



概要

iOSの導入

概要

目次

概要

所有モデル

導入の手順

サポートオプション

まとめ

iPhoneとiPadは、ビジネスと社員の働き方を変革することができます。生産性が大幅に向上し、社員がオフィスにいても、外出先でも、業務をまったく新しい方法で自由に進められるように、柔軟性を提供します。この新しい働き方を取り入れることによって、組織全体にメリットがもたらされます。ユーザーは情報にアクセスしやすくなるので、能力を高め、クリエイティブに問題を解決できるようになります。IT部門はiOSをサポートすることによって、テクノロジーの修正やコストの削減を行うだけでなく、ビジネス戦略を立てて現実的な問題の解決に取り組む部門に変わります。最終的に、すべての人にメリットがもたらされます。社員は活性化し、新しいビジネス機会があらゆる場所で生まれます。

iPhoneとiPadの設定と導入は、これまで以上に簡単になりました。Apple Business Managerと他社製のモバイルデバイス管理ソリューションを使用し、iOSデバイスとアプリケーションの大規模な導入を簡単に行うことができます。

- モバイルデバイス管理 (MDM) を利用すると、デバイスの構成と管理のほか、アプリケーションをワイヤレスで配布および管理できます。
- Apple Business Managerを利用すると、AppleのデバイスのMDMソリューションへの登録を自動化し、IT部門がデバイスに触れることなく構成を行って導入の効率を高めることができます。
- Apple Business Managerを利用すると、アプリケーションや本を一括購入してユーザーにワイヤレスで配付することもできます。

この文書では、組織にiOSデバイスを導入するためのガイダンスを提供します。また、組織の環境に最適な導入計画の作成をサポートします。この概要の「導入の手順」セクションに記載されているプログラムおよびツールの詳細については、オンラインのiOS導入リファレンスhelp.apple.com/deployment/ios/?lang=jaで説明しています。

所有モデル

導入の最初のステップとして重要なのは、所有モデルの評価と、組織に適したモデルの選択です。デバイスを誰が所有するかによって、いくつかのアプローチがあります。まずは、あなたの組織に最適な方法を特定することから始めましょう。

エンタープライズで使用するiOSデバイスの所有モデルは、通常次の2つです。

- 組織所有
- ユーザー所有

ほとんどの組織には推奨モデルがありますが、組織の環境によっては複数のモデルを使用することも考えられます。例えば、ある企業ではオフィスでユーザー所有の戦略を採用し、社員が個人のiPadを設定できるようにしています。ただし同時に、ユーザー個人のデータやアプリケーションに影響を与えることなく企業の情報を保護および管理しています。一方、この企業の小売店舗では組織所有のモデルを使用し、複数の社員でiOSデバイスを共有しながらお客様との取引を処理しています。

これらのモデルを詳しく知れば、あなたの組織の環境に最適な選択肢を見つけやすくなるでしょう。組織に最適なモデルを特定できたら、Appleの導入と管理機能についての詳細をチームで確認してください。

組織所有のデバイス

組織所有モデルを採用する場合、デバイスはAppleまたはApple正規取扱店が通信事業者から購入することができます。この場合、各ユーザーに1台のデバイス（パーソナライズを行う導入）、またはユーザー間で共有するデバイス（パーソナライズを行わない導入）を選択することができます。これらのモデル、Appleの主要なテクノロジー、およびMDMソリューションを組み合わせることによって、デバイスの設定と構成を完全に自動化できます。

パーソナライズを行う。 パーソナライズを行う方法の場合、組織の設定やアプリケーションをワイヤレスで提供するMDMソリューションを利用して、ユーザーに各自のデバイスを登録してもらうことができます。AppleまたはApple正規取扱店が通信事業者から直接購入したデバイスなら、Apple Business Managerを利用して新しいデバイスをMDMソリューションに自動的に登録することもできます。構成が完了すると、ユーザーは組織が提供するアカウントやアプリケーションのほか、自分のアプリケーションやデータでデバイスをパーソナライズすることもできます。

パーソナライズを行わない。 数名でデバイスを共有する場合、またはデバイスが1つの目的に使用される場合（レストランやホテルなど）は、通常IT管理者が中心となってデバイスの構成と管理を行うので、ユーザーが個々に設定を行うことはありません。パーソナライズを行わないデバイスの導入では、一般的にユーザーがアプリケーションをインストールしたり、個人のデータを保存したりすることは許可されません。次ページの表では、組織所有の戦略において管理者とユーザーが必要とする操作をステップ別にまとめています。特に記載がない限り、操作はパーソナライズを行う導入とパーソナライズを行わない導入の両方にあてはまります。

	管理者	ユーザー
準備	- インフラストラクチャの評価 - MDMソリューションの選択 - Apple Business Managerに登録	ユーザーの操作は不要
設定	- デバイスの構成 - アプリケーションや本の配布	ユーザーの操作は不要
導入	- デバイスを配布 パーソナライズを行う場合のみ - ユーザーによるパーソナライズを許可	パーソナライズを行う場合のみ - アプリケーションや本のダウンロードおよびインストール - 該当する場合は、Apple ID、iTunes Store、およびiCloudのアカウントを使用 パーソナライズを行わない場合のみ - ユーザーの操作は不要
管理	- デバイスの管理 - 追加コンテンツの導入および管理	パーソナライズを行う場合のみ - 使用する追加アプリケーションを発見 パーソナライズを行わない場合のみ - ユーザーの操作は不要

ユーザー所有のデバイス

ユーザーがデバイスを購入して設定を行う場合、一般的にBYOD（個人デバイスの持ち込みによる導入）と呼ばれます。この導入ではMDMを利用し、Wi-Fi、Eメール、カレンダーといった企業の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ソリューションへ登録する必要があります。

BYOD。BYODの導入では、ユーザーは自分のデバイスを設定して構成できます。ユーザーが自分のデバイスを組織のMDMソリューションに登録すると、企業のリソースへのアクセス、様々な設定、構成プロファイルや企業アプリケーションのインストールが可能になります。

MDMで個人のデバイスを登録するメリットは、ユーザーのプライバシー、データ、アプリケーションを尊重しながら企業のリソースとデータを安全に管理できるという点です。IT部門は、ユーザーのデバイス上の個人データやアプリケーションに影響を与えることなく、設定の適用、ポリシーへの準拠の監視、企業のデータやアプリケーションの削除ができます。

以下の表では、ユーザー所有の導入の各ステップで、管理者とユーザーに必要な操作をまとめています。

	管理者	ユーザー
準備	- インフラストラクチャの評価 - MDMソリューションの選択 - Apple Business Managerに登録	該当する場合は、Apple ID、iTunes Store、およびiCloudのアカウントを使用
設定	- デバイスの構成 - アプリケーションや本の配布	- 企業のMDMソリューションへの登録を承認 - アプリケーションや本のダウンロードおよびインストール
導入	管理者の操作は不要	ユーザーの操作は不要
管理	- デバイスの管理 - 追加コンテンツの導入および管理	使用する追加アプリケーションを発見

導入の手順

このセクションではデバイスとコンテンツを導入するための環境の準備、デバイスの設定、デバイスの導入、デバイスの管理の4つの手順をより詳しく説明します。手順は、デバイスの所有者が組織かユーザーかによって変わります。

1. 準備する

組織に適した導入モデルを特定できたら、以下の手順に従って導入の基盤を整えます。

この準備は、デバイスが手元に届く前でも行うことができます。

インフラストラクチャの評価

iPhoneとiPadは、企業の最も標準的なIT環境にシームレスに統合できます。既存のネットワークインフラストラクチャを評価して、iOSが提供するメリットを組織がすべて活用できるようにすることが重要です。

Wi-Fiとネットワーク機能

一貫性があり、信頼性の高いワイヤレスネットワークへのアクセスは、iOSデバイスの設定と構成に不可欠です。複数のデバイスからユーザー全員が同時に、企業のWi-Fiネットワークに接続可能であることを確認してください。デバイスがAppleのアクティベーションサーバ、iCloud、iTunes Storeにアクセスできない場合は、ウェブプロキシやファイアウォールのポートを構成しなければならないことがあります。AppleとCiscoは、iPhoneとiPadがCiscoのワイヤレスネットワークと通信する方法を最適化し、その他にも高速ローミングやアプリケーションのためのQuality of Service (QoS) の最適化といった先進的なネットワーキング機能のための方法を確立しました。

お使いのVPNインフラストラクチャを評価して、ユーザーがiOSデバイスからリモートで企業リソースに安全にアクセスできることを確認します。必要な場合にのみVPN接続を開始できるように、iOSのVPNオンデマンドまたはPer-App VPNの機能を利用することを検討してください。Per-App VPNを利用する場合は、お使いのVPNゲートウェイがこれらの機能をサポートしていることを確認し、ユーザー数と接続数の適切な数に対応できる十分なライセンスを購入していることを確認します。

また、ネットワークインフラストラクチャで、Appleの標準ベースのゼロ構成ネットワークプロトコルであるBonjourが、正しく動作するように設定されていることも確認する必要があります。Bonjourによって、デバイスがネットワーク上のサービスを自動的に検出できます。iOSデバイスは、Bonjourを使ってAirPrint対応のプリンタやApple TVのようなAirPlay対応のデバイスに接続することができます。アプリケーションの中には、Bonjourを使用してほかのデバイスを検出し、共同作業や共有を行うものもあります。

企業の導入におけるWi-Fiとネットワークの詳細については、iOS導入リファレンス help.apple.com/deployment/ios/?lang=jaを参照してください。

Bonjourについてさらに詳しく：
apple.com/jp/support/bonjour

Eメール、連絡先、カレンダー

Microsoft Exchangeをご利用の場合は、ActiveSyncサービスが最新で、ネットワークのすべてのユーザーをサポートするよう構成されているか確認してください。クラウドベースのOffice 365を使用している場合は、接続が見込まれるiOSデバイスの数をサポートできる十分なライセンスがあることを確認します。iOSは、OAuth 2.0と多要素認証を利用したOffice 365の先進認証にも対応しています。Exchangeを使用していない場合でも、iOSはIMAP、POP、SMTP、CalDAV、CardDAV、LDAPなど、標準ベースのサーバに対応しています。

コンテンツキャッシュ

コンテンツキャッシュはmacOS High Sierra以降に統合されている機能です。頻繁にリクエストされるAppleサーバからのコンテンツのローカルコピーを保存し、ネットワークでコンテンツのダウンロードに必要な帯域を節約するのに役立ちます。コンテンツキャッシュは、App Store、Mac App Store、iTunes Store、Apple Booksを介したソフトウェアのダウンロードと配布をスピードアップします。

また、ソフトウェアアップデートもキャッシュするため、iOSデバイスにさらに高速にダウンロードできます。コンテンツキャッシュには、テザリングキャッシュサービスが含まれます。このサービスにより、MacはUSB経由で接続された多数のiOSデバイスとインターネット接続を共有できます。

コンテンツキャッシュについてさらに詳しく：

support.apple.com/ja-jp/HT208025

テザリングキャッシュについてさらに詳しく：

support.apple.com/ja-jp/HT207523

iTunesのサポート

iTunesはiOS 5以降のデバイスでは必須ではなくなりましたが、デバイスのアクティベート、メディアの同期、コンピュータへのデバイスのバックアップが行えるため、サポートすることをおすすめします。

iTunesはエンタープライズでの利用に適した導入の構成オプションをいくつかサポートしています。不適切なコンテンツへのアクセスを無効にしたり、ユーザーがiTunes内でアクセスできるネットワークサービスを定義したりするほか、強制的にバックアップを暗号化することもできます。

MDMソリューションの選択

AppleのiOS用の管理フレームワークを利用すると、企業環境でのデバイスの安全な登録やワイヤレスでの設定とアップデート、ポリシーへの準拠の監視、アプリケーションや本の導入、管理対象のデバイスのリモートワイプやロックなどを行うことができます。これらの管理機能は、他社製のMDMソリューションによって提供されます。

様々なサーバプラットフォーム用にいろいろなMDMソリューションが用意されています。提供される管理コンソール、機能、価格は、ソリューションごとに異なります。ソリューションを選択する前に、以下にまとめたリソースを参照して、組織にとって最も重要な管理機能を評価してください。他社製のMDMソリューションのほかに、AppleはプロファイルマネージャというソリューションをmacOS Serverの機能として提供しています。

iOSでのデバイスと企業データの管理についてさらに詳しく：

images.apple.com/jp/business/resources/docs/Managing_Devices_and_Corporate_Data_on_iOS.pdf

プロファイルマネージャについてさらに詳しく：

www.apple.com/jp/macOS/server/features/#profile-manager

Apple Business Managerに登録

Apple Business Managerは、IT部門がデバイス導入の自動化、コンテンツの購入と配布、組織内での役割を管理できる新しいポータルです。既存のモバイルデバイス管理 (MDM) ソリューションとシームレスに連携することで、Apple Business Managerでは、デバイスの登録、コンテンツの導入、管理者権限の委任を簡単に行うことができます。

Device Enrollment Program (DEP) と Volume Purchase Program (VPP) が Apple Business Manager にシームレスに統合され、iOS デバイス、Mac コンピュータ、Apple TV を組織に導入するために必要なものがすべて1か所に集まりました。

デバイス

Apple Business Manager に引き継がれたデバイス登録機能により、企業が所有する Apple デバイスをすばやく効率的に導入できます。

- ユーザーに渡す前に、デバイスに触れたり準備したりする必要がなく、MDM に自動的に登録できます。そのため、ユーザーがデバイスをアクティベートすると同時に、組織の構成が確実に適用されます。
- 設定アシスタントの特定のステップを省略して、ユーザーの設定プロセスを簡略化することで、ユーザーがデバイスをすぐに使えるようにします。また、iOS デバイスや tvOS デバイスでは、監視モードを使うことで、高度なデバイス管理オプション (削除不可の MDM など) が利用できるようになります。
- デバイスの種類に応じてデフォルトのサーバを設定することで、デフォルトの MDM サーバがさらに管理しやすくなります。また、Apple Configurator 2 を使用することで、購入方法にかかわらず iOS デバイスと Apple TV を手動で登録できるようになりました。

コンテンツ

Apple Business Manager の「App とブック」セクションで、コンテンツを簡単に一括購入できるようになりました。社員が使用しているのが iPhone でも、iPad でも、Mac でも、フレキシブルでセキュアな配布方法を利用して、すぐに使える優れたコンテンツを提供できます。注意：一部の国では、Apple Business Manager を使って本を購入することができません。国や地域ごとに利用可能な機能と購入方法について、詳しくは support.apple.com/ja-jp/HT207305 を参照してください。

- アプリケーションや本、カスタムアプリケーションを一括購入できます。ある場所から別の場所へアプリケーションのライセンスを転送したり、ライセンスを同じ場所の購入担当者間で共有したりできます。また、MDM で使用中のライセンスの数を含め、購入履歴をまとめて一覧表示することも可能です。
- 管理対象デバイスまたは承認済みユーザーにアプリケーションや本を直接配布し、どのコンテンツがどのユーザーやデバイスに割り当てられているかを簡単に把握することができます。管理配布により、組織がアプリケーションの所有権を完全に保持したまま、配布プロセス全体をコントロールできます。さらに、デバイスまたはユーザーが必要としなくなったアプリケーションは、割り当てを無効にし、組織内の別のデバイスまたはユーザーに割り当て直すことができます。
- 支払いには、クレジットカードや発注書など、複数の支払い方法を利用できます。組織は一定の金額の Volume Credit を Apple または Apple 正規取扱店から直接購入でき、購入した Volume Credit はアカウントの所有者にストアクレジットとして電子的に届けられます。
- アプリケーションは、そのアプリケーションが利用可能な国なら、どの国のデバイスやユーザーにも配布できるので、複数の国への配布が可能です。デベロッパは App Store で通常の公開手続きをするだけで、複数の国でアプリケーションを提供できます。

役割

Apple Business Managerでは、組織で所有および管理する複数の管理者用アカウントを追加作成できます。また、ユーザーに割り当てる役割にも、いくつかの変更が加えられています。

- デバイスやコンテンツの管理を行うアカウントを追加できるほか、権限の委任や、離職した人の職責の移行を簡単に行うことができます。
- Apple Business Manager内で役割を細かく指定することにより、デバイスやコンテンツの管理権限を特定の人や場所に割り当てることができます。
- 特定のユーザーがサインインできないように、ユーザーアカウントの無効化や削除ができます。

Apple Deployment Programでは、アクセス権の最上位は「エージェント」でした。エージェントは、組織を代表して利用規約を承諾することができました。Apple Business Managerでは、この役割を「管理者」と呼びます。Apple Business Managerでは、1つの組織に5名まで管理者を指定できます。

Apple Deployment Programには、DEPとVPPの「管理者」がいました。Apple Business Managerでは、この管理者を「マネージャ」と呼びます。アップグレードを行うと、DEPの管理者は「デバイスマネージャ」に、VPPの管理者は「コンテンツマネージャ」に置き換えられます。Apple Deployment Programにおいて、ほかの管理者を作成する権限を持っていた管理者は、「ユーザマネージャ」となります。

Apple Business Managerでは、1人のユーザーが複数の役割を持つことができます。複数のプログラムの管理者だったユーザーには、Apple Business Managerで該当する役割がすべて割り当てられます。アップグレード後は、管理者がマネージャの役割の追加、取り消し、変更を行うことができます。ユーザマネージャも、その他のマネージャの役割を変更することができますが、管理者の役割は変更できません。

これまでエージェントや管理者だったアカウントでApple Business Managerにはじめてログインすると、アカウントのApple IDが管理対象Apple IDに変換されます。そのアカウントに2ファクタ認証が設定されていなかった場合は、2ファクタ認証を設定するように要求されます。

管理対象Apple IDは、主にIT管理者がApple Business Managerの機能を管理するために使うものです。iCloudなどのサービスに使ったり、Apple Business Managerの機能の管理とは関係がない一般社員に使用したりしないでください。

Apple Business Managerについてさらに詳しく：

www.apple.com/jp/business/it

Apple Developer Enterprise Programに登録

Apple Developer Enterprise Programに参加すると、社内用iOSアプリケーションを自社で開発できます。このプログラムでは、iOSアプリケーションの開発、テストから、組織内の社員への配布まで、一貫した統合プロセスを提供します。社内用アプリケーションはApp Storeへの提出はせず、Appleによるレビュー、承認、ホストは行われません。

社内アプリケーションは、シンプルな社内ウェブサーバでアプリケーションをホストして配布することも、他社製のMDMソリューションを利用して配布することもできます。MDMを利用して社内アプリケーションを管理するメリットとして、リモートでのアプリケーション構成、バージョンの管理、シングルサインオンの構成や、Per-App VPNなどのネットワークアクセスに対するポリシーの設定、書類をエクスポートできるアプリケーションの制御などが挙げられます。具体的な要件やインフラストラクチャ、必要とするアプリケーションの管理のレベルによって、最も有効なソリューションを決定します。

Apple Developer Enterprise Programについてさらに詳しく：

developer.apple.com/programs/enterprise/jp/

2. 設定する

この手順では、Apple Business Manager、MDMソリューション、またはオプションでApple Configurator 2を利用してデバイスの設定とコンテンツの配布を行います。デバイスの所有者および希望する導入のタイプによって、いくつかのアプローチ方法があります。

自分のデバイスを構成

企業のサービスへのユーザーアクセスを構成するために、複数のオプションを利用することができます。IT部門は、構成プロファイルを配布することによってデバイスを設定できます。監視モードのデバイスでは、追加の構成オプションを利用できます。

MDMを使ったデバイスの構成

デバイスが安全にMDMサーバに登録されると、構成プロファイルによる管理が有効になります。構成プロファイルは、iOSデバイス向けの構成情報が含まれているXMLファイルです。これらのプロファイルにより、設定、アカウント、機能制限、資格情報の構成が自動化されます。手間をかけずに複数のデバイスを構成するには、MDMソリューションから構成プロファイルをワイヤレスで配布するのが最適な方法です。また、プロファイルはEメールの添付ファイルとして送信したり、ウェブページからダウンロードしたり、Apple Configurator 2を使用してデバイスにインストールすることもできます。

- **組織所有のデバイス。**Apple Business Managerを利用して、アクティベーション時にユーザーのデバイスをMDMに自動登録することができます。Apple Business Managerに追加されたすべてのiOSデバイスは、MDMの登録が必須で、常に監視モードになります。
- **ユーザー所有のデバイス。**社員は自分のデバイスをMDMに登録するか自分で決めることができます。また、デバイスから構成プロファイルを削除すれば、いつでもMDMとの関連を解除できます。この際、企業データと設定も削除されます。ただし、組織はユーザーの登録継続を促進する仕組みを考える必要があります。例えば、MDMソリューションを使用して自動的にワイヤレスの資格情報を提供することで、Wi-FiネットワークにアクセスするためにユーザーにMDMへの登録を求めることができます。

デバイスが登録されたら、管理者はMDMポリシー、オプション、またはコマンドを開始できます。iOSデバイスはAppleプッシュ通知サービス (APNs) により管理者のアクションに関する通知を受信し、安全な接続を使ってMDMサーバと直接通信することができます。デバイスはネットワーク接続を利用して、世界中のどこにいてもAPNsコマンドを受信できます。ただし、秘密情報はAPNsでは送信されません。

Apple Configurator 2でデバイスを設定 (オプション)

複数のデバイスをローカル環境で初期導入する場合は、Apple Configurator 2を利用できます。この無料のmacOSアプリケーションによって、iOSデバイスをUSB経由でMacコンピュータに接続し、iOSデバイスを最新バージョンにアップデートしたり、デバイスの設定と制限を設定したり、アプリケーションとその他のコンテンツをインストールしたりすることが可能です。初期設定後は、MDMを使用してワイヤレスで継続的に管理することができます。

Apple Configurator 2のユーザーインターフェイスによって、デバイスと、デバイスで実行したい様々なタスクに集中することができます。Apple Business Managerと統合されているので、組織の設定によりデバイスをMDMに自動的に登録することができます。ブループリントで個々のタスクを組み合わせながら、Apple Configurator 2内でカスタムワークフローを作成することができます。

Apple Configurator 2についてさらに詳しく：

support.apple.com/ja-jp/apple-configurator

監視モードのデバイス

監視モードは、組織が所有するiOSデバイスに追加の管理機能を提供します。AirDropを無効にしたり、デバイスをシングルAppモードにしたりするなどの制限を可能にします。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もできます。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。Apple Business Managerで監視モードを有効化したり、Apple Configurator 2を使って手動で有効にしたりできます。

現時点では監視モードのみの機能を使う予定がなくても、デバイスを監視モードに設定して配布することを検討してください。これにより、将来的に監視モードのみの機能を導入できるメリットがあります。監視モードを使用しなかった場合、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全体を停止するものではなく、むしろ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。監視モードに設定することによって、企業は長期的により多くの選択肢を得られます。

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。

アプリケーションや本の配布

Appleは多岐にわたるプログラムを提供し、iOSで使用可能な魅力的なアプリケーションやコンテンツを組織がうまく活用できるようにサポートしています。こうした機能を活用し、Apple Business Managerで購入したアプリケーションや本、または社内開発したアプリケーションをデバイスやユーザーに配布することが可能です。ユーザーは生産性を高めるために必要なものをすべて入手することができます。購入時、配布方法として管理配布か引き換えコードのいずれかを選択してください。

管理配布

管理配布では、MDMソリューションまたはApple Configurator 2を利用して、アプリケーションを使用できる国のApple Business Managerで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Apple Business Managerアカウントを関連付ける必要があります。MDMサーバに接続されると、デバイスでApp Storeが無効になっていても、Apple Business Managerのアプリケーションと本を割り当てることができます。

- **アプリケーションをデバイスに割り当てる。**MDMソリューションまたはApple Configurator 2を利用して、アプリケーションをデバイスに直接割り当てます。この方法により、初期ロールアウトでのいくつかの手順を省くことができるので、導入が非常に簡単かつ迅速になり、管理対象のデバイスおよびコンテンツを完全に制御できます。アプリケーションがデバイスに割り当てられると、MDMを通じてデバイスにアプリケーションがプッシュされます。ユーザーを招待する必要はありません。そのデバイスを使用するユーザーは、誰でもアプリケーションにアクセスすることができます。
- **アプリケーションや本をユーザーに割り当てる。**その他の方法として、MDMソリューションを使用して、Eメールやプッシュ通知のメッセージでユーザーにアプリケーションや本をダウンロードするよう招待します。ユーザーが招待を承諾するには、個人のApple IDを使ってデバイスにサインインします。Apple IDはApple Business Managerサービスに登録されますが、公開されることはなく、管理者にも表示されません。ユーザーが招待を承諾すると、MDMサーバに接続され、自分に割り当てられたアプリケーションと本を受け取ることができます。アプリケーションはユーザーのすべてのデバイスで自動的にダウンロード可能となるので、管理者が操作する必要はなく、コストも一切かかりません。

デバイスまたはユーザーが割り当てられたアプリケーションを必要としなくなった場合は、割り当てを無効にして別のデバイスまたはユーザーに割り当て直すこともできます。組織は購入したアプリケーションの完全な所有権を持ち、それらを管理することができます。ただし、本は一度配布されると、受け取った人の所有物となり、割り当てを無効にしたり、割り当て直したりすることはできません。

引き換えコード

コンテンツの配布に、引き換えコードを使用することもできます。これは、組織がエンドユーザーのデバイスでMDMを使用できない場合に役立ちます。例えば、フランチャイズビジネスのシナリオの場合です。この方法では、アプリケーションや本の所有権が、コードを引き換えるユーザーに完全に移行します。引き換えコードはスプレッドシート形式で提供され、購入したアプリケーションまたは本のそれぞれにつき、固有のコードが1つずつ与えられます。コードが使用されるたびにApple Business Managerのスプレッドシートが更新されるので、引き換えられたコードの数をいつでも確認できます。コードの配布には、MDM、Apple Configurator 2、Eメール、または社内ウェブサイトを使用します。

Apple Configurator 2を使ってアプリケーションやコンテンツをインストール(オプション)

Apple Configurator 2を使用すると、基本的な設定や構成ができるだけでなく、ユーザーに代わって設定対象のデバイスにアプリケーションやコンテンツをインストールすることができます。パーソナライズを行う導入の場合、アプリケーションをあらかじめインストールすることで時間とネットワーク帯域幅を節約できます。また、パーソナライズを行わない導入では、デバイスにホーム画面に至るまでのすべてを設定することができます。Apple Configurator 2を使用してアプリケーションを構成すると、App Storeのアプリケーション、社内アプリケーション、書類をインストールできます。App Storeのアプリケーションの場合は、Apple Business Managerが必要です。書類はiTunesファイル共有に対応しているアプリケーションで利用できます。iOSデバイスの書類を確認または取得するには、Apple Configurator 2が動作しているMacに対象となるiOSデバイスを接続します。

3. 導入する

iOSによって、社員はデバイスを箱から出してすぐ使いはじめることができます。IT部門の手を借りる必要もありません。

デバイスの配布

最初の2つの手順でデバイスの準備と設定が完了したら、デバイスを配布できるようになります。パーソナライズを行う導入の場合は、デバイスをユーザーに渡してください。ユーザーは簡略化された設定アシスタントを使ってパーソナライズを行い、設定を完了します。パーソナライズを行わない導入の場合は、シフト制社員に配布するか、デバイスの充電と安全な保管が可能なキオスクにデバイスを配置します。

設定アシスタント

iOSのユーザーはデバイスを箱から出すだけで、iOSの設定アシスタントでアクティベートして基本的な設定を行い、すぐに使いはじめることができます。初期設定後は、言語、位置情報、Siri、iCloud、「iPhoneを探す」など、個人の設定もカスタマイズできます。Apple Business Managerに登録されたデバイスは、設定アシスタントの中で自動的にMDMに登録されます。

ユーザーによるパーソナライズを許可

パーソナライズを行う導入およびBYODによる導入の場合、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と生産性が高まります。これは、ユーザー自身が自分のタスクと目標達成のために最適なアプリケーションとコンテンツを選択することができるためです。iOS内の企業データと個人データは分離されて管理されます。

Apple ID

Apple IDは、FaceTime、iMessage、iTunes Store、App Store、Apple BooksやiCloudなど、Appleの様々なサービスへのログインに使用されるIDです。これらのサービスにより、ビジネスタスクの合理化、生産性の向上、コラボレーションのサポートを実現する多彩なコンテンツにアクセスできます。

ユーザーがこれらのサービスを最大限活用するには、自分専用のApple IDを使用する必要があります。Apple IDを持っていないユーザーは、デバイスを受け取る前でもApple IDを作成することができます。ユーザーが個人のApple IDを持っていない場合は、設定アシスタントで作成できます。ユーザーがApple IDを作成するのに、クレジットカードは必要ありません。

クレジットカードを使わずにApple IDを作成する：

support.apple.com/ja-jp/HT204034

Apple IDを作成する：

support.apple.com/ja-jp/HT204316

iCloud

iCloudを利用すると、連絡先、カレンダー、写真など、書類や個人のコンテンツを自動的に同期して、複数のデバイスを最新の状態に保つことができます。また、ユーザーはiOSデバイスがWi-Fiに接続している時に自動でバックアップできるだけでなく、iPhone、iPad、iPod touch、Macを紛失したり盗難に遭ったりした時に、「iPhoneを探す」を使って場所を確認することもできます。

フォトストリーム、iCloudキーチェーン、iCloud Drive、iCloudバックアップなどのサービスは、デバイスで手動で設定するか、構成プロファイルを使って無効にできます。MDMソリューションを利用して、管理対象アプリケーションのデータをiCloudにバックアップできないようにすることも可能です。この機能により、ユーザーは企業の情報をiCloudに保存せずに、個人のデータにはiCloudを利用することができます。Exchangeなどの社内アカウントや社内用アプリケーションに保存されたデータは、iCloudにバックアップされなくなります。

iCloudについてさらに詳しく：

www.apple.com/jp/icloud

4. 管理する

ユーザーがデバイスの使用を開始したら、様々な管理機能をデバイスとコンテンツの長期的な管理および維持に利用することができます。

デバイスの管理

管理対象デバイスは、特定のタスクのセットを通じてMDMサーバにより管理することができます。これらのタスクには、デバイスへの情報クエリのほか、ポリシー違反のデバイスや紛失または盗難に遭ったデバイスを管理できる管理タスクの開始などがあります。

クエリ

MDMサーバはデバイスに対して各種情報を照会できます。シリアル番号、デバイスのUDID、Wi-FiのMACアドレスなどのハードウェアの詳細のほか、iOSのバージョン、デバイスにインストールされているすべてのアプリケーションのリストなど、ソフトウェアの詳細に関する情報を照会できます。このような情報は、MDMソリューションで最新の在庫情報を管理するのに利用したり、経営判断の材料として活用したりできます。また、ユーザーが適切なアプリケーションのセットを維持していることを確認するといった、管理タスクも自動化できます。

管理タスク

デバイスが管理対象になっている場合、MDMサーバは様々な管理タスクを実行できます。これには、ユーザーの操作を必要としない自動での設定変更、パスコードロックされたデバイスのiOSアップデートの実行、リモートによるデバイスのロックまたはワイプ設定、ユーザーがパスワードを忘れた場合にリセットするためのパスコードロックの消去が含まれます。MDMサーバは、iOSデバイスに対し、特定の出力先へAirPlayミラーリングを開始するようリクエストしたり、現在のAirPlayセッションを停止したりできます。

管理対象のソフトウェアアップデート

ユーザーが監視モードのデバイスを手動でワイヤレスアップデートできないように一定期間の制限を行う事ができます。この制限を有効にすると、AppleがiOSのアップデートをリリースした時点から遅延期間のカウントが開始されます。デフォルトの遅延期間は30日です。ただし、このデフォルトは変更することが可能で、アップデートの遅延期間は1日から90日までの間で自由に設定できます。また、モバイルデバイス管理 (MDM) ソリューションを使用すれば、監視モードのデバイスでソフトウェアのアップデートをスケジュールすることもできます。

紛失モード

MDMソリューションでは、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、デバイスが最後にオンラインだった位置をMDMによってリモートから照会するので、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。紛失モードは、「iPhoneを探す」が有効になっていなくても使用可能です。

アクティベーションロック

iOS 7.1以降では、監視モードのデバイスでユーザーが「iPhoneを探す」をオンにした場合に、MDMを使って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、企業はアクティベーションロックの盗難防止機能を活用しながら、ユーザーがApple IDで認証ができない場合には、この機能をバイパスすることができます。

追加コンテンツの導入および管理

組織では、ユーザーの生産性を高めるために、頻繁にアプリケーションの配布が必要になります。同時に、組織はアプリケーションからの社内リソースへの接続方法や、ユーザーが組織を離れた場合にデータを安全に処理する方法も管理しなければなりません。また、ユーザーのプライベートなアプリケーションとデータはそのまま維持しておく必要もあります。

社内アプリケーションポータル

社員がiOSデバイスのためのアプリケーションを簡単に見つけられるように、社内アプリケーションポータルを利用できます。社内アプリケーションポータルは、多くのMDMサーバでソリューションの一部として提供されていますが、独自で開設することも可能です。このポータルから、社内用アプリケーション、App StoreのアプリケーションのURLやApple Business Managerコード、カスタムB2BアプリケーションのApple Business Managerコードへのリンクを張れば、ユーザーはここにアクセスするだけでアプリケーションを入手できます。このサイトを一元的に管理し、セキュリティを確保できます。社内アプリケーションポータルを使えば、社員は必要な承認済みリソースを簡単に見つけることができ、IT部門に問い合わせる必要もありません。

管理対象のコンテンツ

管理対象のコンテンツは、App Storeのアプリケーション、カスタムの社内アプリケーション、アカウント、本、書類のインストール、構成、管理、削除に関係します。

- **管理対象のアプリケーション。**iOSでは、管理対象のアプリケーションとして、無料または有料のアプリケーション、エンタープライズアプリケーションを、MDMを使って組織がワイヤレスで配布できます。またその際企業データの保護とユーザープライバシーの尊重のバランスを適切に保つことができます。MDMサーバを使って管理対象のアプリケーションをリモートで削除できます。また、ユーザーが自分のデバイスをMDMから削除した場合も、管理対象のアプリケーションが削除されます。アプリケーションを削除すると、アプリケーションに関連付けられたデータも削除されます。アプリケーションがApple Business Managerでユーザーに割り当てられたままの場合や、ユーザーが個人のApple IDを使用してアプリケーションのコードを引き換えた場合は、アプリケーションをApp Storeから再度ダウンロードできますが、MDMの管理対象ではありません。
- **管理対象のアカウント。**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活用することができます。MDMソリューションプロバイダおよび社内システムと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。
- **管理対象の本と文書。**MDMツール、本、ePubブック、およびPDF書類は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。また、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。コンテンツが不要になったら、リモートで削除できます。Apple Business Managerで購入した本は、管理配布で割り当てることができますが、無効にしたり割り当て直したりすることはできません。Apple Business Managerを通じて明示的にユーザーに割り当てた本でない限り、ユーザーがすでに購入した本を管理することはできません。

管理対象アプリケーションの構成

アプリケーションのデベロッパは、管理対象アプリケーションとしてインストールされた場合に有効となるアプリケーション設定および機能を提供できます。これらの構成設定は、管理対象アプリケーションのインストール前でも後でもインストールできます。例えば、IT部門がSharepointアプリケーションのデフォルトの環境設定をしておけば、ユーザーは手動でサーバを設定する必要はありません。

主要なMDMソリューションプロバイダがAppConfig Communityを設立し、すべてのアプリケーション開発者が利用可能な管理対象アプリケーションの構成をサポートするための標準スキーマを策定しました。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。このコミュニティは、モバイルアプリケーションを設定および保護する、オープンかつシンプルでより一貫性のある方法を実現することによって、ビジネスのモバイル化を推進しています。

AppConfig Communityについてさらに詳しく(英語) :
www.appconfig.org

管理されたデータフロー

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出ないように、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秘密情報を、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された管理対象のアプリケーションだけが、この仕事用の書類を開くことができます。管理対象外の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によって、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、一部のExtensionにも制限を設定することができます。
- **シングルAppモード。**この設定は、iOSデバイスで1つのアプリケーションしか使用できないように制限します。特定の目的のみで使用する小売業向けPOSや、病院での受付用端末などのキオスクに最適です。デベロッパは、この機能をアプリケーション内で有効にすることで、シングルAppモードのオンとオフが自立的に行われるよう設定することもできます。
- **バックアップの禁止。**この制限により、管理対象のアプリケーションはiCloudまたはiTunesにデータをバックアップすることができなくなります。バックアップを禁止すると、管理対象のアプリケーションがMDMにより削除された場合、ユーザーが後で再インストールしてもデータを復元できなくなります。

サポートオプション

AppleはiOSユーザーおよびIT管理者のために、様々なプログラムとサポートのオプションを提供しています。

AppleCare for Enterprise

完全なサポートを必要とする企業の場合、AppleCare for Enterpriseを利用すれば、社内ヘルプデスクの負担が軽くなります。社員を対象とした電話でのテクニカルサポートを24時間年中無休で提供し、優先度の高い問題には1時間以内に対応します。このプログラムは、Appleのすべてのハードウェア製品およびソフトウェア製品に関するIT部門レベルのサポートを提供するほか、MDMやActive Directoryといった複雑な導入や統合のシナリオにも対応します。

AppleCare OS Support

AppleCare OS Supportは、IT部門に対し、iOS、macOS、およびmacOS Server導入に関するエンタープライズレベルの電話サポートおよびEメールサポートを提供します。購入するサポートのレベルに応じて、24時間年中無休でサポートを提供し、お客様の組織を担当するテクニカルアカウントマネージャを選任します。統合、移行、および高度なサーバ運用の問題について技術者に直接質問できるため、AppleCare OS SupportはITスタッフがデバイスを導入および管理し、問題を解決する効率を高めます。

AppleCare Help Desk Support

AppleCare Help Desk Supportでは、Appleの上級テクニカルサポートスタッフのサポートを優先的に受けることができます。さらに、Apple製ハードウェアの診断と問題解決のためのツールを使って、大規模な組織でのリソース管理の効率アップやサポート応答時間の短縮、トレーニングコストの削減を図ることができます。AppleCare Help Desk Supportでは、ハードウェア／ソフトウェアの診断とトラブルシューティング、iOSデバイスの問題の特定などの問い合わせ件数に制限なしでサポートします。

iOSデバイス利用者のためのAppleCare

すべてのiOSデバイスには、製品購入後1年間のハードウェア製品限定保証と90日間の無償電話サポートが付いています。AppleCare+ for iPhone、AppleCare+ for iPad、AppleCare+ for iPod touchに加入すると、保証とサポートが購入日から2年間に延長されます。Appleのテクニカルサポートにお電話いただければ、専任スペシャリストがご質問にお答えします。Appleは、デバイスの修理が必要になった場合に、便利なサービスオプションも提供します。操作上の不慮の事故による故障の修理などのサービスを、所定のサービス料で最大2回まで受けることができます。

iOS Direct Service Program

AppleCare+のメリットとして、AppleCareに電話したり、Apple Storeに来店しなくても、iOS Direct Service Programにより、ヘルプデスクがデバイスの問題特定をお手伝いすることができます。必要に応じて、あなたの組織はiPhone、iPad、iPod touchの交換や付属のアクセサリを直接注文することができます。

AppleCareプログラムについてさらに詳しく：

www.apple.com/jp/support/professional/

まとめ

企業がiOSデバイスをユーザーグループまたは組織全体のどちらに導入する場合でも、導入と管理を簡単に行うためのオプションが多数用意されています。組織に最適な戦略を選択することで、社員の生産性が向上し、まったく新しい方法で業務を推進することができます。

iOSとエンタープライズIT環境の統合についてさらに詳しく：

www.apple.com/jp/business/products-platform/

1一部のアプリケーションや本は、国や地域、オペロパの選択状況によって利用できない場合があります。[プログラムとコンテンツの提供状況](#)を参照してください。

2一部の機能にはWi-Fi接続が必要です。国によっては一部の機能を利用できない場合があります。iCloudの最小システム条件と推奨されるシステム条件については、support.apple.com/ja-jp/HT204230を参照してください。

© 2018 Apple Inc. All rights reserved. Apple、Appleのロゴ、AirDrop、AirPlay、AirPrint、Apple TV、Bonjour、FaceTime、iMessage、iPad、iPhone、iPod touch、iTunes、Mac、macOS、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。tvOSはApple Inc.の商標です。App Store、AppleCare、Apple Store、Apple Books、iCloud、iCloud Drive、iCloudキーチェーン、iTunes Storeは、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。iOSは米国およびその他の国におけるCiscoの商標または登録商標であり、ライセンスに基づき使用されています。この資料に記載されているその他の製品名および会社名は、各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される場合があります。この資料は情報提供のみを目的として提供されます。Appleはこの資料の使用に関する一切の責任を負いません。