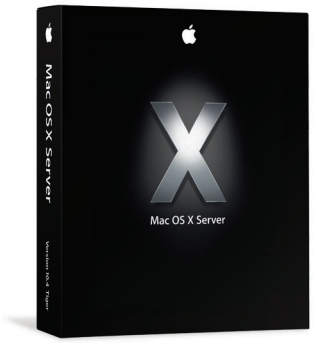



# オープンディレクトリ

アップルが提供する、標準仕様準拠のディレクトリおよびネットワーク認証サービスアーキテクチャ

## 主な機能

**スケーラブルなLDAPディレクトリサーバ**

- 集中化されたデータへの標準仕様アクセスを提供するOpenLDAP
- スケーラブルなデータストレージとハイパフォーマンスのインデックス処理を提供するBerkeley DB
- 最高のスケーラビリティと可用性を提供する、複数のサーバ間でのレプリケーション機能
- 最高20万時間のユーザレコードを誇るテスト済のスケーラビリティ

**統合された認証 オーソリティ**

- MITによるKerberos Key Distribution Center（KDC）認証サービス
- Kerberosを使用したすべてのネットワークリソースに対するセキュアなシングルサインオンをサポート
- 非Kerberosサービスに対して堅牢な認証を行なうSASL
- パスワードポリシーの管理と強制を集約

**各種混合プラットフォーム環境のサポート**

- Windows、Linuxユーザに対するログインおよび認証サービス
- クライアントプラットフォームに依存しない、ユーザ毎の単一ディレクトリレコードおよびパスワード

**システム構築と管理を容易にする専用ツール群**

- 各種サービスのリモートセットアップと管理が可能なサーバ管理ユーティリティ
- ディレクトリおよび認証データベースのバックアップとリストアが行える統合ツール
- ディレクトリレコードの作成と管理を行う革新的なワークグループマネージャユーティリティ

**既存のインフラストラクチャとも互換**

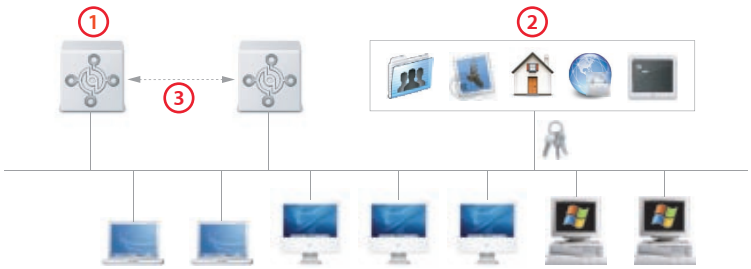
- 各種のLDAPサーバやActive Directoryとの統合も容易
- BSD設定ファイル、NIS、NetInfoなどの（以前の）ディレクトリサービスもサポートしています

Mac OS X Serverには、アップルが提供する標準仕様準拠のディレクトリおよびネットワーク認証サービスアーキテクチャ「オープンディレクトリ」が搭載されています。近代のネットワーク環境における重要なコンポーネントのひとつである「ディレクトリサービス」では、ユーザ、グループ、および組織内のコンピューティングリソースに関する情報を集中管理できます。このデータを中央のレポジトリ内に維持することで、ネットワーク上のすべてのサーバは同じユーザアカウント、設定、認証サービスにアクセスできます。ディレクトリサービスは、管理コストを抑えると同時に、ネットワーク環境のセキュリティと扱いやすさを改善します。

オープンディレクトリの採用により、Mac OS Xクライアントとサーバシステムを、既存のネットワークインフラストラクチャに容易に統合できます。標準仕様準拠のアーキテクチャは各種のLDAPサーバとの互換性や、マイクロソフト社のActive Directoryまたはノベル社のeDirectoryなどの独自サービスを採用している環境との互換性をも提供します。集中ディレクトリサービスを採用していない組織においては、Mac OS X Serverのオープンディレクトリサーバが、ほぼすべてのネットワーク環境の需要を満たす、スケーラブルで構築しやすいソリューションを提供します。

OpenLDAPやKerberosを含むパワフルなオープンソーステクノロジーと、アップルが業界をリードする管理ツール群を組み合わせることにより、オープンディレクトリは極めて簡単な設定と管理が行える強固なディレクトリおよび認証サービスを実現しました。また、ユーザ毎のライセンス料も必要ないため、オープンディレクトリではIT予算を無駄にすることもなく、あなたの組織の必要に応じたスケーラブルなシステム構築が可能です。

**オープンディレクトリの機能一覧**




1. ネットワーク環境内のグループ、コンピュータに関する情報は中央の LDAP データベースに保存されます
2. 統合された認証サービスにより、ネットワークリソースへの Kerberos を使用したセキュアなシングルサインオンが可能
3. ディレクトリと認証サービスのレプリケーションおよび自動ロードバランスにより、可用性とスケーラビリティを確保しています

**投資は無駄にしません**
オープンディレクトリアーキテクチャにより、Mac OS X Serverは既に投資したインフラを無駄にすることなく、ほぼすべての管理されたネットワーク環境でシームレスに動作します。Mac OS X Serverは内蔵されたディレクトリアクセスモジュールを使用して、マイクロソフト社独自のActive Directoryを含む任意のLDAPサーバ内のデータを読み書きできます。また、NIS、NetInfo、ローカルBSD設定ファイル(/etc)などの以前のディレクトリ内のレコードにもアクセス可能です。

## なぜ、ディレクトリサービスを採用するのか?

ユーザやネットワークリソースに関する情報を集中化することで、ディレクトリサービスはネットワーク上のユーザ、グループ、コンピュータを管理するために必要なインフラを提供します。ディレクトリサービスは10人程度の組織だけでなく、数千人のユーザを抱えるエンタープライズネットワークにも利益を与えます。ディレクトリサーバの採用することにより、管理コストを抑え、セキュリティを改善し、より生産的なコンピュータ環境をユーザに与えることが可能になります。

## オープンディレクトリサーバ

Mac OS X Serverに含まれるオープンディレクトリサーバは、高価な独自ソリューションから移行しようとしている企業や施設だけではなく、まだディレクトリサーバを採用していない組織にも最適です。オープンスタンダードに完全準拠しているオープンディレクトリは、強固なLDAPサービスおよび認証サービスを提供します。ユーザライセンス料金が不要な、アップルの革新的な管理ツール群を使用すれば、簡単かつ低コストに集中化したディレクトリおよび認証サービスを実現することが可能です。

## オープンで標準仕様準拠のソリューション

アップルは最も幅広く採用されているオープンソースLDAPサーバ「OpenLDAP」に基にして、Macおよび混合プラットフォーム環境向けのディレクトリサービスを提供するためのオープンディレクトリサーバを開発しました。LDAPはディレクトリアクセスのための標準言語を提供して、異なるプラットフォームからの情報統合と、すべてのネットワークリソースに対する単一のネームスペース定義が行えるようにします。ネットワーク上にMac、Windows、Linuxの各システムが混在する場合でも、単一のディレクトリを設定、管理することで全体を一元管理できるため、それぞれのプラットフォームに対して個別のサーバまたは個別のユーザレコードを維持する必要はありません。これにより、ユーザ環境も効率化されます。ユーザはMac OS X Serverで認証を行うことにより、どのプラットフォームからでも、単一のパスワードだけで、各種のネットワークリソースにアクセスできます。

**どうして、LDAPなのか?**
1995年に初リリースされ、IBMやSunなどの主要ベンダによって実装されたLDAPでは、すべてのネットワークリソースを単一のネームスペースで使用することにより、各プラットフォーム間での管理情報を統合することが可能です。特定のコンピュータプラットフォーム専用の独自のディレクトリサービス(UNIXシステムでのNISおよびNIS+、またはWindowsシステムでのActive Directoryなど)がそれぞれに互換性のないプロトコルでデータを定義していることに比べると、LDAPでは大きな改善が見られます。そのオープンで拡張性のある特性により、LDAPはさまざまなプラットフォームが混在するネットワーク環境におけるデータ集中化において広範囲に採用されています。

**強力なシングルサインオン認証**
オープンディレクトリサーバにはMITのKerberos Key Distribution Center(KDC)を利用した強固な認証サービスが含まれています。Kerberosは強力な認証とシングルサインオンの利便性を提供します。ユーザはユーザ名とパスワードの組み合わせを使用して認証を一度行うだけで、Kerberos対応の各種ネットワークサービスにアクセスできます。Kerberosに対応していないサービスに対しては、統合されたSASLサービスが可能な限り堅牢な認証プロトコルを自動的に選択して認証を行います。信頼性とスケーラビリティオープンディレクトリサーバにおけるディレクトリ情報の保存には、世界で最もスケーラブルなデータベースのひとつであるBerkeley DBが採用されています。数十万人分のユーザレコードも高速にインデックス処理することが可能です。オープンスタンダードのLDAPおよびKerberosテクノロジーにより、さまざまなプラットフォームや各社より提供されるサービスからのクライアントの追加も容易です。また、強固なレプリケーション機能は高い可用性とスケーラビリティを実現します。ディレクトリおよび認証サーバの複製を作成することにより、分散ネットワーク上の高速なクライアント操作に使用されるリモートサーバはもちろん、フェイルオーバー用のサーバのメンテナンスも容易に行えます。

**設定と管理が容易**
容易なディレクトリおよび認証サービスのセットアップに加え、Mac OS X Serverにはディレクトリ情報の定義や管理を容易にするパワフルな管理ツール群が付属します。革新的なワークグループマネージャアプリケーションを使用すれば、ユーザアカウントの設定やアクセス権の設定、コンピューティングリソースの管理なども簡単に行えます。ワークグループマネージャはオープンディレクトリサーバまたはその他のLDAPソリューションを使用してユーザ、グループ、コンピュータ情報の読み書きを行います。

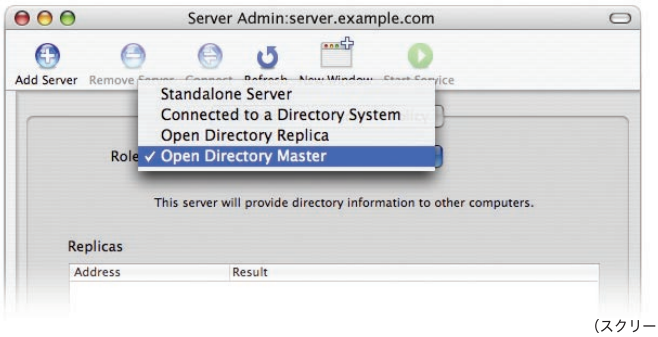
**セキュアなリモート管理**

Mac OS X Serverに添付のサーバ管理、ディレクトリアクセス、ワークグループマネージャユーティリティでは、オープンディレクトリサービスの管理に使いやすいグラフィカルインターフェイス（GUI）が用意されています。これらのアプリケーションはMac OS X v10.4が動作している任意のシステムにインストールできるため、ネットワーク上のどこからでも、あるいはインターネット経由でもサーバの管理が行えます。「ターミナル」アプリケーションを使用すれば、コマンドライン経由でのオープンディレクトリサービス管理も可能です。

## オープンディレクトリサービスの導入

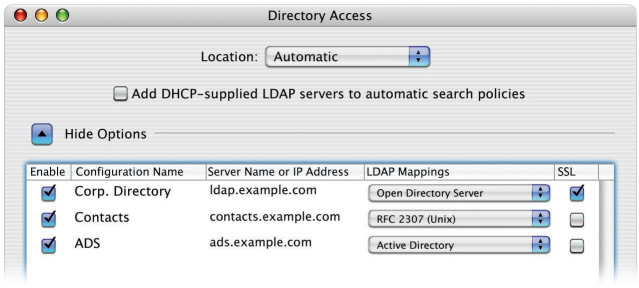
Mac OS X Serverをインストールした場合、セットアップアシスタントが設定プロセスのガイドを行います。数ステップのシンプルな設定画面で、ネットワークのディレクトリおよび認証サービスの設定が行えます。

セットアップの終了後は、サーバ管理ユーティリティを使用して、レプリケーションサービスの設定、Kerberos認証およびパスワードポリシーの管理、オープンディレクトリアクセスおよびエラーログの監視などを行えます。




（スクリーンショットは英語環境です）

必要であれば、ディレクトリアクセスアプリケーションを使用して、サーバのディレクトリ設定を詳細に行えます。例えば、複数のディレクトリドメインへの接続を設定したり、ドメイン内でのサーバの検索順を指定することが可能です。




（スクリーンショットは英語環境です）

**Windowsクライアント向けのNTドメインサービスのホスティング**

アップルはMac OS X Server上でNTドメインサービスのホスティングが行えるように、ポピュラーなオープンソース「Samba 3」プロジェクトをオープンディレクトリに統合しました。Mac OS X Serverをネットワークのプライマリドメインコントローラ（PDC）またはバックアップドメインコントローラ（BDC）に設定できるため、Windowsユーザは PCのログインウインドウを使用して直接にMac OS X Serverに対する認証を行えます。また、NTドメインサービスにより、Windowsクライアント向けのローミングプロファイルおよびネットワークホームディレクトリのホスティングがMac OS X Server上でも可能になります。ディレクトリ内の任意のユーザは、MacまたはWindowsシステムから安全にログインして、ユーザアカウント、認証、ホームディレクトリ、ネットワークリソースなどにアクセスできます。これらの機能により、Mac OS X Serverは置き換えの対象になりつつあるWindows NTやWindows 2000サーバの代替に理想的です。コストの高いActive Directoryインフラに業務を移行する必要はありません。

## SASL

オープンディレクトリサーバはSimple Authentication and Security Layer（SASL）を使用して、NTおよびLAN Manager、CRAM-MD5、APOP、Diffie-Hellman Exchange、Two-Way Random.rなどの認証プロトコルをサポートします。Kerberos非対応のサービスについては、サポートされている範囲で最も堅牢な認証方法を使用して、SASLが自動的に認証を試みます。サーバ管理を使用して、個々のプロトコルを使用または不使用に設定することも可能です。認証はユーザレベルに応じて実行されるため、サーバに接続しようとするユーザの種類に最適な認証方法を設定することが可能です。

### シングルサインオン認証の使用

シングルサインオンにはKerberos対応のネットワークサービスが必要です。ログイン、メール、FTP、SMB/CIFS、AFPファイルサービス、セキュアWebホスティング（SSL経由）、SSHなどの、Mac OS X Server v10.4が提供するほとんどのサービスはKerberos対応になっています。Kerberos非対応のサービスは、サービスのネイティブ認証プロトコルと、Kerberosサービスと同じパスワードを使用して、オープンディレクトリ認証サービス経由での認証が可能です。ただし、Kerberos非対応のサービスでは、ユーザはアクセスの度にパスワードを毎回入力する必要があります。

### 認証サービスとシングルサインオン

組織全体にわたるセキュアリソースへのシングルサインオンアクセスを提供するために、オープンディレクトリに含まれる認証サービスではMITのKerberosテクノロジーを実装しています。強力なKerberos認証を使用することで、シングルサインオンは容易な認証ユーザからのネットワークリソースへのアクセスを実現しながら、セキュリティを最大限に向上しています。

オープンディレクトリはSASLを使用した以前の認証方法もサポートしているため、ユーザは単一のパスワードだけでネットワーク上の全てのリソースを使用可能です。混合プラットフォーム環境においても、ユーザはネットワーク上の任意のシステム（Mac/Windows/Linux）から、単一のユーザ名とパスワードを使用してホームディレクトリ、グループファイルサーバ、その他のリソースにアクセスできます。ユーザ環境を簡素化できることに加え、すべてのネットワークサービスに対してユーザ毎に単一のパスワードで済むため、組織の予算も節約できます。ユーザが忘れたパスワードをリセットするためにシステム管理者やヘルプデスク担当者が消費する時間を大幅に節約でき、同時にネットワークユーザやサポート技術者の生産性を向上させます。

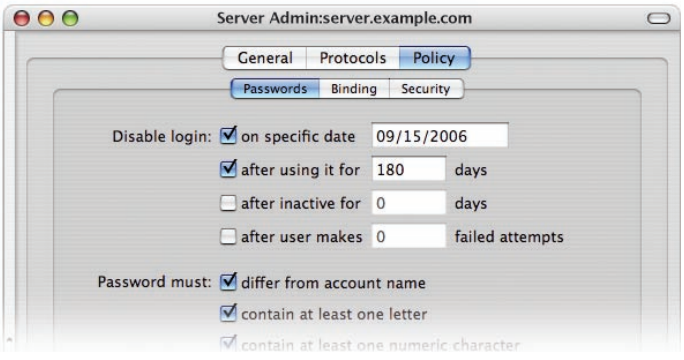
### シングルサインオンの実装

シングルサインオンにより、セキュアなネットワークリソースへのアクセスを実現できます。それぞれのサービス毎に認証を行うのではなく、ログイン時に一回のパスワード入力によってKerberos認証サービス（Key Distribution Center（KDC））に対する認証を行います。KDCはユーザに対して強固に暗号化された「チケット」を発行します。このチケットは全てのKerberos対応ネットワークサービスに対して当該ユーザが安全に認証されたことを保証するため、ユーザは以降のパスワード入力なしに、許可されたネットワークサービスにアクセスすることが可能になります。

Kerberosチケットはユーザの認証クレデンシャルの証明として扱われるため、アクセスする各サーバに対してユーザパスワードが送信されることはありません。この手法では、それぞれの認証毎にネットワーク経由でパスワードを送信する従来の認証システムよりも強固なセキュリティを実現しています。認証チケットはユーザのログアウト時またはチケットの有効期限を過ぎた時点で無効になります。

### 認証ポリシーの管理

サーバ管理を使用することにより、ネットワーク全体にわたるパスワードポリシーの設定と管理が行えます。例えば、次回のログイン時にユーザパスワード変更を強制する、特定の日付以降にユーザアカウントを無効にする、パスワードの最短文字数やその他の条件を強制する、一定期間以上にわたって未使用のアカウントを無効にするなどのことが行えます。ユーザまたはグループに特定のポリシー（ワークグループマネージャを使用して設定）は、サーバ管理を使用して設定された一般ポリシーよりも優先されます。




（スクリーンショットは英語環境です）

**LDAPスキーマのレプリケーション**
Mac OS X Server v10.4の、LDAPディレクトリは独自のカスタムスキーマの保存を行えます。また、オープンディレクトリマスターから全ての複製に対してスキーマを自動的に伝搬させることも可能です。

**オープンディレクトリのレプリケーション**
サーバ管理ではオープンディレクトリのレプリケーションサービス設定も簡単に行えます。レプリケーションにより、ディレクトリおよび認証サービスのホスティングを複数のサーバ上で行って、サービスの可用性やスケーラビリティを向上させることが可能です。それぞれのサーバはオープンディレクトリ情報のコピー（レプリカ）を持っているため、クライアントからの要求に対するサービスは各サーバから行えます。ディレクトリのレプリカはマスターディレクトリとの同期が自動的に行われるため、複数の分散ネットワーク環境にわたって一貫したユーザアカウントおよび認証情報が保証されます。

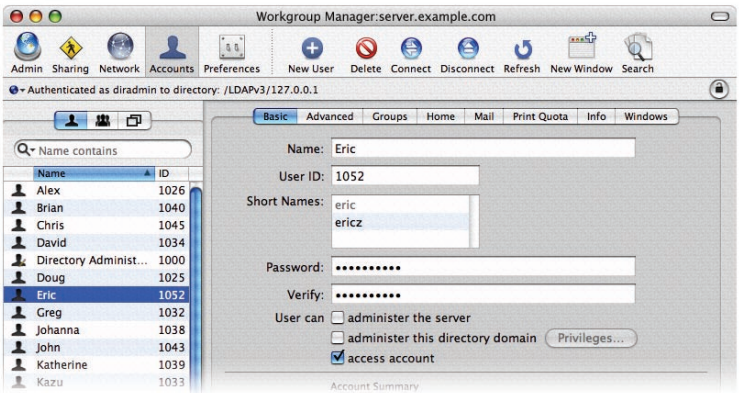

（スクリーンショットは英語環境です）

レプリケーションは高い可用性のネットワークサービスを実現するために不可欠です。冗長で地理的に分散したディレクトリを作成することにより、ハードウェアの故障や大規模な停電に見舞われた際でもディレクトリおよび認証サービスを継続して提供することが可能です。Mac OS X Serverには、レプリケートされたオープンディレクトリサーバ間の負荷を自動調整する機能が用意されています。この機能により、応答性とディレクトリサービスの可用性を最大に保ちながら、ディレクトリインフラストラクチャをスケールアウトすることが可能です。オープンディレクトリのレプリケーションを行った場合は、リモートサイト間でのネットワークトラフィックを削減できるとともに、2ヶ所間でのネットワーク接続が失われた場合においてもディレクトリレコードへの高速アクセスが保証されるため、分散ネットワーク上でのクライアント検索時間を改善できます。

## ディレクトリデータの管理

**ディレクトリサービスの自動検出**
Mac OS Xシステムでは、DHCP Option 95を使用した、ディレクトリサービスの自動検出が行えます。この機能により、DHCPサーバはクライアントへのIPアドレス割り当てと同時に、ディレクトリサーバの割り当てを行うことが可能です。Mac OS X Serverの自動設定機能ではこのテクノロジーを使用してディレクトリ内に保存された設定情報を検索するため、サーバラック全体に収められたサーバ群のセットアップも短時間で行えます。

管理されたネットワーク環境のパワフルな能力を最大限に活かすことが容易になりました。アップルの革新的なワークグループマネージャでは、LDAPディレクトリ情報管理の複雑さをあえて隠蔽して、ユーザアカウント設定、グループ設定、コンピュータ設定の管理などを行うためのシンプルなグラフィカルユーザインターフェイスが用意されています*。ワークグループマネージャでは、ネットワークリソースをディレクトリベースで管理して管理操作を簡略化できるとともに、組織全体にわたるリソースを詳細に制御できます。また、ユーザに合わせてコンピューティング環境を最適化することも可能です。




（スクリーンショットは英語環境です）

## アップルのサーバソリューション

Mac OS X Serverオペレーティングシステム。最新のオープンソーステクノロジーとMacの使いやすさを組み合わせることにより、Mac OS X Serverはアップルのラックマウント型高性能サーバハードウェア「Xserve G5」のパワーを解き放ちます。目を見張るパフォーマンスと巨大なストレージ容量、高バンド幅のI/Oシステム、統合されたリモート管理ツールなどを備えたXserve G5とMac OS X Serverはビジネス、教育機関、研究施設などに理想的なサーバソリューションです。

## さらに詳しい情報

Mac OS X Server、Xserveとその他のアップルサーバソリューションに関する詳細は、www.apple.com/jp/server/をご覧ください。

*Mac OS X v10.2以降が動作しているクライアントシステムが必要です。