

MD-102 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)

MD-102 出題範囲(Skills measured)2026-10-27版 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]

- 準拠する版
- 試験の基本情報
- 5つの分野と配点

第1章 Prepare infrastructure for devices

[1.1.1/1.1.2/1.1.3/1.1.4/1.2.1/1.2.2/1.2.3/1.2.4/1.2.5/1.2.6/1.3.1/1.3.2/1.3.3/1.3.4/1.3.5/1.3.6/1.3.7/1.3.8]

- デバイス ID の3種と参加の種類の選び方 [1.1.1]
- Windows を Entra ID に参加させる方法と設定 [1.1.2]
- Entra ID への登録と、登録と参加の違い [1.1.3]
- デバイスのグループと動的メンバーシップルール [1.1.4]
- 登録の制限と Intune の登録の設定 [1.2.1]
- Windows の自動登録と共同管理、登録失敗の調べ方 [1.2.2]
- iOS/iPadOS・macOS の個人用登録と Apple MDM プッシュ証明書 [1.2.3]
- Android Enterprise の登録の種類と登録プロファイル [1.2.4]
- Apple Business Manager と連携した iOS/macOS の企業登録 (ADE) [1.2.5]
- Samsung Knox Mobile Enrollment と Google ゼロタッチ登録 [1.2.6]
- Intune と Windows 365 のロールの管理 [1.3.1]
- スコープ タグとスコープ付き管理 [1.3.2]
- 複数管理者の承認 (Multi Admin Approval) [1.3.3]
- コンプライアンス ポリシーと非準拠への対応 [1.3.4]
- 準拠済みデバイスを要求する条件付きアクセス [1.3.5]
- Intune による Windows Hello for Business の構成 [1.3.6]
- Windows LAPS の管理 [1.3.7]
- Intune によるローカル グループのメンバーシップ管理 [1.3.8]

サンプルはここまでです

このテキストの位置づけ: 3 点セットの本編。これだけで問題が解けるようになることが目標で、Intune でデバイスとアプリを管理する仕事を、合格ラインの深さで扱う。

進め方: ① 学習用を読む → ② 頻出度別で解き方を掴む → ③ 問題演習で腕試し → ④ 頻出度別に戻って再確認(試験直前もここ)。暗記用は空き時間や用語の再確認に使う。

SAMPLE

この試験の範囲 [overview]

MD-102(Managing and Securing Microsoft 365 Endpoints by using Intune) は、資格 Microsoft 365 Certified: Endpoint Administrator Associate の試験です。Microsoft Intune と Microsoft Entra ID を使って、Windows、iOS/iPadOS、macOS、Android のデバイスを準備し、構成し、保護し、監視する仕事を問います。

問われるのは、次のような判断です。

- どの登録の方法とプロフィールを選ぶか
- どの設定が要るか
- 画面のどこを操作するか
- 問題が起きた時に、どのレポートとログを見るか

準拠する版

このテキストは、**2026 年 10 月 27 日現在のスキル**(Skills measured as of October 27, 2026)に合わせています。

- 英語の試験: 2026 年 10 月 27 日から新しい版
- 日本語の試験: 英語版の約 8 週間後に切り替え(12 月の後半の見込みで、公式に日付はなし)。それまでは前の版(2026 年 7 月 24 日現在のスキル)で出題
- 2 つの版の違い: 名前の言い換えだけ。分野、配点の幅、細目の数は同じ

日本語の試験で旧称が出る可能性があるため、本文では新しい名前を使い、旧称を必要な所で 1 度ずつ添えています。

試験の基本情報

項目	内容
試験名	MD-102: Managing and Securing Microsoft 365 Endpoints by using Intune
資格	Microsoft 365 Certified: Endpoint Administrator Associate
試験時間	100 分
合格	1000 点満点の 700 点以上
問題数	Microsoft は非公表
言語	日本語で受験できます
出題形式	公式は事前に公表しない。選択式のほか、並べ替え、画面のメニューの選択、ケーススタディが出たという受験記がある

問題数、受験料、申し込み、資格の更新の条件は、受験前に Microsoft の公式の試験ページで確認してください。

5つの分野と配点

分野	配点	この本の章
1 デバイスのインフラストラクチャを準備する	20～25%	第 1 章
2 デバイスの管理と保守	25～30%	第 2 章
3 デバイスを保護する	15～20%	第 3 章
4 アプリケーションの管理とセキュリティ保護	15～20%	第 4 章
5 自動化・監視・レポートでエンドポイント操作を最適化する	10～15%	第 5 章

各章の見出しの末尾の [1.1.1] のような番号は、公式の学習ガイドの項目の番号です。各節がどの項目を扱うかを示します。

第1章 Prepare infrastructure for devices

[1.1.1/1.1.2/1.1.3/1.1.4/1.2.1/1.2.2/1.2.3/1.2.4/1.2.5/1.2.6/1.3.1/1.3.2/1.3.3]

公式の分野 1: デバイスのインフラストラクチャを準備する(配点 20〜25%)

この章は、デバイスを Microsoft Entra ID に載せ、Microsoft Intune に登録し、管理者と準拠の仕組みを整えるまでを扱います。流れは3段で、デバイスの身元 (Entra ID) を作り、管理の対象にし (Intune 登録)、アクセスの条件 (ロール・準拠・条件付きアクセス) を決めます。試験は「どの設定が要るか」を場面で問うので、各論点は名前、定義、設定の形、隣との違い、間違えやすい点の順に読んでください。

デバイス ID の3種と参加の種類の選び方 [1.1.1]

Microsoft Entra ID がデバイスに持たせる身元 (デバイス ID) は3種類あり、Microsoft Entra 登録、Microsoft Entra 参加、Microsoft Entra ハイブリッド参加です。3種は1つの組織の中で共存でき、どれか1つに絞る必要はありません。[^c1-1]

Microsoft Entra 登録は、個人所有のデバイス (BYOD) やモバイル端末向けです。デバイスへのサインインは、Microsoft アカウントなどのローカルアカウントのままです。組織のアカウントは、組織のリソースに入る時だけ追加します。所有者は個人でも組織でも構いません。[^c1-2]

Microsoft Entra 参加は、組織所有のデバイス向けです。デバイスへのサインインに組織のアカウントを使います。クラウドだけの組織でも、オンプレミスの Active Directory を持つ組織でも使えます。[^c1-3]

Microsoft Entra ハイブリッド参加は、オンプレミスの Active Directory Domain Services (AD DS) に参加済みの Windows を、Entra ID にも参加させる形です。位置づけは、Entra 参加へ移る途中の暫定的な手段です。[^c1-1]

比較の軸	Entra 登録	Entra 参加	Entra ハイブリッド参加
向く所有者	個人 (BYOD) または組織	組織	組織
サインインに使うアカウント	ローカル (Microsoft アカウント など)	組織のアカウント	組織のアカウント (AD のドメイン)
主な対象	iOS・Android・macOS・Windows	Windows・macOS 13 以降	Windows のみ
場面の目安	私物のスマートフォン	新規購入の会社 PC	AD 参加済みの既存 PC

参加の対象 OS には条件があります。Windows 11 と Windows 10 は対象ですが、Home エディションは除きます。Azure 上の Windows Server 2019 以降の仮想マシンも対象ですが、Server Core は使えません。macOS は 13 以降が対象です。[^c1-3]

参加の種類と OS の組み合わせは、おおまかに次の表のとおりです。

OS	使える ID の種類
Windows 11 / 10	登録、参加、ハイブリッド参加 (Home エディションは登録のみ)
macOS	登録 (Company Portal)。13 以降は参加も対象

OS	使える ID の種類
iOS / iPadOS	登録 (Company Portal または Authenticator)
Android	登録 (Company Portal または Authenticator)

[^c1-3]

選び方は所有者と OS で決まります。私物の端末で、端末へのサインインに組織のアカウントを求めないなら、登録です。会社買った Windows PC をクラウドで管理するなら、参加です。すでに AD に参加している PC を当面そのまま使うなら、ハイブリッド参加になります。Windows の Home エディションは参加できないので、登録を使うしかありません。間違えやすいのは、登録した端末が自動で管理されと考える点です。Entra 登録は ID の話で、設定の強制には Intune への登録が別に要ります。

Windows を Entra ID に参加させる方法と設定 [1.1.2]

Windows を Entra 参加させる方法は3つです。

- OOBЕ (初期設定) または設定アプリで、利用者が自分で参加する自己サービス
- 一括登録 (プロビジョニングパッケージ)
- Windows Autopilot

OOBE では、新しい Windows 11 の初期設定で「職場または学校用にセットアップ」を選び、組織の資格情報でサインインします。インターネット接続が必須で、接続した状態で、セットアップの種類を選ぶ画面に進みます。[^c1-4] 既存の PC は、設定アプリの「アカウント」→「職場または学校にアクセスする」で「接続」を選び、開いた画面で、アカウントを入力する前に「このデバイスを Microsoft Entra ID に参加させる」を選びます。そのあと組織のアカウントでサインインします。[^c1-3]

参加の可否と上限は、Entra 管理センターのデバイス設定で決めます。

設定	既定値	補足
Users may join devices to Microsoft Entra ID	All	Selected (一部のグループ) や None にできる
Maximum number of devices (ユーザーあたり)	50	100 まで上げられる。100 を超える値を入れても 100 になる。Unlimited も選べる
Require multifactor authentication to register or join devices	No	MFA の強制は、条件付きアクセスの「デバイスの登録または参加」で行うことが推奨される
Additional local administrators	なし	指定したユーザーは Microsoft Entra Joined Device Local Administrator ロールになり、テナント全体の参加デバイスに適用される

[^c1-5]

間違えやすい点は2つあります。1つ目は、参加時の MFA を要求したい場面で、この設定の既定は No です。強制は設定の画面ではなく、条件付きアクセスのポリシーで行うのが推奨です。[^c1-5]

2つ目は、ローカル管理者です。追加のローカル管理者は、特定の運用担当者をテナント内の参加済みデバイスすべての管理者にする設定です。ユーザー個別の割り当てではありません。

Entra ID への登録と、登録と参加の違い [1.1.3]

Entra 登録は、利用者が自分のデバイスに職場または学校のアカウントを追加して行います。入口は OS ごとに違います。

OS	登録の入口
Windows 10 以降	設定アプリ (職場または学校アカウントの追加)
iOS・Android	Company Portal または Microsoft Authenticator
macOS	Company Portal

Windows では、設定アプリで職場または学校のアカウントを追加する時に、参加の選択肢を選ばずに職場のメールアドレスでサインインすると、Entra 登録になります。iOS・Android・macOS の登録は、Company Portal を入れて起動し、組織のアカウントでサインインするまで始まりません。

登録したデバイスで使える機能は4つです。クラウドリソースへのシングル サインオン (SSO)、Intune 登録時の条件付きアクセス、アプリ保護ポリシー経由の条件付きアクセス、Authenticator の電話サインインです。[^c1-2]

登録と参加の違いは、サインインに使うアカウントとオンプレミスへの SSO に出ます。

観点	登録	参加
デバイスにサインインするアカウント	ローカルアカウント	組織のアカウント
組織のリソース用アカウント	追加で持つ	サインインそのもの
SSO の範囲	主にクラウドリソース	クラウドとオンプレミスの両方
条件付きアクセス	デバイス ID に適用できる	デバイス ID に適用できる

[^c1-1]

「登録」という語が2つの意味で出る点に注意してください。Entra への登録 (デバイス ID を作ること) と、Intune への登録 (enrollment。MDM の管理下に入ること) は別物です。Entra 登録だけでは、デバイスに構成を強制できません。MDM である Intune に登録して初めて、ポリシーを強制できます。

デバイスのグループと動的メンバーシップルール [1.1.4]

Intune で配布の単位に使うグループは、セキュリティが有効なグループです。メンバーシップの種類は、割り当て (Assigned。手で入れる) と動的 (Dynamic。ルールで入る) の両方が使えます。既定の Microsoft 365 グループはユーザーのみで、デバイスの割り当てには使えません。[^c1-8]

ユーザーのグループとデバイスのグループは使い分けます。ユーザーのグループは、人に付いて回る設定に向き、メールの設定や、どの端末からでも付けたいアプリがその例です。端末に付く設定は、デバイスのグループの役目になります。キオスク端末の構成や、会社所有 PC の BitLocker が該当します。1つの動的ルールにユーザーとデバイスは混在できません。デバイスのルールは、所有者のユーザー属性を参照できず、デバイスの属性だけを使います。[^c1-6]

動的グループの数値は3つ覚えます。1テナントの動的メンバーシップ グループは最大15,000個。メンバーシップ ルール本体は3,072文字まで。ライセンスは、メンバーのユーザーごとに Microsoft Entra ID P1 (または Intune for Education) が要りますが、デバイスだけがメンバーの場合は不要です。[^c1-6]

ルールの書式は「属性 演算子 値」です。デバイスで使う主な属性は次の4つです。

属性	取りうる値	ルールの例
deviceOSType	Windows, iPad, iPhone など	<code>device.deviceOSType -eq "Windows"</code>
deviceOwnership	Personal, Company, Unknown	<code>device.deviceOwnership -eq "Company"</code>
enrollmentProfileName	ADE・Android 専用デバイス・Autopilot の登録プロファイル名	<code>device.enrollmentProfileName -eq "DEP iPhones"</code>
devicePhysicalIds	Autopilot が使う文字列 (ZTDId, OrderID, PurchaseOrderId)	<code>device.devicePhysicalIDs -any _ -startsWith "[ZTDId]"</code>

[^c1-6]

`[ZTDId]` で始まる値を持つのが Autopilot のデバイスなので、上の最後のルールは「Autopilot に登録されたデバイスすべて」を表します。複数の値を持てる属性は `-any _` の形で書きます。複数条件は `-and` と `-or` でつなぎます。参加の種類で絞るなら `deviceTrustType` を使い、AzureAD が Entra 参加、ServerAD がハイブリッド参加、Workplace が Entra 登録を表します。[^c1-6]

動的グループは評価に時間が掛かります。ルールを保存した直後や、デバイスの属性が変わった直後に、メンバーが入るとは限りません。この遅れが問題になる配布には、割り当てフィルターが向きます。

観点	動的グループ	割り当てフィルター
働く場所	Entra ID のグループ。条件付きアクセス・ライセンス・Autopilot など Intune 以外でも使える	Intune のアプリ・ポリシー・プロファイルの割り当て
評価の時期	メンバーシップの処理後(遅れがある)	登録時やチェックインなどポリシー評価の時(遅れなし)
上限	1テナント15,000グループ	1テナント200個、1フィルター3,072文字
前提	なし	管理対象デバイスのフィルターは Intune 登録済みが前提 (管理対象アプリのフィルターは未登録の端末のアプリにも使える)

[^c1-7]

Intune の配布は、フィルターで足りるならフィルターを選びます。条件付きアクセスやライセンスのように、グループでしか指定できない場面だけ、動的グループを使います。フィルターはグループの代わりにならず、グループに掛ける条件という位置づけです[^c1-6]。「割り当てるグループ」を選んだうえで、含める (Include) か除外する (Exclude) かを指定する形になります。

登録の制限と Intune の登録の設定 [1.2.1]

登録の制限は2種類あります。デバイスの種類（プラットフォーム）の制限と、デバイス数の制限です[^c1-9]。どちらにも既定のポリシーが1つあります。それより優先度の高いポリシーを割り当てない限り、既定がすべての登録に適用されます。[^c1-9]

制限	設定できる内容
デバイス数の制限	1人が登録できる台数。1～15
デバイスの種類の制限	プラットフォーム (Android デバイス管理者・Android Enterprise の個人所有仕事用プロファイル・iOS/iPadOS・macOS・Windows)、OS バージョンの最小と最大、Android のメーカー、個人所有デバイスのブロック

OS バージョンの制限は、iOS/iPadOS と Android では Company Portal で登録するデバイスにだけ効きます。メーカーの制限は Android だけです。両方の Android (仕事用プロファイルとデバイス管理者) を許可したグループでは、仕事用プロファイルに対応する端末は仕事用プロファイルで登録されます。[^c1-9]

個人所有のブロックは、「何が会社所有か」の判定に左右されます。

OS	会社所有と扱われる条件
iOS/iPadOS	シリアル番号または IMEI で登録済み、または ADE で登録
macOS	シリアル番号で登録済み、または ADE で登録
Windows	企業登録として認可された方法 (Autopilot、グループ ポリシー、一括プロビジョニング、DEM など)

iOS/iPadOS と macOS は、何もしなければ個人所有扱いです。個人所有をブロックしたのに、会社の端末が登録できなくなる場面では、その端末の識別子を事前に登録したかを疑います。[^c1-9]

制限が効かない登録があります。ユーザー駆動ではない登録には、既定のポリシーだけが適用されます。公式の例は、Autopilot の自己展開と事前プロビジョニング、Windows Configuration Designer による一括登録、Configuration Manager との共同管理、ユーザー関連付けなしの ADE、Azure Virtual Desktop、Windows 365、Android の専用デバイスです。登録の制限はセキュリティ機能ではありません。侵害された端末は属性を偽れるので、悪意のないユーザーに対する努力目標の障壁にとどまります。[^c1-9]

デバイス登録マネージャー (DEM) は、管理者ではない専用のユーザーで、多数のデバイスを登録するための仕組みです。標準の非管理者アカウントが登録できるのは15台までですが、DEM は最大1,000台を登録・管理できます。使う方法は、プロビジョニング パッケージによる一括登録、Company Portal での DEM による登録、Entra 参加での DEM による登録の3つです。DEM の追加と削除には Intune Administrator ロールが必要で、DEM には Intune のユーザーまたはデバイスのライセンスと Entra ユーザーが要ります。ADE とは併用できません。[^c1-10]

同じ目的でも、共同管理、グループ ポリシーによる自動登録、Autopilot なら15台を超えて登録できるので、DEM は不要です。DEM のアカウントは、個人に割り当てない専用のアカウントにします。DEM で登録した端末があるうちは、そのアカウントを削除しません。削除するとそれらの端末に問題が出ます。[^c1-10]

Intune の登録の設定には、ほかに次のものがあります。

- MDM 機関 (MDM authority) : Intune を MDM として使うと宣言する設定です。Apple のデバイスの登録では、この設定が前提になります。[^c1-15]
- デバイス カテゴリ: 管理対象のデバイスに付けるラベルです。カテゴリ名を使って `device.deviceCategory -eq "HR"` のような動的グループのルールを書くと、そのカテゴリのデバイスが自動でグループに入ります。設定には Intune Administrator が必要です。[^c1-11]
- 登録の通知: 登録されたことを利用者に知らせる設定

Windows の自動登録と共同管理、登録失敗の調べ方 [1.2.2]

Windows の自動登録は、Entra 参加や Entra 登録をきっかけに、自動で Intune に登録される仕組みです。設定は Entra 管理センターの「Mobility (MDM and MAM)」で、Microsoft Intune を選んで行います。前提は、Intune のサブスクリプションと、Microsoft Entra ID P1 または P2 です。サインインには Global Administrator のロールが要ります。[^c1-12]

MDM のユーザー スコープは3値です。

値	意味
None	自動 MDM 登録を無効にする。利用者が自分で登録を始める
Some	選択したグループのユーザーだけが自動登録の対象
All	すべてのユーザーが対象

MAM のユーザー スコープ (WIP のユーザー スコープ) も別にあります。両方のスコープに同じユーザーが含まれる場合、企業所有のデバイスでは MDM スコープが優先されます。個人所有のデバイスでは MAM (WIP) のスコープが優先され、Intune に登録されません。BYOD を MDM に登録させたいなら、MAM のスコープを None または Some にします。[^c1-12]

この仕組みを使える場面は5つで、BYOD、一括登録、グループ ポリシー、Windows Autopilot、Configuration Manager との共同管理です。

AD に参加したデバイスは、グループ ポリシー (Enable automatic MDM enrollment using default Microsoft Entra credentials) で自動登録を始められ、GPO を当てる PC はセキュリティ グループのフィルターで絞ります。MDM のユーザー スコープ自体はユーザー単位の設定で、デバイス単位ではありません。Configuration Manager も使っている組織では、共同管理 (co-management) を使います。Configuration Manager と Intune を同時に使い、ワークロード単位で管理の権限を Intune に切り替える方式です。パイロットのコレクションを作れば、一部のデバイスから試せます。Configuration Manager とサードパーティの MDM の併用は、共同管理とは呼ばず、コエグジスタンス (coexistence) と呼びます。[^c1-13]

登録に失敗した時は、原因の見当を次の表で付けます。

症状	原因	直し方
エラー 8018000a「デバイスはすでに登録されている」	別のユーザーがすでに登録・参加済み	先のユーザーの登録を解除する
「This account is not allowed on this phone」	有効な Intune ライセンスがない	ライセンスを割り当てて登録し直す

症状	原因	直し方
0x8007064c「すでに登録されている」	以前に登録済み、登録済みの PC をクローンしたイメージ、または前のアカウントの証明書が残っている	残った Intune の証明書 (Sc_Online_Issuing 発行) と OnlineManagement のレジストリ キーを削除して、登録し直す
MDM 利用規約のエンドポイントのエラー	MDM 利用規約の URL が空か正しくない。または MDM for Microsoft 365 と Intune の併用で、ユーザーに有効なライセンスがない	URL なら Entra の Mobility (MDM and MAM) で Microsoft Intune を開き、Restore default MDM URLs を選ぶ。ライセンスなら Intune か Microsoft 365 のライセンスを割り当て

[^c1-14]

調べる順番は、ユーザーのライセンス、MDM のユーザー スコープ、登録の制限 (プラットフォームと台数) です。それでも原因が分からない時は、デバイス側のイベント ログを見てください。場所は、イベント ビューアーの「アプリケーションとサービス ログ」にある Microsoft、Windows、DeviceManagement-Enterprise-Diagnostics-Provider の Admin です。自動登録の失敗はイベント ID 76 に残ります。MDM のユーザー スコープが None だと自動登録は起きません。[^c1-14]

iOS/iPadOS・macOS の個人用登録と Apple MDM プッシュ証明書 [1.2.3]

Apple のデバイスを管理するには、Apple MDM プッシュ証明書が前提で、iOS/iPadOS と macOS のどの登録方式でも要ります。

プッシュ証明書は365日有効で、毎年更新します。入力した Apple ID は、更新が必要な時期を知らせるために使われます。失効後も30日の猶予があります[^c1-16]。更新は、作成した時と同じ Apple アカウントで行います。別のアカウントで更新すると別の証明書になり、登録済みのデバイスを管理できなくなります。[^c1-16]

作成の手順は4段です。

- 1. Intune 管理センターで CSR (証明書署名要求) をダウンロードする
- 2. Apple Push Certificates Portal で、CSR を使って証明書 (.pem) を作る
- 3. Apple ID を入力する (更新の時期を知らせるために使う)
- 4. .pem を Intune にアップロードする

この順序は、CSR が先で、.pem が後です。Apple の側で作る証明書は、Intune が出す CSR に対応しているからです。[^c1-16]

iOS/iPadOS の個人用登録の方式は、次の表の3つです。

方式	始め方	特徴
アカウント駆動のユーザー登録	利用者が設定アプリで職場アカウントにサインインする	JIT 登録と Microsoft Authenticator を使う。iOS/iPadOS 15 以降。仕事用の領域 (ワーク パーティション) だけを管理する
Company Portal によるデバイス登録	利用者が Company Portal アプリで始める	個人所有でも、端末全体を管理する。端末全体に効く証明書を配れる

方式	始め方	特徴
Company Portal によるユーザー登録	利用者が Company Portal アプリで始める	廃止 (deprecated) され、新しく登録する端末には使えない。すでにこのプロファイルを持つ端末だけがサポートされる

アカウント駆動のユーザー登録は iOS/iPadOS 15 以降が対象です。14.9 以前の端末の扱いは文書によって記述が違います (設定のページは Company Portal 経由のユーザー登録に自動で切り替えると書き、方式の概要のページは Company Portal 経由のユーザー登録を新しい登録には使えない廃止の方式としています)。前提は4つです。MDM 機関の設定、Apple MDM プッシュ証明書、デバイスユーザー用の Managed Apple ID、サービス検出ファイルです。[^c1-15]

サービス検出ファイルは、Apple が Intune に到達するためのものです。https://<ドメイン>/.well-known/com.apple.remotemanagement で公開します。ファイル名に拡張子 (.json など) は付けません。content type は application/json にします。中身の JSON では、Version に mdm-byod、BaseURL に Intune の登録サーバーの URL を書きます。設定が合っていないと、サインイン失敗のメッセージが出ます。内容は「Your Apple ID does not support the expected services on this device」です。[^c1-15]

macOS の個人用登録 (BYOD) は、Company Portal で行います。利用者は Company Portal の Web サイトから、または Company Portal アプリ (aka.ms/EnrollMyMac) から端末を追加します。Mac の登録はすべてユーザー承認 (user-approved) の登録で、macOS 11 以降では監督 (supervision) が自動で有効になります。[^c1-17]

管理できる範囲の違いが問われる場面があります。強制できる設定の範囲は、登録の方式で決まります。Company Portal で登録した Mac はユーザー承認の登録で、ADE や Apple Configurator で登録した監督対象の Mac と同じ水準の制御ができます。アカウント駆動のユーザー登録では、設定が効くのは仕事用の領域だけです[^c1-16]。管理者がリモートで行える操作は、廃止 (Retire)・削除・リモート ロック・同期で、端末全体のワイプはできません。登録を解除すると、仕事用のボリュームと鍵が消えます。Company Portal によるデバイス登録は端末全体を管理するので、個人所有でも端末全体に効く証明書を配れます。Apple の OS の更新のポリシー (宣言型のソフトウェア更新。iOS/iPadOS 17 以降・macOS 14 以降) が効くのは、デバイス登録と ADE の端末で、ユーザー登録は対象外です。

ユーザー登録では、管理対象のボリュームの外にあるアプリを MDM で管理できません。登録の前に利用者が入れたアプリは、利用者が削除しない限り、管理を引き継ぐことも管理版を配ることもできません (アプリ保護ポリシーは効きます)。

Android Enterprise の登録の種類と登録プロファイル [1.2.4]

Android Enterprise の登録は4種類あり、所有者と使い方で選びます。[^c1-18]

種類	略称	所有者	向く場面
個人所有の仕事用プロファイル	BYOD	個人	私物の端末に仕事用の領域だけを作る
会社所有の仕事用プロファイル	COPE	会社	私用も許可する会社端末。別に仕事用プロファイルを作る
完全管理	COBO	会社	仕事専用で1人が使う端末。端末全体を管理する

種類	略称	所有者	向く場面
専用デバイス	COSU	会社	キオスク、サイネージ、チケット印刷など単一用途の端末

選び方の軸は、私用を許すか、端末全体を管理するか、利用者が1人か共有かの3つです。私物の端末なら BYOD です。会社の端末で私用を許すなら COPE です[^c1-18]。仕事専用で、1人が使うなら完全管理です。特定のアプリだけを動かすキオスクのような端末なら専用デバイスです。

専用デバイスでは、アプリとリンクを制限して、端末を本来の用途以外に使わせないようにできます[^c1-18]。専用デバイスのトークンには、Microsoft Entra の共有デバイス モードで登録する種類もあります。なお、完全管理のプロファイルを作ると、既定のプロファイル(名前は Default Fully Managed Profile)とトークンが自動で作られます。[^c1-19][^c1-21]

登録の方法は5つです。QR コード、Google ゼロタッチ、Knox Mobile Enrollment、NFC、トークンの入力です。QR コードは多くの場面で推奨される方法で、初期化した端末の最初の画面を繰り返しタップして QR リーダーを起動し、プロファイルの QR をスキャンします。トークンの入力、QR や NFC が使えない新規または初期化済みの端末向けです。トークンの期限の扱いは、トークンの種類によって同じではありません。専用デバイスのトークンは Intune ライセンスのある全ユーザーに使い、期限切れになりませんが、完全管理と COPE のステージングトークンには期限を指定できます(最長 65 年先)。^[^c1-21]

トークンの期限は、プロファイルの種類で違います。

プロファイル	トークンの扱い
完全管理	既定のトークンに加え、ステージングトークンがある。期限(Token expiration date)はステージングトークンだけで指定でき、最長で65年先まで
会社所有の仕任用プロファイル(COPE)	既定のトークンは自動では失効しない。ステージングトークン(via staging)は期限を指定でき、最長で65年先まで。取り消す(revoke)と、関連するプロファイルが一覧から非表示になる

[^c1-19][^c1-20]

ステージングトークンは、ベンダーや IT 部門が事前の準備をすべて済ませ、利用者は最後に Microsoft Intune アプリへ自分の職場アカウントでサインインして完了する流れです。取り消しは、トークンを即座に無効にする操作です。期限が近いトークンは、新しいトークンに置き換えます。^[^c1-19]

Android Enterprise の管理を始めるには、Intune のテナントと Managed Google Play のアカウントの連携が前提です。連携には Intune Administrator のロール、または組織 (Organization) の読み取りと更新の権限を持つカスタム ロールが必要です。この連携がないと、4つのどの登録も使えません。^[^c1-22]

Android の登録の制限は、登録の制限の機能(前の節)で設定します。プラットフォーム、OS バージョン(Company Portal での登録だけ)、メーカー(Android のみ)、個人所有のブロックが使えます。個人所有の仕任用プロファイルをブロックすると、会社所有の端末だけが登録できます。^[^c1-9]

登録の失敗を調べる時は、次の点を見ます。

- 登録途中で再起動していないか。登録が不完全になり、Intune のポリシーで保護されない状態になることがあります。
- 条件付きアクセスで準拠を必須にして、対象を「すべてのクラウド アプリ」にしていないか。この場合は、Microsoft Intune のクラウド アプリをポリシーから除外します。Android の初期設定は、Chrome のタブで利用者を認証するからです。
- Managed Google Play の連携、トークンの失効、登録の制限で止まっていないか。

[^c1-21]

会社所有の仕事用プロファイルで Android 15 の端末を使い、FRP (工場出荷時リセット保護) のメール設定をしている場合です。設定アプリからリセットした後は、関連する Google アカウントの再入力が必要になります。[^c1-21]

Apple Business Manager と連携した iOS/macOS の企業登録 (ADE) [1.2.5]

会社が購入した Apple 製品は、自動デバイス登録 (ADE。Automated Device Enrollment、旧 DEP) で登録します。電源を入れた端末が自動で Intune に登録される仕組みです。Apple の管理ポータルは、現在 Apple Business (または Apple School Manager) という名前です。学習ガイドでは旧称の Apple Business Manager で書かれているので、以降は ABM と略して同じポータルを指します。[^c1-23][^c1-43]

事前に必要なものは2つです。有効な Apple のトークン (.p7m ファイル) と、ABM で購入した新規または初期化済みのデバイスです。流れは4段です。

- Intune でトークン用の公開鍵をダウンロードし、ABM でサーバー トークン (.p7m) をダウンロードして、Intune にアップロードする
- ABM でデバイスを Intune のサーバーに割り当てる
- Intune で登録プロファイル (登録ポリシー) を作り、デバイスに割り当てる
- 利用者が電源を入れると登録される

登録プロファイルを割り当てるまで、デバイスはアクティブになりません。プロファイルが割り当てられていないデバイスの電源を入れると、登録は失敗します。1つのトークンあたり、登録ポリシーは1,000件までです。そのため、既定のプロファイルを早めに設定しておく運用が勧められています。[^c1-23]

登録プロファイルの主な設定は次のとおりです。

設定	選択肢と意味
ユーザー アフィニティ	あり (Enroll with User Affinity) : Company Portal を使う利用者 所有のデバイス向け。なし (userless) : キオスク、POS、共有デバイス 向け
認証方法 (アフィニティありのとき)	Company Portal、または Setup Assistant with modern authentication (推奨)。従来の認証は非推奨
監視モード (Supervised)	Yes で監視対象になる。管理できる機能が増える
ロックされた登録 (Locked enrollment)	Yes にすると管理プロファイルの削除ボタンが隠れ、利用者は登録 を解除できない

設定	選択肢と意味
Await final configuration	Setup Assistant の終了前に、重要な構成を Intune が先に適用する画面
セットアップ アシスタントの画面	パスワード、位置情報サービス、Apple ID など、表示する画面を選ぶ

[^c1-23][^c1-24]

ABM の外で購入し、あとから ADE に追加したデバイスでは、ロックされた登録が効くまでに猶予があります。最初の 30 日は、削除ボタンが見えます。Await final configuration の既定は、新しい登録ポリシーが Yes、既存のポリシーが No です。待ち時間の最小や最大の規定はなく、検証では多くのデバイスが 15 分以内にホーム画面に進んでいます。設定が反映されるのは構成の適用だけで、アプリは含まれません。[^c1-23][^c1-24]

ADE の登録プロファイルを後から変更しても、すでに割り当て済みのデバイスには反映されません。デバイスを工場出荷時の状態に戻して再度アクティブにする必要があります。例外はデバイス名のテンプレートだけです。[^c1-23]

ADE の Company Portal は、App Store 版ではなく、Intune から VPP アプリとして配布します。デバイス ライセンスを使うのが、条件です。App Store 版は ADE と互換性がありません。Company Portal のライセンスが足りない時や、トークンが期限切れの時は、デバイスの登録がブロックされます。[^c1-23]

ADE トークンの更新と Apple Configurator との違い。ADE のサーバートークンは 1 年で期限が切れるので、毎年更新します。期限は Intune 管理センターに表示され、更新には、作成した時の Apple ID を入力します。ABM 側で新しいトークンをダウンロードすると、Intune が使っているトークンが無効になるので、ダウンロードは更新する時だけにしてください。トークンの作成者の Apple ID のパスワードが変わった時や、作成者が退職した時も更新します。[^c1-44]

Apple Configurator による登録は、ADE と別の道です。ADE で登録しなかった端末を監視モードにするには、Apple Configurator が必要です。Mac に USB で接続して、端末を初期化します。ADE は、電源を入れた後に無線 (OTA) で展開されるので、USB での作業は要りません。大量の端末を扱うなら、監視モードを有効にする手段として ADE が勧められています。[^c1-23]

DEM (前の節) は ADE と互換性がありません。ADE の端末は、DEM のアカウントで登録しません。

Samsung Knox Mobile Enrollment と Google ゼロタッチ登録 [1.2.6]

どちらも、Android 端末を購入元の側で Intune に紐づけておき、電源を入れた時点で自動登録させる一括登録の仕組みです。

Samsung Knox Mobile Enrollment (KME) は、Samsung 製の端末が対象です。専用デバイス、完全管理デバイス、会社所有の仕事用プロファイルの 3 種に使えます。Knox Admin Portal を使うには Samsung Knox のアカウントが必要で、Samsung の承認に 1~2 営業日かかります。[^c1-25]

連携の手順は次のとおりです。

- 1. Intune で、対象の種類の登録プロファイルを作り、トークンを得る
- 2. Knox Admin Portal でプロファイルを作り、EMM に Microsoft Intune を指定する

3. Custom JSON data に `{"com.google.android.apps.work.clouddpc.EXTRA_ENROLLMENT_TOKEN": "<トークン文字列>"}` を入れる

4. デバイスをプロファイルに割り当てる

Custom JSON data は Knox Admin Portal 上では任意に見えますが、Intune では必須です。入れ忘れると登録が成立しません。[^c1-25]

Google のゼロタッチ登録は、Google の対応販売店から購入した端末が対象で、電源を入れると自動でプロビジョニングが始まります。一括の登録や、遠隔地で働く人への配送に向く方法です。Intune でゼロタッチ アカウントを連携すると、完全管理用の既定の構成が作られ、ゼロタッチ ポータルの既定の構成を上書きします[^c1-25]。この既定のトークンは、完全管理専用です。会社所有の仕事用プロファイルや専用デバイスに使う時は、アカウントを連携させず、ゼロタッチ ポータルで構成を作り、DPC extras にトークンを貼ります。[^c1-21]

方法	向く場面	備考
QR コード	端末を手元でスキャンできる。多くの場面で推奨	初期化した端末の最初の画面をタップして QR リーダーを起動
トークンの入力	QR や NFC が使えない新規・初期化済みの端末	登録の方法のページは、トークンは期限切れにならず Intune ライセンスのある全ユーザーに有効と書く(ステージングトークンは期限を指定できる)
KME	Samsung 端末の一括登録	Knox アカウントと Custom JSON が必要
ゼロタッチ	購入元で紐づけた端末の一括登録	既定は完全管理。ほかの種類はポータルで構成して DPC extras にトークンを貼る
NFC	NFC タグを作れる環境	タグは自前のアプリや作成ツールで作る

[^c1-18][^c1-21]

使い分けは端末の入手経路で決まり、Samsung 端末を購入元の登録サービスで一括管理するなら KME、Google の販売店経由ならゼロタッチ、手元に端末があって手作業で登録するなら QR になります。

Intune と Windows 365 のロールの管理 [1.3.1]

Intune の権限は、ロールベースのアクセス制御 (RBAC) で管理します。この RBAC は Microsoft Entra の RBAC を拡張したものです。Global Administrator と Intune Administrator (どちらも Entra のロール) は、Intune のすべてのデータを読み書きできます。特権ロールなので、日常の運用には使いません。使うのは、Intune の組み込みロールやカスタム ロールです。[^c1-26]

Intune の組み込みロールの主なものは次のとおりです。

ロール	役割
Application Manager	モバイルアプリと管理対象アプリを管理する。デバイス情報とデバイス構成プロファイルは読むだけ
Endpoint Security Manager	セキュリティと準拠の機能(セキュリティ ベースライン、デバイスの準拠、条件付きアクセス、Microsoft Defender for Endpoint など)を管理する

ロール	役割
Help Desk Operator	ユーザーとデバイスへのリモート操作を行い、アプリやポリシーをユーザーやデバイスに割り当てられる
Intune Role Administrator	カスタム ロールを管理し、組み込みロールの割り当てを追加できる。管理者へ権限を割り当てられる唯一の Intune ロール
Policy and Profile Manager	準拠ポリシー、構成プロファイル、Apple の登録、セキュリティ ベースラインを管理する
Read Only Operator	情報を読むだけ
School Administrator	Intune for Education を管理する

[^c1-26]

組み込みロールの権限は編集できません。権限を変えたい時は、カスタム ロールを作ります。カスタム ロールは、カテゴリごとに権限（読み取り、作成、更新、削除など）を選んで作ります。[^c1-27]

ロールを管理者に結びつけるのが**ロールの割り当て**です。割り当ては3つの部品で構成されます。

部品	内容
メンバー (Admin Groups)	ロールを持つ管理者のグループ
スコープ グループ (Scope Groups)	管理者が操作できるユーザーとデバイスのグループ
スコープ タグ (Scope tags)	管理者に見えるオブジェクトを絞るタグ

[^c1-26]

Multi Admin Approval を有効にすると、ロールの権限、管理者グループ、メンバー グループの割り当ての変更にも、別の管理者の承認が必要になります。[^c1-27]

Windows 365 のサブスクリプションがあるテナントでは、Intune 管理センターに Cloud PC のロールが加わります。Cloud PC Administrator（読み書き）と Cloud PC Reader（読み取り）です。これらは既定では使えません。Windows 365 向けの操作を任せる担当者には、このロールを割り当てます。Cloud PC を管理できる Microsoft Entra のロールには、Windows 365 Administrator もあります。Cloud PC のプロビジョニングには、Intune Administrator か Windows 365 Administrator のどちらかが要ります。ただし Windows 365 のロールの文書は、Intune の Cloud PC Administrator もプロビジョニングを含めて Cloud PC のすべてを管理できると書いており、文書によって書き方が違います。[^c1-26][^c1-45]

組み込みロールとカスタム ロールの選び方の原則は、最小の権限にすることです。ヘルプ デスクの担当者にリモート操作で利用者を支援させるなら、Help Desk Operator で足ります。ただし Help Desk Operator はアプリやポリシーの割り当てでもできるので、ワイプだけに絞りたい時はカスタム ロールを作ります。読み取りだけの監査担当者には Read Only Operator を割り当てます[^c1-26]。組織固有の組み合わせが要る時に、初めてカスタム ロールを作ります。

スコープ タグとスコープ付き管理 [1.3.2]

ルールが決めるのは、管理者が「できる操作」です。スコープ タグが決めるのは、管理者に「見えるオブジェクト」です。この役割分担は、拠点ごとに管理者を分ける環境（分散した IT）で特に役立ちます。[^c1-28]

スコープ タグは、ポリシー、アプリ、デバイスなどのオブジェクトに付け、ルールの割り当てにも同じタグを付けます。割り当てを持つ管理者は、そのタグが付いたオブジェクトだけを見て、割り当てのルールの権限で操作します。

具体例で見ます[^c1-28]。東京と大阪に拠点があり、各拠点の管理者に自拠点のデバイスだけを管理させたい場面を考えます。Tokyo と Osaka のスコープ タグを作ります。東京の管理者のルール割り当てでは、スコープ グループに東京のデバイス グループを、スコープ タグに Tokyo を指定します[^c1-28]。ポリシーとデバイスにも Tokyo を付けます。大阪も同じ形で作ります。これで、東京の管理者には大阪のポリシーが見えません。

項目	内容
既定のスコープ タグ	スコープ タグに対応していて、タグが付いていないオブジェクトすべてに自動で付く
カスタム タグが1つもない時	一部のポリシーではスコープ タグの画面が出ない
上限	ルールにもオブジェクトにも、割り当てられるタグは最大100個。タグ付きのオブジェクトには少なくとも1つのタグが必要
作成・更新・削除	Intune Administrator の Entra ロールが必要。ルールの割り当てでタグを持つ管理者は、マスター一覧のタグを更新・削除できない

[^c1-28]

間違えやすい点が3つあります。1つ目は、Entra のルールにはスコープ タグが効かないことです。Intune RBAC は Entra のルールには適用されません。そのため Intune Administrator (Intune Service Administrator) は、タグに関係なく Intune のすべてを管理できます。2つ目は、スコープ タグのない割り当てで、この場合はすべてのオブジェクトが見えます。3つ目は、複数の割り当ての統合です。管理者が異なるタグの複数の割り当てに属し、同じ権限カテゴリを持つと、既定では権限が統合され、想定より広いアクセスになります。2026年3月から、Scoped permissions というオプトインのプレビューがあり、一度有効にすると元に戻せません。[^c1-28]

複数管理者の承認 (Multi Admin Approval) [1.3.3]

Multi Admin Approval (MAA) は、重要な変更を、別の管理者が承認するまで適用させない仕組みです。1人の管理者の誤操作や、乗っ取られたアカウントによる変更を防ぎます。[^c1-29]

仕組みは**アクセス ポリシー**で作ります。アクセス ポリシーは、どのリソースの変更に承認を求めるかを決めます。対象にできるのは次の7種類です。

- アプリ (Apps)
- 準拠ポリシー (Compliance policies)
- 構成ポリシー (Configuration policies)
- デバイスの操作 (Device actions: ワイプ、リタイア、削除)
- ロールベースのアクセス制御 (Role-based access control)
- スクリプト (Scripts)

● テナント構成 (Tenant Configuration: デバイス カテゴリ)

アクセス ポリシーの作成と管理には、MAA の権限を含むカスタム Intune ロール (推奨) か、Intune Administrator が必要です。ポリシーの作成直後のポリシー自体にも、別の管理者の承認が要ります。[^c1-29]

承認者の条件は次のとおりです。テナントに管理者のアカウントが少なくとも2つ必要です。承認者は、承認者のグループ (セキュリティ グループのみ) のメンバーで、対象のリソースの Read 権限を持ちます。そのグループ自体を、RBAC のロール割り当てのメンバー グループにします。[^c1-29]

承認の流れは、申請、承認、完了の3段です。

- 1. 申請者が変更を申請し、ビジネス上の理由を入力する
- 2. 別の管理者が承認または却下する
- 3. 元の申請者が Complete を選んで変更を適用し、ステータスが Completed になる

承認された変更は、自動では適用されません。申請者が Complete を選ぶ操作が最後に要ります。3日間処理されない申請は Expired になり、再申請が必要です。各ステータスの変更履歴は最大30日間表示されます。[^c1-29]

自己承認はできません。管理者は、承認者のグループのメンバーであっても、自分の申請を承認できません。Global Administrator や Intune Administrator が出した変更にも、別の管理者の承認が要ります。この決まりがあるので、承認者のグループに申請者以外の管理者が最低1人いなければ、変更は通りません。[^c1-29]

コンプライアンス ポリシーと非準拠への対応 [1.3.4]

コンプライアンス (準拠) ポリシーは、管理対象のデバイスが満たすべき規則と条件の集まりです。満たせば準拠、満たさなければ非準拠と評価されます。この結果を条件付きアクセスに渡すと、非準拠のデバイスから会社のリソースへの接続を止められます。[^c1-30]

Intune の準拠は2つの層に分かれます。

層	内容
コンプライアンス ポリシーの設定 (Compliance policy settings)	テナント全体の設定。すべてのデバイスが受け取る組み込みのポリシーのように働く
デバイスのコンプライアンス ポリシー (Device compliance policies)	プラットフォームごとの規則。グループに配布する

設定できる項目はプラットフォームごとに違うため、ポリシーもプラットフォームごとに別に作ります。対象は Windows、iOS/iPadOS、macOS、Android Enterprise、Android デバイス 管理者、AOSP、Linux、Windows Holographic for Business です。[^c1-30]

設定の主な種類は次の表にまとめました。

区分	例
OS のバージョン	最小と最大の OS バージョン
暗号化	Windows の BitLocker、データストレージの暗号化
パスワード	パスワードの要求、最小の長さ、複雑さ

区分	例
デバイスの状態	脱獄 (jailbreak) や root 化の有無、Secure Boot、コード整合性
デバイスのリスク	Microsoft Defender for Endpoint が評価するリスクのレベルが、指定した値以下か

OS ごとの違いで、試験が狙うのは「強制できる項目が違う」点です。準拠の評価には2つの状態があります。Remediated は、OS が準拠を強制する場合です[^c1-30]。パスワードの設定を OS が強制する場合が、その例です。Quarantined は、OS が強制しない場合で、Android が暗号化を強制しないのがその例です。[^c1-30]

テナント全体の設定は2つです。

設定	既定値	内容
Mark devices with no compliance policy assigned as	Compliant	ポリシーが1つも届いていないデバイスの扱い。条件付きアクセスと併用するなら Not compliant に変える
Compliance status validity period (days)	30日	1～120日で設定できる。この期間内に準拠の状態を報告しないデバイスは非準拠になる

[^c1-30]

1つ目の既定が Compliant なので、ポリシーを割り当て忘れたデバイスは準拠として通ってしまいます。条件付きアクセスで準拠を要求するなら、必ず Not compliant に変えます。ポリシーが割り当てられていない利用者の Company Portal には、「No compliance policies have been assigned」と表示されます。[^c1-30]

非準拠に対する操作 (Actions for noncompliance) は、準拠ポリシーごとに設定します。すべての準拠ポリシーには、Mark device noncompliant が0日で組み込まれています。スケジュールを変えると、この操作が猶予期間になります[^c1-30]。たとえば5日にすると、規則を満たさないデバイスは、満たさなくなってから5日が過ぎるまで非準拠にマークされません。この猶予の間に利用者へ通知し、直す時間を与えられます。[^c1-31]

追加できる操作は4つです。

- メールの送信 (利用者への通知)
- リモートロック
- リタイア リストへの追加 (管理者が明示的にリタイアするまで実行されない)
- プッシュ通知

スケジュール (Schedule (days after noncompliance)) は、整数または0.25日刻み (0.25日は6時間) で指定します。それ以外の値は Microsoft Graph で設定します。準拠に関するメールは、非準拠にマークされてから6時間以内に送られます。送信元は microsoft-noreply@microsoft.com で、宛先は利用者のプロファイルのメール アドレスです (UPN ではありません)。[^c1-31]

間違えやすいのは、リタイアの扱いです。リタイア リストに追加する操作は、デバイスを自動でリタイアしません。リストを見た管理者が、明示的にリタイアして初めて、Intune の管理が外れ、会社のデータが消えます。[^c1-30]

準拠済みデバイスを要求する条件付きアクセス [1.3.5]

条件付きアクセスは、サインインの条件（誰が、どのアプリに、どのデバイスから）を見て、許可やブロックを決める Microsoft Entra の機能です。準拠済みデバイスの要求は、許可の制御 (Grant) で「Require device to be marked as compliant」を選んで作ります。[^c1-32]

典型的なポリシーの形は次のとおりです。

項目	値
ユーザー	All users (緊急アクセス アカウントなどを除外)
対象のリソース	All resources
許可の制御	Require device to be marked as compliant
ポリシーの状態	まず Report-only (レポート専用) で作成

[^c1-32]

作る前に、Intune の準拠ポリシーが必要です。準拠ポリシーがないままポリシーを有効にすると、意図どおりに動きません。先に準拠ポリシーを作り、準拠のデバイスを1台以上用意してから進めます。[^c1-32]

Grant の選択肢には、準拠を求める「Require device to be marked as compliant (Microsoft Intune)」と、ハイブリッド参加を求める「Require Microsoft Entra hybrid joined device」があります。2つ以上を選ぶ時は、Require all (すべて満たす) か Require one (どれか1つ) かを指定します。[^c1-33]

要求	満たすデバイス	向く場面
準拠済み	Entra ID に登録され、Intune に登録され、準拠と評価されたデバイス。Windows 10 以降・iOS・Android・macOS・Linux Ubuntu	構成の状態まで条件にしたい
ハイブリッド参加済み	AD と Entra ID の両方に参加した Windows	オンプレミスの AD に参加した PC だけを通したい

準拠の要求は、デバイスが Intune に登録され、準拠ポリシーで評価されていることを条件にします。ハイブリッド参加は、参加している事実だけを見ます。構成の状態は見ません。BYOD の iPhone を通したいなら、ハイブリッド参加の要求は使えません。オンプレミスの AD と Entra ID の両方に参加した (ハイブリッド参加の) Windows PC だけを通したいなら、ハイブリッド参加の要求が使えます。

ポリシーを新しく作る時は、レポート専用モードで作ります。ポリシーは評価されますが、強制はされません。サインイン ログで、有効にしたら誰が止まるかを事前に確かめられます。結果を確かめてから、状態を On にします。[^c1-32]

注意が3つあります。準拠の要求は、All resources が対象でも、Intune への登録そのものはブロックしません。Authenticator が UserAuthenticationMethod.Read へ行うアクセスもブロックしません。ただし、未登録のユーザーの Intune ポータルを含むすべてのアクセスをブロックし得ます。管理者自身が登録済みのデバイスを持たないと、ポリシーを直せなくなる恐れがあります。緊急アクセス アカウントの除外は、このための備えです。[^c1-32][^c1-34]

非準拠でアクセスできない時の調べ方です。Entra 管理センターの「Entra ID」の「Monitoring & health」から「Sign-in logs」を開き、該当のサインインを選びます。「Conditional Access」タブに、サインインを中断させたポリシーが出

ます[^c1-32]。次に、Intune でそのデバイスの準備の状態を見ます。非準備だった時は、どの設定を満たしていないかまで掘り下げてください。[^c1-34]

Intune による Windows Hello for Business の構成 [1.3.6]

Windows Hello for Business (WHfB) は、パスワードの代わりに、デバイスに結びついた資格情報と、生体認証または PIN による強い2要素の認証を使います。[^c1-35]

仕組みは次のとおりです。プロビジョニングの時に、MFA を通した後で、公開鍵と秘密鍵のペアを作ります。秘密鍵は、TPM があれば TPM で保護されます。TPM がなければ、ソフトウェアで暗号化されます。公開鍵は ID プロバイダー (Entra ID) に登録されるので、秘密鍵そのものは外に出ません。サインインでは、PIN や生体認証でその秘密鍵のロックを開き、秘密鍵で署名します。PIN も秘密鍵も ID プロバイダーには送られず、PIN はデバイスに保存もされません。[^c1-36]

構成の方法は3つあり、働く時期が違います。

方法	働く時期・範囲
登録時のテナント全体のポリシー	デバイスを Intune に登録する時。組織全体に適用され、Autopilot の OOBЕ でも働く
エンドポイント セキュリティの Account protection ポリシー	登録した後。グループごとに配布する
設定カタログ (Settings catalog) またはセキュリティ ベースライン	登録した後。Account protection と同じ設定を設定カタログからも使える

[^c1-35]

テナント全体のポリシーは、Devices > Enrollment の Windows タブを開き、Enrollment options の Windows Hello for Business で作ります。作成と編集には Intune Service Administrator が必要で、ほかの Intune ロールは読み取り専用です。Configure Windows Hello for Business には3つの値があります。Enabled は設定を有効にして構成する値です。Disabled にすると、利用者は WHfB を作れません。Not configured は、Intune が WHfB を制御せず、デバイスの既存の設定をそのまま残す値です。[^c1-35]

テナント全体のポリシーの既定値は次のとおりです。

設定	既定値
Use a Trusted Platform Module (TPM)	Required (TPM があるデバイスだけが WHfB を作れる)。Preferred なら、TPM がなければソフトウェア暗号化も可
最小の PIN の長さ	6文字 (4文字まで下げられる)
最大の PIN の長さ	127文字
大文字・小文字・特殊文字	Not allowed
PIN の有効期限	41日
PIN の履歴	直近5つの再利用を禁止

[^c1-35]

PIN の設定が、デバイス構成のポリシーと WHfB のポリシーの両方で指定されて競合した時は、WHfB のポリシーが適用されます。Windows 10 の Anniversary Update (バージョン 1607) で、デバイス PIN と仕事用 PIN が1つに統合されたためです。[^c1-35]

ハイブリッド環境 (オンプレミスの AD も使う) の展開には、3つの信頼の型があります。

型	必要なもの	位置づけ
クラウド Kerberos 信頼	Entra Kerberos。各 AD サイトに十分な数の読み書き可能なドメインコントローラー (DC)	キー信頼より推奨され、展開が簡単
キーの信頼	DC に証明書	証明書の発行基盤の整備が要る
証明書の信頼	ユーザー証明書と PKI	もっとも手間が掛かる

[^c1-37][^c1-38]

クラウド Kerberos 信頼は、ハイブリッド展開向けで、Entra 参加とハイブリッド参加のどちらにも使えます。「Use certificate for on-premises authentication」のポリシーが有効だと、証明書の信頼が優先されます。クラウド Kerberos 信頼を使うマシンでは、このポリシーを未構成にします。証明書の信頼からクラウド Kerberos 信頼への直接の移行手順はなく、Windows Hello のコンテナを削除してから移行します。[^c1-38]

選び方は、オンプレミスのリソースに SSO が要るかで決まります。クラウドだけのリソースなら、オンプレミスの信頼の型は要りません。オンプレミスの SSO が要るハイブリッド環境で、証明書基盤がない場合は、クラウド Kerberos 信頼が第一の候補です。

Windows LAPS の管理 [1.3.7]

Windows のローカルの組み込み管理者アカウントは、削除できず、デバイスへの全権を持ちます。Windows LAPS (Local Administrator Password Solution) は、このアカウントのパスワードをデバイスごとにランダムにする仕組みです[^c1-40]。パスワードは定期的に変わり、ディレクトリに保存されます。パス・ザ・ハッシュなどの攻撃で、1台の侵害が他の端末へ広がるのを防げるのが利点です。[^c1-41]

前提は3つあります。

前提	内容
参加の種類	Entra 参加または Entra ハイブリッド参加のデバイスだけ。Entra 登録 (ワークスペース参加) のデバイスは未対応
Entra 参加での有効化	Entra 管理センターの Devices > Overview > Device settings で、Enable Local Administrator Password Solution (LAPS) を Yes にする。ハイブリッド参加では不要
ライセンスと OS	Microsoft Entra ID Free 以上と Intune Plan 1。Windows 11 / 10 の対応するアップデートの適用後

[^c1-39][^c1-40]

設定の手順は、Intune 管理センターの Endpoint security > Account protection > Create Policy です。Platform に Windows。Profile に Local admin password solution (Windows LAPS) を選びます。主な設定は次のとおりで

す。

設定	内容
Backup Directory	パスワードの保存先。Entra ID、オンプレミスの Active Directory、または保存しない。保存先は、デバイスの参加の種類に合うものを選ぶ
Administrator Account Name	管理するアカウント。空なら、組み込みの管理者を（名前が変わっていても）RID で識別して対象にする
パスワードの複雑さ・長さ	要件を決める
パスワードの有効期間 (PasswordAgeDays)	自動で変更する間隔
認証後の操作 (Post authentication actions)	管理アカウントのパスワードが使われた後の動作: パスワードのリセット、リセットしてログオフ (CSP の既定)、リセットして再起動など。実行までの待ち時間 (PostAuthenticationResetDelay) も設定できる。いつ・何をするかは文書によって書き方が違い、Intune の概要のページは「パスワードの期限が切れた時」「電源を切る」と書き、CSP のページは「認証の後、猶予期間が過ぎた時」「再起動」と書く

[^c1-40][^c1-41]

間違えやすい点が5つあります。1つ目は、管理できるアカウントがデバイスあたり1つだけという点です。ポリシーで管理するアカウントを別のアカウントに変えると、前のアカウントは LAPS の管理から外れ、その情報は管理センターとディレクトリから見えなくなります。2つ目は、Entra 参加なのに保存先を Active Directory にしても、LAPS は成功しないことです。デバイスは設定を受け取りますが、使えません。3つ目は、競合です。LAPS の CSP は設定ごとに1つの構成しか持てないので、競合する2つのポリシーが届くと処理を完了できません。4つ目は、他の LAPS 設定との関係です。Intune の CSP ポリシーは、グループ ポリシーや従来の Microsoft LAPS の設定より優先されます。5つ目は、存在しない名前のアカウントを指定した場合です。Windows 11 23H2 以前では、何も起きません。エラーも出ません。Windows 11 24H2 以降の自動アカウント管理モードなら、アカウントを作らせることができます。[^c1-40]

手動でパスワードを変更すると、次の自動変更までの日数の数え直しが始まります。たとえば PasswordAgeDays が10日で、3月1日に受け取り、3月5日に管理者が手動で変更したとします。次の自動変更は、3月11日ではなく、3月15日になります。[^c1-40]

パスワードを見られるルールは権限で決まり、パスワードの読み取りには `microsoft.directory/deviceLocalCredentials/password/read` が必要です。この権限を持つ組み込みルールは、Cloud Device Administrator と Intune Administrator です。メタデータ（デバイス名や最後の変更の日時など）だけなら `standard/read` で足り、Security Reader や Helpdesk Administrator も見られます[^c1-40]。Intune の管理センターでパスワードを表示するか手動でローテーションするには、Intune の権限が3つ要ります。Managed devices の Read、Organization の Read、Remote tasks の Rotate Local Admin Password の3つです。この Rotate の権限は、Intune の組み込みルールにも Intune Administrator にも含まれません。カスタム ロールで割り当てます。AD にバックアップした場合は、管理センターにパスワードは表示されません。[^c1-39][^c1-40]

LAPS ポリシーを作る権限は、Security baselines カテゴリの権限で、既定では Endpoint Security Manager に含まれます。割り当てはデバイスのグループが推奨されます。[^c1-40]

監査は、Entra 管理センターの Devices > Overview > Audit logs で行います。検索するアクティビティは、Update device local administrator password と Recover device local administrator password です。パスワードの変更の記録が Update、パスワードの取り出し(回復)の記録が Recover です。Entra のデバイスを削除すると、そのデバイスの LAPS の資格情報も失われ、復元の方法はありません。無効にしたデバイスは、パスワードの変更とバックアップが行われません。[^c1-39][^c1-40]

Intune によるローカル グループのメンバーシップ管理 [1.3.8]

Windows デバイスの組み込みのローカル グループ (Administrators など) のメンバーを、Intune で追加、削除、置き換えられます。設定は Endpoint security > Account protection の「Local user group membership」プロファイルです。対象は Windows 10 20H2 以降と Windows 11 です。[^c1-42]

対象にできるローカル グループは、ログオン時に評価される6つの組み込みグループに限られます。Administrators、Users、Guests、Power Users、Remote Desktop Users、Remote Management Users です。操作 (Group and user action) は3つあります。

操作	動作
Add (Update)	指定したメンバーを追加する。指定していない既存のメンバーは変わらない
Remove (Update)	指定したメンバーを削除する。ほかは変わらない
Add (Replace)	指定外のメンバーをすべて削除して、指定したメンバーに置き換える。制限付きグループ (Restricted Group) と同じ働き

[^c1-42]

メンバーの選び方は2つです。Users は Entra のユーザーやグループを選ぶ方法で、Entra 参加のデバイスだけに使えます。Manual は SID やアカウント名を手で入れる方法で、Entra 参加とハイブリッド参加の両方に使えます。Entra のグループを配った場合、リモート デスクトップの接続には適用されません。Entra 参加のデバイスでリモート デスクトップの権限を制御するには、個々のユーザーの SID を適切なグループに追加します。[^c1-42]

同じグループに Replace と Update の両方を設定すると、Replace が優先され、競合とは扱われません。ポリシーの間で別の競合が起きると、その設定はデバイスに送られず、管理センターに競合が報告されます。プロファイルは、Policy CSP の LocalUsersAndGroups を使います。[^c1-42]

使い分けは目的で決まります。Administrators グループを、決めたメンバーだけに固定したいなら、使うのは Add (Replace) で、Add (Update) ではありません。ヘルプ デスクの担当者を、既存の管理者を消さずに足したい時は Add (Update) を選びます。1.1.2 で扱った Additional local administrators は、Entra 参加のデバイスすべてに作用するテナント全体の設定です。このプロファイルなら、配る対象をグループ単位で絞れます。

サンプルはここまでです

続き(第2章～巻末)は、MD-102 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

MD-102 学習用テキスト(無料サンプル)

版

2026年10月版(MD-102 出題範囲(Skills measured)2026-10-27版 準拠)

発行

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

お問い合わせ

info@shikaku-doujou.com

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

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

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