADA and Industrial Protocols

SCADA and industrial protocols, such as Modbus/TCP, EtherNet/IP, IEC 61850, ICCP and DNP3[28], are critical for communications to most control devices. Unfortunately, many of these protocols were designed without security built in and do not typically require any authentication to remotely execute commands on a control device. These protocols should only be allowed within the control network and not allowed to cross into the corporate network.

5.9 Network Address Translation (NAT)

Network address translation (NAT) is a service where IP addresses used on one side of a network device can be mapped to a different set on the other side on an as-needed basis. It was originally designed for IP address reduction purposes so that an organization with a large number of devices that occasionally needed Internet access could get by with a smaller set of assigned Internet addresses.

To do this, most NAT implementations rely on the premise that not every internal device is actively communicating with external hosts at a given moment. The firewall is configured to have a limited number of outwardly visible IP addresses. When an internal host seeks to communicate with an external host, the firewall remaps the internal IP address and port to one of the currently unused, more limited, public IP addresses, effectively concentrating outgoing traffic into fewer IP addresses. The firewall must track the state of each connection and how each private internal IP address and source port was remapped onto an outwardly visible IP address/port pair. When returning traffic reaches the firewall, the mapping is reversed and the packets forwarded to the proper internal host.

For example, a control network device may need to establish a connection with an external, non-control network host (for instance, to send a critical alert email). NAT allows the internal IP address of the initiating control network host to be replaced by the firewall; subsequent return traffic packets are remapped back to the internal IP address and sent to the appropriate control network device. More specifically, if the control network is assigned the private subnet 192.168.1.xxx and the Internet network expects the device to use the corporate assigned addresses in the range 192.6.yyy.zzz, then a NAT firewall will substitute (and track) a 192.6.yyy.zzz source address into every outbound IP packet generated by a control network device.

Producer-consumer protocols, such as EtherNet/IP and Foundation Fieldbus, are particularly troublesome because NAT does not support the multicast-based traffic that these protocols need to offer their full services.

---

[27] http://en.wikipedia.org/wiki/Blaster_%28computer_worm%29

[28] 15 IEEE 1815-2012, *IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)*,) incorporates DNP3 Secure Authentication version 5 (DNP3-SAv5) which provides strong application layer authentication with remote security credential management. See https://standards.ieee.org/findstds/standard/1815-2012.html.

5.8.10 分散コンポーネントオブジェクトモデル（DCOM）

DCOM はプロセス制御用 OLE（OPC）の基本プロトコルである。マイクロソフトの遠隔手続き呼び出し（RPC）サービスを使用するが、これはパッチを当てないと脆弱性が多い。このような脆弱性は、ブラスターワーム[29]の標的となった。また DCOM を利用する OPC は、多様なポートを動的に開くため（1024～65535)、ファイアウォールでのフィルタリングが極めて困難となる。このプロトコルは、制御ネットワークと DMZ 間でのみ許可すべきで、DMZ と企業ネットワーク間では明示的にブロックすべきである。またユーザは、DCOM 使用デバイスのレジストリ変更時に使用するポートの範囲を限定するのがよい。

5.8.11 SCADA 及び産業用プロトコル

Modbus/TCP、EtherNet/IP、IEC 61850、ICCP、DNP3[30]等の SCADA 及び産業用プロトコルは、ほとんどの制御デバイスへの通信にとって肝要である。残念ながらこれらのプロトコルの多くは、セキュリティを考慮に入れずに設計されており、制御デバイス上でコマンドを遠隔実行する際に、通常認証を必要としない。このようなプロトコルは制御ネットワーク内でのみ許可し、企業ネットワークへの進入は許可すべきでない。

5.9 ネットワークアドレス変換（NAT）

ネットワークアドレス変換（NAT）サービスは、ネットワークデバイスの一方の側で使用している IP アドレスを、必要の都度、他方の側にマップする。元々の設計目的は、時々インターネットアクセスが必要となる多量のデバイスを擁する組織が、少数の割当インターネットアドレスで済むように IP アドレスを減らすことにあった。

そのためほとんどの NAT 実装では、全ての社内デバイスが、ある瞬間に外部ホストと活発に交信するわけではないという前提に立っている。ファイアウォールの設定は、外部から見える IP アドレスの数が限定されるように行う。社内ホストが社外ホストと交信する際、ファイアウォールは、内部 IP アドレスとポートを現在使用していない更に限定されたパブリック IP アドレスにリマップし、送信トラフィックをより少数の IP アドレスに効果的に集結させる。ファイアウォールは、それぞれの接続の状態と、各プライベート内部 IP アドレス及びソースポートが、外部から見える IP アドレス/ポートのペアにどうリマップされたかを追跡しなければならない。戻りトラフィックがファイアウォールに達すると、マッピングが反転し、パケットが正しい社内ホストに転送される。

例えば、制御ネットワークデバイスは、外部の非制御ネットワークホストと接続を確立する必要が生じることがある（重要アラート電子メールの送信など）。NAT は、開始制御ネットワークホストの内部 IP アドレスがファイアウォールにより置換されるようにし、その後の戻りトラフィックパケットは、内部 IP アドレスにリマップされ、正しい制御ネットワークデバイスに送られる。具体的に言うと、制御ネットワークにプライベートサブネット 192.168.1.xxx が割り当てられ、インターネットネットワークはデバイスが 192.6.yyy.zzz の範囲の企業割当アドレスを使用するように予想しているとする。その場合、NAT ファイアウォールは、192.6.yyy.zzz ソースアドレスを、制御ネットワークデバイスが生成する全ての発信 IP パケットに置換（して追跡）する。

EtherNet/IP や Foundation Fieldbus といった生産者・消費者プロトコルは、とりわけ問題が多い。というのは、これらのプロトコルが十分なサービスを提供するために必要とするマルチキャストベースのトラフィックに NAT が対応していないからである。

---

29 http://en.wikipedia.org/wiki/Blaster_%28computer_worm%29

30 IEEE 1815-2012『電力システム通信用 IEEE 規格-分散ネットワークプロトコル（DNP3）』は、DNP3 セキュア認証バージョン 5（DNP3-SAv5）を組み込んでおり、遠隔セキュリティ信頼性管理に強力なアプリケーション層認証を付与する。次の URL を参照のこと。https://standards.ieee.org/findstds/standard/1815-2012.html.

In general, while NAT offers some distinct advantages, its impact on the actual industrial protocols and configuration should be assessed carefully before it is deployed. Furthermore, certain protocols are specifically broken by NAT because of the lack of direct addressing. For example, OPC requires special third-party tunneling software to work with NAT.

5.10 Specific ICS Firewall Issues

In addition to the issues with firewalls and ICS already discussed, there are some additional problems that need to be examined in more detail. The rest of this section discusses three specific areas of concern: the placement of data historians, remote access for ICS support, and multicast traffic.

5.10.1 Data Historians

The existence of shared control network/corporate network servers such as data historians and asset management servers can have a significant impact on firewall design and configuration. In three-zone systems the placement of these servers in a DMZ is relatively straightforward, but in two-zone designs the issues become complex. Placing the historian on the corporate side of the firewall means that a number of insecure protocols, such as Modbus/TCP or DCOM, must be allowed through the firewall and that every control device reporting to the historian is exposed to the corporate side of the network. On the other hand, putting the historian on the control network side means other equally questionable protocols, such as HTTP or SQL, must be allowed through the firewall, and there is now a server accessible to nearly everyone in the organization sitting on the control network.
In general, the best solution is to avoid two-zone systems (no DMZ) and use a three-zone design, placing the data collector in the control network and the historian component in the DMZ.

5.10.2 Remote Support Access

Another issue for ICS firewall design is user and/or vendor remote access into the control network. Any users accessing the control network from remote networks should be required to authenticate using an appropriately strong mechanism such as token-based authentication. While it is possible for the controls group to set up their own remote access system with multi-factor authentication on the DMZ, in most organizations it is typically more efficient to use existing systems set up by the IT department. In this case a connection through the firewall from the IT remote access server is needed.
Remote support personnel connecting over the Internet or via dialup modems should use an encrypted protocol, such as running a corporate VPN connection client, application server, or secure HTTP access, and authenticate using a strong mechanism, such as a token based multi-factor authentication scheme, in order to connect to the general corporate network. Once connected, they should be required to authenticate a second time at the control network firewall using a strong mechanism, such as a token based multi-factor authentication scheme, to gain access to the control network. Proxy servers can also provide additional capabilities for securing remote support access.

5.10.3 Multicast Traffic

Most industrial producer-consumer (or publisher-subscriber) protocols operating over Ethernet, such as EtherNet/IP and Foundation Fieldbus HSE, are IP multicast-based. The first advantage of IP multicasting is network efficiency; by not repeating the data transmission to the multiple destinations, a significant reduction in network load can occur. The second advantage is that the sending host need not be concerned with knowing every IP address of every destination host listening for the broadcast information. The third, and perhaps most important for industrial control purposes, is that a single multicast message offers

全体として、NAT にはいくつか明確な利点があるが、展開するに先立って、実際の産業用プロトコル及び構成に与える影響を慎重に評価すべきである。更に特定のプロトコルは、直接のアドレッシングがないため、NAT により破壊される。例えば OPC は、NAT と共用するためにはサードパーティの特殊トンネリングソフトウエアが必須となる。

5.10 ICS ファイアウォール固有の問題

これまで見てきたファイアウォールと ICS に関わる問題に加えて、更に詳しく考察すべき問題もある。このセクションの残りの部分では、データヒストリアンの配置、ICS サポートのためのリモートアクセス、マルチキャストトラフィックという 3 つの特定分野について考察する。

5.10.1 データヒストリアン

データヒストリアンや資産管理サーバといった共有制御/企業ネットワークサーバの存在は、ファイアウォールの設計や構成に大きな影響を及ぼすことがある。3 ゾーンシステムでは、これらサーバを DMZ に配置するのは比較的単純明快だが、2 ゾーン設計では問題が複雑になる。ヒストリアンをファイアウォールの企業側に置くということは、Modbus/TCP や DCOM といったセキュアでない多数のプロトコルがファイアウォールに入るのを許すことになり、ヒストリアンの下にある全ての制御デバイスがネットワークの企業側にさらされることになる。反対に、ヒストリアンを制御ネットワーク側に置けば、HTTP や SQL といった同様に問題の多いプロトコルがファイアウォールに入るのを許すことになり、制御ネットワーク上にあるサーバに、組織のほぼ全員がアクセスできることになってしまう。

総じて最善のソリューションは、2 ゾーンシステム（DMZ なし）を避けて 3 ゾーンシステムを使用し、データコレクタは制御ネットワーク内に、ヒストリアンコンポーネントは DMZ 内に配置することである。

5.10.2 遠隔サポートシステム

ICS ファイアウォール設計の別の問題は、ユーザ又はベンダーが制御ネットワークにリモートアクセスすることである。遠隔ネットワークから制御ネットワークにアクセスするユーザは、トークンベース認証等の強力なメカニズムを使用して、認証を義務づけるべきである。制御グループが DMZ に多要素認証機能の付いた独自のリモートアクセスシステムを設置するのは可能であるが、ほとんどの組織では、IT 部門が設置した既存システムを利用する方が効率的である。その場合、IT リモートアクセスサーバからファイアウォールを経由する接続が必要となる。

インターネット又はダイアルアップモデム経由で接続する遠隔サポート要員は、企業 VPN 接続クライアント、アプリケーションサーバ、セキュア HTTP アクセス等を実行する暗号プロトコルを使用し、汎用企業ネットワークにアクセスするため、トークンベース多要素認証等の強力なメカニズムを使用して認証を行うべきである。接続したなら、制御ネットワークファイアウォールにおいて、トークンベース多要素認証等の強力なメカニズムを使用して再度認証を求めてから、制御ネットワークへのアクセスを許可すべきである。プロキシサーバも遠隔サポートアクセスのセキュリティを更に向上させる。

5.10.3 マルチキャストトラフィック

EtherNet/IP や Foundation Fieldbus HSE などイーサネット上で機能するほとんどの生産者・消費者（又は発行者・購読者）プロトコルは IP マルチキャストベースである。IP マルチキャスティングの最大の利点はネットワーク効率にある。データ送信を複数の宛先に繰り返す必要がないため、ネットワーク負荷が著しく減る。2 つ目の利点は、送信ホストが、ブロードキャスト情報をリスニングしている全ての宛先ホストの IP アドレスを知る必要がないことである。

far better capabilities for time synchronization between multiple control devices than multiple unicast messages.

If the source and destinations of a multicast packet are connected with no intervening routers or firewalls between them, the multicast transmission is relatively seamless. However, if the source and destinations are not on the same LAN, forwarding the multicast messages to a destination becomes more complicated. To solve the problem of multicast message routing, hosts need to join (or leave) a group by informing the multicast router on their network of the relevant group ID through the use of the Internet Group Management Protocol (IGMP). Multicast routers subsequently know of the members of multicast groups on their network and can decide whether or not to forward a received multicast message onto their network. A multicast routing protocol is also required. From a firewall administration perspective, monitoring and filtering IGMP traffic becomes another series of rule sets to manage, adding to the complexity of the firewall.

Another firewall issue related to multicasting is the use of NAT. A firewall performing NAT that receives a multicast packet from an external host has no reverse mapping for which internal group ID should receive the data. If IGMP-aware, it could broadcast it to every group ID it knows about, because one of them will be correct, but this could cause serious issues if an unintended control packet were broadcast to a critical node. The safest action for the firewall to take is to drop the packet. Thus, multicasting is generally considered NAT-unfriendly.

5.11 Unidirectional Gateways

Hardware-enforced unidirectional gateways (e.g., data diodes) are increasingly deployed at the boundary between ICS and IT networks, as well as between Safety Instrumented System networks and control networks. Unidirectional gateways are a combination of hardware and software. The hardware permits data to flow from one network to another, but is physically unable to send any information at all back into the source network. The software replicates databases and emulates protocol servers and devices.

5.12 Single Points of Failure

Single points of failure can exist at any level of the ANSI/ISO stack. An example is PLC control of safety interlocks. Because security is usually being added to the ICS environment, an evaluation should be done to identify potential failure points and a risk assessment done to evaluate each point’s exposure. Remediation methods can then be postulated and evaluated and a “risk versus reward” determination made and design and implementation done.

5.13 Redundancy and Fault Tolerance

ICS components or networks that are classified as critical to the organization have high availability requirements. One method of achieving high availability is through the use of redundancy. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS, or does not cause another problem elsewhere, such as a cascading event.

The control system should have the ability to execute an appropriate fail-safe process upon the loss of communications with the ICS or the loss of the ICS itself. The organization should define what "loss of communications" means (e.g., 500 milliseconds, 5 seconds, 5 minutes, etc. without communications). The organization should then, based on potential consequences, define the appropriate fail-safe process for their industry.

3 つ目は、おそらく産業用制御目的では最も重要と思われるが、複数制御デバイス間の時間同期にとって、1 つのマルチキャストメッセージの方が複数のユニキャストメッセージよりもはるかに優れていることである。

マルチキャストパケットのソースと宛先が仲介ルータやファイアウォールなしで接続されている場合、マルチキャスト送信は相対的にシームレスである。ただし、ソースと宛先が同じ LAN 上にない場合、マルチキャストメッセージの宛先転送は複雑になる。マルチキャストメッセージルーティングの問題を解決するには、各ホストが 1 つのグループに加入（又は離脱）することである。これを行うに各ホストのネットワーク上のマルチキャストルータに、インターネットグループ管理プロトコル（IGMP）を介して、当該グループ ID を通知する。各マルチキャストルータは、それぞれのネットワーク上のマルチキャストグループメンバーについて知り、受信したマルチキャストメッセージをネットワークに転送するかどうかを決定する。マルチキャストルーティングプロトコルも必要となる。ファイアウォール管理の観点からすれば、IGMP トラフィックの監視及びフィルタリングは、管理すべき別のルールセットとなり、ファイアウォールをいっそう複雑にする。

マルチキャスティングに関連した別のファイアウォールの問題は NAT の使用である。NAT を実行するファイアウォールで、外部ホストからのマルチキャストパケットを受信するものにはリバースマッピングがなく、これについては内部グループ ID がデータを受信すべきである。IGMP が認識していれば、既知のグループ ID 全てにブロードキャストする。その理由は、そのうちの 1 つが正しくても、意図しない制御パケットが重要ノードにブロードキャストされると、大きな問題になる可能性があるからである。ファイアウォールが取り得る最も安全な策は、パケットをドロップすることである。よって、マルチキャスティングは総じて NAT と相性が悪いとみなされる。

5.11 単方向性ゲートウェイ

ハードウエアで強制する単方向性ゲートウェイ（データダイオード等）は、ICS ネットワークと IT ネットワーク間や、安全計装システムネットワークと制御ネットワーク間の境界にますます展開されるようになってきた。単方向性ゲートウェイはハードウエアとソフトウエアを組み合わせたものである。ハードウエアはデータが一方のネットワークから他方のネットワークへ流れるのを許可するが、ソースネットワークに情報を返すことは物理的に不可能である。ソフトウエアはデータベースを複製して、プロトコルサーバ及びデバイスをエミュレートする。

5.12 単一障害点

単一障害点は、ANSI/ISO スタックのどのレベルにもある。一例は安全インターロックの PLC 制御である。セキュリティは通常 ICS 環境に追加されていくものなので、評価を行って障害となり得る点を明らかにし、リスク評価を行って各点のエクスポージャを査定する。
次いで対処方法を想定して評価し、「リスク対報酬」を判定し、設計・実装を行う。

5.13 冗長性とフォールトトレランス

組織にとって重要と分類される ICS コンポーネントやネットワークには、高い可用性要件が課される。高い可用性を実現する 1 つの方法は、冗長性の利用である。また、あるコンポーネントに障害が出た場合でも、ICS に不要のトラフィックを生じさせず、連鎖イベントなど別の問題を派生させてはならない。
制御システムは、ICS との通信喪失時又は ICS そのものの喪失時に、適切なフェールセーフプロセスを実行できる能力を備えているべきである。組織は「通信喪失」の意味を明らかにすべきである（通信途絶で 500 ミリ秒、5 秒、5 分等）。次いで生じ得る結果を基に、産業用の適正なフェールセーフプロセスを明らかにすべきである。

Backups should be performed using the “backup-in-depth” approach, with layers of backups (e.g., local, facility, disaster) that are time-sequenced such that rapid recent local backups are available for immediate use and secure backups are available to recover from a massive security incident. A mixture of backup/restore approaches and storage methods should be used to ensure that backups are rigorously produced, securely stored, and appropriately accessible for restoration.

5.14 Preventing Man-in-the-Middle Attacks

A man-in-the-middle attack requires knowledge of the protocol being manipulated. The Address Resolution Protocol (ARP) man-in-the-middle attack is a popular method for an adversary to gain access to the network flow of information on a target system. This is performed by attacking the network ARP cache tables of the controller and the workstation machines. Using the compromised computer on the control network, the adversary poisons the ARP tables on each host and informs them that they must route all their traffic through a specific IP and hardware address (i.e., the adversary’s machine). By manipulating the ARP tables, the adversary can insert their machine between the two target machines and/or devices.

The ARP man-in-the-middle attack works by initiating gratuitous ARP commands to confuse each host (i.e., ARP poisoning). These ARP commands cause each of the two target hosts to use the MAC address of the adversary as the address for the other target host. When a successful man-in-the-middle attack is performed, the hosts on each side of the attack are unaware that their network data is taking a different route through the adversary’s computer.

Once an adversary has successfully inserted their machine into the information stream, they now have full control over the data communications and could carry out several types of attacks. One possible attack method is the replay attack. In its simplest form, captured data from the control/HMI is modified to instantiate activity when received by the device controller. Captured data reflecting normal operations in the ICS could be played back to the operator as required. This would cause the operator’s HMI to appear to be normal and the attack will go unobserved. During this replay attack the adversary could continue to send commands to the controller and/or field devices to cause an undesirable event while the operator is unaware of the true state of the system.
Another attack that could be carried out with the man-in-the-middle attack is sending false messages to the operator, and could take the form of a false negative or a false positive. This may cause the operator to take an action, such as flipping a breaker, when it is not required, or it may cause the operator to think everything is fine and not take an action when an action is required. The adversary could send commands to the operator’s console indicating a system change, and when the operator follows normal procedures and attempts to correct the problem, the operator’s action could cause an undesirable event. There are variations of the modification and replay of control data which could impact the operations of the system.
Protocol manipulation and the man-in-the-middle attack are among the most popular ways to manipulate insecure protocols, such as those found in control systems. However, there are mitigation techniques [38] that can be applied to secure the systems through MAC address locking, static tables, encryption, authentication, and monitoring.

- **MAC Address Locking** - The ARP man-in-the-middle attack requires the adversary to be connected to the local network or have control of a local computer on the network. Port security, also called MAC address locking, is one method to secure the physical connection at the end of each port on a network switch. High-end corporate class network switches usually have some kind of option for MAC address locking. MAC address locking is very effective against a rogue individual looking to physically plug into the internal network. Without port security, any open network jack on the wall

バックアップは「多層バックアップ」アプローチにより、時系列順になったバックアップ層（ローカル、施設、災害等）に対して実施し、急速に行われた最近のローカルバックアップがすぐに使用できるようにし、セキュアなバックアップが大規模なセキュリティインシデントから復帰する際に利用できるようにする。バックアップ/復元とストレージ法とを併用して、バックアップが厳格に作成され、安全に保管され、適切に復元できるようにする。

5.14 人が介在する攻撃の防止

人が介在する攻撃は、操作中のプロトコルに対する知識が必須となる。宛先解決プロトコル（ARP）の人が介在する攻撃は、攻撃側が標的システム上の情報の流れにアクセスするためのよくある方法である。これを行うには、コントローラ及びワークステーションマシンのネットワーク ARP キャッシュテーブルを攻撃する。制御ネットワーク上の性能が低下したコンピュータを利用して、攻撃側は各ホスト上の ARP テーブルを攻め、全てのトラフィックを特定の IP 及びハードウエアアドレス（攻撃側のマシン）に送るよう指示する。攻撃側は ARP テーブルを操作して、2 台の標的マシン間又はデバイス間に自らのマシンを挿入する。

ARP の人が介在する攻撃は、余計な ARP コマンドを発行して、各ホストを混乱させることで機能する（ARP ポイズニング）。このような ARP コマンドは、2 台の標的ホストのおのおのに、攻撃側の MAC アドレスを他の標的ホスト用のアドレスとして使用するように仕向ける。人が介在する攻撃が成功すると、攻撃の両側のホストが気づかないうちに、ネットワークデータが別経路をたどって攻撃側のコンピュータに流れる。

攻撃側が自らのマシンを首尾よく情報経路に挿入すると、データ通信を全面的に制御でき、種々の攻撃を仕掛けられるようになる。その 1 つがリプレー攻撃である。最も単純な形態は、制御/HMI から捕捉したデータを改変して、デバイスコントローラがこれを受信したときに行動を起こすようにするものである。ICS における正常な業務を反映した捕捉データは、必要に応じて操作員にプレイバックされる。これにより操作員の HMI は見かけ上正常に見え、攻撃は発覚しない。このリプレー攻撃中に、攻撃側はコントローラ又はフィールドデバイスにコマンドを送り続け、有害事象を生じさせることができるが、操作員はシステムの実情に気づかない。

人が介在する攻撃の別のものとして、偽のメッセージを操作員に送り、擬似陰性又は擬似陽性の形態を取るものがある。このため操作員は、ブレーカーを落とすといった不要な対応を取ったり、逆に必要な対応を取らなければならないのに、全て良好と思い込んで何もしないといったことが生じる。攻撃側は操作員のコンソールに、システムの変更を示すコマンドを送り、操作員が通常手順に従って問題を修正しようとすると、それが元で有害事象が発生する。システムの動作に影響する制御データの変更及びリプレーには種々のバリエーションがある。

プロトコル操作と人が介在する攻撃は、制御システムで見られるもののうち、セキュアでないプロトコルを操作する方法として最もよく使用される方法の 1 つである。しかし MAC アドレスロック、スタティックテーブル、暗号化、認証及び監視を通じて、システムをセキュアにするための緩和技術がある[38]。

- MAC アドレスロック - ARP の人が介在する攻撃では、攻撃側がローカルネットワークに接続し、ネットワーク上のローカルコンピュータを制御することが必要となる。MAC アドレスロックとも呼ばれるポートセキュリティは、ネットワークスイッチ上の各ポート端における物理的接続をセキュアにする方法である。ハイエンド企業クラスネットワークスイッチには、通常 MAC アドレスロック用のオプションがいくつか用意されている。MAC アドレスロックは、内部ネットワークへの物理的プラグインを目論む個人に対して極めて有効である。ポートセキュリティがない場合、壁面のオープンネットワークジャックを利用して、

could be used as an avenue onto the corporate network. Port security locks a specific MAC address to a specific port on a managed switch. If the MAC address does not match, the communication link is disabled and the intruder will not be able to achieve their goal. Some of the more advanced switches have an auto resetting option, which will reset the security measure if the original MAC is returned to the port.

Although port security is not attacker proof, it does add a layer of added security to the physical network. It also protects the local network from employees plugging un-patched and out-of-date systems onto the protected network. This reduces the number of target computers a remote adversary can access. These security measures not only protect against attacks from external networks but provide added physical protection as well.

- **Static Tables** – An ICS network that stays relatively static could attempt to implement statically coded ARP tables. Most operating systems have the capability to statically code all of the MAC addresses into the ARP table on each computer. Statically coding the ARP tables on each computer prevents the adversary from changing them by sending ARP reply packets to the victim computer. While this technique is not feasible on a large and/or dynamic corporate network, the limited number of hosts on an ICS network could be effectively protected this way.
- **Encryption** - As a longer-term solution, systems should be designed to include encryption between devices in order to make it very difficult to reverse engineer protocols and forge packets on control system networks. Encrypting the communications between devices would make it nearly impossible to perform this attack. Protocols that provide strong authentication also provide resilience to man-in-the-middle attacks. The impact of encryption on network and operational performance needs to be considered.
- **Authentication -** Protocols with strong authentication provide resilience to man-in-the-middle attacks.
- **Monitoring** - Monitoring for ARP poisoning provides an added layer of defense. There are several programs available (e.g., ARPwatch) that can monitor for changing MAC addresses through the ARP packets.

企業ネットワークへ侵入することができる。ポートセキュリティは、管理されたスイッチ上の特定ポートに特定 MAC アドレスをロックする。MAC アドレスが合わないと、通信リンクが使用不能になり、侵入者は目的を達することができない。より進化したスイッチでは、自動リセットオプションがあり、元の MAC がポートに戻ると、セキュリティ対策がリセットされるようになっている。

ポートセキュリティは、攻撃を寄せ付けないわけではないが、物理ネットワークにセキュリティのレイヤーを追加するものとなる。また従業員がパッチの当たっていない旧式システムで、保護されたネットワークに接続した場合に、ローカルネットワークを保護する。これにより遠隔攻撃でアクセスできる標的コンピュータの数が減る。こうしたセキュリティ対策は、外部ネットワークからの攻撃から保護するだけでなく、物理的保護を増やすことにもなる。

- **スタティックテーブル** - 比較的静的な ICS ネットワークは、静的にコーディングされた ARP テーブルを実装しようとする。ほとんどの OS には、全ての MAC アドレスを各コンピュータの ARP テーブルに静的にコーディングする能力が備わっている。各コンピュータの ARP テーブルへの静的コーディングを行うことにより、攻撃側は、ARP リプライパケットを標的コンピュータに送信して、テーブルを変更することができなくなる。この技術は、大規模な又は動的な企業ネットワークでは実現できないが、ICS ネットワーク上の限定的な数のホストなら、この方法で有効に保護できる。
- **暗号化** - より長期的なソリューションとして、プロトコルのリバースエンジニアリングや制御システムネットワーク上のパケットの偽造を困難にするため、デバイス間の暗号化を設計に含めるべきである。デバイス間の通信を暗号化すれば、この攻撃がほぼ不可能になる。強力な認証を行うプロトコルは、人が介在する攻撃に対する柔軟性も付与する。暗号化によるネットワークや業務パフォーマンスへの影響を検討する必要がある。
- **認証** - 強力な認証メカニズムを持つプロトコルは、人が介在する攻撃に対する柔軟性を付与する。
- **監視** - ARP ポイズニングの監視により防御層が厚くなる。ARP パケットの中で絶えず変化する MAC アドレスを監視できるプログラムがいくつかある（ARP ウォッチ等）。

5.15 Authentication and Authorization

An ICS may contain a large number of systems, each of which must be accessed by a variety of users. Performing the authentication and authorization of these users presents a challenge to the ICS. Managing these user's accounts can be problematic as employees are added, removed, and as their roles change. As the number of systems and users grow, the process of managing these accounts becomes more complicated.

The authentication of a user or system is the process of verifying the claimed identity. Authorization, the process of granting the user access privileges, is determined by applying policy rules to the authenticated identity and other relevant information[31]. Authorization is enforced by some access control mechanism. The authentication process can be used to control access to both systems (e.g. HMIs, field devices, SCADA servers) and networks (e.g., remote substations LANs).

Authentication and authorization can be performed either in a distributed or centralized approach. With distributed authentication and authorization, every system performs these steps on their own. Each system is responsible for storing its own set of user accounts, credentials, and roles and performing the identification and authentication of the user. This approach typically does not require any additional infrastructure. However, this approach is problematic in that it does not scale well as the size of the system increases. For example, if a user leaves the organization, the corresponding user account must be removed from each system individually.

In contrast to the distributed approach, centralized authentication and authorization systems are commonly used to manage larger number of users and accounts. A centralized approach utilizes some central authentication system (e.g., Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP) to store all accounts and manage the authentication and authorization of all individuals and systems. An authentication protocol (e.g., Kerberos, RADIUS, TACACS+) is then used to communicate data between the authentication server and the system performing authentication.

While a centralized approach provides substantially improved scalability, it also presents numerous additional concerns that may impact its use in ICS environments. The following considerations apply:

- Authentication servers create a single system that is responsible for managing all system accounts and must be highly secured.
- The authentications server system requires high availability because its failure may prevent users from authenticating to a system during an emergency. Redundancy may be required.
- Some clients may cache user credentials locally to ensure that users can still be authenticated in the absence of the server. Caching may only be available for users that have recently authenticated. Caching also introduces complications for revocation.
- Networks used to support the authentication protocol must be reliable and secure to ensure authentication attempts are not hindered.

[31] In general, authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes. For further information see NIST SP 800-162, *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, at http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

5.15　認証と権限付与

ICS には多数のシステムが含まれる場合があり、多種多様なユーザがそれぞれにアクセスできなければならない。これらユーザの認証と許可を行うのは ICS にとって重荷となる。従業員の追加、削除と役割の変化に伴い、ユーザアカウントの管理が煩雑になる。システムとユーザの数が増えるにつれて、アカウント管理のプロセスがどんどん複雑化する。

ユーザ又はシステムの許可は、それぞれが主張する ID を検証するプロセスである。権限付与は、ユーザにアクセス権を与えるプロセスで、権限を受ける ID その他関連情報[32]にポリシー規則を適用して判定される。権限付与は何らかのアクセス制御メカニズムにより実行される。権限付与プロセスを利用して、システム（HMIs、フィールドデバイス、SCADA サーバ等）とネットワーク（遠隔サブステーション LAN 等）の両方へのアクセスを制御できる。

認証と権限付与は、分散アプローチでも集中アプローチでも行うことができる。分散認証・権限付与を利用すると、各システムがこれらの手順を独自に行う。各システムはそれぞれの責任でユーザアカウント、認証情報及び役割を保管し、ユーザの識別と権限付与を行う。通常、このアプローチにはほかのインフラが不要である。ただし、システムの増大に伴うスケーラビリティに問題がある。例えば、あるユーザが退社した場合、ユーザアカウントをそれぞれのシステムから削除しなければならない。

分散アプローチとは対照的に、集中認証・権限付与システムは、一般により大規模なユーザ及びアカウントの管理に使用される。集中アプローチは特定の中央認証システム（Microsoft Active Directory、 Lightweight Directory Access Protocol[LDAP]等）を使用して全てのアカウントを保管し、全ユーザ・全システムの認証と権限付与を管理する。次いで権限付与プロトコル（Kerberos、RADIUS、TACACS+等）を使用して認証サーバと認証実施システム間でデータ通信を行う。

集中アプローチではスケーラビリティがかなり向上する反面、ICS 環境で使用した場合の影響については不安が多い。次のような要考慮事項がある。

- 認証サーバが単一システムを創出し、これが全てのシステムアカウントを管理し、高度にセキュアでなければならない。
- 認証サーバシステムは、故障すると緊急時でもユーザはシステム認証ができなくなるため、高い可用性が求められる。冗長性が必要となろう。
- クライアントによっては、ユーザの認証情報をローカルでキャッシュし、サーバがなくてもユーザが認証できるようにしている。キャッシングは、最近認証したユーザにしか利用できない。キャッシングは取消も複雑にする。
- 認証プロトコルをサポートするためのネットワークは信頼性が高くセキュアで、認証の試みが妨げられないようにしなければならない。

[32] 総じて一連の操作をするための権限付与は、主体、対象、求めている操作内容に関係する属性を評価して判定するが、場合によっては、特定の属性に関して許可する操作内容を規定したポリシー、規則又は関係に照らして、環境条件を評価し判定する。詳細は次の URL にある NIST SP 800-162『属性に基づくアクセス制御（ABAC）定義及び考慮』を参照のこと。http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

5.15.1 ICS Implementation Considerations

While centralized authentication and authorization servers are commonly used in an IT environment, there are many challenges to integrating them into ICS. While authentication servers and protocols integrate with many commodity IT products (e.g., Microsoft Windows, Linux, Oracle), often ICS may utilize their own application-specific accounts and authentication mechanisms that were not designed to interface with third party servers and protocols. This limits the adoption of such mechanism in an ICS environment. Older network devices and most field devices do not support any mechanisms to integrated with a centralized authentication system.

5.16 Monitoring, Logging, and Auditing

The security architecture of an ICS must also incorporate mechanisms to monitor, log, and audit activities occurring on various systems and networks. Monitoring, logging, and auditing activities are imperative to understanding the current state of the ICS, validating that the system is operating as intended, and that no policy violations or cyber incidents have hindered the operation of the system. Network security monitoring is valuable to characterize the normal state of the ICS, and can provide indications of compromised systems when signature-based technologies fail. Additionally, strong system monitoring, logging, and auditing is necessary to troubleshoot and perform any necessary forensic analysis of the system[33].

5.17 Incident Detection, Response, and System Recovery

Incidents are inevitable and incident detection, response, and system recovery plans are essential. Major characteristics of a good security program are how soon after an incident has occurred that the incident can be detected and how quickly a system can be recovered after an incident has been detected. Incident response in ICS is closely aligned to disaster recovery, specifically to address the stringent uptime requirements of ICS. Incident Responders must be trained for ICS-specific scenarios, as normal methods of recovering IT systems may not apply to ICS.

[33] For further information see NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)* [55].

5.15.1 ICS 実装上の考慮事項

集中認証サーバ及び集中権限付与サーバは、IT 環境では普通に利用されているが、ICS に両者を組み込むのは問題が多い。認証サーバ及びプロトコルは多くの市販 IT 製品（Microsoft Windows、Linux、Oracle 等）を組み込むが、ICS では独自のアプリケーション固有のアカウントと認証メカニズムを使用することが多く、それらはサードパーティのサーバ及びプロトコルと連携するようにはできていない。そのため ICS 環境ではそうしたメカニズムの採用に限界がある。旧型のネットワークデバイスやほとんどのフィールドデバイスは、集中認証システムに組み込めるメカニズムに対応していない。

5.16 監視、ロギング及び監査

ICS のセキュリティアーキテクチャには、種々システムやネットワークを監視、ログ及び監査できるメカニズムが組み込まれていなければならない。監視、ロギング及び監査活動は ICS の現状を理解し、システムが予定どおり稼働しているか検証し、システムの動作を妨害するようなポリシー違反やサイバーインシデントがないことを検証するために不可欠である。ネットワークセキュリティ監視は、ICS の正常状態の特徴を明確化するために貴重で、署名ベースの技術に障害が出たときに、システム性能が低下した兆候を提示できる。また、トラブルシューティングを行い、システム [34]の必要な調査分析を行うには、強力なシステム監視、ロギング及び監査が必要である。

5.17 インシデント検知、対応及びシステム復旧

インシデントは避けられないので、インシデント検知、対応及びシステム復旧計画が不可欠となる。優秀なセキュリティプログラムの主な特徴は、インシデント発生時にいかに素早く検知し、検知後いかに迅速にシステムを復旧できるかにある。ICS におけるインシデント対応は、災害復旧と密接に連携し、特に ICS の厳格なアップタイム要件について検討する。IT システムの通常の復旧方法は ICS には当てはまらないため、インシデント対応者の訓練は、ICS 固有のシナリオに沿って実施しなければならない。

[34] 詳細は NIST SP 800-94『侵入検知防止システム（IDPS）』[55]を参照のこと。

6. Applying Security Controls to ICS

A single security product or technology cannot adequately protect an ICS. Securing an ICS is based on a combination of effective security policies and a properly configured set of security controls. The selection and implementation of security controls to apply to an ICS can have major implications on the operations, so it is critical to consider:

- Which security controls are needed to adequately mitigate risk to an acceptable level that supports the organizational missions and business functions?
- Have the selected security controls been implemented or is there a realistic implementation plan in place?
- What is the required level of assurance that the selected security controls are implemented correctly, operating as intended, and producing a desired outcome?

As identified in Section 3, the questions should be answered in the context of an effective, organization-wide risk management process and cybersecurity strategy that identifies, mitigates (as necessary), and continuously monitors risks to its ICS. An effective cybersecurity strategy for an ICS should apply defense-in-depth, a technique of layering security mechanisms so that the impact of a failure in any one mechanism is minimized. Use of such a strategy is explored within the security control discussions and their applications to ICS that follow.

6.1 Executing the Risk Management Framework Tasks for Industrial Control Systems

The following describes the process of applying the Risk Management Framework (RMF) to ICS. The process includes a brief description of each activity and identifies supporting NIST documents. The following steps, while shown sequentially, can be implemented in a different order to be consistent with established management and system development life cycle processes [21].

6. ICS へのセキュリティ対策の適用

単一のセキュリティ製品や技術では、ICS をしっかり保護することはできない。ICS のセキュリティ確保は、有効なセキュリティポリシーと構成の行き届いたセキュリティ対策を基調とする。ICS に適用するセキュリティ対策の選定と実装は、業務と密接な関係を持つため、以下について良く検討することが肝要である。

- リスクを許容できるレベルまで緩和し、組織の任務と事業機能を支援できるようにするにはどのセキュリティ対策が必要か。
- 選定したセキュリティ対策は実行されたか、それとも現実的な実行計画があるか。
- 選定したセキュリティ対策を予定どおり正しく実行し、所期の結果を得るにはどの程度の保証レベルが必要か。

セクション 3 で明確にしたように、上記の質問に対する答えは、有効な組織全体のリスク管理プロセスと、組織の ICS リスクを特定し、必要に応じて緩和し、継続的に監視するサイバーセキュリティ戦略に照らして提示されるべきである。ICS の効果的なサイバーセキュリティ戦略は、多層防御として知られるレイヤリングセキュリティメカニズム技術を適用し、あるメカニズムの障害の影響が最小限に食い止められるようにすべきである。このような戦略の使用は、セキュリティ管理に関する議論とその後の ICS への適用の中で策定される。

6.1 産業用制御システム用リスク管理体制の実施

リスク管理体制（RMF）を ICS に適用するためのプロセスを以下に記述する。それぞれの活動に対する概要と NIST の根拠文書を示す。手順を順番に示すが、策定された管理・システム開発ライフサイクルプロセス[21]に従って、順序を変えて実施してもかまわない。

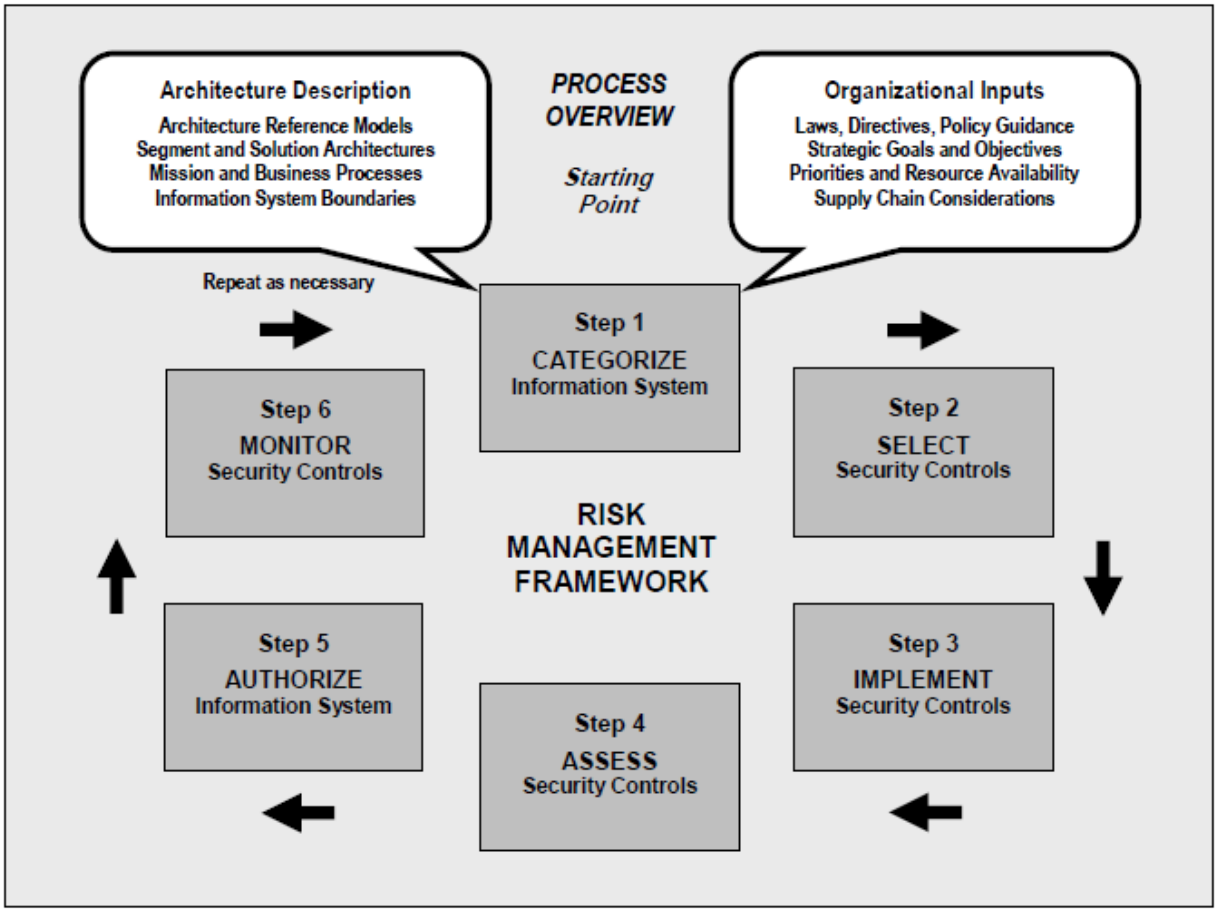

Figure 6-1. Risk Management Framework Tasls

6.1.1 Step 1: Categorize Information System

The first activity in the RMF is to categorize the information and information system according to potential impact of loss. For each information type and information system under consideration, the three FISMA-defined security objectives—confidentiality, integrity, and availability—are associated with one of three levels of potential impact should there be a breach of security. It is important to remember that for an ICS, availability is generally the greatest concern.

The standards and guidance for this categorization process can be found in FIPS 199 [15] and NIST SP 800-60 [25], respectively. NIST is in the process of updating NIST SP 800-60 to provide additional guidance on the categorization of ICS.

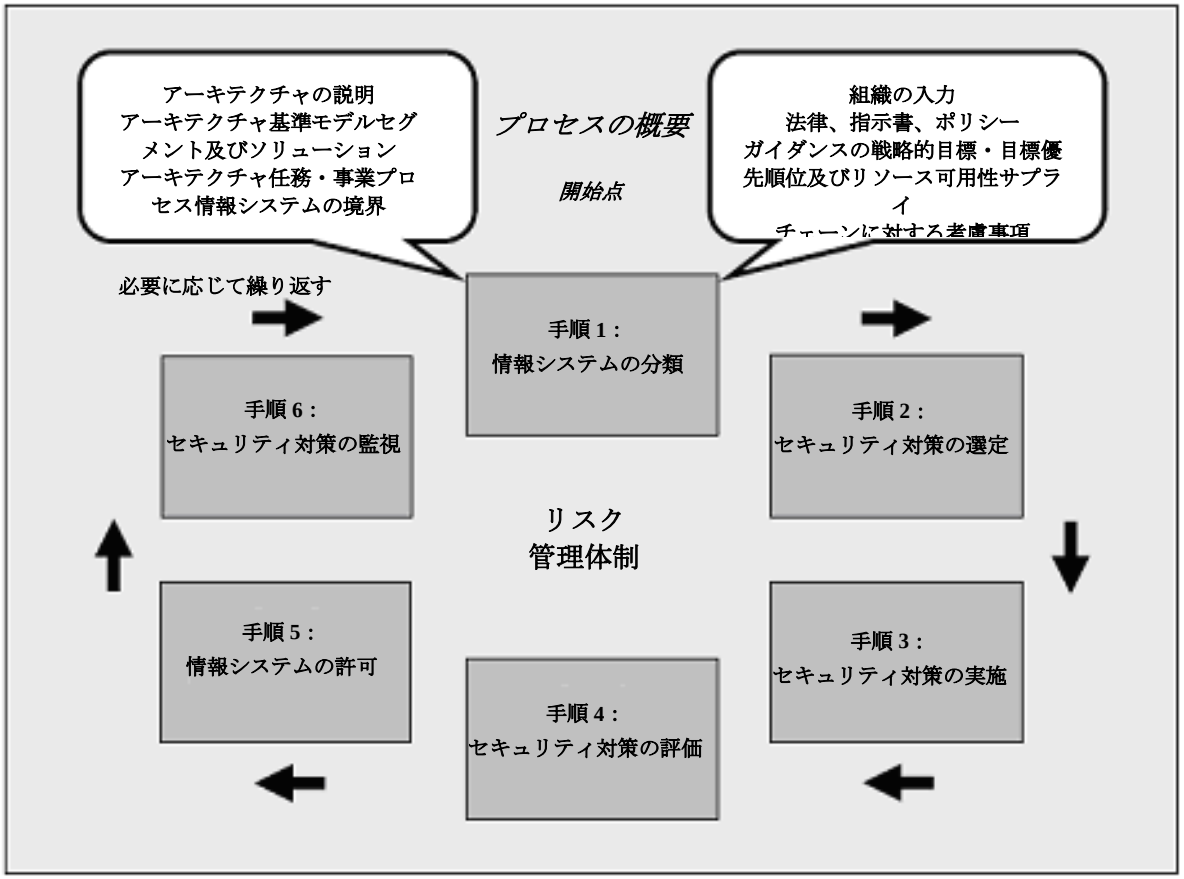

図 6-1.リスク管理体制業務

6.1.1 手順 1：情報システムの分類

RMF の第 1 歩は、喪失時の影響に応じて、情報と情報システムを分類することである。検討中の情報の種類と情報システムごとに、FISMA の定義による機密性・完全性・可用性という 3 つのセキュリティ目標が、セキュリティ違反があった場合の 3 レベルのうちのいずれかに関連づけられる。ICS では総じて可用性が最大の関心事となる点を銘記するのは肝要である。

この分類プロセスの基準とガイダンスは、それぞれ FIPS 199[15]と NIST SP 800-60 [25]にある。NIST では NIST SP 800-60 を改訂中で、ICS の分類に関する補足的なガイダンスを提供する予定である。

The following ICS example is taken from FIPS 199 [15]:

ICS-specific Recommendations and Guidance

A power plant contains a SCADA system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. The resulting security categories, SC, of these information types are expressed as:

SC sensor data = {(**confidentiality**, NA), (integrity, HIGH), (**availability**, HIGH)},

and

SC administrative information = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}.

The resulting security category of the information system is initially expressed as:

SC SCADA system = {(**confidentiality**, LOW), (integrity, HIGH), (**availability**, HIGH)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the SCADA system. The management at the power plant chooses to increase the potential impact from a loss of confidentiality from low to moderate, reflecting a more realistic view of the potential impact on the information system should there be a security breach due to the unauthorized disclosure of system-level information or processing functions. The final security category of the information system is expressed as:

SC SCADA system = {(**confidentiality**, MODERATE), (**integrity**, HIGH), (**availability**, HIGH)}.

FIPS 199 specifies that information systems be categorized as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. Possible definitions for low, moderate, and high levels of security based on impact for ICS based on ISA99 are provided in Table 6-1. Possible definitions for ICS impact levels based on product produced, industry and security concerns are provided in Table 6-2.

Table 6-1. Possible Definitions for ICS Impact Levels Based on ISA99

Impact Category	Low-Impact	Moderate-Impact	High-Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss	$1,000	$100,000	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Minutes	Days	Weeks
Public Image	Temporary damage	Lasting damage	Permanent damage

以下の ICS の例は、FIPS 199[15]から抜粋したものである。

ICS 固有の推奨事項及びガイダンス

ある発電所には、大規模軍事施設への配電を制御する SCADA システムが設置されている。SCADA システムにはリアルタイムセンサデータと定常の管理情報が含まれる。発電所の経営陣は以下のとおり判定している。（1）SCADA システムで取得するセンサデータについては、機密性が失われても影響はなく、完全性が失われるとかなりの影響があり、可用性が失われるとかなりの影響がある。（2）システムが処理する管理情報については、機密性が失われても影響は少なく、完全性が失われても影響は少なく、可用性が失われても影響は少ない。このような情報の種類に基づく結果、セキュリティ分類（SC）は次の式で表すことができる。

SC センサデータ = {(**機密性**、NA), (**完全性**, HIGH), (**可用性**, HIGH)}、また

SC 管理情報 = {(**機密性**、LOW), (**完全性**, LOW), (**可用性**, LOW)}。

情報システムに基づくセキュリティ分類は当初

SC　SCADA システム = {(**機密性**、LOW), (**完全性**, HIGH), (**可用性**, HIGH)}で、

SCADA システムに常駐する情報の種類に基づくセキュリティ目標ごとの影響値は、大又は最大影響度を示している。発電所の経営陣の選択は、機密性が失われたときの影響度を低から中にし、万一システムレベル又は処理機能の漏洩によるセキュリティ違反が生じた際に、情報システムへの影響をより現実的にとらえるようにした。最終的な情報システムに基づくセキュリティ分類は

SC　SCADA システム = {(**信頼性**、MODERATE), (**完全性**, HIGH), (**可用性**, HIGH)}となった。

FIPS 199 では、機密性・完全性・可用性のセキュリティ目標に関する情報システムの分類を低影響度、中影響度、高影響度と定めている。 ISA99 に従った ICS への影響に基づいたセキュリティレベル低・中・高の定義を表 6-1 に示す。生産物、産業及びセキュリティ関心事に基づいた ICS への影響レベルの定義を表 6-2 に示す。

表 6-1. ISA99 に基づく ICS 影響レベルの定義

影響度分類	低	中	高
負傷	応急処置を要する切り傷、打撲	入院が必要	生命・四肢の喪失
金銭的喪失	$1,000	$100,000	数百万
環境放出	一時的ダメージ	長期的ダメージ	永続的ダメージ、現場外のダメージ
生産中断	分	日	週
国民のイメージ	一時的ダメージ	長期的ダメージ	永続的ダメージ

Table 6-2. Possible Definitions for ICS Impact Levels Based on Product Produced, Industry and Security Concerns

Impact Category	Low-Impact	Moderate-Impact	High-Impact
Product Produced	· Non-hazardous materials or products · Non-ingested consumer products	· Some hazardous products or steps during production · High amount of proprietary information	· Critical infrastructure (e.g., electricity) · Hazardous materials · Ingested products
Industry Examples	· Plastic injection molding · Warehouse applications	· Automotive metal industries · Pulp and paper · Semiconductors	· Utilities · Petrochemical · Food and beverage · Pharmaceutical
Security Concerns	· Protection against minor injuries · Ensuring uptime	· Protection against moderate injuries · Ensuring uptime · Capital investment	· Protection against major injuries/loss of life · Ensuring uptime · Capital investment · Trade secrets · Ensuring basic social services · Regulatory compliance

6.1.2 Step 2: Select Security Controls

This framework activity includes the initial selection of minimum security controls planned or in place to protect the information system based on a set of requirements. FIPS 200 documents a set of minimum-security requirements covering 18 security-related areas with regard to protecting the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems [16]. Additional information on each of the 18 security control families is in Section 6.2.

The baseline controls are the starting point for the security control selection process and chosen based on the security category and associate impact level of information systems determined in Step 1.

To address the need for developing community-wide and specialized sets of security controls for information systems and organizations, the concept of ***overlays*** is introduced. An ***overlay*** is a fully specified set of security controls, control enhancements, and supplemental guidance derived from the application of tailoring guidance to security control baselines described in NIST SP 800-53.

In general, overlays are intended to reduce the need for ad hoc tailoring of baselines by organizations through the selection of a set of controls and control enhancements that more closely correspond to common circumstances, situations, and/or conditions. However, the use of overlays does not in any way preclude organizations from performing further tailoring (i.e., overlays can also be subject to tailoring) to reflect organization-specific needs, assumptions, or constraints. For further information on creating overlays, refer to SP 800-53, Section 3.3 and Appendix I.

Appendix G— includes an ICS-specific overlay of applicable NIST SP 800-53 controls that provide tailored baselines for low-impact, moderate-impact, and high-impact ICS. These tailored baselines can be utilized as starting specifications and recommendations that can be applied to specific ICS by responsible personnel. As discussed in earlier sections, the use of an overlay does not in any way preclude organizations from performing further tailoring to add or remove controls and control enhancements (i.e., overlays can also be subject to tailoring) to reflect organization-specific needs, assumptions, or constraints.

表 6-2. 生産物、産業及びセキュリティ関心事に基づく ICS への影響レベルの定義

カテゴリ	低	中	高
生産物	• 危険物・産物以外 • 非摂取型消費財	• 生産時にある程度の危険産物・手順 • 多量の専有情報	• 重要インフラ（電気等） • 危険物 • 摂取型産物
産業例	• プラスチック射出成形 • 倉庫アプリ	• 車両金属業界 • パルプ製紙 • 半導体	• 公共事業 • 石油化学 • 食品飲料 • 薬剤
セキュリティ関心事	• 軽傷予防 • 稼働確保	• 中程度の負傷予防 • 稼働確保 • 資本投資	• 重傷・死亡予防 • 稼働確保 • 資本投資 • 取引上の秘密 • 基本的社会福祉の確保 • 法令遵守

6.1.2 手順 2：セキュリティ対策の選択

この枠組での活動には、一連の要件に基づく情報システムを保護するための計画中又は実施中の最低限のセキュリティ対策の初期選択を行うことが含まれる。FIPS200 には、18 のセキュリティ関連分野を網羅した一連の最低セキュリティ要件が記録されており、連邦情報システムの機密性・完全性・可用性の保護や、これらシステムが処理・保管・送信する情報について取り上げられている[16]。18 のセキュリティ対策分野に関する付加的な情報はセクション 6.2 で取り上げる。

ベースライン制御は、セキュリティ対策選定プロセスの開始点となり、セキュリティ分類と手順 1 で判定された情報システムの影響度に基づいて選択される。

情報システム及び組織向けに、共同体全体の専用セキュリティ対策を策定する必要から、**オーバーレイ**概念が導入されている。**オーバーレイ**は、完全に特化したセキュリティ対策、管理拡張及び補足ガイダンスで、NIST SP 800-53 に記載されているセキュリティ対策ベースライン用ガイダンスから生じたものである。

一般にオーバーレイは、共通的な環境、状況・状態に緊密に対応した一連の制御・制御拡張を選択することで、組織によるその場しのぎのベースライン調整の必要性を減らすことが目的である。ただしオーバーレイを利用しても、組織固有の必要・前提・制約に対応するため、それ以上の調整が全く不要になるわけではない（つまりオーバーレイは調整可能）。オーバーレイの作成については、SP 800-53 のセクション 3.3 と付録 I を参照のこと。

付録 G には、付録 G には、低・中・高影響度 ICS に調整済みベースラインを示した、該当する NIST SP 800-53 制御の固有オーバーレイが含まれている。 これら調整済みベースラインは、責任者が固有の ICS に適用可能な当初の仕様書及び推奨事項として利用できる。前述の通り、オーバーレイを利用しても、組織固有の必要・前提・制約に対応するため、それ以上の調整を加えて、制御・制御拡張の追加・削除を行うような調整が全く不要になるわけではない（つまりオーバーレイは調整可能）。

Additionally, ICS owners can take advantage of the ability to tailor the initial baselines presented in the Appendix G— Overlay when it is not possible or feasible to implement specific security controls contained in the baselines. However, all tailoring activity should, as its primary goal, focus on meeting the intent of the original security controls whenever possible or feasible. For example, in situations where the ICS cannot support, or the organization determines it is not advisable to implement particular security controls or control enhancements in an ICS (e.g., performance, safety, or reliability are adversely impacted), the organization provides a complete and convincing rationale for how the selected compensating controls provide an equivalent security capability or level of protection for the ICS and why the related baseline security controls could not be employed. If the ICS cannot support the use of automated mechanisms, the organization employs non-automated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance in Section 3.3 of NIST SP 800-53. Compensating controls are not exceptions or waivers to the baseline controls; rather, they are alternative safeguards and countermeasures employed within the ICS that accomplish the intent of the original security controls that could not be effectively employed. Organizational decisions on the use of compensating controls are documented in the security plan for the ICS.

6.1.3 Step 3: Implement Security Controls

This activity involves the implementation of security controls in new or legacy information systems. The security control selection process described in this section can be applied to ICS from two different perspectives: (i) new development; and (ii) legacy.

For new development systems, the security control selection process is applied from a requirements definition perspective since the systems do not yet exist and organizations are conducting initial security categorizations. The security controls included in the security plans for the information systems serve as a security specification and are expected to be incorporated into the systems during the development and implementation phases of the system development life cycle.

In contrast, for legacy information systems, the security control selection process is applied from a gap analysis perspective when organizations are anticipating significant changes to the systems (e.g., during major upgrades, modifications, or outsourcing). Since the information systems already exist, organizations in all likelihood have completed the security categorization and security control selection processes resulting in the establishment of previously agreed-upon security controls in the respective security plans and the implementation of those controls within the information systems.

6.1.4 Step 4: Assess Security Controls

This activity determines the extent to which the security controls in the information system are effective in their application. NIST SP 800-53A provides guidance for assessing security controls initially selected from NIST SP 800-53 to ensure that they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system. To accomplish this, NIST SP 800-53A provides expectations based on assurance requirements defined in NIST SP 800-53 for characterizing the expectations of security assessments by FIPS 199 impact level.

6.1.5 Step 5: Authorize Information System

This activity results in a management decision to authorize the operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

また ICS 所有者は、ベースラインに含まれる特定のセキュリティ対策の実施が不可能の場合、付録 G のオーバーレイに示される当初ベースラインの調整機能を利用することができる。ただし全ての調整活動はその主たる目標として、可能な場合には必ず元々のセキュリティ対策の意図に従うようにすべきである。例えば、ICS が対応していない場合、又は特定のセキュリティ対策や管理拡張を ICS で実施するのが得策でないと判断する場合（パフォーマンス、安全性、信頼性が低下するなど）、組織は、代わりに選んだ管理策がどのように ICS に同等のセキュリティ能力や保護レベルを発揮するか、なぜベースラインセキュリティ対策を採用できないかについて、十分納得のいく根拠を示す。ICS が自動メカニズムの使用に対応していない場合、NIST SP 800-53 セクション 3.3.の一般的調整ガイダンスに従い、組織は非自動メカニズムや手順を代替管理として採用する。
代替管理はベースライン管理の例外や放棄ではなく、代替の安全策及び対策として ICS 内で採用され、有効利用できない元々のセキュリティ対策の目的を果たす。代替管理を利用する組織の決定は、ICS のセキュリティ計画書に記録する。

6.1.3 手順 3：セキュリティ対策の実装

この活動は、セキュリティ対策を新規又はレガシー情報システムに実装することが関係する。このセクションで説明するセキュリティ対策選定プロセスは、（1）新規開発、（2）レガシーという 2 つの観点から ICS に適用することができる。

新規開発システムでは、セキュリティ対策選定プロセスは、システムはまだ存在しておらず、組織は最初のセキュリティ分類を実施しつつあるため、要件定義の観点から適用される。情報システムのセキュリティ計画書に含まれたセキュリティ対策は、セキュリティ仕様書となるもので、システム開発ライフサイクル段階で、システムに組み込まれることが期待される。

対照的にレガシー情報システムでは、セキュリティ対策の選定プロセスは、組織がかなりのシステム変更を予期する場合（大がかりな更新、変更、外注等）、格差分析の観点から適用される。情報システムは既に存在しているため組織はあらゆる蓋然性においてセキュリティの分類とセキュリティ対策選定プロセスを実施済みであり、各セキュリティ計画書の中で合意済みのセキュリティ対策が策定され、それらが情報システムで実装されている。

6.1.4 手順 4：セキュリティ対策の評価

この活動は、情報システム中のセキュリティ対策が、それぞれの用途においてどれほど有効であるかを判定する。NIST SP 800-53A では、セキュリティ対策を適正に実装し、予定どおりに動作させ、システムのセキュリティ要件にかなった所期の結果を得るため、NIST SP 800-53 から選んだセキュリティ対策を評価するためのガイダンスが示されている。これを実現するため、NIST SP 800-53A には、FIPS199 の影響レベルに従ったセキュリティ評価予想を特徴付ける、NIST SP 800-53 で定義された保証要件に基づいた期待について記述されている。

6.1.5 手順 5：情報システムの許可

この活動の結果が経営陣の決定となり、情報システムの稼働を許可し、合意されたセキュリティ対策の実装を基調として、組織業務・資産・人員へのリスクを明示的に受け入れることになる。

6.1.6 Step 6: Monitor Security Controls

This activity continuously tracks changes to the information system that may affect security controls and assesses control effectiveness. NIST SP 800-137 provides guidance on information security continuous monitoring [21].

6.2 Guidance on the Application of Security Controls to ICS

Because today's ICS are often a combination of legacy systems, often with a planned life span of twenty to thirty years, or a hybrid of legacy systems augmented with newer hardware and software that are interconnected to other systems, it is often difficult or infeasible to apply some of the security controls contained in NIST SP 800-53. While many controls in Appendix F of NIST SP 800-53 are applicable to ICS as written, several controls did require ICS-specific interpretation and/or augmentation. Appendix I of NIST SP 800-53 provides an example overlay template and additional information on each section of the overlay.

The NIST SP 800-53 controls are organized into 18 families; each family contains security controls related to the general security topic of the family. Security controls may involve aspects of policy, oversight, supervision, manual processes, actions by individuals, or automated mechanisms implemented by information systems/devices. The 18 security-related areas discussed in the following sections are:

- **Access Control (AC):** the process of granting or denying specific requests for obtaining and using information and related information processing services for physical access to areas within the information system environment.
- **Awareness and Training (AT):** policies and procedures to ensure that all information system users are given appropriate security training relative to their usage of the system and that accurate training records are maintained.
- **Audit and Accountability (AU):** independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
- **Security Assessment and Authorization (CA):** assurance that the specified controls are implemented correctly, operating as intended, and producing the desired outcome.
- **Contingency Planning (CP):** policies and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
- **Configuration Management (CM):** policies and procedures for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation.
- **Identification and Authentication (IA):** the process of verifying the identity of a user, process, or device, through the use of specific credentials (e.g., passwords, tokens, biometrics), as a prerequisite for granting access to resources in an IT system.
- **Incident Response (IR):** policies and procedures pertaining to incident response training, testing, handling, monitoring, reporting, and support services.
- **Maintenance (MA):** policies and procedures to manage all maintenance aspects of an information system.

6.1.6 手順 6：セキュリティ対策の監視

この活動は、セキュリティ対策に影響する情報システムの変更を追跡し、管理の効果性を評価する。NIST SP 800-137 に、情報セキュリティの常続監視に係るガイダンスがある[21]。

6.2 ICS へのセキュリティ対策の適用に係るガイダンス

今日の ICS は、予想寿命が 20～30 年のレガシーシステム、他のシステムへ連接された比較的新しいハードウエア/ソフトウエアで強化されたレガシーシステムを併用しているため、NIST SP 800-53 のセキュリティ対策を適用するのは困難又は不可能な場合が多い。NIST SP 800-53 の付録 F に記載される管理策の多くは、記述どおり ICS に適用可能ではあるが、ICS 特有の解釈や補強が必要なものも少なくない。NIST SP 800-53 の付録 I には、オーバーレイテンプレートの例や、オーバーレイの各セクションに関する補足情報もある。

NIST SP 800-53 の管理策は 18 の分野にまとめられ、各分野はそれぞれの全般的セキュリティテーマに関係したセキュリティ対策について取り上げている。セキュリティ対策にはポリシー、指導、監督、手動プロセス、個人の行動、情報システム/デバイスが実装する自動メカニズムの様相が含まれよう。続くセクションで説明する 18 のセキュリティ関連分野は以下のとおり。

- **アクセス制御（AC）**：情報システム環境中のエリアに物理的にアクセスして、情報及び関連情報処理サービスを取得・利用するための明示的要求を許可するか拒絶するかというプロセス。
- **意識及び訓練（AT）**：全ての情報システムユーザがシステム利用に関する適正なセキュリティ訓練を受け、正確な訓練記録を保持するためのポリシー及び手順。
- **監査及び説明責任（AU）**：システム制御の妥当性を評価し、規定のポリシー及び業務手順を遵守させ、制御・ポリシー・手順に必要な変更を推奨するための記録及び活動に対する独立の審査・検証。
- **セキュリティ評価及び権限付与（CA）**：指定の制御を予定どおり正しく実行し、所期の結果を得るための保証。
- **不測事態計画（CP）**：緊急時・システム障害時・災害時に代替地などでコンピュータを操作するなど、業務を維持・復旧するためのポリシー及び手順。
- **構成管理（CM）**：ハードウエア・ファームウエア・ソフトウエア・文書への変更を管理し、システム実装前・中・後の不適切な改変から情報システムを保護するためのポリシー及び手順。
- **識別及び認証（IA）**：IT システム中のリソースへのアクセス許可の前提として、特定の認証情報（パスワード、トークン、バイオメトリクス等）によるユーザ・プロセス・デバイスの ID を検証するプロセス。
- **インシデント対応（IR）**：インシデント対応訓練・試験・処理・監視・報告・支援サービスに係るポリシー及び手順。
- **保守（MA）**：情報システムのあらゆる保守面を管理するためのポリシー及び手順。

- **Media Protection (MP):** policies and procedures to ensure secure handling of media. Controls cover access, labeling, storage, transport, sanitization, destruction, and disposal.
- **Physical and Environmental Protection (PE):** policies and procedures addressing physical, transmission, and display access control as well as environmental controls for conditioning (e.g., temperature, humidity) and emergency provisions (e.g., shutdown, power, lighting, fire protection).
- **Planning (PL):** development and maintenance of a plan to address information system security by performing assessments, specifying and implementing security controls, assigning security levels, and responding to incidents.
- **Personnel Security (PS):** policies and procedures for personnel position categorization, screening, transfer, penalty, and termination; also addresses third-party personnel security.
- **Risk Assessment (RA):** the process of identifying risks to operations, assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact.
- **System and Services Acquisition (SA):** allocation of resources for information system security to be maintained throughout the systems life cycle and the development of acquisition policies based on risk assessment results including requirements, design criteria, test procedures, and associated documentation.
- **System and Communications Protection (SC):** mechanisms for protecting both system and data transmission components.
- **System and Information Integrity (SI):** policies and procedures to protect information systems and their data from design flaws and data modification using functionality verification, data integrity checking, intrusion detection, malicious code detection, and security alert and advisory controls.
- **Program Management (PM):** provides security controls at the organizational rather than the information-system level.

Additionally, Appendix J of NIST SP 800-53 Rev. 4 includes a catalog of Privacy Controls. Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of personally identifiable information (PII).[35] The 8 privacy control families are each aligned with the Fair Information Practice Principles (FIPPS),[36] which are designed to build public trust in an organization's privacy practices and to help organizations avoid tangible costs and intangible damages stemming from privacy incidents.

[35] OMB Memorandum 07-16 defines PII as "information which can be used to distinguish or trace an individual's identity such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." [86]. OMB Memorandum 10-22 reaffirmed this definition [87]. NIST Special Publication 800-122 defines PII as "any information about an individual [that is] maintained by an agency, including: (i) any information that can be used to distinguish or trace an individual 's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information" [88].

[36] The FIPPs are widely accepted in the United States and internationally as a general framework for privacy and are reflected in other federal and international laws and policies. In a number of organizations, FIPPs serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies. The Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP) also provided information and materials in development of the privacy controls [89].

- **メデイア保護（MP）**：メデイアのセキュアな取扱いを行うためのポリシー及び手順。管理策は、アクセス・ラベル・ストレージ・輸送・サニタイズ・破棄・廃棄を対象とする。
- **物理環境上の保護（PE）**：調節（温度、湿度等）及び緊急装置（切断、電力、照明、防火等）の物理的、送信、表示アクセス制御及び環境制御に関するポリシー及び手順。
- **プランニング（PL）。**評価の実施、セキュリティ管理の指定・実施、セキュリティレベルの割当及びインシデント対応による、情報システムセキュリティに関する計画書の作成・維持。
- **人員のセキュリティ（PS）**：人員の配置分類、選抜、転属、罰則及び終了に関するポリシー及び手順で、サードパーティ職員のセキュリティも含める。
- **リスク評価（RA）**：発生確率、その影響、影響を緩和するための付加的セキュリティ対策の判定を通じた業務・資産・人員に対するリスク識別プロセス。
- **システム及びサービスの取得（SA）**：システムのライフサイクル期間を通じて維持すべき情報システムセキュリティに対するリソース割当と、要件・設計基準・試験手順・関連文書を含めたリスク評価結果に基づく取得ポリシー策定。
- **システム及び通信保護（SC）**：システムとデータ送信コンポーネントとを保護するためのメカニズム。
- **システム及び情報の保全（SI）**：機能検証・データ保全チェック・侵入検知・悪質コード検知・セキュリティアラート勧告管理を使用し、設計の欠陥やデータ改変から情報システムやデータを保護するためのポリシー及び手順。
- **プログラム管理（PM）**：情報システムレベルではなく組織レベルでのセキュリティ対策を行う。

以上に加えて、NIST SP 800-53 改訂第 4 版の付録 J にはプライバシー管理策のカタログが掲載されている。プライバシー管理策は、個人を特定可能な情報（PII）に対する保護と適正な取扱を確保するために組織内で採用される管理上の技術的・物理的安全対策である。[37]プライバシー管理の 8 分野がそれぞれ公正情報規範原則（FIPPS）に整合しており、[38]組織のプライバシー規範に対する国民の信頼を醸成し、プライバシーインシデントから生じる有形の経費や無形の損害の回避を目指している。

---

[37] OMB 覚書 07-16 は PII を「氏名、社会保障番号、バイオメトリック記録等を単独で、又は誕生日、出生地、母親の旧姓等特定の個人に結びつくか結びつけられるその他の個人若しくはは身分情報と組み合わせて、個人の身分を判別又は追跡できる情報」と定義している[86]。OMB 覚書 10-22 はこの定義を追認している[87]。NIST SP800-122 は PII を「ある機関が保持している個人に関する情報で、(1) 氏名、社会保障番号、誕生日、出生地、母親の旧姓、バイオメトリック記録等、個人の身分を判別又は追跡できる情報及び (2) 医療、教育、財政、就業情報等、個人に結びつくか結びつけられるその他の情報」と定義している[88]。

[38] FIPPs は、一般的なプライバシー基盤として、米国でも世界的にも広く受け入れられており、他の連邦及び世界的法律やポリシーに反映されている。FIPPs は、多くの組織でプライバシーリスクの分析や適切な緩和策判定時の根拠となっている。連邦企業アーキテクチャセキュリティプライバシープロファイル（FEA-SPP）にもプライバシー管理を策定するための情報や資料が示されている[89]。

Sections 6.2.1 through 6.2.19 introduce each of the SP 800-53 control families and privacy controls, provide background information on the control family, as well as any ICS guidance and implementation considerations for ICS owners. ICS-specific recommendations and guidance, if available, is provided in an outlined box for each section. Much of the ICS-specific guidance was derived from ISA-62443 [34] and the EPRI report: *Supervisory Control and Data Acquisition (SCADA) Systems Security Guide* [62].

6.2.1 Access Control

The security controls that fall within the NIST SP 800-53 Access Control (AC) family provide policies and procedures for specifying the use of system resources by only authorized users, programs, processes, or other systems. This family specifies controls for managing information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Controls cover access and flow enforcement issues such as separation of duties, least privilege, unsuccessful login attempts, system use notification, previous logon notification, concurrent session control, session lock, and session termination. There are also controls to address the use of portable and remote devices and personally owned information systems to access the information system as well as the use of remote access capabilities and the implementation of wireless technologies. Access can take several forms, including viewing, using, and altering specific data or device functions.

Supplemental guidance for the AC controls can be found in the following documents:

- NIST SP 800-63 provides guidance on remote electronic authentication [53].
- NIST SP 800-48 provides guidance on wireless network security with particular emphasis on the IEEE 802.11b and Bluetooth standards 0.
- NIST SP 800-97 provides guidance on IEEE 802.11i wireless network security [64].
- FIPS 201 provides requirements for the personal identity verification of federal employees and contractors [65].
- NIST SP 800-96 provides guidance on PIV card to reader interoperability [66].
- NIST SP 800-73 provides guidance on interfaces for personal identity verification [49].
- NIST SP 800-76 provides guidance on biometrics for personal identity verification [50].
- NIST SP 800-78 provides guidance on cryptographic algorithms and key sizes for personal identity verification [67].

If the new federal Personal Identity Verification (PIV) is used as an identification token, the access control system should conform to the requirements of FIPS 201 and NIST SP 800-73 and employ either cryptographic verification or biometric verification. When token-based access control employs cryptographic verification, the access control system should conform to the requirements of NIST SP 800-78. When token-based access control employs biometric verification, the access control system should conform to the requirements of NIST SP 800-76.

Access control technologies are filter and blocking technologies designed to direct and regulate the flow of information between devices or systems once authorization has been determined. The following sections present several access control technologies and their use with ICS.

セクション 6.2.1～6.2.19 では、SP 800-53 のそれぞれの管理分野とプライバシー管理が示され、制御分野の背景情報のほか、ICS 所有者向けの ICS ガイダンスと実装上の考慮事項が説明されている。ICS 固有の推奨事項とガイダンスが利用可能な場合は、各セクションの囲みに示される。ICS 固有のガイダンスは大半が ISA-62443 [34]と EPRI 報告書『SCADA システムセキュリティガイド』[62]を基にしている。

6.2.1 アクセス制御

NIST SP 800-53 のアクセス制御（AC）ファミリに関するセキュリティ対策には、許可されたユーザ、プログラム、プロセスその他システムのみによるシステムリソースの利用について規定するためのポリシー及び手順が示されている。このファミリは、アカウントの設定・使用開始・変更・見直し・使用禁止・削除等、情報システムのアカウントを管理するための方法を規定する。管理策は、任務の切り分け、最低特権、ログインの失敗、システム利用通知、以前のログオン通知、並行セッション管理、セッションロック、セッション終了等、アクセスとフローの実行問題を網羅している。またポータブルデバイス、遠隔デバイス及び個人保有の情報システムによる情報システムへのアクセスのほか、リモートアクセス機能やワイヤレス技術の実装に関する管理策も取り上げている。アクセスには閲覧、使用、特定データやデバイス機能の変更といったいくつかの形態がある。

AC 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-63：遠隔電子認証に係るガイダンス[53]
- NIST SP 800-48：IEEE 802.11b 及び Bluetooth 規格 0 を重点としたワイヤレスネットワークセキュリティに係るガイダンス
- NIST SP 800-97：IEEE 802.11i ワイヤレスネットワークセキュリティに係るガイダンス[64]
- FIPS 201：連邦職員及び契約従業員の個人身元確認に係る要件[65]
- NIST SP 800-96：PIV カードとリーダーの相互運用に係るガイダンス[66]
- NIST SP 800-73：個人身元確認インタフェースに係るガイダンス[49]
- NIST SP 800-76：個人身元確認バイオメトリクスに係るガイダンス[50]
- NIST SP 800-78：個人身元確認の暗号アルゴリズム及びキーサイズに係るガイダンス[67]

新しい連邦個人身元確認（PIV）を識別トークンとして使用している場合、アクセス制御システムは FIPS 201 及び NIST SP 800-73 の要件に従い、暗号確認又はバイオメトリック確認を採用すべきである。トークンベースのアクセス制御が暗号確認を採用している場合、アクセス制御システムは NIST SP 800-78 の要件に従うべきである。トークンベースのアクセス制御がバイオメトリック確認を採用している場合、アクセス制御システムは NIST SP 800-76 の要件に従うべきである。

アクセス制御技術は、権限付与の確定後に、デバイス間又はシステム間での情報の流れを規制するためのフィルタとブロック技術である。続くセクションでは、いくつかのアクセス制御技術と ICS での使用について示す。

6.2.1.1 Role-based Access Control (RBAC)

RBAC is a technology that has the potential to reduce the complexity and cost of security administration in networks with large numbers of intelligent devices. Under RBAC, security administration is simplified through the use of roles, hierarchies, and constraints to organize user access levels. RBAC reduces costs within an organization because it accepts that employees change roles and responsibilities more frequently than the duties within roles and responsibilities.

ICS-specific Recommendations and Guidance

RBAC can be used to provide a uniform means to manage access to ICS devices while reducing the cost of maintaining individual device access levels and minimizing errors. RBAC should be used to restrict ICS user privileges to only those that are required to perform each person's job (i.e., configuring each role based on the principle of least privilege). The level of access can take several forms, including viewing, using, and altering specific ICS data or device functions.

RBAC tools can set, modify, or remove authorizations in applications, but they do not replace the authorization mechanism; they do not check and authenticate users every time a user wants to access an application. RBAC tools offer interfaces to authorization mechanisms for most current platforms in the IT arena. However, legacy ICS systems or specialized ICS equipment may require development of specialized interface software. This issue is a large problem for ICS that use a number of proprietary operating systems or customized operating system implementations and interfaces.

6.2.1.1 役割に基づくアクセス制御（RBAC）

RBAC は、多数のインテリジェンスデバイスを使用したネットワークの複雑さとセキュリティ対策コストを減らせる技術である。RBAC の下では、役割、階層及びユーザアクセスレベル管理の制約を利用して、セキュリティ対策が簡素化される。RBAC では、従業員の役割・責任内での任務変更よりも、役割・責任の変更をより頻繁に受け入れるので、組織内のコストが減る。

ICS 固有の推奨事項及びガイダンス

RBAC を利用すれば、個々のデバイスアクセスレベルの維持に要するコストを減らし、エラーを最小限に抑えつつ、ICS デバイスへの一様のアクセス管理手段を提供できる。ICS ユーザ権限の付与を業務上必要とする人員に限定するために RBAC を利用すべきである（最小権限原則に基づく役割構成）。アクセスレベルには閲覧、使用、特定 ICS データやデバイス機能の変更といったいくつかの形態がある。

RBAC ツールは、アプリケーションにおける権限付与を設定・変更・削除できるが、権限付与メカニズムの代行はしない。つまり、ユーザがアプリケーションへのアクセスを求めるたびに、チェックや認証を行うことはない。RBAC ツールは、IT 分野におけるほとんどの現行プラットホーム向けに、権限付与メカニズムのインタフェースを提供している。ただしレガシーICS システムや特殊 ICS 装備品には、特殊インタフェースソフトウエアの開発が必要となる場合がある。この問題は、多数の独自 OS やカスタム OS の実装及びインタフェースを利用している ICS で大きな問題となる。

6.2.1.2 Web Servers

Web and Internet technologies are being added to a wide variety of ICS products because they make information more accessible and products more user-friendly and easier to configure remotely. However, they may also add cyber risks and create new security vulnerabilities that need to be addressed.

ICS-specific Recommendations and Guidance

SCADA and historian software vendors typically provide Web servers as a product option so that users outside the control room can access ICS information. In many cases, software components such as ActiveX controls or Java applets must be installed or downloaded onto each client machine accessing the Web server. Some products, such as PLCs and other control devices, are available with embedded Web, FTP, and email servers to make them easier to configure remotely and allow them to generate email notifications and reports when certain conditions occur. When feasible, use HTTPS rather than HTTP, use SFTP or SCP rather than FTP, block inbound FTP and email traffic, etc. Security appliances (or gateways) are beginning to appear with application proxies able to examine Web, FTP, and email traffic to block attacks and prevent downloading of ActiveX® controls or Java® applets.
Unless there is substantial benefit to connecting ICSs to the Internet, the systems are best left not connected.

6.2.1.3 Virtual Local Area Network (VLAN)

VLANs divide physical networks into smaller logical networks to increase performance, improve manageability, and simplify network design. VLANs are achieved through configuration of Ethernet switches. Each VLAN consists of a single broadcast domain that isolates traffic from other VLANs. Just as replacing hubs with switches reduces collisions, using VLANs limits the broadcast traffic, as well as allowing logical subnets to span multiple physical locations. There are two categories of VLANs:

- Static, often referred to as port-based, where switch ports are assigned to a VLAN so that it is transparent to the end user.
- Dynamic, where an end device negotiates VLAN characteristics with the switch or determines the VLAN based on the IP or hardware addresses.

Although more than one IP subnet may coexist on the same VLAN, the general recommendation is to use a one-to-one relationship between subnets and VLANs. This practice requires the use of a router or multi-layer switch to join multiple VLANs. Many routers and firewalls support tagged frames so that a single physical interface can be used to route between multiple logical networks.

VLANs are not typically deployed to address host or network vulnerabilities in the way that firewalls or IDS are deployed. However, when properly configured, VLANs do allow switches to enforce security policies and segregate traffic at the Ethernet layer. Properly segmented networks can also mitigate the risks of broadcast storms that may result from port scanning or worm activity.

Switches have been susceptible to attacks such as MAC spoofing, table overflows, and attacks against the spanning tree protocols, depending on the device and its configuration. VLAN hopping, the ability for an attack to inject frames to unauthorized ports, has been demonstrated using switch spoofing or double-encapsulated frames. These attacks cannot be conducted remotely and require local physical access to the switch. A variety of features such as MAC address filtering, port-based authentication using IEEE 802.1*x*,

6.2.1.2 ウェブサーバ

ウェブ技術及びインターネット技術は、情報へのアクセスが便利になり、ユーザにとって製品が使いやすくなり、遠隔設定が容易になるため、多種多様な ICS 製品に追加されるようになっている。しかしサイバーリスクも高まり、新たなセキュリティ上の脆弱性が生じ、対応が必要となる。

ICS 固有の推奨事項及びガイダンス

SCADA やヒストリアンソフトウエアのベンダーは、通常、ウェブサーバを製品オプションの 1 つとして提供し、制御室の外にいるユーザが ICS 情報にアクセスできるようにしている。多くの場合、ActiveX コントロールや Java アプレットといったソフトウエアコンポーネントを、ウェブサーバにアクセスするクライアントマシンにインストール又はダウンロードしなければならない。PLC その他の制御デバイス等の製品には、ウェブサーバ、FTP サーバ及び電子メールサーバが組み込まれており、遠隔設定が容易で、特定の事態が生じた場合には、電子メール通知やレポートを生成できるようになっている。可能であれば HTTP ではなく HTTPS を、FTP ではなく SFTP 又は SCP を使用し、着信 FTP や電子メールトラフィック等はブロックする。ウェブ、FTP 及び電子メールトラフィックを検査して、攻撃をブロックし、ActiveX®コントロールや Java® アプレットのダウンロードを防止できるセキュリティ装置（又はゲートウェイ）の付いたアプリケーションプロキシが出始めている。
ICS をインターネット接続することの相当の利益がないかぎり、システムを非接続とするのが最善である。

6.2.1.3 仮想 LAN（VLAN）

VLAN は、物理ネットワークをより小さな論理ネットワークに分割し、パフォーマンスと管理性を改善し、ネットワーク設計を簡素化する。VLAN は Ethernet スイッチの設定により実現する。各 VLAN は、トラフィックを他の VLAN から隔離する単一のブロードキャスト領域で構成される。ハブをスイッチに代えると競合が減るように、VLAN を使用すればブロードキャストトラフィックが制限され、論理サブネットが複数の物理的な場所にまたがるようにできる。VLAN には次の 2 種類がある。

- 静的 VLAN：ポートベースと呼ばれることが多く、スイッチポートが VLAN に割り当てられ、エンドユーザに透過である。
- 動的 VLAN：エンドデバイスがスイッチと VLAN 特性についてネゴシエートするか、IP アドレス又はハードウエアアドレスに基づいて VLAN を判定する。

複数の IP サブネットが同じ VLAN 上に共存するが、サブネットと VLAN 間で一対一の関係を利用することが一般的に推奨される。この規範には、複数 VLAN に荷担するためのルータ又はマルチレイヤースイッチが必須となる。ルータやファイアウォールの多くは、タグ付きフレームに対応しており、1 つの物理インタフェースを利用して、複数の論理ネットワーク間で経路指定することができる。

VLAN は、ファイアウォールや IDS と同じような展開方法で、ホストやネットワークの脆弱性に対処するために展開されることはあまりない。しかし正しく設定すると、VLAN はスイッチが接続ポリシーを施行し、トラフィックを Ethernet 層で分離することができる。しっかり分離されたネットワークは、ポートスキャニングやワームにより生じるブロードキャストストームのリスクを緩和できる。

スイッチは、デバイスとその設定に応じて、MAC 偽装、テーブルオーバーフロー、スパニングツリープロトコル攻撃等の攻撃に弱い。攻撃側がフレームを未許可ポートに注入する VLAN ホッピングは、スイッチ偽装や二重カプセルフレームを使用することが分かっている。このような攻撃は遠隔操作ができず、スイッチへのローカルの物理アクセスが必要となる。MAC アドレスフィルタリング、IEEE 802.1*x* を利用したポートベースの認証等の多様な機能や、

and specific vendor recommended practices can be used to mitigate these attacks, depending on the device and implementation.

ICS-specific Recommendations and Guidance

VLANs have been effectively deployed in ICS networks, with each automation cell assigned to a single VLAN to limit unnecessary traffic flooding and allow network devices on the same VLAN to span multiple switches [34].

6.2.1.4 Dial-up Modems

ICS systems have stringent reliability and availability requirements. When there is a need to troubleshoot and repair, the technical resources may not be physically located at the control room or facility. Therefore, ICS often use modems to enable vendors, system integrators, or control engineers maintaining the system to dial in and diagnose, repair, configure, and perform maintenance on the network or component. While this allows easy access for authorized personnel, if the dial-up modems are not properly secured, they can also provide backdoor entries for unauthorized use.
Dial-up often uses remote control software that gives the remote user powerful (administrative or root) access to the target system. Such software usually has security options that should be carefully reviewed and configured.

ICS-specific Recommendations and Guidance

- Consider using callback systems when dial-up modems are installed in an ICS. This ensures that a dialer is an authorized user by having the modem establish the working connection based on the dialer's information and a callback number stored in the ICS approved authorized user list.
- Ensure that default passwords have been changed and strong passwords are in place for each modem.
- Physically identify modems in use to the control room operators.
- Configure remote control software to use unique user names and passwords, strong authentication, encryption if determined appropriate, and audit logs. Use of this software by remote users should be monitored on an almost real-time frequency.
- If feasible, disconnect modems when not in use or consider automating this disconnection process by having modems disconnect after being on for a given amount of time. It should be noted that sometimes modem connections are part of the legal support service agreement with the vendor (e.g., 24x7 support with 15 minute response time). Personnel should be aware that disconnecting/removing the modems may require that contracts be renegotiated.

ベンダーが推奨する特定の規範を利用して、デバイスや実装に応じて、こうした攻撃を緩和できる。

ICS 固有の推奨事項及びガイダンス

VLAN は ICS ネットワークに有効に展開されており、各オートメーションセルを 1 つの VLAN に割り当てて不要なトラフィックの洪水を制限し、同じ VLAN 上のネットワークデバイスが複数スイッチにまたがるようにしている[34]。

6.2.1.4 ダイアルアップモデム

ICS システムの信頼性及び可用性には厳格な要件が課される。トラブルシューティングや修理が必要となる場合、制御室や制御施設に技術リソースが物理的に存在しないこともある。よって ICS では、システム保守を担当するベンダー、システムインテグレータ又は制御エンジニアがモデムを使用してダイアルインし、ネットワークや構成の診断、修理、設定及び保守を行えるようにすることが多い。そうすることで権限を与えられた職員のアクセスが容易になる反面、ダイアルアップモデムのセキュリティがしっかり確保されていないと、不正使用をもくろむバックドア侵入を許すことにもなりかねない。

ダイアルアップでは、遠隔ユーザに目標システムへの上位（管理者又は root）アクセス権を与える遠隔制御ソフトウエアを使用することが多い。通常このようなソフトウエアには、慎重に精査して設定すべきセキュリティオプションが付いている。

ICS 固有の推奨事項及びガイダンス

- ICS にダイアルアップモデムが設置されている場合、コールバックシステムの利用を検討する。これを利用すると、モデムは ICS が認可した認定ユーザリストに保存されている発呼者情報とコールバック番号を基に有効な接続を確立するため、発呼者は確実に認定ユーザとなる。
- モデムごとに必ずデフォルトのパスワードを変更し、強力なパスワードを設定する。
- 使用中の各モデムが制御室オペレータに物理的に識別できるようにする。
- 遠隔制御ソフトウエアを設定し、一意のユーザ名とパスワード、強力な認証、必要であれば暗号化、監査ログを使用できるようにする。遠隔ユーザによる本ソフトウエアの使用を、ほぼリアルタイムで監視すべきである。
- 可能であれば不使用時にはモデムを切断するか、一定時間オンになっている場合にはオフにするような切断プロセスの自動化を検討する。モデム接続は、ベンダーとの法的なサポートサービス契約の一部に含まれている場合もある点を銘記すべきである（15 分対応での年中無休サポートなど）。職員は、モデムの切断や撤去を行うには、契約上協議が必要となることを認識すべきである。

6.2.1.5 Wireless

The use of wireless within an ICS is a risk-based decision that has to be determined by the organization. Generally, wireless LANs should only be deployed where health, safety, environmental, and financial implications are low. NIST SP 800-48 and SP 800-97 provide guidance on wireless network security.

ICS-specific Recommendations and Guidance
Wireless LANs

- Prior to installation, a wireless survey should be performed to determine antenna location and strength to minimize exposure of the wireless network. The survey should take into account the fact that attackers can use powerful directional antennas, which extend the effective range of a wireless LAN beyond the expected standard range. Faraday cages and other methods are also available to minimize exposure of the wireless network outside of the designated areas.
- Wireless users' access should utilize IEEE 802.1*x* authentication using a secure authentication protocol (e.g., Extensible Authentication Protocol [EAP] with TLS [EAP-TLS]) that authenticates users via a user certificates or a Remote Authentication Dial In User Service (RADIUS) server.
- The wireless access points and data servers for wireless worker devices should be located on an isolated network with documented and minimal (single if possible) connections to the ICS network.
- Wireless access points should be configured to have a unique service set identifier (SSID), disable SSID broadcast, and enable MAC filtering at a minimum.
- Wireless devices, if being utilized in a Microsoft Windows ICS network, should be configured into a separate organizational unit of the Windows domain.
- Wireless device communications should be encrypted and integrity-protected. The encryption must not degrade the operational performance of the end device. Encryption at OSI Layer 2 should be considered, rather than at Layer 3 to reduce encryption latency. The use of hardware accelerators to perform cryptographic functions should also be considered.

For mesh networks, consider the use of broadcast key versus public key management implemented at OSI Layer 2 to maximize performance. Asymmetric cryptography should be used to perform administrative functions, and symmetric encryption should be used to secure each data stream as well as network control traffic. An adaptive routing protocol should be considered if the devices are to be used for wireless mobility. The convergence time of the network should be as fast as possible supporting rapid network recovery in the event of a failure or power loss. The use of a mesh network may provide fault tolerance thru alternate route selection and pre-emptive fail-over of the network.

Wireless field networks

The ISA100[39] Committee is working to establish standards, recommended practices, technical reports, and related information that will define procedures for implementing wireless systems in the automation and control environment with a focus on the field level (e.g., IEEE 802.15.4). Guidance is directed towards those responsible for the complete life cycle including the designing, implementing, on-going maintenance, scalability or managing industrial automation and control systems, and applies to users, system integrators, practitioners, and control systems manufacturers and vendors.

[39] Additional information on ISA100 at: http://www.isa.org/isa100.

6.2.1.5　ワイヤレス

ICS 内でのワイヤレスの利用は、リスクに基づく決定事項であり、組織が決定しなければならない。一般にワイヤレス LAN は、健康・安全・環境・財政上の制約が少ない場合にのみ展開すべきである。NIST SP 800-48 及び SP 800-97 には、ワイヤレスネットワーク接続に係るガイダンスがある。

ワイヤレス LAN に係る ICS 固有の推奨事項及びガイダンス

- 設置前に無線状態を調査し、アンテナ位置と強度を判定し、ワイヤレスネットワークの露出度を最小限にする。攻撃側が利用する強力指向性アンテナは、ワイヤレス LAN の有効距離を、標準的な予想距離を超えて延伸できることを念頭に置いて調査を行うべきである。ファラデー箱その他の手段も利用して、所期のエリア外にはみ出るワイヤレスネットワークの露出度を最小に抑える。
- ワイヤレスユーザのアクセスは、ユーザ証明書又は遠隔認証ダイアルインユーザサービス（RADIUS）サーバを介してユーザ認証を行う、セキュアなプロトコル（TLS 付き拡張認証プロトコル[EAP-TLS]等）を使用した IEEE802.1*x* 認証を利用すべきである。
- ワイヤレスアクセスポイント及びワイヤレスワーカデバイス用データサーバは、ICS ネットワーク接続を最小限にし（できれば 1 つのみ）、文書化された隔絶ネットワーク上に置くべきである。
- ワイヤレスアクセスポイントは、サービスセット識別子（SSID）を一意にし、SSID ブロードキャストを使用禁止、最小限の MAC フィルタリングを使用可能に設定すべきである。
- ワイヤレスデバイスを Microsoft Windows ICS ネットワークで使用する場合、Windows 領域の別の組織ユニットに設定すべきである。
- ワイヤレスデバイス通信は、暗号化して保全すべきである。暗号化により、エンドデバイスの動作パフォーマンスが低下してはならない。暗号化の待ち時間を短縮するため、OSI レイヤー3 ではなくレイヤー2 での暗号化を考慮すべきである。また暗号関数を実行するハードウエア加速器の利用も考慮すべきである。

メッシュネットワークでは、パフォーマンスを最大に上げるため、OSI レイヤー2 に実装されるブロードキャストキー対公開鍵管理の使用を検討する。非対称暗号を利用して管理機能を実施し、対称暗号を利用して各データストリームとネットワーク制御トラフィックのセキュリティを確保すべきである。デバイスをワイヤレス移動目的で使用する場合は、最適経路指定プロトコルの利用を考慮すべきである。障害時や電力喪失時のネットワーク回復を早めるため、ネットワークの収束時間はできるだけ短くすべきである。メッシュネットワークを使用することで、代替経路選定と先行的フェイルオーバーを通じて、フォールトトレランスが得られよう。

ワイヤレスフィールドネットワーク

フィールドレベル（IEEE 802.15.4 等）に特化したオートメーション及び制御環境におけるワイヤレスシステムの手順を定めるため、ISA 100[40]委員会は規格、推奨規範、技術レポート及び関連情報の策定に向けて作業中である。産業オートメーション及び制御システムの設計、実装、保守、スケーラビリティ、管理等のライフサイクル担当者向けにガイダンスが提示されており、ユーザ、システムインテグレータ、実施担当者及び制御システムのメーカー/ベンダーに適用される。

40　ISA100 に関する追加情報が次の URL にある。http://www.isa.org/isa100.

6.2.2 Awareness and Training

The security controls that fall within the NIST SP 800-53 Awareness and Training (AT) family provide policy and procedures for ensuring that all users of an information system are provided basic information system security awareness and training materials before authorization to access the system is granted. Personnel training must be monitored and documented.

Supplemental guidance for the AT controls can be found in the following documents:

- NIST SP 800-50 provides guidance on security awareness training [61].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

ICS-specific Recommendations and Guidance

For the ICS environment, this must include control system-specific information security awareness and training for specific ICS applications. In addition, an organization must identify, document, and train all personnel having significant ICS roles and responsibilities. Awareness and training must cover the physical process being controlled as well as the ICS.

Security awareness is a critical part of ICS incident prevention, particularly when it comes to social engineering threats. Social engineering is a technique used to manipulate individuals into giving away private information, such as passwords. This information can then be used to compromise otherwise secure systems.

Implementing an ICS security program may bring changes to the way in which personnel access computer programs, applications, and the computer desktop itself. Organizations should design effective training programs and communication vehicles to help employees understand why new access and control methods are required, ideas they can use to reduce risks, and the impact on the organization if control methods are not incorporated. Training programs also demonstrate management's commitment to, and the value of, a cybersecurity program. Feedback from staff exposed to this type of training can be a valuable source of input for refining the charter and scope of the security program.

6.2.3 Audit and Accountability

An audit is an independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. The security controls that fall within the NIST SP 800-53 Audit and Accountability (AU) family provide policies and procedures for generating audit records, their content, capacity, and retention requirements. The controls also provide safeguards to react to problems such as an audit failure or audit log capacity being reached. Audit data should be protected from modification and be designed with non-repudiation capability.

Supplemental guidance for the AU controls can be found in the following documents:

- NIST SP 800-61 provides guidance on computer security incident handling and audit log retention [59].

6.2.2 意識及び訓練

NIST SP 800-53 の意識及び訓練（AT）ファミリに含まれるセキュリティ対策には、システムへのアクセス権限を付与する前に、情報システムの全ユーザに基本的なシステムセキュリティに対する意識・訓練資料が行き渡るようにするためのポリシー及び手順が定められている。訓練は監視と文書化が求められる。

AT 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-50：セキュリティ意識訓練に係るガイダンス[61]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

ICS 固有の推奨事項及びガイダンス

ICS 環境では、特定の ICS 用途に関する制御システム固有の情報セキュリティ意識・訓練を含めなければならない。また組織は、ICS に大きな役割と責任を有している職員全てを特定し、記録し、訓練しなければならない。意識・訓練は、制御される物理的プロセスと ICS について取り上げなければならない。

セキュリティ意識は、ICS インシデントの予防、特にソーシャルエンジニアリング脅威に関して、ICS の肝要な一部である。ソーシャルエンジニアリングとは、個人を操作してパスワード等の個人情報を引き出す技術のことである。引き出した情報を利用して、システムのセキュリティを低下させることができる。

ICS セキュリティプログラムを実施することで、職員によるコンピュータプログラム、アプリケーション及びコンピュータデスクトップそのものの利用方法を変えることができる。組織は効果的な訓練プログラムと伝達手段を考案して、新たなアクセス・管理要領が必要な理由、リスクを減らすためのアイディア、管理要領が守られない場合の組織への影響について従業員が理解できるようにすべきである。また訓練プログラムでは、サイバーセキュリティプログラムに対する経営陣の強い関心と、プログラムの価値を実証する。被訓練者からのフィードバックは、セキュリティプログラムの憲章及び適用範囲を改善するための貴重な資となる。

6.2.3 監査及び説明責任

監査はシステム制御の妥当性を評価し、規定のポリシー及び業務手順を遵守させ、制御・ポリシー・手順に必要な変更を推奨するための記録及び活動に対する独立の審査・検証である。NIST SP 800-53 の監査及び説明責任（AU）ファミリに含まれるセキュリティ対策では、監査記録、内容、能力及び保持要件に係るポリシー及び手順を定めている。また監査の不備や監査記録能力が限界に達した際の問題に対処するための対策も定められていいる。監査データは改変できないように保護し、否認不能のものとして策定すべきである。

AU 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-61：コンピュータセキュリティインシデントの処理及び監査記録の保持に係るガイダンス[59]

- NIST SP 800-92 provides guidance on log management (including audit logs) [68].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

ICS-specific Recommendations and Guidance

It is necessary to determine that the system is performing as intended. Periodic audits of the ICS should be performed to validate the following items:

- The security controls present during system validation testing (e.g., factory acceptance testing and site acceptance testing) are still installed and operating correctly in the production system.
- The production system is free from security compromises and provides information on the nature and extent of compromises as feasible, should they occur.
- The management of change program is being rigorously followed with an audit trail of reviews and approvals for all changes.

The results from each periodic audit should be expressed in the form of performance against a set of predefined and appropriate metrics to display security performance and security trends. Security performance metrics should be sent to the appropriate stakeholders, along with a view of security performance trends.

Traditionally, the primary basis for audit in IT systems has been recordkeeping. Using appropriate tools within an ICS environment requires extensive knowledge from an IT professional familiar with the ICS, critical production and safety implications for the facility. Many of the process control devices that are integrated into the ICS have been installed for many years and do not have the capability to provide the audit records described in this section. Therefore, the applicability of these more modern tools for auditing system and network activity is dependent upon the capabilities of the components in the ICS.

The critical tasks in managing a network in an ICS environment are ensuring reliability and availability to support safe and efficient operation. In regulated industries, regulatory compliance can add complexity to security and authentication management, registry and installation integrity management, and all functions that can augment an installation and operational qualification exercise. Diligent use of auditing and log management tools can provide valuable assistance in maintaining and proving the integrity of the ICS from installation through the system life cycle. The value of these tools in this environment can be calculated by the effort required to re-qualify or otherwise retest the ICS where the integrity due to attack, accident, or error is in question. The system should provide reliable, synchronized time stamps in support of the audit tools.

Monitoring of sensors, logs, Intrusion Detection Systems (IDS), antivirus, patch management, policy management software, and other security mechanisms should be done on a real-time basis where feasible. A first-line monitoring service would receive alarms, do rapid initial problem determination and take action to alert appropriate facility personnel to intervene.

System auditing utilities should be incorporated into new and existing ICS projects. These auditing utilities should be tested (e.g., off-line on a comparable ICS) before being deployed on an operational ICS. These tools can provide tangible records of evidence and system integrity. Additionally, active log management utilities may actually flag an attack or event in progress and provide location and tracing information to help respond to the incident [34].

- NIST SP 800-92：記録管理（監査記録を含む）に係るガイダンス[68]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

ICS 固有の推奨事項及びガイダンス

システムが予定どおりに稼働しているか判定する必要がある。ICS の定期的監査を行い、次の点を検証すべきである。

- システムの妥当性検証（工場の検収及び現場での検収等）時にあったセキュリティ対策がそのまま設置され、生産システムで正常に稼働している。
- 生産システムにセキュリティ上の性能低下がなく、性能低下が生じた場合には、可能であればその性質や程度について情報を提供する。
- プログラム変更の管理は、全ての変更内容の審査・承認監査証跡に従って遵守されている。

各定期監査の結果は、事前に定められた適正な評価基準に照らして成績の形で記載し、セキュリティパフォーマンスとセキュリティ動向とを示すべきである。セキュリティパフォーマンス評価基準は、セキュリティ動向に関する意見とともに、関係者に送致すべきである。

伝統的に IT システムにおける監査の基本は、記録管理にあった。ICS 環境で適正なツールを使用するには、ICS に通じ、施設に関する重要生産・安全性の制約を理解した IT 専門員の広範な知見が必要となる。ICS に組み込まれたプロセス制御デバイスの多くは、何年も前に設置され、このセクションで述べた監査記録の提供能力がない。したがって、監査システム及びネットワーク活動用のこれら最新ツールの適用は、ICS コンポーネントの能力に左右される。

ICS 環境におけるネットワーク管理の重要タスクは、信頼性と可用性を確保して、安全で効率的な業務を支えることにある。規制を受ける業界では、規制を遵守することでセキュリティと認証管理、帳簿及び施設の完全性管理、施設及び業務適格性演習を強化するためのあらゆる機能が複雑になる。監査・記録管理ツールを利活用することで、インストールからライフサイクル全般を通じて、ICS を保守し完全性を実証する上で、貴重な助けが得られる。ICS 環境におけるこれらツールの価値は、攻撃・実行・過誤等により完全性が疑問視される場合に必要となる、適格性の再取得や ICS の再検査といった労力に照らして計算できよう。システムは監査ツールに対応して、信頼性の高い同期タイムスタンプを備えているべきである。

センサ、ログ、侵入検知システム（IDS）、アンチウイルス、パッチ管理、ポリシー管理ソフトウエアその他のセキュリティメカニズムは、可能であればリアルタイムで実行できるべきである。最前線の監視サービスはアラームを受領し、初期の問題判別を迅速に行い、該当施設職員が対処するようにアクションを起こす。

システム監査ユーティリティを新規及び既存 ICS プロジェクトに組み込むべきである。ユーティリティは、稼働中の ICS に展開する前に、試験を行うべきである（同等の ICS でのオフライン試験）。これらツールは、証拠及びシステムの完全性に関する有形の記録を提供できる。またアクティブログ管理ユーティリティは、進行中の攻撃や事象にフラグを立て、位置と追跡情報を提供して、インシデントへの対応を助ける[34]。

There should be a method for tracing all console activities to a user, either manually (e.g., control room sign in) or automatic (e.g., login at the application and/or OS layer). Policies and procedures for what is logged, how the logs are stored (or printed), how they are protected, who has access to the logs and how/when are they reviewed should be developed. These policies and procedures will vary with the ICS application and platform. Legacy systems typically employ printer loggers, which are reviewed by administrative, operational, and security staff. Logs maintained by the ICS application may be stored at various locations and may or may not be encrypted.

6.2.4 Security Assessment and Authorization

The security controls that fall within the NIST SP 800-53 Assessment and Authorization (CA) family provide the basis for performing periodic assessments and providing certification of the security controls implemented in the information system to determine if the controls are implemented correctly, operating as intended, and producing the desired outcome to meet the system security requirements. A senior organizational official is responsible for accepting residual risk and authorizing system operation. These steps constitute accreditation. In addition, all security controls should be monitored on an ongoing basis. Monitoring activities include configuration management and control of information system components, security impact analysis of changes to the system, ongoing assessment of security controls, and status reporting.
Supplemental guidance for the CA controls can be found in the following documents:

- NIST SP 800-53A provides guidance on security control assessments [23].
- NIST SP 800-37 provides guidance defining the information system boundary and security certification and accreditation of the information system [21].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

6.2.5 Configuration Management

Configuration management policy and procedures are used to control modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications prior to, during, and after system implementation. The security controls that fall within the NIST SP 800-53 Configuration Management (CM) family provide policy and procedures for establishing baseline controls for information systems. Controls are also specified for maintaining, monitoring, and documenting configuration control changes. There should be restricted access to configuration settings, and security settings of IT products should be set to the most restrictive mode consistent with ICS operational requirements.
Supplemental guidance for the CM controls can be found in the following documents:

- NIST SP 800-70 provides guidance on configuration settings for IT products [26].
- NIST SP 800-100 provides guidance on information security governance and planning [27].
- NIST SP 800-128 provides guidance on implementation of a security-focused configuration management program [80].

手動（制御室への立入署名等）又は自動（アプリケーションや OS へのログイン等）による、あるユーザの全てのコンソール活動に対する追跡方法を持つべきである。記録内容、記録の保管（又はプリント）方法、保護要領、記録へのアクセス件保持者、記録の変更方法・時期に関するポリシー及び手順を作成すべきである。ポリシー及び手順は、ICS の用途及びプラットホームにより異なる。レガシーシステムではプリンタロガーを通常、採用しており、管理、業務及びセキュリティ職員が目を通している。ICS アプリケーションが維持するログは、種々の場所に保管され、暗号化されているものもあれば、されていないものもある。

6.2.4 セキュリティ評価及び権限付与

NIST SP 800-53 のセキュリティ評価及び権限付与（CA）ファミリに含まれるセキュリティ対策は、定期的評価を行い、情報システムに実装されているセキュリティ対策の証明書を交付する根拠を定めており、これに従い管理が適性に行われ、予定どおりに稼働し、システムセキュリティ要件に合致した結果になっているかどうかを判定できる。組織の幹部は残留リスクを受け入れ、システムの稼働を許可する責任を有する。このような手順が認定を構成する。また、全てのセキュリティ対策は継続的に監視すべきである。監視活動には情報システムコンポーネントの設定管理、システム変更のセキュリティ影響分析、進展中のセキュリティ対策の評価及び現状報告が含まれる。

CA 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-53A：セキュリティ対策評価に係るガイダンス[23]
- NIST SP 800-37：情報システム境界及び情報システムセキュリティ証明・認定の定義に係るガイダンス[21]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

6.2.5 構成管理

構成管理ポリシー及び手順に従い、ハードウエア・ファームウエア・ソフトウエア・文書への変更を管理し、システム実装前・中・後の不適切な改変から情報システムを保護する。
NIST SP 800-53 の構成管理（CM）ファミリに含まれるセキュリティ対策には、情報システムのベースライン管理を策定するためのポリシー及び手順が定められている。構成管理の変更を維持・監視・記録するための管理もある。構成設定へのアクセスは制限され、IT 製品のセキュリティ設定は、ICS 業務要件に従い最も厳格なモードに設定すべきである。

CM 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-70：IT 製品の構成設定に係るガイダンス[26]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]
- NIST SP 800-128 に、セキュリティ重視構成管理プログラムに係るガイダンス[80]。

ICS-specific Recommendations and Guidance

A formal change management program should be established and procedures used to insure that all modifications to an ICS network meet the same security requirements as the original components identified in the asset evaluation and the associated risk assessment and mitigation plans. Risk assessment should be performed on all changes to the ICS network that could affect security, including configuration changes, the addition of network components, and installation of software. Changes to policies and procedures may also be required. The current ICS network configuration and device configurations must always be known and documented.

6.2.6 Contingency Planning

Contingency plans are designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster. The security controls that fall within the NIST SP 800-53 Contingency Planning (CP) family provide policies and procedures to implement a contingency plan by specifying roles and responsibilities, and assigning personnel and activities associated with restoring the information system after a disruption or failure. Along with planning, controls also exist for contingency training, testing, and plan update, and for backup information processing and storage sites.

Supplemental guidance for the CP controls can be found in the following documents:

- NIST SP 800-34 provides guidance on contingency planning [52].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

ICS-specific Recommendations and Guidance

Contingency plans should cover the full range of failures or problems that could be caused by cyber incidents. Contingency plans should include procedures for restoring systems from known valid backups, separating systems from all non-essential interferences and connections that could permit cybersecurity intrusions, and alternatives to achieve necessary interfaces and coordination. Employees should be trained and familiar with the contents of the contingency plans. Contingency plans should be periodically reviewed with employees responsible for restoration of the ICS, and tested to ensure that they continue to meet their objectives. Organizations also have business continuity plans and disaster recovery plans that are closely related to contingency plans. Because business continuity and disaster recovery plans are particularly important for ICS, they are described in more detail in the sections to follow.

6.2.6.1 Business Continuity Planning

Business continuity planning addresses the overall issue of maintaining or reestablishing production in the case of an interruption. These interruptions may take the form of a natural disaster (e.g., hurricane, tornado, earthquake, flood), an unintentional man-made event (e.g., accidental equipment damage, fire or explosion, operator error), an intentional man-made event (e.g., attack by bomb, firearm or vandalism, attacker or virus), or an equipment failure. From a potential outage perspective, this may involve typical time spans of days, weeks, or months to recover from a natural disaster, or minutes or hours to recover from a malware infection or a mechanical/electrical failure. Because there is often a separate discipline that deals with reliability and electrical/mechanical maintenance, some organizations choose to define business continuity in a way that excludes these sources of failure. Because business continuity also deals primarily with

ICS 固有の推奨事項及びガイダンス

正規の変更管理プログラムを策定し、ICS ネットワークへの全ての変更内容が、資産評価計画書及び関連リスク評価・緩和計画書に特定される当初のコンポーネントと同じセキュリティ要件に合致するように手順を行使しなければならない。リスク評価は、セキュリティに影響する ICS ネットワークへの全ての変更に対して行うべきで、これには構成変更、ネットワークコンポーネントの追加、ソフトウエアのインストールも含まれる。ポリシー及び手順の変更も必要となる。現在の ICS ネットワーク構成とデバイス構成は常に知らされ、記録されていなければならない。

6.2.6 不測事態計画

緊急時対応計画は、緊急時・システム障害時・災害時に代替地などでコンピュータを操作するなど、業務を維持・復旧するために作成される。 NIST SP 800-53 の不測事態計画（CP）ファミリに含まれるセキュリティ対策は、役割と責任を定め、中断・故障後の情報システムの復旧に関連した人員・活動を割り当てて、不測事態計画を実行するためのポリシー及び手順を定めている。
プランニングのみならず、管理は、不測事態対処訓練、試験、計画の更新、バックアップ情報処理・保管サイトについても取り上げている。

CP 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-34：不測事態計画の立案に係るガイダンス[52]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

ICS 固有の推奨事項及びガイダンス

緊急時対応計画は、サイバーインシデントにより生じ得るあらゆる障害や問題について取り上げるべきである。緊急時対応計画には、既知の有効バックアップからシステムを復旧し、サイバーセキュリティ侵入を許す重要でない全ての干渉・接続からシステムを分離するためのポリシー及び手順のほか、必要なインタフェース・調整を実現するための代替方法も含めるべきである。従業員は訓練を受け、不測事態計画の内容に精通しているべきである。計画書は、ICS の復旧担当者とともに定期的に見直し、常に目的に合致しているか試験を行うべきである。組織は、緊急時対応計画と密接な関わりを持つ事業継続計画書と災害復旧計画書も保持する。両計画書は特に ICS にとって重要であるため、続くセクションで詳述する。

6.2.6.1 事業継続計画

事業継続計画の立案では、中断時の生産の維持又は再開に関する全般的な問題を取り上げる。中断には自然災害（ハリケーン、トルネード、地震、洪水等）、人為的な予期しない事象（偶発的な装備品の損害、火災・爆発、操作ミス等）、人為的な故意の事象（爆弾、銃器・破壊行為による攻撃、攻撃者・ウイルス等）、装備品の故障などがある。操業停止の観点からすると、自然災害からの復旧には一般に日・週・月単位の期間を要し、マルウエア感染や機械・電子的故障の場合は分・時間単位となる。

that deals with reliability and electrical/mechanical maintenance, some organizations choose to define business continuity in a way that excludes these sources of failure. Because business continuity also deals primarily with the long-term implications of production outages, some organizations also choose to place a minimum interruption limit on the risks to be considered. For the purposes of ICS cybersecurity, it is recommended that neither of these constraints be made. Long-term outages (disaster recovery) and short-term outages (operational recovery) should both be considered. Because some of these potential interruptions involve man-made events, it is also important to work collaboratively with the physical security organization to understand the relative risks of these events and the physical security countermeasures that are in place to prevent them. It is also important for the physical security organization to understand which areas of a production site house data acquisition and control systems that might have higher-level risks.

Before creating a business continuity plan (BCP) to deal with potential outages, it is important to specify the recovery objectives for the various systems and subsystems involved based on typical business needs. There are two distinct types of objectives: system recovery and data recovery. System recovery involves the recovery of communication links and processing capabilities, and it is usually specified in terms of a Recovery Time Objective (RTO). This is defined as the time required to recover the required communication links and processing capabilities. Data recovery involves the recovery of data describing production or product conditions in the past and is usually specified in terms of a Recovery Point Objective (RPO). This is defined as the longest period of time for which an absence of data can be tolerated.

Once the recovery objectives are defined, a list of potential interruptions should be created and the recovery procedure developed and described. For most of the smaller scale interruptions, repair and replace activities based on a critical spares inventory will prove adequate to meet the recovery objectives. When this is not true, contingency plans need to be developed. Due to the potential cost and importance of these contingency plans, they should be reviewed with the managers responsible for business continuity planning to verify that they are justified. Once the recovery procedures are documented, a schedule should be developed to test part or all of the recovery procedures. Particular attention must be paid to the verification of backups of system configuration data and product or production data. Examples of system configuration data include computer configuration backups, application configuration backups, operational control limits, control bands and setpoints for pre-incident operation for all ICS programmable equipment. Not only should these be tested when they are produced, but the procedures followed for their storage should also be reviewed periodically to verify that the backups are kept in environmental conditions that will not render them unusable and that they are kept in a secure location, so they can be quickly obtained by authorized individuals when needed.

信頼性や電気・機械の保守に関する別の規則も多分にあるため、組織によってはこのような故障原因を排除した上で事業継続を定めているところもある。事業継続は、主に長期的な操業停止の制約を扱うため、考慮すべきリスクに最短中断限界を設定している組織もある。ICS サイバーセキュリティの目的上、このような制約事項は設けないことが薦められる。長期操業停止（災害復旧）と短期操業停止（業務復旧）の両方を検討すべきである。このような中断には人為的な事象も含まれるため、物理的セキュリティ組織と連携して、こうした事象の相対的リスクと、それを防止するために講じられている物理的セキュリティ対策について理解することが肝要である。また物理的セキュリティ組織も、生産現場のどこに高リスクのデータ取得・制御システムがあるかを把握しておくことが肝要である。

操業停止を取り上げた事業継続計画書（BCP）を作成する前に、一般的な事業ニーズに基づき、種々のシステム・サブシステムの復旧対象を指定することが肝要である。復旧対象はシステムとデータの 2 種類である。システム復旧は、通信リンクと処理機能の復旧が関係し、通常、目標復旧時間（RTO）として定められている。これは必須通信リンク及び処理機能を復旧するための時間として定義される。データ復旧は、過去の生産又は製品状態を記述したデータの復旧が関係し、通常、目標復旧時点（RPO）として定められている。これはデータがなくても許容できる最長時間として定義される。

復旧対象を定めたなら、中断可能性リストを作成し、復旧手順を作成し記述すべきである。大抵の小規模中断では、重要補用品在庫に基づく修理・交換で復旧対象に十分対応できる。これが当てはまらない場合には、緊急時対応計画を作成する必要がある。緊急時対応計画のコストと重要性から、緊急時対応計画は事業継続プランニング担当管理者とともに見直し、その妥当性を検証すべきである。復旧手順を文書化したなら、復旧手順の一部又は全部の試験を行うためのスケジュールを立てるべきである。システム構成データ及び製品・生産データのバックアップ検証には、特に注意を払わなければならない。システム構成データの例として、コンピュータ構成バックアップ、アプリケーション構成バックアップ、業務上の管理限界、全ての ICS プログラム可能装備品のインシデント前の管理範囲・設定点等がある。バックアップは作成の都度試験を行うだけでなく、それらの保存手順も定期的に見直して、バックアップが環境条件に適合して利用可能で、セキュアな場所に保管され、必要な場合には権限のある人員がすぐに入手できるようになっているか検証する。

6.2.6.2 Disaster Recovery Planning

A disaster recovery plan (DRP) is a documented process or set of procedures to recover and protect an IT infrastructure in the event of a disaster. The DRP, ordinarily documented in written form, specifies procedures an organization is to follow in the event of a disaster. It is a comprehensive statement of consistent actions to be taken before, during and after a disaster. The disaster could be natural, environmental or man-made. Man-made disasters could be intentional or unintentional.

ICS-specific Recommendations and Guidance

A DRP is essential to continued availability of the ICS. The DRP should include the following items:

- Required response to events or conditions of varying duration and severity that would activate the recovery plan.
- Procedures for operating the ICS in manual mode with all external electronic connections severed until secure conditions can be restored.
- Roles and responsibilities of responders.
- Processes and procedures for the backup and secure storage of information.
- Complete and up-to-date logical network diagram.
- Personnel list for authorized physical and cyber access to the ICS.
- Communication procedure and list of personnel to contact in the case of an emergency including ICS vendors, network administrators, ICS support personnel, etc.
- Current configuration information for all components.
- Schedule for exercising the DRP.

The plan should also indicate requirements for the timely replacement of components in the case of an emergency. If possible, replacements for hard-to-obtain critical components should be kept in inventory.

The security plan should define a comprehensive backup and restore policy. In formulating this policy, the following should be considered:

- The speed at which data or the system must be restored. This requirement may justify the need for a redundant system, spare offline computer, or valid file system backups.
- The frequency at which critical data and configurations are changing. This will dictate the frequency and completeness of backups.
- The safe onsite and offsite storage of full and incremental backups.
- The safe storage of installation media, license keys, and configuration information.
- Identification of individuals responsible for performing, testing, storing, and restoring backups.

6.2.6.2 災害復旧計画

災害復旧計画（DRP）は、災害時に IT インフラを復旧し保護するための文書化されたプロセス又は手順である。DRP は通常文書化され、災害時に組織が取る手順を定める。災害前・中・後に取るべき一貫した行動について、包括的に記述する。災害は自然環境の場合もあれば、人為的なものもある。人為災害は故意又は偶発により生じる。

ICS 固有の推奨事項及びガイダンス

DRP は、ICS の可用性を保持するために不可欠である。DRP には以下を含めるべきである。

- 復旧計画書が発動される事象又は状態の期間と重大性に応じて求められる対応
- 外部への電子接続が全て断たれた中で、セキュアな状態に復旧するまで、手動モードで ICS を稼働させるための手順
- 対応者の役割と責任
- 情報のバックアップとセキュアな保存を行うためのプロセスと手順
- 完全な最新の論理ネットワーク図
- ICS への立入及びサイバーアクセス権限のある人員リスト
- 緊急時の通信手順及び連絡相手のリスト（ICS ベンダー、ネットワーク管理者、ICS サポート要員等を含める）
- 全てのコンポーネントの最新構成情報
- DRP 演習スケジュール

計画書には、緊急時のコンポーネントを適時交換するための要件も含めるべきである。できれば入手困難な重要コンポーネントの代替品は、在庫させておくべきである。

セキュリティ計画書は、包括的なバックアップ及び復旧ポリシーを定めるべきである。ポリシーの策定に当たっては、次の点を考慮に入れるべきである。

- データ又はシステムの復旧に要する速度。この要件があることから冗長システム、スペアのオフラインコンピュータ又は有効ファイルシステムバックアップが必要とされる。
- 重要データ及び構成変更の頻度。これによりバックアップの頻度や完全性が決まる。
- 全面バックアップ及び差分バックアップの安全なオンサイト及びオフサイト保管
- インストールメディア、ライセンスキー及び設定情報の安全な保管
- バックアップの実施・試験・保管・復旧担当者の特定

6.2.7 Identification and Authentication

Authentication describes the process of positively identifying potential network users, hosts, applications, services, and resources using a combination of identification factors or credentials. The result of this authentication process then becomes the basis for permitting or denying further actions (e.g., when an automatic teller machine asks for a PIN). Based on the authentication determination, the system may or may not allow the potential user access to its resources. Authorization is the process of determining who and what should be allowed to have access to a particular resource; access control is the mechanism for enforcing authorization. Access control is described in Section 6.2.1.

There are several possible factors for determining the authenticity of a person, device, or system, including something you know, something you have or something you are. For example, authentication could be based on something known (e.g., PIN number or password), something possessed (e.g., key, dongle, smart card), something you are such as a biological characteristic (e.g., fingerprint, retinal signature), a location (e.g., Global Positioning System [GPS] location access), the time a request is made, or a combination of these attributes. In general, the more factors that are used in the authentication process, the more robust the process will be. When two or more factors are used, the process is known generically as *multi-factor authentication*.
The security controls that fall within the NIST SP 800-53 Identification and Authentication (IA) family provide policy and guidance for the identification and authentication of users of and devices within the information system. These include controls to manage identifiers and authenticators within each technology used (e.g., tokens, certificates, biometrics, passwords, key cards).

Supplemental guidance for the IA controls can be found in the following documents:

- NIST SP 800-63 provides guidance on remote electronic authentication [53].
- NIST SP 800-73 provides guidance on interfaces for personal identity verification [49].
- NIST SP 800-76 provides guidance on biometrics for personal identity verification [50].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

ICS-specific Recommendations and Guidance

Computer systems in ICS environments typically rely on traditional passwords for authentication. Control system suppliers often supply systems with default passwords. These passwords are factory set and are often easy to guess or are changed infrequently, which creates additional security risks. Also, protocols currently used in ICS environments generally have inadequate or no network service authentication. There are now several forms of authentication available in addition to traditional password techniques being used with ICS. Some of these, including password authentication, are presented in the following sections with discussions regarding their use with ICS.

6.2.7 識別及び認証

認証は、ネットワークユーザ、ホスト、アプリケーション、サービス及びリソースを識別要素や認証情報を組み合わせて、能動的に識別するプロセスである。認証プロセスの結果が、次のアクションを許可するか拒絶するかの根拠となる（ATM の PIN 要求時等）。認証判定に基づき、システムはユーザのリソースへのアクセスを許可又は拒絶する。権限付与とは、特定のリソースにアクセスが許される主体を判定するプロセスのことで、アクセス制御とは権限付与を行うメカニズムをいう。アクセス制御についてはセクション 6.2.1 で説明する。

個人、デバイス又はシステムの正当性を判定する要素がいくつかあり、個人が知っていること、持っているもの又は何者であるかなどである。例えば、認証は既知の事柄（PIN 番号やパスワード等）、所有物（キー、ドングル、スマートカード等）、生物学的特徴等の個人情報（指紋、網膜照合等）、場所（全地球測位システム[GPS]位置アクセス等）、要求時刻又はこれら属性を併用して行われる。総じて、認証プロセスで利用する要素が増えれば増えるほど、プロセスは強力になる。2 つ以上の要素を利用するプロセスは多要素認証として知られている。

NIST SP 800-53 の識別及び認証（IA）ファミリに含まれるセキュリティ対策は、情報システムにおけるユーザ及びデバイスの識別及び認証に係るポリシー及びガイダンスを定めている。使用される各技術（トークン、証明書、バイオメトリクス、パスワード、キーカード等）での識別及び認証の管理が含まれている。

IA 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-63：遠隔電子認証に係るガイダンス[53]
- NIST SP 800-73：個人身元確認インタフェースに係るガイダンス[49]
- NIST SP 800-76：個人身元確認バイオメトリクスに係るガイダンス[50]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

ICS 固有の推奨事項及びガイダンス

ICS 環境におけるコンピュータシステムは、一般に伝統的な認証パスワードに依存している。制御システムサプライヤは、デフォルトのパスワードを設定してシステムを供給することが多い。パスワードは工場で設定され、簡単に推測できるものが多く、滅多に変更されないことから、セキュリティリスクとなる。また現在 ICS 環境で利用されているプロトコルのネットワークサービス認証は、総じて不適切であるか全くない。現在では、ICS で利用される伝統的なパスワード技術に加えて、いくつかの認証形態がある。パスワード認証を含め、これらのいくつかを ICS で利用することについて、続くセクションで説明する。

6.2.7.1 Password Authentication

Password authentication technologies determine authenticity based on testing for something the device or human requesting access should know, such as a PIN number or password. Password authentication schemes are thought of as the simplest and most common forms of authentication.
Password vulnerabilities can be reduced by using an active password checker that prohibits weak, recently used, or commonly used passwords. Another weakness is the ease of third-party eavesdropping. Passwords typed at a keyboard are easily observed or recorded, especially in areas where adversaries could plant tiny wireless cameras or keystroke loggers. Network service authentication often transmits passwords as plaintext (unencrypted), allowing any network capture tool to expose the passwords.

ICS-specific Recommendations and Guidance

One problem with passwords unique to the ICS environment is that a user's ability to recall and enter a password may be impacted by the stress of the moment. During a major crisis when human intervention is critically required to control the process, an operator may panic and have difficulty remembering or entering the password and either be locked out completely or be delayed in responding to the event. If the password has been entered wrong and the system has a limit on allowed wrong password entries, the operator may be locked out permanently until an authorized employee can reset the account. Biometric identifiers may have similar drawbacks. Organizations should carefully consider the security needs and the potential ramifications of the use of authentication mechanisms on these critical systems.

In situations where the ICS cannot support, or the organization determines it is not advisable (e.g., performance, safety, or reliability are adversely impacted), to implement authentication mechanisms in an ICS, the organization uses compensating controls, such as rigorous physical security controls (e.g., control center keycard access for authorized users) to provide an equivalent security capability or level of protection for the ICS. This guidance also applies to the use of session lock and session termination in an ICS.
Special consideration must be made when pushing down policies based on login password authentication within the ICS environment. Without an exclusion list based on machine identification (ID), non-operator logon can result in policies being pushed down such as auto- logoff timeout and administrator password replacement that can be detrimental to the operation of the system.

Some ICS operating systems make setting secure passwords difficult, as the password size is very small and the system allows only group passwords at each level of access, not individual passwords. Some industrial (and Internet) protocols transmit passwords in plaintext, making them susceptible to interception. In cases where this practice cannot be avoided, it is important that users have different (and unrelated) passwords for use with encrypted and non-encrypted protocols.

The following are general recommendations and considerations with regards to the use of passwords.

- The length, strength, and complexity of passwords should balance security and operational ease of access within the capabilities of the software and underlying OS.

- Passwords should have appropriate length and complexity for the required security. In particular, they should not be able to be found in a dictionary or contain predictable sequences of numbers or letters.

6.2.7.1 パスワード認証

パスワード認証技術は、アクセスを求めているデバイスや人が知っているべき情報（PIN 番号やパスワード等）を検証して正当性を判定する技術である。パスワード認証法は、認証の最も単純かつ慣用的な形と見なされている。

パスワードの脆弱性は、単純なもの、最近使用したもの、よく使用されるものを禁止するアクティブパスワードチェッカーを利用することで減らすことができる。別の弱点は、サードパーティが容易に傍受できることである。キーボードでタイプしたパスワードは、特に攻撃側が小型ワイヤレスカメラやキーストロークロガーを設置した場所では、容易に観察又は記録できる。ネットワークサービス認証は、パスワードを平文（暗号化なし）で送信することが多く、ネットワークキャプチャツールがあればパスワードが露見してしまう。

ICS 固有の推奨事項及びガイダンス

ICS に一意のパスワードを使用する問題点は、ユーザがパスワードを思い出して入力する能力は、そのときのストレスに影響されることにある。危機の際に、プロセスの制御に人の対応が是非とも必要とされる場合、操作員がパニックに陥り、パスワードが思い出せずにログインできなかったり、対応が遅れたりすることがある。間違ったパスワードを入力し、システムに間違いパスワードの入力制限がある場合、その操作員は、権限のある従業員がアカウントをリセットするまで、ずっとログインできなくなる。バイオメトリック識別子にも同様の欠陥がある。組織は、セキュリティニーズと重要システムにおける認証メカニズムの利用に関する問題について慎重に検討すべきである。

ICS が対応しておらず、又は ICS への認証メカニズムの実装を不適切と判断する場合（パフォーマンス、安全性、信頼性が低下するなど）、組織は厳格な物理的セキュリティ対策等の代替管理を利用して（制御センターへの、権限のあるユーザによるキーカードを利用した立入等）、ICS の同等のセキュリティ機能又は保護レベルを確保する。このガイダンスは、ICS のセッションロック及びセッション終了にも当てはまる。

ICS 環境でのログインパスワード認証を基に、ポリシーを引き下げる場合は、特別な考慮を要する。マシン ID に基づく排除リストがない場合、操作員以外のログオンは、システムの動作を悪化させる自動ログオフタイムアウトや管理者パスワードの置換といった、ポリシーの引き下げが生じ得る。

ICS の OS によっては、パスワードサイズが短く、各レベルでのアクセス時、システムが個人パスワードではなくグループパスワードのみ受け付けるようになっているため、セキュアなパスワード設定が困難である。特定の産業用（及びインターネット）プロトコルは、パスワードを平文で送信するため傍受されやすい。この規範の利用が避けられない場合、ユーザは別の（無関係な）パスワードを持ち、暗号化プロトコル及び非暗号化プロトコルで利用することが肝要である。

以下はパスワードの利用に関する一般的な推奨事項及び考慮事項である。

- パスワードの長さ、強度及び複雑さは、ソフトウエア及び使用 OS の能力内で、セキュリティとアクセスしやすさのバランスを取るべきである。
- パスワードの長さと複雑さは、必要なセキュリティに見合ったものとすべきである。特に辞書に載っている用語や、数字や文字の順序が予想可能なものは使用すべきでない。

- Passwords should be used with care on operator interface devices such as control consoles on critical processes. Using passwords on these consoles could introduce potential safety issues if operators are locked out or delayed access during critical events. Physical security should supplement operator control consoles when password protection is not feasible.
- The keeper of master passwords should be a trusted employee, available during emergencies. Any copies of the master passwords must be stored in a very secure location with limited access.
- The passwords of privileged users (such as network technicians, electrical or electronics technicians and management, and network designers/operators) should be most secure and be changed frequently. Authority to change master passwords should be limited to trusted employees. A password audit record, especially for master passwords, should be maintained separately from the control system.
- In environments with a high risk of interception or intrusion (such as remote operator interfaces in a facility that lacks local physical security access controls), organizations should consider supplementing password authentication with other forms of authentication such as multi-factor authentication using biometric or physical tokens.
- For user authentication purposes, password use is common and generally acceptable for users logging directly into a local device or computer. Passwords should not be sent across any network unless protected by some form of FIPS-approved encryption or salted cryptographic hash specifically designed to prevent replay attacks. It is assumed that the device used to enter a password is connected to the network in a secure manner.
- For network service authentication purposes, passwords should not be passed as plain text. There are more secure alternatives available, such as challenge/response or public key authentication.

6.2.7.2 Challenge/response Authentication

Challenge/response authentication requires that both the service requester and service provider know a "secret" code in advance. When service is requested, the service provider sends a random number or string as a challenge to the service requester. The service requester uses the secret code to generate a unique response for the service provider. If the response is as expected, it proves that the service requester has access to the "secret" without ever exposing the secret on the network.

Challenge/response authentication addresses the security vulnerabilities of traditional password authentication. When passwords (hashed or plain) are sent across a network, a portion of the actual "secret" itself is being sent, giving the secret to the remote device performs authentication. Therefore, traditional password exchange always suffers the risk of discovery or replay. Because the secret is known in advance and never sent in challenge/response systems, the risk of discovery is eliminated. If the service provider can never send the same challenge twice, and the receiver can detect all duplications, the risks of network capture and replay attacks are eliminated.

- 重要プロセスの制御コンソール等、操作員インタフェースデバイスでは、パスワードを注意深く使用すべきである。このようなコンソール上でのパスワードの使用は、緊急時に操作員がログインできず、又は対応が遅れた場合に、安全上の問題が生起する。パスワード保護が利用できない場合、物理的セキュリティは操作員制御コンソールを補完するものとなる。
- マスターパスワードの保管者は、緊急時に連絡が付く信頼の置ける従業員とすべきである。マスターパスワードの写しを作成した場合は、立入が制限された安全な場所に保管しなければならない。
- 特権ユーザ（ネットワーク技術者、電気・電子技師・管理者、ネットワーク設計者・操作員等）のパスワードはセキュアで、頻繁に変更すべきである。マスターパスワードの変更権限は信頼の置ける従業員に限定すべきである。パスワード監査記録、特にマスターパスワード用は、制御システムから独立して保管すべきである。
- 傍受又は侵入リスクの高い環境（ローカルの物理的セキュリティ立入制限のない施設における遠隔操作員インタフェース等）では、組織は、バイオメトリックや物理的トークンを利用した多要素認証等、別形態の補足的パスワード認証を考慮すべきである。
- ユーザ認証目的では、パスワードの利用は一般的で、ユーザが直接ローカルデバイスやコンピュータにログインする方法として広く受け入れられている。特定の形態の FIPS 承認暗号又はリプレー攻撃防止用ソルト併用暗号学的ハッシュで保護されていない場合、パスワードをネットワークを越えて送信すべきでない。パスワード入力デバイスは、セキュアな方法でネットワーク接続されていることが前提である。
- ネットワークサービス認証目的では、パスワードを平文で渡すべきでない。これら以外にも、チャレンジ/レスポンス認証や公開鍵認証等のセキュアな代替手段がある。

6.2.7.2 チャレンジ/レスポンス認証

チャレンジ/レスポンス認証は、サービスの要求側と提供側が前もって「秘密の」コードを知っていなければならない。サービス要求があると、サービスプロバイダはランダムな数字や文字列をチャレンジとして要求者に送信する。要求者は秘密コードを使用して、一意のレスポンスをプロバイダ向けに生成する。レスポンスが期待どおりだと、要求者は、「秘密」をネットワーク上にさらすことなく、秘密へのアクセス権を持っていることになる。

チャレンジ/レスポンス認証は、伝統的なパスワード認証のセキュリティ上の脆弱性に対応するものとなる。ネットワークを越えてパスワード（ハッシュ化又は平文）が送信される場合、実際の「秘密」そのものが送信され、秘密を遠隔デバイスに与えることで認証が行われる。したがって、伝統的なパスワード交換には、常に露見又はリプレーのリスクがつきまとう。チャレンジ/レスポンスシステムでは秘密は事前に知らされ、送信されないため、露見リスクは排除される。サービスプロバイダが同じチャレンジを二度送ることができなければ、受信者が全ての複製を探知しても、ネットワークキャプチャとリプレー攻撃のリスクは排除される。

ICS-specific Recommendations and Guidance

For User Authentication, the direct use of challenge/response authentication may not be feasible for control system due to the possible latency that may be introduced in the necessary fast dynamics required for access to a control system or industrial network. For Network Service Authentication, the use of challenge/response authentication is preferable to more traditional password or source identity authentication schemes.
Challenge/response authentication provides more security than encrypted passwords for user authentication across a network. Managing master encryption algorithms and master passwords becomes increasing more complex as more parties are involved in the security processes and is an important consideration in the robustness of the security scheme.

6.2.7.3 Physical Token Authentication

Physical or token authentication is similar to password authentication, except that these technologies determine authenticity by testing for secret code or key produced by a device or token the person requesting access has in their possession, such as security tokens or smart cards. Increasingly, private keys are being embedded in physical devices such as USB dongles. Some tokens support single-factor authentication only, so that simply having possession of the token is sufficient to be authenticated. Others support multi-factor authentication that requires knowledge of a PIN or password in addition to possessing the token.
The primary vulnerability that token authentication addresses is easily duplicating a secret code or sharing it with others. It eliminates the all-too-common scenario of a password to a "secure" system being left on the wall next to a PC or operator station. The security token cannot be duplicated without special access to equipment and supplies.

A second benefit is that the secret within a physical token can be very large, physically secure, and randomly generated. Because it is embedded in metal or silicon, it does not have the same risks that manually entered passwords do. If a security token is lost or stolen, the authorized user loses access, unlike traditional passwords that can be lost or stolen without notice.

Common forms of physical/token authentication include:

- Traditional physical lock and keys.
- Security cards (e.g., magnetic, smart chip, optical coding).
- Radio frequency devices in the form of cards, key fobs, or mounted tags.
- Dongles with secure encryption keys that attach to the USB, serial, or parallel ports of computers.
- One-time authentication code generators (e.g., key fobs).

For single-factor authentication, the largest weakness is that physically holding the token means access is granted (e.g., anyone finding a set of lost keys now has access to whatever they open). Physical/token authentication is more secure when combined with a second form of authentication, such as a memorized PIN used along with the token.

ICS 固有の推奨事項及びガイダンス

ユーザ認証に関して、制御システムではチャレンジ/レスポンス認証の直接的な使用は不可能かもしれない。と言うのは、制御システム又は産業用ネットワークへのアクセスに必要とされる高速ダイナミクスでは、待ち時間が生じかねないからである。ネットワークサービス認証では、チャレンジ/レスポンス認証の使用は、伝統的なパスワード方式やソース識別認証方式よりも望ましい。

ネットワークを越えるユーザ認証では、チャレンジ/レスポンス認証のセキュリティは暗号パスワードよりも強い。マスター暗号アルゴリズム及びマスターパスワードの管理は、セキュリティプロセスに関係する当事者が増えるにつれて、ますます複雑になっており、セキュリティ体制の堅牢性における重要な考慮事項である。

6.2.7.3 物理的トークン認証

物理的又はトークン認証はパスワード認証に似ているが、違いはアクセス要求者が持っているデバイスやトークン（セキュリティトークンやスマートカード）が生成する秘密コードやキーを検証して認証を判別する点にある。ますます USB ドングル等の物理的デバイスにプライベートキーが埋め込まれるようになっている。単要素認証にしか対応していないトークンもあり、トークンを持っていさえすれば認証に十分ということである。トークンの保有に加えて、PIN やパスワードを要求する多要素認証に対応したものもある。

トークン認証の主な脆弱性は、秘密コードの複製が容易なことと他人との共有が可能なことである。トークンを使えば、「セキュアな」システムのパスワードを PC や操作員ステーションの近くに書きとどめておくような、よくあるシナリオはなくなる。セキュリティトークンの複製は、装備品やサプライ品への特別なアクセス権がなければできない。

2 つ目の利点は、物理的トークン内部の秘密はサイズが大きく、物理的にセキュアで、ランダム生成される。金属やシリコンに埋め込まれているため、マニュアル操作でパスワードを入力するようなリスクはない。セキュリティトークンをなくした場合や盗まれた場合、ユーザはアクセス権を失う。これは気づかないうちになくしたり盗まれたりするパスワードとの違いである。

物理的/トークン認証の共通形態として次のものがある。

- 伝統的な物理ロックとキー
- セキュリティカード（磁気、スマートチップ、光コーディング等）
- カード、キーフォブ又は取付けタグ等の無線周波数デバイス
- USB、コンピュータのシリアル又はパラレルポートに取り付けるセキュアな暗号鍵付きドングル
- ワンタイム認証コードジェネレータ（キーフォブ等）

単要素認証の最大の弱点は、トークンを物理的に保有していればアクセスできることにある（鍵束の拾得者は他人の家に自由に出入りできる）。物理的/トークン認証は、別形態の認証と併用するとセキュリティが向上する（記憶した PIN との併用など）。

ICS-specific Recommendations and Guidance

Multi-factor authentication is an accepted good practice for access to ICS applications from outside the ICS firewall.
Physical/token authentication has the potential for a strong role in ICS environments. An access card or other token can be an effective form of authentication for computer access, as long as the computer is in a secure area (e.g., once the operator has gained access to the room with appropriate secondary authentication, the card alone can be used to enable control actions).

6.2.7.4 Smart Card Authentication

Smart cards are similar to token authentication, but can provide additional functionality. Smart cards can be configured to run multiple on-board applications to support building access, computer dual-factor or triple-factor authentication and cashless vending on a single card, while also acting as the company photo ID for the individual.

Typically, smart cards come in a credit card size form-factor that can be printed, embossed, and individually personalized. Smart cards can be customized, individualized, and issued in-house or outsourced to service providers who typically issue hundreds of thousands of cards per day.
Smart cards enhance software-only solutions, such as password authentication, by offering an additional authentication factor and removing the human element in memorizing complex secrets. They also:

- Isolate security-critical computations, involving authentication, digital signatures, and key exchange from other parts of the system that do not have a need to know.
- Enable portability of credentials and other private information between multiple computer systems.
- Provide tamper-resistant storage for protecting private keys and other forms of personal information.

The majority of issues are logistical around issuing the cards, particularly to replace lost or stolen cards.

ICS-specific Recommendations and Guidance

Although smart cards are relatively inexpensive and offer useful functionality in an industrial control system context, their implementation must be done within the overall security context of the plant. The necessary identification of individuals, issuance of cards, revocation should compromise be suspected, and the assignment of authorizations to authenticated identities, represents a significant initial and on-going challenge. In some cases corporate IT or other resources may be available to assist in the deployment of smart card and public key based infrastructures.

If smart cards are implemented in an industrial control setting, provisions for management of lost or damaged cards should be considered, as well as the costs to incorporate a respective access control system and provide a management process for card distribution and retrieval.

ICS 固有の推奨事項及びガイダンス

多要素認証は、ICS ファイアウォール外から ICS アプリケーションにアクセスする際の受け入れられる優良規範である。

物理的/トークン認証は、ICS 環境で大きな役割を果たす可能性がある。アクセスカードその他のトークンは、コンピュータがセキュアなエリアにある限り、コンピュータへの効果的な認証形態である（操作員が 2 つ目の適正な認証を経て室内に立ち入ると、制御行為を行うにはカードのみとなる）。

6.2.7.4 スマートカード認証

スマートカードはトークン認証に似ているが、付加的な機能がある。スマートカードは、複数のオンボードアプリケーションを実行して、建物への立入、コンピュータの 2 重要素又は 3 重要素認証及び 1 枚のカードでのキャッシュレス販売に対応できるように設定可能で、企業の写真付き個人用 ID カードとしても使用できる。

一般にスマートカードはクレジットカードサイズで、印字・エンボス・個別化が可能である。カスタマイズや個人別の個別化が可能で、組織内で発行できるほか、数十万のカードを毎日発行しているサービスプロバイダに外注することもできる。
スマートカードは、付加的な認証要素を提供し、複雑な秘密を覚えるという人的要因を排除することにより、パスワード認証等のソフトウエアのみに依存するソリューションを拡張する。また次のような特徴がある。

- セキュリティの重要な演算、例えば認証、デジタル署名、知る必要のないシステムの他の部位からのキー交換の隔離
- 複数コンピュータシステム間での認証情報その他個人情報のポータビリティの実現
- プライベートキーその他の個人情報の改変防止保管

問題の大半は、カード発行に関する業務的な内容で、特にカードの紛失・盗難が多い。

ICS 固有の推奨事項及びガイダンス

スマートカードは比較的安価で、産業用制御システムにおいて便利な機能を発揮するが、その実装は、プラントの全体的なセキュリティを考慮した上で行わなければならない。必要な個人識別、カード発行、取消によるマイナス要素を考慮に入れるなら、認証済み個人に対する権限の付与は、当初にもそれ以後も大きな課題となる。場合によっては、企業 IT その他のリソースを利用して、スマートカードと公開鍵ベースのインフラを展開する資とできよう。

スマートカードを産業用制御環境に実装する場合、紛失・毀損カードの管理規定やそれぞれのアクセス制御システムの組込みに要するコストを検討し、カード配布・回収の管理プロセスを定めるべきである。

6.2.7.5 Biometric Authentication

Biometric authentication technologies determine authenticity by determining presumably unique biological characteristics of the human requesting access. Usable biometric features include finger minutiae, facial geometry, retinal and iris signatures, voice patterns, typing patterns, and hand geometry.

Like physical tokens and smart cards, biometric authentication enhances software-only solutions, such as password authentication, by offering an additional authentication factor and removing the human element in memorizing complex secrets. In addition, because biometric characteristics are unique to a given individual, biometric authentication addresses the issues of lost or stolen physical tokens and smart cards. Noted issues with biometric authentication include:

- Distinguishing a real object from a fake (e.g., how to distinguish a real human finger from a silicon-rubber cast of one or a real human voice from a recorded one).
- Generating type-I and type-II errors (the probability of rejecting a valid biometric image, and the probability of accepting an invalid biometric image, respectively). Biometric authentication devices should be configured to the lowest crossover between these two probabilities, also known as the crossover error rate.
- Handling environmental factors such as temperature and humidity to which some biometric devices are sensitive.
- Addressing industrial applications where employees may have on safety glasses and/or gloves and industrial chemicals may impact biometric scanners.
- Retraining biometric scanners that occasionally "drift" over time. Human biometric traits may also shift over time, necessitating periodic scanner retraining.
- Requiring face-to-face technical support and verification for device training, unlike a password that can be given over a phone or an access card that can be handed out by a receptionist.
- Denying needed access to the control system because of a temporary inability of the sensing device to acknowledge a legitimate user.
- Being socially acceptable. Users consider some biometric authentication devices more acceptable than others. For example, retinal scans may be considered very low on the scale of acceptability, while thumb print scanners may be considered high on the scale of acceptability. Users of biometric authentication devices will need to take social acceptability for their target group into consideration when selecting among various biometric authentication technologies.

ICS-specific Recommendations and Guidance

Biometric devices make a useful secondary check versus other forms of authentication that can become lost or borrowed. Using biometric authentication in combination with token-based access control or badge-operated employee time clocks increases the security level. A possible application is in a control room that is environmentally controlled and physically secured [34].

Biometrics can provide a valuable authentication mechanism, but need to be carefully assessed for industrial applications because physical and environmental issues within the installation environment may need to be restructured for reliable authorized authentication. The exact physical and environmental properties of an installation should be coordinated with a system vendor or manufacturer.

6.2.7.5 バイオメトリック認証

バイオメトリック認証技術は、アクセス要求する個人の、各人に固有と考えられている生物学的特徴を判別して認証を判定する。利用できるバイオメトリック特性には指紋、顔の輪郭、網膜及び光彩特性、音声パターン、タイピングパターン、手の輪郭等がある。

物理的トークンやスマートカードと同様、バイオメトリック認証は、付加的な認証要素を提供し、複雑な秘密を覚えるという人的要因を排除することにより、パスワード認証等のソフトウエアのみに依存するソリューションを強化することができる。また、生物学的特徴は特定の個人に固有であることから、バイオメトリック認証は、物理的トークンやスマートカードの紛失・盗難問題に対応するものとなる。

バイオメトリック認証について知られている問題には次のようなものがある。

- 実物と偽物の区別（人の指と型取りしたシリコン製の指、実際の発声と録音した声の区別方法）
- タイプ 1 エラーとタイプ 2 エラーの生成（有効なバイオメトリック画像を拒絶する確率、無効なバイオメトリック画像を受け入れる確率）。バイオメトリック認証デバイスは、これら 2 つの確率の間の最低のクロスオーバーに設定されるべきで、クロスオーバー誤差率としても知られる。
- 特定のバイオメトリックデバイスが敏感に反応する温度・湿度等の環境因子の処理
- 従業員が安全ゴーグルやグローブを着用し、工業用化学物質がバイオメトリックスキャナーに影響する産業用アプリケーションの処理
- 経時的に「ドリフト」するバイオメトリックスキャナーの再訓練。人のバイオメトリック特性は経時的に変化するため、スキャナーの定期的再訓練が必要になる。
- 1 対 1 の技術支援とデバイス訓練の検証が必要。受付係から電話で教えられるパスワードや、手渡し可能なアクセスカードと異なる。
- 適格ユーザを認知する検知デバイスの一時的不調による制御システムへのアクセス拒否
- 社会の受入れ態勢。バイオメトリック認証に対するユーザの受容度はデバイスによりばらつきがある。例えば、受容度は網膜スキャンの場合低く、親指のプリントスキャナーは高い。多様なバイオメトリック技術の中からいずれかを選択する際、バイオメトリック認証デバイスユーザは、対象グループに対する社会の受容度を考慮に入れる必要がある。

ICS 固有の推奨事項及びガイダンス

バイオメトリックデバイスは、紛失したり貸借したりできる他の形態の認証に対して、有用な副次的チェックができる。トークンベースのアクセス制御やバッジ操業する従業員のタイムレコーダと併用すれば、セキュリティレベルが向上する。考えられる用途として、環境的に制御され物理的なセキュリティが確保されている制御室がある[34]。

バイオメトリクスは貴重な認証メカニズムとなるが、信頼性の高い認証を得るには設置環境の物理・環境問題を解決する必要があるため、産業用途としては慎重な評価を要する。設置の正確な物理・環境特性について、システムベンダーやメーカーと調整すべきである。

6.2.8 Incident Response

An incident response plan is documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against an organization's information systems. Response should be measured first and foremost against the "service being provided," not just the system that was compromised. If an incident is discovered, there should be a quick risk assessment performed to evaluate the effect of both the attack and the options to respond. For example, one possible response option is to physically isolate the system under attack. However, this may have such a dire impact on the service that it is dismissed as not viable.

The security controls that fall within the NIST SP 800-53 Incident Response (IR) family provide policies and procedures for incident response monitoring, handling, and reporting. The handling of a security incident includes preparation, detection and analysis, containment, eradication, and recovery. Controls also cover incident response training for personnel and testing the incident response capability for an information system.
Supplemental guidance for the IR controls can be found in the following documents:

- NIST SP 800-61 provides guidance on incident handling and reporting [59].
- NIST SP 800-83 provides guidance on malware incident prevention and handling [60].
- NIST SP 800-100 provides guidance on information security governance and planning [27] .

ICS-specific Recommendations and Guidance

Regardless of the steps taken to protect an ICS, it is always possible that it may be compromised by an intentional or unintentional incident. The following symptoms can arise from normal network problems, but when several symptoms start to appear, a pattern may indicate the ICS is under attack and may be worth investigating further. If the adversary is skilled, it may not be very obvious that an attack is underway.
The symptoms of an incident could include any of the following:

- Unusually heavy network traffic.
- Out of disk space or significantly reduced free disk space.
- Unusually high CPU usage.
- Creation of new user accounts.
- Attempted or actual use of administrator-level accounts.
- Locked-out accounts.
- Account in-use when the user is not at work.
- Cleared log files.
- Full log files with unusually large number of events.

6.2.8 インシデント対応

インシデント対応計画書は、組織の情報システムに対するインシデントの結果を検知し、対応し、局限するための事前に決められた一連の指示又は手順を文書化したものである。対応は、まず計測すること、そして「提供中のサービス」に対して行うものであり、性能が低下したシステムだけに行うのではない。インシデントが発見されたなら、迅速にリスク評価を行い、攻撃の影響と対応オプションの両方を評価する。例えば、対応オプションの一例として、攻撃されたシステムを物理的に隔絶することができよう。ただしこの対応だと、サービスに深刻な影響が及ぶため、実行不能と一蹴される。

NIST SP 800-53 のインシデント対応（IR）ファミリに含まれるセキュリティ対策には、インシデント対応の監視、処理及び報告のためのポリシー及び手順が定められている。セキュリティインシデントの処理には、準備、検出・分析、封じ込め、根絶及び復旧が含まれる。管理策も職員のインシデント対応訓練及び情報システムのインシデント対応能力試験を含む。

IR 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-61：インシデント処理及び報告に係るガイダンス[59]
- NIST SP 800-83：マルウエアインシデント防止及び処理に係るガイダンス[60]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

ICS 固有の推奨事項及びガイダンス

ICS の保護手順とは無関係に、故意又は偶発的なインシデントにより ICS の性能が低下する場合がある。正常なネットワーク問題として以下のような徴候が見られるが、いくつかの徴候が出始めたなら、ICS が攻撃されていることを示すパターンであり、調査を行うに値する。攻撃側が巧妙だと、攻撃中であることが明確にはならない。

インシデントの徴候には次のようなものがある。

- ネットワークトラフィックが異常に重い
- ディスク容量がない又は空き容量が著しく少ない
- CPU 利用率が異常に高い
- 新規ユーザアカウントが作成されている
- 管理者レベルアカウントを使用又は使用しようとした形跡がある
- アカウントがロックアウトされた
- そのユーザが不在なのにアカウントが使用されている
- ログファイルがクリアされている
- ログファイルが一杯でイベント数が異常に多い

- Antivirus or IDS alerts.
- Disabled antivirus software and other security controls.
- Unexpected patch changes.
- Machines connecting to outside IP addresses.
- Requests for information about the system (social engineering attempts).
- Unexpected changes in configuration settings.
- Unexpected system shutdown.

To minimize the effects of these intrusions, it is necessary to plan a response. Incident response planning defines procedures to be followed when an intrusion occurs. NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide* [59], provides guidance on incident response planning, which might include the following items:

- **Classification of Incidents.** The various types of ICS incidents should be identified and classified as to potential impact so that a proper response can be formulated for each potential incident.

- **Response Actions.** There are several responses that can be taken in the event of an incident. These range from doing nothing to full system shutdown (although full shutdown of an ICS is a highly unlikely response). The response taken will depend on the type of incident and its effect on the ICS system and the physical process being controlled. A written plan documenting the types of incidents and the response to each type should be prepared. This will provide guidance during times when there might be confusion or stress due to the incident. This plan should include step-by-step actions to be taken by the various organizations. If there are reporting requirements, these should be noted as well as where the report should be made and phone numbers to reduce reporting confusion.

- **Recovery Actions.** The results of the intrusion could be minor, or the intrusion could cause many problems in the ICS. Risk analysis should be conducted to determine the sensitivity of the physical system being controlled to failure modes in the ICS. In each case, step-by-step recovery actions should be documented so that the system can be returned to normal operations as quickly and safely as possible. Recovery actions for an intrusion that affects operation of the ICS will closely align with the system's Disaster Recovery Plan, and should take into account the planning and coordination already established.

During the preparation of the incident response plan, input should be obtained from the various stakeholders including operations, engineering, IT, system support vendors, management, organized labor, legal, and safety. These stakeholders should also review and approve the plan.

- アンチウイルスアラート又は IDS アラートが出ている
- アンチウイルスソフトウエアその他のセキュリティ対策が無効になっている
- 予定外のパッチ変更がなされている
- マシンが外部 IP アドレスに接続されている
- システムに関する情報請求があった（ソーシャルエンジニアリングのもくろみ）
- 構成の設定に予定外の変更がなされている
- 予定外のシステム遮断があった

このような侵入の影響を最小限に食い止めるため、対応を計画する必要がある。インシデント対応計画の立案では、侵入があった際に取るべき手順を定める。NIST SP 800-61 改訂第 2 版『コンピュータセキュリティインシデントの処理』[59]には、インシデント対応計画の立案に係るガイダンスが示されており、以下の項目が含まれている。

- **インシデントの区分。**種々の ICS インシデントを識別し、影響度を区分し、インシデントごとに適正な対応が取れるようにすべきである。
- **対応行動。**インシデントがおきた際には、取り得る対応がいくつかある。何もしないことからシステムの全面遮断まである（もちろん、ICS の全面遮断はほぼありそうにない対応ではある）。対応はインシデントのタイプ、ICS システムへの影響及び制御中に物理プロセスに応じて取られる。インシデントのタイプと各タイプへの対応を記録した計画書を用意すべきである。それがあると、インシデントによる混乱やストレス下にあってもガイダンスとなる。計画書には、多様な組織が取るべき段階ごとの行動を含めるべきである。報告要件があれば、報告先のほか、報告時の混乱を少なくするため電話番号とともに、要件も記載しておく。
- **復旧対策。**侵入の結果が取るに足りないこともあれば、ICS に多くの問題を生じさせることもある。リスク分析を行い、ICS の故障態様に影響を受ける制御中の物理システムの感度を判定する。いずれの場合も、段階ごとの復旧対策を文書化し、できるだけ迅速かつ安全にシステムが正常業務に復帰できるようにする。ICS の稼働に影響する侵入への復旧対策は、システムの災害復旧計画書と密接に連携し、既になされたプランニングや調整事項を考慮に入れるべきである。

インシデント対応計画書を準備する際には、運用、エンジニアリング、IT、システムサポートベンダー、経営時、組合労働者、法律、安全等の関係者から幅広く意見を聞くべきである。またこれら関係者は、計画書の審査・承認にも関わるべきである。

6.2.9 Maintenance

The security controls that fall within the NIST SP 800-53 Maintenance (MA) family provide policy and procedure for performing routine and preventative maintenance on the components of an information system. This includes the usage of maintenance tools (both local and remote) and management of maintenance personnel.

Supplemental guidance for the MA controls can be found in the following documents:

- NIST SP 800-63 provides guidance on electronic authentication for remote maintenance [53].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

6.2.10 Media Protection

The security controls that fall within the NIST SP 800-53 Media Protection (MP) family provide policies and procedures for limiting the access to media to authorized users. Controls also exist for labeling media for distribution and handling requirements, as well as storage, transport, sanitization (removal of information from digital media), destruction, and disposal of the media.

Supplemental guidance for the MP controls can be found in the following documents:

- NIST SP 800-88 provides guidance on appropriate sanitization equipment, techniques, and procedures [78].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

ICS-specific Recommendations and Guidance

Media assets include removable media and devices such as floppy disks, CDs, DVDs and USB memory sticks, as well as printed reports and documents. Physical security controls should address specific requirements for the safe and secure maintenance of these assets and provide specific guidance for transporting, handling, and erasing or destroying these assets. Security requirements could include safe storage from loss, fire, theft, unintentional distribution, or environmental damage.

If an adversary gains access to backup media associated with an ICS, it could provide valuable data for launching an attack. Recovering an authentication file from the backups might allow an adversary to run password cracking tools and extract usable passwords. In addition, the backups typically contain machine names, IP addresses, software version numbers, usernames, and other data useful in planning an attack. The use of any unauthorized CDs, DVDs, floppy disks, USB memory sticks, or similar removable media on any node that is part of or connected to the ICS should not be permitted in order to prevent the introduction of malware or the inadvertent loss or theft of data. Where the system components use unmodified industry standard protocols, mechanized policy management software can be used to enforce media protection policy.

6.2.9 保守

NIST SP 800-53 の保守（MA）ファミリに含まれるセキュリティ対策は、情報システムコンポーネントの恒常整備と予防整備に係るポリシー及び手順を定めている。これには整備ツール（ローカルと遠隔）の利用及び整備要員の管理も含まれる。

MA 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-63：遠隔保守の電子認証に係るガイダンス[53]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

6.2.10 メデイア保護

NIST SP 800-53 のメデイア保護（MP）ファミリに含まれるセキュリティ対策には、メディアへのアクセスを許可を受けたユーザだけに制限するためのポリシー及び手順が定められている。管理には、配布要件及び処理要件用のメディアのラベリングのほか、メディアの保管、輸送、サニタイズ（デジタルメディアからの情報削除）、破壊、破棄も含まれる。

MP 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-88：適切なサニタイズ装備品、技術及び手順に係るガイダンス[78]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

ICS 固有の推奨事項及びガイダンス

メディア資産にはフロッピーディスク、CD、DVD、USB メモリスティック等の取り外し可能メディア及びデバイスのほか印刷物もある。物理的セキュリティ対策では、これら資産の安全かつセキュアな保守要件を取り上げ、それらの輸送、処理及び消去又は破壊に係る具体的なガイダンスを容易すべきである。セキュリティ要件には、紛失・火災・盗難・想定外の配布・環境被害からの安全な保存を含めることができる。

攻撃側が ICS 関連のバックアップメディアにアクセスすると、貴重なデータを攻撃に利用される可能性がある。攻撃側はバックアップから認証ファイルを回復して、パスワード解析ツールを実行し、パスワードを抜き取ることができる。またバックアップには通常、マシン名、IP アドレス、ソフトウエアのバージョン番号、ユーザ名その他攻撃に役立つデータが入っている。

ICS の一部又は ICS に接続されたノード上の許可されていない CD、DVD、フロッピーディスク、USB メモリスティック等の取り外し可能メディアの使用は、マルウエア又は想定外のデータ喪失・盗難を予防するために許可すべきでない。システムコンポーネントが未修正の業界標準プロトコルを使用する場合、ポリシー管理ソフトウエアを利用してメディア保護ポリシーを施行することができる。

6.2.11 Physical and Environmental Protection

The security controls that fall within the NIST SP 800-53 Physical and Environmental Protection (PE) family provide policy and procedures for all physical access to an information system including designated entry/exit points, transmission media, and display media. These include controls for monitoring physical access, maintaining logs, and handling visitors. This family also includes controls for the deployment and management of emergency protection controls such as emergency shutdown of the IT system, backup for power and lighting, controls for temperature and humidity, and protection against fire and water damage.

Supplemental guidance for the PE controls can be found in the following documents:

- NIST SP 800-46 provides guidance on telecommuting and broadband communication security [51].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

Physical security measures are designed to reduce the risk of accidental or deliberate loss or damage to plant assets and the surrounding environment. The assets being safeguarded may be physical assets such as tools and plant equipment, the environment, the surrounding community, and intellectual property, including proprietary data such as process settings and customer information. The deployment of physical security controls is often subject to environmental, safety, regulatory, legal, and other requirements that must be identified and addressed specific to a given environment. The subject of deploying physical security controls is vast and needs to be specific to the type of protection needed.

ICS-specific Recommendations and Guidance

The physical protection of the cyber components and data associated with the ICS must be addressed as part of the overall security of a plant. Security at many ICS facilities is closely tied to plant safety. A primary goal is to keep people out of hazardous situations without preventing them from doing their job or carrying out emergency procedures. Physical security controls are any physical measures, either active or passive, that limit physical access to any information assets in the ICS environment. These measures are employed to prevent many types of undesirable effects, including:

- Unauthorized physical access to sensitive locations.
- Physical modification, manipulation, theft or other removal, or destruction of existing systems, infrastructure, communications interfaces, personnel, or physical locations.
- Unauthorized observation of sensitive informational assets through visual observation, note taking, photographs, or other means.
- Prevention of unauthorized introduction of new systems, infrastructure, communications interfaces, or other hardware.
- Prevention of unauthorized introduction of devices intentionally designed to cause hardware manipulation, communications eavesdropping, or other harmful impact.

Gaining physical access to a control room or control system components often implies gaining logical access to the process control system as well. Likewise, having logical access to systems such as main servers and control room computers allows an adversary to exercise control over the physical process.

6.2.11 物理環境上の保護（PE）

NIST SP 800-53 の物理環境上の保護（PE）ファミリに含まれているセキュリティ対策には、情報システムへのあらゆる物理的立入に係るポリシー及び手順が定められており、指定された入退場点、送信媒体、表示媒体について記述されている。物理的立入の監視、記録の維持、来訪者の取扱に関する管理も含まれている。またこのファミリには、緊急保護対策の展開及び管理に関する対策も含まれ、IT システムの緊急遮断、電力・照明のバックアップ、温度・湿度管理、火災・水害対策等について取り上げている。

PE 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-46：在宅勤務及びブロードバンド通信に係るガイダンス[51]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

物理的セキュリティ対策は、プラント資産や周辺環境に対する偶発的又は故意の喪失・損害リスクを軽減するためのものである。保護対象されるのは、ツール・プラント装備品、環境、周辺共同体、知的財産（プロセス設定や顧客情報といった専有データ）等の物理的資産が対象である。物理的セキュリティ対策の展開は環境、安全性、規制、法律その他特定の環境に固有の要件により左右されることが多い。物理的セキュリティ対策の展開対象は広範で、必要とされる保護のタイプに特化する必要がある。

ICS 固有の推奨事項及びガイダンス

サイバーコンポーネント及び ICS 関連データの物理的保護は、プラント全体のセキュリティの一環として検討しなければならない。多くの ICS 施設のセキュリティは、プラントの安全性と密接に結びついている。主な目標は、従業員が職務や緊急手順を遂行するのを妨げることなく、危険状態には置かないことにある。物理的セキュリティ対策は、能動的又は受動的な物理的対策で、ICS 環境における情報資産への物理的立入を制限する。このような対策を採用することで、次のような望ましくない種々の影響を防ぐことができる。

- 注意を要する場所への無断立入
- 既存システム、インフラ、通信インタフェース、職員又は場所の物理的変更、操作、盗難その他の除去又は破壊
- 視認、メモ、写真その他の手段による要注意情報資産の無断偵察
- 新規システム、インフラ、通信インタフェースその他ハードウエアの無断導入
- ハードウエア操作、通信傍受その他有害影響を意図したデバイスの無断導入

制御室や制御システムコンポーネントへの立入は、プロセス制御システムへの論理アクセスも可能になることが多い。同様に、メインサーバや制御室のコンピュータ等のシステムへの論理アクセスが得られれば、攻撃側は物理プロセスを制御できるようになる。

If computers are readily accessible, and they have removable media drives (e.g., floppy disks, compact discs, external hard drives) or USB ports, the drives can be fitted with locks or removed from the computers and USB ports disabled. Depending on security needs and risks, it might also be prudent to disable or physically protect power buttons to prevent unauthorized use. For maximum security, servers should be placed in locked areas and authentication mechanisms (such as keys) protected. Also, the network devices on the ICS network, including switches, routers, network jacks, servers, workstations, and controllers, should be located in a secured area that can only be accessed by authorized personnel. The secured area should also be compatible with the environmental requirements of the devices.

A defense-in-depth solution to physical security should include the following attributes:

- **Protection of Physical Locations**. Classic physical security considerations typically refer to a ringed architecture of layered security measures. Creating several physical barriers, both active and passive, around buildings, facilities, rooms, equipment, or other informational assets, establishes these physical security perimeters. Physical security controls meant to protect physical locations include fences, anti-vehicle ditches, earthen mounds, walls, reinforced barricades, gates, or other measures. Most organizations include this layered model by preventing access to the plant first by the use of fences, guard shacks, gates, and locked doors.
- **Access Control.** Access control systems should ensure that only authorized people have access to controlled spaces. An access control system should be flexible. The need for access may be based on time (day vs. night shift), level of training, employment status, work assignment, plant status, and a myriad of other factors. A system must be able to verify that persons being granted access are who they say they are (usually using something the person has, such as an access card or key; something they know, such as a personal identification number (PIN); or something they are, using a biometric device). Access control should be highly reliable, yet not interfere with the routine or emergency duties of plant personnel. Integration of access control into the process system allows a view into not only security access, but also physical and personnel asset tracking, dramatically accelerating response time in emergencies, helping to direct individuals to safe locations, and improving overall productivity. Within an area, access to network and computer cabinets should be limited to only those who have a need, such as network technicians and engineers, or computer maintenance staff. Equipment cabinets should be locked and wiring should be neat and within cabinets. Consider keeping all computers in secure racks and using peripheral extender technology to connect human-machine interfaces to the racked computers.

  Access Monitoring Systems. Access monitoring systems include still and video cameras, sensors, and various types of identification systems. Examples of these systems include cameras that monitor parking lots, convenience stores, or airline security. These devices do not specifically prevent access to a particular location; rather, they store and record either the physical presence or the lack of physical presence of individuals, vehicles, animals, or other physical entities. Adequate lighting should be provided based on the type of access monitoring device deployed.

  Access Limiting Systems. Access limiting systems may employ a combination of devices to physically control or prevent access to protected resources. Access limiting systems include both active and passive security devices such as fences, doors, safes, gates, and guards. They are often coupled with identification and monitoring systems to provide role-based access for specific individuals or groups of individuals.
- **People and Asset Tracking.** Locating people and vehicles in a large installation is important for safety reasons, and it is increasingly important for security reasons as well. Asset location technologies can be used to track the movements of people and vehicles within the plant, to ensure that they stay in authorized areas, to identify personnel needing assistance, and to support emergency response.

コンピュータへのアクセスが容易で、取り外し可能メディアドライブ（フロッピーディスク、CD、外付けハードディスク等）又は USB ポートが付いている場合、ドライブをロックするかコンピュータから取り外し、USB ポートを無効にすることができる。セキュリティ上のニーズ及びリスクに応じて、電源ボタンも無断で操作できないように、使用不能にするか物理的に保護するのがよい。セキュリティを最大化するため、サーバは鍵のかかるエリアに置き、認証メカニズム（キー等）を保護すべきである。また ICS ネットワーク上のネットワークデバイス（スイッチ、ルータ、ネットワークジャック、サーバ、ワークステーション、コントローラ等）は、許可された職員しか立ち入ることのできないセキュアな場所に置くべきである。セキュアな場所は、デバイスの環境要件にも適合しているべきである。

物理的セキュリティの多層防御ソリューションは、次のような属性を含んでいるべきである。

- **場所の保護。**既成の物理的セキュリティでは、考慮事項として通常多重セキュリティ対策のリングアーキテクチャに言及している。建物、施設、部屋、装備品その他情報資産の周りに能動的・受動的物理バリアーを設置し、物理的セキュリティ境界を構築する。場所を保護するための物理的セキュリティ対策にはフェンス、車止め溝、土盛り、壁、バリケード、ゲートその他がある。大抵の組織では、まずフェンス、ガードマン待機所、ゲート及び施錠ドアによりプラントへの立入を防ぐことで、この多重モデルを取り込んでいる。
- **立入管理。**立入管理システムは、許可を受けた人員だけが管理空間に立ち入ることができるようにすべきである。立入管理システムは柔軟性を備えているべきである。立入の必要性は時間（日中・夜間シフト勤務）、訓練レベル、雇用形態、役職、プラントの状態その他多種多様な要因で生じる。システムは、立入許可を受けた人員が自らをどう自称しているか確認できなければならない（通常、立入カードや鍵等の所持物、個人識別番号[PIN]等何らかの知識、バイオメトリックデバイスによる個人情報等を利用する）。立入管理は高い信頼性を持つべきであるが、プラント職員の恒常任務や緊急任務を妨げてはならない。立入管理をプロセスシステムに取り込めば、セキュリティアクセスのみならず、物理的・人的資産の追跡も可能になり、緊急時の対応時間が著しく短縮され、従業員を安全な場所へ誘導する助けとなり、全体的な生産性を高めることができる。エリア内では、ネットワークやコンピュータキャビネットへのアクセスは、ネットワーク技師・エンジニア、コンピュータ保守要員等、必要な人員のみに制限される。装備品キャビネットは施錠し、配線を整理してキャビネット内に納めるべきである。全てのコンピュータを安全なラックに納め、周辺延長技術を利用して、ラックのコンピュータにマンマシンインタフェースを接続する。

  立入監視システム。立入監視システムにはビデオカメラ、センサ及び多様な識別システムが含まれる。システムには駐車場、コンビニエンスストア、航空会社のセキュリティ監視用のカメラも含まれる。これらデバイスは特定の場所への立入を防ぐのではなく、個人、車両、動物その他物体の存在の有無を保存し記録する。監視デバイスの種類に応じて適切な照明を備えるべきである。

  立入制限システム。立入制限システムは、保護リソースを物理的に管理するデバイス又は保護リソースへのアクセスを防止するデバイスを併用する。立入制限システムには、フェンス、ドア、金庫、ゲート、監視等の能動的・受動的セキュリティデバイスが含まれる。識別・監視システムと連動することが多く、特定の個人やグループに役割に応じたアクセスを与える。
- **人員・資産の追跡。**広大な産業施設では、安全上の理由から人や車両を見つけ出すことが重要で、セキュリティ上の理由からもますます重要になっている。プラント内での人や車両の移動を追跡できる資産位置標定技術を使用すれば、許可エリア内にとどまり、支援を必要としている職員を識別し、緊急対応を支援できる。

- **Environmental Factors.** In addressing the security needs of the system and data, it is important to consider environmental factors. For example, if a site is dusty, systems should be placed in a filtered environment. This is particularly important if the dust is likely to be conductive or magnetic, as in the case of sites that process coal or iron. If vibration is likely to be a problem, systems should be mounted on rubber bushings to prevent disk crashes and wiring connection problems. In addition, the environments containing systems and media (e.g., backup tapes, floppy disks) should have stable temperature and humidity. An alarm to the process control system should be generated when environmental specifications such as temperature and humidity are exceeded.
- **Environmental Control Systems**. Heating, ventilation, and air conditioning (HVAC) systems for control rooms must support plant personnel during normal operation and emergency situations, which could include the release of toxic substances. Fire systems must be carefully designed to avoid causing more harm than good (e.g., to avoid mixing water with incompatible products). HVAC and fire systems have significantly increased roles in security that arise from the interdependence of process control and security. For example, fire prevention and HVAC systems that support industrial control computers need to be protected against cyber incidents.
- **Power.** Reliable power for the ICS is essential, so an uninterruptible power supply (UPS) should be provided. If the site has an emergency generator, the UPS battery life may only need to be a few seconds; however, if the site relies on external power, the UPS battery life may need to be hours. It should be sized, at a minimum, so that the system can be shutdown safely.

6.2.11.1 Control Center/Control Room

ICS-specific Recommendations and Guidance

Providing physical security for the control center/control room is essential to reduce the potential of many threats. Control centers/control rooms frequently have consoles continuously logged onto the primary control server, where speed of response and continual view of the plant is of utmost importance. These areas will often contain the servers themselves, other critical computer nodes, and sometimes plant controllers. It is essential that access to these areas be limited to authorized users only, using authentication methods such as smart or magnetic identity cards or biometric devices. In extreme cases, it may be considered necessary to make the control center/control room blast-proof, or to provide an offsite emergency control center/control room so that control can be maintained if the primary control center/control room becomes uninhabitable.

6.2.11.2 Portable Devices

ICS-specific Recommendations and Guidance

Computers and computerized devices used for ICS functions (such as PLC programming) should never be allowed to leave the ICS area. Laptops, portable engineering workstations and handhelds (e.g., 375 HART communicator) should be tightly secured and should never be allowed to be used outside the ICS network. Antivirus and patch management should be kept current.

- **環境要因。**システム及びデータのセキュリティニーズを検討する上で、環境要因を考慮に入れることが肝要である。例えば、現場がほこりっぽい場合、フィルタを導入した環境にシステムを設置すべきである。特に石炭や鉄の処理現場のように、塵芥に導電性や磁性がある場合には特に重要となる。振動が問題になりそうであれば、システムをラバーブッシング上に据え付け、ディスククラッシュや配線接続の問題を予防すべきである。またシステムとメディア（バックアップテープ、フロッピーディスク等）がある環境では、温度・湿度を一定に保つべきである。プロセス制御システムのアラームは、温度・湿度といった環境仕様が限界を超えたときに発生すべきである。
- **環境制御システム。**制御室の暖房換気空調（HVAC）システムは、正常操業時及び緊急事態時にプラント職員を支援できなければならず、これには毒物の排出も含まれる。防火装置の設計は慎重に行い、利点よりも欠点が大きくならないようにしなければならない（水と相容れない物質の混合回避等）。
  プロセス制御とセキュリティの相互依存性により、HVAC システムと防火装置がセキュリティで果たす役割は著しく増大している。例えば、産業用制御コンピュータに対応した防火装置と HVAC システムは、サイバーインシデントから守る必要がある。
- **電源。**ICS には信頼性の高い電源が不可欠なため、無停電電源装置（UPS）を装備すべきである。現場に緊急用の発電機がある場合、UPS のバッテリ寿命は数秒程度でよいが、外部電源に依存している場合は、数時間もたなければならない。少なくとも大きさを定めて、システムが安全に遮断できるようにすべきである。

6.2.11.1　コントロールセンター/制御室

ICS 固有の推奨事項及びガイダンス

種々の脅威の可能性を減らすため、コントロールセンター/制御室の物理的セキュリティの確保が不可欠である。コントロールセンター/制御室には、プライマリ制御サーバに常続的に接続しているコンソールがある場合が多く、対応速度とプラントを継続的に見ることが極めて重要である。サーバその他の重要コンピュータノードがある場合が多く、ときにはプラントコントローラもある。コントロールセンター/制御室への立入は、スマートカード、磁気カード、バイオメトリックデバイス等を利用し、許可を受けたユーザに限定することが肝要である。極端な場合、コントロールセンター/制御室を防爆仕様にしたり、オフサイトの緊急用コントロールセンター/制御室を用意して、プライマリのコントロールセンター/制御室の立入不能時に制御を続行できるような検討も必要になろう。

6.2.11.2　ポータブルデバイス

ICS 固有の推奨事項及びガイダンス

ICS 機能用に利用するコンピュータ及びコンピュータデバイス（PLC プログラミング等）は、ICS エリアから搬出してはならない。ラップトップ、ポータブルエンジニアリングワークステーション及びハンドヘルド（375 HART コミュニケータ等）のセキュリティは厳格にし、ICS ネットワーク外では使用すべきでない。アンチウイルス及びパッチの管理を最新状態に保つべきである。

6.2.11.3 Cabling

ICS-specific Recommendations and Guidance

Cabling design and implementation for the control network should be addressed in the cybersecurity plan. Unshielded twisted pair communications cable, while acceptable for the office environment, is generally not suitable for the plant environment due to its susceptibility to interference from magnetic fields, radio waves, temperature extremes, moisture, dust, and vibration. Industrial RJ-45 connectors should be used in place of other types of twisted pair connectors to provide protection against moisture, dust and vibration. Fiber-optic cable and coaxial cable are often better network cabling choices for the control network because they are immune to many of the typical environmental conditions including electrical and radio frequency interference found in an industrial control environment. Cable and connectors should be color-coded and labeled so that the ICS and IT networks are clearly delineated and the potential for an inadvertent cross-connect is reduced. Cable runs should be installed so that access is minimized (i.e., limited to authorized personnel only) and equipment should be installed in locked cabinets with adequate ventilation and air filtration.

6.2.12 Planning

A security plan is a formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. The security controls that fall within the NIST SP 800-53 Planning (PL) family provide the basis for developing a security plan. These controls also address maintenance issues for periodically updating a security plan. A set of rules describes user responsibilities and expected behavior regarding information system usage with provision for signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the information system.

Supplemental guidance for the PL controls can be found in the following documents:

- NIST SP 800-18 provides guidance on preparing rules of behavior [19].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

ICS-specific Recommendations and Guidance

A security plan for an ICS should build on appropriate existing IT security experience, programs, and practices. However, the critical differences between IT and ICS addressed in Section 2.4 will influence how security will be applied to the ICS. A forward-looking plan is needed to provide a method for continuous security improvements. Whenever a new system is being designed and installed, it is imperative to take the time to address security throughout the lifecycle, from architecture to procurement to installation to maintenance to decommissioning. ICS security is a rapidly evolving field requiring the security planning process to constantly explore emerging ICS security capabilities as well as new threats that are identified by organizations such as the ICS-CERT.

6.2.11.3 ケーブル配線

ICS 固有の推奨事項及びガイダンス

制御ネットワーク用ケーブル配線の設計及び実装は、サイバーセキュリティ計画書の中で取り上げるべきである。通信用のシールドのない撚り対線は、オフィス環境では受け入れられるが、通常プラント環境では磁場、無線周波数、温度の寒暖、湿気、塵芥及び振動による干渉を受けやすいため不向きである。湿気・塵芥・振動対策として、産業用 RJ-45 コネクタをその他の撚り対線コネクタの代わりに使用すべきである。光ケーブル及び同軸ケーブルは、産業用制御環境によくある電気・無線周波数干渉等の環境条件の多くに影響を受けないため、制御ネットワーク用の配線選択肢として良い場合が多い。ケーブル及びコネクタにはカラーコードとラベルを付け、ICS ネットワークと IT ネットワークの識別を明確にし、うっかり交差配線しないようにすべきである。配線は、配線へのアクセスが最小で済むように行い（許可された職員のみ）、装備品は施錠できるキャビネットに収納し、換気と空気濾過を行う。

6.2.12 プランニング

セキュリティ計画書は、情報システムのセキュリティ要件を概説した正式文書で、その要件を満足する実施中又は計画中のセキュリティ対策について記述する。NIST SP 800-53 プランニング（PL）ファミリには、セキュリティ計画書を作成するための根拠が示されている。管理策には、セキュリティ計画書を定期的に更新するための保守問題が含まれる。一連の規則は、情報システムの利用に関するユーザの責任と期待される行動について説明し、情報システムへのアクセス許可を得る前に、ユーザが行動規則を読み、理解し、遵守する旨の署名入り同意書が付いている。

PL 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-18：行動規則の作成に係るガイダンス[19]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

ICS 固有の推奨事項及びガイダンス

ICS のセキュリティ計画書は、該当する既存の IT セキュリティ経験、プログラム及び規範を基本とする。セクション 2.4 で説明した IT と ICS の重要な相違は、ICS へのセキュリティ適用方法に影響する。絶えずセキュリティを改善してための方法を示すため、前向きな計画書が必要となる。新しいシステムを設計・導入する場合は常に、アーキテクチャから調達、導入、保守、廃棄に至るまで、ライフサイクル全体を見通したセキュリティについて考察する時間を取り分けることが肝要である。ICS セキュリティは急速に進展中の分野で、セキュリティのプランニングプロセスでは、ICS セキュリティの新興機能と、ICS-CERT などの機関により特定された新しい脅威を絶えず探索することが求められる。

6.2.13 Personnel Security

The security controls that fall within the NIST SP 800-53 Personnel Security (PS) family provide policies and procedures to reduce the risk of human error, theft, fraud, or other intentional or unintentional misuse of information systems.

Supplemental guidance for the PS controls can be found in the following documents:

- NIST SP 800-35 provides guidance on information technology security services [44].
- NIST SP 800-73 provides guidance on interfaces for personal identity verification [49].
- NIST SP 800-76 provides guidance on biometrics for personal identity verification [50].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

Personnel security measures are meant to reduce the possibility and risk of human error, theft, fraud, or other intentional or unintentional misuse of informational assets. There are three main aspects to personnel security:

- **Hiring Policies.** This includes pre-employment screening such as background checks, the interview process, employment terms and conditions, complete job descriptions and detailing of duties, terms and condition of employment, and legal rights and responsibilities of employees or contractors.
- **Organization Policies and Practices.** These include security policies, information classification, document and media maintenance and handling policies, user training, acceptable usage policies for organization assets, periodic employee performance reviews, appropriate background checks, and any other policies and actions that detail expected and required behavior of organization employees, contractors, and visitors. Organization policies to be enforced should be written down and readily available to all workers through an employee handbook, distributed as email notices, located in a centralized resource area, or posted directly at a worker's area of responsibility.
- **Terms and Conditions of Employment.** This category includes job and position responsibilities, notification to employees of terminable offenses, disciplinary actions and punishments, and periodic employee performance reviews.

ICS-specific Recommendations and Guidance

Positions should be categorized with a risk designation and screening criteria, and individuals filling a position should be screened against this criteria as well as complete an access agreement before being granted access to an information system. Personnel should be screened for the critical positions controlling and maintaining the ICS.

Additionally, training programs should be carefully developed to ensure that each employee has received training relevant and necessary to his job functions. Further, ensure that the employees have demonstrated their competence in their job functions.

6.2.13 人員のセキュリティ

NIST SP 800-53 の人員のセキュリティ（PS）ファミリに含まれるセキュリティ対策は、人的過誤、盗難、詐欺その他故意又は不作為による情報システムの誤用を減らすためのポリシー及び手順を定めている。

PS 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-35：情報技術セキュリティサービスに係るガイダンス[44]
- NIST SP 800-73：個人身元確認インタフェースに係るガイダンス[49]
- NIST SP 800-76：個人身元確認バイオメトリクスに係るガイダンス[50]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

人員のセキュリティ対策は、人的過誤、盗難、詐欺その他故意又は不作為による情報資産の誤用機会を減らすためのものである。人員のセキュリティには次の 3 つの面がある。

- **雇用ポリシー。**これに背景調査、面接プロセス等の雇用前のスクリーニング、雇用契約、職務明細、雇用条件、従業員・請負業者の法的権利と責務が含まれる。
- **組織のポリシー及び規範。**これに含まれるのはセキュリティポリシー、情報区分、文書及びメディアの維持及び取扱ポリシー、ユーザ訓練、組織資産の受け入れられる利用ポリシー、従業員定期勤務評定、関連する背景調査その他従業員・請負業者・来訪者の期待・義務行動を詳述したポリシー及び行為である。施行すべき組織のポリシーは書面にし、従業員ハンドブックを通じて全員が容易に利用でき、電子メール通知で配布され、集中リソースエリアに置かれ、又は従業員の担当エリアに掲示すべきである。
- **雇用条件。**これには職務及び役職の責務、従業員に対する契約解除となる違反の通知、懲罰及び定期勤務評定が含まれる。

ICS 固有の推奨事項及びガイダンス

役職はリスク指定及び選抜基準で分類され、役職に就く個人はこの基準に照らして選抜され、情報システムへのアクセス権を得る前にアクセス同意書を作成すべきである。ICS の制御及び保守を担当する重要役職に就く職員は選抜すべきである。

また慎重に訓練プログラムを作成し、各従業員が職位に応じた訓練を受けられるようにすべきである。更に従業員が職務における適性を実証できるようにする。

6.2.14 Risk Assessment

The security controls that fall within the NIST SP 800-53 Risk Assessment (RA) family provide policy and procedures to develop, distribute, and maintain a documented risk assessment policy that describes purpose, scope, roles, responsibilities, and compliance as well as policy implementation procedures. An information system and associated data is categorized based on the security objectives and a range of risk levels. A risk assessment is performed to identify risks and the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of an information system and data. Also included in these controls are mechanisms for keeping risk assessments up-to-date and performing periodic testing and vulnerability assessments.

Supplemental guidance for the RA controls can be found in the following documents:

- NIST SP 800-30 provides guidance on conducting risk assessments and updates [79].
- NIST SP 800-39 provides guidance on risk management at all organizational levels [20].
- NIST SP 800-40 provides guidance on handling security patches [40].
- NIST SP 800-115 provides guidance on network security testing [41].
- NIST SP 800-60 provides guidance on determining security categories for information types [25].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

ICS-specific Recommendations and Guidance

Organizations must consider the potential consequences resulting from an incident on an ICS. Well-defined policies and procedures lead to mitigation techniques designed to thwart incidents and manage the risk to eliminate or minimize the consequences. The potential degradation of the physical plant, economic status, or stakeholder/national confidence could justify mitigation.

For an ICS, a very important aspect of the risk assessment is to determine the value of the data that is flowing from the control network to the corporate network. In instances where pricing decisions are determined from this data, the data could have a very high value. The fiscal justification for mitigation has to be derived by comparing the mitigation cost to the effects of the consequence. However, it is not possible to define a one-size-fits-all set of security requirements. A very high level of security may be achievable but undesirable in many situations because of the loss of functionality and other associated costs. A well-thought-out security implementation is a balance of risk versus cost. In some situations the risk may be safety, health, or environment-related rather than purely economic. The risk may result in an unrecoverable consequence rather than a temporary financial setback

6.2.15 System and Services Acquisition

The security controls that fall within the NIST SP 800-53 System and Services Acquisition (SA) family provide the basis for developing policies and procedures for acquisition of resources required to adequately protect an information system. These acquisitions are based on security requirements and security specifications. As part of the acquisition procedures, an information system is managed using a system development life cycle methodology that includes information security considerations. As part of acquisition, adequate documentation must be maintained on the information system and constituent components.

6.2.14 リスク評価

NIST SP 800-53 のリスク評価（RA）ファミリに含まれるセキュリティ対策には、目的、適用範囲、役割、責任、コンプライアンス及びポリシー実施手順を記述したリスク評価ポリシー文書を作成・配布・保持するためのポリシー及び手順が定められている。情報システム及び関連データは、セキュリティ目標及びリスクレベルの範囲を基に分類される。リスク評価はリスクと、不正アクセス、利用、漏洩、妨害、改変又は情報システム・データの破壊から生じ得る損害の規模を明らかにするために実施する。またリスク評価を最新状態に保ち、定期的検証及び脆弱性評価を実施するためのメカニズムもこの管理で取り上げる。

RA 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-30：リスク評価の実施及び更新に係るガイダンス[79]
- NIST SP 800-39：あらゆる組織レベルにおけるリスク管理に係るガイダンス[20]
- NIST SP 800-40：セキュリティパッチの取扱に係るガイダンス[40]
- NIST SP 800-115：ネットワークセキュリティの試験に係るガイダンス[41]
- NIST SP 800-60：情報種類のセキュリティ分類判定に係るガイダンス[25]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

ICS 固有の推奨事項及びガイダンス

組織は ICS 上のインシデントから生じ得る結果を検討しなければならない。しっかり定義されたポリシー及び手順は、インシデントを阻止し、リスクを管理して結果を排除又は最小限に食い止めるための緩和技術に通じる。プラント、経済状態又は利害関係者・国民の信頼感が低下することから、緩和策は是非とも必要となる。

ICS におけるリスク評価の極めて重要な一面は、制御ネットワークから企業ネットワークへ流れるデータの価値を判定することである。例えば、このデータを基に価格を決定する場合、データは極めて高い価値を持つ。緩和を正当化する会計上の理由は、緩和に要するコストと結果から生じる影響の比較から引き出さなければならない。とは言え、1 つで全てに適合するようなセキュリティ要件を定義することは不可能である。高レベルのセキュリティは達成可能ではあるが、機能が失われその他関連コストがかかることから、大抵は望ましくない。よく検討されたセキュリティは、リスクとコストのバランスが取れている。ある場合、リスクは純粋な経済よりも、安全、健康又は環境関連となる。リスクは、一時的な財政上の失敗というより、取り返しのつかない結果を招くことがある。

6.2.15 システム及びサービスの取得

NIST SP 800-53 のシステム及びサービスの取得（SA）ファミリに含まれるセキュリティ対策には、情報システムを守るために必要とされるリソースの取得に係るポリシー及び手順の策定根拠が示されている。取得は、セキュリティ要件及びセキュリティ仕様書に基づく。取得手順の一環として、情報システムは、情報セキュリティの考慮事項を含めたシステム開発ライフサイクル方法論を利用して管理される。取得の一環として、情報システム及び構成コンポーネントに関する文書を保持しなければならない。

The SA family also addresses outsourced systems and the inclusion of adequate security controls by vendors as specified by the supported organization. Vendors are also responsible for configuration management and security testing for these outsourced information systems.

Supplemental guidance for the SA controls can be found in the following documents:

- NIST SP 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products [42].
- NIST SP 800-27 provides guidance on engineering principles for information system security [43].
- NIST SP 800-35 provides guidance on information technology security services [44].
- NIST SP 800-36 provides guidance on the selection of information security products [45].
- NIST SP 800-64 provides guidance on security considerations in the system development life cycle [46].
- NIST SP 800-65 provides guidance on integrating security into the capital planning and investment control process [47].
- NIST SP 800-70 provides guidance on configuration settings for information technology products [26].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

ICS-specific Recommendations and Guidance

The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks, and desktop environments should be addressed in a contract agreed between the parties. External suppliers that have an impact on the security of the organization must be held to the same security policies and procedures to maintain the overall level of ICS security. Security policies and procedures of second and third-tier suppliers should also be in compliance with corporate cybersecurity policies and procedures in the case that they impact ICS security.
DHS has developed a procurement language document [48] for specifying security requirements when procuring new systems or maintaining existing systems.

6.2.16 System and Communications Protection

The security controls that fall within the NIST SP 800-53 System and Communications Protection (SC) family provide policy and procedures for protecting systems and data communications components.

Supplemental guidance for the SC controls can be found in the following documents:

- NIST SP 800-28 provides guidance on active content and mobile code [69].
- NIST SP 800-52 provides guidance on Transport Layer Security (TLS) Implementations [70].
- NIST SP 800-56 provides guidance on cryptographic key establishment [71].
- NIST SP 800-57 provides guidance on cryptographic key management [72].

SA ファミリでは外注システムや、サポートを受ける組織が指定したベンダーによるセキュリティ対策の取り込みについても取り上げている。ベンダーは、このような外注情報システムの構成管理及びセキュリティ試験にも責任を負う。

SA 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-23：試験・評価済み情報技術製品の取得及び利用に係るガイダンス[42]
- NIST SP 800-27：情報システムセキュリティのエンジニアリング原則に係るガイダンス[43]
- NIST SP 800-35：情報技術セキュリティサービスに係るガイダンス[44]
- NIST SP 800-36：情報セキュリティ製品の選定に係るガイダンス[45]
- NIST SP 800-64：システム開発ライフサイクルにおけるセキュリティ考慮事項に係るガイダンス[46]
- NIST SP 800-65：資本計画及び投資管理プロセスへのセキュリティ統合に係るガイダンス[47]
- NIST SP 800-70：情報技術製品の構成設定に係るガイダンス[26]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

ICS 固有の推奨事項及びガイダンス

情報システム、ネットワーク及びデスクトップ環境の全部又は一部の管理・対策を外注する際のセキュリティ要件は、両当事者間の契約書で取り上げるべきである。組織のセキュリティに影響を与える社外サプライヤは、ICS セキュリティの全体レベルを維持するための同じセキュリティポリシー及び手順に従わなければならない。孫請け以降のサプライヤのセキュリティポリシー及び手順も、ICS セキュリティに影響する場合は、企業のサイバーセキュリティポリシー及び手順を遵守すべきである。

DHS は、新規システム調達又は既存システム保守の際のセキュリティ要件を定めるための調達言語文書[48]を作成した。

6.2.16 システム及び通信保護

NIST SP 800-53 のシステム及び通信保護（SC）ファミリに含まれるセキュリティ対策には、システム及びデータ通信コンポーネントを保護するためのポリシー及び手順が定められている。

SC 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-28：アクティブコンテンツ及びモバイルコードに係るガイダンス[69]
- NIST SP 800-52：トランスポートレイヤーセキュリティ（TLS）の実装に係るガイダンス[70]
- NIST SP 800-56：暗号鍵の設定に係るガイダンス[71]
- NIST SP 800-57：暗号鍵の管理に係るガイダンス[72]

- NIST SP 800-58 provides guidance on security considerations for VoIP technologies [73].
- NIST SP 800-63 provides guidance on remote electronic authentication [53].
- NIST SP 800-77 provides guidance on IPsec VPNs [74].

6.2.16.1 Encryption

Encryption is the cryptographic transformation of data (called plaintext) into a form (called ciphertext) that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called decryption, which is a transformation that restores encrypted data to its original state [75].

ICS-specific Recommendations and Guidance

Before deploying encryption, first determine if encryption is an appropriate solution for the specific ICS application, because authentication and integrity are generally the key security issues for ICS applications. Other cryptographic solutions such as cryptographic hashes should also be considered.

The use of encryption within an ICS environment could introduce communications latency due to the additional time and computing resources required to encrypt, decrypt, and authenticate each message. For ICS, any latency induced from the use of encryption, or any other security technique, must not degrade the operational performance of the end device or system. Before deploying encryption within an ICS environment, solutions should go through extensive performance testing. Encryption at OSI Layer 2 should be considered, rather than at Layer 3 to reduce encryption latency.

In addition, encrypted messages are often larger than unencrypted messages due to one or more of the following:

- Additional checksums to reduce errors.
- Protocols to control the cryptography.
- Padding (for block ciphers).
- Authentication procedures.
- Other required cryptographic processes.

Cryptography also introduces key management issues. Sound security policies require periodic key changes. This process becomes more difficult as the geographic size of the ICS increases, with extensive SCADA systems being the most severe example. Because site visits to change keys can be costly and slow, it is useful to be able to change keys remotely.

If cryptography is selected, the most effective safeguard is to use a complete cryptographic system approved by the NIST/ Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP)[41]. Within this program standards are maintained to ensure that cryptographic systems were studied carefully for weaknesses by a wide range of experts, rather than being developed by a few engineers in a single organization. At a minimum, certification makes it probable that:

- Some method (such as counter mode) will be used to ensure that the same message does not

[41] Information on the CMVP can be found on the CMVP web site http://csrc.nist.gov/cryptval/cmvp.htm.

- NIST SP 800-58：VoIP 技術のセキュリティ考慮事項に係るガイダンス[73]
- NIST SP 800-63：遠隔電子認証に係るガイダンス[53]
- NIST SP 800-77：IPsec VPNs に係るガイダンス[74]

6.2.16.1 暗号化

暗号化とはデータ（平文と呼ばれる）を暗号変換して、ある形態（暗号文と呼ばれる）にすることで、データの基の意味を秘匿し、知られたり利用されたりできないようにする。変換が逆変換も可能な場合、そのプロセスは復号と呼ばれ、暗号化されたデータを元の状態に戻す[75]。

ICS 固有の推奨事項及びガイダンス

認証と完全性は、総じて ICS 用途では主要なセキュリティ問題となるため、暗号化を行う前に、まずそれが特定の ICS 用途に適したソリューションかどうかを判定する。暗号学的ハッシュ等、その他の暗号ソリューションについても考慮すべきである。

ICS 環境で暗号を使用すると、各メッセージの暗号、復号及び認証に付加的な時間と計算リソースを要するため、通信の待ち時間が生じる場合がある。ICS では、暗号の使用又は他のセキュリティ技術から生じる待ち時間は、エンドデバイスやシステムの運用パフォーマンスを低下させてはならない。ICS 環境で暗号を展開する前に、徹底的なパフォーマンス試験を行うべきである。暗号化の待ち時間を短縮するため、OSI レイヤー3 ではなくレイヤー2 での暗号化を考慮すべきである。

また以下に挙げた理由から、暗号メッセージは平文メッセージより大きくなることが多い。

- エラーを減らすための付加的なチェックサム
- 暗号化を制御するためのプロトコル
- パディング（ブロック暗号用）
- 認証手順
- 他の必須暗号化プロセス

暗号化には鍵管理の問題も生じる。健全なセキュリティポリシーには定期的な鍵の変更が必須である。このプロセスは、ICS の地理的な規模が拡大するといっそう難しくなる。典型例が大規模 SCADA システムである。現場に出向いてキー変更を行うのはコストと時間がかかるため、遠隔操作が便利である。

暗号化の導入を選択したなら、最も効果的な安全対策は、 カナダ通信安全保障局（CSE）の暗号モジュール妥当性検証プログラム（CMVP）[42]が承認した完全な暗号化モジュールを利用することである。このプログラムでは、暗号化システムは単一組織の少数エンジニアに開発を委ねるのではなく、広範な専門家がその弱点を慎重に調査するように基準を定めている。少なくとも認定書は以下の可能性を認めている。

- 特定の方法（カウンターモード等）を利用して、同じメッセージが毎回同じ値を生成しないようにする。

[42] CMVP に関する情報は次の CMVP サイトにある。http://csrc.nist.gov/cryptval/cmvp.htm.
訳注)我が国では、FIPS140-2 に起源を持つ JIS X 19790 に基づく暗号モジュール試験及び認証制度を、IPA セキュリティセンターが運用している(http://www.ipa.go.jp/security/jcmvp/index.html

generate the same value each time.

- ICS messages are protected against replay and forging.
- Key management is secure throughout the life cycle of the key.
- The system is using an effective random number generator.
- The entire system has been implemented securely.

Even then, the technology is effective only if it is an integral part of an effectively enforced information security policy. American Gas Association (AGA) report 12-1 [5] contains an example of such a security policy. While it is directed toward a natural gas SCADA system, many of its policy recommendations could apply to any ICS.

For an ICS, encryption can be deployed as part of a comprehensive, enforced security policy. Organizations should select cryptographic protection based on a risk assessment and the identified value of the information being protected and ICS operating constraints. Specifically, a cryptographic key should be long enough so that guessing it or determining it through analysis takes more effort, time, and cost than the value of the protected asset.

The encryption hardware should be protected from physical tampering and uncontrolled electronic connections. Assuming cryptography is the appropriate solution, organizations should select cryptographic protection with remote key management if the units being protected are so numerous or geographically dispersed that changing keys is difficult or expensive.

Use separate plaintext and ciphertext ports unless the network absolutely requires the restriction to pass both plaintext and ciphertext through each port.

Use only modules that can be certified to comply with a standard, such as FIPS 140-2 [90] through the Cryptographic Module Validation Program (CMVP).

6.2.16.2 Virtual Private Network (VPN)

One method of encrypting communication data is through a VPN, which is a private network that operates as an overlay on a public infrastructure, so that the private network can function across a public network. The most common types of VPN technologies implemented today are:

- **Internet Protocol Security (IPsec).** IPsec is a set of standards defined by IETF to govern the secure communications of data across public networks at the IP layer. IPsec is included in many current operating systems. The intent of the standards is to guarantee interoperability across vendor platforms; however, the reality is that the determination of interoperability of multi-vendor implementations depends on specific implementation testing conducted by the end-user organization. IPsec supports two encryption modes: transport and tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure tunnel mode adds a new header to each packet and encrypts both the original header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet. The protocol has been continually enhanced to address specific requirements, such as extensions to the protocol to address individual user authentication and NAT device transversal. These extensions are typically vendor-specific and can lead to interoperability issues primarily in host-to-security gateway environments. NIST SP 800-77 provides guidance on IPsec VPNs [74].

- ICS メッセージがリプレーや欺瞞から保護される。
- キー管理がキーのライフサイクル中セキュアになる。
- システムが効果的な乱数発生器を使用する。
- システム全体がセキュアに実装される。

それでもこの技術が効果的であるためには、それが有効に実施されている情報セキュリティポリシーの不可欠な一部になっている場合のみである。米国ガス協会（AGA）報告書 12-1[5]には、このようなセキュリティポリシーの一例が載っている。天然ガス SCADA システム向けのものではあるが、そのポリシー推奨事項の多くはどの ICS にも当てはまる。

ICS では、暗号化は包括的なセキュリティ施行の一環として展開可能である。組織は、リスク評価、保護される情報の価値及び ICS 業務の制約事項を基に、暗号化保護を選択すべきである。特に暗号鍵は十分長くし、解析による推測・判別に要する労力・時間・コストが、保護された資産価値に見合わないようにすべきである。

暗号化ハードウエアは、物理的改竄や管理外の電子接続から保護すべきである。暗号化がふさわしいソリューションであるとみなすなら、保護する部署が多く地理的に分散していてキー変更が困難・割高になる場合、組織は遠隔キー管理の可能な暗号化保護を選択すべきである。

ネットワークが平文も暗号文も各ポートから渡すことを絶対的に制限しているのでなければ、平文ポートと暗号文ポートを分離して使用する。

暗号モジュール妥当性検証プログラム（CMVP）を通じて、FIPS 140-2 [90]等の規格に適合したモジュールのみを使用する。

6.2.16.2 仮想プライベートネットワーク（VPN）

通信データを暗号化する 1 つ方法は VPN を経由することである。VPN は公開インフラ上のオーバーレイとして機能し、プライベートネットワークは公開ネットワークとの間で稼働する。今日実装されている最も一般的な VPN 技術には以下がある。

- **インターネットプロトコルセキュリティ（IPSec）。**IPSec は IETF が定義した規格で、IP レイヤーにおける公開ネットワークを越えて、セキュアなデータ通信を制御する。IPSec は現行 OS の多くに組み込まれている。この規格の目的は、ベンダープラットホーム間の相互運用性を保守することにある。ただし現実には、複数ベンダー実装間の相互運用性の判定は、エンドユーザ組織が行う個別の実装試験に左右される。IPSec は、トランスポートとトンネルという 2 つの暗号モードに対応している。トランスポートモードは、各パケットのデータ部分（ペイロード）のみを暗号化し、ヘッダーはそのままにする。よりセキュアなトンネルモードは、各パケットに新しいヘッダーを付け、元のヘッダーとペイロードをともに暗号化する。受信側では、IPSec に適合したデバイスが各パケットを復号する。プロトコルは継続的に拡張され、特定の要件にも対応するようになっており、個々のユーザ認証及び NAT デバイス横断に対応したプロトコル拡張もその中に含まれる。このような拡張は一般にベンダー固有のものであるため、特にホストからセキュリティゲートウェイ環境において、相互運用性の問題点となる。NIST SP 800-77 には、IPsec VPN に係るガイダンス[74]がある。

- **Secure Sockets Layer (SSL).** SSL provides a secure channel between two machines that encrypts the contents of each packet. The IETF made slight modifications to the SSL version 3 protocol and created a new protocol called Transport Layer Security (TLS). The terms "SSL" and "TLS" are often used interchangeably, and this document generically uses the SSL terminology. SSL is most often recognized for securing HTTP traffic; this protocol implementation is known as HTTP Secure (HTTPS). However, SSL is not limited to HTTP traffic; it can be used to secure many different application layer programs. SSL-based VPN products have gained acceptance because of the market for "clientless" VPN products. These products use standard Web browsers as clients, which have built-in SSL support. The "clientless" term means that there is no need to install or configure third-party VPN "client" software on users' systems. NIST SP 800-52 provides guidance on SSL configuration [70].
- **Secure Shell (SSH).** SSH is a command interface and protocol for securely gaining access to a remote computer. It is widely used by network administrators to remotely control Web servers and other types of servers. The latest version, SSH2, is a proposed set of standards from the IETF. Typically, SSH is deployed as a secure alternative to a telnet application. SSH is included in most UNIX distributions, and is typically added to other platforms through a third-party package.

ICS-specific Recommendations and Guidance

VPNs are most often used in the ICS environment to provide secure access from an untrusted network to the ICS control network. Untrusted networks can range from the Internet to the corporate LAN. Properly configured, VPNs can greatly restrict access to and from control system host computers and controllers, thereby improving security. They can also potentially improve control network responsiveness by removing unauthorized non-essential traffic from the intermediary network.

Other possible deployments include using either host-based or mini-standalone security gateways, either interposed before or running on individual control devices. This technique of implementing VPNs on an individual device basis can have significant administration overhead.

VPN devices used to protect control systems should be thoroughly tested to verify that the VPN technology is compatible with the application and that implementation of the VPN devices does not unacceptably affect network traffic characteristics.

- **セキュアソケットレイヤー（SSL）。**SSL は 2 台のマシン間にセキュアな経路を与え、各パケットの内容を暗号化する。IETF は SSL を若干改修して SSL バージョン 3 とし、トランスポートレイヤーセキュリティ（TLS）を新規プロトコルとして作成した。「SSL」と「TLS」は、用語として互換的に使われることが多く、本書では全般的に SSL の用語を用いる。SSL は HTTP トラフィックをセキュアにする技術としてよく知られており、このプロトコル実装は HTTP セキュア（HTTPS）として知られている。しかし SSL は HTTP トラフィックに限定されない。多様なアプリケーション層プログラムをセキュアにするために利用される。SSL ベースの VPN 製品は「クライアントレス」VPN 製品市場のせいで、受け入れられている。こうした製品では、SSL サポートが内蔵された標準的ウェブブラウザーをクライアントとして利用する。「クライアントレス」とは、サードパーティの VPN「クライアント」ソフトウエアをユーザシステムにインストール又は設定する必要がないという意味である。NIST SP 800-52 には、SSL の設定に係るガイダンス[70]がある。
- **セキュアシェル（SSH)。**SSH は、遠隔コンピュータへのセキュアなアクセスを得るためのコマンドインタフェース及びプロトコルである。ウェブサーバその他のサーバを遠隔操作するため、広くネットワーク管理者に利用されている。最新バージョンの SSH2 が新しい規格として、IETF から提唱されている。一般に SSH は、テルネットに代わるセキュアな代替手段として展開されている。SSH はほとんどの UNIX ディストリビューションに組み込まれており、通常、サードパーティパッケージを通じて、他のプラットホームにも追加されている。

ICS 固有の推奨事項及びガイダンス

VPN は、信頼の置けないネットワークから ICS 制御ネットワークへセキュアにアクセスするため、ICS 環境で利用されることが多い。信頼の置けないネットワークとは、インターネットから企業 LAN まで多岐にわたる。正しく設定すれば、VPN は制御システムのホストコンピュータおよびコントローラとのアクセスを著しく制限し、セキュリティを改善する。また未許可の不要トラフィックを媒介ネットワークから除去することで、制御ネットワークの応答感度も改善できる。

その他可能な展開としては、ホストベース又は小型のスタンドアローンセキュリティゲートウェイを個々の制御デバイスの前面に又は連続で配置して使用する案もある。個々のデバイスごとに VPN を実装するこの技術は、管理オーバーヘッドが大きくなる。

制御システムの保護に使用する VPN デバイスは、徹底的に試験を行い、VPN 技術がアプリケーションに適合していること、VPN デバイスの実装によりネットワークトラフィック特性が許容限度を超えて影響されないことを確認すべきである。

6.2.17 System and Information Integrity

Maintaining system and information integrity assures that sensitive data has not been modified or deleted in an unauthorized and undetected manner. The security controls that fall within the NIST SP 800-53 System and Information Integrity (SI) family provide policies and procedures for identifying, reporting, and correcting information system flaws. Controls exist for malicious code detection, spam and spyware protection, and intrusion detection, although they may not be appropriate for all ICS applications. Also provided are controls for receiving security alerts and advisories, and the verification of security functions on the information system. In addition, there are controls within this family to detect and protect against unauthorized changes to software and data, provide restrictions to data input and output, and check for the accuracy, completeness, and validity of data as well as handle error conditions, although they may not be appropriate for all ICS applications.

Supplemental guidance for the SI controls can be found in the following documents:

- NIST SP 800-40 provides guidance on security patch installation [40].
- NIST SP 800-94 provides guidance on Intrusion Detection and Prevention (IDP) Systems [55].
- NIST SP 800-100 provides guidance on information security governance and planning [27].

ICS-specific Recommendations and Guidance

Controls exist for malicious code detection, spam and spyware protection, and intrusion detection, although they may not be appropriate for all ICS applications. ICS-specific recommendations and guidance for these controls are included in Sections **Error! Reference source not found.and 0**.

6.2.17 システム及び情報の保全

システム及び情報保全を維持することにより、要注意データが改変されず、無断で気づかないうちに削除されるようなことがなくなる。NIST SP 800-53 のシステム及び情報の保全（SI）ファミリに含まれるセキュリティ対策には、情報システムの欠陥を識別し、報告し、是正するためのポリシー及び手順が定められている。全ての ICS 用途に適合するわけではないが、悪意あるコードの検出、スパム及びスパイウエア保護及び侵入検知のための対策がある。またセキュリティアラートや勧告を受けるための対策や、情報システム上のセキュリティ機能の検証対策もある。加えて、全ての ICS 用途に適合するわけではないが、このファミリでは、ソフトウエアやデータへの無断変更を検出・防止するための対策、データ入出力を制限するための対策、データの正確性・完全性・妥当性を確認するための対策、エラー状態を処理するための対策もある。

SI 管理の補足的ガイダンスが以下の文書に掲載されている。

- NIST SP 800-40：セキュリティパッチのインストールに係るガイダンス[40]
- NIST SP 800-94：侵入検知及び防止に係るガイダンス[55]
- NIST SP 800-100：情報セキュリティガバナンス及びプランニングに係るガイダンス[27]

ICS 固有の推奨事項及びガイダンス

全ての ICS 用途に適合するわけではないが、悪意あるコードの検出、スパム及びスパイウエア保護及び侵入検知のための対策がある。これら対策に関する ICS 固有の推奨事項及びガイダンスがセクション **Error!Reference source not found.**and 0 にある。

6.2.17.1 Virus and Malicious Code Detection

Antivirus and malware code detection products evaluate files on a computer's storage devices against an inventory of known malware signature files. If one of the files on a computer matches the profile of a known virus, the virus is removed through a disinfection process (e.g., quarantine, deletion) so it cannot infect other local files or communicate across a network to infect other files. Antivirus software can be deployed on workstations, servers, firewalls and handheld devices.

ICS-specific Recommendations and Guidance

Antivirus tools only function effectively when installed, configured, running full-time, and maintained properly against the state of known attack methods and payloads. While antivirus tools are common security practice in IT computer systems, their use with ICS may require adopting special practices including compatibility checks, change management issues, and performance impact metrics. These special practices should be utilized whenever new signatures or new versions of antivirus software are installed.

Major ICS vendors recommend and even support the use of particular antivirus tools. In some cases, control system vendors may have performed regression testing across their product line for supported versions of a particular antivirus tool and also provide associated installation and configuration documentation. There is also an effort to develop a general set of guidelines and test procedures focused on ICS performance impacts to fill the gaps where ICS and antivirus vendor guidance is not available [56].

Generally:

- Windows, Unix, Linux systems, etc. used as consoles, engineering workstations, data historians, HMIs and general purpose SCADA and backup servers can be secured just like commercial IT equipment: install push- or auto-updated antivirus and patch management software with updates distributed via an antivirus server and patch management server located inside the process control network and auto-updated from the IT network.
- Follow vendor recommendations on all other servers and computers (DCS, PLC, instruments) that have time-dependent code, modified or extended the operating system or any other change that makes it different from any standard PC that one could buy at an office supply or computer store. Expect the vendor to make periodic maintenance releases that include security patches.

6.2.17.2 Intrusion Detection and Prevention

Intrusion detection systems (IDS) monitor events on a network, such as traffic patterns, or a system, such as log entries or file accesses, so that they can identify an intruder breaking into or attempting to break into a system [57]. IDS ensure that unusual activity such as new open ports, unusual traffic patterns, or changes to critical operating system files is brought to the attention of the appropriate security personnel.

The two most commonly used types of IDS are:

- **Network-Based IDS.** These systems monitor network traffic and generate alarms when they identify traffic that they deem to be an attack.

6.2.17.1 ウイルス及び悪意あるコードの検出

ウイルス及び悪意あるコードの検出製品は、コンピュータのストレージデバイス上にあるファイルを、既知のマルウエアシグネチャファイルの目録に照らして評価する。コンピュータ上のファイルの 1 つが既知のウイルスのプロファイルに合致すると、そのウイルスは消毒プロセス（検疫、削除等）を通じて排除され、他のローカルファイルやネットワークを越えた他のファイルへの感染力を失う。アンチウイルスソフトウエアはワークステーション、サーバ、ファイアウォール及びハンドヘルドデバイスに展開できる。

ICS 固有の推奨事項及びガイダンス

アンチウイルスツールはインストールされ、設定され、常時実行され、正しく維持されている場合にのみ、既知の攻撃方法及びペイロード状態に対して有効に機能する。IT コンピュータシステムでは一般的なセキュリティ規範となっているが、ICS で使用するには、整合性チェック、管理変更問題、パフォーマンス影響評価基準等の特別な規範を採用する必要がある。このような特別規範は、アンチウイルスソフトウエアの新規シグネチャや新バージョンをインストールしたときには必ず採用すべきである。

大手 ICS ベンダーは、特定のアンチウイルスツールの使用を推奨し、サポートも行っている。場合によっては、制御システムベンダーは、製品系列全体のリグレッション試験を行い、特定のアンチウイルスツールの各バージョンの対応状況を検証していることもあり、関係するインストール及び設定に関する文書も提供している。また ICS アンチウイルスベンダーガイダンスがない場合には、不足を補うため、ICS パフォーマンスの影響に特化した汎用的なガイドライン及び試験手順の作成にも取り組んでいる[56]。

一般的に、

- コンソール、エンジニアリングワークステーション、データヒストリアン、HMI、汎用 SCADA 及びバックアップサーバとして利用する Windows、Unix、Linux システム等は、市販の IT 装備品同様にセキュアにすることが可能である。その場合、プッシュ式又は自動更新式のアンチウイルス及びパッチ管理ソフトウエアをインストールする（更新はプロセス制御ネットワーク内にあるアンチウイルスサーバ及びパッチ管理サーバ経由で配布され、IT ネットワークから自動更新される）。
- 時間依存コードを持ち、OS を改修・拡張するか、その他の変更を加えて、市販の標準 PC とは異なっている上記以外の全てのコンピュータ（DCS、PLC、インスツルメンツ）については、ベンダーの推奨事項に従う。ベンダーが定期的にセキュリティパッチの入った保守リリースを提供することを期待する。

6.2.17.2 侵入検知及び防止

侵入検知システム（IDS）は、トラフィックパターン等のネットワークイベント、ログ項目やファイルアクセス等のシステムを監視し、システムに入り込む侵入者やシステムに入り込もうとする侵入者を見極めることができる[57]。IDS は、ポートの新規開設、通常と異なるトラフィックパターン、重要な OS ファイルへの変更といった普段と違う活動がセキュリティ担当職員の注意を引くようにする。

IDS が使用する一般的な種類は次の 2 つである。

- **ネットワークベース IDS。**システムはネットワークトラフィックを監視して、攻撃と見なされるトラフィックを特定するとアラームを発する。

- **Host-Based IDS.** This software monitors one or more types of characteristics of a system, such as application log file entries, system configuration changes, and access to sensitive data on a system and responds with an alarm or countermeasure when a user attempts to breach security.

ICS-specific Recommendations and Guidance

An effective IDS deployment typically involves both host-based and network-based IDS. In the current ICS environment, network-based IDS are most often deployed between the control network and the corporate network in conjunction with a firewall; host-based IDS are most often deployed on the computers that use general-purpose OSs or applications such as HMIs, SCADA servers, and engineering workstations. Properly configured, an IDS can greatly enhance the security management team's ability to detect attacks entering or leaving the system, thereby improving security. They can also potentially improve a control network's efficiency by detecting non-essential traffic on the network. However, even when IDS are implemented, security staff can primarily recognize individual attacks, as opposed to organized patterns of attacks over time. Network security monitoring and an understanding of the normal state of the ICS network can help distinguish attacks from transient conditions, and both trigger and provide information into events that are outside the normal state.

Current IDS and IPS products are effective in detecting and preventing well-known Internet attacks, but until recently they have not addressed ICS protocol attacks. IDS and IPS vendors are beginning to develop and incorporate attack signatures for various ICS protocols such as Modbus, DNP3, and ICCP [58].

6.2.17.3 Patch Management

Patches are additional pieces of code that have been developed to address specific problems or flaws in existing software. Vulnerabilities are flaws that can be exploited, enabling unauthorized access to IT systems or enabling users to have access to greater privileges than authorized.

A systematic approach to managing and using software patches can help organizations to improve the overall security of their IT systems in a cost-effective way. Organizations that actively manage and use software patches can reduce the chances that the vulnerabilities in their IT systems can be exploited; in addition, they can save time and money that might be spent in responding to vulnerability-related incidents.

NIST SP 800-40 Revision 3 [40] provides guidance for organizational security managers who are responsible for designing and implementing security patch and vulnerability management programs and for testing the effectiveness of the programs in reducing vulnerabilities. The guidance is also useful to system administrators and operations personnel who are responsible for applying and testing patches and for deploying solutions to vulnerability problems.

ICS-specific Recommendations and Guidance

Applying patches to OS components creates another situation where significant care should be exercised in the ICS environment. Patches should be adequately tested (e.g., off-line on a comparable ICS) to determine the acceptability of side effects. Regression testing is advised. It is not uncommon for patches to have an adverse effect on other software. A patch may remove a vulnerability, but it can

■ **ホストベース IDS。**このソフトウエアは、アプリケーションログファイルエントリ、システム設定変更、システム上の要注意データへのアクセスといったシステム特性タイプを 1 つか複数監視して、ユーザがセキュリティ違反をもくろむと、アラーム又は対策をもって対応する。

ICS 固有の推奨事項及びガイダンス

効果的な IDS の展開には、通常ホストベースとネットワークベースの IDS がともに含まれる。現在の ICS 環境では、ネットワークベース IDS は、制御ネットワークとファイアウォール経由の企業ネットワークとの間で展開されることが多い。一方ホストベース IDS は、汎用 OS や HMI、SCADA サーバ、エンジニアリングワークステーション等のアプリケーションを使用するコンピュータで展開されることが多い。正しく設定すれば、IDS はセキュリティチームの能力を著しく向上させ、システムへの侵入・退出を検知し、セキュリティを改善する。またネットワーク上の不要なトラフィックを検出して、制御ネットワークの効率も改善できる。ただし IDS を実装した場合でも、セキュリティ要員は、経時的な攻撃の組織的パターンとは反対に、個々の攻撃を認識できる。ネットワークセキュリティ監視及び ICS ネットワークの正常状態に対する理解があれば、過渡的状態からの攻撃を見極め、正常状態を逸脱したイベントに対してトリガーと情報を発信しやすくなる。

現在の IDS 及び IPS 製品は、良く知られたインターネット攻撃の検知・防止に効果があるが、最近になるまで ICS プロトコル攻撃には対応していなかった。IDS 及び IPS ベンダーは、Modbus、DNP3 及び ICCP 等の多様な ICS プロトコルの攻撃シグネチャを開発し、組み込みつつある[58]。

6.2.17.3 パッチ管理

パッチはコードの追加ピースで、既存ソフトウエアの問題や欠陥に対応するために開発される。脆弱性は悪用可能な欠陥で、IT システムへの不正アクセスを可能にし、ユーザに付与されている以上の権限を与える。

ソフトウエアパッチを体系的に管理・利用する取組をすることで、組織は費用効果の高い方法で、IT システム全体のセキュリティを改善できる。ソフトウエアパッチを積極的に管理・利用する組織では、IT システムの脆弱性を悪用される可能性が減る。また脆弱性に関係したインシデント対応に要する時間とコストも節約できる。

NIST SP 800-40 第 3 版[40]には、セキュリティパッチの設計・実装、脆弱性管理プログラム及び脆弱性軽減プログラムの効果性検証を担当するセキュリティ管理者向けのガイダンスがある。このガイダンスは、パッチの適用と試験、脆弱性問題のソリューション展開を担当するシステム管理者や職員にも役立つ。

ICS 固有の推奨事項及びガイダンス

OS コンポーネントへのパッチ適用は、ICS 環境では特に慎重を期すべき別の状況が生じる。パッチの試験は十分に行い（同等の ICS 環境でオフラインで）、副次的影響の許容度を判定すべきである。リグレッション試験が推奨される。パッチが他のソフトウエアに悪影響を及ぼすことは珍しくない。パッチは脆弱性をなくするが、

also introduce a greater risk from a production or safety perspective. Patching the vulnerability may also change the way the OS or application works with control applications, causing the control application to lose some of its functionality. Another issue is that many ICS utilize older versions of operating systems that are no longer supported by the vendor. Consequently, available patches may not be applicable. Organizations should implement a systematic, accountable, and documented ICS patch management process for managing exposure to vulnerabilities.
Once the decision is made to deploy a patch, there are other tools that automate this process from a centralized server and with confirmation that the patch has been deployed correctly. Consider separating the automated process for ICS patch management from the automated process for non-ICS applications. Patching should be scheduled to occur during planned ICS outages.

6.2.18 Program Management

The security controls that fall within the NIST SP 800-53 Program Management (PM) focus on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs.

Organizations document program management controls in the information security program plan. The organization-wide information security program plan supplements the individual security plans developed for each organizational information system. In addition to documenting the information security program management controls, the security program plan provides a vehicle for the organization, in a central repository, to document all security controls that have been designated as common controls (i.e., security controls inherited by organizational information systems).

6.2.19 Privacy Controls

Protecting the privacy of personally identifiable information (PII)[43] collected, used, maintained, shared, and disposed of by programs and information systems is critical given the advances in information technologies and applications of those technologies. Effective privacy for individuals depends on the safeguards employed within the organizational information systems that are processing, storing, and transmitting PII. Organizations cannot have effective privacy without a foundation of information security. However, privacy is more than security and includes, for example, the principles of transparency, notice, and choice.

The privacy controls focus on information privacy as a value distinct from, but highly interrelated with, information security. The privacy controls are based on the Fair Information Practice Principles (FIPPs) embodied in the Privacy Act of 1974, Section 208 of the E-Government Act of 2002, and related Office of Management and Budget (OMB) guidance. The FIPPs are designed to build public trust in an organization's privacy practices and to help organizations avoid tangible costs and intangible damages stemming from privacy incidents.

[43] OMB Memorandum 07-16 defines PII as "information which can be used to distinguish or trace an individual's identity such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." [86]. OMB Memorandum 10-22 reaffirmed this definition [87]. NIST Special Publication 800-122 defines PII as "any information about an individual [that is] maintained by an agency, including: (i) any information that can be used to distinguish or trace an individual 's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (ii) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information" [88].

生産や安全性の観点からは、より大きなリスクになる場合がある。脆弱性にパッチを当てると、OS やアプリケーションと制御アプリケーションの連動方法が変わり、制御アプリケーションの機能が失われることがある。別の問題として、ベンダーがサポートを打ち切った OS の旧バージョンを使用する ICS が多いことが挙げられる。その結果、入手可能なパッチが適用できないことになる。組織は脆弱性の露出を管理するため、体系的で説明のつく、文書化された ICS パッチ管理プロセスを実行すべきである。

パッチの展開を決定したなら、集中型サーバからこのプロセスを自動化し、パッチが正しく展開されたことを確認できる別のツールがある。ICS パッチ管理の自動化プロセスを、ICS 以外のアプリケーションの自動化プロセスから分離することを検討する。パッチの適用は、計画された ICS の操業停止時に行うように予定すべきである。

6.2.18　プログラム管理

NIST SP 800-53 のプログラム管理（PM）に含まれているセキュリティ対策は、特定の情報システムから独立した、情報セキュリティプログラムの管理に不可欠な、全組織的情報セキュリティ要件に焦点を当てている。

組織は、プログラム管理制御を情報セキュリティプログラム計画書の中に記載する。全組織的情報セキュリティプログラム計画書は、各組織の情報システム用個別セキュリティ計画書を補完する。情報セキュリティプログラム管理対策の文書化に加えて、セキュリティプログラム計画書は、共通管理（組織の情報システムが継承しているセキュリティ対策）として指定されている全てのセキュリティ対策を文書化する手段を集中保管場所に用意する。

6.2.19　プライバシー管理

情報技術の進歩やその技術の適用を考慮すると、プログラム及び情報システムが収集・利用・維持・共有・廃棄した個人を特定可能な情報（PII）[44]のプライバシー保護は重要である。効果的な個人プライバシーは、PII を処理・保管・転送する組織の情報システムで採用されている安全対策に左右される。情報セキュリティの基礎が確立されていない組織には、効果的なプライバシーはない。とは言え、プライバシーはセキュリティ以上のものであり、例えば透明性、通知及び選択の原則が含まれる。

プライバシー管理は、情報セキュリティとの関係は強いものの、それとは別の価値としてのプライバシー情報を重点とする。プライバシー管理は、プライバシー法（1974 年）の公正情報規範原則（FIPPs）、電子政府法（2002 年）第 208 条及び関係する行政予算管理局（OMB）ガイダンスを根拠としている。FIPPs は、組織のプライバシー規範に対する国民の信頼を醸成し、プライバシーインシデントから生じる有形の経費や無形の損害の回避を目指している。

[44] OMB 覚書 07-16 は PII を「氏名、社会保障番号、バイオメトリック記録等を単独で、又は誕生日、出生地、母親の旧姓等特定の個人に結びつくか結びつけられるその他の個人若しくは身分情報と組み合わせて、個人の身分を判別又は追跡できる情報」と定義している[86]。OMB 覚書 10-22 はこの定義を追認している[87]。NIST SP800-122 は PII をある機関が保持している個人に関する情報で、（1）氏名、社会保障番号、誕生日、出生地、母親の旧姓、バイオメトリック記録等、個人の身分を判別又は追跡できる情報及び（2）医療、教育、財政、就業情報等、個人に結びつくか結びつけられるその他の情報」と定義している[88]。

Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII. There are eight privacy control families with each family aligning with one of the FIPPs. The privacy control families can be implemented at the organization, department, agency, component, office, program, or information system level. The privacy controls are structured in a similar manner to the information system security controls in Appendix F of NIST SP 800-53.

The Privacy Appendix of NIST SP 800-53, Rev. 4 [22], provides a structured set of privacy controls, based on international standards and best practices to help organizations enforce requirements derived from federal privacy legislation, policies, regulations, directives, standards, and guidance. Additionally, it establishes a linkage and relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements that may overlap in concept and in implementation within federal information systems, programs, and organizations.

The privacy controls are intended primarily for use by an organization's Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) when working with program managers, information system developers, and information security personnel to determine how best to incorporate effective privacy protections and practices within those programs and/or systems. These controls facilitate the organization's efforts to comply with privacy requirements affecting those programs and/or systems that collect, use, maintain, share, or dispose of PII. This promotes closer cooperation between privacy and security officials within the federal government to help achieve the objectives of senior leaders/executives in enforcing the requirements in federal privacy legislation, policies, regulations, directives, standards, and guidance.

The 8 privacy control families include:

- Authority and Purpose (AP).
- Accountability, Audit, and Risk Management (AR).
- Data Quality and Integrity (DI).
- Data Minimization and Retention (DM).
- Individual Participation and Redress (IP).
- Security (SE).
- Transparency (TR).
- Use Limitation (UL).

プライバシー管理は、PII に対する保護と適正な取扱を確保するために組織内で採用される管理上の技術的・物理的安全対策である。プライバシー管理の 8 ファミリがそれぞれの FIPPS に整合している。プライバシー管理分野は、組織・部署・機関・コンポーネント、オフィス、プログラム又は情報システムレベルで実施できる。プライバシー管理は、NIST SP 800- 53 付録 F にある情報システムのセキュリティ対策と同様の方法で構築される。

NIST SP 800-53 改訂第 4 版[22]には、国際規格及び適性規範に基づいて構築されたプライバシー管理があり、組織が連邦プライバシー法、政策、規則、命令、規格及びガイダンスから生じる要件を実施する助けとなる。また、連邦情報システム、プログラム及び組織内で概念上も実施上も重なり合う、プライバシー要件とセキュリティ要件を施行する上で、プライバシー管理とセキュリティ対策の結びつきや関係についても記述している。

プライバシー管理の目的は、主に組織のプライバシー担当上級官吏（SAOP）/プライバシー担当主任（CPO）がプログラム管理者、情報システム開発者及び情報セキュリティ職員と協働する際に、効果的なプライバシー保護・規範をこれらプログラムやシステムに組み込む最善の方法の判定に使用することにある。このような管理によって、PII を収集・利用・維持・共有・廃棄するプログラムやシステムに影響を与えるプライバシー要件遵守に対する組織の取組が容易になる。これにより連邦政府のプライバシー担当者とセキュリティ担当者間の連携が緊密になり、幹部が連邦プライバシー法、政策、規制、指令、規格及びガイダンスの要件を施行して目標を達成できるようにする。

8 つのプライバシー管理分野は次のとおり。

- 権限及び目的（AP）
- 説明責任、監査及びリスク管理（AR）
- データ品質及び完全性（DI）
- データの最小化及び保持（DM）
- 個人の参加及び賠償（IP）
- セキュリティ（SE）
- 透明性（TR）
- 使用限界（UL）

Appendix A—Acronyms and Abbreviations

Selected acronyms and abbreviations used in the *Guide to Industrial Control Systems (ICS) Security* are defined below.

AC	Alternating Current
ACL	Access Control List
AGA	American Gas Association
API	American Petroleum Institute
ARP	Address Resolution Protocol
BCP	Business Continuity Plan
CIDX	Chemical Industry Data Exchange
CIGRE	International Council on Large Electric Systems
CIP	Critical Infrastructure Protection
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off-the-Shelf
CPNI	Centre for the Protection of National Infrastructure
CPU	Central Processing Unit
CSE	Communications Security Establishment
CSRC	Computer Security Resource Center
CSSC	Control System Security Center
CVE	Common Vulnerabilities and Exposures
DCOM	Distributed Component Object Model
DCS	Distributed Control System(s)
DETL	Distributed Energy Technology Laboratory
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DNP3	DNP3 Distributed Network Protocol (published as IEEE 1815)
DNS	Domain Name System
DOE	Department of Energy
DoS	Denial of Service
DRP	Disaster Recovery Plan
EAP	Extensible Authentication Protocol
EMS	Energy Management System
EPRI	Electric Power Research Institute
ERP	Enterprise Resource Planning
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FTP	File Transfer Protocol
GAO	Government Accountability Office
GPS	Global Positioning System
HMI	Human-Machine Interface
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol

付録 A 頭字語及び略語

産業用制御システム（ICS）セキュリティガイドで使用する主な頭字語及び略語の定義は以下のとおり。

AC	交流
ACL	アクセス制御リスト
AGA	米国ガス協会
API	米国石油協会
ARP	アドレス解決プロトコル
BCP	事業継続計画書
CIDX	化学業界データ交換
CIGRE	国際大電力システム会議
CIP	重要インフラ保護
CMVP	暗号モジュール妥当性検証プログラム
COTS	民生品
CPNI	国家インフラ保護センター
CPU	中央演算装置
CSE	通信セキュリティ局
CSRC	コンピュータセキュリティリソースセンター
CSSC	制御システムセキュリティセンター
CVE	共通脆弱性曝露
DCOM	分散型コンポーネントオブジェクトモデル
DCS	分散制御システム
DETL	分散エネルギー技術研究所
DHS	国土安全保障省
DMZ	非武装地帯
DNP3	DNP3 分散ネットワークプロトコル（IEEE 1815 として発行）
DNS	領域名システム
DOE	エネルギー省
DoS	サービス妨害
DRP	災害復旧計画書
EAP	拡張可能認証プロトコル
EMS	エネルギー管理システム
EPRI	電力研究所
ERP	企業資源計画
FIPS	連邦情報処理規格
FISMA	連邦情報セキュリティ強化法
FTP	ファイル転送プロトコル
GAO	政府説明責任局
GPS	グローバルポジショニングシステム
HMI	マンマシンインタフェース
HSPD	国土安全保障大統領命令
HTTP	ハイパーテキスト転送プロトコル

HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation, and Air Conditioning
I/O	Input/Output
I3P	Institute for Information Infrastructure Protection
IACS	Industrial Automation and Control System
IAONA	Industrial Automation Open Networking Association
ICCP	Inter-control Center Communications Protocol
ICMP	Internet Control Message Protocol
ICS	Industrial Control System(s)
ICS-CERT	Industrial Control Systems - Cyber Emergency Response Team
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
INL	Idaho National Laboratory
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISA	International Society of Automation
ISID	Industrial Security Incident Database
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
LAN	Local Area Network
MAC	Media Access Control
MES	Manufacturing Execution System
MIB	Management Information Base
MTU	Master Terminal Unit (also Master Telemetry Unit)
NAT	Network Address Translation
NCCIC	National Cybersecurity and Communications Integration Center
NCSD	National Cyber Security Division
NERC	North American Electric Reliability Council
NFS	Network File System
NIC	Network Interface Card
NISCC	National Infrastructure Security Coordination Centre
NIST	National Institute of Standards and Technology
NSTB	National SCADA Testbed
OLE	Object Linking and Embedding
OMB	Office of Management and Budget
OPC	OLE for Process Control
OS	Operating System
OSI	Open Systems Interconnection

HTTPS	ハイパーテキスト転送プロトコルセキュア
HVAC	冷暖房空調設備
I/O	入出力
I3P	情報インフラ保護協会
IACS	産業用オートメーション制御システム
IAONA	産業オートメーションオープンネットワークアソシエーション
ICCP	制御間センター通信プロトコル
ICMP	インターネットコントロールメッセージプロトコル
ICS	産業用制御システム
ICS-CERT	産業用制御システム - サイバー緊急対応チーム
IDS	侵入検知システム
IEC	国際電気技術委員会
IED	インテリジェント電子機器
IEEE	電気電子技術者協会
IETF	インターネットエンジニアリングタスクフォース
IGMP	インターネットグループ管理プロトコル
INL	アイダホ国立研究所
IP	インターネットプロトコル
IPS	侵入防止システム
IPsec	インターネットプロトコルセキュリティ
ISA	国際オートメーション協会
ISID	産業セキュリティインシデントデータベース
ISO	国際標準化機構
IT	情報技術
ITL	情報技術研究所
LAN	ローカルエリアネットワーク
MAC	メディアアクセス制御
MES	生産実行システム
MIB	管理情報ベース
MTU	マスター端末装置（マスターテレメトリ装置ともいう）
NAT	ネットワークアドレス変換
NCCIC	米国サイバーセキュリティ通信統合センター
NCSD	米国サイバーセキュリティ部
NERC	北米電力信頼度協議会
NFS	ネットワークファイルシステム
NIC	ネットワークインタフェースカード
NISCC	米国インフラセキュリティ調整センター
NIST	米国標準技術局
NSTB	米国 SCADA テストベッド
OLE	オブジェクトのリンクと埋め込み
OMB	管理予算局
OPC	プロセス制御用 OLE
OS	オペレーティングシステム
OSI	オープンシステム相互接続

PCII	Protected Critical Infrastructure Information
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PID	Proportional – Integral - Derivative
PIV	Personal Identity Verification
PLC	Programmable Logic Controller
PP	Protection Profile
PPP	Point-to-Point Protocol
R&D	Research and Development
RADIUS	Remote Authentication Dial In User Service
RBAC	Role-Based Access Control
RFC	Request for Comments
RMA	Reliability, Maintainability, and Availability
RMF	Risk Management Framework
RPC	Remote Procedure Call
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RTU	Remote Terminal Unit (also Remote Telemetry Unit)
SC	Security Category
SCADA	Supervisory Control and Data Acquisition
SCP	Secure Copy
SFTP	Secure File Transfer Protocol
SIS	Safety Instrumented System
SMTP	Simple Mail Transfer Protocol
SNL	Sandia National Laboratories
SNMP	Simple Network Management Protocol
SP	Special Publication
SPP-ICS	System Protection Profile for Industrial Control Systems
SQL	Structured Query Language
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
VFD	Variable Frequency Drive
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language

PCII	保護された重要インフラ情報
PDA	携帯情報端末
PIN	個人識別番号
PID	比例・積分・微分
PIV	個人の身元確認
PLC	プログラマブル論理制御装置
PP	保護プロファイル
PPP	ポイントツーポイントプロトコル
R&D	研究開発
RADIUS	遠隔認証ダイアルインユーザサービス
RBAC	役割ベースアクセス制御
RFC	コメント要求（リクエスト フォー コメンツ）
RMA	信頼性・保守性・可用性
RMF	リスク管理体制
RPC	遠隔手順呼出し
RPO	目標復旧点
RTO	目標復旧時間
RTU	遠隔端末装置（遠隔テレメトリ装置ともいう）
SC	セキュリティ分類
SCADA	監視制御データ取得（スキャダ）
SCP	セキュアコピー
SFTP	セキュアファイル転送プロトコル
SIS	安全計装システム
SMTP	シンプルメール転送プロトコル
SNL	サンディア国立研究所
SNMP	シンプルネットワーク管理プロトコル
SP	特別出版物
SPP-ICS	産業制御システム用システム保護プロファイル
SQL	構造化照会言語
SSH	セキュアシェル
SSID	サービスセット識別子
SSL	セキュアソケットレイヤー
TCP	通信制御プロトコル
TCP/IP	通信制御プロトコル/インターネットプロトコル
TFTP	トリビアルファイル転送プロトコル
TLS	トランスポート層セキュリティ
UDP	ユーザデータグラムプロトコル
UPS	無停電電源装置
US-CERT	米国コンピュータ緊急時即応チーム
USB	ユニバーサルシリアルバス
VFD	可変周波数駆動
VLAN	仮想 LAN
VPN	仮想プライベートネットワーク
WAN	広域ネットワーク
XML	拡張マークアップ言語

Appendix B—Glossary of Terms

Selected terms used in the *Guide to Industrial Control Systems (ICS) Security* are defined below. Source References for certain definitions are listed at the end of this appendix.

Alternating Current Drive Synonymous with Variable Frequency Drive (VFD).
SOURCE: NIST IR 6859 [2]

Access Control List (ACL) A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resources.
SOURCE: RFC 4949 [75]

Accreditation The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
SOURCE: NIST SP 800-53 [22]

Actuator A device for moving or controlling a mechanism or system. It is operated by a source of energy, typically electric current, hydraulic fluid pressure, or pneumatic pressure, and converts that energy into motion. An actuator is the mechanism by which a control system acts upon an environment. The control system can be simple (a fixed mechanical or electronic system), software-based (e.g. a printer driver, robot control system), or a human or other agent.

Alarm A device or function that signals the existence of an abnormal condition by making an audible or visible discrete change, or both, so as to attract attention to that condition.
SOURCE: ANSI/ISA-5.1-2009

Antivirus Tools Software products and technology used to detect malicious code, prevent it from infecting a system, and remove malicious code that has infected the system.

Application Server A computer responsible for hosting applications to user workstations.

Attack An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.
SOURCE: CNSSI-4009

付録 B　用語集

*産業用制御システム（ICS）セキュリティガイド*で使用する主な用語の定義は以下のとおり。いくつかの定義については、本付録の末尾にその出典が掲載されている。

Alternating Current Drive：交流駆動
可変周波数駆動（VFD）と同義
出典：NIST IR 6859 [2]

Access Control List (ACL)：アクセス制御リスト
リソースへのアクセスを許可されたシステム実体の一致点を列挙することによりシステムリソースへのアクセス制御を行うメカニズム。
出典：RFC 4949 [75]

Accreditation：認定
合意されたセキュリティ対策の実装に基づき、情報システムの運用を認可し、政府機関の業務（任務、機能、イメージ、評判等）、政府機関の資産又は個人のリスクを明示的に受け入れるため政府機関の上級官吏が下す公的管理決定。
出典：NIST SP 800-53 [22]

Actuator：アクチュエータ
機構又はシステムを動かし又は制御するためのデバイス。一般に電流、油圧、空気圧等のエネルギー源で作動し、そのエネルギーを運動に変える。アクチュエータは、制御システムが環境に働きかける機構である。制御システムは単純で（固定機構や電子システム）、ソフトウエアベース（プリンタドライバ、ロボット制御システム等）や人その他による。

Alarm：アラーム
異常状態を知らせるデバイス又は機能で、音や視覚的変化により異常状態に注意を引く。
出典：ANSI/ISA-5.1-2009

Antivirus Tools：アンチウイルスツール
ソフトウエア製品及び技術で、悪意あるコードを検出してシステムへの感染を防ぎ、感染している場合には悪意あるコードを排除する。

Application Server：アプリケーションサーバ
ユーザワークステーションにアプリケーションをホスティングするコンピュータ。

Attack：攻撃
システムサービス、リソース若しくは情報に無断でアクセスしようとするもくろみ又はシステムの完全性、可用性若しくは機密性を低下させようとするもくろみ。
出典：CNSSI-4009

Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. SOURCE: NIST SP 800-53 [22]
Authorization	The right or a permission that is granted to a system entity to access a system resource. SOURCE: RFC 4949 [75]
Backdoor	An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.
Batch Process	A process that leads to the production of finite quantities of material by subjecting quantities of input materials to an ordered set of processing activities over a finite time using one or more pieces of equipment. SOURCE: ANSI/ISA-88.01-1995
Broadcast	Transmission to all devices in a network without any acknowledgment by the receivers. SOURCE: IEC/PAS 62410
Buffer Overflow	A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Adversaries exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. SOURCE: NIST SP 800-28 [69]
Certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. SOURCE: NIST SP 800-37 [21]
Clear Text	Information that is not encrypted.
Communications Router	A communications device that transfers messages between two networks. Common uses for routers include connecting a LAN to a WAN, and connecting MTUs and RTUs to a long-distance network medium for SCADA communication.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. SOURCE: NIST SP 800-53 [22]

Authentication：認証 ユーザ、プロセス又はデバイスの同一性を検証することで、情報システム中のリソースへの前提となることが多い。
出典：NIST SP 800-53 [22]

Authorization：権限付与 システムの実在者がシステムリソースにアクセスするために与えられる権利又は許可。
出典：RFC 4949 [75]

Backdoor：バックドア コンピュータシステムへのアクセスを得る不正な方法。バックドアはセキュリティリスクとなる。

Batch Process：バッチプロセス 大量の入力物を 1 つ又は複数の装備品を用いて、ある時間をかけて順番に一連の処理にかけることにより、限定された量にするプロセス。
出典：ANSI/ISA-88.01-1995

Broadcast：ブロードキャスト ネットワーク内の全てのデバイスに、受け手側の了解を得ることなく送信すること。
出典：IEC/PAS 62410

Buffer Overflow：バッファオーバーフロー 割り当てられた容量を超えて入力がバッファ又はデータ保持領域に置かれ、他の情報を上書きするインタフェースの状態。

攻撃側はこのような状態を利用して、システムをクラッシュさせ、特殊コードを挿入してシステムの制御を得ることができる。
出典：NIST SP 800-28 [69]

Certification：証明 セキュリティ認定を支援するために行う情報システムの管理、運用及び技術上のセキュリティ対策に対する包括的評価で、コントロールがどの程度適正に実装されているか、予定どおりに稼働しているか、システムセキュリティ要件に合致した結果になっているか判定する。
出典：NIST SP 800-37 [21]

Clear Text：平文 暗号化されていない情報。

Communications Router：通信ルータ 2 つのネットワーク間でメッセージを転送する通信デバイス。ルータの一般的な使用方法として、LAN と WAN の接続や、SCADA 通信用の MTU 及び RTU と遠距離ネットワーク媒体の接続がある。

Confidentiality：機密性 情報の利用及び漏洩に公認の制限を課すことで、個人情報及び専有情報を保護する手段も含まれる。
出典：NIST SP 800-53 [22]

Configuration (of a system or device)	Step in system design; for example, selecting functional units, assigning their locations, and defining their interconnections. SOURCE: IEC/PAS 62409
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications before, during, and after system implementation. SOURCE: CNSSI-4009
Continuous Process	A process that operates on the basis of continuous flow, as opposed to batch, intermittent, or sequenced operations.
Control Algorithm	A mathematical representation of the control action to be performed. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Control	The part of the ICS used to perform the monitoring and control of the physical process. This includes all control servers, field devices, actuators, sensors, and their supporting communication systems.
Control Center	An equipment structure or group of structures from which a process is measured, controlled, and/or monitored. SOURCE: ANSI/ISA-51.1-1979
Control Loop	A control loop consists of sensors for measurement, controller hardware such as PLCs, actuators such as control valves, breakers, switches and motors, and the communication of variables. Controlled variables are transmitted to the controller from the sensors. The controller interprets the signals and generates corresponding manipulated variables, based on set points, which it transmits to the actuators. Process changes from disturbances result in new sensor signals, identifying the state of the process, to again be transmitted to the controller.
Control Network	Those networks of an enterprise typically connected to equipment that controls physical processes and that is time or safety critical. The control network can be subdivided into zones, and there can be multiple separate control networks within one enterprise and site. SOURCE: ISA99 [34]
Control Server	A controller that also acts as a server that hosts the control software that communicates with lower-level control devices, such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), over an ICS network. In a SCADA system, this is often called a SCADA server, MTU, or supervisory controller.

Configuration (of a system or device)：
（システム又はデバイスの）構成
システム設計に介入すること。例えば、機能ユニットの選定、場所の割当、それらの相互接続等。
出典：IEC/PAS 62409

Configuration Control：
構成管理
システム実装前・中・後の不適切な改変から情報システムを保護するために、ハードウエア・ファームウエア・ソフトウエア・文書への変更を管理するプロセス。
出典：CNSSI-4009

Continuous Process：
継続プロセス
継続的な流れを基本とする操作プロセスで、バッチ、間欠又は一連操作の反対。

Control Algorithm：
制御アルゴリズム
実施すべき制御行為の数学的表現。出典：オートメーション・システム・計装事典

Control：制御
物理プロセスの監視及び制御を行うために用いる ICS の一部。全ての制御サーバ、フィールドデバイス、アクチュエータ、センサ及びこれらの支援通信システムを含む。

Control Center：
制御センター
1 つ又は一群の装備品構造体で、そこからプロセスを計測し、制御し、監視する。
出典：ANSI/ISA-51.1-1979

Control Loop：
制御ループ
制御ループは計測センサ、制御ハードウエア（PLC 等）、アクチュエータ（制御弁、ブレーカ、スイッチ、モータ等）及び変数の通信で構成される。制御変数はセンサ経由でコントローラに転送される。コントローラは信号を解釈し、設定点を基に対応する操作変数を生成し、アクチュエータに送信する。

妨害の結果プロセスが変更されると、センサ信号が変わり、プロセス状態を識別して、再度コントローラに送信する。

Control Network：
制御ネットワーク
このような企業ネットワークは、一般に物理プロセスをセットする装備品に接続され、時間や安全性の点で重要である。制御ネットワークはゾーンに分かれ、ゾーンごとに 1 つの企業又は現場内に別々な複数の制御ネットワークが存在する。
出典：ISA99 [34]

Control Server：
制御サーバ
サーバとして機能するコントローラで、ICS ネットワーク上で下位レベルのデバイス（RTU、PLC 等）との通信を行う制御ソフトウエアをホストする。SCADA システムでは SCADA サーバ、MTU 又は監視コントローラと呼ばれることが多い。

Control system	A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs and other types of industrial measurement and control systems.
Controlled Variable	The variable that the control system attempts to keep at the set point value. The set point may be constant or variable. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Controller	A device or program that operates automatically to regulate a controlled variable. SOURCE: ANSI/ISA-51.1-1979
Cycle Time	The time, usually expressed in seconds, for a controller to complete one control loop where sensor signals are read into memory, control algorithms are executed, and corresponding control signals are transmitted to actuators that create changes the process resulting in new sensor signals. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Data Diode	A data diode (also referred to as a unidirectional gateway, deterministic one-way boundary device or unidirectional network) is a network appliance or device allowing data to travel only in one direction.
Database	A repository of information that usually holds plant-wide information including process data, recipes, personnel data, and financial data. SOURCE: NIST IR 6859 [2]
Data Historian	A centralized database supporting data analysis using statistical process control techniques.
DC Servo Drive	A type of drive that works specifically with servo motors. It transmits commands to the motor and receives feedback from the servo motor resolver or encoder. SOURCE: NIST IR 6859 [2]

Control System：
制御システム
ある変数の予定値を実現するために、計画的なガイダンス又は操作を利用するシステム。制御システムには SCADA、DCS、PLC その他の産業用計測制御仕様がある。

Controlled Variable：
制御変数
制御システムが設定点を維持しようとする変数。設定点は定数又は変数となる。
出典：オートメーション・システム・計装事典

Controller：
コントローラ
制御変数を自動的に調整するデバイス又はプログラム。出典：ANSI/ISA-51.1-1979

Cycle Time：
サイクル時間
コントローラが 1 つの制御ループを完了するための、通常秒単位で示される時間で、センサ信号がメモリに読み込まれ、制御アルゴリズムが実行され、対応する制御信号がアクチュエータに送られてプロセスを変更し、新たなセンサ信号が生じる。
出典：オートメーション・システム・計装事典

Data Diode：
データダイオード
データダイオード（単方向ゲートウェイ、決定論的一方通行境界デバイス又は単方向ネットワークとも呼ばれる）はネットワーク機器又はデバイスで、データが一方向に流れるようにする。

Database：
データベース
情報が蓄えられたもので、通常プロセスデータ、レシピ、人事データ、会計データ等のプラント全体の情報が蓄積されている。
出典：NIST IR 6859 [2]

Data Historian：
データヒストリアン
集中データベースで、静的プロセス管理技術を用いてデータ解析を行う。

DC Servo Drive：
直流サーボ駆動
特にサーボモータで作動する駆動の種類。コマンドをモータに送信し、サーボモータリゾルバ又はエンコーダからフィードバックを受信する。
出典：NIST IR 6859 [2]

Demilitarized Zone (DMZ)	An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. SOURCE: SP 800-41 [85] A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet. SOURCE: SP 800-45 [91] Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks. SOURCE: CNSSI-4009
Denial of Service (DoS)	The prevention of authorized access to a system resource or the delaying of system operations and functions. SOURCE: RFC 4949 [75]
Diagnostics	Information concerning known failure modes and their characteristics. Such information can be used in troubleshooting and failure analysis to help pinpoint the cause of a failure and help define suitable corrective measures. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Disaster Recovery Plan (DRP)	A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities. SOURCE: NIST SP 800-34 [52]
Discrete Process	A type of process where a specified quantity of material moves as a unit (part or group of parts) between work stations and each unit maintains its unique identity. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Distributed Control System (DCS)	In a control system, refers to control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Distributed Plant	A geographically distributed factory that is accessible through the Internet by an enterprise. SOURCE: NIST IR 6859 [2]

Demilitarized Zone (DMZ)：
非武装地帯

ルーティングファイアウォール上のインタフェースで、ファイアウォールの保護側のインタフェースに似ている。DMZ とファイアウォールの保護側にある別のインタフェース間のトラフィックは、ファイアウォールを通過し、ファイアウォール保護ポリシーが適用される。
出典：SP 800-41 [85]

「中立地帯」として組織のプライベートネットワークとインターネット間に挿入されるホスト又はネットワークセグメント。
出典：SP 800-45 [91]

内部ネットワークと外部ネットワークの間に論理的にある周辺ネットワークセグメント。目的は、外部との情報交換用内部ネットワークの情報保証ポリシーを施行し、内部ネットワークを外部脅威からシールドしつつ、外部の信頼の置けない要求ソースによる情報へのアクセスに制限を課することにある。
出典：CNSSI-4009

Denial of Service (DoS)：
サービス妨害

システムリソースへの公認アクセスを妨げ又はシステムの運用及び機能を遅らせること。
出典：RFC 4949 [75]

Diagnostics：診断

既知の障害態様及びその特徴に関する情報。このような情報はトラブルシューティングや故障解析に使用でき、原因や適正な対策を割り出す助けとなる。
出典：オートメーション・システム・計装事典

Disaster Recovery Plan (DRP)：災害復旧計画書

大規模なハードウエア/ソフトウエア障害や施設破壊の際に重要事項を処理するための文書。
出典：NIST SP 800-34 [52]

Discrete Process：
離散プロセス

指定量の材料がある単位（パーツ又はパーツグループ）としてワークステーション間を移動し、各単位がその固有のアイデンティティを保持するプロセスの種類。出典：オートメーション・システム・計装事典

Distributed Control System (DCS)：
分散制御システム

制御システムにあって、中央に置かれた 1 つの装置ではなく、制御するプロセスについて分散されたインテリジェンスによって行われる制御をいう。出典：オートメーション・システム・計装事典

Distributed Plant：
分散プラント

企業がインターネットを通じてアクセスできる地理的に分散された工場。
出典：NIST IR 6859 [2]

Disterbance	An undesired change in a variable being applied to a system that tends to adversely affect the value of a controlled variable. SOURCE: ANSI/ISA-51.1-1979
Domain	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See Security Domain. SOURCE: CNSSI-4009; SP 800-53 [22]; SP 800-37 [21]
Domain Controller	A server responsible for managing domain information, such as login identification and passwords. SOURCE: NIST IR 6859 [2]
Encryption	Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state. SOURCE: RFC 4949 [75]
Enterprise	An organization that coordinates the operation of one or more processing sites. SOURCE: ANSI/ISA-88.01-1995
Enterprise Resource Planning (ERP) System	A system that integrates enterprise-wide information including human resources, financials, manufacturing, and distribution as well as connects the organization to its customers and suppliers.
Extensible Markup Language (XML)	A specification for a generic syntax to mark data with simple, human-readable tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.
Fault Tolerant	Of a system, having the built-in capability to provide continued, correct execution of its assigned function in the presence of a hardware and/or software fault.
Field Device	Equipment that is connected to the field side on an ICS. Types of field devices include RTUs, PLCs, actuators, sensors, HMIs, and associated communications.
Field Site	A subsystem that is identified by physical, geographical, or logical segmentation within the ICS. A field site may contain RTUs, PLCs, actuators, sensors, HMIs, and associated communications.

Disturbance：撹乱
制御された変数値に悪影響を与えやすいシステムに加えられる望ましくない変数の変更。
出典：ANSI/ISA-51.1-1979

Domain：領域
システムリソース及び共通接続ポリシー、接続モデル又は接続アーキテクチャの規定どおりリソースへのアクセス権を持つシステム実体を含む環境又はコンテキスト。セキュリティ領域を参照。
出典：CNSSI-4009; SP 800-53 [22]; SP 800-37 [21]

Domain Controller：領域コントローラ
ログイン識別やパスワードといった領域情報を管理するサーバ。
出典：NIST IR 6859 [2]

Encryption：暗号化
暗号変換はデータ（平文と呼ばれる）を暗号変換して、ある形態（暗号文と呼ばれる）にすることで、データの元の意味を秘匿し、知られたり利用されたりできないようにする。変換が逆変換も可能な場合、そのプロセスは復号と呼ばれ、暗号化されたデータを元の状態に戻す。
出典：RFC 4949 [75]

Enterprise：企業
1 つまたはそれ以上の処理現場の運用を調整する組織。
出典：ANSI/ISA-88.01-1995

Enterprise Resource Planning (ERP) System：企業資源計画システム
人的資源、財政、生産、流通等の全企業的情報を一体化し、組織をその顧客やサプライヤに接続するシステム。

Extensible Markup Language (XML)：拡張マークアップ言語
データを単純で人が読めるタグを付けて記述する汎用構文仕様で、アプリケーション間及び組織間でのデータの定義、送信、妥当性検証及び解釈を可能にする。

Fault Tolerant：フォールトトレラント
システムで、ハードウエア及びソフトウエアが故障したときでも、割り当てられた機能を継続して正しく実行できる、組み込みの能力。

Field Device：フィールドデバイス
ICS のフィールド側に接続された装備品。種類として RTU、PLC、アクチュエータ、センサ、HMI 及び関連通信機器がある。

Field Site：フィールドサイト
ICS 内の物理的、地理的又は論理的区画により識別されるサブシステム。フィールドサイトには RTU、PLC、アクチュエータ、センサ、HMI 及び関連通信機器がある。

Fieldbus	A digital, serial, multi-drop, two-way data bus or communication path or link between low-level industrial field equipment such as sensors, transducers, actuators, local controllers, and even control room devices. Use of fieldbus technologies eliminates the need of point-to-point wiring between the controller and each device. A protocol is used to define messages over the fieldbus network with each message identifying a particular sensor on the network.
File Transfer Protocol (FTP)	FTP is an Internet standard for transferring files over the Internet. FTP programs and utilities are used to upload and download Web pages, graphics, and other files between local media and a remote server which allows FTP access. SOURCE: API 1164
Firewall	An inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall). SOURCE: RFC 4949 [75] An inter-network connection device that restricts data communication traffic between two connected networks. A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), which forwards or rejects/drops packets on a network. Typically firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open. SOURCE: ISA-62443-1-1 [34]
Human-Machine Interface (HMI)	The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software. SOURCE: NIST IR 6859 [2] Software and hardware that allows human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency. The HMI also allows a control engineer or operator to configure set points or control algorithms and parameters in the controller. The HMI also displays process status information, historical information, reports, and other information to operators, administrators, managers, business partners, and other authorized users. Operators and engineers use HMIs to monitor and configure set points, control algorithms, send commands, and adjust and establish parameters in the controller. The HMI also displays process status information and historical information.
Identification	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. SOURCE: NIST SP 800-47 [92]

Fieldbus：フィールドバス
センサ、トランスデューサ、アクチュエータ、ローカルコントローラ、制御室デバイス等の低レベル産業用フィールド装備品間のデジタル、シリアル、マルチドロップ、双方向データバス、通信経路又はリンク。フィールドバス技術を利用すると、コントローラと各デバイス間での 2 地点間配線の必要がなくなる。プロトコルを使用してフィールドバスネットワーク上のメッセージを定義し、各メッセージはネットワーク上の特定のセンサで識別する。

File Transfer Protocol (FTP)：ファイル転送プロトコル
インターネット上でファイルを転送するインターネット規格。FTP プログラム及びユーティリティを使用して、ウェブページ、グラフィックその他のファイルをローカルメディアと FTP アクセスを許可する遠隔サーバでアップロード/ダウンロードする。
出典：API 1164

Firewall：ファイアウォール
ネットワーク間ゲートウェイで、接続されたネットワーク（ファイアウォールの「中」にある）間でのデータ通信トラフィックを制限し、当該ネットワークのシステムリソースを他のネットワーク（ファイアウォールの「外」にある）からの脅威から守る。
出典：RFC 4949 [75]

接続された 2 つのネットワーク間でデータ通信トラフィックを制限するネットワーク間接続デバイス。ファイアウォールは、汎用コンピュータ又は専用プラットホーム（機器）にインストールされたアプリケーションで、ネットワーク上のパケットを転送又は拒絶/ドロップする。一般にファイアウォールはゾーン境界を定めるのに使用する。ファイアウォールはどのポートを開放するかを制限する。
出典：ISA-62443-1-1 [34]

Human-Machine Interface (HMI)：マンマシンインタフェース
操作員がコントローラと相互作用を行うために使用するハードウエア又はソフトウエア。ボタンやインジケータライトの付いた物理的制御パネルから、カラーグラフィックディスプレイの付いた専用 HMI ソフトウエアを実行する産業用 PC まで多様である。
出典：NIST IR 6859 [2]

操作員が制御中のプロセス状態を監視し、制御設定を変えて制御対象を変更し、緊急時に自動制御運転を手動に変更できるソフトウエア及びハードウエア。制御エンジニアや操作員は、コントローラの設定点又は制御アルゴリズム及びパラメータを変更することもできる。また HMI はプロセス状態、履歴情報、レポートその他の情報を操作員、管理者、マネージャ、ビジネスパートナーその他許可されたユーザに表示する。操作員及びエンジニアは HMI を利用し、設定点を監視・設定し、アルゴリズムを制御し、コマンドを送信し、コントローラのパラメータを調整・設定する。また HMI はプロセスのステータス情報及び履歴情報を表示する。

Identification：識別
ユーザ、プロセス又はデバイスの同一性を検証するプロセスで、通常 IT システム中のリソースへのアクセス付与の前提となる。
出典：NIST SP 800-47 [92]

Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies SOURCE: FIPS 200 [16]; SP 800-53 [22]
Industrial Control System (ICS)	General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).
Information Security Program Plan	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements. SOURCE: NIST SP 800-53 [22]
Input/Output (I/O)	A general term for the equipment that is used to communicate with a computer as well as the data involved in the communications. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Insider	An entity inside the security perimeter that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. SOURCE: RFC 4949 [75]
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. SOURCE: NIST SP 800-53 [22]
Intelligent Electronic Device (IED)	Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g., electronic multifunction meters, digital relays, controllers). SOURCE: AGA 12 [5]
Internet	The single interconnected world-wide system of commercial, government, educational, and other computer networks that share the set of protocols specified by the Internet Architecture Board (IAB) and the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN). SOURCE: RFC 4949 [75]

Incident：インシデント 情報システム又はシステムが処理、保管若しくは送信する情報の機密性、完全性若しくは可用性を現実に又は可能性として危険に陥れる事象又は接続ポリシー、接続手順若しくは妥当な使用ポリシーに違反するか、直ちに違反しそうな事象。
出典：FIPS 200 [16]; SP 800-53 [22]

Industrial Control System (ICS)：産業用制御システム（ICS） 数種の制御システムを包括した汎用的な用語で、これには各種産業部門や重要インフラで使用されている SCADA、DCS、PLC、その他の制御システムの設定が含まれる。ICS は産業上の目的（物品やエネルギーの生産・輸送等）を達成するために併用される制御用コンポーネント（電気・機械・油圧・空気等）が組み合わさって構成されている。

Information Security Program Plan：情報セキュリティプログラム計画書 全組織的情報セキュリティプログラムのセキュリティ要件について概説し、要件を満足するために実施中又は計画中のプログラム管理対策及び共通管理について記述した正式文書。
出典：NIST SP 800-53 [22]

Input/Output (I/O)：入出力 コンピュータと通信するための装備品及び通信に含まれるデータを示す一般用語。
出典：オートメーション・システム・計装事典

Insider：インサイダー セキュリティ境界内にいてシステムリソースへのアクセスが許されているが、許可された以外の方法で使用する実在者。
出典：RFC 4949 [75]

Integrity：完全性 不正な情報の改変又は破壊を防ぐことで、情報の否認防止及び正当性を確保する。
出典：NIST SP 800-53 [22]

Intelligent Electronic Device (IED)：インテリジェント電子機器 1 つ又は複数のプロセスを組み込んだデバイスで、外部ソースとの間でデータ/制御を送受信する能力を持つ（電子多機能メータ、デジタルリレー、コントローラ等）。
出典：AGA 12 [5]

Internet：インターネット 産官学その他のネットワークを 1 つに連接した世界的システムで、インターネットアーキテクチャ委員会（IAB）が指定したプロトコル及び ICANN が管理する名前及びアドレス空間を共有する。出典：RFC 4949 [75]

Intrusion Determination System (IDS)	A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner. SOURCE: RFC 4949 [75]
Intrusion Prevention System (IPS)	A system that can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.
Jitter	The time or phase difference between the data signal and the ideal clock.
Key Logger	A program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures.
Light Tower	A device containing a series of indicator lights and an embedded controller used to indicate the state of a process based on an input signal. SOURCE: NIST IR 6859 [2]
Local Area Network (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.
Machine Controller	A control system/motion network that electronically synchronizes drives within a machine system instead of relying on synchronization via mechanical linkage.
Maintenance	Any act that either prevents the failure or malfunction of equipment or restores its operating capability. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Malware	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code (malware). SOURCE: NIST SP 800-53 [22]
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information security. SOURCE: NIST SP 800-18 [19]
Manipulated Variable	In a process that is intended to regulate some condition, a quantity or a condition that the control alters to initiate a change in the value of the regulated condition. SOURCE: The Automation, Systems, and Instrumentation Dictionary

Intrusion Detection System (IDS)：侵入検知システム	システムリソースに無断でアクセスするもくろみを発見し、リアルタイム又はほぼリアルタイムで警告するために、ネットワーク又はシステムイベントを監視・分析するセキュリティサービス。出典：RFC 4949 [75]
Intrusion Prevention System (IPS)：侵入防止システム	侵入活動を検知し、可能であれば目標に達する前に活動をやめさせることができるシステム。
Jitter：ジッター	データ信号と理想的クロック間の時間差又はフェーズ。
Key Logger：キーロガー	パスワードや暗号鍵を取得し、他のセキュリティ手段を迂回するために、コンピュータのキーボードで押されたキーを記録するプログラム。
Light Tower：ライトタワー	入力信号に基づいてプロセス状態を表示する、一連のインジケータライトと組込みコントローラを備えたデバイス。出典：NIST IR 6859 [2]
Local Area Network (LAN)：ローカルエリアネットワーク	比較的限定されたエリア内に分散し、通信リンクで接続され、それぞれがネットワーク上で連動するコンピュータその他のデバイスグループ。
Machine Controller：マシンコントローラ	マシンシステム内のドライブを、機械式リンク経由の同期に依存せず、電子的に同期する制御システム/モーションネットワーク。
Maintenance：保守	装備品の故障又は不具合を防止又は稼働状態に回復する行為。出典：オートメーション・システム・計装事典
Malware：マルウエア	情報システムの機密性、完全性又は可用性に悪影響する不正アクセスを行うためのソフトウエア又はファームウエア。ウイルス、ワーム、トロイの木馬その他コードベースのものがホストを感染させる。スパイウエアやいくつかの形態のアドウェアも悪意あるコード（マルウエア）の例である。出典：NIST SP 800-53 [22]
Management Controls：管理対策	リスク管理及び情報セキュリティ管理に特化した情報システムのセキュリティ対策（安全策又は対策）。出典：NIST SP 800-18 [19]
Manipulated Variable：操作された変数	特定の状態を調整するためのプロセスにおいて、調整済み状態の値を制御が変更するときの量又は状態。出典：オートメーション・システム・計装事典

Manufacturing Execution System (MES)	A system that uses network computing to automate production control and process automation. By downloading recipes and work schedules and uploading production results, a MES bridges the gap between business and plant-floor or process-control systems. SOURCE: NIST IR 6859 [2]
Master Terminal Unit (MTU)	See *Control Server*.
Modem	A device used to convert serial digital data from a transmitting terminal to a signal suitable for transmission over a telephone channel to reconvert the transmitted signal to serial digital data for the receiving terminal. SOURCE: NIST IR 6859 [2]
Motion Control Network	The network supporting the control applications that move parts in industrial settings, including sequencing, speed control, point-to-point control, and incremental motion. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Network Interface Card (NIC)	A circuit board or card that is installed in a computer so that it can be connected to a network.
Object Linking and Embedding (OLE) for Process Control (OPC)	A set of open standards developed to promote interoperability between disparate field devices, automation/control, and business systems.
Operating System	An integrated collection of service routines for supervising the sequencing of programs by a computer. An operating system may perform the functions of input/output control, resource scheduling, and data management. It provides application programs with the fundamental commands for controlling the computer. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems). SOURCE: NIST SP 800-18 [19]
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Phishing	Tricking individuals into disclosing sensitive personal information by claiming to be a trustworthy entity in an electronic communication (e.g., internet web sites).

Manufacturing Execution System (MES)：生産実行システム
ネットワークコンピューティングを利用して生産制御及びプロセスの自動化を行うシステム。レシピと作業スケジュールをダウンロードし、生産結果をアップロードすることにより、MES は事業システムとプラント現場システム又はプロセス制御システム間のギャップを埋める。
出典：NIST IR 6859 [2]

Master Terminal Unit (MTU)：マスター端末装置
制御サーバを参照。

Modem：モデム
通信端末からのシリアルデジタルデータを電話網通信に適した信号に変換し、受信端末にはシリアルデジタルデータに再変換するためのデバイス。
出典：NIST IR 6859 [2]

Motion Control Network：動作制御ネットワーク
産業環境においてパーツを動かす制御アプリケーションに対応したネットワークで、動作にはシーケンシング、速度制御、2 点間制御、差分動作等がある。
出典：オートメーション・システム・計装事典

Network Interface Card (NIC)：ネットワークインタフェースカード
コンピュータに設置される回路基板又はカードで、コンピュータをネットワークに接続する。

Object Linking and Embedding (OLE) for Process Control (OPC)：プロセス制御用 OLE
異種フィールドデバイス間、オートメーション/制御間及び事業システム間の相互運用性を促進するために開発されたオープン規格。

Operating System：オペレーティングシステム
コンピュータによりプログラムのシーケンシングを監視させる定常サービスの集合体。入出力制御、リソーススケジューリング及びデータ管理を行う。コンピュータを制御するための機能コマンドをアプリケーションプログラムに提供する。
出典：オートメーション・システム・計装事典

Operational Controls：運用制御
主に人間（システムではなく）が実装し実行する情報システムのセキュリティ対策（安全策又は対策）。
出典：NIST SP 800-18 [19]

Password：パスワード
身分を認証又はアクセス権限を確認するための文字列（文字、数字その他記号）。

Phishing：フィッシング
電子通信（インターネットウェブサイト等）において信頼できる実体であると主張することにより、欺いて個人情報を開示させること。

Photo Eye	A light sensitive sensor utilizing photoelectric control that converts a light signal into an electrical signal, ultimately producing a binary signal based on an interruption of a light beam. SOURCE: NIST IR 6859 [2]
Plant	The physical elements necessary to support the physical process. This can include many of the static components not controlled by the ICS; however, the operation of the ICS may impact the adequacy, strength, and durability of the plant's components.
Port	The entry or exit point from a computer for connecting communications or peripheral devices. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Port Scanning	Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports). SOURCE: NIST SP 800-61 [59]
Predisposing Condition	A condition that exists within an organization, a mission/business process, enterprise architecture, or information system including its environment of operation, which contributes to (i.e., increases or decreases) the likelihood that one or more threat events, once initiated, will result in undesirable consequences or adverse impact to organizational operations and assets, individuals, other organizations, or the Nation. SOURCE: SP 800-30 [79]
Pressure Regulator	A device used to control the pressure of a gas or liquid. SOURCE: NIST IR 6859 [2]
Pressure Sensor	A sensor system that produces an electrical signal related to the pressure acting on it by its surrounding medium. Pressure sensors can also use differential pressure to obtain level and flow measurements. SOURCE: NIST IR 6859 [2]
Printer	A device that converts digital data to human-readable text on a paper medium. SOURCE: NIST IR 6859 [2]
Process Controller	A type of computer system, typically rack-mounted, that processes sensor input, executes control algorithms, and computes actuator outputs. SOURCE: NIST IR 6859 [2]

Photo Eye：フォトアイ 光信号を電子信号に変換する光電子制御を利用した感光センサで、光線を中断してバイナリ信号を生成する。
出典：NIST IR 6859 [2]

Plant：プラント 物理プロセスを支えるための物理要素。ICS で制御されない多くの静的コンポーネントが含まれ得るが、ICS の運用はプラットホームコンポーネントの適切性、強度及び耐久性に影響する。

Port：ポート コンピュータが通信機器又は周辺デバイスに接続するための出入口となる点。
出典：オートメーション・システム・計装事典

Port Scanning：ポートスキャニング プログラムを利用して開放されているポート（そこからシステムに接続できるか）を判定すること。
出典：NIST SP 800-61 [59]

Predisposing Condition：素因的状態 組織、任務・事業、企業アーキテクチャ又は情報システム内に存在する状態のことで、いったん発動すると、組織の運営及び資産、個人、他の組織又は国に悪影響を与える脅威事象に寄与（増減）する運用環境が含まれる。
出典：SP 800-30 [79]

Pressure Regulator：圧力レギュレータ ガス又は液体の圧力を制御するデバイス。出典：NIST IR 6859 [2]

Pressure Sensor：圧力センサ 周辺媒体から受ける圧力に関する電気信号を発生するセンサシステム。圧力センサは差圧を利用してレベル及び流量の計測も行う。
出典：NIST IR 6859 [2]

Printer：プリンタ デジタルデータを人が読める紙のテキストに変換するデバイス。出典：NIST IR 6859 [2]

Process Controller：プロセスコントローラ 通常ラックに設置された 1 種のコンピュータシステムで、センサ入力を処理し、制御アルゴリズムを実行し、アクチュエータ出力を計算する。
出典：NIST IR 6859 [2]

Programmable Logic Controller (PLC)	A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing. SOURCE: The Automation, Systems, and Instrumentation Dictionary A small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, switches, and mechanical timer/counters). PLCs have evolved into controllers with the capability of controlling complex processes, and they are used substantially in SCADA systems and DCS. PLCs are also used as the primary controller in smaller system configurations. PLCs are used extensively in almost all industrial processes.
Protocol	A set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. SOURCE: RFC 4949 [75]
Protocol Analyzer	A device or software application that enables the user to analyze the performance of network data so as to ensure that the network and its associated hardware/software are operating within network specifications. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Proximity Sensor	A non-contact sensor with the ability to detect the presence of a target within a specified range. SOURCE: NIST IR 6859 [2]
Proxy Server	A server that services the requests of its clients by forwarding those requests to other servers. SOURCE: CNSSI-4009
Real-Time	Pertaining to the performance of a computation during the actual time that the related physical process transpires so that the results of the computation can be used to guide the physical process. SOURCE: NIST IR 6859 [2]
Redundant Control Server	A backup to the control server that maintains the current state of the control server at all times. SOURCE: NIST IR 6859 [2]
Relay	An electromechanical device that completes or interrupts an electrical circuit by physically moving conductive contacts. The resultant motion can be coupled to another mechanism such as a valve or breaker. SOURCE: The Automation, Systems, and Instrumentation Dictionary

Programmable Logic Controller (PLC)：プログラマブル論理制御装置

ソリッドステート制御システムで、ユーザがプログラム可能なメモリがあり、I/O 制御、論理、タイミング、カウント、3 モード（PID）の制御、通信、演算、データやファイルの処理等の具体的な機能を実装するための命令を格納する。
出典：オートメーション・システム・計装事典

元々は電気的ハードウエア（リレー、スイッチ及び機械的タイマー/カウンター）により実行される論理機能を実行するために設計された小型の産業用コンピュータ。複雑なプロセスの制御能力を持ったコントローラに進化し、SCADA システム及び DCS で多用される。また、より小型のシステム構成中でプライマリコントローラとしても利用されている。PLC はほとんど全ての産業プロセスで広範に利用される。

Protocol：プロトコル

システム間のある種の関係（通信等）を実行し制御するための一連の規則（形式及び手順）。
出典：RFC 4949 [75]

Protocol Analyzer：プロトコル分析器

ネットワーク及び関連ハードウエア/ソフトウエアがネットワーク仕様内で動作するように、ユーザがネットワークデータのパフォーマンスを分析できるようにするデバイスまたはソフトウエア。
出典：オートメーション・システム・計装事典

Proximity Sensor：近接センサ

目標値が指定範囲にあることを検出できる非接触型センサ。
出典：NIST IR 6859 [2]

Proxy Server：プロキシサーバ

クライアントからの要求を他のサーバに転送するサーバ。
出典：CNSSI-4009

Real-Time：リアルタイム

計算に関係する物理プロセスが発生して、計算結果が物理プロセスの制御に利用できる実時間計算をいう。
出典：NIST IR 6859 [2]

Redundant Control Server：冗長制御サーバ

制御サーバのバックアップで、制御サーバの現在の状態を常時保持する。
出典：NIST IR 6859 [2]

Relay：リレー

接点を物理的に動かして電気回路を接続又は中断する電子機械式デバイス。その結果生じる運動は、バルブやブレーカといった別のデバイスに連携する。
出典：オートメーション・システム・計装事典

Remote Access	Access by users (or information systems) communicating external to an information system security perimeter. SOURCE: NIST SP 800-53 [22]
Remote Access Point	Distinct devices, areas and locations of a control network for remotely configuring control systems and accessing process data. Examples include using a mobile device to access data over a LAN through a wireless access point, and using a laptop and modem connection to remotely access an ICS system.
Remote Diagnostics	Diagnostics activities conducted by individuals communicating external to an information system security perimeter.
Remote Maintenance	Maintenance activities conducted by individuals communicating external to an information system security perimeter.
Remote Terminal Unit (RTU)	A computer with radio interfacing used in remote situations where communications via wire is unavailable. Usually used to communicate with remote field equipment. PLCs with radio communication capabilities are also used in place of RTUs. Special purpose data acquisition and control unit designed to support DCS and SCADA remote stations. RTUs are field devices often equipped with network capabilities, which can include wired and wireless radio interfaces to communicate to the supervisory controller. Sometimes PLCs are implemented as field devices to serve as RTUs; in this case, the PLC is often referred to as an RTU.
Resource Starvation	A condition where a computer process cannot be supported by available computer resources. Resource starvation can occur due to the lack of computer resources or the existence of multiple processes that are competing for the same computer resources.
Risk	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring. SOURCE: NIST SP 800-30 [79]
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis. Incorporates threat and vulnerability analyses. SOURCE: NIST SP 800-30 [79]

Remote Access：
リモートアクセス

情報システムのセキュリティ周辺外から通信を行うユーザ（又は情報システム）のアクセス。
出典：NIST SP 800-53 [22]

Remote Access Point：
リモートアクセス点

制御システムを遠隔設定し、プロセスデータにアクセスするための制御ネットワークの明確なデバイス、エリア及び場所。例えばモバイルデバイスを利用して、ワイヤレスアクセス点から LAN 経由のデータアクセス、ラップトップ及びモデムを利用した ICS システムアクセスがある。

Remote Diagnostics：
リモート診断

情報システムセキュリティ周辺外から個人が行う診断活動。

Remote Maintenance：
遠隔保守

情報システムセキュリティ周辺外から個人が行う保守活動。

Remote Terminal Unit (RTU)：
遠隔端末装置

有線通信が利用できない遠隔環境で使用する無線インタフェース付きコンピュータ。通常、遠隔フィールド装備品との通信に使用する。無線通信機能付き PLC も RTU の代わりに使用される。

DCS 及び SCADA 遠隔ステーションをサポートするための特殊目的でのデータ取得制御装置。RTU は、監視コントローラとの通信用有線・無線インタフェース等、ネットワーク機能を装備している場合が多い。PLC はフィールドデバイスとして実装され RTU として利用されることもある。PLC は RTU と呼ばれることが多い。

Resource Starvation：
リソース枯渇

利用可能なコンピュータリソースではコンピュータプロセスがサポートできない状態。コンピュータリソースの欠乏又は同じコンピュータリソースをめぐる複数プロセスの競合により生じることがある。

Risk：リスク

脅威の潜在的影響及び当該脅威が生じる蓋然性に鑑み、情報システムの運用から生じる政府機関の業務（任務、機能、イメージ、評判等）、政府機関の資産又は個人への影響度。
出典：NIST SP 800-30 [79]

Risk Assessment：
リスク評価

発生確率、その影響、影響を緩和するための付加的セキュリティ対策の判定を通じた政府機関の業務（任務、機能、イメージ、評判等）、資産又は個人に対するリスク識別プロセス。リスク管理の一部で、リスク分析と同義。脅威分析及び脆弱性分析を取り入れる。
出典：NIST SP 800-30 [79]

Risk Management	The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. SOURCE: FIPS 200, Adapted [16]
Risk Management Framework	The Risk Management Framework (RMF), presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. SOURCE: SP 800-37 [21]
Router	A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router operates on IP packets. SOURCE: RFC 4949 [75]
Router Flapping	A router that transmits routing updates alternately advertising a destination network first via one route, then via a different route.
Safety Instrumented System (SIS)	A system that is composed of sensors, logic solvers, and final control elements whose purpose is to take the process to a safe state when predetermined conditions are violated. Other terms commonly used include emergency shutdown system (ESS), safety shutdown system (SSD), and safety interlock system (SIS). SOURCE: ANSI/ISA-84.00.01
SCADA Server	The device that acts as the master in a SCADA system. SOURCE: NIST IR 6859 [2]
Security Audit	Independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures. SOURCE: ISO/IEC 7498
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: FIPS PUB 199 [15]

Risk Management：リスク管理
情報システムの運用から生じる、組織の運営（任務、機能、イメージ、評判等）及び資産、個人、他の組織又は国へのリスクを管理するプロセスで、以下を含む。（1）リスク評価の実施、（2）リスク緩和策の実施、（3）情報システムのセキュリティ状態を常続監視するための技術及び手順の採用。
出典：FIPS 200, Adapted [16]

Risk Management Framework：リスク管理体制
NIST SP 800-37 に示されるリスク管理体制（RMF）は、情報セキュリティ活動とリスク管理活動をシステム開発ライフサイクルに統合化するための統制の取れた組織化されたプロセスと定めている。
出典：SP 800-37 [21]

Router：ルータ
OSI レイヤー3 でのネットワークとデータパッケージを中継指向するネットワーク間のゲートウェイとなるコンピュータ。最も一般的な形態のルータは IP パケットで動作する。
出典：RFC 4949 [75]

Router Flapping：ルータフラッピング
経路更新を交互に送信するルータ。宛先ネットワークをまずある経路で広告し、次いで別経路で行う。

Safety Instrumented System (SIS)：安全計装システム
センサ、ロジックソルバー及び最終制御エレメントで構成されるシステムで、目的は予め定められた条件から逸脱した際に、プロセスを安全状態に戻すことにある。一般に使用されるその他の用語として緊急遮断システム（ESS）、安全遮断システム（SSD）、安全連動システム（SIS）等がある。
出典：ANSI/ISA-84.00.01

SCADA Server：SCADA サーバ
SCADA システムでマスターとなるデバイス。
出典：NIST IR 6859 [2]

Security Audit：セキュリティ監査
システム制御の適切性を判定し、規定のセキュリティポリシー及び手順の遵守を確保し、セキュリティサービス違反を検出し、対策として示唆される変更内容を勧告するためのシステムの記録及び活動に対する独立的な審査及び検証。
出典：ISO/IEC 7498

Security Controls：セキュリティ対策
システムとその情報の機密性、完全性及び可用性を保護するための情報システム用管理・運用・技術対策（安全策、対抗手段等）。
出典：FIPS PUB 199 [15]

Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. SOURCE: NIST SP 800-53 [22]
Security Policy	Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from organization or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent. SOURCE: ISA99
Sensor	A device that produces a voltage or current output that is representative of some physical property being measured (e.g., speed, temperature, flow). SOURCE: The Automation, Systems, and Instrumentation Dictionary A device that measures a physical quantity and converts it into a signal which can be read by an observer or by an instrument. A sensor is a device, which responds to an input quantity by generating a functionally related output usually in the form of an electrical or optical signal.
Servo Valve	An actuated valve whose position is controlled using a servo actuator. SOURCE: NIST IR 6859 [2]
Set Point	An input variable that sets the desired value of the controlled variable. This variable may be manually set, automatically set, or programmed. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Simple Network Management Protocol (SNMP)	A standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates. To work with SNMP, network devices utilize a distributed data store called the Management Information Base (MIB). All SNMP-compliant devices contain a MIB which supplies the pertinent attributes of a device. Some attributes are fixed or "hard-coded" in the MIB, while others are dynamic values calculated by agent software running on the device. SOURCE: API 1164
Single Loop Controller	A controller that controls a very small process or a critical process. SOURCE: NIST IR 6859 [2]
Social Engineering	An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. SOURCE: NIST SP 800-61 [59]

Security Plan：
セキュリティ計画書
情報システムのセキュリティ要件を概説した正式文書で、その要件を満足する実施中又は計画中のセキュリティ対策について記述したもの。
出典：NIST SP 800-53 [22]

Security Policy：
セキュリティポリシー
セキュリティポリシーはセキュリティプログラムの目的と制約事項を定義する。ポリシーはいくつかのレベルで作成され、組織又は企業ポリシーから具体的な運用上の制約事項（リモートアクセス等）までである。総じてポリシーは「何が」とか「なぜ」には答えるが、「どのように」という質問には答えていない。通常、技術とは無関係の用語で記述される。
出典：ISA99

Sensor：センサ
計測中の物理特性（速度、温度、流量等）を表した電圧又は電流出力を発生させるデバイス。
出典：オートメーション・システム・計装事典

物理的量を計測して信号に変換するデバイスで、信号は観察者や計器で読み取ることができる。機能的に関わりのある出力を、通常、電気又は光学信号として生成することにより、入力に対応するデバイス。

Servo Valve：
サーボバルブ
サーボアクチュエータを使用して位置を制御する作動弁。
出典：NIST IR 6859 [2]

Set Point：設定点
制御変数の所望の値を設定する入力変数。この変数はマニュアル操作、自動、プログラム化のいずれによっても設定可能である。
出典：オートメーション・システム・計装事典

Simple Network Management Protocol (SNMP)：
シンプルネットワーク管理プロトコル
ネットワーク管理用標準 TCP/IP プロトコル。ネットワーク管理者はこのプロトコルを使用してネットワークの可用性、パフォーマンス及びエラー率を監視する。SNMP に対応して、ネットワークデバイスは管理情報ベース（MIB）と呼ばれる分散データストアを使用する。全ての SNMP 適合デバイスは MIB を持っており、デバイスの関連属性を供給する。ある属性は MIB に固定又は「ハードコード」され、またあるものはデバイスで実行中のエージェントにより計算される動的値となる。
出典：API 1164

Single Loop Controller：
単一ループコントローラ
極めて小さなプロセス又は重要プロセスを制御するコントローラ。出典：NIST IR 6859 [2]

Social Engineering：
ソーシャルエンジニアリング
システムやネットワークの攻撃に使用するため、人を欺いて情報（パスワード等）を漏洩させるもくろみ。
出典：NIST SP 800-61 [59]

Solenoid Value	A valve actuated by an electric coil. A solenoid valve typically has two states: open and closed. SOURCE: NIST IR 6859 [2]
Spyware	Software that is secretly or surreptitiously installed onto an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. SOURCE: NIST SP 800-53 [22]
Statistical Process Control (SPC)	The use of statistical techniques to control the quality of a product or process. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Steady State	A characteristic of a condition, such as value, rate, periodicity, or amplitude, exhibiting only negligible change over an arbitrarily long period of time. SOURCE: ANSI/ISA-51.1-1979
Supervisory Control	A term that is used to imply that the output of a controller or computer program is used as input to other controllers. See *Control Server* SOURCE: The Automation, Systems, and Instrumentation Dictionary
Supervisory Control and Data Acquisition (SCADA)	A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated. SOURCE: The Automation, Systems, and Instrumentation Dictionary
System Security Plan	Formal document that provides an overview of the security requirements for a system and describes the security controls in place or planned for meeting those requirements. SOURCE: NIST SP 800-18, Adapted [19]
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system. SOURCE: NIST SP 800-18 [19]
Temperature Sensor	A sensor system that produces an electrical signal related to its temperature and, as a consequence, senses the temperature of its surrounding medium. SOURCE: NIST IR 6859 [2]

Solenoid Valve：
ソレノイドバルブ
電気コイルで作動する弁。通常「開」と「閉」の 2 つの状態がある。
出典：NIST IR 6859 [2]

Spyware：スパイウエア
気づかれずに個人又は組織の情報を収集するため、秘密裏に又は不正に情報システムに取り付けられるソフトウエアで、悪意あるコードの 1 種。
出典：NIST SP 800-53 [22]

Statistical Process Control (SPC)：
統計的プロセス管理
製品又はプロセスの品質を管理するための統計技術の使用。
出典：オートメーション・システム・計装事典

Steady State：定常状態
値、率、周期、規模等の状態特性をいい、任意の長期間にわたり変化が無視できること。
出典：ANSI/ISA-51.1-1979

Supervisory Control：
監視制御
コントローラ又はコンピュータプログラムの出力が他のコントローラの入力として使用されていることを示す用語。制御サーバを参照
出典：オートメーション・システム・計装事典

Supervisory Control and Data Acquisition (SCADA)：
監視制御データ取得
長距離のデータ収集処理と運用制御を行えるコンピュータ制御システムの汎用的な名称。送配電及びパイプライン等によく利用される。電話回線、マイクロ波、人工衛星等で使用される多様な媒体に特有の通信問題（遅延、データ整合性等）に対応して設計された。通常専用ではなく共有されることが多い。
出典：オートメーション・システム・計装事典

System Security Plan：
システムセキュリティ計画書
システムセキュリティ要件の概要を示し、要件を遵守するために施行中又は計画中のセキュリティ対策について説明した正式文書。
出典：NIST SP 800-18, Adapted [19]

Technical Controls：
技術制御
システムのハードウエア、ソフトウエア又はファームウエアコンポーネントに含まれるメカニズムを通じて、主に情報システムにより実装され実施される情報システム用のセキュリティ対策（安全策又は対抗手段）。
出典：NIST SP 800-18 [19]

Temperature Sensor：
温度センサ
温度に関する電気信号を発生させ、その結果周辺媒体の温度を検知するセンサシステム。
出典：NIST IR 6859 [2]

Threat	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. SOURCE: NIST SP 800-53 [22]
Threat Event	An event or situation that has the potential for causing undesirable consequences or impact. SOURCE: SP 800-30 [79]
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with Threat Agent. SOURCE: FIPS 200 [16]; SP 800-53 [22]; SP 800-53A [23]; SP 800-37 [21]
Transmission Control Protocol (TCP)	TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent. SOURCE: API 1164
Trojan Horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. SOURCE: RFC 4949 [75]
Unauthorized Access	A person gains logical or physical access without permission to a network, system, application, data, or other resource. SOURCE: NIST SP 800-61 [59]
Unidirectional Gateway	Unidirectional gateways are a combination of hardware and software. The hardware permits data to flow from one network to another, but is physically unable to send any information at all back into the source network. The software replicates databases and emulates protocol servers and devices.
Valve	An in-line device in a fluid-flow system that can interrupt flow, regulate the rate of flow, or divert flow to another branch of the system. SOURCE: The Automation, Systems, and Instrumentation Dictionary
Variable Frequency Drive (VFD)	A type of drive that controls the speed, but not the precise position, of a non-servo, AC motor by varying the frequency of the electricity going to that motor. VFDs are typically used for applications where speed and power are important, but precise positioning is not. SOURCE: NIST IR 6859 [2]

Threat：脅威
不正アクセス、破壊、開示、情報の改変又はサービス妨害を通じて、政府機関の業務（任務、機能、イメージ、評判等）、政府機関の資産又は個人に悪影響を及ぼしかねない状況又は事象。
出典：NIST SP 800-53 [22]

Threat Event：脅威事象
望ましくない結果や影響を生じかねない事象又は状況。
出典：SP 800-30 [79]

Threat Source：脅威源
脆弱性又は状況及び方法を故意に利用することをもくろむ意思及び方法で、偶発的に脆弱性を生じさせる原因となり得る。脅威エージェントと同義。
出典：FIPS 200 [16]; SP 800-53 [22]; SP 800-53A [23]; SP 800-37 [21]

Transmission Control Protocol (TCP)：通信制御プロトコル
TCP/IP ネットワークにおける主なプロトコルの 1 つ。IP プロトコルがパケット処理だけなのに対し、TCP は 2 台のホストが接続を確立してデータストリームを交換できるようにする。データの配送を保証し、パケットを送信順に届くようにできる。
出典：API 1164

Trojan Horse：トロイの木馬
コンピュータプログラムで、便利な機能も持つが、隠れた悪意ある機能があり、プログラムを起動したシステム実在者の適格性を利用して、セキュリティ機構に侵入する。
出典：RFC 4949 [75]

Unauthorized Access：不正アクセス
ネットワーク、システム、アプリケーション、データその他のリソースに、人が許可なく論理的又は物理的アクセスすること。
出典：NIST SP 800-61 [59]

Unidirectional Gateway：単方向ゲートウェイ
単方向性ゲートウェイはハードウエアとソフトウエアを組み合わせたものである。ハードウエアはデータが一方のネットワークから他方のネットワークへ流れるのを許可するが、ソースネットワークに情報を返すことは物理的に不可能である。ソフトウエアはデータベースを複製して、プロトコルサーバ及びデバイスをエミュレートする。

Valve：バルブ（弁）
流体システム中のインラインデバイスで、流れを遮断し、流量を調節し、システム中での流れの方向を変えることができる。
出典：オートメーション・システム・計装事典

Variable Frequency Drive (VFD)：可変周波数駆動
モータへの電気周波数を変えることにより、非サーボ型の交流モータの速度を制御する駆動の 1 種で、精確な位置は制御できない。一般に速度と電力が重視され、精確な位置は重要でない用途に利用される。
出典：NIST IR 6859 [2]

Virtual Private Network (VPN)	A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. SOURCE: RFC 4949 [75]
Virus	A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active. SOURCE: RFC 4949 [75]
Virus Definitions	Predefined signatures for known malware used by antivirus detection algorithms.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. SOURCE: NIST SP 800-53 [22]
Whitelist	A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system. SOURCE: SP 800-128 [80]
Wide Area Network (WAN)	A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and that is usually spread over a larger geographic area than that of a LAN. SOURCE: API 1164
Wireless Device	Any device that can connect to an ICS network via radio or infrared waves, usually to collect or monitor data, but also in some cases to modify control set points.
Workstation	A computer used for tasks such as programming, engineering, and design. SOURCE: NIST IR 6859 [2]
Worm	A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. SOURCE: RFC 4949 [75]

Virtual Private Network (VPN)：仮想プライベートネットワーク	限定的に使用される論理的（人工的又は模擬的）コンピューターネットワークで、比較的公開された物理的（現実的）ネットワーク（インターネット等）から構築され、暗号化を利用することが多く（ホスト又はゲートウェイで）、仮想ネットワークリンクを実ネットワークにトンネリングすることが多い。 出典：RFC 4949 [75]
Virus：ウイルス	コンピューターソフトウエアの隠れた自己複製セクションで、通常悪意あるロジックであり、他のプログラムを感染させる（コピーを挿入して自分がプログラムの一部となる）ことで増殖する。ウイルスはそれ自体で実行することはできず、ホストプログラムによってアクティブにされる必要がある。 出典：RFC 4949 [75]
Virus Definitions：ウイルス定義	アンチウイルス検知アルゴリズムで使用される既知のマルウエアの事前定義シグネチャ。
Vulnerability：脆弱性	情報システム、システムセキュリティ手順、内部制御又は実装における弱点で、脅威源により利用又は起動される。 出典：NIST SP 800-53 [22]
Whitelist：ホワイトリスト	善良であることが知られており、組織又は情報システム中で、利用を許可されているホストやアプリケーション等の個別実体リスト。 出典：SP 800-128 [80]
Wide Area Network (WAN)：広域ネットワーク	通常、LAN サービスよりもユーザ数が多く、より広域にまたがってデータ通信サービスを行う物理的又は論理的ネットワーク。 出典：API 1164
Wireless Device：ワイヤレスデバイス	通常、データの収集又は監視を目的に無線又は赤外線で ICS ネットワークに接続できるデバイスで、制御設定点の変更に使用することもある。
Workstation：ワークステーション	プログラミング、エンジニアリング、設計等のタスクに使用するコンピュータ。 出典：NIST IR 6859 [2]
Worm：ワーム	独立して実行できるコンピュータプログラムで、自分自身の完全な動作バージョンを他のホスト上に伝播させ、コンピュータリソースを破壊的に消費する。 出典：RFC 4949 [75]

Appendix C—Threat Sources, Vulnerabilities, and Incidents

Several terms are used to describe the inter-related concepts of threat, threat source, threat event, and incident. A *threat* is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Threats have some intent or method that may exploit of a vulnerability through either intentional or unintentional means, this intent or method referred to as the *threat source*. A *vulnerability* is a weakness in an information system (including an ICS), system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. A *threat event* is an event or situation that has the potential for causing undesirable consequences or impact. When a threat event occurs it becomes an *incident* that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. This section will explore ICS-specific threat sources, vulnerabilities, and incidents.

Threat Sources

Threats to ICS can come from numerous sources, which can be classified as adversarial, accidental, structural, and environmental. Table C-1 lists and defines known threats sources to ICS. It is necessary to create a risk management strategy for the ICS that protects the system against these possible threat sources. The threat source must be well understood in order to define and implement adequate protection. For example, environmental events (e.g. floods, earthquakes) are well understood, but may vary in their magnitude, frequency, and their ability to compound other interconnected events. However, adversarial threats depend on the resources available to the adversary and the emergence of previously unknown vulnerabilities or attacks.

Table C-1. Threats to ICS

Type of Threat Source	Description	Characteristics
ADVERSARIAL - Individual - Outsider - Insider - Trusted Insider - Privileged Insider - Group - Ad hoc - Established - Organization - Competitor - Supplier - Partner - Customer - Nation-State	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (e.g., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies)	Capability, Intent, Targeting
ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

付録 C　脅威源、脆弱性及びインシデント

脅威、脅威源、脅威事象及びインシデントの相互に関連し合った概念を示すのにいくつかの用語が用いられる。脅威とは、不正アクセス、破壊、開示、情報の改変又はサービス妨害により、情報システムを通じて、組織業務（任務、機能、イメージ、評判等）、組織資産、個人、他の組織又は国に悪影響を及ぼしかねない状況又は事象をいう。脅威には、故意又は意図しない手段で脆弱性を利用する意思又は方法があり、この意思又は方法を脅威源という。脆弱性とは情報システム（ICS を含む）、システムセキュリティ手順、内部制御又は実装における弱点で、脅威源により利用又は起動される。脅威事象は、望ましくない結果や影響を生じかねない事象又は状況をいう。脅威事象が生起するとインシデントとなり、インシデントは、情報システム又はシステムが処理・保管・送信する情報の機密性・完全性・可用性を実際に危険に陥れるか、その可能性があり、またセキュリティポリシー、セキュリティ手順又は受け入れられるポリシーの使用の違反又は直ちに違反となる脅威を構成する。このセクションでは、ICS 固有の脅威源、脆弱性及びインシデントについて説明する。

脅威源

ICS の脅威には多様な起源があり、敵性、偶発性、構造性及び環境性に分類できる。表 C-1 は、ICS の既知の脅威とその定義を示す。システムをこのような脅威源から守るため、ICS リスク管理戦略を策定する必要がある。しっかり保護できるよう、脅威源を十分理解しなければならない。例えば、環境的事象（洪水、地震等）についてはよく理解できても、そのマグニチュード、頻度及び他の関連事象と複合したときの潜在力は一様でない。しかし敵性脅威は、敵が利用できるリソースと、以前知られていた脆弱性又は攻撃の出現に依存する。

表 C-1. ICS の脅威

脅威源の種類	内容	特徴
敵性 - 個人 - 部外者 - インサイダー - 信頼の置けるインサイダー - 権限のあるインサイダー - グループ - アドホック - 常勤 - 組織 - 競合相手 - サプライヤ - パートナー - 顧客 - 国・州	組織のサイバーリソース（電子情報、情報・通信技術、これら技術により提供される通信・情報処理能力等）への依存性を利用しようともくろむ個人、グループ、組織又は国	能力、意思、目標選定
偶発性 - ユーザ - 特権ユーザ/管理者	個人が日常業務を果たす際の過誤行為	影響範囲

Type of Threat Source	Description	Characteristics
STRUCTURAL - Information Technology (IT) Equipment - Storage - Processing - Communications - Display - Sensor - Controller - Environmental Controls - Temperature/Humidity Controls - Power Supply - Software - Operating System - Networking - General-Purpose Application - Mission-Specific Application	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects
ENVIRONMENTAL - Natural or man-made disaster - Fire - Flood/Tsunami - Windstorm/Tornado - Hurricane - Earthquake - Bombing - Overrun - Unusual Natural Event (e.g., sunspots) - Infrastructure Failure/Outage - Telecommunications - Electrical Power	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization. Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).	Range of effects

Vulnerabilities and Predisposing Conditions

This section addresses vulnerabilities and predisposing conditions that may be found in typical ICS. *Vulnerabilities* are weaknesses in information systems, system procedures, controls, or implementations the can be exploited by a threat source. *Predisposing conditions* are properties of the organization, mission/business process, architecture, or information systems that contribute to the likelihood of a threat event. The order of these vulnerabilities and predisposing conditions does not necessarily reflect any priority in terms of likelihood of occurrence or severity of impact. Additionally, the vulnerabilities and predisposing conditions identified in this section should not be considered a complete list; it should also not be assumed that these issues are found within every ICS.

脅威源の種類	内容	特徴
構造的 - 情報技術（IT）装備品 - ストレージ - 処理 - 通信 - ディスプレイ - センサ - コントローラ - 環境制御 - 温度・湿度制御 - 電源 - ソフトウエア - オペレーティングシステム - ネットワーキング - 汎用アプリケーション - 任務固有アプリケーション	経年、リソース不足その他の状況による予想運転パラメータを超える装備品、環境制御又はソフトウエアの障害	影響範囲
環境的 - 自然・人為災害 - 火災 - 洪水・津波 - 暴風・トルネード - ハリケーン - 地震 - 爆破 - オーバーラン - 異常天然現象（太陽黒点等） - インフラ障害/停止 - 無線通信 - 電力	自然災害及び組織が依存する重要インフラの障害で、組織の制御外のもの 注：自然・人為災害は重大性と期間により特徴づけられる。しかし脅威源及び脅威事象は特定されているので、重大性と期間は、脅威事象中に含められる（例えばカテゴリー5 のハリケーンは、任務に不可欠なシステムのある施設に甚大な被害を与え、システムが 3 週間使用不能になる）。	影響範囲

脆弱性及び弱点となる状態

このセクションでは、一般的な ICS にありがちな脆弱性と弱点となる状態について取り上げる。脆弱性は情報システム、システム手順、制御又は実装における弱点で、脅威源により利用されやすい。弱点となる状態とは、組織、任務・事業プロセス、アーキテクチャ又は情報システムの特性で、脅威事象が生じる公算を高める。このような脆弱性と弱点となる状態は、発生の公算と影響の重大性の点で必ずしも優先づけがあるわけではない。また、このセクションで取り上げるものが全てというわけでもない。逆にどの ICS にもこれらが必ずあるというものでもない。

The vulnerabilities and predisposing conditions are grouped according to where they exist–such as in the organization's policy and procedures, or the inadequacy of security mechanisms implemented in hardware, firmware, and software. The former are referred to as being in the organization and the latter as being in the system. Understanding the source of vulnerabilities and predisposing conditions can assist in determining optimal mitigation strategies. The groups of vulnerabilities used in this appendix are:

- Policy and Procedure.
- Architecture and Design.
- Configuration and Maintenance.
- Physical.
- Software Development.
- Communication and Network.

Deeper analysis may uncover that causes and observations may not be one-to-one; that is, some underlying causes may exhibit multiple symptoms and some symptoms may come from more than one cause. SP 800-53 contains a taxonomy of security controls, or countermeasures, to mitigate vulnerabilities and predisposing conditions. These are categorized in families, where each family contains security controls related to the general security topic of the family. While the families and controls from 800-53 provide a more complete overview of the potential vulnerabilities and predisposing conditions within in an ICS, this section briefly reviews those issues known to be common within ICS.

Any given ICS will usually exhibit a subset of the identified vulnerabilities, but may also contain additional vulnerabilities and predisposing conditions unique to the particular ICS implementation that do not appear in this appendix. Specific current information on ICS vulnerabilities can be researched at the Industrial Control System Computer Emergency Response Team (ICS-CERT) Web site.[45]

Some vulnerabilities and predisposing conditions can be mitigated; others can only be accepted and controlled by appropriate countermeasures, but will result in some residual risk to the ICS. For example, some existing policies and procedures may be changed with a level of effort that the organization considers acceptable; others are more expeditiously dealt with by instituting additional policies and procedures.

Vulnerabilities in products and services acquired from outside the organization are rarely under the direct control of the organization. Changes may be influenced by market forces, but this is a slow and indirect approach. Instead, the organization may change predisposing conditions to reduce the likelihood that a systemic vulnerability will be exploited.

Policy and Procedure Vulnerabilities and Predisposing Conditions

Vulnerabilities and predisposing conditions are often introduced into the ICS because of incomplete, inappropriate, or nonexistent security policy, including its documentation, implementation guides (e.g., procedures), and enforcement. Management support of security policy and procedures is the cornerstone of any security program. Organization security policy can reduce vulnerabilities by mandating and enforcing proper conduct. Written policy and procedures are mechanisms for informing staff and stakeholders of decisions about behavior that is beneficial to the organization. From this perspective, policy is an educational and instructive way to reduce vulnerabilities. Enforcement is partner to policy, encouraging people to do the "right" thing. Various forms of corrective action are the usual consequences

[45] http://ics-cert.us-cert.gov. http://ics-cert.us-cert.gov..

脆弱性と弱点となる状態は、どこにあるかに応じてグループ分けできる。例えば、組織のポリシー及び手順、ハードウエア、ファームウエア、ソフトウエアのセキュリティメカニズムの不備等である。前者は組織、後者はシステムにあるということになる。脆弱性と弱点となる状態の起源を理解すると、最適の緩和策が決めやすくなる。この付録で使用する脆弱性のグループは以下のとおり。

- ポリシー及び手順
- アーキテクチャ及び設計
- 構成及び保守
- 物理面
- ソフトウエア開発
- 通信及びネットワーク

深く分析すると、原因と観察結果が 1 対 1 でないことが分かる。つまり、特定の根本原因から複数の徴候が生じ、特定の徴候は複数の原因から生じている。SP 800-53 にはセキュリティ対策の分類、言い換えれば脆弱性と弱点となる状態を緩和する対策が載せられている。ファミリ別に分類され、各ファミリにはそのファミリの全般的セキュリティ問題に関するセキュリティ対策が含まれている。800-53 の系列と管理は、ICS 内の脆弱性と弱点となる状態に関するより完成度の高い概説があり、このセクションでは、ICS に共通的な問題を手短に振り返る。

どの ICS でも通常明らかになっている脆弱性の一部が露呈しているが、特定の ICS 実装に固有の、この付録では取り上げられていない脆弱性と弱点となる状態もある。ICS の脆弱性に関する特定の現行情報が産業用制御システムコンピュータ緊急時対応チーム（ICS-CERT）のサイトにある[46]。

いくつかの脆弱性と弱点となる状態は緩和できる。その他については、許容するか適当な対策で管理するしかないが、ICS の残留リスクとなる。例えば、既存ポリシー及び手順は、組織が許容できるあるレベルの取組で変更されるものもあれば、補足的なポリシー及び手順を制定して、もっと迅速に処理できるものもある。

組織外から取得した製品やサービスの脆弱性は、組織の直接の管理下に置かれることはまずない。変更は市場力に影響されるが、緩慢で間接的である。代わりに、組織は弱点となる状態を変えて、システムの脆弱性をつかれる可能性を低くすることができよう。

ポリシー及び手順の脆弱性及び弱点となる状態

脆弱性及び弱点となる状態は、セキュリティポリシーの不備、不適切又は欠如により ICS に持ち込まれることが多く、例えば文書、実施ガイド（手順等）、施行等である。セキュリティ及び手順に対する経営陣による支援は、あらゆるセキュリティプログラムの土台となる。組織のセキュリティポリシーは、適正な行動を義務づけて施行することで、脆弱性を減らすことができる。書面にしたポリシー及び手順は、職員及び関係者に、組織の利益となる行動に関する決定事項を知らしめるメカニズムとなる。この観点から、ポリシーは脆弱性を減らすための教育的・教訓的方法となる。施行はポリシーの「パートナー」であり、「正しい」ことを行うよう人を奨励する。多様な形態の是正処置は、ポリシー及び手順を遵守していない職員に対して通常、適用される。

[46] http://ics-cert.us-cert.gov. http://ics-cert.us-cert.gov.

to personnel not following policy and procedures. Policies should be explicit about the consequences to individuals or organizations that do not conform.

There is usually a complex policy and procedure environment that includes laws and regulations, overlapping jurisdictions and spheres of influence, economics, custom, and history. The larger enterprise is often subdivided into organizational units that should work together to reduce vulnerabilities. The scope and hierarchical relationship among policies and procedures needs to be managed for maximum effectiveness.

Certain controls in SP 800-53 and the ICS overlay in Appendix G— specify responsibilities and requirements for the organization, while others focus on the capabilities and operation of the various systems within the organization. For example, the control AC-6, Least Privilege, states "The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions." The organization has to make decisions that get codified in policy and procedures. Some resulting artifacts, such as job descriptions that include roles, responsibilities, and authority, remain in a form suitable for people, while other artifacts, such as attributes, privileges, and access control rules, are implemented in IT.

Note that the ICS overlay follows SP 800-53 in employing the term "organization" very flexibly so that its guidance can be used by all sizes of organizational entities up and down an organization chart. Specific organizations should be identified, starting with the organization responsible for issuing and maintaining the policy or procedure.

Table C-2 presents examples of observed policy and procedure vulnerabilities for ICS.

Table C-2. Policy and Procedure Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Inadequate security policy for the ICS	Vulnerabilities are often introduced into ICS due to inadequate policies or the lack of policies specifically for control system security. Every countermeasure should be traceable to a policy. This ensures uniformity and accountability. Policy must include portable and mobile devices used with ICS.
No formal ICS security training and awareness program	A documented formal security training and awareness policy and program is designed to keep staff up to date on organizational security policies and procedures as well as threats, industry cybersecurity standards, and recommended practices. Without training on specific ICS policies and procedures, staff cannot be expected to maintain a secure ICS environment.
Absent or deficient ICS equipment implementation guidelines	Equipment implementation guidelines should be kept up to date and readily available. These guidelines are an integral part of security procedures in the event of an ICS malfunction.
Lack of administrative mechanisms for security policy enforcement	Staff responsible for enforcing security should be held accountable for administering documented security policies and procedures.
Inadequate review of the effectiveness of the ICS security controls	Procedures and schedules should exist to determine the extent to which the security program and its constituent controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the ICS. The examination is sometimes called an "audit," "evaluation," or "assessment." Policy should address the stage of the life-cycle, purpose, technical expertise, methodology, and level of independence.

ポリシーは、遵守していない個人又は組織に対し、結果に関して明示的であるべきである。

法規を包含し、影響、経済、習慣及び歴史の管轄及び範囲が重なり合う、複雑なポリシー及び手順環境が常に存在する。大企業は、脆弱性を減らすために協働できる組織単位に細分化されることが多い。ポリシー及び手順間の範囲と階層的関係を管理して、最大の効果を上げるべきである。

SP 800-53 及び付録 G の ICS オーバーレイに含まれている特定の管理には、責任と組織要件が記載されており、また別なものは組織内の多様なシステムの能力と運用が重点になっている。例えば、管理 AC-6 最小権限には、「組織は最小権限の原則を採用し、組織の任務・事業上の機能に応じて割り当てられた仕事を遂行するのに必要なユーザ（又はその代わりとなるプロセス）だけにアクセス権限を与える」とある。組織は決定しなければならず、決定事項はポリシー及び手順に明記される。その結果は、例えば役割・責任・権限を明記した職務明細書となり、職員に適した形態を取るものもあれば、属性・特権・アクセス制御規則のように、IT において実施されるものもある。

ICS オーバーレイは SP 800-53 に準拠して、「組織」という語を極めて柔軟に用いているため、そのガイダンスは、組織の大小様々な部署で使用できる。まずポリシー又は手順の発出・維持を担当する組織を皮切りに、特定の組織を明らかにすべきである。

表 C-2 は、観察されている ICS 用ポリシー及び手順の脆弱性を示す。

表 C-2. ポリシー及び手順の脆弱性及び弱点となる状態

脆弱性	内容
ICS 用セキュリティポリシーの不備	特に制御システムのセキュリティに関するポリシーの不備又は欠如から、ICS に脆弱性が入り込むことが多い。それぞれの対策はポリシーから出ているべきである。これにより統一性と説明責任が確保される。ポリシーは携行/モバイルデバイスも含めなければならない。
正規の ICS セキュリティ訓練・意識プログラム計画の欠如	文書化された正規のセキュリティ訓練・意識ポリシー計画は、常に最新のセキュリティポリシー・手順、脅威、産業用サイバーセキュリティ規格及び推奨規範を職員に知らしめるためにある。具体的な ICS ポリシー及び手順がなければ、職員に ICS 環境のセキュリティを維持できると期待することはできない。
ICS 装備品実装ガイドラインの欠如又は欠陥	装備品実装ガイドラインは最新状態に保ち、すぐに利用できるべきである。ガイドラインは、ICS 障害の際にセキュリティ手順の不可欠な一部となる。
セキュリティポリシーを施行する管理機構の欠如	セキュリティの施行担当職員は、文書化されたセキュリティポリシー及び手順の管理に説明責任を有する。
ICS セキュリティ対策の効果性に対する見直しの不備	セキュリティプログラムとその対策がどの程度適正に実施されているか、予定どおり稼働しているか、所期の結果をもたらしているかを、ICS セキュリティ要件の達成という観点で判定する手順及びスケジュールを定めるべきである。この検証を「監査」、「評価（evaluation）」又は「評価（assessment）」と呼ぶこともある。ポリシーはライフサイクルの段階、目的、技術知見、方法論及び独立レベルを取り上げるべきである。

Vulnerability	Description
No ICS-specific contingency plan	A contingency plan should be prepared, tested and available in the event of a major hardware or software failure or destruction of facilities. Lack of a specific plan for the ICS could lead to extended downtimes and production loss.
Lack of configuration management policy	Lack of policy and procedures for ICS configuration change management can lead to unmanageable and highly vulnerable inventory of hardware, firmware, and software.
Lack of adequate access control policy	Access control enforcement depends of policy the correctly models roles, responsibilities, and authorizations. The policy model must enable the way the organization functions.
Lack of adequate authentication policy	Authentication policies are needed to define when authentication mechanisms (e.g., passwords, smart cards) must be used, how strong they must be, and how they must be maintained. Without policy, systems might not have appropriate authentication controls, making unauthorized access to systems more likely. Authentication policies should be developed as part of an overall ICS security program taking into account the capabilities of the ICS and its personnel to handle more complex passwords and other mechanisms.
Inadequate incident detection and response plan and procedures	Incident detection and response plans, procedures, and methods are necessary for rapidly detecting incidents, minimizing loss and destruction, preserving evidence for later forensic examination, mitigating the weaknesses that were exploited, and restoring ICS services. Establishing a successful incident response capability includes continually monitoring for anomalies, prioritizing the handling of incidents, and implementing effective methods of collecting, analyzing, and reporting data.
Lack of redundancy for critical components	Lack of redundancy in critical components could provide single point of failure possibilities

System Vulnerabilities and Predisposing Conditions

Security controls must clearly identify the systems to which they apply. Systems range widely in size, scope, and capability. At the small end of the spectrum, a system may be an individual hardware or software product or service. At the other end of the spectrum we find large complex systems, systems-of-systems, and networks, all of which incorporate hardware architecture and software framework (including application frameworks), where the combination supports the operation of the ICS.

System vulnerabilities can occur in the hardware, firmware, and software used to build the ICS. Sources of vulnerabilities include design flaws, development flaws, misconfigurations, poor maintenance, poor administration, and connections with other systems and networks. Many of the controls in the SP 800-53 and the ICS overlay in Appendix G— specify what the system must do to mitigate these vulnerabilities. The potential vulnerabilities and predisposing conditions commonly found within ICS systems are categorized with the following tables:

- Table C-3. Architecture and Design Vulnerabilities and Predisposing Conditions.
- Table C-4. Configuration and Maintenance Vulnerabilities and Predisposing Conditions.
- Table C-5. Physical Vulnerabilities and Predisposing Conditions.

脆弱性	内容
ICS 固有の緊急時対応計画の欠如	緊急時対応計画を作成し、検証し、大規模なハードウエア又はソフトウエア障害時や施設破壊時に利用できるようにすべきである。ICS の具体的計画書がないと、ダウンタイムや生産損失が拡大しかねない。
構成管理ポリシーの欠如	ICS 構成管理ポリシー及び手順の欠如は、ハードウエア、ファームウエア及びソフトウエアの管理できない大きな脆弱性につながる。
適正なアクセス制御ポリシーの欠如	アクセス制御の施行は、ポリシーの正しいモデル役割、責任及び権限付与にかかっている。ポリシーモデルは、組織が機能するための方法を実現しなければならない。
適正な認証ポリシーの欠如	認証メカニズム（パスワード、スマートカード等）を利用する際に、認証ポリシーはメカニズムの強度及び維持方法を明らかにする必要がある。ポリシーがなければ、システムは適正な認証管理ができず、無駄アクセスを許すことになる。認証ポリシーは、全体的な ICS セキュリティプログラムの一環として作成し、ICS の能力と、より複雑なパスワードその他のメカニズムを扱う職員の能力とを考慮に入れるべきである。
インシデント検知・対応計画書及び手順の不備	インシデント検知・対応計画書、手順及び方法はインシデントの迅速な検知、損失・破壊の局限、後日必要となる調査検証用証拠の保存、利用された弱点の緩和及び ICS サービスの復旧を行う上で必要である。有効なインシデント対応能力には、異常に対する継続監視、インシデント処理の優先づけ、効果的なデータ収集・分析・報告方法の実施が含まれる。
重要コンポーネントの冗長性の欠如	重要コンポーネントの冗長性の欠如は、単一障害点となりかねない。

システムの脆弱性及び弱点となる状態

セキュリティ対策では、適用対象となるシステムを特定しなければならない。システムの規模、範囲及び能力は多種多様である。最小システムは、個々のハードウエア若しくはソフトウエア製品又はサービスでもよい。反対に最大システムは、大規模複合システム、システム中にシステムのあるもの及びネットワークで、これらはハードウエアアーキテクチャ及びソフトウエアフレームワーク（アプリケーションフレームワーク等）を含み、それらが一体となって ICS の運用を支える。

システム脆弱性は ICS を構築するハードウエア、ファームウエア及びソフトウエアで生じ得る。脆弱性の原因には設計上の欠陥、開発上の欠陥、設定ミス、保守の不備、管理の不備及び他のシステムやネットワークへの接続等がある。SP 800-53 及び付録 G の ICS オーバーレイに含まれている管理の多くは、このような脆弱性を緩和するためにシステムが行わなければならない事柄を規定している。

ICS で一般的に見られる脆弱性及び弱点となる状態を以下の表に分類する。

- 表 C-3.アーキテクチャ及び設計上の脆弱性及び弱点となる状態
- 表 C-4.構成及び保守上の脆弱性及び弱点となる状態
- 表 C-5.物理的脆弱性及び弱点となる状態

- Table C-6. Software Development Vulnerabilities and Predisposing Conditions.
- Table C-7. Communication and Network Configuration Vulnerabilities and Predisposing Conditions.

Table C-3. Architecture and Design Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Inadequate incorporation of security into architecture and design.	Incorporating security into the ICS architecture, design must start with budget, and schedule of the ICS. The security architecture is part of the Enterprise Architecture. The architectures must address the identification and authorization of users, access control mechanism, network topologies, and system configuration and integrity mechanisms.
Insecure architecture allowed to evolve	The network infrastructure environment within the ICS has often been developed and modified based on business and operational requirements, with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within particular portions of the infrastructure. Without remediation, these gaps may represent backdoors into the ICS.
No security perimeter defined	If the ICS does not have a security perimeter clearly defined, then it is not possible to ensure that the necessary security controls are deployed and configured properly. This can lead to unauthorized access to systems and data, as well as other problems.
Control networks used for non-control traffic	Control and non-control traffic have different requirements, such as determinism and reliability, so having both types of traffic on a single network makes it more difficult to configure the network so that it meets the requirements of the control traffic. For example, non-control traffic could inadvertently consume resources that control traffic needs, causing disruptions in ICS functions.
Control network services not within the control network	Where IT services such as Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP) are used by control networks, they are often implemented in the IT network, causing the ICS network to become dependent on the IT network that may not have the reliability and availability requirements needed by the ICS.
Inadequate collection of event data history	Forensic analysis depends on collection and retention of sufficient data. Without proper and accurate data collection, it might be impossible to determine what caused a security incident to occur. Incidents might go unnoticed, leading to additional damage and/or disruption. Regular security monitoring is also needed to identify problems with security controls, such as misconfigurations and failures.

Table C-4. Configuration and Maintenance Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Hardware, firmware, and software not under configuration management.	The organization doesn't know what it has, what versions it has, where they are, or what their patch status is, resulting in an inconsistent, and ineffective defense posture. A process for controlling modifications to hardware, firmware, software, and documentation should be implemented to ensure an ICS is protected against inadequate or improper modifications before, during, and after system implementation. A lack of configuration change management procedures can lead to security oversights, exposures, and risks. To properly secure an ICS, there should be an accurate listing of the assets in the system and their current configurations. These procedures are critical to executing business continuity and disaster recovery plans.

- 表 C-6.ソフトウエア開発上の脆弱性及び弱点となる状態
- 表 C-7.通信及びネットワーク構成上の脆弱性及び弱点となる状態

表 C-3.アーキテクチャ及び設計上の脆弱性及び弱点となる状態

脆弱性	内容
アーキテクチャ及び設計へのセキュリティ組込み上の不備	セキュリティを ICS アーキテクチャに組み込む際、予算及び ICS のスケジュールから設計を開始しなければならない。セキュリティアーキテクチャは企業アーキテクチャの一部となる。アーキテクチャはユーザの識別・認証、アクセス制御メカニズム、ネットワークトポロジー及びシステム構成・完全性メカニズムを取り上げなければならない。
更に進行しそうなセキュアでないアーキテクチャ	ICS 内のネットワークインフラ環境は、事業・運用上の要件を基に開発・改修されていることが多く、変更内容がセキュリティに及ぼす影響はあまり考慮されていない。時間の経過とともに、想定外のセキュリティギャップがインフラの特定部位に生じることがある。対策を取らずにいると、そのようなギャップが ICS のバックドアになることがある。
セキュリティ境界が未定義	ICS のセキュリティ周辺の定義が明らかでないと、必要なセキュリティ対策の展開・設定が正しく実施できない。このためシステムやデータへの不正アクセスを許し、他の問題も発生しかねない。
制御ネットワークを制御以外のトラフィックに使用	決定論や信頼性等、制御トラフィックと非制御トラフィックの要件は異なるため、双方を 1 つのネットワークで使用すると、制御トラフィック要件を達成するためのネットワーク設定が難しくなる。例えば非制御トラフィックは、制御トラフィックが必要とするリソースを想定外に消費することがあり、ICS 機能の中断を招くことがある。
制御ネットワークサービスが制御ネットワーク内にない	制御システムに領域名システム（DNS）や動的ホスト構成プロトコル（DHCP）等の IT サービスを利用している場合、サービスは IT ネットワーク内に実装されていることが多いため、ICS ネットワークが ICS の信頼性及び可用性要件に満たない IT ネットワークに依存する結果になる。
イベントデータヒストリアン収集の不備	調査分析は十分なデータ収集・保持に依存する。適正かつ正確なデータの収集がなければ、セキュリティインシデントの発生理由を判別できない。インシデントに気づかず、損害や中断を拡大しかねない。設定ミスや障害等、セキュリティ対策の問題点を見極めるため、定期的なセキュリティ監視も必要となる。

表 C-4.構成及び保守上の脆弱性及び弱点となる状態

脆弱性	内容
ハードウエア/ファームウエア/ソフトウエアが構成管理外にある	何を使用しているか、どのバージョンか、どこにあるか、パッチステータスがどうなっているかを組織が知らず、一貫性と効果性のない防御態勢になる。ハードウエア/ファームウエア/ソフトウエア・文書への変更を管理するプロセスを実施し、システム実装前・中・後の不適切な改変から ICS を保護する。構成変更管理手順の欠如は、セキュリティの手抜かり、曝露及びリスクにつながる。ICS のセキュリティをしっかり確保するには、システム資産とその現行構成の正確なリストが持つべきである。このような手順が事業継続性と災害復旧計画の実施に重要となる。

Vulnerability	Description
OS and vendor software patches may not be developed until significantly after security vulnerabilities are found	Because of the tight coupling between ICS software and the underlying ICS, changes must undergo expensive and time-consuming comprehensive regression testing. The elapsed time for such testing and subsequent distribution of updated software provides a long window of vulnerability
OS and application security patches are not maintained or vendor declines to patch vulnerability	Out-of-date OSs and applications may contain newly discovered vulnerabilities that could be exploited. Documented procedures should be developed for how security patches will be maintained. Security patch support may not even be available for ICS that use outdated OSs, so procedures should include contingency plans for mitigating vulnerabilities where patches may never be available.
Inadequate testing of security changes	Modifications to hardware, firmware, and software deployed without testing could compromise normal operation of the ICS. Documented procedures should be developed for testing all changes for security impact. The live operational systems should never be used for testing. The testing of system modifications may need to be coordinated with system vendors and integrators.
Poor remote access controls	There are many reasons why an ICS may need to be remotely accessed, including vendors and system integrators performing system maintenance functions, and also ICS engineers accessing geographically remote system components. Remote access capabilities must be adequately controlled to prevent unauthorized individuals from gaining access to the ICS.
Poor configurations are used	Improperly configured systems may leave unnecessary ports and protocols open, these unnecessary functions may contain vulnerabilities that increase the overall risk to the system. Using default configurations often exposes vulnerabilities and exploitable services. All settings should be examined.
Critical configurations are not stored or backed up	Procedures should be available for restoring ICS configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent loss of data. Documented procedures should be developed for maintaining ICS configuration settings.
Data unprotected on portable device	If sensitive data (e.g., passwords, dial-up numbers) is stored in the clear on portable devices such as laptops and mobile devices and these devices are lost or stolen, system security could be compromised. Policy, procedures, and mechanisms are required for protection.
Passwords generation, use, and protection not in accord with policy	There is a large body of experience with using passwords in IT that is applicable to ICS. Password policy and procedure must be followed to be effective. Violations of password policy and procedures can drastically increase ICS vulnerability.
Inadequate access controls applied	Access controls must be matched to the way the organization allocates responsibilities and privilege to its personnel. Poorly specified access controls can result in giving an ICS user too many or too few privileges. The following exemplify each case: • System configured with default access control settings gives an operator administrative privileges • System improperly configured results in an operator being unable to take corrective actions in an emergency situation
Improper data linking	ICS data storage systems may be linked with non-ICS data sources. An example of this is database links, which allow data from one database to be automatically replicated to others. Data linkage may create a vulnerability if it is not properly configured and may allow unauthorized data access or manipulation.
Malware protection not installed or up to date	Installation of malicious software, or malware, is a common attack. Malware protection software, such as antivirus software, must be kept current in a very dynamic environment. Outdated malware protection software and definitions leave the system open to new malware threats.

脆弱性	内容
OS やベンダーのソフトウエアパッチは、セキュリティの脆弱性が明らかになってしばらく経つまでは開発されない。	ICS ソフトウエアと基本 ICS の緊密な結びつきがあるため、変更を加えた場合は、時間とコストのかかる徹底的なリグレッション試験を行わなければならない。このような試験とその後のソフトウエア更新版の配布までの経過時間により、脆弱性の穴は大きくなる。
OS やアプリケーションのセキュリティパッチが保守されず、ベンダーは脆弱性を顧みない	旧式 OS やアプリケーションには、新たに見つかった悪用されやすい脆弱性がある。セキュリティパッチの保守要領に関して、書面にした手順を作成すべきである。旧版 OS を使った ICS では、セキュリティパッチサポートはない場合があるため、手順にはその場合の脆弱性緩和緊急時対応計画も含めるべきである。
セキュリティ変更試験の不備	試験を行わずに展開したハードウエア/ファームウエア/ソフトウエア変更は、ICS の正常運用能力を低下させる可能性がある。全ての変更内容のセキュリティ影響試験に関して、書面にした手順を作成すべきである。稼働中のシステムは決して試験に使うべきでない。システム変更試験は、システムベンダーやインテグレータと連携して行う必要がある。
リモートアクセス制御の不備	ICS へのリモートアクセスが必要な理由は様々で、例えばベンダーやシステムインテグレータの遠隔保守、遠方にいる ICS エンジニアによるシステムコンポーネントの利用などがある。リモートアクセス機能はしっかり管理して、ICS への不正アクセスを防止しなければならない。
設定の不備	システム設定に不備があり、不必要にポートやプロトコルを開放したままにしておくと、脆弱性となりシステムの全体的リスクが高まる。デフォルト設定を使用すると、脆弱性や悪用可能なサービスを露出することになる。全ての設定を検証すべきである。
重要な設定の保存やバックアップがなされていない	偶発的又は攻撃による設定変更があった際に、システムの可用性を維持し、データ喪失を防止するため、ICS 設定の回復手順を利用できるようにすべきである。ICS 設定を維持するため、書面にした手順を作成すべきである。
携行デバイスのデータが保護されていない	注意を要するデータ（パスワード、ダイアルアップ番号等）が平文のままラップトップやモバイルデバイス等の携行デバイス上に保管されていて、デバイスを紛失したり盗まれたりした場合、システムセキュリティが危うくなる。保護ポリシー、手順及びメカニズムが必要となる。
パスワードの生成、使用及び保護がポリシーに従っていない	ICS にも適用可能な IT でのパスワード利用経験が蓄積されている。パスワードポリシー及び手順は効果的でなければならない。パスワードポリシー・手順違反は、ICS の脆弱性を著しく高める。
アクセス制御の不備	アクセス制御と組織が職員に責任及び特権を与える方法は、整合していなければならない。アクセス制御がしっかりしていないと、ICS ユーザの特権に過不足が生じる。以下は過不足の例である。 • デフォルトアクセス設定になったシステムは、操作員に管理者特権を与える。 • システム設定に不備があると、操作員が緊急時に対策を講じることができない。
データリンキングの不備	ICS データストレージシステムは、ICS 以外のデータソースにリンクしている場合がある。一例がデータベースリンクで、あるデータベースのデータが自動的に他のデータベースに複製される。データリンクは設定がしっかりしていないと、脆弱性が生じ、無許可のデータアクセスやデータ操作を許すことになる。
マルウエア保護ソフトウエアがインストールされていないか最新でない	悪意あるソフトウエア（マルウエア）のインストールは一般的な攻撃である。アンチウイルス等のマルウエア保護ソフトウエアは、動的環境において常に最新状態に保たれなければならない。古くなったマルウエア保護ソフトウエア及び定義では、システムが新しいマルウエア脅威にさらされる。

Vulnerability	Description
Malware protection implemented without sufficient testing	Malware protection software deployed without sufficient testing could impact normal operation of the ICS and block the system from performing necessary control actions.
Denial of service (DoS)	ICS software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resource or delaying system operations and functions.
Intrusion detection/prevention software not installed	Incidents can result in loss of system availability and integrity; the capture, modification, and deletion of data; and incorrect execution of control commands. IDS/IPS software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected with worms. IDS/IPS software must be tested prior to deployment to determine that it does not compromise normal operation of the ICS.
Logs not maintained	Without proper and accurate logs, it might be impossible to determine what caused a security event to occur.

Table C-5. Physical Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Unauthorized personnel have physical access to equipment	Physical access to ICS equipment should be restricted to only the necessary personnel, taking into account safety requirements, such as emergency shutdown or restarts. Improper access to ICS equipment can lead to any of the following: • Physical theft of data and hardware • Physical damage or destruction of data and hardware • Unauthorized changes to the functional environment (e.g., data connections, unauthorized use of removable media, adding/removing resources) • Disconnection of physical data links • Undetectable interception of data (keystroke and other input logging)
Radio frequency, electromagnetic pulse (EMP), static discharge, brownouts and voltage spikes	The hardware used for control systems is vulnerable to radio frequency and electro-magnetic pulses (EMP), static discharge, brownouts and voltage spikes.. The impact can range from temporary disruption of command and control to permanent damage to circuit boards. Proper shielding, grounding, power conditioning, and/or surge suppression is recommended.
Lack of backup power	Without backup power to critical assets, a general loss of power will shut down the ICS and could create an unsafe situation. Loss of power could also lead to insecure default settings.
Loss of environmental control	Loss of environmental control (e.g., temperatures, humidity) could lead to equipment damage, such as processors overheating. Some processors will shut down to protect themselves; some may continue to operate but in a minimal capacity and may produce intermittent errors, continually reboot, or become permanently incapacitated.
Unsecured physical ports	Unsecured universal serial bus (USB) and PS/2 ports could allow unauthorized connection of thumb drives, keystroke loggers, etc.

脆弱性	内容
マルウエア保護ソフトウエアを十分試験せずに実装している	十分な試験を行わずにマルウエア保護ソフトウエアを展開すると、ICS の正常運用に影響し、システムの必要な制御動作が妨害される。
サービス妨害（DoS）	ICS ソフトウエアは DoS 攻撃に脆弱性があるかもしれず、システムリソースへの許可されたアクセスを妨げたり、システムの動作や機能を遅らせたりすることがある。
侵入検知・防止ソフトウエアがインストールされていない	インシデントはシステムの可用性及び完全性の喪失、データのキャプチャ・改変・削除及び制御コマンドの不適切な実行に結びつくことがある。IDS/IPS ソフトウエアは、DoS 攻撃等多様な攻撃を停止又は妨害し、ワームに感染したものなど、攻撃された内部ホストの識別も行う。IDS/IPS ソフトウエアは展開前に試験を行い、ICS の正常運用に悪影響がないか判定しなければならない。
ログが維持されていない	適正かつ正確なログがなければ、セキュリティ事象の発生理由を判別できない。

表 C-5.物理的脆弱性及び弱点となる状態

脆弱性	内容
無許可の人員が装備品に近づいている	ICS 装備品への接近は、緊急停止や再始動といった安全要件を考慮に入れて、必要な職員だけに制限すべきである。ICS 装備品に不用意に接近を許すと、次のような結果が生じかねない。 • データ及びハードウエアの盗難 • データ及びハードウエアの損傷や破損 • 許可されていない機能環境の変更（データ接続、取り外し可能メディアの無断使用、リソースの追加・削除） • データリンクの物理的切断 • 検知不能のデータ傍受（キーストロークその他入力記録）
無線周波数・電磁波（EMP）、静電気、電圧低下・電圧ノイズ	制御システムに利用するハードウエアは、無線周波数・電磁波（EMP）、静電気、電圧低下・電圧ノイズに弱い。影響は、一時的なコマンドの中断から回路基板の恒久的損傷まで多岐にわたる。適切なシールド、アース、電圧管理又はサージ電圧抑制が推奨される。
バックアップ電源の欠如	回路へのバックアップ電源がないと、電源の喪失時、ICS が切断されて不安全な状況になりかねない。またセキュアでないデフォルト設定に戻ることがある。
環境制御の喪失	環境制御（温度、湿度等）の喪失は、プロセッサのオーバーヒートなど装備品の損傷につながる。プロセッサによっては自己防護のため切断するものもある。そのまま続行するものもあるが、機能は最小限で、間欠的にエラーとなり、リブートを繰り返し、恒久的に故障することもある。
セキュアでない物理ポート	セキュアでない USB 及び PS/2 ポートは、サムドライブ、キーストロークロガー等の無断接続を許すことになる。

Table C-6. Software Development Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Improper Data Validation	ICS software may not properly validate user inputs or received data to ensure validity. Invalid data may result in numerous vulnerabilities including buffer overflows, command injections, cross-site scripting, and path traversals.
Installed security capabilities not enabled by default	Security capabilities that were installed with the product are useless if they are not enabled or at least identified as being disabled.
Inadequate authentication, privileges, and access control in software	Unauthorized access to configuration and programming software could provide the ability to corrupt a device.

Table C-7. Communication and Network Configuration Vulnerabilities and Predisposing Conditions

Vulnerability	Description
Data flow controls not employed	Data flow controls, based on data characteristics, are needed to restrict which information is permitted between systems. These controls can prevent exfiltration of information and illegal operations.
Firewalls nonexistent or improperly configured	A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks, allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping, and providing individuals with unauthorized access to systems.
Inadequate firewall and router logs	Without proper and accurate logs, it might be impossible to determine what caused a security incident to occur.
Standard, well-documented communication protocols are used in plain text	Adversaries that can monitor the ICS network activity can use a protocol analyzer or other utilities to decode the data transferred by protocols such as telnet, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and Network File System (NFS). The use of such protocols also makes it easier for adversaries to perform attacks against the ICS and manipulate ICS network activity.
Authentication of users, data or devices is substandard or nonexistent	Many ICS protocols have no authentication at any level. Without authentication, there is the potential to replay, modify, or spoof data or to spoof devices such as sensors and user identities.
Use of unsecure industry-wide ICS protocols	ICS protocols often have few or no security capabilities, such as authentication and encryption, to protect data from unauthorized access or tampering. Additionally, incorrect implementation of the protocols can lead to additional vulnerabilities.
Lack of integrity checking for communications	There are no integrity checks built into most industrial control protocols; adversaries could manipulate communications undetected. To ensure integrity, the ICS can use lower-layer protocols (e.g., IPsec) that offer data integrity protection.
Inadequate authentication between wireless clients and access points	Strong mutual authentication between wireless clients and access points is needed to ensure that clients do not connect to a rogue access point deployed by an adversary, and also to ensure that adversaries do not connect to any of the ICS's wireless networks.
Inadequate data protection between wireless clients and access points	Sensitive data between wireless clients and access points should be protected using strong encryption to ensure that adversaries cannot gain unauthorized access to the unencrypted data.

表 C-6.ソフトウエア開発上の脆弱性及び弱点となる状態

脆弱性	内容
データ検証の不備	ICS ソフトウエアは、ユーザ入力や受信データの妥当性検証を正しく行っていないことがある。無効なデータはバッファオーバーフロー、コマンドインジェクション、クロスサイトスクリプティング、パストラバーサル等、種々の脆弱性につながる。
インストールした接続ソフトウエアがデフォルトで機能しない	製品のインストールによるセキュリティ機能は、無効状態を解除して有効にしないと、または少なくとも、無効状態であることが分からないと効果がない。
ソフトウエアの認証・特権・アクセス制御の不備	設定及びプログラミングソフトウエアへの不正アクセスは、デバイスの破壊を許すことになる。

表 C-7.通信及びネットワーク構成上の脆弱性及び弱点となる状態

脆弱性	内容
データフローが制御されていない	データ特性に基づくデータフロー制御は、システム間の情報交換を制御するものであり、制限を加える必要がある。制御により情報の引出しや不法操作を防止できる。
ファイアウォールの欠如又は設定不備	ファイアウォールが正しく設定されていないと、制御ネットワークと企業ネットワーク等のネットワーク間で、データを不必要に通過させ、攻撃及びマルウエアがネットワーク間で拡散し、要注意データが監視・傍受にさらされ、システムへの不正アクセスを許すことになる。
ファイアウォール及びルータのログの不備	適正かつ正確なログがなければ、セキュリティインシデントの発生理由を判別できない。
標準の文書化された通信プロトコルが平文で使用されている	ICS のネットワーク活動を監視する攻撃側は、プロトコルアナライザその他のユーティリティを利用して、テルネット、FTP、HTTP、NFS 等のプロトコルが転送するデータをデコードする。このようなプロトコルを使用すると、攻撃側は、ICS への攻撃や ICS ネットワーク活動の操作を容易にできるようになる。
ユーザ、データ又はデバイス認証の欠如又は不適格	ICS プロトコルの多くは、どのレベルでも認証機能がない。認証がないとデータのリプレー、改変、なりすましや、センサ及びユーザ ID 等のデバイスのなりすましが生じ得る。
業界で多用されるセキュアでない ICS の使用	ICS プロトコルには、認証や暗号化といった、不正アクセスや改竄を防止するセキュリティ機能がほとんど又は全くないものが多い。またプロトコル実装の不備によっても付加的な脆弱性が生じる。
通信完全性確認の欠如	産業用制御プロトコルのほとんどは完全性チェック機能がなく、攻撃側は検知されずに通信を操作できる。完全性を確保するには、データ完全性保護のある下層プロトコル（IPsec 等）を使用することである。
ワイヤレスクライアントとアクセスポイント間の認証の不備	攻撃側が展開したローグアクセスポイントにクライアントが接続しないようにし、攻撃側が ICS ワイヤレスネットワークに接続できないようにするには、ワイヤレスクライアントとアクセスポイント間に強固な相互認証が必要となる。
ワイヤレスクライアントとアクセスポイント間のデータ保護の不備	ワイヤレスクライアントとアクセスポイント間の要注意データは、強固な暗号化により、攻撃側が暗号化されていないデータに不正アクセスできないようにすべきである。

Incidents

A threat event is an event or situations that could potentially cause an undesirable consequence or impact to the ICS resulting from some threat source. In NIST SP 800-30 Rev. 1, Appendix E identifies a broad set of threat events that could potentially impact information systems [79]. The properties of an ICS may also present unique threat events, specifically addressing how the threat events can manipulates the process of the ICS to cause physical damage. Table C-8 provides an overview of potential ICS threat events.

Table C-8. Example Adversarial Incidents

Threat Event	Description
Denial of Control Action	Control systems operation disrupted by delaying or blocking the flow of information, thereby denying availability of the networks to control system operators or causing information transfer bottlenecks or denial of service by IT-resident services (such as DNS)
Control Devices Reprogrammed	Unauthorized changes made to programmed instructions in PLCs, RTUs, DCS, or SCADA controllers, alarm thresholds changed, or unauthorized commands issued to control equipment, which could potentially result in damage to equipment (if tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), causing an environmental incident, or even disabling control equipment
Spoofed System Status Information	False information sent to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators
Control Logic Manipulation	Control system software or configuration settings modified, producing unpredictable results
Safety Systems Modified	Safety systems operation are manipulated such that they either (1) do not operate when needed or (2) perform incorrect control actions that damage the ICS
Malware on Control Systems	Malicious software (e.g., virus, worm, Trojan horse) introduced into the system.

In addition, in control systems that cover a wide geographic area, the remote sites are often not staffed and may not be physically monitored. If such remote systems are physically breached, the adversaries could establish a connection back to the control network.

Sources of Incidents

An accurate accounting of cyber incidents on control systems is difficult to determine. However, individuals in the industry who have been focusing on this issue see similar growth trends between vulnerabilities exposed in traditional IT systems and those being found in control systems. ICS-CERT is a DHS organization that focuses on reducing the risk across critical infrastructure by identifying threats and vulnerabilities, while also providing mitigation strategies. ICS-CERT provides a trusted party where system owners and operators can report information about incidents within their ICS and obtain advice on mitigating their risk. Information submitted by infrastructure owners and operators is protected under the Critical Infrastructure Information Act of 2002 as Protected Critical Infrastructure Information (PCII) from disclosure under the Freedom of Information Act (FOIA), disclosure under state, tribal, and local disclosure laws, use in regulatory actions, and use in civil litigation. In the event of an incident at critical infrastructure facilities, ICS-CERT can also perform onsite deployments to respond to and analyze incidents. ICS-CERT publishes advisories of new security vulnerabilities discovered in common ICS platforms. Figure C-1 demonstrates (1) the number of ICS incidents reported, (2) the number of onsite ICS deployments taken by ICS-CERT, and (3) number of ICS vulnerabilities reported between years 2010 and 2013[47].

[47] https://ics-cert.us-cert.gov/

インシデント

脅威事象とは、なんらかの脅威源に起因して、ICS に望ましくない結果や影響を与えかねない事象又は状況をいう。NIST SP 800-30 第 1 版付録 E には、情報システムに影響を及ぼす多種多様な脅威事象が明らかにされている[79]。ICS の特性も固有の脅威事象となることがあり、物理的損傷を与えるため、脅威事象がどのように ICS のプロセスを操作するかが取り上げられている。表 C-8 に ICS 脅威事象の概要を示す。

表 C-8. 攻撃インシデントの例

脅威事象	内容
制御妨害	情報の流れの遅延又は妨害により制御システムの運用が中断すると、制御システム操作員がネットワークを使用できなくなり、情報転送がボトルネックとなったり、IT 抵抗性のあるサービス（DNS 等）によるサービスの妨害が生じたりする。
制御デバイスのプログラムが変更されている	PLC、RTU、DCS 若しくは SCADA コントローラのプログラム化命令に対する許可されていない変更、アラーム閾の変更又は制御装備品に対する許可されていないコマンド発行は、装備品の損傷（トレランスを超えた場合）やプロセスの過早切断（通信線等）をもたらし、環境インシデントとなるほか、制御製品を無効にする。
システム状態情報のなりすまし	許可されていない変更を隠蔽するか、不適正行為をシステム操作員に開始させるため、偽情報が制御システム操作員に送信される。
制御ロジックの操作	制御システムソフトウエア又は構成設定が変更され、予想不能の結果が生じる。
安全システムの変更	安全システムの動作が操作され、（1）必要なときに稼働しないか、(2)ICS を損傷する不正確な制御を行う。
制御システムにマルウエア	悪意あるソフトウエア（ウイルス、ワーム、トロイの木馬等）がシステムに入り込んでいる。

また区域を網羅する制御システムで、遠隔サイトに職員が配置されておらず、物理的監視ができていない。このような遠隔システムが物理的に侵害されると、攻撃側は制御ネットワークまで接続を確立できる。

インシデントの原因

制御システム上のサイバーインシデントの原因を正確に判別するのは難しい。とは言え、業界でこの問題と取り組んできた人もおり、従来の IT システムで露呈された脆弱性と制御システムで明らかになってきた脆弱性には、共通的なトレンドがあることに気づいている。ICS-CERT は DHS の組織で、脅威や脆弱性を明らかにして重要インフラのリスクを軽減し、緩和策を提供している。ICS-CERT は、システムの保有者や操作員が ICS 内のインシデント情報をレポートし、リスク緩和策に関する助言を得ることができる、信頼の置ける関係者に提供している。インフラ保有者及び操作員から提出された情報は、重要インフラ情報法（2002 年）に従い、情報の自由法（FOIA）に基づく開示、州・部族・地方開示法に基づく開示、規制行為における使用及び民事訴訟における使用に基づき、保護された重要インフラ情報（PCII）として保護を受ける。重要インフラにおけるイベントの際には、ICS-CERT は現場展開して、インシデントの対応と分析に当たる。ICS-CERT は、ICS プラットホームで共通して見つかった接続上の脆弱性について、アドバイサリーを発刊している。図 C-1 に、(1) ICS インシデントの届出件数、(2) ICS-CERT の ICS 現場展開件数、(3) 2010 年～2013 年 ICS 脆弱性届出件数を示す [48]。

[48] https://ics-cert.us-cert.gov/

Other sources of control system impact information show an increase in control system incidents as well. This information should not be assumed to contain all ICS related incidents or discovered vulnerabilities as some information may go unreported.

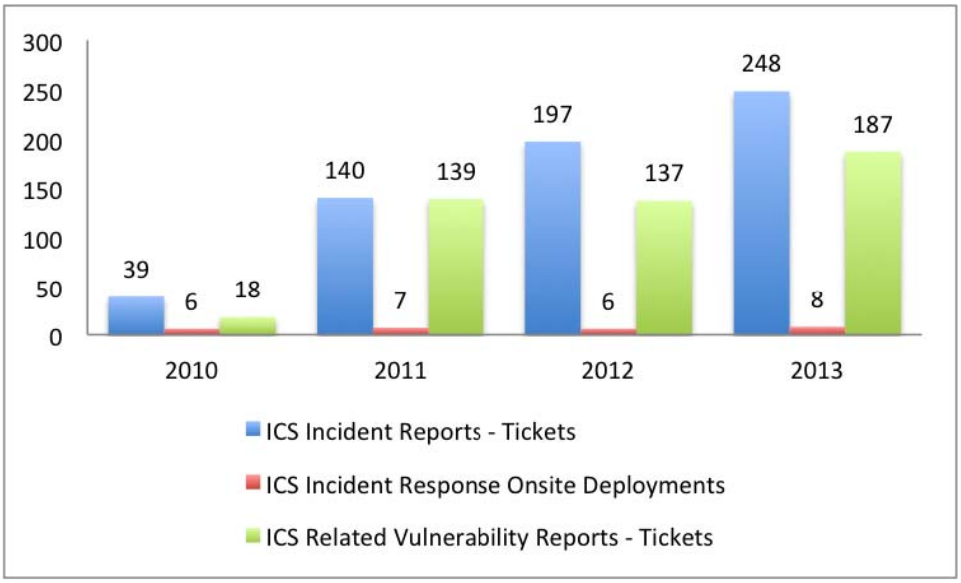

Figure C-1. ICS-CERT Reported Incidents by Year

Documented Incidents

Numerous ICS incidents have been reported that demonstrate how threat sources can negatively impact an ICS. These events help demonstrate the severity of the threat sources, vulnerabilities, and impacts within the ICS domain. As mentioned in Section C.2, the four broad categories of threat sources are adversarial, accidental, structural, and environmental. Often the incident can be the result of multiple threat sources (e.g. an environmental event causes a system failure, which is responded to incorrectly by an operator resulting in an accidental event). Reported incidents from these categories include the following:

Adversarial Events

- **Worcester Air Traffic Communications[49].** In March 1997, a teenager in Worcester, Massachusetts disabled part of the public switched telephone network using a dial-up modem connected to the system. This knocked out phone service at the control tower, airport security, the airport fire department, the weather service, and carriers that use the airport. Also, the tower's main radio transmitter and another transmitter that activates runway lights were shut down, as well as a printer that controllers use to monitor flight progress. The attack also knocked out phone service to 600 homes and businesses in the nearby town of Rutland.

[49] Additional information on the Worcester Air Traffic Communications incident can be found at: http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html

制御システムに影響する情報の他の原因も、制御システムインシデントの増加を示している。未報告の情報もあるため、この情報が ICS 関連インシデント又は解明された脆弱性の全てであると解すべきでない。

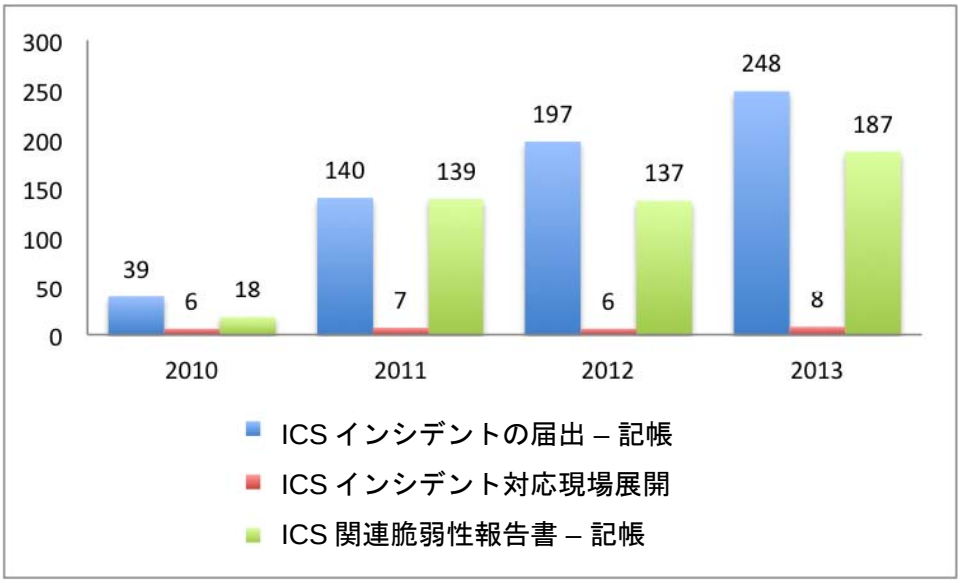

図 C-1. ICS-CERT に届出のあった年度別インシデント件数

文書化されたインシデント

これまで多数の ICS インシデントの届出があり、脅威源が ICS にどのような悪影響を与え得るかを実証している。これらの事象は、脅威源、脆弱性及び ICS ドメイン内での影響の重大性を実証するのに役立つ。セクション C.2 で言及したように、脅威源は敵性、偶発性、構造的及び環境的の 4 つの分類に大別できる。インシデントは複数の脅威源に起因することが少なくない（環境的事象がシステム障害の原因となり、それに対するオペレータの対応がまずいと偶発的事象となる）。届出のあったインシデントには、分類別に次のようなものがある。

敵性事象

- **ウースター航空交通通信** [50]1997 年 3 月、マサチューセッツ州ウースターのティーンエイジャーがダイアルアップモデムでシステムに接続し、公共交換電話網の一部を使用不能にした。このため管制塔、空港警備、空港消防隊、気象サービス及び空港を利用する航空会社に対する電話サービスが麻痺した。また管制塔の主無線送信機や滑走路灯を点灯する送信機が遮断されたほか、飛行の進捗を監視する管制官のプリンタが使えなくなった。この攻撃でラトランド町近傍の一般家庭 600 世帯と企業の電話も使用不能になった。

[50] ウースター航空交通通信インシデントの詳細は次のサイトにある。
http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html

- **Maroochy Shire Sewage Spill**[51]**.** In the spring of 2000, a former employee of an Australian organization that develops manufacturing software applied for a job with the local government, but was rejected. Over a two-month period, the disgruntled rejected employee reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewerage pumping stations and caused malfunctions in their operations, ultimately releasing about 264 000 gallons of raw sewage into nearby rivers and parks.
- **Davis-Besse**[52]**.** In August 2003, the Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours. In addition, the plant's process computer failed, and it took about six hours for it to become available again. Slammer reportedly also affected communications on the control networks of at least five other utilities by propagating so quickly that control system traffic was blocked.
- **Zotob Worm**[53]**.** In August 2005, a round of Internet worm infections knocked 13 of DaimlerChrysler's U.S. automobile manufacturing plants offline for almost an hour, stranding workers as infected Microsoft Windows systems were patched. Plants in Illinois, Indiana, Wisconsin, Ohio, Delaware, and Michigan were knocked offline. While the worm affected primarily Windows 2000 systems, it also affected some early versions of Windows XP. Symptoms include the repeated shutdown and rebooting of a computer. Zotob and its variations caused computer outages at heavy-equipment maker Caterpillar Inc., aircraft-maker Boeing, and several large U.S. news organizations.
- **Stuxnet Worm**[54]**.** Stuxnet was a Microsoft Windows computer worm discovered in July 2010 that specifically targeted industrial software and equipment. The worm initially spread indiscriminately, but included a highly specialized malware payload that was designed to target only specific SCADA systems that were configured to control and monitor specific industrial processes
- **Brute Force Attacks on Internet-Facing Control Systems**[55]. On February 22, 2013 ICS-CERT received a report from a gas compressor station owner about an increase in brute force attempts to access their process control network. The forensic evidence contained 10 separate IPs and additional calls of a similar nature from additional natural gas pipeline asset owners, which yielded 39 additional IPs of concern. Log analysis showed a date range from January 16, 2013 but there have been no reports since March 8, 2013.
- **Shamoon**[56]. Saudi Aramco, which is the world's 8th largest oil refiner, experienced a malware attack that targeted their refineries and overwrote the attacked system's Master Boot Records (MBR), partition tables and other random data files. This caused the systems to become unusable.

---

51 Additional information on the Maroochy Shire Sewage Spill incident can be found at: http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf and http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/ [each accessed 4/16/15].

52 Additional information on the Davis-Besse incident can be found at: http://www.securityfocus.com/news/6767 [accessed 4/16/15].

53 Additional information on the Zotob Worm incident can be found at: http://www.eweek.com/c/a/Security/Zotob-PnP-Worms-Slam-13-DaimlerChrysler-Plants [accessed 4/16/15].

54 Additional information on the Stuxnet worm can be found at: http://en.wikipedia.org/wiki/Stuxnet [accessed 4/16/15].

55 Additional information on ICS-CERT reported incidents can be found at: https://ics-cert.us-cert.gov/Information-Products [accessed 4/16/15].

56 Additional information on Shamoon can be found at: http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2012.pdf [accessed 4/16/15].

- **マルーチー市の下水流出**[57]　2000 年春、豪州の元ソフトウエア開発会社社員が地方自治体職員の募集に応募したが不採用になった。不満を抱いた当人は、2 か月間にわたり 46 回、無線送信機で下水処理装置に侵入した。ある下水ポンプステーションの電子データを改変して、運転障害を発生させ、結局 26 万 4,000 ガロンもの下水を近隣の河川や公園に放出させた。
- **デイビス・ベス**[58]　2003 年 8 月、原子力規制委員会は同年 1 月、スラマーとして知られるマイクロソフト SQL サーバのワームが、オハイオ州オークハーバーにある非稼働中のデイビス・ベス原子力発電所のプライベートコンピュータネットワークに感染していることを確認し、5 時間程度安全監視装置が使用できなかった。また、発電所のプロセスコンピュータが故障し、復旧に約 6 時間要した。報告によればスラマーは、少なくとも他の 5 つの公共事業団体の制御ネットワークの通信にも影響を及ぼし、極めて迅速に伝播して制御システムトラフィックを遮断した。
- **Zotob ワーム**[59]　2005 年 8 月、インターネットワームに感染したダイムラークライスラーの米国自動車生産プラント 13 箇所が約 1 時間にわたりオフラインになり、Windows システムへのパッチ作業の間、作業員が立ち往生した。イリノイ、インディアナ、ウィスコンシン、オハイオ、デラウェア、ミシガンの各州ではプラントがオフラインになった。感染したのは主に Windows2000 だったが、Windows XP の初期バージョンも感染した。感染の徴候は、切断と再起動の繰り返しだった。Zotob 及びその派生型は、大型装備品メーカーの Caterpillar Inc.、航空機メーカーの Boeing、その他大手の報道機関のコンピュータが被害に遭った。
- **Stuxnet ワーム**[60]　Stuxnet は 2010 年 7 月に見つかった Windows コンピュータのワームで、産業用ソフトウエア及び装備品を主な標的としている。当初このワームは対象を選ばず拡散したが、特殊なマルウエアペイロードを組み込んで、特定の産業プロセスの制御・監視に特化した SCADA システムだけを標的とするようになった。
- **インターネットに対面する制御システムへの強力攻撃**[61]　2013 年 2 月 22 日、ICS-CERT はガスコンプレッサステーションの保有者から、制御管理ネットワークへのアクセスをもくろむ強大な力の増加がある旨報告を受けた。調査の結果、別個の IP が 10 と、同種の補足的な呼出しがほかの天然ガスパイプライン保有者からもあり、全部で 39 の追加 IP 事案となった。ログ解析の結果、2013 年 1 月 16 日から始まっていたが、同年 3 月 8 日以降の届出はなかった。
- **シャムーン**[62]　世界第 8 位の製油会社 Saudi Aramco は、同社の製油施設を標的としたマルウエア攻撃に遭い、システムのマスターブートレコード（MBR）、パーティションテーブルその他ランダムデータファイルが書き換えられた。システムは使用不能になった。

57　マルーチー市の下水流出インシデントの詳細は次のサイトにある。http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf and http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/ [each accessed 4/16/15].

58　デイビス・ベスインシデントの詳細は次のサイトにある。http://www.securityfocus.com/news/6767 [accessed 4/16/15].

59　Zotob ワームインシデントの詳細は次のサイトにある。http://www.eweek.com/c/a/Security/Zotob-PnP-Worms-Slam-13-DaimlerChrysler-Plants [accessed 4/16/15].

60　Stuxnet ワームインシデントの詳細は次のサイトにある。http://en.wikipedia.org/wiki/Stuxnet [accessed 4/16/15].

61　ICS-CERT 届出インシデントの詳細は次のサイトにある。https://ics-cert.us-cert.gov/Information-Products [accessed 4/16/15].

62　シャムーンの詳細は次のサイトにある。http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2012.pdf [accessed 4/16/15].

- **German Steel Mill Attack[63].** In 2014, hackers manipulated and disrupted control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive"—though unspecified—damage.

Structural Events

- **CSX Train Signaling System[64].** In August 2003, the Sobig computer virus was blamed for shutting down train signaling systems throughout the east coast of the U.S. The virus infected the computer system at CSX Corp.'s Jacksonville, Florida headquarters, shutting down signaling, dispatching, and other systems. According to Amtrak spokesman Dan Stessel, ten Amtrak trains were affected in the morning. Trains between Pittsburgh and Florence, South Carolina were halted because of dark signals, and one regional Amtrak train from Richmond, Virginia to Washington and New York was delayed for more than two hours. Long-distance trains were also delayed between four and six hours.
- **Northeast Power Blackout[65].** In August 2003, failure of the alarm processor in First Energy's SCADA system prevented control room operators from having adequate *situational awareness* of critical operational changes to the electrical grid. Additionally, effective reliability oversight was prevented when the state estimator at the Midwest Independent System Operator failed due to incomplete information on topology changes, preventing contingency analysis. Several key 345 kV transmission lines in Northern Ohio tripped due to contact with trees. This eventually initiated cascading overloads of additional 345 kV and 138 kV lines, leading to an uncontrolled cascading failure of the grid. A total of 61 800 MW load was lost as 508 generating units at 265 power plants tripped.
- **Taum Sauk Water Storage Dam Failure[66]**. In December 2005, the Taum Sauk Water Storage Dam suffered a catastrophic failure releasing a billion gallons of water. The failure of the reservoir occurred as the reservoir was being filled to capacity or may have possibly been overtopped. The current working theory is that the reservoir's berm was overtopped when the routine nightly pump-back operation failed to cease when the reservoir was filled. According to the utility, the gauges at the dam read differently than the gauges at the Osage plant at the Lake of the Ozarks, which monitors and operates the Taum Sauk plant remotely. The stations are linked together using a network of microwave towers, and there are no operators on-site at Taum Sauk.
- **Bellingham, Washington Gasoline Pipeline Failure[67].** In June 1999, 900 000 liters (237 000 gallons) of gasoline leaked from a 16 in. (40.64 cm) pipeline and ignited 1.5 hours later causing 3 deaths, 8 injuries, and extensive property damage. The pipeline failure was exacerbated by control systems not able to perform control and monitoring functions. "Immediately prior to and during the incident, the SCADA system exhibited poor performance that inhibited the pipeline controllers from seeing and reacting to the development of an abnormal pipeline operation." A key recommendation

---

63 Additional information on the German steel mill incident can be found at: http://www.wired.com/2015/01/german-steel-mill-hack-destruction/ [accessed 4/16/15].

64 Additional information on the CSX Train Signaling System incident can be found at: http://www.cbsnews.com/stories/2003/08/21/tech/main569418.shtml and http://www.informationweek.com/story/showArticle.jhtml?articleID=13100807 [each accessed 4/16/15].

65 Additional information on the Northeast Power Blackout incident can be found at: http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinalImplementationReport%282%29.pdf [accessed 4/16/15]. http://www.oe.energy.gov/DocumentsandMedia/BlackoutFinal-Web.pdf

66 Additional information on the Taum Sauk Water Storage Dam Failure incident can be found at: http://www.ferc.gov/industries/hydropower/safety/projects/taum-sauk/ipoc-rpt/full-rpt.pdf [accessed 4/16/15].

67 Additional information on the Bellingham, Washington Gasoline Pipeline Failure incident can be found at http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report%2020Sep071.pdf and http://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf [each accessed 4/16/15].

■ **ドイツ鉄工所攻撃** [68]　2014 年にハッカーは制御システムを操作して中断し、高炉が正常に遮断できなくなり、特定不能の「大規模」損害に至った。

構造的事象

■ **CSX 列車信号システム** [69]　2003 年 8 月、Sobig コンピュータウイルスが原因と言わる列車信号システムの遮断が米国東海岸一帯を襲った。ウイルスは CSX Corp.のフロリダ（ジャクソンビル）本部コンピュータシステムに感染し、信号、ディスパッチその他のシステムを遮断した。Amtrak のスポークスマン Dan Stessel によれば、その朝列車 10 両に影響が出た。サウスカロライナ州ピッツバーグとフローレンス間で、暗信号のため列車が立ち往生し、リッチモンド、バージニア、ワシントン、ニューヨーク間でも 2 時間以上にわたりダイヤに遅れが生じた。長距離列車にも 4～6 時間の遅れが出た。

■ **北東部の停電** [70]　2003 年 8 月、First Energy の SCADA システムのアラームプロセッサが故障し、配電網の重大な運用変更があったことに、制御室操作員が気づかなかった。また、Midwest Independent System Operator の査定官が、トポロジー変更に関する情報の不備から職務を遂行できず、不測事態分析が不能で、信頼性に対する効果的な監督業務が阻害された。オハイオ州北部の主要な 345kV 送電線が、樹木と接触したために遮断された。このため連鎖的な過負荷が別の 345kV 及び 138kV にかかり、送電網の制御不能な連鎖障害に至った。結局 265 の発電所の発電装置 508 基が遮断され、合計 61,800MW が失われた。

■ **Taum Sauk 貯水ダムの障害** [71]　2005 年 12 月、**Taum Sauk** 貯水ダムが壊滅的な被害に遭い、数十億ガロンの水が放出された。障害は、貯水池が満水あるいはそれを越えたために生じた。現在の作業理論では、貯水池の満水時に、毎夜行われるポンプバック操作が停止せず、貯水池の頂部から溢れ出たとされている。事業者によれば、ダムのゲージと、Taum Sauk 発電所を遠隔監視・運用する Ozarks 湖にある Osage 発電所のゲージの値表示が違っていた。各ステーションは、マイクロ波タワーのネットワークを利用して結ばれており、Taum Sauk には現場操作員がいない。

■ **ワシントン州ベリンガムのガソリンパイプライン障害** [72]　1999 年 6 月、ガソリン 90 万リットル（23 万 7,000 ガロン）が 16 インチ（40.64cm）のパイプラインから漏れ、1 時間半後に発火し、死者 3 人、負傷者 8 人のほか甚大な物損が生じた。制御システムの制御・監視機能が働かず、パイプライン障害が悪化した。「インシデントの直前及び最中に、SCADA システムのパフォーマンスが劣り、パイプライン操作員は、異常なパイプライン動作に対して、確認も対処もできなかった。

68　ドイツの鉄工所インシデントの詳細は次のサイトにある。http://www.wired.com/2015/01/german-steel-mill-hack-destruction/ [accessed 4/16/15].

69　CSX 列車信号システムインシデントの詳細は次のサイトにある。http://www.cbsnews.com/stories/2003/08/21/tech/main569418.shtml and http://www.informationweek.com/story/showArticle.jhtml?articleID=13100807 [each accessed 4/16/15].

70　北東部の停電インシデントの詳細は次のサイトにある。http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinalImplementationReport%282%29.pdf [accessed 4/16/15]. http://www.oe.energy.gov/DocumentsandMedia/BlackoutFinal-Web.pdf

71　Taum Sauk 貯水ダム障害インシデントの詳細は次のサイトにある。http://www.ferc.gov/industries/hydropower/safety/projects/taum-sauk/ipoc-rpt/full-rpt.pdf [accessed 4/16/15].

72　ワシントン州ベリンガムのガソリンパイプライン障害インシデントの詳細は次のサイトにある。http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report%2020Sep071.pdf and http://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf [each accessed 4/16/15].

from the NTSB report issued October 2002 was to utilize an off-line development and testing system for implementing and testing changes to the SCADA database.

- **Browns Ferry-3 PLC Failure**[73]. In August 2006, TVA was forced to manually shut down one of their plant's two reactors after unresponsive PLCs problems caused two water pumps to fail and threatened the stability of the plant itself. Although there were dual redundant PLCs, they were connected to the same Ethernet network. Later testing on the failed devices discovered that they would crash when they encountered excessive network traffic.

Environmental Events

- **Fukushima Daiichi Nuclear Disaster**[74]. The Great East Japan Earthquake on 11 March 2011 struck off the coast of Japan, sending a massive tsunami inland towards the nuclear plant. The tsunami compromised the plants seawall, flooding much of the plant including the location housing the emergency generators. This emergency power was critical to operate the control rooms and also to provide coolant water for the reactors. The loss of coolant caused the reactor cores to overheat to the point where the fuel's zirconium cladding reacted with water, releasing hydrogen gas and fueling large explosions in three of the four reactor buildings. This resulted in large-scale radiation leakage that has impacted plant employees, nearby citizens, and the local environment. Post event analysis found that the plant's emergency response center had insufficient secure communication lines to provide other areas of the plant with information on key safety related instrumentation.

Accidental Events

- **Vulnerability Scanner Incidents**[75]**.** While a ping sweep was being performed on an active SCADA network that controlled 3 meter (9 foot) robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated. In a separate incident, a ping sweep was being performed on an ICS network to identify all hosts that were attached to the network, for inventory purposes, and it caused a system controlling the creation of integrated circuits in the fabrication plant to hang. This test resulted in the destruction of $50,000 worth of wafers.
- **Penetration Testing Incident**[76]**.** A natural gas utility hired an IT security consulting organization to conduct penetration testing on its corporate IT network. The consulting organization carelessly ventured into a part of the network that was directly connected to the SCADA system. The penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours. The outcome was the loss of service to its customer base for those four hours.

---

73 Additional information on the Browns Ferry -3 PLC Failure incident can be found at: http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf [accessed 4/16/15].

74 Additional information can be found at: http://www-pub.iaea.org/MTCD/meetings/PDFplus/2011/cn200/documentation/cn200_Final-Fukushima-Mission_Report.pdf and http://pbadupws.nrc.gov/docs/ML1414/ML14140A185.pdf [each accessed 4/16/15].

75 Additional information on the vulnerability scanner incidents can be found at: http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2005_2846p.pdfhttp://www.sandia.gov/scada/documents/sand_2005_2846p.pdf [accessed 4/16/15].

76 Additional information on penetration testing incidents can be found at: http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2005_2846p.pdf [accessed 4/16/15].

2002 年 10 月発行の NTSB 報告書の主な推奨事項は、SCADA データベースへの変更の実装及び試験は、オフライン開発試験システムを使用することになっている。

- **Browns Ferry-3 台の PLC 障害**[77]　2006 年 8 月、PLC が反応しなくなり 2 基の水ポンプが止まり、発電所自体の安定性維持が危うくなったため、2 基の原子炉のうちの 1 基を手動で停止した。2 重冗長性の PLC だったが、いずれも同じ Ethernet ネットワークに接続されていた。故障したデバイスを後日試験した結果、ネットワークトラフィックが過大になり、クラッシュしていたことが分かった。

環境的事象

- **福島第 1 原子炉災害**[78]　2011 年 3 月 11 日、東日本大地震が日本の沖合で発生し、大型の津波が発電所を襲った。津波は発電所の防波堤を突破し、緊急用発電機を収容した場所も含め、発電所の大部分が浸水した。この緊急用電力は、制御室の運用と原子炉用冷却水の給水に不可欠だった。冷却水が失われたため炉心が過熱し、燃料のジルコニウム被覆が水と反応して水素を放出し、4 棟ある建屋の 3 棟で爆発が生じた。このため大規模の放射能漏れが生じ、発電所従業員、近隣住人及び地元環境に影響が及んだ。事後解析の結果、重要な安全関連計装情報を発電所の他のエリアに伝えるための緊急時対応センターの通信線に不備があった。

偶発的事象

- **脆弱性スキャナーインシデント**[79]　3m（9 フィート）のロボットアームを制御するアクティブ SCADA システムネットワークで、ピンスイープを行っていたところ、1 本のアームがアクティブになりほぼ 180° 振れた。ピンスイープの開始前、アーム操作員はスタンバイモードだった。別のインシデントでは、ICS ネットワークでピンスイープを行い、在庫管理目的で、ネットワークに接続している全てのホストを識別していたところ、IC の作成を制御している製造プラントのシステムをハングさせた。結果として、5 万ドル分のウェハーが破損した。
- **ペネトレーション・テスト・インシデント**[80]　天然ガス事業体は、自社 IT ネットワークのペネトレーション・テスト実施のため、IT 接続コンサルティング組織を雇用した。コンサルティング組織は、不注意にも SCADA システムに直接つながったネットワークの一部に入った。ペネトレーション・テストのせいで SCADA システムがロックし、同事業体は 4 時間にわたりガスを配送できなかった。結果は 4 時間にわたる顧客へのサービス提供の喪失となった。

---

77 Browns Ferry-3 台の PLC 障害インシデントの詳細は次のサイトにある。http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf [accessed 4/16/15].

78 詳細は次のサイトにある。http://www-pub.iaea.org/MTCD/meetings/PDFplus/2011/cn200/documentation/cn200_Final-Fukushima-Mission_Report.pdf and http://pbadupws.nrc.gov/docs/ML1414/ML14140A185.pdf [each accessed 4/16/15].

79 脆弱性スキャナーインシデントの詳細は次のサイトにある。http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2005_2846p.pdfhttp://www.sandia.gov/scada/documents/sand_2005_2846p.pdf [accessed 4/16/15].

80 ペネトレーション・テスト・インシデントの詳細は次のサイトにある。http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2005_2846p.pdf [accessed 4/16/15].

Appendix D—Current Activities in Industrial Control System Security

This appendix contains abstracts of some of the many activities that are addressing ICS cybersecurity. Please be aware that organization descriptions and related information provided in this appendix has been drawn primarily from the listed organizations' Web sites and from other reliable public sources, but has not been verified. Readers are encouraged to contact the organizations directly for the most up-to-date and complete information.

American Gas Association (AGA) Standard 12, "Cryptographic Protection of SCADA Communications"

American Gas Association: **http://www.aga.org/**

The American Gas Association, representing 195 local energy utility organizations that deliver natural gas to more than 56 million homes, businesses, and industries throughout the United States, advocates the interests of its energy utility members and their customers, and provides information and services. The AGA 12 series of documents recommends practices designed to protect SCADA communications against cyber incidents. The recommended practices focus on ensuring the confidentiality of SCADA communications.

The purpose of the AGA 12 series is to save SCADA system owners' time and effort by recommending a comprehensive system designed specifically to protect SCADA communications using cryptography. The AGA 12 series may be applied to water, wastewater, and electric SCADA-based distribution systems because of their similarities with natural gas systems, however timing requirements may be different. Recommendations included in the series 12 documents may also apply to other ICS. Additional topics planned for future addendums in this series include key management, protection of data at rest, and security policies.

American Petroleum Institute (API) Standard 1164, "Pipeline SCADA Security"

American Petroleum Institute: **http://www.api.org/**

The American Petroleum Institute represents more than 400 members involved in all aspects of the oil and natural gas industry. API 1164 provides guidance to the operators of oil and natural gas pipeline systems for managing SCADA system integrity and security. The guideline is specifically designed to provide operators with a description of industry practices in SCADA security, and to provide the framework needed to develop sound security practices within the operator's individual organizations. It stresses the importance of operators understanding system vulnerability and risks when reviewing the SCADA system for possible system improvements. API 1164 provides a means to improve the security of SCADA pipeline operations by:

- Listing the processes used to identify and analyze the SCADA system's susceptibility to incidents.
- Providing a comprehensive list of practices to harden the core architecture.
- Providing examples of industry recommended practices.

The guideline targets small to medium pipeline operators with limited IT security resources. The guideline is applicable to most SCADA systems, not just oil and natural gas SCADA systems. The appendices of the document include a checklist for assessing a SCADA system and an example of a SCADA control system security plan.

付録 D　産業用制御システムセキュリティにおける現在の活動

この付録では、ICS サイバーセキュリティを対象とした諸活動のいくつかを取りまとめる。記載されている組織と関連情報は、主に記載されている組織のウェブサイトその他信頼できる公開の出所から取ったもので、未検証であることに留意されたい。直接これら組織に問い合わせ、最新情報を入手するように奨励する。

米国ガス協会（AGA）規格 12「SCADA 通信の暗号化保護」

米国ガス協会：**http://www.aga.org/**

195 の地方エネルギー供給事業体を代表する米国ガス協会は、全米の一般家庭 5,600 万世帯、企業及び業界に天然ガスを供給し、事業者と顧客双方の利益を擁護し、情報及びサービスを提供している。AGA12 シリーズは、SCADA システムをサイバーインシデントから守るための規範を推奨している。推奨規範は、SCADA 通信の機密性の確保に重点を置いている。

同シリーズの目的は、暗号を利用して SCADA 通信を保護する包括的システムの推奨により、SCADA システム保有者の時間と労力を節約することにある。同シリーズは、天然ガスシステムとの共通性が多い水道、下水及び SCADA ベースの配電システムに適用できるが、タイミングに関する要件は異なることがある。
推奨事項は他の ICS にも適用できる。補遺として将来計画されているものには、重要管理事項、休眠中のデータ保護、セキュリティポリシー等がある。

米国石油協会（API）規格 1164「パイプライン SCADA セキュリティ」

米国石油協会：**http://www.api.org/**

米国石油協会は、石油及び天然ガス業界のあらゆる面に従事する 400 以上のメンバーを代表している。API1164 は、SCADA システムの完全性及びセキュリティの管理に携わる、石油及び天然ガスパイプラインシステム操作員向けガイダンスとなる。特に SCADA セキュリティの業界規範について説明し、操作員の組織における健全なセキュリティ規範を策定するための基本構成を示している。SCADA システムを精査して改善を図る際に、操作員がシステムの脆弱性とリスクを理解する大切さを強調している。API1164 は、SCADA パイプライン運用のセキュリティを向上させる手段として、以下を挙げている。

- SCADA システムのインシデント感受性を識別・分析するためのプロセスの列挙
- コアアーキテクチャを強固にするための包括的規範リストの作成
- 業界推奨規範の例示

このガイドラインは、IT セキュリティリソースが限られた中小規模のパイプライン事業者を対象としている。石油及び天然ガスのみならず、ほとんどの SCADA システムに適用できる。ガイドラインの付録には、SCADA システム評価のチェックリストや SCADA 制御システムセキュリティ計画書の例もある。

Electric Power Research Institute (EPRI)

http://www.epri.com/Our-Work/Pages/Cyber-Security.aspx,
http://smartgrid.epri.com/NESCOR.aspx

The Electric Power Research Institute (EPRI) is a nonprofit center for public interest energy and environmental research. EPRI brings together member organizations, the Institute's scientists and engineers, and other leading experts to work collaboratively on solutions to the challenges of electric power. These solutions span nearly every area of power generation, delivery, and use, including health, safety, and environment. EPRI's members represent over 90% of the electricity generated in the United States.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) operates within the National Cybersecurity and Integration Center (NCCIC), a division of the Department of Homeland Security's Office of Cybersecurity and Communications (DHS CS&C). NCCIC/ICS-CERT is a key component of the DHS Strategy for Securing Control Systems. The primary goal of the Strategy is to build a long-term common vision where effective risk management of control systems security can be realized through successful coordination efforts. ICS-CERT provides a control system security focus in collaboration with US-CERT to:

- Respond to and analyze control systems related incidents.
- Conduct vulnerability and malware analysis.
- Provide onsite support for incident response and forensic analysis.
- Provide situational awareness in the form of actionable intelligence.
- Coordinate the responsible disclosure of vulnerabilities/mitigations.
- Share and coordinate vulnerability information and threat analysis through information products and alerts.

ICS-CERT coordinates control systems-related security incidents and information sharing with Federal, State, and local agencies and organizations, the intelligence community, and private sector constituents, including vendors, owners and operators, and international and private sector CERTs. The focus on control systems cybersecurity provides a direct path for coordination of activities among all members of the critical infrastructure stakeholder community.

As a functional component of the NCCIC, ICS-CERT provides focused operational capabilities for defense of control system environments against emerging cyber threats.

ICS-CERT provides efficient coordination of control-systems-related security incidents and information sharing with federal, state, and local agencies and organizations, the Intelligence Community, private sector constituents including vendors, owners, and operators, and international and private sector computer security incident response teams (CSIRTs). The focus on control systems cybersecurity provides a direct path for coordination of activities for all members of the stakeholder community.

米国電力研究所（EPRI）

http://www.epri.com/Our-Work/Pages/Cyber-Security.aspx,
http://smartgrid.epri.com/NESCOR.aspx

米国電力研究所（EPRI）は、公益エネルギー環境研究に関する非営利団体である。加盟団体、研究所の科学者・エンジニアその他専門家を束ねて、電力問題の解決に取り組んでいる。解決策は発電、配電、利用などあらゆる分野にまたがり、健康、安全、環境等も含まれる。加盟メンバーは、米国発電量の 90%以上を生産している。

産業用制御システムサイバー緊急対応チーム(ICS-CERT)

https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team

産業用制御システムサイバー緊急対応チーム(ICS-CERT)は、国家サイバーセキュリティ通信統合センター(NCCIC)内で、国土安全保障省のサイバーセキュリティ通信局（DHS CS&C）の下にある。NCCIC/ICS-CERT は、制御サービスのセキュリティを確保する DHS 施策の主要な構成要素である。この施策の主な目的は、長期の共通的ビジョンを打ち立て、相互連携を通じて制御システムセキュリティの効果的リスク管理を実現することにある。ICS-CERT は US-CERT との連携を通じて、以下を重点とする制御システムセキュリティを推進する。

- 制御システム関連インシデントへの対応と分析
- 脆弱性とマルウエアの分析
- 現場でのインシデント対応と調査分析支援
- 実用的な情報提供による意識の高揚
- 脆弱性・緩和策の責任ある開示の調整
- 情報通知・アラートによる脆弱性情報と脅威分析の共有と調整

ICS-CERT は制御システム関連セキュリティインシデントと情報を調整し、国・州・地方自治体・組織・情報共同体・民間企業（ベンダー・保有者・国際民間企業 CERT 等）と共有する。制御システムのサイバーセキュリティに注力することで、全重要インフラ関係者間の活動を直接調整する道筋が開ける。

NCCIC の機能要素として ICS-CERT は、制御システム環境を新興サイバー脅威から守るため、集中的な運用能力を付与する。

ICS-CERT は制御システム関連セキュリティインシデントと情報を調整し、国・州・地方自治体・組織・情報共同体・民間企業（ベンダー・保有者・操作員・国際/民間企業コンピュータセキュリティインシデント対応チーム[CSIRT]等）と共有する。制御システムのサイバーセキュリティに注力することで、全関係者に活動を直接調整する道筋を開く。

ICS-CERT Cyber Security Evaluation Tool (CSET®)

http://ics-cert.us-cert.gov/Assessments

The Cyber Security Evaluation Tool (CSET®) is a DHS product that assists organizations in protecting their key national cyber assets. It was developed under the direction of the DHS ICS-CERT by cybersecurity experts and with assistance from NIST. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.

CSET is a desktop software tool that guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cyber systems. The tool derives the recommendations from a database of cybersecurity standards, guidelines, and practices. Each recommendation is linked to a set of actions that can be applied to enhance cybersecurity controls.

CSET has been designed for easy installation and use on a stand-alone laptop or workstation. It incorporates a variety of available standards from organizations such as NIST, NERC, Transportation Security Administration (TSA), U.S. Department of Defense (DoD), and others. When the tool user selects one or more of the standards, CSET will open a set of questions to be answered. The answers to these questions will be compared against a selected security assurance level, and a detailed report will be generated to show areas for potential improvement. CSET provides an excellent means to perform a self-assessment of the security posture of your control system environment.

ICS-CERT Recommended Practices

https://ics-cert.us-cert.gov/Introduction-Recommended-Practices

ICS-CERT works with the control systems community to ensure that recommended practices, which are made available, have been vetted by subject-matter experts in industry before being made publicly available in support of this program.

Recommended practices are developed to help users reduce their exposure and susceptibility to cyber attacks. These recommendations are based on understanding the cyber threats, control systems vulnerabilities and attack paths, and secure architecture design.

The recommended practices working group selects topics to be implemented in the recommended practices section. Additional supporting documents detailing a wide variety of control systems topics associated with cyber vulnerabilities and their mitigation have been developed and vetted by the working group for accuracy. These documents will be updated and topics added to address additional content and emerging issues.

ICS-CERT サイバーセキュリティ評価ツール(CSET®)

http://ics-cert.us-cert.gov/Assessments

ICS-CERT サイバーセキュリティ評価ツール(CSET®)は、組織が国の重要サイバー資産を守るのを支援する DHS の製品である。DHS ICS-CERT の指導下で、NIST の支援を得てサイバーセキュリティ専門家が開発した。サイバーシステム及びネットワークのセキュリティ状態を評価する際の体系的かつ反復的な取組が可能となる。あらゆる産業用制御及び IT システムに関係した高度の詳細な疑問に答えている。

CSET はデスクトップソフトウエアツールで、制御システム及び情報技術ネットワークセキュリティ規範を、広く認められた業界基準に照らして、段階的に評価することができる。CSET により、組織の企業・産業用制御サイバーシステムのサイバーセキュリティ状態を改善するための優先的推奨事項リストを作成できる。このツールは、サイバーセキュリティ基準、ガイドライン及び規範データベースから推奨事項を導き出す。それぞれの推奨事項は、サイバーセキュリティ管理の拡張に適用可能な一連の行動に結びついている。

CSET は、スタンドアローンラップトップやワークステーションに、簡単にインストールして利用できるようになっている。NIST、NERC、運輸保安局(TSA)、国防総省その他の組織から入手可能な種々の基準が取りまとめてられている。ツールのユーザがこれら基準のいずれかを選択すると、一連の質問が提示される。質問への回答を、選択されたセキュリティ保証レベルと照らし合わせ、改善できる分野を示した詳細なレポートが作成されるようになっている。CSET は、制御システム環境のセキュリティ状態を自己評価できる優れた手段となる。

ICS-CERT 推奨規範

https://ics-cert.us-cert.gov/Introduction-Recommended-Practices

ICS-CERT は制御システムの共同体と連携し、入手可能になった推奨規範を公開する前に、業界の対象専門家に検証を依頼する。

推奨規範は、サイバー攻撃に対する露出や感受性を減らすために作成される。サイバー脅威、制御システムの脆弱性・攻撃経路及びセキュアなアーキテクチャ設計に対する理解を基にしている。

推奨規範作業グループは、推奨規範セクションで取り上げるべき論題を選定する。サイバー脆弱性とその緩和策に関する多様な制御システム論題について詳述した補足文書が作業グループにより作成され、正確性が検証されている。文書は更新され、補足的な内容や新しい問題を取り上げた論題が追加される。

Institute of Electrical and Electronics Engineers, Inc. (IEEE)

http://www.ieee.org

IEEE 1686-2007 – Standard for Substation IED Cybersecurity Capabilities. The functions and features to be provided in substation intelligent electronic devices (lEDs) to accommodate critical infrastructure protection programs are defined in this standard. Security regarding the access, operation, configuration, firmware revision, and data retrieval from an IED is addressed in this standard. Communications for the purpose of power system protection (teleprotection) is not addressed. Encryption for the secure transmission of data both within and external to the substation, including supervisory control and data acquisition, is not part of this standard as this is addressed in other efforts."

IEEE P1711 - Standard for a Cryptographic Protocol for Cybersecurity of Substation Serial Links. This standard defines a cryptographic protocol to provide integrity, and optional confidentiality, for cybersecurity of serial links. It does not address specific applications or hardware implementations, and is independent of the underlying communications protocol.

IEEE 1815-2012 - Standard for Electric Power System Communications-Distributed Network Protocol (DNP3). This standard describes the DNP3 SCADA protocol, incorporating version five of the application-layer authentication procedure called DNP3 Secure Authentication (DNP3-SAv5). DNP3-SAv5 uses a HMAC process to verify that data and commands are received (without tampering) from authorized individual users or devices while limiting computational and communications overhead. SAv5 supports remote update (add/change/revoke) of user credentials using either symmetric or PKI techniques. SAv5 authenticates but does not encrypt messages, hence it does not provide confidentiality. SAv5 can be used together with encryption techniques such as TLS or IEEE 1711 where confidentiality is required.

Institute for Information Infrastructure Protection (I3P)

http://www.thei3p.org/

The I3P is a consortium of leading national cybersecurity institutions, including academic research centers, government laboratories, and non-profit organizations. It was founded in September 2001 to help meet a well-documented need for improved research and development (R&D) to protect the nation's information infrastructure against catastrophic failures. The institute's main role is to coordinate a national cybersecurity R&D program and help build bridges between academia, industry, and government. The I3P continues to work toward identifying and addressing critical research problems in information infrastructure protection and opening information channels between researchers, policymakers, and infrastructure operators. Currently, the I3P does the following:

- Fosters collaboration among academia, industry, and government on pressing cybersecurity problems.
- Develops, manages, and supports national-scale research projects.
- Provides research fellowship opportunities to qualified post-doctoral researchers, faculty, and research scientists.
- Hosts workshops, meetings, and events on cybersecurity and information infrastructure protection issues.
- Builds and supports a knowledge base as an online vehicle for sharing and distributing information to I3P members and others working on information security challenges.

電気電子技術者協会（IEEE）

http://www.ieee.org

IEEE 1686-2007 – 変電所 IED サイバーセキュリティ規格。重要インフラ防護プログラムに合った変電所情報電子デバイス（IEDs）に記載する機能・特性は、この規格で定義される。アクセス、運用、構成、ファームウエア改正及び IED からのデータ取得は、この規格で取り上げられる。電力システム保護用通信（通信保護）は対象外となる。SCADA を含めた変電所内外でのセキュアなデータ通信のための暗号化は、別に扱われるため、この規格では取り上げられない。

IEEE P1711 - 変電所シリアルリンクのサイバーセキュリティ用暗号化プロトコル規格。この規格は暗号化プロトコルについて定め、シリアルリンクの完全性及びオプションの機密性について規定する。特定のアプリケーションやハードウエア実装は取り上げず、基本通信プロトコルには依存していない。

IEEE 1815-2012 - 電力システム通信・配電網プロトコル規格(DNP3)。この規格は、DNP3 セキュア認証(DNP3-SAv5)と呼ばれるアプリケーション層認証手順のバージョン 5 を取り入れた、DNP3 SCADA について記述している。DNP3-SAv5 は HMAC プロセスを使用して、演算及び通信オーバーヘッドを抑えつつ、権限あるユーザ又はデバイスからデータ及びコマンドを（改竄なく）受信したかどうかを検証する。SAv5 は、対称技術又は PKI 技術を用いてユーザ認証情報の遠隔更新（追加・変更・取消）をサポートする。認証は行うが、機密性がないためメッセージの暗号化は行わない。機密性が必要な場合は、TLS や IEEE 1711 等の暗号化技術を併用する。

情報インフラ保護研究所（I3P）

http://www.thei3p.org/

I3P は大学の研究所、国立研究所、NPO 等の主要サイバーセキュリティ機関からなるコンソーシアムである。国の情報インフラを壊滅的障害から守る目的で、研究開発を改善して文書化するため 2001 年 9 月に創設された。主な役割は、国のサイバーセキュリティ研究開発プログラムの調整を行い、産官学の連携を図ることにある。I3P は情報インフラの保護における重要な研究上の問題を明らかにして取り上げるとともに、研究者、政策立案者及びインフラ運用者間の情報経路の開拓を目指している。現在次のような取組を行っている。

- サイバーセキュリティ問題と取り組む産官学間の連携強化
- 国家規模の研究プロジェクトの策定・管理・支援
- 有資格博士課程修了後研究者・教員・研究者への研究機会の提供
- サイバーセキュリティ・情報インフラ保護問題に関するワークショップ・会議・イベントの開催
- I3P メンバーその他情報セキュリティ問題関係者への情報共有・配信媒体としての知識基盤の構築

International Electrotechnical Commission (IEC) Technical Committees 65 and 57

http://www.iec.ch/

IEC is a standards organization that prepares and publishes international standards for all electrical, electronic, and related technologies. These standards serve as a basis for creating national standards and as references for drafting international tenders and contracts. IEC's members include manufacturers, providers, distributors, vendors, consumers, and users, all levels of governmental agencies, professional societies, trade associations, and standards developers from over 60 countries.

In 2004 the IEC Technical Sub-Committee 65C (Industrial Networks), through its working group WG13 (cybersecurity), started to address security issues - within the IEC 61784 standard – for field buses and other industrial communication networks. Results of this work are outlined in part 4, entitled "Digital data communications for measurement and control – Profiles for secure communications in industrial networks."

TC65 WG10 is working to extend this field level communication to address security standards across common automation networking scenarios. The standard being drafted as a result of this work is IEC 62443, entitled "Security for industrial process measurement and control – Network and system security." It is based on a modular security architecture consisting of requirement sets. These modules are mapped into ICS component and network architecture. The resulting requirements can then be formulated for use as the basis for Requests for Proposals (RFP) for data communication standards, and security audits.

TC 57 is focused on Power Systems Management and Associated Information Exchange and is divided up into a series of working groups. Each working group is comprised of members of national standards committees from the countries that participate in the IEC. Each working group is responsible for the development of standards within its domain. The current working groups are:

- WG 3: Telecontrol protocols.
- WG 9: Distribution automation using distribution line carrier systems.
- WG 10: Power system IED communication and associated data models.
- WG 13: Energy management system application program interface (EMS-API).
- WG 14: System interfaces for distribution management (SIDM).
- WG 15: Data and communication security.
- WG 16: Deregulated energy market communications.
- WG 17: Communications Systems for Distributed Energy Resources (DER).
- WG 18: Hydroelectric power plants – Communication for monitoring and control.
- WG 19: Interoperability within TC 57 in the long term.
- WG 20: Planning of (single-sideband) power line carrier systems (IEC 60495) Planning of (single-sideband) power line carrier systems (IEC 60663).
- WG 21: Interfaces and protocol profiles relevant to systems connected to the electrical grid.

国際電気標準会議（IEC）技術委員会 65 及び 57

http://www.iec.ch/

IEC はあらゆる電気、電子及び関連技術に関する国際規格を作成し、発表する規格組織である。規格は、国の規格作成の根拠となり、国際入札・契約を起草する際の参考となる。IEC メンバーはメーカー、プロバイダ、流通業者、ベンダー、消費者・ユーザ、各級レベルの行政機関、専門家協会、貿易協会及び 60 か国の規格作成団体である。

IEC 技術下部委員会 65C（産業用ネットワーク）は 2004 年、その作業グループ WG13（サイバーセキュリティ）を通じて、IEC61784 規格の一部として、フィールドバスその他産業用通信ネットワークのセキュリティ問題の検討に着手した。この作業の結果は、パート 4「計測制御のためのデジタルデータ通信ー産業用ネットワークにおけるセキュアな通信のプロファイル」に概説されている。

TC65 WG10 は、このフィールドレベル通信を拡張して、共通オートメーションネットワーキングシナリオでのセキュリティ規格を取り上げた。その結果起草された規格が IEC 62433 で、『産業用計測制御のセキュリティ - ネットワーク及びシステムセキュリティ』と題する。いくつかの要件からなるモジュール式のセキュリティアーキテクチャを基本としている。それぞれのモジュールは、ICS コンポーネント及びネットワークアーキテクチャにマッピングされる。そこから要件が定められ、データ通信規格及びセキュリティ監査に対する提案要求（RFP）の基礎として利用される。

TC57 は電力システム管理及び関連情報交換に特化しており、一連のグループに分化している。各作業グループは、IEC 加盟各国の規格委員会メンバーで構成されている。各グループは、それぞれのドメイン内での規格作成を担当する。現在の作業グループは以下のとおり。

- WG 3：遠隔制御プロトコル
- WG 9：配電線搬送システムを利用した配電自動化
- WG 10：電力システム IED 通信及び関連データモデル
- WG 13：緊急管理システムアプリケーションプログラムインタフェース（EMS-API）
- WG 14：配電管理システムインタフェース（SIDM）
- WG 15：データ及び通信セキュリティ
- WG 16：エネルギー市場通信の規制緩和
- WG 17：分散エネルギーリソース通信システム（DER）
- WG 18：水力発電所 - 監視制御用通信
- WG 19：TC57 内での長期相互運用性
- WG 20：（単側波帯）送電線搬送システムのプランニング（IEC 60495）、（単側波帯）送電線搬送システムのプランニング（IEC 60663）
- WG 21：配電網接続システムに係るインタフェース及びプロトコルプロファイル

ISA99 Industrial Automation and Control Systems Security Standards

http://www.isa.org/isa99

The ISA99 standards development committee brings together industrial cybersecurity experts from across the globe to develop ISA standards on industrial automation and control system (IACS) security. This original and ongoing ISA99 work is being standardized by the IEC in producing the multi-standard IEC 62443 series. The committee's focus is to improve the confidentiality, integrity, and availability of components or systems used for automation or control and provides criteria for procuring and implementing secure control systems. Compliance with the committee's guidance will improve industrial automation and control system electronic security, and will help identify vulnerabilities and address them, thereby reducing the risk of compromising confidential information or causing industrial automation control system degradation or failure.
All ISA-62443 standards and technical reports are organized into four general categories called General, Policies and Procedures, System, and Component.

- General category includes common or foundational information such as concepts, models and terminology. Also included are work products that describe security metrics and security life cycles for IACS.
- Policies and Procedures category of work products targets the Asset Owner. These address various aspects of creating and maintaining an effective IACS security program.
- System category includes work products that describe system design guidance and requirements for the secure integration of control systems. Core in this is the zone and conduit design model.
- Component category includes work products that describe the specific product development and technical requirements of control system products. This is primarily intended for control product vendors, but can be used by integrator and asset owners for to assist in the procurement of secure products.

The current status of the ISA-62443 documents is provided on the ISA99 Wiki at http://isa99.isa.org/ISA99 Wiki/

General

- **ISA-62443-1-1 (IEC/TS 62443-1-1)** (formerly referred to as "ISA-99 Part 1") was originally published as ISA standard ANSI/ISA-99.00.01-2007, as well as an IEC technical specification IEC/TS 62443-1-1. The ISA99 committee is currently revising it to make it align with other documents in the series, and to clarify normative content.
- **ISA-TR62443-1-2 (IEC 62443-1-2)** is a master glossary of terms used by the ISA99 committee. This document is a working draft.
- **ISA-62443-1-3 (IEC 62443-1-3)** identifies a set of compliance metrics for IACS security. This document is currently under development and the committee will be releasing a draft for comment in 2013.
- **ISA-TR62443-1-4 (IEC/TS 62443-1-4)** defines the IACS security life cycle and use case. This work product has been proposed as part of the series, but as of January 2013 development had not yet started.

ISA99 産業オートメーション及び制御システムセキュリティ規格

http://www.isa.org/isa99

ISA99 規格作成委員会は、世界の産業サイバーセキュリティ専門家を招集して、産業オートメーション制御システム（IACS）セキュリティの ISA 規格の作成に取り組んでいる。当初及び現行の ISA99 作業は、IEC により標準化され、複数の規格 IEC62443 シリーズの作成を目指している。委員会の焦点は、自動化や制御に使用するコンポーネントやシステムの機密性・完全性・可用性を改善し、セキュアな制御システムの調達・実装基準を定めることにある。委員会のガイダンスに従うことで、産業オートメーションや制御システムの電子的セキュリティが改善され、脆弱性と対処方法が明らかになり、秘密情報の漏洩や産業オートメーション制御システムの劣化・故障リスクが減る。

ISA-62443 規格及び技術報告書は、どれも全般、ポリシー・手順、システム及びコンポーネントのいずれかに分類される。

- 全般区分には概念・モデル・用語といった共通的又は基本的情報が含まれる。また、IACS のセキュリティ評価基準及びセキュリティライフサイクルについて記述した作業成果も含まれる。
- 作業成果のポリシー・手順区分は、資産保有者を対象にしたものである。効果的な IACS セキュリティプログラムの作成及び保守の様々な面を取り上げている。
- システム区分には、制御システムのセキュアな統合化に関するシステム設計ガイダンスと要件について記述した作業成果が含まれる。中心となるのは地域及びコンジット設計モデルである。
- コンポーネント区分には、特定製品の開発と制御システム製品の技術要件について記述した作業成果が含まれる。主な対象は制御製品ベンダーであるが、インテグレータや資産保有者がセキュアな製品を調達する際の資とすることもできる。

ISA-62443 文書の現状については、次の ISA99 Wiki サイトで確認できる。
http://isa99.isa.org/ISA99 Wiki/

全般

- **ISA-62443-1-1 (IEC/TS 62443-1-1)**（旧称『ISA-99 Part 1』）は当初 ISA 規格 ANSI/ISA-99.00.01-2007 及び IEC 技術仕様書 IEC/TS 62443-1-1 として発表された。ISA99 委員会は、シリーズの他の文書との整合性を確保し、標準的な内容を明確にするため、現在これの見直し中である。
- **ISA-TR62443-1-2 (IEC 62443-1-2)**は、ISA99 が使用する用語の総用語集である。まだ草案段階にある。
- **ISA-62443-1-3 (IEC 62443-1-3)**は、IACS セキュリティの一連のコンプライアンス評価基準となる。現在作成中で、2013 年に案を発表し、意見を募集する。
- **ISA-TR62443-1-4 (IEC/TS 62443-1-4)**は、IACS のセキュリティライフサイクルと使用例を記載している。この作業成果はシリーズの一部として提唱されたが、2013 年 1 月時点で作成に未着手である。

Policies and Procedures

- **ISA-62443-2-1 (IEC 62443-2-1)** (formerly referred to as "ANSI/ISA 99.02.01-2009 or ISA-99 Part 2") addresses how to establish an IACS security program. This standard is approved and published the IEC as IEC 62443-2-1. It now being revised to permit closer alignment with the ISO 27000 series of standards.
- **ISA-TR62443-2-2 (IEC 62443-2-2)** addresses how to operate an IACS security program. This standard is currently under development.
- **ISA-TR62443-2-3 (IEC/TR 62443-2-3)** is a technical report on the subject of patch management in IACS environments. This report is currently under development.
- **ISA-62443-2-4 (IEC 62443-2-4)** focuses on the certification of IACS supplier security policies and practices. This document was adopted from the WIB organization and is now a working product of the IEC TC65/WG10 committee. The proposed ISA version will be a U.S. national publication of the IEC standard.

System

- **ISA-TR62443-3-1** (**IEC/TR 62443-3-1**) is a technical report on the subject of suitable technologies for IACS security. This report is approved and published as ANSI/ISA-TR99.00.01-2007 and is now being revised.
- **ISA-62443-3-2 (IEC 62443-3-2)** addresses how to define security assurance levels using the zones and conduits concept. This standard is currently under development.
- **ISA-62443-3-3 (IEC 62443-3-3)** defines detailed technical requirements for IACS security. This standard has been published as ANSI/ISA-62443-3-3 (99.03.03)-2013. It was previously numbered as ISA-99.03.03.

Component

- **ISA-62443-4-1 (IEC 62443-4-1)** addresses the requirements for the development of secure IACS products and solutions. This standard is currently under development.
- **ISA-62443-4-2 (IEC 62443-4-2)** series address detailed technical requirements for IACS components level. This standard is currently under development.

ISA100 Wireless Systems for Automation

http://www.isa.org/isa100

The ISA100 Committee will establish standards, recommended practices, technical reports, and related information that will define procedures for implementing wireless systems in the automation and control environment with a focus on the field level. Guidance is directed towards those responsible for the complete life cycle including the designing, implementing, on-going maintenance, scalability or managing industrial automation and control systems, and shall apply to users, system integrators, practitioners, and control systems manufacturers and vendors.

ポリシー及び手順

- **ISA-62443-2-1 (IEC 62443-2-1)** (旧称『ANSI/ISA 99.02.01-2009 又は ISA-99 Part 2』)は、IACS セキュリティプログラムの策定方法を取り上げている。この規格は承認され、IEC 62443-2-1 として発表された。現在 ISO27000 シリーズ規格との整合性を確保するため改訂中である。
- **ISA-TR62443-2-2 (IEC 62443-2-2)**は、IACS セキュリティプログラムの運用方法を取り上げる。この規格は現在作成中である。
- **ISA-TR62443-2-3 (IEC/TR 62443-2-3)**は、IACS 環境におけるパッチ管理に関する技術報告書である。この報告書は現在作成中である。
- **ISA-62443-2-4 (IEC 62443-2-4)**は、IACS サプライヤのセキュリティポリシー及び規範の認定書に特化している。本書は WIB 組織が採用し、IEC TC65/WG10 委員会の作業成果となっている。ISA 版の案は、IEC 規格の政府文書となろう。

システム

- **ISA-TR62443-3-1 (IEC/TR 62443-3-1)**は、IACS セキュリティの適合技術に関する技術報告書である。本報告書は承認され、ANSI/ISA-TR99.00.01-2007 として発表され、現在改訂中である。
- **ISA-62443-3-2 (IEC 62443-3-2)**は、地域及びコンジット設計概念を利用したセキュリティ保証レベルの定義方法について取り上げている。この規格は現在作成中である。
- **ISA-62443-3-3 (IEC 62443-3-3)**は、IACS セキュリティの詳細な技術要件について明らかにしている。この規格は ANSI/ISA-62443-3-3 (99.03.03)-2013 として発表された。旧番号は ISA-99.03.03 だった。

コンポーネント

- **ISA-62443-4-1 (IEC 62443-4-1)**は、セキュアな IACS 製品及びソリューションの開発要件について取り上げている。この規格は現在作成中である。
- **ISA-62443-4-2 (IEC 62443-4-2)**シリーズは、IACS コンポーネントレベルの詳細な技術要件について取り上げている。この規格は現在作成中である。

ISA100 オートメーション用ワイヤレスシステム

http://www.isa.org/isa100

ISA100 委員会は、フィールドレベルに特化したオートメーション及び制御環境におけるワイヤレスシステムの手順を規定した規格や推奨規範を定め、技術報告書や関連情報を配信する。ガイダンスは産業オートメーション及び制御システムの設計、実装、恒常的保守、スケーラビリティ、管理等ライフサイクル全般の担当者を対象とし、ユーザ、システムインテグレータ、実務従事者及び制御システムメーカー・ベンダーに適用される。

ISO 27001

http://www.iso.org/, http://www.27000.org

ISO 27001 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System. The objective of the standard itself is to "provide requirements for establishing, implementing, maintaining and continuously improving an Information Security Management System (ISMS)." Regarding its adoption, this should be a strategic decision. Further, "The design and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization." The content sections of the standard include:

- Context of the Organization.
- Information Security Leadership.
- Planning an ISMS.
- Support.
- Operation.
- Performance Evaluation.
- Improvement.
- Annex A – List of controls and their objectives.

The 2005 version of the standard heavily employed the Plan-Do-Check-Act model to structure the processes, and reflect the principles set out in the OECG guidelines (see oecd.org). However, the latest, 2013 version, places more emphasis on measuring and evaluating how well an organization's ISMS is performing.

ISO 27001

http://www.iso.org/, http://www.27000.org

ISO27001 は、情報セキュリティ管理システムの確立、実装、運用、監視、調査、保守及び改善に関するモデルとなる。この企画の目的は、「情報セキュリティ管理システム（ISMS）の確立、実装、保守及び継続的改善に関する要件を示す」ことにある。その採用については、戦略的な決定事項となる。更に「組織の情報セキュリティ管理システムの設計及び実装は、組織の必要・目的、セキュリティ要件、組織的プロセス及び組織の規模・構造に影響される」。規格の目次構成は以下のとおり。

- 組織の情況
- 情報セキュリティの指導
- ISMS のプランニング
- 支援
- 運用
- 業績評価
- 改善
- 付録 A - 制御とその目的リスト

2005 年版規格では、計画・実行・確認・行動モデルを大いに取り入れ、プロセスを構造化し、OECG ガイドラインに記載されている原則を反映している（oecd.org を参照）。しかし最新の 2013 年版では、組織の ISMS 業務遂行状況の計測・評価にいっそうの重点が置かれている。

ISO 27002

http://www.iso.org/, http://www.27000.org

ISO 27002 "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization." The actual controls listed in the standard are intended to address the specific requirements identified via a formal risk assessment. The standard is also intended to provide a guide for the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities."[81]

In 2013 the current version was published. ISO 27002:2013 contains 114 controls, fewer than the 133 documented in the 2005 version. However for additional granularity, these are presented in 14 sections, rather than the original 11:

- Security Policy.
- Organization of Information Security.
- Human Resource Security.
- Asset Management.
- Access Control.
- Cryptography.
- Physical and Environmental Security.
- Operations Security.
- Communications Security.
- Information Systems Acquisition, Development, Maintenance.
- Supplier Relationships.
- Information Security Incident Management.
- Information Security Aspects of Business Continuity.
- Compliance.

[81] http://www.27000.org/iso-27002.htm.

ISO 27002

http://www.iso.org/, http://www.27000.org

ISO　27002 は「組織内における情報セキュリティ管理の開始、実装、保守及び改善に関するガイドラインと一般原則を定めた」。規格のリストに含まれている実際の制御は、正規のリスク評価で定められた具体的要件を取り上げている。また「組織のセキュリティ基準及び効果的なセキュリティ管理規範（の発展に向けたガイドを与え）、組織間活動への信頼の醸成に資する」ことを目的としている。[82]

現行版は 2013 年に発表された。ISO 27002:2013 には 114 の制御が納められており、2005 年版の 133 よりも減っている。ただしセクションは 11 から次の 14 に増え、きめ細かくなっている。

- セクションポリシー
- 情報セキュリティ組織
- 人的資産のセキュリティ
- 資産管理
- アクセス制御
- 暗号化
- 物理的・環境的セキュリティ
- 運用セキュリティ
- 通信セキュリティ
- 情報システムの取得・開発・保守
- サプライヤとの関係
- 情報セキュリティインシデント管理
- 情報セキュリティ面から見た事業継続性
- コンプライアンス

[82] http://www.27000.org/iso-27002.htm.

International Council on Large Electric Systems (CIGRE)

http://www.cigre.org/

The International Council on Large Electric Systems (CIGRE) is a nonprofit international association based in France. It has established several study committees to promote and facilitate the international exchange of knowledge in the electrical industry by identifying recommended practices and developing recommendations. Three of its study committees focus on control systems:

- The objectives of the B3 Substations Committee include the adoption of technological advances in equipment and systems to achieve increased reliability and availability.
- The C2 System Operation and Control Committee focuses on the technical capabilities needed for the secure and economical operation of existing power systems including control centers and operators.
- The D2 Information Systems and Telecommunication for Power Systems Committee monitors emerging technologies in the industry and evaluates their possible impact. In addition, it focuses on the security requirements of the information systems and services of control systems.

LOGIIC – Linking the Oil and Gas Industry to Improve Cybersecurity

http://www.dhs.gov/csd-logiic

The LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) program is an ongoing collaboration of oil and natural gas companies and the DHS Science and Technology Directorate (S&T). LOGIIC was formed in 2004 to facilitate cooperative research, development, testing, and evaluation procedures to improve cybersecurity in petroleum industry digital control systems. The program undertakes collaborative R&D projects to improve the level of cybersecurity in critical systems of interest to the oil and natural gas sector. The program objective is to promote the interests of the sector while maintaining impartiality, the independence of the participants, and vendor neutrality. After a successful first project, the LOGIIC consortium was formally established as a collaboration between DHS, the Automation Federation, and five of the major oil and gas companies. The LOGIIC program has completed several R&D projects, and more projects are being planned and started.

国際大電力システム会議（CIGRE）

http://www.cigre.org/

CIGRE はフランスに拠点を置く非営利国際機関である。いくつかの研究委員会があり、推奨規範の定義づけや推奨事項の策定を通じて、電力業界における国際的な意見交換を促進している。このうち次の 3 委員会が制御システムに特化している。

- B3 変電所委員会の目的には、装備品やシステムの技術的進歩を取り入れて、信頼性と可用性を確保することが含まれる。
- C2 システム運用制御委員会は、制御センターや操作員を含めた既存電力システムの運用をセキュアかつ経済的にするための技術力に重点を置いている。
- D2 電力システム用情報システム電気通信委員会は、業界の新興技術を注視し、その影響を評価する。また制御システムの情報システム・サービスに関するセキュリティ要件をも重視している。

LOGIIC – サイバーセキュリティを改善する石油・ガス業界の連携

http://www.dhs.gov/csd-logiic

LOGIIC（サイバーセキュリティを改善する石油・ガス業界の連携）プログラムは、石油・ガス会社及び DHS 科学技術局（S&T）間で現在進展中の協力活動である。LOGIIC は 2004 年に制定され、共同研究・開発・試験・評価手順を促進し、石油業界のデジタル制御システムのサイバーセキュリティ向上を目指している。 石油・天然ガス業界の利益に直結した重要システムのサイバーセキュリティレベルを上げるため、共同研究・開発を手がけている。プログラムの目的は、メンバー間の公平、独立性及びベンダーの中立性を保ちつつ、業界の利益を促進することにある。最初のプロジェクトが成功した後、LOGIIC コンソーシアムが DHS、オートメーション連盟及び石油・ガス大手 5 社間で正式に発足した。これまでいくつかの研究開発プロジェクトが完了しており、今後更に新規計画が予定されている。

National SCADA Test Bed (NSTB)

http://energy.sandia.gov/infrastructure-security/cyber/scada-systems/testbeds/national-scada-testbed/

The National Supervisory Control and Data Acquisition (SCADA) Test Bed is a DOE Office of Electricity Delivery and Energy Reliability (OE) -sponsored resource to help secure our nation's energy control systems. It combines state-of-the-art operational system testing facilities with research, development, and training to discover and address critical security vulnerabilities and threats to the energy sector.

Working in partnership with the energy sector, the National SCADA Test Bed seeks to:

- Identify and mitigate existing vulnerabilities.
- Facilitate development of security standards.
- Serve as an independent entity to test SCADA systems and related control system technologies.
- Identify and promote best cybersecurity practices.
- Increase awareness of control systems security within the energy sector.
- Develop advanced control system architectures and technologies that are more secure and robust.

Partners in the NSTB include Idaho National Laboratory, Sandia National Laboratories, Argonne National Laboratory, Pacific Northwest National Laboratory, and the National Institute of Standards and Technology.

米国 SCADA テストベッド（NSTB）

http://energy.sandia.gov/infrastructure-security/cyber/scada-systems/testbeds/national-scada-testbed/

米国 SCADA テストベッドは、DOE の配電エネルギー信頼性局（OE）の支援によるリソースで、米国のエネルギー制御システムのセキュア化を助成する。最新の運用システム試験施設と研究・開発・訓練を一体化して、エネルギー業界にとっての重大なセキュリティ脆弱性・脅威を見つけて取り組む。

エネルギー業界と連携し、米国 SCADA テストベッドは以下を目標としている。

- 既存の脆弱性を明らかにして緩和する
- セキュリティ規格の開発を促進する
- SCADA システム技術及び関連制御システム技術の独立試験機関として機能する
- サイバーセキュリティの最良規範を定めて促進する
- エネルギー業界における制御システムセキュリティに対する意識を高める
- よりセキュアで強固な最新制御システムアーキテクチャ及び技術を開発する

NSTB にはアイダホ国立研究所、サンディア国立研究所、アーゴン国立研究所、太平洋北西国立研究所及び米国標準技術局が加盟している。

NIST Special Publication 800 Series Security Guidelines

http://csrc.nist.gov/publications/nistpubs/index.html

The NIST Special Publication 800 series of documents on information technology reports on the NIST Information Technology Laboratory (ITL) research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. In addition to NIST SP 800-82, the following is a listing of some additional 800 series documents that have significant relevance to the ICS security community. These as well as many others are available through the URL listed above.

- NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems* [19].
- NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [79].
- NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* [21].
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* [20].
- NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies* [40].
- NIST SP 800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy* [85].
- NIST SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks* 0.
- NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* [61].
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [22].
- NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans* [23].
- NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide* [59].
- NIST SP 800-63-2, *Electronic Authentication Guideline* [53].
- NIST SP 800-64 Revision 2, *Security Considerations in the Information System Development Life Cycle* [46].
- NIST SP 800-70 Revision 2, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers* [26].
- NIST SP 800-77, *Guide to IPsec VPNs* [74].
- NIST SP 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* [60].
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response* [93].

NIST 特別出版物 800 シリーズセキュリティガイドライン

http://csrc.nist.gov/publications/nistpubs/index.html

SP800 シリーズは、情報技術研究所（ITL）の研究、ガイダンス及びコンピュータセキュリティにおける取組並びに産官学との連携に関する情報技術報告書である。重点分野として暗号技術とその応用、最新認証、公開鍵インフラ、インターネット作業のセキュリティ、基準・保証、セキュリティ管理・支援等が含まれている。NIST SP 800-82 に加えて、ICS セキュリティ関係者に大いに関係するものとして、次の 800 シリーズ文書も用意されている。これら以外にも、上記の URL から利用できるものがある。

- NIST SP 800-18 第 1 版『連邦情報システム用セキュリティ計画書の作成ガイド』[19]
- NIST SP 800-30 第 1 版『リスク評価実施ガイド』[79]
- NIST SP 800-37 第 1 版『連邦情報システムへのリスク管理体系適用ガイド：セキュリティライフサイクルアプローチ』[21]
- NIST SP 800-39『情報セキュリティリスクの管理：組織、任務及び情報システム概説』[20]
- NIST SP 800-40 第 3 版『企業パッチ管理技術ガイド』[40]
- NIST SP 800-41 第 1 版『ファイアウォール及びファイアウォールポリシーガイドライン』[85]
- NIST SP 800-48 第 1 版『レガシーIEEE 802.11 ワイヤレスネットワークセキュリティガイド』[0]
- NIST SP 800-50『情報技術セキュリティ意識訓練プログラムの構築』[61]
- NIST SP 800-53 第 4 版『連邦情報システム・組織のセキュリティ・プライバシー管理』[22]
- NIST SP 800-53A 第 4 版『連邦情報システム・組織のセキュリティ・プライバシー管理評価：効果的セキュリティ評価計画書の作成』[23]
- NIST SP 800-61 第 2 版『コンピュータセキュリティインシデント処理ガイド』[59]
- NIST SP 800-63-2『電子認証ガイドライン』[53]
- NIST SP 800-64 第 2 版『情報システム開発ライフサイクルにおけるセキュリティ考慮事項』[46]
- NIST SP 800-70 第 2 版『IT 製品の国家チェックリストプログラム：チェックリストユーザ・開発者ガイドライン』[26]
- NIST SP 800-77『IPSsec VPNs ガイド』[74]
- NIST SP 800-83 第 1 版『マルウエアインシデント防止及びデスクトップ・ラップトップの取扱ガイド』[60]
- NIST SP 800-86『インシデント対応時の調査技術の適用ガイド』[93]

- NIST SP 800-88 Revision 1, *Guidelines for Media Sanitization* [78].
- NIST SP 800-92, *Guide to Computer Security Log Management* [68].
- NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)* [55].
- NIST SP 800-97, *Establishing Robust Security Networks: a Guide to IEEE 802.11i* [64].
- NIST SP 800-100, *Information Security Handbook: A Guide for Managers* [27].
- NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices* [94].
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment* [41].
- NIST SP 800-123, *Guide to General Server Security* [95].
- NIST SP 800-127, *Guide to Securing WiMAX Wireless Communications* [96].
- NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems* [97].
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* [81].

NIST Cybersecurity Framework

http://www.nist.gov/cyberframework/index.cfm

Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013 [83]. It directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices – for reducing cyber risks to critical infrastructure.

NIST released the first version of the Framework for Improving Critical Infrastructure Cybersecurity on February 12, 2014 [83]. The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

The Department of Homeland Security's Critical Infrastructure Cyber Community C³ Voluntary Program helps align critical infrastructure owners and operators with existing resources that will assist their efforts to adopt the Cybersecurity Framework and manage their cyber risks. Learn more about the C³ Voluntary Program by visiting: www.dhs.gov/ccubedvp.

NIST has also issued a companion Roadmap that discusses NIST's next steps with the Framework and identifies key areas of cybersecurity development, alignment, and collaboration.

- NIST SP 800-88 第 1 版『メディアサニタイズガイドライン』[78]
- NIST SP 800-92『コンピュータセキュリティログ管理ガイド』[68]
- NIST SP 800-94『侵入検知防止システム（IDPS）ガイド』[55]
- NIST SP 800-97『強固なセキュリティネットワークの構築：IEEE 802.11i ガイド』[64]
- NIST SP 800-100『情報セキュリティハンドブック：管理者ガイド』[27]
- NIST SP 800-111『エンドユーザデバイス用ストレージ暗号化技術ガイド』[94]
- NIST SP 800-115『情報セキュリティ試験評価技術ガイド』[41]
- NIST SP 800-123『一般的サーバセキュリティガイド』[95]
- NIST SP 800-127『WiMAX ワイヤレス通信ガイド』[96]
- NIST SP 800-128『情報システムのセキュリティ重視設定管理ガイド』[97]
- NIST SP 800-137『連邦情報システム・組織の情報セキュリティ継続監視』[81]

NIST のサイバーセキュリティ体系

http://www.nist.gov/cyberframework/index.cfm

米国の国家・経済安全保障は、信頼性の高い重要インフラの機能に依存しているとして、大統領命令 13636 重要インフラサイバーセキュリティの改善を 2013 年 2 月に発令した[83]。その中で NIST は関係者と連携し、既存の規格、ガイドライン及び規範を基に、重要インフラへのサイバーリスクの軽減に向けて、自発的な体系を構築するよう命ぜられた。

NIST は 2014 年 2 月 14 日、重要インフラサイバーセキュリティ改善体系第 1 版を発表した[83]。産・官間の連携で構築された体系は、重要インフラ保護を促進する規格、ガイドライン及び規範から構成されている。優先順位づけされ柔軟性があり、反復可能で費用効果の高い取組により、重要インフラの所有者及び運用者がサイバーセキュリティ関連リスクを管理できるように支援する。

国土安全保障省の重要インフラサイバーコミュニティ C³ 任意プログラムは、重要インフラの保有者及び操作員が既存リソースを活用しつつ、サイバーセキュリティ体系を取り入れ、サイバーリスクを管理する資となる。C³ 任意プログラムの詳細は以下の URL にある。
www.dhs.gov/ccubedvp.

NIST は手引きとなるロードマップも発表し、この体系の次なるステップについて説明し、サイバーセキュリティ開発・調整・連携の主な分野を明らかにしている。

NIST Industrial Control System Security Project

http://csrc.nist.gov/groups/SMA/fisma/ics/

As part of the continuing effort to provide effective security standards and guidance to federal agencies and their contractors in support of the Federal Information Security Management Act and as part of the effort to protect the nation's critical infrastructure, NIST continues to work with public and private sector entities on sector-specific security issues.
Industrial and process control systems are an integral part of the US critical infrastructure and the protection of those systems is a priority for the federal government. This project intends to build upon the current FISMA security standards and provide targeted extensions and/or interpretations of those standards for industrial and process controls systems where needed. Since many industrial and process controls systems are supporting private sector organizations, NIST will collaborate with ongoing standards efforts addressing these sector-specific types of systems.

NIST Cybersecurity for Manufacturing Systems Project

http://www.nist.gov/el/isd/cs/csms.cfm

Smart manufacturing systems need to be protected from vulnerabilities that may arise as a result of their increased connectivity, use of wireless networks and sensors, and use of widespread information technology. Manufacturers are hesitant to adopt common security technologies, such as encryption and device authentication, due to concern for potential negative performance impacts in their systems. This is exacerbated by a threat environment that has changed dramatically with the appearance of advanced persistent attacks specifically targeting industrial systems, such as Stuxnet. This project will develop a cybersecurity risk management framework with supporting guidelines, methods, metrics and tools to enable manufacturers, technology providers, and solution providers to assess and assure cybersecurity for smart manufacturing systems. The cybersecurity risk management framework and methodology will stimulate manufacturer adoption and enable effective use of security technologies, leading to smart manufacturing systems that offer security, reliability, resilience and continuity in the face of disruption and major incidents.

NIST Cybersecurity for Smart Grid Systems Project

http://www.nist.gov/el/smartgrid/cybersg.cfm

Smart grid cybersecurity must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. The Smart Grid Interoperability Panel (SGIP) Cybersecurity Committee (SGCC), which is led and managed by the NIST Information Technology Laboratory (ITL), Computer Security Division, is moving forward in fiscal year 2014 to address the critical cybersecurity needs in the areas of Advanced Metering Infrastructure (AMI) security requirements, cloud computing, supply chain, and privacy recommendations related to emerging standards. This project will provide foundational cybersecurity guidance, cybersecurity reviews of standards and requirements, outreach, and foster collaborations in the cross-cutting issue of cybersecurity in the smart grid.

NIST 産業用制御システムセキュリティプロジェクト

http://csrc.nist.gov/groups/SMA/fisma/ics/

連邦政府機関及び連邦情報セキュリティ管理法を支える契約業者に効果的なセキュリティ規格・ガイダンスを提供する継続的な取組の一環として、また国の重要インフラを保護する取組の一環として、NIST は官民諸団体と連携して、業界固有のセキュリティ問題と継続的に協働している。産業用システム及びプロセス制御システムは、米国の重要インフラの不可欠な一部であり、これらシステムに対する保護は、連邦政府の優先的課題である。本プロジェクトは、現行 FISMA セキュリティ規格を基礎として、これら産業用システム及びプロセス制御システムの規格を、必要に応じて拡張・解釈することを主眼としている。多くの産業用システム及びプロセス制御システムは、民間業界組織を支えているため、NIST は、このような業界固有のシステムを対象とした現行規格の取組と連携している。

生産システムプロジェクト用 NIST サイバーセキュリティ

http://www.nist.gov/el/isd/cs/csms.cfm

スマート生産システムは、接続数、ワイヤレスネットワーク/センサの利用及び広範な情報技術の利用が増えた結果、脆弱性が生じたため保護が必要となる。メーカーは、システムにマイナスの影響が出ることを恐れて、暗号化やデバイス認証といった、一般的なセキュリティ技術の採用に消極的である。Stuxnet のような産業用システムに特化した執拗な攻撃が出現したために、脅威環境が激変したこととあいまって、いっそう事態は悪化する。本プロジェクトでは、根拠となるガイドライン、方法、評価基準及びツールの伴ったサイバーセキュリティリスク管理体系を策定し、メーカー、技術提供者及びソリューション提供者がスマート生産システム用サイバーセキュリティの評価・保証を実施できるようにする。サイバーセキュリティリスク管理体系及び方法論は、メーカーがセキュリティ技術を採用して有効利用する弾みをつけ、中断や大規模インシデント時のセキュリティ、信頼性、柔軟性及び継続性を確保できるスマート生産システムへ導くものとなる。

スマートグリッドシステムプロジェクト用 NIST サイバーセキュリティ

http://www.nist.gov/el/smartgrid/cybersg.cfm

スマートグリッドサイバーセキュリティでは、不満を抱いた従業員、産業スパイ、テロリスト等による計画的な攻撃だけでなく、ユーザの過誤、装備品障害及び自然災害に起因する情報インフラの想定外の機能低下も検討対象にしなければならない。NIST の情報技術研究所（ITL）コンピュータセキュリティ部の監督下にあるスマートグリッド相互運用パネル（SGIP）サイバーセキュリティ委員会は 2014 会計年度に、最新計量インフラ（AMI）セキュリティ要件、クラウドコンピューティング、サプライチェーン及び新興規格関連民間推奨事項分野での重要サイバーセキュリティの必要性の検討に向けて活動を開始した。本プロジェクトは基本的サイバーセキュリティガイダンス、規格及び要件のサイバーセキュリティ調査について記述し、スマートグリッドの分野横断的なサイバーセキュリティ問題での連携を構築する。

NIST Smart Grid System Testbed Facility

http://www.nist.gov/el/smartgrid/sgtf.cfm

NIST is charged by the 2007 Energy Independence and Security Act (EISA) with facilitation of interoperability standards to enable successful implementation of the evolving cyber-physical national electric grid system known as the smart grid (SG). The Smart Grid Testbed Facility will create a unique set of interconnected and interacting labs in several key measurement areas—contiguously located on the NIST Gaithersburg site—that will accelerate the development of SG interoperability standards by providing a combined testbed platform for system measurements, characterization of smart grid protocols, and validation of SG standards, with particular emphasis on microgrids. (A microgrid is defined as a subset of the grid which has the capability of being quickly disconnected from, and functioning independently of, the larger grid.) Measurements will include eight areas: power conditioning, synchrophasor metrology, cybersecurity, precision time synchronization, electric power metering, modeling/evaluation of SG communications, sensor interfaces, and energy storage. The testbed will serve as a core Smart Grid Program research facility to address measurement needs of the evolving SG industrial community including the measurement and validation issues.

North American Electric Reliability Corporation (NERC)

http://www.nerc.com/

NERC's mission is to improve the reliability and security of the bulk power system in North America. To achieve that, NERC develops and enforces reliability standards; monitors the bulk power system; assesses future adequacy; audits owners, operators, and users for preparedness; and educates and trains industry personnel. NERC is a self-regulatory organization that relies on the diverse and collective expertise of industry participants. As the Electric Reliability Organization, NERC is subject to audit by the U.S. Federal Energy Regulatory Commission and governmental authorities in Canada

NERC has issued a set of cybersecurity standards to reduce the risk of compromise to electrical generation resources and high-voltage transmission systems above 100 kV, also referred to as bulk electric systems. Bulk electric systems include Balancing Authorities, Reliability Coordinators, Interchange Authorities, Transmission Providers, Transmission Owners, Transmission Operators, Generation Owners, Generation Operators, and Load Serving Entities. The cybersecurity standards include audit measures and levels of non-compliance that can be tied to penalties.

The set of NERC cybersecurity Standards includes the following:

- CIP-002, *Cyber Security - Critical Cyber Asset Identification*.
- CIP-003, *Cyber Security - Security Management Controls*.
- CIP-004, *Cyber Security - Personnel & Training*.
- CIP-005, *Cyber Security - Electronic Security Perimeter(s)*.
- CIP-006, *Cyber Security - Physical Security of Critical Cyber Assets*.
- CIP-007, *Cyber Security - Systems Security Management*.
- CIP-008, *Cyber Security - Incident Reporting and Response Planning*.
- CIP-009, *Cyber Security - Recovery Plans for Critical Cyber Assets*.

NIST スマートグリッドシステムテストベッド施設

http://www.nist.gov/el/smartgrid/sgtf.cfm

NIST は 2007 年、エネルギー独立セキュリティ法（EISA）により、スマートグリッド（SG）として知られる国のサイバー物理的配電システムを効果的に実装するための相互運用性規格を作成するよう義務づけられた。スマートグリッドシステムテストベッド施設は、相互接続され相互作用する一連の研究所群をいくつかの重要計測エリア内に構築し（NIST のゲイサーズバーグ施設に隣接）、システム計測、スマートグリッドプロトコルの特性分析及び SG 規格検証用の結合テストベッドプラットホームを提供することにより、特にマイクログリッドを重点とした SG 相互運用性規格の作成を急いでいる。（マイクログリッドは、大規模グリッドから迅速に分離して、独立した機能能力を発揮するグリッドサブセットと定義される。）次の 8 項目を計測する。電力状態、シンクロフェーザ計測、サイバーセキュリティ、精密時間同期、電力測定、SG 通信のモデリング・評価、センサインターフェイス及びエネルギー保存。テストベッドは、中核的なスマートグリッドプログラム研究施設として機能し、計測・検証問題を含めて進展中の、SG 産業共同体の計測ニーズに対応している。

北米電力信頼性評議会（NERC）

http://www.nerc.com/

NERC の任務は、北米における大電力システムの信頼性とセキュリティを改善することにある。このため NERC は、信頼性規格の作成・施行、大電力システムの監視、将来的な妥当性の評価、保有者・操作員・ユーザの即応性監査、業界職員の教育訓練を行っている。NERC は自主規制組織で、業界参加者の多様かつ包括的専門知識に依存している。電力信頼性組織として、米国の連邦エネルギー規制委員会とカナダの行政当局の監査を受ける義務がある。

発電リソース及び 100kV 超高電圧送電システム（大電力システムともいう）の機能低下リスクを軽減するため、NERC は一連のサイバーセキュリティ規格を発表してきた。大電力システには事業者（Balancing Authorities）、信頼性コーディネータ、送電プロバイダ、送電保有者、送電事業者、発電保有者、発電事業者及び小売事業者が含まれる。サイバーセキュリティ規格には、監査手段及び罰則に結びつく各級ノンコンプライアンスが含まれる。

一連の NERC サイバーセキュリティ規格には以下のものがある。

- CIP-002『サイバーセキュリティ - 重要サイバー資産の識別』
- CIP-003『サイバーセキュリティ - セキュリティ管理対策』
- CIP-004『サイバーセキュリティ - 職員及び訓練』
- CIP-005『サイバーセキュリティ - 電子セキュリティの周辺』
- CIP-006『サイバーセキュリティ - 重要サイバー資産の物理的セキュリティ』
- CIP-007『サイバーセキュリティ - システムセキュリティ管理』
- CIP-008『サイバーセキュリティ - インシデントの届出及び対応計画の立案』
- CIP-009『サイバーセキュリティ - 重要サイバー資産復旧計画』

SANS ICS Security Courses

http://ics.sans.org/

The ICS curriculum provides hands-on training courses focused on Attacking and Defending ICS environments. These courses equip both security professionals and control system engineers with the knowledge and skills they need to safeguard our critical infrastructures.

The Global Industrial Cyber Security Professional (GICSP) is the newest certification in the Global Information Assurance Certification (GIAC) family and focuses on the foundational knowledge of securing critical infrastructure assets. The GICSP bridges together IT, engineering and cybersecurity to achieve security for industrial control systems from design through retirement.

Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG)

http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

The primary goal of the working group is to develop an overall cybersecurity strategy for the Smart Grid that includes a risk mitigation strategy to ensure interoperability of solutions across different domains/components of the infrastructure. The cybersecurity strategy needs to address prevention, detection, response, and recovery. Implementation of a cybersecurity strategy requires the definition and implementation of an overall cybersecurity risk assessment process for the Smart Grid.

The working group's effort is documented in NIST Interagency Report (NISTIR) 7628 Revision 1, *Guidelines for Smart Grid Cybersecurity* [98].

SANS ICS セキュリティ課程

http://ics.sans.org/

ICS カリキュラムは、ICS 環境に対する攻撃と防御に特化した実地訓練課程である。セキュリティ専門員と制御システムエンジニア双方に、重要インフラを守るための知識と技量を教示する。

世界産業サイバーセキュリティ専門家（GICSP）は、世界情報保証認定書（GIAC）ファミリの中でも最新の認定書で、重要インフラ資産のセキュリティに関する基本知識を重視している。GICSP は、IT、エンジニアリング及びサイバーセキュリティの架け橋となり、設計から用途廃止まで、産業用制御システムのセキュリティを実現する。

スマートグリッド相互運用性パネル（SGIP）サイバーセキュリティ作業グループ（CSWG）

http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG

作業グループの主な目的は、スマートグリッドのサイバーセキュリティ戦略を策定することにあり、それにはインフラの種々の領域・コンポーネントにまたがるソリューションの相互運用性を確保するためのリスク緩和策も含まれる。サイバーセキュリティ戦略は、予防・検知・対応・復旧を取り上げる必要がある。サイバーセキュリティ戦略を実施するには、スマートグリッドの全般的サイバーセキュリティリスク評価プロセスを明らかにして、実施する必要がある。

作業グループの取組は、NIST 政府機関間報告書（NISTIR）7628 第 1 版『スマートグリッドサイバーセキュリティガイドライン』に記載されている[98]。

Appendix E—ICS Security Capabilities and Tools

This section provides an overview of security capabilities that are available to or being developed in support of the ICS community. There are several security products that are marketed specifically for ICS, while others are general IT security products that are being used with ICS. Many of the products available offer "single point solutions," where a single security product offers multiple levels of protection. In addition to available products, this section also discusses some research and development work towards new products and technologies. Each organization should make a risk-based determination whether to employ the security capabilities and tools mentioned in this appendix.

Data Diode

A data diode (also referred to as a unidirectional gateway, deterministic one-way boundary device or unidirectional network) is a network appliance or device allowing data to travel only in one direction, used in guaranteeing information security or protection of critical digital systems, such as industrial control systems, from inbound cyber attacks. While use of these devices is common in high security environments such as defense, where they serve as connections between two or more networks of differing security classifications, the technology is also being used to enforce one-way communications outbound from critical digital systems to untrusted networks.

Encryption

Encryption protects the confidentiality of data by encoding the data to ensure that only the intended recipient can decode it. There are some commercially available encryption products designed specifically for ICS applications, as well as general encryption products that support basic serial and Ethernet-based communications.

Firewalls

Firewalls are commonly used to segregate networks to protect and isolate ICS. These implementations use commercially available firewalls that are focused on Internet and corporate application layer protocols and are not equipped to handle ICS protocols. Research was performed by an IT security vendor in 2003 to develop a Modbus-based firewall that allows policy decisions to be made on Modbus/TCP header values just as traditional firewalls filter on TCP/UDP ports and IP addresses [76]. There are currently several firewalls available for ICS.

Intrusion Detection and Prevention

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are being deployed on ICS networks and components to detect well-known cyber attacks. Network IDS products monitor network traffic and use various detection methods, such as comparing portions of the traffic to signatures of known attacks. In contrast, host intrusion detection uses software loaded on a host computer, often with attack signatures, to monitor ongoing events and data on a computer system for possible exploits. IPS products take intrusion detection a step further by automatically acting on detected exploits to attempt to stop them [57].

The required task of a security team to constantly monitor, evaluate, and quickly respond to intrusion detection events is sometimes contracted to a managed security service provider (MSSP). MSSPs have correlation and analysis engines to process and reduce the vast amounts of events logged per day to a small subset that needs to be manually evaluated. There are also correlation and analysis engine products available to large organizations wanting to perform this function in-house. Security information and event

付録 E ICS セキュリティ機能及びツール

このセクションでは、ICS 共同体が利用できるセキュリティ機能や、現在開発中のものについて概説する。市場には ICS に特化したセキュリティ製品がいくつかあり、ICS で利用されている一般的な IT セキュリティ製品もある。入手可能な製品の多くは「単一ソリューション」で、1 つのセキュリティ製品が多様なレベルの保護を与えている。入手可能な製品に加えて、このセクションでは、新製品・新技術に向けた研究開発についてもいくつか取り上げる。各組織は、この付録で言及されているセキュリティ機能及びツールの採用の是非について、リスクに立脚して判断すべきである。

データダイオード

データダイオード（単方向ゲートウェイ、決定論的一方通行境界デバイス又は単方向ネットワークとも呼ばれる）は、ネットワーク機器又はデバイスで、データを一方向にのみ流して、情報セキュリティを保証し、産業用制御システム等の重要デジタルシステムを外部サイバー攻撃から保護する。このようなデバイスの利用は、国防等のハイセキュリティ環境では普通に見られ、異種セキュリティ区分を有する、2 つ以上のネットワーク間の接続を確立し、その技術は、重要デジタルシステムから外部の信頼できないネットワークに向かう単方向の通信にも利用される。

暗号化

暗号化は、データをコード化して所期の受信者だけが復号できるようにすることで、データの機密性を保護する。ICS 用途に特化した市販の暗号化製品がいくつかあり、基本的なシリアル及び Ethernet ベースの通信に対応した汎用暗号化製品もある。

ファイアウォール

ファイアウォールは通常、ネットワークを分離して ICS を保護・隔離するために使用する。実装は、インターネット及び企業アプリケーション層プロトコルに特化し、ICS プロトコルは処理しない市販のファイアウォールを使用して行う。2003 年に IT セキュリティベンダーが Modbus ベースファイアウォールの開発に向けて研究を行った。これは従来のファイアウォールが TCP/UDP ポート及び IP アドレスでフィルタリングを行うように、Modbus/TCP ヘッダー値でポリシー決定を行うことができる。現在 ICS 用に利用できるファイアウォールがいくつかある。

侵入検知及び防止

侵入検知システム（IDS）及び侵入防止システム（IPS）は、既知のサイバー攻撃を検知するため、ICS ネットワーク及びコンポーネントに展開されている。ネットワーク IDS 製品はネットワークトラフィックを監視し、既知の攻撃のトラフィックシグネチャの一部を比較するなど、種々の検知方法を利用している。対照的にホスト侵入検知では、ホストコンピュータにインストールしたソフトウエアを利用し、多くは攻撃シグネチャを参考にして、コンピュータシステム上で進行中の事象及びデータを監視し、悪用の有無を検知する。IPS 製品は、侵入検知から一歩進めて、検知した悪用の中止を試みる[57]。

セキュリティチームに求められる侵入検知の常続監視・評価・迅速対応という業務は、管理セキュリティサービスプロバイダ（MSSP）に委託されることもある。MSSP の相関分析エンジンは、毎日記録される膨大な事象を処理して小さなサブセットにし、マニュアル操作で評価できるようにする。この機能を社内で果たしたい大企業向けに、相関分析エンジン製品が用意されている。セキュリティ情報・事象管理（SIEM）製品を利用して、IDS 及び IPS ログの事象のほか、他のコンピュータシステム、アプリケーション、インフラ装備品その他ハードウエア/ソフトウエアの監査ログを監視・分析・相関して、侵入のもくろみを検出している組織もある。

management (SIEM) products are used in some organizations to monitor, analyze, and correlate events from IDS and IPS logs, as well as audit logs from other computer systems, applications, infrastructure equipment, and other hardware and software, to look for intrusion attempts.

IDS and IPS vendors are developing and incorporating attack signatures for various ICS protocols such as Modbus, DNP3, and ICCP [58]. Snort rules have been developed for Modbus TCP, DNP3, and ICCP. Snort is an open source network intrusion detection and prevention system using a rule-driven language to perform signature, protocol, and anomaly-based inspections. Rules for DNP3 and Modbus protocols have also been added to the Bro IDS platform.

As with any software added to an ICS component, the addition of host IDS or IPS software could affect system performance. IPSs are commonplace in today's information security industry, but can be very resource intensive. These systems have the ability to automatically reconfigure systems if an intrusion attempt is identified. This automated and fast reaction is designed to prevent successful exploits; however, an automated tool such as this could be used by an adversary to adversely affect the operation on an ICS by shutting down segments of a network or server. False positives can also hinder ICS operation.

Malware/Antivirus Software

Because early malware threats were primarily viruses, the software to detect and remove malware has historically been called "antivirus software," even though it can detect many types of malware. Antivirus software is used to counter the threats of malware by evaluating files on a computer's storage devices (some tools also detect malware in real-time at the network perimeter and/or on the user's workstation) against an inventory of malware signature files. If one of the files on a computer matches the profile of known malware, the malware is removed through a disinfection process so it cannot infect other local files or communicate across a network to infect other files on other computers. There are also techniques available to identify unknown malware "in-the-wild" when a signature file is not yet available.

Many end-users and vendors of ICS are recommending the use of COTS antivirus software with their systems and have even developed installation and configuration guidance based on their own laboratory testing. Some ICS vendors recommend the use of antivirus software with their products, but offer little to no guidance. Some end users and vendors are hesitant to use antivirus software due to fears that its use would cause ICS performance problems or even failure. NIST and Sandia National Laboratories (SNL) conducted a study and produced a report aimed at helping ICS owners/operators to deploy antivirus software and to minimize and assess performance impacts of workstation and server-based antivirus products. This study assembled ICS-based antivirus knowledge and serves as a starting point or a secondary resource when installing, configuring, running, and maintaining antivirus software on an ICS [56]. In many cases, performance impacts can be reduced through configuration settings as well as antivirus scanning and maintenance scheduling outside of the antivirus software practices recommended for typical IT systems.

In summary, COTS antivirus software can be used successfully on most ICS components. However, special ICS specific considerations should be taken into account during the selection, installation, configuration, operational, and maintenance procedures. ICS end-users should consult with the ICS vendors regarding the use of antivirus software.

IDS 及び IPS ベンダーは、Modbus、DNP3 及び ICCP 等、種々の ICS プロトコルの攻撃シグネチャを作成し、組み込んでいる[58]。Modbus TCP、DNP3 及び ICCP 向けに Snort ルールが作成されている。Snort とはオープンソースネットワーク侵入検知防止システムのことで、ルールドリブン言語を使用して、シグネチャ、プロトコル及び異状を主体に検査を行う。DNP3 及び Modbus プロトコルのルールも Bro IDS プラットホームに追加されている。

ICS コンポーネントに追加される他のソフトウエアと同様、ホスト IDS 又は IPS ソフトウエアの追加は、システムパフォーマンスに影響することがある。IPSs は昨今の情報セキュリティ業界では普通に見られるが、極めて資源を消費する。これらのシステムでは、侵入のもくろみが検知されると、システム設定を自動的に変更する能力が備わっている。このような自動迅速対応は悪用を防止するためのものであるが、攻撃側に逆用され、ネットワークやサーバのセグメントを切断することにより、ICS 運用に悪影響が及ぶ場合がある。擬陽性によっても ICS 運用が阻害される。

マルウエア/アンチウイルスソフトウエア

初期のマルウエア脅威は主にウイルスであったため、マルウエア検出・排除ソフトウエアは、種々のマルウエアに対する検出能力を持つものの、従来「アンチウイルスソフトウエア」と呼ばれてきた。アンチウイルスソフトウエアは、マルウエアシグネチャファイルの目録に照らして、コンピュータのストレージデバイス上のファイルを評価し（ツールによってはネットワーク周辺又はユーザワークステーション上でリアルタイムにマルウエアを検出するものもある）、マルウエアの脅威に対抗する。コンピュータ上のファイルの 1 つが既知のマルウエアのプロファイルに一致すると、消毒プロセスを経てそのマルウエアは排除され、他のローカルファイルやネットワークを越えた他のコンピュータ上のファイルへの感染は生じなくなる。またシグネチャファイルがない場合でも、未知の「野生」マルウエアを識別する技術も利用できる。

多くの ICS エンドユーザ及びベンダーは、システムへの COTS アンチウイルスソフトウエアの導入を推奨しており、独自のラボ試験を基に、インストール・設定ガイダンスも作成している。ICS ベンダーによっては、自社製品にアンチウイルスソフトウエアの使用を推奨しているものの、ガイダンスが全く又はほとんど用意できていない場合もある。アンチウイルスソフトウエアの利用により、ICS のパフォーマンス問題や障害が発生するのを恐れて、使用に消極的なユーザやベンダーもいる。NIST とサンディア国立研究所（SNL）は調査を行い、ICS 保有者・操作員向けレポートを作成し、アンチウイルスソフトウエアの展開を助け、ワークステーション/サーバベースアンチウイルス製品のパフォーマンス影響を最小化し、評価する資としている。本研究により ICS ベースのアンチウイルス知見がまとまり、ICS へのアンチウイルスソフトウエアのインストール・設定・実行・保守を行う際の出発点又は二次リソースとなっている[56]。多くの場合、設定やアンチウイルススキャニング・保守スケジュールを、一般的な IT システムで推奨されているアンチウイルスソフトウエア規範を離れて実施することで、パフォーマンス影響を減らすことができる。

まとめとして、COTS アンチウイルスソフトウエアは、ほとんどの ICS コンポーネントで使用可能である。ただしその選定・インストール・設定・運用・保守手順に際しては、特殊な ICS 固有の考慮事項を検討に入れるべきである。ICS エンドユーザは、アンチウイルスソフトウエアの使用に関して、ICS ベンダーに相談すべきである。

Vulnerability Assessment Tools

There are many tools available for performing network vulnerability assessments for typical IT networks; however, the impacts these tools may have on the operation of an ICS should be carefully considered [77]. The additional traffic and exploits used during active vulnerability and penetration testing, combined with the limited resources of many ICS, have been known to cause ICS to malfunction. As guidance in this area, SNL developed a preferred list of vulnerability and penetration testing techniques for ICS [77]. These are less intrusive methods, passive instead of active, to collect the majority of information that is often queried by automated vulnerability and penetration testing tools. These methods are intended to allow collection of the necessary vulnerability information without the risk of causing a failure while testing.

Sophia is a patent-pending, passive, real-time diagnostic and security tool designed and built specifically for control systems professionals. Sophia builds and maintains an ICS network fingerprint and continuously monitors activity against it, with white, gray and black-listing capabilities, alerting its managers of any abnormal activity for further investigation, monitoring and/or action. Beta testing conducted by the Battelle Energy Alliance (BEA) at the Idaho National Laboratories (INL) recently concluded with a group of over 30 participants, including major utilities and control system vendors. Those Beta participants reported immediate benefits in the fingerprinting process and longer-term benefits in monitoring, securing, and making on-going modifications to ICS configurations during the Beta testing period. Beta participants, as well as non-participants, who have been following the development of Sophia by BEA/INL, have long expressed interest in obtaining commercial grade Sophia software, services and support. Beta testing has proven that this suite of tools offers unique capabilities, including visualization of activity and tailored reporting to meet customer needs.
Shodan is a search engine that lets you find specific types of computers (routers, servers, etc.) on the Internet using a variety of filters. Some have also described it as a search engine of service banners, which are meta-data the server sends back to the client. This can be information about the server software, what options the service supports, a welcome message or anything else that the client can find out before interacting with the server. Shodan users are able to find systems including traffic lights, security cameras, home heating systems as well as control systems. Users can use Shodan to determine if any of the devices on their ICS are accessible from the internet.

The Cyber Security Evaluation Tool (CSET) is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets. It was developed under the direction of the DHS Industrial Control System Cyber Emergency Response Team (ICS-CERT) by cybersecurity experts and with assistance from NIST. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems. CSET is a desktop software tool that guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cyber systems. The tool derives the recommendations from a database of cybersecurity standards, guidelines, and practices. Each recommendation is linked to a set of actions that can be applied to enhance cybersecurity controls. CSET has been designed for easy installation and use on a stand-alone laptop or workstation. It incorporates a variety of available standards from organizations such as NIST, NERC, TSA, DoD, and others. When the tool user selects one or more of the standards, CSET will open a set of questions to be answered. The answers to these questions will be compared against a selected security assurance level, and a detailed report will be generated to show areas for potential improvement. CSET provides an excellent means to perform a self-assessment of the security posture of your control system environment.

脆弱性評価ツール

一般的な IT ネットワークの脆弱性評価用ツールは多数あるが、これらが ICS の運用に及ぼす影響を慎重に検討すべきである[77]。多くの ICS のリソースを制限した、アクティブ脆弱性・ペネトレーション・テストにおいて、付加的なトラフィックや脆弱性の悪用があると、ICS に障害の出ることが分かっている。この分野でのガイダンスとして、SNL は ICS の好ましい脆弱性・ペネトレーション・テスト技術リストを作成した[77]。これらはより侵襲性の少ない方法で、アクティブというよりもパッシブであり、自動化脆弱性・ペネトレーション・テストツールから照会を受けることが多い情報の大半を収集できる。このような方法は、試験時に障害を発生させることなく、必要な脆弱性情報を収集できるようになっている。

Sophia は特許申請中のパッシブ、リアルタイム診断・セキュリティツールで、制御システム専門員用に設計・構築されている。ICS ネットワークフィンガープリントを生成して維持し、それに対する活動を常続的に監視する。ホワイトリスト、グレーリスト及びブラックリストの作成能力があり、詳細な調査・監視・行動を要する異常活動について管理者に警報を発する。アイダホ国立研究所（INL）において Battelle Energy Alliance（BEA）によるベータ試験が行われ、大手公共企業や制御システムベンダー等 30 を超えるグループが参加して、このほど終了した。
参加者は、フィンガープリント処理には当面の利益があり、ベータ試験期間中の ICS 設定の監視・セキュリティ確保・設定変更には長期的利益があると報告している。参加者のみならず、BEA/INL による Sophia の成り行きを注視してきた非参加者も、市販レベルの Sophia ソフトウエア、サービス及びサポートに関心を寄せている。ベータ試験により、このツールには活動の視覚化、顧客需要に合わせたカスタマイズ化報告等のユニークな機能があることが実証されている。

Shodan は検索エンジンで、種々のフィルタを使用して、インターネット上の特殊なコンピュータ（ルータ、サーバ等）を探し出すことができる。サーバがクライアントに送り返すメタデータである、サービスバナーの検索エンジンと評する向きもある。これはサーバソフトウエア、サービスの対応オプション、ウェルカムメッセージ、サーバとの相互作用を行う前にクライアントが検索できるその他についての情報となる。Shodan ユーザは信号機、セキュリティカメラ、家庭暖房システム、制御システム等のシステムを検索できる。これを利用すれば、インターネット経由でアクセス可能な ICS 上のデバイスを判別できる。

サイバーセキュリティ評価ツール(CSET)は、組織が国の重要サイバー資産を守るのを支援する国土安全保障省(DHS)の製品である。DHS 産業用制御システムサイバー緊急対応チーム(ICS-CERT)の指導下で、NIST の支援を得てサイバーセキュリティ専門家が開発した。サイバーシステム及びネットワークのセキュリティ状態を評価する際の体系的かつ反復的な取組が可能となる。あらゆる産業用制御及び IT システムに関係した高度の詳細な疑問に答えている。CSET はデスクトップソフトウエアツールで、制御システム及び情報技術ネットワークセキュリティ規範を、広く認められた業界基準に照らして、段階的に評価することができる。CSET により、組織の企業・産業用制御サイバーシステムのサイバーセキュリティ状態を改善するための優先的推奨事項リストを作成できる。このツールは、サイバーセキュリティ基準、ガイドライン及び規範データベースから推奨事項を導き出す。それぞれの推奨事項は、サイバーセキュリティ制御の拡張に適用可能な一連の行動に結びついている。CSET は、スタンドアローンラップトップやワークステーションに、簡単にインストールして利用できるようになっている。NIST、NERC、TSA、DoD その他の組織から入手可能な種々の基準が取りまとめてられている。ツールのユーザがこれら基準のいずれかを選択すると、一連の質問が提示される。質問への回答を、選択されたセキュリティ保証レベルと照らし合わせ、改善できる分野を示した詳細なレポートが作成されるようになっている。CSET は、制御システム環境のセキュリティ状態を自己評価できる優れた手段となる。

SamuraiSTFU is the Samurai Project's Security Testing Framework for Utilities and takes best in breed security tools for traditional network and web penetration testing and adds specialized tools for embedded and RF testing and mixes in energy sector context, documentation and sample files. It also includes emulators for SCADA, Smart Meters, and other types of energy sector systems to provide leverage for a full test lab.

ICS owners must make the individuals using vulnerability assessment tools aware of the criticality of continuous operation and the risks involved with performing these tests on operational systems. It may be possible to mitigate these risks by performing tests on ICS components such as redundant servers or independent test systems in a laboratory setting. Laboratory tests can be used to screen out test procedures that might harm the operational system. Even with very good configuration management to assure that the test system is highly representative, tests on the actual system are likely to uncover flaws not represented in the laboratory.

SamuraiSTFU は、ユーティリティ用サムライプロジェクトのセキュリティ試験体系で、伝統的なネットワーク/ウェブペネトレーション・テスト用セキュリティツールの最良のものを使用し、組込み/RF 試験用の特殊ツールを加え、エネルギー業界において文書とファイルを一体化する。また SCADA、スマートメーターその他エネルギー業界のシステム用エミュレータを組み込んで、全面試験ラボに弾みを付けている。

ICS 保有者は、脆弱性評価ツールを使用して、個々人が継続運用の重要性と、こうした試験を運用システムで行う場合のリスクを認識させなければならない。冗長サーバやラボ環境にある独立試験システム等の ICS コンポーネントで試験を行うことにより、このようなリスクを緩和することができる。ラボ試験を行えば、運用システムに有害な試験手順を排除できる。極めて良好な設定管理で試験システムが代表的なものになるようにしても、実際のシステムで行う試験は、ラボでは分からない欠陥を検出できることがある。

Appendix F—References

[1] Fraser, Roy E., *Process Measurement and Control:Introduction to Sensors, Communication, Adjustment, and Control*, Upper Saddle River, New Jersey:Prentice-Hall, Inc., 2001.

[2] Falco, Joe, et al., *IT Security for Industrial Control Systems*, NIST Internal Report (NISTIR) 6859, February 2002, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=821684 [accessed 4/16/15].

[3] Bailey, David, and Edwin Wright, *Practical SCADA for Industry*, Vancouver: IDC Technologies, 2003.

[4] Boyer, Stuart, *SCADA:Supervisory Control and Data Acquisition*.4th ed. Research Triangle Park, North Carolina:International Society of Automation, 2010.

[5] American Gas Association, AGA Report No. 12, *Cryptographic Protection of SCADA Communications, Part 1:Background, Policies and Test Plan*, September, March 14, 2006.

[6] Erickson, Kelvin, and John Hedrick, *Plantwide Process Control*, New York:John Wiley & Sons, Inc., 1999.

[7] Berge, Jonas, *Fieldbuses for Process Control:Engineering, Operation, and Maintenance*, Research Triangle Park, North Carolina:ISA, 2002.

[8] Peerenboom, James, "Infrastructure Interdependencies:Overview of Concepts and Terminology," invited paper, *NSF/OSTP Workshop on Critical Infrastructure:Needs in Interdisciplinary Research and Graduate Training*, Washington, D.C., June 14-15, 2001.

[9] Rinaldi, Steven, et al., "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, (December 2001), pp. 11-25, http://dx.doi.org/10.1109/37.969131.

[10] GAO-04-354, *Critical Infrastructure Protection:Challenges and Efforts to Secure Control Systems*, U.S. GAO, 2004, http://www.gao.gov/new.items/d04354.pdf.

[11] Weiss, Joseph, "Current Status of Cybersecurity of Control Systems," Presentation to Georgia Tech Protective Relay Conference, May 8, 2003.

[12] Keeney, Michelle et al., *Insider Threat Study:Computer System Sabotage in Critical Infrastructure Sectors*, United States Secret Service and Carnegie Mellon Software Institute, 2005, http://www.cert.org/archive/pdf/insidercross051105.pdf.

[13] Federal Information Security Management Act of 2002, Pub.L. 107-347 (Title III), 116 Stat 2946, http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf [accessed 4/16/15].

[14] Federal Information Security Management Act Implementation Project [Web site], http://csrc.nist.gov/groups/SMA/fisma/index.html [accessed 4/16/15].

[15] U.S. Department of Commerce, Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [accessed 4/16/15].

[16] U.S. Department of Commerce, Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf [accessed 4/16/15].

[17] Knapp, Eric, *Industrial Network Security:Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Waltham, Massachusetts:Syngress, 2011.

[18] U.S. Government Accountability Office (GAO), GAO-15-6, *Federal Facility Cybersecurity:DHS and GSA Should Address Cyber Risk to Building and Access Control Systems*, December 12, 2014, http://www.gao.gov/products/GAO-15-6 [accessed 4/16/15].

[19] Swanson, Marianne, et al., NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006, http://csrc.nist.gov/publications/PubsSPs.html#800-18 [accessed 4/16/15].

[20] Joint Task Force Transformation Initiative, NIST SP 800-39, *Managing Information Security Risk:Organization, Mission, and Information System View*, March 2011, http://csrc.nist.gov/publications/PubsSPs.html#800-39 [accessed 4/16/15].

[21] Joint Task Force Transformation Initiative, NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*, February 2010 (updated June 5, 2014), http://dx.doi.org/10.6028/NIST.SP.800-37r1.

[22] Joint Task Force Transformation Initiative, NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 22, 2015), http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[23] Joint Task Force Transformation Initiative, NIST SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations:Building Effective Security Assessment Plans*, December 2014 (updated December 18, 2014), http://dx.doi.org/10.6028/NIST.SP.800-53Ar4.

[24] Barker, William, NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003, http://csrc.nist.gov/publications/PubsSPs.html#800-59 [accessed 4/16/15].

[25] Stine, Kevin, et al., NIST SP 800-60 Revision 1 (2 vols.), *Guide for Mapping Types of Information and Information systems to Security Categories*, August 2008, http://csrc.nist.gov/publications/PubsSPs.html#800-60 [accessed 4/16/15].

[26] Quinn, Stephen, et al., NIST SP 800-70 Revision 2, *National Checklist Program for IT Products:Guidelines for Checklist Users and Developers*, February 2011, http://csrc.nist.gov/publications/PubsSPs.html#800-70 [accessed 4/16/15].

[27] Bowen, Pauline, et al., NIST SP 800-100, *Information Security Handbook:A Guide for Managers*, October 2006 (updated March 7, 2007), http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-100 [accessed 4/16/15].

[28] NIST Security Configurations Checklists Program for IT Products [Web site], http://web.nvd.nist.gov/view/ncp/repository [accessed 4/16/15].

[29] Stamp, Jason, et al., *Common Vulnerabilities in Critical Infrastructure Control Systems*, Sandia National Laboratories, 2003, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.132.3264&rep=rep1&type=pdf.

[30] *SCADA Security - Advice for CEOs*, IT Security Expert Advisory Group (ITSEAG)

[31] Franz, Matthew, *Vulnerability Testing of Industrial Network Devices*, Critical Infrastructure Assurance Group, Cisco Systems, 2003, http://blogfranz.googlecode.com/files/franz-isa-device-testing-oct03.pdf.

[32] Duggan, David, et al., *Penetration Testing of Industrial Control Systems*, Sandia National Laboratories, Report No SAND2005-2846P, 2005.

[33] President's Critical Infrastructure Protection Board, and U.S. Department of Energy, Office of Energy Assurance, *21 Steps to Improve Cybersecurity of SCADA Networks*, [2002], http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf [accessed 4/16/15].

[34] ISA-62443[multiple parts], *Security for Industrial Automation and Control Systems*, Research Triangle Park, North Carolina:International Society of Automation, http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx [accessed 4/16/15].

[35] Centre for the Protection of National Infrastructure (CPNI), *Firewall Deployment for SCADA and Process Control Networks:Good Practice Guide*, February 15, 2005, http://energy.gov/sites/prod/files/Good%20Practices%20Guide%20for%20Firewall%20Deployment.pdf [accessed 4/16/15].

[36] U.S. Department of Homeland Security, *Recommended Practice:Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*, October 2009, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf [accessed 4/16/15].

[37] Industrial Automation Open Networking Association (IAONA), *The IAONA Handbook for Network Security*, Version 1.3, 2005, http://www.iaona.org/pictures/files/1122888138-IAONA_HNS_1_3-reduced_050725.pdf [accessed 4/16/15].

[38] U.S. Department of Homeland Security, *Common Cybersecurity Vulnerabilities in Industrial Control Systems*, May 2011, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf [accessed 4/16/15].

[39] NIST SP 800-12, *An Introduction to Computer Security:The NIST Handbook*, 1995, http://csrc.nist.gov/publications/PubsSPs.html.

[40] Souppaya, Murugiah, and Karen Scarfone, NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*, July 2013, http://dx.doi.org/10.6028/NIST.SP.800-40r3.

[41] Scarfone, Karen, et al., NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-115 [accessed 4/16/15].

[42] Roback, Edward, NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/ Use of Tested/Evaluated Products*, August 2000, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-23 [accessed 4/16/15].

[43] Stoneburner, Gary, et al., NIST SP 800-27 Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-27A [accessed 4/16/15].

[44] Grance, Tim, et al., NIST SP 800-35, *Guide to Information Technology Security Services*, October 2003, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-35 [accessed 4/16/15].

[45] Grance, Tim, et al., NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, October 2003, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-36 [accessed 4/16/15].

[46] Grance, Tim, et al., NIST SP 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-64 [accessed 4/16/15].

[47] Hash, Joan, et al., NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, January 2005, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-65 [accessed 4/16/15].

[48] U.S. Department of Homeland Security, *Department of Homeland Security:Cyber Security Procurement Language for Control Systems*, September 2009 https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf [accessed 4/16/15].

[49] Dray, James, et al., NIST SP 800-73-3, *Interfaces for Personal Identity Verification* (4 parts), February 2010, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-73 [accessed 4/16/15].

[50] Grother, Patrick, et al., NIST SP 800-76-2, *Biometric Data Specification for Personal Identity Verification*, July 2013, http://dx.doi.org/10.6028/NIST.SP.800-76-2.

[51] Kuhn, D. Richard, et al., NIST SP 800-46 Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-46 [accessed 4/16/15].

[52] Swanson, Marianne, et al., NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-34 [accessed 4/16/15].

[53] Burr, William, et al., NIST SP 800-63-2, *Electronic Authentication Guideline*, August 2013, http://dx.doi.org/10.6028/NIST.SP.800-63-2.

[54] Bace, Rebecca, and Mell, Peter, NIST SP 800-31, *Intrusion Detection Systems*, 2001, http://csrc.nist.gov/publications/PubsSPs.html.

[55] Scarfone, Karen, and Peter Mell, NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-94 [accessed 4/16/15].

[56] Falco, Joe, et al., NIST SP 1058, *Using Host-based Anti-virus Software on Industrial Control Systems:Integration Guidance and a Test Methodology for Assessing Performance Impacts*, September 18, 2006, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=823596 [accessed 4/16/15].

[57] Peterson, Dale, "Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks," *ISA Automation West (AUTOWEST 2004)*, Long Beach, California, April 2004, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.121.3420&rep=rep1&type=pdf [accessed 4/16/15].

[58] Symantec Corporation, "Symantec Expands SCADA Protection for Electric Utilities," [press release], September 14, 2005, http://www.symantec.com/about/news/release/article.jsp?prid=20050914_01 [accessed 4/16/15].

[59] Grance, Tim, et al., NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*, August 2012, http://dx.doi.org/10.6028/NIST.SP.800-61r2.

[60] Mell, Peter, et al., NIST SP 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, July 2013, http://dx.doi.org/10.6028/NIST.SP.800-83r1.

[61] Wilson, Mark, and Joan Hash, NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-50 [accessed 4/16/15].

[62] Mix, S., *Supervisory Control and Data Acquisition (SCADA) Systems Security Guide*, Electric Power Research Institute (EPRI), 2003.

[63] Scarfone, Karen, et al., NIST SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, July 2008, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-48 [accessed 4/16/15].

[64] Frankel, Sheila, et al, NIST SP 800-97, *Establishing Wireless Robust Security Networks: a Guide to IEEE 802.11i*, February 2007, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-97 [accessed 4/16/15].

[65] U.S. Department of Commerce, Federal Information Processing Standards (FIPS) Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013, http://dx.doi.org/10.6028/NIST.FIPS.201-2.

[66] Dray, James, et al, NIST SP 800-96, *PIV Card to Reader Interoperability Guidelines*, September 2006, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-96 [accessed 4/16/15].

[67] Polk, W. Timothy, et al, NIST SP 800-78-3, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, December 2010, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-78 [accessed 4/16/15].

[68] Kent, Karen, and Murugiah Souppaya, NIST SP 800-92, *Guide to Computer Security Log Management*, September 2006, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-92 [accessed 4/16/15].

[69] Jansen, Wayne, et al., NIST SP 800-28 Version 2, *Guidelines on Active Content and Mobile Code*, March 2008, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-28 [accessed 4/16/15].

[70] Polk, Tim, et al., NIST SP 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, April 2014, http://dx.doi.org/10.6028/NIST.SP.800-52r1.

[71] Barker, Elaine, et al., NIST SP 800-56A Revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, May 2013, http://dx.doi.org/10.6028/NIST.SP.800-56Ar2.

[72] Baker, Elaine, et al., NIST SP 800-57 (3 parts), *Recommendation for Key Management*:Part 1 Revision 3, *General*, July 2012 http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-57pt1; Part 2, *Best Practices for Key Management Organization*, August 2005, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-57pt2; Part 3 Revision 1, *Application-Specific Key Management Guidance*, January 2015, http://dx.doi.org/10.6028/NIST.SP.800-57pt3r1.

[73] Kuhn, D. Richard, et al., NIST SP 800-58, *Security Considerations for Voice Over IP Systems*, January 2005, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-58 [accessed 4/16/15].

[74] Frankel, Sheila, et al., NIST SP 800-77, *Guide to IPsec VPNs*, December 2005, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-77 [accessed 4/16/15].

[75] Shirey, R., *Internet Security Glossary, Version 2*, RFC 4949, August 2007, http://www.rfc-editor.org/rfc/rfc4949.txt [accessed 4/16/15].

[76] Franz, Matthew, and Venkat Pothamsetty, *ModbusFW:Deep Packet Inspection for Industrial Ethernet*, Critical Infrastructure Assurance Group, Cisco Systems, 2004, http://blogfranz.googlecode.com/files/franz-niscc-modbusfw-may04.pdf [accessed 4/16/15].

[77] Duggan, David, *Penetration Testing of Industrial Control Systems*, SAND2005-2846P, Sandia National Laboratories, March 2005, http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2005_2846p.pdf [accessed 4/16/15].

[78] Kissel, Richard, et al., NIST SP 800-88 Revision 1, *Guidelines for Media Sanitization*, December 2014, http://dx.doi.org/10.6028/NIST.SP.800-88r1.

[79] Joint Task Force Transformation Initiative, NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, September 2012, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-30 [accessed 4/16/15].

[80] Johnson, Arnold, et al., NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-128 [accessed 4/16/15].

[81] Dempsey, Kelley, et al., NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011, http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-137 [accessed 4/16/15].

[82] Waltermire, David, et al., NIST SP 800-126 Revision 2, *The Technical Specification for the Security Content Automation Protocol (SCAP):SCAP Version 1.2*, September 2011 (updated March 19, 2012), http://csrc.nist.gov/publications/PubsSPs.htmlhttp://csrc.nist.gov/publications/PubsSPs.html#800-126-rev2 [accessed 4/16/15].

[83] Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf [accessed 4/16/15].

[84] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.0, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf [accessed 4/16/15].

[85] Scarfone, Karen, and Paul Hoffman, NIST SP 800-41 Revision 1, *Guidelines on Firewalls and Firewall Policy*, September 2009, http://csrc.nist.gov/publications/PubsSPs.html#800-41 [accessed 4/16/15].

[86] Office of Management and Budget, OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf [accessed 4/16/15].

[87] Office of Management and Budget, OMB Memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, June 25, 2010, https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf [accessed 4/16/15].

[88] McCallister, Erika, et al., NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010, http://csrc.nist.gov/publications/PubsSPs.html#800-122 [accessed 4/16/15].

[89] *Federal Enterprise Architecture Security and Privacy Profile, Version 3.0*, September 2010, https://cio.gov/wp-content/uploads/downloads/2012/09/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf [accessed 4/16/15].

[90] U.S. Department of Commerce, Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001 (Change Notice 2, 12/3/2002), http://csrc.nist.gov/publications/PubsFIPS.html#140-2 [accessed 4/16/15].

[91] Tracy, Miles, et al., NIST SP 800-45 Version 2, Guidelines on Electronic Mail Security, February 2007, http://csrc.nist.gov/publications/PubsSPs.html#800-45 [accessed 4/16/15].

[92] Grance, Tim, et al., NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002, http://csrc.nist.gov/publications/PubsSPs.html#800-47 [accessed 4/16/15].

[93] Kent, Karen, et al., NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response, August 2006, http://csrc.nist.gov/publications/PubsSPs.html#800-86 [accessed 4/16/15].

[94] Scarfone, Karen, et al., NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices, November 2007, http://csrc.nist.gov/publications/PubsSPs.html#800-111 [accessed 4/16/15].

[95] Scarfone, Karen, et al., NIST SP 800-123, Guide to General Server Security, July 2008, http://csrc.nist.gov/publications/PubsSPs.html#800-123 [accessed 4/16/15].

[96] Scarfone, Karen, et al., NIST SP 800-127, Guide to Securing WiMAX Wireless Communications, September 2010, http://csrc.nist.gov/publications/PubsSPs.html#800-127 [accessed 4/16/15].

[97] Johnson, Arnold, et al., NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, August 2011, http://csrc.nist.gov/publications/PubsSPs.html#800-128 [accessed 4/16/15].

[98] Smart Grid Interoperability Panel, Smart Grid Cybersecurity Committee, NISTIR 7628 Revision 1, Guidelines for Smart Grid Cybersecurity, September 2014, http://dx.doi.org/10.6028/NIST.IR.7628r1 [accessed 4/16/15].

[99] Kissel, Richard (ed.), NISTIR 7298 Revision 2, Glossary of Key Information Security Terms, May 2013, http://dx.doi.org/10.6028/NIST.IR.7298r2 [accessed 4/16/15].

Appendix G—ICS Overlay

NOTE TO READERS

The ICS overlay is a partial tailoring of the controls and control baselines in SP 800-53, Revision 4, and adds supplementary guidance specific to ICS. The concept of overlays is introduced in Appendix I of SP 800-53, Revision 4. The ICS overlay is intended to be applicable to all ICS systems in all industrial sectors. Further tailoring can be performed to add specificity to a particular sector (e.g., pipeline, energy). Ultimately, an overlay may be produced for a specific system (e.g., the XYZ company). This ICS overlay constitutes supplemental guidance and tailoring for SP 800-53, Revision 4. Please be sure you are looking at the correct version of SP 800-53. Duplicating Appendix F of SP 800-53 would increase the size of this Appendix by over 65 pages. Therefore, the drafting committee has decided to not duplicate Appendix F. The reader should have SP 800-53, Revision 4 available. The authoring team also considered that this ICS overlay may serve as a model for other overlays. Feedback on this Appendix's structure would be appreciated, especially in the following areas: the level of abstraction and whether the examples provided in the supplemental guidance are sufficient/beneficial for implementation.

Since the ICS overlay exists in the context of SP 800-53, Revision 4, it is important to review that context. SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, represents the most comprehensive update to the security controls catalog since its inception in 2005. This update was motivated principally by the expanding threat space—characterized by the increasing sophistication of cyber attacks and the operations tempo of adversaries (i.e., the frequency of such attacks, the professionalism of the attackers, and the persistence of targeting by attackers). State-of-the-practice security controls and control enhancements have been developed and integrated into the catalog addressing such areas as: mobile and cloud computing; applications security; trustworthiness, assurance, and resiliency of information systems; insider threat; supply chain security; and the advanced persistent threat.

To take advantage of the expanded set of security and privacy controls, and to give organizations greater flexibility and agility in defending their information systems, the concept of overlays was introduced in this revision. Overlays provide a structured approach to help organizations tailor security control baselines and develop specialized security plans that can be applied to specific missions/business functions, environments of operation, and/or technologies. This specialization approach is important as the number of threat-driven controls and control enhancements in the catalog increases and organizations develop risk management strategies to address their specific protection needs within defined risk tolerances.

付録 G　ICS オーバーレイ

読者への注記

ICS オーバーレイは、SP 800-53 第 4 版に示される制御及び制御ベースラインを部分的にカスタマイズしたもので、ICS に特化した補足ガイダンスとなる。オーバーレイの概念は SP 800-53 第 4 版の付録 I に説明がある。ICS オーバーレイは、あらゆる産業界のあらゆる ICS システムに適用するようにできている。更にカスタマイズして、特定の業界向けにすることもできる（パイプライン、エネルギー等）。最終的には、1 つのオーバーレイを 1 つのシステム用に作成できる（XYZ 社用等）。ICS オーバーレイは、SP 800-53 第 4 版の補足ガイダンスカスタマイズ版となる。該当する SP 800-53 を使用するよう留意されたい。SP 800-53 の付録 F を再録すると、紙数が 65 ページ増えることになるので、起案委員会は複写しないことにした。読者は SP 800-53 第 4 版を手許に置くようにすべきである。また執筆チームは、この ICS オーバーレイが他のオーバーレイのひな形となるようにした。付録の構成、特に概念化のレベル及び補足ガイダンスの提示例は、実装上十分で役立つかどうかについて、フィードバックをいただければ幸いである。

ICS オーバーレイは、SP 800-53 第 4 版の文脈に沿って存在しているため、その文脈を見直すことは肝要である。SP 800-53 第 4 版の連邦情報システム・組織のセキュリティ・プライバシー管理には、2005 年の概念化以来のセキュリティ対策カタログに対する包括的な更新内容が示されている。更新は、サイバー攻撃がますます巧妙化し、脅威が拡大していることが主な理由である（攻撃の頻度、攻撃側の専門化、標的に対する執拗性等）。実用に供されるセキュリティ対策や管理拡張は、進展を遂げ、次の分野のカタログに組み込まれている。モバイル/クラウドコンピューティング。アプリケーションセキュリティ。情報システムの信頼性・保証・弾力性。インサイダー脅威。サプライチェーンセキュリティ。最新の持続的脅威。

拡張されたセキュリティ/プライバシー管理を利用し、情報システムを守るための柔軟性と機敏性を組織に増し加えるため、オーバーレイ概念がこの版に導入された。オーバーレイは系統立った取組で、組織がセキュリティ対策のベースラインを微調整し、固有の任務・事業機能、運用環境又は技術に適用可能な独自のセキュリティ計画書を作成するのを支援する。脅威に対応したカタログの管理及びその拡張件数が増えており、各組織はリスク管理戦略を作成し、固有の保護ニーズを規定のリスクトレランス内で取り上げているため、この独自化に向けた取組は肝要である。

Identification

This overlay may be referenced as the NIST Special Publication 800-82 Revision 2 Industrial Control System Overlay ("NIST SP 800-82 Rev 2 ICS Overlay"). It is based on NIST SP 800-53 Revision 4 [22].

NIST developed this overlay in furtherance of its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283), Presidential Policy Directive (PPD)-21 and Executive Order 13636. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. Comments may be directed to icsoverlaycomments@nist.gov.

Overlay Characteristics

Industrial Control Systems (ICS) are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods). Supervisory control and data acquisition (SCADA) systems are generally used to control dispersed assets using centralized data acquisition and supervisory control. Distributed Control Systems (DCS) are generally used to control production systems within a local area such as a factory using supervisory and regulatory control. Programmable Logic Controllers (PLCs) are generally used for discrete control for specific applications and generally provide regulatory control. These control systems are vital to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems. It is important to note that approximately 90 percent of the nation's critical infrastructures are privately owned and operated. Federal agencies also operate many of the ICS mentioned above; other examples include air traffic control and materials handling (e.g., Postal Service mail handling.)

Applicability

The purpose of this overlay is to provide guidance for securing ICS, including SCADA and DCS systems, PLCs, and other systems performing industrial control functions. This overlay has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis.

Overlay Summary

Table G-1 provides a summary of the security controls and control enhancements from NIST SP 800-53 Appendix F [22, App. F] that have been allocated to the initial security control baselines (i.e., Low, Moderate, and High) along with indications of ICS Supplemental Guidance and ICS tailoring. Controls and control enhancements for which there is ICS Supplemental Guidance are **bolded**. If the control baselines are supplemented by the addition of a control to the baseline, the control or control enhancement is underlined. If a control or control enhancement is removed from the baseline, the control or control enhancement is ~~struck-out~~.

Example:

AU-4	Audit Storage Capacity	AU-4 **(1)**	AU-4 **(1)**	AU-4 **(1)**

In this example, ICS Supplemental Guidance was added to Control Enhancement 1 of AU-4 (bolded). In addition, Control Enhancement 1 of AU-4 was added to the Low, Moderate (Mod), and High baselines (underlined).

識別

このオーバーレイは NIST SP 800-82 第 2 版産業用制御システムオーバーレイ(『NIST SP 800-82 第 2 版 ICS オーバーレイ』)と呼ばれることがある。これは NIST SP 800-53 第 4 版[22]に基づいている。

NIST は、2014 年連邦情報強化法(FISMA)(Public Law 113-283)、大統領政策指示(PPD)-21 及び大統領命令 13636 に従い、その法的責務を推進するためにこのオーバーレイを作成した。NIST はあらゆる政府機関業務・資産の情報セキュリティを確保するため、最低要件等を含んだ規格及びガイドラインの作成を担当しているが、このような規格及びガイドラインは、このようなシステムに対する施策権限を持った連邦行政官の明確な承認がなければ、国のセキュリティシステムには適用されない。意見は次宛に寄せられたい。icsoverlaycomments@nist.gov.

オーバーレイの特徴

産業用制御システム（ICS）は一般的に電気、上下水、石油・ガス、輸送、化学、医薬品、パルプ・製紙、食品・飲料及び組立製造（自動車、航空宇宙、耐久消費財等）業界で利用されている。SCADA は、通常、集中データ取得監視制御により、分散化された資産を制御するために使用する。DCS は、通常、ローカルエリア内にある工場等の生産システムを、監視・規制制御により制御するために使用する。プログラマブル論理コントローラ（PLC）は、通常、特殊用途での離散制御に使用し、規制制御を通常行う。このような制御システムは、高度に連携・相互依存したシステムとなる、米国の重要インフラの運営に緊要な役割を果たしている。国の重要インフラのおよそ 90%は、私企業が保有し運営している点を銘記するのは肝要である。連邦政府機関も前述の ICS の多くを運営しているが、そのほかにも航空交通管制や物流処理（港湾業務、郵便等）などがある。

適用性

このオーバーレイの目的は、SCADA システム、DCS システム、PLC その他産業用制御機能をつかさどるシステム等、ICS のセキュリティを確保するためのガイダンスとなる。連邦政府機関向けに準備されている。非政府組織が自主的に利用してもかまわない。

オーバーレイのまとめ

表 G-1 は、NIST SP 800-53 付録 F[22, App. F]のセキュリティ対策及び管理拡張をまとめたものである。管理拡張は、当初のセキュリティ対策ベースライン（低・中・高）に、ICS 補足ガイダンス及び ICS のカスタマイズとともに割り当てられたものである。ICS 補足ガイダンスのある管理及び管理拡張は**太字**になっている。対策ベースラインに補足管理が追加されている場合、管理及び管理拡張に下線が付いている。管理及び管理拡張がベースラインから削除されている場合、~~線で消されている。~~

例

AU-4	監査ストレージ容量	AU-4 **(1)**	AU-4 **(1)**	AU-4 **(1)**

この例では、ICS 補足ガイダンスが管理拡張 AU-4 の 1（太字）に追加されている。また、管理拡張 AU-4 の 1 が低・中・高ベースラインに追加されている（下線）。

Table G-1 Security Control Baselines

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
AC-1	Access Control Policy and Procedures	**AC-1**	**AC-1**	**AC-1**
AC-2	Account Management	**AC-2**	**AC-2 (1) (2) (3) (4)**	**AC-2 (1) (2) (3) (4) (5)** (11) (12) (13)
AC-3	Access Enforcement	**AC-3**	**AC-3**	**AC-3**
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	**AC-5**	**AC-5**
AC-6	Least Privilege	Not Selected	**AC-6 (1) (2) (5) (9) (10)**	**AC-6 (1) (2) (3) (5) (9) (10)**
AC-7	Unsuccessful Logon Attempts	**AC-7**	**AC-7**	**AC-7**
AC-8	System Use Notification	**AC-8**	**AC-8**	**AC-8**
AC-10	Concurrent Session Control	Not Selected	Not Selected	**AC-10**
AC-11	Session Lock	Not Selected	**AC-11 (1)**	**AC-11 (1)**
AC-12	Session Termination	Not Selected	**AC-12**	**AC-12**
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14	AC-14
AC-17	Remote Access	**AC-17**	**AC-17 (1) (2) (3) (4)**	**AC-17 (1) (2) (3) (4)**
AC-18	Wireless Access	**AC-18**	**AC-18 (1)**	**AC-18 (1) (4)** (5)
AC-19	Access Control for Mobile Devices	**AC-19**	**AC-19** (5)	**AC-19** (5)
AC-20	Use of External Information Systems	**AC-20**	**AC-20** (1) (2)	**AC-20** (1) (2)
AC-21	Collaboration and Information Sharing	**AC-21**	**AC-21**	**AC-21**
AC-22	Publicly Accessible Content	**AC-22**	**AC-22**	**AC-22**
AT-1	Security Awareness and Training Policy and Procedures	**AT-1**	**AT-1**	**AT-1**
AT-2	Security Awareness Training	**AT-2**	**AT-2** (2)	**AT-2** (2)
AT-3	Role-Based Security Training	**AT-3**	**AT-3**	**AT-3**
AT-4	Security Training Records	AT-4	AT-4	AT-4
AU-1	Audit and Accountability Policy and Procedures	**AU-1**	**AU-1**	**AU-1**
AU-2	Audit Events	**AU-2**	**AU-2** (3)	**AU-2** (3)
AU-3	Content of Audit Records	**AU-3**	**AU-3** (1)	**AU-3** (1) (2)
AU-4	Audit Storage Capacity	AU-4 **(1)**	AU-4 **(1)**	AU-4 **(1)**
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	AU-6	AU-6 **(1)** (3)	AU-6 **(1)** (3) (5) (6)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	**AU-8**	**AU-8 (1)**	**AU-8 (1)**
AU-9	Protection of Audit Information	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Non-repudiation	Not Selected	Not Selected	**AU-10**
AU-11	Audit Record Retention	AU-11	AU-11	AU-11

表 G-1　セキュリティ対策ベースライン

管理番号	管理名	当初の対策ベースライン		
		低	中	高
AC-1	アクセス制御ポリシー・手順	**AC-1**	**AC-1**	**AC-1**
AC-2	アカウント管理	**AC-2**	**AC-2 (1) (2) (3) (4)**	**AC-2 (1) (2) (3) (4) (5)** (11) (12) (13)
AC-3	アクセス施行	**AC-3**	**AC-3**	**AC-3**
AC-4	情報フロー施行	未選択	AC-4	AC-4
AC-5	任務の分割	未選択	**AC-5**	**AC-5**
AC-6	最小権限	未選択	**AC-6 (1) (2) (5) (9) (10)**	**AC-6 (1) (2) (3) (5) (9) (10)**
AC-7	ログイン失敗	**AC-7**	**AC-7**	**AC-7**
AC-8	システム利用通知	**AC-8**	**AC-8**	**AC-8**
AC-10	現行セッション管理	未選択	未選択	**AC-10**
AC-11	セッションロック	未選択	**AC-11 (1)**	**AC-11 (1)**
AC-12	セッション終了	未選択	**AC-12**	**AC-12**
AC-14	識別・認証のない許可済み行為	AC-14	AC-14	AC-14
AC-17	リモートアクセス	**AC-17**	**AC-17 (1) (2) (3) (4)**	**AC-17 (1) (2) (3) (4)**
AC-18	ワイヤレスアクセス	**AC-18**	**AC-18 (1)**	**AC-18 (1) (4)** (5)
AC-19	モバイルデバイス用アクセス制御	**AC-19**	**AC-19** (5)	**AC-19** (5)
AC-20	外部情報システムの利用	**AC-20**	**AC-20** (1) (2)	**AC-20** (1) (2)
AC-21	連携・情報共有	**AC-21**	**AC-21**	**AC-21**
AC-22	公開コンテンツ	**AC-22**	**AC-22**	**AC-22**
AT-1	セキュリティ意識・訓練ポリシー・手順	**AT-1**	**AT-1**	**AT-1**
AT-2	セキュリティ意識訓練	**AT-2**	**AT-2** (2)	**AT-2** (2)
AT-3	役割ベースセキュリティ訓練	**AT-3**	**AT-3**	**AT-3**
AT-4	セキュリティ訓練記録	AT-4	AT-4	AT-4
AU-1	監査・説明責任ポリシー・手順	**AU-1**	**AU-1**	**AU-1**
AU-2	監査事象	**AU-2**	**AU-2** (3)	**AU-2** (3)
AU-3	監査記録内容	**AU-3**	**AU-3** (1)	**AU-3** (1) (2)
AU-4	監査ストレージ容量	AU-4 **(1)**	AU-4 **(1)**	AU-4 **(1)**
AU-5	監査処理不備への対応	AU-5	AU-5	AU-5 (1) (2)
AU-6	監査の審査・分析・報告	AU-6	AU-6 **(1)** (3)	AU-6 **(1)** (3) (5) (6)
AU-7	監査削減・報告書作成	未選択	AU-7 (1)	AU-7 (1)
AU-8	タイムスタンプ	**AU-8**	**AU-8 (1)**	**AU-8 (1)**
AU-9	監査情報の保護	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	否認防止	未選択	未選択	**AU-10**
AU-11	監査記録保留	AU-11	AU-11	AU-11

AU-12	Audit Generation	AU-12	AU-12	AU-12 **(1) (3)**
CA-1	Security Assessment and Authorization Policies and Procedures	**CA-1**	**CA-1**	**CA-1**
CA-2	Security Assessments	**CA-2**	**CA-2** (1)	**CA-2** (1) **(2)**
CA-3	System Interconnections	**CA-3**	**CA-3** (5)	**CA-3** (5)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Authorization	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	**CA-7**	**CA-7** (1)	**CA-7** (1)
CA-8	Penetration Testing	Not Selected	Not Selected	**CA-8**
CA-9	Internal System Connections	**CA-9**	**CA-9**	**CA-9**
CM-1	Configuration Management Policy and Procedures	**CM-1**	**CM-1**	**CM-1**
CM-2	Baseline Configuration	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	**CM-4**	**CM-4**	**CM-4** (1)
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 **(1) (2) (3)**
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	**CM-7 (1)**	**CM-7** (1) (2) ~~(4)~~ (5)	**CM-7** (1) (2) (5)
CM-8	Information System Component Inventory	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	**CM-10**	**CM-10**	**CM-10**
CM-11	User-Installed Software	CM-11	CM-11	CM-11
CP-1	Contingency Planning Policy and Procedures	**CP-1**	**CP-1**	**CP-1**
CP-2	Contingency Plan	**CP-2**	**CP-2 (1) (3) (8)**	**CP-2 (1) (2) (3) (4) (5) (8)**
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	**CP-8** (1) (2)	**CP-8** (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	Information System Recovery and Reconstitution	**CP-10**	**CP-10** (2)	**CP-10** (2) (4)
CP-12	Safe Mode	**CP-12**	**CP-12**	**CP-12**
IA-1	Identification and Authentication Policy and Procedures	**IA-1**	**IA-1**	**IA-1**
IA-2	Identification and Authentication (Organizational Users)	**IA-2 (1) (12)**	**IA-2 (1) (2) (3) (8)** (11) **(12)**	**IA-2 (1) (2) (3) (4) (8) (9)** (11) **(12)**
IA-3	Device Identification and Authentication	**IA-3**	**IA-3 (1) (4)**	**IA-3 (1) (4)**
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	**IA-5** (1) (11)	**IA-5** (1) (2) (3) (11)	**IA-5** (1) (2) (3) (11)

AU-12	監査作成	AU-12	AU-12	AU-12 **(1) (3)**
CA-1	セキュリティ評価・権限付与ポリシー・手順	**CA-1**	**CA-1**	**CA-1**
CA-2	セキュリティ評価	**CA-2**	**CA-2** (1)	**CA-2** (1) **(2)**
CA-3	システム相互連接	**CA-3**	**CA-3** (5)	**CA-3** (5)
CA-5	行動・マイルストーン計画書	CA-5	CA-5	CA-5
CA-6	セキュリティ権限	CA-6	CA-6	CA-6
CA-7	継続監視	**CA-7**	**CA-7** (1)	**CA-7** (1)
CA-8	ペネトレーション・テスト	未選択	未選択	**CA-8**
CA-9	内部システム接続	**CA-9**	**CA-9**	**CA-9**
CM-1	設定管理ポリシー・手順	**CM-1**	**CM-1**	**CM-1**
CM-2	ベースライン設定	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	設定変更管理	未選択	CM-3 (2)	CM-3 (1) (2)
CM-4	接続影響分析	**CM-4**	**CM-4**	**CM-4** (1)
CM-5	変更用アクセス制限	未選択	CM-5	CM-5 **(1) (2) (3)**
CM-6	構成設定	CM-6	CM-6	CM-6 (1) (2)
CM-7	最低限機能	**CM-7 (1)**	**CM-7** (1) (2) ~~(4)~~ (5)	**CM-7** (1) (2) (5)
CM-8	情報システムコンポーネント目録	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	設定管理計画書	未選択	CM-9	CM-9
CM-10	ソフトウエア使用制限	**CM-10**	**CM-10**	**CM-10**
CM-11	ユーザがインストールしたソフトウエア	CM-11	CM-11	CM-11
CP-1	不測事態計画ポリシー・手順	**CP-1**	**CP-1**	**CP-1**
CP-2	緊急時対応計画	**CP-2**	**CP-2 (1) (3) (8)**	**CP-2 (1) (2) (3) (4) (5) (8)**
CP-3	不測事態訓練	CP-3	CP-3	CP-3 (1)
CP-4	緊急時対応計画訓練	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-6	代替ストレージサイト	未選択	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	代替処理サイト	未選択	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	電気通信サービス	未選択	**CP-8** (1) (2)	**CP-8** (1) (2) (3) (4)
CP-9	情報システムバックアップ	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	情報システムの復旧・再構築	**CP-10**	CP-10 (2)	**CP-10** (2) (4)
CP-12	セーフモード	**CP-12**	**CP-12**	**CP-12**
IA-1	識別・認証ポリシー・手順	**IA-1**	**IA-1**	**IA-1**
IA-2	識別・認証（組織ユーザ）	**IA-2 (1) (12)**	**IA-2 (1) (2) (3) (8)** (11) **(12)**	**IA-2 (1) (2) (3) (4) (8) (9)** (11) **(12)**
IA-3	デバイス識別・認証	**IA-3**	**IA-3 (1) (4)**	**IA-3 (1) (4)**
IA-4	識別子管理	IA-4	IA-4	IA-4
IA-5	認証コード管理	**IA-5** (1) (11)	**IA-5** (1) (2) (3) (11)	**IA-5** (1) (2) (3) (11)

IA-6	Authenticator Feedback	**IA-6**	**IA-6**	**IA-6**
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	**IA-8 (1) (2) (3) (4)**	**IA-8 (1) (2) (3) (4)**	**IA-8 (1) (2) (3) (4)**
IR-1	Incident Response Policy and Procedures	**IR-1**	**IR-1**	**IR-1**
IR-2	Incident Response Training	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing	Not Selected	IR-3 (2)	IR-3 (2)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	Incident Monitoring	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	**IR-6**	**IR-6 (1)**	**IR-6 (1)**
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	IR-8	IR-8	IR-8
MA-1	System Maintenance Policy and Procedures	**MA-1**	**MA-1**	**MA-1**
MA-2	Controlled Maintenance	MA-2	MA-2	MA-2 (2)
MA-3	Maintenance Tools	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Nonlocal Maintenance	MA-4	MA-4 (2)	MA-4 (2) **(3)**
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5 (1)
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6
MP-1	Media Protection Policy and Procedures	**MP-1**	**MP-1**	**MP-1**
MP-2	Media Access	MP-2	MP-2	MP-2
MP-3	Media Marking	Not Selected	MP-3	MP-3
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (4)	MP-5 (4)
MP-6	Media Sanitization	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	Media Use	MP-7	MP-7 (1)	MP-7 (1)
PE-1	Physical and Environmental Protection Policy and Procedures	**PE-1**	**PE-1**	**PE-1**
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	Not Selected	PE-4	PE-4
PE-5	Access Control for Output Devices	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	**PE-6**	**PE-6** (1) **(4)**	**PE-6** (1) **(4)**
PE-8	Visitor Access Records	PE-8	PE-8	PE-8 (1)
PE-9	Power Equipment and Cabling	Not Selected	PE-9 (1)	PE-9 (1)
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10
PE-11	Emergency Power	PE-11 (1)	PE-11 (1)	PE-11 (1) (2)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	**PE-13**	**PE-13** (3)	**PE-13** (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	**PE-15**	**PE-15**	**PE-15** (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	Not Selected	PE-18
PL-1	Security Planning Policy and Procedures	**PL-1**	**PL-1**	**PL-1**
PL-2	System Security Plan	PL-2 (3)	PL-2 (3)	PL-2 (3)
PL-4	Rules of Behavior	PL-4	PL-4 (1)	PL-4 (1)
PL-7	Security Concept of Operations		PL-7	PL-7

IA-6	認証フィードバック	**IA-6**	**IA-6**	**IA-6**
IA-7	暗号化モジュール認証	IA-7	IA-7	IA-7
IA-8	識別・認証（組織外ユーザ）	**IA-8 (1) (2) (3) (4)**	**IA-8 (1) (2) (3) (4)**	**IA-8 (1) (2) (3) (4)**
IR-1	インシデント対応ポリシー・手順	**IR-1**	**IR-1**	**IR-1**
IR-2	インシデント対応訓練	IR-2	IR-2	IR-2 (1) (2)
IR-3	インシデント対応試験	未選択	IR-3 (2)	IR-3 (2)
IR-4	インシデント処理	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	インシデント監視	IR-5	IR-5	IR-5 (1)
IR-6	インシデント報告	**IR-6**	**IR-6 (1)**	**IR-6 (1)**
IR-7	インシデント対応支援	IR-7	IR-7 (1)	IR-7 (1)
IR-8	インシデント対応計画書	IR-8	IR-8	IR-8
MA-1	システム保守ポリシー・手順	**MA-1**	**MA-1**	**MA-1**
MA-2	管理保守	MA-2	MA-2	MA-2 (2)
MA-3	保守ツール	未選択	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	ローカル以外の保守	MA-4	MA-4 (2)	MA-4 (2) **(3)**
MA-5	保守要員	MA-5	MA-5	MA-5 (1)
MA-6	適時的保守	未選択	MA-6	MA-6
MP-1	メディア保護ポリシー・手順	**MP-1**	**MP-1**	**MP-1**
MP-2	メディアアクセス	MP-2	MP-2	MP-2
MP-3	メディアマーキング	未選択	MP-3	MP-3
MP-4	メディアストレージ	未選択	MP-4	MP-4
MP-5	メディア転送	未選択	MP-5 (4)	MP-5 (4)
MP-6	メディアサニタイズ	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	メディア利用	MP-7	MP-7 (1)	MP-7 (1)
PE-1	物理環境保護ポリシー・手順	**PE-1**	**PE-1**	**PE-1**
PE-2	物理的アクセス権限	PE-2	PE-2	PE-2
PE-3	物理的アクセス制御	PE-3	PE-3	PE-3 (1)
PE-4	通信メディアのアクセス制御	未選択	PE-4	PE-4
PE-5	出力デバイスのアクセス制御	未選択	PE-5	PE-5
PE-6	物理的アクセス監視	**PE-6**	**PE-6** (1) **(4)**	**PE-6** (1) **(4)**
PE-8	来訪者立入記録	PE-8	PE-8	PE-8 (1)
PE-9	電気装置及び配線	未選択	PE-9 (1)	PE-9 (1)
PE-10	緊急遮断	未選択	PE-10	PE-10
PE-11	緊急電源	PE-11 (1)	PE-11 (1)	PE-11 (1) (2)
PE-12	緊急照明	PE-12	PE-12	PE-12
PE-13	防火	**PE-13**	PE-13 (3)	**PE-13** (1) (2) (3)
PE-14	温度・湿度制御	PE-14	PE-14	PE-14
PE-15	水害防護	**PE-15**	**PE-15**	PE-15 (1)
PE-16	配送・撤去	PE-16	PE-16	PE-16
PE-17	代替作業場	未選択	PE-17	PE-17
PE-18	情報システムコンポーネントの場所	未選択	未選択	PE-18
PL-1	セキュリティ計画ポリシー・手順	**PL-1**	**PL-1**	**PL-1**
PL-2	システムセキュリティ計画書	PL-2 (3)	PL-2 (3)	PL-2 (3)
PL-4	行動規則	PL-4	PL-4 (1)	PL-4 (1)
PL-7	運用セキュリティ概念		PL-7	PL-7

PL-8	Information Security Architecture	Not Selected	PL-8	PL-8
PS-1	Personnel Security Policy and Procedures	**PS-1**	**PS-1**	**PS-1**
PS-2	Position Risk Designation	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4 (2)
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
RA-1	Risk Assessment Policy and Procedures	**RA-1**	**RA-1**	**RA-1**
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-5	Vulnerability Scanning	**RA-5**	**RA-5** (1) (2) (5)	**RA-5** (1) (2) (4) (5)
SA-1	System and Services Acquisition Policy and Procedures	**SA-1**	**SA-1**	**SA-1**
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	System Development Life Cycle	SA-3	SA-3	SA-3
SA-4	Acquisition Process	**SA-4 (10)**	**SA-4 (1) (2) (9) (10)**	**SA-4 (1) (2) (9) (10)**
SA-5	Information System Documentation	SA-5	SA-5	SA-5
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8
SA-9	External Information System Services	SA-9	SA-9 (2)	SA-9 (2)
SA-10	Developer Configuration Management	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing and Evaluation	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	Not Selected	Not Selected	SA-12
SA-15	Development Process, Standards, and Tools	Not Selected	Not Selected	SA-15
SA-16	Developer-Provided Training	Not Selected	Not Selected	SA-16
SA-17	Developer Security Architecture and Design	Not Selected	Not Selected	SA-17
SC-1	System and Communications Protection Policy and Procedures	**SC-1**	**SC-1**	**SC-1**
SC-2	Application Partitioning	Not Selected	**SC-2**	**SC-2**
SC-3	Security Function Isolation	Not Selected	Not Selected	**SC-3**
SC-4	Information in Shared Resources	Not Selected	**SC-4**	**SC-4**
SC-5	Denial of Service Protection	**SC-5**	**SC-5**	**SC-5**
SC-7	Boundary Protection	SC-7	SC-7 (3) (4) (5) (7) **(18)**	SC-7 (3) (4) (5) (7) (8) **(18)** (21)
SC-8	Transmission Confidentiality and Integrity	Not Selected	SC-8 **(1)**	SC-8 **(1)**
SC-10	Network Disconnect	Not Selected	**SC-10**	**SC-10**
SC-12	Cryptographic Key Establishment and Management	**SC-12**	**SC-12**	**SC-12** (1)
SC-13	Cryptographic Protection	SC-13	SC-13	SC-13
SC-15	Collaborative Computing Devices	SC-15	SC-15	SC-15
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	**SC-19**	**SC-19**
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	**SC-20**	**SC-20**	**SC-20**

PL-8	情報セキュリティアーキテクチャ	未選択	PL-8	PL-8
PS-1	人員のセキュリティポリシー・手順	**PS-1**	**PS-1**	**PS-1**
PS-2	配置リスク指定	PS-2	PS-2	PS-2
PS-3	人選	PS-3	PS-3	PS-3
PS-4	退職	PS-4	PS-4	PS-4 (2)
PS-5	転勤	PS-5	PS-5	PS-5
PS-6	アクセス同意	PS-6	PS-6	PS-6
PS-7	サードパーティ社員セキュリティ	PS-7	PS-7	PS-7
PS-8	懲戒	PS-8	PS-8	PS-8
RA-1	リスク評価ポリシー・手順	**RA-1**	**RA-1**	**RA-1**
RA-2	セキュリティ分類	RA-2	RA-2	RA-2
RA-3	リスク評価	RA-3	RA-3	RA-3
RA-5	脆弱性検索	**RA-5**	**RA-5** (1) (2) (5)	**RA-5** (1) (2) (4) (5)
SA-1	システム及びサービス取得ポリシー・手順	**SA-1**	**SA-1**	**SA-1**
SA-2	リソース割当	SA-2	SA-2	SA-2
SA-3	システム開発ライフサイクル	SA-3	SA-3	SA-3
SA-4	取得プロセス	**SA-4 (10)**	**SA-4 (1) (2) (9) (10)**	**SA-4 (1) (2) (9) (10)**
SA-5	情報システム文書化	SA-5	SA-5	SA-5
SA-8	セキュリティエンジニアリング原則	未選択	SA-8	SA-8
SA-9	外部情報システムサービス	SA-9	SA-9 (2)	SA-9 (2)
SA-10	開発者設定管理	未選択	SA-10	SA-10
SA-11	開発者セキュリティ試験評価	未選択	SA-11	SA-11
SA-12	サプライチェーン保護	未選択	未選択	SA-12
SA-15	開発プロセス・規格・ツール	未選択	未選択	SA-15
SA-16	開発者による訓練	未選択	未選択	SA-16
SA-17	開発者セキュリティアーキテクチャ・設計	未選択	未選択	SA-17
SC-1	システム通信保護ポリシー・手順	**SC-1**	**SC-1**	**SC-1**
SC-2	アプリケーション分割	未選択	**SC-2**	**SC-2**
SC-3	セキュリティ機能隔絶	未選択	未選択	**SC-3**
SC-4	共有リソース内情報	未選択	**SC-4**	**SC-4**
SC-5	サービス保護妨害	**SC-5**	**SC-5**	**SC-5**
SC-7	境界の保護	SC-7	SC-7 (3) (4) (5) (7) **(18)**	SC-7 (3) (4) (5) (7) (8) **(18)** (21)
SC-8	通信機密性・完全性	未選択	SC-8 (1)	SC-8 (1)
SC-10	ネットワーク切断	未選択	**SC-10**	**SC-10**
SC-12	暗号鍵設定管理	**SC-12**	**SC-12**	SC-12 (1)
SC-13	暗号保護	SC-13	SC-13	SC-13
SC-15	共同コンピューティングデバイス	SC-15	SC-15	SC-15
SC-17	PKI 証明書	未選択	SC-17	SC-17
SC-18	モバイルコード	未選択	SC-18	SC-18
SC-19	VoIP	未選択	**SC-19**	**SC-19**
SC-20	セキュアな名前/アドレス解決サービス（権限ソース）	**SC-20**	**SC-20**	**SC-20**

SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	**SC-21**	**SC-21**	**SC-21**
SC-22	Architecture and Provisioning for Name/Address Resolution Service	**SC-22**	**SC-22**	**SC-22**
SC-23	Session Authenticity	Not Selected	**SC-23**	**SC-23**
SC-24	Fail in Known State	Not Selected	**SC-24**	**SC-24**
SC-28	Protection of Information at Rest	Not Selected	**SC-28**	**SC-28**
SC-39	Process Isolation	**SC-39**	**SC-39**	**SC-39**
SC-41	Port and I/O Device Access	**SC-41**	**SC-41**	**SC-41**
SI-1	System and Information Integrity Policy and Procedures	**SI-1**	**SI-1**	**SI-1**
SI-2	Flaw Remediation	**SI-2**	**SI-2 (2)**	**SI-2** (1) **(2)**
SI-3	Malicious Code Protection	**SI-3**	**SI-3 (1) (2)**	**SI-3 (1) (2)**
SI-4	Information System Monitoring	**SI-4**	**SI-4 (2) (4) (5)**	**SI-4 (2) (4) (5)**
SI-5	Security Alerts, Advisories, and Directives	**SI-5**	**SI-5**	**SI-5** (1)
SI-6	Security Function Verification	Not Selected	Not Selected	**SI-6**
SI-7	Software, Firmware, and Information Integrity	Not Selected	**SI-7 (1) (7)**	**SI-7 (1) (2) (5) (7)** (14)
SI-8	Spam Protection	Not Selected	**SI-8 (1) (2)**	**SI-8 (1) (2)**
SI-10	Information Input Validation	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Handling and Retention	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	Not Selected	Not Selected	**SI-13**
SI-14	Non-Persistence	Not Selected	Not Selected	Not Selected
SI-15	Information Output Filtering	Not Selected	Not Selected	Not Selected
SI-16	Memory Protection	Not Selected	SI-16	SI-16
SI-17	Fail-Safe Procedures	SI-17	SI-17	SI-17

SC-21	セキュアな名前/アドレス解決サービス（再帰又はキャッシングリゾルバ）	SC-21	SC-21	SC-21
SC-22	名前/アドレス解決サービス用アーキテクチャープロビジョニング	**SC-22**	**SC-22**	**SC-22**
SC-23	セッション信頼性	未選択	**SC-23**	**SC-23**
SC-24	既知状態の失敗	未選択	**SC-24**	**SC-24**
SC-28	休眠情報の保護	未選択	**SC-28**	**SC-28**
SC-39	プロセス隔離	**SC-39**	**SC-39**	**SC-39**
SC-41	ポート及び I/O デバイスアクセス	**SC-41**	**SC-41**	**SC-41**
SI-1	システム情報完全性ポリシー・手順	**SI-1**	**SI-1**	**SI-1**
SI-2	欠陥修正	**SI-2**	**SI-2 (2)**	**SI-2** (1) **(2)**
SI-3	悪意あるコード保護	**SI-3**	**SI-3 (1) (2)**	**SI-3 (1) (2)**
SI-4	情報システム監視	**SI-4**	**SI-4 (2) (4) (5)**	**SI-4 (2) (4) (5)**
SI-5	セキュリティ警報・勧告・指示	**SI-5**	**SI-5**	SI-5 (1)
SI-6	セキュリティ機能検証	未選択	未選択	**SI-6**
SI-7	ソフトウエア・ファームウエア・情報の完全性	未選択	**SI-7 (1) (7)**	**SI-7 (1) (2) (5) (7)** (14)
SI-8	スパム保護	未選択	**SI-8 (1) (2)**	**SI-8 (1) (2)**
SI-10	情報入力検証	未選択	SI-10	SI-10
SI-11	エラー処理	未選択	SI-11	SI-11
SI-12	情報処理保留	SI-12	SI-12	SI-12
SI-13	予想される故障の防止	未選択	未選択	**SI-13**
SI-14	非執拗性	未選択	未選択	未選択
SI-15	情報出力フィルタリング	未選択	未選択	未選択
SI-16	メモリ保護	未選択	SI-16	SI-16
SI-17	フェールセーフ手順	SI-17	SI-17	SI-17

The PM-family is deployed organization-wide, supporting the information security program. It is not associated with security control baselines and is independent of any system impact level.

PM-1	Information Security Program Plan	**PM-1**
PM-2	Senior Information Security Officer	PM-2
PM-3	Information Security Resources	**PM-3**
PM-4	Plan of Action and Milestones Process	**PM-4**
PM-5	Information System Inventory	PM-5
PM-6	Information Security Measures of Performance	PM-6
PM-7	Enterprise Architecture	**PM-7**
PM-8	Critical Infrastructure Plan	**PM-8**
PM-9	Risk Management Strategy	**PM-9**
PM-10	Security Authorization Process	**PM-10**
PM-11	Mission/Business Process Definition	**PM-11**
PM-12	Insider Threat Program	PM-12
PM-13	Information Security Workforce	**PM-13**
PM-14	Testing, Training, and Monitoring	PM-14
PM-15	Contacts with Security Groups and Associations	PM-15
PM-16	Threat Awareness Program	PM-16

PM ファミリは全組織に展開され、情報セキュリティプログラムを支えている。セキュリティ対策ベースラインは付随しておらず、いかなるシステム影響レベルとも無関係である。

PM-1	情報セキュリティプログラム計画書	**PM-1**
PM-2	上級情報セキュリティ担当官	PM-2
PM-3	情報セキュリティリソース	**PM-3**
PM-4	行動・マイルストーンプロセス計画書	**PM-4**
PM-5	情報システム目録	PM-5
PM-6	情報セキュリティに関するパフォーマンスの計測	PM-6
PM-7	企業アーキテクチャ	**PM-7**
PM-8	重要インフラ計画書	**PM-8**
PM-9	リスク管理戦略	**PM-9**
PM-10	セキュリティ権限プロセス	**PM-10**
PM-11	任務・事業プロセス定義	**PM-11**
PM-12	インサイダー脅威プログラム	PM-12
PM-13	情報セキュリティリワークフォース	**PM-13**
PM-14	試験・訓練・監視	PM-14
PM-15	セキュリティグループ・協会との契約	PM-15
PM-16	脅威意識プログラム	PM-16

Tailoring Considerations

Due to the unique characteristics of ICS, these systems may require a greater use of compensating security controls than is the case for general purpose information systems. Compensating controls are not exceptions or waivers to the baseline controls; rather, they are alternative safeguards and countermeasures employed within the ICS that accomplish the intent of the original security controls that could not be effectively employed. See "Selecting Compensating Security Controls" in section 3.2 of NIST SP 800-53 Rev. 4 [22].

In situations where the ICS cannot support, or the organization determines it is not advisable to implement, particular security controls or control enhancements in an ICS (e.g., performance, safety, or reliability are adversely impacted), the organization provides a complete and convincing rationale for how the selected compensating controls provide an equivalent security capability or level of protection for the ICS and why the related baseline security controls could not be employed.

In accordance with the Technology-related Considerations of the Scoping Guidance in NIST SP 800-53 Rev. 4, section 3.2, if automated mechanisms are not readily available, cost-effective, or technically feasible in the ICS, compensating security controls, implemented through nonautomated mechanisms or procedures are employed [22].

Compensating controls are alternative security controls employed by organizations in lieu of specific controls in the baselines—controls that provide equivalent or comparable protection for organizational information systems and the information processed, stored, or transmitted by those systems.[83] This may occur, for example, when organizations are unable to effectively implement specific security controls in the baselines or when, due to the specific nature of the ICS or environments of operation, the controls in the baselines are not a cost-effective means of obtaining the needed risk mitigation. Compensating controls may include control enhancements that supplement the baseline. Using compensating controls may involve a trade-off between additional risk and reduced functionality. Every use of compensating controls should involve a risk-based determination of: (i) how much residual risk to accept, and (ii) how much functionality should be reduced. Compensating controls may be employed by organizations under the following conditions:

- Organizations select compensating controls from NIST SP 800-53 Rev. 4, Appendix F. If appropriate compensating controls are not available, organizations adopt suitable compensating controls from other sources [84]
- Organizations provide supporting rationale for how compensating controls provide equivalent security capabilities for organizational information systems and why the baseline security controls could not be employed.
- Organizations assess and accept the risk associated with implementing compensating controls in ICS.

Organizational decisions on the use of compensating controls are documented in the security plan for the ICS.

---

[83] 42 More than one compensating control may be required to provide the equivalent protection for a particular security control in Appendix F. For example, organizations with significant staff limitations may compensate for the separation of duty security control by strengthening the audit, accountability, and personnel security controls.

[84] 43 Organizations should make every attempt to select compensating controls from the security control catalog in Appendix F. Organization-defined compensating controls are employed *only* when organizations determine that the security control catalog does not contain suitable compensating controls.

カスタマイズの考慮事項

ICS 独特の特徴から、これらシステムに必要とされる補償セキュリティ管理は、汎用の情報システムよりも多い。代替管理はベースライン管理の例外や放棄ではなく、代替の安全策及び対策として ICS 内で採用され、有効利用できない元のセキュリティ対策の目的を果たす。NIST SP 800-53 第 4 版[22]のセクション 3.2「補償セキュリティ対策」を参照のこと。

ICS が ICS におけるセキュリティ対策若しくは管理拡張に対応していない場合又は組織が ICS におけるセキュリティ対策若しくは管理拡張の実装を不適と判断する場合（パフォーマンス、安全性、信頼性への悪影響等）、選定した補償的管理策に同等のセキュリティ機能又は同等レベルの ICS 保護能力があり、関連ベースラインセキュリティ対策が採用できなかった理由について、組織は納得のいく理由を示す。

自動化メカニズムがすぐに利用できない、費用効果がない又は技術的に不可能な場合、NIST SP 800-53 第 4 版のセクション 3.2 の「適用範囲ガイダンスの技術関連考慮事項」に従い、補償セキュリティ対策を非自動化メカニズム又は手順の実施を通じて採用する[22]。

補償的管理策は、特定のベースライン管理に代えて組織が取る代替セキュリティ対策で、組織の情報システムとそこで処理、保管又は送信される情報に同等の保護を与えるものをいう。[85] 例えば、特定のベースライン管理を効果的に実施できない場合や、ICS 固有の性質若しくは運用環境に起因して、ベースラインの管理がリスク緩和上費用対効果のない場合に、補償的管理策が講じられる。補償的管理策には、ベースラインを補完する管理拡張が含まれることがある。補償的管理策を行うには、リスク増加と機能低下のバランスが関係してくる。必ず(1)許容できるリスクの程度と、(2) どの程度機能が低下するかを、リスクに基づいて判断すべきである。組織は、次のような条件の下で補償的管理策を採用できる。

- 適当な補償的管理策を NIST SP 800-53 第 4 版付録 F から選ぶ[86]。適当な補償的管理策が同付録にない場合、他のソースから適当な補償的管理策を採用する。
- 組織は、補償的管理策が情報システムに対して同等のセキュリティ機能を有し、ベースラインセキュリティ対策が採用できなかった根拠となる理由を示す。
- 組織は、ICS における補償的管理策の実施に付随するリスクを評価し受け入れる。

代替管理を利用する組織の決定は、ICS のセキュリティ計画書に記録する。

---

85 付録 F の特定のセキュリティ対策に同等の保護を与えるには、補償管理が複数必要となることもある。例えば、職員数が限られている組織では、監査管理、説明責任管理及び職員のセキュリティ対策を強化して、セキュリティ管理任務を分割することになろう。

86 組織はあらゆる努力を払って、付録 F のセキュリティ対策カタログから補償的管理策を選ぶべきである。組織が自ら定義した補償的管理策は、同カタログに適当なものがない場合にのみ採用する。

Controls that contain assignments (e.g., *Assignment: organization-defined conditions or trigger events*) may be tailored out of the baseline. This is equivalent to assigning a value of "none." The assignment may take on different values for different impact baselines.

Non-Addressable and Non-Routable Communications

The unique network properties within ICS warrant specific attention when applying certain security controls. Many of the controls in NIST SP 800-53 Rev. 4 that pertain to communication, devices, and interfaces implicitly assume the applicability of addressable and routable protocols such as the TCP/IP Internet protocol suite[87] or layers 1, 2, and 3 of the Open Systems Interconnection (OSI) model (ISO/IEC 7498-1). Some devices, or subsystems, used in ICS are exceptions to this assumption. This section addresses how the controls may be appropriately tailored. Tailoring is primarily required due to the following situations:

- *Capabilities not present*. The intent of certain controls may be more easily achieved through compensating controls due to certain network properties or capabilities not existing in the ICS subsystem. For example, physical protections (e.g., locked cabinets) may be used to secure an entire point-to-point communication channel as a means to compensate for a lack of protocols that support authentication. Security controls may warrant additional supplemental guidance to help ensure the implementation of the control or compensating control provides the appropriate level of protection.
- *Non-applicable security controls*. Many communication protocols found within an ICS may have limited functionality (e.g., not addressable or routable). Security controls dealing with addressing and routing may not be applicable to these protocols.

Security controls for devices that communicate point-to-point using standards and protocols that do not include addressing generally require tailoring. A modem connected to a computer through an RS-232 interface is an example. RS-232 was commonly employed in ICS equipment that is currently in use, even if it has been superseded in newer equipment. In telecommunications, RS-232 is the traditional name for a series of standards for serial binary single-ended data and control signals connecting between *DTE* (data terminal equipment) and *DCE* (data circuit-terminating equipment, originally defined as *data communication equipment*). The current version of the standard is Telecommunications Industry Association *(TIA)-232-F, Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*, issued in 1997.

An RS-232 serial port was once a standard feature of small computing devices, such as ICS subsystems, used for connections to peripheral devices. However, the low transmission speed, large voltage swing, and large standard connectors motivated development of the Universal Serial Bus (USB), which has displaced RS-232 from most of its peripheral interface roles. RS-232 devices are still found, especially in industrial machines, networking equipment, and scientific instruments.

Layered Network Models

The layered network models used in both TCP/IP and OSI can provide a basis for understanding the various properties of network communications and will help identify how security controls can be appropriately applied to systems and networks. The following table introduces key properties about the physical, data link, and network layers regarding the application of security controls.

[87] 44 Currently, the Internet Engineering Task Force, or IETF, manages the TCP/IP protocol suite.

割当（組織が定義した条件やトリガー事象等）は、ベースラインを基にカスタマイズできる。これは「なし」の値を割り当てるのと同じことである。割当は、影響ベースラインが異なると値も異なることがある。

アドレス指定又は経路指定のない通信

特定のセキュリティ対策を適用する場合、ICS 内での固有のネットワーク特性に特に留意すべきである。NIST SP 800-53 第 4 版の通信、デバイス及びインタフェースに関する管理の多くは、TCP/IP インターネットスイート[88]やオープンシステム間相互連接（OSI）モデル(ISO/IEC 7498-1)の TCP/IP レイヤー1、2、3 等、アドレス指定可能又は経路指定可能プロトコルを適用することを暗黙の前提にしている。ICS で使用するある種のデバイスやサブシステムは、この前提の例外となる。このセクションでは、管理の適正なカスタマイズ方法について取り上げる。カスタマイズは、主として次のような場合に必要となる。

- *機能がない*。特定の管理の目的は、特定のネットワーク特性又は機能が ICS サブシステムにないため、補償的管理策により容易に達成可能である。例えば物理的保護（キャビネットの施錠等）は、認証機能付きプロトコルがない場合の補償手段として、2 点間通信チャンネルのセキュア化に利用できる。セキュリティ対策は付加的な補足ガイダンスとして、管理又は補償的管理策による適性レベルの保護の確保に役立つ。
- *適用可能なセキュリティ対策がない*。ICS で使用されているプロトコルの多くは、機能が限られている（アドレス指定やルート指定ができない等）。アドレス及びルートに関するセキュリティ対策は、このようなプロトコルには適用できない。

アドレス指定のない規格及びプロトコルを使用した 2 点間通信を行うデバイスのセキュリティ対策には、通常、カスタマイズが必要となる。RS-232 インタフェース経由のコンピュータに接続されたモデルがその一例である。RS-232 は、現在利用されている ICS 装備品で一般的に使用されていた（そうした装備品が新しいものに換装されている場合であっても）。電気通信において RS-232 は、DTE（データ端末装置）と DCE（データ回線終端装置、元はデータ通信装置）間のシリアルバイナリシングルエンドデータ制御信号規格の伝統的な名称である。現行版規格は米国電気通信工業会（TIA）-232-F「シリアルバイナリデータ交換によるデータ端末装置データ回線端末装置間インタフェース」として、1997 年に発表された。

RS-232 シリアルポートは、ICS サブシステム等の小型コンピューティングデバイスの規格機能として、周辺デバイスへの接続に使用された。しかし通信速度が遅く、電圧振幅が大きく、規格コネクタが大きいことから USB が開発され、RS-232 の周辺インタフェースとしての役割は終わった。RS-232 デバイスは、特に産業用マシン、ネットワーキング装置及び科学計装機器で今でも使用されている。

階層型ネットワークモデル

TCP/IP と OSI の双方で使用されている 階層型ネットワークモデルは、ネットワーク通信を理解する基本で、システム及びネットワークに適用すべきセキュリティ対策要領の識別に役立つ。次の表は、セキュリティ対策の適用に関する物理的階層、データリンク階層及びネットワーク階層の重要特性を示す。

[88] 現在インターネットタスクフォース（IETF）が TCP/IP プロトコルスイートの管理を行っている。

Network Layer	***Layer properties***
Physical	***Physical Medium*** – A network's physical medium, specifically whether it's wired or wireless can drive the application/tailoring of certain controls. Wireless connections cannot be physically protected; therefore, compensating controls focusing on physical security cannot be used. *Topology* – The physical topologies may also determine how controls are tailored. For example point-to-point topologies (e.g., RS-232) generally do not need physically addressable interfaces, while multipoint topologies (e.g., IEEE 802.3 Ethernet) do require physically addressable interfaces.
Data link	***Physically Addressable*** – Multipoint protocols require physically addressable interfaces to allow for multiple systems to communicate. Systems that are not physically addressable can only be accessed by those systems with which it shared point-to-point connections.
Network	***Network Addressable/Routable*** – Network addressable/routable systems can be accessed by any system on an internetwork. That is, communications can be routed between networks. If a system is not network addressable/routable, it can only be accessed by systems with which it shares a local network connection.

Definitions

Terms used in this overlay are defined in Appendix B— or in NIST Internal Report (NISTIR) 7298 Revision 2, *Glossary of Key Information Security Terms* [99].

Additional Information or Instructions

None at this time. Organizations may provide any additional information or instructions relevant to the overlay not covered in the previous sections.

ネットワーク層	階層特性
物理	**物理的媒体** - ネットワークの物理的媒体で、特に有線/無線の違いにより、特定の管理の適用かカスタマイズかが決まる。 ワイヤレス接続は物理的に保護できないため、物理的セキュリティに特化した補償的管理策は利用できない。 トポロジー - 物理的トポロジーも管理のカスタマイズ方法を決定づける。例えば 2 点間トポロジー（RS-232 等）は、通常、物理的にアドレス指定可能なインタフェースが不要であるが、マルチポイントトポロジー（IEEE 802.3 Ethernet 等）では必要となる。
データリンク	**物理的アドレス指定可能** - マルチポイントプロトコルは、複数システム間の通信用に、物理的にアドレス指定可能なインタフェースを必要とする。物理的アドレス指定不能のシステムには、共有 2 点間通信のあるシステム以外にはアクセスできない。
ネットワーク	**ネットワークアドレス指定可能/ルート指定可能** - アドレス/ルート指定可能システムには、ネットワーク間のどのシステムからもアクセスできる。つまり通信は、ネットワーク間で経路指定される。あるシステムがアドレス/ルート指定不能の場合、アクセスできるのはローカルネットワーク接続を共有するシステムのみとなる。

定義

このオーバーレイで使用する用語は、付録 B 又は NIST 内部報告書(NISTIR)7298 第 2 版要情報セキュリティ用語集[99]に定義がある。

補足情報又は指示

現在のところない。組織は、前のセクションにないオーバーレイに関する補足情報又は指示を与えることができる。

Detailed Overlay Control Specifications

This Overlay is based on the NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, which provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors (both intentional and unintentional). The security and privacy controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. The publication also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability). Addressing both security functionality and assurance helps to ensure that information technology component products and the information systems built from those products using sound system and security engineering principles are sufficiently trustworthy.

In preparation for selecting and specifying the appropriate security controls for organizational information systems and their respective environments of operation, organizations first determine the criticality and sensitivity of the information to be processed, stored, or transmitted by those systems. This process is known as security categorization. FIPS 199 [15] enables federal agencies to establish security categories for both information and information systems. Other documents, such as those produced by ISA and CNSS, also provide guidance for defining low, moderate, and high levels of security based on impact. The security categories are based on the potential impact on an organization or on people (employees and/or the public) should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals' safety, health and life. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

This overlay provides ICS Supplemental Guidance for the security controls and control enhancements prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. This overlay contains a tailoring of the security control baselines; its specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. This overlay is high-level, applicable to all ICS; it may be used as the basis for more specific overlays. Use cases for specific systems in specific environments may be separately published (e.g., as a NISTIR).

詳細オーバーレイ管理仕様書

このオーバーレイは NIST SP 800-53 第 4 版「連邦情報システム・組織のセキュリティ・プライバシー管理」を基にしている。第 4 版には組織運用（任務、機能、イメージ、評判等）、組織資産、個人、他の組織及び国を敵のサイバー攻撃、自然災害、構造的障害及び人的過誤（意図的又は偶発的）等の様々な脅威から保護するための連邦情報システム・組織及び管理選定プロセスのセキュリティ・プライバシー管理カタログが示されている。セキュリティ・プライバシー管理はカスタマイズが可能で、情報セキュリティ・プライバシーのリスクを管理する全組織的プロセスの一環として実施される。管理は、法令、大統領令、政策、指示、規則、規格又は任務・事業ニーズから生じた連邦政府及び重要インフラ全体の様々なセキュリティ・プライバシー要件を対象としている。この文書には、特殊管理やオーバーレイを固有の任務・事業機能、技術又は運用環境に合わせて策定する方法が説明されている。最後にセキュリティ対策カタログは、機能的な面（セキュリティ機能・メカニズムの強度）と保証面（実施したセキュリティ能力の信頼性）の両方からセキュリティを検討する。機能と保証の両面を取り上げることで、情報技術コンポーネント製品と、その製品を使用して、しっかりしたシステム原則とセキュリティエンジニアリング原則を適用し、構築された情報システムが十分信頼に応えられるものとなる。

組織の情報システムとそれぞれの運用環境に対するセキュリティ対策を選定・指定するための準備として、まず組織は、それらシステムにより処理、保管又は送信される情報の重要性と要注意性を判定する。このプロセスはセキュリティ分類として知られている。FIPS 199[15]は、連邦政府機関が情報及び情報システム用のセキュリティ分類を設定できるように示している。ISA や CNSS により作成された他の文書も、影響度に応じて低・中・高レベルを定めるガイダンスを示している。

セキュリティ分類は、特定の事象が起きて、組織の任務遂行、資産保護、法的責任の遂行、日常業務の維持及び個人の安全・健康・生命保護に必要とされる情報や情報システムが危険に陥る場合の、組織又は個人（従業員又は国民）に及ぶ影響度を基にしている。セキュリティ分類は脆弱性及び脅威情報と合わせて、組織に対するリスク評価に使用すべきである。

このオーバーレイは、情報の機密性、完全性及び可用性を保護するために、また、定められた一連のセキュリティ要件を満たすために、情報システムや組織向けに作成されたセキュリティ対策・管理拡張用 ICS 補足ガイダンスとなる。セキュリティ管理ベースラインのカスタマイズが含まれ、その仕様は元のセキュリティ管理ベースライン仕様よりも厳しい場合もあれば緩い場合もあり、種々の情報システムに適用可能である。このオーバーレイは高レベルで、全ての ICS に適用可能であり、より多くの個別オーバーレイの基礎として使用できる。具体的な環境における特定システムでの使用例は別途示されている（NISTIR 等）。

Figure G-1 uses the AU-4 control as an example of the format and content of the detailed overlay control specifications.

❶ Control number and title.
❷ Column for control and control enhancement number.
❸ Column for control and control enhancement name.
❹ Columns for baselines. If the baselines have been supplemented, then SUPPLEMENTED appears.
❺ A row for each control or control enhancement.
❻ Columns for LOW, MODERATE, and HIGH baselines.
❼ "Selected" indicates the control is selected in NIST SP 800-53 Rev. 4. "Added" indicates the control is added to a baseline in the ICS overlay. A blank cell indicates the control is not selected. "Removed" indicates the control is removed from the baseline.
❽ The ICS Supplemental Guidance. If there is none, that is stated.
❾ The Control Enhancement ICS Supplemental Guidance. If there is none, that is stated.
❿ The rationale for changing the presence of a control or control enhancement in the baseline.

❶ **AU-4 AUDIT STORAGE CAPACITY**

	❷ CNTL NO.	❸ CONTROL NAME *Control Enhancement Name*	❹ SUPPLEMENTED CONTROL BASELINES			
			LOW	MOD	HIGH	❻
❺	AU-4	**Audit Storage Capacity**	Selected	Selected	Selected	❼
	AU-4 (1)	*AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*	Added	Added	Added	

❽ No ICS Supplemental Guidance.

❾ Control Enhancement: (1) ICS Supplemental Guidance: Legacy ICS typically are typically configured with remote storage on a separate information system (e.g., the historian in the DMZ accumulates historical operational ICS data and is backed up for storage at a different site). ICS are currently using online backup services and increasingly moving to Cloud based and Virtualized services. Retention of some data (e.g., SCADA telemetry) may be required by regulatory authorities.

❿ Rationale for adding control to baseline: Legacy ICS components typically do not have capacity to store or analyze audit data. The retention periods for some data, particularly compliance data, may require large volumes of storage.

Figure G-1 Detailed Overlay Control Specifications Illustrated

NIST SP 800-53 Rev. 4, Appendix F, contains Supplemental Guidance for all Controls and Control Enhancements [22]. ICS Supplemental Guidance in this overlay provides organizations with additional information on the application of the security controls and control enhancements in NIST SP 800-53 Rev. 4, Appendix F, to ICS and the environments in which these specialized systems operate. The ICS Supplemental Guidance also provides information as to why a particular security control or control enhancement may not be applicable in some ICS environments and may be a candidate for tailoring (i.e., the application of scoping guidance and/or compensating controls).

図 G-1 は、詳細なオーバーレイ管理仕様の様式及び内容の一例として、AU-4 管理を使用している。

❶ 管理の番号と題名
❷ 管理・管理拡張番号を示すカラム
❸ 管理・管理拡張名を示すカラム
❹ ベースラインを示すカラム。ベースラインの補足がある場合、「補足（SUPPLEMENTED）」と表示される。
❺ 各管理・管理拡張を示す行。
❻ 低・中・高及び高ベースラインを示すカラム
❼ 「選定」は NIST SP 800-53 第 4 版で管理が選定されていることを示す。「追加」は管理が ICS オーバーレイのベースラインに追加されていることを示す。空白セルは管理が選定されていないことを示す。「削除」は管理がベースラインから削除されたことを示す。
❽ ICS 補足ガイダンス。何もない場合、その旨の記述がある。
❾ 管理拡張 ICS 補足ガイダンス。何もない場合、その旨の記述がある。
❿ ベースラインの管理・管理拡張の有無が変わった理由

❶ **AU-4 AUDIT STORAGE CAPACITY**

	❷ CNTL NO.	❸ CONTROL NAME *Control Enhancement Name*	❹ SUPPLEMENTED CONTROL BASELINES			
			LOW	MOD	HIGH	❻
❺	AU-4	Audit Storage Capacity	Selected	Selected	Selected	❼
	AU-4 (1)	*AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*	Added	Added	Added	

❽ ICS 補足ガイダンスなし

❾ **管理拡張**：(1) ICS 補足ガイダンス：レガシーICS は、一般に別個の情報システム上の遠隔ストレージで設定されている（DMZ のヒストリアン等で、ICS の運用履歴データを蓄積し、別サイトのストレージに保管する）。ICS は今のところオンラインバックアップサービスを利用しているが、クラウドベースの仮想サービスに次第に移行している。特定のデータ（SCADA テレメトリ-等）の保持が規制当局から義務づけられる場合がある。

❿ **ベースラインに管理を追加する理由**：一般にレガシーICS コンポーネントには、監査データの保存又は分析容量がない。特定のデータ、特にコンプライアンスデータの保持期間によって、保管量が大きくなる。

図 G-1 詳細オーバーレイ管理仕様の説明

NIST SP 800-53 第 4 版付録 F に、全ての管理・管理拡張補足ガイダンスがある[22]。このオーバーレイの ICS 補足ガイダンスは、NIST SP 800-53 第 4 版の付録 F に記載されるセキュリティ対策及び管理拡張を、ICS 及びこれら専用システムの実行環境に適用するための補足情報を示す。また、ICS 環境によっては特定のセキュリティ対策や管理拡張が適用できず、調整が必要となる理由についても示す（スコーピングガイダンス又は補償制御）。

ACCESS CONTROL – AC

Tailoring Considerations for Access Control Family

Before implementing controls in the AC family, consider the tradeoffs among security, privacy, latency, performance, throughput, and reliability. For example, the organization considers whether latency induced from the use of confidentiality and integrity mechanisms employing cryptographic mechanisms would adversely impact the operational performance of the ICS.

In situations where the ICS cannot support the specific Access Control requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-1	**Access Control Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems. ICS access by vendors and maintenance staff can occur over a very large facility footprint or geographic area and into unobserved spaces such as mechanical/electrical rooms, ceilings, floors, field substations, switch and valve vaults, and pump stations.

AC-2 ACCOUNT MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-2	**Account Management**	Selected	Selected	Selected
AC-2 (1)	*ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT*		Selected	Selected
AC-2 (2)	*ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS*		Selected	Selected
AC-2 (3)	*ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS*		Selected	Selected
AC-2 (4)	*ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS*		Selected	Selected
AC-2 (5)	*ACCOUNT MANAGEMENT | INACTIVITY LOGOUT / TYPICAL USAGE MONITORING*			Selected
AC-2 (11)	*ACCOUNT MANAGEMENT | USAGE CONDITIONS*			Selected
AC-2 (12)	*ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE*			Selected
AC-2 (13)	*ACCOUNT MANAGEMENT | ACCOUNT REVIEWS*			Selected

ICS Supplemental Guidance: Example compensating controls include providing increased physical security, personnel security, intrusion detection, auditing measures.

Control Enhancement: (1, 3, 4) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.

Control Enhancement: (2) ICS Supplemental Guidance: In situations where the ICS (e.g., field devices) cannot support temporary or emergency accounts, this enhancement does not apply. Example compensating controls include employing nonautomated mechanisms or procedures.

Control Enhancement: (5) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.

Control Enhancement: (11, 12, 13) No ICS Supplemental Guidance.

アクセス制御 - AC

アクセス制御ファミリのカスタマイズ考慮事項
AC ファミリで管理を実施する前に、セキュリティ、プライバシー、待ち時間、パフォーマンス、スループット、信頼性を比較考量する。例えば、暗号メカニズムを採用して機密性及び完全性メカニズムを利用することにより生じる待ち時間が、ICS の運用パフォーマンスを阻害しないか組織は検討する。
ICS がある制御の特定のアクセス制御要件に対応していない状況では、全体的なカスタマイズガイダンスに従って補償的管理策を採用する。補償管理の例が必要に応じて、管理策ごとに示される。

補足ガイダンス
利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、ICS 補足ガイダンスと併用すべきである。

AC-1 アクセス制御ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン 低	中	高
AC-1	**アクセス制御ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。ベンダー及び保守要員による ICS へのアクセスは、機械・電気室、天井、床、変電設備、スイッチ・バルブ室、ポンプ室等、広範な施設及び地域や監視下にない空間にまたがっている。

AC-2 アカウント管理

管理番号	管理名 *管理拡張名*	管理ベースライン 低	中	高
AC-2	**アカウント管理**	選定	選定	選定
AC-2 (1)	*アカウント管理 | 動システムアカウント管理*		選定	選定
AC-2 (2)	*アカウント管理 |臨時・緊急用アカウントの削除*		選定	選定
AC-2 (3)	*アカウント管理 |無活動アカウントの無効化*		選定	選定
AC-2 (4)	*アカウント管理 | 自動監査行為*		選定	選定
AC-2 (5)	*アカウント管理 | 無活動ログアウト・一般的利用監視*			選定
AC-2 (11)	*アカウント管理 | 利用状態*			選定
AC-2 (12)	*アカウント管理 | アカウント監視・非対称利用*			選定
AC-2 (13)	*アカウント管理 | アカウント審査*			選定

ICS 補足ガイダンス：補償的管理策の例として、物理的セキュリティ、人的セキュリティ、侵入検知、監査手段の強化がある。
管理拡張：(1, 3, 4) ICS 補足ガイダンス：補償的管理策の例として、非自動メカニズム又は手順がある。
管理拡張：(2) ICS 補足ガイダンス：ICS（フィールドデバイス等）が臨時又は緊急アカウントに対応できない場合、この拡張は適用されない。補償的管理策の例として、非自動メカニズム又は手順がある。
管理拡張：(5) ICS 補足ガイダンス：補償的管理策の例として、非自動メカニズム又は手順がある。
管理拡張：(11, 12, 13) ICS 補足ガイダンスなし

AC-3 ACCESS ENFORCEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-3	**Access Enforcement**	Selected	Selected	Selected

ICS Supplemental Guidance: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS. Example compensating controls include encapsulation. Policy for logical access control to Non-Addressable and Non-Routable system resources and the associated information is made explicit. Access control mechanisms include hardware, firmware, and software that controls or has device access, such as device drivers and communications controllers. Physical access control may serve as a compensating control for logical access control, however, it may not provide sufficient granularity in situations where users require access to different functions. Logical access enforcement may be implemented in encapsulating hardware and software.

AC-4 INFORMATION FLOW ENFORCEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-4	**Information Flow Enforcement**		Selected	Selected

ICS Supplemental Guidance: Physical addresses (e.g., a serial port) may be implicitly or explicitly associated with labels or attributes (e.g., hardware I/O address). Manual methods are typically static. Label or attribute policy mechanisms may be implemented in hardware, firmware, and software that controls or has device access, such as device drivers and communications controllers. Information flow policy may be supported by labeling or coloring physical connectors as an aid to manual hookup. Inspection of message content may enforce information flow policy. For example, a message containing a command to an actuator may not be permitted to flow between the control network and any other network.

AC-5 SEPARATION OF DUTIES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-5	**Separation of Duties**		Selected	Selected

ICS Supplemental Guidance: Example compensating controls include providing increased personnel security and auditing. The organization carefully considers the appropriateness of a single individual performing multiple critical roles.

AC-6 LEAST PRIVILEGE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-6	**Least Privilege**		**Selected**	**Selected**
AC-6 (1)	*LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*		Selected	Selected
AC-6 (2)	*LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*		Selected	Selected
AC-6 (3)	*LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*			Selected
AC-6 (5)	*LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*		Selected	Selected
AC-6 (9)	*LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*		Selected	Selected
AC-6 (10)	*LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*		Selected	Selected

ICS Supplemental Guidance: Example compensating controls include providing increased personnel security and auditing. The organization carefully considers the appropriateness of a single individual having multiple critical

AC-3 アクセスの施行

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-3	**アクセス施行**	選定	選定	選定

ICS 補足ガイダンス：組織は、アクセス施行メカニズムが ICS の運用パフォーマンスに悪影響しないようにする。補償管理にはカプセル化がある。アドレス/ルート指定不能システムリソース及び関連情報への論理アクセス制御ポリシーは明確にする。アクセス制御メカニズムには、ハードウエア、ファームウエアのほか、デバイスドライバや通信コントローラ等、デバイスの制御又はアクセスを行うソフトウエアがある。物理的アクセス制御は、論理アクセス制御に代わる補償的管理策となるが、ユーザが別機能へのアクセスを求める場合のきめ細かさがない。論理アクセス施行は、ハードウエアとソフトウエアのカプセル化で実施できる。

AC-4 情報フローの施行

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-4	**情報フロー施行**		選定	選定

ICS 補足ガイダンス：物理アドレス（シリアルポート等）は、黙示的又は明示的にラベル又は属性（ハードウエア I/O アドレス等）に関連づける。マニュアル操作は一般に静的である。ラベル又は属性メカニズムは、ハードウエア、ファームウエアのほか、デバイスドライバや通信コントローラ等、デバイスの制御又はアクセスを行うソフトウエアに実装される。情報フローポリシーは、マニュアル操作作業の助けとして、物理的コネクタへのラベル付けや着色により支えられる。メッセージ内容の検査は、情報フローポリシーを施行するものとなる。例えば、アクチュエータへのコマンドを含んだメッセージは、制御ネットワークと他のネットワーク間で流れないようにしなければならない。

AC-5 任務分担

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-5	**任務分担**		選定	選定

ICS 補足ガイダンス：補償的管理策の例として、人的セキュリティと監査の強化がある。組織は、1 人で複数の重要な役割を果たすのが適切かどうか、慎重に検討する。

AC-6 最小権限

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-6	**最小権限**		選定	選定
AC-6 (1)	*最小権限 | セキュリティ機能へのアクセス許可*		選定	選定
AC-6 (2)	*最小権限 | 非セキュリティ機能への無権限アクセス*		選定	選定
AC-6 (3)	*最小権限 | 特権コマンドへのネットワークアクセス*			選定
AC-6 (5)	*最小権限 | 特権アカウント*		選定	選定
AC-6 (9)	*最小権限 | 特権機能の監査利用*		選定	選定
AC-6 (10)	*最小権限 | 無権限ユーザによる特権機能の実行禁止*		選定	選定

ICS 補足ガイダンス：補償的管理策の例として、人的セキュリティと監査の強化がある。組織は、1 人で複数の重要特権を持つのが適切かどうか、慎重に検討する。

privileges. System privilege models may be tailored to enforce integrity and availability (e.g., lower privileges include read access and higher privileges include write access).

Control Enhancement: (1) ICS Supplemental Guidance: In situations where the ICS cannot support access control to security functions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (2) ICS Supplemental Guidance: In situations where the ICS cannot support access control to nonsecurity functions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (3) ICS Supplemental Guidance: In situations where the ICS cannot support network access control to privileged commands, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (5) ICS Supplemental Guidance: In situations where the ICS cannot support access control to privileged accounts, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (9) ICS Supplemental Guidance: In general, audit record processing is not performed on the ICS, but on a separate information system. Example compensating controls include providing an auditing capability on a separate information system.

Control Enhancement: (10) ICS Supplemental Guidance: Example compensating controls include enhanced auditing.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-7	**Unsuccessful Login Attempts**	Selected	Selected	Selected

ICS Supplemental Guidance: Many ICS must remain continuously on and operators remain logged onto the system at all times. A "log-over" capability may be employed. Example compensating controls include logging or recording all unsuccessful login attempts and alerting ICS security personnel though alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded.

AC-8 SYSTEM USE NOTIFICATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-8	**System Use Notification**	Selected	Selected	Selected

ICS Supplemental Guidance: Many ICS must remain continuously on and system use notification may not be supported or effective. Example compensating controls include posting physical notices in ICS facilities.

AC-10 CONCURRENT SESSION CONTROL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-10	**Concurrent Session Control**			Selected

ICS Supplemental Guidance: The number, account type, and privileges of concurrent sessions takes into account the roles and responsibilities of the affected individuals. Example compensating controls include providing increased auditing measures.

システム特権モデルをカスタマイズして、完全性と可用性を施行できる（より低い特権には読み取りアクセス、より高い特権には書き込みアクセスがある）。

管理拡張：(1) ICS 補足ガイダンス：ICS がセキュリティ機能へのアクセス制御に対応していない状況では、全体的なカスタマイズガイダンスに従って、組織は非自動メカニズム又は手順を採用する。

管理拡張：(2) ICS 補足ガイダンス：ICS が非セキュリティ機能へのアクセス制御に対応していない状況では、全体的なカスタマイズガイダンスに従って、組織は非自動メカニズム又は手順を採用する。

管理拡張：(3) ICS 補足ガイダンス：ICS が特権コマンドへのネットワークアクセス制御に対応していない状況では、全体的なカスタマイズガイダンスに従って、組織は非自動メカニズム又は手順を採用する。

管理拡張：(5) ICS 補足ガイダンス：ICS が特権アカウントへのアクセス制御に対応していない状況では、全体的なカスタマイズガイダンスに従って、組織は非自動メカニズム又は手順を採用する。

管理拡張：(9) ICS 補足ガイダンス：総じて、監査記録処理は ICS で行われず、別個の情報システムで行われる。補償的管理策の例として、別個の情報システムへの監査能力の付与がある。

管理拡張：(10) ICS 補足ガイダンス：補償的管理策の例として、拡張監査がある。

AC-7 ログイン失敗

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-7	ログイン失敗	選定	選定	選定

ICS 補足ガイダンス：多くの ICS は電源を入れたままにしなければならず、操作員も常時システムにログオン状態を維持している。「ログオーバー」機能を採用できる。補償的管理策の例として、全てログイン失敗時のログ又は記録を取り、予め決めた連続失敗数に達すると、ICS セキュリティ担当者にアラームその他の手段で警報を送るようにできる。

AC-8 システム利用通知

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-8	システム利用通知	選定	選定	選定

ICS 補足ガイダンス：多くの ICS は電源を入れたままにしておかなければならず、システム利用通知は対応しないか効果的でない。補償的管理策の例として、ICS 施設内に通知を掲示する方法がある。

AC-10 同時セッション管理

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-10	同時セッション管理			選定

ICS 補足ガイダンス：同時セッションの番号、アカウントタイプ及び特権には、影響を受ける個人の役割と責任を考慮に入れる。補償的管理策の例として、監査手段の強化がある。

AC-11 SESSION LOCK

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-11	**Session Lock**		Selected	Selected
AC-11 (1)	*SESSION LOCK | PATTERN-HIDING DISPLAYS*		Selected	Selected

ICS Supplemental Guidance: This control assumes a staffed environment where users interact with information system displays. When this assumption does not apply the organization tailors the control appropriately (e.g., the ICS may be physically protected by placement in a locked enclosure). The control may also be tailored for ICS that are not configured with displays, but which have the capability to support displays (e.g., ICS to which a maintenance technician may attach a display). In some cases, session lock for ICS operator workstations/nodes is not advised (e.g., when immediate operator responses are required in emergency situations). Example compensating controls include locating the display in an area with physical access controls that limit access to individuals with permission and need-to-know for the displayed information.

Control Enhancement: (1) ICS Supplemental Guidance: ICS may employ physical protection to prevent access to a display or to prevent attachment of a display. In situations where the ICS cannot conceal displayed information, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-12 SESSION TERMINATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-12	**Session Termination**		Selected	Selected

ICS Supplemental Guidance: Example compensating controls include providing increased auditing measures or limiting remote access privileges to key personnel.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-14	**Permitted Actions without Identification or Authentication**		Selected	Selected

No ICS Supplemental Guidance.

AC-17 REMOTE ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-17	**Remote Access**	Selected	Selected	Selected
AC-17 (1)	*REMOTE ACCESS | AUTOMATED MONITORING / CONTROL*		Selected	Selected
AC-17 (2)	*REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY / INTEGRITY USING ENCRYPTION*		Selected	Selected
AC-17 (3)	*REMOTE ACCESS | MANAGED ACCESS CONTROL POINTS*		Selected	Selected
AC-17 (4)	*REMOTE ACCESS | PRIVILEGED COMMANDS / ACCESS*		Selected	Selected

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (1) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures as compensating controls (e.g., following manual authentication [see IA-2], dial-in remote access may be enabled for a specified period of time or a call may be placed from the ICS site to the authenticated remote entity.

AC-11 セッションロック

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-11	**セッションロック**		選定	選定
AC-11 (1)	*セッションロック パターン非表示*		選定	選定

ICS 補足ガイダンス：この管理は、ユーザが情報システムディスプレイとやり取りを行う有人環境を想定している。想定と異なる環境では、組織は管理を適切にカスタマイズする（鍵のかかるキャビネットなど ICS の物理的保護等）。補償的管理策の例として、ディスプレイが設定されていないものの、接続しようと思えばできる ICS のカスタマイズがある（保守技術者によるディスプレイの設置等）。場合によっては、ICS 操作員ワークステーション/ノードのセッションロックが推奨できないこともある（緊急時に操作員の即時対応が必要等）。補償的管理策の例として、権限があり表示情報を知る必要のある人員だけが立入できる場所に、ディスプレイを設置することがある。

管理拡張：(1) ICS 補足ガイダンス：ディスプレイへのアクセスやディスプレイの接続を防止する物理的保護を採用できる。ICS が表示情報を隠蔽できない状況では、全体的なカスタマイズガイダンスに従って、組織は非自動メカニズム又は手順を補償的管理策として採用する。

AC-12 セッション終了

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-12	**セッション終了**		選定	選定

ICS 補足ガイダンス：補償的管理策の例として、監査手段の強化やリモートアクセス特権を重要な人員に制限する方法がある。

AC-14 識別・認証のない許可された行為

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-14	**識別・認証のない許可された行為**		選定	選定

ICS 補足ガイダンスなし

AC-17 リモートアクセス

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-17	**リモートアクセス**	選定	選定	選定
AC-17 (1)	*リモートアクセス | 自動監視・管理*		選定	選定
AC-17 (2)	*リモートアクセス | 暗号化による機密性・完全性の保護*		選定	選定
AC-17 (3)	*リモートアクセス | 管理アクセス制御ポイント*		選定	選定
AC-17 (4)	*リモートアクセス | 特権コマンド・アクセス*		選定	選定

ICS 補足ガイダンス：ICS がこの管理要素の一部又は全部を実行できない状況では、全体的なカスタマイズガイダンスに従って、組織は非自動メカニズム又は手順を補償的管理策として採用する。

管理拡張：(1) ICS 補足ガイダンス：補償的管理策の例として、非自動メカニズム又は手順を補償的管理策として採用できる（手動認証に従い[IA-2 参照]、ダイアルインリモートアクセスを一定期間有効にするか、発呼を ICS サイトから認証済み遠隔機関に移設するなど）。

Control Enhancement: (2) ICS Supplemental Guidance: ICS security objectives often rank confidentiality below availability and integrity. The organization explores all possible cryptographic mechanism (e.g., encryption, digital signature, hash function). Each mechanism has a different delay impact. Example compensating controls include providing increased auditing for remote sessions or limiting remote access privileges to key personnel).

Control Enhancement: (3) ICS Supplemental Guidance: Example compensating controls include connection-specific manual authentication of the remote entity.

Control Enhancement: (4) No ICS Supplemental Guidance.

ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-18 WIRELESS ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-18	**Wireless Access**	Selected	Selected	Selected
AC-18 (1)	*WIRELESS ACCESS | AUTHENTICATION AND ENCRYPTION*		Selected	Selected
AC-18 (4)	*WIRELESS ACCESS | RESTRICT CONFIGURATIONS BY USERS*			Selected
AC-18 (5)	*WIRELESS ACCESS | CONFINE WIRELESS COMMUNICATIONS*			Selected

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (1) ICS Supplemental Guidance: See AC-17 Control Enhancement: (1) ICS Supplemental Guidance. Example compensating controls include providing increased auditing for wireless access or limiting wireless access privileges to key personnel.

Control Enhancement: (4) (5) No ICS Supplemental Guidance.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-19	**Access Control for Mobile Devices**	Selected	Selected	Selected
AC-19 (5)	*ACCESS CONTROL FOR MOBILE DEVICES | FULL DEVICE / CONTAINER-BASED ENCRYPTION*		Selected	Selected

No ICS Supplemental Guidance.

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-20	**Use of External Information Systems**	Selected	Selected	Selected
AC-20 (1)	*USE OF EXTERNAL INFORMATION SYSTEMS | LIMITS ON AUTHORIZED USE*		Selected	Selected
AC-20 (2)	*USE OF EXTERNAL INFORMATION SYSTEMS | PORTABLE STORAGE MEDIA*		Selected	Selected

ICS Supplemental Guidance: Organizations refine the definition of “external” to reflect lines of authority and responsibility; granularity of organization entity; and their relationships. An organization may consider a system to be external if that system performs different functions, implements different policies, comes under different managers, or does not provide sufficient visibility into the implementation of security controls to allow the establishment of a satisfactory trust relationship. For example, a process control system and a business data processing system would typically be considered external to each other. Access to an ICS for support by a business partner, such as a vendor or support contractor, is another common example. The definition and trustworthiness of external information systems is reexamined with respect to ICS functions, purposes, technology, and limitations to

管理拡張：(2) ICS 補足ガイダンス：ICS のセキュリティ目標では、機密性が可用性及び完全性よりも下位にランクされることが多い。組織はあらゆる暗号メカニズムを活用する（暗号化、デジタル署名、ハッシュ関数等）。各メカニズムの遅延影響はそれぞれ異なる。補償的管理策の例として、遠隔セッションに対する監査の強化やリモートアクセス特権を重要な人員に制限する方法がある。

管理拡張：(3) ICS 補足ガイダンス：補償的管理策の例として、遠隔機関の接続固有の手動認証がある。

管理拡張：(4) ICS 補足ガイダンスなし

ICS 補足ガイダンス：補償的管理策の例として、全体的なカスタマイズガイダンスに従って、非自動メカニズム又は手順を補償的管理策として採用できる。

AC-18 ワイヤレスアクセス

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-18	**ワイヤレスアクセス**	選定	選定	選定
AC-18 (1)	*ワイヤレスアクセス | 認証・暗号化*		選定	選定
AC-18 (4)	*ワイヤレスアクセス | ユーザ設定の制限*			選定
AC-18 (5)	*ワイヤレスアクセス | ワイヤレス通信の封じ込め*			選定

ICS 補足ガイダンス：ICS がこの管理要素の一部又は全部を実行できない状況では、全体的なカスタマイズガイダンスに従って、組織は他のメカニズム又は手順を補償的管理策として採用する。

管理拡張：(1) ICS 補足ガイダンス：AC-17 管理拡張を参照：(1) ICS 補足ガイダンス。補償的管理策の例として、ワイヤレスアクセスに対する監査の強化やワイヤレスアクセス特権を重要な人員に制限する方法がある。

管理拡張：(4) (5) ICS 補足ガイダンスなし

AC-19 モバイルデバイス用アクセス制御

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-19	**モバイルデバイス用アクセス制御**	選定	選定	選定
AC-19 (5)	**モバイルデバイス用アクセス制御** | *フルデバイス/コンテナベース暗号化*		選定	選定

ICS 補足ガイダンスなし

AC-20 外部情報システムの利用

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-20	**外部情報システムの利用**	選定	選定	選定
AC-20 (1)	*外部情報システムの利用 | 許可された利用の制限*		選定	選定
AC-20 (2)	*外部情報システムの利用 | 携行ストレージメディア*		選定	選定

ICS 補足ガイダンス：「外部」の定義を精査して、権限・責任、組織実体の粒度及びそれらの関係を反映する。あるシステムが違う機能を実行し、違うポリシーを採用し、管理者が違い、満足できる信頼関係を築くためのセキュリティ対策の可視化が不十分な場合、組織はそれを外部とみなせる。例えば、プロセス制御システムと事業用データ処理システムは、通常相互に外部とみなされる。ベンダーやサポート契約者等、事業提携者からの支援で ICS にアクセスする場合も、よくある外部の例である。ICS の機能、目的、技術及び制限に関して、外部情報システムの定義と信頼性を再検証し、

establish a clear documented technical or business case for use and an acceptance of the risk inherent in the use of an external information system.

Control Enhancement: (1, 2) No ICS Supplemental Guidance.

AC-21 INFORMATION SHARING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-21	**Collaboration and Information Sharing**	Added	Selected	Selected

ICS Supplemental Guidance: The organization should collaborate and share information about potential incidents on a timely basis. The DHS National Cybersecurity & Communications Integration Center (NCCIC), http://www.dhs.gov/about-national-cybersecurity-communications-integration-center serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) http://ics-cert.us-cert.gov/ics-cert/ collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. Organizations should consider having both an unclassified and classified information sharing capability.

Rationale for adding AC-21 to low baseline: ICS systems provide essential services and control functions and are often connected to other ICS systems or business systems that can be vectors of attack. It is therefore necessary to provide a uniform defense encompassing all baselines.

AC-22 PUBLICLY ACCESSIBLE CONTENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-22	**Publicly Accessible Content**	Selected	Selected	Selected

ICS Supplemental Guidance: Generally, public access to ICS systems is not permitted. Selected information may be transferred to a publicly accessible information system, possibly with added controls (e.g., introduction of fuzziness or delay).

外部情報システムの利用と、利用に伴うリスクを受け入れる旨の明確な技術・事業文書を作成する。

管理拡張：(1) (2) ICS 補足ガイダンスなし

AC-21 情報共有

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-21	**連携・情報共有**	追加	選定	選定

ICS 補足ガイダンス：組織は、生じ得るインシデントに関して、連携し情報を適時に共有すべきである。下記 DHS 国家サイバーセキュリティ通信統合センター(NCCIC)は集中所在地として機能し、サイバーセキュリティと通信の信頼性に関わる運用要素はそこで調整され、統合化されている。http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

下記産業用制御システムサイバー緊急対応チーム(ICS-CERT)は、海外及び民間のコンピュータ緊急対応チーム(CERT)と連携して、制御システム関連セキュリティインシデント情報と緩和対策を共有している。

http://ics-cert.us-cert.gov/ics-cert/

組織は、秘密情報と普通情報の共有化について検討すべきである。

AC-21 を低ベースラインに追加する理由：ICS システムは、重要なサービスと制御機能を提供しており、攻撃経路となり得る他の ICS システムや事業システムに接続していることが多い。したがって、全てのベースラインを網羅した統一的な防御が必要となる。

AC-22 公開コンテンツ

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AC-22	**公開コンテンツ**	選定	選定	選定

ICS 補足ガイダンス：一般的に、ICS システムへの公開アクセスは許可されていない。選別した情報が、付加的な管理制限（曖昧さや遅れ等）を加えた上で、公開の情報システムに転送されることもある。

AWARENESS AND TRAINING – AT

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AT-1	**Security Awareness and Training Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

AT-2 SECURITY AWARENESS TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AT-2	**Security Awareness**	Selected	Selected	Selected

ICS Supplemental Guidance: Security awareness training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security awareness program is consistent with the requirements of the security awareness and training policy established by the organization.

Control Enhancement: (2) No ICS Supplemental Guidance.

AT-3 ROLE-BASED SECURITY TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AT-3	**Role-Based Security Training**	Selected	Selected	Selected

ICS Supplemental Guidance: Security training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security training program is consistent with the requirements of the security awareness and training policy established by the organization.

AT-4 SECURITY TRAINING RECORDS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AT-4	**Security Training Records**	Selected	Selected	Selected

No ICS Supplemental Guidance.

意識・訓練 – AT

補足ガイダンス

利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

AT-1　セキュリティ意識・訓練ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AT-1	セキュリティ意識・訓練ポリシー・手順	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

AT-2　セキュリティ意識訓練

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AT-2	セキュリティ意識	選定	選定	選定

ICS 補足ガイダンス：セキュリティ意識訓練には、ICS 固有ポリシー、標準運用手順、セキュリティ動向及び脆弱性に対する当初の訓練と定期的な復習が含まれる。ICS セキュリティ意識プログラムは、組織が設定したセキュリティ意識・訓練ポリシー要件と整合している。

管理拡張：(2) ICS 補足ガイダンスなし

AT-3　役割ベースセキュリティ訓練

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AT-3	役割ベースセキュリティ訓練	選定	選定	選定

ICS 補足ガイダンス：セキュリティ訓練には、ICS 固有ポリシー、標準運用手順、セキュリティ動向及び脆弱性に対する当初の訓練と定期的な復習が含まれる。ICS セキュリティプログラムは、組織が設定したセキュリティ意識・訓練ポリシー要件と整合している。

AT-4　セキュリティ訓練記録

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AT-4	セキュリティ訓練記録	選定	選定	選定

ICS 補足ガイダンスなし

AUDITING AND ACCOUNTABILITY – AU

Tailoring Considerations for Audit Family

In general, audit information and audit tools are not present on legacy ICS, but on a separate information system (e.g., the historian). In situations where the ICS cannot support the specific Audit and Accountability requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-1	**Audit and Accountability Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

AU-2 AUDIT EVENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-2	**Auditable Events**	Selected	Selected	Selected
AU-2 (3)	*AUDITABLE EVENTS | REVIEWS AND UPDATES*		Selected	Selected

ICS Supplemental Guidance: The organization may designate ICS events as audit events, requiring that ICS data and/or telemetry be recorded as audit data.

Control Enhancement: (3) No ICS Supplemental Guidance.

AU-3 CONTENT OF AUDIT RECORDS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-3	**Content of Audit Records**	Selected	Selected	Selected
AU-3 (1)	*CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*		Selected	Selected
AU-3 (2)	*CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*			Selected

ICS Supplemental Guidance: Example compensating controls include providing an auditing capability on a separate information system.

Control Enhancement: (1, 2) No ICS Supplemental Guidance.

AU-4 AUDIT STORAGE CAPACITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-4	**Audit Storage Capacity**	Selected	Selected	Selected
AU-4 (1)	*AUDIT STORAGE CAPACITY | TRANSFER TO ALTERNATE STORAGE*	Added	Added	Added

No ICS Supplemental Guidance.

Control Enhancement: (1) ICS Supplemental Guidance: Legacy ICS are typically configured with remote storage on a separate information system (e.g., the historian accumulates historical operational ICS data and is backed up for

監査・説明責任 – AU

監査ファミリのカスタマイズ考慮事項

一般に、監査情報や監査ツールは、レガシーICS にはないが、別個の情報システム上にある（ヒストリアン等）。ICS がある制御の特定の監査・説明責任要件に対応していない状況では、全体的なカスタマイズガイダンスに従って補償的管理策を採用する。補償的管理策の例が必要に応じて、管理策ごとに示される。

補足ガイダンス

利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

AU-1 監査・説明責任ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AU-1	**監査・説明責任ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

AU-2 監査事象

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AU-2	**監査事象**	選定	選定	選定
AU-2 (3)	*監査事象 | 審査・更新*		選定	選定

ICS 補足ガイダンス：組織は ICS 事象を監査事象と指定し、ICS データやテレメトリ-を監査データとしての記録を義務づける。

管理拡張：(3) ICS 補足ガイダンスなし

AU-3 監査記録内容

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AU-3	**監査記録内容**	選定	選定	選定
AU-3 (1)	*監査記録内容| 補足監査情報*		選定	選定
AU-3 (2)	*監査記録内容 | 計画監査記録内容の集中管理*			選定

ICS 補足ガイダンス：補償的管理策の例として、別個の情報システムへの監査能力の付与がある。

管理拡張：(1) (2) ICS 補足ガイダンスなし

AU-4 監査ストレージ容量

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AU-4	**監査ストレージ容量**	選定	選定	選定
AU-4 (1)	*監査ストレージ容量 | 代替ストレージへの移行*	追加	追加	追加

ICS 補足ガイダンスなし

管理拡張：(1) ICS 補足ガイダンス：通常レガシーICS は、別個の情報システム上の遠隔ストレージに設定がある（ヒストリアンは ICS の運用履歴データを蓄積し、別サイトのストレージに保管する）。

storage at a different site). ICS are currently using online backup services and increasingly moving to Cloud based and Virtualized services. Retention of some data (e.g., SCADA telemetry) may be required by regulatory authorities.

Rationale for adding AU-4 (1) to all baselines: Legacy ICS components typically do not have capacity to store or analyze audit data. The retention periods for some data, particularly compliance data, may require large volumes of storage.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-5	**Response to Audit Processing Failures**	Selected	Selected	Selected
AU-5 (1)	*RESPONSE TO AUDIT PROCESSING FAILURES | AUDIT STORAGE CAPACITY*			Selected
AU-5 (2)	*RESPONSE TO AUDIT PROCESSING FAILURES | REAL-TIME ALERTS*			Selected

No ICS Supplemental Guidance.

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-6	**Audit Review, Analysis, and Reporting**	Selected	Selected	Selected
AU-6 (1)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | PROCESS INTEGRATION*		Selected	Selected
AU-6 (3)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES*		Selected	Selected
AU-6 (5)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | INTEGRATION / SCANNING AND MONITORING CAPABILITIES*			Selected
AU-6 (6)	*AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING*			Selected

No ICS Supplemental Guidance.

Control Enhancement: (1) ICS Supplemental Guidance: Example compensating controls include manual mechanisms or procedures.

Control Enhancement: (3, 5, 6) No ICS Supplemental Guidance.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-7	**Audit Reduction and Report Generation**		Selected	Selected
AU-7 (1)	*AUDIT REDUCTION AND REPORT GENERATION | AUTOMATIC PROCESSING*		Selected	Selected

No ICS Supplemental Guidance.

Control Enhancement: (1) No ICS Supplemental Guidance.

AU-8 TIME STAMPS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-8	**Time Stamps**	Selected	Selected	Selected
AU-8 (1)	*TIME STAMPS | SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE*		Selected	Selected

ICS Supplemental Guidance: Example compensating controls include using a separate information system designated as an authoritative time source.

Control Enhancement: (1) ICS Supplemental Guidance: ICS employ suitable mechanisms (e.g., GPS, IEEE 1588) for time stamps.

ICS は今のところオンラインバックアップサービスを利用しているが、クラウドベースの仮想サービスに次第に移行している。特定のデータ（SCADA テレメトリー等）の保持が規制当局から義務づけられる場合がある。

AU-4 (1)を全てのベースラインに追加する理由：一般にレガシーICS コンポーネントには、監査データの保存又は分析容量がない。特定のデータ、特にコンプライアンスデータの保持期間によって保管量が大きくなる。

AU-5　監査処理不備への対応

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AU-5	**監査処理不備への対応**	選定	選定	選定
AU-5 (1)	*監査処理不備への対応 | 監査ストレージ容量*			選定
AU-5 (2)	*監査処理不備への対応 | リアルタイム警報*			選定

ICS 補足ガイダンスなし

AU-6　監査の審査・分析・報告

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AU-6	**監査の審査・分析・報告**	選定	選定	選定
AU-6 (1)	*監査の審査・分析・報告 | プロセスの一体化*		選定	選定
AU-6 (3)	*監査の審査・分析・報告 | 監査レポジトリの相関*		選定	選定
AU-6 (5)	*監査の審査・分析・報告 | 一体化スキャン・監視能力*			選定
AU-6 (6)	*監査の審査・分析・報告 | 物理的監視との相関*			選定

ICS 補足ガイダンスなし

管理拡張：(1) ICS 補足ガイダンス：補償的管理策の例として、手動メカニズム又は手順がある。

管理拡張：(3, 5, 6) ICS 補足ガイダンスなし

AU-7　監査削減・報告書作成

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AU-7	**監査削減・報告書作成**		選定	選定
AU-7 (1)	*監査削減・報告書作成 | 自動処理*		選定	選定

ICS 補足ガイダンスなし

管理拡張：(1) ICS 補足ガイダンスなし

AU-8　タイムスタンプ

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AU-8	**タイムスタンプ**	選定	選定	選定
AU-8 (1)	*タイムスタンプ | 公認時間ソースとの同期*		選定	選定

ICS 補足ガイダンス：補償的管理策の例として、公認時間ソースに指定された別個の情報システムを利用する方法がある。

管理拡張：(1) ICS 補足ガイダンス：タイムスタンプとして、ICS では適正なメカニズムを採用する（全地球測位システム[GPS]、IEEE 1588 等）。

AU-9 PROTECTION OF AUDIT INFORMATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-9	**Protection of Audit Information**	Selected	Selected	Selected
AU-9 (2)	*PROTECTION OF AUDIT INFORMATION | AUDIT BACKUP ON SEPARATE PHYSICAL SYSTEMS / COMPONENTS*			Selected
AU-9 (3)	*PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION*			Selected
AU-9 (4)	*PROTECTION OF AUDIT INFORMATION | ACCESS BY SUBSET OF PRIVILEGED USERS*		Selected	Selected

No ICS Supplemental Guidance.

AU-10 NON-REPUDIATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-10	**Non-repudiation**			Selected

ICS Supplemental Guidance: Example compensating controls include providing non-repudiation on a separate information system.

AU-11 AUDIT RECORD RETENTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-11	**Audit Record Retention**	Selected	Selected	Selected

No ICS Supplemental Guidance.

AU-12 AUDIT GENERATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-12	**Audit Generation**	Selected	Selected	Selected
AU-12 (1)	*AUDIT GENERATION | SYSTEM-WIDE / TIME-CORRELATED AUDIT TRAIL*			Selected
AU-12 (3)	*AUDIT GENERATION | CHANGES BY AUTHORIZED INDIVIDUALS*			Selected

No ICS Supplemental Guidance.

Control Enhancement: (1) ICS Supplemental Guidance: Example compensating controls include providing time-correlated audit records on a separate information system.

Control Enhancement: (3) ICS Supplemental Guidance: Example compensating controls include employing nonautomated mechanisms or procedures.

AU-9 監査情報の保護

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AU-9	**監査情報の保護**	選定	選定	選定
AU-9 (2)	*監査情報の保護 | 別の物理システム/コンポーネントへの監査バックアップ*			選定
AU-9 (3)	*監査情報の保護 | 暗号化保護*			選定
AU-9 (4)	*監査情報の保護 | 特権ユーザのサブセットによるアクセス*		選定	選定

ICS 補足ガイダンスなし

AU-10 否認防止

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AU-10	**否認防止**			選定

ICS 補足ガイダンス：補償的管理策の例として、別個の情報システムへの否認防止機能の付与がある。

AU-11 監査記録保持

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AU-11	**監査記録保留**	選定	選定	選定

ICS 補足ガイダンスなし

AU-12 監査作成

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
AU-12	**監査作成**	選定	選定	選定
AU-12 (1)	*監査作成 | 全システム | 時間相関監査証跡*			選定
AU-12 (3)	*監査作成 | 権限ある個人による変更*			選定

ICS 補足ガイダンスなし

管理拡張：(1) ICS 補足ガイダンス：補償的管理策の例として、別個の情報システムへの時間相関監査記録の付与がある。

管理拡張：(3) ICS 補足ガイダンス：補償的管理策の例として、非自動メカニズム又は手順がある。

SECURITY ASSESSMENT AND AUTHORIZATION – CA

Tailoring Considerations for Security Assessment and Authorization Family

In situations where the ICS cannot support the specific Security Assessment and Authorization requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-1	**Security Assessment and Authorization Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

CA-2 SECURITY ASSESSMENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-2	**Security Assessments**	Selected	Selected	Selected
CA-2 (1)	*SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS*		Selected	Selected
CA-2 (2)	*SECURITY ASSESSMENTS | TYPES OF ASSESSMENTS*			Selected

ICS Supplemental Guidance: Assessments are performed and documented by qualified assessors (i.e., experienced in assessing ICS) authorized by the organization. The organization ensures that assessments do not interfere with ICS functions. The individual/group conducting the assessment fully understands the organizational information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. The organization ensures that the assessment does not affect system operation or result in unintentional system modification. If assessment activities must be performed on the production ICS, it may need to be taken off-line before an assessment can be conducted. If an ICS must be taken off-line to conduct an assessment, the assessment is scheduled to occur during planned ICS outages whenever possible.

Control Enhancement: (1) No ICS Supplemental Guidance.

Control Enhancement: (2) ICS Supplemental Guidance: The organization conducts risk analysis to support the selection of assessment target (e.g., the live system, an off-line replica, a simulation).

CA-3 SYSTEM INTERCONNECTIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-3	**Information System Connections**	Selected	Selected	Selected
CA-3 (5)	*SYSTEM INTERCONNECTIONS | RESTRICTIONS ON EXTERNAL SYSTEM CONNECTIONS*			Selected

ICS Supplemental Guidance: Organizations perform risk-benefit analysis to support determination whether an ICS should be connected to other information system(s). The Authorizing Official fully understands the organizational information security policies and procedures; the ICS security policies and procedures; the risks to organizational operations and assets, individuals, other organizations, and the Nation associated with the connection to other information system(s); and the specific health, safety, and environmental risks associated with a particular interconnection. The AO documents risk acceptance in the ICS system security plan.

Control Enhancement: (5) No ICS Supplemental Guidance.

セキュリティ評価・権限付与 – CA

セキュリティ評価・権限付与ファミリのカスタマイズ考慮事項

ICS がある制御の特定のセキュリティ評価・権限付与要件に対応していない状況では、全体的なカスタマイズガイダンスに従って補償的管理策を採用する。補償管理の例が必要に応じて、管理策ごとに示される。

補足ガイダンス

利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

CA-1　セキュリティ評価・権限付与ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CA-1	**セキュリティ評価・権限付与ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

CA-2　セキュリティ評価

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CA-2	**セキュリティ評価**	選定	選定	選定
CA-2 (1)	*セキュリティ評価 | 独立評価者*		選定	選定
CA-2 (2)	*セキュリティ評価 | 評価の種類*			選定

ICS 補足ガイダンス：有資格者（ICS 評価熟練者）による評価を行い文書化し、組織の承認を得る。評価が ICS 機能と干渉しないようにする。評価を行う個人やグループは、組織の情報セキュリティポリシー・手順、ICS のセキュリティポリシー・手順及び特定の施設やプロセスに付随する具体的な健康・安全・環境リスクを十分理解する。組織は評価によってシステム運用が影響を受けず、意図しないシステム変更にならないようにする。評価活動を生産 ICS で実施しなければならない場合、評価の実施前にオフラインにする必要がある場合がある。オフラインにしなければならない場合、可能であれば、予め計画された ICS の操業停止時に評価を行うように予定を組む。

管理拡張：(1) ICS 補足ガイダンスなし

管理拡張：(2) ICS 補足ガイダンス：組織はリスク分析を行い、評価対象の選別を支援する（ライブシステム、オフラインレプリカ、シミュレーション等）。

CA-3　システム連接

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CA-3	**情報システムの接続**	選定	選定	選定
CA-3 (5)	*システム連接 | 外部システムとの接続制限*		選定	選定

ICS 補足ガイダンス：組織はリスク便益分析を行い、ICS と他の情報システムとの接続の是非を判断する。許可権者は、次の事項について十分理解する。組織の情報セキュリティポリシー・手順。ICS のセキュリティポリシー・手順。他の情報システムへの接続に付随する組織の運用、資産、個人、他の組織及び国に対するリスク。特定の連接に付随する具体的な健康・安全・環境リスク。AO は、ICS システムセキュリティ計画書におけるリスク受容性について記載している。

管理拡張：(5) ICS 補足ガイダンスなし

CA-5 PLAN OF ACTION AND MILESTONES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-5	**Plan of Action and Milestones**	Selected	Selected	Selected

No ICS Supplemental Guidance.

CA-6 SECURITY AUTHORIZATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-6	**Security Authorization**	Selected	Selected	Selected

No ICS Supplemental Guidance.

CA-7 CONTINUOUS MONITORING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-7	**Continuous Monitoring**	Selected	Selected	Selected
CA-7 (1)	*CONTINUOUS MONITORING | INDEPENDENT ASSESSMENT*		Selected	Selected

ICS Supplemental Guidance: Continuous monitoring programs for ICS are designed, documented, and implemented by qualified personnel (i.e., experienced with ICS) selected by the organization. The organization ensures that continuous monitoring does not interfere with ICS functions. The individual/group designing and conducting the continuous monitoring fully understands the organizational information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. The organization ensures that continuous monitoring does not affect system operation or result in intentional or unintentional system modification. Example compensating controls include external monitoring.

Control Enhancement: (1) No ICS Supplemental Guidance.

CA-8 PENETRATION TESTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-8	**Penetration Testing**			Selected

ICS Supplemental Guidance: Penetration testing is used with care on ICS networks to ensure that ICS functions are not adversely impacted by the testing process. In general, ICS are highly sensitive to timing constraints and have limited resources. Example compensating controls include employing a replicated, virtualized, or simulated system to conduct penetration testing. Production ICS may need to be taken off-line before testing can be conducted. If ICS are taken off-line for testing, tests are scheduled to occur during planned ICS outages whenever possible. If penetration testing is performed on non-ICS networks, extra care is taken to ensure that tests do not propagate into the ICS network.

CA-5 行動・マイルストーン計画書

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CA-5	**行動・マイルストーン計画書**	選定	選定	選定

ICS 補足ガイダンスなし

CA-6 セキュリティ権限

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CA-6	**セキュリティ権限**	選定	選定	選定

ICS 補足ガイダンスなし

CA-7 継続監視

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CA-7	**継続監視**	選定	選定	選定
CA-7 (1)	*継続監視 | 独立評価*		選定	選定

ICS 補足ガイダンス：ICS の継続監視は、組織が選任した有資格者が考案し、文書化し、実施する（ICS の熟練者等）。継続監視が ICS 機能と干渉しないようにする。継続監視を考案して実施する個人やグループは、組織の情報セキュリティポリシー・手順、ICS のセキュリティポリシー・手順及び特定の計津やプロセスに付随する具体的な健康・安全・環境リスクを十分理解する。組織は継続監視によってシステム運用が影響を受けず、故意又は意図しないシステム変更にならないようにする。補償的管理策の例として、外部監視がある。

管理拡張：(1) ICS 補足ガイダンスなし

CA-8 ペネトレーション・テスト

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CA-8	**ペネトレーション・テスト**			選定

ICS 補足ガイダンス：ICS ネットワークでのペネトレーション・テストは慎重に行い、試験プロセスにより ICS 機能に悪影響が及ばないようにする。総じて ICS は、時間的制約に敏感で、リソースに限界がある。補償的管理策の例として、複製、仮想又は模擬システムでペネトレーション・テストを行う方法がある。生産 ICS は、試験前にオフラインにする必要がある。オフラインにする場合、可能であれば、予め計画された ICS の操業停止時に試験を行うように予定を組む。ペネトレーション・テストを ICS 以外のネットワークで行う場合、試験が ICS に持ち込まれないように注意する。

CA-9 INTERNAL SYSTEM CONNECTIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CA-9	**Internal System Connections**	Selected	Selected	Selected

ICS Supplemental Guidance: Organizations perform risk-benefit analysis to support determination whether an ICS should be connected to other internal information system(s) and (separate) constituent system components. The Authorizing Official fully understands the organizational information security policies and procedures; the ICS security policies and procedures; the risks to organizational operations and assets, individuals, other organizations, and the Nation associated with the connected to other information system(s) and (separate) constituent system components, whether by authorizing each individual internal connection or authorizing internal connections for a class of components with common characteristics and/or configurations; and the specific health, safety, and environmental risks associated with a particular interconnection. The AO documents risk acceptance in the ICS system security plan.

CA-9 内部システム接続

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CA-9	内部システム接続	選定	選定	選定

ICS 補足ガイダンス：組織はリスク便益分析を行い、ICS と他の内部情報システムや（別）構成システムコンポーネントとの接続の是非を判断する。許可権者は、次の事項について十分理解する。組織の情報セキュリティポリシー・手順。ICS のセキュリティポリシー・手順。個々人の内部接続を許可するか、共通特性・設定のコンポーネントクラスへの内部接続を許可することにより、他の情報システム及び（別）構成システムコンポーネントへの接続に伴う組織の運用、資産、個人、他の組織及び国に対するリスク。特定の連接に付随する具体的な健康・安全・環境リスク。AO は、ICS システムセキュリティ計画書におけるリスク受容性について記載している。

CONFIGURATION MANAGEMENT – CM

Tailoring Considerations for Configuration Management Family

In situations where the ICS cannot be configured to restrict the use of unnecessary functions or cannot support the use of automated mechanisms to implement configuration management functions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance
Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-1	**Configuration Management Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

CM-2 BASELINE CONFIGURATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-2	**Baseline Configuration**	Selected	Selected	Selected
CM-2 (1)	*BASELINE CONFIGURATION | REVIEWS AND UPDATES*		Selected	Selected
CM-2 (2)	*BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY*			Selected
CM-2 (3)	*BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS*		Selected	Selected
CM-2 (7)	*BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS*		Selected	Selected

No ICS Supplemental Guidance.

CM-3 CONFIGURATION CHANGE CONTROL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-3	**Configuration Change Control**		Selected	Selected
CM-3 (1)	*CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT / NOTIFICATION / PROHIBITION OF CHANGES*			Selected
CM-3 (2)	*CONFIGURATION CHANGE CONTROL | TEST / VALIDATE / DOCUMENT CHANGES*		Selected	Selected

No ICS Supplemental Guidance.

CM-4 SECURITY IMPACT ANALYSIS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-4	**Security Impact Analysis**	Selected	Selected	Selected
CM-4 (1)	*SECURITY IMPACT ANALYSIS | SEPARATE TEST ENVIRONMENTS*			Selected

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies.
Control Enhancement: (1) No ICS Supplemental Guidance.

設定管理 – CM

設定管理ファミリのカスタマイズ考慮事項

ICS で不要な機能の制限や設定管理機能の自動メカニズムの利用ができない状況では、全体的なカスタマイズガイダンスに従って、組織は非自動メカニズム又は手順を補償的管理策として採用する。補償的管理策の例が必要に応じて、管理策ごとに示される。

補足ガイダンス

利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

CM-1　設定管理ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CM-1	**設定管理ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

CM-2　ベースライン設定

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CM-2	**ベースライン設定**	選定	選定	選定
CM-2 (1)	*ベースライン設定 | 審査・更新*		選定	選定
CM-2 (2)	*ベースライン設定 | 正確性・カレンシーの自動サポート*			選定
CM-2 (3)	*ベースライン設定 | 以前の設定保持*		選定	選定
CM-2 (7)	*ベースライン設定 | 高リスクエリア用システム・コンポーネント・デバイスの設定*		選定	選定

ICS 補足ガイダンスなし

CM-3　設定変更管理

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CM-3	**設定変更管理**		選定	選定
CM-3 (1)	*設定変更管理 | 自動文書化・通知・変更禁止*			選定
CM-3 (2)	*設定変更管理 | 試験・検証・文書変更*		選定	選定

ICS 補足ガイダンスなし

CM-4　セキュリティ影響分析

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CM-4	**セキュリティ影響分析**	選定	選定	選定
CM-4 (1)	*セキュリティ影響分析 | 独立試験環境*			選定

ICS 補足ガイダンス：組織は ICS の安全性とセキュリティの相互関係を検討する。
管理拡張：(1) ICS 補足ガイダンスなし

CM-5 ACCESS RESTRICTIONS FOR CHANGE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-5	**Access Restrictions for Change**		Selected	Selected
CM-5 (1)	*ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT / AUDITING*			Selected
CM-5 (2)	*ACCESS RESTRICTIONS FOR CHANGE | AUDIT SYSTEM CHANGES*			Selected
CM-5 (3)	*ACCESS RESTRICTIONS FOR CHANGE | SIGNED COMPONENTS*			Selected

No ICS Supplemental Guidance.

CM-6 CONFIGURATION SETTINGS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-6	**Configuration Settings**	Selected	Selected	Selected
CM-6 (1)	*CONFIGURATION SETTINGS | AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION*			Selected
CM-6 (2)	*CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES*			Selected

No ICS Supplemental Guidance.

CM-7 LEAST FUNCTIONALITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-7	**Least Functionality**	Selected	Selected	Selected
CM-7 (1)	*LEAST FUNCTIONALITY | PERIODIC REVIEW*	Added	Selected	Selected
CM-7 (2)	*LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION*		Removed	Selected
CM-7 (4)	*LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE*		Added	Selected

ICS Supplemental Guidance: Ports, as used in NIST SP 800-53 Rev. 4, are part of the address space in network protocols and are often associated with specific protocols or functions. As such, ports are not relevant to non-routable protocols and devices. When dealing with non-routable and non-addressable protocols and devices, prohibiting or restricting the use of specified functions, protocols, and/or services must be implemented for the (sub)system granularity that is available (e.g., at a low level, interrupts could be disabled; at a high level, set points could be made read-only except for privileged users). Example compensating controls include employing nonautomated mechanisms or procedures.

Control Enhancement: (1, 2, 5) No ICS Supplemental Guidance.

Control Baseline Supplement Rationale: (1) Periodic review and removal of unnecessary and/or nonsecure functions, ports, protocols, and services are added to the LOW baseline because many of the LOW impact ICS components could adversely affect the systems to which they are connected.

(4, 5) Whitelisting (CE 5) is more effective than blacklisting (CE 4). The set of applications that run in ICS is essentially static, making whitelisting practical. ICS-CERT recommends deploying application whitelisting on ICS. Reference: http://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-8	**Information System Component Inventory**	Selected	Selected	Selected
CM-8 (1)	*INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS*		Selected	Selected
CM-8 (2)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*			Selected
CM-8 (3)	*INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION*		Selected	Selected

CM-5　変更用アクセス制限

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CM-5	**変更用アクセス制限**		選定	選定
CM-5 (1)	*変更用アクセス制限 | 自動アクセスの施行 / 監査*			選定
CM-5 (2)	*変更用アクセス制限 | 監査システム変更*			選定
CM-5 (3)	*変更用アクセス制限 | 署名コンポーネント*			選定

ICS 補足ガイダンスなし

CM-6　構成設定

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CM-6	**構成設定**	選定	選定	選定
CM-6 (1)	*構成設定 | 自動集中管理アプリケーション / 検証*			選定
CM-6 (2)	*構成設定 | 無断変更対応*			選定

ICS 補足ガイダンスなし

CM-7　最小権限

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CM-7	**最低限機能**	選定	選定	選定
CM-7 (1)	*最低限機能 | 定期的見直し*	追加	選定	選定
CM-7 (2)	*最低限機能 | プログラム実行防止*		削除	選定
CM-7 (4)	*最低限機能 | 未許可ソフトウエア*		追加	選定

ICS 補足ガイダンス：NIST SP 800-53 第 4 版で使用されるポートは、ネットワークプロトコルにおけるアドレス空間の一部で、特定のプロトコルや機能に関連づけられていることが多い。このようなポートは、経路指定不能プロトコル及びデバイスではない。アドレス/ルート指定不能プロトコル及びデバイスの場合、指定機能、プロトコル又はサービス利用の禁止又は制限は、利用できる（サブ）システムの粒度に実装しなければならない（低レベルでは中断を無効にし、高レベルでは設定点を特権ユーザ以外は読み取り専用とするなど）。補償的管理策の例として、非自動メカニズム又は手順がある。-

管理拡張：(1, 2, 5) ICS 補足ガイダンスなし

管理ベースライン補足理由：(1)不要又はセキュアでない機能、ポート、プロトコル及びサービスの定期的な見直しと削除を低ベースラインに追加した。理由は影響度低の ICS コンポーネントの多くは、接続先システムに悪影響を及ぼすため。

(4, 5) ホワイトリスト(CE 5)はブラックリスト(CE 4)よりも効果的。ICS で実行するアプリケーションセットは基本的に静的であるため、ホワイトリストが現実的である。ICS-CERT は、ホワイトリストアプリケーションの ICS 展開を推奨している。参考文献：http://ics-cert.us- cert.gov/tips/ICS-TIP-12-146-01B

CM-8　情報システムコンポーネント目録

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CM-8	**情報システムコンポーネント目録**	選定	選定	選定
CM-8 (1)	*情報システムコンポーネント目録 | インストール・削除時の更新*		選定	選定
CM-8 (2)	*情報システムコンポーネント目録 | 自動保守*			選定
CM-8 (3)	*情報システムコンポーネント目録 | 自動無許可コンポーネント検知*		選定	選定

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-8 (4)	*INFORMATION SYSTEM COMPONENT INVENTORY | PROPERTY ACCOUNTABILITY INFORMATION*			Selected
CM-8 (5)	*INFORMATION SYSTEM COMPONENT INVENTORY | ALL COMPONENTS WITHIN AUTHORIZATION BOUNDARY*		Selected	Selected

No ICS Supplemental Guidance.

CM-9 CONFIGURATION MANAGEMENT PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-9	**Configuration Management Plan**		Selected	Selected

No ICS Supplemental Guidance.

CM-10 SOFTWARE USAGE RESTRICTIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-10	**Software Usage Restrictions**	Selected	Selected	Selected

No ICS Supplemental Guidance.

CM-11 USER-INSTALLED SOFTWARE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-11	**User-Installed Software**	Selected	Selected	Selected

No ICS Supplemental Guidance.

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CM-8 (4)	*情報システムコンポーネント目録 | 資産説明責任情報*			選定
CM-8 (5)	*情報システムコンポーネント目録 | 全コンポーネントが権限内*		選定	選定

ICS 補足ガイダンスなし

CM-9　設定管理計画書

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CM-9	**設定管理計画書**		選定	選定

ICS 補足ガイダンスなし

CM-10　ソフトウエア使用制限

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CM-10	**ソフトウエア使用制限**	選定	選定	選定

ICS 補足ガイダンスなし

CM-11　ユーザがインストールしたソフトウエア

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CM-11	**ユーザがインストールしたソフトウエア**	選定	選定	選定

ICS 補足ガイダンスなし

CONTINGENCY PLANNING - CP

Tailoring Considerations for Contingency Planning Family

ICS systems often contain a physical component at a fixed location. Such components may not be relocated logically. Some replacement components may not be readily available. Continuance of essential missions and business functions with little or no loss of operational continuity may not be possible. In situations where the organization cannot provide necessary essential services, support, or automated mechanisms during contingency operations, the organization provides nonautomated mechanisms or predetermined procedures as compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-1	**Contingency Planning Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

CP-2 CONTINGENCY PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-2	**Contingency Plan**	Selected	Selected	Selected
CP-2 (1)	*CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*		Selected	Selected
CP-2 (2)	*CONTINGENCY PLAN | CAPACITY PLANNING*			Selected
CP-2 (3)	*CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*		Selected	Selected
CP-2 (4)	*CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS*			Selected
CP-2 (5)	*CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS*			Selected
CP-2 (8)	*CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*		Selected	Selected

ICS Supplemental Guidance: The organization defines contingency plans for categories of disruptions or failures. In the event of a loss of processing within the ICS or communication with operational facilities, the ICS executes predetermined procedures (e.g., alert the operator of the failure and then do nothing, alert the operator and then safely shut down the industrial process, alert the operator and then maintain the last operational setting prior to failure).

Control Enhancement: (1) ICS Supplemental Guidance: Organizational elements responsible for related plans may include suppliers such as electric power, fuel, fresh water and wastewater.

Control Enhancement: (2) No ICS Supplemental Guidance.

Control Enhancement: (3, 4) ICS Supplemental Guidance: Plans for the resumption of essential missions and business functions, and for resumption of all missions and business functions take into account the effects of the disruption on the environment of operation. Restoration and resumption plans should include prioritization of efforts. Disruptions may affect the quality and quantity of resources in the environment, such as electric power, fuel, fresh water and wastewater, and the ability of these suppliers to also resume provision of essential mission and business functions. Contingency plans for widespread disruption may involve specialized organizations (e.g., FEMA, emergency services, regulatory authorities). Reference: NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs.

Control Enhancement: (5, 8) No ICS Supplemental Guidance.

不測事態計画 - CP

不測事態計画ファミリのカスタマイズ考慮事項
ICS システムには、定められた場所に物理コンポーネントがある場合が多い。それらは論理的な移動ができない。代わりのコンポーネントがすぐに利用できないものもある。中断がほとんど又は全く許されない重要任務や事業もある。不測事態運用中に、必要な重要サービス、サポート又は自動メカニズムを提供できない状況では、全体的なカスタマイズガイダンスに従って、組織は非自動メカニズム又は事前設定手順を補償的管理策として採用する。補償的管理策の例が必要に応じて、管理策ごとに示される。

補足ガイダンス
利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

CP-1　不測事態計画ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CP-1	**不測事態計画ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

CP-2　緊急時対応計画

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CP-2	**緊急時対応計画**	選定	選定	選定
CP-2 (1)	*緊急時対応計画 | 関連計画書との整合*		選定	選定
CP-2 (2)	*緊急時対応計画 | 容量計画*			選定
CP-2 (3)	*緊急時対応計画 | 重要任務・事業機能の再開*		選定	選定
CP-2 (4)	*緊急時対応計画 | 全任務・事業機能の再開*			選定
CP-2 (5)	*緊急時対応計画 | 重要任務・事業機能の再開*			選定
CP-2 (8)	*緊急時対応計画 | 重要資産識別*		選定	選定

ICS 補足ガイダンス：組織は、中断や故障の分類別に緊急時対応計画を定める。ICS 内での処理や運用施設との通信が失われた場合、ICS は予め定められた手順を実行する（操作員に警報を発信して何もしない、操作員に警報を発信して産業プロセスを安全に遮断する、操作員に警報を発信して故障直前の動作を維持するなど）。

管理拡張：(1) ICS 補足ガイダンス：関連計画書の担当部署には、電力、燃料、上下水道等のサプライヤも含まれる。

管理拡張：(2) ICS 補足ガイダンスなし

管理拡張：(3, 4) ICS 補足ガイダンス：重要任務・事業機能の再開に関する計画書及び全ての任務・事業機能の再開に関する計画書には、運用環境が崩壊した場合の影響を考慮に入れる。復旧・再開計画書には、取組の優先順位を含めるべきである。中断が生じると電力、燃料、上下水道等のリソースの質・量のみならず、重要任務・事業を再開するサプライヤの能力にも影響が出る。大規模中断の緊急時対応計画には、特別組織を含める（FEMA、緊急サービス、規制当局等）。参考文献：NFPA 1600:災害・気球時管理・事業継続プログラムの基準

管理拡張：(5) (8) ICS 補足ガイダンスなし

CP-3 CONTINGENCY TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-3	**Contingency Training**	Selected	Selected	Selected
CP-3 (1)	*CONTINGENCY TRAINING | SIMULATED EVENTS*			Selected

No ICS Supplemental Guidance.

CP-4 CONTINGENCY PLAN TESTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-4	**Contingency Plan Testing**	Selected	Selected	Selected
CP-4 (1)	*CONTINGENCY PLAN TESTING | COORDINATE WITH RELATED PLANS*		Selected	Selected
P-4 (2)	*CONTINGENCY PLAN TESTING | ALTERNATE PROCESSING SITE*			Selected

No ICS Supplemental Guidance.

CP-6 ALTERNATE STORAGE SITE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-6	**Alternate Storage Site**		Selected	Selected
CP-6 (1)	*ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*		Selected	Selected
CP-6 (2)	*ALTERNATE STORAGE SITE | RECOVERY TIME / POINT OBJECTIVES*			Selected
CP-6 (3)	*ALTERNATE STORAGE SITE | ACCESSIBILITY*		Selected	Selected

No ICS Supplemental Guidance.

CP-7 ALTERNATE PROCESSING SITE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-7	**Alternate Processing Site**		Selected	Selected
CP-7 (1)	*ALTERNATE PROCESSING SITE | SEPARATION FROM PRIMARY SITE*		Selected	Selected
CP-7 (2)	*ALTERNATE PROCESSING SITE | ACCESSIBILITY*		Selected	Selected
CP-7 (3)	*ALTERNATE PROCESSING SITE | PRIORITY OF SERVICE*		Selected	Selected
CP-7 (4)	*ALTERNATE PROCESSING SITE | CONFIGURATION FOR USE*			Selected

No ICS Supplemental Guidance.

CP-8 TELECOMMUNICATIONS SERVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-8	**Telecommunications Services**		Selected	Selected
CP-8 (1)	*TELECOMMUNICATIONS SERVICES | PRIORITY OF SERVICE PROVISIONS*		Selected	Selected
CP-8 (2)	*TELECOMMUNICATIONS SERVICES | SINGLE POINTS OF FAILURE*		Selected	Selected
CP-8 (3)	*TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY / ALTERNATE PROVIDERS*			Selected
CP-8 (4)	*TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*			Selected

ICS Supplemental Guidance: Quality of service factors for ICS include latency and throughput.

Control Enhancement: (1, 2, 3, 4) No ICS Supplemental Guidance.

CP-3 不測事態訓練

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CP-3	**不測事態訓練**	選定	選定	選定
CP-3 (1)	*不測事態訓練 | 模擬事象*			選定

ICS 補足ガイダンスなし

CP-4 緊急時対応計画の検証

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CP-4	**緊急時対応計画の検証**	選定	選定	選定
CP-4 (1)	*緊急時対応計画の検証 | 関連計画書との整合*		選定	選定
P-4 (2)	*緊急時対応計画の検証 | 代替処理サイト*			選定

ICS 補足ガイダンスなし

CP-6 代替ストレージサイト

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CP-6	**代替ストレージサイト**		選定	選定
CP-6 (1)	*代替ストレージサイト | プライマリサイトからの分離*		選定	選定
CP-6 (2)	*代替ストレージサイト | 復旧時間・ポイント目標*			選定
CP-6 (3)	*代替ストレージサイト | アクセシビリティ*		選定	選定

ICS 補足ガイダンスなし

CP-7 代替処理サイト

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CP-7	**代替処理サイト**		選定	選定
CP-7 (1)	*代替処理サイト | プライマリサイトからの分離*		選定	選定
CP-7 (2)	*代替処理サイト | アクセシビリティ*		選定	選定
CP-7 (3)	*代替処理サイト | サービスの優先順位*		選定	選定
CP-7 (4)	*代替処理サイト | 利用向け設定*			選定

ICS 補足ガイダンスなし

CP-8 電気通信サービス

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CP-8	**電気通信サービス**		選定	選定
CP-8 (1)	*電気通信サービス | サービス提供の優先順位*		選定	選定
CP-8 (2)	*電気通信サービス | 障害単点*		選定	選定
CP-8 (3)	*電気通信サービス | 主・副プロバイダの分割*			選定
CP-8 (4)	*電気通信サービス | プロバイダの不測事態体計画書*			選定

ICS 補足ガイダンス：ICS のサービス品質には待ち時間とスループットが含まれる。
管理拡張：(1, 2, 3, 4) ICS 補足ガイダンスなし

CP-9 INFORMATION SYSTEM BACKUP

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-9	**Information System Backup**	Selected	Selected	Selected
CP-9 (1)	*INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*		Selected	Selected
CP-9 (2)	*INFORMATION SYSTEM BACKUP | TEST RESTORATION USING SAMPLING*			Selected
CP-9 (3)	*INFORMATION SYSTEM BACKUP | SEPARATE STORAGE FOR CRITICAL INFORMATION*			Selected
CP-9 (5)	*INFORMATION SYSTEM BACKUP | TRANSFER TO ALTERNATE SITE*			Selected

No ICS Supplemental Guidance.

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-10	**Information System Recovery and Reconstitution**	Selected	Selected	Selected
CP-10 (2)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | TRANSACTION RECOVERY*		Selected	Selected
CP-10 (4)	*INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | RESTORE WITHIN TIME PERIOD*			Selected

ICS Supplemental Guidance: Reconstitution of the ICS includes consideration whether system state variables should be restored to initial values or values before disruption (e.g., are valves restored to full open, full closed, or settings prior to disruption). Restoring system state variables may be disruptive to ongoing physical processes (e.g., valves initially closed may adversely affect system cooling).

Control Enhancement: (2, 4) No ICS Supplemental Guidance.

CP-12 SAFE MODE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
CP-12	**Safe Mode**	Added	Added	Added

ICS Supplemental Guidance: The organization-defined conditions and corresponding restrictions of safe mode of operation may vary among baselines. The same condition(s) may trigger different response depending on the impact level. The conditions may be external to the ICS (e.g., electricity supply brown-out). Related controls: SI-17.

Rationale for adding CP-12 to all baselines: This control provides a framework for the organization to plan their policy and procedures for dealing with conditions beyond their control in the environment of operations. Creating a written record of the decision process for selecting incidents and appropriate response is part of risk management in light of changing environment of operations.

CP-9 情報システムバックアップ

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CP-9	**情報システムバックアップ**	選定	選定	選定
CP-9 (1)	*情報システムバックアップ | 信頼性・完全性の検証*		選定	選定
CP-9 (2)	*情報システムバックアップ | サンプリングによる復旧試験*			選定
CP-9 (3)	*情報システムバックアップ | 重要情報の分離保管*			選定
CP-9 (5)	*情報システムバックアップ | 代替サイトへの移行*			選定

ICS 補足ガイダンスなし

CP-10 情報システムの復旧・再構築

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CP-10	**情報システムの復旧・再構築**	選定	選定	選定
CP-10 (2)	*情報システムの復旧・再構築 |* *トランザクションの復旧*		選定	選定
CP-10 (4)	*情報システムの復旧・再構築 | 期限内の復旧*			選定

ICS 補足ガイダンス：ICS の再構築には、システム状態変数を中断前の初期値に戻すかどうかの検討が含まれる（バルブは全開か全閉か、中断前の設定値かなど）。システム状態変数を元に戻すと、進行中の物理プロセスが中断する場合がある（バルブが閉じてシステムの冷却に悪影響等）。

管理拡張：(2) (4) ICS 補足ガイダンスなし

CP-12 セーフモード

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
CP-12	**セーフモード**	追加	追加	追加

ICS 補足ガイダンス：組織が定義した条件及び対応する安全運用モードの制限は、ベースラインによってまちまちである。同じ条件でも、影響度によって別の対応となる。条件は ICS にとって、外部のものとなる（停電等）。関連する管理：SI-17

CP-12 を全てのベースラインに追加する理由：この管理は、組織が運用環境で自らの制御が及ばない条件を扱う場合に、ポリシー・手順を計画する体系となる。インシデントと適切な対応を選ぶ際の決定プロセスを文書にすることは、運用環境の変化という観点から、リスク管理の一部となる

IDENTIFICATION AND AUTHENTICATION - IA

Tailoring Considerations for Identification and Authentication Family

Before implementing controls in the IA family, consider the tradeoffs among security, privacy, latency, performance, and throughput. For example, the organization considers whether latency induced from the use of authentication mechanisms employing cryptographic mechanisms would adversely impact the operational performance of the ICS.

In situations where the ICS cannot support the specific Identification and Authentication requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-1	**Security Identification and Authentication Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

IA-2 USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-2	**Identification and Authentication (Organizational Users)**	Selected	Selected	Selected
IA-2 (1)	*IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS*	Selected	Selected	Selected
IA-2 (2)	*IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS*		Selected	Selected
IA-2 (3)	*IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO PRIVILEGED ACCOUNTS*		Selected	Selected
IA-2 (4)	*IDENTIFICATION AND AUTHENTICATION | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS*			Selected
IA-2 (8)	*IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT*		Selected	Selected
IA-2 (9)	*IDENTIFICATION AND AUTHENTICATION | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT*			Selected
IA-2 (11)	*IDENTIFICATION AND AUTHENTICATION | REMOTE ACCESS - SEPARATE DEVICE*		Selected	Selected
IA-2 (12)	*IDENTIFICATION AND AUTHENTICATION | ACCEPTANCE OF PIV CREDENTIALS*	Selected	Selected	Selected

ICS Supplemental Guidance: Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For certain ICS, the capability for immediate operator interaction is critical. Local emergency actions for ICS are not hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical security controls. Example compensating controls include providing increased physical security, personnel security, and auditing measures. For example, manual voice authentication of remote personnel and local, manual actions may be required in order to establish a remote access. See AC-17 ICS Supplemental Guidance. Local user access to ICS components is enabled only when necessary, approved, and authenticated.

識別及び認証 - IA

識別及び認証ファミリのカスタマイズ考慮事項
IA ファミリで管理を実施する前に、セキュリティ、プライバシー、待ち時間、パフォーマンス、スループットを比較考量する。例えば、暗号メカニズムを採用して認証メカニズムを利用するにより生じる待ち時間が、ICS の運用パフォーマンスを阻害しないか組織は検討する。
ICS がある制御の特定の識別・認証要件に対応していない状況では、全体的なカスタマイズガイダンスに従って補償的管理策を採用する。
補償的管理策の例が必要に応じて、管理策ごとに示される。

補足ガイダンス
利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて ICS 補足ガイダンスと併用すべきである。

IA-1 識別・認証ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IA-1	**セキュリティ識別・認証ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

IA-2 ユーザ識別・認証（組織ユーザ）

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IA-2	**識別・認証（組織ユーザ）**	選定	選定	選定
IA-2 (1)	*識別・認証 | 特権アカウントへのネットワークアクセス*	選定	選定	選定
IA-2 (2)	*識別・認証 | 特権のないアカウントへのネットワークアクセス*		選定	選定
IA-2 (3)	*識別・認証 | 特権アカウントへのローカルアクセス*		選定	選定
IA-2 (4)	*識別・認証 | 特権のないアカウントへのローカルアクセス*			選定
IA-2 (8)	*識別・認証 | 特権アカウントへのネットワークアクセス - リプレー抵抗*		選定	選定
IA-2 (9)	*識別・認証 | 特権のないアカウントへのネットワークアクセス - リプレー抵抗*			選定
IA-2 (11)	*識別・認証 | リモートアクセス - 別デバイス*		選定	選定
IA-2 (12)	*識別・認証 | PIV 認証情報の受諾*	選定	選定	選定

ICS 補足ガイダンス：ユーザが 1 つのグループとして機能する場合（制御室操作員等）、ユーザの識別及び認証は役割ベース、グループベース又はデバイスベースとなる。ある種の ICS では、操作員の即時対応が緊要である。ICS のローカル緊急対応は、識別・認証要件に阻害されない。このようなシステムへのアクセスは、適正な物理的セキュリティ対策により制限される。
補償的管理策の例として、物理的セキュリティ、人的セキュリティ、監査手段の強化がある。例えば、リモートアクセスを確立するために、遠隔職員の手動音声認証及びローカルの手動対応が必要となる。AC-17 補足ガイダンスを参照。ICS コンポーネントへのローカルユーザアクセスは、必要時に承認と権限がある場合のみ許可される。

Control Enhancement: (1, 2, 3, 4) ICS Supplemental Guidance: Example compensating controls include implementing physical security measures.

Control Enhancement: (8, 9) ICS Supplemental Guidance: Example compensating controls include provide replay-resistance in an external system.

Control Enhancement: (11) No ICS Supplemental Guidance.

Control Enhancement: (12) ICS Supplemental Guidance: Example compensating controls include implementing support for PIV external to the ICS.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-3	**Device Identification and Authentication**	Added	Selected	Selected
IA-3 (1)	*DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*		Added	Added
IA-3 (4)	*DEVICE IDENTIFICATION AND AUTHENTICATION | DEVICE ATTESTATION*		Added	Added

ICS Supplemental Guidance: The organization may permit connection of devices, also known as non-person entities (NPE), belonging to and authorized by another organization (e.g., business partners) to their ICS. Especially when these devices are non-local, their identification and authentication can be vital. Organizations may perform risk and impact analysis to determine the required strength of authentication mechanisms. Example compensating controls for devices and protocols which do not provide authentication for remote network connections, include implementing physical security measures.

Control Enhancement: (1, 4) ICS Supplemental Guidance: Configuration management for NPE identification and authentication customarily involves a human surrogate or representative for the NPE. Devices are provided with their identification and authentication credentials based on assertions by the human surrogate. The human surrogate also responds to events and anomalies (e.g., credential expiration). Credentials for software entities (e.g., autonomous processes not associated with a specific person) based on properties of that software (e.g., digital signatures) may change every time the software is changed or patched. Special purpose hardware (e.g., custom integrated circuits and printed-circuit boards) may exhibit similar dependencies. Organization definition of parameters may be different among the impact levels.

Rationale (applies to control and control enhancements): ICS may exchange information with many external systems and devices. Identifying and authenticating the devices introduces situations that do not exist with humans. These controls include assignments that enable the organization to categorize devices by types, models, or other group characteristics. Assignments also enable the organizations to select appropriate controls for local, remote, and network connections.

IA-4 IDENTIFIER MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-4	**Identifier Management**	Selected	Selected	Selected

No ICS Supplemental Guidance.

管理拡張：(1, 2, 3, 4) ICS 補足ガイダンス：補償的管理策の例として、物理的セキュリティ対策がある。

管理拡張：(8, 9) ICS 補足ガイダンス：補償的管理策の例として、外部システムへのリプレー抵抗性の付与がある。

管理拡張：(11) ICS 補足ガイダンスなし

管理拡張：(12) ICS 補足ガイダンス：補償的管理策の例として、ICS 外部に対する PIV 対応の実装がある。

IA-3 デバイス識別・認証

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IA-3	***デバイス識別・認証***	追加	選定	選定
IA-3 (1)	***デバイス識別・認証*** | ***暗号化双方向認証***		追加	追加
IA-3 (4)	***デバイス識別・認証*** | ***デバイス認証***		追加	追加

ICS 補足ガイダンス：組織は、よその組織（提携企業等）が承認している保有デバイス（人間以外の実体[NPE]としても知られる）による自社 ICS への接続を認める場合がある。このようなデバイスがローカル以外の場合、識別と認証が重要となる。組織はリスク・影響分析を行い、認証メカニズムの必要強度を判定する。遠隔ネットワーク接続の認証がないデバイス及びプロトコルに対する補償的管理策の例として、物理的セキュリティ対策がある。

管理拡張：(1, 4) ICS 補足ガイダンス：NEP の識別・認証に対する設定管理には、通常、人物を NEP に代える方法がある。人物の代理認証を基に、デバイスに識別・認証情報が付与される。人物の代理により、事象及び異状事態にも対応する（認証情報の期限切れ等）。ソフトウエアの特性（デジタル署名等）に基づくソフトウエア実体の認証情報（特定の人物に関連づけられていない自律プロセス等）は、ソフトウエアが変更され、パッチが当てられるたびに変わる。特殊目的のハードウエア（カスタム IC 基板やプリント基板等）は、似たような依存性を持つ。組織のパラメータ定義は、影響度により異なる。

理由（管理・管理拡張に適用）：ICS は、多数の外部システムやデバイスと情報交換を行う。デバイスの識別・認証は、人間では存在しない状況を生じる。このような管理には、組織がデバイスをタイプ、モデルその他グループ特性で分類するための割当が含まれる。またこの割当により、ローカル接続、遠隔接続及びネットワーク接続を選択することができる。

IA-4 識別子管理

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IA-4	**識別子管理**	選定	選定	選定

ICS 補足ガイダンスなし

IA-5 AUTHENTICATOR MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-5	**Authenticator Management**	Selected	Selected	Selected
IA-5 (1)	*AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION*	Selected	Selected	Selected
IA-5 (2)	*AUTHENTICATOR MANAGEMENT | PKI-BASED AUTHENTICATION*		Selected	Selected
IA-5 (3)	*AUTHENTICATOR MANAGEMENT | IN PERSON REGISTRATION*		Selected	Selected
IA-5 (11)	*AUTHENTICATOR MANAGEMENT | HARDWARE TOKEN-BASED AUTHENTICATION*	Selected	Selected	Selected

ICS Supplemental Guidance: Example compensating controls include physical access control, encapsulating the ICS to provide authentication external to the ICS.

Control Enhancement: (1, 2, 3, 11) No ICS Supplemental Guidance.

IA-6 AUTHENTICATOR FEEDBACK

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-6	**Authenticator Feedback**	Selected	Selected	Selected

ICS Supplemental Guidance: This control assumes a visual interface that provides feedback of authentication information during the authentication process. When ICS authentication uses an interface that does not support visual feedback, (e.g., protocol-based authentication) this control may be tailored out.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-7	**Cryptographic Module Authentication**	Selected	Selected	Selected

No ICS Supplemental Guidance.

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-8	**Identification and Authentication (Non-Organizational Users)**	Selected	Selected	Selected
IA-8 (1)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES*	Selected	Selected	Selected
IA-8 (2)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | ACCEPTANCE OF THIRD-PARTY CREDENTIALS*	Selected	Selected	Selected
IA-8 (3)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-APPROVED PRODUCTS*	Selected	Selected	Selected
IA-8 (4)	*IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | USE OF FICAM-ISSUED PROFILES*	Selected	Selected	Selected

ICS Supplemental Guidance: The ICS Supplemental Guidance for IA-2, Identification and Authentication (Organizational Users), is applicable for Non- Organizational Users.

Control Enhancement: (1, 2, 3, 4) ICS Supplemental Guidance: Example compensating controls include implementing support external to the ICS and multi-factor authentication.

IA-5 認証コード管理

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IA-5	**認証コード管理**	選定	選定	選定
IA-5 (1)	*認証コード管理 | パスワードベース認証*	選定	選定	選定
IA-5 (2)	*認証コード管理 | PKI ベース認証*		選定	選定
IA-5 (3)	*認証コード管理 | 直接登録*		選定	選定
IA-5 (11)	*認証コード管理 | ハードウエアのトークンベース認証*	選定	選定	選定

ICS 補足ガイダンス：補償的管理策の例として、物理的アクセス制御、ICS のカプセル化による ICS 外部認証がある。

管理拡張：(1, 2, 3, 11) ICS 補足ガイダンスなし

IA-6 認証コードフィードバック

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IA-6	**認証フィードバック**	選定	選定	選定

ICS 補足ガイダンス：この管理は、認証中の認証情報をフィードバックする視覚インタフェースを想定している。視覚フィードバックに対応していないインタフェースの ICS 認証の場合（プロトコルベース認証等）、カスタマイズする。

IA-7 暗号化モジュール認証

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IA-7	**暗号化モジュール認証**	選定	選定	選定

ICS 補足ガイダンスなし

IA-8 識別・認証(組織外ユーザ)

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IA-8	**識別・認証（組織外ユーザ）**	選定	選定	選定
IA-8 (1)	*識別・認証（組織外ユーザ）| 他機関 PIV 認証情報の許諾*	選定	選定	選定
IA-8 (2)	*識別・認証（組織外ユーザ）| サードパーティ認証情報の許諾*	選定	選定	選定
IA-8 (3)	*識別・認証（組織外ユーザ）| FICAM 認定製品の使用*	選定	選定	選定
IA-8 (4)	*識別・認証（組織外ユーザ）| FICAM 発行プロファイルの使用*	選定	選定	選定

ICS 補足ガイダンス：IA-2 識別・認証に関する ICS 補足ガイダンス（組織ユーザ）は、組織外ユーザに適用できる。

管理拡張：(1, 2, 3, 4) ICS 補足ガイダンス：補償的管理策の例として、ICS の外部及び多要素認証への対応実装がある。

INCIDENT RESPONSE - IR

Tailoring Considerations for Incident Response Family

The automated mechanisms used to support the tracking of security incidents are typically not part of, or connected to, the ICS.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-1	**Incident Response Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

IR-2 INCIDENT RESPONSE TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-2	**Incident Response Training**	Selected	Selected	Selected
IR-2 (1)	*INCIDENT RESPONSE TRAINING | SIMULATED EVENTS*			Selected
IR-2 (2)	*INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS*			Selected

No ICS Supplemental Guidance.

IR-3 INCIDENT RESPONSE TESTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-3	**Incident Response Testing**		Selected	Selected
IR-3 (2)	*INCIDENT RESPONSE TESTING | COORDINATION WITH RELATED PLANS*		Selected	Selected

No ICS Supplemental Guidance.

IR-4 INCIDENT HANDLING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-4	**Incident Handling**	Selected	Selected	Selected
IR-4 (1)	*INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES*		Selected	Selected
IR-4 (4)	*INCIDENT HANDLING | INFORMATION CORRELATION*			Selected

No ICS Supplemental Guidance.

インシデント対応 - IR

インシデント対応ファミリのカスタマイズ考慮事項

接続インシデント追跡用に使用する自動メカニズムは、通常 ICS の一部ではなく、ICS に接続されてもいない。

補足ガイダンス

利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

IR-1 インシデント対応ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IR-1	**インシデント対応ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

IR-2 インシデント対応訓練

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IR-2	**インシデント対応訓練**	選定	選定	選定
IR-2 (1)	*インシデント対応訓練 | 模擬事象*			選定
IR-2 (2)	*インシデント対応訓練 | 自動訓練環境*			選定

ICS 補足ガイダンスなし

IR-3 インシデント対応試験

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IR-3	**インシデント対応試験**		選定	選定
IR-3 (2)	*インシデント対応訓練 | 関連計画書との整合*		選定	選定

ICS 補足ガイダンスなし

IR-4 インシデントハンドリング

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IR-4	**インシデント処理**	選定	選定	選定
IR-4 (1)	*インシデント処理 | 自動インシデント処理プロセス*		選定	選定
IR-4 (4)	*インシデント処理 | 情報相関*			選定

ICS 補足ガイダンスなし

IR-5 INCIDENT MONITORING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-5	**Incident Monitoring**	Selected	Selected	Selected
IR-5 (1)	*INCIDENT MONITORING | AUTOMATED TRACKING / DATA COLLECTION / ANALYSIS*			Selected

No ICS Supplemental Guidance.

IR-6 INCIDENT REPORTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-6	**Incident Reporting**	Selected	Selected	Selected
IR-6 (1)	*INCIDENT REPORTING | AUTOMATED REPORTING*		Selected	Selected

ICS Supplemental Guidance: The organization should report incidents on a timely basis. The DHS National Cybersecurity & Communications Integration Center (NCCIC), http://www.dhs.gov/about-national-cybersecurity-communications-integration-center, serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) http://ics-cert.us-cert.gov/ics-cert/, collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

Control Enhancement: (1) ICS Supplemental Guidance: The automated mechanisms used to support the incident reporting process are not necessarily part of, or connected to, the ICS.

IR-7 INCIDENT RESPONSE ASSISTANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-7	**Incident Response Assistance**	Selected	Selected	Selected
IR-7 (1)	*INCIDENT RESPONSE ASSISTANCE | AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION / SUPPORT*		Selected	Selected

No ICS Supplemental Guidance.

IR-8 INCIDENT RESPONSE PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
IR-8	**Incident Response Plan**	Selected	Selected	Selected

No ICS Supplemental Guidance.

IR-5インシデント監視

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IR-5	**インシデント監視**	選定	選定	選定
IR-5 (1)	*インシデント監視 | 自動追跡・データ収集・分析*			選定

ICS 補足ガイダンスなし

IR-6　インシデント報告

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IR-6	**インシデント報告**	選定	選定	選定
IR-6 (1)	*インシデント報告 | 自動報告*		選定	選定

ICS 補足ガイダンス：組織は、タイムリーにインシデント報告を行うべきである。下記 DHS 国家サイバーセキュリティ通信統合センター(NCCIC)は集中所在地として機能し、サイバーセキュリティと通信の信頼性に関わる運用部署はそこで調整され、統合化されている。
http://www.dhs.gov/about-national-cybersecurity-communications-integration-center
下記産業用制御システムサイバー緊急対応チーム(ICS-CERT)は、海外及び民間のコンピュータ緊急対応チーム(CERT)と連携して、制御システム関連セキュリティインシデント情報と緩和対策を共有している。http://ics-cert.us-cert.gov/ics-cert/

管理拡張：(1) ICS 補足ガイダンス：インシデント報告プロセスへの対応に使用する自動メカニズムは、必ずしも ICS の一部ではなく、ICS に接続されているわけではない。

IR-7　インシデント対応支援

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IR-7	**インシデント対応支援**	選定	選定	選定
IR-7 (1)	*インシデント対応支援 | 情報・サポート可用性への自動対応*		選定	選定

ICS 補足ガイダンスなし

IR-8　インシデント対応計画

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
IR-8	**インシデント対応計画書**	選定	選定	選定

ICS 補足ガイダンスなし

MAINTENANCE - MA

Tailoring Considerations for Maintenance Family

The automated mechanisms used to schedule, conduct, and document maintenance and repairs are not necessarily part of, or connected to, the ICS.

In situations where the ICS cannot support the specific Maintenance requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NISTSP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-1	**Maintenance Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

MA-2 CONTROLLED MAINTENANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-2	**Controlled Maintenance**	Selected	Selected	Selected
MA-2 (2)	*CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES*			Selected

No ICS Supplemental Guidance.

MA-3 MAINTENANCE TOOLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-3	**Maintenance Tools**		Selected	Selected
MA-3 (1)	*MAINTENANCE TOOLS | INSPECT TOOLS*		Selected	Selected
MA-3 (2)	*MAINTENANCE TOOLS | INSPECT MEDIA*		Selected	Selected
MA-3 (3)	*MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*			Selected

No ICS Supplemental Guidance.

保守 - MA

保守ファミリのカスタマイズ考慮事項
保守・修理の予定作成、実施及び文書化に使用する自動メカニズムは、必ずしも ICS の一部ではなく、ICS に接続されているわけではない。
ICS がある制御の特定の保守要件に対応していない状況では、全体的なカスタマイズガイダンスに従って補償的管理策を採用する。補償的管理策の例が必要に応じて、管理策ごとに示される。

補足ガイダンス
利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

MA-1 システム保守ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MA-1	**保守ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

MA-2 管理保守

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MA-2	**管理保守**	選定	選定	選定
MA-2 (2)	*管理保守 | 自動保守活動*			選定

ICS 補足ガイダンスなし

MA-3 保守ツール

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MA-3	**保守ツール**		選定	選定
MA-3 (1)	*保守ツール | 検査ツール*		選定	選定
MA-3 (2)	*保守ツール | 検査媒体*		選定	選定
MA-3 (3)	*保守ツール | 無断削除防止*			選定

ICS 補足ガイダンスなし

MA-4 NONLOCAL MAINTENANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-4	**Non-Local Maintenance**	Selected	Selected	Selected
MA-4 (2)	*NON-LOCAL MAINTENANCE | DOCUMENT NON-LOCAL MAINTENANCE*		Selected	Selected
MA-4 (3)	*NON-LOCAL MAINTENANCE | COMPARABLE SECURITY / SANITIZATION*			Selected

No ICS Supplemental Guidance.

Control Enhancement: (2) No ICS Supplemental Guidance.

Control Enhancement: (3) ICS Supplemental Guidance: In crisis or emergency situations, the organization may need immediate access to non-local maintenance and diagnostic services in order to restore essential ICS operations or services. Example compensating controls include limiting the extent of the maintenance and diagnostic services to the minimum essential activities, carefully monitoring and auditing the non-local maintenance and diagnostic activities.

MA-5 MAINTENANCE PERSONNEL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-5	**Maintenance Personnel**	Selected	Selected	Selected
MA-5 (1)	*MAINTENANCE PERSONNEL | INDIVIDUALS WITHOUT APPROPRIATE ACCESS*			Selected

No ICS Supplemental Guidance.

MA-6 TIMELY MAINTENANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-6	**Timely Maintenance**		Selected	Selected

No ICS Supplemental Guidance.

MA-4 非ローカル保守

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MA-4	**非ローカル保守**	選定	選定	選定
MA-4 (2)	***非ローカル保守*** **| 非ローカル保守** *の文書化*		選定	選定
MA-4 (3)	***非ローカル保守*** *| 同等セキュリティ・サニタイズ*			選定

ICS 補足ガイダンスなし

管理拡張：(2) ICS 補足ガイダンスなし

管理拡張：(3) ICS 補足ガイダンス：危機又は緊急事態には、重要 ICS 運用又はサービスを復旧するため、組織は非ローカル保守及び診断サービスを直ちに利用する必要がある。補償的管理策の例として、保守及び診断サービスを最低限必要な程度に限定し、非ローカル保守及び診断活動を慎重に監視・監査する。

MA-5 保守要員

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MA-5	**保守要員**	選定	選定	選定
MA-5 (1)	*保守要員 | 適性アクセス以外の個人*			選定

ICS 補足ガイダンスなし

MA-6 適時的保守

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MA-6	**適時的保守**		選定	選定

ICS 補足ガイダンスなし

MEDIA PROTECTION –MP

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-1	**Media Protection Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

MP-2 MEDIA ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-2	**Media Access**	Selected	Selected	Selected

No ICS Supplemental Guidance.

MP-3 MEDIA MARKING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-3	**Media Marking**		Selected	Selected

No ICS Supplemental Guidance.

MP-4 MEDIA STORAGE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-4	**Media Storage**		Selected	Selected

No ICS Supplemental Guidance.

MP-5 MEDIA TRANSPORT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-5	**Media Transport**		Selected	Selected
MP-5 (4)	*MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*		Selected	Selected

No ICS Supplemental Guidance.

メディア保護 –MP

補足ガイダンス
利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

MP-1　メディア保護ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MP-1	**メディア保護ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

MP-2　メディアアクセス

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MP-2	**メディアアクセス**	選定	選定	選定

ICS 補足ガイダンスなし

MP-3　メディアマーキング

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MP-3	**メディアマーキング**		選定	選定

ICS 補足ガイダンスなし

MP-4　メディアストレージ

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MP-4	**メディアストレージ**		選定	選定

ICS 補足ガイダンスなし

MP-5　メディア転送

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MP-5	**メディア転送**		選定	選定
MP-5 (4)	*メディア転送 | 暗号化保護*		選定	選定

ICS 補足ガイダンスなし

MP-6 MEDIA SANITIZATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-6	**Media Sanitization**	Selected	Selected	Selected
MP-6 (1)	*MEDIA SANITIZATION | TRACKING / DOCUMENTING / VERIFYING*			Selected
MP-6 (2)	*MEDIA SANITIZATION | EQUIPMENT TESTING*			Selected
MP-6 (3)	*MEDIA SANITIZATION | NON-DESTRUCTIVE TECHNIQUES*			Selected

No ICS Supplemental Guidance.

MP-7 MEDIA USE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
MP-7	**Media Use**	Selected	Selected	Selected
MP-7 (1)	*MEDIA USE | ORGANIZATIONAL RESTRICTIONS*		Selected	Selected

No ICS Supplemental Guidance.

MP-6　メディアサニタイズ

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MP-6	**メディアサニタイズ**	選定	選定	選定
MP-6 (1)	*メディアサニタイズ | 追跡・文書化・検証*			選定
MP-6 (2)	*メディアサニタイズ | 装備品試験*			選定
MP-6 (3)	*メディアサニタイズ | 非破壊技術*			選定

ICS 補足ガイダンスなし

MP-7　メディア利用

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
MP-7	**メディア利用**	選定	選定	選定
MP-7 (1)	*メディア利用 | 組織上の制限*		選定	選定

ICS 補足ガイダンスなし

PHYSICAL AND ENVIRONMENTAL PROTECTION – PE

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-1	**Physical and Environmental Protection Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems. The ICS components can be distributed over a large facility footprint or geographic area and can be an entry point into the entire organizational network ICS. Regulatory controls may also apply.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-2	**Physical Access Authorizations**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PE-3 PHYSICAL ACCESS CONTROL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-3	**Physical Access Control**	Selected	Selected	Selected
PE-3 (1)	*PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*			Selected

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies. The organization considers access requirements in emergency situations. During an emergency-related event, the organization may restrict access to ICS facilities and assets to authorized individuals only. ICS are often constructed of devices that either do not have or cannot use comprehensive access control capabilities due to time-restrictive safety constraints. Physical access controls and defense-in-depth measures are used by the organization when necessary and possible to supplement ICS security when electronic mechanisms are unable to fulfill the security requirements of the organization's security plan. Primary nodes, distribution closets, and mechanical/electrical rooms should be locked and require key or electronic access control and incorporate intrusion detection sensors.

Control Enhancement: (1) No ICS Supplemental Guidance.

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-4	**Access Control for Transmission Medium**		Selected	Selected

No ICS Supplemental Guidance.

物理的環境的保護 – PE

補足ガイダンス
利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

PE-1　物理的環境的保護ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-1	**物理環境保護ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。ICS コンポーネントは、広範な施設及び地域にまたがって分散しており、組織の ICS ネットワークへの入口になっている場合もある。規制管理も適用できよう。

PE-2　物理的アクセス権限

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-2	**物理的アクセス権限**	選定	選定	選定

ICS 補足ガイダンスなし

PE-3　物理的アクセス制御

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-3	**物理的アクセス制御**	選定	選定	選定
PE-3 (1)	*物理的アクセス制御 | 情報システムアクセス*			選定

ICS 補足ガイダンス：組織は ICS の安全性とセキュリティの相互関係を検討する。組織は、緊急状況下でのアクセス要件を検討する。緊急関連事象が発生した場合、組織は ICS 施設及び資産へのアクセスを権限のある人物だけに制限する。ICS は、時間的な制約から安全性に限界があるため、包括的なアクセス制御能力がないか利用できないデバイスで構成されていることが多い。電子的メカニズムでは組織のセキュリティ計画書要件に満たない場合、ICS セキュリティにとって必要かつ補足可能であれば、物理的アクセス制御及び多層防御対策を採用する。主要ノード、配電クローゼット及び機械・電気室は施錠し、鍵又は電子的手段でアクセス制御し、侵入検知センサを取り付ける。
管理拡張：(1) ICS 補足ガイダンスなし

PE-4　通信メディアのアクセス制御

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-4	**通信メディアのアクセス制御**		選定	選定

ICS 補足ガイダンスなし

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-5	**Access Control for Output Devices**		Selected	Selected

No ICS Supplemental Guidance.

PE-6 MONITORING PHYSICAL ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-6	**Monitoring Physical Access**	Selected	Selected	Selected
PE-6 (1)	*MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*		Selected	Selected
PE-6 (4)	*MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*		Added	Selected

ICS Supplemental Guidance: Physical access controls and defense-in-depth measures are used as compensating controls by the organization when necessary and possible to supplement ICS security when electronic mechanisms are unable to monitor, detect and alarm when an ICS has been accessed. These compensating controls are in addition to the PE-6 controls (e.g., employing PE-3(4) Lockable Casings and/or PE-3(5) Tamper Protection).

Control Enhancement: (1) No ICS Supplemental Guidance.

Control Enhancement: (4) ICS Supplemental Guidance: The locations of ICS components (e.g., field devices, remote terminal units) can include various remote locations (e.g., substations, pumping stations).

Rationale (adding CE 4 to MODERATE baseline): Many of the ICS components are in remote geographical and dispersed locations with little capability to monitor all ICS components. Other components may be in ceilings, floors, or distribution closets with minimal physical barriers to detect, delay or deny access to the devices and no electronic surveillance or guard forces response capability.

PE-8 VISITOR ACCESS RECORDS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-8	**Visitor Access Records**	Selected	Selected	Selected
PE-8 (1)	*VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW*			Selected

No ICS Supplemental Guidance.

PE-9 POWER EQUIPMENT AND CABLING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-9	**Power Equipment and Cabling**		Selected	Selected
PE-9 (1)	*POWER EQUIPMENT AND CABLING | REDUNDANT CABLING*		Added	Added

No ICS Supplemental Guidance.

Control Enhancement: (1) No ICS Supplemental Guidance.

Rationale (for adding (1): Continuity of ICS control and operation requires redundant power cabling.

PE-5　出力デバイスのアクセス制御

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-5	**出力デバイスのアクセス制御**		選定	選定

ICS 補足ガイダンスなし

PE-6　物理的アクセス監視

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-6	**物理的アクセス監視**	選定	選定	選定
PE-6 (1)	*物理的アクセス監視 | 侵入アラーム・サーベイランス装置*		選定	選定
PE-6 (4)	*物理的アクセス監視 | 情報システムへの物理的アクセス監視*		追加	選定

ICS 補足ガイダンス：電子的メカニズムでは ICS へのアクセスを監視・検知・警報できない場合、ICS セキュリティにとって必要かつ補足可能であれば、物理的アクセス制御及び多層防御対策を補償的管理策として採用する。このような補償的管理策は、PE-6 管理を補足するものとなる（PE-3(4)施錠可能金庫又は PE-3(5)改竄防止）。

管理拡張：(1) ICS 補足ガイダンスなし

管理拡張：(4) ICS 補足ガイダンス：ICS コンポーネント（フィールドデバイス、遠隔端末装置等）の場所には、様々な遠隔地が含まれる（変電所、ポンプステーション等）。

理由（CE 4 を中ベースラインに追加）：ICS コンポーネントの多くは遠隔地に点在しているため、すべてを監視することはほぼ不可能である。天井、床及び配電クローゼットに配置されているものもあり、アクセスを検知・遅延・防止する物理的障壁は乏しく、電子的サーベイランスや警備員等の備えもない。

PE-8　来訪者立入記録

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-8	**来訪者立入記録**	選定	選定	選定
PE-8 (1)	*来訪者立入記録 | 自動記録保守 見直し*			選定

ICS 補足ガイダンスなし

PE-9　電気装置及び配線

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-9	**電気装置及び配線**		選定	選定
PE-9 (1)	*電気装置及び配線 | 冗長配線*		追加	追加

ICS 補足ガイダンスなし

管理拡張：(1) ICS 補足ガイダンスなし

理由（(1)の追加）：ICS 制御・運用を継続するために電源ケーブルの冗長化が必要。

PE-10 EMERGENCY SHUTOFF

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-10	**Emergency Shutoff**		Selected	Selected

ICS Supplemental Guidance: It may not be possible or advisable to shutoff power to some ICS. Example compensating controls include fail in known state and emergency procedures.

PE-11 EMERGENCY POWER

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-11	**Emergency Power**	Added	Selected	Selected
PE-11 (1)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*	Added	Added	Selected
PE-11 (2)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - SELF-CONTAINED*			Added

ICS Supplemental Guidance: Emergency power production, transmission and distribution systems are a type of ICS that are required to meet extremely high performance specifications. The systems are governed by international, national, state and local building codes, must be tested on a continual basis, and must be repaired and placed back into operations within a short period of time. Traditionally, emergency power has been provided by generators for short to mid-term power (typically for fire and life safety systems, some IT load, and evacuation transport) and UPS battery packs in distribution closets and within work areas to allow some level of business continuity and for the orderly shutdown of non-essential IT and facility systems. Traditional emergency power systems typically are off-line until a loss of power occurs and are typically on a separate network and control system specific to the facility they support. New methods of energy generation and storage (e.g., solar voltaic, geothermal, flywheel, microgrid, distributed energy) that have a real-time demand and storage connection to local utilities or cross connected to multiple facilities should be carefully analyzed to ensure that the power can meet the load and signal quality without disruption of mission essential functions.

Control Enhancement: (1) No ICS Supplemental Guidance.

Rationale for adding control to baseline: ICS may support critical activities which will be needed for safety and reliability even in the absence of reliable power from the public grid.

PE-12 EMERGENCY LIGHTING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-12	**Emergency Lighting**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PE-10 緊急遮断

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-10	**緊急遮断**		選定	選定

ICS 補足ガイダンス：特定の ICS の電源遮断は不可能又は推奨できない。補償的管理策の例として、既知状態の失敗及び緊急手順がある。

PE-11 緊急電源

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-11	**緊急電源**	追加	選定	選定
PE-11 (1)	*緊急電源 | 長期代替電源 - 最低限の運用能力*	追加	追加	選定
PE-11 (2)	*緊急電源 | 長期代替電源 - 内蔵型*			追加

ICS 補足ガイダンス：緊急発電・送配電システムは一種の ICS で、極めて高度な性能仕様要件が課される。国際・国家・州・自治体の建築法に準拠し、定期的試験が課され、短期間に修理・復旧できなければならない。従来、緊急電源として短・中期用発電機（通常火災・安全装置、特定の IT 作業及び避難輸送）と UPS バッテリーパックが配電クローゼットや作業エリアに設置されており、ある程度の事業継続や不要 IT 装置・施設装置の秩序だった遮断ができるようになっている。従来緊急電源装置は、電源が失われるまでオフラインになっていることが多く、対応する施設固有の別ネットワーク及び制御システム上に置かれている。新たなエネルギー発生・保存手段（太陽光、地熱、フライホイール、マイクログリッド、分散エネルギー等）で、地方公共事業者や複数施設にリアルタイム需要・蓄積接続してものについては、重大な任務・機能を中断することなく、電力が負荷・信号品質要件を満たせるか、慎重に分析すべきである。

管理拡張：(1) ICS 補足ガイダンスなし

ベースラインに管理を追加する理由：公共配電網からの電力を当てにできない場合であっても、ICS は、安全性や信頼性の確保に必要な重要活動を支えている。

PE-12 緊急照明

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-12	**緊急照明**	選定	選定	選定

ICS 補足ガイダンスなし

PE-13 FIRE PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-13	**Fire Protection**	Selected	Selected	Selected
PE-13 (1)	*FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*			Selected
PE-13 (2)	*FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*			Selected
PE-13 (3)	*FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*		Selected	Selected

ICS Supplemental Guidance: Fire suppression mechanisms should take the ICS environment into account (e.g., water sprinkler systems could be hazardous in specific environments).

Control Enhancement: (1, 2, 3) No ICS Supplemental Guidance.

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-14	**Temperature and Humidity Controls**	Selected	Selected	Selected

ICS Supplemental Guidance: Temperature and humidity controls are typically components of other ICS systems such as the HVAC, process, or lighting systems, or can be a standalone and unique ICS system. ICS can operate in extreme environments and both interior and exterior locations. For a specific ICS, the temperature and humidity design and operational parameters dictate the performance specifications. As ICS and IS become interconnected and the network provides connectivity across the hybrid domain, power circuits, distribution closets, routers and switches that support fire protection and life safety systems must be maintained at the proper temperature and humidity.

PE-15 WATER DAMAGE PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-15	**Water Damage Protection**	Selected	Selected	Selected
PE-15 (1)	*WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*			Selected

ICS Supplemental Guidance: Water damage protection and use of shutoff and isolation valves is both a procedural action, and also a specific type of ICS. ICS that are used in the manufacturing, hydropower, transportation/navigation, water and wastewater industries rely on the movement of water and are specifically designed to manage the quantity/flow and pressure of water. As ICS and IS become interconnected and the network provides connectivity across the hybrid domain, power circuits, distribution closets, routers and switches that support fire protection and life safety systems should ensure that water will not disable the system (e.g. a fire that activates the sprinkler system does not spray onto the fire control servers, router, switches and short out the alarms, egress systems, emergency lighting, and suppression systems).

Control Enhancement: (1) No ICS Supplemental Guidance.

PE-16 DELIVERY AND REMOVAL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-16	**Delivery and Removal**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PE-13　防火

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-13	**防火**	選定	選定	選定
PE-13 (1)	*防火 | 検知デバイス・システム*			選定
PE-13 (2)	*防火 | 消火デバイス・システム*			選定
PE-13 (3)	*防火 | 自動消火*		選定	選定

ICS 補足ガイダンス：消化機構には ICS 環境を考慮に入れる（スプリンクラーは環境により有害）。

管理拡張：(1, 2, 3) ICS 補足ガイダンスなし

PE-14　温度・湿度制御

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-14	**温度・湿度制御**	選定	選定	選定

ICS 補足ガイダンス：温度・湿度制御は HVAC、プロセス、照明装置等の ICS システムのコンポーネントであり、スタンドアローン型システムもあれば特有の ICS システムもある。ICS は屋内外の過酷な環境下に置かれる場合がある。ある種の ICS は、温度・湿度設計や運用パラメータによって性能仕様が決まる。ICS と IS は連接され、ネットワークはハイブリッド領域にまたがるため、防火装置や生命安全装置を支える電気回路、配電クローゼット、ルータ及びスイッチは、適性温度・湿度に保たれなければならない。

PE-15　水害防護

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-15	**水害防護**	選定	選定	選定
PE-15 (1)	*水害防護 | 自動対応*			選定

ICS 補足ガイダンス：水害防護と閉止・遮断弁の使用は、ともに手順行為であり、同時にある種の ICS でもある。製造・水力発電・輸送/運航・上下水道業界で使用される ICS は、水の運動に依存しており、特に水の量・流量及び圧力を管理するように設計されている。ICS と IS は連接され、ネットワークはハイブリッドドメインにまたがるため、防火装置や生命安全装置を支える電気回路、配電クローゼット、ルータ及びスイッチは、水害でシステムが作動不能にならないようにすべきである（火事でスプリンクラーが作動しても、防火サーバ、ルータ、スイッチには水がかからないようにし、アラーム、脱出システム、緊急照明、消火システムがショートしないようにする）。

管理拡張：(1) ICS 補足ガイダンスなし

PE-16　配送・撤去

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-16	**配送・撤去**	選定	選定	選定

ICS 補足ガイダンスなし

PE-17 ALTERNATE WORK SITE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-17	**Alternate Work Site**		Selected	Selected

No ICS Supplemental Guidance.

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-18	**Location of Information System Components**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PE-17　代替作業場

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-17	**代替作業場**		選定	選定

ICS 補足ガイダンスなし

PE-18　情報システムコンポーネントの場所

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PE-18	**情報システムコンポーネント**	選定	選定	選定

ICS 補足ガイダンスなし

PLANNING – PL

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-1	**Security Planning Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

PL-2 SYSTEM SECURITY PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-2	**System Security Plan**	Selected	Selected	Selected
PL-2 (3)	*SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES*	Added	Selected	Selected

No ICS Supplemental Guidance.

Control Enhancement: (3) No ICS Supplemental Guidance.

Rationale for adding PL-2 (3) to low baseline: When systems are highly inter-connected, coordinated planning is essential. A low impact system could adversely affect a higher impact system.

PL-4 RULES OF BEHAVIOR

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-4	**Rules of Behavior**	Selected	Selected	Selected
PL-4 (1)	*RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS*		Selected	Selected

No ICS Supplemental Guidance.

PL-7 SECURITY CONCEPT OF OPERATIONS (CONOPS)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-7	**Security Concept of Operations**		Added	Added

No ICS Supplemental Guidance.

Rationale for adding PL-7 to moderate and high baselines: ICS are complex systems. Organizations typically employ a CONOPS to help define a system and share that understanding with personnel involved with that system and other systems with which it interacts. A CONOPS often helps identify information protection requirements.

プランニング – PL

補足ガイダンス
利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

PL-1　セキュリティ計画ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PL-1	**セキュリティ計画ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

PL-2　システムのセキュリティ計画書

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PL-2	**システムセキュリティ計画書**	選定	選定	選定
PL-2 (3)	*システムセキュリティ計画書 | 他の組織との計画・調整*	追加	選定	選定

ICS 補足ガイダンスなし
管理拡張：(3) ICS 補足ガイダンスなし
PL-2 (3)を低ベースラインに追加する理由：システム同士が高度に相互連接している場合、計画の調整が肝要である。影響度の低いシステムが高いシステムに悪影響を与えることがある。

PL-4　行動規則

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PL-4	**行動規則**	選定	選定	選定
PL-4 (1)	*行動規則 | ソーシャルメディア/ネットワーキングの制限*		選定	選定

ICS 補足ガイダンスなし

PL-7　運用セキュリティ概念 (CONOPS)

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PL-7	**運用セキュリティ概念**		追加	追加

ICS 補足ガイダンスなし
PL-7 を中・高ベースラインに追加する理由：ICS システムが複雑なため。通常、組織は CONOPS を採用して、システムを定義し、当該システムや相互作用を行う他のシステムの関係者と理解を共有する。CONOPS は、情報保護要件を明らかにする上で役立つことが多い。

PL-8 INFORMATION SECURITY ARCHITECTURE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PL-8	**Information Security Architecture**		Selected	Selected

No ICS Supplemental Guidance.

PL-8 情報セキュリティアーキテクチャ

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PL-8	情報セキュリティアーキテクチャ		選定	選定

ICS 補足ガイダンスなし

PERSONNEL SECURITY – PS

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-1	**Personnel Security Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

PS-2 POSITION RISK DESIGNATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-2	**Position Risk Designation**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PS-3 PERSONNEL SCREENING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-3	**Personnel Screening**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PS-4 PERSONNEL TERMINATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-4	**Personnel Termination**	Selected	Selected	Selected
PS-4 (2)	*PERSONNEL TERMINATION | AUTOMATED NOTIFICATION*			Selected

No ICS Supplemental Guidance.

PS-5 PERSONNEL TRANSFER

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-5	**Personnel Transfer**	Selected	Selected	Selected

No ICS Supplemental Guidance.

人員のセキュリティ – PS

補足ガイダンス
利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

PS-1　人員のセキュリティポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PS-1	**人員のセキュリティポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

PS-2　配置リスク指定

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PS-2	**配置リスク指定**	選定	選定	選定

ICS 補足ガイダンスなし

PS-3　人選

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PS-3	**人選**	選定	選定	選定

ICS 補足ガイダンスなし

PS-4　退職

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PS-4	**退職**	選定	選定	選定
PS-4 (2)	*退職 | 自動通知*			選定

ICS 補足ガイダンスなし

PS-5　転勤

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PS-5	**転勤**	選定	選定	選定

ICS 補足ガイダンスなし

PS-6 ACCESS AGREEMENTS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-6	**Access Agreements**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PS-7 THIRD-PARTY PERSONNEL SECURITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-7	**Third-Party Personnel Security**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PS-8 PERSONNEL SANCTIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
PS-8	**Personnel Sanctions**	Selected	Selected	Selected

No ICS Supplemental Guidance.

PS-6 アクセス同意

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PS-6	アクセス同意	選定	選定	選定

ICS 補足ガイダンスなし

PS-7 サードパーティ社員セキュリティ

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PS-7	サードパーティ社員セキュリティ	選定	選定	選定

ICS 補足ガイダンスなし

PS-8 懲戒

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
PS-8	懲戒	選定	選定	選定

ICS 補足ガイダンスなし

RISK ASSESSMENT – RA

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-1	**Risk Assessment Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

RA-2 SECURITY CATEGORIZATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-2	**Security Categorization**	Selected	Selected	Selected

No ICS Supplemental Guidance.

RA-3 RISK ASSESSMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-3	**Risk Assessment**	Selected	Selected	Selected

No ICS Supplemental Guidance.

RA-5 VULNERABILITY SCANNING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
RA-5	**Vulnerability Scanning**	Selected	Selected	Selected
RA-5 (1)	*VULNERABILITY SCANNING | UPDATE TOOL CAPABILITY*		Selected	Selected
RA-5 (2)	*VULNERABILITY SCANNING | UPDATE BY FREQUENCY / PRIOR TO NEW SCAN / WHEN IDENTIFIED*		Selected	Selected
RA-5 (4)	*VULNERABILITY SCANNING | DISCOVERABLE INFORMATION*			Selected
RA-5 (5)	*VULNERABILITY SCANNING | PRIVILEGED ACCESS*		Selected	Selected

ICS Supplemental Guidance: Active vulnerability scanning, which introduces network traffic, is used with care on ICS systems to ensure that ICS functions are not adversely impacted by the scanning process. The organization makes a risk-based determination whether to employ active scanning. Passive monitoring /sniffing may be used as part of a compensating control. Example compensating controls include providing a replicated, virtualized, or simulated system to conduct scanning. Production ICS may need to be taken off-line before scanning can be conducted. If ICS are taken off-line for scanning, scans are scheduled to occur during planned ICS outages whenever possible. If vulnerability scanning tools are used on non-ICS networks, extra care is taken to ensure that they do not scan the ICS network. Network scanning is not applicable to non-addressable communications. Vulnerability examination may be performed using other mechanisms than scanning to identify the objects being examined. Host-based vulnerability examination is an example compensating control.
Control Enhancement: (1, 2, 4, 5) No ICS Supplemental Guidance.

リスク評価 – RA

補足ガイダンス
利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

RA-1　リスク評価ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
RA-1	**リスク評価ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

RA-2　セキュリティ分類

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
RA-2	**セキュリティ分類**	選定	選定	選定

ICS 補足ガイダンスなし

RA-3　リスク評価

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
RA-3	**リスク評価**	選定	選定	選定

ICS 補足ガイダンスなし

RA-5　脆弱性検索

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
RA-5	**脆弱性検索**	選定	選定	選定
RA-5 (1)	*脆弱性検索 | 更新ツール機能*		選定	選定
RA-5 (2)	*検脆弱性索 | 新規スキャン前・識別時の周波数による更新*		選定	選定
RA-5 (4)	*脆弱性検索 | 検出可能情報*			選定
RA-5 (5)	*脆弱性検索 | 特権アクセス*		選定	選定

ICS 補足ガイダンス：アクティブ脆弱性計画検索は、ネットワークトラフィックを生じるので ICS システム上で慎重に行い、検索プロセスにより ICS 機能に悪影響が及ばないようにする。組織はリスクに立脚して、アクティブ検索実行の是非を判断する。パッシブ監視・スニッフィングは、補償的管理策の一環として使用できる。補償的管理策の例として、複製、仮想又は模擬システムで検索する方法がある。生産 ICS は、検索前にオフラインにする必要がある。オフラインにする場合、可能であれば、予め計画された ICS の操業停止時に検索を行うように予定を組む。脆弱性検索ツールを ICS 以外のネットワークで行う場合、検索が ICS ネットワークに及ばないように注意する。ネットワーク検索は、アドレス指定不能の通信には適用されない。

脆弱性検証は、検証中の対象を識別する検索以外のメカニズムを使用して行う。ホストベースの脆弱性検証は、補償的管理策の一例である。

管理拡張：(1, 2, 4, 5) ICS 補足ガイダンスなし

SYSTEM AND SERVICES ACQUISITION – SA

Tailoring Considerations for System and Services Acquisition Family

In situations where the ICS cannot support the specific System and Services Acquisition requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-1	**System and Services Acquisition Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

SA-2 ALLOCATION OF RESOURCES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-2	**Allocation of Resources**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SA-3 SYSTEM DEVELOPMENT LIFE CYCLE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-3	**System Development Life Cycle**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SA-4 ACQUISITION PROCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-4	**Acquisition Process**	Selected	Selected	Selected
SA-4 (1)	*ACQUISITION PROCESS | FUNCTIONAL PROPERTIES OF SECURITY CONTROLS*		Selected	Selected
SA-4 (2)	*ACQUISITION PROCESS | DESIGN / IMPLEMENTATION INFORMATION FOR SECURITY CONTROLS*		Selected	Selected
SA-4 (9)	*ACQUISITION PROCESS | FUNCTIONS / PORTS / PROTOCOLS / SERVICES IN USE*		Selected	Selected
SA-4 (10)	*ACQUISITION PROCESS | USE OF APPROVED PIV PRODUCTS*	Selected	Selected	Selected

ICS Supplemental Guidance: Since ICS security has historically focused on physical protection and isolation, vendors and developers may be unfamiliar with cybersecurity. Organizations should anticipate a need to engage with ICS suppliers to raise awareness of cybersecurity needs. The SCADA/Control Systems Procurement Project provides example cybersecurity procurement language for ICS. References: Web: https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf

Control Enhancements: (1, 2, 9) ICS Supplemental Guidance: Developers may not have access to required information.

システム及びサービス取得 – SA

システム及びサービス取得ファミリのカスタマイズ考慮事項
ICS がある制御の特定のシステム及びサービス取得要件に対応していない状況では、全体的なカスタマイズガイダンスに従って補償的管理策を採用する。
補償的管理策の例が必要に応じて、管理策ごとに示される。

補足ガイダンス
利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

SA-1　システム及びサービス取得ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-1	**システム及びサービス取得ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

SA-2　リソース割当

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-2	**リソース割当**	選定	選定	選定

ICS 補足ガイダンスなし

SA-3　システム開発ライフサイクル

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-3	**システム開発ライフサイクル**	選定	選定	選定

ICS 補足ガイダンスなし

SA-4　取得プロセス

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-4	**取得プロセス**	選定	選定	選定
SA-4 (1)	*取得プロセス | セキュリティ対策の機能特性*		選定	選定
SA-4 (2)	*取得プロセス | セキュリティ対策の設計・実装情報*		選定	選定
SA-4 (9)	*取得プロセス | 機能・ポート・プロトコル 実用サービス*		選定	選定
SA-4 (10)	*取得プロセス | 認可済み PIV 製品の利用*	選定	選定	選定

ICS 補足ガイダンス：ICS のセキュリティは、歴史的に物理的な保護と隔離が重点だったため、ベンダーや開発者はサイバーセキュリティになじみがない。組織は ICS サプライヤとともに、サイバーセキュリティに対する意識高揚の必要性を予期すべきである。SCADA 制御システム調達プロジェクトには、ICS のサイバーセキュリティ用語が示されている。参考文献：ウェブ：https://ics-cert.us- cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf
管理拡張：(1, 2, 9) ICS 補足ガイダンス：開発者は必要な情報を利用できない可能性がある。

Control Enhancement: (10) ICS Supplemental Guidance: Example compensating controls include employing external products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability in conjunction with ICS products.

SA-5 INFORMATION SYSTEM DOCUMENTATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-5	**Information System Documentation**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SA-8 SECURITY ENGINEERING PRINCIPLES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-8	**Security Engineering Principles**		Selected	Selected

No ICS Supplemental Guidance.

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-9	**External Information System Services**	Selected	Selected	Selected
SA-9 (2)	*EXTERNAL INFORMATION SYSTEMS | IDENTIFICATION OF FUNCTIONS / PORTS / PROTOCOLS / SERVICES*		Selected	Selected

No ICS Supplemental Guidance.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-10	**Developer Configuration Management**		Selected	Selected

No ICS Supplemental Guidance.

SA-11 DEVELOPER SECURITY TESTING AND EVALUATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-11	**Developer Security Testing and Evaluation**		Selected	Selected

No ICS Supplemental Guidance.

SA-12 SUPPLY CHAIN PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-12	**Supply Chain Protection**			Selected

No ICS Supplemental Guidance.

管理拡張：(10) ICS 補足ガイダンス：補償的管理策の例として、ICS 製品に関連した身分証明（PIV）機能の FIPS 201 承認製品リストの外部製品採用がある。

SA-5　情報システム文書化

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-5	**情報システム文書化**	選定	選定	選定

ICS 補足ガイダンスなし

SA-8　セキュリティエンジニアリング原則

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-8	**セキュリティエンジニアリンク原則**		選定	選定

ICS 補足ガイダンスなし

SA-9　外部情報システムサービス

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-9	**外部情報システムサービス**	選定	選定	選定
SA-9 (2)	*外部情報システム | 機能・ポート・プロトコル・サービスの識別*		選定	選定

ICS 補足ガイダンスなし

SA-10　開発者設定管理

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-10	**開発者設定管理**		選定	選定

ICS 補足ガイダンスなし

SA-11　開発者セキュリティ試験評価

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-11	**開発者セキュリティ試験評価**		選定	選定

ICS 補足ガイダンスなし

SA-12　サプライチェーン保護

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-12	**サプライチェーン保護**			選定

ICS 補足ガイダンスなし

SA-15 DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-15	**Development Process, Standards, and Tools**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SA-16 DEVELOPER-PROVIDED TRAINING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-16	**Developer-Provided Training**			Selected

No ICS Supplemental Guidance.

SA-17 DEVELOPER SECURITY ARCHITECTURE AND DESIGN

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-17	**Developer Security Architecture and Design**			Selected

No ICS Supplemental Guidance.

SA-15　開発プロセス・規格・ツール

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-15	**開発プロセス・規格・ツール**			選定

ICS 補足ガイダンスなし

SA-16　開発者による訓練

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-16	**開発者による訓練**			選定

ICS 補足ガイダンスなし

SA-17　開発者セキュリティアーキテクチャ・設計

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SA-17	**開発者セキュリティアーキテクチャ・設計**			選定

ICS 補足ガイダンスなし

SYSTEM AND COMMUNICATIONS PROTECTION - SC

Tailoring Considerations for System and Communications Protection Family

The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. While the legacy devices commonly found within ICS often lack direct support of cryptographic functions, compensating controls (e.g., encapsulations) may be used to meet the intent of the control.

In situations where the ICS cannot support the specific System and Communications Protection requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-1	**System and Communications Protection Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

SC-2 APPLICATION PARTITIONING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-2	**Application Partitioning**		Selected	Selected

ICS Supplemental Guidance: Systems used to manage the ICS should be separate from the operational ICS components. Example compensating controls include providing increased auditing measures.

SC-3 SECURITY FUNCTION ISOLATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-3	**Security Function Isolation**			Selected

ICS Supplemental Guidance: Example compensating controls include providing increased auditing measures, limiting network connectivity, architectural allocation.

SC-4 INFORMATION IN SHARED RESOURCES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-4	**Information in Shared Resources**		Selected	Selected

ICS Supplemental Guidance: Example compensating controls include architecting the use of the ICS to prevent sharing system resources.

システム及び通信保護 - SC

システム及び通信保護ファミリのカスタマイズ考慮事項
暗号化の使用は、セキュリティ上の必要性とシステムパフォーマンスへの悪影響を慎重に考慮して判断する。例えば、暗号を利用するにより生じる待ち時間が、ICS の運用パフォーマンスを阻害しないか組織は検討する。通常 ICS に見られるレガシーデバイスは、暗号関数に直接対応していないことが多いため、補償的管理策（カプセル化等）を使用して、管理目的を達成する。
ICS がある制御の特定のシステム及び通信保護要件に対応していない状況では、全体的なカスタマイズガイダンスに従って補償的管理策を採用する。補償的管理策の例が必要に応じて、管理策ごとに示される。

補足ガイダンス
利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

SC-1　システム及び通信保護ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-1	システム通信保護ポリシー・手順	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

SC-2　アプリケーション分割

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-2	アプリケーション分割		選定	選定

ICS 補足ガイダンス：ICS の管理に使用するシステムは、実用 ICS コンポーネントと別にすべきである。補償的管理策の例として、監査手段の強化がある。

SC-3　セキュリティ機能の隔離

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-3	セキュリティ機能の隔離			選定

ICS 補足ガイダンス：補償的管理策の例として、監査手段の強化、ネットワーク接続の制限、アーキテクチャ割当がある。

SC-4　共有リソース内情報

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-4	共有リソース内情報		選定	選定

ICS 補足ガイダンス：補償的管理策の例として、ICS の使用要領を設定してシステムリソースを共有しないようにする方法がある。

SC-5 DENIAL OF SERVICE PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-5	**Denial of Service Protection**	Selected	Selected	Selected

ICS Supplemental Guidance: Example compensating controls include ensuring a loss of communication results in the ICS operating in nominal or safe mode. Risk-based analysis informs the establishment of policy and procedure.

SC-7 BOUNDARY PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-7	**Boundary Protection**	Selected	Selected	Selected
SC-7 (3)	*BOUNDARY PROTECTION | ACCESS POINTS*		Selected	Selected
SC-7 (4)	*BOUNDARY PROTECTION | EXTERNAL TELECOMMUNICATIONS SERVICES*		Selected	Selected
SC-7 (5)	*BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION*		Selected	Selected
SC-7 (7)	*BOUNDARY PROTECTION | PREVENT SPLIT TUNNELING FOR REMOTE DEVICES*		Selected	Selected
SC-7 (8)	*BOUNDARY PROTECTION | ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS*			Selected
SC-7 (18)	*BOUNDARY PROTECTION | FAIL SECURE*		Added	**Selected**
SC-7 (21)	*BOUNDARY PROTECTION | ISOLATION OF INFORMATION SYSTEM COMPONENTS*			Selected

No ICS Supplemental Guidance.

Control Enhancement: (3, 4, 5, 7, 8, 21) No ICS Supplemental Guidance.

Control Enhancement: (18) ICS Supplemental Guidance: The organization selects an appropriate failure mode (e.g., permit or block all communications).

Rationale for adding SC-7 (18) to Moderate Baseline: As part of the architecture and design of the ICS, the organization selects an appropriate failure mode in accordance with the function performed by the ICS and the operational environment. The ability to choose the failure mode for the physical part of the ICS differentiates the ICS from other IT systems. This choice may be a significant influence in mitigating the impact of a failure.

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-8	**Transmission Confidentiality and Integrity**		Selected	Selected
SC-8 (1)	**transmission confidentiality and integrity | cryptographic or alternate physical protection**		Selected	Selected

No ICS Supplemental Guidance.

Control Enhancement: (1) ICS Supplemental Guidance: The organization explores all possible cryptographic integrity mechanisms (e.g., digital signature, hash function). Each mechanism has a different delay impact.

SC-10 NETWORK DISCONNECT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-10	**Network Disconnect**		Selected	Selected

ICS Supplemental Guidance: Example compensating controls include providing increased auditing measures or limiting remote access privileges to key personnel.

SC-5　サービス保護妨害

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-5	**サービス保護妨害**	選定	選定	選定

ICS 補足ガイダンス：補償的管理策の例として、通信喪失時に ICS の運用が公称モード又はセーフモードになるようにする方法がある。リスクに立脚した分析により、ポリシー・手順の設定情報が得られる。

SC-7　境界の保護

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-7	**境界の保護**	選定	選定	選定
SC-7 (3)	*境界の保護 | アクセスポイント*		選定	選定
SC-7 (4)	*境界の保護 | 外部電気通信サービス*		選定	選定
SC-7 (5)	*境界の保護 | デフォルトで拒絶・例外で許諾*		選定	選定
SC-7 (7)	*境界の保護 | 遠隔デバイスのスプリットトンネリング防止*		選定	選定
SC-7 (8)	*境界の保護 | 認証済みプロへのキシサーバトラフィックの経路指定*			選定
SC-7 (18)	*境界の保護 | フェールセキュア*		追加	**選定**
SC-7 (21)	*境界の保護 | 情報システムコンポーネントの隔離*			選定

ICS 補足ガイダンスなし

管理拡張：(3, 4, 5, 7, 8, 21) ICS 補足ガイダンスなし

管理拡張：(18) ICS 補足ガイダンス：組織は適当な故障モードを選択する（全ての通信を許可又はブロック等）。

SC-7 (18)を中ベースラインに追加する理由：ICS アーキテクチャ及び設計の一貫として、組織は、ICS 及び運用環境が実施する機能に従い、適当な故障モードを選択する。ICS の物理部分に故障モードを選択できる能力は、ICS と他の IT システムとの違いである。この選択は、故障の影響を緩和する上で大きな効果がある。

SC-8　通信機密性・完全性

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-8	**通信機密性・完全性**		選定	選定
SC-8 (1)	*通信機密性・完全性 | 暗号化又は代替物理的保護*		選定	選定

ICS 補足ガイダンスなし

管理拡張：(1) ICS 補足ガイダンス：組織はあらゆる暗号保全メカニズムを活用する（デジタル署名、ハッシュ関数等）。各メカニズムの遅延影響はそれぞれ異なる。

SC-10　ネットワーク切断

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-10	**ネットワーク切断**		選定	選定

ICS 補足ガイダンス：補償的管理策の例として、監査手段の強化やリモートアクセス特権を重要な人員に制限する方法がある。

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-12	**Cryptographic Key Establishment and Management**	Selected	Selected	Selected
SC-12 (1)	*CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY*			Selected

ICS Supplemental Guidance: The use of cryptographic key management in ICS is intended to support internal nonpublic use.
Control Enhancement: (1) No ICS Supplemental Guidance.

SC-13 CRYPTOGRAPHIC PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-13	**Cryptographic Protection**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SC-15 COLLABORATIVE COMPUTING DEVICES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-15	**Collaborative Computing Devices**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-17	**Public Key Infrastructure Certificates**		Selected	Selected

No ICS Supplemental Guidance.

SC-18 MOBILE CODE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-18	**Mobile Code**		Selected	Selected

No ICS Supplemental Guidance.

SC-19 VOICE OVER INTERNET PROTOCOL

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-19	**Voice Over Internet Protocol**		Selected	Selected

ICS Supplemental Guidance: The use of VoIP technologies is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-12 暗号鍵設定管理

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-12	**暗号鍵設定管理**	選定	選定	選定
SC-12 (1)	*暗号鍵設定管理 | 可用性*			選定

ICS 補足ガイダンス：暗号鍵管理を ICS で使用する目的は、内部の非公開利用に対応するためである。

管理拡張：(1) ICS 補足ガイダンスなし

SC-13 暗号保護

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-13	**暗号保護**	選定	選定	選定

ICS 補足ガイダンスなし

SC-15 共同コンピューティングデバイス

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-15	**共同コンピューティングデバイス**	選定	選定	選定

ICS 補足ガイダンスなし

SC-17 公開鍵インフラ証明書

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-17	**公開鍵インフラ証明書**		選定	選定

ICS 補足ガイダンスなし

SC-18 モバイルコード

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-18	**モバイルコード**		選定	選定

ICS 補足ガイダンスなし

SC-19 VoIP

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-19	**VoIP**		選定	選定

ICS 補足ガイダンス：VoIP 技術の利用は、ICS の運用に悪影響がないことを検証し、慎重に検討してから判断する。

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-20	**Secure Name /Address Resolution Service (Authoritative Source)**	Selected	Selected	Selected

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operation of the ICS.

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-21	**Secure Name /Address Resolution Service (Recursive or Caching Resolver)**	Selected	Selected	Selected

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operation of the ICS.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-22	**Architecture and Provisioning for Name/Address Resolution Service**	Selected	Selected	Selected

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-23 SESSION AUTHENTICITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-23	**Session Authenticity**		Selected	Selected

ICS Supplemental Guidance: Example compensating controls include auditing measures.

SC-24 FAIL IN KNOWN STATE

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-24	**Fail in Known State**		Added	Selected

ICS Supplemental Guidance: The organization selects an appropriate failure state. Preserving ICS state information includes consistency among ICS state variables and the physical state which the ICS represents (e.g., whether valves are open or closed, communication permitted or blocked, continue operations).

Rationale for adding SC-24 to moderate baseline: As part of the architecture and design of the ICS, the organization selects an appropriate failure state of an ICS in accordance with the function performed by the ICS and the operational environment. The ability to choose the failure mode for the physical part of the ICS differentiates the ICS from other IT systems. This choice may be a significant influence in mitigating the impact of a failure, since it may be disruptive to ongoing physical processes (e.g., valves failing in closed position may adversely affect system cooling).

SC-20　セキュアな名前/アドレス解決サービス（権限ソース）

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-20	セキュアな名前/アドレス解決サービス（権限ソース）	選定	選定	選定

ICS 補足ガイダンス：セキュアな名前/アドレス解決サービスの利用は、ICS の運用に悪影響がないことを検証し、慎重に検討してから判断する。

SC-21　セキュアな名前/アドレス解決サービス（再帰又はキャッシングリゾルバ）

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-21	セキュアな名前/アドレス解決サービス（再帰又はキャッシングリゾルバ）	選定	選定	選定

ICS 補足ガイダンス：セキュアな名前/アドレス解決サービスの利用は、ICS の運用に悪影響がないことを検証し、慎重に検討してから判断する。

SC-22　名前/アドレス解決サービス用アーキテクチャープロビジョニング

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-22	名前/アドレス解決サービス用アーキテクチャープロビジョニング	選定	選定	選定

ICS 補足ガイダンス：セキュアな名前/アドレス解決サービスの利用は、ICS の運用に悪影響がないことを検証し、慎重に検討してから判断する。

SC-23　セッション認証

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-23	セッション認証		選定	選定

ICS 補足ガイダンス：補償的管理策の例として、監査手段がある。

SC-24　既知状態の失敗

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-24	既知状態の失敗		追加	選定

ICS 補足ガイダンス：組織は適当な故障状態を選択する。ICS 状態情報の保存には、ICS 状態変数と ICS の物理的状態の整合性が含まれる（バルブの開又は閉、通信の許可又はブロック等）。

SC-24 を中ベースラインに追加する理由：ICS アーキテクチャ及び設計の一貫として、組織は、ICS 及び運用環境が実施する機能に従い、適当な ICS の故障状態を選択する。ICS の物理部分に故障モードを選択できる能力は、ICS と他の IT システムとの違いである。この選択は、進行中の物理プロセスを中断するため、故障の影響を緩和する上で大きな効果がある（バルブが閉位置になるとシステム冷却に悪影響が出るなど）。

SC-28 PROTECTION OF INFORMATION AT REST

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-28	**Protection of Information at Rest**		Selected	Selected

ICS Supplemental Guidance: The use of cryptographic mechanisms is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-39 PROCESS ISOLATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-39	**Process Isolation**	Selected	Selected	Selected

ICS Supplemental Guidance: Example compensating controls include partition processes to separate platforms.

SC-41 PORT AND I/O DEVICE ACCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SC-41	**Port and I/O Device Access**	Added	Added	Added

No ICS Supplemental Guidance.

Rationale for adding SC-24 to all baselines: The function of ICS can be readily determined in advance, making it easier to identify ports and I/O devices that are unnecessary. Disabling or removing ports reinforces air-gap policy.

SC-28　休眠情報の保護

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-28	休眠情報の保護		選定	選定

ICS 補足ガイダンス：暗号メカニズムの利用は、ICS の運用に悪影響がないことを検証し、慎重に検討してから判断する。

SC-39　プロセス隔離

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-39	プロセス隔離	選定	選定	選定

ICS 補足ガイダンス：補償的管理策の例として、プラットホームを分離するためのパーティションプロセスがある。

SC-41　ポート及び I/O デバイスアクセス

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SC-41	ポート及び I/O デバイスアクセス	追加	追加	追加

ICS 補足ガイダンスなし

SC-24 を全てのベースラインに追加する理由：ICS の機能は予めすぐに決められるようにし、不要なポート及び I/O デバイスの識別を容易にする。ポートの無効化や削除は、エアギャップポリシーを強化する。

SYSTEM AND INFORMATION INTEGRITY - SI

Tailoring Considerations for System and Information Integrity Family

In situations where the ICS cannot support the specific System and Information Integrity requirements of a control, the organization employs compensating controls in accordance with the general tailoring guidance. Examples of compensating controls are given with each control, as appropriate.

Supplemental Guidance
Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-1	**System and Information Integrity Policy and Procedures**	Selected	Selected	Selected

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS and the relationship to non-ICS systems.

SI-2 FLAW REMEDIATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-2	**Flaw Remediation**	Selected	Selected	Selected
SI-2 (1)	*FLAW REMEDIATION | CENTRAL MANAGEMENT*			Selected
SI-2 (2)	*FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS*		Selected	Selected

ICS Supplemental Guidance: Flaw Remediation is complicated since many ICS employ operating systems and other software that is not current, is no longer being maintained by the vendors, and is not resistant to current threats. ICS operators are often dependent on product vendors to validate the operability of a patch and also sometimes to perform the installation. Often flaws cannot be remediated based on circumstances outside of the ICS operator's control (e.g., lack of a vendor patch). Sometime the organization has no choice but to accept additional risk. In these situations, compensating controls should be implemented (e.g., limit the exposure of the vulnerable system). Other compensating controls that do not decrease the residual risk but increase the ability to respond may be desirable (e.g., provide a timely response in case of an incident; devise a plan to ensure the ICS can identify the exploitation of the flaw). Testing flaw remediation in an ICS may require more resources than the organization can commit.

Control Enhancement: (1) No ICS Supplemental Guidance.

Control Enhancement: (2) ICS Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to conduct and report on the status of flaw remediation, the organization employs nonautomated mechanisms or procedures which incorporate methods to apply, track, and verify mitigation efforts as compensating controls in accordance with the general tailoring guidance.

SI-3 MALICIOUS CODE PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-3	**Malicious Code Protection**	Selected	Selected	Selected
SI-3 (1)	*MALICIOUS CODE PROTECTION | CENTRAL MANAGEMENT*		Selected	Selected
SI-3 (2)	*MALICIOUS CODE PROTECTION | AUTOMATIC UPDATES*		Selected	Selected

ICS Supplemental Guidance: The use and deployment of malicious code protection is determined after careful consideration and after verification that it does not adversely impact the operation of the ICS. Malicious code

システム及び情報の完全性 - SI

システム及び情報の安全性ファミリのカスタマイズ考慮事項

ICS がある制御の特定のシステム及び情報完全性要件に対応していない状況では、全体的なカスタマイズガイダンスに従って補償的管理策を採用する。
補償的管理策の例が必要に応じて、管理策ごとに示される。

補足ガイダンス

利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

SI-1　システム及び情報完全性ポリシー・手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-1	**システム情報完全性ポリシー・手順**	選定	選定	選定

ICS 補足ガイダンス：ポリシーは特に ICS の固有の特性・要件及び ICS 以外のシステムとの関係を取り上げる。

SI-2　欠陥修正

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-2	**欠陥修正**	選定	選定	選定
SI-2 (1)	*欠陥修正 | 集中管理*			選定
SI-2 (2)	*欠陥修正 | 自動欠陥修正状態*		選定	選定

ICS 補足ガイダンス：ICS の多くは最新版以外の OS やソフトウエアを使用し、ベンダーも保守を行っておらず、最新の脅威に抵抗性がないため、欠陥修正は複雑となる。ICS 操作員は、パッチの動作検証や、ときにはインストールを行うだけでも、製品ベンダーに依存することが多い。ICS 操作員の管理能力を超えている状況では、欠陥の修正ができないことが多い（ベンダーパッチの欠如等）。組織は、付加的なリスクを受け入れざるを得ないことがある。このような状況では、補償的管理策を行う（脆弱なシステムの露出制限等）。その他の補償的管理策としては、残留リスクは減らせないまでも、対応能力が高めるようなものが望ましい（インシデント時にタイムリーな対応や、悪用されている欠陥を特定できる計画の作成等）。ICS の欠陥修正検証は、組織が投入できる以上のリソースを要する場合がある。

管理拡張：(1) ICS 補足ガイダンスなし

管理拡張：(2) ICS 補足ガイダンス：ICS が欠陥修正実施・報告の自動メカニズムに対応していない状況では、全体的なカスタマイズガイダンスに従って、組織は非自動メカニズム又は手順を緩和努力の適用・追跡・検証のための補償的管理策として採用する。

SI-3　悪意あるコード保護

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-3	**悪意あるコード保護**	選定	選定	選定
SI-3 (1)	*悪意あるコード保護 | 集中管理*		選定	選定
SI-3 (2)	*悪意あるコード保護 | 自動更新*		選定	選定

ICS 補足ガイダンス：悪意あるコード保護の利用は、ICS の運用に悪影響がないことを検証し、慎重に検討してから判断する。悪意あるコード

protection tools should be configured to minimize their potential impact on the ICS (e.g., employ notification rather than quarantine). Example compensating controls include increased traffic monitoring and auditing.

Control Enhancement: (1) ICS Supplemental Guidance: The organization implements central management of malicious code protection with consideration of the impact on operation of the ICS. Example compensating controls include increased auditing.

Control Enhancement: (2) ICS Supplemental Guidance: The organization implements automatic updates of malicious code protection with consideration of the impact on operation of the ICS. In situations where the ICS cannot support the use of automatic update of malicious code protection, the organization employs nonautomated procedures as compensating controls in accordance with the general tailoring guidance.

SI-4 INFORMATION SYSTEM MONITORING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-4	**Information System Monitoring**	Selected	Selected	Selected
SI-4 (2)	*INFORMATION SYSTEM MONITORING | AUTOMATED TOOLS FOR REAL-TIME ANALYSIS*		Selected	Selected
SI-4 (4)	*INFORMATION SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC*		Selected	Selected
SI-4 (5)	*INFORMATION SYSTEM MONITORING | SYSTEM-GENERATED ALERTS*		Selected	Selected

ICS Supplemental Guidance: The organization ensures that the use of monitoring tools and techniques does not adversely impact the operational performance of the ICS. Example compensating controls include deploying sufficient network monitoring.

Control Enhancement: (2) ICS Supplemental Guidance: In situations where the ICS cannot support the use of automated tools to support near-real-time analysis of events, the organization employs compensating controls (e.g., providing an auditing capability on a separate system, nonautomated mechanisms or procedures) in accordance with the general tailoring guidance.

Control Enhancement: (4) ICS Supplemental Guidance: In situations where the ICS cannot monitor inbound and outbound communications traffic, the organization employs compensating controls include providing a monitoring capability on a separate information system.

Control Enhancement: (5) ICS Supplemental Guidance: Example compensating controls include manual methods of generating alerts.

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-5	**Security Alerts, Advisories, and Directives**	Selected	Selected	Selected
SI-5 (1)	*SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | AUTOMATED ALERTS AND ADVISORIES*			Selected

ICS Supplemental Guidance: The DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) generates security alerts and advisories relative to ICS http://ics-cert.us-cert.gov/ .

Control Enhancement: (1) No ICS Supplemental Guidance.

SI-6 SECURITY FUNCTIONALITY VERIFICATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-6	**Security Function Verification**			Selected

ICS Supplemental Guidance: The shutting down and restarting of the ICS may not always be feasible upon the identification of an anomaly; these actions should be scheduled according to ICS operational requirements.

保護ツールは、ICS への影響が最小になるように設定すべきである（検疫ではなく通知を採用するなど）。補償的管理策の例として、トラフィック監視と監査の強化がある。

管理拡張：(1) ICS 補足ガイダンス：組織は、ICS の運用への影響を考慮に入れて、悪意あるコード保護の集中管理を実施する。補償的管理策の例として、監査の強化がある。

管理拡張：(2) ICS 補足ガイダンス：組織は、ICS の運用への影響を考慮に入れて、悪意あるコード保護の自動更新を実施する。ICS が悪意あるコード保護の自動更新利用に対応していない状況では、組織は、全体的なカスタマイズガイダンスに従って非自動メカニズムを補償的管理策として採用する。

SI-4　情報システム監視

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-4	**情報システム監視**	選定	選定	選定
SI-4 (2)	*情報システム監視 | リアルタイム分析用自動ツール*		選定	選定
SI-4 (4)	*情報システム監視 | 着信・発信通信トラフィック*		選定	選定
SI-4 (5)	*情報システム監視 | システム生成アラート*		選定	選定

ICS 補足ガイダンス：組織は、監視ツール・技術の利用が ICS の運用パフォーマンスに悪影響しないようにする。補償的管理策の例として、十分なネットワーク監視の展開がある。

管理拡張：(2) ICS 補足ガイダンス：ICS がほぼリアルタイムでの事象分析対応自動ツールに対応していない状況では、組織は、全体的なカスタマイズガイダンスに従って補償的管理策を採用する（別システムへの監査機能付与、非自動メカニズム・手順等）。

管理拡張：(4) ICS 補足ガイダンス：ICS が着信・発信通信トラフィックを監視できない状況では、組織は、別情報システムへの監視機能付与等の補償的管理策を採用する。

管理拡張：(5) ICS 補足ガイダンス：補償的管理策の例として、手動によるアラート生成がある。

SI-5　セキュリティ警報・勧告・指示

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-5	**セキュリティ警報・勧告・指示**	選定	選定	選定
SI-5 (1)	*セキュリティ警報・勧告・指示 | 自動アラート・勧告*			選定

ICS 補足ガイダンス：DHS の産業用制御システムサイバー緊急対応チーム(ICS-CERT)は、ICS に関連した接続アラート及び勧告を作成している。http://ics-cert.us-cert.gov/

管理拡張：(1) ICS 補足ガイダンスなし

SI-6　セキュリティ機能検証

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-6	**セキュリティ機能検証**			選定

ICS 補足ガイダンス：ICS の遮断及び再起動は、異状検出時に必ずしも直ちに可能ではない。ICS 運用要件に従ってスケジュールを立てるべきである。

SI-7 SOFTWARE AND INFORMATION INTEGRITY

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-7	**Software, Firmware, and Information Integrity**		Selected	Selected
SI-7 (1)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS*		Selected	Selected
SI-7 (2)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS*			Selected
SI-7 (5)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS*			Selected
SI-7 (7)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE*		Selected	Selected
SI-7 (14)	*SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE CODE*			Selected

ICS Supplemental Guidance: The organization determines whether the use of integrity verification applications would adversely impact the operation of the ICS and employs compensating controls (e.g., manual integrity verifications that do not affect performance.

Control Enhancements: (1) ICS Supplemental Guidance: The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the ICS.

Control Enhancement: (2) ICS Supplemental Guidance: In situations where the organization cannot employ automated tools that provide notification of integrity discrepancies, the organization employs nonautomated mechanisms or procedures. Example compensating controls include performing scheduled manual inspections for integrity violations.

Control Enhancement: (5) ICS Supplemental Guidance: The shutting down and restarting of the ICS may not always be feasible upon the identification of an anomaly; these actions should be scheduled according to ICS operational requirements.

Control Enhancement: (7) ICS Supplemental Guidance: In situations where the ICS cannot detect unauthorized security-relevant changes, the organization employs compensating controls (e.g., manual procedures) in accordance with the general tailoring guidance.

Control Enhancement: (14) No ICS Supplemental Guidance.

SI-8 SPAM PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-8	**Spam Protection**		Selected	Selected
SI-8 (1)	*SPAM PROTECTION | CENTRAL MANAGEMENT OF PROTECTION MECHANISMS*		Selected	Selected
SI-8 (2)	*SPAM PROTECTION | AUTOMATIC UPDATES*		Selected	Selected

ICS Supplemental Guidance: ICS spam protection may be implemented by removing spam transport mechanisms, functions and services (e.g., electronic mail, Internet access) from the ICS. If any spam transport mechanisms, functions and services are present in the ICS, spam protection in ICS takes into account operational characteristics of ICS that differ from general purpose information systems, (e.g., unusual traffic flow that may be misinterpreted and detected as spam. Example compensating controls include whitelist mail transfer agents (MTA), digitally signed messages, acceptable sources, and acceptable message types.

Control Enhancement: (1) ICS Supplemental Guidance: Example compensating controls include employing local mechanisms or procedures.

Control Enhancement: (2) No ICS Supplemental Guidance.

SI-7 ソフトウエア及び情報の完全性

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-7	**ソフトウエア・ファームウエア・情報の完全性**		選定	選定
SI-7 (1)	*ソフトウエア・ファームウエア・情報の完全性 | 完全性チェック*		選定	選定
SI-7 (2)	*ソフトウエア・ファームウエア・情報の完全性 | 完全性違反の自動通知*			選定
SI-7 (5)	*ソフトウエア・ファームウエア・情報の完全性 | 完全性違反の自動対応*			選定
SI-7 (7)	*ソフトウエア・ファームウエア・情報の完全性 | 検出・対応の一体化*		選定	選定
SI-7 (14)	*ソフトウエア・ファームウエア・情報の完全性 | バイナリ又はマシン実行可能コード*			選定

ICS 補足ガイダンス：組織は、完全性検証アプリケーションの利用により、ICS の運用に悪影響が及ばないか判定し、補償的管理策を採用する（パフォーマンスに影響しない手動検証等）。

管理拡張：(1) ICS 補足ガイダンス：組織は、完全性検証アプリケーションの利用が ICS の運用パフォーマンスに悪影響しないようにする。

管理拡張：(2) ICS 補足ガイダンス：完全性の不備を通知する自動ツールを採用できない状況では、組織は、非自動メカニズム・手順を採用する。補償的管理策の例として、完全性違反に対するスケジュール化された手動点検の実施がある。

管理拡張：(5) ICS 補足ガイダンス：ICS の遮断及び再起動は、異状検出時に必ずしも直ちに可能というわけではない。ICS 運用要件に従ってスケジュールを立てるべきである。

管理拡張：(7) ICS 補足ガイダンス：ICS がセキュリティ関連の無断変更を検出できない状況では、組織は、全体的なカスタマイズガイダンスに従って補償的管理策（手動手順等）を採用する。

管理拡張：(14) ICS 補足ガイダンスなし

SI-8 スパム保護

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-8	**スパム保護**		選定	選定
SI-8 (1)	*スパム保護 | 保護メカニズムの集中管理*		選定	選定
SI-8 (2)	*スパム保護 | 自動更新*		選定	選定

ICS 補足ガイダンス：ICS のスパム保護は、スパム転送メカニズム、機能及びサービス（電子メール、インターネットアクセス等）を排除することにより行われる。スパム転送メカニズム、機能及びサービスが ICS に存在している場合、ICS のスパム保護は、汎用的な情報システム（スパムとして誤解・検出される通常と違うトラフィックフロー等）とは異なる ICS の運用特性を考慮に入れる。補償的管理策の例として、ホワイトリストメール転送エージェント（MTA）、デジタル署名入りメッセージ、受け入れられるソース、受け入れられるメッセージタイプがある。

管理拡張：(1) ICS 補足ガイダンス：補償的管理策の例として、ローカルメカニズム又はローカル手順がある。

管理拡張：(2) ICS 補足ガイダンスなし

SI-10 INFORMATION INPUT VALIDATION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-10	**Information Input Validation**		Selected	Selected

No ICS Supplemental Guidance.

SI-11 ERROR HANDLING

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-11	**Error Handling**		Selected	Selected

No ICS Supplemental Guidance.

SI-12 INFORMATION HANDLING AND RETENTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-12	**Information Handling and Retention**	Selected	Selected	Selected

No ICS Supplemental Guidance.

SI-13 PREDICTABLE FAILURE PREVENTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-13	**Predictable Failure Prevention**			Added

ICS Supplemental Guidance: Failures in ICS can be stochastic or deterministic. Stochastic failures can be analyzed using probability theory, while analysis of deterministic failures is based on non-random properties of the system. Known ICS failure modes and causes are considered. The calculation and use of statistical descriptors, such as Mean Time To Failure (MTTF), should incorporate additional analysis to determine how those failures manifest within the cyber and physical domains. Knowledge of these possible manifestations may be necessary to detect whether a failure has occurred within the ICS, as failures of the information systems may not be easily identifiable. Emergent properties, which may arise both within the information systems and physical processes, can potentially cause system failures should be incorporated into the analysis. For example, cumulative effects of resource exhaustion (e.g., memory leakage) or errors (e.g., rounding and truncation) can occur when ICS processes execute for unexpectedly long periods. Deterministic failures (e.g., integer counter overflow), once identified, are preventable.

Often substitute components may not be available or may not be sufficient to protect against faults occurring before predicted failure. Non-automated mechanisms or physical safeguards should be in place in order to protect against these failures.
In addition to information concerning newly discovered vulnerabilities (i.e., latent flaws) potentially affecting the system/applications that are discovered by forensic studies, new vulnerabilities may be identified by organizations with responsibility for disseminating vulnerability information (e.g., ICS-CERT) based upon an analysis of a similar pattern of incidents reported to them or vulnerabilities reported by other researchers.

Related controls: IR-5, IR-6, RA-5, SI-2, SI-5, SI-11.

Rationale for adding control to baseline: ICS are designed and built with certain boundary conditions, design parameters, and assumptions about their environment and mode of operation. ICS may run much longer than conventional systems, allowing latent flaws to become effective that are not manifest in other environments. For example, integer overflow might never occur in systems that are re-initialized more frequently than the occurrence of the overflow. Experience and forensic studies of anomalies and incidents in ICS can lead to identification of emergent properties that were previously unknown, unexpected, or unanticipated. Preventative and restorative

SI-10　情報入力検証

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-10	情報入力検証		選定	選定

ICS 補足ガイダンスなし

SI-11　エラー処理

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-11	エラー処理		選定	選定

ICS 補足ガイダンスなし

SI-12　情報処理保留

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-12	情報処理保留	選定	選定	選定

ICS 補足ガイダンスなし

SI-13　予想される故障の防止

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-13	予想される故障の防止			追加

ICS 補足ガイダンス：ICS における故障は、確率的なものか決定論的なもののいずれかである。確率的故障は確立理論で分析でき、決定論的故障の分析は、システムの非ランダム特性を根拠に行う。既知の ICS 故障モード及び原因について考慮する。平均故障時間（MTTF）等の統計記述子の計算及び使用は、サイバー領域及び物理領域におけるそのような故障の出現の仕方を判別する際の補足的な分析力となる。情報システムの故障は容易には特定できないため、そうした出現に関する知識は、ICS での故障発生の有無を判断するのに必要となる。情報システムでも物理プロセスでも生じる創発特性は、システム故障になりかねないため、分析に含めるべきである。例えば、ICS プロセスの実行が予定以上に長びくと、リソースの枯渇（メモリリーク等）による累積影響やエラー（数値の切上げ・切下げ・切捨て等）が生じる。一度特定された決定論的故障（整数カウンタのオーバーフロー等）は予防可能である。

予想される故障よりも前に発生する故障に対しては、代替コンポーネントがないか、あっても十分には防止できない。このような故障に対しては、非自動メカニズム又は物理的対策を講じるべきである。

調査で新たに見つかった、システムやアプリケーションに影響を与えかねない脆弱性（潜在的欠陥）情報に加えて、脆弱性情報の配布担当機関（ICS-CERT 等）によっても新規の脆弱性が明らかにされることがある。そうした情報は、届出のあった同種パターンや外部研究者らから得た脆弱性分析に基づいている。

関連する管理：IR-5, IR-6, RA-5, SI-2, SI-5, SI-11

ベースラインに管理を追加する理由：ICS の設計及び構築には、特定の境界条件、設計パラメータ及び環境・運用モード想定が盛り込まれている。ICS の運転時間は、在来システムよりもはるかに長く、他の環境では表面に出てこない潜在的欠陥が現れる。例えば、整数のオーバーフローは、オーバーフロー頻度よりも多く再初期化されるシステムでは、まず生じることがない。ICS における異常及びインシデントの調査経験が、それまで知られておらず、予想・予期されていなかった創発特性の特定に結びついている。

actions (e.g., re-starting the system or application) are prudent but may not be acceptable for operational reasons in ICS.

SI-16 MEMORY PROTECTION

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-16	**Memory Protection**		Selected	Selected

No ICS Supplemental Guidance.

SI-17 FAIL-SAFE PROCEDURES

CNTL NO.	CONTROL NAME *Control Enhancement Name*	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-17	**Fail-Safe Procedures**	Added	Added	Added

ICS Supplemental Guidance: The selected failure conditions and corresponding procedures may vary among baselines. The same failure event may trigger different response depending on the impact level. Mechanical and analog system can be used to provide mechanisms to ensure fail-safe procedures. Fail-safe states should incorporate potential impacts to human safety, physical systems, and the environment. Related controls: CP-6.

Rationale for adding SI-17 to all baselines: This control provides a structure for the organization to identify their policy and procedures for dealing with failures and other incidents. Creating a written record of the decision process for selecting incidents and appropriate response is part of risk management in light of changing environment of operations.

予防・回復行動（システムやアプリケーションの再起動等）は良識的な方法ではあるが、ICS の運用上の理由から受け入れられない。

SI-16 メモリ保護

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-16	メモリ保護		選定	選定

ICS 補足ガイダンスなし

SI-17 フェールセーフ手順

管理番号	管理名 *管理拡張名*	管理ベースライン		
		低	中	高
SI-17	フェールセーフ手順	追加	追加	追加

ICS 補足ガイダンス：選定した故障条件と対応手順は、ベースラインに応じて異なる。同じ故障事象でも、影響度によって別の対応となる。機械式・アナログシステムを使用して、フェールセーフ手順メカニズムを備えることができる。フェールセーフ状態は、人員の安全、物理システム及び環境に影響を及ぼしかねない。関連する管理：CP-6

SI-17 を全てのベースラインに追加する理由：組織はこの管理により、故障その他のインシデント処理のポリシー・手順を明らかにできる。インシデントと適切な対応を選ぶ際の決定プロセスを文書にすることは、運用環境の変化という観点から、リスク管理の一部となる

ORGANIZATION-WIDE INFORMATION SECURITY PROGRAM MANAGEMENT CONTROLS - PM

Characteristics of Organization-Wide Information Security Program Management Control Family

Organization-Wide Information Security Program Management Controls are deployed organization-wide supporting the information security program. They are not associated with security control baselines and are independent of any system impact level.

Supplemental Guidance

Supplemental Guidance for all Controls and Control Enhancements in NIST SP 800-53 Rev. 4, Appendix F, should be used in conjunction with the ICS Supplemental Guidance in this overlay, if any.

PM-1 INFORMATION SECURITY PROGRAM PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-1	**Information Security Program Plan Policy and Procedures**

ICS Supplemental Guidance: The policy specifically addresses the unique properties and requirements of ICS, the relationship to non-ICS systems, and the relationship to other programs concerned with operational characteristics of ICS (e.g., safety, efficiency, reliability, resilience).

PM-2 SENIOR INFORMATION SECURITY OFFICER

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-2	**Senior Information Security Officer**

No ICS Supplemental Guidance.

PM-3 INFORMATION SECURITY RESOURCES

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-3	**Information Security Resources**

ICS Supplemental Guidance: Capital planning and investment decisions address all of the relevant technologies and all phases of the life cycle and needs to be informed by ICS experts as well as other subject matter experts (e.g., information security). Marshaling interdisciplinary working teams to advise capital planning and investment decisions can help tradeoff and balance among conflicting equities, objectives, and responsibilities such as capability, adaptability, resilience, safety, security, usability, and efficiency.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-4	**Plan of Action and Milestones Process**

ICS Supplemental Guidance: The plan of action and milestones includes both computational and physical ICS components. Records of observed shortcomings and appropriate remedial action may be maintained in a single document or in multiple coordinated documents (e.g., future engineering plans).

全組織的情報セキュリティプログラム管理対策 - PM

全組織的情報セキュリティプログラム管理対策ファミリの特徴
全組織的情報セキュリティプログラム管理対策は、全組織に展開され、情報セキュリティプログラムを支える。セキュリティ対策ベースラインは付随しておらず、いかなるシステム影響レベルとも無関係である。

補足ガイダンス
利用できる場合には、NIST SP 800-53 第 4 版付録 F にある全ての管理・管理拡張用補足ガイダンスを、このオーバーレイにおいて、ICS 補足ガイダンスと併用すべきである。

PM-1　情報セキュリティプログラム計画書

管理番号	管理名 *管理拡張名*
PM-1	情報セキュリティプログラム計画書ポリシー・手順

ICS 補足ガイダンス：特にポリシーは、ICS 独特の特性及び要件、ICS 以外のシステムとの関係及び ICS の運用特性に関係する他のプログラムとの関係（安全性、効率、信頼性、弾力性等）を取り上げる。

PM-2　上級情報セキュリティ担当官

管理番号	管理名 *管理拡張名*
PM-2	上級情報セキュリティ担当官

ICS 補足ガイダンスなし

PL-3　情報セキュリティリソース

管理番号	管理名 *管理拡張名*
PM-3	情報セキュリティリソース

ICS 補足ガイダンス：主要プランニング及び投資決定は、関係する全技術、全ライフサイクル段階及び ICS 専門家その他の専門家（情報セキュリティ等）からの情報を必要とする分野について取り上げる。主要プランニング及び投資決定について助言する分野横断的な作業チームを結集すれば、能力・適応性・弾力性・安全性・セキュリティ・ユーザビリティ・効率等の公正、目的及び責任の競合について比較考量し、バランスを取る上で支援を差し伸べることができる。

PM-4　行動・マイルストーンプロセス計画書

管理番号	管理名 *管理拡張名*
PM-4	行動・マイルストーンプロセス計画書

ICS 補足ガイダンス：行動・マイルストーン計画書には、コンピュータ関係と物理両面での ICS コンポーネントが含まれる。観察された欠点及び適切な修正処置は、1 冊の文書又は複数の連携文書（将来のエンジニアリング計画書等）として維持する。

PM-5 INFORMATION SYSTEM INVENTORY

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-5	**Information System Inventory**

No ICS Supplemental Guidance.

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-6	**Information Security Measures of Performance**

No ICS Supplemental Guidance.

PM-7 ENTERPRISE ARCHITECTURE

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-7	**Enterprise Architecture**

No ICS Supplemental Guidance.

PM-8 CRITICAL INFRASTRUCTURE PLAN

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-8	**Critical Infrastructure Plan**

No ICS Supplemental Guidance.
References: Executive Order 13636– Improving Critical Infrastructure Cybersecurity, February 12, 2013

PM-9 RISK MANAGEMENT STRATEGY

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-9	**Risk Management Strategy**

ICS Supplemental Guidance: Risk management of ICS is considered along with other organizational risks affecting mission/business success from an organization-wide perspective. Organization-wide risk management strategy includes sector-specific guidance as appropriate.

PM-10 SECURITY AUTHORIZATION PROCESS

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-10	**Security Authorization Process**

ICS Supplemental Guidance: The authorization to operate processes for ICS involves multiple disciplines that have existing approval and risk management process (e.g., physical security, safety). Organization-wide risk management requires harmonization among these disciplines.

PM-5　情報システム目録

管理番号	管理名 *管理拡張名*
PM-5	情報システム目録

ICS 補足ガイダンスなし

PM-6　情報セキュリティに関するパフォーマンス計測

管理番号	管理名 *管理拡張名*
PM-6	情報セキュリティに関するパフォーマンス計測

ICS 補足ガイダンスなし

PM-7　企業アーキテクチャ

管理番号	管理名 *管理拡張名*
PM-7	企業アーキテクチャ

ICS 補足ガイダンスなし

PM-8　重要インフラ計画書

管理番号	管理名 *管理拡張名*
PM-8	重要インフラ計画書

ICS 補足ガイダンスなし

参考文献：大統領命令 13636「重要インフラストラクチャのサイバーセキュリティ改善」（2013 年 2 月 12 日）

PM-9　リスク管理戦略

管理番号	管理名 *管理拡張名*
PM-9	リスク管理戦略

ICS 補足ガイダンス：ICS のリスク管理は、全組織的観点に立ち、任務・事業の成否に影響する組織の他のリスクと合わせて検討する。全組織的管理戦略には、必要に応じて部門固有のガイダンスが含まれる。

PM-10　セキュリティ権限プロセス

管理番号	管理名 *管理拡張名*
PM-10	セキュリティ権限プロセス

ICS 補足ガイダンス：ICS のプロセスを操作する権限には、多数の領域が関係しており、既存の承認・リスク管理プロセスがある（物理的セキュリティ、安全性等）。全組織的リスク管理には、これら領域間での規制が必要となる。

PM-11 MISSION/BUSINESS PROCESS DEFINITION

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-11	**Mission/Business Process Definition**

ICS Supplemental Guidance: Mission/business processes refinement requires protection of physical assets from damage originating in the cyber domain. These needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy.

PM-12 INSIDER THREAT PROGRAM

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-13	**Information Security Workforce**

No ICS Supplemental Guidance.

PM-13 INFORMATION SECURITY WORKFORCE

ICS Supplemental Guidance: All aspects of information security workforce development and improvement programs include knowledge and skill levels in both computational and physical ICS components.

PM-14 TESTING, TRAINING, AND MONITORING

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-14	**Testing, Training, and Monitoring**

No ICS Supplemental Guidance.

PM-15 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-15	**Contacts with Security Groups and Associations**

No ICS Supplemental Guidance.

PM-16 THREAT AWARENESS PROGRAM

CNTL NO.	CONTROL NAME *Control Enhancement Name*
PM-16	**Threat Awareness Program**

ICS Supplemental Guidance: The organization should collaborate and share information about potential incidents on a timely basis. The DHS National Cybersecurity & Communications Integration Center (NCCIC), http://www.dhs.gov/about-national-cybersecurity-communications-integration-center serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) http://ics-cert.us-cert.gov/ics-cert/ collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. Organizations should consider having both an unclassified and classified information sharing capability.

PM-11　任務・事業プロセス定義

管理番号	管理名 *管理拡張名*
PM-11	任務・事業プロセス定義

ICS 補足ガイダンス：任務・事業プロセスを洗練させるには、物理的資産をサイバー領域に起因する損害から保護しなければならない。このような需要は、組織が明らかにした任務・事業上の需要、需要を満たすために選んだ任務・事業プロセス及び組織のリスク管理戦略から生じる。

PM-12　インサイダー脅威プログラム

管理番号	管理名 *管理拡張名*
PM-12	インサイダー脅威プログラム

ICS 補足ガイダンスなし

PL-3　情報セキュリティワークフォース

管理番号	管理名 *管理拡張名*
PM-13	情報セキュリティワークフォース

ICS 補足ガイダンス：情報セキュリティワークフォース開発改善プログラムのあらゆる面には、コンピュータ関係と物理両面での ICS コンポーネントに関する知識・技量レベルが含まれる。

PM-14　試験・訓練・監視

管理番号	管理名 *管理拡張名*
PM-14	試験・訓練・監視

ICS 補足ガイダンスなし

PM-15　セキュリティグループ・協会との連絡

管理番号	管理名 *管理拡張名*
PM-15	セキュリティグループ・協会との連絡

ICS 補足ガイダンスなし

PM-16　脅威意識プログラム

管理番号	管理名 *管理拡張名*
PM-16	脅威意識プログラム

ICS 補足ガイダンス：組織は、生じ得るインシデントに関して連携し情報を適時に共有すべきである。下記 DHS 国家サイバーセキュリティ通信統合センター(NCCIC)は集中所在地として機能し、サイバーセキュリティと通信の信頼性に関わる運用要素はそこで調整され、統合化されている。http://www.dhs.gov/about-national-cybersecurity-communications-integration-center 下記産業用制御システムサイバー緊急対応チーム(ICS-CERT)は、海外及び民間のコンピュータ緊急対応チーム(CERT)と連携して、制御システム関連セキュリティインシデント情報と緩和対策を共有している。http://ics-cert.us-cert.gov/ics-cert/
組織は、秘密情報と普通情報の共有化について検討すべきである。