TenantSnap

Microsoft Intune

# Intune 構成設計書（サンプル）

サンプル株式会社 情報システム部

発行者: TenantSnap

エクスポート日時: 2026年8月22日 18:10（JST）

Microsoft Graph API より自動生成

本書の記載範囲について

- 本書は Microsoft Intune から取得できる情報をもとに自動作成しています。
- テンプレート形式のプロファイルでは各設定の「現在の値」のみを記載し、既定値そのものは表示していません（Microsoft の仕様による制限です）。
- 設定カタログ・エンドポイントセキュリティでは、管理者が設定した項目を Microsoft 提供の説明とともに記載しています。

# 目　次

# 概要（構成サマリ）

この設計書に含まれる主な設定の件数をまとめたものです。件数のみを示し、設定の良し悪しの評価は行いません。詳しい内容は各章をご覧ください。

| 項目 | 件数 |
|---|---|
| 条件付きアクセスポリシー | 1 件 |
| コンプライアンスポリシー | 4 件 |
| 設定カタログ / エンドポイントセキュリティ | 0 件 |
| デバイス構成プロファイル | 7 件 |
| アプリ | 3 件 |
| グループ | 3 件 |
| 割り当てフィルター | 3 件 |

# 第1部 共通設定

## 1. ライセンス管理

| SKU | 状態 | 購入数 | 割り当て済み | 残数 | 停止/警告 |
|---|---|---|---|---|---|
| SPB | 有効 | 1 | 1 | 0 | |

## 2. 条件付きアクセスポリシー

| ポリシー名 | 状態 |
|---|---|
| [TenantSnap-Seed] 条件付きアクセス（無効・サンプル） | 無効 |

■ [TenantSnap-Seed] 条件付きアクセス（無効・サンプル） の詳細

| 項目 | 内容 |
|---|---|
| 状態 | 無効 |
| 対象ユーザー | 含む: なし |
| 対象アプリ | 含む: すべてのクラウドアプリ |
| クライアントアプリ | すべて |
| 許可制御 | 多要素認証（MFA） |

※ グループ・名前付き場所・組み込みロール・主なクラウドアプリは名称で表示します。個別ユーザー名は、ディレクトリの読み取り権限（User.Read.All）が付与されている場合に名称で表示します（未付与・カスタムアプリ・解決できなかった対象は ID（GUID）で表示されます）。

## 3. 名前付き場所（Named Locations）

| 名前 | 種別 | 信頼 | 対象（IP 範囲 / 国・地域） |
|---|---|---|---|
| [TenantSnap-Seed] 本社ネットワーク（名前付き場所・サンプル） | IP 範囲 | 信頼なし | 203.0.113.0/24 |

## 4. デバイス登録設定

### 登録構成

| 設定名 | 種別 | 優先度 | 割当先 |
|---|---|---|---|
| All users and all devices | デバイス登録数の制限 | 0 | 全デバイス |
| All users and all devices | プラットフォーム登録制限 | 0 | 全デバイス |

| 設定名 | 種別 | 優先度 | 割当先 |
|---|---|---|---|
| All users and all devices | 登録状態ページ（ESP） | 0 | 全デバイス |
| All users and all devices | Windows Hello for Business 設定 | 0 | 全デバイス |
| All users and all devices | | 0 | 全デバイス |

※ この表は、各設定の「現在の値」を記載しています。その値が初期値（既定値）のままか、管理者が設定した値かは区別していません。また、各設定の既定値そのものは表示していません（Microsoft の仕様による制限のためです）。どの設定を意図的に構成したかを確認するには、Intune 管理センターの該当プロファイルをご参照ください。設定項目名と値は、よく使われるものを日本語で表示しています。訳語を用意していないものや、Microsoft が日本語の名称を提供していない設定（ADMX 形式の管理用テンプレートを取り込んだ設定など）は、誤った訳を出さないため英語のまま表示します。「未構成」と表示される設定は、このプロファイルでは制御していません。「いいえ」または「未構成」だった設定は、設定されている項目が読み取りにくくなるため、表のあとに項目名をまとめて記載しています。

### ■ All users and all devices の運用メモ（説明）

This is the default Device Limit Restriction applied with the lowest priority to all users regardless of group membership.

### ■ All users and all devices の設定値

| 設定項目 | 値 |
|---|---|
| priority | 0 |
| limit | 5 |
| 登録の構成の種類 | 登録台数の上限 |

### ■ All users and all devices の運用メモ（説明）

This is the default Device Type Restriction applied with the lowest priority to all users regardless of group membership.

### ■ All users and all devices の設定値

| 設定項目 | 値 |
|---|---|
| priority | 0 |
| iOS/iPadOS の登録制限 | platformBlocked: いいえ、personalDeviceEnrollmentBlocked: いいえ |
| Windows の登録制限 | platformBlocked: いいえ、personalDeviceEnrollmentBlocked: いいえ |
| Windows Mobile の登録制限 | platformBlocked: はい、personalDeviceEnrollmentBlocked: いいえ |
| Android（デバイス管理者）の登録制限 | platformBlocked: いいえ、personalDeviceEnrollmentBlocked: いいえ |

| 設定項目 | 値 |
|---|---|
| macOS の登録制限 | platformBlocked: いいえ、personalDeviceEnrollmentBlocked: いいえ |
| Android Enterprise の登録制限 | platformBlocked: いいえ、personalDeviceEnrollmentBlocked: いいえ |
| 登録の構成の種類 | プラットフォーム制限 |
| macOS の登録制限 | platformBlocked: いいえ、personalDeviceEnrollmentBlocked: いいえ |
| tvosRestriction | platformBlocked: いいえ、personalDeviceEnrollmentBlocked: いいえ |
| visionOSRestriction | platformBlocked: いいえ、personalDeviceEnrollmentBlocked: いいえ |
| Windows Home エディションの登録制限 | platformBlocked: いいえ、personalDeviceEnrollmentBlocked: いいえ |

### ■ All users and all devices の運用メモ（説明）

This is the default enrollment status screen configuration applied with the lowest priority to all users and all devices regardless of group membership.

### ■ All users and all devices の設定値

| 設定項目 | 値 |
|---|---|
| priority | 0 |
| 利用者による設定のやり直しを禁止する | はい |
| 登録の構成の種類 | 登録状態ページ |
| インストール状況を表示する最大時間（分） | 0 |

「いいえ」または「未構成」だった設定（8 件）：アプリのインストール完了を待たずに進める、インストール失敗時に端末のリセットを許可する、インストール失敗時に端末の利用を許可する、インストール失敗時のログ収集を許可する、2人目以降の利用者の状況追跡を無効にする、品質更新プログラムをインストールする、showInstallationProgress、trackInstallProgressForAutopilotOnly

### ■ All users and all devices の運用メモ（説明）

This is the default Windows Hello for Business configuration applied with the lowest priority to all users regardless of group membership.

### ■ All users and all devices の設定値

| 設定項目 | 値 |
|---|---|
| priority | 0 |

| 設定項目 | 値 |
|---|---|
| PIN の最小文字数 | 6 |
| PIN の最大文字数 | 127 |
| PIN に大文字を使う | 使用しない |
| PIN に小文字を使う | 使用しない |
| PIN に記号を使う | 使用しない |
| unlockWithBiometricsEnabled | はい |
| remotePassportEnabled | はい |
| 再利用を禁止する過去の PIN の数 | 0 |
| PIN の有効期限（日） | 0 |
| 登録の構成の種類 | Windows Hello for Business |
| サインインのセキュリティ強化 | 0 |

「いいえ」または「未構成」だった設定（4 件）：state、Windows Hello の利用に TPM を必須にする、顔認証のなりすまし対策（拡張生体認証）、サインイン用セキュリティ キーの利用

### ■ All users and all devices の運用メモ（説明）

This is the default Windows Restore configuration applied with the lowest priority to all users and all devices regardless of group membership.

### ■ All users and all devices の設定値

| 設定項目 | 値 |
|---|---|
| priority | 0 |
| 登録の構成の種類 | Windows バックアップと復元 |

## 利用規約（Terms and Conditions）

| 規約名 | タイトル | バージョン |
|---|---|---|
| [TenantSnap-Seed] 利用規約（サンプル） | 利用規約（検証用サンプル） | 1 |

## デバイスカテゴリ

| カテゴリ名 | 説明 |
|---|---|
| [TenantSnap-Seed] 営業部端末（デバイスカテゴリ・サンプル） | 【意図】端末を用途・部門別に分類し、棚卸しと割り当ての絞り込みを容易にする。<br>【確認】登録時のカテゴリ選択を必須にするかは別途検討。 |

## 企業デバイス識別子（コーポレート識別子）

※ 会社所有のデバイスを事前に登録しておくための識別子（IMEI やシリアル番号）の一覧です。ここに登録された端末は、登録時に会社所有として扱われます。

登録されていません

### 登録済みデバイス（台帳）

※ Intune に登録され管理されている端末の台数と内訳です（設計書を作成した時点の状態）。端末ごとの明細（デバイス名・利用者・シリアル番号）は、「登録済みデバイスの明細を出力する」がオンのとき付録 K に掲載します。

登録されていません

## 5. グループ

| グループ名 | 種類 | メールアドレス | メンバーシップ | 説明 |
|---|---|---|---|---|
| パキケトゥス | Microsoft 365 | msteams_●●●●●●@●●●●●●●.onmicrosoft.com | 割り当て | |
| Group for Answers in Viva Engage – DO NOT DELETE 175983198208 | Microsoft 365 | groupforanswersinvivaengagedonotdelete●●●●●●●●●●●●●●●●@●●●●●●●.onmicrosoft.com | 割り当て | Group that stores content and metadata for Answers in Viva Engage in network 175983198208. Deleting this this group will disrupt Answers in Viva Engage. |
| All Company | Microsoft 365 | allcompany@●●●●●●●.onmicrosoft.com | 割り当て | This is the default group for everyone in the network |

## 6. 割り当てフィルター

| フィルター名 | プラットフォーム | ルール |
|---|---|---|
| [TenantSnap-Seed] 割り当てフィルター（Android・サンプル） | Android | (device.model -eq "Android") |
| [TenantSnap-Seed] 割り当てフィルター（iOS・サンプル） | iOS/iPadOS | (device.model -contains "iPhone") |
| [TenantSnap-Seed] 割り当てフィルター（サンプル） | Windows 10 以降 | (device.manufacturer -eq "Contoso") |

## 7. アプリ保護ポリシー（MAM）

| ポリシー名 | プラットフォーム | 割当先 |
|---|---|---|
| [TenantSnap-Seed] アプリ保護（iOS・サンプル） | iOS | 未割り当て |
| [TenantSnap-Seed] アプリ保護（Android・サンプル） | Android | 未割り当て |

※ この表は、各設定の「現在の値」を記載しています。その値が初期値（既定値）のままか、管理者が設定した値かは区別していませ

ん。また、各設定の既定値そのものは表示していません（Microsoft の仕様による制限のためです）。どの設定を意図的に構成したかを確認するには、Intune 管理センターの該当プロファイルをご参照ください。設定項目名と値は、よく使われるものを日本語で表示しています。訳語を用意していないものや、Microsoft が日本語の名称を提供していない設定（ADMX 形式の管理用テンプレートを取り込んだ設定など）は、誤った訳を出さないため英語のまま表示します。「未構成」と表示される設定は、このプロファイルでは制御していません。「いいえ」または「未構成」だった設定は、設定されている項目が読み取りにくくなるため、表のあとに項目名をまとめて記載しています。

### ■ [TenantSnap-Seed] アプリ保護（iOS・サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | 私用 iPhone（BYOD）でも業務データを保護するため、PIN 必須・管理アプリ間のみコピー許可とする。 |
| 戻し方 | ポリシー解除で制限解除。 |
| 確認 | 個人データには触れない（MAM のみ）ことを利用者へ周知。 |

### ■ [TenantSnap-Seed] アプリ保護（iOS・サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| オフラインのままアクセスを許す時間 | PT1M |
| オンラインでアクセス条件を再確認する間隔 | PT1M |
| 受け取りを許可するデータの送信元 | すべてのアプリ |
| 送信を許可するデータの送信先 | 管理対象アプリのみ |
| クリップボードの共有を許可する範囲 | すべてのアプリ |
| オフラインのまま経過したらデータを消去する期間 | P1D |
| PIN を必須にする | はい |
| PIN の入力を許可する回数 | 5 |
| PIN の最小文字数 | 4 |
| PIN に使える文字の種類 | 数字のみ |
| PIN の再設定を求めるまでの期間 | PT0S |
| アプリのデータの暗号化方法 | デバイスの設定に従う |
| deployedAppCount | 0 |
| クリップボードで例外的に共有できる文字数 | 0 |
| 端末が準拠していないときの動作 | アクセスをブロック |
| 許可されていない iOS 端末の機種のときの動作 | アクセスをブロック |
| PIN の入力回数を超えたときの動作 | アクセスをブロック |
| 対象にするアプリの種類 | 選択したアプリ |
| dialerRestrictionLevel | すべてのアプリ |
| 対象から除外するアプリ（プロトコル） | name: Default、value: skype;app- |

| 設定項目 | 値 |
| --- | --- |
| | settings;calshow;itms;itmss;itms-apps;itms-appss;itms-services; |
| 対象から除外するユニバーサル リンク | http://maps.apple.com、https://maps.apple.com、http://facetime.apple.com、https://facetime.apple.com |
| 管理対象のユニバーサル リンク | http://*.sharepoint.com/*、http://*.sharepoint-df.com/*、http://*.yammer.com/*、http://*.onedrive.com/*、http://tasks.office.com/*、http://to-do.microsoft.com/sharing*、http://web.microsoftstream.com/video/*、http://msit.microsoftstream.com/video/*、http://*.powerbi.com/*、http://app.powerbi.cn/*、http://app.powerbigov.us/*、http://app.powerbi.de/*、http://*.service-now.com/*、http://*.appsplatform.us/*、http://*.powerapps.cn/*、http://*.powerapps.com/*、http://*.powerapps.us/*、http://*teams.microsoft.com/l/*、http://*devspaces.skype.com/l/*、http://*teams.live.com/l/*、http://*collab.apps.mil/l/*、http://*teams.microsoft.us/l/*、http://*teams-fl.microsoft.com/l/*、http://*.zoom.us/*、http://zoom.us/*、https://*.sharepoint.com/*、https://*.sharepoint-df.com/*、https://*.yammer.com/*、https://*.onedrive.com/*、https://tasks.office.com/*、https://to-do.microsoft.com/sharing*、https://web.microsoftstream.com/video/*、https://msit.microsoftstream.com/video/*、https://*.powerbi.com/*、https://app.powerbi.cn/*、https://app.powerbigov.us/*、https://app.powerbi.de/*、https://*.service-now.com/*、https://*.appsplatform.us/*、https://*.powerapps.cn/*、https://*.powerapps.com/*、https://*.powerapps.us/*、https://*teams.microsoft.com/l/*、https://*devspaces.skype.com/l/*、https:// |

| 設定項目 | 値 |
|---|---|
| | *teams.live.com/l/*、https://*collab.apps.mil/l/*、https://*teams.microsoft.us/l/*、https://*teams-fl.microsoft.com/l/*、https://*.zoom.us/*、https://zoom.us/* |
| モバイル脅威対策で条件を満たさないときの動作 | アクセスをブロック |
| notificationRestriction | 許可 |
| 再利用を禁止する過去の PIN の数 | 0 |
| protectedMessagingRedirectAppType | すべてのアプリ |
| purviewContentEvaluationRequired | notRequired |
| targetedAppManagementLevels | 指定なし |

「いいえ」または「未構成」だった設定（20 件）：組織の資格情報でのサインインを必須にする、データのバックアップを禁止する、端末が準拠していることを必須にする、リンクを管理対象のブラウザーで開くことを必須にする、名前を付けて保存を禁止する、単純な PIN を禁止する、連絡先の同期を禁止する、印刷を禁止する、指紋認証を禁止する、端末に PIN があればアプリの PIN を求めない、リンクを開くブラウザー、isAssigned、Face ID を禁止する、ウィジェットの内容の同期を許可する、組織の文書への外部データの取り込みを禁止する、管理対象データの送信時の保護を無効にする、共有先を管理対象アプリだけに絞る、許容する端末の脅威レベルの上限、提供元不明のデータの取り込みを保護する、サード パーティー製キーボードを禁止する

### ■ [TenantSnap-Seed] アプリ保護（Android・サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | 私用 Android（BYOD）の業務データ保護。PIN 必須・管理アプリ間のみコピー許可。 |
| 戻し方 | ポリシー解除で制限解除。 |

### ■ [TenantSnap-Seed] アプリ保護（Android・サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| オフラインのままアクセスを許す時間 | PT1M |
| オンラインでアクセス条件を再確認する間隔 | PT1M |
| 受け取りを許可するデータの送信元 | すべてのアプリ |
| 送信を許可するデータの送信先 | 管理対象アプリのみ |
| クリップボードの共有を許可する範囲 | すべてのアプリ |
| オフラインのまま経過したらデータを消去する期間 | P1D |
| PIN を必須にする | はい |
| PIN の入力を許可する回数 | 5 |
| PIN の最小文字数 | 4 |
| PIN に使える文字の種類 | 数字のみ |
| PIN の再設定を求めるまでの期間 | PT0S |

| 設定項目 | 値 |
|---|---|
| deployedAppCount | 0 |
| 必要な Android セキュリティ パッチの最低バージョン | 0000-00-00 |
| 警告を出す Android セキュリティ パッチのバージョン | 0000-00-00 |
| クリップボードで例外的に共有できる文字数 | 0 |
| 許可されていない製造元のときの動作 | アクセスをブロック |
| 許可されていない Android 端末の機種のときの動作 | アクセスをブロック |
| アプリの確認に失敗したときの動作 | アクセスをブロック |
| 端末の構成証明に失敗したときの動作 | アクセスをブロック |
| 端末が準拠していないときの動作 | アクセスをブロック |
| 端末にロックが設定されていないときの動作 | アクセスをブロック |
| PIN の入力回数を超えたときの動作 | アクセスをブロック |
| 対象にするアプリの種類 | 選択したアプリ |
| ポータル サイトの更新を待てる日数 | 0 |
| dialerRestrictionLevel | すべてのアプリ |
| 対象から除外するアプリ（パッケージ） | name: Default |
| データを消去する Android セキュリティ パッチのバージョン | 0000-00-00 |
| モバイル脅威対策で条件を満たさないときの動作 | アクセスをブロック |
| notificationRestriction | 許可 |
| 再利用を禁止する過去の PIN の数 | 0 |
| protectedMessagingRedirectAppType | すべてのアプリ |
| purviewContentEvaluationRequired | notRequired |
| Play Integrity のアプリ確認の種類 | 要求しない |
| Play Integrity の端末構成証明の種類 | 要求しない |
| requiredAndroidSafetyNetEvaluationType | 基本 |
| targetedAppManagementLevels | 指定なし |
| warnAfterCompanyPortalUpdateDeferralInDays | 0 |
| wipeAfterCompanyPortalUpdateDeferralInDays | 0 |

「いいえ」または「未構成」だった設定（23 件）：組織の資格情報でのサインインを必須にする、データのバックアップを禁止する、端末が準拠していることを必須にする、リンクを管理対象のブラウザーで開くことを必須にする、名前を付けて保存を禁止する、単純な PIN を禁止する、連絡先の同期を禁止する、印刷を禁止する、指紋認証を禁止する、端末に PIN があればアプリの PIN を求めない、リンクを開くブラウザー、isAssigned、画面のキャプチャを禁止する、端末が暗号化されていればアプリの暗号化を行わない、アプリのデータを暗号化する、生体認証を禁止する、組織の文書への外部データの取り込みを禁止する、起動時に VPN へ接続する、端末のロックを必須にする、利用できるキーボードを制限する、許容する端末の脅威レベルの上限、クラス3の生体認証を必須にする、生体認証を変更したあとに PIN を要求する

## 8. アプリ構成ポリシー

（データなし）

# 第2部 テナント管理

## 9. ロール・スコープタグ

### スコープタグ

| 名前 | 説明 |
|---|---|
| Default | Default Role Scope Tag. This will exist by default on all Intune entities whenever a user defined Role Scope Tag is not present. |
| [TenantSnap-Seed] 営業部（スコープタグ・サンプル） | 【意図】部門ごとに管理対象を分離（RBAC）し、担当者が自部門のみを操作できるようにする。【責任者】情報システム部 管理者 |

### ロール定義

| ロール名 | 種類 | 説明 |
|---|---|---|
| Policy and Profile manager | 組み込み | Policy and Profile Managers manage compliance policy, configuration profiles, Apple enrollment, Android Enterprise enrollment profiles and corporate device identifiers. |
| School Administrator | 組み込み | School Administrators can manage apps and settings for their groups. They can take remote actions on devices, including remotely locking them, restarting them, and retiring them from management. |
| Multi Admin Approval Policy Manager | 組み込み | Multi Admin Approval Policy Manager can manage the access policies that configure Multi-admin approval including approving changes to existing policy or creating new access policies. |
| Endpoint Privilege Reader | 組み込み | Endpoint Privilege Readers can view Endpoint Privilege Management (EPM) policies in |

| ロール名 | 種類 | 説明 |
|---|---|---|
| | | the Intune console. |
| Help Desk Operator | 組み込み | Help Desk Operators perform remote tasks on users and devices and can assign applications or policies to users or devices. |
| Application Manager | 組み込み | Application Managers manage mobile and managed applications, can read device information and can view device configuration profiles. |
| Endpoint Security Manager | 組み込み | Manages security and compliance features such as security baselines, device compliance, conditional access, and Microsoft Defender ATP. |
| Endpoint Privilege Manager | 組み込み | Endpoint Privilege Managers can manage Endpoint Privilege Management (EPM) policies in the Intune console. |
| Read Only Operator | 組み込み | Read Only Operators view user, device, enrollment, configuration and application information and cannot make changes to Intune. |
| Intune Role Administrator | 組み込み | Intune Role Administrators manage custom Intune roles and add assignments for built-in Intune roles. It is the only Intune role that can assign permissions to Administrators. |

### ロール割り当て

（データなし）

## 10. 証明書（Cloud PKI）

（データなし）

## 11. 通知テンプレート

| テンプレート名 | 既定のロケール | ブランド設定 |
|---|---|---|

| テンプレート名 | 既定のロケール | ブランド設定 |
|---|---|---|
| [TenantSnap-Seed] 通知テンプレート（サンプル） | | includeCompanyName |

## 12. 接続コネクタ・パートナー連携

※ 証明書コネクタ（NDES）・Mobile Threat Defense（MTD）コネクタ・パートナー連携（コンプライアンス／デバイス管理パートナー＝Jamf 等）の接続状態を記載します。オンプレミスの証明書発行や外部サービスとの連携の有無・状態を確認できます。

### 証明書コネクタ（NDES）

構成されていません

### Mobile Threat Defense（MTD）コネクタ

構成されていません

### コンプライアンス パートナー（Jamf 等）

| パートナー | 接続状態 | iOS | Android | macOS | 最終ハートビート |
|---|---|---|---|---|---|
| Relution | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| Mosyle Onek12 | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| MobileIron Device Compliance Cloud | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| CLOMO MDM | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| SureMDM | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| Workspace ONE Conditional Access | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| ArborXR | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| baramundi EMM | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| Mosyle Fuse | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| mobiconnect | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| Scalefusion | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| midpoints mobile.profiler | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |

| パートナー | 接続状態 | iOS | Android | macOS | 最終ハートビート |
|---|---|---|---|---|---|
| Addigy | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| Jamf Device Compliance | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| 7P Conditional Access | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| IBM MaaS360 | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| Citrix Workspace Device Compliance | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| AppTec360 Endpoint Manager | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| SOTI MobiControl | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| MobileIron Device Compliance On-prem | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| Kandji Device Compliance | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| Fleet | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| Hexnode UEM | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |
| BlackBerry UEM Azure Conditional Access | 不明 | 無効 | 無効 | 無効 | 1年1月1日 09:18（JST） |

### デバイス管理パートナー

| パートナー | 接続状態 | 種別 | 構成済み | 最終ハートビート |
|---|---|---|---|---|
| Jamf | 不明 | singleTenantApp | 無効 | 1年1月1日 09:18（JST） |

### リモート支援コネクタ（Remote Help / TeamViewer）

| パートナー | 接続状態 | 最終接続 |
|---|---|---|
| TeamViewerV2 | notOnboarded | 10000年1月1日 08:59（JST） |
| TeamViewer | notOnboarded | 1970年1月1日 09:00（JST） |

## 13. 多段階管理者承認（Multi Admin Approval）

※ 重要な操作（アプリ・スクリプト・ロール等の変更）に、別の管理者による承認を必須にする設定です。対象の操作種別と、承認で

きる管理者グループを記載します。

構成されていません

## 14. ポリシーセット

※ ポリシーセットは、構成プロファイルやアプリなどを1つにまとめて割り当てる単位です。セットの名称・状態を記載します（各項目の詳細は該当の章に記載しています）。

構成されていません

## 15. その他の管理設定

### カスタム コンプライアンス スクリプト（Windows）

構成されていません

### アプリ カテゴリ

| カテゴリ名 | 最終更新 |
|---|---|
| Data Management | 1年1月1日 09:18（JST） |
| Other Apps | 1年1月1日 09:18（JST） |
| Business | 1年1月1日 09:18（JST） |
| Photos & Media | 1年1月1日 09:18（JST） |
| Development & Design | 1年1月1日 09:18（JST） |
| Computer Management | 1年1月1日 09:18（JST） |
| Productivity | 1年1月1日 09:18（JST） |
| Books & Reference | 1年1月1日 09:18（JST） |
| Collaboration & Social | 1年1月1日 09:18（JST） |

### デバイスのクリーンアップ規則（非アクティブの自動削除）

※ 一定の日数 Intune に接続していないデバイスを自動的に削除する設定です。未設定または 0 日の場合、自動削除は行われません。

取得不可（Microsoft Intune 側で許可されていません）

# 第3部 Windows

## 16. デバイス構成プロファイル（Windows）

### 構成プロファイル

| プロファイル名 | 種別 | 説明 | 割当先 |
|---|---|---|---|
| [TenantSnap-Seed] Windows スタート メニュー レイアウト（サンプル） | Windows 一般設定 | 【意図】共用 PC のスタート メニューを業務アプリのタイルだけに固定し、利用者が並びを変えられないようにする。【戻し方】本プロファイルの割り当てを解除すると既定のスタート メニューに戻る。【確認】レイアウト XML は LayoutModification スキーマに従う。【責任者】情報システム部 端末管理チーム | 未割り当て |
| [TenantSnap-Seed] Windows デバイス構成（サンプル） | Windows 一般設定 | 【意図】社用 Windows 端末に最低限のパスワード要件（8文字以上・簡単なPIN禁止）を課し、無人放置時のリスクを下げる。【戻し方】本プロファイルの割り当てを解除すれば従来動作に戻る。【確認】既存ユーザーのサインインに影響しないことを検証済み。【責任者】情報システム部 端末管理チーム | パキケトゥス |

※ この表は、各設定の「現在の値」を記載しています。その値が初期値（既定値）のままか、管理者が設定した値かは区別していません。また、各設定の既定値そのものは表示していません（Microsoft の仕様による制限のためです）。どの設定を意図的に構成したかを確認するには、Intune 管理センターの該当プロファイルをご参照ください。設定項目名と値は、よく使われるものを日本語で表示しています。訳語を用意していないものや、Microsoft が日本語の名称を提供していない設定（ADMX 形式の管理用テンプレートを取り込んだ設定など）は、誤った訳を出さないため英語のまま表示します。「未構成」と表示される設定は、このプロファイルでは制御していません。「いいえ」または「未構成」だった設定は、設定されている項目が読み取りにくくなるため、表のあとに項目名をまとめて記載しています。

#### ■ [TenantSnap-Seed] Windows スタート メニュー レイアウト（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | 共用 PC のスタート メニューを業務アプリ |

| 項目 | 内容 |
|---|---|
| | のタイルだけに固定し、利用者が並びを変えられないようにする。 |
| 戻し方 | 本プロファイルの割り当てを解除すると既定のスタート メニューに戻る。 |
| 確認 | レイアウト XML は LayoutModification スキーマに従う。 |
| 責任者 | 情報システム部 端末管理チーム |

### ■ [TenantSnap-Seed] Windows スタート メニュー レイアウト（サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| パスワードの種類 | デバイスの既定（種類を指定しません） |

「いいえ」または「未構成」だった設定（225 件）：プロキシ設定を端末全体に適用する、プロキシの自動検出を無効にする、Bluetooth のアドバタイズを禁止する、Bluetooth の検出可能モードを禁止する、Bluetooth の事前ペアリングを禁止する、Edge の自動入力を禁止する、Edge の利用を禁止する、Edge の Cookie の扱い、Edge の開発者ツールを禁止する、Edge の「追跡しない」要求の送信を禁止する、Edge の拡張機能を禁止する、Edge の InPrivate 閲覧を禁止する、Edge の JavaScript を禁止する、Edge のパスワード マネージャーを禁止する、Edge のアドレス バーの候補表示を無効にする、Edge の互換性リストの利用を禁止する、Edge の終了時に閲覧データを消去する、Edge のスタート ページの変更を許可する、Edge の初回起動ページを表示しない、Edge のライブ タイル用データ収集を禁止する、お気に入りを Internet Explorer と同期する、ローミング中のデータ通信を禁止する、モバイル通信での VPN を禁止する、ローミング中の VPN を禁止する、リアルタイム監視を必須にする、動作の監視を必須にする、ネットワーク検査システムを必須にする、ダウンロードしたファイルを検査する、Internet Explorer で読み込むスクリプトを検査する、利用者に Defender の画面を表示しない、ファイルの動きを監視する、圧縮ファイルを検査する、受信メールを検査する、フル スキャンでリムーバブル ドライブも検査する、フル スキャンでネットワーク ドライブも検査する、ネットワーク上のファイルを検査する、クラウド保護を必須にする、クラウド保護のブロック レベル、サンプル送信時に確認する、検査の種類、システム検査のスケジュール、画面がロックされるまでの時間の変更を許可する、ロック画面にアクション センターの通知を出さない、ロック画面で Cortana を使わせない、ロック画面にトースト通知を出さない、単純なパスワードを禁止する、パスワードを必須にする、スリープからの復帰時にパスワードを要求する、広告 ID の利用、ペアリングと同意の確認を自動で承諾する、入力候補の個人用設定を禁止する、検索で発音区別記号を使わせない、検索の言語の自動判定を無効にする、暗号化された項目を検索インデックスに含めない、リモートからの検索を許可する、インデックス作成の一時停止を無効にする、リムーバブル ドライブをインデックスに含めない、インデックスのサイズを自動で管理する、設定アプリを開かせない、設定の「システム」を開かせない、設定の「デバイス」を開かせない、設定の「ネットワークとインターネット」を開かせない、設定の「個人用設定」を開かせない、設定の「アカウント」を開かせない、設定の「時刻と言語」を開かせない、設定の「簡単操作」を開かせない、設定の「プライバシー」を開かせない、設定の「更新とセキュリティ」を開かせない、設定の「アプリ」を開かせない、設定の「ゲーム」を開かせない、SmartScreen のアプリ インストール制御を有効にする、タスク バーからのピン留め解除を禁止する、スタート メニューのアプリ一覧の表示、スタート メニューの「アカウント設定の変更」を隠す、よく使うアプリを隠す、スタート メニューの「休止状態」を隠す、スタート メニューの「ロック」を隠す、スタート メニューの電源ボタンを隠す、最近使った項目（ジャンプ リスト）を隠す、最近追加したアプリを隠す、スタート メニューの「再起動」を隠す、スタート メニューの「シャットダウン」を隠す、スタート メニューの「サインアウト」を隠す、スタート メニューの「スリープ」を隠す、スタート メニューの「アカウントの切り替え」を隠す、スタート メニューのユーザー アイコンを隠す、スタート メニューの表示モード、スタート メニューに「ドキュメント」を表示する、スタート メニューに「ダウンロード」を表示する、スタート メニューに「エクスプローラー」を表示する、スタート メニューに「ホームグループ」を表示する、スタート メニューに「ミュージック」を表示する、スタート メニューに「ネットワーク」を表示する、スタート メニューに「個人用フォルダー」を表示する、スタート メニューに「ピクチャ」を表示する、スタート メニューに「設定」を表示する、スタート メニューに「ビデオ」を表示する、diagnosticsDataSubmissionMode、OneDrive のファイル同期を無効にする、消費者向け機能の表示を禁止する、Windows スポットライトを禁止する、アクション センターでのスポットライトを禁止する、カスタマイズされた表示を禁止する、サード パーティーの通知を禁止する、ようこそ画面の表示を禁止する、Windows のヒントの表示を禁止する、ロック画面の Windows スポットライト、Microsoft アカウント以外のメール追加を禁止する、盗難防止モードを禁止する、Bluetooth を禁止する、カメラを禁止する、接続されたデバイス サービスを禁止する、ルート証明書の手動インストールを禁止する、コピーと貼り付けを禁止する、Cortana を禁止する、端末からの初期化を禁止する、利用者による登録解除を禁止する、セーフ サーチの強さ、Edge のポップアップを禁止する、Edge の検索候補を禁止する、イントラネット サイトを Internet Explorer で開かない、イントラネット サイトを Internet Explorer で開く、

Edge で SmartScreen を必須にする、Edge の about:flags ページを開かせない、SmartScreen の警告を無視できないようにする、ファイルの SmartScreen 警告を無視できないようにする、WebRTC でのローカル IP アドレスの露出を禁止する、インターネット共有を禁止する、プロビジョニング パッケージの追加を禁止する、プロビジョニング パッケージの削除を禁止する、システム時刻の変更を禁止する、デバイス名の変更を禁止する、地域の変更を禁止する、言語の変更を禁止する、電源とスリープの変更を禁止する、位置情報サービスを禁止する、Microsoft アカウントの利用を禁止する、Microsoft アカウントの設定同期を禁止する、NFC を禁止する、リセット保護を禁止する、画面のキャプチャを禁止する、リムーバブル ストレージを禁止する、モバイル端末の暗号化を必須にする、USB を禁止する、音声の録音を禁止する、オープンなホットスポットへの自動接続を禁止する、Wi-Fi を禁止する、Wi-Fi の手動設定を禁止する、この端末への画面投影を禁止する、投影先からの操作を禁止する、ワイヤレス ディスプレイの接続に PIN を要求する、Microsoft Store を禁止する、信頼されたアプリのサイドロード、Microsoft Store アプリの自動更新を禁止する、開発者モードの利用、ユーザー間でアプリ データを共有する、Microsoft Store 由来のアプリを禁止する、プライベート ストアのみ利用できるようにする、アプリのデータをシステム ボリュームに限定する、アプリのインストール先をシステム ボリュームに限定する、ゲーム録画（ゲーム DVR）を禁止する、デバイスの検出を禁止する、SIM が無いときのエラー表示を禁止する、タスク スイッチャーを禁止する、ユーザーの簡易切り替えを禁止する、初期セットアップ中にネットワーク接続を必須にする、音声によるアプリの起動、MSI インストールの利用者による制御を許可する、MSI を常に昇格した権限でインストールする、別の端末からのサインインを許可する、Web サインインの利用、近くのデバイスからの Bluetooth 接続要求を禁止する、モバイル データの利用、FIPS 準拠のアルゴリズムを使う、アクセス時の保護を無効にする、実行できなかったフル スキャンの追いかけ実行を無効にする、実行できなかったクイック スキャンの追いかけ実行を無効にする、望ましくない可能性のあるアプリへの動作、スケジュール検査を低い CPU 優先度で実行する、Edge のお気に入りの編集を禁止する、Edge の全画面表示を禁止する、Edge の事前起動を禁止する、Edge からの印刷を禁止する、Edge の閲覧履歴の保存を禁止する、Edge の検索エンジンの変更を禁止する、Edge の拡張機能のサイドロードを禁止する、Edge のタブの事前読み込みを禁止する、Edge の新しいタブに Web コンテンツを表示しない、Edge のお気に入りバーの表示、Edge のホーム ボタンの構成を有効にする、Edge のキオスク モードの制限、Edge の起動時に開くページ、Edge で証明書エラーを無視できないようにする、Internet Explorer で開くときにメッセージを表示する、Microsoft 365 分析へのテレメトリ送信、自動再展開を有効にする、ブラウザーの設定を同期しない、ファイルの検索（Find My Files）、Windows Ink ワークスペースへのアクセス、Windows Ink ワークスペースの利用、Windows Ink の推奨アプリを表示しない、ロック画面で音声によるアプリの起動、MMS を禁止する、RCS を禁止する、メッセージの同期を禁止する、Microsoft アカウント サインイン アシスタント、電源ボタンの動作（バッテリー時）、電源ボタンの動作（電源接続時）、ハイブリッド スリープ（バッテリー時）、ハイブリッド スリープ（電源接続時）、カバーを閉じたときの動作（バッテリー時）、カバーを閉じたときの動作（電源接続時）、スリープ ボタンの動作（バッテリー時）、スリープ ボタンの動作（電源接続時）、プリンターの追加を禁止する、アクティビティの履歴を禁止する、アクティビティの公開を禁止する、初回起動時のプライバシー設定画面を表示しない、検索に Web の結果を含めない、検索で位置情報を使わせない、検索で位置情報を使わせない、Microsoft Entra 参加時の自動暗号化を禁止する、SmartScreen のアプリ インストール制御、タスク マネージャーからのタスク終了を禁止する、組み込みアプリをアンインストールする

### ■ [TenantSnap-Seed] Windows デバイス構成（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | 社用 Windows 端末に最低限のパスワード要件（8文字以上・簡単なPIN禁止）を課し、無人放置時のリスクを下げる。 |
| 戻し方 | 本プロファイルの割り当てを解除すれば従来動作に戻る。 |
| 確認 | 既存ユーザーのサインインに影響しないことを検証済み。 |
| 責任者 | 情報システム部 端末管理チーム |

### ■ [TenantSnap-Seed] Windows デバイス構成（サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| 単純なパスワードを禁止する | はい |
| パスワードの最小文字数 | 8 |
| パスワードを必須にする | はい |

| 設定項目 | 値 |
|---|---|
| パスワードの種類 | デバイスの既定（種類を指定しません） |

「いいえ」または「未構成」だった設定（223 件）：プロキシ設定を端末全体に適用する、プロキシの自動検出を無効にする、Bluetooth のアドバタイズを禁止する、Bluetooth の検出可能モードを禁止する、Bluetooth の事前ペアリングを禁止する、Edge の自動入力を禁止する、Edge の利用を禁止する、Edge の Cookie の扱い、Edge の開発者ツールを禁止する、Edge の「追跡しない」要求の送信を禁止する、Edge の拡張機能を禁止する、Edge の InPrivate 閲覧を禁止する、Edge の JavaScript を禁止する、Edge のパスワード マネージャーを禁止する、Edge のアドレス バーの候補表示を無効にする、Edge の互換性リストの利用を禁止する、Edge の終了時に閲覧データを消去する、Edge のスタート ページの変更を許可する、Edge の初回起動ページを表示しない、Edge のライブ タイル用データ収集を禁止する、お気に入りを Internet Explorer と同期する、ローミング中のデータ通信を禁止する、モバイル通信での VPN を禁止する、ローミング中の VPN を禁止する、リアルタイム監視を必須にする、動作の監視を必須にする、ネットワーク検査システムを必須にする、ダウンロードしたファイルを検査する、Internet Explorer で読み込むスクリプトを検査する、利用者に Defender の画面を表示しない、ファイルの動きを監視する、圧縮ファイルを検査する、受信メールを検査する、フル スキャンでリムーバブル ドライブも検査する、フル スキャンでネットワーク ドライブも検査する、ネットワーク上のファイルを検査する、クラウド保護を必須にする、クラウド保護のブロック レベル、サンプル送信時に確認する、検査の種類、システム検査のスケジュール、画面がロックされるまでの時間の変更を許可する、ロック画面にアクション センターの通知を出さない、ロック画面で Cortana を使わせない、ロック画面にトースト通知を出さない、スリープからの復帰時にパスワードを要求する、広告 ID の利用、ペアリングと同意の確認を自動で承諾する、入力候補の個人用設定を禁止する、検索で発音区別記号を使わせない、検索の言語の自動判定を無効にする、暗号化された項目を検索インデックスに含めない、リモートからの検索を許可する、インデックス作成の一時停止を無効にする、リムーバブル ドライブをインデックスに含めない、インデックスのサイズを自動で管理する、設定アプリを開かせない、設定の「システム」を開かせない、設定の「デバイス」を開かせない、設定の「ネットワークとインターネット」を開かせない、設定の「個人用設定」を開かせない、設定の「アカウント」を開かせない、設定の「時刻と言語」を開かせない、設定の「簡単操作」を開かせない、設定の「プライバシー」を開かせない、設定の「更新とセキュリティ」を開かせない、設定の「アプリ」を開かせない、設定の「ゲーム」を開かせない、SmartScreen のアプリ インストール制御を有効にする、タスク バーからのピン留め解除を禁止する、スタート メニューのアプリ一覧の表示、スタート メニューの「アカウント設定の変更」を隠す、よく使うアプリを隠す、スタート メニューの「休止状態」を隠す、スタート メニューの「ロック」を隠す、スタート メニューの電源ボタンを隠す、最近使った項目（ジャンプ リスト）を隠す、最近追加したアプリを隠す、スタート メニューの「再起動」を隠す、スタート メニューの「シャットダウン」を隠す、スタート メニューの「サインアウト」を隠す、スタート メニューの「スリープ」を隠す、スタート メニューの「アカウントの切り替え」を隠す、スタート メニューのユーザー アイコンを隠す、スタート メニューの表示モード、スタート メニューに「ドキュメント」を表示する、スタート メニューに「ダウンロード」を表示する、スタート メニューに「エクスプローラー」を表示する、スタート メニューに「ホームグループ」を表示する、スタート メニューに「ミュージック」を表示する、スタート メニューに「ネットワーク」を表示する、スタート メニューに「個人用フォルダー」を表示する、スタート メニューに「ピクチャ」を表示する、スタート メニューに「設定」を表示する、スタート メニューに「ビデオ」を表示する、diagnosticsDataSubmissionMode、OneDrive のファイル同期を無効にする、消費者向け機能の表示を禁止する、Windows スポットライトを禁止する、アクション センターでのスポットライトを禁止する、カスタマイズされた表示を禁止する、サード パーティーの通知を禁止する、ようこそ画面の表示を禁止する、Windows のヒントの表示を禁止する、ロック画面の Windows スポットライト、Microsoft アカウント以外のメール追加を禁止する、盗難防止モードを禁止する、Bluetooth を禁止する、カメラを禁止する、接続されたデバイス サービスを禁止する、ルート証明書の手動インストールを禁止する、コピーと貼り付けを禁止する、Cortana を禁止する、端末からの初期化を禁止する、利用者による登録解除を禁止する、セーフ サーチの強さ、Edge のポップアップを禁止する、Edge の検索候補を禁止する、イントラネット サイトを Internet Explorer で開かない、イントラネット サイトを Internet Explorer で開く、Edge で SmartScreen を必須にする、Edge の about:flags ページを開かせない、SmartScreen の警告を無視できないようにする、ファイルの SmartScreen 警告を無視できないようにする、WebRTC でのローカル IP アドレスの露出を禁止する、インターネット共有を禁止する、プロビジョニング パッケージの追加を禁止する、プロビジョニング パッケージの削除を禁止する、システム時刻の変更を禁止する、デバイス名の変更を禁止する、地域の変更を禁止する、言語の変更を禁止する、電源とスリープの変更を禁止する、位置情報サービスを禁止する、Microsoft アカウントの利用を禁止する、Microsoft アカウントの設定同期を禁止する、NFC を禁止する、リセット保護を禁止する、画面のキャプチャを禁止する、リムーバブル ストレージを禁止する、モバイル端末の暗号化を必須にする、USB を禁止する、音声の録音を禁止する、オープンなホットスポットへの自動接続を禁止する、Wi-Fi を禁止する、Wi-Fi の手動設定を禁止する、この端末への画面投影を禁止する、投影先からの操作を禁止する、ワイヤレス ディスプレイの接続に PIN を要求する、Microsoft Store を禁止する、信頼されたアプリのサイドロード、Microsoft Store アプリの自動更新を禁止する、開発者モードの利用、ユーザー間でアプリ データを共有する、Microsoft Store 由来のアプリを禁止する、プライベート ストアのみ利用できるようにする、アプリのデータをシステム ボリュームに限定する、アプリのインストール先をシステム ボリュームに限定する、ゲーム録画（ゲーム DVR）を禁止する、デバイスの検出を禁止する、SIM が無いときのエラー表示を禁止する、タスク スイッチャーを禁止する、ユーザーの簡易切り替えを禁止する、初期セットアップ中にネットワーク接続を必須にする、音声によるアプリの起動、MSI インストールの利用者による制御を許可する、MSI を常に昇格した権限でインストールする、別の端末からのサインインを許可する、Web サインインの利用、近くのデバイスからの Bluetooth 接続要求を禁止する、モバイル データの利用、FIPS 準拠のアルゴリズムを使う、アクセス時の保護を無効にする、実行できなかったフル スキャンの追いかけ実行を無効に

する、実行できなかったクイック スキャンの追いかけ実行を無効にする、望ましくない可能性のあるアプリへの動作、スケジュール検査を低い CPU 優先度で実行する、Edge のお気に入りの編集を禁止する、Edge の全画面表示を禁止する、Edge の事前起動を禁止する、Edge からの印刷を禁止する、Edge の閲覧履歴の保存を禁止する、Edge の検索エンジンの変更を禁止する、Edge の拡張機能のサイドロードを禁止する、Edge のタブの事前読み込みを禁止する、Edge の新しいタブに Web コンテンツを表示しない、Edge のお気に入りバーの表示、Edge のホーム ボタンの構成を有効にする、Edge のキオスク モードの制限、Edge の起動時に開くページ、Edge で証明書エラーを無視できないようにする、Internet Explorer で開くときにメッセージを表示する、Microsoft 365 分析へのテレメトリ送信、自動再展開を有効にする、ブラウザーの設定を同期しない、ファイルの検索（Find My Files）、Windows Ink ワークスペースへのアクセス、Windows Ink ワークスペースの利用、Windows Ink の推奨アプリを表示しない、ロック画面で音声によるアプリの起動、MMS を禁止する、RCS を禁止する、メッセージの同期を禁止する、Microsoft アカウント サインイン アシスタント、電源ボタンの動作（バッテリー時）、電源ボタンの動作（電源接続時）、ハイブリッド スリープ（バッテリー時）、ハイブリッド スリープ（電源接続時）、カバーを閉じたときの動作（バッテリー時）、カバーを閉じたときの動作（電源接続時）、スリープ ボタンの動作（バッテリー時）、スリープ ボタンの動作（電源接続時）、プリンターの追加を禁止する、アクティビティの履歴を禁止する、アクティビティの公開を禁止する、初回起動時のプライバシー設定画面を表示しない、検索に Web の結果を含めない、検索で位置情報を使わせない、検索で位置情報を使わせない、Microsoft Entra 参加時の自動暗号化を禁止する、SmartScreen のアプリ インストール制御、タスク マネージャーからのタスク終了を禁止する、組み込みアプリをアンインストールする

### 設定カタログ プロファイル（Settings Catalog）

構成されていません

## 17. コンプライアンスポリシー（Windows）

| ポリシー名 | 種別 | 説明 | 割当先 |
|---|---|---|---|
| [TenantSnap-Seed] Windows コンプライアンス（サンプル） | Windows コンプライアンスポリシー | 【意図】最低 OS バージョン（20H1 以上）とパスワードを満たさない端末を「非準拠」と判定し、条件付きアクセスでの制御に備える。【確認】非準拠時のブロック猶予0時間で運用合意済み。【責任者】情報システム部 セキュリティ担当 | 未割り当て |

※ この表は、各設定の「現在の値」を記載しています。その値が初期値（既定値）のままか、管理者が設定した値かは区別していません。また、各設定の既定値そのものは表示していません（Microsoft の仕様による制限のためです）。どの設定を意図的に構成したかを確認するには、Intune 管理センターの該当プロファイルをご参照ください。設定項目名と値は、よく使われるものを日本語で表示しています。訳語を用意していないものや、Microsoft が日本語の名称を提供していない設定（ADMX 形式の管理用テンプレートを取り込んだ設定など）は、誤った訳を出さないため英語のまま表示します。「未構成」と表示される設定は、このプロファイルでは制御していません。「いいえ」または「未構成」だった設定は、設定されている項目が読み取りにくくなるため、表のあとに項目名をまとめて記載しています。

### ■ [TenantSnap-Seed] Windows コンプライアンス（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | 最低 OS バージョン（20H1 以上）とパスワードを満たさない端末を「非準拠」と判定し、条件付きアクセスでの制御に備える。 |
| 確認 | 非準拠時のブロック猶予0時間で運用合意済み。 |

| 項目 | 内容 |
|---|---|
| 責任者 | 情報システム部 セキュリティ担当 |

■ [TenantSnap-Seed] Windows コンプライアンス（サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| パスワードを必須にする | はい |
| パスワードの最小文字数 | 8 |
| パスワードの種類 | デバイスの既定（種類を指定しません） |
| osMinimumVersion | 10.0.19041 |

「いいえ」または「未構成」だった設定（22 件）：単純なパスワードを禁止する、アイドル状態からの復帰にパスワードを必須にする、正常性の証明（構成証明）を必須にする、早期起動マルウェア対策ドライバーを有効にする、bitLockerEnabled、secureBootEnabled、codeIntegrityEnabled、端末の暗号化を必須にする、ファイアウォールを必須にする、スパイウェア対策を必須にする、ウイルス対策を必須にする、Configuration Manager の準拠を必須にする、Defender を有効にする、モバイル脅威対策を必須にする、許容する脅威レベルの上限、firmwareProtectionEnabled、kernelDmaProtectionEnabled、memoryIntegrityEnabled、rtpEnabled、signatureOutOfDate、TPM（セキュリティ チップ）を必須にする、virtualizationBasedSecurityEnabled

## 18. 管理用テンプレート（ADMX）

| テンプレート名 | 説明 | 割当先 |
|---|---|---|
| [TenantSnap-Seed] 管理用テンプレート（サンプル） | 【意図】従来のグループポリシー（GPO）から Intune へ移行する際の受け皿（サンプルのため設定値は未投入）。【戻し方】本構成を削除。 | パキケトゥス |

## 19. Windows Update 管理

### 機能更新プログラム（Feature Updates）

| プロファイル名 | 対象バージョン | 割当先 |
|---|---|---|
| [TenantSnap-Seed] 機能更新（サンプル） | Windows 11, version 23H2 | パキケトゥス |

※ この表は、各設定の「現在の値」を記載しています。その値が初期値（既定値）のままか、管理者が設定した値かは区別していません。また、各設定の既定値そのものは表示していません（Microsoft の仕様による制限のためです）。どの設定を意図的に構成したかを確認するには、Intune 管理センターの該当プロファイルをご参照ください。設定項目名と値は、よく使われるものを日本語で表示しています。訳語を用意していないものや、Microsoft が日本語の名称を提供していない設定（ADMX 形式の管理用テンプレートを取り込んだ設定など）は、誤った訳を出さないため英語のまま表示します。「未構成」と表示される設定は、このプロファイルでは制御していません。「いいえ」または「未構成」だった設定は、設定されている項目が読み取りにくくなるため、表のあとに項目名をまとめて記載しています。

■ [TenantSnap-Seed] 機能更新（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | Windows 11 の機能更新を「23H2」に固 |

| 項目 | 内容 |
|---|---|
| | 定し、検証前の意図しない大型更新を防ぐ。 |
| 確認 | 次期バージョンへの更新は検証後に手動で引き上げる。 |
| 責任者 | 情報システム部 端末管理チーム |

■ [TenantSnap-Seed] 機能更新（サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| endOfSupportDate | 2026-11-10T00:00:00Z |
| rolloutSettings | |

「いいえ」または「未構成」だった設定（2 件）：Windows 11 の対象外の端末に最新の Windows 10 を入れる、任意の機能更新プログラムをインストールする

### 品質更新プログラム（Quality Updates）

（データなし）

### ドライバー更新プログラム（Driver Updates）

（データなし）

## 20. アプリ管理（Win32 / WinGet / PowerShell / プロアクティブ修復）

### アプリ一覧

（データなし）

### PowerShell スクリプト

| スクリプト名 | ファイル名 | 実行アカウント | 署名チェック | 説明 | 割当先 |
|---|---|---|---|---|---|
| [TenantSnap-Seed] PowerShell スクリプト（サンプル） | tenantsnap-seed-sample.ps1 | システム | なし | 【意図】端末初期化時に一度だけ走らせる構成スクリプトの雛形（サンプルは何もしない exit 0）。【戻し方】スクリプトの割り当て解除。【責任者】情報システム部 | 未割り当て |

### プロアクティブ修復（検出 / 修復スクリプト）

| スクリプトパッケージ名 | 発行元 | 実行アカウント | 割当先 |
|---|---|---|---|

| スクリプトパッケージ名 | 発行元 | 実行アカウント | 割当先 |
|---|---|---|---|
| [TenantSnap-Seed] プロアクティブ修復（サンプル） | TenantSnap | システム | 未割り当て |

## 21. Windows Autopilot

### 展開プロファイル

（データなし）

### デバイス準備ポリシー（Windows Autopilot デバイス準備）

構成されていません

### 登録済みデバイス

※ Windows Autopilot にあらかじめ登録されている端末の台数と内訳です。端末ごとの明細（シリアル番号・割り当てユーザー）は、「Autopilot 登録デバイスの明細を出力する」がオンのとき付録 J に掲載します。

登録されていません

## 22. セキュリティベースライン

（データなし）

## 23. エンドポイントセキュリティ（Defender / BitLocker / FW / EDR / 特権管理）

### セキュリティポリシー

（データなし）

### 特権管理（Endpoint Privilege Management）

構成されていません（Intune Suite アドオン）

# 第4部 macOS

## 24. デバイス構成プロファイル（macOS）

### 構成プロファイル

| プロファイル名 | 種別 | 説明 | 割当先 |
|---|---|---|---|
| [TenantSnap-Seed] macOS デバイス構成（サンプル） | macOS 一般設定 | 【意図】macOS でもパスワード必須（8文字以上）にして Windows と要件を揃える。【戻し方】割り当て解除で復帰。【責任者】情報システム部 | 未割り当て |

※ この表は、各設定の「現在の値」を記載しています。その値が初期値（既定値）のままか、管理者が設定した値かは区別していません。また、各設定の既定値そのものは表示していません（Microsoft の仕様による制限のためです）。どの設定を意図的に構成したかを確認するには、Intune 管理センターの該当プロファイルをご参照ください。設定項目名と値は、よく使われるものを日本語で表示しています。訳語を用意していないものや、Microsoft が日本語の名称を提供していない設定（ADMX 形式の管理用テンプレートを取り込んだ設定など）は、誤った訳を出さないため英語のまま表示します。「未構成」と表示される設定は、このプロファイルでは制御していません。「いいえ」または「未構成」だった設定は、設定されている項目が読み取りにくくなるため、表のあとに項目名をまとめて記載しています。

#### ■ [TenantSnap-Seed] macOS デバイス構成（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | macOS でもパスワード必須（8文字以上）にして Windows と要件を揃える。 |
| 戻し方 | 割り当て解除で復帰。 |
| 責任者 | 情報システム部 |

#### ■ [TenantSnap-Seed] macOS デバイス構成（サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| compliantAppListType | 指定なし |
| パスワードの最小文字数 | 8 |
| パスワードの種類 | デバイスの既定（種類を指定しません） |
| パスワードを必須にする | はい |

「いいえ」または「未構成」だった設定（40 件）：単純なパスワードを禁止する、監視対象の端末でアクティベーション ロックを許可する、addingGameCenterFriendsBlocked、AirDrop を禁止する、Apple Watch による自動ロック解除を禁止する、カメラを禁止する、クラスルーム アプリからの画面監視を禁止する、クラスルーム アプリの画面監視を確認なしで許可する、クラスへの自動参加を強制する、クラスからの退出に許可を必須にする、クラスルームのアプリ・端末ロックを確認なしで許可する、contentCachingBlocked、definitionLookupBlocked、eraseContentAndSettingsBlocked、Game Center を禁止する、作業の引き継ぎ（Handoff）を禁止する、連絡先の iCloud 同期を禁止する、ブックマークの iCloud 同期を禁止する、カレンダーの iCloud 同期を禁止する、iCloud のドキュメント同期を禁止する、メールの iCloud 同期を禁止する、メモの iCloud 同期を禁止する、iCloud 写真を禁

止する、リマインダーの iCloud 同期を禁止する、デスクトップと書類の iCloud 同期を禁止する、iCloud プライベート リレーを禁止する、iTunes のファイル共有を禁止する、Apple Music を禁止する、音声入力を禁止する、keychainBlockCloudSync、multiplayerGamingBlocked、AirDrop でのパスワード共有を禁止する、パスワードの自動入力を禁止する、指紋によるロック解除を禁止する、パスワードの変更を禁止する、近くのデバイスへのパスワード要求を禁止する、Safari の自動入力を禁止する、画面のキャプチャを禁止する、spotlightBlockInternetResults、壁紙の変更を禁止する

### 設定カタログ プロファイル（Settings Catalog）

構成されていません

## 25. コンプライアンスポリシー（macOS）

| ポリシー名 | 種別 | 説明 | 割当先 |
|---|---|---|---|
| [TenantSnap-Seed] macOS コンプライアンス（サンプル） | macOS コンプライアンスポリシー | 【意図】macOS のパスワード必須を準拠条件にして、Windows と同等のベースラインを担保する。【戻し方】ポリシー削除で解除。 | 未割り当て |

※ この表は、各設定の「現在の値」を記載しています。その値が初期値（既定値）のままか、管理者が設定した値かは区別していません。また、各設定の既定値そのものは表示していません（Microsoft の仕様による制限のためです）。どの設定を意図的に構成したかを確認するには、Intune 管理センターの該当プロファイルをご参照ください。設定項目名と値は、よく使われるものを日本語で表示しています。訳語を用意していないものや、Microsoft が日本語の名称を提供していない設定（ADMX 形式の管理用テンプレートを取り込んだ設定など）は、誤った訳を出さないため英語のまま表示します。「未構成」と表示される設定は、このプロファイルでは制御していません。「いいえ」または「未構成」だった設定は、設定されている項目が読み取りにくくなるため、表のあとに項目名をまとめて記載しています。

### ■ [TenantSnap-Seed] macOS コンプライアンス（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | macOS のパスワード必須を準拠条件にして、Windows と同等のベースラインを担保する。 |
| 戻し方 | ポリシー削除で解除。 |

### ■ [TenantSnap-Seed] macOS コンプライアンス（サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| パスワードを必須にする | はい |
| パスワードの最小文字数 | 8 |
| パスワードの種類 | デバイスの既定（種類を指定しません） |

「いいえ」または「未構成」だった設定（10 件）：単純なパスワードを禁止する、systemIntegrityProtectionEnabled、モバイル脅威対策を必須にする、許容する脅威レベルの上限、端末の暗号化を必須にする、ファイアウォールを有効にする、受信をすべてブロックする、ステルス モードを有効にする、Defender for Endpoint で許容するリスク レベルの上限、gatekeeperAllowedAppSource

## 26. アプリ管理（PKG/DMG / シェルスクリプト）

### アプリ一覧

（データなし）

### シェルスクリプト

| スクリプト名 | ファイル名 | 実行アカウント | 実行間隔 | 説明 | 割当先 |
|---|---|---|---|---|---|
| [TenantSnap-Seed] シェルスクリプト（サンプル） | tenantsnap-seed-sample.sh | システム | 1日ごと | 【意図】macOS端末で定期実行する保守スクリプトの雛形（サンプルは exit 0）。【確認】実行間隔は1日1回。 | 未割り当て |

## 27. 登録プロファイル（ADE / Apple Business Manager）

### Apple Business Manager トークン

（データなし）

### 登録プロファイル（詳細パラメータ）

登録プロファイルは構成されていません

## 28. macOSセキュリティ設定（FileVault / Gatekeeper）

### セキュリティポリシー（FileVault / ディスク暗号化 等）

構成されていません

### セキュリティ関連の構成プロファイル

（データなし）

# 第5部 iOS / iPadOS

## 29. デバイス構成プロファイル（iOS）

### 構成プロファイル

| プロファイル名 | 種別 | 説明 | 割当先 |
|---|---|---|---|
| [TenantSnap-Seed] iOS コンテンツ制限・日本（サンプル） | iosGeneralDeviceConfiguration | 【意図】国内向け貸与 iPad で、視聴できる映画を R15+ 相当までに制限する。【戻し方】本プロファイルの割り当てを解除する。【確認】レーティング地域が日本の端末でのみ有効。【責任者】情報システム部 端末管理チーム | 未割り当て |
| [TenantSnap-Seed] iOS コンテンツ制限・米国（サンプル） | iosGeneralDeviceConfiguration | 【意図】北米拠点の貸与 iPad で、映画は PG-13・テレビは TV-14 までに制限する。【戻し方】本プロファイルの割り当てを解除する。【確認】レーティング地域が米国の端末でのみ有効。【責任者】情報システム部 端末管理チーム | 未割り当て |
| [TenantSnap-Seed] iOS デバイス構成（サンプル） | iosGeneralDeviceConfiguration | 【意図】iPhone/iPad に 6桁以上のパスコードを必須化し紛失時の情報漏えいを抑止。【確認】対象ユーザーへ事前周知済み。【戻し方】プロファイル削除で解除。 | 未割り当て |

※ この表は、各設定の「現在の値」を記載しています。その値が初期値（既定値）のままか、管理者が設定した値かは区別していません。また、各設定の既定値そのものは表示していません（Microsoft の仕様による制限のためです）。どの設定を意図的に構成したかを確認するには、Intune 管理センターの該当プロファイルをご参照ください。設定項目名と値は、よく使われるものを日本語で表示しています。訳語を用意していないものや、Microsoft が日本語の名称を提供していない設定（ADMX 形式の管理用テンプレートを取り込んだ設定など）は、誤った訳を出さないため英語のまま表示します。「未構成」と表示される設定は、このプロファイルでは制御していません。「いいえ」または「未構成」だった設定は、設定されている項目が読み取りにくくなるため、表のあとに項目名をまとめて記載しています。

#### ■ [TenantSnap-Seed] iOS コンテンツ制限・日本（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|

| 項目 | 内容 |
|---|---|
| 意図 | 国内向け貸与 iPad で、視聴できる映画を R15+ 相当までに制限する。 |
| 戻し方 | 本プロファイルの割り当てを解除する。 |
| 確認 | レーティング地域が日本の端末でのみ有効。 |
| 責任者 | 情報システム部 端末管理チーム |

### ■ [TenantSnap-Seed] iOS コンテンツ制限・日本（サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| アプリ一覧の扱い（表示／非表示） | 指定なし |
| compliantAppListType | 指定なし |
| アプリの年齢制限 | すべて許可 |
| パスコードの種類 | デバイスの既定（種類を指定しません） |
| Safari の Cookie の扱い | ブラウザーの既定 |
| コンテンツのレーティング（日本） | 映画のレーティング: 15 歳以上、テレビ番組のレーティング: すべて許可 |

「いいえ」または「未構成」だった設定（155 件）：アカウントの変更を禁止する、監視対象の端末でアクティベーション ロックを許可する、AirDrop を禁止する、AirDrop を管理対象外の送信先として扱う、AirPlay の送信時にペアリング用パスワードを必須にする、Apple Watch のペアリングを禁止する、Apple Watch の手首検出を必須にする、Apple News を禁止する、他の端末で購入したアプリの自動ダウンロードを禁止する、App Store を禁止する、アプリ内課金を禁止する、App Store アプリからのインストールを禁止する、App Store の利用時にパスワードを要求する、Bluetooth の設定変更を禁止する、カメラを禁止する、データ ローミングを禁止する、ローミング中のバックグラウンド取得を禁止する、アプリごとのモバイル データ設定の変更を禁止する、インターネット共有（テザリング）を禁止する、音声ローミングを禁止する、信頼されていない TLS 証明書を禁止する、クラスルーム アプリからの画面監視を禁止する、クラスルーム アプリの画面監視を確認なしで許可する、構成プロファイルの変更を禁止する、definitionLookupBlocked、端末側での機能制限の設定を禁止する、「すべてのコンテンツと設定を消去」を禁止する、デバイス名の変更を禁止する、診断データの送信を禁止する、診断データの送信設定の変更を禁止する、管理対象の書類を管理対象外のアプリで開かせない、管理対象外の書類を管理対象のアプリで開かせない、社内アプリの信頼を禁止する、社内アプリの信頼設定の変更を禁止する、FaceTime を禁止する、友達を探すを禁止する、Game Center の友達追加を禁止する、マルチプレイヤー ゲームを禁止する、Game Center を禁止する、hostPairingBlocked、ブックストアを禁止する、成人向けの書籍を禁止する、作業の引き継ぎ（Handoff）を禁止する、iCloud バックアップを禁止する、iCloud のドキュメント同期を禁止する、管理対象アプリの iCloud 同期を禁止する、iCloud 写真を禁止する、マイフォトストリームの同期を禁止する、共有アルバムを禁止する、iCloud バックアップの暗号化を必須にする、露骨な表現のコンテンツを禁止する、Apple Music を禁止する、iTunes Radio を禁止する、キーボードの自動修正を禁止する、音声入力を禁止する、予測入力を禁止する、キーボード ショートカットを禁止する、スペル チェックを禁止する、キオスク モードで読み上げを許可する、キオスク モードで AssistiveTouch の設定を許可する、キオスク モードで自動ロックを許可する、キオスク モードで色の反転設定を許可する、キオスク モードで着信スイッチを許可する、キオスク モードで画面の回転を許可する、キオスク モードでスリープ ボタンを許可する、キオスク モードでタッチ操作を許可する、キオスク モードで VoiceOver の設定を許可する、キオスク モードで音量ボタンを許可する、キオスク モードでズームの設定を許可する、キオスク モードで AssistiveTouch を必須にする、キオスク モードで色の反転を必須にする、キオスク モードでモノラル音声を必須にする、キオスク モードで VoiceOver を必須にする、キオスク モードでズームを必須にする、ロック画面でコントロール センターを使わせない、ロック画面で通知ビューを使わせない、ロック画面で Wallet を使わせない、ロック画面で今日の表示を使わせない、messagesBlocked、notificationsBlockSettingsModification、指紋によるロック解除を禁止する、登録済みの指紋の変更を禁止する、パスコードの変更を禁止する、単純なパスコードを禁止する、パスコードを必須にする、podcastsBlocked、Safari の自動入力を禁止する、Safari の JavaScript を禁止する、Safari のポップアップを禁止する、Safari を禁止する、Safari の詐欺サイト警告を必須にする、画面のキャプチャを禁止する、Siri を禁止する、ロック中の Siri を禁止する、Siri のユーザー作成コンテンツの参照を禁止する、Siri の不適切な言葉のフィルターを必須にする、spotlightBlockInternetResults、voiceDialingBlocked、壁紙の変更を禁止する、構成済みの Wi-Fi にのみ接続する、AirPrint の資格情報の保存を禁止する、AirPrint を

禁止する、AirPrint の iBeacon 検出を禁止する、AirPrint に信頼された TLS を必須にする、App Clip を禁止する、アプリの削除を禁止する、パーソナライズされた広告を禁止する、自動入力に認証を必須にする、自動ロック解除を禁止する、システム アプリの削除を禁止する、インターネット共有の設定変更を禁止する、モバイル プランの変更を禁止する、クラスへの自動参加を強制する、クラスからの退出に許可を必須にする、クラスルームのアプリ・端末ロックを確認なしで許可する、管理対象から管理対象外への連絡先の書き込みを許可する、管理対象外から管理対象への連絡先の読み取りを許可する、continuousPathKeyboardBlocked、dateAndTimeForceSetAutomatically、社内ブックのバックアップを禁止する、社内ブックのメタデータ同期を禁止する、esimBlockModification、ファイル アプリからのネットワーク ドライブ接続を禁止する、filesUsbDriveAccessBlocked、「探す」の端末検索を禁止する、「探す」の友達検索を禁止する、iCloud プライベート リレーを禁止する、iTunes を禁止する、keychainBlockCloudSync、キオスク モードで音声コントロールの変更を許可する、キオスク モードで使うアプリの種類、キオスク モードで自動ロックを禁止する、キオスク モードで着信スイッチを禁止する、キオスク モードで画面の回転を禁止する、キオスク モードでスリープ ボタンを禁止する、キオスク モードでタッチ操作を禁止する、キオスク モードで音量ボタンを禁止する、キオスク モードで音声コントロールを有効にする、管理対象のペーストボードを必須にする、NFC を禁止する、音声入力を端末内だけで処理する、翻訳を端末内だけで処理する、AirDrop でのパスワード共有を禁止する、パスワードの自動入力を禁止する、近くのデバイスへのパスワード要求を禁止する、pkiBlockOTAUpdates、広告のトラッキング制限を強制する、proximityBlockSetupToNewDevice、sharedDeviceBlockTemporarySessions、softwareUpdatesForceDelayed、未ペアリングの外部デバイスからの復旧起動を許可する、usbRestrictedModeBlocked、VPN の作成を禁止する、許可された Wi-Fi にのみ接続する、Wi-Fi を常にオンにする

### ■ [TenantSnap-Seed] iOS コンテンツ制限・米国（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | 北米拠点の貸与 iPad で、映画は PG-13・テレビは TV-14 までに制限する。 |
| 戻し方 | 本プロファイルの割り当てを解除する。 |
| 確認 | レーティング地域が米国の端末でのみ有効。 |
| 責任者 | 情報システム部 端末管理チーム |

### ■ [TenantSnap-Seed] iOS コンテンツ制限・米国（サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| アプリ一覧の扱い（表示／非表示） | 指定なし |
| compliantAppListType | 指定なし |
| アプリの年齢制限 | すべて許可 |
| パスコードの種類 | デバイスの既定（種類を指定しません） |
| Safari の Cookie の扱い | ブラウザーの既定 |
| コンテンツのレーティング（米国） | 映画のレーティング: 13 歳未満は保護者の指導が必要、テレビ番組のレーティング: 14 歳以上 |

「いいえ」または「未構成」だった設定（155 件）：アカウントの変更を禁止する、監視対象の端末でアクティベーション ロックを許可する、AirDrop を禁止する、AirDrop を管理対象外の送信先として扱う、AirPlay の送信時にペアリング用パスワードを必須にする、Apple Watch のペアリングを禁止する、Apple Watch の手首検出を必須にする、Apple News を禁止する、他の端末で購入したアプリの自動ダウンロードを禁止する、App Store を禁止する、アプリ内課金を禁止する、App Store アプリからのインストールを禁止する、App Store の利用時にパスワードを要求する、Bluetooth の設定変更を禁止する、カメラを禁止する、データ ローミングを禁止する、ローミング中のバックグラウンド取得を禁止する、アプリごとのモバイル データ設定の変更を禁止する、インターネット共有（テザリング）を禁止する、音声ローミングを禁止する、信頼されていない TLS 証明書を禁止する、クラスルーム アプリからの画面監視を禁止する、クラスルーム アプリの画面監視を確認なしで許可する、構成プロファイルの変更を禁止する、definitionLookupBlocked、端末側での機能制限の設定を禁止する、「すべてのコンテンツと設定を消去」を禁止する、デバイス名の変更を禁止する、診断データの送信を禁止する、診断データの送信設定の変更を禁止する、管理対象の書類を管理対象外のアプリで開かせない、管理対象外の書類

を管理対象のアプリで開かせない、社内アプリの信頼を禁止する、社内アプリの信頼設定の変更を禁止する、FaceTime を禁止する、友達を探すを禁止する、Game Center の友達追加を禁止する、マルチプレイヤー ゲームを禁止する、Game Center を禁止する、hostPairingBlocked、ブックストアを禁止する、成人向けの書籍を禁止する、作業の引き継ぎ（Handoff）を禁止する、iCloud バックアップを禁止する、iCloud のドキュメント同期を禁止する、管理対象アプリの iCloud 同期を禁止する、iCloud 写真を禁止する、マイ フォトストリームの同期を禁止する、共有アルバムを禁止する、iCloud バックアップの暗号化を必須にする、露骨な表現のコンテンツを禁止する、Apple Music を禁止する、iTunes Radio を禁止する、キーボードの自動修正を禁止する、音声入力を禁止する、予測入力を禁止する、キーボード ショートカットを禁止する、スペル チェックを禁止する、キオスク モードで読み上げを許可する、キオスク モードで AssistiveTouch の設定を許可する、キオスク モードで自動ロックを許可する、キオスク モードで色の反転設定を許可する、キオスク モードで着信スイッチを許可する、キオスク モードで画面の回転を許可する、キオスク モードでスリープ ボタンを許可する、キオスク モードでタッチ操作を許可する、キオスク モードで VoiceOver の設定を許可する、キオスク モードで音量ボタンを許可する、キオスク モードでズームの設定を許可する、キオスク モードで AssistiveTouch を必須にする、キオスク モードで色の反転を必須にする、キオスク モードでモノラル音声を必須にする、キオスク モードで VoiceOver を必須にする、キオスク モードでズームを必須にする、ロック画面でコントロール センターを使わせない、ロック画面で通知ビューを使わせない、ロック画面で Wallet を使わせない、ロック画面で今日の表示を使わせない、messagesBlocked、notificationsBlockSettingsModification、指紋によるロック解除を禁止する、登録済みの指紋の変更を禁止する、パスコードの変更を禁止する、単純なパスコードを禁止する、パスコードを必須にする、podcastsBlocked、Safari の自動入力を禁止する、Safari の JavaScript を禁止する、Safari のポップアップを禁止する、Safari を禁止する、Safari の詐欺サイト警告を必須にする、画面のキャプチャを禁止する、Siri を禁止する、ロック中の Siri を禁止する、Siri のユーザー作成コンテンツの参照を禁止する、Siri の不適切な言葉のフィルターを必須にする、spotlightBlockInternetResults、voiceDialingBlocked、壁紙の変更を禁止する、構成済みの Wi-Fi にのみ接続する、AirPrint の資格情報の保存を禁止する、AirPrint を禁止する、AirPrint の iBeacon 検出を禁止する、AirPrint に信頼された TLS を必須にする、App Clip を禁止する、アプリの削除を禁止する、パーソナライズされた広告を禁止する、自動入力に認証を必須にする、自動ロック解除を禁止する、システム アプリの削除を禁止する、インターネット共有の設定変更を禁止する、モバイル プランの変更を禁止する、クラスへの自動参加を強制する、クラスからの退出に許可を必須にする、クラスルームのアプリ・端末ロックを確認なしで許可する、管理対象から管理対象外への連絡先の書き込みを許可する、管理対象外から管理対象への連絡先の読み取りを許可する、continuousPathKeyboardBlocked、dateAndTimeForceSetAutomatically、社内ブックのバックアップを禁止する、社内ブックのメタデータ同期を禁止する、esimBlockModification、ファイル アプリからのネットワーク ドライブ接続を禁止する、filesUsbDriveAccessBlocked、「探す」の端末検索を禁止する、「探す」の友達検索を禁止する、iCloud プライベート リレーを禁止する、iTunes を禁止する、keychainBlockCloudSync、キオスク モードで音声コントロールの変更を許可する、キオスク モードで使うアプリの種類、キオスク モードで自動ロックを禁止する、キオスク モードで着信スイッチを禁止する、キオスク モードで画面の回転を禁止する、キオスク モードでスリープ ボタンを禁止する、キオスク モードでタッチ操作を禁止する、キオスク モードで音量ボタンを禁止する、キオスク モードで音声コントロールを有効にする、管理対象のペーストボードを必須にする、NFC を禁止する、音声入力を端末内だけで処理する、翻訳を端末内だけで処理する、AirDrop でのパスワード共有を禁止する、パスワードの自動入力を禁止する、近くのデバイスへのパスワード要求を禁止する、pkiBlockOTAUpdates、広告のトラッキング制限を強制する、proximityBlockSetupToNewDevice、sharedDeviceBlockTemporarySessions、softwareUpdatesForceDelayed、未ペアリングの外部デバイスからの復旧起動を許可する、usbRestrictedModeBlocked、VPN の作成を禁止する、許可された Wi-Fi にのみ接続する、Wi-Fi を常にオンにする

### ■ [TenantSnap-Seed] iOS デバイス構成（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | iPhone/iPad に6桁以上のパスコードを必須化し紛失時の情報漏えいを抑止。 |
| 確認 | 対象ユーザーへ事前周知済み。 |
| 戻し方 | プロファイル削除で解除。 |

### ■ [TenantSnap-Seed] iOS デバイス構成（サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| アプリ一覧の扱い（表示／非表示） | 指定なし |
| compliantAppListType | 指定なし |
| アプリの年齢制限 | すべて許可 |
| パスコードの最小文字数 | 6 |

| 設定項目 | 値 |
|---|---|
| パスコードの種類 | デバイスの既定（種類を指定しません） |
| パスコードを必須にする | はい |
| Safari の Cookie の扱い | ブラウザーの既定 |

「いいえ」または「未構成」だった設定（154 件）：アカウントの変更を禁止する、監視対象の端末でアクティベーション ロックを許可する、AirDrop を禁止する、AirDrop を管理対象外の送信先として扱う、AirPlay の送信時にペアリング用パスワードを必須にする、Apple Watch のペアリングを禁止する、Apple Watch の手首検出を必須にする、Apple News を禁止する、他の端末で購入したアプリの自動ダウンロードを禁止する、App Store を禁止する、アプリ内課金を禁止する、App Store アプリからのインストールを禁止する、App Store の利用時にパスワードを要求する、Bluetooth の設定変更を禁止する、カメラを禁止する、データ ローミングを禁止する、ローミング中のバックグラウンド取得を禁止する、アプリごとのモバイル データ設定の変更を禁止する、インターネット共有（テザリング）を禁止する、音声ローミングを禁止する、信頼されていない TLS 証明書を禁止する、クラスルーム アプリからの画面監視を禁止する、クラスルーム アプリの画面監視を確認なしで許可する、構成プロファイルの変更を禁止する、definitionLookupBlocked、端末側での機能制限の設定を禁止する、「すべてのコンテンツと設定を消去」を禁止する、デバイス名の変更を禁止する、診断データの送信を禁止する、診断データの送信設定の変更を禁止する、管理対象の書類を管理対象外のアプリで開かせない、管理対象外の書類を管理対象のアプリで開かせない、社内アプリの信頼を禁止する、社内アプリの信頼設定の変更を禁止する、FaceTime を禁止する、友達を探すを禁止する、Game Center の友達追加を禁止する、マルチプレイヤー ゲームを禁止する、Game Center を禁止する、hostPairingBlocked、ブックストアを禁止する、成人向けの書籍を禁止する、作業の引き継ぎ（Handoff）を禁止する、iCloud バックアップを禁止する、iCloud のドキュメント同期を禁止する、管理対象アプリの iCloud 同期を禁止する、iCloud 写真を禁止する、マイ フォトストリームの同期を禁止する、共有アルバムを禁止する、iCloud バックアップの暗号化を必須にする、露骨な表現のコンテンツを禁止する、Apple Music を禁止する、iTunes Radio を禁止する、キーボードの自動修正を禁止する、音声入力を禁止する、予測入力を禁止する、キーボード ショートカットを禁止する、スペル チェックを禁止する、キオスク モードで読み上げを許可する、キオスク モードで AssistiveTouch の設定を許可する、キオスク モードで自動ロックを許可する、キオスク モードで色の反転設定を許可する、キオスク モードで着信スイッチを許可する、キオスク モードで画面の回転を許可する、キオスク モードでスリープ ボタンを許可する、キオスク モードでタッチ操作を許可する、キオスク モードで VoiceOver の設定を許可する、キオスク モードで音量ボタンを許可する、キオスク モードでズームの設定を許可する、キオスク モードで AssistiveTouch を必須にする、キオスク モードで色の反転を必須にする、キオスク モードでモノラル音声を必須にする、キオスク モードで VoiceOver を必須にする、キオスク モードでズームを必須にする、ロック画面でコントロール センターを使わせない、ロック画面で通知ビューを使わせない、ロック画面で Wallet を使わせない、ロック画面で今日の表示を使わせない、messagesBlocked、notificationsBlockSettingsModification、指紋によるロック解除を禁止する、登録済みの指紋の変更を禁止する、パスコードの変更を禁止する、単純なパスコードを禁止する、podcastsBlocked、Safari の自動入力を禁止する、Safari の JavaScript を禁止する、Safari のポップアップを禁止する、Safari を禁止する、Safari の詐欺サイト警告を必須にする、画面のキャプチャを禁止する、Siri を禁止する、ロック中の Siri を禁止する、Siri のユーザー作成コンテンツの参照を禁止する、Siri の不適切な言葉のフィルターを必須にする、spotlightBlockInternetResults、voiceDialingBlocked、壁紙の変更を禁止する、構成済みの Wi-Fi にのみ接続する、AirPrint の資格情報の保存を禁止する、AirPrint を禁止する、AirPrint の iBeacon 検出を禁止する、AirPrint に信頼された TLS を必須にする、App Clip を禁止する、アプリの削除を禁止する、パーソナライズされた広告を禁止する、自動入力に認証を必須にする、自動ロック解除を禁止する、システム アプリの削除を禁止する、インターネット共有の設定変更を禁止する、モバイル プランの変更を禁止する、クラスへの自動参加を強制する、クラスからの退出に許可を必須にする、クラスルームのアプリ・端末ロックを確認なしで許可する、管理対象から管理対象外への連絡先の書き込みを許可する、管理対象外から管理対象への連絡先の読み取りを許可する、continuousPathKeyboardBlocked、dateAndTimeForceSetAutomatically、社内ブックのバックアップを禁止する、社内ブックのメタデータ同期を禁止する、esimBlockModification、ファイル アプリからのネットワーク ドライブ接続を禁止する、filesUsbDriveAccessBlocked、「探す」の端末検索を禁止する、「探す」の友達検索を禁止する、iCloud プライベート リレーを禁止する、iTunes を禁止する、keychainBlockCloudSync、キオスク モードで音声コントロールの変更を許可する、キオスク モードで使うアプリの種類、キオスク モードで自動ロックを禁止する、キオスク モードで着信スイッチを禁止する、キオスク モードで画面の回転を禁止する、キオスク モードでスリープ ボタンを禁止する、キオスク モードでタッチ操作を禁止する、キオスク モードで音量ボタンを禁止する、キオスク モードで音声コントロールを有効にする、管理対象のペーストボードを必須にする、NFC を禁止する、音声入力を端末内だけで処理する、翻訳を端末内だけで処理する、AirDrop でのパスワード共有を禁止する、パスワードの自動入力を禁止する、近くのデバイスへのパスワード要求を禁止する、pkiBlockOTAUpdates、広告のトラッキング制限を強制する、proximityBlockSetupToNewDevice、sharedDeviceBlockTemporarySessions、softwareUpdatesForceDelayed、未ペアリングの外部デバイスからの復旧起動を許可する、usbRestrictedModeBlocked、VPN の作成を禁止する、許可された Wi-Fi にのみ接続する、Wi-Fi を常にオンにする

## 設定カタログ プロファイル（Settings Catalog）

構成されていません

## 30. コンプライアンスポリシー（iOS）

| ポリシー名 | 種別 | 説明 | 割当先 |
|---|---|---|---|
| [TenantSnap-Seed] iOS コンプライアンス（サンプル） | iOS/iPadOS コンプライアンスポリシー | 【意図】パスコード未設定の iOS 端末を非準拠とし、社内リソースへのアクセスを抑止する。【確認】私用端末（BYOD）には別途アプリ保護で対応。 | 未割り当て |

※ この表は、各設定の「現在の値」を記載しています。その値が初期値（既定値）のままか、管理者が設定した値かは区別していません。また、各設定の既定値そのものは表示していません（Microsoft の仕様による制限のためです）。どの設定を意図的に構成したかを確認するには、Intune 管理センターの該当プロファイルをご参照ください。設定項目名と値は、よく使われるものを日本語で表示しています。訳語を用意していないものや、Microsoft が日本語の名称を提供していない設定（ADMX 形式の管理用テンプレートを取り込んだ設定など）は、誤った訳を出さないため英語のまま表示します。「未構成」と表示される設定は、このプロファイルでは制御していません。「いいえ」または「未構成」だった設定は、設定されている項目が読み取りにくくなるため、表のあとに項目名をまとめて記載しています。

### ■ [TenantSnap-Seed] iOS コンプライアンス（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | パスコード未設定の iOS 端末を非準拠とし、社内リソースへのアクセスを抑止する。 |
| 確認 | 私用端末（BYOD）には別途アプリ保護で対応。 |

### ■ [TenantSnap-Seed] iOS コンプライアンス（サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| パスコードの最小文字数 | 6 |
| パスコードの種類 | デバイスの既定（種類を指定しません） |
| パスコードを必須にする | はい |

「いいえ」または「未構成」だった設定（6 件）：単純なパスコードを禁止する、改造された端末（Jailbreak/root）を禁止する、モバイル脅威対策を必須にする、許容する脅威レベルの上限、管理対象のメール プロファイルを必須にする、Defender for Endpoint で許容するリスク レベルの上限

## 31. アプリ管理（iOS/iPadOS）

### アプリ一覧

| アプリ名 | 種別 | 発行元 | 開発者 | バージョン | 状態 | 割当先 |
|---|---|---|---|---|---|---|
| [TenantSnap-Seed] iOS ストアアプリ（サンプル） | iOS/iPadOS ストアアプリ | TenantSnap | | | 処理中 | 未割り当て |

# 32. iOS 登録（Apple MDM プッシュ証明書 / VPP トークン）

※ iOS / iPadOS デバイスを Intune で管理するために必要な、Apple との連携設定です。証明書やトークンそのもの（秘密情報）は設計書には出力せず、有効期限など運用に必要な情報のみを記載します。

## Apple MDM プッシュ証明書

構成されていません（iOS/iPadOS の管理にはこの証明書が必要です）

## VPP（アプリ一括購入）トークン

構成されていません

# 第6部 Android

## 33. デバイス構成プロファイル（Android）

### 構成プロファイル

| プロファイル名 | 種別 | 説明 | 割当先 |
|---|---|---|---|
| [TenantSnap-Seed] Android デバイス構成（サンプル） | androidWorkProfileGeneralDeviceConfiguration | 【意図】Android 仕事用プロファイルの基本パスワード要件（6文字以上）を定義。【戻し方】割り当て解除で復帰。【責任者】情報システム部 | 未割り当て |

※ この表は、各設定の「現在の値」を記載しています。その値が初期値（既定値）のままか、管理者が設定した値かは区別していません。また、各設定の既定値そのものは表示していません（Microsoft の仕様による制限のためです）。どの設定を意図的に構成したかを確認するには、Intune 管理センターの該当プロファイルをご参照ください。設定項目名と値は、よく使われるものを日本語で表示しています。訳語を用意していないものや、Microsoft が日本語の名称を提供していない設定（ADMX 形式の管理用テンプレートを取り込んだ設定など）は、誤った訳を出さないため英語のまま表示します。「未構成」と表示される設定は、このプロファイルでは制御していません。「いいえ」または「未構成」だった設定は、設定されている項目が読み取りにくくなるため、表のあとに項目名をまとめて記載しています。

#### ■ [TenantSnap-Seed] Android デバイス構成（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | Android 仕事用プロファイルの基本パスワード要件（6文字以上）を定義。 |
| 戻し方 | 割り当て解除で復帰。 |
| 責任者 | 情報システム部 |

#### ■ [TenantSnap-Seed] Android デバイス構成（サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| パスワードの最小文字数 | 6 |
| パスワードの種類 | デバイスの既定（種類を指定しません） |
| プロファイル間のデータ共有 | デバイスの既定 |
| アプリの権限要求の既定の動作 | デバイスの既定 |
| 仕事用プロファイルのパスワードの種類 | デバイスの既定（種類を指定しません） |
| パスワードの複雑さの要件 | 要件なし |
| 仕事用プロファイルで使えるアカウント | Google アカウント以外を許可 |
| 仕事用プロファイルのパスワードの複雑さの要件 | 要件なし |

「いいえ」または「未構成」だった設定（23 件）：指紋によるロック解除を禁止する、スマートロック（信頼エージェント）を禁止する、仕事用プロファイルでロック中の通知を出さない、仕事用プロファイルでのアカウント追加を禁止する、仕事用プロファイルの連絡先を Bluetooth で共有する、仕事用プロファイルで画面のキャプチャを禁止する、プロファイル間の発信者番号の表示を禁止する、仕事用プロファイルのカメラを禁止する、プロファイル間の連絡先検索を禁止する、プロファイル間のコピーと貼り付けを禁止する、仕事用プロファイルで指紋によるロック解除を禁止する、workProfilePasswordBlockTrustAgents、仕事用プロファイルにパスワードを必須にする、アプリの確認（Play プロテクト）を必須にする、個人用と仕事用で同じパスワードを使うことを禁止する、顔認証によるロック解除を禁止する、虹彩認証によるロック解除を禁止する、常時接続 VPN のロックダウン モードを有効にする、仕事用プロファイルで提供元不明のアプリを許可する、仕事用プロファイルのウィジェットを許可する、個人用で提供元不明のアプリを禁止する、仕事用プロファイルで顔認証によるロック解除を禁止する、仕事用プロファイルで虹彩認証によるロック解除を禁止する

### 設定カタログ プロファイル（Settings Catalog）

構成されていません

## 34. コンプライアンスポリシー（Android）

| ポリシー名 | 種別 | 説明 | 割当先 |
|---|---|---|---|
| [TenantSnap-Seed] Android コンプライアンス（サンプル） | Android (Work Profile) コンプライアンスポリシー | 【意図】Android のパスワード必須を準拠条件に設定。【戻し方】ポリシー削除で解除。【責任者】情報システム部 | 未割り当て |

※ この表は、各設定の「現在の値」を記載しています。その値が初期値（既定値）のままか、管理者が設定した値かは区別していません。また、各設定の既定値そのものは表示していません（Microsoft の仕様による制限のためです）。どの設定を意図的に構成したかを確認するには、Intune 管理センターの該当プロファイルをご参照ください。設定項目名と値は、よく使われるものを日本語で表示しています。訳語を用意していないものや、Microsoft が日本語の名称を提供していない設定（ADMX 形式の管理用テンプレートを取り込んだ設定など）は、誤った訳を出さないため英語のまま表示します。「未構成」と表示される設定は、このプロファイルでは制御していません。「いいえ」または「未構成」だった設定は、設定されている項目が読み取りにくくなるため、表のあとに項目名をまとめて記載しています。

### ■ [TenantSnap-Seed] Android コンプライアンス（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | Android のパスワード必須を準拠条件に設定。 |
| 戻し方 | ポリシー削除で解除。 |
| 責任者 | 情報システム部 |

### ■ [TenantSnap-Seed] Android コンプライアンス（サンプル） の設定値

| 設定項目 | 値 |
|---|---|
| パスワードを必須にする | はい |
| パスワードの最小文字数 | 6 |
| パスワードの種類 | デバイスの既定（種類を指定しません） |
| パスワードの複雑さの要件 | 要件なし |
| Play Integrity の評価の種類 | 基本 |
| 仕事用プロファイルのパスワードの種類 | デバイスの既定（種類を指定しません） |

| 設定項目 | 値 |
|---|---|
| 仕事用プロファイルのパスワードの複雑さの要件 | 要件なし |

「いいえ」または「未構成」だった設定（14 件）：提供元不明のアプリのインストールを禁止する、USB デバッグを無効にする、アプリの確認（Play プロテクト）を必須にする、モバイル脅威対策を必須にする、許容する脅威レベルの上限、改造された端末（Jailbreak/root）を禁止する、端末の暗号化を必須にする、Play Integrity の基本的な整合性を必須にする、Play Integrity の認定端末を必須にする、Google Play 開発者サービスを必須にする、セキュリティ プロバイダーの更新を必須にする、ポータル サイト アプリの整合性を必須にする、Defender for Endpoint で許容するリスク レベルの上限、仕事用プロファイルにパスワードを必須にする

## 35. アプリ管理（Android）

### アプリ一覧

| アプリ名 | 種別 | 発行元 | 開発者 | バージョン | 状態 | 割当先 |
|---|---|---|---|---|---|---|
| [TenantSnap-Seed] Android ストアアプリ（サンプル） | Android ストアアプリ | TenantSnap | | | 公開済み | パキケトゥス［必須］ |

## 36. Android Enterprise（managed Google Play 連携 / 登録プロファイル）

※ Android を Intune で管理するための Google（managed Google Play）との連携設定と、デバイスの登録方法（登録プロファイル）です。登録トークン・QR コード・Wi-Fi パスワードなどの秘密情報は設計書には出力せず、連携状態や有効期限など運用に必要な情報のみを記載します。

### managed Google Play 連携状態

| 連携状態 | 組織名 | 連携した管理者 | 登録できるユーザー | アプリ同期の結果 | 最終アプリ同期 |
|---|---|---|---|---|---|
| 未連携 | | | なし（登録不可） | 未同期 | |

### 登録プロファイル（Device Owner）

構成されていません

# 第7部 Linux

## 37. Linux（設定カタログ）

※ Intune の Linux 管理（Ubuntu・RHEL 等）は、デバイス構成もコンプライアンスも「設定カタログ」で行います（Windows などのようなテンプレート型のプロファイルはありません）。

### 設定カタログ プロファイル（Linux）

| ポリシー名 | 説明 | 割当先 |
|---|---|---|
| [TenantSnap-Seed] Linux Defender 設定（サンプル） | 【意図】Linux 端末（Ubuntu/RHEL 等）の Microsoft Defender でリアルタイム保護を有効化する。【戻し方】本ポリシーの割り当て解除。【責任者】情報システム部 セキュリティ担当 | 未割り当て |

※ 各設定の下の薄い文字は、その設定の説明（Microsoft が提供）です。青いリンクは、その設定の解説ページ（Microsoft 提供）です。「既定との差分」は、その設定が Microsoft の初期値のままか、変更されているかを示します（空欄は初期値を判定できなかった設定です）。名称・説明・解説ページが取得できなかった設定は、内部で使われる管理用の名称（英語）で表示しています。

#### ■ [TenantSnap-Seed] Linux Defender 設定（サンプル） の運用メモ（説明）

| 項目 | 内容 |
|---|---|
| 意図 | Linux 端末（Ubuntu/RHEL 等）の Microsoft Defender でリアルタイム保護を有効化する。 |
| 戻し方 | 本ポリシーの割り当て解除。 |
| 責任者 | 情報システム部 セキュリティ担当 |

#### ■ [TenantSnap-Seed] Linux Defender 設定（サンプル） の設定値

| 設定項目 | 値 | 既定との差分 |
|---|---|---|
| linux_mdatp_managed_antivirusengine_enablerealtimeprotection | linux_mdatp_managed_antivirusengine_enablerealtimeprotection_true | |

# 第8部 変更履歴

## 38. 変更履歴（差分＋監査ログ統合）

変更なし

# 付録 A. 名称と ID の対応表

本文の各表では読みやすさのため内部 ID（識別子）を省略しています。サポートへのお問い合わせや Microsoft Intune 管理センターでの特定が必要な場合は、以下の対応表をご利用ください。

## デバイス構成プロファイル

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] Android デバイス構成（サンプル） | 25f73262-fb88-4984-90d5-d0439e7838e2 |
| [TenantSnap-Seed] iOS コンテンツ制限・日本（サンプル） | 9ad24f2e-338c-44cf-8a00-d145bb58a625 |
| [TenantSnap-Seed] iOS コンテンツ制限・米国（サンプル） | 463184b8-1bd5-4795-814e-e74a9ddd4b74 |
| [TenantSnap-Seed] iOS デバイス構成（サンプル） | b26acdf6-7e42-4e91-a29e-1cc4de50cc6c |
| [TenantSnap-Seed] macOS デバイス構成（サンプル） | ac92c907-d892-4476-ba6b-b2bf8012cf24 |
| [TenantSnap-Seed] Windows スタート メニュー レイアウト（サンプル） | 5b7bf6c4-d1d7-455b-bdac-06b42989715e |
| [TenantSnap-Seed] Windows デバイス構成（サンプル） | c76b5b6e-4fcd-4cf1-84ec-7a52c27e72eb |

## コンプライアンスポリシー

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] Android コンプライアンス（サンプル） | 4c630bb7-d81b-4736-a558-59dfed065178 |
| [TenantSnap-Seed] macOS コンプライアンス（サンプル） | 6ce8324d-6f7d-43de-b4c1-d1088cd0532d |
| [TenantSnap-Seed] iOS コンプライアンス（サンプル） | 9b79414e-5a96-4b99-a2a1-704056d01522 |
| [TenantSnap-Seed] Windows コンプライアンス（サンプル） | e1a311b6-3d71-4b50-a367-1246a9edbf67 |

## アプリ

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] Android ストアアプリ（サンプル） | cfe58af6-8d27-4762-bbda-d4b752be13d0 |
| [TenantSnap-Seed] iOS ストアアプリ（サンプル） | 35b73a5b-d911-478c-96d7-6364840c560f |
| [TenantSnap-Seed] 社内ポータル（Web アプリ・サンプル） | 69ca390c-d4b3-426f-b573-7859b570afca |

## デバイス登録設定

| 名称 | ID |
|---|---|
| All users and all devices | 7e10b473-285b-469e-bea2- |

| 名称 | ID |
|---|---|
| | de2851f2b914_DefaultLimit |
| All users and all devices | 7e10b473-285b-469e-bea2-de2851f2b914_DefaultPlatformRestrictions |
| All users and all devices | 7e10b473-285b-469e-bea2-de2851f2b914_DefaultWindows10EnrollmentCompletionPageConfiguration |
| All users and all devices | 7e10b473-285b-469e-bea2-de2851f2b914_DefaultWindowsHelloForBusiness |
| All users and all devices | 7e10b473-285b-469e-bea2-de2851f2b914_WindowsRestore |

## ロール定義

| 名称 | ID |
|---|---|
| Policy and Profile manager | 0bd113fe-6be5-400c-a28f-ae5553f9c0be |
| School Administrator | 2f9f4f7e-2d13-427b-adf2-361a1eef7ae8 |
| Multi Admin Approval Policy Manager | 5500eb3c-d329-45fd-b3a9-5f87c2cc5e03 |
| Endpoint Privilege Reader | 9553af24-bd83-4ac3-a339-0e58f9e5478e |
| Help Desk Operator | 9e0cc482-82df-4ab2-a24c-0c23a3f52e1e |
| Application Manager | c1d9fcbb-cba5-40b0-bf6b-527006585f4b |
| Endpoint Security Manager | c56d53a2-73d0-4502-b6bd-4a9d3dba28d5 |
| Endpoint Privilege Manager | e9a9f614-7527-44e2-a61a-1879747ccfd7 |
| Read Only Operator | fa1d7878-e8cb-41a1-8254-0142355c9f84 |
| Intune Role Administrator | fb2603eb-3c87-4be3-8b5b-d58a5b4a0bc0 |

## 条件付きアクセスポリシー

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] 条件付きアクセス（無効・サンプル） | 14499e64-0ff9-4ac6-8710-4b1ad5253c6e |

## 名前付き場所

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] 本社ネットワーク（名前付き場所・サンプル） | 0fbb99a5-ca41-46d2-a317-7b25c0c41d1f |

## グループ

| 名称 | ID |
|---|---|
| パキケトゥス | 93943697-f54e-422d-a345-e51c17c6fe78 |
| Group for Answers in Viva Engage – DO NOT DELETE 175983198208 | b3d8bae3-8115-460c-b5a0-5f8d9fd5a7fc |
| All Company | f47a6db4-c2c7-4986-8095-d25d38fa29bc |

## アプリ保護ポリシー（iOS）

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] アプリ保護（iOS・サンプル） | T_55c21eb3-155c-4985-981c-df3f62234ed3 |

## アプリ保護ポリシー（Android）

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] アプリ保護（Android・サンプル） | T_9ceb4aee-c43d-4614-9281-348e0c1872ba |

## 利用規約

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] 利用規約（サンプル） | fe5c9095-4729-4e33-a715-7a18e6f6d21b |

## デバイスカテゴリ

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] 営業部端末（デバイスカテゴリ・サンプル） | 2fabe41c-0649-4340-9426-44a667fac5b8 |

## 通知テンプレート

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] 通知テンプレート（サンプル） | 3581448b-5fa3-4b10-8fae-e805f27c2c80 |

## スコープタグ

| 名称 | ID |
|---|---|
| Default | 0 |
| [TenantSnap-Seed] 営業部（スコープタグ・サンプル） | 7 |

## 割り当てフィルター

| 名称 | ID |
|---|---|

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] 割り当てフィルター（Android・サンプル） | 5bbd49b8-f866-4fae-b0af-b1ea7dfd5aeb |
| [TenantSnap-Seed] 割り当てフィルター（iOS・サンプル） | 1c15437a-1008-488e-93bd-b33a4addd4e3 |
| [TenantSnap-Seed] 割り当てフィルター（サンプル） | afa2ff6d-c078-4bfc-98ae-f5c9a6e0d618 |

## 管理用テンプレート

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] 管理用テンプレート（サンプル） | 32739008-2329-4cd0-b822-5cca9f5107c6 |

## 機能更新プログラム

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] 機能更新（サンプル） | 784fe3ba-8275-4f98-acad-e5eadbec30b2 |

## PowerShell スクリプト

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] PowerShell スクリプト（サンプル） | 0a8801bb-80d3-4162-aeda-d2141c9465a2 |

## シェルスクリプト

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] シェルスクリプト（サンプル） | dbc8e284-bdd4-424b-955d-4b53ecffcc11 |

## プロアクティブ修復スクリプト

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] プロアクティブ修復（サンプル） | 3409eb77-0ee7-4b4b-9933-ea73ec7f1a07 |

## エンドポイントセキュリティ

| 名称 | ID |
|---|---|
| [TenantSnap-Seed] Linux Defender 設定（サンプル） | b3e05868-55d2-4f60-9f29-b1241f160c72 |

# 付録 B. 設計意図（説明）が未記入の項目

運用設計書として整備するうえで、各ポリシー・アプリの「説明」欄に設計意図（なぜその設定にしたか・変更してよい条件・元に戻す方法・確認方法・責任者など）を記入しておくことをおすすめします。以下は、現時点で説明が未記入の項目の一覧です。Microsoft Intune 管理センターで各オブジェクトの「説明」欄に追記すると、次回以降の設計書に反映されます。

（対象のポリシー・アプリはすべて説明が記入されています。運用設計書としての整備が進んでいます。）

# 付録 C. 割り当ての見直し候補

ポリシーやアプリの割り当てのうち、見直しの参考になりそうな項目を一覧にしました。「未割り当て」「全体への割り当て」「除外グループあり」「名称が検証用・一時利用を思わせるもの」を、名称と割り当ての内容にもとづいて機械的に抽出したものです。実際に修正・削除してよいかは、運用状況をご確認のうえお客様で判断してください。

## デバイス構成プロファイル（7 件）

| 名称 | 割当先 | 見直しの観点 |
|---|---|---|
| [TenantSnap-Seed] Android デバイス構成（サンプル） | 未割り当て | 未割り当て / 名称が検証用・一時利用の可能性 |
| [TenantSnap-Seed] iOS コンテンツ制限・日本（サンプル） | 未割り当て | 未割り当て / 名称が検証用・一時利用の可能性 |
| [TenantSnap-Seed] iOS コンテンツ制限・米国（サンプル） | 未割り当て | 未割り当て / 名称が検証用・一時利用の可能性 |
| [TenantSnap-Seed] iOS デバイス構成（サンプル） | 未割り当て | 未割り当て / 名称が検証用・一時利用の可能性 |
| [TenantSnap-Seed] macOS デバイス構成（サンプル） | 未割り当て | 未割り当て / 名称が検証用・一時利用の可能性 |
| [TenantSnap-Seed] Windows スタート メニュー レイアウト（サンプル） | 未割り当て | 未割り当て / 名称が検証用・一時利用の可能性 |
| [TenantSnap-Seed] Windows デバイス構成（サンプル） | パキケトゥス | 名称が検証用・一時利用の可能性 |

## コンプライアンスポリシー（4 件）

| 名称 | 割当先 | 見直しの観点 |
|---|---|---|
| [TenantSnap-Seed] Android コンプライアンス（サンプル） | 未割り当て | 未割り当て / 名称が検証用・一時利用の可能性 |
| [TenantSnap-Seed] macOS コンプライアンス（サンプル） | 未割り当て | 未割り当て / 名称が検証用・一時利用の可能性 |
| [TenantSnap-Seed] iOS コンプライアンス（サンプル） | 未割り当て | 未割り当て / 名称が検証用・一時利用の可能性 |
| [TenantSnap-Seed] Windows コンプライアンス（サンプル） | 未割り当て | 未割り当て / 名称が検証用・一時利用の可能性 |

## アプリ（3 件）

| 名称 | 割当先 | 見直しの観点 |
|---|---|---|
| [TenantSnap-Seed] Android ストアアプリ（サンプル） | パキケトゥス［必須］ | 名称が検証用・一時利用の可能性 |
| [TenantSnap-Seed] iOS ストアアプリ（サンプル） | 未割り当て | 未割り当て / 名称が検証用・一 |

| 名称 | 割当先 | 見直しの観点 |
|---|---|---|
| | | 時利用の可能性 |
| [TenantSnap-Seed] 社内ポータル（Web アプリ・サンプル） | 未割り当て | 未割り当て / 名称が検証用・一時利用の可能性 |

# 付録 M. 割り当ての棚卸し一覧

どのポリシー・アプリが、どの割り当て先（グループ・全ユーザー・全デバイス）に割り当てられているかの一覧です。割り当て1件を1行として、含める割り当てと除外の割り当て、適用されている割り当てフィルターを事実のまま並べています。後半には、割り当て先から引ける一覧（このグループにはどのポリシーが当たるか）を載せています。

## ポリシー別の割り当て一覧

### デバイス構成プロファイル（7 件）

| 名称 | 割当先 | 含む/除外 | 割り当てフィルター |
|---|---|---|---|
| [TenantSnap-Seed] Android デバイス構成（サンプル） | （未割り当て） | — | — |
| [TenantSnap-Seed] iOS コンテンツ制限・日本（サンプル） | （未割り当て） | — | — |
| [TenantSnap-Seed] iOS コンテンツ制限・米国（サンプル） | （未割り当て） | — | — |
| [TenantSnap-Seed] iOS デバイス構成（サンプル） | （未割り当て） | — | — |
| [TenantSnap-Seed] macOS デバイス構成（サンプル） | （未割り当て） | — | — |
| [TenantSnap-Seed] Windows スタート メニュー レイアウト（サンプル） | （未割り当て） | — | — |
| [TenantSnap-Seed] Windows デバイス構成（サンプル） | パキケトゥス | 含む | [TenantSnap-Seed] 割り当てフィルター（サンプル） ［含む］ |

### コンプライアンスポリシー（4 件）

| 名称 | 割当先 | 含む/除外 |
|---|---|---|
| [TenantSnap-Seed] Android コンプライアンス（サンプル） | （未割り当て） | — |
| [TenantSnap-Seed] macOS コンプライアンス（サンプル） | （未割り当て） | — |
| [TenantSnap-Seed] iOS コンプライアンス（サンプル） | （未割り当て） | — |
| [TenantSnap-Seed] Windows コンプライアンス（サンプル） | （未割り当て） | — |

### アプリ（3 件）

| 名称 | 割当先 | 含む/除外 | 割り当てフィルター | 目的 |
|---|---|---|---|---|
| [TenantSnap-Seed] Android ストア | パキケトゥス | 含む | [TenantSnap-Seed] | 必須 |

| 名称 | 割当先 | 含む/除外 | 割り当てフィルター | 目的 |
|---|---|---|---|---|
| アプリ（サンプル） | | | 割り当てフィルター（Android・サンプル）［含む］ | |
| [TenantSnap-Seed] iOS ストアアプリ（サンプル） | （未割り当て） | — | — | |
| [TenantSnap-Seed] 社内ポータル（Web アプリ・サンプル） | （未割り当て） | — | — | |

## デバイス登録設定（5 件）

| 名称 | 割当先 | 含む/除外 | 割り当てフィルター |
|---|---|---|---|
| All users and all devices | 全デバイス | 含む | — |
| All users and all devices | 全デバイス | 含む | — |
| All users and all devices | 全デバイス | 含む | — |
| All users and all devices | 全デバイス | 含む | — |
| All users and all devices | 全デバイス | 含む | — |

## アプリ保護ポリシー（iOS）（1 件）

| 名称 | 割当先 | 含む/除外 |
|---|---|---|
| [TenantSnap-Seed] アプリ保護（iOS・サンプル） | （未割り当て） | — |

## アプリ保護ポリシー（Android）（1 件）

| 名称 | 割当先 | 含む/除外 |
|---|---|---|
| [TenantSnap-Seed] アプリ保護（Android・サンプル） | （未割り当て） | — |

## 管理用テンプレート（1 件）

| 名称 | 割当先 | 含む/除外 | 割り当てフィルター |
|---|---|---|---|
| [TenantSnap-Seed] 管理用テンプレート（サンプル） | パキケトゥス | 含む | [TenantSnap-Seed] 割り当てフィルター（サンプル）［含む］ |

## 機能更新プログラム（1 件）

| 名称 | 割当先 | 含む/除外 | 割り当てフィルター |
|---|---|---|---|
| [TenantSnap-Seed] 機能更新（サンプル） | パキケトゥス | 含む | — |

## PowerShell スクリプト（1 件）

| 名称 | 割当先 | 含む/除外 |
|---|---|---|
| [TenantSnap-Seed] PowerShell スクリプト（サンプル） | （未割り当て） | — |

### シェルスクリプト（1 件）

| 名称 | 割当先 | 含む/除外 |
|---|---|---|
| [TenantSnap-Seed] シェルスクリプト（サンプル） | （未割り当て） | — |

### プロアクティブ修復スクリプト（1 件）

| 名称 | 割当先 | 含む/除外 |
|---|---|---|
| [TenantSnap-Seed] プロアクティブ修復（サンプル） | （未割り当て） | — |

### エンドポイントセキュリティ（1 件）

| 名称 | 割当先 | 含む/除外 |
|---|---|---|
| [TenantSnap-Seed] Linux Defender 設定（サンプル） | （未割り当て） | — |

## グループ別の割り当て一覧

割り当て先ごとに、その対象へ割り当てられているポリシー・アプリをまとめたものです。グループの棚卸し（この割り当て先に何が当たっているか）にご利用ください。

| 割当先 | 含む/除外 | 分類 | 名称 |
|---|---|---|---|
| パキケトゥス | 含む | アプリ | [TenantSnap-Seed] Android ストアアプリ（サンプル） |
| パキケトゥス | 含む | デバイス構成プロファイル | [TenantSnap-Seed] Windows デバイス構成（サンプル） |
| パキケトゥス | 含む | 機能更新プログラム | [TenantSnap-Seed] 機能更新（サンプル） |
| パキケトゥス | 含む | 管理用テンプレート | [TenantSnap-Seed] 管理用テンプレート（サンプル） |
| 全デバイス | 含む | デバイス登録設定 | All users and all devices |
| 全デバイス | 含む | デバイス登録設定 | All users and all devices |
| 全デバイス | 含む | デバイス登録設定 | All users and all devices |
| 全デバイス | 含む | デバイス登録設定 | All users and all devices |
| 全デバイス | 含む | デバイス登録設定 | All users and all devices |

※ 取得したグループのうち、ポリシー・アプリの割り当てに使われていないものが 2 件あります（グループそのものの一覧は「グルー

プ」の章をご覧ください）。