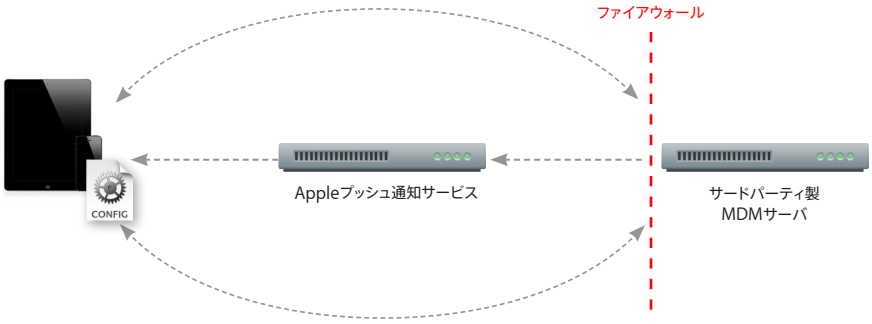
iPhoneとiPadの配備
モバイルデバイス管理

iOSは、組織を横断して広範に配備されたiPhoneやiPadを管理するモバイルデバイス管理（MDM）をサポートしています。
MDM機能は、構成プロファイル、ワイヤレス登録、Appleプッシュ通知サービスなど、既存のiOSテクノロジーを基に構築されており、社内またはサードパーティ製のサーバソリューションと統合できます。これにより、IT部門は、iPhoneやiPadをエンタープライズ環境に安全に導入し、設定の構成や更新をワイヤレスで行い、企業のポリシーへの準拠状況を監視し、さらには管理対象のデバイスをリモートで消去したりロックしたりすることが可能になります。

iPhoneおよびiPadの管理

iOSデバイスの管理は、モバイルデバイス管理（MDM）サーバを介して行います。このサーバはIT部門が社内に設置することも、社外のソリューションプロバイダから購入することもできます。デバイスはサーバと通信して、保留になっているタスクがあるかどうかを確認し、適切なアクションで応答します。これらのタスクには、ポリシーのアップデート、要求されたデバイスやネットワーク情報の提供、設定とデータの削除などがあります。

管理機能のほとんどはバックグラウンドで実行されるので、ユーザーの操作は必要ありません。たとえば、IT部門がVPNインフラストラクチャを更新する場合、MDMサーバが、iPhoneやiPadにワイヤレスで新しいアカウント情報を設定します。その後、社員がVPNを使用する際には、適切な構成がすでに設定されているので、社員はヘルプデスクに問い合わせたり、設定を手動で変更したりする必要はありません。



iOSとSCEP
iOSはSCEP（Simple Certificate Enrollment Protocol）をサポートしています。SCEPはIETFのインターネットドラフトで、証明書の大規模な配布を簡単に行える方法を提供するよう設計されています。SCEPを利用すれば、固有名証明書をワイヤレスでiPhoneやiPadに登録し、企業サービスに対する認証に使用することができます。

モバイルデバイス管理（MDM）とAppleプッシュ通知サービス

MDMサーバがiPhoneまたはiPadとの通信を行う場合は、Appleプッシュ通知サービスを使って、サーバへのチェックインを促すサイレント通知がデバイスに送信されます。デバイスに通知するプロセスでは、Appleプッシュ通知サービスとの間で機密情報のやり取りは行われません。プッシュ通知によって実行されるタスクは、MDMサーバをチェックするようにデバイスに合図を送ることのみとなります。すべての構成情報、設定、照会は、サーバから直接iOSデバイスに送信され、デバイスとMDMサーバの間では暗号化されたSSL/TLS接続が使用されます。iOSは、バッテリー駆動時間、パフォーマンス、信頼性といったユーザーエクスペリエンスへの影響を最小限に抑えるために、すべてのMDMのリクエストやアクションをバックグラウンドで処理します。

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、デバイスの登録を開始できます。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iOSデバイスがファイアウォールの内側にある場合、MDMサーバを正しく機能させるために、ネットワークの構成が必要となる場合があります。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場合は、TCPポート2196も開く必要があります。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。

プッシュサービス用のIPアドレスの範囲は変更される場合があるため、MDMサーバはIPアドレスではなくホスト名で接続するのが理想的です。プッシュサービスでは、同一のホスト名に対して異なるIPアドレスを生成する負荷分散スキームが使用されます。ホスト名はgateway.push.apple.com（開発用プッシュ通知環境ではgateway.sandbox.push.apple.com）です。また、17.0.0.0/8アドレスブロック全体がAppleに割り当てられるため、その範囲を指定するファイアウォールのルールを確立できます。

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

登録

モバイルデバイス管理サーバとネットワークの設定が完了して最初のiPhoneまたはiPadの管理作業は、MDMサーバを使用して登録することです。これにより、デバイスとサーバの関係が確立され、その後はユーザーが操作しなくても、必要に応じてデバイスを管理できるようになります。

この操作は、iPhoneまたはiPadをUSB経由でコンピュータに接続することで行えますが、ほとんどのソリューションでは登録プロファイルをワイヤレスで配信できます。MDMベンダーによって方法が異なり、アプリケーションを使用してこのプロセスを開始する場合と、ユーザーをウェブポータルに移動させて登録を開始する場合があります。どちらの方法にもそれぞれのメリットがありますが、両方ともSafariを経由したワイヤレス登録プロセスの起動に使用されます。

登録プロセスの概要

ワイヤレス登録のプロセスには、自動ワークフローで組み合わせて、エンタープライズ環境で最も拡張性の高い方法でデバイスを安全に登録できるようにするフェーズが含まれています。フェーズは以下のとおりです。

1. ユーザー認証

ユーザー認証では、受信した登録リクエストが権限のあるユーザーからのものであることと、証明書の登録に進む前にユーザーのデバイス情報が記録されていることが確認されます。登録プロセスを開始するようユーザーに通知する際、管理者は、ウェブポータル、Eメール、SMSメッセージ、アプリケーションを利用できます。

2. 証明書登録

ユーザーの認証後は、iOSによってSimple Certificate Enrollment Protocol（SCEP）で証明書登録要求が生成されます。この登録リクエストはエンタープライズ認証局（CA）に直接送信され、iPhoneやiPadはCAからのレスポンスとして固有名証明書を受信できます。

3. デバイスの構成

ID証明書がインストールされると、デバイスは暗号化された構成情報をワイヤレスで受信できます。この情報は、対象のデバイスにのみインストールすることができ、情報には、デバイスがMDMサーバに接続するために必要な設定が含まれています。

登録プロセスの最後の段階では、デバイスにインストール画面が表示され、ユーザーは、MDMサーバがそのデバイスに対してどのようなアクセス権を持つのかを確認できます。プロファイルのインストールに同意すると、ユーザーのデバイスは自動的に登録されます。それ以上の操作は必要ありません。

管理対象のデバイスとしてiPhoneやiPadを登録すると、MDMサーバから動的に設定の構成や情報照会を行ったり、リモートワイプを実行したりできるようになります。

管理

モバイルデバイス管理には、MDMサーバがiOSデバイスに対して実行できる数多くの機能が用意されています。これには、構成プロファイルやプロビジョニングプロファイルのインストールと削除、アプリケーションの管理、MDMサーバとの関係の停止、デバイスのリモートワイプなどが含まれます。

管理対象の構成

デバイスの構成プロセスの初期の段階で、MDMサーバは、バックグラウンドでインストールされた構成プロファイルをiPhoneとiPadにプッシュします。時間がたつと、登録時に実装された設定とポリシーは更新または変更が必要になる場合があります。そうした変更を行うために、MDMサーバは、新しい構成プロファイルをインストールし、既存のプロファイルをいつでも変更または削除できます。また、ユーザーの場所や組織内での役割によっては、状況に応じた構成をiOSデバイスにインストールする必要が出てくる場合もあります。たとえば、ユーザーが海外出張している場合、MDMサーバはメールアカウントの同期を自動ではなく手動で行うように強制できます。通信業者のローミング費用が発生しないように、MDMサーバを使って、リモートで音声サービスやデータサービスを無効にすることもできます。

管理されたアプリケーション

MDMサーバはApp Storeから入手したサードパーティ製アプリケーションや、企業の社内アプリケーションを管理することができます。サーバは管理されたアプリケーションとそれに関連付けられたデータを必要に応じて削除できるほか、MDMプロファイルが削除された時にアプリケーションを削除するかどうか指定することも可能です。さらに、MDMサーバでは、管理されたアプリケーションのデータがiTunesとiCloudにバックアップされないように指定できます。

管理されたアプリケーションをインストールするために、MDMサーバからユーザーのデバイスにインストールコマンドが送信されます。管理されたアプリケーションをインストールするには、ユーザーの承認が必要です。MDMサーバが管理されたアプリケーションをApp Storeからインストールするようにリクエストすると、そのアプリケーションは、インストール時に使用されるiTunesアカウントで引き換えられます。有料アプリケーションの場合、MDMサーバはVolume Purchasing Program（VPP）引き換えコードを送信する必要があります。VPPの詳細については、www.apple.com/jp/business/vpp/をご覧ください。App Storeが無効化されている場合、ユーザーのデバイスにApp Storeのアプリケーションをインストールすることはできません。

監視対象デバイスをMDMで管理する

Apple Configuratorを使ってアクティベートしたデバイスは「監視」の対象になり、追加の設定や制限をインストールすることができます。Apple Configuratorによって監視対象になったデバイスには、適用可能な設定や制限をすべて、MDMを介してワイヤレスでインストールすることもできます。Apple ConfiguratorとMDMでデバイスの構成と管理を行う方法の詳細は、「iPhoneとiPadの配備：Apple Configurator」を参照してください。

デバイスの削除または消去

デバイスがポリシーから外れているか、紛失または盗難されたことが判明した場合、または従業員が退社した場合、MDMサーバはさまざまな方法で社内情報を保護するアクションを実行します。

IT管理者は、MDMサーバの情報を含む構成プロファイルを削除することで、デバイスとのMDM関係を終了させることができます。これによって、その構成プロファイルに基づいてインストールされたアカウント、設定、アプリケーションはすべて削除されます。別の方法として、MDM構成プロファイルはそのままにしておき、削除を要する構成プロファイル、プロビジョニングプロファイル、管理されたアプリケーションだけを、MDMを使って削除することも可能です。このアプローチでは、デバイスをMDMの管理下に留めておくことができ、ポリシー違反が解決した場合に再登録を行う必要もありません。

どちらの方法でも、IT部門はポリシーに準拠しているユーザーおよびデバイスに対してのみ情報を提供すると共に、音楽、写真、個人用アプリケーションといったユーザーの個人データに影響を与えることなく、確実に会社のデータを削除することができます。

デバイス上のすべてのメディアとデータを完全に削除し、出荷時の状態に戻す必要がある場合は、MDMによってiPhone/iPadのリモートワイプを行います。紛失したデバイスをまだユーザーが探している状況であれば、デバイスにリモートロックコマンドを送る方法もあります。デバイスの画面はロックされ、解除するにはユーザーのパスコードが必要です。

ユーザーが単にパスコードを忘れてしまった場合は、MDMサーバでデバイスのパスコードを削除し、60分以内に新しいパスコードを作成するようにユーザーに指示を出すことができます。

サポートされている管理コマンド

管理対象の構成

- 構成プロファイルのインストール
- 構成プロファイルの削除
- データローミング
- 音声ローミング（一部のキャリアでは使用不可）

管理されたアプリケーション

- 管理されたアプリケーションのインストール
- 管理されたアプリケーションの削除
- 管理されたアプリケーションの一覧
- プロビジョニングプロファイルのインストール
- プロビジョニングプロファイルの削除

セキュリティコマンド

- リモートワイプ
- リモートロック
- パスコードの消去

設定

デバイスのアカウント、ポリシー、制限を構成するため、MDMサーバは「構成プロファイル」と呼ばれるファイルをデバイスに送信します。プロファイルは自動的にインストールされます。構成プロファイルはXMLファイルです。このファイルには、アカウント情報、パスコードポリシー、制限、そのほかのデバイス設定など、デバイスとエンタープライズシステムの連係を可能にするための設定や権限が含まれています。デバイスの構成を前述の登録プロセスと組み合わせることで、IT部門は、信頼できるユーザーだけが企業サービスにアクセスしていることと、定められたポリシーに従ってユーザーのデバイスが適切に構成されていることを確信できます。

構成プロファイルは署名による暗号化が可能なので、設定を変更したり、ほかの人と共有したりすることはできません。

サポートされる設定可能なアイテム

アカウント

- Exchange ActiveSync
- IMAP/POP Eメール
- Wi-Fi
- VPN
- LDAP
- CardDAV
- CalDAV
- 照会するカレンダー

パスコードポリシー

- デバイスでのパスコードの要求
- 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
- 自動ロックまでの時間
- パスコードの履歴
- デバイスロックの猶予期間
- 入力を失敗できる回数

セキュリティとプライバシー

- 診断データをAppleに送信することを許可
- 信頼されていないTLS証明書の受け入れをユーザーに許可
- 強制的に暗号化バックアップ

監視対象のみの制限

- iMessageを許可
- Game Centerを許可
- アプリケーションの削除を許可
- iBookstoreを許可
- iBookstoreの成人向けコンテンツを許可
- Siriの不適切な単語フィルタを有効にする
- 構成プロファイルの手動インストールを許可

そのほかの設定

- 資格情報
- ウェブクリップ
- SCEP設定
- APN設定
- グローバルHTTPプロキシ（監視対象のみ）
- シングルアプリケーションモード（監視対象のみ）

デバイスの機能

- アプリケーションのインストールを許可
- Siriを許可
- デバイスのロック中にSiriを許可
- ロック中のPassbook通知を許可
- カメラの使用を許可
- FaceTimeを許可
- 画面の取り込みを許可
- ローミング中の自動同期を許可
- メール履歴の同期を許可
- 音声ダイヤルを許可
- In-App Purchaseを許可
- 購入時に常にiTunes Storeのパスワードを要求
- マルチプレイヤーゲームを許可
- Game Centerの友人の追加を許可

アプリケーション

- YouTubeの使用を許可
- iTunes Storeの使用を許可
- Safariの使用を許可
- Safariのセキュリティ設定

iCloud

- バックアップを許可
- 書類同期を許可
- フォトストリームを許可
- 共有フォトストリームを許可

コンテンツレーティング

- 不適切なミュージックとPodcastを許可
- レーティングの地域の設定
- 許可されるコンテンツレーティングの設定

デバイスのクエリ

MDMサーバには、構成に加え、多様な情報についてデバイスにクエリする機能があります。この情報を使って、デバイスが常に必要なポリシーに準拠していることを確認できます。

サポートされているクエリ

デバイス情報

- UDID（Unique Device Identifier）
- デバイス名
- iOSおよびビルドバージョン
- モデル名および番号
- シリアル番号
- 容量と空き領域
- IMEI
- モデムファームウェア
- バッテリー残量
- 監視のステータス

ネットワーク情報

- ICCID
- Bluetooth®およびWi-FiのMACアドレス
- 現在のキャリアのネットワーク
- 加入者のキャリアのネットワーク
- キャリア設定のバージョン
- 電話番号
- データローミング設定（オン／オフ）

コンプライアンスとセキュリティ情報

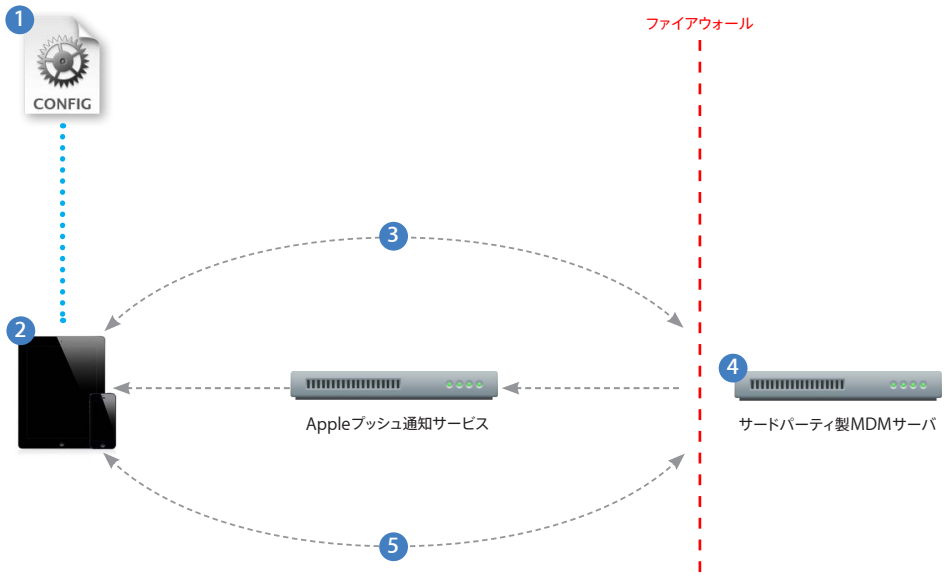
- インストールされている構成プロファイル
- 有効期限付きでインストールされている証明書
- 適用されているすべての制限の一覧
- ハードウェア暗号化機能
- パスコードの設定有無

アプリケーション

- インストールされているアプリケーション（アプリケーションID、名前、バージョン、サイズ、およびアプリケーションのデータサイズ）
- 有効期限付きでインストールされているプロビジョニングプロファイル

プロセス概要

次の図は、モバイルデバイス管理（MDM）サーバの基本的な配備例を示しています。



1. モバイルデバイス管理サーバの情報を含む構成プロファイルがデバイスに送信されます。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. ユーザーはプロファイルをインストールして、デバイスが管理されることを許可します。
3. プロファイルがインストールされるとデバイスが登録されます。サーバはデバイスを検証してアクセスを許可します。
4. タスクやクエリを確認するためにチェックインするよう、サーバからデバイスにプッシュ通知が送信されます。
5. デバイスはHTTPSを使用して直接サーバに接続します。サーバがコマンドまたは要求情報を送信します。

モバイルデバイス管理の詳細については、www.apple.com/jp/iphone/business/integration/mdmを参照してください。

©2012 Apple Inc. All Rights Reserved.Apple、Appleのロゴ、FaceTime、iPad、iPhone、iTunes、Passbook、Safari、Siriは、米国およびその他の国で登録されたApple Inc.の商標です。iMessageはApple Inc.の商標です。iCloudおよびiTunes Storeは、米国およびその他の国で登録されたApple Inc.のサービスマークです。App StoreおよびiBookstoreは、Apple Inc.のサービスマークです。Bluetoothのワードマークとロゴは、Bluetooth SIG, Inc.が所有する登録商標であり、Appleはライセンスに基づきこのマークを使用しています。本書に記載されているその他の製品名および会社名はそれぞれの会社の商標である場合があります。製品仕様は予告なく変更する可能性があります。2012年9月