

Active Directory から始める Azure移行

双日テックイノベーション株式会社
クラウドソリューション事業本部
長澤 祥司



1. 今、求められているセキュリティ
2. Microsoft Entra ID とは？
3. Microsoft Entra IDでユーザーを管理するには？
4. Microsoft Entra IDでデバイスを管理するには？
5. セキュリティを高めるために
6. 教育リソース・その他のご紹介

第1章

いま、求められているセキュリティ

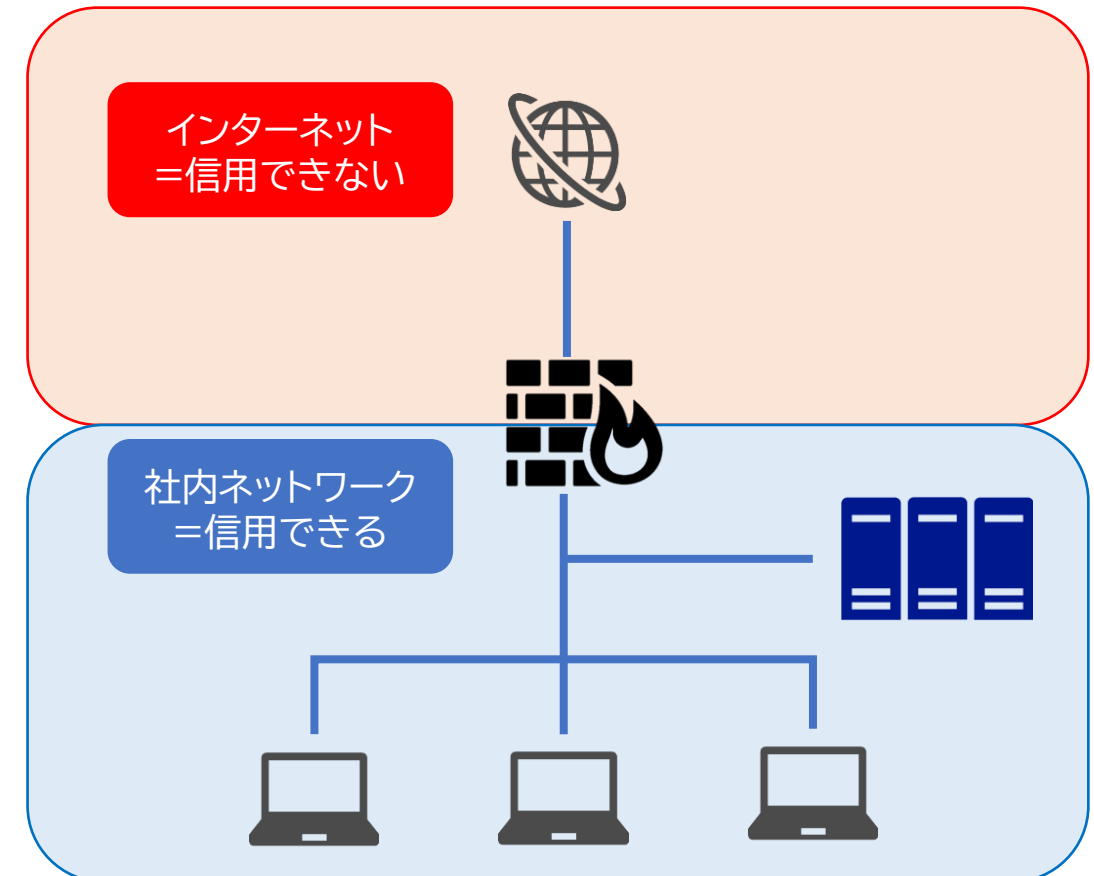


1. 今、求められているセキュリティ

従来のセキュリティ境界は？

従来のセキュリティ対策方法の主流は「境界型」の対策。境界型の対策では、ファイアウォールなどでネットワーク境界を監視・保護することで、境界内部の安全性を確保されていた。

境界型セキュリティモデル

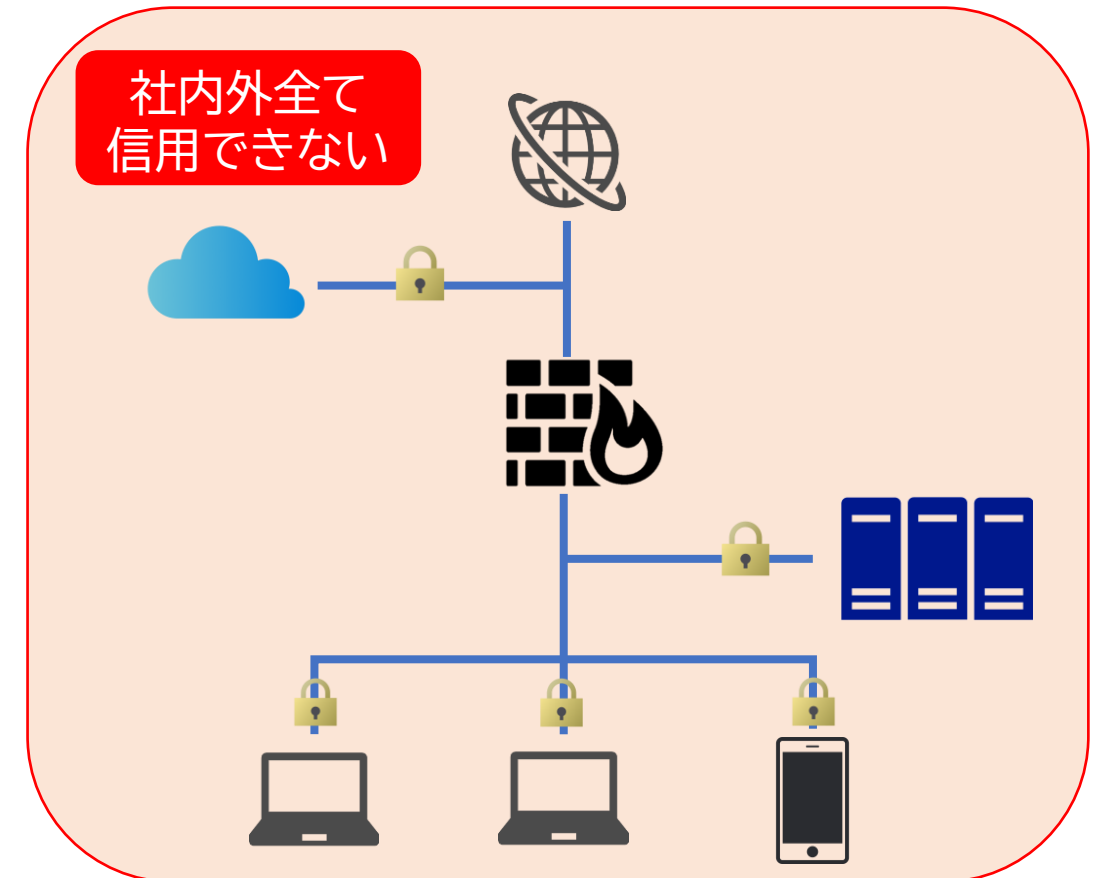


1. 今、求められているセキュリティ

現在のセキュリティ境界は？

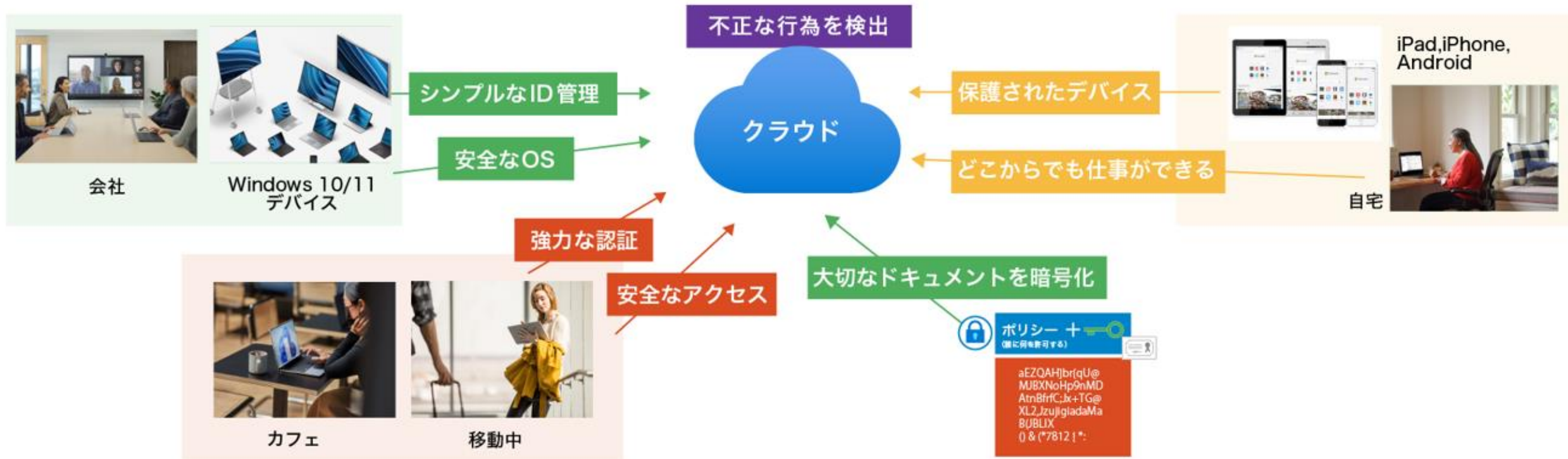
クラウドサービス利用の急増などを背景として、境界型のセキュリティ対策には限界が見られるようになり「全てを信頼せずあらゆる環境において認証・認可を行う」という「ゼロトラストセキュリティ」という考えが主流。

ゼロトラストセキュリティ



1. 今、求められているセキュリティ

ゼロトラストセキュリティ実現に有効なMicrosoft Entra ID



第 2 章

Microsoft Entra IDとは？



2. Microsoft Entra IDとは

Microsoft Entra ID とは？

Microsoftが提供する統合型のクラウド ID およびアクセス管理ソリューション

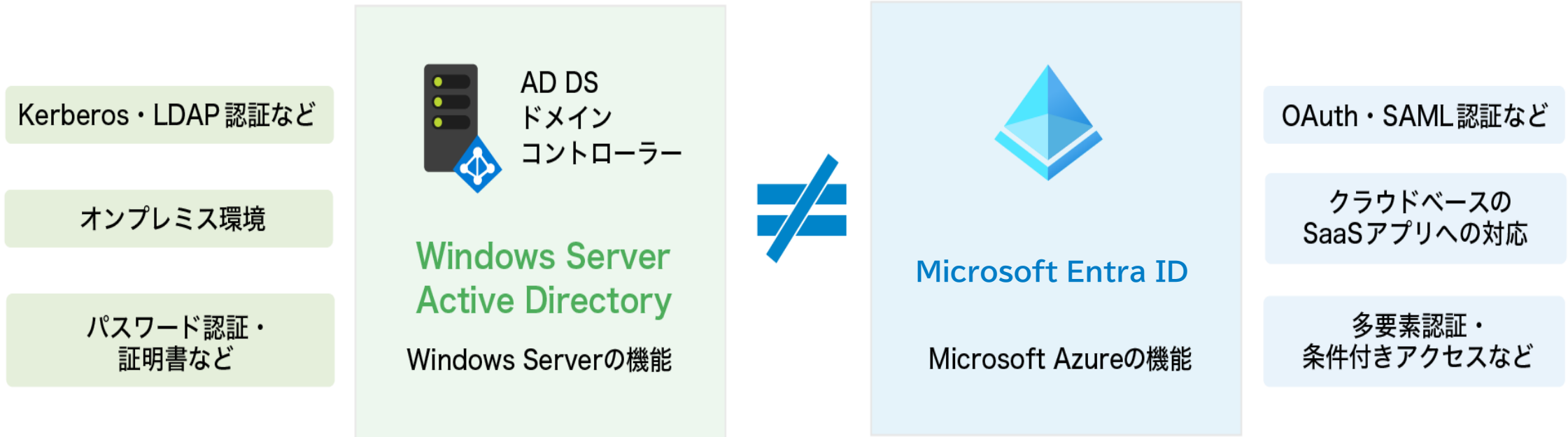
- ID管理(オンプレミスActive Directoryとも統合可能)
- シングルサインオン
- アクセス制御(条件付きアクセス)



Azure Active Directory(Azure AD)が、2023年10月1日より「Microsoft Entra ID」に改名されました。

Microsoft Entra IDとオンプレミスADの違い

Microsoft Entra IDとオンプレミスADは別ものです！



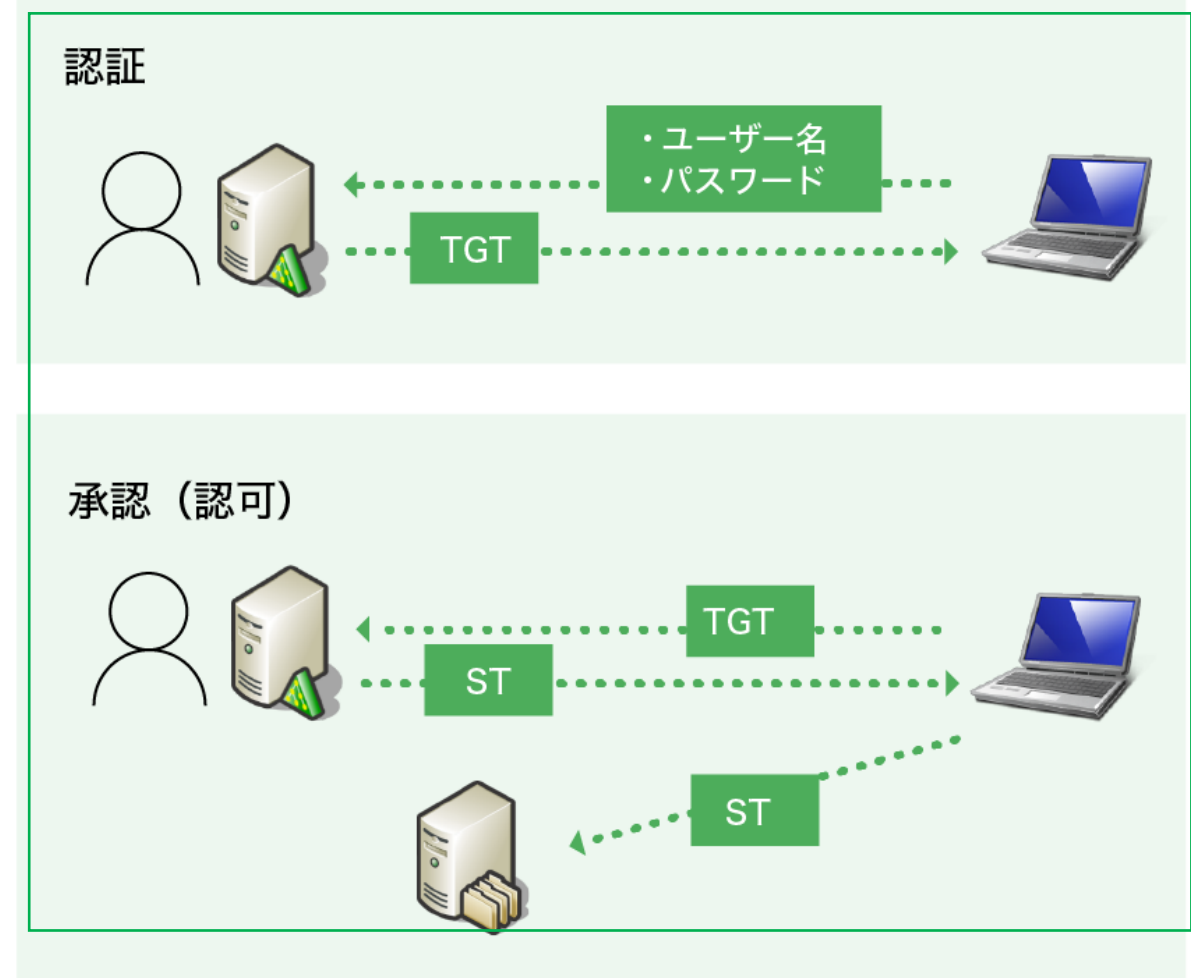
オンプレミスADにおける認証・認可方法

認証

- 本人確認の機能
- 一般的にはユーザー名とパスワードを使用して本人確認を行う。
- 本人確認ができると、Kerberos Ticket Granting Ticket(TGT)が発行される

承認(認可)

- ユーザーがリソースにアクセス可能かを確認する機能
- TGTをドメインコントローラーに提示して、サーバにアクセス可能か問い合わせをする。
- アクセス可能なユーザーであることが確認できるとService Ticket(ST)が発行され、アクセスが認可される。



2. Microsoft Entra IDとは

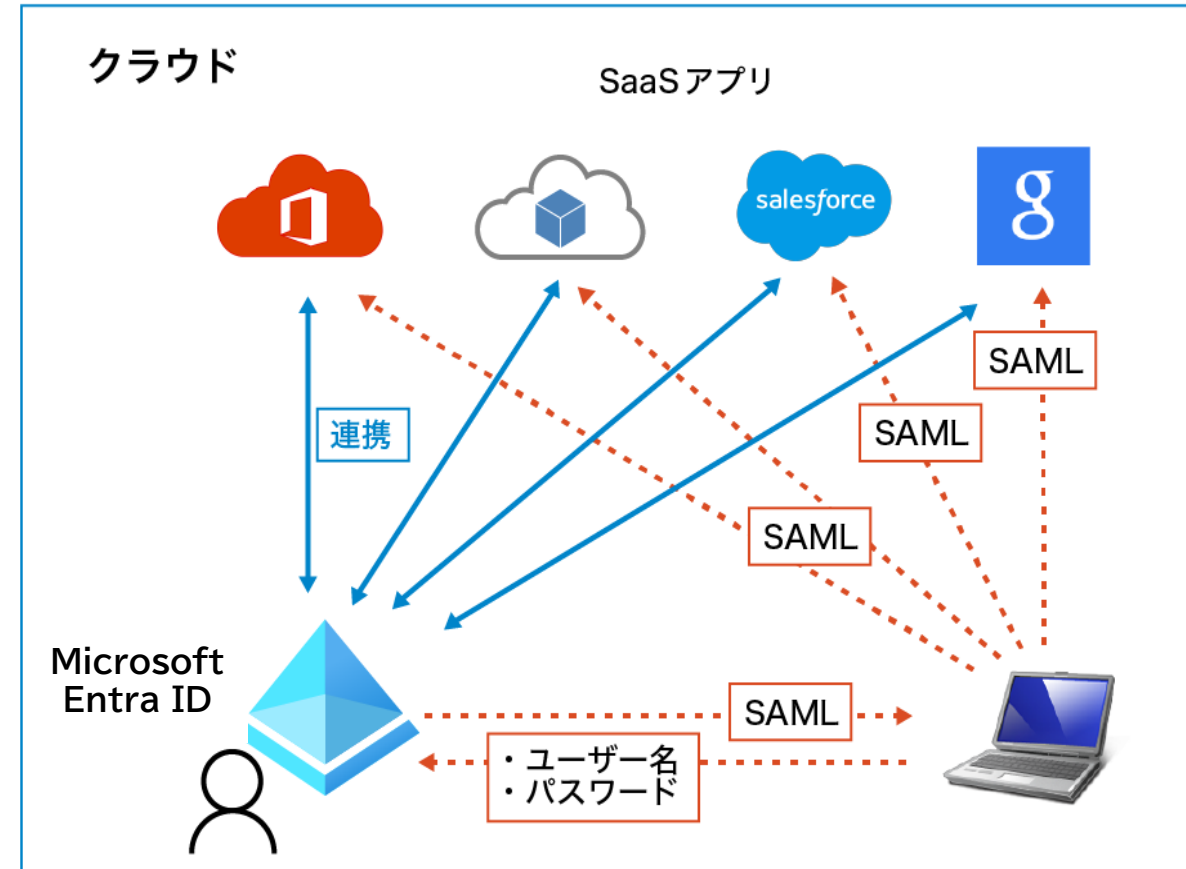
Microsoft Entra IDにおける認証・認可方法

認証

- パブリッククラウドサービスのため場所を問わずどこからでも認証が可能。
- ID、パスワードに加えて、スマートデバイスを利用した**多要素認証**や、場所・デバイス状態などにより認証可否を判断する**条件付きアクセス**などの機能を利用ができる

承認(認可)

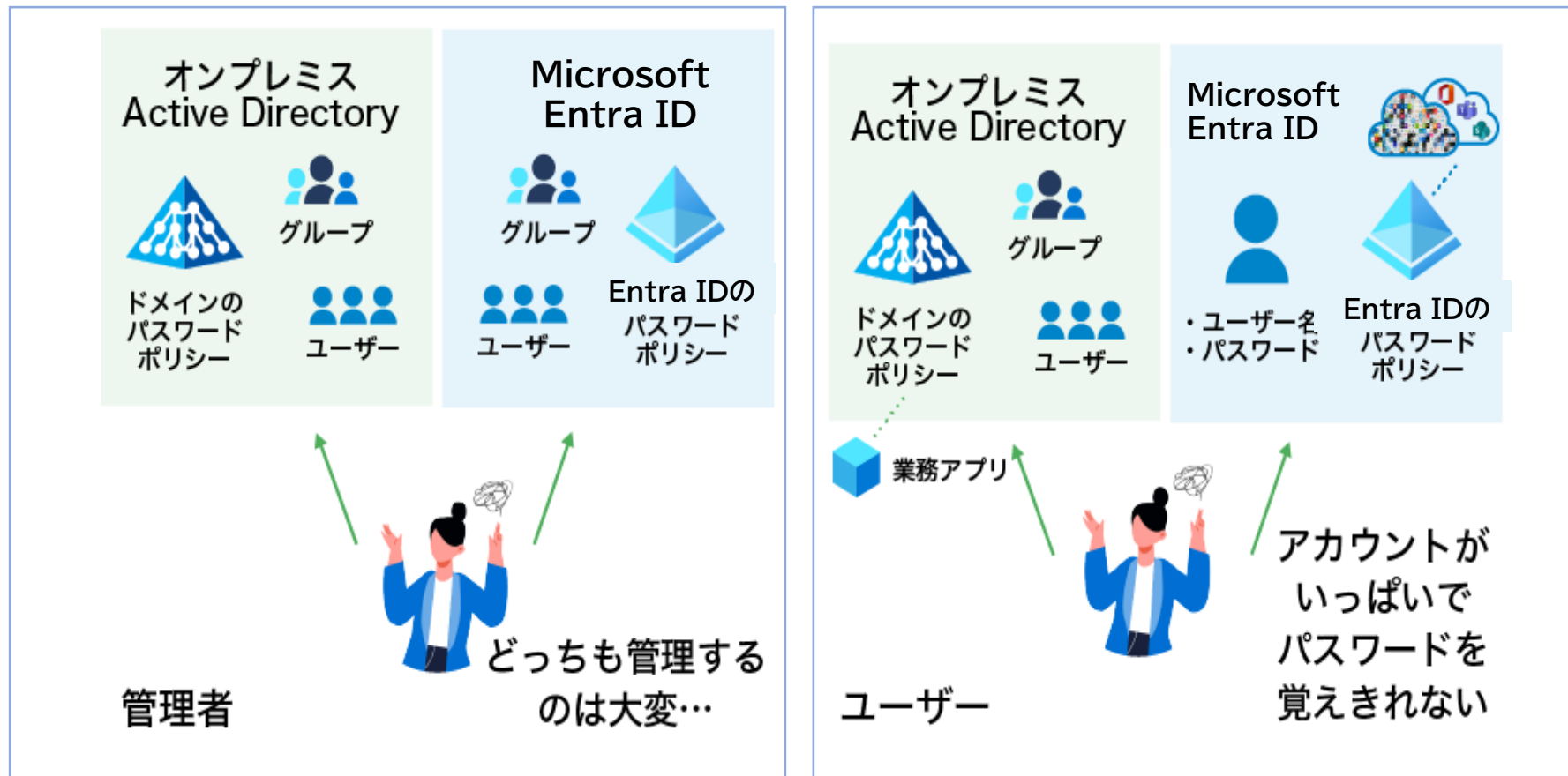
- SAML等の認証方式にも対応しており、Microsoft製品以外の**SaaSアプリの認可**も可能



2. Microsoft Entra IDとは

2つのディレクトリがバラバラの場合だと……

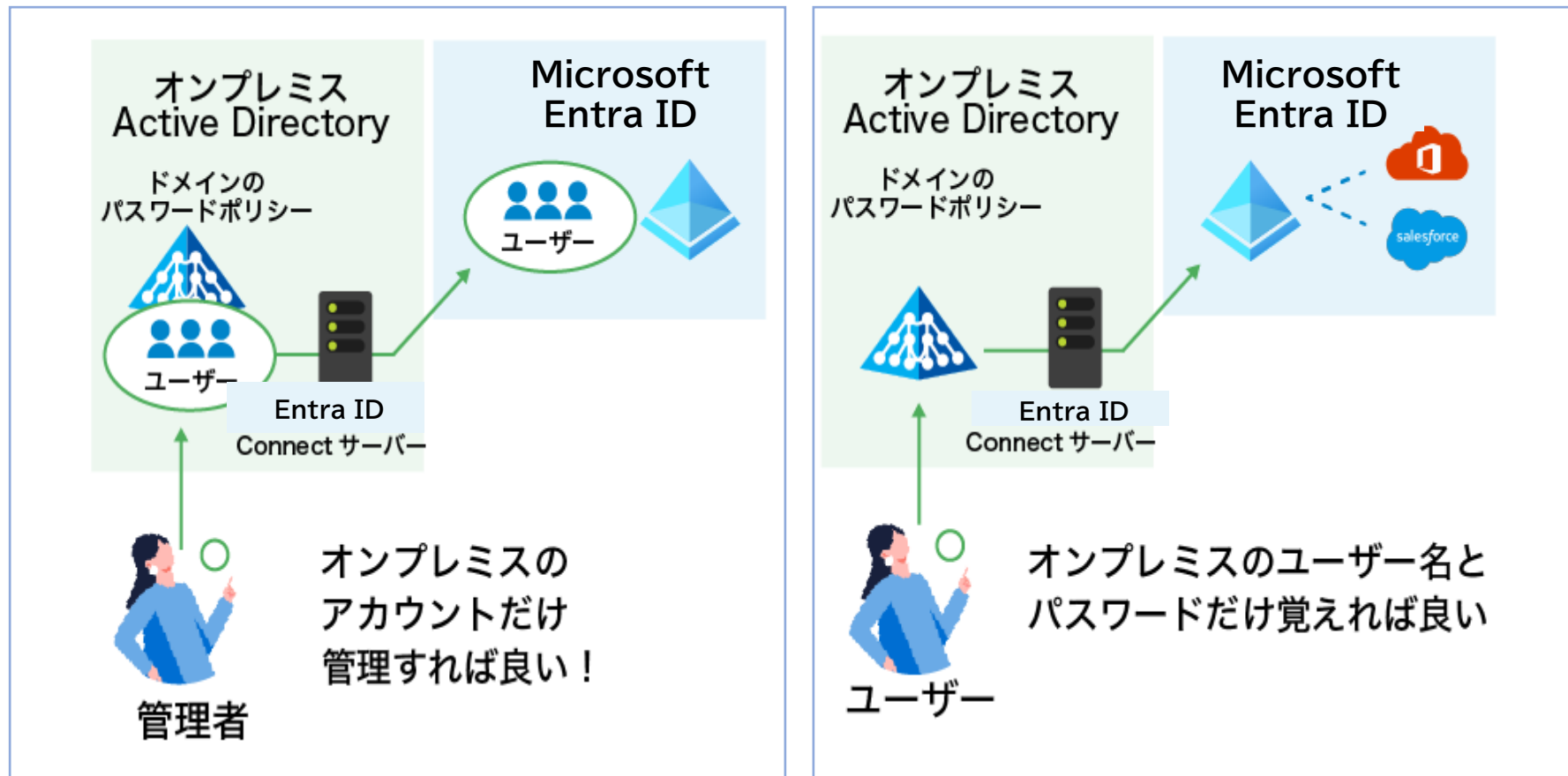
管理者とユーザーの負担が大きくなる



2. Microsoft Entra IDとは

オンプレADとEntraIDを統合すると…

管理者の作業負荷が低減され、ユーザーの利便性が向上する



第 3 章

Microsoft Entra IDで ユーザーを管理するには？



3. Microsoft Entra IDにおけるユーザー管理方法

Entra IDにおけるユーザーの作成方法

Azure Portalにログインの上、Microsoft Entra IDの「ユーザー」から「すべてのユーザー」を選択し、「新しいユーザー」を実行することでユーザーを作成できます。

新しいユーザーの作成 ...
組織内に新しい内部ユーザーを作成する

基本 プロパティ 割り当て 確認と作成

組織内に新しいユーザーを作成します。このユーザーは alice@contoso.com

ID

ユーザー プリンシパル名 *

メール ニックネーム *

表示名 *

パスワード *

有効なアカウント ①

既定の onmicrosoft.com ドメイン名または追加したカスタムドメイン名を指定する。

ドメインが一覧にありませんか? 詳細情報

レビューと作成 < 前へ 次: プロパティ >

Entra IDにおけるグループの作成方法

Azure Portalにログインの上、Microsoft Entra ID ディレクトリの「グループ」から「すべてのグループ」を選択の上、「新しいグループ」を実行することで作成できます。

The screenshot displays the Microsoft Entra ID 'New Group' page. On the left sidebar, the 'グループ' (Groups) section is highlighted with a red box, and the '新しいグループ' (New Group) button is also highlighted. A red arrow points from this button to the '新しいグループ' (New Group) page on the right. The page shows the following fields:

- ホーム > グループ | すべてのグループ > 新しいグループ ...
- フィードバックがある場合
- グループの種類 * ①: セキュリティ
- グループ名 * ①: グループの名前を入力してください
- 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 Microsoft Entra ロールを割り当てることができる ①: はい (selected), いいえ
- メンバーシップの種類 * ①: 割り当て済み
- 所有者: 所有者が選択されていません
- メンバー: メンバーが選択されていません

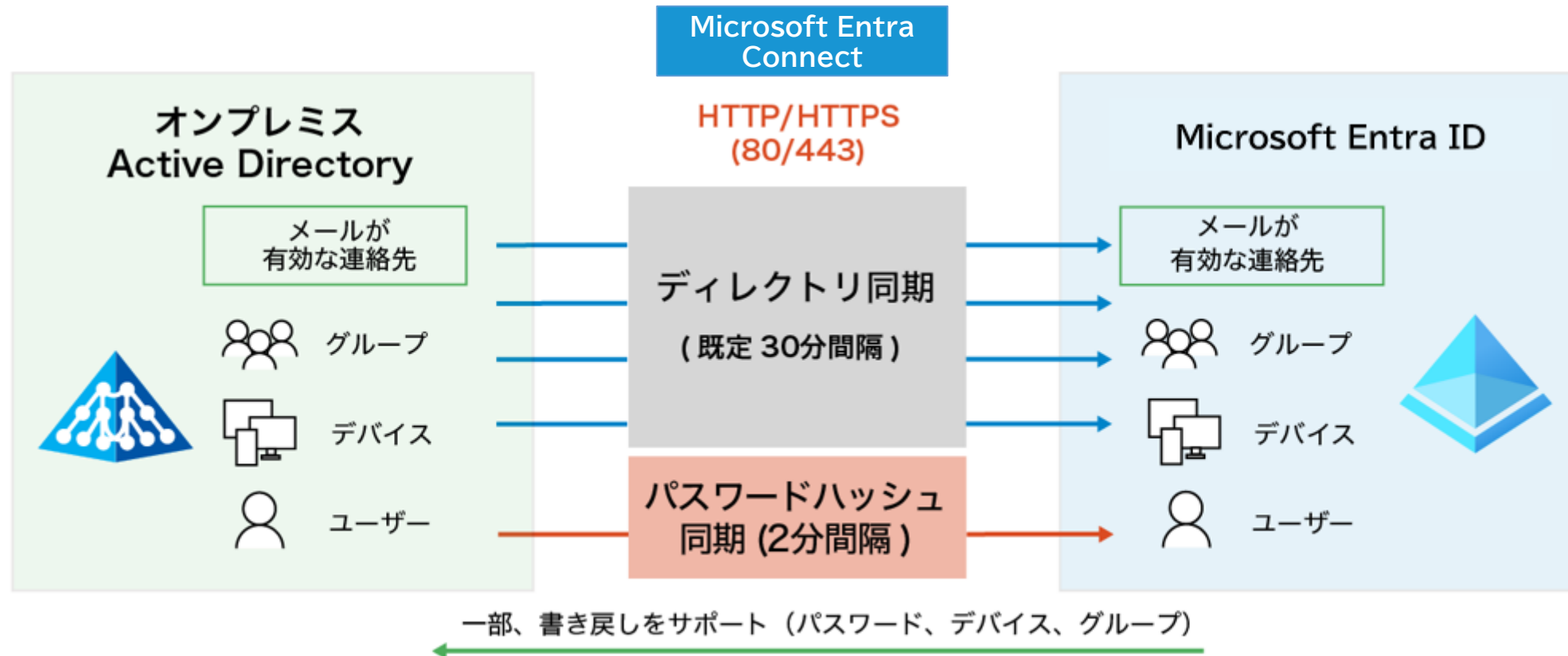
Microsoft Entra IDで利用できる主なグループ

種類	概要
Microsoft 365 グループ	社内外のユーザー間での共同作業に使用する
配布グループ	複数のユーザーにメール通知を送信するのに使用する
セキュリティグループ	SharePointサイトなどのリソースへのアクセスを許可するために使用する
メールが有効なセキュリティグループ	上記に加え、ユーザーにメールで通知を送信するために使用する
共有メールボックス	サポート用など、複数のユーザーが同じメールボックスを利用する場合に使用する
動的配布グループ	組織内でのメールメッセージやその他の情報の大量送信を行うために使用する

3. Microsoft Entra IDにおけるユーザー管理方法

オンプレミスADからMicrosoft Entra IDへの同期を活用する

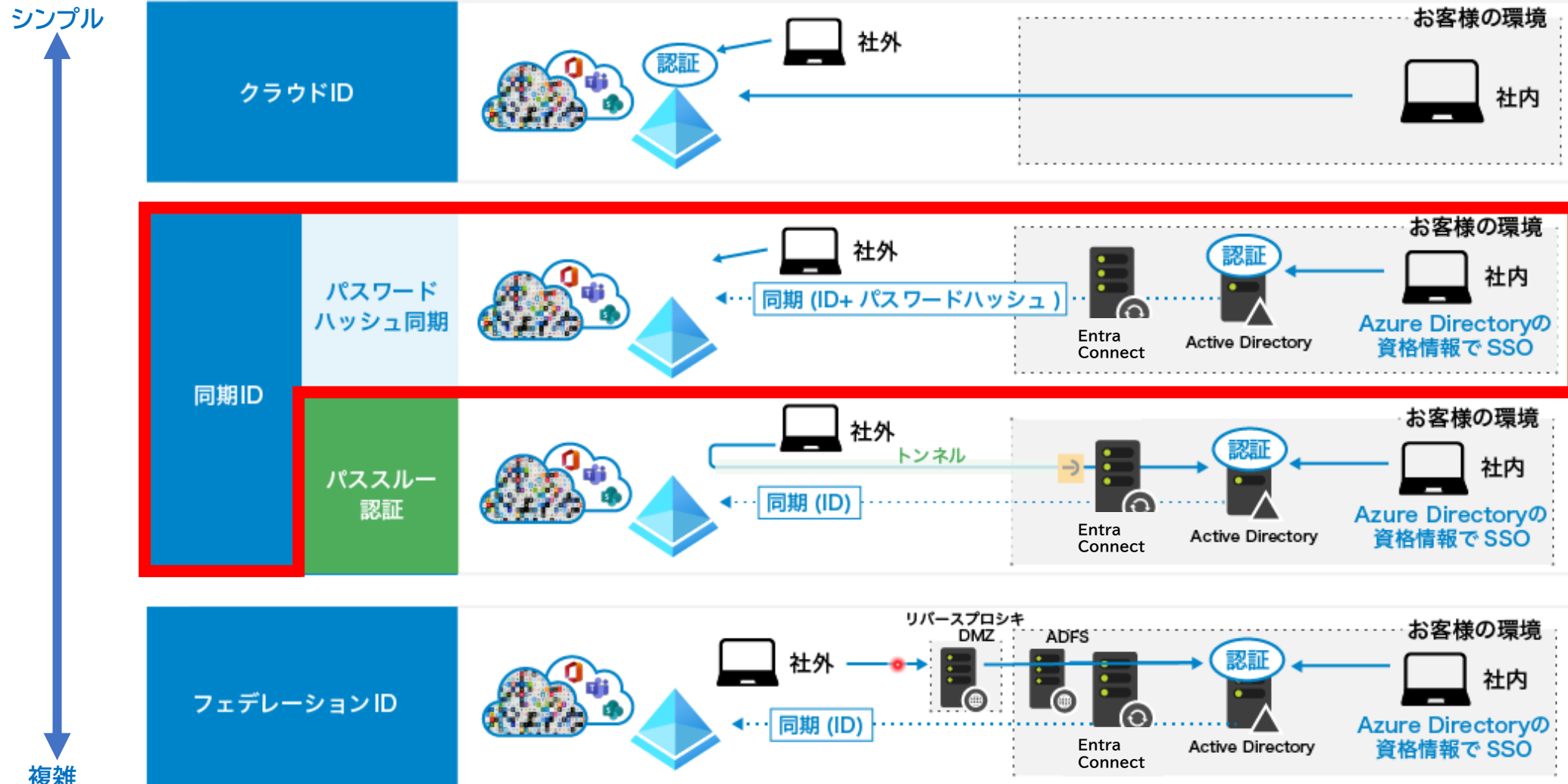
ディレクトリ同期によって、オンプレミスADの管理のみでオンプレミスADとMicrosoft Entra IDの併用が可能



3. Microsoft Entra IDにおけるユーザー管理方法

認証基盤の構成オプション

クラウドサービス(Office365等)に対する認証イメージ
※主な組み合わせの例となり、認証の流れは簡略化しています



可用性や構成がシンプルのため推奨構成

第4章

Microsoft Entra IDで デバイスを管理するには？

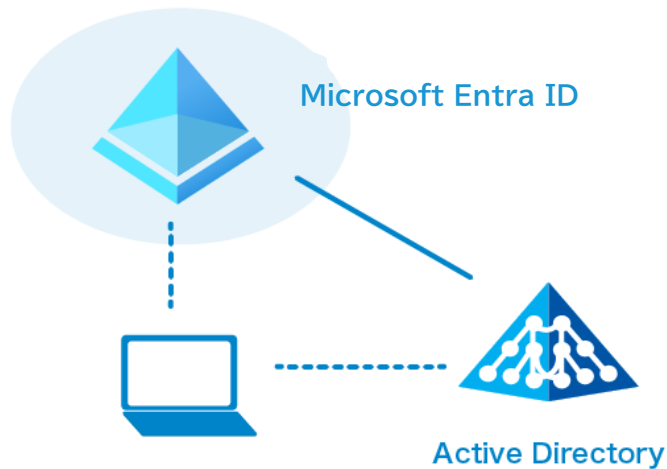


デバイス管理の選択肢

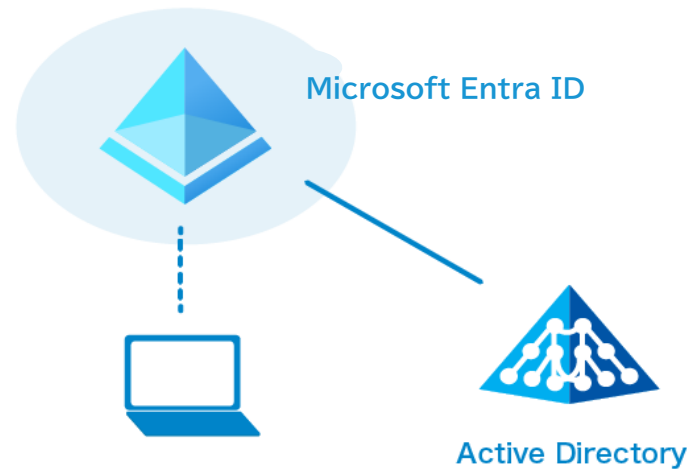
クラウドベースデバイス管理のメリット

- ① クラウド上でのアクセスコントロールによるゼロトラスト環境構築
- ② クラウドリソースに対するシングルサインオン

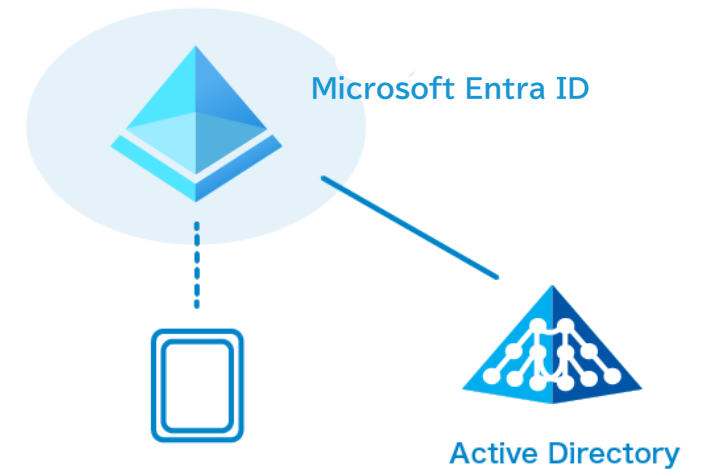
1 Microsoft Entra join (Microsoft Entra 参加)



2 Microsoft Entra hybrid join (Microsoft Entra ハイブリッド参加)

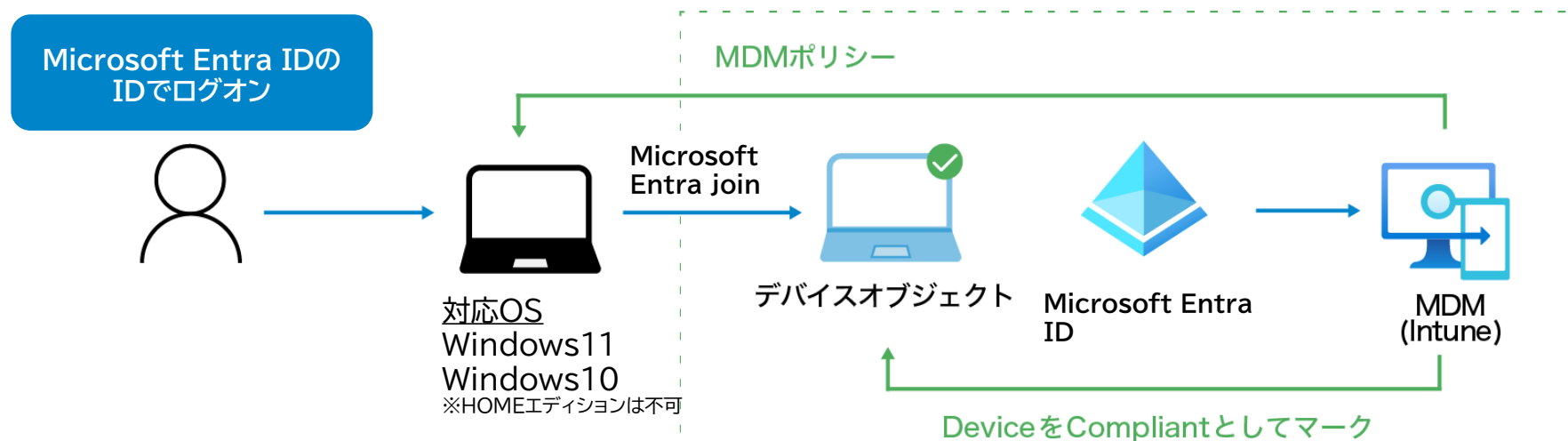


3 Microsoft Entra registered (Microsoft Entra 登録)



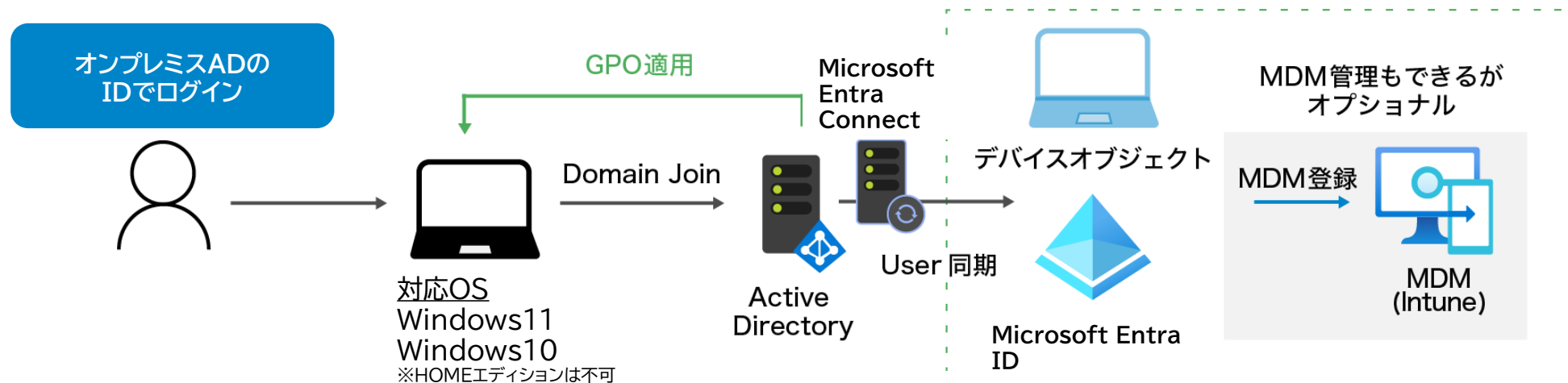
①Microsoft Entra join(Microsoft Entra 参加)とは

- クラウドを中心とした管理
- Microsoft EntraのIDを利用してPCにログオン
- デバイスの情報はMicrosoft Entraに保持
- デバイスへのポリシー適応はMicrosoft Intune(MDM)で実施
- クラウド、オンプレミス両方へのシングルサインオンを提供



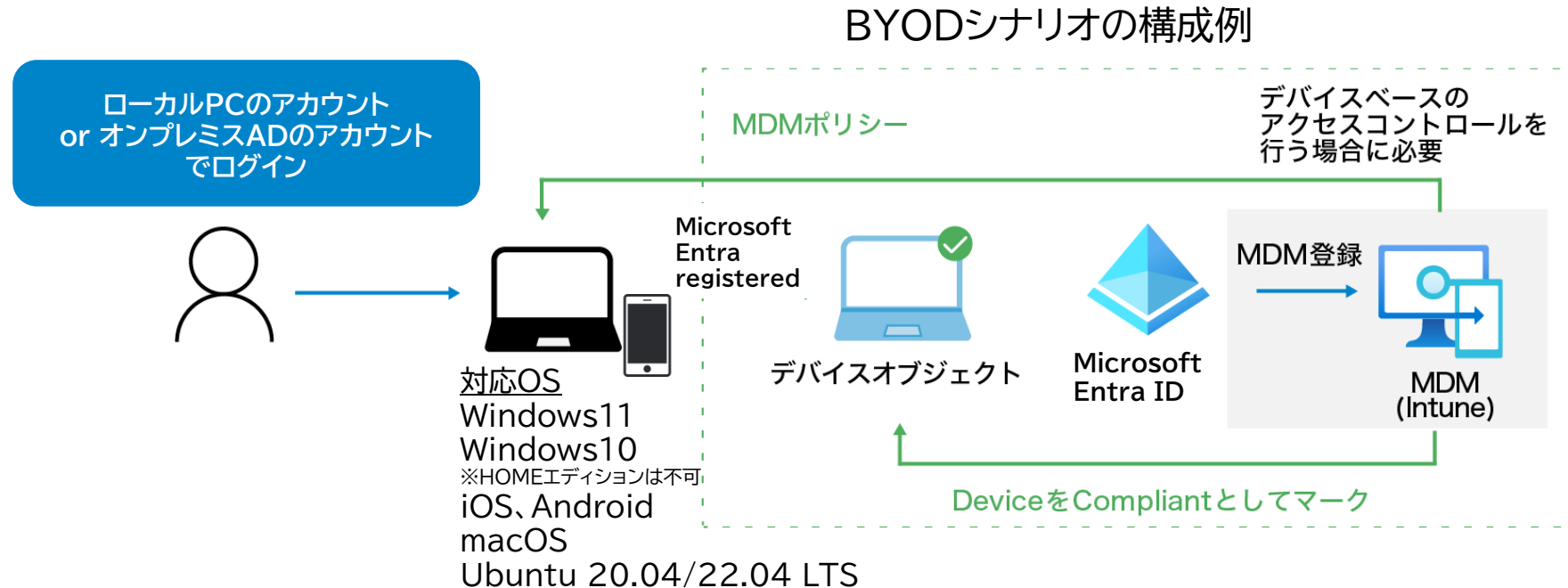
②Microsoft Entra hybrid join(Microsoft Entra ハイブリッド参加)とは

- 既存のオンプレミスActive Directory基盤を活用しつつ、クラウドを利用する場合に適している
- オンプレミスActive DirectoryのIDを利用してPCにログオン
- Domain Joinの状態はそのまま
- デバイスの情報はActive DirectoryとMicrosoft Entra両方に保持
- デバイスのポリシー適用はGPO(グループポリシー)にて実施
- クラウド、オンプレミス両方へのシングルサインオンを提供



③Microsoft Entra registered(Microsoft Entra 登録)

- 会社で管理されていないデバイス(例:組織外のデバイス、BYOD)を想定した管理
- Windows OSデバイスに加え、Android、iOS、macOSでも利用可能
- PCへのログオン方法はローカルアカウントかActive Directoryアカウント
- クラウドリソースに対するシングルサインオンを提供



Microsoft Entra ID joinとHybrid Microsoft Entra ID joinの比較表

種類	Microsoft Entra join	Microsoft Entra hybrid join
デバイスが登録される場所	Microsoft Entra ID にのみ登録される	オンプレミスADとMicrosoft Entra IDの両方に登録される
シングルサインオン	オンプレミス、クラウドのどちらのリソースにもSSO可能 オンプレミスリソースはKerberos認証を利用 クラウドリソースはPRT(プライマリ更新トークン)を利用	
対応OS	Windows11 Windows10	Windows11 Windows10
構成方法	ユーザー側での操作が必要 Windows Autopilotで半自動化も可能	管理者作業のみ (ユーザー側での作業不要)
デバイス管理の方法	MDMを利用 (Intune Co-managementも利用可能)	GPO、SCCMを利用 (Intune Co-managementも利用可能)

Windowsデバイス管理のベストプラクティスとは

Q: Microsoft Entra hybrid joinとMicrosoft Entra joinどちらが良い？
→既存オンプレADに参加済みのWindowsデバイスは、Hybrid Azure join
新しいWindowsデバイスはMicrosoft Entra joinを検討する

- Microsoft Entra joinにより、DCとの接続性(社内ネットワーク)への依存がなくせる
- Microsoft Entra joinで運用するための準備を進める
 1. GPO(グループポリシー)管理→Intune(MDM)管理
 2. デバイスセットアップのプロセスがモダン化される(Autopilot)

Windowsデバイス管理の ベストプラクティス

1

Microsoft Entra hybrid joinの構成にする

2

Microsoft Entra Joinでも運用ができるように準備する

3

準備ができたなら新規端末からMicrosoft Entra Join に切り替える

第5章

セキュリティを高めるために



5. セキュリティを高めるために

多要素認証(MFA)

- Entra IDで多要素認証を有効にし、シンプルな認証(本人確認)方法を2つ組み合わせて、認証を強化する
 1. ユーザーが知っているもの(通常はパスワード)。
 2. ユーザーが持っているもの
(携帯電話やハードウェア キーのように、簡単には複製できない信頼できるデバイスなど)
 3. ユーザー自身(指紋スキャンや顔面認識などの生体認証)。



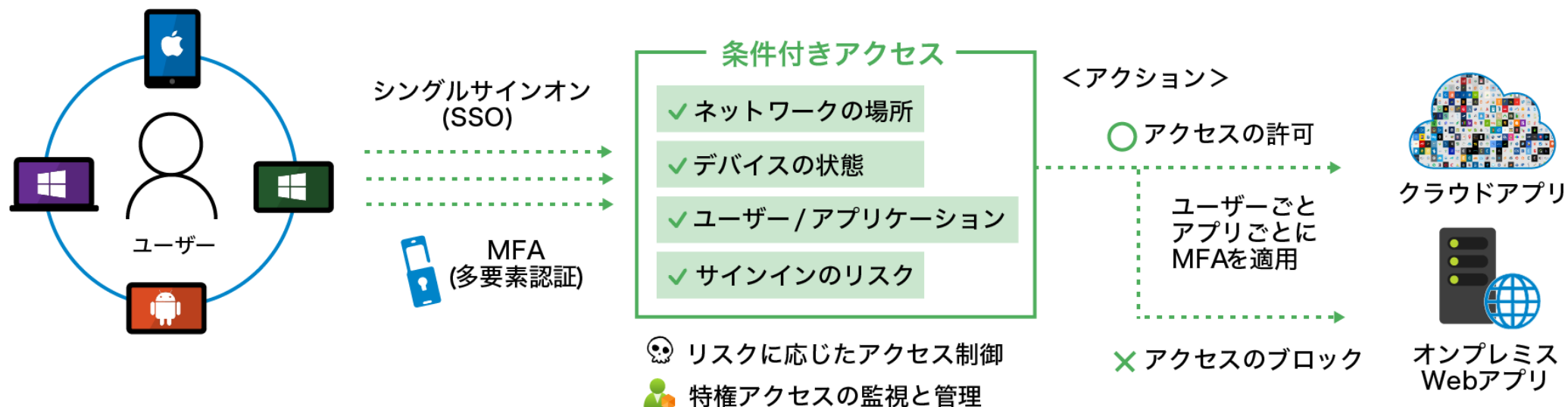
5. セキュリティを高めるために

Microsoft
Entra ID P1

Microsoft
Entra ID P2

条件付きアクセス

- 標的型攻撃の入口対策の1つ
- Intuneと組み合わせることで、デバイスベースのアクセス制御を行える。
※その場合は別途Microsoft Intune ライセンスが必要

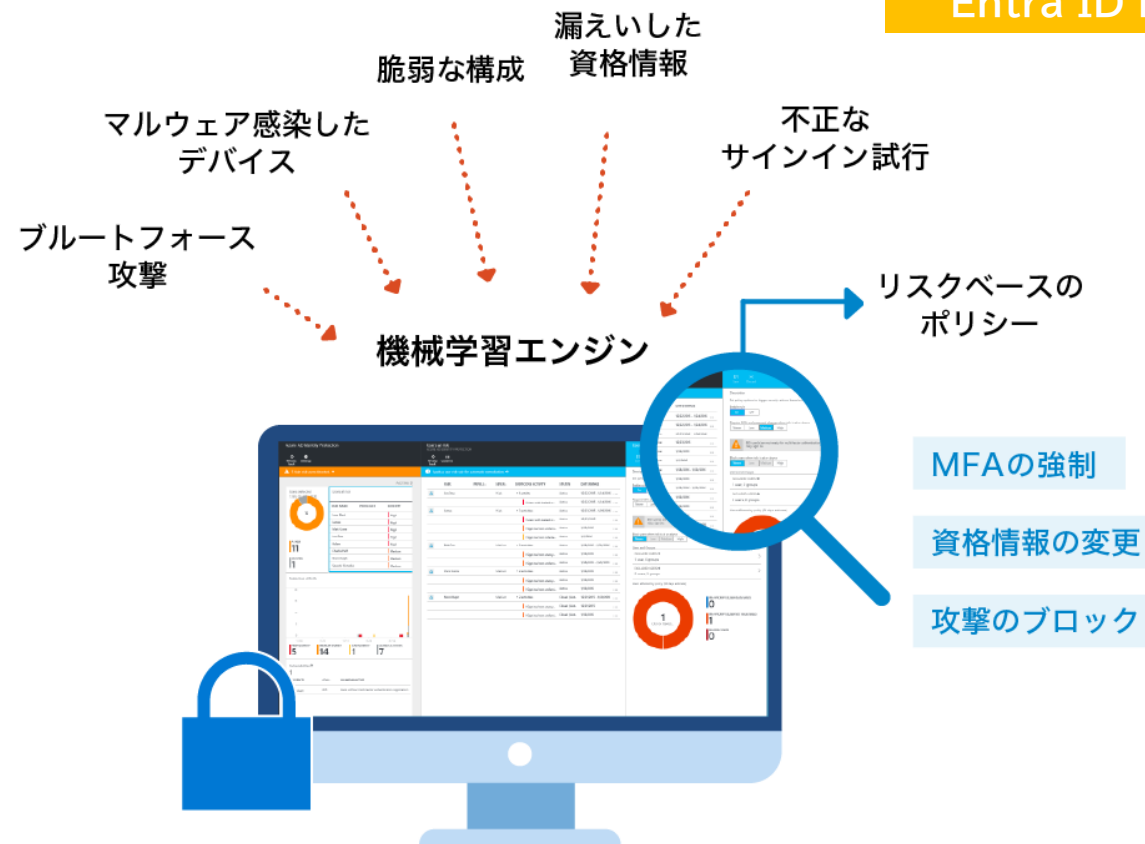


5. セキュリティを高めるために

Microsoft Entra ID Protection

- 機械学習エンジンとヒューリスティックルールにより、以下を検出する
 - 脆弱なアカウント
 - 怪しいサインインイベント
 - 怪しいユーザーイベント
- リスクイベントの内容に基づいてリスクレベルを計算し、レポートとアラートを生成する。
- リスクレベルに基づいて、ポリシーを実行し、組織のIDを自動的に保護する。
※手動で対応することも可能

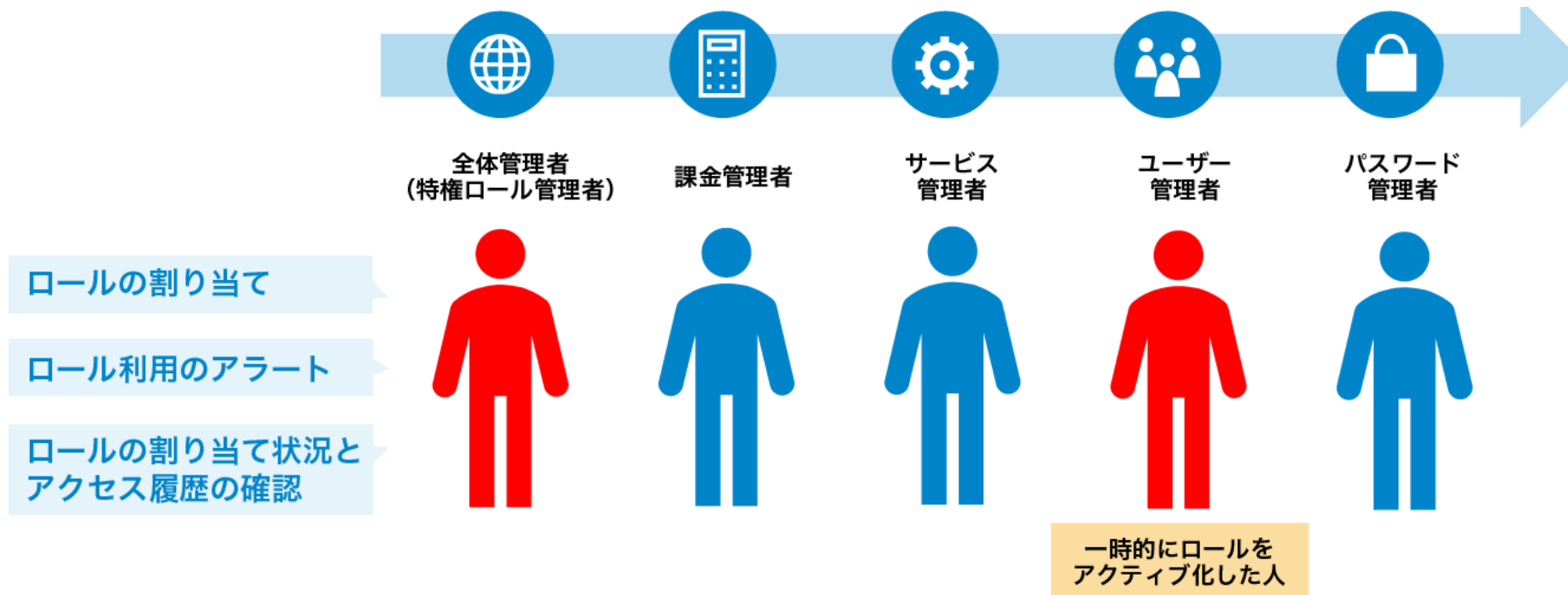
Microsoft
Entra ID P2



Microsoft Entra Privileged Identity Management(特権ID管理)

Microsoft
Entra ID P2

- PIMにより、Microsoft Entra ID の管理者権限が割り当てられているユーザーの特定や権限の利用状況、権限の一時的な割り当て、アラートなど権限の利用を一元的に管理が可能



ご清聴ありがとうございました