

Microsoft 365 Copilot およびエージェント 管理の基礎(AB-900) 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)

AB-900 出題範囲(Skills measured as of October 14, 2026)準拠
2026年10月版

ご利用にあたって

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

SAMPLE

目次

この試験の範囲 [overview]

第1章 Identify the core features and objects of Microsoft 365 services

[1.1.1/1.1.2/1.1.3/1.1.4/1.1.5/1.1.6/1.2.1/1.2.2/1.2.3/1.2.4/1.2.5/1.3.1/1.3.2/1.3.3/1.3.4/1.3.5/1.3.6/1.3.7/1.3.8/1.3.9]

ライセンスの種類と割り当てが機能のアクセスを決める [1.1.1]

Microsoft 365 管理センターで見る組織の構成 [1.1.2]

Exchange 管理センターで構成するオブジェクト [1.1.3]

SharePoint 管理センターで構成するオブジェクト [1.1.4]

SharePoint のサイトの役割と権限 [1.1.5]

Teams 管理センターで構成するチーム・チャネル・ポリシー [1.1.6]

ゼロトラストの基本原則 [1.2.1]

認可とロール [1.2.2]

認証方法 [1.2.3]

脅威の保護とインテリジェンス [1.2.4]

Microsoft Defender XDR の機能 [1.2.5]

Microsoft Entra ID の機能 [1.3.1]

条件付きアクセスのポリシー [1.3.2]

SSO の目的と利点 [1.3.3]

ユーザーとグループのセキュリティ オブジェクト [1.3.4]

サインインの問題のトラブルシューティング [1.3.5]

ID セキュリティスコアの解釈 [1.3.6]

監査ログの確認 [1.3.7]

Privileged Identity Management (PIM) の役割 [1.3.8]

アプリの登録とエンタープライズ アプリケーション [1.3.9]

サンプルはここまでです

3冊の使い方は、ダウンロード欄の案内を参照してください。

SAMPLE

この試験の範囲 [overview]

AB-900(Microsoft 365 Certified: Copilot and Agent Administration Fundamentals)は、Microsoft 365 の基本的なサービスと、データの保護と管理、Copilot とエージェントの管理の基礎を問う入門の試験です。レベルは Fundamentals(Beginner)。試験時間は 45 分で、合格には 1000 点満点の 700 点以上が要ります。

出題範囲は 3 つの分野に分かれます。この教材も、同じ順に章を立てます(下の表)。配点は、学習ガイドの「Skills at a glance」にある割合です。

分野	配点	内容
1 Identify the core features and objects of Microsoft 365 services	30～35%	ユーザー、グループ、Exchange・SharePoint・Teams の基本、ID とセキュリティの基本
2 Understand data protection and governance tasks for Microsoft 365 and Copilot	35～40%	Purview の機能、Copilot とデータの保護、リスクの発見、SharePoint の過剰共有の対処
3 Perform basic administrative tasks for Copilot and agents	25～30%	Copilot の機能とライセンス、Copilot の管理、エージェントの管理

学習ガイドの細目は 53 個。節の見出しの後ろにある [1.1.1] のような印が、その細目の番号です。2026 年 10 月 14 日の改訂で変わったのは、細目 1.3.9 の語が Enterprise apps から Enterprise applications になった 1 語だけ。本文は新しい語で書き、古い語も併記します。

第1章 Identify the core features and objects of Microsoft 365 services

[1.1.1/1.1.2/1.1.3/1.1.4/1.1.5/1.1.6/1.2.1/1.2.2/1.2.3/1.2.4/1.2.5/1.3.1/1.3.2/1.3.3/1.3.4/1.3.5/1.3.6/1.3.7/1.3.8/1.3.9/1.3.10/1.3.11/1.3.12/1.3.13/1.3.14/1.3.15/1.3.16/1.3.17/1.3.18/1.3.19/1.3.20/1.3.21/1.3.22/1.3.23/1.3.24/1.3.25/1.3.26/1.3.27/1.3.28/1.3.29/1.3.30/1.3.31/1.3.32/1.3.33/1.3.34/1.3.35/1.3.36/1.3.37/1.3.38/1.3.39/1.3.40/1.3.41/1.3.42/1.3.43/1.3.44/1.3.45/1.3.46/1.3.47/1.3.48/1.3.49/1.3.50/1.3.51/1.3.52/1.3.53/1.3.54/1.3.55/1.3.56/1.3.57/1.3.58/1.3.59/1.3.60/1.3.61/1.3.62/1.3.63/1.3.64/1.3.65/1.3.66/1.3.67/1.3.68/1.3.69/1.3.70/1.3.71/1.3.72/1.3.73/1.3.74/1.3.75/1.3.76/1.3.77/1.3.78/1.3.79/1.3.80/1.3.81/1.3.82/1.3.83/1.3.84/1.3.85/1.3.86/1.3.87/1.3.88/1.3.89/1.3.90/1.3.91/1.3.92/1.3.93/1.3.94/1.3.95/1.3.96/1.3.97/1.3.98/1.3.99/1.3.100]

ライセンスの種類と割り当てが機能のアクセスを決める [1.1.1]

Microsoft 365 のサービスは、ユーザーにライセンスを割り当てて初めて使えます。管理者が持っている権限とは別の話です。ライセンスは「どのサービスを使えるか」を決め、ルールは「どの管理操作ができるか」を決めます。この2つを取り違えると、設定の問題と権限の問題を見分けられません。

ライセンスの種類は大きく4つあります。

種類	中身の見方
Microsoft 365 Business 系	中小企業向け。Business Premium は Entra ID P1 などのセキュリティ機能を含む
Microsoft 365 E3・E5	大企業向けの上位プラン。E5 は Entra ID P2 や Defender 系を含む
Microsoft 365 F1・F3	現場の従業員向け。機能は絞られ、Entra ID P1 を含む
アドオン	既存のプランに足す。Copilot のライセンスもこの形で足す

ライセンスには複数のサービスが入っています。既定ではサービスが全部ユーザーに割り当てられます。不要なサービスはチェックを外して止められます。ライセンスは同じ製品名でも複数のサブスクリプションが重なることがあり、ライセンスのページでは合計で出ます (5本と8本なら13本)。「自分の製品」のページはサブスクリプションごとの行です。ユーザーが自分で買ったセルフサービス購入のサブスクリプションは、管理者がライセンスを割り当てたり外したりできません。管理者が引き継げば管理できます。

割り当ての2つの方法。ユーザーに直接割り当てる方法と、グループに割り当てる方法があります。

単位	割り当てる場所
ユーザー単位	「ユーザー > アクティブなユーザー」で対象を選ぶ
製品単位・グループ単位	「課金情報 > ライセンス」のページ

割り当て画面では、ユーザーやグループを一度に最大20まで追加できます。ユーザーの追加の時にライセンスを選べ、必要なアプリだけに絞れます。追加にはライセンス管理者かユーザー管理者が必要です。複数ユーザーの一括追加は CSV を使い、列見出しも列の順番も変えられません。新しいユーザーのパスワードは、既定で自動作成され、初回サインインで変更を求められます。

ライセンスを割り当てる前に、「使用場所 (Usage location)」を指定します (サービスが国によって使えないことがあるため)。グループベースで場所のないユーザーは、テナントの場所を引き継ぎます。

アクティブなユーザーの標準フィルターは次の9つです。

- 課金管理者
- グローバル管理者

- ゲスト
- ヘルプデスク管理者
- ライセンスあり
- サービス サポート管理者
- ライセンスなし
- ユーザー管理者
- エラーのあるユーザー

カスタムのユーザー ビューは最大50まで作れ、作ると全管理者に見えます。標準ビューは編集も削除もできません。
[^c1-1]

グループ ベースのライセンス

グループにライセンスを割り当てると、メンバー全員にライセンスが付きます。対象はセキュリティ グループ、メール有効グループ、Microsoft 365 グループです。割り当てられるロールは、グループ管理者、ライセンス管理者、ユーザー管理者のどれかです。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割り当てても、ライセンスが付くのは1段目のメンバーだけです。管理センターでは一度に最大20グループまで割り当てられ、エラーの再処理も一度に最大20ユーザーです。成功した人と失敗した人の一覧は999人ずつのページ表示です(下までスクロールすると次が読み込まれます)。

エラーは「課金情報 > ライセンス」で製品を開き、「エラーと問題」タブで確認します。「再処理」で再試行できます。代表的な原因は3つです(ライセンスの不足、サービス プランの競合、使用場所が無効)。

ユーザーをグループAからグループBへ移す時は、順序を守ります。

1. 先に移動先のグループへ追加する
2. 新しいライセンスの適用を確認する
3. 元のグループから外す

先に外すと、処理が終わるまで一時的にライセンスなしになります。[^c1-2]

ライセンスを外した時と無い時

状況	起きること
ライセンスを外した直後の Exchange Online のデータ	30日間は保持される。30日を過ぎると削除されて戻せない。保持ラベルや保持ポリシーに合う内容は、検出のために残る
OneDrive のファイル	ライセンスを外しても消えない。ユーザー自体を削除するか、Active Directory 同期で外れた時に対象になる
Microsoft 365 アプリが入ったままの端末	「ライセンスのない製品」のメッセージとライセンス認証エラーが出る
ユーザーを削除した時	そのライセンスはすぐ他の人に割り当てられる状態に戻る
移行でメールボックスだけ追加し、ライセンスを割り当てない	猶予30日の後にメールボックスが無効になる

間違えやすいのは、「ライセンスを外すとデータがすぐ消える」という思い込みです。メールは30日の猶予があり、OneDrive は消えません。逆に、猶予があるからといってライセンスなしで使い続けられるわけではありません。サービスそのものは使えなくなります。[^c1-3]

Microsoft 365 管理センターで見る組織の構成 [1.1.2]

Microsoft 365 管理センターは、ライセンス、ユーザー、ドメイン、組織の設定を扱う入口です。ここでは「設定 > ドメイン」と「設定 > 組織設定」の2つを覚えます。

ドメインの追加。ドメインとは、メール アドレスの @ の後ろや Web アドレスの www の後ろの名前です (contoso.com など)。カスタムドメインはブランドとメールの評判に効きます。「設定 > ドメイン」で「ドメインの追加」を選びます。初回は「セットアップ」の「カスタムドメインを設定する」から始めます。ドメインを追加、変更、削除できるのはドメイン名管理者です。テナント全体に効くため、一般のユーザーやカスタムの管理者は使えません。

所有確認はレジストラーの DNS で行います。方法は3通りあります。

- 1. TXT レコードを足す
- 2. TXT が足せない時は MX レコードを足す
- 3. ドメインの Web サイトの最上位に確認用のテキストファイルを置く

確認は最大10分で終わります。レジストラーによっては最大48時間かかります。Domain Connect に対応するレジストラーなら、所有確認と必要な DNS レコードの追加を自動で行えます (推奨)。対応しなければ手で足します。必要なレコードの種類に対応しない DNS ホストでは一部の機能が動かないため、対応するレジストラーへの移管が勧められています (DNS レコードには A、CNAME、MX、TXT、SRV などの種類があり、TXT は所有確認と SPF、MX はメールの配送先に使います)。

メールは優先度の数字が小さい MX サーバーに届きます。メール用の MX は最小の数 (通常0) にして、所有確認用の MX より高い優先度 にします。SPF の TXT レコードは1つだけにし、既にあれば Microsoft 365 の値を足します。新しくは作りません。メール移行では、ドメインを追加した後、MX レコードを Microsoft 365 に向ける前に、ユーザーとメールボックスを作ります。メールを止めないためです。

既定のドメインと onmicrosoft.com。テナントを作ると onmicrosoft.com のドメインが付きます。新しいメールアドレスに使うドメインが「既定のドメイン」です。カスタムドメインを1つ以上足してから、「設定 > ドメイン」で対象を選び「既定に設定」にします。変えても既存のアカウントには効かず、新しいアカウントだけに効きます。

組織の設定。「設定 > 組織設定」には「サービス」「セキュリティとプライバシー」「組織のプロファイル」のタブがあります。リリースの設定は「組織のプロファイル」タブにあり、変更にはグローバル管理者が必要です。選択肢は3つです。

選択肢	内容
標準リリース	既定。全般提供と同時に届く
組織全体の対象指定リリース	全員が先行して受け取る
選択したユーザーだけの対象指定リリース	一部のユーザーだけ先行する

変更が効くまで最大24時間かかります。組織単位で配られる機能は、一部のユーザーだけを登録しても早く届きません。300人を超える組織では、組織全体を対象指定にせず、テスト用のテナントを使うよう勧められています。対象指

定リリースは2026年11月に新規の登録ができなくなり、2027年1月に終了します。未設定のままなら終了時に標準リリースになります。政府クラウド (GCC・GCC High・DoD) では標準リリースが対応するオプションで、延期リリースとFrontier は使えません。[^c1-4]

Exchange 管理センターで構成するオブジェクト [1.1.3]

Exchange 管理センター (EAC) は、メールボックスとグループを扱う管理センターです。受信者は次の種類に分かれます。

受信者の種類	意味
ユーザー メールボックス	1人が使う通常のメールボックス
共有メールボックス	複数人で使うメールボックス
会議室・備品	予約できるリソース
メール連絡先	社外のアドレス
メール ユーザー	社外のアドレスと組織のアカウントを持つ
グループ類	配布・メール有効セキュリティ・動的配布・Microsoft 365 グループ
メール有効パブリック フォルダー	共有のフォルダー

メールボックスの種類と使い分け

共有メールボックスは、複数のユーザーが同じ受信トレイと予定表を使う箱です。

項目	内容
容量	50 GB まではライセンス不要。上限は50 GB で、Exchange Online Plan 2 を割り当てると100 GB
訴訟ホールド	Plan 2、または Plan 1 と Exchange Online Archiving が必要
使うユーザー	自分のライセンス付きメールボックスが必要
利用者数	最大25人。多い時は Microsoft 365 グループを使う。組織の外の人は使えない

共有メールボックスのユーザー アカウントでは、直接サインインしません。サインインはブロックしたままにします。パスワードは誰も知らない自動生成です。共有メールボックス自体にユーザー名とパスワード (セキュリティ コンテキスト) がなく、暗号化キーを持てません。そこから送るメールは暗号化できません。容量がいっぱいになると、しばらくは受信できても送信ができなくなります。さらに経つと受信も止まり、送信者に配信不能通知が返ります。メッセージの削除は防げません。削除を制限したい時や社外の人も使いたい時は、Microsoft 365 グループを検討します。

リソース メールボックスは会議室と備品の2つで、会議の招待を自動で承諾または辞退できます。Exchange 管理センターの「受信者 > リソース」で追加します。リソースの設定にグループを指定する時、入れ子のグループは効きません。**会議室リスト**は、会議室メールボックスだけを入れた特別な配布グループです。作れるのは Exchange Online PowerShell だけで、管理センターからは作れません。

予約の設定	既定
予約できる期間	180日先まで
1回の最大の長さ	24時間
定期的な会議	許可
就業時間内のみ予約を許可	未選択(時間外も予約可)。就業時間の既定は月～金の8:00～17:00
予約の承認者(予約代理人)	既定は自動で承諾または辞退。代理人を指定すると、すべての依頼が代理人に回って手動で承認される

受信者のグループ

メール系のグループは4種類あります。

グループ	特徴
配布グループ(配布リスト)	メールの宛先になる。既定は組織内の人からのメッセージだけを許可し、外からのメールは拒否。所有者は最低1人
動的配布グループ	条件(受信者の種類、部署など)でメンバーが決まる
メール有効セキュリティグループ	宛先になり、セキュリティプリンシパルなのでアクセス許可も付けられる
Microsoft 365 グループ	メールと共有ワークスペースが付く。配布リストのメンバーにはできない

アクセス権を付けられるのはセキュリティグループです。配布グループに入れられないのは、Microsoft 365 グループとメール非有効の Entra ユーザーです(ユーザー、共有、会議室、備品の各メールボックス、メール ユーザー、連絡先は入れられます)。

動的配布グループの注意点。EAC で作れるのは既定のフィルター(簡易フィルター)だけです。使える属性は、都道府県・会社・部署・カスタム属性1～15で、複数ルールの結合は AND だけです。OR などが必要ならカスタム受信者フィルターを使い、これは PowerShell で作ります。メンバーの一覧は、作成時、ルール変更時、定期の更新で計算されます。定期の更新は少なくとも24時間に1回で、間は古いままです(部署を移った人にまだ届くことがあります)。2026年5月末からは、ルールに合うメンバーが5,000以下なら、作成やルール変更の直後に計算されてすぐ使えます。5,000を超えると背景処理で最大2時間かかります。Exchange Online の動的配布グループは Entra ID にも社内の AD にも同期されないで、条件付きアクセスの対象に使えません。

「グローバル アドレス一覧から非表示にする」を選んでも、アドレスを直接入力すれば送信はできます。[^c1-6]

メールボックスの権限

権限	できること	見え方
フル アクセス	メールボックスを開いて中身を読む。送信は含まない	既定で Autodiscover により相手の Outlook に自動で開く(メール有効セキュリティグループに付けた場合は自動では開かない)

権限	できること	見え方
送信者として送信 (Send As)	メールボックス (グループ) 本人として送る	本人から届いたように見え、代理を示す表示が出ない
代理人として送信 (Send on Behalf)	「〇〇の代理で」と送る	「代理人 on behalf of メールボックス」と表示され、返信は元のメールボックスに届く

読んで返信までさせたい場面では、フル アクセスと Send As の両方が要ります。フル アクセスだけでは送信できないからです。この3つは、アドレス一覧から非表示にしたメールボックスでは使えません。探索メールボックスは既定で非表示です。[^c1-7]

SharePoint 管理センターで構成するオブジェクト [1.1.4]

SharePoint の部品は3つに分けて覚えます。

部品	役割
チーム サイト	共同作業向け。メンバー全員が作り手。Microsoft 365 グループ接続が既定
コミュニケーション サイト	発信と閲覧向け。作り手は少なく、読み手が多い
ハブサイト	サイト群をつなぐ

ハブ サイト。関連するサイトをまとめ、ナビゲーションとテーマとニュースを共有します。提供するの、共有のナビゲーションとブランド、コンテンツと検索のロールアップ、ハブのホーム画面の3つです。関連付けても、各サイトの権限は変わりません。1つのサイトが関連付けられるハブは1つだけです。ハブのナビゲーションには自動では入りません (ハブの所有者が決めます)。ニュースは関連付けたサイトからハブへ上がるだけで、ハブから下には流れません。広く届けたい時は、ハブに投稿します。関連付けを許可するサイト所有者は、SharePoint 管理者が絞れます。組織で作れるハブは最大2,000です。ハブのナビゲーションは、技術的な上限が500で、性能の面から100以内が勧められます (つまり実運用の目安は100)。

ドキュメント ライブラリ・リスト・フォルダー

ライブラリはファイルの置き場で、リストは表形式のデータの置き場です。フォルダーは、ライブラリの中の区切りにすぎません。ライブラリにはバージョン管理があり、編集のたびに版を残して前の版に戻せます。10万項目を超えるリスト、ライブラリ、フォルダーでは、そのもの自体のアクセス許可の継承を切れません (中の個々の項目、つまりフォルダーやファイルは、継承を切れませす)。

項目	上限
1ファイル	250 GB まで。リスト項目の添付は250 MB。複数ファイルの ZIP ダウンロードは20 GB
リスト	最大3,000万項目
ライブラリ	3,000万のファイルとフォルダー
パス全体	ファイル名を含むデコード後で400文字以内 (OneDrive・SharePoint)

項目	上限
1サイトのリストとライブラリ	合わせて2,000
組織全体のサイト数	200万サイト (サイト コレクション)
1サイトの容量	25 TB
組織のストレージ	1 TB に、購入したライセンス1つにつき10 GB を足す (プランによる)

SharePoint 管理センターで行う操作

「アクティブなサイト」で、サイトの作成、ストレージの上限、サイト管理者とメンバーの変更を行います。作成は「作成」を押し、チーム サイト、コミュニケーション サイト、その他のサイトから選びます。必要なのは SharePoint 管理者以上です。同じアドレスのサイトが既にあると、空いているアドレスに自動で変わります。サイト作成時に選ぶ言語は、後から変えられません。

クラシック サイトでは、テンプレートを選び、URL のパスは /sites/ か /teams/ を選びます。ストレージのクォータは MB で指定します。/personal/ (OneDrive) や /search、コンテンツ ハブなどの一部の URL とテンプレートのサイトは、アクティブなサイトの一覧に出ません。組織レベルの共有設定もこの管理センターで行います。[^c1-8]

SharePoint のサイトの役割と権限 [1.1.5]

既定のグループと権限レベル

サイトには既定で3つのグループがあります。

グループ	権限レベル
所有者	フル コントロール
メンバー	編集
閲覧者	閲覧 (読み取り)

既定の権限レベルには、フル コントロール、デザイン、編集、投稿、閲覧、制限付きアクセス (とその変形の Web のみの制限付きアクセス)、承認、階層の管理、制限付き閲覧、表示のみがあります。フル コントロールと制限付きアクセスだけは、カスタマイズも削除もできません。

投稿 (Contribute) は、項目とドキュメントの表示、追加、更新、削除ができます。編集 (Edit) は、それに加えてリストの追加、編集、削除もできます。メンバー グループの既定は編集です。「制限付きアクセス」は、特定の1項目だけを共有された人に、そこへたどり着くために SharePoint が自動で付けます。手動では割り当てられません。「表示のみ」は、ブラウザーで開けるファイルを見られても、ダウンロードはできません。動画や .png のようにブラウザーで開けない種類は、ダウンロードを防げません。

チーム サイトの権限は、関連付けた Microsoft 365 グループで管理すると簡単です。コミュニケーション サイトは、組み込みの SharePoint グループで管理します。公開 (Public) の設定で作ったモダンなチーム サイトでは、「Everyone except external users」が、メンバー グループに自動で入ります (プライベートのチーム サイトでは入りません) (外部ユーザーを除くディレクトリの全員を含むセキュリティグループです)。サイトの所有者とメンバーは、既定で新しいユーザーを追加できます。

継承と継承の中止

サイト コレクション管理者がルートのサイトで権限を設定すると、下位のサイト、リスト、ライブラリ、項目が継承します。継承を止めると、そこから先は独自の権限になります（アクセス権のない人にファイルを共有すると、そのファイルの権限の継承は自動で止まります）。フォルダーや項目へ個別に共有できる反面、独自の権限が増えるほど管理は複雑になるため、必要な所に絞ります。

共有リンクと外部共有のレベル

共有リンクは4種類です。

種類	対象
すべてのユーザー (Anyone)	リンクを知る人は誰でも
組織内のユーザー	組織のメンバー
既存のアクセス権を持つユーザー	すでに権限がある人
特定のユーザー	指定した人

外部共有のレベルは、すべてのユーザー、新規と既存のゲスト、既存のゲスト、組織内のユーザーのみ、の4段階です。サイトの設定は組織の設定より緩くできません。OneDrive の設定も、SharePoint より厳しくはできても緩くはできません。

サイトごとに既定のリンクの種類と権限を変えるには、SharePoint 管理センターの「アクティブなサイト」でサイトを選び、「共有」の「既定の共有リンクの種類」で「組織レベルの設定と同じ」を外します。Teams のプライベートチャネルと共有チャネルのサイトだけは、Set-SPOSite で設定します（管理センターでは変えられません）。

秘密度ラベルでも、サイトや個々のドキュメントの既定の共有リンクの種類と権限を決められます。組織の既定の共有リンクの種類が「すべてのユーザー」でも、サイトがサインインか確認コードのゲストとの共有だけを許す設定なら、既定のリンクは「組織内のユーザーのみ」になります（社外へは「特定のユーザー」に変えて共有します）。

既定では、ゲストが外部に共有するにはフル コントロールが必要です。ゲストのアクセスには期限を付けられます。「ゲストのアクセスは次の日数で自動的に期限切れ」に日数を設定します。確認コードで入る人に再認証を求める日数は、「確認コードを使うユーザーは次の日数後に再認証が必要」という別の項目で設定します。

Entra B2B 連携が無効だと、ファイルの共有ではゲスト アカウントが作られません。有効にすると、ファイルやフォルダーの共有でも必ずゲスト アカウントが作られ、Entra の設定が効きます。サイトの共有は常に B2B です。OneDrive の所有者に閲覧者の名前を見せる設定は、既定でオンです。SharePoint ではサイト側で所有者が有効にし、組織とサイトの両方がオンの時だけ表示されます。[^c1-9]

Teams 管理センターで構成するチーム・チャネル・ポリシー [1.1.6]

チームとチャネルの種類

チームを作ると、裏に Microsoft 365 グループが作られ、SharePoint のチーム サイトも自動で作られます。チャネルの「ファイル」タブのファイルは、SharePoint に保存されます。プライベートと共有のチャネルにも、それぞれサイトが作られます。チームのロールは、所有者とメンバーの2つです（所有者は共同所有者を作れます）。モデレーションを使えば、チャネル単位でモデレーターも置けます。

既定では、すべてのユーザーがチームを作れます。制限するには、Teams のロールとアクセス許可の割り当てで変えます。公開のチームは、組織の誰でも参加でき、最大10,000人です。組織全体のチームは、ユーザーが10,000人を超える組織では作れません。

チャンネル	参加者	作れる人と制約
標準	チームの全員	
プライベート	チームのメンバーから選んだ人	既定でチーム所有者とメンバーが作れる（ゲストは作れない）。作った人が所有者で、直接メンバーを追加、削除できるのは所有者だけ。ゲストをメンバーにできる
共有	チームの内外の選んだ人。チームの外や組織の外の人を入れる	作れるのはチーム所有者だけ（メンバーは不可）。Entra のゲストはメンバーにできない

プライベートと共有のチャンネルは、作った後で別のチームへ移せず、標準チャンネルとの相互の変換もできません。プライベート チャンネルは、以前の1チーム30個の制限がなくなり、チーム全体の上限（最大1,000チャンネル）に含まれます。チーム メンバーが抜けると、全プライベート チャンネルからも外れます。プライベート チャンネルの所有者が組織を離れるなどでいなくなると、そのチャンネルのメンバーの1人が自動でチャンネルの所有者に昇格します（最後の所有者はクライアントから外せません）。

共有チャンネルに組織外の人を入れるには、Entra のクロステナント アクセス設定が双方の組織に必要です。削除した共有チャンネルは30日以内なら復元でき、以前のメンバーも戻ります。チームの削除と復元も30日で、共有チャンネルごと戻ります。チームを複製しても共有チャンネルは複製されません。チームをアーカイブすると、親チーム以外へのチーム共有は外れ、個人の共有だけが残ります。[^c1-10]

Teams のポリシーと割り当て

ポリシーは、会議、メッセージ、アプリなどの機能ごとに、できることを決めます。割り当ての優先順位は次のとおりです。

- 1. ユーザーに直接割り当てたポリシー
- 2. グループに割り当てたポリシー
- 3. 組織全体の既定 (Global)

ユーザーへの割り当ては、Teams 管理センターの「ユーザー > ユーザーの管理」でユーザーを選び、「設定の編集」で行います。各ポリシーのページの「ユーザーの割り当て」からも行え、PowerShell では Grant- で始まるコマンドを使います。

グループへの割り当ては、セキュリティ グループ、Microsoft 365 グループ、配布リストに行えます。5万ユーザー以下のグループが推奨で、届くのは直接のメンバーだけです。入れ子のグループには届きません。グループ メンバーシップを非表示にしたグループ（クラス チームの既定）には使えません。ポリシーを外すには、各ポリシーを Global に戻します（一括で外す機能もあります）。2025年5月5日から Skype コンシューマーとの相互運用は終了し、関連ポリシーも廃止されました。[^c1-11]

外部アクセスとゲスト アクセスの違い

項目	外部アクセス	ゲスト アクセス
できること	Microsoft ID を持つ他組織の人を探し、チャット、通話、会議をする	チームに招待して、チャネルやファイルで共同作業をさせる
既定	有効（組織の設定もユーザーのポリシーも既定でオン）	Teams 管理センターの「ゲスト アクセス」でオンとオフを切り替える
相手の扱い	相手は自分の組織のアカウントのまま	Entra B2B のゲストとして自分のディレクトリに追加される

外部アクセスは既定で有効で、すべての外部ドメインとのやり取りが許されています。場面で判断するなら、「会議と連絡だけで済む相手」は外部アクセス、「チームのファイルや会話に入れたい相手」はゲスト アクセスです。共有チャネルは、ゲストを作らずに他組織の人に入れられる点が両者の中間にあたります。[^c1-12]

ゼロトラストの基本原則 [1.2.1]

ゼロトラストは、「決して信頼せず、常に検証する (never trust, always verify)」という考え方です。ネットワークの内側ほど安全だと考える従来の境界型は、ID の侵害、フィッシング、セッションハイジャックのような、場所に依存しない攻撃に対応できません。信頼のモデルは「既定で信頼する (trust-by-default)」から「例外として信頼する (trust-by-exception)」に変わります。

原則は3つです。

原則	意味	実装のしかた
明示的に検証する (Verify explicitly)	利用できる信号をすべて使って、アクセスのたびに認証と認可を判断する	誰が要求しているか、どのデバイスか、場所と振る舞い、リスクの水準の4つを確かめる
最小特権のアクセス (Use least privilege access)	必要なアクセスだけを与える	ユーザーとワークロードに、必要な最短の期間だけ与える
侵害を想定する (Assume breach)	攻撃者がすでに内部にいる前提で設計する	被害を限定し、素早い検知と対応を重視する

「継続的な検証」は、一度の認証で信頼し続けません。アクセスのたびに、ユーザー、場所、デバイス、リスクの信号で判断します。

ゼロトラストが守る対象は、ID、エンドポイント（デバイス）、アプリ、データ、インフラ、ネットワークです（それぞれに実装の手引きがあります）。成果は次のように表れます。アクセスが明示的に許可されて継続評価され、条件付きで一時的になり、権限が狭い範囲に限られます。オンプレミス、クラウド、SaaS、AI のワークロードに同じ制御が効きます（検知と対応も組み込まれます）。

セキュリティは技術だけの話ではありません。資格情報の共有や未承認のデータ利用のような人とプロセスもリスクになります。継続的な検証と最小特権は、人的要因の影響を減らします。

導入は段階的に進め、要素は次の3つです。

- ビジネス シナリオ (守りたい成果の優先順位)
- セキュリティの領域 (戦略、設計、プロセス、制御)

- テクノロジの柱 (ID、データ、デバイスなど)

入口はゼロトラストの導入パス (adoption path) です。現状の評価は Zero Trust assessment、実装は技術的ソリューションの手引きを使います。

「侵害を想定する」は、侵害を許す意味ではありません。起きた時の被害を小さくする設計のことです。「最小特権」は、権限の量だけでなく期間も絞ります。[^c1-13]

認可とロール [1.2.2]

認証は「誰か」を確かめ、認可は「何をしてよいか」を決めます。サインインでパスワードや MFA を使う段階が認証で、その後にロールやアクセス許可でできる操作が決まる段階が認可です。

Microsoft 365 の管理者ロールは、ロールベースのアクセス制御 (RBAC) で権限を分けます。守る原則は3つです。

1. グローバル管理者を最小限にする
2. 最小権限のロールを割り当てる
3. 管理者全員に MFA を必須にする

管理センターの「ユーザー > アクティブなユーザー」で対象ユーザーを選び、ロールを割り当てます。「ロールの割り当て」ページでは、ロールごとの権限と、割り当て済みの管理者を見られます。設定や画面で権限がないと表示されるのは、そのロールに権限がないためです (別の管理者に正しいロールを頼みます)。

ロール	できること
グローバル管理者	ほぼ無制限。サブスクリプションを購入してサインアップした人が自動でなる。全ユーザーと他の管理者のパスワードをリセットできる
グローバル閲覧者	グローバル管理者が見られる管理者機能と設定を見られる。編集はできない
課金管理者	購入、サブスクリプション、サービス要求、サービス正常性
ヘルプデスク管理者	パスワードのリセット、ユーザーの強制サインアウト、サービス要求の管理
パスワード管理者	ユーザーのパスワードのリセット (限られた範囲)
ライセンス管理者	ライセンスの割り当てと削除、使用場所の編集、グループ ベースのライセンスの再処理
ユーザー管理者	ユーザーとライセンスの管理
グループ管理者	グループの作成、編集、削除、復元。グループの作成、有効期限、名前付けのポリシー
Exchange 管理者	Exchange Online (Send As などの委任も)
SharePoint 管理者	SharePoint 管理センター (サイトの作成と削除)
Teams 管理者	Teams 管理センター (会議、組織全体の設定)
セキュリティ管理者	Microsoft 365 のセキュリティ制御と監視
セキュリティ閲覧者	セキュリティの読み取りのみ

ロール	できること
レポート閲覧者	管理センターの使用状況とアクティビティのレポート、Power BI の導入/パック。エージェントの概要とレジストリも閲覧
メッセージ センター閲覧者	メッセージ センターの通知を監視し、週次のメール ダイジェストを受け取る。データ プライバシーのメッセージはグローバル管理者とプライバシー閲覧者だけ
AI 管理者	Microsoft Copilot のあらゆる面と、統合アプリ ページの AI 関連サービス、拡張機能、Copilot エージェントを管理する

グローバル管理者はほぼ全権を持つので、日常の作業は小さいロールで足ります。たとえば「パスワードを忘れた人の対応だけをさせたい」ならヘルプデスク管理者、「ライセンスの付け外しだけ」ならライセンス管理者です。AI 管理者は、ユーザーのライセンスやサインインを扱いません。テナント全体の Microsoft 365 ワークロード管理までは与えられません。セキュリティ管理者とセキュリティ閲覧者は、管理センターでエージェントを見られても、公開やライフサイクル管理はできません。

アクセス許可の種類。アプリのアクセス許可は2種類に分かれます。

種類	動き方	同意
委任されたアクセス許可 (スコープ)	サインインしたユーザーに代わって動く。そのユーザーが見られない物には触れない	ユーザーが自分のデータに同意できる。管理者は全ユーザー分を同意できる
アプリケーションのアクセス許可 (アプリ ロール)	ユーザーなしでアプリ自身が動く	管理者だけ

同意 (consent) は、ユーザーまたは管理者がアプリにリソースへのアクセスを承認することです。管理者の同意が求められるのは、高い特権のアクセス許可が要求され、まだ同意がない時です。独自のアプリ スコープだけの要求は高特権とみなされず、管理者の同意は要りません。同意の結果として、委任は OAuth2PermissionGrant、アプリケーションは appRoleAssignment が作られます。[^c1-14]

認証方法 [1.2.3]

認証方法は、使える場面が方法ごとに決まっています。場面は3つの区分で見ます(主な認証の第1要素、多要素認証 (MFA) の第2要素、セルフサービス パスワード リセット (SSPR) とアカウント回復)。

方法	内容と注意
パスワード	従来の第1要素
Microsoft Authenticator	プッシュ通知とパスワードレス。セキュリティの既定値群では番号の入力を求める (MFA 疲労攻撃の対策)
パスキー (FIDO2)	FIDO 標準で、オリジンに結び付く公開鍵暗号。秘密鍵はデバイス、公開鍵はサービス側。生体認証か PIN と組むと MFA になる
Windows Hello for Business	端末に結び付いたパスワードレス認証
証明書ベース認証 (CBA)	証明書で認証する
一時アクセス パス (TAP)	期限付きのコード。パスワードレスの方法の登録などに使う

方法	内容と注意
SMS・音声通話	電話で受け取る。フィッシングには弱い
ソフトウェア OATH トークン、ハードウェア OATH トークン(プレビュー)	ワンタイム コードを作るトークン
メール ワンタイム パスコード	テナントのメンバーは SSPR で使える。サインインに使えるのはゲストだけ(構成した場合)。MFA の第2要素には使えない

パスワードレスとフィッシングに強い MFA

推奨されるフィッシングに強い方法は、Windows Hello for Business、パスキー (FIDO2) と FIDO2 セキュリティ キー、証明書ベース認証 (CBA) の3系統です。

パスキー	内容
デバイス固定	Microsoft Authenticator と FIDO2 セキュリティ キー。秘密鍵がデバイスから出ない
同期型	iCloud キーチェーンや Google パスワード マネージャーなど。クラウド経由で複数の端末に同期される

登録時に提供元の真正性を FIDO Metadata Service で確かめる仕組みを、構成証明 (attestation) と呼びます。Entra のパスキー プロファイルで有効にすると、デバイス固定のみが許可され、同期型は除外されます。規制の厳しい業種や特権ユーザーには、FIDO2 セキュリティ キーが勧められます(機器、教育、ヘルプデスクの費用は増えます)。一般には、同期型が低コストの代替です。

認証強度 (Authentication strength)。条件付きアクセスの制御の1つで、リソースに使える認証方法の組み合わせを指定します。条件付きアクセスには Entra ID P1 が必要です。組み込みは3つです。

組み込みの強度	中身の例
多要素認証 (MFA) 強度	複数の要素を求める
パスワードレス MFA 強度	パスワードを使わない方法
フィッシング耐性のある MFA 強度	FIDO2 セキュリティ キー、Windows Hello for Business (またはプラットフォーム資格情報)、証明書ベース認証 (多要素)

組み込みの強度は変更できません。新しい方法が出た時は Microsoft が更新します。使うには、条件付きアクセス ポリシーの許可の制御で「認証強度を要求する」を選び、組み込みがカスタムの強度を指定します。使いどころは、機密リソース、アプリ内の機密操作 (認証コンテキスト)、社外ネットワークから機密アプリへの接続、高リスクのユーザー、ゲスト (クロステナント設定) です。

たとえば「管理者のサインインをフィッシングから守りたい」なら、認証強度でフィッシング耐性のある MFA を要求します。SMS や音声通話は、この強度を満たしません。

セルフサービス パスワード リセット (SSPR)

SSPR は、ユーザーが自分でパスワードをリセットする機能です。一般ユーザーには既定では有効になっていません (管理者 ロールを持つアカウントは既定で有効です)。ユーザーが先に認証方法を登録し、登録は

<https://aka.ms/ssprsetup>で行います。登録を必須にすると、サインイン時に未登録の人へ促します(閉じても毎回出ます)。管理者のポリシーで、リセットに必要な方法を1つか2つに決めます。Entra の管理者ロールを持つユーザーには、強い2つのゲートのポリシーがかかり、一般ユーザーの設定とは違います(試用の最初の30日などは1つのゲート)。登録情報の再確認は0〜730日で設定でき、0は再確認を求めません。オンプレミスで管理するパスワードは、書き戻しを入れないと SSPR で変えられません。

SSPR が動かない時の確認順は決まっています。

- 1. SSPR を有効にしているか
- 2. ポリシーに合う認証方法が登録されているか (1つ必要か、2つ必要か)
- 3. パスワードがオンプレミスの管理なら、書き戻しがあるか

この順に確かめます。[^c1-15]

脅威の保護とインテリジェンス [1.2.4]

代表的な脅威を4つ挙げます。

脅威	内容
フィッシング	偽のメールやサイトで資格情報を盗む
マルウェア	悪意あるソフトウェア
ランサムウェア	データを暗号化して身代金を要求する
パスワードスプレー	多数のアカウントに少数の共通パスワードを試す

BEC (ビジネスメール詐欺) は、メールで人をだます攻撃です。

脅威分析 (Threat analytics)

脅威分析は、Microsoft のセキュリティ研究者による製品内の脅威インテリジェンスで、攻撃を直接止める機能ではありません。新しい脅威の報告、組織への影響と露出、推奨の対策を見せ、Microsoft Defender ポータルから開きます。レポートは、追跡中の脅威の分析と防御の手引きに、自組織のデータ (脅威が活動中か、保護が入っているか) を重ねたものです。Microsoft の一次情報と OSINT (公開情報) の両方が元になっています (Microsoft だけの情報ではありません)。

ダッシュボードは、「最新の脅威」「影響が大きい脅威」「露出が最も高い脅威」の3区画に分かれ、露出は関連する脆弱性の深刻度と影響を受けるデバイス数で計算されます。

タグはランサムウェア、フィッシング、アクティビティグループ、脆弱性の4つで、分類 (Category) では Actor (攻撃者のプロフィール) や OSINT (公開情報の記事) で絞れます。使うには Microsoft Defender 製品のライセンスが1つ以上必要です。Defender for Endpoint P1 だけは例外で、アクセスは付きません。権限は「セキュリティデータの基本 (読み取り)」でレポートと関連インシデント、資産を見られます。露出データと推奨アクションには、脆弱性管理 (読み取り) と Exposure Management (読み取り) が要ります。

Defender for Office 365 の保護の段階

段階	守る内容	含まれるライセンス
組み込みの保護 (全クラウド メールボックス)	量が多い既知の攻撃を防ぐ	Exchange Online を持つ全員
Plan 1	ゼロデイマルウェア、フィッシング、BEC	Microsoft 365 E3/G3、Business Premium など
Plan 2	攻撃シミュレーション、侵害後の調査、ハンティング、自動化	A5/E5/G5 など

組み込みの保護に含まれるのは、次の機能です。

- マルウェア対策
- スпам対策 (一括メール含む)
- フィッシング (なりすまし) 対策
- 送信スパム対策
- 接続フィルター
- 検疫と検疫ポリシー
- 管理者の報告
- テナントの許可/ブロック リスト

Plan 1 が足すのは、Safe Attachments (メール、および SharePoint、OneDrive、Teams のファイル)、Safe Links (メール、Office クライアント、Teams)、リアルタイム検出、ユーザー タグ (優先アカウント)、Teams の ZAP などです。

Plan 2 は、さらに次を足します。

- 攻撃シミュレーショントレーニング
- 優先アカウント保護
- Threat Explorer (Plan 1 のリアルタイム検出の代わり)
- キャンペーン
- Teams メッセージの高度な追跡 (ハンティング)
- 自動調査と対応 (AIR)

Plan 1 と Plan 2 は、多くのサブスクリプションへのアドオンも可能です (Plan 2 は Defender ポータルで90日の無料試用ができます)。

安全なリンクは、クリック時に URL を確かめます。安全な添付ファイルは、添付を隔離した環境で開いて確かめます。ZAP (ゼロアワー自動消去) は、配信後にマルウェアやフィッシングと判明したメッセージを自動で取り除く機能で、メールと Teams メッセージで使えます。Safe Documents は、Microsoft 365 A5 か Microsoft Defender スイートのライセンスのユーザーが使えます。Defender for Office 365 の Plan には含まれません。

メール認証は、onmicrosoft.com だけの場合もカスタム ドメインの場合も、使用中と未使用のドメインに SPF、DKIM、DMARC を設定します。[^c1-16]

Microsoft Defender XDR の機能 [1.2.5]

Defender XDR は、エンドポイント、ID、メール、アプリにまたがり、攻撃の前も後も、検出、防止、調査、対応を統合して調整する防御スイートで、ライセンスのある製品の信号を相関させます。

Defender XDR の構成

製品	守る対象
Defender for Endpoint	エンドポイント (デバイス)
Defender Vulnerability Management	資産の脆弱性
Defender for Office 365	メールと共同作業
Defender for Identity と Entra ID Protection	ID。Defender for Identity はオンプレミス AD の信号
Defender for Cloud Apps	SaaS アプリ

信号の元には、これらに加えて次があります (Defender for Cloud、Microsoft Purview の DLP、アプリ ガバナンス、Insider Risk Management、Exposure Management)。

製品をまたぐ層は、信号の共有と自動アクションで連携します。アラートとイベントと資産を結び付けて、攻撃の全体像 (インシデント) にします。自動修復 (自己修復) も行い、エンドポイント、ID、メール、クラウド アプリを横断した脅威ハンティングもできます。自動攻撃の中断は、複数のワークロードの高い確信度の信号を相関させ、進行中の攻撃に封じ込めを自動で適用して、横移動を食い止める機能です (英語名は Automatic attack disruption)。

インシデントとアラート・自動調査と対応

アラートは脅威の検出の信号で、インシデントは関連するアラートをまとめ、攻撃の全体を示す入れ物です。アラートの出どころは、Defender の各サービス、統合した他のサービス、Microsoft Sentinel、Defender XDR 自身の相関による検出です (Sentinel は接続すると生データも相関に使われます)。

インシデントには、次が含まれます。

- アラートとイベントのタイムライン
- 使われた戦術
- 関係するユーザーとデバイス
- 攻撃の相互関係の図
- 自動調査と対応のログ
- 証拠
- 攻撃ストーリーのテキスト要約

影響範囲、影響を受けた資産、自動修復のアクションは、1つのインシデントにまとめて統合インシデント キューで見られ、単一の画面は Defender ポータル (security.microsoft.com) です。「インシデント ケース」は推奨の管理体験 (プレビュー) で、従来のインシデント体験と併存します (タスクを使って、運用チームで調査を進められます)。

自動調査と対応 (AIR) は、アラートからインシデントができると、証拠ごとに判定を付けます。判定は3つです。

- 悪意あり (Malicious)

- 疑わしい(Suspicious)
- 脅威なし(No threats found)

修復アクション（ファイルの隔離、プロセスの停止、デバイスの隔離、URL のブロックなど）は、構成により自動で実行されるか、承認が必要です。すべてアクション センターに並びます。調査中に出た関連アラートは調査に追加され、影響を受けた資産が他で見つかれば、調査の範囲が広がります。AIR は「仮想のアナリスト」として Tier 1/2 の運用チームを助け、24時間365日の調査と修復の手間を減らします（対象は、デバイス、メールとコンテンツ、ID にまがります）。

Defender XDR は、個別の製品の「置き換え」ではありません。それらを束ねる層で、守る対象は個別の Defender 製品が受け持ちます。[^\c1-17]

Microsoft Entra ID の機能 [1.3.1]

Microsoft Entra ID は、クラウドの ID とアクセスを管理するサービスです。Microsoft 365 や Azure を契約すると、テナントが自動で Entra のテナントになります。テナントは組織専用のディレクトリで、Entra ID は ID プロバイダーとして、サインインの認証を引き受けます。Entra 製品ファミリーは、ゼロトラストの実装のための ID とネットワークアクセスの製品群です（下の表）。

製品	役割
Entra ID	中核の ID とアクセスの管理
Entra Domain Services	グループポリシー、LDAP、Kerberos/NTLM 認証を提供するマネージドドメイン。現代の認証を使えない従来型アプリ向け
Entra Private Access	VPN なしで社内アプリやリソースに安全に接続する
Entra Internet Access	SaaS や Microsoft 365 を含むインターネットのアクセスを守る（Web コンテンツ フィルターなど）
Entra ID Governance	アクセス要求、割り当て、レビューを自動化し、ID のライフサイクルを管理する。入社でユーザー、グループ、ライセンスを自動割り当てし、退職で解除する
Entra ID Protection	ID に基づくリスクを検出、報告し、リスクベースの条件付きアクセスで自動修復する
Entra Verified ID	分散 ID (DID) の標準に基づく資格情報の検証サービス。デジタル卒業証書のような検証可能な資格情報を発行、提示できる
Entra External ID	パートナー、ゲスト、顧客などの外部の ID が安全にアクセスするための製品

エディション (Free・P1・P2)

エディション	主な機能	含まれる製品
Free	基本的な ID 管理	Microsoft 365 などに含まれる
P1	条件付きアクセス、動的グループなど	Microsoft 365 E3・E5・E7、F1・F3、Enterprise Mobility + Security E3、Business Premium。単体でも購入できる

エディション	主な機能	含まれる製品
P2	ID 保護、PIM など	Microsoft 365 E5・E7、Microsoft Defender スイート、EMS E5。Business Premium でも Defender スイートの追加で含まれる

Entra スイートは、Private Access、Internet Access、ID Governance、ID Protection、Verified ID (プレミアム機能) を組み合わせたスイートです。Entra アプリケーション プロキシには、P1 または P2 が必要です。

ハイブリッド ID

オンプレミスの Active Directory とクラウドをつなぐ方式は、認証をどこで処理するかで分かります (同期のツールは Entra Connect と Cloud Sync)。

方式	認証の場所	特徴
パスワード ハッシュ同期	クラウド (Entra ID)	最も簡単。オンプレミスと同じユーザー名とパスワードを使える。パスワードは平文でも元に戻せる暗号でも Entra ID に保存されない
パススルー認証	オンプレミスの AD で確かめる	サーバーのソフトウェア エージェントが検証する。アカウントの状態、パスワード ポリシー、サインイン時間をすぐに強制したい要件に向く
フェデレーション	AD FS などの信頼する別システム	認証を渡す

パスワード ハッシュ同期とパススルー認証が「クラウド認証」、フェデレーションが「フェデレーション認証」です。漏えいした資格情報の検出には、どの方式でもパスワード ハッシュ同期が必要です。認証方式は ID のコントロール プレーンの基礎で、クラウドのすべてのデータへのアクセスを左右します。変更には計画、テスト、停止時間が要る場合があり、段階的ロールアウトで切り替えを試せます (一度に全員を切り替える必要はありません)。

外部 ID (B2B)

B2B コラボレーションでは、外部の人は自分の会社や個人の ID でサインインし、ゲストとして自社のアプリを使います。パートナーは Entra アカウントの有無を問わず入れて、外部アカウントのパスワード管理、同期、ライフサイクル管理が要りません。B2B は既定で有効で、メールのワンタイム パスコードも既定で有効です (無効にしていない限り、すぐ使えます)。

成立には、2つの設定の両方での許可が必要です。

設定	決めること
クロステナント アクセス設定	他の Entra 組織と、どのユーザーが認証できるか (受信と送信)
外部コラボレーション設定	誰がゲストを招待できるか

ゲストの追加は、Entra 管理センターで新しいゲスト ユーザーを作成します (ユーザーの追加と似た手順で、アプリやグループに割り当てます)。Azure グローバルと、Azure Government や 21Vianet のような別の国別クラウドの間で

は、両方のテナントが Microsoft クラウド設定で相手を許可します。そのうえでクロステナント アクセスを構成します。
[^c1-18]

条件付きアクセスのポリシー [1.3.2]

条件付きアクセスは、「もし(割り当て) なら、こうする(アクセス制御)」という if-then のポリシーです。一次認証(第1要素)の後に評価されます。DoS 攻撃などの最前線の防御を目的としたものではありません。

構成要素

要素	内容
割り当て: ユーザーとグループ	全員、グループ、ディレクトリ ロール、外部ゲスト、エージェント
割り当て: 対象リソース	クラウド アプリ、ユーザー アクション、認証コンテキスト
割り当て: ネットワーク	IP の場所(国と地域を含む)
条件(シグナル)	デバイス(プラットフォーム、状態、フィルター)、アプリケーション、リアルタイムと計算されたリスク(ID 保護)、Defender for Cloud Apps
許可の制御	多要素認証を要求、認証強度を要求、準拠済みデバイス、ハイブリッド参加のデバイス、承認済みクライアント アプリ、アプリ保護ポリシー、パスワードの変更、利用規約。最も厳しい決定は「アクセスのブロック」
セッションの制御	アプリの適用制限、Defender for Cloud Apps、トークンの有効期間

許可の制御は、「選んだ制御をすべて要求」と「いずれか1つを要求」から選べます。1人に複数のポリシーが当たる時は、すべてを満たす必要があります。許可の制御を満たした後に、セッションの制御がかかります(満たすまで、セッションの制御には進みません)。求める順番は、多要素認証、準拠デバイス、Entra ハイブリッド参加デバイス、承認済みクライアント アプリ、アプリ保護ポリシー、パスワードの変更、利用規約、カスタム制御の順です(セッション制御は、すべて満たした後です)。

評価は2つのフェーズで進みます。フェーズ1では、ネットワークの場所やデバイス ID などのセッションの詳細を集めます(有効とレポート専用の両方)。フェーズ2で要件を適用します(有効なポリシーのみ)。ブロックがあればここで止まります。ロールやグループを対象にしたポリシーは、トークンの発行時にだけ評価されます。後から追加されたユーザーは、新しいトークンを取るまで対象になりません。PIM のロール有効化時に評価を起こすことが推奨されます。

よく使うポリシーとレポート専用モード

よく使うポリシー	設定の考え方
管理者に MFA を求める	ユーザーにディレクトリ ロールを選び、許可の制御で多要素認証を要求する
レガシー認証をブロックする	クライアント アプリの条件でレガシー クライアントを選び、アクセスのブロック
場所とデバイスで絞る	信頼する場所以外からは MFA、または準拠済みデバイスを要求

レポート専用モードは、ポリシーを評価しますが適用しません。本番に出す前の影響確認に使います。結果は、サインインログの「条件付きアクセス」「レポート専用」タブに出ます。Azure Monitor の条件付きアクセス インサイトのブック、ポリシーの影響（プレビュー）でも見られます。結果は4種類です。

結果	意味
Report-only: Success	条件を満たし、要件も満たした
Report-only: Failure	条件を満たしたが、要件を満たせなかった
Report-only: User action required	条件を満たし、ユーザーの操作があれば要件を満たせた
Report-only: Not applied	条件に合わなかった

「ユーザー アクション」のスキープの項目は評価できません。準拠デバイスを要求するポリシーは、強制しなくても macOS、iOS、Android でデバイス証明書の選択を求めるプロンプトが出ることがあります。

セキュリティの既定値群と条件付きアクセスの違い

セキュリティの既定値群 (security defaults) は、Entra が用意した一括の基本設定です。有効にすると、次の制御が入ります。

- 全ユーザーの MFA 登録
- 管理者への MFA
- 必要時の MFA
- レガシー認証のブロック
- デバイス コードフローのブロック
- Azure portal など特権操作の保護

2019年10月22日以降に作られたテナントでは、既定で有効場合があります。新しいテナントでは、作成後24時間の猶予の後に強制されます。切り替えは、Entra 管理センターの「Entra ID > 概要 > プロパティ」で「セキュリティの既定値群の管理」を開き、「有効」にして保存します。切り替えに必要なのは、少なくとも条件付きアクセス管理者のロールです（それ未満のロールでは変更できません）。

比べる点	セキュリティの既定値群	条件付きアクセス
設定の細かさ	一括。個別の調整はできない	割り当てと条件を自分で組む
向く組織	Entra ID の無料版を使う、どこから始めるか分からない組織	P1/P2 を持つ組織、複雑な要件のある組織
併用	条件付きアクセスと同時に使えない	使う時はセキュリティの既定値群を無効にする

「P1 を持たず、まず全員に MFA を入れたい」ならセキュリティの既定値群です。「営業部だけ、社外ネットワークからのみ MFA」なら条件付きアクセスです（セキュリティの既定値群では対象を絞れません）。[^c1-19]

SSO の目的と利点 [1.3.3]

SSO (シングル サインオン) は、1組の資格情報でサインインし、割り当てられたアプリを再サインインなしで開ける仕組みです。利用者側の利点は4つあります。

- 使い勝手が上がる
- 資格情報の露出が減り、一貫したポリシーを使える
- アクセス管理を ID プロバイダー1か所に集約できる
- パスワード リセットの問い合わせが減る

アプリ提供側 (ISV) にとっては、エンタープライズ対応、導入の迅速化、競争力、ユーザー管理の簡素化が利点です (顧客の ID システムに任せられます)。

流れは4段階です。

1. ユーザーがアプリを開く
2. アプリがユーザーを Entra ID ヘリダイレクトする
3. Entra ID が資格情報を確認する
4. Entra ID が ID を確認し、アプリがアクセスを許可する

アプリは資格情報を直接扱いません。

SSO の方式

方式	内容
SAML 2.0	成熟した XML ベース。従来の Web アプリや詳細な属性が要する場合
OpenID Connect (OIDC)	OAuth 2.0 の上の JSON トークン。現代の Web、モバイル、API、ISV には作りやすい
パスワード ベース	ユーザー名とパスワードでサインインするアプリ向け。Entra ID が資格情報を安全に保存してアプリに再生する。フェデレーション非対応のアプリ、特にアプリケーション プロキシ経由のオンプレミスアプリで使う
リンク	ユーザー ポータルにアプリのリンクを出すだけで、本当の SSO ではない (段階的な移行用)
無効	アプリごとに別々にサインインする (テスト用や統合サインインが不要のアプリ)

SAML と OIDC は、Entra ID が認証して標準プロトコルでアプリに ID 情報を渡す、フェデレーション ベースの SSO で、最も豊かな統合です。クラウド (SaaS) のアプリは通常 SAML か OIDC、オンプレミスはフェデレーションか、アプリケーション プロキシ経由のパスワード ベース、ハイブリッドは両方の組み合わせです。SSO 対応で割り当てられたアプリは、「マイ アプリ」ポータルで1か所から見つけて起動できます。管理側ではエンタープライズ アプリケーションの画面で SSO を構成します。[^c1-20]

ユーザーとグループのセキュリティ オブジェクト [1.3.4]

ユーザーの種類

ワークフォース テナントのユーザーは4種類で、認証のしかたと権限の組み合わせで決まります。

種類	内容
内部メンバー	正社員など
内部ゲスト	テナント内のアカウントでゲスト権限
外部メンバー	外部のアカウントで認証するが、メンバー権限。マルチテナント組織に多い
外部ゲスト	本当のゲスト (B2B で招待)

クラウドだけのユーザーと、オンプレミスから同期したユーザーという分け方もあります。オンプレミスから同期したグループは、オンプレミスでしか管理できません。

操作	必要なロール
ユーザーの作成	ユーザー管理者
外部ゲストの招待	ゲスト招待者 (Guest Inviter)
Entra のロールの割り当て	特権ロール管理者

ロールは常に最小特権のものを使います。ユーザーの作成時には、最大20のロールと最大20のグループを割り当てられます (それ以上は作成後に追加します)。

グループの種類と使い分け

種類	用途	メンバー
セキュリティグループ	リソースへのアクセス制御	ユーザー、デバイス、サービス プリンシパル
Microsoft 365 グループ	共同作業。共有メールボックスと予定表、SharePoint、Planner、Teams のメンバーシップが付く	ユーザーだけ
配布グループ	メールの配信	メール系

Microsoft 365 グループは、管理者が許可すれば社外の人でもメンバーにでき、外部送信者も許可できます。SharePoint の3グループ (所有者、メンバー、閲覧者) に追加すると、サイトの権限を与えられます。配布リストとメール有効セキュリティグループは、Exchange 管理センターか Microsoft 365 管理センターで管理します。

Microsoft 365 管理センターで扱うグループの種類は、次の6つです。

- Microsoft 365 グループ
- 配布グループ
- セキュリティグループ
- メール有効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

動的メンバーシップを使えるのは、Entra ID の Microsoft 365 グループとセキュリティグループだけです。配布グループや共有メールボックスでは使えません。セキュリティグループを別のセキュリティグループに入れる入れ子では、親グループのメンバーだけが共有リソースにアクセスできます。ロールをグループに割り当て、職務や部署でメンバーを入れる管理もできます。グループの有効期限ポリシーは、使われていない Microsoft 365 グループを指定の期間の後に自動で削除します。

場面ごとの基本は3通りです。

- ファイルへのアクセス権を付けたい: セキュリティグループ
- チャット、ファイル、予定表をまとめて持たせたい: Microsoft 365 グループ
- メールを一斉送信したい: 配布グループ

割り当てのメンバーシップと動的メンバーシップ

メンバーシップの種類は3つあります。

- 割り当て済み (Assigned)
- ユーザーの動的メンバーシップ
- デバイスの動的メンバーシップ

動的はユーザーかデバイスの一方だけで、混ぜたルールは書けません。動的グループは、属性のルールでユーザーかデバイスを自動で入れます。単一の式は「<プロパティ> <演算子> <値>」の書式です。ルールビルダーは最大5つの式までで、5つを超える式、直属の部下、-contains、演算子の優先順位、複雑な式はテキストボックスで書きます。ユーザーやデバイスの属性が変わると、ディレクトリ内のすべての動的グループのルールが評価されて、追加と削除が行われます。

動的グループのメンバーであるユーザー1人ごとに、Entra ID P1 (または Intune for Education) が必要です (ユニークなユーザーで数えます)。デバイスのメンバーにはライセンスが要りません。グループの安全性は、ルールで参照する属性を誰が書き換えられるか (オンプレミス AD の SELF 書き込みなど) で決まります。ロールを割り当てられるグループは動的にできず、割り当て済みだけです。[¹^c1-21]

サインインの問題のトラブルシューティング [1.3.5]

サインインの問題は、次の順に進めます。

- 「何が起きたか」をサインイン ログで見る
- 「なぜか」を What If で再現する
- 「リスクか」を ID 保護で確かめる

症状・疑い	使うツール
特定のユーザーが入れない原因を知りたい	サインイン ログ
条件付きアクセスのどのポリシーが当たるか知りたい	What If ツール

症状・疑い	使うツール
不審なサインインやアカウント侵害の疑い	ID 保護のリスクのあるサインイン、リスクのあるユーザー
MFA を完了できない	MFA の登録と再登録

サインイン ログ

サインイン ログは、Entra 管理センターの「Entra ID > 監視と正常性 > サインイン ログ」で開きます。見るには、少なくともレポート閲覧者が必要です。ログの種類は、対話型のユーザー、非対話型のユーザー、サービス プリンシパル、マネージド ID の4つです。読む観点は3つで、Who (サインインしたユーザー)、How (使ったクライアント アプリ)、What (アクセスしたリソース)に分かれます。項目はシステムが生成するので、変更も削除もできません。ログで答えられる質問は、今週あるアプリにサインインしたユーザー数、直近24時間の失敗数、ブラウザーや OS の傾向などです (マネージド ID とサービス プリンシパルが使った Azure リソースも分かります)。エラー コードと、条件付きアクセスの結果 (成功、失敗、適用なし) から原因を絞ります。

Entra のアクティビティログには、サインイン、監査 (変更の記録)、サインアップ (外部テナントのみ、プレビュー)、プロビジョニング (ServiceNow へのグループ作成など) の種類があります。

What If ツール

What If は、「Entra ID > 条件付きアクセス > ポリシー > What If」にあります。ユーザーとサインインの条件を入れて、どの条件付きアクセスのポリシーが当たるかを確かめます。評価するのは、有効なポリシーとレポート専用のポリシーだけで、無効のポリシーは含みません。必須の条件は4つあります。

- ID (ユーザー、エージェント ID、単一テナントのサービス プリンシパル)
- 対象リソース
- デバイス プラットフォーム
- クライアント アプリ

ほかの条件は、省略すると「なし」になります。結果は、適用されるポリシー (満たすべき許可とセッション制御付き) と、適用されないポリシー (最初に満たさなかった条件が理由) に分かれて出ます。条件付きアクセスのサービス依存関係はテストしません。たとえば Teams の評価に Exchange のポリシーは含まれません。

リスクのあるサインインとリスクのあるユーザー

ID 保護は Entra ID P2 (または Entra Suite) が必要です。検出はリアルタイムかオフラインで、匿名 IP アドレスからのアクティビティ (オフライン)、不審な MFA 承認 (リアルタイム)、漏えいした資格情報、特殊な移動などがあります。ほとんどの検出の詳細は P2 が要ります。P2 がないと、詳細のない「追加のリスクが検出されました (Additional risk detected)」だけが出ます。また、管理者が「ユーザーの侵害を確認」すると、非プレミアムの検出として記録されます (確認の操作は管理者が行います)。

レポート	内容
リスク検出	個々の検出
リスクのあるサインイン	1つ以上の検出があるサインイン
リスクのあるユーザー	リスクのあるサインインが検出があるユーザー

サインインのたびにリアルタイムの検出がすべて実行され、侵害の可能性を示すサインイン セッションのリスクレベルが出ます。ポリシーはこのレベルで動きます。修復は2通りです。自動修復は、リスクベースの条件付きアクセスで強力な認証、MFA、安全なパスワード変更を求め、済めばリスクは自動で修復されます。そうでなければ手動修復となり、管理者が確認して、却下、侵害の確認、パスワード リセットなどを行います(ここまでがID 保護の修復の流れ)。

MFA の登録と再登録

セキュリティの既定値群では、Authenticator の承認時に番号の入力を求められます。MFA の登録の14日の猶予は、2024年7月29日からなくなりました。MFA の登録が壊れたり端末を失ったりした場合は、管理者が認証方法を再登録させます。[^c1-22]

ID セキュリティ スコアの解釈 [1.3.6]

スコアの読み方

ID セキュリティ スコアは、Entra の推奨事項のうち ID のセキュリティの項目が、どれだけ実施済みかを割合で示す指標です。Microsoft の推奨との一致度で、無料と有料のどちらの顧客も使えます(一部の推奨は有料ライセンスが必要です)。24時間ごとにセキュリティ構成を推奨と比べて、新しいスコアを計算します。「Entra ID > Identity Secure Score」で見ます。

必要な権限	ロール
スコアを開いて見る手順	少なくともグローバル閲覧者でサインイン
改善アクションを見る(更新はしない)	少なくともサービス サポート管理者
改善アクションの状態を更新する	少なくとも SharePoint 管理者

改善の操作の状態は、対応予定 (To address)、計画済み (Planned)、リスクの受け入れ (Risk accepted)、サードパーティで解決 (Resolved through third party)、代替の軽減策で解決 (Resolved through alternate mitigation) です。推奨の例は次のとおりです。

- グローバル管理者を2人以上にする
- 信頼できないアプリへのユーザー同意を許さない
- パスワードを期限切れにしない
- レガシー認証をブロックするポリシーを入れる
- ハイブリッドならパスワード ハッシュ同期を使う
- SSPR を有効にする
- 全ユーザーが MFA を完了できるようにする

採点は二値(設定していれば100%)か、一部の達成で部分点です。「[Not Scored]」の操作は、実施できても点になりません。

ID セキュリティスコアと Microsoft セキュア スコアの違い

	ID セキュリティスコア	Microsoft セキュア スコア
範囲	ID に関する推奨	組織全体のセキュリティの状態 (ID はその一部)
場所	Entra 管理センター	Microsoft Defender ポータル
見方	推奨の達成の割合	点数。高いほど推奨を実施している

ID セキュリティスコアは、Microsoft セキュア スコアの ID の部分と同じものです。セキュア スコアの目的は、現状の報告、可視性とガイダンスによる改善、ベンチマークと KPI の設定の3つです (似た組織との比較もできます)。

1つの推奨アクションは10点以下で、多くは二値です。たとえば全100ユーザー中50人を MFA で守っていれば、10点中5点の部分点になります。画面のスコアはリアルタイムで更新され、達成点は毎日同期されます。Teams と Entra の推奨は、構成が変わると状態が更新され、加えて Teams は月に1回、Entra は週に1回更新されます (即時とは限りません)。

点が付く行動は、次の3つです。

- 推奨のセキュリティ機能を構成する
- セキュリティ関連のタスクを行う
- Microsoft 以外のアプリや代替の軽減策で対処する (「サードパーティで解決」など)

ライセンスのある製品の推奨が表示され、製品ごとにエディションに関係なく、考えられる推奨の全体が見えます。Defender XDR ポータルの履歴タブで、変化の理由を確認できます。[^c1-23]

監査ログの確認 [1.3.7]

監査ログは2系統あります。**Entra の監査ログとサインイン ログ**と、**Microsoft Purview 監査 (統合監査ログ)**です。この2つは別物で、保持期間も見場所も違います。

	Entra の監査ログとサインイン ログ	Microsoft 365 統合監査ログ (UAL)
記録	監査＝テナントへの変更 (ユーザー、グループ、アプリ、ライセンスなど)。サインイン＝誰がどのリソースにどう入ったか	Microsoft 365 全体のユーザーと管理者のアクティビティ
保持	Free は7日。P1・P2 は30日	Purview 監査が決める。Entra のライセンス変更の影響を受けない
見る場所	Entra 管理センター	Microsoft Purview ポータルの監査検索

Entra の監査ログで答えられる質問は、次の3系統です。

- ユーザー (変更の種類と数、パスワード変更)
- グループ (追加、所有者の変更、ライセンス)
- アプリ (更新、削除、サービス プリンシパルの変更、作成者と理由、名前の変更)

MFA 使用状況レポートの保持は、Free・P1・P2のどれでも30日です。リスクのあるユーザーのレポートは期限なしで、収集は ID 保護センターを使い始めた時に始まります。ログの収集開始は、P1/P2/Workload ID Premium ではサブスクリプション開始時、Free では Entra ID を最初に開いた時かレポート API を最初に使った時です。アップグレード後にデータがなければ、表示まで最大3日かかります。Graph アクティビティ ログは P1/P2 のみで、転送しないと保持されません。保持を伸ばすには、Entra の監査とサインインのデータを Azure のストレージ アカウントや分析ツールに転送します。

Purview 監査。

	Audit (Standard)	Audit (Premium)
有効化	既定で有効	追加ライセンスが必要
保持	180日	1年まで(保持ポリシーで設定)。10年はアドオン
機能	検索ツール、Search-UnifiedAuditLog、CSV エクスポート、Office 365 管理アクティビティ API	Standard の機能に加え、監査ログ保持ポリシー、インテリジェントな洞察、高帯域の API

Standard の保持は以前は90日でした。2023年10月17日より前に生成されたログは90日、それ以降は180日です。10年の保持には、Audit (Premium) のライセンスに加えて、ユーザーごとに「10年の監査ログ保持」のアドオンライセンスが必要です。[^c1-24]

Privileged Identity Management (PIM) の役割 [1.3.8]

PIM は、Microsoft Entra ID、Azure、Microsoft 365、SaaS アプリの重要なリソースへの特権アクセスを、管理、制御、監視する機能です。ジャストインタイム(必要な時だけ)の特権アクセスを与えます。常に管理者権限を持たせておくと、アカウントが盗まれた時の被害が大きくなります。そのため、必要な時だけ権限を有効にさせます(権限は期限が来ると外れます)。

PIM の機能	内容
期間指定	開始と終了の日付を決める
承認	有効化に承認を要求する
MFA	有効化に MFA を強制する
正当な理由	有効化の時に理由を入力させる
通知	有効化を通知する
アクセス レビュー	割り当てを定期的に見直す
監査履歴	ダウンロードできる
保護	最後のアクティブなグローバル管理者と特権ロール管理者の割り当ては外せない

対象の割り当てとアクティブな割り当て

用語	意味
対象 (eligible)	使う時に有効化 (activate) の操作が必要。MFA、理由、承認などを求められる
アクティブ (active)	操作なしで権限が使える
有効化 (activate)	対象の人がロールを使うための操作

eligible でも active でも、得られるアクセスは同じです。違うのは、使う前に操作が要るかかどうかだけで、権限の中身は変わりません。「普段は権限を持たせず、障害対応の時だけグローバル管理者にしたい」なら eligible の割り当てにします。PIM で他の管理者の割り当てを管理できるのは、Entra ロールでは特権ロール管理者かグローバル管理者だけで、一般のユーザー管理者は管理できません。Azure リソースのロールは、サブスクリプション管理者、リソースの所有者、ユーザー アクセス管理者が管理します。

PIM には Microsoft Entra ID P2 か Microsoft Entra ID Governance のライセンスが必要です。セットアップ後、左のメニューに「タスク」「管理」「アクティビティ」が出て、Entra ロール、Azure リソースのロール、グループを管理できます (画面の構成)。条件付きアクセスと組み合わせる場合、ロールやグループを対象にしたポリシーは新しいトークンの発行時にしか評価されません。そのため、PIM の有効化時に評価を起こすことが推奨されます。[^c1-25]

アプリの登録とエンタープライズ アプリケーション [1.3.9]

アプリが Entra ID でサインインやリソース アクセスを使うには、アプリをテナントに登録します (App registration)。登録するとアプリケーション オブジェクトと、アプリ (クライアント) ID ができます。試験範囲の項目名は「Understand App registrations and Enterprise applications」です。2026年10月14日の改訂で、「Enterprise apps」から「Enterprise applications」に変わりました。管理画面の名前は「エンタープライズ アプリケーション」です。

用語	中身	管理画面
アプリケーション オブジェクト	アプリの「設計図」。全テナントで使うグローバルな表現で、ホーム テナントにだけある	アプリの登録
サービス プリンシパル	アプリがテナントのリソースを使うための、テナントごとの実体。登録が同意の時に作られる	エンタープライズ アプリケーション

アプリケーション オブジェクトが示すのは3つです。サービスがアクセス用のトークンを発行する方法、アプリが必要とするかもしれないリソース、アプリができる操作です。1つのアプリケーション オブジェクトに複数のサービス プリンシパルが結び付きます (1対多)。アプリを使うテナントごとに必要です。単一テナントのアプリはサービス プリンシパルが1つ (ホーム テナント)、マルチテナントのアプリは使うテナントごとに作られます。アプリを登録すると、ホーム テナントにアプリケーション オブジェクトとサービス プリンシパル オブジェクトが自動で作られます (Microsoft Graph API で登録した場合は手動で作ります)。

サービス プリンシパルは3種類です。

- アプリケーション (グローバルなアプリケーション オブジェクトのテナント内の実体)
- マネージド ID (資格情報の管理が要らない)

- レガシー (アプリの登録の導入前に作られたアプリ)

サービス プリンシパルを探すには、アプリの登録の概要で「ローカル ディレクトリ のマネージド アプリケーション」を選びます。PowerShell なら Get-MgServicePrincipal、Azure CLI なら az ad sp list を使います (画面を使わない方法)。エンタープライズ アプリケーションの画面では、テナント内のサービス プリンシパルを一覧と管理でき、権限、ユーザーが同意した許可、同意したユーザーなどを確認できます。

アクセス許可と同意

許可	動き方	同意できる人
委任された許可	サインインしたユーザーに代わって動き、そのユーザーが見られる範囲だけ	ユーザー自身。管理者は全ユーザー分を同意できる
アプリケーションの許可 (アプリ ロール)	ユーザーなしでアプリ自身として動き、許可に結び付くデータ全部に届く	原則として管理者だけ

同意の種類は、静的 (登録で構成) と動的 (サインイン時に要求) があります。「バックグラウンドで全員のメールを処理するアプリ」はアプリケーションの許可で、管理者の同意が要ります。「サインインした本人の予定表を読むアプリ」は委任された許可で、本人が同意できます。[^c1-26]

サンプルはここまでです

続き(第2章～巻末)は、AB-900 問題集のご購入で、頻出度別ノート・暗記用ノートと合わせて3点すべてダウンロードできます。

SAMPLE

Microsoft 365 Copilot およびエージェント管理の基礎(AB-900) 学習用テキスト(無料サンプル)

版

2026年10月版(AB-900 出題範囲(Skills measured as of October 14, 2026)準拠)

発行

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

お問い合わせ

info@shikaku-doujou.com

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

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

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