iOSでのデバイスおよび企業データの管理

目次

概要

あらゆる企業が、iPhoneとiPadを使って社員を支援しています。

モバイル戦略を成功させるには、IT部門による管理とユーザーイネーブルメントのバランスを取ることが非常に重要です。自分のアプリケーションやコンテンツでiOSデバイスをパーソナライズすることによって、ユーザーはデバイスの所有者としてより強く責任感を持ち、さらに高いレベルでの取り組みや生産性向上につながります。これは、仕事のデータと個人のデータをシームレスに分離し、企業データとアプリケーションを別々に管理するスマートな方法を提供するAppleの管理フレームワークによって可能になります。また、ユーザーは自分のデバイスがどのように管理されているかを把握し、プライバシーが保護されていると安心することができます。

この文書では、IT部門による必須の管理を行いながら、ユーザーが業務を進めるうえで最適なツールを得られるようにする方法について、ガイダンスを提供します。この文書は「iOS導入リファレンス」を補足するものです。「iOS導入リファレンス」は、エンタープライズにおけるiOSデバイスの導入と管理に関する包括的なオンライン技術資料です。

「iOS導入リファレンス」は、help.apple.com/deployment/ios/?lang=jaから参照できます。

管理の基本

iOSにはアカウント設定の簡素化、ポリシーの設定、アプリケーションの配布、リモートによるデバイスの機能制限の適用を可能にする幅広い技術が内蔵されており、iPhoneとiPadを効率的に導入できます。

管理のアプローチ

Appleの管理フレームワークは、モバイルデバイス管理の基礎となります。iOSにはこのフレームワークが組み込まれており、組織は単に機能を制限したり無効化するのではなく、簡単な操作で必要な機能を管理できるようになります。その結果Appleの管理フレームワークは、サードパーティ製モバイルデバイス管理（MDM）ソリューションによるデバイス、アプリケーション、およびデータのきめ細かな制御を実現します。そして最も重要なのは、ユーザー体験を低下させたり社員のプライバシーを犠牲にすることなく、必要な管理ができるという点です。

市場のほかのデバイス管理方法では、MDM機能をエンタープライズモバイル管理（EMM）、モバイルアプリケーション管理（MAM）といった名前で呼ぶこともありますが、組織のデバイスと企業データをワイヤレスで管理するという目的には変わりありません。Appleの管理フレームワークはiOSに組み込まれているので、MDMソリューションのプロバイダから別のエージェントアプリケーションを入手する必要はありません。

仕事のデータと個人のデータの分離

組織がサポートするデバイスがユーザー所有であっても企業所有であっても、IT部門の管理目標を実現しながら、ユーザーの仕事の生産性を最大限に高めることができます。仕事のデータと個人のデータは別々に管理されますが、ユーザー体験の一貫性は維持されます。これにより、同じデバイス上に人気の仕事効率化のためのアプリケーションと企業アプリケーションをインストールしておけるので、社員はより自由に仕事ができます。iOSはユーザー体験を低下させたり操作が面倒だったりするコンテナなどのサードパーティ製ソリューションを使わずにこれを実現します。

様々な管理モデル

ほかのプラットフォーム上の問題（iOSでは見られない問題）を解決するために、コンテナが構築されることがよくあります。同じデバイス上で2つの別々の環境を作成して実行させる、デュアルペルソナ戦略を使うコンテナがあります。また、コードベースの統合またはアプリケーションラッピングソリューションを通じてアプリケーション自体をコンテナ化するものもあります。どの方法も、ユーザーの生産性にとって障害となります。複数のワークスペースでログインとログアウトを繰り返さなければならなかったり、独自のコードへの依存性を追加することによりオペレーティングシステムのアップデートとの互換性を失うことがあります。

コンテナを使わなくなった組織は、iOSに搭載されている管理コントロールによって、ユーザーの個人的な体験を最適化し、生産性を高められることを実際に目の当たりにしています。デバイスをユーザーにとって仕事にもプライベートにも使いにくいものにするのではなく、ポリシーコントロールを使用して見えないところでシームレスにデータの流れを制御することができます。

企業データの管理

iOSでは、デバイスの機能を制限する必要はありません。主要なテクノロジーがアプリケーション間での企業データの流れを制御し、企業データがユーザー個人のアプリケーションやクラウドサービスに漏れないように保護します。

コンテンツの管理

コンテンツの管理とは、App Storeのアプリケーション、カスタム社内アプリケーション、アカウント、本、ドメインのインストール、構成、管理、削除を対象とします。

- **アプリケーションの管理。** MDMを使ってインストールするアプリケーションは、管理対象アプリケーションと呼ばれます。App Storeの無料アプリケーションや有料アプリケーション、またはカスタム社内アプリケーションのいずれかであり、MDMでワイヤレスにインストールできます。管理対象アプリケーションは機密情報を含むことが多く、ユーザーがダウンロードするアプリケーションよりもさらに細かく制御できます。MDMサーバは管理対象アプリケーションとそれに関連付けられたデータをオンデマンドで削除できるほか、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示することも可能です。また、MDMサーバは、アプリケーションデータがiTunesやiCloudにバックアップされないようにすることができます。
- **アカウントの管理。** MDMによってEメールやその他のアカウントを自動的に設定できるため、ユーザーはすぐにデバイスを使用できるようになります。MDMソリューションプロバイダと社内システム間の統合方法にもよりますが、ユーザー名、Eメールアドレス、該当する場合は認証と署名のための証明書IDもアカウントペイロードにあらかじめ入力しておくことができます。MDMで設定できるアカウントのタイプは、IMAP/POP、CalDAV、照会カレンダー、CardDAV、Exchange ActiveSync、およびLDAPです。
- **本の管理。** MDMを使えば本、ePubブック、およびPDF文書を自動的にユーザーデバイスにプッシュできるので、社員は必要なものをいつも手元に置くことができます。管理対象の本は、管理対象のアプリケーションでしか共有できず、管理対象のアカウントでしかEメール送信できません。不要になった資料は、リモートで削除できます。
- **ドメインの管理。** Safariからのダウンロードは、管理対象のドメインからダウンロードされた場合、管理対象の文書とみなされます。特定のURLとサブドメインを管理することができます。例えば、ユーザーが管理対象のドメインからPDFファイルをダウンロードする際、そのPDFファイルは管理対象の文書の設定すべてに準拠していなければなりません。ドメインに続くパスはデフォルトで管理対象です。

管理配布

管理配布では、MDMソリューションまたはApple Configurator 2を使って、VPPから購入したアプリケーションと本を管理できます。管理配布を有効にするには、まずセキュアなトークンでMDMソリューションとVPPアカウントを関連付ける必要があります。MDMサーバをVPPと連動させたら、アプリケーションをデバイスに直接割り当てます。ユーザーがApple IDを入力する必要はありません。デバイスにアプリケーションをインストールできるようになると、ユーザーに通知が届きます。デバイスが監視モードの場合は、ユーザーに通知されることなく、アプリケーションがデバイスにサイレントでプッシュされます。

MDMソリューションを使ってアプリケーションを完全に制御するには、アプリケーションをデバイスに直接割り当てます。

Managed app configuration

Managed App Configurationでは、MDMがiOSに搭載されているネイティブ管理フレームワークで導入時または導入後にアプリケーションを設定できます。このフレームワークによって、デベロッパはアプリケーションが管理対象としてインストールされた場合に有効となるよう実装された設定について識別することができます。社員はカスタム設定を行わなくても、この方法で設定されたアプリケーションをすぐに使い始めることができます。IT部門は、アプリケーション内の企業データが安全に取り扱われることを保証できます。独自のSDKやアプリケーションラッピングは必要ありません。

アプリケーション開発者が管理対象のアプリケーションの設定を使用して有効化できる機能には、アプリケーションの設定、アプリケーションのバックアップ制限、画面キャプチャの制限、アプリケーションのリモートワイプなどがあります。

AppConfig Communityでは、モバイルオペレーティングシステムのネイティブ機能に関連するツールやベストプラクティスを提供しています。このコミュニティの主要なMDMソリューションプロバイダが確立した標準のスキーマを使えば、すべてのアプリケーションデベロッパはManaged App Configurationに対応できます。コミュニティは、より一貫性のある、オープンかつシンプルな方法でモバイルアプリケーションの設定および保護を実現することで、ビジネスのモバイル化を推進しています。

AppConfig Communityの詳細については、www.appconfig.orgを参照してください。

データの流れを管理

MDMソリューションは、企業データがユーザー個人のアプリケーションやクラウドサービスに漏れないように、企業データを詳細レベルで管理できる機能を提供しています。

- **Managed Open In**。Managed Open Inとは、一連の制限によって管理対象ソースからの添付ファイルや文書を管理対象でない出力先で開けないようにする機能です。反対に、管理対象でないソースからの添付ファイルや文書を管理対象の出力先で開くこともできません。例えば、組織が管理するEメールアカウントに添付された機密情報を、ユーザー個人のアプリケーションで開くことはできません。MDMによってインストールおよび管理されているアプリケーションだけが、この仕事用の文書を開くことができます。管理されていない個人のアプリケーションは、添付ファイルを開く際の選択可能なアプリケーションのリストに表示されません。Managed Open Inによる制限は、管理対象のアプリケーション、アカウント、本、およびドメインのほかに、いくつかのExtensionに対しても効力があります。

企業データを保護するため、MDMによってインストールおよび管理されるアプリケーションでのみこの仕事用の書類を開くことができます。

- **Managed Extension**。App Extensionにより、サードパーティデベロッパはほかのアプリケーションやiOSに内蔵された主要システム（通知センターなど）に機能を提供でき、アプリケーション間の新しいビジネスワークフローを実現できます。Managed Open Inを使うと、管理されていないExtensionは管理対象アプリケーションとやり取りできなくなります。以下は、様々なExtensionのタイプの例です。
  - **ドキュメントプロバイダExtension** を使うと、仕事効率化アプリケーションは不要なコピーを作成することなく、様々なクラウドサービスから文書を開くことができます。
  - **Action Extension** を使うと、ユーザーはほかのアプリケーションのコンテキスト内でコンテンツの操作や表示ができます。例えば、Safari上で表示された文字を翻訳する時にこのアクションを使うことができます。
  - **カスタムキーボードExtension** では、iOSに内蔵されたキーボード以外のキーボードが使えるようになります。Managed Open Inにより、承認されていないキーボードを企業アプリケーションで使用できないようにすることが可能です。
  - **Today Extension** はウィジェットとも呼ばれ、通知センターの「今日」表示に、ひと目でわかる情報を配信するために使用されます。これは、ユーザーがアプリケーションの最新情報をすぐに確認でき、シンプルな操作でアプリケーションを起動して詳細情報を確認できる、優れた方法です。
  - **Share Extension** は、情報投稿サイト、アップロードサービスなどを利用し、情報を共有するための便利な手段を提供します。例えば、共有ボタンがあるアプリケーションで、ユーザーは情報投稿ウェブサイトを表すShare Extensionを選択してコメントなどのコンテンツを投稿できます。

柔軟な管理オプション

Appleの管理フレームワークには柔軟性があり、エンタープライズでのユーザー所有および企業所有のデバイスを管理するための、バランスの取れたアプローチを提供します。iOSと共にサードパーティ製のMDMソリューションを使う場合、非常にオープンな方法を採用するものから必要に応じた精度の管理を行うものまで、幅広いデバイス管理オプションがあります。

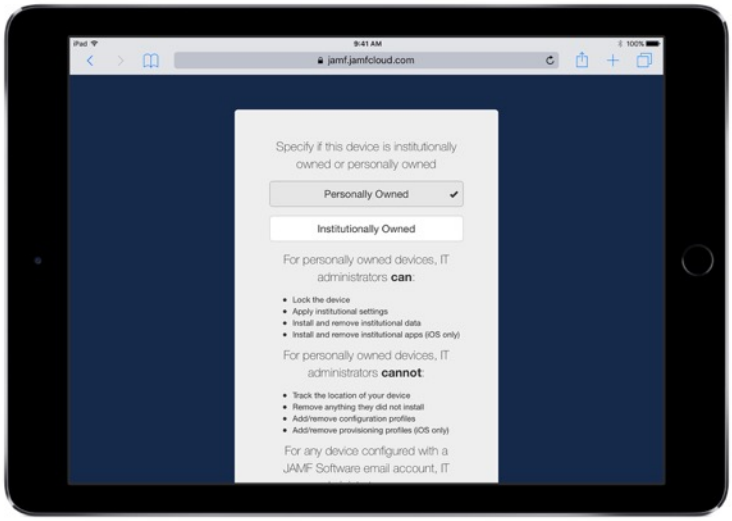
所有モデル

組織におけるデバイスの所有モデルによって、デバイスとアプリケーションの管理方法が異なります。通常、エンタープライズで採用されるiOSデバイスの所有モデルは、ユーザー所有と企業所有の2つです。

ユーザー所有のデバイス

ユーザー所有のデバイスにおける導入について、iOSはユーザーによるパーソナライズされた設定およびデバイスの設定方法に関する透明性を提供します。また、組織が個人のデータにアクセスしないことが保証されます。

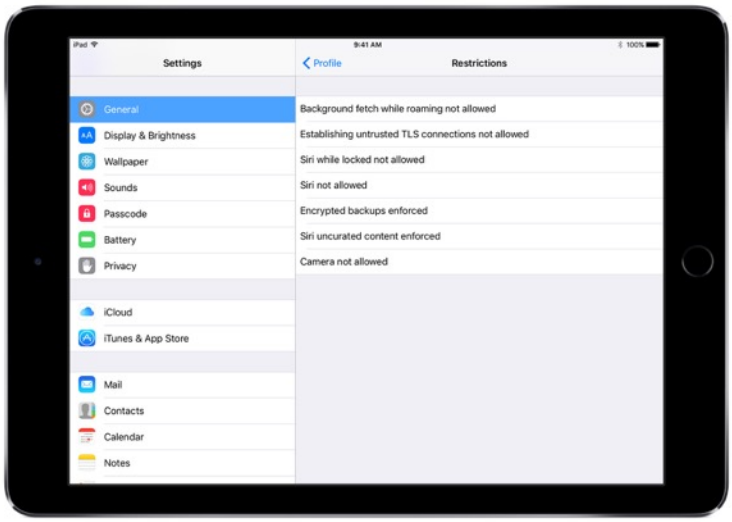
- **オプトイン／オプトアウト方式の登録。**ユーザーがデバイスを購入して設定する場合（一般にBYODと呼ばれる方法）でも、Wi-Fi、Eメール、カレンダーといった企業向けサービスへのアクセスを提供できます。ユーザーは、組織のMDMソリューションへの登録をオプトインするだけです。iOSデバイスでMDMに初めて登録すると、ユーザーのデバイスでMDMサーバがアクセスできる対象や、構成する機能に関する情報が提供されます。これによって、ユーザーは何が管理されているかを把握でき、組織とユーザーとの信頼関係が確立されます。管理が不要になった場合は、いつでもユーザーがデバイスから管理プロファイルを削除することによってオプトアウトできることをユーザーに伝えることが重要です。ユーザーがオプトアウトすると、MDMによってインストールされた企業のアカウントとアプリケーションがすべて削除されます。



サードパーティ製のMDMソリューションは通常、社員が使いやすいインターフェイスを提供しているため、安心して登録をオプトインできます。*

*画面は、Jamfより転載を許可していただいたものです。

- **透明性の向上。**MDMに登録すると、社員は設定からどのアプリケーション、本、アカウントが管理されているか、どのような制限が課されているかを簡単に見ることができます。MDMによってインストールされたすべてのエンタープライズ設定、アカウント、およびコンテンツには管理対象のフラグがiOSによって設定されます。



設定内の構成プロファイルのユーザーインターフェイスは、デバイスで何が設定されているかを具体的に表示します。

- **ユーザーのプライバシー。**IT部門はMDMサーバを使ってiOSデバイスとやり取りできますが、すべての設定とアカウント情報が公開されるわけではありません。MDMによってプロビジョニングされた企業のアカウント、設定、および情報は管理できますが、ユーザー個人のアカウントにはアクセスできません。実際には、企業が管理するアプリケーション内のデータを保護する機能によって、ユーザーの個人的なコンテンツが企業のデータストリームに入らないようにしています。

  以下の例は、サードパーティ製MDMサーバが個人のiOSデバイス上の何を表示でき、何を表示できないかを示しています。

MDMから確認できる内容	MDMからは確認できない内容
デバイス名	個人または業務に関するEメール、カレンダー、連絡先
電話番号	SMSやiMessage
シリアル番号	Safariの履歴
モデル名と番号	FaceTimeまたは電話の通話履歴
容量と使用可能な空き領域	個人のリマインダーとメモ
iOSのバージョン番号	アプリケーションの利用頻度
インストールされたアプリケーション	デバイスの位置情報

- **デバイスのパーソナライズ。**企業は、ユーザーが自分のApple IDを使ってデバイスをパーソナライズできるようにすることによって、デバイスに対するユーザーの所有権と責任が大きくなり、自分が仕事をやり遂げるのに最適なアプリケーションやコンテンツを選ぶことができるので生産性が向上するということに気付いています。

企業所有のデバイス

企業所有の導入では、各ユーザーにデバイスを提供するパーソナライズの導入、または複数のユーザーがローテーションでデバイスを使用する非パーソナライズの導入があります。自動登録、ロック可能なMDM設定、監視モード、常時接続VPNなどのiOS機能は、デバイスが企業固有の要件に基づいて設定されていることを確実にし、企業データが保護されていることを保証しながらコントロールを強化します。

- **自動登録。** Device Enrollment Program（DEP）によって、企業が所有するiPhoneデバイス、iPadデバイス、Macシステムの初期設定時のMDM登録を自動化できます。登録を必須にし、解除できないようにすることや、登録時にデバイスを監視モードにすること、ユーザーが基本的な設定手順をスキップできるようにすることができます。

DEPを使うと、iOSデバイスはMDMソリューションにより、設定アシスタントで自動的に構成されます。

- **監視モードのデバイス。** 監視モードは、企業所有のiOSデバイスに追加の管理機能を提供します。グローバルプロキシによってウェブフィルタリングを有効化してユーザーのウェブトラフィックが組織のガイドラインから逸脱しないようにしたり、ユーザーがデバイスを出荷時の設定にリセットできないようにしたりできます。デフォルトでは、iOSデバイスはすべて監視モードではありません。DEPから、もしくはApple Configurator 2を使って手動で有効化できます。

現時点で監視モード専用の機能を使う予定がなくても、設定時にデバイスを監視モードにして、そうした機能を利用することも将来的には検討してください。監視モードを使用しない場合、導入済みのデバイスをワイプしなければならなくなります。監視モードはデバイスの機能を制限するものではなく、管理機能を拡張することによって企業所有のデバイスの使用をより良くさせるものです。監視モードは長期的に、企業により多くのオプションを提供します。

監視モードの設定についての詳細は、iOS導入リファレンスを参照してください。

機能制限

iOSは以下のカテゴリの機能制限に対応しています。IT部門は、組織のニーズに応じてワイヤレスでこれらの機能制限を設定できます。ユーザーの操作は必要ありません。

- デバイスの機能
- 監視モードの設定
- セキュリティとプライバシーの設定
- アプリケーションの使用
- iCloudの設定
- プロファイルマネージャのユーザーとユーザーグループの制限

以下のカテゴリは、DEPを使用してMDMソリューションに登録されたiOSデバイスに適用されます。

- 登録オプション
- 設定アシスタントのオプション

その他の管理機能

デバイスのクエリ

デバイスの構成だけでなく、MDMサーバはデバイスの様々な情報を問い合わせることができます。この情報には、デバイスの詳細、ネットワーク、アプリケーションID、コンプライアンスやセキュリティデータなどが含まれます。この情報によって、デバイスが必要なポリシーに常に準拠していることを確認できます。MDMサーバは、情報を収集する頻度を決定します。

以下は、iOSデバイスでクエリできる情報の例です。

- デバイスの詳細（名前）
- モデル、iOSのバージョン、シリアル番号
- ネットワーク情報
- ローミングの状況、MACアドレス
- インストールされているアプリケーション
- アプリケーション名、バージョン、サイズ
- 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設定、ポリシー、証明書
- 暗号化の状態

紛失モード

iOS 9.3以降では、MDMソリューションが監視モードのデバイスをリモートで紛失モードにできます。この操作を行うとデバイスはロックされ、ロック画面に電話番号を含むメッセージを表示できます。

紛失モードでは、MDMがデバイスの位置をクエリするので、紛失または盗難に遭った監視モードのデバイスの位置を特定できます。「iPhoneを探す」が有効になっていなくても紛失モードを使うことができます。

MDMがリモートで紛失モードを無効にすると、デバイスのロックが解除され、その位置情報が収集されます。透明性を維持するため、紛失モードがオフになったことがユーザーに通知されます。

紛失したデバイスを
MDMが紛失モードにすると、
デバイスはロックされ、
画面にメッセージを
表示したり、デバイスの
現在地を特定したりできます。

アクティベーションロック

iOS 7.1以降では、MDMを使って、監視モードのデバイスでユーザーが「iPhoneを探す」を有効にした場合にアクティベーションロックを有効にできます。これにより、組織はアクティベーションロックの盗難抑止機能を利用できます。ユーザーがApple IDを使ってアクティベーションロックを削除せずに退職 してしまった場合などでも、この機能をバイパスすることができます。

MDMソリューションはバイパスコードを取得でき、ユーザーはデバイスのアクティベーションロックを次のように有効化できます。

- MDMソリューションがアクティベーションロックを許可している時に「iPhoneを探す」を有効にすると、その時点でアクティベーションロックが有効になります。
- MDMソリューションがアクティベーションロックを許可している時に「iPhoneを探す」が無効化されていると、次にユーザーが「iPhoneを探す」を有効にした時にアクティベーションロックが有効になります。

まとめ

iOSの管理フレームワークにより、企業とユーザーの両者にとって最適な結果がもたらされます。IT部門はデバイスを設定、管理、保護したり、デバイスを経由する企業データをコントロールできます。同時に、ユーザーは使い慣れたデバイスで素晴らしい仕事をするための支持を得られます。