iOSおよびiPadOS
導入の概要

概要

目次

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とiPadOSをサポートすることによって、技術的な問題の解決やコストの削減を行うだけでなく、ビジネス戦略の立案に関わりビジネスの課題の解決に取り組む部門に変わります。最終的に、すべての社員にメリットがもたらされます。会社全体が活性化し、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（MDM）ソリューションを使用することで、iOSおよびiPadOS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できます。
- Apple Business Managerを利用すると、Microsoft Azure ADによるFederated Authenticationを使用する管理対象Apple IDを社員用に作成することもできます。

この文書では、組織にiOSおよびiPadOS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。これらのトピックの詳細は、オンラインの「iPhoneとiPadの導入リファレンス」（support.apple.com/ja-jp/guide/deployment-reference-ios）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されるiOSおよびiPadOS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、この会社の小売店舗では、組織所有のモデルを使用し、複数の社員でiOSおよびiPadOSデバイスを共有しながら顧客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が提供する導入と管理の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

組織所有のモデルを採用する場合、日常的に使用できるように各社員にデバイスを配布することも、同じ業務を担当する社員間でデバイスを共有することも、また、特定のアプリケーション専用にデバイスを構成することもできます。ユーザー個人に配布されたデバイスは、そのユーザーがパーソナライズすることができます。単一のアプリケーション専用に固定されたデバイスや、ユーザー間で共有するデバイスでは、通常エンドユーザーがパーソナライズすることはありません。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Device Enrollmentに対応するApple正規取扱店か通信事業者から直接購入したデバイスであれば、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。これをAutomated Device Enrollmentと呼びます。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管理者が一元的にデバイスの構成と管理を行うため、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。Apple Business ManagerのAutomated Device Enrollmentでは、パーソナライズを行わないデバイスの設定を自動化することもできます。次頁の表では、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、App 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、iOS 13およびiPadOSの新しいUser Enrollmentオプションを使って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。

BYODによる導入では、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。ユーザーは、組織のMDMソリューションへ登録することを選択する必要があります。

個人デバイス向けのUser Enrollment機能により、ユーザーのプライバシー、個人データ、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ます。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、特定の設定のみを適用し、ポリシーへの準拠を監視して、必要であれば企業のデータやアプリケーションのみを削除できます。

User Enrollmentには以下が含まれます。

- **管理対象Apple ID。**デバイス上で個人認証して、Appleサービスにアクセスできるようにするため、User Enrollmentは管理対象Apple IDと統合されています。管理対象Apple IDは、ユーザーがサインインに使っている個人用のApple IDと併用できます。管理対象Apple IDはApple Business Manager内で作成され、Microsoft Azure Active Directoryとの Federated Authenticationによってプロビジョニングされます。
- **データの分離。**User Enrollmentを行うと、デバイス上で、管理対象のアカウント、アプリケーション、データ用に分離されたAPFSボリュームが作成されます。この管理対象のボリュームは暗号化によってデバイスの残りの部分と切り離されます。
- **BYOD向けの管理機能。**User Enrollmentはユーザー所有のデバイス向けに作られており、IT部門は構成とポリシーのサブセットを管理することはできる一方、特定の管理タスクは制限されます。例えば、デバイス全体をリモートで消去したり、個人情報を収集したりすることはできません。

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、個人用および管理対象のApple ID、App Store、およびiCloudのアカウントを使用
設定	• デバイスの設定 • 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

MDMのUser Enrollmentについてさらに詳しく：
support.apple.com/ja-jp/guide/mdm

Federated Authenticationについてさらに詳しく：
support.apple.com/ja-jp/guide/apple-business-manager

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決定したら、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、ほとんどの標準的な企業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およびiPadOS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にアクセスできることは、iOSおよびiPadOS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接続できるキャパシティがあることを会社のWi-Fiネットワークで確認してください。デバイスがAppleのアクティベーションサーバ、iCloud、App 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の構成を変更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およびiPadOS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およびiPadOS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、適切な数のユーザーおよび接続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、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、ネットワークインフラストラクチャが設定されていることも確認する必要があります。Bonjourには、ネットワーク上のサービスをデバイスが自動的に検出できるようにする役割があります。iOSおよびiPadOS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。

Wi-Fiおよびネットワークについてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-ios

Bonjourについてさらに詳しく（英語）：
developer.apple.com/library

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およびiPadOS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およびiPadOSは、OAuth 2.0と多要素認証を利用する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およびiPadOS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サーバのコンテンツはローカルにコピーが保存されるため、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、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およびiPadOS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およびiPadOS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/guide/deployment-reference-ios

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

MDMソリューションの選択

AppleのiOSおよびiPadOS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ソリューションを通じて提供されます。

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。

デバイスと企業データの管理についてさらに詳しく：
apple.com/jp/business/site/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf

Apple Business Managerに登録

Apple Business Managerは、IT管理者がiPhone、iPad、iPod touch、Apple TV、およびMacをすべて1か所から導入できる、ウェブベースのポータルです。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係することで、Apple Business Managerでは、デバイス導入の自動化、アプリケーション購入とコンテンツ配布、社員の管理対象Apple IDの作成を簡単に行うことができます。

Device Enrollment Program（DEP）とVolume Purchase Program（VPP）はApple Business Managerに完全に統合され、Appleのデバイスを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。2019年12月1日より、統合前のプログラムは使用できなくなります。

デバイス

Apple Business Managerでは、Automated Device Enrollmentによって、企業が所有するAppleデバイスをすばやく効率的に導入し、デバイスに触れたり準備したりすることなくMDMに登録できます。

- 設定アシスタントのステップを合理化することで、ユーザーの設定プロセスを簡略化できます。社員はアクティベーション後すぐに正しい構成を確実に受け取れるようになります。IT部門はこのプロセスをさらにカスタマイズし、同意文書、企業のブランディング、最新の認証方法を社員に提供できるようになりました。
- 監視モードによるほかの導入モデルでは利用できない追加のデバイス管理機能や、削除不可能なMDM登録といった機能により、会社所有のデバイスをより高度なレベルで制御できます。
- 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iPhone、iPad、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では、コンテンツを簡単に一括購入できます。社員が使用するデバイスが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。

- 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、社内で開発したアプリケーションも入手できます。ある拠点から別の拠点へアプリケーションのライセンスを転送したり、ライセンスを同じ拠点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。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方法を利用できます。組織は一定の金額のVolume Creditを現地通貨でAppleまたはApple正規取扱店から購入でき（利用可能な場合）、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。

注意：一部の国と地域では、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。

ユーザー

Apple Business Managerでは、組織が社員用のアカウントを作成して管理できます。このアカウントは既存のインフラに統合され、Appleのアプリケーションやサービス、Apple Business Managerへのアクセスを提供します。

- 管理対象Apple IDを作成すれば、社員はAppleのアプリケーションやサービスを使って共同作業できるほか、iCloud Driveを使用する管理対象アプリケーションで業務用データにアクセスできるようになります。管理対象Apple IDは、組織が所有および管理します。
- Apple Business ManagerをMicrosoft Azure Active Directoryに接続して、Federated Authenticationを活用することもできます。対応するAppleデバイスで社員が既存の資格情報を使ってはじめてサインインすると、管理対象Apple IDが自動的に作成されます。
- iOS 13、iPadOS、macOS Catalinaで利用可能になった新しいUser Enrollment機能を使うと、社員が所有するデバイスで個人用と管理対象の両方のApple IDを使用することができます。また、どのデバイスでも、管理対象Apple IDをプライマリ（かつ唯一の）Apple IDとして使うこともできます。Appleデバイスにはじめてサインインした後は、管理対象Apple IDでウェブ上のiCloudにアクセスすることもできます。
- 社内のIT部門にその他の役割を割り当て、Apple Business Managerでデバイス、アプリケーション、アカウントを効率的に管理することができます。管理者の役割を使用すると、必要に応じて利用規約に同意したり、離職した人の権限を簡単に移行したりできます。

注意：User Enrollmentは、現在iCloud Driveをサポートしていません。管理対象Apple IDがデバイス上の唯一のApple IDである場合にはiCloud Driveを使うことができます。

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は、アプリケーションを開発、テスト、ユーザーに配布するための全ツールのセットを提供します。アプリケーションを配布する際は、ウェブサーバでホストするか、MDMソリューションを使います。MacのアプリケーションとインストーラにDeveloper IDを使って署名して認証を受けると、Gatekeeperに対応できます。Gatekeeperは、マルウェアからmacOSを保護する機能です。

Developer Enterprise Programについてさらに詳しく：
developer.apple.com/programs/enterprise/jp

2. 設定する

このステップでは、Apple Business Manager、MDMソリューション、Apple Configurator 2（オプション）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。

デバイスの構成

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およびiPadOS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およびiPadOSデバイスは、MDMに強制的に登録され、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、企業の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Wi-Fiネットワークの資格情報を自動で提供するようにした上で、MDMへの登録をWi-Fiアクセスのための条件とすることなどができます。

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。デバイスに対して実行できる管理アクションは、監視モードの有無や登録方法によって異なります。iOSまたはiPadOS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。ネットワーク接続さえあれば、世界中のどこにいてもデバイスは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）

ローカル環境で複数のデバイスを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アプリケーションを使用すると、iOSおよびiPadOSデバイスをUSB経由でMacコンピュータに接続し、デバイスを最新バージョンのiOSまたはiPadOS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は、デバイスとデバイスに関して実行する各タスクの管理に特化したユーザーインターフェイスを持ちます。Apple Business Managerと連係することで、組織の設定を使用してデバイスをMDMに自動的に登録することができます。また、ブループリントで個々のタスクを組み合わせながら、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およびiPadOS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することもできます。デフォルトでは、iOSおよびiPadOSデバイスはいずれも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専用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専用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を固定化するものではなく、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能力を高めるものです。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。

監視モードのデバイスの制限についてさらに詳しく：
support.apple.com/ja-jp/guide/mdm

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およびiPadOS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、または社内で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する必要があります。

管理配布

MDMソリューションまたはApple Configurator 2を利用すると、管理配布により、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。購入した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であればどこでも配布できます。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。この方法では、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ため、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。**別の方法として、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する方法があります。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ができます。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を使用してデバイスを構成する場合、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およびiPadOS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およびiPadOSデバイスを接続します。

3. 導入する

iPhoneおよびiPadでは、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、用途に応じて、シフト制社員に配布したり、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たりすることになります。

設定アシスタント

ユーザーはデバイスを箱から出してすぐに、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、ただち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、「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の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ぶことができるためです。

Apple IDと管理対象Apple ID

社員がApple IDを使ってAppleのサービス（FaceTime、iMessage、App Store、iCloudなど）にサインインすると、ビジネスタスクの合理化、生産性の向上、共同作業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。

管理対象Apple IDは、通常のApple IDと同じように個人デバイスのサインインに使用します。また、iCloudなどのAppleのサービスにアクセスしたり、iWorkやメモを使って共同制作したりするほか、Apple Business Managerにアクセスする場合にも使用します。通常のApple IDとは異なり、管理対象Apple IDは組織が所有および管理します。パスワードのリセットや役割ベースの管理も組織が行います。管理対象Apple IDでは、一部の制限が設定されています。

User Enrollmentで登録されたデバイスには管理対象Apple IDが必要です。User Enrollmentでは、オプションで個人のApple IDも併用できます。ほかの登録オプションでは、個人用または管理対象のいずれかのApple IDのみサポートされます。複数のApple IDをサポートしているのは、User Enrollmentのみです。

ユーザーがこれらのサービスを最大限活用するには、自分のApple ID、または自分用に作成された管理対象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。

管理対象Apple IDについてさらに詳しく：
support.apple.com/ja-jp/guide/apple-business-manager

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、複数のデバイス間で最新の状態に保つことができます。「探す」を使うと、ユーザーは、紛失や盗難に遭ったMac、iPhone、iPad、iPod touchの場所を特定できます。手動でデバイスを操作するか、MDMを使って設定を行うことで、制限を施すことができ、iCloudキーチェーンやiCloud Driveなど、iCloudの特定部分を無効にすることができます。これにより、組織はどのアカウントにどのデータが保存されるのかについて、より細かく制御できます。

iCloudの管理についてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-ios

4. 管理する

ユーザーがデバイスの使用を開始したら、様々な管理機能を利用してデバイスとコンテンツの長期的な管理と維持を行うことができます。

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に対応するための管理タスクの実行などがあります。

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またはiPadOS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ソリューションでインベントリの情報を随時更新するのに利用したり、管理上の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ソフトウェアアップデートの実行、リモートからのデバイスのロックまたはワイプ、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解除が含まれます。MDMサーバは、iPhoneまたはiPad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ことができます。この制限を有効にすると、AppleがiOSまたはiPadOSのアップデートをリリースした時点から保留期間のカウントが開始されます。デフォルトの保留期間は30日です。ただし、このデフォルト期間は変更することが可能で、アップデートの保留期間は1日から90日までの間で自由に設定できます。また、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から紛失モードにすることができます。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「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、この盗難防止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、ユーザーが離職し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

社内アプリケーションポータルを利用すると、社員がiPhoneまたはiPad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、Apple Business Managerコード、カスタムアプリケーションなどのリンクを張れば、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。管理者は管理とセキュリティの確保をこのサイトで一元的に行うことができます。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およびiPadOSでは、管理対象のアプリケーションにすることで、無料または有料のアプリケーションやエンタープライズアプリケーションをMDMによりワイヤレスで配布できるようになります。またその際に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。管理対象のアプリケーションは、MDMサーバを使って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は削除されます。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の管理対象ではなくなります。

- **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メールアドレスに加え、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。

- **管理対象の本と書類。**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。

Managed App Configuration

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デベロッパが利用可能なManaged App Configuration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ための、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):
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流出しないように、企業データを細かな単位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またはiPadOS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律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またはコンピュータ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は復元できません。

サポートオプション

Appleは、iOSおよびiPadOSユーザーと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

包括的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、iPadOS、macOS、およびmacOS Serverの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ーを選任します。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各種ツールが提供されるため、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、ハードウェアやソフトウェアの診断とトラブルシューティング、iOSおよびiPadOSデバイスの問題の切り分けなどを、インシデント件数の制限なくサポートします。

iOSおよびiPadOSデバイス利用者のためのAppleCare

すべてのiOSおよびiPadOS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。さらに、AppleCare+では、過失や事故による損傷に対する修理などのサービスを最大2回まで所定のサービス料で利用することができます。

iOS Direct Service Program

AppleCare+のメリットとして、iOS Direct Service Programをご利用いただくと、AppleCareに電話したり、Apple Storeに来店することなく、社内ヘルプデスクでデバイスの問題のスクリーニングを行うことができます。必要であれば、あなたの組織はiPhone、iPad、iPod touchの交換品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：
apple.com/jp/support/professional/

まとめ

企業がiPhoneまたはiPadをユーザーグループまたは組織全体のいずれ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、仕事を遂行するまったく新しい方法を手に入れることができます。

iOSおよびiPadOSの導入、管理、セキュリティ機能についてさらに詳しく：
support.apple.com/ja-jp/guide/deployment-reference-ios

IT向けモバイルデバイス管理設定についてさらに詳しく：
support.apple.com/ja-jp/guide/mdm

Apple Business Managerについてさらに詳しく：
support.apple.com/ja-jp/guide/apple-business-manager

ビジネス向けの管理対象Apple IDについてさらに詳しく：
apple.com/jp/business/site/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Apple at Workについてさらに詳しく：
www.apple.com/jp/business/

IT部門向けの機能についてさらに詳しく：
www.apple.com/jp/business/it/

Appleプラットフォームのセキュリティについてさらに詳しく：
support.apple.com/ja-jp/guide/security/welcome/web

利用可能なAppleCareプログラムを探す：
www.apple.com/jp/support/professional/

Appleのトレーニングと認定資格を調べる（英語）：
training.apple.com

Apple Professional Serviceに問い合わせる：
consultingservices@apple.com

一部のアプリケーションや本は、国や地域、デベロッ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。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。