【Microsoft Entra ID】
サービス概要とプラン比較

2025年4月30日

改定履歴

版数	発行日	改訂内容
第1版	2025年4月30日	初版発行

本資料の内容は 2025/4/30 時点のものです。製品のアップデートにより変更となる場合がございます旨でご了承ください。

Agenda

1. 前提情報
    1. 用語集
    2. 資料の構成と目的
2. Microsoft Entra ID とは
    1. Microsoft Entra ID とは
    2. Microsoft Entra ID と Active Directory の違い
    3. 他製品との比較
3. Microsoft Entra ID の主な機能
    1. Microsoft Entra ID の主な機能
    2. シングル サインオン (SSO)
    3. 多要素認証 (MFA)
    4. 条件付きアクセス
    5. ID 保護
    6. 特権 ID 管理
    7. セルフサービス
    8. 統合型の管理センター
4. Microsoft Entra ID プラン比較
    1. Microsoft Entra ID プラン比較
    2. Microsoft Entra の各プランを含むMicrosoft 365 ライセンス比較
    3. Microsoft Entra ID Free で利用できる機能
    4. Microsoft Entra ID P2 ライセンスで使える機能
    5. Microsoft Entra Suite について
    6. プラン選択のポイント

1. 前提情報

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	Microsoft Entra Permissions Management	クラウド環境のアクセス権限を管理するツール。たとえば、Microsoft Azure、アマゾン ウェブ サービス (AWS)、Google Cloud Platform (GCP) のマルチクラウド インフラストラクチャ全体で、過剰な特権が与えられたワークロードとユーザー ID、アクション、リソースなどが対象となる。
2	Kerberos	ネットワーク認証プロトコル。チケットを使って安全な通信を実現し、ユーザーの身元を確認する。
3	LDAP	ディレクトリサービスにアクセスするためのプロトコル。ユーザー情報やグループ情報の管理に使用され、検索や認証を行う。
4	Active Directory（AD）	Microsoftのディレクトリサービス。ユーザー、グループ、コンピュータなどのリソースを一元管理し、ネットワークのセキュリティを維持する。
5	IdP (Identity Provider)	ユーザー認証を提供するサービス。シングルサインオンをサポートし、複数のアプリケーションへのアクセスを簡素化する。
6	SAML (Security Assertion Markup Language)	XMLベースの認証・認可の標準規格で、WebブラウザとIdP（Identity Provider）、SP（サービスプロバイダ）間で認証情報を交換する。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
7	OpenID Connect	OAuth 2.0を基にした認証プロトコルで、ユーザーIDの確認を行い、JSON形式で情報を交換する。
8	WS-Federation	Microsoftが提案したWebサービス用のフェデレーションプロトコルで、異なるセキュリティドメイン間でのユーザー認証に使用される。
9	ゼロトラスト セキュリティ	従来の「社内は安全だが、外部は危険」という「境界型防御」に代わる新しいセキュリティアプローチ。 ネットワーク内外のすべてのアクセスを信頼せず、常に検証することが基本となる。 特にクラウドサービスやテレワークの普及により、従来のセキュリティ方法では不十分とされ、ゼロトラストが注目されている。 Microsoft Entra IDでは、条件付きアクセスを使用して、ゼロトラストの概念を実現し、アクセスを動的に制御する。
10	リスクベース認証	サインインを行う際の情報を分析し、異常やリスクを検出する仕組み。リスクがあると判定された場合は、追加で認証情報（SMS コードや生体認証 など）を要求する。例えば、通常と異なる位置情報・時間帯・デバイスからのアクセスや匿名 IP アドレスの使用、漏洩した資格情報をもってのサインインなどがリスクが高いと判断する。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
11	アクティブ化	ユーザーに一時的に特権ロールを付与するために、事前に設定したアクションを実行するプロセス。多要素認証 (MFA) 要求、アクセス権利用の理由記載要求など。
12	2段階認証	ユーザー認証のセキュリティを強化するための方法。パスワードに加えて、追加の認証手段（例：SMSコード、認証アプリ）を使用する。
13	アクセス パッケージ	ユーザーが業務を行う上で必要なリソースと、そのリソースへのアクセス権を一括管理・提供するための機能。設定可能なリソースにはグループとチーム、アプリケーション、SharePoint サイト、Microsoft Entra ロールがある。 IT 管理部門の担当者はアクセス管理が必要なリソースに対しアクセスパッケージを作成、利用者は該当するアクセスパッケージに対し利用申請を行う。 なお、エンタイトルメント管理に属する機能のため、Microsoft Entra ID P2 ライセンスが必要。
14	VPN	公共のインターネットを通じてプライベートネットワークを拡張する技術。データを暗号化して安全な通信を提供し、リモートアクセスやプライバシー保護に利用される。
15	セキュアWebゲートウェイ（SWG）	インターネットアクセスを保護するためのソリューション。Webトラフィックをフィルタリングし、悪意のあるサイトやコンテンツへのアクセスを防ぐことで、企業のセキュリティを強化する。

1.2. 資料の構成と目的

■ ID とアクセス管理を強化

企業の規模や業界を問わず、セキュリティを確保しながら、従業員や外部ユーザーのアクセスを効率的に管理できることが求められています。

Microsoft Entra ID はシングルサインオン (SSO) や多要素認証 (MFA)、条件付きアクセスなどの高度な機能を提供し、セキュリティと利便性を両立させます。

■資料の構成

本資料では、第2章で Microsoft Entra ID の概要について説明します。

第3章では、Microsoft Entra ID の主要機能について機能概要、利用時のポイントを解説します。

最後に、Microsoft Entra ID 各プランと機能を比較し、組織に最適なプランを選択するための情報を提供します。

■資料の目的

Microsoft Entra ID の導入に際して、Microsoft Entra ID の機能や利用時のポイントをまとめたナレッジを提供し、ライセンス選定や組織の運用設計を支援します。

2. Microsoft Entra ID とは

2.1. Microsoft Entra ID とは

Microsoft Entra ID は Microsoft 社が提供するセキュリティ製品群「Microsoft Entra」の製品の一つで、**ID およびアクセス管理**を担うサービスです。2023年10月より従来の Azure Active Directory (Azure AD) から Microsoft Entra ID へ名称変更されました。

Microsoft Entra ID を通し、多要素認証、条件付きアクセスによる権限管理、第三者による不正アクセスの検知など様々なサービスへの安全なアクセスを実現できます。

Microsoft Entra ID の利用目的

■効率的なユーザー管理
ユーザーやグループの管理を容易にする機能が提供されており、管理者の負担が軽減されます。

■セキュリティの向上
多要素認証、条件付きアクセスといった機能が備えられており、不正アクセスやデータ漏洩のリスクを減らせます。

■クラウドへのスムーズな移行
クラウドサービスとの親和性が高く、導入が簡単です。
また、既存のオンプレミス環境と連携し併用できるため、必要に応じて段階的にクラウド環境への移行も可能です。

■コストの最適化
サーバー購入などの初期費用を抑えられます。また、利用状況に応じた従量課金制でのため、無駄なコストの削減につながります。

Microsoft Entra とは

Microsoft 社が提供するアクセス管理や ID 管理のための包括的な製品群です。製品群には Microsoft Entra ID (ID とアクセスの管理ツール)、Microsoft Entra Private Access (外部から社内リソースに安全にアクセスできる)、Microsoft Entra Permissions Management (クラウド環境のセキュリティを強化する) などユーザーの認証とアクセスのセキュリティ強化をサポートする複数のサービスが含まれています。

2.2. Microsoft Entra ID と Active Directory の違い

Microsoft Entra ID と Active Directory (AD) はどちらも Microsoft 社が提供するユーザー管理サービスで、組織内のユーザーID やパスワードの一元管理、アクセス権限の制御などのディレクトリサービスを提供しています。

しかし、Active Directoryは主にオンプレミス環境での使用が前提とされているのに対し、Microsoft Entra ID はクラウド環境に特化した機能が搭載されています。

Microsoft Entra ID と Active Directory の違いを簡単にまとめると以下のようになります。

	Microsoft Entra ID	Active Directory（AD）
運用環境	**クラウド**	**オンプレミス**
対象とするリソース	クラウドアプリケーションやクラウドリソース	社内のコンピューターやサーバー、ファイルサーバー
認証プロトコル	SAML、WS-Federation、OpenID Connect、OAuth など	Kerberos、LDAP
利用シーン	リモートワークやモバイルデバイスの管理	社内機器の管理

二つは別のサービスですが、Microsoft Entra ID とオンプレミス Active Directory の間でユーザー情報を同期し、効率よく一元管理を行うことが可能です。

2.3. 他製品との比較

Microsoft Entra ID のような、クラウドベースの ID 管理サービスは IDaaS (Identity as a Service) と分類されます。
IDaaS には「シングルサインオン (SSO)」「多要素認証 (MFA)」「アクセス管理」「ID の一元管理」などの機能が搭載されています。様々な IDaaS サービスが提供されており、組織の要件に合わせて製品を選択する必要があります。

■製品を選ぶ基準の例
・組織が使用するサービスやアプリと連携できるか
・グループウェアと連携が簡単か
・ユーザーの認証手段が組織の特性に合っているか
・セキュリティ要件を満たしているか

代表的な IDaaS サービスを比較すると以下のようになります。

項目	Microsoft Entra ID	Okta	HENNGE One	GMOトラストログイン
SSO 機能	高い	非常に高い	高い	高い
MFA 機能	高い	非常に高い	高い	高い
サービス連携の容易性	中程度	非常に高い	中程度	中程度
日本国内企業向け対応	中程度	中程度	非常に高い	非常に高い
Microsoft 製品との連携	非常に高い	中程度	中程度	中程度

3. Microsoft Entra ID の主な機能

3.1. Microsoft Entra ID の主な機能

Microsoft Entra ID で主要とする機能は以下のようなものがあります。各機能についての詳細は次のページから紹介します。

主な機能	機能概要
アプリ統合とシングル サインオン (SSO)	企業が利用するさまざまなクラウドやオンプレミス アプリケーションと Microsoft Entra ID を統合し、ユーザーが一度サインインするだけで複数のサービスやシステムにアクセスできる
パスワードレスと多要素認証 (MFA)	パスワードより安全な認証方法を導入する（生体認証、セキュリティキー、Authenticator など）また、ログイン時に複数の要素（例：パスワード＋スマホ通知）で認証する
条件付きアクセス	指定した条件（ネットワーク、デバイス など）に合わせてユーザーのアクセスを制御する
ID 保護	サインインのリスクや通常とは異なるユーザー行動が特定できたらアクセスを制御する
特権 ID 管理	組織内の特権 ID のアクセスを管理・制御・監視できる
エンドユーザー セルフサービス	エンドユーザーが自分の ID を管理（パスワードの変更やリセット、アカウントの管理 など）できる
統合型の管理センター	ID とアクセスを一元管理するためのポータルを利用できる

3.2. Microsoft Entra ID の主な機能：シングル サインオン (SSO)

シングル サインオン (SSO)とは、ユーザーが 1回のサインインを行えばクラウド・オンプレミスを問わず すべてのサービスに同じ資格情報でアクセスできるようになる仕組みです。

アプリケーションなどサービス側がどのように認証を行うかによって、SSO の方式を選択します。Microsoft Entra ID で利用可能な SSO の方式は以下のような種類があります。

認証方式	仕組み	利用シナリオ
フェデレーション	複数のサービスを利用する際、異なるシステムやサービス間で認証情報を連携する (認証画面を表示しないで利用) 仕組み。 フェデレーション方式では、パスワードではなくチケットと呼ばれる情報をユーザーと IdP (Identity Provider) がやり取りし、認証を行う。	・以下プロトコルを対応しているアプリケーション - SAML - OpenID Connect - WS-Federation
パスワードベース	WEBブラウザーの拡張機能にアプリケーションのログイン情報を事前記録することで、次回以降のログイン時には Microsoft Entra ID が代理でID/PWを送信する。	・アプリケーション側でSAMLがサポートされていない ・ID/PWで認証するアプリケーション
リンクベース	組織の Microsoft 365 ポータル画面からアプリケーションへ移動するリンクを設置する。 Microsoft Entra ID を通したサインイン機能はなし。	・特定の Web リンクを設定しユーザーへアクセスページを案内する ・認証を必要としないアプリケーションのリンクを追加

3.2. Microsoft Entra ID の主な機能：シングル サインオン (SSO)

メリット

■ユーザーの利便性向上
・一度のログインで、複数のアプリケーションやサービスにアクセス可能
・ID/パスワードを複数管理する必要がない

■セキュリティの強化
・アカウントの管理が簡単になり、セキュリティポリシーの適用が統一される

■運用管理の効率化
・管理者側のアカウント管理の作業負担を軽減
・システムへのログインデータを一元管理できる

注意点

■依存リスク
・SSO が障害などにより利用できない場合、関連するすべてのサービスにアクセスできなくなる可能性

■パスワードのセキュリティ確保
・ 1つのアカウントに依存するため、そのアカウントが漏洩した場合は被害が大きくなる可能性
⇒セキュリティポリシーや多要素認証 (MFA)との併用を推奨

フェデレーション方式のプロトコル

SAML (Security Assertion Markup Language)：XMLベースの認証・認可の標準規格で、Webブラウザと IdP (Identity Provider)、SP (サービスプロバイダ) 間で認証情報を交換する。

OpenID Connect：OAuth 2.0を基にした認証プロトコルで、ユーザー ID の確認を行い、JSON 形式で情報を交換する。

WS-Federation：Microsoft 社が提案した Web サービス用のフェデレーションプロトコルで、異なるセキュリティドメイン間でのユーザー認証に使用される。

3.3. Microsoft Entra ID の主な機能：多要素認証 (MFA)

多要素認証 (MFA：Multi-Factor Authentication) とは、サインインを行うユーザーに別の形式の認証を求める仕組みです。
従来の ID/PW のみで認証を行う場合、パスワードの使いまわしや漏洩などによりセキュリティのリスクが高まります。そこで、複数の認証要素を組み合わせて認証を行うことでセキュリティ強化を目指します。

Microsoft Entra ID の多要素認証は以下のうち 2つ以上を組み合わせて利用できます。
・知識情報：パスワード、セキュリティの質問 など
・所持情報：携帯電話、ハードウェア キー など
・生体情報：指紋スキャン、顔面認識 など

メリット

■セキュリティの強化
・複数要素での認証を行うことで、セキュリティ強化

■運用管理の効率化
・条件付きアクセスと組み合わせ設定することで、特定の条件下で多要素認証を要求できる

注意点

■導入時の設定
・ユーザーの認証情報について登録作業が発生するため導入時の工数がかかる

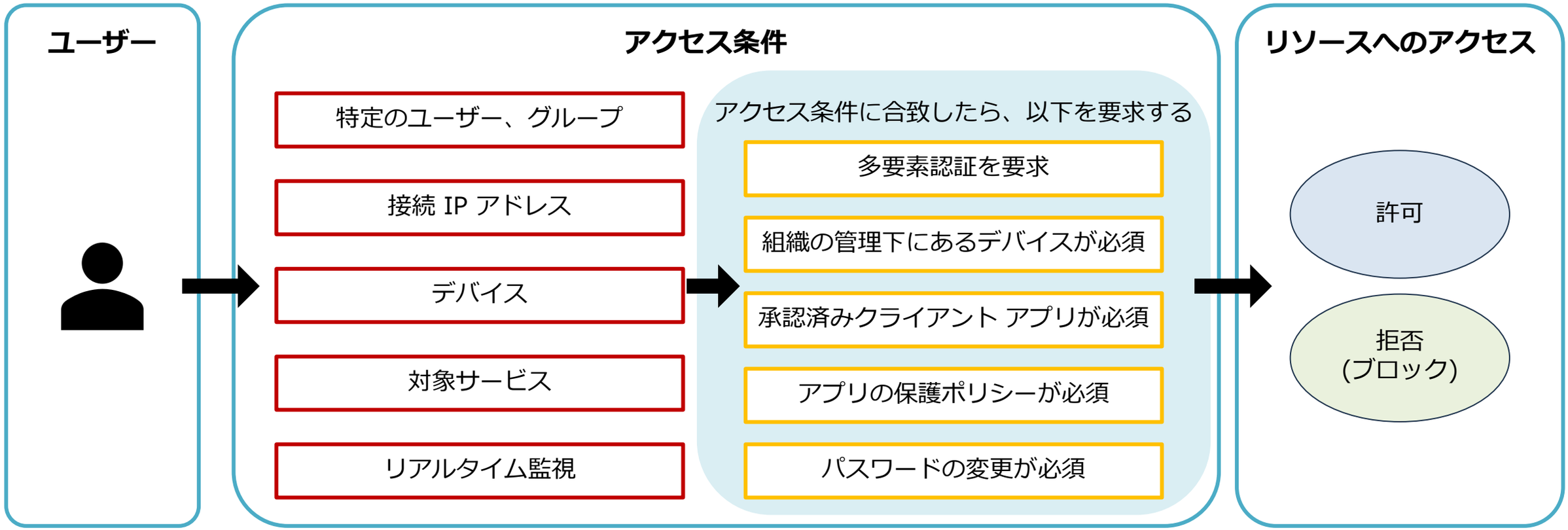
■コストの発生
・認証要素確保のために新しいデバイスやライセンス購入が必要な場合がある

■認証方法の選定
・必要に応じた認証方法を適切に選択する必要がある

3.4. Microsoft Entra ID の主な機能：条件付きアクセス

条件付きのアクセスは、**クラウド上で提供されているサービスへのアクセスを制御**する機能です。**指定した条件に合ったサインインに対してポリシーを適用し、制御を適用**します。一方で、ポリシーの条件に合わないサインインに対しては制御が適用されず、結果としてアクセスが許可されます。

条件付きアクセルの制御イメージ



3.4. Microsoft Entra ID の主な機能：条件付きアクセス

メリット

■セキュリティの強化
・ユーザーのアクセス状況に応じて適切な認証を要求し、不正アクセスを防止できる

■柔軟なアクセス制御
・デバイスの状態や場所に応じたアクセス制限を設定できる

■ゼロトラスト セキュリティの実現
・すべてのアクセスを検証し、信頼できるアクセスのみ許可できる

■コンプライアンス対応
・監査ログを記録し、規制要件を満たすための証拠を確保できる

注意点

■ポリシー設計の複雑さ
・要件によっては設計が複雑になる可能性がある

■ユーザーの利便性とのバランス
・厳格な制御を行うと、ユーザーの利便性が低下する可能性がある

■ライセンス要件
・一部の高度な機能を利用するには、Microsoft Entra ID の P1 または P2 のライセンスが必要

ゼロトラスト セキュリティとは

従来の「社内は安全だが、外部は危険」という「境界型防御」に代わる新しいセキュリティアプローチ。

ネットワーク内外のすべてのアクセスを信頼せず、常に検証することが基本となる。
特にクラウドサービスやテレワークの普及により、従来のセキュリティ方法では不十分とされ、ゼロトラストが注目されている。
Microsoft Entra ID では、条件付きアクセスを使用して、ゼロトラストの概念を実現し、アクセスを動的に制御する。

3.5. Microsoft Entra ID の主な機能：ID 保護

Microsoft Entra の ID保護は、高度な機械学習を通して **ID 侵害のリスクを検出し防止する**セキュリティサービスです。**ユーザー リスク、サインイン リスク**について検出し、追加認証情報を要求する、アクセスを許可・制限するなどを行います。

・ユーザー リスク：ID のセキュリティが侵害されている可能性がある

・サインイン リスク：特定のサインインが ID の所有者自身によって行われたものではない可能性がある

主な機能

リスクの検出

すべてのサインインに対し検出を実行、ログインが侵害された可能性のリスクレベルを示します。このリスクレベルに基づいてポリシーが適用されます。

検出には 2種類があります。
・リアルタイム検出：サインイン時の検出
・オフライン検出：脅威がアカウントにアクセスした方法、正当なユーザーへの影響に関するより多くの分析情報を提供

調査

検出されたリスクについて管理者のためのレポートを作成します。

3つの主要レポートが用意されています。
・リスク検出：検出された各リスクの情報
・危険なサインイン：サインインに対して 1 つ以上のリスクが検出されたとき報告
・危険なユーザー：複数の危険なサインイン、または複数のリスクが検出された場合報告

リスク修復

ユーザーまたはサインインのリスクポリシーに対し条件付きアクセスと組み合わせて、リスクが感知されたサインインについては正常なアクセスである確認を自動で行います。

または、管理者の手動設定によりリスクの確認、管理を行います。

3.5. Microsoft Entra ID の主な機能：ID 保護

メリット

■リスクベースのアクセス制御
・ユーザーのサインイン時にリスクを判定し、自動で適切なポリシー（追加の認証情報要求やアクセス制限など）を適用することで、不正アクセスを防止できる

■リアルタイムでの脅威検出
・機械学習を活用し、不正なアクセスの兆候を迅速に検出する

■管理者向けのレポート提供
・リスクが高いユーザーやサインインに関するレポートを提供し、セキュリティ対策の強化に役立つ

注意点

■ユーザーの利便性とのバランス
・厳格な制御を行うと、ユーザーの利便性が低下する可能性がある

■誤検知への対応
・正規のユーザーのアクセスについてリスクと判定される場合があり、例外処理や管理者による手動調査が必要になる可能性がある

■ログの監視と分析工数
・運用開始後も定期的にログを確認、監視する必要がある

■ライセンス要件
・一部の制限的な機能を除き、Microsoft Entra ID P2 ライセンスが必要

リスクベース認証 とは

サインインを行う際の情報を分析し、異常やリスクを検出する仕組み。リスクがあると判定された場合は、追加で認証情報（SMS コードや生体認証 など）を要求する。例えば、通常と異なる位置情報・時間帯・デバイスからのアクセスや匿名 IP アドレスの使用、漏洩した資格情報をもってのサインインなどがリスクが高いと判断する。

3.6. Microsoft Entra ID の主な機能：特権 ID 管理

特権 ID 管理 (PIM： Privileged Identity Management) は特別なアクセス権限を持つ ID を管理できる機能です。
特権 ID が付与されたユーザーは、組織のセキュリティに関わる幅広い操作が可能になります。そのため、セキュリティ上のリスクを検討し適切に管理する必要があります。

主な機能

アクセス権の割り当て・承認

Microsoft Entra ロール・Azure リソース ロール・グループに対してアクセス権の割り当てを行います。

また、ユーザーからの特権アクセス権の付与申請に対し承認・許可します。

Just-In-Time (JIT) アクセス

ユーザーが 必要な時に、必要な期間だけ特権アクセス権を使用するよう制御します。

アクセス許可の有効期限が切れた後はアクセス権を利用できなくなります。

監査

規定で過去30日間のロール割り当て・権限利用のログを確認できます。

ロールの必要性を確認するためのアクセス レビューや、社内・外部監査のための監査履歴をダウンロードできます。

設定内容の例

- 開始日と終了日を使用した期限付きアクセス権をリソースに割り当てる
- ロールをアクティブ化するために多要素認証を強制する
- なぜユーザーをアクティブ化するのかを把握するために理由を使用する
- 特権ロールがアクティブ化されたときに通知を受け取る

アクティブ化 とは

ユーザーに一時的に特権ロールを付与するために、事前に設定したアクションを実行するプロセス。多要素認証 (MFA) 要求、アクセス権利用の理由記載要求など。

3.6. Microsoft Entra ID の主な機能：特権 ID 管理

メリット

■セキュリティの向上

・特権アカウントの不正使用を防ぎ、セキュリティのリスクを軽減

■特権アクセス権管理の効率化

・JIT アクセスやアクセスレビューにより、管理の手間を削減

■コンプライアンス対応

・規制遵守を支援

・監査に必要なログデータの確保

注意点

■初期セットアップ、運用の複雑さ

・適切な役割やポリシーの設定が必要であり、要件によっては設計が複雑になる可能性がある

・定期的なレビューやポリシーの更新など、運用に伴う負担が増える可能性がある

■ライセンス要件

・Microsoft Entra ID P2 ライセンスが必要

Microsoft が推奨する管理権限アカウントの保護

管理権限に対するリスク（与える**スコープ・時間**）を低減する。また、運用上の工夫を通しリスクを予防・検出する。

・重大な影響がある管理者の数を最小限にする

・管理者用のアカウントを分離する

・アクセス権付与を継続しない

・緊急時に管理アクセス権を取得するためのアカウントを確保する

※Microsoft ドキュメント参照：Azure の管理

3.7. Microsoft Entra ID の主な機能：セルフサービス

セルフサービスとは、エンドユーザーが自分自身のアカウント情報を管理できる機能です。ユーザーはパスワードのリセット、アカウントのロック解除、多要素認証の設定などの操作ができるようになります。

ユーザーはこういった対応をわざわざ IT 管理部門の担当者に問い合わせる必要がなくなるため、素早い問題解決ができ、また IT 管理部門の負担軽減にも繋がります。

主な機能

マイ アプリ

・自分がアクセス権を持っているアプリケーションを確認する
・組織が利用を許可した新しいアプリケーションに対しエンドユーザーがアクセスを申請する
・エンドユーザーをアプリケーションへのアクセス管理者にする
・アプリケーションの個人コレクションを作成する

マイ アカウント

・自分のパスワードをリセットする
・自分のアカウントのロック解除を行う
・接続しているデバイスを管理する
・プロファイル/セキュリティ情報を更新する
・2 段階認証方法を設定する
・認証アプリを設定する

自分のサインイン

・自分のアカウントのサインイン履歴を確認する

マイ アクセス

・アクセス パッケージを要求する
・自分のアクセス パッケージを管理する

3.7. Microsoft Entra ID の主な機能：セルフサービス

メリット

■業務の効率化

・ユーザー自身で自分のアカウントを管理できることで、IT 管理部門の負担を軽減

・アカウント管理の課題について自己解決ができ、ユーザーのエクスペリエンス向上につながる

■コスト削減

・IT 管理部門の問い合わせ対応回数が減り、運用コストの削減につながる

注意点

■ユーザー教育が必要

・セルフサービス機能を適切に活用するためのトレーニングが求められる

■誤操作によるトラブル

・ユーザーが誤った設定変更をしてしまうリスク

■特定のアクセス要求の承認プロセスが必要

・セキュリティを安全に維持するために、管理者による承認が必要な場合がある

アクセス パッケージ とは

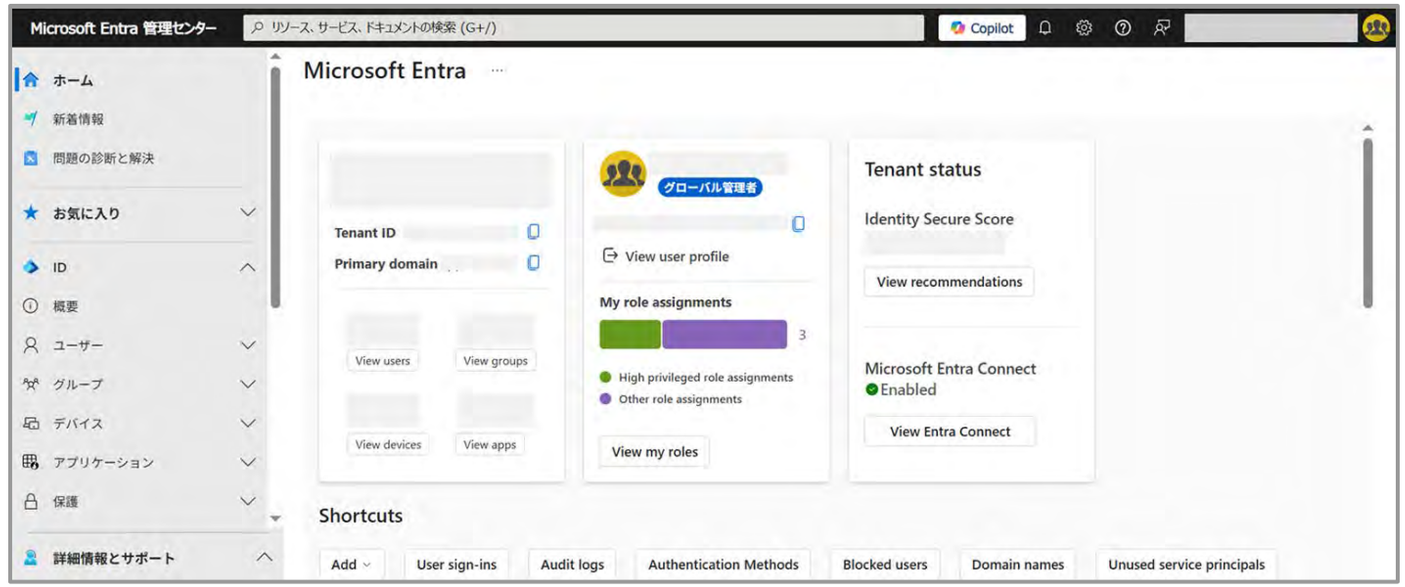
ユーザーが業務を行う上で必要なリソースと、そのリソースへのアクセス権を一括管理・提供するための機能。設定可能なリソースにはグループとチーム、アプリケーション、SharePoint サイト、Microsoft Entra ロールがある。
IT 管理部門の担当者はアクセス管理が必要なリソースに対しアクセスパッケージを作成、利用者は該当するアクセスパッケージに対し利用申請を行う。
なお、エンタイトルメント管理に属する機能のため、Microsoft Entra ID P2 ライセンスが必要。

3.8. Microsoft Entra ID の主な機能：統合型の管理センター

Microsoft Entra ID を含む、「Microsoft Entra」製品群の機能を管理できる Web ベースのインタフェースが用意されており、それが **Microsoft Entra 管理センター** です。組織の管理責任者、または特権ロールを持つユーザーは Microsoft Entra 管理センターにて、組織のユーザー、デバイス、アプリケーション、各種サービスの管理を行います。

Microsoft Entra 管理センターで利用できる機能

- テナント、ユーザー、グループ、デバイス、アプリケーション、ロール、ライセンスなどの ID 管理
- 条件付きアクセス、多要素認証、パスワードのリセットなどを含む ID 保護
- エンタイトルメント管理、アクセス レビュー、ライフサイクル ワークフローなどを含む ID ガバナンス
- 環境全体のユーザー ID、アクション、リソースなどを含む権限管理
- その他 新機能のリリース など



4. Microsoft Entra ID プラン比較

4.1. Microsoft Entra ID プラン比較

Microsoft Entra IDの各プランには、一般的なID管理とセキュリティ機能（SSO、多要素認証、条件付きアクセスなど）が備わっています。
上記に加えた他機能については、プランによって利用できる機能が異なります。
本章では、Microsoft Entra IDのプランについて比較します。

機能/Microsoft Entra ID プラン	Microsoft Entra ID Free	Microsoft Entra ID P1	Microsoft Entra ID P2
アプリ統合とシングル サインオン (SSO)	△ ※1	○	○
パスワードレスと多要素認証 (MFA)	△	○	○
条件付きアクセス	×	○	○
ID 保護	△	△	○
特権 ID 管理	×	×	○
エンドユーザー セルフサービス	△	△	○
統合型の管理センター	△	○	○

最新情報は Microsoft公式ページをご確認ください。

※1 △は一部対応の表記です。フル機能を利用したい場合、基本的にプラン全体のアップグレードが必要となります。

4.2. Microsoft Entra の各プランを含むMicrosoft 365 ライセンス比較

Microsoft Entra ID の各プランは、Microsoft 365 のライセンスに組み込まれており、ライセンスごとにその内容は異なります。
Entra ID Free の機能は全てのライセンスに含まれますが、Entra ID P1/P2 の機能が含まれるのは Business Premium からとなります。
Microsoft Entra ID のプランがそれぞれどの Microsoft 365 ライセンスに含まれるかを比較します。

Microsoft 365 ライセンス/ Microsoft Entra ID プラン	Microsoft Entra ID P1	Microsoft Entra ID P2	Microsoft Entra Suite ※1
Business Basic	×	×	×
Business Standard	×	×	×
Business Premium	○	×	×
Microsoft 365 E3	○	×	×
Microsoft 365 E5	○	○	×

最新情報は Microsoft公式ページをご確認ください。
Entra ID の各プランは、アドオンとして追加購入が可能です。　参考情報

※1 Entra ID P1/P2 をベースに、ID ガバナンス、Verified ID、Private/Internet Access などの追加機能を含むプランです。
Entra Suite はどの Microsoft 365 プランにも含まれておらず、別途アドオンとして購入する必要があります。利用には、Entra ID P1 もしくは P2 のライセンスが必要であり、P2 およびMicrosoft 365 E5 を利用している場合は特別価格を利用できます。　参考情報

4.3. Microsoft Entra ID Free で利用できる機能

Microsoft Entra ID Free ライセンスでは、利用できる機能が一部に限定されています。Free ライセンスで提供される主な機能とその制限について以下に一部抜粋しました。これらの機能を利用要件に含む場合は Microsoft Entra ID P1以上のライセンス導入を検討する必要があります。

Free ライセンスで利用できる機能

■一部のシングルサインオン (SSO) 機能

・ユーザー単位での SSO 設定およびアプリへのアクセス許可設定

・事前に提供されている一部エンタープライズ アプリケーションへの SSO 設定

■制限された多要素認証

・管理者とユーザーに MFA を自動適用

※Microsoft が推奨する最低限のセキュリティ既定 (Security Defaults) を利用

※アプリやユーザーを指定しない一括設定のみ可能

・モバイル認証アプリ (Microsoft Authenticator) を利用した MFA が可能

■基本的なセキュリティポリシー

・条件付きアクセス機能は提供されない

・脆弱なパスワードをユーザーが設定できないよう自動制御

※クラウド専用ユーザーに対してのみ可能

P1 ライセンス以上で提供される機能

■要件に合わせた幅広いシングルサインオン (SSO) 機能

・グループ単位での SSO 設定およびアプリへのアクセス許可設定

・組織が必要とする独自のクラウド・オンプレミスアプリケーションに対し SSO 設定可能

■多様なパスワードレス認証に対応

・条件付きアクセスと組み合わせた MFA 利用可能

・複数のパスワードレス認証（Windows Hello、FIDO2キー、Microsoft Authenticator など）に対応

・オンプレミス アプリケーション用の MFA 提供

■条件付きアクセスの設定

・デバイス、場所、リスクレベルに応じ、条件付きアクセスポリシーを設定可能

4.4. Microsoft Entra ID P2 ライセンスで使える機能

Microsoft Entra ID P2 ライセンスは、Entra ID P1 ライセンスの機能に加え、より高度なセキュリティ機能を提供しています。P1 ライセンスでは提供されていない機能を以下に一部抜粋しました。以下の機能が利用要件に含まれている場合は Microsoft Entra ID P2 ライセンスの利用を検討する必要があります。

ID 保護

※p.18~19 参照

■機能概要

組織の ID に対し、リスクベースで検出・調査・修復を行う

■P2 ライセンスで使える機能

リスクポリシーの設定、セキュリティレポートの作成・確認、リスク発生時のアラートなど

活用シナリオ

・特定ユーザー ID がいつものログインとは異なる国からアクセスした場合、パスワードリセットを要求する

・短時間で発生した複数回のログイン失敗を検知し、多要素認証を要求する

・脆弱なアカウントを感知しセキュリティ担当者に通知する

特権 ID 管理

※p.20~21 参照

■機能概要

組織内の特権アクセスを効率的に管理、制御、監視する

■P2 ライセンスで使える機能

すべての機能。

アクセス権の割り当て、承認、Just-In-Time (JIT) アクセスの制御など

活用シナリオ

・IT 管理者が特定の作業を実施する際、一時的に必要な管理者権限を取得する。また、作業後は付与していた権限を自動で解除する

・緊急対応時にのみ管理者権限を付与し、通常時は制限する

・重要なリソースへのアクセスとアクションを監査する

4.4. Microsoft Entra ID P2 ライセンスで使える機能

アクセス レビュー

※高度な機能は Microsoft Entra Suite 必要

■機能概要

組織がユーザーのアクセス権を定期的に確認し、適切なユーザーのみが継続的なアクセス権を持つように管理する

■P2 ライセンスで使える機能

アクセスレビューの自動化、ゲストユーザーのアクセス権管理、アクセスの自動適用など

活用シナリオ

・特定アクセス権を付与されたユーザーが実際その権限を利用しているか、権限棚卸しを実施する

・重要なアプリケーションやデータへのアクセスを自動で定期的にレビューし、レビュー結果を権限管理者へレポートする

・テナント内のゲストユーザーの利用状況を定期的に確認する

エンタイトルメント管理

※高度な機能は Microsoft Entra Suite 必要

■機能概要

組織内のリソース（グループ、アプリケーション、Share Point Online サイト、Microsoft Entra ロール）へのユーザーアクセスを自動化を通して効率的に管理する

■P2 ライセンスで使える機能

条件付きアクセスポリシーに基づいてアクセス権の付与および削除、アクセス パッケージの管理、ゲストユーザーのアクセス権管理など

活用シナリオ

・プロジェクトに参加する組織外のユーザーに、プロジェクト上で必要な各種リソースへのアクセス権限を一括で付与・削除する

・一般社員、情シス担当者など業務に必要な各種リソースへのアクセス権限をまとめたカタログを用意し管理する

・ユーザー自ら必要な権限を把握し一括でアクセス権申請を行う

・期間などの条件に合わせて自動的に付与された権限を剥奪する

4.5. Microsoft Entra Suite について

Microsoft Entra Suite は、ID 管理やアクセス制御など以下5つの製品を組み合わせた統合ソリューションのライセンスで、
従業員がクラウドや社内リソースにどこからでも安全にアクセスできるようにします。

主な機能	機能概要
Microsoft Entra Private Access	**従来のVPNを置き換える、ゼロトラストネットワークアクセス (ZTNA) ソリューション**で、ユーザーがどこからでも安全にプライベートリソースやアプリケーションにアクセスできるようにする。条件付きアクセスポリシーを使用して、アクセス制御を強化し、セキュリティを向上させる。
Microsoft Entra Internet Access	**ID中心のクラウド型セキュアWebゲートウェイ（SWG）**ソリューション。 Webコンテンツフィルタリング等により、悪意のあるインターネットトラフィックやその他のサイバー脅威から保護し、インターネットリソースやSaaSアプリケーションに安全にアクセスすることが可能。
Microsoft Entra ID Governance	**適切なユーザーが適切なリソースに適切なアクセス権を持つことを自動的に確認**するためのソリューション。ID ライフサイクルの自動化、リソースのアクセス権限の自動割り当て等を通じて、セキュリティを強化し、コンプライアンスを維持する。
Microsoft Entra ID Protection	高度な機械学習を通して ID 侵害のリスクを検出し防止するセキュリティサービス。 詳細は「3.5. Microsoft Entra ID の主な機能：ID 保護」に記載
Microsoft Entra Verified ID	ユーザーのデジタルIDを安全に検証し、リアルタイムの自撮りと写真を照合することで高保証の本人確認を行う**顔チェックや、**運転免許証や社員証などの**デジタル資格情報の発行・検証を行う**ソリューション。

利用条件

Microsoft Entra Suite は、どの Microsoft 365 プランにも含まれていないため、追加で購入する必要があります。
Microsoft Entra ID P1 または P2、もしくはこれらを含む Microsoft 365 プラン（Business Premium 以上）が必要です。

4.6. プラン選択のポイント

前述したように、Microsoft Entra ID のプランによって利用できる機能に違いがあります。
これらの違いを理解し、ビジネスの規模やニーズに応じて最適なプランを選択することが重要です。

小規模・個人向けプラン

Microsoft Entra ID Free：Microsoft 365 や Azure などサブスクリプションを利用しており、基本的な ID 管理機能のみ利用する場合

中規模向けプラン

Microsoft Entra ID P1：300ユーザー以下の組織で、条件付きアクセスや多要素認証を導入したセキュリティ管理が必要な場合に最適

大規模向けプラン

Microsoft Entra ID P2：大規模な組織向けで、特権 ID 管理やリスクベース認証などの高度なセキュリティ機能が必要な場合に最適

Microsoft 365 導入済みの場合

Microsoft 365 Suite :

大規模な組織向けで、外部パートナーとの協力が多い企業や 複雑な組織構成で多くのユーザーのアクセス管理をする必要がある場合に最適