IT資格道場

MS-700 学習用テキスト

予備知識ゼロから合格ラインへ —— 読んで理解する1冊目

無料サンプル(第1章まで)

MS-700 出題範囲(Skills measured)2026-10-27版 準拠
2026年11月版

SAMPLE

© IT資格道場｜無料サンプル｜転載・再配布・AI学習利用禁止

ご利用にあたって

- このテキストは「IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルも著作物です。転載・改変しての再配布・二次販売はできません。
- AI モデルの学習データとしてのご利用(学習目的の入力・データセット化を含む)はできません。
- 製品版(学習用テキスト・頻出度別ノート・暗記用ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

SAMPLE

目次

第1章 Configure and manage a Teams environment [1.1.1/1.1.2/1.1.3/1.1.4/1.2.1/1.2.2/1.2.3/1.2.4/1.2.5/1.2.6/1.2.7/1.2.8/1.2.9/1.2.10/1.3.1/1.3.2/1.3.3/1.3.4/1

- 音声・ビデオ・会議・イベントの帯域幅を見積もる [1.1.1]
- Teams Network planner で影響を分析する [1.1.2]
- Teams が使うポートとプロトコル [1.1.3]
- ネットワークの準備状況を評価するツール [1.1.4]
- セキュリティとコンプライアンス機能のライセンス [1.2.1]
- セキュリティとコンプライアンスのアラート ポリシー [1.2.2]
- Teams 管理者ロールの選択 [1.2.3]
- Defender for Office 365 の脅威ポリシー [1.2.4]
- 保持ポリシー [1.2.5]
- 秘密度ラベルと発行ポリシー [1.2.6]
- Purview DLP ポリシー [1.2.7]
- Teams の条件付きアクセス [1.2.8]
- Purview 情報バリア [1.2.9]
- コミュニケーション コンプライアンスとインサイダー リスク管理 [1.2.10]
- ライフサイクル管理のライセンス [1.3.1]
- Teams のコンテンツの保存先 [1.3.2]
- 更新ポリシー [1.3.3]
- ポリシー パッケージ [1.3.4]
- ポリシーの割り当て [1.3.5]
- Microsoft 365 グループの作成の制限 [1.3.6]
- Microsoft 365 グループの有効期限ポリシー [1.3.7]
- グループの名前付けポリシーとブロックされた単語 [1.3.8]
- チームのアーカイブ、削除、アーカイブ解除 [1.3.9]
- 削除した Microsoft 365 グループの復元 [1.3.10]
- Entra のアクセス レビューを使う場面 [1.3.11]
- PowerShell と Microsoft Graph での操作 [1.3.12]
- 外部コラボレーションのライセンス [1.4.1]
- SharePoint と OneDrive の外部共有設定 [1.4.2]
- Teams 管理センターの外部アクセス [1.4.3]
- 特定のユーザーとグループのドメイン別の外部アクセス [1.4.4]
- Entra ID の外部コラボレーション設定 [1.4.5]
- 4つの管理センターでのゲスト アクセスと共有 [1.4.6]
- 特定のチームへのゲスト アクセスを制御する [1.4.7]
- チームとテナントからゲストを削除する [1.4.8]
- 共有チャネルの外部アクセス [1.4.9]
- B2B direct connect のクロステナント アクセス設定 [1.4.10]
- マルチテナント組織（MTO） [1.4.11]
- Teams Phone とリソース アカウントのライセンス [1.5.1]

SAMPLE

Teams デバイスのライセンス [1.5.2]
Teams デバイスの構成プロファイル [1.5.3]
Teams Rooms のアカウントとシステム [1.5.4]
デバイスの設定とファームウェア [1.5.5]
Teams デバイス タグ [1.5.6]
新しいデバイスのリモート サインイン [1.5.7]
VDI 用の Teams [1.5.8]

サンプルはここまでです

SAMPLE

> **このテキストの位置づけ**: 3 点セットの本編。**これだけで問題が解けるようになる**ことが目標で、設定名・既定値・上限の数字・権限を持つ人を、合格ラインの深さで扱う。
>
> 進め方: ① 学習用を読む → ② 頻出度別で解き方を掴む → ③ 問題演習で腕試し → ④ 頻出度別に戻って再確認(試験直前もここ)。暗記用は空き時間や用語の再確認に使う。

MS-700(Microsoft 365 Certified: Teams Administrator Associate) は、Microsoft Teams の環境を構成し、チーム・会議・電話を管理し、監視して障害を切り分ける力を問う試験です。この本文は公式の学習ガイドの 4 つの領域に沿って、章を分けています。

- 第1章: Teams 環境の構成と管理
- 第2章: チーム、チャネル、チャット、アプリの管理
- 第3章: 会議と通話の管理
- 第4章: Teams の監視、レポート、トラブルシューティング

SAMPLE

第1章 Configure and manage a Teams environment [1.1.1/1.1.2/1.1.3/1.1.4/1.2.1/1.2.2/1.2.3/1.2.4/1.2.5/1.2.6/1.2.7/1.2.8/1.

音声・ビデオ・会議・イベントの帯域幅を見積もる [1.1.1]

帯域幅の値はユーザー単位ではなく、エンドポイント単位です。PC とモバイルの両方で会議に入れば2エンドポイントです。単位は kbps で、上り/下りの順に書きます。[^c1-1]

種類	最小	推奨	最高
音声（1対1も会議も同じ）	10/10	58/58	76/76
ビデオ 1対1	150/150	1,500/1,500	4,000/4,000
ビデオ会議	150/200	2,500/4,000	4,000/4,000
画面共有 1対1	200/200	1,500/1,500	4,000/4,000
画面共有 会議	250/250	2,500/2,500	4,000/4,000

見積もりは「同時に使うエンドポイント数 × 推奨値」です。40人が同時にビデオ会議に入ると、上り 100 Mbps、下り 160 Mbps になります。音声だけの100エンドポイントなら 5.8 Mbps。帯域が足りない時、Teams は映像より音声の品質を優先します。

帯域	品質
制限なし	最大 1080p、ビデオと共有は最大 30 fps。HD は 1.5 Mbps 未満で出せる
最小	ビデオ通話は最大 240p、画面共有は適応 1.875〜7.5 fps、大ギャラリーは最大 540p

イベントは eCDN がない場合、拠点ごとに視聴者1人あたり約 2 Mbps（1080p なら 3 Mbps）で見積もります。500人の拠点なら 1,000 Mbps（1080p は 1,500 Mbps）です。人数の多い拠点では、eCDN を入れて帯域を抑えます。会議側の抑制手段は2つ。会議ポリシーの Media rate (Kbps) とビデオの制限です。Media rate はユーザー単位で、最小は 30 Kbps、上りと下りに同じ値で効きます。Teams の Web クライアントには効きません。

組織全体の品質と信頼性は Call Quality Dashboard（CQD）の集計で見ます。個別ユーザーの調査は、CQD ではなく Teams 管理センターです。

Teams Network planner で影響を分析する [1.1.2]

Network planner の場所は、Teams 管理センターの Planning。使えるロールは次の3つです。

- Global Administrator
- Teams Administrator
- Teams Communications Administrator

出力は、Teams と cloud voice に要るネットワーク要件を拠点ごとに計算したレポートです。見え方は2つあります。活動ごとの計算表と、全体の帯域ニーズです。[^c1-2]

SAMPLE

入力は3段で組みます。

1. ペルソナを決める
2. ネットワーク プランにサイトを追加する
3. レポートを作る

ペルソナは利用者の使い方の型です。推奨は office workers、remote workers、Teams Rooms System の3種です。推奨を使うと、ユーザーは office worker 80%、remote worker 20% に自動で配分されます。カスタム ペルソナは、Personas タブの「+ Custom persona」で作ります。入れるのは名前、説明、権限。上限は3つで、推奨で足りない時に使います。

サイトは建物や事業所で、WAN でつなぐとインターネットや PSTN の出口を共有できます。ローカル接続のサイトから先に作ります。必須の設定はネットワーク ユーザー数だけ。ほかの設定項目は次の4つです。

- WAN-enabled
- WAN capacity
- インターネット出口（Local/Remote）
- PSTN 出口（none/local/remote）

具体的な帯域推奨をレポートに出すには、WAN 容量とインターネット容量の数値が要ります。空のままでは出ません。レポートは Reports タブの「Start a report」から始めます。サイトのユーザーをペルソナへ配分し、「Generate report」を押して保存します。

Teams が使うポートとプロトコル [1.1.3]

Teams が要るポートは次のとおりです。[^c1-3]

- TCP 80 と 443
- UDP 3478（STUN）
- UDP 3479（音声）
- UDP 3480（ビデオ）
- UDP 3481（共有/VBSS）

メディアは RTP で運び、SRTP で守ります。遅延に敏感なので UDP が最適です。TCP や HTTP トンネルは最後の手段で、品質は下がります。

Microsoft 365 のエンドポイントは Optimize、Allow、Default の3カテゴリです。Teams も前の2つだけを使うわけではありません。メディア（ID 11）は Optimize、シグナリング（ID 12）は Allow で、Teams の節には Default の行（ID 16、17、19、27、127 など）もあります。[^c1-4]

カテゴリ	Teams での例
Optimize	ID 11（メディア）。52.112.0.0/14 と 52.122.0.0/15 に UDP 3478〜3481
Allow	ID 12（シグナリング）。.teams.microsoft.com、.lync.com など。TCP 443/80 と UDP 443

SAMPLE

ER 列が Yes なら、そのセットは ExpressRoute に対応します。データは毎月初めに必要なら更新されます。新しい IP と URL は有効化の30日前に公開されます。

メディアに VPN は勧められません。Optimize の宛先は、VPN とプロキシを迂回させます（スプリット トンネル）。パケットシェーパーとパケット検査装置も、品質を大きく下げます。

オンプレミスの Skype for Business とフェデレーションするなら、DNS に SRV レコードを足します。

項目	値
名前	sipfederationtls（TCP）
優先度/重み/ポート	100 / 1 / 5061
ターゲット	sipfed.online.lync.com

QoS は送信元ポートと DSCP の組で覚えます。[^c1-5]

種類	送信元ポート	DSCP
音声	50,000〜50,019	46（EF）
ビデオ	50,020〜50,039	34（AF41）
画面共有	50,040〜50,059	18（AF21）
通話・会議のシグナリング（UDP）	50,070〜50,089	40（CS5）

シグナリングのポートは変更できません。実装は、クライアントの DSCP マーキングと、ルーターのポートベース ACL の組み合わせが推奨です。

ネットワークの準備状況を評価するツール [1.1.4]

見分け方は、Teams の通話だけを測るか、Microsoft 365 全体の出口と DNS まで見るかです。

Microsoft Teams Network Assessment Tool は、Windows 用のダウンロード ツールです。実行の形で役割が変わります。[^c1-6]

実行	テスト	見るもの
`NetworkAssessmentTool.exe`	接続	Teams に要る IP アドレスとポートへ届くか
`NetworkAssessmentTool.exe /qualitycheck`	品質	最寄りのエッジへパケットを流して損失・ジッター・往復時間

届かない宛先が残ったまま品質を測っても意味がないので、先に引数なしで接続を確かめ、届かない宛先があればファイアウォールを直してから、/qualitycheck で品質を測ります。

Microsoft 365 ネットワーク接続テスト ツールは、Web サイトと、高度なテストを動かす Windows クライアントの2部構成です。高度なテストには .NET 6.0 Runtime が要ります。Run test の順序は次のとおりです。[^c1-7]

1. 拠点の特定
2. JavaScript の TCP 遅延テスト

SAMPLE

3. 高度なクライアントのダウンロードと実行
4. 結果のアップロード

サインインして実行すると、レポートは管理者へ共有され、テナントへ上がります。

Teams の判定は次の3つで、項目ごとに表の値を下回れば合格です。

項目	合格
UDP パケット損失	1.00% 未満
遅延	100 ms 未満
ジッター	30 ms 未満

メディア接続（UDP）が塞がれると、TCP で動くことはあっても音声と映像は劣化します。ほかの判定は次の表のとおり。

洞察	条件
ネットワーク出口が遠い	拠点から出口まで 500 マイル（800 km）超（TCP 遅延が 25 ms 超増える見込み）
VPN スプリット トンネル	Exchange Online、SharePoint Online、Teams の Optimize ごとに split out・tunneled・選択的トンネルを判定。すべて split out か選択的トンネルなら合格

レポートの共有のしかた（テナント内のユーザーとの共有、サインイン不要の ReportID リンク）は、管理者が選び、レポートは既定で90日後に失効します。

管理センターの洞察は、日次集計の製品内測定。このツールは、利用者側でローカルに1回だけ動かして深く調べます。

セキュリティとコンプライアンス機能のライセンス [1.2.1]

使える機能は、契約している Microsoft 365 / Office 365 とスタンドアロン ライセンスで決まります。[^c1-8] 全ライセンス共通で入る保護は3つ。SharePoint・OneDrive・Teams の組み込みウイルス対策、外部ドメインの異常レポート、ほぼリアルタイムの URL 警告です。

契約	Teams で加わる機能
Defender for Office 365 Plan 1	Safe Links、Safe Attachments、Tenant Allow/Block List、ZAP for Teams
Plan 2 / Microsoft 365 E5	Plan 1 に加え、Teams チャットからのユーザー削除、メッセージの高度なハンティング
Teams Premium	追加ライセンス。Teams の代わりにならず、両方が要る

ZAP for Teams には Plan 1 か Plan 2 が要ります。しきい値型と異常検知型のアラート ポリシーは、E5/G5 か、E1/E3 に Defender for Office 365 P2 などを足した契約が対象。E1/E3 だけでは毎回発報型しか使えません。

SAMPLE

Teams Premium を管理するには、有効な Teams Premium ライセンスがテナントに最低1つ要ります。2026年4月1日から、従来は Teams Premium 限定だった一部機能が Teams Enterprise に含まれるようになりました。[^c1-9]

コンテンツ検索と eDiscovery（Standard/Premium）は、Purview 側で有効化する作業が要りません。

セキュリティとコンプライアンスのアラート ポリシー [1.2.2]

アラート ポリシーは、Defender ポータルの Email & collaboration > Policies & rules > Alert policy で作ります。[^c1-10] 作成と編集は Manage Alerts ロール、表示だけなら View-Only Manage Alerts ロールです。

項目	値
カテゴリ	Data loss prevention、Information governance、Mail flow、Permissions、Threat management、Others
重大度	Low、Medium、High、Informational
反映の遅れ	作成・更新から発報まで最大24時間
異常検知	基準値の確立に最大7日。その間アラートは出ない

Teams の既定アラートは2つあります。

- Safe Links 保護リンクのクリック
- Teams メッセージがセキュリティ リスクとして報告された時（重大度は Low。E5/G5 か Defender アドオンが要る）

ポリシーでは、しきい値とメール通知の有無を決められます。

Teams 管理センターのリアルタイムのアラートは別物です。規則は、アプリの申請（App submissions）、デバイスのオフライン（Device state rule）、進行中の会議の音声・ビデオ・画面共有の品質の5つで、Teams Rooms や電話に限った規則ではありません。アラート ポリシー（Defender ポータル）側は、コンテンツと操作がポリシーに触れたかを見ます。

Teams 管理者ロールの選択 [1.2.3]

最小特権が原則です。Global Administrator は、既存ロールで対応できない緊急時だけ使います。ロールの付与は Microsoft Entra ID で行います。[^c1-11]

ロール	できること
Teams Administrator	Teams 全体。会議・音声・メッセージング・組織全体設定・チーム管理・デバイス管理。グループの管理と作成
Teams Communications Administrator	通話と会議。会議・音声ポリシー、電話番号、リソース アカウント、CQD
Teams Communications Support Engineer	高度なツールで通信問題を調べる。ユーザーの通話品質、CQD
Teams Communications Support Specialist	基本ツール。検索した特定ユーザーの情報だけ
Teams Devices Administrator	認定デバイスの構成・更新・状態・再起動。通話品質データと通話分析は不可

SAMPLE

ロール	できること
Teams Reader	管理センターの読み取り専用。更新は不可
Teams Telephony Administrator	通話ポリシー、電話番号、音声アプリ、リソース アカウント、PSTN 使用状況レポート

リソース アカウントの作成と管理には、Teams 系の管理者ロールに加えて User Administrator が要ります。

Defender for Office 365 の脅威ポリシー [1.2.4]

Teams を守る機能は3つです。[^c1-12]

機能	Teams での動き
Safe Links	クリック時に既知の悪意あるリンクを検証。URL は書き換えない。悪意なら警告ページ。ポリシーの Teams セクションで On（推奨）。既定の Safe Links ポリシーはない（ただし Built-in protection の事前設定ポリシーが、Defender for Office 365 のライセンスが1つ以上あるテナントでは Teams を含めて全受信者に Safe Links を当てる）。デスクトップ、Web、モバイルで有効
Safe Attachments	SharePoint・OneDrive・Teams 向け。ポリシーなしでグローバルに有効/無効
ZAP for Teams	配信後にマルウェアか高信頼度フィッシングと判明した内部メッセージを隔離

ZAP の最初のブロックは配信直後で、ZAP は配信後最大48時間まで動きます。設定は Defender ポータルの Settings > Email & collaboration > Microsoft Teams protection で On にします。隔離ポリシーは既定で AdminOnlyAccess。管理者だけが管理し、ユーザーへの隔離通知は届きません。

ZAP の制約は4つです。

- 外部メッセージのチャットは対象外
- プライベート チャネルは対象外
- GCC、GCC High、DoD は対象外
- 除外は送信者でなく受信者に効く（グループ チャットは全員が除外された時だけ何もしない）

既知の悪意ある URL は、全ライセンスに含まれるほぼリアルタイムの URL の保護により、警告付きで配信されます（Safe Links とは別の仕組み）。ユーザーは Teams のメッセージをセキュリティ リスクとして報告できます。

保持ポリシー [1.2.5]

Teams の保持ポリシーは、場所として Teams channel messages、Teams chats、Teams call logs などを個別に選びます。チャネル メッセージの場所には、プライベート チャネルも含まれます。Teams の場所を選んだ保持ポリシーでは、ほかの場所（OneDrive など）は自動で外れるので、1 本のポリシーに入れられません。[^c1-13] 保持が働くのは、メッセージ本体でなくコピーです。チャットのコピーは、各参加ユーザーのメールボックスの隠しフォルダー。チャネル メッセージは、グループ メールボックスの隠しフォルダーです。

SAMPLE

コピー先	メールボックスの種類
クラウド ユーザーのチャット	UserMailbox
オンプレミス ユーザー	MailUser
標準チャネル	GroupMailbox
共有チャネル	SubstrateGroup

期限切れの項目は、隠しフォルダー SubstrateHolds へ移ります。ここは完全削除前のソフト削除の置き場です。タイマー ジョブの周期は通常1〜7日。SubstrateHolds に最低1日置いてから、完全に削除します。1日で削除する設定でも、完全削除まで16日かかることがあります（公式の例）。

保持されない項目は次の5つです。

- コード スニペット
- モバイルで録音したボイス メモ
- サムネイル
- アナウンス画像
- リアクション

通話ログは既定で無期限に保持され、消すには通話ログ用の保持ポリシーを使います。別組織のアカウントで参加した外部ユーザーのメッセージは、そのテナントに保存されます。自組織のポリシーでは削除できません。共有チャネルとプライベート チャネルは、親チームの設定を継承します。

Teams で使うメールとファイルは、Teams の保持ポリシーに含まれません。Microsoft 365 グループのチームのファイルは Microsoft 365 Group mailboxes & sites の場所、グループに接続しないサイト（共有チャネル・プライベート チャネルのサイトなど）は SharePoint classic and communication sites の場所のポリシーで扱います。チャット会議の録画とトランスクリプトには、主催者の OneDrive を場所に含めたポリシーが要ります。チャネル会議のものはファイルとして含まれます。

保持ポリシーは、サイトやメールボックス単位で同じ設定を当てる仕組み。保持ラベルは項目単位で、項目を移動しても付いて回ります。ポリシーは付いて回りません。優先の原則のうち、主なものは次の2つです（このほか、削除どうしでは最も短い削除期間が勝ちます）。

- 保持は完全削除に勝ち、最も長い保持期間が勝つ
- 保持ラベルの削除アクションは、保持ポリシーの削除アクションに勝つ

秘密度ラベルと発行ポリシー [1.2.6]

流れは、ラベルを作り、ラベルを含むラベル ポリシーを作って対象ユーザーへ公開する順です。作成は Purview ポータルの Information Protection > Sensitivity labels で「+ Create a label」です。[^c1-14]

コンテナー向けラベルは、スコープで Groups & sites を選びます。Teams、Microsoft 365 グループ、SharePoint サイトに、次などを設定できます。

- プライバシー（Public/Private）

SAMPLE

- 外部ユーザー アクセス
- 外部共有
- 非管理対象デバイスからのアクセス
- 認証コンテキスト

有効化は2段です。Entra ID でラベル サポートを有効にし、Security & Compliance PowerShell の Execute-AzureAdLabelSync で同期します。非管理対象デバイスと認証コンテキストは条件付きアクセスと連動するので、先にそちらを構成します。コンテナーのラベルは、中のアイテムへ継承されません。共有チャネルは親チームのラベルを自動で継承し、変更も削除もできません。プライバシーを Public/Private に設定すると値がロックされ、ラベルを外さない限り変えられません。

会議向けラベルは、スコープで Files & other data assets、Emails、Meetings の3つを選びます。Meetings だけは選べません。保護設定では「Protect Teams meetings and chat」を選びます。ラベルで適用できる設定は次のとおりです。

- ロビーを迂回できる人、発表できる人
- 録画と文字起こしができる人
- 会議の映像と音声の暗号化、自動録画
- ビデオの透かし
- チャット等のコピー防止
- 画面共有中の機密コンテンツ検出

一部の設定は Teams Premium が要ります。ないと Purview ポータルにライセンス不足の情報バーが出ます。S/MIME か Double Key Encryption を使うラベルは、予定表・会議・チャットを保護できません。ライブ イベント（2026年6月30日に廃止済み）にはラベルを適用できません。会議中にラベルを変えても、主催者が会議を終了して再開するまで、録画・暗号化・透かしは反映されません。

ラベル ポリシーで設定するのは、会議と予定への既定ラベル、ラベル付けの必須化、共有ファイルからのラベル継承です。Teams の既定ラベルは、新規の予定にだけ適用されます。

Purview DLP ポリシー [1.2.7]

Teams のチャットとチャネル メッセージ（プライベート チャネル含む）の DLP は、E5/A5/G5 系が対象です。E3 の DLP は SharePoint・OneDrive・Exchange で、Teams 経由で共有したファイルも範囲に入ります。[^c1-15]

ゲストに機密情報を送るチャットやチャネル メッセージは、数秒以内に自動で削除されます。条件は、自テナントがチャットやスレッドの開始者であること。ゲストと共有したファイルに機密情報があれば開けなくなりますが、ポリシーに SharePoint と OneDrive を含める必要があります。

スコープで守られる範囲は変わります。

スコープ	保護される範囲
個別のユーザー アカウント	1:1 と n 人のチャット。標準・プライベート・共有チャネルは保護されない

SAMPLE

スコープ	保護される範囲
グループ（セキュリティ、配布、Microsoft 365）	チャットと全チャネルのメッセージ

共有チャネルは送信者の身元で評価され、各ユーザーのホーム テナントのポリシーが当たります。外部アクセスの複数テナント チャットは、チャットを開始したホスト テナントのポリシー。

一致するとポリシー ヒントが出て、送信者はポリシーを上書きするか、管理者に通知できます。ブロックされた時の見え方は2つ。アクティビティ通知のプレビューは「Preview Unavailable」になります。送信者には「Your message has been blocked」のアクティビティが作られます。Teams の DLP は、Exchange や SharePoint のようなメール通知を送りません。

Teams の条件付きアクセス [1.2.8]

条件付きアクセスは「if-then」のポリシーです。リソースへアクセスするなら、多要素認証などの操作を完了する、という形になります。第1要素認証の後で強制され、DoS の最前線防御ではありません。Microsoft Entra ID P1 が要り、Microsoft 365 Business Premium でも使えます。[^c1-16]

Teams は、条件付きアクセスのクラウド アプリとして単独で対応します。ただし Exchange Online と SharePoint に依存します。そちらにもポリシーがないと、ユーザーがリソースへ直接アクセスできる場合があります。依存関係の問題を避けるため、個別アプリより Office 365 アプリ グループ全体を対象にします。

複数のポリシーが当たる時は、該当するすべてを満たす必要があります（論理 AND）。評価は2段です。フェーズ1でセッション情報（ネットワーク場所、デバイス ID）を集め、フェーズ2で強制します。ブロックの付与制御があれば、そこで止まります。

付与制御	内容
Block access	アクセスを止める
要求できるもの	多要素認証、準拠デバイス、Entra ハイブリッド参加デバイス、承認済みクライアント アプリ、アプリ保護ポリシー、パスワード変更、利用規約

Outlook や Teams モバイルなどのパブリック クライアント自体には、ポリシーが当たりません。要求先のリソースで当たります。ロールやグループを対象にしたポリシーはトークン発行時にだけ評価されるので、追加直後のユーザーは新しいトークンを得るまで対象になりません。

Purview 情報バリア [1.2.9]

情報バリアは、Teams、SharePoint、OneDrive で、グループ間やユーザー間の双方向のコミュニケーションを制限するソリューションです。[^c1-17] Teams で防ぐ行為は、ユーザー検索、メンバー追加、チャット開始、グループ チャット、会議の招待、画面共有、通話、ファイル共有、共有リンク経由のアクセスです。

制約は4つあります。

- 双方向のみ。一方向の制限はできない
- メールは制限できない（Exchange のメール フロー ルールを使う）

SAMPLE

- Teams 作成時に関連付く SharePoint サイトには、既定で適用されない
- IB のグループはテナントをまたいで作れない。ゲストにも適用され、グローバル アドレス一覧で探索できる必要がある

セグメントは、レガシー モードでなければ5,000まで、複数セグメントへの割り当ても可能です。レガシー モードは最大250で、1ユーザーは1セグメントのみ。前提は、Teams で scoped directory search を有効にし、少なくとも24時間待ってからポリシーを定義することです。管理するのは IB Compliance Management ロール。

ポリシーを変えた後、1:1 チャットは通信不可になると読み取り専用になります。グループ チャットは、該当ユーザーが除外されて新しい会話を見られなくなる一方、過去の会話は見えます。

コミュニケーション コンプライアンスとインサイダー リスク管理 [1.2.10]

使い分けは、見る対象の違い。コミュニケーション コンプライアンスは、メッセージの内容の不適切さを見ます。インサイダー リスク管理は、ログから得た複数のシグナルで、ユーザーの行動リスクを見ます。[^c1-18]

コミュニケーション コンプライアンスの検出対象は、規制違反（SEC、FINRA など）、機密情報、嫌がらせや脅迫的な言葉、アダルト コンテンツです。事前定義かカスタムのポリシーで社内外のやり取りを調べ、指名されたレビュー担当者が確認して対処します。対象サービスは、メール、Teams、Copilot、Viva Engage、サードパーティです。

ユース ケースは3つの観点で出ます。

- 社内ポリシー（ハラスメントなど）
- リスク管理（M&A など機密案件の不正な連絡、利益相反）
- 規制遵守（FINRA Rule 3110 など）

Teams は、公開・非公開チャネルのチャットと個別チャットが対象です。ユーザー、配布グループ、特定チャネルは手動で追加します。会議トランスクリプトの検出はプレビュー。

インサイダー リスク管理が特定するのは、IP の窃盗、データ漏えい、セキュリティ違反。悪意と不注意の両方の内部リスクが対象です。主なポリシー テンプレートは次のとおりです（ほかに Patient data misuse、Risky AI usage、Risky Agents、Risky browser usage、退職者・優先ユーザー・リスクの高いユーザー向けの Security policy violations があります）。

- Data theft by departing users（退職者）
- Data leaks
- Data leaks by priority users
- Data leaks by risky users
- Security policy violations

流れは、ポリシー、アラート（Needs review）、トリアージ、調査（ケース）、アクションの順。深刻なら eDiscovery（Premium）へエスカレーションします。ポリシーを作る前でも、insider risk analytics で潜在的なリスクを評価できます。両機能とも、Azure の依存関係で対応する地域のテナントでだけ使えます。

SAMPLE

ライフサイクル管理のライセンス [1.3.1]

ライセンスは「所有していれば足り、割り当ては不要」なものと、「割り当てが要る」ものに分かれます。[^c1-19]

機能	要るもの
有効期限ポリシー	対象グループのメンバー全員分の Entra ID P1 か P2（所有で足りる）
名前付けポリシー	メンバーである各ユニーク ユーザー分の Entra ID P1 か Entra Basic EDU（所有で足りる）
グループ作成の制限	設定する管理者と、作成を許可されたグループのメンバーに P1/P2 か Basic EDU を割り当てる。作成できない一般メンバーは不要
アクセス レビュー	Entra ID Governance か Entra Suite（一部機能は P2 でも動く）
非アクティブ ユーザー、推奨付き、複数リソースのレビュー	Entra ID Governance
カスタム ポリシー パッケージ	対象ユーザーに Teams Premium（定義済みパッケージは不要）

Teams Premium の高度なコラボレーション分析（非アクティブなチームのインサイト）には、全ユーザーへの割り当てが要ります。有効期限ポリシーの構成は、Groups Administrator か User Administrator が行います。

Teams のコンテンツの保存先 [1.3.2]

Teams の土台は Microsoft 365 グループと Graph。チームを作ると、次の5つが作られます。[^c1-20]

- Microsoft 365 グループ
- SharePoint サイトとドキュメント ライブラリ
- Exchange Online の共有メールボックス
- Exchange Online の予定表
- OneNote ノートブック

データ	保存先
チャネルのファイル、OneNote、Wiki タブ	チームの SharePoint サイト
1:1・グループ チャットのファイル	共有した人の OneDrive
チャット メッセージのコピー	参加ユーザー各自のメールボックスの隠しフォルダー
標準チャネルのメッセージのコピー	グループ メールボックス（共有チャネルは SubstrateGroup。オンプレミス ユーザーのチャットは MailUser）
チャット会議の録画・トランスクリプト	主催者の OneDrive
チャネル会議の録画	チャネルに関連付けた SharePoint サイト
ボイスメール（録音と文字起こし）	ユーザーの Exchange メールボックス

メッセージの一次保存先は Azure ベースのチャット サービスです。メールボックスには、コンプライアンス用のコピーが入ります。プライベート チャネルのメッセージの保存先は、2025年末にかけて、ユーザーのメールボックスからグループ メールボックスへ移す変更が告知されています。

SAMPLE

データは、組織に関連付けた地理リージョンに置かれます。確認は Microsoft 365 管理センターの Data location。取り込み後、探索可能になるまで最大24時間かかります。

更新ポリシー [1.3.3]

Teams クライアントは月2回更新され、利用可能になると自動で入ります。確認のタイミングは、アプリ起動時と、数時間ごとのバックグラウンド（Windows と Mac）。更新にはユーザーのサインインが要ります。[^c1-21]

古さ	動作
1〜3か月古い	更新を促す通知
3か月より古い	更新・IT 管理者へ連絡・Web 版を続ける、を選ぶブロック ページ

重大な更新は即時。通常のスケジュールは無視して出ます。Windows は Delivery Optimization で差分だけを取り、反映にはアプリの再起動が要ります。Mac は Microsoft AutoUpdate で自己更新します。自動では再起動しません。

更新ポリシーが変えるのは、プレビュー機能の見せ方です。管理センターの Teams > Teams Update policies で作り、「Show Teams preview features」を選びます。[^c1-22]

設定	動作
On for users in Current Channel (Preview)（既定）	Office の Current Channel (Preview) のユーザーに有効。本人は切れない（既定の設定は、Office の更新チャネルに連動する）
Users can opt in	Office のチャネルを問わず許可。本人が Teams で Public preview をオンにする
Off	プレビュー機能は使えない
On for everyone	全員に有効。本人は切れない

ポリシーは特定のユーザーへ割り当てます。グローバルを上書きしません。Teams on the web ではデバイス ポリシーが当たらず、「On for users in Current Channel (Preview)」は Off 扱いです。PowerShell は Set-CsTeamsUpdateManagementPolicy を使います。

ポリシー パッケージ [1.3.4]

ポリシー パッケージは、似た役割のユーザーに割り当てる、定義済みのポリシーと設定の集まりです。含められるポリシーは11種類です。[^c1-23]

- Messaging、Meeting、App setup、Calling
- Live events、Call park、Teams
- Voice routing、Caller ID、Update、Events

定義済みパッケージは次の5系統です。

- Education（高等・小学・中学の学生と教師）
- Frontline manager/worker

SAMPLE

- Healthcare（clinical worker・information worker・patient room）
- Public safety officer
- Small and medium business user（Business Voice の有無）

割り当てると、個々のポリシー名にパッケージ名が付きます（Education (Teacher) なら Education_Teacher）。パッケージ内の設定を変えれば、割り当て済みの全ユーザーに反映されます。使う順は View、Customize、Assign です。

カスタム パッケージは、左ペインの Policy packages で Add し、名前、説明、含めるポリシーを選んで Save します。対象ユーザーに Teams Premium が要ります。割り当て先は個別のユーザー、グループ、ユーザーの一括（バッチ）の3つ。管理は管理センターか PowerShell です。カスタムのポリシーを割り当てない限り、ユーザーにはグローバル（組織全体の既定）ポリシーが自動で適用されます。Teams ポリシーでは、グローバルの編集や割り当ての反映に24時間かかることがあります。

ポリシーの割り当て [1.3.5]

適用の優先順位は次のとおりです。[^c1-24]

1. ユーザーへの直接割り当て（個別も一括も）
2. グループ割り当て（複数なら、ランクが最も高いもの。1が最上位）
3. グローバル（Org-wide default）

直接割り当てがある間は、グループのポリシーは効かないので、グループのポリシーを継承させるには直接割り当てを外します。グループへの割り当て自体はすぐ終わりますが、メンバーへの伝播はバックグラウンドで行われ、時間がかかることがあります。グループ割り当てでランクを指定しないと、最も低いランクが付きます。グループから外せば、下位のランクは自動で繰り上がります。ランクの変更は、一度削除してからのやり直し。

グループ割り当ての制約は次のとおりです。

制約	内容
伝播	直接のメンバーだけ。入れ子グループには伝播しない（入れ子にできるのはセキュリティ グループの中。Microsoft 365 グループにはセキュリティ グループを入れ子にできない）
使えないグループ	HiddenGroupMembership が有効なもの（クラスのチームは既定で有効）
対応しないポリシー	Teams App Permission、Teams Upgrade、Dialout。PowerShell のリファレンスは Network Roaming、Emergency Call Routing、Voice Applications も挙げる
上限	1つのポリシー種別につき最大64グループ
反映	割り当ては即時。メンバーへの伝播はバックグラウンドで、大きいグループほど遅い
規模	5万ユーザーまでを推奨
対象	Microsoft 365 グループ、セキュリティ グループ、配布リスト

使い分けは次の4つです。

SAMPLE

- 少数のユーザー: 個別の割り当て
- 役割ごとに複数のポリシー: ポリシー パッケージ
- グループ所属ベース: グループ割り当て
- 数百〜数千人: 一括（バッチ）の割り当て

基本は、グローバルを最大数のユーザーに当て、特別な人にだけ個別に割り当てることです。

PowerShell は、Grant にグループを指定する形です。

操作	コマンド
グループに割り当て	`Grant-CsTeamsMeetingPolicy -Group <グループ ID> -PolicyName "..." -Rank 1`
グループ割り当ての新規作成	New-CsGroupPolicyAssignment（将来は廃止予定。Grant-Cs の -Group が後継）
グループ割り当ての確認	Get-CsGroupPolicyAssignment
ユーザーの有効なポリシー	Get-CsUserPolicyAssignment（Get-CsOnlineUser は直接割り当てだけを表示）

Microsoft 365 グループの作成の制限 [1.3.6]

既定は、全ユーザーが作成できる状態。制限は、特定の Microsoft 365 グループかセキュリティ グループのメンバーにだけ許可する形です。影響は、グループに依存する全サービスに及びます。Outlook、SharePoint、Viva Engage、Teams、Planner、Power BI（classic）、Project for the web などです。[^c1-25]

PowerShell は Microsoft Graph PowerShell の Beta モジュールで、Group.Unified の設定を変えます。

設定	値
EnableGroupCreation	False
GroupCreationAllowedGroupId	許可グループの ID
解除	$GroupName を空に、$AllowGroupCreation を $true にして再実行

制御用のグループは組織で1つだけで、ほかのグループを入れ子にできます。許可したい人は、所有者でなくメンバーとして入れます。

制限を回避できるのは、特定の管理者ロール。Microsoft 365 全体管理者は、M365 管理センター、Planner、Exchange、SharePoint から作れます。Teams からは作れません。Teams Administrator（旧名 Teams Service Administrator）は、Teams 管理センターと Entra ID から作れます。反映には30分以上かかることがあります。

Microsoft 365 グループの有効期限ポリシー [1.3.7]

対象は Entra ID の Microsoft 365 グループだけで、組織ごとにポリシーは1つ。[^c1-19] 設定は、Entra 管理センターの Groups > All groups の Expiration です。決めるのは、有効期間（日数）、所有者がいない場合の通知先メール、対象（全て/選択/なし）の3つです。

SAMPLE

項目	値
有効期間	30日以上（プリセットかカスタム）
選択して適用できるグループ	最大500（全グループなら制限なし）
通知メール	有効期限の30日前、15日前、1日前（自動更新されない場合）
自動更新	活動に基づき期限の約35日前。所有者に通知なし
削除と復元	期限の1日後に削除。削除後30日は復元可（変更不可）

自動更新のきっかけは次の活動です。

- Outlook
- SharePoint（ファイルの表示・編集・ダウンロード・移動・共有・アップロード）
- Teams（「チャネルを訪問」するだけ）
- Viva Engage

所有者のいないグループの通知は、設定した代替メールへ送られます。Teams で使うグループの有効期限の通知は、Teams Owners フィードに出ます。リーガル ホールド中のグループ メールボックスは、期限切れで削除されても完全には消えません。

構成は Groups Administrator か User Administrator です。一般ユーザーは、自分が所有するグループの更新と復元だけ。PowerShell のコマンドレットは次の3組です。

- New/Get/Update/Remove-MgGroupLifecyclePolicy
- Add-MgGroupToLifecyclePolicy、Remove-MgGroupFromLifecyclePolicy
- Invoke-MgRenewGroup

グループの名前付けポリシーとブロックされた単語 [1.3.8]

方法は2つ、接頭辞・接尾辞の命名ポリシーと、カスタムのブロックされた単語です。[^c1-27] 構造は Prefix[GroupName]Suffix で、[GroupName] は設定内に1つだけ。PowerShell では必ず含めます。接頭辞・接尾辞とグループ名を含め、合計63文字までです。たとえば HR-Payroll_Tokyo のように組み立てます。

項目	値
使える属性	[Department]、[Company]、[Office]、[StateOrProvince]、[CountryOrRegion]、[Title]（拡張属性・カスタム属性は非対応で固定文字列扱い）
ブロック単語	カンマ区切りで最大5,000個。大文字小文字は区別しない。グループ名とエイリアスの両方に効く
判定	完全一致（「lass」をブロックしても「Class」は使える）

構成に要るのは、Global Administrator、Group Administrator、Directory Writer のいずれか。Global Administrator と User Administrator は対象外で、ブロック単語を含む名前でも作れます。全ワークロードで作成・編集時に適用され、既存グループは所有者が名前を編集した時点で適用されます。

SAMPLE

PowerShell は、Group.Unified の 2 つの値を Update-MgBetaDirectorySetting で更新します。値は PrefixSuffixNamingRequirement と CustomBlockedWordsList。Exchange のグループ命名ポリシーと重なる時は、Entra ID のポリシーが勝ちます。Exchange 側は効きません。

チームのアーカイブ、削除、アーカイブ解除 [1.3.9]

違いは、復旧できるかどうか。[^c1-28]

操作	結果
アーカイブ	活動が停止。プライベート チャネルとサイトもアーカイブされる。メンバーの追加・削除やロール更新、チャネル・ファイル・チャットの閲覧はできる。再有効化できる
削除	チャネル、ファイル、チャットも削除。M365 グループの復元で戻す（Teams 管理センターの Manage teams > View deleted team からも Restore できる。既定30日、復元に最大24時間）。保持下のサイトは保持期間まで残る

勧められる順序は、先にアーカイブして、不要と確信してから削除することです。アーカイブは、Teams service admin が管理センターで行うか、チームの所有者が行います。手順は、チーム名を開いて Archive、確認画面でもう一度 Archive です。「Make the SharePoint site read-only for team members」を選ぶと、サイトと Wiki タブの編集を防げます（所有者は編集できる）。

アーカイブ後の状態は Archived で、一時的に Hidden teams、その後は Manage teams の Archived に出ます。解除は Restore。Active に戻るまで時間がかかり、Your teams には自動で戻りません。削除は Delete を選び、確認でもう一度 Delete を選びます。

削除したチームの PowerShell での復元は、次の順です。

1. Connect-MgGraph
2. Get-MgDirectoryDeletedItem で一覧
3. Restore-MgDirectoryDeletedItem -DirectoryObjectId で復元
4. Get-MgGroup で確認

Graph の archive API でも、同じ操作を自動化できます。

削除した Microsoft 365 グループの復元 [1.3.10]

Microsoft 365 グループとクラウド セキュリティ グループは、削除後30日間は非表示で保持され、復元できます。この30日は変更できません。[^c1-29] 配布グループでは使えません。クラウド セキュリティ グループの対応はプレビューで、パブリック クラウドのみです。

ロール	復元できる範囲
Global Administrator、Group Administrator、Partner Tier 2 Support、Intune Administrator	任意の削除済みグループ
User Administrator、Partner Tier 1 Support	Global Administrator ロールに割り当てられたグループを除く

SAMPLE

ロール	復元できる範囲
一般ユーザー	自分が所有するグループのみ

Entra 管理センターは、Groups > All groups の Deleted groups ペインで「Restore group」を選びます。完全に消すのも同じ Deleted groups ペインで、対象を選んで「Delete permanently」を選びます（管理者のみ）。PowerShell は、Get-MgBetaDirectoryDeletedGroup で一覧します。戻すのは Restore-MgBetaDirectoryDeletedItem -DirectoryObjectId です。完全削除は Remove-MgBetaDirectoryDeletedItem。

ドキュメントや SharePoint サイトを含むグループは、完全に戻るまで最大24時間かかります。復元後は、Exchange の左ナビにグループが現れ、Planner のプランと SharePoint サイトも使えます。動的グループは、復元すると新しいグループ扱い。ルールでメンバーが入り直し、最大24時間かかります。

復元できない時の確認先は次の4つ。

- 削除から30日を過ぎている
- 配布グループである
- 教育テナントで OneDrive for Business ストレージを使っている（セキュリティ グループのソフト削除が未対応）
- クラシック Web パーツのオーディエンス ターゲティングを使っている（同上）

Entra のアクセス レビューを使う場面 [1.3.11]

アクセス レビューは、グループ メンバーシップ、エンタープライズ アプリへのアクセス、ロール割り当てを管理する機能です。[^c1-30] 使う場面の例は次のとおりです。

- HR データが Entra ID になく、動的メンバーシップのルールを作れない
- 招待したゲストが業務にまだ要るかを、所有者に確認させたい
- 特権ロールのユーザーが多すぎる
- グループを新しい目的で使う
- 重要データへのアクセス、ポリシー例外リストを保つ

週次、月次、四半期、年次などで繰り返せます。作成は ID Governance > Access Reviews の「New access review」で「Teams + Groups」を選びます。ゲストを持つ全 M365 グループか、選んだチームを対象にします。全グループ指定には、動的グループとロール割り当て可能グループが含まれず、対象はゲストのみです。非アクティブなユーザーだけを対象にもでき、Days inactive の上限は730日。

レビュー担当者は、グループ所有者（チームとグループのみ）、選択したユーザーやグループ、本人（セルフレビュー）、マネージャーから選びます。マネージャー未設定や所有者不在に備え、フォールバックを指定できます。入れ子グループの扱いは、平坦化。削除対象でも入れ子グループからは外れず、直接メンバーシップからだけ削除されます。作成に要るのは、少なくとも Identity Governance Administrator ロール。設定を有効にすれば、M365 とセキュリティ グループの所有者も作れます。

SAMPLE

PowerShell と Microsoft Graph での操作 [1.3.12]

Teams PowerShell モジュールには、Windows PowerShell 5.1、または全プラットフォームで PowerShell 7.2 以降が要ります。[^c1-31]

操作	コマンド
インストール	Install-Module -Name MicrosoftTeams
サインイン	Connect-MicrosoftTeams
更新	Update-Module MicrosoftTeams
削除	Uninstall-Module

更新は、セッションにインポート済みだと失敗します。新しい管理者セッションで実行します。

用途	コマンドレット
チーム	New-Team、Get-Team、Set-Team
メンバー	Add-TeamUser、Remove-TeamUser
チャネル	New-TeamChannel、Remove-TeamChannel
ユーザーの確認	Get-CsOnlineUser
ポリシー	Get、New、Set、Remove、Grant
構成（組織全体のみ）	Get/Set-CsTeamsClientConfiguration

チーム管理のコマンドレットは、一般ユーザーも実行できます。ただし作用するのは、所有・参加するチームだけ。Global Administrator か Teams Administrator なら、全チームを操作できます。

操作	コマンド
ユーザーに割り当て	`Grant-Cs<PolicyName>`
ユーザーを組織の既定に戻す	`Grant-Cs<PolicyName> -Identity <User> -PolicyName $null`
グローバルを既定値に戻す	`Remove-Cs<PolicyName> -Identity Global`

Microsoft Graph は、チームの作成、チャネル、タブ、アプリを自動化する API です。[^c1-32]

操作	内容
チーム作成	POST /teams。成功で 202 Accepted と teamsAsyncOperation へのリンク。firstChannelName の既定は General
最小権限	委任もアプリケーションも Team.Create（Group.ReadWrite.All などは旧互換で非推奨）
メンバー追加	POST /teams/{team-id}/members（成功で 201 Created）。最小権限は TeamMember.ReadWriteNonOwnerRole.All。アプリケーション権限ではゲストを追加できない

SAMPLE

操作	内容
アーカイブ	POST /teams/{id}/archive。非同期。チームとグループに所有者が要る。解除は unarchive
読み取り専用	shouldSetSpoSiteReadOnlyForMembers を true（アプリケーション コンテキストでは未対応）

外部コラボレーションのライセンス [1.4.1]

ゲスト アクセスに、追加の Microsoft 365 ライセンスは要りません。前提は Business Standard、Enterprise、Education のいずれかのサブスクリプションです。ゲストには、Microsoft Entra External ID の課金モデルが当たります。基本は月間アクティブ ユーザー（MAU）で、暦月内に認証したユニークな外部ユーザー数です。[^c1-33]

課金されるのは UserType が Guest の外部ユーザーだけで、Member は対象外です。ゲストに ID Governance の高度な機能を使うと、MAU ベースの ID Governance アドオンが加わります。ゲストにできるのは組織外の人だけ。ライセンスのないゲストは Office.com で閲覧・編集できますが、デスクトップ版 Office は入れられません。

SharePoint と OneDrive の外部共有設定 [1.4.2]

外部共有のモデルは2つ。SharePoint external authentication と、Entra B2B との統合です。B2B 統合を有効にすると、ファイルやフォルダーの共有でも常にゲスト アカウントが作られ、Entra の設定が適用されます。無効なら、ファイルやフォルダーの共有ではゲスト アカウントは作られません（サイトの共有は常に Entra B2B を使い、ゲスト アカウントが作られます）。[^c1-34]

組織レベルは、SharePoint 管理センターの Policies > Sharing の External sharing で、4段階から選びます。

レベル	意味
Anyone	リンクを知っていれば認証なしでアクセス
New and existing guests	新規も既存もゲストとして認証が要る
Existing guests	すでにディレクトリにいるゲストのみ
Only people in your organization	外部共有なし

外部共有は、既定でオンです。OneDrive の設定は、SharePoint より厳しくできますが、緩くはできません。サイトの設定も、組織と同じか、より制限的でなければなりません。食い違うと最も制限的な値が効きます。サイトごとの変更に要るのは、少なくとも SharePoint Administrator ロール。サイト所有者は変更できません（Active sites > Settings > More sharing settings）。

既定の共有は、OneDrive が Anyone、Classic・Communication・グループなしのモダン サイトが Only people in your organization です。グループ接続サイトは Groups の設定次第です。

ドメイン制限は最大5,000ドメインで、Set-SPOTenant を使います。共有を制限すると、ゲストは通常1時間以内にアクセスを失います。

SAMPLE

Teams 管理センターの外部アクセス [1.4.3]

設定場所は Users > External access。外部アクセスは既定で有効で、組織設定とユーザー ポリシーがどちらも既定でオンです。構成の対象は3つあります。[^c1-35]

- 他の Microsoft 365 組織（チャットと会議）
- 組織に管理されない Teams ユーザー（チャットのみ）
- Skype ユーザー（チャットのみ）

信頼するドメインは4通りです。

シナリオ	内容
Allow all external domains	既定
Allow only specific external domains	許可リストのみ
Block specific domains	拒否リスト
Block all external domains	全部拒否

ドメインをブロックしても、サブドメインは既定ではブロックされません。Set-CsTenantFederationConfiguration の -BlockAllSubdomains で、全サブドメインをブロックします。特定の外部ユーザーのブロック リストは、最大200ユーザーです。組織設定の PowerShell は -AllowFederatedUsers、-AllowedDomains、-BlockedDomains です。非管理 Teams と Skype のチャットは、次の3つで制御します。

- -AllowTeamsConsumer
- -AllowTeamsConsumerInbound
- -AllowPublicUsers

外部ドメインとやり取りするには、相手組織もこちらを信頼する必要があります。相手のユーザーも、外部アクセスが有効でなければなりません。

外部アクセス（フェデレーション）とゲスト アクセスは、別の仕組みです。外部アクセスは、自分のテナントのまま外部ユーザーとチャットや会議をします。チームへの参加、チャネル、チームのファイルへのアクセスはできません。ゲスト アクセスは、ゲスト アカウントでチーム、チャネル、ファイルに入れます。

特定のユーザーとグループのドメイン別の外部アクセス [1.4.4]

先に組織の外部アクセスを有効にします。その上で、外部アクセス ポリシーが、どのユーザーが組織外とチャットや会議をできるかを決めます。作成は Users > External access の Policies タブで + Add。Global（Org-wide default）ポリシーのドメインの管理方法は変更できず、常に Use organization settings です。[^c1-35]

ポリシーのドメイン管理は5方式です。

方式	PowerShell の値（-CommunicationWithExternalOrgs）
Use organization settings（既定）	OrganizationDefault
Allow all external domains	AllowAllExternalDomains

SAMPLE

方式	PowerShell の値(-CommunicationWithExternalOrgs)
Allow only specific external domains	AllowSpecificExternalDomains
Block only specific external domains	BlockSpecificExternalDomains
Block all external domains	公式ページに -CommunicationWithExternalOrgs の値の記載なし(他組織との通信そのものは -EnableFederationAccess で止める)

リストは、1ポリシーあたり各100ドメインまでです。ドメインの粒度制御には、3つの条件があります。組織レベルの Manage external domains for this organization がオンであること。ポリシーがユーザーかグループに割り当て済みであること。相手の組織もこちらとのフェデレーションを許可していること。テナント設定の AllowFederatedUsers が $False だと、機能しません。カスタム ポリシーのあるユーザーでは、そのポリシーが組織設定に勝ちます。

特定のユーザーだけに許可するには、既定の組織全体ポリシーのコントロールをオフにします。次に、オンにした新規ポリシーを作って、対象者に割り当てます。一括割り当ては New-CsBatchPolicyAssignmentOperation -PolicyType ExternalAccessPolicy です。

Entra ID の外部コラボレーション設定 [1.4.5]

設定場所は、Entra 管理センターの Entra ID > External Identities > External collaboration settings。更新に要るのは、Global Administrator か External Identity Provider Administrator など。[^c1-37] 設定は4領域です。

- Determine guest user access
- Specify who can invite guests
- Enable guest self-service sign-up via user flows
- Allow or block domains

ゲストのアクセス	内容
Same access as members	最も包括的
Limited access(既定)	ユーザーやグループの列挙は禁止。非表示でないグループのメンバーシップは見える
Restricted to their own directory objects	最も制限的。自分のプロファイルのみ

招待は、既定で B2B ゲストを含む全ユーザーができます。設定は4段階です。

- Anyone in the organization
- Member users and users assigned to specific admin roles
- Only users assigned to specific admin roles
- No one in the organization

「特定の管理ロールのみ」でも、Guest Inviter ロールがあれば招待できます(User Administrator か Guest Inviter)。Collaboration restrictions では、指定ドメインへの招待を許可リストか拒否リストで決めます。外部ユーザーの退出設定は、テナントにプライバシー情報を追加した場合だけ構成できます。

SAMPLE

4つの管理センターでのゲスト アクセスと共有 [1.4.6]

Teams のゲスト アクセスは、Teams 管理センターだけでは完結しません。4か所の設定がそろって通ります。[^c1-38]

管理センター	場所と内容
Teams	Users > Guest access を On。Calling、Meeting、Messaging を On/Off
Microsoft 365	Settings > Org settings > Services の Microsoft 365 Groups。組織外アクセスと所有者による社外ユーザー追加（既定はオン）
Microsoft Entra	External collaboration settings の Guest user access と Guest invite settings
SharePoint	Policies > Sharing の External sharing

SharePoint と OneDrive で誰がゲストを招待できるかは、サイトの共有では常に、ファイルとフォルダーの共有では B2B 統合が有効な時に、Entra の外部コラボレーション設定（Guest invite settings）で決まります。B2B 統合が無効なら、ファイルとフォルダーの共有は SharePoint 側の設定で決まります。ゲストの画面共有は Not enabled、Single application、Entire screen から選びます。Teams のゲスト アクセスをオフにした場合、既存ゲストはチームへ入れません。チームからは削除されず @mention もでき、オンに戻せばアクセスが戻ります。

招待できない時は、止まっている場所を探します。見る場所は5つです。

- Teams のゲスト アクセスがオフ
- Microsoft 365 Groups の設定でゲストが禁止
- Entra の招待設定が No one か管理ロールのみ
- Collaboration restrictions のドメイン拒否
- SharePoint の共有レベルが Only people in your organization

特定のチームへのゲスト アクセスを制御する [1.4.7]

秘密度ラベルを使っているなら、グループ単位のゲスト制御はラベルで行うのが推奨です。[^c1-39] ラベルのスコープで Groups & sites を選びます。設定は、Define protection settings for groups and sites ページにあります。項目は Privacy and external user access settings。External user access は、所有者がコンテナーにゲストを追加できるかを制御します。有効化は2段です。Entra でコンテナー ラベルを有効にし、Execute-AzureAdLabelSync で同期します。External users access の変更が効くのは、新規ユーザーだけ。すでに入っているゲストは、設定を外した後もアクセスを失いません。

ラベルを使わない方法は、Microsoft Graph PowerShell（beta）の group.unified.guest テンプレートです。AllowToAddGuests を false にします。要るのは Global Administrator。Teams のゲストのブロックは、関連付けた Microsoft 365 グループに対して行います。どちらも新規ゲストの追加を防ぐだけで、既存のゲストは削除されません。

SAMPLE

チームとテナントからゲストを削除する [1.4.8]

ゲストは、チームから自分で退出できます。ただしディレクトリのゲスト アカウントは残り、Entra 管理者が削除する必要があります。[^c1-40]

範囲	手段
チームから外す	所有者、または管理センター
テナントから消す	Microsoft 365 管理センターの Users > Guest users > Delete a user、または Entra 管理センターの Users > Delete user

ユーザー削除に要るのは、少なくとも User Administrator ロールです。Privileged Authentication Administrator は、管理者も含めて削除できます。削除したユーザーは Deleted users に30日間表示され、その間は復元できます。チームへ追加してからアクセスできるまでは、最大12時間。

組織の外部共有を一度オフにして戻すと、ゲストはアクセスを取り戻します。定期的な整理の道具は、Entra のアクセス レビュー。実施できるのは、管理者、ゲスト本人、アプリ所有者です。

共有チャネルの外部アクセス [1.4.9]

共有チャネルは、チームにいない人を招待できるスペース。アクセスできるのは、共有チャネルの所有者とメンバーだけです。[^c1-41] 作成できるのはチーム所有者のみで、作成者が共有チャネルの所有者になります。既定で有効で、チャネル ポリシーが3つを制御します。

- 作成できるか
- 組織外と共有できるか
- 外部の共有チャネルへ参加できるか

組織外と共有するには、Entra のクロステナント アクセス設定が要ります。相手の組織側も、同じ構成を済ませている必要があります。外部参加者はゲスト アカウントを使いません。Entra ゲスト アカウントを持つ人（メンバーに変換されたものを含む）は、共有チャネルに追加できません。

能力	できるチャネル
チームに追加せず人を追加できる	共有チャネルのみ
ゲストが参加できない	共有チャネルのみ
B2B direct connect の外部参加者が参加できる	共有チャネルのみ

各共有チャネルには専用の SharePoint サイトがあり、親チームのラベルを継承します。親チームの人や管理者も、チャネル メンバーでなければ入れません。メッセージは、グループ メールボックスでなく専用のシステム メールボックスに入ります。削除から30日以内なら、メンバーシップごと復元可能。B2B direct connect ユーザーには、ホスト組織の条件付きアクセスが適用されます。情報バリアは、ホスト組織のユーザーだけが対象。

B2B direct connect のクロステナント アクセス設定 [1.4.10]

B2B direct connect は、2つの Entra 組織が相互の信頼を設定する External ID の機能で、現在は Teams の共有チャネルで使います。両組織が互いに許可して初めて成立します。一方が受信を許可しても、相手が送信を有効にする

SAMPLE

まで共有できません。[^c1-42]

項目	内容
初期状態	テナント全体の送信と、全外部組織からの受信がブロック
B2B collaboration の既定	有効。MFA とデバイスのクレームは信頼されない
設定場所	Entra 管理センターの External Identities > Cross-tenant access settings（Default settings か Organizational settings）
必要なロール	少なくとも Security Administrator（Teams 管理者は読み取りのみ）

受信と送信のそれぞれに、2つの設定があります。Access status は Allow access か Block access。Applies to は、全員か、特定のユーザー・グループ・アプリです。特定の外部ユーザーとグループの指定には Entra ID P1、特定アプリの選択には P1 か P2 が要ります。受信の既定設定では、ユーザーやグループを個別に指定できません。

信頼設定は3つで、外部組織のクレームを条件付きアクセスが信頼するかを決めます。

- Trust multi-factor authentication from Microsoft Entra tenants
- Trust compliant devices
- Trust Microsoft Entra hybrid joined devices

Automatically redeem invitations with the tenant をオンにすると、初回の同意プロンプトが出ません。B2B direct connect のユーザーは、自分のディレクトリに存在せず、共有チャネルだけに入れます。B2B collaboration のゲストは、ユーザー オブジェクトとして管理され、共有チャネルには入れません。

マルチテナント組織（MTO）[1.4.11]

MTO は、組織が所有する Entra テナントの境界を定義する機能です。ディレクトリ上はテナント グループとして表され、招待と承諾で構成します。[^c1-43] Microsoft 365 管理センターでは、Global Administrator が作ります。場所は Settings > Org settings > Organization profile の Multitenant collaboration > Get started。選ぶのは Create a new multitenant organization です。入れるのは名前、説明、招待するテナント ID。作成時には、「Allow users to sync into this tenant from the other tenants」と、同意プロンプトの抑止のチェックボックスを選びます。

招待が承諾されると、`MTO_Sync_<TenantID>` というクロステナント同期の構成が追加されます。同期は、まだ開始されません。MTO のテンプレートは、受信と送信の招待を自動引き換えにします。既存の MTO へは Add new tenants でテナント ID を追加し、参加手順を相手の Global Administrator にメールします。

新しい Teams の統合された共同作業体験には、Entra での MTO の表現が要ります。共同作業するユーザーは、B2B の Member としてプロビジョニングします。同期ユーザーの既定の userType は Member。すでに Guest だった B2B ID は、Guest のままです。

クロステナント同期は、B2B collaboration のユーザーを作成・更新・削除する一方向の同期です。MTO と同期は互いに独立ですが、どちらも B2B collaboration に依存します。複雑なトポロジ（マルチハブ/スポークなど）には、Entra のクロステナント同期が向きます。管理センターは、同期の構成を用意するだけで、同期は開始しません。

SAMPLE

Teams Phone とリソース アカウントのライセンス [1.5.1]

自分の電話番号で通話するユーザーには、Teams と Teams Phone（旧名 Microsoft 365 Phone System）を含むライセンスが要ります。Microsoft 365 E5 系なら、スタンドアロンの Teams Phone Standard を足す必要はありません。[^c1-44] Teams Phone の種類は3つで、それぞれ前提ライセンスの購入が要ります。

種類	備考
Teams Phone Standard	標準
Teams Phone Standard for Frontline Workers	前提は Microsoft 365 F1/F3 か Office 365 F3
Teams Phone with Calling Plan	通話プラン込み

PSTN は、Teams Phone ライセンスとは別物。Microsoft を PSTN 事業者にするなら、Microsoft Calling Plan ライセンスが追加で要ります。Shared Calling は、複数ユーザーが1つの番号を共有する方式で、ユーザー側は Teams Phone ライセンスだけで足ります（共有番号を持つリソース アカウントには、Teams Phone Resource Account ライセンスが要ります）。

リソース アカウントは、自動応答（Auto Attendant）や通話キューなど、音声アプリ用の専用アカウントです。Microsoft 365 アプリへのサインインには使えません。ライセンスは Microsoft Teams Phone Resource Account で、自動応答と通話キュー1つにつき1ライセンスです。Teams Phone を含むサブスクリプションにはゼロ円の割り当てがあり、不足分は有料で追加します。[^c1-45] 割り当ては、Microsoft 365 管理センターの Users > Active users の Licenses and Apps です。Teams Phone Standard から切り替える時は、旧ライセンスの削除と新ライセンスの追加を同じ操作で行います。

作成は Teams 管理センターの Voice > Resource accounts の Add。入れるのは、Display name、Username、Resource account type（Auto attendant か Call queue）です。必要なロールは2つあります。1つは User Administrator です。もう1つは、次のいずれかの Teams 管理者ロールです。

- Teams Telephony Administrator
- Teams Communications Administrator
- Teams Administrator

Teams デバイスのライセンス [1.5.2]

Teams Rooms のライセンスは Pro と Basic の2つです。[^c1-46]

項目	Basic	Pro
上限	組織で最大25（26台目から Pro）	なし
対象	Teams Rooms システムのみ。Teams Panels は不可	Rooms システムと Panels の両方
1部屋	1台の認定システム。同じ部屋で同じリソース アカウントを複数の Rooms システムにサインインさせるには Pro が要る	同じ部屋の複数の Rooms システム可（部屋をまたいで同じアカウントを使うのは Basic も Pro も規約違反）
管理機能	高度な機能は含まれない	リモート デバイス管理、条件付きアクセス、詳細なデバイス分析

SAMPLE

項目	Basic	Pro
含まれるサービス	含まれない	Teams Phone Standard、Intune、Entra ID P1、Defender for Endpoint Plan 2 など

Teams Rooms システムとは、Windows のコンピュート モジュールとタッチ コンソール、Android 端末とタッチ コンソール、Surface Hub のことです。共有の場所で会議に参加する共有会議デバイスは、サインイン、匿名参加、リソース アカウント認証のどれでも Rooms ライセンスが要ります。旧 Standard と Premium は期限まで使えますが、自動移行はありません。期限後は Pro（推奨）か Basic を購入します。

Teams Shared Space ライセンスは、2026年4月以前の名称が Shared Devices です。[^c1-47] 対象は、Teams Phone デバイス（共用エリア）、Teams panels、デスク ドック、共有デバイスとしての Android 携帯です。Teams Rooms では機能しません。

項目	内容
1ライセンスの効果	4つの予約可能デスクか BYOD ルームを有効化（8ドル）。1つを予約可能デスクか BYOD ルームに使うと、0ドルの Single Space ライセンスが3つ付き、残り3か所に割り当てる（合わせて4か所）。Single Space は予約可能デスク、BYOD ルーム、スペース分析に使うもので、デバイスには使えない
デバイス	1ライセンスで1台。デバイスに使うと Single Space は取れない

Teams デバイスの構成プロファイル [1.5.3]

構成プロファイルは、Android デバイスの設定を管理します。対象は、Teams Rooms on Android、Teams displays、Teams phone、Teams panels。作成は Teams Devices > デバイスの種類 > Configuration profiles の Add です。名前と説明、設定を入れ、Review changes から Save changes を選びます。[^c1-48] 新規プロファイルの設定は、すべて既定で Not configured です。

Partial application では、プロファイルで明示的に構成した設定だけが適用され、既存のデバイス設定は変わりません。Partial application に対応していないファームウェアのデバイス（OEM の対応表に載っていないもの）に割り当てると、未構成の設定も含め、すべてが既定値で適用されます。割り当ての手順は次のとおりです。

1. デバイスの種類を選ぶ
2. 1台以上を選び、Assign configuration を選ぶ
3. プロファイルを検索して Apply

編集は、割り当て済みのデバイスへ自動で適用されます。設定を変えずに再適用するには、Reassign config を使います。デバイスの設定の変更、再起動、更新管理に要るのは、Teams Administrator か Teams Devices Administrator。

TAC の構成プロファイルは、Pro Management Portal（PMP）の Settings Templates としてインポートできます。設計の基本は、設定の組み合わせごとにプロファイルを1つ作ること。命名規則を決め、要件が同じデバイスをまとめて、プロファイル数を最小にします。

SAMPLE

Teams Rooms のアカウントとシステム [1.5.4]

Teams Rooms は、Teams Rooms システムごとに専用のリソース アカウントが要ります（Pro で、同じ部屋の複数の Rooms システムに同じアカウントでサインインする場合を除く）。Teams Panels は、同じ部屋の Teams Rooms のリソース アカウントでサインインします。Teams デバイス用の Microsoft 365 リソース アカウントは、Exchange Online のメールボックスに結び付き、部屋の予約を可能にします。通話キューや自動応答用の Teams リソース アカウントとは別物です。[^c1-49]

要件は次のとおりです。

項目	内容
ライセンス	Teams Rooms Basic か Pro
パスワード	有効期限なし（Password never expires）が要件。Update-MgUser -PasswordPolicies DisablePasswordExpiration
UPN	SMTP アドレスと一致
時間帯	既定は Pacific Standard Time。設置場所に合わせる
初回サインイン時のパスワード変更	要求しない（要求するとサインインで問題が出る）
Exchange オンプレミス	予定表を読むためにハイブリッド構成が必須
セキュリティ	Entra の Security defaults には非対応。条件付きアクセスで保護（条件付きアクセスを使うテナントでは Security defaults を無効にする）

作成は、Microsoft 365 管理センターの Resources > Rooms & equipment > Add resource で名前、メール、容量を入れます。続けて Users > Active users で、パスワードをリセットしてライセンスを割り当てます。予約の既定は、繰り返し会議を許可、会議要求の自動承諾、予約期間180日、最大会議時間24時間。Set-CalendarProcessing は、AutomateProcessing を AutoAccept にします。ProcessExternalMeetingMessages を $true にするなどが推奨です。帯域幅ポリシーは 10 Mbps 以上が推奨です。

プラットフォームは2つです。Teams Rooms on Windows はコンピュート モジュールとタッチ コンソール。Teams Rooms on Android は Android 端末とタッチ コンソールです。

デバイスの設定とファームウェア [1.5.5]

Teams 管理センターでデバイスを選んで Update を選ぶと、ソフトウェアとファームウェアの更新を確認でき、入れるものを選べます。[^c1-48] Teams Rooms on Windows の設定変更は、Teams Devices > Teams Rooms on Windows の画面で行う。1台以上を選び、Edit settings を選びます。複数を選ぶと、変更値が全デバイスの値を置き換えます。再起動は、即時か Schedule restart で、日時はデバイスのローカル時刻。Queued や Scheduled の操作は History からキャンセルできますが、進行中と完了は不可です。

Teams で認定されたデバイスは、ユーザーが初めて Teams にサインインした時に自動登録されます。電話、Teams Rooms on Android、Teams displays、Teams panels は、Intune にサインアップ済みなら自動で Intune に登録されます。準拠確認と条件付きアクセスの対象になります。

PMP の更新の動きは次の表。

SAMPLE

項目	内容
更新のフェーズ（TAC）	Validation 0-15日、General 16-45日、Final 46-60日
更新のリング（PMP の既定）	Staging 0-6日、General 7-13日、Executive 14-20日（PMP の方が速い）

リングでの管理に切り替えると、TAC では管理できず、元に戻せません。

Teams デバイス タグ [1.5.6]

デバイス タグは、デバイスをグループ化して管理しやすくするもの。タグが付く先は、デバイスにサインインしているリソース アカウントです。アカウントを別のデバイスへサインインし直すと、タグも新しいデバイスに付きます。タグは最大25文字で、管理は Teams Administrator か Teams Devices Administrator です。[^c1-51]

操作は次のとおりです。

操作	方法
作成	デバイス ペインの Actions > All device tags で + Add
付与	デバイスを選び Manage tags。既存を選ぶか新規を追加して Apply
削除	付いている全デバイスから外してから。Untag devices で一括で外せる

フィルターは2通りです。Match all of these conditions は、指定した全タグを持つデバイスを返します。Match any one of these conditions は、いずれかを持つデバイスを返します。デバイス ペイン（Phones、Teams Rooms など）が返すのは、そのペインの種別のデバイスだけ。TAC のタグの取り込み先は、PMP のグループ。

新しいデバイスのリモート サインイン [1.5.7]

リモート プロビジョニングの流れは4段。[^c1-52]

1. IT 管理者が、MAC アドレスかハードウェア ID を Pro Management Portal に登録する
2. 確認コードを作る
3. 現地の人が、そのコードを Android デバイスに入れる
4. サインイン コードが PMP に出て、遠隔でサインインを完了する

対象は、Teams Rooms on Android、Teams panel、Teams phone、SIP gateway デバイスです。登録は PMP の Planning > Android Devices で Add（一括は Upload）します。入れるのは、ID の種類（macAddress か hardwareId）と ID、任意で場所です。登録したデバイスの表示は Ready for provisioning。確認コードは、一括でもデバイス単位でも作れます。有効期間は24時間。

現地では、設定の Provision device を選び、デバイス固有のコードを入れます。その後のデバイスは Waiting for sign in タブに出て、microsoft.com/devicelogin に表示されたコードでサインインを完了します。

サインアウトしたデバイスの再サインインは、PMP の Rooms で対象を選び、Account タブの Generate code でコードを作って行います。PMP へのアクセスに要るロールは2系統です。Entra ロールなら Global Administrator、

SAMPLE

Teams Administrator、Teams Devices Administrator、Global Reader。PMP 組み込みなら Teams Rooms Pro Manager、Site Lead、Site Technician です。

VDI 用の Teams [1.5.8]

新しい VDI ソリューションは、仮想デスクトップでマルチメディアの配信を最適化する新しいアーキテクチャです。[^c1-53] 構成要素は3つです。

要素	内容
SlimCore	メディア エンジン（OS 依存で VDI ベンダー非依存）。Teams のバージョンごとに自動更新されるMSIX（新しい分割パッケージでは Host 約 100 KB と Framework 約 60 MB）を、Microsoft の公開 CDN から配信
プラグイン	クライアント側の仮想チャネル DLL（約 600 KB）。SlimCore のダウンロードとクリーンアップを担う
Teams vdiBridge	サーバー側の仮想チャネル モジュール

最適化を制御するのは、VDI ポリシーの VDI2Optimization。既定は Enabled で、これが唯一の制御点です。ユーザーごとに止めるには、ポリシーを作って割り当てます。作成は New-CsTeamsVdiPolicy -VDI2Optimization "Disabled"、割り当ては Grant-CsTeamsVdiPolicy です。既定の VDI ポリシーは、DisableCallsAndMeetings と DisableAudioVideoInCallsAndMeetings がどちらも False。

従来の WebRTC ベースの最適化は、廃止が予定されています。対象は、Windows エンドポイントから Citrix と AVD/Windows 365 へのもの。時期は、2026年10月1日にサポート終了、2027年4月1日に提供終了です。新しい最適化が既定になります。

要件です。メディアは UDP 3478〜3481 と TCP 443/80、UDP 443 を使います。VM の要件は、Windows 10.0.19041 以上か、Windows Server 2022（20348.2402）以上・Windows Server 2025（26100.2886）以上（Windows Server 2022 は 2026 年 10 月のサポート終了が告知されています）。Server 2016 と 2019 は非対応です。

SAMPLE

サンプルはここまでです

続き(第2章〜巻末)は、MS-700 問題集のご購入で、頻出度別ノート・暗記用ノートと合わせて3点すべてダウンロードできます。

SAMPLE

MS-700 学習用テキスト(無料サンプル)

版
2026年11月版(MS-700 出題範囲(Skills measured)2026-10-27版 準拠)

発行
IT資格道場(https://www.shikaku-doujou.com)

お問い合わせ
info@shikaku-doujou.com

Microsoft、Microsoft 365、Microsoft Teams、Microsoft Entra、Windows および Microsoft の製品名・サービス名は、Microsoft Corporation の米国およびその他の国における商標または登録商標です。記載されているその他の会社名・製品名・サービス名は、各社の商標または登録商標です。

本教材は公式シラバスの内容を基に作成したもので、Microsoft Corporation との提携・承認関係はありません。

本文・図表・設問はすべてオリジナルの著作物です。無断での転載・複製・再配布・二次販売はできません。お気づきの点は info@shikaku-doujou.com までご連絡ください。

SAMPLE