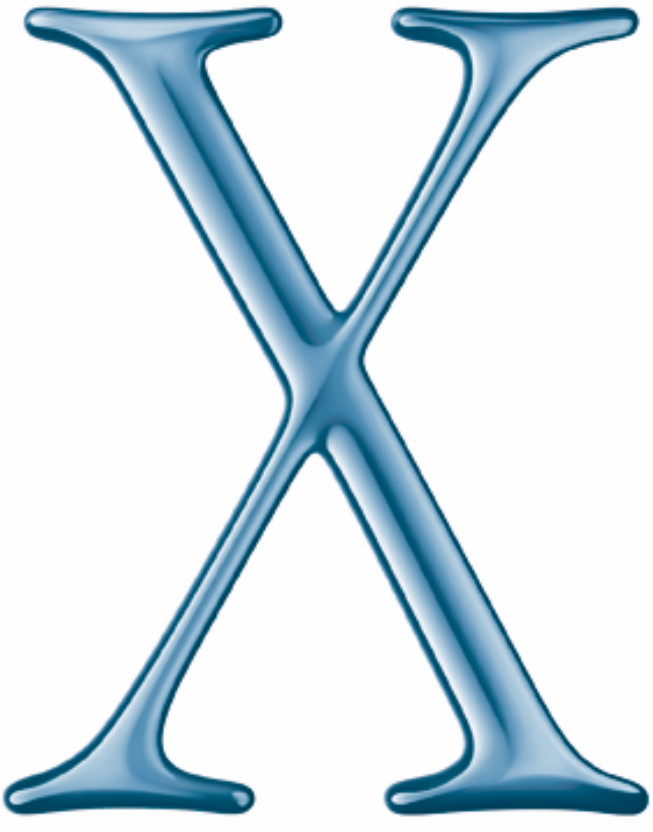


Mac OS X Server
管理者ガイド

Mac OS X Server ソフトウェアの機能と
ネットワークでの使いかたに関する情報が書かれています

J062-8441/7-26-01

目次

このマニュアルの使いかた

このマニュアルについて

初めてネットワークに挑戦する方も、経験豊富な管理者の方も、このマニュアルを読むことから始めてください。使用するサーバの目的に応じて、お読みになる章を選んでください。

- 19 ページの第 1 章「Mac OS X Server の管理」は、「Mac OS X Server」の使いかた、提供するサービス、管理方法、および最初の設定方法の概要を知りたい場合にお読みください。
- 第 2 章、第 3 章、および第 4 章では、「Mac OS X Server」の主要なコンポーネントであるディレクトリサービス、ユーザとグループ、および共有の 3 つについて説明します。ほとんどのサービスがこれら 3 つのコンポーネントの設定に依存しているので、これらの章を読むことをお勧めします。
- 第 5 章「ファイルサービス」では、「Mac OS X Server」に含まれるファイルサービスについて説明します。ファイルサービスには、Apple ファイルサービス、Windows サービス、NFS（Network File System）サービス、および FTP（File Transfer Protocol）サービスがあります。
- 第 6 章「プリントサービス」では、Macintosh、Windows、およびその他のコンピュータのユーザの間で PostScript™ 互換のプリンタを共有する方法について説明します。
- 第 7 章「Web サービス」では、「Mac OS X Server」の Web サービスについて説明します。Web サーバでセキュリティによって保護されたトランザクションを設定する方法、および複数の Web サイトを運用する方法が分かります。
- 第 8 章「メールサービス」では、インターネット上でのメールの使いかたや自分のネットワークに最適なプロトコルの選びかたなど、「Mac OS X Server」のメールサービスに関する情報を記載しています。
- 第 9 章「QuickTime Streaming Server」では、メディアをインターネット経由でリアルタイムに配信できるサービスについて説明します。
- 第 10 章「Macintosh マネージメントサービス」では、「Macintosh マネージャ」を使用してクライアントコンピュータをより効率的に管理する方法に関する情報が書かれています。

- 第 11 章「NetBoot」では、「NetBoot」について説明します。「NetBoot」によって、管理者は、サーバ上の起動ディスクイメージを更新するだけでクライアントコンピュータの設定と更新を即座に行うことができます。
- 第 12 章「ネットワークサービス」では、SLP（Service Location Protocol）DA（Directory Agent）サービス、DHCP（Dynamic Host Configuration Protocol）サービス、DNS（Domain Name System）サービス、IP フィルタサービスなど、「Mac OS X Server」のネットワークサービスに関する情報を記載しています。
- 付録 A「詳細なトピック」では、高度なサーバ管理について詳しく知りたい管理者を対象とした補足情報を記載しています。
- 付録 B「Mac OS X Server のインフォメーションワークシート」では、サーバに関する情報を記録するための用紙を記載しています。
- 用語集は、このマニュアルに記載されている頭字語とその定義の一覧です。

ユーザに提供する予定のあるサービスについて書かれた章をお読みください。サービスについての章では、それぞれのサービスの動作、機能、使いかた、および最初の設定方法の概要を説明しています。また、あまりなじみのないサービスに関する章もひととおりお読みください。これまで使ったことのないサービスの中に、自分のネットワークをより効率的に運用し、ユーザのために性能の向上を図ることのできるものが見つかるかもしれません。

いくつかの章の後半には、サービスの「内部」に関するセクションがあります。このセクションでは、経験豊富なユーザを対象とした、より詳しい技術情報を記載しています。このセクションは、ソフトウェアや特定のサービスの裏側で実行されているプロトコルに関する理解を深めたい場合にお読みください。

ほとんどの章の最後に「その他の情報」というセクションがあります。このセクションでは、サービスに関してより詳しい情報を見つけることができる Web サイトと参考資料を紹介しています。

Mac OS X Server を初めて設定する

「Mac OS X Server」のインストールと設定がまだ済んでいない場合は、今すぐ行ってください。サーバのインストールと設定の方法については、ソフトウェアに同梱の折り込みカード「Mac OS X Server をお使いになる前に」を参照してください。そのマニュアルの手順が完了したら、このマニュアルの第 1 章の手順説明に従って各サービスの最初の設定を行ってください。

日常行う管理作業についてヘルプを参照する

設定の変更、サービスの監視、サービスログの表示、またはその他の管理作業を行いたいときは、各サーバ管理プログラムで利用可能なオンラインヘルプで、ステップバイステップ形式の手順説明を検索することができます。

その他の情報

以下のマニュアルを、www.apple.co.jp/macosxserver/ で入手できます。

- 「Mac OS X Server 移行ガイド」では、「AppleShare IP」、「Macintosh マネージャ」、および「Mac OS X Server」バージョン 1.2 から「Mac OS X Server」にアップグレードする手順について説明しています。
- 「NetInfo　活用ガイド」では、「Mac OS X」に組み込まれたディレクトリシステムと、「Mac OS X」ネットワークを十分に活用するための NetInfo および「Mac OS X Server」の設定方法について説明しています。

1

Mac OS X Server の管理

この章では、「Mac OS X Server」を紹介し、その管理の概要を説明します。また、サーバの運用を開始する際に役立つ次の情報も示します。

- 35 ページの「サーバを初めて設定する」では、サーバをすばやく起動し、稼動させるための手順を説明します。
- 40 ページの「Mac OS X Server およびサーバ管理に関するその他の情報」では、サーバ管理を初めて行う方および経験豊富なサーバ管理者のそれぞれに適した、サーバおよびネットワーク管理情報の入手先を示します。

Mac OS X Server とは？

Mac OS X Server は、インターネットやローカルネットワーク上のユーザに対して、あらゆる範囲のサービスを提供する高度なサーバプラットフォームです。

- メールやファイル共有などのサービスを使って、ユーザを相互に接続できます。
- プリンタやコンピュータなどのシステムリソースを共有できます。
- Web サイトやストリーミングビデオなどのインターネットサービスのホストとして機能することができます。
- デスクトップのリソースや個人用ファイルなど、ネットワークユーザに表示される内容をカスタマイズできます。

この章では、「Mac OS X Server」に含まれるサービスを紹介し、それを管理するために使用するプログラムの概要を説明します。最初に、教育、出版、およびインターネットサービスの各環境で、サービスをどのような形で利用できるかについて説明します。次に、各サービスの機能について説明し、これらのサービスを管理するアプリケーションについて簡単に説明します。最後に、サーバを起動し、稼動させるための手順を説明します。

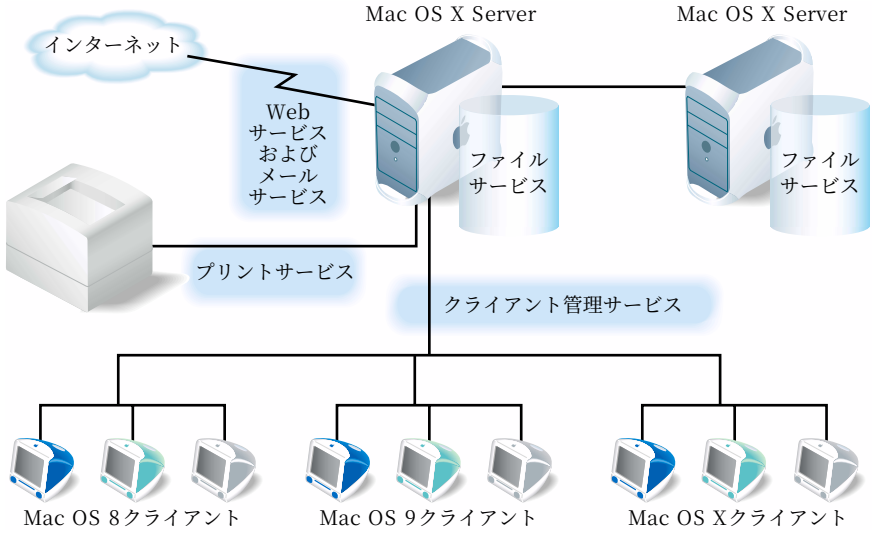
Mac OS X Server を使用する

サーバは、さまざまな環境における要望を満たすことができます。このセクションでは、一般的な次の 4 つの環境を例として取り上げます。

- 初等／中等教育環境
- 高等教育環境
- デザイン／出版ビジネス
- Web サービスプロバイダ

初等／中等教育環境

教育環境におけるサーバは、生徒がインターネットにアクセスしたり、メールを送信したり、ファイルを管理したり、ビデオを表示したり、書類をプリントしたりできるようにする必要があります。また、教師が授業計画やほかの講義の教材を始め、生徒の記録や集中管理されている情報にアクセスできるようにする必要があります。「Mac OS X Server」の Web サービス、メールサービス、プリントサービス、およびファイルサービスは、このような要望にすべて対応します。



初等／中等教育環境をサポートするサーバには、いくつかの特別な要件があります。

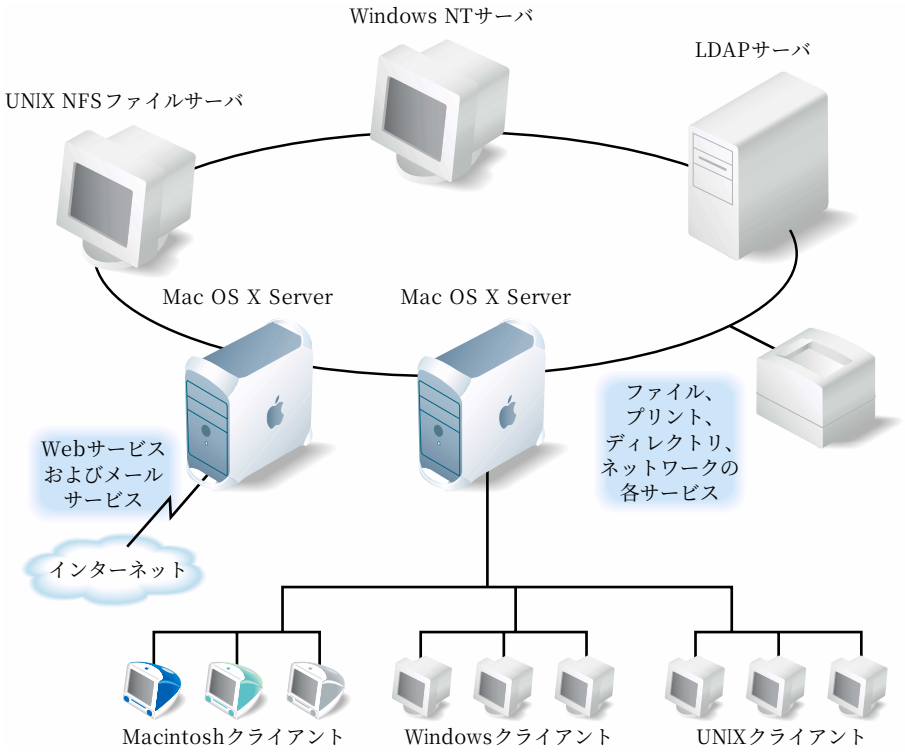
- 生徒のワークステーション環境を制御する手段を備えている必要があります。「Mac OS X Server」ソフトウェアには、クライアント管理サービスが含まれています。これによって、生徒が使用する Macintosh コンピュータを管理および監視することができます。

  たとえば、Macintosh マネージメントサービスを使えば、生徒がアクセスできるアプリケーションを管理することができます。また、アプリケーションの環境設定、デスクトップの外観、およびその他の個々のデスクトップ設定を定義することもできます。これによって、生徒は、ネットワーク上の異なるコンピュータで同じ環境を利用できます。

- 同じインターネットリソースに対して同時に行われる要求を効率的に処理する必要があります。「Mac OS X Server」は、キャッシュに対応する Web プロキシサービスを備えています。このため、すでにダウンロードされている Web コンテンツが再び要求された場合、これを再度取り込む必要はありません。

高等教育環境

専門学校や大学では、学生と、彼らが使用するワークステーションが多様であるために、サーバの要件はさらに複雑で、多岐にわたります。サーバの要件が複雑な場合は、すべての機能を備えたファイルサービスとネットワークサービスが必要です。

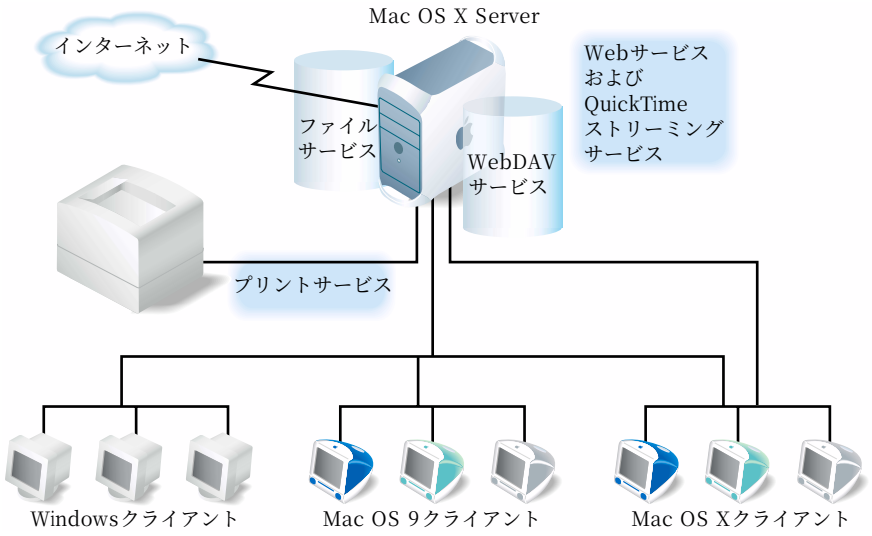


- さまざまな種類のクライアントコンピュータ（Macintosh、Windows、UNIX、Linux など）を使用する環境では、柔軟性に優れたファイルアクセスのサポートが必要です。「Mac OS X Server」の高度にスケーラブルな IP ベースのファイルサービスでは、ネットワーク上のどの場所からでも、AFP（Apple File Protocol）、NFS（Network File System）、FTP（File Transfer Protocol）、および SMB（Server Message Block）を使ってファイルにアクセスできるようサポートしています。

- サーバは、業界標準のTCPプリントプロトコルであるLPRや、Windows SMBプロトコルを使って送信されたプリントジョブに対して、PostScript 互換のプリントスプールおよびジョブアカウントを提供します。
- 高等教育ネットワークはさまざまな種類のコンピュータで構成され 、複雑であるため、ネットワークサービスはきわめて重要です。DNS （Domain Name System）サービスと SLP（Service Location Protocol）サービスは、クライアントのコンピュータやサービスがネットワーク上のリソースを検索するためのサービスで、「Mac OS X Server」が提供するサービスの中の2つの例に過ぎません。DHCP（Dynamic Host Configuration Protocol）によって、学生がポータブルコンピュータを使ってネットワークにログインすることができます。
- 「Mac OS X Server」ネットワークサービスの1つであるIPフィルタリングは、重要なデータを保護するセキュリティファイアウォールを実現します。
- ユーザ情報およびネットワークリソース情報は、NetInfo などのディレクトリシステムから取り込み、LDAP（Lightweight Directory Access Protocol）サーバなどの既存の基盤に統合できる必要があります。「Mac OS X Server」は、この情報にアクセスするように簡単に設定できます。

デザイン／出版ビジネス

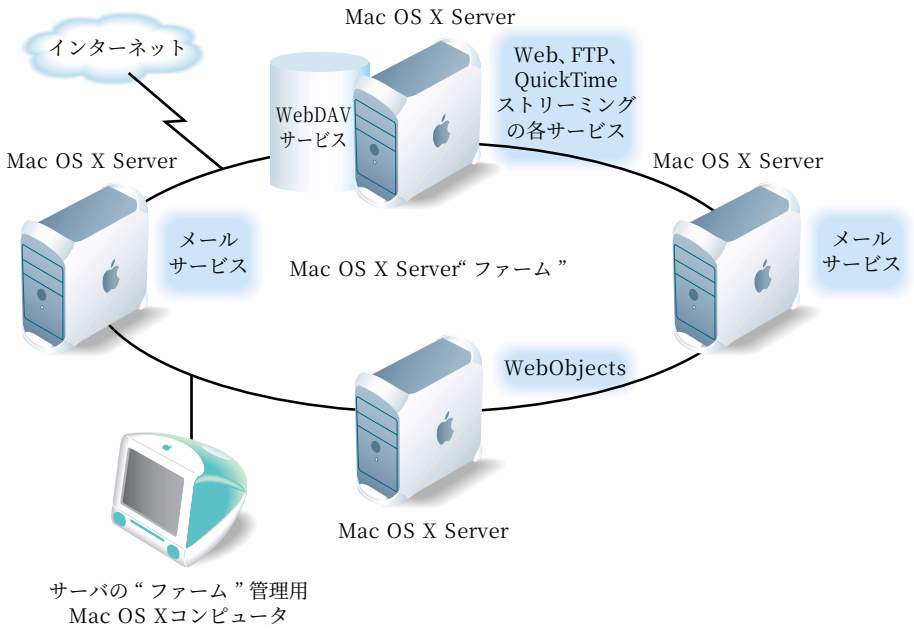
「Mac OS X Server」は、インターネットデザイナーおよびインターネットパブリッシャーのワークフローに関する要望を完全に満たすことができるサービスを備えています。



- 今や人気のある Apache Web サーバが、「Mac OS X Server」に組み込まれています。
- サーバの Web サービスに統合されている WebDAV（Web-based Distributed Authoring and Versioning）テクノロジーによって、「Mac OS X」がインストールされたコンピュータからドラッグ & ドロップでパブリッシングとファイル共有を行うことができます。
- ビデオの場合、QuickTime ストリーミングサービスによって、ストリーミングビデオをクライアントコンピュータにリアルタイムでブロードキャストできます。
- AFP（Apple Filing Protocol）によって、ワークグループのメンバー間でサイズの大きいファイルを転送できます。

Web サービスプロバイダ

「Mac OS X Server」は、電子商取引の Web サイトを運用したり、高い可用性と拡張性が要求される その他のインターネットサービスを提供するために必要なサポートを備えています。



- Web サービスの中心は、オープンソースの HTTP Web サーバである Apache です。1 台のサーバで、それぞれが独自のアドレスを持つ複数の Web サイトを運用できます（マルチリンクマルチホーミング）。1 枚の Ethernet カードで複数のアドレスをサポートするように、サーバを設定することができます（仮想ホスティング）。
- Web サービスでは、安全なインターネット接続を実現するために SSL（Secure Sockets Layer）保護をサポートします。
- サーバには、「WebObjects」ソフトウェアセットの配布コンポーネントが含まれています。このアプリケーションサービスによって、複数のデータベースに接続し、HTML と Java™ を動的に生成できる電子商取引用アプリケーションを配布できます。
- 「Mac OS X Server」には、Perl、JavaServlets、JavaServer Pages、および PHP のサポートも組み込まれています。
- 「QuickTime Streaming Server」によって、業界標準のストリーミングプロトコルを使用して、視聴者にリアルタイムでマルチメディアをブロードキャストできます。
- サービスまたは電源に異常が発生した場合、サーバは自動的に再起動します。これによって、サービスの可用性が最大化されます。

Mac OS X Server に含まれているサービス

このセクションでは、次の「Mac OS X Server」サービスについて説明します。

- ディレクトリサービス
- ファイルサービス
- プリントサービス
- Web サービス
- メールサービス
- QuickTime ストリーミングサービス
- クライアント管理サービス
- ネットワークサービス
- アプリケーションサービス

ディレクトリサービス

ディレクトリサービスは、認証と権限の付与に必要なユーザおよびグループ（ユーザの集まり）情報を探すために、サーバで使用されます。ディレクトリサービスによって、サーバに直接保存されている、またはサーバ間でユーザ情報を共有するために設定された場所に保存されているユーザ情報を検索するように、サーバを設定することができます。

通常、ユーザ情報は組み込みの NetInfo ディレクトリシステムを使って保存しますが、標準の Lightweight Directory Access Protocol（LDAP）サーバからこれを取り込むこともできます。ユーザ名を複数のディレクトリシステムに保存している状態でユーザを確認する必要が生じた場合、サーバは自動的に指定の場所を指定された順序で検索します。

ファイルサービス

ファイルサービスによって、クライアントユーザは、ネットワーク上のファイル、アプリケーション、およびその他のリソースにアクセスできます。「Mac OS X Server」は、次のファイルサービスを備えています。

- Apple ファイルサービス
- Windows サービス
- FTP サービス
- NFS サービス

Apple ファイルサービス

Apple ファイルサービスでは、AFP（Apple Filing Protocol）を使用して、Macintosh クライアントとリソースを共有できます。Macintosh ユーザは、サーバに接続し、自分のコンピュータ上にフォルダやファイルがあるかのように、これらにアクセスすることができます。「Mac OS X」のユーザは、「Finder」の「移動」メニューの「サーバへ接続」を使ってサーバにアクセスします。また、Mac OS X コンピュータの起動時にコンピュータにディレクトリを自動的にマウントさせることもできます。「Mac OS 8」と「Mac OS 9」のユーザは、「セレクタ」または「ネットワークブラウザ」を使用します。Apple ファイルサービスは、オペレーティングシステム環境と完全に統合しており、ファイルのエイリアスや「Sherlock」などの機能のサポートを提供します。

Windows サービス

Windows サービスによって、Windows コンピュータまたは Windows 互換コンピュータのユーザは、「Mac OS X Server」のリソースを利用することができます。新たなソフトウェアを必要とすることなく、Windows ユーザは、いつも使用している「ネットワークコンピュータ」ウインドウを使って、サーバを検索し、ファイルやプリントキューを参照することができます。

FTP サービス

FTP（File Transfer Protocol）によって、ユーザは、インターネット上でファイルを転送できます。FTP をサポートするコンピュータのユーザであれば、通常はインターネットブラウザや FTP クライアントアプリケーションを使って、サーバからファイルをダウンロードできます。また、FTP では、標準的な手段を使って、既知のユーザおよび匿名のユーザとサーバとの間でファイルを転送することもできます。

NFS サービス

NFS サービスによって、NFS クライアントソフトウェアを持つユーザに対して、ディレクトリ（フォルダ）を利用可能にすることができます。NFS は、UNIX クライアントのディレクトリをエクスポートするときにしばしば使用されます。

プリントサービス

プリントサービスによって、Macintosh、Windows、および UNIX コンピュータからプリントジョブを送信するユーザ間で、PostScript 互換のプリンタを共有できます。ユーザのコンピュータが、標準の LPR プロトコルまたは Windows SMB プロトコルを使ってプリントするように設定されている場合、サーバによる管理が設定されているプリンタに対して、プリントジョブを送信できます。

Web サービス

「Mac OS X Server」の Web サービスの中心は、最も広く使われているオープンソースの Web サーバである Apache です。すでに Apache をお使いの方は、Apache のログファイル分析ツール、設定ファイルの操作手順、および一般的なマニュアル類を継続してご利用いただけます。

「Mac OS X Server」の Web サービスでは、Web 環境をカスタマイズする機能も利用できます。Web サイトに任意の数のドメインを設定したり、SSL ベースの安全な通信をサイト単位で設定したり、CGI、WebObjects、Perl、PHP、Java Servlets などのアプリケーションサービスの組み込みサポートを利用したりすることができます。

Web サービスに含まれている WebDAV（Web-based Distributed Authoring and Versioning）によって、ユーザはサイトの稼働中に Web ページをチェックアウトし、変更を加え、チェックインして戻すことができます。WebDAV は、特に Web コンテンツの作成者を対象とするファイルサーバを提供します。

メールサービス

メールサービスによって、ネットワークやインターネットを経由するメールサービスをユーザに対して提供することができます。サービスにはジャンクメール防御の機能が組み込まれているばかりでなく、複数ドメインのメールをサポートします。標準のメールプロトコルは、すべてサポートされています。IMAP（Internet Message Access Protocol）、POP（Post Office Protocol）、および SMTP（Simple Mail Transfer Protocol）が、そのプロトコルです。

インターネットを経由するメールサービスを提供するには、ネットワーク上に Domain Name System（DNS）サービスを定義するか、インターネットサービスプロバイダ（ISP）から提供される DNS サービスを利用します。DNS は、「Mac OS X Server」ネットワークサービスの 1 つであり、SMTP によるメール処理に必要なシステムです。

QuickTime ストリーミングサービス

QuickTime Streaming Server（QTSS）によって、業界標準の RTSP/RTP プロトコルを使用して、リアルタイムでマルチメディアをストリーミングできます。

ライブメディアおよび記録済みのメディアを、インターネットを介して Macintosh ユーザと Windows ユーザの両方に配信できます。または、ストリーミングされたメディアを、別のストリーミングサーバに中継することができます。ユニキャストストリーミングまたはマルチキャストストリーミングが可能です。ユニキャストストリーミングでは、1つのストリームを各クライアントに個別に送信します。マルチキャストストリーミングでは、ストリームをクライアントのグループに送信します。

クライアント管理サービス

クライアント管理サービスによって、Macintosh クライアントユーザの使用環境を簡素化し、制御することができます。

Macintosh マネージメントサービス

Macintosh マネージメントサービスによって、アプリケーション、ホームディレクトリ、およびプリンタへのユーザアクセスを制御するためのネットワーク全体のポリシーを設定することができます。ユーザがログインしたときに表示される環境を定義することもできます。このサービスでは、「Mac OS 8.1」以降がインストールされているクライアントを管理することができます。

NetBoot

「NetBoot」によって、Macintosh クライアントコンピュータを、「Mac OS X Server」が提供する「Mac OS 9」オペレーティングシステムを使って起動することができます。

「NetBoot」を使用すると、起動イメージを単にアップデートすることによって、Mac OS 9 コンピュータを設定およびアップデートすることができます。サーバは、すべての Mac OS 9 コンピュータに「システムフォルダ」およびアプリケーションフォルダが含まれる起動イメージを提供します。サーバに加えるすべての変更は、クライアントコンピュータの再起動時に、自動的にクライアントコンピュータに反映されます。

ネットワークサービス

「Mac OS X Server」は次のネットワークサービスを備えており、TCP/IP ネットワーク上でのインターネット通信を管理することができます。

- SLP DA サービス
- DHCP サービス
- DNS サービス
- IP フィルタサービス

SLP DA サービス

SLP（Service Location Protocol）は、ネットワークで利用可能なサービスに枠組みを提供して、ユーザがサービスにアクセスしやすいようにします。

ファイルサーバや WebDAV サーバなど、URL を使ってアドレスを指定できるものはすべて、ネットワークサービスと見なすことができます。ネットワークにサービスを追加すると、SLP を使ってネットワーク上にそのサービスが登録されます。手動でサービスを設定する必要はありません。クライアントコンピュータがネットワークサービスを検索する必要がある場合は、SLP を使って目的の種類のサービスを検索します。クライアントコンピュータの要求に一致するすべての登録サービスが表示されるので、ユーザはこの中から使用するサービスを選ぶことができます。

SLP DA（Directory Agent）は基本となる SLP を拡張したもので、登録されているネットワークサービスに対して集中リポジトリを使用します。DA を設定することによって、1 つまたは複数のスコープ（サービスのグループ）のサービスを追跡することができます。クライアントコンピュータがネットワークサービスを検索する場合、クライアントコンピュータが接続しているスコープの DA が応答し、利用できるネットワークサービスのリストが表示されます。クライアントコンピュータはローカルのサービスを検索するだけなので、ネットワークを流れる通信の量が最低限に抑えられ、ユーザはよりすばやくネットワークサービスに接続できます。

DHCP サービス

DHCP（Dynamic Host Configuration Protocol）は、サーバからクライアントコンピュータの IP アドレスを管理し、動的に割り当てるためのプロトコルです。定義する IP アドレスのブロックから、サーバは未使用のアドレスを探し出し、必要に応じてこれをクライアントコンピュータに「リース」します。組織が所有する IP アドレスの個数よりもクライアント数の方が多い場合に、DHCP は特に効果的です。IP アドレスは必要に応じて割り当てられます。不要になると、ほかのクライアントがその IP アドレスを使用できるようになります。

DNS サービス

DNS（Domain Name System）によってユーザは、IP アドレス（192.168.11.12 など）ではなくドメイン名（server.apple.com など）を指定して、Web サーバやファイルサーバなどのネットワークリソースに接続できます。DNS は、IP アドレスをドメイン名にマップする分散型のデータベースです。

DNS サービスを提供するサーバでは、名前と、名前に関連付けられている IP アドレスのリストを保持しています。コンピュータは、名前に対応する IP アドレスを検索する必要がある場合、DNS サーバ（ネームサーバとも呼ばれています）にメッセージを送信します。ネームサーバでは IP アドレスを探し出し、これをコンピュータに送り返します。ネームサーバがローカルに IP アドレスを所有していない場合は、インターネット上の別のネームサーバにメッセージを送信します。この処理は、IP アドレスが見つかるまで続きます。

SMTP メールサービスを使用する場合、またはプライマリドメイン内にサブドメインを作成したい場合は、DNS を使用します。複数の Web サイトを運用している場合も、DNS を使用します。ISP が、使用しているネットワーク内で DNS を取り扱っていない場合は、「Mac OS X Server」がインストールされたサーバ上に DNS サーバを設定できます。

IP フィルタサービス

IP フィルタサービスによって、不正侵入者からサーバおよびサーバに保管されたコンテンツを保護できます。IP フィルタサービスは、ソフトウェアのファイアウォールとして使用でき、受信する IP パケットをスキャンし、定義されたフィルタに基づいてそのパケットを受け付けたり拒否したりすることができます。

特定の IP アドレスからのパケットを対象に、サーバ全体に制限を設定することができます。各サービス（Web、メール、FTP など）が使用するポートを対象にフィルタを定義することによって、各サービスへのアクセスを制限することもできます。

アプリケーションサービス

「WebObjects」は、電子商取引用アプリケーションやその他のインターネットアプリケーションを開発および配布する上で、柔軟性に優れたスケーラブルな手段を提供します。「WebObjects」アプリケーションは、複数のデータベースに接続し、HTML コンテンツを動的に生成することができます。

サーバは、「WebObjects」の配布システムと、「WebObjects」アプリケーションを配布できる無制限のライセンスを備えています。「WebObjects」アプリケーションを作成したい場合は、「WebObjects」開発ツールを購入することもできます。

本書では、これ以降、「WebObjects」について説明することはありません。「WebObjects」の情報およびマニュアルについては、以下の「WebObjects」Webサイトを参照してください。

www.apple.co.jp

サービスを管理する

このセクションでは、「Mac OS X Server」のサービスを設定および管理するときに使用する管理アプリケーションを紹介し、その使いかたについて簡単に説明します。

- 「Server Admin」: ほとんどのサービスを設定および管理する場合、サーバのユーザアカウントを設定および管理する場合、および共有ポイント（サーバ上でユーザに共有させたいフォルダやディスクなどの項目）を設定する場合に、「Server Admin」を使用します。

  「Server Admin」は、サーバ上と遠隔地のどちらからでも使用できます。お使いのサーバと Mac OS X コンピュータまたは別のサーバとの間では、暗号を用いた安全な通信が行われます。「Server Admin」には、各サービスを管理するための個別のモジュールが用意されています。詳しくは、31 ページの「Server Admin」を参照してください。

- 「Macintosh マネージャ」:「Mac OS 8.1」から「Mac OS 9.1」までのバージョンがインストールされたコンピュータを対象に、認証を設定し、ユーザ環境を定義するときは、「Macintosh マネージャ」を使用します。

  このアプリケーション（34 ページの「Macintosh マネージャ」を参照）は、「Mac OS 9」以降がインストールされたコンピュータで使用できます。

- 「Streaming Server Admin」: このブラウザベースのアプリケーションにより、Web ブラウザを使ってストリーミングサービスを設定し、管理することができます。

  このアプリケーション（34 ページの「Streaming Server Admin」を参照）は、「Netscape Navigator®」、「Netscape Communicator」、または「Microsoft Internet Explorer」のバージョン 4.5 以降がインストールされているコンピュータから使用できます。

- 「NetBoot Desktop Admin」:「NetBoot」クライアントが起動するときに使用するシステムイメージに対して項目をインストール、アップデート、または取り除くときは、「NetBoot Desktop Admin」を使用します。

  「NetBoot Desktop Admin」は、「Mac OS 9」がインストールされているクライアントコンピュータから使用できます。このアプリケーションについて詳しくは、35 ページの「NetBoot Desktop Admin」を参照してください。

Server Admin

「Server Admin」は、1 つまたは複数の「Mac OS X Server」のサービスを管理する目的で、ローカルに（サーバ上で）使用することも、遠隔地で（「Mac OS X」が稼動するコンピュータまたは別の「Mac OS X Server」から）使用することもできます。

「Mac OS X Server」をインストールすると、自動的に「Server Admin」がサーバにインストールされます。「Server Admin」のリモートコンポーネントを Mac OS X コンピュータにインストールするときは、次のように操作します。

1. ネットワークが設定されている Mac OS X コンピュータの CD-ROM ドライブに、「Mac OS X Server」の CD をセットします。
2. 「Admin Install」フォルダを開き、インストーラパッケージの「Admin_Install.mpkg」をダブルクリックします。
3. 「カスタムインストール」オプションを選び、「Server Admin」を選びます。

   「Server Admin」が「/Applications/Utilities/」にインストールされます。

Server Admin にログインする

「Server Admin」にログインするときは、次のように操作します。

1. 「Dock」内の「Server Admin」アイコンをクリックして、「Server Admin」（/Applications/Utilities にあります）を開きます。

2. 管理したい「Mac OS X Server」の IP アドレスまたはドメイン名を入力します。デフォルトでは、ローカルサーバの IP アドレスがログインウインドウに表示されます。別のサーバを管理するときは、そのサーバのアドレスまたはドメイン名を入力します。次に、サーバの管理者のユーザ名とパスワードを入力します。
3. 「接続」をクリックします。

   各サーバにログインし、各自のツールバーから管理することによって、複数のサーバを同時に管理することができます。

ツールバーを使用する

「Server Admin」を開き、サーバにログインすると、そのサーバのツールバーが表示されます。ツールバーの 4 つのタブに配置されたサービスモジュールを使って、各サービスを管理することができます。

サービスモジュールを使用する目的と、本書内で各モジュールについて詳しい情報が記載されている箇所を、以下にまとめて示します。

目的	使用するモジュール	詳しい情報の参照先
サーバに関する情報を表示する	「サーバ情報」モジュール（「一般」タブ）	34 ページ
サーバのログを表示する	「ログビューア」（「一般」タブ）	33 ページ
ディレクトリサービスを設定および管理する	「ディレクトリサービス」の「Mac OS X」ユーティリティ	41 ページ
ユーザを設定および管理する	「ユーザとグループ」モジュール（「一般」タブ） 「共有」モジュール（「一般」タブ）	57 ページ 73 ページ
Macintosh マネージメントサービスを操作する	「Macintosh Mgr」モジュール（「一般」タブ）	195 ページ
ファイルサービスを設定および管理する	「ファイルとプリント」タブの各モジュール	
■ Apple ファイルサービス	■ 「Apple」	85 ページ
■ Windows サービス	■ 「Windows」	93 ページ
■ FTP サービス	■ 「FTP」	104 ページ
■ NFS サービス	■ 「NFS」	100 ページ
プリントサービスを設定および管理する	「プリント」モジュール（「ファイルとプリント」タブ）	111 ページ
Web サービスを設定および管理する	「Web サービス」モジュール（「インターネット」タブ）	121 ページ

目的	使用するモジュール	詳しい情報の参照先
メールサービスを設定および管理する	「メールサービス」モジュール（「インターネット」タブ）	153 ページ
ネットワークサービスを設定および管理する	「ネットワーク」タブの各モジュール	
■ SLP DA サービス	■ 「SLP サービス」	264 ページ
■ DHCP サービス	■ 「DHCP/NetBoot」	271 ページ
■ DNS サービス	■ 「DNS」	280 ページ
■ IP フィルタサービス	■ 「IP フィルタ」	285 ページ

「Server Admin」モジュールをクリックすると、コマンドのメニューが表示されます。コマンドを使ってサービスを管理する方法については、上の表に示されているページ、またはモジュールに関するオンスクリーンヘルプを参照してください。「Server Admin」の一般的な使いかたについては、「Server Admin」メニューバーの「ヘルプ」メニューを参照してください。

ツールバーの下部にあるステータスバーには、稼働中のサービスの個数と、注意を要する状態を知らせる警告が表示されます。地球のマークは、動作中のサービスを示します。三角形で囲まれた「!」マークは、警告を示します。これらのマークは、個々のモジュールのアイコン上、および警告の状態にあるモジュールが含まれるタブ上にも表示されます。

ログを表示する

「ログビューア」を使用すると、サーバ上で稼動している各種のサービスとアプリケーションによってログに記録される、エラーやその他の注目すべきイベントを監視することができます。「ログビューア」のウインドウは、新しいログが記録されるたびに動的にアップデートされるので、複数のサービスをリアルタイムで監視できます。

「ログビューア」をクリックし、そのログを表示したいサービスを選びます。たとえば、プリントサービスのログやサーバの各プリントキューのログを表示するときは、「プリントサービス」を選びます。目的のサービスが表示されない場合は、サービスが稼動していることを確認し、システムログをチェックしてください（「ログビューア」メニューから「System Software」を選び、次に「表示」ポップアップメニューから「System Log」を選びます）。

本書の後ろの章とオンスクリーンヘルプには、特定のサービスのログに関する説明があります。「ログビューア」の使いかたと、各種のサービスで管理されるログの設定および表示についても、ヘルプを参照してください。

サーバに関する情報を表示する

「サーバ情報」をクリックし、「サーバ情報を表示」を選ぶと、サーバのシリアル番号とネットワークの特性が表示されます。

サーバのシリアル番号を変更する必要がある場合は、「サーバ情報」をクリックし、「製品のシリアル番号を変更」を選びます。

Macintosh マネージャ

「Macintosh マネージャ」アプリケーションは、Macintosh マネージメントサービスを管理し、ネットワーク上のクライアントコンピュータのユーザ環境を設定するために使用します。「Macintosh マネージャ」は、ローカル（サーバ上）で、または遠隔地（「Mac OS X Server」と同じネットワーク上にある Mac OS 9 コンピュータまたは Mac OS X コンピュータ）から使用できます。

「Macintosh マネージャ」に加えて、2 つの「Server Admin」モジュールを使って Macintosh マネージメントサービスを管理することもできます。「ユーザとグループ」と「共有」です。これらすべてのアプリケーションについて詳しくは、195 ページを参照してください。

Macintosh マネージャにログインする

「Dock」内のアイコンをクリックして、「Macintosh マネージャ」を開きます。サーバ管理者のユーザ名とパスワードを使ってログインします。サーバ管理者としてログインすると、「Macintosh マネージャ」のグローバル管理者のアクセス権が自動的に許可されます。ログイン後は、ユーザの追加、ワークグループの作成、およびネットワーク上のコンピュータの管理が可能です。

「Macintosh マネージャ」を開くには、「Server Admin」の「一般」タブで「Macintosh Mgr」をクリックし、「Macintosh マネージャを開く」を選ぶこともできます。

Macintosh マネージメントサービスを開始する／停止する

Macintosh マネージメントサービスを開始したり停止したりするときは、「Server Admin」の「Macintosh Mgr」モジュールを使用します。「Macintosh Mgr」モジュールを使って、サーバの起動時に Macintosh マネージメントサービスを自動的に開始するかどうかを指定することもできます。

Streaming Server Admin

「Streaming Server Admin」は、Web ブラウザが稼動しているコンピュータから使用できます。「Streaming Server Admin」を開くときは、ブラウザを開き、サーバ上の「Streaming Server Admin」の URL を入力します。次に、ストリーミングサーバの管理者のログイン ID とパスワードを入力します。確立される接続は、安全性の高いものです。

「Streaming Server Admin」について詳しくは、173 ページの第 9 章「QuickTime Streaming Server」を参照してください。

NetBoot Desktop Admin

Mac OS 9 コンピュータ上で、「セレクタ」を使って「NetBoot」サーバボリュームを探し、サーバ管理者としてサーバにログインします。これによって、「NetBoot Desktop Admin」を開き、起動イメージに対して変更を加えることができます。「NetBoot Desktop Admin」を使用するときは、画面上の指示に従ってください。

「NetBoot」の管理については、245 ページを参照してください。

サーバを初めて設定する

サーバをすばやく起動し、稼動させるときは、次のように操作します。手順 8 まで完了すると、ユーザがサーバにアクセスし、Apple ファイルサービスの基本的な機能を利用できるようになります。手順 9 には、ユーザに提供したいその他のサービスを設定するための手順を参照できる、このガイド内の場所を示します。

手順 1：サーバおよびサーバ管理アプリケーションの概要を知る

この章の前半部分をまだお読みになっていない場合は、お読みください。前半のセクションでは、ビジネス環境および教育環境における「Mac OS X Server」の一般的な使用例が説明されています。また、ユーザに提供できるサービスの紹介、およびサーバの管理に使用するアプリケーションの概要も示されています。

これらのセクションは、残りの手順を進める際に出てくる、用語および概念を理解するために役立ちます。

手順 2：サーバをインストールする

「Mac OS X Server をお使いになる前に」のワークシートおよび手順を使用して、サーバをインストールし、ネットワーク上で使用できる状態に設定します。

手順 3：ログインする

手順 2 で指定したオーナー／管理者の名前とパスワードを使用して、サーバにログインします。次に、以下の手順で「Server Admin」アプリケーションにログインします。

1. 「Dock」または「Applications/Utilities」から、「Server Admin」を開きます。
2. 「アドレス」欄に、手順2でサーバに割り当てたIPアドレスまたはドメイン名を入力します。
3. 「ユーザ名」欄に、オーナー／管理者の名前を入力します。「パスワード」欄に、オーナー／管理者のパスワードを入力します。
4. 「接続」をクリックします。

手順 4：共有ポイントを作成する

共有ポイントとは、ユーザが共有するファイルが保管されたハードディスク（またはハードディスクのパーティション）、CD-ROM ディスク、またはフォルダのことです。たとえば、サーバ管理者が教師である場合、数学、英語、生物学などの各クラスについて共有ポイントを設定すれば、クラスごとに生徒全員が同じ課題や資料にアクセスできるようになります。

共有ポイントを作成するときは、次のように操作します。

1. 「Finder」ウインドウで、共有ポイントを置きたいフォルダを開きます。「ファイル」メニューから「新規フォルダ」を選びます。共有ポイントの名前を入力します。

2 「Server Admin」で、「ファイルとプリント」タブをクリックし、Apple ファイルサービスが稼動していることを確認します。稼動していない場合は、「Apple」をクリックし、「Apple ファイルサービスを開始」を選びます。

3 「一般」タブをクリックします。次に、「共有」をクリックし、「アクセス権を設定」を選びます。先ほど作成したフォルダを選び、「選択」をクリックします。

4 「この項目とその内容を共有する」をクリックし、「保存」をクリックします。

5 作成したい共有ポイントごとに、手順 1 ～ 4 を繰り返します。

手順 5：ホームディレクトリのデフォルト設定を定義する

ホームディレクトリとは、ユーザの個人ファイルを保管するフォルダのことです。たとえば、生徒が、それぞれ自分のホームディレクトリに、授業のノートや作業中の課題を保管することができます。

ホームディレクトリのデフォルト設定を定義しておくと、サーバに新しいユーザを定義したときに、そのユーザにホームディレクトリが自動的に作成されます。ホームディレクトリのデフォルト設定を定義するときは、次のように操作します。

1 「Server Admin」の「一般」タブで、「U&G」をクリックし、「デフォルトのホームディレクトリ」を選びます。

2 「ローカル」を選んで、単純なデフォルト設定を定義します。デフォルト設定は、後で必要に応じて変更できます。

3 「共有ポイント」ポップアップリストから、ホームディレクトリを置きたい共有ポイントを選びます。あらかじめ定義されている「Users」共有ポイントを選ぶか、自分で作成した共有ポイントのいずれかを選ぶことができます。

4 「保存」をクリックします。

新しいユーザを定義すると常に、選択した共有ポイントにそのユーザの「ユーザ名」でユーザのホームディレクトリが作成されます。ユーザは、ホームディレクトリを所有することになります。つまり、ユーザは、自分のホームディレクトリに対する読み出し／書き込みのアクセス権を持ち、ホームディレクトリ内のファイルに対するアクセスを完全に制御できるということです。

手順 6：ユーザを定義する

サーバを使用できるようにするユーザを定義するときは、次のように操作します。

1 「Server Admin」の「一般」タブで、「U&G」をクリックし、「新規ユーザ」を選びます。

2 「名前」フィールドに、ユーザを識別するための名前（たとえば「Bob W. Brown, Jr」など）を入力します

3 「ユーザ名」フィールドに、ユーザのユーザ名を入力します。ユーザは、手順 2 で指定した名前でサーバにログインできますが、ユーザ名のほうが便利です。ユーザのホームディレクトリ名には、ユーザ名が使われます。また、サーバにメールサービスを設定する場合は、ユーザのメールアドレスにもユーザ名が使われます。

通常、ユーザ名は 8 文字（半角英数文字）以下で指定します。使用できるのは、英数字、ハイフン（-）、およびアンダースコア（_）のみです。

4 「パスワード」フィールドに、ユーザがサーバにログインするために使用するパスワードを入力します。最初はサーバ管理者がパスワードを定義しますが、ユーザは、サーバへのログイン時に、または「システム環境設定」の「パスワード」パネルを使って、パスワードを変更することができます。権限がないユーザが簡単に推測できないようなパスワードを入力します。

パスワードは大文字と小文字が区別されます。入力時に画面に表示されることはありません。パスワードを入力する前に caps lock キーを押していないことを確認してください。空白文字と、option キーを使った文字の組み合わせは使用しないでください。

5 ユーザがサーバを管理できるようにしたい場合は、「ユーザがサーバを管理できるようにする」を選びます。サーバを初めて設定した場合、これを管理できるのは設定時に指定されたオーナーおよび管理者だけです。サーバ管理者は、すべてのサーバ管理アプリケーションを使用でき、サーバのすべての機能にアクセスできます。

6 ユーザがサーバにログインできるようにするために、「ユーザにログインを許可する」を選びます。次に、「保存」をクリックします。

7 サーバにアクセスできるようにしたいユーザごとに、手順 1 ～ 6 を繰り返します。

手順 7：グループを定義する

グループとは、類似した要求を持つユーザの集まりのことです。たとえば、数学クラスの生徒を数学クラスグループにまとめ、数学グループの共有ポイント内にあるファイルに対するグループアクセス権を与えることができます。

グループを使用すると、共有リソースの管理を簡略化できます。特定のリソースを必要とするユーザに個別にアクセス権を与える代わりに、それらのユーザを 1 つのグループにまとめて、そのグループにアクセス権を与えることができます。

グループを定義するときは、次のように操作します。

1 「Server Admin」の「一般」タブで、「U&G」をクリックし、「新規グループ」を選びます。

2 グループの名前を入力します。このグループにメールを送信できるようにしたい場合は、空白文字や option キーを使った文字を使用しないでください。

3 グループにユーザを追加するときは、「U&G リストを開く」をクリックします。追加したいユーザを探し、グループの設定ウインドウにドラッグします。

4 「保存」をクリックします。

手順 8：共有ポイントへのアクセス権を割り当てる

定義したユーザおよびグループに、共有ポイントへのアクセス権を割り当てるときは、次のように操作します。

1 「Server Admin」の「一般」タブで、「共有」をクリックし、「ディスクと共有ポイントを表示」を選びます。

2 共有ポイントをダブルクリックします。

3 「一般」タブで、「U&G」をクリックし、「U&G リストを開く」を選びます。

4 共有ポイントのオーナーを変更するときは、「ユーザとグループのリスト」ウインドウから「共有」ウインドウの「オーナー」フィールドにユーザをドラッグします。「オーナー」フィールドの右のポップアップメニューを使用して、オーナーのアクセス権を設定します。

5 グループにアクセス権を割り当てるときは、「ユーザとグループのリスト」ウインドウから「共有」ウインドウの「グループ」フィールドにグループをドラッグします。次に、「グループ」フィールドの右のポップアップメニューを使用して、グループのアクセス権を設定します。たとえば、グループが数学クラスグループである場合、数学クラスの生徒が共有ポイント内の情報を読み出すことはできても変更できないようにするときは、「読み出し専用」のアクセス権を与えます。

6 サーバにログインできるすべてのユーザにアクセス権を割り当てるときは、「全員」の右のポップアップメニューを使用します。

手順 9：必要に応じて、追加するサービスを設定する

追加したいサービスを決め、次の表に示す章を参照します。最初に目的の章を読み、内容を理解します。次に、サービスを設定する前に行う作業、およびそのサービスを初めて設定するときの手順に関する指示に従います。これらの情報に従うことによって、各サービスを設定できます。詳しい手順については、オンスクリーンヘルプも参照できます。

目的	設定する項目	参照先
共有ポイント内のフォルダやファイルにアクセス権を割り当てる	フォルダとファイル、およびアクセス権	第 4 章、73 ページの「共有」
Apple ファイルサービスの機能を追加する	Apple ファイルサービス	第 5 章、85 ページの「ファイルサービス」
Windows ユーザにファイルサービスおよびプリントサービスを提供する	Windows サービス	第 5 章、93 ページの「ファイルサービス」
ユーザが NFS クライアントソフトウェアからフォルダを利用できるようにする	NFS サービス	第 5 章、100 ページの「ファイルサービス」
ユーザが FTP を使ってサーバからファイルを転送できるようにする	FTP サービス	第 5 章、104 ページの「ファイルサービス」
ユーザ間でプリンタを共有する	プリントサービス	第 6 章、111 ページの「プリントサービス」

目的	設定する項目	参照先
サーバに Web サイトまたは WebDAV サポートを設定する	Web サービス	第 7 章、121 ページの「Web サービス」
ユーザにメールサービスを提供する	メールサービス	第 8 章、153 ページの「メールサービス」
サーバからリアルタイムでマルチメディアをブロードキャストする	QuickTime ストリーミングサービス	第 9 章、173 ページの「QuickTime Streaming Server」
「Mac OS 8.1」以降のユーザ環境を管理する	Macintosh マネージメントサービス	第 10 章、195 ページの「Macintosh マネージメントサービス」
すべての Mac OS 9 クライアントコンピュータに同一の「システムフォルダ」およびアプリケーションフォルダを提供する	NetBoot	第 11 章、245 ページの「NetBoot」
URL でアクセス可能なネットワーク装置の登録を自動化する	SLP DA サービス	第 12 章、263 ページの「ネットワークサービス」
クライアントコンピュータに IP アドレスを動的に割り当てる	DHCP サービス	第 12 章、271 ページの「ネットワークサービス」
ドメインネームサーバを設定する	DNS サービス	第 12 章、280 ページの「ネットワークサービス」
サーバが受信する IP パケットをフィルタリングする	IP フィルタサービス	第 12 章、285 ページの「ネットワークサービス」
複数の「Mac OS X Server」や Mac OS X コンピュータ間でユーザ情報を共有する	ディレクトリサービス	第 2 章、41 ページの「ディレクトリサービス」

Mac OS X Server およびサーバ管理に関するその他の情報

サーバとネットワークの管理を始めたばかりの方の場合

「Mac OS X Server」について詳しくは、次に示す「Mac OS X Server」の Web サイトを参照してください。

www.apple.co.jp/macosxserver

オンラインディスカッショングループに参加すると、同じ立場の人と知り合うことができます。発生した問題の多くは、ほかのサーバ管理者によってすでに解決されている可能性があります。アップル社が提供しているリストを探すときは、次の Web サイトを参照してください。

www.lists.apple.com

次の参考書籍を入手することを検討してください。これらには、背景にある情報、基本概念の説明、およびネットワークを最大限に活用するためのアイディアが記載されています。

- 「Teach Yourself Networking Visually」Paul Whitehead ／ Ruth Maran 著（IDG Books Worldwide 社発行、1998 年）。
- 「Internet and Intranet Engineering」Daniel Minoli 著（McGraw-Hill 社発行、1997 年）。

さらに、NetworkMagazine.com では、次の Web サイトで多くのオンラインチュートリアルを提供しています。

www.networkmagazine.com

経験豊富なサーバ管理者の場合

すでにネットワーク管理に関する知識があり、「Mac OS X Server」、「Linux」、「UNIX」、または同等のオペレーティングシステムを使用した経験がある場合は、次の参考書籍が役に立つでしょう。

- 「Mac OS X Server」に関連したトピックを説明している O'Reilly & Associates 社発行の各種の書籍。「Internet Core Protocols: The Definitive Reference, DNS and BIND」や「TCP/IP Network Administration」などがその例です。より詳しい情報については、「Apache: The Definitive Guide」、「Writing Apache Modules with Perl and C」、「Web Performance Tuning」、および「Web Security & Commerce」を参照してください。これらも、O'Reilly and Associates 社の発行です。次の O'Reilly & Associates 社の Web サイトを参照してください。

  www.oreilly.co.jp

- Apache について詳しくは、Apache の Web サイトを参照してください。

  www.apache.or.jp

「Mac OS X Server」に用意されている管理ツールを使用することはできますが、「Terminal」アプリケーションに組み込まれているコマンドラインインタフェースから、大部分の UNIX コマンドおよびシェルスクリプトを実行できます。コマンドラインインタフェースにアクセスするためには、管理者としてサーバにログインし、「/Applications/Utilities/」内の「Terminal」アプリケーションに移動します。さまざまな推奨事項については、301 ページの付録 A「詳細なトピック」を参照してください。

2

ディレクトリサービス

ディレクトリサービスとは？

「Mac OS X Server」は、ディレクトリサービスを使用してユーザに関する情報を検索します。サーバは、認証用とさまざまなサービスをサポートするために、ユーザ情報を必要とします。

認証で必要なユーザ情報

ユーザが「Mac OS X Server」にログインすると、サーバは、そのユーザを認証します。つまり、有効なユーザであるかどうかを判断します。有効なユーザだけがサーバにアクセスしたり、サーバのサービスを利用したりすることができます。

ユーザを認証する際、サーバはユーザに関する次の情報を調査します。

- ユーザ名
- パスワード
- ユーザ ID

ユーザが使用するサービスが何であるかにかかわらず、少なくともサーバへのアクセスを許可する各ユーザのユーザ名、パスワード、およびユーザ ID が、サーバがアクセス可能な場所に保管されていなければなりません。ユーザが認証されるためには、ユーザがログインするときに入力するユーザ名とパスワードが、サーバで定義されているいずれかのユーザのものと一致する必要があります。

サーバが必要とするその他のユーザ情報

個別のサービスでは、その他のユーザ情報が必要です。たとえば、メールサービスでは各ユーザのメールの設定、Macintosh マネージメントサービスではユーザのホームディレクトリに関する情報が必要です。ほとんどのサービスで、ユーザ ID が必要です。

ユーザが認証された後で、各サービスがアクセスする必要のあるデータについては、301 ページの付録 A「詳細なトピック」を参照してください。

ユーザ情報を定義する場所

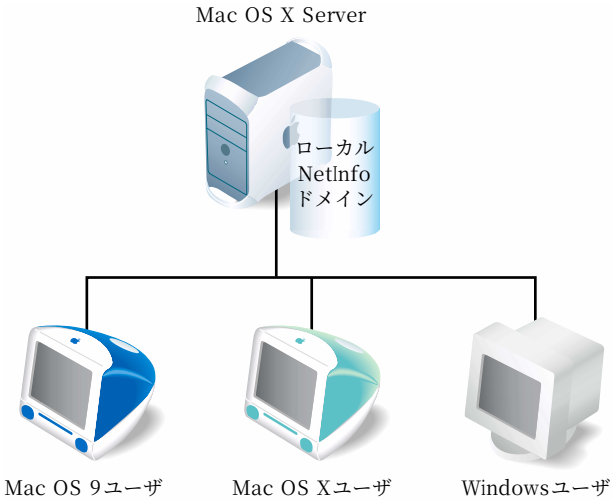
NetInfo データベースでは、ディレクトリサービスが必要とするユーザ情報は「Mac OS X Server」に保管されます。NetInfo データベースは、ドメインと呼ばれます。

「Mac OS X Server」は、LDAP（Lightweight Directory Access Protocol）サーバと呼ばれる標準のサーバから情報を取り込むこともできます。LDAP サーバは、多くの場合、ユーザ情報の要求を処理するために使用されます。

サーバのユーザ情報を保管する場所は、それを共有する必要があるかどうかによって決まります。

サーバ上のユーザ情報を共有しない場合

サーバが、ネットワーク上の別の「Mac OS X Server」からその情報を取得されることのないユーザに対応している場合、ユーザ情報を、ローカルに、つまりそのサーバ自体に置く必要があります。この場合、ユーザ情報は、サーバの NetInfo ドメイン（ローカルドメインと呼ばれます）に保管されます。

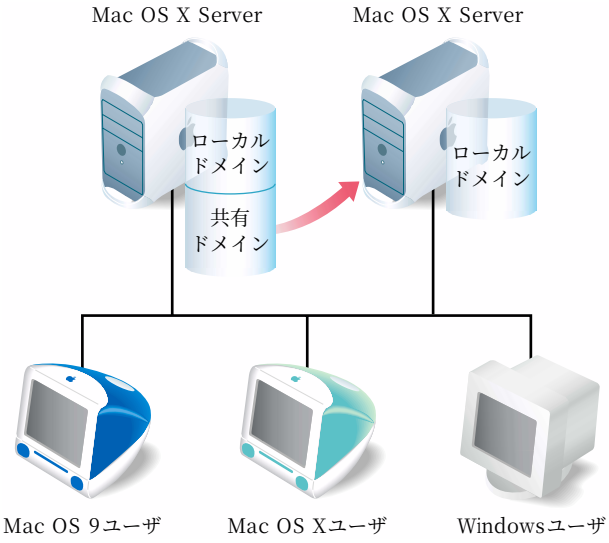


ユーザがサーバにログインすると、ディレクトリサービスは、ローカルドメインでそのユーザを検索します。ユーザがサーバにログインできるのは、そのユーザがローカルドメインで定義されている場合だけです。

すべての「Mac OS X Server」にはローカルドメインがあります。ローカルドメインで定義されているユーザを見ることができるのは、そのドメインが置かれているコンピュータだけです。スタンドアロンサーバや、シンプルなネットワークのサーバの場合は、ローカルドメインでのユーザの定義が適しています。しかし、多くの場合は、複数のコンピュータでユーザ情報を共有するほうが効率的です。ユーザデータを共有することによって、データの冗長性を最小限に抑えられます。ユーザのデータが変更された場合に、変更しなければならない箇所が少なくて済みます。

サーバ上のユーザ情報を共有できる場合

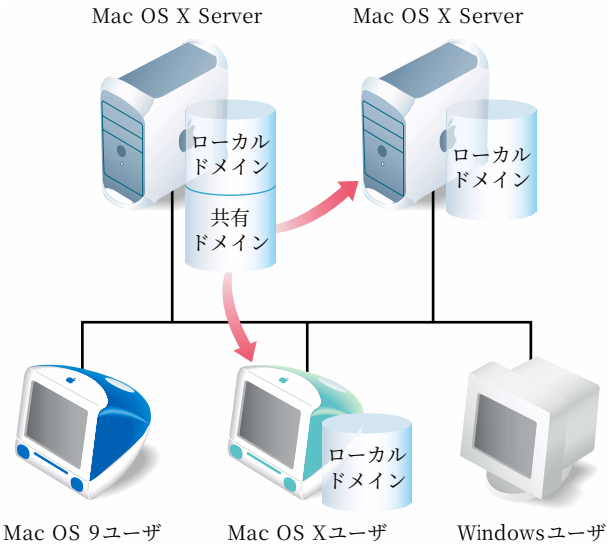
ネットワーク上の複数の「Mac OS X Server」がユーザにサービスを提供している場合は、いずれかのサーバのNetInfoドメインに保管されているユーザ情報をサーバ間で共有することができます。



NetInfo情報を複数の「Mac OS X Server」に公開するときは、共有ドメインを定義します。

上の図では、共有ドメインに定義されたユーザは 2 つのサーバにアクセスできます。ユーザがいずれかのサーバにログインすると、ディレクトリサービスは、そのサーバのローカルドメインでユーザを検索します。ユーザが見つからなければ、ディレクトリサービスは共有ドメインでユーザを検索します。

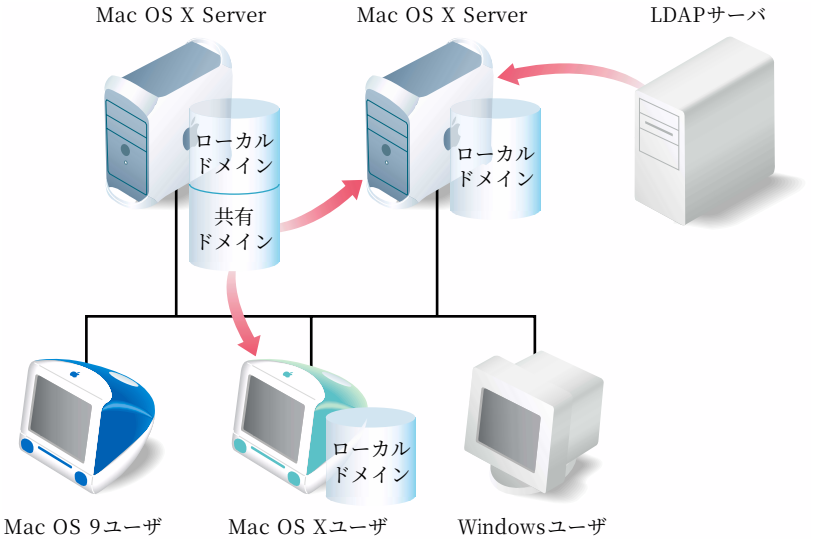
共有ドメインは、「Mac OS X」が稼動するコンピュータの使用権限を管理するときにも使用できます：



「Mac OS X Server」と同様、「Mac OS X」の稼動するコンピュータは常にローカル NetInfo ドメインを保持します。上の図では、「Mac OS X」のローカルドメインまたはサーバの共有ドメインで定義されているユーザが、Mac OS X コンピュータを使用できます。

サーバの外部にある情報を共有できる場合

大学や世界的規模の企業などの組織では、LDAP サーバを使ってユーザ情報を管理します。「Mac OS X Server」は、これらの標準のシステムからユーザ情報を取り込むように設定することができます。

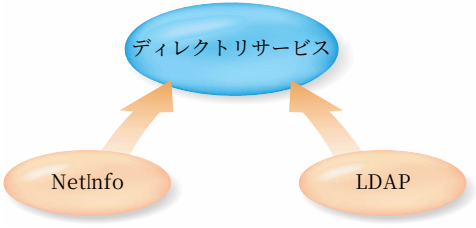


ユーザがいずれかの「Mac OS X Server」にログインすると、ディレクトリサービスは、NetInfo ドメインで、ローカルドメインから順にユーザを検索します。しかし、ユーザが見つからない場合、サーバが LDAP サーバを使うように設定されていると、サーバは、LDAP サーバを参照してユーザに関する情報を検索します。

サーバがユーザ情報を見つける方法

ディレクトリサービスは「Mac OS X Server」の基本的な構造の一部であり、集中管理されたロードマップを提供します。このロードマップは、サーバが、ユーザ、グループ（ユーザの集まり）、装置など、サーバが対応しているすべてのユーザおよびリソースに関する情報を探すために使用します。

サーバがユーザ情報を必要とする場合は、ディレクトリサービスがその検索場所を識別します。



また、サーバが、複数のサーバの NetInfo ドメインや、1 つ以上の LDAP サーバなど、複数の場所に保存されているユーザ情報にアクセスする必要がある場合は、ディレクトリサービスが、その検索する順序も制御します。

検索する場所と順序は、サーバの検索ポリシーと呼ばれます。ユーザがログインすると、ディレクトリサービスはローカル NetInfo ドメインでユーザを検索し、次に、設定されている検索ポリシーに従って、共有ドメインや LDAP サーバを検索します。

NetInfo を使用する

NetInfo によって、「Mac OS X Server」上のユーザ情報を保管および管理できます。

サーバには、常に少なくとも 1 つの NetInfo ドメイン（つまり、ローカルドメイン）が定義されています。ローカルドメインに保管されている情報を見ることができるのは、それが置かれているサーバだけです。この情報をほかのサーバと共有することはできません。このため、ローカルドメインで定義されているユーザがアクセスできるのは、そのローカルドメインが置かれているサーバだけです。

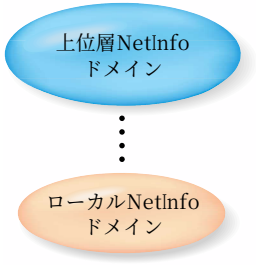
NetInfo ドメインの情報を共有したい場合は、ローカルドメインを、上位層ドメインと呼ばれる共有ドメインの下位層に設定する必要があります。

NetInfo を設定する前に

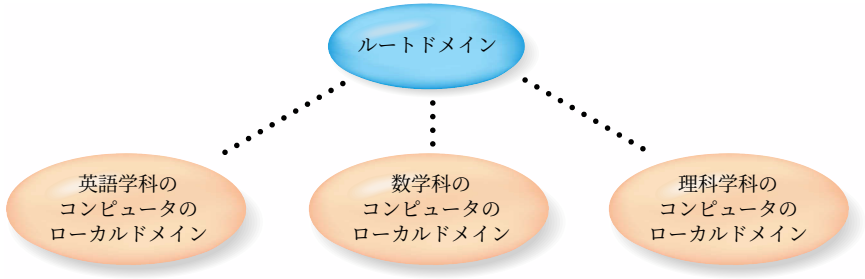
NetInfo の共有ドメインを利用する場合は、上位層と下位層の階層構造を理解する必要があります。

2 つのレベルの階層構造

最もシンプルな階層構造は、2 つのレベルの階層構造です。

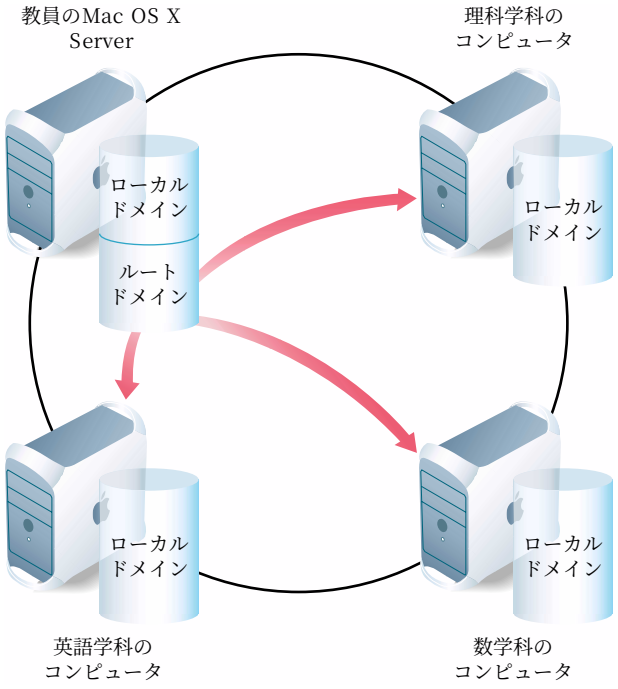


2 つのレベルの階層構造を使用できるケースについて、次に説明します：



各学科（英語、数学、理科）には、専用のコンピュータがあります。各学科の生徒は、その学科のコンピュータのローカルドメインでユーザとして定義されています。これらの 3 つの学科の上位層は同じ（つまり、ルートドメイン）で、すべての教師が定義されています。教師は、ルートドメインのメンバーとして、すべての学科コンピュータ上のサービスを使用できます。各ローカルドメインのメンバーは、自分のローカルドメインが置かれているサーバ上のサービスのみを使用できます。

ローカルドメインはそれぞれのサーバ上にありますが、上位層ドメインは、下位層ドメインのコンピュータからアクセス可能な任意の「Mac OS X Server」上に置くことができます。この例では、ルートドメインは、学科サーバからアクセス可能な任意のサーバ上に置くことができます。たとえば、いずれかの学科サーバ上に置いたり、下の図に示すように、ネットワーク上のまったく別のサーバに置いたりすることができます。

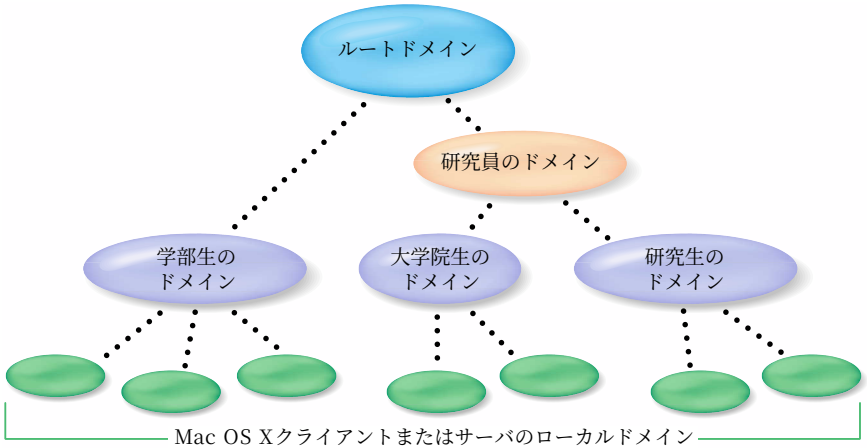


教師が3つの学科サーバのいずれかにログインしたときに、ローカルドメインでその教師が見つからない場合は、サーバはルートドメインを検索します。

ルートドメインは、特殊な共有ドメインです。ルートドメインは、NetInfo階層構造の常に最上位にある共有ドメインです。ルートドメインは、階層構造を使用するすべてのコンピュータに公開されます。この例の共有ドメインはルートドメインだけですが、より複雑な階層構造では複数の共有ドメインが存在することもあります。

より複雑な階層構造

NetInfo は、複数の階層を持つドメインの構造にも対応しています。数多くのユーザがいる複雑なネットワークでは、このような構成が便利です。ただし、その管理方法はより複雑になります。



このケースでは、ルートドメインで定義されている教師は、ローカルドメインが置かれている任意の Mac OS X コンピュータを使用できます。研究員のドメインで定義されている研究員は、上位層ドメインが大学院生または研究生のいずれかであるローカルドメインの Mac OS X コンピュータにログインできます。これは、研究員のドメインが、大学院生のドメインと研究生のドメインの上位層ドメインであるからです。

サーバが NetInfo の階層構造を検索する方法

デフォルトの検索設定では、サーバは、NetInfo ドメインで、ローカルドメインから順にユーザを検索します。

- サーバのローカルドメインに上位層がない場合、サーバは、ローカルドメインだけを検索します。
- サーバのローカルドメインに上位層 NetInfo ドメインがある場合は、ローカルドメインでユーザが見つからないときに、サーバは、その上位層ドメインを検索します。ローカルドメインの上位層でユーザが見つからないときに、その上位層ドメインが 2 番目の上位層ドメインの下位層として定義されている場合は、2 番目の上位層ドメインが検索されます。それでもユーザが見つからない場合、サーバは、NetInfo 階層を上方向に順番に検索します。サーバは、ユーザが見つかるか、または最上位の上位層を検索するまで、検索し続けます。

サーバがほかの NetInfo ドメインを検索するように設定したい場合、または LDAP サーバが検索されるように指定したい場合は、「Directory Setup」アプリケーションを使って検索ポリシーをカスタマイズします。その方法については、52 ページの「検索ポリシーを設定する」を参照してください。

NetInfo を初めて設定する

NetInfo ドメインを設定するときは、次のように操作します。

手順 1：サーバへのアクセス要件を評価する

「Mac OS X Server」にアクセスする必要があるユーザを識別します。

LDAP サーバからユーザ情報にアクセスできない場合、または「Mac OS X Server」で最も簡単にユーザ情報を管理する場合は、それらのユーザを NetInfo ドメインで定義します。

手順 2：NetInfo の階層構造を設計する

ユーザ情報をローカル NetInfo ドメインに保管するか、NetInfo ドメインに保管してサーバ間で共有するかを決定します。使用する共有ドメインと下位層ドメイン、共有ドメインを置くサーバ、およびドメイン間の上位層と下位層の関係を決定しながら、NetInfo の階層構造を設計します。通常、任意のドメインに関連付けるユーザ数は、10,000 人未満にします。

NetInfo 階層構造の構成の決定方法については、「NetInfo 活用ガイド」の第 2 章「NetInfo のプランニング」を参照してください。

手順 3：NetInfo の階層構造を設定する

NetInfo の階層構造を設定するときは、主に次の手順で行います。

1. 共有ドメインを設定します。共有ドメインのホストにするサーバごとに、共有ドメインを作成し、目的の階層構造にバインドします。
2. Mac OS X コンピュータごとにローカルドメインを設定し、上位層ドメインとして機能させる共有ドメインにバインドします。
3. 複製を設定します。共有ドメインを複製すれば、データアクセスの速度と信頼性を向上させることができます。
4. Windows ユーザの認証を設定します。NetInfo と暗号化パスワードを使って Windows ユーザを認証する場合は、NetInfo 階層構造内のすべてのドメインで「Authentication Manager」を使用可能にします。
5. ユーザやグループなど、共有する情報を共有ドメインに読み込みます。

各手順について詳しくは、「NetInfo 活用ガイド」の第 3 章「NetInfo の階層構造を設定する」を参照してください。

手順 4：検索ポリシーをカスタマイズする（省略できます）

デフォルトの NetInfo の検索ポリシーがサーバの目的に適していない場合は、「Directory Setup」を使って検索ポリシーをカスタマイズします。その方法については、52 ページの「検索ポリシーを設定する」を参照してください。

LDAP を使用する

サーバには LDAP 対応機能が組み込まれているので、サーバは LDAP V2 サーバからユーザ情報を取り込むことができます。

LDAP サーバは、ユーザ、グループ、プリンタ、サーバなど、さまざまなユーザやネットワークリソースの情報を管理することができます。LDAP サーバをいったん設定すると、「Mac OS X Server」がそのサーバにアクセスしてユーザ情報およびその他の情報を取り込めるように簡単に設定することができます。

LDAP サーバへのアクセスを設定する前に

LDAP サーバが「Mac OS X Server」のユーザ情報の情報源として機能するためには、LDAP サーバが LDAP ベースの認証とパスワードの確認に対応できるように設定する必要があります。LDAP サーバへのアクセスは、LDAP サーバとそのデータの管理を担当するシステム管理者が設定します。

ユーザ認証のための適切な情報を提供するために、LDAP サーバには次の 4 つの項目に関するエントリと属性が設定されている必要があります。ユーザ名（「RecordName」フィールドと「RealName」フィールド）、パスワード、およびユーザ ID です。ユーザがアクセスする必要がある「Mac OS X Server」サービスによって、補足情報が必要になることもあります。

LDAP サーバがすべての必要なデータを提供するように設定したら、各データ項目の検索基準と属性名を紙に書き留めておいてください。この情報は、「Mac OS X Server」が LDAP にアクセスできるように設定するときに必要です。

LDAP を初めて設定する

サーバが LDAP サーバにアクセスするように設定するには、次の手順に従ってください。詳しくは 323 ページの「LDAP アクセスを設定する」を参照してください。

手順 1：LDAP サーバのデータを準備する

サーバ認証で必要なデータ、およびデータを使用するその他のサービスで必要なデータを提供できるように、LDAP サーバのエントリと属性を必要に応じて変更します。「Mac OS X Server」が使用する LDAP データの全仕様については、314 ページの「LDAP データの仕様」を参照してください。適切なフォーマットで情報を提供するためには、LDAP サーバの情報を追加、変更、または再構成する必要があるかもしれません。

手順 2：LDAP に対応できるようにする

「Directory Setup」アプリケーション（「Applications/Utilities」にあります）を開きます。カギをクリックして、サーバ管理者としてログインします。「Directory Setup」の「サービス」パネルの「LDAPv2」を選択して、「設定」をクリックします。

手順 3：LDAP サーバを識別する

「固有名」パネルで、LDAP サーバのドメイン名または IP アドレスを指定します。

手順 4：LDAP の検索基準を定義する

「レコード」パネルで、「Users」というレコードタイプを、ユーザ情報を提供する LDAP サーバ上の 1 つまたは複数の検索基準にマッピングします（たとえば、o= 人、ou= 会社名など）。また、LDAP サーバからグループ情報を取り込む場合は、レコードタイプ「Groups」もマッピングします。

手順 5：ユーザおよびグループ情報のデータタイプをマッピングする

「データ」パネルで、少なくとも「RecordName」、「RealName」、「Password」、および「UniqueID」というデータタイプを、それらの値を提供する LDAP フィールドにマッピングします。たとえば、UniqueID は userid という名前の LDAP フィールドに保管できます。ほかの情報を取り込む場合は、別の適切なデータタイプを必要に応じてマッピングします。

手順 6：接続属性を定義する

「アクセス」パネルで、LDAP サーバでのデータの検索の最大所要時間などの、ユーザのサーバと LDAP サーバの間に確立する接続特性を示す情報を入力します。

手順 7：LDAP データを使用する方法を指定する

LDAP サーバをサーバの検索ポリシーに追加するか、または LDAP サーバの特定ユーザのエイリアスを定義します。その方法については、「検索ポリシーを設定する」を参照してください。

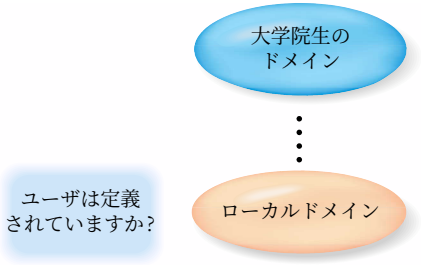
検索ポリシーを設定する

サーバは、その検索ポリシーで指定されている場所でユーザ情報を検索します。

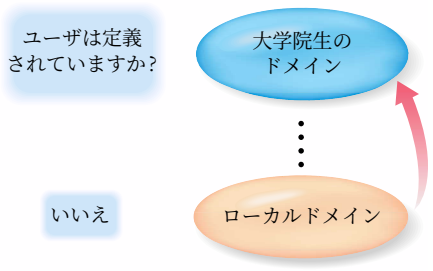
ユーザ情報の保管に NetInfo ドメインだけを使っている場合は、通常、デフォルトの検索ポリシーを適用できます。ただし、LDAP サーバまたは別の NetInfo ドメインを検索するときは、「Directory Setup」を使って検索ポリシーをカスタマイズして定義します。

デフォルトの検索ポリシー

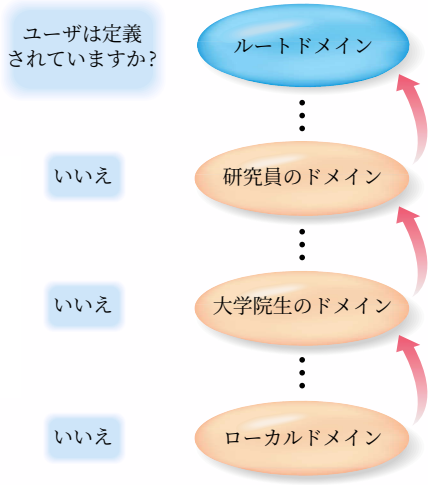
ユーザがログインしようとすると、「Mac OS X Server」は常に自分のローカル NetInfo ドメインを検索します。



ローカルドメインでユーザが見つからない場合は、そのローカルドメインに定義されている任意の上位層ドメインを検索します。

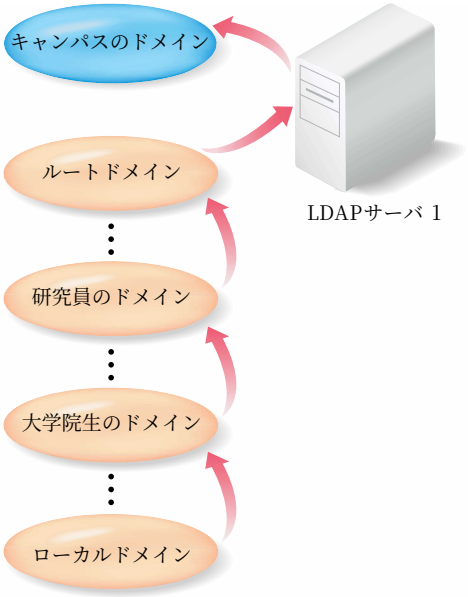


それでもユーザが見つからない場合は、NetInfo の階層構造で 1 つ上のレベルにある上位層を検索します。同様に、ルートドメインまで検索し続けます。



カスタム検索

デフォルトの検索ポリシーには含まれない LDAP サーバまたは NetInfo ドメインを使ってユーザに関する情報を入手する場合、「Directory Setup」アプリケーションを使ってカスタムの検索ポリシーを設定します。カスタマイズした検索ポリシーの例を次に示します。

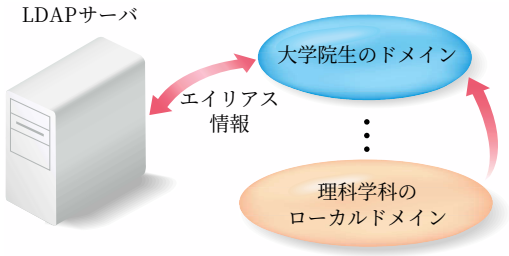


このケースでは、デフォルトの検索ポリシーのドメインでユーザが見つからないときに、ユーザ情報として LDAP サーバ 1 が参照されています。ユーザ情報がその LDAP サーバ上で見つからない場合は、「Campus」という名前の NetInfo ドメインが検索されます。

エイリアスを使用する

検索ポリシーで指定されているどの場所にも情報が保管されていないユーザを、サーバが認証できるようにしたい場合があります。

サーバがこのようなユーザを検索できるようにするためには、検索ポリシーで指定されているいずれかの NetInfo ドメインでユーザのエイリアスを定義します。エイリアスとは、ユーザ情報が実際に保管されている場所へのポインタです。サーバがエイリアスを使ってユーザを認証する必要がある場合、そのサーバは、ユーザ情報が実際に置かれている場所からその情報を取り込みます。次の図を参照してください。



上の図では、大学院生のドメインにユーザのエイリアスが定義されています。このエイリアスを使って、ユーザの情報を LDAP サーバから取り込みます。ユーザがローカルまたは大学院生のドメインで見つからないとき、LDAP サーバ全体の検索を行う必要はありません。検索は、エイリアスが参照するユーザに対してのみ行われます。

このようなケースを設定するには、LDAP サーバにアクセスしても検索ポリシーに LDAP サーバを追加しないように、サーバを設定します。次に、LDAP サーバ上の各ユーザのエイリアスを、検索ポリシーで指定されている NetInfo ドメインで作成します。

エイリアスを作成するときは、「Server Admin」の「ユーザとグループ」モジュールを使用します。詳しくは、「ユーザとグループ」のオンスクリーンヘルプを参照してください。

検索ポリシーを設定する前に

サーバの検索ポリシーを定義する前に、サーバが検索するように設定したい NetInfo ドメインまたは LDAP サーバに、「Mac OS X Server」がアクセスできるように設定されていることを確認します。

1 つ以上の NetInfo ドメインでエイリアスを定義することが、各ユーザにとって役に立つかどうかも判断します。

検索ポリシーを初めて設定する

手順 1：デフォルトの検索ポリシーを適用できるかどうかを判断する

デフォルトの NetInfo の検索ポリシーを適用できる場合は、これで操作は完了です。それ以外の場合は、手順 2 に進んでください。

手順 2：Directory Setup を開く

「Directory Setup」アプリケーション（「Applications/Utilities」にあります）を開きます。

手順 3：サーバの検索ポリシーオプションを定義する

「認証」パネルで、「検索」ポップアップメニューを使って、設定したい検索ポリシーを選びます。

- 「NetInfoネットワーク」はデフォルトのNetInfoの検索ポリシーです。この検索ポリシーは、サーバに上位層 NetInfo ドメインが設定されている場合に使用できます。この検索ポリシーを使用するサーバは、ユーザ情報を、まずローカルドメインで検索し、次に上位層ドメインの階層を上方向に順番に検索します。
- 「ローカルディレクトリ」を使用すると、サーバは、ローカルの NetInfo ディレクトリだけを使ってユーザを検索します。
- 「カスタムパス」を使用して、サーバがデフォルトの NetInfo 検索ポリシーで NetInfo ドメインを検索した後に検索する場所を指定します。サーバ用に設定されている LDAP サーバを選択するか、デフォルトの検索ポリシーにない NetInfo ドメインを選択します。詳しくは、323 ページの「LDAP アクセスを設定する」を参照してください。

手順 4：個人のアプリケーションの検索ポリシーを定義する（省略できます）

サーバの検索ポリシーを設定できるだけでなく、検索ポリシーを、メールまたは個人情報マネージャなどの個人のアプリケーションで使用できるように定義できます。これを行うには、「コンタクト」パネルを使用し、手順 3 に書かれた操作を行います。

3

ユーザとグループ

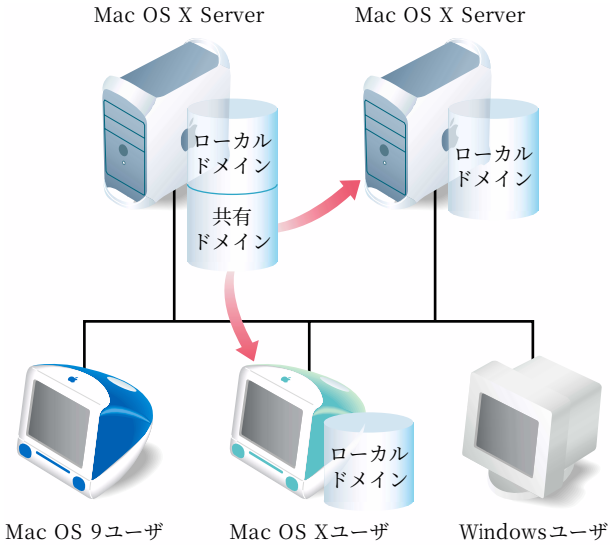
ユーザとグループとは？

個別のユーザまたはグループ（類似した要求を持つユーザの集まり）に、「Mac OS X Server」とそのサービスに対するアクセス権を与えるときは、ユーザとグループを定義します。

この章では、ユーザとグループの属性の概要と、その設定方法について説明します。

ユーザ情報の使用方法

「Mac OS X Server」は、管理者が定義するユーザ情報を使って、ユーザを認証し、ユーザが特定のサービスを使用する権限を与えられているかどうかを判断します。ユーザ情報は、ドメインと呼ばれる NetInfo データベースに保管されます。



各 Mac OS X コンピュータおよび「Mac OS X Server」には、ローカルドメインがあります。ローカルドメインで定義されているユーザのみが、そのローカルドメインが置かれているコンピュータを使用できます。前に示された図では、サーバのローカルドメインで定義されたユーザのみが、そのサーバへのアクセス権を持ちます。また、Mac OS X コンピュータのローカルドメインで定義されているユーザのみが、そのコンピュータにログインできます。

「Mac OS X Server」には、共有ドメインが定義されている場合もあります。共有ドメインには、ネットワーク上の複数の Mac OS X コンピュータおよびサーバが利用するユーザ情報が保管されます。共有ドメインで定義されたユーザは、その共有ドメインからユーザ情報を取り込むように設定されたどのコンピュータも使用することができます。前に示された図では、共有ドメインで定義されたユーザは、サーバと Mac OS X コンピュータのどちらにもログインできます。ユーザがログインしたときにそのユーザがローカルドメインに見つからない場合は、共有ドメインが参照されます。

サーバのローカル NetInfo ドメインおよび共有 NetInfo ドメインでユーザとグループを定義するときは、「Server Admin」の「ユーザとグループ」モジュールを使用します。

また、LDAP（Lightweight Directory Access Protocol）サーバからユーザ情報を取り込むようにサーバを設定することもできます。LDAP サーバを使ってユーザ情報を取り込む方法については、51 ページの「LDAP を使用する」を参照してください。

ユーザの特徴

ユーザを定義するときは、そのユーザを認証するために必要な情報を指定します。つまり、ユーザ名、パスワード、およびユーザ ID を指定します。ユーザが使用するサービスにかかわらず、これらの情報は必須です。ユーザがログイン時に認証されるためには、そのユーザが入力するユーザ名とパスワードが、サーバで定義されているいずれかのユーザのものと一致する必要があります。

その他のユーザ情報は、個別のサービスで使用されます。ユーザが権限を与えられている操作を判断したり、ユーザの環境を個別に設定したりするために使用されます。たとえば、次の情報が使用されます。

- サーバに対するユーザのアクセス権情報によって、ユーザがそのサーバを管理できるかどうかが決まります。管理者のアクセス権を持っているユーザだけが、「Server Admin」やその他のサーバ管理アプリケーションを使用できます。
- ユーザのメール情報には、ユーザのメールアカウントの属性が記録されています。この情報は、メールサービスで使用されます（153 ページ）。
- Macintosh マネージメントサービス（195 ページ）、Web サービス（121 ページ）、Apple ファイルサービス（85 ページ）、および NFS（Network File System）サービス（100 ページ）では、ユーザのホームディレクトリ情報が使用されます。ホームディレクトリとは、ユーザのファイルと環境設定が保存されるネットワーク上の場所のことです。

グループの特徴

グループとは、類似した要求を持つユーザの単なる集まりのことです。たとえば、すべての英語教師を 1 つのグループにまとめ、そのグループに、「Mac OS X Server」上の特定のファイルまたはフォルダに対するアクセス権を与えることができます。

グループを使用すると、共有リソースの管理を簡略化できます。つまり、特定のリソースを必要とするユーザに個別にアクセス権を与える代わりに、それらのユーザを 1 つのグループにまとめて、そのグループにアクセス権を与えることができます。

ユーザとグループを設定する前に

1 つまたは複数の「Mac OS X Server」でユーザとグループを設定する前に、以下のことを確認してください。

- すべての「Mac OS X Server」が必要なユーザ情報にアクセスできるように、ユーザ情報を保管する方法を考えます。また、そのために必要な共有 NetInfo ドメインまたは LDAP サーバを設定します。設定方法については、第 2 章「ディレクトリサービス」を参照してください。
- 1つのサーバに複数の NetInfo ドメインがある場合は、それぞれのドメインで定義するユーザを決めます。

参考：ユーザの追加を始めるときに、どの NetInfo ドメインも準備が完了していない場合は、ほかのサーバの既存の NetInfo ドメインにユーザを追加します。(ローカルドメインはいつでも使用できます。)「ユーザとグループ」モジュールを使えば、後でユーザやグループを別のドメインまたはサーバに簡単に移動できます。操作手順については、「ユーザとグループ」のオンスクリーンヘルプを参照してください。

- サーバに対して類似した要求を持つユーザを識別します。それらのユーザは、グループとしてまとめることができます。

ユーザとグループを初めて設定する

「Mac OS X Server」でユーザとグループを設定するときは、次のように操作します。これらの手順を実行するために追加情報が必要な場合は、「Server Admin」で「U&G」をクリックし、「ヘルプ」を選びます。

手順 1：サーバの設定時に定義した管理者アカウントを変更する

「設定アシスタント」を使ってサーバを設定するときは、オーナーまたは管理者のパスワードを指定します。指定したパスワードは、サーバのルートパスワードにもなります。「Server Admin」の「ユーザとグループ」モジュールを使って、ルートパスワードとは異なるパスワードを持つ管理者ユーザを作成します。サーバ管理者に、ルートのアクセス権は必要ありません。

ルートパスワードは安全な場所に保管し、その使用には細心の注意を払う必要があります。ルートユーザには、システムファイルも含めて、システムに対するすべてのアクセス権が与えられます。必要に応じて、「ユーザとグループ」モジュールを使ってルートパスワードを変更できます。ルートユーザに設定を行うときは、「ユーザとグループのリストを表示」を選び、「システムユーザとグループを表示」を選びます。

手順 2：新規ユーザを作成する

新規ユーザアカウントを作成するときは、「Server Admin」の「ユーザとグループ」モジュールを使用します。サーバに複数の NetInfo ドメインがある場合は、ユーザを作成するドメインを選びます。ユーザの設定の説明については、次のセクション「ユーザの設定」を参照してください。

手順 3：新規グループを作成する（省略できます）

グループを使いたい場合は、「Server Admin」の「ユーザとグループ」モジュールを使って新規グループを作成します。サーバに複数の NetInfo ドメインがある場合は、新規グループを作成するドメインを選びます。グループの設定の説明については、68 ページの「グループの設定」を参照してください。

ユーザの設定

ユーザの設定を表示するときは、「Server Admin」の「一般」タブをクリックします。次のいずれかの操作を行います。

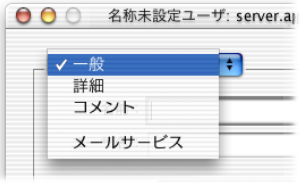
新規ユーザを作成するときは、次のように操作します。

- 「U&G」をクリックし、「新規ユーザ」を選びます。NetInfo ドメインのリストが表示された場合は、ユーザを作成したい NetInfo ドメインを選びます。
- 「ユーザとグループ」ウインドウで「新規ユーザ」ボタンが利用可能な場合は、このボタンをクリックします。（新規ユーザは、現在操作しているドメインに作成されます。）

ユーザを編集するときは、次のように操作します。

- ウインドウ（たとえば、「U&G の検索結果」ウインドウ）でユーザの名前を選び、「編集」ボタンをクリックします。

ユーザの設定のウインドウには、次の 4 つのパネルがあります。「一般」、「詳細」、「コメント」、および「メールサービス」パネルです。ウインドウの上端にあるポップアップメニューから、設定したいパネルを選びます。



一般的なユーザ設定

名前

ユーザを識別するために使用する名前を入力します。たとえば、「Bob W. Brown, Jr」と入力します。

ユーザ名

ログイン名を入力します。この名前は、メールアドレスとして使用される場合もあります。この名前に指定できるのは、英数字、ハイフン（-）、およびアンダースコア（_）のみです。通常は 8 文字（半角英数文字）以下で指定します。

パスワード

ユーザのパスワードを入力します。ユーザは、サーバにログインするときにこのパスワードを入力します。パスワードでは大文字と小文字が区別されます。入力時に画面上に表示されることはありません。ユーザはログイン時にパスワードを変更できます。

パスワードは、権限がないユーザが簡単に推測できないように、英数字と記号を組み合わせて指定します。空白文字と、option キーを使った文字の組み合わせは使用しないでください。また、ユーザのコンピュータで入力できない文字も使用しないでください。（コンピュータによっては、2 バイトの文字や、先頭や途中に空白などが含まれるパスワードに対応していない場合があります。）「Mac OS X Server」の各サービスでのパスワード要件については、71 ページの「Mac OS X Server でのパスワードの制限」を参照してください。

検証

「パスワード」フィールドに入力したパスワードを、このフィールドに再入力します。

ユーザがサーバを管理できるようにする

ユーザがサーバを管理できるように設定したい場合は、このオプションを選びます。「Mac OS X Server」を初めてインストールした場合、これを管理できるのはサーバの設定時に指定されたオーナーおよび管理者だけです。サーバ管理者は、「Mac OS X Server」およびそのほかのサーバ管理アプリケーションを使用できます。また、サーバのすべての機能にアクセスできます。

ユーザにログインを許可する

ユーザがサーバにログインできるように設定したい場合は、このオプションを選びます。このオプションは、デフォルトで選択されます。このオプションを選択しなかった場合でも、ユーザへのメール配送が停止することはありません。メール配送を停止するときは、「メールサービス」パネルを使用します。

詳細なユーザ設定

ユーザ ID

これは、ユーザを一意に識別する番号です。この番号によって、ユーザが「Mac OS X Server」上で持つアクセス権が決まります。たとえば、ユーザ ID は、共有ポイントに関するアクセス権を管理するために使用されます。アクセス権については、第 4 章「共有」を参照してください。

ユーザ ID は、新規ユーザの作成時に自動的に割り当てられますが、後で変更することができます。サーバの検索ポリシー内で一意の、100 以上の値を割り当てます。（検索ポリシーについては、52 ページの「検索ポリシーを設定する」を参照してください。）最大値は、2,147,483,647 です。99 以下のユーザ ID は、システムアカウントに割り当てられます。これらの ID を持つユーザは削除できません。また、これらのユーザを変更しないでください。

プライマリグループ

ユーザを自動的に所属させるグループの ID を入力します。デフォルトでは、20 に設定されます。

ログインシェル

ユーザがサーバにコマンドライン操作をするときに使用するデフォルトのシェルを選びます。「なし」を選ぶと、ユーザはコマンドラインを使用できなくなります。ユーザが SSH を使ってサーバにアクセスできないようにしたい場合に便利です。

ホームディレクトリ

ユーザのホームディレクトリを定義します。これは、ユーザが個人的に使用するためのフォルダです。「Finder」の「移動」メニューから「ホーム」を選ぶと、自動的に表示されます。ホームディレクトリは、共有ポイントと呼ばれる特別なディレクトリの中に置く必要があります。

ホームディレクトリを定義する前に、そのホームディレクトリを置く共有ポイントを用意する必要があります。ホームディレクトリのデフォルトの共有ポイント（「Users」）を使用するか、共有ポイントを新しく作成します。共有ポイントのオーナーには、読み出し／書き込みのアクセス権を割り当て、共有ポイントの「グループ」および「全員」には、読み出しのアクセス権を割り当てます。共有ポイントおよびアクセス権については、73 ページの第 4 章「共有」を参照してください。また、ホームディレクトリの共有ポイントを作成する手順については、「ユーザとグループ」の「ヘルプ」を参照してください。

ユーザを最初に定義するときは、ホームディレクトリのデフォルト設定がユーザに割り当てられます。（ホームディレクトリのデフォルト設定は、「U&G」メニューの「デフォルトのホームディレクトリ」コマンドを使って定義できます。）各ユーザのデフォルト設定は、以下の方法で変更できます。

- ユーザにホームディレクトリを割り当てないときは、「なし」を選びます。
- ユーザが定義されているサーバ上にホームディレクトリを作成するときは、「ローカル」を選びます。「共有ポイント」ポップアップメニューから選んだ共有ポイントに、ユーザのユーザ名と同じ名前のディレクトリが作成されます。たとえば、共有ポイントが「Users」の場合、「Mary」という名前のユーザのホームディレクトリは「Users/Mary」フォルダになります。ホームディレクトリ名は、「共有ポイント」ポップアップメニューの下の「パス：」の横に表示されます。

ホームディレクトリ名の下には、共有ポイントに対するホームディレクトリの相対パスが表示されます。

「Server Admin」によってホームディレクトリが作成されると、ユーザは、そのホームディレクトリのオーナーとして定義され、読み出し／書き込みのアクセス権が割り当てられます。

- 別のサーバにホームディレクトリを定義したい場合、またはホームディレクトリのパスと名前を自分で指定したい場合は、「カスタム」を選びます。

重要 「Server Admin」では、ログインしたサーバ上にだけホームディレクトリが自動的に作成されます。ユーザのホームディレクトリをリモートサーバ上に置きたい場合は、ホームディレクトリを手動で作成してから、「詳細」パネルを使ってユーザをホームディレクトリに関連付けてください。ホームディレクトリを手動で定義する方法については、オンスクリーンヘルプを参照してください。

「カスタム」オプションは、ホームディレクトリを共有ポイント内の複数のサブディレクトリに再編成する場合などに使います。たとえば、「Users」が共有ポイントの場合、教師または生徒のホームディレクトリを「Teachers」サブディレクトリと「Students」サブディレクトリに分類すると、教師のホームディレクトリは「Users/Teachers/Smith」、生徒のホームディレクトリは「Users/Students/Mary」になります。ホームディレクトリが共有ポイント内の最上位にないので、このようなホームディレクトリを定義するときは「カスタム」オプションを使用します。

「サーバ」フィールドにサーバの DNS 名または IP アドレスを入力し、「共有ポイント」フィールドに共有ポイントを入力します。「パス」フィールドには、ホームディレクトリのフォルダ名を、共有ポイント内でのパスを含めて入力します。「パス」フィールドの下には、共有ポイントに対するホームディレクトリの相対パスが表示されます。

「カスタム」オプションを使って、ローカルサーバ上にホームディレクトリを作成します。次に、「共有」モジュールを使って、ユーザをそのホームディレクトリの所有者として定義し、所有者に読み出し／書き込みアクセス権を割り当てます。アクセス権を定義する方法については、73 ページの第 4 章「共有」を参照してください。

ネットワークユーザに対して、ホームディレクトリを自動的に表示することができます。その手順については、70 ページの「ホームディレクトリが自動的にマウントされるように設定する」を参照してください。

ユーザのコメント

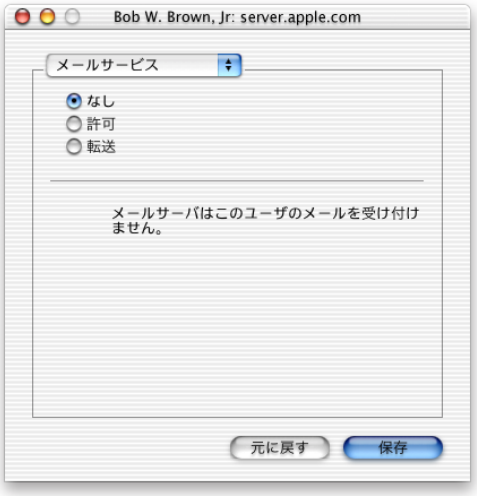
ユーザに関する一般的な情報を入力するときは、「コメント」パネルを使用します。コメントは、半角で 32,767 文字、全角で 16,383 文字まで入力できます。

メールサービスの設定

「メールサービス」パネルでは、ユーザがメールを使用できるかどうかを指定し、ユーザのメールアカウントを設定することができます。これらの設定を使ってユーザにメールサービスを提供する方法について詳しくは、153 ページの第 8 章「メールサービス」を参照してください。

メール配送を停止する

ユーザのメール配送を停止するときは、「なし」をクリックします。



メール配送を開始する

ユーザのメール配送を開始して、メールアカウントのオプションを設定するときは、「許可」をクリックします。

サーバにあるメールアカウント

ユーザのメールが配送されるサーバの IP アドレスまたは DNS 名を入力します。

メールの使用方法の選択

ユーザのメールアカウントで使用するプロトコルを選びます。選択できるのは、POP（Post Office Protocol）、IMAP（Internet Message Access Protocol）、またはその両方です。これらのプロトコルについては、153 ページの第 8 章「メールサービス」を参照してください。

オプション

メールアカウントの追加オプションを設定するときにクリックします。

POP と IMAP で別の受付箱を使用する

それぞれ別の受付箱を使って POP メールと IMAP メールを管理するときは、このオプションを選びます。

IMAP フォルダリストに POP メールボックスを表示する

「POP Inbox」という名前の IMAP フォルダを表示するときは、このオプションを選びます。

NotifyMail を許可する

新着メールが到着したらユーザのメールアプリケーションに自動的に通知するときは、このオプションを選びます。通知が送られる IP アドレスは、ユーザが前回ログインしたときの IP アドレス、または指定したアドレスです。

メールを転送する

「転送」をクリックしてアドレスを指定することによって、ユーザのメールを特定のメールアドレスに転送できます。

グループの設定

グループの設定を表示するときは、「Server Admin」の「一般」タブをクリックし、以下のいずれかの操作を行います。

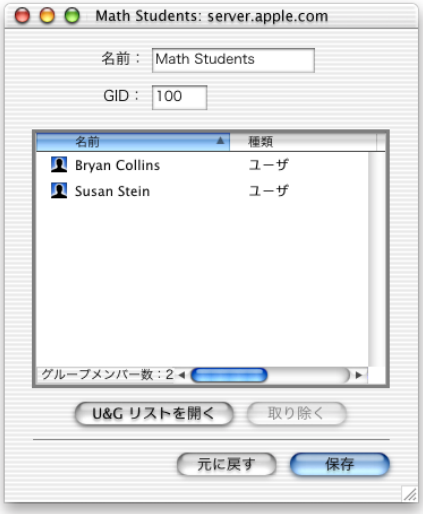
新規グループを作成するときは、次のように操作します。

- 「U&G」をクリックし、「新規グループ」を選びます。ドメインのリストが表示された場合は、新しいグループを作成したいドメインを選びます。
- 「ユーザとグループ」ウインドウで「新規グループ」ボタンが利用可能な場合は、このボタンをクリックします。（新規グループは、現在操作しているドメインに作成されます。）

グループを編集するときは、次のように操作します。

- グループのリストが表示されるウインドウ（たとえば、「U&G の検索結果」ウインドウ）でグループの名前を選び、「編集」ボタンをクリックします。

このウインドウを使ってグループの設定を操作します。



名前

グループの名前を入力します。このグループにメールを送信できるようにしたい場合は、名前に空白文字や option キーを使った文字を使用しないでください。

GID

これは、グループの ID です。この ID によって、そのグループのメンバーがサーバ上で実行できる操作が決まります。たとえば、グループ ID は、共有ポイントに関するアクセス権を追跡するために内部で使用されます。アクセス権について詳しくは、第 4 章「共有」を参照してください。

グループ ID は、新規グループの作成時に自動的に割り当てられますが、後で変更することができます。ユーザ ID には、操作している NetInfo ドメイン内で一意の、100 より大きい値を割り当てます。100 よりも小さい ID を持つグループは削除できません。

名前、種類、ID、場所

グループに現在関連付けられているユーザの特徴です。「種類」は、ユーザが管理者のアクセス権を持っている場合は「管理者」となり、それ以外の場合は「ユーザ」となります。「場所」は、そのユーザが定義されている NetInfo ドメインを示します。すべての列が表示されない場合は、横方向にスクロールします。

グループにユーザを追加するときは、「U&G リストを開く」をクリックし、「ユーザとグループのリスト」からグループの設定のウインドウにユーザをドラッグします。グループからユーザを取り除きたい場合は、目的のユーザを選び、「取り除く」をクリックします。

ユーザとグループの上手な使いかたとヒント

このセクションでは、ユーザとグループを管理するために役立ついくつかの技術について説明します。

ユーザとグループを書き出す／読み込む

場合によっては、ユーザを個別に追加するのではなく、ユーザやグループの情報をテキストファイルに保存し、そのファイルからユーザとグループを追加することがあります。この方法は、同じネットワーク上にない複数のサーバに、同じユーザとグループを追加したい場合などに便利です。

「ユーザとグループ」モジュールを使って、任意の「Mac OS X Server」上の NetInfo ドメインに、ファイルからユーザとグループを読み込むことができます。ファイルを作成するときは、次のいずれかの操作を行います。

- 「ユーザとグループ」モジュールを使って、ファイルを自動的に作成することができます。この処理は、ユーザとグループの「書き出し」と呼ばれます。
- また、ファイルを手動で作成することもできます。ファイルのフォーマットと手順については、308 ページの「ユーザとグループを読み込む／書き出すためのファイルフォーマット」を参照してください。

「ユーザとグループ」モジュールを使ってユーザおよびグループの書き出しや読み込みを行う手順については、ヘルプも参照してください。

ホームディレクトリが自動的にマウントされるように設定する

ユーザが「Finder」の「移動」メニューから「ホーム」を選んだときに、そのユーザのホームディレクトリが自動的に表示されるようにします。

また、ネットワークユーザにもホームディレクトリを自動的に表示できます。ネットワークユーザにホームディレクトリが自動的にマウントされるように設定するには、次のように操作します：

手順 1：NetInfo を設定する

ホームディレクトリを置きたいサーバに、共有 NetInfo ドメインを作成します。自動的なマウントを利用可能にしたい Mac OS X コンピュータの検索ポリシーに、このドメインを含める必要があります。NetInfo ドメインと検索ポリシーの定義については、41 ページの第 2 章「ディレクトリサービス」を参照してください。

手順 2：サーバに共有ポイントを設定する

「Server Admin」の「共有」モジュールを使って、サーバに共有ポイントを作成し、その共有ポイントを自動的にマウントするように設定します（80 ページ）。個々の手順については、オンスクリーンヘルプを参照してください。

手順 3：ユーザが自動的に接続解除されないことを確認する

「Server Admin」の「Apple ファイルサービス」モジュールを使って、ユーザが一定の時間サーバを使用しなかったときに接続が自動的に解除されないことを確認します。「アイドル状態のユーザ」パネルで、「接続解除するまでのアイドル時間」を選ばないようにします。この設定について詳しくは、90 ページを参照してください。

手順 4：ユーザとそのホームディレクトリを定義する

「Server Admin」の「ユーザとグループ」モジュールを使って、手順 1 で作成した共有 NetInfo ドメインに、ユーザと、必要に応じてエイリアスを定義します。ユーザにホームディレクトリを設定するときに、手順 2 で設定した共有ポイントを選びます。

Mac OS X Server でのパスワードの制限

「Mac OS X Server」でパスワードが必要なアプリケーションおよびサービスの大部分は、先頭または末尾にスペースを含まない 7 ビットまたは 8 ビット ASCII 文字のパスワードに対応しています。サーバのユーザにパスワードを定義するときに、次の表を参考にして、考慮する必要のある制限を確認してください。

サービスまたはアプリケーション	7 ビット ASCII 文字のパスワード使用可	8 ビット ASCII 文字のパスワード使用可	2 バイト文字のパスワード使用可
Apple ファイルサービス	×	×	
FTP（File Transfer Protocol）サービス	×		
IMAP	×	×（一部の IMAP クライアント）	
Macintosh マネージャ	×	×	
POP3	×		
Server Admin	×	×	
Web サービス	×		
Windows サービス	×		

ユーザとグループに関する問題を解決する

ユーザが自分のホームディレクトリのファイルにアクセスできない場合：

ホームディレクトリが置かれている共有ポイントおよびホームディレクトリにアクセスする権利を、ユーザが持っていることを確認します。ユーザには、共有ポイントに対する読み出しのアクセス権、およびホームディレクトリに対する読み出し／書き込みのアクセス権を割り当てる必要があります。

共有 NetInfo ドメインに定義されている Mac OS X ユーザがログインできない場合：

ユーザが共有 NetInfo ドメインのアカウントを使って Mac OS X コンピュータにログインしようとしたときに、そのドメインをホストとするサーバがアクセスできない状態にある場合、この問題が発生します。ユーザは、NetInfo アカウントを使用するようにコンピュータを設定した際に自動的に作成されたローカルユーザアカウントを使えば、Mac OS X コンピュータにログインできます。ユーザの名前は「administrator」（ユーザ名は「admin」）、パスワードは NetInfo パスワードになります。

4

共有

共有とは？

「Mac OS X Server」の「共有」モジュールによって、ほかのユーザと共有したい情報を指定したり、アクセス権を割り当ててその情報を参照および使用できるユーザを制限したりすることができます。

共有項目は、1 つ以上の共有ポイントに保存されます。共有ポイントとは、ネットワーク経由でアクセスできるフォルダ、ハードディスク（またはハードディスクのパーティション）、または CD のことです。つまり、共有項目グループの最上位レベルにあるアクセスポイントのことです。共有ポイントは、デスクトップ上ではマウントされたボリュームとして、また「Mac OS X」の「Finder」ではボリュームとしてユーザに表示されます。

アクセス権とは、ほかのユーザと共有したい任意の項目に割り当てるアクセスのレベルのことです。Apple ファイルサービス、Windows ファイルサービス（SMB）、NFS（Network File System）サービス、FTP（File Transfer Protocol）サービスなど、ほかのサービスで使用される共有ポイントおよびアクセス権を設定するときは、「Server Admin」の「共有」モジュールを使用します。

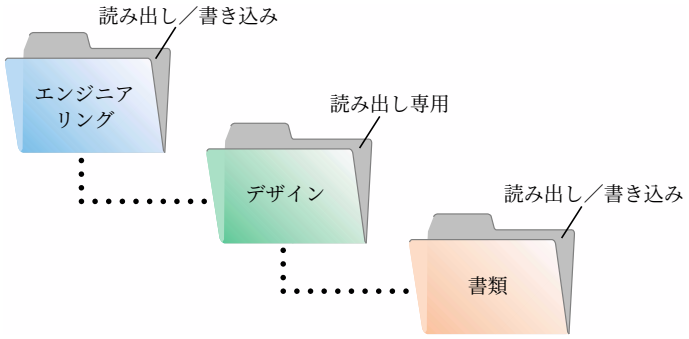
参考：「QuickTime Streaming Server」および Web サービスでは、独自のアクセス権の設定を使用します。「QuickTime Streaming Server」について詳しくは、第 9 章を参照してください。Web のアクセス権については、134 ページの「Web サイトのアクセスの設定」を参照してください。

アクセス権を割り当てる前に

アクセス権を割り当てる前に、共有項目のアクセス権について理解する必要があります。また、共有項目に対するアクセス権が必要なユーザと、それらのユーザに割り当てるアクセス権のタイプについても考慮する必要があります。

アクセス権の維持

共有ポイントおよび共有項目（ファイルを含む）では、それぞれ独自のアクセス権を設定します。項目を別のフォルダに移動した場合は、移動元での項目のアクセス権が維持され、移動先のフォルダのアクセス権が自動的に適用されるわけではありません。次の図では、2 番目のフォルダ（「デザイン」）と 3 番目の共有フォルダ（「書類」）に、これらの上位層フォルダとは異なるアクセス権が割り当てられています。



アクセス権のタイプ

共有ポイント、フォルダ、またはファイルに割り当てることができるアクセス権のタイプは、次の 4 つです。「読み出し／書き込み」、「読み出し専用」、「書き込み専用」、「なし」の 4 つです。次の表に、さまざまなタイプの共有項目（ファイル、フォルダ、共有ポイント）へのユーザアクセスが、権限によってどのような影響を受けるかを示します。

ユーザの操作	読み出し／書き込み	読み出し専用	書き込み専用	なし
共有ファイルを開く	可能	可能	不可	不可
共有ファイルをコピーする	可能	可能	不可	不可
共有ファイルの内容を編集する	可能	不可	不可	不可
共有フォルダまたは共有ポイントを開く	可能	可能	不可	不可
共有フォルダまたは共有ポイントをコピーする	可能	可能	不可	不可
項目を共有フォルダまたは共有ポイント内に移動する	可能	不可	可能	不可
項目を共有フォルダまたは共有ポイント外に移動する	可能	不可	不可	不可

フォルダに書き込み専用のアクセス権を割り当てることにより、ドロップボックスを作成できます。フォルダの所有者はドロップボックスの内容を表示および変更できますが、ほかのすべてのユーザはその内容を表示することはできず、その中にコピーすることだけが可能です。

ユーザの分類

アクセス権は、以下の3種類のユーザの分類に対して個別に割り当てることができます。

オーナー

ファイルサーバ上に新しい項目（ファイルまたはフォルダ）を作成したユーザが、その項目のオーナーです。オーナーには、そのフォルダの読み出し／書き込みのアクセス権が自動的に割り当てられます。項目のアクセス権を変更できるユーザは、そのオーナーとサーバ管理者だけです。管理者または項目のオーナーは、共有項目の所有権を別のユーザに譲ることができます。

グループ

ファイルとフォルダに対して同じアクセス権が必要なユーザは、グループアカウントにまとめることができます。1 つの共有項目に対するアクセス権は、1 つのグループにのみ割り当てることができます。グループの作成について詳しくは、57 ページの第 3 章「ユーザとグループ」を参照してください。

全員

全員とは、ファイルサーバにログインできるすべてのユーザのことです。登録ユーザ、ゲスト、anonymous FTP ユーザ、Web サイト利用者などがそうです。

アクセス権の階層構造

1 人のユーザが複数のユーザの分類に含まれていて、各分類に異なるアクセス権が割り当てられている場合は、以下の規則が適用されます。

- グループのアクセス権の方が全員のアクセス権よりも優先されます。
- オーナーのアクセス権の方がグループのアクセス権よりも優先されます。

たとえば、ユーザが共有項目のオーナーであると同時に、その共有項目に割り当てられたグループのメンバーである場合、そのユーザのアクセス権は、オーナーに割り当てられたアクセス権になります。

クライアントユーザとアクセス権

ユーザは、サーバ上に、または自分のデスクトップ上の共有フォルダに自分で作成したファイルまたはフォルダのアクセス権を設定できます。「AppleShare Client」ソフトウェアのユーザは、所有するフォルダのアクセス権を設定できます。Windows のファイル共有のユーザは、フォルダのプロパティを設定することはできますが、アクセス権を設定することはできません。

セキュリティの問題

データおよびネットワークのセキュリティの問題は重要です。ネットワークを保護する最も効果的な方法は、ファイル、フォルダ、および共有ポイントの作成時に適切なアクセス権を割り当てることです。

特にインターネットに接続している場合は、共有ポイントを作成してそのアクセス権を与えるときに注意してください。全員またはワールド（NFS サービスの場合）のアクセス権を与えると、インターネット上の全ユーザにデータが公開される可能性があります。

未登録ユーザ（ゲスト）によるアクセスを制限する

どのファイルサービスを設定するときも、ゲストアクセスを許可するかどうかを選ぶことができます。ゲストとは、有効なユーザ名やパスワードを入力しなくても匿名でサーバに接続できるユーザのことです。匿名で接続しているユーザによるアクセスは、全員のアクセス権が設定されたファイルおよびフォルダに制限されます。

不正なアクセスから情報を保護したり、情報や機器に損害を与える可能性のあるソフトウェアが導入されないようにするときは、「Server Admin」の「共有」モジュールを使って以下の防止策をとってください。

- ボリューム全体ではなくフォルダを個別に共有します。フォルダには、共有したい項目だけを保存します。
- ゲストにアクセスさせたくないフォルダに対して、全員に「なし」のアクセス権を割り当てます。項目のアクセス権をこのように設定した場合、これらの項目にアクセスできるのは、項目のオーナーまたはグループだけです。
- ゲストが利用できるファイルはすべて、1 つのフォルダまたはフォルダのセットに保存します。そのフォルダおよび内部の各ファイルに対して全員の分類に「読み出し専用」のアクセス権を割り当てます。
- ゲストがフォルダの項目を変更したり追加したりする必要がある場合にのみ、そのフォルダに対して、全員の分類に「読み出し／書き込み」のアクセス権を割り当てます。このフォルダの中にある情報のバックアップコピーを保存していることを確認してください。また、このフォルダに変更や追加が行われたかどうか、頻繁に確認してください。さらに、ウイルス防止プログラムを使って、サーバがウイルスに感染していないかどうかも定期的に確認してください。
- フォルダに変更や追加が行われたかどうか、頻繁に確認してください。また、ウイルス防止プログラムを使って、サーバがウイルスに感染していないかどうかも定期的に確認してください。
- 「Server Admin」で「FTP」モジュールを使って、anonymous FTP アクセスを禁止します。
- NFS ボリュームをワールドに書き出さないでください。エクスポートは、特定の範囲のコンピュータのみに制限してください。

共有を初めて設定する

共有ポイントおよび共有項目を作成して、それらのアクセス権を設定するときは、「Server Admin」の「共有」モジュールを使用します。アクセス権を設定するときは、グループを探すために「Server Admin」の「ユーザとグループ」モジュールも使用する必要があります。

共有を初めて設定するための手順について、以下に説明します。これらの手順を実行するときにさらに情報が必要な場合は、「Server Admin」で「共有」をクリックし、「ヘルプ」を選びます。

手順 1：ファイルサービスを開始する

サーバを遠隔地から管理する場合、共有ポイントを選んでアクセス権を設定するときは、Apple ファイルサービスが動作中でなければなりません。動作中かどうかが分からない場合は、簡単にチェックできます。「Server Admin」で「ファイルとプリント」タブをクリックします。動作中のサービスのアイコンには、地球のマークが表示されます。目的のファイルサービスに地球のマークが表示されない場合、サービスのアイコンをクリックし、「開始」メニュー項目を選びます。

手順 2：共有ポイントを作成する

共有したい項目を作成していない場合は、作成します。ディスクを複数のボリュームに分割して、各ボリュームに異なるアクセス権を与えたり、複数のフォルダを作成して、それぞれ異なるアクセスのレベルを設定したりすることができます。

新しいフォルダを作成するときは、そのフォルダを置きたいディスクまたはフォルダを開きます。「ファイル」メニューから「新規フォルダ」を選び、新しいフォルダの名前を入力します。

手順 3：共有ポイントのアクセス権を設定する

「一般」タブをクリックし、「共有」をクリックしてから、「アクセス権を設定」を選びます。共有したい項目を選び、「選択」をクリックします。共有ポイントの「共有」ウインドウが表示され、目的のアクセスレベルを設定できます。

共有ポイントのアクセス権をユーザおよびグループに割り当てるときは 、「U&G」をクリックし、「ユーザとグループのリストを表示」または「ユーザとグループを検索」を選びます。「検索」を選んだ場合、目的のユーザまたはグループを検索します。目的のユーザまたはグループの名前を、共有ウインドウの適切なフィールドにドラッグします。

オーナー、グループ、および全員のアクセス権を、各フィールドの横のポップアップメニューから選びます。割り当てたアクセス権は、Apple ファイルサービス、Windows サービス、および FTP サービスで使用されます。

共有の設定

共有ポイントのアクセス権は、共有ウインドウで設定します。共有ウインドウを表示するときは、「Server Admin」で「共有」をクリックします。その後、次のいずれかの操作を行います。

- 「アクセス権を設定」を選び、項目を選んでから、「選択」をクリックします。
- 「ディスクと共有ポイントを表示」を選び、項目を選んでから、「アクセス権」をクリックします。

ポップアップメニューから「一般」、「自動マウント」、または「NFS アクセス制御」を選んで、共有項目のアクセス権を設定します。以下のセクションでは、各パネルで使用できる設定について個別に説明します。

一般設定

共有ポイントおよび共有項目のアクセス権を設定するときは、「一般」パネルを使用します。

この項目とその内容を共有する

AFP、Windows、および FTP アクセス用の共有ポイントを設定するときは、このオプションを選びます。NFS アクセス用の共有ポイントの設定方法については、81 ページの「NFS アクセス制御の設定」を参照してください。これらのアクセス方法のどちらかまたは両方の項目を共有できます。

オーナー

「Server Admin」の「ユーザとグループのリスト」から、このフィールドにユーザをドラッグします。項目のデフォルトのオーナーは、その作成者です。

グループ

「Server Admin」の「ユーザとグループのリスト」から、グループをドラッグします。グループにアクセス権を与えたくない場合は、グループのアクセス権を「なし」に設定します。

全員

全員とは、ファイルサーバにログインできるすべてのユーザのことです。登録ユーザ、ゲスト、anonymous FTP ユーザ、Web サイト利用者などがそうです。全員にアクセス権を与えたくない場合は、全員のアクセス権を「なし」に設定します。

アクセス権

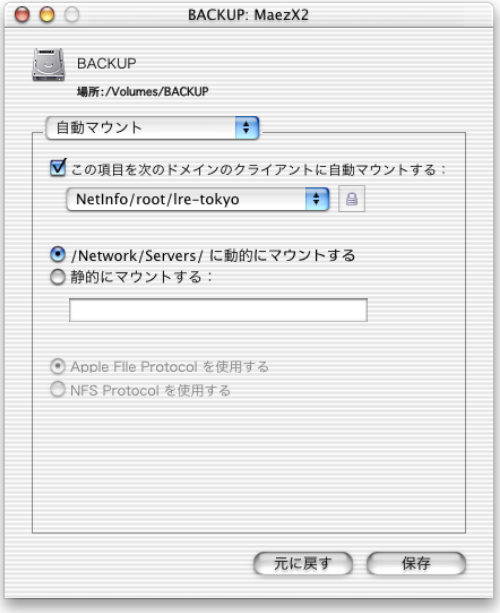
オーナー、グループ、および全員のアクセス権のレベルは、各ユーザの分類の右側に表示されるポップアップメニューで選びます。

コピー

この共有ポイントのアクセス権を、共有ポイント内のすべての項目（ファイルおよびフォルダ）にコピーするときは、このボタンをクリックします。この設定によって、ほかのユーザが設定したアクセス権が上書きされます。

自動マウントの設定

Apple ファイルサービスまたは NFS サービスで自動マウントする共有ポイント（ファイルではない）を設定するときは、「自動マウント」パネルを使用します。「自動マウント」パネルを表示するには、「ディスクと共有ポイント」ウインドウで共有項目を選び、「アクセス権」をクリックします。次に、共有ポイント名の下のポップアップメニューから「自動マウント」を選びます。



この項目を次のドメインのクライアントに自動マウントする

この共有項目を公開（または自動マウント）したい NetInfo の共有ドメインを選びます。この共有ドメインを使用するように設定したコンピュータでは、共有ポイントが自動的にマウントされます。

このドメインの変更権限を持つユーザの、ユーザ名とパスワードを要求されます。認証が終了したら、「この項目を次のドメインのクライアントに自動マウントする」をクリックします。

/Network/Servers/ に動的にマウントする

クライアントユーザが、各自のコンピュータの「/Network/Servers」フォルダ内の共有ポイントを見えるようにしたい場合は、このオプションを選びます。ユーザがフォルダ内の共有ポイントをダブルクリックすると、その共有ポイントがユーザのデスクトップまたは「Finder」（ユーザの「システム環境設定」の設定によります）にマウントされます。

静的にマウントする

クライアントコンピュータの起動時に共有ポイントが自動的にマウントされるようにしたい場合は、このオプションを選びます。項目を表示したい場所を選びます。ホームディレクトリでは静的なマウントを使用しないでください。

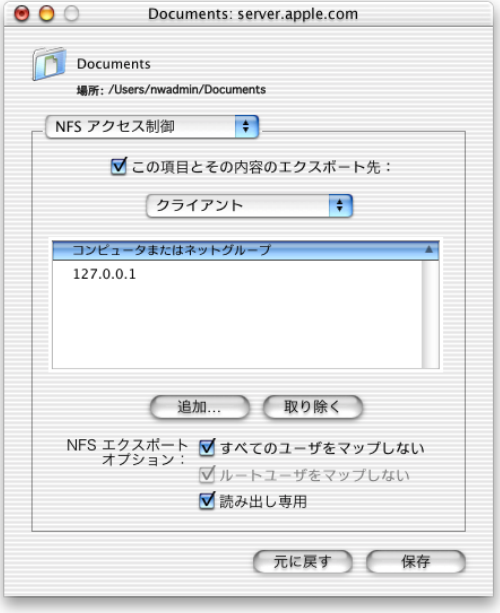
自動マウントオプション

AFP および NFS アクセス用に共有ポイントを設定した場合は、いずれかのラジオボタンをクリックして、共有ポイントのマウントに使用したいプロトコルを指定します。

NFS アクセス制御の設定

NFS（Network File System）共有ポイントのエクスポートとそのアクセス権を設定するときは、「NFS アクセス制御」パネルを使用します。NFS では、ほかのファイルサービスとは異なる方法で認証を行います。つまり、ユーザ名とパスワードではなく IP アドレスを使ってアクセスを許可します。NFS 共有ポイントは、有効なクライアントコンピュータにエクスポートされます。これらのエクスポートは、指定した場所でボリュームとしてマウントされます。NFS エクスポートを Apple ファイルサービスや Windows サービスの共有ポイントにできますが、必ずしもそうする必要はありません。

「NFS アクセス制御」設定を表示するときは、「共有」をクリックし、「アクセス権を設定」を選びます。共有したい項目を選び、「選択」をクリックします。項目名の下のポップアップメニューで、「NFS アクセス制御」を選びます。これらの設定について詳しくは、102 ページを参照してください。



共有に関する問題を解決する

ユーザが共有項目を見つけることができない場合：

その項目のアクセス権をチェックします。項目のある共有ポイントとその項目に至るまでのそれぞれのフォルダに対して、ユーザは、少なくとも読み出しのアクセス権を持っている必要があります。

参考：サーバ管理者とユーザとでは、共有ポイントの見えかたが異なります。管理者は、サーバ上のすべての共有ポイントを見ることができます。ユーザが見ることのできる共有ポイントを確認するときは、ユーザの名前とパスワードを使ってログインします。

ユーザが CD-ROM ディスクにアクセスできない場合：

- CD-ROM ディスクを共有ポイントに設定してあることを確認します。
- 複数の CD を共有している場合は、それぞれに固有の名前があることを確認します。

5

ファイルサービス

ファイルサービスとは？

ファイルサービスによって、クライアントユーザは、ネットワーク上のファイル、アプリケーション、およびその他のリソースにアクセスできます。ファイルサービスの設定、開始と停止、および状況の確認を行うときは、「Server Admin」を使用します。各サービスのゲスト（未登録ユーザ）アクセスを許可するときは、そのサービスのモジュールを使用しますが、共有する項目へのアクセスを制御するときは、「Server Admin」の「共有」モジュールを使用します。共有について詳しくは、第 4 章「共有」を参照してください。

「Mac OS X Server」には 4 つのファイルサービスが含まれます。

- Apple ファイルサービスは、AFP（Apple Filing Protocol）を使って、Macintosh または Macintosh 互換のオペレーティングシステムを使用するクライアントとのリソースの共有を提供します。
- Windows サービスは、SMB（Server Message Block）プロトコルを使って、Windows または Windows 互換のオペレーティングシステムを使用するクライアントとのリソースの共有、および Windows クライアントの名前解決サービスを提供します。
- NFS（Network File System）サービスによって、NFS クライアントソフトウェアを持つユーザに対して、ディレクトリ（フォルダ）を利用可能にすることができます。
- FTP（File Transfer Protocol）サービスによって、FTP を使用しているすべてのユーザとファイルを共有できます。

ファイルサービスを設定する前に

データとネットワークのセキュリティは、ファイルサービスを設定するときに考慮する必要がある最も重要な問題です。

ファイルとフォルダのアクセス権を設定する

個々のファイルの権限の設定は、サーバを保護する上で最も重要なことです。「Mac OS X」では、ファイルごとに独自のアクセス権の設定を使用します。これらの設定は、その上位層フォルダのアクセス権の設定には依存しません。ユーザは、サーバ上にユーザ自身で保存したファイルまたはフォルダのアクセス権を設定できます。また、サーバ管理者は、共有ポイントに対して同様の操作を行うことができます。共有ポイントの設定およびアクセス権の割り当てについて詳しくは、第 4 章「共有」を参照してください。

ゲストアクセスを制限する

どのファイルサービスを設定するときも、ゲストアクセスを許可するかどうかを選ぶことができます。ゲストとは、有効なユーザ名やパスワードを入力しなくても匿名でサーバに接続できるユーザのことです。匿名で接続しているユーザによるアクセスは、全員のアクセス権が設定されたファイルおよびフォルダに制限されます。

不正なアクセスから情報を保護したり、情報や機器に損害を与える可能性のあるソフトウェアが導入されないようにするときは、「Server Admin」の「共有」モジュールを使って以下の防止策をとってください。

- ボリューム全体ではなくフォルダを個別に共有します。フォルダには、共有したい項目だけを保存します。
- ゲストにアクセスさせたくないフォルダに対して、全員に「なし」のアクセス権を割り当てます。項目のアクセス権をこのように設定した場合、これらの項目にアクセスできるのは、項目のオーナーまたはグループだけです。
- ゲストが利用できるファイルはすべて、1 つのフォルダまたはフォルダのセットに保存します。そのフォルダおよび内部の各ファイルに対して全員の分類に「読み出し専用」のアクセス権を割り当てます。
- ゲストがフォルダの項目を変更したり追加したりする必要がある場合にのみ、そのフォルダに対して、全員の分類に「読み出し／書き込み」のアクセス権を割り当てます。このフォルダの中にある情報のバックアップコピーを保存していることを確認してください。また、このフォルダに変更や追加が行われたかどうか、頻繁に確認してください。さらに、ウイルス防止プログラムを使って、サーバがウイルスに感染していないかどうかも定期的に確認してください。
- フォルダに変更や追加が行われたかどうか、頻繁に確認してください。また、ウイルス防止プログラムを使って、サーバがウイルスに感染していないかどうかも定期的に確認してください。
- 「Server Admin」で「FTP」モジュールを使用して、anonymous FTP によるアクセスを禁止します。
- NFS ボリュームをワールドに書き出さないでください。エクスポートは、特定の範囲のコンピュータのみに制限してください。

登録ユーザにのみアクセスを許可する

ゲストがサーバにアクセスできないようにしたい場合は、各ファイルサービスでゲストアクセスが許可されていないことを確認します。サービスのモジュールで「ゲストアクセスを許可する」の隣にチェックマークが付いている場合は、ゲストアクセスが許可されています。チェックボックスをクリックしてチェックマークを外し、ゲストアクセスを禁止します。

Apple ファイルサービス

Apple ファイルサービスによって、Macintosh クライアントユーザはサーバに接続し、ユーザ自身のコンピュータ上にフォルダやファイルがあるかのように、これらにアクセスすることができます。「AppleShare IP 6.3」を熟知している方は、「Mac OS X Server」の Apple ファイルサービスが同じように機能することを理解できるでしょう。Apple ファイルサービスでは、Unicode ファイル名や 64 ビットのファイルサイズなどの新しい機能に対応している、AFP（Apple Filing Protocol）のバージョン 3.0 を使用しています。

ただし、新しい Apple ファイルサービスは、接続方法として AppleTalk をサポートしていない点が異なります。AppleTalk を使用するクライアントは、「セレクタ」を使ってネットワーク上のサーバを探すことはできますが、接続するときは TCP/IP を使用します。

Apple ファイルサービスは、Unicode ファイル名に対応しています。この規格では、言語や、言語を表示するために使用されるオペレーティングシステムにかかわらず、各文字に一意な数値が割り当てられます。

Apple ファイルサービスを設定する前に

「Mac OS X Server」の設定アシスタントで Apple ファイルサービスを開始すると、サーバは即座にネットワーク上で使用できるようになります。ただし、適切なアクセス権が設定された共有ポイントを作成し、権限を与えられたユーザを作成するまでは、どのユーザもサーバに接続することはできません。これらのトピックについて詳しくは、第 4 章「共有」および第 3 章「ユーザとグループ」を参照してください。

互換性のある AppleShare のバージョンを確認する

Apple ファイルサーバにアクセスするためには、クライアントコンピュータに、「AppleShare」のバージョン 3.7 以降がインストールされている必要があります。クライアントで使用されている Mac OS のバージョンをサポートする、「AppleShare」クライアントソフトウェアの最新バージョンは、アップル社のサポート用 Web サイト（www.apple.co.jp/support）で確認できます。

クライアントコンピュータで AppleTalk を使用可能にする

AppleTalk 経由で（「セレクタ」を使って）Apple ファイルサーバを検索するには、クライアントユーザが AppleTalk を使用できる必要があります。「Mac OS X」でこの操作を行うときは、「システム環境設定」を開いて、「ネットワーク」をクリックします。「Mac OS 9」以前では、「AppleTalk」コントロールパネルを使用します。

Apple ファイルサービスを初めて設定する

「Mac OS X Server」のインストール時に、設定アシスタントで Apple ファイルサービスを設定した場合は、Apple ファイルサービスを使うために追加の操作を行う必要はありません。ただし、デフォルトの設定が目的に合っているかどうかを確認してください。「Mac OS X Server」のインストール時に Apple ファイルサービスを設定しなかった場合は、ここで設定することができます。

手順 1：Apple ファイルサービスを設定する

「Server Admin」で「ファイルとプリント」タブをクリックしてから、「Apple」をクリックし、「Apple ファイルサービスを設定」を選びます。「Apple ファイルサービスの設定」ウインドウの 4 つのタブをそれぞれクリックして、必要な設定を行います。設定可能な内容について詳しくは、86 ページの「Apple ファイルサービスの設定」を参照してください。

手順 2：Apple ファイルサービスを開始する

「Apple」をクリックし、「Apple ファイルサービスを開始」を選びます。サービスが開始すると、サービスのアイコンに地球のマークが表示されます。

手順 3：共有ポイント、およびユーザとグループを作成する

サーバ上で利用できるようにしたい共有ポイント（共有フォルダとディスク）にアクセス権を設定する必要があります。情報にアクセスできるように設定したいユーザとグループにも、アクセス権を割り当てる必要があります。これらの作業を行う方法については、第 4 章「共有」および第 3 章「ユーザとグループ」を参照してください。

Apple ファイルサービスの設定

Apple ファイルサービスの設定にアクセスするには、「ファイルとプリント」タブをクリックしてから「Apple」をクリックし、メニューから「Apple ファイルサービスを設定」を選びます。4 つのタブをそれぞれクリックして、パネルの設定を表示します。以下のセクションでは、各パネルで使用できる設定について個別に説明します。

一般設定

サーバの識別情報の設定、自動起動の設定、およびログインメッセージの作成を行うときは、「一般」パネルを使用します。「一般」パネルにアクセスするには、「Apple」をクリックしてから「Apple ファイルサービスを設定」を選びます。

コンピュータ名

「セレクタ」または「ネットワークブラウザ」を使用するときにユーザに示したい名前を入力します。ここに入力する名前は、ネットワークに接続したすべてのコンピュータ間で一意でなければなりません。このフィールドを空白にしておくと、IP アドレスがサーバ名としてネットワークに登録され、このフィールドにはサーバの DNS 名が表示されます。

システム起動時に Apple ファイルサービスを開始する

電源が切れたり、その他の不測の事態が発生した後でサーバを再起動したときに、ファイルサービスを利用可能にする場合は、このオプションを選びます。通常は、このオプションを選択しておくことをお勧めします。

Network Service Locator に登録する

ユーザがこのサーバを、「Mac OS X」の「サーバへ接続」パネル、または「Mac OS 9」の「ネットワークブラウザ」で見ることができるようにしたい場合は、このオプションを選びます。このオプションは、「Mac OS 9」以降がインストールされたクライアントコンピュータで利用できます。

このオプションをオンにする場合は、ネットワークルータ上の IP マルチキャスティングも使用可能にする必要があります。SLP（Service Location Protocol）および IP マルチキャストについて詳しくは、第 12 章「ネットワークサービス」を参照してください。クライアントおよびルータの機能について詳しくは、265 ページを参照してください。

初期メッセージ

ユーザが接続したときに表示したいメッセージを入力します。

参考：ログインメッセージが表示されない場合は、ユーザのコンピュータのソフトウェアをアップグレードしてください。クライアントコンピュータは、「AppleShare Client」ソフトウェアのバージョン 3.7 以降を使用する必要があります。

同じユーザに同じメッセージを 2 回送らない

ログインメッセージを 1 回だけ表示する場合は、このオプションを選びます。メッセージを変更した場合は、ユーザが次回サーバに接続したときに、その新しいメッセージが表示されます。

アクセスの設定

クライアント接続およびゲストアクセスを設定するときは、「アクセス」パネルを使用します。「アクセス」パネルを表示するには、「Apple」をクリックして「Apple ファイルサービスを設定」を選び、「アクセス」タブをクリックします。

ゲストアクセスを許可する

未登録ユーザがファイルサーバにアクセスできるようにしたい場合は、このオプションを選びます。ゲストアクセスは、適切なアクセス権が設定されたファイルやその他の項目に、ユーザが一時的にアクセスできるようにするときに便利な方法です。

クライアントの最大接続数（ゲストを含む）

サーバに同時に接続できるユーザ数を制限したくない場合は、「無制限」を選びます。サーバでたくさんのサービスを提供している場合は、クライアント接続の数を制限することでサーバの性能を向上させることができます。この操作を行うときは、「無制限」の下のボタンをクリックし、制限値として設定したい接続数を入力します。

ゲストの最大接続数

ゲストアクセスを許可していて、サーバに同時に接続できるゲストユーザ数を制限したくない場合は、「無制限」を選びます。最大クライアント接続数のうち、ゲストが使用できる数を指定したい場合は、「無制限」の下のボタンをクリックし、許可したい接続数を入力します。

AppleTalk を使用するブラウズをクライアントに許可する

クライアントユーザが「セレクタ」を使ってファイルサーバを検索できるようにしたい場合は、このオプションを選びます。「セレクタ」を使ったサーバ検索を可能にするには、クライアントコンピュータとサーバの両方で AppleTalk を使用可能にする必要があります。

古いクライアント用にエンコードする

クライアントユーザが使用している文字セットと一致する文字セットをサーバ用に選びます。「Mac OS 9」以前のクライアントが接続すると、サーバは、ファイル名をシステムの UTF-8 から指定された文字セットに変換します。

ログの設定

Apple ファイルサービスのログを設定および管理するときは、「ログ」パネルを使用します。「ログ」パネルを表示するには、「Apple」をクリックして「Apple ファイルサービスを設定」を選び、「ログ」タブをクリックします。

アクセスログを許可する

アクセスログを作成したい場合は、このオプションを選びます。アクセスログには、指定したイベントに関する情報が保存されます。ログファイルのサイズは、使用可能なディスク容量によってのみ制限されます。もちろん、指定するイベントの数が多くなるほど、ログファイルは大きくなります。記録するイベントを選ぶときは、サーバのディスク容量も考慮してください。

_ 日ごとにアーカイブを作成する

ログファイルの内容をアーカイブに保存する頻度を指定したい場合は、このオプションを選びます。指定した日数を経過すると、サーバはログファイルを閉じ、現在の日付を含む名前に変更して、新しいログファイルを開きます。アーカイブに保存されたログは、記録のために保存することができます。または、不要になったら削除して、ディスク領域を開放することもできます。デフォルトの設定は 7 日間です。

アクセスログに含めるイベントを選択する

Apple ファイルサービスで記録したいイベントを選びます。ここで指定した操作をユーザが実行するたびに、項目が記録されます。

エラーログ：_ 日ごとにアーカイブを作成する

エラーログファイルの内容をアーカイブに保存する頻度を指定したい場合は、このオプションを選びます。指定した日数を経過すると、サーバはログファイルを閉じ、現在の日付を含む名前に変更して、新しいログファイルを開きます。アーカイブに保存されたログは、記録のために保存することができます。または、不要になったら削除して、ディスク領域を開放することもできます。デフォルトの設定は 7 日間です。

アイドル状態のユーザの設定

アイドル状態のユーザの設定を構成および管理するときは、「アイドル状態のユーザ」パネルを使用します。「アイドル状態のユーザ」とは、サーバに接続しているが、サーバのボリュームを一定時間使用しなかったユーザのことです。「アイドル状態のユーザ」パネルを表示するときは、「Apple」をクリックして「Apple ファイルサービスを設定」を選んでから、「アイドル状態のユーザ」タブをクリックします。

クライアントに _ 時間スリープを許可する。(この間アイドル状態として表示されません。)

スリープモードにあるクライアントコンピュータの接続をサーバが解除しないようにする場合は、このオプションを選びます。スリープとは、クライアントコンピュータがほとんど電力を消費しない状態のことです。「省エネルギー」ソフトウェアがインストールされたコンピュータでは、ユーザは一定時間使用されなかったコンピュータをスリープするように設定できます。

接続解除するまでのアイドル時間

一定時間の経過後に、アイドル状態のユーザの接続を解除したい場合は、このオプションを選びます。こうすることで、現在のユーザがサーバリソースを利用できるようになります。さらに、権限のないユーザが、だれも使用していないコンピュータを使ってネットワーク上の情報にアクセスすることを防止できる場合があります。

除くユーザ

接続を解除しないユーザを選択します。

- ゲスト
- 登録ユーザ（管理者やゲストではない任意のユーザ）
- 管理者
- ファイルを開いているアイドル状態のユーザ

重要　最後のオプションを選ばなかった場合は、ファイルを開いているすべてのアイドル状態のユーザ（ゲスト、登録ユーザ、または管理者）が接続を解除され、保存していない変更内容を失います。

解除を知らせるメッセージ

ユーザが接続を解除されたときに表示したいメッセージを入力します。メッセージを入力しなかった場合は、接続が一定時間アイドル状態だったために接続が解除されたことを通知する、デフォルトのメッセージが表示されます。

すべてのクライアントコンピュータが接続解除のメッセージを表示できるわけではありません。

Apple ファイルサービスに関する問題を解決する

ユーザがファイルサーバを見つけることができない場合：

- ユーザのコンピュータと、Apple ファイルサービスを実行しているコンピュータで、ネットワークが正しく設定されていることを確認します。ユーザのコンピュータからほかのネットワークリソースに接続できない場合は、ネットワーク接続が機能していない可能性があります。
- ファイルサーバが動作中であることを確認します。サーバが動作中かどうかを調べるときは、「PING」ユーティリティを使用できます。
- ユーザが AppleTalk を介して（「セレクタ」で）サーバを検索している場合は、「Apple ファイルサービスの設定」ウインドウの「アクセス」パネルで AppleTalk を介したブラウズが使用可能になっているかどうかを確認し、AppleTalk がサーバとユーザのコンピュータの両方で動作中であることを確認します。
- ファイルサーバに割り当てられている名前をチェックして、ユーザが見ている名前が正しい名前かどうか確認します。

ユーザがファイルサーバに接続できない場合：

- ユーザが正しい名前とパスワードを入力していることを確認します。ユーザ名の大文字と小文字は区別されませんが、パスワードは大文字と小文字が区別されます。
- 「Server Admin」の「ユーザとグループ」モジュールで、そのユーザのログインが有効になっていることを確認します。
- 「Appleファイルサービスの状況」ウインドウでクライアント接続が最大数に達したかどうかを確認します。最大数に達している場合、ほかのユーザは後で接続を試みる必要があります。
- ユーザとグループを管理するサーバが動作中であることを確認します。
- ユーザのコンピュータに「AppleShare 3.7」以降がインストールされているかどうかを確認します。
- ユーザが遠隔地からサーバに接続しようとしている場合は、IPフィルタサービスの設定で 548 番のポートへのアクセスが許可されていることを確認します。IP フィルタリングについて詳しくは、285 ページの「IP フィルタサービス」を参照してください。

Apple ファイルサービスの仕様

使用許諾契約に応じた最大接続ユーザ数	無制限（ハードウェアに依存）
最大ボリュームサイズ	2 テラバイト
TCP ポート番号	548
ログファイルの場所	/Library/Logs（「AppleFileService」フォルダの中にあります）

Windows サービス

「Mac OS X Server」の Windows サービスは、Windows クライアントに 4 つのサービスを提供します。追加のソフトウェアは必要ありません。各サービスは、次のとおりです。

- ファイルサービスによって、Windows クライアントは、TCP/IP 経由で SMB（Server Message Block）プロトコルを使って、「Mac OS X Server」に接続できます。
- プリントサービスによって、Windows クライアントは、ネットワーク上の PostScript プリンタを使ってプリントできます。プリントサービスも SMB を使用しています。
- WINS（Windows Internet Naming Service）によって、ユーザは、複数のサブネット間で名前とアドレスの解決を行うことができます。
- ブラウズによって、クライアントは利用可能なサーバを複数のサブネット間でブラウズすることができます。

Windows サービスは、Unicode（すべての文字表現に 16 ビット識別子を使用する標準規格）を使ってクライアントに適した言語を表示します。古いクライアントコンピュータは Unicode を使用していないため、Windows サービスは、Samba コードページに対応しています。このコードページは、ネイティブ Unicode からユーザが指定した言語への変換を行います。

Windows サービスを設定する前に

「Mac OS X Server」で Windows サービスを提供する場合は、以下のセクションを参照して、考慮すべき点について確認してください。また、お使いの「Windows」のバージョンに関する Microsoft 社のマニュアルも確認して、クライアントソフトウェアの機能について詳しく調べてください。

Windows クライアントをサポートするための要件

Windows クライアントをサポートするために必要なのは、「Mac OS X Server」ソフトウェアだけです。アップル社の従来のサーバ製品とは異なり、「Mac OS X Server」には、Windows クライアントコンピュータ用に組み込みのブラウズサービスおよび名前解決サービスが付属しています。お使いのサーバで WINS を使用するか、または既存の WINS サーバに登録できます。

また、「Mac OS X Server」の Windows サービスは、Windows マスターブラウザサービスおよびドメインマスターブラウザサービスも提供します。つまり、Windows コンピュータの「ネットワークコンピュータ」ウインドウにサーバを表示するために、ネットワーク上に Windows サーバやプライマリドメインコントローラを置く必要はありません 。また、Windows クライアントは、サーバのサブネット以外のサブネットにあってもかまいません。

最適なクロスプラットフォームの環境を整える

「Mac OS」と「Windows」のコンピュータでは、ファイルの保存と管理の方法が異なります。最適なクロスプラットフォームの環境を整えるためには、Windows ユーザだけが使用する共有ポイントを少なくとも 1 つ設定する必要があります。さらに、以下のガイドラインに従うことによって、ユーザの環境を改善することができます。

- 両方のプラットフォームで、適合するバージョンのアプリケーションソフトウェアを使用します。
- ファイルを変更するときは、作成元のアプリケーションだけを使用します。

- ファイル名は半角英数文字で 31 文字以内にします。
- アクセント記号の付いた記号や文字を共有項目の名前に使用しないでください。

Windows のユーザパスワードの確認

「Mac OS X Server」は、Windows のユーザパスワードを照合する 2 つの方法を提供します。

- 暗号化パスワードによる照合。最も安全であり、Windows コンピュータがローカルネットワーク（LAN）上でサポートしているデフォルトの技術であるため、これが望ましい方法です。この方法では、暗号化されたパスワードが Windows コンピュータと「Mac OS X Server」間で送信されます。

  暗号化パスワードによる照合を使用するときは、NetInfo 階層構造内のすべてのドメインで「Authentication Manager」を使用可能にし、ドメインごとに暗号化キーを定義します。「Authentication Manager」が使用可能なときは、NetInfo のユーザレコードに「tim_passwd」プロパティが保存されます。このプロパティは、暗号化キーを使ってクリアーテキストパスワードを入手するときに、復号化されます。暗号化キーは、ルートだけが読み出すことができる、サーバ上のファイルに保存されています。

- クリアーテキストパスワードによる照合。この方法は、重要度の低いユーザ認証情報だけに使用してください。クリアーテキストパスワードによる照合を使用するときは、Windows コンピュータを個別に設定する必要があります。クリアーテキストパスワードによる照合の設定方法については、Windowsのマニュアルを参照してください。

  クリアーテキストパスワードによる照合を使用すると、パスワードは復元できない形式で保管されます。NetInfo パスワードの値が「passwd」プロパティに関連付けられている場合、一方向ハッシュが使用されるため、簡単には解読できません。一方向ハッシュは、同じパスワードに対して使用すると、結果は常に同じになります。

暗号化パスワードによる照合を設定するには、階層構造内のすべての Mac OS X コンピュータ上で「Authentication Manager」を使用可能にします。「Authentication Manager」の設定について詳しくは、「NetInfo 活用ガイド」（www.apple.co.jp/macosxserver/ にあります）を参照してください。

Windows サービスを初めて設定する

Windows サービスは、開始するだけで設定できます。ほとんどの場合は、デフォルトの設定で正しく動作しますが、設定を確認して、自分のネットワークに合わない設定は変更してください。設定できる内容の説明については、次の「Windows サービスの設定」を参照してください。

Windows サービスを初めて設定するときは、次の手順に従って行います。これらの手順について詳しい説明が必要な場合はオンスクリーンヘルプを参照してください。

手順 1：Windows サービスを設定する

Windows サービスにアクセスするには、「ファイルとプリント」タブをクリックしてから「Windows」をクリックし、「Windows サービスを設定」を選びます。「Windows サービスの設定」ウインドウの 4 つのタブをそれぞれクリックして設定を確認し、必要に応じて変更を行います。使用可能な設定の説明については、次のセクション「Windows サービスの設定」を参照してください。

手順 2：Windows サービスを開始する

動作中でない場合は、「Windows サービスを開始」を選びます。サービスが開始すると、サービスのアイコンに地球のマークが表示されます。

手順 3：クライアントの設定を確認する

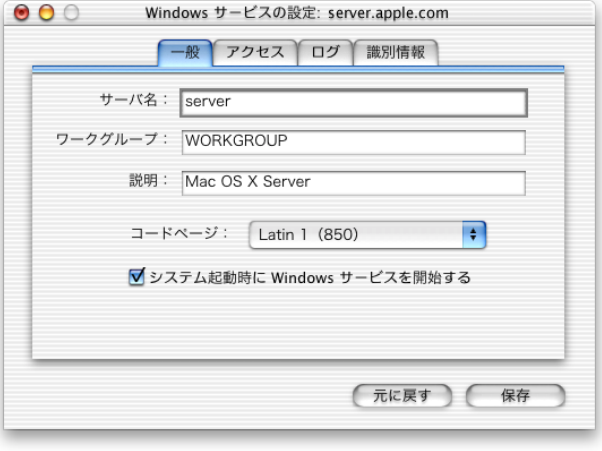
Windows サービスを設定したら、Windows クライアントコンピュータが TCP/IP 経由で接続するように適切に設定されているかどうかを確認してください。この設定について詳しい情報が必要な場合は、「Windows」のネットワークに関するマニュアルを参照してください。

Windows サービスの設定

Windows サービスにアクセスするには、「ファイルとプリント」タブをクリックしてから「Windows」をクリックし、「Windows サービスを設定」を選びます。4 つのタブをそれぞれクリックして、パネルの設定を表示します。以下のセクションでは、各パネルで使用できる設定について個別に説明します。

一般設定

Windows サーバの識別情報の設定、および自動起動の設定を行うときは、「一般」パネルを使用します。「一般」パネルにアクセスするには、「Windows」をクリックしてから「Windows サービスを設定」を選びます。



サーバ名

ユーザが接続したときに表示するサーバ名を入力します。デフォルトの名前は、Windows ファイルサーバの NetBIOS 名です。名前は半角英数文字で 15 文字以内にしてください。特殊文字や、コンマ、ピリオドを含めることはできません。

実際には、サーバ名とその省略した DNS ホスト名を一致させます。たとえば、サーバのエントリが「server.apple.com」として DNS サーバに登録されている場合、サーバの名前を「server」とします。

ワークグループ

「ネットワークコンピュータ」ウインドウに表示したいワークグループの名前を入力します。サブネットにWindowsのドメインがある場合は、そのドメインの1つをワークグループの名前として使って、クライアントがサブネット間でアクセスしやすくします。ドメインがない場合は、正しいグループ名をWindowsネットワーク管理者に問い合わせてください。ワークグループ名は、半角英数文字で15文字以内にする必要があります。

説明

自分やユーザにとって役立つ説明を半角英数文字で43文字以内で入力します。この説明はクライアントコンピュータの「ネットワークコンピュータ」ウインドウに表示されます。省略することもできます。

コードページ

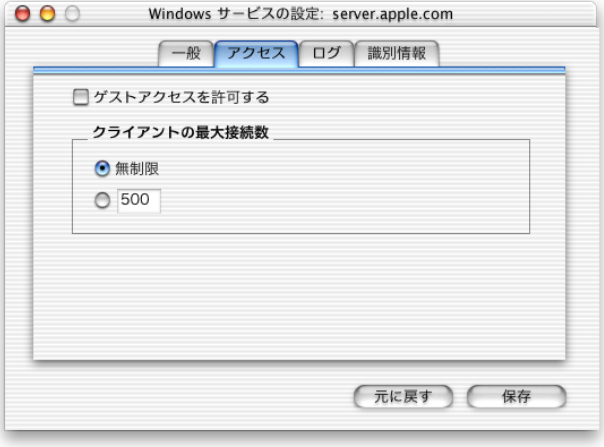
クライアントコンピュータが使用する言語のコードページを選びます。

システム起動時にWindowsサービスを開始する

電源が切れたり、その他の不測の事態が発生した後でファイルサーバを再起動したい場合は、このオプションを選びます。通常は、このオプションを選ぶことをお勧めします。

アクセスの設定

ゲストアクセスを許可し、最大クライアント接続数を設定するときは、「アクセス」パネルを使用します。「アクセス」パネルにアクセスするには、「Windows」をクリックしてから「Windowsサービスを設定」を選び、「アクセス」タブをクリックします。



ゲストアクセスを許可する

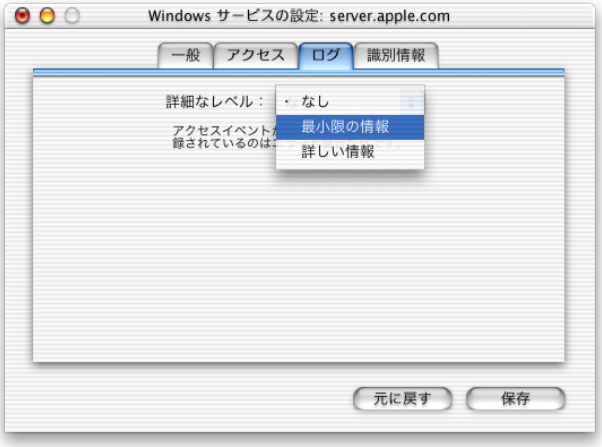
未登録ユーザが Windows ファイル共有を使用できるようにする場合にのみ、このオプションを選びます。これは、適切なアクセス権が設定されたファイルやその他の項目に、ユーザが一時的にアクセスできるようにするときに便利な方法です。

クライアントの最大接続数

許可したい最大同時接続数を入力します。この数は、所有するソフトウェアのライセンスによって制限されます。サーバでたくさんのサービスを提供している場合は、最大接続数を、サーバで許可されているライセンスよりも小さい値に設定することで、サーバの性能を向上させることができます。

ログの設定

ログの詳細のレベルを選ぶときは、「ログ」パネルを使用します。「ログ」パネルにアクセスするには、「Windows」をクリックしてから「Windows サービスを設定」を選び、「ログ」タブをクリックします。



詳細なレベル

記録したい詳細レベルを選びます。記録が詳細になればなるほど、ログファイルは大きくなります。下の表は、それぞれのオプションに対する詳細のレベルを示しています。

記録されるイベント	なし	最小限の情報	詳しい情報
サーバの開始と停止	なし	あり	あり
ユーザのログインの失敗	なし	あり	あり
警告とエラー	あり	あり	あり
ブラウザ名登録のイベント	なし	あり	あり
アクセスイベント（ファイルが開かれたり、変更されたり、読み込まれたりするごと）	なし	なし	あり

識別情報の設定

名前解決を設定して、サブネット間のブラウズを許可するときは、「識別情報」パネルを使用します。「識別情報」パネルにアクセスするときは、「Windows」をクリックして「Windows サービスを設定」を選び、「識別情報」タブをクリックします。

WINS

WINS サーバに登録したいかどうかを選びます。ローカルまたは外部のサーバを選ぶことができます。次の選択肢があります。

- 「切」: サーバは、外部の WINS サーバまたはローカルの名前解決サーバのどちらにも登録しません。
- 「WINS サーバを使用する」: ファイルサーバが、ローカルの名前解決サービスを提供します。これによって、ユーザは、複数のサブネット間で名前とアドレスの解決を行うことができます。
- 「WINS サーバに登録する」: Windows クライアントと Windows サーバがすべて同じサブネット上にないときに、ネットワーク上に WINS サーバがある場合は、この設定を選びます。次に、WINS サーバの IP アドレスまたは DNS 名を入力します。

ワークグループ／ドメイン

マスターブラウザまたはドメインマスターブラウザによるドメインブラウズサービスを使用するかどうかを選びます。次の選択肢があります。

- 「マスターブラウザ」: 1 つのサブネット内でサーバをブラウズおよび検索することができます。
- 「ドメインマスターブラウザ」: 複数のサブネット間でサーバをブラウズおよび検索することができます。

Windows サービスに関する問題を解決する

ユーザのコンピュータで、「ネットワークコンピュータ」に Windows サーバが表示されない場合は、以下のことを確認してください。

- ユーザのコンピュータで TCP/IP が正しく設定されていることと、適切な Windows ネットワークソフトウェアがインストールされていることを確かめます。
- Windows ユーザのゲストアクセスを許可します。
- クライアントコンピュータの「DOS プロンプト」で、「ping [IP アドレス]」と入力します。ここで「IP アドレス」は、自分サーバのアドレスです。PING に失敗した場合、TCP/IP に問題があります。
- ユーザのコンピュータがサーバとは別のサブネット上にある場合は、ネットワーク上に WINS サーバがある必要があります。

参考：Windows コンピュータのネットワーク機能が正しく設定され、ネットワークに正しく接続されていれば、「ネットワークコンピュータ」ウインドウにサーバのアイコンが表示されていない場合でも、クライアントユーザはファイルサーバに接続することができます。詳しくは、「Server Admin ヘルプ」の「ネットワークの識別情報を使用して Windows サーバに接続する」を参照してください。

Windows ユーザがログインできない場合：

- ユーザのレコードがある NetInfo ドメインと、NetInfo 階層構造のほかのすべての NetInfo ドメインに対して「Authentication Manager」が使用可能であることを確認します。
- ユーザのパスワードを設定し直して、もう一度実行してみます。
- クリアーテキストパスワード確認を使用した Windows ユーザの認証を有効にします。

Windows サービスの仕様

使用許諾契約に応じた最大接続ユーザ数	1000
最大ボリュームサイズ	2 テラバイト
TCP ポート番号	139
UDP ポート番号	137、138
ログファイルの場所	/Library/Logs（「WindowsFileServices」フォルダの中にあります）

NFS（Network File System）サービス

Apple ファイルサービス、Windows ファイル共有、および FTP サービスは、ユーザ名とパスワードに基づいてユーザの共有項目への接続を許可します。NFS の場合は異なり、コンピュータの IP アドレスに基づいて、情報にアクセスできるかどうかを判断します。つまり、だれが使用しているかにかかわらず、特定のクライアントコンピュータから特定の共有ポイントにアクセスすることができます。そのコンピュータを起動すれば、いくつかのボリュームまたはフォルダが自動的にマウントされ（または利用可能になり）、コンピュータを使用する任意のユーザがそれらのボリュームまたはフォルダにアクセスすることができます。

NFS では、項目を「共有」するのではなく、「エクスポート」します。エクスポートは、共有ポイントを特定の場所に公開することと似ています。NFS サービスを設定および管理するときは、「Server Admin」の「NFS」モジュールを使用します。エクスポートしたい共有ポイントまたはフォルダのアクセス権およびアクセスレベルを設定するときは、「Server Admin」の「共有」モジュールも使用します。

NFS サービスを使用する状況

NFS は、「Mac OS X Server」のほかのファイルサービスとは異なり、高精度なアクセスレベル設定を提供しません。共有項目は、クライアントコンピュータの 1 つのセット、または「ワールド」にエクスポートすることができます。NFS ボリュームをワールドにエクスポートするということは、サーバにアクセスできるユーザ（anonymous FTP ユーザを含む）はだれでも、そのボリュームにもアクセスできるようになるので注意が必要です。

信頼できるクライアントコンピュータがあるローカルエリアネットワーク（LAN）を使用している場合、または Apple ファイル共有や Windows ファイル共有を使用できない環境で操作している場合にのみ、NFS サービスを使用することをお勧めします。インターネットにアクセスでき、「ワールド」にエクスポートする場合は、サーバにファイアウォールが必要です。

NFS サービスを設定する前に

NFS でエクスポートする場合は、セキュリティの問題について考慮する必要があります。NFS はセキュリティで保護されたネットワーク環境用に作られたものであり、クライアントコンピュータとクライアントを管理するユーザを信用しています。

NFS では、ユーザが別のユーザのファイルの所有権を獲得することができます。たとえば、ユーザ ID が 1234 のユーザが所有するファイルがサーバ上にあり、そのファイルが含まれるフォルダをエクスポートしたとします。リモートコンピュータのユーザは、そのコンピュータ上でローカルユーザを作成して、1234 というユーザ ID を割り当てることができます。このユーザは、そのフォルダをマウントすることができ、ファイルの元のオーナーと同じアクセス権を持つことになります。

一意なユーザ ID を作成し、ユーザ情報を保護することによって、このような状況を防止することができます。

NFS を初めて設定する

手順 1：NFS サービスを設定する

「Server Admin」で「ファイルとプリント」タブをクリックし、「NFS」をクリックしてから「NFS を設定」を選びます。同時に許可するデーモン（クライアントの要求を扱うサーバプロセス）の最大数を設定し、クライアントにデータを送信するために TCP を使うか、UDP を使うかを選びます。これらのオプションについて詳しくは、「NFS サービスの設定」を参照してください。

手順 2：フォルダをエクスポートし、NFS サービスを起動する

NFS を初めて設定するときは、少なくとも 1 つのフォルダを共有する必要があります。これを実行するには、「Server Admin」の「一般」タブをクリックし、「共有」をクリックしてから「アクセス権を設定」を選びます。共有するフォルダを選び、「選択」をクリックします。ポップアップメニューから「一般」、「自動マウント」、および「NFS アクセス制御」を選んで、希望する設定を行います。設定できるオプションについては、102 ページの「NFS アクセス制御の設定」を参照してください。

NFS サービスを開始または停止する必要はありません。エクスポートする共有ポイントを定義すると、サービスは自動的に開始します。すべてのエクスポートを削除すると、サービスは停止します。「Server Admin」の「NFS」アイコンに地球のマークがあるかどうかを見ることで、NFS サービスが実行中かどうかを知ることができます。

NFS サービスの設定

NFS サービスは、「NFS を設定」ウインドウを使って設定します。このウインドウにアクセスするときは、「ファイルとプリント」タブをクリックしてから、「NFS」をクリックし、「NFS を設定」を選びます。

サーバのデーモン数

同時に許可したい nfsd デーモンの最大数を入力します。nfsd デーモンとは、バックグラウンドで継続的に実行されるサーバプロセスで、マウントされた共有ポイントに対する読み出しと書き込みを処理します。利用可能なデーモンの数が多くなるほど、同時に処理できるクライアントの数は多くなります。「Mac OS X Server」の場合は、サーバ上のデーモンの最大数を 4 ～ 6 の範囲に設定します。

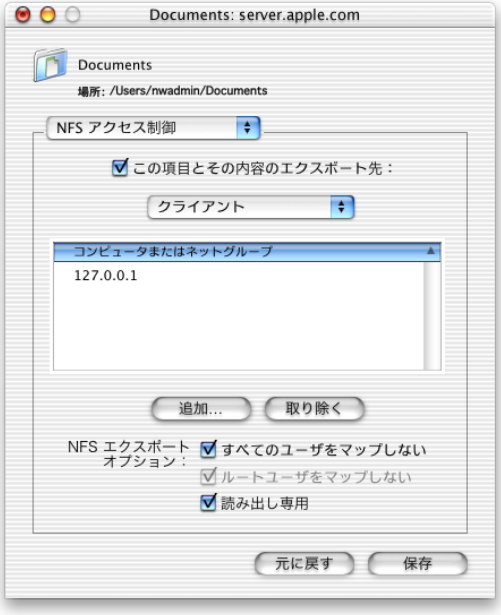
サービスの経由先

クライアントコンピュータにデータを提供する方法を選びます。

- 「tcp」： TCP（Transmission Control Protocol）は、データをパケット（IP を使ってネットワーク経由で送信されるデータの小さな集まり）に分割し、エラー訂正を使って情報が正しく転送されたかどうかを確認します。
- 「udp」： UDP（User Datagram Protocol）はデータをパケットに分割しないので、システムリソースの消費が少なくなります。TCP よりも拡張性が高いので、負荷の高いサーバに適しています。
- 「tcp と udp」： 特定のパフォーマンス上の問題がない限り、TCP と UDP の両方を選択してください。TCP はクライアントのパフォーマンスを向上させ、UDP はサーバにかかる負荷を少なくします。

NFS アクセス制御の設定

「NFS アクセス制御」パネルを使って、エクスポートの作成およびアクセス権の設定を行います。「NFS アクセス制御」パネルを表示するには、「Server Admin」の「一般」タブをクリックします。「共有」をクリックして、「ディスクと共有ポイントを表示」を選びます。共有項目を選択して「アクセス権」をクリックしてから、共有項目名の下にあるポップアップメニューから「NFS アクセス制御」を選びます。



この項目とその内容のエクスポート先

項目をエクスポートしてユーザが利用できるようにするときは、このオプションを選びます。この情報を利用可能にするユーザを選びます。ポップアップメニューから、または「クライアント」「ワールド」を選べます。「ワールド」へのエクスポートを選んだ場合、セキュリティが危険にさらされる可能性があります。

デフォルト設定では、NFS はクライアントアドレス 127.0.0.1（サーバコンピュータへのループバック）にエクスポートされます。これにより、不注意でフォルダを「ワールド」にエクスポートしてしまうことを防げます。

「追加」と「取り除く」

「追加」をクリックして、このエクスポートを受信可能なクライアントを指定します。表示されたテキストボックスに、IP アドレスまたはホスト名を入力して、「コンピュータまたはネットグループ」リストに追加します。リストから IP アドレスを選んで「取り除く」をクリックして、エクスポートのリストからクライアントを削除します。

NFS エクスポートオプション

「ルートユーザをマップしない」： リモートクライアントシステムで「ルート」として識別されるユーザに、最小限の読み出し、書き込み、コマンド実行権限を与える場合、このオプションを選びます。

「すべてのユーザをマップしない」： すべてのユーザに、最小限の読み出し、書き込み、コマンド実行権限を与える場合、このオプションを選びます。

「読み出し専用」： 共有項目の内容変更をいかなる方法によってもクライアントユーザに許可しない場合、このオプションを選びます。これにより、共有項目に設定されたほかのすべての権限は上書きされます。たとえば、「全員」の分類に Apple ファイルサービスの項目の読み出し／書き込み権限を許可しているとき、この項目を「読み出し専用」権限を持つ「ワールド」への NFS エクスポートとして定義することもできます。

FTP（File Transfer Protocol）サービス

FTP によって、コンピュータは、インターネット上でファイルを転送できます。FTP に対応したオペレーティングシステムを使用しているクライアントであれば、設定したアクセス権に応じて、ファイルサーバに接続してファイルをダウンロードできます。ほとんどのインターネットブラウザおよび多数のフリーウェアアプリケーションを使って、FTP サーバにアクセスできます。

FTP サービスを設定する前に

FTP サービスを提供するかどうかを判断するときは、共有する必要がある情報のタイプとクライアントについて考慮しなければなりません。FTP は、アプリケーションやデータベースなど、サイズの大きいファイルを転送する場合に適しています。さらに、ゲスト（anonymous）ユーザがファイルをダウンロードできるようにしたい場合にも、FTP を使って安全にこのサービスを提供することができます。

anonymous FTP ユーザ（ゲスト）の制限

anonymous FTP を使用可能にすると、未知のユーザにサーバを公開することになるため、サーバをセキュリティ上の危険にさらすことになります。サーバのファイルおよびフォルダに設定するアクセス権は、情報のセキュリティを保つ上で最も重要です。

anonymous FTP ユーザには、「uploads」という共有ポイントにファイルをアップロードすることだけが許可されます。共有ポイント「uploads」が存在しない場合、anonymous ユーザはファイルを一切アップロードすることができません。

FTP サーバのセキュリティを保護するために、デフォルトの設定では、anonymous ユーザは次の操作を行うことができません。

- ファイルを削除する
- ファイルの名前を変更する
- ファイルを上書きする
- ファイルのアクセス権を変更する

FTP サービスを初めて設定する

手順 1：共有ポイントを作成する

FTP を介して利用可能にしたい共有ポイントを設定するときは、「Server Admin」の「共有」モジュールを使用します。共有ポイントの作成方法については、76 ページの「共有を初めて設定する」を参照してください。

手順 2：FTP サービスを設定する

FTP サービスのほとんどの設定は、サービスの開始時にバックグラウンドで行われます。ただし、ゲストアクセスの許可や、同時にログインできるゲストおよび登録ユーザの最大数の設定など、いくつかの設定を変更できます。

FTP サービスの設定にアクセスするときは、「Server Admin」で「ファイルとプリント」タブをクリックしてから、「FTP」をクリックし、「FTP を設定」を選びます。使用可能な設定の説明については、次のセクション「FTP サービスの設定」を参照してください。

手順 3：FTP サービスを開始する

「FTP」をクリックしてから、「FTP サービスを開始」を選びます。サービスが開始すると、サービスのアイコンに地球のマークが表示されます。

手順 4：anonymous FTP サービスを設定する（省略できます）

ゲストアクセスを許可した場合、anonymous ユーザは「ftp」または「anonymous」というユーザ名を使ってログインできます。anonymous ユーザは、ログインするためのパスワードは必要ありませんが、メールアドレスを入力するように促されます。

ゲストアクセスを許可するときは、「FTP」をクリックしてから、「FTP を設定」を選びます。次に、「anonymous（匿名）でのアクセスを有効にする」を選びます。

ゲストユーザにファイルのアップロードを許可する場合、「uploads」という名前のフォルダを作成し、「Server Admin」の「共有」モジュールを使って適切なアクセス権限を割り当てます。

FTP サービスの設定

FTP サービスの設定にアクセスするときは、「Server Admin」で「FTP」をクリックし、「FTP を設定」を選びます。

最大数 _ の実際のユーザを許可

このフィールドに値を入力して、同時にサーバに接続できる登録ユーザの最大数を設定します。実際のユーザとは、「Server Admin」の「ユーザとグループ」モジュールで追加されたユーザのことです。

anonymous（匿名）でのアクセスを有効にする

anonymous ユーザがサーバに接続してファイルを転送できるようにする場合は、このチェックボックスにチェックマークを付けます。共有ポイントに割り当てられたアクセス権をよく調べて、セキュリティホールがないことを確認します。情報のセキュリティの保護について詳しくは、第 4 章「共有」を参照してください。

最大数 _ の anonymous（匿名）のユーザを許可

このフィールドに値を入力して、同時にサーバに接続できる anonymous ユーザの最大数を設定します。

FTP サービスに関する上手な使いかたとヒント

ユーザにメッセージを表示する

「Mac OS X Server」の FTP サービスを使用すると、実際のユーザおよび anonymous FTP ユーザがサーバにログインしたときに、それらのユーザに送信する特定のメッセージを作成できます。FTP クライアントによっては、メッセージが分かりにくい場所に表示されたり、まったく表示されなかったりする場合があります。たとえば、FTP クライアントの「Fetch」では、バナーメッセージが「RemoteHostname Messages」ウインドウに表示されます。

バナーメッセージ

ユーザが最初に FTP サーバへの接続を試みると、ログインプロンプトの表示前にメッセージが表示されます。このメッセージは、「TextEdit」などのテキストエディタを使って変更できます。次のディレクトリ内の「banner.txt」というファイルを検索してください。

/Library/FTPServer/Messages/banner.txt

ウェルカムメッセージ

FTP サーバへのログインに成功すると、ウェルカムメッセージが表示されます。このメッセージは、「TextEdit」などのテキストエディタを使って変更できます。次のディレクトリ内の「welcome.txt」というファイルを検索してください。

/Library/FTPServer/Messages/welcome.txt

メッセージ

ユーザが「message.txt」という名前のファイルを含むディレクトリに移動すると、このファイルの内容がメッセージとして表示されます。このメッセージが表示されるのは、FTP セッションの間、ユーザがこのディレクトリに最初に接続したときだけです。このメッセージを使って、重要事項や注意する必要がある変更などをユーザに通知できます。

README メッセージ

「README」という名前のファイルをディレクトリに置くこともできます。ユーザが「README」ファイルを含むディレクトリに移動すると、このファイルが存在すること、およびこのファイルの最終更新日時を通知するメッセージが表示されます。ユーザは、そのファイルを開いて読むかどうかを選ぶことができます。

FTP サービスの内側

「Mac OS X Server」の FTP サービスは、「wu-FTPd」として知られる、ワシントン大学の FTP サーバのソースコードに基づいています。ただし、ユーザの環境を改善するために、元のソースコードにいくつかの変更が加えられています。これらの違いの一部について、このセクションで説明します。

セキュリティで保護された FTP 環境

ほとんどの FTP サーバは、制限されたディレクトリ環境を提供して、FTP ユーザがサーバ内の特定の領域のみを利用できるようにします。ユーザに表示されるのはこの領域内のボリュームだけであるため、サーバのセキュリティが十分に確保されます。ただし、ユーザが、この限定された領域外でマウントされたボリュームにアクセスすることはできません。シンボリックリンクやエイリアスを使って、サーバ内に設定された境界を越えることはできません。

「Mac OS X Server」の FTP サービスでは、セキュリティの確保された FTP 環境を確保しつつ、新たな方法が採用されています。FTP ユーザは、ボリュームに設定されたアクセス権が許す限り、サーバ上の任意の場所にマウントされたボリュームにアクセスできます。FTP ユーザは、「Server Admin」の「共有」モジュールで設定した任意の共有ポイントを見ることができます。データのセキュリティを制御するためには、共有ポイントに対して適切なアクセス権を設定します。共有ポイントの作成について詳しくは、第 4 章「共有」を参照してください。

実際のユーザのホームディレクトリ

標準の FTP サーバは、実際のユーザ（登録されたユーザ名とパスワードを使ってログインするユーザ）が信頼でき、サーバに対するすべてのアクセス権を持たせるに値することを想定しています。現在では、管理者の知らない登録ユーザが何千も存在するため、インターネットの初期に採用されていたこの方法はもはや有効な方法ではなくなっています。一方、「Mac OS X Server」の FTP サービスでは、実際のおよび anonymous ユーザを常に制限された FTP 環境に配置します。ただし、実際のユーザのホームディレクトリが制限された環境の中で利用可能な場合は、実際のユーザをそのディレクトリに接続します。たとえば、ユーザのホームディレクトリが共有ポイントの中にあり、アクセス権によってユーザが自分のホームディレクトリにアクセスできる場合、ユーザはログイン後にホームディレクトリに移動します。

重要なのは、実際のユーザと anonymous ユーザの両方が、共有ポイント内のホームディレクトリを表示できる点です。ただし、適切なアクセス権が設定されていない限り、どちらのユーザもこれらのディレクトリにアクセスすることはできません。

重要　ホームディレクトリを持たない、またはホームディレクトリがアクセス権を持つ共有ポイント内にない実際のユーザは、制限された FTP 環境のルートレベルに配置されます。

自動ファイル変換

「Mac OS X Server」の FTP サービスでは、ユーザは、圧縮または圧縮解除されたサーバ上の情報を要求できます。「.z」や「.gz」などのファイル名の拡張子は、ファイルが圧縮されていることを示します。ユーザが「Hamlet.txt」という名前のファイルを要求したときに、サーバに「Hamlet.txt.Z」という名前のファイルだけがある場合、ユーザが圧縮解除されたバージョンを要求していることが分かるので、サーバはファイルを圧縮解除されたフォーマットで提供します。

標準のファイル圧縮フォーマットに加え、「Mac OS X Server」は HFS または非 HFS ボリュームからファイルを読み出して、MacBinary（.bin）フォーマットに変換することができます。これは、Macintosh オペレーティングシステムで最も一般的に使用されているファイル圧縮フォーマットの 1 つです。

次の表に、一般的なファイル拡張子、および各拡張子が示す圧縮タイプを示します。

ファイル拡張子	意味
.Z	UNIX compress で圧縮されたファイル
.bin	MacBinary エンコード
.tar	UNIX tar アーカイブ
.tZ	UNIX compress で圧縮された tar アーカイブ
.tar.Z	UNIX compress で圧縮された tar アーカイブ
.crc	UNIX チェックサムファイル

FTP サービスに関する問題を解決する

anonymous FTP ユーザが接続できない場合：

- ゲストアクセスが許可されていることを確認します。
- anonymous　ユーザの接続が最大数に達したかどうかを確認します。これを行うときは、「Server Admin」の「ネットワーク」タブをクリックし、「FTP」をクリックしてから、「FTP を設定」を選びます。

クライアントが FTP サーバに接続できない場合：

クライアントが FTP 受動（passive）モードを使用しているかどうかを確認し、使用している場合は無効にします。受動（passive）モードでは、FTP サーバは、動的に決定されるポートでクライアントに対して接続を開きます。このポートが、IP フィルタサービスで設定されたポートフィルタと競合する可能性があります。

FTP 接続が拒否される場合：

- ユーザが入力したサーバの DNS 名または IP アドレスが正しいことを確認します。
- FTP サービスを開始していることを確認します。
- 共有ボリュームに対してユーザが適切なアクセス権を持っていることを確認します。
- 接続の数が最大値に達していないかどうかを確認します。これを行うときは、「Server Admin」の「ネットワーク」タブをクリックし、「FTP」をクリックしてから、「FTP を設定」を選びます。
- ユーザのコンピュータで TCP/IP が正しく設定されていることを確認します。TCP/IP 設定に問題がないと思われる場合は、「PING」ユーティリティを使ってネットワーク接続を確認します。
- FTP サーバの DNS 名の代わりに IP アドレスを使って接続してみて、DNS に問題があるかどうかを確認します。IP アドレスで接続できる場合は、DNS サーバに問題がある可能性があります。

- ユーザが自分のユーザ名を正しく入力していることと、正しいパスワードを入力していることを確認します。特殊文字または 2 バイト文字を含むユーザ名とパスワードは、無効です。ユーザ名を表示するには、「ユーザとグループのリスト」でユーザの名前をダブルクリックします。
- ディレクトリサービスに問題があるかどうか、およびディレクトリサービスサーバが動作中でネットワークに接続されているかどうかを確認します。ディレクトリサービスに関するヘルプについては、第 2 章「ディレクトリサービス」を参照してください。
- IP フィルタサービスが適切なポートにアクセスできるように設定されているかどうかを確認します。それでもクライアントが接続できない場合、クライアントが FTP 受動（passive）モードを使っていればそれがオフになっているかどうか確認します。受動（passive）モードでは、FTP サーバは、動的に決定されるポートでクライアントに対して接続を開きます。このポートが、IP フィルタサービスで設定されたポートフィルタと競合する可能性があります。一般的な TCP および UDP ポートのリストについては、301 ページの「Mac OS X コンピュータが使用するポート」を参照してください。

FTP サービスの仕様

使用許諾契約に応じた、最大接続ユーザ数（デフォルトの設定では、実際のユーザが 50 で、anonymous ユーザが 50 です）。	1000
FTP ポート番号	21
ユーザの接続を解除するまでに許可されるログインの失敗の数	3

ファイルサービスに関するその他の情報

「Mac OS X Server」のファイルサービスで使用されるプロトコルについて詳しくは、次の参考資料を参照してください。

- AFP（Apple Filing Protocol）： developer.apple.com/ja/index.html
- SMB（Server Message Block）プロトコル（Windows ファイルサービス）： www.samba.gr.jp
- FTP： FTP に関する RFC（Request for Comments）の書類は、次の Web サイトで見つけることができます。 www.faqs.org/rfcs/rfc959.html

  RFC の書類には、プロトコルやサービスの概要が記載されていて、サーバの管理を始めたばかりの方にとって参考になります。また、詳細な技術情報も記載されているので、経験豊富な管理者にとっても参考になります。RFC ドキュメントは、次の Web サイトで番号で検索することができます。 www.faqs.org/rfcs

  FTP に関する UNIX のマニュアルを入手するときは、「Mac OS X」で「Terminal」アプリケーションを開きます。プロンプトに「man ftp」と入力し、return キーを押します。
- NFS： NFS に関する UNIX のマニュアルを入手するときは、「Mac OS X」で「Terminal」アプリケーションを開きます。プロンプトに「man nfs」と入力し、return キーを押します。

6

プリントサービス

プリントサービスとは？

プリントサービスを使用すると、業界標準のLPRプリントプロトコルまたはWindows SMB（Server Message Block）プロトコルを使ってプリントジョブを送信するクライアントユーザ間で、PostScript 互換のプリンタを共有することができます。

プリントサービスを管理するときは、次のアプリケーションが役立ちます。

- 「Print Center」アプリケーションを使って、共有したいプリンタを選びます。
- 「Mac OS X Server」の「プリント」モジュールを使って、プリントサービスの一般的な設定およびプリントキューの共有方法を設定し、共有プリンタに送信されたプリントジョブを管理します。
- 「Server Admin」の「ログビューア」を使って、プリントジョブのアカウントに関する情報を参照します。

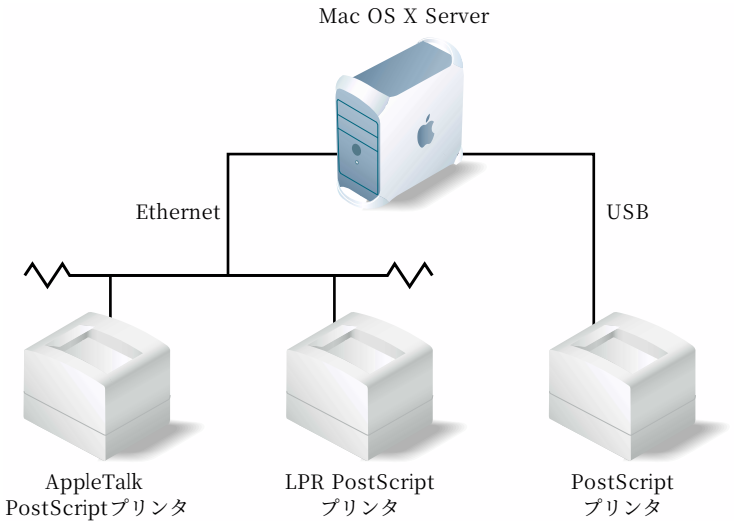
この章では、まずこれらの作業の概要を説明してから、プリントサービスの設定方法およびトラブルへの対処法について説明します。

プリンタをサーバに接続する

「Mac OS X」の「Print Center」アプリケーション（「Applications/Utilities」内）を使ってプリンタをサーバに「追加」し、共有したい各プリンタのプリントキューを作成します。「Print Center」を使って追加できる PostScript 互換プリンタであれば、任意のプリンタを共有できます。

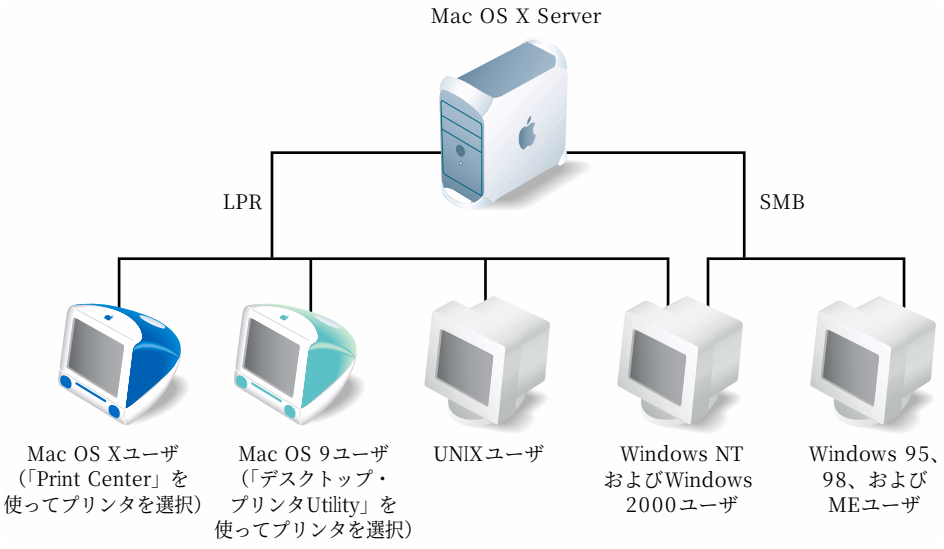
直接サーバに接続された PostScript 互換プリンタも共有することができます。この場合は、プリンタにキューを追加する必要はありません。キューは、「Print Center」を開いたときに自動的に作成されます。

ネットワークインタフェースを備えた共有 PostScript 互換プリンタは、AppleTalk または業界標準の（TCP/IP に基づいた）LPR プロトコルを使ってネットワークに接続することができます。直接接続されたプリンタは、USB（Universal Serial Bus）接続を使用します。



ネットワーク上でキューを共有する

LPR プロトコルまたは SMB プロトコルを使ってプリントジョブを送信するユーザが、共有プリンタをネットワーク上で使用することができます。



Macintosh、UNIX、および特定の Windows コンピュータ（「Windows NT」や「Windows 2000」など）はすべて LPR に対応しています。追加のソフトウェアをインストールする必要はありません。Windows コンピュータ（「Windows 95」、「Windows 98」、および「Windows ME」を含む）はすべて SMB に対応しています。

参考：LPR サポートが組み込まれていない Windows コンピュータでは、他社製の LPR ドライバを使用できます。

プリントキューとプリントジョブを管理する

ユーザが共有プリンタに送信したプリントジョブは、プリンタのキューに自動的に送られます。これらのプリントジョブは、プリンタが利用可能になるか、または設定した基準が満たされるまで、保留になります。たとえば、「Server Admin」の「プリント」モジュールでは次の基準を設定することができます。

- キュー内のプリントジョブの優先順位を設定できます。優先順位が「至急」に設定されたジョブは、優先順位が「通常」または「低」に設定されたジョブより先にプリントされます。
- ジョブが指定した時間にプリントされるようにスケジュールを設定できます。たとえば、時間がかかるジョブは、深夜や早朝など、プリンタがあまり使用されない時間に自動的に開始するようにスケジュールを設定できます。
- プリントジョブを保留（無期延期）にすることができます。たとえば、特定のジョブの保留を解除してプリントする前に、そのユーザが、プリントの枚数の上限や予算を超えていないかどうかを確認する必要がある場合が考えられます。

プリントジョブを監視する

「Server Admin」の「プリント」モジュールの「プリントモニタ」を使用すると、プリンタとそのジョブの最新状況を確認できます。特定のプリンタに、プリント待ちのジョブがたくさんあるかどうか、またはプリンタに問題が発生していないかどうかをひと目で確認することができます。

「プリント」モジュールには「キューモニタ」もあります。これを使用すると、プリントキューのジョブの詳細を確認できます。各ジョブについて、ジョブを送信したユーザ、ページ数、および優先順位が表示されます。また、キュー内のジョブを保留または削除したり、ジョブに優先順位を設定したりすることができます。

また、「Server Admin」の「ログビューア」を使って、プリントログを表示して、プリント状況を追跡することもできます。プリントサービスログには、プリントサービスの開始および停止やプリントキューの保留などのイベントが記録されます。プリントキューごとのログには、特定のプリンタにジョブを送信したユーザやジョブのサイズなど、個々のプリントジョブに関する情報が記録されます。

プリントサービスを設定する前に

プリントサービスを設定する前に、特定のプリンタを次のユーザが使用するかどうかを判断します。

- LPR プロトコルを使ってプリントジョブを送信するユーザ
- SMB プロトコルを使ってプリントジョブを送信するユーザ

プリントサービスを初めて設定する

プリントサービスを設定するときは、キューを管理および共有したいプリンタを「Print Center」を使って追加し、「Server Admin」の「プリント」モジュールを使って各キューを設定します。プリンタを追加した後は、キューまたはジョブの管理に「Print Center」は使用しないでください。「Print Center」ではなく、「Server Admin」の「プリント」モジュールを使用します。

プリントサービスを設定するときは、次のように操作します。

手順 1：プリンタを追加する

「Print Center」を使って、「Mac OS X Server」で管理したい、USB 接続ではないプリンタをそれぞれ追加します。その方法については、「Print Center」のオンスクリーンヘルプを参照してください。プリンタを追加すると、そのプリントキューが自動的に定義されます。

手順 2：プリントサービスを設定する

「Server Admin」の「プリント」モジュールを使って、プリントサービスを設定します。利用可能な設定の説明については、115 ページの「プリントサービスの一般設定」を参照してください。

手順 3：プリントキューを設定する

「Server Admin」の「プリント」モジュールを使って、追加したプリンタごとにキューを設定します。プリントキューの設定の説明については、116 ページの「プリントキューの設定」を参照してください。

手順 4：プリントサービスを開始する

プリントサービスが動作中でない場合は、「プリント」をクリックし、「プリントサービスを開始」を選びます。「Mac OS X Server」の起動時にプリントサービスが自動的に開始するように設定することができます。その手順については、115 ページの「プリントサービスの一般設定」を参照してください。

手順 5：Windows サービスを開始する（省略できます）

SMB を使ってプリントジョブを送信する Windows ユーザがプリントできるようにするときは、Windows サービスが動作中で、1 つ以上のプリントキューで SMB が使用可能であることを確認します。Windows サービスについて詳しくは、93 ページの「Windows サービス」を参照してください。SMB ユーザ用にプリントキューを共有する方法については、116 ページの「プリントキューの設定」を参照してください。新規キューを作成したときに、自動的にそのキューで SMB を使ってプリントできるようにする方法については、115 ページの「プリントサービスの一般設定」を参照してください。

手順 6：クライアントコンピュータからプリントを設定する

手順 3 で設定したキューに対して Mac OS 8、Mac OS 9、および Mac OS X コンピュータからプリント設定を行う手順については、プリントサービスに関するオンスクリーンヘルプを参照してください。

プリントサービスの設定

プリントサービスの設定にアクセスするときは、「Server Admin」で「ファイルとプリント」タブをクリックし、「プリント」をクリックして、適切なコマンドを選びます。

プリントサービスの一般設定

プリントサービスの一般的な動作を制御する設定にアクセスするときは、「プリント」をクリックし、「プリントサービスを設定」を選びます。

システム起動時にプリントサービスを開始する

サーバの起動時にプリントサービスを自動的に開始したい場合は、このオプションを選びます。

Windows プリント用に新規キューを自動的に共有する

SMB プロトコルを使ってプリントする Windows ユーザが、「Print Center」を使って作成された新規プリントキューを自動的に使用できるようにしたい場合は、このオプションを選びます。このオプションを選ぶ場合は、Windows サービスが動作中であることを確認してください。Windows サービスについて詳しくは、93 ページの「Windows サービス」を参照してください。

LPR のデフォルトキュー

キュー名が指定されていない LPR プリントジョブが送信された場合に使用したいキューを選びます。ユーザがプリンタ名を指定せずに、サーバのドメイン名または IP アドレスを使ってジョブを送信した場合、そのジョブにキュー名はありません。デフォルトキューを使用すれば、クライアントコンピュータでは、キュー名を指定する必要がないため、プリント設定を簡略化できます。

サーバのログ

プリントサービスのログをアーカイブに保存して新しいログを開始する頻度を指定するときは、このオプションを選び、日数を入力します。

キューのログ

各プリントキューのログをアーカイブに保存して新しいログを開始する頻度を指定するときは、このオプションを選び、日数を入力します。

プリントキューの設定

キューの共有方法を管理し、キュー内の新規ジョブをプリントするデフォルトの時刻を指定するときは、「プリントモニタ」ウインドウでキュー名を選び、「編集」ボタンをクリックします。(「プリントモニタ」のウインドウを開くときは、「ファイルとプリント」タブで「プリント」をクリックし、「プリントモニタを表示」を選びます。)

キュー名

「Print Center」でプリンタを追加すると、そのプリンタ名と同じ名前のキューが作成されます。「キュー名」フィールドに名前を入力することによって、共有に使用するキュー名を必要に応じて変更できます (たとえば、ユーザには別のキュー名を表示したい場合など)。キュー名を入力しても、「Print Center」でのキュー名は変更されません。

キューを使ってプリントを行うユーザにプリンタ名の制限がある場合は、キュー名を変更した方がよいこともあります。たとえば、Windows クライアントによっては名前が半角英数文字で 12 文字までに制限されている場合があり、LPR クライアントによっては空白が含まれる名前に対応していない場合があります。

プリンタ

これは「Print Center」でのキュー名です。

キューの共有

LPR プロトコルを使ってジョブを送信するユーザがキューを利用できるようにする場合は、「LPR」を選びます。デフォルトの設定では、すべての新規プリントキューで LPR が選択されます。

SMB プロトコルを使ってジョブを送信する Windows ユーザがキューを利用できるようにする場合は、「Windows printing（SMB）」を選びます。このオプションを選ぶ場合は、Windows サービスが動作中であることを確認してください。Windows サービスについて詳しくは、93 ページの「Windows サービス」を参照してください。新規のキューに対して、自動的にそのキューで SMB を使ってプリントできるようにする方法については、115 ページの「プリントサービスの一般設定」を参照してください。

PostScript 互換ではないプリンタの場合、これらのチェックボックスは使用できません。

ドメインの中の LPR キューの共有

NetInfo の共有ドメインにプリントキューを追加すると、そのドメインにアクセスするように設定された Mac OS X コンピュータのユーザは、「Print Center」のディレクトリサービス一覧からキューを選ぶことによって、そのキューを使ってプリントを行うことができるようになります。

共有ドメインにプリントキューを追加するときは、ポップアップメニューから共有ドメインを選び、ドメインが置かれているサーバの管理者のユーザ名とパスワードを入力します。NetInfo の共有ドメインにキューを追加したくない場合は、「なし」を選びます。

NetInfo ドメインでの LPR キューの共有を設定した後は、サーバで「Print Center」を使って、ディレクトリサービスの一覧からキューを選んでキューを追加しないでください。

ジョブの優先順位

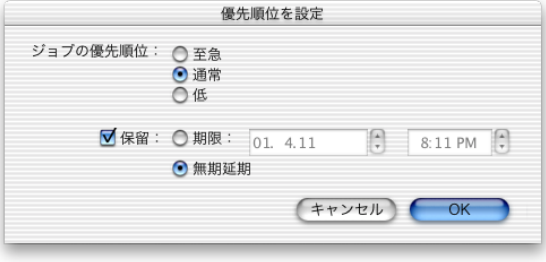
このキュー内の新規のプリントジョブに割り当てたいデフォルトの優先順位を選びます。ジョブは優先順位に従ってプリントされます。「至急」のジョブが最初にプリントされ、次に「通常」のジョブ、「低」のジョブの順にプリントされます。プリントジョブの設定を使って、個別のジョブのデフォルトの優先順位を上書きすることができます。その方法については、以下の「プリントジョブの設定」を参照してください。

保留

キューに送信されるすべての新規ジョブのプリントを延期するときは、「保留」を選びます。ジョブをプリントする時刻を指定するか、またはプリントを無期延期にすることができます。

プリントジョブの設定

特定のジョブをプリントする時刻を設定するときは、「キューモニタ」ウインドウでその名前を選び、「優先順位」ボタンをクリックします。（「キューモニタ」を開くときは、「プリントモニタ」ウインドウでキューを選び、「キューモニタを表示」をクリックします。）



ジョブの優先順位

ジョブに割り当てたい優先順位を選びます。「至急」のジョブが最初にプリントされ、次に「通常」のジョブ、「低」のジョブの順にプリントされます。キュー内で同じ優先順位が割り当てられている場合は、ジョブは古い順にプリントされます。

保留

ジョブのプリントを延期するときは、「保留」を選びます。ジョブをプリントする日時を指定するか、またはプリントを無期延期にすることができます。ジョブの保留を解除するときは、「保留」の選択を解除するか、「キューモニタ」ウインドウで「解除」をクリックします。ジョブは、キュー内で同じ優先順位が割り当てられた、保留になっていないその他のジョブの後でプリントされます。保留になっていないジョブがプリントされるのは、そのキューが保留になっていない場合だけです。

プリントサービスに関する問題を解決する

プリントに関する問題を解決または回避するときは、次の方法を試してください。

プリントサービスが開始しない場合：

- サーバの起動時にプリントサービスが自動的に開始するように設定したい場合は、「プリントサービスを設定」ウインドウで「システム起動時にプリントサービスを開始する」チェックボックスにチェックマークが付いていることを確認します。
- サーバのシリアル番号が正しく入力されていて、有効期限が過ぎていないことを確認するときは、「一般」タブをクリックし、「サーバ情報」をクリックして、「サーバ情報を表示」を選びます。
- プリントサービスログで追加情報を確認するときは、「一般」タブをクリックし、「ログビューア」をクリックして、「プリントサービス」を選びます。「ログビューア」ウインドウでサーバのログを選びます。

ユーザがプリントできない場合：

- プリントサービスが動作中であることを確認します。
- 「プリントモニタ」ウインドウを開いて、ユーザがプリントしているキューがあることを確認します。Mac OS 8 または Mac OS 9 コンピュータの場合は、「デスクトップ・プリンタ Utility」を使ってプリンタ設定が正しいことを確認します。
- ユーザがプリントしているキューが、正しく共有されていることを確認します。SMB を使用するのは、Windows ユーザだけです。LPR は標準のプロトコルで、Macintosh や UNIX などのコンピュータだけでなく、（一部の）Windows コンピュータのユーザがプリントするために使用できます。
- 「Mac OS 8」と「Mac OS 9」のクライアントの場合は、TCP/IP が正しく設定されていることを確認します。
- Windows NT 4.x のクライアントがサーバに対してプリントできない場合は、キュー名が、プリンタまたはサーバの TCP/IP アドレスになっていないことを確認します。プリンタまたはサーバのアドレスではなく DNS ホスト名を使用するか、DNS ホスト名がない場合は、英数字のみを含むキュー名を入力します。

プリントジョブが受け付けられ、エラーメッセージも表示されないが、プリントされない場合：

- 「プリントモニタ」ウインドウをチェックして、キューが保留になっていないことを確認します。
- プリンタが、サーバ、またはサーバが接続されているネットワークに接続されていることを確認します。
- プリンタの電源が入っていることと、プリンタ自体に問題（用紙切れ、紙詰まりなど）がないことを確認します。
- プリントログで詳しい情報を確認します。「一般」タブをクリックし、「ログビューア」をクリックして、「プリントサービス」を選びます。「ログビューア」ウインドウで、サーバのログを選んでプリントサービスのログ全般を確認するか、またはキュー名を選んで特定のプリンタのログを確認します。

7

Web サービス

Web サービスとは？

「Mac OS X Server」の Web サービスは、統合されたインターネットサーバソリューションを提供します。Web サービスは簡単に設定して管理できるので、経験豊富な Web 管理者でなくても複数の Web サイトを設定し、Web サーバの設定と監視を行うことができます。

「Mac OS X Server」の Web サービスでは、オープンソースの HTTP Web サーバである Apache を使用しています。「AppleShare IP」をお使いの方、および初めて Web 管理者になった方でも、「Server Admin」を使って Web サービスを管理できるので、高度な設定や設定ファイルについての知識は必要ありません。Apache を熟知している Web 管理者の方であれば、Apache の高度な機能を使って Web サービスを管理することができます。

さらに、Mac OS X Server「Mac OS X Server」の Web サービスには高性能のフロントエンドキャッシュが含まれており、更新されない HTML ページを扱う Web サイトの性能を向上させることができます。このキャッシュによって、サーバは要求されるたびに静的なデータにアクセスする必要がなくなります。

Web サービスには、WebDAV（Web-based Distributed Authoring and Versioning）のサポートも含まれています。WebDAV 機能を使用すると、クライアントユーザはサイトが稼働中に Web ページをチェックアウトし、変更を加え、チェックインして戻すことができます。また、WebDAV には豊富なコマンドセットが用意されています。これによって、「Mac OS X」がインストールされているクライアントコンピュータは、WebDAV 対応の Web サーバをファイルサーバであるかのように使用できます。

Web サービスを設定する前に

このセクションには、初めて Web サービスを設定する前に知っておく必要のある情報が記載されています。経験豊富な Web 管理者の方も、これまでと違った機能や動作が説明されている可能性がありますので、このセクションをお読みください。

Web サービスを設定する

「Server Admin」を使って、使用頻度の高い Web サービスの機能のセットアップと設定を行うことができます。Apache を熟知していて、「Server Admin」にはない Apache の Web サーバの機能を使用する必要がある場合は、適宜設定ファイルを変更することができます。ただし、アップル社では Apache の設定ファイルの変更に関する技術サポートは提供していません。ファイルを変更する場合は、必ず最初にバックアップコピーを作成してください。このようにすると、問題が発生したときにそのコピーを使って元に戻すことができます。

Apache モジュールについて詳しくは、Japan Apache User Group の Web サイト（www.apache.or.jp）を参照してください。

セキュリティで保護されたトランザクションを提供する

サーバ上のトランザクションをセキュリティで保護するときは、SSL（Secure Sockets Layer）保護を設定します。SSL を使うと、暗号化された認証済みの情報をインターネット経由で送信できます。たとえば、Web サイトでクレジットカードのトランザクションを行う場合に、サイトで送受信される情報を SSL を使って保護することができます。

セキュリティで保護されたトランザクションの設定方法について詳しくは、142 ページの「SSL（Secure Sockets Layer）サービスを設定する」を参照してください。

Web サイトを設定する

Web サイトを開設する前に、次の作業を行う必要があります。

- ドメイン名をドメイン名管理機関に登録します
- サーバに Web サイト用のフォルダを作成します
- 作成したフォルダに、ユーザが接続したときに表示されるデフォルトのページを作成します
- インターネットに接続する場合は、DNS サービスを適切に設定します（イントラネット上のサイトの場合は DNS は必要はありません）

サイトの準備ができたら、「Server Admin」を使って公開（使用可能に）します。「Web サービスを設定」ウインドウの「サイト」パネルでは、新しいサイトを追加したり、開設した各サイトのさまざまな設定を選んだりすることができます。サイトの設定について詳しくは、130 ページ以降の説明をお読みください。また、サイトの設定時に行う作業のいくつかについては、「Server Admin ヘルプ」も参照してください。

複数の Web サイトを運用する

Web サーバ上で複数の Web サイトを同時に運用することができます。サイトの設定によって、各サイトのドメイン名、IP アドレス、またはポートを同じにすることもできます。ただし、ドメイン名、IP アドレス、およびポートの組み合わせは一意に割り当てる必要があります。使用するドメイン名は、ドメイン名管理機関（InterNIC）に登録する必要があります。登録していないと、そのドメイン名に関連付けられている Web サイトをインターネットで見ることはできません。（追加登録名ごとに登録料がかかります。）

複数のドメイン名と 1 つの IP アドレスを使って Web サイトを設定する場合、HTTP1.1 以上に対応していない古いブラウザでは、そのサイトにアクセスできません（ブラウザで「Host」リクエストヘッダが無視されます）。この問題を避けたい場合は、1 つの IP アドレスにつき 1 つのドメイン名を使ってサイトを設定してください。

WebDAV のセキュリティを理解する

WebDAV を使用すると、ユーザはサイトが稼働中でも Web サイトのファイルを更新できます。WebDAV を使用する場合は、ユーザが更新するサイト内のファイルとフォルダに対して、Web サーバが書き込みのアクセス権を持っている必要があります。このようにアクセス権を設定すると、サイトの管理者がほかのサイトを変更できる可能性があるため、そのサーバでほかのサービスを実行している場合、セキュリティ上の重要な問題になる可能性があります。

この問題は、「Server Admin」の「共有」モジュールを使ってサイトのファイルに適切なアクセス権を設定することで回避できます。「Mac OS X Server」では、Apache プロセスが属する「www」というグループが「ユーザとグループのリスト」に追加されます。この www グループには、Web サイト内のファイルへの「読み出し／書き込み」のアクセス権を与える必要があります。また、Web サイト管理者（オーナー）に「読み出し／書き込み」のアクセス権を与え、「全員」には「なし」を与えます。

Web サイトのセキュリティに不安がある場合は、WebDAV の代わりに Apple ファイルサービスまたは FTP サービスを使って Web サイトのコンテンツを変更するようにします。WebDAV のアクセス権について詳しくは、149 ページの「WebDAV の保護領域とアクセス権を理解する」を参照してください。

Web サービスを初めて設定する

Web サービスを初めて設定するときは、次の手順に従って行います。これらの作業の実行について詳しくは、Web サービスのヘルプを参照してください。

手順 1：「Documents」フォルダを設定する

サーバソフトウェアをインストールすると、「Documents」というフォルダが自動的に作成されます。「Documents」フォルダには、Web サイトを通じて利用できるようにする項目を保存します。情報を整理したいときは、「Documents」フォルダの中にフォルダを作成できます。このフォルダは、次のディレクトリにあります。

/Library/WebServer/Documents

また、登録ユーザのホームディレクトリにはそれぞれ、「Sites」フォルダが作成されます。このフォルダに保存した画像や HTML ページは、次の URL で提供されます。

http://server.example.com/~username/

手順 2：デフォルトのページを作成する

ユーザが Web サイトに接続すると、必ずデフォルトのページが表示されます。ソフトウェアをインストールした初期の状態では、「Documents」フォルダ内の「index.html」ファイルがデフォルトのページになります。このファイルを自分の Web サイトの最初のページと置き換えて、「index.html」という名前を付けます。別のファイル名を使用したい場合は、必ずサイトの設定ウインドウの「一般」パネルでデフォルトの書類名を変更してください。

Web サイトの設定について詳しくは、130 ページの「Web サイトの設定」を参照してください。

手順 3：Web サイトにアクセス権を割り当てる

サーバで実行する Apache のプロセスには、Web サイトのファイルとフォルダへのアクセス権が与えられている必要があります。このアクセス権を与えるために、「Mac OS X Server」によって、Apache プロセスが属する「www」というグループがサーバの「ユーザとグループ」データベースにインストールされます。この www グループには、Web サイトのファイルへの「読み出し専用」のアクセス権を与える必要があります。これによって、ユーザがサイトに接続したときに、www グループが Web サイトのファイルをブラウザに転送できるようになります。アクセス権の割り当てについて詳しくは、第 4 章「共有」を参照してください。

手順 4：Web サービスを設定する

デフォルトの設定は、1 つの Web サイトを運用するほとんどの Web サーバで、そのまま使用することができます。Web サービスと Web サイトの基本的な機能はすべて「Server Admin」で設定できます。詳しい設定オプションについては、147 ページの「Apache の詳しい設定」を参照してください。

ユーザの Web サイトを運用するときは、少なくとも 1 つの Web サイトを設定する必要があります。その Web サイトの設定を、サーバ上のすべてのユーザ Web サイトに適用したい場合は、デフォルトのサイトを「/Users」に設定する必要があります。

設定を表示するときは、「Web サービス」をクリックし、「Web サービスを設定」を選びます。必要に応じてサーバと Web サイトの設定を選びます。これらの設定について詳しくは、125 ページの「Web サービスの設定」を参照してください。

手順 5：Web サービスを開始する

「Web サービス」をクリックし、「Web サービスを開始」を選びます。サービスが稼働中のときは、「Web サービス」のアイコンに地球のマークが表示されます。

重要　Web サーバを開始および停止するときは、常に「Server Admin」を使用してください。コマンドラインから Web サーバを開始しても、「Server Admin」は Web サーバを停止できず、Web サーバの稼動状態も認識しません。

手順 6：Web サイトに接続する

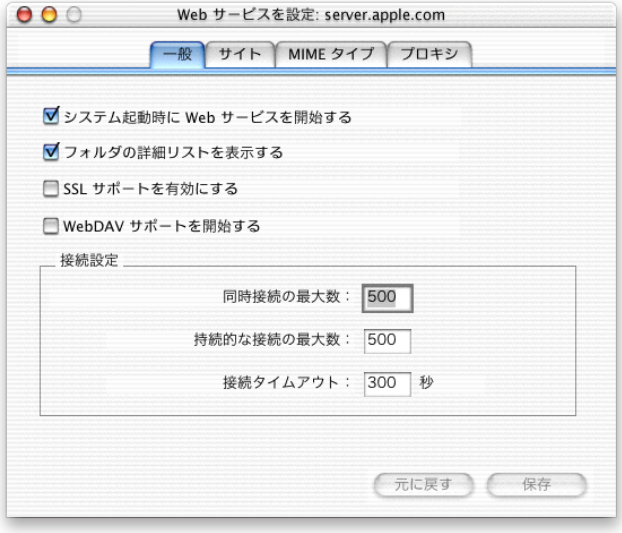
Web サイトが正常に稼動していることを確かめるときは、ブラウザを開いて、インターネット経由で自分の Web サイトに接続してみます。Web サイトが正常に稼動していない場合は、149 ページの「Web サービスに関する問題を解決する」を参照してください。

Web サービスの設定

「Web サービスを設定」ウインドウでは、Web サーバと Web サイトのすべてのオプションを設定および変更することができます。「Web サービスを設定」ウインドウを表示するときは、「Server Admin」の「Web サービス」ボタンをクリックし、「Web サービスを設定」を選びます。5 つのタブのいずれかをクリックして、そのタブのパネルの設定を表示します。以下のセクションでは、各パネルで使用できる設定について個別に説明します。

Web サービスの一般設定

自動的に開始するオプションなど、サーバの一般的なオプションを設定するときは、「Web サービスを設定」ウインドウの「一般」パネルを使います。



システム起動時に Web サービスを開始する

サーバの起動時に Web サービスを開始するときは、このオプションを選びます。通常は、このオプションを選択しておくことをお勧めします。選択されていれば、電源が切れたり、その他の不測の事態が発生してサーバが再起動した場合でも、Web サービスを利用できます。

フォルダの詳細リストを表示する

Web サイトのフォルダの内容に関するフォーマット済みのリストを表示するときは、このオプションを選びます。ユーザがサイトの URL に接続すると、通常はデフォルトの Web ページ（「index.html」など）が表示されます。デフォルトの Web ページが存在しない場合、Web サイトでフォルダのインデックス作成が許可されていると、フォルダの内容のリストがユーザに表示されます。サイトのフォルダのリスト表示を許可する方法については、131 ページの「Web サイトの一般設定」を参照してください。

SSL サポートを有効にする

Web サイトに安全に接続するには、このオプションを選びます。SSL を使用可能にする場合は、各サイトのポート番号を 443 に変更する必要があります。

SSL を使用可能にするには、あらかじめ認証プロバイダから証明ファイルを入手し、SSL サービスを設定しておく必要があります。詳しくは、142 ページの「SSL（Secure Sockets Layer）サービスを設定する」を参照してください。

WebDAV サポートを開始する

ユーザが WebDAV（Web-based Distributed Authoring and Versioning）を使用できるようにしたいときは、このオプションを選びます。WebDAV を許可する場合は、各 Web サイトに「保護領域」を設定して、サイトを変更できるユーザを管理する必要もあります。WebDAV の使用について詳しくは、149 ページの「WebDAV の保護領域とアクセス権を理解する」を参照してください。

同時接続の最大数

サーバの 1 つの Web サイトで同時に受け付けられる接続の最大数を入力します。デフォルトの最大値は 500 です。サーバでの同時接続が最大数に達すると、その後の接続要求に対しては、サーバがビジー状態であることを示すメッセージが表示されます。

持続的な接続の最大数

クライアントコンピュータが 1 つの接続で作成できる接続要求の最大数を入力します。固定接続を使用すると、サーバが、1 つの接続で複数のトランザクションを処理できるようになります。これによって、サーバの性能を向上させることができます。1 つの接続に許可する要求数を制限したくない場合は、ゼロに設定します。しかし、デフォルト設定の 500 を使うと、性能が向上します。

参考：このオプションを使用する場合は、パフォーマンスキャッシュを無効にする必要があります。

接続タイムアウト

Web サーバによってセッションが切断されるまでの秒数を入力します。この時間を経過しても要求がない場合はセッションが切断されます。このオプションを使用する場合は、パフォーマンスキャッシュを無効にする必要があります。

Web サービスのサイトの設定

「サイト」パネルには、Web サイトの一覧と、それぞれのサイトに関するいくつかの基本的な情報が表示されます。「サイト」パネルは、新しいサイトを追加、または既存のサイトの設定を変更する場合に使用します。「サイト」パネルを表示するときは、「Web サービス」をクリックし、「Webサービスを設定」を選び、「サイト」タブをクリックします。

有効

サイトを有効または無効にするときは、このチェックボックスを使用します。デフォルトでは、新しいサイトを作成したときに、このチェックボックスにチェックマークが付けられます。サイトを無効にした場合、設定はそのまま保持されますが、サイトに送信された要求は無視されます。

追加と複製

新しい Web サイトをリストに追加し、そのサイトの設定を行うときは、「追加」ボタンをクリックします。または、新しいサイトで必要な設定がほとんど指定されている Web サイトを選び、「複製」をクリックして複製サイトを作成します。その後、複製サイトの設定を変更して、新しいサイトとして保存することができます。

編集

サイトを変更するときは、Web サイトを選び、「編集」をクリックします。Web サイトの設定について詳しくは、130 ページの「Web サイトの設定」を参照してください。

削除

リストから Web サイトを取り除きたいときは、Web サイトを選び、「削除」をクリックします。この操作によって「Web サービスを設定」リストから目的の Web サイトの名前と設定が削除されますが、サーバから Web サイトとその内容が取り除かれることはありません。

Web サービスの MIME タイプの設定

MIME（Multipurpose Internet Mail Extension）とは、ファイルの内容を記述するためのインターネットの規格です。「MIME タイプ」パネルでは、ブラウザが特定のファイルタイプを要求したときに、Web サーバがどのように応答するかを設定できます。MIME タイプと MIME タイプマッピングについて詳しくは、141 ページの「MIME（Multipurpose Internet Mail Extension）を理解する」を参照してください。

「MIME タイプ」パネルを表示するときは、「Web サービス」をクリックし、「Web サービスを設定」を選び、「MIME タイプ」タブをクリックします。

拡張子

「拡張子」は、オーディオ、テキスト、ビデオなど、ファイル内のデータの種類を表します。

Web サーバの動作

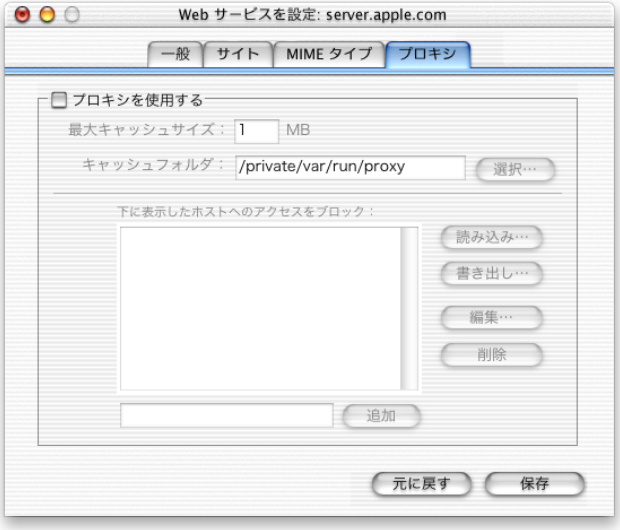
「Web サーバの動作」は、Web サーバが特定の拡張子を持つファイルの要求を受信したときに、どのように動作するかを指定します。動作、応答、またはその両方を指定できます。

追加、編集、複製、および削除

新しい MIME タイプを作成するとき、または既存の MIME タイプを変更するときは、これらのボタンをクリックします。

Web サービスのプロキシの設定

Web サーバをユーザのプロキシとして使用すると、アクセス頻度の高い Web サイトをキャッシュに保存してサーバの性能を向上させることができます。「プロキシ」パネルを表示するときは、「Web サービス」をクリックし、「Web サービスを設定」を選び、「プロキシ」タブをクリックします。



プロキシを使用する

サーバをユーザのプロキシとして使用するときは、このチェックボックスを使用します。サーバをプロキシとして使用すると、たとえば、授業の課題で生徒全員が同じ Web サイトにアクセスするような場合に役に立ちます。生徒全員が同時に接続しようとすると、サーバは、接続要求を統合し接続先のサイトをキャッシュするので、性能が向上します。プロキシサービスを使用するときは、クライアントユーザの Web ブラウザの環境設定で、使用する Web サーバをプロキシサーバとして指定する必要があります。

最大キャッシュサイズ

クライアントコンピュータが要求したほかのWebサイトをキャッシュするために使用するディスク容量の最大値を入力します。キャッシュは、低速のインターネット接続での性能を最適化するために役立ちます。キャッシュが最大のサイズに達すると、キャッシュフォルダから最も古いファイルが削除されます。

キャッシュフォルダ

キャッシュの保存場所として使用するフォルダのパスとフォルダ名を入力します。ファイルサービスが稼動中の場合、またはサーバで「Server Admin」を使用している場合は、「選択」ボタンをクリックして目的のフォルダを検索することができます。

下に表示したホストへのアクセスをブロック

「追加」ボタンをクリックし、キャッシュしたくない Web サイトのドメイン名または IP アドレスを入力します。サーバがクライアントユーザの Web ブラウザでプロキシサーバとして指定されている限り、このリストに追加したサイトはキャッシュされません。好ましくない Web サイトをここに指定することをお勧めします。

読み込み

キャッシュしたくない Web サイトのリストを読み込むときは、このボタンをクリックします。リストはテキストファイルでなければなりません。また、ホスト名が余白（ライン、スペース、またはタブ）で区切られている必要があります。

書き出し

ブロックするホストのリストをテキストファイルに書き出すときは、このボタンをクリックします。

Web サイトの設定

Web サイトの設定には、サイトの設定ウインドウを使用します。このウインドウを開くときは、「Web サービス」をクリックし、「Web サービスを設定」を選び、「サイト」タブをクリックします。新しいサイト用のウインドウを開くときは、「追加」をクリックします。既存のサイト用のウインドウを開くときは、リストで目的のサイトを選び「編集」または「複製」をクリックします。

設定のウインドウには、次の 4 つのパネルがあります。「一般」、「ログ」、「アクセス」、および「セキュリティ」です。このウインドウで設定した内容は、Web サイトに個別に適用されます。Web サービス全体に適用されることはありません。ただし、一部の設定は、Web サービスの設定に依存します。たとえば、ある Web サイトで SSL を使用可能にする場合は、Web サービスでも SSL を使用可能にする必要があります。これらの 3 つのパネルの設定について、次に説明します。

Web サイトの一般設定

名前やポート番号などの一般的なオプションをサイトごとに設定するときは、サイトの設定ウインドウの「一般」パネルを使用します。Web サイトの「一般」パネルを表示するときは、「Web サービス」をクリックし、「Web サービスを設定」を選び、「サイト」タブをクリックします。「追加」をクリックするか、あるいはサイトを選んでから「編集」または「複製」をクリックします。

名前

サイトの省略しないドメイン名を入力します。ホスト名のみを入力するのではありません。たとえば、server.apple.com が省略していない完全なドメイン名です。

IP アドレス

サイトの IP アドレスを入力します。運用する Web サイトごとに、IP アドレスとポート番号の一意の組み合わせか、またはサーバの別のホスト名を指定する必要があります。異なる IP アドレスを設定した場合は、複数の IP アドレスの IP パケットを受け付けるようにサーバコンピュータを設定しなければなりません。複数の IP アドレスの割り当てについて詳しくは、305 ページの「ポートに複数の IP アドレスを設定する」を参照してください。

ポート

このサイトへの接続に使用するポートを選びます。サーバのデフォルトでは、サーバの Web サイトへの接続にはすべてポート 80 が使用されますが、Web サイトごとに使用するポートを変更することができます。最大 8999 までの任意のポート番号を選ぶことができます。ただし、ほかのサービス（FTP、Apple ファイル共有、SMTP 接続など）が使用していないポートを選ぶようにします。

このサイトで SSL を使用可能にする場合は、SSL のデフォルトの HTTPS ポートであるポート 443 を使用してください。TCP ポートと UDP ポートの番号のリスト、およびそれらのポートを使用するサービスについては、301 ページの「Mac OS X コンピュータが使用するポート」を参照してください。

Web フォルダ

このサイトのルートとして使用したいディレクトリへのパスを入力します。ファイルサービスが稼動中の場合、またはサーバで「Server Admin」を使用している場合は、「選択」をクリックして目的のフォルダを参照することができます。

デフォルトの書類名

ユーザがファイル名ではなくドメイン名またはディレクトリ名でサイトに接続したときに、表示するファイルの名前を入力します。ソフトウェアをインストールした初期の状態では、デフォルトの書類名は「index.html」です。デフォルトの書類がない場合は、ディレクトリのリストが表示されます（ディレクトリのリスト表示が許可されている場合）。詳しくは、125 ページの「フォルダの詳細リストを表示する」、および以下の「パフォーマンスキャッシュを使用する」オプションの説明を参照してください。

参考：「デフォルトの書類名」フィールドには、複数のファイル名を指定できます。スペースを含むファイル名は、引用符で囲む必要があります。各ファイル名はスペースで区切ります。

パフォーマンスキャッシュを使用する

Web サイトに更新されない HTML ファイルがあり、そのページの利用率が高いことが予想される場合は、このオプションを選びます。Web ページのほとんどが動的に更新される場合は、キャッシュを使用可能にしないでください。パフォーマンスキャッシュについて詳しくは、148 ページの「動的な Web ページのキャッシュを無効にする」を参照してください。

フォルダのリスト表示を許可する

ユーザがこのサイトに接続したときに、デフォルトの書類の代わりに Web フォルダの内容のリストを表示したい場合は、このオプションを選びます。リスト表示を許可していない場合で、デフォルトの Web ページが存在しないときは、アクセスが拒否されたことを知らせるメッセージが表示されます。

WebDAV を許可する

このサイトで WebDAV を使用するときは、このオプションを選びます。「Web サービスを設定」ウインドウの「一般」パネルでも、WebDAV を使用可能にする必要があります。

CGI の実行を許可する

Web フォルダに保存されている CGI（Common Gateway Interface）プログラムを実行したいときは、このオプションを選びます。CGI プログラムについて詳しくは、140 ページの「CGI（Common Gateway Interface）スクリプトを使用する」を参照してください。

管理者のメールアドレス

クライアントに送信されるすべてのエラーメッセージで、返信用メールアドレスとして使用するアドレスを入力します。Apache のデフォルトのエラーページには、指定するアドレスへのリンクが含まれます。クライアントユーザは、Web サイトに関する問題が発生したときに、このリンクを使ってフィードバックを返すことができます。

Web サイトのログの設定

サイトの設定ウインドウの「ログ」パネルでは、サイトごとにログを設定し、記録を許可することができます。「ログ」パネルを表示するときは、「Web サービス」をクリックし、「Web サービスを設定」を選び、「サイト」タブをクリックします。「追加」をクリックするか、あるいはサイトを選んでから「編集」または「複製」をクリックします。次に、「ログ」タブをクリックします。

アクセスログを許可する

Web サイトにアクセスがあるたびにログ項目を作成するときは、この欄をクリックします。

_ 日ごとにアーカイブを作成する

各ログファイルにイベントを記録する期間を日数で入力します。指定した期間が過ぎると、現在のログが保存され、そのファイル名に日付が追加されます。また、新しいログファイルでの記録が開始されます。

場所

ログファイルを保存したい場所のパスとファイル名を入力します。ファイルサービスが稼動中の場合、またはサーバで「Server Admin」を使用している場合は、「選択」をクリックして目的の場所を参照することができます。ログファイルのデフォルトの場所は、「/var/log/httpd/」です。

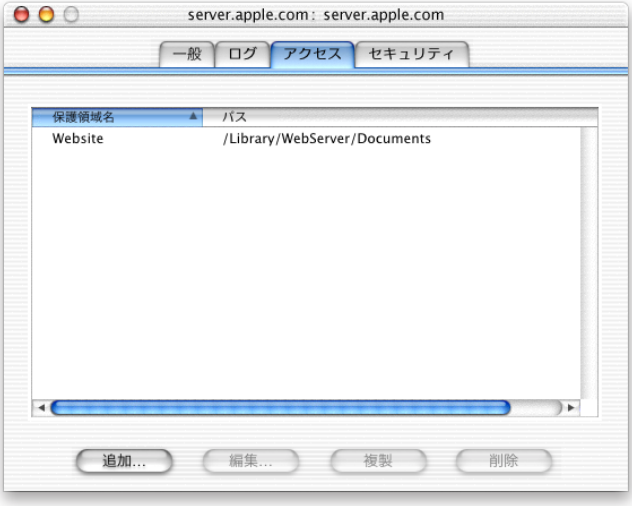
エラーログを許可する

このWebサイトで発生したエラーをログに記録するときは、この欄をクリックします。

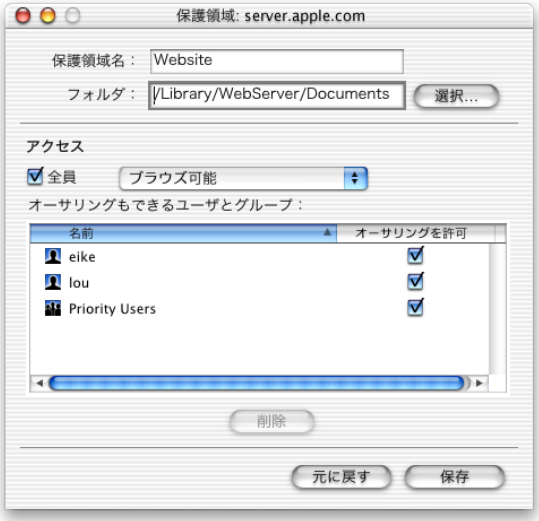
Webサイトのアクセスの設定

サイトの設定ウインドウの「アクセス」パネルでは、「保護領域」、つまりサイト内の場所を設定できます。WebDAVを許可しているときは、サイトが稼動中でも、ユーザはこれらの「保護領域」に対して表示または変更を行うことができます。保護領域の作成とアクセス権の割り当てについて詳しくは、149ページの「WebDAVの保護領域とアクセス権を理解する」を参照してください。

「アクセス」パネルを表示するときは、「Web サービス」をクリックし、「Web サービスを設定」を選び、「サイト」タブをクリックします。「追加」をクリックするか、あるいはサイトを選んでから「編集」または「複製」をクリックします。次に、「アクセス」タブをクリックします。



保護領域を選んで「編集」または「複製」をクリックするか、あるいは「追加」をクリックし、次の図に表示されたパネルを使って新しい保護領域を定義します。



保護領域名

ユーザがログインしたときに表示される名前を入力します。デフォルトの保護領域名はWebサイトの名前です。保護領域には、固有の名前を使用することをお勧めします。

フォルダ

アクセスを制限したいWebサイト内の場所へのパスを入力します。ファイルサービスが稼動中の場合、またはサーバで「Server Admin」を使用している場合は、「選択」をクリックして目的の場所を参照することができます。

全員

このチェックボックスをクリックし、全員に設定したいアクセスレベルを選びます（全員とは、Webサイトにアクセスできる任意のユーザです）。「ブラウズ可能」または「ブラウズとオーサリング可能」のいずれかを選びます。選択したアクセスレベルに応じて、その他の設定を選びます。

- このチェックボックスにチェックマークを付け、「ブラウズ可能」を選んだ場合は、「オーサリングもできるユーザとグループ」リストが下に表示されます。このリストを使って、特定のユーザにオーサリングの許可を設定します。
- このチェックボックスにチェックマークを付け、「ブラウズとオーサリング可能」を選んだ場合は、追加設定するアクセス権がないため、「ユーザとグループ」リストが隠されます。
- このチェックボックスにチェックマークを付けない場合は、ポップアップメニューが使用できなくなり、「ブラウズとオーサリングができるユーザとグループ」リストが下に表示されます。このリストを使って、特定のユーザにブラウズまたはオーサリングの許可を設定します。

ユーザとグループ

このリストを使用して、特定のユーザにブラウズとオーサリングの許可を与えることができます。このリストは、全員にブラウズの許可を設定したときか、または全員にアクセス権を設定しなかったときに表示されます。「Mac OS X Server」の「ユーザとグループのリスト」からこのリストにユーザまたはグループの名前をドラッグしない限り、リストには何も表示されません。

オーサリングを許可

ユーザまたはグループに保護領域に対するオーサリングの許可を与えるときは、このオプションを選びます。

削除

この保護領域への特定のユーザまたはグループのアクセスを拒否するときは、「ユーザとグループ」リストから該当する名前を選び、このボタンをクリックします。

Web サイトのセキュリティの設定

サイトの設定ウインドウの「セキュリティ」パネルでは、各 Web サイトに対して安全なトランザクションを設定し、使用可能にすることができます。「セキュリティ」パネルを表示するときは、「Web サービス」をクリックし、「Web サービスを設定」を選び、「サイト」タブをクリックします。「追加」をクリックするか、あるいはサイトを選んでから「編集」または「複製」をクリックします。次に、「セキュリティ」タブをクリックします。SSL（Secure Sockets Layer）サービスの設定について詳しくは、142 ページの「SSL（Secure Sockets Layer）サービスを設定する」を参照してください。

Secure Socket Layer (SSL) を使用する

各 Web サイトで SSL を使用するときは、このオプションを選びます。「Web サービスを設定」ウインドウの「一般」パネルで、Web サービス全体で SSL サポートが有効になっていることを確認してください。

証明書ファイルを編集

このボタンをクリックし、証明書ファイルの内容を入力します。証明書ファイルとは、認証局から与えられたセキュアサーバ ID が記載されている「server.crt」という名前のファイルです。次のディレクトリにあります。

/etc/httpd/ssl.crt/

キーファイルを編集

このボタンをクリックし、キーファイルの内容を入力します。キーファイルとは、証明書署名要求（CSR：Certificate Signing Request）を生成したときに設定した「key.pem」という名前のファイルです。

CA 証明書ファイルを編集

このボタンをクリックして、認証局から受け取った CA 証明書ファイルの内容を入力します。（このファイルは必要に応じて認証局から受け取ります。詳しくは、142 ページの「SSL（Secure Sockets Layer）サービスを設定する」を参照してください。）

パスフレーズ

CSR の作成時に設定した SSL パスフレーズを入力するときは、このボタンをクリックします。パスフレーズは、サーバの証明書キーのロックを解除します。

SSL ログファイル

SSL イベントを記録するログファイルの場所と名前を入力します。ファイルサービスが稼動中の場合、またはサーバで「Server Admin」を使用している場合は、「選択」をクリックして目的のファイルを検索することができます。

Web サービスに関する上手な使いかたとヒント

Web サービスの性能を最適化したり、セキュリティホールを回避したり、Web サービスの管理方法をカスタマイズしたりする場合、さまざまな方法があります。このセクションでは、Web サービスを始めるにあたって役立つ情報を提供し、基本操作よりもさらに詳しい操作について説明します。

固定接続を使ってサーバの性能を向上させる

通常、HTTP 要求と応答では、それぞれ別の TCP 接続が使用されます。クライアントコンピュータがサーバに要求を送信すると、サーバは接続を開き、要求を受信してから、接続を閉じます。要求に応答するために、サーバは別の接続を開き、応答してから、接続を閉じます。このように繰り返し接続を開いたり閉じたりするのは、効率的でない上、性能が低下します。

固定接続を使用すると、サーバが、1つの接続で複数のトランザクションを処理できるようになります。サーバとクライアントコンピュータの両方が固定接続に対応している必要があります。（一般的なブラウザは固定接続に対応しています。）固定接続が機能するためには、送信されている情報のサイズが分かっている必要があります。たとえば、画像ファイルおよび更新されないHTMLページの長さは事前に分かります。CGI（Common Gateway Interface）スクリプトおよび動的に生成されるHTMLページの場合は、その長さを事前に知ることはできません。

固定接続で発生可能な要求の数を制限できます。ゼロを設定すると、1つの接続あたりに許可される要求の数は制限されなくなります。しかし、デフォルト設定の500を使うと、性能が向上します。

Webモジュールを使用する

モジュールは、Apacheの Webサーバソフトウェア用の「プラグイン」で、Webサイトに機能を追加します。Apache には標準的なモジュールが付属しています。そのほかのモジュールは、ソフトウェアメーカーから購入したり、インターネットからダウンロードすることができます。利用可能なApacheモジュールについては、次のWebサイトを参照してください。

- www.apache.or.jp/jdocs/mod/

サーバにインストール済みのWebモジュールのリストを表示するときは、「Server Admin」で「Webサービス」をクリックし、「Webサービスの状況を表示」を選びます。

モジュールをインストールするときは、モジュールソフトウェアに付属のマニュアルの指示に従って操作します。Webサーバは次のディレクトリからモジュールをロードします。

/usr/libexec/httpd/

また、新しいモジュールをロードして追加するためには、「httpd.conf」ファイルを変更する必要があります。

Macintosh固有のモジュール

「Mac OS X Server」の Web サービスでは、Macintosh に固有のモジュールがインストールされます。このセクションでは、これらのモジュールについて説明します。

mod_macbinary_apple

このモジュールによって、ファイルがMacBinaryフォーマットでパッケージ化されます。このフォーマットを使うと、Macintosh ファイルを Web サイトから直接ダウンロードすることができます。ユーザは、ファイルのアクセスに使用する URL に「.bin」を追加することによって、通常の Web ブラウザで MacBinary ファイルをダウンロードできます。

mod_sherlock_apple

このモジュールによって、Apache は、「Sherlock」を使った関連性のランキングに基づくWebサイトの検索を実行できます。「Sherlock」を使ってサイトのインデックスを作成すると、Webサイトを検索するためのフィールドをユーザに提供できます。サイトのURLには「.sherlock」を追加する必要があります。

mod_auth_apple

このモジュールによって、Web サイトでは、サーバの検索ポリシーにあるディレクトリサービスドメインでユーザを検索して、そのユーザを認証できるようになります。認証を使用している場合、Web サイト利用者は、サイト内の情報にアクセスするときにユーザ名とパスワードを要求されます。

mod_redirectacgi_apple

このモジュールを「ACGI Enabler」アプリケーションと共に使用することによって、ユーザは、ACGI プログラム（Mac OS CGI）を実行できるようになります。ACGI を使用可能にするには、管理者としてログインし、「ACGI Enabler」アプリケーションを開きます。アプリケーションからログアウトしないでください。ACGI を使用するためにはこのアプリケーションを稼動させておく必要があります。

mod_hfs_apple

このモジュールを使用すると、ユーザは、HFS ボリュームの URL を入力するときに大文字と小文字を正しく区別しなければならなくなります。このモジュールによって、大文字と小文字が区別されないボリュームのセキュリティを高めることができます。この制限をボリュームに適用すると、大文字と小文字を間違えてボリュームの URL を指定したユーザには、URL が見つからなかったことを示すメッセージが表示されます。

オープンソースのモジュール

「Mac OS X Server」には、一般的なオープンソースモジュールが付属しています。付属しているモジュールには、Tomcat、PHP: Hypertext Preprocessor、mod_perl、および MySQL があります。

Tomcat

Java によく似たスクリプト機能を使用する「Tomcat」モジュールは、Java Community Process で開発された、相互に補足的な次の 2 つのテクノロジーの公式なリファレンスインプリメンテーションです。

- Java Servlet 2.2。Java Servlet APIの仕様については、次のサイトを参照してください。
  java.sun.com/products/servlets
- JavaServer Pages 1.1。このAPIの仕様については、次のサイトを参照してください。
  java.sun.com/products/jsp

「Tomcat」を使用したい場合は、まずこれを起動する必要があります。次のように操作します。

1. 「/private/etc/httpd/httpd.conf」を開きます。
2. 「Tomcat」サーバの設定に関する行のコメントを解除するか、ファイルの最後に次の行を追加します：

```
LoadModule jserv_module /usr/libexec/httpd/mod_jserv.so
AddModule mod_jserv.c
Include /private/etc/httpd/tomcat.conf
```

3. 「Server Admin」を使って、「/usr/webapps/ROOT」を指す仮想ホストサイトを作成します。
4. 「Terminal」アプリケーションを開き、次を入力して、「Tomcat」を起動します。

```
/usr/bin/tomcat.sh start
```

5 Web ブラウザを使ってサイトの URL を入力し、「Tomcat」が予期する通りに動作するかどうかを確認します。(URL は次のようになります。「example.com」はサイトのドメイン名になります。)

```
http://www.example.com/
```

「Tomcat」の説明といくつかの例については、「/etc/httpd/tomcat.conf」を参照してください。

PHP：Hypertext Preprocessor

PHP を使用すると、C によく似た HTML 埋め込み型のスクリプト言語をサーバ側で使用することによって、動的な Web コンテンツを処理することができます。Web 開発者は、PHP コードを HTML コードに埋め込みます。この方法によって、プログラマは、HTML を生成するプログラムを作成するのではなく、HTML スクリプトに動的なロジックを直接統合することができます。

PHP は CGI 機能を備えており、広い範囲にわたるデータベースをサポートします。クライアントサイドの JavaScript とは異なり、PHP コードはサーバ上で実行されます。

このモジュールについて詳しくは、www.php.gr.jp を参照してください。

mod_perl

このモジュールによって完全な Perl インタプリタが「Mac OS X Server」に統合されるので、既存の Perl CGI スクリプトを変更せずに実行できます。この統合によって、スクリプトは高速に実行され、使用するシステムリソースは少なくて済みます。このモジュールについて詳しくは、perl.apache.org を参照してください。

MySQL

MySQL は、Web サーバのリレーショナルデータベース管理のソリューションを提供します。このモジュールを使用すると、異なるテーブルまたはデータベース内のデータを連結し、Web サイトに情報として提供することができます。このモジュールについて詳しくは、www.mysql.com を参照してください。

CGI（Common Gateway Interface）スクリプトを使用する

ユーザが Web サイトに接続すると、通常は、更新されない html ページまたは画像を受信します。CGI（Common Gateway Interface）スクリプト、つまり CGI プログラムを使用すると、Web サイトにサービスを提供するアプリケーションと Web サイトとの間で情報をやり取りすることによって、Web サイトに動的な機能を追加できます。たとえば、ユーザがサイトのフォームに必要事項を記入した場合に、CGI を使ってそのデータを処理するアプリケーションにメッセージを送信し、ユーザに応答を送り返すことができます。「Mac OS」の CGI は、通常は AppleScript にしますが、アプリケーションにすることもできます。

また、CGI は単独でカスタム機能を実行することもできます。たとえば、ユーザが Web サイトにアクセスするたびに利用者数を生成し、動的に生成した数を Web ページに挿入できます。

CGI を使用するときは、次のように操作します。

手順 1：CGI をインストールする

以下の場所のいずれかに CGI をインストールします。

1 つのサイト用： Web サイトの「Documents」フォルダに CGI をインストールします。CGI の名前の末尾に「.cgi」を付けます。「Documents」フォルダに CGI をインストールする場合は、サイトで CGI の実行を許可する必要があります。

すべてのサイト用：「/Library/WebServer/CGI-Executables」フォルダに CGI をインストールします。サイトで CGI を実行できるようにするには、サイトの URL に /cgi-bin/ を含める必要があります。CGI の実行を許可する必要はありません。インストールされていれば、実行されます。

手順 2：サイトの CGI の実行を許可する

「Server Admin」で「Web サービス」をクリックし、「Web サービスを設定」を選び、「サイト」タブをクリックします。リストから Web サイトを選択し、「編集」をクリックします。次に、サイトの設定ウインドウの「一般」パネルで「CGIの実行を許可する」を選びます。

手順 3：Web サービスを再起動する

変更を適用するために、Web サービスを停止してから、再び開始する必要があります。

MIME（Multipurpose Internet Mail Extension）を理解する

MIME（Multipurpose Internet Mail Extension）とは、Web ブラウザが特定の特性を持つファイルを要求したときに、どのように動作するかを指定するためのインターネットの規格です。Web サーバの応答は、ファイルの拡張子に基づいて選ぶことができます。選ぶことのできる応答は、Webサーバにインストールしたモジュールによって異なります。ファイル拡張子とそれに関連付けられている応答との各組み合わせを、MIME タイプマッピングと呼びます。

MIME の拡張子

拡張子は、ファイル内のデータの種類を表します。以下に例を示します。

- txt は、テキストファイルです
- cgi は、CGI（Common Gateway Interface）ファイルです
- gif は、GIF（画像）ファイルです
- au は、サウンドファイルです
- tiff は、TIFF（画像）ファイルです

「Mac OS X Server」では、MIME タイプの拡張子のデフォルトのリストがインストールされます。必要な拡張子がリストにない場合は、「Server Admin」を使って拡張子をリストに追加できます。

Web サーバの応答

ファイルが要求されると、Web サーバはファイルの拡張子に指定されている応答を使用してファイルを処理します。応答は、動作または MIME タイプのいずれかになります。可能な応答には、以下のものがあります。

- MIME タイプでファイルを返す（返したいマッピングを入力します）
- send-as-is（ファイルをそのままの状態で送信します）
- cgi-script（指定した CGI スクリプトを実行します）
- imap-file（IMAP メールメッセージを生成します）
- mac-binary（MacBinary フォーマットで圧縮されたファイルをダウンロードします）

MIME タイプマッピングは、「text/plain」のように、スラッシュで 2 つのサブフィールドに分けて示します。「Mac OS X Server」には、デフォルトの MIME タイプマッピングのリストが付属しています。これらの MIME タイプマッピングを編集したり、ほかの MIME タイプマッピングを追加したりできます。

応答として MIME タイプを指定すると、サーバは、要求されたデータのタイプを識別し、指定された応答を送ります。たとえば、拡張子に「jpg」の付いたファイルをブラウザが要求し、「jpg」に関連付けられた MIME タイプマッピングが「image/jpeg」である場合、サーバは、画像ファイルを送る必要があり、画像フォーマットが JPEG であることを知ることができます。サーバは、要求されたデータを提供する以外は何もする必要がありません。

動作は、別の方法で処理されます。拡張子に動作をマップすると、サーバは、プログラムまたはスクリプトを実行し、その結果を要求元のブラウザに提供します。たとえば、拡張子に「cgi」の付いたファイルをブラウザが要求し、「cgi」に関連付けられた応答が「cgi-script」という動作である場合、サーバは、スクリプトを実行し、その結果のデータを要求元のブラウザに送り返します。

MIME タイプエディタ

「Server Admin」で MIME タイプを作成し、それをサーバの応答にマップできます。「MIME タイプエディタ」を表示するときは、「MIME タイプ」パネルの「追加」をクリックするか、または既存の MIME タイプを選んで「編集」をクリックします。このエディタの図を次に示します。

SSL（Secure Sockets Layer）サービスを設定する

ユーザが Web サイトから商品を購入できるようにする場合などに、サーバでのトランザクションをセキュリティで保護するときは、SSL（Secure Sockets Layer）保護を設定します。SSL を使うと、暗号化された認証済みの情報をインターネット経由で送信できます。たとえば、Web サイトでクレジットカードのトランザクションを実行可能にしたいときに、サイトで送受信される情報を保護することができます。

証明書署名要求（CSR：Certificate Signing Request）を生成すると、認証局から証明書が送られてきます。この証明書はサーバにインストールします。また、CA 証明書（ca.crt）が送られてくることもあります。このファイルは、任意でインストールします。通常、CA 証明書は、「Internet Explorer」などのクライアントアプリケーション側に置かれ、サーバの証明書が正しい機関から発行されたものであることの確認に使用されます。ただし、CA 証明書の期限が切れたり、更新されたために、一部のクライアントアプリケーションで最新の状態になっていない可能性があります。

SSL を設定するときは、以下の手順に従って操作します。

手順 1：サーバ用の証明書署名要求（CSR）を生成する

証明書署名要求（CSR：Certificate Signing Request）とは、サーバの証明書の作成に必要な情報が含まれているファイルです。

サーバ用の CSR を生成するときは、次のように操作します。

1. ルートパスワードを使ってサーバにログインし、「Terminal」アプリケーションを開きます。
2. プロンプトで以下のコマンドを入力し、各コマンドの最後で return キーを押します。

```
cd
openssl md5 * > rand.dat
openssl genrsa -rand rand.dat -des 1024 > key.pem
```

3. 次に表示されるプロンプトでパスフレーズを入力し、return キーを押します。

   作成するパスフレーズは、サーバの証明書キーのロックを解除します。Web サーバで SSL を使用可能にするときに、このパスフレーズを使用します。

4. 次の名前のフォルダがサーバにない場合は作成します。

   /etc/httpd/ssl.key/

   手順 2 で作成した「key.pem」ファイルのコピーを作成し、"server.key" に名前を変更します。その後、「server.key」をこのフォルダにコピーします。

5. プロンプトで次のコマンドを入力し、return キーを押します。

```
openssl req -new -key key.pem -out csr.pem
```

6. 入力を求められたら、以下の情報を入力します。
   - 国： 組織の所在地の国名です。
   - 都道府県： 都道府県名を完全表記で入力します。
   - 地域名： 組織の所在地の市区町村名です。
   - 組織名： ドメイン名が登録されている組織の名前でなければなりません。
   - 部門： 通常、部署などの名前です。
   - Web サーバのコモンネーム： server.apple.com などの DNS 名です。
   - メールアドレス： 証明書を受信するメールアドレスです。

   「csr.pem」ファイルは、提供した情報に基づいて生成されます。プロンプトで次のコマンドを入力し、return キーを押します。

```
cat csr.pem
```

「cat」コマンドによって、手順 5 で作成したファイル（「csr.pem」）の内容が一覧表示されます。「Begin Certificate Request」という言葉の後に暗号メッセージが表示されます。メッセージは「End Certificate Request」で終わります。この部分が証明書署名要求（CSR：Certificate Signing Request）です。

手順 2：Web サイト証明書を入手する

各 Web サイトの証明書を、発行機関から購入する必要があります。

証明書を購入するときは、以下の点に注意してください。

- 自分の所属する組織が登録者として InterNIC に登録しているドメイン名を提供する必要があります。
- ソフトウェアメーカーの選択を求められたら、「Apache Freeware with SSLeay」を選びます。
- すでに証明書署名要求（CSR：Certificate Signing Request）を生成済みなので、CSR を求められたときに、テキストエディタで CSR を開き、CSR ファイルの内容をコピーして発行機関の Web サイトの適切なテキストフィールドにペーストします。

処理が完了すると、セキュアサーバ ID が含まれているメッセージを受信します。このメッセージがサーバ証明書です。証明書を受信したら、「server.crt」という名前のファイルとして Web サーバのハードディスクに保存します。

手順 3：サーバに証明書をインストールする

1. サーバにルートとしてログインします。
2. 次の名前のフォルダがサーバにない場合は作成します。

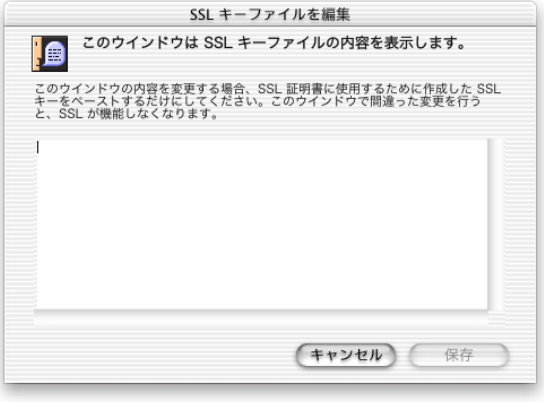
   /etc/httpd/ssl.crt/
3. 「server.crt」（セキュアサーバ ID を含むファイル）をフォルダにコピーします。

手順 4：サイトで SSL を使用可能にする

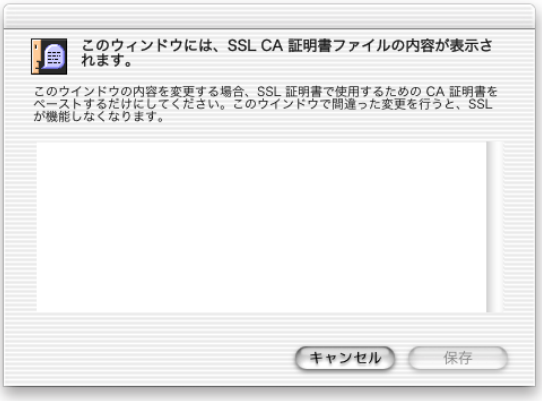
1. 「Server Admin」で「Web サービス」をクリックし、「Web サービスを設定」を選びます。
2. サイト全体に対して「SSL を使用する」が選択されていることを確認します。
3. 「サイト」をクリックし、証明書を使用するサイトを選んで、「編集」をクリックします。
4. 「Secure Socket Layer (SSL) を使用する」を選びます。

5 「証明書ファイルを編集」をクリックし、証明書ファイル（発行機関から入手した証明書）のテキストをテキスト フィールドにペーストします。次に、「保存」をクリックします。

6 「キーファイルを編集」をクリックし、キーファイル（前に作成した「key.pem」ファイル）のテキストをテキスト フィールドにペーストします。次に、「保存」をクリックします。



7 「CA証明書ファイルを編集」をクリックし、「ca.crt」ファイルのテキストをテキストフィールドにペーストします。（「ca.cert」ファイルは、認証局から必要に応じて受け取るファイルです。）「保存」をクリックします。



8 tab キーを押して「パスフレーズ」フィールドに移動し、CSR のパスフレーズを入力して、「保存」をクリックします。

9 SSL トランザクションを記録するログファイルの場所を設定し、「保存」をクリックします。

10 Web サービスを停止してから開始します。

サービスの状況と性能を監視する

Web サービスでは、サーバの状況を監視し、効率的に稼動させるために利用できる便利なツールが 3 つ用意されています。アクセスログ、エラーログ、および状況ウインドウです。

アクセスログとエラーログ

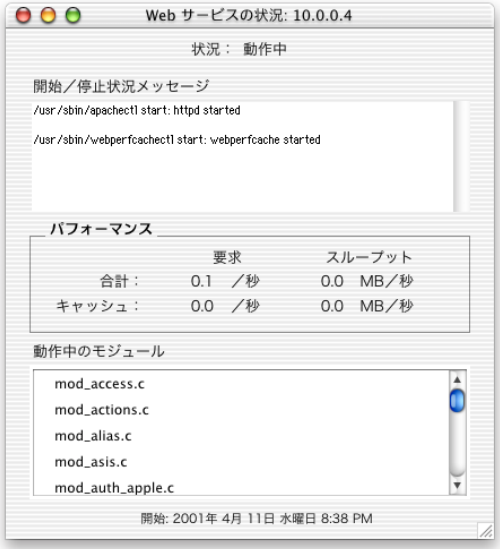
Web サービスのアクセスログとエラーログは「Server Admin」を使用して遠隔地から表示できます。「ログビューア」をクリックし、「Web サービス」を選んで、ポップアップメニューから「access.log」または「error.log」を選びます。Web サイトのサイズおよび目的によっては、ログに大量の項目が記録される可能性があります。「Mac OS X Server」の Web サービスでは、標準の Apache ログフォーマットが使用されているので、他社製のどのログ分析ツールを使用してもこのログデータを解釈できます。サイトの設定ウインドウの「ログ」パネルで、ログファイルの保存場所を指定できます。ログファイルのデフォルトの場所は、「/var/log/httpd/」です。

状況ウインドウ

また、サーバの状況は、「Server Admin」の「Web サービスの状況」ウインドウでも監視できます。このウインドウを開くときは、「Web サービス」をクリックし、「Web サービスの状況を表示」を選びます。「Web サービスの状況」ウインドウには、サーバとパフォーマンスキャッシュの現在の状態が表示されます。Web サービスが稼動していない場合は、ウインドウに「状況：停止中」というメッセージと、サーバが停止した日時が表示されます。

Web サービスが稼働中の場合、下のようなウインドウが表示されます。サーバの状況に関するメッセージが、「開始／停止状況メッセージ」フィールドに表示されます。メッセージの意味については、Apache の Web サイトを参照してください。

現在の要求と現在のスループットには、Apache とパフォーマンスキャッシュの両方のデータが含まれています。パフォーマンスキャッシュの要求とスループットには、パフォーマンスキャッシュのデータのみが含まれています。



Apache の詳しい設定

熟練した Apache Web 管理者の場合は、Apache の設定ファイル「httpd.conf」を変更することで Web サービスを設定できます。変更点が多い場合は、「Server Admin」ではなく、Apache の設定ファイルだけを使って Web サービスを設定してください。

「Server Admin」で行う設定（命令）は、「Server Admin」の設定ファイル「httpd_macosxserver.conf」に書き込まれます。重複または矛盾した設定をしないように、Apache の設定ファイルでは、「Server Admin」で指定できる命令および設定の先頭にシャープ記号（#）が付いています。Apache は、先頭にシャープ記号が付いている命令を無視します。

たとえば、固定接続（KeepAlive）の命令が、Apache の設定ファイル（「httpd.conf」）で次のように示されているとします。

```
#KeepAlive Off
```

しかし、「Server Admin」で固定接続を使用可能にすると、「httpd_macosxserver.conf」ファイルには、次の命令が示されます。

```
KeepAlive On
```

Apache の設定ファイルでは「使用不可」の指示の先頭にシャープ記号が付いているので、矛盾は起こりません。Apache は、「Server Admin」の設定ファイルに示されている指示だけを読み取ります。

重要 「Server Admin」で使用される設定は、すべて「httpd.conf」ファイルに記述されており、その先頭にシャープ記号（#）が付いています。これらは変更しないでください。変更すると Web サービスで予期しない結果が生じることがあります。

> 警告 どのような場合でも、「httpd_macosxserver.conf」ファイルは変更しないでください。

Apache およびその使いかたについて詳しくは、Apache の Web サイト（www.apache.or.jp）を参照してください。

動的な Web ページのキャッシュを無効にする

サイトに動的な Web ページ（CGI スクリプトで生成されたページや、頻繁に更新されるデータベースなど）がある場合は、これらのページがキャッシュに保持されないようにする必要があります。キャッシュに保持されていると、サイトで古い情報や誤った情報を提供してしまう可能性があります。

Web サーバは、サーバ上のどの HTML ファイルにも、キャッシュ内での有効期限を示すタグが自動的に追加されるように設定されています。デフォルトでは、キャッシュ内において、HTML ページは 1 秒で、GIF ファイルは 1 時間で期限切れになります。

サイトで古い情報や誤った情報が提供されているときは、次のいずれかの対策を実行します。

- 「Server Admin」の「Web サービスを設定」ウインドウでパフォーマンスキャッシュが有効になっていないことを確認します。
- CGI スクリプト（または動的な HTML ページを生成するプログラム）を変更して、動的な HTML ページのそれぞれのソースに「Cache-Control: no-cache」タグが追加されるようにします。
- 「httpd.conf」ファイルで、GIF ファイルがキャッシュされていなかどうかを確認します。

GIF ファイルがキャッシュされている場合は、「httpd.conf」ファイルを変更してキャッシュを中止できます。そのためには、次のように操作します。

1. テキストエディタで「httpd.conf」ファイルを開きます。
2. 次の行を見つけます。

```
ExpiresByType image/gif A3600
```

このコマンドは、GIF ファイルに 1 時間（3600 秒）のキャッシュ期間を割り当てるように Web サーバに指示します。

3 次に示すように、行の先頭にシャープ記号（#）を挿入します。

```
#ExpiresByType image/gif A3600
```

シャープ記号を挿入すると、「Server Admin」では GIF ファイルをキャッシュする指示が無視されるため、GIF ファイルはキャッシュされなくなります。

4 Web サービスを再起動します。

WebDAV の保護領域とアクセス権を理解する

WebDAV を使って Web サイトでライブオーサリングを提供する場合は、保護領域を作成し、ユーザのアクセス権を設定する必要があります。運用している各サイトは、多数の保護領域に分割し、それぞれにブラウズまたはオーサリングのアクセス権を持つユーザとグループを設定できます。Web サイトをインターネット上に公開する場合は、保護領域は必要ないかもしれません。

保護領域を定義する

保護領域（通常はフォルダ、つまりディレクトリ）を定義すると、保護領域に設定したアクセス権はそのディレクトリの内容すべてに適用されます。既存の保護領域内のフォルダのいずれかに新しい保護領域を定義した場合、新しい保護領域のアクセス権はそのフォルダおよび内容のみに適用されます。保護領域の作成とアクセス権の設定について詳しくは、134 ページの「Web サイトのアクセスの設定」を参照してください。

WebDAV のアクセス権を設定する

サーバで実行する Apache のプロセスでは、Web サイトのファイルとフォルダにアクセスする必要があります。このために、「Mac OS X Server」によって、Apache プロセスが属する「www」というグループがサーバの「ユーザとグループのリスト」にインストールされます。この www グループには、Web サイトのファイルへの読み出しのアクセス権を与える必要があります。これよって、ユーザがサイトに接続したときに、www グループが Web サイトのファイルをブラウザに転送できるようになります。WebDAV を使用する場合、www グループには Web サイト内のファイルおよびフォルダへの書き込みのアクセス権も必要になります。

Web サービスに関する問題を解決する

ユーザがサーバ上の Web サイトに接続できない場合：

- Web サービスが開始しており、サイトが使用可能であることを確認します。
- 「Web サービスの状況」ウインドウの「開始／停止状況メッセージ」フィールドでメッセージを確認します。メッセージの意味については、Apache の Web サイト（www.apache.or.jp）を参照してください。
- ユーザが正しい URL を入力して Web サーバに接続していることを確認します。
- デフォルトの Web フォルダとして正しいフォルダが選択されていることを確認します。デフォルトの書類のページとして正しい HTML ファイルが選択されていることを確認します。
- Web サイトが特定のユーザに制限されている場合は、このユーザが Web サイトへのアクセス権を持っていることを確認します。

- ユーザのコンピュータで TCP/IP が正しく設定されていることを確認します。TCP/IP 設定に問題がないと思われる場合は、ネットワーク接続を確認できる「PING」ユーティリティを使用してください。
- DNS に問題がないことを確認します。DNS 名の代わりにサーバの IP アドレスを使って接続してみます。
- Web サイトの IP アドレスとドメイン名が DNS サーバに正しく登録されていることを確認します。

Web モジュールが予想通りに動作しない場合：

- モジュールが正しく動作しない原因について、「ログビューア」のエラーログを確認します。
- モジュールが Web サーバに付属していた場合は、そのモジュールについて Apache の説明書を確認し、モジュールの動作仕様が自分の予想と同じであることを確認します。
- モジュールを自分でインストールした場合は、Web モジュールに付属していた説明書を確認し、モジュールが正しくインストールされており、使用しているサーバソフトウェアとの互換性があることを確認します。

「Mac OS X Server」でサポートされる Apache のモジュールについて詳しくは、次の Web サイトを参照してください。www.apache.or.jp/jdocs/mod/

CGI が動作しない場合：

- CGI のコードを調べて、CGI が実行可能ファイルとして指定されていることを確認します。これが指定されていない場合は、「Server Admin」で CGI の実行が可能になっていても、CGI はサーバで実行されません。
- CGI のコードを調べて、適切なアクセス権が与えられていることを確認します。「Mac OS X Server」では、Apache プロセスが属する「www」というグループがサーバの「ユーザとグループ」リストにインストールされます。CGI に対する適切なアクセス権（読み出し専用、または読み出し／書き込み）を www グループに与える必要があります。

Web サービスの仕様

同時接続の最大数	技術的な制限はありません。最大数は、お使いのハードウェアの処理能力およびサーバソフトウェアの設定によって異なります。
サポートする規格	HTTP1.1 以前の規格に完全に対応しています。
ネットワークサービスのサーバ名の長さの最大値	NSL（Network Service Locator）によって決まります。
アイドル状態接続のタイムアウト	60 秒（再設定できます）
CGI のタイムアウト	60 秒
Web サービスのポート番号	80（再設定できます）

Web サービスに関するその他の情報

設定ファイルおよび Apache Web サービスのその他の要素については、次の参考文献を参照してください。

- 「Apache: The Definitive Guide」第 2 版、Ben Laurie、Peter Laurie 共著（O'Reilly and Associates 社発行、1999 年）
- 「Writing Apache Modules with Perl and C」、Lincoln Stein、Doug MacEachern 共著（O'Reilly and Associates 社発行、1999 年）
- 「Web Performance Tuning」、Patrick Killelea 著（O'Reilly and Associates 社発行、1998 年）
- 「Web Security & Commerce」、Simson Garfinkel、Gene Spafford 共著（O'Reilly and Associates 社発行、1997 年）
- Apache について詳しくは、Apache の Web サイトを参照してください。 www.apache.or.jp
- WebDAV クライアントで使用するメソッドの包括的なリストについては、「RFC 2518」を参照してください。RFC ドキュメントには、プロトコルやサービスの概要が記載されていて、サーバの管理を始めたばかりの方にとって参考になります。また、詳細な技術情報も記載されているので、経験豊富な管理者にとっても参考になります。RFC ドキュメントは、次の Web サイトで番号で検索することができます。
  www.faqs.org/rfcs

8

メールサービス

メールサービスとは？

「Mac OS X Server」のメールサービスによって、ネットワークやインターネットを経由するメールサービスを、ユーザに提供することができます。インターネットを経由してユーザがメールを送受信できるようにしたい場合、すべての標準規格のインターネットメールプロトコルを使って、メールサービスを設定できます。IMAP（Internet Message Access Protocol）、POP（Post Office Protocol）、および SMTP（Simple Mail Transfer Protocol）が、そのプロトコルです。

標準的なメールの設定では、ローカルサーバにおいて SMTP を使ってメールを送信し、POP と IMAP を使ってメッセージを受信します。この 3 つのプロトコルについて、以下に説明します。

POP（Post Office Protocol）

POP（Post Office Protocol）はメールの受信時に使用されるプロトコルです。メールの送信時には使用されません。POPは共有サーバにメールを配送します。ユーザのコンピュータは定期的にサーバに接続し、待機中のすべてのメールをダウンロードします。ユーザがメールをダウンロードすると、メールはユーザのコンピュータにだけ保存されます。ユーザはサーバとの接続を解除して、メールを読んだり、整理したり、返信したり、または新しいメールを作成したりできます。POP は、メールを保管し、特定のアドレスにメールを配送するという点で、郵便局に似ています。

ユーザがメールをダウンロードすると、そのメールを保存する必要がないことが、POP の 1 つの利点です。このためサーバは、IMAP プロトコルを使用するときほど多くの保管場所を必要としません。ただし、メールはサーバから取り除かれてしまうため、クライアントコンピュータのハードディスクが壊れて、メールファイルを失ってしまった場合には、データのバックアップを使用しない限り、これらのファイルを回復する手段はありません。

クライアントユーザが、自宅、会社、携帯機器で外出先からなど、異なる場所からメールにアクセスする場合、POP は必ずしも最適な手段ではありません。ユーザがメールを読むと、そのメールはサーバからダウンロードされ、完全にサーバから取り除かれます。ユーザが後で別のコンピュータからログインしても、以前に読んだメールを読むことはできません。

IMAP（Internet Message Access Protocol）

IMAP（Internet Message Access Protocol）はクライアント／サーバ対応のメールプロトコルで、ユーザはインターネット上のどの位置からでも自分のメールにアクセスすることができます。ユーザは、さまざまな業界標準のインターネットメールアプリケーションや、IMAP 準拠のメールクライアントを使って、メールを送受信することができます。

IMAP の場合、クライアントユーザのメールはサーバ上のリモートメールボックスに保存されます。メールは、まるでユーザのローカルコンピュータ上にあるかのように、ユーザに対して表示されます。IMAP は、POP と同じようにメールをサーバに配送します。ただし、ユーザがメールを削除するまで、サーバからメールが取り除かれることはありません。

IMAP は、一般的なクライアント／サーバモデルによく似ています。つまり、ユーザのコンピュータは、サーバに対して、指定のメッセージのヘッダや本文を要求したり、特定の条件を満たすメッセージを検索したりできます。これらのメッセージは、ユーザがメッセージを開くとダウンロードされます。

SMTP（Simple Mail Transfer Protocol）

SMTP（Simple Mail Transfer Protocol）は、メールを送信および転送するときに使用される TCP/IP プロトコルです。受信メッセージをキューに保存する能力に限界があるため、通常はメールを送信するときだけ使用され、メールを受信するときには POP または IMAP が使用されます。

メールサービスを設定する前に

メールサービスを管理する方法は、メールサーバの構成によって異なります。ネットワーク上でのメールサービスの使用については、このセクションを参照してください。「Mac OS X」のメールサービスは、1 台または複数のサーバにインストールして実行することができます。

サーバが 1 台の場合のメールサービス

1 台のサーバがメールサービスを提供する場合、すべてのユーザは同じメールサーバにメッセージを送ります。ユーザのメールアプリケーションが、ユーザのコンピュータにメッセージをダウンロードすることを要求するまで、メッセージはサーバに保管されます。

複数のドメインが対象のメールサービス

「Mac OS X Server」を使用して、複数のドメインを対象にメールサービスを設定することもできます。たとえば、メールサービスをビル内の、それぞれ独自のドメイン名を持つ複数の会社に提供している場合、それぞれのドメインにメールサービスを設定できます。

つまり、組織内のユーザ数がメールサーバの同時ユーザ接続制限（接続の種類 —POP または IMAP— サーバの利用状況によって異なります）より多い場合、あるいはメッセージの保管容量が制限より多い場合は、複数のサーバにメールサービスを分散することが望まれます。

サーバ間でメールサービスを共有すると、パフォーマンス（メールシステムで処理できる接続とメッセージ数を含みます）を改善することができますが、「ユーザとグループ」データベース、DNS エントリ、およびメールサービスの管理により注意を払う必要があります。

複数のサーバ間でメールサービスを共有する場合、各サーバは、保管と転送の処理に関わります。各メールサーバは、接続してくるユーザ宛の受信メッセージを保管し、別のサーバに接続するユーザ宛の受信メッセージを転送します。

インターネットベースのメールサービスの MX レコード

メールサービスを設定すると、受信メールはコンピュータ（またはメールホスト）に配送され、ユーザがホストに接続して取り出すまでこのコンピュータに保存されます。また、メールホストが使用できない場合にメールを受信する代替コンピュータを設定しておく必要もあります。送信メールはユーザのコンピュータから送信メールホストに送信され、インターネット上の別のメールホストに送信されます。メールは、宛先のユーザのメールを保持するメールホストに到達するまで転送されます。

インターネットを経由するメールサービスを提供するには、ネットワーク上に DNS（Domain Name System）サービスを定義するか、インターネットサービスプロバイダから提供される DNS サービスを利用します。メールサーバは、DNS から、ほかのメールサーバの IP アドレスを取得します。インターネットを経由するメールサービスを提供する場合、メールサービスを提供するドメインごとに、適切な MX（Mail Exchange）レコードで DNS サービスを設定する必要があります。MX レコードは DNS テーブル内のエントリで、ドメインがメールを処理する方法を指定します。あるドメインに対してインターネット上の別のメールサーバがメールを配送してくる場合、メールサーバではドメインの MX レコードを要求します。そして、MX レコードに指定されているメールサーバ宛に、メールが送られます。

MX レコードの作成について詳しくは、282 ページの「DNS をメールサービスとともに使用する」を参照してください。

メールサービスを初めて設定する

手順 1：MX レコードを設定する

ユーザがインターネットを介してメールを送受信できるようにしたい場合は、DNS サービスがサーバの適切な MX レコードで設定されている必要があります。インターネットサービスプロバイダ（ISP：Internet service provider）がネットワークに対して DNS サービスを提供する場合は、ISP に連絡し、自分の MX レコードを設定してもらいます。DNS について詳しくは、280 ページの「DNS（Domain Name System）サービス」を参照してください。

手順 2：メールサービスを開始する

サーバコンピュータが、「日付と時刻」環境設定において正しい日付、時刻、時間帯、および夏時間の設定を示していることを確認します。メールサービスでは、この情報を元に各メッセージのタイムスタンプを設定します。タイムスタンプが正しくないと、ほかのメールサーバがメッセージを正しく処理できないことがあります。

この情報を確認したら、「メールサービス」をクリックし、「メールサービスを開始」を選びます。「設定アシスタント」を使用してメールサービスを開始した場合は、これをいったん停止し、再び起動して、加えた変更を反映します。

手順 3：メールサービスを設定する

メールの処理方法、使用するプロトコル、メールをサーバから削除する頻度など、メールサービスのいくつかの設定を選択する必要があります。「Server Admin」で、「メールサービス」をクリックし、「メールサービスを設定」を選びます。「メールサービスを設定」ウインドウ（以下を参照してください）には、4 つのパネルがあります。「一般」、「メッセージ」、「フィルタ」、および「プロトコル」です。各パネルをクリックし、必要な設定を選びます。これらの設定について詳しくは、158 ページの「メールサービスの設定」を参照してください。

手順 4：デフォルトのホスト設定を選ぶ

ホストとは、ユーザがメールを受信したり送信したりするドメインのことです。メールサービスがほかのホストに対してどのように動作するかについて、デフォルトの設定を選ぶ必要があります。そうするには、「Server Admin」で「メールサービス」をクリックし、「ホストを設定」を選びます。以下に示すデフォルトの「ホストを設定」ウインドウには、3 つのパネルがあります。「受信メール」、「送信メール」、および「ネットワークの設定」です。各パネルをクリックし、目的の設定を選びます。これらの設定について詳しくは、166 ページの「ホストの設定」を参照してください。

手順 5：ユーザのメールを有効にして postmaster アカウントを作成する

メールサーバは、「ユーザとグループ」の情報を使って、ユーザのメールを処理する方法を判断します。ユーザレコードを作成するときに、1 人のユーザに対してメールを設定できます。または、既存のユーザに対していつでもメールサービスを許可できます。各ユーザのメール属性を定義する方法について詳しくは、「ユーザとグループ」の章の 65 ページの「メールサービスの設定」を参照してください。

「postmaster」という名前のユーザアカウントを作成する必要もあります。メールサーバは、特定の動作を行うときにこのユーザを探します。postmaster に対してメールを許可し、postmaster 宛のメールを別のメールアカウントに転送できます。

「postmaster」という語は 10 文字ですが、ユーザ名には 8 文字までしか使用できないことに注意してください。メールサーバを設定するときは、ユーザの長い名前を使用でき、8 文字のユーザ名に制限されません。ユーザを「postmaster」という長い名前で作成し、そのユーザ名に「postmstr」といった短い名前を設定します。

メールサービスの設定

メールサービスの設定によって、サーバがメールを処理する方法を設定します。ローカルメールサーバ名、サーバによる保管メッセージおよびエラーログの処理方法、および使用するメールプロトコルやジャンクメール対策を指定できます。

メールの設定にアクセスするときは、「メールサービス」をクリックし、「メールサービスを設定」を選びます。タブをクリックして、該当するパネルの設定を確認します。以下のセクションでは、各パネルで使用できる設定について個別に説明します。

一般設定

一般設定を使用すると、自動起動を有効にし、ローカルメールサーバ名を登録することができます。

システム起動時にメールサーバを開始する

サーバの起動時にメールサービスを開始するときは、このオプションを選びます。このオプションを選ぶと、停電やその他の不測の事態が発生しても、ユーザは引き続きメールサービスを利用することができます。

ローカルメールサーバ名

このリストには、メールサーバが担当するすべてのドメイン名が含まれます。サーバ宛のメールアドレスで、「@」の後に指定されると思われる名前をすべて入力する必要があります。たとえば、リストは、ドメイン名や会社名などを表すスペルのバリエーションを含めたりします。メール設定は、このリスト内のドメイン名に対して適用されます。MX レコードが設定されている場合は、このリストに項目を追加する必要はありません。メールサーバが通常に動作する中で検出する名前が追加されます。

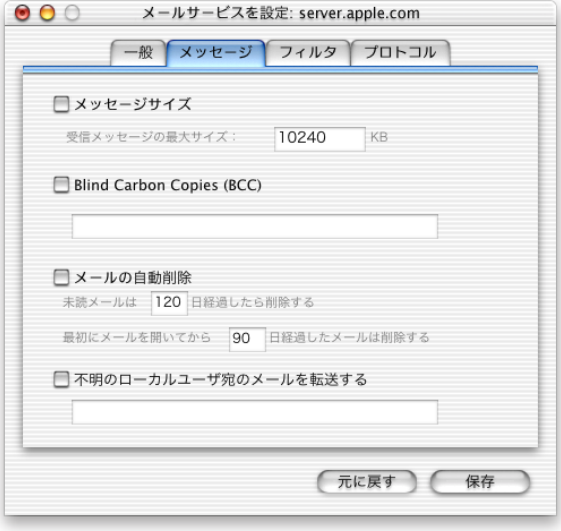
このリスト内に、MX レコードを含まないドメイン名が存在する場合、そのドメイン名はこのメールサーバによってのみ認識されます。このドメイン名に送信される外部からのメールは、送り返されます。このリストに MX レコードのないドメイン名を含める場合は、ローカル（内部）メール用としてのみ使用してください。ローカルメールとして使用する場合、時間の短縮になります。

「追加」と「取り除く」

「追加」をクリックして、メールサーバに管理させたいドメイン名をテキストフィールドに入力します。リストから名前を取り除きたい場合は、目的の名前を選び、「取り除く」をクリックします。

メッセージの設定

「メッセージ」パネルにアクセスするには、「メールサービス」をクリックして「メールサービスを設定」を選んでから、「メッセージ」タブをクリックします。このパネルでは、メッセージサイズの制限の指定、BCC と転送の設定、およびメール削除のスケジュール設定を行います。



メッセージサイズ

受信メッセージのサイズの上限を設定したい場合は、このオプションを選びます。次に、「受信メッセージの最大サイズ」欄にキロバイトの単位で値を入力します。

Blind Carbon Copies（BCC）

サーバが受信するすべてのメッセージの Bcc を指定したユーザまたはグループに送信したい場合は、このオプションを選択して、そのユーザまたはグループの名前をテキストフィールドに入力します（ユーザまたはグループの名前は、「Mac OS X Server」の「ユーザとグループ」リストからドラッグすることもできます）。グループに送信するメッセージの監視が必要な場合は、このオプションを選択します。このオプションを選ぶと、組織の規模によっては大量のメールが発生するので注意してください。

メールの自動削除

指定の時間が経過するとサーバからメールが自動的に削除されるようにしたい場合は、このオプションを選びます。次に、未読メールと既読メールのフィールドに日数を入力します。（この設定を使用しない場合は、日数を入力しないでください。）ディスク容量が問題になる場合に、このオプションを設定することをお勧めします。メールの自動削除によって、IMAP フォルダ内のメッセージを含めて、サーバからメールが永久に取り除かれます。

不明のローカルユーザ宛のメールを転送する

不明なローカルユーザ宛のメールを受信した場合に、これを組織内の別のユーザまたはグループに転送する場合は、このオプションを選びます。テキストフィールドにユーザ名またはグループ名を入力します。このユーザまたはグループが、宛先が間違っているすべてのメールを受信します。

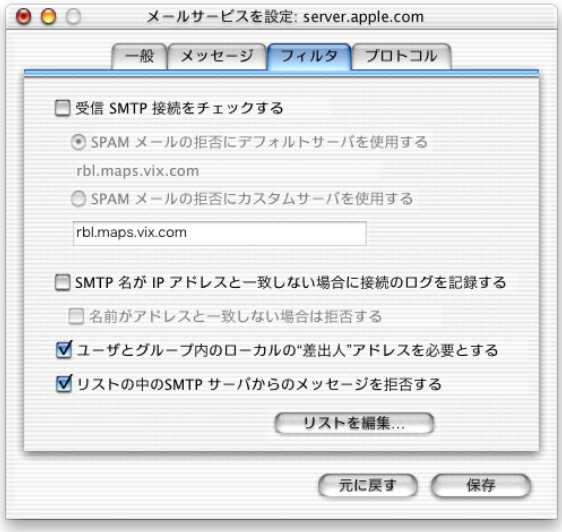
このオプションは、アドレスが間違っているメールを確実に配送する手段として使用することができます。サーバに送られてきたメールのユーザ名にスペルミスがある場合、これを送信者に送り返すのではなく、ユーザのメールボックスに手動で配送することができます。「support@examle.com」などのように、ユーザアカウントが指定されていない部門宛のメールを、その部門の通信担当者に転送することもできます。

フィルタの設定

メールサービスのフィルタ設定を設定することによって、一方的に送りつけられてくるメールの量を減らすことができます。これらのオプションのいくつかを使用可能にすると、サーバは、DNS エントリをチェックしてメッセージの送信者の IP アドレスと名前が一致するかどうかを確認するか、ORBS（Open Relay Behaviour-modification System）サーバをチェックして、メッセージが既知の「ジャンクメール」送信者から送信されたものかどうかを確認します。

これらの処理には DNS へのアクセスが含まれるので、メールサーバの性能が低下する可能性があります。

「フィルタ」パネルにアクセスするには、「メールサービス」をクリックして「メールサービスを設定」を選択し、次に「フィルタ」タブをクリックします。



受信 SMTP 接続をチェックする

受信接続を許可したり拒否したりする前に、接続要求を調べたい場合は、このオプションを選びます。このオプションを選んだ場合は、メールを拒否するのに使いたいメールサーバを指定する必要もあります。デフォルトの ORBS サーバを選ぶか、「SPAM メールの拒否にカスタムサーバを使用する」を選んでテキストフィールドにサーバ名を入力することで、別の ORBS サーバを選ぶことができます。

SMTP 名が IP アドレスと一致しない場合に接続のログを記録する

受信メッセージに IP アドレスと一致しない SMTP 名があるときは常にログ項目を作成したい場合は、このオプションを選びます。その後もメールは受信されますが、後で処理方法を決定できるように、ログに項目が書き込まれます。

名前がアドレスと一致しない場合は拒否する

一致しないメールを、ログに記録すると同時に拒否したい場合は、このオプションを選びます。

ユーザとグループ内のローカル " 差出人 " アドレスを必要とする

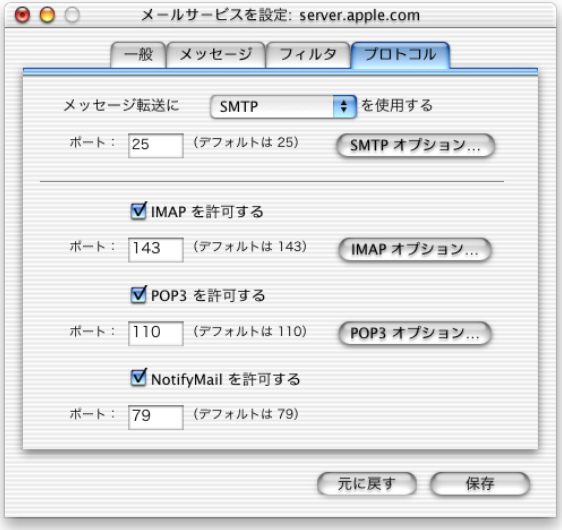
ローカルの「ユーザとグループ」リストに指定されていないアドレスからの受信メールを拒否する場合は、このオプションを選びます。たとえば、ユーザ「Someone」が someone@example.com からメールを送信する場合、「Someone」がお使いの「ユーザとグループ」リストに指定されていなければ、メールサーバはメッセージを拒否します。この設定を使用することで、サーバがジャンクメールのリレーポイントとして利用されることを防ぐことができます。リレーポイントとは、知らないうちにジャンクメッセージを受信し、別のサーバにただちに転送してしまうサーバのことです。

SMTP サーバからのメッセージを拒否する

メールを受信しない SMTP サーバのリストを作成する場合、このオプションを選びます。次に「サーバを編集」をクリックして、ドメイン名を「SMTP サーバ拒否リスト」に追加します。

プロトコルの設定

「プロトコル」パネルで、サーバで使用したいメールプロトコルを選択して設定することができます。「プロトコル」パネルにアクセスするには、「メールサービス」をクリックして「メールサービスを設定」を選んでから、「プロトコル」タブをクリックします。



メッセージ転送に _ を使用する

送信メッセージの処理方法を選びます。「SMTP」、「Sendmail」、または「なし」を選ぶことができます。「SMTP」を選ぶと「SMTP オプション」ボタンが使用可能になります。

「Sendmail」を選んだ場合、「Mac OS X」メールサーバではなく「Sendmail」が、すべての受信および送信 SMTP メールを処理します。ローカルメールサーバに送信されるすべてのメールは「Sendmail」アプリケーションが処理し、配信のために「Mac OS X」メールサーバに転送されます。POP と IMAP はそのまま通常どおり機能しますが、SMTP メールは「Sendmail」アプリケーションのルールと設定に従うようになります。

新しい送信メールが送信されないようにする必要がある場合は、「なし」を選びます。これは、問題のある部分を隔離したり、同じコンピュータ上で実行しているほかのメールサービスソフトウェアとの衝突を防ぐために行うこともできます。

受信メールのオプション

IMAP、POP3、NotifyMail を使用するときは、「許可」ボタンを選択します。次に、各プロトコルで使用したいポートを選びます。それぞれのデフォルトのポートは、「ポート」フィールドの隣に表示されています。独自のポートを選ぶこともできますが、注意して行ってください。ほかのホストにメールを送信しても、そのメールが、送信先で予測しているポート以外のポートからのものであれば、メールを配送できないことがあります。また、別のサービスが使用しているポートは使用しないでください。一般的なポートの利用状況の一覧については、301 ページの「Mac OS X コンピュータが使用するポート」を参照してください。

各プロトコルには独自の「オプション」ボタンがあり、さらに設定を選ぶことができます。これらのオプションパネルについては次のセクションで説明します。

NotifyMail を許可する

待機中のメールがあることをサーバからメールクライアントに通知させたい場合は、このオプションを選びます。次に、この機能で使用するポートを選びます。

SMTP のオプション設定

受信応答名

SMTP を使ったネットワーク操作が発生したときに、送信元のサーバに送り返したいドメイン名を入力します。この設定のデフォルト値は、プライマリメールサーバの名前です。この名前を変更すると、メールサーバの本当の身元を隠すことができるので、一方的に送りつけられてくるメールを制限できる場合があります。

送信応答名

外部のホストに対して示すドメイン名を入力します。この名前は、送信するメールメッセージに付加されます。この名前の変更には、長所と短所があります。ネットワーク上に NAT（Network Address Translation）ファイアウォールがある場合は、その変更が要求されることがあります。ただし、この操作を行うと、メールサーバが送信元のアドレスを認識しないため、メールの受信がメールサーバにより拒否される場合があります。

ホストが送信先のバックアップの場合は SMTP リレーを許可する

ほかのメールサーバのバックアップとして動作させているとき、自分のジャンクメールフィルタ設定をそのホストのメールには適用しない場合は、このオプションを選びます。

配信できないメールの未配信レポートを postmaster に送信する

メールを配送することができず、かつ送信者に通知できないときに、postmaster にこのことを通知したい場合は、このオプションを選びます。通常は、メールを配送できなかったことを伝えるレポートは送信者に返されます。何らかの理由でレポートを配送できない場合は、このオプションを選ぶことによって、レポートを postmaster のアカウントに送信できます。「postmaster」という名前のユーザアカウントが「ユーザとグループ」で設定されている必要があります。

バルクメールの未配信レポートを許可する

バルクメールの送信者が配送できなかったことを伝えるレポートを受け取るように設定する場合は、このオプションを選びます。通常、バルクメールに設定されているメールは、配送できなかったことを伝えるレポートを生成しません。

IMAP のオプション設定

受信応答名

IMAP を使ったネットワーク操作が発生したときに、接続元の IMAP クライアントに送り返したいドメイン名を入力します。

IMAP 管理者アクセスを許可する

メールサーバの管理者がメールデータベースの内容を表示および変更することを許可したい場合は、このオプションを選びます。

ポート

管理者が IMAP メッセージを表示するときに使用するポート番号を入力します。デフォルト以外のポートを選ぶ場合は、別のサービスやプロトコルですでに使用されているポートを選ばないように注意してください。このポートに対して IP フィルタサービスを設定することによって、セキュリティを強化することもできます。一般的なポートの利用状況の一覧については、301 ページの「Mac OS X コンピュータが使用するポート」を参照してください。

IMAP フォルダ名の大文字／小文字を区別する

同じ名前でも大文字と小文字を区別して IMAP フォルダを作成することをユーザに許可したい場合は、このオプションを選びます。たとえば、「Urgent」と「urgent」は、それぞれ異なる 2 つのフォルダとして作成することができます。

単一 IP アドレスでのユーザごとの接続数

各ユーザが 1 つの IP アドレスで確立できる IMAP 接続の数を入力します。デフォルトの設定は 32 です。1 ～ 999 までの範囲で設定可能です。

_ 分後、接続を終了する

接続にアイドル状態を許可する時間を分単位で入力します。この時間に達すると、接続が解除されます。デフォルト値は 30 分です。1 ～ 999 までの範囲で設定可能です。アイドル状態の接続を解除すると、メールサービスのパフォーマンスが向上します。

POP3 のオプション設定

受信応答名

POP を使ったネットワーク操作が発生したときに、接続元の POP クライアントに送り返したいドメイン名を入力します。

ホストの設定

デフォルトの「ホストを設定」ウインドウで、メールホストのデフォルト設定を作成できます。デフォルトの「ホストを設定」ウインドウにアクセスするには、「メールサービス」をクリックしてから「ホストを設定」を選びます。「受信メール」、「送信メール」、および「ネットワークの設定」という 3 つのパネルについて、次のセクションで説明しています。

受信メールの設定

このパネルでは、ホストが受信メールを処理する方法を設定します。「受信メール」パネルにアクセスするには、「メールサービス」をクリックしてから「ホストを設定」を選び、「受信メール」タブをクリックします。

ローカルのアドレスのみにメールを配信する（SMTP リレーなし）

メールサーバによるメールの配送を、このメールサーバ上の有効なアドレスのみに限定したい場合は、このオプションを選びます。このオプションは、このホストがメールのエンドポイント、つまり最終的な配送ポイントである場合にのみ選んでください。

重要　このメールサーバが別のホストのバックアップサーバとして指定されていたり、別のサーバの SMTP リレーサーバとして指定されていたりする場合、このオプションを選ぶと別のホストにメールを送信できないことがあります。

受信拒否をエラーログに記録する

メールが拒否されたときにエラーログに項目を作成したい場合は、このオプションを選びます。

すべてのメッセージの Bcc を送信する宛先

すべての受信メッセージの Bcc（blind carbon copy）を、指定する 1 つのアドレスまたはグループに送信したい場合は、このオプションを選びます。入力欄にユーザまたはグループの名前を入力します。

送信メールの設定

このパネルでは、ホストが送信メールを処理する方法を設定します。「送信メール」パネルにアクセスするには、「メールサービス」をクリックしてから「ホストを設定」を選び、「送信メール」タブをクリックします。

送信メールを許可

ホストのドメインの外部へメールを送信することを許可したい場合は、ポップアップメニューからこのオプションを選びます。

ローカルユーザに限定

メールの送信をホストのドメインに限定したい場合は、ポップアップメニューからこのオプションを選びます。このオプションを選ぶと、このパネルのほかの部分は利用できなくなります。ローカルエリアネットワーク（LAN）上のユーザの場合はこのオプションを選ぶことができますが、別の SMTP サーバの場合はこのオプションを選ばないでください。

メッセージを _ 時間保持したら期限切れにする

サーバがメッセージ配信の試行を停止するまでの時間を、時間単位で入力します。デフォルト値は 72 時間です。指定した時間内にメールを配信できない場合、ユーザに未配信レポートが送られ、メッセージは削除されます。

接続に失敗したら _ 分ごとに再試行する

サーバが別の SMTP サーバへの接続を試みる間隔を、分単位で入力します。最小時間は 1 分、デフォルトは 20 分です。

メールが配信されないことを _ 時間後に送信者に通知する

メッセージが配送されていないことを送信者に通知する場合は、このオプションを選びます。次に、送信者への通知を試みる制限時間を、時間単位で入力します。サーバは、「メッセージを _ 時間保持したら期限切れにする」で設定した制限時間になるまで、メールの配送を試みます。デフォルトは 4 時間です。

メールが配信されないことを postmaster に通知する

メールが配信できなかったときに postmaster に通知したい場合は、このオプションを選びます。通常は、メールを配送できなかったことを伝えるレポートは送信者に返されます。何らかの理由でレポートを配送できない場合は、このオプションを選ぶことによって、レポートを postmaster のアカウントに送信できます。「postmaster」という名前のユーザアカウントが「ユーザとグループ」で設定されている必要があります。

すべての SMTP メールをリレーする経由先

すべての送信メールが別のサーバを経由するように設定したい場合は、このオプションを選びます。テキストフィールドにサーバの DNS 名を入力します。サーバは送信メールをまとめて別のサーバに送信します。この別のサーバは、メールを配送するプロキシとして動作します。接続速度が遅い場合や接続する回数ごとに課金される場合は、この設定が便利です。場合によっては、この設定を使って、特定のファイアウォール制限に対処する必要があります。

ネットワークの設定

このパネルでは、送信用の SMTP ポートを選び、DNS、キャッシュ、およびタイムアウトのオプションを設定します。「ネットワークの設定」パネルにアクセスするには、「メールサービス」をクリックしてから「ホストを設定」を選び、「ネットワークの設定」タブをクリックします。

DNS リクエスト

サービスに対して要求する DNS レコードの種類を選びます。「MX リスト」、「A レコード」、またはその両方を選ぶことができます。A レコードは、ホスト名を IP アドレスに一致させます。MX レコードは、メールの転送先であるコンピュータをドメイン内で指定する、DNS テーブル内のエントリです。MX レコードについて詳しくは、155 ページを参照してください。

キャッシュ設定

サーバでは、確認済みのドメイン名をキャッシュに保存し、特に指定されない限り、情報を再び確認することはありません。この機能によって、メールサーバがメッセージごとに DNS サーバにアクセスする必要がないので、性能が向上します。キャッシュに対して、次の設定を選ぶことができます。

「DNS の TTL（Time to Live）設定を適用する」： デフォルトの DNS 設定を使用したい場合は、この設定を選びます。通常、メールは、接続が確立されるまで繰り返し再送されます。TTL によって、サーバが情報を求めて DNS にアクセスする頻度が制限されます。この制限を超えると送信の試行が停止され、配送できなかったことを伝えるレポートが作成されます。

「DNS 情報をキャッシュする _ 分」： キャッシュ内の DNS 情報を定期的にアップデートしたい場合は、このオプションを選びます。次に、情報をキャッシュに保存したい時間を分単位で入力します。この値は、デフォルトの TTL DNS 設定を上書きします。

タイムアウト

指定した時間を超える場合は常に、接続試行が停止し、接続が「タイムアウト」になったことが通知されます。接続が遅い場合や断続的な場合にタイムアウトが頻繁に発生するときは、この時間を長めに設定します。

「接続」： 接続が確立されるまでの時間を、秒単位で入力します。

「読み出し／書き込み」： メッセージの読み出しおよび書き込みを行う時間を、秒単位で入力します。この時間を過ぎると「タイムアウト」となり、接続が切断されます。

送信用 SMTP ポート

送信用の SMTP パケットで使用したいポート番号を入力します。デフォルト以外のポートを選ぶ場合は、別のサービスやプロトコルですでに使用されているポートを選ばないように注意してください。

メールサービスに関するその他の情報

メールプロトコルおよびその他のテクノロジーに関する一般的な情報については、次の参考書籍を参照してください。

- メールサービスの全般的な入門書としては、「Internet Messaging」（David Strom、Marshall T. Rose 共著、Prentice Hall 社発行、1998 年）が適しています。
- MX レコードについて詳しくは、「DNS and BIND」（第 3 版、Paul Albitz ／ Cricket Liu ／ Mike Loukides 共著、O'Reilly and Associates 社発行、1998 年）の中の「DNS and Electronic Mail」を参照してください。
- 「Removing the Spam : Email Processing and Filtering」（Geoff Mulligan 著、Addison-Wesley Networking Basics Series、1999 年）も参考になります。
- メールの標準については、「Essential E-Mail Standards : RFCs and Protocols Made Practical」（Pete Loshin 著、John Wiley & Sons、1999 年）を参照してください。

各種のメールプロトコル、DNS、およびその他の関連トピックに関して、大量の情報がインターネット上にあります。

RFC（Request for Comments）ドキュメントには、プロトコルやサービスの概要と、プロトコルの動作に関する詳しい情報が記載されています。サーバの管理を始めたばかりの方にとって、RFC の背景の情報は参考になることでしょう。経験豊富なサーバ管理者の場合、RFC ドキュメントによって、プロトコルに関する詳細な技術情報をすべて確認できます。RFC ドキュメントは、次の Web サイトで番号で検索することができます。
www.faqs.org/rfcs

メールプロトコルの動作の技術的な内容について詳しくは、次の RFC ドキュメントを参照してください。

- POP：「RFC 1725」
- IMAP：「RFC 2060」
- SMTP：「RFC 821」および「RFC 822」

メールサービスに関する簡単な説明については、次の Web サイトを参照してください。

- www.whatis.com

  技術用語を検索すると、その用語に関する簡単な説明を見つけることができます。この Web サイトでは、特定のテクノロジーの動作に関するより詳しい情報へのリンク集も用意されています。

9

QuickTime Streaming Server

QuickTime Streaming Server とは？

QuickTime Streaming Server（QTSS）は、メディアをインターネット経由でリアルタイムに配信できるテクノロジーです。ストリーミングによって、ユーザはライブメディアまたは記録済みメディアのブロードキャストを視聴したり、記録済みメディアをオンデマンドで視聴したりすることができます。ユーザはコンピュータで受信され次第、ストリーミングメディアを見ることができ、ファイルがダウンロードされるのを待つ必要がありません。

次に示すのは、QuickTime Streaming Server の主な機能です。

- 「スキッププロテクション」機能によって、インターネットでの通信障害や混雑からストリーミングを保護し、品質を向上させます。この機能は、ストリーミングのクライアントが QuickTime 5 を使用しているときに使用できます。
- 2 つの認証方式「ダイジェスト」と「ベーシック」によって、保護されたメディアへのアクセスを柔軟に制御できます。
- 「プレイリスト」機能によって、一連のメディアファイルをライブブロードキャストであるかのように簡単にストリーミングできます。この機能を利用して、仮想的なラジオ局を開設および管理することなどができます。
- Web ベースの管理によって、ローカルとリモートのどちらでもストリーミングサーバを簡単に設定および監視できます。
- リレーによって、サーバの階層を何層かに設定し、事実上無限のクライアントにストリーミングをブロードキャストできます。

ストリーミングメディアを視聴する方

「QuickTime Streaming Server」からのストリーミングは、Macintosh と Windows のどちらのユーザでも、「QuickTime Player」または QuickTime 対応のアプリケーションを使って視聴できます。「QuickTime Player」は、アップル社の Web サイトで無償で配布されています。また、QuickTime プラグインがインストールされていれば、ストリーミングを Web ブラウザから視聴できるように設定することもできます。

ユーザが Web ページを介してストリーミングメディアの再生を開始する場合は、QuickTime プラグインがサーバに要求を送信します。

ユーザが「QuickTime Player」を使ってオンデマンドでマルチメディアを視聴する場合、クライアントコンピュータがサーバにマルチメディアファイルの再生要求を送信します。サーバはヒントムービーファイルを探し、見つかった場合にクライアントコンピュータにメディアを送信します。

ユーザがライブブロードキャストを視聴する場合、QuickTime ストリーミングのクライアント（たとえば「QuickTime Player」）が QuickTime Streaming Server に要求を送信します。このサーバは SDP（Session Description Protocol）ファイルを探し、見つかった場合にメディアをクライアントコンピュータに送信し始めます。SDP ファイルには、ライブブロードキャストのフォーマット、タイミング、および著作者に関する情報が含まれています。SDP ファイルは、ブロードキャスト用ソフトウェアによって、ライブメディアの取り込みに使用されるコンピュータ上に作成されます。しかし、メディアをブロードキャストするときは、あらかじめこの SDP ファイルをストリーミングサーバにコピーしておく必要があります。

ユーザが記録済みのブロードキャストを視聴する場合も、同様のプロセスが発生します。つまり、サーバが SDP ファイルを探します。この場合は、プレイリストのブロードキャストを開始すると、SDP ファイルが自動的に作成されます。SDP ファイルがストリーミングサーバ上に作成されていない場合は、記録済みのメディアをブロードキャストする前に、ストリーミングサーバに SDP ファイルをコピーする必要があります。

QuickTime Streaming Server を使用する状況

音声や映像をインターネット経由でリアルタイムに配信することに興味のある人ならだれでも、QuickTime Streaming Server を使用することができます。たとえば QuickTime ストリーミングを次のような目的で使用できます。

- 1 日 24 時間放送できるインターネットラジオ局の開設
- コンサート、会社での会議、学校での集会など、ライブイベントのブロードキャスト
- 要望に応じて視聴できる講義ビデオを使った、遠隔学習 Web サイトの創設

QuickTime Streaming Server を設定する前に

QuickTime Streaming Server を設定する前に、次のストリーミングサーバの要件を確かめてください。

クライアントコンピュータの要件

- QuickTime 4 以降をインストールしたコンピュータであれば、QuickTime Streaming Server からストリーミングされたメディアを視聴することができます。必須ではありませんが、推奨は QuickTime 5 です。

  「QuickTime」クライアントソフトウェアは、「QuickTime」の Web サイト（www.apple.co.jp/quicktime）からダウンロードできます。

サーバの要件

- 「QuickTime Streaming Server」ソフトウェアは、Power Mac G4、Macintosh Server G4、Power Mac G4 Cube、Power Macintosh G3、Macintosh Server G3、および iMac で使用できます。
- 最新バージョンの「Mac OS X Server」をインストールする必要があります。

- 128 MB（メガバイト）以上の RAM が必要です。サーバ上の通信量が多くなると予想される場合は、512 MB 以上の RAM および 500 MHz 以上のプロセッサを使用することをお勧めします。

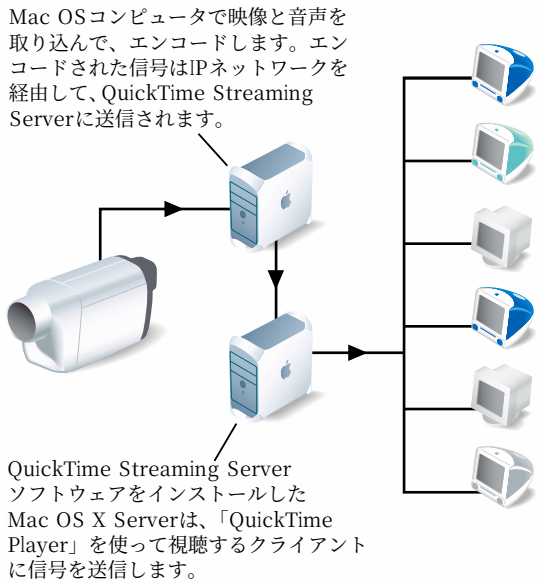
ライブブロードキャストの要件

ライブ音声またはライブ映像をストリーミングするためには、以下の機器を用意する必要があります。

- 音声、映像、またはその両方を記録できる機器。
- ブロードキャスト用ソフトウェアがインストールされ、ビデオキャプチャカードまたはオーディオキャプチャカードが搭載されているコンピュータ。FireWire 接続のあるコンピュータを使用することもできます。このコンピュータでライブ音声またはライブ映像を取り込み、エンコードしてから、ストリーミングサーバにブロードキャストします。

ライブ映像用の設定例

下の図は、ライブ映像とライブ音声をストリーミングするための設定を示しています。（ほとんどのビデオカメラにはマイクロフォンが内蔵されています。）マイクロフォン、ミキサー、およびその他の適切な音声機器を使うと、音声だけをストリーミングすることができます。



QuickTime Streaming Server を初めて設定する

「QuickTime Streaming Server」の設定と管理を行うときは、Web ベースの「Streaming Server Admin」プログラムを使用します。「Streaming Server Admin」を使用するには、バージョン 4.5 以降の「Netscape Navigator」、「Netscape Communicator」、または「Microsoft Internet Explorer」を実行できるコンピュータが必要です。

手順 1：「Streaming Server Admin」を開く

「Streaming Server Admin」を開くときは、次のように操作します。

1. Web ブラウザを開きます。
2. サーバ上の「Streaming Server Admin」の URL を入力します（必ずコロンとポート番号 1220 を追加します）。

   たとえば、次の情報が使用されます。

   ```
   http://www.myserver.com:1220
   ```

   「www.myserver.com」の部分をお使いのサーバの名前に置き換えてください。
3. ログインとパスワードのテキストフィールドにストリーミングサーバの管理者 ID とパスワードを入力し、「送信」をクリックします。ID は「streamingadmin」で、デフォルトのパスワードは「default」です。

   「Streaming Server Admin」の Web ページが表示され、サーバの動作状況が表示されます。ページの上部にある「状況」、「設定」、または「ログ」をクリックしてこれらの領域を管理します。

   参考：「QuickTime Streaming Server」が正しくインストールされた場合は、「Dock」から「Streaming Server Admin」を開くこともできます。

   「Streaming Server Admin」の使用中にヘルプを表示するときは、「?」マークをクリックします。

手順 2：ストリーミングサーバの設定を選ぶ

ストリーミングサーバの設定を変更するときは、次のように操作します。

1. 「設定」をクリックします。
2. 「一般設定」、「ログ設定」、または「プレイリスト設定」をクリックします。
3. 必要な変更を行って「送信」をクリックします。

利用可能な設定について詳しくは、177 ページの「ストリーミングサーバの設定」を参照してください。

手順 3：ストリーミングメディアを表示するための Web ページを作成する（省略できます）

ストリーミングメディアは、Web ページに埋め込むことができます。このようにしておくと、視聴者はその Web サイトの URL を入力することによって、任意の Web ブラウザでメディアを視聴できます。

たとえば、ユーザは次のような URL を入力できます。

```
http://www.mywebpage.com/
```

この場合、「www.mywebpage.com」の部分をお使いの Web サイトの DNS 名に置き換えます。

ストリーミングメディアを埋め込んだ Web ページを作成する

Web ページにストリーミングメディアを埋め込むときは、HTML の「EMBED」タグを使用します。「EMBED」タグの機能と使用方法について詳しくは、www.apple.co.jp/quicktime/authoring を参照してください。

次のサンプルコードは、Web ページ上でムービー「sample.mov」にグラフィックのリンクを指定しています。（QuickTime に付属の「Sample Movie」の名前を変更して、試しに使うことができます。）ユーザがリンクをクリックすると、「QuickTime Player」でムービーのストリーミングが開始します。

```
<HTML>
<BODY>
This is a sample use of the EMBED tag.<BR>
<EMBED SRC="http://my.webserver.com/linkimage.mov" width="150"
       height="64" href="rtsp://my.streamingserver.com/
       sample.mov" target="QuickTimePlayer">
</BODY>
</HTML>
```

「SRC」属性で指定されている URL は、静止画像「linkimage.mov」へのリンクです。この画像が、ストリーミングムービーへのリンクになります。「width」および「height」属性はそれぞれ、画像領域の幅と高さを指定します。「HREF」属性は、画像がクリックされたときに再生を開始するストリーミングムービーの URL を指定します。

また、ストリーミングサーバ上のメディアを指す RTSP URL を使用し、ストリーミングトラックを含むリファレンスムービーを作成することによって、ユーザが Web ページ上でストリーミングメディアを視聴できるようにすることも可能です。作成したリファレンスムービーを Web サイトと同じディレクトリに保存し、Web ページにリファレンスムービーへのリンクを作成します。リファレンスムービーの作成について詳しくは、developer.apple.com/quicktime/quicktimeintro/tools/index.html で「WebMaster Tools」の「MakeRefMovie」ツールを参照してください。

リファレンスムービーは、テキストファイルのようにシンプルにすることができます。ファイル名には拡張子「.mov」を付けます（「ref.mov」など）。ファイルのコンテンツのフォーマットは、次のようになります。

```
rtsptext rtsp://my.streamingserver.com/sample.mov
```

ストリーミングサーバの設定

一般設定

ムービーディレクトリ

指定した「ムービーディレクトリ」内のヒントされたメディアはすべてストリーミングに使用できます。以下のものを使用できます。

- 個々のファイル
- ファイルを含んでいるディレクトリ
- ほかの場所にあるメディアへのリンク

「ムービーディレクトリ」のデフォルトの場所は「/Library/QuickTimeStreaming/Movies/」です。別のボリュームの別のディレクトリを選ぶことができます。

認証方式

「ベーシック」または「ダイジェスト」を選びます。デフォルトでは、より安全性の高い「ダイジェスト」認証がサーバで使用されます。ただし、「ダイジェスト」認証では、ユーザがバージョン 5 以降の「Quicktime」を使って接続する必要があります。「ベーシック」認証を使用すると、「ダイジェスト」認証に比べてセキュリティ保護は強力でなくなりますが、「QuickTime」の以前のバージョンと互換性があります。

ポート 80 のストリーミング

HTTP ポート 80 を経由して QuickTime ストリーミングを提供するかどうかを選択します。ファイアウォールで保護されたクライアントにストリーミングを提供する必要がある場合は、ポート 80 経由のストリーミングを有効にする必要があります。ポート 80 の HTTP ストリーミングを使用しても、ほかのポートでの HTTP ストリーミングは使用できます。ただし、同じサーバ上で Web サービスも提供する場合は、QuickTime ストリーミングがポート 80 の HTTP トラフィックを妨げる可能性があります(詳しくは、188 ページの「ポート 80 のストリーミング」を参照してください)。

最大接続数

最大接続数に達すると、接続しようとしたユーザには、サーバにアクセスが集中していることを示すメッセージ（エラー 453）が表示されます。使用可能な帯域幅、提供するメディアファイルのサイズ、およびブロードキャストの対象とするクライアント数のバランスをうまくとるようにしてください。

最大スループット

これは、サーバの最大スループットです。最大スループットに達すると、ほかのユーザは接続できません。接続しようとしたユーザには、サーバにアクセスが集中していることを示すメッセージ（エラー 453）が表示されます。「QuickTime Streaming Server」は、ネットワーク上でほかのデバイスとスループットを共有することがあることに注意してください。

システム起動時にサーバを開始

コンピュータを再起動したときに、常にサーバを開始し直します。

「Streaming Server」の管理者のパスワード

ストリーミングサーバの管理者のログインパスワードを入力します。次の行にもう一度ログインパスワードを入力して確認します。デフォルトのパスワードは「default」ですが、パスワードを変更することができます。

ログの設定

フィールド内の情報を変更したり、必要なボタンをクリックしたりして設定を調整します。一定の日数または一定のサイズ（KB 単位）に達したら、ログがリセットされるように指定することができます。「送信」をクリックすると、変更が反映されます。

エラーログ

エラーログでは、エラーと情報メッセージが示されます。この情報は、サーバのトラブルに対処するときに利用できます。完全なエラーログは、「/Library/QuickTimeStreaming/Logs/Error.log」ディレクトリにあります。

アクセスログ

「アクセスログ」には、記録がリセットされて以降、各メディアファイルがアクセスされた回数、アクセスされた日時、およびそのメディアファイルにアクセスしたユーザが示されます。アクセスエラーもこのログに記録されます。完全なアクセスログは、「/Library/QuickTimeStreaming/Logs/StreamingServer.log」ディレクトリにあります。

接続中のユーザ

このパネルには、ストリーミングサーバに接続しているクライアントのリストが表示されます。また、クライアントが視聴しているムービーやクライアントの IP アドレスなどの追加情報も表示されます。以下に説明する画面コントロールを使用すると、この情報をさまざまな形式で表示できます。

表示する数

ポップアップメニューから数値を選んで、表示するユーザの数を 4 変更します。

このページのアップデートの間隔

ポップアップメニューから数値を選んで、リストが更新される頻度を変更します。

並べ替えの順序を選択する

ポップアップメニューから「昇順」または「降順」を選んで、並び順を選択します。

並べ替えの列を選択する

列ラベルをクリックして、接続中のユーザのリストを並べ替える基準を選びます。

ストリーミングサーバの上手な使いかたとヒント

ストリーミングするライブメディアを用意する

ライブ音声またはライブ映像をストリーミングするときは、以下の操作を行う必要があります。

1. ブロードキャスト用ソフトウェアに付属のマニュアルの指示に従って、ブロードキャスト用ソフトウェアを設定します。
2. 音声機器または映像機器を、信号の取り込みとエンコードに使用するコンピュータに接続します。
3. ブロードキャスト用ソフトウェアを使って、ライブ信号の取り込みとエンコードに使用するコンピュータで SDP（Session Description Protocol）ファイルを作成します。

   詳しくは、お使いのブロードキャスト用ソフトウェアに付属のマニュアルを参照してください。
4. SDP ファイルを「QuickTime Streaming Server」コンピュータにコピーします。

   SDP ファイルは、必ずストリーミングに使用するディレクトリにコピーしてください。
5. ストリーミングメディアを Web ページで表示したい場合は、「EMBED」タグを使用するか QuickTime リファレンスムービーを別に作成して Web ページを作成します（176 ページの「ストリーミングメディアを埋め込んだ Web ページを作成する」を参照してください）。

6 ストリーミングサーバが開始していることを確認します。

7 ブロードキャスト用ソフトウェアに付属のマニュアルの指示に従って、ブロードキャスト用ソフトウェアを開始します。

8 ユーザに、SDP ファイルへの RTSP URL、または Web サーバに保存した QuickTime リファレンスムービーへの HTTP URL を提供して、ストリーミングメディアの視聴方法を知らせます。

ストリーミングする保存済みメディアを用意する

ストリーミングする保存済みメディアを用意するときは、次のように操作します。

手順 1：メディアにヒントトラックを追加する

ヒントトラックには、ストリーミングサーバがメディアを正しくストリーミングするために必要な情報が含まれています。ほとんどのオーサリング用アプリケーションでは、メディアをヒントされた QuickTime ムービーとして書き出すことができます。「QuickTime Pro」があれば、「QuickTime Player」を使ってムービーをヒントすることもできます。「QuickTime Pro」は「Mac OS」コンピュータと「Windows」コンピュータで使用することができます。システム要件とインストールの手順については、QuickTime の Web サイトで確認してください。

メディアファイル内のトラックは、それぞれ独自のヒントトラックを持ちます。たとえば、1 個の音声トラックと 1 個の映像トラックがあるムービーの場合は、2 つのヒントトラックがあります。1 つは音声トラック用で、もう 1 つは映像トラック用です。

「QuickTime Player」を使ってムービーをヒントムービーとして書き出すと、QuickTime によって自動的に適切な数のヒントトラックが追加されます。

QuickTime ムービーをヒントムービーとして書き出すときは、次のように操作します。

1 「Mac OS」コンピュータまたは「Windows」コンピュータで「QuickTime Player」を開きます。（この操作には「QuickTime Pro」が必要です。）

2 ヒントしたいメディアファイルを開きます。

3 「ファイル」メニューから「書き出し」を選びます。

4 ポップアップメニューから「ムービーからヒントムービーへ」を選び、新しいファイル名を入力します。

5 「書き出し」ダイアログボックスで「オプション」をクリックします。

6 「サーバ用にヒントを最適化」を選びます。この手順は省略できます。このオプションを選ぶと、サーバの能力が向上し、より多くのクライアントにストリーミングできるようになりますが、ファイルのサイズが 2 倍になることがあります。

7 「OK」をクリックします。

8 「保存」をクリックします。

手順 2：メディアファイルを QuickTime Streaming Server にコピーする

SDP ファイルは、必ずストリーミングに使用するディレクトリにコピーしてください。

複数のソースを持つメディアファイルをストリーミングする

多くの場合、QuickTime ムービーは、複数のメディアファイルのコンテンツで構成されます。たとえば、1 つの映像クリップを 1 つ以上の CD トラックの音楽と組み合わせることがあります。QuickTime ムービーを書き出すときは、すべてのソースメディアが含まれるように「独立再生形式」のファイルにしてください。これによってサーバの性能が向上します。

独立再生形式ではないムービーをストリーミングするときは、ヒントするほかに、次の操作を行う必要があります。

- ムービーで必要なファイルをすべて同じフォルダまたはディレクトリにコピーします。
- すべてのファイルを「QuickTime Streaming Admin」で「ムービーディレクトリ」に指定したサーバ上のディレクトリに保存します。

プレイリストを使って記録済みの音声または映像をブロードキャストする

記録済みの QuickTime メディアファイルが特定の順番（プレイリスト）で再生されるように設定しておくと、仮想の「ラジオ局」やビデオ放送を実現できます。一連のプレイリストを設定し、それぞれの「再生」ボタンをクリックすると、「QuickTime Streaming Server」にメディアがブロードキャストされ、設定した順番（ランダムまたは順序通り）で視聴者にメディアが配信されます。メディアはあらかじめ記録されたものですが、視聴者にはライブブロードキャストのように見えます。ブロードキャストを視聴しようとするすべての人が、同じメディアを視聴します。

メディアをブロードキャストするときは、以下の操作を行う必要があります。

手順 1：QuickTime メディアとリファレンスムービーファイルを用意する

「QuickTime Streaming Server」がストリーミング可能なメディアであれば、どのようなメディアでもブロードキャストできます。

メディアを用意するときは、次のように操作します。

- プレイリストのムービーでは、それぞれ同じトラック数および同じ種類のトラックを使用します。すべてのメディアファイルが互換性のある種類のメディアを含んでいることを確認します。たとえば、すべての音声トラックで同じエンコード方式、圧縮方法、およびビットレートを使用する必要があります。また、すべての映像トラックでも同じエンコード方式、圧縮方法、およびビットレートを使用する必要があります。
- 各ファイル内のメディアを同じ方法でフォーマットします。たとえば、映像トラックが含まれるそれぞれのファイルで、同じフレームサイズを使用します。
- 各項目がヒントされた QuickTime ムービーであることを確認します。

QuickTime メディアとリファレンスムービーファイルを用意するときは、次のように操作します。

- 通常、プレイリストの最初のメディアファイルをリファレンスムービーとして指定します。ただし、リファレンスムービーを別にオーサリングすることができます。
- リファレンスムービーを別にオーサリングする場合、このリファレンスムービーは、実際のメディアファイルと同じトラック数、トラックの種類、エンコード方式、圧縮方法、およびビットレートが使用された、ヒントされた QuickTime ムービーである必要があります。

手順 2：プレイリストを作成する

プレイリストを作成するときは、次のように操作します。

1. 「Streaming Server Admin」の「設定」をクリックし、さらに「プレイリスト設定」をクリックします。
2. 「新しいプレイリストを作成」をクリックします。
3. プレイリストの名前を入力します。
4. ポップアップメニューを使って再生モードを設定します。
   - 「シーケンシャル」：メディアはプレイリストファイルの順にブロードキャストされます。最後のメディアファイルの再生が完了すると、ブロードキャストが停止します。
   - 「シーケンシャル（繰り返しあり）」：メディアはプレイリストファイルの順にブロードキャストされます。最後のメディアファイルの再生が完了すると、同じ順番でプレイリストが繰り返されます。
   - 「ランダム（重み付けあり）」：メディアは、項目の再生頻度を決めるために、7 で指定する重み付けに従ってランダムにブロードキャストされます。メディアは、ブロードキャストを停止するまで、ランダムに再生され続けます。
5. エラーメッセージなど、ブロードキャストに関する情報をサーバでログファイルに記録したいときは、「ログを作成する」をクリックします。
6. 「項目を追加／削除」をクリックして、ムービーファイルをプレイリストに追加します。
7. メディアファイルの順序と重み付けを設定します。

   プレイリスト内のメディアは、指定した順番またはランダムにブロードキャストできます。また、リストを 1 回だけブロードキャストすることも、繰り返しブロードキャストすることもできます。

   メディアをランダムにブロードキャストする場合は、リスト内の各メディアファイルに「重み付け」を指定できます。重み付けは 1 ～ 10 の数値で、この数値によって項目を再生する頻度が決まります。10 の重み付けが指定されたメディアファイルは、10 未満の重み付けが指定されたメディアファイルよりも再生頻度が高くなります。（重み付けはムービー名の後に指定します。）メディアファイルのデフォルトの重み付けは 10 です。重み付けを使用するほかに、ほかのメディアファイルが指定した数だけ再生されるまで、メディアファイルが再び再生されないようにすることもできます。
8. リストにあるほかの項目を繰り返す前に再生する項目の数を設定します（重み付けを使用する場合）。
9. 「送信」をクリックしてプレイリストを保存します。

   参考：ヒントされたメディアファイルとプレイリストは、サーバの任意の場所に保管できます。指定した「ムービーディレクトリ」以外の場所でもかまいません。ヒントされたメディアファイルを「ムービーディレクトリ」以外の場所に保管した場合、このファイルをプレイリストの一部としてブロードキャストできますが、QuickTime クライアントからこれらのファイルに直接アクセスすることはできません。

手順 3：ブロードキャストサービスを開始する

ブロードキャストサービスを開始および停止するときは、「Streaming Server Admin」の「プレイリスト設定」パネルに戻ります。プレイリストのブロードキャストを開始するときは、「操作」列の「再生」ボタンをクリックし、停止するときは「停止」ボタンをクリックします。

手順 4：ブロードキャストへの接続方法をユーザに知らせる

ユーザがブロードキャストに接続するためには、「QuickTime Player」など、QuickTime メディアを再生できるソフトウェアが必要です。

最適の結果を得るためには、最新バージョンの「QuickTime」ソフトウェアをインストールする必要があります。

ストリーミングメディアを表示する Web ページを作成すると、ユーザは QuickTime プラグインがインストールされたWebブラウザを使ってブロードキャストに接続することができます。Web ページの URL をユーザに提供し、クリックしたときにメディアが再生するようにリンクを正しく埋め込む必要があります（176 ページの「ストリーミングメディアを埋め込んだ Web ページを作成する」を参照してください）。

ユーザが「QuickTime Player」を使ってブロードキャストを視聴する場合は、プレイリストのブロードキャストに接続する SDP ファイルの URL をユーザに提供する必要があります。

プレイリストに関する問題を解決する

ログを許可すると、ブロードキャスト中に発生したトラブルの対処にログファイルを利用できます。

プレイリスト内のメディアがブロードキャストされていない場合：

- 「Streaming Server Admin」をチェックして、ストリーミングサーバが動作していることを確認します。
- ストリーミングサーバが動作している場合、サーバコンピュータにある「ProcessViewer」を使って、「PlaylistBroadcaster」というプロセスが実行されていることを確認します。「PlaylistBroadcaster」プロセスが実行されていてもメディアがブロードキャストされていない場合は、いったんブロードキャストを停止し、ブロードキャストの SDP ファイルを「QuickTime Streaming Server」の「ムービーディレクトリ」から削除した後、ブロードキャストを再開します。ブロードキャストを再開すると、新しい SDP ファイルが生成されます。

プレイリスト内のメディアがランダムにブロードキャストされていない場合：

「ランダム（重み付けあり）」再生モードが指定されていることを確認します。

メディアが一度再生されて停止する場合：

再生モードが「シーケンシャル（繰り返しあり）」または「ランダム（重み付けあり）」に設定されていることを確認します。

プレイリストを「ランダム（重み付けあり）」でブロードキャストし、繰り返す項目にゼロ以外の数値を設定している場合は、その数値がプレイリストのメディアファイルの数よりも小さい数値であることを確認します。

プレイリスト内の一部のメディアが再生されない場合：

プレイリスト内の各メディアファイルに割り当てた重み付けを確認します。プレイリストを変更した場合は、変更が反映されるようにブロードキャストをいったん停止してから再び開始する必要があります。

メディアが正しくストリーミングされていない場合：

プレイリスト内のすべてのファイルについて、メディアのコンテンツ、フォーマット、およびエンコード方式が同じであることを確認します。また、ユーザが各自のコンピュータに最新バージョンの「QuickTime」ソフトウェアをインストールしていることを確認します。

ストリーミング速度が遅い場合：
各メディアファイルがサーバ用に最適化されたヒントムービーであることを確認します。

QuickTime Streaming Server の内側

互換性のあるファイルフォーマット

以下に示すメディアファイルは、ヒントされたメディアである限り、「QuickTime Streaming Server」を使ってストリーミングし、「QuickTime Player」で再生することができます。

分類	フォーマット
ビデオ	AVI
オーディオ	AIFF/AIFC
	SoundDesigner II
	System 7 Sound
	μLaw (AU)
	WAV
MIDI	Karaoke MIDI
	Standard MIDI

メディアファイルは、次の方式で圧縮できます。

分類	圧縮／解凍方式（CODEC）
推奨するビデオ形式	Sorenson Video
	H.263
	Motion JPEG A
	H.261
サポートするビデオ形式	Animation
	Cinepak
	Graphics
	Motion JPEG B
	MPEG-1
	Photo JPEG
	Video
	None

分類	圧縮／解凍方式（CODEC）
推奨するオーディオ形式	MP3
	QDesign Music codec
	QUALCOMM Pure Voice
	DVI 4:1
	ALaw 2:1
	ALaw 2:1
	16-bit raw
サポートするオーディオ形式	IMA 4:1
	MACE 3:1
	MACE 6:1

ストリーミングメディアへのアクセスを制御する

「QuickTime Streaming Server」には認証モジュール「QTSSAccessModule」が付属しており、これを使ってストリーミングメディアファイルへのアクセスを制御できます。サポートされている認証方式は 2 種類あります。「ベーシック」と「ダイジェスト」です。デフォルトでは、より安全性の高い「ダイジェスト」認証がサーバで使用されます。

「QTSSAccessModule」では、ストリーミングメディアへのアクセス制御だけではなく、ストリーミングサーバに対するプレイリストおよび管理者のアクセスも制御できます。リレーサーバからストリーミングされるメディアへのアクセスは制御できません。リレーされるメディアの認証は、リレーサーバの管理者が設定する必要があります。

「QTSSAccessModule」は「QuickTime Streaming Server」に内蔵しているため、常に使用できます。

保護されたメディアにアクセスするためのクライアントの要件

「ダイジェスト」認証が有効になっているメディアファイルにアクセスするためには、ユーザは「QuickTime 5」以降を使用する必要があります。「QuickTime Streaming Server」で「ベーシック」認証を使用するように設定されている場合は、ユーザは「QuickTime 4.1」以降を使用する必要があります。ユーザがメディアファイルを視聴するためには、自分のユーザ名とパスワードを入力する必要があります。それよりも古いバージョンの「QuickTime」を使用しているユーザがメディアファイルにアクセスしようとすると、「401：認証されませんでした」というエラーメッセージが表示されます。

アクセス制御を設定する

アクセス制御を機能させるには、「ムービーディレクトリ」に指定したディレクトリにアクセスファイルを置く必要があります。「QuickTime Streaming Server」の「ムービーディレクトリ」にアクセスファイルがないと、すべてのクライアントがこのディレクトリのメディアにアクセスすることができます。

アクセス制御を設定するには、以下の操作を行う必要があります。

- アクセスファイルを作成します
- ユーザファイルを作成します
- ユーザファイルにユーザを追加します

必要に応じて、グループファイルも作成できます。

手順 1：アクセスファイルを作成する

アクセスファイルは、ユーザとグループに関する情報が記述されている、「qtaccess」と呼ばれるテキストファイルです。このファイルに記述されているユーザとグループには、アクセスファイルが保存されているディレクトリ内にあるメディアを視聴する権限が与えられます。ストリーミングメディアを保存するディレクトリは、ほかのディレクトリを含むことが可能であり、それぞれのディレクトリはそれぞれのアクセスファイルを持つことができます。ユーザがメディアファイルを視聴しようとすると、サーバが、メディアを視聴する権限がユーザにあるかどうかを確認します。サーバは、まずメディアファイルがあるディレクトリ内でアクセスファイルを探します。アクセスファイルが見つからない場合は、そのディレクトリ内にあるディレクトリでアクセスファイルを探します。最初に見つかったアクセスファイルを使って、ユーザにメディアファイルを視聴する権限が与えられているかどうかを判断します。

参考：「QuickTime Streaming Server」のアクセスファイルは、Apache Web サーバのアクセスファイルと同様に機能します。

アクセスファイルは任意のテキストエディタで作成できます。ファイル名は「qtaccess」とする必要があります。また、次の形式で記述する必要があります。

```
AuthName<message>
AuthUserFile <user filename>
AuthGroupFile <group filename>
require user <username1> <username2>
require group <groupname1> <groupname2>
```

山かっこで囲まれていない文字列は、キーワードです。山かっこ内には、必要な情報を記述します。

- 「message」は、ログインウインドウが表示されたときにユーザに示すテキストです。省略してもかまいません。

  メッセージに空白文字（単語間のスペースなど）を入れる場合は、メッセージ全体を引用符で囲んでください。
- 「user filename」は、ユーザファイルのパスとファイル名です。デフォルト設定は「/etc/streaming/qtusers」です。
- 「group filename」は、グループファイルのパスとファイル名です。デフォルト設定は「/etc/streaming/qtgroups」です。グループファイルは省略してもかまいません。多数のユーザがいる場合は、1 つ以上のグループを設定してからグループ名を入力した方が、ユーザを個別に記述するよりも簡単な場合があります。
- 「username」は、ログインとメディアファイルを視聴する権限が与えられているユーザです。このユーザ名は、指定したユーザファイルに記述されている必要があります。「valid-user」を指定することもできます。「valid-user」はすべての有効なユーザを示します。
- 「groupname」は、ログインとメディアファイルの視聴の権限が与えられているメンバーで構成されるグループです。グループとそのメンバーは、指定したグループファイルに記述されている必要があります。

追加のユーザタグ

このセクションでは、「qtaccess」ファイルに追加できるタグについて説明します。

- valid-user

  「valid-user」は、「qtusers」ファイルに定義されたすべてのユーザを示します。

  ステートメント「require valid-user」を指定すると、「qtusers」ファイルで認証されているすべてのユーザにメディアファイルへのアクセス権を与えることができます。このタグを使用すると、サーバは、メディアを視聴するためのユーザ名とパスワードをユーザに求めます。

- any-user

  「any-user」は、ユーザがメディアを視聴する際に認証を行わないことを示します。ステートメント「require any-user」を指定すると、すべてのユーザにアクセス権が与えられます。アクセスする際に、名前とパスワードは要求されません。

手順 2：ユーザファイルを作成する

ユーザがメディアファイルにアクセスできるようにするためには、そのユーザをユーザファイルに追加する必要があります。

ユーザファイルを作成するときは、「Terminal」ウインドウを開き、次のように入力します。

```
qtpasswd -c <authentication realm> <user filename> <user-name>
```

「authentication realm」は、認証ウインドウでクライアントユーザに表示するメッセージです。「ベーシック」認証の場合、アクセスファイルに「AuthName」キーワードが指定されているときは、アクセスファイルに示された保護領域がユーザに表示されます。「AuthName」キーワードが指定されていないときは、ユーザファイルに示されている保護領域がユーザに表示されます。「ダイジェスト」認証の場合は、アクセスファイルの「AuthName」キーワードは無視され、ユーザファイルに示されている認証の保護領域が常にクライアントユーザに表示されます。「ダイジェスト」認証を使用する場合は、ユーザファイルを作成した後で保護領域を変更することはできません。保護領域を変更する必要がある場合は、ユーザファイルを作成し直す必要があります。

そのユーザのパスワードを入力するように求められます。指定したユーザを含むファイルが作成されます。

参考：`-c` オプションは、ファイルの作成を指定します。このオプションは 1 回しか使用できません。既存のファイルにこのオプションを使用すると、ファイルを上書きするかどうかのメッセージが表示されます。

手順 3：ユーザファイルにユーザを追加する

ユーザファイルにユーザを追加するには、「Terminal」ウインドウを開き、次のように入力します。

```
qtpasswd <user filename><user-name>
```

そのユーザのパスワードを入力するように求められます。要求されたら、もう一度同じパスワードを入力します。

手順 4：グループを追加する／削除する

グループファイルは任意のテキストエディタで作成できます。ただし、次の形式で作成する必要があります。

```
<groupname>: <user-name1> <user-name2> <user-name3>
```

グループを追加または削除するときは、作成したグループファイルを編集します。

ユーザファイルまたはグループファイルを変更する

ユーザファイルまたはグループファイルからユーザを削除するときは、次のように操作します。

- テキストエディタを使ってユーザファイルまたはグループファイルを開きます。ユーザファイルからはユーザ名と暗号化されたパスワードの行を削除します。グループファイルからはユーザ名を削除します。

ユーザのパスワードを変更するときは、次の操作を行います。

- 「Terminal」ウインドウを開き、次のように入力します。

```
qtpasswd <user filename> <user-name>
```

そのユーザのパスワードを入力するように求められます。入力したパスワードが、ファイルに記述されているパスワードと置き換わります。

ファイアウォールまたはアドレス変換を使用するネットワークを介してメディアを視聴する

「QuickTime Streaming Server」は UDP（User Datagram Protocol）パケットを使ってデータを送信します。ネットワーク上の情報を保護するように設計されているファイアウォールでは、多くの場合、UDP パケットがブロックされます。UDP パケットをブロックするファイアウォールで保護されたクライアントコンピュータは、ストリーミングメディアを受信できません。ただし、「QuickTime Streaming Server」では、HTTP 接続を介してストリーミングすることもできます。この方法を使えば、非常に厳しく設定されたファイアウォールを経由した場合でもストリーミングメディアを視聴できます。

アドレス変換を使用するネットワーク上にある一部のクライアントコンピュータも、UDP パケットを受信できないことがあります。ただし、HTTP 接続を介してストリーミングされるメディアを受信することはできます。

ユーザがファイアウォール経由またはアドレス変換を使用するネットワーク経由でメディアを視聴するときに問題が発生した場合は、ユーザの「QuickTime」ソフトウェアを最新バージョンにアップグレードしてください。それでも問題が解決しない場合、ネットワーク管理者はユーザに「QuickTime 設定」コントロールパネルの「ストリーミングプロキシ」パネルと「ストリーミング・トランスポート」パネルの適切な設定を知らせる必要があります。

また、ネットワーク管理者は、RTP と RTSP スループットが許可されるようにファイアウォールソフトウェアを設定することもできます。

ポート 80 のストリーミング

インターネット上でストリーミングサーバを設定していて、一部のユーザは Web での通信のみ許可するファイアウォールの背後にあると思われる場合、ポート 80 のストリーミングを使用する必要があります。そのように設定すると、「QuickTime Streaming Server」は、Web での通信のデフォルト設定であるポート 80 での接続を受け入れるため、「QuickTime」のクライアントは、Web での通信のみ許可するファイアウォールの背後であっても、ストリーミングサーバに接続することが可能になります。

ポート 80 のストリーミングを許可すると、ストリーミングサーバと同じコンピュータで Web サーバを実行することができなくなります。ただし、次の方法のいずれかを行えば、Web サーバを実行できます。

- サーバに複数のIPアドレスを設定します。これらのIPアドレスは、同じネットワークインタフェースカードまたは複数のインタフェースカードのどちらにでも割り当てることができます。Web サーバとストリーミングサーバが異なる IP アドレスで接続を受け付けるように設定します。
- Web サーバがポート 80 以外の接続を受け付けるように設定します。この場合は、Web サーバを指すすべての URL を、変更先のポート番号を指定するように変更する必要があります。

リレーを設定する

メディアストリーミングは、基本的に次の 2 つの方法のいずれかでサーバからクライアントコンピュータに送信されます。

- ユニキャストは、1 対 1 で転送されます。ストリーミングを視聴するクライアントコンピュータは、それぞれ独自のストリーミングを受信します。
- マルチキャストストリーミングは、グループアドレスに送信されます。つまり、複数のクライアントコンピュータが同じストリーミングを視聴できます。

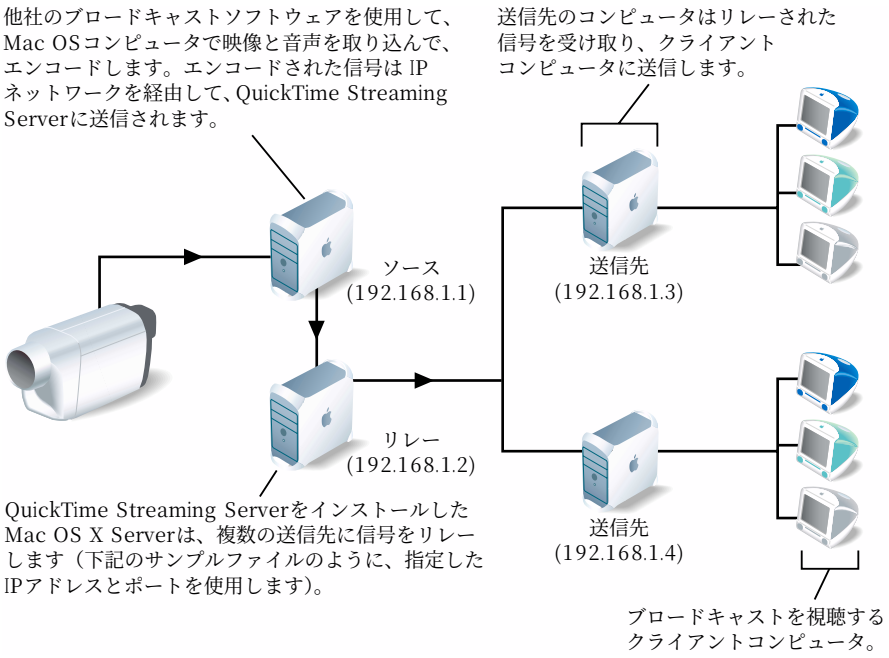
リレーとは、外部からのブロードキャスト（ユニキャストまたはマルチキャスト）を受信し、そのブロードキャストを 1 つ以上の送信先アドレスに転送、あるいはリレーすることです（ブロードキャストをリレーするときも、ユニキャストおよびマルチキャストが可能です）。複数のブロードキャストを同時にリレーするようにサーバを設定することができます。リレーはマルチキャストの利点を活かし、データを複数の送信先に同時にストリーミングすることができます。これは、同じデータを必要とするユーザが多数いる場合に、マルチメディアなどの広帯域幅のデータを送信する方法として効率的です。

リレーは、複数の層で構成されたストリーミングサーバを使用して大規模なブロードキャストを行うときにも使用できます。たとえば、3,000 人のクライアントがライブブロードキャストを視聴すると予想され、ブロードキャストの処理に 5 つのサーバを使用する場合は、リレーとして動作するストリーミングサーバにブロードキャストを送るようにブロードキャスト用アプリケーションを設定します。次に、リレーによって、ブロードキャストのコピーを 5 つのストリーミングサーバにそれぞれ転送します。

また、リレーによって、IP マルチキャストを利用することもできます。マルチキャストとは、1 つのストリーミングを複数のクライアントが視聴できるようにするためのインターネット技術です。これによって、帯域幅を節約することができます。ただし、クライアントとサーバの間にあるすべてのルータで IP マルチキャストが使用可能になっている必要があります。また、一部のインターネットルータでは、マルチキャストを使用できないようになっています。

企業や大学のイントラネットなど、ブロードキャストを行うネットワークでマルチキャストが使用可能である場合は、リレーを使用することによって、受信ユニキャストを受け取り、それをマルチキャストとしてリレーすることができます。リレーされたマルチキャストは、ストリーミングを受信しようとするすべてのクライアントが視聴できます。また、リレーを使用して、受信マルチキャストを受け取り、それをユニキャストとしてリレーすることもできます。これは、マルチキャストをネットワーク全体には配信したくない場合に便利です。

ライブブロードキャストのリレーの設定例



リレー設定ファイルを設定する

リレー設定ファイルを作成し、「/etc/streaming」ディレクトリにコピーすることで、リレーを設定します。リレー設定ファイルを作成する最も簡単な方法は、ストリーミングサーバソフトウェアに付属のサンプルファイルを編集することです。サンプルファイルのパスとファイル名は、「/etc/streaming/streamingrelay.conf」です。

1つのリレー設定単位は、リレーソースと1つ以上のリレー送信先から成ります。リレー送信先の情報は、リレーソースの情報の直後に記述する必要があります。1 つの設定ファイルに複数のリレー設定単位を記述することができます。

次の例には、1つのソースと 2 つの送信先が含まれています。

重要「relay_source」と「relay_destination」を記述するときは、異なる行に分けて記述する必要があります。また、それぞれが必ず 1 行になるようにします。

リレー設定ファイルの例：

```
relay_source "in_addr=192.168.1.1 src_addr=192.168.1.2
       in_ports=5000 5002 5004 ttl=15"
relay_destination "dest_addr=192.168.1.3 out_addr=192.168.1.2
       dest_ports=6980 6982 6984"
relay_destination "dest_addr=192.168.1.4 out_addr=192.168.1.2
       dest_ports=10010 10012 10014 ttl=15"
```

リレー設定ファイルで使用できるキーワードと値を、以下に示します。

キーワード	値
relay_source	このキーワードに続けて、キーワード in_addr、src_addr、in_ports、ttl、および各キーワードの適切な値を記述します。
in_addr	入力元の IP アドレス。ソースのブロードキャストがマルチキャストの場合は、マルチキャストの IP アドレスです。ソースのブロードキャストがユニキャストの場合は、ソースコンピュータの IP アドレスのいずれかである必要があります。
src_addr	ソースの IP アドレス（省略できます）。
in_ports	ソースのブロードキャストの RTP ストリーミングのポート番号です。この番号は、偶数である必要があります。入力ポートの番号は、出力ポートの番号と一致する必要があります。ポート番号が一意で、重複していないことを確認してください。
ttl	Time-to-live 値です（マルチキャストソースの場合）。Time-to-live 値は、メディアストリーミングがあるルータから別のルータに通過できる回数を指定するために、マルチキャストとともに使用されます。指定した回数を超えると、ストリーミングは転送されなくなります。 0 ～ 255 の任意の数値を指定できます。値が 1 の場合は、ローカルエリアネットワークのクライアントコンピュータまで到達します。数値が大きくなるほど、マルチキャストのパケットが送信される距離も長くなります。
relay_destination	このキーワードに続けて、キーワード dest_addr、out_addr、dest_ports、ttl、および各キーワードの適切な値を記述します。
dest_addr	リレーの送信先 IP アドレス（ユニキャストまたはマルチキャスト）です。
out_addr	マルチキャストのパケットを送信するインタフェースの IP アドレスです（省略できます）。明示的に設定しない場合、出力インタフェースが自動的に選択されます。
dest_ports	送信先のリレーの RTP ストリーミングのポート番号です。この番号は、偶数である必要があります。出力ポートの番号は、入力ポートの番号と一致する必要があります。ポート番号が一意で、重複していないことを確認してください。5000 以上で始まる空きポート番号を使用してください。
include	このキーワードに続けて、リレー設定ファイルのパスとファイル名を記述します。

設定ファイルでは、スペースを含む文字列を入力する場合、文字列を引用符で囲む必要があります。たとえば、「My Streaming Server」ではなく「“ My Streaming Server ”」と入力します。

リレーを開始する／停止する

リレーを停止するときは、「/etc/streaming」ディレクトリにあるリレー設定ファイルを削除するか、名前を変更します。その後「QuickTime Streaming Server」をいったん停止してから再開します。

リレーを開始するときは、リレー設定ファイルを「/etc/streaming」ディレクトリに作成するか、またはコピーします。その後「QuickTime Streaming Server」をいったん停止してから再開します。

QuickTime Streaming Server に関する問題を解決する

Streaming Server Admin が応答しない場合：

「streamingadminserver.pl」スクリプトが実行されていることを確認します。実行されていない場合は、「/Applications/Utilities」にある「Terminal」アプリケーションを起動し、「su root」と入力し、管理者のパスワードを入力して、ルート管理者となります。次に、「Terminal」アプリケーションに「streamingadminserver.pl」と入力して、「Streaming Server Admin」プロセスを開始します。

サーバが開始しない場合、または突然終了してしまう場合：

- エラーログを確認します。
- 「QuickTimeStreamingServer」ファイルが「/usr/local/sbin/」ディレクトリにあるかを確かめます。

ストリーミングサーバコンピュータがクラッシュ、または再起動した場合：

- コンピュータが起動したら、プレイリストが再生中であることが「Streaming Server Admin」に示されていても、すべてのプレイリストを再開する必要があります。
- プレイリストを再開する前に、「QuickTime Streaming Server」が動作していることを確かめます。

メディアファイルが正しくストリーミングされない場合：

- エラーログを確認します。
- ムービーファイルが「QuickTime Streaming Server」に対応していることを確かめます。184 ページの互換性のあるファイルフォーマットのリストを確認します。
- サンプルムービーをストリーミングしてみて、サーバがそれをストリーミングできるかどうかを確認します。サンプルムービーは、サーバに付属しています。

  サンプルムービーがストリーミングされる場合は、ムービーファイルの作成方法に問題があると考えられます。ムービーを作成し直してください。

  サンプルムービーがストリーミングされない場合は、サーバコンピュータまたはネットワークに問題があると考えられます。

- 「サーバ用にヒントを最適化」オプションを選んで、ムービーをヒントし直してみてください。
- ストリーミングサーバの状況を確認し、必要であれば、最大接続数または最大スループットを減らします。
- 「Mac OS」クライアントコンピュータで問題が発生する場合は、クライアントコンピュータの「TCP/IP」コントロールパネルを開き、「MacIP」が選択されていないことを確認します。
- クライアントコンピュータで問題が発生する場合は、ユーザの「QuickTime 設定」コントロールパネルの「ストリーミングプロキシ」パネルと「ストリーミング・トランスポート」パネルが適切に設定されていることを確認します。クライアントコンピュータのネットワークの管理者は、正しい設定を提供することができます。
- 複数のライブストリーミングをリフレクトしている場合、それぞれのストリーミングで異なる UDP ポートが使用されていることを確認します。そうでない場合、クライアントコンピュータにエラー 500 のメッセージが表示されます。ポートはリレー設定ファイルで指定します。
- ブロードキャストするファイルフォーマットをクライアントソフトウェアがサポートしていることを確認します。
- URL が正しいかどうかを確認します。

ストリーミングサービスの速度が遅い場合：

- QuickTime ムービーをストリーミングしている場合、オーサリングアプリケーションを使ってムービーを独立再生形式にします。また、ストリーミングサービス用にヒントを最適化していることを確認します。
- 接続数の最大値またはスループットの最大値を減らします。
- ほかのサービスを停止します。
- サーバの性能を向上させるため、メディアファイルを別のハードディスクに保存します。

  「QuickTime Streaming Server」で使用できる「ムービーディレクトリ」は 1 つだけなので、「Streaming Server Admin」で選択した「ムービーディレクトリ」から別のハードディスクのメディアファイルへのリンクを作成する必要があります。そのためには、次のように操作します。

  - 「QuickTime Streaming Server」が動作しているコンピュータで、メディアが含まれているフォルダを、別のディスクから「ムービーディレクトリ」として選択しているフォルダに control キーを押しながらドラッグします。

ユーザがライブストリーミングメディアを視聴することができない場合：

- 音声機器または映像機器から、信号の取り込みとエンコードに使用するコンピュータに信号を取り込んでいることを確認します。
- SDP ファイルが、ストリーミングサーバの「ムービーディレクトリ」に保存されていることを確認します。

QuickTime Streaming Server に関するその他の情報

「QuickTime Streaming Server」について詳しくは、以下を参照してください。

- 「QuickTime Streaming Server」の Web サイト：

  www.apple.co.jp/quicktime/authoring/qtss/

- IP Multicast Initiative の Web サイト

  www.iijnet.or.jp/ipmulticast/

- ディスカッションメーリングリスト

  lists.apple.com

  「QuickTime Streaming Server」の開発者の方は、Streaming-Server-Developers リストを探してください。

  「QuickTime Streaming Server」のユーザの方は、Streaming-Server-Users リストを探してください。

10

Macintosh マネージメントサービス

Macintosh マネージメントサービスとは？

Macintosh マネージメントサービスによって、アプリケーション、ファイルサーバボリューム、およびプリンタへのユーザアクセスを制御するためのネットワーク全体のポリシーを設定することができます。ユーザがログインしたときに表示される環境を定義することもできます。「Macintosh マネージャ」は、「NetBoot」クライアントコンピュータに認証および初期設定管理を提供する場合、特に役に立ちます。

Macintosh マネージメントサービスを使用する状況

次の状況に当てはまる場合は、Macintosh マネージメントサービスの使用を検討してください。

- Macintoshコンピュータで構成されるネットワークの管理にかかるコストを削減したい
- ユーザがどのコンピュータからでも自分の書類にアクセスできるようにすると同時に、一貫性のある制御されたインタフェースを提供したい
- 管理部門、教室、人の出入りが自由な研究室など、重要な場所でのコンピュータ使用に対してセキュリティを設定する必要がある

例：Macintosh マネージャを使ってコンピュータへのアクセスを制御する

ムービーを制作および編集するために、多数の Macintosh コンピュータを新しく購入したとします。場所に余裕がないので、新しいコンピュータを、普段使っているほかのコンピュータと一緒に、人の出入りが自由な研究室に設置しなければなりませんでした。「Macintosh マネージャ」を使用すると、ビデオの制作作業に関わるユーザだけに新しいコンピュータを確保することができます。このためには、特定のユーザを「ビデオ制作」ワークグループに割り当て、ビデオ制作用コンピュータの特別な「リスト」を作成し、ビデオ制作ワークグループにのみ、そのコンピュータへのアクセスを許可します。

Macintosh マネージャを設定する前に

「Macintosh マネージャ」を設定する前に、以下のシステム要件が満たされていることを確認します。

クライアントコンピュータの要件

- 「Mac OS 8.1」～「Mac OS 9.x」
- 使用可能な RAM が 1 MB 以上
- 「パネル」環境を使用する場合は 16 ビットモニタを推奨

管理コンピュータの要件

- 「Mac OS 9」以降、または「Mac OS X」
- 使用可能な RAM が 2 MB 以上
- 800 × 600 以上の解像度を持つモニタ

Macintosh マネージャを初めて設定する

「Macintosh マネージャ」の基本的な初期設定を行うときは、次のように操作します。

手順 1：ホームディレクトリを持つユーザが、「ユーザとグループ」に存在することを確認する

「Macintosh マネージャ」に読み込まれたユーザは、最初に「Mac OS X Server」の「ユーザとグループ」データベースに存在している必要があります。読み込みを行う予定のユーザには、ホームディレクトリも必要です。詳しくは、59 ページの「ユーザとグループを初めて設定する」を参照してください。

手順 2：Macintosh マネージメントサービスが稼動中であることを確認する

「Server Admin」の「Macintosh マネージャ」モジュールを使って、サービスが稼動しているかどうかを確認します。サービスが稼動している場合は、サービスのアイコンに地球のマークが表示され、最初のメニュー項目が「Macintosh マネージャサービスを停止」になります。メニュー項目が「Macintosh マネージャサービスを開始」の場合は、それを選んで「Macintosh マネージャ」を開始します。

手順 3：管理者としてログインする

「Server Admin」の「Macintosh Mgr」モジュールを使用するか、「Dock」の「Macintosh マネージャ」アイコンをクリックして、「Macintosh マネージャ」を開きます。「Mac OS X Server」の管理者アカウントを使って、サーバにログインします。（これ以降は、このアカウントを使って、または設定したほかの管理者アカウントを使って、ログインすることができます。）

手順 4：ユーザアカウントを追加する

「Macintosh マネージャ」の「ユーザ」パネルで、「Mac OS X Server」からユーザを読み込みます。ユーザアカウントと共に、名前やメールアドレスなどの必須のユーザ情報が、「Macintosh マネージャ」に読み込まれます。ユーザをすぐに読み込まない場合は、「その他のユーザ」アカウントを設定して、「Mac OS X Server」名とパスワードを使用したアクセスをただちにユーザに許可できます（228 ページの「読み込まれていないユーザにすばやいアクセスを提供する」を参照してください）。ユーザを追加したら、「Macintosh マネージャ」固有のオプション（ユーザのタイプや所属グループなど）を設定することもできます。

手順 5：Macintosh マネージャの管理者を作成する

「Macintosh マネージャ」の管理者アカウントを少なくとも 1 つ作成し、ほかのユーザがセキュリティを省略できないようにする必要があります。「Macintosh マネージャ」の管理者は、すべての「Macintosh マネージャ」設定を管理します。また、各ユーザのパスワードを使ってそのユーザ（ほかの「Macintosh マネージャ」管理者を除く）としてログインできます。

ユーザアカウントやワークグループを追加したり変更したりする権限が必要なほかの人（教師や技術的なコーディネータなど）に対して、ワークグループ管理者のアカウントを設定することもできます。提出フォルダにアクセスすることもできます。ワークグループの管理者は、Macintosh マネージャの管理者がアクセスするための「Macintosh マネージャ」機能のすべてを使用します。

手順 6：ワークグループを作成する

ユーザのワークグループを少なくとも 1 つ作成する必要があります。ワークグループによって、アクセス権、およびソフトウェア、プリンタ、コンピュータなどの共有リソースに基づいてユーザをグループ化できます。たとえば、特定のタイプのユーザを対象に 1 つのワークグループを作成し、あるプロジェクトで特定のプリンタを使用する必要があるユーザを対象に別のワークグループを作成できます。

ユーザは、ワークグループに割り当てられるまで、「Macintosh マネージャ」ネットワークにログインできません。（ユーザは複数のワークグループに所属できます。）

詳しくは、229 ページの「ネットワークの要望を満たすワークグループを作成する」を参照してください。

手順 7：セキュリティオプションを設定する

「グローバル」パネルでいくつかのセキュリティオプションを設定することによって、情報を保護し、ネットワークへのアクセスを制御する必要があります。

ネットワークに「Mac OS 9」より以前のクライアントコンピュータが含まれている場合は、「グローバル」パネル内の「セキュリティ」パネルを使って、ユーザの初期設定（デスクトップのピクチャや Web ブラウザの設定とよく使う項目など）をどのように取り扱い、「Mac OS 9」より以前のクライアントユーザに対してどのように保存するかを指定します。次のいずれかを選びます。

- “ 初期設定 ”フォルダ全体をコピーする： ユーザの「初期設定」フォルダ内のすべての項目が、その内容や大きさにかかわらず、ログイン時にサーバからコピーされ、ログアウト時にはサーバにコピーされます。不要な項目や大きな項目をコピーすると、ログイン時間とログアウト時間が増える可能性があるので注意してください。

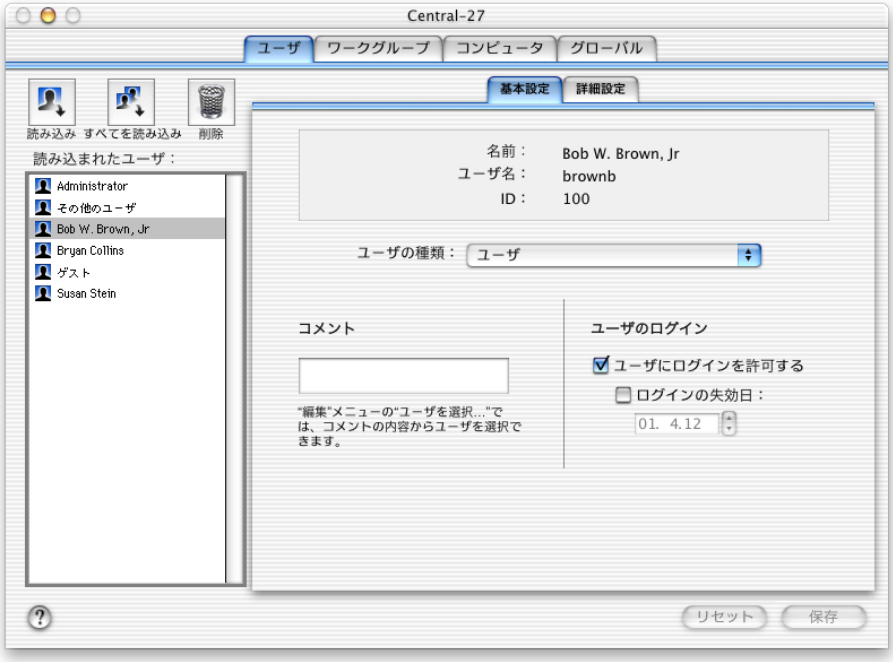
- インターネットまたは管理者が定義した初期設定だけをコピーする：「Managed Preferences」を使用している場合は、「Preserved Preferences」フォルダ内の初期設定がコピーされます（232 ページの「Macintosh マネージャが初期設定に従って動作する仕組み」）。「Managed Preferences」フォルダを使用していない場合は、ユーザのログイン時に、次のファイルとフォルダがサーバからコピーされます。「StuffIt Expander Preferences」、「RealAudio™ Player Preferences」、「Internet Preferences」、「NCSA Telnet Preferences」、「Fetch Prefs」、「NewsWatcher Prefs」、「JPEGView Preferences」、「Netscape」、および「Explorer」（「Netscape」フォルダと「Explorer」フォルダ内のキャッシュフォルダは削除されます）。

Macintosh マネージャの設定

Macintosh マネージメントサービスの設定にアクセスするには、「Macintosh マネージャ」を開いて、サーバにログインし、変更する設定のタブをクリックします。

ユーザの基本設定

「ユーザ」パネル内の「基本設定」パネルでは、「Macintosh マネージャ」ユーザの基本オプションを設定できます。



名前、ユーザ名、および ID

これらの要素は、「ユーザとグループ」データベースから読み込まれます。ここで変更することはできません。

「ユーザ名」は、「Server Admin」アプリケーションで設定したユーザ名です。ユーザは、フルネームの代わりにユーザ名を使って「Macintosh マネージャ」やほかのネットワークサービスにログインします。ユーザがメールアドレスを持っていない場合、「Macintosh マネージャ」はユーザ名および「コンピュータ」パネル内の「コントロール」パネルで指定したドメインに基づいて、アドレスを割り当てることができます。

ユーザの種類

「ユーザの種類」ポップアップメニューを使用すると、次の 3 種類のユーザアカウントのいずれかをユーザに割り当てることができます。

- 「ユーザ」アカウントは、日常業務でコンピュータを使用する人々（通常は学生や従業員）が使用します。この種類のユーザには、「Macintosh マネージャ」管理アプリケーションを使用する権限がありません。
- 「ワークグループ管理者」アカウントは、ユーザアカウントやワークグループを追加または変更する権限を必要とする人々（通常は教師や管理者）が使用します。「Macintosh マネージャ」の管理者は、ワークグループ管理者に使用を許可する「Macintosh マネージャ」の機能を決定します。ワークグループ管理者は、管理する各ワークグループのメンバーであることが必要です。
- 「Macintosh マネージャ管理者」アカウントは、ネットワークを管理する人々、およびすべてのユーザやワークグループに影響を与えるオプションを設定する人々が使用します。「Macintosh マネージャ」管理者は、有効な「Macintosh マネージャ」の機能すべてを使用できます。ワークグループ管理者や「Macintosh マネージャ」管理者のアカウントを設定できるのは、このタイプのユーザだけです。

各ユーザおよびワークグループ管理者をワークグループに割り当てる必要があります。そうしないと、ユーザはログインできません。

コメント

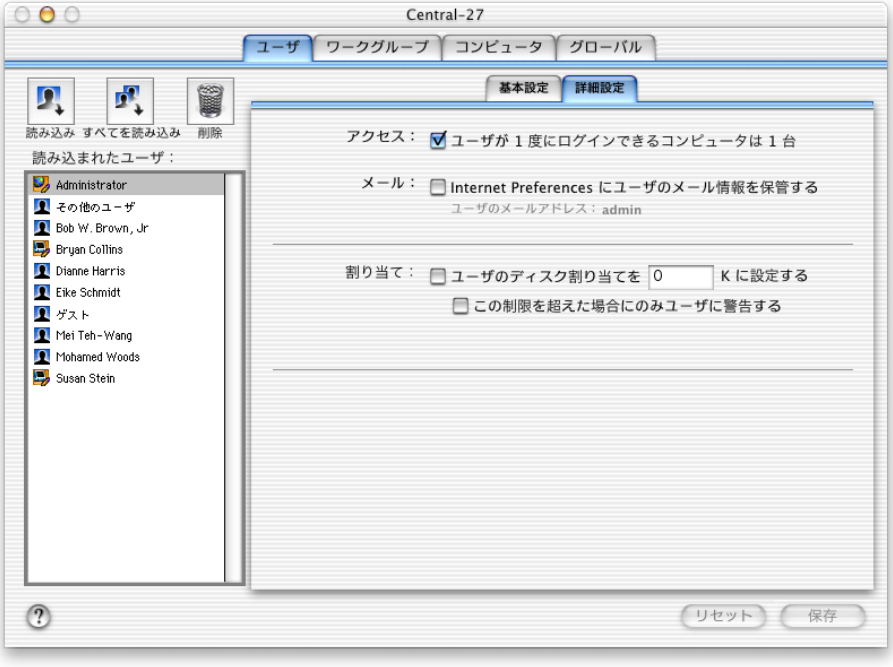
ユーザの識別に役立つ任意の情報を入力できます（半角 63 文字、全角 31 文字まで）。

ユーザのログイン

- 「ユーザにログインを許可する」を選ぶと、「Macintosh マネージャ」を使って管理するすべてのコンピュータにログインできます。この設定を使用不可にすることで、ユーザアカウントをただちに取り除くことができます。
- 「ログインの失効日」を選ぶと、指定した日付に「Macintosh マネージャ」内のユーザアカウントが無効になります。

ユーザの詳細設定

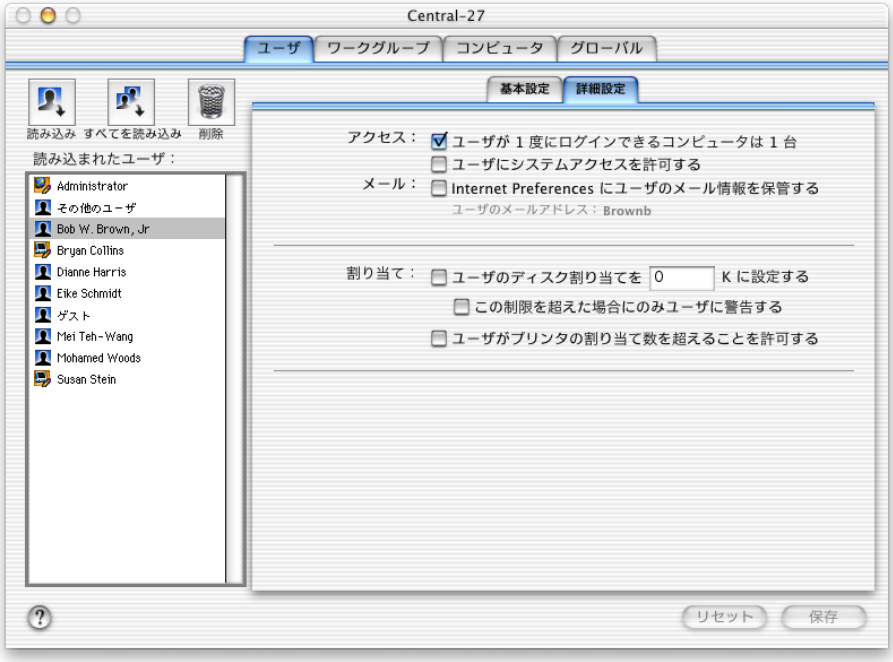
「ユーザ」パネル内の「詳細設定」パネルでは、「Macintosh マネージャ」ユーザの詳細オプションを設定できます。ユーザの種類（「基本設定」パネルで設定）により、表示されるオプションは異なります。



「Macintosh マネージャ」管理者用の「詳細設定」パネル

アクセス

- 「ユーザが 1 度にログインできるコンピュータは 1 台」を選ぶと、ユーザが一度に許可される接続は、この「Macintosh Management Server」に接続されたコンピュータのうちの 1 台のみになります。この制限を適用されたユーザは、使用しているコンピュータからログアウトしてからでないと、別のコンピュータにログインまたはチェックアウトできません。



ユーザ用の「詳細設定」パネル

- 「ユーザにシステムアクセスを許可する」を選ぶと、ユーザは、「Finder」および「システムフォルダ」を含む、クライアントコンピュータのすべての項目にアクセスできます。システムアクセスが可能なユーザがクライアントコンピュータにログインすると、ログインダイアログに「システムアクセス」が選択肢の 1 つとして表示されます。「Macintosh マネージャ」管理者は、常にシステムアクセスできます。

メール

「Internet Preferences にユーザメール情報を保管する」を選ぶと、ユーザのログイン時に「Macintosh マネージャ」がメールサーバをチェックしてメッセージを確認します。ユーザは、POP（Post Office Protocol）または IMAP メールアカウントを持っている必要があります。「Macintosh マネージャ」にユーザを最初に読み込む際、各ユーザのメールアカウント名およびメールサーバのデータが、ほかのユーザデータとともに「Mac OS X Server」ユーザデータベースから読み込まれます。ユーザのメール情報が「Mac OS X Server」データベースに存在しない場合、「コンピュータ」パネル内の「コントロール」パネルにメールサーバのデータを入力できます。

「Macintosh マネージャ」でメールの自動チェックを設定するには、「ワークグループ」パネル内の「オプション」パネルで、ログイン時のメールチェックを有効にする必要があります。また、ユーザがメールソフトウェアにアクセスする必要もあります。

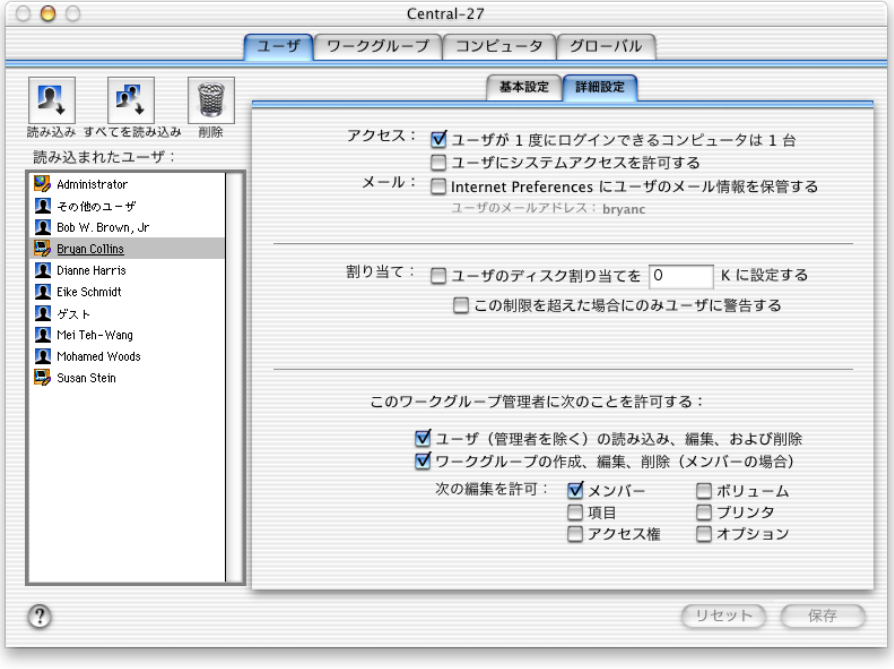
割り当て

- 「ユーザのディスク割り当てを _K に設定する」を選び、フィールドに値を入力すると、ユーザがホームディレクトリで使用可能なディスク容量を制限できます。「この制限を超えた場合にのみユーザに警告する」を選ぶと、ディスク容量の制限を超えた場合、「Macintosh マネージャ」からユーザに警告が表示されます。ただし、ユーザが追加文書を保存できなくなることはありません。
- 「ユーザがプリンタの割り当て数を超えることを許可する」を選ぶと、ユーザは、「ワークグループ」パネル内の「プリンタ」パネルで設定されたプリンタの割り当てを超過できるようになります。

参考：「その他のユーザ」を選んだ場合、「詳細設定」パネルには「ユーザがプリンタの割り当て数を超えることを許可する」だけが表示されます。

このワークグループ管理者に次のことを許可する

「ユーザ（管理者を除く）の読み込み、編集、および削除」および「ワークグループの作成、編集、削除（メンバーの場合）」を選択すると、ユーザが該当するタスクを実行できるようになります。これらの設定は、ユーザがワークグループ管理者である場合にのみ表示されます。



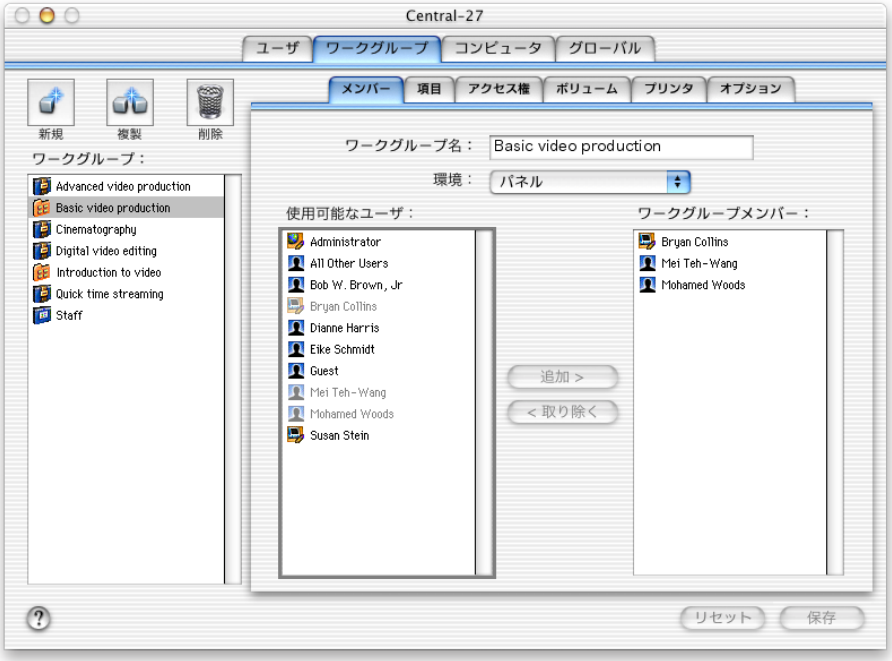
ワークグループ用の「詳細設定」パネル

次の編集を許可

ユーザにワークグループの作成、編集、および削除を許可する場合、ワークグループ管理者が変更できるようにするワークグループの設定パネルを選択します。たとえば、ユーザをワークグループに追加、またはワークグループから削除できるようにあるユーザを設定するときワークグループのほかの設定は変更できないようにしたい場合、「メンバー」オプションだけを選択することもできます。

ワークグループのメンバー設定

「ワークグループ」パネル内の「メンバー」パネルで、環境の選択およびワークグループへのメンバーの追加を実行できます。各ユーザまたはワークグループ管理者は、ログインするために少なくとも 1 つのワークグループに割り当てられる必要があります。ユーザは、最大 42 までのワークグループのメンバーになれます。



ワークグループ名

ワークグループ名には、ピリオド、アンダースコア、ダッシュ、空白など、キーボードから入力可能な文字の大半を含めることができます（コロン（:）を除く）。ただし、半角で 31 文字、全角で 15 文字を超えてはなりません。

環境

「環境」で、ワークグループ内のユーザに表示されるインタフェース、およびワークグループのメンバーが持つネットワークリソースへのアクセス権のタイプが決まります。設定可能な環境は、次の 3 タイプです。

- 「Finder」は、「Mac OS」の標準デスクトップです。ユーザには、ほとんど制限が課されません。
- 「制限付き Finder」は、「Mac OS」の標準デスクトップに似ていますが、ユーザが実行可能な操作を制限することにより、ワークステーションの不正操作を防ぎます。
- 「パネル」は、初心者（特に子供たち）がコンピュータを容易に利用できるように、大きなアイコンを使用した単純なインタフェースを提供します。「パネル」環境では、ユーザが起動ボリュームに直接アクセスしないため、最大限のセキュリティが維持されます。サーバボリュームやリムーバブルメディアへのアクセスを許可すると、各ボリュームやメディアが、マウント時にパネルとして表示されます。「コンピュータ」パネル内の「ログイン」パネルで、ワークグループおよびユーザ書類パネルの名前を指定できます。

使用可能なユーザ

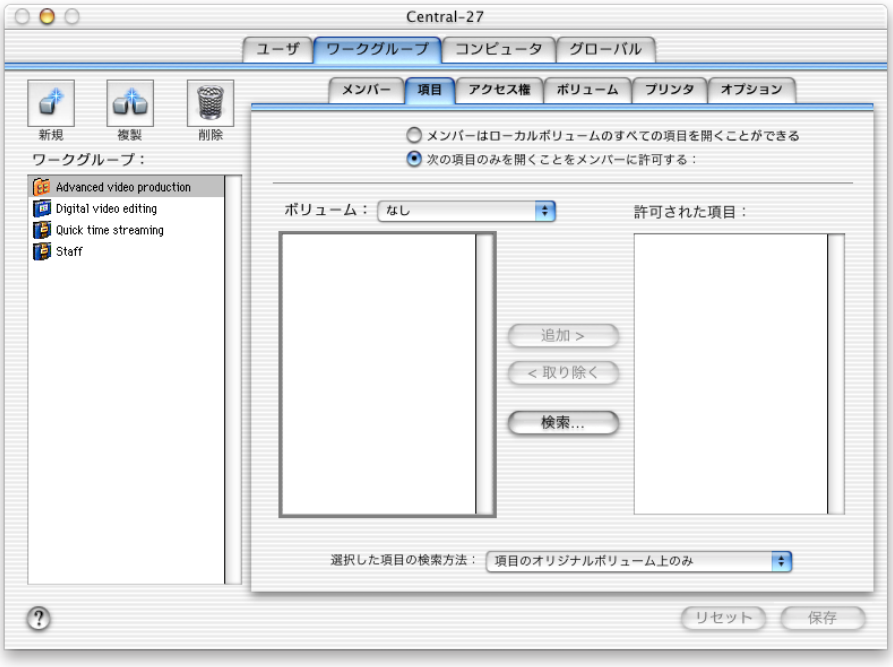
このリストで、「その他のユーザ」アカウントを含む、読み込まれたすべての「Macintosh マネージャ」ユーザの名前が表示されます。リスト内でユーザをクリックしてから、「追加」をクリックし、ワークグループにユーザを追加します。このリストでユーザをクリックして、「ワークグループメンバー」リストにドラッグすることもできます。

ワークグループメンバー

「ワークグループメンバー」のユーザの種類は、ユーザ、ワークグループ管理者、「Macintosh マネージャ」管理者のいずれかになります。ワークグループは、最大 1500 までのメンバーを保持できます。ワークグループからユーザを削除するときは、リストでユーザを選び、「取り除く」をクリックします。

ワークグループの項目設定

「ワークグループ」パネル内の「項目」パネルを使用すると、クライアントコンピュータのファイルおよびアプリケーションを、ワークグループメンバーから利用可能にできます。



メンバーはローカルボリュームのすべての項目を開くことができる

このオプションを選ぶと、メンバーはローカルボリューム上の任意のファイルを開くことができます。このオプションを選ぶと、「ショートカット項目」リストも設定できます。ワークグループメンバーは、ここで設定する一群のアプリケーションにすばやくアクセスできます。

次の項目のみを開くことをメンバーに許可する

このオプションを選ぶと、ワークグループメンバーからのアクセスが、選択した項目のみに制限されます。このオプションを選ぶ場合、下の「許可された項目」リストを設定する必要があります。

ボリューム

ショートカット項目または許可された項目を設定する場合、「ボリューム」ポップアップメニューで、項目が存在するボリュームを選びます。選択したボリュームに存在する項目が、下のフィールドに表示されます。該当する項目を選択してドラッグするか、「追加」をクリックして、右のリストに追加します。

ショートカット項目

ワークグループのメンバーにすべての項目へのアクセスを許可しているか、「Finder」ワークグループの場合に、このリストが表示されます。メンバーは、リストに追加された項目にすばやくアクセスできます。これらのアイテムは、「制限付き Finder」ワークグループのフォルダ内、および「パネル」ワークグループのパネル上にまとめて表示されます。ショートカット項目のリストは、必要な場合に設定してください。

参考：「Finder」環境では、「ショートカット項目」リストだけが表示されます。リストに項目を追加すると、追加した項目のエイリアスがユーザのデスクトップに表示されます。

許可された項目

ワークグループのメンバーに、選択した項目だけを開く許可を与えている場合、このリストが表示されます。ユーザにアクセスを許可する項目をすべて、「許可された項目」リストに追加する必要があります。これらのアイテムは、「制限付き Finder」ワークグループのフォルダ内、および「パネル」ワークグループのパネル上にまとめて表示されます。

選択した項目の検索方法

アプリケーションまたは書類を「許可された項目」とした場合、その項目は元のアプリケーションまたは書類のエイリアスとして保存されます。ユーザのログイン時に、コンピュータは許可された項目の元のファイルをそれぞれ検索し、そのエイリアスをクライアントコンピュータにダウンロードします。

「選択した項目の検索方法」ポップアップメニューで次のいずれかを選ぶことにより、コンピュータがワークグループ項目を検索する場所を指定できます。

- 「項目のオリジナルボリューム上のみ」を選ぶと、項目が最初に存在していたボリューム上（サーバボリュームまたはローカルボリューム）で検索を実行します。コンピュータが検索できるのは、マウントされたボリュームだけです。
- 「まずローカルボリューム上から」を選ぶと、クライアントコンピュータから利用可能なローカルボリュームだけで検索を実行します。項目が見つからず、かつ元の項目がサーバ上に存在していた場合、コンピュータは、マウントされたボリュームをすべて検索します。
- 「まずワークグループサーバのボリューム上から」を選ぶと、ワークグループが保存されたボリュームで検索を実行します。項目が見つからない場合、コンピュータは起動ボリュームおよびほかのローカルボリューム上で項目を検索します。
- 「ローカルボリューム上のみ」を選ぶと、ローカルにマウントされたボリューム（起動ボリューム、追加パーティション、および直接接続されたハードディスクを含む）で項目が検索されます。
- 「ワークグループサーバのボリューム上のみ」を選ぶと、コンピュータは、そのワークグループ用にマウントされたすべての AFP（Apple Filing Protocol）ボリュームで、項目を検索します。これらのボリューム内で項目が見つからない場合、その項目を開くことはできません。

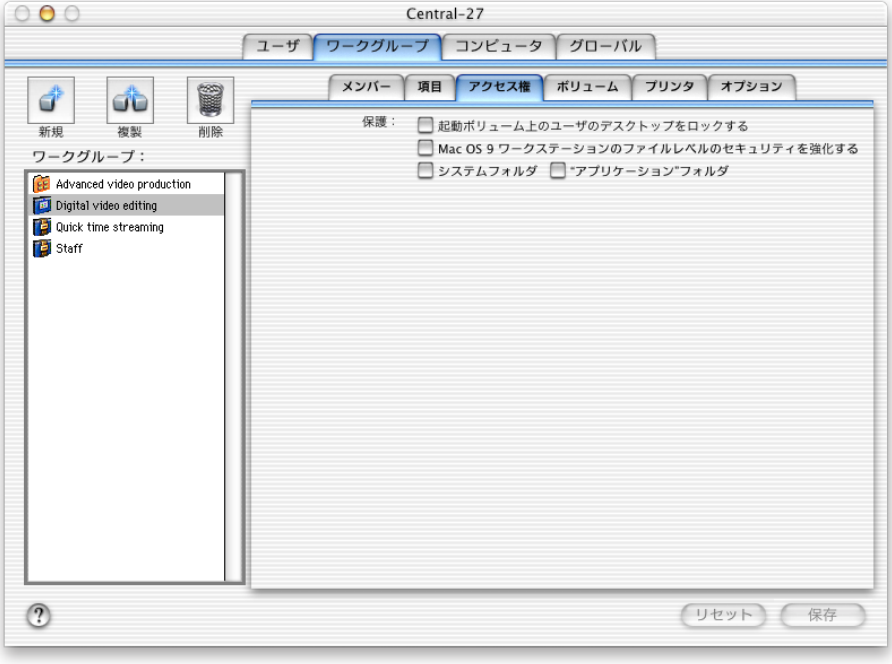
「NetBoot」クライアントコンピュータの場合、ローカルボリュームは、コンピュータ内のハードディスク、またはコンピュータに直接接続されたすべての外部ハードディスクになることに注意してください。「NetBoot」クライアントコンピュータの起動ボリュームは、リモートボリュームですが、ローカルボリュームのように扱われます。

重要　個人ファイルの共有が有効になっているか、AFP ファイルサービスを実行中のコンピュータで「Macintosh マネージャ」アプリケーションを使用している場合、ワークステーションの項目を承認すると、予期しない結果になることがあります。問題が発生した場合は、ファイルサービスがインストールされていないコンピュータで、「Macintosh マネージャ」を使用してください。「選択した項目の検索方法」で「ローカルボリューム上のみ」を選択した状態ですべての項目を承認する場合、予期しない結果にはならず、ファイルサービスが稼動しているコンピュータで「Macintosh マネージャ」を使用できます。

ワークグループの権限設定

「ワークグループ」パネル内の「アクセス権」パネルでは、各ワークグループのさまざまなの設定を選ぶことができます。

ワークグループに設定可能な権限は、ワークグループのデスクトップ環境によって異なります。「Finder」ワークグループの権限の大半は制限できません。一方、「パネル」および「制限付きFinder」ワークグループには、設定可能な多数のオプションが存在します。

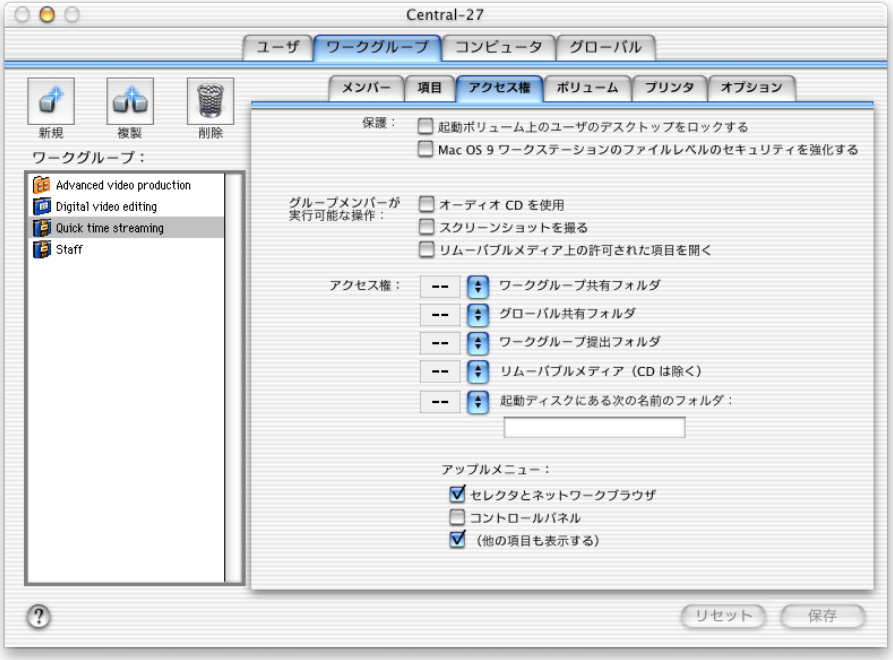


「Finder」ワークグループの「アクセス権」パネル

保護

アプリケーションからクライアントコンピュータの特定の領域を変更できるかどうかを制御することにより、ワークステーションのセキュリティを強化できます。

- 「起動ボリューム上のユーザのデスクトップをロックする」を選ぶと、ユーザまたはアプリケーションがデスクトップに対して変更または書き込みを行うことができなくなります。
- 「Mac OS 9 ワークステーションのファイルレベルのセキュリティを強化する」を選ぶと、厳密なセキュリティ保護を設定できます。ファイルレベルのセキュリティを強化すると、アプリケーションから制限された領域に書き込むことができなくなります。ただし、以前のアプリケーションの中には適正に起動しないか、ディスクエラーを表示するものもあります。ファイルレベルのセキュリティを設定しない場合、アプリケーションは任意の場所に情報を書き込むことができます。
- 「システムフォルダ」および“アプリケーション”フォルダ」を選択すると、「システムフォルダ」、「アプリケーション」フォルダのいずれかまたは両方（「Finder」ワークグループの場合）を保護できます。前もって「アプリケーション」フォルダを作成して、起動ディスクのトップレベルに配置しておく必要があります。



「制限付き Finder」ワークグループの「アクセス権」パネル

グループメンバーが実行可能な操作

- 「パネル」および「制限付き Finder」ワークグループのメンバーにコンピュータでのオーディオ CD の再生を許可する場合は、「オーディオ CD を使用」を選びます。オーディオ CD とは、最初のトラックにオーディオデータが格納された CD のことです。クライアントコンピュータは、オーディオ CD を個別に識別することができません。このため、指定できるのは、すべてのオーディオ CD へのアクセスを許可するか、または制限するかになります。
- 「パネル」および「制限付き Finder」ワークグループのメンバーにスクリーンショットの撮影を許可する場合は、「スクリーンショットを撮る」を選びます。スクリーンショットは、ユーザの「書類」フォルダに自動的に保存されます。ディスク領域が不足する恐れがある場合、ユーザによるスクリーンショットの撮影を制限してください。
- 「パネル」および「制限付き Finder」ワークグループのメンバーに対し、リムーバブルメディア（CD 以外）上の任意のアプリケーションを開くことを許可する場合、「リムーバブルメディア上の許可された項目を開く」を選びます。「グローバル」パネル内の「CD-ROM」パネルで、CD および DVD に対するオプションを設定できます。リムーバブルメディア上の承認されたアプリケーションを開くことをユーザに許可する場合、クライアントコンピュータがウイルスの影響を受けやすくなることに注意してください。ウイルスに感染する危険を減らすため、使用する前にリムーバブルメディアのウイルスチェックを行わない限り、この設定を無効にしてください。

アクセス権

次の場所に対して、「読み出し専用」、「書き込み専用」、「読み出し／書き込み」、またはアクセス権なしのいずれかを選ぶことができます。

- ワークグループ共有フォルダ：「オプション」パネルでワークグループデータボリュームを選ぶと、このフォルダがワークグループ用に作成されます。このフォルダを使用できるのは、ワークグループのメンバーだけです。
- グローバル共有フォルダ：「オプション」パネルでワークグループデータボリュームを選ぶと、このフォルダが作成されます。ワークグループフォルダを同じボリューム上に保持するすべてのワークグループのメンバーは、そのフォルダにアクセスできます。
- ワークグループ提出フォルダ：「オプション」パネルでワークグループデータボリュームを選ぶと、ワークグループの受け渡し用フォルダを設定できます。この機能を利用するには、少なくとも 1 人のワークグループ管理者または「Macintosh マネージャ」管理者がワークグループのメンバーであることが必要です。フォルダを表示できるのは、管理者だけです。ワークグループのメンバーは、「パネル」環境で「ファイル」メニューの「提出」を選ぶか、「制限付き Finder」環境で項目を「提出」フォルダにドラッグすることにより、項目をフォルダに含めます。
- リムーバブルメディア（CD は除く）： これには、フロッピーディスク、Zip ディスク、および着脱可能なその他のすべてのメディアが含まれます（CD を除く）。CD および DVD に対するオプションは、「グローバル」パネル内の「CD-ROM」パネルで設定できます。

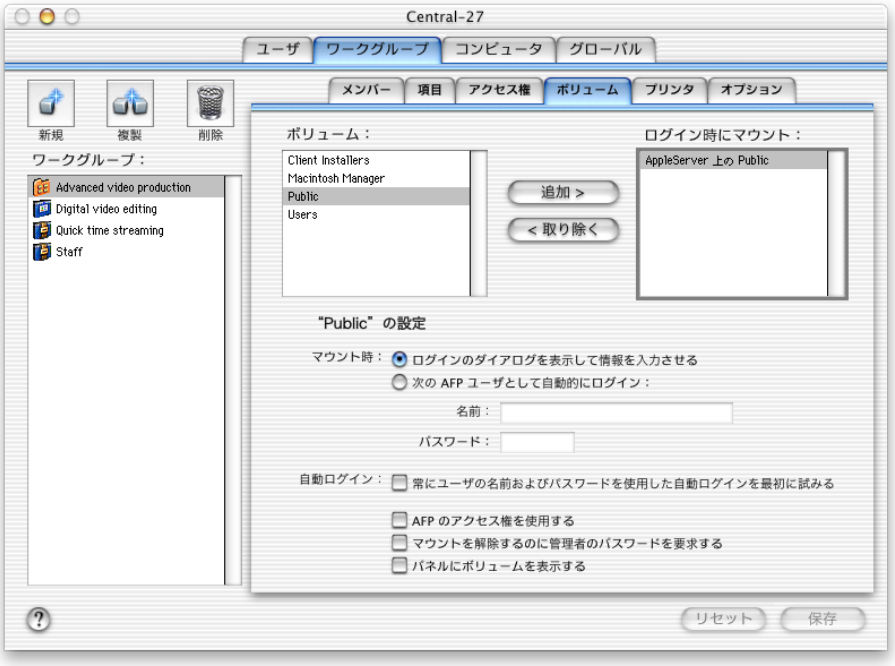
- 起動ディスクにある次の名前のフォルダ：「Macintosh マネージャ」管理者は、クライアントコンピュータの起動ディスクに、役割の異なる 2 つのタイプのフォルダを作成できます。最初のタイプは、任意の名前（Scratch など）を付けることのできる標準フォルダで、「読み出し専用」または「読み出し／書き込み」を設定することができます。このタイプのフォルダは、クリップアートの保存用、または Web ブラウザのダウンロード用に使用できます。また、ビデオおよびオーディオキャプチャアプリケーションの作業ファイルは、リモートボリュームに保存したり、リモートボリュームからコピーする必要がないため、このタイプのフォルダに保存するのに適しています。もう 1 つのタイプのフォルダでは、フォルダに黒丸（option + 8）で始まる名前（•Special Apps など）を付けることにより、フォルダのコンテンツに特別なアクセス権を設定できます。フォルダ名が黒丸で始まる場合、ユーザはそのフォルダ内の任意のアプリケーションを開くことができます。そのアプリケーションが、ユーザのワークグループの承認された項目のリストに含まれているかどうかには影響されません。たとえば、高度なグラフィックス環境を実装する研究室では、「iMovie」ではなく、「Final Cut Pro」がインストールされたコンピュータが数台存在することがあります。管理者は、これら数台のコンピュータ用に別のワークグループを作成する代わりに、名前が黒丸で始まる特別なフォルダをコンピュータに作成し、その内部に「Final Cut Pro」を格納できます。同じワークグループに所属するほかのコンピュータのユーザには、保存場所として使用可能な空のフォルダが表示されます。特別なフォルダに「Final Cut Pro」がインストールされたコンピュータのユーザは、使用するコンピュータ上の「Final Cut Pro」だけを開くことができます。この機能は、「制限付き Finder」および「パネル」ワークグループの両方で有効です。特別なフォルダを使用する場合、特別な注意が必要です。このフォルダにコピーされたアプリケーションはすべて、開くことが可能になります。このため、開いてはならないアプリケーションがローカルハードディスク上に存在する場合、そのアプリケーションをコンピュータから取り除く必要があります。

アップルメニュー

「セレクタとネットワークブラウザ」、「コントロールパネル」、および「（ほかの項目も表示する）」のうち、「パネル」および「制限付き Finder」ワークグループのメンバーのアップルメニューに表示する項目を選びます。「パネル」ワークグループの場合、「ファイル」および「特別」メニューに表示される項目を制限することもできます。チェックされた項目がメニューに表示されます。3 タイプのワークグループのいずれの場合でも、使用が禁止されたコントロールパネルが存在します。これらのコントロールパネルは、「AppleTalk」、「日付と時刻」、「機能拡張マネージャ」、「ファイル共有」、「キーチェーンアクセス」、「作業環境マネージャ」、「マルチユーザ」、「起動ディスク」、および「TCP/IP」です。

ワークグループのボリューム設定

「ワークグループ」パネル内の「ボリューム」パネルを使って、各ワークグループのさまざまなボリューム設定を選ぶことができます。



ボリューム

このリストには、使用可能なすべてのボリュームが表示されます。「Server Admin」を使って設定されたすべての共有ポイントも、このリストに含まれます。ワークグループのメンバーのログイン時にボリュームがマウントされるようにするには、ボリュームを選んで右のリストにドラッグするか、ボリュームを選んでから「追加」をクリックします。

ログイン時にマウント

このリストには、ワークグループのユーザがクライアントコンピュータにログインするときに、マウントするように選択したすべてのボリュームが表示されます。リストからボリュームを取り除くには、目的の名前を選び、「取り除く」をクリックします。

マウント時

ボリュームのマウント時に、ログイン名およびパスワードが要求されます。次のオプションのいずれかを選ぶことにより、必要な情報を提供できます。

- 「Macintosh マネージャ」で使用するユーザ名およびパスワードを使用しないボリュームをマウントする場合、「ユーザにログインを促す」を選びます。ユーザには、ボリュームに対する有効な名前とパスワードの入力が求められます。
- 「この AFP ユーザとして自動的にログイン」を選ぶと、すべてのユーザに同じユーザ名でのログインが許可されます。この場合、アクセス権を個別に制御することも、サーバにログインしたユーザを追跡することもできないため、各ユーザにユーザ名の入力を求める場合と同じセキュリティを確保することはできません。

常にユーザの名前およびパスワードを使用した自動ログインを最初に試みる

このオプションを選ぶと、自動ログインが失敗した場合にのみ、マウントオプションとして選択した設定が使用されます。自動ログインを選択しない場合、使用されるオプションは、選択したマウントオプションだけです。

AFP のアクセス権を使用する

このオプションを選ぶと、すでに確立された AFP（Apple Filing Protocol）権限を使ってボリュームへのアクセスが制御されます。このオプションを使用できるのは、「パネル」および「制限付き Finder」環境だけです。

マウントを解除するのに管理者のパスワードを要求する

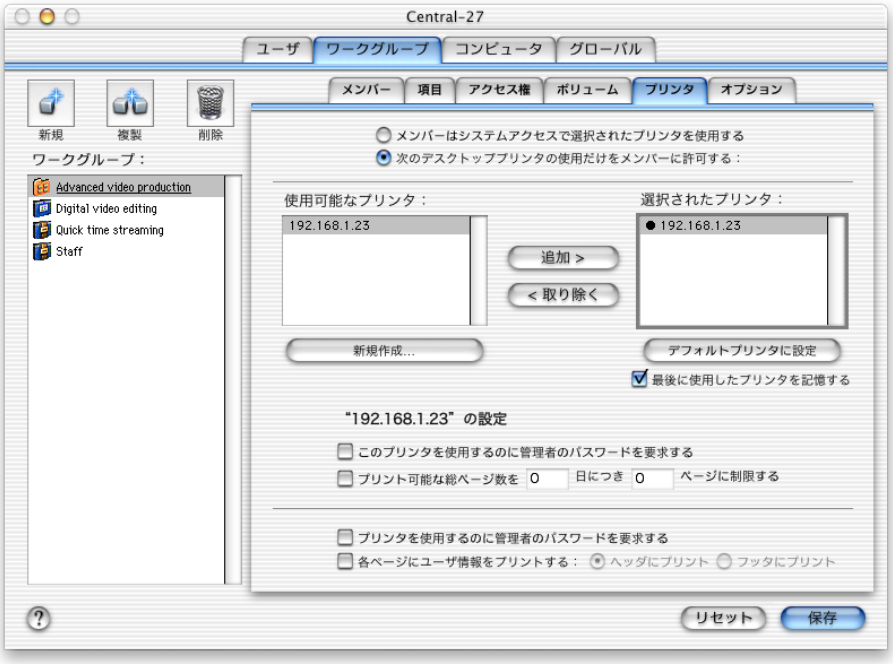
このオプションを選ぶと、ボリュームのマウント解除に、ワークグループ管理者または「Macintosh マネージャ」管理者のパスワードが必要になります。

パネルにボリュームを表示する

このオプションを選ぶと、「パネル」環境のパネルにボリュームが表示されます。

ワークグループのプリンタ設定

「ワークグループ」パネル内の「プリンタ」パネルを使って、各ワークグループのさまざまなプリンタ設定を選ぶことができます。



メンバーはシステムアクセスで選択されたプリンタを使用する

ユーザがプリントするとき、「システムアクセス」ワークグループを使ってログインしたユーザによって、または「Macintosh マネージャ」の起動前に別のユーザによってクライアントコンピュータのデフォルトプリンタに割り当てられたプリンタを使用するように設定する場合、このオプションを選びます。このプリンタをデスクトップ・プリンタにすることはできますが、必ずしもそうする必要はありません。使用するプリンタがデスクトップ・プリントに対応していない場合、このオプションを使ってユーザに印刷を許可する必要があります。

「システムアクセス」プリンタを設定する場合、管理者は「システムアクセス」ワークグループを使用して各クライアントコンピュータにログインし、「セレクタ」を使ってプリンタを選ぶ必要があります。ワークグループで「システムアクセス」プリンタの使用を指定し、クライアントコンピュータからプリンタを選ばないとき、コンピュータにログインするユーザは、「セレクタ」へのアクセス権がない場合、プリントできなくなります。「セレクタ」を表示可能なユーザは、表示された中からプリンタを選ぶことができます。「Mac OS X」で「Macintosh マネージャ」を使用する場合、「システムアクセス」プリンタとして選べるのは、PostScript™ 互換のプリンタだけです。

ユーザがクライアントコンピュータからログアウトする際、管理者が「システムアクセス」プリンタとして選択したプリンタが、再びデフォルトのプリンタになります。

次のデスクトッププリンタの使用だけをメンバーに許可する

このオプションを選ぶと、1 台以上のデスクトップ・プリンタをワークグループで使用できるようになります。「使用可能なプリンタ」リストから「選択されたプリンタ」に各プリンタをドラッグしてから、使用するプリンタをクリックし、設定を行います。デスクトップ・プリンタが「Macintosh マネージャ」で適正に動作するには、「システムアクセス」ワークグループでログインしたユーザが各クライアントコンピュータ上でそのプリンタの設定を行う必要があります。「システムアクセス」で設定されていないプリンタは、使用できない可能性があるか、安定した動作を期待できません。

使用可能なプリンタ

このリストには、ワークグループで使用可能なすべてのデスクトップ・プリンタが表示されます。プリンタを「選択されたプリンタ」リストに追加するには、プリンタを選択してから「追加」をクリックします。目的のデスクトップ・プリンタが表示されない場合、「新規作成」をクリックして設定できます。

選択されたプリンタ

このリストには、ワークグループで使用可能なすべてのデスクトップ・プリンタが表示されます。あるプリンタをワークグループのデフォルトプリンタにする場合、プリンタを選択してから「デフォルトプリンタに設定」をクリックします。

このプリンタを使用するのに管理者のパスワードを要求する

このオプションを選ぶと、選択したデスクトップ・プリンタを使用するために、ワークグループ管理者または「Macintosh マネージャ」管理者のパスワードが必要になります。ユーザに管理者パスワードを知らせることは決してしないでください。管理者アカウントのセキュリティを確保するために、管理者権限を保持しないワークグループ管理者アカウントを設定し、このアカウントのパスワードを使ってプリントを行うことができます。

プリント可能な総ページ数を _ 日につき _ ページに制限する

このオプションを選んで、ページ数および日数を入力すると、ワークグループのメンバーが指定した日数内にプリント可能なページ数が制限されます。「ユーザ」パネル内の「詳細設定」パネルで、この割り当てをユーザごとに上書きできます。割り当てを設定できるのは、デスクトップ・プリンタの割り当てだけです。

ページ数は、紙の枚数のことではなく、書類のページ数を指します。ユーザが 1 枚の紙に 2 ページプリントすると、ページ数は紙の枚数の 2 倍になります。プリントジョブが適正に終了したかどうかに関係なく（たとえば、紙詰まりがあっても）、ページ数は数えられます。

プリンタを使用するのに管理者のパスワードを要求する

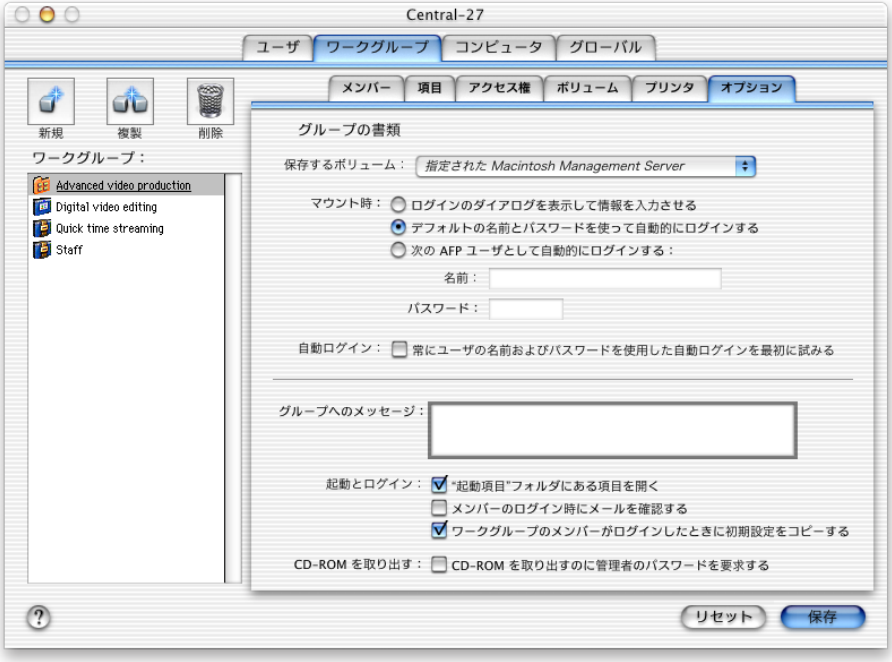
このオプションを選ぶと、任意のデスクトップ・プリンタまたは特定のデスクトップ・プリンタを使用するために、ワークグループ管理者または「Macintosh マネージャ」管理者のパスワードが必要になります。ユーザに管理者パスワードを知らせることは決してしないでください。管理者アカウントのセキュリティを確保するために、管理者権限を保持しないワークグループ管理者アカウントを設定し、このアカウントのパスワードを使ってプリントを行うことができます。

各ページにユーザ情報をプリントする

このオプションを選ぶと、各ページの一番上または一番下にユーザ名、ワークグループ名、プリント時刻がプリントされます。この情報により、ページ上のほかの情報が上書きされる場合があります。

ワークグループのオプション設定

「ワークグループ」パネル内の「オプション」パネルを使って、共有グループ書類ボリュームや、ログイン時に発生するイベントなど、各ワークグループのさまざまな設定を選ぶことができます。



保存するボリューム

ワークグループに共有書類の保存およびアクセスを可能にするボリュームを選択します。このボリュームは、ワークグループ共有ボリュームまたはワークグループデータボリュームと呼ばれます。

マウント時

ユーザがワークグループ共有ボリュームにログインする方法を選びます。

- 「ログインのダイアログを表示して情報を入力させる」は、ボリュームの有効な名前とパスワードの入力をユーザに要求します。この設定は、「Mac OS X Server」データベースからインポートしたユーザ名とパスワードを使用しないボリュームをマウントする場合に有用です。

- 「デフォルトの名前とパスワードを使って自動的にログインする」は、ワークグループボリュームとして「指定された Macintosh Management Server」を選んだ場合に設定できます。このオプションを選ぶと、コンピュータは、一般ユーザ名およびパスワードを使ってワークグループボリュームにログインします。一般ユーザは、自動的に設定されます。この場合、アクセス権を個別に制御することも、サーバにログインしたユーザを追跡することもできないため、各ユーザにユーザ名の入力を求める場合と同じセキュリティを確保することはできません。
- 「次の AFP ユーザとして自動的にログインする」は、すべてのユーザを同じユーザ名でログインします。この場合、アクセス権を個別に制御することも、サーバにログインしたユーザを追跡することもできないため、各ユーザにユーザ名の入力を求める場合と同じセキュリティを確保することはできません。

参考：「Macintosh マネージャ 2.0」では、ワークグループデータボリュームは、ユーザ書類の保存用ボリュームとは別のボリュームになります。ワークグループデータボリュームには、グローバル共有フォルダ、ワークグループ共有フォルダ、および「Managed Preferences」フォルダが含まれます。一方ユーザ書類は、「Mac OS X Server」の「ユーザとグループ」で定義されたホームディレクトリボリュームに保存されます。

常にユーザの名前およびパスワードを使用したログインを最初に試みる

このオプションを選ぶと、コンピュータは、ユーザの「Macintosh マネージャ」名およびパスワード（「Mac OS X Server」データベースから読み込まれた）を使ってワークグループボリュームへのログインを試みます。

グループへのメッセージ

ユーザがワークグループにログインするときに表示するメッセージを入力します。

起動とログイン

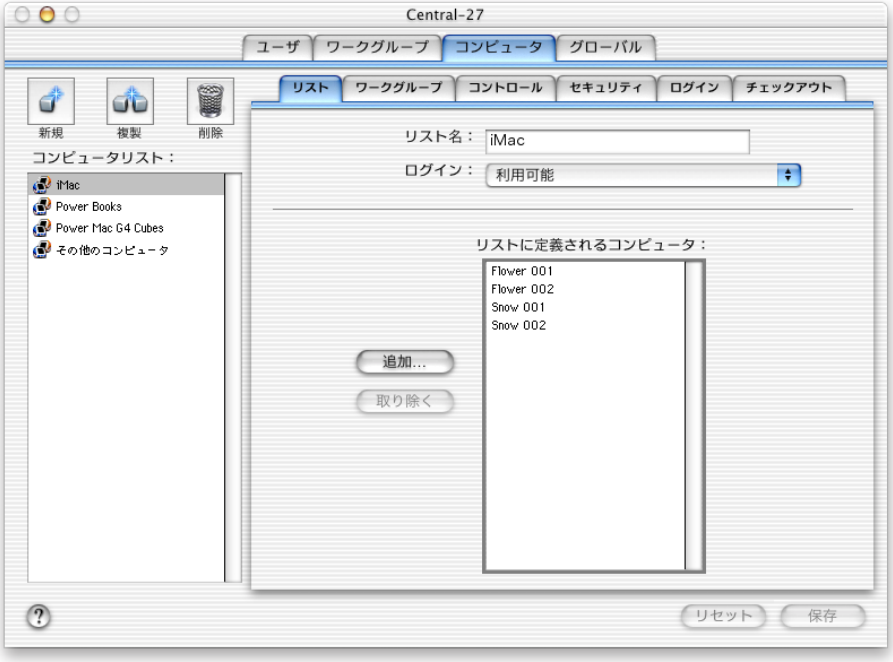
- 〝起動項目〟フォルダにある項目を開く」を選ぶと、「起動項目」フォルダ内の項目がユーザのログイン時に自動的に開きます。「Mac OS 9」以降のコンピュータでは、該当するフォルダは、「Macintosh Management Server」の「/Library/Startup Items」ディレクトリです。「Mac OS 9」より前のコンピュータでは、該当するフォルダは、クライアントのハードディスクの「システムフォルダ」内の「起動項目」フォルダです。
- 「メンバーのログイン時にメールを確認する」を選ぶと、ユーザが POP メールアカウントを持っている場合に、ログイン時にメールチェックが行われます。ユーザがメールアドレスを持っていない場合、「コンピュータ」パネル内の「コントロール」パネルでメールサーバの設定を行う必要があります。メールサーバの設定を行うと、「Macintosh マネージャ」がアドレスを生成します。
- 「ワークグループのメンバーがログインしたときに初期設定をコピーする」を選ぶと、ログイン時に「グローバル」パネル内の「セキュリティ」パネルで設定した初期設定がコピーされます（「Mac OS 9」より前のクライアントコンピュータのみ）。「Mac OS 9」以降のクライアントコンピュータでは、初期設定はサーバ上に保管されており、コピーする必要はないため、この設定は不要です。

CD-ROM ディスクを取り出す

「CD-ROM を取り出すのに管理者のパスワードを要求する」を選ぶと、CD-ROM ディスクを取り出すときに、ワークグループ管理者または「Macintosh マネージャ」管理者の名前とパスワードが必要になります（これは「Finder」ワークグループには適用されません）。

コンピュータのリスト設定

「リスト」パネルの設定内容は、選択中のコンピュータリストのすべてのコンピュータに適用されます。コンピュータリストを使用すると、コンピュータおよびワークグループにアクセス可能なユーザをさらに細かく設定できます。たとえば、職員で構成されるワークグループに、特定のコンピュータのセットを使用するように割り当てることができます。ネットワーク上のほかのコンピュータにログインするユーザは、職員を含めだれも「職員」ワークグループにアクセスすることはできなくなります。これにより、管理者はソフトウェアおよびハードウェアへのアクセスをより柔軟に制御できます。



リスト名

「リスト名」には、ピリオド、アンダースコア、ダッシュ、空白など、キーボードから入力可能な文字の大半を含めることができます（コロン（:）を除く）。ただし、半角で 31 文字、全角で 15 文字を超えてはなりません。

ログイン

「ログイン」ポップアップメニューには、4 つのオプションがあります。

- 「利用可能」を選ぶと、ユーザのログインが可能になります。コンピュータのメンテナンス作業（ソフトウェアのインストールやハードディスク整備用ソフトウェアの実行など）を行う場合を除き、通常はこれを選びます。
- 「利用不可 - ユーザが選択」を選ぶと、「システム終了」を選んで「Finder」を表示するか（管理者のパスワードが要求されます）、「Macintosh マネージャ」サーバを選ぶか、ユーザに選択させます。
- 「利用不可 - Finder に切り替える」を選ぶと、ユーザの自動ログインを実行して、「Finder」を表示します。

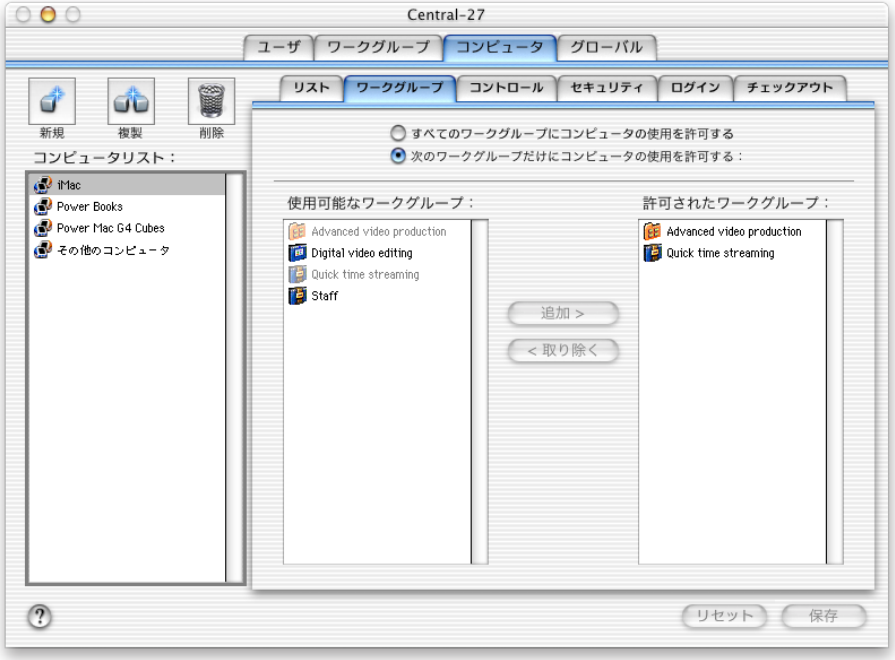
■ 「利用不可 - 別のサーバを選択」を選ぶと、ユーザは、別の「Macintosh Management Server」を選ぶよう促されます。

リストに定義されるコンピュータ

このフィールドには、選択したリスト内のすべてのコンピュータが表示されます。リストにコンピュータを追加するには、「追加」をクリックします。コンピュータを削除するには、削除するコンピュータを選んで、「取り除く」をクリックします。

コンピュータのワークグループ設定

「コンピュータ」パネル内の「ワークグループ」パネルを使用して、リスト内のコンピュータの使用を、特定のワークグループに制限できます。たとえば、学校では、職員室に設置されたコンピュータへのログインを、「Teachers」ワークグループのユーザにのみ許可することができます。



すべてのワークグループにコンピュータの使用を許可する

このオプションを選ぶと、すべてのワークグループのユーザが、選択したコンピュータリスト内のコンピュータの使用を許可されます。

次のワークグループだけにコンピュータの使用を許可する

このオプションを選ぶと、選択したリスト内のコンピュータを使用できるワークグループが指定されます。

使用可能なワークグループ

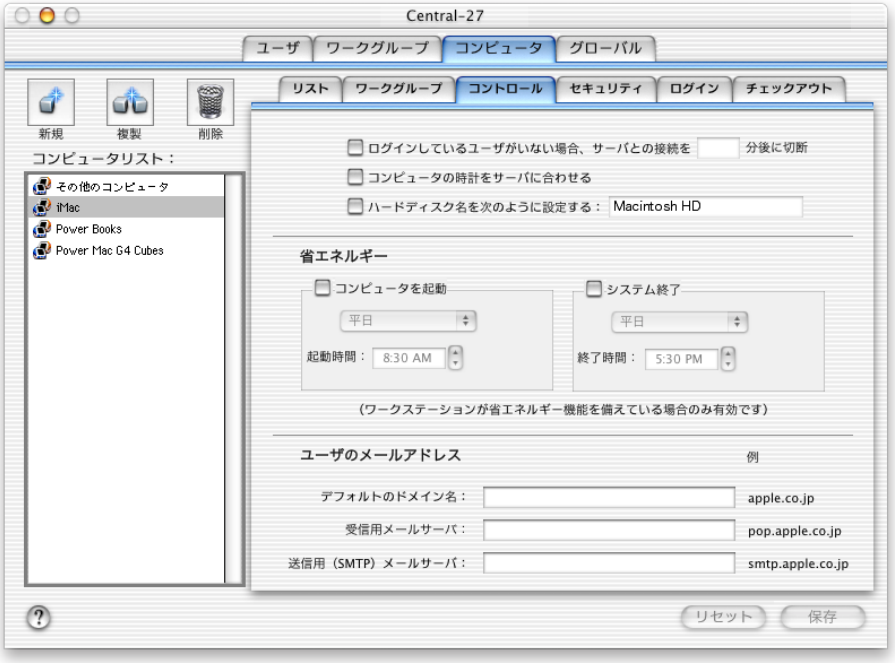
このリストには、「Macintosh マネージャ」のワークグループがすべて表示されます。このリストを設定できるのは、上に表示された「次のワークグループだけにコンピュータの使用を許可する」を選んだ場合だけです。選択したコンピュータリスト内のコンピュータへのアクセスをワークグループに許可するには、ワークグループを選んで「追加」をクリックします。

許可されたワークグループ

このリストには、選択したコンピュータリスト内のコンピュータへのアクセスが許可されたワークグループが表示されます。

コンピュータの制御設定

「コントロール」パネルで設定する内容は、選択中のコンピュータリスト内のすべてのコンピュータに適用されます。



ログインしているユーザがいない場合、サーバとの接続を _ 分後に切断

このオプションを選んだ場合、指定した時間（分）が経過するとコンピュータはサーバへの問い合わせを中止します。コンピュータにログイン画面が表示された状態で、メニューバーのサーバアイコンに緑色の X が表示されます。コンピュータは、ユーザが再びログインするまで、サーバに対して更新やほかのトラフィックを確認することはありません。この設定を使用すると、ネットワークのトラフィックを最小限に抑えることができますが、ユーザが再びログインおよびログアウトするまで自動更新は行われません。

コンピュータの時計をサーバに合わせる

このオプションを選ぶと、ネットワークの Network Time Protocol サーバにアクセスできない場合、コンピュータの時計をサーバの時計に同期させます。

ハードディスク名を次のように設定する

このオプションを選んで名前を入力すると、「Macintosh マネージャ」により、クライアントハードディスクの名前が指定した名前に変更されます。このオプションは、主に「NetBoot」クライアントでの使用を意図しています。「NetBoot」クライアントでは、起動ボリュームのデフォルト名は「NetBoot HD」です。たとえば、名前を「Macintosh HD」に変更することで、これらのクライアントで使用されるすべてのアプリケーションのパス名を、「NetBoot」ではないコンピュータのパス名と同じにできます。「NetBoot」ではないコンピュータ環境では、この設定は必要な場合にのみ設定するだけでかまいません。

省エネルギー

「省エネルギー」では、省電力機能をサポートするクライアントコンピュータでの、システムの自動起動および終了時間を設定できます。この設定を使用できるかどうかは、コンピュータの「コントロールパネル」フォルダに「省エネルギー」コントロールパネル（バージョン 2.0 以降）が存在するかどうかで見分けることができます。コンピュータによっては、選んだ設定によって、システム終了ではなくスリープすることがあります。

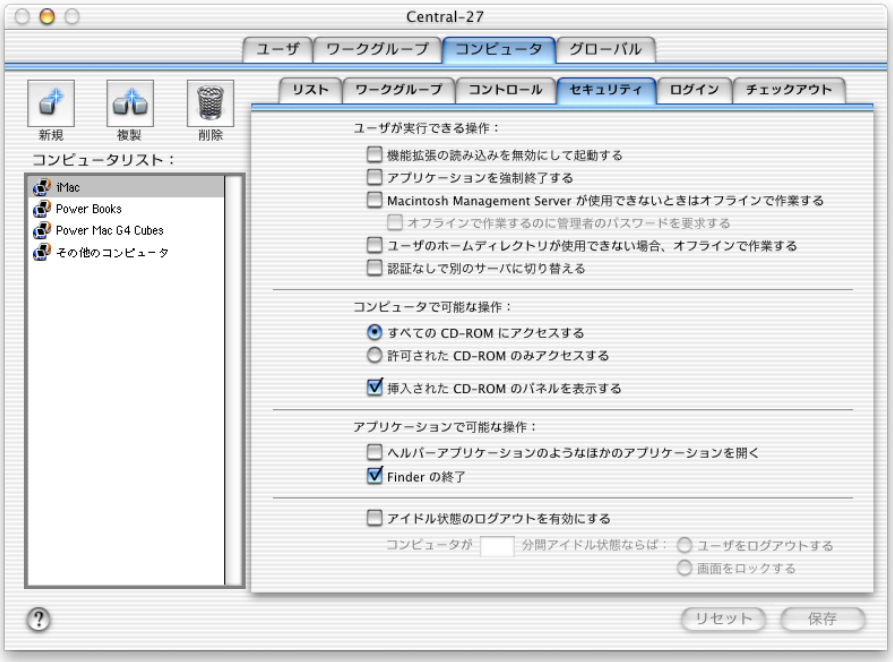
ユーザのメールアドレス

「Macintosh マネージャ」は、「デフォルトのドメイン名」フィールドで指定したユーザのエイリアスおよびドメイン名を使って、メールアドレスを持たないユーザのメールアドレスを作成できます。POP（受信メール）および SMTP（送信メール）サーバのアドレスも入力する必要があります。ユーザが「Macintosh マネージャ」ネットワークに接続する際、インポートされたすべてのメール設定で、「Macintosh マネージャ」のメール設定が上書きされます。

ユーザのログイン時にメッセージをチェックするには、「ワークグループ」タブの「オプション」パネルで、「メンバーのログイン時にメールを確認する」を選びます。

コンピュータのセキュリティ設定

「セキュリティ」パネルで設定する内容は、選択中のコンピュータリスト内のすべてのコンピュータに適用されます。



ユーザが実行できる操作

- 「機能拡張の読み込みを無効にして起動する」を選ぶと、ユーザは起動時に shift キーを押して、機能拡張を無効にできます。shift キーを押すと、ほかの機能拡張は無効になりますが、「Macintosh マネージャ」機能拡張は無効になりません。
- 「アプリケーションを強制終了する」を選ぶと、コマンド + option + esc キーを押してアプリケーションを強制終了できるようになります。これには、セキュリティ上の危険があります。
- 「Macintosh Management Serverが使用できないときはオフラインで作業する」を選ぶと、サーバボリュームを使用できない場合でもユーザがコンピュータを使用できるようになります。
- 「ユーザのホームディレクトリが使用できない場合、オフラインで作業する」を選ぶと、ホームディレクトリの保存先ボリュームを使用できない場合、ユーザがオフラインで作業できるようになります。
- 「認証なしで別のサーバに切り替える」は、クライアントコンピュータに対し、管理パスワードがなくても別の「Macintosh Management Server」へ切り替えます。この設定により、セキュリティが低下する場合があります。以前のバージョンの「Macintosh Management Server」ソフトウェアの稼動するサーバが存在する場合、この設定には注意が必要です。クライアントコンピュータを以前のサーバに切り替えたときに、古いクライアントソフトウェアがインストールされる可能性があります。

コンピュータで可能な操作

- 「すべての CD-ROM にアクセスする」を選ぶと、ユーザは、すべての CD-ROM および DVD-ROM ディスクへのアクセスを許可されます。
- 「許可された CD-ROM のみアクセスする」を選ぶと、承認されたディスクのリストにアクセスが制限されます。この設定を選ぶ場合、「グローバル」パネル内の「CD-ROM」パネルで、承認されたディスクのリストを設定する必要があります。
- 「挿入された CD-ROM のパネルを表示する」を選ぶと、CD-ROM のセット時にパネルが表示されます（「パネル」環境の場合）。

アプリケーションで可能な操作

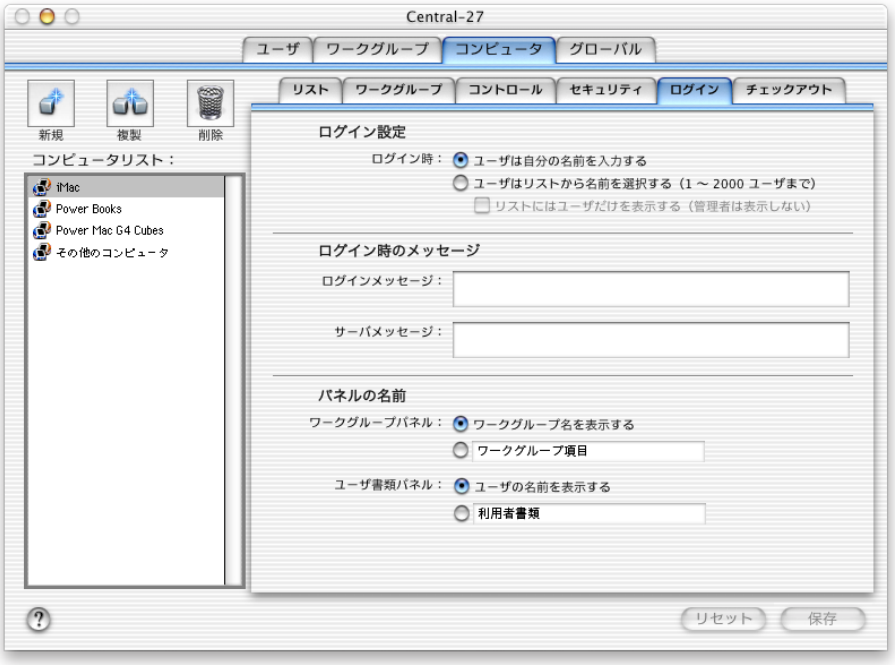
- 「ヘルパーアプリケーションのようなほかのアプリケーションを開く」を選ぶと、必要に応じてアプリケーションからヘルパーアプリケーションを開けるようになります。この設定を有効にしない場合、アプリケーションから、特定機能をユーザに提供するほかのアプリケーションを開くことはできません。たとえば、Web ブラウザから、PictureViewerなどのヘルパーアプリケーションを開くことはできなくなります。この設定を有効にすると、セキュリティが低下する場合があります。
- 「Finder の終了」を選ぶと、インストーラなどのアプリケーションから Mac OS 9 コンピュータの「Finder」の終了が可能になります。このオプションを選ぶと、アプリケーションがセキュリティを無視してしまうことがあります。このオプションを選ばない場合、「Finder」を終了させる必要のあるアプリケーションが正しく動作しない場合があります。

アイドル状態のログアウトを有効にする

このオプションを選んで時間（分）を入力すると、ユーザがワークグループからログアウトされるか、画面がロックされるまでのアイドル状態の時間が設定されます。「ユーザをログアウトする」を選ぶと、ユーザに未保存の書類を保存する機会を与えてから、ログイン画面に戻ります。ユーザは、「保存」ダイアログを終了して操作を継続することはできません。「画面をロックする」を選ぶと、画面の表示が消え、ログアウトするか、パスワードを入力して作業を継続するかを選択するダイアログが表示されます。

コンピュータのログイン設定

「ログイン」パネルで設定する内容は、選択中のコンピュータリスト内のすべてのコンピュータに適用されます。



ログイン設定

ユーザによるコンピュータへのログイン方法について、次の 2 つのオプションのいずれかを選択できます。

- 「ユーザは自分の名前を入力する」を選ぶと、ユーザは、ログインダイアログにユーザ名を自分で入力することを求められます。「ユーザは自分の名前を入力する」は、通常、リストから名前を選ぶ場合よりも高速で、セキュリティも向上します。ただし、ユーザは自分の名前を知っている必要があります。
- 「ユーザはリストから名前を選択する（1 ～ 2000 ユーザまで）」を選ぶと、ユーザはリストをスクロールして自分の名前を選ぶことができます。100 以上のユーザが登録されている場合、リストの表示に時間がかかるため、通常、速度が低下します。2000 以上の「Macintosh マネージャ」アカウントを保持している場合、このオプションは使用できません。

ログイン時のメッセージ

作成可能なログインメッセージには、次の 2 つのタイプがあります（半角で 127 文字、全角で 63 文字以内）。

- 「ログインメッセージ」は、選択したコンピュータリストのログインダイアログに表示されます。
- 「サーバメッセージ」は、選択したリスト内のコンピュータにユーザがログインした後に表示されます。

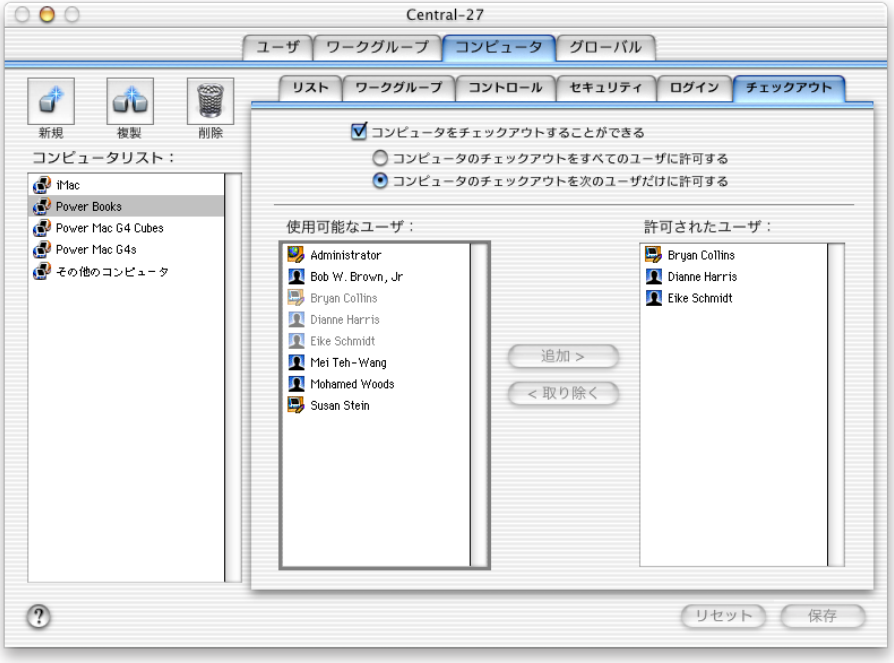
パネルの名前

「パネル」環境で表示されるワークグループおよびユーザ書類パネルの名前を変更できます。

- 「ワークグループ名を表示する」を選ぶと、ワークグループ書類パネルに各ワークグループの名前が表示されます。または、下のボタンをクリックしてフィールドに別の名前を入力します。
- 「ユーザの名前を表示する」を選ぶと、ユーザ書類パネルに各ユーザの名前が表示されます。または、下のボタンをクリックしてフィールドに別の名前を入力します。

コンピュータのチェックアウト設定

「コンピュータ」パネルの「チェックアウト」パネルを使用して、ユーザにコンピュータからのチェックアウトを許可できます。たとえば、ユーザはポータブルコンピュータをチェックアウトして自宅に持ち返り、放課後にも作業を継続することができます。コンピュータがチェックアウトされた後でも、「Macintosh マネージャ」のセキュリティ機能は引き続き有効です。



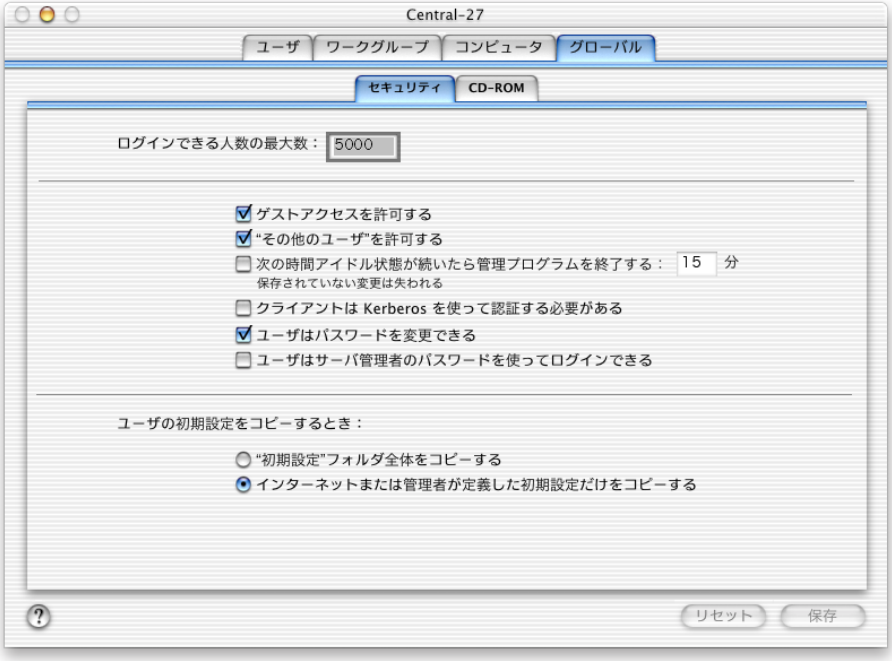
コンピュータをチェックアウトすることができる

このオプションを選ぶと、ユーザはこのコンピュータリスト内のコンピュータをチェックアウトできるようになります。

- 「コンピュータのチェックアウトをすべてのユーザに許可する」を選ぶと、すべてのユーザが、このリスト内の任意のコンピュータをチェックアウトできるようになります。
- 「コンピュータのチェックアウトを次のユーザだけに許可する」を選ぶと、チェックアウトの実行が、選択したユーザだけに制限されます。

グローバルなセキュリティ設定

「グローバル」パネル内の「セキュリティ」パネルのオプションを使って、「Macintosh マネージャ」ネットワークの完成度を保ち、ユーザの書類を不正操作から防ぐことができます。



ログインできる人数の最大数

サーバの状況ログに含めるログ項目の最大数を入力します。ログは、「レポート」メニューを使って表示できます。

ゲストアクセスを許可する

このオプションを選ぶと、ゲストユーザにログインが許可されます（ゲストユーザがワークグループに追加されている場合）。

“ その他のユーザ ” を許可する

このオプションを選ぶと、「Macintosh マネージャ」にユーザが読み込まれていなくても、「ユーザとグループ」に名前とパスワードが存在するユーザにクライアントコンピュータへのアクセスが許可されます。

次の時間アイドル状態が続いたら管理プログラムを終了する

「Macintosh マネージャ」管理プログラムが自動的に終了するまでの、動作のない時間（分）を設定するときに選択します。

クライアントは Kerberos を使って認証する必要がある

Kerberos ネットワーク認証プロトコルを使用して、クライアントログイン情報を検証する場合、このオプションを選びます。

ユーザはパスワードを変更できる

これを選ぶと、すべてのユーザが自分のパスワードを変更できるようになります。このアクセス権を無効にすると、ユーザのログインダイアログに表示されるパスワード変更オプションは利用できなくなります。

ユーザはサーバ管理者のパスワードを使ってログインできる

このオプションを選ぶと、システム管理者は、任意のユーザアカウントで（ユーザの名前と管理者のパスワードを使って）ログインできるようになります。

ユーザの初期設定をコピーするとき

次の 2 つの設定は、「Mac OS 9」より前のクライアントコンピュータにユーザの初期設定をコピーする方法を制御します。「Mac OS 9」より前のクライアントコンピュータにログインしている間、ユーザはデスクトップピクチャなどの初期設定を変更できます。ただし、ログアウト時に初期設定が保存されるのは、初期設定を保存する許可を与えた場合だけです。

- 「“初期設定”フォルダ全体をコピーする」は、「Macintosh マネージャ」に対し、項目の種類やサイズに関係なく、「初期設定」フォルダ内のすべての項目のコピーを強制します。不必要な、またはサイズの大きい項目をコピーすると、ログインおよびログアウトにかかる時間が長くなることに注意してください。
- 「インターネットまたは管理者が定義した初期設定だけをコピーする」を選ぶと、「Macintosh マネージャ」は、次のファイルおよびフォルダをユーザのログイン時に常にコピーします。
  - StuffIt Expander Preferences
  - RealAudio™ Player Preferences
  - Internet Preferences
  - NCSA Telnet Preferences
  - Fetch Prefs
  - NewsWatcher Prefs
  - JPEGView Preferences
  - Netscape
  - Explorer

「Netscape」および「Explorer」の場合、フォルダはコピーされますが、内部のキャッシュフォルダは削除されます。

グローバル CD-ROM 設定

「グローバル」パネル内の「CD-ROM」パネルを使って、すべての CD-ROM および DVD-ROM ディスクへのアクセスを許可することも、リストに含まれるディスクにアクセスを制限することもできます。使用可能なディスクのリストにディスクを追加すると、その内容を表示できます。ディスク上のすべての項目へのアクセスを許可することも、選択したアイテムのみにアクセスを制限することもできます。

オーディオ CD の使用を許可する場合、「ワークグループ」パネル内の「アクセス権」パネルを使用します。

Macintosh マネージャの上手な使いかたとヒント

このセクションでは、「Macintosh マネージャ」を効率的に使用するためのヒントとアドバイスを示します。

読み込まれていないユーザにすばやいアクセスを提供する

ユーザに認証されたアクセスを提供し、カスタマイズ環境を設定する、最も簡単で便利な方法は、「読み込まれたユーザ」リストの「その他のユーザ」アカウントを利用することです。「その他のユーザ」アカウントにログインを許可すると、「Mac OS X Server」の「ユーザとグループ」データベースにアカウントを持つユーザは、「Macintosh マネージャ」にユーザが読み込まれていなくても、クライアントコンピュータにログインできるようになります。これらのユーザは、「Macintosh マネージャ」の「その他のユーザ」アカウントで設定したアクセス権限および環境を保持し、自分用のホームディレクトリ、初期設定、および書類にアクセスできます。(「その他のユーザ」機能は、ゲストアクセスとは異なります。ゲストは、パスワード認証を取得せず、ファイルや初期設定を保存することもできません。)

たとえば、集中ユーザデータベースのある大学では、コンピュータ室の Macintosh マネージメントサービスは、「その他のユーザ」アカウントを使用する場合にのみ設定できます。「Mac OS X Server」アカウントを持つキャンパスのユーザはすべて、コンピュータ室に行き、ホームディレクトリ、初期設定、および書類にアクセスできます。これらのユーザを、最初に個別に「Macintosh マネージャ」にインポートする必要はありません。

参考:「その他のユーザ」アカウントを使って、コンピュータをチェックアウトしたり、オフラインのコンピュータで作業を行うことはできません。「その他のユーザ」アカウントを使ってログインしたユーザには、ディスクの割り当ては適用されません。

「その他のユーザ」の設定

「その他のユーザ」アカウントを設定する場合、次のように操作します。

1. 「その他のユーザ」アカウントが「Macintosh マネージャ」の「読み込まれたユーザ」リストに表示されない場合、「グローバル」パネルの「セキュリティ」タブをクリックしてから「“その他のユーザ”を許可する」をクリックします。
2. 「ユーザ」タブをクリックして、「読み込まれたユーザ」リストの「その他のユーザ」を選びます。
3. 「ユーザ」パネル内の「基本設定」および「詳細設定」パネルで、必要な変更を行います。
4. 「ワークグループ」タブをクリックして、「その他のユーザ」アカウントをワークグループに追加します。
5. 「その他のユーザ」アカウントに合わせて、ワークグループの設定を変更します。
6. コンピュータが、「コンピュータ」パネルのワークグループから利用可能になっていることを確認します。

ログイン時の「その他のユーザ」の表示方法

ログイン時に名前とパスワードを入力するようクライアントコンピュータを設定している場合、ユーザは「Macintosh マネージャ」のログインダイアログで、「Mac OS X Server」のユーザ名とパスワードを入力するだけです。ログイン時にユーザがリストから名前を選ぶ場合は、リストの一番上、「ゲスト」のすぐ下に、「その他のユーザ」が表示されます。ユーザが「その他のユーザ」アカウントを選ぶと、ログインダイアログが表示されて、「Mac OS X Server」名およびパスワードを入力できます。

大規模なネットワークまたは拡張するネットワーク上で Macintosh マネージャを設定する

多数のユーザが利用する大規模なネットワークの場合、複数のサーバボリュームが必要になる場合があります。また、ネットワークに別のサーバまたはパーティションが必要になる場合もあります。そのような場合、簡単に移行できるように、設定を行うことが期待されます。解決策としては、共有グループファイル、ホームディレクトリ、クリップアートフォルダ、部門またはクラスの Web サイト、共有する CD、および特別なネットワークアプリケーションなどを保管するサーバを追加設定します。このように設定すると、「Macintosh マネージャ」にログインしたユーザは、ほかのボリューム上にあるものを含めて、ほかの共有ポイントにあるコンテンツにアクセスすることができます。共有グループファイルの保管場所は、「ワークグループ」パネルの「オプション」パネルで選びます。

複数の共有ポイントを設定する利点は、関連するファイルを管理可能なグループにまとめておくことができることです。そして、ハードディスクのパーティションや別のサーバを追加する必要がある場合に、この新しいボリュームに共有ポイントを簡単に移動できます。

ネットワークの要望を満たすワークグループを作成する

「Macintosh マネージャ」で行う設定の多くは、個別のユーザが対象ではなく、ユーザのワークグループが対象です。ユーザの設定を指定するときは、目的のユーザをワークグループに追加する必要があります。

ワークグループを設定するときは、共通プロジェクトと、そのプロジェクトの必要性について考慮します。たとえば、次の点を検討してください。

- 一部のユーザ（ゲストユーザなど）に、制限付きのデスクトップ環境を許可しますか？制限付きのデスクトップ環境には、特定のメニュー項目や、ローカルフォルダおよびローカルアプリケーションなどへのアクセスの制限が含まれます。

  該当する場合、これらのユーザ用のワークグループを作成して、デスクトップ環境を割り当てます。詳しくは、230 ページの「ワークグループのデスクトップ環境を選ぶ」を参照してください。

- 一部のユーザに、特定のアプリケーションとファイルに簡単にアクセスすることを許可しますか？

  該当する場合、アクセス権を許可するユーザのワークグループを作成します。

- 書類に対して共同作業を行うために、共有フォルダへのアクセスを必要とするユーザがいますか？

  該当する場合、これらのユーザだけで構成されるワークグループが存在することを確認し、共有ワークグループフォルダを設定します。

- 一部のユーザに、管理者だけ（教師やスーパーバイザなど）が開くことができるフォルダにチェックインすることを許可しますか？

  該当する場合、このようなユーザだけで構成されるワークグループを作成し、そのワークグループに対して提出フォルダを設定します。
- 一部のユーザに特定のプリンタへの特別アクセスを許可しますか？

  該当する場合、このようなユーザだけで構成されるワークグループがあることを確認し、そのプリンタへのアクセス権を許可します。
- 特定のユーザグループに対し、指定したコンピュータの使用を制限しますか？

  該当する場合、このようなユーザだけで構成されるワークグループを作成し、「コンピュータ」パネルを使って、目的のコンピュータを含む「リスト」を作成し、目的のワークグループをそのリストに割り当てます。

1 人のユーザを複数のワークグループに割り当てることができることに注意してください。

ワークグループのデスクトップ環境を選ぶ

ワークグループのデスクトップ環境によって、ワークグループ内のユーザに表示されるインタフェースと、ワークグループのメンバーがネットワークリソースに対して許可されるアクセス権のタイプが決まります。

「ワークグループ」パネルの「メンバー」パネルで、以下のいずれかの環境タイプを選びます。

環境	説明	使用する状況
Finder	■ 標準の「Mac OS」デスクトップと同様の外観で、同じように動作します。 ■ ユーザは、ローカルハードディスク上のすべてのアプリケーションについて、制限を受けずにアクセスできます。 ■ ユーザのホームディレクトリはログイン時にマウントされ、特定のコントロールパネルの使用が制限されます。	ユーザに最大限の柔軟性を許可したい場合、かつ、管理者による制御が必ずしも優先されない場合。

環境	説明	使用する状況
制限付き Finder	■ 標準の「Mac OS」デスクトップと外観は同様ですが、ユーザが実行できる操作が制限されます。 ■ ユーザはローカルハードディスクを参照することはできますが、自分のコンピュータ上で開くことができるものが、管理者によって決められています。	ユーザに標準の「Mac OS」デスクトップへのアクセスを許可する一方で、クライアントコンピュータで開くことができるものを制限する場合。
パネル	■ 大きなアイコンの単純なインタフェースで、初心者のユーザがコンピュータを簡単に使用できることを目的とします。ワークグループに割り当てられている項目のみが表示され、ユーザがアクセスできます。 ■ サーバボリュームやリムーバブルメディアへのアクセスを許可すると、各ボリュームやメディアが、マウント時にパネルとして表示されます。 ■ パネル名を指定できます（「コンピュータ」パネルの「ログイン」パネルにおいて）。	ユーザに最も単純な環境を提供したい場合。または、ユーザがコンピュータで実行できる操作について、管理者に最大限に制御させたい場合。あるいは、その両方が該当する場合。

セキュリティを最大限に強化する

「Macintosh マネージャ」を使ってセキュリティを最大限に強化するには、多くの方法があります。その方法について詳しくは、「Macintosh マネージャ」のヘルプを参照してください。

- 登録されていないユーザによるアクセスを禁止する
- 起動環境、システム設定、およびその他の管理オプションへの変更を禁止する
- アプリケーションがセキュリティを省略することを禁止する
- アプリケーションが別のアプリケーションを開くことを禁止する
- CD へのアクセスを制限する
- リムーバブルメディア上でのアプリケーションの使用を制限する

オンスクリーンヘルプにアクセスするには、「ヘルプ」メニューから「Macintosh マネージャヘルプ」を選ぶか、「Macintosh マネージャ」ウインドウの任意のパネルの左下に表示される「?」マークをクリックします。

Macintosh マネージャの内側

このセクションでは、「Macintosh マネージャ」がどのように動作するか、「内側」の情報について説明します。問題が発生してトラブルを解決するときに、この情報は特に役に立ちます。

Macintosh マネージャが起動する仕組み

クライアントコンピュータが起動し、ユーザがログインすると、次の動作が起こります。

- ログイン用のダイアログが表示されます。「Macintosh マネージャ」の設定方法に応じて、ユーザは名前を入力するか、リストから名前を選びます。
- 「Macintosh マネージャ」は、「Mac OS X Server」ディレクトリを使ってユーザ名とパスワードを検証します。次に、「Macintosh マネージャ」は、自分のデータベースを調べて、ユーザにアカウントがあるかどうかを確認します。
- ユーザが複数のワークグループに所属している場合は、所属しているワークグループのリストから目的のワークグループを選びます。
- 「Macintosh マネージャ」が、ユーザ、ワークグループ、およびコンピュータのデータベースを検索し、開きます。
- ワークグループの環境とその他の設定が有効になります。
- ユーザに対して、サーバとワークグループのログインメッセージ（ある場合）が表示されます。
- ユーザのデスクトップに書類フォルダのエイリアスが表示されます（ユーザが「パネル」環境にある場合を除く）。

Macintosh マネージャが初期設定に従って動作する仕組み

このセクションでは、ユーザ固有の初期設定（Web ブラウザの「お気に入り」やデスクトップの背景など）が「Macintosh マネージャ」の環境にどのように保管されるかについて説明し、管理者が「Managed Preferences」フォルダを使って初期設定を制御する方法について説明します。「Mac OS 9」のコンピュータと「Mac OS 9」より前のコンピュータとでは、初期設定の処理方法に違いがあります。これらの違いについては、随時説明します。

初期設定の保管場所

デフォルトでは、初期設定の保存およびアクセスは、次の方法で行われます。

- クライアントがログインしていない場合：「Mac OS 9」のクライアントコンピュータも「Mac OS 9」より前のクライアントコンピュータも、個別の初期設定の大半はサーバに保管されます。
- クライアントユーザが「Macintosh マネージャ」にログインする場合：「Macintosh マネージャ」によりユーザ固有の初期設定が検索され、ユーザのログイン期間中有効になります。ログイン中の初期設定の保管場所は、クライアントコンピュータが「Mac OS 9」か、それ以前の「Mac OS」かによって異なります。
  - Mac OS 9 より前のクライアント： 初期設定は、クライアントコンピュータのハードディスクに存在する「システムフォルダ」内の「初期設定」フォルダに保管されます。
  - Mac OS 9 クライアント： 初期設定は、ユーザのホームディレクトリの「/Library/Preferences」フォルダに保存されます。

Mac OS 9 ユーザの初期設定が、クライアントのハードディスク上に存在する「ユーザ」フォルダ内の「初期設定」フォルダに保存される場合もありますが、「システムフォルダ」内の「初期設定」フォルダに保存されることはありません。

「Managed Preferences」を使用する

「Managed Preferences」を使用すると、特定の要件や目的に合わせて初期設定の処理方法を変更できます。たとえば、ユーザがあらかじめ定義された初期設定のセットを常に最初に使用するか、またはユーザが設定した初期設定の中には決して上書きされないものがあるかどうかを設定できます。

「Managed Preferences」は、「Initial Preferences」、「Forced Preferences」、および「Preserved Preferences」の 3 つにグループ化できます。これらのカテゴリを使用できるかどうかは、クライアントコンピュータ上の「Mac OS」のバージョンに依存します。

	Mac OS 9 クライアント	Mac OS 9 より前のクライアント：
Initial Preferences	可能	可能
Forced Preferences	可能	可能
Preserved Preferences	不可	可能

「Initial Preferences」フォルダ、「Forced Preferences」フォルダ、および「Preserved Preferences」フォルダを含む「Managed Preferences」フォルダが、ワークグループのメンバーが最初にログインするときに作成されます。

「Managed Preferences」を使用するには、次のように操作します。

1. 「ワークグループ」パネル内の「ボリューム」パネルで、ワークグループデータボリュームを設定します。
2. クライアントコンピュータから、ワークグループのデータボリュームにログインします。

   空の「Initial Preferences」フォルダ、「Forced Preferences」フォルダ、および「Preserved Preferences」フォルダを含む「Managed Preferences」フォルダが、ワークグループのデータボリューム上に自動的に作成されます。
3. 「Initial Preferences」フォルダまたは「Forced Preferences」フォルダに保存する初期設定を作成します。
4. 作成した初期設定を、ワークグループのデータボリューム上にある「Initial Preferences」フォルダまたは「Forced Preferences」にコピーします。
5. 「Mac OS 9」より以前のクライアントコンピュータを対象に「Preserved Preferences」を作成する場合は、目的の初期設定と同じ名前のファイルまたはフォルダ、あるいはその両方を、「Preserved Preferences」フォルダに設定します。

   実際の初期設定がファイル形式の場合、「Preserved Preferences」フォルダに設定する同じ名前の項目は、ファイルでなければなりません。同様に、実際の初期設定がフォルダの場合は、同じ名前の項目はフォルダでなければなりません。
6. ワークグループのデータボリュームごとに、手順 1 ～ 5 を繰り返します。

   各「Managed Preferences」の使用方法について詳しくは、次のセクションを参照してください。

Initial Preferences

「Initial Preferences」フォルダは、ログインのたびに各ユーザに特定の初期設定ファイルを提供します。ユーザが「Initial Preferences」フォルダにすでに初期設定を保持している場合、「Macintosh マネージャ」はユーザの初期設定を置き換えることはしません。ユーザがログインするたびにこの処理が繰り返されるため、ソフトウェアを追加すると、「Initial Preferences」フォルダに追加の初期設定ファイルを保管できます。新規インストールしたソフトウェアをユーザが最初に使用する際、新規ソフトウェアの初期設定ファイルのコピーが、ユーザの「初期設定」フォルダに保管されます。

ユーザが最初にログインすると、「Initial Preferences」フォルダを使用しているかどうかに関係なく、いくつかの初期設定が作成されます。次の項目を「Initial Preferences」フォルダに保管すると、これらの項目はユーザのフォルダにはコピーされません。

- Apple Menu Options Prefs
- AppSwitcher 初期設定
- Internet Preferences
- キーボード初期設定
- キーチェーン
- 作業環境マネージャ初期設定
- Mac OS 初期設定
- TSM Preferences
- ユーザの初期設定

例：「Initial Preferences」フォルダを使用する場合

たとえば、すべてのユーザの最初のログイン時に、あらかじめ設定された「Internet Explorer」のブックマークおよび初期設定を提供する場合を考えましょう。この場合、次の手順を実行します。

1. 管理用コンピュータで、ブックマークおよび初期設定を設定します。
2. 管理用コンピュータの「システムフォルダ」内の「初期設定」フォルダを開き、「Explorer」フォルダを見つけます。「Explorer」フォルダ全体を、「Macintosh マネージャ」サーバの「Initial Preferences」フォルダにコピーします。

クライアントのログイン時の処理は、次のようになります。

- Mac OS 9 クライアントのログイン時：「Macintosh マネージャ」は、ユーザのホームディレクトリの「/Library/Preferences」フォルダで、「Explorer」という名前のフォルダを検索します。「Macintosh マネージャ」がユーザのフォルダ内に「Explorer」フォルダを見つけられない場合、「Initial Preferences」フォルダから「Explorer」フォルダ（およびその内容）をユーザのフォルダに新たにコピーします。

ユーザのフォルダ内に「Explorer」フォルダがすでに存在する場合、「Macintosh マネージャ」によって既存のフォルダが更新されます。つまり、同じ名前の古いファイルが新しいファイルに置き換えられ、クライアントが前回ログインした後で「Forced Preferences」フォルダに置いたファイルが追加されます。ユーザの「初期設定」フォルダおよび「Forced Preferences」フォルダ内に、一意名が一致しないファイルまたはフォルダが存在する場合、「Macintosh マネージャ」による更新は行われません。一意名が一致しないファイルが増えてディスク領域が不足するのを防ぐには、必要に応じてユーザの「初期設定」フォルダを確認してください。

- 「Mac OS 9」より前のクライアントのログイン時：「Macintosh マネージャ」は、「Explorer」という名前のフォルダを 2 つの場所で検索します。1 つの場所は、ユーザのホームディレクトリ内の「初期設定」フォルダで、もう 1 つは、クライアントコンピュータの「システムフォルダ」内の「初期設定」フォルダです。ユーザの「初期設定」フォルダ内に目的のフォルダが見つからない場合、「Macintosh マネージャ」は、「Explorer」フォルダのコピーをユーザの「初期設定」フォルダ、およびクライアントコンピュータの「初期設定」フォルダにコピーします。クライアントコンピュータの「初期設定」フォルダに「Explorer」フォルダがすでに存在する場合には、新たにコピーされるフォルダで上書きされます。ユーザの「初期設定」フォルダに目的のフォルダが存在する場合、コピーは行われません。

参考：「Mac OS 9」より前のコンピュータの場合、「Macintosh マネージャ」は、2 つの場所のいずれかで「Explorer」フォルダを見つけることができない場合、「Explorer」フォルダをその場所にだけコピーします。このため、ユーザが使用するコンピュータを別のクライアントコンピュータに変えると、ユーザの環境が一貫性のないものになります。

Forced Preferences

「Forced Preferences」フォルダを使用すると、ユーザがログインするたびに、指定した初期設定セットを使って初期環境が設定されます。ユーザが自分の初期設定を変更すると、ユーザの次回のログイン時に、これらの初期設定が「Forced Preferences」フォルダの初期設定と置き換わります。

例：「Forced Preferences」フォルダを使用する場合

たとえば、ログインするたびに、すべてのユーザに、あらかじめ設定された Internet Explorer のブックマークおよび初期設定を提供する場合を考えましょう。この場合、次の手順を実行します。

1. 管理用コンピュータで、ブックマークおよび初期設定を設定します。
2. 管理用コンピュータの「システムフォルダ」内の「初期設定」フォルダを開き、「Explorer」フォルダを見つけます。「Explorer」フォルダ全体を、「Macintosh マネージャ」サーバの「Forced Preferences」フォルダにコピーします。

クライアントのログイン時の処理は、次のようになります。

- Mac OS 9 クライアントのログイン時：「Macintosh マネージャ」は、ユーザのホームディレクトリの「/Library/Preferences」フォルダで、「Explorer」という名前のフォルダを検索します。「Macintosh マネージャ」がユーザのフォルダ内に「Explorer」フォルダを見つけられない場合、「Forced Preferences」フォルダから「Explorer」フォルダ（およびその内容）をユーザのフォルダに新たにコピーします。ユーザのフォルダ内に「Explorer」フォルダがすでに存在する場合、「Macintosh マネージャ」は既存のフォルダを削除して、「Forced Preferences」フォルダの「Explorer」フォルダと置き換えます。

- 「Mac OS 9」より前のクライアントのログイン時：「Macintosh マネージャ」は、ほかのコピーが存在するかどうかに関係なく、「Explorer」フォルダを、「Forced Preferences」フォルダからクライアントコンピュータの「システムフォルダ」内の「初期設定」にコピーします。ユーザのホームディレクトリ内の「初期設定」フォルダにコピーされるファイルやフォルダはありません。

Preserved Preferences

「Preserved Preferences」フォルダは、「Mac OS 9」より前のクライアントコンピュータでのみ機能します。「Preserved Preferences」フォルダに保管したファイルおよびフォルダは、決してコピーされません。「Macintosh マネージャ」は、「Preserved Preferences」フォルダ内のファイルおよびフォルダをスキャンして、中に含まれるすべての項目のリストを作成します。「Macintosh マネージャ」はこのリストを使って、ログインおよびログアウト時に、サーバとクライアントコンピュータ間でコピーする必要のある初期設定を判断します。「Preserved Preferences」フォルダを使ってコピーする初期設定を制限することにより、ログインおよびログアウトにかかる時間を短縮できます。

「Preserved Preferences」フォルダ内に存在するかどうかに関係なく常にコピーされる初期設定もあれば、「Preserved Preferences」フォルダ内に存在しても決してコピーされない初期設定もあります。

常にコピーされる初期設定	コピーされない初期設定
コントロールバー初期設定	AppleTalk 初期設定
日付 & 時刻初期設定	Client Prefs
Finder 設定	ColorSync プロファイル
Mac OS 初期設定	デスクトップピクチャ初期設定
パネル設定	省エネルギー初期設定
	機能拡張マネージャ設定
	Multi-User 項目
	Multi-User 設定
	Open Transport 初期設定
	リモートアクセス
	TCP/IP 初期設定
	Users & Groups Data File
	Users & Groups Data File Backup

- ユーザが「Mac OS 9」より前のクライアントコンピュータにログインする場合：「Macintosh マネージャ」は「Preserved Preferences」フォルダをスキャンして、ファイル名およびフォルダ名を含むリストを作成します。「Macintosh マネージャ」は、「常にコピーする」リストの項目名を追加して、組み合わされたリストを作成します。「Macintosh マネージャ」は、組み合わせたリストに含まれるすべてのファイルおよびフォルダを、サーバに存在するユーザ固有の「初期設定」フォルダからクライアントコンピュータの「初期設定」フォルダにコピーします。クライアントの「初期設定」フォルダに存在する、組み合わされたリスト内の名前と同じ名前を持つすべてのファイルおよびフォルダは、削除されます。リスト内の項目が、サーバに存在するユーザの「初期設定」フォルダにも、クライアントコンピュータ上の「初期設定」フォルダにも存在しない場合、その項目はスキップされます。
- ユーザのログアウト時：「Macintosh マネージャ」は、同じ手順を使って、クライアントコンピュータの「初期設定」フォルダから、サーバに存在するユーザの「初期設定」フォルダにコピーする初期設定を決定します。組み合わされたリスト内の項目と一致するすべての項目が、クライアントコンピュータの「初期設定」フォルダから削除されます。

  参考：「システムアクセス」ワークグループを使ってログインするユーザは、あるアプリケーションを使用できない場合があります。これは、最後のユーザのログアウト後に、アプリケーションの初期設定が「初期設定」フォルダから削除されてしまうためです。

Macintosh マネージャでセキュリティを保護する仕組み

「Macintosh マネージャ」は、クライアントコンピュータのユーザが、shift キーを押したままコンピュータを起動しても、システム機能拡張の使用を停止できないように設計されています。ユーザは、「機能拡張マネージャ」コントロールパネルで「Macintosh マネージャ」を停止できません。また、「Macintosh マネージャ」の機能拡張を、「システムフォルダ」内の「機能拡張」フォルダから移動することもできません。

「Macintosh マネージャ」には、このほかにも、セキュリティを保護する多くの方法があります。次の方法は、すべてのデスクトップ環境で動作します。その多くはデフォルトで有効になっていますが、いくつかの方法は「Macintosh マネージャ」の管理者が無効にできます。

- どの環境においても、ユーザは、特定のシステム設定の変更が制限されています。これには、ネットワークの設定（「AppleTalk」コントロールパネルと「TCP/IP」コントロールパネル）、「省エネルギー」の設定、および「マルチユーザ」の設定が含まれます。
- ユーザは、ワークグループに含まれるかどうかにかかわらず、ほかのユーザのホームディレクトリへのアクセスを拒否されます。
- ユーザは、「Macintosh マネージャ」のファイルの名前を変更したり、ファイルタイプやファイルクリエータを変更したりすることはできません。
- ユーザがコンピュータをシステム終了したり再起動したりするときに、ユーザの変更は保存されます。
- ユーザは、「Macintosh　マネージャ」のセキュリティを回避するために、アプリケーションを強制的に終了することはできません。（「コンピュータ」パネルの「セキュリティ」パネルで、このオプションを有効にする必要があります。）
- ユーザは、管理者のパスワードを指定せずに、リムーバブルメディアを取り出したり、サーバボリュームのマウントを解除したりできません。（「ワークグループ」パネルの「オプション」パネル、または「コンピュータ」パネルの「セキュリティ」パネルで、これらのオプションを有効にする必要があります。）

サーバからクライアントコンピュータをアップデートする仕組み

「Macintosh マネージャ」の設定情報が含まれる「Multi-User 項目」フォルダのコピーが、各クライアントコンピュータの「システムフォルダ」に自動的に保管されます（「Multi-User 項目」フォルダについて詳しくは、239 ページの「Macintosh マネージャの共有ポイントについて」を参照してください）。このフォルダによってユーザはオフラインで操作することが可能となり、「Macintosh マネージャ」はクライアントコンピュータ上でよりすばやく情報を検索できるので、パフォーマンスが最適化されます。「Multi-User 項目」フォルダには、「Macintosh Management Server」の場所に関する情報が含まれているため、通常、ユーザはログインするときにサーバを選ぶ必要がありません。「初期設定」フォルダにある「Multi-User 項目」フォルダの中に、「Multi-User 項目キャッシュ」フォルダも作成されます。このキャッシュフォルダには、ログインを高速化する項目が含まれています。

クライアントの「Multi-User 項目」フォルダが削除されると、クライアントは、サーバから新しいコピーを新規にダウンロードします。「Macintosh マネージャ」で変更を加えると、クライアントの「Multi-User 項目」フォルダもアップデートされます。クライアントコンピュータがサーバに接続しているが、ユーザはログインしていない場合、「Macintosh マネージャ」は、アップデートが必要な項目がないかどうかを定期的に調べます。ユーザがコンピュータにログインしている場合は、「Macintosh マネージャ」が変更された情報がないかどうかを調べることはありません。ユーザがログアウトするまで、アップデートは行われません。コンピュータが一定時間アイドル状態にあったためにサーバから自動的に切断される場合、ユーザがワークステーションに対しログインおよびログアウトを実行するまで、アップデートのチェックは行われません。

Macintosh マネージャがユーザ、ワークグループ、およびコンピュータのリストを追跡する仕組み

ユーザ、ワークグループ、およびコンピュータに関する情報は、「ユーザ」フォルダ、「グループ」フォルダ、および「コンピュータ」フォルダにあるデータベースファイルに保管されます。（これらのフォルダは、次のセクションで説明する「Macintosh マネージャ」の共有ポイント内の「Multi-User 項目」フォルダにあります。）各フォルダには、2 つのデータベースファイルがあります。一方のファイルにはデータベース内の各レコードの索引（ワークグループの名前など）が含まれ、他方のファイルには各レコードの固有の情報（ワークグループのメンバー、アクセス権、環境など）が含まれています。

ユーザデータベース、グループデータベース、およびコンピュータデータベースは、大きなリレーショナルデータベースの一部ではありませんが、各データベースはほかのデータベースに保存されている情報を相互に参照します。たとえば、ユーザデータベースには、ユーザが所属するワークグループのリストが含まれます。データベース間の一貫性を維持するために、「Macintosh マネージャ」は、データベースの参照を次々に調べ、必要に応じてデータベースをアップデートします。データベースが正しく動作するために、データベースに対して各自で操作を実行する必要はありません。データベースを直接変更することを試みると、不一致が発生し、データベースに保存されている情報が失われることがあります。このような事態が発生した場合は、「Macintosh マネージャ」管理プログラムを使って、またはバックアップコピーから情報を復元することによって、ユーザ、ワークグループ、およびコンピュータの情報を再作成する必要があります。

Macintosh マネージャの共有ポイントについて

「Macintosh Management Server」ソフトウェアをインストールすると、「Macintosh Manager」という名前の共有ポイントがサーバ上に作成されます。「Macintosh マネージャ」が共有ポイントにアクセスできるよう、適切なアクセス権が設定されます。「Macintosh マネージャ」の共有ポイントは、主にデータベースによって利用されます。ユーザは共有ポイントの内容を表示することはできませんし、直接やり取りすることもありません。

「Macintosh マネージャ」の共有ポイントは、共有ポイントの名前が同じで、フォルダが共有ポイントに存在し、アクセス権が同じである限り、別のボリュームに移動できます。

「Multi-User 項目」フォルダ

これらのフォルダは、「Macintosh マネージャ」の共有ポイント内の「Multi-User 項目」フォルダにあります。ここには、「Macintosh Management Server」の場所、ワークグループ項目へのエイリアス、キャッシュ情報、ユーザリスト／グループリスト／コンピュータリストのデータベースなど、「Macintosh マネージャ」を使って設定するオプションに関する情報が含まれています。「Multi-User 項目」フォルダには、次のものが含まれています。

- 「利用状況」: このファイルは、ログ項目で構成されています。プリンタの使用やその他の状況のレポートなど、各種のレポートを生成するときに使用されます。
- 「CD-ROM 設定」: このファイルは、ユーザが使用を許可されている CD のリストと、各 CD 固有の項目の設定で構成されています。
- 「コンピュータ」: このフォルダには、設定した各コンピュータリストの「Macintosh マネージャ」設定を保管しているデータベースが含まれています。
- 「グループ」: このフォルダには、各ワークグループに対応するフォルダと、各ワークグループの「Macintosh マネージャ」設定を保管しているデータベースファイルが含まれています。圧縮された形式のワークグループの項目は、サーバ上に保管されます。（項目へのエイリアスは、クライアントコンピュータ上に保管されます。）
- 「Multi-User 項目」ファイル: このファイルは、「Multi-User 項目」フォルダに現在含まれているファイルのアーカイブで構成されています。ファイルを開いたり、変更したりしないでください。削除されると、次に「Macintosh マネージャ」を使用するときに再作成されます。
- 「プリンタ」: このフォルダには、「Macintosh マネージャ」で設定したデスクトップ・プリンタを表すファイルが含まれています。ワークグループが使用するデスクトップ・プリンタごとにファイルが作成されます。デスクトップ・プリンタを使用するワークグループにユーザがログインすると、プリンタファイルがクライアントコンピュータのデスクトップにコピーされます。

  プリンタ情報を変更するときは、「Macintosh マネージャ」を使用してください。「プリンタ」フォルダ内の項目を開いたり、取り除いたりしないでください。このフォルダからプリンタファイルを削除すると、そのプリンタを使おうとするワークグループのメンバーに対して、プリンタが見つからないというメッセージが表示されます。
- 「ユーザ」: このフォルダには、各ユーザアカウントの「Macintosh マネージャ」設定を保管しているデータベースファイルと、少なくとも 1 回サーバにログインしたことがある各ユーザのフォルダが含まれています。

Macintosh マネージャと NetBoot サービスを一緒に使用する

「NetBoot」と「Macintosh マネージャ」を一緒に使用する必要はありませんが、共に使用することによって、研究室と教室における各コンピュータのシステム設定の管理が一層簡単になります。

「Macintosh マネージャ」で「NetBoot」を使用するには、「NetBoot Desktop Admin」ユーティリティを使って、「マルチユーザ」コントロールパネルのオプションを変更して、「NetBoot」クライアントコンピュータが、起動時に「Macintosh マネージャ」からアカウント情報を取得できるようにします（255 ページの「NetBoot Desktop Admin を使用する」を参照してください）。

例：小学校に新しいコンピュータ室が開設された場合

学校には、次に示す技術目標があります。

- 読み書きや計算など、さまざまな科目における教育目標の達成を支援する。
- すべてのコンピュータに同じソフトウェアが用意された状態にする。
- 生徒がどのような使いかたをしても、コンピュータとネットワークリソースを保護し、デスクトップのセキュリティを向上する。
- 管理しやすいネットワークを構築する。
- 書類を集中して保管する。

これらの技術目標は、次のネットワーク運用法によってサポートされます。

- 「NetBoot」クライアントコンピュータの起動元の Mac OS イメージを含み、「Macintosh Management Server」ソフトウェアのインストールされたサーバを使用します。サーバには、ユーザの書類とアプリケーションも保管されます。
- 「Macintosh マネージャ」を使って、デスクトップのセキュリティを向上するオプションを設定します。
- 教師に対してワークグループの管理者アカウントを設定し、「Macintosh マネージャ」を使ってユーザアカウントとワークグループを管理する方法を指導します。
- クライアントコンピュータを、サーバ上の「Mac OS」イメージから起動するように設定します。

クライアントコンピュータでは、「NetBoot」サーバによって提供されるシステムソフトウェアを使用するため、各コンピュータが使用するソフトウェアのバージョンおよびアクセスするアプリケーションを、同一にできます。セッションの際にユーザがどのような変更を加えても、ユーザがログアウトすると、コンピュータは同じシステム設定に戻ります。

「Macintosh マネージャ」を使って、生徒がアクセスできるネットワークリソースを制御することによって、デスクトップのセキュリティを保護することができます。保護できるのは「システムフォルダ」と「アプリケーション」フォルダで、アプリケーションを使用するときのセキュリティを向上するためのオプションを設定できます。

ユーザアプリケーションは、サーバ上に保管されるディスクイメージにのみインストールされるので、ネットワークの管理は簡単です。いったんネットワークを設定すると、日常的な管理業務はほとんど必要ありません。教師は、サーバに接続しているどのコンピュータからでも、ユーザアカウントとワークグループを管理できます。教師は、ネットワークを介して課題を出したり、集めたりすることができます。教師は、授業に役立つネットワークリソース、アプリケーション、および CD を利用できるようにすることもできます。

Macintosh マネージャに関する問題を解決する

このセクションでは、「Macintosh マネージャ」を使用する際に直面する問題について扱います。複雑な問題を解決する場合は、232 ページの「Macintosh マネージャの内側」も参考になるので参照してください。

Macintosh マネージャにログインするときの問題

管理者のパスワードを忘れた場合：

「Mac OS X Server」のシステム管理者に連絡してください。または、「Server Admin」アプリケーションを使って管理者のパスワードを変更します。

ユーザがWebページからファイル（メディアファイルなど）を開くことができない場合：

ユーザのワークグループ設定で、アプリケーションが別のアプリケーションを開くことを許可されているかどうかを確認します。（「コンピュータ」パネルの「セキュリティ」パネルを参照してください。）ユーザが Web ページからアプリケーションを開けるようにする場合は、「アプリケーションで可能な操作」欄の「ヘルパーアプリケーションのようなほかのアプリケーションを開く」を選びます。

クライアントコンピュータがサーバを見つけることができない、または接続できない場合：

- サーバが稼動中であることを確認してください。サーバが起動した直後の場合は、サーバが表示されるのに多少時間がかかることがあります。
- ネットワークに AppleTalk ゾーンが指定されている場合、「Mac OS 9」より以前のコンピュータのユーザは、目的のサーバが含まれているゾーンを選ぶ必要があるかもしれません。Mac OS 9 コンピュータの場合は、「ネットワークブラウザ」を使って、サーバに接続していることを確認します。最適なパフォーマンスを得るため、クライアントコンピュータからサーバへの接続を、AppleTalk ではなく TCP/IP で設定することをお勧めします。
- クライアントコンピュータがメモリ不足でなく、ネットワークに接続したままであることを確認します。
- 多くのコンピュータが同時に起動する場合は、ネットワークの負荷が重い可能性があります。一度に起動するコンピュータの台数を減らしてみてください。

別の環境から「Finder」にアクセスできない：

- 「ようこそ」ダイアログボックスが表示されたときに、コマンド＋shift ＋ esc キーを押します。次にコンピュータ所有者のパスワード、または管理者の名前およびパスワードを入力します。
- システムアクセスが許可されている場合は、ログインするときに「システムアクセス」ワークグループを選びます。
- システムアクセスが許可されておらず、「Finder」に定期的にアクセスする必要がある場合は、お使いのアカウントに対してシステムアクセスを許可するように、「Macintosh マネージャ」の管理者に依頼してください。

クライアントユーザに発生する可能性がある問題

ユーザがサーバにログインできない場合：

サーバに十分なディスクの空き容量があることを確認します。ユーザのアカウントが削除されていたり、パスワードが変更されていないことを確認します。また、「ユーザ」パネル内の「基本設定」パネルをチェックして、ユーザのログインアクセスが無効になっているかどうかを確認します。

ユーザのコンピュータが停止する場合：

コンピュータが「Mac OS 9」より以前のシステムソフトウェアを使用している場合は、ファイル共有が無効になっていることを確認します。

ユーザがアプリケーションを開くことができない、アプリケーションが正しく動作しない場合：

- 「Mac OS 9 ワークステーションのファイルレベルのセキュリティを強化する」がこのワークグループに対して有効に設定されている場合、以前のアプリケーションの中には正しく動作しないで、エラーを表示するものもあります（207 ページの「ワークグループの権限設定」を参照してください）。
- アプリケーションによっては、「システムフォルダ」内の「初期設定」フォルダ以外の場所に、特殊なファイルを書き込んだり作成したりします。アプリケーションに関するトラブルがある場合、このことが原因の可能性があります。クライアントコンピュータの「アプリケーション」フォルダにある、「その他のアプリケーション •」（名前の最後の文字は黒丸（option ＋ 8）である必要があります）という名前のフォルダに、該当するアプリケーションのフォルダ（およびそのすべての内容）を入れてみてください。（このフォルダは、「Mac OS 9.1」以降のインストールされたコンピュータでは「Applications（Mac OS 9）」という名前です。）アプリケーションを「その他のアプリケーション •」フォルダに配置すると、そのアプリケーションは動作に必要なプラグインとファイルを読み出し、書き込み、および開くことができます。

ログイン先のボリュームを「セレクタ」で表示できない場合：

「ワークグループ」パネルの「ボリューム」パネルで「パネルにボリュームを表示する」を選ばない限り、「パネル」環境で、マウントされているボリュームがユーザに表示されることはありません。

共有ファイルへのアクセスに関して問題がある場合：

ユーザが複数のワークグループに所属しているかどうかを確認します。どのワークグループの共有ワークグループフォルダも、デフォルトでは、同じサーバボリュームにあります。ただし、ワークグループ書類が別のボリュームに保管されている場合、ワークグループを変更しない限り、ユーザがすべての共有書類にアクセスできない可能性があります。「AppleShare」を新しいバージョンにアップグレードするか、「Server Admin」を使ってユーザのホームディレクトリを別のボリュームに移動する必要があります。

アプリケーションが必要とするファイルをユーザが開くことができない場合：

ユーザのホームディレクトリ以外の場所にある書類にアクセスできる権利を、ユーザに許可していない可能性があります。別のフォルダへの一時的なアクセス権をユーザに許可することができます。「ワークグループ」パネルの「アクセス権」パネルを参照してください。

ワークグループデータボリュームは作成されたが、共有ワークグループ書類が「パネル」環境に表示されない場合：

- 「ユーザ」フォルダの場所が変更されていないことを確認します。「ユーザ」フォルダは、通常、サーバボリュームまたはワークグループデータボリュームの一番上のレベルにあります。
- 選んだワークグループデータボリュームに共有書類があることを確認します。

アプリケーション間でドラッグ & ドロップできない場合：

セキュリティ上の理由から、大部分のドラッグ & ドロップ機能は使用できないようになっています。コピー & ペーストを使用してください。

間違ったアプリケーションが開く場合：

各アプリケーションは、アプリケーションのファイル名ではなく、4 桁のクリエータ ID で識別されます。2 つのアプリケーションが同じクリエータ ID を持つ場合、間違ったアプリケーションが開く可能性があります。クライアントコンピュータのデスクトップを再構築してみてください。

ユーザがホームディレクトリにアクセスできない場合：

- 「Server Admin」の「ユーザとグループ」モジュールで、ユーザのホームディレクトリが設定されていることを確認してください。
- ホームディレクトリのアクセス権が正しく設定されていることを確認してください。
- ユーザのホームディレクトリが置かれたサーバが稼動していることを確認してください。

Macintosh マネージャに関するその他の情報

「Macintosh マネージャ」に関する詳しい情報については、以下を参照してください。

- AppleCare の Web サイトでは、製品の問題、使用、および動作に関する技術的な記事のデータベースである TIL をはじめ、さまざまな情報が用意されています。

  www.apple.co.jp/support

- ディスカッションリスト（「Mac OS X Server」および「Macintosh マネージャ」）では、ほかのサーバ管理者とアイデアやヒントを交換することができます。次の Web サイトで、ディスカッションリストに参加できます。

  www.lists.apple.com

11

NetBoot

NetBoot とは？

「NetBoot」を使うと、ネットワーク管理者は、クライアントが起動するときに使用するサーバ上のディスクイメージをアップデートするだけで、Mac OS 9 クライアントコンピュータの設定とアップデートをすばやく行うことができます。各ディスクイメージには「システムフォルダ」が含まれており、すべてのクライアントはここから起動することができます。「NetBoot」を使うことにより、サーバで設定済みの初期イメージをクライアントシステムに確実に反映することができます。サーバに加えるすべての変更は、クライアントコンピュータの再起動時に、自動的にクライアントコンピュータに反映されます。「Macintosh マネージャ」を使って、認証および個人の作業環境を、任意の「NetBoot」クライアントコンピュータのユーザに提供することができます。

NetBoot を使用する状況

「NetBoot」は、ネットワークで Macintosh コンピュータを使用する組織を対象として設計されています。iMac のような低コストで管理しやすいコンピュータを使って、教師がコンピュータ技術を教室に導入する際に、「NetBoot」は便利です。「NetBoot」は、次のことを行いたい教育者には理想的です。

- より多くの生徒がもっとコンピュータを利用できるようにしたい
- 限られた予算の中で、技術目標を達成したい
- コンピュータ関連設備の管理コストを削減したい
- 既存の技術資源から最大限のものを得たい

Macintosh ネットワークを使ったビジネス、特に、データ入力やワープロとして主に使用していたコンピュータの入れ替えを考えているビジネスでも、「NetBoot」サーバは理想的です。これらのビジネスでは、低コストの Macintosh ハードウェアを使い、「NetBoot」が可能にする管理要件の低減を利用して、コンピュータにかかるコストを最低限にすることができます。

NetBoot を設定する前に

「NetBoot」を設定する前に、以下のシステム要件に注意してください。

クライアントコンピュータの要件

- 「Mac OS X Server」に付属の「Mac OS 9.1」イメージ
- iMac、iBook、Power Macintosh G3（ブルーとホワイト）、Power Mac G4、Power Mac G4 Cube、PowerBook（FireWire）、または PowerBook G4
- 64 MB（メガバイト）以上のランダムアクセスメモリ（RAM）

「Mac OS X Server」から起動する各コンピュータには、それがネットワーク上での一意の装置であることを識別するための IP アドレスが必要です。このバージョンの「NetBoot」では、クライアントコンピュータは DHCP を使って IP アドレスを取得できます。（この機能を利用できるのは、特定の機種の Macintosh だけです。）前のバージョンの「NetBoot」では、BootP で IP アドレスを取得して起動することしかできませんでした。このバージョンの「NetBoot」は、DHCP と BootP の両方をサポートします。クライアントコンピュータがこの両方をサポートする場合、IP アドレスの取得方法として優先されるのは DHCP です。

「NetBoot」サーバを設定するためには、次の手順を実行する必要があります。

1. DHCP を使って起動できるコンピュータと BootP を必要とするコンピュータを決定します。詳細については、248 ページの「クライアント IP アドレス」を参照してください。
2. BootPを使って起動するコンピュータの場合、割り当てたい特定の範囲のIPアドレスを決定します。
3. 次のセクション「ネットワークの計画を立てる」を読んで、「NetBoot」の設定に必要な情報を集めてください。この章の後ろのほうにある「NetBoot サーバ ワークシート」を使って情報を整理することができます。

ネットワークの計画を立てる

ネットワークの構築を計画する場合、ネットワークの設定時に使用する情報を収集する必要があります。この情報は、253 ページの NetBoot サーバワークシートに記入できます。

手順 1：サーバに接続するクライアント数を確認する

サーバに接続できる「NetBoot」クライアントコンピュータの数は、サーバの構成だけでなく、その他の多くの要素によっても変わります。以下の構成の「NetBoot」サーバでは、50 台の「NetBoot」クライアントコンピュータを容易にサポートできます。

- Macintosh G3 または G4 コンピュータ（400 MHz 以上のプロセッサ搭載）
- 256 MB の RAM
- 2 つ以上の 9 GB（ギガバイト）のハードディスク（ハードディスクが複数あると「NetBoot」はより効率的にリソースを割り当てることができます。）
- ギガビット Ethernet：4 ポート、100Base-T 以上の高速 Ethernet カード

別の構成のサーバを使用したい場合や、25 台より多くのクライアントコンピュータをサポートしたい場合は、以下の要素を考慮してください。

- Ethernet の速度： 最適な性能を得るためには、クライアントとサーバの両方で 100Base-T 以上の速度での接続を強くお勧めします。
- ハードディスクの容量と「NetBoot」クライアントコンピュータの台数：「NetBoot」サーバには、それに接続されたクライアントごとのハードディスクの空き容量が必要です。必要な空き容量は、システムイメージのサイズと構成によって異なります。
- ハードディスクの容量とユーザの数： ユーザ数が多い場合は、ユーザの書類を保管するためのファイルサーバをネットワーク上に別に追加することを検討してください。デフォルトの設定では、「Macintosh マネージャ」を使用している場合、ユーザの書類と初期設定は「NetBoot」サーバに保存され、AFP（Apple Filing Protocol）サーバがこの情報を保存します。
- サーバとクライアントの位置：「NetBoot」クライアントコンピュータで BootP を使用する必要がある場合、それらのコンピュータはサーバと同じサブネット上にある必要があり、そのサブネット上の BootP サーバは 1 つだけになります。ただし、イメージ用には同じサブネット上に複数の「NetBoot」サーバを置くことができます。
- サーバの Ethernet ポートの数： 4 ポートの 100Base-T カードを使用している場合、「NetBoot」クライアントをサーバ上の複数の Ethernet ポートに割り当てることで、パフォーマンスが向上します。ポートを追加するには、Ethernet カードを追加するか、またはマルチポート Ethernet カードの複数のポートを使用することができます。各ポートは、別のセグメントを提供する必要があります。

手順 2：「NetBoot 設定アシスタント」の情報を集める

「NetBoot」クライアントとして使用する Ethernet ポートごとに、このセクションに記載されている情報が必要です。これらの情報を集めて、253 ページの「NetBoot サーバ ワークシート」にそれを記入してください。

サーバに付属しているソフトウェアを購入した場合、サーバには 5 つまでの Ethernet ポートが付いています。そのうちの 1 つは、サーバに付属の内蔵 Ethernet ポートです。その他のポートは、サーバに取り付けられた Ethernet カードのポートです。ポートの数は、サーバの構成によって異なります。サーバから「NetBoot」クライアントに接続するときは、100Base-T 以上の Ethernet を使用してください。

ポート IP アドレスとサブネットマスク

「NetBoot」クライアントに使用する各 Ethernet ポートには、IP アドレスとサブネットマスクが必要です。また、このポートに接続する「NetBoot」クライアントの IP アドレスにローカルトラフィックを制限するサブネットマスクを使用する必要があります。

クライアント IP アドレス

DHCP を使用できる「NetBoot」クライアントと、使用できない「NetBoot」クライアントを決定します。以下の Macintosh コンピュータは、DHCP を使用できます。

- すべてのスロットイン方式の iMac
- すべての iBook
- すべての Power Mac G4
- すべての Power Mac G4 Cube
- すべての FireWire PowerBook
- すべての PowerBook G4

その他の機種については、この機能を使用可能にしたり、コンピュータにこの機能があるかどうかを確認するために、最新のファームウェアアップデート（アップル社の Web サイトにあります）を行うことが必要になる場合もあります。（アップデートの必要がない場合は、アップデータがメッセージを表示します。）

- DHCP を使用するクライアントの場合：

  クライアントコンピュータがDHCPを使用できる場合、DHCPサーバがそのコンピュータと同じサブネット上にない場合でも、「NetBoot」サーバワークシートにそのコンピュータの IP アドレスを記入する必要はありません。

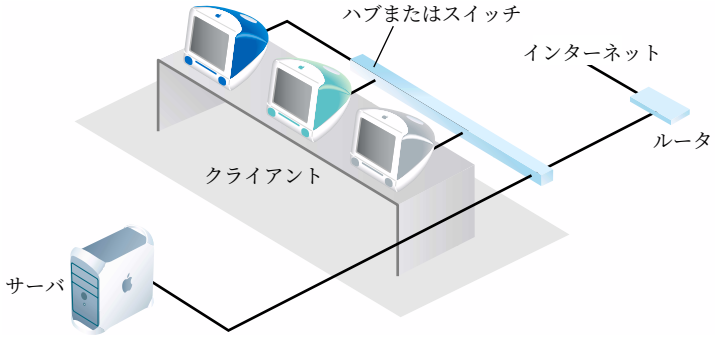
- BootP を使用するクライアントの場合：

  BootP を使用する各ポートに接続されている「NetBoot」クライアントの場合は、IP アドレスの範囲を 1 つ以上提供する必要があります。各コンピュータに最低 1 つの IP アドレスが必要です。ただし、拡張性を持たせるためにいくつか余分に割り当てておくことをお勧めします。

IP ルーティング情報

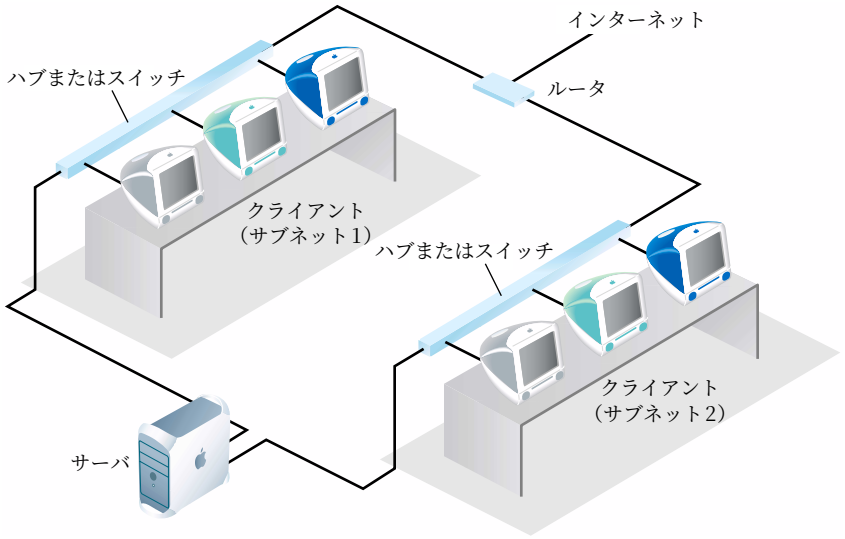
「NetBoot 設定アシスタント」に提供する必要のある IP ルーティング情報は、ネットワークの構成によって異なります。

この場合、サーバは 1 つのサブネット上の「NetBoot」クライアントのピアです。「NetBoot」クライアントはそれぞれ直接ルータに接続されています。このような構成の場合は、「NetBoot 設定アシスタント」の「NetBoot クライアントの IP ルーティング」パネルで「ピア」を選びます。「ルータの IP アドレス」に、ルータの IP アドレスを入力します。



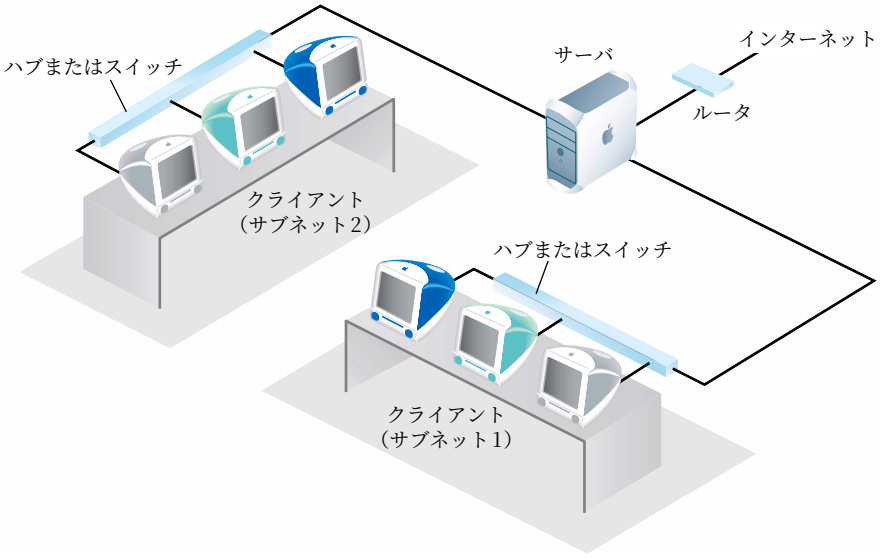
「NetBoot」クライアントを直接ルータに接続する場合

下の図の構成は、前の構成と似ていますが、2 つの「NetBoot」クライアントサブネットがある点が異なります。サブネットはそれぞれルータの別のポート、およびサーバの別のポートに接続されています。このような構成の場合は、「NetBoot 設定アシスタント」の「NetBoot クライアントの IP ルーティング」パネルで「ピア」を選びます。「ルータの IP アドレス」に、そのサブネットに接続するルータのポートの IP アドレスを入力します。



「NetBoot」クライアントを直接ルータに接続する場合

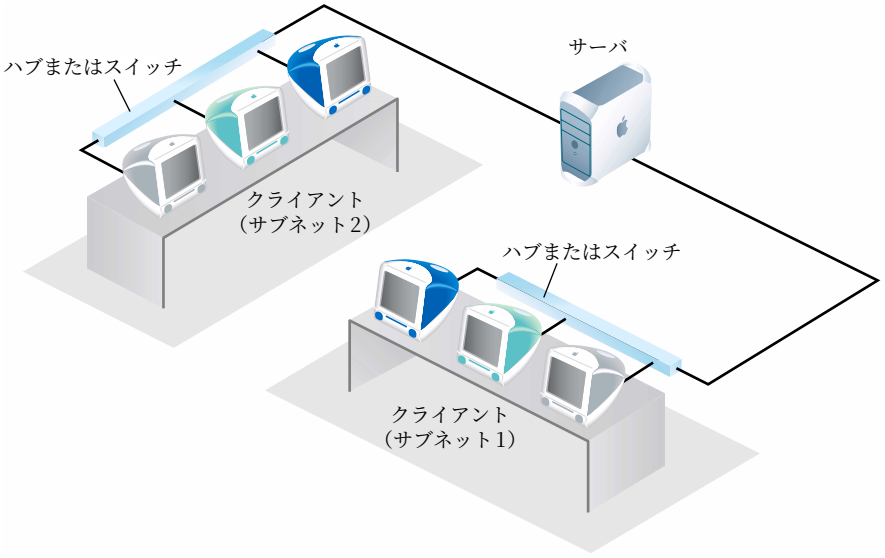
この構成では、サーバは1つまたは複数の「NetBoot」クライアントサブネットへのルータとして動作します。このような構成の場合は、「NetBoot 設定アシスタント」の「NetBoot クライアントの IP ルーティング」パネルで「ゲートウェイ」を選びます。ルータアドレスを提供する必要はありません。



サーバがルータへのゲートウェイである場合

参考：インターネットにアクセスするクライアントの場合、サーバがクライアントサブネットのゲートウェイとして動作することを示すように、ルーティングテーブルを更新する必要があります。クライアントサブネットごとに別のエントリを作成する必要があります。ルーティングテーブルを変更するときは、ルータに付属のソフトウェアを使用します。

このような構成の場合は、「NetBoot 設定アシスタント」の IP ルーティングの設定パネルで「ゲートウェイ」を選びます。ルータの IP アドレスを提供する必要はありません。



ルータなし―「NetBoot」クライアントがインターネットから孤立している場合

NetBoot サーバワークシート

各 Ethernet ポートに、次の情報を指定する必要があります。ポートの数は、サーバの構成によって異なります。

NetBootポート計画

次の情報をIPアドレス形式で指定してください（124.50.66.93など）。

内蔵のEthernetポート

IPアドレス： . . .

サブネットマスク： . . .

ルータアドレス： . . .

BootPのアドレス範囲（任意）： 開始 . . . 終了 . . .

サーバはピアとゲートウェイのどちらか? ☐ ピア ☐ ゲートウェイ

Ethernetカードポート1

IPアドレス： . . .

サブネットマスク： . . .

ルータアドレス： . . .

BootPのアドレス範囲（任意）： 開始 . . . 終了 . . .

サーバはピアとゲートウェイのどちらか? ☐ ピア ☐ ゲートウェイ

Ethernetカードポート2

IPアドレス： . . .

サブネットマスク： . . .

ルータアドレス： . . .

BootPのアドレス範囲（任意）： 開始 . . . 終了 . . .

サーバはピアとゲートウェイのどちらか? ☐ ピア ☐ ゲートウェイ

Ethernetカードポート3

IPアドレス： . . .

サブネットマスク： . . .

ルータアドレス： . . .

BootPのアドレス範囲（任意）： 開始 . . . 終了 . . .

サーバはピアとゲートウェイのどちらか? ☐ ピア ☐ ゲートウェイ

Ethernetカードポート4

IPアドレス： . . .

サブネットマスク： . . .

ルータアドレス： . . .

BootPのアドレス範囲（任意）： 開始 . . . 終了 . . .

サーバはピアとゲートウェイのどちらか? ☐ ピア ☐ ゲートウェイ

NetBoot サーバソフトウェアを初めて設定する

セクション 246 ページの「ネットワークの計画を立てる」をまだ読んでいなくて、上の NetBoot サーバワークシートに必要事項を記入していない場合は、先に進む前にそのセクションを読み、記入してください。「NetBoot 設定アシスタント」を使用するときに、この情報が必要になります。

手順 1：「NetBoot」サーバソフトウェアをインストールする（省略できます）

お使いのソフトウェアをサーバと共に購入した場合、「NetBoot」サーバソフトウェアはすでにインストールされています。この手順を飛ばして、手順 2 に進んでください。

ハードウェアなしで「Mac OS X Server」ソフトウェアを購入した場合は、「NetBoot」サーバソフトウェアをインストールする必要があります。これは、「Mac OS X Server」ソフトウェアに付属の CD にあります。「NetBoot」サーバソフトウェアは、「Mac OS X Server」ソフトウェアがすでにインストールされ、設定が済んでいるコンピュータにインストールする必要があります。

「NetBoot」サーバソフトウェアをインストールするときは、次のように操作します。

1. 「NetBoot」の CD をコンピュータの CD-ROM ドライブにセットします。
2. 「NetBoot」の CD のアイコンをダブルクリックします。
3. 「NetBoot.pkg」をダブルクリックします。
4. 画面に表示される指示に従って操作してください。「Mac OS X Server」の設定アシスタントを使用したときに設定した管理者のパスワードを使用します。

   このインストーラの指示に従って、ソフトウェアのインストールに必要な手順を実行します。

手順 2：「NetBoot 設定アシスタント」を使う

「NetBoot」ソフトウェアのインストールが終わると、自動的に設定アシスタントが開きます。アシスタントを開いていない場合は、次の手順で開きます。

1. 「Mac OS X Server」に管理者としてログインします。「Mac OS X Server」の設定アシスタントを使用したときに設定した管理者のパスワードを使用します。
2. 「/Applications/Utilities」ディレクトリの「Assistant」をダブルクリックします。
3. 「Assistants」ウインドウが開いたら、「NetBoot設定アシスタント」をダブルクリックします。
4. 画面に表示される指示に従って操作してください。

   設定アシスタントの指示に従って、ソフトウェアの設定に必要な手順を実行します。それぞれの手順について詳しく知りたいときは、ウインドウの「詳しい情報を見る」ボタンをクリックします。

   今後、設定情報を変更する必要がある場合、「NetBoot 設定アシスタント」を使用します。

手順 3：「Macintosh マネージャ」を設定する

「Macintosh マネージャ」を使用して「NetBoot」クライアントユーザに認証と個人的な作業環境を提供する場合は、「Macintosh マネージャ」が設定されていることと、ユーザが「Mac OS X Server」の「ユーザとグループ」データベースから読み込まれていることを確認してください。「Macintosh マネージャ」ワークグループと必要な設定を設定してください（195 ページの第 10 章「Macintosh マネージメントサービス」を参照してください）。「システムアクセス」ワークグループに、最低でも 1 つの「Macintosh マネージャ」管理者ユーザが割り当てられていることを確認してください。

手順 4：「NetBoot」クライアントコンピュータを起動する

「NetBoot」サーバから起動できる「Mac OS」コンピュータであれば、「NetBoot」クライアントコンピュータとして使用することができます。

コンピュータのファームウェアをアップデートする必要がある場合は、この段階でアップデートします。詳細については、アップル社の Web サイトを参照してください。

「NetBoot」クライアントコンピュータを起動するときは、次のように操作します。

1. クライアントコンピュータをネットワークに接続します。
2. N キーを押したままクライアントコンピュータを起動します。

コンピュータは「NetBoot」サーバを検索します。クライアントコンピュータがサーバを検索して起動するには、数秒かかることがあります。1 分以上たってもコンピュータが起動しない場合は、261 ページの「NetBoot に関する問題を解決する」を参照してください。

いったんコンピュータが起動したら、「NetBoot HD」という名前のボリュームが現れます。

「起動ディスク」コントロールパネルを開き、「ネットワーク」を選びます。

次回コンピュータを起動するときに、N キーを押す必要はありません。いったん「NetBoot」サーバからコンピュータを起動すると、問題（サーバの停止など）が発生したり、「起動ディスク」コントロールパネルで起動ディスクを変更しない限り、常に「NetBoot」サーバから起動します。

NetBoot Desktop Admin を使用する

「NetBoot」クライアントコンピュータを起動したときに現れる「NetBoot HD」ボリュームは読み出し専用のディスクイメージのため、変更することはできません。このディスクイメージに新しいソフトウェアをインストールしたり、システム構成を変更したりするときは、「NetBoot Desktop Admin」アプリケーションを使用して、ディスクイメージの変更可能なコピーを作成します。変更が完了すると、「NetBoot Desktop Admin」によって既存のディスクイメージと変更済みのディスクイメージが置き換えられます。

ソフトウェアをインストールする／ディスクイメージを変更する

ソフトウェアをインストールしたり、「NetBoot HD」ディスクイメージを変更したりするときは、「NetBoot」クライアントコンピュータから起動して、「NetBoot」サーバボリュームに接続してから、「NetBoot Desktop Admin」プログラムを開く必要があります。これについては、以下の手順で説明します。「NetBoot Desktop Admin」を実行する「NetBoot」クライアントコンピュータが最後に再起動するまで、変更したユーザもほかのユーザも変更後の内容を利用できません。

開始する前に、以下の情報が必要です。

- 「NetBoot」サーバボリュームに対して読み出し／書き込みのアクセス権を持つユーザの名前とパスワード（たとえば、「Mac OS X Server」の管理者）。

参考：「NetBoot」クライアントコンピュータで「Macintosh マネージャ」を使用している場合、クライアントコンピュータを起動または再起動するたびに、「システムアクセス」ワークグループに属する「Macintosh マネージャ」管理者としてログインする必要があります。

ソフトウェアをインストールしたり、「NetBoot HD」ディスクイメージを変更したりするときは、次のように操作します。

1. 読み出し／書き込みアクセス権を持つユーザ（たとえば、「Mac OS X Server」の管理者）としてサーバボリュームにログインして、「NetBoot Desktop Admin」アプリケーションを開きます。

   移動していないかぎり、アプリケーションは「NetBoot Desktop Admin」フォルダにインストールされています。このフォルダは「NetBoot」サーバの「Admin」フォルダにあります。

2. 新しいソフトウェアをインストールする場合は、必要に応じてディスクイメージのサイズを大きくします。

   ディスクイメージに、目的のソフトウェアをインストールするのに十分な空きがあることを確認します。イメージを大きくするときは、必要なサイズだけ拡大するようにします。バックアップコピーに戻す以外に、イメージのサイズを小さくする方法はありません。

   参考：新しいバージョンの「Mac OS」をインストールする場合は、「NetBoot HD」ディスクイメージのサイズを少なくとも 50 MB 増やしてください。

3. 「プライベートコピーの作成」をクリックします。

   「NetBoot Desktop Admin」はディスクイメージのコピーを作成します。この操作には数分かかります。プロセスを中断しないでください。完了すると、「NetBoot」クライアントコンピュータは自動的に再起動します。

   重要　ディスクイメージのコピーは、作成に使用した「NetBoot」クライアントコンピュータに関連付けられているので、そのイメージを変更するときは、同じコンピュータを使用する必要があります。別のコンピュータを使用すると、変更したユーザは変更後の内容を見ることができず、ほかのユーザも変更後の内容を利用できません。また、権限のないユーザがそのディスクイメージを変更する危険性が増します。

4 ソフトウェアをインストールするか、システム設定に変更を加えます。

ソフトウェアをインストールするときは、ソフトウェアに付属のマニュアルのインストールの説明に従って操作します。必要に応じて、コンピュータを再起動します。

アプリケーションをインストールする場合は、そのアプリケーションを開きます。アプリケーションを開くと、必要に応じて、登録番号の入力が求められます。この段階で登録番号を入力しないと、ユーザがアプリケーションを開くたびに、登録番号を入力しなければならなくなります。さらに、ほとんどのアプリケーションは「システムフォルダ」に環境設定ファイルを作成します。ここでアプリケーションを開かないと、環境設定が存在しないためにユーザがアプリケーションを開くことができない場合があります。

5 「ゴミ箱」の中に、保存しておきたいファイルがないことを確かめてください。(「ゴミ箱」は、次の手順で自動的に空になります。)

参考：使用中のファイルが入っているためにゴミ箱を空にできない場合は、コンピュータを再起動する必要があります。

6 「NetBoot Desktop Admin」アプリケーションを開いて、次に「保存」または「破棄する」をクリックします。コンピュータは自動的に再起動します。

ほかの変更が必要な場合は、「終了」をクリックして手順5に戻ります。

7 「NetBoot」クライアントコンピュータを再度起動して、次に「NetBoot Desktop Admin」アプリケーションを開きます。

古いディスクイメージのバックアップコピーを保存しておきたい場合は、「以前のディスクをバックアップとして残す」オプションを選択したままにします。バックアップコピーは、「NetBoot」サーバの「Shared Images」フォルダの中の「Backup Images」に保管されます。

8 手順6で「保存」をクリックした場合は、「再起動」をクリックします。それ以外の場合は、「OK」をクリックします。

「再起動」をクリックすると、「NetBoot Desktop Admin」は変更を保存し、古いディスクイメージを削除し、コンピュータを再起動します。変更後の内容は、次回「NetBoot」クライアントコンピュータを再起動したときに利用可能になります。「OK」をクリックすると、「NetBoot Desktop Admin」は古いディスクイメージを削除します。

NetBoot に関する上手な使いかたとヒント

NetBoot のパフォーマンスを向上させる

多くの要因が「NetBoot」クライアントのパフォーマンスに影響を及ぼします。いくつかの要因を調整して、「NetBoot」クライアントの起動時間を減らしたり、クライアントのパフォーマンスを向上させたり、サポートできるクライアントの数を増やしたりすることができます。また、ネットワークとサーバのパフォーマンスを向上させるための調整も可能です。

ネットワークのパフォーマンスを最適化するために調整する要因は、ネットワークの設定によって異なります。最良の方法は、最も著しい効果があると思われる領域を見つけて、まず最初にそこを変更することです。ここで推奨するいくつかの変更を行うだけでも、著しく改善されることがお分かりになるでしょう。

ネットワークパフォーマンスの要因

- 100Base-T またはそれ以上の高速 Ethernet ネットワークで、サーバとクライアントが同じセグメントまたはハブにつながっている場合、最高のパフォーマンスを得ることができます。サーバが 10Base-T「スイッチング」ネットワークに 100Base-T 以上の高速接続をしている場合は、クライアントコンピュータ用に少なくとも 10Base-T の「スイッチング」Ethernet を使用できます。「NetBoot」が 10Base-T のスイッチング Ethernet ネットワークで動作している場合でも、100Base-T 以上の高速接続が最適なパフォーマンスを提供します。
- 各セグメントまたはハブに接続するクライアントコンピュータの数を決定するために、「NetBoot」ネットワークを設定する前に使用パターンを分析します。かなり激しく使用する可能性があれば、いくつかのサービス（「Apple ファイルサービス」または「Macintosh マネージャ」など）を複数のサーバの間に分割させる必要があるかもしれません。
- 「NetBoot」環境では常に、ハブではなくスイッチを使用するほうがパフォーマンスが向上します。

NetBoot と AirMac

「NetBoot」クライアントでの AirMac ワイヤレス技術の使用は、アップル社はサポートしていません。

サーバパフォーマンスの要因

- 単一サーバのネットワークでは、ネットワーク上のクライアントはすべて、起動、仮想メモリへのアクセス、およびファイルとアプリケーションへのアクセスのために同じサーバを使用します。これは、サーバのハードディスクとネットワークに対して大きな負担をかけます。サーバにインストールされている RAM の容量を最低でも 256 MB に増やすと、サーバのハードディスクにかかる負荷を減らすことができます。
- サーバの処理速度も重要で、単一サーバネットワークでは特に重要です。常に、サーバとして利用できるコンピュータのうち、サポートされている最高速のものを使用してください。
- 「Macintosh マネージャ」を使用している場合、ハードディスクをもう 1 台追加することでパフォーマンスを向上させることもできます。これは、「Macintosh Management Server」が、同じサーバボリュームへのアクセスを、多数のクライアントに同時に許可するためです。
- ユーザ書類の保管用にもう 1 つの AFP（Apple Filing Protocol）互換サーバを使用すると、サーバの負担をさらに減らすことができます。
- 「NetBoot」および「Macintosh マネージャ」と関連付けられたシステムファイルを、再調整したい場合もあるでしょう。ただし、間違った方法でこれを行うと、サーバが使用不能になることがあります。システムファイルの再調整はお勧めできません。

クライアントパフォーマンスの要因

- 最も信頼性のある性能向上の方法は、おそらく、各クライアントコンピュータにインストールされている RAM を増やすことです。これによりクライアントが仮想メモリを使う必要がなくなり、クライアントがメモリキャッシュをより多く使えるようになります。
- また、クライアントコンピュータがネットワークから（デフォルト）ではなくクライアントハードディスクから仮想メモリを使うように設定することによって、クライアントのパフォーマンスを高めることもできます。これにより、アプリケーションを開いているときは特に、ネットワークトラフィックとサーバのハードディスク上の負荷を減らすことができ、より良いクライアントパフォーマンスを提供できます。クライアントが仮想メモリをクライアントハードディスクから使用できるようにするには、256 ページの「ソフトウェアをインストールする／ディスクイメージを変更する」に記載されているように、「NetBoot Desktop Admin」を使ってサーバ上のシステムイメージを変更します。いったん変更用にイメージをコピーしてから再起動し、「メモリ」コントロールパネルを開いて、「仮想メモリ」領域のローカルハードディスクを選択します。仮想メモリの設定を変更した後、再び「NetBoot Desktop Admin」を使って「共有可能な」新しいシステムイメージをにします。すべての「NetBoot」クライアントのローカルハードディスクの名前が同じであることを確認します。
- クライアントにインストールされているRAMの容量が大きい場合は、仮想メモリをオフにすることが必要になる場合があります。ただし、「Mac OS 9」では仮想メモリはデフォルトの設定でオンであり、通常もオンにしておくことをお勧めします。
- 「Macintosh　マネージャ」を使用している場合は、これによって各ユーザの初期設定ファイルを保存できます。これらのファイルはサーバに保存されます。保存する初期設定が多くなると、ユーザのログイン時にクライアントコンピュータが初期設定をロードする時間が長くかかるようになります。ログインの直後に長い遅れがある場合は、「Macintosh マネージャ」で保存している初期設定の数を減らすことを考慮してください。

  最も重要なこととして、ユーザの Web ブラウザのキャッシュは保存しないでください。インターネットブラウザを頻繁に使用する環境では、ブラウザのキャッシュはすぐに大きくなってしまう可能性があります。ブラウザのキャッシュを保存しないように「Macintosh マネージャ」を設定すると、このような大きなファイルがサーバとクライアントの間で転送されなくなるため、ログイン後の起動時間を劇的に減らすことができます。

パフォーマンスについてのまとめ

最良のパフォーマンスを得るためには、次のヒントに従ってください。

- サーバから「NetBoot」クライアントがあるネットワークへの接続には、常に 100Base-T 以上の高速 Ethernet 接続を使用してください。
- 最低でも、クライアントからネットワークへの接続は、全二重 10Base-T のスイッチング Ethernet 接続にすることをお勧めします。100Base-T 以上の高速 Ethernet の全二重または半二重接続をお勧めします。Ethernet スイッチは、二重モードの自動ネゴシエーションをサポートするように設定してください。

- ユーザの使用パターンをサポートするサーバ、ネットワーク、およびクライアント設定を選んでください。
- ネットワークに、より多くのサーバを追加して、「NetBoot」、「Macintosh マネージャ」、および Apple ファイルサービスをサーバ間で分割することを考慮してください。
- サーバに追加のRAMをインストールして、サーバのハードディスクにかかる負荷を減らしてください。
- サーバにハードディスクを追加して、パフォーマンスを向上させてください。
- 単一サーバネットワークでは特に、サーバとして最高速のコンピュータを使用してください。
- 「NetBoot」クライアントに追加の RAM をインストールして、ネットワーク全体にわたる仮想メモリの使用を減らしてください。
- 「NetBoot」クライアントを、ローカルハードディスクから仮想メモリを使用するように設定してください。
- 「Macintosh マネージャ」がユーザ用に保存する初期設定の数を減らしてください。
- Web ブラウザのキャッシュを保存しないでください。

NetBoot の内側

以前のバージョンの「NetBoot」に「System」ディスクイメージと「Application」ディスクイメージが両方とも含まれていた場合にかぎり、現在「NetBoot」サーバが必要とするのは 1 つのイメージ（「NetBoot HD」ディスクイメージ）だけです。「NetBoot HD」ディスクイメージにアプリケーションをインストールするか、または「Application」ディスクイメージを引き続き使用することができます。また、「Application」ディスクイメージに対して変更を加えるときに、引き続き「NetBoot Desktop Admin」を使用することもできます。

重要 「NetBoot」クライアントコンピュータは、「NetBoot」サーバの提供する「Mac OS 9.1」イメージを使用する必要があるため、クライアントコンピュータごとに「Mac OS 9.1」のライセンスが必要です。つまり、「Mac OS 9.1」がクライアントコンピュータに入っているか、「Mac OS 9.1」のライセンスを購入する必要があります。「Mac OS X Server」と「NetBoot」サーバの使用許諾契約には、「Mac OS」のライセンスは含まれていません。

「Mac OS 9」を使用する「NetBoot」クライアントコンピュータには、64 MB のメモリが必要です。「NetBoot」クライアントコンピュータにこれだけのメモリがない場合は、「NetBoot Desktop Admin」を使って、仮想メモリをこの量と同じかそれ以上の量に増やします。仮想メモリを増やすときは、「NetBoot HD」イメージのプライベートコピーから再起動した後で、「メモリ」コントロールパネルを使用します。クライアントコンピュータのローカルハードディスクへの仮想メモリの割り当ては、可能な限りこれらの推奨事項に従ってください（259 ページの「クライアントパフォーマンスの要因」を参照）。

NetBoot に関する問題を解決する

「NetBoot」クライアントコンピュータが起動しない場合：

- ほかのコンピュータがネットワーク上で負荷の高い要求を出しているために、コンピュータがすぐに起動しないことがあります。数分待ってから、再度、起動してみてください。
- すべてのケーブルが適切に接続されていること、起動しないコンピュータおよびサーバの電源が接続されていることを確認します。詳しくは、クライアントコンピュータに付属のトラブル対処の情報を参照してください。
- Ethernetケーブルの片方の終端がコンピュータのEthernetポートに差し込まれていて、もう一方の終端がスイッチまたはハブの作動中の Ethernet コネクタに差し込まれていることを確認します。
- 自分のネットワークに割り当てられている IP アドレスの数を超えていないことを確認します。
- クライアントコンピュータにメモリまたは拡張カードを取り付けた場合は、正しく取り付けられていることを確認します。
- サーバに複数のEthernetカードがある場合、またはマルチポートEthernetカードで複数のポートを使用している場合は、同じカードまたは同じポートを使用しているほかのコンピュータを起動できるかどうかを確認します。起動できない場合は、サーバで設定した Ethernet ポートが、クライアントコンピュータが接続されたポートと同じであることを確認します。マルチポートカードの Ethernet ポート 1 を、Ethernet ポート 4 と間違えることがよくあります。Macintosh サーバにあらかじめインストールされているカードの場合、コンピュータの裏側から見るとポート番号が左から右に 4、3、2、1 となっています。
- コンピュータに「システムフォルダ」が保存されているローカルハードディスクがある場合は、Ethernet ケーブルを外して、ローカルハードディスクからコンピュータを起動してみます。その後、Ethernet ケーブルを接続し直して、ネットワークからコンピュータを起動してみます。

「Macintosh マネージャ」の使用中にユーザが「NetBoot」クライアントにログインできない場合：

- ユーザがほかのコンピュータにログインできるかどうかを確認します。ユーザがほかのコンピュータにログインできる場合、問題のクライアントコンピュータは、そのユーザのアカウントが登録されていない「Macintosh マネージャ」サーバに接続されている可能性があります。複数の「Macintosh マネージャ」サーバがある場合は、ユーザが自分のアカウントが登録されているサーバを選択したことを確認します。
- 「Macintoshマネージャ」を開き、ユーザが少なくとも1つのワークグループのメンバーであることを確認します。
- 「Macintosh マネージャ」を開き、ユーザのパスワードを再設定します。

12

ネットワークサービス

ネットワークサービスとは？

ネットワークサービスは、TCP/IP ネットワークでのインターネット通信を制御します。「Mac OS X Server」は、次のネットワークサービスを備えています。

- SLP（Service Location Protocol）DA（Directory Agent）サービス
- DHCP（Dynamic Host Configuration Protocol）サービス
- DNS（Domain Name System）サービス
- IP フィルタサービス

ネットワークサービスは、会社の IP アドレスの管理、ネットワークリソースの構成、ドメイン名の管理、および不必要なインターネット接続をブロックするための IP フィルタの設定を行うときに使用します。中規模から大規模なネットワークの場合は、ネットワークサービスが役立つでしょう。

この章では、「Mac OS X Server」で提供される 4 つのネットワークサービスについて、それぞれのセクションが設けられています。各セクションには、サービスの動作、機能、および最初の設定方法について理解しておく必要のある情報が記載されています。また、主な設定パネルのスクリーンショットを示して、これらのパネルのオプションについて説明しています。ほとんどのセクションには、経験豊富なネットワーク管理者を対象とした情報と、追加情報の参照先も記載されています。

SLP（Service Location Protocol）DA（Directory Agent）サービス

SLP DA サービスでは、ネットワークで利用可能なサービス（またはリソース）に枠組みを提供して、ユーザがサービスにアクセスしやすいようにします。URL を使ってアクセスできるものはすべて、ネットワークサービスと見なすことができます。ファイルサーバ、WebDAV サーバ、NFS サーバ、プリンタ、個人用の Web サーバなどがその例です。

ネットワークにサービスを追加すると、SLP を使用してネットワーク上にそのサービスが「登録」されます（サービスの存在を知らせ、提供するサービスが識別されます）。手動で設定する必要はありません。クライアントコンピュータがネットワークサービスを検索する必要がある場合は、SLP を使って目的の種類のサービスを検索します。クライアントコンピュータの要求に一致するすべての登録サービスが表示されるので、ユーザはこの中から使用するサービスを選ぶことができます。

SLP DA（Directory Agent）は基本となる SLP を拡張したもので、登録されているネットワークサービスを中央リポジトリに保管します。DA を設定することによって、1 つまたは複数のスコープ（サービスのグループ）のサービスを追跡することができます。クライアントコンピュータがネットワークサービスを検索する場合、クライアントコンピュータが接続しているスコープの DA が応答し、利用できるサービスのリストが表示されます。クライアントコンピュータはローカルのサービスを検索するだけなので、ネットワークを流れる通信の量が最低限に抑えられ、ユーザはよりすばやくネットワークサービスに接続できます。

SLP DA サービスを使用する状況

通常、SLP サービスはネットワーク上のすべての SLP サービスに要求を送信するため、実質的にはネットワークを流れる通信量を増大させる可能性があります。大規模なネットワークの場合、SLP 通信によってネットワークの性能が低下し、ネットワークサービスを検索するときに、ユーザが待たされる時間が長くなる可能性があります。SLP DA サービスを設定することによって、SLP の性能を向上させることができます。また、クライアントコンピュータは最も近くにあるディレクトリエージェントにサービスを問い合わせることが可能で、サービスは複数のディレクトリエージェントに登録できるので、複数のディレクトリエージェントを設定することも検討してください。

SLP DA サービスを設定する前に

SLP DA サービスを設定する前に、このセクションを読んで、スコープの定義、クライアントとルータの互換性の確認について理解してください。

スコープを定義する

スコープを定義するためには、ネットワーク上のコンピュータをどのように構成したいかを決める必要があります。スコープとして、コンピュータの論理的なグループ（製造部門で使用するすべてのコンピュータなど）、または物理的なグループ（1 階にあるすべてのコンピュータなど）を設定することができます。スコープは、ネットワークの一部または全体として定義できます。ネットワークを複数のスコープに分割しない場合でも、SLP DA サービスを使用するためには少なくとも 1 つのスコープを設定する必要があります。

クライアントとルータの互換性

SLP DA サービスを使用するためには、クライアントコンピュータが「Mac OS 9.1」以降を使用している必要があります。「Mac OS 9.0」の SLP では、引き続き IP マルチキャストが使用されます。ネットワークで IP マルチキャスト機能のないルータを使用している場合は、ルータをアップグレードするかまたはトンネリングを設定する必要があります。トンネリングについては、ルータに付属のマニュアルを参照してください。

SLP DA サービスを初めて設定する

SLP DA を初めて設定するときは、次の手順に従って行います。これらの作業を行うためにより詳しい情報が必要な場合は、オンスクリーンヘルプを参照してください。

手順 1：ログを設定する

イベントのログを記録すると、SLP DA の状況を監視するのに役立ちます。問題が発生した場合、またはサービスの性能を向上させたい場合に、ログ項目を参照すると重要な診断情報を得ることができます。SLP DA サービスのエラーは自動的にログに記録されますが、ほかの種類のイベントも記録されるように SLP DA サービスを設定することもできます。

ログの設定を表示するときは、「ネットワーク」タブをクリックし、「SLP サービス」をクリックし、「SLP DA を設定」を選びます。必要な設定を選びます。設定については、267 ページの「SLP DA サービスの設定」を参照してください。

手順 2：ネットワークのスコープを作成する

スコープを作成するときは、「SLP サービス」をクリックし、「登録サービスを表示」を選びます。「登録サービス」ウインドウが表示されます。

「新規スコープ」をクリックし、下の図の「スコープを追加」ダイアログボックスに作成中のスコープの名前を入力します。SLP DA サービスは入力する名前を正しい形式に変換し、「登録サービス」ウインドウのリストにそれを追加します。

手順 3：各スコープにネットワークサービスを割り当てる

スコープを作成したら、それにネットワークサービスを割り当てることができます。「登録サービス」ウインドウの「新規サービス」をクリックします。「プロキシサービスを追加」ダイアログボックス（下の図）で、スコープを選び、必要なサービスを追加できます。「プロキシサービスを追加」ダイアログボックスについては、268 ページの「登録サービスの設定」を参照してください。

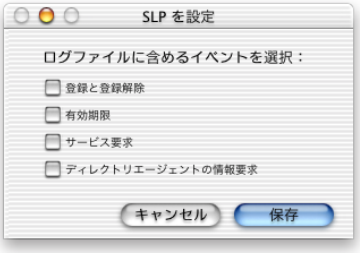
手順 4：SLP DA サービスを開始する

SLP DA サービスを開始するときは、「SLP サービス」をクリックし、「SLP DA を開始」を選びます。サービスを開始すると、サービスのアイコンに地球のマークが表示されます。ネットワーク上のサービスがディレクトリエージェントに登録されると、適切なスコープの下にある「登録サービス」ウインドウに表示されます。

SLP DA サービスの設定

SLP DA を設定する

「SLP を設定」ウインドウでは、SLP DA サービスのログの設定を選ぶことができます。このウインドウにアクセスするときは、「ネットワーク」タブをクリックし、「SLP サービス」をクリックし、「SLP DA を設定」を選びます。



登録と登録解除

サービスが登録および登録解除されたときにログを記録したい場合は、このオプションを選びます。サービスは定期的に再登録されますが、サービスを手動で登録することもできます。サービスの利用が一定期間ないと、サービスは登録解除されます。

有効期限

サービスが登録解除されたときにだけログを記録したい場合は、このオプションを選びます。このオプションを選ぶと、登録と登録解除の両方をログに記録した場合と比べて作成されるログ項目の数が少なくなります。

サービス要求

クライアントコンピュータがネットワークサービスを要求したときにログを記録したい場合は、このオプションを選びます。ネットワーク上ではサービス要求が頻繁に発生するので、このオプションを選択すると多数のログ項目が作成されることがあります。

ディレクトリエージェントの情報要求

クライアントコンピュータがディレクトリエージェントに関する情報を検索または要求したときにログを記録したい場合は、このオプションを選びます。このオプションを選択した場合も、多数のログ項目が作成されることがあります。

登録サービスの設定

「登録サービス」ウインドウでは、スコープと登録サービスを表示できます。また、スコープとサービスの作成と管理も行うことができます。ウインドウの最上部で、接続している「Mac OS X Server」のホスト名と IP アドレス、表示中のサービスの数、および登録サービスの総数を見ることができます。

「登録サービス」ウインドウにアクセスするときは、「SLP サービス」をクリックし、「登録サービスを表示」を選びます。

このリストには、このサーバに定義されているすべてのスコープが表示されます。スコープの隣にある三角形をクリックして、そのスコープに登録されているサービスを表示します。

表示

「表示」ポップアップメニューから表示したいサービスの種類を選びます。「すべてのサービス」を選んだり、利用可能なほかの種類のサービスから選ぶことができます。

取り除く

リストのスコープまたはサービスを選び、「取り除く」をクリックして、サービスを登録解除するか、またはスコープを取り除きます。ローカルではないサービスを登録解除しても、そのサービスがディレクトリエージェントで再登録される場合は、一時的な解除になることがあります。

新規スコープ

新しいスコープを作成するときは、「新規スコープ」をクリックします。

新規サービス

サービスを SLP DA に登録し、選択されているスコープに割り当てるときは、「新規サービス」をクリックします。下の図に示す「プロキシサービスを追加」ダイアログボックスが表示されます。

スコープ

サービスを追加したいスコープを選びます。

URL

サービスの URL を入力します。

属性リスト

このフィールドにサービスに関する情報を入力します。属性とは、サービス名や 1 分間にプリントできるページ数など、サービスを説明するプロパティのことです。このフィールドは必要に応じて入力します。正しいフォーマットが分からない場合は、入力しないでください。属性の詳細については、270 ページの「属性リストを使用する」を参照してください。

SLP DA サービスに関する上手な使いかたとヒント

SLP DAサービスには､経験豊富な管理者の方を対象とした追加機能がいくつかあります。

ログを使用する

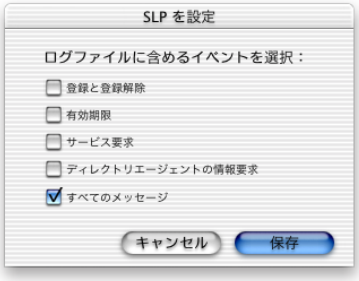
SLP DA サービスのログ項目は、システムログに保存されます。システムログにアクセスするときは、「Server Admin」の「一般」タブをクリックし、「ログビューア」をクリックして、「System Software」を選びます。ポップアップメニューから「System Log」を選びます。システムログには数百ものログ項目が記録されることがあるので、SLP DA サービスのイベントを探すときは「slpd」を検索します。

ログを設定するときは、ログに記録したいイベントの種類を選びます。次の表は、ログに記録されるイベントの種類に関連付けられているエラー文字列のリストです。

エラー文字列	SLP DA サービスのイベント
REG	登録と登録解除
EXP	有効期限（登録解除されたサービス）
SR	サービス要求
DA	ディレクトリエージェントの情報要求
ERR	SLP エラー

デバッグメッセージをログに記録する

この章の最初の方で説明したログオプションのほかに、デバッグメッセージをはじめ、すべてのイベントをログに記録することを選択できます。これは、経験豊富なシステム管理者の方に役立つ機能です。デバッグメッセージをログに記録するときは、option キーを押したまま「SLP サービス」をクリックし、「SLP DA を設定」を選びます。「すべてのメッセージ」が「SLP を設定」ウインドウに表示されます。



属性リストを使用する

サービスは属性のリストと共に、ネットワーク上で存在をアピールすることができます。これらの属性は、特定のフォーマットに従う文字列エンコードとして一覧表示されます。ディレクトリエージェントは、クライアント要求を適切なサービスに対応付けるために、属性リストを使用します。

Amazon という名前のネットワークプリンタの属性リストの例を示します。Amazon は、スコープ「Research」にある LPR プリンタです。管理者が入力する属性リストは、次のようになります。

(Name＝Amazon),(Description＝For research dept only),(Protocol＝LPR), (location-description＝bldg 6),(media-size＝na-letter),(resolution＝res-600),x-OK

サービスの属性リストを作成した場合、ディレクトリエージェントはサービスの検索時にこのリストをスキャンする必要があります。このため、属性リストのフォーマットが正しくないと、ディレクトリエージェントがサービスを使用するのをブロックしてしまうことがあります。

DHCP（Dynamic Host Configuration Protocol）サービス

DHCP サービスを使用すると、サーバからクライアントコンピュータの IP アドレスを管理し、割り当てることができます。DHCP サーバを設定するときは、クライアントに対して利用可能にすることができる IP アドレスのブロックを割り当てます。クライアントコンピュータは、起動するたびに、DHCP サーバ（ネットワーク上に複数設置できます）を検索し、見つかった DHCP サーバに IP アドレスを要求します。DHCP サーバは利用可能な IP アドレスを確認し、「リース期間」（クライアントコンピュータがその IP アドレスを使用できる期間）および設定情報と共に IP アドレスをクライアントコンピュータに送信します。

DHCP モジュールを使用すると、「Server Admin」で次の操作を行うことができます。

- DHCP サービスを設定し、管理する
- サブネットを作成し、管理する
- クライアントコンピュータに DNS および NetInfo オプションを設定する
- DHCP と「NetBoot」のクライアントコンピュータを表示する

DHCP サービスを使用する状況

組織内のクライアントの数が IP アドレスよりも多い場合は、DHCP サービスを使用するとよいでしょう。IP アドレスは必要に応じて割り当てられます。不要になると、ほかのクライアントがその IP アドレスを使用できるようになります。必要であれば、ネットワークで静的 IP アドレスと動的 IP アドレスを組み合わせて使用できます。IP アドレスの静的な割り当てと動的な割り当てについて詳しくは、次のセクションをお読みください。

組織の規模が大きい場合は、DHCP サービスが提供するその他の機能（クライアントコンピュータに対する DNS および NetInfo オプションの設定など）のいくつかが役に立ちます。

クライアント用に十分な数の IP アドレスがある小規模なネットワークの場合は、DHCP サービスを使用する必要はないこともあります。すべてのネットワーククライアントに静的 IP アドレスを割り当てるときは、この章の後半で説明する方法のいずれかを使用してください。

DHCP サービスを設定する前に

DHCP サービスを設定する前に、このセクションで、サブネットの作成、静的および動的 IP アドレスの割り当て、ネットワーク上でのサーバの配置、および予約済み IP アドレスの無効化に関する情報を読んでください。

サブネットを作成する

サブネットは、同じネットワーク上にあるクライアントコンピュータをグループ化したもので、これにより管理が簡単になります。自分の目的に合うサブネットを構成できます。たとえば、組織内のグループ別にサブネットを作成したり、建物のフロア別に作成したりすることができます。クライアントコンピュータをサブネットにグループ化した後は、サブネット内のすべてのコンピュータに対して一度にオプションを設定することができます。クライアントコンピュータに個別にオプションを設定する必要はありません。

IP アドレスを動的に割り当てる

動的に割り当てた場合、IP アドレスは期間限定（リース期間）で割り当てられるか、またはクライアントコンピュータで IP アドレスが不要になるまで割り当てられます。どちらか最初に該当した方が適用されます。非常に短いリース期間を使用すると、DHCP は、利用可能な IP アドレスよりもコンピュータの数が多いネットワークを動的に再設定できます。

静的 IP アドレスを使用する

静的 IP アドレスは、一度だけコンピュータやデバイスに割り当てられ、変更されません。Web サーバなど、インターネット上に常駐する必要のあるコンピュータに静的 IP アドレスを割り当てることがあります。プリンタなど、継続的にネットワークユーザが使用できるようにする必要のあるその他の装置にも、静的 IP アドレスを使用するとよいでしょう。

「Server Admin」では、静的 IP アドレスを割り当てるために BootP プロトコル（DHCP の基盤となるプロトコル）を使って bootp デーモンを設定する方法を提供していません。これを行うには、「Mac OS X」で「NetInfo Manager」アプリケーションを使って、ローカル NetInfo データベースに適切なプロパティを作成します。

DHCP サーバを探す

クライアントコンピュータは、DHCP サーバを探す場合、メッセージをブロードキャストします。DHCP サーバがクライアントコンピュータとは異なるサブネット上にある場合は、サブネット間を接続するルータがクライアントのブロードキャストと DHCP サーバの応答を転送できることを確認する必要があります。ネットワークに BootP 通信をリレーできるリレーエージェントプログラムがある場合は、そのプログラムが DHCP を補助します。リレープログラムがない場合は、DHCP サーバをクライアントと同じサブネットに配置する必要があります。

予約済み IP アドレスを割り当てる

IP アドレスの中には、個々のホストに割り当てることができないものがあります。これらには、ループバック用の予約済みアドレスと、マルチキャストで使用するための予約済みアドレスがあります。ISP は、このようなアドレスをユーザに割り当てません。DHCP をこのようなアドレスを使うように設定しようとすると、アドレスが無効なので有効なアドレスを入力する必要があるという警告が出されます。

DHCP サービスを初めて設定する

「Mac OS X Server」をインストールしたときに「設定アシスタント」を使ってサーバ上のポートを設定した場合は、いくつかの DHCP 情報がすでに設定されています。DHCP サービスの設定を完了するためには、このセクションの手順に従って操作する必要があります。各手順の設定の選択については、次のセクション「DHCP サービスの設定」を参照してください。

手順 1：サブネットを作成する

「Server Admin」の「ネットワーク」タブをクリックしてから「DHCP/NetBoot」をクリックし、「DHCP を設定」を選びます。「設定アシスタント」でポートを設定すると、「サブネット」パネルにポート情報が表示されます。（表示されるサブネットアドレス範囲のリストは、ホストのローカル NetInfo データベースから抽出したものです。最初は、利用可能な Ethernet ポートのそれぞれに対して、1 つのサブネットアドレス範囲が設定されています。）

「新規」ボタンをクリックして新しいサブネットを作成するか、または既存のサブネットを選んで「編集」をクリックします。

サブネットの設定ウインドウの「一般」パネルで、各サブネットに対して IP アドレスの範囲を設定し、ルータアドレスを指定する必要があります。ネットワーク上でルータを使用しない場合は、「ルータ」フィールドにサーバの IP アドレスを入力します。「DHCP を使用する」をクリックすると、IP アドレスのリース期間を選択できます。

「DNS」および「NetInfo」タブをクリックして、クライアントコンピュータのオプションを設定します。サーバのデフォルト設定がある場合は、各パネルにすでに表示されています。これらのパネルでオプションを設定することによって、DHCP サービスの開始時にクライアントコンピュータの起動ポイントが提供されます。

手順 2：DHCP サービスのログを設定する

DHCP の状況とエラーをログに記録しておくと、要求を監視したり、サーバの問題を確認したりするのに役立てることができます。

DHCP サービスはシステムログファイルに診断メッセージを記録します。ログファイルが過度に大きくなるのを防止するときは、「DHCP を設定」ウインドウの「ログ」パネルで「重大なエラーのみ（簡易）」を選択することで、ほとんどのメッセージの記録を抑制できます。

手順 3：DHCP サービスを開始する

「DHCP/NetBoot」をクリックして、「DHCP を開始」を選びます。サーバが正常に起動すると、メニュー項目が「DHCP を停止」に変わり、「DHCP/NetBoot」アイコンに地球のマークが表示されます。

DHCP サービスの設定

「DHCP を設定」を表示するには、「Server Admin」の「ネットワーク」タブをクリックしてから「DHCP/NetBoot」をクリックし、「DHCP を設定」を選びます。「DHCP を設定」ウインドウには 2 つのパネルがあります。「サブネット」パネルと「ログ」パネルです。

ログの設定

「DHCP を設定」ウインドウの「ログ」タブをクリックして、ログの設定を表示します。

ログ：警告とエラー（通常）

データが一貫していない場合に警告されますが、DHCP サーバは動作し続けます。

ログ：重大なエラーのみ（簡易）

重大なエラーは、すぐに対応する必要がある状況（たとえば、DHCP サーバが起動できない場合）を示しています。

サブネットの設定

「DHCP を設定」ウインドウの「サブネット」タブをクリックして、サブネットの設定を表示します。

「新規」をクリックするか、リストにあるサブネットを選択し、「編集」をクリックしてサブネットの設定ウインドウを表示します。このウインドウには 3 つのパネルがあります。「一般」、「NetInfo」、および「DNS」です。次のセクションでは、これらのパネルの設定について個別に説明します。

サブネットの一般設定

サブネットの設定ウインドウの「一般」パネルでは、サブネットが使用するポートやサブネット名など、サブネットの一般的なオプションを設定できます。

サブネット名

サブネットの名前を入力します。「ドイツ研」や「5 階」など、サブネットの目的が分かりやすい名前を選びます。

ポート

ポップアップメニューからこのサブネットのポートを選びます。メニューには、サーバにインストールされているネットワークインタフェースの番号が表示されます。

開始と終了

このサブネットアドレス範囲の開始および終了 IP アドレスを入力します。新しいサブネットアドレス範囲を作成することで、このサブネットの 2 番目のブロックのアドレスを設定することができます。サブネットに複数の範囲を割り当てる場合、その範囲が重複しないようにします。

サブネットマスク

この IP アドレスの範囲のサブネットマスクを入力します。「デフォルトを使う」をクリックすると、DHCP サーバによって自動的にサブネットマスクが設定されます。

ルータ

ポートのアドレス範囲は、サーバの「ネットワーク環境設定」に定義されています。サブネットが外部との通信に別のポートを使用する場合は、ルータアドレスを入力する必要があります。

DHCP を使用する

このサブネット内のクライアントがDHCPを使ってサービスにアクセスするようにしたい場合は、「DHCP を使用する」をクリックします。クライアントコンピュータは、起動時に使用可能な IP アドレスを受信します。

リース期間

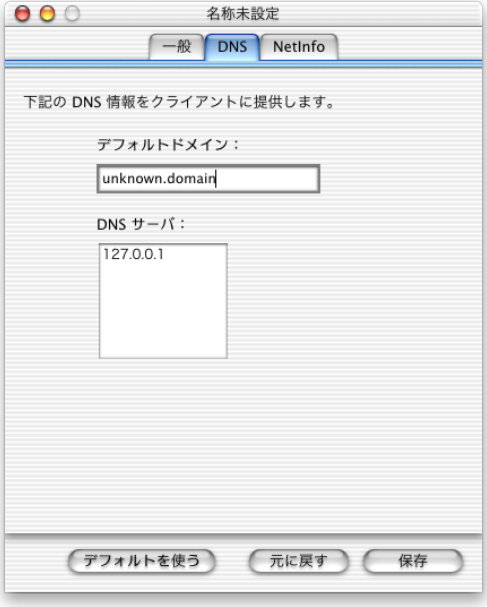
このウインドウに数字を入力し、ポップアップメニューから値を選んで、クライアントコンピュータが IP アドレスを使用できる期間を制限します。リース期間が半分経過したときに、そのアドレスがまだ使用中であれば、再度リース期間がネゴシエートされます。

デフォルトを使う

このポートのデフォルトのサブネットアドレス範囲を使用するときは、このボタンをクリックします。デフォルトの範囲には、IP アドレスとサブネットマスクに基づいた、ポートに対して有効なすべてのアドレスが含まれます。

サブネットの DNS の設定

サブネットの設定ウインドウの「DNS」パネルでは、サブネット内のクライアントコンピュータに提供する DNS 情報を指定できます。



デフォルトドメイン

このサブネットに関連付けるドメイン名を入力します。

DNS サーバ

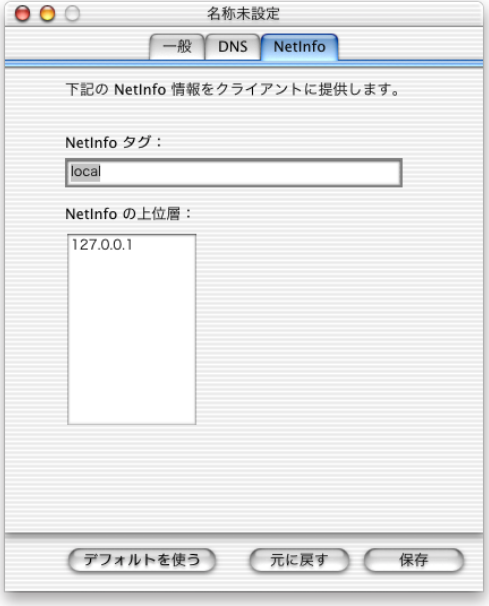
このサブネットのクライアントコンピュータに DNS 情報を提供するサーバの IP アドレスを入力します。少なくとも 2 台の DNS サーバをリストに追加して、1 台のサーバが使用不能になってもネットワークサービスに支障がないようにします。3 つまで入力できます。

デフォルトを使う

「デフォルトを使う」をクリックすると、DHCP サービスは、ドメイン名とデフォルトの DNS サーバを提供する DNS ルックアップから DNS 情報を入手します。

サブネットの NetInfo の設定

「NetInfo」パネルでは、サブネット内のクライアントコンピュータを特定の NetInfo データベースまたはドメインに「バインド」できます。NetInfo について詳しくは、第 2 章「ディレクトリサービス」を参照してください。



NetInfo タグ

このサブネットが情報を問い合わせる NetInfo ドメインの名前を入力します。この名前はテキスト文字列形式のタグで、たとえば「network」のようになります。

NetInfo の上位層

このサブネットをバインドしたいサーバごとに、IP アドレスを入力します。上位層サーバにバインドすることは、別の場所からログインしても、情報に同様にアクセスすることをクライアントユーザに許可したい場合に便利です。サブネットごとに複数の上位層をバインドできます。

デフォルトを使う

サーバのデフォルトを使うときは、このボタンをクリックします。

DHCP サービスに関する上手な使いかたとヒント

DHCP サービスには、DHCP と「NetBoot」のクライアントコンピュータを監視するための便利なツールがいくつか用意されています。DHCP と「NetBoot」のクライアントリストの表示、および DHCP エラーのシステムログの確認を行うことができます。

DHCP と NetBoot のクライアントリストを表示する

DHCP のクライアントリストと「NetBoot」のクライアントリストには、指定した時間にデータベース内のクライアントの簡易レポートが表示されます。リストは 5 分間隔で更新されますが、「リフレッシュ」をクリックして手動で更新することもできます。どちらのリストでも、列見出しをクリックして並べ替え条件を変更できます。

「DHCP クライアント」ウインドウでは、各クライアントに関する以下の情報が表示されます。

- クライアントに与えられた IP アドレス。decline されたアドレスの場合は、「残り時間」列に「declined」という文字列が表示されます。
- リース期間の残りの日数。24 時間未満になった場合は、その時間数と分数。
- DHCP クライアントの ID。通常は、ハードウェアアドレスと同じですが、異なる場合もあります。
- コンピュータ名
- ハードウェアアドレス

「NetBoot クライアント」ウインドウでは、各クライアントに関する以下の情報が表示されます。

- クライアントが使用する起動ディスクイメージへのパス
- （TCP/IP コントロールパネルからの）クライアントの Ethernet アドレス
- システムソフトウェアのバージョンと CPU の種類

DHCP のログ項目を表示する

DHCP イベントのログは、システムログに記録されます。このログを表示するときは、「Server Admin」の「一般」タブをクリックし、「ログビューア」をクリックして、「System Software」を選びます。ポップアップメニューから「System Log」を選びます。DHCP 項目の前には「bootpd」が付きます。

DNS（Domain Name System）サービス

クライアントがWebサーバやファイルサーバなどのネットワークリソースに接続したい場合に、IP アドレス（111.222.33.3 など）の代わりに、ドメイン名（www.example.com など）でリソースを要求できます。DNS は IP アドレスをドメイン名にマッピングする分散型のデータベースで、これを使用してクライアントは要求したリソースを見つけます。

DNS サーバでは、ドメイン名と、各ドメイン名に関連付けられている IP アドレスのリストを保持しています。コンピュータは、名前に対応する IP アドレスを検索する必要がある場合、DNS サーバ（ネームサーバとも呼ばれています）にメッセージを送信します。ネームサーバでは IP アドレスを探し出し、これをコンピュータに送り返します。ネームサーバがローカルに IP アドレスを所有していない場合は、インターネット上の別のネームサーバにメッセージを送信します。この処理は、IP アドレスが見つかるまで続きます。

「Mac OS X Server」は、DNS プロトコル用に BIND（Berkeley Internet Name Domain）を使用しています。BIND はオープンソースを実現しており、インターネット上の大半のネームサーバで使われています。

DNS サービスを使用する状況

お使いのネットワークの DNS サービスを処理するインターネットサービスプロバイダ（ISP）がなく、次の内容のいずれかに該当する場合は、DNS サービスを設定する必要があります。

- ネットワークにメールサーバがある。
- プライマリドメイン内にサブドメインを作成したい。

DNS サービスを設定する前に

ネットワークで DNS を使用するかどうかを検討するための情報については、このセクションをお読みください。また、自分の DNS サーバを設定する前に、DNS について理解しておいてください。DNS に関する情報源としては、Paul Albitz and Cricket Liu 著、「DNS and BIND、第 3 版」（O'Reilly and Associates, 2001）があります。

複数のネームサーバを設定する

少なくとも 1 台のプライマリネームサーバとセカンダリネームサーバを設定する必要があります。このようにしておくと、プライマリネームサーバが予期せず停止したときでも、セカンダリネームサーバがユーザにサービスを提供し続けることができます。セカンダリネームサーバは、プライマリサーバから定期的にすべての情報を移動することによって、プライマリサーバの情報を入手しています。

通常、ドメイン内の DNS サーバは、ほかのサーバの DNS 情報をキャッシュします。このことも、DNS サービスを確実に利用できるようにするのに役立ちます。DNS 情報は、通常、設定された時間だけキャッシュされます。この時間は TTL（time-to-live）値と呼ばれます。ドメイン名と IP アドレスのペアがキャッシュに保存されている時間が TTL 値を超えると、ネームサーバのキャッシュからエントリが削除されます。（プライマリ DNS サーバからは削除されません。）

DNS サービスを初めて設定する

外部 DNS ネームサーバを使用していて、その IP アドレスを「設定アシスタント」で入力したときは、ほかには何もする必要はありません。自分の DNS サーバを設定するときは、このセクションの手順に従ってください。

手順 1：ドメイン名を登録する

ドメイン名の登録は、集中管理組織（InterNIC）によって管理されています。InterNIC への登録では、ドメイン名がインターネット上で一意であることが確認されます。（詳しくは www.internic.net を参照してください。）ドメイン名を登録しないと、自分のネットワークがインターネットを介して通信することはできません。

ドメイン名を登録した後は、ネットワークにサブドメイン名と IP アドレスを追跡するための DNS サーバを設定してあれば、そのドメイン内にサブドメインを作成できます。

たとえば、アップル社は「.com」ドメインにあり、サブドメインの「corp」（corp.apple.com）および「austin」（austin.apple.com）を所有しています。アップル社の DNS サーバは、ホスト（コンピュータ）名、静的 IP アドレス、エイリアス、MX（Mail Exchanger）など、サブドメインの情報を追跡するようになっています。

手順 2：BIND を設定する

BIND は、DNS を実現するプログラムの名前です。これは、プログラムの実行中はネームデーモン、または named とも呼ばれます。BIND を設定するには、設定ファイルとゾーンファイルを変更する必要があります。

設定ファイルは次のディレクトリにあります。

/etc/named.conf

ゾーンファイルの名前はサーバの IP アドレスに基づき、「db.」で始まります。たとえば、ゾーンファイル「db.192.168.12.1」は次のディレクトリにあります。

/var/named/db.192.168.12.1

手順 3：MX（Mail Exchange）レコードを設定する（省略できます）

インターネットを介してメールサービスを提供するときは、サーバに MX レコードを設定する必要があります。これについては、次のセクションを参照してください。

手順 4：DNS サービスを開始する

DNS サービスを開始するときは、「Server Admin」の「ネットワーク」タブをクリックし、「DNS」をクリックしてから、「DNS を開始」を選びます。「DNS」アイコン上に地球が表示され、サービスの実行中は最初のメニュー項目が「DNS を停止」に変わります。

DNS サービスに関する上手な使いかたとヒント

DNS をメールサービスとともに使用する

自分のネットワークでメールサービスを提供する予定がある場合は、受信メールがネットワーク上の適切なメールホストに送信されるように DNS を設定する必要があります。メールサービスを設定するときは、「メールエクスチェンジャ」または「MX ホスト」として知られている一連のホストを、異なる優先順位にして定義します。優先順位の一番高いホストが最初にメールを受信します。このホストを利用できない場合は、優先順位が次に高いホストがメールを受信し、そのホストが利用できなければ次の優先順位のホストというように続きます。

たとえば、メールサーバのホスト名が「reliable」で、「example.com」ドメインにあるとします。MX レコードがない場合、ユーザのメールアドレスには次のように、メールサーバコンピュータの名前が含まれているはずです。

user-name@reliable.example.com

メールサーバを変更したい場合やメールをリダイレクトしたい場合は、メールを送信してくる可能性があるすべての人に、ユーザの新しいアドレスを通知する必要があります。または、メールサーバで処理したいドメインごとに MX レコードを作成すると、メールを正しいコンピュータに送信することができます。

MX レコードを設定する場合は、ドメインの中でメールを受信できる可能性があるすべてのコンピュータのリストを指定してください。これによって、サーバにアクセスが集中している状態や停止状態でも、リスト上の別のサーバにメールが送信されます。リスト上の各コンピュータには、優先順位が割り当てられます。一番小さな番号のものが、最初に試行されます。そのコンピュータを使用できない場合は、次に小さな番号を持つコンピュータが試行されます。以降についても同様です。コンピュータが使用できる場合は、そのコンピュータがメールを保管し、メインメールサーバが使用可能になった時点で、そのサーバにメールを送信します。そして、サーバがメールを配送します。サンプルのリストを以下に示します。

example.com

10 reliable.example.com
20 our-backup.example.com
30 last-resort.example.com

MX レコードは、送信メールにも使用されます。メールサーバがメールを送信する場合、MX レコードを参照し、送信先がローカルか、またはインターネット上の場所であるかを確認します。次に、同じ処理が逆の順序で行われます。送信先のメインサーバを利用できない場合、メールサーバは、メールを受信するコンピュータを見つけるまで、その送信先の MX レコードリストにあるすべてのコンピュータを試していきます。

DNS サーバに MX 情報を正しく入力しないと、メールは機能しません。MX レコードについては、この章の最後に記載されている資料を参照してください。

DNS を動的に割り当てた IP アドレスと併用する

ダイナミック DNS は、ネームサーバに編集後のリストを再ロードするように指示しなくても、IP アドレス／ドメイン名リストを変更できるメカニズムです。つまり、ネームサーバを遠隔地から更新し、DNS データを簡単に変更できます。

DHCP サービスとともにダイナミック DNS を使用することができます。DHCP は、各クライアントコンピュータの起動時に動的 IP アドレスを割り当てます。DHCP サーバは IP アドレスをランダムに割り当てるため、これらのアドレスにそのつど意味のある DNS 名を割り当てると便利です。たとえば、「Bob」が出社して自分のコンピュータを起動し、DHCP サーバが Bob のコンピュータに動的 IP アドレスを割り当てた場合、その IP アドレスに DNS エントリの「bob.example.com」が割り当てられるようにできます。コンピュータを起動するたびに Bob の IP アドレスが変更されても、Bob の DNS 名は常に同じです。これによって、ユーザは Bob の IP アドレスを知らなくても Bob のコンピュータと通信できます。

ダイナミック DNS は、モデムを使用してインターネットに接続するユーザに静的なホスト名を提供するときにも使用できます。ISP は、接続のたびにホームコンピュータに同じホスト名が割り当てられるように、ダイナミック DNS を設定できます。

DNS サービスを監視する

「Server Admin」を使用して、DNS の状態をチェックしたり、サーバ問い合わせ統計を見ることができます。

ここに示されている「DNS の統計」ウインドウには、さまざまな種類の問い合わせの統計がリストされています。「DNS の統計」ウインドウを表示するときは、「ネットワーク」タブをクリックし、「DNS」をクリックしてから、「DNS の統計」を選びます。

- NS（Name Server）：指定したゾーンの認証されたネームサーバを問い合わせます。
- A（Address）：ドメイン名に関連付けられた IP アドレスを問い合わせます。
- CName（Canonical Name）：「ニックネーム」か「エイリアス」が指定されているときに、サーバの「実際の名前」を問い合わせます。たとえば、mail.apple.com の正規の名前は MailSrv473.apple.com である可能性があります。

- PTR（Pointer）：指定した IP アドレスのドメイン名を問い合わせます（ルックアップの逆）。
- MX（Mail Exchanger）：メール用に使用するゾーン内のコンピュータを問い合わせます。
- SOA（Start Of Authority）：ほかのネームサーバと共有しているネームサーバ情報と、可能であればそのネームサーバの技術的な問い合わせ先のメールアドレスを問い合わせます。
- TXT（Text）：管理者が使用するテキストレコード。

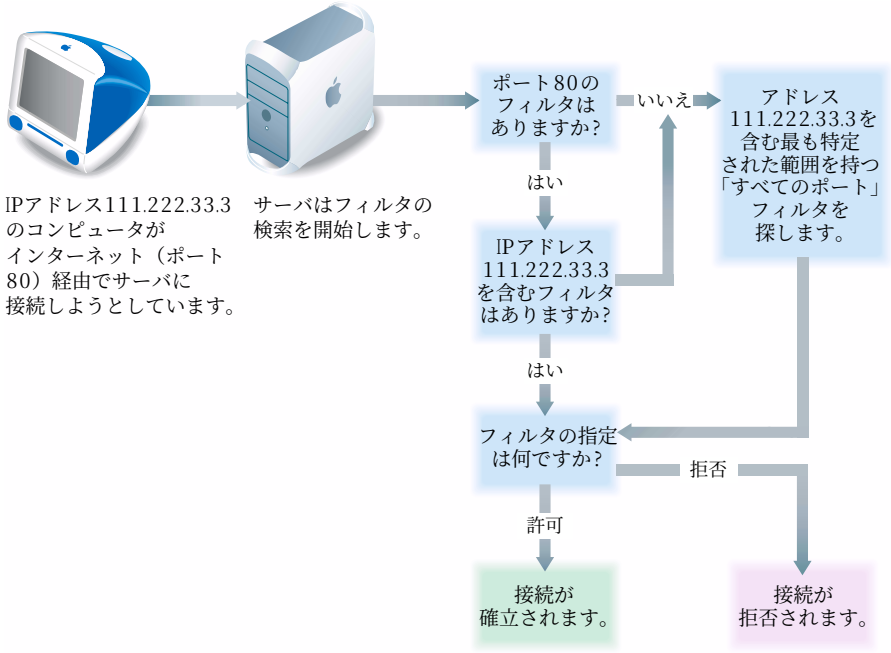
ここに示されている「DNS の状況」ウインドウを表示するときは、「ネットワーク」タブをクリックし、「DNS」をクリックしてから、「DNS の状況」を選びます。

IP フィルタサービス

IP フィルタサービスとは？

IP フィルタサービスは、「Mac OS X Server」上で実行されているネットワークアプリケーションを保護するソフトウェアファイアウォールです。IP フィルタサービスを開始することは、アクセスを制限する壁を作るようなものです。IP フィルタサービスでは、受信する IP パケットをスキャンし、作成するフィルタセットに基づいてパケットを拒否したり受け取ったりします。サーバで稼動している IP サービスへのアクセスを制限したり、すべての受信用クライアントのフィルタやクライアント IP アドレスの範囲をカスタマイズすることができます。

Web や FTP などのサービスは、サーバで TCP ポート番号または UDP ポート番号によって識別されます。コンピュータがサービスに接続しようとすると、IP フィルタサービスはフィルタリストをスキャンして一致するポート番号を探します。ポート番号がフィルタリストにあれば、適用されるフィルタは、最も特定されたアドレス範囲を含むものです。ポート番号がリストになければ、最も特定されたアドレス範囲を含む「すべてのポート」フィルタが使われます。このプロセスを説明するフローチャートを次に示します。



作成するポートフィルタは TCP パケットに適用され、UDP（User Datagram Protocol）パケットにも適用できます。また、ICMP（Internet Control Message Protocol）、IGMP（Internet Group Management Protocol）、およびNetInfoパケットを制限するフィルタも設定できます。

重要　初めて IP フィルタサービスを開始するときは、フィルタを変更してアクセスを許可しない限り、すべての受信 TCP パケットが拒否されます。デフォルトの設定では、特別に許可されていないアドレスはすべて拒否されます。つまり、サーバへのアクセスを許可したい場合はフィルタを作成する必要があります。IP フィルタサービスを停止すると、すべてのアドレスがサーバへのアクセスを許可されます。

IP フィルタサービスを使用する状況

インターネットを介してデータを共有する場合に、不正なアクセスからデータを保護する専用ルータまたはファイアウォールがないときは、IP フィルタサービスを使用する必要があります。このサービスは、小規模から中規模の企業、学校、および小さいオフィスまたはホームオフィスで効果があります。

ファイアウォールを備えた大規模な組織の場合は、IP フィルタサービスを使ってサーバをより細かく制御することができます。たとえば、大規模な企業の個々のワークグループや、学校組織の中の個々の学校の場合は、IP フィルタサービスを使ってそれぞれのサーバへのアクセスを制御することができます。

IP フィルタサービスを設定する前に

IP フィルタサービスを開始すると、デフォルトの設定により、リモートコンピュータがすべての受信パケットにアクセスできなくなります。これにより、最も高いレベルのセキュリティが提供されます。そのため、新しい IP フィルタを追加して、サービスを必要とするクライアントへのアクセスをサーバに許可します。

まず、サーバで提供したいサービスを検討します。一般に、メールサービス、Web サービス、および FTP サービスの場合は、インターネット上のコンピュータからのアクセスが必要です。ファイルサービスとプリントサービスの場合は、ローカルサブネットに制限されることがほとんどです。

IPフィルタサービスで保護したいサービスを決めたら、次のことを行う必要があります。

- サーバへのアクセスを許可したい IP アドレスを決める。
- サーバへのアクセスを拒否したい IP アドレスを決める。

次に、適切なフィルタを作成します。

IP フィルタの動作とその作成方法については、以降のセクションをお読みください。

フィルタとは？

フィルタは IP アドレスとサブネットマスクで構成されます。ポート番号とアクセスの種類が含まれる場合もあります。IP アドレスとサブネットマスクによって、フィルタが適用される IP アドレスの範囲が決まります。

IP アドレス

IP アドレスは、0 ～ 255 の範囲の値を持つ 4 つのセグメントから成り、ドット（.）で区切られています（たとえば、192.168.12.12）。IP アドレスのセグメントは、一般的なものから特定なものの順に並んでいます（たとえば、最初のセグメントは会社全体のすべてのコンピュータが所有する場合がありますが、最後のセグメントは建物のあるフロアの特定のコンピュータが所有します）。

サブネットマスク

サブネットマスクは、IP アドレスと同様に、4 つのセグメントから成ります。マスクは、指定した IP アドレスのどのセグメントが変化するか、どの範囲で変化するかを示しています。サブネットマスクセグメントでは、次の値だけを使用できます。

- 0
- 128
- 192
- 224
- 240
- 248
- 252
- 254
- 255

マスクのセグメントは一般的なものから特定のものの順に並んでいるので、0 を指定するサブネットマスクのセグメントが最初の方にあればあるほど、アドレスの範囲が大きくなります。最も範囲の狭いサブネットマスクは 255.255.255.255 で、1 つの IP アドレスを示します。

サブネットマスクのセグメントに 255 以外の値を使用した場合、その右側のセグメントには 0 を使用しなければなりません。以下に示すサブネットマスクの例は無効です。これは、それぞれ、255 以外の値の次に 0 以外の値が続いているためです。

- 255.255.128.255
- 255.0.128.128
- 255.255.252.255

アドレスの範囲を使用する

「Server Admin」を使ってフィルタを作成する場合は、IP アドレスとサブネットマスクを入力します。「Server Admin」によってその結果のアドレス範囲が表示されるので、サブネットマスクを使ってその範囲を変更できます。アドレスのセグメントの可能な値の範囲を示すとき、そのセグメントはワイルドカードと呼ばれます。下の表は、特定の目的を達成するために作成されたアドレス範囲の例です。

目的	サンプル IP アドレス	サブネットマスク	アドレスの範囲
1 つの IP アドレスを指定するフィルタを作成する	10.221.41.33	255.255.255.255	10.221.41.33（1 つのアドレス）
IP アドレスの最後のセグメントをワイルドカードにするフィルタを作成する	10.221.41.33	255.255.255.0	10.221.41.0 ～ 10.221.41.255
3 番目のセグメントの一部と 4 番目のセグメントのすべてをワイルドカードのままにしておくフィルタを作成する	10.221.41.33	255.255.252.0	10.221.40.0 ～ 10.221.43.255
すべての受信アドレスに適用するフィルタを作成する		「すべての IP アドレス」を選ぶ	すべての IP アドレス

IP アドレスの優先順位

1 つのポート番号に対して複数のフィルタを作成した場合、最も特定されたアドレス範囲を含むフィルタが優先されます。次の表は、これがどのように機能するかを示しています。最初の行の指定範囲内のアドレスから要求があった場合、アクセスは許可されます。最初の行のアドレス範囲以外のアドレスから要求があった場合は、2 番目の行がチェックされます。最後の行（「すべて」）は、アクセスを拒否します。まったく同じアドレスの範囲に対して「拒否」と「許可」の両方を設定することはできません。

ポート	IP アドレス	マスク	アクセスモード	結果
80（Web）	10.221.41.33	255.255.255.255	許可	アドレス 10.221.41.33 は許可されます。
80（Web）	10.221.41.33	255.255.252.0	許可	10.221.40.0 ～ 10.221.43.255 の範囲のアドレスは許可されます。
80（Web）		すべて	拒否	すべてのアドレスが拒否されます。

複数の IP アドレス

サーバでは複数の IP アドレスをサポートできますが、IP フィルタサービスによって 1 つのフィルタセットがすべてのサーバ IP アドレスに適用されます。複数のエイリアス IP アドレスを作成する場合は、作成するフィルタがこれらの IP アドレスのすべてに適用されます。

IP フィルタサービスを初めて設定する

作成する必要のあるフィルタを決めたら、以下の手順に従って IP フィルタサービスを設定します。これらの手順についてより詳しく知りたい場合は、IP フィルタのヘルプを参照してください。

手順 1：IP フィルタサービスを設定する

IP フィルタサービスを設定するときは、「Server Admin」の「ネットワーク」タブをクリックします。次に「IP フィルタ」をクリックし、「IP フィルタサービスを設定」を選びます。IP フィルタサービスを設定して、拒否されたパケットと許可されたパケットを記録したり、自動的に開始したり、拒否を処理する方法を指定したり、TCP ポートフィルタを UDP とほかのパケットに適用したり、NetInfo のアクセスを設定したりすることができます。

設定について詳しくは、290 ページの「IP フィルタサービスの設定」を参照してください。

手順 2：IP フィルタリストにフィルタを追加する

IP フィルタの動作とその作成方法については、286 ページの「IP フィルタサービスを設定する前に」を参照してください。

フィルタを追加するときは、「IP フィルタ」をクリックし、「IP フィルタのリストを表示」を選びます。次に「新規」をクリックして、フィルタを作成します。新しいフィルタの作成について詳しくは、295 ページの「IP フィルタウインドウの設定」を参照してください。

手順 3：IP フィルタサービスを開始する

「IP フィルタ」をクリックし、「IP フィルタサービスを開始」を選びます。

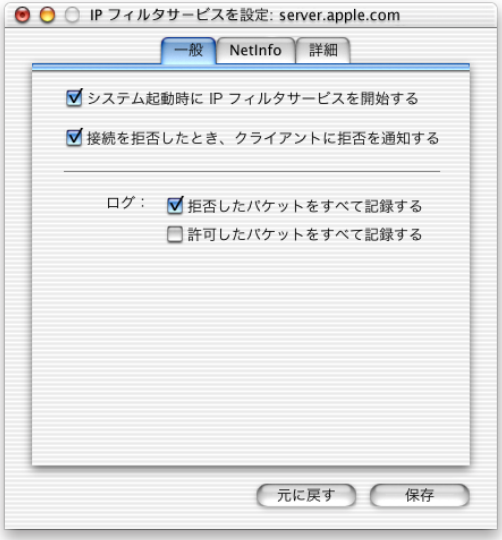
重要 IP フィルタサービスを開始してからフィルタを追加したり変更したりした場合、新しいフィルタは、サーバとの間にすでに確立している接続に影響を与えます。たとえば、IP フィルタサービスを開始した後に FTP サーバへのアクセスをすべて拒否した場合、すでに FTP サーバに接続していたコンピュータの接続は解除されます。

IP フィルタサービスの設定

「IP フィルタサービスを設定」ウインドウを使用して、一般的な設定、フィルタが NetInfo と UDP に適用される方法の設定、およびログ記録の設定を行います。IP フィルタサービスの設定にアクセスするときは、「Server Admin」の「ネットワーク」タブをクリックします。次に「IP フィルタ」をクリックし、「IP フィルタサービスを設定」を選びます。「IP フィルタサービスを設定」ウインドウには、3 つのタブがあります。「一般」、「NetInfo」、および「詳細」です。次のセクションでは、各パネルの設定内容について説明します。

一般設定

自動開始の設定、ログの設定、および拒否の処理方法の指定を行うときは、「一般」パネルを使用します。「一般」パネルを表示するときは、「IP フィルタ」をクリックし、「IP フィルタサービスを設定」を選びます。



システム起動時に IP フィルタサービスを開始する

サーバの起動時に IP フィルタサービスを自動的に開始したい場合は、このオプションを選びます。このオプションを選ぶと、電源が切れたり、予期せずシステムが終了したときでも、確実にフィルタリングを行うことができます。

接続を拒否したとき、クライアントに拒否を通知

接続試行が拒否されたクライアントに返信を送るときは、このオプションを選びます。

重要　このオプションによってクライアントの接続の再試行によるサーバのオーバーフローを防止できるため、通常は、このオプションを選択してください。ただし、悪意のあるユーザが、この返信設定を悪用して、拒否されたため返信を送ったことを示すメッセージをクライアントに送信することによって、「サービス拒否攻撃」を行う可能性があります。298 ページの「サービス拒否攻撃を防止する」を参照してください。

拒否したパケットをすべて記録する

リスト内のフィルタのいずれかによって拒否されたすべての接続試行に対してログ項目を作成するときは、このオプションを選びます。

許可したパケットをすべて記録する

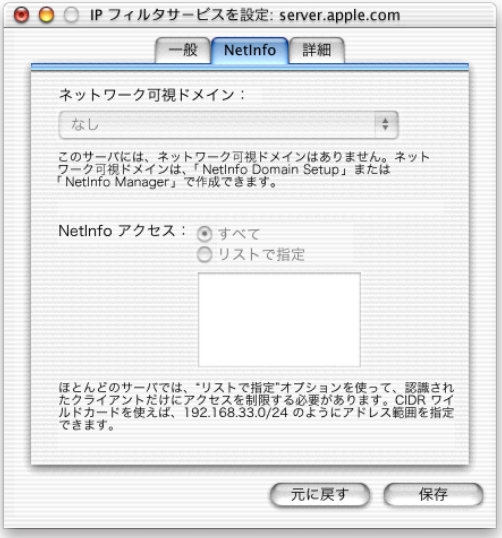
リスト内のフィルタによって許可されたすべての接続に対してログ項目を作成するときは、このオプションを選びます。

重要　上記のログ記録のオプションは両方とも多数のログ項目を生成するため、ディスクの空き領域が少なくなり、サーバの性能が低下する可能性があります。期間を制限して、「許可したパケットをすべて記録する」だけを使用することをお勧めします。

NetInfo の設定

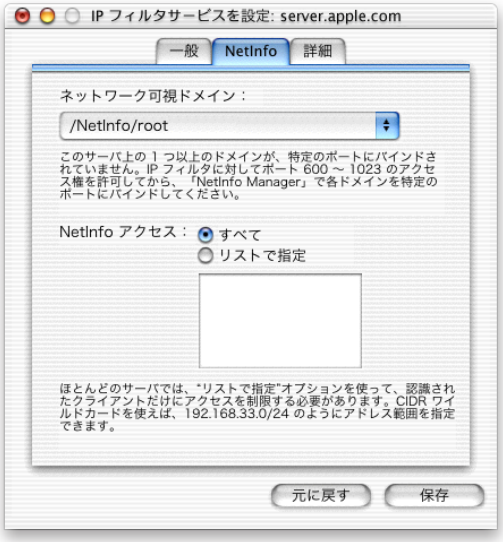
NetInfo の共有ドメインへのアクセスを許可または拒否するときは、「NetInfo」パネルを使用します。「NetInfo」パネルにアクセスするときは、「IP フィルタ」をクリックし、「IP フィルタサービスを設定」を選びます。次に、「NetInfo」タブをクリックします。

サーバ上に NetInfo の共有ドメインが存在しない場合は、「NetInfo」パネルが使用できなくなります。

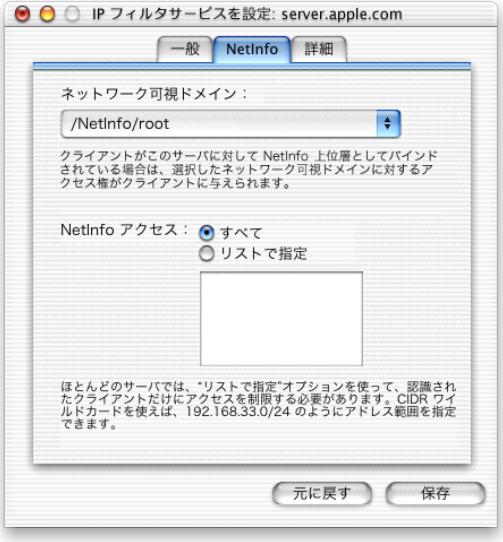


サーバ上に 1 つ以上の NetInfo 共有ドメインが存在する場合は、「ネットワーク可視ドメイン」ポップアップメニューから目的のドメインを選びます。

ドメインが特定のポートを使用するように設定されていない場合は、NetInfo は 600 ～ 1023 の範囲からポートを動的に選びます。これらのポートへのアクセスを許可する IP アドレスを指定する必要があります。



特定のポートを使用するようにドメインが設定されている場合は、このポートを使用できる IP アドレスを指定できます。特定のポートを使用するように NetInfo の共有ドメインを設定する方法については、オンスクリーンヘルプを参照してください。



すべて

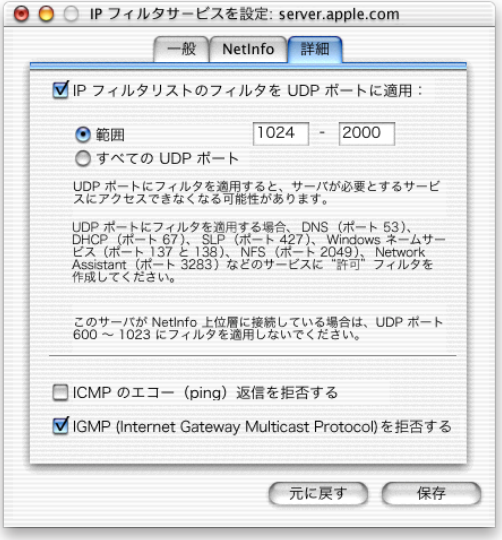
特定の NetInfo 共有ドメインへのアクセス権をすべての IP アドレスに許可するときは、このオプションを選択します。このオプションを選択するには、ファイアウォールを配置して、内部ネットワークをインターネットから保護し、NetInfo によって使用されるポート（111 および 600 ～ 1023、またはドメインに設定した特定のポート）に対する外部トラフィックを除外する必要があります。このような別のファイアウォールがない状態でこの設定を使用すると、サーバでセキュリティ上の問題が発生する可能性があります。

リストで指定

NetInfo のアクセスを持つ IP アドレスを指定するときは、このオプションを選択します。入力フィールドに IP アドレスを入力し、return キーを押してから次の IP アドレスを入力します。IP アドレスの範囲を入力するときは、IP アドレスの後ろにスラッシュ（/）を入力します。たとえば、192.168.33.3/24 は、192.168.33.0 ～ 192.168.33.255 までの範囲を意味します。

詳細な設定

「詳細」パネルでは、TCP ポートに適用するフィルタのリストを使って UDP ポートを制限します。「詳細」パネルを表示するときは、「IP フィルタ」をクリックし、「IP フィルタサービスを設定」を選びます。次に、「詳細」タブをクリックします。



IP フィルタリストのフィルタを UDP ポートに適用

UDP ポートにフィルタを適用するときは、このオプションを選び、UDP ポートの範囲を指定するか、「すべての UDP ポート」を選びます。デフォルトの設定では、すべての UDP メッセージが許可されています。フィルタを適用する UDP ポートは少なめにしてください。UDP を使って多くのサービスがサーバと通信し、「拒否」フィルタがサーバトラフィックで停滞を作ってしまうことがあります。ここで設定する前に、301 ページの「Mac OS X コンピュータが使用するポート」で UDP ポートのリストを確認してください。

また、特定のサービスに対して「許可」フィルタを作成して、ブロックされないようにする必要もあります。これらのサービスには次のものがあります。

- ポート 53 の DNS
- ポート 67 の DHCP
- ポート 427 の SLP
- ポート 137 および 138 の Windows ネームサービスの参照
- ポート 3283 の「Network Assistant」
- ポート 2049 の NFS

サービスによっては 1023 を超える UDP ポートが自動的に割り当てられるため、正確なポート番号をあらかじめ決めておくことができない場合があります。詳細については、301 ページの「Mac OS X コンピュータが使用するポート」を参照してください。

ICMP のエコー（ping）返信を拒否する

ほかのホストサーバからの「PING」に応答したくない場合は、このオプションを選びます。「PING」は、ICMP（Internet Control Message Protocol）に基づく共通ネットワーク管理ツールです。「PING」は、一連のパケットを 2 台のホスト間で往復で送信し、往復の平均時間を計測して、損失率を計算することで、ネットワークサーバが使用可能かどうかを判断します。ネットワークの「PING」に応答しないと、サービス拒否攻撃を防止できます。ただし、サーバに「PING」することに依存しているほかのサービスは、その存在を検出することができません。

IGMP（Internet Gateway Multicast Protocol）を拒否する

マルチキャストネットワークをサポートしないときは、このオプションを選択します。IGMP は、一部のホストとルータがパケットをホストのリストに送信するときに使用します。「Quick Time Streaming Server」は、SLP（Service Location Protocol）と同様にマルチキャストアドレス方式を使用します。IGMP を拒否すると、この種類のサービスが正しく実行されなくなります。

IP フィルタウインドウの設定

IP フィルタは、IP フィルタサービスの IP フィルタリストを使用して管理します。IP フィルタのウインドウを開くときは、「IP フィルタのリスト」ウインドウの下部にあるボタンのいずれかをクリックします。既存のフィルタを選択して、「編集」または「複製」ボタンをクリックすると、選択したフィルタの現在の情報が入っているウインドウが表示されます。IP フィルタリストの使用については、299 ページの「IP フィルタリストを使用する」を参照してください。

新しい IP フィルタを作成するときは、「新規」ボタンをクリックします。

アクセス

このフィルタで、指定した IP アドレスでのサーバへのアクセスを許可するか、または拒否するかを選びます。

ポート番号

ポップアップメニューからポート番号を選びます。サーバのすべてのポートに適用されるフィルタを作成したい場合は、「すべてのポート」を選びます。使用したいポートがメニューに表示されない場合は、テキストフィールドにポート番号を入力します。TCP ポートと UDP ポートの番号のリストについては、301 ページの「Mac OS X コンピュータが使用するポート」を参照してください。

ポート名

標準のポート番号以外の番号を入力した場合は、そのポートの使いかたを覚えておくために名前を入力します。

適用先

このフィルタを適用する IP アドレスを選びます。次の選択肢があります。

- すべての IP アドレス
- IP アドレスの範囲
- 1 つの IP アドレス

IP アドレス

このフィルタを適用したい IP アドレスを入力します。「すべての IP アドレス」を選んだ場合、このフィールドは使用できません。

IP アドレスを検索

フィルタを適用したい IP アドレスが分からない場合は、このボタンをクリックします。IP アドレスを検索するための DNS ホスト名を入力します。「適用」をクリックして、見つかった IP アドレスを「IP フィルタ」ウインドウの「IP アドレス」フィールドに入力します。

サブネットマスク

「IP アドレスの範囲」を選択した場合は、適用したいサブネットマスクを入力します。このフィールドの下に、アドレス範囲の検索結果が表示されます。サブネットマスクの使いかたについては、288 ページの「アドレスの範囲を使用する」を参照してください。

自分のサブネットを使用する

サーバの「ネットワーク環境設定」に保存されているサブネットマスクの値を使用するときは、このボタンをクリックします。

IP フィルタサービスに関する上手な使いかたとヒント

作成する IP フィルタは協調して動作して、ネットワークのセキュリティを提供します。以下の例は、特定の目的を達成するためのフィルタの使いかたを示しています。

インターネットユーザのアクセスをブロックする

サーバの Web サービスへのアクセスをサブネット上のユーザには許可し、インターネット上の不特定の人には拒否する場合：

アクセス	ポート	IP アドレス
許可	80（Web）	「Server Admin」で「IP アドレスの範囲」を選択し、「IP フィルタ」ウインドウの「自分のサブネットを利用する」をクリックします。
拒否	80（Web）	すべて

ジャンクメールをブロックする

IP アドレスが 17.128.100.0 のジャンクメール送信者からのメールを拒否し、その他のインターネットメールを許可するときは、次のようにします。

アクセス	ポート	IP アドレス
拒否	25（SMTP）	17.128.100.0
許可	25（SMTP）	すべて

重要　受信 SMTP メールをブロックするために作成するフィルタには、非常に特定されたアドレス範囲を設定します。たとえば、すべてのアドレスからのメールをポート 25 で拒否するフィルタを設定すると、ユーザにすべてのメールが配信されなくなります。

Apple ファイルサーバへのユーザのアクセスを許可する

IP アドレスが 10.221.41.33 のユーザに Apple ファイルサーバへのアクセスを許可するときは、次のようにします。

アクセス	ポート	IP アドレス
許可	548（AFP/TCP）	10.221.41.33
拒否	548（AFP/TCP）	すべて

ログを使用して IP フィルタサービスを監視する

IP フィルタサービスを設定するとき、拒否されたパケットおよび許可されたパケットをログに記録することを選択できます。「Server Admin」の「ログビューア」で、「Mac OS X Server」のすべてのサービスログにアクセスできます。「ログビューア」をクリックし、「System Software」を選んでから「System Log」を選んで、「ipfw」で始まる項目を探します。

「Server Admin」で作成するフィルタは、基礎となるフィルタリングソフトウェアの 1 つまたは複数のルールに相当します。適用されるルール、クライアントとサーバの IP アドレス、およびその他の情報は、ログ項目に表示されます。ルールとそれらの意味について詳しくは、306 ページの「ipfw を使って IP フィルタルールを作成する」を参照してください。

ここで、IP フィルタのログ項目の例とそれらの解釈を示します。

ログの例 1

```
Dec 12 13:08:16 ballch5 mach_kernel: ipfw: 65000 Unreach TCP
       10.221.41.33:2190 192.168.12.12:80 in via en0
```

このエントリは、IP フィルタサービスがルール 65000 を使用して、10.221.41.33:2190 上のリモートクライアントが Ethernet ポート 0 を経由する Web ポート 80 のサーバ 192.168.12.12 にアクセスすることを拒否した（未到達）ことを示しています。

ログの例 2

```
Dec 12 13:20:15 mayalu6 mach_kernel: ipfw: 100 Accept TCP
       10.221.41.33:721 192.168.12.12:515 in via en0
```

このエントリは、IP フィルタサービスがルール 100 を使用して、10.221.41.33:721 のリモートクライアントが Ethernet ポート 0 を経由する LPR プリントポート 515 のサーバ 192.168.12.12 にアクセスすることを許可したことを示しています。

ログの例 3

```
Dec 12 13:33:15 smithy2 mach_kernel: ipfw: 10 Accept TCP
       192.168.12.12:49152 192.168.12.12:660 out via lo0
```

このエントリは、IP フィルタサービスがルール 10 を使用して、ループバック装置 0 を経由するポート 660 の自分自身にパケットを送信したことを示しています。

サービス拒否攻撃を防止する

サーバは、アクセスが拒否されているクライアントから TCP 接続要求を受信した場合、デフォルトの設定では接続拒否の通知を送ります。こうすることで、拒否されたクライアントが要求を繰り返し送信することを防止できます。しかし、悪意のあるユーザが、アクセスが拒否されている IP アドレスから TCP 接続の要求を送信し続け、サーバに強制的に応答を送信させ続ける場合があります。この場合、ほかのユーザがサーバに接続しようとしても接続できなくなります。これは「サービス拒否攻撃（Dinial of Service Attacks）」の一種です。

このような攻撃を防止するためには、「IP フィルタサービスを設定」ウインドウの「一般」パネルで「接続を拒否したとき、クライアントに拒否を通知」オプションを選択しないでください。このオプションをオフにすると、クライアントが接続を再試行するため、サーバが混雑する可能性があることに注意してください。このオプションは、サーバがこの種類の攻撃を受けやすいと考える根拠がある場合にのみ選びます。

デフォルトの IP フィルタ状態を変更する

「すべてのポート」フィルタの「すべて」は、IP フィルタサービスのデフォルトのフィルタです。リストされているポートのアドレス範囲内にない、または「すべてのポート」フィルタのアドレス範囲内にない受信パケットはすべて、「すべて」の設定に従って、許可または拒否されます。

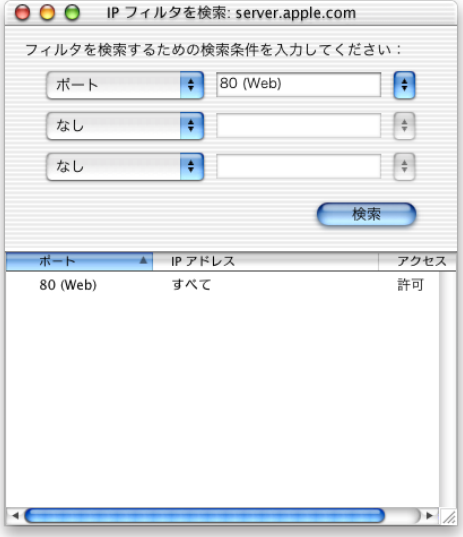
初めて IP フィルタサービスを開始するとき、デフォルトの設定により「すべてのポート」フィルタ「すべて」はアクセス拒否になっています。これにより、許可するつもりではなかったサービスにアクセスを許可してしまうという事態を防ぐことができます。必要であれば、「すべて」に設定されているアクセスを変更することができます。ただし、安易に変更しないでください。デフォルトをアクセス許可に変更すると、保護を必要とするすべてのサービスに対して非常に特殊なポートフィルタを設定して、サービスへのアクセスを明示的に拒否しなければならなくなります。

IP フィルタリストを使用する

IP フィルタリストには、サーバのすべてのフィルタが表示されます。フィルタは、番号順にリストされているポート番号ごとにグループ化されます。ポートのフィルタは、最も特定された IP アドレス範囲（または、1 つのアドレス）のフィルタから最も広いアドレス範囲（または「すべて」）のフィルタまで、優先順位順に表示されます。

295 ページで説明しているように、フィルタを選択した後、「複製」または「編集」ボタンをクリックすると、「IP フィルタ」ウインドウを開くことができます。

「検索」ボタンは、設定したフィルタに関する問題の発見とセキュリティホールのチェックに役立つ高機能なツールです。「検索」ボタンをクリックすると、「IP フィルタを検索」ウインドウが表示されます。



ポップアップメニューから使用したい検索条件を選びます。ポート、IP アドレス、およびアクセスの種類（許可または拒否）で検索できます。検索結果は、ウインドウの下部分に表示されます。

IP フィルタサービスに関する問題を解決する

TCP/IP 経由でサーバにアクセスできない場合は、以下の操作を試してください。

- フィルタリストでフィルタを確認します。IP フィルタサービスを開始していても新しいフィルタを追加していない場合、デフォルトの設定では、サーバへの TCP アクセスがすべて拒否されます。
- IP フィルタサービスを停止します。指定した IP アドレスを所有するコンピュータへのアクセスを許可する新しいフィルタを、フィルタリストに追加します。その後、IP フィルタサービスを開始します。

特定のフィルタを探すのが困難な場合は、以下の操作を試してください。

- 「IP フィルタのリスト」ウインドウの「検索」ボタンを使って、IP アドレス、ポート、またはアクセスの種類で特定のフィルタを検索します。

拒否されたパケットを表示したい場合は、以下の操作を試してください。

- 「IP フィルタサービスを設定」ウインドウで、拒否したパケットのログの記録を開始します。ログ項目を表示するときは、「Server Admin」の「一般」タブをクリックし、「ログビューア」をクリックします。「System Software」をクリックし、ポップアップメニューから「System Log」を選びます。

ネットワークサービスに関するその他の情報

RFC（Request for Comments）ドキュメントには、プロトコルやサービスの概要と、プロトコルの動作に関する詳細が記載されています。サーバの管理を始めたばかりの方にとって、RFC の背景情報は参考になることでしょう。経験豊富なサーバ管理者の場合、RFC ドキュメントによって、プロトコルに関する詳細な技術情報をすべて確認できます。RFC ドキュメントは、次の Web サイトで番号で検索することができます。www.faqs.org/rfcs

次の項目について詳しくは、記載されている RFC ドキュメントを参照してください。

- DHCP：「RFC 2131」
- ダイナミック DNS：「RFC 2136」および「RFC 2137」
- SLP DA：「RFC 2608」
- IP フィルタサービス： ICMP については「RFC 792」を参照してください。IGMP については、「RFC 1112」の「Appendix I」に記載されています。重要なマルチキャストアドレスについては、最新の「Assigned Numbers」に関する RFC（現時点では「RFC 1700」）に記載されています。

DNS および BIND の詳細については、次の書籍を参照してください。

- 「DNS and BIND」第 3 版、Paul Albitz、Cricket Liu、Mike Loukides 共著 (O'Reilly and Associates 社発行、1998)
- International Software Consortium の Web サイト（www.isc.org）

付 録 A

詳細なトピック

この付録では、経験豊富なシステム管理者やネットワーク管理者にとって役に立つ情報を記載しています。

- 「TCP/IPに関するトピック」には、Mac OS Xコンピュータが使用するTCPおよびUDPポートのリストやプライベート TCP/IP ネットワークの設定方法の説明など、さまざまな項目があります。
- 308ページの「ユーザとグループを読み込む／書き出すためのファイルフォーマット」には、ファイルにユーザとグループを記述するときに使うXML文の例があります。
- 314ページの「LDAP データの仕様」では、LDAP サーバから取り込まれるユーザおよびネットワークサービスデータの適当なフォーマットについて説明し、LDAP サーバのアクセスの設定方法を順を追って説明します。
- 328ページの「サーバ情報のバックアップを作成する」では、サーバ上の NetInfo データやサービス固有のデータのバックアップを作成する手順について説明します。

TCP/IP に関するトピック

このセクションでは、高度なTCP/IP設定を行う上で参考になる情報について説明します。

Mac OS X コンピュータが使用するポート

次の表は、Mac OS X コンピュータと「Mac OS X Server」が通常に使用する TCP ポート番号と UDP ポート番号を示します。これらのポートは、IP フィルタを設定するときに使用できます。

参考：表に記載されている RFC を確認するときは www.faqs.org/rfcs を参照してください。

TCP ポート	使用する目的	参照
7	echo	RFC 792
20	FTP データ	RFC 959
21	FTP コントロール	RFC 959

TCP ポート	使用する目的	参照
22	ssh（secure shell）	
23	Telnet	RFC 854
25	SMTP（メール）	RFC 821
53	DNS	RFC 1034
79	Finger	RFC 1288
80	HTTP（Web）	RFC 2068
88	Kerberos	RFC 1510
110	POP3（メール）	RFC 1081
111	RPC（Remote Procedure Call）	RFC 1057
113	AUTH	RFC 931
115	sftp	
119	NNTP（ニュース）	RFC 977
139	Windows ファイルおよびプリント（SMB）	RFC 100
143	IMAP（メールアクセス）	RFC 2060
389	LDAP（ディレクトリ）	RFC 2251
427	SLP（サービスの場所）	
443	SSL（HTTPS）	
514	shell	
515	LPR（プリント）	RFC 1179
532	netnews	
548	AFP（AppleShare）	
554	Real Time Streaming Protocol（QTSS）	RFC 2326
600 ～ 1023	「Mac OS X」の RPC ベースのサービス（NetInfo など）	
626	IMAP 管理（「Mac OS X」メールサービスおよび AppleShare IP 6.x メール）	
660	Server Admin	
985	NetInfo（「NetInfo Domain Setup」を使って共有ドメインを作成した場合）	

TCP ポート	使用する目的	参照
7070	Real Time Streaming Protocol（QTSS）	
8000 ～ 8999	Web サービス	
16080	パフォーマンスキャッシュを使用する Web サービス	
2236	Macintosh マネージャ	
24000 ～ 24999	パフォーマンスキャッシュを使用する Web サービス	

UDP ポート	使用する目的	参照
7	echo	
53	DNS	
67	DHCP Server（BootP）	
68	DHCP Client	
69	TFTP（Trivial File Transfer Protocol）	
111	RPC（Remote Procedure Call）	
123	Network Time Protocol	
137	WINS（Windows ネームサービス）	
138	Windows データグラムサービス	
161	SNMP（Simple Network Management Protocol）	
427	SLP（サービスの場所）	
497	Retrospect	
513	who	
514	Syslog	
554	Real Time Streaming Protocol（QTSS）	
600 ～ 1023	「Mac OS X」の RPC ベースのサービス（NetInfo など）	
985	NetInfo（「NetInfo Domain Setup」を使って共有ドメインを作成した場合）	
2049	NFS（Network File System）	
3283	Apple Network Assistant	

UDP ポート	使用する目的	参照
6970 以上	QTSS	
7070	Real-Time Streaming Protocol の代替（QTSS）	

プライベートな TCP/IP ネットワークを設定する

ローカルエリアネットワークをインターネットに接続する場合は、インターネットにとって一意な IP アドレスとその他の情報を使って、サーバとクライアントコンピュータを設定する必要があります。IP アドレスはインターネットサービスプロバイダ（ISP：Internet Service Provider）から取得します。

ローカルエリアネットワークをインターネットには接続しないが、ネットワーク上で情報を転送するプロトコルとして TCP/IP を使用したい場合は、「プライベート」な TCP/IP ネットワークを設定することができます。プライベートネットワークを設定するときは、IANA（Internet Assigned Numbers Authority）がプライベートイントラネット用に確保している IP アドレスのブロックから、IP アドレスを選びます。

- 10.0.0.0 ～ 10.255.255.255（10/8 プレフィクス）
- 172.16.0.0 ～ 172.31.255.255（172.16/12 プレフィクス）
- 192.168.0.0 ～ 192.168.255.255（192.168/16 プレフィクス）

重要　将来、インターネットに接続する可能性がある場合は、プライベートネットワークを設定するときに、インターネットレジストリに登録し、レジストリから提供される IP アドレスを使用するようにしてください。これを行わないと、ネットワーク上のすべてのコンピュータを再構築する必要が生じます。

プライベートな TCP/IP ネットワークを設定するときは、DNS サービスを提供することもできます。ローカルエリアネットワーク上に TCP/IP と DNS を設定することによって、ファイル、Web、メール、およびネットワーク上のその他のサービスに、簡単にアクセスすることができます。

ポートに複数の IP アドレスを設定する

初めてサーバを設定するときは、設定アシスタントを使って、サーバ上で利用できる Ethernet ポートごとに 1 つの IP アドレスを設定できます。

場合によっては特定のポートに複数の IP アドレスを設定したいこともあります。たとえば、サーバを使って複数の Web サイトを運営するときに、同じポートにあるさまざまなドメイン名（URL）の要求を受け入れたい場合などです。この場合は、ドメイン名ごとに 1 つの設定を持つようにポートに複数の設定を行ってから、「Server Admin」で Web モジュールを使って各サイトを特定の設定にマッピングする必要があります。

1 つのポートに複数の IP アドレスを設定するには次の手順に従ってください。

1. 「システム環境設定」を開いて、「ネットワーク」をクリックします。
2. 「設定」ポップアップメニューで「詳細」を選びます。
3. 「新規」をクリックします。
4. 新しいポート設定の名前を入力して、「ポート」ポップアップメニューから設定しているポートを選びます。「OK」をクリックします。
5. 「設定」ポップアップメニューで、今追加したポート設定を選びます。
6. 「TCP/IP」タブをクリックし、「設定」ポップアップメニューから「手入力」を選びます。新しい IP アドレスとポートに関するその他の情報を入力します。「保存」をクリックします。

ipfw を使って IP フィルタルールを作成する

「ipfw」コマンドと「Server Admin」の「IP フィルタ」モジュールを共に使用することで、次の操作を実行できます。

- 「IP フィルタ」モジュールで作成したルールを表示します。各フィルタは、1 つまたは複数のルールに相当します。
- 「IP フィルタ」モジュールでは定義できない特性のフィルタを作成します。たとえば、特定の種類の IP プロトコル固有のルールを使用できます。または、発信パケットをフィルタリングしたり、ブロックしたりすることができます。
- ルールが適用される回数をカウントします。

「ipfw」を使用する場合は、「IP フィルタ」モジュールを使って作成したルールを変更しないように注意してください。「IP フィルタ」モジュールに対する変更は、永久的ではありません。IP フィルタサービスが再起動すると、「IP フィルタ」モジュールを使って定義されたルールは再作成されます。以下は、「IP フィルタ」モジュールがルール番号を割り当てる方法をまとめたものです。

ルール番号	「IP フィルタ」モジュールの使用目的
10	ループバック
20	127.0.0.0/8 との間のすべてのパケットを破棄します（ブロードキャスト）
30	224.0.0.0/3 からのすべてのパケットを破棄します（ブロードキャスト）
40	224.0.0.0/3 への TCP パケットを破棄します（ブロードキャスト）
100 ～ 64000	ユーザ定義のポート固有のフィルタ
63200	「icmp」エコー返信のアクセスを拒否します。「IP フィルタサービスを設定」ウインドウの「詳細」パネルで「ICMP のエコー返信を拒否する」を選ぶと作成されます。
63300	「igmp」のアクセスを拒否します。「IP フィルタサービスを設定」ウインドウの「詳細」パネルで「IGMP を拒否する」を選ぶと作成されます。
63400	TCP パケットまたは UDP パケットがポート 111（NetInfo に必要です）にアクセスすることを許可します。NetInfo の共有ドメインがサーバ上に見つかったときに作成されます。
63500	ユーザ指定の TCP および UDP パケットが、NetInfo の共有ドメインに必要なポートにアクセスすることを許可します。静的なポートを使用するか、600 ～ 1023 のポートが動的に選択されるように NetInfo を設定できます。次に、「IP フィルタサービスを設定」ウインドウを使って、すべてまたは特定のクライアントがこれらのポートにアクセスするのを許可します。
64000 ～ 65000	「すべてのポート」用のユーザ定義のフィルタ

サーバで現在定義されているルールを確認するときは、「Terminal」アプリケーションを使って「ipfw show」コマンドを実行します。「show」コマンドを実行すると、情報が 4 つの列で表示されます。

列	情報
1	ルール番号。番号が小さいほど、ルールの優先順位は高くなります。
2	フィルタが定義されて以来、適用された回数。
3	フィルタが適用されたバイト数。
4	ルールの説明。

```
ipfw show

0010    260     32688   allow log ip from any to any via lo*
0020    0       0       deny log ip from 127.0.0.0/8 to any in
0020    0       0       deny log ip from any to 127.0.0.0/8 in
0030    0       0       deny log ip from 224.0.0.0/3 to any in
0040    0       0       deny log tcp from any to 224.0.0.0/3 in
00100   1       52      allow log tcp from 111.222.33.3
        to 111.222.31.3 660 in
...
```

新しいルールを作成するときは、「ipfw add」コマンドを使用します。次の例では、ルール 200 を定義しています。このルールでは、IP アドレスが 10.123.123.123 であるクライアントからの TCP パケットが、IP アドレスが 17.123.123.123 であるシステムのポート 80 にアクセスすることを禁止しています。

```
ipfw add 200 deny tcp from 10.123.123.123 to 17.123.123.123 80
```

ルールを削除するときは、「ipfw delete」コマンドを使用します。次の例では、ルール 200 を削除します。

```
ipfw delete 200
```

詳しくは、「ipfw」に関する man ページを参照してください。

TCP/IP の設定に関するその他の情報

TCP/IP プロトコルの入門書については、次の書籍を参照してください。

- 「TCP/IP Illustrated, Volume 1: The Protocols」W. Richard Stevens 著（Addison-Wesley Professional Computing Series 社発行、1994 年）

次の書籍には、TCP/IP 管理者向けのヒントとガイドラインが説明されています。

- 「TCP/IP Network Administration」第 2 版、Craig Hunt 著（O'Reilly and Associates 社発行、1997 年）

プライベートネットワークの設定についての詳細は、次の Web サイトの「RFC 1918」の情報を参照してください。

www.faqs.org/rfcs

ユーザとグループを読み込む／書き出すためのファイルフォーマット

「Server Admin」の「ユーザとグループ」モジュールを使用すると、NetInfo ドメイン内のユーザとグループをファイルに書き出し、そのファイルを使って、別のサーバ上の NetInfo ドメインに定義を読み込むことができます。ユーザとグループの情報をエンコードするときに使用されるフォーマットは XML です。

テキスト編集アプリケーションを使って、ユーザとグループの XML 定義で構成されるファイルを手動で作成することもできます。

参考：ホームディレクトリの情報は書き出されません。また、手動で XML ファイルにエンコードすることもできません。ユーザを NetInfo ドメインに読み込むと、デフォルトのホームディレクトリ設定によってホームディレクトリが設定されます。ユーザをサーバ上の NetInfo ドメインに読み込む前に、サーバ上で「Server Admin」の「ユーザとグループ」モジュールを使って、デフォルトのホームディレクトリ設定を設定してください。

このセクションでは、ユーザとグループのファイルの例を示し、ファイルをエンコードする方法について説明します。

XML ファイルの例

サンプルファイルは、3 種類の情報で構成されています。

- ヘッダ情報： ヘッダでは、ファイルの本体に含まれる要素（uglist、user、group など）を定義します。ファイルの本体に指定するユーザ情報は、グループ情報の前に指定する必要があります。サンプルファイルの中では、1 というラベルの行から 2 というラベルの行までの範囲がヘッダです。
- ユーザ情報： サンプルファイルには、「Bob Smith」と「Jane Doe」という 2 人のユーザを記述する属性が含まれています。Bob の定義はラベル 4 ～ 40 の範囲で、Jane の定義はラベル 41 ～ 42 の範囲です。
- グループ情報： サンプルファイルには、「Imported Group」という名前のグループと、「Primary」という名前のグループに関する情報が含まれています。各グループに Bob Smith と Jane Doe が属しています。最初のグループの定義はラベル 43 ～ 48 の範囲です。2 番目のグループはラベル 49 から始まり、ラベル 50 で終了します。

```
<!XML version="1.0"                                                    <--1
<!DOCTYPE MacOSXServer100 [
    <!ELEMENT uglist ( user | group ) >
    <!ELEMENT user ( nameList? pass? homeDir? pluginDataList ) >
        <!Imported Group user
            comment CDATA #IMPLIED
            uid CDATA #IMPLIED
            gid CDATA #IMPLIED
            shell CDATA #IMPLIED
            logEnabled ( canLogin | noLogin ) "canLogin"
            isAdminUser ( isAdmin | notAdmin ) "notAdmin"
        >
    <!ELEMENT nameList name >
    <!ELEMENT name EMPTY >
        <!Imported Group name
            text CDATA
        >
    <!ELEMENT pass EMPTY
        <!Imported Group pass
            format ( crypt| clearText | secure) "clearText"
            text CDATA
        >
    <!ELEMENT pluginDataList pluginData >
    <!ELEMENT pluginData EMPTY >
        <!Imported Group pluginData
            signature CDATA #REQUIRED
            data CDATA #REQUIRED
        >
    <!ELEMENT group memberName >
        <!Imported Group group
            name CDATA #REQUIRED
            gid CDATA #IMPLIED
        >
    <!ELEMENT memberName EMPTY >
        <!Imported Group memberName
            name CDATA #REQUIRED
        >
]>                                                                     <--2
```

```
<uglist>                                                    <--3
    <user                                                   <--4
        logEnabled = "canLogin"                             <--5
        isAdminUser = "notAdmin"                            <--6
        uid = "1200"                                        <--7
        gid = "0"                                           <--8
        shell = "/bin/tcsh">                                <--9
        < namelist >                                        <--10
            < name                                          <--11
                text = "bsmith" />
            < name
                text = "Bob Smith" />
        < /namelist >                                       <--12
        < pass                                              <--13
            format = "clearText"                            <--14
            text = "password" />                            <--15
        <pluginDataList>                                    <--16
            <pluginData
                signature = "Mail"
                data = "<dict>                              <--17
                    <key>kAttributeVersion</key>            <--18
                    <string>AppleMail 1.0</string>          <--19

                    <key>kMailAccountState</key>            <--20
                    <string>Enabled</string>                <--21

                    <key>kIMAPLoginState</key>              <--22
                    <string>IMAPAllowed</string>            <--23

                    <key>kPOP3LoginState</key>              <--24
                    <string>POP3Allowed</string>            <--25

                    <key>kMailAccountLocation</key>         <--26
                    <string>domain.example.com</string>     <--27

                    <key>kAutoForwardValue</key>            <--28
                    <string>user@example.com</string>       <--29

                    <key>kNotificationState</key>           <--30
                    <string>NotificationStaticIP</string>   <--31

                    <key>kNotificationStaticIPValue</key>   <--32
                    <string>[1.2.3.4]</string>              <--33

                    <key>kSeparateInboxState</key>          <--34
                    <string>OneInbox</string>               <--35
```

```
                    <key>kShowPOP3InboxInIMAP</key>                <--36
                    <string>HidePOP3Inbox</string>                 <--37

                </dict>">                                          <--38
            </pluginDataList>                                      <--39
        </user>                                                    <--40

        <user                                                      <--41
            loginEnabled = "canLogin"
            isAdminUser = "notAdmin"
            uid = "1201"
            gid = "10"
            shell = "None">
            <namelist>
                <name = "jdoe" />
                <text = "Jane Doe" />
            </namelist>
            <pass
                format = "clearText"
                text = "password2" />
        </user>                                                    <--42

        <group                                                     <--43
            name = "Imported Group"                                <--44
            gid = "2000" >                                         <--45
            <memberName                                            <--46
                name = "bsmithî />                                 <--47
            <memberName
                name = "jdoe" />
        </group>                                                   <--48

        <group                                                     <--49
            name = "Primary"
            gid = "10" >
            <memberName
                name = "bsmith" />
            <memberName
                name = "jdoe" />
        </group>                                                   <--50

    </uglist>                                                      <--51
```

ユーザとグループのファイルを自分で作成する

「Server Admin」の「ユーザとグループ」モジュールを使って読み込むことができるテキストファイルに情報を入力するときは、次のように操作します。

1. テキスト編集アプリケーションを開きます。
2. ファイルの先頭に、サンプルの1行目から2行目までのヘッダ情報で示した通り、そのまま正確に入力します。
3. 3行目の通りに情報をそのまま正確に入力します。この行は、ユーザとグループの情報が開始することを表します。
4. 4行目の通りに情報をそのまま正確に入力します。この行は、最初のユーザ定義が開始することを表します。
5. ユーザがサーバにログインできるかどうかを指定する属性を入力します。使用するフォーマットについては、5行目を参照してください。ログインを許可するときは「canLogin」、ログインを禁止するときは「noLogin」を、引用符で囲んで指定します。
6. ユーザがサーバ管理者として動作できるかどうかを指定する属性を入力します。使用するフォーマットについては、6行目を参照してください。ユーザに対して管理者権限を使用可能にするには「isAdmin」、使用禁止にするには「notAdmin」を、引用符で囲んで指定します。
7. 7行目に示されているように、ユーザIDを引用符で囲んで入力します。ユーザIDは、ユーザを一意に識別する番号です。
8. 8行目に示されているように、ユーザのプライマリグループIDを引用符で囲んで入力します。プライマリグループIDは、ファイルの後半（手順14～20）で定義されるグループを表す番号です。
9. サーバでコマンドライン操作として使用するには、デフォルトのシェルを識別します。使用するフォーマットについては、9行目を参照してください。スクリプトのパスとファイル名、または「None」（コマンドラインにアクセスしないようにする場合）を、引用符で囲んで入力します。
10. 10～12行目に示されているように、ユーザ名を入力します。引用符で囲まれている情報（割り当てる名前）以外はすべて、そのまま正確に入力します。
11. 13～15行目に示されているように、ユーザのパスワードをそのまま正確に入力します。13行目と14行目に示されているように、情報をそのまま正確に指定します。次の行では、15行目に示されているように、ユーザのパスワード文字列を引用符で囲んで指定します。
12. ユーザが「Mac OS X Server」上でメールサービスを使用しない場合は、この手順は除きます。それ以外の場合は、ユーザのメール属性を次のように入力します。
    a. 16～19行目の通りに情報をそのまま正確に入力します。
    b. ユーザのメールの処理方法（メールの状態）を定義する2行を入力します。20行目にある属性を、そのまま正確に指定します。21行目に示されているように、属性の値を指定します。メール配信を無効にするには「Off」、有効にするには「Enabled」、ユーザのメールを転送するには「Forward」の値を使用します。

c ユーザの IMAP ログイン属性を定義する 2 行を入力します。これは、ユーザが Internet Message Access Protocol を使ってメールにアクセスできるかどうかを指定するものです。22 行目にある属性を、そのまま正確に指定します。23 行目に示されているように、属性の値を指定します。IMAP を使ってメールにアクセスすることをユーザに許可するときは「IMAPAllowed」、IMAP アクセスを禁止するときは「IMAPDeny」を指定します。

d ユーザの POP3 ログイン属性を定義する 2 行を入力します。これは、ユーザが Post Office Protocol を使ってメールにアクセスできるかどうかを指定するものです。24 行目にある属性を、そのまま正確に指定します。25 行目に示されているように、属性の値を指定します。POP3 を使ってメールにアクセスすることをユーザに許可するときは「POP3Allowed」、POP3 アクセスを禁止するときは「POP3Deny」を指定します。

e ユーザのメールアカウントの位置属性を定義する 2 行を入力します。これは、ユーザのメールが保管される場所を指定するものです。26 行目にある属性を、そのまま正確に指定します。27 行目に示されているように、属性の値を指定します。ユーザのメールが保管されるサーバのドメイン名または IP アドレスを指定します。

f ユーザのメールアカウント状況に「Forward」という値を割り当てた場合は、ユーザの自動転送属性を定義する 2 行を入力します。28 行目にある属性を、そのまま正確に指定します。29 行目に示されているように、属性の値を指定します。RFC 822 の有効なメールアドレスの値を使用します。

g ユーザの通知属性を定義する 2 行を入力します。これは、新しいメールが到着したときに自動的にユーザに通知するかどうかを指定するものです。30 行目にある属性を、そのまま正確に指定します。31 行目に示されているように、属性の値を指定します。自動通知を避けるには「NotificationOff」、ユーザが最後にログインしたアドレスに通知を送るには「NotificationLastIP」、特定の IP アドレスに通知を送るには「NotificationStaticIP」の値を使用します。

h ユーザの通知属性に「NotificationStaticIP」を割り当てた場合は、通知の静的 IP アドレス属性を定義する 2 行を入力します。32 行目にある属性を、そのまま正確に指定します。33 行目に示されているように、IP アドレスを指定します。

i ユーザの個別の受付箱属性を定義する 2 行を入力します。これは、ユーザが異なる受付箱を使って POP3 メールと IMAP メールを管理するかどうかを指定するものです。34 行目にある属性を、そのまま正確に指定します。35 行目に示されているように、属性の値を指定します。異なる受付箱の使用を許可するときは、「DualInbox」を指定します。それ以外の場合は、「OneInbox」を指定します。

j IMAP 属性にユーザの表示 POP3 受付箱を定義する 2 行を入力します。これは、「POP Inbox」という IMAP フォルダが表示されるかどうかを指定するものです。36 行目にある属性を、そのまま正確に指定します。37 行目に示されているように、属性の値を指定します。このフォルダを表示するには、「ShowPOP3Inbox」を指定します。それ以外の場合は、「HidePOP3Inbox」を指定します。

k 38 ～ 40 行目をそのまま正確に入力して、ユーザ定義を終了します。

13 ファイルに追加したいユーザごとに、手順 4 ～ 12 を繰り返します。

14 43 行目の通りに情報をそのまま正確に入力します。この行は、最初のユーザ定義が開始することを表します。

15 44 行目に示されているように、グループ名を引用符で囲んで入力します。

16 45 行目に示されているように、グループ名を引用符で囲んで入力します。

17 ファイルにすでに定義したユーザの中で、グループに所属させたいユーザの名前を入力します。46 行目に示されている情報をそのまま正確に入力します。次の行では、47 行目を参考にして、ユーザのユーザ名を引用符で囲んで指定します。

18 グループに追加したいユーザごとに、手順 17 を繰り返します。

19 48 行目をそのまま正確に入力して、グループ定義を終了します。

20 ファイルに定義したいグループごとに、手順 14 ～ 19 を繰り返します。

21 ファイルの最後に 51 行目の情報をそのまま正確に入力します。この行は、ユーザ情報とグループ情報の終了を表します。

22 拡張子「xml」を指定してファイルを保存します。

23 「Server Admin」で「ユーザとグループ」モジュールを使って、ユーザとグループの定義をファイルに読み込みます。デフォルトのホームディレクトリ設定を使って、ホームディレクトリが設定されます。

XML に関するその他の情報

XML ファイルの作成と編集については、次の参考書籍を参照してください。

- 「The XML Pocket Reference」Robert Eckstein 著（O'Reilly 社発行、1999 年）
- 「Presenting XML」Richard Light 著（Sams.Net Publishing 社発行、1997 年）
- 「Learning XML」Erik Ray ／ Christopher Maoen 共著（O' Reilly 社発行、2000 年 11 月）
- 「The XML Handbook」Charles F. Goforth 著（Prentice Hall PTR 社発行、1998 年）

XML に関する書籍の総合リストについては、次の Web サイトを参照してください。

www.oasis-open.org/cover/bib-strt.html

LDAP データの仕様

このセクションでは、次の場合にサーバが LDAP サーバから取り込むことができるデータについて説明します。

- ユーザを認証する／ユーザに権限を与える
- AFP サーバやプリンタなどのネットワークサービスを検索する

「Directory Setup」アプリケーションで明示的なマッピングを行わない場合に使用される、デフォルトの LDAP データ項目名についても説明します。

「Directory Setup」アプリケーションを使って、LDAP サーバ上にあるデータを使用するように「Mac OS X Server」を設定する方法についても説明します。「Mac OS X Server」がアクセスするすべての LDAP サーバが、必要なデータをこのセクションで説明しているフォーマットで提供する必要があります。

ユーザデータをマッピングする

次の表は、「Mac OS X Server」がユーザに関するデータを使用する方法を示します。サーバが LDAP サーバから取得するデータ項目を判断してください。一番左の列の「全サービス」には、AFP、SMB、FTP、HTTP、NFS、WebDAV、POP、IMAP、「Server Admin」、「Mac OS X」ログインウインドウ、および「Macintosh マネージャ」が含まれることに注意してください。

サーバコンポーネント	使用されるデータ項目	依存性
全サービス	RecordName	認証の際に必要です。
全サービス	RealName	認証の際に必要です。
全サービス	Password	認証の際に必要です。 LDAP サーバに暗号式のパスワードが含まれている場合は、これが取得され、認証用に使用されます。それ以外の場合は、LDAP サーバが LDAP BIND コマンドを使ってパスワードを検証します。
全サービス	UniqueID	権限を付与するときに必要です（ファイルのアクセス権やメールアカウントなど）。
全サービス	PrimaryGroupID	省略できますが、指定することをお勧めします。権限を付与するときに使用します（ファイルのアクセス権やメールアカウントなど）。
■ FTP サービス ■ Web サービス ■ Apple ファイルサービス ■ NFS サービス ■ Macintosh マネージャ ■ Mac OS X ログインウインドウ ■ アプリケーションおよびシステム環境設定	HomeDirectory	省略できます。
メールサービス	MailAttribute	サーバ上のメールサービスにログインするときに必要です。
メールサービス	EMailAddress	省略できます。

「Directory Setup」を使って、サーバが LDAP サーバにアクセスするように設定する場合は、「レコード」パネルを使って、「Users」というレコードタイプを、目的のユーザデータ項目を提供する LDAP サーバ上の 1 つまたは複数の検索基準にマッピングします。次に、「データ」パネルを使って、各項目を、その値を提供する 1 つまたは複数の LDAP フィールドにマッピングします。サーバが必要とする各ユーザデータ項目が、次の表に示すフォーマットで、LDAP サーバ上に指定されている必要があります。

データ項目	LDAP マッピング フォーマット	値の例
RecordName： ユーザに関連付けられている名前のリスト。認証の際には、RecordName と RealName が両方とも指定されている必要があります	ASCII	Dave David Mac DMacSmith
RealName： 1 つの名前で、通常はユーザのフルネーム	ASCII	David L. MacSmith, Jr.
UniqueID： 一意なユーザ識別子	0 ～ 9 の数字で構成される符号なし 32 ビット ASCII 文字列	範囲は 100 ～ 4,294,967,295 です。 100 より小さい値はシステムアカウントで使用します。0 はシステム用に予約されています。
Password： ユーザのパスワード	UNIX crypt	
PrimaryGroupID： ユーザのプライマリグループ関係	0 ～ 9 の数字で構成される符号なし 32 ビット ASCII 文字列	範囲は 0 ～ 4,294,967,295 です。
Comment： 希望するユーザ書類	ASCII	John is in charge of product marketing.
UserShell: サーバで使用するコマンドライン操作のデフォルトのシェルの位置	パス名	/bin/tcsh /bin/sh None

データ項目	LDAP マッピングフォーマット	値の例
MailAttribute： ユーザのメールサービス設定。各フィールドについては、次の表を参照してください。	Mac OS X プロパティリスト	<dict> <key>kAttributeVersion</key> <string>Apple Mail 1.0</string> <key>kAutoForwardValue</key> <string>user@example.com</string> <key>kIMAPLoginState</key> <string>IMAPAllowed</string> <key>kMailAccountLocation</key> <string>domain.example.com</string> <key>kMailAccountState</key> <string>Enabled</string> <key>kNotificationState</key> <string>NotificationStaticIP</string> <key>kNotificationStaticIPValue</key> <string>[1.2.3.4]</string> <key>kPOP3LoginState</key> <string>POP3Allowed</string> <key>kSeparateInboxState</key> <string>OneInbox</string> <key>kShowPOP3InboxInIMAP</key> <string>HidePOP3Inbox</string> </dict>
EMailAddress： ユーザに対して MailAttribute が定義されていない場合に、メールが自動的に転送されるメールアドレス	RFC 822 の正式なメールアドレスまたは有効な「mailto:」URL	user@example.com mailto:user@example.com
HomeDirectory： AFP ベースのホームディレクトリの場所	Mac OS X プロパティリスト	<homeDir> <url>afp://server/sharepoint</url> <path>usershomedirectory</path> </homeDir> 次の例では、Tom King のホームディレクトリは K-M/Tom King です。これは共有ポイントディレクトリ「Users」の下にあります。 <homeDir> <url>afp://example.com/Users</url> <path>K-M/Tom King</path> </homeDir>

サーバが LDAP サーバから取得することが設定されている各 MailAttribute フィールドは、次の表に示すフォーマットで指定されている必要があります。フィールドの値が適切でない場合、MailAttribute は無視されます（つまり、MailAccountState が「Off」として処理されます）。

MailAttribute フィールド	LDAP マッピング フォーマット	値の例
AttributeVersion	必須の値で、「AppleMail 1.0」が設定されている必要があります。大文字と小文字は区別されません。	<key>kAttributeVersion</key> <string>AppleMail 1.0</string>
MailAccountState	ユーザのメールの状況を示す必須のキーワードです。大文字と小文字は区別されません。次のいずれかの値を設定する必要があります。「Off」、「Enabled」、または「Forward」。	<key>kMailAccountState</key> <string>Enabled</string>
POP3LoginState	ユーザが POP を介してメールにアクセスできるかどうかを示す必須のキーワードです。大文字と小文字は区別されません。次のいずれかの値を設定する必要があります。「POP3Allowed」または「POP3Deny」。	<key>kPOP3LoginState</key> <string>POP3Deny</string>
IMAPLoginState	ユーザが IMAP を介してメールにアクセスできるかどうかを示す必須のキーワードです。大文字と小文字は区別されません。次のいずれかの値を設定する必要があります。「IMAPAllowed」または「IMAPDeny」。	<key>kIMAPLoginState</key> <string>IMAPAllowed</string>
MailAccountLocation	ユーザのメールが保管される「Mac OS X Server」のドメイン名または IP アドレスを示す必須の値です。	<key>kMailAccountLocation</key> <string>domain.example.com </string>

MailAttribute フィールド	LDAP マッピング フォーマット	値の例
AutoForwardValue	MailAccountState の値が「Forward」の場合のみ必須なフィールドです。値は、RFC 822 の有効なメールアドレスでなければなりません。	<key>kAutoForwardValue</key> <string>user@example.com</string>
NotificationState	新しいメールが到着したときにユーザに通知するかどうかを示すオプションのキーワードです。指定する場合は、次のいずれかの値を設定する必要があります。「NotificationOff」、「NotificationLastIP」、または「NotificationStaticIP」。 フィールドの指定を省略すると、「NotificationOff」が指定されたものと見なされます。	<key>kNotificationState</key> <string>NotificationOff</string>
NotificationStaticIPValue	オプションの IP アドレスです。角かっこで囲み、ドットで区切った 10 進数形式で指定します（[xxx.xxx.xxx.xxx]）。 このフィールドの指定を省略すると、NotificationState は「NotificationLastIP」と解釈されます。フィールドは、NotificationState の値が「NotificationStaticIP」の場合のみ使用されます。	<key>kNotificationStaticIPValue</key> <string>[1.2.3.4]</string>

MailAttribute フィールド	LDAP マッピング フォーマット	値の例
SeparateInboxState	ユーザが異なる受付箱を使って POP メールと IMAP メールを管理するかどうかを示すオプションのキーワードです。大文字と小文字は区別されません。指定する場合は、次のいずれかの値を設定する必要があります。「OneInbox」または「DualInbox」。 値の指定を省略すると、「OneInbox」が指定されたものと見なされます。	<key>kSeparateInboxState</key> <string>OneInbox</string>
ShowPOP3InboxInIMAP	POP メッセージをユーザの IMAP フォルダリストに表示するかどうかを示すオプションのキーワードです。大文字と小文字は区別されません。指定する場合は、次のいずれかの値を設定する必要があります。「ShowPOP3Inbox」または「HidePOP3Inbox」。 フィールドの指定を省略すると、「ShowPOP3Inbox」が指定されたものと見なされます。	<key>kShowPOP3InboxInIMAP</key> <string>HidePOP3Inbox</string>

ネットワークサービスデータをマッピングする

サーバが、ファイルサーバやプリンタなどのネットワークサービスを表す LDAP データにアクセスするように設定することができます。NSL（Network Service Locator）を使用してネットワークサービスを検出する「Mac OS X」アプリケーションは、このデータを使って、ユーザがこれらのサービスを利用できるようにします。

たとえば、ユーザにアクセス権を許可したい Web サーバに関するレコードが LDAP サーバに保管されている場合、ユーザが「サーバへ接続」コマンドを選ぶと、「Finder」にこれらの Web サーバが一覧表示されます。

サーバが LDAP ネットワークサービスデータにアクセスするように設定する場合は、「Directory Setup」の「レコード」パネルを使って、レコードタイプを、ネットワークデータを提供する LDAP サーバ上の 1 つまたは複数の検索基準にマッピングします。「AFPServer」、「WebServer」、「Printers」などのレコードタイプを選ぶことができます。次に、レコードタイプごとに、「データ」パネルを使って、次の表に示されている 2 つのデータ項目を、その値を提供する1つまたは複数のLDAPフィールドにマッピングします。

データ項目	LDAP マッピングフォーマット	値の例
RecordName： レコードの名前	ASCII	Mrs. Jones' classroom
URLForNSL： サービスのネットワーク上の位置	有効な URL	afp://afp.example.org/ https://securesite.example.org

デフォルトのマッピングを使用する

LDAP サーバを設定するのが初めての場合は、デフォルトの LDAP データ項目名を利用することができます。LDAP フィールド名が次の表に示す名前と同じ場合は、「Directory Setup」の「データ」パネルを使って名前をマッピングする必要はありません。

データ項目	デフォルトの LDAP フィールド名
RecordName	cn、sn、dn
EMailAddress	mail、email
UniqueID	unixid
RealName	realname
MailAttribute	applemail
Comment	comment
Group	grouplist
Password	passwd
PrimaryGroupID	groupid
HomeDirectory	home、homeloc
URLForNSL	networklocurl
GroupMembership	userlist
RecordAlias	aliasdata
UserShell	shell

Group は任意でユーザレコードと関連付けられていて、ユーザが所属するグループをリスト表示するのに対し、GroupMembership はグループに所属するユーザをリスト表示します。

LDAP アクセスを設定する

このセクションでは、次のユーザの例のように、LDAP サーバから取り込み可能なユーザのすべてのデータに対する、LDAP アクセスの設定方法を説明します。

データ項目	LDAP フィールド名の例	LDAP 値の例
RecordName	shortname	bsmith
UniqueID	userid	1200
RealName	realname	Bob Smith
MailAttribute	applemail	<dict> <key>kAttributeVersion</key> <string>Apple Mail 1.0</string> <key>kAutoForwardValue</key> <string>user@example.com</string> <key>kIMAPLoginState</key> <string>IMAPAllowed</string> <key>kMailAccountLocation</key> <string>domain.example.com</string> <key>kMailAccountState</key> <string>Enabled</string> <key>kNotificationState</key> <string>NotificationStaticIP</string> <key>kNotificationStaticIPValue</key> <string>[1.2.3.4]</string> <key>kPOP3LoginState</key> <string>POP3Allowed</string> <key>kSeparateInboxState</key> <string>OneInbox</string> <key>kShowPOP3InboxInIMAP</key> <string>HidePOP3Inbox</string> </dict>
Comment	comment	Bob is a good resource for network administration.
Password	passwd	「パスワード」属性が削除されているかマッピングされていない場合、「Mac OS X Server」は、LDAP BIND コマンドを使ってユーザを認証しようとします。それ以外の場合は、「パスワード」フィールドには UNIX の暗号パスワードがあるはずです。サーバはこのパスワードを認証用に使用します。
PrimaryGroupID	primarygroupid	10

データ項目	LDAP フィールド名の例	LDAP 値の例
HomeDirectory	homedir	ユーザのホームディレクトリである R-S/Bob Smith は、「Users」という名前の共有ポイントディレクトリの中にあります。 <homeDir> <url>afp://example.com/Users</url> <path>R-S/Bob Smith</path> </homeDir>
UserShell	loginshell	/bin/sh

また、LDAP がグループに関する情報にアクセスするように設定する方法も説明します。

データ項目	LDAP フィールド名の例	LDAP 値の例
RecordName	gn	Primary
UniqueID	groupid	10
GroupMembership	groupmemberlist	bsmith, jdoe

LDAP データを使ってユーザに管理者の権限を割り当てることはできません。ユーザがサーバ管理アプリケーションを使用できるようにしたい場合は、「Server Admin」の「ユーザとグループ」モジュールを使用して、サーバのローカル NetInfo ドメイン内の「管理者」グループにユーザを追加します。

ユーザおよびグループ情報にアクセスするようにサーバを設定するときは、次の手順に従います。

1 LDAP サーバを設定する：

a LDAP サーバが LDAP に基づいた認証とパスワード確認をサポートするように設定します。

b 必要に応じて LDAP サーバ項目と属性を変更して、「Mac OS X Server」が必要とするデータを入力します。

2 「Mac OS X Server」が LDAP をサポートできるようにする：

a 「Directory Setup」アプリケーション（「Applications/Utilities」にあります）を開きます。

b カギをクリックして、サーバ管理者としてログインします。

c 「LDAPv2」を選んでから、「設定」をクリックします。

d 「新規」をクリックします。

3 LDAP サーバを識別する：

a 「固有名」タブをクリックします。

b 「名前」フィールドで、LDAP サーバの記述名を入力します。

c 「アドレス」フィールドで、LDAP サーバのドメイン名または IP アドレスを入力します。

4 ユーザ情報で使用する LDAP の検索基準を定義する：

a 「レコード」タブをクリックします。

b 「レコードのタイプ」リストで「Users」を選びます。次に、デフォルトの「マップ先」（ou= 人、o= 会社名）を編集して、ユーザ情報を提供する LDAP サーバ上の 1 つ以上の検索基準を指定します。

c 「レコードのタイプ」リストで「Groups」を選びます。次に、デフォルトの「マップ先」（ou= グループ、o= 会社名）を編集して、グループ情報を提供する LDAP サーバ上の 1 つ以上の検索基準を指定します。

5 ユーザデータをマッピングする：

a 「データ」タブをクリックして、「Mac OS X Server」が必要とするユーザ情報を、データを提供するための LDAP サーバフィールドにマッピングします。315 ページの「ユーザデータをマッピングする」では、LDAP サーバから返される個々のデータ項目値のフォーマットについて説明しています。

b ユーザを認識する名前（ユーザ名など）をマッピングします。「データのタイプ」列で「RecordName」を選びます。「マップ先」列で、必要に応じてデフォルトの LDAP フィールド名（cn、sn、および dn）を変更して、ユーザ名を保存する 1 つまたは複数の LDAP フィールドを識別します。

c ユーザ ID（ユーザを一意に識別する番号）をマッピングします。「データのタイプ」列で「UniqueID」を選びます。次に、必要であればデフォルトの LDAP フィールド名（unixid）を変更して、ユーザ ID を保存する LDAP フィールドを識別します。

d ユーザのフルネームをマッピングします。「データのタイプ」列で「RealName」を選びます。次に、必要であればデフォルトの LDAP フィールド名（realname）を変更して、フルネームを保存する LDAP フィールドを識別します。

e ユーザがサーバ上でメールサービスを使用する場合は、メール属性をマッピングします。「データのタイプ」列で「MailAttribute」を選びます。次に、必要に応じてデフォルトの LDAP フィールド名（applemail）を変更して、必須フォーマットでメール属性を保存する LDAP フィールドを識別します。

メール属性を持たないユーザの場合は、転送アドレスをマッピングします。「データのタイプ」列で「EMailAddress」を選びます。次に、必要に応じてデフォルトの LDAP フィールド名（mail および email）を変更して、転送アドレスを保存する LDAP フィールドを識別します。

f LDAP サーバがユーザパスワードを UNIX 暗号フォーマットで保存する場合のみ、ユーザパスワードをマッピングします。必要であればデフォルトの LDAP フィールド名（passwd）を変更して、パスワードを保存する LDAP フィールドを識別します。

g プライマリグループ ID をマッピングします。「データのタイプ」列で「PrimaryGroupID」を選びます。次に、必要に応じてデフォルトの LDAP フィールド名（groupid）を変更して、ユーザのプライマリグループのグループ ID を保存する LDAP フィールドを識別します。

h ホームディレクトリをマッピングします。「データのタイプ」列で「HomeDirectory」を選びます。次に、必要に応じてデフォルトの LDAP フィールド名（home および homeloc）を変更して、必須フォーマットでホームディレクトリ情報を保存する LDAP フィールドを識別します。

i ユーザログインシェル（サーバでコマンドライン操作として使われる、デフォルトのシェル）をマッピングします。「データのタイプ」列で「UserShell」を選びます。次に、必要であればデフォルトの LDAP フィールド名（shell）を変更して、シェルのパスおよびファイル名を保存する LDAP フィールドを識別します。コマンドライン操作を許可しない場合は「None」を入力します。

6 グループデータをマッピングする（必要な場合）：

a 「データ」パネルで、「Mac OS X Server」が必要とするグループ情報を、データの取り込みに使われる LDAP サーバフィールドにマッピングします。

b グループ名をマッピングします。「データのタイプ」列で「RecordName」を選びます。「マップ先」列で、グループ名を保存する 1 つまたは複数の LDAP フィールドを入力します。

c グループ ID（グループを一意に識別する番号）をマッピングします。「データのタイプ」列で「UniqueID」を選びます。次に、グループ ID を保存する LDAP フィールドを入力します。

d グループメンバーをマッピングします。「データのタイプ」列で「GroupMembership」を選びます。次に、必要に応じてデフォルトの LDAP フィールド名（userlist）を変更して、グループに関連付けられたユーザのリストを保存する LDAP フィールドを識別します。ユーザはそのユーザ名で識別する必要があります。

7 「Mac OS X Server」と LDAP サーバの間の接続の属性を定義する：

a 「アクセス」タブをクリックします。

b 「Mac OS X Server」が名前とパスワードを使わずに LDAP サーバと接続する場合は、「匿名アクセスを使う」を選びます。名前とパスワードを使う場合は、「以下の名前とパスワードを使う」を選び、LDAP サーバ接続を確立するときに使用されるサーバ識別名（cn＝admin、cn＝users、dc＝example、dc＝com など）とパスワードを入力します。必ず、LDAP サーバが受け入れる名前とパスワードを指定してください。

c 開始と終了のタイムアウトの秒数を入力します。これは、接続の最大持続時間を定義します。デフォルトは 120 秒です。

d 検索タイムアウトの秒数を入力します。これは、LDAP サーバ上でのデータ検索の最大所要時間を定義します。デフォルトは 120 秒です。

e 接続に使用するポートを識別します。デフォルトはポート 389 です。必ず、LDAP サーバが実際に使用する番号を指定してください。

f 「OK」をクリックします。

g 「使用可」チェックボックスにチェックマークを付けて、設定されている LDAP サーバをディレクトリサービスが使用できるようにしてから、ウインドウを閉じて「保存」をクリックします。

h 「サービス」タブで、「LDAPv2」チェックボックスにチェックマークを付け、使用可能であれば「適用」をクリックします。

8 「Mac OS X Server」で LDAP サーバに保存されているデータを使用する方法を指定する：

a サーバが設定されている NetInfo ドメインにユーザの情報が見つからないときに、常にサーバに LDAP サーバのレコードを検索させたい場合は、検索ポリシーに LDAP サーバを追加します。

「認証」タブをクリックします。「検索」ポップアップメニューから「NetInfo ネットワーク」を選んで、サーバに設定されているデフォルトの NetInfo 階層構造を表示します。階層構造に 1 つまたは複数の上位層ドメインが含まれている場合は、それらをメモします。

「検索」ポップアップメニューから「カスタムパス」を選びます。サーバのデフォルトの NetInfo 階層構造に 1 つまたは複数の上位層ドメインがある場合は、各上位層ドメインをリストに追加します。「追加」をクリックしてローカルドメインの上位層ドメインを選びます。さらに上位層ドメインがあれば、「追加」をクリックして次の上位層ドメインを選び、デフォルトの NetInfo 階層構造にあるすべてのドメインがリスト表示されるまでこれを続けます。

LDAP サーバを検索ポリシーに追加するには、「追加」をクリックし、その LDAP サーバを選んでから、「追加」をクリックします。必要であれば、その「LDAP サーバ」項目をドラッグして、デフォルトの NetInfo 階層構造の下に表示させます。リストの中で「LDAP サーバ」の上にある項目にユーザの情報がないとき、リストの中で上にあるものが、先に検索されます。「適用」をクリックします。

b NetInfo ドメインに特定のユーザの情報が見つからないときにだけ、サーバに LDAP サーバのレコードを検索させたい場合は、それらのユーザのそれぞれにエイリアスを定義します。

「Server Admin」の「一般」タブで、「U&G」をクリックし、「ユーザとグループを検索」を選びます。「検索対象」ポップアップメニューから「選択したディレクトリ」を選んで、LDAP サーバを選択します。ユーザの検索基準を設定し、次に「検索」をクリックします。「U&G」メニューから「ユーザとグループのリストを表示」を選んでから、エイリアスを追加したいドメインを選択します。「検索結果」ウインドウから「ユーザとグループのリスト」ウインドウへ、ユーザをドラッグします。

サーバ情報のバックアップを作成する

サーバに問題が発生してファイルの復元が必要になったときにデータの損失を最小限に抑えるため、定期的にサーバのシステムファイルのバックアップを作成してください。

最低でも、次の情報を含むファイルのバックアップを作成してください。

- ルートおよび管理者のユーザ ID： システムファイルは、作成された時点に存在するルートまたはシステム管理者のユーザ ID によって所有されています。システムファイルを復元する際は、元のアクセス権を保持するように、同じ ID がサーバに存在する必要があります。これらのユーザ ID を確実に再作成できるようにするには、「Server Admin」の「ユーザとグループ」モジュールを使って、サーバのユーザとグループ情報を、定期的にファイルに書き出します。
- NetInfo データ： NetInfo ドメイン関連の情報は、/var/db/netinfo/ にあるファイルに保存されています。ディレクトリ全体のバックアップを作成してください。

  Windows クライアントの「Authentication Manager」が使用可能なときは、サーバ上の各 NetInfo ドメインの暗号化パスワードを含むファイルが /var/db/netinfo/ に保存されています。NetInfo データベース名が MyDomain の場合、暗号化キーファイルは .MyDomain.tim です。
- メールデータベース： メールサービスデータベースは /Library/AppleMailServer/MacOSXMailDB にあります。このファイルのバックアップを作成してください。
- ディレクトリサービスの設定：「Directory Setup」アプリケーションを使って設定した設定は、/Library/Preferences/DirectoryService/ にあります。ディレクトリ全体のバックアップを作成してください。

付 録

B

Mac OS X Server のインフォメーションワークシート

この付録には、サーバに関する情報を記録するための用紙が含まれています。これは、サーバのインストール用 CD に同梱の折り込みカード、「Mac OS X Server をお使いになる前に」にあるワークシートと同じものです。何枚か必要な場合は、この付録のワークシートをコピーしてお使いください。

このワークシートの使用方法について詳しくは、「Mac OS X Server をお使いになる前に」を参照してください。

Mac OS X Server インフォメーションワークシート

「Mac OS X Server」の設定アシスタントでは、このワークシートに記載されている情報が必要になります。ネットワークおよび Ethernet ポートに関して不明な情報がある場合は、ネットワーク管理者またはインターネットサービスプロバイダ（ISP）に問い合わせてください。

重要

このワークシートにはセキュリティに関する重要な情報が含まれています。安全な場所に保管してください。

識別情報	
「Mac OS X Server」のシリアル番号	CD にプリントされている番号を入力します：

セキュリティ情報	
管理者（オーナー）名	半角で 99 文字以下の名前を入力します（名前にはスペースを含めることができます）：
管理者のユーザ名	半角で 8 文字以下の名前を入力します。ピリオド（.）、ハイフン（-）、またはアンダースコア（_）以外の特殊文字は使用できません：
管理者のパスワード	パスワードを入力するときに caps lock キーが押されていないことを確認します。このパスワードは、ルートユーザのパスワードとしても使用されます。ルートユーザのパスワードは、後で変更できます：

ネットワーク情報	
NetInfo のデータ共有（1 つを選びます）	☐ サーバでローカル NetInfo ドメインのみを使用します。 ☐ サーバからほかのサーバの NetInfo ドメインにアクセスします： アクセス先のサーバの静的 IP アドレスを入力します： NetInfo ドメインのファイル名（サーバタグ）を入力します。設定アシスタントを使ってドメインを設定した場合は「network」と指定します： 参考： 選ぶオプションがわからない場合は、1 つ目のオプションを選びます。NetInfo について詳しくは、「管理者ガイド」および「NetInfo 活用ガイド」を参照してください。
サーバのホスト名	文字で始まり、英数字またはアンダースコア（_）のみを含む名前を入力します：
ドメインネームサーバ（DNS）の IP アドレス	
DNS 検索ドメイン	必要に応じて、1 つまたは複数のドメイン名（「apple.com」など）を入力します。複数指定する場合はカンマで区切ります：
サーバの AppleTalk 名	半角で 31 文字以下、全角で 15 文字以下の名前を入力します：

続く

Mac OS X Server インフォメーションワークシート（続き）

お使いのサーバには、Ethernet ポートが内蔵されています。また、Ethernet カードを使って Ethernet ポートを追加している場合もあります。設定アシスタントでは、各ポートの使用方法（TCP/IP または AppleTalk、またはその両方）を指定し、ポートのアドレス情報を入力します。ただし、AppleTalk は、1 つのポートだけで使用でき、Apple ファイルサービスとプリントサービスの両方に使用できます。

TCP/IP または AppleTalk、またはその両方を選択しないと、設定アシスタントではポートを設定できません。選んだ各ポートには、アドレス情報を入力するパネルが表示されます。

ヒント

マルチポート Ethernet カードを使う場合は、ネットワークの専門家に相談してください。

設定アシスタントでは、ポートを 1 つは設定する必要があります。残りのポートは、「システム環境設定」の「ネットワーク」パネルで設定できます。

Ethernet ポートの計画

TCP/IP または AppleTalk 、またはその両方を選択します（AppleTalk は 1 つのポートでしか使用できません）。

内蔵 Ethernet ポート：	TCP/IP ☐	AppleTalk ☐		Ethernet カードポート 3：	TCP/IP ☐	AppleTalk ☐	
Ethernet カードポート 1：	TCP/IP ☐	AppleTalk ☐		Ethernet カードポート 4：	TCP/IP ☐	AppleTalk ☐	
Ethernet カードポート 2：	TCP/IP ☐	AppleTalk ☐					

IP アドレス形式（「192.168.12.12」など）で以下の情報を記入します：

内蔵 Ethernet ポート

IP アドレス： . . .

サブネットマスク： . . .

ルータアドレス： . . .

Ethernet カードポート 1

IP アドレス： . . .

サブネットマスク： . . .

ルータアドレス： . . .

Ethernet カードポート 2

IP アドレス： . . .

サブネットマスク： . . .

ルータアドレス： . . .

Ethernet カードポート 3

IP アドレス： . . .

サブネットマスク： . . .

ルータアドレス： . . .

Ethernet カードポート 4

IP アドレス： . . .

サブネットマスク： . . .

ルータアドレス： . . .

用語集

A、B

AFP（Apple Filing Protocol）Macintosh または Macintosh 互換のコンピュータが、ファイルとネットワークサービスを共有するために使用するクライアント／サーバ対応のプロトコル。AFP は、TCP/IP とその他のプロトコルを使って、ネットワーク上のコンピュータ間で通信します。

C

CGI（Common Gateway Interface）Webサイトに動的な機能を追加するスクリプトまたはプログラム。CGI は、Web サイトにサービスを提供するアプリケーションと Web サイトの間で情報を双方向に送信します。たとえば、ユーザがサイトのフォームに必要事項を記入すると、CGIはそのデータを処理するアプリケーションにメッセージを送信し、ユーザに応答を送り返すことができます。

D、E

DHCP（Dynamic Host Configuration Protocol）クライアントコンピュータに IP アドレスを割り当てるためのプロトコル。クライアントコンピュータは、起動するたびに DHCP サーバを検索し、見つかった DHCP サーバに IP アドレスを要求します。DHCP サーバでは使用可能な IP アドレスを調べ、これを「リース期間」と共にクライアントコンピュータに送信します。「リース期間」とは、クライアントコンピュータがアドレスを使用できる期間です。

DNS（Domain Name System）IPアドレスをドメイン名にマップする分散型のデータベース。DNS サーバは、名前およびそれぞれの名前に関連付けられた IP アドレスのリストを保持しています。コンピュータは、名前に対応する IP アドレスを検索する必要がある場合、DNS サーバ（ネームサーバとも呼ばれています）にメッセージを送信します。ネームサーバでは IP アドレスを探し出し、これをコンピュータに送り返します。ネームサーバがローカルに IP アドレスを所有していない場合は、インターネット上の別のネームサーバにメッセージを送信します。この処理は、IP アドレスが見つかるまで続きます。

F、G

FTP（File Transfer Protocol）コンピュータがネットワーク経由でファイルを転送する際に使用するプロトコル。FTP をサポートするオペレーティングシステムを使っている FTP クライアントは、各自のアクセス権に応じて、ファイルサーバに接続し、ファイルをダウンロードできます。ほとんどのインターネットブラウザおよび多数のフリーウェアアプリケーションを使って、FTP サーバにアクセスできます。

H

HTML（Hypertext Markup Language）World Wide Web ブラウザのページに表示されるファイルに挿入される記号やコードのセット。マークアップは、Web ブラウザに対して、Web ページの文字列や画像をユーザにどのように表示するかを指定します。

HTTP（Hypertext Transfer Protocol）World Wide Web 上でファイルを交換するときの規則のセットを定義するアプリケーションプロトコル。

I、J、K

IANA（Internet Assigned Numbers Authority）IP アドレスやプロトコルパラメータの割り当て、およびドメイン名の管理を行う組織。

ICMP（Internet Control Message Protocol）ホストサーバとゲートウェイとの間で使用される、メッセージ制御およびエラーレポートプロトコル。たとえば、インターネットソフトウェアアプリケーションの中には、これを使って 2 つのホスト間にパケットを送信し、往復にかかる時間を計測してネットワークの問題を発見するものがあります。

IGMP（Internet Group Management Protocol）参加を希望するホストのリストにホストとルータがパケットを送信する際に使用するインターネットプロトコル。これは、マルチキャストとして知られています。「Quick Time Streaming Server」は、SLP（Service Location Protocol）と同様にマルチキャストアドレス方式を使用します。

IMAP（Internet Message Access Protocol）ユーザがインターネット上のどの位置からでも自分のメールにアクセスが可能なクライアント／サーバ対応のメールプロトコル。ユーザがメールをダウンロードしても、そのメールはサーバから自動的に取り除かれません。

ISP（Internet service provider）インターネットへのアクセスを販売し、場合によってはメールサービスや電子商取引用アプリケーションのWebホストとしての機能を提供するビジネス。

L

LDAP（Lightweight Directory Access Protocol）ディレクトリサービスにアクセスするときに使用する標準規格のクライアント／サーバ対応のプロトコル。

LPR（Line Printer Remote）TCP/IP を経由してプリントするときに使用する標準規格のプロトコル。

M

MBONE（Multicast Backbone）IP マルチキャストをサポートする仮想ネットワーク。インターネットと同じ物理メディアを使用しますが、ユニキャストのデータパケットとして表示されるように、マルチキャストのデータパケットを再パッケージするように設計されています。

MIME（Multipurpose Internet Mail Extension）Web ブラウザが特定の特性を持つファイルを要求したときに、どのように動作するかを指定するためのインターネットの規格。ファイルの拡張子はファイルのタイプを表します。特定の拡張子を持つファイルをサーバが受信したときに、サーバがどのように動作するかを指定します。拡張子とそれに関連付けられた応答を、「MIME タイプマッピング」と呼びます。

MX レコード（Mail Exchange レコード）ドメインがメールを処理する方法を指定する、DNS テーブル内のエントリ。あるドメインに対してインターネット上のメールサーバがメールを配送してくる場合、メールサーバではドメインの MX レコードを要求します。そして、MX レコードに指定されているコンピュータ宛に、メールが送られます。

N

NetBIOS（Network Basic Input/Output System）異なるコンピュータ上のアプリケーションが、ローカルエリアネットワークの中で通信するときに使用するプログラム。

NFS（Network File System）遠隔地からユーザが、まるでローカルファイルであるかのようにファイルにアクセスできるようにする、TCP/IP を使ったクライアント／サーバプロトコル。NFS では、ユーザ名とパスワードではなく、IP アドレスに基づいて、コンピュータに共有ボリュームをエクスポートします。

NSL（Network Service Locator）TCP/IP ベースのネットワークリソースを簡単に検索するためのアップル社のテクノロジー。

O

ORBS（Open Relay Behaviour-modification System）DNS ルックアップを介してアクセス可能なデータベース。既知の SPAM 送信者（ジャンクメール送信者）の追跡に使用します。データベースには、第三者のリレーを許可することが知られている SMTP サーバが含まれています。ジャンクメール送信者は、これらのサーバを使ってジャンクメールを転送します。

P

POP（Post Office Protocol）メールを受信するときに使用するメールプロトコル。メールはダウンロードされ、ユーザのコンピュータに保管されます。

Q

QTSS（QuickTime Streaming Server）インターネットを経由してリアルタイムでメディアを配送するためのテクノロジー。

R

RTP（Real-Time Transport Protocol）リアルタイムデータ（音声、映像、シミュレーションデータなど）を、マルチキャストネットワークサービスまたはユニキャストネットワークサービスを介して送信するアプリケーションに適した、終端間のネットワーク転送プロトコル。

RTSP（Real Time Streaming Protocol）リアルタイムプロパティを持つデータの配送を制御するアプリケーションレベルのプロトコル。RTSP は、音声や映像などのリアルタイムデータの、制御されたオンデマンド配送を実現する、拡張可能なフレームワークを提供します。データソースには、供給されるライブデータや保存されているクリップが含まれます。このプロトコルの目的は、複数のデータ配送セッションを制御し、UDP、マルチキャスト UDP、TCP などの配送チャネルを選ぶ手段を提供し、RTP に基づく配送メカニズムを選ぶ手段を提供することです。

S

SDP（Session Description Protocol）QTSS（Quicktime Streaming Server）と共に使用されるプロトコル。SDP ファイルには、ライブストリーミングブロードキャストのフォーマット、タイミング、および著作者に関する情報が含まれます。

SLP（Service Location Protocol）DA（Directory Agent）ネットワーク上で使用可能なサービスを登録し、ユーザがこれに簡単にアクセスできるようにするためのプロトコル。ネットワークにサービスを追加すると、SLP を使ってネットワーク上にそのサービスが登録されます。SLP DA（Directory Agent）は基本となる SLP を拡張したもので、登録されているネットワークサービスに対して集中リポジトリを使用します。

SMB（Server Message Block）クライアントコンピュータがファイルやネットワークサービスにアクセスするときに使用するプロトコル。TCP/IP、インターネット、およびその他のネットワークプロトコル上で使用できます。Windows サービスでは、SMB を使って、サーバ、プリンタ、およびその他のネットワークリソースへのアクセスを提供します。

SMTP（Simple Mail Transfer Protocol）メールを送信および転送するときに使用する TCP/IP プロトコル。受信メッセージをキューに保存する能力に限界があるため、通常はメールを送信するときだけ使用され、メールを受信するときには POP または IMAP が使用されます。

SSL（Secure Sockets Layer）暗号化された認証済みの情報をインターネット上で送信するためのインターネットプロトコル。

T

TCP（Transmission Control Protocol）インターネットを経由してコンピュータ間でメッセージ単位の形式のデータを送信するときに、IP（Internet Protocol）と共に使用される方式。IP がデータの実際の配送に対処するのに対して、TCP は、データの個別の単位（パケットと呼ばれます）を追跡します。このパケットは、効率的にインターネットをルーティングするためにメッセージを分割したものです。

TTL（Time-to-Live）DNS 情報をキャッシュに保管するために指定する時間。ドメイン名と IP アドレスのペアがキャッシュに保管されている時間が TTL 値を超えると、ネームサーバのキャッシュからエントリが削除されます（ただし、プライマリ DNS サーバからは削除されません）。

U

UDP（User Datagram Protocol）IP（Internet Protocol）を使って、ネットワーク内のあるコンピュータから別のコンピュータにデータ単位（データグラムと呼ばれます）を送信する通信方法。交換するデータ単位がきわめて小さいネットワークアプリケーションの場合は、TCP ではなく UDP を使用できます。

URL（Uniform Resource Locator）インターネット上でアクセスできるファイルのアドレス。URL は、リソースにアクセスするために必要なプロトコルの名前、インターネット上の特定のコンピュータを識別するドメイン名、およびコンピュータ上でのファイル位置を表す階層で構成されます。

USB（Universal Serial Bus）安価な直接接続ケーブルを使って、コンピュータと周辺機器の間で通信するための規格。

V

VPN（Virtual Private Network）インターネットなどのパブリックネットワークでセキュリティ保護された通信を提供するための、暗号化およびほかの技術を使ったネットワーク。一般に、VPN は、専用回線を使用する実際のプライベートネットワークよりも安価ですが、両方の終端で同じ暗号化システムを使用する必要があります。暗号化は、ファイアウォールソフトウェアまたはルータによって行われます。

W

WebDAV（Web-based Distributed Authoring and Versioning）サイトが稼働中でもクライアントユーザが Web ページをチェックアウトし、変更を加え、チェックインして戻すことができるライブオーサリング環境。

WINS（Windows Internet Naming Service）Windows コンピュータが、クライアント名と IP アドレスを照合するときに使用する名前解決サービス。WINS サーバは、ローカルネットワーク上に配置することも、外部のインターネット上に配置することもできます。

X、Y、Z

XML（Extensible Markup Language）Web 上でアクセスされる書類とデータの汎用フォーマット。

索引

調べたい項目が索引にないときは、お使いのコンピュータのヘルプメニューにある、オンスクリーンヘルプをご覧ください。

調べたい項目が索引にないときは、お使いのコンピュータのヘルプメニューにある、オンスクリーンヘルプをご覧ください。

E

F

G

H

I

K

L

M

調べたい項目が索引にないときは、お使いのコンピュータのヘルプメニューにある、オンスクリーンヘルプをご覧ください。

N

O

P

Q

調べたい項目が索引にないときは、お使いのコンピュータのヘルプメニューにある、オンスクリーンヘルプをご覧ください。

R

S

T

U

V

W

調べたい項目が索引にないときは、お使いのコンピュータのヘルプメニューにある、オンスクリーンヘルプをご覧ください。

X

あ

い

え

お

調べたい項目が索引にないときは、お使いのコンピュータのヘルプメニューにある、オンスクリーンヘルプをご覧ください。

け

こ

さ

し

す

調べたい項目が索引にないときは、お使いのコンピュータのヘルプメニューにある、オンスクリーンヘルプをご覧ください。

な

に

ね

は

ひ

ふ

調べたい項目が索引にないときは、お使いのコンピュータのヘルプメニューにある、オンスクリーンヘルプをご覧ください。

へ

調べたい項目が索引にないときは、お使いのコンピュータのヘルプメニューにある、オンスクリーンヘルプをご覧ください。

も

ゆ

調べたい項目が索引にないときは、お使いのコンピュータのヘルプメニューにある、オンスクリーンヘルプをご覧ください。