mstep

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

2021.04.08
Ver 4.4m

2-1

2 章：Microsoft Intune

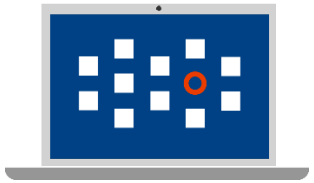
- Intune の概要
- Intune によるモバイル デバイス管理（MDM）
- Intune によるモバイル アプリ管理（MAM）
- Microsoft Defender for Endpoint との統合
- デバイスの登録
- Windows 10 の Azure AD 参加とハイブリッド Azure AD 参加

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)

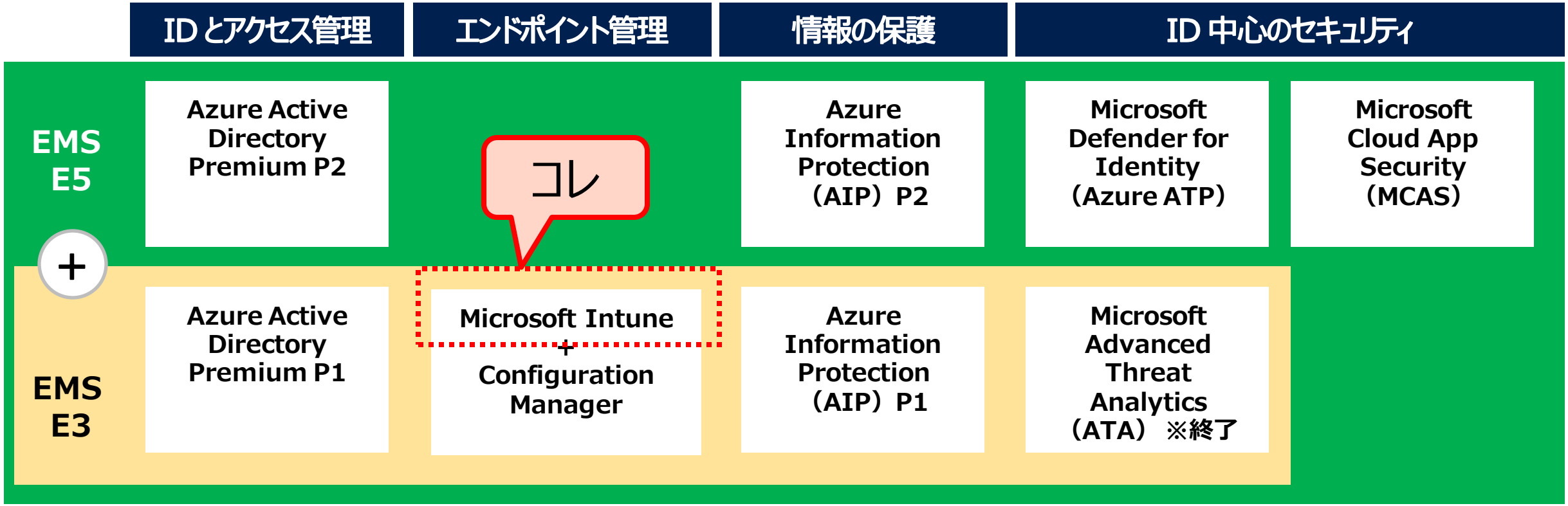
クラウド アプリのセキュリティ

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

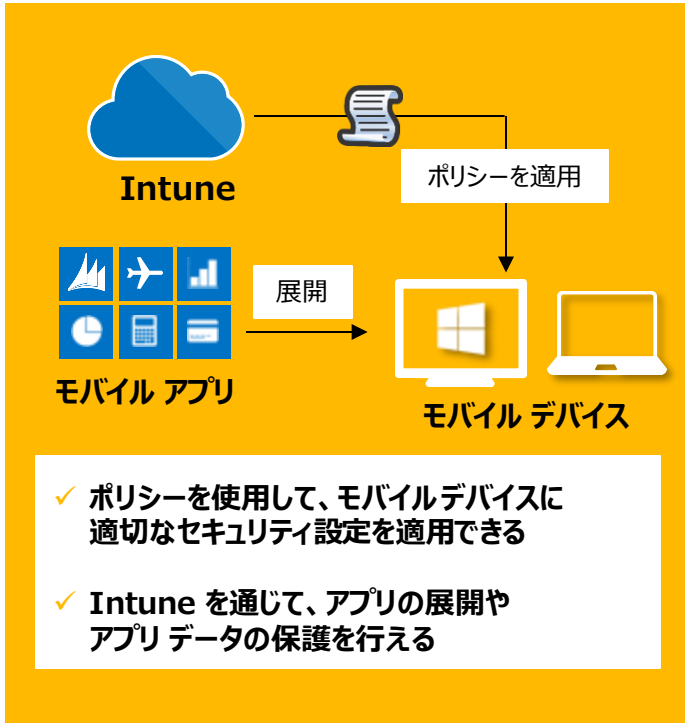


「Enterprise Mobility + Security 価格オプション」
https://www.microsoft.com/ja-jp/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing

Microsoft Intune とは

Microsoft Intune

- 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



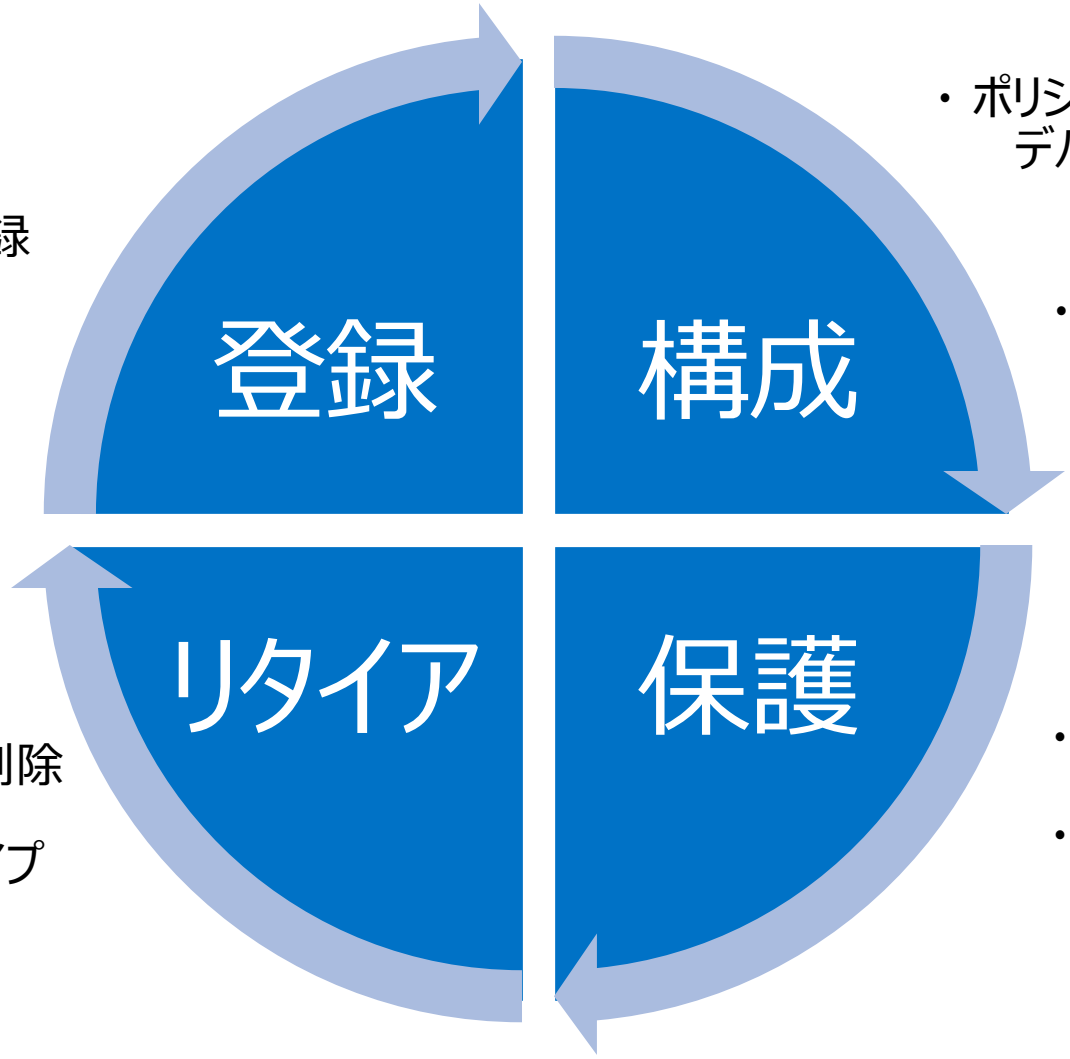
MDM（Mobile Device Management）

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したアクセス制限
- 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



・デバイスを登録

・ポリシー適用による
デバイスの構成

・アプリの展開
※ アプリのライフ サイクル

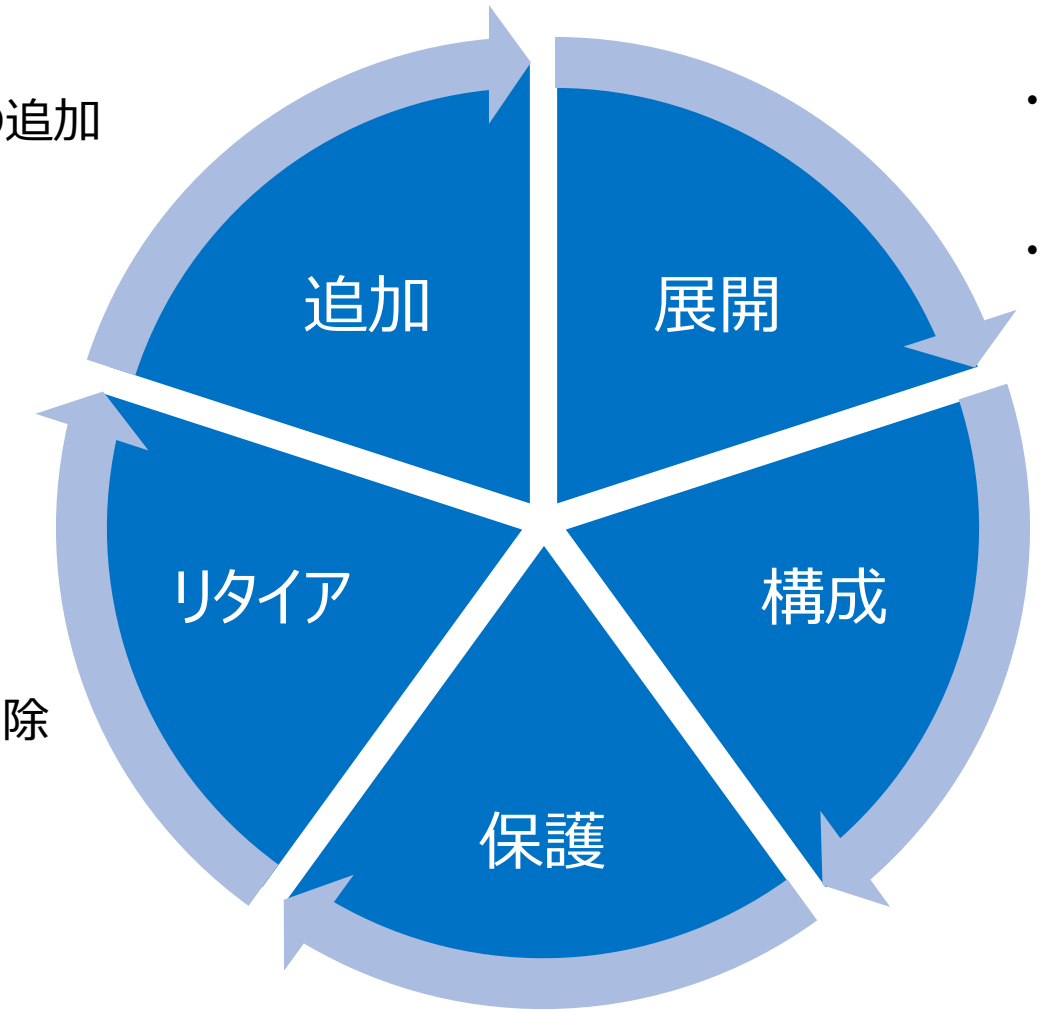
・不正アクセスからの保護

・アクセス制御

・インベントリから削除

・機密データのワイプ

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

・アプリの更新
（新しいバージョンのリリース）

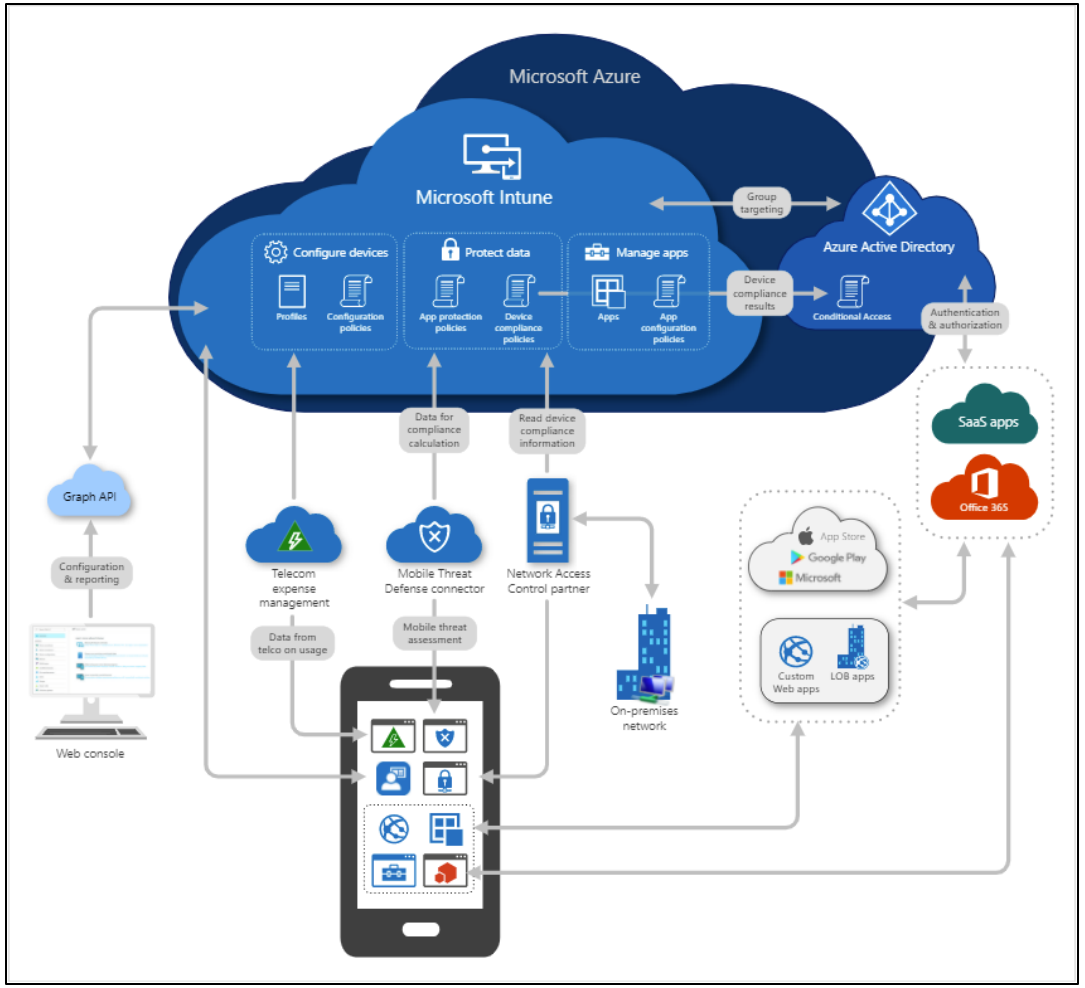
・アプリのデータ保護
  - 条件付きアクセス（アクセス制御）
  - アプリ保護ポリシー（会社データ保護）

・インベントリから削除

・アン インストール

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

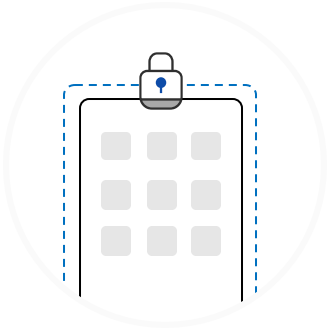


「**Microsoft Intune の概要**」より引用
https://docs.microsoft.com/ja-jp/mem/intune/fundamentals/what-is-intune

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

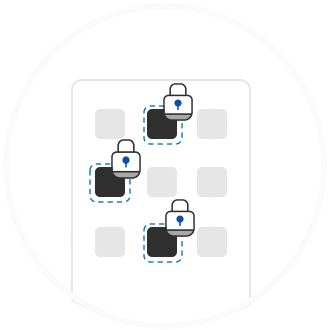
構成、証明書、
プロファイルの
プロビジョニング

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



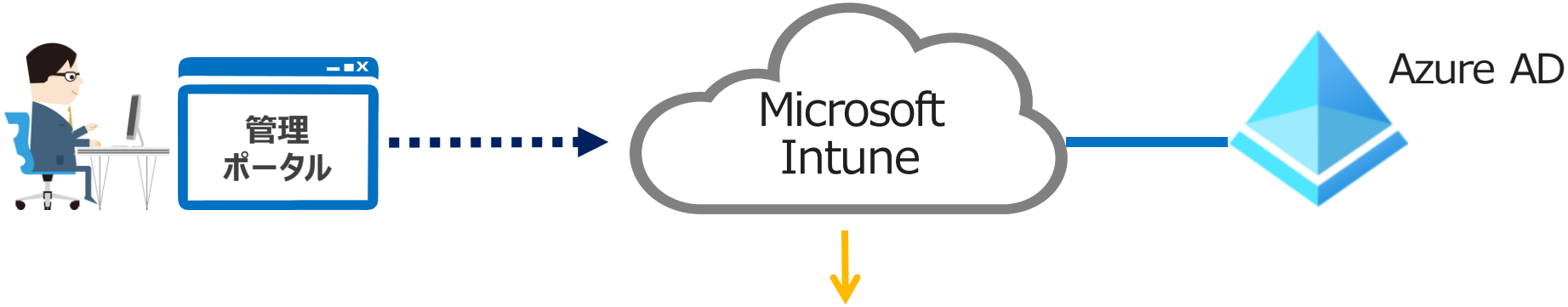
ユーザー向けの
モバイル アプリの展開

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

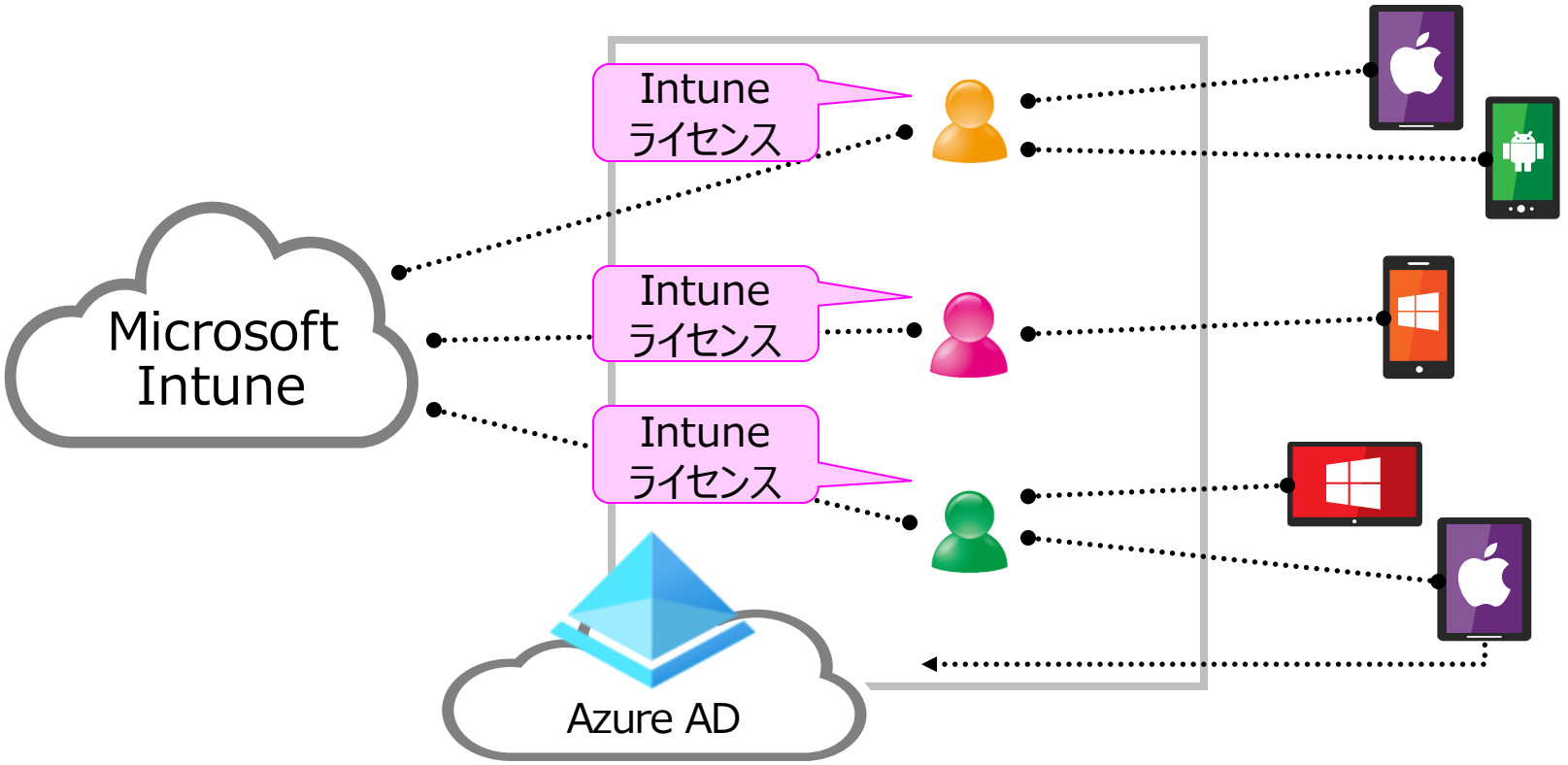
Google
- Android 5.0 以降
- Android エンタープライズ

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 登録できる
デバイス数

1 ユーザーあたり
既定 5 台
（最大 15 台）

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 機関の設定（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

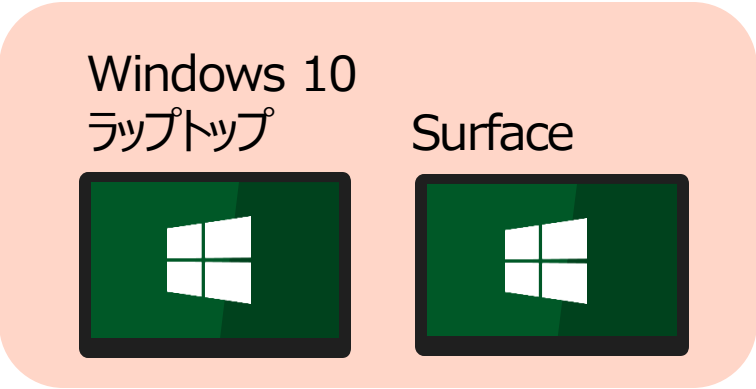
2-2

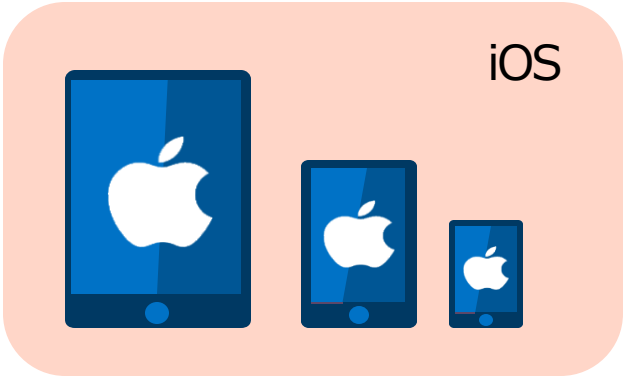
2 章：Microsoft Intune

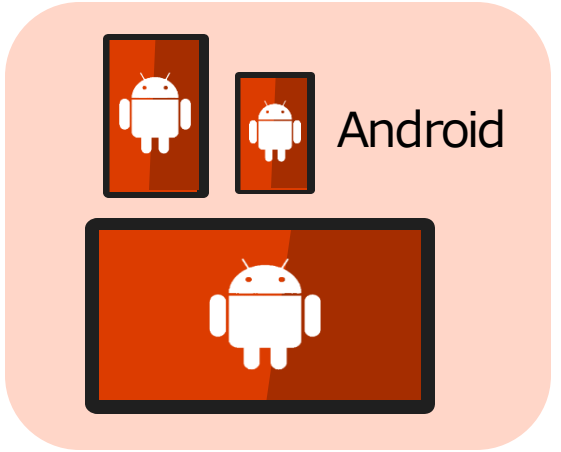
- Intune の概要
- Intune によるモバイル デバイス管理（MDM）
- Intune によるモバイル アプリ管理（MAM）
- Microsoft Defender for Endpoint との統合
- デバイスの登録
- Windows 10 の Azure AD 参加とハイブリッド Azure AD 参加

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



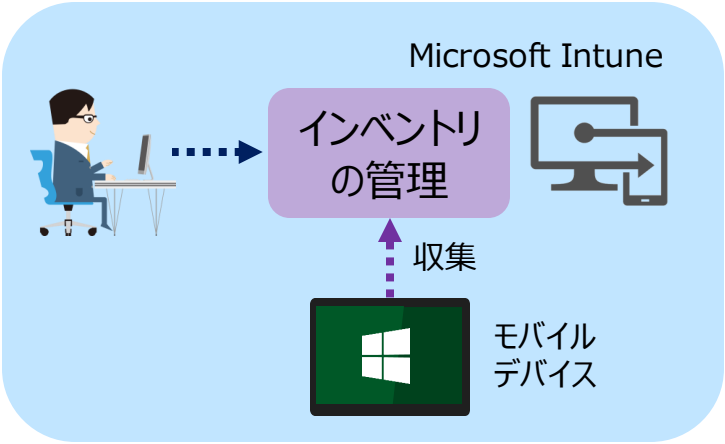


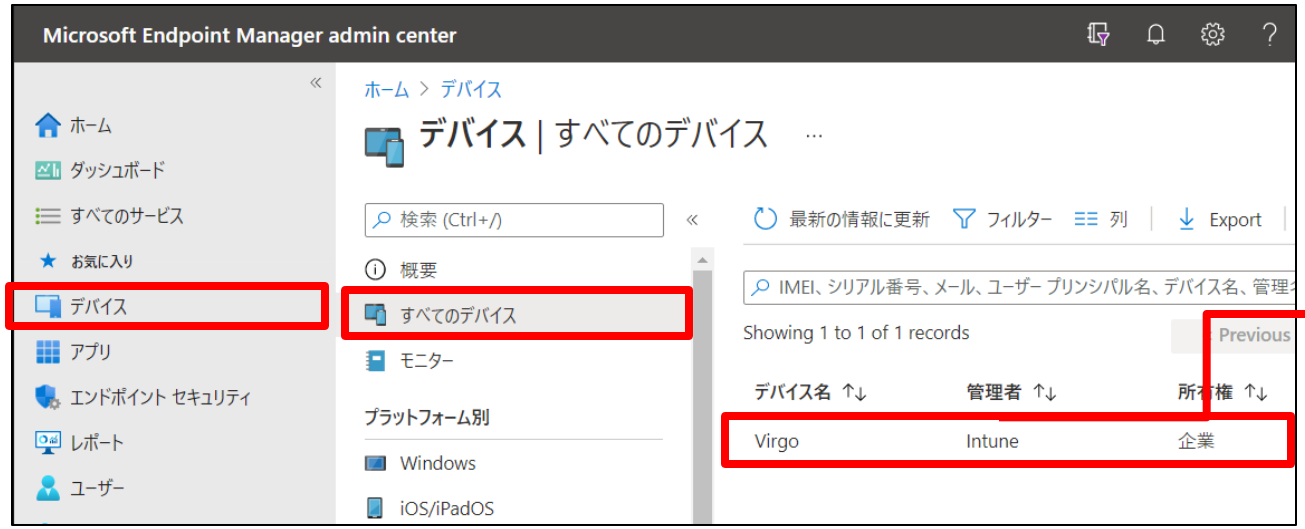


「Microsoft Intune デバイスの管理とは」
https://docs.microsoft.com/ja-jp/mem/intune/remote-actions/device-management

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ーで、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）

[応用] 会社所有デバイスの事前登録

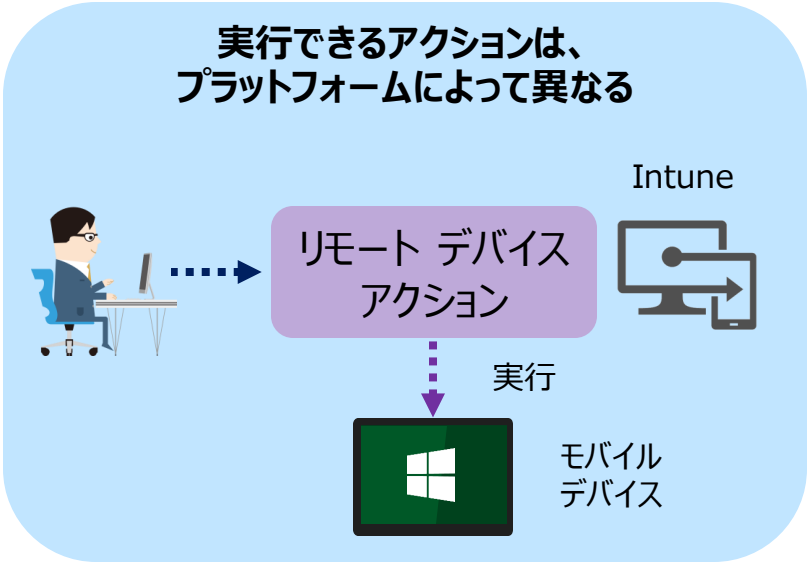
- 企業所有のデバイスのみを登録させるには、企業所有デバイスの ID（IMEI 番号、シリアル番号）の事前登録が必要

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

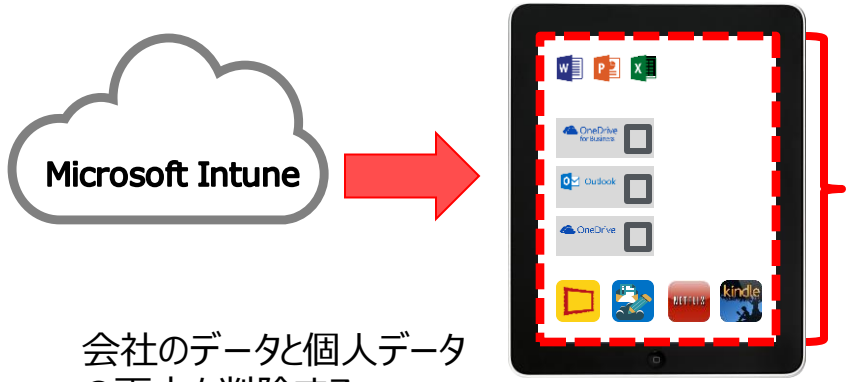
「Microsoft Intune デバイスの管理とは」の「行えるデバイス アクション」
https://docs.microsoft.com/ja-jp/mem/intune/remote-actions/device-management#available-device-actions

例）デバイス紛失時の対応

リモート ロック

ロック画面に移行し、
第三者に利用されることを防止

出荷時の設定（ワイプ）



会社のデータと個人データ
の両方を削除する

デバイス内の
すべてのアプリと
データを削除

パスコードのリセット

パスコードを変更することで、第三者に
パスコードを知られた場合にアクセスできなくする

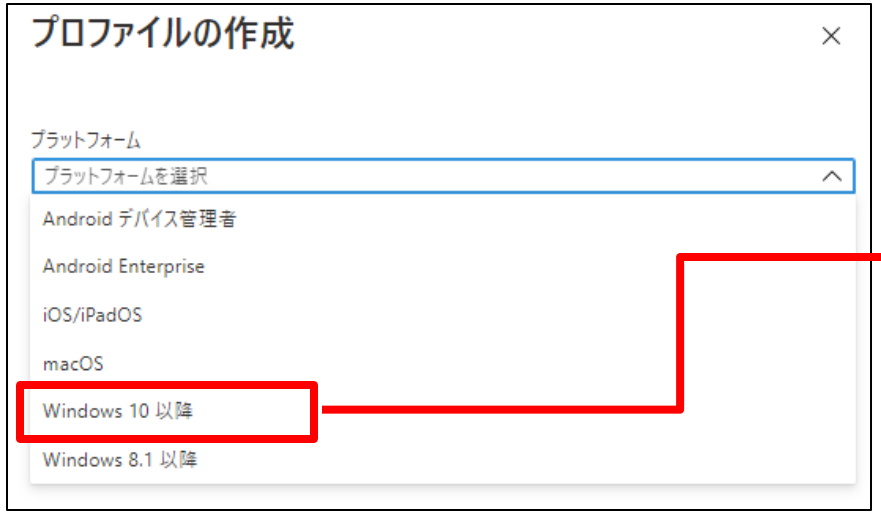
iOS/iPad デバイスの検索

紛失したまたは盗まれた
iOS デバイスの場所をマップに表示

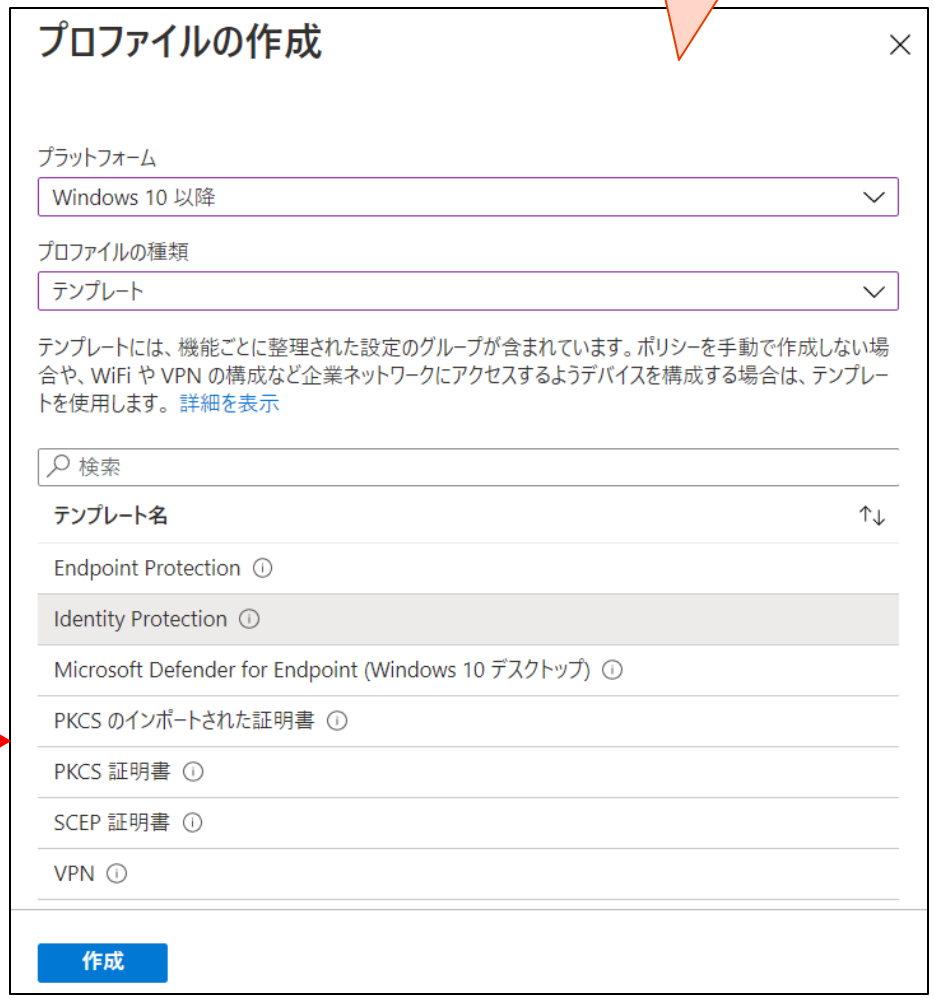
3. デバイスの構成と管理

- **“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

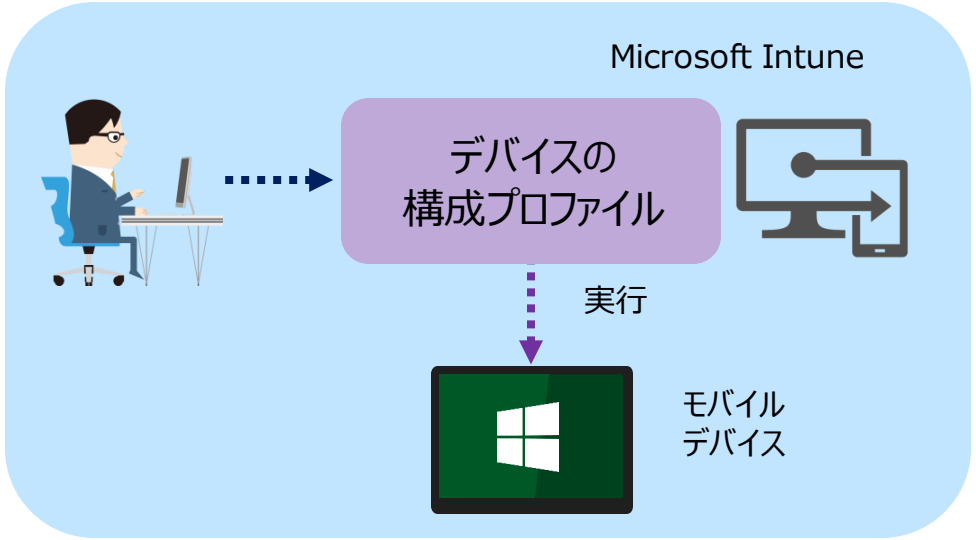


Windows 10 以降



代表的なデバイスの構成プロファイル

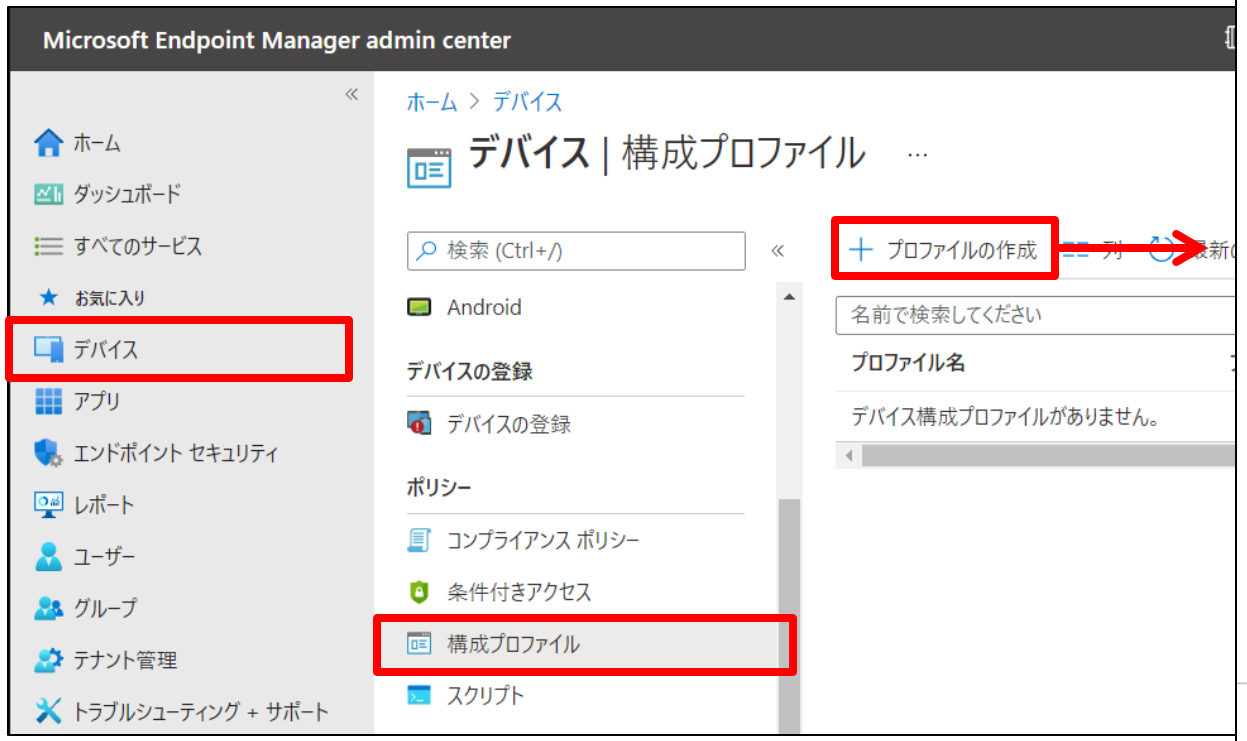
- 証明書
- 電子メール
- VPN
- Wi-Fi
- デバイスの制限
- カスタム プロファイル
- デバイスの機能（iOS/iPadOS、macOS）
- 更新ポリシー（iOS/iPadOS）
- 管理用テンプレート（Windows 10 以降）
- 配信の最適化（Windows 10 以降）
- ドメイン参加（Windows 10 以降）
- Defender for Endpoint（Windows 10 以降）
- ID 保護（Windows 10 以降、Windows Holographic for Business）　など



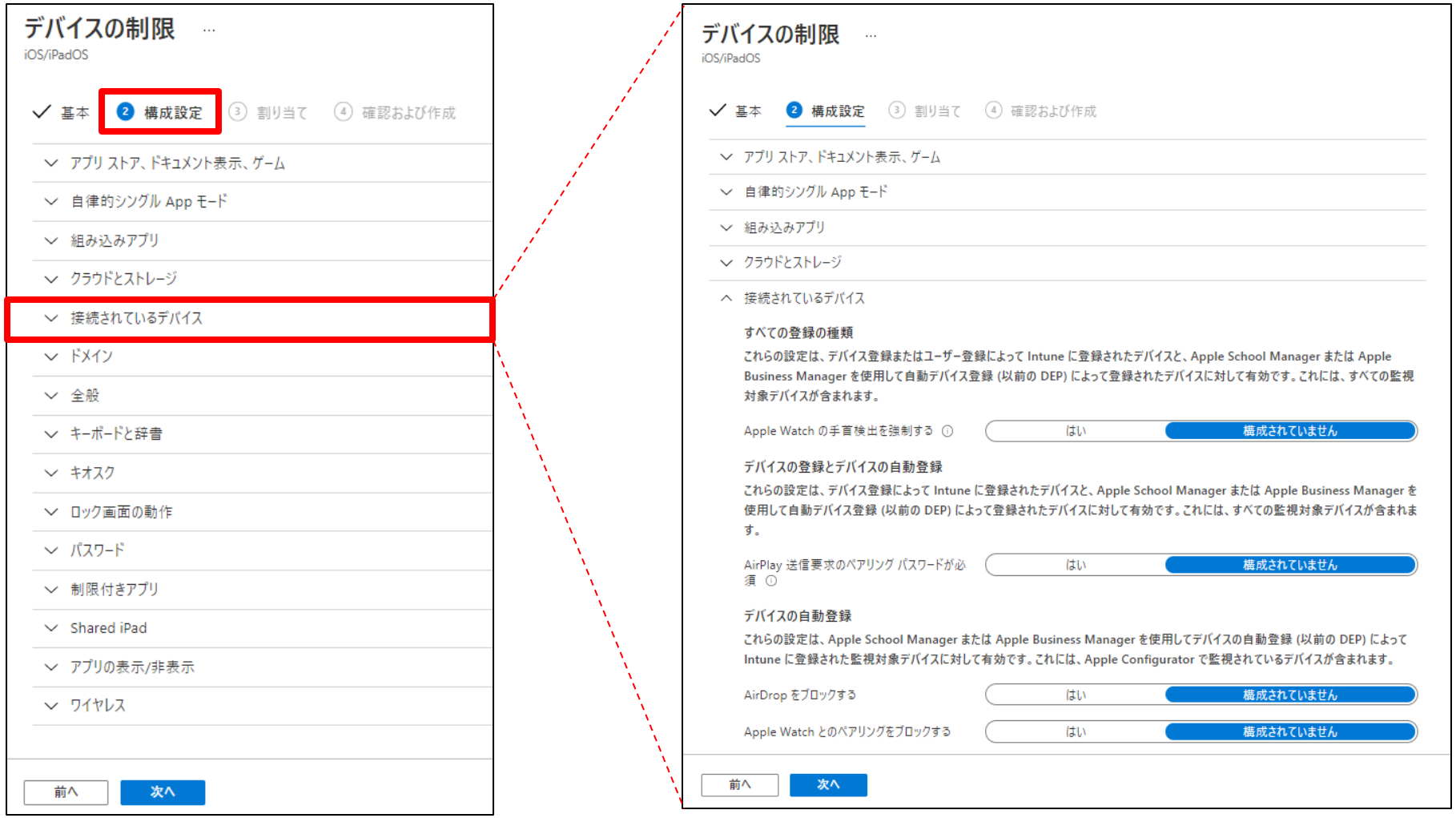
「Microsoft Intune でデバイス プロファイルを使用してデバイスに機能と設定を適用する」
https://docs.microsoft.com/ja-jp/mem/intune/configuration/device-profiles

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



「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

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）**専用ユーザーがいない**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

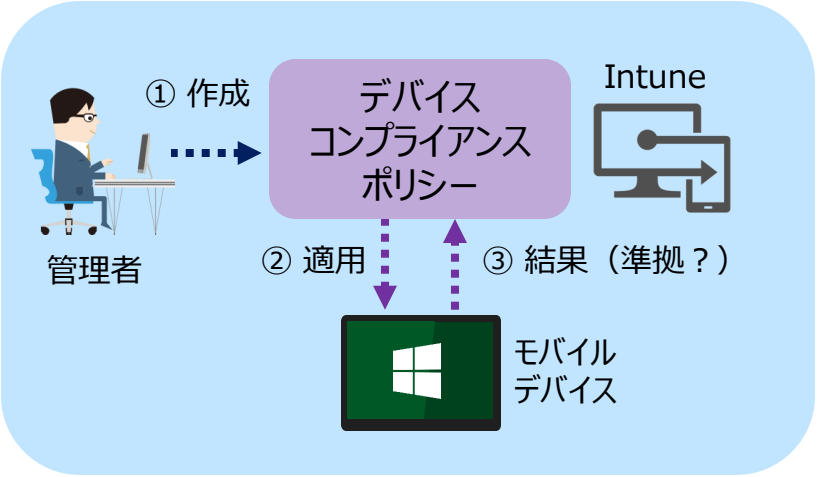
複数のポリシーが同じユーザーまたはデバイスに割り当てられている場合、

- 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

- 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

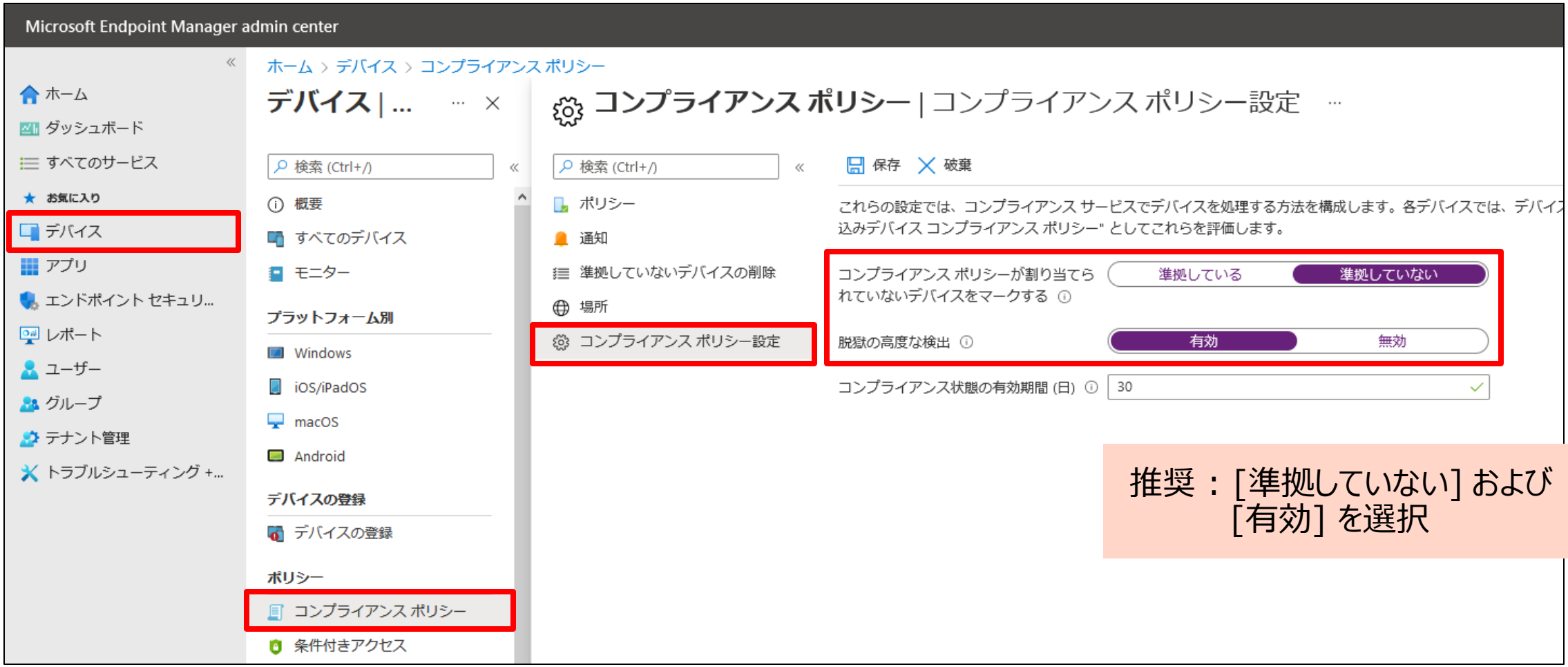
＋

② デバイス コンプライアンス ポリシー

- 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

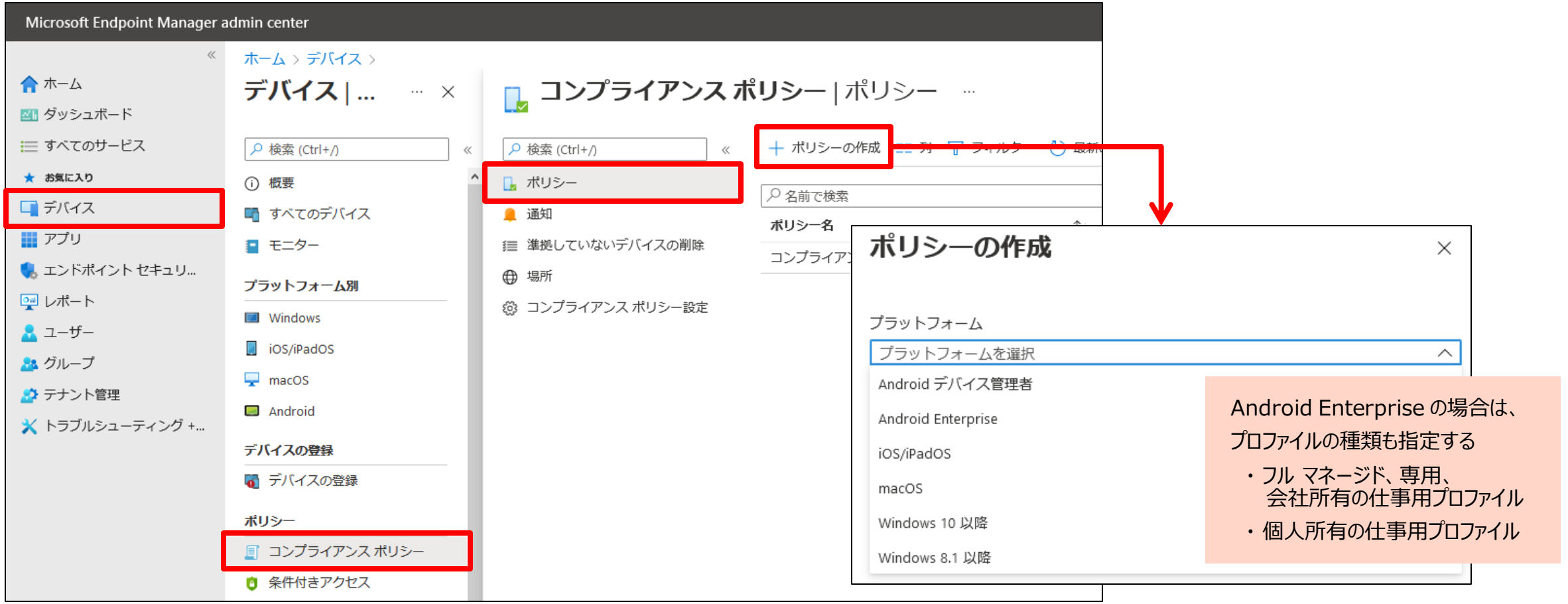
- [デバイス] – [コンプライアンス ポリシ] の [コンプライアンス ポリシー設定]



推奨：[準拠していない] および
[有効] を選択

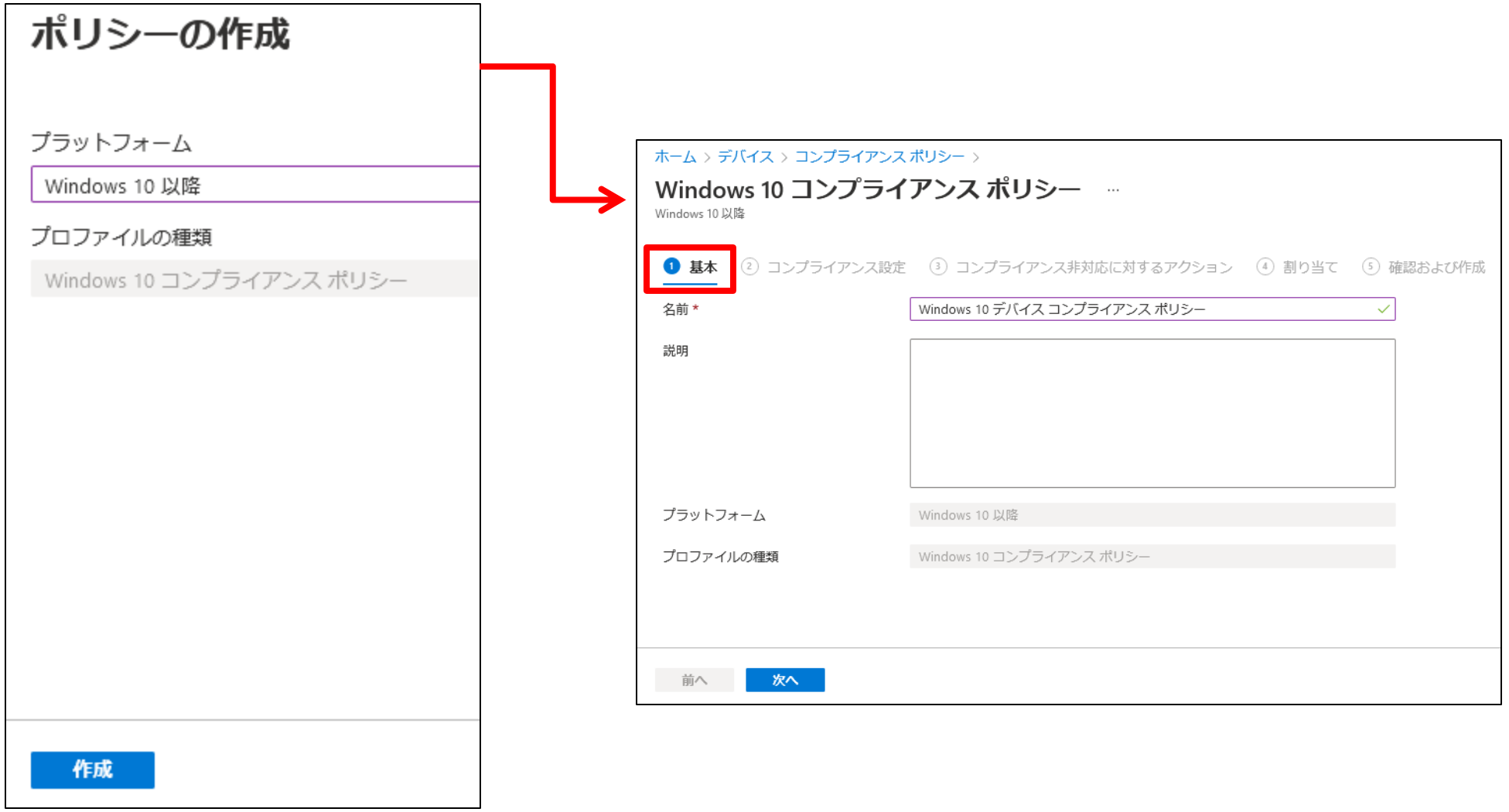
② デバイス コンプライアンス ポリシー

- [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

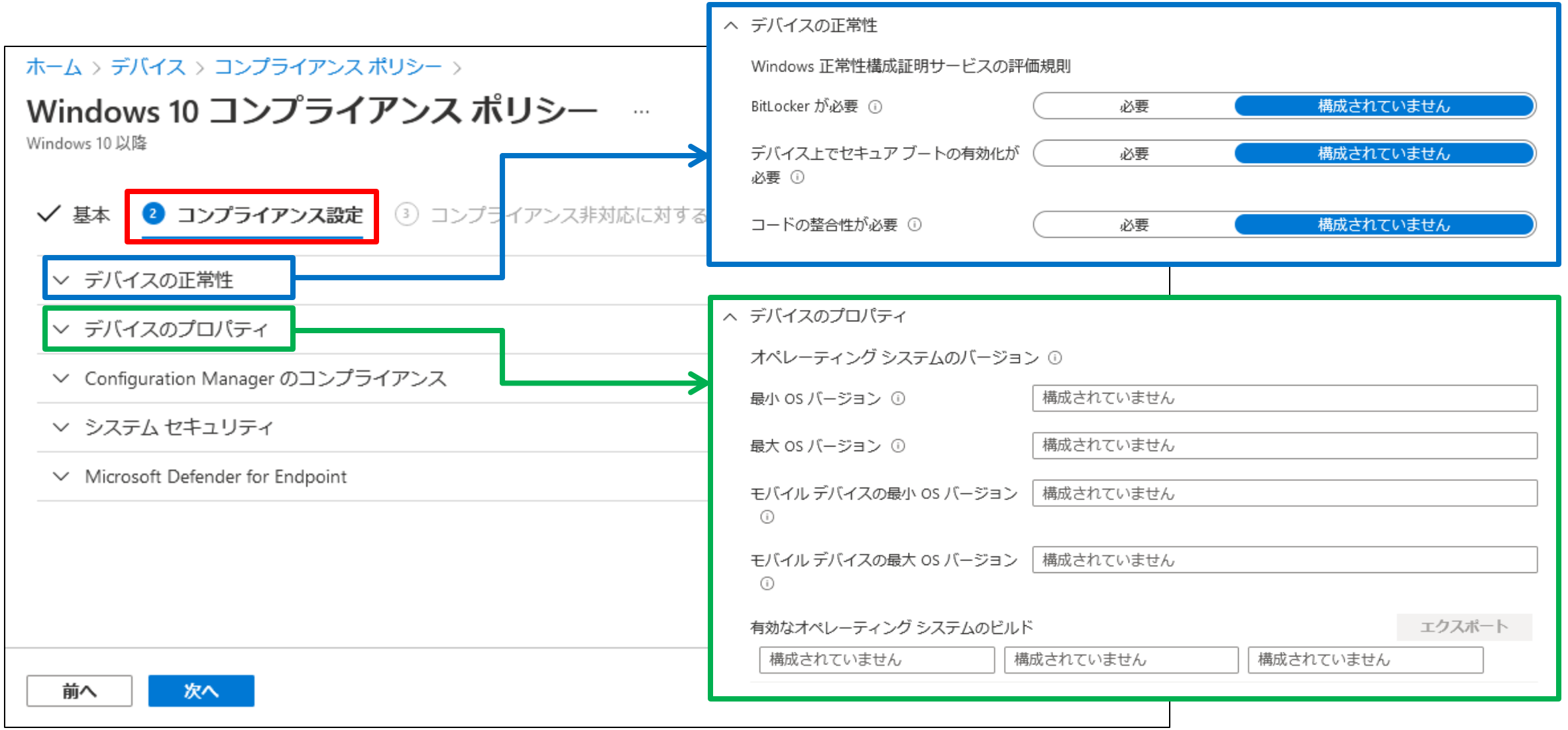


例）Windows 10 のデバイス コンプライアンス ポリシーの作成

- 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



[コンプライアンス設定] タブ



[参考] 技術資料

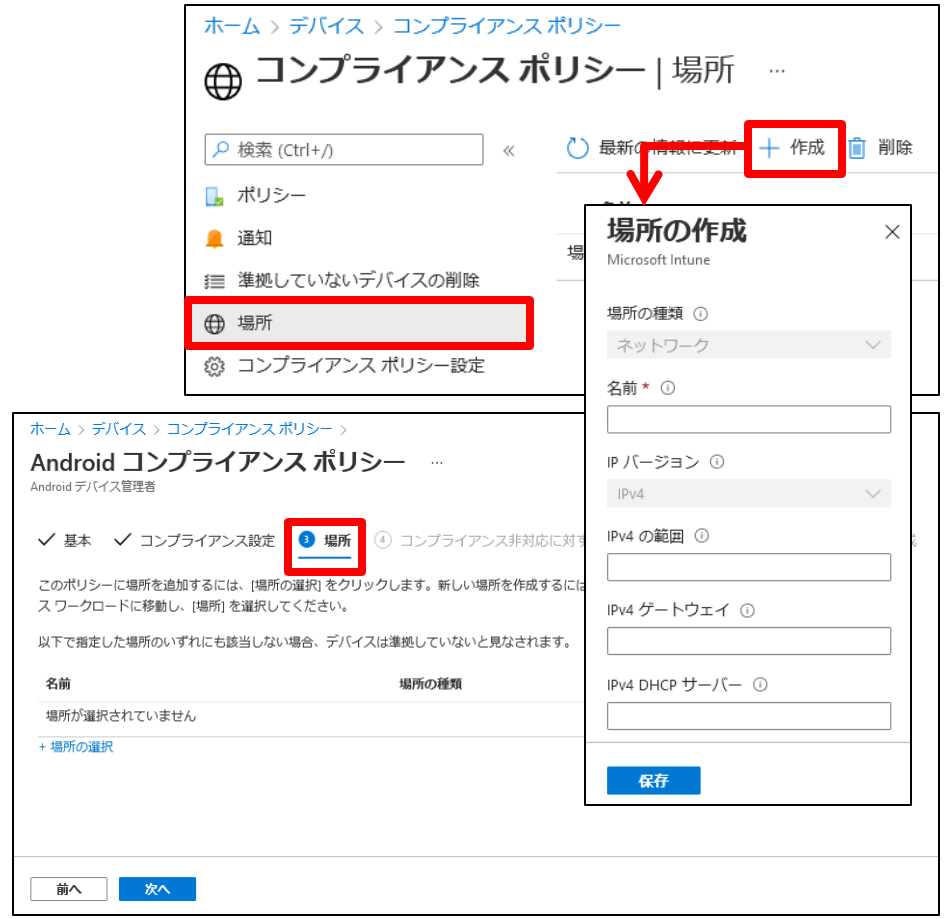
- **「Intune を使用してデバイスを準拠または非準拠としてマークするための Windows 10 以降の設定」**
  - https://docs.microsoft.com/ja-jp/mem/intune/protect/compliance-policy-create-windows
- **「Intune を使用してデバイスを準拠または非準拠としてマークするための iOS および iPadOS 設定」**
  - https://docs.microsoft.com/ja-jp/mem/intune/protect/compliance-policy-create-ios
- **「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。

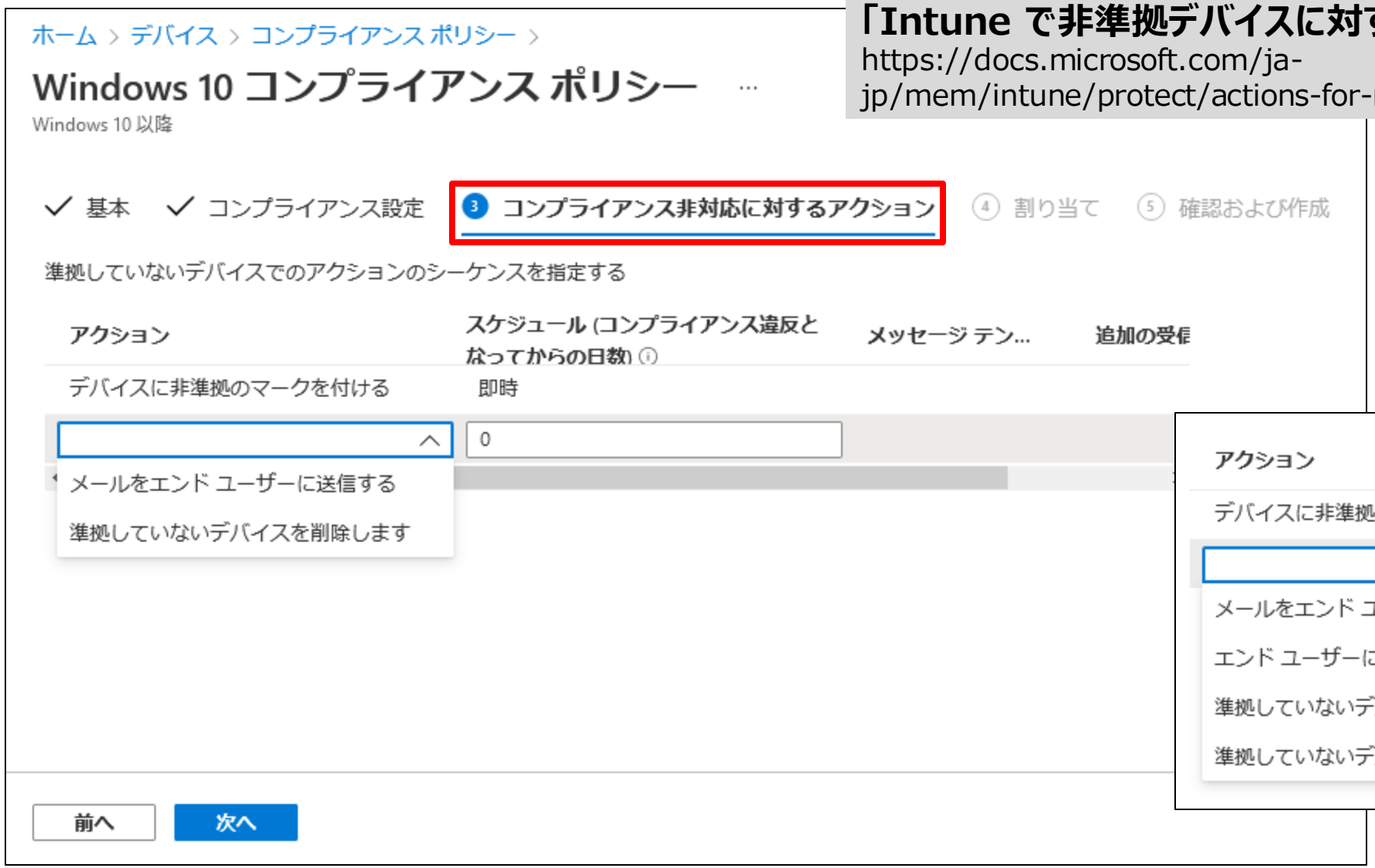
- 「Android デバイス管理者」プロファイルでのみサポート（Android デバイス 6.0 以降）



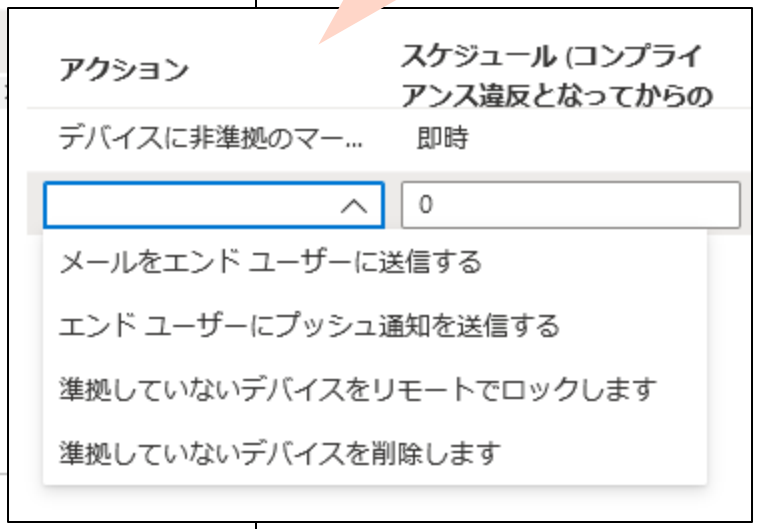
「Intune で場所（ネットワーク フェンス）を使用する」
https://docs.microsoft.com/ja-jp/mem/intune/protect/use-network-locations

[コンプライアンス非対応に対するアクション] タブ

「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

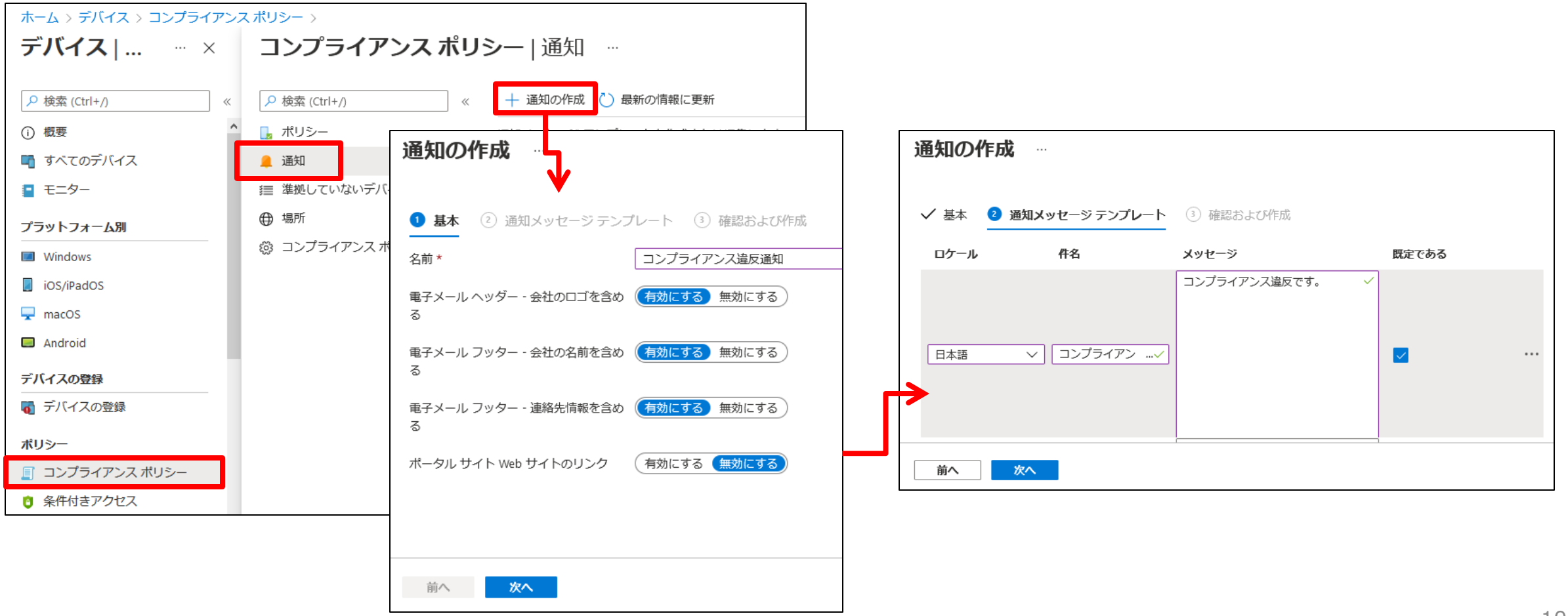


iOS/iPadOS、Android、Android Enterprise の場合



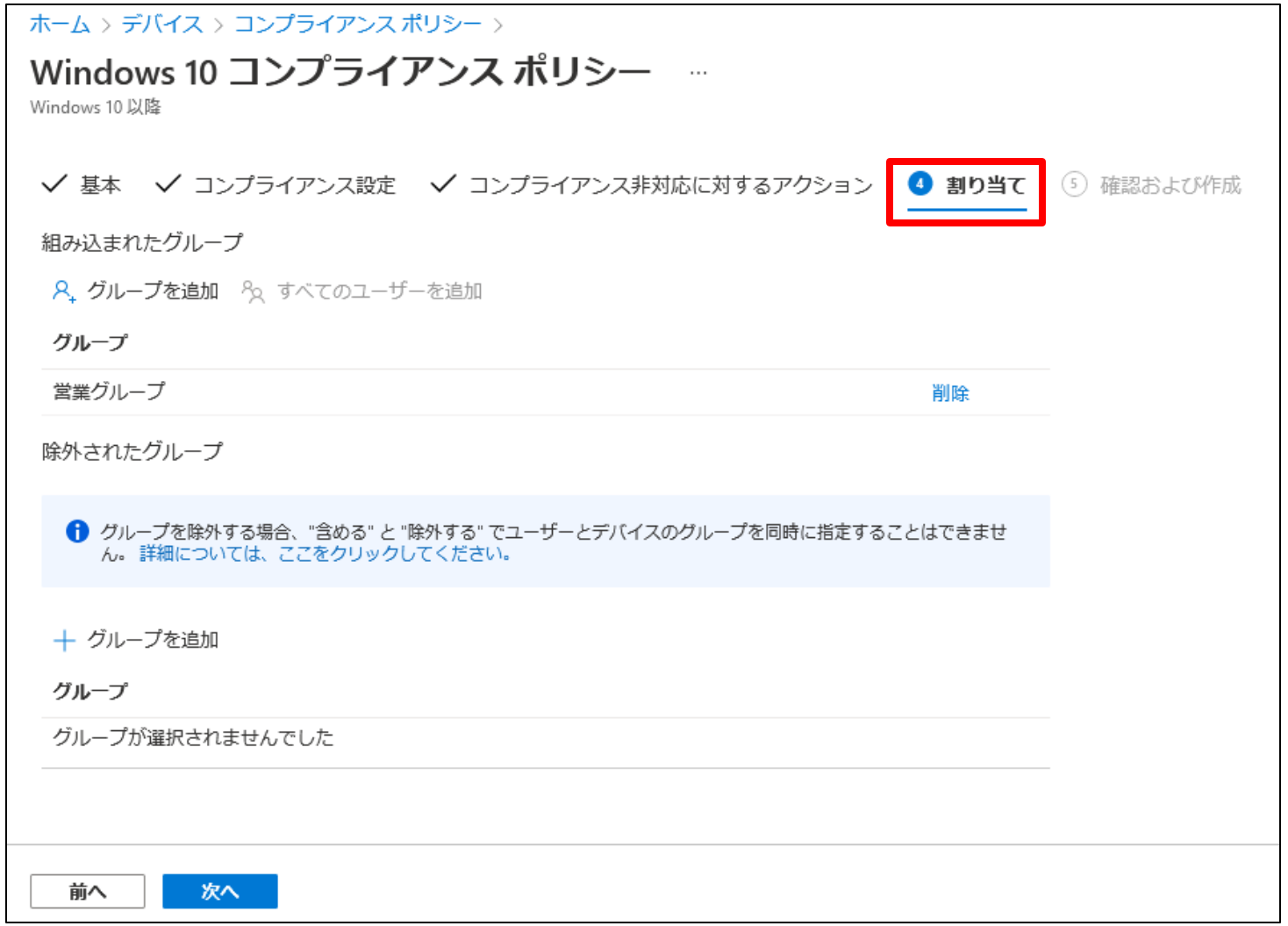
[参考] コンプライアンス ポリシーの通知の作成

- [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



[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



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	• **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	• 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

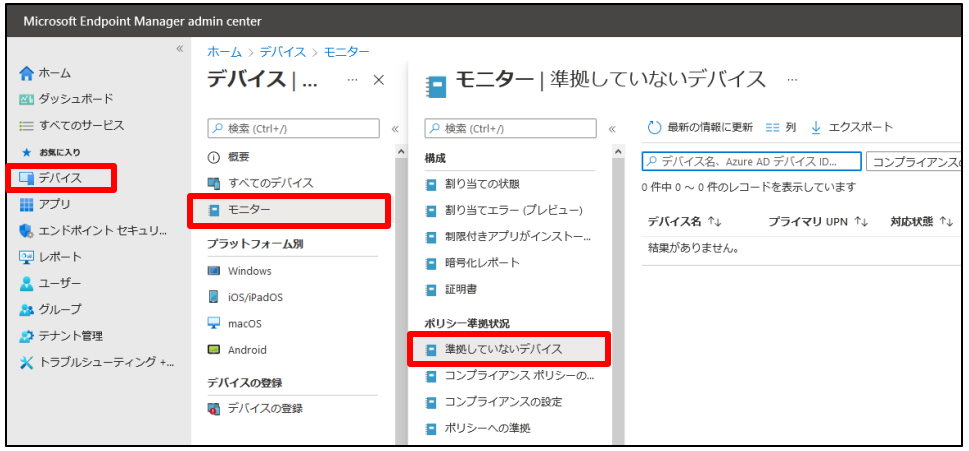
「準拠している/準拠していない」の確認

- [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

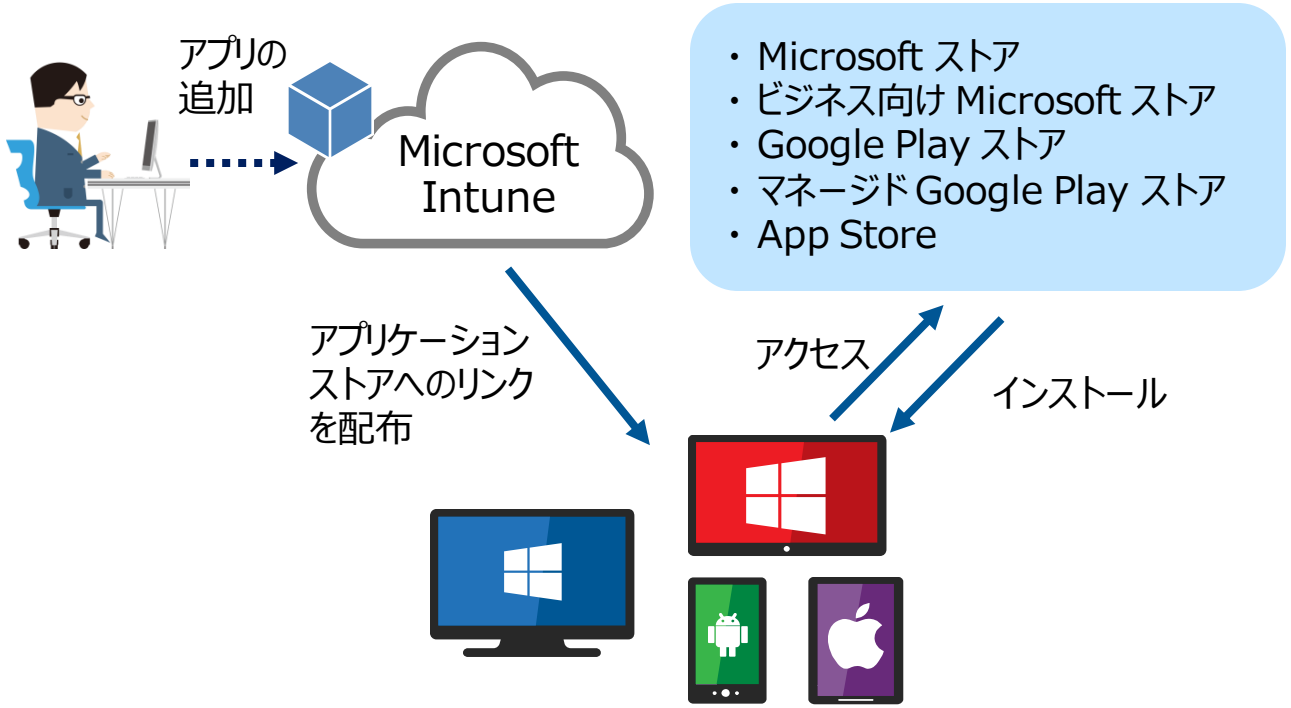
・Intune MDM + MAM
・デバイス登録なしの MAM

「Microsoft Intune アプリの管理とは」
https://docs.microsoft.com/ja-jp/mem/intune/apps/app-management

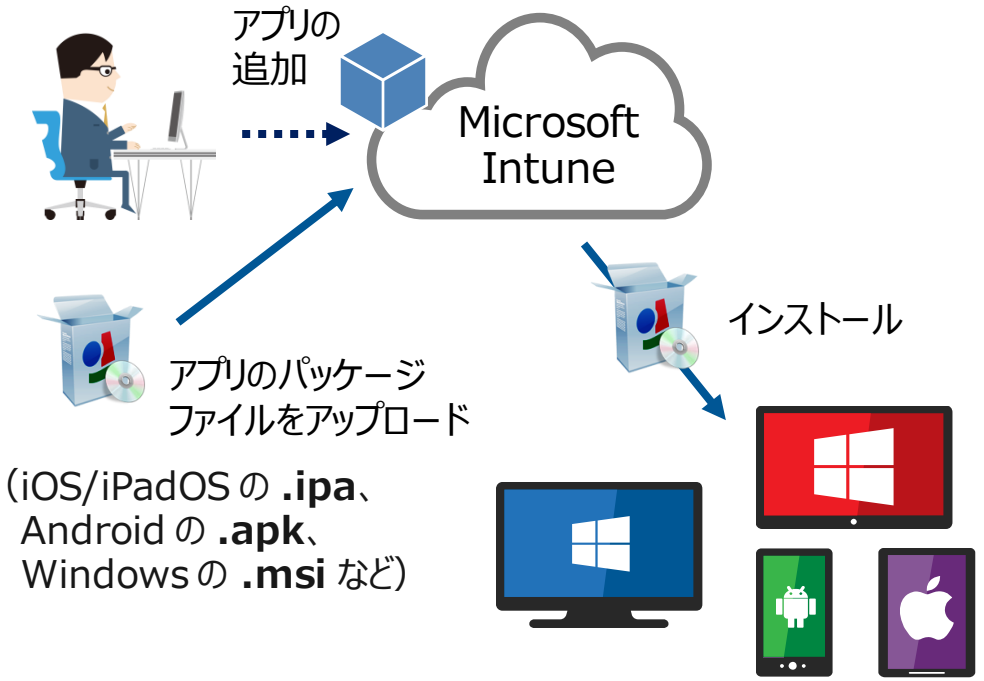
1. アプリの展開

- 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

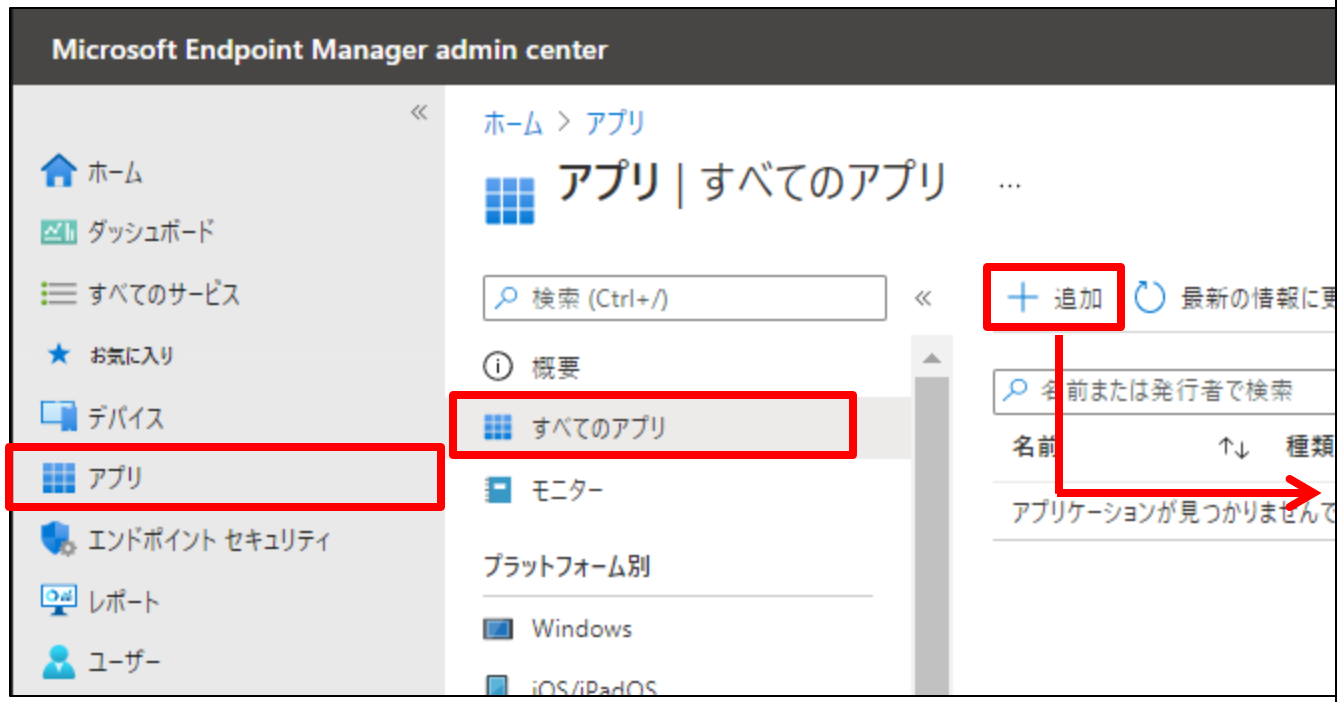
- 組織で使用しているモバイル デバイスに、さまざまな種類のアプリを展開できる
  - 24 時間以内に必要なアプリを自動的にインストール、更新、または削除

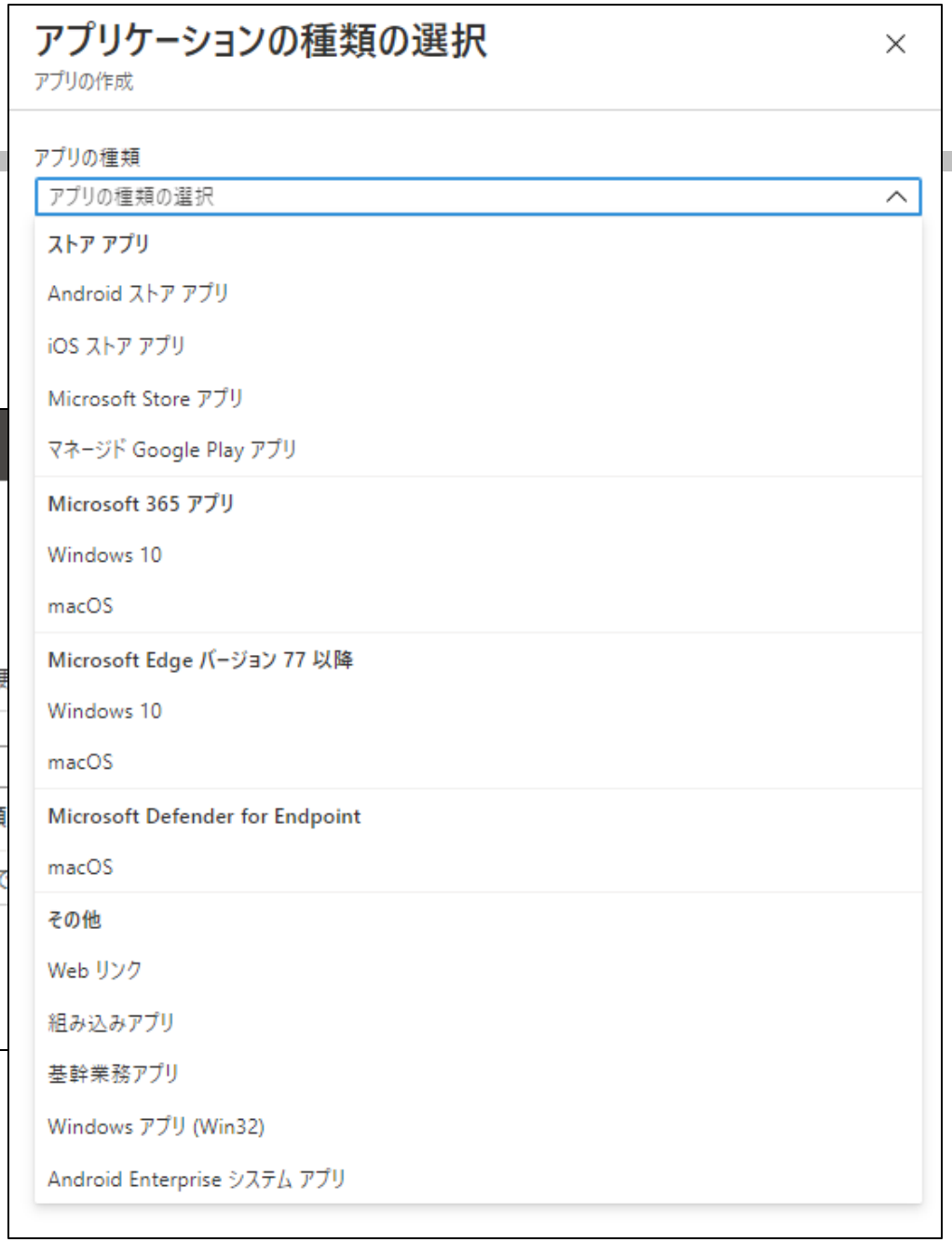
アプリの種類	インストール	アプリの更新
ストア アプリ	・Intune によって、アプリがデバイスにインストールされる	自動
社内で作成されたアプリ （基幹業務アプリ）	・管理者がインストール ファイルを準備する ・Intune によって、アプリがデバイスにインストールされる	ユーザーが手動で更新
組み込まれているアプリ （組み込みアプリ）	・Intune によって、アプリがデバイスにインストールされる	自動
Web アプリ（Web リンク）	・Intune によって、デバイスのホーム画面に Web アプリのショートカットが作成される	自動
Microsoft サービスからのアプリ	・Intune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

[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 * ⓘ アプリ ストアを検索します

名前 * ⓘ Microsoft Outlook

説明 * ⓘ 「最強の iPhone 用メール アプリ」- The Verge

発行元 * ⓘ Microsoft Corporation

アプリ ストアの URL https://apps.apple.com/jp/app/microsoft-outlook/id951937596?uo=4

最低限のオペレーティング システム * ⓘ iOS 8.0

適用可能なデバイスの種類 * ⓘ 2 項目が選択されました

カテゴリ ⓘ 0 項目が選択されました

ポータル サイトでおすすめアプリとして表示する ⓘ はい いいえ

情報 URL ⓘ 有効な URL を入力してください

プライバシー URL ⓘ 有効な URL を入力してください

開発者 ⓘ

所有者 ⓘ

メモ ⓘ

ロゴ ⓘ 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

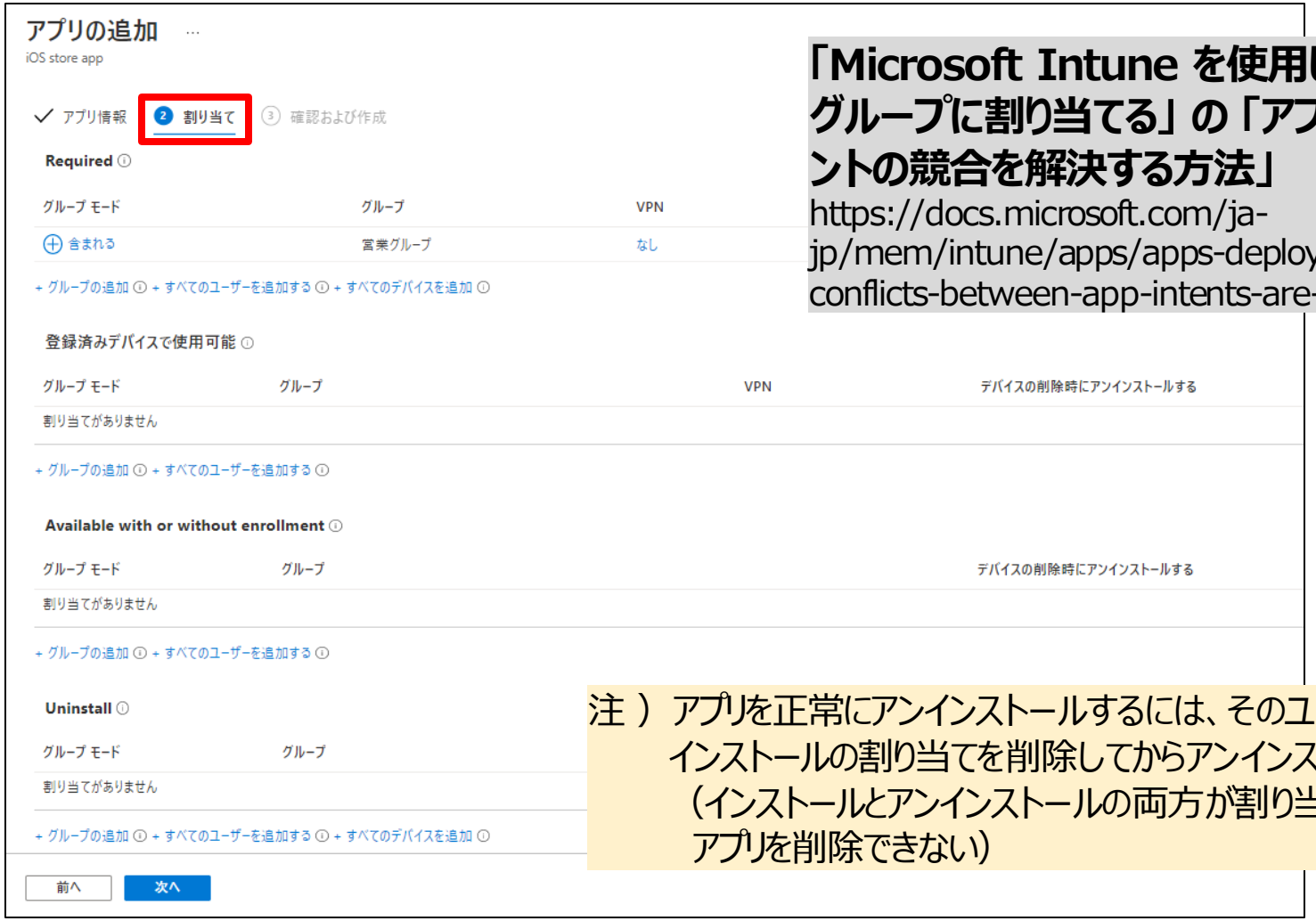
- 競合が起こらないように、アプリを展開したいグループを指定

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



「Microsoft Intune を使用してアプリをグループに割り当てる」の「アプリのインテント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

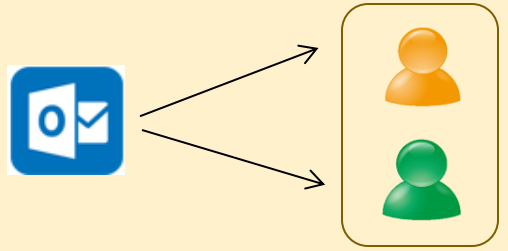
注 ） アプリを正常にアンインストールするには、そのユーザーへのインストールの割り当てを削除してからアンインストールする（インストールとアンインストールの両方が割り当てられると、アプリを削除できない）

アプリのグループへの割り当て

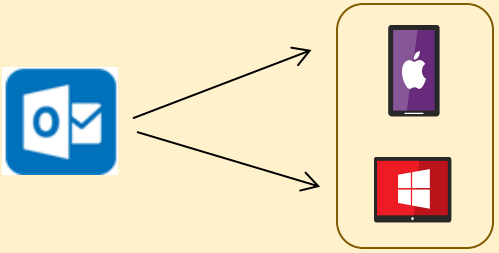
- Intune にデバイスを登録しているか否かで、割り当てに違いがある

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

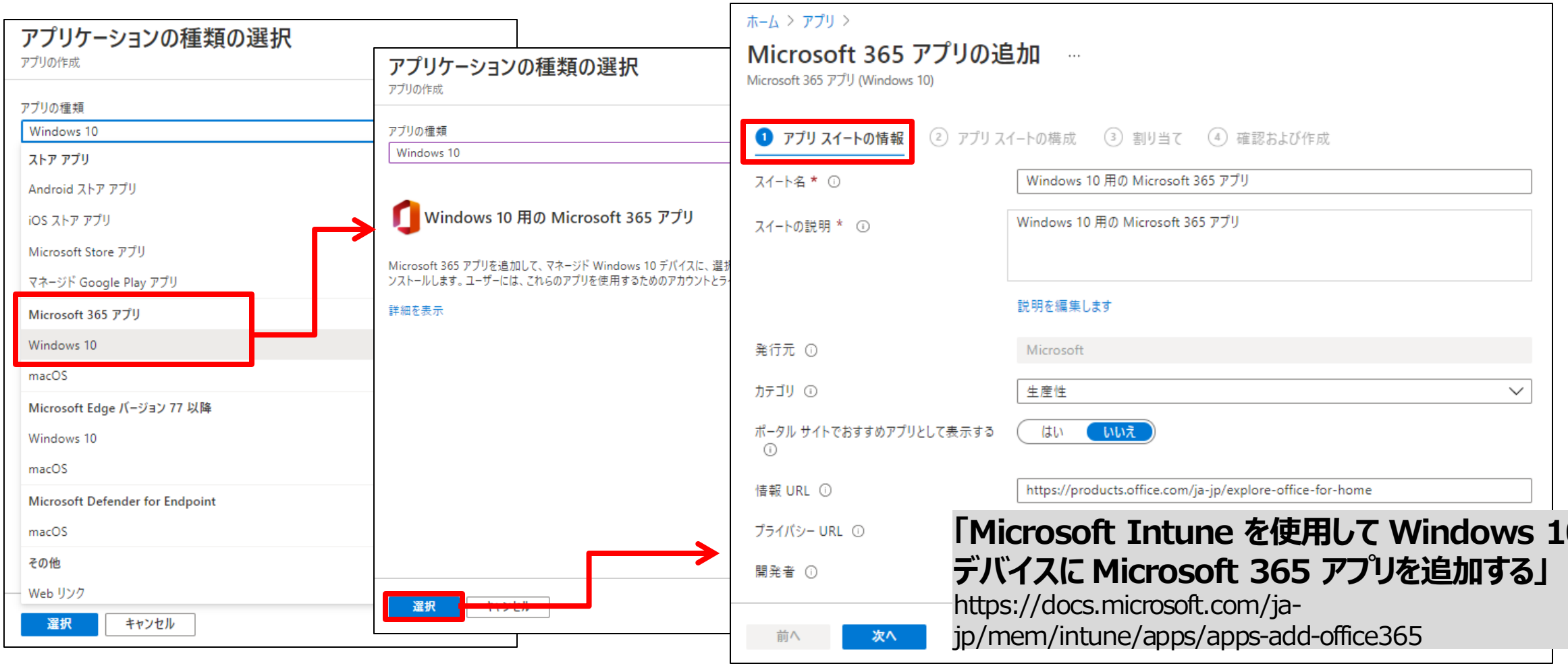
- 管理者がアンインストールの命令を展開したが、
  アプリをデバイスからアンインストールできなかった場合、
  24 時間以内に Intune でコンプライアンスが評価され、アプリをアンインストールする

[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

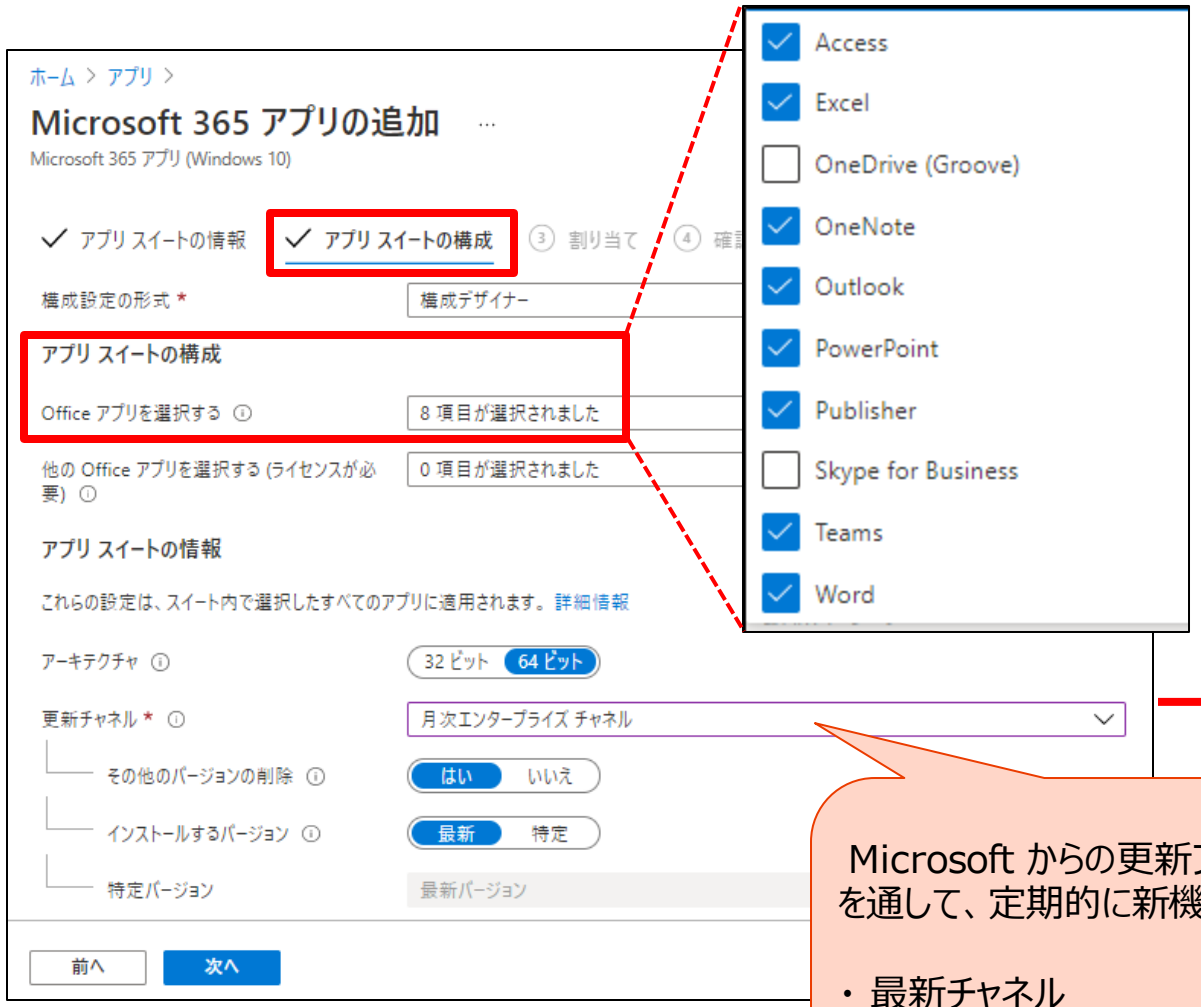
例 2）Windows 10「Microsoft 365」アプリ の追加

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



「Microsoft Intune を使用して Windows 10 デバイスに Microsoft 365 アプリを追加する」
https://docs.microsoft.com/ja-jp/mem/intune/apps/apps-add-office365

（続き）



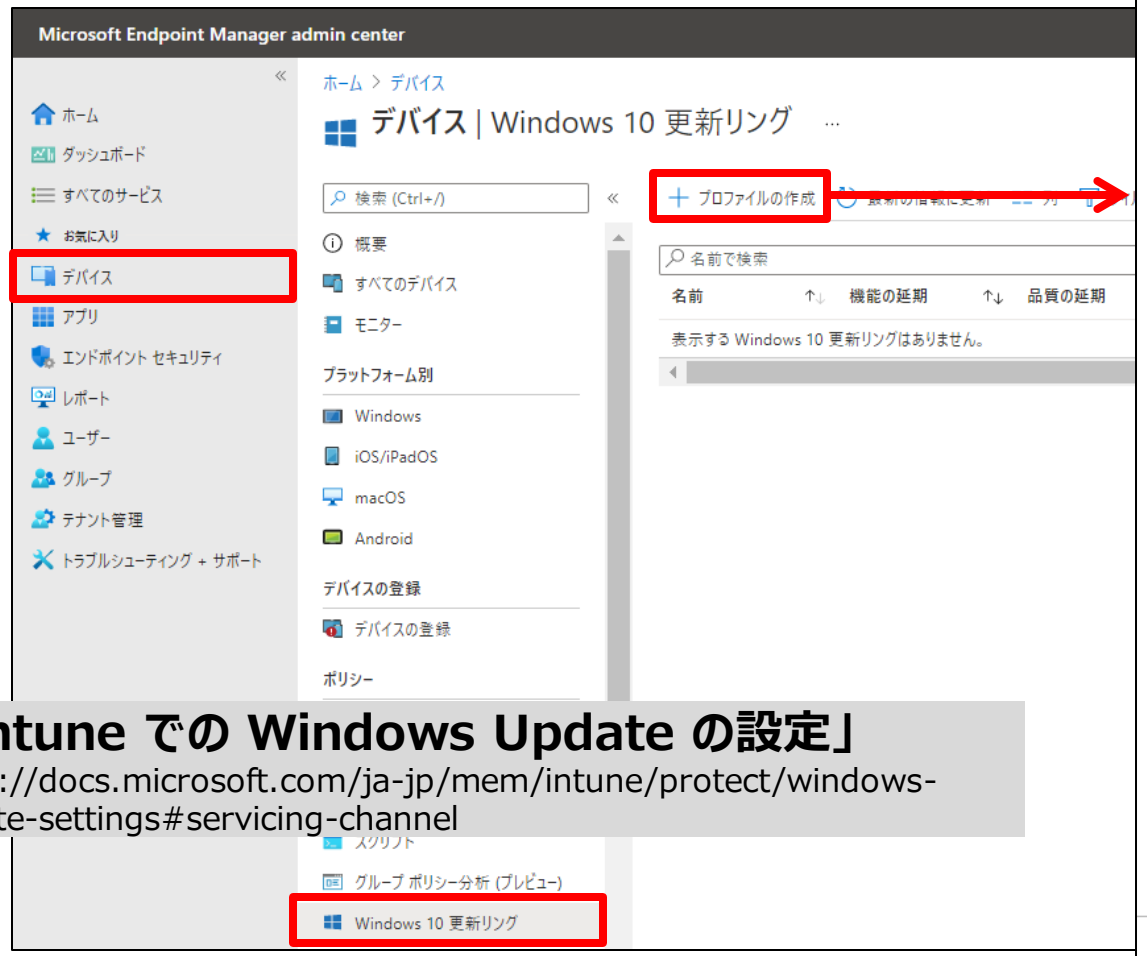
Microsoft からの更新プログラムを通して、定期的に新機能を取得

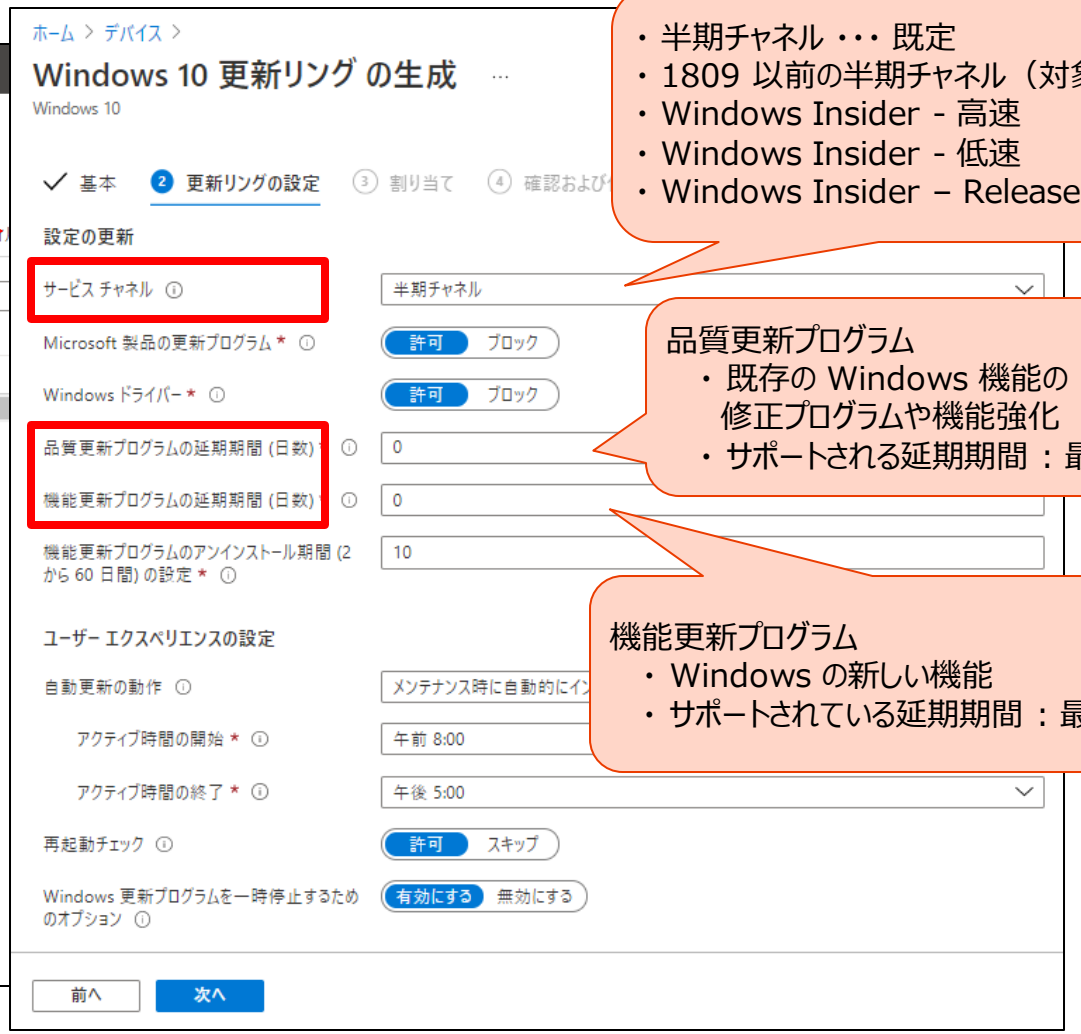
- 最新チャネル
- 月次エンタープライズ チャネル
- 半期エンタープライズ チャネル

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

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]





・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

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

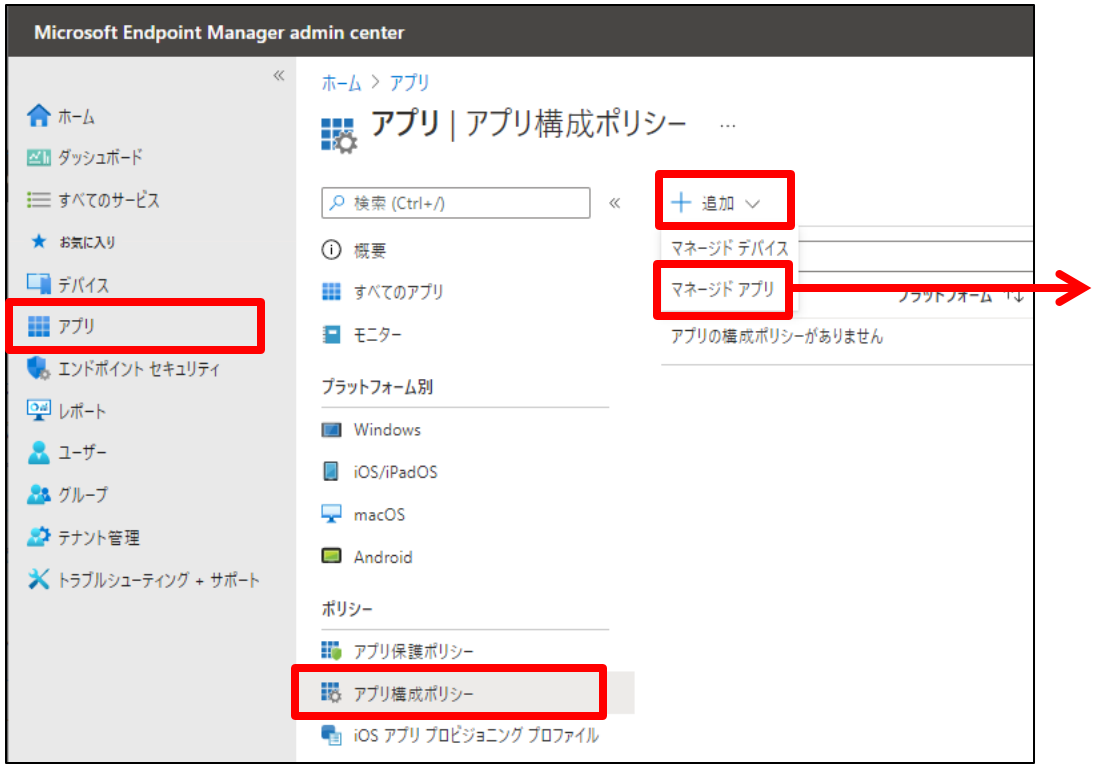
2. アプリの構成

- **“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

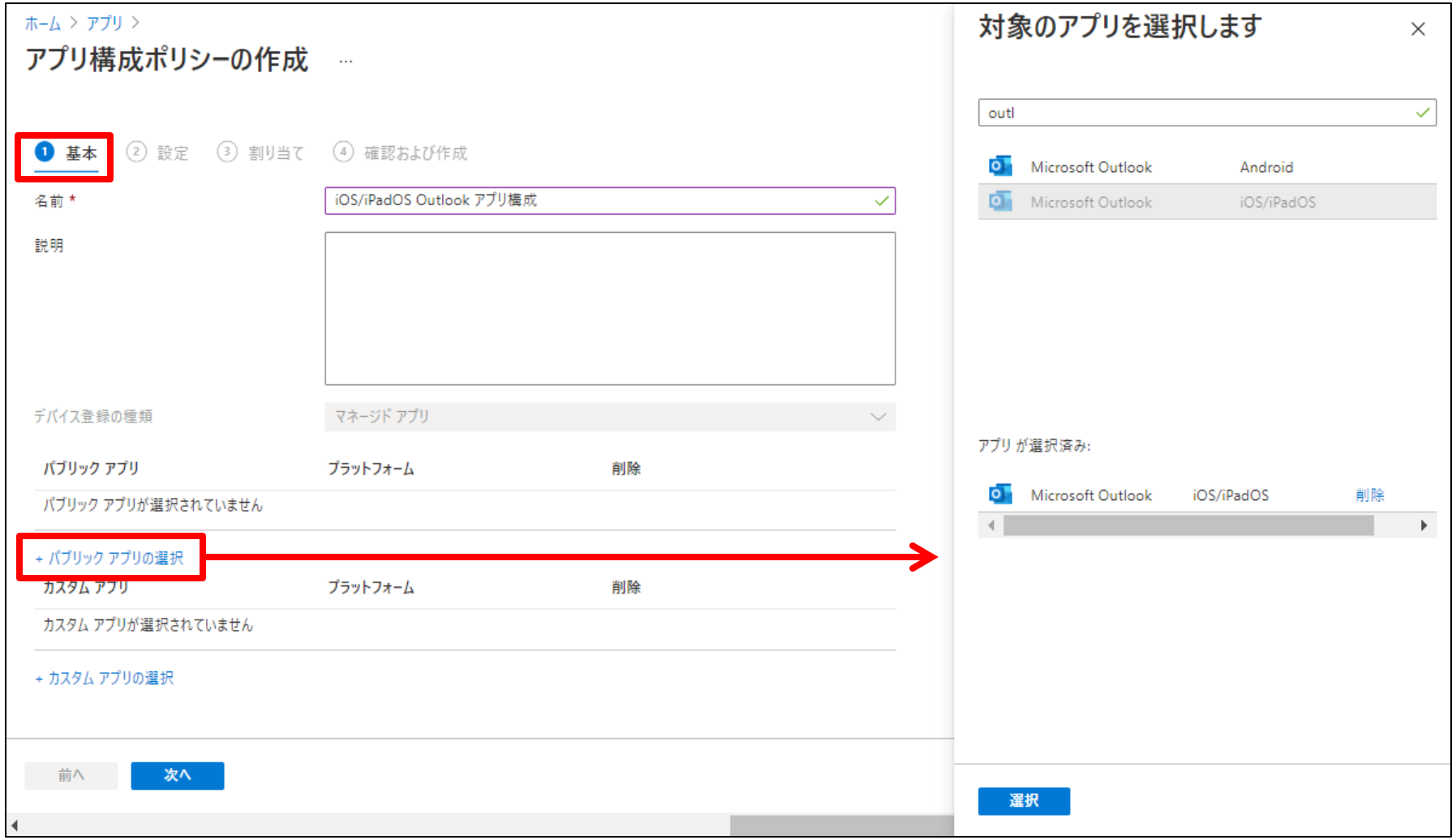
「Microsoft Intune 用アプリ構成ポリシー」
https://docs.microsoft.com/ja-jp/mem/intune/apps/app-configuration-policies-overview

[アプリ] – [アプリ構成ポリシー] の [+ 追加]



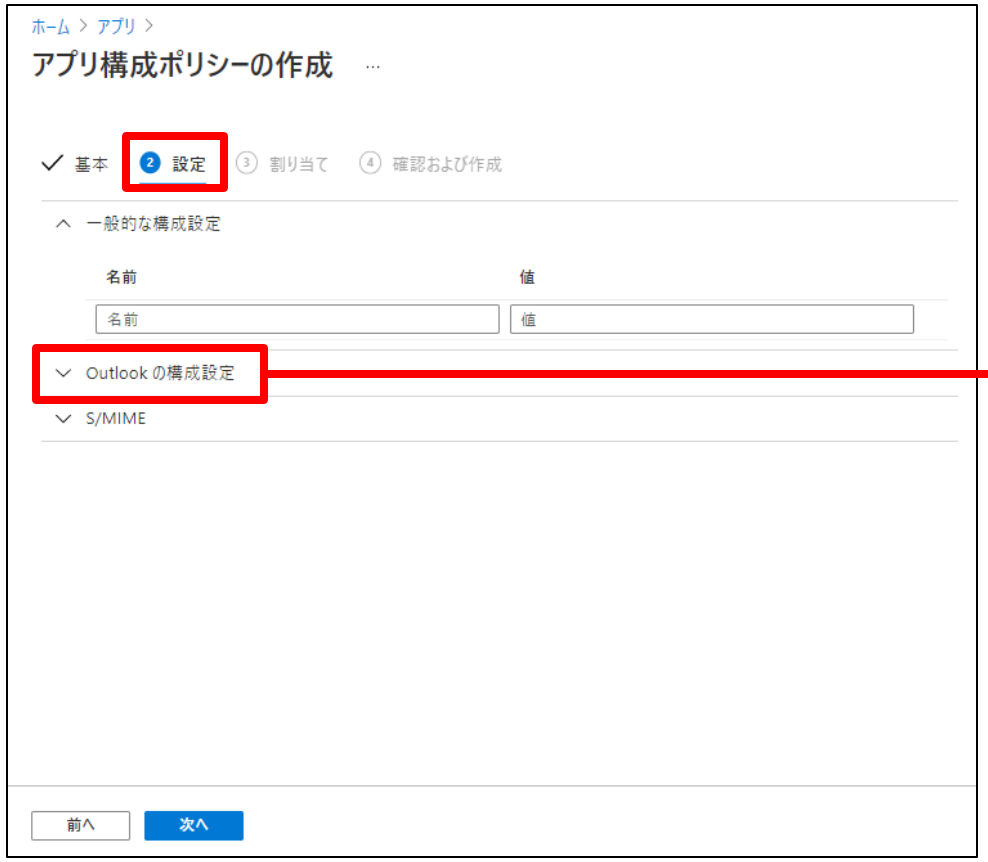
例）iOS/iPadOS の「Microsoft Outlook」の構成

- [基本] タブで、構成対象となるアプリを選択



[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



[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

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

「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

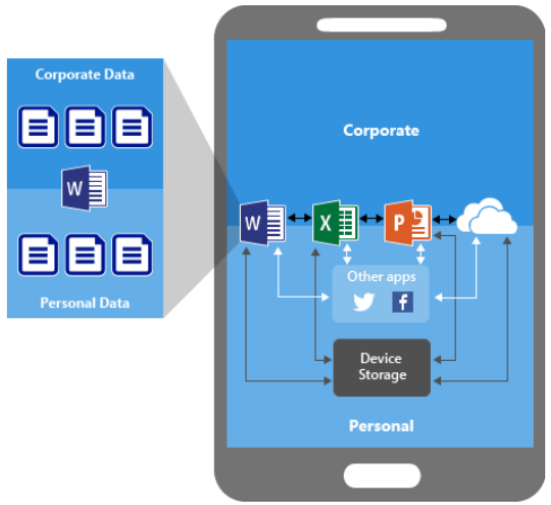
- アプリ保護ポリシーを適用できるデバイス
  - その 1：Intune に登録されているデバイス（会社所有デバイス）
  - その 2：サード パーティ製の MDM ツールに登録されているデバイス（会社所有デバイス）
  - その 3：いずれの MDM ツールにも登録されていないデバイス（個人所有デバイス）

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

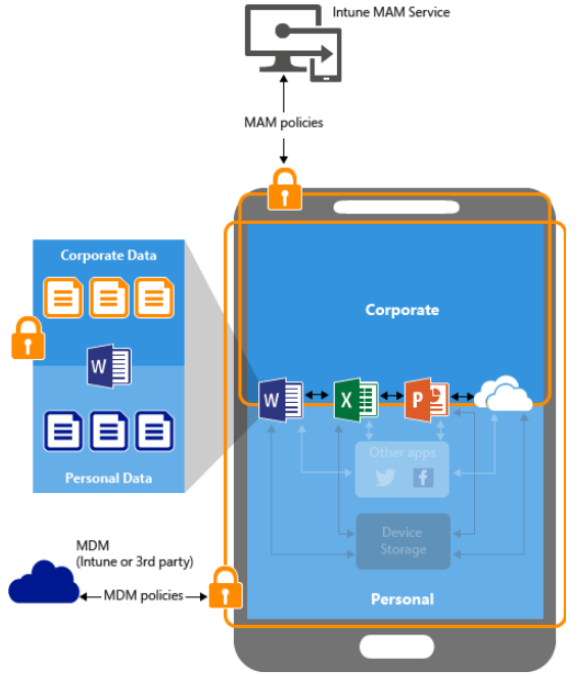


- 組織のデータと個人データが混在する
- 組織のデータが個人の記憶域に保存されたり、管理範囲外のアプリに転送されたり、データ損失を招く危険がある

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



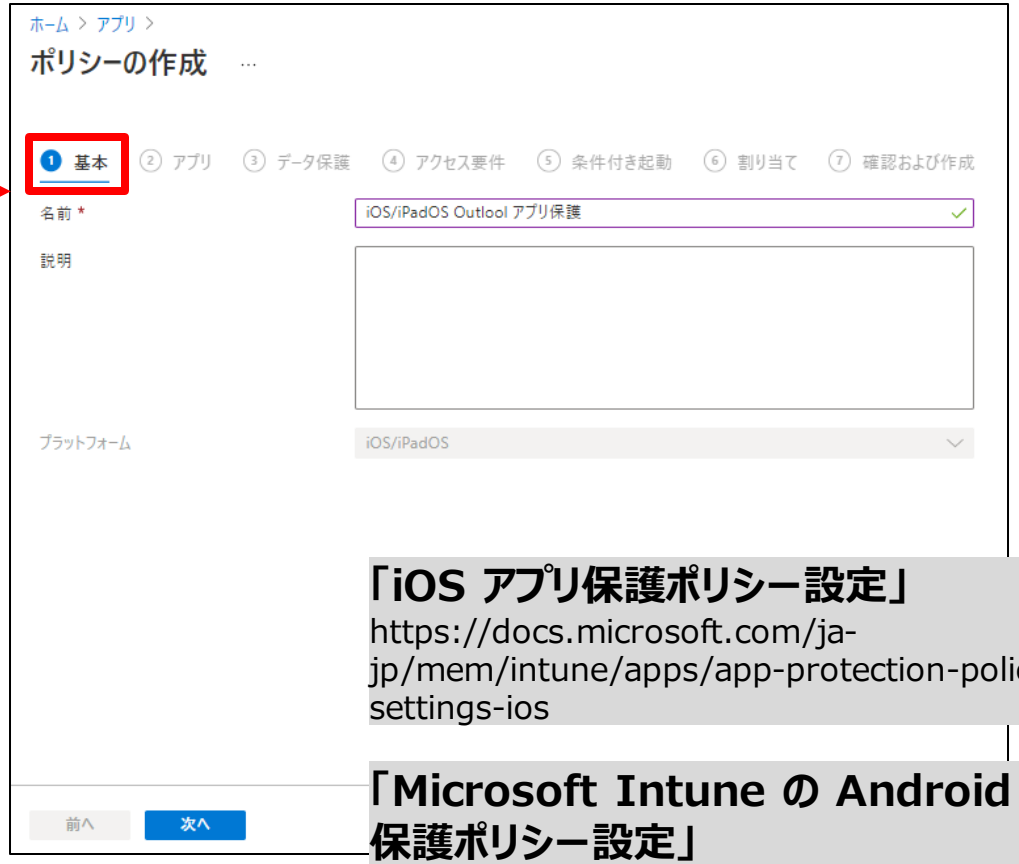
パターン 2 の構成 +

- 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



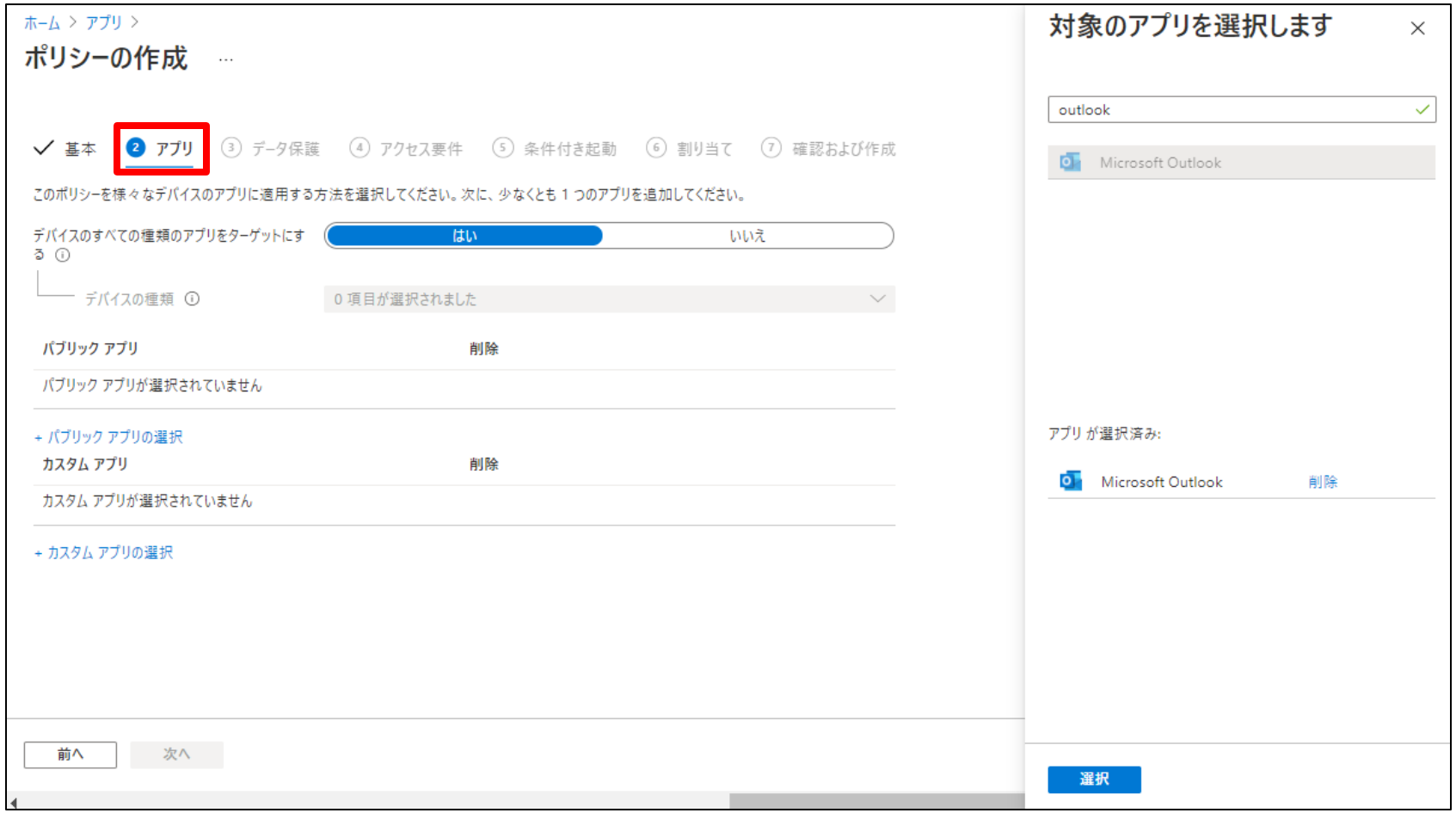
「アプリ保護ポリシーを作成して割り当てる方法」
https://docs.microsoft.com/ja-jp/mem/intune/apps/app-protection-policies

「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] タブ

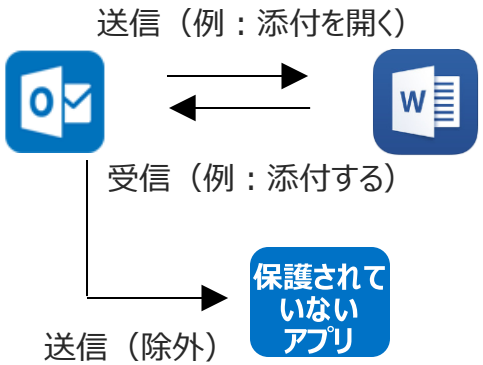
- アプリ保護ポリシーを適用するアプリを選択



[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

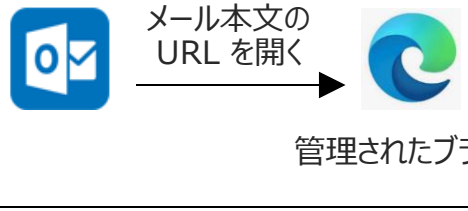
組織データの送信、受信



組織データのコピーを保存

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

[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

「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

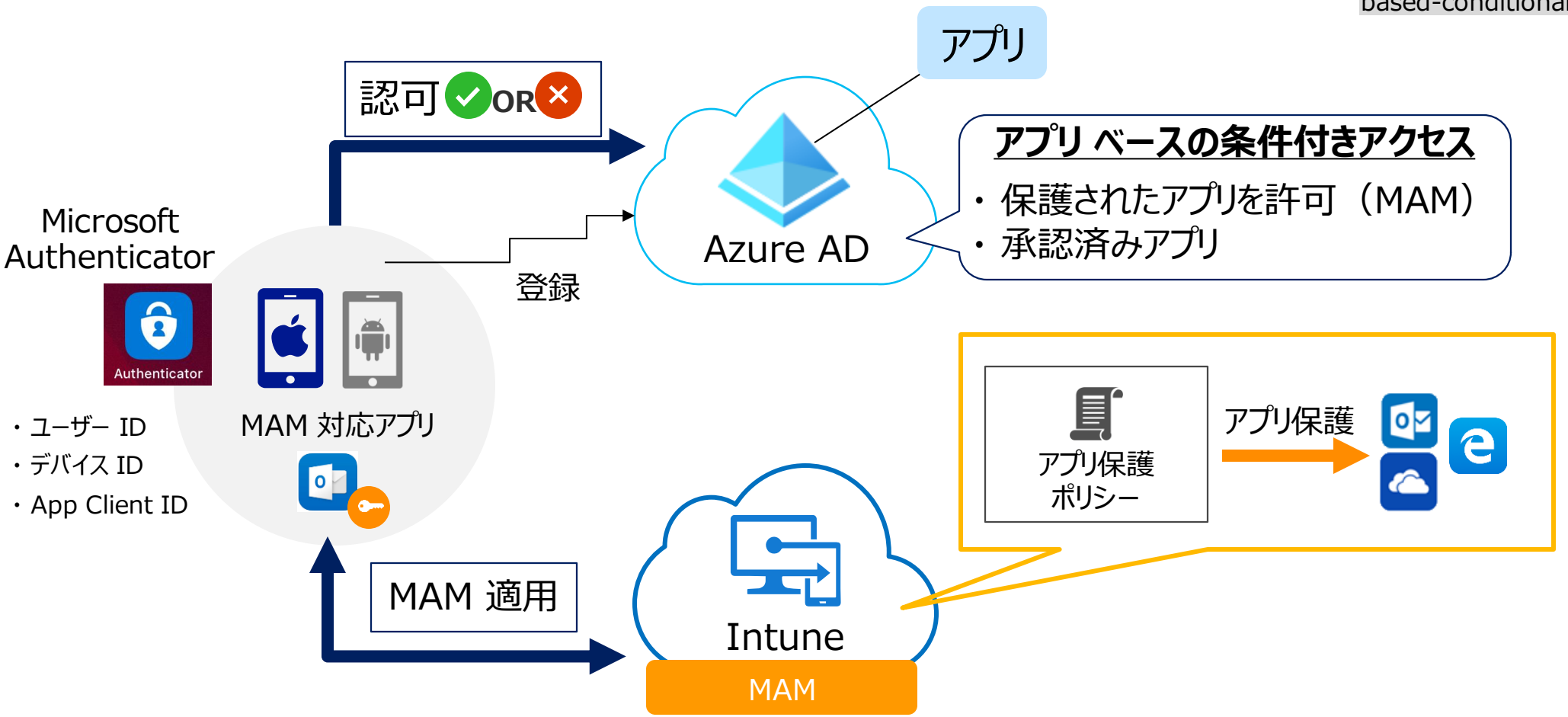
4. アプリに対する条件付きアクセス

Azure AD Premium P1

Intune

- 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

Azure AD Premium P1

Intune

- 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）

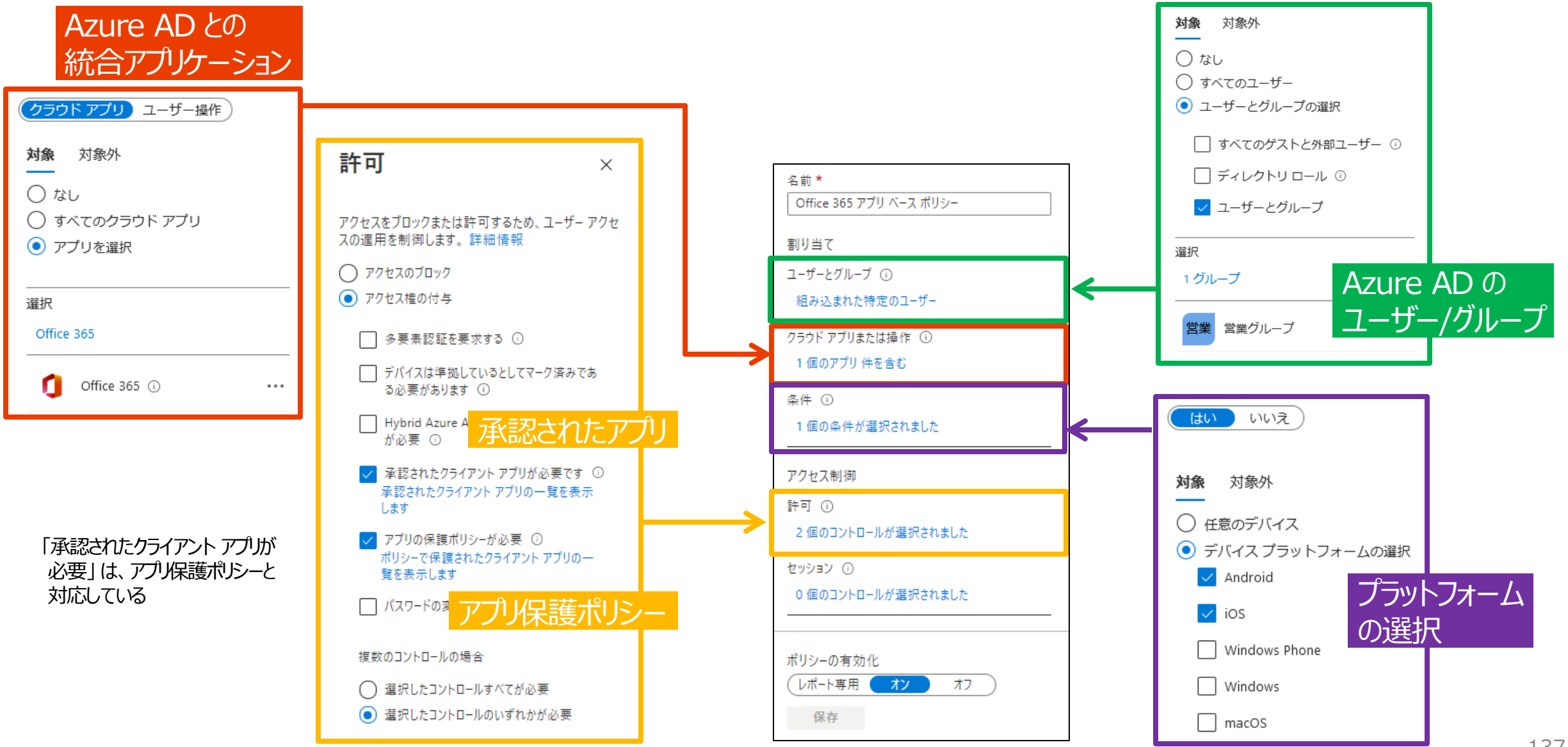
[デバイス] – [条件付きアクセス] – [ポリシー] の [＋ 新しいポリシー] で作成

「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

例）保護されたアプリからのアクセスを許可

Azure AD Premium P1

Intune



「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

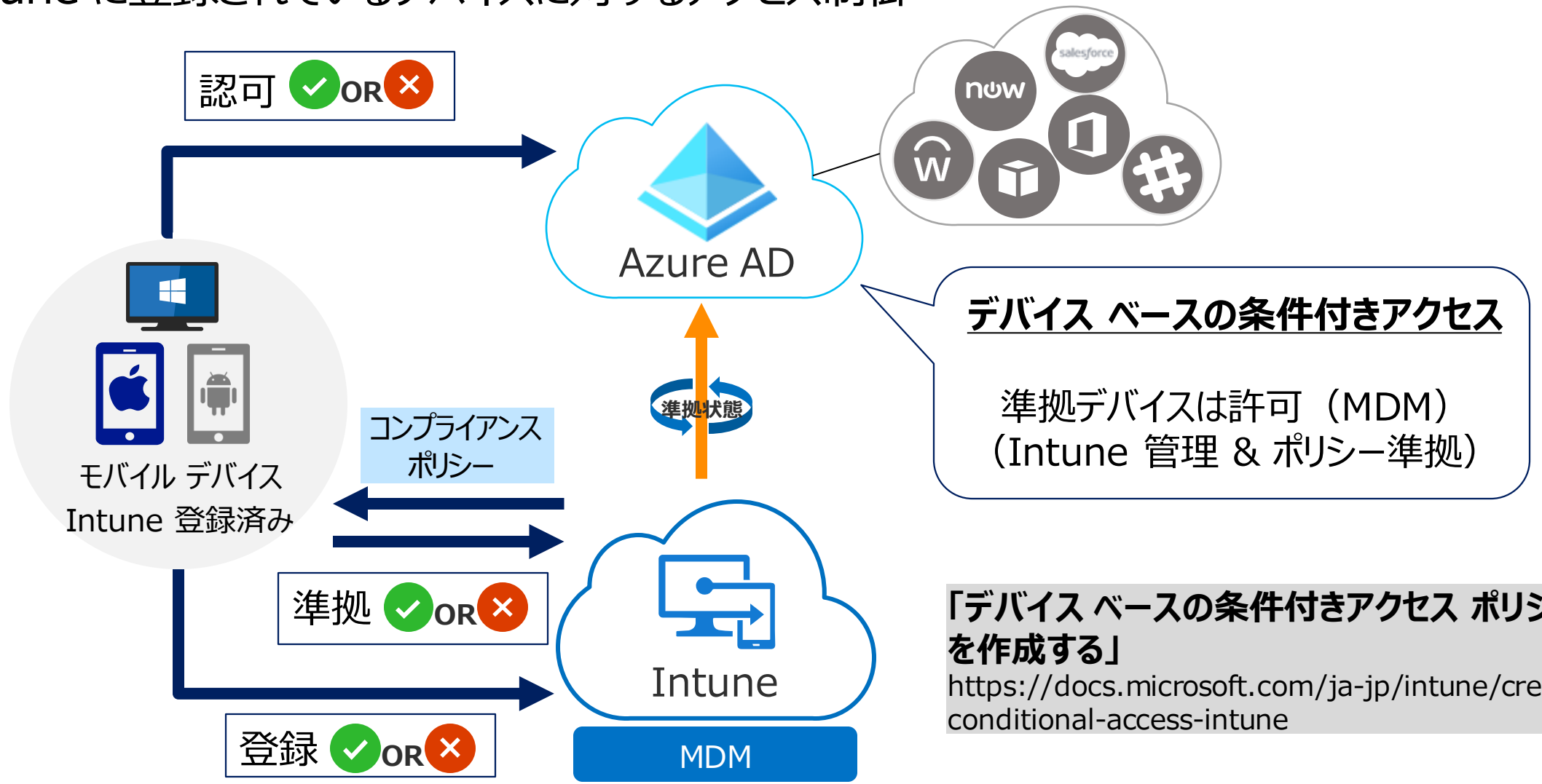
2 章：Microsoft Intune

- 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

Azure AD Premium P1
Intune

- 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 ベースの条件付きアクセス ポリシーを作成する」
https://docs.microsoft.com/ja-jp/intune/create-conditional-access-intune

デバイス準拠の判断

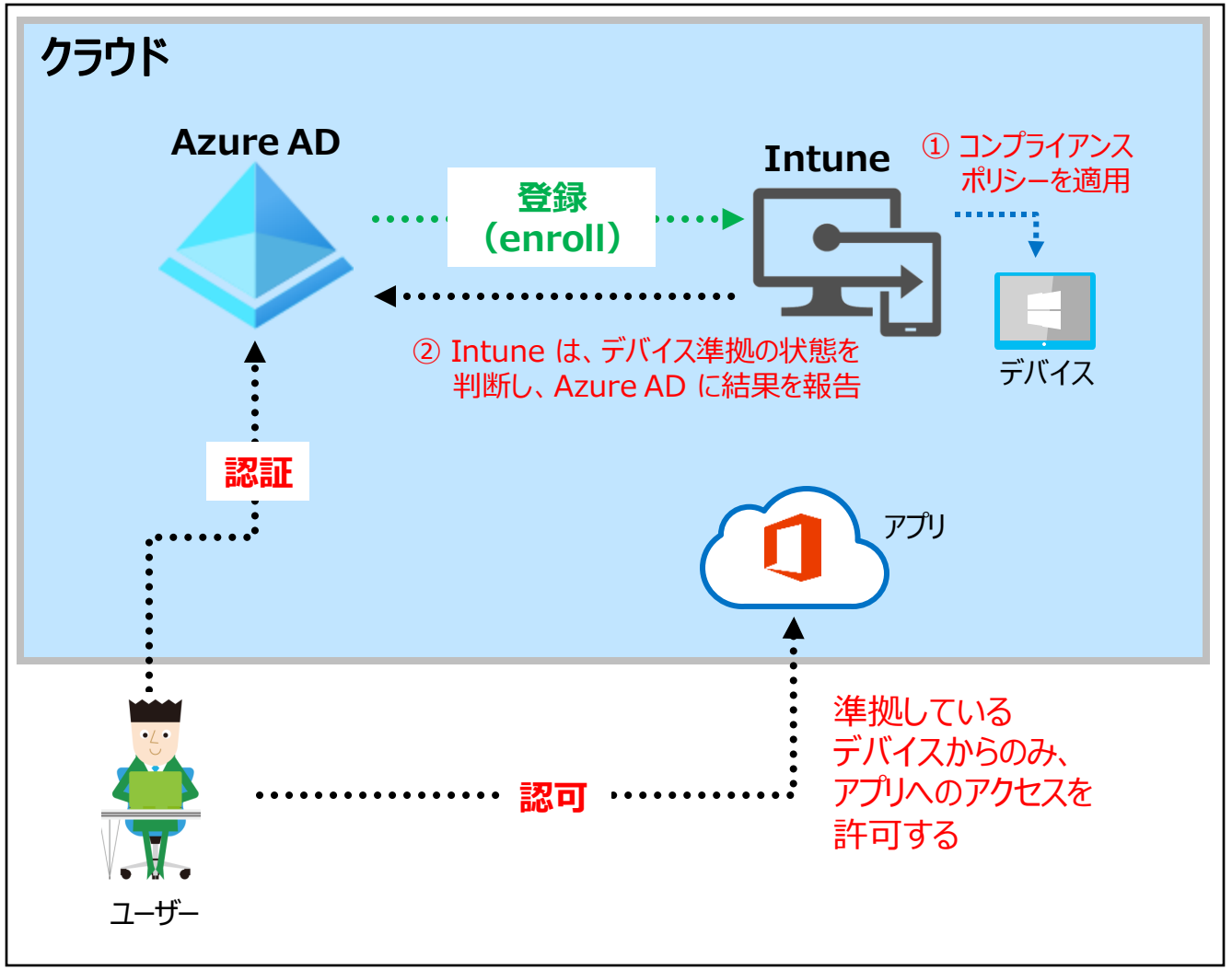
Azure AD Premium P1

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

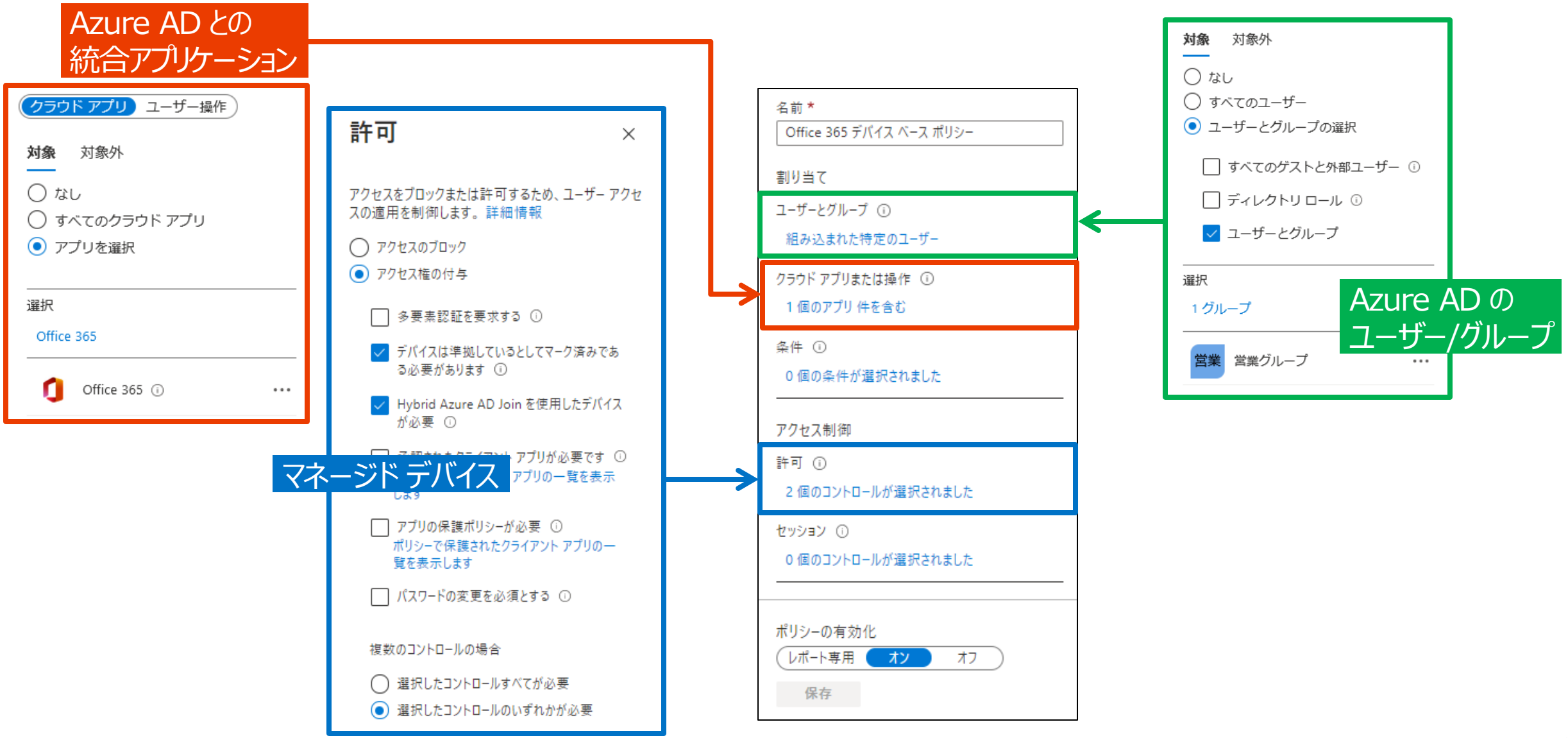
3. アプリケーションに対して、**デバイス ベースの条件付きアクセス** を実行
   - 組織の方針に準拠しているデバイスからのみ、アプリへのアクセスを許可することができる



例）マネージド デバイスからのアクセスを許可

Azure AD Premium P1

Intune

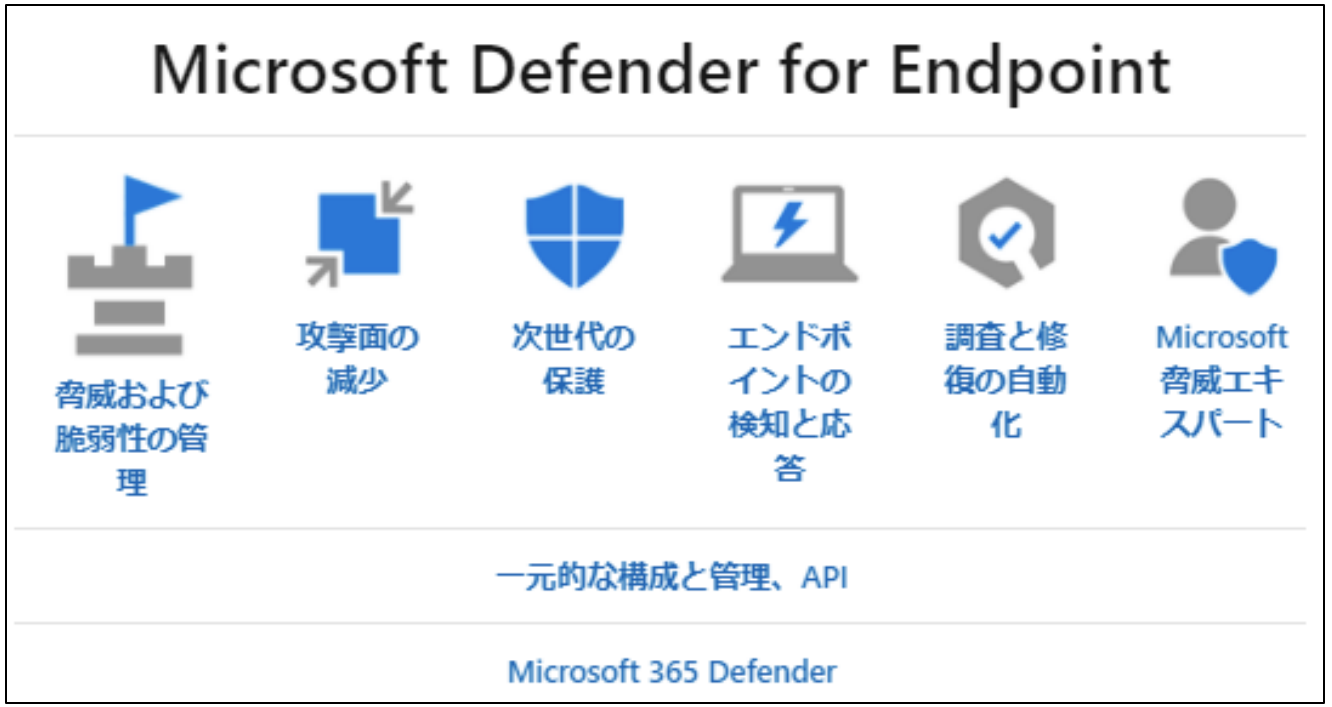


[参考] 技術資料

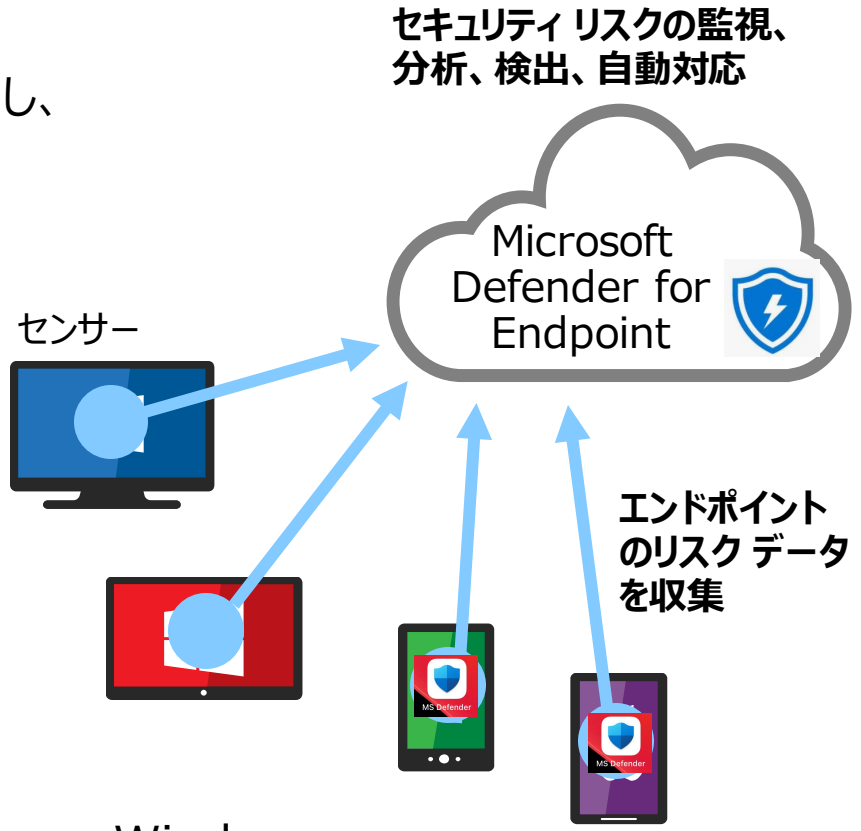
- **マネージド デバイス + Azure AD 条件付きアクセス**
- **「方法:条件付きアクセスを使用してクラウド アプリへのアクセスにマネージドデバイスを要求する」**
  - https://docs.microsoft.com/ja-jp/azure/active-directory/conditional-access/require-managed-devices

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



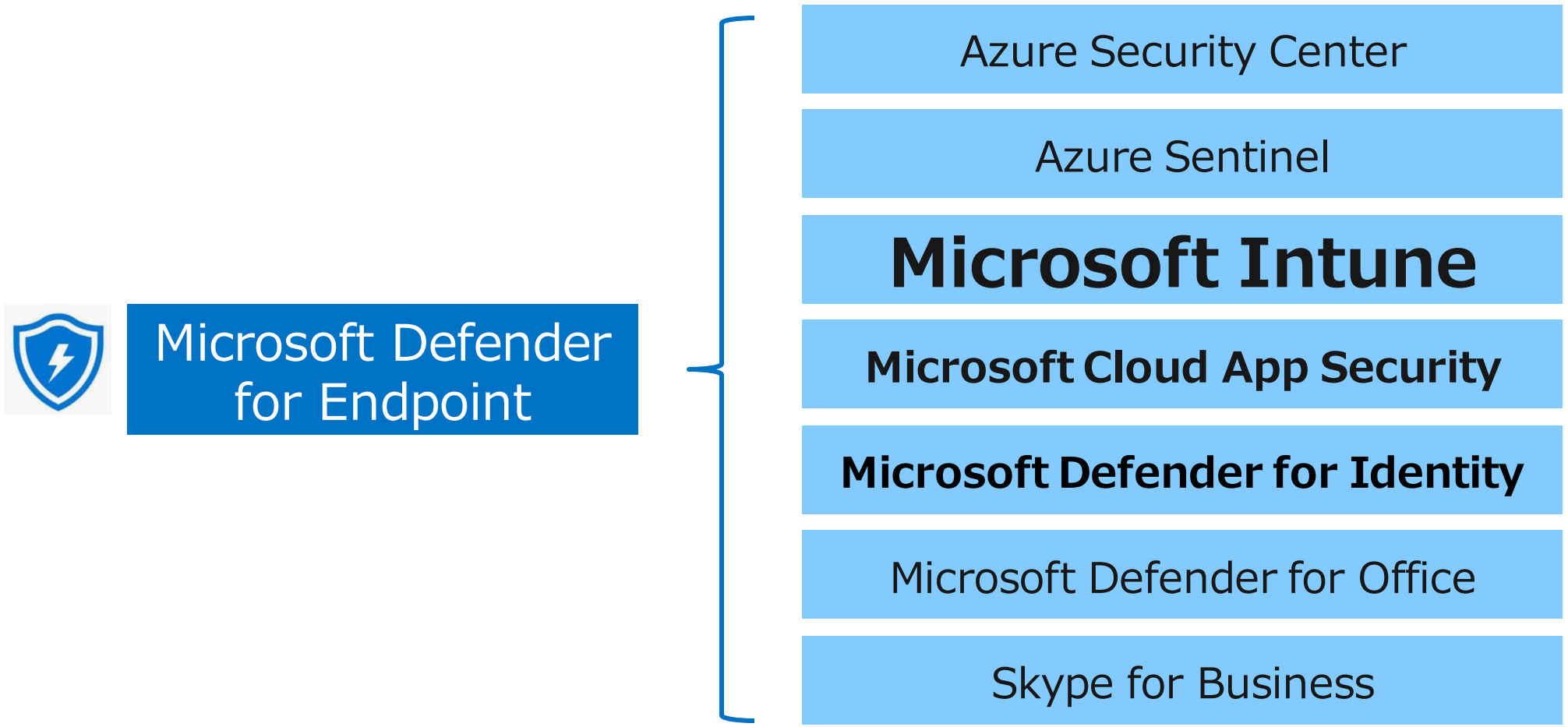
「脅威の防止」より引用
https://docs.microsoft.com/ja-jp/windows/security/threat-protection/



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

Microsoft ソリューションとの連携

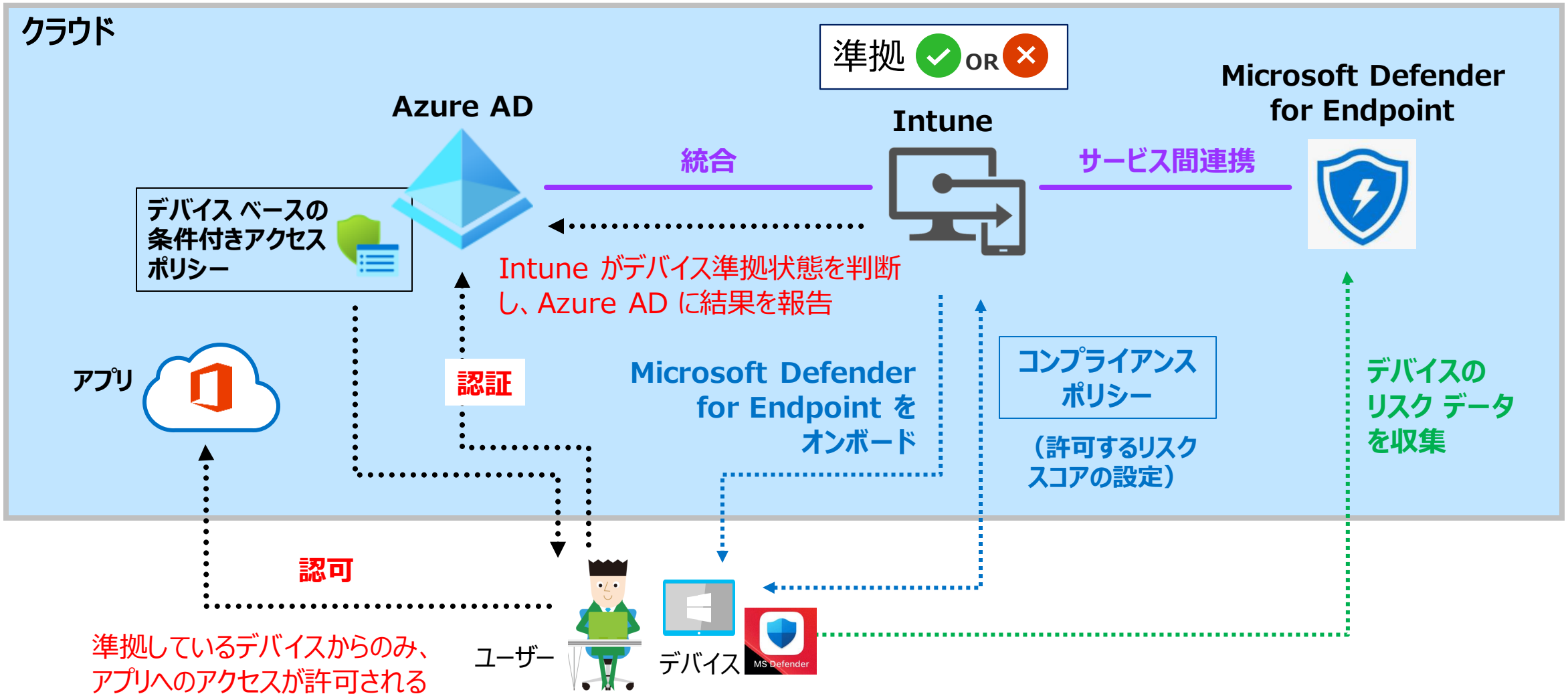
- Microsoft Defender for Endpoint は、
  さまざまな Microsoft ソリューションとの直接統合できる



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

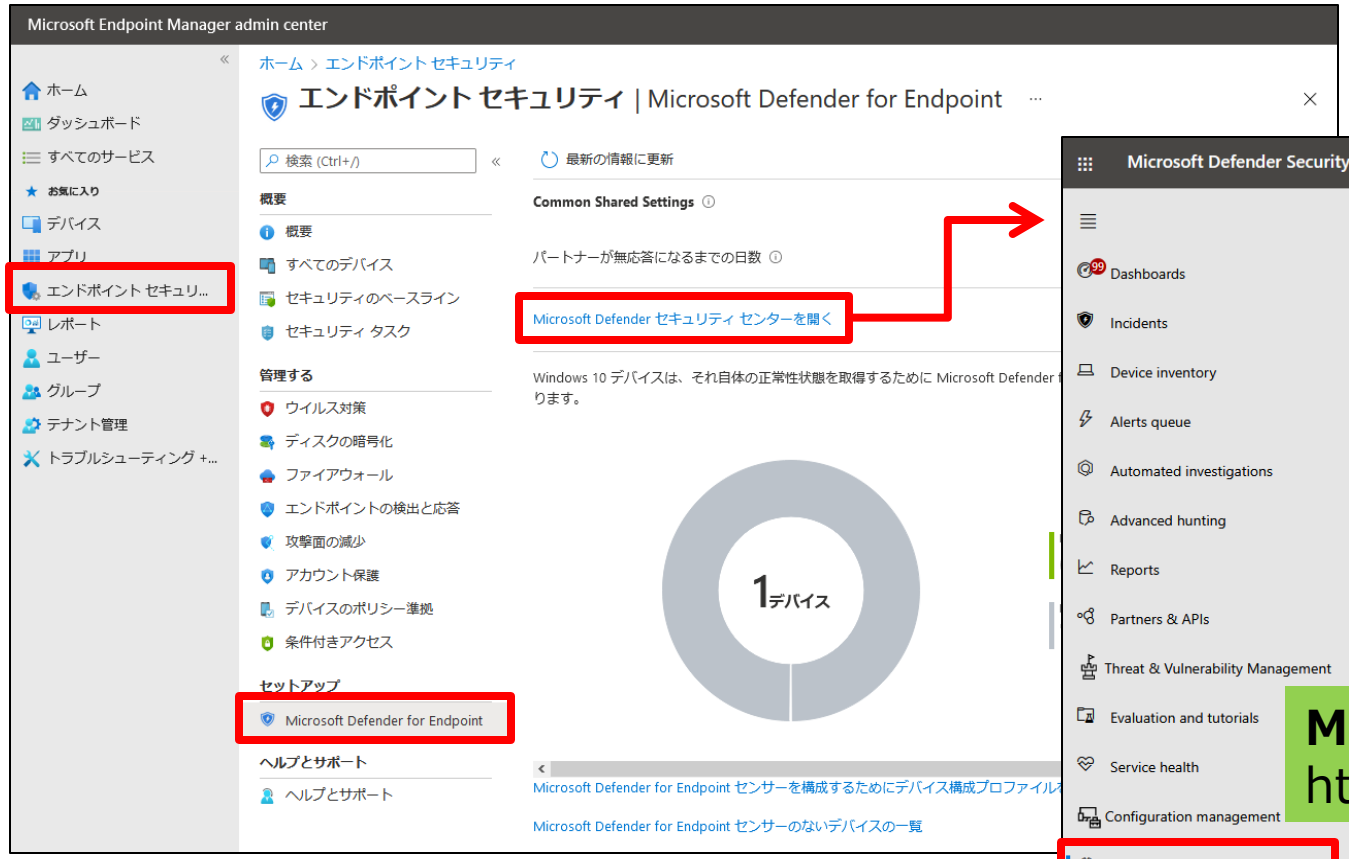
- 構成手順
  - 手順 1. テナントに対する Microsoft Defender for Endpoint の有効化
  - 手順 2. デバイスのオンボード（Microsoft Defender for Endpoint の展開）
  - 手順 3. デバイスのリスク スコアの設定 ・・・ Intune のコンプライアンス ポリシー
  - 手順 4. 高度なデバイス ベースの条件付きアクセス ポリシーの作成
    - 想定したリスク レベルを超えるデバイスからクラウド アプリへのアクセスをブロック

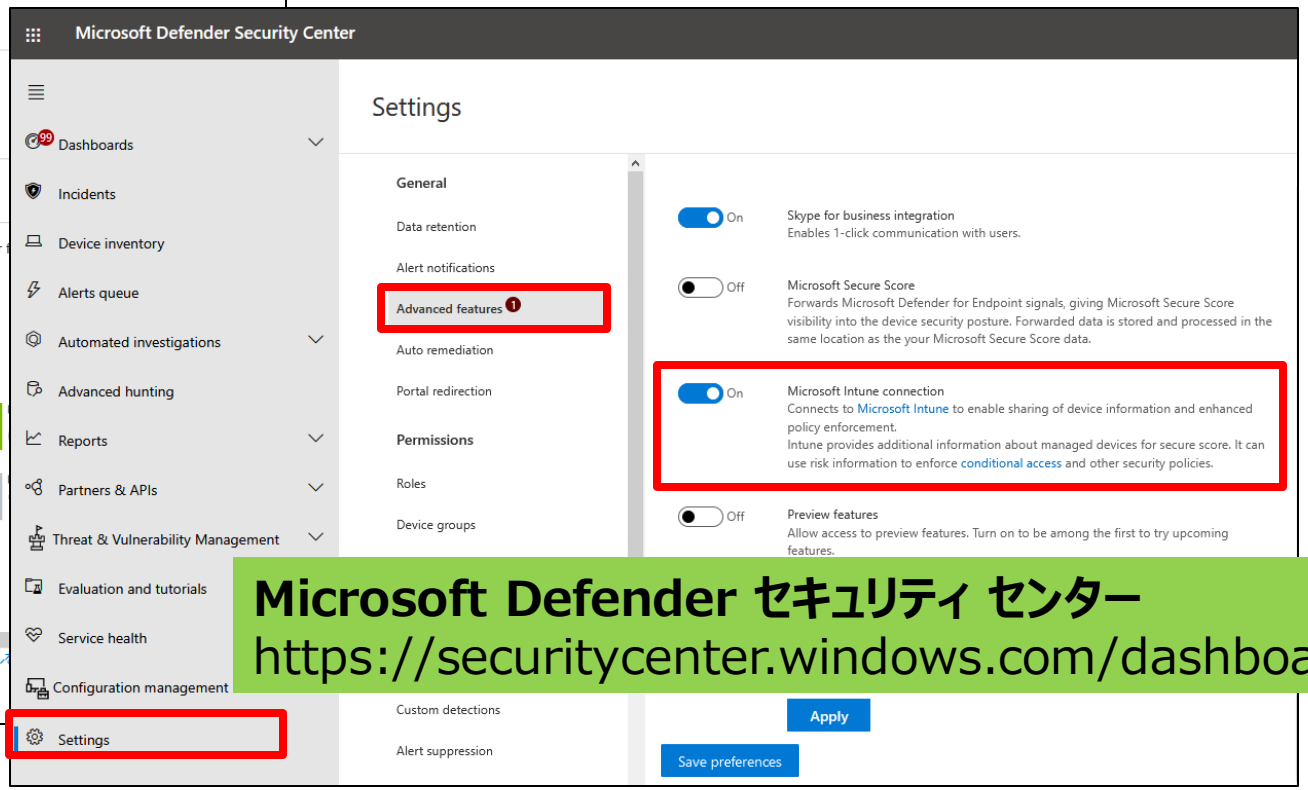
「Intune で Microsoft Defender for Endpoint を構成する」
https://docs.microsoft.com/ja-jp/mem/intune/protect/advanced-threat-protection-configure

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

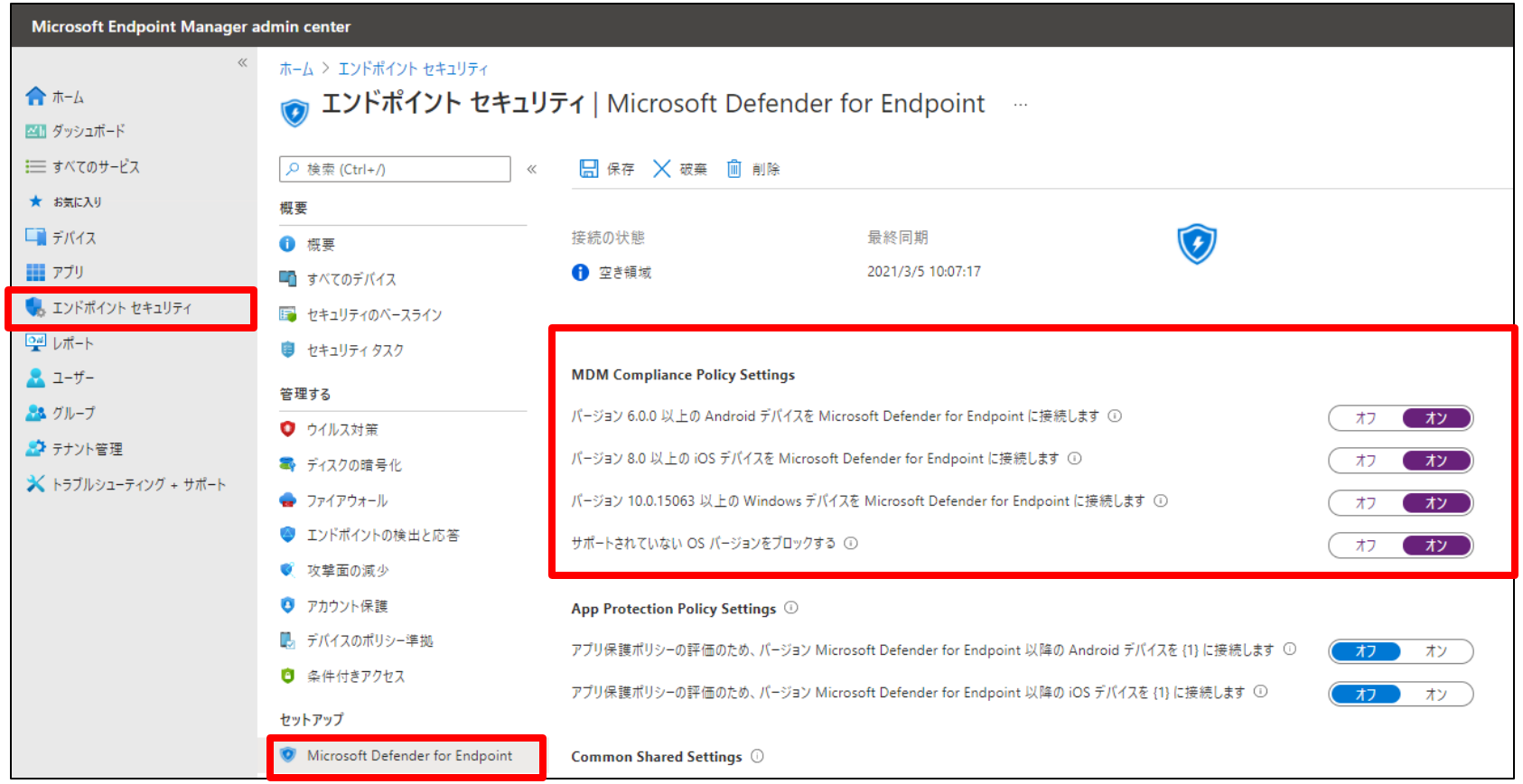




Microsoft Defender セキュリティ センター
https://securitycenter.windows.com/dashboard

(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

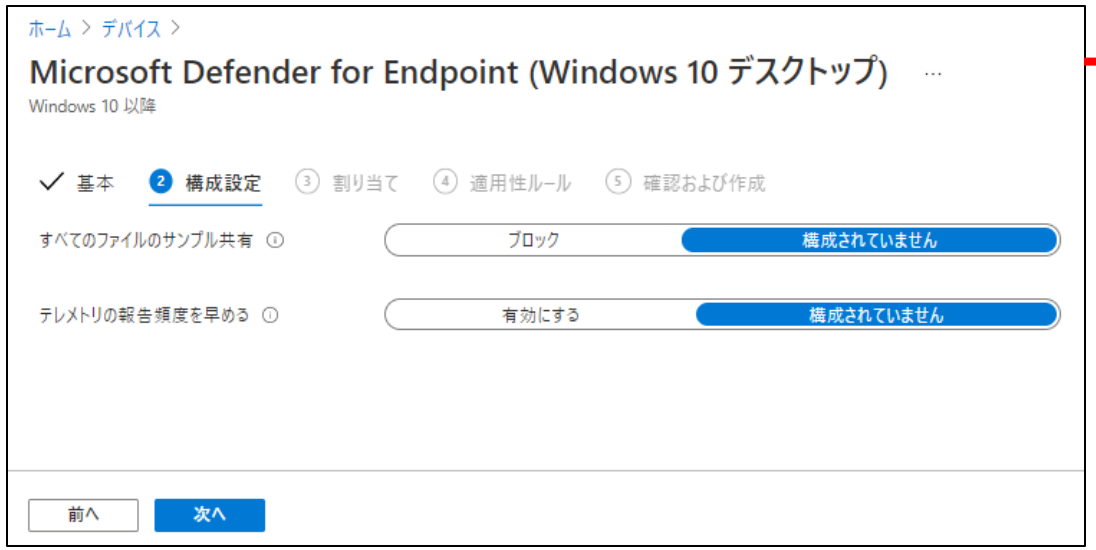


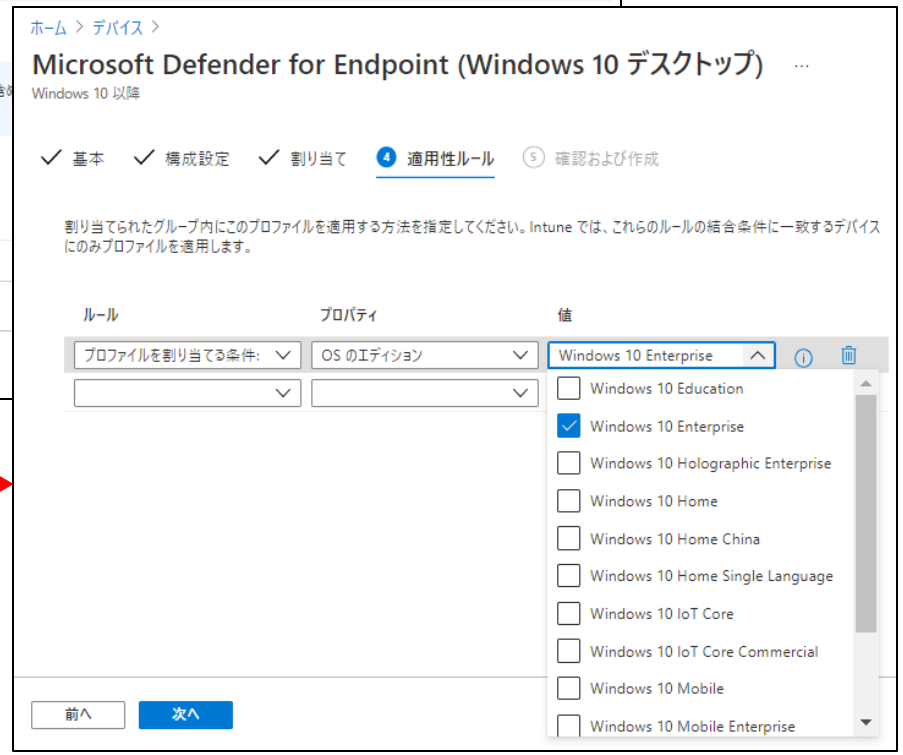
手順 2. デバイスのオンボード（展開）

- 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

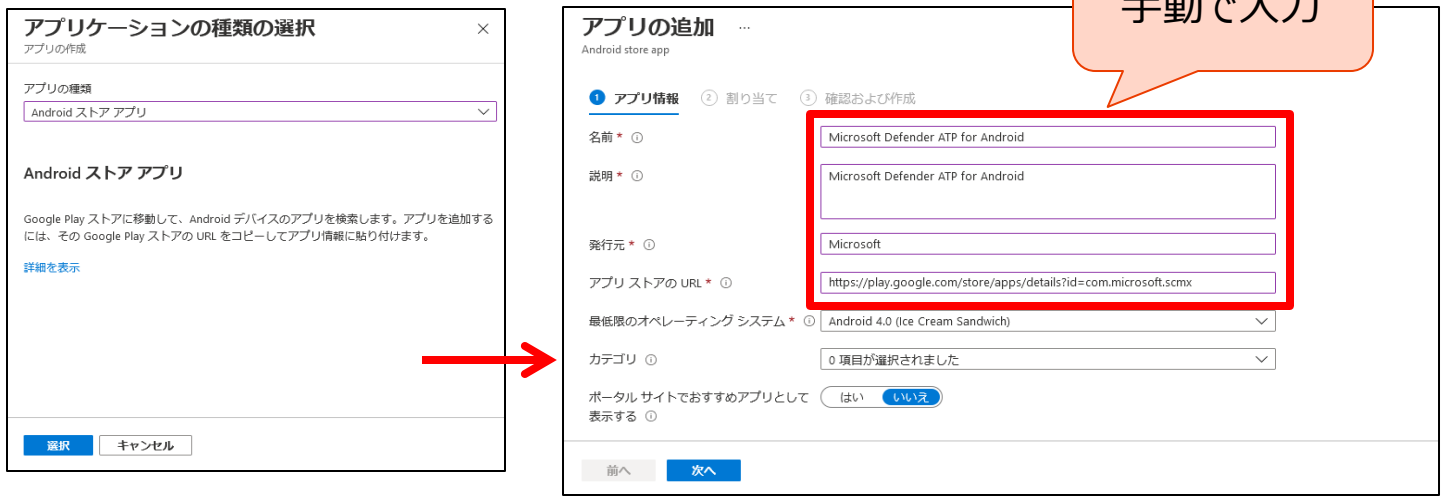
iOS/iPadOS デバイスと Android デバイスのオンボード

- iOS/iPadOS デバイス

アプリ ストア内で検索

オンボードされた Microsoft Defender for Endpoint

- Android デバイス



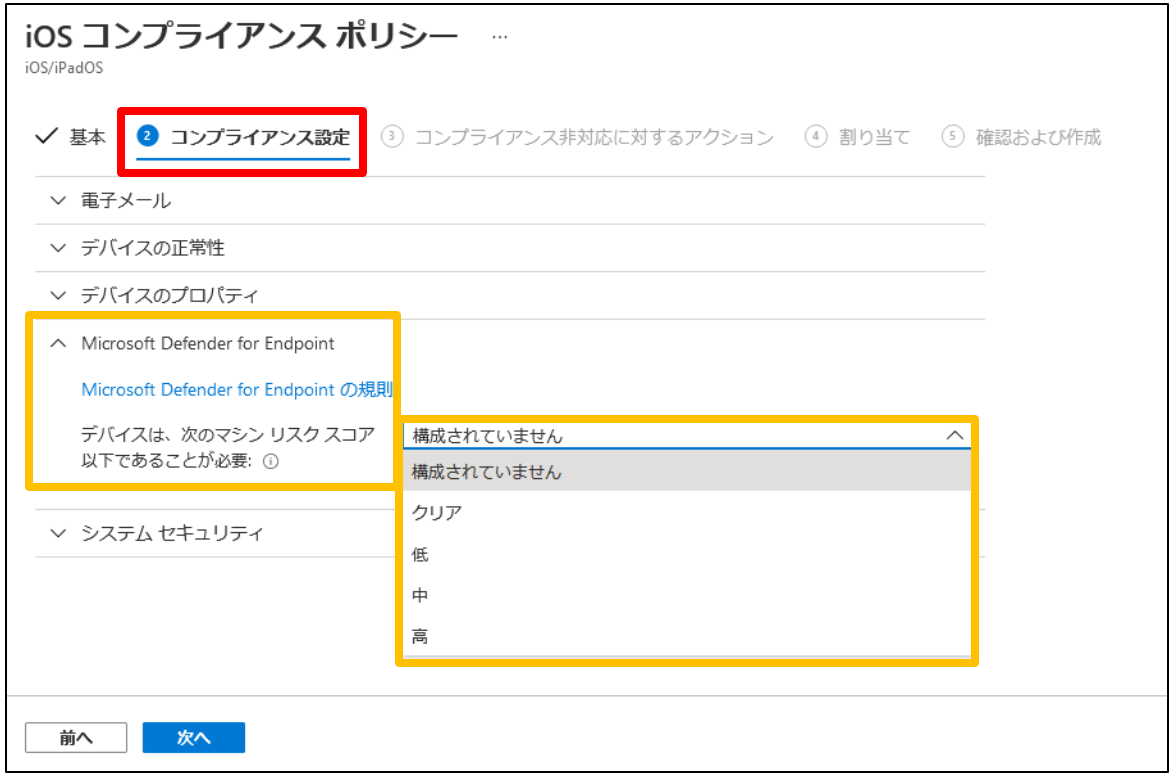
手動で入力

[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

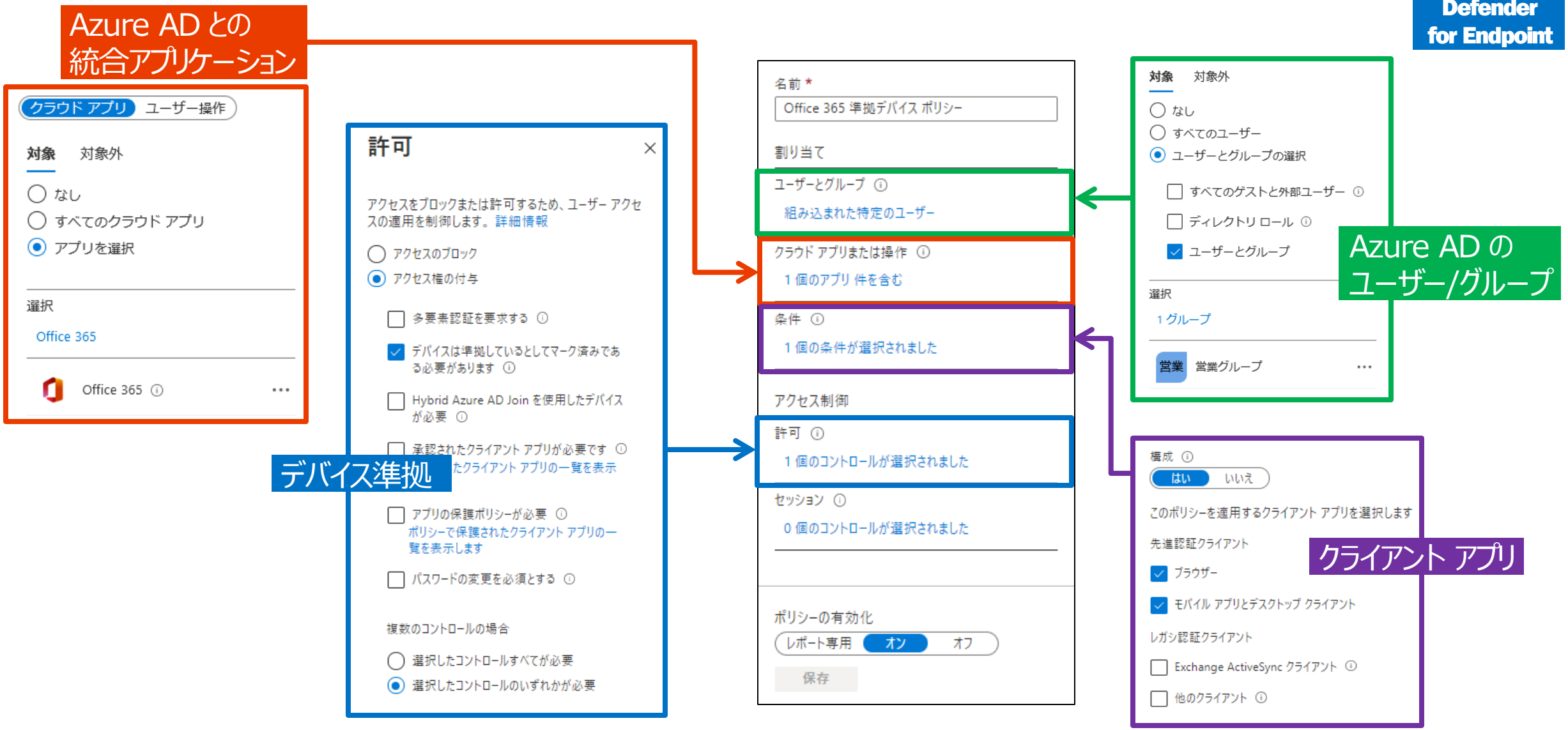


手順 4. 高度なデバイス ベースの条件付きアクセス ポリシーの作成

Azure AD Premium P1

Intune

Microsoft Defender for Endpoint



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

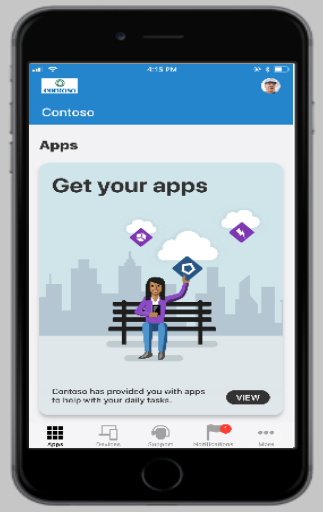
その他のデバイスの登録と構成

- 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



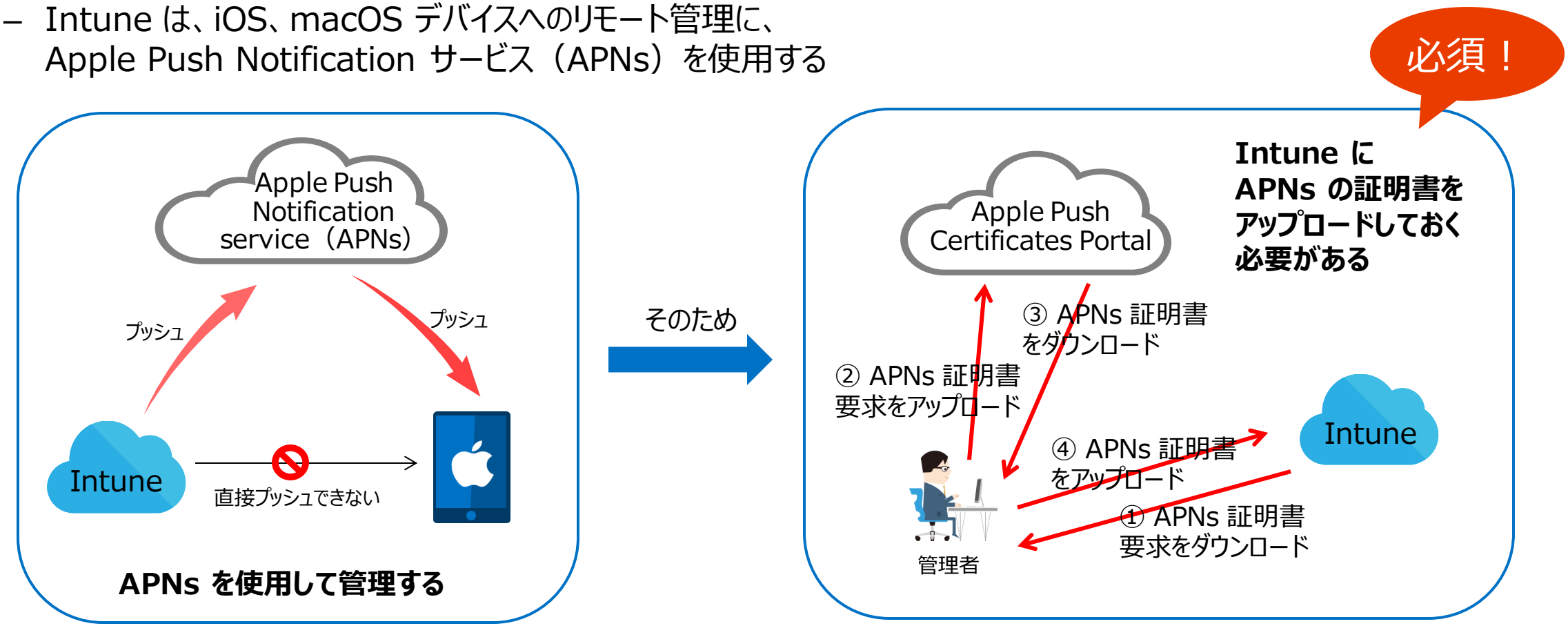
ユーザー所有の iOS/iPadOS デバイス（BYOD）

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



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

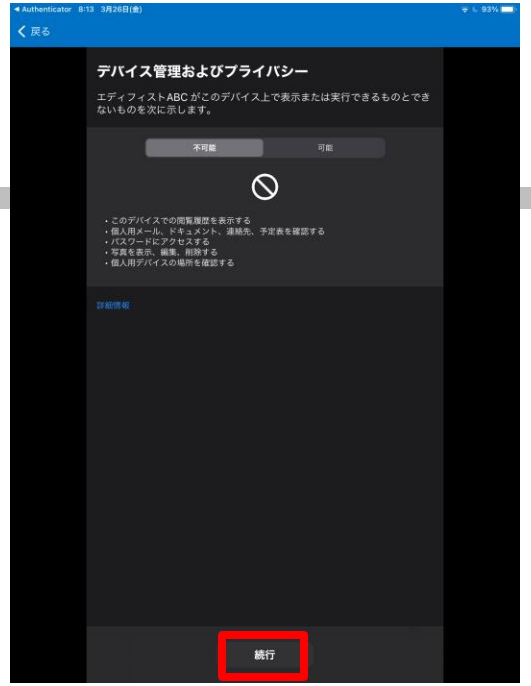
手順 3. 指示にしたがって、デバイスを登録する

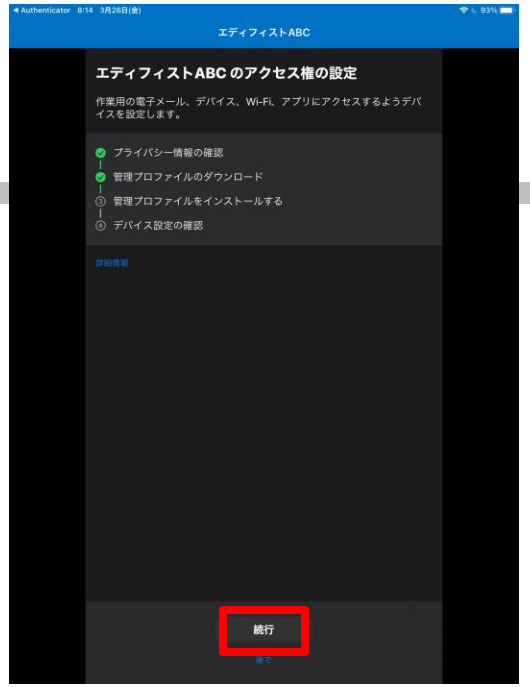
App Store の「Intune ポータル サイト」
https://apps.apple.com/jp/app/intune-%E3%83%9D%E3%83%BC%E3%82%BF%E3%83%AB-%E3%82%B5%E3%82%A4%E3%83%88/id719171358

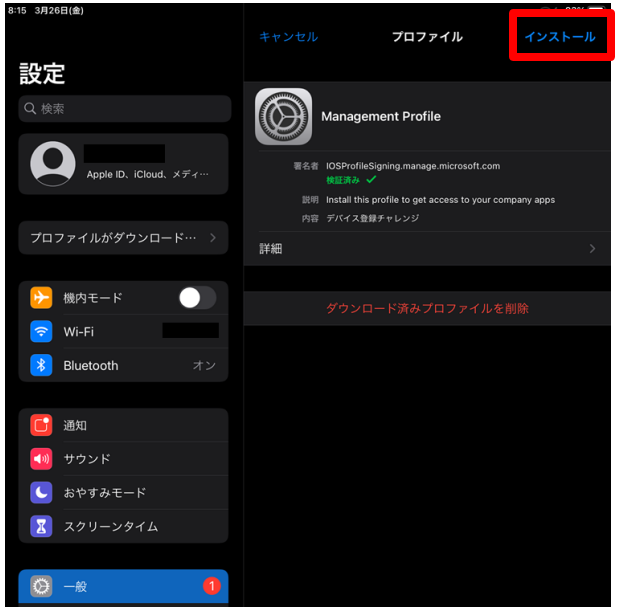
「iOS デバイスからの会社のリソースへのアクセスを設定する」
https://docs.microsoft.com/ja-jp/mem/intune/user-help/enroll-your-device-in-intune-ios

ポータル


エディフィストABC
エディフィストABC のアクセス権の設定
作業用の電子メール、デバイス、Wi-Fi、アプリにアクセスするようデバイスを設定します。
プライバシー情報の確認
管理プロファイルのダウンロード
管理プロファイルをインストールする
デバイス設定の確認
詳細情報
開始


戻る
デバイス管理およびプライバシー
エディフィストABC がこのデバイス上で表示または実行できるものとできないものを次に示します。
不可能
可能
・このデバイスでの閲覧履歴を表示する
・個人用メール、ドキュメント、連絡先、予定表を確認する
・パスワードにアクセスする
・写真を表示、編集、削除する
・個人用デバイスの場所を確認する
詳細情報
続行


エディフィストABC
エディフィストABC のアクセス権の設定
作業用の電子メール、デバイス、Wi-Fi、アプリにアクセスするようデバイスを設定します。
プライバシー情報の確認
管理プロファイルのダウンロード
管理プロファイルをインストールする
デバイス設定の確認
詳細情報
続行


設定
検索
Apple ID、iCloud、メディ…
プロファイルがダウンロード…
機内モード
Wi-Fi
Bluetooth
オン
通知
サウンド
おやすみモード
スクリーンタイム
一般
キャンセル
プロファイル
インストール
Management Profile
署名者 IOSProfileSigning.manage.microsoft.com
検証済み
説明 Install this profile to get access to your company apps
内容 デバイス登録チャレンジ
詳細
ダウンロード済みプロファイルを削除


エディフィストABC
すべての設定が完了しました。
作業用の電子メール、デバイス、Wi-Fi、アプリにアクセスできるようになりました。
プライバシー情報の確認
管理プロファイルのダウンロード
管理プロファイルをインストールする
デバイス設定の確認
詳細情報
完了


エディフィストABC
URAN iPad
名前の変更
デバイスの設定状態
会社のリソースにアクセスできます
最終確認日時
2021年3月26日 10:23
状態の確認
製造元
Apple
モデル
iPad
オペレーティング システム
iOS
所有権の種類
個人
追加の詳細
元の名前
URAN iPad
アプリ
デバイス
サポート
通知
その他


Appのインストール
エディフィストABCによりApp Storeから App "Microsoft Word"がインストールされ、管理されます。
お使いのiTunesアカウントにはこのAppの料金は課金されません。
キャンセル
インストール


Word


MS Defender

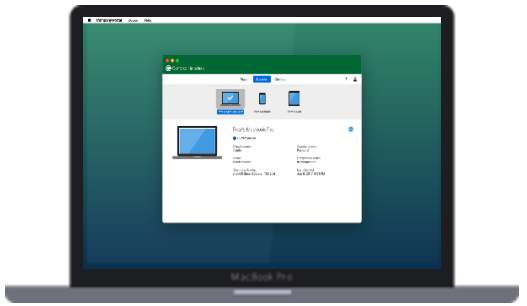

Microsoft Defender for Endp
Web 保護
デバイスは安全です
問題は見つかりませんでした
Web 保護
問題は見つかりませんでした
Web 保護はオンです
Web 保護は、ブラウザベースの攻撃からユーザーを保護するのに役立ちます。
無効にする
この設定は管理者によって管理されています

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

「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

- **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



[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/macos-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 の仕事用プロファイ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る

Android デバイスの登録

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 仕事用プロファイル 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

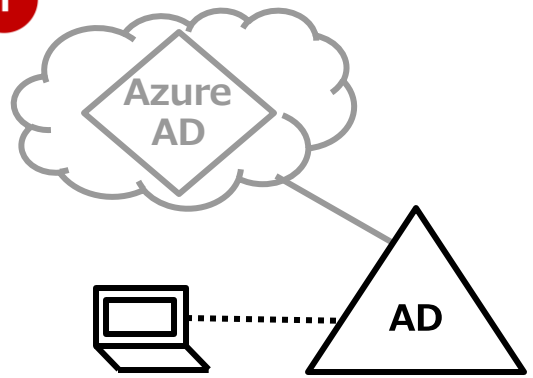
Windows 10 の Azure AD 参加とデバイス登録

- 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

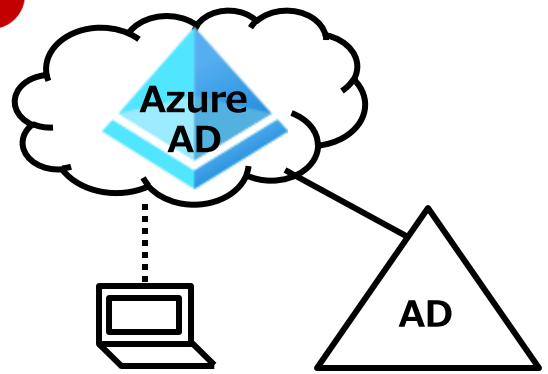
会社所有のデバイス

1



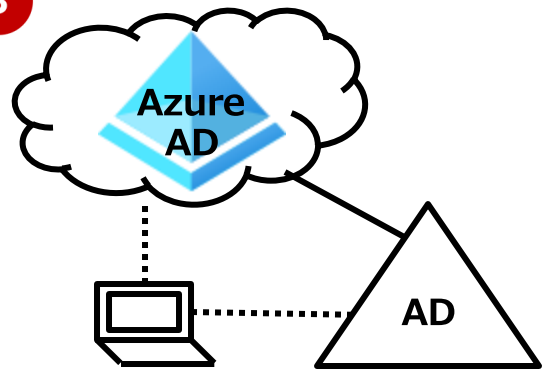
・ドメイン参加
・ConfigMgr 管理

2



・Azure AD 参加
・Intune 管理

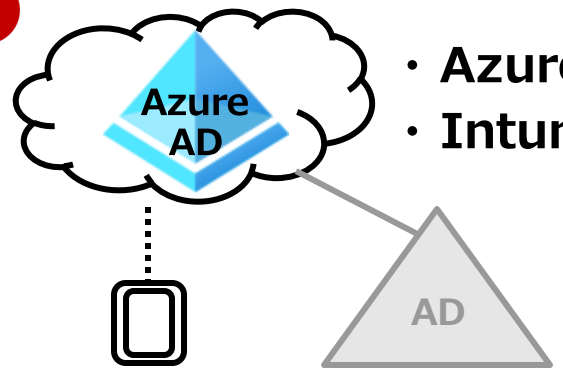
3



・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

4



・Azure AD 登録
・Intune 管理

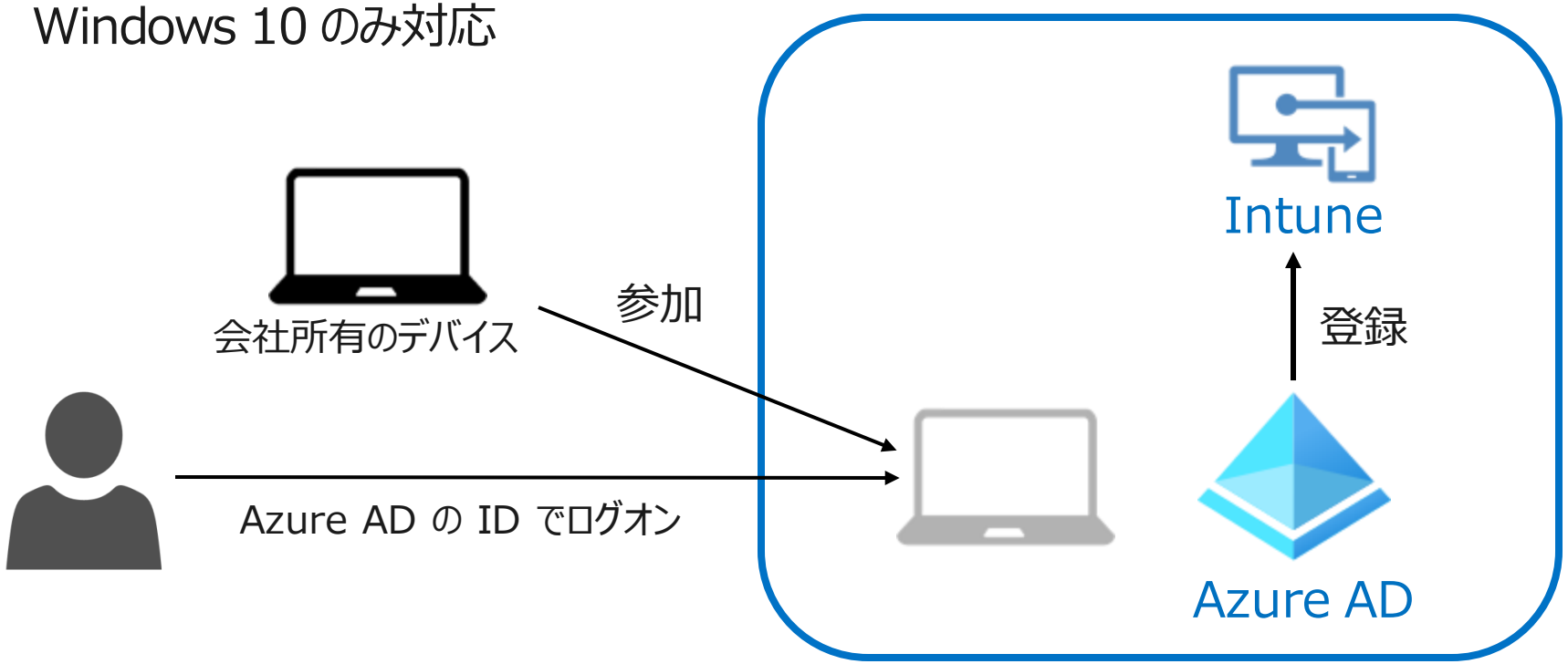
「デバイス ID とは」
https://docs.microsoft.com/ja-jp/azure/active-directory/devices/overview

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 にログオン
- 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-sso

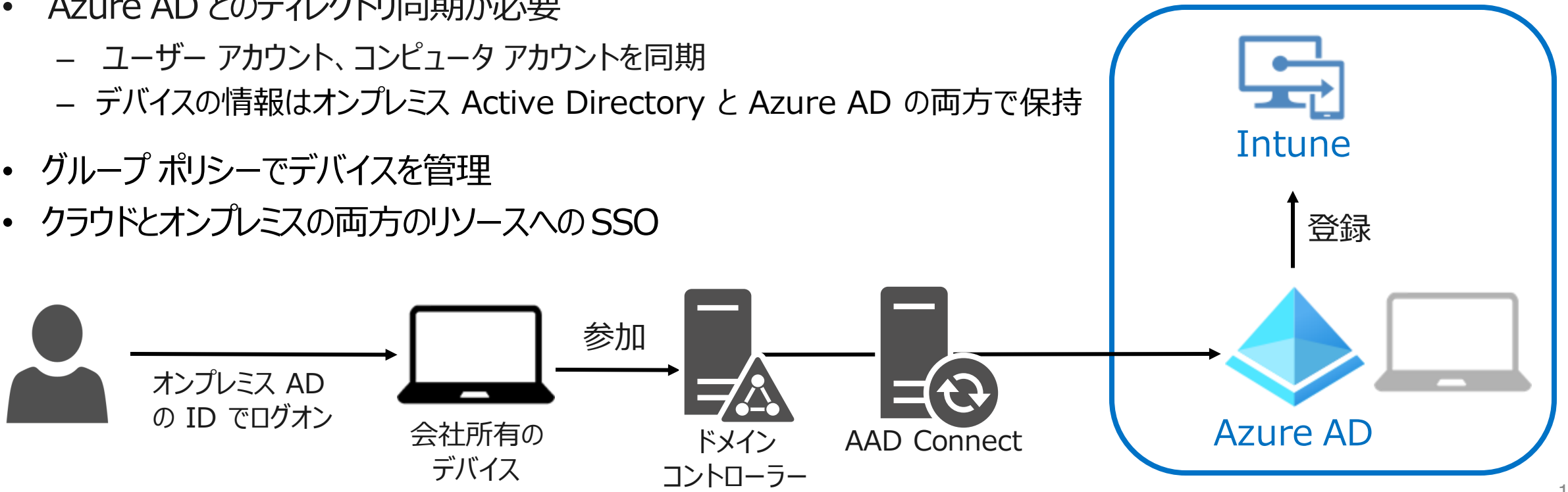


「Azure AD 参加済みデバイス」
https://docs.microsoft.com/ja-jp/azure/active-directory/devices/concept-azure-ad-join

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 にログオン
- 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

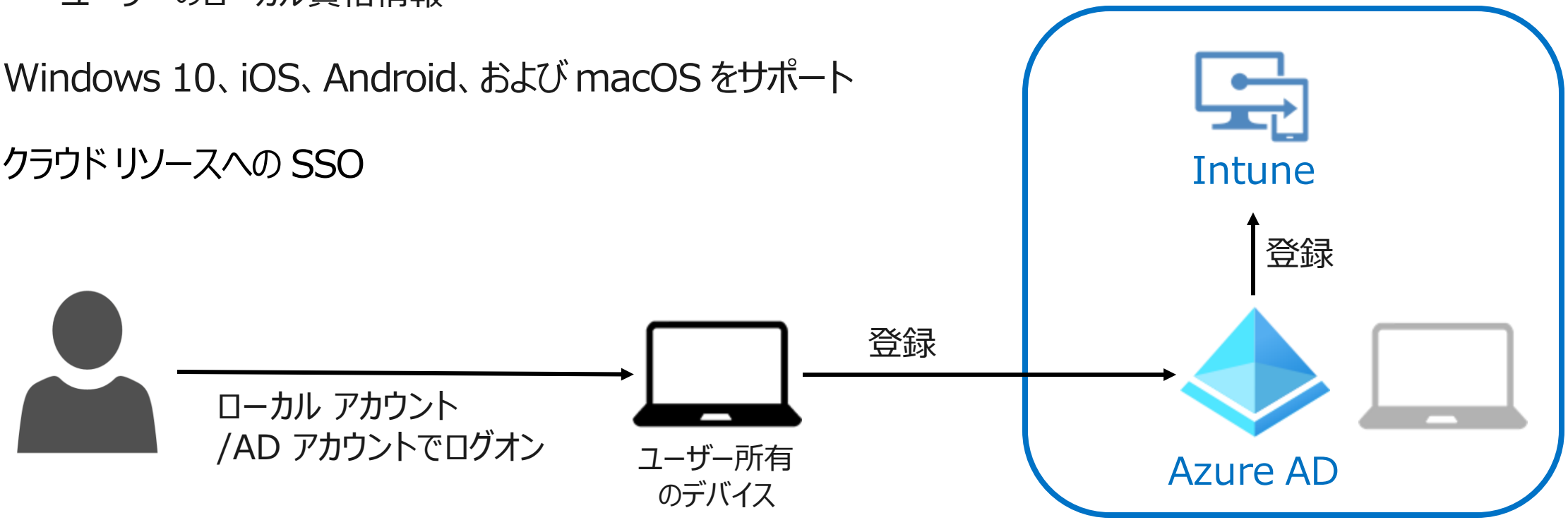
「ハイブリッド Azure AD 参加済みデバイス」
https://docs.microsoft.com/ja-jp/azure/active-directory/devices/concept-azure-ad-join-hybrid



4 Azure AD 登録

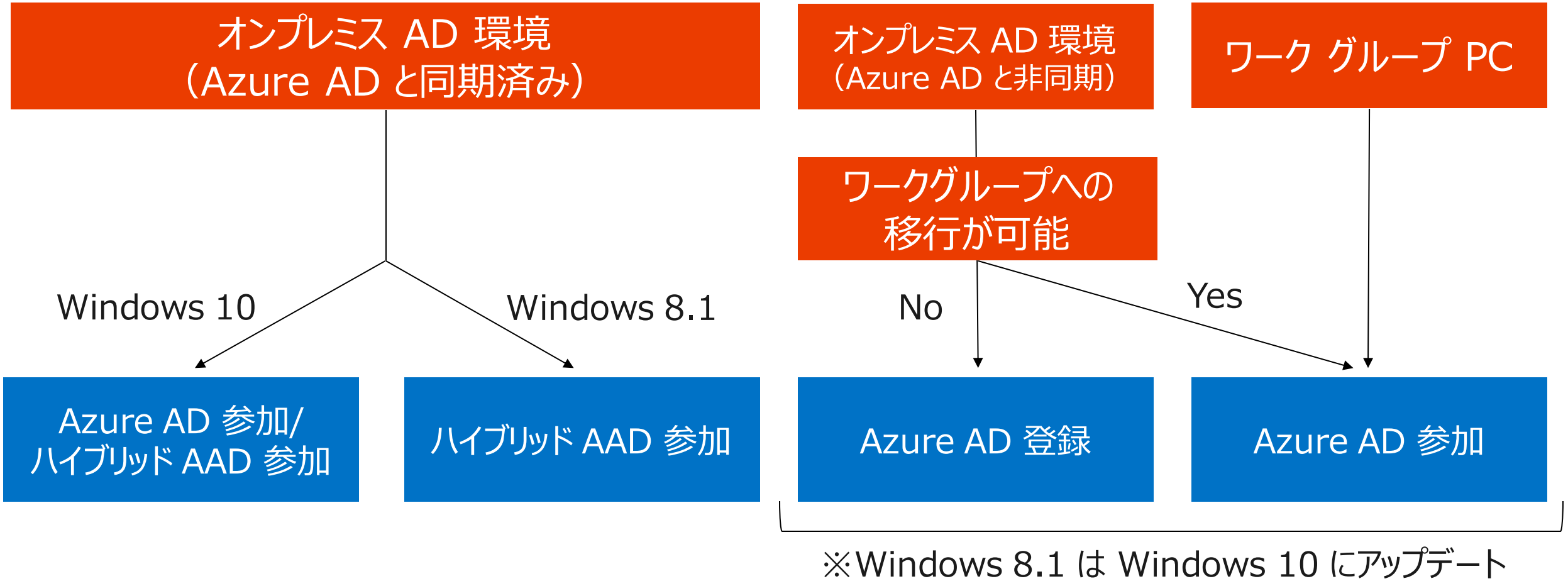
- ユーザー所有デバイス向けのデバイス登録オプション（BYOD）
  - ユーザー所有デバイスを使用して、Azure AD 管理下の組織のリソースにアクセスできるようにする構成
- デバイスへのログオン方法は変わらない
  - ユーザーのローカル資格情報
- Windows 10、iOS、Android、および macOS をサポート
- クラウドリソースへの SSO

「Azure AD 登録済みデバイス」
https://docs.microsoft.com/ja-jp/azure/active-directory/devices/concept-azure-ad-register



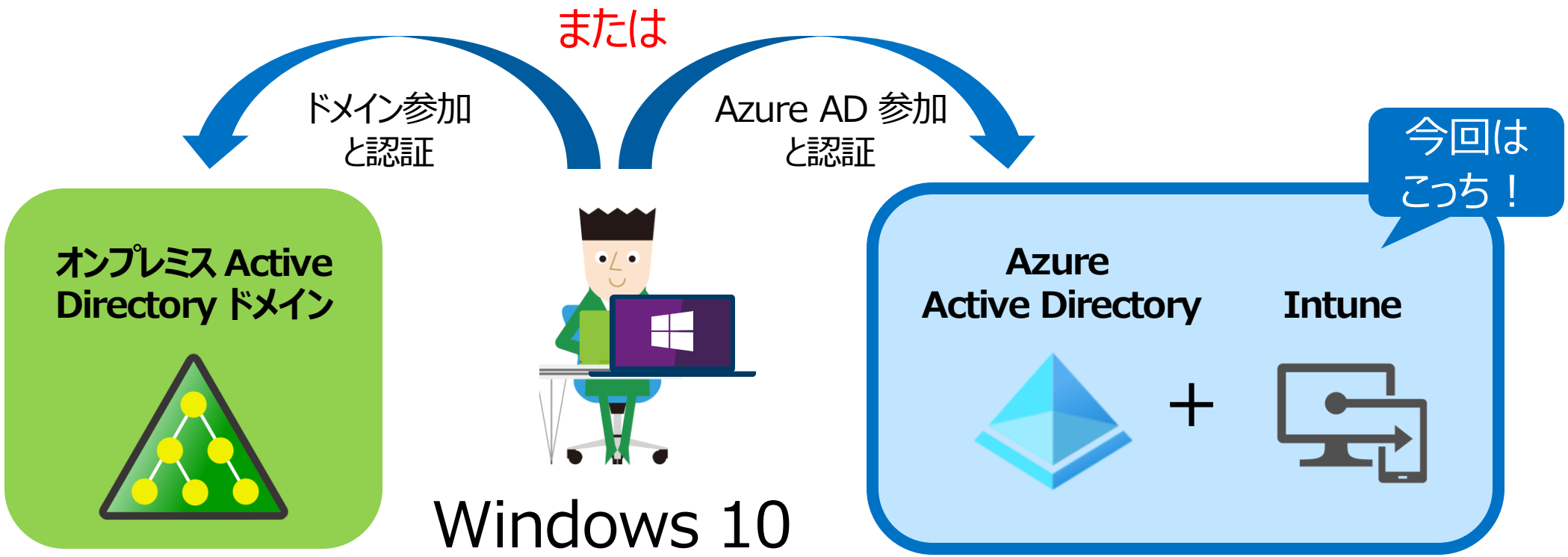
3 つの管理方式の選択

- 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



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



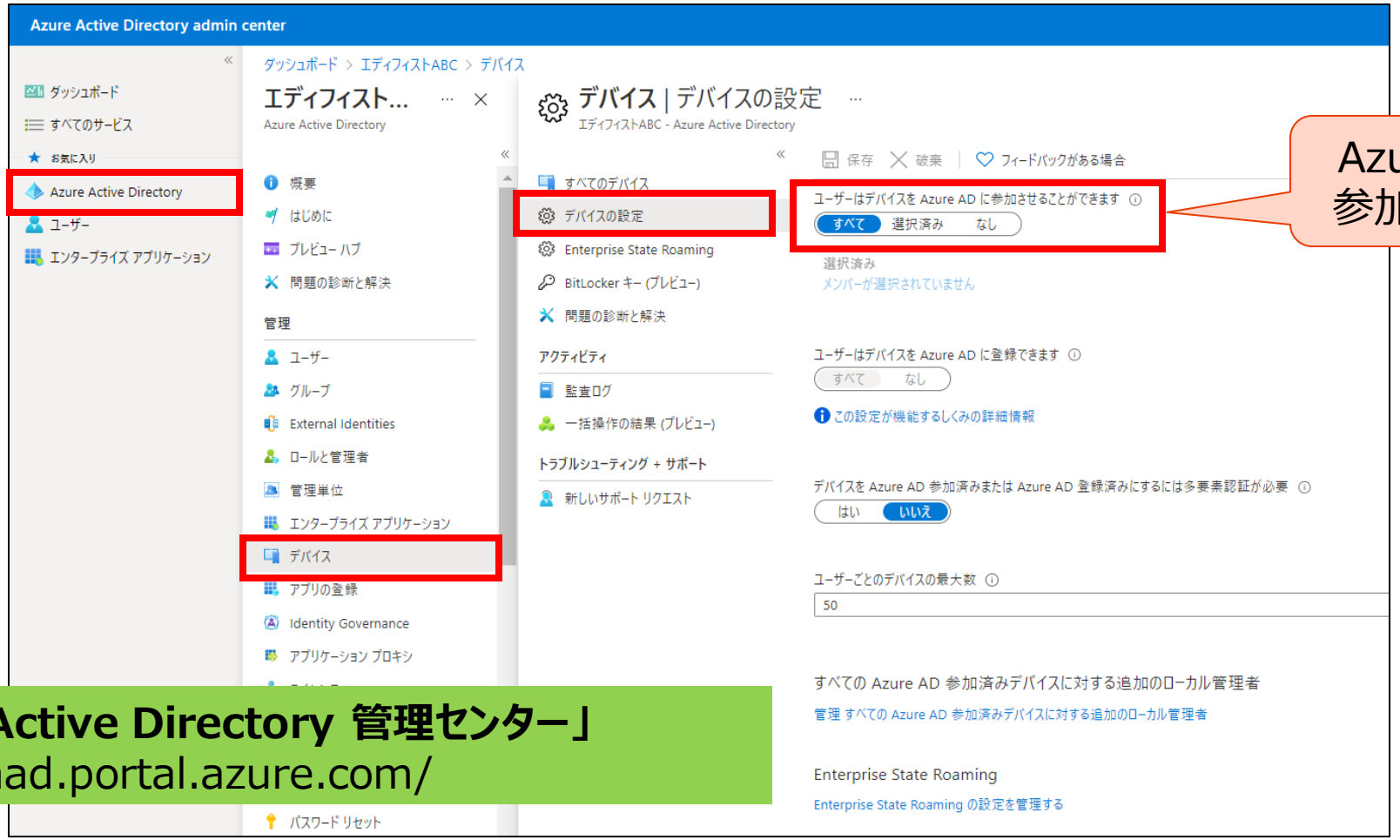
[比較] ドメイン参加と Azure AD 参加

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 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）

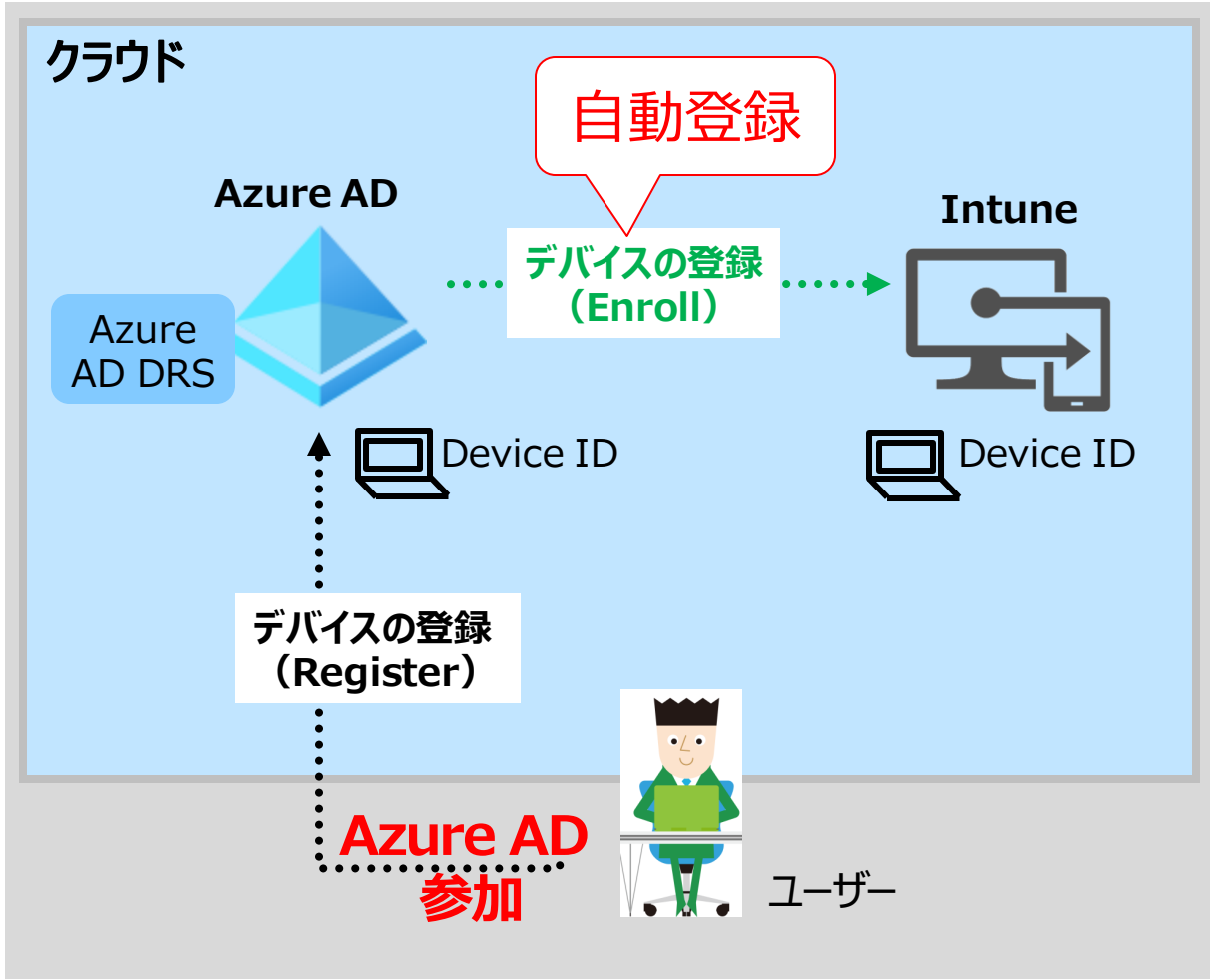
※ デバイス登録制限ポリシーが複数構成されている場合、最も高い優先度のデバイス登録制限が適用される

※ 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

Azure AD Premium P1
Intune

- 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

Azure AD Premium P1

Intune

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

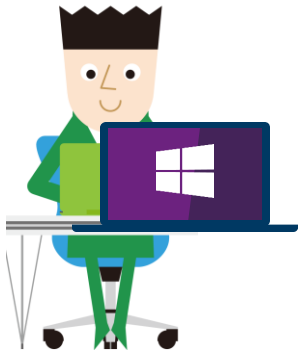
※ 組織が所有するデバイスで、両方のスコープが有効な場合、MDM ユーザー スコープが優先される

※ 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

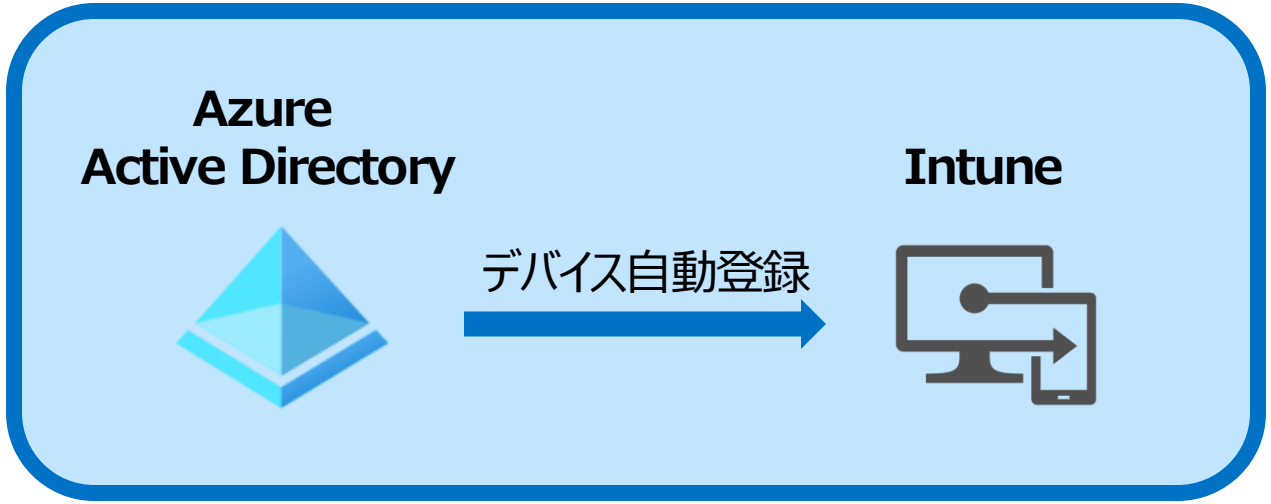
Azure AD 参加とデバイス登録の実行
ユーザー操作

- 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



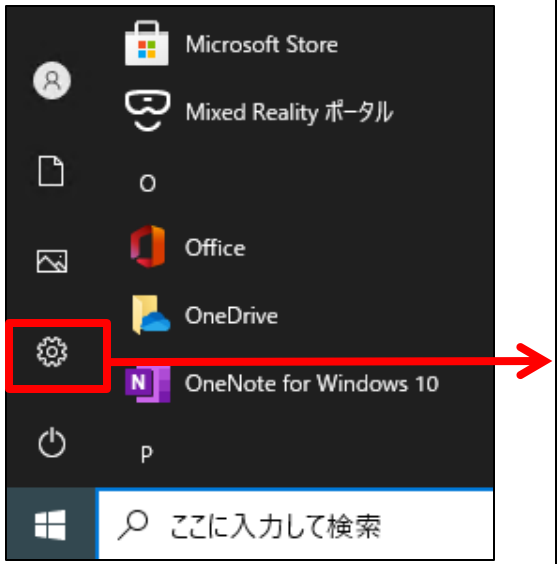
Windows 10

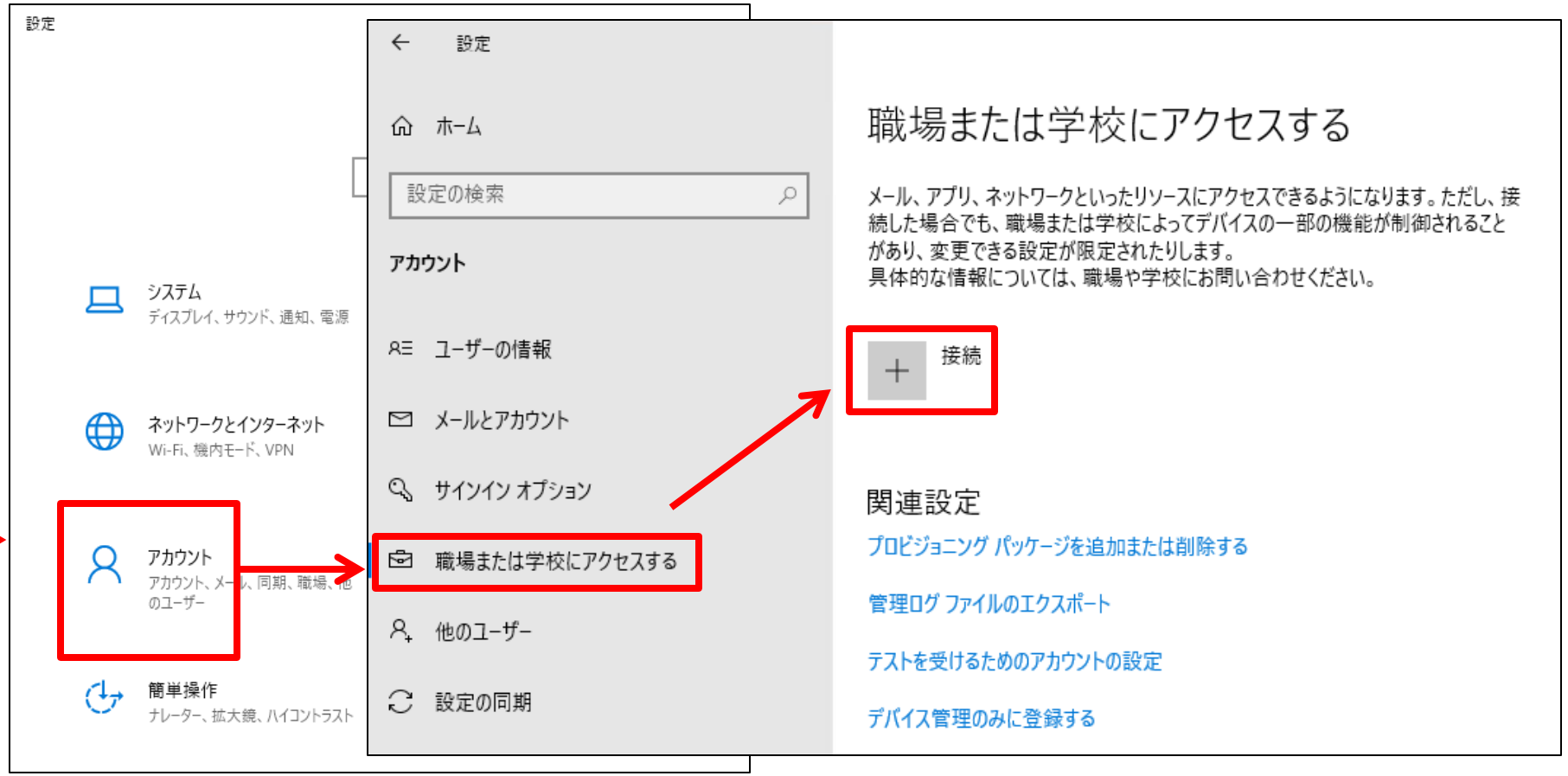


① Azure AD への参加　1/3

ユーザー操作

- 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]

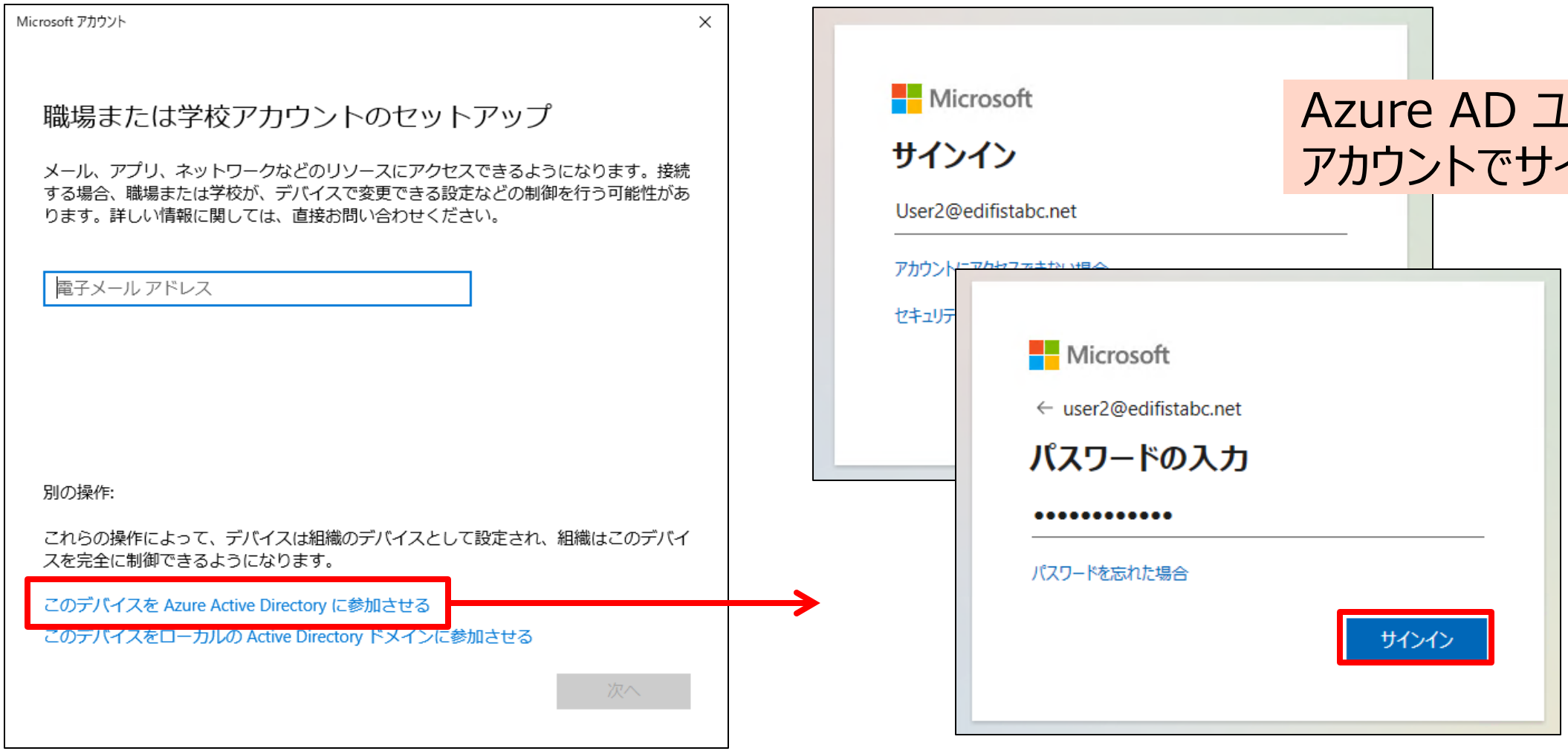




① Azure AD への参加　2/3

ユーザー操作

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

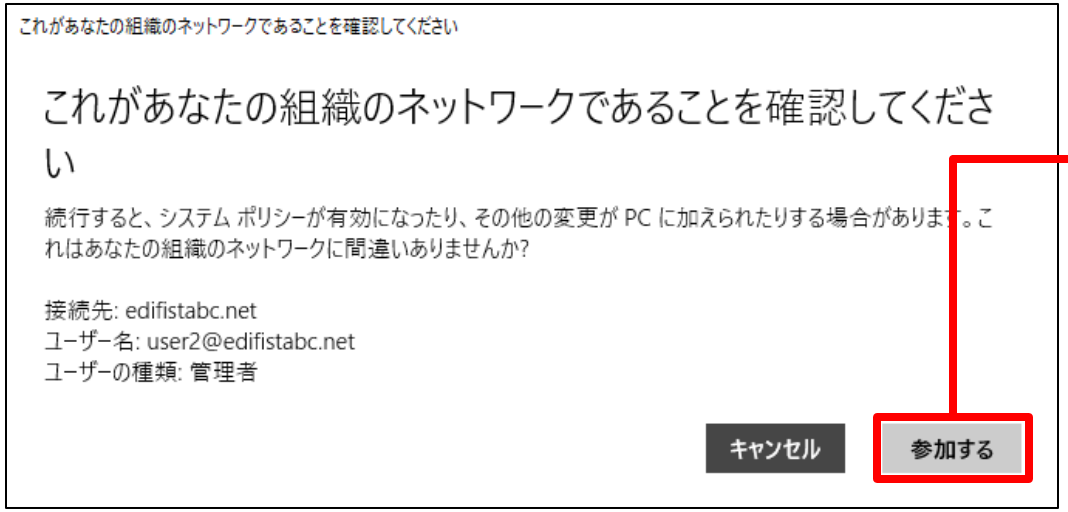


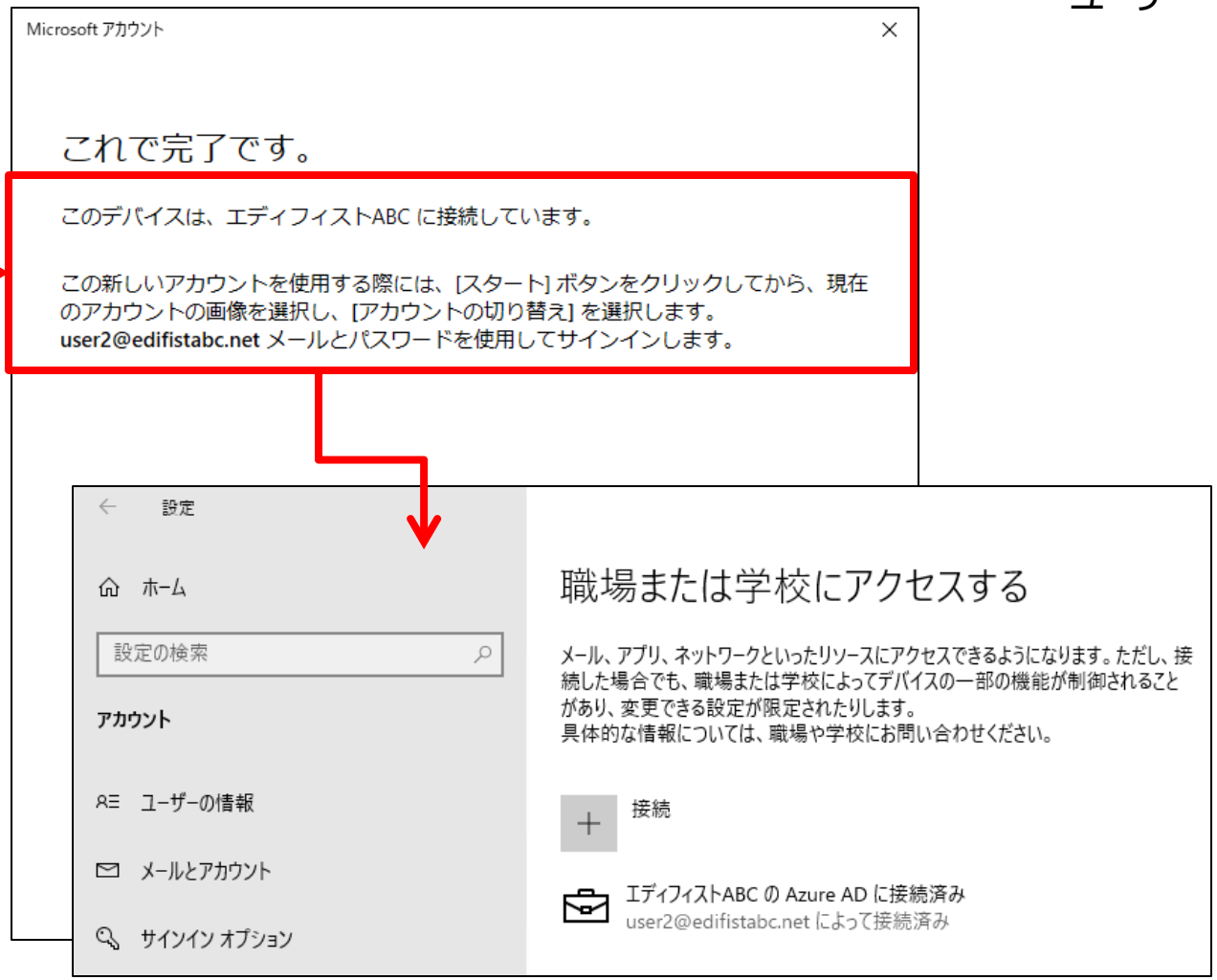
① Azure AD への参加　3/3

ユーザー操作

ユーザー

- [参加する] をクリック

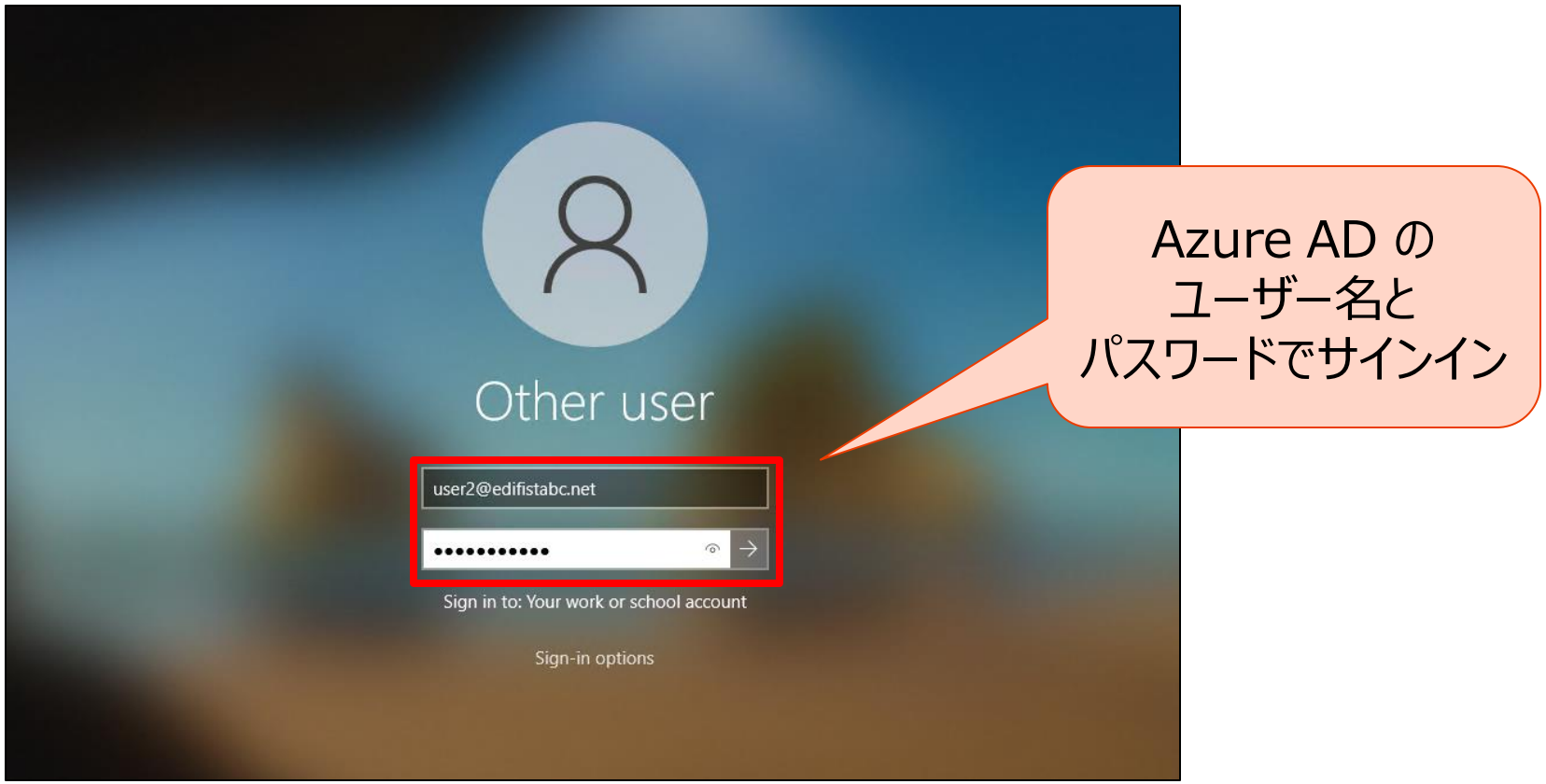




② Azure AD へのサインイン

ユーザー操作

- 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



[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

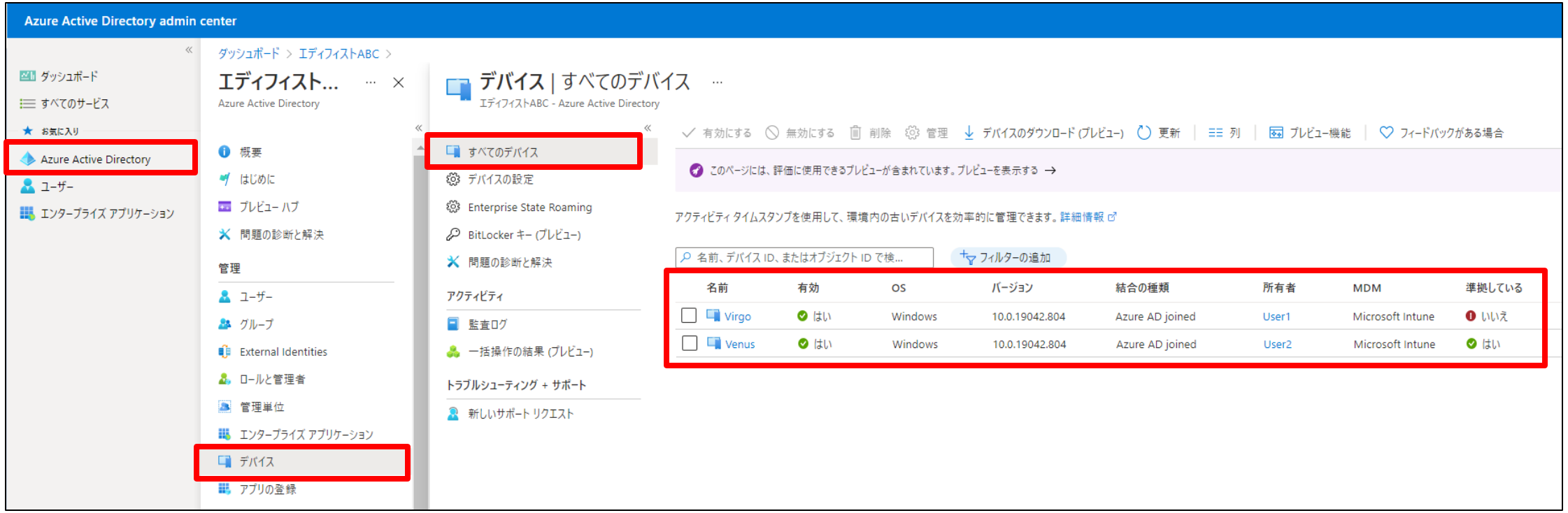
- プロキシ経由でインターネットにアクセスする必要がある組織の場合は、
  Web プロキシ自動発見（WPAD）を構成する

「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



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

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）

ユーザー

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

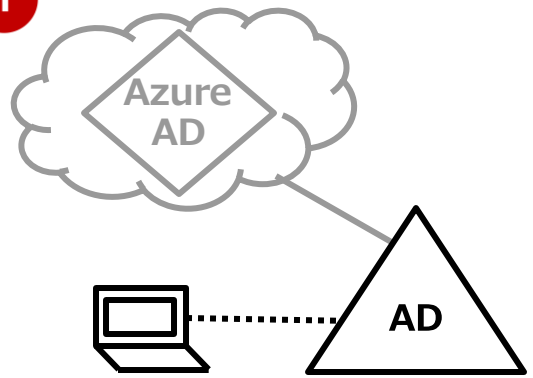
1 デバイス ベースの条件付きアクセス

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

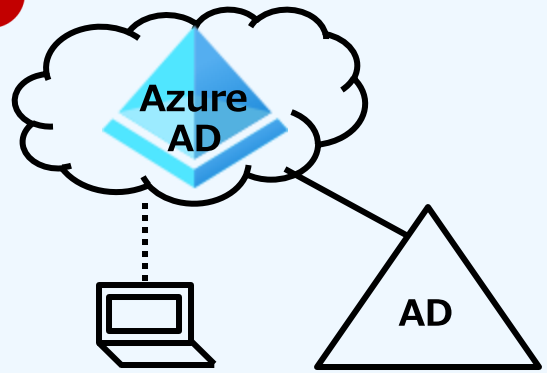
ユーザー所有のデバイス

1



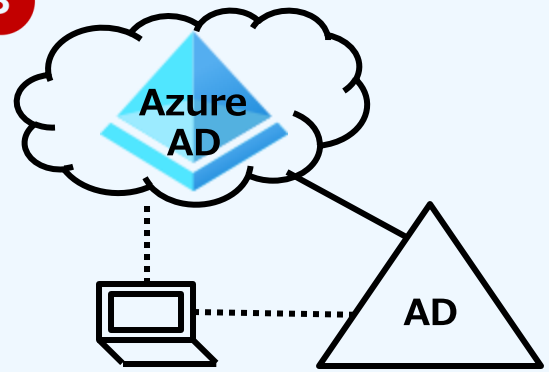
・ドメイン参加
・ConfigMgr 管理

2



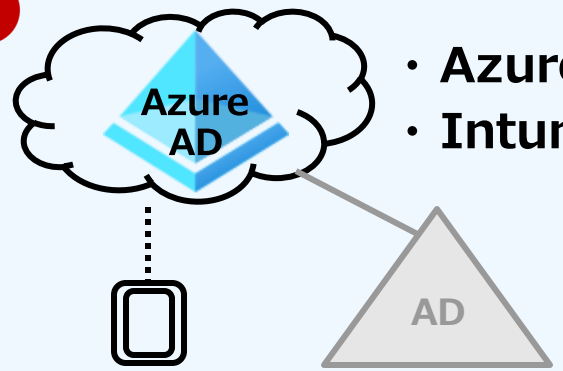
・Azure AD 参加
・Intune 管理

3



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

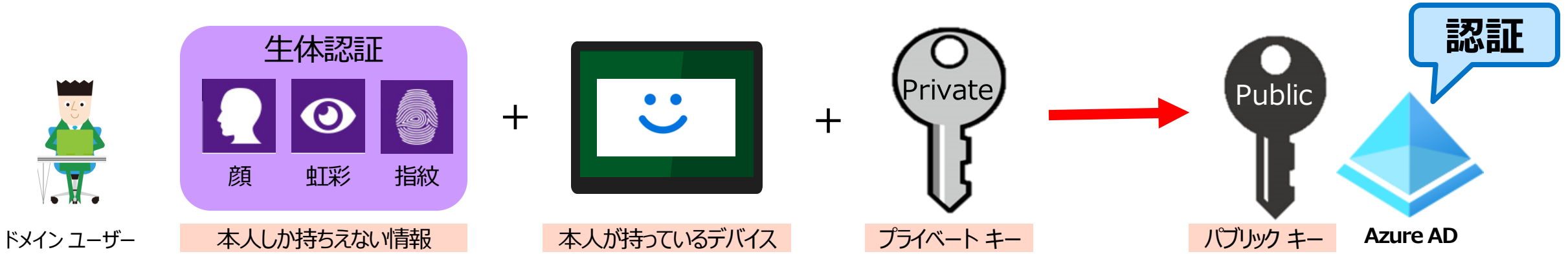
4

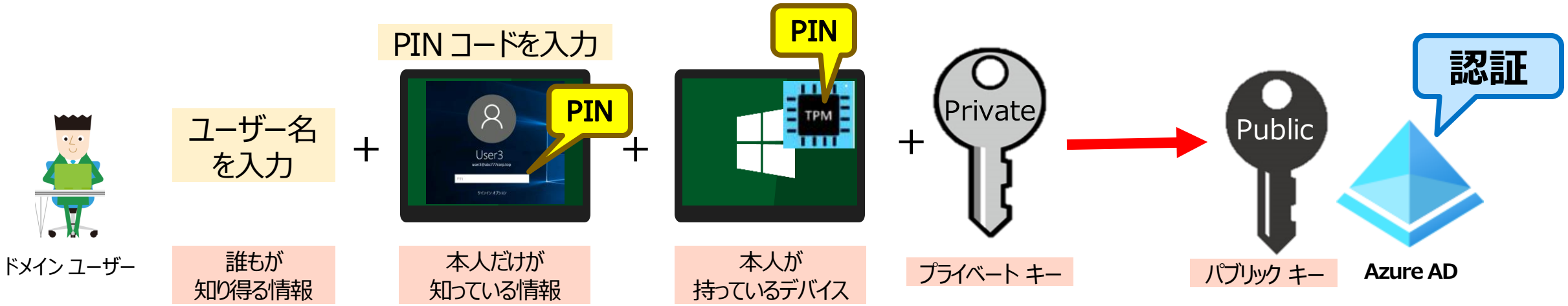


・Azure AD 登録
・Intune 管理

2 Windows Hello for Business による認証の強化

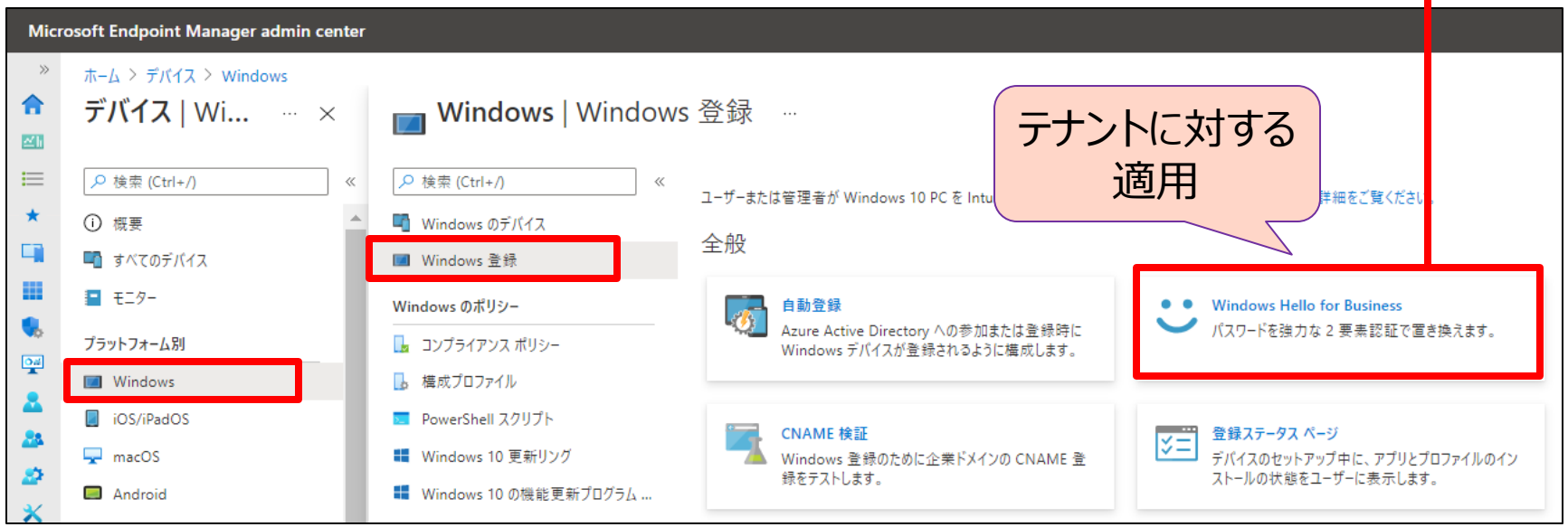
- 生体（または PIN）および キー ペア を使用する、Windows 10 の認証機能
  - パスワードを使用しない認証





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

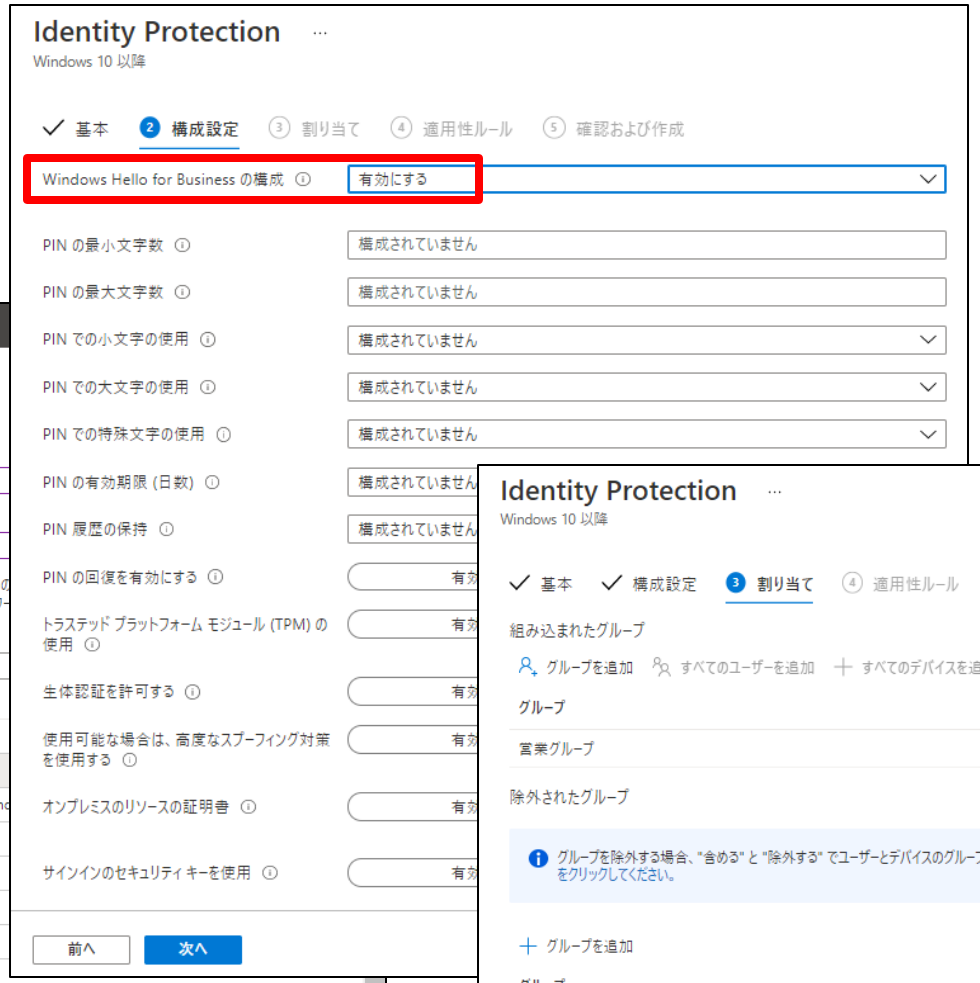


「Windows Hello for Business」
https://docs.microsoft.com/ja-jp/windows/security/identity-protection/hello-for-business/hello-overview

「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）

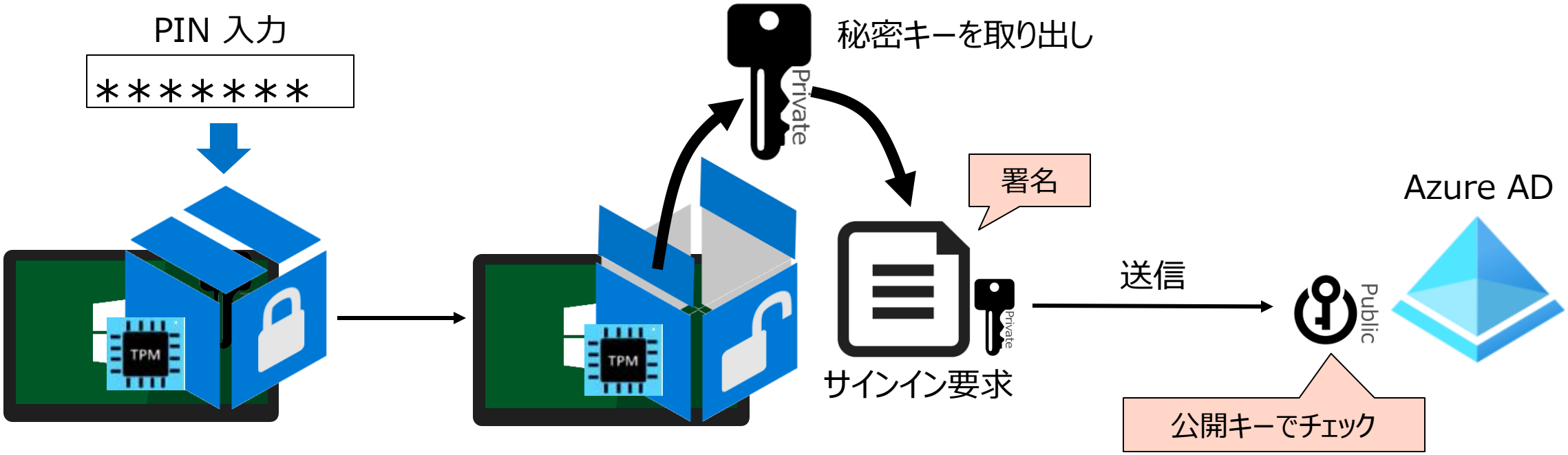
- Microsoft Intune の [デバイス] – [構成プロファイル] の作成で、「Windows 10 以降」プラットフォームの「Identity Protection」テンプレートを選択



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

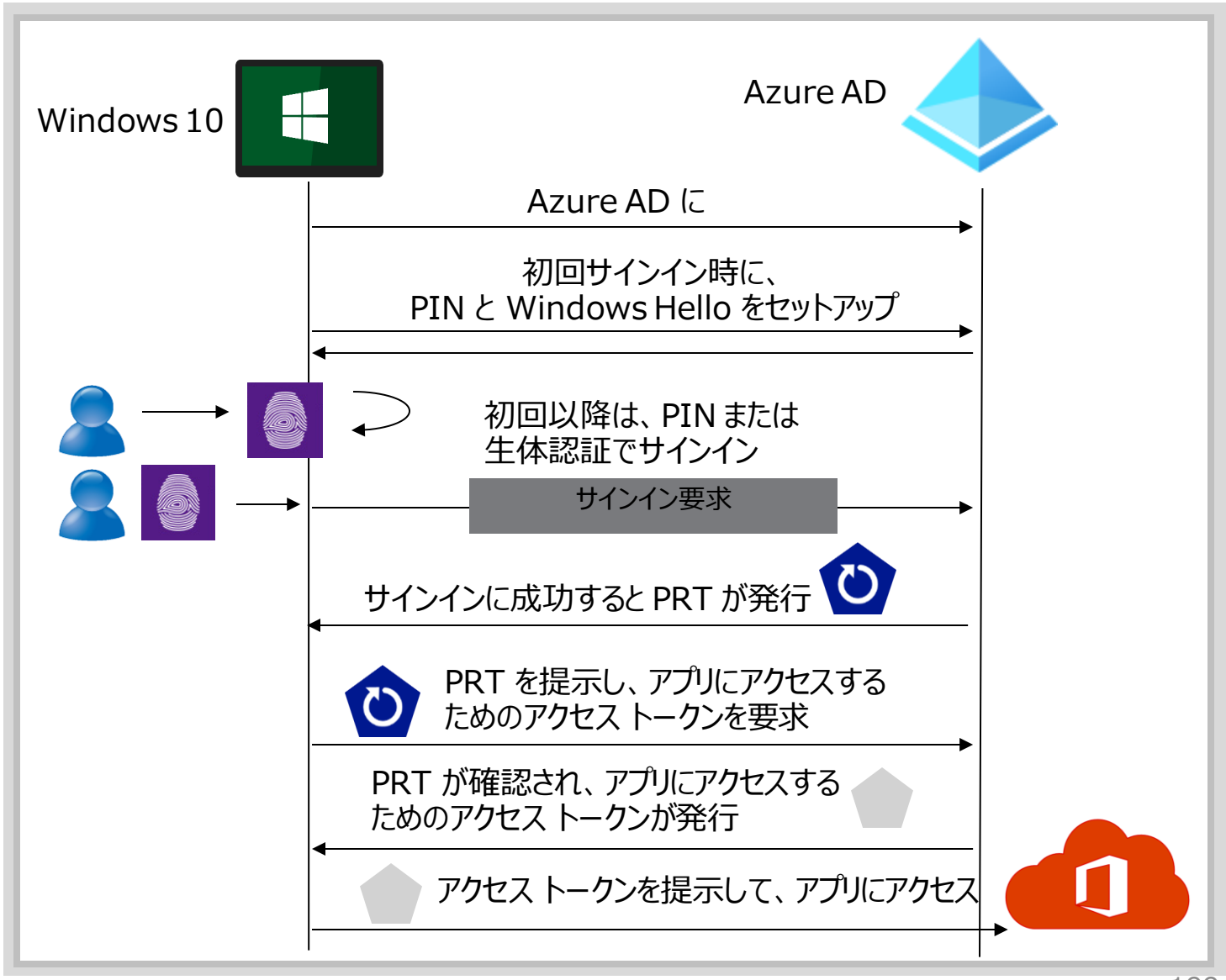
- Windows Hello for Business では、
  PIN を入力して、デバイスに保存されている秘密キーを取り出し、
  その秘密キーで署名したサインイン要求を、Azure AD に送る
  - PIN やパスワードは送信しない



[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

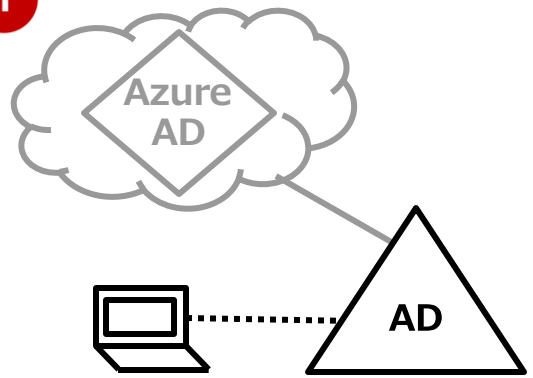
「Microsoft Intune がインストールされた Windows 10 デバイス上で Windows Hello for Business を使用する」
https://docs.microsoft.com/ja-jp/mem/intune/protect/identity-protection-configure



3. ハイブリッド Azure AD 参加

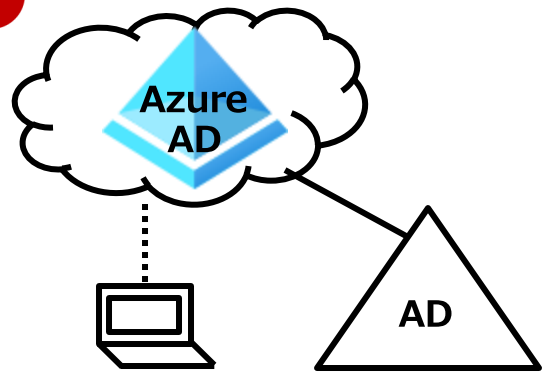
会社所有のデバイス

1



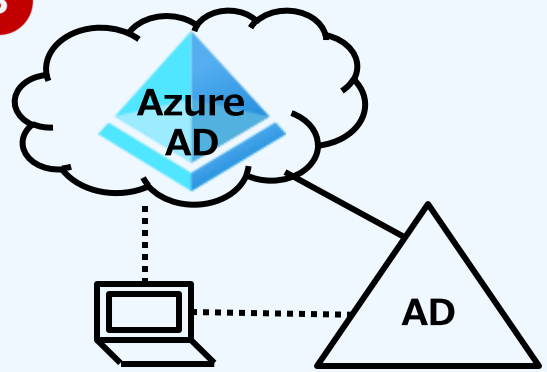
・ドメイン参加
・ConfigMgr 管理

2



・Azure AD 参加
・Intune 管理

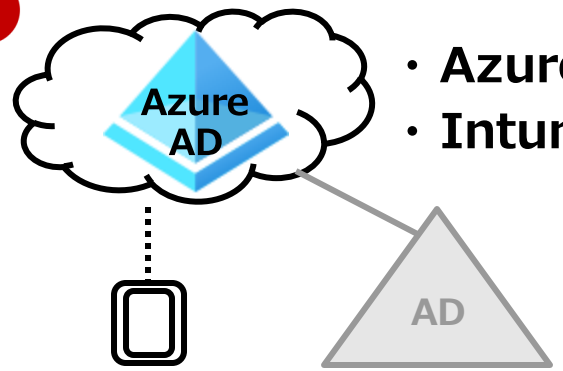
3



・**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

4



・Azure AD 登録
・Intune 管理

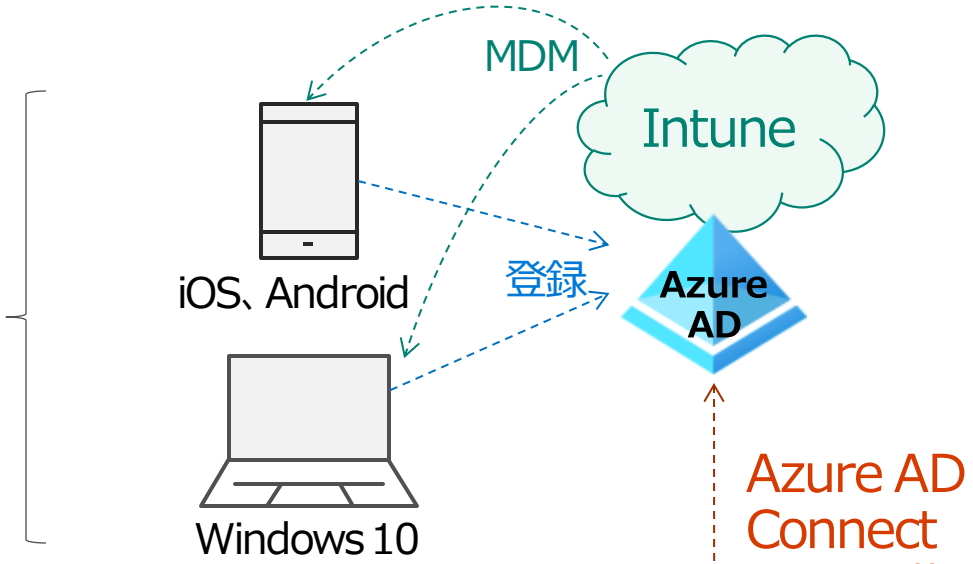
“ハイブリッド Azure AD 参加”は、オンプレミスのドメインに参加しているデバイスを Azure AD に自動的に登録すること

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

ハイブリッド Azure AD 参加を構成できる
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

マネージド環境

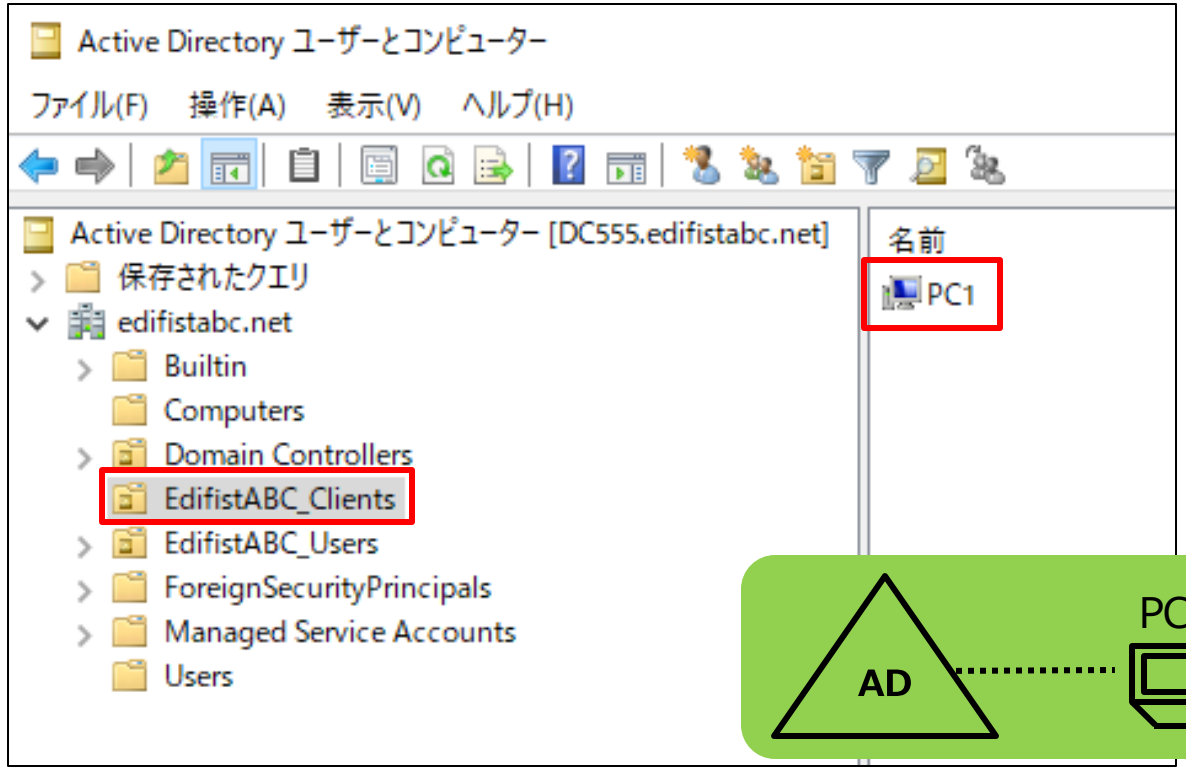
ハイブリッド Azure AD 構成の前提条件　1/2

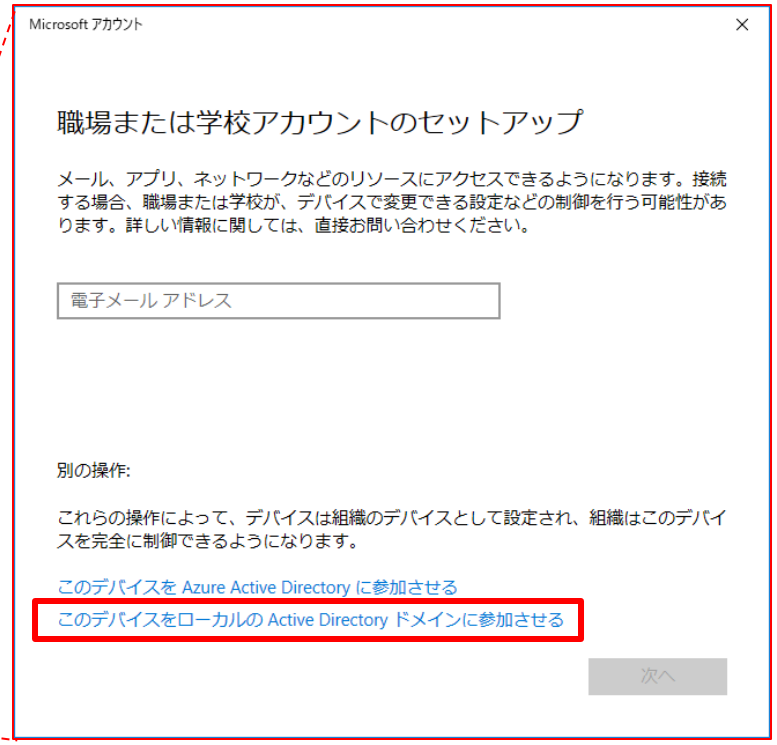
- Azure AD Connect の最新バージョン（1.1.819.0 以降）
- Azure AD テナントの全体管理者の資格情報
- 各フォレストのエンタープライズ管理者の資格情報

- 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 Widows 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

ハイブリッド Azure AD 構成の前提条件　2/2

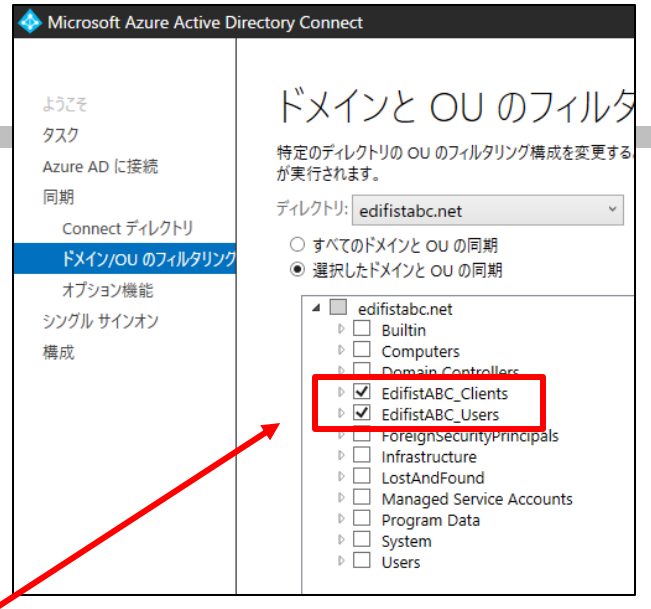
- Windows コンピューターがドメインに参加していること
  - ドメインに参加した Windows コンピューター オブジェクトを、
    Azure AD Connect によるディレクトリ同期の、対象となる OU に移動しておく（必要に応じて）





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

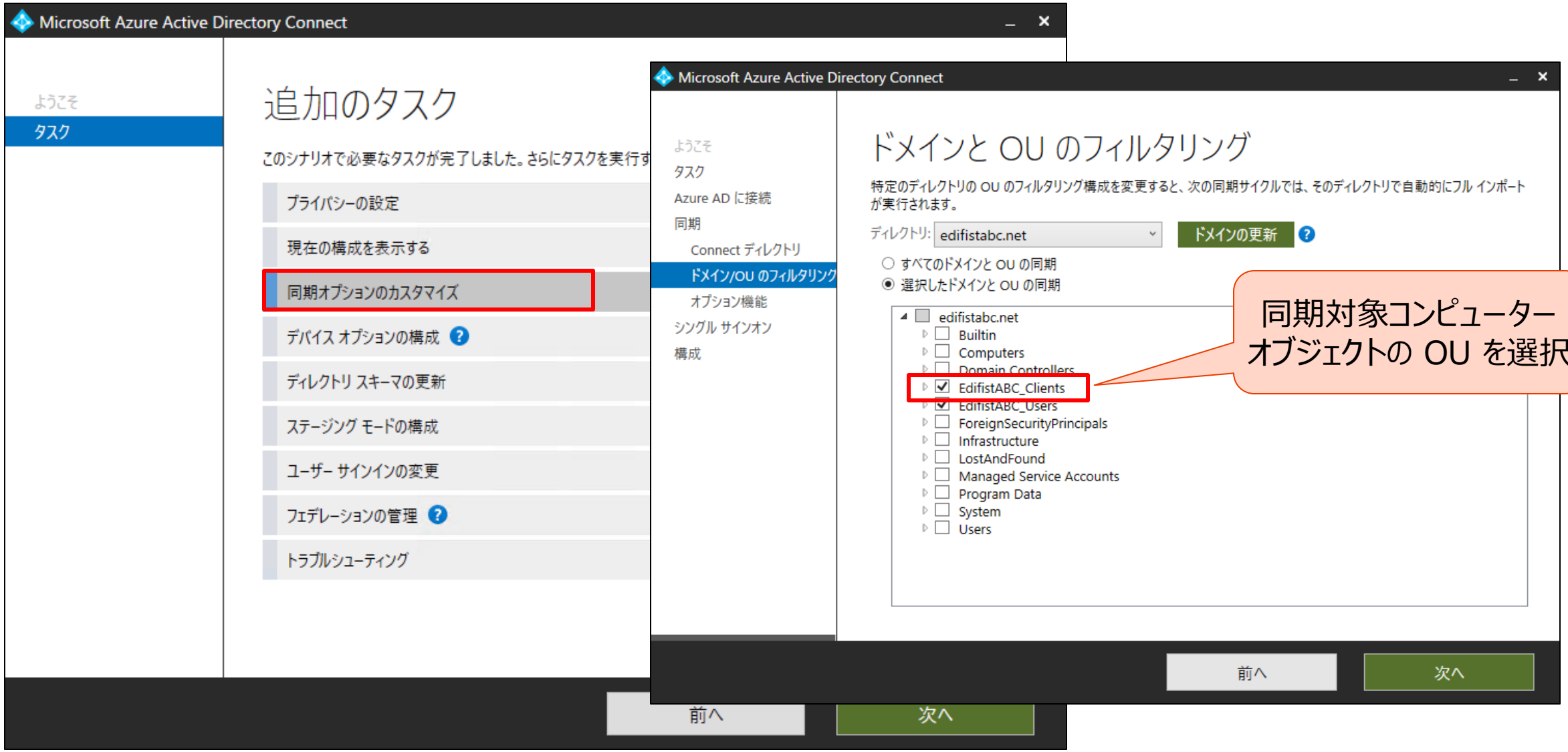


⇒ Active Directory の構成パーティションに、デバイス登録先となる Azure AD テナントを示す SCP オブジェクトが作成される

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

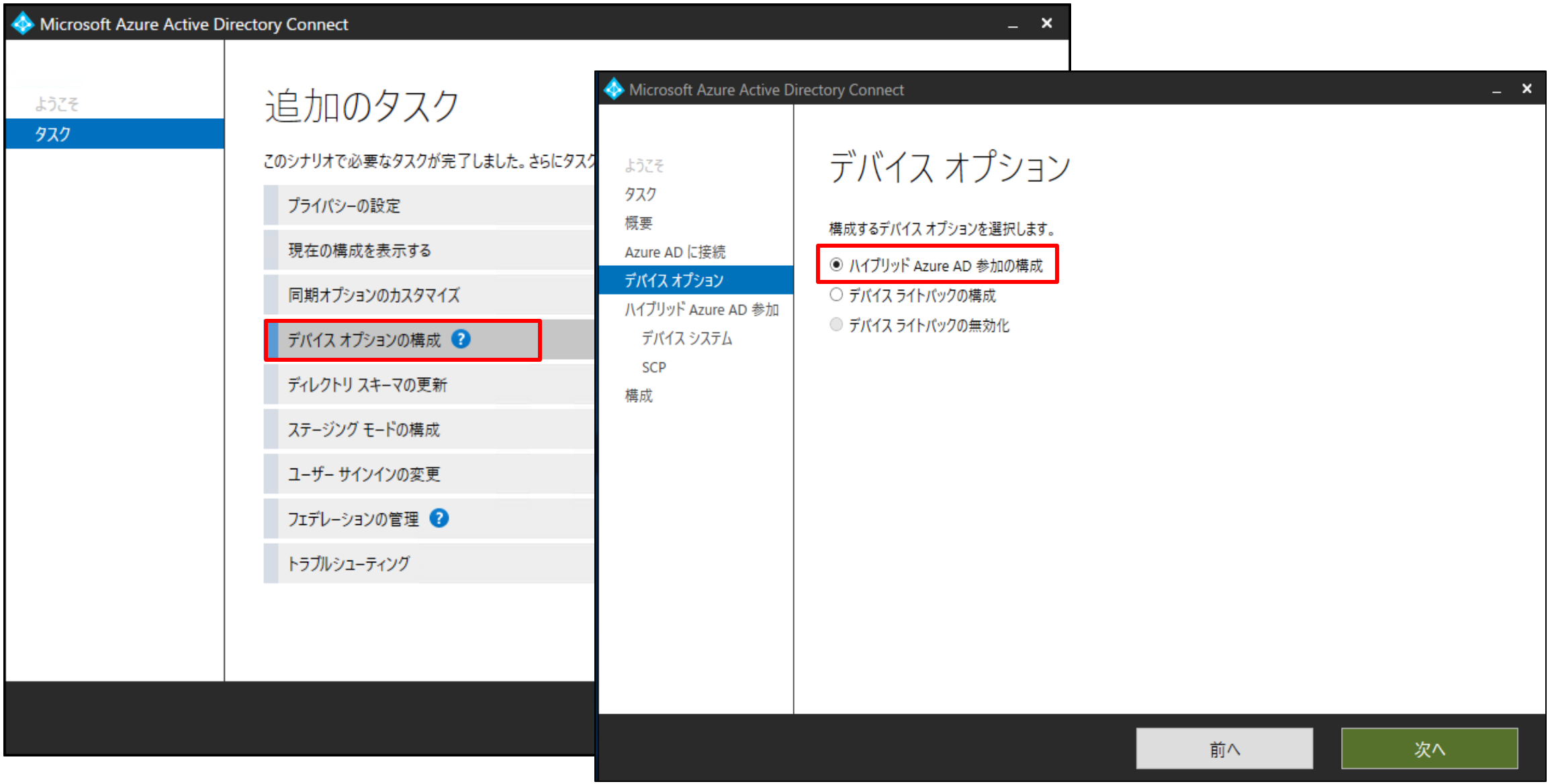
① 同期オプションのカスタマイズ

Azure AD Connect 構成ウィザード



② デバイス オプションの構成

Azure AD Connect 構成ウィザード

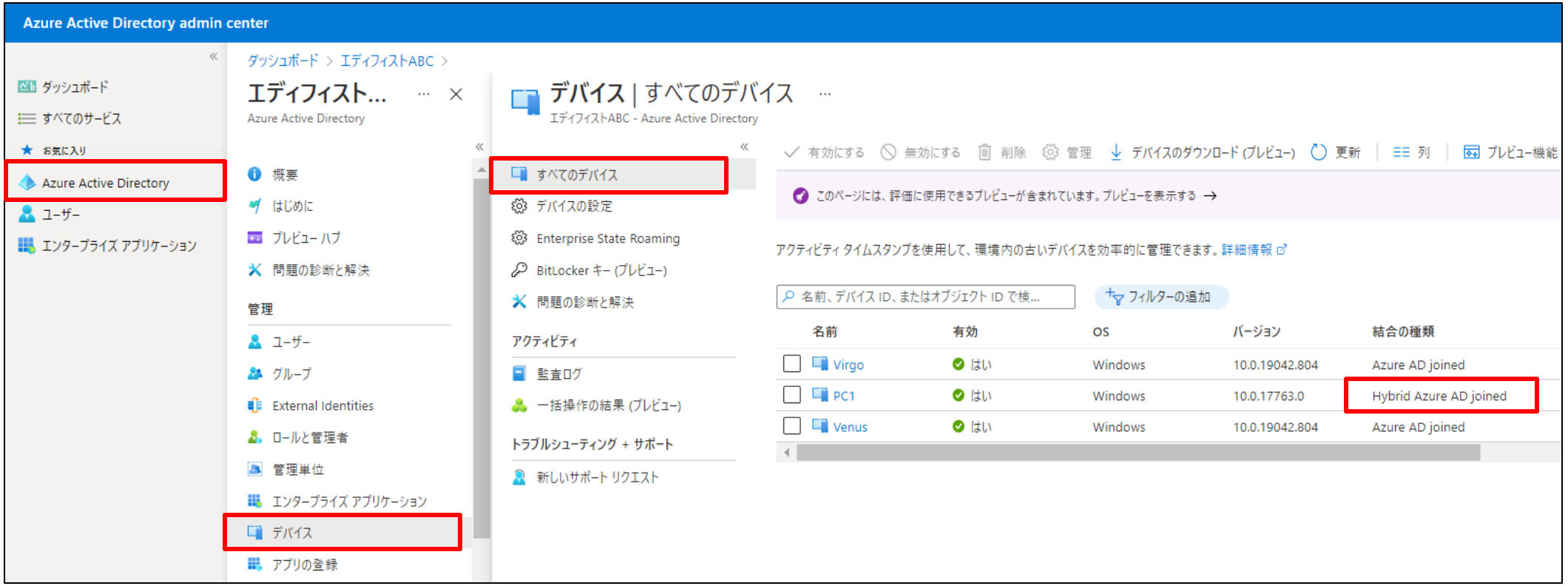


(続き)


Microsoft Azure Active Directory Connect
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
デバイスのオペレーティング シス
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
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
前
Microsoft Azure Active Directory Connect
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
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
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。
ConfigureSCP.ps1 のダウンロード
前へ
次へ

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

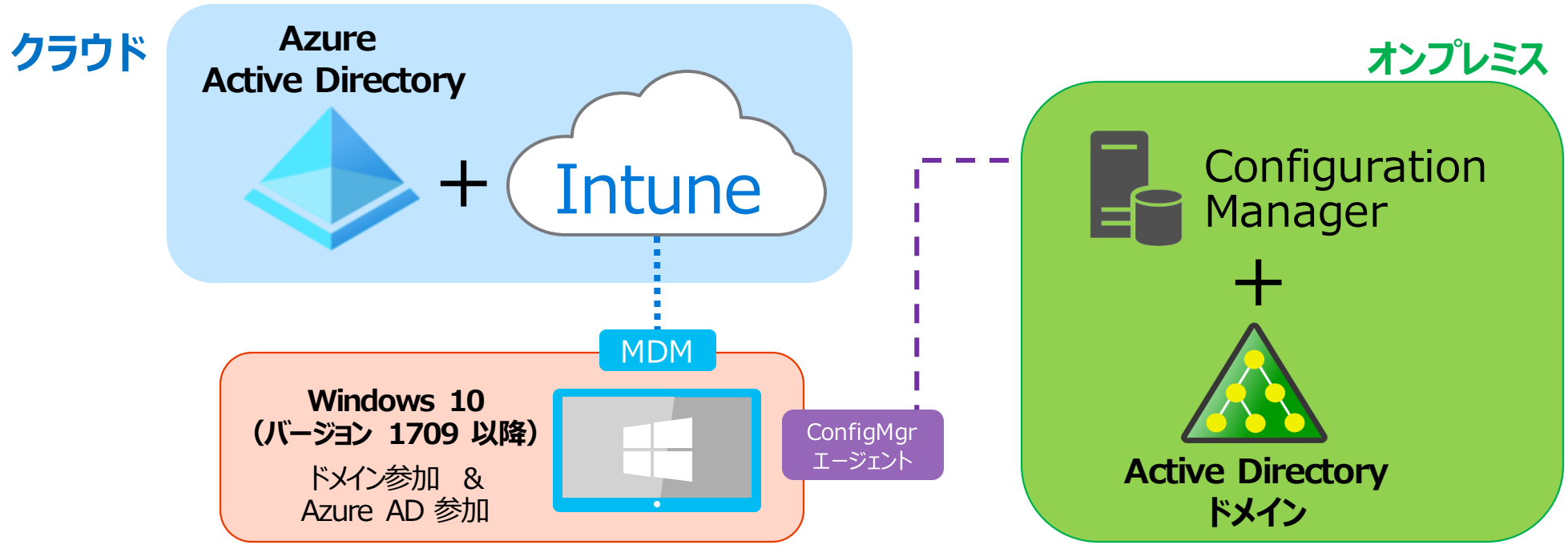


「ハイブリッド Azure AD 参加の構成後のタスク」
https://docs.microsoft.com/ja-jp/azure/active-directory/hybrid/how-to-connect-fed-hybrid-azure-ad-join-post-config-tasks

4. 共同管理（Co-Management）

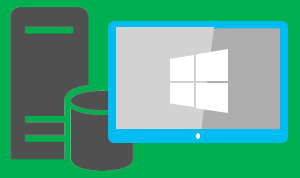
- Windows 10 デバイスを、「Microsoft Endpoint Configuration Manager（MECM）」と「Intune」の両方で管理すること

- “共同管理” は、Intune 移行への “最初のステップ”



「共同管理とは」 https://docs.microsoft.com/ja-jp/mem/configmgr/comanage/overview

「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

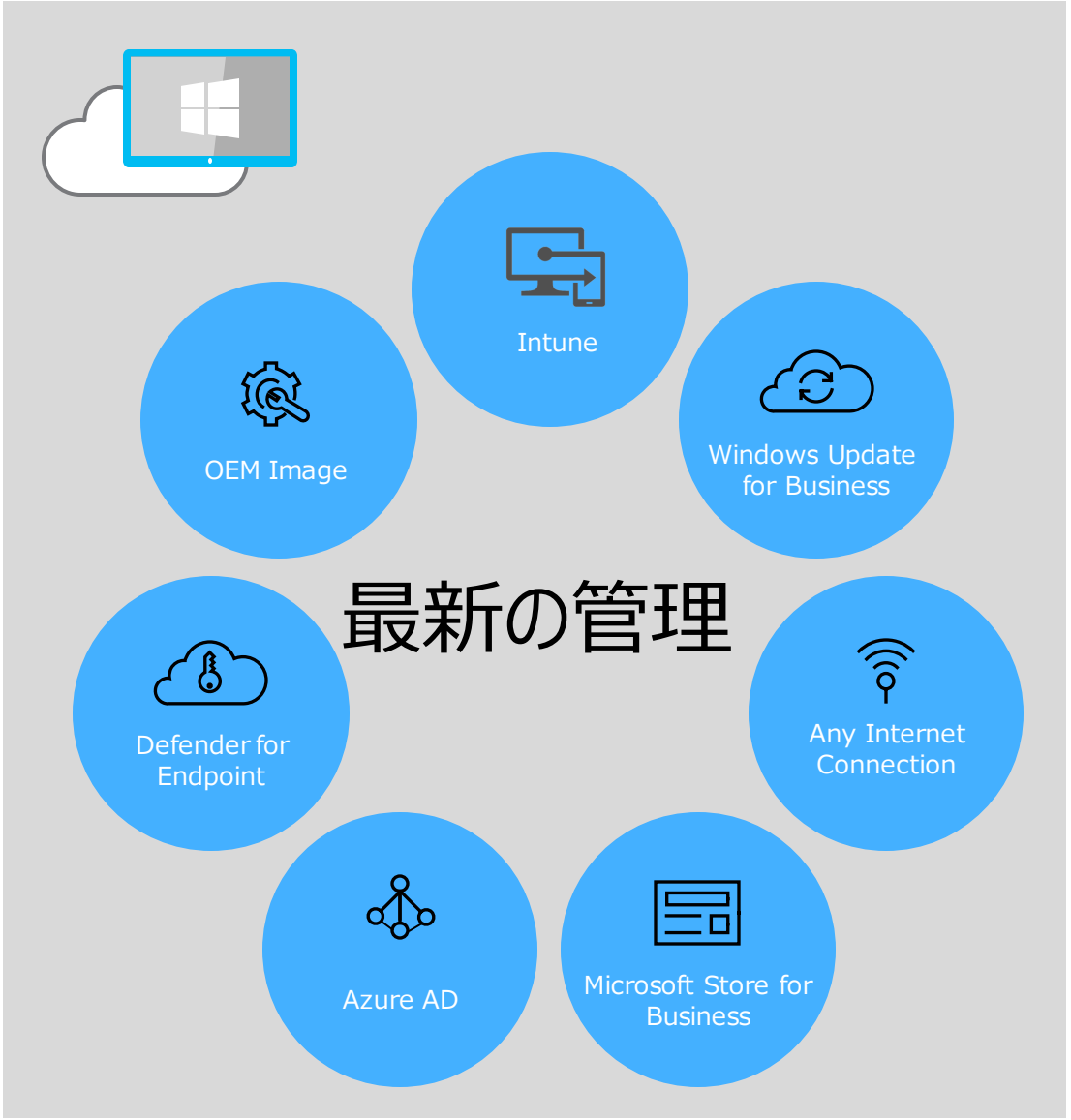
クラウド ベースの管理 & SaaS アプリ

自動管理

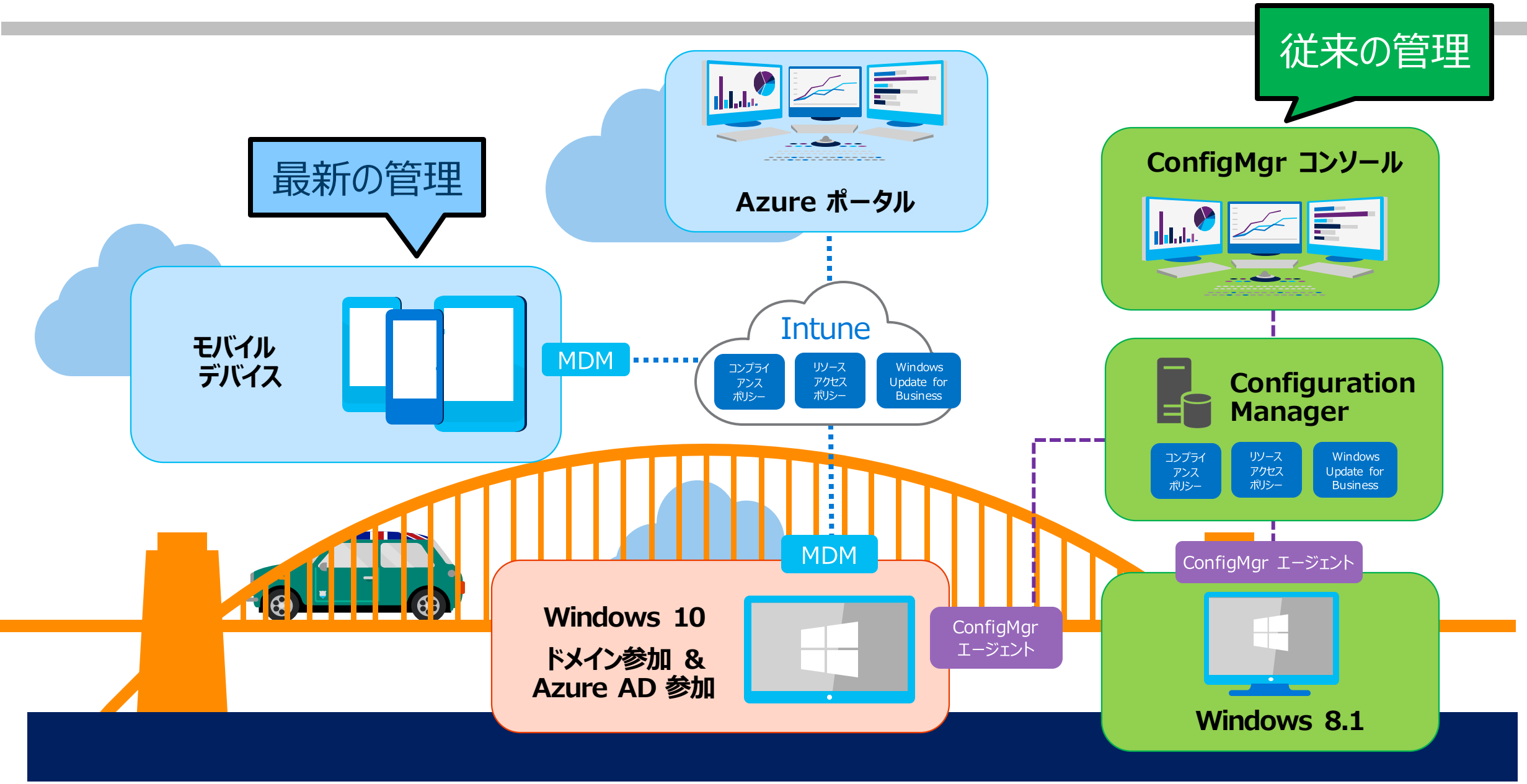
プロアクティブ
（先を見越して、事前に行動する）

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

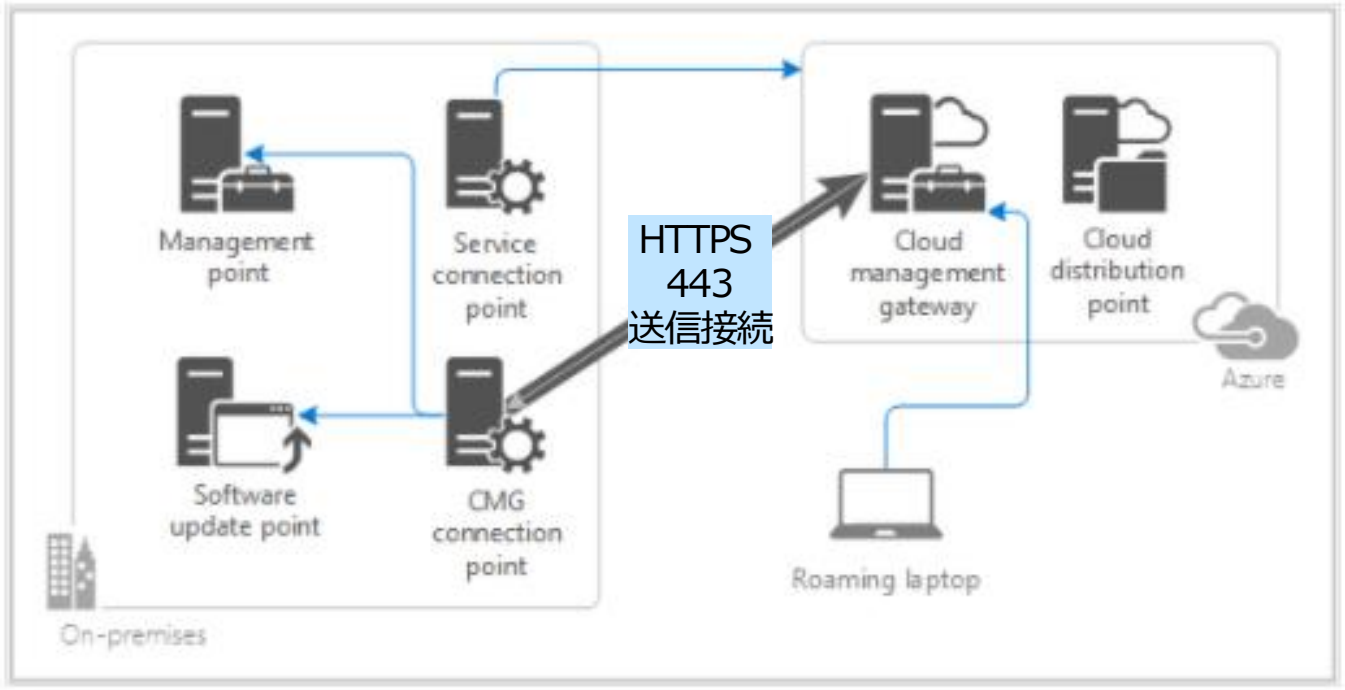
- ハイブリッド Azure AD 参加の構成が必要
  - パスワード ハッシュ同期 + SSO
  - パススルー認証 + SSO
  - AD FS によるフェデレーション SSO

「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/cmg/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！