



Microsoft 365 Enterprise セキュリティ基礎と応用

(EMS - Microsoft Intune、
Azure Information Protection、
Microsoft Cloud App Security)

レベル 200 - 300

© 2021 Microsoft Corporation. All rights reserved.

本情報の内容（添付文書、リンク先などを含む）は、作成日時点でのものであり、予告なく変更される場合があります。

2-1

2章： Microsoft Intune

- Intune の概要
- Intune によるモバイル デバイス管理 (MDM)
- Intune によるモバイル アプリ管理 (MAM)
- Microsoft Defender for Endpoint との統合
- デバイスの登録
- Windows 10 の Azure AD 参加とハイブリッド Azure AD 参加



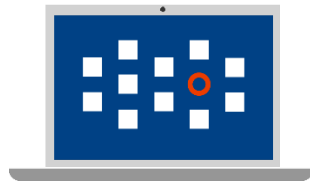
エンドポイントの管理

2 章



ID とアクセス
の管理

Azure Active
Directory
Premium



オンプレミスの
ID 保護

Microsoft
Defender for
Identity
(Azure ATP)



エンドポイント
の管理

Microsoft
Intune +
Configuration
Manager



情報の保護

Azure
Information
Protection
(AIP)



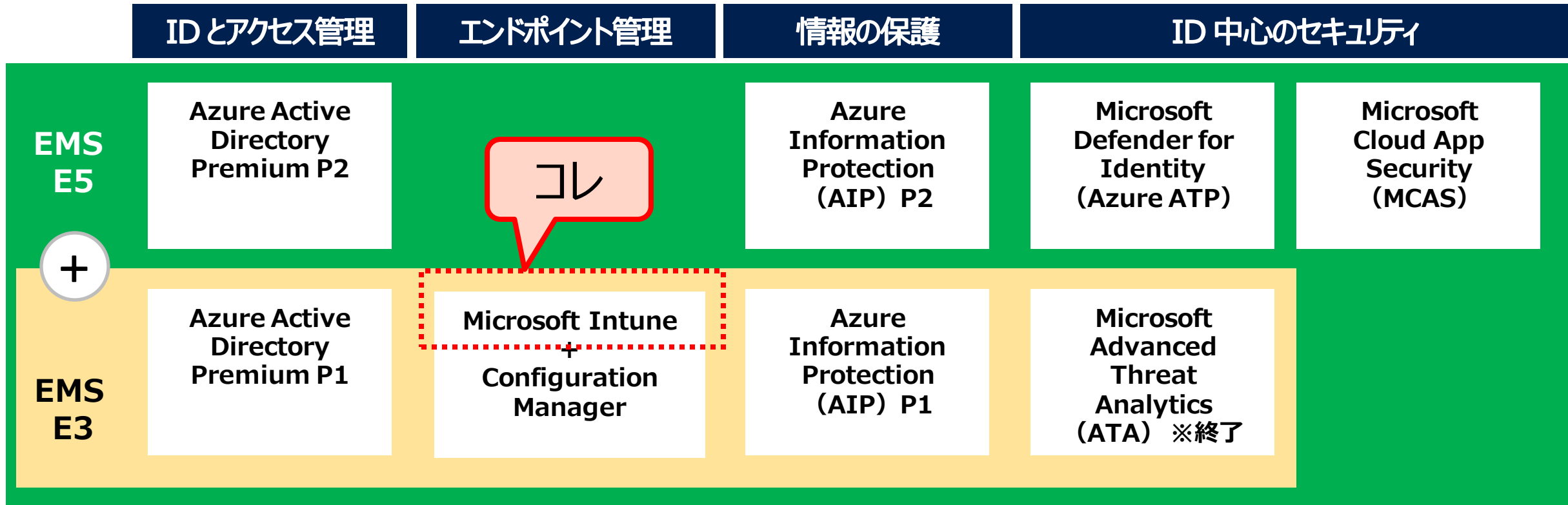
クラウド アプリの
セキュリティ

Microsoft Cloud
App Security
(MCAS)

Enterprise Mobility + Security (EMS) E5

Microsoft Intune ライセンス

- EMS E3 に、Microsoft Intune ライセンスが含まれる
- Microsoft Intune の中に、Microsoft Endpoint Configuration Manager を使用する権限も含まれる

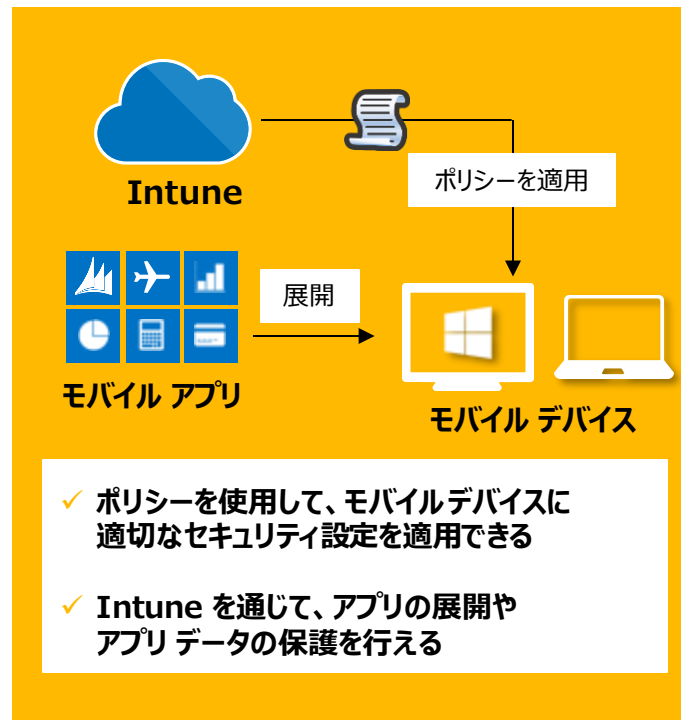


「Enterprise Mobility + Security 価格オプション」

<https://www.microsoft.com/ja-jp/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing>

Microsoft Intune とは

- マイクロソフトが提供する、パブリック クラウドの MDM/MAM サービス
 - iOS/iPadOS、Android、Windows、macOS デバイス、および モバイル アプリを管理する
 - デバイスやアプリを、組織のセキュリティ要件に準拠させることができる
 - それらのデバイスやアプリがアクセスする、組織のリソースやデータをセキュリティで保護する



MDM (Mobile Device Management)

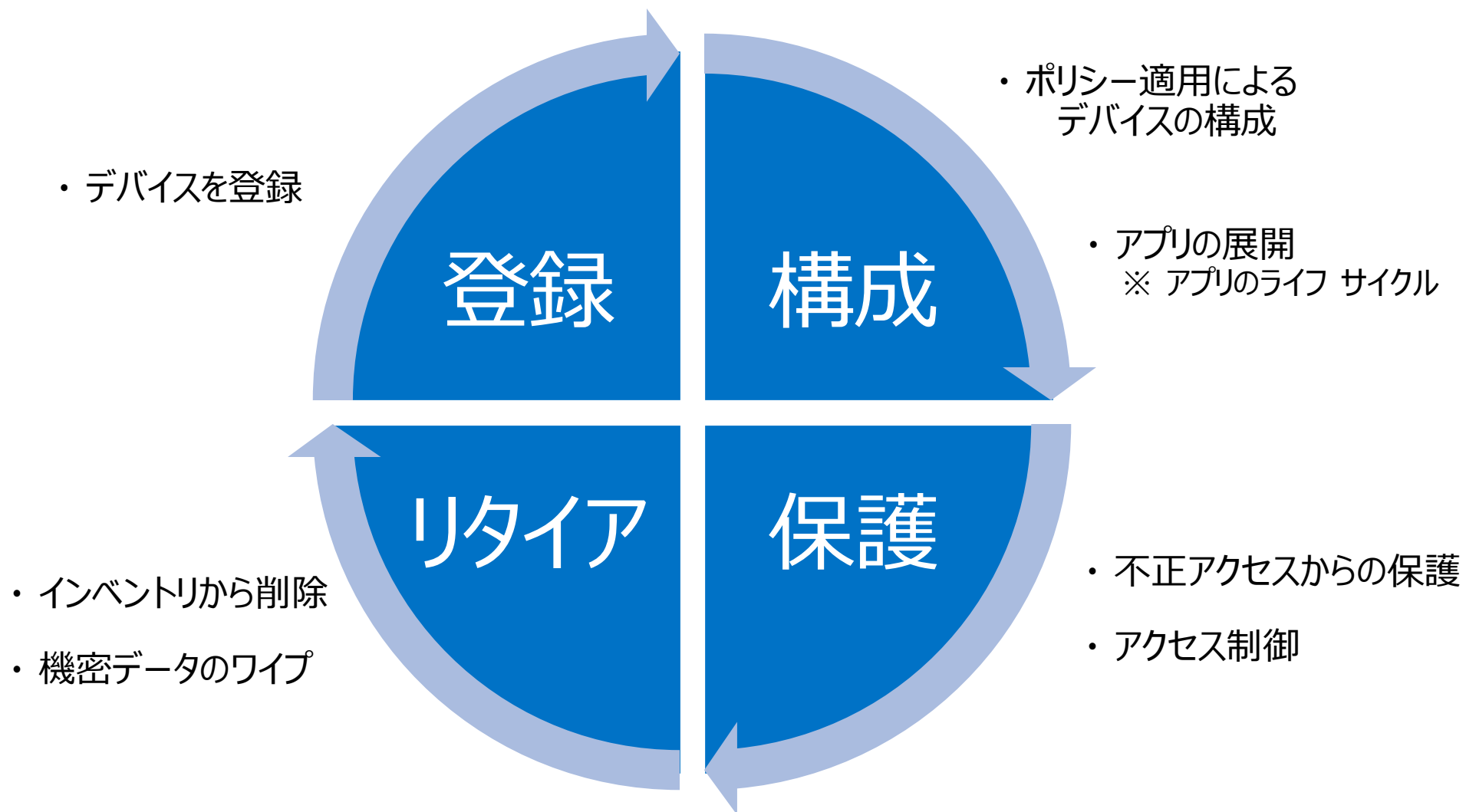
組織で所有するモバイル デバイスの管理
(スマートフォン、タブレット、ラップトップなど)

MAM (Mobile Application Management)

組織または個人のモバイル デバイス内の
アプリケーションやデータの管理

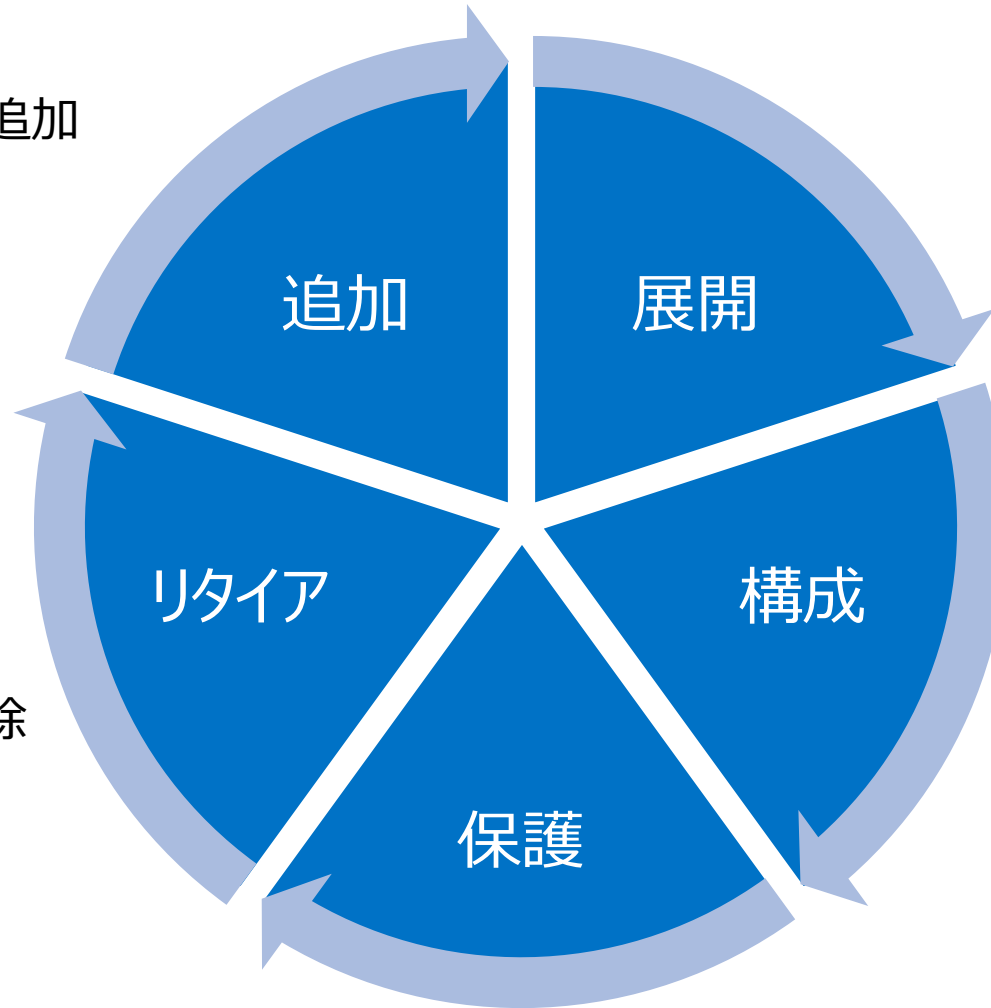
- 業務アプリケーションの展開
- 個人のアプリケーションやデータと切り離れたアクセス制限
- 紛失/盗難時の情報漏えい対策 など

モバイル デバイス管理 (MDM) のライフ サイクル



モバイル アプリ管理 (MAM) のライフ サイクル

- Intune へのアプリの追加
 - ストア アプリ
 - 自社開発アプリ



- 管理対象のユーザーとデバイスへのアプリの割り当て
- 使用状況の追跡

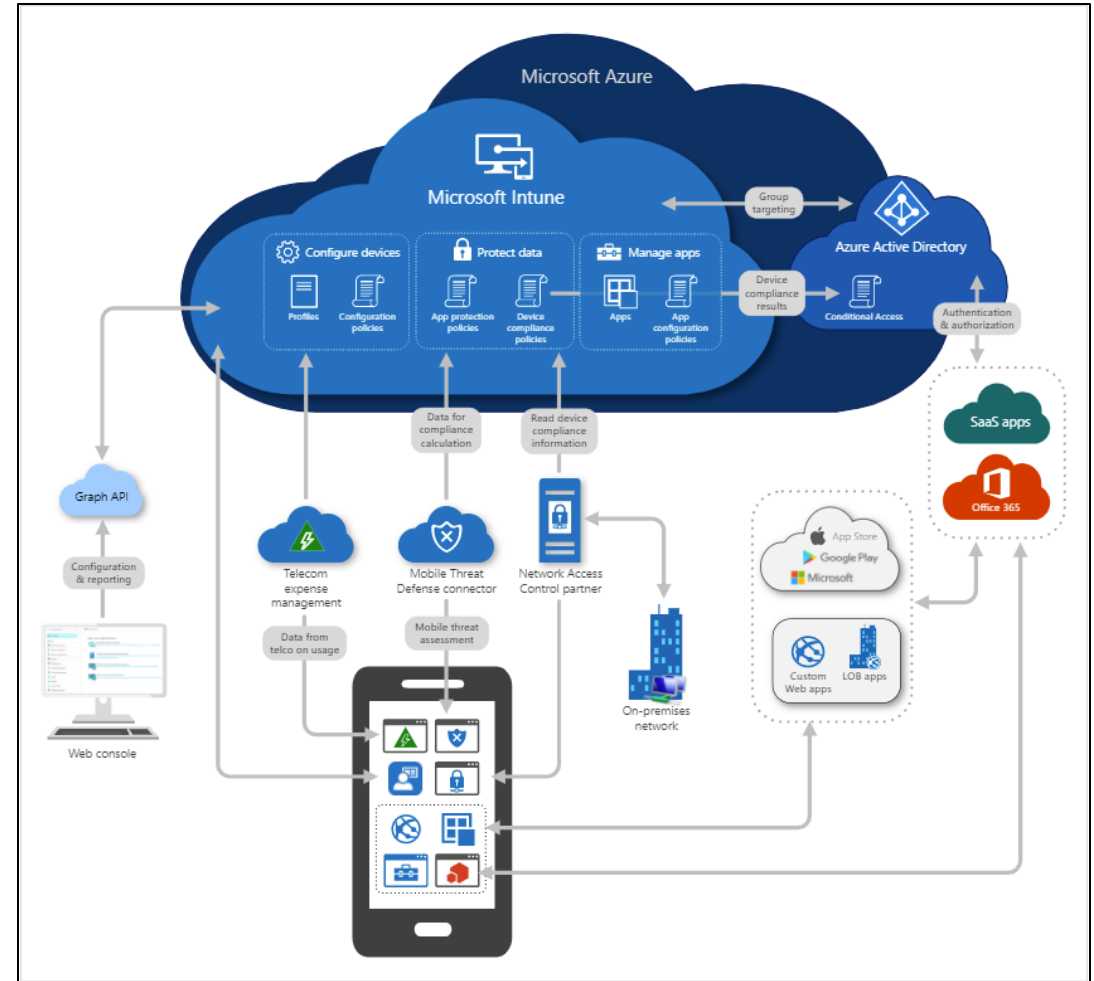
- インベントリから削除
- アンインストール

- アプリの更新
(新しいバージョンのリリース)

- アプリのデータ保護
 - 条件付きアクセス (アクセス制御)
 - アプリ保護ポリシー (会社データ保護)

Microsoft Intune のアーキテクチャ

- Intune は、Microsoft Azure と Microsoft 365 (EMS E3) に含まれているサービス
- Azure Active Directory と統合
 - Azure AD の強力な認証/認可、および Azure AD のセキュリティ機能を活用できる
例) 条件付きアクセス ポリシーなど
- アプリのデータ保護のため、Azure Information Protection (AIP) とも統合できる
- Microsoft 365 スイートのアプリとも統合できる
例) Microsoft Teams、OneNote など



「Microsoft Intune の概要」より引用

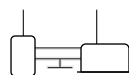
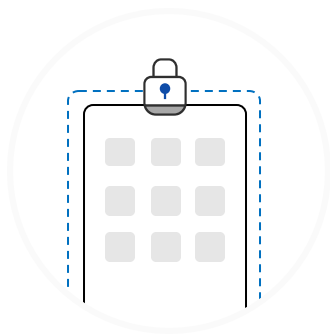
<https://docs.microsoft.com/ja-jp/mem/intune/fundamentals/what-is-intune>

MDM と MAM の Azure AD 条件付きアクセス ポリシー

Mobile Device Management (MDM)

条件付きアクセス ポリシー :

Intune で管理された
ポリシー準拠デバイスのみアクセスを許可



デバイスの
登録および管理



構成、証明書、
プロファイルの
プロビジョニング



レポート &
デバイス準拠の評価



デバイスから
会社データを削除

Mobile Application Management (MAM)

条件付きアクセス ポリシー :

Intune で保護された
アプリのみアクセスを許可



ユーザー向けの
モバイル アプリの展開



アプリの構成

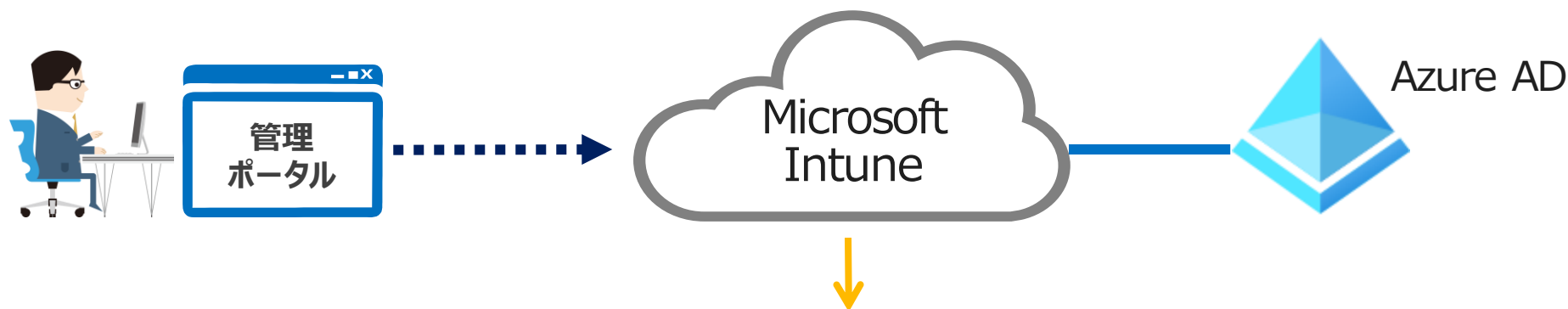


アプリ インベントリ
& 使用率をレポート



モバイル アプリを
保護、および
会社のデータを削除

Intune がサポートしているデバイスの OS



Apple

- Apple iOS 12.0 以降
- Apple iPadOS 13.0 以降
- macOS X 10.13 以降

Google

- Android 5.0 以降
- Android エンタープライズ

Windows

- Surface Hub
- Windows 10
- Windows 10 IoT Enterprise (x86、x64)
- Windows Holographic for Business
- Windows 10 Teams (Surface Hub)
- Windows 10 1709 (RS3) 以降、Windows 8.1 RT、Windows 8.1 (維持モード) が実行されている PC

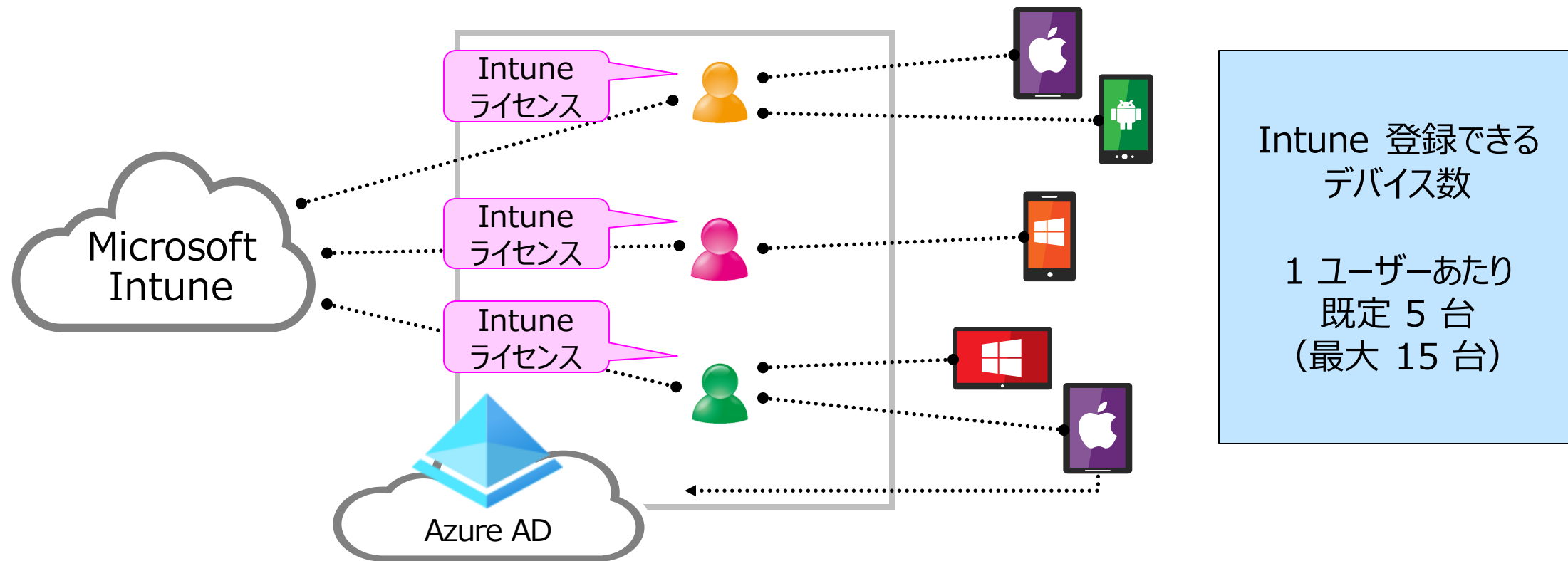


「Intune でサポートされるオペレーティング システムとブラウザー」

<https://docs.microsoft.com/ja-jp/mem/intune/fundamentals/supported-devices-browsers>

ユーザーとデバイスを紐づけた管理

- モバイル デバイスを Azure AD ユーザーと関連付けて管理する
- ユーザー単位のライセンス



Intune の一般的なシナリオ

- すべての従業員に BYOD (Bring your own device) を提供する
- 社員向けに、会社所有のスマートフォンを用意する
- 社員向けに、制限付きの共有タブレットを用意する
- 従業員が、管理されていない公共の場所から Microsoft 365 に安全にアクセスできるようにする

など

モバイル デバイスから
組織のリソースやデータに
安全にアクセスできるように
保護したい

「Microsoft Intune の一般的な使用方法」

<https://docs.microsoft.com/ja-jp/mem/intune/fundamentals/common-scenarios>

Intune のセットアップ手順

- 手順 1 : サポートされる構成や要件の確認
- 手順 2 : Intune へのサインイン
- 手順 3 : ドメイン名の構成
- **手順 4 : ユーザーとグループの追加**
- 手順 5 : ライセンスの割り当て

- 手順 6 : MDM 機能の設定 (1911 サービス リリース以降は自動設定)
- 手順 7 : アプリの追加 ※ 後述
- 手順 8 : デバイスの構成 ※ 後述
- 手順 9 : Intune ポータル サイトのカスタマイズ
- 手順 10 : デバイスの登録 ※ 後述
- 手順 11 : アプリ ポリシー構成 ※ 後述

「Intune をセットアップする」

<https://docs.microsoft.com/ja-jp/mem/intune/fundamentals/setup-steps>

手順 4 : ユーザーとグループの追加

- デバイスとユーザーの管理に、Azure AD のグループを使用
 - 地理的な場所、部門、ハードウェアの特性ごとにグループを作成し、ユーザーやデバイスを整理する
 - 特に、大規模なタスクを管理する際にグループを活用する

※ 動的デバイス グループの場合は、メンバーの反映に少し時間がかかる

例) デバイスをメンバーとする動的グループ

Microsoft Endpoint Manager admin center

ホーム > グループ > 新しいグループ ...

グループの種類 * ①
セキュリティ

グループ名 * ①
すべての Windows デバイス

グループの説明 ①
グループの説明を入力してください

グループに Azure AD ロールを割り当てることができる (プレビュー) ①
はい いいえ

メンバーシップの種類 * ①
動的デバイス

所有者
所有者が選択されていません

動的なデバイス メンバー * ①
動的クエリの編集

動的メンバーシップ ルール ...

保存 破棄 フィードバックがある場合

ルールの構成 ルールの検証 (プレビュー)

ルールビルダーまたはルール構文テキストボックスを使用して、動的メンバーシップの規則を作成または編集できます。 ① 詳細情報

および/または	プロパティ	演算子	値
	deviceOSType	Equals	Windows

+ 式の追加

規則の構文 編集

```
(device.deviceOSType -eq "Windows")
```

作成

2-2

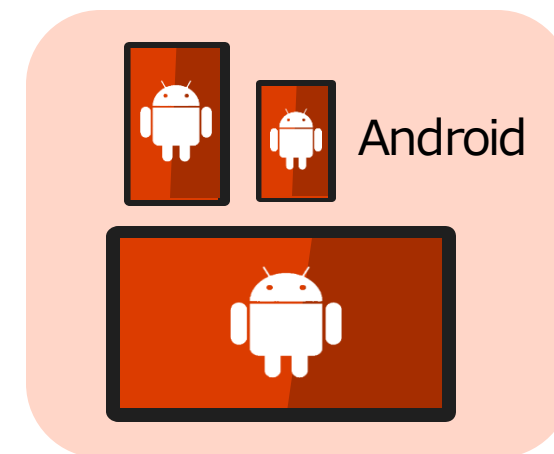
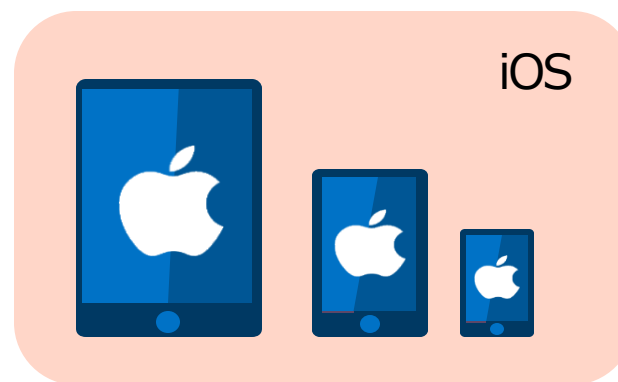
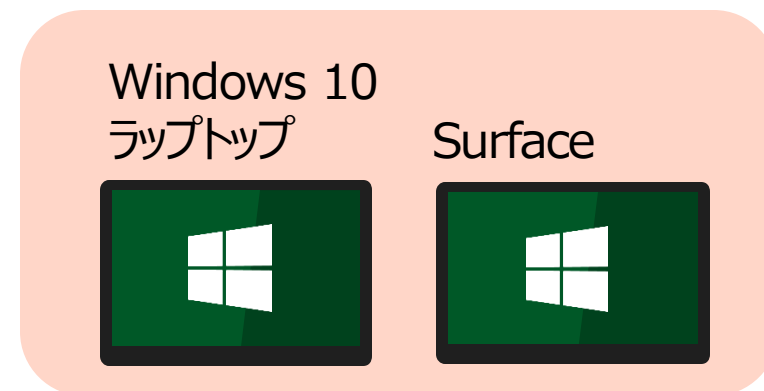
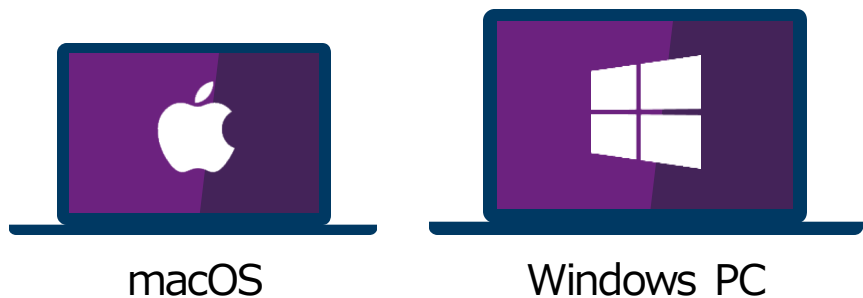
2章： Microsoft Intune

- Intune の概要
- Intune によるモバイル デバイス管理 (MDM)
- Intune によるモバイル アプリ管理 (MAM)
- Microsoft Defender for Endpoint との統合
- デバイスの登録
- Windows 10 の Azure AD 参加とハイブリッド Azure AD 参加



Intune によるデバイス管理 (MDM)

1. デバイス インベントリの表示
2. リモート デバイス アクションの実行
3. デバイスの構成と管理
4. デバイスのコンプライアンス管理

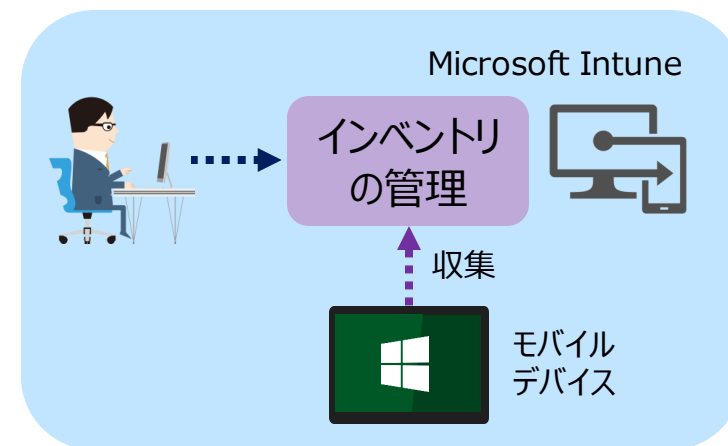


「Microsoft Intune デバイスの管理とは」

<https://docs.microsoft.com/ja-jp/mem/intune/remote-actions/device-management>

1. デバイス インベントリの表示

- Intune に登録されたデバイスは、自動的にインベントリを収集する
- 収集した情報を、管理ポータルで参照できる



[デバイス] - [すべてのデバイス] で対象となるデバイスを選択し、ハードウェアや検出されたアプリの情報を表示できる

「Intune でのデータ収集」

<https://docs.microsoft.com/ja-jp/mem/intune/protect/privacy-data-collect>

会社所有のデバイス

- Intune は、次のように登録されたデバイスを会社所有とする
 - デバイス登録マネージャー アカウントで登録されたデバイス・・・すべてのプラットフォーム
 - Apple Device Enrollment Program、Apple School Manager、Apple Configurator で登録されたデバイス・・・iOS/iPadOS
 - IMEI（International Mobile Equipment Identifier/国際携帯機器識別）番号で、登録前に会社所有と識別されたデバイス・・・IMEI 番号を持つすべてのプラットフォーム
 - シリアル番号で、登録前に会社所有として識別されたデバイス・・・iOS/iPadOS、macOS、Android
 - **職場または学校の資格情報を使用して Azure AD 参加したデバイス・・・Windows 10**
 - デバイスのプロパティで、会社として設定されているデバイス

※ Azure AD 登録されたデバイスは、個人用とマークされる

「デバイスの企業所有としての識別」

<https://docs.microsoft.com/ja-jp/mem/intune/enrollment/corporate-identifiers-add>

[応用] ユーザー所有のデバイス登録の許可/ブロック

- ユーザー所有のデバイス登録をブロックすることもできる（既定は許可）

Microsoft Endpoint Manager admin center

ホーム > デバイス > デバイスの登録 > すべてのユーザー

デバイス | デ... ×

検索 (Ctrl+/) << 検索 (Ctrl+/) << + 作成の制限 ↓

Windows 登録
Apple 登録
Android 登録
登録制限
業務用デバイスの ID
デバイス登録マネージャー

デバイスの登録 | 登録制限 ...

デバイスは、そのユーザーに割り当てられている優先順位の最も高い登録制限に準拠している必要があります。優先順位既定の制限を編集することはできませんが、削除することはできません。詳細をご覧ください。

デバイスの種類の制限
登録できるプラットフォーム、バージョン、および管理の種類を定義します。

優先度	名前	割り当て済み
既定	すべてのユーザー	はい

プラットフォームの設定 編集

種類	プラットフォーム	最小	最大	個人所有
Android Enterprise (仕事用プロファイル)	許可			許可
Android デバイス管理者	許可			許可
iOS/iPadOS	許可			許可
macOS	許可	N/A	N/A	許可
Windows (MDM)	許可			許可

[応用] 会社所有デバイスの事前登録

- 企業所有のデバイスのみを登録させるには、企業所有デバイスの ID (IMEI 番号、シリアル番号) の事前登録が必要

Microsoft Endpoint Manager admin center

ホーム > デバイス > デバイスの登録

デバイス | デ... ×

検索 (Ctrl+/)

概要

すべてのデバイス

モニター

プラットフォーム別

Windows

iOS/iPadOS

macOS

Android

デバイスの登録

デバイスの登録 | 業務用デバイスの ID ...

検索 (Ctrl+/)

+ 追加 ▼ 削除 最新の情報に更新

CSV ファイルのアップロード

手動で入力

識別子

結果なし

業務用デバイスの ID

デバイス登録マネージャー

ID の追加 ...

業務用デバイスの ID

デバイスの ID と詳細を追加するためにリストをインポートできます。

ID の種類を選びます ○

IMEI

IMEI

シリアル (Android, iOS, macOS のみ)

IMEI = International
Mobile Equipment
Identity

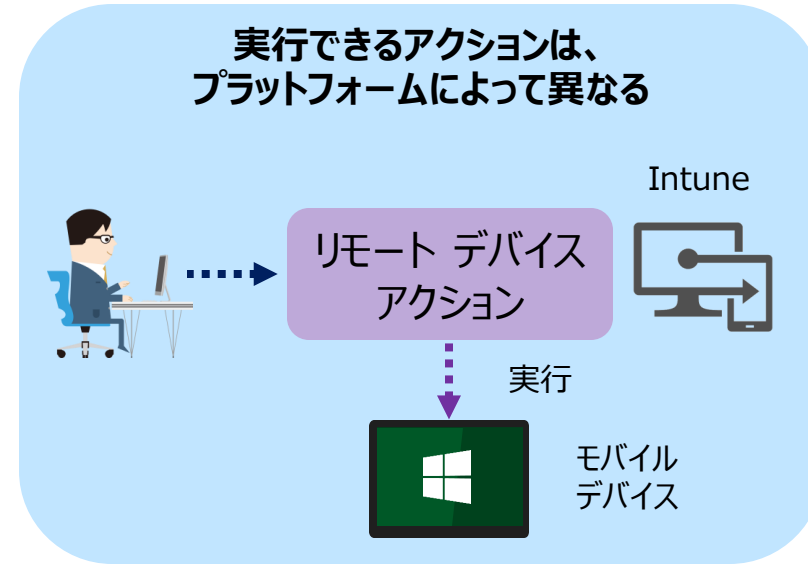
国際移動体装置識別番号
(端末識別番号)

2. リモート デバイス アクションの実行

- リモートから、さまざまな命令を実行できる

※ は、デバイスの一括操作が可能

- リモート ロック
- パスコードのリセット
- Windows 10 の PIN のリセット
- ワイプ ※
- インベントリから削除 ※
- デバイスの削除 ※
- 再起動 ※
- 紛失したデバイスの検索 (iOS/iPadOS のみ)
- 紛失モードの有効化 (iOS/iPadOS のみ)
- 監視モードの有効化 (iOS/iPadOS のみ)
- アクティベーション ロックの無効化 (iOS/iPadOS のみ)
- デバイスの同期 ※



- 現在のユーザーのログアウト (iOS/iPadOS のみ)
- 共有デバイスからユーザーを削除 (iOS/iPadOS のみ)
- プライマリ ユーザーの確認 など

「Microsoft Intune デバイスの管理とは」の「行えるデバイス アクション」

<https://docs.microsoft.com/ja-jp/mem/intune/remote-actions/device-management#available-device-actions>

例) デバイス紛失時の対応

リモートロック



出荷時の設定 (ワイプ)



パスコードのリセット



iOS/iPad デバイスの検索



3. デバイスの構成と管理

Windows 10
以降

- “デバイスの構成プロファイル” を使用して、管理対象デバイスのプラットフォームごとにデバイスの機能や構成を管理できる

プラットフォーム
を選択

プロフィールの作成

プラットフォーム

プラットフォームを選択

- Android デバイス管理者
- Android Enterprise
- iOS/iPadOS
- macOS
- Windows 10 以降**
- Windows 8.1 以降

プロフィールの作成

プラットフォーム

Windows 10 以降

プロフィールの種類

テンプレート

テンプレートには、機能ごとに整理された設定のグループが含まれています。ポリシーを手動で作成しない場合や、WiFi や VPN の構成など企業ネットワークにアクセスするようデバイスを構成する場合は、テンプレートを使用します。 [詳細を表示](#)

検索

テンプレート名

Endpoint Protection

Identity Protection

Microsoft Defender for Endpoint (Windows 10 デスクトップ)

PKCS のインポートされた証明書

PKCS 証明書

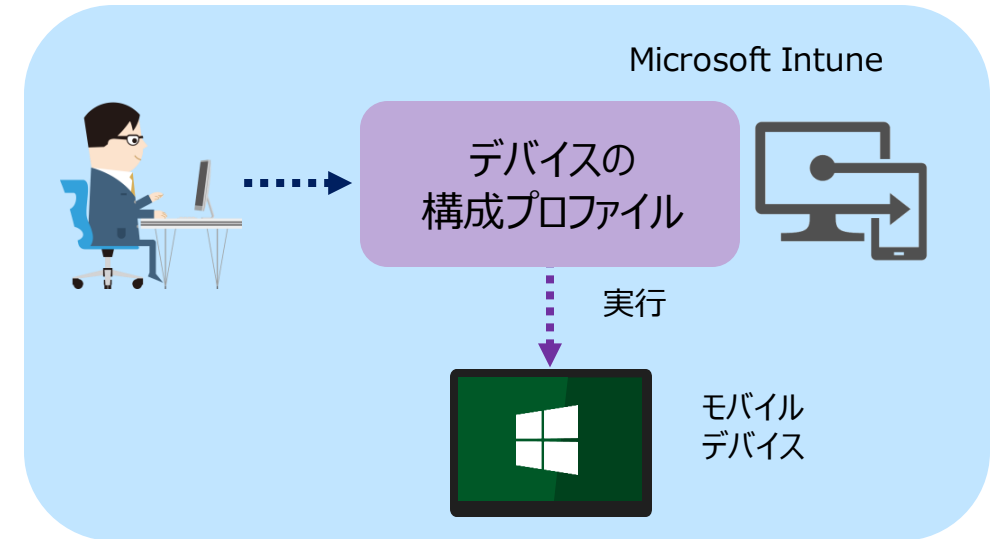
SCEP 証明書

VPN

作成

代表的なデバイスの構成プロファイル

- 証明書
- 電子メール
- VPN
- Wi-Fi
- デバイスの制限
- カスタム プロファイル
- デバイスの機能 (iOS/iPadOS、macOS)
- 更新ポリシー (iOS/iPadOS)
- 管理用テンプレート (Windows 10 以降)
- 配信の最適化 (Windows 10 以降)
- ドメイン参加 (Windows 10 以降)
- Defender for Endpoint (Windows 10 以降)
- ID 保護 (Windows 10 以降、Windows Holographic for Business) など

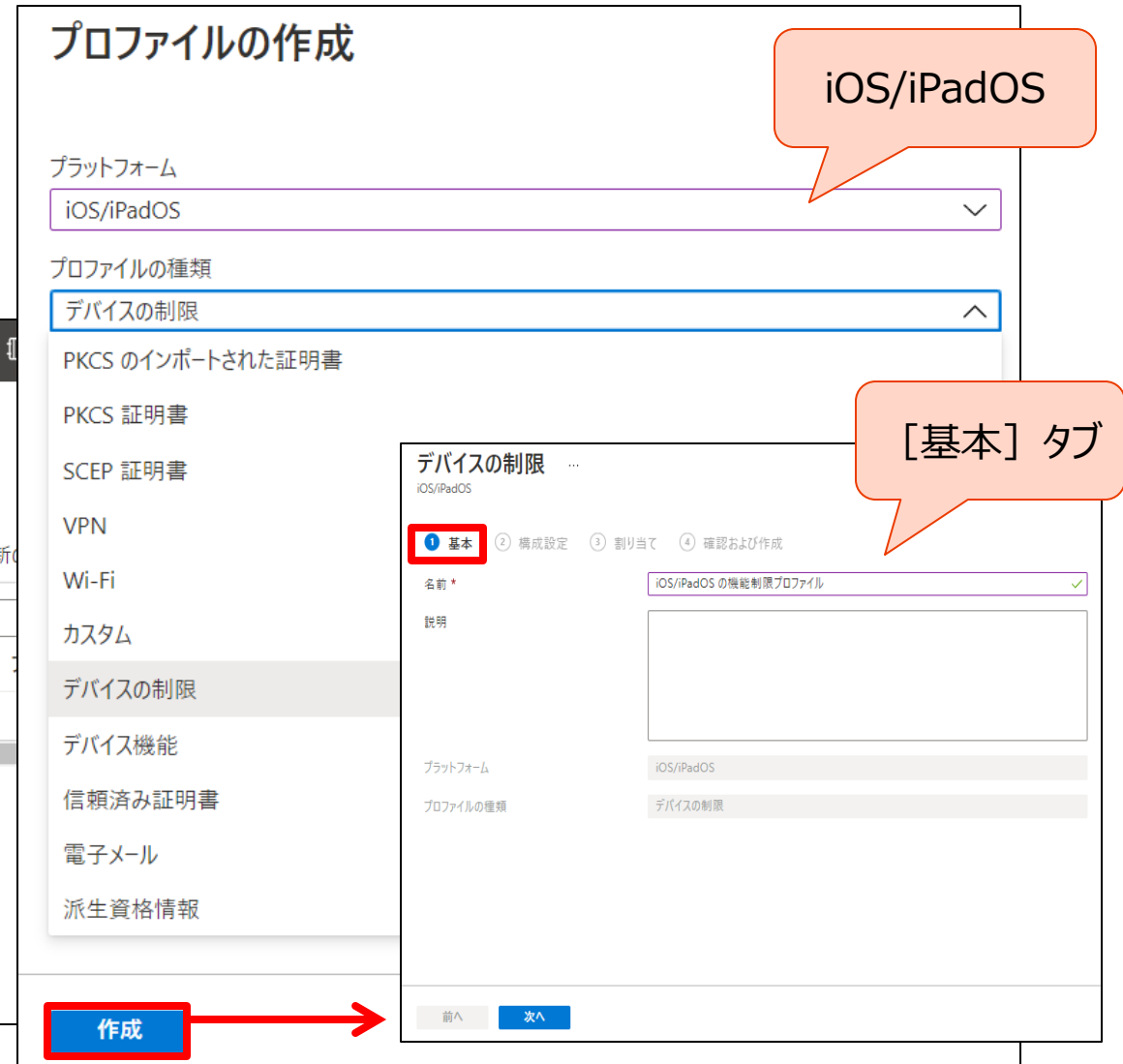
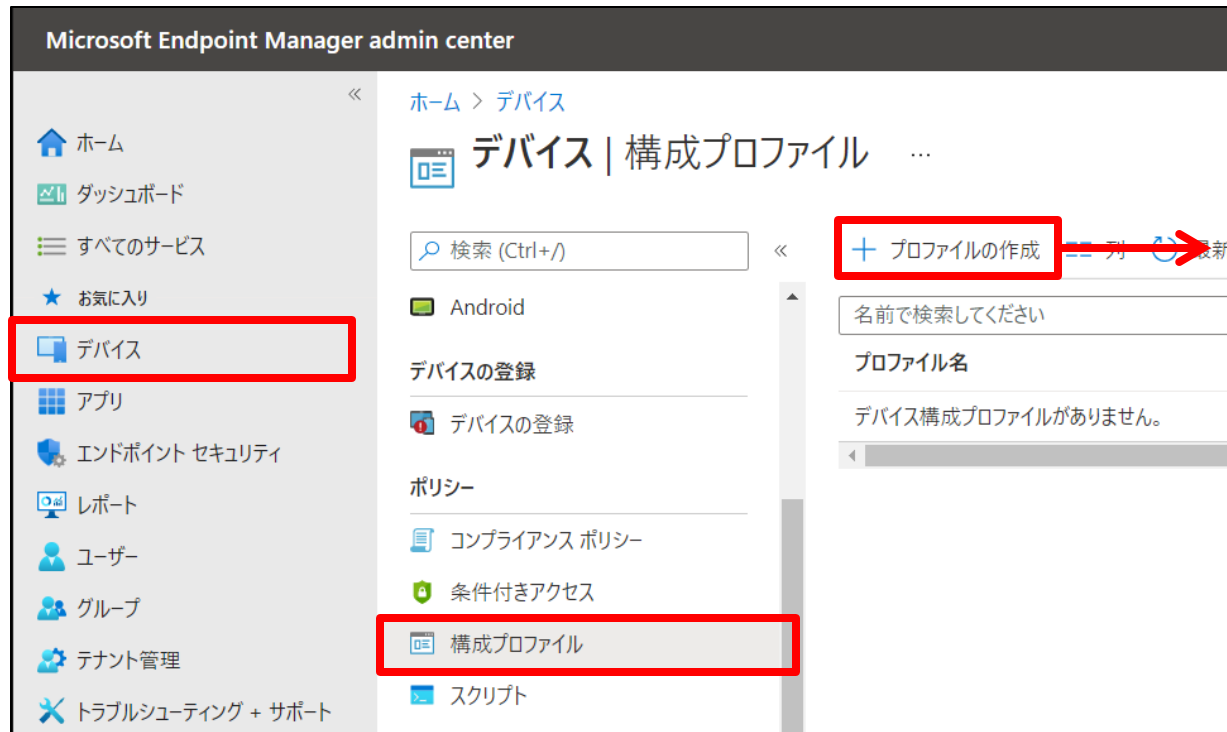


「Microsoft Intune でデバイス プロファイルを使用してデバイスに機能と設定を適用する」

<https://docs.microsoft.com/ja-jp/mem/intune/configuration/device-profiles>

例) iOS/iPadOS「デバイスの制限」プロファイルの作成

- [デバイス] - [構成プロファイル] の [プロファイルの作成] で、プラットフォームとプロファイルの種類を指定



[構成設定] タブ

デバイスの制限 ...
iOS/iPadOS

✓ 基本 2 構成設定 ③ 割り当て ④ 確認および作成

- ▼ アプリストア、ドキュメント表示、ゲーム
- ▼ 自律的シングル App モード
- ▼ 組み込みアプリ
- ▼ クラウドとストレージ
- ▼ 接続されているデバイス
- ▼ ドメイン
- ▼ 全般
- ▼ キーボードと辞書
- ▼ キオスク
- ▼ ロック画面の動作
- ▼ パスワード
- ▼ 制限付きアプリ
- ▼ Shared iPad
- ▼ アプリの表示/非表示
- ▼ ワイヤレス

前へ 次へ

デバイスの制限 ...
iOS/iPadOS

✓ 基本 2 構成設定 ③ 割り当て ④ 確認および作成

- ▼ アプリストア、ドキュメント表示、ゲーム
- ▼ 自律的シングル App モード
- ▼ 組み込みアプリ
- ▼ クラウドとストレージ
- ▲ 接続されているデバイス

すべての登録の種類

これらの設定は、デバイス登録またはユーザー登録によって Intune に登録されたデバイスと、Apple School Manager または Apple Business Manager を使用して自動デバイス登録 (以前の DEP) によって登録されたデバイスに対して有効です。これには、すべての監視対象デバイスが含まれます。

Apple Watch の手首検出を強制する ⓘ はい 構成されていません

デバイスの登録とデバイスの自動登録

これらの設定は、デバイス登録によって Intune に登録されたデバイスと、Apple School Manager または Apple Business Manager を使用して自動デバイス登録 (以前の DEP) によって登録されたデバイスに対して有効です。これには、すべての監視対象デバイスが含まれます。

AirPlay 送信要求のペアリング パスワードが必須 ⓘ はい 構成されていません

デバイスの自動登録

これらの設定は、Apple School Manager または Apple Business Manager を使用してデバイスの自動登録 (以前の DEP) によって Intune に登録された監視対象デバイスに対して有効です。これには、Apple Configurator で監視されているデバイスが含まれます。

AirDrop をブロックする はい 構成されていません

Apple Watch とのペアリングをブロックする はい 構成されていません

前へ 次へ

「Microsoft Intune でのデバイス プロファイルの作成」

<https://docs.microsoft.com/ja-jp/mem/intune/configuration/device-profile-create>

[割り当て] タブ

- デバイス構成プロファイルを適用したい Azure AD グループを指定

<構成プロファイルの段階的な展開>

Pilot 用のユーザー グループと Full-Scale 用のユーザー グループを作成

Pilot 用の構成プロファイルと Full-Scale 用の構成プロファイルを作成

設定の変更や展開を、 Pilot 用の構成プロファイルから行う

The screenshot shows the 'Assign' tab in the Azure AD console for a device restriction profile. The title is 'デバイスの制限' (Device Restrictions) with a subtitle 'iOS/iPadOS'. The progress bar shows four steps: 1. 基本 (Basic), 2. 構成設定 (Configuration), 3. 割り当て (Assign) - highlighted with a red box, and 4. 確認および作成 (Review and Create). Below the progress bar, there are three options to add groups: 'グループを追加' (Add group), 'すべてのユーザーを追加' (Add all users), and 'すべてのデバイスを追加' (Add all devices). The 'グループ' (Groups) section shows a table with one entry: '営業グループ' (Sales Group) with a '削除' (Delete) button. Below this, there is a section for '除外されたグループ' (Excluded groups) with a blue information box stating: 'グループを除外する場合、"含める"と"除外する"でユーザーとデバイスのグループを同時に指定することはできません。詳細については、ここをクリックしてください。' (When excluding a group, you cannot specify user and device groups at the same time using 'Include' and 'Exclude'. For more details, click here.). At the bottom, there are two buttons: '前へ' (Previous) and '次へ' (Next).

ユーザー グループとデバイス グループ

適用先にどちらを指定するかは、目標によって異なる

• ユーザー グループ

- 常にユーザーに対して適用される
- ユーザーが使用するデバイスに関係なく、プロファイルで構成した設定や規則を常にユーザーに対して有効にする場合は、ユーザー グループを使用する

- 例 1) あるユーザーが 職場用に Surface Pro と 個人用に iOS を使用していて、両方のデバイスに、組織のヘルプ デスク アイコンを配置したい
- 例 2) ユーザーが、会社所有の新しいデバイスを受け取り、自身の Azure AD アカウントでデバイスにサインインすると、Azure AD に自動的に登録され、Intune によって自動的に管理されているデバイス
- 例 3) ユーザーがデバイスにサインインするたびに、OneDrive や Office などのアプリの機能を制御することが必要な場合

• デバイス グループ

- 常にデバイスに対して適用される
- どのユーザーがサインインしているかに関係なく、プロファイルで構成した設定や規則を常にデバイスに対して有効にする場合は、デバイス グループを使用する

- 例 1) 専用ユーザーがないデバイスの管理に便利
- 例 2) デバイスを使用しているユーザーに関係なく、デバイスのカメラを無効にしたい
- 例 3) デバイスを使用しているユーザーに関係なく、Microsoft Edge の一部の設定を制御したい (ダウンロードのブロック、Cookie の構成など)

デバイスのチェックイン スケジュール

構成プロファイル、デバイスコンプライアンスポリシー、アプリ、アプリ保護ポリシー



- プラットフォームごとに異なる
- ユーザーが手動で同期を実行することもできる

プラットフォーム	頻度
iOS/iPadOS	1 時間まで 15 分ごと、その後は約 8 時間ごと
macOS	1 時間まで 15 分ごと、その後は約 8 時間ごと
Android	15 分まで 3 分ごと、その後の 2 時間は 15 分ごと、その後は約 8 時間ごと
デバイスとして登録された Windows 10 PC	15 分まで 3 分ごと、その後の 2 時間は 15 分ごと、その後は約 8 時間ごと
Windows Phone	15 分まで 5 分ごと、その後の 2 時間は 15 分ごと、その後は約 8 時間ごと
Windows 8.1	15 分まで 5 分ごと、その後の 2 時間は 15 分ごと、その後は約 8 時間ごと

「Microsoft Intune でのデバイス ポリシーとプロファイルの一般的な質問と回答」

<https://docs.microsoft.com/ja-jp/intune/configuration/device-profile-troubleshoot#how-long-does-it-take-for-devices-to-get-a-policy-profile-or-app-after-they-are-assigned>

Tips ! デバイス構成プロファイル

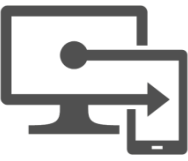
複数のポリシーが同じユーザーまたはデバイスに割り当てられている場合、

- 制限レベルが異なる 2 つの構成プロファイルが適用された場合、より安全なポリシーが優先される
- 複数の構成プロファイルの設定が競合する場合、Intune に競合の状況が表示される（手動で解決する）

「Microsoft Intune でのデバイス ポリシーとプロファイルの一般的な質問と回答」の「複数のポリシーが同じユーザーまたはデバイスに割り当てられる場合、どの設定が適用されるのかどうすればわかりますか」
<https://docs.microsoft.com/ja-jp/mem/intune/configuration/device-profile-troubleshoot#if-multiple-policies-are-assigned-to-the-same-user-or-device-how-do-i-know-which-settings-gets-applied>



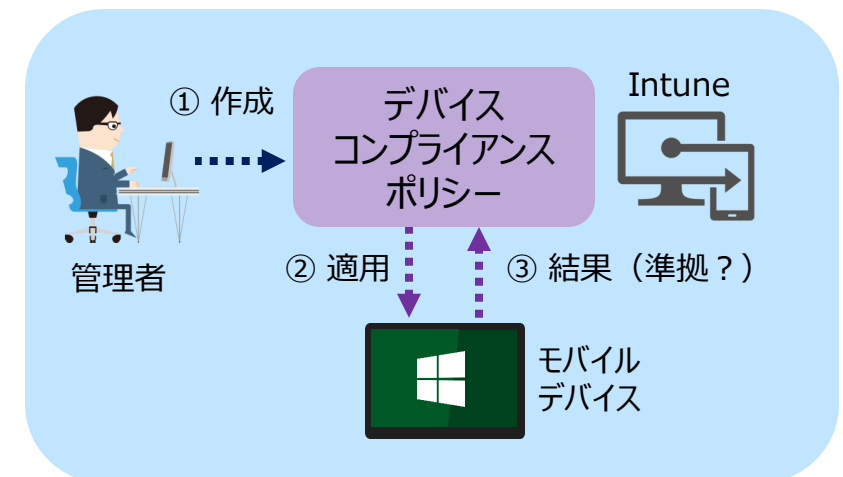
4. デバイスのコンプライアンス管理



- “**コンプライアンス ポリシー**” は、組織のデータを保護するために、ユーザーやデバイスが 守るべきルールおよび設定の定義
 - 準拠ユーザーおよびデバイスであるために満たす必要があるルールや設定の定義
 - 非準拠のデバイスに適用されるアクション
 - 条件付きアクセスと組み合わせて、ルールを満たしていないユーザーとデバイスをブロック

「コンプライアンス ポリシーを使用して、Intune で管理するデバイスのルールを設定する」

<https://docs.microsoft.com/ja-jp/mem/intune/protect/device-compliance-get-started>



2つのコンプライアンスポリシー

- Intune のコンプライアンス ポリシーは、次の 2 つの組み合わせで評価される

① コンプライアンス ポリシー設定



② デバイス コンプライアンス ポリシー

- すべてのデバイスに適用される、テナント全体の設定
- Intune 環境でのコンプライアンス ポリシーの動作のベースラインの設定

- ユーザーまたはグループに割り当てる、プラットフォームごとのルール
 - パスワードを使用したデバイスへのアクセス
 - 暗号化
 - デバイスが脱獄またはルート化されているか
 - 必要な最小 OS バージョン
 - 許可される最大 OS バージョン など

① コンプライアンス ポリシー設定

- [デバイス] – [コンプライアンス ポリシ] の [コンプライアンス ポリシー設定]

Microsoft Endpoint Manager admin center

ホーム > デバイス > コンプライアンス ポリシー

デバイス | ... ×

検索 (Ctrl+/)

概要

すべてのデバイス

モニター

プラットフォーム別

Windows

iOS/iPadOS

macOS

Android

デバイスの登録

デバイスの登録

ポリシー

コンプライアンス ポリシー

条件付きアクセス

コンプライアンス ポリシー | コンプライアンス ポリシー設定 ...

検索 (Ctrl+/)

保存 × 破棄

ポリシー

通知

準拠していないデバイスの削除

場所

コンプライアンス ポリシー設定

これらの設定では、コンプライアンス サービスでデバイスを処理する方法を構成します。各デバイスでは、デバイス込みデバイス コンプライアンス ポリシー"としてこれら进行评估します。

コンプライアンス ポリシーが割り当てられていないデバイスをマークする ①

脱獄の高度な検出 ①

コンプライアンス状態の有効期間 (日) ① 30 ✓

推奨 : [準拠していない] および [有効] を選択

② デバイス コンプライアンス ポリシー

- [デバイス] - [コンプライアンス ポリシー] - [ポリシー] の [+ ポリシーの作成] で、プラットフォームごとのデバイス コンプライアンス ポリシーを作成できる

The screenshot shows the Microsoft Endpoint Manager admin center interface. The left sidebar has 'デバイス' (Devices) highlighted with a red box. The main content area shows the breadcrumb path 'ホーム > デバイス > デバイス | ...' and the 'コンプライアンス ポリシー | ポリシー' page. The '+ ポリシーの作成' button is highlighted with a red box. A red arrow points from this button to a 'ポリシーの作成' (Create Policy) dialog box. The dialog box shows a dropdown menu for 'プラットフォーム' (Platform) with options: 'プラットフォームを選択' (Select platform), 'Android デバイスマネージャー' (Android Device Manager), 'Android Enterprise', 'iOS/iPadOS', 'macOS', 'Windows 10 以降' (Windows 10 and later), and 'Windows 8.1 以降' (Windows 8.1 and later). A red box highlights the 'Android Enterprise' option. A text box on the right explains that for Android Enterprise, the profile type must also be specified.

Android Enterprise の場合は、
プロファイルの種類も指定する

- フル マネージド、専用、
会社所有の仕事用プロファイル
- 個人所有の仕事用プロファイル

例) Windows 10 のデバイスコンプライアンスポリシーの作成

- プラットフォームで [Windows 10 以降] を選択し、[基本] タブでポリシー名を入力する

ポリシーの作成

プラットフォーム

Windows 10 以降

プロファイルの種類

Windows 10 コンプライアンス ポリシー

作成

ホーム > デバイス > コンプライアンスポリシー >

Windows 10 コンプライアンス ポリシー ...

Windows 10 以降

① 基本 ② コンプライアンス設定 ③ コンプライアンス非対応に対するアクション ④ 割り当て ⑤ 確認および作成

名前 * Windows 10 デバイス コンプライアンス ポリシー ✓

説明

プラットフォーム Windows 10 以降

プロファイルの種類 Windows 10 コンプライアンス ポリシー

前へ 次へ

[コンプライアンス設定] タブ

ホーム > デバイス > コンプライアンスポリシー >

Windows 10 コンプライアンス ポリシー ...

Windows 10 以降

✓ 基本 **2 コンプライアンス設定** ③ コンプライアンス非対応に対する

- ▼ デバイスの正常性
- ▼ デバイスのプロパティ
- ▼ Configuration Manager のコンプライアンス
- ▼ システム セキュリティ
- ▼ Microsoft Defender for Endpoint

前へ 次へ

↑ デバイスの正常性

Windows 正常性構成証明サービスの評価規則

BitLocker が必要 ①	必要	構成されていません
デバイス上でセキュアブートの有効化が必要 ①	必要	構成されていません
コードの整合性が必要 ①	必要	構成されていません

↑ デバイスのプロパティ

オペレーティング システムのバージョン ①

最小 OS バージョン ①	構成されていません
最大 OS バージョン ①	構成されていません
モバイル デバイスの最小 OS バージョン ①	構成されていません
モバイル デバイスの最大 OS バージョン ①	構成されていません

有効なオペレーティング システムのビルド エクスポート

構成されていません	構成されていません	構成されていません
-----------	-----------	-----------

[参考] 技術資料

- 「Intune を使用してデバイスを準拠または非準拠としてマークするための Windows 10 以降の設定」
 - <https://docs.microsoft.com/ja-jp/mem/intune/protect/compliance-policy-create-windows>
- 「Intune を使用してデバイスを準拠または非準拠としてマークするための iOS および iPadOS 設定」
 - <https://docs.microsoft.com/ja-jp/mem/intune/protect/compliance-policy-create-ios>
- 「Intune を使用してデバイスを準拠または非準拠としてマークするための macOS 設定」
 - <https://docs.microsoft.com/ja-jp/mem/intune/protect/compliance-policy-create-mac-os>
- 「Intune を使用してデバイスを準拠または非準拠としてマークするための Android 設定」
 - <https://docs.microsoft.com/ja-jp/mem/intune/protect/compliance-policy-create-android>
- 「Intune を使用してデバイスを準拠または非準拠としてマークするための Android エンタープライズ設定」
 - <https://docs.microsoft.com/ja-jp/mem/intune/protect/compliance-policy-create-android-for-work>
- 「Intune を使用してデバイスを準拠または非準拠としてマークするための Windows 8.1 設定」
 - <https://docs.microsoft.com/ja-jp/mem/intune/protect/compliance-policy-create-windows-8-1>

[参考] 場所ベースの判断（ネットワーク フェンス）

- デバイスが許可されたネットワークに接続されているときにのみ、組織のリソースにアクセスできるようにするため、デバイスが許可された場所を離れたときに、組織のリソースへのアクセスをブロックできるポリシー

例) ある工場で、一部の従業員が Android デバイスを使用している。この工場では、工場外に Android デバイスを持ち出すことを禁止している。もし、ある従業員が Android デバイスを工場外に持ち出してしまったとしても、組織ネットワークへの無許可のアクセスを防止することができる。

- 「Android デバイス管理者」プロファイルでのみサポート（Android デバイス 6.0 以降）

「Intune で場所（ネットワーク フェンス）を使用する」

<https://docs.microsoft.com/ja-jp/mem/intune/protect/use-network-locations>

The screenshot displays the Microsoft Intune console interface. At the top, the breadcrumb navigation reads 'ホーム > デバイス > コンプライアンス ポリシー'. The main heading is 'コンプライアンス ポリシー | 場所 ...'. Below this, there is a search bar and a '+ 作成' button. A red box highlights the '+ 作成' button, and a red arrow points from it to a '場所の作成' (Create Location) dialog box. The dialog box is titled '場所の作成' and shows 'Microsoft Intune' as the parent. It has a dropdown menu for '場所の種類' (Location Type) set to 'ネットワーク' (Network). There are input fields for '名前 *' (Name) and 'IP バージョン' (IP Version) set to 'IPv4'. There are also input fields for 'IPv4 の範囲' (IPv4 Range), 'IPv4 ゲートウェイ' (IPv4 Gateway), and 'IPv4 DHCP サーバー' (IPv4 DHCP Server). A '保存' (Save) button is at the bottom of the dialog. In the background, the 'Android コンプライアンス ポリシー' (Android Compliance Policy) page is visible, with a red box highlighting the '場所' (Location) tab. Below the dialog, there is a table with columns '名前' (Name) and '場所の種類' (Location Type), and a row with the text '場所が選択されていません' (No location selected). At the bottom of the page, there are '前へ' (Previous) and '次へ' (Next) buttons.

[コンプライアンス非対応に対するアクション] タブ

ホーム > デバイス > コンプライアンスポリシー >

Windows 10 コンプライアンスポリシー ...

Windows 10 以降

✓ 基本 ✓ コンプライアンス設定 **3 コンプライアンス非対応に対するアクション** ④ 割り当て ⑤ 確認および作成

準拠していないデバイスでのアクションのシーケンスを指定する

アクション	スケジュール (コンプライアンス違反となつてからの日数) ①	メッセージテン...	追加の受信
デバイスに非準拠のマークを付ける	即時		

<input type="text" value=""/>	<input type="text" value="0"/>
メールをエンド ユーザーに送信する	
準拠していないデバイスを削除します	

「Intune で非準拠デバイスに対するアクションを構成する」

<https://docs.microsoft.com/ja-jp/mem/intune/protect/actions-for-noncompliance>

iOS/iPadOS、Android、Android Enterprise の場合

アクション	スケジュール (コンプライアンス違反となつてからの日数)
デバイスに非準拠のマー...	即時
<input type="text" value=""/>	<input type="text" value="0"/>
メールをエンド ユーザーに送信する	
エンド ユーザーにプッシュ通知を送信する	
準拠していないデバイスをリモートでロックします	
準拠していないデバイスを削除します	

前へ

次へ

[参考] コンプライアンス ポリシーの通知の作成

- [コンプライアンス ポリシー] - [通知] で、ユーザー への通知メッセージのテンプレートを作成できる

ホーム > デバイス > コンプライアンス ポリシー >

デバイス | ... × コンプライアンス ポリシー | 通知 ...

検索 (Ctrl+/) << 検索 (Ctrl+/) << + 通知の作成 最新の情報に更新

概要

すべてのデバイス

モニター

プラットフォーム別

Windows

iOS/iPadOS

macOS

Android

デバイスの登録

デバイスの登録

ポリシー

コンプライアンス ポリシー

条件付きアクセス

通知

ポリシー

準備していないデバイス

場所

コンプライアンス ポリシー

通知の作成 ...

1 基本 2 通知メッセージテンプレート 3 確認および作成

名前 *

電子メール ヘッダー - 会社のロゴを含める

電子メール フッター - 会社の名前を含める

電子メール フッター - 連絡先情報を含める

ポータル サイト Web サイトのリンク

前へ 次へ

通知の作成 ...

✓ 基本 2 通知メッセージテンプレート 3 確認および作成

ロケール	件名	メッセージ	既定である
日本語	コンプライアンス ...	コンプライアンス違反です。 ✓	<input checked="" type="checkbox"/>

前へ 次へ

[割り当て] タブ

- デバイス コンプライアンス ポリシーを適用したい Azure AD グループを指定

ホーム > デバイス > コンプライアンス ポリシー >

Windows 10 コンプライアンス ポリシー ...

Windows 10 以降

✓ 基本 ✓ コンプライアンス設定 ✓ コンプライアンス非対応に対するアクション **4 割り当て** 5 確認および作成

組み込まれたグループ

[グループを追加](#) [すべてのユーザーを追加](#)

グループ	
営業グループ	削除

除外されたグループ

i グループを除外する場合、"含める" と "除外する" でユーザーとデバイスのグループを同時に指定することはできません。詳細については、[ここをクリックしてください](#)。

[+ グループを追加](#)

グループ
グループが選択されませんでした

[前へ](#) [次へ](#)

ユーザー グループと デバイス グループ

- デバイス コンプライアンス ポリシーは、ユーザー グループ および デバイス グループ のいずれにも割り当て可能

グループへの割り当て	適用シナリオ
ユーザー グループへの割り当て	<ul style="list-style-type: none">• 条件付きアクセスとの連携を利用する場合に必要• グループのメンバーであるユーザーが使用する、すべてのデバイスでポリシーがチェックされる
デバイス グループへの割り当て	<ul style="list-style-type: none">• 共有 PC など、ユーザーに紐づかないデバイスの管理で使用する

「条件付きアクセスのトラブルシューティング」

<https://docs.microsoft.com/ja-jp/troubleshoot/mem/intune/troubleshoot-conditional-access>

Tips ! デバイス コンプライアンス ポリシー

- 複数のデバイス コンプライアンス ポリシーを設定した場合、最も安全なポリシーが優先される
- 構成プロファイルとデバイス コンプライアンス ポリシーの設定が競合した場合、常に、デバイス コンプライアンス ポリシーが優先される

「Intune デバイスのコンプライアンス対応ポリシーの監視」の「Intune のポリシー競合の解決方法」

<https://docs.microsoft.com/ja-jp/mem/intune/protect/compliance-policy-monitor#how-intune-resolves-policy-conflicts>



「準拠している/準拠していない」の確認

- [デバイス] - [概要] - [対応状況] タブ

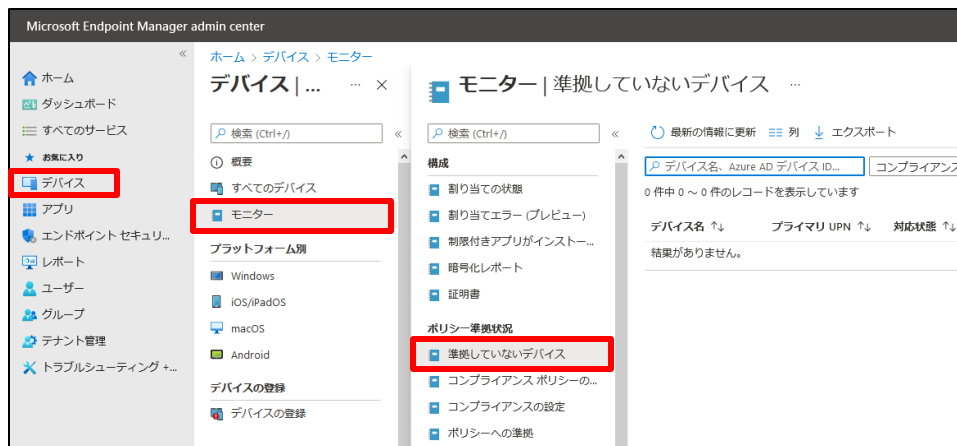


＜ダッシュボードで監視できる項目＞

- 全体的なデバイスのコンプライアンス
- ポリシーごとのデバイスのコンプライアンス対応
- 設定ごとのデバイスのコンプライアンス対応
- 脅威エージェントの状態
- デバイスの保護の状態

※ デバイスのコンプライアンス評価は、
デバイスのチェックイン スケジュールに従って行われる

- [デバイス] - [モニター] - [準拠していないデバイス]



それぞれのモニター画面で、
CSV ファイルへのエクスポートも可能

「Intune デバイスのコンプライアンス対応ポリシーの監視」
<https://docs.microsoft.com/ja-jp/mem/intune/protect/compliance-policy-monitor>

2-3

2章： Microsoft Intune

- Intune の概要
- Intune によるモバイル デバイス管理 (MDM)
- Intune によるモバイル アプリ管理 (MAM)
- Microsoft Defender for Endpoint との統合
- デバイスの登録
- Windows 10 の Azure AD 参加とハイブリッド Azure AD 参加



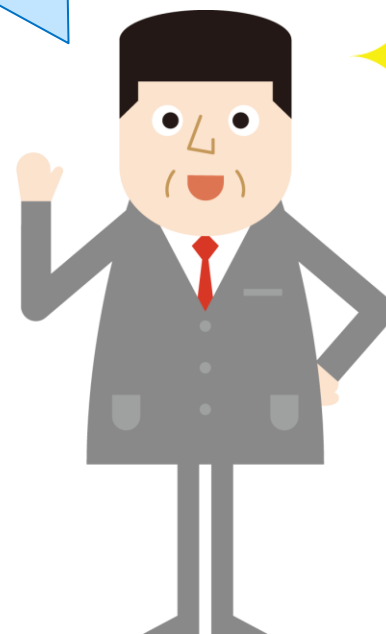
Intune のモバイル アプリ管理 (MAM)

- ユーザーへのモバイル アプリの公開、プッシュ、更新、構成、セキュリティ保護、監視など

1. アプリの展開
2. アプリの構成
3. アプリのデータ保護
4. アプリに対する条件付きアクセス

次の 2 つの構成をサポート

- Intune MDM + MAM
- デバイス登録なしの MAM



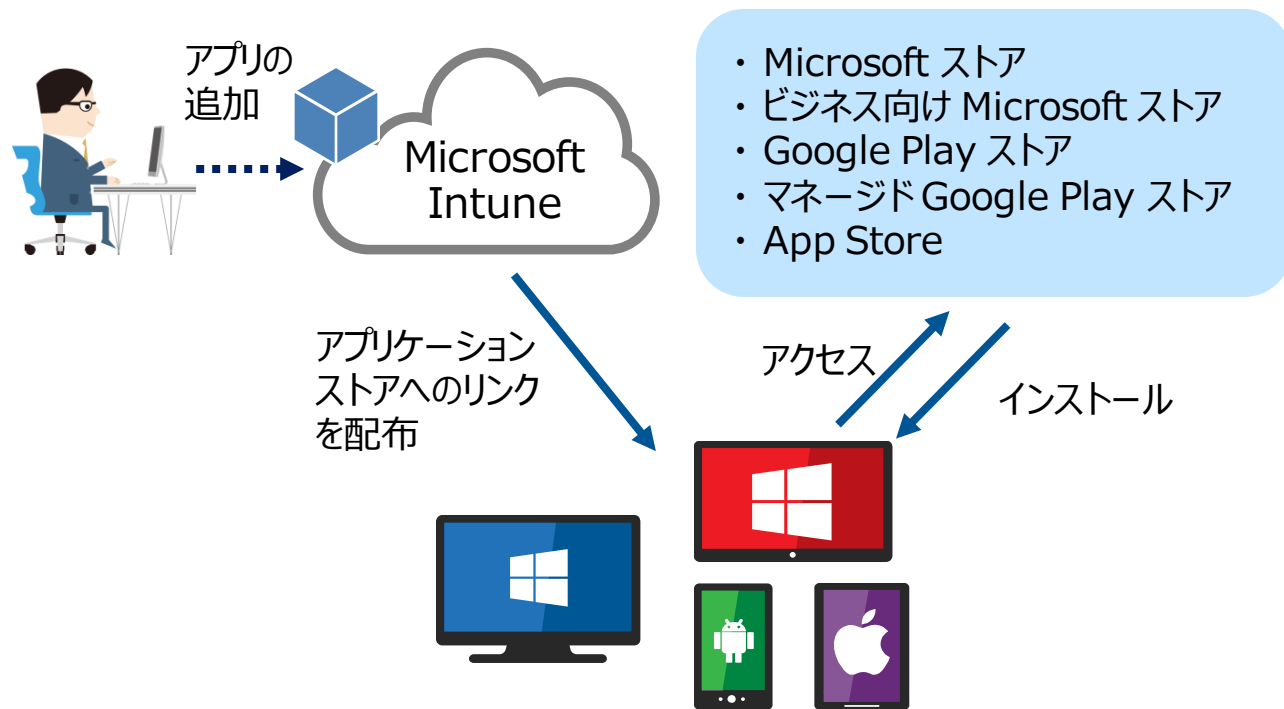
「Microsoft Intune アプリの管理とは」

<https://docs.microsoft.com/ja-jp/mem/intune/apps/app-management>

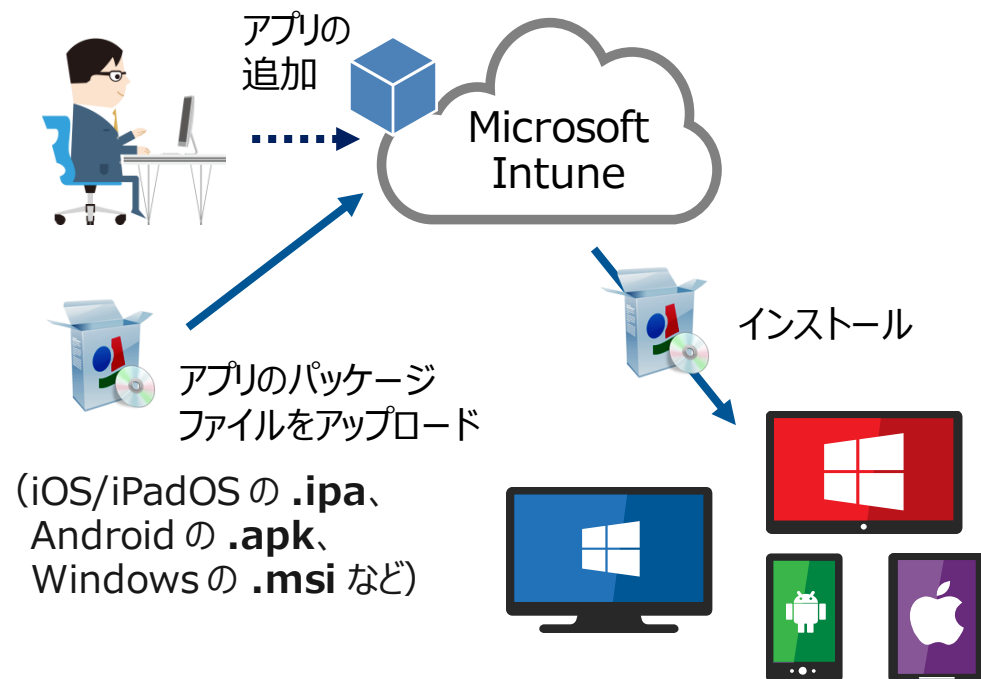
1. アプリの展開

- アプリの種類によって、展開方法が異なる

例) ストア アプリの展開



例) 基幹業務アプリの展開



さまざまな種類のアプリ

- 組織で使用しているモバイル デバイスに、さまざまな種類のアプリを展開できる
 - 24 時間以内に必要なアプリを自動的にインストール、更新、または削除

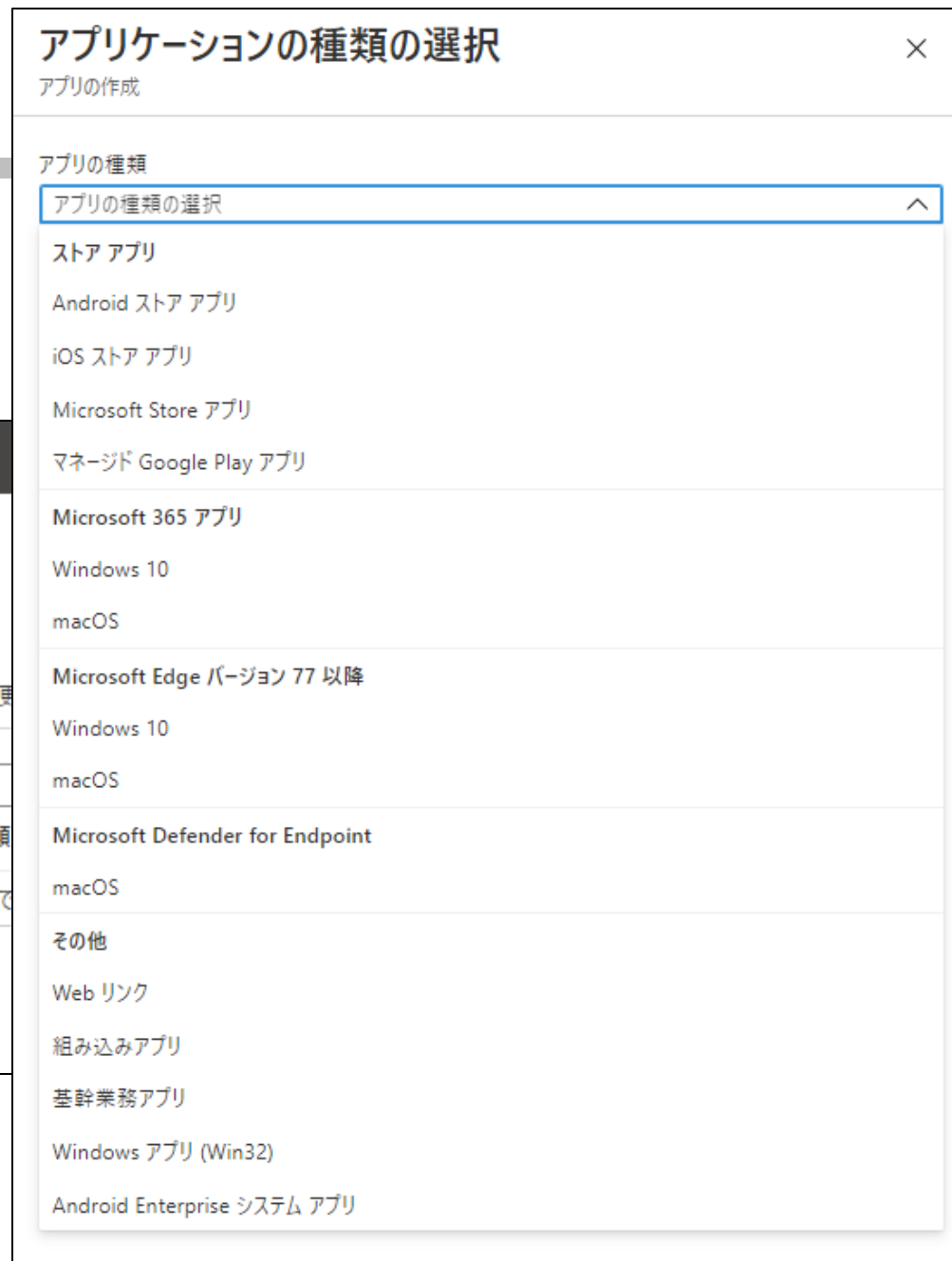
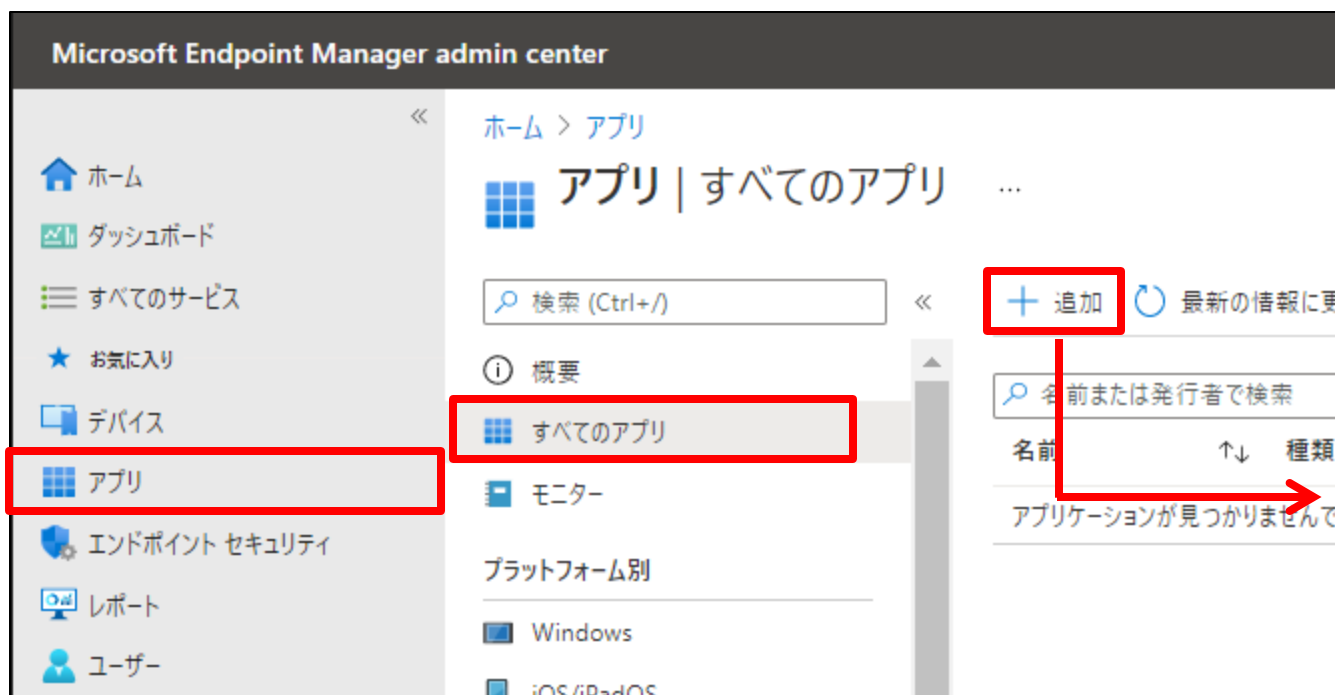
アプリの種類	インストール	アプリの更新
ストア アプリ	• Intune によって、アプリがデバイスにインストールされる	自動
社内で作成されたアプリ (基幹業務アプリ)	• 管理者がインストール ファイルを準備する • Intune によって、アプリがデバイスにインストールされる	ユーザーが手動で更新
組み込まれているアプリ (組み込みアプリ)	• Intune によって、アプリがデバイスにインストールされる	自動
Web アプリ (Web リンク)	• Intune によって、デバイスのホーム画面に Web アプリのショートカットが作成される	自動
Microsoft サービスからのアプリ	• Intune によって、ポータル サイトにショートカットが 作成 される	自動

「Microsoft Intune にアプリを追加する」

<https://docs.microsoft.com/ja-jp/intune/apps-add>

アプリの追加

- [アプリ] – [すべてのアプリ] の [+ 追加] で、アプリケーションの種類を選択



例 1) iOS ストア アプリ「Microsoft Outlook」の追加

- アプリの種類で [iOS ストア アプリ] を選択
- [アプリ情報] タブから「アプリストア」にアクセスし、展開するアプリを選択

The screenshot illustrates the process of adding an iOS app to a mobile application. It is divided into three main sections:

- Left Panel (Application Type Selection):** Titled "アプリケーションの種類を選択" (Select Application Type). Under "アプリの種類" (Application Type), "iOS ストア アプリ" (iOS Store App) is selected and highlighted with a red box. A red arrow points from this box to the "アプリ情報" (App Info) tab in the middle panel.
- Middle Panel (App Addition):** Titled "アプリの追加" (Add App). It shows the "アプリ情報" (App Info) tab selected, also highlighted with a red box. Below it, the "アプリの選択" (Select App) step is active. A red box highlights the "アプリストアを検索します" (Search App Store) button. A callout bubble points to this button with the text "アプリストアにアクセス" (Access App Store).
- Right Panel (App Search Results):** Titled "アプリストアを検索します" (Search App Store). The search term "outlook" is entered. The results list includes "Microsoft Outlook" by "Microsoft Corporation", which is highlighted with a red box. Other apps like "Microsoft OneDrive", "myMail", "Yahoo!メール", "Gmail", "Mail.ru", and "メール" (Apple) are also listed.

[アプリ情報] タブ

- デバイス構成プロファイルの名前を入力



アプリの追加 ...

iOS store app

✓ **アプリ情報** ② 割り当て ③ 確認および作成

アプリの選択 * ① [アプリストアを検索します](#)

名前 * ①

説明 * ①

発行元 * ①

アプリストアの URL

最低限のオペレーティング システム * ①

適用可能なデバイスの種類 * ①

カテゴリ ①

ポータルサイトでおすすめアプリとして表示する ①

情報 URL ①

プライバシー URL ①

開発者 ①

所有者 ①

メモ ①

ロゴ ① [画像の変更](#)

前へ 次へ

アプリストアの
Outlook
アプリの URL

[割り当て] タブ

- 競合が起こらないように、アプリを展開したいグループを指定

このアプリを必須にする
グループを選択

このアプリを使用できるようにする
グループを選択

デバイス登録の有無に関わらず、
このアプリを使用できるようにする
グループを選択

アプリをアンインストールする
グループを選択

アプリの追加 ...
iOS store app

✓ アプリ情報 2 割り当て 3 確認および作成

Required ①

グループ モード	グループ	VPN
含まれる	営業グループ	なし

+ グループの追加 ① + すべてのユーザーを追加する ① + すべてのデバイスを追加 ①

登録済みデバイスで使用可能 ①

グループ モード	グループ	VPN	デバイスの削除時にアンインストールする
割り当てがありません			

+ グループの追加 ① + すべてのユーザーを追加する ①

Available with or without enrollment ①

グループ モード	グループ	デバイスの削除時にアンインストールする
割り当てがありません		

+ グループの追加 ① + すべてのユーザーを追加する ①

Uninstall ①

グループ モード	グループ
割り当てがありません	

+ グループの追加 ① + すべてのユーザーを追加する ① + すべてのデバイスを追加 ①

前へ 次へ

「Microsoft Intune を使用してアプリをグループに割り当てる」の「アプリのIntentの競合を解決する方法」
<https://docs.microsoft.com/ja-jp/mem/intune/apps/apps-deploy#how-conflicts-between-app-intents-are-resolved>

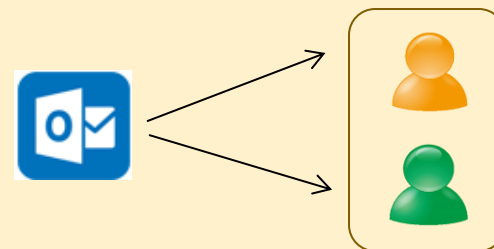
注) アプリを正常にアンインストールするには、そのユーザーへのインストールの割り当てを削除してからアンインストールする (インストールとアンインストールの両方が割り当てられると、アプリを削除できない)

アプリのグループへの割り当て

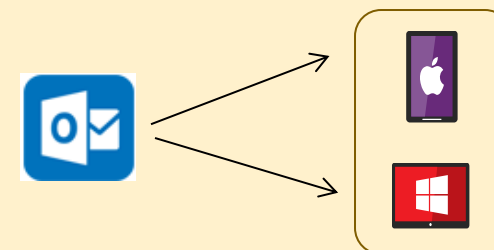
- Intune にデバイスを登録しているか否かで、割り当てに違いがある

オプション	MDM + MAM	デバイス登録なしの MAM
ユーザーへの割り当て	○	○
デバイスへの割り当て	○	×
ラップされたアプリ、または Intune SDK が組み込まれた アプリの割り当て (アプリ保護ポリシー用)	○	○
"使用可能" として割り当て	○	○
"必須" として割り当て	○	×
アプリのアンインストール	○	×
Intune からのアプリの更新プログラムの受信	○	×
エンドユーザーによる Intune ポータル サイト アプリ からの使用可能なアプリのインストール	○	×
エンドユーザーによる Web ベースの Intune ポータル サイトからの使用可能なアプリのインストール	○	○

ユーザー グループへの割り当て



デバイス グループへの割り当て



[参考] 自動的に再インストール、更新、削除

- ユーザーのデバイスにインストールされる必要があるアプリを、ユーザーがアンインストールした場合、24 時間以内に Intune によってアプリが自動的に再インストールされる
- 必要なアプリのインストールに失敗した場合、または何らかの理由でアプリがデバイス上に存在しない場合、24 時間以内に Intune でコンプライアンスが評価され、アプリが再インストールされる
- Intune によってインストールされるように構成したアプリを、管理者が v1 から v2 に更新し、アプリの前のバージョンがユーザーのデバイスに存在している場合、24 時間以内に Intune によってアプリが更新される
- 管理者がアンインストールの命令を展開したが、アプリをデバイスからアンインストールできなかった場合、24 時間以内に Intune でコンプライアンスが評価され、アプリをアンインストールする

[参考] 技術資料

- **「Android ストア アプリを Microsoft Intune に追加する」**
 - <https://docs.microsoft.com/ja-jp/intune/store-apps-android>
- **「iOS ストア アプリを Microsoft Intune に追加する」**
 - <https://docs.microsoft.com/ja-jp/intune/store-apps-ios>
- **「Microsoft Store アプリを Microsoft Intune に追加する」**
 - <https://docs.microsoft.com/ja-jp/intune/store-apps-windows>
- **「Windows の基幹業務アプリを Microsoft Intune に追加する」**
 - <https://docs.microsoft.com/ja-jp/intune/lob-apps-windows>
- **「Microsoft Intune での Win32 アプリの管理」**
 - <https://docs.microsoft.com/ja-jp/intune/apps-win32-app-management>

例 2) Windows 10 「Microsoft 365」アプリの追加

- Windows 10 と macOS デバイスは、「Microsoft 365 アプリ」を選択できる

The image shows a three-step process for adding a Microsoft 365 app to Windows 10. The first step, 'アプリケーションの種類を選択' (Select application type), shows a list of options with 'Microsoft 365 アプリ' highlighted in red. The second step, also titled 'アプリケーションの種類を選択', shows the selected app type and a '選択' (Select) button highlighted in red. The third step, 'Microsoft 365 アプリの追加' (Add Microsoft 365 app), shows the configuration screen with the '1 アプリスイートの情報' (1 App suite information) step highlighted in red. The configuration fields include: 'スイート名' (Suite name) set to 'Windows 10 用の Microsoft 365 アプリ', 'スイートの説明' (Suite description) set to 'Windows 10 用の Microsoft 365 アプリ', '発行元' (Publisher) set to 'Microsoft', 'カテゴリ' (Category) set to '生産性' (Productivity), 'ポータルサイトでおすすりアプリとして表示する' (Display as recommended app on portal site) set to 'いいえ' (No), and '情報 URL' (Info URL) set to 'https://products.office.com/ja-jp/explore-office-for-home'. A grey box at the bottom right contains the text: 「Microsoft Intune を使用して Windows 10 デバイスに Microsoft 365 アプリを追加する」 (Add Microsoft 365 app to Windows 10 devices using Microsoft Intune) and the URL 'https://docs.microsoft.com/ja-jp/mem/intune/apps/apps-add-office365'.

(続き)

ホーム > アプリ > Microsoft 365 アプリの追加 ...
Microsoft 365 アプリ (Windows 10)

✓ アプリスイートの情報 ✓ **アプリスイートの構成** ③ 割り当て ④ 確認

構成設定の形式 * 構成デザイナー

アプリスイートの構成

Office アプリを選択する ① 8 項目が選択されました

他の Office アプリを選択する (ライセンスが必要) ① 0 項目が選択されました

アプリスイートの情報

これらの設定は、スイート内で選択したすべてのアプリに適用されます。詳細情報

アーキテクチャ ① 32 ビット **64 ビット**

更新チャンネル * ① 月次エンタープライズチャンネル

その他のバージョンの削除 ① はい いいえ

インストールするバージョン ① **最新** 特定

特定バージョン 最新バージョン

前へ 次へ

32 ビット **64 ビット**

✓ Access

✓ Excel

OneDrive (Groove)

✓ OneNote

✓ Outlook

✓ PowerPoint

✓ Publisher

Skype for Business

✓ Teams

✓ Word

ホーム > アプリ > Microsoft 365 アプリの追加 ...
Microsoft 365 アプリ (Windows 10)

✓ アプリスイートの情報 ✓ アプリスイートの構成 **③ 割り当て** ④ 確認および作成

Required ①

グループモード グループ

⊕ 含まれる 富業グループ

+ グループの追加 ① + すべてのユーザーを追加する ① + すべてのデバイスを追加 ①

登録済みデバイスで使用可能 ①

グループモード グループ

割り当てがありません

+ グループの追加 ① + すべてのユーザーを追加する ①

Uninstall ①

グループモード グループ

割り当てがありません

+ グループの追加 ① + すべてのユーザーを追加する ① + すべてのデバイスを追加 ①

前へ 次へ

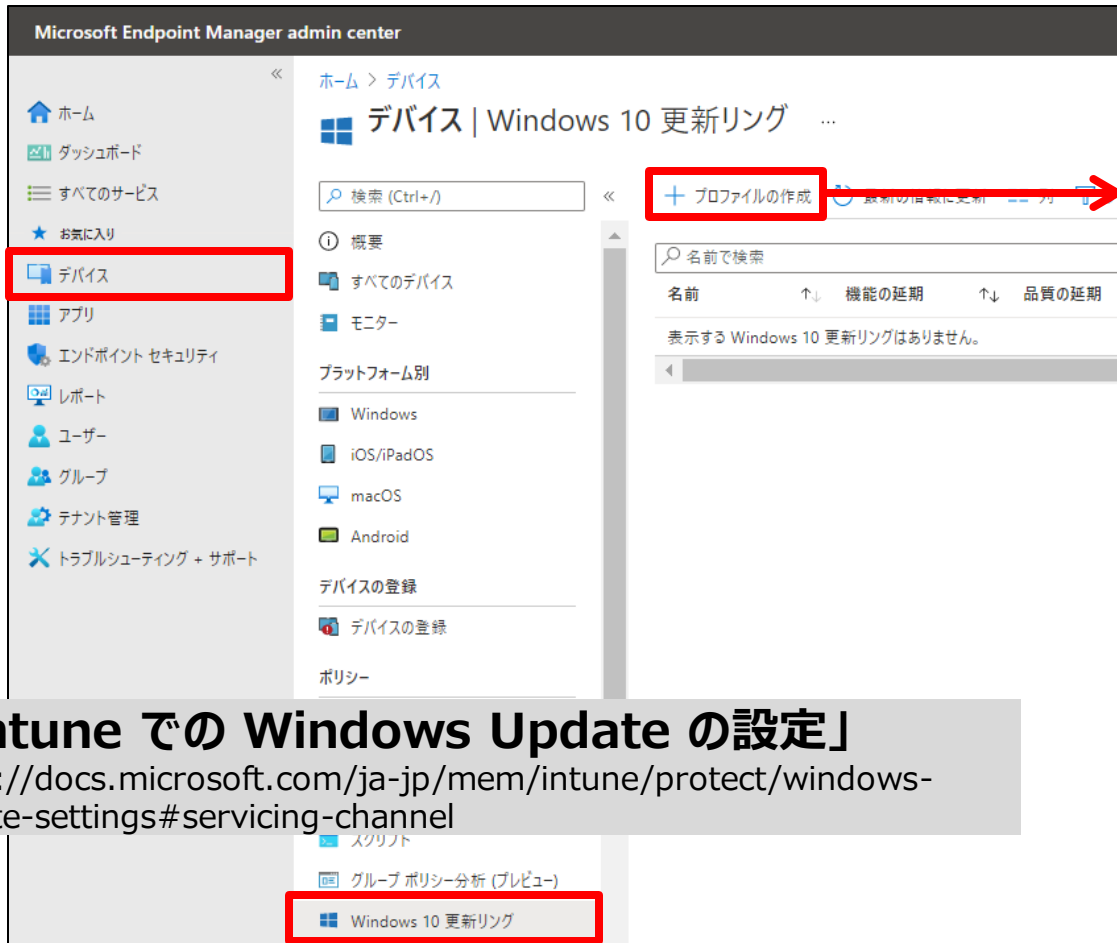
「Microsoft 365 Apps の更新チャンネルの概要」
<https://docs.microsoft.com/ja-jp/deployoffice/overview-update-channels>

Microsoft からの更新プログラムを通して、定期的に新機能を取得

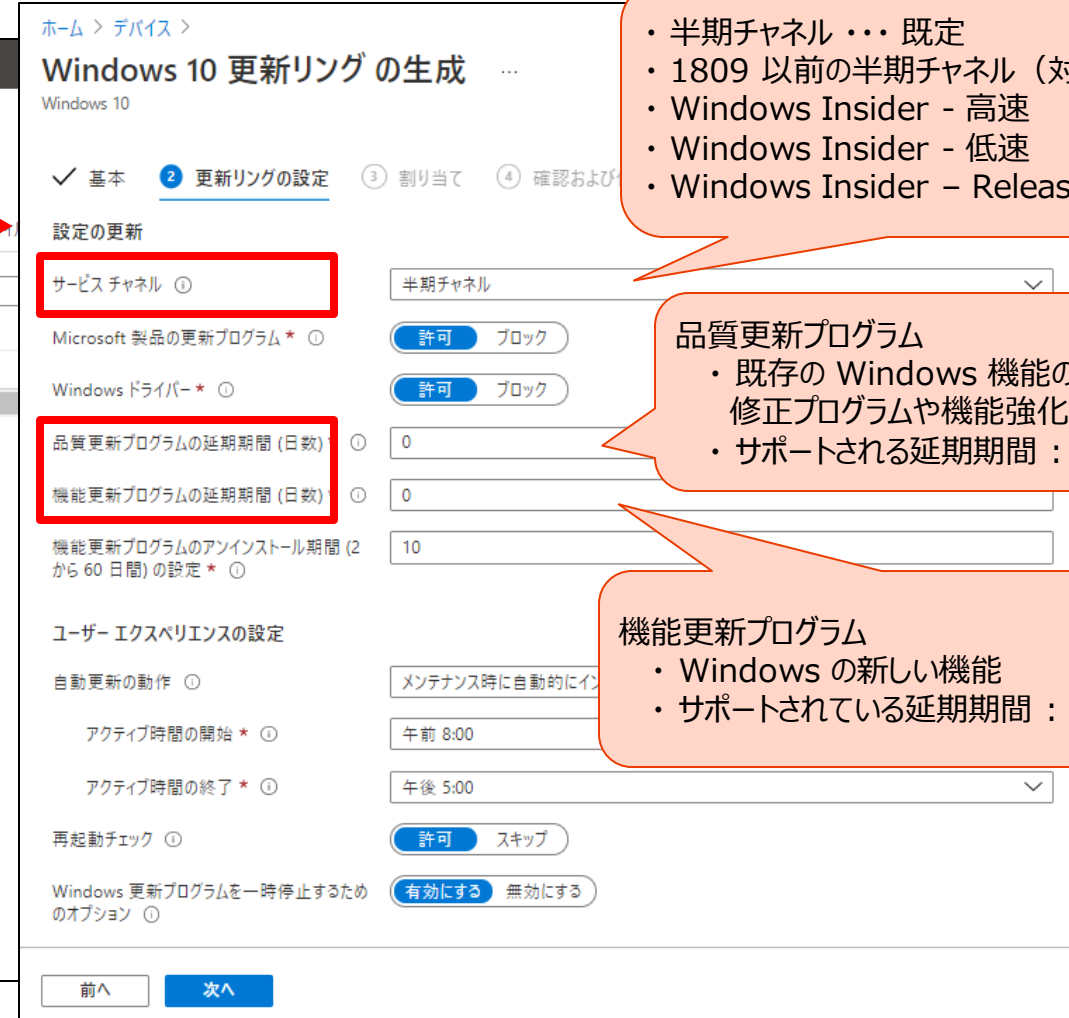
- 最新チャンネル
- 月次エンタープライズ チャンネル
- 半期エンタープライズ チャンネル

Windows 10 の更新プログラムの構成

- [デバイス] – [Windows 10 更新リング] の [+ プロファイルの作成]



「Intune での Windows Update の設定」
<https://docs.microsoft.com/ja-jp/mem/intune/protect/windows-update-settings#servicing-channel>



- 半期チャネル・・・既定
- 1809 以前の半期チャネル (対象指定)
- Windows Insider - 高速
- Windows Insider - 低速
- Windows Insider - Release Preview

品質更新プログラム

- 既存の Windows 機能の修正プログラムや機能強化
- サポートされる延期期間：最大 30 日

機能更新プログラム

- Windows の新しい機能
- サポートされている延期期間：最大 365 日

2. アプリの構成

- “アプリ構成ポリシー” を使用することで、ユーザーがアプリを実行する前に、アプリを構成できる

- アプリの実行前に構成設定を割り当てできる
- ユーザーの操作は不要
- 構成できる項目は、アプリによって異なる
 - 言語の設定、セキュリティ設定、会社のロゴなどのブランド設定 など
 - 詳細は、アプリケーション ベンダーに要確認

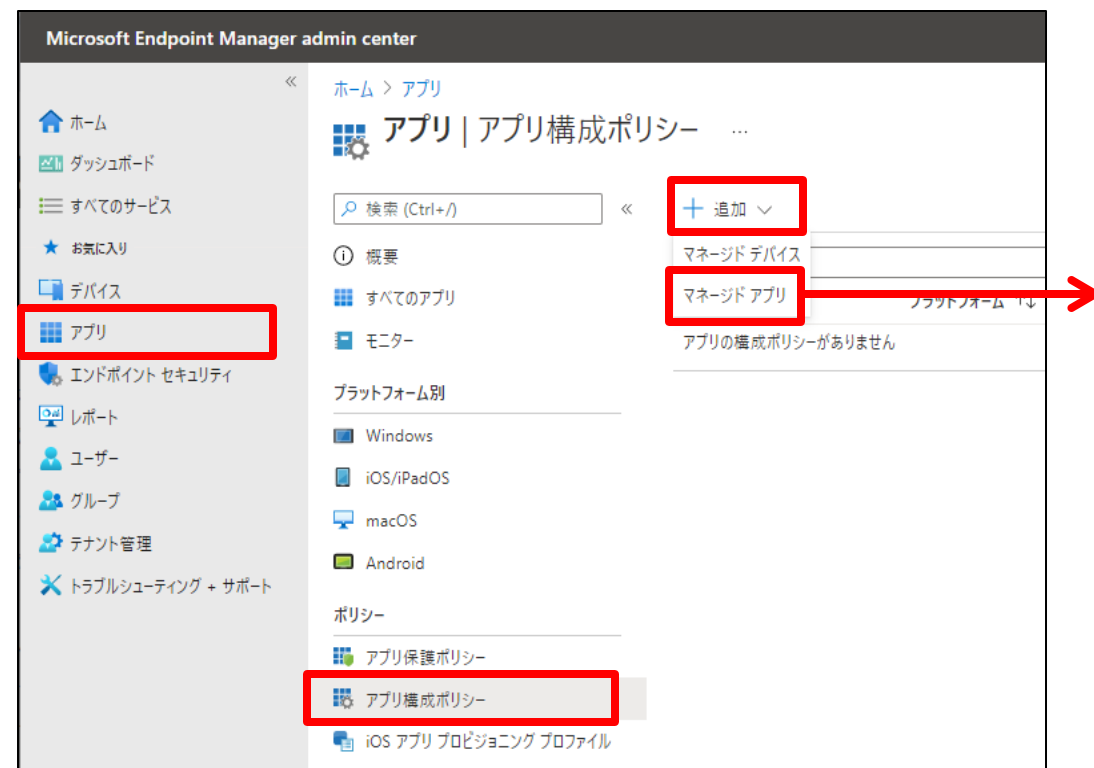
- アプリ構成ポリシーのオプション

- マネージド デバイス
 - MDM OS チャンネルを介して、アプリ構成が配信される
- マネージド アプリ
 - アプリ保護ポリシー チャンネルを介して、アプリ構成が配信される

「Microsoft Intune 用アプリ構成ポリシー」

<https://docs.microsoft.com/ja-jp/mem/intune/apps/app-configuration-policies-overview>

[アプリ] – [アプリ構成ポリシー] の [+ 追加]



例) iOS/iPadOS の「Microsoft Outlook」の構成

- [基本] タブで、構成対象となるアプリを選択

The screenshot displays the 'アプリ構成ポリシーの作成' (Create Application Configuration Policy) screen in the Microsoft Intune console. The '基本' (Basic) tab is selected and highlighted with a red box. The policy name is 'iOS/iPadOS Outlook アプリ構成'. The 'デバイス登録の種類' (Device enrollment type) is set to 'マネージド アプリ' (Managed app). Under 'パブリック アプリ' (Public app), the '+ パブリック アプリの選択' (Select public app) button is highlighted with a red box, and a red arrow points from it to the selection dialog on the right. The dialog, titled '対象のアプリを選択します' (Select target app), shows a search for 'outl' and lists 'Microsoft Outlook' for 'iOS/iPadOS' as the selected option. A '選択' (Select) button is visible at the bottom of the dialog.

ホーム > アプリ > アプリ構成ポリシーの作成 ...

① 基本 ② 設定 ③ 割り当て ④ 確認および作成

名前 * iOS/iPadOS Outlook アプリ構成 ✓

説明

デバイス登録の種類 マネージド アプリ

パブリック アプリ プラットフォーム 削除

パブリック アプリが選択されていません

+ パブリック アプリの選択

カスタム アプリ プラットフォーム 削除

カスタム アプリが選択されていません

+ カスタム アプリの選択

前へ 次へ

対象のアプリを選択します

outl ✓

Microsoft Outlook Android

Microsoft Outlook iOS/iPadOS

アプリ が選択済み:

Microsoft Outlook iOS/iPadOS 削除

選択

[設定] タブ

- 一般的な構成設定は、名前と値で定義
- 固有の構成設定が用意されているアプリもある

ホーム > アプリ >
アプリ構成ポリシーの作成 ...

✓ 基本 2 設定 ③ 割り当て ④ 確認および作成

一般的な構成設定

名前	値
<input type="text" value="名前"/>	<input type="text" value="値"/>

Outlook の構成設定

S/MIME

前へ 次へ

ホーム > アプリ >
アプリ構成ポリシーの作成 ...

✓ 基本 2 設定 ③ 割り当て ④ 確認および作成

一般的な構成設定

Outlook の構成設定

Outlook

一般的なアプリの構成

優先受信トレイ ①

アプリへのアクセスに生体認証が必要 ①

ユーザーに設定の変更を許可する ①

連絡先を保存する ①

ユーザーに設定の変更を許可する ①

外部受信者のメール ヒント ①

外部画像をブロックする ①

ユーザーに設定の変更を許可する ①

既定のアプリ署名 ①

前へ 次へ

[割り当て] タブ

- アプリ構成ポリシーを適用したい Azure AD グループを指定
- 割り当てたアプリ構成ポリシーは、
 - アプリ保護ポリシーと共に展開されている場合
⇒ 30 分間隔でチェックインされる
 - アプリ保護ポリシーと共に展開されていない場合
⇒ 720 分間隔でチェックインされる

ホーム > アプリ > アプリ構成ポリシーの作成 ...

✓ 基本 ✓ 設定 **3 割り当て** ④ 確認および作成

組み込まれたグループ

🔍 グループの追加

グループ

営業グループ 削除

除外されたグループ

i グループを除外する場合、"含める"と"除外する"でユーザーとデバイスのグループを同時に指定することはできません。詳細については、[ここをクリックしてください](#)。

+ グループの追加

グループ

グループが選択されませんでした

前へ 次へ

3. アプリのデータ保護

- “**アプリ保護ポリシー (APP)**” は、組織のデータが安全な状態にあるか、または マネージド アプリ内に格納されていることを保証するルール
 - 組織のデータに対してのみ適用され、アプリレベルで組織のデータを保護できる
 - 個人データには影響を与えることなく、組織のデータを保護できる
- **アプリ保護ポリシーを適用できるデバイス**
 - その 1 : Intune に登録されているデバイス (会社所有デバイス)
 - その 2 : サードパーティ製の MDM ツールに登録されているデバイス (会社所有デバイス)
 - その 3 : いずれの MDM ツールにも登録されていないデバイス (個人所有デバイス)

「MAM とアプリの保護に関してよく寄せられる質問」

<https://docs.microsoft.com/ja-jp/mem/intune/apps/mam-faq>

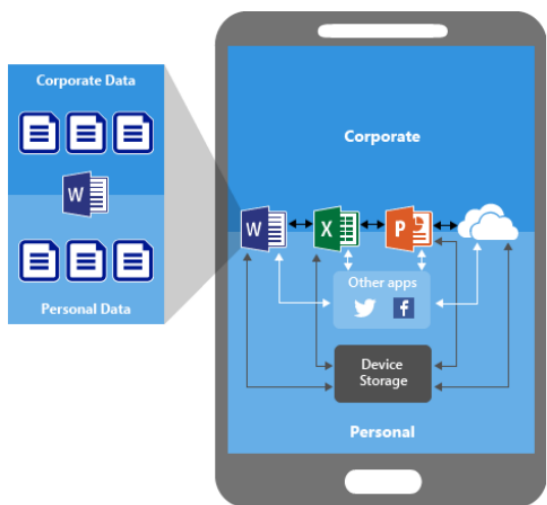


つまり、MAM ポリシーは、MDM ソリューションに依存せずに使用できる

※ MDM で管理されているデバイスに制限の軽い MAM ポリシーを割り当てて、MDM で管理されていないデバイスに制限の厳しい MAM ポリシーを割り当てることもできる

アプリ保護ポリシーのある/なし

パターン 1 : アプリ保護ポリシーのないアプリ



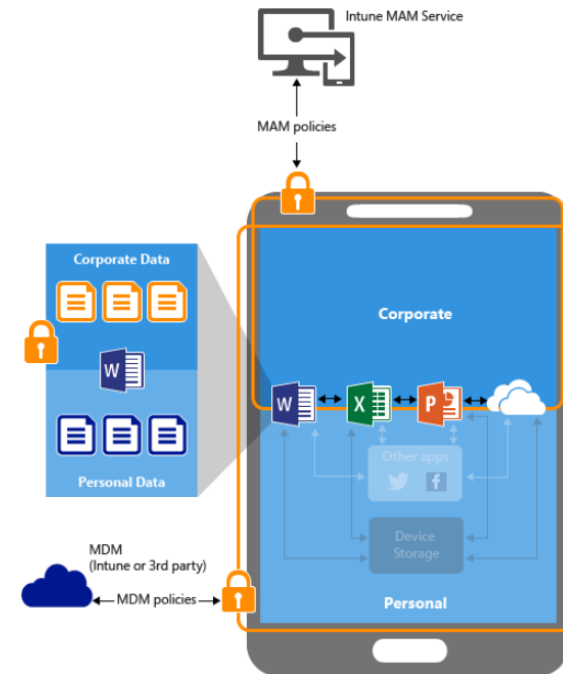
- 組織のデータと個人データが混在する
- 組織のデータが個人の記憶域に保存されたり、管理範囲外のアプリに転送されたり、データ損失を招く危険がある

パターン 2 : アプリ保護ポリシーによるデータ保護



- デバイスのローカル ストレージに組織のデータが保存されることを禁止できる
- アプリ保護ポリシーで保護されていないアプリへの、データ移動を制限できる

パターン 3 : MDM +アプリ保護ポリシーによるデータ保護



パターン 2 の構成 +

- アプリをデバイスに展開できる
- デバイスのポリシー準拠と管理を継続的に提供できる

「アプリ保護ポリシーの概要」より引用

<https://docs.microsoft.com/ja-jp/mem/intune/apps/app-protection-policy>

例) iOS/iPadOS「Microsoft Outlook」のアプリ保護

- [アプリ保護ポリシー] – [+ ポリシーの作成] で、プラットフォームを選択し、アプリ保護ポリシーを作成



「iOS アプリ保護ポリシー設定」

<https://docs.microsoft.com/ja-jp/mem/intune/apps/app-protection-policy-settings-ios>

「Microsoft Intune の Android アプリ保護ポリシー設定」

<https://docs.microsoft.com/ja-jp/mem/intune/apps/app-protection-policy-settings-android>

「アプリ保護ポリシーを作成して割り当てる方法」

<https://docs.microsoft.com/ja-jp/mem/intune/apps/app-protection-policies>

[アプリ] タブ

- アプリ保護ポリシーを適用するアプリを選択

ホーム > アプリ > ポリシーの作成 ...

✓ 基本 **2 アプリ** ③ データ保護 ④ アクセス要件 ⑤ 条件付き起動 ⑥ 割り当て ⑦ 確認および作成

このポリシーを様々なデバイスのアプリに適用する方法を選択してください。次に、少なくとも 1 つのアプリを追加してください。

デバイスのすべての種類のアプリをターゲットにする ① はい いいえ

デバイスの種類 ① 0 項目が選択されました

パブリック アプリ 削除
パブリック アプリが選択されていません

+ パブリック アプリの選択

カスタム アプリ 削除
カスタム アプリが選択されていません

+ カスタム アプリの選択

前へ 次へ

対象のアプリを選択します ×

outlook ✓

Microsoft Outlook

アプリが選択済み:
Microsoft Outlook 削除

選択

[データ保護] タブ

- 他のアプリへのデータ転送禁止や暗号化など、データ保護ルールを構成する

ホーム > アプリ > ポリシーの作成 ...

✓ 基本 ✓ アプリ **3 データ保護** ④ アクセス要件 ⑤ 条件付き起動 ⑥ 割り当て ⑦ 確認および作成

このグループには、切り取り、コピー、貼り付け、名前を付けて保存を制限するなどのデータ損失防止 (DLP) コントロールが含まれています。これらの設定によって、ユーザーがアプリ内でデータを操作する方法が決まります。

データ転送

iTunes と iCloud のバックアップに組織データをバックアップ ① 許可 ブロック

他のアプリに組織データを送信 ① ポリシー マネージド アプリ

除外するアプリを選択します 選択

組織データのコピーを保存 ① 許可 ブロック

選択したサービスにユーザーがコピーを保存することを許可 ① 0 項目が選択されました

電話通信データの転送先 ① 任意の電話アプリ

ダイヤラー アプリ URL スキーム

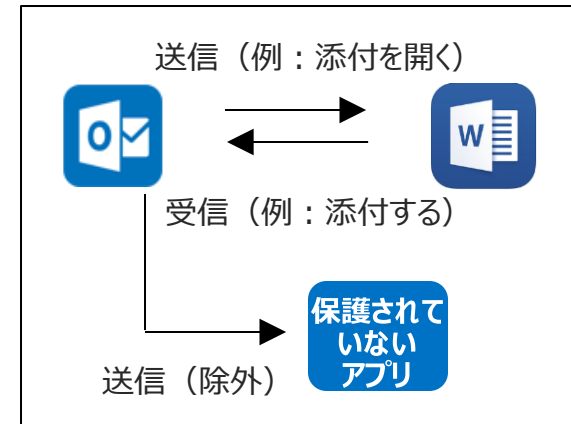
他のアプリからデータを受信 ① ポリシー マネージド アプリ

データを開いて組織ドキュメントに読み込む ① 許可 ブロック

選択したサービスからデータを開くことをユーザーに許可する ① 3 項目が選択されました

前へ 次へ

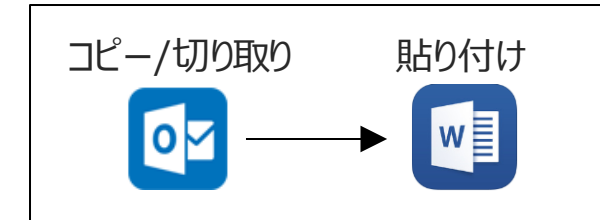
組織データの送信、受信



組織データのコピーを保存

OneDrive
 SharePoint
 ローカル

コピー、切り取り、貼り付け



Web コンテンツの共有



[アクセス要件] タブ と [条件付き起動] タブ

- [アクセス要件] タブ … アプリへのアクセスに使用する PIN や資格情報の構成
- [条件付き起動] タブ … アプリ保護ポリシーのサインイン セキュリティ要件のための設定

ホーム > アプリ >
ポリシーの作成 …

✓ 基本 ✓ アプリ ✓ データ保護 **4 アクセス要件** 5 条件付き起動 6 割り当て 7 確認および作成

ユーザーが作業コンテキスト内のアプリにアクセスするために満たす必要がある PIN と資格情報の要件を構成します。

アクセスに PIN を使用 必要 不要

PIN の種類 数値 パスコード

単純な PIN 許可 ブロック

PIN の最小長を選択

アクセスに PIN ではなく Touch ID を使用 (iOS 8 以降/iPadOS) 許可 ブロック

タイムアウト後は PIN で生体認証をオーバーライドする 必要 不要

タイムアウト (非アクティブ分数)

アクセスに PIN ではなく Face ID を使用 (iOS 11 以降/iPadOS) 許可 ブロック

PIN をリセットするまでの日数 はい いいえ

日数

デバイスの PIN が設定されている場合のアプリ PIN 必要 不要

前へ 次へ

ホーム > アプリ >
ポリシーの作成 …

✓ 基本 ✓ アプリ ✓ データ保護 ✓ アクセス要件 **5 条件付き起動** 6 割り当て 7 確認および作成

アクセス保護ポリシーのサインイン セキュリティ要件を設定します。【設定】を選択して、会社のアプリにサインインするユーザーが満たす必要がある【値】を入力します。次に、ユーザーが要件を満たしていない場合に実行する【アクション】を選択します。場合によっては、1 つの設定に複数のアクションを構成できます。条件付き起動アクションの詳細情報。

アプリの条件

設定	値	操作
PIN の最大試行回数	5	PIN のリセット …
オフラインの猶予期間	720	アクセスのブロック (分) …
オフラインの猶予期間	90	データをワイプ (日) …

デバイスの条件

アプリ保護ポリシーを使って、デバイス ベースの条件に対して次の条件付き起動設定を構成します。

登録済みデバイスについて類似のデバイス ベースの設定を構成できます。登録済みデバイスのデバイス コンプライアンス設定の構成については、こちらを参照してください。

設定	値	操作
脱獄またはルート化されたデバイス		アクセス禁止 …

前へ 次へ

[割り当て] タブ

- アプリ保護ポリシーを適用したい Azure AD グループに割り当てる

ホーム > アプリ > ポリシーの作成 ...

✓ 基本 ✓ アプリ ✓ データ保護 ✓ アクセス要件 ✓ 条件付き起動 **6 割り当て** ⑦ 確認および作成

組み込まれたグループ

🔍 グループの追加

グループ

営業グループ	削除
--------	----

除外されたグループ

i グループを除外する場合、「含める」と「除外する」でユーザーとデバイスのグループを同時に指定することはできません。詳細については、[ここ](#)をクリックしてください。

+ グループの追加

グループ

グループが選択されませんでした

前へ 次へ

「アプリ保護ポリシーを監視する方法」

<https://docs.microsoft.com/ja-jp/mem/intune/apps/app-protection-policies-monitor>

アプリ保護ポリシーが適用されたユーザー画面

- 会社データの情報漏えいを防止（アプリのアクセス要件、操作制限、暗号化、条件付き起動、リモートワイプ）



アプリの起動に
PIN/資格情報を要求



個人領域への添付ファイルの
保存を制御

会社メールの返信/転送、
送信者の変更を制御

管理外アプリへの
メール本文のコピー/
切り取り & ペーストを制御

Tips ! アプリ保護ポリシー

- アプリ保護ポリシーのプロファイル設定が同じ場合、競合が発生する
 - たとえば、コピー/貼り付けの設定以外同じ MAM ポリシーを 2 つ構成した場合、コピー/貼り付けの項目は最も厳しい値に設定され、残りの項目は構成したとおりに適用される
- 1 つのアプリに 2 つのアプリ保護ポリシーを、同時に適用した場合、両方が競合状態になり、競合する設定は、最も制限が厳しい値に設定される
- 1 つのアプリに 2 つのアプリ保護ポリシーを、異なるタイミングで適用した場合、最初のアプリ保護ポリシーが優先され、適用されたままになる
 - 2 つ目のアプリ保護ポリシーは競合を示す

「Microsoft Intune でのデバイス ポリシーとプロファイルの一般的な質問と回答」の「アプリ保護ポリシー同士が競合している場合はどうなりますか。どのポリシーがアプリに適用されますか」

<https://docs.microsoft.com/ja-jp/mem/intune/configuration/device-profile-troubleshoot#what-happens-when-app-protection-policies-conflict-with-each-other-which-one-is-applied-to-the-app>

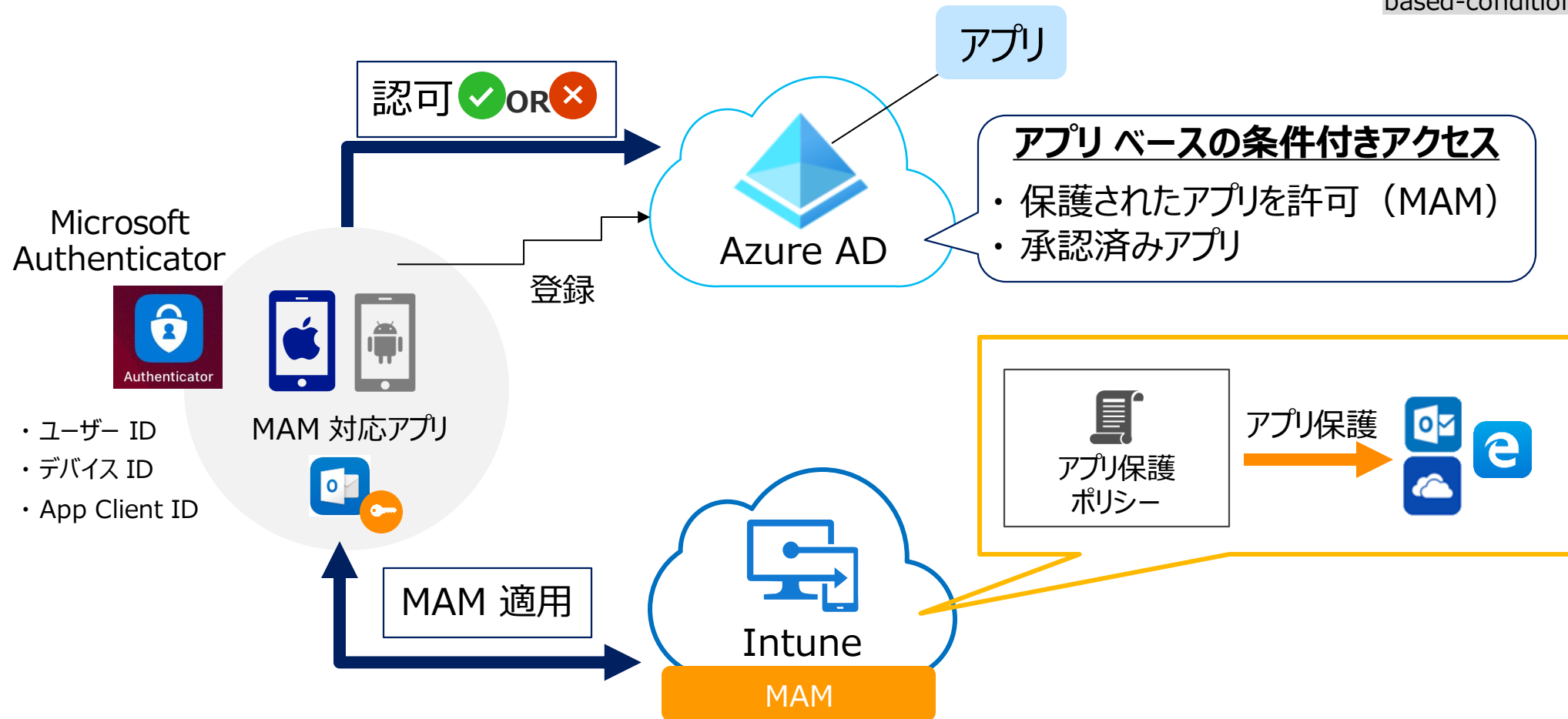


4. アプリに対する条件付きアクセス

- Intune に登録されていないデバイスでも使用できる
- アプリベースの条件付きアクセスは、iOS/iPad OS と Android のみサポート

「Intune でのアプリベースの条件付きアクセス」

<https://docs.microsoft.com/ja-jp/mem/intune/protect/app-based-conditional-access-intune>



Intune + Azure AD の条件付きアクセス

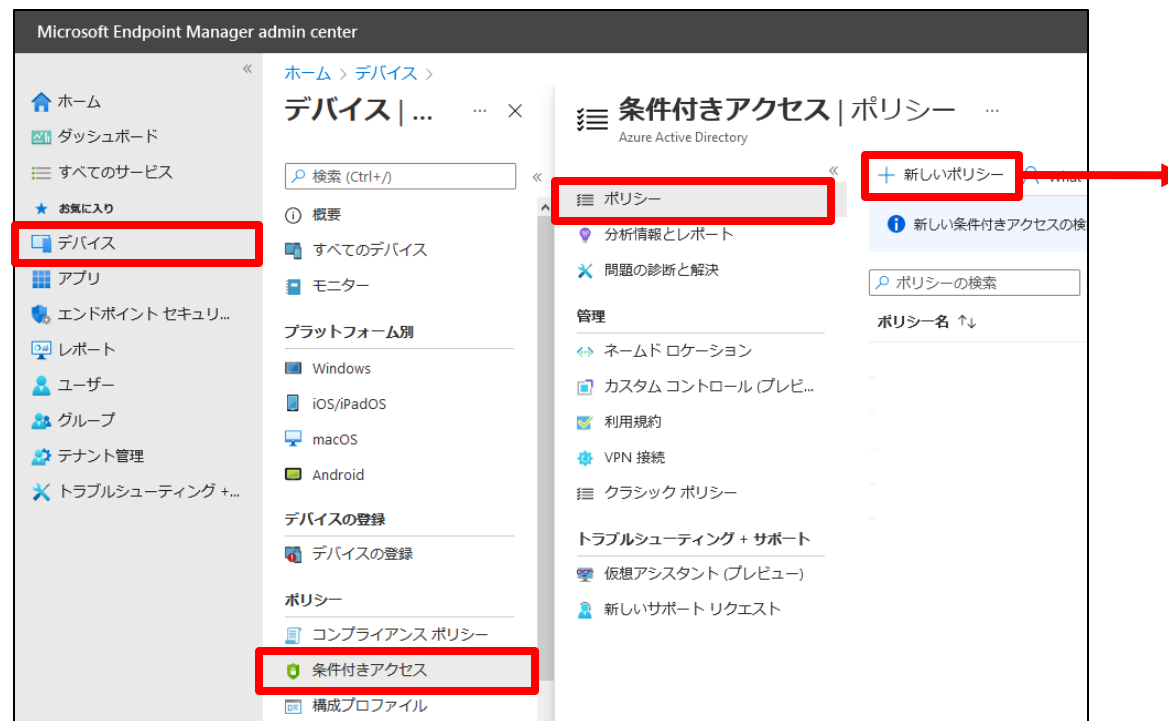
- 条件付きアクセスは、Azure AD Premium P1 の機能
- Azure AD + Intune で、2 種類の条件付きアクセスを作成できる

- ① アプリ ベースの条件付きアクセス
- ② デバイス ベースの条件付きアクセス (後述)

[デバイス] - [条件付きアクセス]
- [ポリシー] の
[+ 新しいポリシー] で作成

「条件付きアクセスと Intune について説明します」

<https://docs.microsoft.com/ja-jp/mem/intune/protect/conditional-access>



Azure AD Premium P1
Intune

新規 ...

条件付きアクセス ポリシー

シグナルを統合し、意思決定を行い、組織のポリシーを適用するために、条件付きアクセス ポリシーに基づいてユーザー アクセスを制御します。 [詳細情報](#)

名前 *

例: 'デバイス準拠アプリ ポリシー'

割り当て

ユーザーとグループ ①

0 個のユーザーとグループが選択されました

クラウド アプリまたは操作 ①

クラウド アプリまたは操作が選択されていません

条件 ①

0 個の条件が選択されました

アクセス制御

許可 ①

0 個のコントロールが選択されました

セッション ①

0 個のコントロールが選択されました

ポリシーの有効化

レポート専用 オン オフ

作成

例) 保護されたアプリからのアクセスを許可

Azure AD との 統合アプリケーション

クラウド アプリ ユーザー操作

対象 対象外

なし

すべてのクラウド アプリ

アプリを選択

選択

Office 365

Office 365 ⓘ ...

許可

アクセスをブロックまたは許可するため、ユーザー アクセスの適用を制御します。詳細情報

アクセスのブロック

アクセス権の付与

多要素認証を要求する ⓘ

デバイスは準拠しているとしてマーク済みである必要があります ⓘ

Hybrid Azure A が必要 ⓘ

承認されたクライアント アプリが必要です ⓘ
承認されたクライアント アプリの一覧を表示します

アプリの保護ポリシーが必要 ⓘ
ポリシーで保護されたクライアント アプリの一覧を表示します

パスワードの...

複数のコントロールの場合

選択したコントロールすべてが必要

選択したコントロールのいずれかが必要

承認されたアプリ

アプリ保護ポリシー

名前 *

Office 365 アプリ ベース ポリシー

割り当て

ユーザーとグループ ⓘ

組み込まれた特定のユーザー

クラウド アプリまたは操作 ⓘ

1 個のアプリ 件を含む

条件 ⓘ

1 個の条件が選択されました

アクセス制御

許可 ⓘ

2 個のコントロールが選択されました

セッション ⓘ

0 個のコントロールが選択されました

ポリシーの有効化

レポート専用 オン オフ

保存

対象 対象外

なし

すべてのユーザー

ユーザーとグループの選択

すべてのゲストと外部ユーザー ⓘ

ディレクトリ ロール ⓘ

ユーザーとグループ

選択

1 グループ

営業 営業グループ

Azure AD の
ユーザー/グループ

はい いいえ

対象 対象外

任意のデバイス

デバイス プラットフォームの選択

Android

iOS

Windows Phone

Windows

macOS

プラットフォーム
の選択

「承認されたクライアント アプリが必要」は、アプリ保護ポリシーと対応している

[参考] 技術資料

- **アプリ保護ポリシー + 承認済みクライアント アプリ + Azure AD 条件付きアクセス**

「方法:条件付きアクセスを使用して、クラウドアプリへのアクセスにアプリ保護ポリシーと承認済みクライアント アプリの使用を必須にする」

- <https://docs.microsoft.com/ja-jp/azure/active-directory/conditional-access/app-protection-based-conditional-access>

- **承認済みクライアント アプリ + Azure AD 条件付きアクセス**

「方法:条件付きアクセスを使用してクラウドアプリへのアクセスに承認されたクライアント アプリを要求する」

- <https://docs.microsoft.com/ja-jp/azure/active-directory/conditional-access/app-based-conditional-access>

2-4

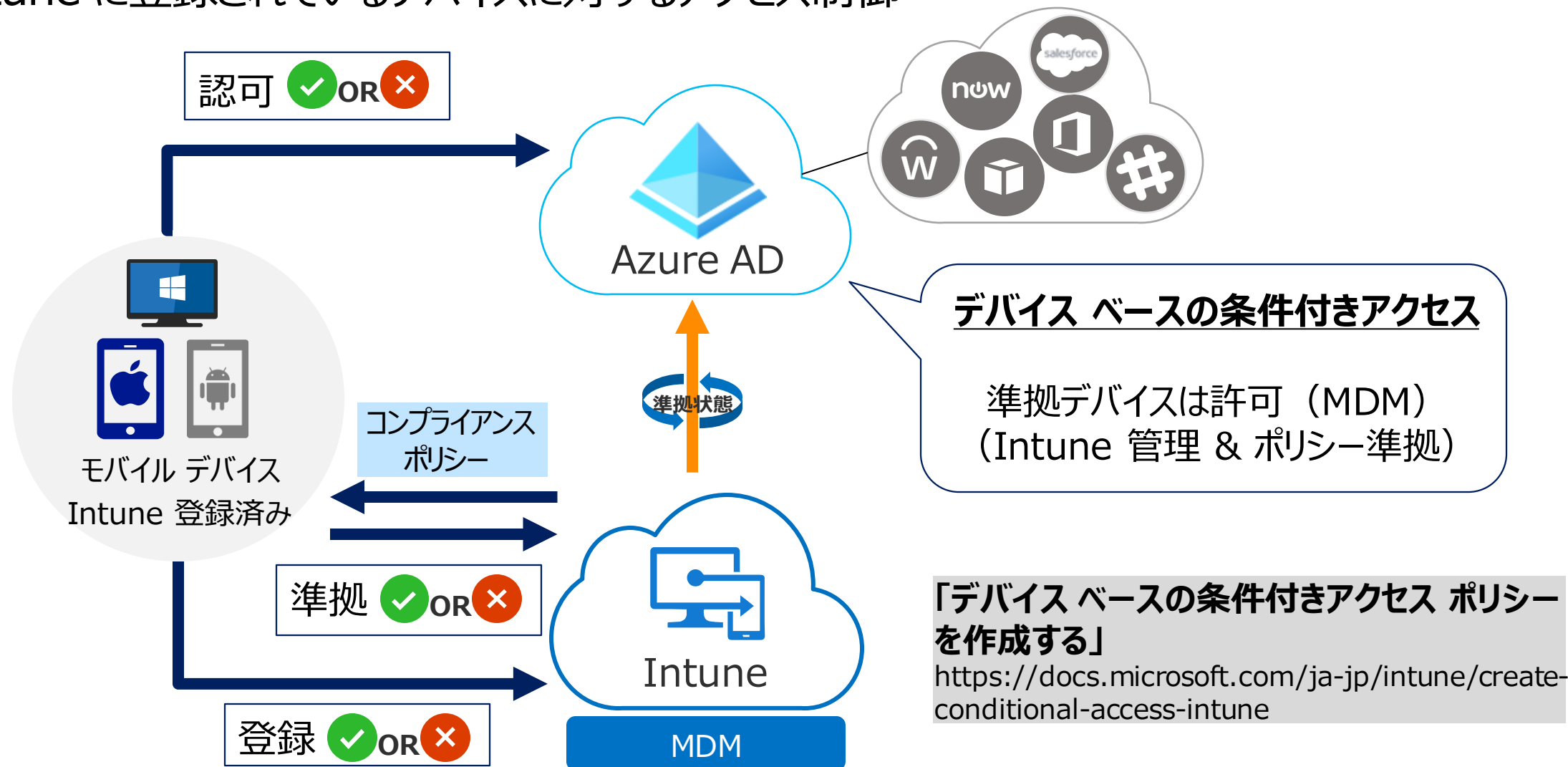
2章： Microsoft Intune

- Intune の概要
- Intune によるモバイル デバイス管理 (MDM)
- Intune によるモバイル アプリ管理 (MAM)
- Microsoft Defender for Endpoint との統合
- デバイスの登録
- Windows 10 の Azure AD 参加とハイブリッド Azure AD 参加



基本的なデバイス ベースの条件付きアクセス

- Intune に登録されているデバイスに対するアクセス制御



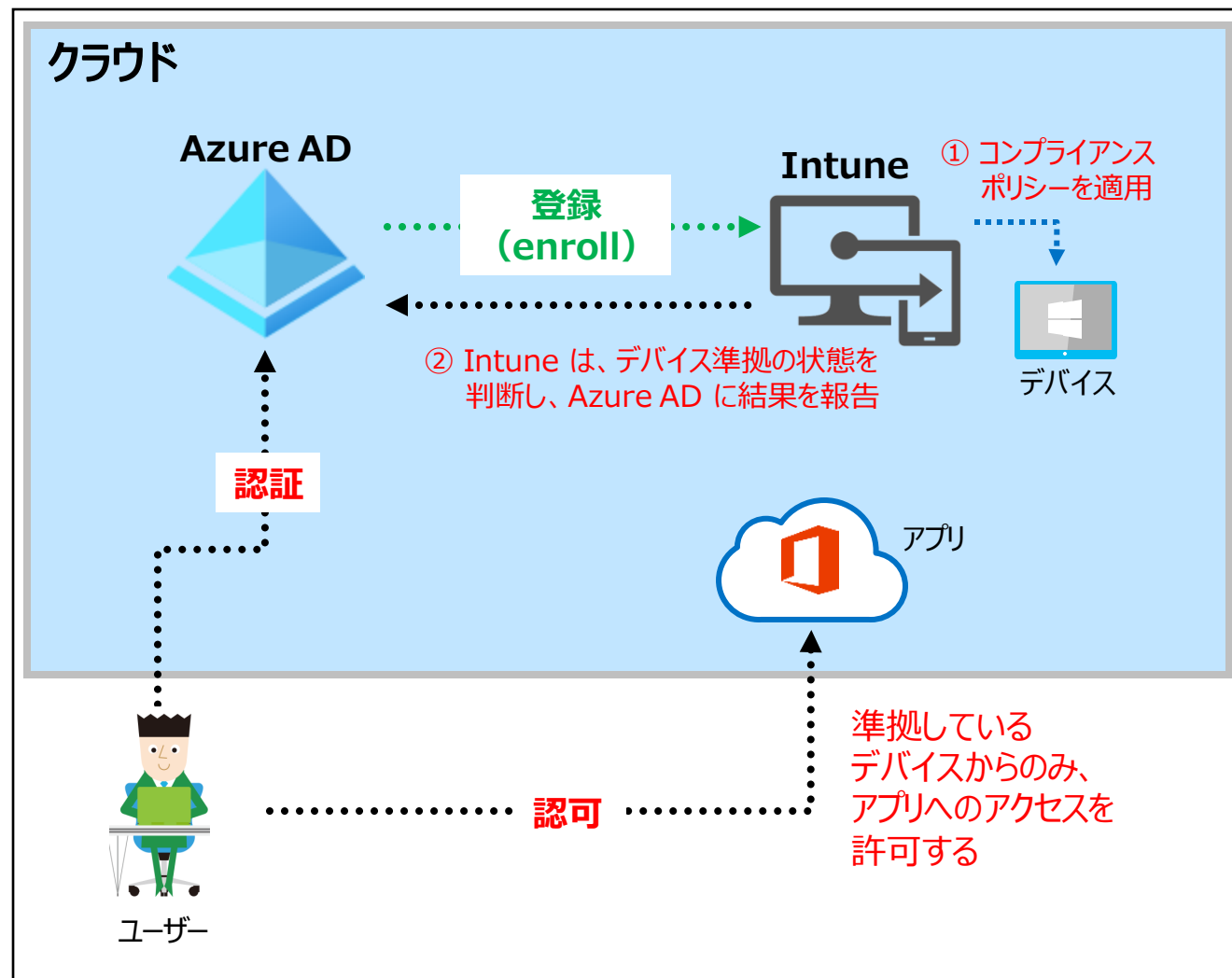
デバイス準拠の判断



Azure AD
Premium P1

Intune

1. デバイスに、Intune の **コンプライアンス ポリシー** を適用
2. Intune が、**デバイス準拠** の状態を判断し、Azure AD に結果を報告
3. アプリケーションに対して、**デバイス ベースの条件付きアクセス** を実行
 - 組織の方針に準拠しているデバイスからのみ、アプリへのアクセスを許可することができる



例) マネージド デバイスからのアクセスを許可

Azure AD との 統合アプリケーション

クラウド アプリ ユーザー操作

対象 対象外

なし

すべてのクラウド アプリ

アプリを選択

選択

Office 365

Office 365

許可

アクセスをブロックまたは許可するため、ユーザー アクセスの適用を制御します。 [詳細情報](#)

アクセスのブロック

アクセス権の付与

多要素認証を要求する

デバイスは準拠しているとしてマーク済みである必要があります

Hybrid Azure AD Join を使用したデバイスが必要

子認証またはコンソール アプリが必要です
アプリの一覧を表示します

アプリの保護ポリシーが必要
ポリシーで保護されたクライアント アプリの一覧を表示します

パスワードの変更を必須とする

複数のコントロールの場合

選択したコントロールすべてが必要

選択したコントロールのいずれかが必要

マネージド デバイス

名前 *

Office 365 デバイス ベース ポリシー

割り当て

ユーザーとグループ

組み込まれた特定のユーザー

クラウド アプリまたは操作

1 個のアプリ 件を含む

条件

0 個の条件が選択されました

アクセス制御

許可

2 個のコントロールが選択されました

セッション

0 個のコントロールが選択されました

ポリシーの有効化

レポート専用 オン オフ

対象 対象外

なし

すべてのユーザー

ユーザーとグループの選択

すべてのゲストと外部ユーザー

ディレクトリ ロール

ユーザーとグループ

選択

1 グループ

営業グループ

Azure AD の
ユーザー/グループ

[参考] 技術資料

- マネージド デバイス + Azure AD 条件付きアクセス
- 「方法:条件付きアクセスを使用してクラウドアプリへのアクセスにマネージドデバイスを要求する」
 - <https://docs.microsoft.com/ja-jp/azure/active-directory/conditional-access/require-managed-devices>

Microsoft Defender for Endpoint

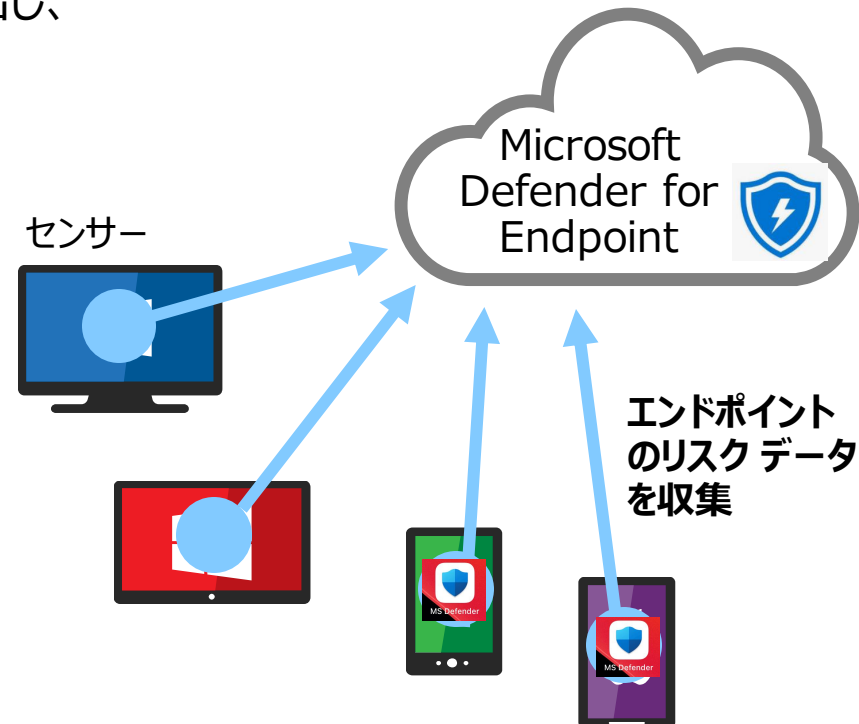
(旧称 : Microsoft Defender ATP)



- Microsoft のエンドポイント セキュリティ ソリューション

- エンドポイントをサイバー脅威から保護し、高度な攻撃とデータ侵害を検出し、セキュリティ インシデントを自動化し、セキュリティの状態を改善する

セキュリティリスクの監視、
分析、検出、自動対応



- Windows
- Windows Server
- iOS/iPadOS、macOS
- Android
- Linux

「脅威の防止」より引用

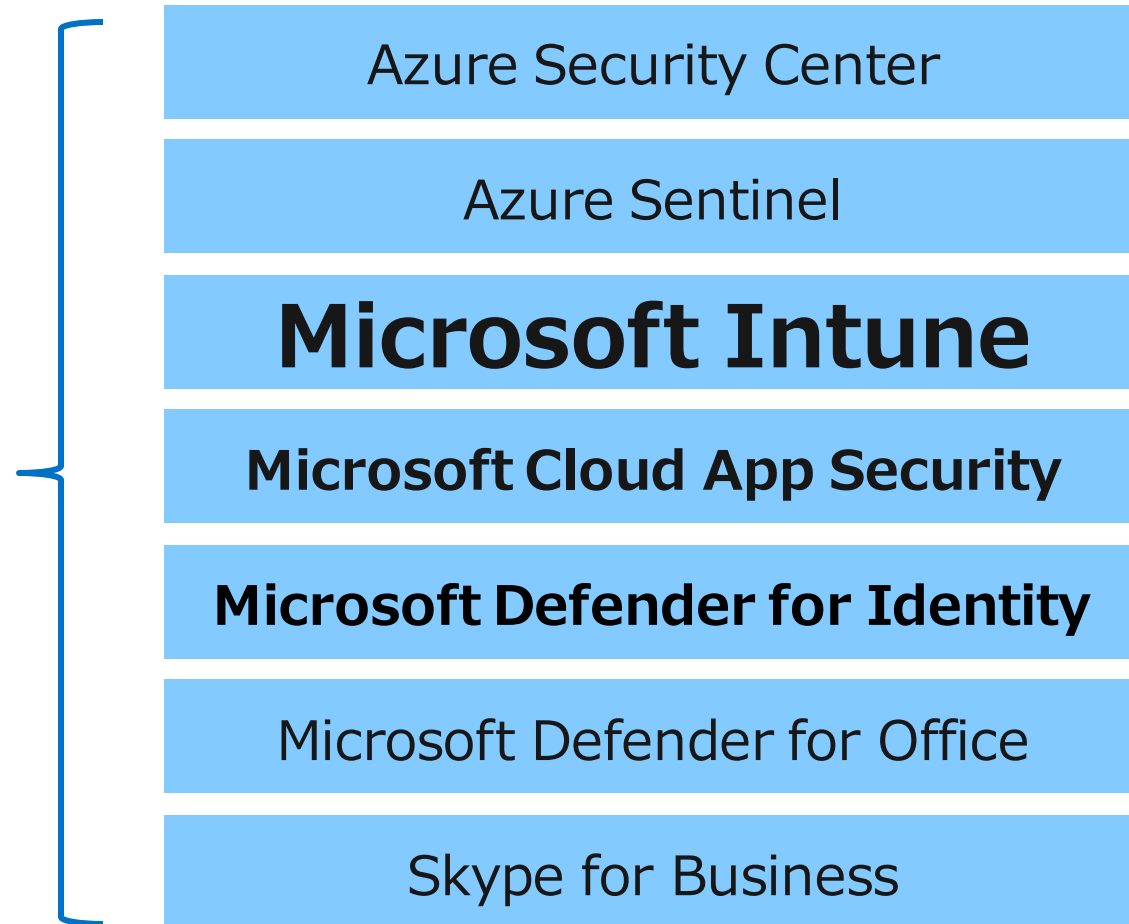
<https://docs.microsoft.com/ja-jp/windows/security/threat-protection/>

Microsoft ソリューションとの連携

- Microsoft Defender for Endpoint は、さまざまな Microsoft ソリューションとの直接統合できる



Microsoft Defender
for Endpoint



高度なデバイス ベースの条件付きアクセス

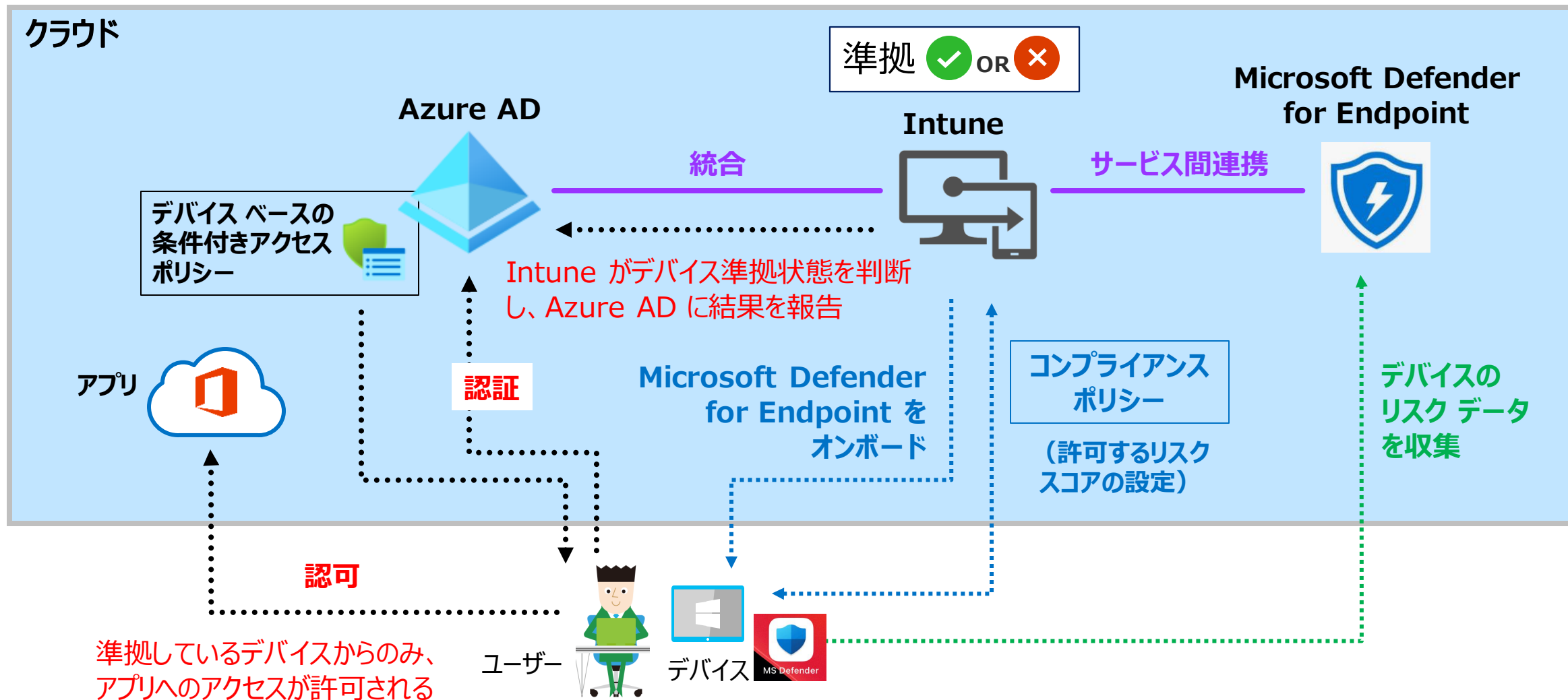


Azure AD
Premium P1

Intune

Microsoft
Defender
for Endpoint

- コンプライアンス ポリシーで設定した脅威レベルを超えたデバイスからクラウド アプリへのアクセスをブロック



Microsoft Defender for Endpoint と Intune の統合

- 構成手順

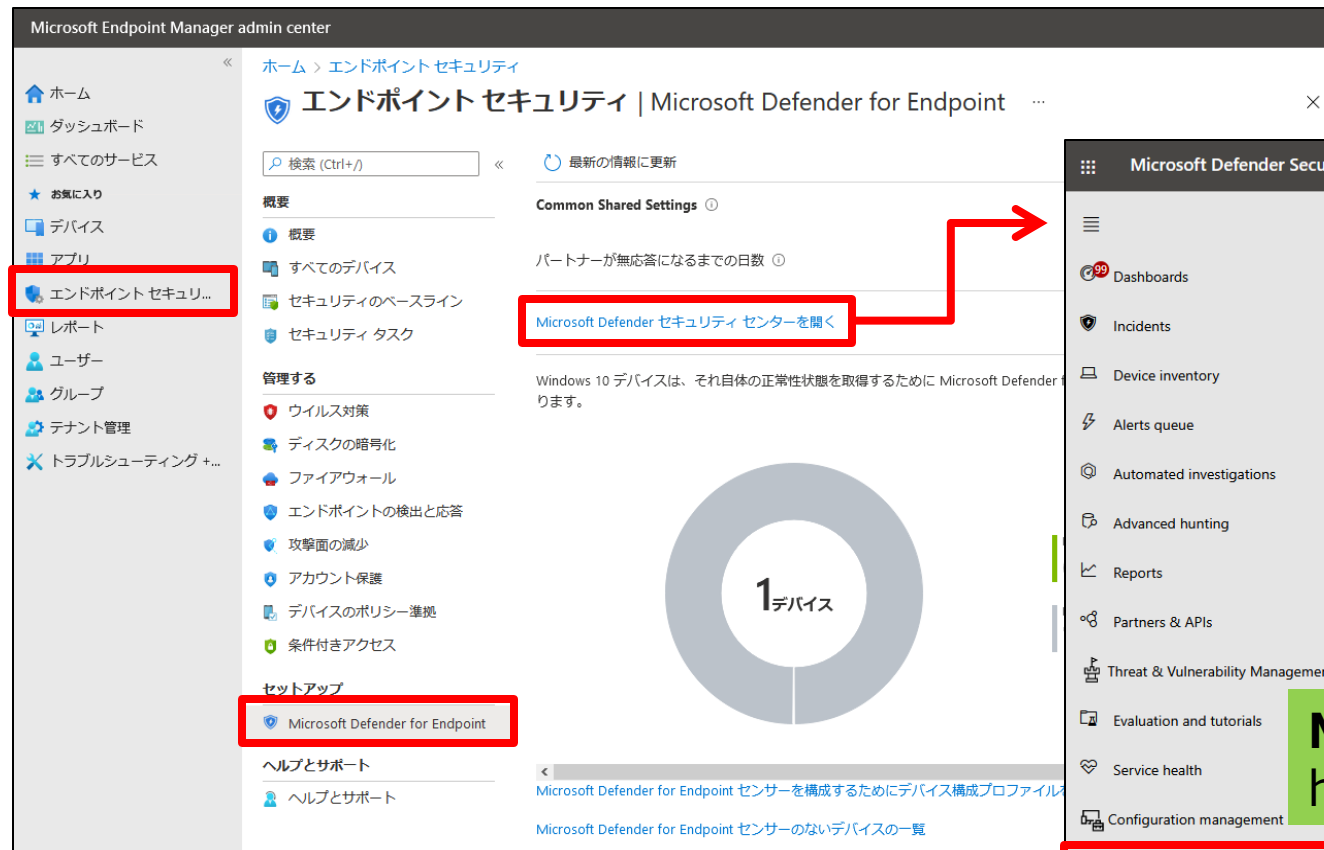
- 手順 1. テナントに対する Microsoft Defender for Endpoint の有効化
- 手順 2. デバイスのオンボード（Microsoft Defender for Endpoint の展開）
- 手順 3. デバイスのリスク スコアの設定 … Intune のコンプライアンス ポリシー
- 手順 4. 高度なデバイス ベースの条件付きアクセス ポリシーの作成
 - 想定したリスク レベルを超えるデバイスからクラウド アプリへのアクセスをブロック

「Intune で Microsoft Defender for Endpoint を構成する」

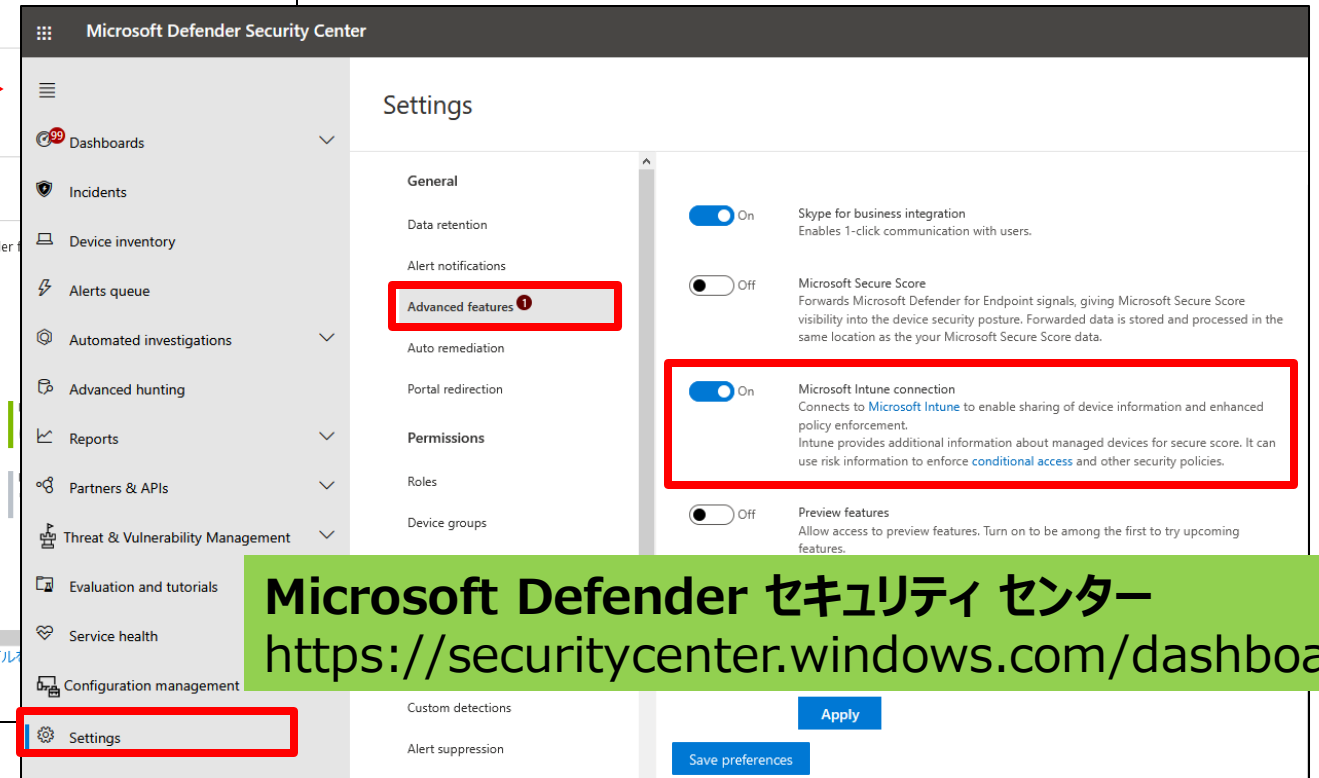
<https://docs.microsoft.com/ja-jp/mem/intune/protect/advanced-threat-protection-configure>

手順 1. テナントに対する Microsoft Defender for Endpoint の有効化

- ① Microsoft Endpoint Manager 管理センターで、
[エンドポイント セキュリティ] – [Microsoft Defender for Endpoint] から [Microsoft Defender セキュリティ センター] を開く



- ② Microsoft Defender セキュリティ センターで、
[Settings] – [Advanced Features] の
[Microsoft Intune connections] を有効化し、構成を保存



(続き)

- ③ Microsoft Endpoint Manager 管理センターで、
[エンドポイント セキュリティ] – [Microsoft Defender for Endpoint] の
Microsoft Defender for Endpoint の各項目を有効化し、構成を保存

The screenshot displays the Microsoft Endpoint Manager admin center interface. The left-hand navigation pane shows the 'エンドポイント セキュリティ' (Endpoint Security) menu item highlighted with a red box. The main content area is titled 'エンドポイント セキュリティ | Microsoft Defender for Endpoint'. Below the title, there is a search bar and action buttons for '保存' (Save), '破棄' (Delete), and '削除' (Remove). The '概要' (Overview) section shows the connection status as '空き領域' (No space) and the last sync time as '2021/3/5 10:07:17'. The 'MDM Compliance Policy Settings' section is highlighted with a red box and contains the following settings:

設定項目	状態
バージョン 6.0.0 以上の Android デバイスを Microsoft Defender for Endpoint に接続します	オン
バージョン 8.0 以上の iOS デバイスを Microsoft Defender for Endpoint に接続します	オン
バージョン 10.0.15063 以上の Windows デバイスを Microsoft Defender for Endpoint に接続します	オン
サポートされていない OS バージョンをブロックする	オン

Below this section, the 'App Protection Policy Settings' section shows two settings, both of which are also turned on:

設定項目	状態
アプリ保護ポリシーの評価のため、バージョン Microsoft Defender for Endpoint 以降の Android デバイスを (1) に接続します	オン
アプリ保護ポリシーの評価のため、バージョン Microsoft Defender for Endpoint 以降の iOS デバイスを (1) に接続します	オン

At the bottom of the page, the 'Microsoft Defender for Endpoint' menu item in the left navigation pane is also highlighted with a red box.

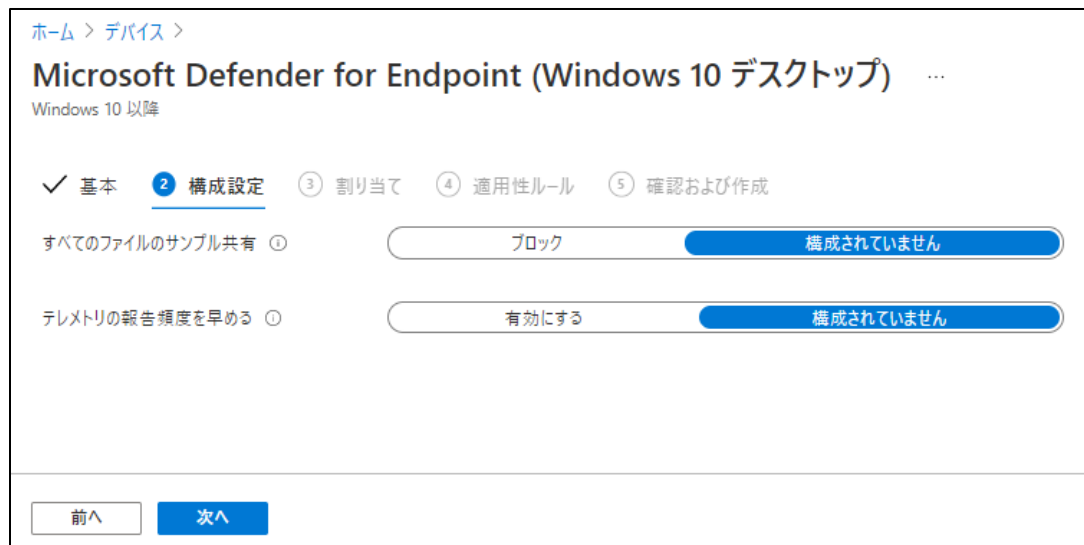
手順 2. デバイスのオンボード（展開）

- Intune で管理するデバイスに Microsoft Defender for Endpoint をオンボード（展開）
 - プラットフォームごとにオンボード（展開）手順が異なる

例) Windows デバイスは、構成プロファイルでオンボードできる



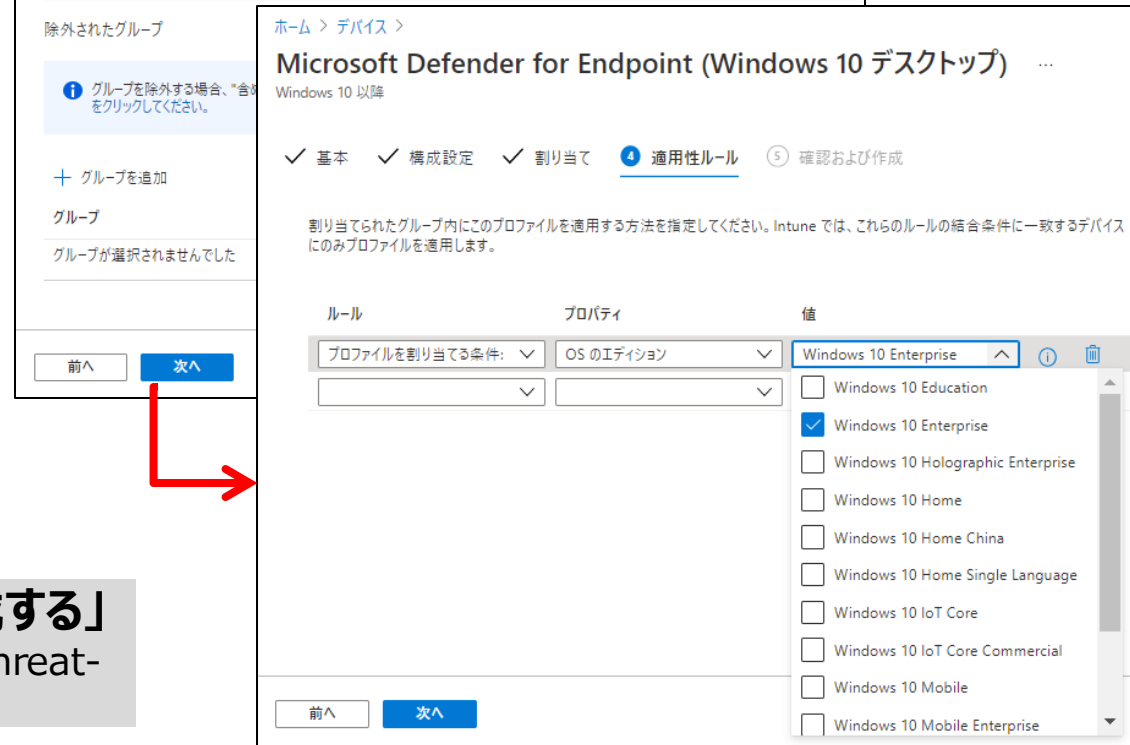
Windows 10 デバイスのオンボード



ユーザー グループに展開する場合、
ポリシーが適用されてデバイスをオンボードする前に、
ユーザーがデバイスにサインインしておく必要がある

「Intune で Microsoft Defender for Endpoint を構成する」

<https://docs.microsoft.com/ja-jp/mem/intune/protect/advanced-threat-protection-configure>

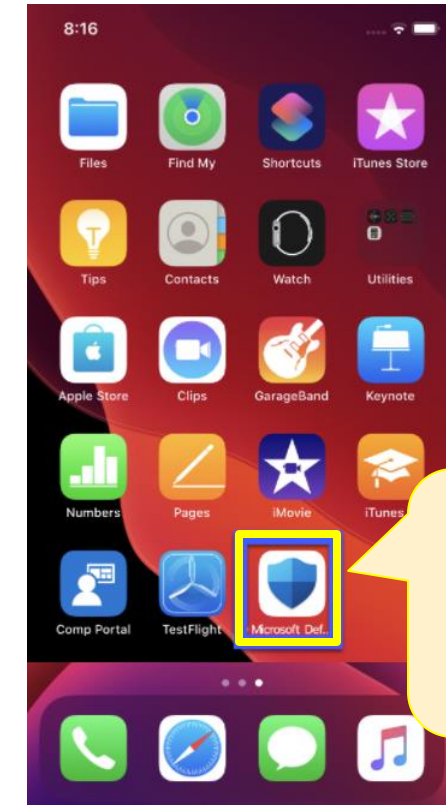


iOS/iPadOS デバイスと Android デバイスのオンボード

• iOS/iPadOS デバイス



• Android デバイス

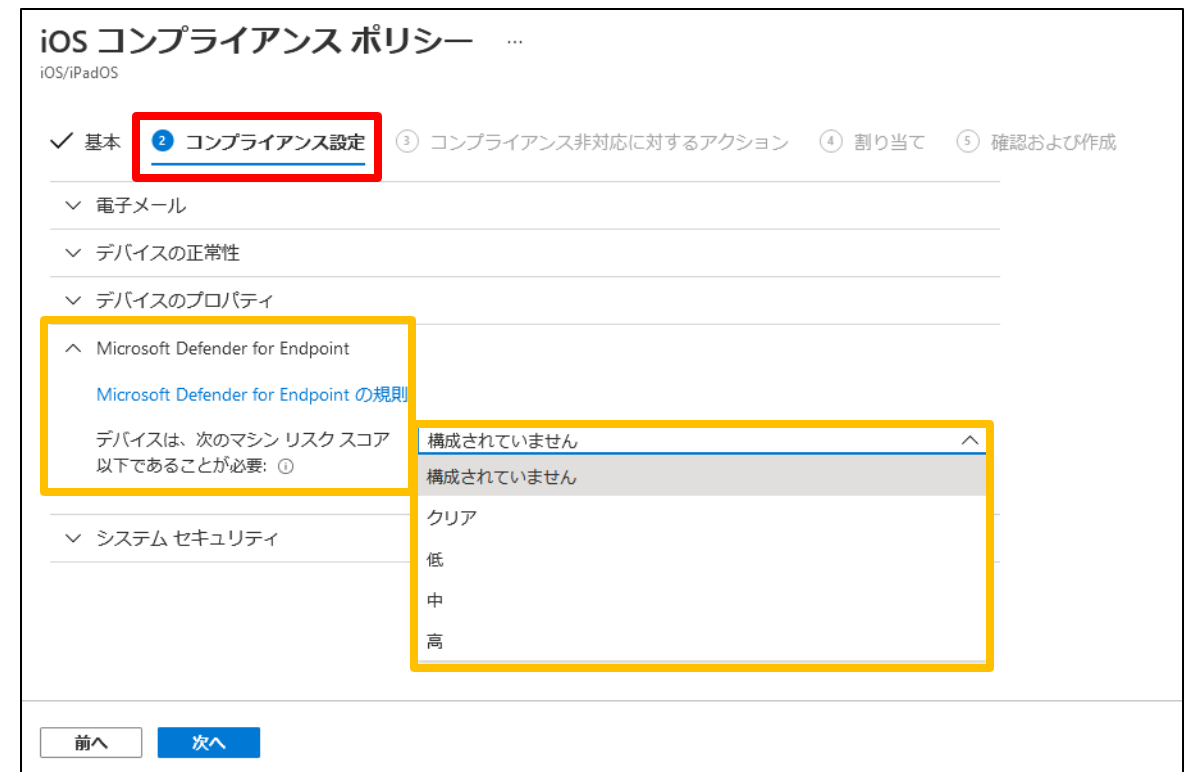


[参考] 技術資料

- **「iOS 向け Microsoft Defender for Endpoint」・・・前提条件**
 - <https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios>
- **「iOS 用エンドポイント用 Microsoft Defender の展開」**
 - <https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-atp/ios-install>
- **「iOS 機能のエンドポイント用に Microsoft Defender を構成する」**
 - <https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-atp/ios-configure-features>
- **「Android 向け Microsoft Defender for Endpoint」・・・前提条件**
 - <https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-android>
- **「Microsoft Intune を使用してAndroid 向け Microsoft Defender for Endpoint を展開する」**
 - <https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-atp/android-intune>
- **「Android のエンドポイント向け Defender の機能を構成する」**
 - <https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-atp/android-configure>

手順 3. デバイスのリスクスコアの設定

- コンプライアンス ポリシーで、デバイスのリスクスコアの最大許容値を設定する
- このリスクスコアを超えるデバイスには、非準拠のマークが付けられる
- 脅威レベル
 - クリア
 - セキュリティ上もっとも安全なレベル
 - デバイスには既存のいかなる脅威も存在できない
 - 低
 - デバイスに低レベルの脅威が存在する場合でも、準拠と判断する
 - 中
 - デバイスに低または中レベルの脅威が存在する場合でも、準拠と判断する
 - 高
 - 最も安全性が低いレベル
 - デバイスに低、中、高レベルの脅威が存在する場合でも、すべての脅威が許容される



手順 4. 高度なデバイス ベースの 条件付きアクセス ポリシーの作成

Azure AD
Premium P1

Intune

Microsoft
Defender
for Endpoint

Azure AD との
統合アプリケーション

クラウド アプリ ユーザー操作

対象 対象外

なし

すべてのクラウド アプリ

アプリを選択

選択

Office 365

Office 365 ⓘ

許可

アクセスをブロックまたは許可するため、ユーザー アクセスの適用を制御します。詳細情報

アクセスのブロック

アクセス権の付与

多要素認証を要求する ⓘ

デバイスは準拠しているとしてマーク済みである必要があります ⓘ

Hybrid Azure AD Join を使用したデバイスが必要 ⓘ

承認されたクライアント アプリが必要です ⓘ
承認されたクライアント アプリの一覧を表示

アプリの保護ポリシーが必要 ⓘ
ポリシーで保護されたクライアント アプリの一覧を表示します

パスワードの変更を必須とする ⓘ

複数のコントロールの場合

選択したコントロールすべてが必要

選択したコントロールのいずれかが必要

デバイス準拠

名前 *

Office 365 準拠デバイス ポリシー

割り当て

ユーザーとグループ ⓘ

組み込まれた特定のユーザー

クラウド アプリまたは操作 ⓘ

1 個のアプリ 件を含む

条件 ⓘ

1 個の条件が選択されました

アクセス制御

許可 ⓘ

1 個のコントロールが選択されました

セッション ⓘ

0 個のコントロールが選択されました

ポリシーの有効化

レポート専用 オン オフ

保存

対象 対象外

なし

すべてのユーザー

ユーザーとグループの選択

すべてのゲストと外部ユーザー ⓘ

ディレクトリ ロール ⓘ

ユーザーとグループ

選択

1 グループ

営業 営業グループ ...

Azure AD の
ユーザー/グループ

構成 ⓘ

はい いいえ

このポリシーを適用するクライアント アプリを選択します

先進認証クライアント

ブラウザー

モバイル アプリとデスクトップ クライアント

レガシ認証クライアント

Exchange ActiveSync クライアント ⓘ

他のクライアント ⓘ

クライアント アプリ

2-5

2章： Microsoft Intune

- Intune の概要
- Intune によるモバイル デバイス管理 (MDM)
- Intune によるモバイル アプリ管理 (MAM)
- Microsoft Defender for Endpoint との統合
- デバイスの登録
- Windows 10 の Azure AD 参加とハイブリッド Azure AD 参加



その他のデバイスの登録と構成

- iOS/iPadOS、macOS デバイスの登録
- Android デバイスの登録

1. iOS/iPadOS と macOS デバイス

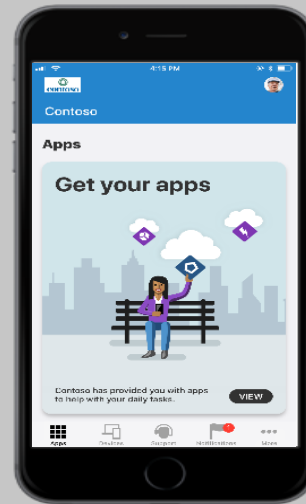
- Apple iOS 12.0 以降
- Apple iPadOS 13.0 以降
- macOS X 10.13 以降

「Intune に iOS/iPadOS デバイスを登録する」

<https://docs.microsoft.com/ja-jp/mem/intune/enrollment/ios-enroll>



ユーザー所有の iOS/iPadOS デバイス (BYOD)



会社所有の iOS/iPadOS デバイス

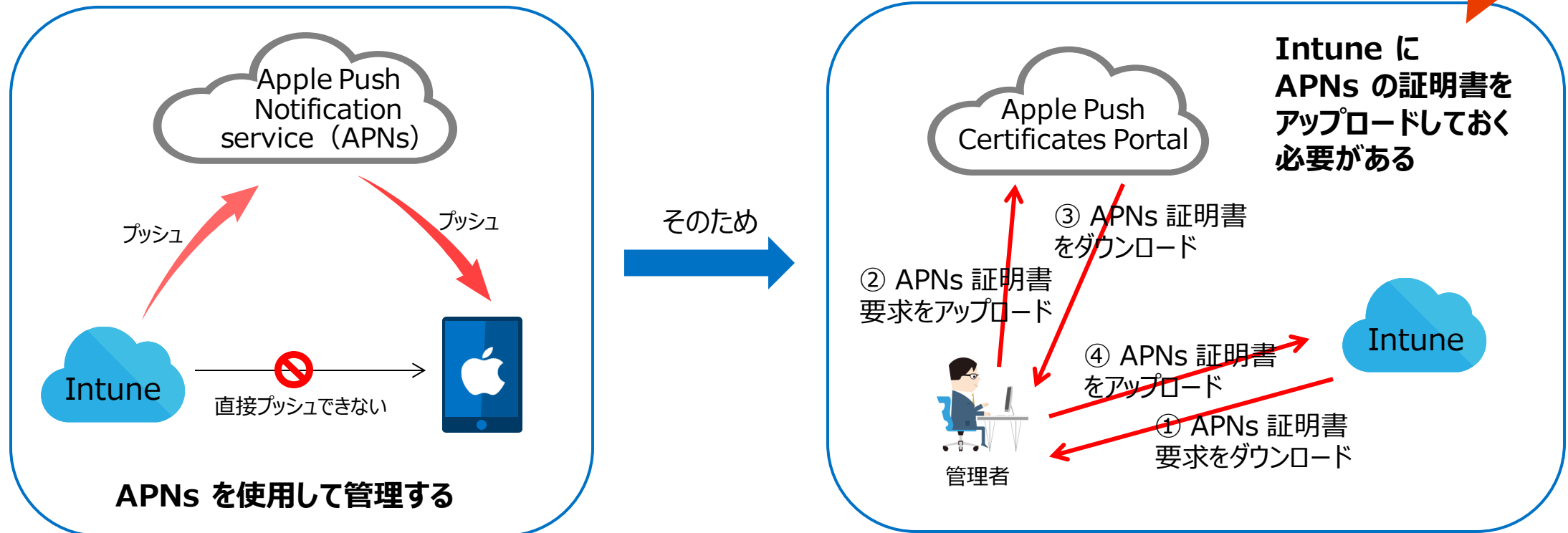
iOS/iPadOS のアプリ管理
(MAM のみ)

iOS/iPadOS のデバイス管理 + アプリ管理
(MDM + MAM)

Apple MDM プッシュ通知証明書

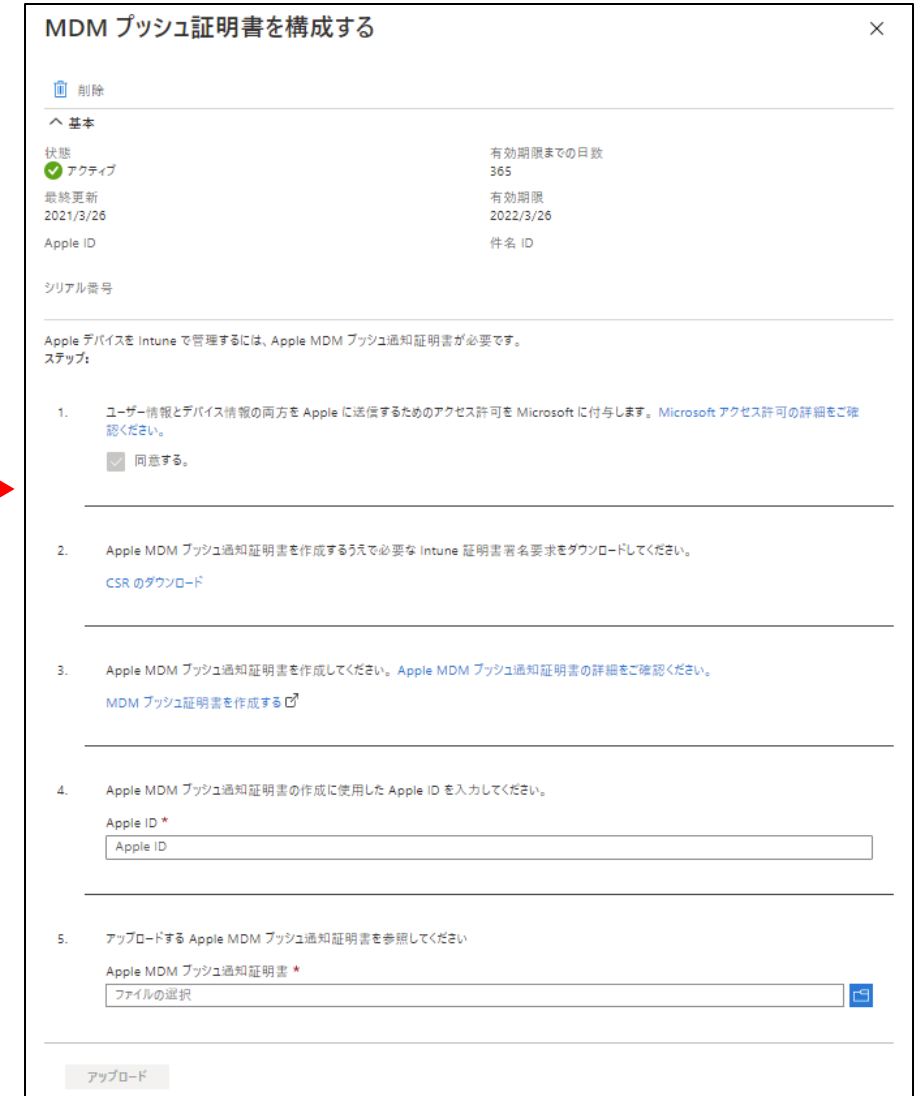
- Intune から、iOS および macOS デバイスを管理するには、Apple MDM プッシュ通知証明書（Apple Push Notification サービスの証明書）が必要
 - Intune は、iOS、macOS デバイスへのリモート管理に、Apple Push Notification サービス（APNs）を使用する

必須！



Apple MDM プッシュ通知証明書の取得

- 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



「Apple MDM プッシュ証明書を取得する」

<https://docs.microsoft.com/ja-jp/mem/intune/enrollment/apple-mdm-push-certificate-get>

会社所有の iOS/iPadOS デバイスの登録

- Apple の自動デバイス登録 (Apple Device Enrollment; ADE)
 - 登録プロファイルを“無線で”展開して、デバイスを管理対象として登録
- Apple School Manager
 - 学校向けのデバイス購入と登録プログラムで、ADE と同様の方法で登録
- Apple Configurator
 - mac コンピューターで実行している Apple Configurator を使用して登録
 - デバイスを USB 接続して、登録プロファイルをインストール
 - 方法 1：セットアップ アシスタントの登録
 - デバイスをワイプし、デバイスの新しいユーザー用に会社のポリシーをインストール
 - 方法 2：直接登録
 - デバイスをワイプせず、定義済みのポリシーでデバイスを登録

ユーザーによる iOS/iPadOS デバイスの登録

手順 1. App Store から “Intune ポータル サイト” アプリをダウンロード

手順 2. “Intune ポータル サイト” アプリを開き、職場または学校アカウントでサインイン

手順 3. 指示にしたがって、デバイスを登録する

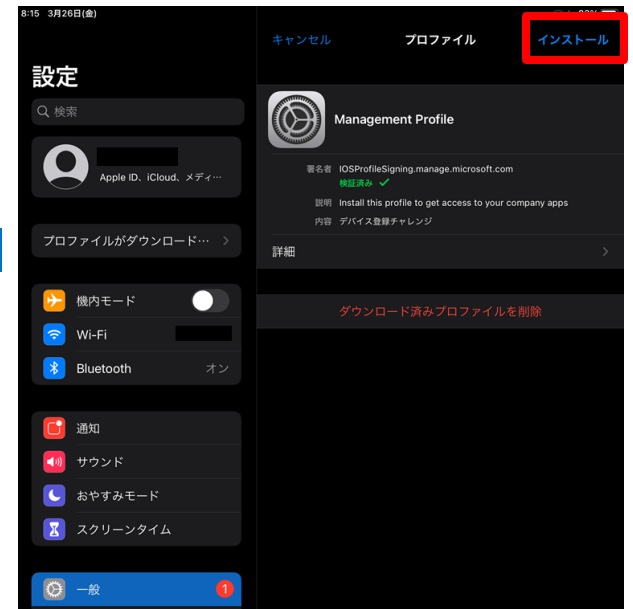
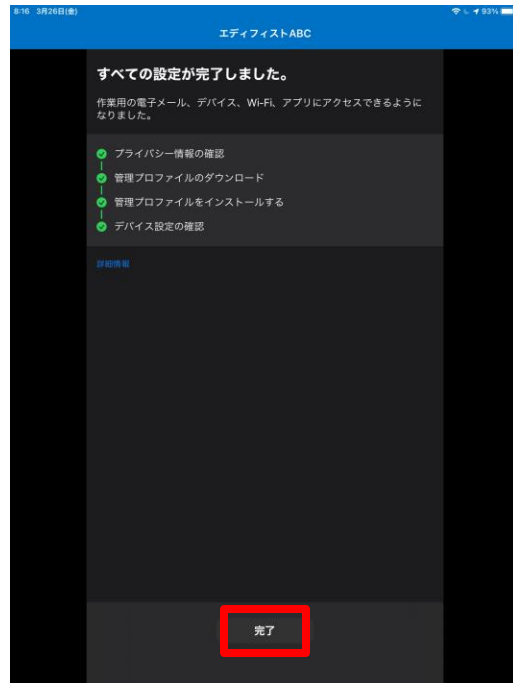
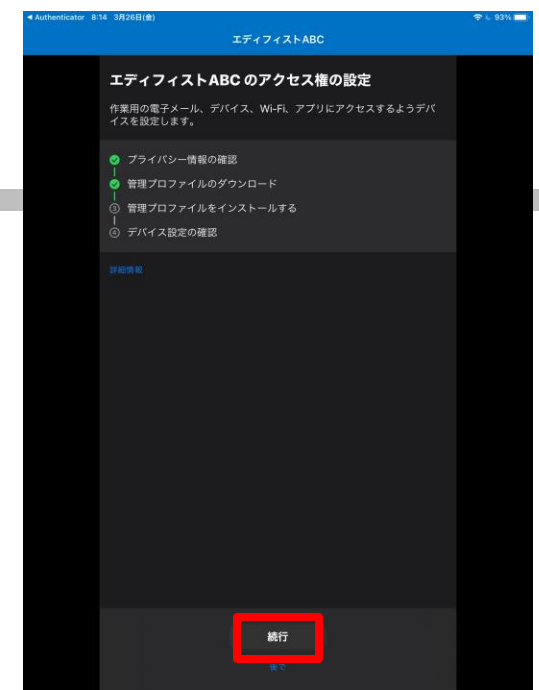
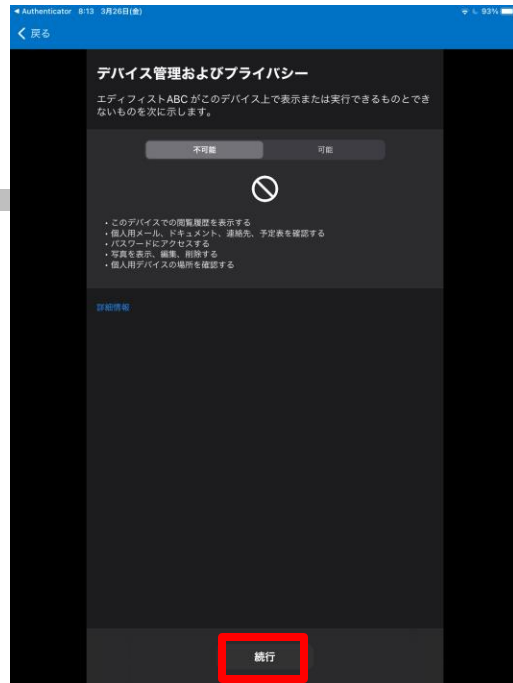
App Store の「Intune ポータル サイト」

<https://apps.apple.com/jp/app/intune-%E3%83%9D%E3%83%BC%E3%82%BF%E3%83%AB-%E3%82%B5%E3%82%A4%E3%83%88/id719171358>

「iOS デバイスからの会社のリソースへのアクセスを設定する」

<https://docs.microsoft.com/ja-jp/mem/intune/user-help/enroll-your-device-in-intune-ios>







macOS デバイスの登録

- **ユーザー所有の macOS デバイス (BYOD)**

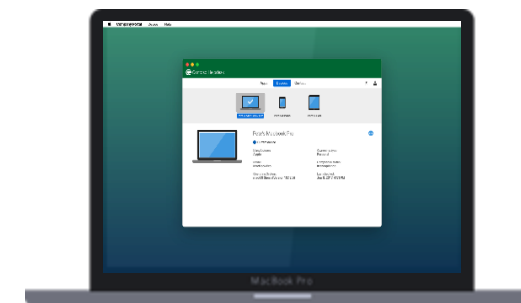
- Intune のポータル サイト Web サイトにアクセスする
 - <https://portal.manage.microsoft.com/>
- mac ポータル サイト アプリをダウンロードする
 - <https://aka.ms/EnrollMyMac>

- **会社所有の macOS デバイス**

- Apple の自動デバイス登録 (ADE)
- デバイス登録マネージャー (DEM)
 - DEM アカウントを使用して、最大 1,000 台のモバイル デバイスを登録
- Apple Configurator の直接登録

「Intune で macOS デバイスの登録を
セットアップする」

<https://docs.microsoft.com/ja-jp/mem/intune/enrollment/macos-enroll>



[参考] 技術資料

- **「Intune に iOS/iPadOS デバイスを登録する」**
 - <https://docs.microsoft.com/ja-jp/mem/intune/enrollment/ios-enroll>
- **「Apple の Automated Device Enrollment を使用して iOS/iPadOS デバイスを自動登録する」**
 - <https://docs.microsoft.com/ja-jp/mem/intune/enrollment/device-enrollment-program-enroll-ios>
- **「Intune で macOS デバイスの登録をセットアップする」**
 - <https://docs.microsoft.com/ja-jp/mem/intune/enrollment/mac-os-enroll>
- **「macOS デバイスの直接登録の使用」**
 - <https://docs.microsoft.com/ja-jp/mem/intune/enrollment/device-enrollment-direct-enroll-macos>

2. Android デバイス

- Android Enterprise は、Google が提供する企業向け端末管理プログラム

ユーザー所有 (BYOD)

会社所有

Intune
アプリ保護
(MAM)

Android Enterprise

仕事用プロファイルを備えたデバイス
(Work Profile)

専用端末
(Dedicated
Device)

完全管理されたデバイス
(Full Managed)

アプリのみ
管理

- 個人用と仕事用の環境を分けて作る
- それぞれの環境にアプリ をインストールすることで、個人利用が可能なデバイスとして設定

- 会社所有のデバイスを単一用途の企業専用端末として設定
- キオスク スタイルのデバイス

- 会社支給用のデバイス
- 完全に企業の管理下において制御することで、ビジネス専用端末として設定する

マネージド Google Play アカウントに Intune アカウントを接続

- Android Enterprise の仕事用プロフィールを備えたデバイス、専用端末、フル マネージド デバイスをサポートするには、Intune テナント アカウントを マネージド Google Play アカウントに接続する必要があります

The image shows two screenshots illustrating the connection process between Intune and Managed Google Play.

Left Screenshot: Microsoft Endpoint Manager admin center

- The left sidebar shows the navigation menu with "デバイスの登録" (Device Enrollment) highlighted in a red box.
- The main content area is titled "デバイスの登録 | Android 登録" (Device Enrollment | Android Enrollment).
- Under "Android 登録", the "マネージド Google Play" (Managed Google Play) option is highlighted with a red box. Below it, the text reads: "マネージド Google Play アカウントを Intune にリンクします。" (Link the Managed Google Play account to Intune).
- Other options listed include Windows 登録, Apple 登録, 登録制限, 業務用デバイスの ID, and デバイス登録マネージャー.

Right Screenshot: Managed Google Play app interface

- The top banner says "Android を仕事に活用" (Use Android for work) with a "スタートガイド" (Get started) button.
- The "マネージド Google" (Managed Google) section shows the status: "Android の登録" (Android enrollment) is "切断" (Disconnected).
- The "基本" (Basic) section shows: "状態" (Status) as "セットアップが完了していません" (Setup is not complete), "Google アカウント" (Google account) as "利用不可" (Not available), and "組織" (Organization) as "利用不可" (Not available).
- The "Android Enterprise デバイスを管理するには、Intune を、会社のマネージド Google Play アカウントに接続する必要があります。" (To manage Android Enterprise devices, you need to connect Intune to your company's Managed Google Play account.) message is present.
- There are two numbered steps: 1. "ユーザー情報とデバイス情報の両方を Google に送信するためのアクセス許可を Microsoft に付与します。" (Grant Microsoft access to send user and device info to Google.) and 2. "Android Enterprise 登録を有効にするため、ご使用の Intune テナントを Google 管理者アカウントに接続します。" (Connect your Intune tenant to the Google admin account to enable Android Enterprise enrollment.).
- A blue button at the bottom says "Google を起動して今すぐ接続します。" (Open Google and connect now).

Red arrows indicate the flow from the "Managed Google Play" option in the admin center to the corresponding section in the app, and from the app's status section to the "Android を仕事に活用" banner.

Android デバイスの登録

Microsoft Endpoint Manager admin center

ホーム > デバイス > デバイスの登録

デバイス | デ... ×

検索 (Ctrl+/)

概要

すべてのデバイス

モニター

プラットフォーム別

Windows

iOS/iPadOS

macOS

Android

デバイスの登録

デバイスの登録

ポリシー

コンプライアンス ポリシー

条件付きアクセス

構成プロファイル

スクリプト

グループ ポリシー分析 (プレビュー)

Windows 10 更新リング

Windows 10 の機能更新ブログ...

iOS または iPadOS のポリシーの...

登録制限

eSIM 携帯ネットワーク プロファイ...

ポリシー セット

その他

デバイスのクリーンアップ ルール

デバイスの登録 | Android 登録 ...

検索 (Ctrl+/)

Intune でデバイスのセットアップを開始するには、Android 管理ソリューションと登録プロファイルの種類を選択してください。Android Enterprise ソリューションを使用している場合は、組織の Google Play アカウントを Intune にリンクしてから、他の操作を行ってください。 [詳細をご覧ください。](#)

Windows 登録

Apple 登録

Android 登録

登録制限

業務用デバイスの ID

デバイス登録マネージャー

Android Enterprise

必要なコンポーネント

マネージド Google Play

マネージド Google Play アカウントを Intune にリンクします。

登録プロファイル

仕事用プロフィールを備えた個人所有のデバイス

仕事用プロフィールで個人の登録を管理します。

会社が所有する専用端末

キオスクおよびタスク デバイスについて、デバイス所有者の登録を管理します。

会社が所有する完全に管理されたユーザー デバイス

ユーザー デバイスについて、デバイス所有者の登録を管理します。

仕事用プロフィールを備えた会社所有のデバイス (プレビュー)

仕事用プロフィールを備えた会社のデバイスの登録を管理します。

Android デバイスマネージャー

必要なコンポーネント

デバイス管理者特権を持つ個人所有のデバイスと会社所有のデバイス

Android デバイスマネージャーを使って、個人および会社所有のデバイスを管理します。

会社が所有する完全に管理されたユーザー デバイス ×

Android の登録

会社所有のデバイスをエンドユーザーが登録できるようにします。ユーザー デバイスを登録するために、指定された登録トークンをコピーして、エンドユーザーに送信してください。 [詳細をご覧ください。](#)

または、ゼロ タッチを利用して Android デバイス向けの自動プロビジョニングを構成できます。この機能の構成は、Intune 管理コンソールでは現在利用できませんが、今後利用可能になる予定です。

ゼロ タッチ ポータルで自動プロビジョニングの展開を構成します。 [🔗](#)

会社が所有するユーザー デバイスの登録をユーザーに許可する

登録トークン

以下の登録トークンを強調表示してコピーし、エンドユーザーに送信するか、ヘルプデスクのサイトに投稿して、エンドユーザーがデバイスを登録できるようにしてください。この単一のトークンはすべてのユーザーに対して有効であり、有効期限はありません。 [詳細をご覧ください。](#)

業務用デバイスの登録トークン

以下のトークンを業務用デバイスでスキャンして、デバイスを会社に登録します。 [詳細をご覧ください。](#)

トークン

MYKKCATG

Android Enterprise の登録プロファイルの作成

※ Android のデバイス管理者機能が、Android Enterprise に置き換えられた。継続的にデバイスを管理し、セキュリティを確保するには、すべての新しい登録に Android Enterprise を使用することをオススメ

[参考] 技術資料

- **「Android Enterprise フル マネージド デバイスの Intune 登録を設定する」**
 - <https://docs.microsoft.com/ja-jp/mem/intune/enrollment/android-fully-managed-enroll>
- **「Android Enterprise 仕事用プロフィール デバイスの登録を設定する」**
 - <https://docs.microsoft.com/ja-jp/intune/android-work-profile-enroll>
- **「Android Enterprise 専用デバイスの Intune 登録を設定する」**
 - <https://docs.microsoft.com/ja-jp/mem/intune/enrollment/android-kiosk-enroll>

2-6

2章： Microsoft Intune

- Intune の概要
- Intune によるモバイル デバイス管理 (MDM)
- Intune によるモバイル アプリ管理 (MAM)
- Microsoft Defender for Endpoint との統合
- デバイスの登録
- Windows 10 の Azure AD 参加とハイブリッド Azure AD 参加

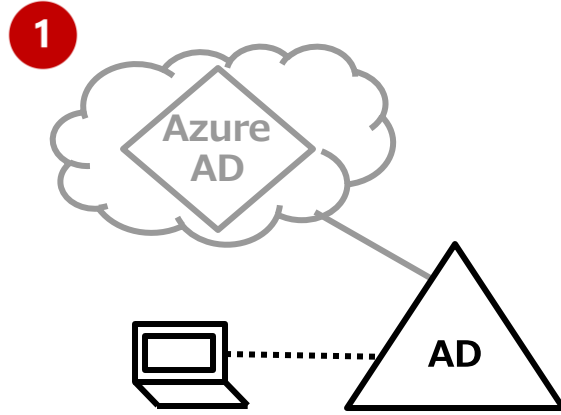


Windows 10 の Azure AD 参加とデバイス登録

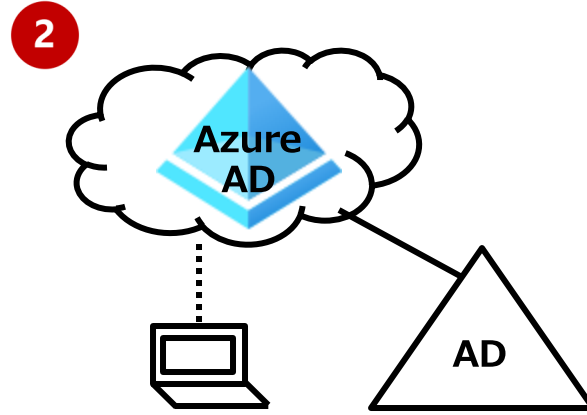
- Windows PC 管理の方式
- Azure AD 参加
- ハイブリッド Azure AD 参加
- 共同管理 (Co-Management)

1. Windows PC 管理の方式

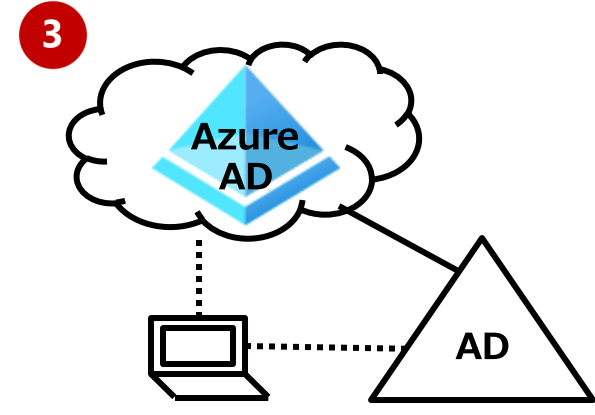
会社所有のデバイス



- ・ドメイン参加
- ・ConfigMgr 管理

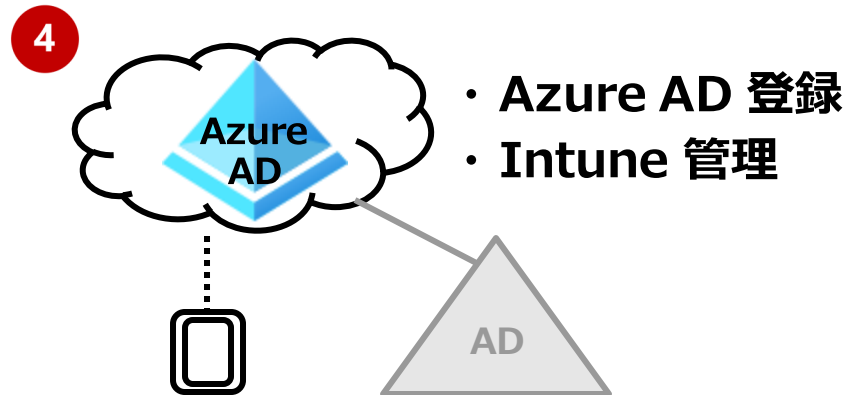


- ・ Azure AD 参加
- ・ Intune 管理



- ・ ハイブリッド Azure AD 参加
- ・ ConfigMgr と Intune の共同管理

ユーザー所有のデバイス



- ・ Azure AD 登録
- ・ Intune 管理

「デバイス ID とは」

<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/overview>

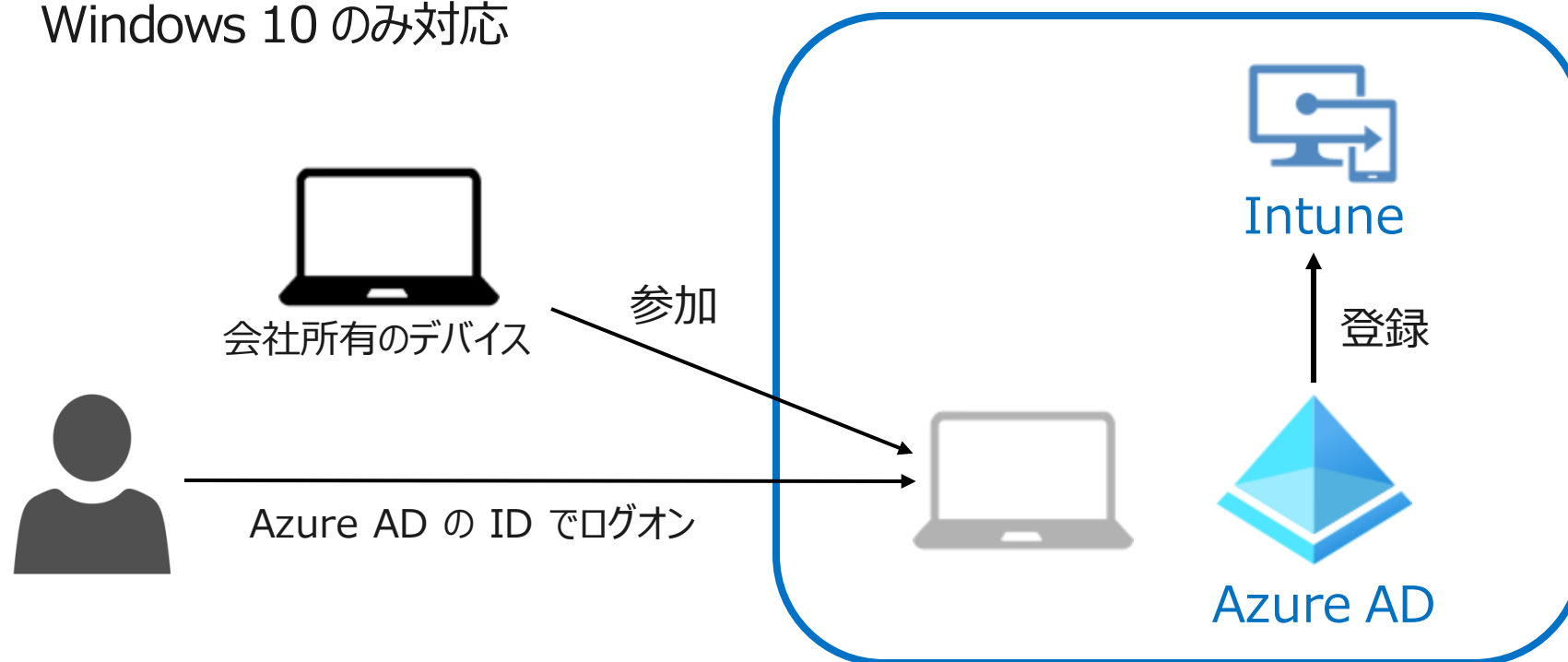
2 Azure AD 参加

- クラウドを中心とした組織に適している
 - オンプレミス Active Directory に参加している場合は利用不可
- Azure AD の ID で PC にログイン
- Windows 10 のみ対応

- クラウドとオンプレミスの両方のリソースへの SSO

「Azure AD 参加済みデバイス上でオンプレミスリソースへの SSO が機能するしくみ」

<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/azuread-join-ss0>



「Azure AD 参加済みデバイス」

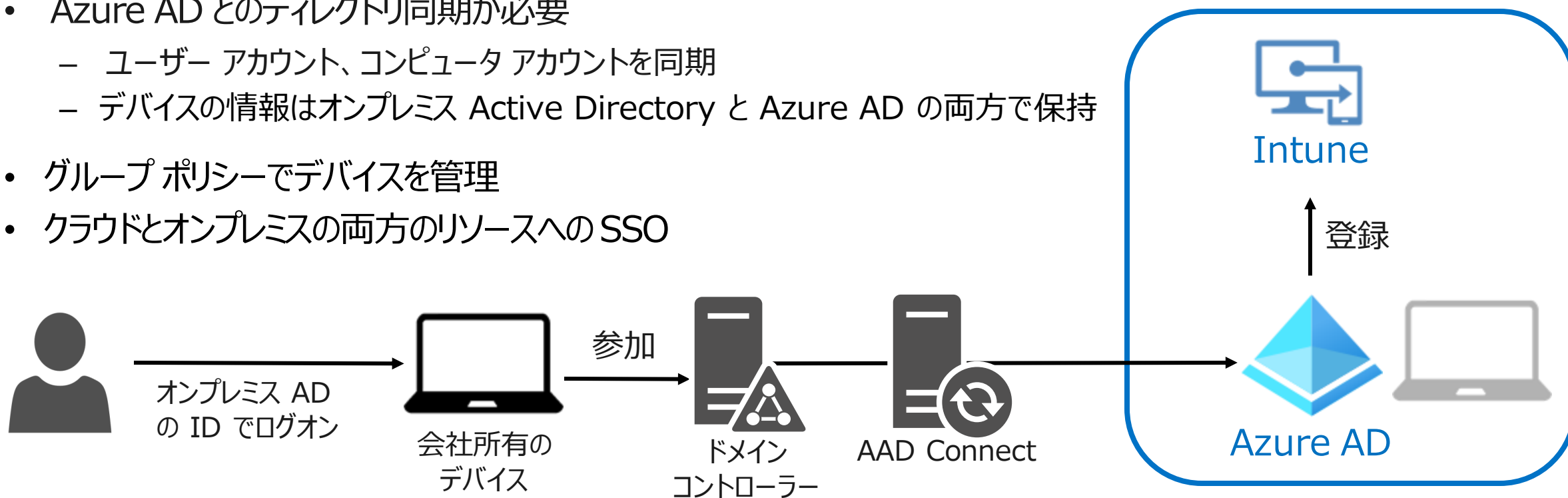
<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/concept-azure-ad-join>

3 ハイブリッド Azure AD 参加

- 既存のオンプレミス Active Directory 基盤を活用してクラウドを利用する組織に適している
 - ドメイン参加の状態はそのまま
- オンプレミス Active Directory の ID で、PC にログイン
- Windows 8.1、10 および Windows Server 2008 以降をサポート
- Azure AD とのディレクトリ同期が必要
 - ユーザー アカウント、コンピュータ アカウントを同期
 - デバイスの情報はオンプレミス Active Directory と Azure AD の両方で保持
- グループ ポリシーでデバイスを管理
- クラウドとオンプレミスの両方のリソースへの SSO

「ハイブリッド Azure AD 参加済みデバイス」

<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/concept-azure-ad-join-hybrid>

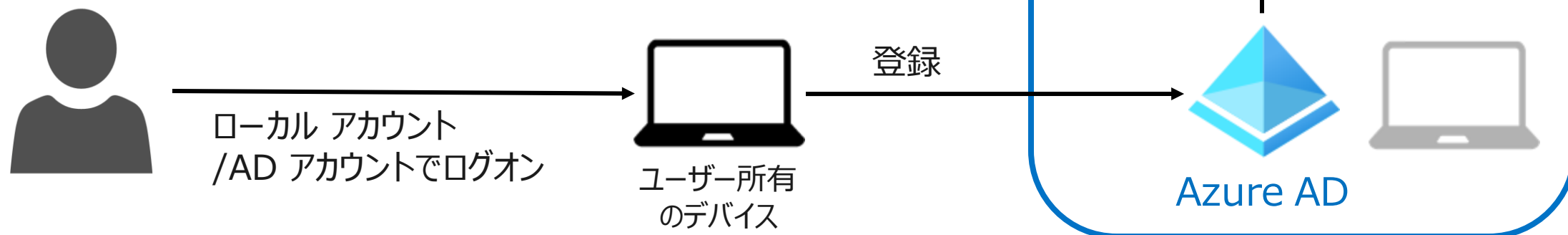


4 Azure AD 登録

- ユーザー所有デバイス向けのデバイス登録オプション (BYOD)
 - ユーザー所有デバイスを使用して、Azure AD 管理下の組織のリソースにアクセスできるようにする構成
- デバイスへのログオン方法は変わらない
 - ユーザーのローカル資格情報
- Windows 10、iOS、Android、および macOS をサポート
- クラウドリソースへの SSO

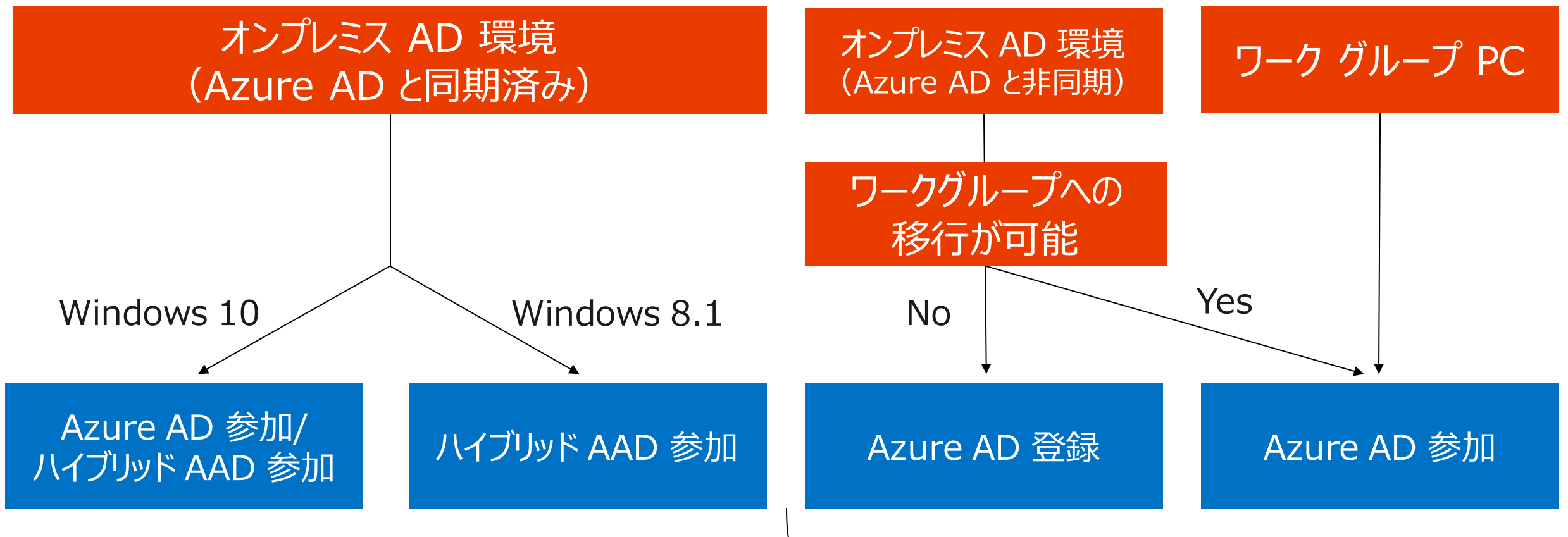
「Azure AD 登録済みデバイス」

<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/concept-azure-ad-register>



3つの管理方式の選択

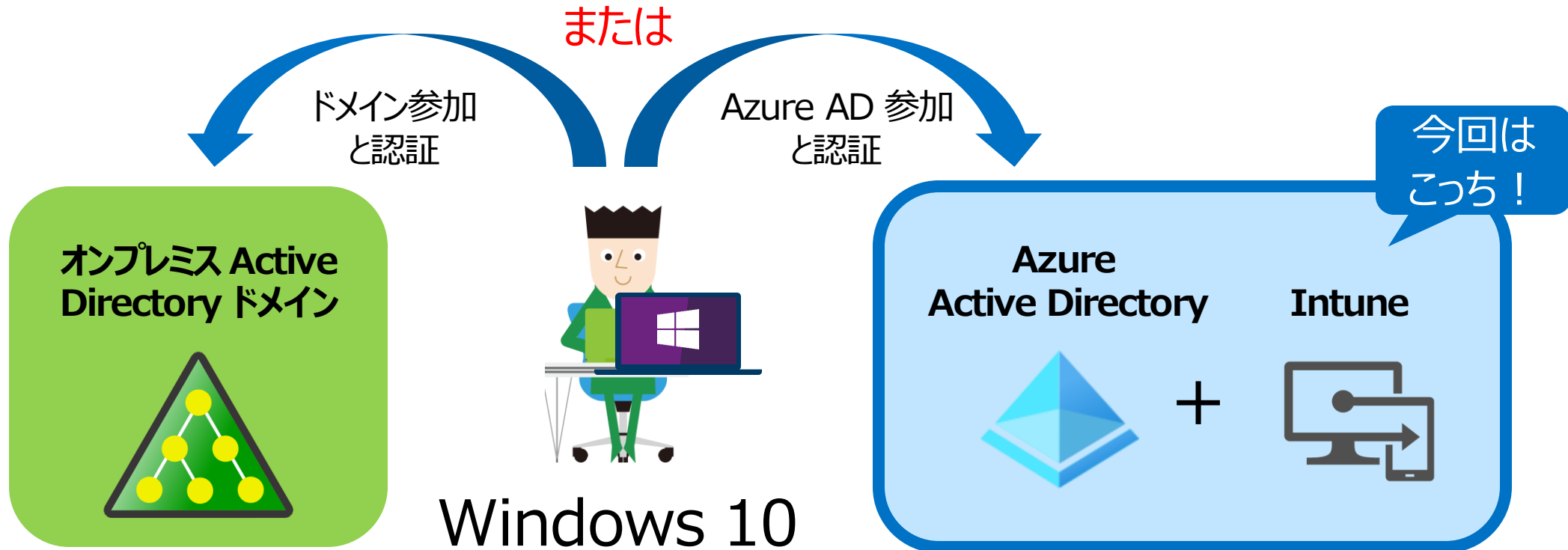
- オンプレミス Active Directory 環境や OS により、構成可能な方式が決まる



※Windows 8.1 は Windows 10 にアップデート

2. Azure AD 参加

- Windows 10 は、オンプレミスのドメイン または Azure AD に参加できる



[比較] ドメイン参加と Azure AD 参加

今回は
こっち！

	ドメイン参加	Azure AD 参加
SSO の対象となるアプリケーション	Web アプリケーション、 ファイル サーバー など	Web アプリケーション
ユーザー認証	ドメイン コントローラーが認証 (パスワードがネットワークを経由する)	デバイス内で認証 (パスワードがネットワークを経由しない)
参加可能なデバイスの種類	Windows デバイス全般	Windows 10 のみ
デバイス管理の方法	グループ ポリシー	MDM ツール (Microsoft Intune など)
デバイス登録と認証	登録時にコンピューター アカウントと パスワードが生成され、コンピューター アカウントのパスワードによって認証される	登録時にキー ペアが生成され、 秘密キーによって署名されたサインイン 要求が、公開キーで検証され、認証される
認証によって発行されるチケット	TGT (Ticket Granting Ticket)	PRT (Primary Refresh Token)
リソース アクセスのためのチケット	ST (Service Ticket)	アクセストークン

Azure AD 参加の有効化



- Azure AD テナントで、Azure AD 参加が許可されている必要がある（既定は有効）
 - Azure AD テナントの [デバイス] – [デバイスの設定]

Azure Active Directory admin center

ダッシュボード > エディファストABC > デバイス

エディファスト... x

Azure Active Directory

デバイス | デバイスの設定 ...

エディファストABC - Azure Active Directory

保存 破棄 フィードバックがある場合

すべてのデバイス

デバイスの設定

Enterprise State Roaming

BitLocker キー (プレビュー)

問題の診断と解決

アクティビティ

監査ログ

一括操作の結果 (プレビュー)

トラブルシューティング + サポート

新しいサポート リクエスト

パスワードリセット

ユーザーはデバイスを Azure AD に参加させることができます ⓘ

すべて 選択済み なし

選択済み

メンバーが選択されていません

ユーザーはデバイスを Azure AD に登録できます ⓘ

すべて なし

この設定が機能するしくみの詳細情報

デバイスを Azure AD 参加済みまたは Azure AD 登録済みにするには多要素認証が必要 ⓘ

はい いいえ

ユーザーごとのデバイスの最大数 ⓘ

50

すべての Azure AD 参加済みデバイスに対する追加のローカル管理者

管理 すべての Azure AD 参加済みデバイスに対する追加のローカル管理者

Enterprise State Roaming

Enterprise State Roaming の設定を管理する

Azure AD
参加の許可

「Azure Active Directory 管理センター」
<https://aad.portal.azure.com/>

Intune へのデバイス登録の有効化



- Microsoft Intune の [デバイス] – [デバイスの登録] – [登録制限] で、Intune に登録できるプラットフォームの種類や台数を制限できる（既定のポリシーでは、すべてのプラットフォームを許可、5 台/ユーザー）

Microsoft Endpoint Manager admin center

ホーム > デバイス > デバイスの登録

デバイス | デ... ×

デバイスの登録 | 登録制限 ...

作成の制限

Windows 登録

Apple 登録

Android 登録

登録制限

業務用デバイスの ID

デバイス登録マネージャー

デバイスの種類の制限

登録できるプラットフォーム、バージョン、および管理の種類を定義します。

優先度	名前
既定	すべてのユーザー

デバイスの上限数の制限

各ユーザーが登録できるデバイス数を定義します。

優先度	名前	デバイスの
既定	すべてのユーザー	5

ホーム > デバイス > デバイスの登録 > すべてのユーザー

すべてのユーザー | プロパティ ...

概要

基本

名前

説明

プラットフォームの設定 編集

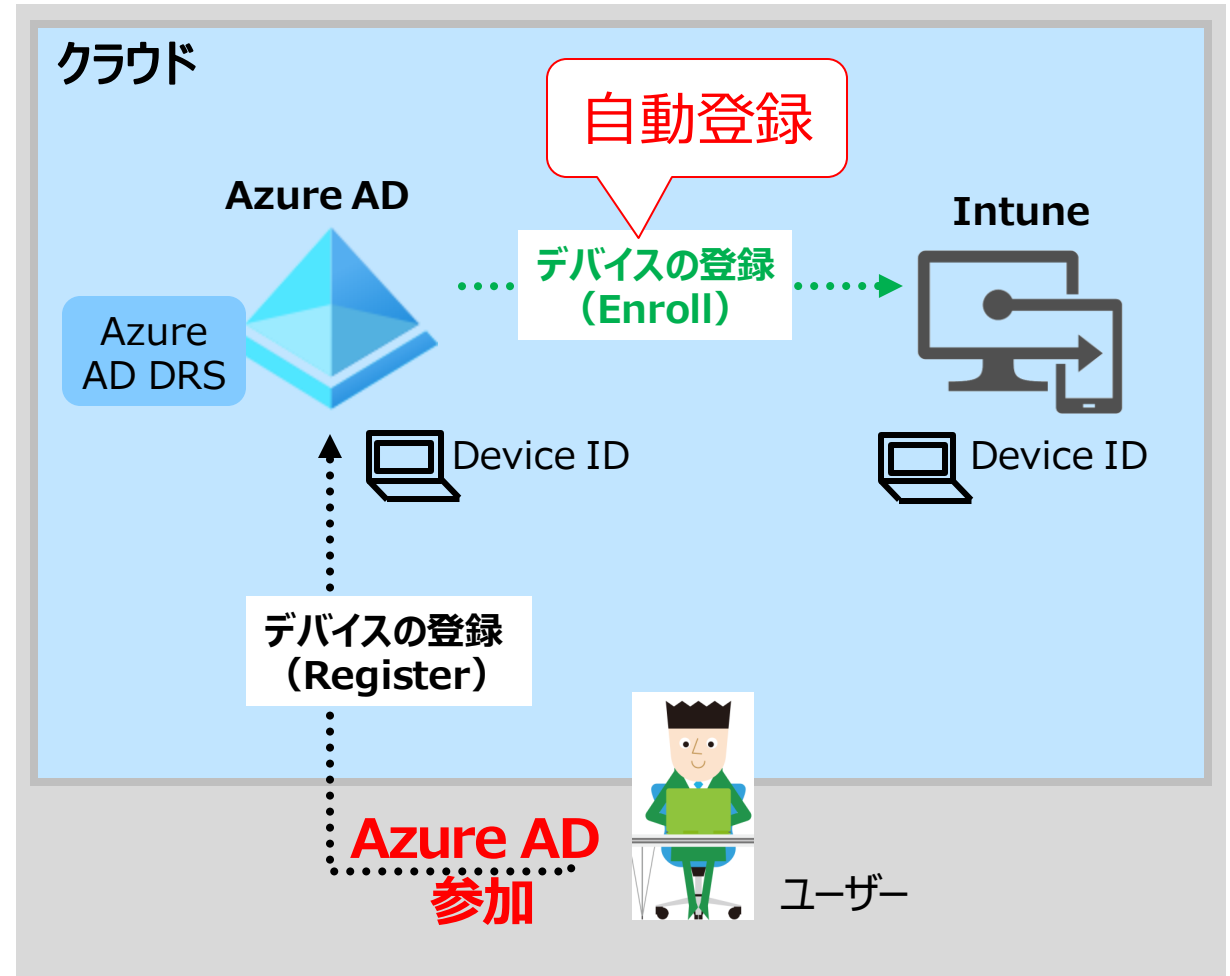
種類	プラットフォーム
Android Enterprise (仕事用プロファイル)	許可
Android デバイス管理者	許可
iOS/iPadOS	許可
macOS	許可
Windows (MDM)	許可

※ デバイス登録制限ポリシーが複数構成されている場合、
最も高い優先度のデバイス登録制限が適用される

※ 優先度は、小さい値が優先される

Azure AD から Intune への自動登録

- Windows 10 が Azure AD 参加する際に、Intune にもデバイスが自動登録されるように構成できる



「Windows デバイスの登録をセットアップする」

<https://docs.microsoft.com/ja-jp/mem/intune/enrollment/windows-enroll>

Azure AD から Intune への自動登録の構成

- [モビリティ (MDM および MAM)] - [Microsoft Intune] で構成する

The screenshot displays the Microsoft Endpoint Manager admin center interface. The left-hand navigation pane shows the 'デバイス' (Devices) menu item highlighted with a red box. The main content area is divided into three sections: 'Windows | Windows 登録' (Windows | Windows enrollment), 'Windows のポリシー' (Windows policies), and '構成' (Configuration). The '構成' section is further divided into 'MDM ユーザー スコープ' (MDM user scope) and 'MAM ユーザー スコープ' (MAM user scope). The 'MDM ユーザー スコープ' section is highlighted with a red box and contains the following configuration items:

項目	設定	ステータス
MDM ユーザー スコープ	なし 一部 すべて	
MDM 利用規約 URL	https://portal.manage.microsoft.com/TermsOfUse.aspx	✓
MDM 探索 URL	https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc	✓
MDM 準拠 URL	https://portal.manage.microsoft.com/?portalAction=Compliance	✓

The 'MAM ユーザー スコープ' section is also visible and contains the following configuration items:

項目	設定	ステータス
MAM ユーザー スコープ	なし 一部 すべて	
MAM 利用規約 URL		✓
MAM 探索 URL	https://wip.mam.manage.microsoft.com/Enroll	✓
MAM 準拠 URL		✓

A red arrow points from the '自動登録' (Automatic enrollment) section to the '構成' (Configuration) section, indicating the flow of configuration.

※ 組織が所有するデバイスで、両方のスコープが有効な場合、MDM ユーザー スコープが優先される

※ ユーザー所有のデバイスで、MAM ユーザー スコープと MDM ユーザー スコープ両方が有効な場合、MAM ユーザー スコープが優先される

Azure AD 参加とデバイス登録の実行

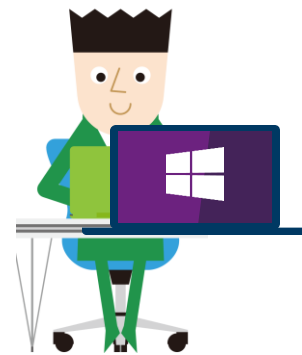
ユーザー操作



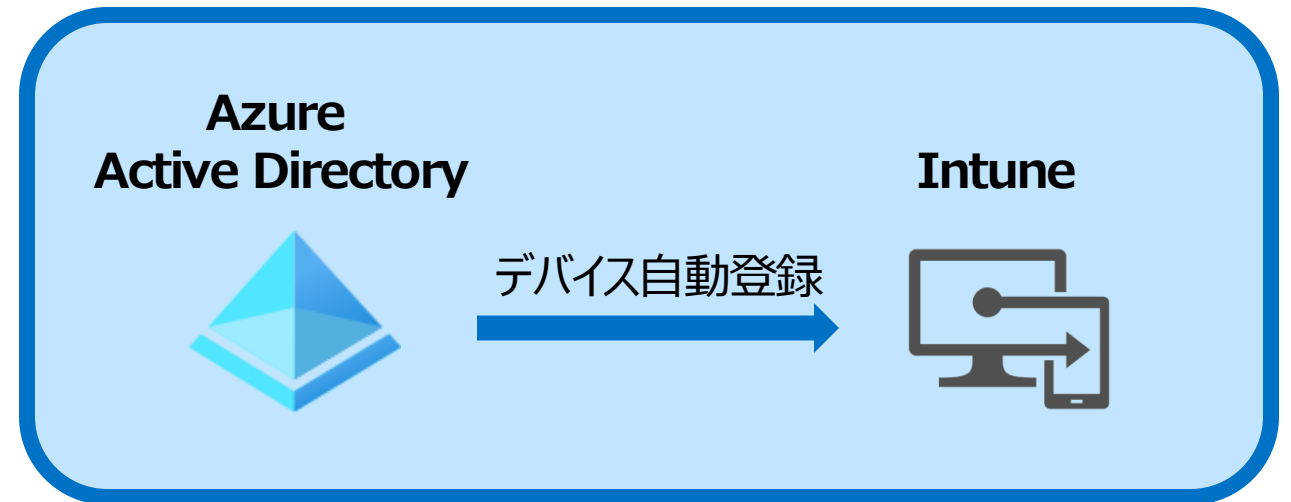
ユーザー

- Azure AD 参加は、Windows 10 のみサポートされている
 - Intune へのデバイス自動登録機能によって、Intune にも自動登録させることができる

- ① Azure AD への参加
- ② Azure AD へのサインイン



Windows 10



① Azure AD への参加 1/3

ユーザー操作



ユーザー

- Windows 10 デバイスの [設定] - [アカウント] - [職場または学校にアクセスする] の [+ 接続]

The screenshot illustrates the navigation path in the Windows 10 Settings application. On the left, the Start menu is shown with the Settings gear icon highlighted by a red box. An arrow points from this icon to the main Settings window. In the main window, the 'アカウント' (Accounts) category is highlighted with a red box. An arrow points from 'アカウント' to the '職場または学校にアクセスする' (Connect to a workplace or school) option, which is also highlighted with a red box. A second arrow points from this option to the '+ 接続' (Connect) button, which is highlighted with a red box. The right pane shows the '職場または学校にアクセスする' settings page, including a search bar, a description of access, and a list of related settings.

設定

ホーム

設定の検索

アカウント

システム
ディスプレイ、サウンド、通知、電源

ネットワークとインターネット
Wi-Fi、機内モード、VPN

ユーザーの情報

メールとアカウント

サインイン オプション

職場または学校にアクセスする

他のユーザー

設定の同期

簡単操作
ナレーター、拡大鏡、ハイコントラスト

職場または学校にアクセスする

メール、アプリ、ネットワークといったリソースにアクセスできるようになります。ただし、接続した場合でも、職場または学校によってデバイスの一部の機能が制御されることがあり、変更できる設定が限定されたりします。
具体的な情報については、職場や学校にお問い合わせください。

+ 接続

関連設定

プロビジョニング パッケージを追加または削除する

管理ログ ファイルのエクスポート

テストを受けるためのアカウントの設定

デバイス管理のみに登録する

① Azure AD への参加 2/3

ユーザー操作



ユーザー

- [このデバイスを Azure Active Directory に参加させる] リンクをクリック

Microsoft アカウント

職場または学校アカウントのセットアップ

メール、アプリ、ネットワークなどのリソースにアクセスできるようになります。接続する場合、職場または学校が、デバイスで変更できる設定などの制御を行う可能性があります。詳しい情報に関しては、直接お問い合わせください。

別の操作:

これらの操作によって、デバイスは組織のデバイスとして設定され、組織はこのデバイスを完全に制御できるようになります。

[このデバイスを Azure Active Directory に参加させる](#)

[このデバイスをローカルの Active Directory ドメインに参加させる](#)

次へ

Microsoft

サインイン

User2@edifistabc.net

アカウントにアクセスできない場合

セキュリティ

Microsoft

← user2@edifistabc.net

パスワードの入力

.....

[パスワードを忘れた場合](#)

サインイン

Azure AD ユーザー
アカウントでサインイン

① Azure AD への参加 3/3

ユーザー操作



ユーザー

• [参加する] をクリック

これがあなたの組織のネットワークであることを確認してください

これがあなたの組織のネットワークであることを確認してください

続行すると、システム ポリシーが有効になったり、その他の変更が PC に加えられたりする場合があります。これはあなたの組織のネットワークに間違いありませんか?

接続先: edifistabc.net
ユーザー名: user2@edifistabc.net
ユーザーの種類: 管理者

キャンセル **参加する**

Microsoft アカウント

これで完了です。

このデバイスは、エディフィストABC に接続しています。

この新しいアカウントを使用する際には、[スタート] ボタンをクリックしてから、現在のアカウントの画像を選択し、[アカウントの切り替え] を選択します。
user2@edifistabc.net メールとパスワードを使用してサインインします。

設定

ホーム

設定の検索

アカウント

ユーザーの情報

メールとアカウント

サインイン オプション

職場または学校にアクセスする

メール、アプリ、ネットワークといったリソースにアクセスできるようになります。ただし、接続した場合でも、職場または学校によってデバイスの一部の機能が制御されることがあり、変更できる設定が限定されたりします。具体的な情報については、職場や学校にお問い合わせください。

接続

エディフィストABC の Azure AD に接続済み
user2@edifistabc.net によって接続済み

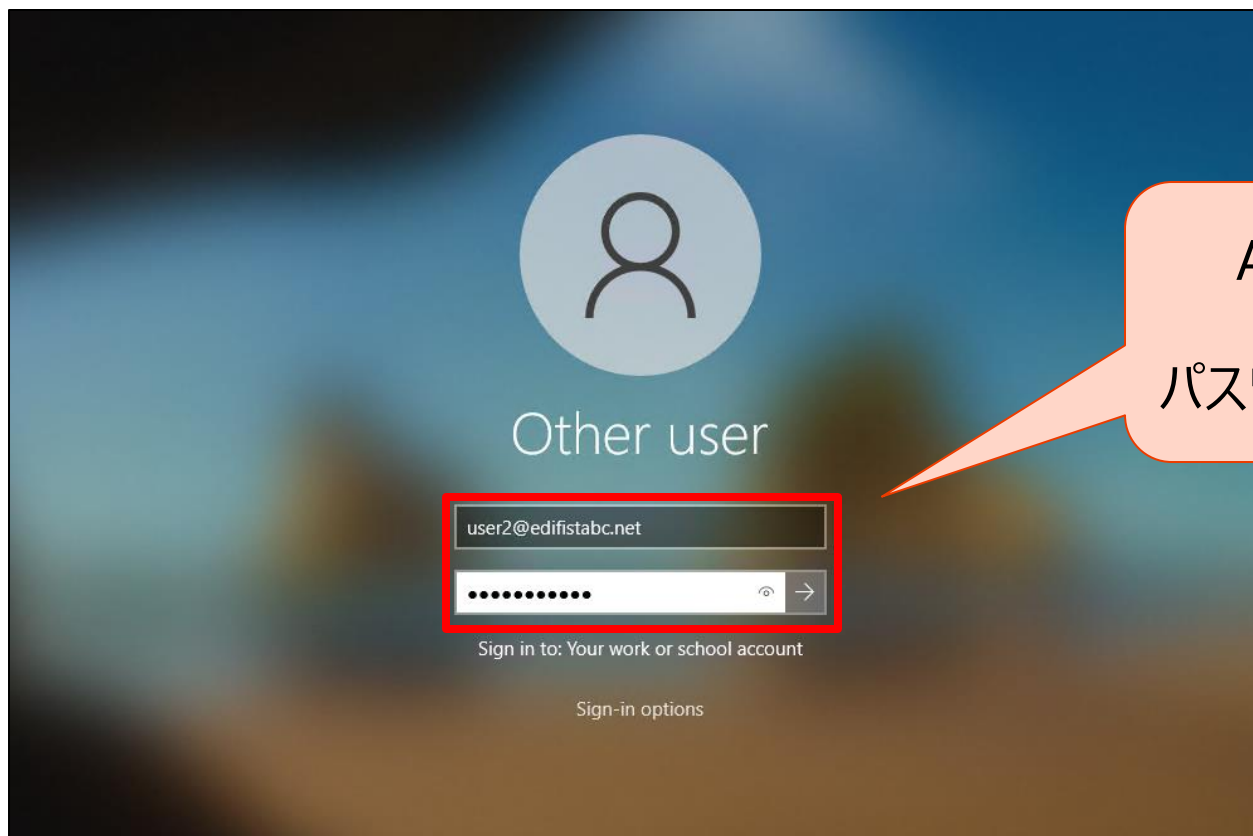
② Azure AD へのサインイン

ユーザー操作



ユーザー

- Azure AD 参加が完了すると、Azure AD の ID で、その Windows 10 デバイスにサインインできるようになる
 - サインイン画面で、[他のユーザー] をクリックし、Azure AD ユーザー名とパスワードでサインイン



Azure AD の
ユーザー名と
パスワードでサインイン

[参考] 技術資料

- 組織ネットワーク内のコンピューターから、次の URL にアクセスできることを確認する
 - <https://enterpriseregistration.windows.net>
 - <https://login.microsoftonline.com>
 - <https://device.login.microsoftonline.com>
- プロキシ経由でインターネットにアクセスする必要がある組織の場合は、Web プロキシ自動発見 (WPAD) を構成する

「チュートリアル: マネージド ドメイン用のハイブリッド Azure Active Directory 参加の構成」

<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/hybrid-azuread-join-managed-domains>

「ハイブリッド ID で必要なポートとプロトコル」

<https://docs.microsoft.com/ja-jp/azure/active-directory/hybrid/reference-connect-ports>

Azure AD に登録された Windows 10 デバイス



- Azure AD 参加によって登録されたデバイスは、Azure AD 参加を行ったユーザーと関連付けて管理される
 - Azure AD の [デバイス]、または Azure AD ユーザーの [デバイス] から確認できる

Azure Active Directory admin center

ダッシュボード > エディファストABC > エディファスト... Azure Active Directory

デバイス | すべてのデバイス

名前	有効	OS	バージョン	結合の種類	所有者	MDM	準拠している
Virgo	はい	Windows	10.0.19042.804	Azure AD joined	User1	Microsoft Intune	いいえ
Venus	はい	Windows	10.0.19042.804	Azure AD joined	User2	Microsoft Intune	はい

Intune に登録された Windows 10 デバイス



- Azure AD 参加と同時に Intune に登録されたデバイスは、Microsoft Intune の [デバイス] の [すべてのデバイス] で確認できる

Microsoft Endpoint Manager admin center

ホーム > デバイス

デバイス | すべてのデバイス ...

検索 (Ctrl+/) | 最新の情報に更新 | フィルター | 列 | Export | デバイスの一括操作

IMEI、シリアル番号、メール、ユーザープリンシパル名、デバイス名、管理名、電話番号、モデル、製造元で検索してください

Showing 1 to 2 of 2 records

デバイス名 ↑↓	管理者 ↑↓	所有権 ↑↓	対応 ↑↓	OS	OS のバージョン ↑↓	最後のチェックイン ↑↓
Venus	Intune	企業	✔️ 準拠している	Windows	10.0.19042.804	2021/3/7 午後10:08:33
Virgo	Intune	企業	❌ 準拠していない	Windows	10.0.19042.804	2021/3/7 午後10:14:34

Windows 10 デバイスへのポリシーの適用

- 自動同期 …… 登録 30 分後まで 3 分ごと、その後 8 時間ごと（自動）
- 手動同期 …… Windows 10 の [設定] – [アカウント] – [職場または学校にアクセスする] で、Azure AD への接続の [情報] をクリックし、[同期] をクリック（ユーザー操作）



The screenshot shows the Windows 10 Settings app. The 'アカウント' (Accounts) section is highlighted with a red box. Within it, '職場または学校にアクセスする' (Access your workplace or school) is also highlighted with a red box. A red arrow points from the 'アカウント' section to this option. Below this, the '職場または学校にアクセスする' screen is shown, with the '接続' (Connect) button highlighted. A purple arrow points from the '接続' button to the '接続情報' (Connection information) screen. On this screen, the '同期' (Sync) button is highlighted with a purple box. A purple speech bubble points to the '同期' button with the text 'Intune からポリシーなどを同期' (Sync policies, etc. from Intune).

設定

ホーム

設定の検索

システム
ディスプレイ、サウンド、通知、電源

ネットワークとインターネット
Wi-Fi、機内モード、VPN

アカウント
アカウント、メール、同期、職場または学校にアクセスするのユーザー

簡単操作
レター、拡大鏡、ハイコントラスト

職場または学校にアクセスする

接続

エディファイトABC の Azure AD に接続済み
user2@edifistabc.net によって接続済み
アカウントの管理

情報 切断

同期

接続情報

管理サーバーのアドレス:
https://r.manage.microsoft.com/devicegatewayproxy/cimhandler.ashx
Exchange ID:
E0692485EBAAA468DDB3BCFA42C14D24

デバイスの同期状態

同期は、セキュリティ ポリシー、ネットワーク ポリシー、管理対象アプリケーションを最新の状態に保ちます。
前回試行した同期:
正しく同期されました
2021/03/07 22:08:32

Intune から
ポリシーなどを同期



Azure AD
参加

+

Intune への
デバイス登録

デバイスが、Azure AD と Intune の
両方に登録されることにより、

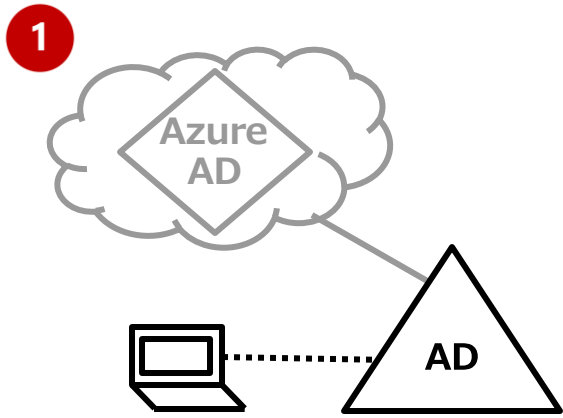
次の構成が可能になります。

- 1 デバイス ベースの条件付きアクセス
- 2 Windows Hello for Business
による認証の強化

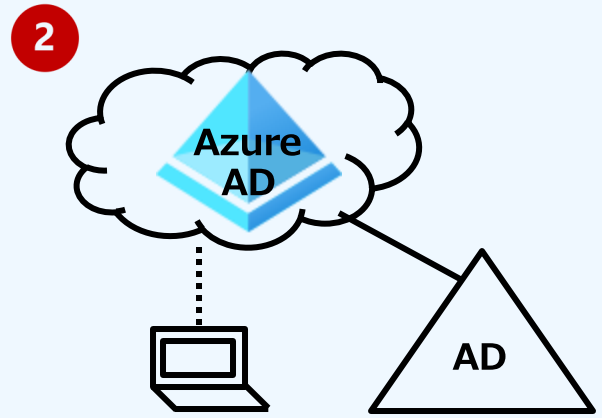
1 デバイス ベースの条件付きアクセス

デバイス ベースの
条件付きアクセスを
サポートする構成

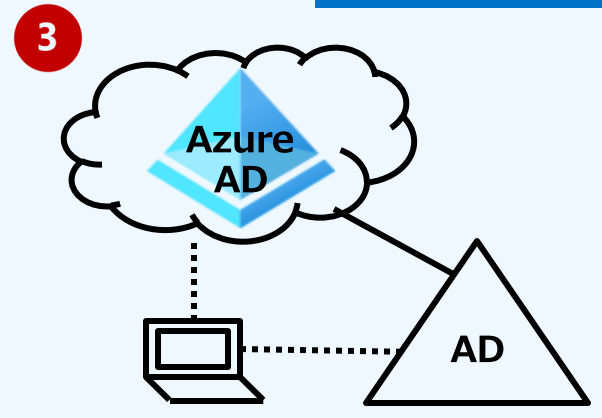
会社所有のデバイス



- ・ドメイン参加
- ・ConfigMgr 管理

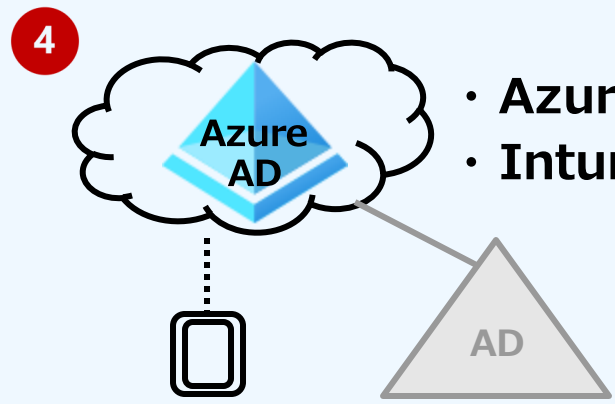


- ・ Azure AD 参加
- ・ Intune 管理



- ・ ハイブリッド Azure AD 参加
- ・ ConfigMgr と Intune の
共同管理

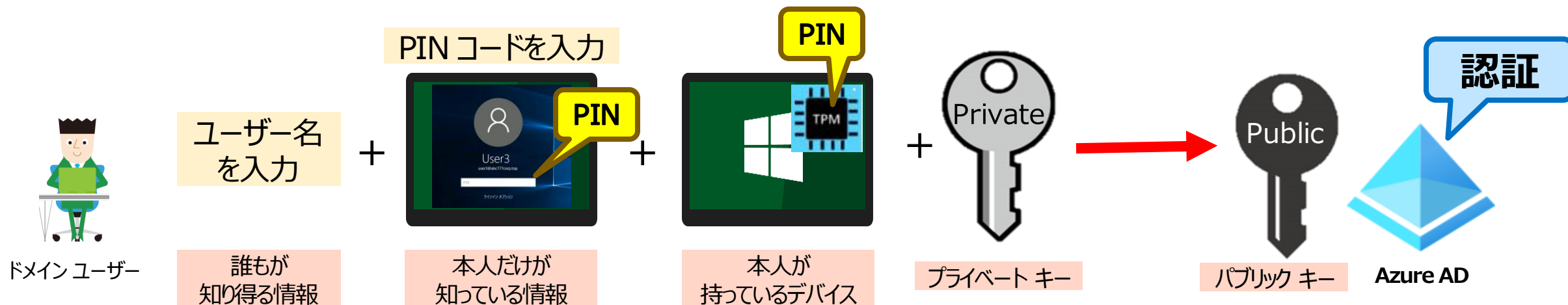
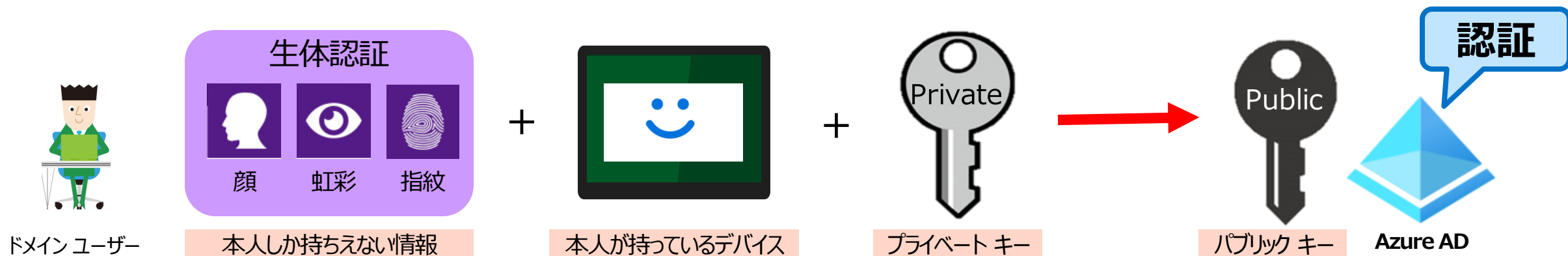
ユーザー所有の
デバイス



- ・ Azure AD 登録
- ・ Intune 管理

2 Windows Hello for Business による認証の強化

- 生体（または PIN）および キー ペア を使用する、Windows 10 の認証機能
 - パスワードを使用しない認証



Windows Hello for Business の有効化と構成 (1)

- Microsoft Intune の [デバイス] - [Windows 登録] の [Windows Hello for Business] で構成する

The screenshot shows the Microsoft Endpoint Manager admin center interface. The breadcrumb navigation is 'ホーム > デバイス > Windows'. The left sidebar has 'デバイス | Wi...' selected. The main content area shows 'Windows | Windows 登録' with a search bar. Below the search bar, 'Windows のデバイス' and 'Windows 登録' are listed, with 'Windows 登録' highlighted in a red box. A callout bubble points to this box with the text 'テナントに対する適用'. In the main content area, the 'Windows Hello for Business' tile is highlighted in a red box. The tile text reads: 'Windows Hello for Business パスワードを強力な 2 要素認証で置き換えます。' A red arrow points from this tile to the configuration window on the right.

The screenshot shows the 'Windows Hello for Business' configuration window. The title is 'Windows Hello for Business' with a close button. The subtitle is 'Windows の登録'. The '基本' section shows '更新日時' as '21/01/08 午後6:23' and '割当先' as 'すべてのユーザー'. Below this, there is a description: 'Windows Hello for Business を設定すると、ユーザーが生体認証などのジェスチャまたは PIN を使ってデバイスにアクセスできるようになります。詳細をご覧ください。' and another line: 'Windows Hello for Business と Microsoft Intune の統合について'. The '名前' section is set to 'All users and all devices'. The '説明' section contains the text: 'This is the default Windows Hello for Business configuration applied with the lowest priority to all users regardless of group membership.' The 'Windows Hello for Business の構成' section has a dropdown menu set to '有効'. The 'トラステッド プラットフォーム モジュール (TPM) を使用する' section has radio buttons for '必須' and '優先', with '優先' selected. The 'PIN の長さの最小値' is set to '6', 'PIN の長さの最大値' is '127', 'PIN での小文字の使用' is '許可しない', 'PIN での大文字の使用' is '許可しない', 'PIN での特殊文字の使用' is '許可しない', and 'PIN の有効期間 (日)' is 'しない'. At the bottom, there are '保存' and '破棄' buttons.

「Windows Hello for Business」

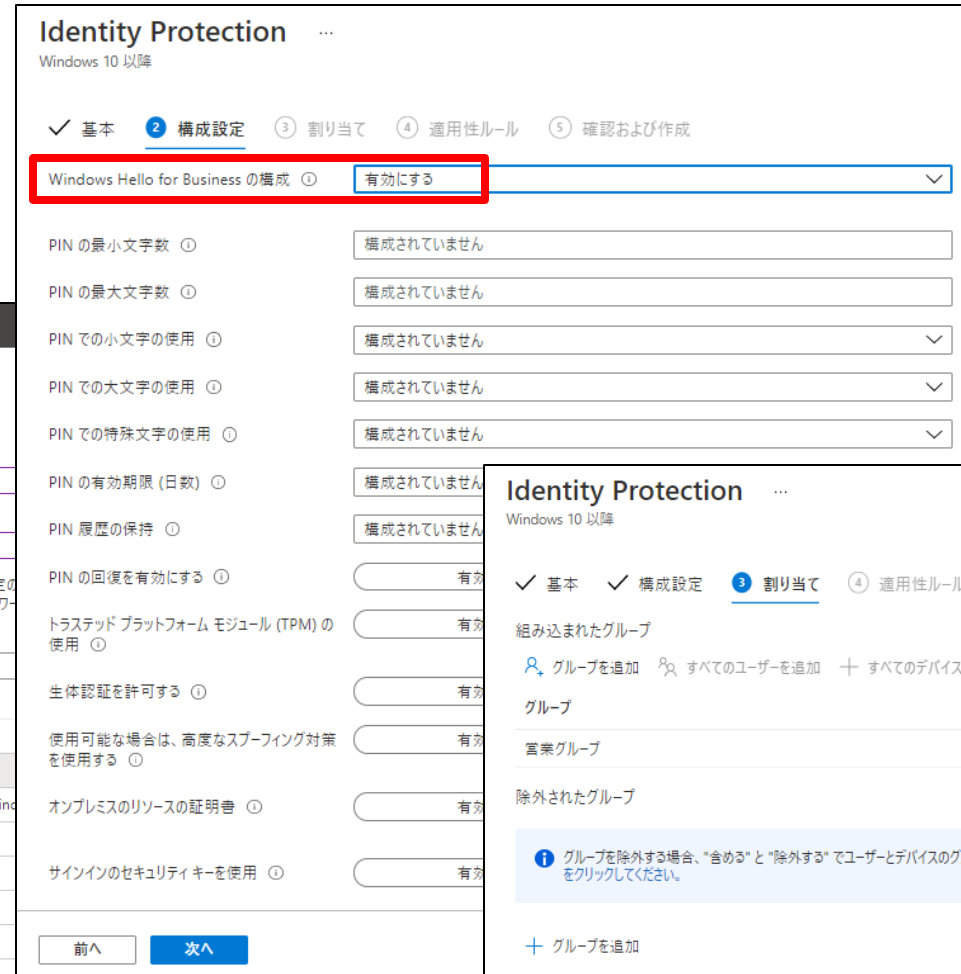
<https://docs.microsoft.com/ja-jp/windows/security/identity-protection/hello-for-business/hello-overview>

「Windows Hello for Business と Microsoft Intune の統合」

<https://docs.microsoft.com/ja-jp/mem/intune/protect/windows-hello>

Windows Hello for Business の有効化と構成 (2)

- Microsoft Intune の [デバイス] – [構成プロファイル] の作成で、「Windows 10 以降」プラットフォームの「Identity Protection」テンプレートを選択

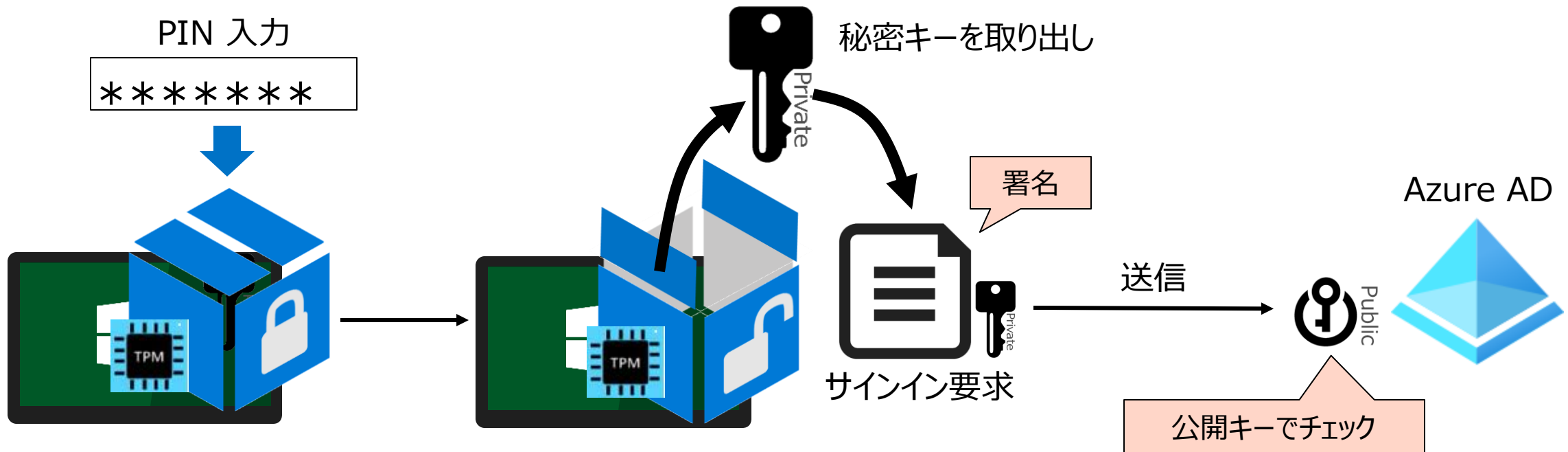


一部のグループにのみ適用できる



[参考] Windows Hello for Business のサインイン要求

- Windows Hello for Business では、PIN を入力して、デバイスに保存されている秘密キーを取り出し、その秘密キーで署名したサインイン要求を、Azure AD に送る
 - PIN やパスワードは送信しない

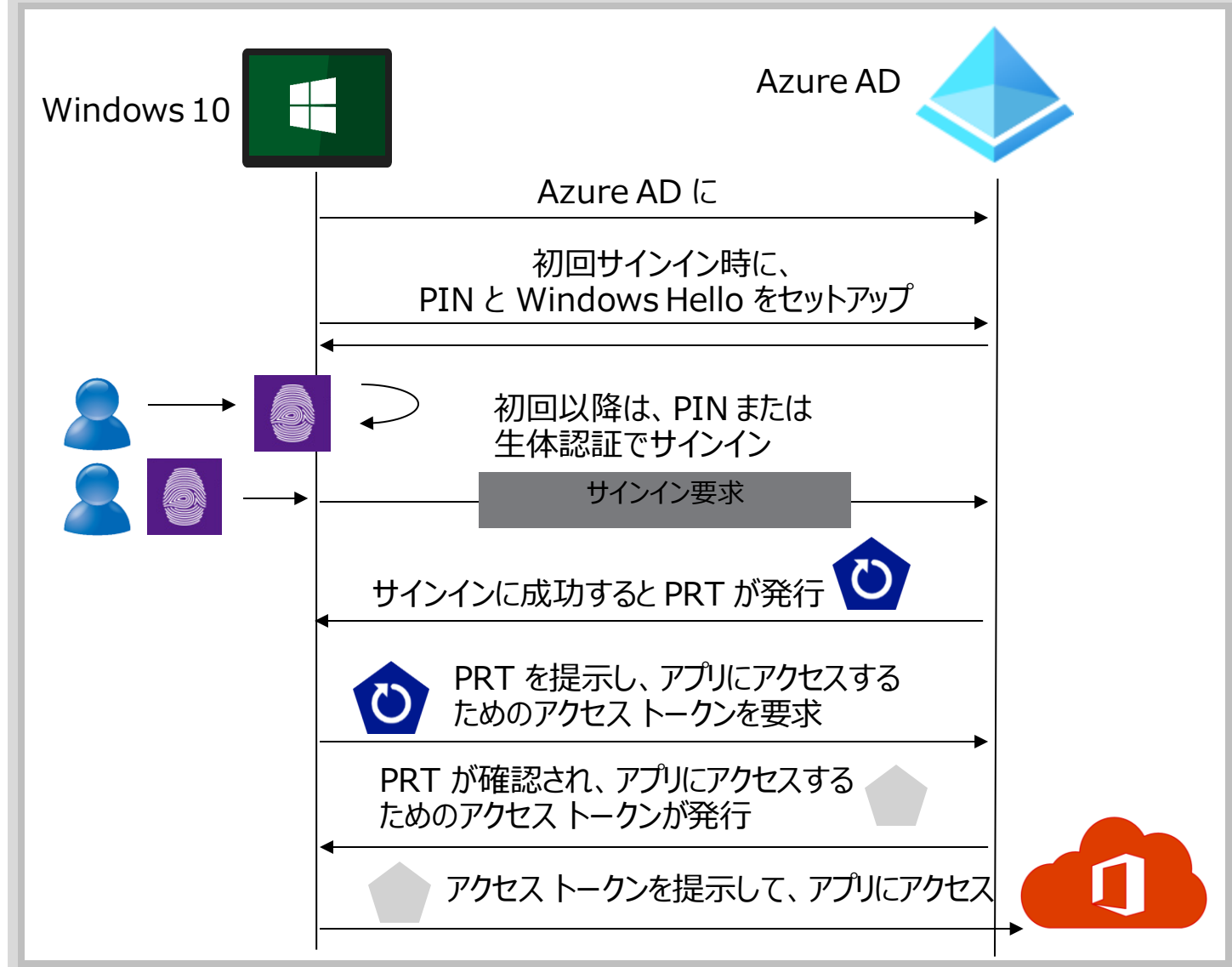


[参考] Windows Hello for Business の認証/認可フロー

- Azure AD へのサインインに成功すると、Primary Refresh Token (PRT) が発行される
- Azure AD に PRT を提示して、アプリケーションにアクセスするためのアクセストークンを発行してもらう
- アプリケーションにアクセストークンを提示して、アプリケーションにアクセスする

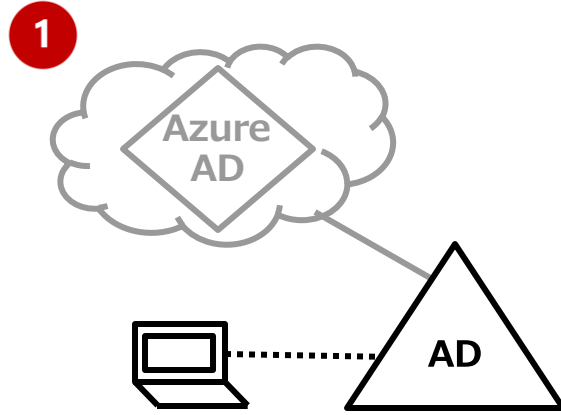
「Microsoft Intune がインストールされた Windows 10 デバイス上で Windows Hello for Business を使用する」

<https://docs.microsoft.com/ja-jp/mem/intune/protect/identity-protection-configure>

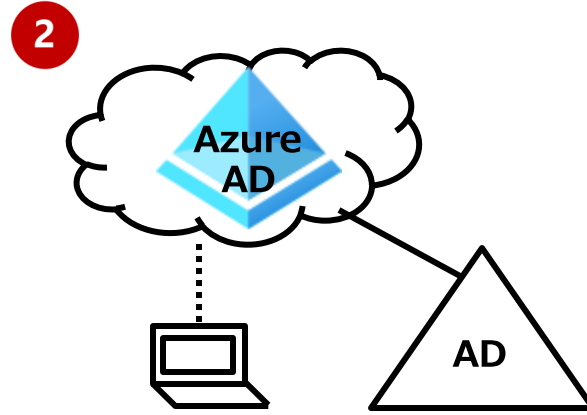


3. ハイブリッド Azure AD 参加

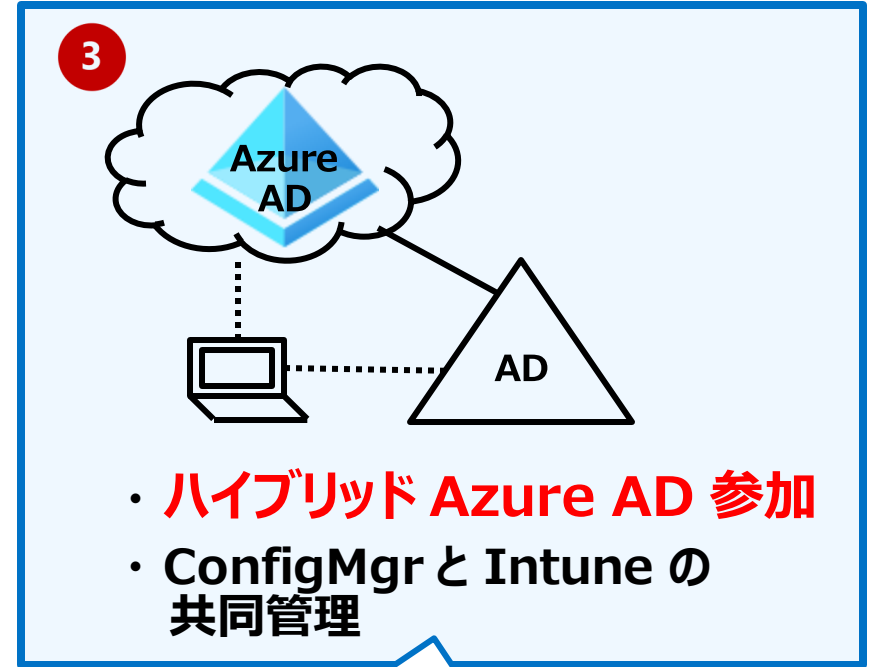
会社所有のデバイス



- ・ドメイン参加
- ・ConfigMgr 管理

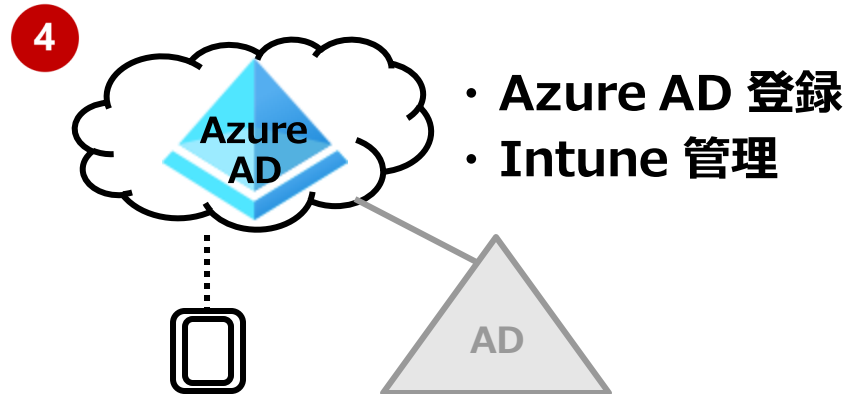


- ・ Azure AD 参加
- ・ Intune 管理



- ・ **ハイブリッド Azure AD 参加**
- ・ ConfigMgr と Intune の 共同管理

ユーザー所有のデバイス



- ・ Azure AD 登録
- ・ Intune 管理

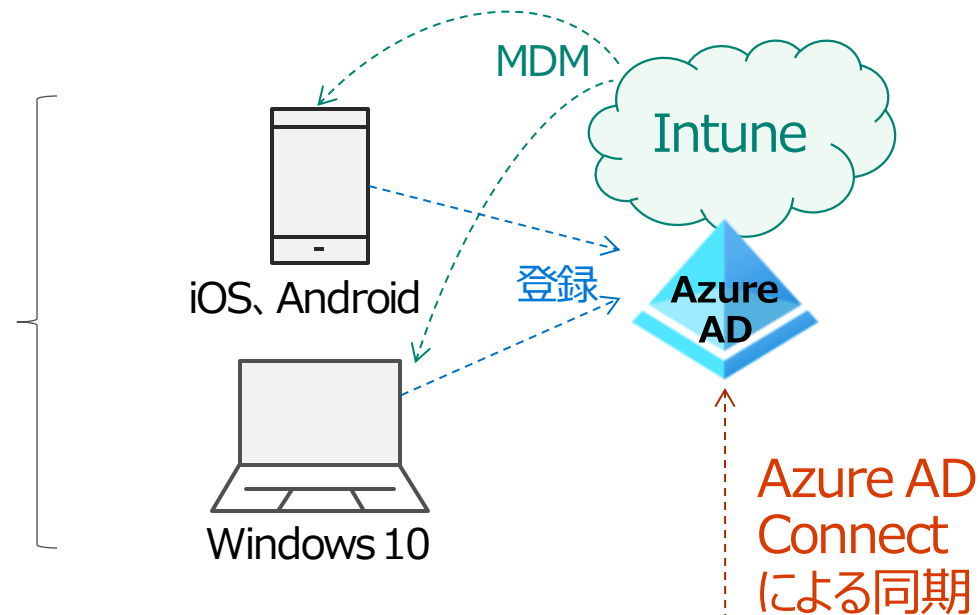
“ハイブリッド Azure AD 参加”
は、オンプレミスのドメインに参加しているデバイスを Azure AD に自動的に登録すること

ユーザーは、オンプレミス ID で PC にサインインする

Intune によるマネージド デバイス

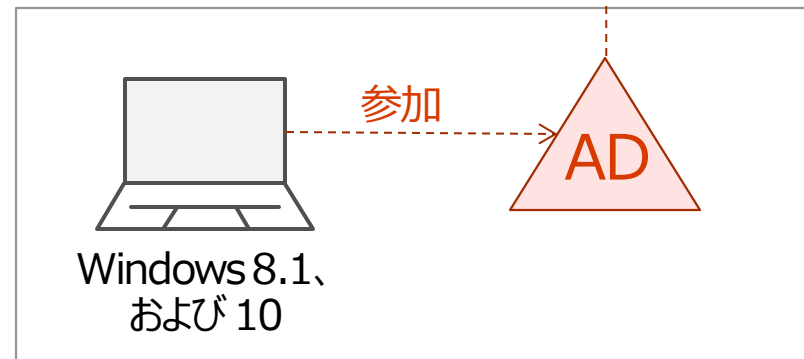
Intune 準拠デバイス

- Azure AD と Intune に登録し、管理されている (MDM)
- Intune のコンプライアンス ポリシーに準拠している



ハイブリッド Azure AD 参加デバイス

- オンプレミス Active Directory に参加している
- Azure AD Connect によって、オンプレミス Active Directory と Azure AD のデバイスが紐づいている



ハイブリッド Azure AD 参加の サポート対象デバイス

- 最新の Windows デバイス (ベスト プラクティス)
 - Windows 10
 - Windows Server 2016 (バージョン 1803 以降)
 - Windows Server 2016
- ダウンレベルの Windows デバイス
 - Windows 8.1
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2

「方法:Hybrid Azure Active Directory 参加の実装を計画する」

<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/hybrid-azuread-join-plan>

オンプレミス Active Directory ドメインの環境

- マネージド環境

- パスワード ハッシュ同期 (PHS) + SSO
- パススルー認証 (PTA) + SSO

「チュートリアル: マネージド ドメイン用のハイブリッド Azure Active Directory 参加の構成」

<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/hybrid-azuread-join-managed-domains>

- フェデレーション環境

- フェデレーションを構成しているドメイン

「チュートリアル: フェデレーション ドメイン用のハイブリッド Azure Active Directory 参加の構成」

<https://docs.microsoft.com/ja-jp/azure/active-directory/devices/hybrid-azuread-join-federated-domains>

ハイブリッド Azure AD 構成の前提条件 1/2

- Azure AD Connect の最新バージョン（1.1.819.0 以降）
- Azure AD テナントの全体管理者の資格情報
- 各フォレストのエンタープライズ管理者の資格情報
- Windows コンピューターが、組織のネットワーク内から次の Microsoft リソースにアクセスできることを確認する
 - Azure AD に Windows コンピューターを登録するために使用する
 - <https://enterpriseregistration.windows.net>
 - <https://login.microsoftonline.com>
 - <https://device.login.microsoftonline.com>
 - SSO 構成の場合に使用する
 - <https://autologon.microsoftazuread-sso.com>

```
C:\Windows\system32\cmd.exe
c:\>nslookup enterpriseregistration.windows.net
Server: UnKnown
Address: ::1

Non-authoritative answer:
Name:      www.tm.prd.adrs.akadns.net
Address:  40.126.13.232
Aliases:  enterpriseregistration.windows.net
          adrs.privatelink.msidentity.com
          prd.adrs.msidentity.com

c:\>nslookup login.microsoftonline.com
Server: UnKnown
Address: ::1

Non-authoritative answer:
Name:      www.tm.a.prd.aadg.akadns.net
Addresses: 40.126.38.18
           20.190.166.130
           40.126.38.65
           20.190.166.129
           20.190.166.66
           40.126.38.16
           40.126.38.23
           20.190.166.65
Aliases:  login.microsoftonline.com
          a.privatelink.msidentity.com
          prda.aadg.msidentity.com

c:\>nslookup device.login.microsoftonline.com
Server: UnKnown
Address: ::1

Non-authoritative answer:
Name:      www.tm.a.prd.aadg.akadns.net
Addresses: 20.190.166.130
           40.126.38.65
           20.190.166.129
           20.190.166.66
           40.126.38.16
           40.126.38.23
           20.190.166.65
           40.126.38.18
Aliases:  device.login.microsoftonline.com
          a.privatelink.msidentity.com
          prda.aadg.msidentity.com
```

ハイブリッド Azure AD 構成の前提条件 2/2

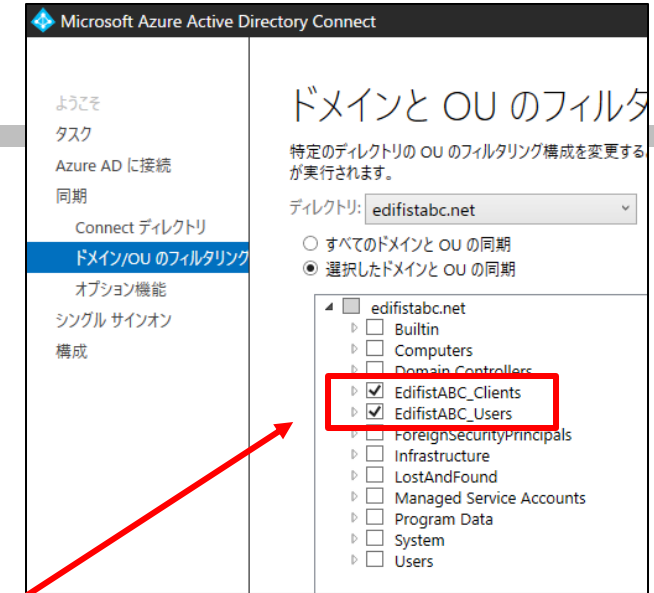
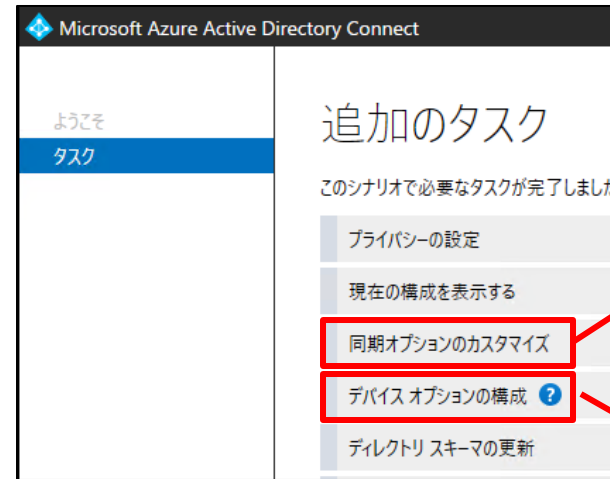
- Windows コンピューターがドメインに参加していること
 - ドメインに参加した Windows コンピューター オブジェクトを、Azure AD Connect によるディレクトリ同期の、対象となる OU に移動しておく（必要に応じて）

The image shows a screenshot of the Active Directory console and a Microsoft Account setup dialog. The console window, titled "Active Directory ユーザーとコンピューター", displays the hierarchy of the domain "edifistabc.net". The "Domain Controllers" folder is expanded, and the "EdifistABC_Clients" folder is highlighted with a red box. A red box also highlights the "PC1" object in the "名前" (Name) column. Below the console, a green diagram shows a triangle labeled "AD" connected by a dashed line to a laptop icon labeled "PC1". To the right, a "Microsoft アカウント" dialog box is shown, titled "職場または学校アカウントのセットアップ". It contains a text box for "電子メールアドレス" and a "次へ" (Next) button. Two options are listed under "別の操作:" (Other actions): "このデバイスを Azure Active Directory に参加させる" (Join this device to Azure Active Directory) and "このデバイスをローカルの Active Directory ドメインに参加させる" (Join this device to the local Active Directory domain). The second option is highlighted with a red box.

ハイブリッド Azure AD 参加の構成

Azure AD Connect 構成ウィザード

- ① [同期オプションのカスタマイズ]
 - Windows コンピュータ オブジェクトの OU を、ディレクトリ同期対象として設定する
- ② [デバイス オプションの構成]
 - [ハイブリッド Azure AD 参加の構成] オプションを構成する



⇒ Active Directory の構成パーティションに、デバイス登録先となる Azure AD テナントを示す SCP オブジェクトが作成される

⇒ Windows コンピューターが、ハイブリッド Azure AD 参加する



① 同期オプションのカスタマイズ

Azure AD Connect 構成ウィザード

The screenshot displays the Microsoft Azure Active Directory Connect wizard. The main window shows the '追加のタスク' (Additional tasks) section with a list of tasks. The '同期オプションのカスタマイズ' (Customize sync options) task is highlighted with a red box. A secondary window titled 'ドメインと OU のフィルタリング' (Domain and OU filtering) is open, showing the 'edifistabc.net' directory selected. Under the 'edifistabc.net' tree, the 'EdifistABC_Clients' OU is checked and highlighted with a red box. A callout bubble points to this selection with the text '同期対象コンピューターオブジェクトの OU を選択' (Select the OU for computer objects to be synchronized). The wizard includes navigation buttons '前へ' (Previous) and '次へ' (Next) at the bottom.

Microsoft Azure Active Directory Connect

ようこそ
タスク

追加のタスク

このシナリオに必要なタスクが完了しました。さらにタスクを実行する

- プライバシーの設定
- 現在の構成を表示する
- 同期オプションのカスタマイズ**
- デバイス オプションの構成 ?
- ディレクトリ スキーマの更新
- ステージング モードの構成
- ユーザー サインインの変更
- フェデレーションの管理 ?
- トラブルシューティング

Microsoft Azure Active Directory Connect

ようこそ
タスク
Azure AD に接続
同期
Connect ディレクトリ
ドメイン/OU のフィルタリング
オプション機能
シングル サインオン
構成

ドメインと OU のフィルタリング

特定のディレクトリの OU のフィルタリング構成を変更すると、次の同期サイクルでは、そのディレクトリで自動的にフル インポートが実行されます。

ディレクトリ:

すべてのドメインと OU の同期
 選択したドメインと OU の同期

- edifistabc.net
 - BuiltIn
 - Computers
 - Domain Controllers
 - EdifistABC_Clients
 - EdifistABC_Users
 - ForeignSecurityPrincipals
 - Infrastructure
 - LostAndFound
 - Managed Service Accounts
 - Program Data
 - System
 - Users

同期対象コンピューターオブジェクトの OU を選択

前へ 次へ

前へ 次へ

② デバイス オプションの構成

Azure AD Connect 構成ウィザード

The image shows two overlapping windows from the Microsoft Azure Active Directory Connect wizard. The background window is titled '追加のタスク' (Additional Tasks) and lists various configuration steps. The foreground window is titled 'デバイス オプション' (Device Options) and allows the user to select a device option for synchronization.

追加のタスク (Additional Tasks)

- ようこそ
- タスク
- プライバシーの設定
- 現在の構成を表示する
- 同期オプションのカスタマイズ
- デバイス オプションの構成 ?**
- ディレクトリスキーマの更新
- ステージング モードの構成
- ユーザー サインインの変更
- フェデレーションの管理 ?
- トラブルシューティング

デバイス オプション (Device Options)

構成するデバイス オプションを選択します。

- ハイブリッド Azure AD 参加の構成
- デバイス ライトバックの構成
- デバイス ライトバックの無効化

Navigation buttons: 前へ (Previous), 次へ (Next)

(続き)

The screenshot displays two overlapping windows from the Microsoft Azure Active Directory Connect console. The background window is on the 'デバイスのオペレーティング システム' (Device Operating System) page, and the foreground window is on the 'SCP の構成' (SCP Configuration) page.

Background Window: デバイスのオペレーティング システム

- Left sidebar: ようこそ, タスク, 概要, Azure AD に接続, デバイス オプション, ハイブリッド Azure AD 参加, **デバイス システム**, SCP, 構成
- Main content: **デバイスのオペレーティング システム**
Active Directory 環境内のデバイスで使用されているオペレーティング システムを選択します。
 Windows 10 以降のドメインに参加しているデバイス。 ?
 サポートされている Windows ダウンレベルドメインに参加しているデバイス

Foreground Window: SCP の構成

- Left sidebar: ようこそ, タスク, 概要, Azure AD に接続, デバイス オプション, ハイブリッド Azure AD 参加, **デバイス システム**, **SCP**, 構成
- Main content: **SCP の構成**
Azure AD テナントの情報を検出するためにデバイスでサービス接続ポイント (SCP) が使用されています。デバイスが別のフォレストにある場合、各フォレストに SCP が必要です。Azure AD Connect は SCP を構成することができ、SCP を構成するスクリプトを提供することもできます。
Azure AD Connect で SCP を構成するフォレストを選択します。 ?

フォレスト ?	認証サービス ?	エンタープライズ管理者 ?	
<input checked="" type="checkbox"/> edifistabc.net	Azure Active Directory	EDIFISTABC¥admin	編集

フォレストのエンタープライズ管理者の資格情報をお持ちでない場合は、この PowerShell スクリプトをダウンロードして SCP をオフラインで構成することもできます。 ?
ConfigureSCPps1 のダウンロード

Navigation buttons at the bottom: 前 (Previous), 次へ (Next)

ハイブリッド Azure AD 参加した Windows 10

- Azure AD の [デバイス] – [すべてのデバイス] で確認

Azure Active Directory admin center

ダッシュボード > エディファストABC > エディファスト... > デバイス | すべてのデバイス

すべてのデバイス

このページには、評価に使用できるプレビューが含まれています。プレビューを表示する →

アクティビティ タイムスタンプを使用して、環境内の古いデバイスを効率的に管理できます。詳細情報

名前、デバイス ID、またはオブジェクト ID で検...

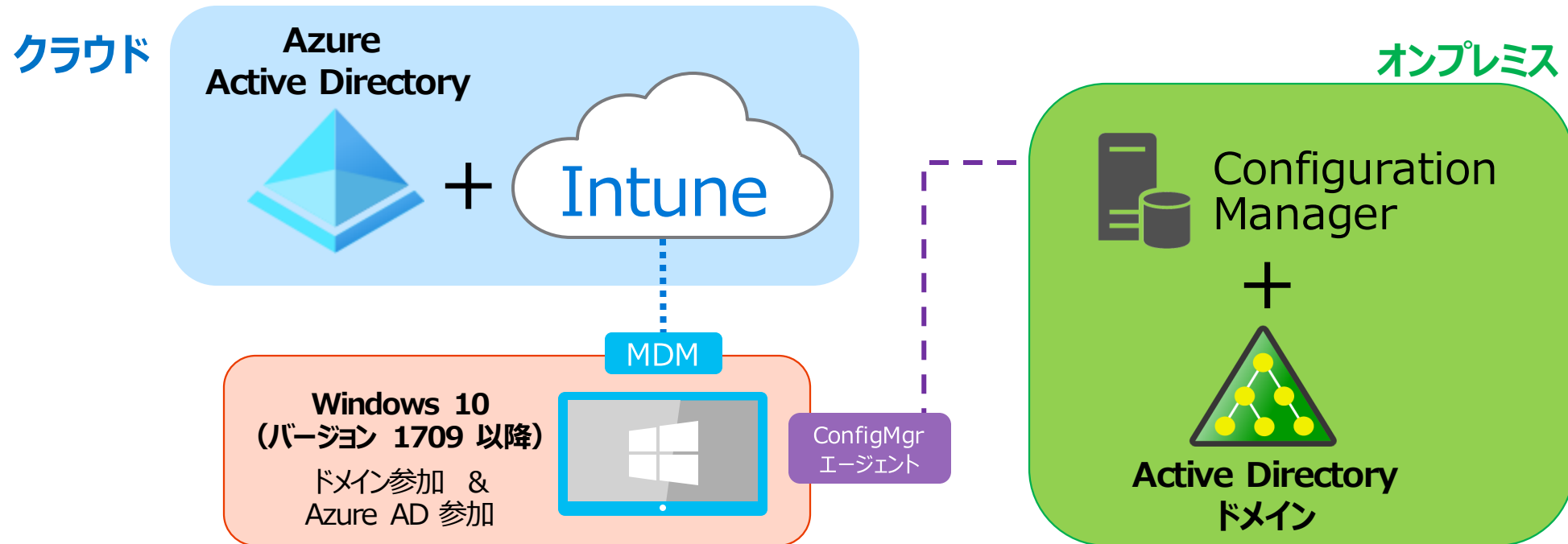
名前	有効	OS	バージョン	結合の種類
Virgo	はい	Windows	10.0.19042.804	Azure AD joined
PC1	はい	Windows	10.0.17763.0	Hybrid Azure AD joined
Venus	はい	Windows	10.0.19042.804	Azure AD joined

「ハイブリッド Azure AD 参加の構成後のタスク」

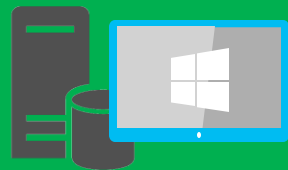
<https://docs.microsoft.com/ja-jp/azure/active-directory/hybrid/how-to-connect-fed-hybrid-azure-ad-join-post-config-tasks>

4. 共同管理 (Co-Management)

- Windows 10 デバイスを、「Microsoft Endpoint Configuration Manager (MECM)」と「Intune」の両方で管理すること
- “共同管理” は、Intune 移行への “最初のステップ”



「従来の管理」と「最新の管理」の特徴



従来の管理

シングル デバイス

会社所有のデバイス

組織ネットワーク& レガシー アプリ

手動管理

リアクティブ
(事が起こってから、行動する)

管理者による管理



最新の管理

マルチ デバイス

ユーザー所有/会社所有のデバイス

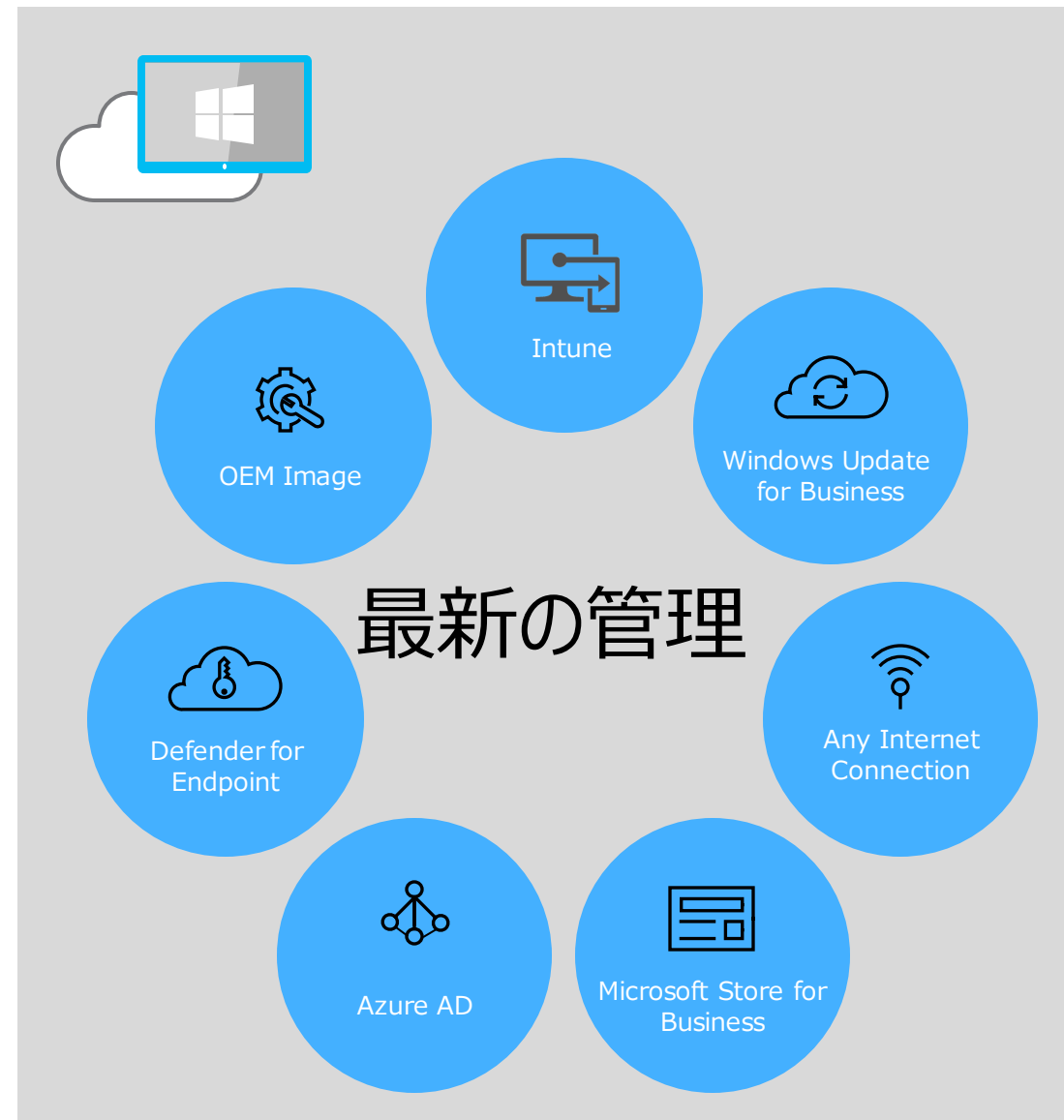
クラウド ベースの管理 & SaaS アプリ

自動管理

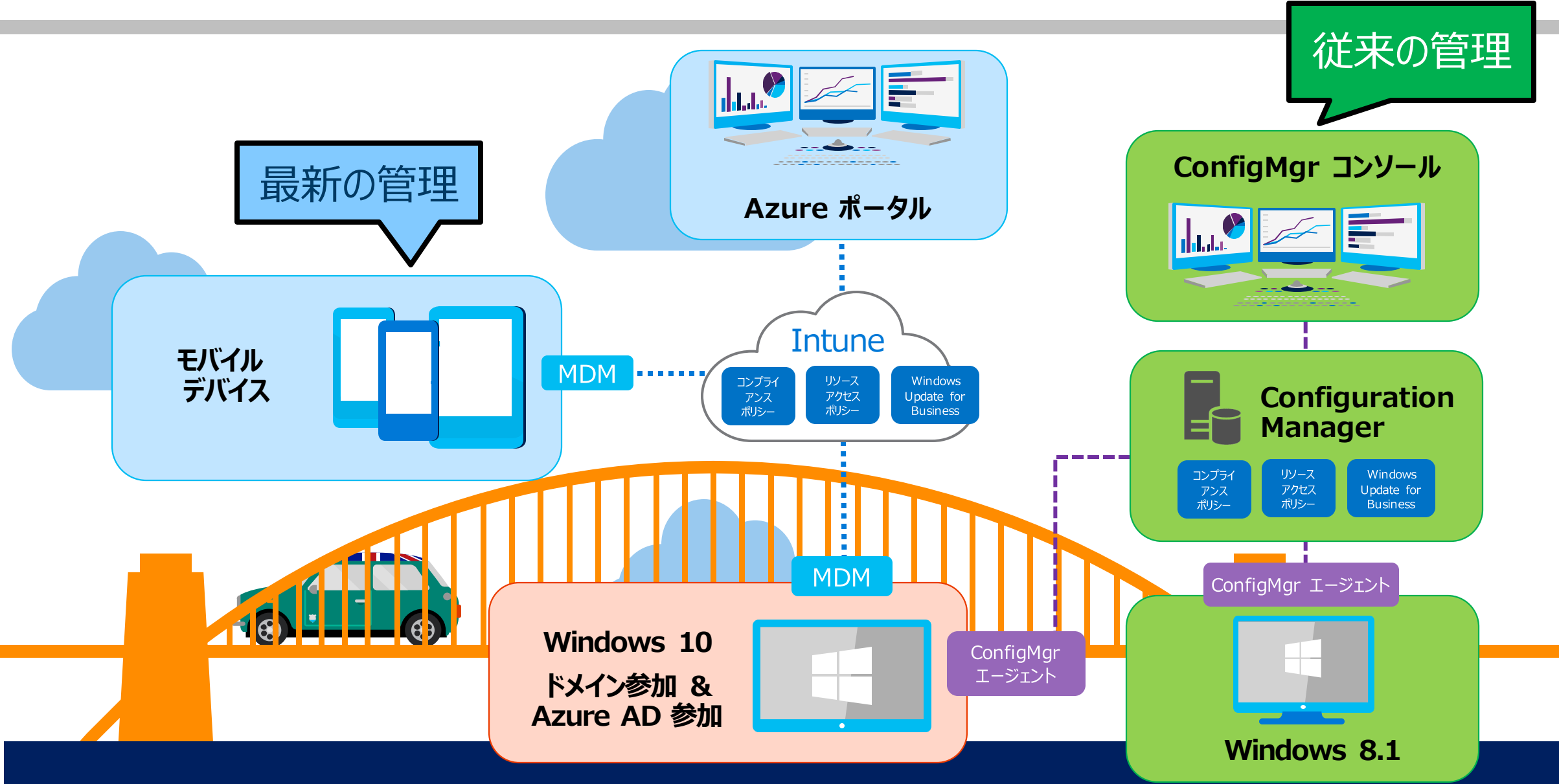
プロアクティブ
(先を見越して、事前に行動する)

セルフ サービス

「従来の管理」と「最新の管理」の要素



“共同管理”は、「従来の管理」から「最新の管理」への“橋渡し”



“共同管理”の2つのパス (パス 1)

- パス 1 : 既存の Configuration Manager クライアントを Intune に自動登録



- ハイブリッド Azure AD 参加の構成が必要
 - パスワード ハッシュ同期 + SSO
 - パススルー認証 + SSO
 - AD FS によるフェデレーション SSO

「共同管理へのパス」

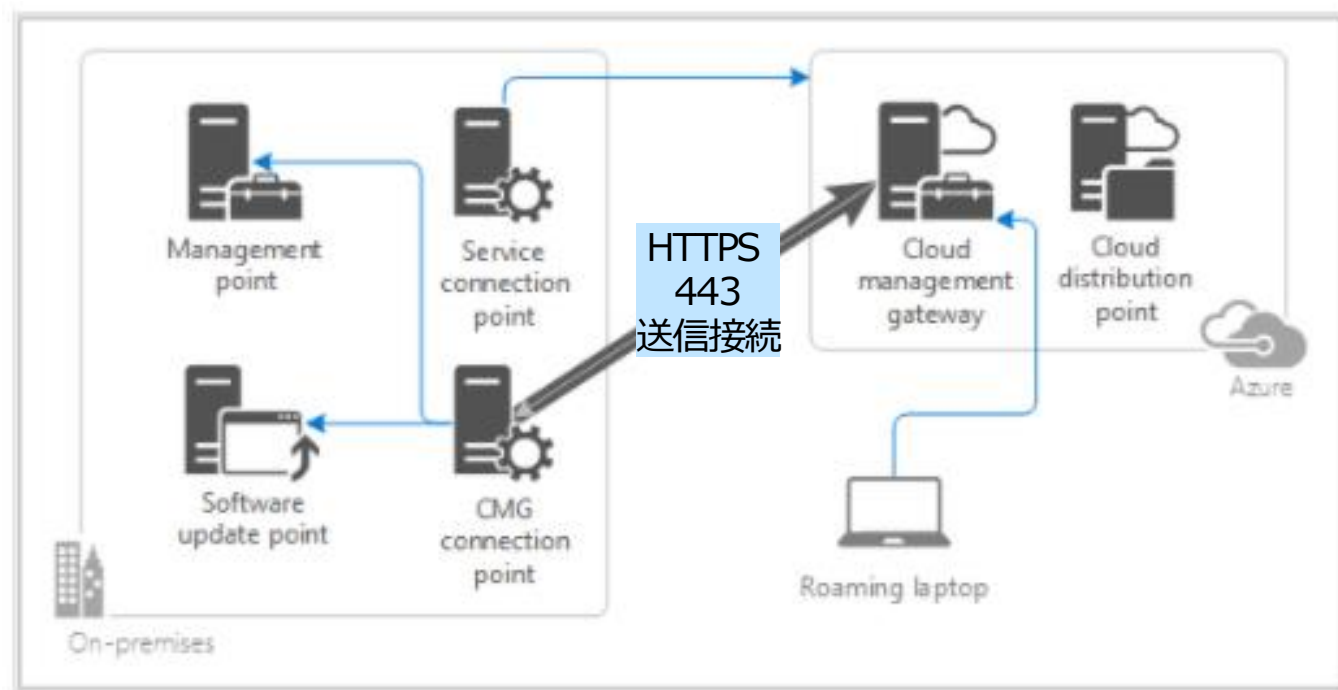
<https://docs.microsoft.com/ja-jp/mem/configmgr/comanage/quickstart-paths>

「チュートリアル: 既存の Configuration Manager クライアントの共同管理を有効にする」

<https://docs.microsoft.com/ja-jp/mem/configmgr/comanage/tutorial-co-manage-clients>

“共同管理”の2つのパス (パス2)

- パス2: Microsoft Endpoint Configuration Manager (MECM) のクラウド管理ゲートウェイ (CMG) による管理
 - MECM から Azure に CMG クラウド サービスを展開し、インターネットから共同管理を行える
 - ハイブリッド Azure AD 参加の構成不要



「チュートリアル:新しいインターネットベースのデバイスの共同管理を有効にする」

<https://docs.microsoft.com/ja-jp/mem/configmgr/comanage/tutorial-co-manage-new-devices>

「クラウド管理ゲートウェイの概要」より引用

<https://docs.microsoft.com/ja-jp/mem/configmgr/core/clients/manage/cmgs/overview>

最終的に Windows 10 を Microsoft 365 の最先端のセキュリティ機能で保護！

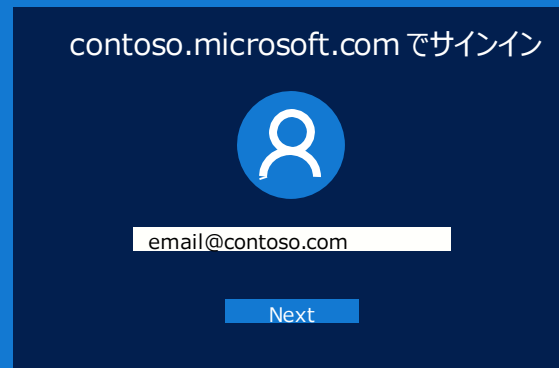
管理およびセキュリティの簡素化

クラウド ベースの管理機能を利用することで、
制御性を保ちながら自社のペースで移行できる



セルフ サービスによる展開

セルフ サービス エクスペリエンスで、
簡単に新しい PC を業務用に設定できる



企業の資格情報でログインすると、
デバイスを自動で構成

Microsoft
クラウド



常に最新バージョンを維持

最新の機能とセキュリティを提供

クラウドの更新なら、
オンプレミスの更新サーバーは
必要ない

更新プログラムの
運用対象と
タイミングを制御
できる

先を見越したインサイト

先を見越したインサイトを入手して、
問題が発生する前に診断して解決できる

クラウド インテリジェンスを
使用して、Windows 10 や
Office 365 ProPlus を適
切にアップグレードできる



© 2021 Microsoft Corporation. All rights reserved.

本情報の内容（添付文書、リンク先などを含む）は、作成日時点でのものであり、予告なく変更される場合があります。