Appleテクニカルホワイトペーパー

構成プロファイルを使用したOS Xの管理

OS X Mountain Lion v10.8

目次

構成プロファイルについて

概要

iOSデバイスでは、環境設定と事前構成の設定をモバイルデバイス管理（MDM）テクノロジーと構成プロファイルを使って管理します。

Appleは、OS X Lion以降、iOSで使用されている構成プロファイルとMDMテクノロジーをOS Xにも拡大しました。構成プロファイルは、管理対象の環境設定システムと同じ環境設定ポリシーを導入できるだけでなく、ディレクトリサービスのバインディング、802.1X構成、証明書配布などの、強力で新しい構成オプションを備えています。

OS X管理の変化

OS Xは、学校や企業などの組織がOS Xコンピュータを導入し、管理する数多くの新しい機会を提供します。最も重要な変化が見られるのは、管理の領域です。

構成プロファイルに対して行った変更が、Apple プッシュ通知サービス (APNs) によって、MDMサーバと管理対象のOS Xコンピュータの間で連係できるので、ポリシーの変更が即座にクライアントコンピュータに反映されます。またMDMソリューションの多くは柔軟性に富んでいて、ユーザーが自分自身でMacを管理システムに登録できます。APNsとMDMを組み合わせて使用すると、ユーザーまたは管理者が、紛失したMacをロックしたり、さらにはデータを消去したりすることができます。

Macの新規導入を計画するにあたって、重要なポリシーソリューションとなるのが構成プロファイルです。OS Xコンピュータ上で、管理対象の環境設定と構成プロファイルのポリシーと設定を混在させることはできますが、従来のMacの導入環境では構成プロファイルを使用できないので、このように変更しても意味がありません。

OS XにMDMのサポートを追加することで、AppleはすべてのAppleデバイスに対応する構成と管理の統合システムを提供できるようになりました。開発者は、それぞれのMDMソリューションにOS Xのサポートを追加することによって、ハードウェア、ソフトウェア、管理の観点からMacの管理に必要なリソースを簡素化できます。

MDMサーバと統合する際、構成プロファイルをワイヤレスでMacに配布できるので、導入を自動で管理できます。ユーザーはMDMサーバでMacを管理できるように登録するだけです。後はシステムがすべて処理します。

利点

OS Xで構成プロファイルがサポートされることで、Mac管理がシンプルになるとともに、次のような利点があります。

- **処理能力と柔軟性の向上**。プロファイルは、管理対象の環境設定よりも、Macの導入を管理するためのオプションを数多く備えています。しかも構成プロファイルがサポートされるようになっても、管理対象の環境設定は、任意のアプリケーションコントロールを含め、すべてこれまでどおり機能します。構成プロファイルとともに使用した場合も、管理対象の環境設定が持つ柔軟性はそのままで、しかも構成プロファイルが管理対象の環境設定を通じて追加の機能を提供します。たとえば、802.1Xの構成や、Mac上のキーチェーンへの証明書のインストールなどを行うことができます。

- **モバイルデバイス管理が可能。**構成プロファイルを使ったiOSの管理は、その大部分をMDMサーバ経由で行います。OS XでもMDMがサポートされるようになったので、モバイルデバイスと同様の柔軟性がMacで実現します。
- **既存のファイル形式の利用。**構成プロファイルは、Mac上では新機能ですが、iOS管理者にとっては使い慣れた機能なので、iOSの構成プロファイルの作成で培った専門知識をMacに応用することができます。
- **iOSとの共通性の確立**。構成プロファイルへの移行によって、OS XとiOSの間の共通の構成テクノロジーが確立されました。ファイル形式が2つのプラットフォームで共通な上、ポリシーキーはその多くが共有されています。

目的

多数のOS Xコンピュータを導入し管理するためのプロセスを合理化する必要がある場合、1つの強力で柔軟な方法は1つまたは複数の構成プロファイルをコンピュータにインストールすることです。構成プロファイルは、コンピュータが情報システムと連係して動作するように、すばやく設定するための設定内容のリストです。

たとえば、コンピュータがメールサーバにアクセスするように設定したり、Wi-Fiや企業内ネットワークに接続する方法を定義したりすることができます。構成プロファイルは、設定をロックするためにも使用できます。

構成プロファイルを使用して、たとえば、Eメール、スケジュール管理などのアカウント設定に加え、それらすべてのアカウントの認証情報、さらにはネットワーク設定、パスコードポリシー、デバイス制限などを設定できます。

以下に、構成プロファイルに追加できる設定のタイプの例を示します。

- パスコードとセキュリティポリシー
- Wi-Fi、VPN、および802.1Xなどのネットワーク設定
- Eメール、LDAP、スケジュール管理、インスタントメッセージ、インスタントメッセージングなどのアカウントの設定
- 資格情報とその鍵
- ログイン項目
- Dock環境設定
- Gatekeeper設定
- ペアレンタルコントロール
- 特定の環境設定ドメイン用のキー値ペアを使ったカスタム設定

使用可能なすべての構成プロファイル設定のリストについては、付録Aを参照してください。

カテゴリー

OS Xコンピュータには、次の2つのカテゴリーのプロファイルをインストールできます。

- **ユーザープロファイル。**アカウント名、パスワード、ペアレンタルコントロールなど、個別のユーザーまたはユーザグループに関する設定が含まれています。
- **デバイスプロファイル。**ディレクトリのバインディング、省エネルギー、制限など、個別のデバイスまたはデバイスグループに関する設定が含まれています。

OS Xでは、デバイスまたはデバイスグループ用に作成されたプロファイルは、システムレベルで適用されます。これに対して、ユーザーまたはユーザグループ用に作成されたプロファイルは、ユーザーレベルで適用されます。

タイプ

OS Xコンピュータにインストールできるプロファイルには、構成プロファイル、管理されたプロファイル、信頼プロファイルの3つの基本的なタイプがあります。

構成プロファイル

個々のユーザーやユーザグループ、デバイスやデバイスグループに対して、異なる設定を持つ一意の構成プロファイルを適用できます。組織は構成プロファイルを使用することにより、デバイスや、デバイスを必要とする人々向けの基本レベルの設定を、すぐに簡単に共有できます。その上で、追加の構成プロファイルを割り当てることで、設定をカスタマイズして組織の要件に対応できます。

たとえば、ある教員用のMacBook Proを構成する場合、その教員用のユーザーアカウントを作成した後、そのユーザーを「教員」グループと「MacBook Pro」グループに配置します。これにより、2セットのデフォルト設定（それぞれのグループのデフォルト設定）が割り当てられ、その後、ユーザーに応じた設定を追加してカスタマイズすることができます。

IT部門が有効に活用できるその他のタイプのユーザグループやデバイスグループとして、「実習室のコンピュータ」「営業部員用のコンピュータ」「学生用のコンピュータ」などがあります。たとえば、営業部員用のコンピュータグループの場合、制限のペイロードやVPNのペイロードを、プロファイルのデフォルト設定に含めることがあります。両方のペイロードが同じプロファイルに含まれているため、ユーザーは両方をインストールする必要があります。ユーザーが制限事項を回避しようとして構成プロファイルを削除すると、VPNアクセスも削除されます。

管理されたプロファイル

管理されたプロファイルは、MDMサーバによってデバイスにインストールされる構成プロファイルです。ほかの構成プロファイルと同様、管理されたプロファイルもエンドユーザーが削除できないようにロックできます。管理されたプロファイルを導入すると、プライマリMDMプロファイルは、登録後にMDMによって配布されるあらゆる内容を管理します。またシステムに対する次のような複数の「権限」が含まれています。

- コンピュータ上のすべてのデータの消去
- 構成プロファイルの追加または削除
- 通知に対応可能
- セキュリティ、コンピュータ、ネットワーク、インストールされたアプリケーション、インストールされたプロファイルなど、さまざまな設定に関する情報の問い合わせ

1台のデバイスにインストールできる、管理されたまたは管理されていない構成プロファイルの数には制限がありません。どちらのタイプのプロファイルもインストールできる柔軟性があるため、ポリシーと設定を異なるプロファイルに分割できます。たとえば、エンドユーザーに対して、任意のシステムにアクセスするための、ロック解除された複数のプロファイルのインストールを許可し、その一方で、ロックされている管理対象の2つのプロファイル（1つは会社のネットワークにアクセスするため、もう1つは会社のセキュリティポリシーを適用するため）をインストールするよう求めることもできます。

MDMサーバは、管理されたプロファイルのアップデートと削除を実行します。プライマリMDMプロファイルはロック解除されている必要があるため、エンドユーザーはどのような場合もMDMからオプトアウトできます。エンドユーザーは次の選択ができます。

- **MDMから完全にオプトアウトする。**すべての管理されたプロファイルが削除されます。MDMサーバとエンドユーザーのデバイス間の関係が終了し、MDMサーバ上のインベントリから削除されます。
- **管理下にとどまる。**ただし、1つ、または複数のロック解除された（プライマリMDMプロファイル以外の）管理されたプロファイルを削除します。デバイスはMDMサーバとの関係を維持します。

たとえば、エンドユーザーがEメール設定を含んだプロファイルを削除すると、MDMサーバは関連するプロファイル設定（Eメール、連絡先、カレンダーなど）をデバイスから削除します。サーバ上のデータに影響はありません。残りの管理されていないプロファイルにも影響はありません。デバイスがオプトアウトされたことは、MDMサーバに通知されません。

信頼プロファイル

信頼プロファイルは、自己署名証明書を使用するMDMサーバによって生成されるプロファイルです。このプロファイルには、必須情報、証明書、セキュリティキーが含まれます。管理対象デバイスにインストールされた場合に、MDMサーバと管理対象デバイス間の通信がセキュリティ保護され、真正であることを保証します。

構造と形式

構成プロファイルは、OS Xコンピュータへの構成情報の配布に使用できるXMLファイルです。これらのXMLファイルは、キー値ペアをプロパティリスト（.plist）形式で保存します。またファイル名に.mobileconfigという拡張子が付いています。

OS XとiOSは、構成プロファイルに同じファイル形式を使用します。このファイルには、OS Xの多くのファイルと同様、ターゲットデバイスの設定に関するXML情報が含まれています。これらの構成プロファイルのデータ値はBase64エンコードで保存されます。しかし、これらのファイルはテキストファイルなので、.plist形式を読み書きには任意のXMLエディタまたはテキストエディタを使用することができます。

ペイロード

構成プロファイルを使用して、OS Xコンピュータの特定の（1つまたは複数の）設定値を設定できます。個々の構成プロファイルには、1つまたは複数のペイロードが含

まれています。ペイロードは、たとえばWi-FiやVPNの設定など、特定のタイプの設定の集合です。

新しい構成プロファイルを作成する場合、1つまたは複数のプロファイルのペイロードに設定を指定することができます。各ペイロードの設定フィールドには、ペイロードの目的と使用方法が示されています。入力が必須のフィールドには、赤い円で囲まれた白い矢印が表示されています。

構成プロファイルの内容を表示すると、ペイロードが標準のキー値ペアとして指定されていることがわかります。そのため、XMLに関する詳細な知識がなくてもファイルの内容を簡単に理解できます。

以下に例を示します。

```
<key>PayloadType</key>
<string>com.apple.webClip.managed</string>
```

「PayloadType」というキーに対して、「com.apple.webClip.managed」という値が指定されています。この値は、構成プロファイルのこのセクションのペイロードには、ウェブクリップの情報が含まれていることを示します。

構成プロファイルの形式について詳しくは、付録Cの例を参照してください。

構成プロファイルの作成

概要

新しい構成プロファイルを作成する場合、以下で説明するいずれかのツールを使用して、プロファイルのペイロードを設定します。プロファイルマネージャをはじめとするGUIベースのツールを使用する場合、各ペイロード設定フィールドに、その目的と使用方法の簡単な説明が表示されます。プロファイルマネージャでは、入力が必須のフィールドには、赤い円で囲まれた白い矢印が表示されています。

多くのペイロードでは、ユーザー名とパスワードを指定できます。この情報を記述しない場合、プロファイルをインストールする際に、エンドユーザーがユーザー名とパスワードを入力する必要があります。ベストプラクティスとして、パスワードを含むペイロードは、内容を保護するために暗号化された形式で配布します。

必須のキー

構成プロファイルには必須のキーがいくつかあります。キーは特定の機能に関連した必須のコード行です。独自のプロファイルを記述する場合、次の標準的なキーを組み込む必要があります。

- **PayloadVersion：**PayloadVersionキーは、構成プロファイル内の個別のプロファイルではなく、構成プロファイル全体のバージョンを示します。
- **PayloadUUID：**PayloadUUIDキーは、そのプロファイルに対する全体的に一意の識別子です。実際の内容は重要ではありませんが、全体的に一意である必要があります。OS Xでは、`uuidgen(1)`コマンドを使ってUUIDを生成することができます。
- **PayloadType：**PayloadTypeキーは、「Configuration」という値のみをサポートしています。
- **PayloadIdentifier：**PayloadIdentifierキーは、新規プロファイルを既存のプロファイルと置き換えるか、それとも既存のプロファイルに追加するかを決定します。

標準的なキーに加えて、各ペイロードタイプは、そのペイロードタイプに固有のキーを含みます。

キーおよびペイロードについて詳しくは、付録Aを参照してください。

「一般」設定

構成プロファイルでは、上記で説明した必須キーと「一般」設定のペイロードのみが必須のペイロードです。このペイロードは、構成プロファイルの名前と識別子を設定します。構成プロファイルを常に整理された状態に保つために、一貫した命名規則と、バージョン番号と日付の入ったわかりやすい説明を使用する必要があります。構成プロファイルごとに、固有の識別子フィールドを指定することが重要です。後で作成されたプロファイルに同一の識別子が指定されていると、元のプロファイルと置き換えられてしまうからです。署名され、暗号化されたプロファイルの場合、そのプロファイルの作成に使用したツールの証明書キーが要求されるため、適切なプロファイルの作成が特に重要です。

「一般」設定ペイロードは、プロファイルのインストール後にエンドユーザーがそのプロファイルを削除できるかどうかを指定するためにも使用されます。

複数のペイロード

構成プロファイルには複数のペイロードを指定して、複数のサービスや設定を構成できます。たとえば、Wi-Fi用とEthernet用に別個のネットワークペイロードを作成することもできます。

1台のデバイス、または多数のデバイス用に、すべてのペイロードを含んだ単一の構成プロファイルを作成することは可能ですが、情報の種類別に個別の構成プロファイルを作成すれば、更新と配布がより簡単になります。ベストプラクティスは、パスワードのような機密情報を含むプロファイルをグループ化することです。たとえば、VPNペイロードとWi-Fiペイロードを1つの構成プロファイルにグループ化することができます。

時間を節約できるベストプラクティスは、複数の構成プロファイルのテンプレートを作成し、ディスク上の1つのファイルに保存することです。プロファイルの各テンプレートには、適用する組織のポリシーを定義し、ほかのプロファイルを作成する時はそのテンプレートを再度使用します。

ツール

構成プロファイルは、次のような多様なツールを使用して作成できます。

- OS X Serverに含まれているプロファイルマネージャ
- サードパーティが提供するモバイルデバイス管理（MDM）ソリューション
- テキストエディタやスクリプト作成ソリューションを使用した手動による記述

プロファイルマネージャ

プロファイルマネージャは、Appleが提供するMDMソリューションで、OS X Serverに含まれています。このソフトウェアでは、使いやすいウェブアプリケーションによってOS X用とiOS用の両方のプロファイルを作成できます。

プロファイルマネージャは、3つのコンポーネントで構成されています。これらを組み合わせて、クライアントの設定、デバイスの管理方法、設定をユーザーとデバイスに送信する方法を指定できます。

ウェブベースの管理ツール

プロファイルマネージャのウェブアプリケーションでは、デバイスの設定を構成し、登録済みのデバイスとデバイスグループを管理し、登録済みのデバイスに対するタスクを実行または監視します。

セルフサービス用のユーザーポータル

プロファイルマネージャのユーザーポータルは、管理ツールで定義した設定を配布するための使いやすい安全なウェブサイトです。ユーザーは、各自のOS Xコンピュータを使ってウェブベースのポータルに接続します。ログインした後、管理者によって各自に割り当てられている設定をダウンロードし、インストールすることができます。

また、プロファイルマネージャがMDMサーバとして使用されている場合、ユーザーはこのサイトを利用して、OS Xコンピュータをモバイルデバイス管理の対象として登録します。

モバイルデバイス管理サーバ

プロファイルマネージャは、MDMサーバも提供します。このサーバを使うと、登録済みのOS XコンピュータとiOSデバイスをリモートで管理できます。デバイスがプロファイルマネージャに登録されると、管理者は、そのデバイスの設定をネットワーク経由でアップデートし（ユーザーによる操作は不要）、レポートの作成、デバイスのロックやワイプなどのタスクを実行することができます。

重要：自分のデバイス用に構成プロファイルを作成するには、プロファイルマネージャサービスがサーバ上で有効な状態に構成されていることを確認しておく必要があります。プロファイルマネージャサービスの設定方法について詳しくは、「プロファイルマネージャヘルプ」を参照してください。

サードパーティ製のMDM

構成プロファイルは、サードパーティ製のMDMソリューションを使用して作成することもできます。管理対象のデバイスを登録すると、MDMサーバにより、動的に設定とポリシーを構成できるようになります。サーバは構成プロファイルを通じてデバイスに構成を送信します。プロファイルは自動的にインストールされます。

手動

構成プロファイルはテキストベースのXMLファイルなので、標準のテキストエディタを使用して構成プロファイルを手動で作成できます。このプロセスは、スクリプトによって自動化することもできます。プレーンテキストのサンプル構成プロファイルについては、付録Cを参照してください。

重要：プロファイルを手動で作成する場合、XMLキー値ペアの構造、形式、内容だけでなく、必須のキーとペイロードを覚えておくことが重要です。

構成プロファイルのセキュリティ保護

構成プロファイルは、署名と暗号化によって、変更や表示を防止できます。またパスコードでロックすることでエンドユーザーが削除できないようにして、構成プロファイルを保護することもできます。

署名と暗号化

構成プロファイルのペイロードデータには、アカウント情報やパスワードなどの機密情報が含まれている場合があります。プロファイルマネージャは、構成プロファイルに保存されたデータを保護するため、内蔵のセキュリティ機能を提供します。

署名されたプロファイルは、同じソースによって署名され、同じ識別子を持つ別のプロファイルによってのみ置き換えられます。暗号化されたプロファイルはデータの整合性を保証し、機密のポリシー情報を保護します。プロファイルマネージャを使用して構成プロファイルに署名することで、特定のデバイスの使用を制限し、プロファイルに含まれる設定を部外者が変更したり、表示したりできないようにします。

プロファイルマネージャを使用して構成プロファイルを作成する場合、次のセキュリティ機能を利用できます。

- **なし。**このオプションではプレーンテキストの.mobileconfigファイルを作成します。このファイルはどのデバイスにもインストールできます。ファイルが調べられた場合でも簡単にのぞき見されないように、一部の内容は隠されています。
- **構成プロファイルに署名。**このオプションでは、署名された.mobileconfigファイルを作成します。このファイルはプロファイルが変更されない限り、どのデバイスにもインストールできます。インストール後は、同じ識別子を持ち、同じ証明書によって署名された別のプロファイルによってのみ、プロファイルを更新できます。

プロファイルマネージャは、構成プロファイルに署名できるため、デバイスは構成プロファイルが変更されていないことを確認できます。これには、プロファイルマネージャで作成できるコード署名証明書が必要です。あるいは、設定した信頼チェーンに登録されている署名証明書を使用することもできます。Serverアプリケーションの「プロファイルマネージャ」ペインでプロファイルの署名を有効にし、システムキーチェーンでインストール済みのコード署名証明書を選択できます。その後ユーザーに対し、ユーザーポータルから信頼プロファイルをダウンロードし、署名されたプロファイルを確認するための中間証明書をインストールするように伝えます。

ベストプラクティスは、構成プロファイルに署名をすることです。署名されたプロファイルの場合、改ざんを検出できるからです。

暗号化

MDMサーバと管理対象のデバイスの間のすべての通信は暗号化されています。プロファイルマネージャとクライアントデバイスの間の通信は、HTTPSを介し、セキュアソケットレイヤー（SSL）またはトランスポートレイヤーセキュリティ（TLS）が使用されます。構成プロファイルがプロファイルマネージャサーバからクリアテキストで転送されることはありません。このHTTPS通信の要件があるので、クライアントデバイスは、SSL証明書の発行元である認証機関（CA）を信頼する必要があります。

既知のCAによって署名されたSSL証明書を使用している場合、それ以上の作業は必要ありません。プロファイルマネージャサービスで自己署名証明書を使用している場合、登録する前に、そのルートCAをクライアントデバイスに読み込む必要があります。プロファイルマネージャを使用すると、このプロセスが非常に簡単になります。

プロファイルマネージャは、自己署名証明書で使用されていることを検出すると、信頼プロファイルを生成します。このプロファイルは、プロファイルマネージャ管理ツールからダウンロードできます。また、ユーザーは「マイデバイス」ユーザーポータルの「ダウンロード」セクションからインストールすることもできます。

さらにセキュリティを強化するために、プロファイルコード署名を有効にすることができます。この機能では、コード署名証明書を使用して個々の構成プロファイルに暗号化された署名を行います。デバイスはプロファイルがMDMサービスによって発行されたこと、また改ざんされていないことを確認できます。

SSL証明書と同様、クライアントデバイスは、コード署名証明書に署名したCAを信頼する必要があります。コード署名証明書を購入した場合は、それ以上の作業は必要ありません。自己署名証明書を使用している場合は、登録する前に、プロファイルマネージャの信頼プロファイルをインストールする必要があります。

構成プロファイルの導入

概要

ポリシーを定義し、ポリシーを適用する構成プロファイルを作成したら、次は導入方法を選択します。構成プロファイルをMacにインストールする方法はいくつかあります。適切な方法または方法の組み合わせは、組織が個々の方法を評価して決定する必要があります。

構成プロファイルをOS Xコンピュータに導入するには、次の2つの手順を実行します。

- 構成プロファイルを必要なルート証明書および中間証明書とともにデバイスに配布します。
- ルート証明書、中間証明書、ユーザーIDとともに構成プロファイルをデバイスにインストールします。

プロファイルの配布

プロファイルマネージャの管理ツールから構成プロファイル（.mobileconfigファイル）と信頼プロファイルをダウンロードし、Eメールでユーザーに送信するか、作成したウェブサイトに掲載します。ユーザーはファイルを受信するかダウンロードすると、自分のOS Xコンピュータにインストールできるようになります。

Eメールによる手動処理

最も直接的なインストール戦略は、プロファイルをEメールで直接エンドユーザーに送信することです。この方法は、小規模な導入作業に加え、Wi-Fiアクセスポイントやモバイルデバイス管理（MDM）の登録プロファイルなどの一般的なポリシー設定の配布に適しています。構成プロファイルは、Eメールの添付ファイルとして配布できます。エンドユーザーはOS Xコンピュータでメールメッセージを受信し、添付ファイルをダブルクリックしてプロファイルをインストールします。

プロファイルをEメールで配布する場合、OS Xコンピュータがファイルを認識してインストールできるよう、ファイルの圧縮やファイル拡張子（.mobileconfig）の変更を行わないことが重要です。

ウェブサイト経由の手動処理

プロファイルはファイルベースなので、ユーザーがダウンロードできるように任意のウェブサーバまたはファイルサーバ経由で提供することができます。この導入スタイルでは、サーバの標準のアクセス制御リスト（ACL）を使用して、ユーザーがアクセスできるプロファイルを決定できます。

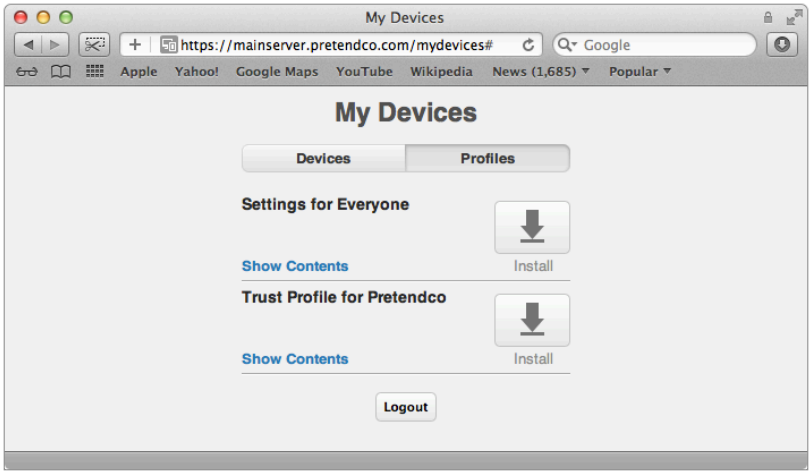
エンドユーザーには、構成プロファイルがあるウェブページのURLを教えてください。エンドユーザーは自分のOS Xコンピュータでウェブページを表示し、プロファイルをダウンロードします。

構成プロファイルをウェブサイトに投稿する準備ができたら、.mobileconfigファイルの圧縮やファイル拡張子の変更を行わないでください。変更すると、OS Xコンピュータがプロファイルを認識してインストールできなくなります。

セルフサービスポータル経由の手動処理

プロファイルマネージャに内蔵されたユーザーポータルを使用して、ユーザーが手動でインストールできるように構成プロファイルを配布します。ユーザーがユーザポータルにログインすると、管理者が割り当てたプロファイルが表示され、個々のプロファイルをダウンロードできます。登録済のOS Xコンピュータでは、自動的にインストールが始まります。

ユーザーは、プロファイルマネージャに内蔵のユーザーポータルから、設定を含む構成プロファイルおよび証明書を含む信頼プロファイルをダウンロードしてインストールします。ユーザーポータルを使用すると、ユーザーは、自分自身またはユーザグループに割り当てられた構成プロファイルを確実に受け取ります。



MDMを使用した自動処理

MDMサーバを使用すると、登録済みのOS Xコンピュータに構成プロファイルを自動的に配布できます。たとえば、プロファイルマネージャのMDMサーバを有効にすると、登録済みのOS Xコンピュータを対象として、構成プロファイルと証明書のインストール、削除、アップデートをリモートで実行できます。これにより、構成プロファイルをネットワーク経由でOS Xコンピュータに自動的に配布できます。

プロファイルのインストール

最も基本的な配布方法では、構成プロファイルファイルをユーザーに配布し、受け取ったユーザーがそれらのファイルをダブルクリックしてインストールします。

手動インストール用の構成プロファイルをプロファイルマネージャを使用して生成するには、適切な設定値を構成し、プロファイル情報画面で「ダウンロード」ボタンをクリックするだけです。

ユーザーが構成プロファイルをインストールする際、プロファイルの内容の確認を求めるメッセージが表示されます。管理対象の設定によっては、プロファイルのインストールに、Macの管理者権限が必要なことがあります。インストールの間、エンドユーザーはプロファイルに指定されなかった必要情報（パスワードなど）や、指定された設定によって要求されるその他の情報を入力する必要があります。また、ユーザー

はプロファイルに含まれる証明書を利用するのに必要なパスワードの入力も求められます。

インストールプロセスの一環として、デバイスはサーバからExchangeポリシーを取得するか、またはMDMサーバからポリシーを取得し、それらのポリシーを更新します。デバイスまたはExchangeポリシーによってパスコード設定が適用される場合、インストールを完了するには、エンドユーザーがポリシーに準拠するパスコードを入力する必要があります。

インストールが正常に完了しない場合、エンドユーザーが入力した情報はまったく保存されません。

Finder経由の手動処理

プロファイルを手動でインストールするには、OS Xコンピュータ上でユーザーがアクセスできる場所（Finderのデスクトップなど）にプロファイルをコピーし、ダブルクリックしてインストールするだけです。

プロファイルをインストールし終わると、「システム環境設定」の「プロファイル」ペインにプロファイル名が表示されます。「プロファイル」ペインには、リモート管理プロファイルや信頼プロファイルなど、システムにインストールされているすべてのユーザーとデバイスプロファイルがリストされます。ユーザーは個々のプロファイルに関する詳細を表示して、プロファイルの追加と削除を実行できます。

Apple Remote Desktopによる自動処理

Apple Remote Desktopなどのクライアント管理ソフトウェアを使用して、自動的にプロファイルをインストールすることができます。Apple Remote Desktopには、リモートファイルコピー、パッケージのインストール、AppleScript、Automatorアクション、UNIXシェルスクリプティングのサポートが内蔵され、多数のOS Xコンピュータでソフトウェアをインストールし管理するための柔軟でパワフルなオプションを提供します。

システムイメージユーティリティを使用した自動処理

システムイメージユーティリティ（SIU）には、構成プロファイルのインストールのサポートが含まれています。OS X以降、SIUには「構成プロファイルを追加」というAutomatorアクションが追加されて拡張されています。このアクションを使用すると、適用する構成プロファイルをNetInstallとNetRestoreの両方の導入イメージに追加することができます。

Automatorアクションは、目的のアクションをSIUライブラリから新しい、または既存のワークフローにドラッグするだけで使用できます。その後、プロファイルを追加し、インストールする順番に並べ替えます。インストールの順番には十分に注意を払ってください。たとえば、ルートCA証明書は、通常、802.1XやVPNの設定などのペイロードを含むプロファイルの前にインストールする必要があります。

ターミナル経由の自動処理（コマンドライン）

構成プロファイルは、ターミナルの`profiles`コマンドを使用して、コマンドライン（スクリプト経由）で管理できます。このツールを使用すると、ユーザーレベルとシステムレベルの両方の構成プロファイルとプロビジョニングプロファイルのインストール、クエリ、削除を実行できます。このツールでは、標準のシェルスクリプトや

Apple Remote Desktopを使用して、またはインストーラパッケージ内のポストフライトスクリプトとして簡単にスクリプトを作成できます。

profilesコマンドは、ポリシーをシステムとユーザードメインのどちらに適用するかを決定するPayloadScopeキーを無視します。profilesコマンドは、ルート権限で実行するとシステムを対象とする構成プロファイルがインストールされます。通常のユーザーとしてこのツールを実行すると、ポリシー設定が対象のユーザーのドメインに適用されます。

重要：profilesコマンドは「/usr/bin」ディレクトリにあります。この位置から移動しないでください。バイナリを移動すると、予期しない動作が発生することがあります。

「testfile.mobileconfig」という構成プロファイルを現在のユーザーにインストールするには：

```
profiles -I -F /testfile.mobileconfig
```

現在のユーザーから「/profiles/testfile2.mobileconfig」という構成プロファイルを削除するには：

```
profiles -R -F /profiles/testfile2.mobileconfig
```

現在のユーザーに対してインストールされている構成プロファイルに関する情報を表示するには：

```
profiles -L
```

profilesコマンドについて詳しくは、ターミナルを起動し、プロンプトで「man profiles」と入力してください。

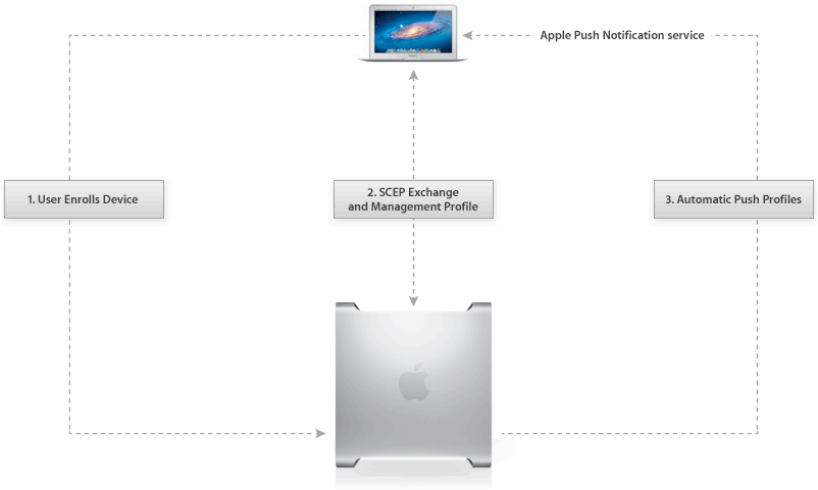
モバイルデバイス管理

より包括的な制御とプロビジョニングが必要な場合、MDMシステムがニーズに対応する可能性があります。数多くのベンダーが、OS Xと連係するMDMシステムを提供しています。この文書では、OS X Serverに含まれるプロファイルマネージャを例として使用していますが、基本的なプロセスとプロファイルペイロードの互換性はすべてのMDMソリューションに共通です。

MDMソリューションでは、ユーザーとデバイスの固有名に基づいて、構成プロファイルを自動的に導入できます。導入作業が省力化され、プロファイルの設定と範囲を定義するだけになりました。デバイスは登録プロファイルを使って登録するか、ユーザーがセルフサービス型のポータルで登録します。登録後、設定をデバイスにプッシュすることができ、ハードウェアとソフトウェアのインベントリが取得され、リモートロックやワイプなどの損失防止テクニックが利用できます。

MDMの概要

MDMの基本的なワークフローは単純です。ユーザーがデバイスを自分で登録できるようにするか、登録プロファイルを提供するかの選択肢があります。登録プロファイルを使用する場合、デバイスは特定のユーザーアカウントには関連付けられません。したがって、ユーザーベースまたはユーザグループベースの自動プッシュプロファイルを使用して、それらのデバイスを管理することはできません。そのため、このようなデバイスの多くは、実験室のワークステーションやキオスクなどの共有デバイスに使用されます。



MDMワークフローの概略

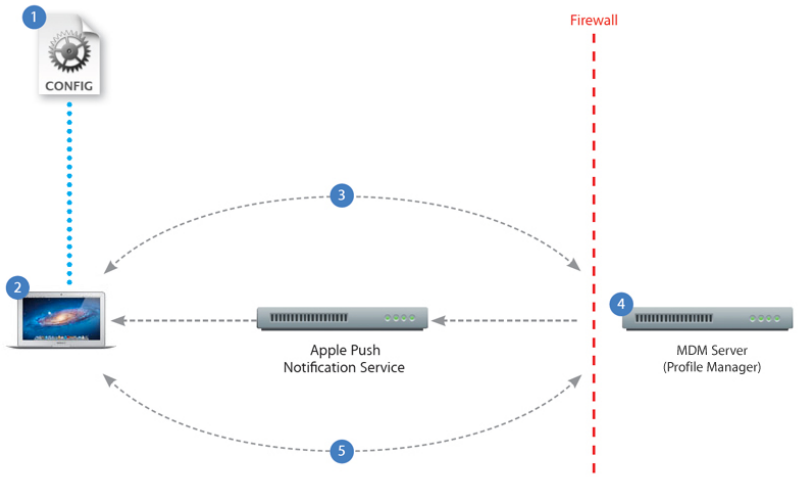
プロセスの最初の手順では、ユーザーがデバイスを登録します。この例では、ユーザーがプロファイルマネージャのマイデバイスポータルにログインし、ボタンをクリックしてMacを登録します。

ユーザーが登録プロセスを開始すると、SafariによってOver-the-Air Enrollmentプロファイルがダウンロードされます。このプロファイルは、「システム環境設定」の「プロファイル」ペインで自動的に開きます。

ユーザーがOver-the-Air Enrollmentプロファイルを受け入れると、Simple Certificate Enrollment Protocol（SCEP）トランザクションが実行されます。SCEPプロセスは、MDMサービスに対してクライアントデバイスを一意に識別する証明書を安全に生成します。

登録段階を完了するには、管理プロファイルをクライアントに配布する必要があります。このプロファイルによりMacが管理下に置かれます。自動プッシュプロファイルの配信およびリモートロックとワイプが即座に有効になります。これらの機能は、登録時にユーザーに明確に示されます。ユーザーは、管理プロファイルを受け入れてプロセスを完了する必要があります。

登録プロセスの完了後、OS Xコンピュータへのインストールが必要なプロファイルがMDMサービスによって判定されます（存在する場合）。該当する構成プロファイルが検出されると、そのクライアントへのプッシュ通知が送信されます。クライアントはAppleプッシュ通知サービス（APNs）からプッシュ通知を受信すると、SSL経由でMDMサーバに連絡し、アップデートされて配信が必要な構成プロファイルがないかを確認します。その後、これらのプロファイルがダウンロードされて自動的に適用されます。



Appleプッシュ通知サービスを使ったモバイルデバイス管理

1. モバイルデバイス管理サーバの情報を保存している構成プロファイルがコンピュータに送信されます。ユーザーに対して、サーバによる管理対象や問い合わせ対象に関する情報が提示されます。
2. ユーザーが、管理対象のコンピュータにオプトインするためのプロファイルをインストールします。
3. プロファイルのインストール時に、登録が行われます。サーバがコンピュータを検証し、アクセスを許可します。

4. サーバがコンピュータに対し、タスクまたはクエリのためのチェックインを求めるプッシュ通知を送信します。
5. コンピュータがHTTPS経由でサーバに直接接続します。サーバがコマンドまたは要求情報を送信します。

デバイスの登録

OS Xコンピュータをリモートに設定し管理するには、その前にそれらのコンピュータをプロファイルマネージャの管理対象として個別に登録する必要があります。OS Xコンピュータをサーバに登録するには、ユーザーが、登録プロファイルをインストールする必要があります。OS Xコンピュータの所有者に対し、プロファイルマネージャのユーザーポータルを使用して、OS Xコンピュータを自分で登録できるようにすることができます。OS Xコンピュータの登録後は、アップデートした構成プロファイル、またはユーザー、デバイス、デバイスグループのいずれかに送信された構成プロファイルが、ユーザーの介入なしにインストールされます。

Simple Certificate Enrollment Protocol

登録プロセスの重要な部分として、Simple Certificate Enrollment Protocol（SCEP）プロセスがあります。MDMシステムで使用した場合、SCEPは次の2つの重要な役割を果たします。

- MDMサーバとOS Xクライアントの間で証明書を交換するためのルートを提供します。
- 証明書失効リスト（CRL）へのアクセスを提供します。これによりクライアントは、構成プロファイルへの署名に使用する認証情報と証明書を検証できるようになります。

重要：SCEPが適切に機能するためには、クライアントがポート1640でHTTPを介してサーバにアクセスできる必要があります。アクセスできない場合、MDMは機能しません。

手動によるプロファイルのダウンロード

手動によるプロファイルのインストールは、Appleプッシュ通知サービスも、さらにはMDM登録もなしに、プロファイルマネージャが生成したポリシーをOS Xコンピュータに配置できる簡単な方法です。しかし、インストール後、これらの構成プロファイルが変更されても、その変更内容は自動的にクライアントに送信されません。

MDM信頼プロファイルやWi-Fiアクセス設定など、きわめて静的なポリシーペイロードには、ダウンロードプロファイルがよく使用されます。

グループごとの割り当て

ダウンロードプロファイルは、プロファイルマネージャで作成する際、デバイス、ユーザー、デバイスやユーザーのグループのいずれかい割り当てることができます。これにより、特定の構成プロファイルにアクセスできるユーザーを簡単に定義できます。

信頼プロファイルなどのグローバルプロファイルは、すべてのユーザーが利用できます。

ユーザーポータルからのプロファイルのダウンロード

プロファイルマネージャのユーザーポータルは、管理者が管理ツールを使って定義した設定を配布するための、使いやすい安全なウェブサイトです。ユーザーは、各自のOS Xコンピュータを使ってウェブベースのポータルに接続します。「マイデバイス」のポータルページにログインすると、そのユーザーに対して割り当てた設定が、「プロファイル」タブからダウンロードしてインストールできるようになります。

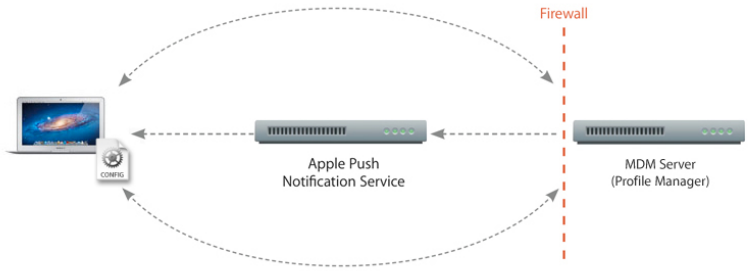
個々のダウンロードプロファイルがリストされ、ユーザーはペイロードの内容を表示した上でインストールすることができます。その後、各プロファイルの横にあるインストールボタンをクリックすると、インストールが完了します。

重要：プロファイルマネージャのユーザーポータルを使って、自分のOS Xに構成プロファイルをインストールするには、プロファイルマネージャサービスがサーバ上で有効な状態に構成されていることを確認しておく必要があります。プロファイルマネージャサービスの設定方法について、詳しくは「プロファイルマネージャヘルプ」を参照してください。

MDMとAppleプッシュ通知サービス

MDMサーバは、登録済みのOS Xコンピュータと通信する必要が生じた場合、サイレント通知をAppleプッシュ通知サービス経由で相手側コンピュータに送信して、コンピュータにサーバへのチェックインを要求します。コンピュータへの通知のプロセスで、詳細情報がAppleプッシュ通知サービスとの間で送受信されることはありません。プッシュ通知が実行するタスクは、相手方コンピュータがMDMサーバにチェックインするように伝えることだけです。すべての構成情報、設定、およびクエリは、コンピュータとMDMサーバ間の暗号化されたSSL/TLS接続を介して、サーバからOS Xコンピュータに直接送信されます。MDMのすべてのリクエストとアクションはバックグラウンドで処理され、バッテリー駆動時間や性能、信頼性への影響が抑えられます。

プッシュ通知サーバがMDMサーバからのコマンドを認識できるようにするには、まずサーバに証明書をインストールする必要があります。この証明書は、Apple Push Certificates Portalでリクエストし、ダウンロードする必要があります。Appleプッシュ通知証明書がMDMサーバにアップロードされると、コンピュータを登録できます。MDM用にAppleプッシュ通知証明書をリクエストする方法の詳細については、www.apple.com/jp/iphone/business/integration/mdm/を参照してください。



Appleプッシュ通知ネットワークの設定

MDMサーバとOS Xコンピュータがファイアウォールの内部にある場合、MDMサービスが正しく機能するために、ネットワークの設定が必要になることがあります。MDMサーバからAppleプッシュ通知サービスに通知を送信するには、TCPポート2195が開いている必要があります。フィードバックサービスを利用するには、TCPポート2196も開いている必要があります。Wi-Fiでデバイスからプッシュサービスに接続するには、TCPポート5223が開いている必要があります。

プッシュ通知サービスに対するIPアドレスの範囲は変更される場合があります。MDMサーバは、IPアドレスではなく、ホスト名によって接続するようになることが考えられます。プッシュサービスは、負荷分散方式を採用しています。この方式では同じホスト名に対して複数のIPアドレスを割り当てます。このホスト名は、「gateway.push.apple.com」です（開発プッシュ通知環境の場合は、「gateway.sandbox.push.apple.com」）。さらに「17.0.0.0/8」というアドレスブロック全体がAppleに割り当てられているため、その範囲を指定するようにファイアウォールのルールを設定できます。

詳しくは、MDMベンダーに問い合わせるか、Developer LibraryのDeveloper Technical Note TN2265の「Troubleshooting Push Notifications」（英語、https://developer.apple.com/library/mac/#technotes/tn2265/_index.html）を参照してください。

設定を導入する場合に最も柔軟な方法は、MDMサーバからOS Xコンピュータに自動的にプロファイルをプッシュすることです。これによってユーザーの操作なしにポリシーが導入、アップデートされるとともに、ポリシーが常に最新の状態に維持されます。OS XコンピュータをMDMサービスに登録すると、自動プッシュプロファイルで設定を自動的に配布できます。個々のOS XコンピュータをMDMサーバに手動で接続する必要はありません。

プロファイルマネージャをはじめとするMDMサーバから自動的にプロファイルをプッシュする鍵は、Appleプッシュ通知サービス（APNs）です。

Appleプッシュ通知サービスはAppleが管理するサービスです。MDMサービスはAPNsを使用して、利用可能な構成プロファイルの有無や、管理対象のOS XコンピュータとiOSデバイスへの変更に関するメッセージ（プッシュ通知）を送信します。プロファイルマネージャを設定する際、APNsの使用に必要な証明書の取得プロセスが、OS X ServerにあるServerアプリケーションによって表示されます。

デバイスはAPNsとの通信を確立すると、その接続を維持し、プッシュ通知に対して待機します。そのため、着信側のポートマッピングは不要です。

プッシュ通知プロセスの概略は以下のとおりです。

1. APNs接続を使用するアプリケーションが、プッシュ通知サービス証明書を使用してサービスに接続します。
2. 認証後、サービスがJSON形式のプロパティリストをAPNsに送信します。APNsは、256バイトを超える通知を拒否します。
3. APNsは、通知ペイロードのデバイストークンを使用してクライアントの位置を確認し、通知をクライアントに配布します。

OS XコンピュータおよびMDMがAPNsと通信を行うには、TCPポート5223、2195、2196でAppleネットワークに到達できる必要があります。AppleはAPNsのIP

アドレス範囲をパブリッシュしていないので、サービスの拡張性を最大限柔軟に確保するためには、そのトラフィックが17.0.0.0ネットワークに到達できる必要があります。17ネットはその全体がAppleによって安全に維持され、管理されています。

プロファイルの通知

管理対象のデバイスでプロファイルのペイロードを変更する必要がある場合、MDMサーバはその特定のデバイスまたはデバイスグループに対し、プッシュ通知を送信します。通知ペイロードには、デバイスがMDMに接続して構成プロファイルのアップデートを確認する必要があるという内容のみが含まれています。

重要：ポリシー情報が通知メッセージで送信されることは絶対にありません。また管理対象のデバイスが、APNs経由でデータを送り返すこともありません。

デバイスはプッシュ通知を受信すると、SSL経由でプロファイルマネージャに接続し、設定のアップデートを確認して適用します。プロファイルのアップデートが完了したら、MDMクライアントは新しいステータスを示すようにサーバで自分の情報をアップデートします。

このプロセスは高速で安全な上、ユーザーに意識させないように処理されます。

構成プロファイルの編集と削除

手動でインストールしたプロファイルは、新しいプロファイルをエンドユーザーに配布してアップデートすることができます。ただし、一意の識別子が一致し、新しいプロファイル（署名されている場合）が同じソースによって署名されている必要があります。

更新されたプロファイルをOS Xコンピュータにインストールする場合、識別子の値とすでにデバイス上にあるプロファイルが比較されます。新しいプロファイルの識別子が一意なら、プロファイルをデバイスに追加できます。識別子がすでにインストールされているプロファイルと一致する場合は、すでにデバイス上にある設定が新しいプロファイル内の情報に置き換えられます（Exchange設定の場合を除く）。

OS X Serverのプロファイルマネージャサービスのようなサードパーティ製MDMソリューションを使用して構成プロファイルを管理している場合は、MDMを使ってワイヤレスでプロファイルの更新と削除ができます。

編集

プロファイルマネージャサービスのようなサードパーティ製MDMソリューションを使用して既存の構成プロファイルを編集できます。エンドユーザーのデバイスにすでにインストールされているプロファイルを、更新したプロファイルに置き換える場合、「一般」設定ペイロードの「識別子」フィールドで同じ値を使用する必要があります。

重要：プロファイルマネージャを使用してデバイスの構成プロファイルをアップデートするには、プロファイルマネージャサービスがサーバ上で有効な状態に構成されていること、また、デバイスがサーバで管理できるように登録されていることを確認しておく必要があります。プロファイルマネージャサービスの設定方法およびデバイスの登録方法について詳しくは、「プロファイルマネージャヘルプ」を参照してください。

プロファイルの削除

プロファイルは、複数の方法によってOS Xコンピュータから削除できます。ユーザーが自ら手動でプロファイルを削除するには、「システム環境設定」の「プロファイル」を使用するか、ターミナルコマンドラインアプリケーションで、`profiles`コマンドを使用します。

管理対象のデバイスにあるプロファイルは、MDMサーバを使用し、Appleプッシュ通知サービス経由でコマンドを送信して削除することもできます。

デバイスからプロファイルを削除する方法は、プロファイルのロックステータスによって異なります。ロックが解除されているプロファイルは、ユーザーが手動でプロファイルを削除できます。デバイスにロックされたプロファイルを配布することもできます。プロファイルをデバイスにロックした場合、インストール済みのプロファイルを削除するには、デバイスのすべてのデータをワイプするか、パスコードを入力するしかありません。構成プロファイルのロックは、エンドユーザーがデバイスからプロファイルを削除するのを防ぐために推奨されています。ロックする際に利用可能なオプションは次のとおりです。

- **常に確認：**このオプションは、エンドユーザーに常にプロファイルの削除を許可します。
- **認証時：**このオプションは、デバイス上でプロファイルの削除を許可する認証パスワードを管理者が指定します。
- **しない：**このオプションは、プロファイルが新しいバージョンのプロファイルによって更新されることを許可します。ただし、プロファイルの削除は許可しません。

プロファイルで自動削除の日時や時間の間隔を設定することもできます。設定すると、プロファイルは設定した日時に有効期限が切れ、削除されます。

関連資料

構成プロファイルの参考資料

プロファイルマネージャヘルプ：構成プロファイルについて

証明書

Apple Push Certificates Portal（英語）

Troubleshooting Push Notifications（英語）

OS X Mountain Lion：証明書について

OS X Mountain Lion：証明書が受け入れられない場合

Mail (Mountain Lion)：証明書を信頼する

OS X Mountain Lion：証明書信頼ポリシー

ADCertificatePayloadPluginを使ってMicrosoft認証局からの証明書を要求する方法

OS X Server

プロファイルマネージャヘルプ

OS X Server：Active Directoryまたは他社のLDAPサービスでプロファイルマネージャおよびWikiサービスを使う

OS X Server：ユーザの操作が必要なプロファイルのインストール

OS X Serverの技術仕様

Apple ソフトウェア製品で使われる一般的なTCPおよびUDPポート

付録A：プロファイルの参考資料

ユーザープロファイルのペイロードの参考資料

OS Xコンピュータのユーザーおよびユーザグループ構成プロファイルでは、次のペイロードを設定できます。

一般	プロファイルの配布タイプ 組織 説明 同意 セキュリティ プロファイルの自動削除
パスコード	単純値を許可 英数字の値が必要 最小のパスコード長 複合文字の最小数 パスコードの有効期限（日） 自動ロック（分） 入力を失敗できる回数
メール	IMAPアカウントの構成 POPアカウントの構成 SMTPアカウントの構成
Exchange	Exchangeアカウントの構成
LDAP	連絡先LDAPの構成
CardDAV	連絡先LDAPの構成
CalDAV	カレンダーサーバアカウントの構成
ネットワーク	ネットワークインターフェイス（EthernetまたはWi-Fi） SSID（Wi-Fi） 非公開ネットワーク（Wi-Fi） 自動接続（Wi-Fi） プロキシ設定（Wi-Fi） セキュリティの種類（Wi-Fi） パスワード（Wi-Fi） ネットワークセキュリティ設定（プロトコルおよび信頼Ethernet） 受け入れるEAPの種類（Ethernet）
VPN	VPNクライアント設定 VPNオンデマンド
証明書	X.509証明書
SCEP	SCEPサーバ設定
ウェブクリップ	ウェブクリップペイロード
セキュリティとプライバシー	使用状況と診断情報をオプトアウト ユーザーのGatekeeper設定変更を許可しない

識別情報	ユーザーの表示名 Eメールアドレス ユーザー名 パスワード
制限	「環境設定」ペインのアクセス アプリケーションの起動コントロール ウィジェットの起動コントロール メディアアクセスコントロール AirDropのアクセス
メッセージ	Jabberアカウントの設定 AIMアカウントの設定
AD証明書	Microsoft認証局（CA）自動登録設定
ログイン項目	アプリケーションの自動起動 項目の自動起動 ネットワークマウントへの自動接続
モバイル環境	モバイルアカウントの作成 モバイルアカウントの有効期限 ポータブルホームディレクトリのシンクルール
Dock	Dock項目の設定 Dockの表示設定
プリント	プリンタリストの設定 プリントジョブのフッタ
ペアレンタルコントロール	コンテンツフィルタ 時間制限
カスタム	任意のアプリケーション環境設定

デバイスプロファイルのペイロードの参考資料

OS Xコンピュータのデバイスおよびデバイスグループ構成プロファイルでは、次のペイロードを設定できます。

一般	プロファイルの配布タイプ 組織 説明 同意 セキュリティ プロファイルの自動削除
パスコード	単純値を許可 英数字の値が必要 最小のパスコード長 複合文字の最小数 パスコードの有効期限（日） 自動ロック（分） 入力を失敗できる回数

ネットワーク	ネットワークインターフェイス（EthernetまたはWi-Fi） SSID（Wi-Fi） 非公開ネットワーク（Wi-Fi） 自動接続（Wi-Fi） プロキシ設定（Wi-Fi） セキュリティの種類（Wi-Fi） パスワード（Wi-Fi） ネットワークセキュリティ設定（プロトコルおよび信頼Ethernet） 受け入れるEAPの種類（Ethernet）
VPN	VPNクライアント設定 VPNオンデマンド
証明書	X.509証明書
SCEP	SCEPサーバ設定
セキュリティとプライバシー	使用状況と診断情報をオプトアウト ユーザーのGatekeeper設定変更を許可しない Gatekeeperセキュリティ設定
識別情報	ユーザーの表示名 Eメールアドレス ユーザー名 パスワード
制限	「環境設定」ペインのアクセス アプリケーションの起動コントロール ウィジェットの起動コントロール メディアアクセスコントロール
ディレクトリ	Active Directoryのバインド設定 Open Directoryのバインド設定
AD証明書	Microsoft認証局（CA）自動登録設定
ログインウインドウ	ログインパネルの見出し ログインウインドウのメッセージ ログインウインドウのスタイル ログインウインドウACL ログインウインドウスクリプト
ログイン項目	アプリケーションの自動起動 項目の自動起動 ネットワークマウントへの自動接続
モバイル環境	モバイルアカウントの作成 モバイルアカウントの有効期限 ポータブルホームディレクトリのシンクルール
Dock	Dock項目の設定 Dockの表示設定
ソフトウェアアップデート	Software Update Server設定
プリント	プリンタリストの設定 プリントジョブのフッタ
省エネルギー	システムのスリープ設定 スリープ設定を表示 スケジュール済みスリープ／スリープ解除設定

ペアレンタルコントロール	コンテンツフィルタ 時間制限
カスタム	任意のアプリケーション環境設定

付録B：サービスポートに関する参考資料

プロファイルマネージャで必須のTCPポート

サービス	TCPポート
HTTP	80
HTTPS	443
SCEP	1640
APNs	5223、2195、2196

付録C：サンプルプロファイル

デバイス構成プロファイルの例

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN""http://
www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

<dict>

        <key>PayloadDescription</key>

        <string>Sample Device configuration profile</string>

        <key>PayloadDisplayName</key>

        <string>Settings for Example Device</string>

        <key>PayloadIdentifier</key>

        <string>com.apple.mdm.mainserver.pretendco.com.
850bb6c0-45ee-012f-27bb-482a140c4fbd.alacarte</string>

        <key>PayloadOrganization</key>

        <string>Pretendco</string>

        <key>PayloadRemovalDisallowed</key>

        <false/>

        <key>PayloadScope</key>

        <string>System</string>

        <key>PayloadType</key>

        <string>Configuration</string>

        <key>PayloadUUID</key>

        <string>850bb6c0-45ee-012f-27bb-482a140c4fbd</string>

        <key>PayloadVersion</key>

        <integer>1</integer>

</dict>

</plist>
```

ユーザー構成プロファイルの例

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN""http://
www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

<dict>

        <key>PayloadDescription</key>

        <string>Sample user configuration profile</string>

        <key>PayloadDisplayName</key>

        <string>Settings for User 01</string>

        <key>PayloadIdentifier</key>

        <string>com.apple.mdm.mainserver.pretendco.com.
3a3b4a60-45ec-012f-27a6-482a140c4fbd.alacarte</string>

        <key>PayloadOrganization</key>

        <string>Pretendco</string>

        <key>PayloadRemovalDisallowed</key>

        <false/>

        <key>PayloadScope</key>

        <string>User</string>

        <key>PayloadType</key>

        <string>Configuration</string>

        <key>PayloadUUID</key>

        <string>3a3b4a60-45ec-012f-27a6-482a140c4fbd</string>

        <key>PayloadVersion</key>

        <integer>1</integer>

</dict>

</plist>
```

2013年1月15日