



iPhone と iPad の配備 モバイルデバイス管理

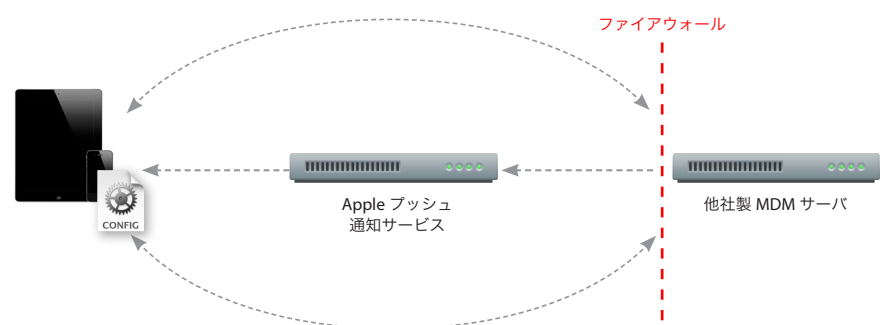


iOS は、組織を横断して広範に配備された iPhone や iPad を管理するモバイルデバイス管理 (MDM) をサポートしています。MDM 機能は、構成プロファイル、無線 (OTA) 登録、Apple プッシュ通知サービスなど、既存の iOS テクノロジーを基に構築されており、社内または他社製のサーバソリューションと統合できます。これにより、IT 部門は、iPhone や iPad をエンタープライズ環境に安全に導入し、設定の構成や更新をワイヤレスで行い、企業のポリシーへの準拠状況を監視し、さらには管理対象のデバイスをリモートで消去したりロックすることが可能になります。

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を行い、保留中のタスクがあるかどうかを確認し、それに応じて適切なアクションを実行します。タスクには、ポリシーの更新、要求されたデバイスまたはネットワーク情報の提供、設定および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、ユーザの操作は必要ありません。例えば、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、固有名証明書を無線で 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、最初に証明書がサーバ上にインストールされます。この証明書は、Apple Push Certificates Portal からリクエストおよびダウンロードできます。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 用の Apple プッシュ通知証明書のリクエストについて詳しくは、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 を開く必要があります。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。デバイスが Wi-Fi 経由でプッシュ通知サービスに接続する場合は、TCP ポート 5223 を開きます。

プッシュ通知サービス用の 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。プッシュ通知サービスでは、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は 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」(http://developer.apple.com/library/ios/#technotes/tn2265/_index.html) を参照してください。

登録

MDM サーバとネットワークの構成が完了したら、iPhone または iPad を管理する最初のステップとして、MDM サーバへの登録を行います。これにより、デバイスとサーバの間で関係が確立され、その後、ユーザが操作しなくてもオンデマンドで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 を経由した無線 (OTA) 登録プロセスの起動に使用されます。

登録プロセス概要

無線（OTA）での登録には、3つのフェーズがあります。この3つのフェーズを、自動化されたワークフローと組み合わせれば、最も拡張性の高い方法で、企業にデバイスを安全に導入することができます。フェーズは以下のとおりです。

1. ユーザ認証

ユーザ認証では、受信した登録リクエストが権限のあるユーザ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. 証明書の登録

ユーザ認証が完了すると、iOSはSCEP（Simple Certificate Enrollment Protocol）を使用して証明書登録リクエストを生成します。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

固有名証明書のインストールが完了すると、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、ユーザのデバイスは自動的に登録されます。それ以上の操作は不要です。

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できるようになります。

構成

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、パスワードポリシー、制限、その他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と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。

サポートされている構成可能な設定 アカウント

- Exchange ActiveSync
- IMAP/POP E メール
- Wi-Fi
- VPN
- LDAP
- CardDAV
- CalDAV
- 照会したカレンダー

パスワードポリシー

- デバイスのパスワードが必要
- 単純値を許可
- 英数字の値が必要
- 最小のパスワード長
- 複合文字の最小数
- パスワードの有効期限
- 自動ロックまでの時間
- パスワードの履歴
- 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
- ユーザが信頼できない証明書を受け入れることを許可
- 強制的に暗号化バックアップ

その他の設定

- 資格情報
- Web クリップ
- SCEP 設定
- APN 設定

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
- 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
- 音声ダイヤルを許可
- アプリケーション内での購入を許可
- 購入時に必ずストアパスワードを要求
- マルチプレイヤーゲームを許可
- Game Center に友達の追加を許可

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
- 書類の同期を許可
- フォトストリームを許可

コンテンツレート

- 不適切な内容の音楽と Podcast を許可
- レーティングの地域
- 許可されるコンテンツレーティング

デバイス情報の照会

MDM サーバでは、構成だけでなく、デバイスの様々な情報の照会も行えます。この情報を使用して、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
- 容量と使用可能な空き領域
- IMEI
- モデムのファームウェア
- バッテリー残量

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

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。

管理対象の設定

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。例えば、ユーザ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シンク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。

管理対象のアプリケーション

MDM サーバでは、App Store から入手できる他社製アプリケーションと、社内向けアプリケーションを管理できます。管理対象のアプリケーションとその関連データをオンデマンドで削除する、または 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を指定する、といったこともサーバで管理できます。また、MDM サーバでは、管理対象のアプリケーションのデータが iTunes や iCloud にバックアップされないようにすることもできます。

管理対象の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。管理対象のアプリケーションには、インストール前にユーザによる承認が必要です。App Storeが無効になっていると、ユーザのデバイスに App Store にある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。

デバイスの削除またはワイプ

デバイスがポリシーに違反している場合、紛失したり盗難された場合、あるいは従業員が会社を退職する場合に備え、MDM サーバには企業のデータを保護するための様々な方法が用意されています。

IT 管理者は、MDM サーバ情報を含んだ構成プロファイルを削除することで、MDM とデバイスとの関係を停止できます。こうすることで、アカウント、設定、そのプロファイルでインストールしたアプリケーションがすべて削除されます。または、MDM 構成プロファイルを残しておき、MDM を使用して、特定の構成プロファイル、プロビジョニングプロファイル、管理対象のアプリケーションだけを削除することもできます。この方法を使えば、デバイスは MDM によって管理された状態のままなので、デバイスが再度ポリシーに準拠した際の再登録の手間を省きます。

いずれの方法でも、IT 管理者は、ポリシーに準拠したユーザとデバイスのみに関与し、音楽、写真、個人用のアプリケーションといった個人データに影響を与えることなく企業のデータを削除できます。

デバイス上のすべてのメディアやデータを完全に削除し、デバイスを工場出荷時の設定に戻す場合は、MDM で iPhone と iPad に対してリモートワイプを実行できます。ユーザのデバイスがどうしても見つからない場合、IT 管理者はデバイスに対してリモートロックコマンドを送信することもできます。このコマンドによって、画面がロックされ、ユーザのパスコードを入力しない限り、ロックを解除できなくなります。

ユーザ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

管理対象の設定

- 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）

管理対象のアプリケーション

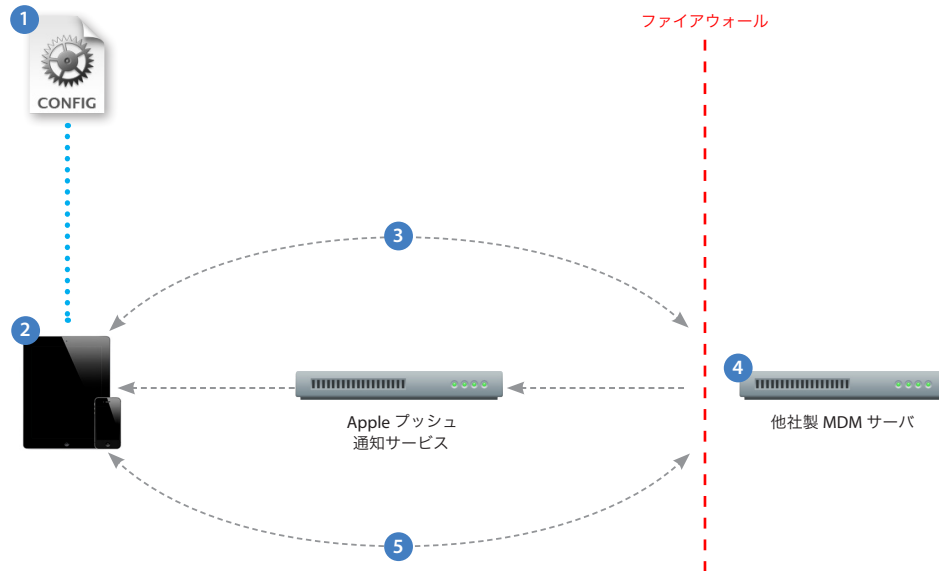
- 管理対象のアプリケーションのインストール
- 管理対象のアプリケーションの削除
- 管理対象のアプリケーションの一覧
- プロビジョニングプロファイルのインストール
- プロビジョニングプロファイルの削除

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

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 MDM 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。サーバで管理される情報、サーバが照会する情報がユーザーに提供されます。
- ② ユーザ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。サーバはコマンドを送信するか、情報を要求します。

モバイルデバイス管理について詳しくは、www.apple.com/jp/iphone/business/integration/mdm を参照してください。