IT資格道場

SC-300 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)

SC-300 出題範囲(Study guide・Skills measured as of 2026-04-27)準拠
2026年7月版

本書のご利用にあたって

- 本書は「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。
- 無料サンプルであっても著作物です。本書の転載・改変しての再配布・二次販売を禁じます。
- 本書を AI モデルの学習データとして利用すること(学習目的の入力・データセット化を含む)を禁じます。
- 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。

不正な配布を見つけた場合は info@shikaku-doujou.com までご連絡ください。

目次

この教材群の使い方(3点セット)

種類	役割
① 学習用テキスト(本書)	これだけで問題が解けるようになる本編
② 頻出度別ノート	テキストを読んだら次はこれ。頻出順に絞った問題と解説で「解ける」に橋渡し。試験直前の最終チェックにも
③ 暗記用ノート	覚えるべき要点だけを一問一答に凝縮。空き時間の反復と用語の再確認用

使い方: 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。

このテキストの位置づけ: 本書は①の学習用テキストです。まずはここを通読し、これだけで問題が解けるようになることを目標にしてください。

はじめに ―― この教材の使い方

このテキストは、Microsoft が実施する **Exam SC-300: Microsoft Identity and Access Administrator**（認定名 **Microsoft Certified: Cloud and AI Security Engineer Associate**）に合格することを目的に作られています。

Associate 級が問うのは「Microsoft Entra ID とは何か」ではなく、**与えられた要件（誰に・何を・どの条件で・いつまで許すか、誰が承認し、どう見直すか）のもとで、どの機能をどう構成すれば満たせるか**です。公式の Study guide は 4 つの主題（ユーザー ID の実装と管理／認証とアクセス管理の実装／ワークロード ID の計画と実装／ID ガバナンスの計画と自動化）から成り、本書はそ

の順番どおりに第1章〜第4章を置いています。ハイブリッド ID（Connect Sync・Cloud Sync）、Conditional Access と認証強度、Global Secure Access、ワークロード ID、entitlement management と access reviews が、この試験の背骨です。

本書は Microsoft の公式教材ではなく、IT資格道場が独自に書き下ろしたオリジナルの教材です。実際に出題された問題を再現したものではありません。

試験の基本情報

項目	内容
試験名	Exam SC-300: Microsoft Identity and Access Administrator
認定	Microsoft Certified: Cloud and AI Security Engineer Associate
運営	Microsoft（Pearson VUE のテストセンター、またはオンライン監督試験）
試験時間	**100分**
合格ライン	**700 / 1,000**
受験言語	**日本語あり**（英語ほか全10言語で提供）

Microsoft は問題数と出題形式の内訳を公表していません（「対話型の要素を含むことがある」とだけ案内しています）。**受験料・試験時間・出題範囲は改定されることがあります。** お申し込みの前に、Microsoft Learn の公式ページで最新の情報をご確認ください。

試験は英語で出題されます —— 本書の書き方

本書は日本語で書いていますが、**サービス名・機能名・設定項目名は英語表記のまま**にしています（例：Conditional Access、Privileged Identity Management (PIM)、Just-in-time (JIT) VM access、Data collection rules (DCR)）。本番の設問文・選択肢に出るのはこの英語表記であり、日本語訳を覚えても画面には出てきません。本文を読みながら、英語の名前を見た瞬間に「どの主題の、どの場面の機能か」が出る状態を作ってください。

なお、公式 Study guide は「希望する言語で試験が提供されていない場合は、追加で 30 分を申請できる」と案内しています（「If the exam isn't available in your preferred language, you can request an additional 30 minutes to complete the exam.」）。SC-300 は英語のみの提供なので、日本語を希望する受験者はこの延長を申請できます。申請の手順と適用条件は、お申し込み時に Microsoft Learn の公式ページでご確認ください。

出題範囲の全体像 —— 4つの主題と本書の章

主題	分野	採点対象に占める割合（公式）	本書
1	ユーザー ID の実装と管理	**20–25%**	第1章
2	認証とアクセス管理を実装する	**25–30%**	第2章
3	ワークロード ID の計画と実装	**20–25%**	第3章
4	ID ガバナンスの計画と自動化	**20–25%**	第4章

本書の章の並びは、Study guide の並びとまったく同じです。節見出しの末尾にある `[1.1]` のような番号は、Study guide の到達目標（Skills measured）の番号です。Microsoft は主題ごとの割合を幅で公表しており、到達目標単位の出題数は公表していません。本書もそれ以上の数字は書きません。

全設問に効く判断軸 ——「3つの問い」

問い	何を切り分けるか	分かれ方
問い1: 誰の ID の話か	従業員／外部ユーザー（B2B）／ワークロード（アプリ・マネージド ID）／管理者	同じ「アクセスを制御する」でも、Conditional Access・Cross-tenant access settings・app roles・PIM は対象が違い、要件が誰を指しているかで答えが決まります
問い2: 認証か、認可か、ガバナンスか	本人確認（MFA・パスワードレス）／許可の付与（ロール・同意・CA）／見直しと期限（PIM・access reviews・entitlement management）	「定期的に見直したい」に認証系の機能を選ぶ肢は誤答です
問い3: 最小権限・最小露出で満たせているか	スコープ・期間・経路	要件を満たす案が複数あるとき、正解はより狭いスコープ・より短い期間・より閉じた経路のものです

4ステップ学習法

購入者限定テキストは3冊で1セットです。

- **STEP 1（理解する）**：本書「学習用テキスト」を通読し、4つの主題の地図と3つの問いを頭に入れる
- **STEP 2（解き方を掴む）**：「頻出度別ノート」で頻出度の高い論点を解いて、解き方を掴む
- **STEP 3（腕試し）**：本サイトの問題演習で、択一・問題と解決策（はい/いいえ）・組み立て式に慣れる
- **STEP 4（再確認）**：「頻出度別ノート」に戻って総ざらい。試験直前もここへ戻る

「暗記用テキスト」は本線には入れません。通勤時間や休憩時間など、**空き時間の反復と用語の再確認**に並走させてください。

それでは、第1章から始めます。

第1章 ユーザー ID の実装と管理(ドメイン1・採点対象の 20–25%)

この章は SC-300 の土台にあたる分野です。テナントそのものの設定、ユーザーとグループ、外部ユーザー、そしてオンプレミスの Active Directory とのハイブリッド構成 —— これ以降の章(認証とアクセス管理、ワークロード ID、ID ガバナンス)は、すべてこの章で作った土台の上に載ります。

問われるのは「Microsoft Entra ID とは何か」ではありません。**与えられた要件(委任の範囲・ライセンス・オンプレミスの制約・監査要件・可用性)のもとで、どう構成すれば要件を満たすか**です。

同じ「ユーザー ID」という言葉でも、Fundamentals 系の試験と SC-300 では問われ方が違います。前者は「administrative unit とは何ですか」と聞き、SC-300 は「**この委任要件を満たすのは administrative unit か、カスタムロールか、restricted management administrative unit か。なぜ他の2つでは要件を満たさないか**」と聞きます。したがって本章では、機能ごとに次の4つをそろえて覚えます。

1. **できること**(機能の定義)
2. **できないこと・制約**(誤答肢はここを突いてきます)
3. **必要なライセンスとロール**(「P1 が要るか」「Global Administrator で足りるか」が正誤を分ける)
4. **他の候補との分かれ目**(どの条件で選択が切り替わるか)

出題は択一と複数選択に加え、「問題と解決策」形式(提示された解決策で目的を達成できるか はい/いいえ)、対応付け、並べ替えが混在します。**問題と解決策形式では、同じシナリオが3回連続で提示され、解決策だけが差し替わり**

ます。3問とも「はい」のことも3問とも「いいえ」のこともあるため、前の問題の答えを根拠にしないでください。

シナリオの最後の1〜2文に「**最小限の管理作業で**」「**最小特権の原則に従って**」「**追加のライセンスを購入せずに**」といった評価軸が置かれます。技術的に正しい選択肢が複数並ぶのが普通で、**評価軸に照らして最良のものだけが正解**です。

1-1 Microsoft Entra テナントを構成して管理する [1.1]

1-1-1 テナントと管理の入口 —— この節の全体像 [1.1]

Microsoft Entra テナントは、組織のディレクトリの境界そのものです。ユーザー・グループ・デバイス・アプリケーション・ロールは、すべて1つのテナントに属します。この節で扱うのは、**テナント全体にかかる設定**と、**その設定を誰にどこまで任せるか(委任)**の2つです。

到達目標 1.1 の箇条書きは、次の3つのかたまりに整理できます。

かたまり	対応する箇条書き	中心となる問い
委任の設計	built-in and custom Microsoft Entra roles / administrative units をいつ使うか / administrative units の構成 / effective permissions の評価	「誰に、何を、どの範囲まで許すか」
組織の名前空間	domains の構成 (Microsoft Entra ID と Microsoft 365)	「このテナントはどのドメイン名を名乗るか」

かたまり	対応する箇条書き	中心となる問い
利用者から見えるもの・既定の振る舞い	Company branding settings / tenant properties, user settings, group settings, device settings	「サインイン画面と既定の権限をどう作るか」

1-1-2 組み込みロールとカスタムロールの構成と管理(built-in and custom Microsoft Entra roles)[1.1]

Microsoft Entra roles は、Microsoft Entra ID のリソース(ユーザー・グループ・アプリケーションなど、Microsoft Graph API 経由で扱う対象)へのアクセスを制御します。これは **Azure roles**(Azure RBAC)とは別系統の仕組みです。ここは最初に必ず切り分けておきます。

観点	Microsoft Entra roles	Azure roles(Azure RBAC)
制御する対象	Microsoft Entra ID のリソース(users、groups、applications)	Azure のリソース(仮想マシン、ストレージ アカウントなど)
経由する API	Microsoft Graph API	Azure Resource Manager
スコープ	テナント / administrative unit / Microsoft Entra リソース(グループ、エンタープライズ アプリケーション、アプリの登録)	管理グループ / サブスクリプション / リソース グループ / リソース
アクセス許可の相互流用	**不可**。Microsoft Entra ロールのアクセス許可を Azure カスタムロールに入れることはできない	**不可**。逆も同じ

> **よく出る取り違え**: 「User Administrator を割り当てたのに、仮想マシンを作れない」は仕様どおりです。Microsoft Entra ロールは Azure リソースを触れません。逆に「Owner(Azure ロール)を持っているのに、ユーザーのパスワードをリセットできない」も仕様どおりです。

ロール定義とロール割り当ての2段構えを理解しておきます。ロール割り当ては、次の3つの要素からできています。

要素	意味	取りうる値
セキュリティ プリンシパル	アクセス許可を受け取る側	ユーザー / **role-assignable group**(ロール割り当て可能グループ)/ サービス プリンシパル
ロール定義	アクセス許可の集まり	built-in role(変更不可) / custom role
スコープ	アクセス許可が及ぶ範囲	テナント / administrative unit / Microsoft Entra リソース

built-in roles(組み込みロール) は Microsoft が用意した固定のロールで、**定義を変更できません**。使用は**無料**です。一方 **custom roles(カスタムロール)** は、あらかじめ用意されたアクセス許可の一覧から必要なものだけを選んで作る独自のロールで、**カスタムロールの割り当てを受けるユーザーごとに Microsoft Entra ID P1 ライセンスが必要**です。

カスタムロールを作る手順は2段階です。**まずロール定義を作り、次にそれをスコープつきで割り当てる**。定義は1つ作っておけば、異なるスコープで何度でも割り当てられます —— この分離が、「開発者 A には Contoso 経費精算ア

プリだけ、開発者 B にはテナント内の全アプリ」という使い分けを可能にします。

試験で押さえるべき組み込みロールを、機能ごとに整理します。

ロール	できること	分かれ目
Global Administrator	ほぼすべての管理操作。他ユーザーへのロール割り当ても可能	最小特権の原則に反するため、シナリオで「最小特権」が評価軸なら**ほぼ確実に誤答肢**
Privileged Role Administrator	ロールの割り当て・削除、カスタムロールの作成、administrative unit の管理、PIM の設定	「ロールを割り当てる権限だけを渡したい」ならこれ。Global Administrator は不要
User Administrator	ユーザーとグループの全般管理。限定管理者のパスワード リセットを含む	ユーザー作成・削除・ライセンス割り当てまで。ロールの割り当ては範囲外
Helpdesk Administrator	非管理者のパスワード リセット	administrative unit スコープと組み合わせる定番。**管理者ロールを持つユーザーのパスワードはリセットできない**
Password Administrator	非管理者のパスワード リセット	Helpdesk Administrator より狭い(サービス要求などができない)
Authentication Administrator	非管理者の認証方法の参照・設定・リセット	MFA の再登録要求などに使う
Privileged Authentication Administrator	**管理者を含む全ユーザー**の認証方法の参照・設定・リセット	「Global Administrator の MFA をリセットしたい」の正解

ロール	できること	分かれ目
Groups Administrator	グループの全般管理	administrative unit スコープに割り当て可能
License Administrator	ライセンスの割り当て・削除・更新	ライセンスだけを任せたいときの最小特権解
Domain Name Administrator	ドメイン名の管理	ドメインの追加・検証・削除の**最小特権ロール**
Organizational Branding Administrator	Company branding の構成	ブランド設定の**最小特権ロール**
External Identity Provider Administrator	外部 ID プロバイダー(SAML/WS-Fed など)と外部コラボレーション設定の構成	1.3 で再登場
Guest Inviter	ゲストの招待のみ	「招待だけさせたい」の最小特権解
Hybrid Identity Administrator	ハイブリッド ID の構成(Connect、staged rollout)	1.4 で再登場
Attribute Definition Administrator	custom security attributes の定義	1.2 で再登場。**Global Administrator は既定で権限を持たない**
Attribute Assignment Administrator	custom security attributes の割り当て	同上
Cloud Device Administrator	デバイスの有効化・無効化・削除、BitLocker 回復キーの参照	administrative unit スコープに割り当て可能
Tenant Creator	新しいテナントの作成	非管理者のテナント作成を制限した後、特定ユーザーにだけ許すときに使う

ロール	できること	分かれ目
Directory Readers	ディレクトリの読み取り	サービス プリンシパルやゲストに administrative unit スコープのロールを使わせるとき、**テナント スコープで別途必要**になる

role-assignable group(ロール割り当て可能グループ) は、ロールをグループに割り当てるための特別なグループです。**Microsoft Entra ID P1 が必要**で、作成時に「Microsoft Entra ロールにこのグループを割り当てることができる」を有効にしなければならず、**後から変更できません**。また、**メンバーシップは割り当て(Assigned)である必要があり、動的メンバーシップは使えません**。これは「グループのルールを書き換えるだけで特権を奪える」経路を塞ぐための設計です。

> **よく出る取り違え**:「既存のセキュリティ グループにロールを割り当てたい」→ 一覧に出てこないのは仕様です。role-assignable group として**新規に作り直す**必要があります。動的メンバーシップ グループを role-assignable にすることもできません。

カスタムロールを選ぶべき場面は次の2つに絞られます。

1. **組み込みロールでは広すぎる**。たとえば「アプリの登録の資格情報だけを更新させたい」場合、Application Administrator は広すぎます。
2. **スコープを単一リソースに絞りたい**。たとえば「Contoso Widget Builder というアプリの登録1つだけを管理させたい」場合です。

スコープの書き方は、対応付け・並べ替え問題の根拠になるので厳密に覚えます。Microsoft Graph でロール割り当てを作るときの `directoryScopeId` は

次のとおりです。

スコープ	directoryScopeId の値	意味
テナント全体	`/`	テナント内の全オブジェクト
administrative unit	`/administrativeUnits/<AU の ID>`	**その AU の "メンバー" を管理できる**(AU 自体ではない)
単一の Microsoft Entra リソース	`/<オブジェクト ID>`	**そのオブジェクト自体を管理できる**(グループの場合、メンバーであるユーザーには及ばない)

> **落とし穴**: `/administrativeUnits/<ID>` と `/<ID>` の違いは意図的な設計です。前者は「箱の中身」、後者は「その物自体」。**コンテナー スコープ(テナント、AU)はコンテナー内のオブジェクトに対する権限を与えるが、コンテナー自体への権限は与えない**。逆に**リソース スコープはそのリソース自体への権限を与えるが、その先(グループのメンバー)には及ばない**。

コンテナー スコープ(テナント、AU)は中のオブジェクトへの権限を与えるが、
コンテナー自体への権限は与えない。
リソース スコープはそのリソース自体への権限を与えるが、
その先(グループのメンバー)には及ばない。

図 1-1　ロール割り当ての3要素と、スコープの書き方(directoryScopeId)

ロールの割り当て方には3つの選択肢があり、必要なライセンスが違います。

方法	必要ライセンス	特徴
ユーザーへの直接割り当て	不要(組み込みロールの場合)	既定の方法。恒久的にアクティブ
role-assignable group への割り当て	**Microsoft Entra ID P1**	グループの出入りで権限を付け外しできる。一貫性が保てる
Privileged Identity Management (PIM) による割り当て	**Microsoft Entra ID P2**	**eligible(対象)割り当て**による just-in-time の昇格、期限付き割り当て、承認、監査

> **分かれ目**:「管理者権限を常時保持させたくない」「昇格時に承認と理由入力を求めたい」なら **PIM(P2)**。「グループの操作で権限を管理したい」だけなら **role-assignable group(P1)**。前者を P1 で実現しようとする選択肢は誤答です。

ロール割り当ての作成・一覧表示は、**Microsoft Entra admin center**、**Microsoft Graph PowerShell**、**Microsoft Graph API** で行えます。**Azure CLI は Microsoft Entra のロール割り当てに対応していません** —— これは「PowerShell と CLI のどちらでもできる」と書かれた選択肢を切るための知識です。

PowerShell での典型的な流れは次のとおりです。

```
Connect-MgGraph -Scopes "RoleManagement.ReadWrite.Directory"
$user = Get-MgUser -Filter "userPrincipalName eq 'alice@contoso.com'"
$roleDefinition = Get-MgRoleManagementDirectoryRoleDefinition -Filter
"displayName eq 'User Administrator'"
$adminUnit = Get-MgDirectoryAdministrativeUnit -Filter "displayName eq
'Seattle Admin Unit'"
$directoryScope = '/administrativeUnits/' + $adminUnit.Id
New-MgRoleManagementDirectoryRoleAssignment -DirectoryScopeId
$directoryScope -PrincipalId $user.Id -RoleDefinitionId
$roleDefinition.Id
```

1-1-3 administrative units をいつ使うか(Recommend when to use administrative units)[1.1]

administrative unit(管理単位、AU) は、Microsoft Entra のリソースを入れる**コンテナー**です。中に入れられるのは **users、groups、devices の3種類だけ**です。

AU の目的はただ一つ —— **ロールのアクセス許可を、組織の一部分に限定すること**です。逆に言えば、**AU に属していないユーザーにロールを割り当てると、そのロールのスコープはテナント全体になります。**

推奨する典型シナリオを場面で押さえます。

場面	なぜ AU が答えになるか
大学に複数の独立した学部があり、学部ごとに IT 管理チームがいる	学部ごとに AU を作り、学部の学生と職員を入れ、その AU スコープで User Administrator を割り当てる。**他学部のユーザーは管理できない**
IT 部門が地理的に分散していて、地域ごとに Helpdesk がいる	地域ごとに AU を作り、Helpdesk Administrator を AU スコープで割り当てる。**担当地域のユーザーのパスワードだけリセットできる**
合併で半自律的な子組織が複数ある	子組織ごとに AU を作る

ユーザーは**複数の AU のメンバーになれます。**地理(Seattle)と部門(Marketing)の両方の AU に同じユーザーが入る、という設計は正しい使い方です。

AU の制約を押さえます。誤答肢はここを突いてきます。

- **AU は入れ子にできません**(nested administrative units は不可)。

- **AU は Microsoft Entra ID Governance では現在利用できません。**
- **AU にグループを入れると、管理対象になるのはグループそのものであって、グループのメンバーではありません。**
- **AU は管理アクセス許可のスコープを限定するだけで、既定のユーザー権限による閲覧を止めるものではありません。**AU 外のユーザーやグループを一覧で見ること自体は止められません(Microsoft 365 管理センターでは絞り込まれますが、Microsoft Entra admin center や PowerShell では見えます)。

> **よく出る取り違え(最重要)**:「Sales グループを AU に入れて User Administrator を割り当てたので、Sales グループのメンバーのパスワードをリセットできる」—— **できません。**グループを AU に入れると管理できるのは**グループ名とグループのメンバーシップ**だけです。メンバーであるユーザーのプロパティ・認証方法・パスワードを管理するには、**そのユーザー自身を AU のメンバーとして直接追加する**必要があります。

この違いを表にすると次のとおりです(AU にグループだけを入れ、User Administrator を AU スコープで割り当てた場合)。

操作	可否
グループの名前を管理する	可
グループのメンバーシップを管理する	可
グループの**個々のメンバー**のユーザー プロパティを管理する	不可
グループの**個々のメンバー**の認証方法を管理する	不可

操作	可否
グループの**個々のメンバー**のパスワードをリセットする	不可

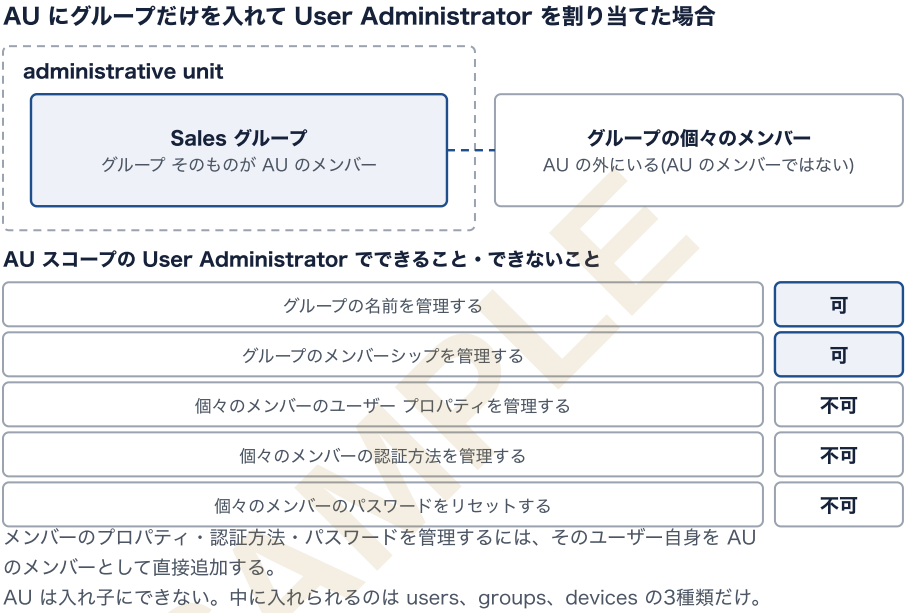

図 1-2　AU にグループだけを入れて User Administrator を割り当てた場合

ライセンス要件は3層に分かれています。ここは「追加のライセンス購入なしで」という評価軸のシナリオで効きます。

対象	必要ライセンス
AU を**作成**する	Microsoft Entra ID Free
AU スコープでディレクトリ ロールを**割り当てられる管理者**	**Microsoft Entra ID P1**(管理者1人につき1つ)
AU の**メンバー**	Microsoft Entra ID Free

対象	必要ライセンス
動的メンバーシップ ルールで AU のメンバーを決める場合の AU メンバー	**Microsoft Entra ID P1**(メンバー1人につき1つ)

1-1-4 administrative units の構成と管理 [1.1]

AU の作成・メンバー追加・ロール割り当ては、**Microsoft Entra admin center**、**PowerShell**、**Microsoft Graph API** で行えます。実施には **Privileged Role Administrator** が必要です。

構成の順序は並べ替え問題の定番です。

1. **AU を作成する**(Entra ID > Roles & admins > Admin units)
2. **メンバーを追加する**(users、groups、devices を手動、または動的メンバーシップ ルールで)
3. **AU スコープでロールを割り当てる**(AU の「Roles and administrators」から)
4. 割り当てた管理者に **Microsoft Entra ID P1 ライセンス**があることを確認する

メンバーの入れ方には手動と動的の2つがあり、対応状況が違います。

操作	Microsoft Graph / PowerShell	Microsoft Entra admin center	Microsoft 365 管理センター
AU の作成・削除	可	可	可
メンバーの追加・削除	可	可	可
AU スコープの管理者の割り当て	可	可	可

操作	Microsoft Graph / PowerShell	Microsoft Entra admin center	Microsoft 365 管理センター
ルールによる users または devices の動的な追加・削除	可	可	**不可**
ルールによる groups の動的な追加・削除	**不可**	**不可**	**不可**

> **よく出る取り違え**:「グループを動的ルールで AU に自動追加したい」――**できません**。動的メンバーシップ ルールで AU に入れられるのは **users と devices だけ**です。

AU スコープに割り当てられる主なロールは次のとおりです。加えて、**users・groups・devices のいずれかに関係するアクセス許可を1つ以上含むカスタムロール**なら AU スコープに割り当てられます。

ロール	AU スコープでできること
Authentication Administrator	AU 内の**非管理者**の認証方法の参照・設定・リセット
Privileged Authentication Administrator	**管理者を含む**全ユーザーの認証方法の参照・設定・リセット
Attribute Assignment Administrator / Reader	AU 内のユーザーとサービス プリンシパルの custom security attributes の更新 / 読み取り
Cloud Device Administrator	AU 内のデバイスの管理
Groups Administrator	AU 内のグループの全般管理

ロール	AU スコープでできること
Helpdesk Administrator / Password Administrator	AU 内の**非管理者**のパスワード リセット
License Administrator	AU 内のライセンス割り当ての管理
Printer Administrator	プリンターとコネクタの管理
SharePoint Administrator	AU 内の Microsoft 365 グループの管理 (**SharePoint 管理センターは使えない**)
Teams Administrator	AU 内の Microsoft 365 グループの管理 (**Teams 管理センターは使えない**)
User Administrator	AU 内のユーザーとグループの全般管理

AU スコープのロールには、対象が管理者だった場合に制限がかかる操作があります。次の操作は、**対象ユーザーが何らかのロールを持つ管理者の場合、実行できません。**

- ユーザーの認証方法の読み取りと変更
- ユーザーのパスワードのリセット
- 電話番号・代替メール アドレス・OAuth シークレット キーなど機微なプロパティの変更
- ユーザー アカウントの削除または復元

AU スコープに割り当てられるセキュリティ プリンシパルは、ユーザー、role-assignable group、サービス プリンシパルの3つです。ただし、**サービス プリンシパルとゲスト ユーザーは、既定でディレクトリの読み取り権限を持たない**ため、AU スコープのロールだけでは実際には操作できません。**テナント スコープで Directory Readers(または読み取りを含む別のロール)を追加で割**

り当てる必要があります。ディレクトリ読み取り権限を AU スコープに限定することは現時点でできません。

restricted management administrative units(制限付き管理単位)

通常の AU が「**一部の管理者に、一部のオブジェクトを管理させる**」ための仕組みなのに対し、**restricted management administrative unit** は「**指定した管理者以外の全員から、オブジェクトを守る**」ための仕組みです。向きが逆です。

使う場面は次のとおりです。

- 役員アカウントとそのデバイスを、Helpdesk Administrator によるパスワード リセットや BitLocker 回復キー参照から守りたい
- 特定の国・地域の管理者だけがリソースを管理できる、というコンプライアンス統制を実装したい
- 機微なアプリケーションへのアクセスを制御しているセキュリティ グループを、テナント全体のグループ管理者から守りたい

誰がオブジェクトを変更できるかが最大の論点です。

ロール	スコープ	制限付き AU 内のオブジェクトを変更できるか
Global Administrator	テナント	**不可**
Privileged Role Administrator	テナント	**不可**
Groups Administrator / User Administrator など	テナント	不可
グループやデバイスの**所有者**	—	不可

ロール	スコープ	制限付き AU 内のオブジェクトを変更できるか
AU スコープに割り当て可能なロール	**その制限付き AU**	**可**
AU スコープに割り当て可能なロール	別の**制限付き** AU(対象オブジェクトがそのメンバー)	可
AU スコープに割り当て可能なロール	別の**通常の** AU(対象オブジェクトがそのメンバー)	不可

> **これが最も出る一点**: **Global Administrator でも、制限付き AU 内のオブジェクトは変更できません**。ただし Global Administrator と Privileged Role Administrator は、**制限付き AU 自体は管理できます** —— 作成・削除、メンバーの追加・削除、AU スコープのロール割り当て、そして**自分自身をその AU スコープのロールに割り当てること**ができます。この自己割り当ては**監査可能なイベント**として記録されます。

ブロックされる操作と、されない操作を切り分けます。制限が及ぶのは**Microsoft Entra のプロパティを直接変更する操作**だけで、Microsoft 365 サービス側の関連オブジェクトへの操作には及びません。

操作	ブロック	許可
UPN や写真などの標準プロパティの**読み取り**		可
ユーザー・グループ・デバイスの Microsoft Entra プロパティの変更	不可	
ユーザー・グループ・デバイスの削除	不可	

操作	ブロック	許可
ユーザーのパスワード更新	不可	
制限付き AU 内のグループの所有者・メンバーの変更	不可	
制限付き AU 内のユーザー等を、**他のグループに追加**する		可
Exchange でメールとメールボックス設定を変更する		可
Intune でデバイスにポリシーを適用する		可
SharePoint でグループをサイト所有者に追加・削除する		可
ライセンスの割り当てと usage location の更新		可

メンバーにできるオブジェクトの種類も通常の AU と違います。

オブジェクトの種類	通常の AU	制限付き AU
Users	可	可
Devices	可	可
Groups(セキュリティ)	可	可
Groups(Microsoft 365)	可	**不可**
Groups(メールが有効なセキュリティ)	可	**不可**

オブジェクトの種類	通常の AU	制限付き AU
Groups(配布)	可	**不可**

制限と注意点は次のとおりです。

- **制限付きの設定は AU の作成時にのみ指定でき、作成後に変更できません。**
- 制限付き AU 内のグループとユーザーは、**Privileged Identity Management、entitlement management、lifecycle workflows、access reviews といった Microsoft Entra ID Governance の機能で管理できません。**
- role-assignable group を制限付き AU に入れると、**そのメンバーシップを変更できなくなります。**所有者は管理できず、Global Administrator と Privileged Role Administrator も(AU スコープに割り当てられないため)変更できません。
- **Global Administrator を制限付き AU に入れると、そのユーザーのパスワードを誰もリセットできなくなります**(Global Administrator のパスワードをリセットできるロールが AU スコープに割り当てられないため)。いったん AU から外す必要があります。
- 制限付き AU を削除しても、**元メンバーからすべての保護が外れるまで最大30分かかります。**
- **1つのテナントにつき制限付き AU は最大100個**です。
- **アプリケーションは既定で制限付き AU 内のオブジェクトを変更できません。**Microsoft Graph のアプリケーション アクセス許可を与えても適用されず、**その制限付き AU のスコープでアプリケーションに Microsoft Entra ロールを割り当てる**必要があります。

- ライセンス要件は通常の AU と同じで、**管理者ごとに Microsoft Entra ID P1**、メンバーは Free です。

制限付き AU に関する操作は監査ログに記録されます。AU の作成時は `IsMemberManagementRestricted` = true が、カテゴリ `AdministrativeUnit` の「Add administrative unit」として残ります。

1-1-5 Microsoft Entra ロールの有効なアクセス許可の評価 (Evaluate effective permissions)[1.1]

「このユーザーは結局どこまでできるのか」を答えるのが effective permissions の評価です。**アクセスは1本の割り当てだけでは決まりません**。

Microsoft Entra ID がアクセス可否を判定する流れは次のとおりです。

1. ユーザー(またはサービス プリンシパル)が Microsoft Graph エンドポイント向けのトークンを取得する
2. そのトークンで Microsoft Graph 経由の API 呼び出しを行う
3. Microsoft Entra ID が、アクセス トークンの `wids` **クレーム**に基づいてロール メンバーシップを評価する、または**対象リソースに適用される全ロール割り当て(直接・グループ経由の両方)**を取得する
4. API 呼び出しの操作が、そのリソースに対して持つロールに含まれるかを判定する
5. 要求されたスコープでその操作を持つロールがなければ、アクセスは許可されない

したがって effective permissions を出すには、**次の3つを全部集める**必要があります。

集めるもの	どこで見るか
直接のロール割り当て	Entra ID > Roles & admins。**CSV としてダウンロード**できる。Microsoft Graph の List unifiedRoleAssignments でも取得可
グループ経由の間接的なロール割り当て	role-assignable group のメンバーシップをたどる
スコープ(テナント / AU / リソース)	各ロール割り当ての `directoryScopeId`

「誰が何にアクセスできるか」を組織全体で把握するには、ロール割り当てだけでは足りません。次の道具を組み合わせます。この対応関係は対応付け問題の材料になります。

見たいもの	使う道具
テナント/アプリ/AU スコープで Microsoft Entra ロールを持つ人	ロール割り当ての一覧(CSV ダウンロード、Graph API)
あるエンタープライズ アプリケーションにアクセスできるユーザーとグループ	アプリへのユーザーとグループの割り当て
ユーザーまたは管理者が同意した委任アクセス許可とアプリケーション アクセス許可	アプリケーションに付与されたアクセス許可のレビュー
ビジネス属性から見たアクセスの棚卸し	**custom security attributes** によるタグ付けとフィルター
現在も必要かどうかの定期確認	**access reviews**(Microsoft Entra ID Governance または Microsoft Entra Suite。一部機能は P2 でも動作)、**PIM access reviews**
access package 経由で付与されたアクセス	**entitlement management**
実際にアクセスした人と、その条件	**sign-in logs**

見たいもの	使う道具
ロール割り当てやグループ メンバーシップの**変更履歴**	**audit logs**

> **切り分けの一言**: **audit logs は構成の変更を記録し、sign-in logs はサインイン イベントを記録します**。「権限を与えられたこと」と「実際に行使されたこと」を区別するには両方が要ります。大規模テナントでは Log Analytics ワークスペースにログをストリーミングして分析します(詳細は 4.4)。

AU スコープでの実効権限を評価するときの注意を再掲します。

- AU スコープのロールは**AU のメンバーに対してのみ**効き、**テナント全体の設定や構成には及びません**。たとえば AU スコープの Groups Administrator は、AU 内のグループを管理できますが、**有効期限ポリシーやグループ名前付けポリシーといったテナント レベルのグループ設定は変更できません**。
- 対象が管理者ロールを持つユーザーの場合、パスワード リセットなどの操作は制限されます。
- ユーザーが AU に属していなければ、そのユーザーへのロール割り当てのスコープは**テナント全体**です。

1-1-6 Microsoft Entra ID と Microsoft 365 のドメインの構成と管理 [1.1]

ドメイン名は、ユーザー名やメール アドレスの一部であり、グループのアドレスの一部であり、アプリケーションの App ID URI の一部にもなります。

テナントを作成すると、`<組織名>.onmicrosoft.com` **という初期ドメイン**が自動で作られ、これが最初の**プライマリ ドメイン**になります。プライマリドメインは、**新しいユーザーを作るときの既定のドメイン名**です。

カスタム ドメインの追加と検証の手順は並べ替え問題の定番です。

1. Entra ID > Domain names > Custom domain names でドメイン名を追加する
2. Microsoft Entra ID が表示する **TXT レコード(または MX レコード)** を、DNS ホスティング プロバイダーに登録する
3. Microsoft Entra ID で検証(Verify)を実行する
4. 必要なら **Make primary** でプライマリドメインに変更する

必要なロールは Domain Name Administrator です —— ドメイン管理の最小特権ロールとして覚えます。Global Administrator でもできますが、最小特権が評価軸なら誤答です。

数の上限を覚えます。

条件	上限
マネージド ドメイン名	**5,000**
全ドメインをオンプレミス Active Directory とのフェデレーション用に構成する場合	各組織あたり **2,500**

サブドメインの扱いは頻出です。`europe.contoso.com` を追加したい場合、**まずルート ドメイン** `contoso.com` **を追加して検証すれば、Microsoft Entra ID がサブドメインを自動で検証します。**ただし、`contoso.com` **を別のテナントで既に検証済みの場合**は、`europe.contoso.com` を自分のテナントで検証できます —— このときは TXT レコードの追加を求められます。

プライマリ ドメインの変更については次の2点を押さえます。

- プライマリ ドメインにできるのは、**検証済みで、かつフェデレーションされていない**カスタム ドメインです。
- **プライマリ ドメインを変更しても、既存ユーザーのユーザー名は変わりません。**

ドメインの削除は、「削除できない理由」を問う形で出ます。次のいずれかに該当すると削除できません。

- そのドメイン名を含む**ユーザー名・メール アドレス・プロキシ アドレス**を持つユーザーがいる
- そのドメイン名を含む**メール アドレスまたはプロキシ アドレス**を持つグループがある
- そのドメイン名を含む **App ID URI** を持つアプリケーションがある

また、**削除操作を実行するアカウント自身が、削除しようとしているドメイン名を使っていてはいけません。**`admin@contoso.com` で `contoso.com` は削除できません。`admin@contoso.onmicrosoft.com` のような初期ドメインまたは別のカスタム ドメインのアカウントでサインインし直します。削除は非同期のバックグラウンド処理で、**完了まで最大24時間**かかることがあります。

ForceDelete オプションは、参照を一括で初期ドメインへ書き換えてから削除する機能です。次の動作を行います。

- ドメイン名を参照するユーザーの **UPN・EmailAddress・ProxyAddress** を初期ドメイン名へ変更する
- ドメイン名を参照するグループの **EmailAddress** を初期ドメイン名へ変更する

- ドメイン名を参照するアプリケーションの **identifierUris** を初期ドメイン名へ変更する
- 影響を受けたユーザー アカウントを無効化する

ForceDelete が使えない条件も押さえます。

- 参照が **1,000 件以上**ある
- 名前変更対象のアプリケーションの1つが**マルチテナント アプリ**である
- ドメインを Microsoft 365 のドメイン サブスクリプション サービスで購入した
- 他の顧客組織の代理管理を行うパートナー管理者である
- **ドメインの認証タイプが Federated である**(この場合、オンプレミスの Active Directory 側でユーザー/グループの名前変更または削除を行ってから、再度ドメインの削除を試みる)

なお、Exchange が provisioning しているオブジェクト(メールが有効なセキュリティ グループ、配布リスト)は、**Exchange 管理センターで手動で片付ける**必要があります。

> **運用上の注意**: **Microsoft は1つのドメイン名を複数の Microsoft Entra テナントで検証させません**。いったんテナントからドメインを削除すると、その後に別のテナントで追加・検証された場合、**自分のテナントで再追加・再検証できなくなります**。

1-1-7 Company branding settings の構成 [1.1]

Company branding は、テナントへのすべてのサインインに適用される見た目を作る機能です。

ライセンス要件は、次のいずれかです。

- **Microsoft Entra ID P1 または P2**
- **Microsoft 365 Business Standard**
- **SharePoint (Plan 1)**

必要なロールは Organizational Branding Administrator です(最小特権ロール)。設定場所は Entra ID > Custom Branding です。

カスタマイズできる要素は次のとおりです。要素と場所の対応は、対応付け問題の材料になります。

要素	どこに出るか
Favicon	ブラウザー タブの左側の小さいアイコン
Header	サインイン ページ最上部の帯
Header logo	サインイン ページの左上のロゴ
Background image	サインイン ボックスの背後の全面
Page background color	背景画像が読み込めないときに代わりに表示される色
Banner logo	サインイン ボックスの上部のロゴ
Sign-in page title / description	バナー ロゴの下の大きめのテキストと説明
Username hint text	ユーザー名入力欄のヒント
Sign-in page text	ユーザー名欄の下のテキスト
Self-service password reset のリンク	サインイン ページ テキストの下
Footer(Privacy & Cookies / Terms of Use)	ページ下部

要素	どこに出るか
Template(レイアウト)	全画面背景 / 部分画面背景 の2種類
Square logo (light theme) / (dark theme)	Microsoft Entra Web インターフェイスと Windows で組織を表す

画像のサイズと容量の要件は数値で問われることがあります。推奨形式は**PNG(JPG も可)**です。

要素	サイズ	最大ファイル サイズ
Favicon	32×32 px	5 KB
Background image	1920×1080 px	300 KB
Header logo	245×36 px	10 KB
Banner logo	245×36 px	50 KB
Square logo(light / dark)	240×240 px	50 KB

動作の注意点を押さえます。

- **すべてのブランド要素は任意**です。指定しなかった要素には既定値が残ります。
- **外部 URL はサインイン画面でクリックできません。**テキストとして表示されるだけです。
- **サインイン ページのブランドは個人用 Microsoft アカウントには適用されません。**
- **Sign-in page text は Unicode で 1,024 文字以内**です。書式は `[text](link)`(ハイパーリンク)、`**text**`(太字)、`*text*`(斜体)、`++text++`(下線)で指定します。

- **ブラウザーの言語ごとにブランドを追加**でき、その設定は既定のブランドを上書きします。アラビア語やヘブライ語など右から左に読む言語には、レイアウトが自動的に対応します。
- **既定のサインイン エクスペリエンスは作成後に削除できません**が、すべてのカスタム設定を取り除くことはできます。
- **Custom CSS には期限があります。2026年1月5日より後に作成されたテナントでは custom CSS を利用できません。**また **2026年7月21日以降、2026年1月6日より前に作成されたテナントでも、まだ custom CSS を使っていない場合は構成できません。**レイアウトと配置に関するプロパティ(`position`、`margin`、`transform`、`overflow` など)は非推奨化が進んでいます。

SaaS・マルチテナント アプリケーション(`https://myapps.microsoft.com` や `https://outlook.com` など)では、**ユーザーがメール アドレスまたは電話番号を入力して「次へ」を選んだ後にはじめて**、カスタマイズしたサインイン ページが表示されます。最初の画面からブランドを出したい場合は、**Home Realm Discovery の `whr` クエリ文字列パラメーター**を使います(例:`https://myapps.microsoft.com/?whr=contoso.com`)。

B2B のブランド表示は 1.3 と関係します。**テナントをまたいでサインインする B2B コラボレーション ユーザーには、そのユーザーのホーム テナントのブランドが表示されます**(ホーム テナントにカスタム ブランドが設定されていなくても既定のブランドが出ます)。

1-1-8 tenant properties、user settings、group settings、device settings の構成 [1.1]

ここは「既定でユーザーに何ができてしまうのか」を制御する設定群です。**既定値を覚えておかないと、「制限するにはどの設定を変えるか」に答えられま**

せん。

tenant properties(テナントのプロパティ)

テナントのプロパティには、組織名、テナント ID、国/地域、通知言語、そして**技術連絡先とプライバシー情報**が含まれます。プライバシー情報(プライバシーステートメント URL とプライバシー連絡先)は、**External user leave settings を構成するための前提条件**です —— プライバシー情報をテナントに追加していないと、この設定は選べません。

テナントのプロパティでは、**「非管理者ユーザーによるテナントの作成を制限する」**も構成します。既定では非管理者でもテナントを作成でき、**作成者は自動的にそのテナントの Global Administrator になります**。この作成は監査ログにカテゴリ `DirectoryManagement`、アクティビティ `Create Company` として記録されます。制限を「はい」にすると、**Tenant Creator ロールを持つユーザーだけ**が作成できます。

user settings(ユーザー設定)—— 既定のユーザー権限

メンバー ユーザーが既定でできることを押さえます。

- **アプリケーションを登録する**
- 自分のプロフィール写真と携帯電話番号を管理する
- 自分のパスワードを変更する
- **B2B ゲストを招待する**
- **セキュリティ グループと Microsoft 365 グループを作成する**
- 全ユーザーと連絡先を列挙し、公開プロパティを読み取る
- 全グループを列挙し、プロパティと(非表示でない)メンバーシップを読み取る

- 全デバイスを列挙し、全プロパティを読み取る
- 全ドメインと会社情報を読み取る
- **すべての管理ロールとそのメンバーシップ、administrative unit のプロパティとメンバーシップを読み取る**
- 全ライセンス サブスクリプションを読み取る

制限できる設定は次のとおりです。

設定	「いいえ」にすると	例外
Register applications(アプリケーションの登録)	ユーザーがアプリの登録を作成できなくなる	**Application Developer** ロールを付けると個別に許可できる
Allow users to connect work or school account with LinkedIn	職場/学校アカウントと LinkedIn アカウントの連携を禁止	—
Create security groups	ユーザーがセキュリティ グループを作成できなくなる	**User Administrator** 以上は引き続き作成可能
Create Microsoft 365 groups	ユーザーが Microsoft 365 グループを作成できなくなる。**「Some」にすると特定のユーザー群にだけ許可**できる	**User Administrator** 以上は引き続き作成可能
Restrict access to Microsoft Entra administration portal	非管理者が Microsoft Entra admin center のよく使うページを読み込めなくなる	管理ロール(カスタムロール含む)を持つユーザーには適用されない
Restrict non-admin users from creating tenants	非管理者がテナントを作成できなくなる	**Tenant Creator** ロールを付けると個別に許可できる

設定	「いいえ」にすると	例外
Read other users(Graph / PowerShell のみ)	非管理者がディレクトリからユーザー情報を読めなくなる	特殊な状況向け。Microsoft Teams など他サービスに影響するため**非推奨**

> **試験で最重要の注意：Restrict access to Microsoft Entra administration portal はセキュリティ対策ではありません。**これは「カジュアルな閲覧に摩擦を加える」設定で、**PowerShell・Microsoft Graph API・その他ツールからのプログラム的アクセスをブロックしません。**また、ディープ リンクを持っていればほとんどのページに到達できます。**確実に止めたいなら、Windows Azure Service Management API を対象にした Conditional Access ポリシーを使います。**この設定を「これで管理ポータルへのアクセスを防げる」と説明する選択肢は誤答です。

オブジェクトの所有権による権限も忘れがちです。ユーザーは、自分が作成したアプリケーション・エンタープライズ アプリケーション・グループの**所有者に自動的に追加**され、そのオブジェクトのプロパティとメンバーシップ、他の所有者の追加・削除ができます。ただし、**グループの所有者がメンバーを追加・削除できるのは、そのグループのメンバーシップの種類が「Assigned(割り当て済み)」の場合だけ**です。また、**動的メンバーシップ グループの所有者がルールを編集するには、Groups Administrator、Intune Administrator、または User Administrator のロールが必要**です。

ゲスト ユーザーの既定の権限は 1.3 で詳しく扱いますが、user settings 側にも次の2つがあります。

設定	内容
Guest user access restrictions	3段階(メンバーと同等 / 既定の限定的アクセス / 自分のオブジェクトのみ)
Guests can invite	ゲストが他のゲストを招待できるか

group settings(グループ設定)

グループ設定には、上記の「セキュリティ グループの作成」「Microsoft 365 グループの作成」に加えて、**self-service group management(セルフサービス グループ管理)**、**グループの有効期限ポリシー**、**グループの名前付けポリシー**があります。これらは**テナント レベルの設定**であり、**AU スコープの Groups Administrator では変更できません。**

グループの可視性(`visibility` プロパティ)を `Public` にすると、ユーザーはセルフサービスでグループに参加できます。**制限付き AU 内のグループを Public にすることは推奨されません。**

device settings(デバイス設定)

デバイス設定は Entra ID > Devices > All devices > Device settings にあります。

設定	取りうる値	意味
Users may join devices to Microsoft Entra ID	All / Selected / None	Microsoft Entra join を実行できるユーザーの範囲
Users may register their devices with Microsoft Entra ID	All / None	Microsoft Entra registration の可否

設定	取りうる値	意味
Require Multifactor Authentication to register or join devices	Yes / No	参加・登録時に MFA を要求するか
Maximum number of devices per user	数値 / Unlimited	1ユーザーが登録できるデバイス数の上限
Additional local administrators on Microsoft Entra joined devices	None / Selected	Microsoft Entra 参加デバイスのローカル Administrators グループに追加するユーザー
Restrict users from recovering the BitLocker key(s) for their owned devices	Yes / No	「はい」にすると、ユーザーは自分の所有デバイスの BitLocker キーをセルフサービスで取得できなくなる
Enterprise State Roaming	有効 / 無効	設定をデバイス間で同期する

推奨と出題: MFA の強制については、**device settings の「Require Multifactor Authentication to join devices」ではなく、Conditional Access のユーザー アクション「Register or join devices」を使うことが推奨**されています。「最も柔軟に、条件付きで MFA を要求したい」なら Conditional Access が正解です。

1-1-9 到達目標 1.1 の分かれ目の早見表 [1.1]

要件	正解	なぜ他は違うか
地域ごとの Helpdesk に、担当地域のユーザーのパスワード リセットだけを任せたい	**AU を作り、Helpdesk Administrator を AU スコープで割り当てる**	テナント スコープの Helpdesk Administrator では全ユーザーが対象になる
役員アカウントを、テナント全体の Helpdesk Administrator から守りたい	**restricted management AU に入れる**	通常の AU は「一部を任せる」仕組みで、テナント スコープの管理者は依然として操作できる
Global Administrator でも触れないようにしたい	**restricted management AU**(ただし AU 自体の管理と自己割り当ては可能)	通常の AU では Global Administrator を止められない
アプリの登録1つだけの資格情報更新を任せたい	**カスタムロールを作り、そのアプリの登録をスコープに割り当てる**(P1)	Application Administrator はテナント全体に及ぶ
管理者権限を常時保持させず、必要時だけ昇格させたい	**PIM**(P2)	role-assignable group(P1)では常時アクティブになる
グループの出入りで権限を管理したい(承認は不要)	**role-assignable group**(P1)	PIM は P2 が必要で、要件に対して過剰
ドメインの追加・検証だけを任せたい	**Domain Name Administrator**	Global Administrator は最小特権に反する
サインイン ページのロゴを変えたい	**Organizational Branding Administrator + P1 または Microsoft 365 Business Standard または SharePoint (Plan 1)**	Free ライセンスでは不可

要件	正解	なぜ他は違うか
非管理者に管理ポータルを触らせたくない(確実に)	**Windows Azure Service Management API を対象にした Conditional Access**	「Restrict access to Microsoft Entra administration portal」はセキュリティ対策ではない
ゲストの招待だけを特定ユーザーに任せたい	**Guest Inviter** ロール	User Administrator は広すぎる
Global Administrator の MFA をリセットしたい	**Privileged Authentication Administrator**	Authentication Administrator は非管理者のみが対象
AU にグループを入れたので、そのメンバーのパスワードもリセットできるか	**できない。ユーザーを AU に直接追加する**	グループの AU 追加は、グループ自体のみを管理範囲にする

1-2 Microsoft Entra ID の作成、構成、管理 [1.2]

1-2-1 users の作成、構成、管理(Create, configure, and manage users)[1.2]

Microsoft Entra ID のユーザーは、**どこで作られ、どこが正(source of authority)か**で3種類に分かれます。この分類が、「そのユーザーの属性をどこで直すか」という設問の根拠になります。

種類	作られ方	属性を変更する場所	見分け方
クラウドのみのユーザー	Microsoft Entra admin center、PowerShell、Graph API で直接作成	Microsoft Entra ID	Directory synced = No
同期されたユーザー	オンプレミス Active Directory から Microsoft Entra Connect Sync または Cloud Sync で同期	**オンプレミスの Active Directory**(クラウド側では多くの属性が読み取り専用)	Directory synced = Yes(`onPremisesSyncEnabled` = true)
外部ユーザー (B2B)	招待、セルフサービス サインアップ、cross-tenant synchronization	ホーム テナント側	UPN に `#EXT#` を含む(1.3 で詳述)

> **よく出る取り違え**:「同期ユーザーの部署名をクラウド側で直したい」——既定ではできません。オンプレミス側で直して次の同期サイクルを待つのが正解です。ただし例外があり、**custom security attributes はオンプレミスから同期されたユーザーにも割り当てられます**(1-2-3)。

ユーザー作成時に必ず必要な項目は、表示名(displayName)とユーザー プリンシパル名(userPrincipalName)、および初期パスワードです。加えて、**ライセンスを割り当てるには usage location(使用場所)が必須**です —— これは 1-2-6 で詳述しますが、ユーザー作成フローに組み込んでおくのが推奨です。

ユーザーの削除と復元も押さえます。削除されたユーザーは **soft delete(論理削除)** され、**30日間**は復元できます。30日を過ぎると hard delete(物理削除)され、復元できません。

ユーザーの無効化とセッションの取り消しは 2.1 の主題ですが、ユーザー管理としても登場します。`accountEnabled` を false にするとサインインがブロックされます。

Sponsor(スポンサー)属性は、ゲスト ユーザーを招待したユーザーが既定値として設定される属性です。外部ユーザーのライフサイクル管理(4.1)で使われます。

1-2-2 groups の作成、構成、管理(Create, configure, and manage groups)[1.2]

グループには2つの軸があります。**グループの種類**と**メンバーシップの種類**です。この2軸の組み合わせで、できることが決まります。

グループの種類

種類	何のためのものか	メンバーになれるもの
セキュリティ グループ	リソースへのアクセス制御、ライセンス割り当て、Conditional Access の対象指定	**ユーザー または デバイス**(両方を混ぜることはできない)
Microsoft 365 グループ	メールボックス、SharePoint サイト、Teams などの共同作業リソースを伴う	**ユーザーのみ**(デバイスは不可)

メンバーシップの種類

種類	内容	ライセンス
Assigned(割り当て済み)	管理者や所有者が手動でメンバーを追加・削除する	Free
Dynamic User(動的ユーザー)	ユーザー属性のルールでメンバーが自動決定される	**Microsoft Entra ID P1**
Dynamic Device(動的デバイス)	デバイス属性のルールでメンバーが自動決定される	**Microsoft Entra ID P1**(デバイス自体にはライセンス不要)

動的メンバーシップ グループ(rules for dynamic membership groups)の要点を押さえます。

- **1つのテナントに動的メンバーシップ グループは最大 15,000 個**です。
- **ユーザーとデバイスを混ぜたルールは書けません。**
- **デバイスの所有者のユーザー属性に基づいてデバイス グループを作ることはできません。**デバイス ルールが参照できるのはデバイス属性だけです。
- **動的メンバーシップ グループのメンバーを手動で追加・削除することはできません。**
- ライセンスは、**動的メンバーシップ グループのメンバーである一意のユーザーごとに P1** が必要です(実際にライセンスを割り当てる必要はありませんが、人数分の在庫が要ります)。
- **メンバーシップ ルールの本文は 3,072 文字以内**です。

ルールの構文は `<プロパティ> <演算子> <値>` です。プロパティ名は `<オブジェクト>.<プロパティ>` の形で、**大文字と小文字が区別されます。**

```
user.department -eq "Sales"
(user.department -eq "Sales") -or (user.department -eq "Marketing")
(user.department -eq "Sales") -and -not (user.jobTitle -startsWith
"SDE")
```

主な演算子は次のとおりです。

演算子	意味
`-eq` / `-ne`	等しい / 等しくない
`-startsWith` / `-notStartsWith`	前方一致 / 前方不一致
`-endsWith` / `-notEndsWith`	後方一致 / 後方不一致
`-contains` / `-notContains`	部分一致(**コレクションの要素一致ではない**)
`-match` / `-notMatch`	正規表現の一致 / 不一致
`-in` / `-notIn`	複数値のリストと突き合わせる(`["A","B"]` の形)
`-le` / `-ge`	以下 / 以上(`employeeHireDate` で使う)
`-any` / `-all`	多値プロパティのいずれか / すべてが条件を満たす
`-and` / `-or` / `-not`	論理演算子

演算子の優先順位(高い順)は次のとおりです。丸括弧は優先順位を変えたいときにだけ使います。

```
-eq -ne -startsWith -notStartsWith -contains -notContains -match -
notMatch -in -notIn
-not
-and
-or
-any -all
```

よく使うルールのパターンを型で覚えます。

やりたいこと	ルール
全ユーザー(ゲスト含む)	`user.objectId -ne null`
全メンバー ユーザー(ゲストを除く)	`(user.objectId -ne null) -and (user.userType -eq "Member")`
全デバイス	`device.objectId -ne null`
プロキシ アドレスが `contoso` で始まる人	`(user.proxyAddresses -any (_ -startsWith "contoso"))`
特定のマネージャーの直属の部下	`Direct Reports for "<マネージャーのオブジェクト ID>"`
Microsoft Entra 参加デバイス	`device.deviceTrustType -eq "AzureAD"`
Microsoft Entra ハイブリッド参加デバイス	`device.deviceTrustType -eq "ServerAD"`
Microsoft Entra 登録デバイス	`device.deviceTrustType -eq "Workplace"`
会社所有デバイス	`device.deviceOwnership -eq "Company"`

やりたいこと	ルール
Intune 管理デバイス	`device.deviceManagementAppId -eq "0000000a-0000-0000-c000-000000000000"`
拡張属性が Marketing	`(user.extensionAttribute15 -eq "Marketing")`

> **落とし穴(直属の部下ルール)**: `Direct Reports for "..."` のルールは、**マネージャー自身もグループに追加されます**。また、**孫にあたる部下(部下の部下)は含まれず、他のメンバーシップ ルールと組み合わせることもできません**。

> **落とし穴(null の扱い)**: null を比較するときは `-eq` または `-ne` を使います。**`-not` を比較演算子として null に使うとエラーになります**。`null` を引用符で囲むと、文字列リテラルの "null" として解釈されます。

ルール ビルダーは Azure portal / Microsoft Entra admin center 上の GUI で、**最大5つの式**まで組み立てられます。ただし次の場合はテキスト ボックスで直接書く必要があります。

- 式が6つ以上あるルール
- 直属の部下のルール
- `-contains` / `-notContains` を使うルール
- 演算子の優先順位を明示するルール
- `(user.proxyAddresses -any (_ -startsWith "contoso"))` のような複雑な式

- **デバイス ベースの動的メンバーシップ グループ**(ルール ビルダーは**ユーザー ベースのみ**対応)

多値プロパティ(`assignedPlans`、`proxyAddresses`、`otherMails`、`memberOf`)には `-any` / `-all` とアンダースコア `_` を使います。

```
user.assignedPlans -any (assignedPlan.servicePlanId -eq "efb87545-963c-4e0d-99df-69c6916d9eb0" -and assignedPlan.capabilityStatus -eq "Enabled")
```

セキュリティ上の注意として、**動的メンバーシップ ルールが参照する属性の書き込み権限を先に確認する**ことが求められます。とくにオンプレミス Active Directory から同期される属性には、ユーザー自身が自分の値を書き換えられる(SELF write)権限が設定されていることがあります。**その属性でアクセス制御用のグループを作ると、ユーザーが自分でグループに入れてしまいます。**なお **role-assignable group は動的メンバーシップを許さない設計なので、この経路のリスクがありません。**

Microsoft 365 グループのセルフサービス作成の制御は 1-1-8 の group settings で扱ったとおり、user settings 側で「No」または「Some」に設定します。

1-2-3 custom security attributes の管理(Manage custom security attributes)[1.2]

custom security attributes(カスタム セキュリティ属性) は、テナント独自に定義できるキーと値の組です。単なる拡張ではなく、**アクセス制御の判断材料**として使えるところが要点です。

使いどころは次のとおりです。

- ユーザー プロフィールを拡張する(例: 全社員に「時給」属性を持たせる)
- **その属性を管理者だけが見られるようにする**
- 数百から数千のアプリケーションを分類し、監査用の絞り込み可能な棚卸しを作る
- **Azure attribute-based access control (Azure ABAC)** の条件として使い、プロジェクトに属する Azure Storage BLOB へのアクセスを許可する

extensions(拡張)との違いが最も出る比較です。

機能	extensions	custom security attributes
対象オブジェクト	拡張の種類による	**ユーザーとサービス プリンシパルのみ**
アクセス制限	**なし**。オブジェクトを読める人は誰でも拡張データを読める	**あり**。読み書きが専用のアクセス許可と RBAC で制限される
使いどころ	アプリケーションが使うデータ、機微でないデータ	**機微なデータ**、認可のシナリオ
ライセンス	全エディション	全エディション(**無料**、Azure サブスクリプションに含まれる)

割り当てられるオブジェクトは、**Microsoft Entra のユーザー**と**エンタープライズ アプリケーション(サービス プリンシパル)** の2つだけです。**サポートされない領域**は、Microsoft Entra Domain Services、**SAML トークンのクレーム**、**JSON Web Token のクレーム**です。

構成の順序は並べ替え問題の定番です。

1. **アクセス許可を確認する** —— Attribute Definition Administrator または Attribute Assignment Administrator に割り当てられているか。割り当てるには **Privileged Role Administrator** 以上が必要
2. **attribute set(属性セット)を追加する** —— 関連する属性をまとめる入れ物
3. **attribute set を管理する** —— 誰がその属性セットの属性を読める/定義できる/割り当てられるかを指定する
4. **属性を定義する** —— データ型(Boolean / Integer / String)、単一値か複数値か、定義済みの値か自由入力かを指定する
5. **属性を割り当てる** —— ユーザーやサービス プリンシパルに値を付ける
6. **属性を使う** —— フィルターで絞り込む、Azure ロール割り当ての条件に使う

ロールと権限は、この節で最も出る一点です。

ロール	できること
Attribute Definition Reader	attribute set と属性定義の読み取り
Attribute Definition Administrator	attribute set と属性定義の**すべての管理**(定義の最小ロール)
Attribute Assignment Reader	attribute set・属性定義の読み取り、ユーザーとサービス プリンシパルの属性の**キーと値の読み取り**
Attribute Assignment Administrator	上記に加え、キーと値の**読み取りと更新**(割り当ての最小ロール)
Attribute Log Reader	custom security attributes の監査ログの読み取り

ロール	できること
Attribute Log Administrator	監査ログの読み取りと、custom security attributes の診断設定の構成

> **これが最重要: Global Administrator をはじめとする他の管理者ロールは、既定では custom security attributes を読み取る・定義する・割り当てる権限を持ちません。**「Global Administrator なのに属性が見えない」は仕様です。これらのロールは**テナント スコープでも attribute set スコープでも割り当てられます。**

属性のプロパティのうち、**後から変更できないもの**が問われます。

プロパティ	必須	後から変更可能
Attribute set name	必須	**不可**
Attribute set description	任意	可
Maximum number of attributes	任意	可
Attribute set(どのセットに属するか)	必須	**不可**
Attribute name	必須	**不可**
Attribute description	任意	可
Data type(Boolean / Integer / String)	必須	**不可**
Allow multiple values to be assigned	必須	**不可**(Boolean のときは「はい」にできない)

プロパティ	必須	後から変更可能
Only allow predefined values to be assigned	必須	**「はい」から「いいえ」へは変更可。「いいえ」から「はい」へは不可**(Boolean のときは「はい」にできない)
Predefined value is active	任意	可
Attribute is active	任意	可

上限値は数値問題の材料です。

リソース	上限
テナントあたりの属性定義	**500**(アクティブな属性のみが対象)
テナントあたりの attribute set	**500**
attribute set 名の長さ	32 文字
属性名の長さ	32 文字
説明の長さ	128 文字
属性定義あたりの定義済みの値	**100**
属性値の長さ	64 文字
1オブジェクトあたりに割り当てられる属性値	**50**(単一値と複数値に分散可能。例: 10個の値を持つ属性5つ、または1個の値を持つ属性50個)

attribute set 名と属性名には**空白と特殊文字が使えず、数字で始めることもできません。**属性の値には全ての特殊文字が使えますが、**Azure Storage の BLOB インデックス タグと併用する場合は、空白・`+`・`-`・`.`・`:`・`=`・`_`・`/` のみ**が許されます。

1-2-4 Microsoft Entra admin center と PowerShell による一括操作の自動化(Automate bulk operations)[1.2]

bulk operations(一括操作) は、CSV ファイルを使ってユーザーの作成・削除・招待などをまとめて行う仕組みです。Microsoft Entra admin center から実行できるものと、PowerShell / Graph でしかできないものがあります。

Microsoft Entra admin center でできる一括操作

操作	場所	必要ロール
Bulk create(ユーザーの一括作成)	Entra ID > Users > Bulk create	**User Administrator** 以上
Bulk invite(外部ゲストの一括招待)	Entra ID > External Identities	Guest Inviter 以上
Bulk delete(ユーザーの一括削除)	Entra ID > Users	User Administrator 以上
Bulk restore(削除済みユーザーの一括復元)	Entra ID > Users > Deleted users	User Administrator 以上
Download users / groups / group members(一覧のダウンロード)	各一覧ページ	読み取り権限

CSV テンプレートの構造は、失敗の原因を問う設問で使われます。

- **1行目のバージョン番号**(例: `version:v1.0`)は、テンプレートに含まれていれば**削除も変更もしてはいけません**。
- **2行目は列見出し**で、形式は `<項目名> [プロパティ名] <Required または空白>` です(例: `Name [displayName] Required`)。

- **3行目は例の値**の行で、**自分のデータに置き換える必要があります。**1件だけ登録する場合でも、**3行目を残して4行目に自分のエントリを追加します。**
- **テンプレートの形式は操作ごとに異なります。**ユーザーの一括作成や削除のテンプレートには `version:v1.0` 行がありますが、グループ メンバーの操作のテンプレートは列見出しから始まります。**必ずその操作用のテンプレートをポータルからダウンロード**し、ダウンロードしたとおりの行構成を保ちます。
- **列を追加しても無視されます。**
- **前後の空白に注意**します。とくに **User principal name の前後の空白はインポート失敗の原因**になります。
- **Initial password は現在有効なパスワード ポリシーに準拠**していなければなりません。

ユーザーの一括作成で必須の列は最初の4つだけです。

列	プロパティ
Name	`displayName`
User name	`userPrincipalName`
Initial password	`passwordProfile`
Block sign in (Yes/No)	`accountEnabled`

残りの列(givenName、surname、jobTitle、department、usageLocation、city 、state 、country 、physicalDeliveryOfficeName 、postalCode 、telephoneNumber、mobile、streetAddress)はすべて任意です。

> **重要な仕様: Bulk create は内部のメンバー アカウントを、CSV で指定したパスワードで作成します。招待メールは送信されません。**サインイン資格情報は自分の手段で伝える必要があります。**外部ゲストを一括で招待し招待メールを送りたいなら、Bulk create ではなく Bulk invite** を使います。この切り分けが「問題と解決策」形式で問われます。

実行結果の確認は **Bulk operation results** ページで行います。エラーが出た場合は結果ファイルをダウンロードでき、各エラーの理由が記載されています。

サービスの制限として、**一括操作が1時間以内に完了しないと問題が起きる**ことがあります。回避策は**1バッチあたりの処理レコード数を分割する**ことです。エクスポート前にグループの種類やユーザー名でフィルターして結果セットを絞る、といった対策が推奨されます。

PowerShell による代替も押さえます。Microsoft Graph PowerShell SDK を使えば、admin center の一括操作より柔軟に処理できます。

```
Connect-MgGraph -Scopes "User.ReadWrite.All"
Import-Csv .\users.csv | ForEach-Object {
    $passwordProfile = @{ Password = $_.Password;
ForceChangePasswordNextSignIn = $true }
    New-MgUser -DisplayName $_.DisplayName -UserPrincipalName
$_.UserPrincipalName `
        -MailNickname $_.MailNickname -AccountEnabled -PasswordProfile
$passwordProfile `
        -UsageLocation $_.UsageLocation
}
Get-MgUser -Filter "UserType eq 'Member'"
```

グループへのライセンス割り当ては `Set-MgGroupLicense`、ユーザーの取得は `Get-MgUser`、デバイスの取得は `Get-MgDevice` を使います。**Azure CLI は Microsoft Entra のロール割り当てに対応していない**点は 1-1-2 で述べたとおりです。

1-2-5 Microsoft Entra ID における device join と device registration の管理 [1.2]

デバイス ID は、Microsoft Entra ID 内のオブジェクトです。ユーザーやグループやアプリケーションと同じように扱われ、**デバイス ベースの Conditional Access ポリシー**と **Intune による MDM** の前提になります。

デバイス ID を得る方法は3つです。この比較表が対応付け問題の中心になります。

観点	Microsoft Entra registration	Microsoft Entra join	Microsoft Entra hybrid join
想定するデバイス	**BYOD(個人所有)**、携帯電話・タブレット	**組織所有**の Windows 10 / Windows 11、Azure 上の VM として動く Windows Server 2019 以降	オンプレミス Active Directory に参加済みの組織所有デバイス
オンプレミス AD への参加	不要	**不要**	**必要**(AD と Microsoft Entra ID の両方に参加)
位置づけ	個人デバイスから会社リソースへ	クラウド ファーストの目標形	**Microsoft Entra join へ向かう途中段階**
管理方法	MDM(Intune)/ MAM	**MDM のみ**。グループ ポリシーは使えない	グループ ポリシー + Configuration Manager、または co-management
プロビジョニング	ユーザーが「職場または学校アカウントを追加」	セルフサービス (OOBE / 設定)、**Windows Autopilot**、**Bulk enrollment**	Microsoft Entra Connect による構成

3つの方式は1つの組織内で共存できます。

Microsoft Entra join の前提条件を押さえます。

- **Windows 10 と Windows 11 のみ対応**です。それ以前の Windows や他の OS には対応しません。

- **FIPS 準拠の TPM 2.0 はサポートされますが、TPM 1.2 はサポートされません。**FIPS 準拠の TPM 1.2 を持つデバイスでは、参加前に FIPS モードを無効にする必要があります。
- **System Preparation Tool(Sysprep)などのイメージング ツールでは展開できません。**
- **グループ ポリシーは使えません。**管理は MDM のみです。
- オンプレミスの UPN と Microsoft Entra の UPN が**異なる構成はサポートされません。**

ID インフラの前提も分かれ目になります。

環境	要件
マネージド環境	password hash synchronization または pass-through authentication に seamless SSO を組み合わせる
フェデレーション環境	ID プロバイダーが **WS-Fed と WS-Trust の両方**をサポートする必要がある。**WS-Fed はデバイスを Microsoft Entra ID に参加させるために、WS-Trust は Microsoft Entra 参加デバイスにサインインするために必要**

AD FS を使う場合は、次の WS-Trust エンドポイントを有効にします。`/adfs/services/trust/2005/usernamemixed`、`/adfs/services/trust/13/usernamemixed`、`/adfs/services/trust/2005/certificatemixed`、`/adfs/services/trust/13/certificatemixed`。

プロビジョニングの3方式を比較します。

要素	セルフサービス	Windows Autopilot	Bulk enrollment
ユーザーの操作が必要	必要	必要	**不要**
IT 側の作業	不要	必要	必要
使える場面	**OOBE と設定の両方**	**OOBE のみ**	**OOBE のみ**
主要ユーザーへのローカル管理者権限	**既定で付与される**	構成可能	**付与されない**
デバイス OEM のサポートが必要	不要	**必要**	不要

> **よく出る取り違え**:「セルフサービスで Microsoft Entra join したユーザーはローカル管理者になる」―― そのとおりですが、**これはそのデバイスに限ったローカル管理者権限であって、Microsoft Entra のディレクトリ ロールを付与するものではありません**。

MDM のユーザー スコープは「Some」か「All」で設定します。

- **ユーザーが MDM のスコープ内**: **Microsoft Entra ID P1 または P2 のサブスクリプションがあれば、Microsoft Entra join と同時に MDM 登録が自動化されます**。スコープ内の全ユーザーに MDM 用の適切なライセンスが必要で、**MDM 登録に失敗すると Microsoft Entra join 自体がロールバックされます**。
- **ユーザーがスコープ外**: Microsoft Entra join は MDM 登録なしで完了し、**管理されていないデバイス**になります。

Microsoft Entra join でできないことも誤答肢の材料です。

- **マシン認証に依存するオンプレミス アプリケーション**はサポートされません。
- **オンプレミスのコンピューター オブジェクトと証明書を使う RADIUS 認証**(Wi-Fi アクセス ポイントへの接続など)はサポートされません。代替として、**Intune 経由でプッシュした証明書、またはユーザー資格情報**で認証します。
- **リモート デスクトップ**で Microsoft Entra 参加デバイスに接続するには、接続元も Microsoft Entra 参加または Microsoft Entra ハイブリッド参加である必要があります(Windows 10 2004 以降は Microsoft Entra 登録デバイスからも可能)。

リソースへのアクセスと SSO については、Microsoft Entra ID に登録・参加したデバイスは**クラウド リソースへの SSO** を得ます。さらに **Microsoft Entra 参加デバイスは、オンプレミス リソースへの SSO** も得られます(ドメイン コントローラーへの見通しがある場合)。

1-2-6 ライセンスの割り当て、変更、レポート(Assign, modify, and report on licenses)[1.2]

ライセンスの割り当て方は2つあり、**混在した状態を読み解けるか**が問われます。

方法	特徴	見え方
直接割り当て	ユーザー個々にライセンスを付ける	ユーザーのライセンス ページで「直接」

方法	特徴	見え方
group-based licensing(グループ ベースのライセンス)	セキュリティ グループ、メールが有効なグループ、Microsoft 365 グループにライセンスを割り当て、メンバーが継承する	「継承(inherited)」

usage location(使用場所)の要件が最頻出です。**一部の Microsoft サービスはすべての地域で利用できないため、ライセンスを割り当てる前に管理者がユーザーの場所を指定しなければなりません。グループ ベースのライセンスでは、使用場所が指定されていないユーザーはテナントの場所を継承します。**複数の地域にユーザーがいる場合は、**ユーザー作成フローの一部として常に使用場所を設定することが推奨**されます。

必要なロールは **Groups Administrator、License Administrator、または User Administrator** 以上です。最小特権なら **License Administrator** です。

グループ ベースのライセンスの制約を押さえます。

- **入れ子のグループには対応していません。**入れ子のグループにライセンスを割り当てても、**第1階層のグループのメンバーにしかライセンスが割り当てられません。**
- **一度に最大 20 グループ**にライセンスを割り当てられます。
- **Reprocess(再処理)は一度に最大 20 ユーザー**まで処理します。
- 成功・失敗したユーザーの一覧は **999 人ずつのページ**で表示されます。
- 10万人規模の大きなグループでライセンスを割り当てたり変更したりすると、**パフォーマンスに影響**します。高負荷時にはライセンス変更やメンバーシップ変更の処理に長い時間がかかることがあります。

ライセンス付きグループ間でユーザーを移動する順序は並べ替え問題の定番です。

1. **先に移動先のグループにユーザーを追加する**
2. ユーザーの Licenses ページで**新しいライセンスが適用されたことを確認する**
3. **元のグループからユーザーを削除する**

> **なぜこの順序か**: 先に元のグループから削除すると、グループ ベースのライセンスが新しい割り当ての処理を終えるまで、**そのユーザーはライセンスなしの状態**になり、ライセンス サービスへのアクセスを一時的に失います。処理時間はテナントの規模と負荷によって変わるため、大規模テナントや高負荷時にはこの空白が予想以上に長くなります。

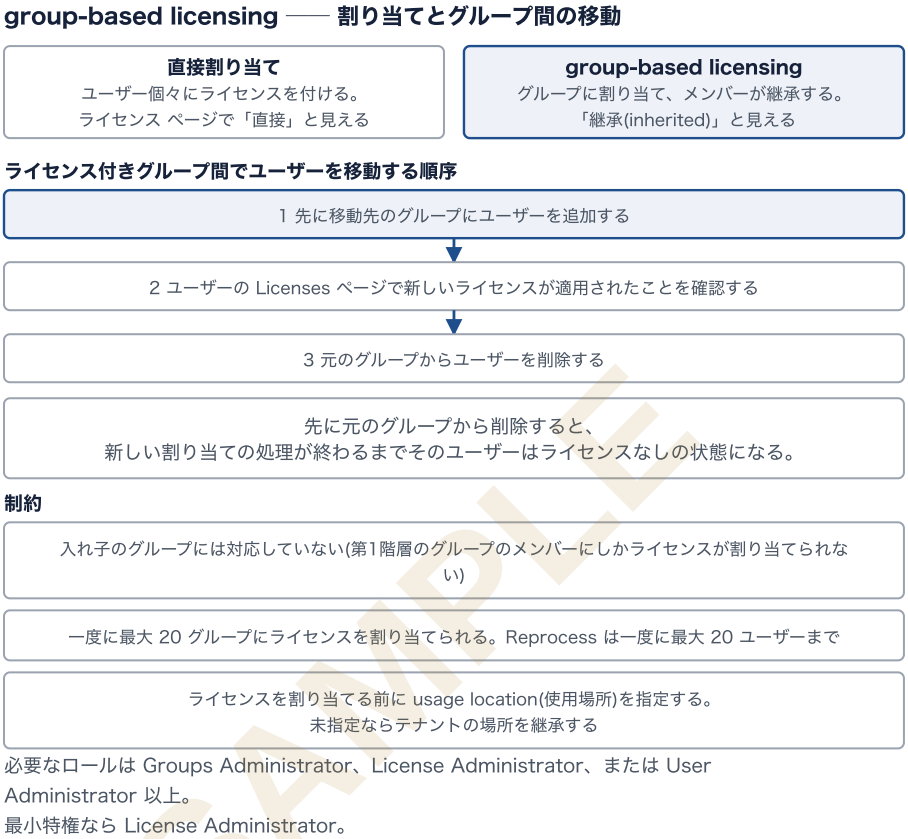

図 1-3　group-based licensing —— 割り当てとグループ間の移動

ライセンス割り当ての問題は、Licenses ページの製品詳細から**「Errors & issues」タブ**で確認します。代表的なエラーは次のとおりです。

エラー	意味	対処
Insufficient licenses(ライセンス不足)	利用可能なライセンス数が足りない	ライセンスを追加購入するか、不要な割り当てを外す

エラー	意味	対処
Conflicting service plans(サービス プランの競合)	同時に割り当てられない2つのサービス プランが当たっている	一方の製品で該当サービス プランを無効にする
Missing dependencies(依存関係の欠落)	前提となるサービス プランが有効でない	前提のサービス プランを有効にする
Proxy address issues(プロキシ アドレスの重複)	同じプロキシ アドレスを持つユーザーが他にいる	重複を解消する
Usage location problems(使用場所の問題)	ユーザーの使用場所でそのサービスが提供されていない、または未設定	使用場所を設定・変更する

サービス プランの有効化・無効化は、「Turn apps and services on or off」から行います。たとえば Microsoft 365 E3 を割り当てつつ、Yammer だけを無効にする、といった構成ができます。この状態は動的メンバーシップ ルールからも参照でき、`assignedPlans` の `servicePlanId` と `capabilityStatus -eq "Enabled"` で「特定のサービス プランが有効なユーザー」のグループを作れます。

レポートは、Microsoft 365 管理センターの Billing > Licenses ページ、Microsoft Entra admin center のライセンス ページ、および PowerShell(`Get-MgUserLicenseDetail` など)で取得します。

1-2-7 到達目標 1.2 の分かれ目の早見表 [1.2]

要件	正解	なぜ他は違うか
部署が Sales のユーザーを自動でグループに入れたい	**動的ユーザー グループ**(P1)	Assigned では手動運用になる

要件	正解	なぜ他は違うか
Microsoft Entra 参加デバイスだけを Conditional Access の対象にしたい	**動的デバイス グループ** `device.deviceTrustType -eq "AzureAD"`	ユーザー属性ではデバイスを選べない
ロールをグループに割り当てたい	**role-assignable group**(Assigned のみ)	動的メンバーシップ グループは role-assignable にできない
機微な属性を付けたいが、Global Administrator には見せたくない	**custom security attributes**	extensions はオブジェクトを読める人が誰でも読める
属性で Azure Storage BLOB へのアクセスを絞りたい	**custom security attributes + Azure ABAC**	ディレクトリ拡張では ABAC 条件に使えない
500 人の社員アカウントをまとめて作りたい(招待メールは不要)	**Bulk create**	Bulk invite は外部ゲストの招待用
200 社の取引先担当者を招待メール付きでまとめて招待したい	**Bulk invite**	Bulk create は招待メールを送らない
個人所有のスマートフォンから会社アプリを使わせたい	**Microsoft Entra registration**	join は組織所有の Windows デバイス向け
新品の Windows 11 を IT が事前構成し、ユーザーの初回起動で自動参加させたい	**Windows Autopilot**	Bulk enrollment は OOBE のみだがユーザー操作なしの管理者主導型
ライセンス割り当てだけを任せたい	**License Administrator**	User Administrator は広すぎる

要件	正解	なぜ他は違うか
ライセンスを割り当てたのにエラーになる	**usage location を確認する**	使用場所未設定はライセンス割り当ての典型的な失敗要因
ライセンス付きグループ間でユーザーを移す	**追加 → 確認 → 削除の順**	先に削除するとライセンスの空白期間が生じる

1-3 外部ユーザーとテナントの ID の実装と管理 [1.3]

1-3-1 この節の全体像 —— 3つの設定面を混同しない [1.3]

外部ユーザーの制御には**3つの独立した設定面**があり、これを混同すると設問が解けません。まずここを固定します。

設定面	対象	どこで設定するか	何を決めるか
External collaboration settings	**Microsoft Entra 以外の ID を含む全ゲスト**(ソーシャル ID、IT 管理外の外部アカウント)	Entra ID > External Identities > External collaboration settings	ゲストが**ディレクトリで何を見られるか、誰がゲストを招待できるか、どのドメインを許可/拒否するか**
Cross-tenant access settings	**他の Microsoft Entra 組織**(および Microsoft クラウドをまたぐ場合)	Entra ID > External Identities > Cross-tenant access settings	**受信・送信のアクセス、MFA とデバイスクレームの信頼、cross-tenant synchronization の許可、tenant restrictions**

設定面	対象	どこで設定するか	何を決めるか
All identity providers	外部 ID プロバイダー	Entra ID > External Identities > All identity providers	**SAML/WS-Fed フェデレーション**、ソーシャル ID、email one-time passcode

> **切り分けの一言：相手が Microsoft Entra 組織なら cross-tenant access settings、それ以外(ソーシャル ID など)を含む一般的なゲスト制御なら external collaboration settings。**この一文が、この節の設問の半分を解きます。

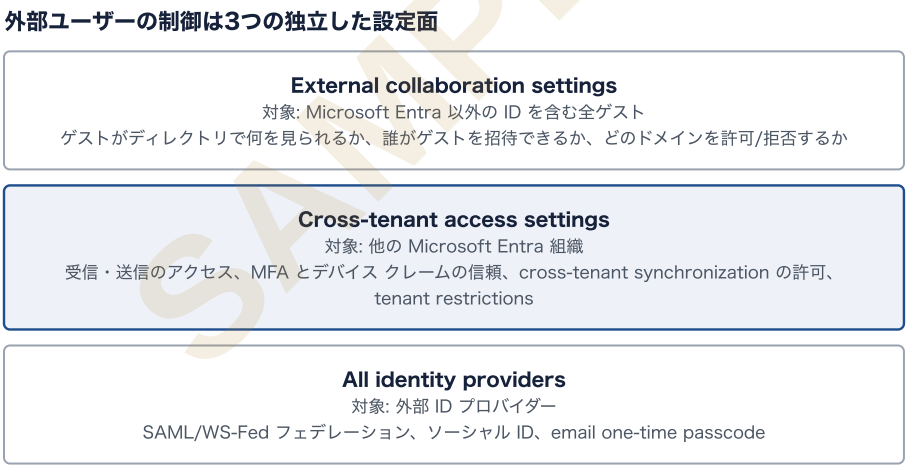

図 1-4　外部ユーザーの制御は3つの独立した設定面

1-3-2 B2B コラボレーション ユーザーのプロパティ [1.3]

B2B コラボレーションでは、外部ユーザーが**自分の資格情報で**リソース テナントにサインインします。**リソース テナント側には、従業員と同じディレクトリにユーザー オブジェクトが作られます**。このオブジェクトは既定で限定的な特権しか持ちませんが、従業員と同じようにグループに追加したりアプリケーションに割り当てたりできます。

B2B コラボレーション ユーザーは、**認証がどこで行われるか(内部/外部)** と**組織との関係(guest/member)** の2軸で4種類に分かれます。

種類	認証	UserType	典型例
External guest	外部の Microsoft Entra 組織または外部 ID プロバイダー	**Guest**	一般的な取引先・パートナー。最も多い
External member	外部の Microsoft Entra 組織または外部 ID プロバイダー	**Member**	マルチテナント組織で、他テナントのリソースにメンバー相当のアクセスが要る場合
Internal guest	内部(リソース テナント)	**Guest**	B2B 以前に、外部の人へ内部資格情報を作って渡していた形。B2B へ移行するのが推奨
Internal member	内部	**Member**	自組織の従業員

UserType プロパティは「そのユーザーと組織との関係」を示すだけです。**サインインの方法やディレクトリ ロールとは無関係**です。

値	意味
Member	ホスト組織の従業員。社内専用サイトへのアクセスが期待される
Guest	社内の人とは見なされない外部の協力者・パートナー・顧客

UPN の形は必ず問われます。`john@contoso.com` を `fabrikam` ディレクトリに外部ユーザーとして追加すると、UPN は `john_contoso.com#EXT#@fabrikam.onmicrosoft.com` になります。

Identities プロパティは、そのユーザーの主要な ID プロバイダーを示します。**UserType とは独立**しており、Identities の値から UserType は決まりません。

Identities の値	サインインの状態
ExternalAzureAD	外部の Microsoft Entra 組織のアカウントで認証する
Microsoft account	Microsoft アカウントで認証する
{ホストのドメイン}	この組織の Microsoft Entra アカウントで認証する(内部資格情報の外部ユーザー)
google.com	Gmail アカウントでセルフサービス サインアップした
facebook.com	Facebook アカウントでセルフサービス サインアップした
mail	**email one-time passcode (OTP)** でサインアップした

Identities の値	サインインの状態
{issuer URI}	Microsoft Entra ID を使わず、**SAML/WS-Fed ベースの ID プロバイダー**を使う外部組織に所属する

電話サインインは外部ユーザーではサポートされません。B2B アカウントは `phone` を ID プロバイダーとして使えません。

招待の引き換え(invitation redemption)の前後で、オブジェクトの見え方が変わります。

段階	Identities	Invitation state(externalUserState)
招待後・引き換え前	**ホスト組織のドメイン**(資格情報は関連付けられていない)	**Pending acceptance**
引き換え後	ユーザーの ID プロバイダーに応じて更新される	**Accepted**

招待を送ったユーザーは、**Sponsor 属性の既定値**としてゲスト ユーザー アカウントに設定されます。

email one-time passcode は、**新規テナントすべてと、明示的に無効化していない既存テナントで既定で有効**です。**この機能を無効にした場合のフォールバックは、招待相手に Microsoft アカウントの作成を促す動作**になります。

UserType の変換は、Microsoft Entra admin center でプロファイルを編集するか PowerShell で行えます。ただし UserType は組織との関係を表すプ

ロパティなので、**関係が変わったときにだけ変更すべき**です。B2B ユーザーをメンバーとして招待したい場合は、**B2B Invitation Manager API** を使います。

ゲストの既定の権限は 1-1-8 の表のとおりで、ゲストは全ユーザー・全グループの列挙ができません。必要に応じてゲストを管理者ロールに追加することも、既定の制限を外してメンバーと同等にすることもできます。**ゲスト オブジェクトは既定で Exchange のグローバル アドレス一覧に表示されません**が、Microsoft Graph PowerShell で表示させることができます。

ゲストのメール アドレスの更新については、ゲストが引き換え後にメール アドレスを変更しても、**リソース テナントのゲスト オブジェクトへ自動で同期されません**。Microsoft Graph API、Exchange 管理センター、または Exchange Online PowerShell で `mail` プロパティを更新します。

なお **B2B ゲスト ユーザーは Microsoft Teams の共有チャネルではサポートされません**。共有チャネルには **B2B direct connect** を使います。

1-3-3 External collaboration settings の管理 [1.3]

必要なロールは、Microsoft Entra admin center では **Global Administrator** または **External Identity Provider Administrator** です。Microsoft Graph を使う場合は、設定ごとにより低い特権のロールが使えることがあります。

Guest user access(ゲスト ユーザーのアクセス) は3段階です。

設定	内容
Guest users have the same access as members (most inclusive)	ゲストにメンバーと同じアクセスを与える

設定	内容
Guest users have limited access to properties and memberships of directory objects(既定)	ユーザー・グループ・その他ディレクトリ リソースの列挙などを禁止する。**非表示でないグループのメンバーシップは見える**
Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)	自分のプロファイルのみ。**他ユーザーのプロファイル、グループ、グループ メンバーシップは一切見えない**(UPN・オブジェクト ID・表示名で検索してもアクセスできない)

> **注意**: 最も制限的な設定でも、**Microsoft Teams など一部の Microsoft 365 サービスで参加済みグループへのアクセスは防げません**。また、**この設定にかかわらず、ゲストを管理者ロールに追加することはできます**。

Guest invite settings(ゲスト招待の設定) は4段階です。既定では**組織内の全ユーザー(ゲストを含む)がゲストを招待できます**。

設定	誰が招待できるか
Anyone in the organization can invite guest users including guests and non-admins (most inclusive)	ゲストを含む全員
Member users and users assigned to specific admin roles can invite guest users including guests with member permissions	メンバー ユーザーと、特定の管理者ロールを持つユーザー
Only users assigned to specific admin roles can invite guest users	**User Administrator** または **Guest Inviter** ロールを持つユーザーのみ
No one in the organization can invite guest users including admins (most restrictive)	誰も招待できない

> **設計の型**:「招待を絞りたいが、担当者には招待させたい」の答えは、**「Only users assigned to specific admin roles」に設定し、担当者に Guest Inviter ロールを割り当てる**です。Guest Inviter は、より高い特権の管理者ロールを与えずに招待だけを許すためのロールです。

Enable guest self-service sign up via user flows を「はい」にすると、自作アプリケーションに**セルフサービス サインアップのユーザー フロー**を追加でき、ユーザーがサインアップして新しいゲスト アカウントを作れるようになります。

External user leave settings(外部ユーザーの離脱設定) は、外部ユーザーが自分で組織から離脱できるかを制御します。

設定	内容
Yes	管理者やプライバシー連絡先の承認なしで、ユーザー自身が離脱できる
No	自分では離脱できず、管理者またはプライバシー連絡先に連絡するよう案内される

> **前提条件**: **テナントにプライバシー情報を追加していないと、External user leave settings は構成できません**(設定自体が表示されません)。これは 1-1-8 の tenant properties と結びつく一点です。

Collaboration restrictions(コラボレーションの制限) では、指定したドメインへの招待を**許可(allow list)または拒否(deny list)** します。複数ドメインは1行に1つずつ入力します。**許可リストと拒否リストは同時に使えず、どちらか一方だけ**が有効です。

Microsoft Graph API での構成先も対応付けで問われます。

設定	Microsoft Graph のリソース タイプ
Guest user access restrictions / Guest invite restrictions	`authorizationPolicy`
Enable guest self-service sign up via user flows	`authenticationFlowsPolicy`
External user leave settings	`externalidentitiespolicy`
Email one-time passcode の設定	`emailAuthenticationMethodConfiguration`

B2B ユーザーのサインイン ログについては、B2B ユーザーがリソース テナントにサインインすると、**ホーム テナントとリソース テナントの両方にサインイン ログが生成されます**。ログには、使用されたアプリケーション、メール アドレス、両テナントの名前とテナント ID が含まれます。

1-3-4 外部ユーザーの招待(個別・一括)と外部ユーザー アカウントの管理 [1.3]

外部ユーザーの招待(**Invite external users, individually or in bulk**)には、個別と一括の2つの経路があります。

個別の招待は Entra ID > Users > New user > **Invite external user** から行います。招待メールが送られ、ユーザーが引き換えるとアカウントが有効になります。

一括招待は External Identities の **Bulk invite** から CSV で行います。1-2-4 で述べたとおり、**Bulk create(内部メンバー アカウントを作る・招待メールは送らない)とは別物**です。

招待の引き換え順序 (redemption order) は、cross-tenant access settings の **Redemption order タブ**で構成します。既定の引き換え順序を上書きし、ゲストがどの ID プロバイダーでサインインするかの優先順位を変えられます。

- **Primary identity providers(プライマリ ID プロバイダー)**: 他の認証ソースとのフェデレーションを持つプロバイダー
- **Fallback identity providers(フォールバック ID プロバイダー)**: **Microsoft account (MSA)** と **email one-time passcode** の2つ

> **重要な制約**: **フォールバック ID プロバイダーの両方を同時に無効にすることはできません。**プライマリをすべて無効にしてフォールバックだけを使うことはできます。**Microsoft アカウントでの引き換えを禁止したい場合は、フォールバックのオプションで Microsoft アカウントをオフにします。**この場合、email one-time passcode を有効にしておく必要があります。**既に Microsoft アカウントでサインインしている既存ゲストは、そのまま Microsoft アカウントを使い続けます。**新しい設定を適用するには、**引き換え状態のリセット(reset redemption status)** が必要です。

既知の制限として、既存の SSO セッションを持つ Microsoft Entra ID ユーザーが email OTP で認証する場合、**「別のアカウントを使用する」を選んでユーザー名を再入力しないと OTP フローが起動しません。**

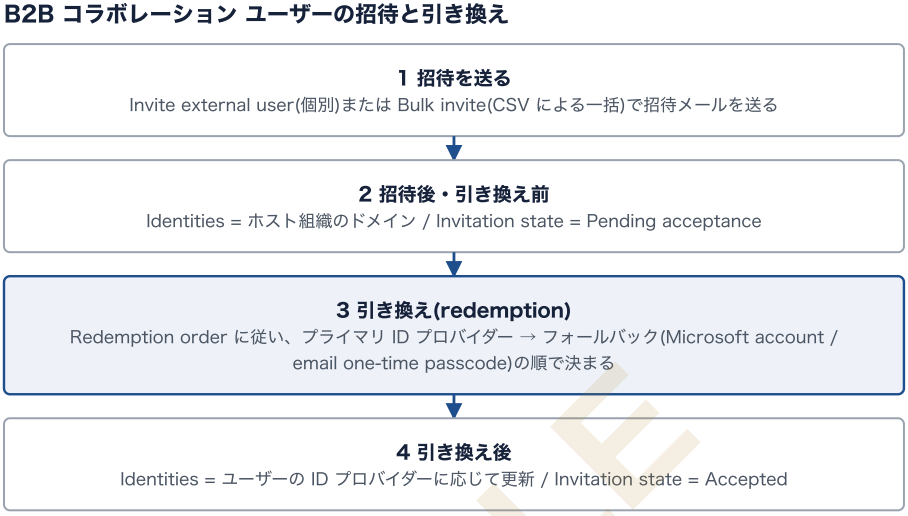

図 1-5　B2B コラボレーション ユーザーの招待と引き換え

外部ユーザー アカウントの管理では、次を行います。

- Users 一覧で **Add filter** から **User type** を Guest に絞り、ゲストだけを表示する
- ゲストのプロファイルで **Invitation state** を確認する
- **引き換え状態のリセット**により、招待を送り直す(フェデレーション構成の削除後にアクセスを回復させる場合にも使う)
- ゲストを削除する(soft delete され、30日間は復元可能)
- 4.1 の **entitlement management** による外部ユーザーのライフサイクル管理につなげる

1-3-5 Cross-tenant access settings の実装(Implement Cross-tenant access settings)[1.3]

cross-tenant access settings は、**他の Microsoft Entra 組織および Microsoft Azure クラウドとの連携**を、**B2B collaboration** と **B2B direct connect** の両面から制御する仕組みです。**追加できる組織の数に上限はありません**。

3つの設定の軸を押さえます。

軸	内容
Outbound access settings(送信)	**自組織のユーザーが外部組織のリソースにアクセスできるか**。全員に適用することも、特定のユーザー・グループ・アプリケーションを指定することもできる
Inbound access settings(受信)	**外部組織のユーザーが自組織のリソースにアクセスできるか**。同様に対象を絞れる
Trust settings(信頼設定・受信側)	外部組織の **MFA、compliant device、Microsoft Entra hybrid joined device のクレームを、自分の Conditional Access ポリシーが信頼するか**

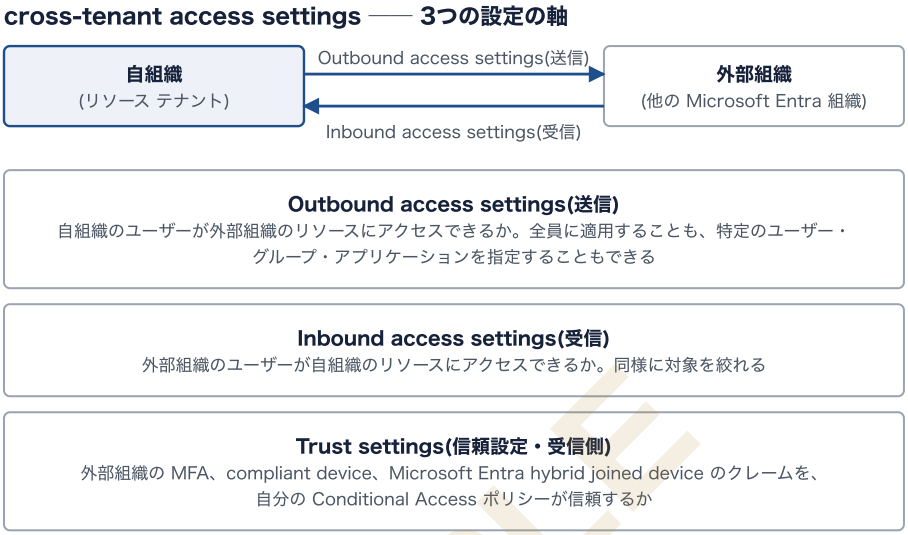

図 1-6　cross-tenant access settings —— 3つの設定の軸

> **trust settings の効き方**: MFA を信頼するように構成すると、**MFA ポリシー自体は引き続き外部ユーザーに適用されますが、ホーム テナントで既に MFA を完了しているユーザーは、自テナントで再度 MFA を求められません。**「取引先の担当者が毎回 MFA を2回やらされる」問題の答えがこれです。

Default settings(既定の設定) は、カスタム設定を構成していないすべての外部 Microsoft Entra 組織に適用されます。**初期状態**は次のとおりです。

項目	初期状態
B2B collaboration	**有効**。全内部ユーザーが外部ゲストを招待でき、外部組織にゲストとして招待されることもできる。**他の Microsoft Entra 組織の MFA とデバイス クレームは信頼しない**
B2B direct connect	**ブロック**。すべての外部 Microsoft Entra テナントに対して、受信・送信の両方がブロックされる
Organizational settings	**既定では1つも追加されていない**。したがって全外部組織が B2B コラボレーションの対象になる
Cross-tenant sync	他テナントからのユーザー同期は行われない

Organizational settings(組織別の設定) は特定の組織を追加して個別に構成するもので、**既定の設定より優先されます**。

B2B direct connect は相互の信頼関係が前提です。**自組織と外部組織の両方が、受信と送信の cross-tenant access settings で相互に有効化する必要があります**。B2B direct connect は **Teams Connect の共有チャネル**を支える基盤技術で、**Teams の共有チャネル以外への拡張予定はありません**。また、**異なる Microsoft クラウドのテナントとの B2B direct connect はサポートされません**。

Automatic redemption setting(自動引き換え設定) は、受信・送信の両方に存在する組織単位の信頼設定で、**初回アクセス時の同意プロンプトを省略**します。適用される場面は3つです。

項目	cross-tenant synchronization	B2B collaboration	B2B direct connect
自動引き換え設定	**必須**	任意	任意
招待メールを受け取るか	いいえ	いいえ	該当なし
同意プロンプトを受け入れる必要があるか	いいえ	いいえ	いいえ
通知メールを受け取るか	いいえ	**はい**	該当なし

> **最重要**: **同意プロンプトが省略されるのは、ホーム/ソース テナントの "送信" と、リソース/ターゲット テナントの "受信" の両方でこの設定を選んだ場合だけ**です。片方だけでは省略されません。この対応関係は「はい/いいえ」形式で問われます。

Cross-tenant synchronization settings は、**受信専用の組織別設定**です。ターゲット テナント側で「**Allow user synchronization into this tenant**」「**Allow group synchronization into this tenant**」のチェックボックスを設定します。**これらの設定は、手動招待や entitlement management など他のプロセスで作られた B2B 招待には影響しません**。

Tenant restrictions(テナント制限) は、**管理下のデバイスでユーザーが使える外部アカウントの種類を制御**します。対象は、ユーザーが未知のテナントに作ったアカウントと、外部組織がユーザーに与えたアカウントです。**tenant restrictions は他の cross-tenant access settings から独立**しており、受信・送信・信頼の設定は tenant restrictions に影響しません。テナント制限でこれらの外部アカウントを禁止し、代わりに B2B コラボレーションを使わせる

ことで、Conditional Access と MFA の強制、受信・送信アクセスの管理、雇用状態の変化や資格情報の侵害時のセッションと資格情報の失効、サインインログでの追跡ができるようになります。

Microsoft cloud settings は、異なる Microsoft Azure クラウドの組織との連携を可能にします。相互の B2B コラボレーションを確立できる組み合わせは次のとおりです。

- Microsoft Azure 商用クラウド ⇔ Microsoft Azure Government(Office GCC-High と DoD クラウドを含む)
- Microsoft Azure 商用クラウド ⇔ 21Vianet が運営する Microsoft Azure

ライセンスとロールは次のとおりです。

- Azure portal で cross-tenant access settings を構成するには、**Security Administrator** 以上、またはカスタムロールが必要です。
- **trust settings を構成する、または特定のユーザー・グループ・アプリケーションにアクセス設定を適用するには、Microsoft Entra ID P1 が必要**です。ライセンスは**構成するテナント側**に必要です。**B2B direct connect のように相互の信頼関係が必要な場合は、両方のテナントに P1** が必要です。

構成時の重要な注意点を押さえます。

- **既定の受信または送信の設定をブロックに変更すると、既存の業務上重要なアクセスがブロックされる可能性があります。**
- **ユーザーとグループに構成したアクセス設定は、アプリケーションのアクセス設定と一致していなければなりません。**矛盾する設定は許されず、構成しようとすると警告が出ます。たとえば、全外部ユーザーとグループの受信アクセスをブロックするなら、全アプリケーションへのアクセスもブロッ

クする必要があります。逆に、全ユーザーの送信アクセスを許可するなら、外部アプリケーションへの全アクセスをブロックすることはできず、少なくとも1つのアプリケーションへのアクセスを許可する必要があります。

- **既定で全アプリへのアクセスをブロックすると、Microsoft Rights Management Service(Office 365 メッセージ暗号化)で暗号化されたメールが読めなくなります。**回避するには、送信設定でアプリ ID `00000012-0000-0000-c000-000000000000` へのアクセスを許可します。
- **MFA または利用規約(ToU)を要求する Conditional Access ポリシーが、MFA 登録や ToU の同意そのものを妨げることがあります。**回避するには、送信設定(ホーム テナント)と受信設定(リソース テナント)で、**MFA 登録用に** `0000000c-0000-0000-c000-000000000000` **(Microsoft App Access Panel)、ToU 用に** `d52792f4-ba38-424d-8140-ada5b883f293` **(Microsoft Entra Terms of Use)** へのアクセスを許可します。なお、**受信設定の構成は UI の制限により Microsoft Graph API で行う必要があります。**
- 外部ユーザーに対して MFA を信頼する場合は、**Microsoft Entra ID Protection の MFA 登録ポリシーから外部ユーザーを除外することを検討**します。両方のポリシーが存在すると、外部ユーザーは要件を満たせなくなります。

cross-tenant access settings の変更は protected actions(保護されたアクション) と見なされ、Conditional Access ポリシーで追加保護できます(2.2 の主題)。

変更の追跡には、Microsoft Entra の監査ログでカテゴリ `CrossTenantAccessSettings` を絞り込みます。

設定前の実態把握の道具も対応付けで問われます。ログの保持期間が30日のことがあるため、事前確認が推奨されます。

道具	方法
PowerShell(クロステナントのサインイン アクティビティ)	**MSIdentityTools** の `Get-MSIDCrossTenantAccessActivity.ps1`
PowerShell(サインイン ログ)	`Get-MgAuditLogSignIn`
Azure Monitor	**Cross-tenant access activity ブック**
SIEM	サインイン ログをエクスポートしている場合、SIEM から取得

1-3-6 cross-tenant synchronization の実装と管理 [1.3]

cross-tenant synchronization(クロステナント同期) は、**1つの組織内の複数テナントにまたがって、B2B コラボレーション ユーザーとグループの作成・更新・削除を自動化**する機能です。目的は3つです。

1. マルチテナント組織でのシームレスなコラボレーション
2. B2B コラボレーション ユーザーの**ライフサイクル管理の自動化**
3. **ユーザーが組織を離れたときの B2B アカウントの自動削除**

プロパティを押さえます。

- **Microsoft Entra のプロビジョニング エンジン**に基づいています。
- **ソース テナントからの push(プッシュ)処理**であり、ターゲット テナントからの pull ではありません。
- **ソース テナントの internal member のみを push できます**。ソース テナントの外部ユーザー(internal guest を含む)は同期できません。

- **同期対象のユーザーはソース テナントで構成**します。
- **属性マッピングもソース テナントで構成**します。
- **ターゲット テナントの管理者は、いつでも同期を停止できます**。

どちらのテナントで何を構成するかは、対応付け問題の材料です。

テナント	Cross-tenant access settings	Automatic redemption	Sync settings の構成	対象ユーザーの指定
ソース テナント	—	必要	**必要**	**必要**
ターゲット テナント	**必要**	必要	—	—

構成の順序は並べ替え問題の定番です。

1. **組織内のテナントの構造を決める**(中央テナント型、サテライト型、メッシュ型などのトポロジ)
2. **ターゲット テナントで cross-tenant synchronization を有効にする** —— Cross-tenant access settings で「Allow user synchronization into this tenant」と B2B 自動引き換えのチェックボックスを有効にする
3. **ソース テナントで B2B 自動引き換えを有効にし、Cross-tenant synchronization ペインで同期ジョブを設定する** —— 同期するユーザー、含める属性、変換を指定する
4. **少数のユーザーでテストし**、必要な属性がそろっているか確認する
5. 対象ユーザーを増やして展開する

同期の頻度は、**開始間隔が 40 分に固定**されています。同期時間はスコープ内のユーザー数で変わり、**初回の同期サイクルは、その後の増分サイクルよりかなり長くかかります**。

同期できるオブジェクトと属性を押さえます。

項目	内容
同期できるオブジェクト	**ユーザーとセキュリティ グループ。デバイスと連絡先は非対応**
同期できるユーザーの種類	ソース テナントの **internal member のみ**。internal guest は不可
ターゲットでの作成形態	**external member(既定)** または **external guest**
同期できる属性	`displayName`、`userPrincipalName`、ディレクトリ拡張属性など。`manager` は **Azure 商用クラウドでサポート**(米国政府クラウドは非対応)
同期できない属性	**写真、custom security attributes、ディレクトリ外のユーザー属性**

グループ同期の制約は細かく問われます。

ソース	ターゲット
サポート: セキュリティ グループ(静的・動的の両方)、Microsoft 365 グループ	**サポート**: セキュリティ グループ(静的)のみ
非対応: メールが有効なセキュリティ グループ、共有メールボックス、動的配布グループ、配布グループ	**非対応**: Microsoft 365 グループ、メールが有効なセキュリティ グループ、共有メールボックス、動的配布グループ、配布グループ

加えて次の制約があります。

- **role assignable としてグループを作成することはサポートされません。**
- **入れ子のグループはサポートされません。**

- **同期スコープを「Sync only assigned users and groups」に設定する必要があります。**グループ同期を有効にすると**「Sync all users」は使えません。**
- **クラウド環境をまたぐグループ同期はサポートされません。**
- **ターゲット テナントでグループに加えた変更は自動的に上書きされません。**ソース テナントでグループが変更されたときにだけ上書きされます。
- **cross-tenant synchronization 以外の方法で作られたグループは、同期の対象になりません。**ターゲットに同名のグループが既にあっても更新しません。

既存の B2B ユーザーの扱いは頻出です。cross-tenant synchronization は `alternativeSecurityIdentifier` **という内部属性**を使って、ソース テナントの内部ユーザーとターゲット テナントの外部(B2B)ユーザーを一意に突き合わせます。これにより**既存の B2B ユーザーを更新**し、ユーザーごとにアカウントが1つだけになるようにできます。**ただし、ソース テナントの内部ユーザーとターゲット テナントの内部ユーザー(member でも guest でも)を突き合わせることはできません。**既定では `userType` **は guest から member へ更新されません**が、属性マッピングで構成できます。

プロビジョニング解除(deprovisioning) の条件は、「はい/いいえ」形式で問われます。**次の操作がソース テナントで起きると、ターゲット テナントでユーザーが soft delete されます。**

- ソース テナントでユーザーを削除する
- cross-tenant synchronization の構成からユーザーの割り当てを外す
- 構成に割り当てられているグループからユーザーを外す
- ユーザーの属性が変わり、スコープ フィルターの条件を満たさなくなる

一方、**ソース テナントでサインインをブロック(`accountEnabled = false`)しただけでは削除されず、ターゲット側でもサインインがブロックされるだけ**です。soft delete されたユーザーは、**30日以内**にソース テナントで復元・再割り当てされスコープ条件を再び満たせば、ターゲットでも復元されます。30日を過ぎると自動的に hard delete されます。

ターゲット テナント側での上書きの挙動も押さえます。**ソース テナントで変更がなければ、ターゲット テナントで加えた属性変更は残ります**。ソース テナントで変更があると、次の同期サイクルでターゲットのユーザーはソースに合わせて更新されます。**ターゲット テナントでサインインをブロックしても、ソース テナントで変更が検出されるとブロックが解除されます**。

ライセンス要件は、「どちらのテナントに何が要るか」で問われます。

シナリオ	ソース テナント	ターゲット テナント
ユーザーの cross-tenant synchronization(同一クラウド)	**Microsoft Entra ID P1**(同期される各ユーザーに1つ)	不要
グループの cross-tenant synchronization(同一クラウド)	**Microsoft Entra ID Governance または Microsoft Entra Suite**	不要
cross-cloud synchronization	**Microsoft Entra ID Governance または Microsoft Entra Suite**	不要

> **切り分け**: **ライセンスはソース テナント側に必要**です。ターゲット テナントには不要ですが、ターゲット側で使う機能次第で別途ライセンスが必要になることがあります。

cross-cloud synchronization のサポートされる組み合わせは次のとおりです。`manager` **属性の同期は cross-cloud ではサポートされません。**

ソース	ターゲット
Azure 商用	Azure Government
Azure Government	Azure 商用
Azure 商用	21Vianet が運営する Azure(中国)

使ってはいけない場面も明示されています。

- **組織をまたぐ利用(自分のマルチテナント組織の外)** は、プライバシー上の理由から想定されていません。組織をまたいで B2B ユーザーを招待するなら、**entitlement management** を使います。
- **テナント移行の道具ではありません。**同期されたユーザーの認証にはソース テナントが必要であり、SharePoint や OneDrive のユーザー データの移行も別途必要になるためです。
- **SCIM は使っていません。**Microsoft Entra ID は SCIM クライアントをサポートしますが、SCIM サーバーはサポートしていません。

トポロジは、単一方向のピアツーピア同期として構成します。**1つのソースから複数のターゲットへ、また複数のソースから1つのターゲットへ**複数のインスタンスを構成できますが、**あるソースとターゲットの組み合わせに存在できる同期インスタンスは1つだけ**です。

1-3-7 外部 ID プロバイダーの構成 —— SAML と WS-Fed [1.3]

SAML/WS-Fed identity provider federation(direct federation、直接フェデレーション) は、**SAML または WS-Fed の ID プロバイダーを使う外部組織と直接フェデレーションする**機能です。外部組織のユーザーは、**自組織が**

管理するアカウントのまま、招待の引き換えやセルフサービス サインアップを通じて、こちらのアプリやリソースにサインインできます。**新しい Microsoft Entra の資格情報を作る必要がありません**。

構成の順序は並べ替え問題の中心です。

1. **パートナーが DNS の TXT レコードを更新する必要があるかを判定する**
2. **パートナー組織の IdP を構成する**(必要なクレームと証明書利用者信頼)
3. **Microsoft Entra External ID 側でフェデレーションを構成する**
4. **引き換え順序(redemption order)を構成する**

手順1(DNS) の判定基準は明快です。**パートナーの IdP のパッシブ認証 URL のドメインが、対象ドメインまたはそのホストと一致するか**を見ます。

パッシブ認証エンドポイント (fabrikam.com のフェデレーションの場合)	DNS 変更
`https://fabrikam.com` または `https://sts.fabrikam.com/adfs` (同一ドメイン内のホスト)	**不要**
`https://fabrikamconglomerate.com/adfs` または `https://fabrikam.co.uk/adfs`	**必要**。パートナーが TXT レコードを追加する

TXT レコードの形は次のとおりです。

```
fabrikam.com.  IN   TXT
DirectFedAuthUrl=https://fabrikamconglomerate.com/adfs
```

手順2(IdP 側の構成) で必要な属性とクレームは、数値・文字列としてそのまま出題されます。

SAML 2.0 の場合 —— IdP からの応答に必要な属性

属性	従業員テナント(workforce tenant)での値
AssertionConsumerService	`https://login.microsoftonline.com/login.srf`
Audience	`https://login.microsoftonline.com/<tenant ID>/` (推奨。テナント指定のエンドポイント)
Issuer	パートナーの IdP の issuer URI

SAML 2.0 の場合 —— IdP が発行するトークンに必要なクレーム

属性名	値
NameID Format	`urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`	ユーザーのメール アドレス

WS-Fed の場合 —— IdP からのメッセージに必要な属性

属性	従業員テナントでの値
PassiveRequestorEndpoint	`https://login.microsoftonline.com/login.srf`
Audience	`https://login.microsoftonline.com/<tenant ID>/` (推奨)

属性	従業員テナントでの値
Issuer	パートナーの IdP の issuer URI

WS-Fed の場合 —— IdP が発行するトークンに必要なクレーム

属性	値
ImmutableID	`http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID`
emailaddress	`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`

> **SAML と WS-Fed の分かれ目**: **必要なクレームが違います**。SAML 2.0 は **NameID Format** と **emailaddress**、WS-Fed は **ImmutableID** と **emailaddress** です。この差が対応付け問題になります。また、**WS-Fed のプロバイダーで Microsoft Entra ID との互換性がテストされているのは AD FS と Shibboleth の2つだけ**です。

Audience の注意として、既存のグローバル エンドポイント(`urn:federation:MicrosoftOnline`)で構成されたフェデレーションは動き続けますが、**新しいフェデレーションでは、外部 IdP がグローバルの issuer URL を期待していると動作しません**。新規はテナント指定のエンドポイントを使います。

Issuer の形式にも制約があります。**IdP の Issuer 値は、RFC 3986 形式に従う有効な URI でなければなりません**(例: `https://testdev.example.com`)。**単語1つや URI でない値(例: `testdev`)はサポートされず、ポータルで拒否されます**。

手順3(Microsoft Entra 側の構成) は、Entra ID > External Identities > **All identity providers** > **Custom** タブ > **Add new** > **SAML/WS-Fed** から行います。**必要なロールは External Identity Provider Administrator** 以上です。

入力する項目は次のとおりです。

- **Display name**
- **Identity provider protocol**(SAML または WS-Fed)
- **Domainless**(選ぶとユーザーのメール アドレスのドメイン チェックを行わない)
- **Domain name of federating IdP**(初回は1つだけ。後から追加可能)
- **Issuer URI**(SAML)または **Entity ID**(WS-Fed)
- **Passive authentication endpoint**(SAML)または **Passive requestor endpoint**(WS-Fed)。**https のみサポート**
- **Certificate**(署名証明書の ID)
- **Metadata URL**

> **Metadata URL の重要性**: **Metadata URL は任意ですが、強く推奨されます。**指定しておくと、**署名証明書の有効期限切れ時に Microsoft Entra ID が自動更新できます。**指定しない場合、または有効期限前に証明書がローテーションされた場合、**署名証明書を手動で更新する必要があります。**

メタデータ ファイルがあれば **Parse metadata file** で自動入力でき、なければ **Input metadata manually** で手入力します。**フェデレーション ポリシー**

が有効になるまで 5〜10 分かかります。この間、そのドメインのセルフサービス サインアップや招待の引き換えを試みてはいけません。

手順4(引き換え順序) は、検証済みドメインで B2B コラボレーションのフェデレーションを構成した場合に必要です。**cross-tenant access settings の受信 B2B コラボレーションの「Redemption order」タブで、SAML/WS-Fed identity providers を Primary identity providers の一番上に移動**します。

Microsoft Entra ID の検証済みドメインとの直接フェデレーションもサポートされています。**別の Microsoft Entra テナントで検証済みのドメインに対して、外部 IdP との直接フェデレーションを設定できます。**ただし、**同じテナント内で検証済みのドメインに対して直接フェデレーションを設定することはできません。**

Domainless SAML IdP federation(ドメインレス フェデレーション) は、**ユーザーのメール ドメインと IdP に構成されたドメインの一致を要求しない**構成です。従来のフェデレーションではメール クレームのドメインが検証され、一致しないと次のエラーになります。

```
AADSTS5000819: SAML Assertion is invalid. Email address claim is
missing or does not match domain from an external realm.
```

ドメインレスを有効にすると、**Microsoft Entra ID は Issuer URI の関連付けに基づいて認証要求をルーティング**し、メール ドメインの照合を行いません。yahoo.com や gmail.com など任意のドメインのメール アドレスで認証できます。**1つのテナントに構成できるワイルドカード IdP は現在1つだけ**です。招待時には、**リダイレクト URL に `domain_hint` パラメーターを含め、その値を SAML IdP 構成の Issuer URI と一致させます。**

フェデレーションの削除には順序があります。**Domains 列で1つを残して他のドメインをすべて削除してから、Delete Configuration を実行**します。フェデレーションを削除すると、**既に招待を引き換えたフェデレーション ゲスト ユーザーはサインインできなくなります**。再びアクセスさせるには**引き換え状態のリセット**が必要です。

既知の問題として、**IdP の構成を保存していなくても、無効なドメイン名を入力すると IdP 構成が削除されてしまう**という不具合があります。

1-3-8 到達目標 1.3 の分かれ目の早見表 [1.3]

要件	正解	なぜ他は違うか
取引先(Microsoft Entra 組織)の MFA を信頼して二重の MFA をなくしたい	**cross-tenant access settings の trust settings**(P1・受信側)	external collaboration settings に信頼設定はない
ゲストが他のユーザーやグループを一切見られないようにしたい	**external collaboration settings の最も制限的な Guest user access**	cross-tenant access settings はディレクトリの可視性を制御しない
特定の担当者にだけゲストの招待を許したい	**招待設定を「Only users assigned to specific admin roles」にし、Guest Inviter を割り当てる**	User Administrator は広すぎる
自社の複数テナント間でユーザーを自動作成・自動削除したい	**cross-tenant synchronization**(ソース側に P1)	手動招待ではライフサイクル管理が自動化されない
取引先(別組織)のユーザーを継続的に招待・管理したい	**entitlement management**	cross-tenant synchronization は自組織のマルチテナント向け

要件	正解	なぜ他は違うか
同意プロンプトを出さずにゲストにアクセスさせたい	**ホーム側の送信とリソース側の受信の両方で automatic redemption を有効化**	片方だけでは省略されない
ゲストが Microsoft アカウントで引き換えるのをやめさせたい	**Redemption order でフォールバックの Microsoft アカウントをオフにし、email OTP を有効にする**	フォールバックを両方無効にはできない
AD FS を使う取引先のユーザーを、こちらの資格情報を作らずにサインインさせたい	**SAML/WS-Fed direct federation**	B2B の通常招待では、ソーシャル ID か Microsoft アカウントか OTP になる
ユーザーのメール ドメインが IdP のドメインと一致しない	**Domainless SAML IdP federation**	通常のフェデレーションでは AADSTS5000819 になる
署名証明書の期限切れで止まるのを避けたい	**Metadata URL を指定する**	証明書 ID だけでは自動更新されない
管理下デバイスで未知のテナントのアカウントを使わせたくない	**tenant restrictions**	受信・送信設定は自組織のリソースへのアクセスを制御するもので、外部アカウントの利用自体は止められない
Teams の共有チャネルで外部組織と共同作業したい	**B2B direct connect**(双方が受信・送信を相互に有効化)	B2B コラボレーション ゲストは共有チャネルでサポートされない

1-4 ハイブリッド ID を実装および管理する [1.4]

1-4-1 この節の全体像 —— 同期と認証は別の軸 [1.4]

ハイブリッド ID の設問でつまずく最大の原因は、**「同期の仕組み」と「認証の方法」を1つの軸だと思い込むこと**です。この2つは独立しています。

軸	選択肢	決めること
同期(プロビジョニング)	**Microsoft Entra Connect Sync / Microsoft Entra Cloud Sync**	オンプレミス AD のユーザー・グループ・連絡先を、どうやってクラウドへ運ぶか
認証(サインイン)	**password hash synchronization (PHS) / pass-through authentication (PTA) / federation(AD FS)**	ユーザーがサインインするとき、パスワードをどこで検証するか

> **公式に明記されている一点: 認証方法は、使用する同期テクノロジ(Connect Sync でも Cloud Sync でも)とは独立して適用されます。同期テクノロジの選択が、ユーザー サインインの認証動作を決めたり変えたりすることはありません。**「Cloud Sync だから PTA が使える/使えない」といった因果を作る選択肢は、この一文で切れます。

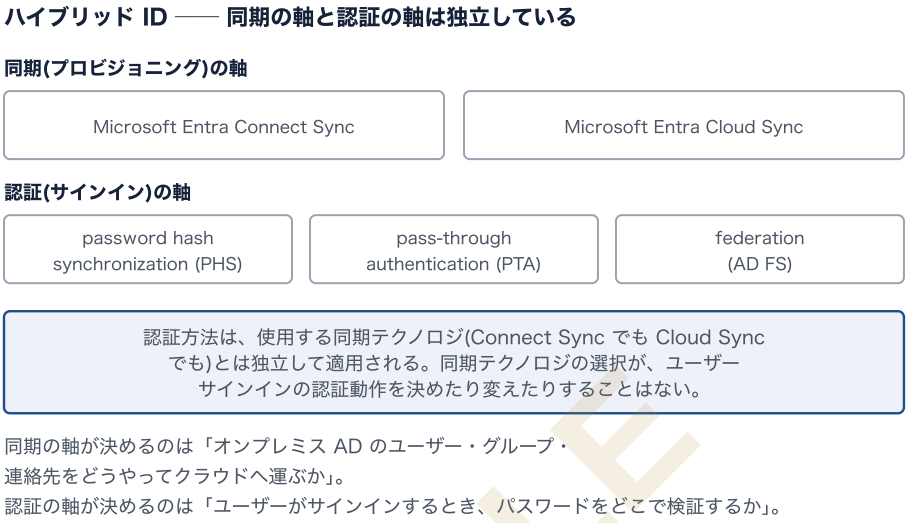

図 1-7　ハイブリッド ID —— 同期の軸と認証の軸は独立している

この節の箇条書きは、上の2軸に seamless SSO(サインイン体験)、AD FS からの移行(移行手順)、Connect Health(監視)を足した構成です。

1-4-2 Microsoft Entra Connect Sync の実装と管理 [1.4]

Microsoft Entra Connect は、ハイブリッド ID を実現するオンプレミスに置く Microsoft のアプリケーションです。**利用は無料**で、Azure サブスクリプションに含まれます。

Microsoft Entra Connect の機能は次の5つです。

機能	内容
Password hash synchronization	オンプレミス AD のパスワードのハッシュを Microsoft Entra ID と同期するサインイン方法

機能	内容
Pass-through authentication	オンプレミスと同じパスワードを使わせるが、フェデレーション環境の追加インフラを必要としないサインイン方法
Federation integration	オンプレミスの AD FS インフラを使ったハイブリッド環境の構成。証明書の更新や AD FS サーバーの追加展開といった管理機能も提供する(**任意の機能**)
Synchronization	ユーザー・グループ・その他オブジェクトを作成し、オンプレミスの ID 情報とクラウドを一致させる。**パスワード ハッシュの同期を含む**
Health Monitoring	Microsoft Entra Connect Health による監視。Microsoft Entra admin center から一元的に確認できる

Microsoft Entra Connect V2 は、旧版で使われていた古い基盤コンポーネントを新しいものに置き換えた版です。**Azure AD Connect V1 は 2022年8月31日に廃止され、サポートされていません。V1 のインストールは予期せず動作を停止する可能性があります。**V2 での主な変更は次のとおりです。**V2.0 のリリースに新機能は含まれていません** —— 基盤コンポーネントの更新だけです。

変更点	内容
SQL Server 2019 LocalDB	旧版は SQL Server 2012 LocalDB。SQL Server 2012 は 2022年7月に延長サポート終了
MSAL 認証ライブラリ	旧版は ADAL。ADAL は 2022年12月に非推奨

変更点	内容
Visual C++ Redist 14	SQL Server 2019 の要件。パッケージと共にインストールされる
TLS 1.2	**バージョン 2.3.20.0 以降は TLS 1.2 が必須**。更新前に TLS 1.2 を有効にしておく必要がある
全バイナリを SHA2 で署名	SHA1 署名のバイナリを廃止
Windows Server 2012 / 2012 R2 は非対応	SQL Server 2019 が Windows Server 2016 以降を要求するため。**古い Windows Server にはインストールできない**
PowerShell 5.0	新しい前提条件。Windows Server 2016 以降には既に含まれる

移行のポイントは次のとおりです。

- **どのバージョンからでも V2 へのアップグレードがサポートされます。**
- **構成のエクスポート/インポート機能**を使えば、現在のサーバーの構成を新しいサーバーへ移せます。OS のバージョンも一緒に上げるときの定番の手段です。
- **自動アップグレードを有効にしている場合、Windows Server 2016 以降で TLS 1.2 が有効なら自動的に最新版へ上がります。**
- **V2 へのアップグレードで SQL 2012 コンポーネントが自動的にアンインストールされることはありません。**
- **アップグレード後に ADSync の PowerShell コマンドレットが動かないのは既知の問題**です。PowerShell セッションを再起動し、`Import-module -Name "C:\Program Files\Microsoft Azure AD Sync\Bin\ADSync"` でモジュールを読み込み直します。

- **Microsoft Entra Connect Health for Sync には Microsoft Entra Connect Sync V2 が必要**です。

Microsoft は Cloud Sync への移行を推奨しています。「Microsoft Entra Cloud Sync は同期の将来形であり、Microsoft Entra Connect を置き換えるもの」と明記されています。**Check sync ツール**で、Cloud Sync が自組織に適しているかを判定できます。

1-4-3 Microsoft Entra Cloud Sync の実装と管理 [1.4]

Microsoft Entra Cloud Sync は、**Active Directory と Microsoft Entra ID の間でユーザー・グループ・連絡先を同期する、クラウド管理型のハイブリッド ID 同期サービス**です。**Microsoft のハイブリッド ID における戦略的方向性**と位置づけられています。

2つのコンポーネントからなります。

コンポーネント	役割
Microsoft Entra provisioning agent	Active Directory と Microsoft Entra ID をつなぐ**軽量なオンプレミス エージェント**。**Microsoft Entra Application Proxy と Pass-Through Authentication と同じ実績ある技術**を使い、**送信接続のみ**を必要とし、**クラウドから自動更新**される
Microsoft Entra provisioning service	同期の構成・スケジュール・処理を管理する**クラウド側のオーケストレーション サービス。スケジューラー ベースで、同期は2分ごと**に行われる

動作の流れは次のとおりです。Cloud Sync は **SCIM(System for Cross-domain Identity Management)標準**を利用しています。

1. **エージェントの通信**: プロビジョニング エージェントは **Azure Service Bus を通じて、Microsoft Entra サービスへの永続的な送信接続を維持**し、同期要求を待ち受ける
2. **要求の処理**: 同期時に、エージェントがクラウド サービスから **SCIM 要求**を受け取り、Active Directory に問い合わせる
3. **データのフィルタリングと変換**: エージェントが、構成されたスコープ ルールと属性マッピングに基づいてデータをフィルターし変換してから応答を返す
4. **クラウドでの処理**: プロビジョニング サービスが応答を処理して Microsoft Entra ID に変更をコミットし、**ウォーターマークによる追跡**で増分更新を扱う

Cloud Sync の主要な機能を押さえます。ここが Connect Sync との差を作ります。

機能	内容
クラウド管理の構成	すべての同期構成が Microsoft Entra ID に保存され、Microsoft Entra admin center から管理される。**VPN なしでどこからでも設定変更・状態監視・トラブルシューティングができる**
複数エージェントによる高可用性	**複数のアクティブなプロビジョニング エージェント**を別々のサーバーに展開でき、**構成変更なしで自動フェールオーバー**する。個々のエージェントが利用できなくなっても同期は継続する

機能	内容
切断されたフォレストの同期 (disconnected forest synchronization)	**複数の切断された Active Directory フォレストを、複雑な構成や複数の同期インスタンスなしでネイティブに扱える。**合併・買収、歴史的な複数フォレスト環境、フォレストを接続できないシナリオに対応
簡素なインストールと管理	軽量エージェントは最小限のサーバー リソースで動き、**ドメイン コントローラー上にも専用サーバー上にも展開できる。**セキュリティ更新とパッチは自動
高度なプロビジョニング シナリオ	**クラウドから AD へのプロビジョニング**(オンプレミス アプリを統制するための AD へのグループ プロビジョニングなど)に対応

Cloud Sync を検討すべき場面は次のとおりです。

- 合併・買収で、**切断されたフォレストを迅速に統合**する必要がある
- **単一障害点をなくし**、同期の信頼性を高めたい
- 管理を簡素化し、オンプレミス インフラを減らしたい
- **フォレストの統合が現実的でない**マルチフォレスト組織
- クラウド ファーストの ID 戦略を実装し、**クラウドから AD へのプロビジョニング**が必要

Cloud Sync が利用できるクラウドは、Microsoft 商用、米国政府、**21Vianet(中国)** です。ただし **21Vianet(中国)クラウドでは、オンプレミス ID 向けの SSPR を Cloud Sync と併用できません。**

Microsoft Entra ecosystem との統合では、**Microsoft Entra ID Governance**(ハイブリッド ID のライフサイクル管理とアクセス ガバナンス)、**Source of Authority (SOA) management**(Microsoft Entra ID を権威あ

る ID ソースにするクラウド ファースト戦略)、**HR 主導のプロビジョニング**との連携がサポートされます。

Connect Sync と Cloud Sync の使い分けは、次の観点で判断します。

観点	Microsoft Entra Connect Sync	Microsoft Entra Cloud Sync
オーケストレーションの場所	**オンプレミス**(同期サーバー)	**Microsoft Online Services(クラウド)**
構成の保存場所	オンプレミスのサーバー	**Microsoft Entra ID**
高可用性	**ステージング モードのサーバーを別途用意**(スタンバイ構成)	**複数のアクティブ エージェントによる自動フェールオーバー**
切断されたフォレスト	複雑な構成が必要	**ネイティブに対応**
エージェントの更新	サーバーの保守が必要(自動アップグレード機能あり)	**クラウドから自動更新**
同期間隔	既定の同期スケジューラー サイクル	**2分ごと**
位置づけ	従来からの方式	**Microsoft の戦略的方向性・将来形**

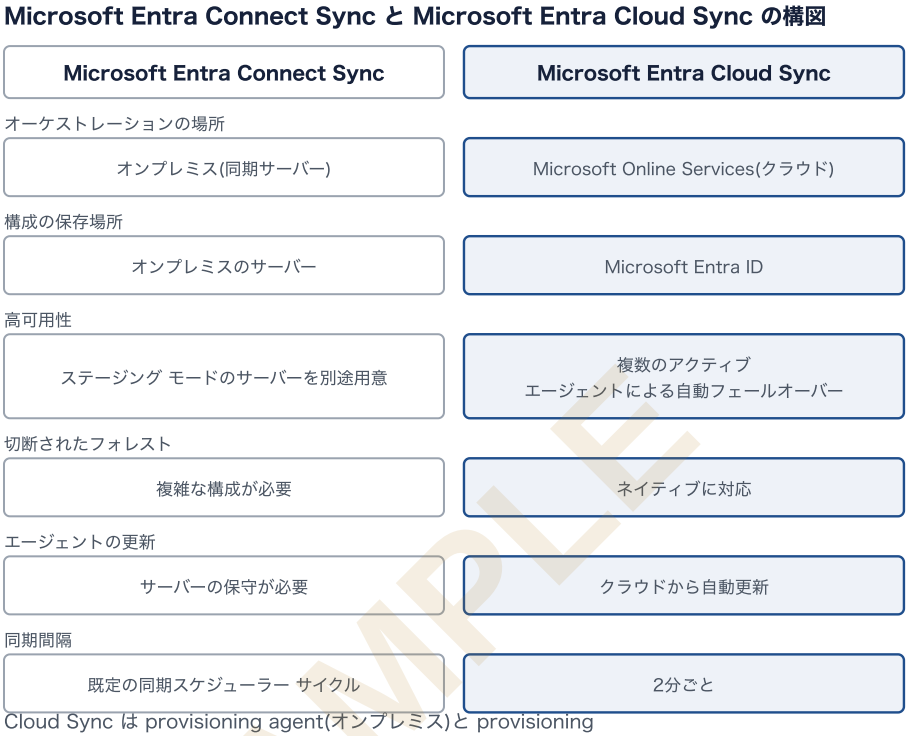

図 1-8　Microsoft Entra Connect Sync と Microsoft Entra Cloud Sync の構図

1-4-4 password hash synchronization (PHS) の実装と管理 [1.4]

password hash synchronization は、**オンプレミス ディレクトリのオブジェクトに対する認証を有効にする最も簡単な方法**です。ユーザーはオンプレミスと同じユーザー名とパスワードを使え、**追加のインフラを展開する必要がありません。**

動作の要点を押さえます。

- **認証はクラウドで行われます。**パスワード ハッシュが同期され、Microsoft Entra ID が資格情報を検証します。
- **パスワードは Microsoft Entra ID にクリア テキストでも、可逆的なアルゴリズムで暗号化された形でも保存されません。**
- **有効にすると、password hash synchronization は Microsoft Entra Connect Sync のプロセスの一部として2分ごとに実行されます。**
- **オンプレミス以外のサーバー要件はありません。**インターネットやネットワークの追加要件もなく、**TLS/SSL 証明書も不要**です。
- **専用の正常性監視ソリューションは不要**です。

PHS が必須になる機能は最頻出です。

- **Microsoft Entra ID Protection**(P2 が必要)は、**どのサインイン方法を選んでいても、"漏洩した資格情報を持つユーザー" レポートを提供するために password hash synchronization を必要とします。**
- **Microsoft Entra Domain Services** は、マネージド ドメインで企業の資格情報をプロビジョニングするために password hash synchronization を必要とします。

> **これが最も出る一点: PTA やフェデレーションを主要な認証方法にしている組織でも、Microsoft は PHS を併せて有効にすることを推奨しています。**理由は3つです。**(1) 高可用性とディザスター リカバリー**(PTA とフェデレーションはオンプレミス インフラに依存する)、**(2) オンプレミス障害の生存性**(ランサムウェア攻撃などでオンプレミス サーバーが落ちても、PHS を事前に有効にしていた組織は主要認証方法を PHS に切り替えて数時間で復旧できた。有効にしていなかった組織はオンプレミス ID インフラの復旧に数週間かかった)、**(3) ID 保護**(漏洩資格情報の検出)。

PHS の考慮事項(制約) も押さえます。

- **オンプレミスのアカウント状態の変更が即座に反映されません。**ユーザー アカウントの状態が Microsoft Entra ID に同期されるまで、クラウド アプリへのアクセスが続きます。**アカウントの一括無効化などの後は、新しい同期サイクルを走らせる**ことで対処します。
- **サポートされるアカウント状態は「無効化されたアカウント」のみで、最大30分の遅れがあります。アカウントのロックアウト、アカウントの有効期限、パスワードの有効期限、サインイン時間**は反映されません。
- **パスワードの有効期限切れとアカウントのロックアウト状態は、Microsoft Entra Connect では Microsoft Entra ID に同期されません。**ユーザーのパスワードを変更して「次回サインイン時にパスワードの変更が必要」フラグを設定すると、**ユーザーがパスワードを変更するまでパスワード ハッシュは同期されません。**
- **オンプレミスでパスワードを変更した場合、新しいパスワード ハッシュが Microsoft Entra ID に同期されるまで、そのパスワードではサインインできません。**この同期は通常2分ごとですが、構成により変わります。
- **PHS で MFA を使う組織は、Microsoft Entra multifactor authentication または Conditional Access のカスタム制御を使う必要があります。フェデレーションに依存するサード パーティやオンプレミスの MFA は使えません。**

PHS でサポートされるサインインの種類は、UserPrincipalName + パスワード、**seamless SSO による Windows 統合認証**、**Alternate login ID**、Microsoft Entra 参加デバイス、Microsoft Entra ハイブリッド参加デバイス、証明書とスマート カード認証です。

高可用性については、PHS を使ったクラウド認証は、Microsoft の全データセンターにスケールするクラウド サービスとして高可用性が確保されています。**PHS が長時間止まらないようにするには、2台目の Microsoft Entra Connect サーバーをステージング モードのスタンバイ構成で展開**します。

高度なシナリオとして、**smart password lockout** と **漏洩資格情報レポート(P2)** がサポートされます。**Windows Hello for Business** は **Key trust model** と **Hybrid Cloud Trust** に対応します。

1-4-5 pass-through authentication (PTA) の実装と管理 [1.4]

pass-through authentication は、**1台以上のオンプレミス サーバー上で動くソフトウェア エージェント**を使って、Microsoft Entra の認証サービスにシンプルなパスワード検証を提供する方法です。**サーバーがオンプレミスの Active Directory に対して直接ユーザーを検証するため、パスワードの検証がクラウドで行われません。**

> **正確な表現に注意**: 比較表では、PTA の「認証はどこで行われるか」は「**クラウド。ただしオンプレミスの認証エージェントとのセキュアなパスワード検証交換の後**」と記されています。「パスワードの検証はオンプレミスで行われるが、認証フロー自体はクラウドを経由する」という理解が正確です。

PTA を選ぶ理由は明確です。**オンプレミスのユーザー アカウント状態、パスワード ポリシー、サインイン時間を即座に適用するというセキュリティ要件がある組織**です。

サポートされるアカウント状態が、PHS との最大の差です。

アカウント状態	PHS	PTA	フェデレーション (AD FS)
無効化されたアカウント	対応(**最大30分の遅れ**)	**対応**	対応
アカウントのロックアウト	非対応	**対応**	対応
アカウントの有効期限	非対応	**対応**	対応
パスワードの有効期限	非対応	**対応**	対応
サインイン時間 (logon hours)	非対応	**対応**	対応

3つの認証方法 —— パスワードをどこで検証するか

password hash synchronization (PHS)
認証はクラウドで行われる。パスワード ハッシュが同期され、Microsoft Entra ID が資格情報を検証する。オンプレミス以外のサーバー要件はなく、TLS/SSL 証明書も不要

pass-through authentication (PTA)
オンプレミス サーバー上の軽量エージェントが Active Directory に対して直接ユーザーを検証する。エージェントはインターネットへの送信アクセスとドメイン コントローラーへのアクセスが必要。境界ネットワーク(DMZ)への展開はサポートされない

federation(AD FS)
オンプレミスの AD FS インフラを使う。Microsoft Entra Connect の Federation integration は任意の機能

オンプレミスのアカウント状態が即座に効くか

項目	PHS	PTA	AD FS
無効化されたアカウント	対応	対応	対応
アカウントのロックアウト	非対応	対応	対応
アカウントの有効期限	非対応	対応	対応
パスワードの有効期限	非対応	対応	対応
サインイン時間(logon hours)	非対応	対応	対応

無効化されたアカウントは、PHS では最大30分の遅れがある。
PTA やフェデレーションを主要な認証方法にしている組織でも、Microsoft は PHS を併せて有効にすることを推奨している。
PHS からのフェールオーバーは自動では起きない —— Microsoft Entra Connect でサインオン方法を手動で切り替える。

図 1-9　3つの認証方法 —— パスワードをどこで検証するか

PTA の展開要件を押さえます。

- **1台以上(推奨は3台)の軽量エージェント**を既存のサーバーにインストールします。
- エージェントは**オンプレミスの Active Directory Domain Services(ドメイン コントローラーを含む)にアクセスできる**必要があります。

- エージェントは**インターネットへの送信アクセス**とドメイン コントローラーへのアクセスが必要です。
- **PTA はドメイン コントローラーへの制約のないネットワーク アクセスを必要とするため、エージェントを境界ネットワーク(DMZ)に展開することはサポートされません。**
- **すべてのネットワーク トラフィックは暗号化され、認証要求に限定**されます。
- **TLS/SSL 証明書は不要**です。
- 正常性監視は **Microsoft Entra admin center からエージェントの状態**として提供されます(AD FS のような Connect Health は必須ではありません)。

高可用性については、**Microsoft Entra Connect サーバー上の最初のエージェントに加えて、2台の追加のパススルー認証エージェントを展開すること**が推奨されます。**3台展開しておけば、1台がメンテナンスで停止している間にもう1台が故障しても認証が継続**します。

PHS をバックアップ認証方法として使う構成が定番です。**ただしフェールオーバーは自動では起きません。Microsoft Entra Connect を使ってサインオン方法を手動で切り替える必要があります。**この「自動ではない」が「はい/いいえ」形式で問われます。

PTA での MFA も PHS と同じ制約です。**Microsoft Entra multifactor authentication または Conditional Access のカスタム制御を使う必要があり、フェデレーションに依存するサード パーティやオンプレミスの MFA は使えません。漏洩資格情報の検出など高度な機能には、PTA を選んでいても PHS の展開が必要**です。

PTA でサポートされる高度なシナリオは **smart password lockout** です。**Windows Hello for Business** は **Key trust model** と **Hybrid Cloud Trust** に対応しますが、**どちらも Windows Server 2016 のドメイン機能レベルが必要**です。

1-4-6 seamless single sign-on (SSO) の実装と管理 [1.4]

Microsoft Entra seamless single sign-on(seamless SSO) は、**企業ネットワークに接続された企業デバイス上のユーザーを自動的にサインインさせる**機能です。有効にすると、ユーザーは Microsoft Entra ID へのサインインでパスワードを入力する必要がなくなり、多くの場合ユーザー名の入力すら不要になります。

組み合わせられる認証方法が最初の分かれ目です。

認証方法	seamless SSO
password hash synchronization	組み合わせ可能
pass-through authentication	組み合わせ可能
Active Directory Federation Services (AD FS)	適用されない

PRT による SSO との使い分けが2つ目の分かれ目です。

デバイス	推奨
Windows 10、Windows Server 2016 以降	primary refresh token (PRT) による SSO
Windows 7、Windows 8.1	seamless SSO

seamless SSO はデバイスがドメインに参加している必要がありますが、Windows 10 の Microsoft Entra 参加デバイスや Microsoft Entra ハイブリッド参加デバイスでは使われません。Microsoft Entra 参加、Microsoft Entra ハイブリッド参加、Microsoft Entra 登録デバイスでの SSO は **primary refresh token (PRT)** に基づいて動作します。

主な利点は次のとおりです。

- **オンプレミスに追加のコンポーネントが不要**です。
- **グループ ポリシーで一部または全ユーザーに展開**できます。
- **AD FS インフラなしで、Windows 10 以外のデバイスを Microsoft Entra ID に登録**できます(workplace-join クライアントのバージョン 2.1 以降が必要)。
- **無料の機能**であり、有料エディションの Microsoft Entra ID は不要です。

機能の詳細を押さえます。

- **サインインのユーザー名は、オンプレミスの既定のユーザー名 (`userPrincipalName`)でも、Microsoft Entra Connect で構成した別の属性(Alternate ID)でもかまいません。**どちらでも動くのは、**seamless SSO が Kerberos チケットの `securityIdentifier` クレームを使って Microsoft Entra ID 側のユーザー オブジェクトを探す**ためです。
- **seamless SSO は日和見的(opportunistic)な機能**です。**何らかの理由で失敗した場合、ユーザーのサインイン体験は通常どおりに戻ります**(サインイン ページでパスワードを入力する)。
- アプリケーションが `domain_hint` **(OpenID Connect)または** `whr` **(SAML)** パラメーター(テナントを識別)、あるいは `login_hint` パラメ

ーター(ユーザーを識別)を Microsoft Entra のサインイン要求に渡すと、**ユーザー名もパスワードも入力せずに自動サインイン**されます。

- アプリケーションが **共通エンドポイント**（`https://login.microsoftonline.com/common/<...>`）**ではなく、テナント指定のエンドポイント**（`https://login.microsoftonline.com/contoso.com/<..>` **または** `https://login.microsoftonline.com/<tenant_ID>/<..>`）にサインイン要求を送る場合も、サイレント サインインになります。
- **サインアウトはサポートされます**。これにより、seamless SSO で自動サインインされる代わりに、別の Microsoft Entra アカウントを選べます。
- **Microsoft 365 の Win32 クライアント(Outlook、Word、Excel など)は、バージョン 16.0.8730.xxxx 以降で非対話フローによりサポート**されます。OneDrive はサイレント サインインのために **OneDrive silent config 機能**を有効にする必要があります。
- **Microsoft Entra Connect から有効化**します。

有効化の手順(PowerShell)は並べ替え問題の材料です。**Active Directory フォレストごとに個別に有効化**します。

1. Microsoft Entra Connect サーバーにサインインする
2. `%programfiles%\Microsoft Entra Connect` フォルダーへ移動する
3. `Import-Module .\AzureADSSO.psd1` でモジュールをインポートする
4. PowerShell を管理者として実行し、`New-AzureADSSOAuthenticationContext` を呼ぶ(Hybrid Identity Administrator の資格情報を入力)
5. `Get-AzureADSSOStatus | ConvertFrom-Json` で、この機能が有効になっているフォレストの一覧を確認する(**テナント レベルの既定は false**)

6. `$creds = Get-Credential` で対象フォレストのドメイン管理者の資格情報を入力する
7. `Enable-AzureADSSOForest -OnPremCredentials $creds` を実行する。このコマンドが、**seamless SSO に必要な `AZUREADSSOACC` コンピューター アカウントをオンプレミスのドメイン コントローラーに作成**する
8. **seamless SSO は URL がイントラネット ゾーンにあることを必要とします**。グループ ポリシーでその URL を配布する

> **必要なロール**: **seamless SSO を特定の Active Directory フォレストで有効にするにはドメイン管理者**が、**テナント側の操作には Hybrid Identity Administrator** が必要です。

ブラウザーのサポートは、**Kerberos 認証が可能なプラットフォームとブラウザー**上で、**モダン認証をサポートする Web ブラウザー ベースのクライアントと Office クライアント**が対象です。

OS \ ブラウザー	Microsoft Edge	Google Chrome	Mozilla Firefox	Safari
Windows 10 / 11	対応	対応	対応(追加構成が必要)	該当なし
Windows 8.1	対応 (Chromium 版)	対応	対応(追加構成が必要)	該当なし
Windows 8	該当なし	対応	対応(追加構成が必要)	該当なし
Windows Server 2012 R2 以降	対応 (Chromium 版)	対応	対応(追加構成が必要)	該当なし

OS \ ブラウザー	Microsoft Edge	Google Chrome	Mozilla Firefox	Safari
Mac OS X	該当なし	対応(追加構成が必要)	対応(追加構成が必要)	対応(追加構成が必要)

Microsoft Edge legacy はサポートされなくなりました。

1-4-7 AD FS から他の認証・認可メカニズムへの移行 [1.4]

フェデレーション(AD FS)からクラウド認証への移行は、**staged rollout(段階的ロールアウト)によるテスト → ドメインのカットオーバー**という2段階で進みます。**この2つを混同しないことが最重要**です。

staged rollout(SRO)とは何か

staged rollout は、**フェデレーション ドメインを持つ組織が、ドメイン全体をフェデレーションからマネージドへ切り替える前に、一部のユーザー グループでクラウド認証をテストするための一時的なテスト メカニズム**です。

> **絶対に押さえる一点: staged rollout は恒久的な構成として設計されていません。staged rollout はドメインをフェデレーションからマネージドへ切り替えません。最終的なカットオーバーは、Microsoft Entra Connect または PowerShell を使って別途行う必要があります。**
> 「staged rollout で全ユーザーを移せば移行完了」という選択肢は誤答です。

ベスト プラクティスとして次が挙げられています。

- staged rollout は、ドメイン全体の変更の前にクラウド認証の動作を検証する**パイロット グループにのみ**使う

- **テスト中はフェデレーション IdP を維持し**、認証のフォールバック経路を確保する
- 明確な移行計画がない限り、**全ユーザーを staged rollout に入れない**
- テスト中は認証フローを監視して異常を早期に検出する
- テストが成功したら**速やかにマネージド認証へカットオーバー**する

前提条件

- **フェデレーション ドメインを持つ Microsoft Entra テナント**があること
- 移行先として **password hash synchronization**、**pass-through authentication**、**Microsoft Entra certificate-based authentication (CBA) 設定** のいずれかを決めていること
- サイレント サインイン体験のために **SSO を有効にする**ことが推奨される (Windows 7 / 8.1 のドメイン参加デバイスは seamless SSO、Windows 10 / Windows Server 2016 以降は **PRT による SSO**)
- **移行対象ユーザー向けのテナント ブランディングと Conditional Access ポリシーを事前に構成**しておくこと
- **フェデレーションからクラウド認証へ移行した場合、DirSync 設定** `synchronizeUpnForManagedUsersEnabled` **が** `true` **になっていることを確認する。**そうでないと、マネージド認証を使うライセンス付きユーザー アカウントの UPN や代替ログイン ID への同期更新が許可されない
- Microsoft Entra MFA を使う予定なら、**combined registration(統合登録)を有効化**することが推奨される
- **staged rollout の機能を使うには、テナントで Hybrid Identity Administrator である必要がある**

- seamless SSO を特定の Active Directory フォレストで有効にするには**ドメイン管理者**が必要
- ハイブリッド Microsoft Entra ID または Microsoft Entra join を展開する場合は **Windows 10 1903 更新プログラム**へのアップグレードが必要

サポートされるシナリオ

- **Microsoft Entra Connect でプロビジョニングされたユーザーのみ。クラウドのみのユーザーには適用されません。**
- **ブラウザーとモダン認証クライアントでのサインイン トラフィック。レガシ認証を使うアプリケーションやクラウド サービスは、フェデレーション認証フローにフォールバック**します(モダン認証を無効にした Exchange Online、モダン認証非対応の Outlook 2010 など)。
- **グループ内のユーザー数に上限はありません。ただし機能ごとに最大10グループ**です(password hash sync に10、pass-through authentication に10、seamless SSO に10)。
- **Windows 10 バージョン 1903 以降**で、ユーザーの UPN がルーティング可能かつドメイン サフィックスが Microsoft Entra ID で検証済みの場合、**フェデレーション サーバーへの見通しなしに Windows 10 ハイブリッド参加または Microsoft Entra join の primary refresh token を取得**できます。
- **Autopilot 登録は Windows 10 バージョン 1909 以降**で staged rollout でサポートされます。

サポートされないシナリオ

- **POP3 や SMTP などのレガシ認証**

- **セキュリティ グループに staged rollout が有効な場合、オンプレミス ドメインへの書き戻しを伴う SSPR はサポートされません**
- `domain_hint` **クエリ パラメーターを送るアプリケーション**では、staged rollout の対象ユーザーでもフェデレーション認証が使われ続けます
- **機能ごとに最大10グループ、入れ子のグループは非対応、動的グループは非対応、グループ内の連絡先オブジェクトはグループの追加をブロックする**
- **セキュリティ グループを初めて追加するときは、UX のタイムアウトを避けるために 200 ユーザーまで**に制限されます。追加後は、必要に応じてグループへ直接ユーザーを追加できます
- **PHS で staged rollout 中は、既定でパスワードの有効期限が適用されません。**適用するには `CloudPasswordPolicyForPasswordSyncedUsersEnabled` を有効にします。有効にすると、**パスワードの有効期限ポリシーはオンプレミスでパスワードが設定された時点から90日に設定され、カスタマイズできません。**staged rollout 中の `PasswordPolicies` 属性のプログラムによる更新はサポートされません
- **Windows 10 バージョン 1903 より前**の Windows 10 ハイブリッド参加または Microsoft Entra join の primary refresh token 取得は、**フェデレーション サーバーの WS-Trust エンドポイントにフォールバック**します
- **ユーザーのオンプレミス UPN がルーティング不可能な場合**、すべてのバージョンで WS-Trust エンドポイントにフォールバックし、**staged migration が完了してフェデレーションに依存しなくなると動作しなくなります**
- **Windows 10 バージョン 1903 以降の非永続的 VDI 環境**では、フェデレーション ドメインのままにする必要があります。**非永続的 VDI ではマネージド ドメインへの移行がサポートされません**

- **フェデレーション サーバーを登録機関として発行された証明書を使う Windows Hello for Business ハイブリッド証明書信頼**、または**スマート カード ユーザー**のシナリオはサポートされません
- **オンプレミスの Multi-Factor Authentication Server を使っている、スマート カードで認証している、現在のサーバーがフェデレーション固有の機能を提供している、サード パーティのフェデレーション ソリューションからマネージド サービスへ移行する** —— これらに当てはまる場合は影響を検討してから始めます

有効にできる組み合わせ

組み合わせ	可否
Password hash sync + Seamless SSO	可
Pass-through authentication + Seamless SSO	可
Password hash sync + Pass-through authentication + Seamless SSO	**不可**
Certificate-based authentication 設定	可
Azure multifactor authentication	可

> **注意: seamless SSO が適用されるのは、ユーザーが seamless SSO のグループにも入っていて、かつ PTA または PHS のグループにも入っている場合だけ**です。

事前準備(prework)

PHS の事前準備

1. Microsoft Entra Connect の **Optional features** ページで password hash sync を有効にする
2. **完全な password hash sync サイクルが実行され、全ユーザーのパスワード ハッシュが Microsoft Entra ID に同期されたことを確認する**

PTA の事前準備

1. **pass-through authentication エージェントを動かすサーバーを特定する。Microsoft Entra Connect サーバーは選ばない。**ドメイン参加済みで、選択したユーザーを Active Directory で認証でき、送信ポートと URL で Microsoft Entra ID と通信できることを確認する
2. Microsoft Entra Connect authentication agent をダウンロードしてサーバーにインストールする
3. 高可用性のために、他のサーバーにも認証エージェントを追加インストールする
4. **smart lockout 設定を適切に構成する**(悪意ある第三者によるオンプレミス アカウントのロックアウトを防ぐため)

有効化の手順

1. **Hybrid Identity Administrator** として Microsoft Entra admin center にサインインする
2. **Entra ID > Entra Connect > Connect sync** に移動する
3. **Staged rollout of cloud authentication** の下で「Enable staged rollout for managed user sign-in」を選ぶ
4. 有効にするオプション(Password Hash Sync、Pass-through authentication、Seamless single sign-on、Certificate-based Authentication)のコントロールを On にする

5. 選んだ機能にグループを追加する。**タイムアウトを避けるため、セキュリティ グループのメンバーは初期状態で 200 人以下**にする

> **反映のタイミング**: **グループのメンバーは自動的に staged rollout で有効になります**。新しいグループを追加すると、**グループ内のユーザー(新しいグループでは最大200人)は直ちにマネージド認証に更新されます**。一方、**グループを編集(ユーザーの追加・削除)した場合、変更が反映されるまで最大24時間かかることがあります**。

移行の前後で起きる追加サインイン

staged rollout の出入りで、必ず1回の追加サインインが発生することが問われます。

場面	挙動
staged rollout にユーザーを追加した	認証体験は即座にフェデレーションからマネージドへ切り替わらない。**既存のフェデレーション認証方法で対話型サインインを1回完了する必要がある**。その後、以降のサインインでマネージド認証が適用される
staged rollout からユーザーを削除した	ユーザーはマネージド認証を使い続ける。**Microsoft Entra 経由で対話型サインインを1回完了する必要がある**。その後、フェデレーション認証に戻る
Microsoft Entra ID Protection の修復イベント	SSPR、リスクの修復、リスクの却下などが staged rollout の状態をリセットすることがあり、次回サインインでフェデレーション IdP にリダイレクトされる。**フェデレーション認証で対話型サインインを1回完了すると、マネージド認証が再確立される**

追加のフェデレーション サインインを避ける回避策が推奨されています。**Microsoft Entra は Temporary Access Pass (TAP) をフェデレーション IdP へのリダイレクトより先に評価する**ため、次の順序で進めます。

1. ユーザーを staged rollout グループに追加する
2. **そのユーザーに Temporary Access Pass (TAP) を発行する**
3. ユーザーが TAP で Microsoft Entra にサインインする
4. サインインが成功すると、そのユーザーは staged rollout の一員として認識され、**Microsoft Authenticator やパスキーなど追加の認証方法を登録**できる

監査・検証・監視

監査イベントは次の場面で記録されます。

- password hash sync、pass-through authentication、seamless SSO の staged rollout を有効にしたとき
- それぞれの機能にグループを追加したとき
- グループに追加されたユーザーが staged rollout で有効になったとき

検証の方法は次のとおりです。

テスト対象	手順	期待される挙動
PHS / PTA(ユーザー名とパスワード)	**エクストラネット**からプライベート ブラウザー セッションで `https://myapps.microsoft.com` を開き、対象ユーザーの UPN を入力する	**フェデレーション ログイン ページにリダイレクトされず、Microsoft Entra のテナント ブランド付きサインイン ページで入力を求められる**

テスト対象	手順	期待される挙動
seamless SSO	**イントラネット**からブラウザー セッションで `https://myapps.microsoft.com` を開き、対象ユーザーの UPN を入力する	**「Trying to sign you in ...」のメッセージが表示された後、サイレントにサインインされる**

いずれの場合も、**サインイン アクティビティ レポート**を UserPrincipalName で絞り込んで成功を確認します。まだ AD FS で発生しているサインインを追跡するには、AD FS のイベントとログを確認します。

監視は、Microsoft Entra admin center の **Hybrid Auth ブック**で行います。staged rollout に追加・削除されたユーザーとグループ、staged rollout 中のユーザーのサインインを監視できます。

PHS の staged rollout 中は、パスワード変更が反映されるまで同期時間により最大2分かかります。パスワード変更後のヘルプデスクへの問い合わせを避けるため、ユーザーに事前に伝えておきます。

ユーザーの削除と機能の無効化

グループからユーザーを削除すると、そのユーザーの staged rollout が無効になります。staged rollout 機能自体を無効にするには、コントロールを Off に戻します。

> **証明書ベースの認証での注意: 証明書で Windows デバイスにサインインしているユーザーを、証明書ベースの認証の staged rollout グループから削除する場合、そのユーザーを Microsoft Entra ID で証明書ベースの認証方法に対して有効なままにしておくことが推奨されます。**ユーザーが Windows にサインインし、フェデレーション ID プロバイダーを使っ

> て primary refresh token を更新できるだけの期間、有効なままにしておく必要があります。

フェデレーション認証を選ぶべき場面(移行しない判断)

移行の設問は「移行できるか」だけでなく「移行すべきでないか」も問われます。**フェデレーションが必要になるのは、Microsoft Entra ID がネイティブにサポートしない認証要件がある場合**です。

- **フェデレーション ID プロバイダーを必要とするサード パーティの MFA プロバイダー**
- **サード パーティの認証ソリューションによる認証**
- **UPN(`user@domain.com`)ではなく sAMAccountName(`DOMAIN\username`)でのサインインが必要**
- **マルチサイトの低遅延認証システム、AD FS エクストラネット ロックアウト、サード パーティ ID システムとの統合**

フェデレーションのインフラ要件も比較で問われます。

項目	PHS	PTA	フェデレーション (AD FS)
Microsoft Entra Connect 以外のオンプレミス サーバー要件	**なし**	認証エージェントごとに1台	**AD FS サーバー2台以上 + 境界/DMZ ネットワークに WAP サーバー2台以上**

項目	PHS	PTA	フェデレーション (AD FS)
ネットワーク要件	なし	認証エージェントを動かすサーバーからの**送信インターネット アクセス**	**境界の WAP サーバーへの受信インターネット アクセス**、WAP から AD FS サーバーへの受信ネットワーク アクセス、**ネットワーク負荷分散**
TLS/SSL 証明書	不要	不要	**必要**
正常性監視	不要	Microsoft Entra admin center のエージェント状態	**Microsoft Entra Connect Health**
MFA の選択肢	Microsoft Entra MFA、Conditional Access のカスタム制御	同左	同左 + **サード パーティ MFA**
Windows Hello for Business	Key trust、Hybrid Cloud Trust	Key trust、Hybrid Cloud Trust	Key trust、Hybrid Cloud Trust、**Certificate trust model**
サインイン ページのブランド変更	**P1 または P2 が必要**	**P1 または P2 が必要**	可能
Conditional Access の選択肢	Microsoft Entra Conditional Access(P1 / P2)	同左	同左 + **AD FS アクセス制御ポリシー**
レガシ プロトコルのブロック	可	可	可

ルーティング不可能なドメイン(Microsoft Entra ID で検証できないドメイン)を使う場合は、**Alternate login ID のサポート**という追加構成が必要です。また、**フェデレーションでサード パーティの MFA プロバイダーを使う場合、デバイスを Microsoft Entra ID に参加させるには、そのプロバイダーが WS-Trust をサポートしている必要があります。**

Microsoft Entra Connect を展開する際は、サポートされているトポロジのいずれかを実装する必要があります。

1-4-8 Microsoft Entra Connect Health の実装と管理 [1.4]

Microsoft Entra Connect Health は、**オンプレミスの ID インフラを堅牢に監視**し、Microsoft 365 および Microsoft Online Services への信頼性の高い接続を維持するための機能です。**主要な ID コンポーネントを監視し、それらに関する重要なデータ ポイントに容易にアクセスできるようにする**ことで実現されます。

ライセンス要件は Microsoft Entra ID P1 です。**Microsoft Entra Connect 自体は無料**ですが、**Connect Health には P1 が必要**という差が問われます。

情報は Microsoft Entra Connect Health ポータル(Microsoft Entra admin center) に表示され、**アラート、パフォーマンス監視、使用状況分析**などを一元的に確認できます。導入は、**オンプレミスの各 ID サーバーにエージェントをインストールするだけ**です。

監視対象は次の3つです。

監視対象	内容
AD FS	フェデレーション サーバーと、エクストラネット アクセス向けの認証をサポートする **Web アプリケーション プロキシ サーバー**の監視
Microsoft Entra Connect Sync	同期サービスの監視、同期エラーの把握
Active Directory Domain Services	ドメイン コントローラーの監視

AD FS 向けの Connect Health がサポートする OS は、**Windows Server 2012 R2**、**Windows Server 2016**、**Windows Server 2019**、**Windows Server 2022**、**Windows Server 2025** です。

AD FS 向けの主な機能を、利点とベスト プラクティスの対応で押さえます。

利点	具体的な内容
セキュリティの強化	**エクストラネット ロックアウトの傾向**、**失敗したサインインのレポート**、プライバシーへの準拠
すべての重大な AD FS システムの問題に対するアラート	サーバーの構成と可用性、パフォーマンスと接続性、定期的な保守
展開と管理の容易さ	エージェントの迅速なインストール、**エージェントの最新版への自動アップグレード**、数分でポータルにデータが表示される
豊富な使用状況メトリック	**上位のアプリケーションの使用状況**、ネットワークの場所と TCP 接続、サーバーごとのトークン要求数
優れたユーザー エクスペリエンス	Microsoft Entra admin center のダッシュボード形式、**メールによるアラート**

Connect Health の前提として、**Microsoft Entra Connect Health for Sync には Microsoft Entra Connect Sync V2 が必要**です。**Azure AD Connect V1 を使っている場合は最新版へアップグレードする必要があり、V1 との組み合わせでは Connect Health for Sync が動作しません。**

> **PTA との切り分け**: **AD FS の正常性監視ソリューションは Microsoft Entra Connect Health です。**一方、**PTA のエージェント状態は Microsoft Entra admin center で提供され、Connect Health は必須ではありません。PHS には正常性監視ソリューションが不要**です。この3者の対応関係は対応付け問題の定番です。

1-4-9 到達目標 1.4 の分かれ目の早見表 [1.4]

要件	正解	なぜ他は違うか
最小限の労力でオンプレミス ユーザーにクラウド認証をさせたい	**password hash synchronization**	PTA はエージェント、フェデレーションは AD FS + WAP が要る
オンプレミスのアカウント ロックアウト・サインイン時間を即座に適用したい	**pass-through authentication**	PHS は無効化アカウントのみ(最大30分の遅れ)で、ロックアウト・有効期限・サインイン時間には対応しない
漏洩した資格情報のレポートを使いたい	**password hash synchronization を有効にする**(+ ID Protection は P2)	認証方法が PTA でもフェデレーションでも、PHS の有効化が別途必要
Microsoft Entra Domain Services を使いたい	**password hash synchronization**	どのサインイン方法を選んでも PHS が必要

要件	正解	なぜ他は違うか
サード パーティ MFA(フェデレーション依存)を使いたい	**フェデレーション(AD FS)**	PHS と PTA では Microsoft Entra MFA か Conditional Access のカスタム制御しか使えない
`DOMAIN\username` 形式でサインインさせたい	**フェデレーション(AD FS)**	PHS と PTA は UPN + パスワードのみ
オンプレミス障害時にもクラウド アプリを使い続けたい	**PHS を併用しておく**(切り替えは Microsoft Entra Connect で手動)	PTA とフェデレーションはオンプレミスに依存し、フェールオーバーは自動ではない
切断された複数フォレストを1つのテナントに同期したい	**Microsoft Entra Cloud Sync**	Connect Sync では複雑な構成が必要
同期サーバーの単一障害点をなくしたい	**Cloud Sync の複数アクティブ エージェント**	Connect Sync のステージング モードは手動での切り替えを伴うスタンバイ
Windows 7 のドメイン参加 PC でパスワード入力をなくしたい	**seamless SSO**	Windows 10 以降は PRT による SSO が推奨
Microsoft Entra 参加の Windows 11 で SSO を効かせたい	**primary refresh token (PRT)**	seamless SSO は Microsoft Entra 参加/ハイブリッド参加デバイスでは使われない
AD FS を使いながらクラウド認証をテストしたい	**staged rollout**	直接カットオーバーすると全ユーザーが影響を受ける

要件	正解	なぜ他は違うか
staged rollout の後の最終移行	**Microsoft Entra Connect または PowerShell でドメインをフェデレーションからマネージドへ変換**	staged rollout はドメインを切り替えない
staged rollout で追加のフェデレーション サインインを避けたい	**Temporary Access Pass (TAP) を発行して初回サインインさせる**	何もしないと1回の対話型フェデレーション サインインが必要
AD FS サーバーとエクストラネット ロックアウトの傾向を監視したい	**Microsoft Entra Connect Health**(P1)	PTA のエージェント状態は admin center で見られるが、AD FS の詳細監視は Connect Health
PHS の正常性を監視する仕組みを追加したい	**不要**(PHS は正常性監視ソリューション不要)	Connect Health は AD FS・Connect Sync・AD DS の監視が主眼

1-5 第1章の総まとめ —— 4つの到達目標をつなぐ線 [1.1/1.2/1.3/1.4]

1-5-1 「範囲を絞る」道具の使い分け [1.1/1.2/1.3]

この章には「範囲を絞る」道具が何度も出てきます。似ているようで目的が違うので、1枚にまとめておきます。

道具	絞る対象	目的	ライセンス
administrative unit	管理者のアクセス許可	組織の一部分だけを管理させる	管理者に P1

道具	絞る対象	目的	ライセンス
restricted management administrative unit	オブジェクトへの変更操作	**指定した管理者以外の全員から守る** (Global Administrator も含む)	管理者に P1
カスタムロール + リソース スコープ	管理者のアクセス許可	単一のアプリの登録・グループなどに限定する	割り当てを受けるユーザーに P1
PIM	権限を持つ時間	常時保持をやめ、必要時だけ昇格させる	P2
Guest user access restrictions	ゲストの閲覧範囲	ディレクトリの可視性を制限する	Free
Cross-tenant access settings	外部組織との受信・送信	相手が Microsoft Entra 組織の場合の連携を制御する	trust settings や個別指定に P1
Tenant restrictions	管理下デバイスで使える外部アカウント	未承認テナントのアカウント利用を止める	—

1-5-2 ライセンスの境目(Free / P1 / P2 / Governance) [1.1/1.2/1.3/1.4]

「追加のライセンスを購入せずに」という評価軸の設問で、この表がそのまま答えになります。

ライセンス	この章で該当する機能
Free	組み込みロールの使用、AU の**作成**、Microsoft Entra Connect と Cloud Sync、**seamless SSO**、PHS / PTA、custom security attributes、bulk operations、Assigned メンバーシップのグループ
P1	**カスタムロール、role-assignable group、AU 管理者、restricted management AU 管理者、動的メンバーシップ グループ、Company branding**(または Microsoft 365 Business Standard / SharePoint Plan 1)、**Conditional Access、cross-tenant access settings の trust settings と個別指定、cross-tenant synchronization(ユーザー・ソース側)、Microsoft Entra Connect Health、MDM 自動登録**
P2	**PIM、Microsoft Entra ID Protection**(漏洩資格情報レポート含む)
Microsoft Entra ID Governance / Microsoft Entra Suite	**cross-tenant synchronization のグループ同期、cross-cloud synchronization**、access reviews、entitlement management(一部機能は P2 でも動作)

1-5-3 手順の順序(並べ替え問題の骨格)[1.1/1.2/1.3/1.4]

作業	順序
AU による委任	AU を作成 → メンバーを追加 → AU スコープでロールを割り当て → 管理者の P1 を確認

作業	順序
カスタム ドメイン	ドメインを追加 → TXT/MX レコードを DNS に登録 → 検証 → 必要ならプライマリに変更
custom security attributes	ロールを確認 → attribute set を追加 → attribute set の委任を設定 → 属性を定義 → 属性を割り当て → フィルターや ABAC で使う
ライセンス付きグループの移動	移動先に追加 → ライセンス適用を確認 → 元から削除
cross-tenant synchronization	トポロジを決める → **ターゲット**で同期と自動引き換えを有効化 → **ソース**で自動引き換えを有効化し同期ジョブを構成 → 少数でテスト → 展開
SAML/WS-Fed フェデレーション	DNS の TXT が必要か判定 → パートナーの IdP を構成 → Microsoft Entra 側でフェデレーションを構成 → 引き換え順序を構成
seamless SSO	Connect サーバーでモジュールをインポート → 認証コンテキストを作成 → 状態を確認 → ドメイン管理者の資格情報を取得 → `Enable-AzureADSSOForest` を実行 → グループ ポリシーで URL をイントラネット ゾーンへ配布
AD FS からの移行	移行先の認証方法を決める → 事前準備 (PHS の完全サイクル、PTA のエージェント展開)→ staged rollout を有効化しグループを追加 → 検証と監視 → **ドメインをマネージドへカットオーバー**

1-5-4 誤答肢の作られ方(この章の頻出パターン)[1.1/1.2/1.3/1.4]

1. **ライセンスの取り違え**:「カスタムロールで実現する」と書きつつ P1 がない前提、「PIM で just-in-time にする」と書きつつ P2 がない前提。
2. **スコープの取り違え**: AU にグループを入れてメンバーのパスワードをリセットしようとする、`/administrativeUnits/<ID>` と `/<ID>` の混同。
3. **設定面の取り違え**: 外部の Microsoft Entra 組織の話なのに external collaboration settings を出す、逆にソーシャル ID の話なのに cross-tenant access settings を出す。
4. **同期と認証の混同**:「Cloud Sync に変えたから PTA が使えなくなる」型。**同期テクノロジは認証動作を決めません**。
5. **一時的な仕組みを恒久解として使う**: staged rollout をゴールとして提示する。
6. **セキュリティ対策ではない設定をセキュリティ対策として提示する**:「Restrict access to Microsoft Entra administration portal」で管理ポータルへのアクセスを防げる、とする。
7. **自動と手動の取り違え**: PTA から PHS へのフェールオーバーが自動で起きる、とする。実際は Microsoft Entra Connect で手動切り替えです。
8. **一括操作の取り違え**: 外部ゲストを招待メール付きで招待したいのに Bulk create を選ぶ。
9. **片側だけの設定**: automatic redemption を片方のテナントだけで有効にして同意プロンプトが消えると考える。
10. **既定値の取り違え**: B2B direct connect が既定で有効だと考える(実際は**既定でブロック**)、B2B collaboration が既定で無効だと考える(実際は**既定で有効**)。

この章で作った土台 —— テナント設定、委任の範囲、ユーザーとグループ、外部ユーザー、ハイブリッド ID —— の上に、第2章の認証と Conditional Access、第3章のワークロード ID、第4章の ID ガバナンスが載ります。とくに**administrative unit のスコープ**、**role-assignable group**、**動的メンバーシップ グループ**、**UserType**、**PHS の必須性**は、後の章で繰り返し前提として使われます。

サンプルはここまでです

続き(第2章〜巻末)は、SC-300 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。

SC-300 学習用テキスト(無料サンプル)

版

2026年7月版(SC-300 出題範囲(Study guide・Skills measured as of 2026-04-27)準拠)

発行

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

お問い合わせ

info@shikaku-doujou.com