



【Microsoft 365】 Teams の外部ユーザー

2026年04月30日

改訂履歴

版数	発行日	改訂内容
第1版	2026年04月30日	初版発行

本資料の内容は 2026/04/30 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あります旨ご了承ください。

Agenda

1. 前提情報

1. 本書の目的とゴール
2. 用語集

2. Teams 外部ユーザーの概要

1. 外部ユーザーとのコミュニケーション
2. 外部ユーザー招待が必要となるビジネス背景
3. 外部ユーザーの種類
4. ゲストユーザー
5. 他社テナント所属の外部ユーザー
6. 組織管理されていない Microsoft 個人アカウント
7. 各ユーザーの機能比較表
8. 各ユーザーのユースケース比較表

3. セキュリティ設定

1. セキュリティ設定の必要権限
2. セキュリティ設定の概要
3. Entra 管理センターにおけるテナント設定
4. Teams 管理センターにおけるテナント設定
5. Teams の会議・ポリシー設定
6. SharePoint 管理センターにおける外部・ファイル共有設定

4. 想定されるトラブルと解決策

1. 想定されるトラブルと解決策



1. 前提情報

1.1. 本書の目的とゴール

目的

本資料は、利用者または運用ベンダーが、Teams における外部ユーザー招待の仕組みを理解し、外部ユーザーを招待する方法の概要を把握することを目的とし、そのために必要な関連情報や知識をまとめ提示するものです。

ゴール

本資料を通し、利用者または運用ベンダーが Teams での外部ユーザー招待のパターンを理解したうえで、自身の運用方針に沿った招待方法を選択・運用できる状態を目指します。

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	ID 管理従業員や外部ユーザーのアカウントを作成・変更・削除し、業務システムへのアクセス権を組織として一元管理する仕組み。
2	多要素認証	ユーザーがサインインする際に、パスワードに加えて SMS や認証アプリなどの追加確認を必須とし、不正ログインを防止する認証方式。
3	条件付きアクセス	サインイン時の場所、使用デバイス、ユーザー種別、リスクレベルなどの条件に基づいて、アクセス許可や多要素認証の要否を制御するセキュリティ機能。
4	ドメイン	組織を識別するために使用されるインターネット上の名前、ユーザーのメールアドレスや Microsoft 365 へのサインイン名の一部として利用される。
5	テナント	Microsoft Entra ID や Microsoft 365 において、組織ごとに分離されたユーザー・設定・データを管理するための独立した管理単位。
6	監査ログ	ユーザーの操作や管理者による設定変更などを記録し、「誰が・いつ・何をしたか」を後から確認するためのログ。
7	Entra 管理センター	Microsoft Entra ID におけるユーザー、認証、アクセス制御、外部コラボレーションなどを管理するための管理ポータル。
8	内部ユーザー	自組織の Microsoft Entra ID テナントに所属し、組織が管理するアカウントを持つユーザー。
9	所有者権限	Teams のチームや Microsoft 365 グループにおいて、メンバー管理や設定変更、削除などを行える最上位の管理権限。

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	Teams 管理センター	Microsoft Teams の外部アクセス、ゲストアクセス、会議設定、ポリシーなどを管理者が一元的に設定・管理するための管理ポータル。
11	ユーザープリンシパル名	Microsoft Entra ID においてユーザーを一意に識別するサインイン用の名前で、通常はメールアドレス形式（例：user@domain）で表される。
12	チーム	同じ目的や業務を持つメンバーをまとめるための最上位の単位で、メンバーはチームに参加することで、その配下の会話・会議・ファイルにアクセスできるようになる。
13	チャンネル	チームに参加しているメンバーの中で、特定の業務テーマや話題ごとに会話・会議・ファイルを分けて管理するための場所。
14	チャット	チームやチャンネルに属さず、個人または少人数で即時的にやり取りを行うためのコミュニケーション手段。
15	オンボーディング	新しく参加するユーザーが業務やシステムを利用できるように、アカウント付与や操作説明などを段階的に行うプロセス。
16	Microsoft Entra ID P1	Microsoft Entra ID（旧 Azure Active Directory）の有料アドオンライセンスのひとつで、ユーザーのサインインやアクセスを条件付きで制御するための機能を追加するライセンス。
17	外部ユーザーの脱退設定	テナントにプライバシー情報が設定されていることを前提に、ゲストが自分で組織から退出できるかを制御する機能。



2. Teams 外部ユーザーの概要

2.1. 外部ユーザーとのコミュニケーション

本ページでは、Microsoft Teams（以後、Teams）の基本的な機能と、外部ユーザーとのコミュニケーション方法について説明します。



Teams とは

- ✓ 組織内外のメンバーと、会議・チャット・通話を行うためのコミュニケーション基盤
- ✓ 業務に必要な情報ややり取りを、チームや会話単位で整理・共有ができる
- ✓ Microsoft 365 の各種アプリと連携し、業務を進めるための共通の作業空間を提供する

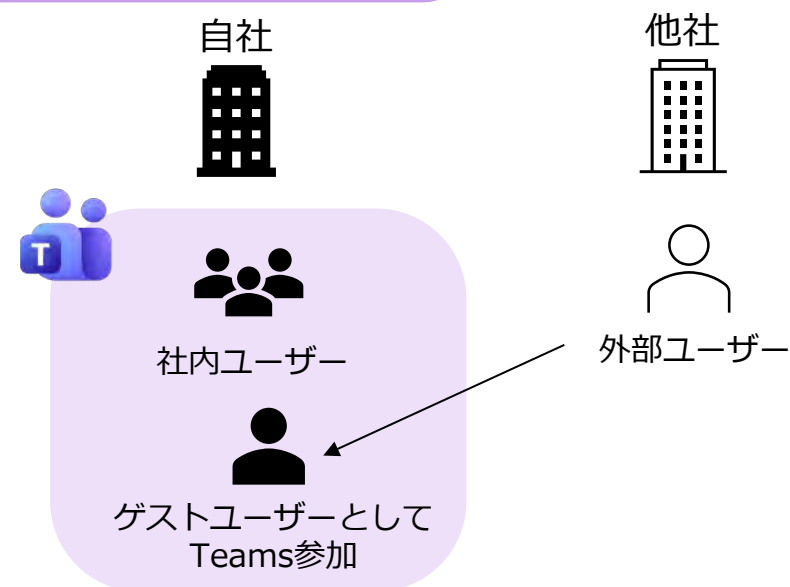
外部ユーザーの概要説明

Teams で外部ユーザーとして扱われるユーザーは、以下 3 種類です。

1. ゲストユーザー
2. 他社テナント所属の外部ユーザー
3. 組織管理されていない Microsoft 個人アカウント

これらはいずれもご利用しているテナントに存在しないユーザーですが、業務への関与度や利用期間、ユーザーの管理方法が異なります。そのため、利用目的や状況に応じて適切に使い分けることが重要です。

概要イメージ図



2.2. 外部ユーザー招待が必要となるビジネス背景

近年、多くの組織では業務が社内だけで完結することは少なくなり、取引先・パートナー企業・委託先・顧客など、社外のユーザーと日常的に連携しながら業務を進めることが一般的になっています。このような環境において、外部ユーザーを安全かつ効率的に招待し、必要な範囲でコラボレーションできる仕組みが求められています。

社外との会議・打ち合わせの オンライン化

商談、定例会、プロジェクト報告など、多くのコミュニケーションがオンライン会議へ移行し、社外の参加者を Teams 会議に招待するニーズが急増しています。



社外メンバーと継続的に共同作業を 行う機会の増加

取引先と共同でプロジェクトを進めること、また、パートナー企業と Teams のチャンネル上で日常的にコミュニケーションするなどファイル共有やチャンネルでのやり取りも増加しています。



セキュリティ・コンプライアンス要求 の高度化

社外とのやり取りをメール添付や個別のファイル共有サービスで行うと、アクセス権の把握や、操作履歴の確認が難しくなる場合があります。そこで、Teams でのコミュニケーションを起点にし、Entra ID で外部ユーザーを管理することで、「誰が・どの情報」にアクセスしているかを可視化・制御しながら安全にやり取りをしたいというニーズが高まっています。



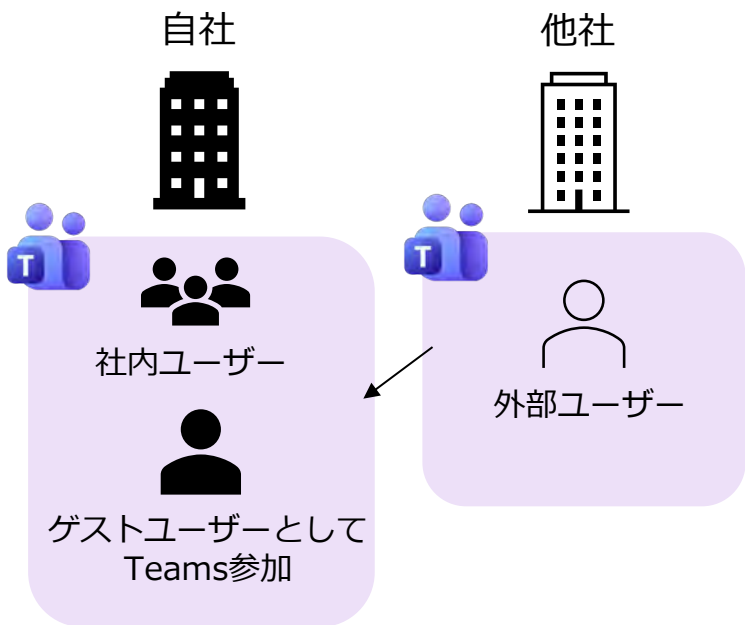
Teams では「会議だけの一時的な外部参加」から「ファイル共有やチャンネルを含む継続的な共同作業」まで、外部ユーザーの関与度やセキュリティ要件に応じて使い分けることで、効率的かつ安全に一元的なコラボレーションを実現できます。

2.3. 外部ユーザーの種類

外部ユーザーについては前述していますが、本章では各ユーザーについてあらためて整理します。この分類を正しく理解することは、適切な招待方式の選択や、セキュリティ・運用ルールを設計するうえで非常に重要です。本ページでは、各ユーザーの違いについて説明します。

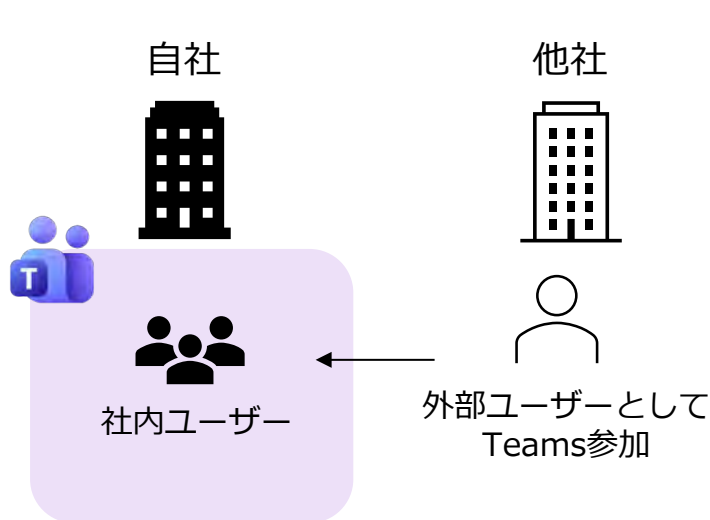
ゲストユーザー

外部ユーザーを Entra ID に**ゲストとして登録**し、自組織の Entra ID 管理配下で Teams や SharePoint の利用を可能にする外部ユーザーです。



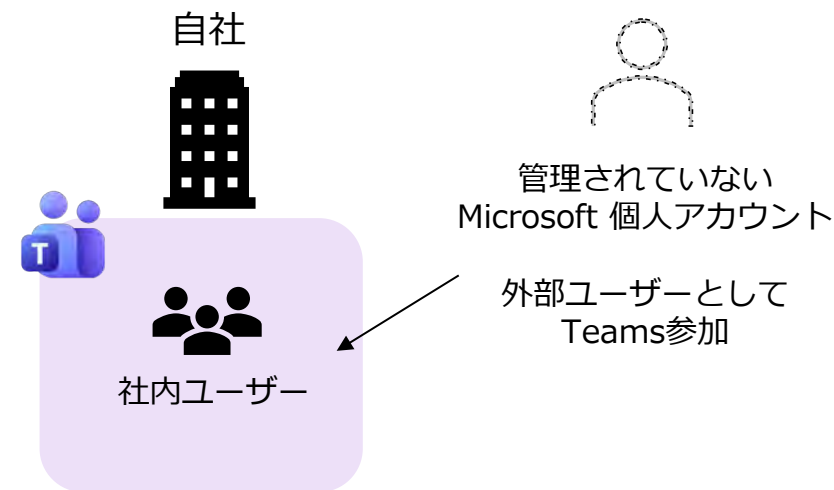
他社テナント所属の外部ユーザー

自組織の Entra ID に登録することなく、他社テナントに所属しているアカウントを用いて、会議招待などを通じて Teams の会議やチャットに参加する外部ユーザーです。



組織管理されていない Microsoft 個人アカウント

どこの組織のテナント管理下にもなく、個人のアカウントとして、会議招待などを通じて一時的に Teams に参加する外部ユーザーです。



次のページより、それぞれのユーザーの特徴や登録方法について詳しく説明します。

2.4. ゲストユーザー

ゲストユーザーは、外部ユーザーを Microsoft Entra ID に「ゲスト」として登録し、自組織の Entra ID 管理配下で Teams や SharePoint の利用を可能にする外部ユーザー形態です。内部ユーザーとは区別されつつも、組織のセキュリティ制御と権限管理の対象として扱われます。

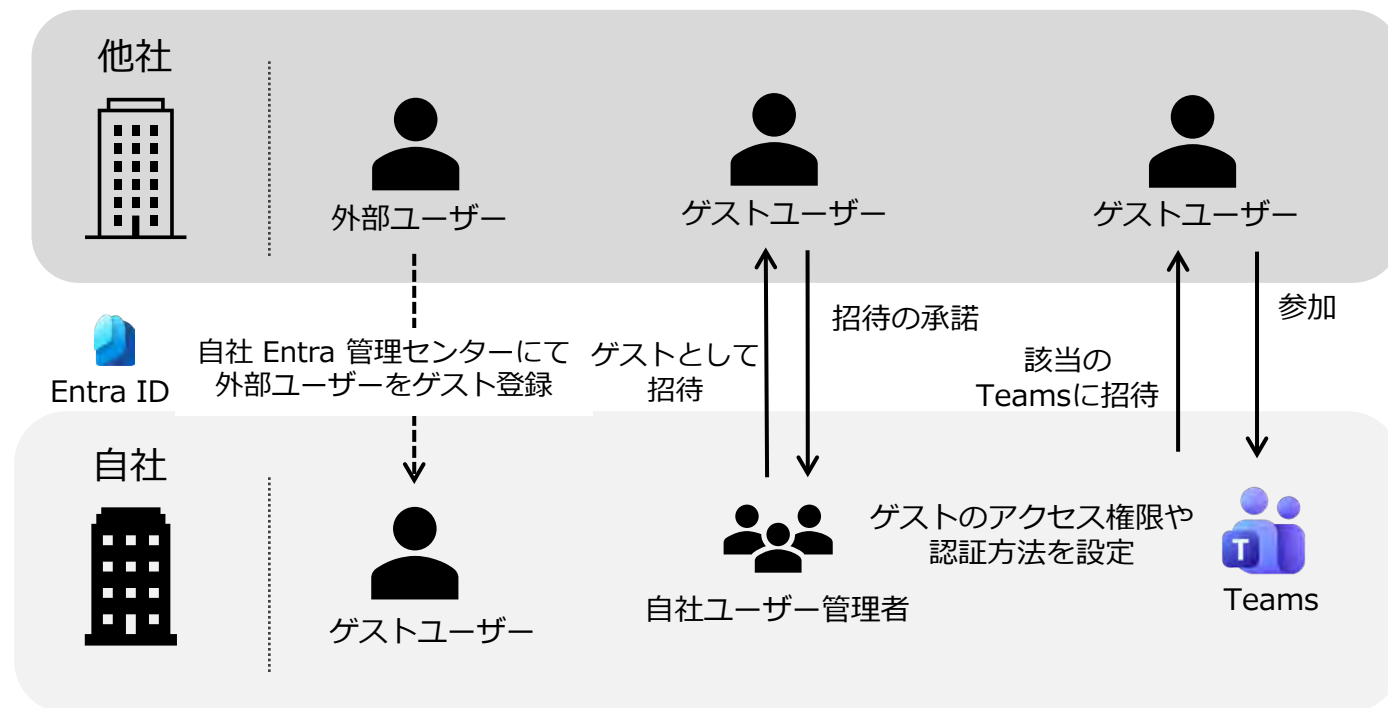
特徴

- 外部ユーザーが自組織テナントに**ゲストユーザー**として登録される
- Teams でのチーム参加、チャンネル投稿、チャット、通話、会議参加が可能である
- Teams や SharePoint、Entra ID のサインインログや監査ログの対象となる
- Teams におけるファイルの保存先である SharePoint や OneDrive によってファイル共有・共同編集が可能である

注意点

- ゲストユーザーは、Teams 上で利用が終了しても、自動削除されないため、利用終了後には削除するなど、棚卸しをする必要がある
- 設計を誤ると、意図しない範囲までアクセス権を与えてしまう可能性がある

イメージ図



2.4. ゲストユーザー

本ページでは、ゲストユーザーにおけるセキュリティ制御とユースケースについて説明します。

セキュリティ制御

セキュリティ制御とは、外部ユーザーを誰まで受け入れ、どの条件で参加させ、参加後に何をさせるかを、複数の設定で段階的に制限・管理する仕組みです。

ゲストユーザーにおけるセキュリティ制御は、外部ユーザーを自組織の Microsoft Entra ID にゲストとして登録し、多要素認証や条件付きアクセスなどの Microsoft Entra ID のセキュリティに加えて、Teams での利用範囲やファイルへのアクセス権限、会議中の挙動までを組織側で主体的に制御することができます。

ユースケース

・プロジェクトベースで外部企業と共同作業を行う場合

外部企業の担当者を必要な期間・範囲に限定して招待し、セキュリティを維持しながら日常的な会話や会議、資料共有などの共同作業を行いたいケース

・継続的なファイル共有・共同編集が必要な場合

資料やファイルを外部ユーザーと安全に共有し、最新版を保ちながら同時編集する必要があるケース

・業務範囲に応じてアクセス権限を明確に制御したい場合

Teams や SharePoint 上の情報資産のうち、業務上必要な範囲のみにアクセスを許可し、組織として情報公開範囲を管理・統制したいケース

項目	詳細
制御できること	<ul style="list-style-type: none">・ 認証強度（多要素認証、認証条件）・ 条件付きアクセス（場所・デバイス・リスク等）・ チーム、チャンネル、ファイル単位のアクセス権管理・ 会議中の動作（ロビー、画面共有、発表者可否など）
制御できないこと	<ul style="list-style-type: none">・ 内部ユーザーと完全に同等な権限（所有者権限など） ※ゲストユーザーには、内部ユーザーと同等の権限は付与できません。

2.4. ゲストユーザー

利用可能な Teams の機能

ゲストユーザーをチームやチャンネル、チャットに招待するための前提条件として、Teams 管理センターにてゲストアクセスを有効にする必要があります。設定手順については[こちら](#)をご確認ください。

項目	可否	詳細
予定された会議の参加	●	Teams または Outlook の会議招待にメールアドレスを追加で参加可能
チャンネル会議への参加	●	ゲストが所属するチームの標準チャンネル会議に参加可能
1:1チャット	●	社内ユーザーと個別にチャット可能
グループチャット	●	複数人（社内+他ゲスト）とのチャットが可能
通話（音声またはビデオ）	●	1:1 通話、グループチャット起点の通話が可能
チャンネル投稿・会話	●	権限のある標準チャンネルで投稿・返信が可能
チームへの参加	●	チームメンバーとして追加されることで参加可能
ファイル共有	●	Teams や SharePoint 経由でファイル閲覧・編集が可能（設定依存）
会議チャット	●	会議中および会議後のチャットを利用可能

2.4. ゲストユーザー

Entra 管理センターにて外部ユーザーを自組織のゲストユーザーとして登録することで、ゲストユーザーをチームやチャンネル、チャットに招待することができます。本ページでは、自組織のゲストユーザーとして登録する方法について説明し、次のページより、新規チーム・チャンネル・チャットへの招待方法を説明します。

ゲスト登録方法

■ 自組織にゲストユーザーを登録

1. Microsoft Entra 管理センター（<https://entra.microsoft.com>）にサインイン
2. [Entra ID]> [ユーザー]
3. [新しいユーザー]> [外部ユーザーの招待]
4. 詳細を設定
5. [確認と招待]> [招待]

登録後は、登録したユーザーに招待メールが届きます。ゲストユーザーは、招待メールが届いたら招待の承諾をします。また、該当のユーザープリンシパル名には「#EXT#」という表記が付きます。これは、自組織のユーザーではなく外部ユーザーであることを示します。

ホーム > ユーザー > 外部ユーザーの招待

外部ユーザーの招待

自分の組織と共同作業するよう外部ユーザーを招待する

基本 • プロパティ 割り当て 確認と招待

Starting December 2025, B2B invitation emails will be sent from your organization's primary domain (e.g., contoso.onmicrosoft.com) instead of Microsoft.com. [Learn More](#)

組織と共同作業を行う新しいゲストユーザーを招待します。ユーザーはメールで招待を受け取り、それを受け入れると共同作業を開始できます。 [詳細情報](#)

ID

メールアドレス

表示名

招待メッセージ

招待メッセージの送信

メッセージ

CC 受信者

招待リダイレクト URL

レビューと招待 戻る 次へ: プロパティ

2.4. ゲストユーザー

新規チーム・チャンネル・チャットへ招待

ゲストユーザーをチーム、チャンネル、チャットへ招待したい場合、Teams アプリにて招待する必要があります。以下では新規チーム、チャンネル、チャットへの招待方法について説明します。

■ゲストを新規チーム・チャンネル・チャットへ招待

1. Teams アプリにて、左側のタブより[チャット]を選択
2. [チャット]の隣にある作成タブより作成したいものを選択
3. 招待したい組織内・ゲストユーザーを招待し、作成

※反映には時間がかかる場合があります。



2.4. ゲストユーザー

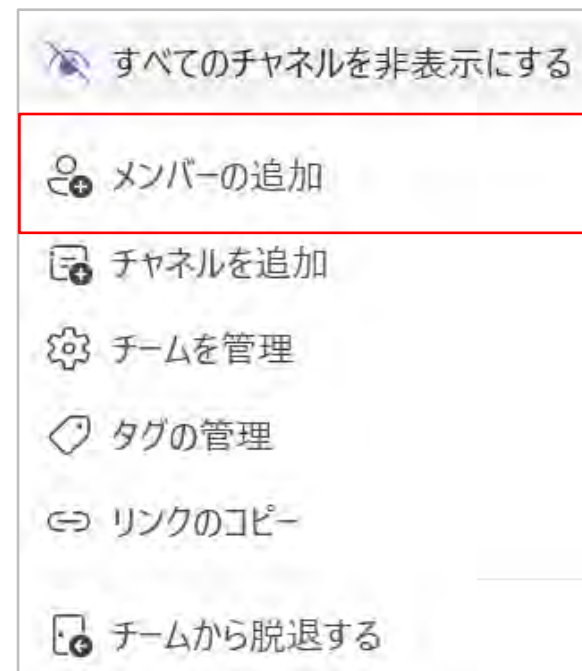
既存チームへの招待方法

既存のチームにゲストユーザーを招待する際は、該当のチームを選択し、招待します。

■ゲストを既存チームへ招待

1. Teams アプリにて、招待したいチームを右クリックし、[メンバーの追加]を選択
2. 登録したゲストユーザーのドメインを入力し、追加

※反映には時間がかかる場合があります。



2.5. 他社テナント所属の外部ユーザー

他社テナント所属の外部ユーザーは、外部ユーザーを Microsoft Entra ID に登録されることなく、会議招待などを通じて Teams の会議やチャットに参加する外部ユーザー形態です。セキュリティ制御であるユーザーの認証や Entra ID 管理は相手先テナント側に委ねられます。

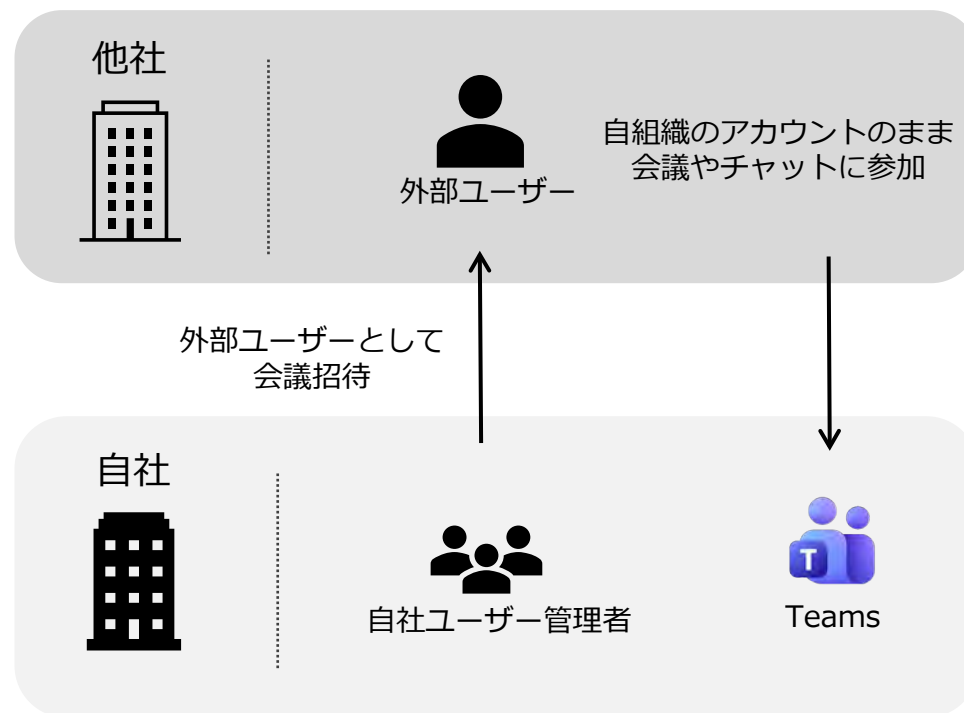
特徴

- 自組織テナントにユーザー登録を行わずに利用できる
- 会議やチャット、通話といった基本的なコミュニケーションができる
- 許可、拒否ドメインで組織単位の制御ができる

注意点

- Teams のチームとチャンネルには参加できない
- SharePoint や OneDrive の ファイル共有は原則できない
- 自組織側で多要素認証や条件付きアクセスを直接適用できない

イメージ図



2.5. 他社テナント所属の外部ユーザー

本ページでは、他社テナント所属の外部ユーザーにおけるセキュリティ制御とユースケースについて説明します。

セキュリティ制御

他社テナント所属の外部ユーザーにおけるセキュリティ制御は、ユーザーの認証や Entra ID 管理を相手先テナントに委ねます。なお、Teams の外部アクセス設定や会議設定によって制御できる「参加や通信を許可するかどうか」と「会議中の挙動」については自組織で行います。

ユースケース

- ・ **自組織にユーザー登録せず、他社担当者との会議や簡易的なやり取りを行う場合**
他社テナントの担当者を自組織へ登録せず、外部アクセスや会議招待を通じて、必要なタイミングで会議や打ち合わせを実施したいケース
- ・ **チャットや通話を中心とした外部連絡を行う場合**
継続的なチーム参加やファイル共有は行わず、外部ユーザーとの連絡手段として、チャットや通話といったコミュニケーション機能のみを利用するケース
- ・ **ファイル共有を伴わない短期・低リスクの外部連携を行いたい場合**
情報資産へのアクセスを許可せず、業務調整や確認といった限定的なやり取りを、短期間かつ低リスクで行いたいケース

項目	詳細
制御できること	<ul style="list-style-type: none">・ 許可またはブロックする外部ドメインの指定・ 会議中の動作（ロビー、画面共有、発表者可否など）
制御できないこと	<ul style="list-style-type: none">・ 多要素認証や条件付きアクセスの直接適用・ チーム、チャンネル、ファイル単位の権限管理・ 外部ユーザーの ID 属性や認証強度の把握

2.5. 他社テナント所属の外部ユーザー

利用可能な Teams の機能

他社テナント所属の外部ユーザーとチャットや通話を始める前提条件として、Teams 管理センターにて外部アクセスが有効になっていること、また、相手先テナント側でも外部アクセスが有効になっている必要があります。
外部アクセスの有効化手順につきましては、[こちら](#)をご確認ください。

項目	可否	詳細
予定された会議の参加	●	会議招待メールのリンクから参加可能
チャンネル会議への参加	×	チームやチャンネルに所属できないため参加不可
1:1チャット	●	メールアドレス指定により 1:1 チャットが可能
グループチャット	●	複数人（社内+他社）を含めたチャットが可能
通話（音声またはビデオ）	●	1:1 通話、グループチャット起点の通話が可能
チャンネル投稿・会話	×	チャンネルに参加できないため投稿不可
チームへの参加	×	ゲスト登録をしないため参加不可
ファイル共有	×	Teams 上のファイル機能を使った共有は不可
会議チャット	●	会議中および会議後のチャットを利用可能

2.5. 他社テナント所属の外部ユーザー

新規チャット・通話を開始する

他社テナント所属の外部ユーザーとは、主に、会議、1:1チャット、グループチャット、通話が可能となります。下記よりそれぞれの方法について紹介します。

■新規チャット（1:1もしくはグループ）を開始する

1. Teams アプリにて、左側のタブより[チャット]を選択
2. [チャット]の隣にある作成タブより作成したいものを選択
3. チャットを行いたいメンバーを招待

※反映には時間がかかる場合があります。

■通話（1:1もしくはグループ通話）を開始する

1. グループの場合、作成したグループチャットにて、音声通話またはビデオ通話を開始
2. 個人の場合は、個人のチャットにて、音声通話またはビデオ通話を開始



2.6. 組織管理されていない Microsoft 個人アカウント

組織管理されていない Microsoft 個人アカウントとは、自組織や他社の Microsoft Entra ID で管理されていない個人のアカウントとして、Teams に参加する外部ユーザーを指します。このユーザーには、組織のセキュリティ制御は適用されず、会議参加を中心とした例外的な利用形態として扱われます。

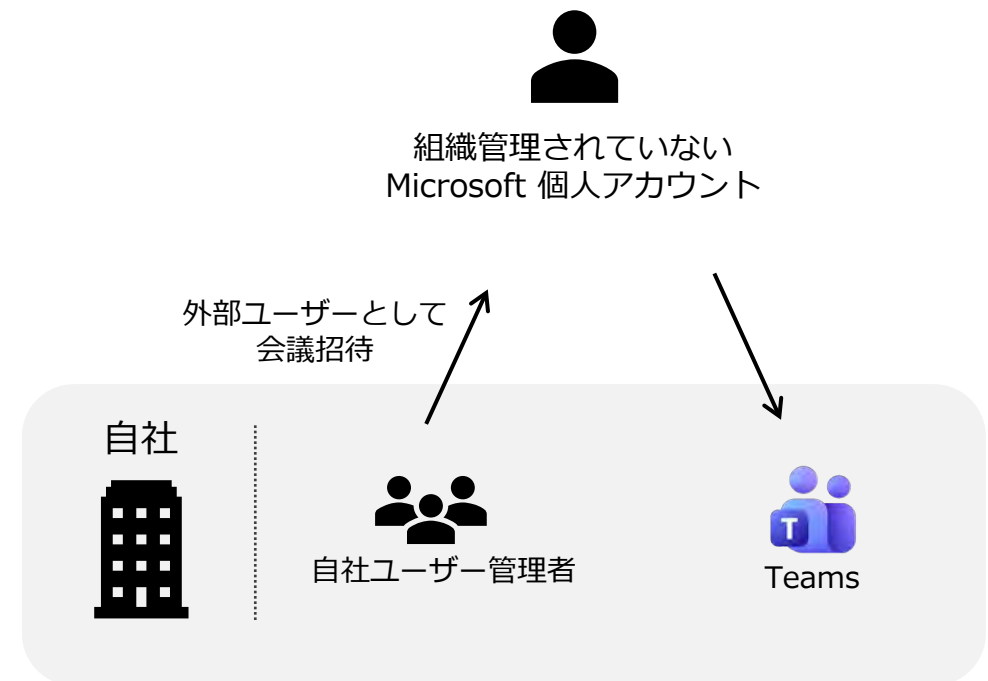
特徴

- ・組織アカウントを持たなくても参加できる
- ・参加までの手続きが最小限で済む
- ・導入やオンボーディングが不要である

注意点

- ・認証強度やデバイス状態が不明で、セキュリティリスクが最も高いため、単発・一時利用が前提となる
- ・ユーザー単位の権限管理ができない
- ・チームやチャンネルへの参加、ファイル共有はできない

イメージ図



2.6. 組織管理されていない Microsoft 個人アカウント

本ページでは、組織管理されていない Microsoft 個人アカウントにおけるセキュリティ制御とユースケースについて説明します。

セキュリティ制御

管理されていない Microsoft 個人アカウントのセキュリティ制御は、外部ユーザーの ID や認証を自組織では管理せず、Teams の会議設定を用いて匿名参加の可否や会議中の挙動（ロビー、画面共有、チャットなど）を制御することができます。

項目	詳細
制御できること	<ul style="list-style-type: none">・会議への参加可否（匿名参加の許可、禁止）・会議中の動作制御（ロビー、画面共有、チャット可否）
制御できないこと	<ul style="list-style-type: none">・多要素認証や条件付きアクセスの直接適用・チーム、チャンネル、ファイル単位の権限管理・外部ユーザーの ID 属性や認証強度の把握

ユースケース

・単発の商談や説明会などの場合

企業テナントやゲスト登録を前提とせず、会議リンクから誰でも参加できる形で、短時間または一度きりの商談や説明会を実施するケース

・初回打ち合わせや一時的な会議などの場合

相手の IT 環境や所属組織が未確定な段階でも、事前準備なく会議に参加してもらい、関係構築の初期コミュニケーションを行うケース

・即時性を優先し、ゲスト登録を避けたい場合

ユーザー登録や承認フローに時間をかけず、スピードを重視してその場限りの会議参加を可能にしたいケース

2.6. 組織管理されていない Microsoft 個人アカウント

利用可能な Teams の機能

組織管理されていない個人アカウントと会議を始める前提条件として、Teams 管理センターにて外部アクセスの管理されていない個人アカウントとのチャットや会議を行う設定が有効になっている必要があります。有効化手順につきましては、[こちら](#)をご確認ください。

ユーザー	可否	詳細
予定された会議の参加	●	招待メールの会議リンクから参加可能
チャンネル会議への参加	×	チームやチャンネルへの所属は不可
1:1チャット	●	Microsoft アカウント同士での 1:1 チャットが可能
グループチャット	●	社内+個人 Microsoft アカウントを含むグループで可能
通話（音声またはビデオ）	●	1:1 通話やグループチャット起点の通話が可能
チャンネル投稿・会話	×	チャンネルに参加できないため不可
チームへの参加	×	ゲスト登録をしないため参加不可
ファイル共有	×	Teams 上のファイル機能を使った共有は不可
会議チャット	●	会議中および会議後のチャットの利用は可能

2.7. 各ユーザーの機能比較表

ゲストユーザー、他社テナント所属の外部ユーザー、組織管理されていない Microsoft 個人アカウントそれぞれの機能を一覧で比較します。会社の運用方針によって、各ユーザーを使い分ける必要があるため、以下の表より必要な権限を確認します。

項目	ゲストユーザー	他社テナント所属の外部ユーザー	組織管理されていない Microsoft 個人アカウント
予定された会議の参加	●	●	●
チャンネル会議への参加	●	×	×
1:1チャット	●	●	●
グループチャット	●	●	●
通話（音声またはビデオ）	●	●	●
チャンネル投稿・会話	●	×	×
チームへの参加	●	×	×
ファイル共有	●	×	×
会議チャット	●	●	●

2.8. 各ユーザーのユースケース比較表

ゲストユーザー、他社テナント所属の外部ユーザー、組織管理されていない Microsoft 個人アカウントそれぞれのユーザーがどのような場合に適しているかを以下の表にて説明します。

項目	ゲストユーザー	他社テナント所属の外部ユーザー	組織管理されていない Microsoft 個人アカウント
適しているケース	外部ユーザーを業務メンバーとして扱う必要があるケース	外部ユーザーと連絡・調整だけを行いたいケース	相手の IT 環境が不明でもすぐに会議を実施したいケース
想定される業務	委託業務、共同プロジェクト、継続支援	取引先との定例連絡、ミーティング	初回商談、説明会、問い合わせ対応
利用期間	中～長期	短～中期	単発・一時利用
情報の扱い	業務に必要な情報資産の共有を可能とする	情報資産は共有不可とする	情報資産は共有不可とする
ユーザーの管理方針	自組織が責任を持って管理を行う	管理は相手組織に委ねる	管理しない

ポイント

ユーザーの選択において、外部のユーザーとどれぐらいの期間業務を行うか、どのように情報やユーザーを管理したいかが重要となります。



3. セキュリティ設定

3.1. セキュリティ設定の必要権限

セキュリティ設定は、Entra 管理センター、Teams 管理センター、Teams アプリ、SharePoint 管理センターにて行うことができます。なお、各セキュリティ設定を行う前提条件として、ユーザーの操作権限が必要となります。そのため、各セキュリティ設定場所で必要となる権限について説明いたします。

Entra 管理センター

・ **グローバル管理者権限**

Teams 管理センター

・ **Teams 管理者**
※上位の権限であるグローバル管理者権限でも操作は可能となります。

Teams アプリ

・ **会議の主催者**（一般ユーザー）

SharePoint 管理センター

・ **SharePoint 管理者**
※上位の権限であるグローバル管理者権限でも操作は可能となります。

次のページより、各設定について詳細を説明します。

3.2. セキュリティ設定の概要

各セキュリティ設定の詳細、考えるポイントや注意点について説明します。

Entra 管理センター

外部コラボレーション

詳細：

- ・ゲストユーザーのアクセス制限
- ・ゲスト招待の制限
- ・外部ユーザーの脱退設定
- ・コラボレーションの制限

考えるポイント：

- ✓ 外部ユーザーの受け入れ可否
- ✓ 招待を誰に許可するか

注意点：

- ✓ テナント全体に反映される

条件付きアクセス

詳細：

- ・多要素認証の要求
- ・デバイス要件等

考えるポイント：

- ✓ 認証強度レベル
- ✓ 社内ユーザーとの条件

注意点：

- ✓ 設定ミスにより、正当なユーザーもサインイン不可となる
- ✓ Microsoft Entra ID P1以上のライセンスが必要

Teams 管理センター

ゲストアクセス

詳細：

- ・通話の設定
- ・ミーティング、メッセージングの設定

考えるポイント：

- ✓ 許可する機能
- ✓ 内部ユーザーとの差別化

注意点：

- ✓ ゲストアクセスを有効化しないと利用不可
- ✓ 設定のレベル

外部アクセス

詳細：

- ・外部ドメインの許可またはブロック
- ・組織管理されていない外部ユーザーとのチャット、会議の許可またはブロック
- ・ポリシー設定

考えるポイント：

- ✓ 他社テナントとの通信可否

注意点：

- ✓ 相手テナント側の設定に挙動が左右される
- ✓ ユーザー管理や権限設定はできない

会議設定

詳細：

- ・参加者の設定等

考えるポイント：

- ✓ 外部参加者や匿名ユーザーを会議に参加させるか

注意点：

- ✓ 全会議に影響
- ✓ 匿名参加可能にするとなりすましのリスクが高まる

3.2. セキュリティ設定の概要

Teams アプリ

会議オプション

詳細：

- ・待機室の利用可否等

考えるポイント：

- ✓ 会議中に外部参加者がどこまで操作できるか
- ✓ 発表者や画面共有の制御ルールをどうするか

注意点：

- ✓ 会議ポリシーをユーザー単位で適切に割り当てないと、会議中の挙動が参加者ごとに不統一になる

SharePoint 管理センター

共有

詳細：

- ・ SharePoint、OneDriveの外部共有の許可レベル
- ・ ファイルとフォルダーの許可レベル等

考えるポイント：

- ✓ 外部ユーザーにファイル共有を許可するか
- ✓ 閲覧のみか編集可かなど、共有レベルをどうするか

注意点：

- ✓ Teams のファイル共有は SharePoint 設定に依存する
- ✓ 共有範囲を広げすぎると、情報漏えいリスクが高まる

3.3. Entra 管理センターにおけるテナント設定

Entra 管理センターでは、外部コラボレーションによって外部ユーザーをゲストとして招待できるかを制御し、条件付きアクセス（※Microsoft Entra ID P1以上のライセンス必須）によって、そのユーザーがどの認証条件を満たした場合に Teams を含む Microsoft 365 にサインインできるかを制御します。

外部コラボレーション

ここでは、外部ユーザーをゲストとして招待してよいか、誰が招待できるか、どの外部ドメインを許可またはブロックするかといった、外部ユーザーを組織に**入れるかどうか**を制御します。

なお、外部コラボレーションの設定はテナント全体に影響するため、個別の利用シーンではなく、会社全体の運用方針やセキュリティポリシーに基づいて慎重に設定する必要があります。

■流れ

1. Entra 管理センターにサインイン
2. [Entra ID]より[External Identities]をクリック
3. [外部コラボレーションの設定]より各項目設定

External Identities | 外部コラボレーションの設定

検索

保存 破棄

概要

テナント間アクセス設定

すべての ID プロバイダー

外部コラボレーションの設定

問題の診断と解決

セルフサービス サインアップ

カスタムのユーザー属性

すべての API コネクタ

カスタム認証拡張機能

ユーザー フロー

サブスクリプション

リンクされたサブスクリプション

ライフサイクル管理

利用規約

ゲストのメール ワンタイム パスコードが、すべての ID プロバイダーに移動されました。 →

ゲストユーザーのアクセス

ゲストユーザーのアクセス制限 ⓘ

詳細情報

ゲストユーザーは、メンバーと同じアクセス権を持ちます (制限が最も少ない)

ゲストユーザーは、ディレクトリ オブジェクトのプロパティとメンバーシップへのアクセスが制限されます

ゲストユーザーのアクセスは、各自のディレクトリ オブジェクトのプロパティとメンバーシップに制限されます (最も制限が多い)

ゲスト招待の設定

ゲスト招待の制限 ⓘ

詳細情報

ゲストと非管理者を含む組織内のすべてのユーザーがゲストユーザーを招待できる (最も包括的)

メンバー アクセス許可を持つゲストを含むメンバー ユーザーと特定の管理者ロールに割り当てられたユーザーがゲストユーザーを招待できる

特定の管理者ロールに割り当てられているユーザーのみがゲストユーザーを招待できる

管理者を含む組織内のすべてのユーザーがゲストユーザーを招待できない (最も制限的)

ユーザー フローによるゲスト セルフサービスのサインアップを有効にする ⓘ

3.3. Entra 管理センターにおけるテナント設定

条件付きアクセス

多要素認証の必須化、アクセス元の場所、利用デバイス、サインインリスクなどを条件として定義し、条件を満たさない場合はサインイン自体をブロックします。

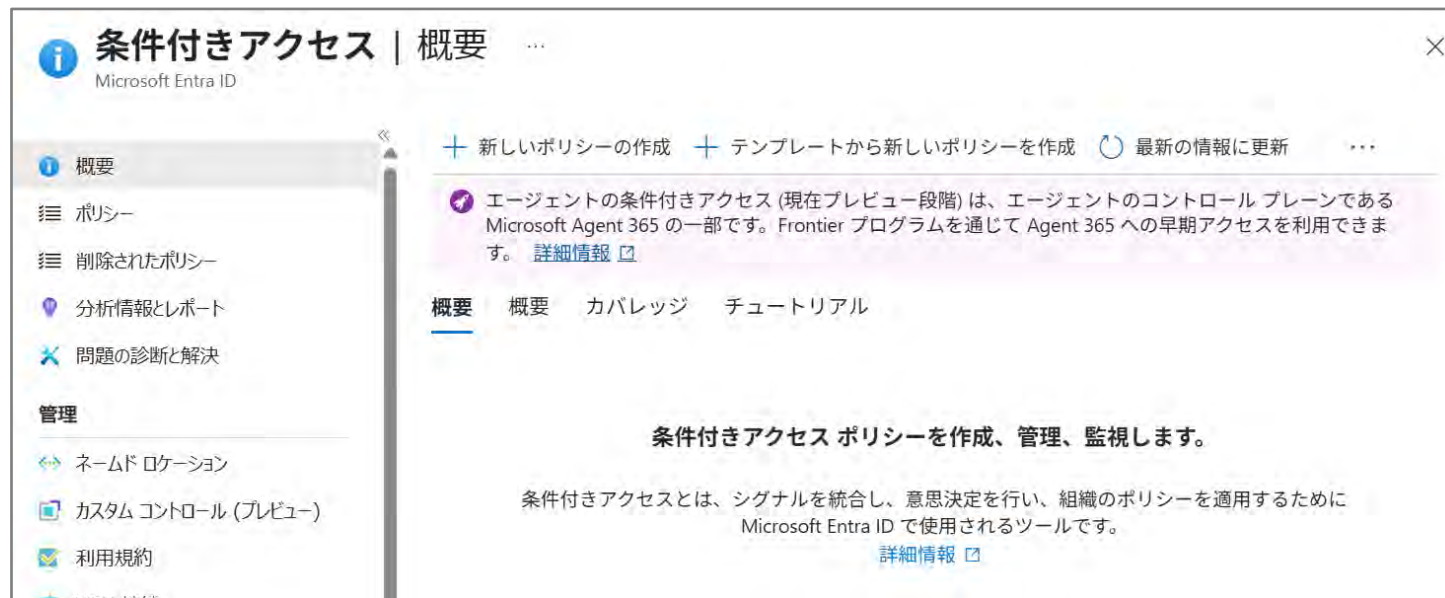
■必要なライセンス

Microsoft Entra ID P1 以上のライセンス

Microsoft Entra ID P1 以上のライセンスを利用しない場合は、外部コラボレーションの設定により、外部ユーザーを招待できる範囲や受け入れ条件を制御することが、Entra ID 管理における基本的な統制手段となります。

■流れ

1. Entra 管理センターにサインイン
2. [Entra ID]より[条件付きアクセス]をクリック
3. [新しいポリシーの作成]より設定



3.4. Teams 管理センターにおけるテナント設定

外部ユーザーの Teams の権限設定は Teams 管理センターから行います。本ページでは、ゲストアクセス・外部アクセスの各設定について説明します。ここでの設定は前提条件となり、無効化されている場合は、ゲストユーザーとの個別の会議設定やユーザー操作は行うことができませんのでご注意ください。

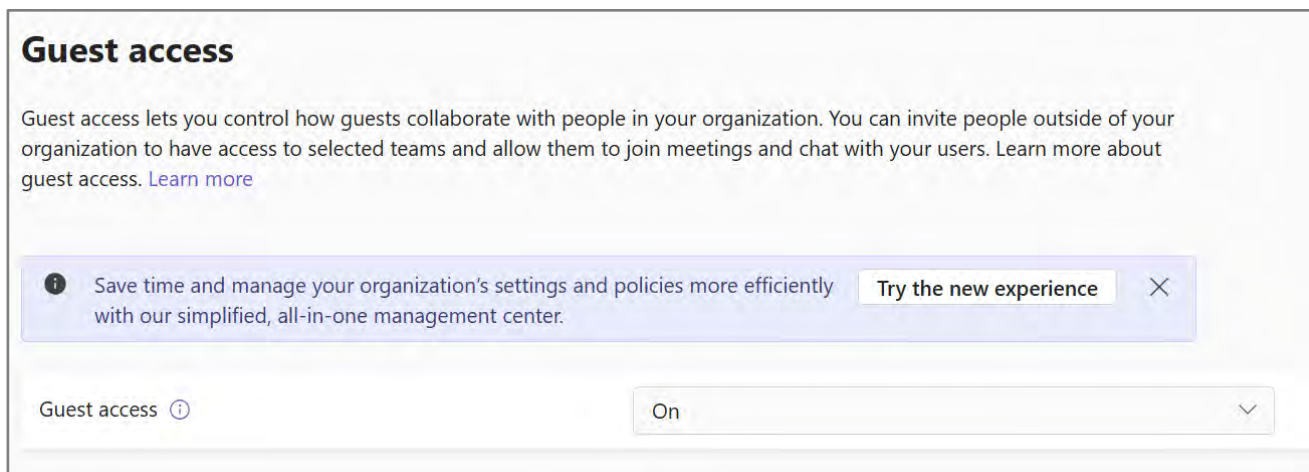
ゲストアクセス

ゲストアクセスは、Entra ID に登録されたゲストユーザーが Teams をどこまで利用できるかを制御するための設定です。Teams 管理センターにてゲストアクセスをオンにした場合、**通話・会議・メッセージング**において、ゲストユーザーの挙動を制御することができます。各項目より、詳細な権限の設定を行うことができます。

■流れ

1. Teams 管理センター
(<https://admin.teams.microsoft.com/>) にサインイン
2. [External collaboration] (外部連携) より[Guest access] (ゲストアクセス) をクリック

- [Guest access]を[on]にした場合
[calling] (通話)、[Meeting] (会議)、および [Messaging] (メッセージング) において、ゲストに何を許可する必要があるかに応じてオンに設定します。
- [Guest access]を[off]にした場合
詳細設定は不要です。なお、オフにした場合はEntra ID に登録されたゲストユーザーは Teams を一切利用できなくなり、既存のゲストユーザーにも影響を受けます。



※ Microsoft 社の仕様上、英語表記となります。

3.4. Teams 管理センターにおけるテナント設定

外部アクセス

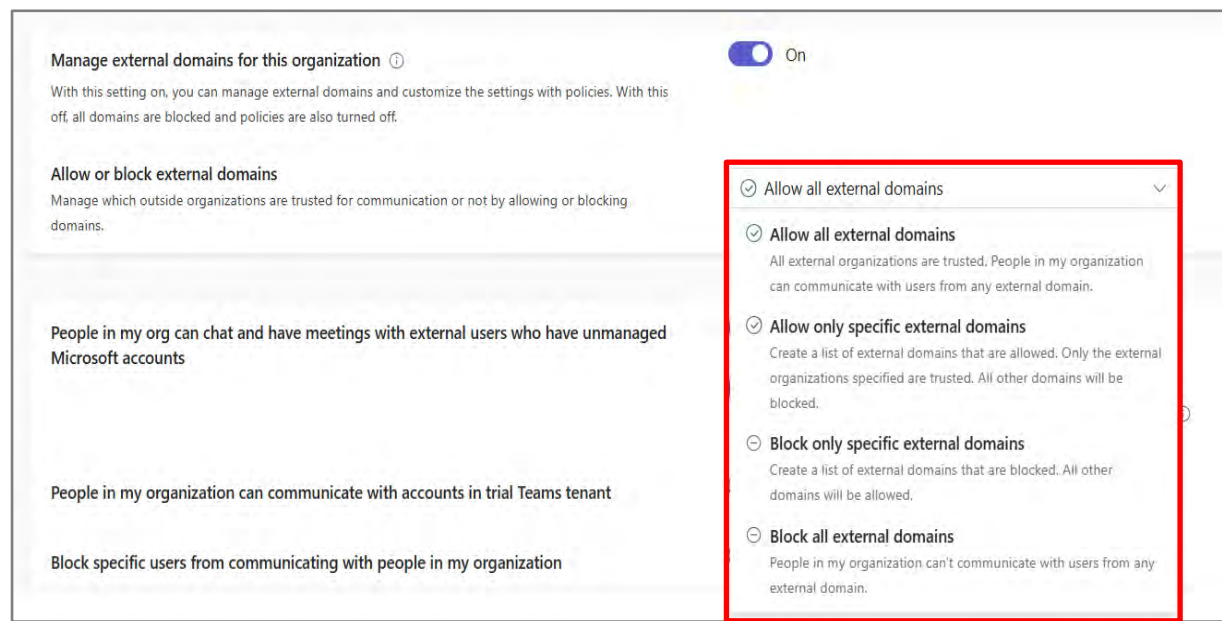
外部アクセスは、他社テナント所属の外部ユーザーと、チャットや通話、会議などの通信を許可するかどうかを制御する設定です。

■ 他社テナントのユーザー管理

他社テナント所属の外部ユーザーとの通信を許可するか、特定のドメインを許可またはブロックするか、すべてブロックするかを選択できます。特定のドメインについては、選択肢をクリックした際に、詳細を設定することが可能となります。

■ 流れ

1. Teams 管理センターにサインイン
2. [External collaboration] (外部連携) より[External access] (外部アクセス) をクリック
3. [Manage external domains for this organization] (この組織の外部ドメインを管理する) を[on]にした場合、以下より詳細を選択
 - Allow all external domains (すべての外部ドメインを許可する)
 - Allow only specific external domains (特定の外部ドメインのみを許可する)
 - Block only specific external domains (特定の外部ドメインをブロックする)
 - Block all external domains (すべての外部ドメインをブロックする)



※ Microsoft 社の仕様上、英語表記となります。

3.4. Teams 管理センターにおけるテナント設定

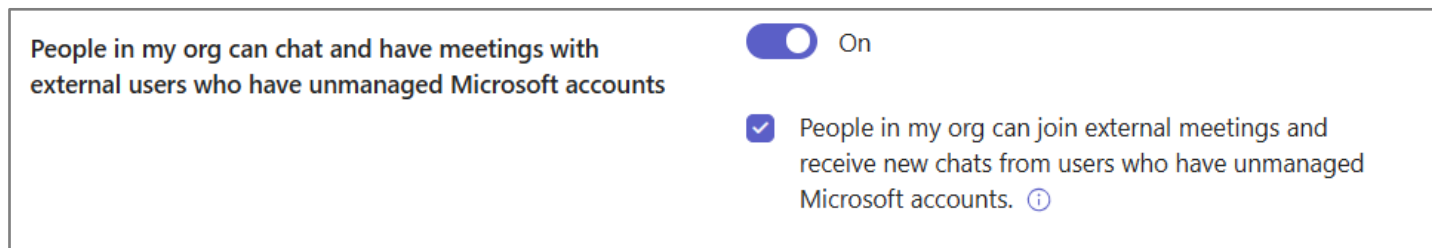
外部アクセス

組織管理されていない Microsoft 個人アカウントとのチャットや会議の許可・ブロックを行います。ここでは、なりすましなどのセキュリティリスクを防止することができます。

■ 流れ

1. Teams 管理センターにサインイン
2. [External collaboration] (外部連携) より [External access] (外部アクセス) をクリック
3. [People in my org can chat and have meetings with external users who have unmanaged Microsoft accounts] (私の組織のメンバーは、管理されていない Microsoft アカウントを持つ外部ユーザーとチャットや会議を行うことができます。) を [on]もしくは[off]を選択

※既定の設定では「オン」になっています。



※ Microsoft 社の仕様上、英語表記となります。

3.4. Teams 管理センターにおけるテナント設定

Teams 管理センターで設定できる会議設定は、組織として匿名ユーザーを含む Teams 会議を開催してよいかの前提条件を、テナント全体に適用することができます。

会議設定

会議設定では、匿名ユーザーの会議参加の制限を設定することができます。

■ 流れ

1. Teams 管理センターにサインイン
2. [Meetings] (会議) より[Meeting settings] (会議設定) をクリック
3. [Anonymous users can join a meeting] (匿名ユーザーも会議に参加できます) を[on]または[off]に設定。
また、[Anonymous users can interact with apps in meetings] (匿名ユーザーは会議でアプリとやり取りできます) も同様に設定。

■ 匿名ユーザー

匿名ユーザーとは、以下のユーザーを指します。

- 職場または学校アカウントを使用して Teams にログインしていないユーザー
- 外部アクセスで信頼設定が行われていない組織、もしくは組織単位では信頼していない外部組織から参加するユーザー

Meeting settings

Meeting settings let you customize meeting invitations, set up cross-cloud relationships, and manage network settings for all Teams meetings in your organization. [Learn more about meeting settings](#)

Save time and manage your organization's settings and policies more efficiently with our simplified, all-in-one management center. [Try the new experience](#) ×

Participants

Anonymous users can join a meeting ⓘ On

Find related settings at [Meetings > Meeting settings](#)

Anonymous users can interact with apps in meetings On

※ Microsoft 社の仕様上、英語表記となります。

3.5. Teams の会議オプション

Teams アプリで設定できる会議オプションは、待機室や発表者、画面共有など、会議ごとに主催者が会議中の挙動を調整するための設定ができます。

会議オプション

Teams の会議オプションは、Teams にて、外部ユーザーやゲストユーザーが会議に参加した際の具体的な挙動を制御する設定です。テナント設定で外部参加が許可されている場合に、ロビーからの参加許可ができる人など、会議開催における詳細設定ができます。

■流れ

1. Teams を開く
 2. [カレンダー]> [新規]> [チャンネル]をクリック
 3. [オプション]> [その他のオプション]をクリック
 4. [会議のオプション]にて詳細設定が可能
- ※[その他のオプション]が表示されないものについては、詳細設定は不可

会議のオプション

- 会議へのアクセス
- ロール
- 運用ツール
- 参加状況
- レコーディングと文字起こし
- Copilot とその他の AI

会議へのアクセス

ロビーを迂回するユーザー
[全員] が選択されている場合でも、組織のポリシーにより、特定の参加者は、組織のメンバーまたは信頼された組織が参加するまでロビーで待機する必要がある場合があります。これには、アカウントなしで参加するユーザー、信頼されていない組織のユーザー、ダイヤルインしているユーザーが含まれます。

組織内のユーザーおよびゲスト

ダイヤルインしている人はロビーをバイパスできる

ロビーからの参加を許可できる人

開催者、共同開催者、発表者

参加画面に会議情報を表示する
タイトルと開始時刻、参加した他のユーザー数、開催者のプレゼンスなど、会議の詳細を表示します。

ロビーを通過できるユーザー

ダイヤルインしているユーザーの参加または退出を通知する

土曜日の参加者に、参加前に自身の情報を確認してもらう

戻る

3.6. SharePoint 管理センターにおける外部・ファイル共有設定

Teams で扱うファイルは、SharePoint または OneDrive に保存されます。そのため、Teams でのファイル共有や共同編集におけるゲストユーザーのアクセス範囲は、SharePoint 管理センターで設定・管理します。Teams でゲストユーザーがファイルにアクセスできるかどうかは、SharePoint または OneDrive の外部共有設定に依存します。

外部共有

外部共有の設定では、ゲストユーザーに対して、SharePoint や OneDrive に基づくファイルやフォルダーを共有できる範囲をテナント全体で設定することができます。

■ 流れ

1. SharePoint 管理センターにサインイン
2. [ポリシー]より[共有]をクリック
3. [外部共有]より、SharePoint や OneDrive それぞれの共有権限のレベルを選択

※外部共有の詳細設定にて、その他の詳細項目設定可能

外部共有

コンテンツを共有できる相手:

SharePoint OneDrive

最も制限が少ない

最も制限が多い

すべてのユーザー
ユーザーは、サインインが必要ないリンクを使用してファイルとフォルダーを共有できます。

新規および既存のゲスト
ゲストは、サインインするか、認証コードを入力する必要があります。

既存のゲスト
既に組織のディレクトリ内にあるゲストのみです。

自分の組織内のユーザーのみ
外部共有は許可されていません。

個々のサイトと OneDrive の共有をさらに制限することができます。 [詳細情報](#)

外部共有の詳細設定 ▾

- ドメインごとに外部共有を制限する
- 特定のセキュリティグループのユーザーのみに外部共有を許可する
- ゲストが所有していないアイテムを共有できるようにする
- サイトまたは OneDrive へのゲストアクセスは、この日数が経過すると自動的に有効期限切れになります [詳細情報](#) 3/6
- 確認コードを使用するユーザーは、この日数の後に再認証を行う必要があります [詳細情報](#) ① 3/6

3.6. SharePoint 管理センターにおける外部・ファイル共有設定

ファイル共有

ファイルとフォルダーのリンクの設定では、ユーザーが、SharePoint や OneDrive に保存されているファイルやフォルダーを共有する際に、既定で選択されるリンクの権限を設定することができます。

また、リンクにおいて、表示 or 編集のどちらを既定のアクセス権にするかについても設定することができます。

■流れ

1. SharePoint 管理センターにサインイン
2. [ポリシー]より[共有]をクリック
3. [外部共有]より、[ファイルとフォルダーのリンク]
[その他の設定]にて権限を選択

ファイルとフォルダーのリンク

SharePoint と OneDrive でユーザーがファイルとフォルダーを共有するときに、既定で選択されるリンクの種類を選択します。

- 特定のユーザー (ユーザーが指定したユーザーのみ)
- 自分の組織内のユーザーのみ
- リンクを知っているユーザー

共有リンクに既定で選択されるアクセス許可を選択してください。

- 表示
- 編集

その他の設定

- 所有者に OneDrive ファイルを表示したユーザーの名前を表示する
- SharePoint でファイルまたはページを参照したユーザーの名前を表示するかどうかをサイトの所有者が選択できます
- ファイルとフォルダーを共有する場合に短いリンクを使用する



4. 想定されるトラブルと解決策

4.1. 想定されるトラブルと解決策

ゲストユーザーや外部ユーザーとの連携によって想定されるトラブルについて、考えられる原因とその解決策を紹介します。

ゲストトラブル① 招待メールが届かない

■ 状況

Entra 管理センターにてゲスト登録を行ったが、登録したゲストユーザーに招待メールが届かない

■ 考えられる原因

- ・送付先の迷惑メール対策により招待メールがブロック/隔離されている
- ・ゲスト登録をする側が招待を完了していない

■ 解決策

- ・Entra ID 管理画面で招待の状態を確認
- ・招待メールの再送 or 招待 URL を送付
- ・ゲストユーザー側で、迷惑メールやゴミ箱を確認

ゲストトラブル② ゲストがチームやファイルに アクセスできない

■ 状況

ゲストユーザーが該当のチームやファイルにアクセスすることができない

■ 考えられる原因

- ・ゲスト登録はされているが、Teams チームに追加されていない
- ・SharePoint の外部共有が制限されている

■ 解決策

- ・ゲストが対象の Teams チームに追加されているかを確認
- ・SharePoint 管理センターにて外部共有の権限を確認

外部トラブル① 外部ユーザーがチャットや会議に参加できない

■ 状況

外部ユーザーが招待されたチャットや会議に入ろうとしたが、参加することが出来ない

■ 考えられる原因

- ・組織側で外部アクセスがブロックされている
- ・外部アクセスは許可されているが、機能単位の制限がかかっている

■ 解決策

- Teams 管理センター → [External access] より、以下を確認
- ・外部ドメインは許可されているか
- ・その他関連する項目が許可されているか