【Microsoft Intune】iOS：Apple Business Manager + Intune（ADE連携）設定手順

2025年6月30日

改定履歴

版数	発行日	改訂内容
第1版	2025年6月30日	初版発行

本資料の内容は 2025/6/30 時点のものです。製品のアップデートにより変更となる場合がございます旨でご了承ください。

Agenda

1. 前提情報
    1. 前提条件
    2. 用語集

2. 設定概要
    1. 全体概要図
    2. ABM（ Apple Business Manager ）とは
    3. ADE（Automated Device Enrollment）とは

3. 前提条件
    1. 実行前チェックリスト
    2. ABM 初期登録と販売店連携
    3. Apple MDM プッシュ証明書の登録

4. 設定手順
    1. 設定概要
    2. Apple MDM プッシュ証明書の登録
    3. ABMとIntuneの連携
    4. ABM上でデバイスをIntuneに割り当て
    5. 登録プロファイル作成
    6. アプリ・構成プロファイル配布
    7. iOS端末の初回セットアップ（ゼロタッチ導入）

1. 前提情報

1.1. 前提条件

- iOS端末を Microsoft Intune に登録・管理する方法には、主に以下の2つのパターンがあります。

  ① **新規購入端末を Apple Business Manager（ABM）経由で自動登録（ADE）する方法**
  ② **既存端末や個人所有端末（BYOD）をユーザー操作で手動登録する方法**

  本資料では、①の **新規購入端末を対象とした ABM＋Intune（ADE連携）による自動登録手順** を解説しています。

- この方法では、IT管理者が事前に ABM や Intune の設定を行うことで、従業員は端末を開封・起動するだけで、自動的に管理下へ登録され、業務アプリや設定が適用されるため、**ユーザーの作業負荷を最小限に抑えた “ゼロタッチ導入”** が可能になります。
- 一方、既に所有している端末や ABM に登録されていない端末は、本資料の対象外です。
- この手順書は、主に営業支援メンバーや社内導入を検討する担当者が、ADE 方式による iOS 管理の流れを理解し、顧客提案や社内展開に活用できるよう構成されています。設定の全体像に加え、必要な前提条件、管理者および従業員それぞれの作業手順を整理しています。
- 本資料を通じて、次のようなことが分かるようになります。

  ✓ Apple Business Manager および ADE の基本概念
  ✓ Intune と ABM を連携して自動登録を実現する手順
  ✓ 初期構成に必要な証明書やプロファイルの準備方法
  ✓ 管理者・従業員それぞれの役割と作業内容

なお、一部画面キャプチャがないものに関しては文章での記載のみとさせていただいております。

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	D-U-N-S® Number	企業コードの付与管理システム、並びに同システムによって各企業に付与された９桁の企業コードです。世界6億件超の企業に付与され、企業を重複なく一意に識別可能です。DUNSナンバーは、顧客の管理や様々なプロプラムに活用されています。
2	CSR	CSRファイルは「証明書を発行するための申請書のようなもの」で、その都度必要な情報（公開鍵、識別情報など）を含んで動的に生成されます。 したがって、1回作成したものを使い回すことはできません。
3	BYOD（Bring Your Own Device）	従業員が個人所有のスマートフォンやノートPCなどの電子デバイスをビジネスで利用するという意味です。
4	Apple school Manager（ASM）	Apple School Managerは、サードパーティのモバイルデバイス管理（MDM）ソリューションと連携する、IT管理者向けのシンプルなWebベースのポータルです。組織がiPhone、iPad、Mac、Apple TV、Apple Watch、Apple Vision Proのいずれを使用しているかにかかわらず、コンテンツを簡単に一括購入することができます。
5	Apple Account	旧Apple ID。Apple Accountとは、App Store、Apple Music、iCloud、iMessage、FaceTimeなどのAppleのサービスを利用するときに使うアカウントのことです。1つのApple AccountでAppleのすべてのサービスにサインインできます。

1.2. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
6	管理対象 Apple Account（Managed Apple Account）	Appleが提供する組織用のApple Accountです。個人用Apple Accountは、個人が自由に作成・管理するのに対し、管理対象 Apple Account は組織での利用を想定しているため、組織に所属している従業員を、管理者が一括で作成・管理を行うことが可能です。ABMは組織管理のためのポータルであり、セキュリティや権限管理の観点から、個人のApple Account ではなく、組織が管理する管理対象 Apple Account での運用が必須とされています。これにより、管理者の権限や利用範囲を企業側で一元管理できます。管理対象 Apple AccountはABM上で作成することが可能です。
7	ゼロタッチ	、ITデバイスの導入や設定を、IT担当者がクラウド上から遠隔で自動的に行う手法のことです。利用者はデバイスを受け取って電源を入れるだけで、必要な設定やアプリが自動でインストールされ、すぐに使い始められます
8	構成プロファイル	構成プロファイルとは、主にAppleデバイス（iPhone、iPad、Macなど）の設定をまとめて管理するためのファイル形式です。XML形式で記述され、Wi-Fi設定、VPN設定、パスコードポリシー、機能制限など、様々な設定をデバイスに適用できます。企業や学校で多数のデバイスを管理する際に、一括で設定を配布・適用するために利用されることが多いです。
9	Apple アクティベーションサーバー	Appleのアクティベーションサーバーとは、Appleデバイス（iPhone、iPad、iPod touch、Apple Watch、Macなど）のアクティベーション（初期設定）や、アクティベーションロックなどの機能を管理するAppleのサーバー

2. 設定概要

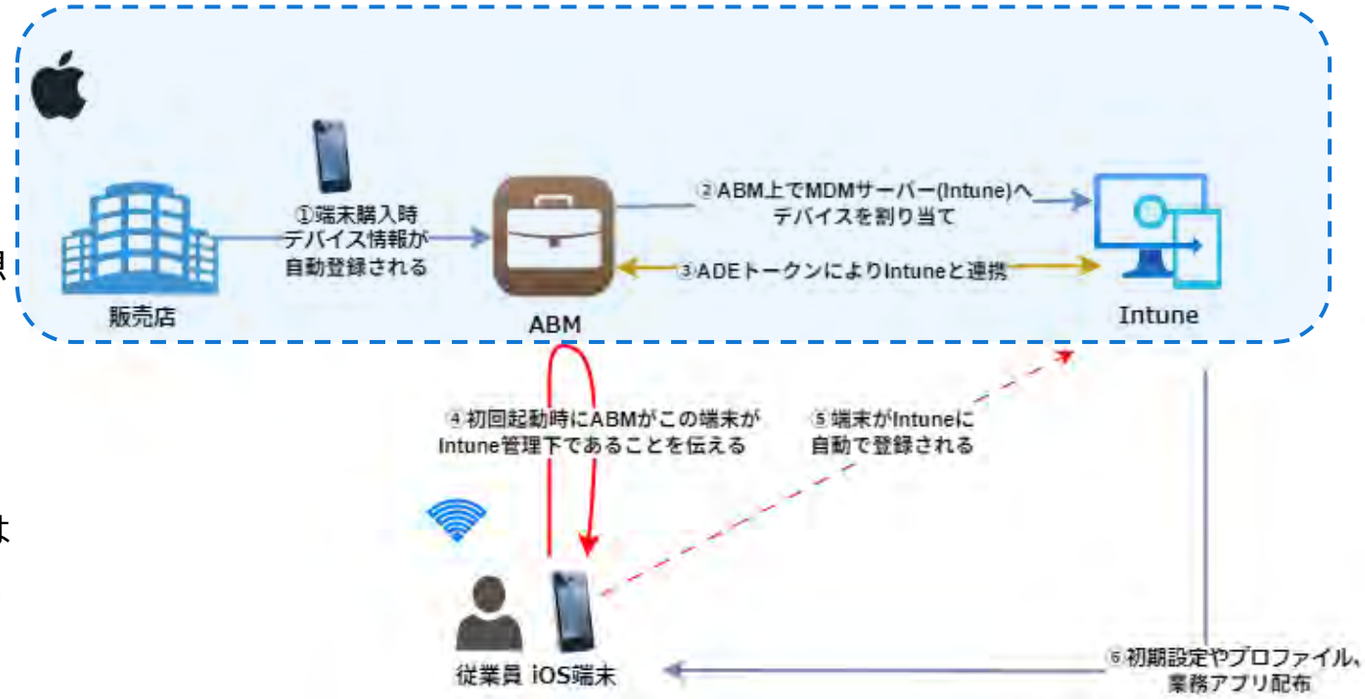
2.1. 全体概要図

Apple Business Manager（ABM）とMicrosoft Intuneを連携させることで、iOS端末のキッティング作業を自動化し、一貫したセキュリティ設定・業務アプリの配布が可能になります。本手順の全体の流れは以下のとおりです。

①Apple認定の販売店（ABM対応）からiOS端末を購入し、組織IDを事前に共有しておくことで、購入した端末は自動的にApple Business Manager（ABM）に登録されます。

②ABM上で、該当端末をMicrosoft IntuneのMDMサーバー（仮想的な登録先）に割り当てておくことで、初回起動時に自動でIntuneへの登録が行われる準備が整います。

③ABMとIntuneはADEトークンにより連携されており、Intuneは ABMから割り当てられた端末情報を取得します。管理者はIntune上で「自動登録プロファイル」や「業務用アプリの配布設定」などを事前に作成しておきます。



2.1. 全体概要図

④従業員が端末の電源を入れ、Wi-Fiに接続すると、端末はAppleのアクティベーションサーバーに接続し、自身がABM登録済みであることを確認します。ABMの指示により、IntuneからMDM構成プロファイルが自動で取得・インストールされます。

⑤Intuneは端末から送信された登録要求を受信し、事前に作成された自動登録プロファイルに基づき、端末を自動的に管理対象デバイスとして登録します。登録が完了すると、端末はIntuneポータル上に表示され、各種ポリシー適用やリモート管理が可能な状態になります。

⑥構成プロファイルの適用やアプリ配布が自動で行われ、端末は企業管理下に置かれます。

これにより、IT部門による個別の端末設定作業を省略しつつ、統一されたポリシー適用とセキュリティ管理が可能となります。

次のページより、ABM、ADEについてそれぞれ解説をしています。

2.2. ABM（Apple Business Manager）とは

ABM（Apple Business Manager）とは

Apple Business Manager（以下、ABM）は、Apple社が提供するサードパーティのモバイルデバイス管理（MDM）ソリューションと連携する、IT管理者向けのシンプルなWebベースのポータルです。組織がiPhone、iPad、Mac、Apple TV、Apple Watch、Apple Vision Proのいずれを使用しているかに関わらず、コンテンツを簡単に一括購入することができます。

ABMでできること

自動登録	• Apple認定販売店から購入したデバイスをMDM（Intune）へ自動登録できるようにする
アプリの一括配布	• Apple storeのアプリを一括購入し、ライセンス管理下で配布することが可能です
デバイスの一覧管理	• 組織が購入・登録したApple製品の一覧をABMで一元管理
Apple Accountの管理	• 従業員が使用する管理対象Apple Accountを組織で発行・制御可能

2.2. ABM（Apple Business Manager）とは

注意点

ABMを登録するにはD-U-N-Sナンバーが必要となるため、個人の方はABMを利用することができません。
また、登録の際は他のAppleサービスで使われていない、新しいApple Accountが必要です。

Apple School Manager（ASM）について

※ABMと同じような機能を有しているApple School Manager（ASM）というものもありますが、
ABMの使用対象は企業・法人であるのに対し、ASMの使用対象は教育機関や学校であり、これらの端末を
管理する際に利用します。

2.3. ADE（ Automated Device Enrollment ）とは

ADE（Automated Device Enrollment ）とは

Automated Device Enrollment （以下、ADE） は、Appleが提供するゼロタッチ導入方式で、ABM とMDM（Intune）を連携させて、iPhoneやiPadの初期セットアップを自動化する機能です。通常、iPadやiPhone、MacPCなどを導入する場合、キッティングを行う必要があり、作業をモバイル端末の数だけ繰り返す必要があります。数台なら問題ないかもしれませんが、端末の数が増えれば増えるほど、導入にかかる負担も大きくなります。ADEを利用することで、これらの作業を簡略化し、Appleデバイスが素早く利用可能となります。

管理者は端末を手動で設定する必要がなく、ユーザーが電源を入れるだけで、以下(図右側)が自動的に行われます。
ADE未対応の場合とADE対応の場合を比較してまとめています。

	ADE未対応（手動）	ADE対応（自動）
初期設定	• 端末1台ずつ管理者がキッティング作業/設定	• 電源を入れるだけでMDMへの登録が完了（ゼロタッチ）
アプリ配布	• App Storeから手動でインストール	• 初回起動時に自動で設定適用（Intuneで一元配布）
セキュリティ	• 従業員ごとに設定内容は異なる	• パスコード・証明書・制限などのセキュリティ設定がIntuneで強制
Apple Account	• 個人のApple Accountが必要となる	• ユーザーがApple Accountを所持しなくとも運用可能（管理対象Apple Accountも利用可能）

2.3. ADE（ Automated Device Enrollment ）とは

ADEを利用するメリット

- ✓ ゼロタッチ導入：従業員は電源を入れるだけ
- ✓ セキュリティ強化：監視モード・制限ポリシーを自動適用
- ✓ ITの運用負荷を軽減：配布・設定・回収・再利用が効率化
- ✓ 再初期化しても自動登録が継続：盗難や私物化を防止

ADEを使わないIntune登録の主なユースケース

すべての利用シーンでADEが使えるわけではありません。
以下のようなユースケースでは、ADEを使用せずにIntuneへ手動登録またはユーザー主導の登録を行う必要があります。

ユースケース	理由	登録方法
BYOD端末	・ADEは企業が購入、管理する端末にしか使うことはできない ・個人端末に「監視モード」や強制管理を適用することは難しい	Intuneポータルから手動でIntuneに登録
ADE非対応のiOS端末	・シリアル番号がABMに登録されていないため、ADEの対象外	従業員or管理者がIntuneアプリ経由でプロファイルをインストール

3. 前提条件

3.1.実行前チェックリスト

設定を開始する前に、以下の要件をすべて満たしているかを事前に確認する必要があります。
これらの前提条件が未整備のまま進めると、正常に端末がIntuneに登録されない、または設定が反映されない可能性があります。

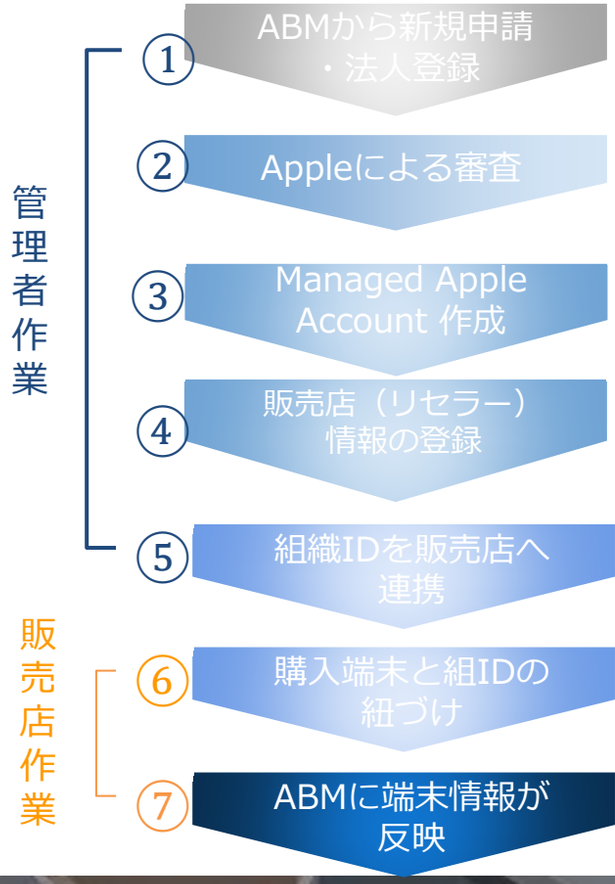
実行前に確認すべきポイント

内容	確認内容	補足
Intuneライセンスの割り当て	Intuneを使用するためにはライセンスが必要となります。対象ユーザーにIntuneライセンスが付与されていることを必ず確認します。	Microsoft 365の一部ライセンス（ E3、E5、F1、F3等）にはIntune Plan1が含まれています。
Intune管理者アカウントの用意	Intuneを組織で安全に運用するためには、個人ではなく専用の管理者アカウントを準備することが推奨されます。	
ADE対応iOS端末の準備	ADEの機能を利用するためには、ADEに対応している端末を所持します。（対応端末は右に記載しています） また、未開封、未初期化の状態であることを確認します	・iOS 7 以降を搭載した iOS デバイス iPadOS デバイス ・OS X Mavericks 10.9 以降を搭載した Mac コンピュータ ・tvOS 10.2 以降を搭載した Apple TV デバイス (第 4 世代以降
ABM用のアカウントの準備	最低でも以下のアカウントが必要です ・ABM申請用のApple Account（申請用） ・管理対象 Apple Account (Managed Apple Account)	ABMは組織管理のためのポータルであり、セキュリティや権限管理の観点から、申請用のアカウントとは異なる、組織が管理する管理対象 Apple Account での運用が必須とされています。

3.2. ABM 初期登録と販売店連携

管理者作業

iOS端末をゼロタッチで管理開始するには、購入前にABMへの登録が必要です。また、ABMに登録されていない状態で端末を購入すると、自動登録（ADE）が行われず、端末ごとに手動設定が必要になります。そのため、ABMの初期登録と、販売店との事前連携（組織IDの共有）は非常に重要なステップです。詳細の手順は、Apple Business Manager の公式ユーザーガイドをご参照ください。（本資料では手順は省略します）なお①～④については販売店から端末を購入する前に事前に行う必要があります。



自社組織をAppleに登録申請します。なお、ABMへの登録は一度設定すれば繰り返し行う必要はありません
この法人はABMを使用してApple製品を一括管理したいという申し出をAppleに行います
実際に会社の詳細情報やD-U-N-S番号を入力します。登録に必要な情報は次のページにて説明しています。

通常は数日～1週間程度かかります

Apple Accountは個人用ではなく、法人用のManaged Apple Accountとして作成します
Intune連携・MDM設定・販売店連携などすべてに必要となります

iOS端末をABMに自動登録（ADE対応）させるには、Apple認定販売店（リセラー）をABMに登録しておく必要があります。ABMログイン後、販売店が提供するリセラーIDを入力・保存します

ABMに自社組織が登録されたあとに、Apple認定販売店に「この会社の端末として紐づけてください」と伝える作業です。ABMから組織IDを確認し、販売店に連絡をします

販売店は、顧客から共有された⑤の組織IDを Apple との販売システムに登録し、端末情報（シリアル番号など）と紐づけて Apple に報告します

登録完了後、ABM上に購入端末が表示されます

3.2. ABM 初期登録と販売店連携

管理者作業

①ABMから新規申請・法人登録

前ページのABMの登録の際に必要な情報は以下となります。

登録にはD-U-N-Sナンバーが必要となるため、個人の方はABM利用することができません。
また、登録の際は他のAppleサービスで使われていない、新しいApple Accountが必要です。

Apple Account	ABM申請に使用するApple Accountは、会社のドメインで個人のAccountに紐づかない管理用のメールで作成してください。（例：admin@xx.jp）
組織の公式ドメインメール	会社のドメインのアドレスを使用
組織情報	会社名、法人の電話番号
D-U-N-S番号	企業を一意に識別する番号。申請が必要です。 申請方法はこちらを参照してください。

3.2. ABM 初期登録と販売店連携

管理者作業

④販売店情報の登録

iOS端末をABMに自動登録（ADE対応）させるには、Apple認定販売店（リセラー）をABMに登録しておく必要があります。
ABMへログインを行い、販売店が提供するリセラーIDを入力する手順を以下に解説します。

手順

1. ABMへ管理者Apple Accountにてサインインします
2. 「環境設定」＞ 「MDMサーバの割り当て」を選択します
3. [お客様番号]セクションにある「編集」をクリックします
4. お客様番号または販売代理店暗号を入力して[完了]を選択します

3.3. Apple MDM プッシュ証明書の登録

管理者作業

Apple MDM プッシュ証明書の登録

Microsoft Intune で iOS/iPadOS および macOS デバイスを管理するには Apple MDM プッシュ証明書が必要となります。
次の設定手順にて詳しく説明をします

なぜ登録が必要なのか

Appleのセキュリティポリシー上、外部システム（Intuneなど）がApple端末に指示を出すためには、Appleが発行する信頼済みの証明書が必要です。
この証明書があることで、Appleは「この管理者（Intuneテナント）は正規の管理者である」と認識します。
Appleが提供する「APNs（Apple Push Notification service）」を使って、IntuneがiOS端末に命令（例：アプリのインストール、設定の変更など）を送信することを可能にします。
この証明書がなければ、IntuneからiOS端末への管理命令は一切届かないため、MDM管理が成立しません。

注意点

証明書には更新期限があり、**毎年更新が必要です。**
期限が切れるとMDMの通知が届かなくなり、端末管理ができなくなります。
更新は同じApple Accountで行う必要があります。

4. 設定手順

4.1. 設定概要

あらかじめ ABM の登録および初期設定が完了していることを前提に、Microsoft Intune と連携して iOS 端末を自動で企業管理下に登録する手順を、6ステップで解説します。デバイスの割り当てから Intune 登録、アプリや構成プロファイルの自動配布までを順に実施することで、従業員が端末を開封してすぐに業務利用を開始できる、ゼロタッチ運用を実現します。

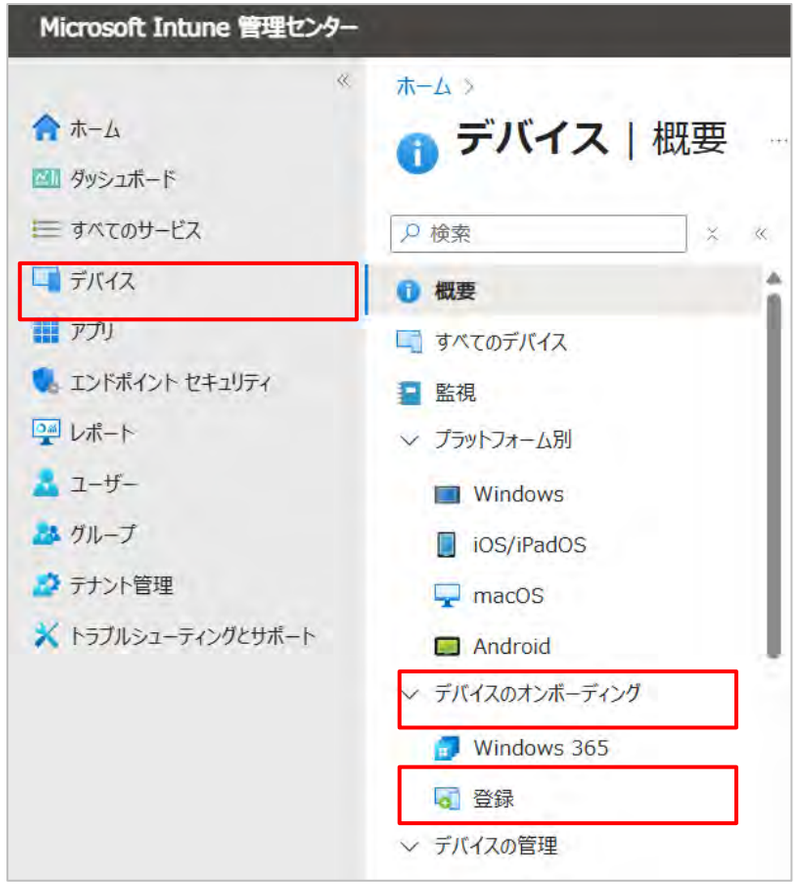
Apple MDM プッシュ証明書の登録	ABMとIntuneの連携	ABM上でデバイスをIntuneに割り当て	登録プロファイル作成	アプリ・構成プロファイル配布	iOS端末の初回セットアップ
Intune と Apple デバイス間の信頼通信を確立するための証明書を登録します。	ABM に Intune を MDM サーバーとして登録し、デバイス割り当て先を設定します。	ABM 上で購入済み端末を Intune に割り当て、自動登録対象とします。	デバイス登録時の設定内容（構成や認証方法など）を定義します。	Intune 経由で業務アプリやセキュリティ設定が端末に自動配布されます。	ユーザーが端末を起動し、プロファイルが自動適用され Intune に登録されます。

4.2. Apple MDM プッシュ証明書の登録

管理者作業

以下に登録手順をまとめています。Intune管理センター、Apple プッシュ証明書ポータルでの作業が必要となります。

■Intune管理センターでの作業

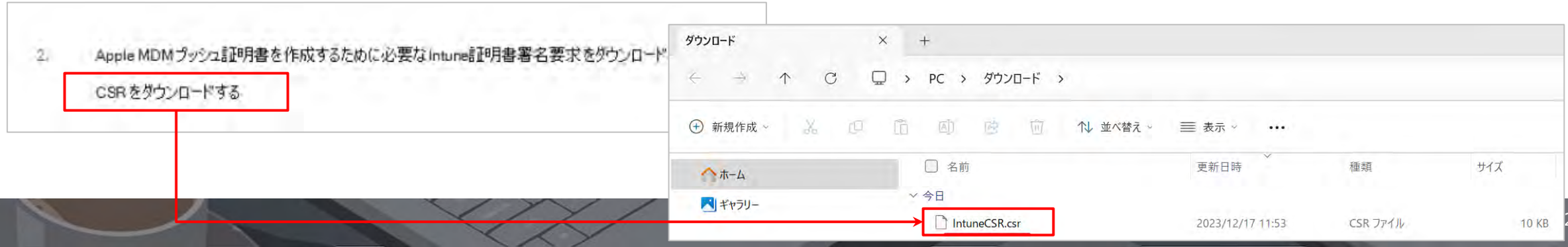


手順

1. Microsoft Intune 管理センターへアクセスしサインインします
2. [デバイス] ＞ [デバイスのオンボーディング] ＞ [登録]を選択します
3. [Apple]タブを選択します
4. [Apple MDM プッシュ証明書]を選択し、MDMプッシュ証明書の設定画面を開きます

4.2. Apple MDM プッシュ証明書の登録

管理者作業



手順

5. [ユーザー情報とデバイスの情報の両方をAppleに送信するためのアクセス許可をMicrosoftに付与します。] に [同意する]を選択します

5. [CSRをダウンロードする]を選択し、要求ファイルをダウンロードしてPCに保存します。（CSR ファイルは、Apple プッシュ通知証明書ポータルから信頼関係の証明書を要求するのに使用します。）

4.2. Apple MDM プッシュ証明書の登録

管理者作業

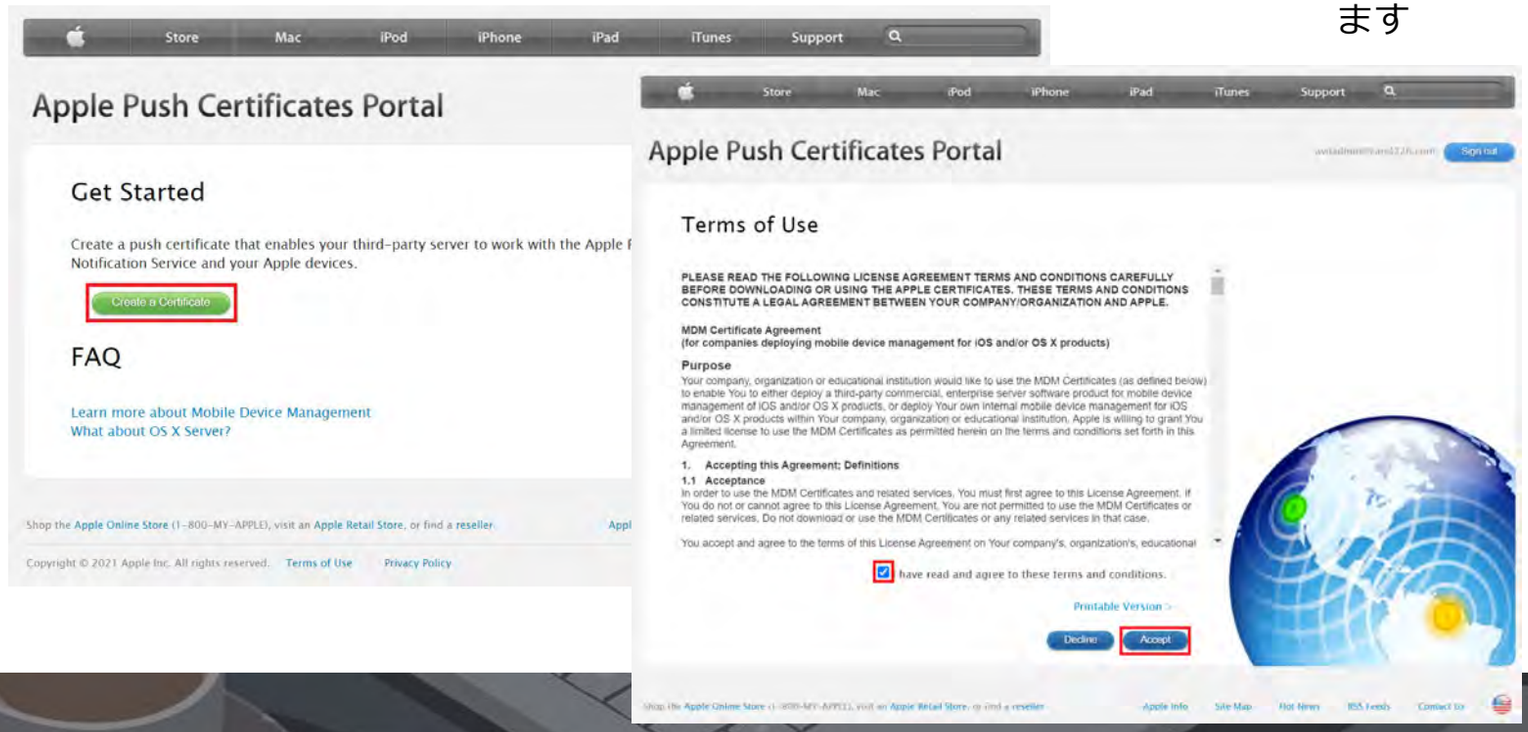
手順

7. [MDM プッシュ証明書を作成する]を選択して、Apple プッシュ通知証明書ポータルへ移動します。

4.2. Apple MDM プッシュ証明書の登録

管理者作業

■Apple プッシュ通知証明書ポータルでの作業

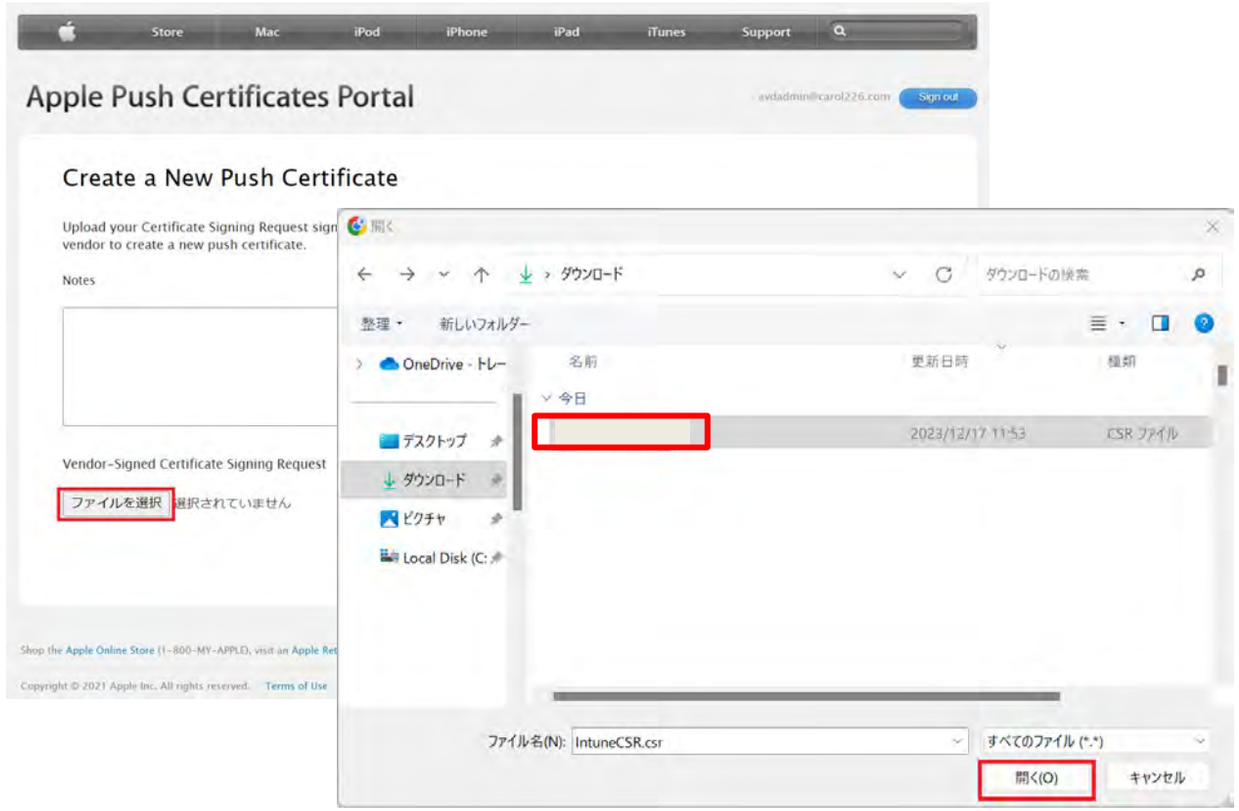


手順

1. 事前に手配していた会社のApple IDを入力し、ポータルにサインインします
2. Apple Push Certificates Portal にサインインされるため、[Create a Certificate] を選択します。
3. 契約条件を読み、同意欄にチェックを入れ [Accept] を選択します

4.2. Apple MDM プッシュ証明書の登録

管理者作業

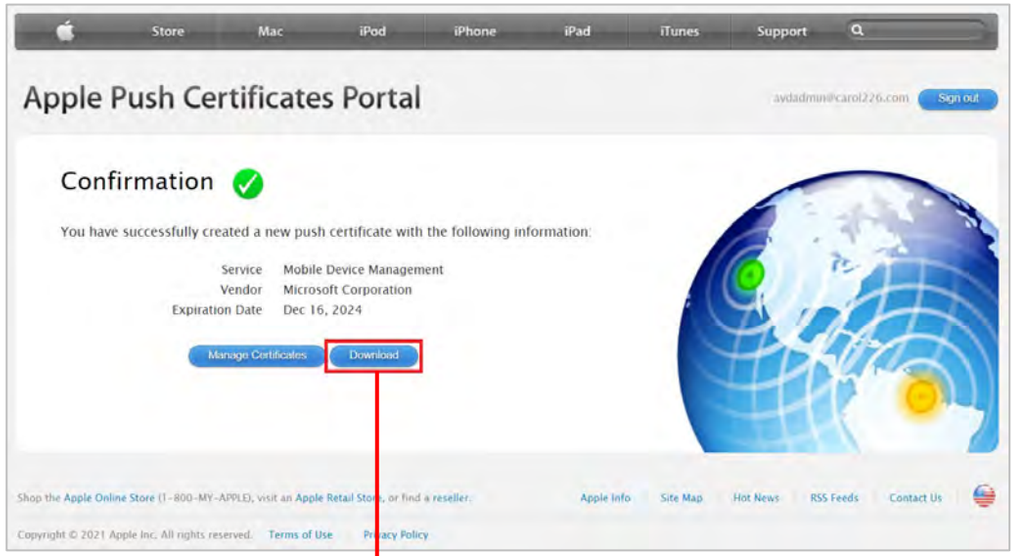


手順

4. [ファイルの選択]を選択し、Intune管理センターでダウンロードしたCSRファイルを選択します
5. ファイルが選択されたことを確認し、[Upload]を選択します

4.1. Apple MDM プッシュ証明書の登録

管理者作業



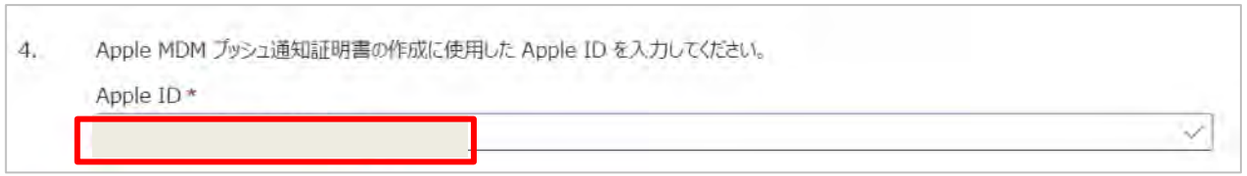
手順

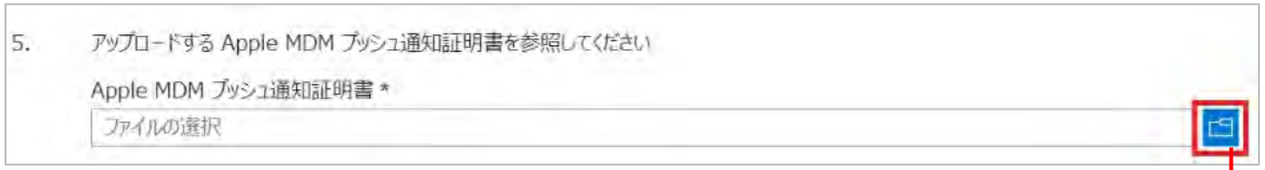
6. ”Confirmation”の画面で[Download]を選択します
　　証明書ファイル(.pem)がPCにダウンロードされます。のちに使用するためこのファイルは保存しておきます。

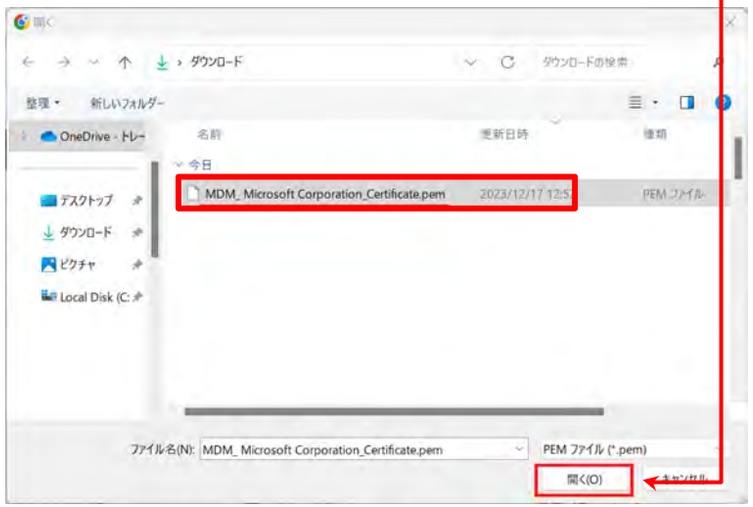
4.2. Apple MDM プッシュ証明書の登録

管理者作業

■ **Intune管理センターでの作業**







手順

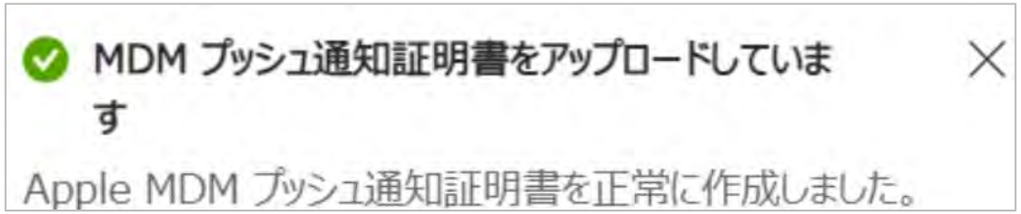
7. Intuneの管理センターにて、項番4にApple MDM プッシュ証明書の作成に使用したApple IDを入力します

7. 項番5にて[フォルダー]アイコンを選択します

7. Apple ポータルでダウンロードした証明書ファイル(.pem)を選択します

4.2. Apple MDM プッシュ証明書の登録

管理者作業



手順

10. 「アップロード」をクリックして、MDMプッシュ証明書の構成を完了します
11. その後[Apple MDM プッシュ通知証明書を正常に作成しました]と表示されれば完了です

4.3. ABMとIntuneの連携

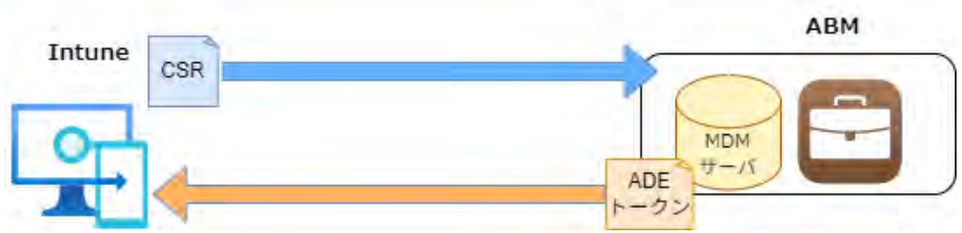
管理者作業

ABMと Intune の連携

ABMとIntuneの連携は、Appleが提供するADEの仕組みを使うために必要です。
iOS端末を安全かつ統一的に管理するためには、ABMとIntuneの連携が不可欠です。
この連携により、端末を開封して起動するだけで自動的にIntuneに登録され、従業員がMDM登録をスキップすることができなくなります。
さらに、設定やアプリを一括で配布できるため、初期設定の手間を大幅に削減でき、管理のばらつきや登録漏れといったリスクも防止できます。つまり、ABMとの連携は、セキュリティの確保と運用効率の両立を実現するための重要な仕組みです。

作業の流れ

1. Intune で CSR（証明書署名要求）を作成・ダウンロード
2. ABM にログインし、MDM サーバーを作成（CSRファイルをアップロード）
3. ABM から発行される ADEトークン（.p7m）をダウンロード
4. Intuneにて、ABM からダウンロードしたトークンをアップロードし登録完了



4.3. ABMとIntuneの連携

管理者作業

■Intune管理センターでの作業

手順

手順①：CSRファイルの作成

1. Microsoft Intune 管理ポータルにアクセスします
2. 左メニューから、「デバイス」＞[デバイスのオンボーディング]から「登録」を選択します
3. 「登録プログラムのトークン」を選択します

4.3. ABMとIntuneの連携

管理者作業

手順

4. 基本タブで次の操作を行います

・[ユーザー情報とデバイスの情報の両方を Apple に送信するためのアクセス許可をMicrosoftに付与します]に[同意する]にチェックを いれます

・[トークンを作成するために必要なIntune公開キー証明書をダウンロードします。] を選択します

CSRファイル（.csr）をダウンロードし、ローカルに保存します

このファイルを次のステップでABMにアップロードします

4.3. ABMとIntuneの連携

管理者作業

■ABMでの作業

手順

手順②：MDMサーバー作成

1. ABM にサインインします
2. 「環境設定」＞「MDMサーバー」＞「追加」 を選択します
3. 以下の情報を入力します
   ・入力名前：例）Intune MDM
   ・トークンアップロード：手順①にてIntuneからダウンロードした .csr ファイルをアップロードします
   「保存」または「続行」をクリックします

手順③：ABMからトークン（.p7m）をダウンロード

1. アップロードが完了すると、ABMが トークン（.p7mファイル） を生成します
2. そのファイルをPCにダウンロードします

4.3. ABMとIntuneの連携

管理者作業

■Intune管理センターでの作業

手順

手順④：トークンをアップロード

1. Microsoft Intune 管理ポータルにアクセスします
2. 左メニューから　「デバイス」＞「iOS/iPadOS登録」＞「Enrollment Program トークンの追加] をクリックします
3. トークンの作成画面が表示されるので以下の情報を入力します
   ・名前：任意
   ・MDMサーバーの名前：任意
   ・トークンファイル：ABMからダウンロードしたファイルをアップロードします

1. 「次へ」をクリックします
2. 内容を確認して問題なければ[作成]をクリックします
3. 正常に完了すると、Intuneに[Enrollment programトークン]が登録され、ABMとIntuneが接続された状態になります

4.4. ABM上でデバイスをIntuneに割り当て

管理者作業

ABM上でデバイスをIntuneに割り当て

iOS端末を自動的にIntuneに登録させるため（ADE＝自動デバイス登録）に必要な作業となります。
ABMでは、Appleが出荷・販売した端末を管理対象として扱いますが、どのMDM（Intuneなど）で管理させるかは明示的に「割り当て」をする必要があります。
割り当てが行われていない場合、デバイスを起動しても Intuneに登録されず、自動構成・管理が行えません。

■ABMでの作業

手順

手順①：対象デバイスを検索して選択

1. ABM にサインインします
2. 左上の「デバイス」をクリックします
3. 「検索」ボックスに以下のいずれかで検索します
   - シリアル番号
   - オーダー番号（出荷番号）
   - デバイスの種類
4. 検索結果から該当デバイスをチェックボックスで選択します

4.4. ABM上でデバイスをIntuneに割り当て

管理者作業

手順

手順②： MDMサーバー（Intune）に割り当て

1. 右上の「アクション」メニューから「サーバに割り当て」を選択します
2. MDMサーバーの一覧から、Intune用に作成したサーバー名を選択します
3. 「続行」＞「完了」で設定反映されます

この割り当てが完了すると、該当iOSデバイスが開封・初期起動された際、自動的にIntune登録処理が開始されます。

4.5. 登録（Enrollment）プロファイル作成

管理者作業

Intuneで登録プロファイル作成

ABM でIntuneとデバイスを連携しただけでは、iOS端末にどのような設定を適用すべきかまでは定義されていません。
そのため、Microsoft Intune側で「iOS登録プロファイル（ADE用）」を作成し、
対象のデバイスに初期設定を指示する必要があります

■Intune管理センターでの作業

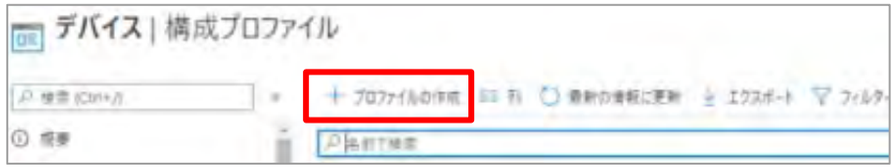
手順

手順①：登録プロファイルを作成

1. Microsoft Intune 管理ポータルにアクセスします
2. 左メニューから「デバイス」＞「iOS/iPadOS登録」＞「Enrollment Program トークン」を選択します
3. 作成済みのADEトークンを選択します

4.5. 登録プロファイル作成

管理者作業



手順

手順②： プロファイル作成/設定

1. トークンの詳細画面でタブ[プロファイル]を選択し「プロファイルの作成」をクリックします
2. プロファイルの基本情報を入力します（名前・説明等）
3. プロファイルの構成内容を指定します。

手順③： プロファイルの割り当て

1. デバイスに対して割り当てるグループを選択します（事前にグループの設定必要あり）
2. 内容を確認して[作成]をクリックします

4.6. アプリ・設定の配布

管理者作業

アプリ・構成プロファイルの配布

ABMとIntuneの連携、ユーザーによる端末登録が完了しただけでは、iOSデバイスにはまだ業務に必要なアプリケーションやネットワーク・セキュリティ設定が適用されていません。このステップでは、Intuneを通じて以下を配布・適用します。

- 業務用アプリ（App Store / 独自アプリ）
- カメラやApp Store制限、パスコード設定などの構成ポリシー
- Wi-Fi、VPN、メールなどの自動設定

アプリや構成プロファイルは、端末が Intune に登録された時点で自動配布されるよう、**事前に Intune 側で作成・割り当てを済ませておく必要があります。**

■Intune管理センターでの作業

手順

手順①：業務アプリの配布設定

1. Intune 管理ポータル → 左メニュー「アプリ」＞「iOS/iPadOS」を開きます

4.6. アプリ・設定の配布

管理者作業

手順

2. 「追加」をクリックします
3. [iOSストアアプリ]を選択し、「選択」をクリックします
4. [アプリストアを検索します]をクリックします

4.6. アプリ・設定の配布

管理者作業

手順

5. 検索先のAppleストアの国を[日本]に変更し。配布するアプリを検索します
6. 検索結果の一覧から対象アプリを選択し、[選択]をクリックします

4.6. アプリ・設定の配布

管理者作業

手順

7. アプリの情報が表示されます。利用方法にあわせて設定し、[次へ]をクリックします
8. [Required] の項目にアプリの自動配布先グループを指定します。

4.6. アプリ・設定の配布

管理者作業

手順

9. アプリの配布の設定が完了しました。
このアプリ配布設定が iOS/iPadOS デバイスに展開されると、画面上にアプリのインストール画面が表示されます。
[インストール] をタップすると、アプリがインストールされます。

手順②： 構成プロファイルの作成と配布

1. Intune 管理ポータル → 「デバイス」＞「iOS/iPadOS」＞「構成プロファイル」へ進みます
2. 「プロファイルの作成」をクリックします
3. プラットフォーム：iOS/iPadOS、プロファイルの種類：テンプレートを選択します
4. 各項目を必要に応じて構成し、割り当て対象のデバイスグループを指定します
5. 対象端末にIntune端末登録完了後、自動的に適用されます

Intune 側であらかじめ構成プロファイルや業務アプリを設定し、対象のデバイスグループに割り当てておくことで、
初期セットアップ完了後の iOS 端末に対し、自動的にアプリとポリシーが配布され、利用準備が整います。

4.7. iOS端末の初回セットアップ（ゼロタッチ導入）

従業員作業

iOS端末の初回セットアップ

従業員が業務用iPhone・iPadを初めて起動し、会社の管理下で使用可能な状態にするための重要なステップです。ABM で Intune に割り当て済みの iOS 端末を、ユーザーが初めて起動すると、
AppleのADEにより、MDM構成が自動的に適用され、企業管理下の Intune 登録デバイスとしてセットアップされます。
これにより、手動での設定や管理者の初期対応を一切不要にし、業務利用できる状態へ自動構成されます（ゼロタッチ導入）。

手順

1. iOS端末の電源をオンにします
   Wifiに接続します
1. リモートマネージメント画面が表示されるので、「次へ」をクリックします。これにより端末がIntuneのMDMサーバーへ自動登録され、構成プロファイルの適用が開始されます。
2. Microsoft アカウントでサインインをします（必要に応じて）
3. 自動的に構成プロファイル・アプリが適されます