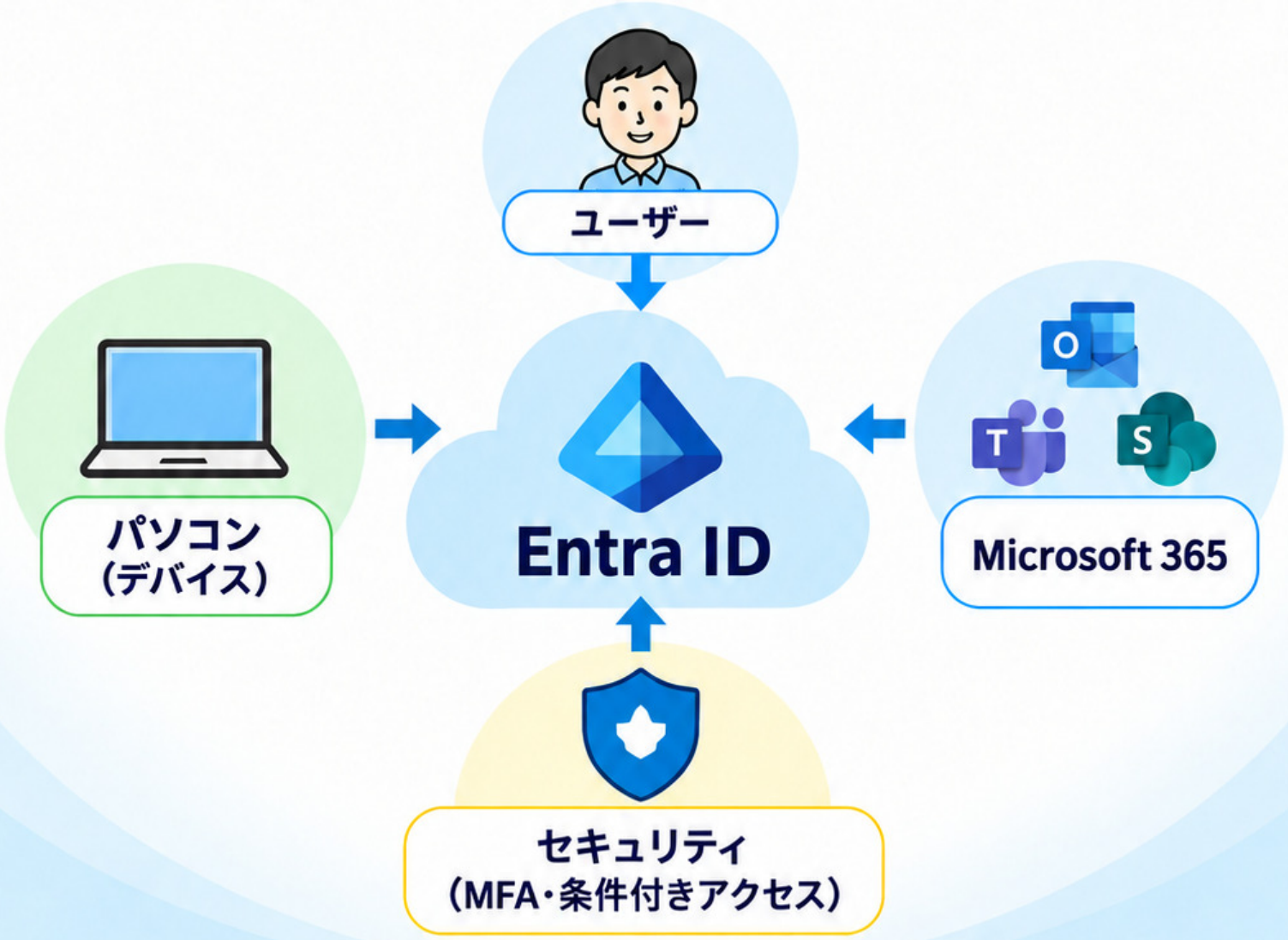
情シス初心者のための
図でわかる
Entra ID 入門

Microsoft 365の「ユーザー」「パソコン」「MFA」
「条件付きアクセス」がつながってわかる



難しい言葉を覚える前に、まず全体像を理解する。

Microsoft Entra IDを初めて学ぶ
情シス担当者・PC管理担当者のための入門書

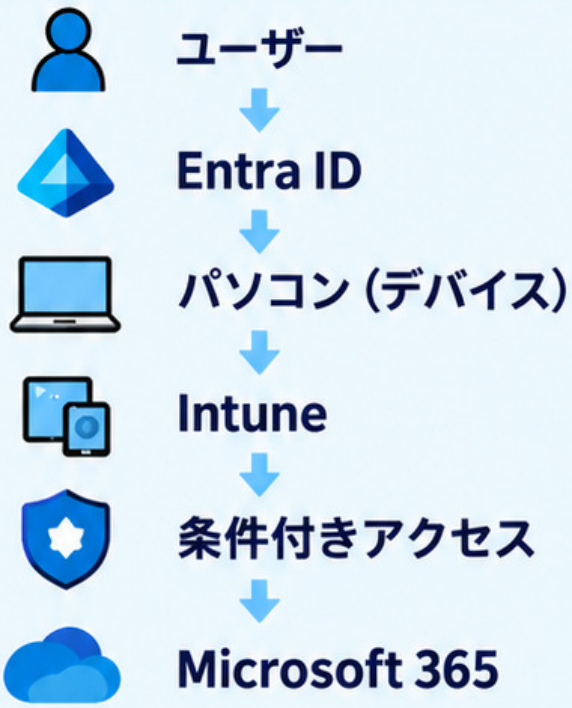
1 この本は何のための本？

Entra IDを調べると、知らない言葉が次々に出てきませんか？

結局、何がどうつながっているの？

この本では、最初から全部覚えません。
まず、「それぞれが何のためにあるのか」を図でつなげます。

この本を読み終わると…



この流れが
「ああ、そういうことか」
と分かる状態を目指します。

ここだけ覚える

細かい設定方法を覚える前に、
まず全体の関係を理解しましょう。
Entra IDは、関係がつながると
一気に分かりやすくなります。

2 Entra IDって、そもそも何？

まずは、これだけ覚えてください。

Entra IDは「会社のログイン管理の中心」です。

会社では、「誰でも Microsoft 365 を使ってよい」わけではありません。
そこで Entra ID が、「あなたは誰ですか？」を確認します。
確認できたユーザーに、Microsoft 365 などの会社のサービスを
利用させます。

もう少しだけ正確にいうと

Entra ID では、「誰なのか」だけでなく、「何を使わせてよいのか」も
管理します。

ここだけ覚える

**Entra ID = 誰がログインしているのかを確認し、
何を使わせるかを管理する仕組み**

今はこれだけ分かれば十分です。

3 「Entra」と「Entra ID」は同じもの？

実は、同じではありません。

Microsoft の資料を見ると、「Microsoft Entra」と
「Microsoft Entra ID」という2つの名前が出てきます。
初心者が混乱しやすいところです。

Microsoft Entra

ID・アクセス・セキュリティ関連の製品グループ

Microsoft Entra ID
ユーザーやアクセスを管理する
中心的なサービス

- ID ガバナンス
- 外部 ID
  （ゲストユーザーなど）
- その他の
  Entra 製品

Entra とは？

Microsoft の ID・アクセス・
セキュリティ関連製品の
グループ名と考えてください。

Entra ID とは？

その中にある、ユーザーや
アクセスを管理する
中心的なサービスです。

たとえるなら…

Microsoft 365

Word / Excel / Teams / SharePoint など

＋

Microsoft Entra

Entra ID
その他の Entra 製品

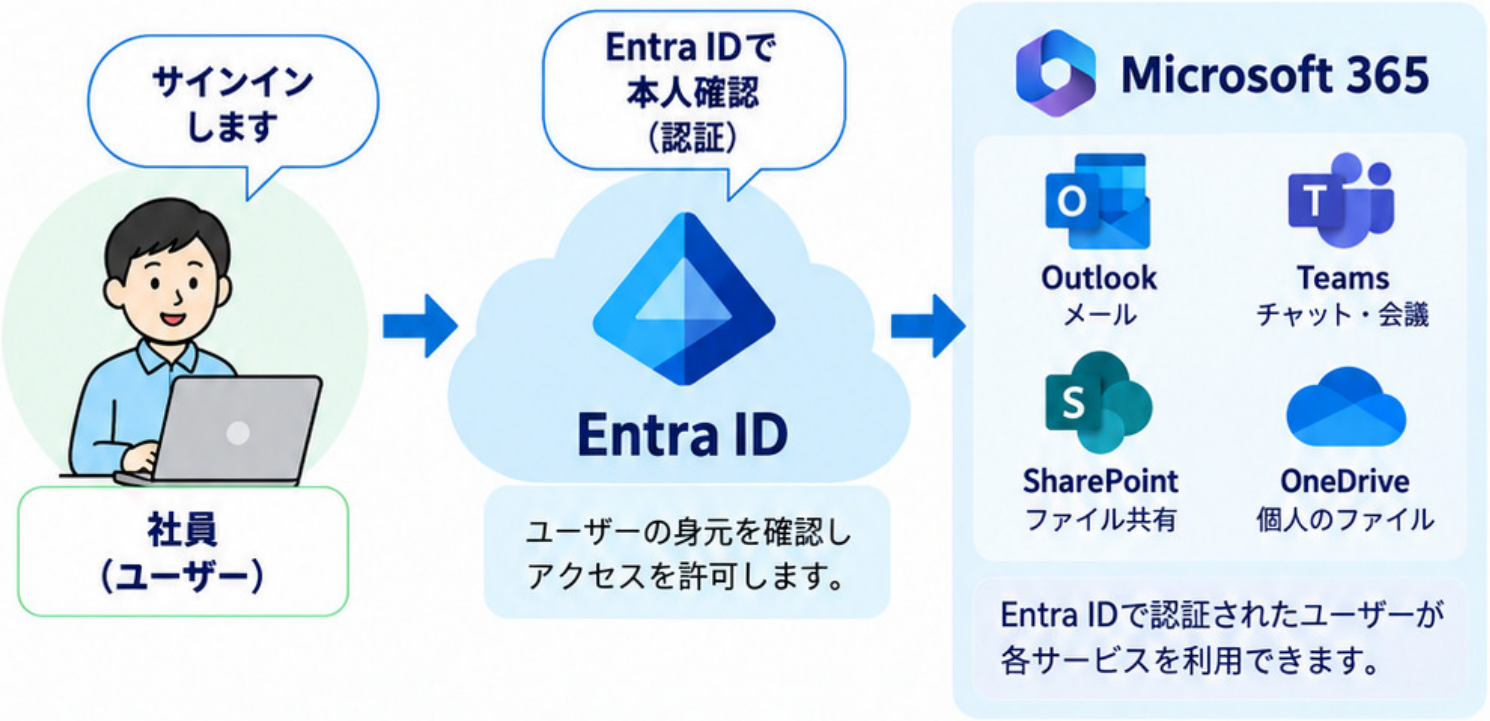
ここだけ覚える

Entra ＝ 製品ファミリ　Entra ID ＝ 今回学ぶ中心サービス

この本では、基本的に Entra ID を学びます。

4 Microsoft 365 と Entra ID はどうつながっている？

Microsoft 365を使うとき、裏側ではEntra IDが重要な役割を持っています。



Outlook、Teams、SharePoint、OneDrive など、Microsoft 365 にはそれぞれ役割を持つサービスがあります。これらのサービスはそれぞれ機能を提供していますが、**「誰が使えるのか」というユーザーの身元（ID）は、Entra IDで一元的に管理されています。**

シンプルに流れを表すと…

だからEntra IDが重要

会社でMicrosoft 365を使うには、「誰が使えるのか」をきちんと管理する必要があります。Entra IDは、Microsoft 365を利用するための**ユーザーを管理する中心の仕組み**です。

ここだけ覚える

Microsoft 365を使う「人」を管理する中心が Entra ID

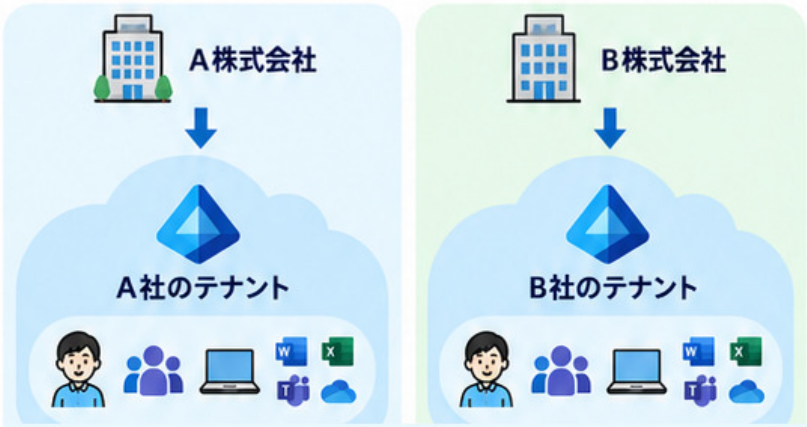
次のページでは…… 会社ごとにユーザーをどこへ登録しているのか？そこで登場するのが「テナント」です。 »»

5 テナントって何？

Entra IDで、組織が利用する“専用の管理スペース”がテナントです。

テナントは、組織が利用する独立した管理スペースです。
ユーザー、グループ、デバイス、設定などをこの中で管理します。

テナントは互いに独立した管理領域です



通常、別テナントのユーザーや設定は
直接管理できません。

テナントの中にあるもの

ユーザー
サインインする人のアカウントです。

グループ
ユーザーをまとめたグループです。

デバイス
会社で使うパソコンやスマートフォンなどのデバイスです。

ライセンスや設定
Microsoft 365 のライセンスや、セキュリティなどの各種設定です。

ここだけ覚える

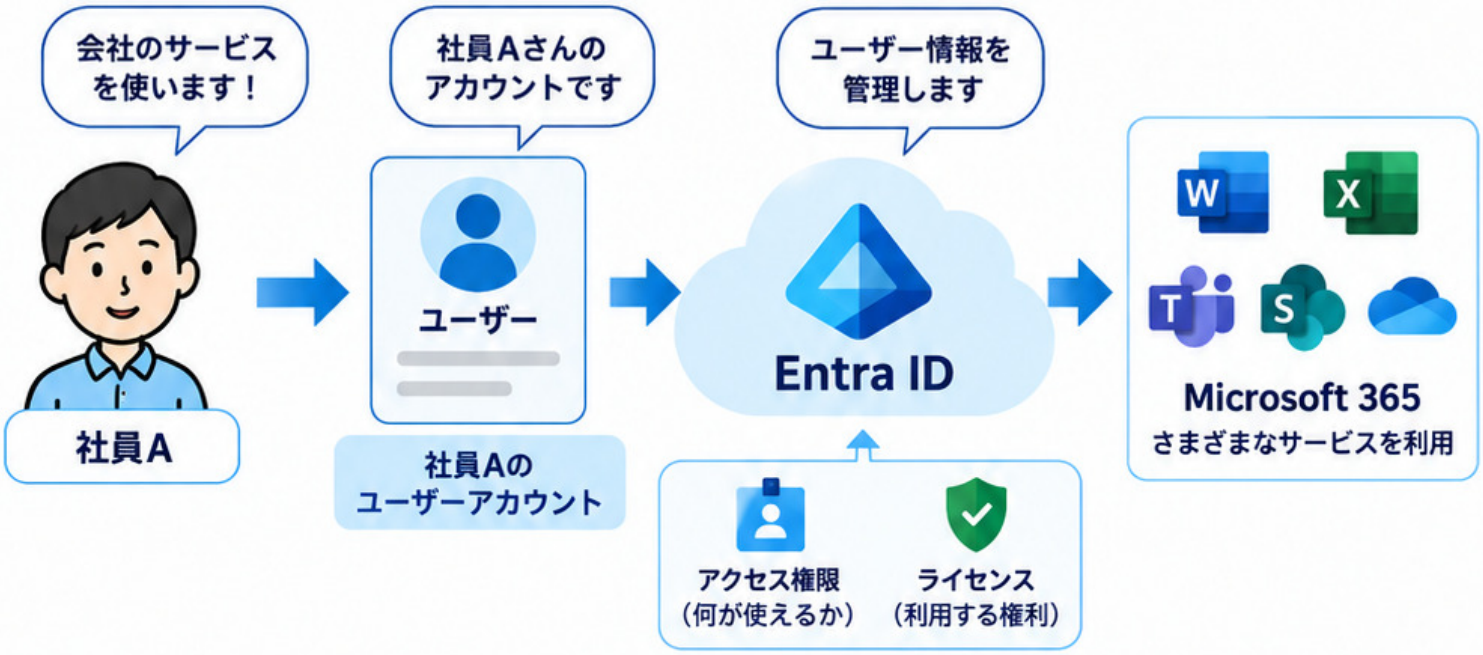
テナント ＝ 組織が利用する独立した管理スペース

次のページでは……

テナントの中で、実際にサインインする「ユーザー」を見ていきます。

6 ユーザーって何？

ユーザーは、会社でサービスを使う人の“アカウント”です。



ユーザーは、会社でサインインするための入口です。
誰がログインするのか、何を使えるのかを管理します。

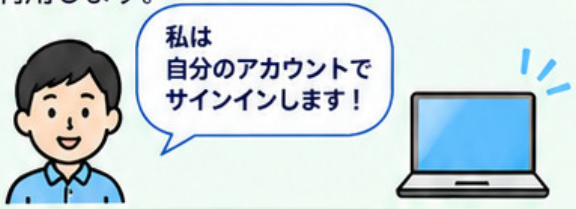
ユーザーで管理するもの

Entra ID のユーザーには、次のような情報を登録して管理します。

- **名前**（表示名・氏名）
- **サインイン ID**（メールアドレスなど）
- **ライセンス**（使えるサービス）
- **所属グループ**（役割・部署など）

1人に1つが基本

通常、1人の社員に対して1つのユーザーアカウントを使います。それぞれの人が自分のアカウントでサインインし、許可されたサービスを利用します。



1人に1つのアカウントで、安全にサービスを利用できます。

ここだけ覚える

ユーザー ＝ 会社で使う人のアカウント

ユーザーは、会社のサービスにサインインするための入口です。誰が、何を使えるのかを管理します。

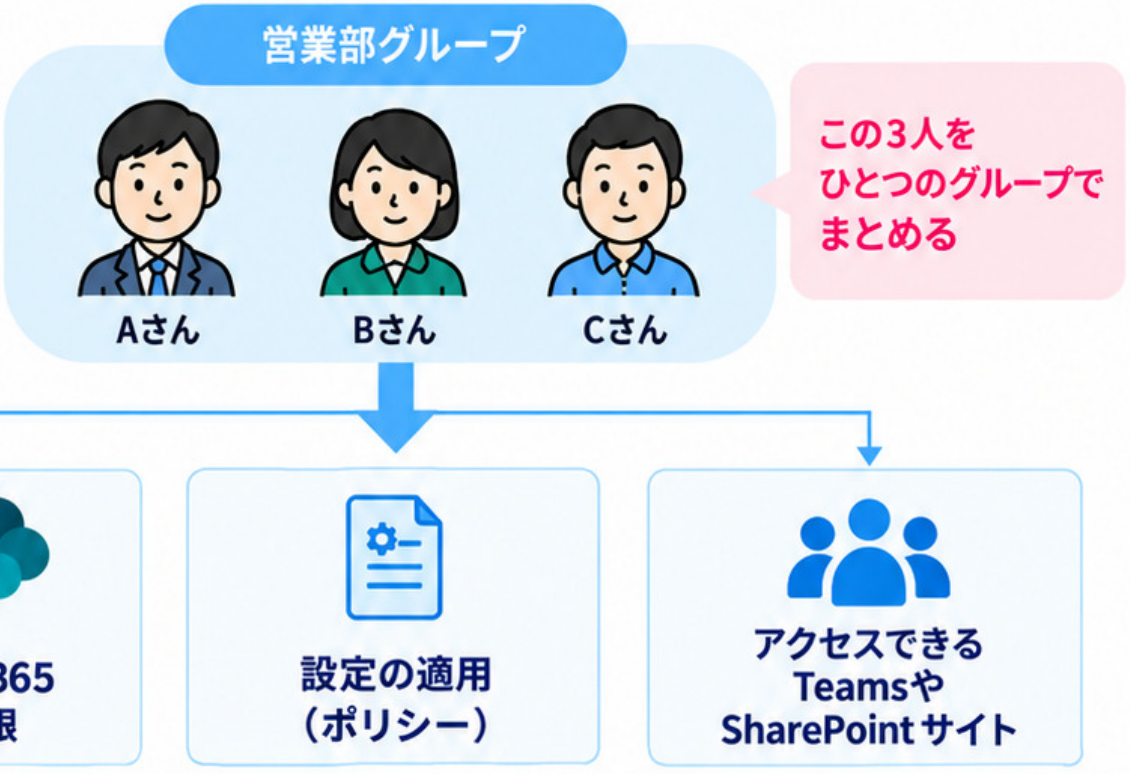
次のページでは……
複数のユーザーをまとめて管理しやすくする「グループ」を見ていきます。

7 グループって何？

グループは、ユーザーをまとめるための「グループ（入れ物）」です。

Entra IDでは、複数のユーザーをまとめて、同じ設定や権限を適用するために「グループ」を使います。

グループのイメージ



グループに設定すれば、1人ずつ設定する必要がありません。

グループの種類（主なもの）

セキュリティ グループ
アクセス制御の管理によく使います。

Microsoft 365 グループ
TeamsやSharePointなどの共同作業に使います。

配布グループ
メールの一斉送信などに使います。
（アクセス制御には使いません）

まずは「ユーザーをまとめるための入れ物」と覚えましょう！

ここだけ覚える

グループ ＝ ユーザーをまとめて同じ設定や権限を適用するための入れ物

8 なぜグループを使うの？

グループを使うと、管理がラクでミスも減ります。

グループを使わずに１人ずつ設定すると、ユーザーが増えるたびに作業が必要になり、
時間がかかり、設定漏れの原因になります。

グループを使わない場合（1人ずつ設定）

- Aさんに設定
- Bさんに設定
- Cさんに設定
- ⋮

- 時間がかかる
- 設定漏れのリスク
- あとからの変更も大変

グループを使う場合（まとめて設定）

営業部グループに設定

- Aさん
- Bさん
- Cさん
- ⋮

- 1回の設定でOK
- 設定漏れが減る
- あとからの変更も簡単

ユーザーが増えても、グループに入れるだけで同じ設定が自動的に適用されます。

グループの活用例

Teams	✔ 部署ごとのチームメンバー管理 ✔ 特定のチームだけ利用を許可
SharePoint	✔ サイトのアクセス権限 ✔ 部署ごとの共有フォルダー管理
Microsoft 365（ライセンス）	✔ グループ単位でライセンスを割り当て ✔ 追加・削除もグループの変更だけ
デバイス・ポリシー（Intune）	✔ 部署ごとに異なる設定を適用 ✔ グループでまとめて管理

ここだけ覚える

グループを使うと、まとめて設定できて管理がラクになる

9 管理者とロールって何？

管理者は、設定できる範囲が違います。「ロール」で必要な権限だけを割り当てます。

Entra IDでは、ユーザーごとに「ロール」を割り当てて、できることの範囲を決めます。
全員にすべての権限を与えるのではなく、必要な人に必要な権限だけを付与するのが基本です。

管理者と一般ユーザーの違い

一般ユーザー

- 普段の業務で利用するユーザー
- 自分の情報は変更できる
- 他のユーザーや設定は変更できない

管理者

- Entra IDの設定を管理できる
- ユーザー・グループ・デバイスなどを管理できる
- ロールによってできる範囲が異なる

主な管理者ロールの例

ロール名	主なできること
グローバル管理者	すべての設定を管理できる（強力な権限）
ユーザー管理者	ユーザーとグループの管理
クラウド デバイス管理者	デバイスの管理
セキュリティ管理者	条件付きアクセスやセキュリティ設定の管理
ヘルプデスク管理者	パスワードのリセットなどサポート業務

なぜ必要な権限だけにするの？

必要な権限だけを
割り当てることで、
より安全に運用できます！

- 誤操作のリスクを減らす
- 不正アクセスのリスクを減らす
- 責任の範囲を明確にする
- 監査・記録を残しやすくする

ここだけ覚える

ロール ＝ できることの範囲
必要な人に、必要な権限だけを割り当てる

10 デバイスって何？

デバイスは、会社で使うパソコンやスマートフォンなどの“端末”です。

Entra IDでは、「誰が使うか」だけでなく、「どの端末を使うか」も管理します。

ユーザーとデバイス

デバイスの例

パソコン
会社で使うノートPCやデスクトップPCなどです。

スマートフォン
会社で使うiPhoneやAndroidなどです。

タブレット
会社で使うiPadやAndroidタブレットなどです。

なぜデバイスも大事なの？

デバイスを把握することで、より安全に会社の環境を守ることができます！

- 会社の端末かを確認するため
- 安全な端末かを判断するため
- どの端末でアクセスしているかを把握するため

ここだけ覚える

デバイス ＝ 会社で使う端末
Entra ID は「誰」だけでなく「どの端末」も見ている

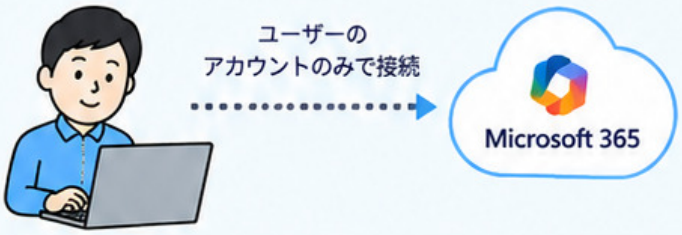
11 パソコンを Entra ID に登録するとどうなる？

パソコンを Entra ID に登録すると、このPC は組織と関係のある端末だと認識されます。

パソコンを Entra ID に登録（参加）すると、Entra ID がそのパソコンを「組織のデバイス」として管理できるようになり、ユーザー・デバイス・アプリを組み合わせた、より安全なアクセス制御ができるようになります。

登録前と登録後の違い

登録前（個人のパソコン）



- パソコンは個人の端末として扱われる
- 端末の状態（更新プログラム、暗号化など）はわからない
- ユーザーのアカウントだけでサービスにサインインする

登録後（Entra ID に登録されたパソコン）

- パソコンが Entra ID に登録され、組織のデバイスとして認識される
- 端末の情報（種類・状態・所有者など）を管理できるようになる
- ユーザー＋デバイスの両方を使ったアクセス制御が可能になる

Entra ID に登録することでできること

より安全なアクセス

- 特定の端末からのみアクセスを許可
- 会社のルールを満たした端末だけアクセスを許可
- 不正な端末からのアクセスを防止

端末の情報を管理

- どのような端末が登録されているかを確認できる
- OS の種類やバージョン、所有者の情報を管理できる

Intune と連携

- 登録された端末を Intune で管理できる
- セキュリティ設定やアプリの配布が可能になる

条件付きアクセスに活用

- 端末の状態（準拠しているか）を条件にしてアクセスを制御できる
- 社外からのアクセス時に、管理されていない端末はブロックするなどの対策ができる

登録によって管理できる主な情報

Entra ID に登録されたパソコンの例

デバイス名	PC-001
デバイスの種類	Windows
OS のバージョン	Windows 11
所有者	会社（組織所有）
登録の状態	Entra ID に登録済み
管理の状態	Intune で管理中
準拠の状態	準拠（コンプライアント）

このような情報をもとに、「この端末は安全かどうか」を判断できます。

- OS は最新か
- 暗号化が有効か
- 会社が許可した端末か
- Intune で管理されているか
- 組織のセキュリティルールに準拠しているか

パソコンを Entra ID に登録することで、
ユーザーと端末の両方を使った、より安全な環境を作ることができます。

ここだけ覚える

パソコンを Entra ID に登録すると、組織のデバイスとして管理でき、より安全なアクセス制御ができるようになる

12 Registered・Joined・Hybrid Joinedって何？

パソコンを Entra ID に登録する方法は3種類あります。

パソコンを Entra ID に登録（デバイス登録）する方法には、「Microsoft Entra registered」「Microsoft Entra joined」「Microsoft Entra hybrid joined」の3種類があります。それぞれの特徴と利用シーンを理解しておきましょう。

3種類の違い（概要）

Microsoft Entra registered
（登録済みデバイス）

既存のパソコンに、組織アカウントを追加して登録する方法

既存の Windows / macOS / スマートフォンなどを Entra ID に登録

主な対象	個人所有の端末（BYOD など）
サインイン方法	個人のアカウント＋組織アカウントを追加
管理の範囲	ユーザーのアカウント情報（デバイスの一部情報のみ）
主なメリット	既存端末をそのまま使える 導入が簡単
主な制限	デバイスの詳細な管理はできない

Microsoft Entra joined
（参加済みデバイス）

最初から Entra ID に参加させて使用する方法

セットアップ時や初期化後に Entra ID に参加して使用

主な対象	組織が所有する端末（会社のパソコン）
サインイン方法	通常は組織アカウント（Entra ID アカウント）
管理の範囲	デバイスの情報を管理（Intune と連携して詳細な管理が可能）
主なメリット	強固な管理ができる セキュリティが高い
主な制限	個人利用の端末には不向き（初期設定が必要）

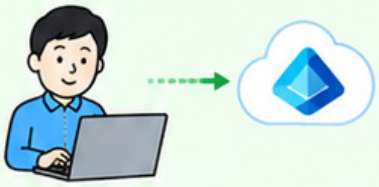
Microsoft Entra hybrid joined
（ハイブリッド参加済みデバイス）

オンプレミスの Active Directory と Entra ID の両方に参加する方法

主な対象	既存のオンプレミス環境がある組織の端末
サインイン方法	社内の Active Directory アカウント（オンプレミスのアカウント）
管理の範囲	オンプレミスと Entra ID の両方で管理（Intune とも連携可能）
主なメリット	既存のオンプレミス環境を活かせる 段階的なクラウド移行ができる
主な制限	構成がやや複雑 オンプレミス環境が必要

利用シーンのイメージ

個人や持ち込み端末の例

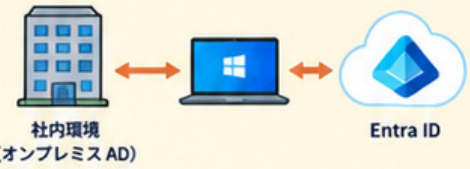


- 自宅のパソコンを業務でも使いたい
- 個人のスマートフォンで会社のメールを使いたい
- 会社から支給されていない端末を利用する

会社のパソコンの例

- 会社から支給されたパソコンを使用
- 最初から Entra ID に参加させて運用
- Intune と連携してセキュリティ設定を適用する

既存環境がある会社の例



- 既に社内に Active Directory がある
- 従来の環境を維持しながらクラウドも活用
- 段階的にクラウドへ移行したい

利用する端末の種類や会社の環境に応じて、最適な登録方法を選びましょう。

ここだけ覚える

パソコンを Entra ID に登録する方法は、「registered」「joined」「hybrid joined」の3種類がある

13 会社のパソコンならどれを使う？

使う端末や会社の環境によって、選ぶ登録方法が変わります。

前のページで見た registered・joined・hybrid joined は、どれが一番良いというより、どんな端末・どんな会社環境で使うかで選びます。

まずは3つの考え方

個人の端末を使う

registered

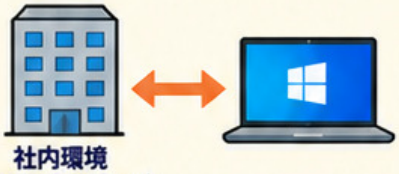
- BYODや持ち込み端末
- 個人PC・個人スマホで会社サービスを使う
- 端末そのものの強い管理には向かない

会社のパソコンを使う

joined

- 会社支給のWindows PC
- Entra ID中心で運用
- Intuneと相性が良い

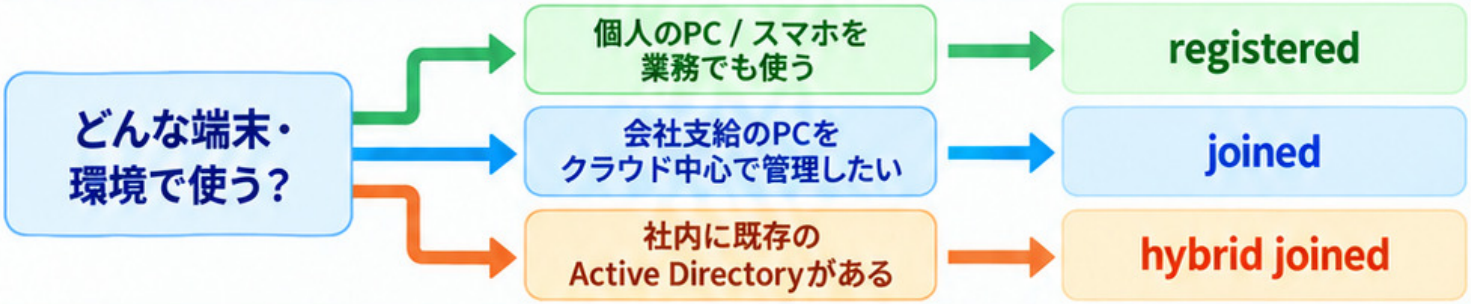
既存の社内ADがある



hybrid joined

- 既存のActive Directoryあり
- 従来の社内環境を活かす
- 段階的にクラウドへ移行しやすい

選び方の目安



初心者向けの考え方

BYODなら registered を考える

会社支給PCなら joined をまず考える

既存ADがある会社は hybrid joined も候補

ここだけ覚える

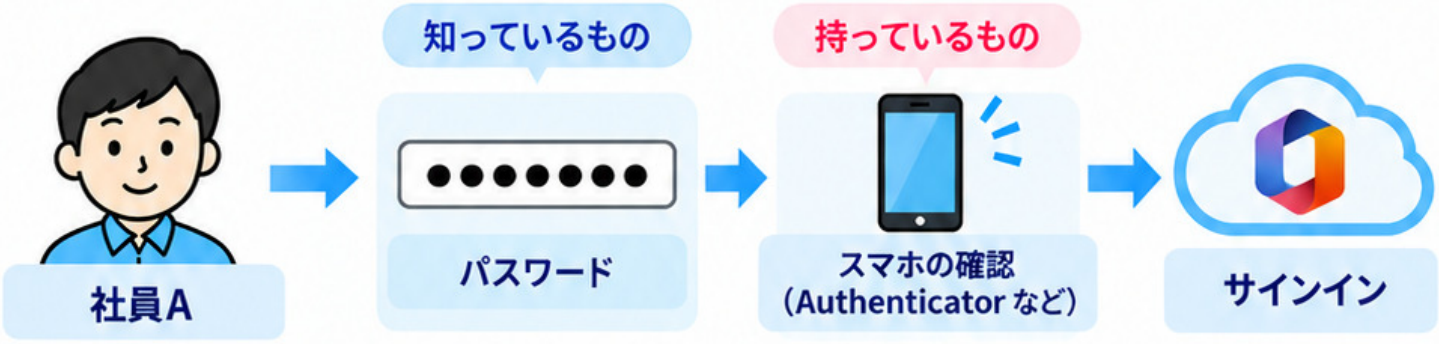
個人端末なら registered
会社PCなら joined
既存ADがあるなら hybrid joined を考える

14 MFAって何？

MFAは、異なる種類の認証要素を2つ以上組み合わせて本人確認する仕組みです。

MFAは「多要素認証」のことです。Entra IDでは、サインイン時に本人確認を強化するために使います。

MFAのイメージ



2つの確認を組み合わせて、本人かどうかをより確実に確認します。

なぜMFAが必要なの？

パスワードだけ

- パスワードが漏れると突破されることがある
- フィッシングや使い回しに弱い
- 本人かどうかの確認が足りない

MFAあり

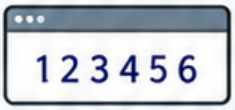
- パスワードだけでは入れない
- スマホ確認などが必要
- 不正サインインのリスクを減らせる

MFAの例

Authenticatorアプリ

通知を承認する

確認コード



6桁のコードを入力

SMS

届いたコードで確認

MFAで覚えたいこと

まずは「パスワード＋もう1つ」と覚えればOKです！

- パスワードだけより安全
- 本人確認を強化できる
- 条件付きアクセスと組み合わせて使うことが多い
- 会社のMicrosoft 365利用でも重要

ここだけ覚える

MFA＝異なる種類の認証要素を2つ以上組み合わせて本人確認を強くする仕組み

15 認証とアクセス許可は同じ？

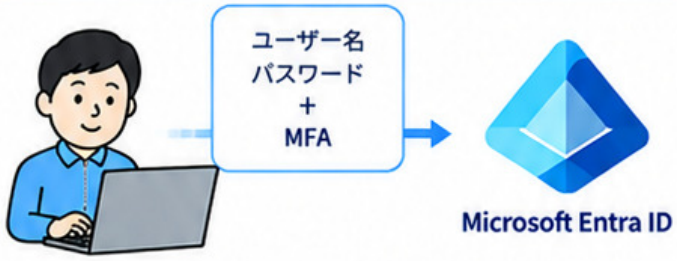
「認証」と「アクセス許可」は別のものです。

Microsoft 365 を利用する際には、まず「あなたは誰か？」を確認するための認証が行われます。
その後、「そのユーザーに、このサービスを使わせてよいか？」を判断して、アクセスが許可されます。
認証とアクセス許可は役割が異なり、組み合わせて使うことで、より安全な環境を実現できます。

① 認証（Authentication）

あなたは誰ですか？を確認する

サインイン時に、ユーザーが本人であることを確認します。
パスワードや MFA などを使って、なりすましを防ぎます。

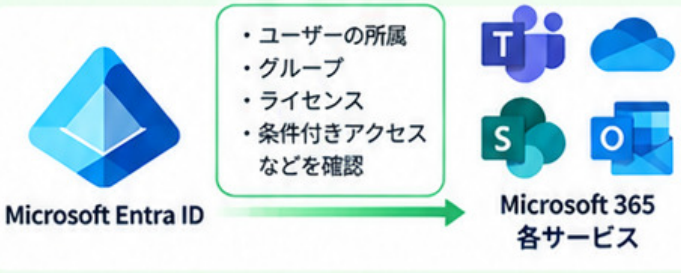


認証で使われる主な方法

② アクセス許可（Authorization）

このサービスを使わせてよいですか？を判断する

認証が成功した後に、そのユーザーに対して、どのサービスやデータにアクセスを許可するかを判断します。
ユーザーの所属、役割、グループ、条件付きアクセスなどのポリシーに基づいて制御されます。



アクセス許可で使われる主な要素

全体の流れ

具体例で見てみましょう

例 1：認証は成功したが、アクセスが許可されない

正しいパスワードと MFA でサインインできたが、
特定のグループに所属していないため、
SharePoint のサイトにアクセスできない。

例 2：アクセス条件を満たしていないため拒否される

正しい認証はできたが、
会社のルールに準拠していない端末
（Intune で管理されていない端末）からの
アクセスのため、条件付きアクセスにより
Microsoft 365 へのアクセスがブロックされる。

ここだけ覚える

**認証は「あなたは誰か？」を確認し、
アクセス許可は「使わせてよいか？」を判断する。これらは別のものです。**

16 条件付きアクセスって何？

条件付きアクセスは、『もし〇〇なら△△する』でアクセスを制御する仕組みです。

条件付きアクセスは、サインインした人や端末の状態などを見て、Microsoft 365 へのアクセスを許可するか、MFAを求めるか、ブロックするかを決めます。

条件付きアクセスの考え方

条件を見て、「どうするか」を決めます。

具体例

社外からアクセス

MFAを要求

いつもと違う場所なら、本人確認を強化

会社PCからアクセス

許可

会社が認識している端末なら、利用を許可しやすい

会社ルールを満たしていない端末

ブロック

安全でない端末からのアクセスを止める

何のために使うの？

- 不正アクセスのリスクを減らす
- MFAを必要なときだけ求められる
- 安全な端末だけ利用を許可できる
- 会社のルールに合わせたアクセス制御ができる

ここだけ覚える

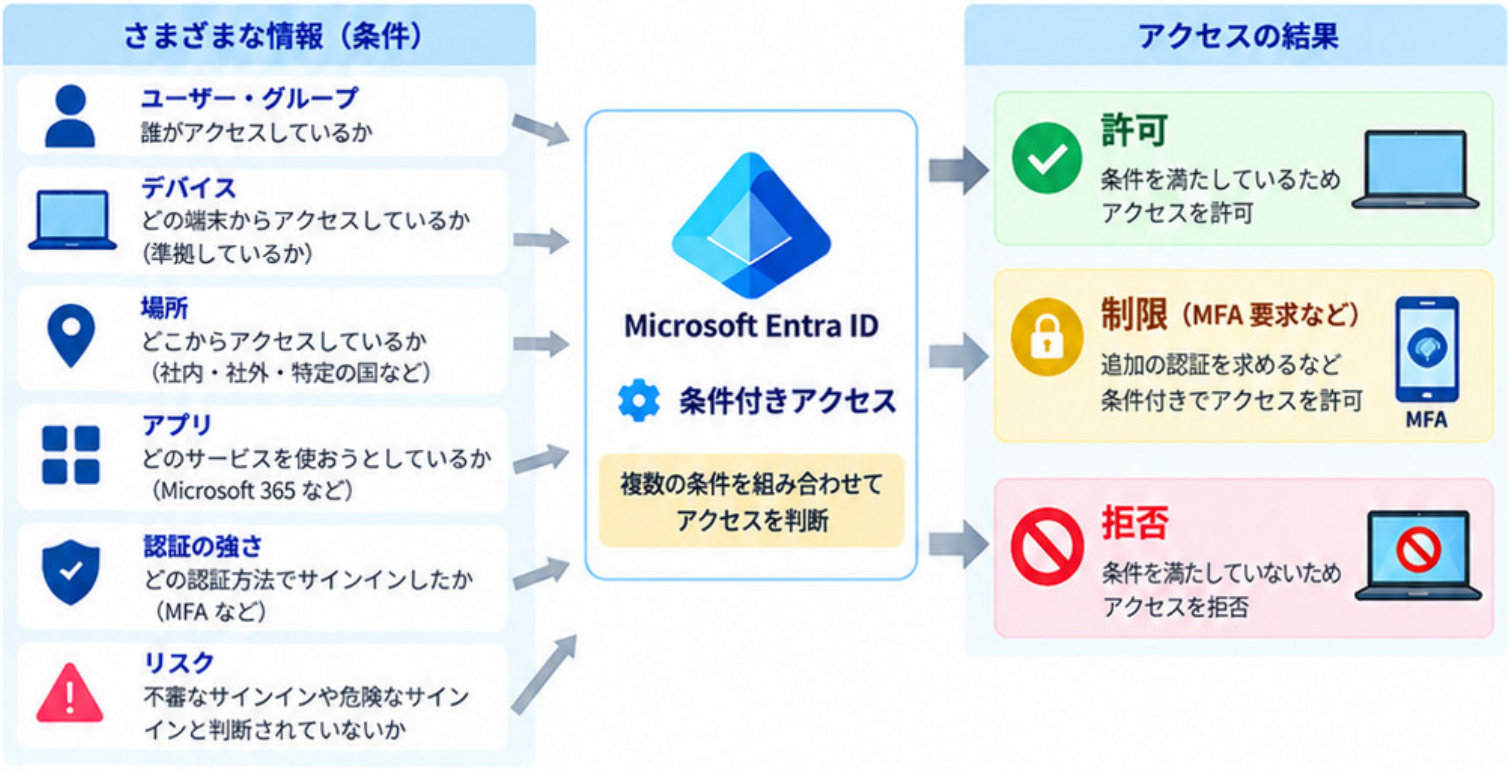
条件付きアクセス＝『どんな条件なら使わせるか』を決める仕組み

17 条件付きアクセスは何を見ている？

条件付きアクセスは、さまざまな情報を組み合わせてアクセスを判断します。

条件付きアクセスは、単に「場所（IPアドレス）」だけを見ているわけではありません。
ユーザー・グループ・デバイスの状態・場所・アプリ・認証の強さ（MFA）・リスク など、複数の条件を組み合わせて、そのアクセスを許可するか、制限するか、拒否するかを判断します。

条件付きアクセスの判断イメージ



主な条件の詳細

ユーザー・グループ
- 特定のユーザー
- 特定のグループ
- 役割（管理者など）

デバイス
- 準拠しているか（Intune の準拠状態）
- デバイスの種類
- 登録の種類（Joined / Registered など）

場所
- 社内ネットワーク
- 特定の IPアドレス
- 特定の国 / 地域
- 匿名の通信（VPN / プロキシ）

アプリ
- Microsoft 365
- 特定のアプリ
- すべてのクラウドアプリ
- カスタムアプリ

認証の強さ
- MFA の有無
- 認証方法の種類
- 認証強度（強/中など）

リスク
- ユーザーのリスク
- サインインのリスク
- 危険なサインイン
- 新しい場所からのアクセス

具体的な判断例

例1：社外からのアクセスは MFA を要求

- 条件：場所 ＝ 社外
- 結果：MFA を要求
- 目的：社外からの不正アクセスを防止

例2：Intune で準拠していない端末は拒否

- 条件：デバイスの状態 ＝ 非準拠
- 結果：アクセスを拒否
- 目的：セキュリティ要件を満たさない端末の利用を防止

例3：特定のアプリは管理者だけ許可

- 条件：アプリ ＝ 管理用ポータル
  ユーザー ＝ 管理者グループ
- 結果：アクセスを許可
- 目的：管理者以外の誤操作や情報漏えいを防止

ここだけ覚える

条件付きアクセスは、ユーザー・デバイス・場所・アプリ・認証・リスク など複数の情報を組み合わせて、アクセスを判断する

18 Entra IDとIntuneは何が違う？

Entra IDは「誰・どのデバイスか」を管理し、Intuneは「そのデバイスをどう管理するか」を管理します。

Entra IDとIntuneは、どちらもMicrosoftのクラウドサービスですが、役割が異なります。
Entra IDでユーザーとデバイスを識別し、Intuneでデバイスの設定・セキュリティを管理します。
この2つが連携し、条件付きアクセスで「安全なデバイスからのみアクセスを許可する」といった制御が実現できます。

Microsoft Entra ID（ID とアクセスの管理）

誰が・どのデバイスで・どのサービスにアクセスするのかを管理する

主な役割	• ユーザー、グループ、デバイスの識別 • 認証（サインイン） • アクセス制御（条件付きアクセス など）
管理するもの	• ユーザー（アカウント） • グループ • デバイスの登録状態 • サインインの履歴・リスク
主な機能	• Azure Active Directory（Entra ID） • 条件付きアクセス • 多要素認証（MFA） • ID Protection（リスク検出）など
得られる効果	• 適切な人が適切なデバイスから適切なサービスにアクセスできる • 不正アクセスの防止

Microsoft Intune（デバイスの管理）

登録されたデバイスに対して、設定・セキュリティ・アプリを管理する

主な役割	• デバイスの設定管理 • セキュリティポリシーの適用 • アプリの配布 • デバイスの状態を監視
管理するもの	• Windows / macOS / iOS / Android などのデバイス • デバイスの設定（構成プロファイル） • セキュリティ対策（準拠ポリシー） • 業務用アプリ
主な機能	• MDM自動登録（Windowsなど） • 構成プロファイル • コンプライアンスポリシー • アプリの配布 • リモートワイプ、紛失対策 など
得られる効果	• 会社のルールに従った安全なデバイス利用 • セキュリティ設定の標準化 • 紛失・盗難時の対応

3つのサービスの関係

Microsoft Entra ID
- ユーザーとデバイスを識別
- 認証を行う
- 条件付きアクセスでアクセスを制御

→ デバイスの状態を連携

Microsoft Intune
- デバイスを管理
- 設定やセキュリティを適用
- デバイスの準拠状態（コンプライアンス）を評価

→ 評価結果を条件付きアクセスに連携

条件付きアクセス
- ユーザー・デバイス・場所などの条件を評価
- 許可 / 制限（MFA要求）/ 拒否 を実行
- 安全なデバイスからのみ Microsoft 365 などにアクセス

具体例で比較してみましょう

例：新しいパソコンを会社で利用する場合

1. IntuneへMDM自動登録される
2. Intune に自動で登録される
3. Intune からセキュリティ設定やアプリを適用する

例：会社のルールに準拠していないパソコンでアクセスした場合

1. Intune で「準拠していない」と判定
2. 条件付きアクセスがその情報を受け取りアクセスを制限
3. Microsoft 365 にアクセスできない

ここだけ覚える

Entra ID は「誰・どのデバイスか」を管理し、Intune は「そのデバイスをどう管理するか」を管理する

19 デバイスの登録方法（Windows の例）

Windows のパソコンを Entra ID に登録し、Intune に自動登録することができます。

Windows 11では、初期設定時などに会社のアカウントで Microsoft Entra ID へ参加すると、設定により Intune へ自動登録できます。管理者側であらかじめ自動登録を設定しておくと、ユーザーの操作を減らしてスムーズに登録できます。

登録の流れ（Windows 11 の例）

1 会社アカウントでサインイン

Windows の初期設定または設定から、会社のアカウントでサインインします。

2 Entra ID に参加

初期設定や設定画面で Microsoft Entra ID への参加を選ぶと、組織のデバイスとして参加します。

3 Intune に自動登録

自動登録の設定により、Intune にデバイスが自動的に登録されます。

4 ポリシーの適用

登録後、Intune から構成プロファイルやセキュリティポリシーが自動的に適用されます。

5 業務で利用開始

必要な設定が適用された状態で、業務に利用できます。

管理者側の事前設定

1. Microsoft Intune 管理センターで、対象ユーザーまたはグループに MDM ユーザー スコープを設定します。
2. **デバイスの登録制限（必要に応じて）**
   登録できるデバイスの種類（Windows / iOS / Android など）や、登録の上限数を設定します。
3. **構成プロファイル・ポリシーの作成**
   セキュリティ設定、アプリの配布、コンプライアンス ポリシーなどを作成し、対象のユーザーまたはデバイスに割り当てます。

自動登録の設定手順（Microsoft Intune 管理センター）

1. **Microsoft Intune 管理センターにサインイン**
2. **デバイス > 登録 > Windows > 自動登録 を開く**
3. **MDM ユーザー スコープを設定**
   ・すべて／一部／なし
4. 必要に応じて登録制限を設定
   ・プラットフォーム／OSバージョン
   ・所有形態／登録台数など
5. **設定を保存する**

登録後の確認方法

Entra ID での確認

- Microsoft Entra 管理センター
- デバイス > すべてのデバイス
- 登録されたデバイスの一覧で状態を確認

デバイス名	PC-001
OS	Windows 11
参加の種類	Microsoft Entra 参加済み
所有者	ユーザー名

Intune での確認

- Microsoft Intune 管理センター
- デバイス > すべてのデバイス
- 管理の状態、コンプライアンスの状態、適用されたポリシーを確認

デバイス名	PC-001
管理の状態	管理中
コンプライアンス	準拠
最終チェックイン	2026/09/16 10:24

よくある質問

Q ユーザーがサインインすると必ず Intune に登録されますか？
A いいえ。Microsoft Entra ID への参加など、自動登録の条件を満たしたときに登録されます。

Q 既に使用しているパソコンを後から登録できますか？
A はい。［職場または学校にアクセス］から［このデバイスを Microsoft Entra ID に参加させる］を選択します。

Q 個人のパソコンも登録されてしまいますか？
A MDM ユーザー スコープや登録制限で対象を制御できます。

Q 登録を解除するにはどうすればよいですか？
A Intune または Entra ID からデバイスを削除し、必要に応じて Windows 側の接続も解除します。

ここだけ覚える

Windows 11では、Microsoft Entra IDへの参加時に、設定済みなら Intuneへ自動登録できます。

ここまで読んだら、次はWeb版へ

Microsoft Entra IDを実際に使う

このPDFでは、Entra IDの全体像と主要な用語の関係を図で整理しました。
Web版では、各テーマの詳しい解説や実際の設定・運用に関する記事を公開しています。

PCエビデンス - Microsoft Entra ID 入門

https://pc-evidence.com/entra/

ユーザー・MFA・条件付きアクセス・Intuneまで、Webで詳しく確認できます。

利用時の注意

Microsoft製品の名称・画面・仕様は変更される場合があります。
実際の設定や運用では、最新のMicrosoft公式情報もあわせて確認してください。