【Microsoft Entra ID】テナント制限について

2026年4月30日

改訂履歴

版数	発行日	改訂内容
第1版	2026年4月30日	初版発行

本資料の内容は 2026/4/30 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ご了承ください。

Agenda

1.前提情報
    1. 本資料の目的
    2. 用語集
2.背景・基本概念
    1. テナント制限の概要
    2. テナント制限の利用背景
3. 機能・仕組み
    1. テナント制限 v1 の仕組み
    2. テナント制限 v2 の仕組み
    3. 認証プレーン保護とデータプレーン保護
    4. v1 と v2 の比較
4.導入・構成・設定・考慮事項
    1. v1の導入手順
    2. v2の導入手順
    3. ハイブリッド構成での考慮事項
5.運用管理
    1. 運用時のヘッダー確認とログ確認

1. 前提情報

1.1. 本書の目的

目的

本書は、Microsoft Entra ID のテナント制限について、設計・導入・運用を行う担当者が必要な知識を体系的に理解することを目的としています。テナント制限の仕組みや制御できる範囲、想定される利用シナリオを整理するとともに、導入時および運用時に考慮すべきポイントを明確にし、適切なセキュリティ対策の実現を支援します。

※本資料で扱うテナント制限 v2 は、2026/4/30現在プレビュー段階の機能です。
今後仕様や画面構成、動作が変更される可能性があります。
実際の導入や運用にあたっては、最新の公式ドキュメントをご確認ください。

1.2. 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	Entra ID	Microsoft が提供するクラウド型の ID（ユーザー）管理サービス。
2	シャドー IT	企業が把握・管理していない状態で、従業員が個人的にクラウドサービスやITツールを業務に利用する仕組み。
3	SaaS	ソフトウェアをインターネット経由で提供し、利用者がインストールせずに使えるサービス形態。
4	プロキシ	利用者とインターネットの間に入り、通信を中継・制御する仕組み。
5	HTTP ヘッダー	HTTP 通信で送信される付加情報で、認証情報や通信条件などをサーバーに伝える仕組み。
6	ゼロトラスト	「すべてのアクセスを信用しない」ことを前提に、常に認証と検証を行うセキュリティの考え方。
7	テナント	Microsoft クラウドサービス上で作成される、組織ごとに分離された利用環境（専用の管理単位）。
8	テナント ID	テナントを一意に識別するための ID。
9	条件付きアクセス	ユーザーや場所、デバイスの状態などの条件に応じてアクセスを制御するセキュリティ機能。

1.2. 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
10	デバイス管理	PC やスマートフォンなどの端末を一元的に管理し、セキュリティ設定や利用ルールを制御する仕組み。
11	プロキシ依存	通信の制御やセキュリティ対策をプロキシサーバーに頼っている状態。
12	レガシー	古い設計や仕組みのまま使われ続けているシステムや技術のこと。本資料においてはテナント制限v1。
13	Microsoft Entra 管理センター	ユーザーやデバイス、アプリのアクセス権を一元的に管理し、組織のIDとセキュリティを安全に運用するための管理ポータル。
14		
15		
16		
17		
18		

2. 背景・基本概念

2.1. テナント制限の概要

本ページでは、Entra ID のサービス概要とテナント制限の機能について説明します。

Entra ID とは

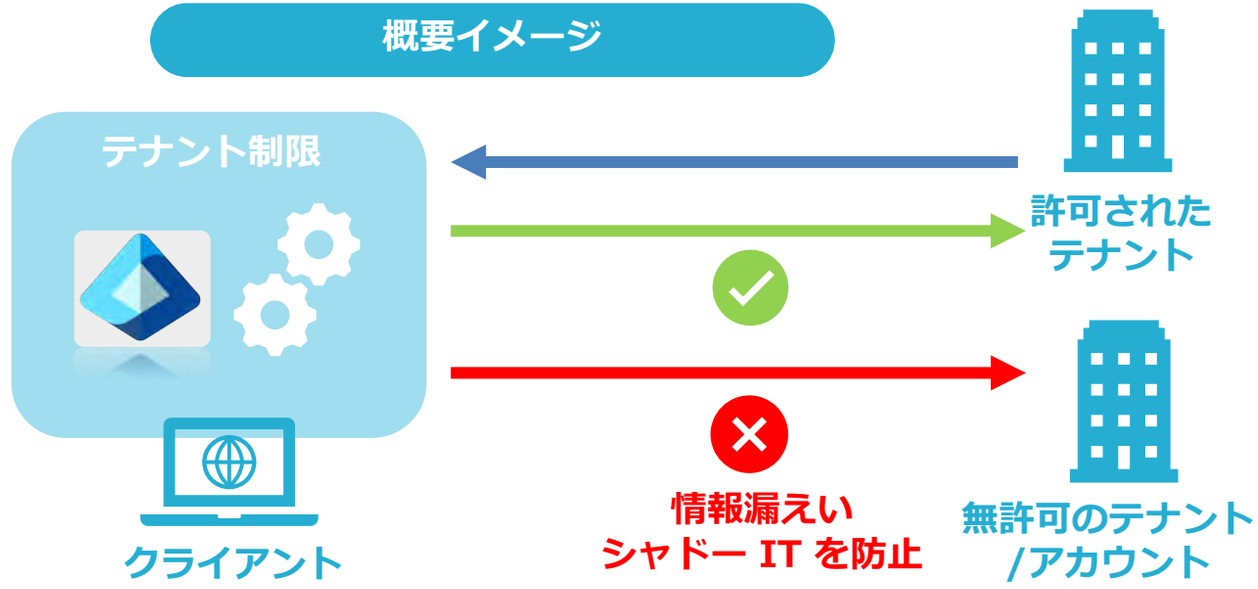
- ✓ Microsoft が提供するクラウド型の ID・認証サービス。
- ✓ ユーザー、グループ、サインインを一元的に管理できる。
- ✓ Microsoft 365 や Azure、SaaS への安全なアクセスを実現。

テナント制限の概要

テナント制限は、**ユーザーがサインインできる Microsoft 365 テナントを制御する仕組み**です。
主に、以下のテナントへのサインインを制限し、あらかじめ許可されたテナントのみアクセスを許可することで情報漏洩やシャドー IT を防止する目的で利用します。

- ✓ 会社が管理していない外部テナント
- ✓ 個人用アカウントや無許可の組織テナント

概要イメージ



2.2. テナント制限の利用背景

以下は、テナント制限を利用する際の基本的な背景を整理したものです。

テナント制限の利用背景

■ 個人アカウントや他社テナントへのサインイン防止

業務用デバイスから、ユーザーが個人の Microsoft アカウントや会社が許可していない他社テナントにサインインしてしまうケースがあります。これにより、業務データが意図せず外部環境に保存されるリスクが生じます。テナント制限は、**許可されたテナント以外へのサインインを防ぐために利用されます。**

■ 情報漏えい・データ持ち出しリスクの低減

SharePoint、OneDrive、Teams などのクラウドサービスは便利な反面、アクセス先を誤ると会社の情報が外部テナントに流出する可能性があります。テナント制限を導入することで、**業務データの保存先・利用先を組織が管理できる状態を維持できます。**

■ ハイブリッドワーク環境への対応

在宅勤務やモバイルワークが一般化し、ユーザーが社内外さまざまな場所からクラウドにアクセスするようになりました。このような環境では、ネットワークに依存しない形でサインイン先を制御する必要があります。テナント制限は、**場所を問わず一貫したアクセス制御を実現するために利用されます。**

■ ゼロトラストセキュリティの実現

ゼロトラストでは「ネットワークを信頼しない」ことが前提となります。誰が、どこから、どのテナントにアクセスしているのかを常に検証する必要があります。テナント制限は、「アクセス先のテナント」も制御対象に含めることで、**ゼロトラストを補強する仕組みとして導入されます。**

3. 機能・仕組み

3.1. テナント制限 v1 の仕組み

現在 Microsoft 社ではテナント制限 v1 (以降：v1) とテナント制限 v2 (以降：v2) という 2 種類のテナント制限方法を提供しています。
本章ではそれぞれの仕組みやメリット、注意点について説明します。

仕組みイメージ

v1 は、指定した Entra ID テナント以外へのサインインを、**プロキシ（ネットワーク）側でブロックする仕組み**です。

管理者がプロキシに許可テナントを設定し、プロキシが社内ネットワーク経由の通信に許可テナント情報を付加、Entra ID がその情報を基にサインインを許可することで制御します。

メリット

- ✓ 社内ネットワークから許可した Entra ID テナントのみにサインインを限定できる
- ✓ 管理対象外テナントへの 情報漏えいリスクを低減できる
- ✓ Entra ID の設定変更が不要で、プロキシで制御できる

注意点

- ✓ 社内ネットワーク経由の通信のみ有効（社外・モバイル回線は対象外）
- ✓ プロキシや HTTP ヘッダー設定が必要で、ネットワーク設計の理解が必須
- ✓ ユーザー単位・端末単位の柔軟な制御は不可

3.2.　テナント制限 v2 の仕組み

本ページでは現在プレビュー機能として提供されている v2 について説明します。

仕組みイメージ

v2 は、条件付きアクセスを利用して、指定した Entra ID テナント以外へのサインインを、**Entra ID 側で制御・ブロックする仕組み**です。

プロキシやネットワークに依存せず、Entra ID の条件付きアクセスによって、許可されたテナントへのサインインのみを制御・許可します。

メリット

✓ Entra ID ベースでテナント制御ができる
（ネットワークやプロキシに依存しない）
✓ 社内・社外を問わず、どこからのサインインでも制御できる
✓ ユーザーやグループ単位で、柔軟なポリシー設計ができる
✓ MFA やデバイス条件など、他のセキュリティ条件と組み合わせできる

注意点

✓ プレビュー機能のため、本番利用には慎重な検討が必要
✓ 条件付きアクセスの設計の知識が必要
✓ 利用には Microsoft Entra ID P1 以上のライセンスが必要
✓ 将来的に仕様変更の可能性がある

3.3. 認証プレーン保護とデータ プレーン保護

テナント制限 v2 では、認証段階での制御（認証プレーン保護）に加え、リソースアクセス段階での制御（データプレーン保護）を組み合わせることで、より強固なテナント制御を実現します。

認証プレーン保護

テナントにいないアカウントのサインインをブロックする仕組み

不正な第三者がテナントにサインインしようとした際、そのサインインをブロックすることで、攻撃者が外部メールを介してデータを漏洩するのを防ぐことができます。

v2 の場合、Entra 管理センター内でポリシーを作成することで保護が可能です。

データ プレーン保護

認証を経ないアクセスを防ぐ仕組み

不正な第三者が Teams 会議や SharePoint ファイルに匿名でアクセスしようとしても、認証に失敗した場合はアクセスをブロックすることで、不正なリソースへのアクセスを防ぐことができます。

補足

v1 は企業プロキシを前提に、許可したテナントのみサインインを許可する認証保護を提供します。
v2 ではプロキシ有無に依存せず、認証保護とデータアクセス保護が可能です。
ただしプロキシ経由の通信のみを対象にする方式では、サインイン時に付与される情報のみを制御できるため、認証保護のみが対象となり、認証後のデータアクセスには保護が適用されません。

3.4. v1 と v2 の比較

本ページでは、テナント制限における v1 と v2 の違いについて、比較表形式で整理しています。

v1 / v2 の比較表

	v1	v2
判定の起点	アクセス元ネットワーク	ユーザー認証時
制御の起点	プロキシ	Entra ID
設定場所	プロキシ設定	Microsoft Entra 管理センター
制御粒度	テナント単位	ユーザー・グループ・アプリ単位
認証プレーン保護	△	○
データプレーン保護	×	○
向いているユースケース	社内ネットワークから特定テナントのみ許可	ユーザーの ID・条件に基づき 特定テナントのみ許可
必要なライセンス	不要 （Microsoft Entra ID Free の機能範囲で利用可）	Microsoft Entra ID P1 以上
適用範囲	社内ネットワークのみ	すべてのアクセス
在宅・モバイル環境からのアクセス制御	△ （VPNで社内ネットワーク経由であれば可）	○
ゼロトラスト適合	×	○
Microsoft社の推奨	レガシー	推奨

4.導入・構成・設定・考慮事項

4.1. v1の導入手順

本章では、Entra ID におけるテナント制限(v1/v2)を構成するための一連の設定手順を説明します。
以下の図は、v1 を設定・適用する際の全体の流れを示したものです。

どのテナントへのサインインを許可するかを明確にする

✓自社テナントや、業務上利用を認めているテナントを洗い出す

✓各テナントの テナント ID を事前に取得しておく

✓このテナント ID が、後続の制御判断の「基準情報」になる

すべての対象通信を制御ポイントに集約する

✓社員の Microsoft 365 サインインへの通信が必ず社内プロキシを通過するようにネットワークを設計する

✓制御を回避できる通信経路が存在しないよう、インターネットへ接続できるすべての経路を確認する

Entra ID に「許可テナント情報」を伝える

✓プロキシで Microsoft クラウド宛の通信を識別する

✓対象となる通信に対し、許可するテナント ID を含む専用の HTTP ヘッダーを付与する

サインインの可否を最終判断する

✓ Entra ID がサインイン要求を受信し、HTTP ヘッダー内の「許可テナント ID」と、実際のサインイン先テナントを照合する

→一致していれば サインイン許可
→一致しなければ サインイン拒否

ポイント

v1 ではユーザー別の制御ができないため、全ユーザーに影響することを前提に、業務上必要なテナントのみを許可する運用が推奨されます。
業務上必要なテナントのみに限定することで、意図しない外部テナントへのサインインを防止できます。

4.1. v1の導入手順

本ページでは v1の導入手順のプロキシでHTTP ヘッダーを付ける方法について抜粋し、説明します。

許可するテナントを決める → 社内プロキシを経由させる → **プロキシで HTTP ヘッダーを付ける** → Entra ID がサインインを判定する

社内で利用しているプロキシの設定画面で以下の通りヘッダーを追加します。

Restrict-Access-To-Tenants

「どのテナントへのサインインを許可するか」を指定するヘッダー

このヘッダーには、ユーザーがアクセスを許可されているテナントの一覧を設定します。
値には、テナントを識別できる情報をカンマ（,）区切りで指定します。

指定できるものは、次のいずれかです。
- ✓テナントのドメイン名（例：contoso.com）
- ✓onmicrosoft.com のドメイン
- ✓テナント ID（ディレクトリ ID）

Restrict-Access-Context

「このテナントがテナント制限を設定している管理元である」ことを示すヘッダー

このヘッダーには、自分のテナントのテナント ID を 1 つだけ指定します。

どのテナントがテナント制限を適用しているのかを、Entra ID 側に伝える役割があります。

※必ずアクセスさせたい自社テナントを指定します。

手順の詳細はMicrosoft社公開記事を確認してください。→ [テナントへのアクセスを制限する]

4.2. v2の導入手順

以下の図は、テナント制限のv2を設定・適用する際の全体の流れを示したものです。

許可するテナントを決める → **Entra 管理センターで設定する** → **条件付きアクセスと連携する** → **Entra ID がサインインを判定する**

どのテナントへのサインインを組織として認めるかを明確にする

✓自社テナントを基本とし、業務上必要な外部テナントがあれば洗い出す

✓取引先テナントや検証用テナントなど、業務要件に基づいて可否を判断する

Entra ID に設定するテナント制限のルールを決める

✓管理者が Microsoft Entra 管理センターにサインイン

✓テナント制限に関するポリシーを作成

✓許可するテナントの情報を、クラウド上の設定として登録する

誰に・どの条件でテナント制限を適用するかを決める

✓条件付きアクセスを使って対象ユーザー、対象グループを指定する

✓「許可されたテナントのみサインイン可能」という制御をポリシーとして適用

サインイン時に最終的な可否判断を行う

✓Entra ID がサインイン要求を受信

✓Entra ID が以下を総合的に評価

・サインイン先テナント
・条件付きアクセスポリシー
・許可テナント設定

ポイント

v2 では条件付きアクセスとの組み合わせが可能であるため、ユーザーやグループ単位で柔軟に制御することが可能です。
そのため、まずは影響範囲を限定したポリシーを作成し、特定のユーザーや検証用グループから段階的に適用することを推奨します。
これにより、業務影響を最小限に抑えながら、安全にテナント制限を導入できます。

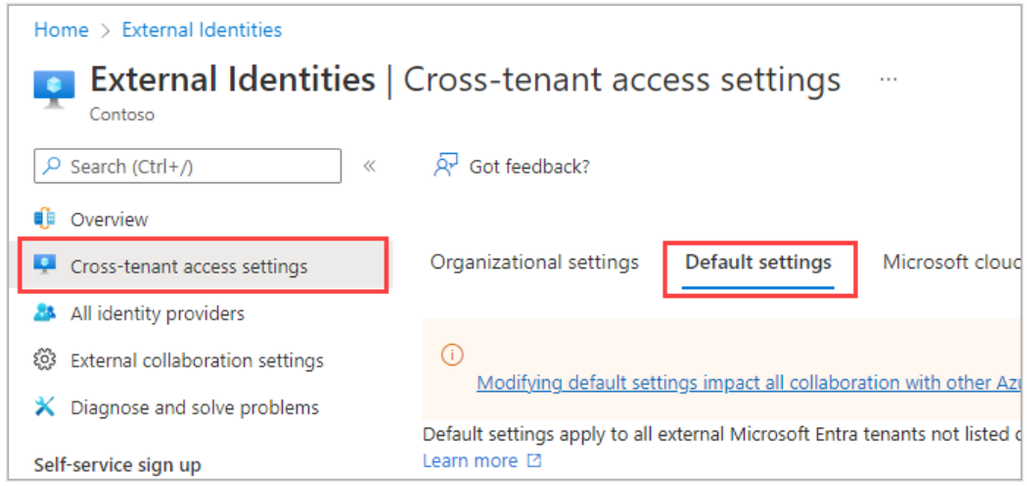
4.2. v2の導入手順

本ページではv2の導入手順のEntra 管理センターで設定する方法について抜粋し、説明します。

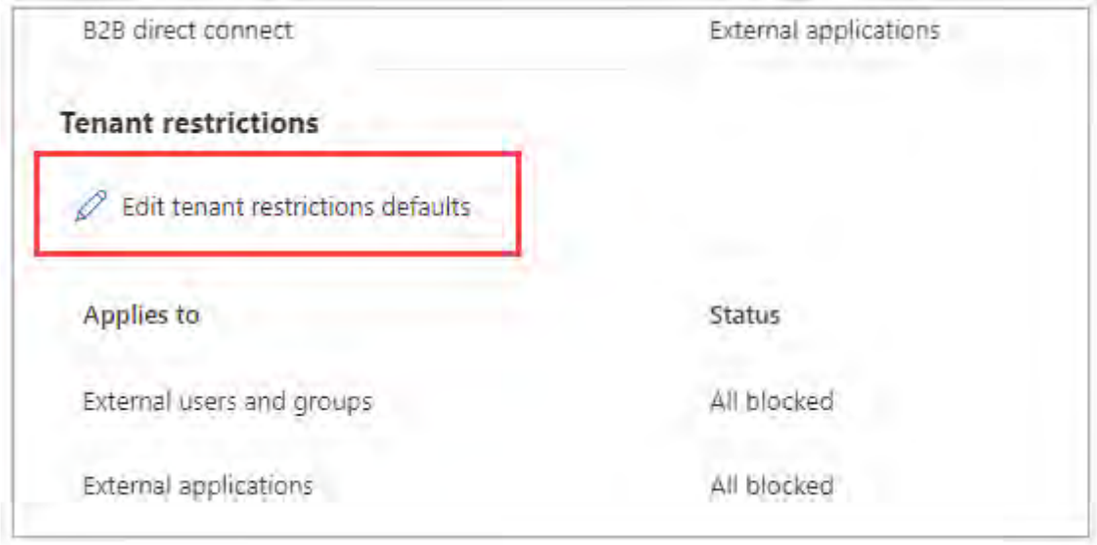
許可するテナントを決める → **Entra 管理センターで設定する** → 条件付きアクセスと連携する → Entra ID がサインインを判定する

Entra ID側でのポリシー設定場所

Entra ID>外部アイデンティティ>
テナント間のアクセス設定>[既定の設定] タブを選択します。



[テナント制限の既定の編集] リンクを選択し
「どの外部テナントを許可するか」を定義します。



手順の詳細はMicrosoft社公開記事を確認してください。→ **テナント制限 v2 を設定する**

4.3. ハイブリッド構成での考慮事項

テナント制限のハイブリッド構成では、アクセス元（社内／社外）によって適用される制御が変わる点を考慮した設計が重要です。

アクセス元（社内／社外）によるテナント制限

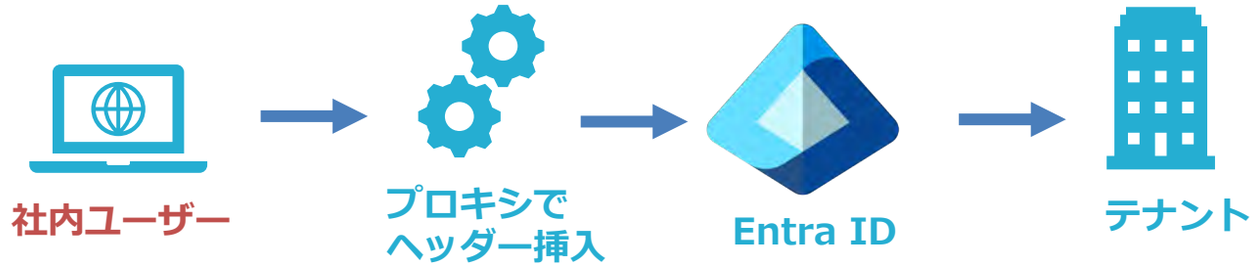
v1 は企業プロキシを前提とするため、プロキシ経由のサインインのみが制御対象となります。

そのため、v1 のみでは社外からのアクセスに対して制御が及ばず、ハイブリッド構成では一貫したアクセス制御が難しくなります。

一方、v2 はハイブリッド構成やゼロトラストの考え方を踏まえ、クラウド側のポリシーで制御されるため、ネットワーク構成に依存せず一貫したサインイン制御が可能です。

また、条件付きアクセスやデバイス管理（Intune など）と組み合わせることで、認証やデバイス状態も含めた多層的なセキュリティを実現できます。

v1：（企業プロキシを通過した通信のみが制御対象）



v2：（ネットワーク構成に依存せず一貫したサインイン制御が可能）

5. 運用管理

5.1. 運用時のヘッダー確認とログ確認

テナント制限では、設定を行うだけでなく、実際に制御が機能しているかを確認することが重要です。
本ページでは、設定後に確認すべき「ヘッダー」と「ログ」について説明します。

プロキシ側のヘッダー確認（v1）

・Microsoft 365／Entra ID 宛ての通信に対して、テナント制限用の HTTP ヘッダーが正しく付与されていることを確認します。

・ヘッダーに指定されているテナント ID が、許可したテナントのものになっていることを確認します。

・対象となる通信先が Microsoft 宛ての通信であることを確認し、不要な通信に誤って適用されていないかもあわせて確認します。

Entra ID側のログ確認（v1/v2）

・サインインログを確認し、テナント制限によってサインインがブロックされているかどうかを確認します。

・ブロックされた場合は、その理由がテナント制限によるものかをログ上で確認します。

・ポリシーの評価結果を確認し、条件付きアクセスなど他の制御が影響していないかを切り分けます。

運用時の注意点

✓ 許可テナントを変更した際は、設定内容が正しく反映されているかを必ず再確認します。変更には時間がかかる可能性があります。
✓ 設定投入後は、必ず想定通り設定がされているか必ずサインインを試しログを確認してください。
✓ 運用開始後、想定通りの挙動にならばい場合ユーザー事にサインインログを確認し切り分けが必要になります。
✓ Entra ID 側のログ確認は、テナント制限v1とv2どちらの場合も必要です。