【Microsoft Entra Suite】Global Secure Accessのサービス概要

2026年1月30日

改訂履歴

版数	発行日	改訂内容
第1版	2026年1月30日	初版発行
第2版	2026年2月27日	[3.5. Microsoft サービス向けのEntra Internet Access]の章に 「ユニバーサル テナント制限」の説明を追加

本資料の内容は 2026/2/27 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ご了承ください。

Agenda

1. 前提情報
    1. 用語集
2. Microsoft Entra SuiteとGlobal Secure Access
    1. Microsoft Entra Suiteとは
    2. Global Secure Accessとは
    3. Global Secure Access の仕組み
3. Entra Internet Accessの機能概要
    1. Entra Internet Accessとは
    2. 特徴① 条件付きアクセスとの統合による高度なアクセス制御
    3. 特徴② Web コンテンツフィルタリング
    4. 特徴③ トランスポート層セキュリティ（TLS）検査
    5. Microsoft サービス向けのEntra Internet Access
    6. 導入メリットと注意点
    7. ユースケース：インターネット利用の安全性向上
4. Entra Private Accessの機能概要
    1. Entra Private Accessとは
    2. 特徴① プライベート ネットワーク コネクタ
    3. 特徴② クイックアクセスアプリ
    4. 特徴③ グローバル セキュア アクセス アプリ
    5. 導入メリットと注意点
    6. ユースケース：プライベートアプリ・社内リソースへのアクセス
5. ライセンス要件

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	条件付きアクセス	ユーザーやデバイスの状態に応じてアクセス可否を自動判定する仕組み。ゼロトラストの基盤となる制御方法。
2	Secure Web Gateway（SWG）	インターネットへの接続を検査・制御するクラウド型ゲートウェイ。悪意ある通信や不正サイトへのアクセスを遮断する。
3	VPN	暗号化トンネルを用いて遠隔地から内部ネットワークへ安全に接続する技術。
4	BYOD（Bring Your Own Device）	従業員が個人所有のデバイス（スマートフォン、PC、タブレット）を業務利用する運用モデル。
5	Security Service Edge（SSE）	SWGやZTNA などを統合したクラウドベースのセキュリティサービス群。ユーザーの場所に依存しない一貫した保護を提供する。
6	エッジロケーション	ユーザーに近い場所に配置された分散拠点。遅延を減らし高速なクラウド接続を実現する。
7	WAN	地理的に離れた拠点間を接続する広域ネットワーク。企業ネットワークの基盤として利用される。
8	Entra 参加 / ハイブリッド参加	デバイスをクラウド（Entra ID）またはオンプレミスとクラウドの両方に登録する方式。 クラウド管理や条件付きアクセスをデバイス単位で適用可能にする。
9	FQDN（完全修飾ドメイン）	インターネット上でホストを一意に識別する完全なドメイン名。DNS 解決に必須となる表記。
10	IPSecトンネル	IPレイヤーで通信データを暗号化・認証するプロトコル群。トンネルモードとトランスポートモードを持ち、安全なネットワーク接続を構成する基盤技術。
11	トランスポート層セキュリティ（TLS）	通信の暗号化とサーバー認証を提供するプロトコル。HTTPS の基盤としてインターネット通信を保護する。
12	Web トラフィック	WebブラウザなどでHTTP/HTTPS通信のデータ。ほとんどがTCP 80/443で送受信される。

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
13	TCP 80/443	ポート80はHTTP、443はHTTPSで使用される標準通信ポート。インターネットアクセスの大半を占める基本ポート。
14	Zero Trust Network Access（ZTNA）	信頼を前提とせず、ユーザーとデバイスを検証して必要最小限のアプリへ安全にアクセスさせる仕組み。VPN を置き換えるゼロトラスト型リモートアクセス。
15	IoT 機器	ネットワークに接続される家電やセンサーなどの物理デバイス群。多様で管理が難しく、セキュリティリスクになりやすい。
16	HTTPS	TLS により通信内容を暗号化する HTTP の拡張版。Web 上での安全なデータ送受信の標準方式。
17	ローカルブレイクアウト	拠点や端末からインターネットへ直接アクセスさせる方式。遅延や帯域の負荷を減らしクラウド利用を高速化する。
18	ワイルドカード	任意の文字列を一括指定するための特殊記号。証明書やFQDNの指定で複数ドメインをまとめて扱う際に用いられる。
19	SNI（Server Name Indication）	TLS ハンドシェイクで接続先ホスト名を示す拡張機能。複数ドメインの証明書を同一IPで扱う際に必要になる。
20	データ損失防止	機密情報の漏洩や不正持ち出しを防ぐ仕組み。ファイル内容や通信を検査し、リスクある操作を自動的に制御する。
21	プロキシサーバー	クライアントとインターネットの中継役として動作するサーバー。アクセス制御、キャッシュ、ログ取得などを行う。
22	横移動リスク	侵害された端末から他のシステムへ攻撃が広がるリスク。ネットワーク内の過剰な信頼や許可が原因となる。
23	帯域幅	ネットワークが一定時間に転送できるデータ量の上限。通信速度の指標となり、混雑時の性能に影響する。
24	アウトバウンド接続	内部ネットワークから外部（インターネットなど）への通信。SWG やファイアウォールで最も制御対象となる。

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
25	ポート	通信サービスを識別するための番号。TCP/UDPで定義され、アプリケーションごとに異なる。
26	RDP・SSH・SMB	RDP はリモートデスクトップ接続、SSH は暗号化されたリモートシェル、SMB はファイル共有に用いられる通信プロトコル。いずれも攻撃対象になりやすく、保護が重要となる。
27	UDP	コネクションレスで軽量な転送を行うプロトコル。リアルタイム通信に向くが信頼制御を持たない。
28	インバウンド	外部から内部ネットワークへ向かう通信。ファイアウォールで最も厳しく制御される。
29	ステートレス	通信状態を保持せず、各パケットを個別に処理する方式。高速だがセッション管理には不向き。
30	Entra Application Proxy	アプリケーションへの接続を中継し、認証やアクセス制御を挟むためのプロキシ。オンプレアプリを安全に外部公開する用途で利用される。アクセス管理・認証は Microsoft Entra IDに統合される。
31	プロトコル	通信の形式や手順を定めた規約。ネットワーク機器やアプリケーションが相互にデータ交換するための共通ルール。
32	Microsoft Entra ID	Microsoft が提供するクラウドベースの認証・アクセス管理サービス。 組織のユーザーアカウントを一元的に管理し、アプリケーションやデバイスへのアクセスを安全に制御するための仕組み。
33	Entra管理センター	Microsoft Entra の ID・アクセス管理を行うための管理ポータル。ユーザー、グループ、アプリ、条件付きアクセス、認証方法、デバイスなどの設定を一元管理するための Web 管理インターフェイス。
34	トラフィックログ	ネットワーク通信の詳細を記録するログ。ユーザーやデバイスがどの宛先へどの通信を行い、結果がどうであったかを可視化・分析するためのログ。
35	ゼロトラスト	すべてのアクセスを信頼せず、常に検証することを前提とするセキュリティモデル。ネットワーク境界に依存しない保護を目指す。「明示的検証」「最小権限」「侵害前提」の3原則を基本とする。

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
36	明示的検証	ユーザー・デバイス・アプリ・ネットワークなど、利用状況すべてを基に毎回アクセスを検証する。推測による信頼を行わない。
37	侵害前提	侵害が起きている前提で設計し、横展開を防ぐ仕組みを常に組み込む。ログ監視、セグメント化、迅速な検出・対応を重視。
38	MFA（多要素認証）	パスワードに加え、デバイス、認証アプリ、電話、指紋など複数の要素を組み合わせて本人確認を行う仕組み。
39	マルウェア検査	デバイスやファイル、ネットワーク通信を解析し、ウイルス、ランサムウェアなどの悪意あるソフトウェアを検出する仕組み。
40	フィッシング	偽のメールや Web サイトを使って、ユーザーにパスワード、クレジットカード情報、認証コードなどを入力させて盗み取る攻撃手法。
41	脆弱性	ソフトウェア、OS、ネットワーク、設定などに存在するセキュリティ上の欠陥。
42	パッチ適用	脆弱性や不具合を修正するために提供される更新プログラム（パッチ）をシステムに適用する作業。
43	レガシーアプリ	古い技術や旧バージョンのフレームワーク・OS に依存し、最新のセキュリティ要件やクラウド環境に適合しないアプリケーション。
44	CPE機器	拠点側に設置されるルーターやファイアウォールなど、サービス提供側ネットワークとの接続点となるネットワーク装置。 拠点から GSA へ向けた IPSec トンネルの終端として機能し、トラフィックを外部へ中継する役割を持つ。
45	IKEv2	IPsec トンネルを張るときの認証と暗号化の仕組みを担うプロトコル。
46	BGP	拠点と GSA 間で経路情報を交換し、動的ルーティングを実現するために使用されるインターネット標準のルーティングプロトコル。
47	バイパス	特定の通信や処理を本来通過すべきセキュリティ機能や経路を経由させずに直接アクセスさせる動作。

2. Microsoft Entra Suiteと Global Secure Access

2.1. Microsoft Entra Suiteとは

Microsoft Entra Suiteとは、「Microsoft Entra ID」の認証・SSO・条件付きアクセスを基盤として、ID管理とアクセス制御を強化するクラウドサービス群（アドオン製品）です。
従業員が社内外問わず、安全にクラウドやオンプレミスのアプリへアクセスできるよう、ネットワークアクセス・ID保護・本人確認・ガバナンスを組み合わせた統合的な仕組みを提供します。

Entra Suite の構成要素

Entra Suiteは5つの製品群で構成されます。本資料では、「ネットワークアクセス保護」の製品について紹介します。

カテゴリ	製品名	説明
ネットワークアクセス保護	**Entra Internet Access**	**インターネットや SaaS アプリへの通信を保護する**Secure Web Gateway（SWG）です。 危険なサイトや不審な通信を遮断し、安全にインターネットを利用できる環境を提供します。
	Entra Private Access	**VPN を使わずに、社内アプリや内部リソースへ安全に接続できる**Zero Trust Network Access（ZTNA）です。ユーザーのID情報を基にアクセス権限を制御します。
ID保護と認証	**Entra ID Protection**	**サインインリスクや異常なアクティビティを自動で検出し、不正アクセスをリアルタイムにブロックする** ID セキュリティ機能です。
	Entra Verified ID	**信頼できるデジタル身分証明書を発行・検証できる**サービスです。 本人確認や入社時のリモートオンボーディングなどを、安全かつ簡易に実現します。
IDガバナンス	**Entra ID Governance**	**ユーザーのアクセス権を入社・異動・退職といったライフサイクルに沿って自動管理できる**サービスです。権限の付与・削除やアクセスレビューを効率化し、コンプライアンスを強化できます。

2.2. Global Secure Accessとは

Global Secure Access（以降、GSA） とは、Microsoft Entra が提供する **Security Service Edge（SSE）ソリューション**で、
前項で説明した、以下2つのサービスを統合したネットワークセキュリティ機能です。

- **Microsoft Entra Internet Access**
- **Microsoft Entra Private Access**

インターネットやSaaS、社内アプリへの通信を保護し、悪意あるアクセスや不審な通信をブロックすることで安全な接続を実現します。
さらに、ユーザーやデバイスの状態に応じて必要なアプリだけに最小権限でアクセスできるゼロトラスト制御を提供します。

GSAが必要とされる背景

■働き方の変化
リモートワークが一般化し、従来の「社内ネットワーク中心のセキュリティ対策」では安全を保てなくなったため。

■従来型 VPN の構造的なリスク
VPNは一度接続するとネットワーク全体へ広い権限が与えられるため、侵害時に横移動を許す危険がある。

■ゼロトラストへの移行が必須に
ゼロトラストの「明示的検証」「最小権限」「侵害前提」を満たすために、ID起点のアクセス制御が必要になった。

■SaaS/インターネット利用急増による新たな脅威
Web・SaaSアクセスが増え、インターネット経由の脅威対策がこれまで以上に重要となった。

2.2. Global Secure Accessとは

特徴と役割

ゼロトラストに基づく アクセス制御

ID・デバイス状態・リスクなどを評価し、「誰が・どの状態でアクセスするか」を軸に安全な接続を実現。

インターネットと 社内リソースの双方を保護

Internet Access：SaaS・Webへの安全なアクセスを提供。
Private Access：VPN なしで社内・プライベートリソースに安全に接続。

Microsoft のグローバル ネットワークを活用

世界 70 地域・190 以上のエッジロケーションを持つ Microsoft のグローバル WAN を活用し、安定した高速通信と安全なアクセス経路を提供。

統合ログ・可視化・ ポリシー管理の統合

通信ログ、条件付きアクセス、Web フィルタリングなどを一つの管理基盤（Entra管理センター）で統合的に可視化・運用可能。

主要要素

GSA は複数の主要要素が連携して安全なアクセスを実現します。まず各要素の役割を整理し、次のスライドで全体の動作の流れを説明します。

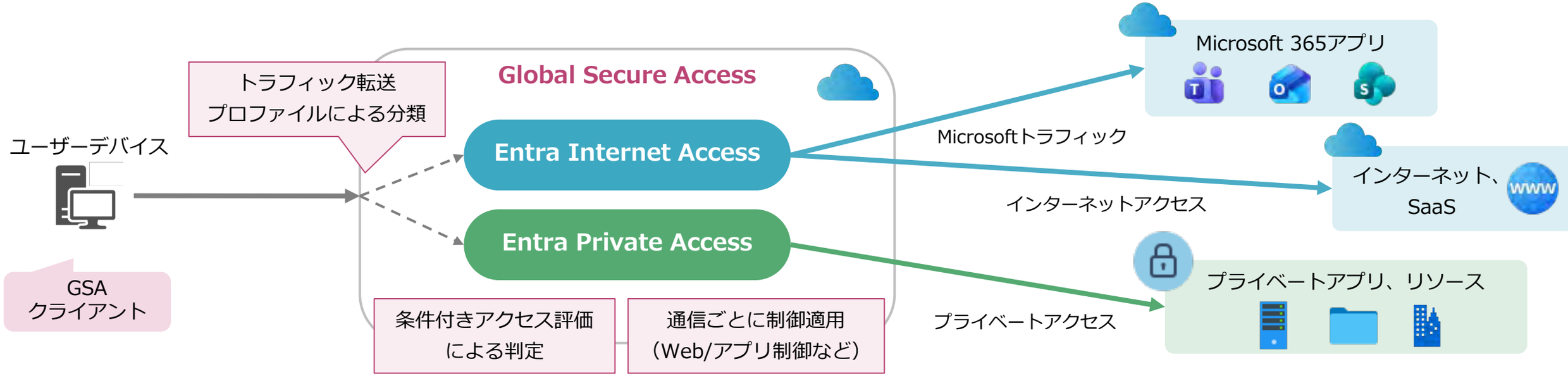
主要要素	説明
GSA クライアント（Global Secure Access Client）	ユーザーデバイス上で動作し、対象となる通信をデバイスから取得するエージェント。 取得したトラフィックを GSA へ転送する役割を担う。
トラフィック転送プロファイル	ユーザーデバイス上で取得した通信を、どの種類のトラフィックとして GSA に送るかを定義する設定。
条件付きアクセス評価	通信ごとに実行されるセキュリティチェック。ユーザー/デバイス/リスク状態に加え、GSA 経由かどうか（ネットワーク準拠）などを確認し、アクセス可否や適用する制御を判断する。

2.3. Global Secure Access の仕組み

Global Secure Access の仕組み

本図は、Global Secure Accessにおけるネットワーク全体の動作イメージを示したものです。

1. GSA クライアントがユーザーデバイスの通信を取得し、GSAへ送信する。
2. 通信はトラフィック転送プロファイルに従って、種類ごと（Microsoft、インターネット、プライベート）に分類される。
3. Entra IDによる条件付きアクセスのセキュリティ評価が行われ、通信が許可されるかどうかが判定される。
4. 許可された通信は、トラフィックの種類に応じて Entra Internet Access または Entra Private Access により、制御・処理される。
5. 最終的に、クラウドアプリやインターネット、社内リソースへ安全に接続される。



2.3. Global Secure Access の仕組み

補足：GSA クライアントについて

Global Secure Access の仕組みを支える基盤として、**ユーザーデバイス側で通信を取得・転送する役割を担う**のが「GSA クライアント」です。
このクライアントが端末とGlobal Secure Accessを接続することで、インターネット・Microsoft 365・社内リソースへのアクセスに一貫したセキュリティ評価と制御を適用できるようになります。

GSA クライアントの役割

- ユーザー端末にインストールされ、端末上の対象となるネットワーク通信を捕捉し、Global Secure Access に転送するエージェント
- Entra Internet Access（EIA）/Entra Private Access（EPA）共通で使用されるクライアント
- 転送された通信は、条件付きアクセスや Web 制御の評価を受ける

⇒ **端末とクラウド側のゼロトラスト制御をつなぐ“入り口（エントリーポイント）”として機能**

GSA クライアントの対応環境と導入要件

- 対応デバイス
  - ・Windows 10 / 11（Entra 参加 / ハイブリッド参加済みデバイス）
  - ・AndroidOS
  - ・iOS / macOS（プレビュー段階）
- Windowsクライアントの場合、Entra 参加/ハイブリッド参加が必須のため、BYOD などの“登録済みデバイスのみ”の環境では導入不可。
- インストールは管理者による実行が前提であり、配布方法としては Microsoft Intune による一括配布のほか、手動インストールも可能。
- GSA クライアントはインターネットに接続できることが前提であり、通信が遮断された端末では利用できない。

2.3. Global Secure Access の仕組み

補足：トラフィック転送プロファイルについて

Global Secure Accessの全体像を理解したうえで、実際にユーザーの通信がどのように仕分けられ、適切な経路に送られるのかを把握することが重要になります。このスライドでは、この動作の中心となる “トラフィック転送プロファイル” の仕組みと役割を説明します。

トラフィック転送プロファイルとは

Global Secure Access がどの通信を取得し、どの経路で処理するかを決定するための分類ルールです。
通信はこのプロファイルに基づいて種類ごとに判定され、適切なサービスへ転送されます。
これにより、組織は必要なトラフィックだけを選択的に保護し、ポリシーを一元的に適用できるようになります。

トラフィック転送プロファイルの種類	説明
Microsoft トラフィック プロファイル	Exchange Online、SharePoint、OneDrive、Teams など Microsoft 365 の通信を対象とする。 これらの通信をGSA 経由で転送するか、通常の経路で直接アクセス（バイパス）するかを管理者が設定可能。
プライベート アクセス プロファイル	社内アプリやオンプレミスサーバーなど、プライベートリソースへのアクセスを対象とする。 アクセス先の FQDN / IP などを指定することで、これらの通信を GSA 経由で安全に提供できる。
インターネット アクセス プロファイル	一般的な SaaS やインターネットサイトなど、Microsoft 以外の Web サービスへの通信を対象とする。 TCP 80/443 のWeb通信をデフォルトで取得し、必要に応じて管理者が FQDN/IP で除外設定を追加できる。

▼ トラフィック評価順序

Microsoft トラフィック プロファイル ⇒ プライベート アクセス プロファイル ⇒ インターネット アクセス プロファイル　で評価がされます。
各プロファイル条件に一致しない通信（例：管理者がバイパスとして指定した FQDN/IP など）はGSAに転送されず、従来どおりの経路を通ります。

2.3. Global Secure Access の仕組み

Global Secure Access では、ユーザーデバイスにGSAクライアントをインストールして接続する方式に加えて、拠点や工場などのネットワーク全体を接続する**リモート ネットワーク方式**も利用できます。

リモートネットワーク接続とは

拠点ネットワーク全体を IPSecを使ってGlobal Secure Accessに接続する仕組みです。
これにより、拠点からのすべての通信を自動的にGSAへルーティングでき、クライアント接続と同じゼロトラスト制御を一括適用できます。
IoT 機器や共有 PC、工場端末など、クライアントをインストールできない環境でも拠点単位で安全に保護できる点が大きな特徴です。

リモートネットワーク方式の仕組み

1. 拠点機器とGlobal Secure Access エンドポイント間に IPSec トンネルを確立。
2. 拠点ネットワークからの通信は、IPSecトンネル経由でGlobal Secure Accessに安全に転送。
3. 通信は、Entra Internet Accessのポリシーに基づいて制御・処理される。
4. 最終的に、Microsoft 365アプリやSaaSへ安全に接続される。

※Entra Private Accessはリモートネットワーク方式が非対応のため、GSAクライアントの利用が必須です。

2.3. Global Secure Access の仕組み

リモートネットワーク方式の導入方法

- 対応環境
  IPsec / IKEv2 / BGPのプロトコルに対応したオンプレミスの CPE（拠点ルーター）で接続可能。
- 導入方法
  Entra 管理センターでリモートネットワークを作成し、CPE（拠点ルーター）の情報を登録。
  管理センターで生成された接続情報をもとに、拠点側の CPE に設定を投入し、GSAと拠点間で IPsec トンネルを確立する。

接続方式の比較

GSAの2つの接続方式（クライアント方式／リモートネットワーク方式）の違いをまとめた比較表です。端末単位でのゼロトラスト適用なら
クライアント方式、クライアントが入れられない機器や拠点丸ごとの接続が必要な場合はリモートネットワーク方式が適しています。

観点	GSAクライアント	リモートネットワーク方式
接続方式	デバイスに GSA クライアントを入れて接続	拠点ルーターと GSA 間で IPSec トンネルを構築
用途	・インターネット、Microsoft 365、社内システムへ安全にアクセスするためのユーザーデバイス向け	・GSA クライアントを入れられないデバイス ・拠点丸ごと保護に適用
メリット	・ユーザー・デバイス・アプリ単位でアクセスを細かく制御できる（ゼロトラストの実装がしやすい）	・クライアント不要で非対応デバイスも保護可能
主な制限 / デメリット	・クライアント非対応デバイスは利用不可	・**条件付きアクセス利用不可** ・**Entra Private Accessが非対応** ・拠点単位の制御になるため、デバイス単位のゼロトラスト評価が不可
導入・運用	・デバイスへ GSAクライアントを入れるだけで即利用可能 ・ユーザー追加や端末入替時もシンプル（ネットワーク構築不要）	・導入時に CPE機器設定/IPSecトンネル構築 が必要 ・構成要素が多く、拠点追加や変更時の作業負荷が大きい

3. Entra Internet Accessの機能概要

3.1. Entra Internet Accessとは

Microsoft Entra Internet Access（EIA）は、IDを中心とした**Secure Web Gateway（SWG）**として、**インターネットや SaaS へのアクセスを保護するクラウド型セキュリティサービス**です。Web コンテンツフィルタリングや脅威対策により、ユーザーとデバイスをインターネット上の危険から守り、条件付きアクセスと連携して細かなアクセス制御を実現します。

Entra Internet Access は、以下のような課題を抱える組織に最適なソリューションです。

- ✓ インターネットやSaaS利用のセキュリティをIDベースで強化したい
- ✓ 暗号化通信（HTTPS）も検査して脅威を未然に防ぎたい
- ✓ 業務外サイトや危険サイトへのアクセスを確実に制御したい
- ✓ インターネット通信のログ可視化や監査を強化したい

特徴

■条件付きアクセスとの統合による高度なアクセス制御

条件付きアクセスとネイティブに連携し、ユーザーやデバイスに基づいたネットワーク制御を実現します。
ネットワーク全体の通信に対して、一貫した条件付きアクセスのポリシーを適用できます。

■Web コンテンツフィルタリング

Web カテゴリや特定ドメインに基づきアクセスを許可・ブロックできます。業務上不要・危険なサイトの遮断と、必要サイトの例外許可を柔軟に設定できます。

■トランスポート層セキュリティ（TLS）検査

暗号化通信（HTTPSなど）を一時的に復号・検査し、安全性を確認したうえで再暗号化することで、暗号化トラフィックにも統一されたセキュリティ制御を適用できます。

3.2. 特徴① 条件付きアクセスとの統合による高度なアクセス制御

Entra Internet Accessは条件付きアクセスとの連携により、ネットワーク経由の通信にもゼロトラストに基づく一貫したアクセス制御を適用できます。この**ネットワークレベルの制御を可能にする仕組みが、ユニバーサル条件付きアクセス**です。

ユニバーサル条件付きアクセスとは

Global Secure Access（GSA）経由のネットワーク通信に、条件付きアクセスを直接適用できる仕組みです。
Microsoft 365 やインターネットなどのトラフィックを種類ごとに判定し、ユーザーやデバイスの状態に応じてアクセスを許可・制御できるため、ネットワーク通信を統一的に保護できます。

従来の条件付きアクセス

- クラウドアプリやMicrosoft 365アプリに対して適用
- ネットワーク通信そのもの（インターネット/SaaS）は対象外

ユニバーサル条件付きアクセス

- GSA経由のネットワーク通信にも適用可能
- Microsoftとインターネットアクセスの双方に適用

主なポイント

- **GSA 経由トラフィックの条件付きアクセス判定**
  GSA 経由の通信に条件付きアクセスを適用し、許可された通信のみ通過させる。
- **ユーザー・デバイス条件にもとづくアクセス判断**
  ユーザー属性・デバイス準拠・リスクに基づき、通信を統一基準で制御する。
- **「準拠ネットワーク」条件による不正経路の遮断**
  GSA 経由の通信のみ許可するポリシーが利用可能。
  不正経路（ローカルブレイクアウト等）をブロックする。

適用範囲

対象：Microsoft トラフィック / インターネット アクセス
非対象：プライベート アクセス
（アプリ単位で個別に条件付きアクセスを設定）

適用方式

・GSA クライアント方式のみ適用可能
・リモートネットワーク方式は「拠点単位の接続」のため、ユーザー/デバイス情報が取得できず対象外

3.2. 特徴① 条件付きアクセスとの統合による高度なアクセス制御

条件付きアクセスの評価項目例

ユニバーサル条件付きアクセスでは、通常の条件付きアクセスと同じ評価項目を用いてアクセス制御を行うことができます。

評価項目	説明
ユーザー属性	所属グループ・役割・アカウント状態などに基づき判定（例：管理者のみ許可、特定部門のみ許可 など）
デバイス準拠状態	Intune準拠、OSバージョン、暗号化、ウイルス対策、登録状態（Entra ID 登録/参加）などを評価
準拠ネットワーク（GSA 経由）	通信がGSA経由かどうかを条件として評価
サインインリスク	異常な位置情報・漏洩資格情報・不審な活動などのサインインリスクを判定
場所（ロケーション）	許可されたネットワーク範囲や国/地域などを条件として評価（例：海外からのアクセスを制限 など）
MFA（多要素認証）要求	多要素認証が必要かどうかを評価し、必要に応じて追加認証を要求

制御例

- **通信プロファイルごとの制御**
  Microsoft 365：準拠デバイスのみ許可、非準拠デバイスはブロック。
  インターネット：MFA を必須とし、高リスクユーザーはブロック。
- **ユーザー/デバイス状態にもとづく制御**
  デバイスが非準拠、またはユーザーが高リスクの場合は通信をブロック。

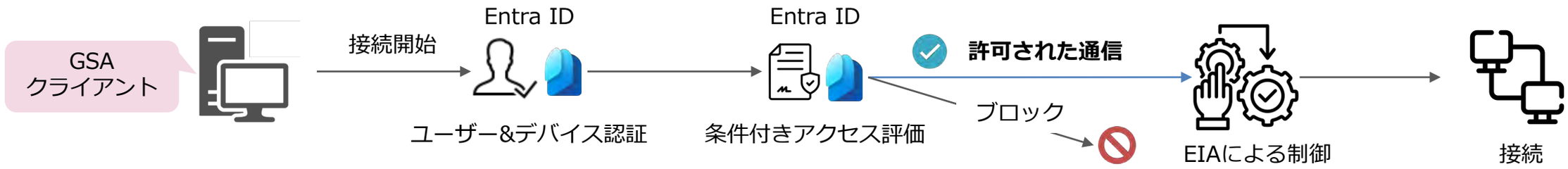
補足：通常の条件付きアクセスについて

条件付きアクセスは、ユーザー・デバイス・場所・リスクなどを評価し、**クラウドアプリへのアクセス可否を制御する** Entra ID の機能です。
EIA はこの判定ロジックを**インターネットアクセスに拡張して利用できる点が特徴**で、ネットワークアクセスに対しても同じ基準で一貫した制御が可能になります。

3.2. 特徴① 条件付きアクセスとの統合による高度なアクセス制御

仕組み

1. 端末にインストールされたGSAクライアントが接続を開始する。
2. **Entra ID**へリダイレクトされ、**ユーザー&デバイス認証**が実行される。
3. 認証後、**ユニバーサル条件付きアクセス評価がネットワーク通信に対して実行**される。
   ユーザー・グループ・デバイス準拠状態・サインインリスク・準拠ネットワーク（GSA経由）・ロケーション・MFA要求など
4. 条件付きアクセスの判定に基づき、**通信（インターネット / Microsoft）が許可 or ブロック**される。
   許可された通信のみが Entra Internet Access（EIA）へ進む。
   ブロック判定の場合は接続できず、インターネットや Microsoft 365 への通信は行えない。
5. EIAでは事前に設定されたネットワーク制御が適用され、Microsoft 365 や SaaS、インターネットへの安全な接続が確保される。



3.3. 特徴② Web コンテンツフィルタリング

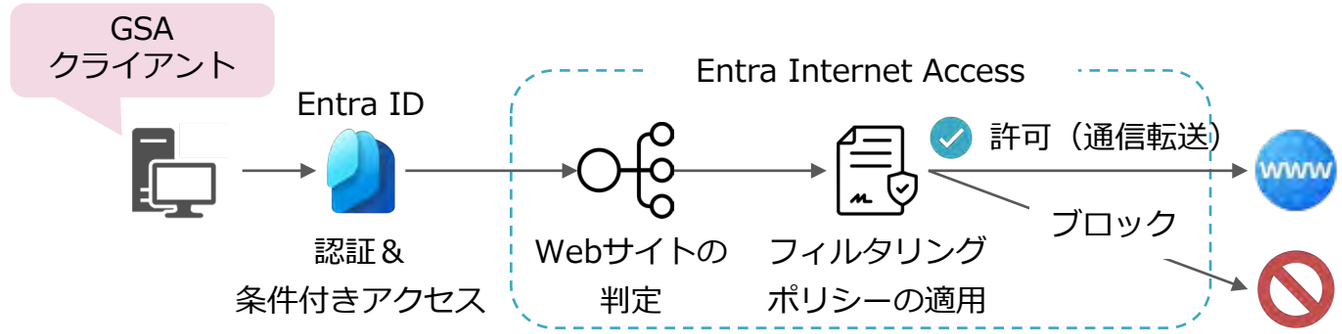
Web コンテンツフィルタリングとは、**インターネット上のサイトをカテゴリやドメイン別に識別し、組織のポリシーに基づいてアクセスを許可・制御する仕組み**です。業務に不要なサイトやリスクの高いサイトへのアクセスを防ぎ、セキュリティを強化しながら生産性を高めます。

主な機能

- **カテゴリ別のサイト制御**
  ギャンブル・SNS・ショッピングなど、サイトのカテゴリに基づいてアクセスを許可/ブロック。
- **FQDN（完全修飾ドメイン）単位での細かい制御**
  ドメイン名（例：example.com）単位でアクセスを許可/ブロック。ワイルドカード（*.example.com）も使用可能。
- **特定 URL の個別制御（※プレビュー機能）**
  完全な URL 単位で制御（例：https://example.com/path/page.html）。
- **Web フィルタリングポリシー**
  サイトカテゴリ・ドメイン・URLなどの制御内容をまとめて管理し、適用ルールを一元的に定義する機能。
- **ID・デバイス状態に応じた動的なアクセス制御**
  条件付きアクセスと連携し、ユーザー条件やデバイスの準拠状況に応じて、適用されるWeb フィルタリングポリシーを切り替え可能。

処理の流れ

1. GSAクライアントがデバイスの通信を取得し、Entra IDで認証される。
2. 条件付きアクセスにより、接続可否と適用するWebフィルタリングポリシーが決まる。
3. GSA クライアントが通信をEIAに転送し、通信種別に応じてアクセス先Webサイトを判定する。
   HTTP通信：URLを参照してサイトを識別
   HTTPS通信：TLSのSNI（Server Name Indication）からドメインを識別
4. 事前に定義したWebフィルタリングポリシーが適用され、Web サイトへのアクセスを許可/ブロックする。



3.4. 特徴③ トランスポート層セキュリティ（TLS）検査

トランスポート層セキュリティ（TLS）検査とは、暗号化された HTTPS 通信を **一時的に復号 → 内容を検査 → 再暗号化** することで、暗号化通信の中に隠れた脅威（マルウェア、情報漏洩、悪意あるアクセス）を検知できる仕組みです。

なぜ必要なのか

- 多くの Web 通信が HTTPS で暗号化されており、攻撃やデータ漏洩も暗号化の中に隠れてしまう
- 暗号化されたままでは、従来のフィルタリングや脅威検知が十分に機能しない

⇒トランスポート層セキュリティ（TLS）検査は、**暗号化による“見えない領域”を安全に可視化するための技術**

主な機能

- **暗号化通信（HTTPS）を一時的に復号して検査できる**
  暗号化の裏に隠れたマルウェア・情報漏洩などの脅威を発見。
- **検査後は再度暗号化して Web サイトへ安全に送信する**
  デバイス⇔GSA、GSA⇔Webサーバーで2本のTLS通信を確立し、通信の安全性を維持。
- **高度なセキュリティ制御（Webコンテンツフィルタリング・マルウェア検査・データ損失防止）が可能になる**

仕組み

1. デバイスはまずGSAに[**TLS 接続①**]を確立する。
2. GSA は受信したHTTPSを一時的に復号し、内容を検査する。
3. Webコンテンツフィルタリングなどのセキュリティ制御を適用する。
4. 検査後、通信を再暗号化し、Webサーバーへ[**TLS 接続②**]で転送する。

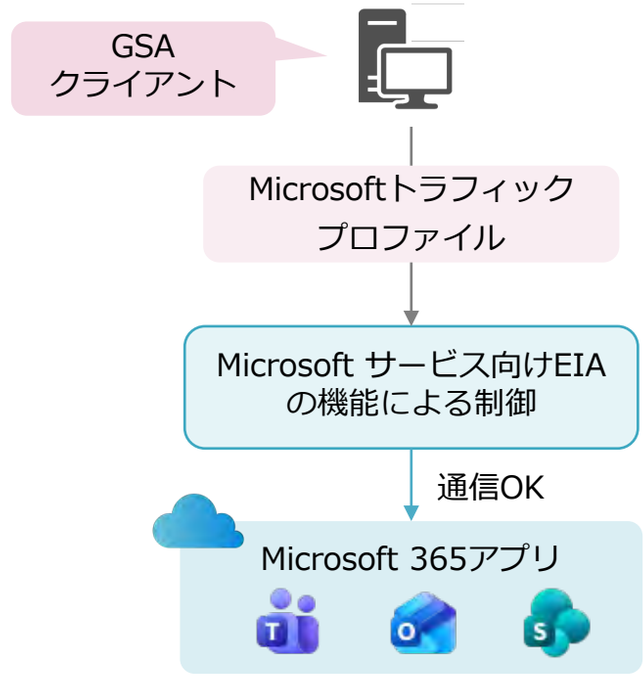
◎2本のTLS接続により、通信区間（端末 ⇔ GSA ⇔ Web サーバー）は常に暗号化され、復号は GSA 内部のみで実施されるため安全性が維持される。
→ 通信は常に暗号化された状態で送受信される。
◎ブロック対象の場合は、通信を停止する。

3.5. Microsoft サービス向けのEntra Internet Access

通常のEIA機能に加え、Microsoftサービス向けのEIAは、**Microsoft サービスへの接続を最適化する専用機能を提供**します。
専用経路による低遅延アクセス、条件付きアクセスとの統合、テナント制限やログ精度の向上など、Microsoft サービス利用時のセキュリティ・パフォーマンス・可視化を強化する仕組みが追加されています。

主な機能

- **Microsoftトラフィックプロファイルによる直接接続**
  - ・デスクトップクライアントやリモート拠点から、Microsoftトラフィックプロファイルを利用し、TeamsやSharePointなどのMicrosoftサービスに最適化経路で直接接続。
- **Entra ID 条件付きアクセスと統合**
  - ・ネットワーク準拠チェックを利用し、Microsoft 365アプリケーションに対するアクセス制御を強化。
- **テナント制限によるデータ保護**（※詳細は次スライドにて説明）
  - ・Microsoft 365 から未許可の外部テナントへの接続を制御し、データ流出を防止する。
- **詳細なネットワーク可視化**
  - ・TeamsやSharePointなどのMicrosoft 365通信について、許可/ブロックの結果を含む詳細ログを取得し、ユーザー・デバイス・テナントの関係性を可視化するダッシュボードを提供。



補足：Microsoft サービス向けEIAと通常EIAの違い

通常のEIAは、**Web 全般のトラフィックを対象にセキュリティ制御**（ユニバーサル条件付きアクセス、Webコンテンツフィルタリングなど）を提供する**“インターネット保護レイヤー”**です。一方、Microsoft サービス向けEIAは、**Microsoft 365やEntra IDへの接続を最適化**し、認証統合やテナント制御など**“Microsoft サービス専用の強化レイヤー”**を提供します。

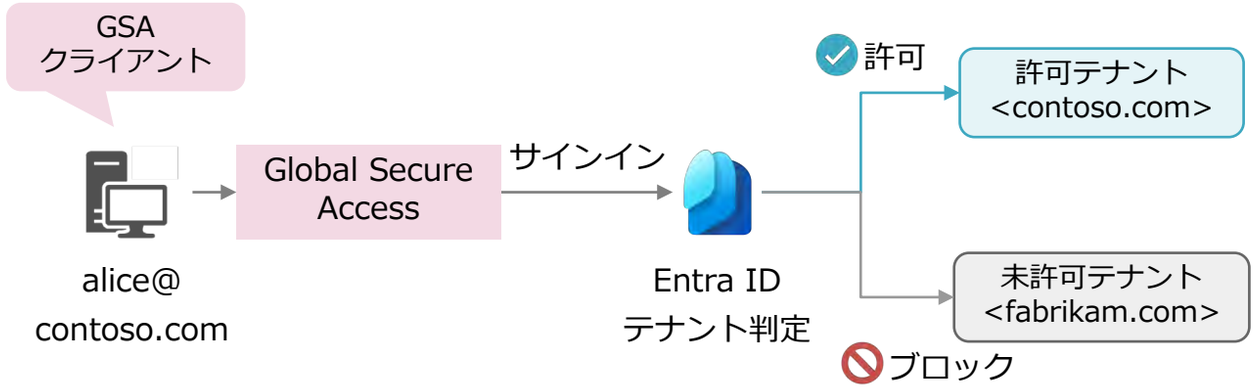
3.5. Microsoft サービス向けのEntra Internet Access

組織が管理するデバイスやネットワークから、サインイン可能な Microsoft テナントを限定することで、意図しない外部テナントへのサインインやデータ流出を防止できます。この テナント単位のアクセス制御をクラウド側で一貫して実現する仕組みが**ユニバーサル テナント制限**です。

ユニバーサル テナント制限の仕組み

GSA は、組織の管理デバイスやネットワークからのMicrosoft サービス通信を制御ポイントとして集約し、Entra ID により許可された Microsoft テナントのみへのサインインを可能にします。

- ユーザーデバイスのMicrosoft サービス向け通信が **GSA を経由**
- GSA経由の通信に対して、**Entra ID がサインイン先テナントを判定**
- 管理者が許可したテナントのみサインインを許可
- **未許可テナントへのサインイン試行をブロック**



ポイント

- ✓ 管理者が許可した Microsoft テナントにのみサインイン可能
- ✓ GSAを経由する通信をクラウド側で一元的に制御することで、利用環境（OS・ブラウザ・接続場所）に依存せず、同一の制御を適用
- ✓ 許可されていない外部テナント経由でのデータ持ち出しを防止

防げる代表的なリスク

- 社給 PC から個人テナント/攻撃者テナントへのサインイン
- 組織管理の PC やネットワークから、個人用・外部組織の Microsoft 365（OneDrive / Outlook）を利用した意図しないデータの持ち出し

3.6. 導入メリットと注意点

メリット

- **ゼロトラスト前提のアクセス制御**
  ネットワーク境界に依存せず、「誰が・どの端末で・何にアクセスするか」に基づいてアクセス可否を判断する。
- **高度な Web フィルタリング**
  カテゴリや FQDN によるアクセス制御で危険サイトや不要サイトを確実にブロック。
- **脅威防御とTLS検査**
  マルウェア検知やTLS検査により脅威対策を強化。
- **Microsoft 365 への最適化**
  Microsoft のグローバルネットワーク経由で最適なルートに接続されるため、Microsoft 365 をより安定かつ高速に利用できる。
- **Microsoft Entra ID との統合による一元管理**
  Entra ID と統合されているため、ID 管理・条件付きアクセス・セキュリティログ確認を1つの管理画面でまとめて運用できる。
- **利用状況の可視化**
  トラフィックログにより、ユーザーがどのサイト（宛先ドメイン）へアクセスしたかなどのインターネット利用データを収集し、監査や調査に活用。

注意点

- **事前のユースケース整理と適用範囲の明確化**
  制御するカテゴリやドメイン、対象となるユーザー・端末を整理し、全トラフィックに適用するか段階的に展開するかなど、適用範囲を明確に設計する必要がある。
- **GSA クライアント展開が前提**
  管理者がデバイスへGSAクライアントを導入して、あわせて管理側でトラフィック転送設定を有効化・構成する必要がある。
- **既存のネットワーク機器との競合**
  既存のプロキシサーバーやウイルス対策ソフト、既存のVPNクライアントと競合し、通信不安定になる可能性があるため、事前の検証（PoC）が不可欠。
- **業務影響を考慮したポリシー設計が必要**
  Web制御やアクセス制限を厳しくしすぎると、業務アプリの通信に影響する可能性あり。
- **ログ・トラブルシュート体制の整理**
  接続不可時に「Entra側/デバイス側/アプリ側」のどこで問題が起きているか切り分けられるようにする。

3.7. ユースケース：インターネット利用の安全性向上

ここでは、Entra Internet Access をどのように活用できるかをイメージしていただくため、代表的な活用シナリオを紹介します。

要件・課題

- 業務に不要・危険な Web サイト（SNS、動画、ギャンブル等）へのアクセスを制御したい
- ユーザー・端末ごとに異なるアクセス要件を柔軟に適用したい
- HTTPS化により暗号化通信の内容が見えず、従来の社内ネットワーク中心のセキュリティ対策では十分に対処できない
- セキュリティ監査・インシデント調査のための詳細なログを一元的に取得したい

利用機能

- **Web コンテンツフィルタリング（カテゴリ/FQDN ベース）**
  業務外・危険カテゴリのサイトをブロック（例：SNS・動画・ギャンブルをブロックし、業務に必要な特定ドメインのみ許可するなど）
- **ユニバーサル条件付きアクセス**
  ユーザー属性・デバイス状態に基づき、インターネット通信自体へアクセス条件を適用（準拠デバイスのみ許可）
- **TLS検査**
  HTTPSの中身を検査し、フィッシング・悪意あるファイルなどを検知
- **トラフィックログの収集・可視化**
  「誰が・いつ・どこへアクセスしたか」を記録し、分析・監査に活用。

活用ポイント

- ✓ ID・デバイス状態を基準にした**ゼロトラスト型Webアクセス制御**が行える。
- ✓ ユニバーサル条件付きアクセスにより、アプリだけでなく**インターネット通信全体**を統合ポリシーで管理。
- ✓ TLS検査で暗号化通信のリスクも可視化し、**高度な攻撃を防止**。
- ✓ **詳細ログ**（トラフィックログや監査ログなど）により監査・インシデント調査の品質が向上。
- ✓ Web アクセス制御とログ管理が**Microsoft Entra上で一元化**され、管理効率とガバナンスが大幅に向上。

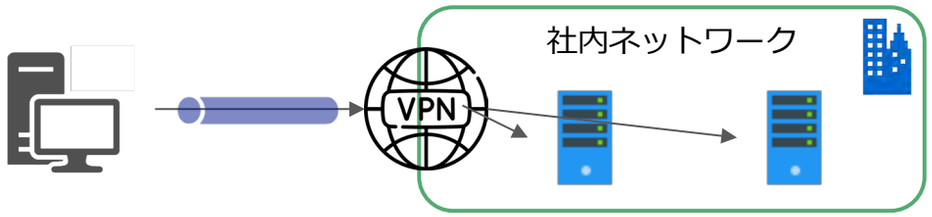
4. Entra Private Accessの機能概要

4.1. Entra Private Accessとは

Microsoft Entra Private Access（EPA）は、ID を中心とした **Zero Trust Network Access（ZTNA）**を実現し、**プライベートアプリケーションへのアクセスを安全に提供するクラウド型セキュリティサービス**です。
従来の VPN に代わり、プライベートネットワークコネクタを通じて、社内リソースへのアクセスを安全に提供します。

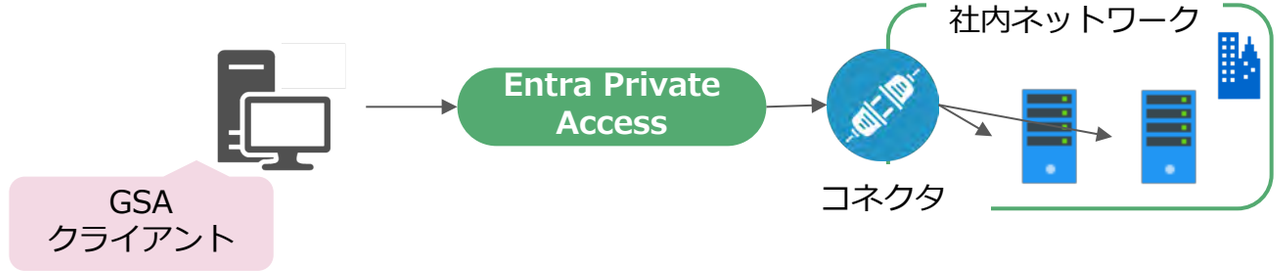
従来のリモートアクセス（VPN）の課題

- **セキュリティリスク**
  - ・VPN装置はインターネットに公開され、脆弱性攻撃の対象に
  - ・接続後は広いネットワークアクセスが可能で横移動リスクが高い
- **パフォーマンス低下**
  - ・利用集中で帯域が逼迫、通信が遅くなる
  - ・地理的な VPN 集中拠点による遅延
- **運用負担**
  - ・VPN 装置のパッチ適用・証明書管理・台数増強が必要
  - ・拠点追加のたびにネットワーク設計が必要



Entra Private Accessで解決できるポイント

- **VPN 機器が不要で、安全性が向上**
  - ・インターネットに装置を公開しないため攻撃リスクが低い
- **必要なアプリだけにアクセスできる（最小権限）**
  - ・ネットワーク全体ではなく、アプリ単位で安全に接続
- **強力な認証（条件付きアクセス）が使える**
  - ・MFA やデバイス準拠、リスク判定でアクセスを制御
- **ユーザー操作不要でシームレスに接続**
  - ・クライアントが自動で最適な経路に接続するため、VPN のような手動操作が不要

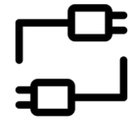


4.1. Entra Private Accessとは

Entra Private Access は、組織がプライベートとみなすFQDNやIPアドレスへのアクセスを安全に管理し、ユーザーがVPNを使わずに内部アプリへシームレスに接続できるようにするゼロトラスト基盤です。
クイックアクセスやアプリごとのアクセス構成、さらに条件付きアクセスと組み合わせることで、プライベートリソースへのアクセスを柔軟かつ安全に最適化します。

特徴

■プライベート ネットワーク コネクタ



オンプレミス環境やクラウド上のWindows Serverに配置し、Microsoft のクラウドと安全なアウトバウンド接続を確立するエージェントです。
VPN 装置のようにインターネット側へポートを公開する必要がなく、許可された通信だけを社内リソースへ安全に中継します。
これにより、ユーザーは追加操作なしで社内システムへシームレスにアクセスできます。

■クイックアクセスアプリ

IPアドレスやFQDNをまとめてプライベートリソースとして指定し、必要な範囲のみ安全にアクセスさせることができます。ネットワーク全体を開放せず、最小限の領域をゼロトラストで保護します。

■グローバル セキュア アクセス アプリ

RDP・SSH・SMB などの社内アプリへのアクセスを、アプリ単位で細かく制御できます。
条件付きアクセスと連携し、ユーザーごとに利用可能なアプリを限定することで、最小権限アクセスを実現します。

4.2. 特徴① プライベート ネットワーク コネクタ

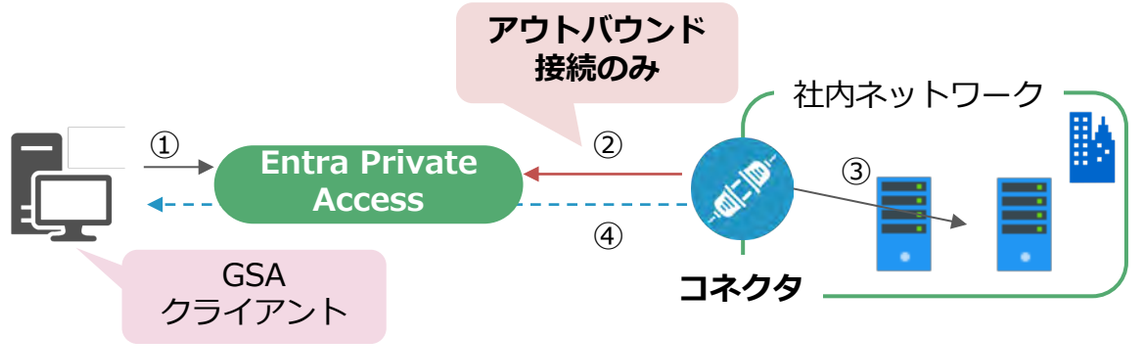
プライベート ネットワーク コネクタとは、プライベートネットワーク内の Windows Server にインストールする軽量エージェントで、
“橋渡し役”として Entra Private Access と社内リソースを安全に接続する中核コンポーネントです。

ポイント

- ✓ **アウトバウンド接続のみで EPA と通信（インバウンド不要）**
  コネクタからクラウド側（EPA）へ“内部から外へ向かう通信”だけで動作するため、外部公開や公開IPが不要で攻撃対象領域を大幅に削減。
- ✓ **ステートレス設計（設定はクラウド側で集中管理）**
  コネクタ側に設定を保持しないため、追加・復旧がシンプルで運用負荷が小さい。
- ✓ **複数コネクタをまとめて冗長化（コネクタグループ）**
  グループ化したコネクタ間で処理が分散されるため、安定した接続が維持される。
- ✓ **幅広い社内アプリに対応（Web だけでなく RDP・SMB などの非 Web アプリにも対応）**
  Entra には、オンプレミスの Web アプリ（HTTP/HTTPS）を公開するための機能として”Entra Application Proxy”が提供されている。
  EPAは、Web アプリに加えて非Webアプリ（RDP・SSH・SMBなど）にも対応しており、より幅広い社内アプリを安全に公開できる。

動作イメージ

1. ユーザー端末の GSA クライアントが通信を検出して EPA へ送信。
2. コネクタは内部ネットワークからEPA へ**アウトバウンド接続**を張り、
   EPA は許可されたリクエストをその接続経由でコネクタへ送る。
3. コネクタが内部のプライベートリソースへ代理でアクセスする。
4. 応答は コネクタ → EPA → 端末 の順に戻り、端末はプライベートリソースを利用できる。



4.3. 特徴② クイックアクセスアプリ

クイックアクセスアプリは、Entra Private Access において「**IPアドレスやFQDNなどをまとめて “許可された通信の一覧（許可リスト）” として登録し、ユーザーが安全にアクセスできるようにする仕組み**」です。
VPN のようにネットワーク全体を開放せず、必要な範囲だけをゼロトラストで保護しながら提供できるのが特徴です。

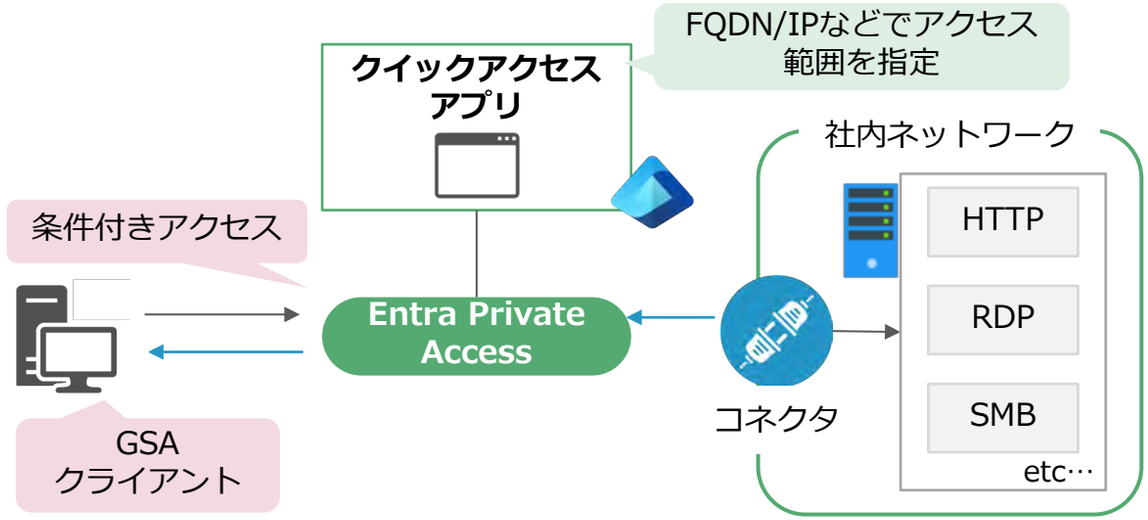
ポイント

✓ **主要なネットワークリソースを一括登録**
・FQDN / IP / IP 範囲 / ポート / プロトコル（HTTP・RDP・SMB など）のアクセス対象となる内部リソースを、クイックアクセスアプリにまとめて登録できる。
・登録した範囲だけがユーザーのアクセス対象となるため、必要最小限のアクセス範囲をシンプルに構成できる。

✓ **管理者はFQDN/IP単位で最小権限アクセスを実現**
・条件付きアクセスと統合され、ユーザー・グループ・デバイス状態・場所などの条件に基づいてアクセス可否を判定できる。

仕組み

1. GSA クライアントが通信先 FQDN/IP/ポートを検出し、**クイックアクセスアプリと照合一致した通信だけがEPAへ送信**
2. Entra ID がユーザー/デバイス状態に基づいて条件付きアクセスを評価
3. EPA が評価結果を適用し、許可された通信のみ通過
4. **許可された通信だけがプライベート ネットワーク コネクタに届き**、安全に社内ネットワークへ接続される
5. ユーザーはネットワーク全体ではなく、必要最小限のリソースだけにアクセスできる



4.4. 特徴③ グローバル セキュア アクセス アプリ

グローバル セキュア アクセス アプリとは、Entra Private Accessにおいて、**アプリケーション単位でアクセス制御を行うための仕組み**です。
前述のクイックアクセスアプリが複数の内部リソース（FQDN・IP範囲・プロトコル）をネットワーク単位でまとめてアクセスを許可するのに対し、グローバル セキュア アクセス アプリは、業務アプリごとにアクセス条件を細かく設定できることが特徴です。

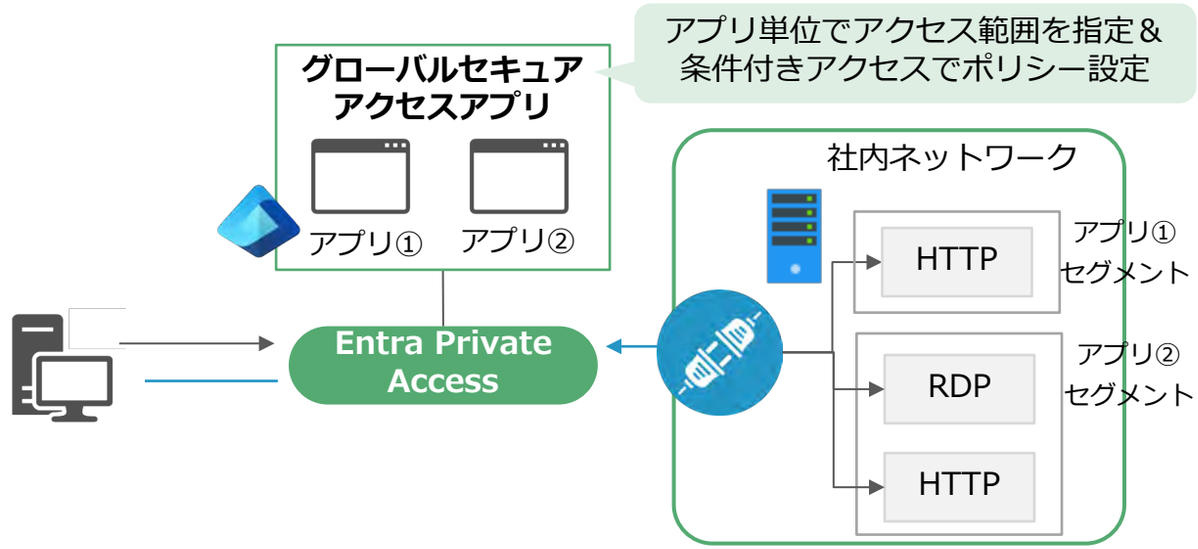
ポイント

✓ **アプリ単位で柔軟なアクセス制御**
- 部門、プロジェクト、外部パートナーなど特定のユーザー群にだけ、必要なアプリへのアクセスを許可できる。
- アプリごとに MFA、準拠デバイス、場所など異なる条件付きアクセスを適用可能。
- アプリ登録対象（FQDN / IP / IP範囲 / ポート / プロトコル）はクイックアクセスと同様。

✓ **最小権限アクセスの実現**
- 保護領域とアプリごとの細かなアクセス権を両立
- 例：アプリA＝社内限定、アプリB＝特定デバイス＋MFA

アプリの登録例

アプリ①：社内ポータル（HTTP）
- FQDN：intranet.company.local
- ポート：80 / 443
- アクセス対象：社員のみ
- 条件付きアクセス：社内ネットワーク＋準拠デバイス



4.4. 特徴③ グローバル セキュア アクセス アプリ

プライベートリソースへのアクセス方式として「クイックアクセス」と「グローバルセキュアアクセスアプリ」の2種類が提供されます。
本スライドでは、両者の違いを整理し、どのようなユースケースで使い分けるべきかを解説します。
ゼロトラスト実現に向けた段階的な移行や、VPN 代替からアプリ単位のセグメント化まで、目的に応じた最適な選択を理解することができます。

観点	クイックアクセスアプリ	グローバルセキュアアクセスアプリ
目的 / 用途	・ネットワーク単位で広めに社内リソースへアクセスを許可したい場合 ・早期にプライベートアクセス環境を立ち上げたい組織に最適	・特定アプリケーションへ**最小権限アクセス**を実現したい場合 ・アプリ単位で厳密にアクセス制御したい組織に最適
対象・制御粒度	ネットワーク単位（中程度の粒度） ・FQDN / IP / プロトコルで許可	アプリ単位（**細かい粒度**） ・アプリごとにセグメント化し、個別にアクセス制御
条件付きアクセス	アプリ全体に共通のポリシーを適用、分離は不可	**アプリごとに異なるポリシー設定が可能** ユーザー属性・デバイス状態・場所などを個別に制御
構成の手軽さ	**比較的容易**（最速で導入できる）	中程度（アプリごとに設定が必要で柔軟だが、手間は増える）
向いている環境	まずは GSA を導入して社内アクセスを確保したい組織	部門別・アプリ別にきめ細かくアクセス制御をしたい組織

ポイント

- ✓ クイックアクセスアプリ：移行初期フェーズに最も適しており、VPN 代替の入口として利用を推奨
- ✓ グローバルセキュアアクセスアプリ：最小権限や部門別の制御など、細かい制御が求められる本番稼働やゼロトラストの実現

4.5. 導入メリットと注意点

メリット

- **ゼロトラストネットワークアクセス（ZTNA）を実現**
  ID中心のアクセス制御により、どこからでもプライベートアプリ・リソースへ安全にアクセス可能。
- **VPN の代替として利用できる**
  デバイスからGSAクライアントを利用し、プライベートネットワークへ安全に接続可能。外部にVPNエンドポイントを公開する必要がない。
- **細かいアプリ単位のアクセス制御（最小権限）**
  アプリ単位でユーザー割り当て・条件付きアクセスを設定可能。
- **広範なアプリケーションに対応（TCP/UDP も可）**
  Web 以外にも DB、RDP、ファイル共有などに対応し、レガシーアプリもゼロトラスト化できる。
- **条件付きアクセスとの統合が容易**
  アプリ単位でMFAやデバイス要件などのポリシーを適用できる。
- **Microsoft全体のID体系と統合**
  Entra ID の既存ポリシーをそのまま利用でき、統合的なアクセス管理が可能。

注意点

- **プライベート ネットワーク コネクタの前提条件が必要**
  Windows Server、アウトバウンド許可の要件や、
  配置場所・冗長構成などの設計を事前に整理する。
- **既存VPNとの共存・切り替え計画が重要**
  既存VPNやSSEとの併用時はルーティング重複の影響に注意（運用ポリシー上の優先度設計や切り替え計画が必要）。
- **条件付きアクセス設計の影響範囲が大きい**
  設定ミスにより業務アプリへアクセス不可になるリスクがある。
- **アプリ通信要件の整理が必須**
  通信要件（FQDN、IP、ポート、プロトコル）の事前棚卸しが必須。
- **アプリ単位のアクセス制御における工数増加**
  設定変更や見直しの頻度が増えることで運用工数が増大しやすい。
- **GSA クライアント展開が前提**
  管理者がデバイスへGSAクライアントを導入して、あわせて管理側でトラフィック転送設定を有効化・構成する必要がある。

4.6. ユースケース：プライベートアプリ・社内リソースへのアクセス

ここでは、Entra Private Access をどのように活用できるかをイメージしていただくため、代表的な活用シナリオを紹介します。

要件・課題

- 社員が自宅・外出先から VPN を使わずに社内システムへ安全にアクセスしたい
- アプリによってアクセスさせるユーザー・条件を細かく変えたい（部門ごと・機密性の高いアプリのみ等）。
- 安全な接続デバイス（準拠デバイス、Entra 参加デバイス）のみ社内リソースへ接続させたい。
- RDP、ファイルサーバーなど Web 以外のプロトコルも安全に公開したい。

利用機能

- **クイックアクセスアプリ（移行初期・VPNの代替）**
  許可対象の FQDN/IP/ポートだけをトンネル化し、RDP・ファイル共有等も含めて必要な範囲のみ安全にアクセスさせる。
- **グローバル セキュア アクセス アプリ（本番運用）**
  アプリ単位のアクセス構成で公開対象（FQDN/IP/ポート）を細かく定義し、部門や役割ごとに割り当てを分離する。
- **条件付きアクセス**
  “準拠デバイスのみ許可”、“リスク時はブロック”などのポリシーを適用し、接続状況に応じて動的にアクセス制御を行う。
- **トラフィックログの収集・可視化**
  「誰が・いつ・どこへアクセスしたか」を記録し、分析・監査に活用。

活用ポイント

- ✓ **許可したアプリ・ネットワーク範囲だけにアクセスを限定**し、RDP やファイルサーバーなど非 Web プロトコルも安全に利用可能。
- ✓ アプリ単位でユーザー/部門ごとにアクセス権を分離し、**条件付きアクセスと組み合わせて最小権限を徹底**。
- ✓ デバイス準拠・リスク状況に応じてアクセス可否を自動判定し、侵害リスクを早期に防止。
- ✓ **詳細ログ**（トラフィックログや監査ログなど）により監査・インシデント調査の品質が向上。
- ✓ アクセス制御とログ管理が **Entra に統合**され、運用効率とガバナンスが向上。

5. ライセンス要件

5.1. ライセンス要件

Global Secure AccessはEntra Internet Access（EIA）とEntra Private Access（EPA）で構成され、利用には共通ライセンスと機能別ライセンスが必要です。

共通で必ず必要となるライセンス

GSAを利用するには、**Microsoft Entra ID P1**以上が必要です。Entra ID P1 以上が含まれるMicrosoft 365 のライセンスは以下の通りです。
Microsoft Entra ID P1：Business Premium・E3
Microsoft Entra ID P2：E5

機能別で必要となる追加ライセンス

- **Microsoft Entra Internet Access（スタンドアロン）**
  Entra Internet Access（EIA）機能を単体で利用する場合に必要
- **Microsoft Entra Private Access（スタンドアロン）**
  Entra Private Access（EPA）機能を単体で利用する場合に必要
- **Microsoft Entra Suite（包括ライセンス）**
  EIA・EPAを含む、5つの機能をまとめて含む包括ライセンス　※含まれる製品の詳細は「2.1. Microsoft Entra Suiteとは」を参照

補足

- Microsoft サービス向けのEntra Internet Accessの機能は、Entra ID P1/P2のライセンスに含まれています。
- リモートネットワークの帯域幅は、購入したライセンス数に応じて加算され、確保した帯域幅は、IPsec トンネルごとに 250 / 500 / 750 / 1000 Mbps のいずれかの単位で割り当てることができます。　参考情報