



教育機関向け
Intune for Education 概要

日本マイクロソフト株式会社

2020年8月版



本資料についての注意点



- タイミングによっては、最新の情報が反映されていない場合がございます。必要に応じて最新情報をご確認ください。
- 内容を精査しておりますが、一部に「一般企業向け」の情報が含まれている可能性がございます。
- ライセンス部分に関して「教育機関向け」と異なる可能性がございますので、購入検討の際は改めてご確認ください。

Microsoft 製品での教育環境の実現

① ユーザー ID



Azure AD

- クラウドの ID 管理サービス
- ユーザー情報やライセンスの管理
- 他クラウドサービス・アプリと連携

Office 365 のユーザー情報やライセンス管理、クラウド ID 管理サービス。クラウドアプリとの連携や ID 保護機能まで搭載したクラウド サービスの中核となる存在。
様々なオプション機能を有しているが、教育ではユーザーの管理で利用。

② 教育用ツール



Office 365

- コミュニケーション ツール群
- チャットや授業、課題管理など
- 生徒が Web やアプリで使用

いわゆる Word や Excel といった Office アプリケーションから近年はクラウド上で使える Office ツールまで提供。
教育では統合コミュニケーションツール "Teams" が中心となり、オンライン授業や課題の提出などの先生・生徒のコミュニケーションに使用。

③ 端末管理ツール



intune

- クラウドの端末管理サービス
- 設定やアプリの配布
- 管理者が使用

モバイルデバイス管理 (MDM) を提供するクラウド サービス。
主にデバイスの管理、設定などのポリシー配布、アプリの配布が可能。
教育では端末への設定・ポリシーの配布が中心となる

④ 端末



Windows 10

- 端末の基本ソフト (OS)
- セキュリティ標準装備
- クラウド・モバイル管理対応

端末用の基本ソフト (OS) で、現在も世界の約 80% のシェア。
最新の Windows 10 では、クラウド対応のための細かなバージョンアップへの対応や、モバイル端末として管理することが可能。

端末管理ツール – Intune for Education

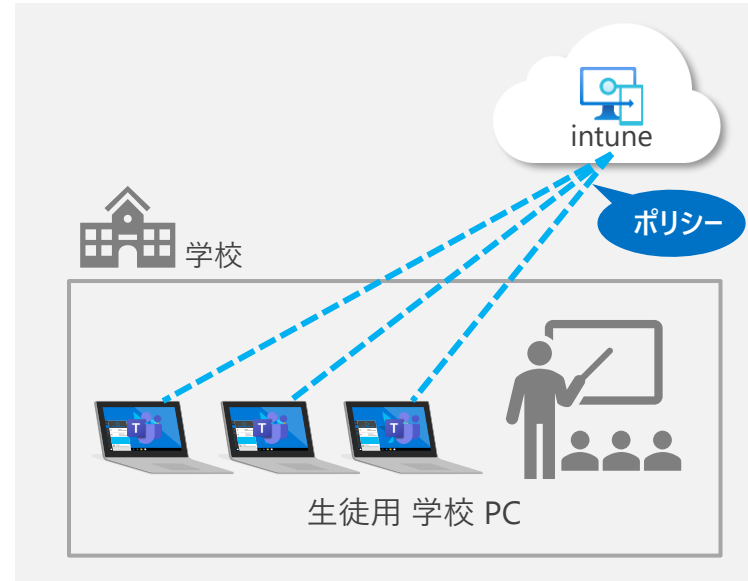
③ 端末管理ツール



intune

- クラウドの端末管理サービス
- 設定やアプリの配布
- 管理者が使用

モバイルデバイス管理 (MDM) を提供するクラウド サービス。
主にデバイスの管理、設定などのポリシー配布、アプリの配布が可能。
教育では端末への設定・ポリシーの配布が中心となる



Intune 動作イメージ



管理コンソール (ブラウザで管理者がアクセス)

普段の運用に必要なこと

- 端末の状態の監視 (アップデートがされているかなど)
- 端末紛失時のワイプ
- 必要に応じて、端末の設定の変更
- 必要に応じて、アプリケーションの配布・設定

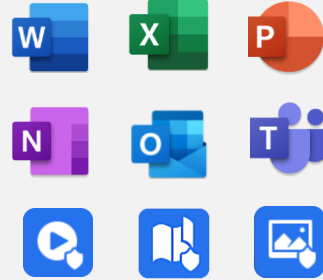
Microsoft Intune

教育機関で
主に利用するポイント

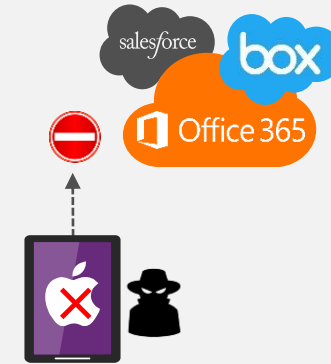
デバイスの管理
(MDM)



アプリの管理
(MAM)



アクセス制御



Microsoft Intune

Intune を使用すると、管理者はデバイスの設定や管理を一元化することが可能です。



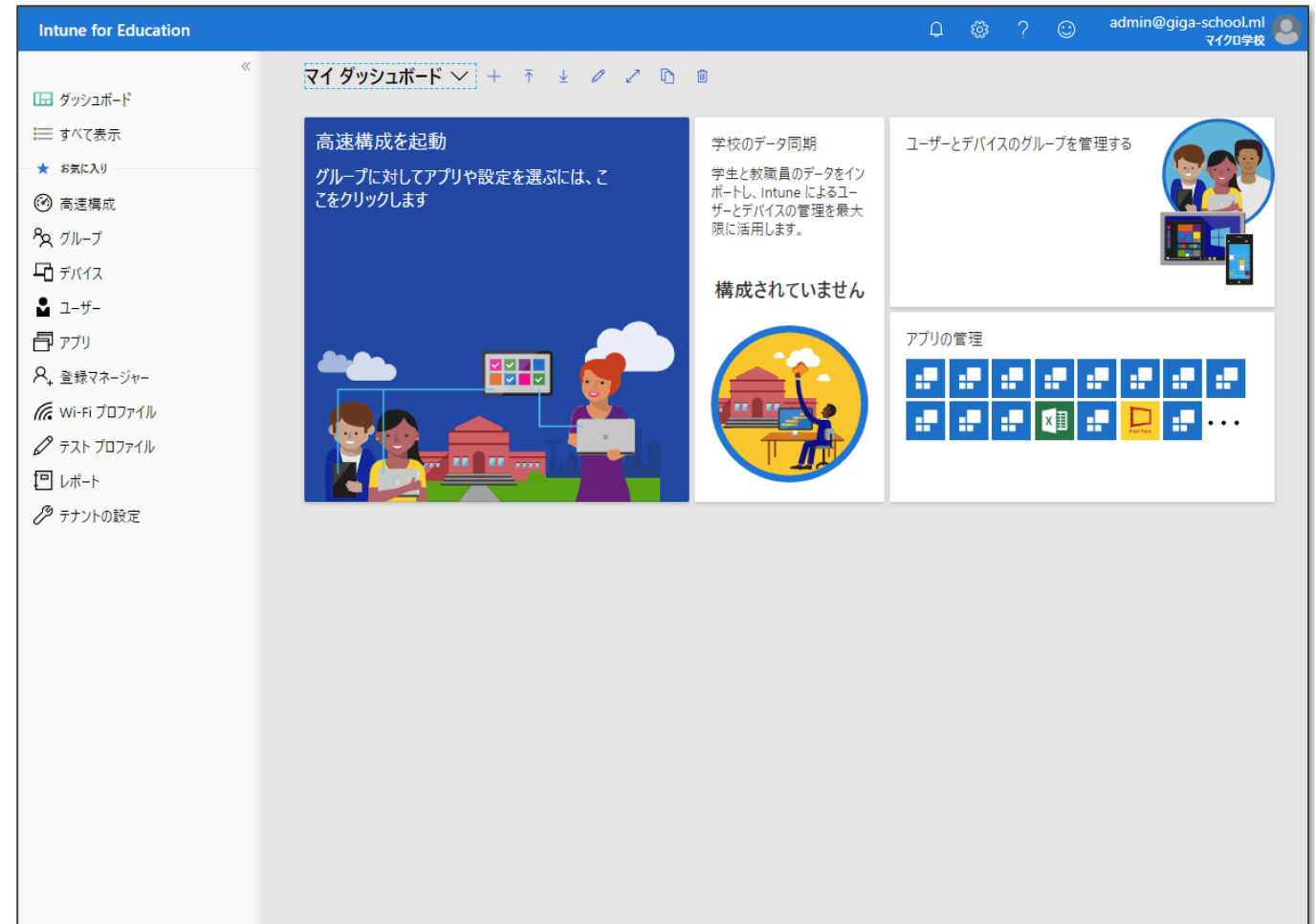
Intune for Education

デバイス管理 (MDM) ツール Intune の教育機関向けエディション

- 学生が教室データにアクセスするとき使用するデバイスの管理
- 学校のセキュリティ要件をデバイスとアプリに適用
- 学生が教室で使用するアプリを構成して割り当て

教育用の Intune とは

<https://docs.microsoft.com/ja-jp/intune-education/what-is-intune-for-education/>



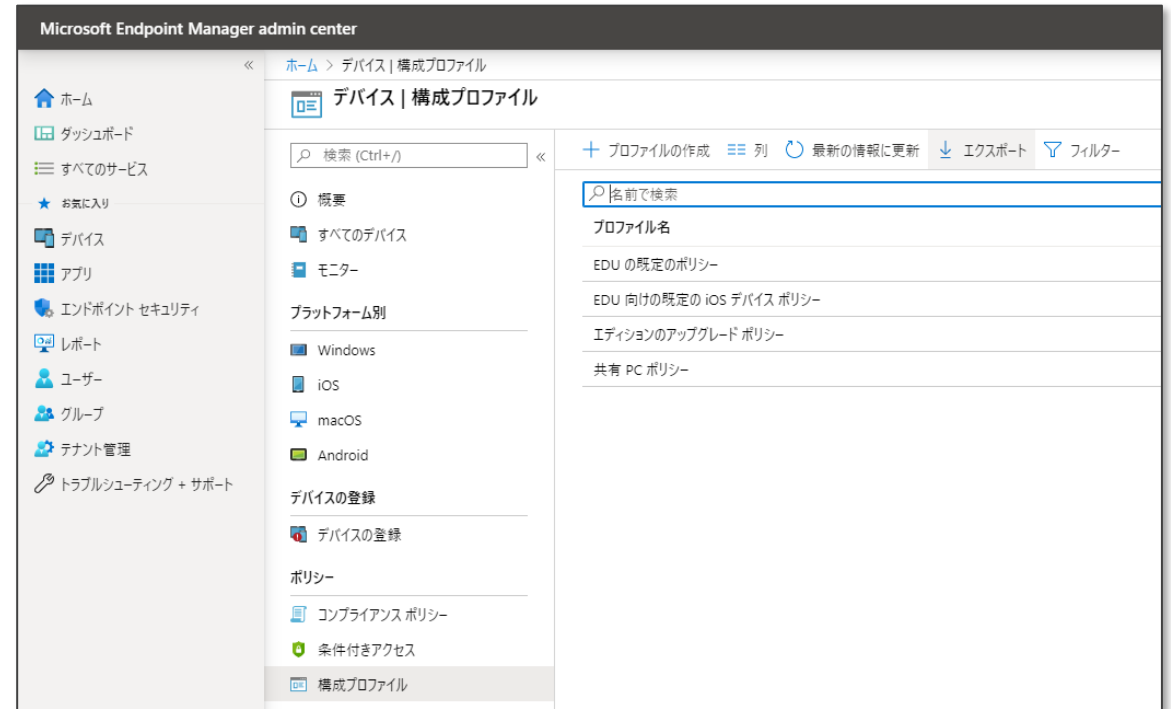
Intune for Education の管理画面

Microsoft Intune / Intune for Education の違い

教育機関向けの簡易ビューを提供しているのが「Intune for Education」
実態は「Microsoft Intune」が稼働しており、詳細な操作が必要な場合に活用が可能



Intune for Education の管理画面



Intune (Microsoft Endpoint Manager) 管理画面

Intune for Education 最小要件

サポートされている OS

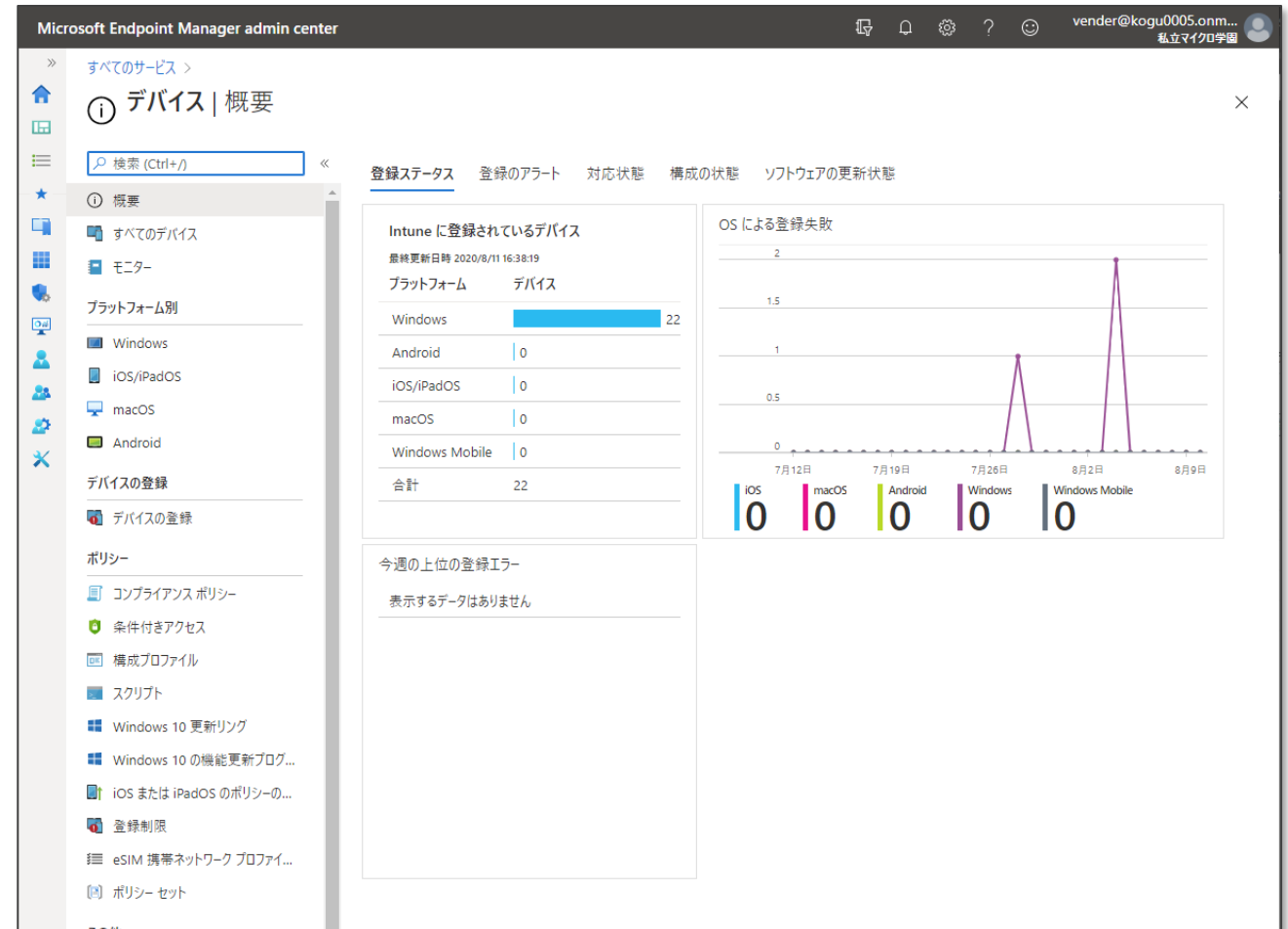
- Windows 10 (Home、Pro、Education、および Enterprise)
- Apple iOS 11.0 以降
- Apple iPadOS 13.0 以降
- Apple Mac OS X 10.12 以降
- Google Android 5.0 以降

サポートされているブラウザ

- Microsoft Edge (最新バージョン)
- Microsoft Internet Explorer 11
- Safari (最新バージョン、Mac のみ)
- Chrome (最新バージョン)
- Firefox (最新バージョン)

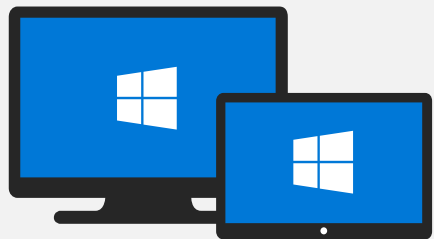
Intune でサポートされるオペレーティング システムとブラウザ

<https://docs.microsoft.com/ja-jp/mem/intune/fundamentals/supported-devices-browsers>



Intune の管理コンソール - ブラウザーでアクセスをする

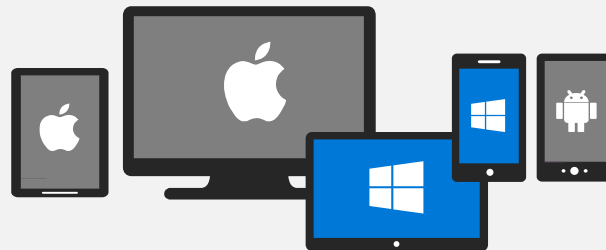
Intune for Education の優位性



シンプルな Windows 10 管理

効率化された登録、展開、管理

Microsoft Intune for Education は、学校の IT 管理者が Windows 10 デバイスを簡単に管理し、学校ですでに使用しているアプリケーションを管理・展開できるようにします。



完全な管理

クロスプラットフォームのサポート

Intune for Education には Intune 管理コンソールが含まれており、新たなインフラストラクチャやソフトウェアに投資することなく、エコシステム内の多様なデバイスを管理することができます。



Microsoft サービスとの統合

簡単なデバイスとユーザーの管理、 手頃な価格の教育機関向けのサービス

統合ソリューションの一環として、Intune for Education には、Microsoft のクラウドサービスとの完全な統合と Office 365 の管理の容易さが含まれています。

学ぶための条件づくり

Microsoft Educationは、デバイスの管理が簡単な、手頃な価格で安全な学習プラットフォームであり、コラボレーションツールやアプリなど、教師や学生が好む機能を備えています。

Intune for Education

Intune for Educationは、教育技術の管理と接続に特化して設計されたソリューションです。



シンプルでパワフル

Intune for Educationは、Office 365、Adobe Photoshop、STEM 用のアプリケーションなど、教室のニーズを満たし、学生の能力を引き出す強力なWindows 10デバイスやアプリケーションを簡単に導入して管理する方法を提供します。



Intune* は強力なアプリと複数のOSを管理します。

*Intune for Educationでは、企業向けのフルIntuneコンソールが利用可能です。



コネクテッドで未来にも対応

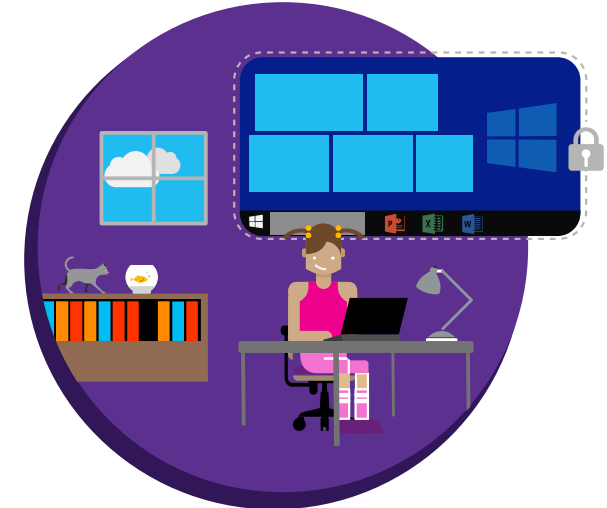
Intune for Education は、School Data Sync、Teams、OneNote と統合されており、シームレスに連携しているため、教師は生徒の創造性を引き出し、将来に備えたスキルを身につけることができます。



Windows 10 デバイスはオンラインとオフラインでの生産性を可能に

Azure Active Directory

Azure Active Directoryは、ID認証のための高速なシングルサインオンを可能にし、学生や教師が教育や学習の重要な作業に取り掛かることができるようになります。



セキュリティと生産性

Azure Active Directory は Intune for Education と連携しているため、学生は迅速にサインオンし、学校や自宅、オンラインおよびオフラインでの共同作業に必要なすべてのツールに安全にアクセスすることができます。



Azure ADは、学生の機密情報を保護し、決して収集されません。

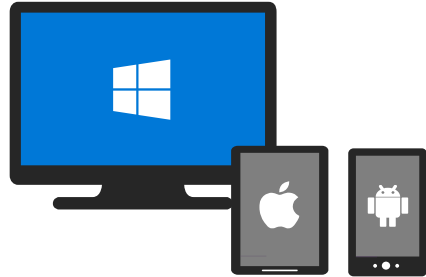


Intune for Education デバイス管理 (MDM)

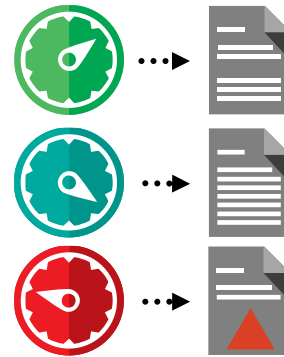
Intune によるデバイスの管理



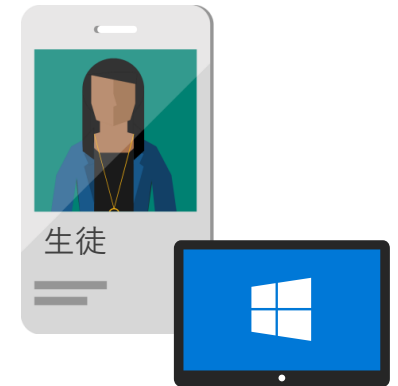
包括的なセキュリティ ポリシー
を各プラットフォームに強制



プラットフォームごとに幅広い構成
設定を利用できる



各設定について、適用可能性、
適合性、またはエラーの有無
に関するレポートを提供



ポリシーをユーザー グループや
デバイスグループに適用できる

Windows OS の初期設定イメージ

GIGAスクールのPCを想定した初期設定のポイント

構成プロファイルの展開

更新プログラム適用に関連する設定
Windows Update for Business

更新プログラム配信に関連する設定
配信の最適化

ハードディスク暗号化の強制
BitLocker

ウイルス対策ソフトの設定
Windows Defenderウイルス対策

各種デバイス制御
電源や機能の制限

ブラウザの設定
Microsoft Edge

認証・パスワード ポリシー

Office 365関連の設定
Onedrive for Business

ユーザーの標準設定

アプリの展開

Webブラウザの展開
Microsoft Edge

コミュニケーションツール
Teams

クライアントアプリケーション
Office 365 ProPlus

電子教科書

各種ユーティリティ
QRコードリーダーなど

各種リソース
フォントなど

ユーザープロファイルとデータの同期

ユーザーの個人設定
Enterprise State Roaming

ユーザーの個人データ
Onedrive for Business

ユーザーのブラウザプロファイル
Microsoft Edge

クラウド上の構成管理基盤、
および OneDrive for Business から
指定されたデバイスとユーザーに応じた
展開が行われる



Intune によるデバイスの管理

Intune for Education にて約 150 項目の設定
Intune を使用すれば約 300 項目の設定が可能

設定項目例

- ブラウザーの設定
- Bluetoothやカメラの利用許可/不許可
- Wi-Fiの設定 (SSID / Password)
- Microsoft Defender ウイルス対策の設定
- 更新プログラムのダウンロード/適用時間設定
- アプリの配信設定

Microsoft Intune でデバイス プロファイルを使用して
デバイスに機能と設定を適用する

<https://docs.microsoft.com/ja-jp/mem/intune/configuration/device-profiles>

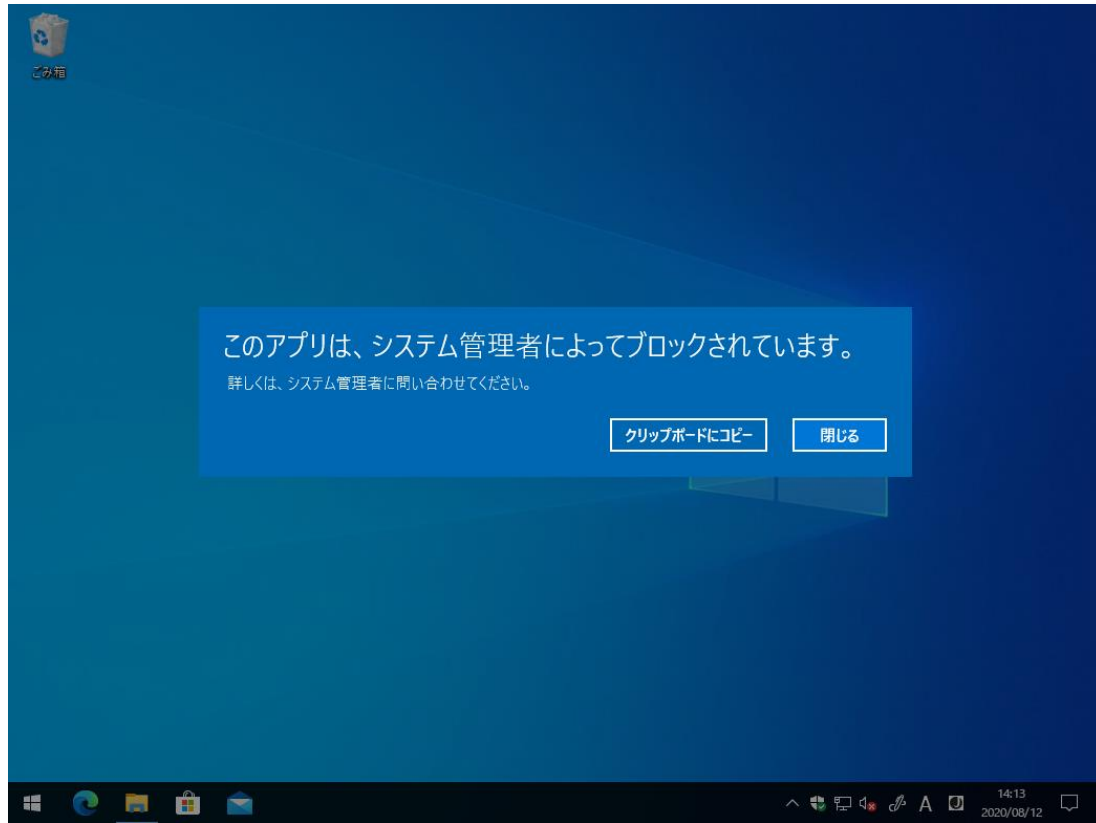
The screenshot shows the 'Intune for Education' interface. The top navigation bar includes the user 'admin@giga-school.ml' and the organization 'マイクロ学校'. The main content area is titled 'グループ - すべてのデバイス | Windows デバイスの設定'. Under the 'セキュリティ' (Security) section, the 'Windows Defender' settings are displayed. These settings include:

- Windows Defender 設定へのユーザーのアクセスをブロックする: ブロック
- リアルタイム監視を有効にする: 有効にする
- 動作の監視を有効にする: 有効にする
- 不審なファイルを Microsoft に送信するかユーザーに確認する: データを送信しない
- 実行するシステム スキャンの種類: クイック スキャン
- スケジュール日: 毎日
- スケジュールされた時刻: 午前 2:00
- キャッチアップ クイック スキャンのブロック: ブロックされていません。
- 毎日のクイック スキャンの時刻: 午前 2:00
- すべてのダウンロード ファイルをスキャンする: 有効にする
- Microsoft Web ブラウザーが実行するスクリプトをスキャンする: 有効にする
- フル スキャン中にリムーバブル ドライブをスキャンする: 有効にする
- ネットワーク上で開いたファイルをスキャンする: 有効にする
- フル スキャン中にリモートフォルダーをスキャンする: 有効にする

Intune for Education の「セキュリティ」項目の設定画面

Intune によるデバイスの管理例 – いたずらの防止

Intune でポリシーを設定することにより、デバイスへの制限をすることが可能



Intune for Education の設定により「Microsoft Store」起動をブロック

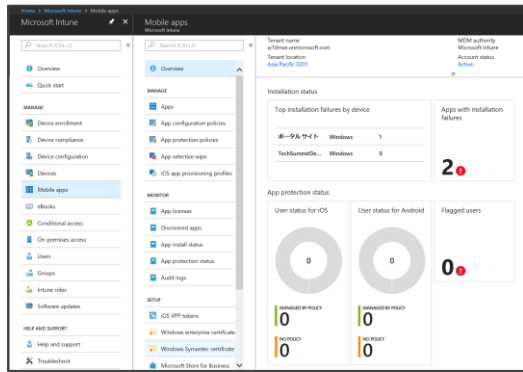


アプリのインストール時に管理者権限を要求

参考：MDM ポリシーとグループポリシー

Intune から Windows 10 デバイスに適用できる構成ポリシー、セキュリティポリシーは以下のように用意されており、MDM として新たに設計されたポリシー (Configuration Service Provider) に加えて、ADMX ベースポリシーを使用することで従来のグループポリシーで設定できる項目も設定可能

さらに PowerShell スクリプトを PC に展開して起動することが可能なので、広範囲の設定をPCに対して行うことが可能



Intune の管理コンソール

デバイスの設定・制限項目

- 予めUIが用意されている項目
- Configuration Service Providerの呼び出し
- ADMXベースポリシー

PowerShell スクリプトを端末上で実行



MDM で ADMX ベースのポリシーを有効にする

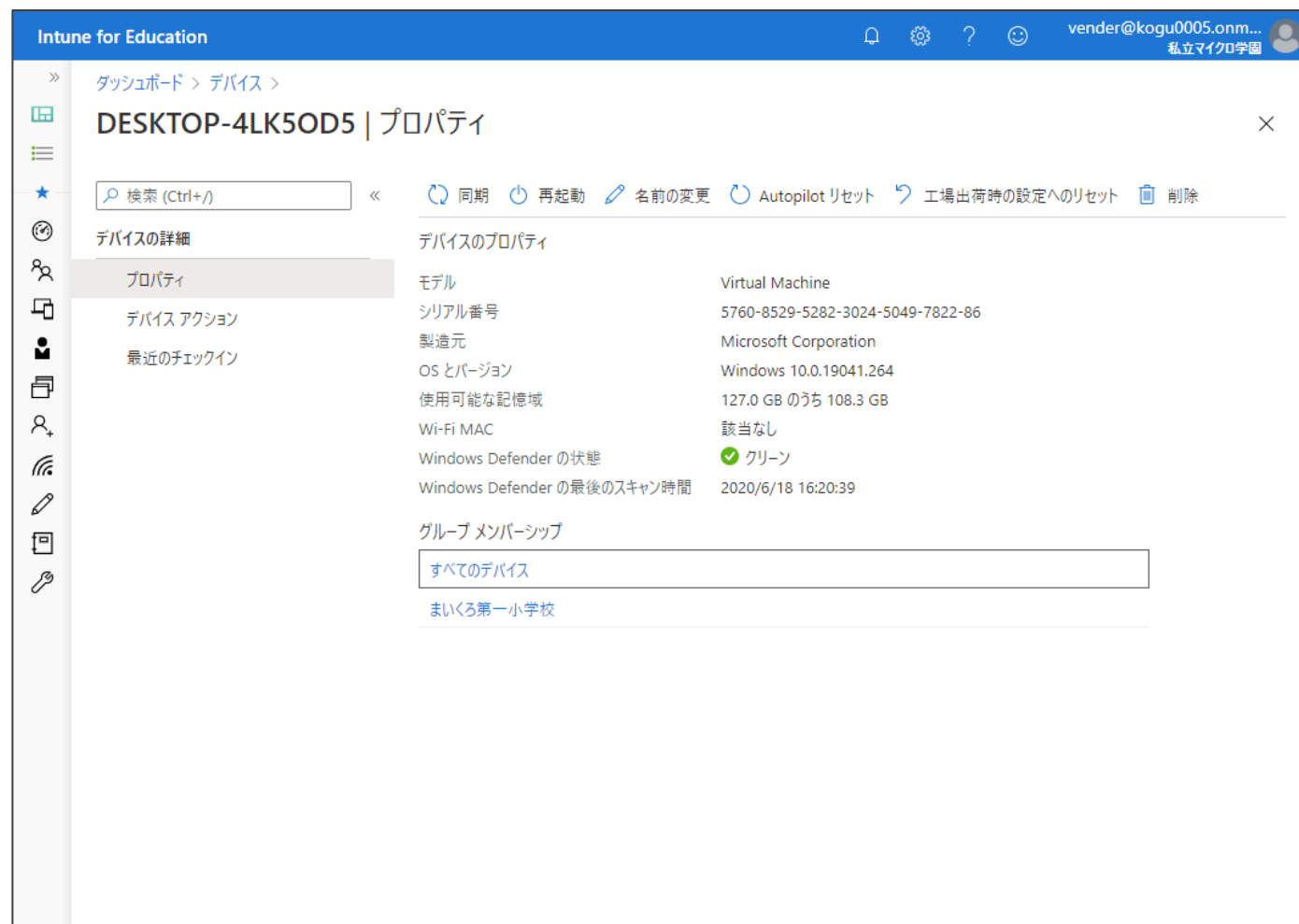
<https://docs.microsoft.com/en-us/windows/client-management/mdm/enable-admx-backed-policies-in-mdm>

Intune デバイスアクションのリモート実行

デバイス アクションをリモートで実行可能。
紛失したデバイスのデータの削除などが行える

アクション例

- ワイプ – 出荷時の既定の設定に
- 削除 – Intune ポータルからデバイスの削除
- 再起動 – デバイスの再起動
- スキャン – ウイルス対策のスキャンの実行
- ウイルス対策の更新 – 最新の定義ファイルに



Intune を使ったデバイス アクションのリモート実行

<https://docs.microsoft.com/ja-jp/mem/intune/remote-actions/>

Intune for Education の「セキュリティ」項目の設定画面

Intune によるアプリ配信

① アプリを入手

業務用のアプリなどのパッケージを準備



LOB Apps

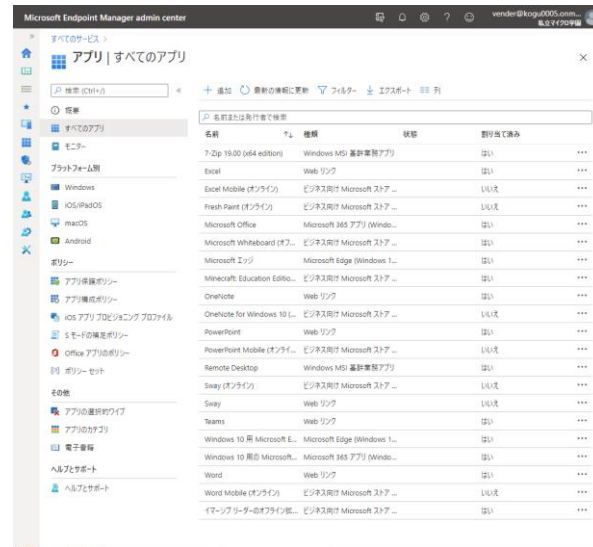
Microsoft Store アプリを選択



Store for Business

② アプリの配信設定

管理者が Intune の管理コンソールにて
アプリの配信設定を実施



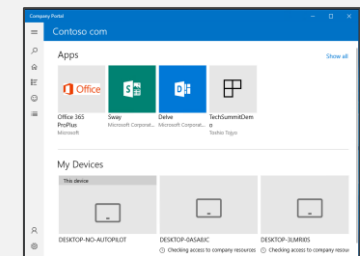
Intune の管理コンソール

③ インストール

「必須」と設定すると自動的にインストール



アプリをポータルアプリ上に一覧表示
ユーザーが選択してインストール可能



Company portal app

Intune によるアプリ配信

様々な種類のアプリ展開シナリオをサポート
アプリをユーザーとデバイスに割り当てることが可能

アクション例

- デスクトップアプリ (MSI)
- Microsoft Store アプリ
- Web アプリ
- PowerShell スクリプト
- Win32 アプリ

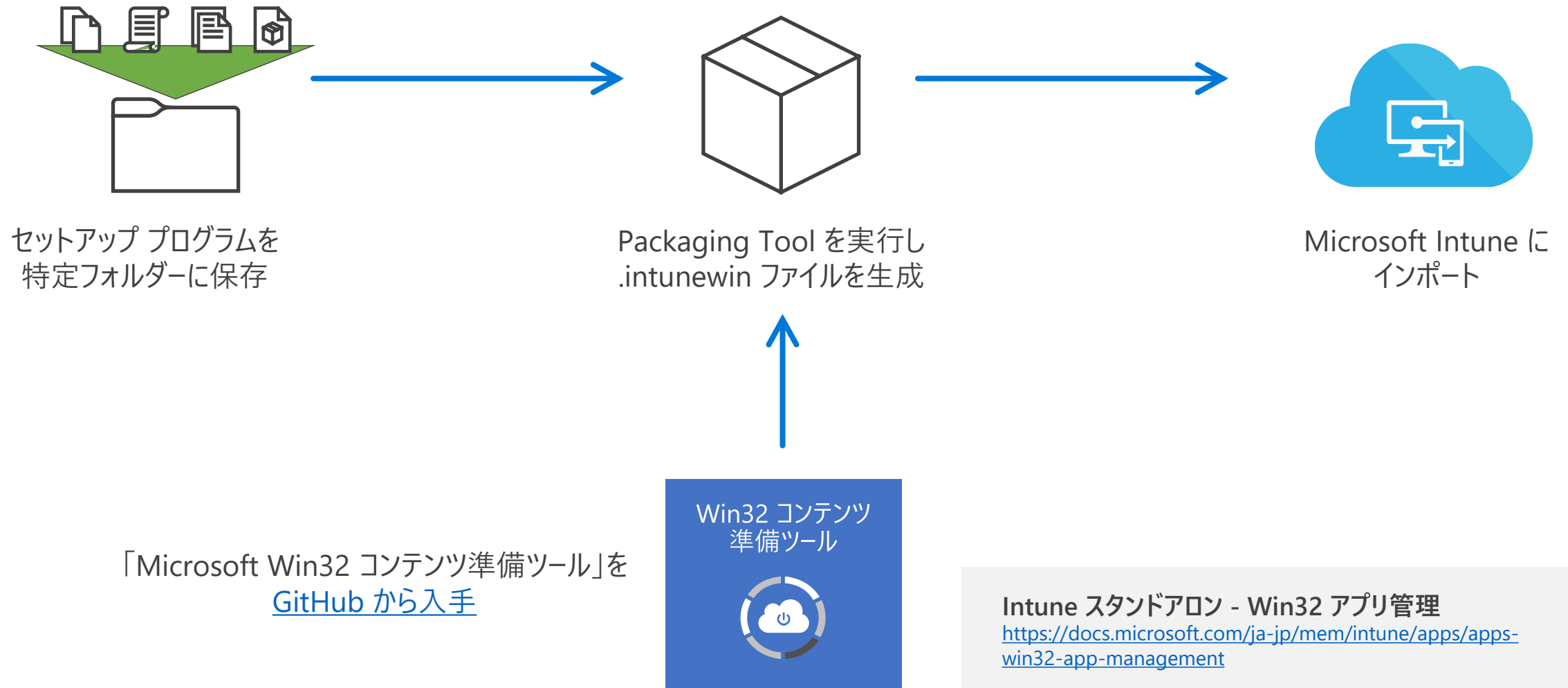
Microsoft Intune を使用する Windows 10 アプリの展開

<https://docs.microsoft.com/ja-jp/mem/intune/apps/apps-windows-10-app-deploy>

名前	アプリの種類	割り当て済み	最終変更
Excel	Web アプリ	いいえ	2020/7/9 11:01:42
Fresh Paint	Microsoft Store アプリ	いいえ	2020/7/19 0:23:54
Microsoft Whiteboard	Microsoft Store アプリ	いいえ	2020/8/11 9:45:29
Minecraft: Education Edition	Microsoft Store アプリ	いいえ	2020/8/7 12:06:45
OneNote	Web アプリ	いいえ	2020/7/9 11:01:42
OneNote for Windows 10	Microsoft Store アプリ	いいえ	2020/7/19 0:23:55
PowerPoint	Web アプリ	いいえ	2020/7/9 11:01:42
Schoology Learning	Web アプリ	いいえ	2020/7/9 11:01:42
Sway	Web アプリ	いいえ	2020/7/9 11:01:42
Sway	Microsoft Store アプリ	いいえ	2020/7/19 0:23:54

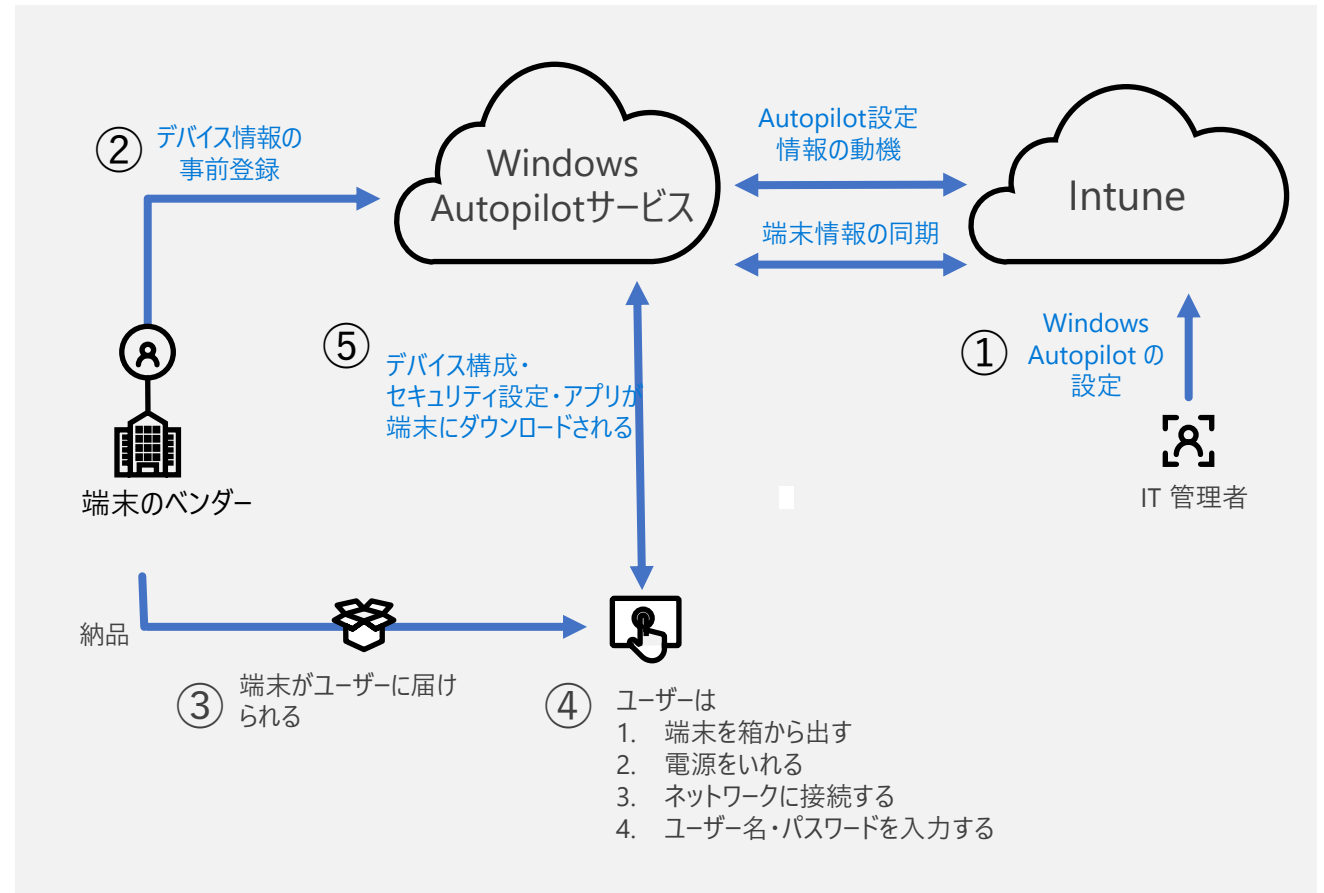
Intune for Education の「アプリ」の設定画面

Intune による Win32 アプリ配信



Windows の初期展開 - Windows Autopilot

- Windows 10 端末の初期設定時に、自動的に Azure AD に参加し、Intune にエンロールする機能
- ユーザーは、新しく届いた端末に電源を入れ、ネットワークに接続し、ユーザー名・パスワードを入力するだけで、端末の設定・アプリのインストールはすべて自動的に行われる
- 通常の OA 用端末のほか、特定のアプリのみを実行する Kiosk 端末の設定も可能
- SCCM との連携により、Windows 7, 8.1からのアップグレードと Windows 10 の設定をシームレスに行うことも可能



Windows 10 の展開手法の選択 – Autopilot

クラウドを活用した 3 つのステップ



OEM・リセラーによる作業

顧客の Azure テナントに新規デバイスを自動登録
デバイス グループの作成のためのデバイスの関連づけ
顧客が指定したラベルによってデバイスをタグ付け
オプションでイメージをプリインストールして提供



管理者による作業

プロパティ設定
(配置モード、Azure AD への参加の種類など)
Out-of-box experience (OOBE) 設定
(プライバシー設定、ユーザー アカウントの種類など)

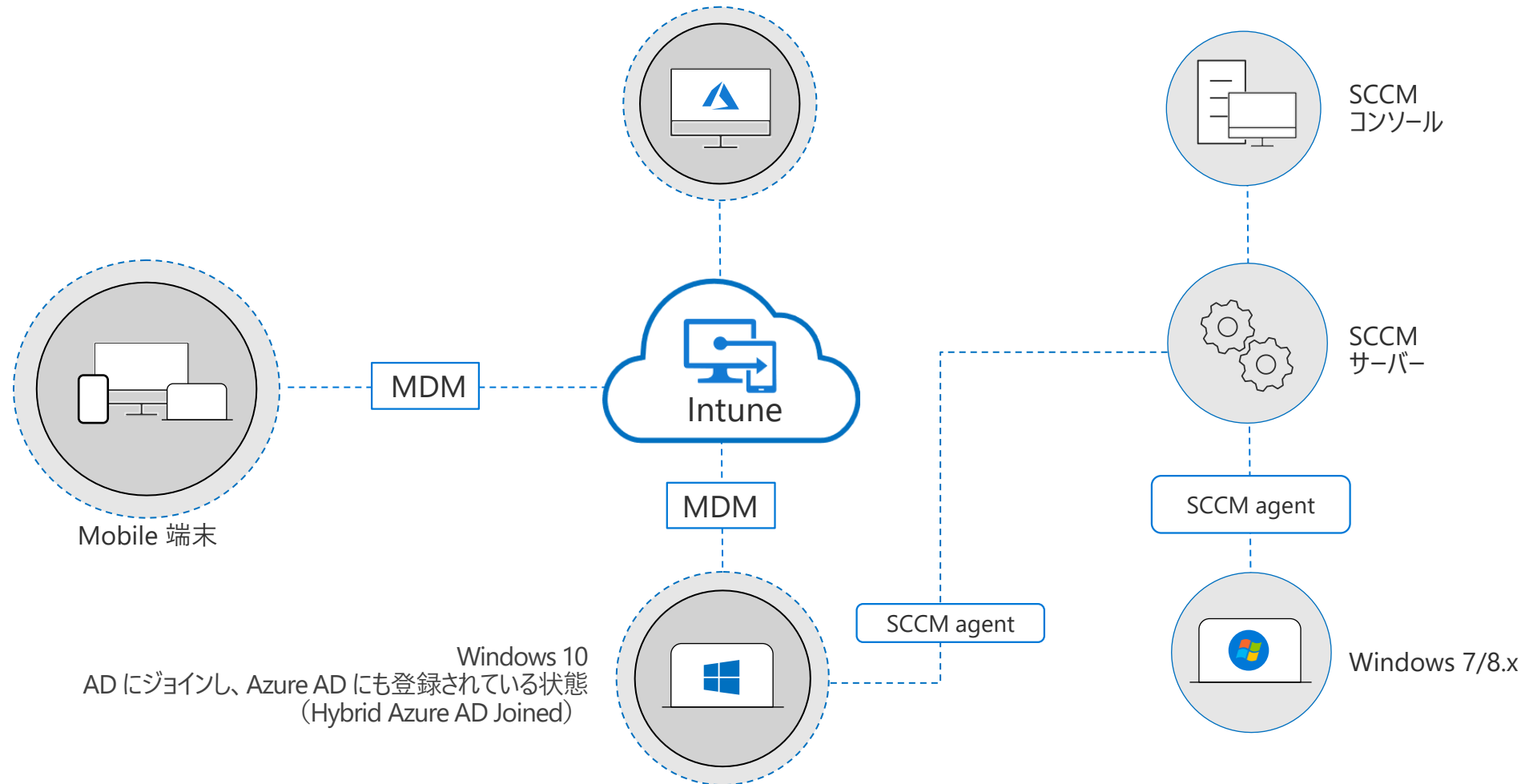


ユーザーによるセルフサービス

箱から取り出し電源を入れる
キーボードと言語の設定

Configuration Manager との共同管理

オンプレミス Active Directory + Configuration Manager とクラウドの Azure AD + Intune の両方から Windows 10 を管理することが可能
オンプレミス側からの管理が優先している状態でも、リモートワイプなどの MDM (Intune) の機能は有効





Intune for Education 更新の管理

Intune for Education による Windows 更新の管理

Windows Update による自動更新の適用タイミングの調整が可能

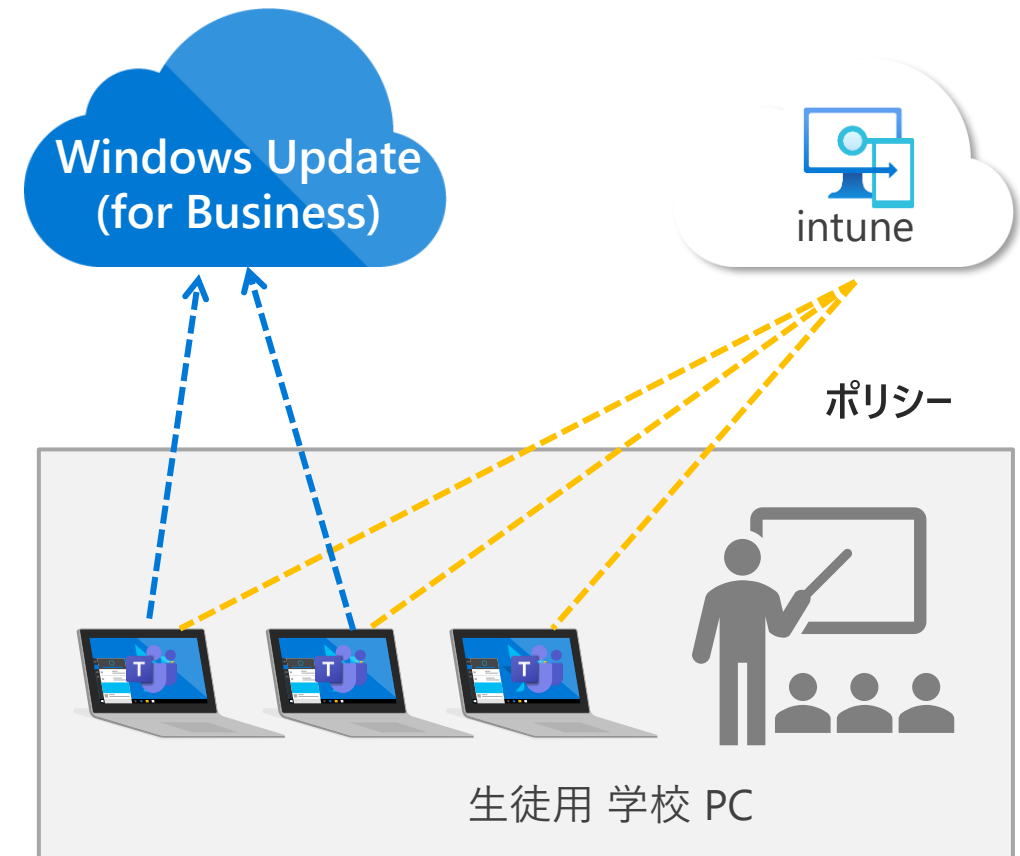
Intune for Education による管理

管理下のデバイスに対してアップデートのタイミングを制御



The screenshot shows the Intune for Education console interface. The main content area is titled "グループ - Ring 1 | Windows デバイスの設定" (Group - Ring 1 | Windows Device Settings). Under the "更新" (Updates) section, there are several settings for Windows Update, including "プランチ準備レベル" (Planned Readiness Level) set to "ユーザー定義" (User-defined), "更新プログラムが利用可能になるタイミングの詳細" (Details of when updates become available), and "機能更新プログラムが利用可能になった後、延期する日数" (Number of days to defer after a feature update becomes available). A callout bubble points to these settings.

例えば、
昼間はアップデートしないように、
夜間にアップデートを設定する



Windows 10 の更新プログラム

2 種類の更新プログラムを提供

品質更新プログラム

(QU : Quality Update)

1 か月に 1 度

約 100 MB ~ 400 MB 弱

- 従来の更新プログラムに相当
- 品質の向上とセキュリティの修正を目的
- 複数の問題を包括した 1 つの更新プログラム
- 各バージョンごとに 18 ヶ月間リリース

機能更新プログラム

(FU : Feature Update)

半年に 1 度

差分更新や圧縮にて 約 2GB 程度

- 従来のサービスパックに相当
- 新機能の追加や改善を目的
- サービスチャネルによる適用タイミングの選択

更新プログラムの配信オプション ① – グループ分け

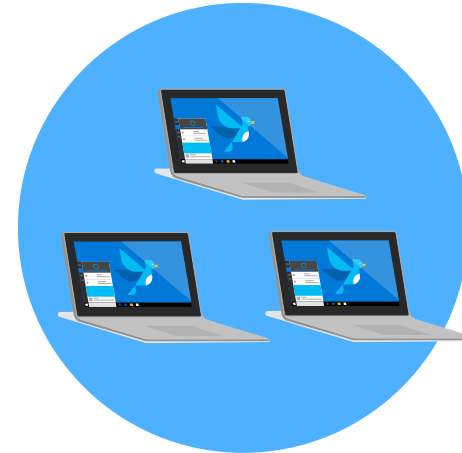
グループを分けて配信

クライアントをいくつかのグループに分け、配信を段階的に行う。

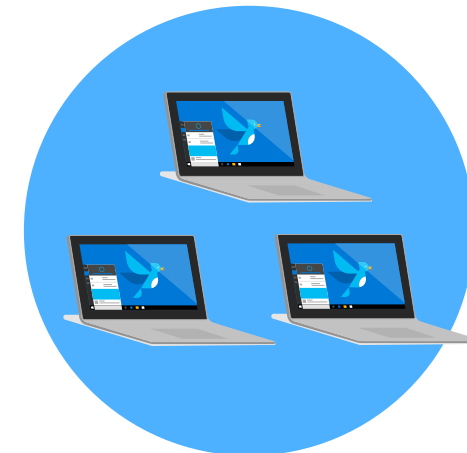
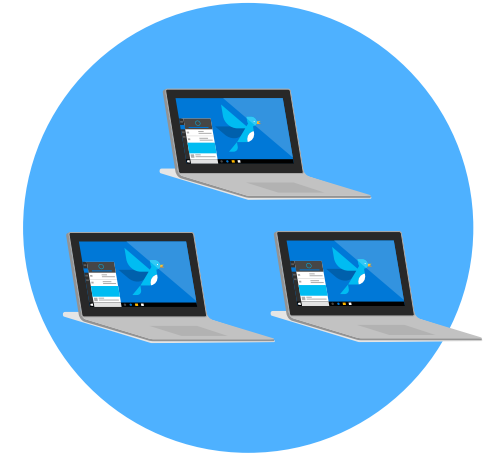
ダウンロードを行うクライアントの台数を制限することで、ネットワーク圧迫のピークを分散させる。
またバージョンアップ時の問題発生などのリスクに備える

Intune で Windows 10 ソフトウェア更新プログラムを管理する
<https://docs.microsoft.com/ja-jp/mem/intune/protect/windows-update-for-business-configure>

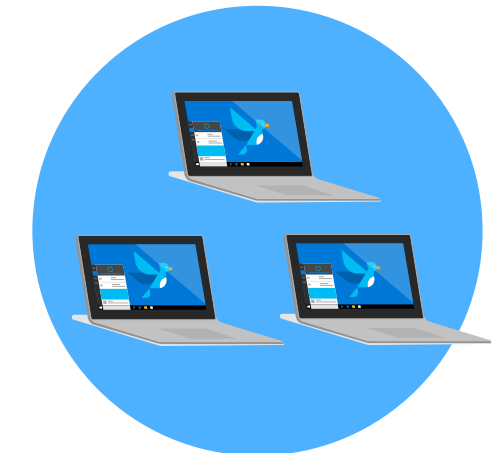
グループ A : 1 週目に配信



グループ B : 2 週目に配信



グループ C : 3 週目に配信



グループ D : 4 週目に配信

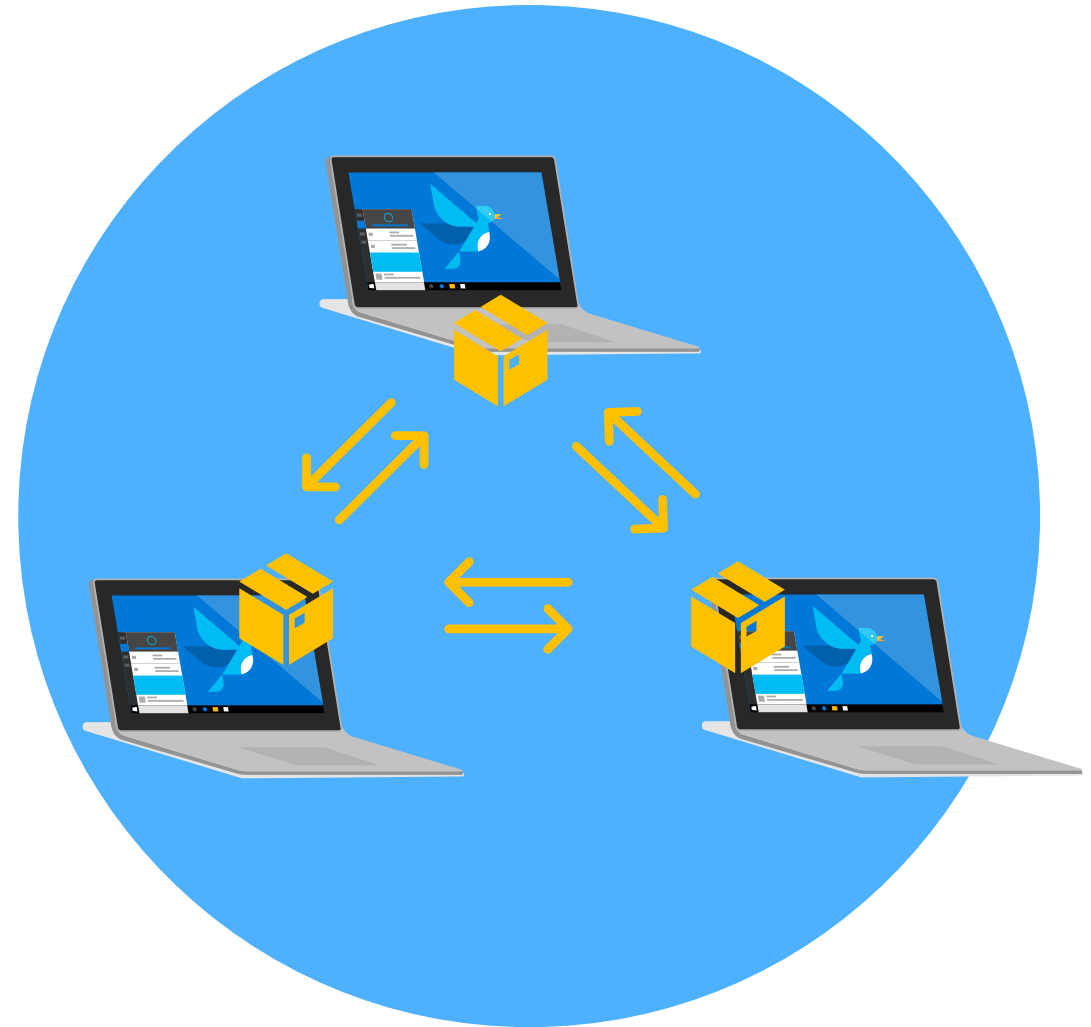
更新プログラムの配信オプション ② – キャッシュの共有

キャッシュの共有

既に更新プログラムをダウンロードした端末から、更新プログラムのキャッシュ (断片) を共有して取得
近くの端末から効率よく更新プログラムを配信可能

また帯域制限なども設定することが可能で、
ネットワークの負荷がかからないようにコントロールが可能

Windows 10 更新プログラムの配信の最適化
<https://docs.microsoft.com/ja-jp/windows/deployment/update/waas-delivery-optimization>



ダッシュボード > グループ >

グループ – Ring 1 | Windows デバイスの設定

- ダッシュボード
- すべて表示
- お気に入り
- 高速構成
- グループ
- デバイス
- ユーザー
- アプリ
- 登録マネージャー
- Wi-Fi プロファイル
- テスト プロファイル
- レポート
- テナントの設定

- 概要
- グループのメンバー
 - デバイス
 - ユーザー
- アプリ
 - Web アプリ
 - Windows アプリ
 - iOS アプリ
- 設定
 - Windows デバイスの設定
 - iOS デバイスの設定
- 管理者
 - このグループの管理者
 - このグループによる管理
- 履歴
 - グループの履歴

保存 変更を破棄

更新

ランチ準備レベル 更新プログラムが利用可能になるタイミングの詳細	ユーザー定義
更新プログラムをインストールする方法とタイミングを構成する	構成されていません
機能更新プログラムが利用可能になった後、延期する日数 (0 - 365)	0
品質更新プログラムが利用可能になった後、延期する日数 (0 - 30)	0
アンインストール ファイルを削除するまでの日数 (2-60)	構成されていません
Windows Update 通知	構成されていません
手動の Windows Update をブロックする	構成されていません
Windows Update の一時停止をブロックする	構成されていません
生徒が Windows 10 プレリリース機能を参照することを許可する	構成されていません
配信の最適化モード ダウンロード モード オプションに関する詳細	ユーザー定義

エディションのアップグレード

このグループに割り当てられているアップグレード ポリシーを詳しく見る

+ 新しいエディションのアップグレード ポリシーを割り当てる

アップグレード プロファイル名	ポリシー	モード
Edition Upgrade Policy	構成されていません	S モードの切り替え
		S モードのままにする

- ユーザー エクスベリエンス
- テスト プロファイル

Intune for Education

Windows の更新の設定画面

Office 365 の更新管理

基本は自動更新

月例のプログラムでは、数十 MB ~ 100 MB 弱
という程度であり自動更新をする前提

初期設定のみを行い、自動更新を行う

Microsoft 365 アプリ用更新プログラムのダウンロード サイズ
<https://docs.microsoft.com/ja-jp/officeupdates/download-sizes-microsoft365-apps-updates>

更新プログラム チャンネルとターゲット バージョンの設定を使用して、
Microsoft Intune 管理用テンプレートで Office 365 を更新する
<https://docs.microsoft.com/ja-jp/mem/intune/configuration/administrative-templates-update-office>



Microsoft Endpoint Manager admin center

ホーム > デバイス | 構成プロファイル >
プロフィールの作成
Administrative Templates

基本 構成設定 3 スコープタグ 4 割り当て 5 確認および作成

すべての設定
▼ コンピューターの構成
▼ Microsoft Office 2016 (マシン)
更新
▼ ユーザーの構成

更新

コンピューターの構成/Microsoft Office 2016 (マシン)/更新

項目の検索とフィルタ...

設定名	↑ ↓	状態
Bing を既定の検索エンジンに設定する Bing...		構成さ
BITS を優先する		構成さ
Microsoft Teams を Office の新規インス...		構成さ
Office 2019 を Office 365 ProPlus にアップ...		構成さ
Office 365 クライアント管理		構成さ
Office が特定のバージョンに更新されないよう...		構成さ
Office の更新プログラムのダウンロードとインス...		構成さ
オンライン修復		構成さ
ターゲット バージョン		構成さ
チャンネルの更新		構成さ
更新の有効/無効を切り替えるオプションを非...		構成さ
更新プログラムのパス		構成さ
更新期限		構成さ
更新通知の非表示		構成さ
自動更新を有効にする		構成さ

このポリシー設定では、Office の更新プログラムを直接 Office Content Delivery Network (CDN) から取得するよう設定済みの場合に、どの更新チャンネルから取得するかを制御します。

このポリシー設定を有効にすると、Office の更新プログラムは管理者が選択した更新チャンネルから取得されます。

このポリシー設定を無効にした場合や構成しなかった場合は、Office の更新プログラムは既定のチャンネルから、または Office 展開ツールで指定されたチャンネルから取得されます。どれが既定のチャンネルであるかは、インストール済みの Office 製品によって決まります。

重要: このポリシー設定が適用されるのは、Office 365 のプランに付属する Office クライアント (Office 365 ProPlus など) のみです。このポリシー設定は、Office 365 のプランに付属する製品である Visio と Project にも適用されます。このポリシーは、Windows インストーラ (MSI) を使用してインストールされた Office 製品には影響しません。

設定の種類: デバイス
サポート対象: Windows Server 2008 R2、Windows 7 またはそれ以降

有効 無効 構成されていません

チャンネル名:
月次チャンネル

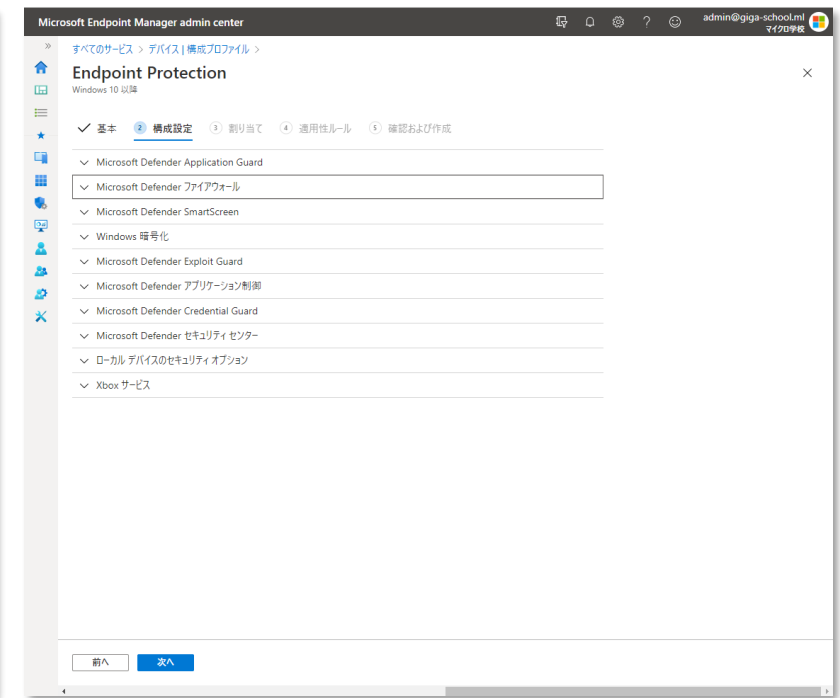
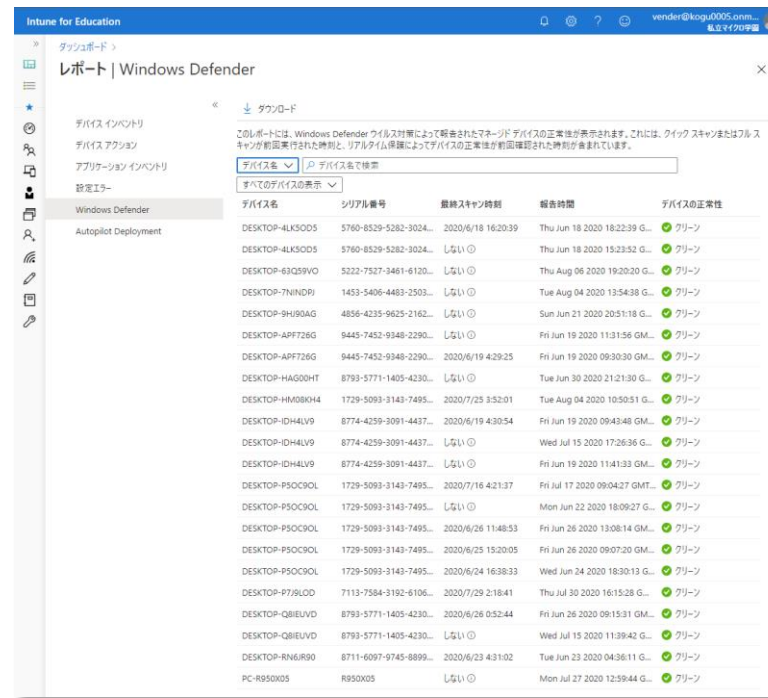
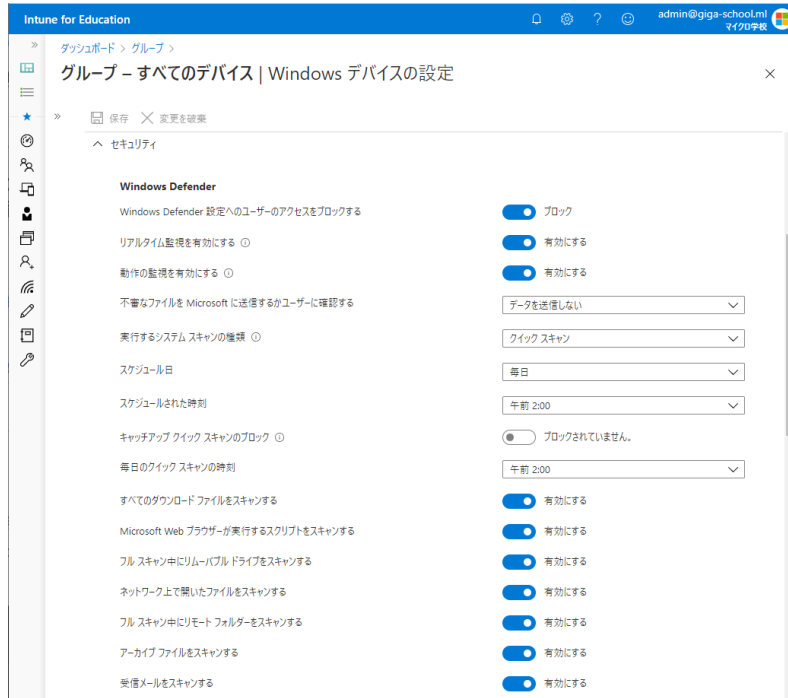
前へ 次へ OK

Intune (Microsoft Endpoint Manager) 管理画面でのプロフィールの作成



Intune for Education による セキュリティの管理

Intune for Education によるセキュリティ管理



Intune for Education でのセキュリティ設定

Microsoft Defender ウィルス対策や
Microsoft Defender SmartScreen の設定は
Intune の管理コンソールから設定が可能

Intune for Education のレポート

Microsoft Defender ウィルス対策の
現状の確認は Intune のレポートより確認可能

※ 過去のそれぞれの端末のウイルス感染状況の確認や、
ウイルス感染時のメール通知などが必要な場合には、
別途製品 (Microsoft Defender ATP 等) が必要となります。

Microsoft Endpoint Manager での設定

Microsoft Endpoint Manager Admin Center
から intune の設定を実施することにより、
Intune for Education のメニューには表示されない、
より詳細な設定を行うことが可能



Microsoft Defender ウィルス対策

メール、アプリ、クラウド、Web 上のウイルス、マルウェア、スパイウェアなどのソフトウェア脅威に対して、
包括的・継続的に、かつリアルタイムでデバイスを保護

- Windows 10 標準搭載
- 無償利用可能
- 高度な機械学習モデル、および汎用的でヒューリスティックなテクノロジー、クラウド型保護を利用して、未知のウイルスもリアルタイムに検出
- Microsoft 製品のインフラを活用して管理が可能
※ 管理製品の使用のためのライセンスは別途必要

Windows 10、Windows Server 2016、Windows Server 2019 での次世代の保護

<https://docs.microsoft.com/ja-jp/windows/security/threat-protection/microsoft-defender-antivirus/microsoft-defender-antivirus-in-windows-10>



Intune (Microsoft Endpoint Manager) による管理

Intune for Education より詳細な設定や確認が必要な場合は Intune のコンソールから設定が可能

脅威エージェントの状態

Defender ウイルス対策のリアルタイム保護の状況や AV エンジンや定義のバージョンなどの詳細ステータスを確認することが可能



注意：アラートについて

Defender ウイルス対策により「ウイルスを検知した」という旨のアラートの情報の出力やそれをメール通知するという機能は Intune にはありません。Education においては、各端末で自動対処・駆除までが想定されています。もし、アラートを監視したいなどのさらなる要望には、Microsoft Defender ATP をご検討いただいています。

Microsoft Endpoint Manager admin center

ホーム > デバイス > モニター > 脅威エージェントの状態 | クリーン (4)

検索 (Ctrl+/) 列 エクスポート

脅威エージェントの状態

デバイス	リアルタイム保護	AV エンジンのバージョン	定義のバージョン
DESKTOP-VSF4250	有効	1.1.17100.2	1.317.1512.0
Gibson-Client01	有効	1.1.17200.2	1.317.1684.0
Gibson-Client01	有効	1.1.17000.7	1.315.1117.0
Gibson-Client02	有効	1.1.17100.2	1.317.1684.0

列

- デバイス
- ユーザー
- 最後のチェックイン
- リアルタイム保護
- ネットワークの保護
- AV エンジンのバージョン
- 定義のバージョン
- クイック スキャンの期限が過ぎています
- フル スキャンの期限が過ぎています
- 定義の更新
- デバイスの再起動が必要です
- フル スキャンが必要
- Defender バージョン
- クイック スキャンの時間
- フル スキャンの時間
- クイック スキャンの定義のバージョン
- フル スキャンの定義のバージョン

Intune の管理画面 [デバイス] - [モニター] - [脅威エージェントの状態]

Microsoft Defender ファイアウォール

Windows に標準搭載されたパーソナルファイアウォール
Intune で設定の管理が可能

- Windows 10 標準搭載
- 無償利用可能
- 不正な通信からのブロック
(送受信、プログラム、ポート、IP アドレス等)
- プロファイルごとに設定が可能
(ドメイン、プライベート、パブリック)

セキュリティが強化された Windows Defender ファイアウォール
<https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security>



Windows 10 : [Windows セキュリティ] – [ファイアウォールとネットワーク保護]

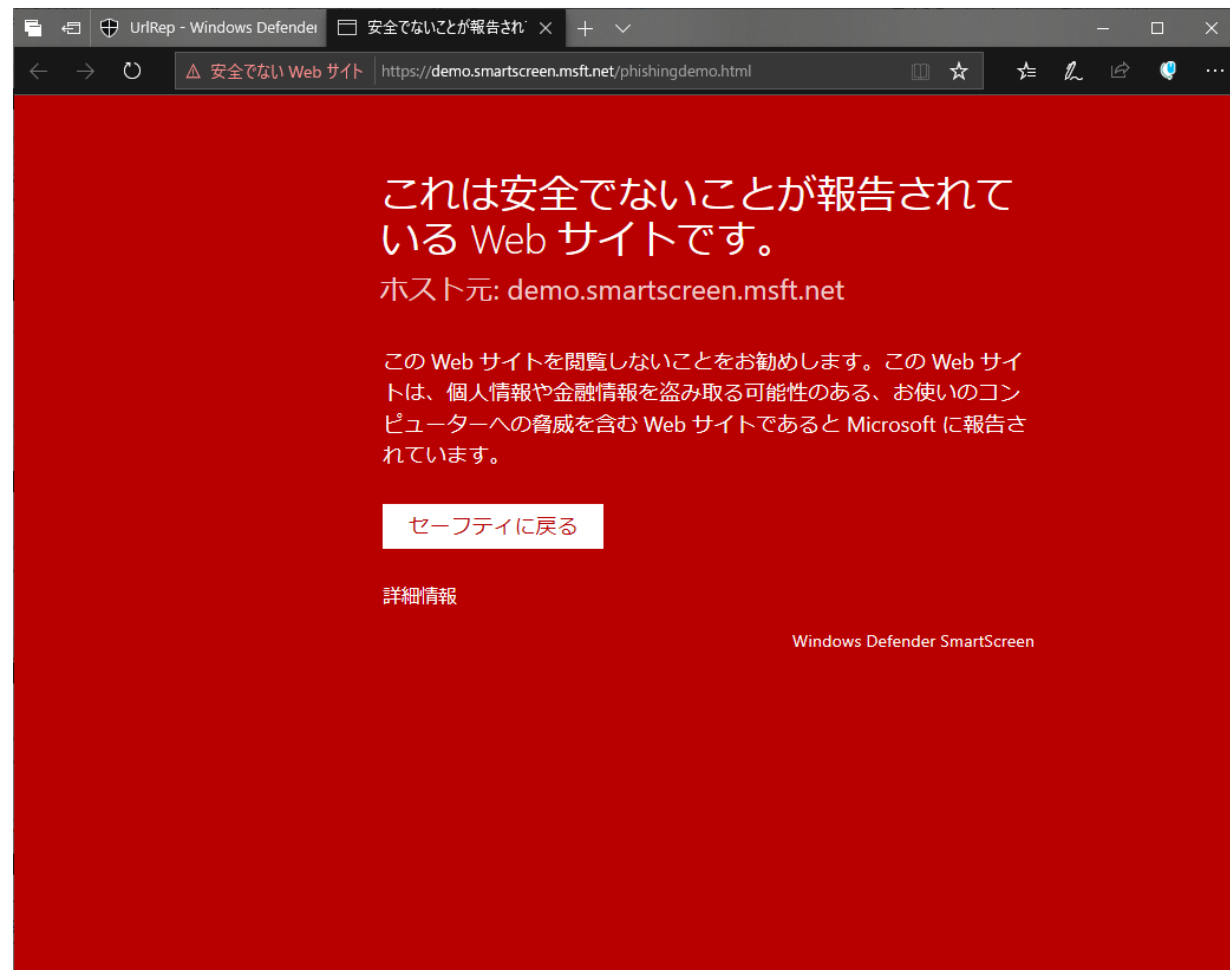
Microsoft Defender SmartScreen

報告されているフィッシング詐欺サイトおよび悪意のあるサイトを動的な一覧と照合し、警告を表示
Intune で設定の管理が可能

- Windows 10 標準搭載
- 無償利用可能
- 不正な Web サイトからの保護
- 不正な Web サイトからダウンロードされたファイルをブロック

Windows Defender SmartScreen

<https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-defender-smartscreen/windows-defender-smartscreen-overview>



Microsoft Defender SmartScreen で Web サイトをブロックした様子



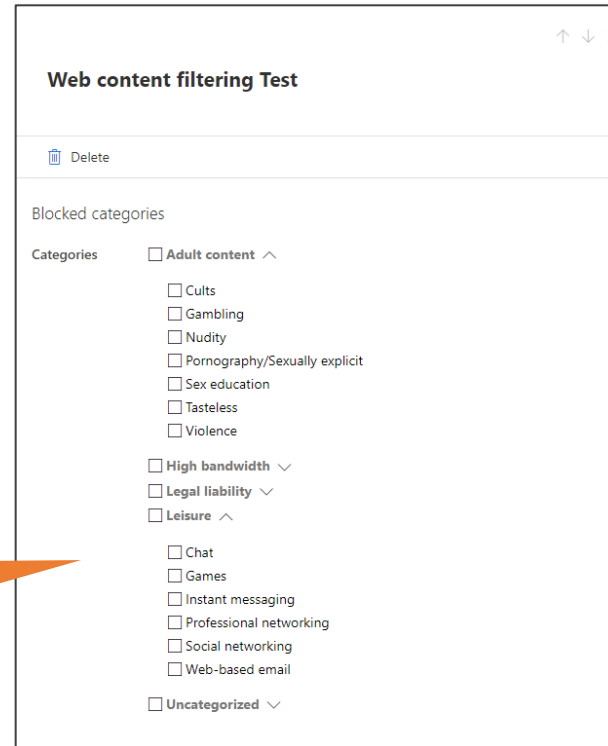
Microsoft Defender ATP

生徒向けお勧め機能 - Web コンテンツフィルタリング (Preview)

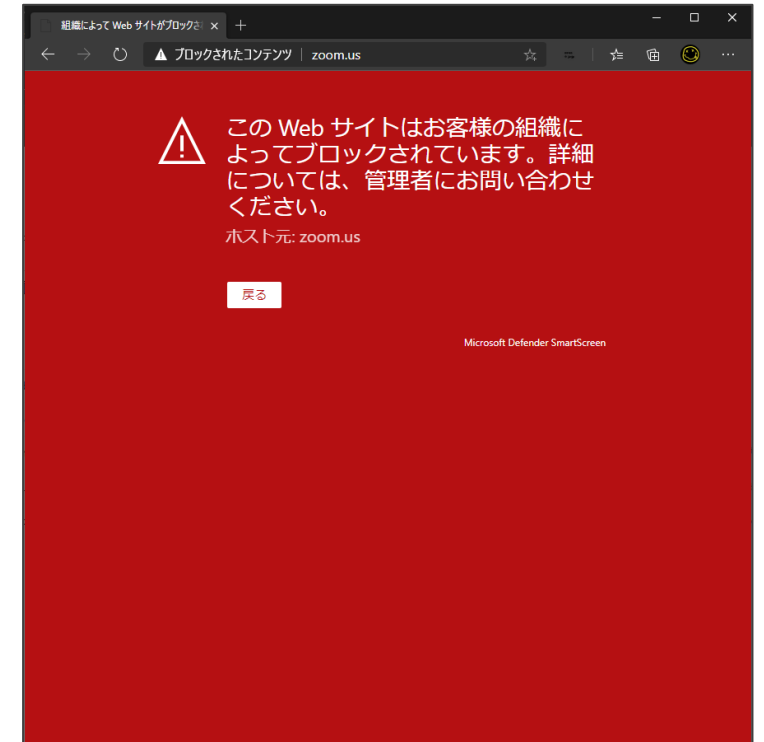
Cyren 社のインテリジェンスを使用し、望ましくない Web ページからの保護が可能
特に難しい設定はなく、Defender ATP のコンソールからカテゴリを選択するのみ。

例えば、、、

- アダルトサイト
- 動画サイト
- ゲーム関連
- SNS



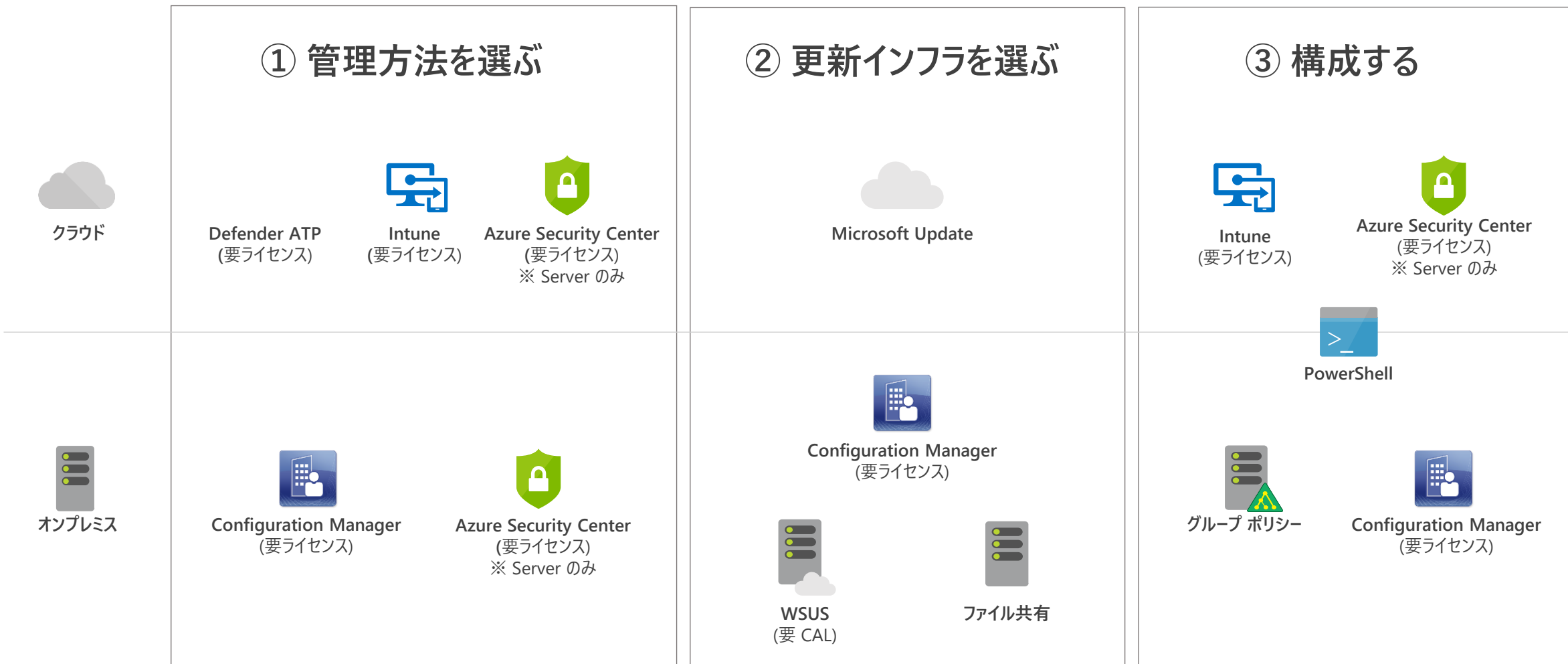
ブロックしたいカテゴリを選ぶだけ



ブロック動作サンプル

Microsoft Defender ウイルス対策 – 企業での管理

Microsoft Defender ウイルス対策自体をクライアント PC で利用するのは無償
一方で企業が各 PC 上での管理やアラートの把握には有償ソリューションが必要



Microsoft Defender ウィルス対策 - 展開・管理手段

	クライアント ライセンス	展開	構成	レポート・管理
Windows 10	OS 標準 (ライセンス不要)	OS 標準 (インストール済み)	<ul style="list-style-type: none"> ■ Configuration Manager ■ Group Policies ■ PowerShell ■ Azure Security Center 	<ul style="list-style-type: none"> ■ Microsoft Defender ATP ■ Configuration Manager ■ Microsoft Intune*1
Windows 8.1 Windows 7	Configuration Manager With Endpoint Protection	Configuration Manager	<ul style="list-style-type: none"> ■ Configuration Manager 	<ul style="list-style-type: none"> ■ Microsoft Defender ATP ■ Configuration Manager
Windows Server 1803 Windows Server 2019	OS 標準 (ライセンス不要)	OS 標準 (インストール済み)	<ul style="list-style-type: none"> ■ Configuration Manager ■ Group Policies ■ PowerShell ■ Azure Security Center 	<ul style="list-style-type: none"> ■ Microsoft Defender ATP ■ Configuration Manager ■ Azure Security Center
Windows Server 2016	OS 標準 (ライセンス不要)	OS 標準 (インストール済み)	<ul style="list-style-type: none"> ■ Configuration Manager ■ Group Policies ■ PowerShell ■ Azure Security Center 	<ul style="list-style-type: none"> ■ Microsoft Defender ATP ■ Configuration Manager ■ Azure Security Center
Windows Server 2012 R2	Configuration Manager With Endpoint Protection	Configuration Manager	<ul style="list-style-type: none"> ■ Configuration Manager ■ Azure Security Center 	<ul style="list-style-type: none"> ■ Microsoft Defender ATP ■ Configuration Manager ■ Azure Security Center
Windows Server 2012 Windows Server 2008 R2	Configuration Manager With Endpoint Protection	Configuration Manager	<ul style="list-style-type: none"> ■ Configuration Manager ■ Azure Security Center 	<ul style="list-style-type: none"> ■ Microsoft Defender ATP ■ Configuration Manager ■ Azure Security Center

*1 Microsoft Intune もしくは、Microsoft Endpoint Manager Admin Center で コンプライアンス ポリシーによるウィルス対策の適合状況の確認のみ可能

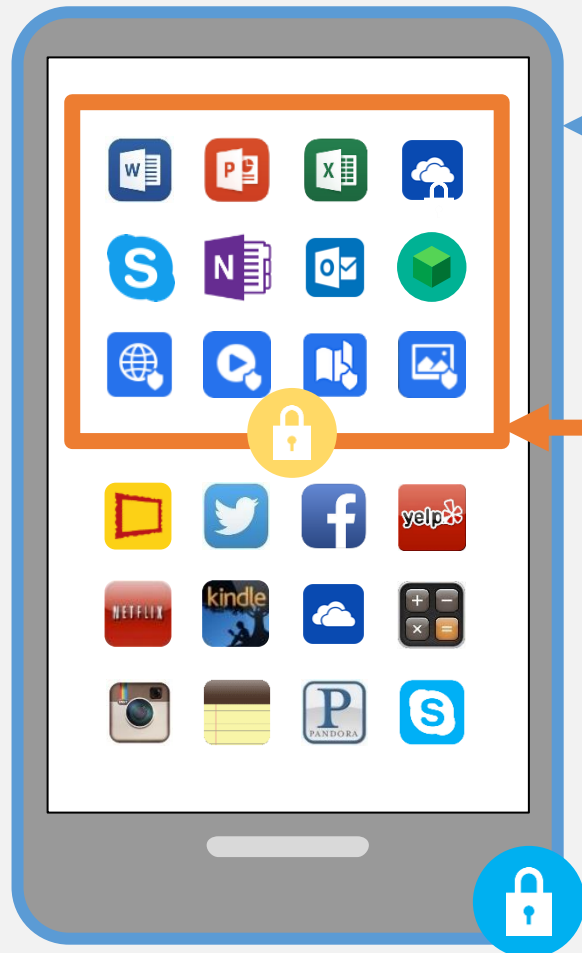


Intune for Education アプリケーション管理 (MAM)

モバイルのアプリとデータは保護できていますか？

利用者

IT 管理者



デバイスのセキュリティポリシー

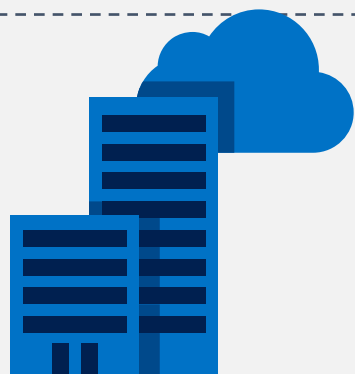
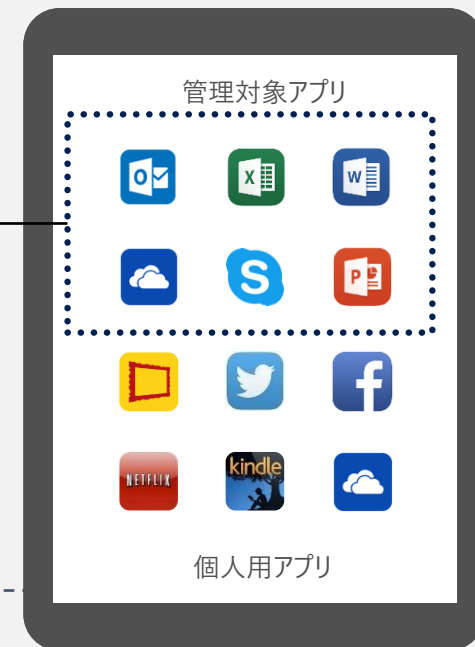
モバイルデバイスの管理
(MDM)

アプリのセキュリティポリシー

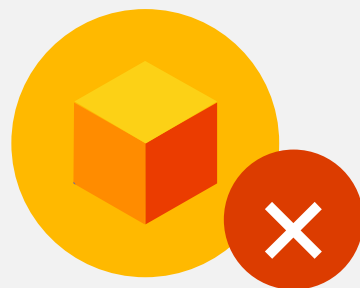
モバイルアプリの管理
(MAM)

Microsoft Intune

モバイルのアプリケーションを制御する



企業データへの
アクセス要件を強制



不正なデバイスからのア
プリ起動を禁止



保存されている
データの暗号化を強制

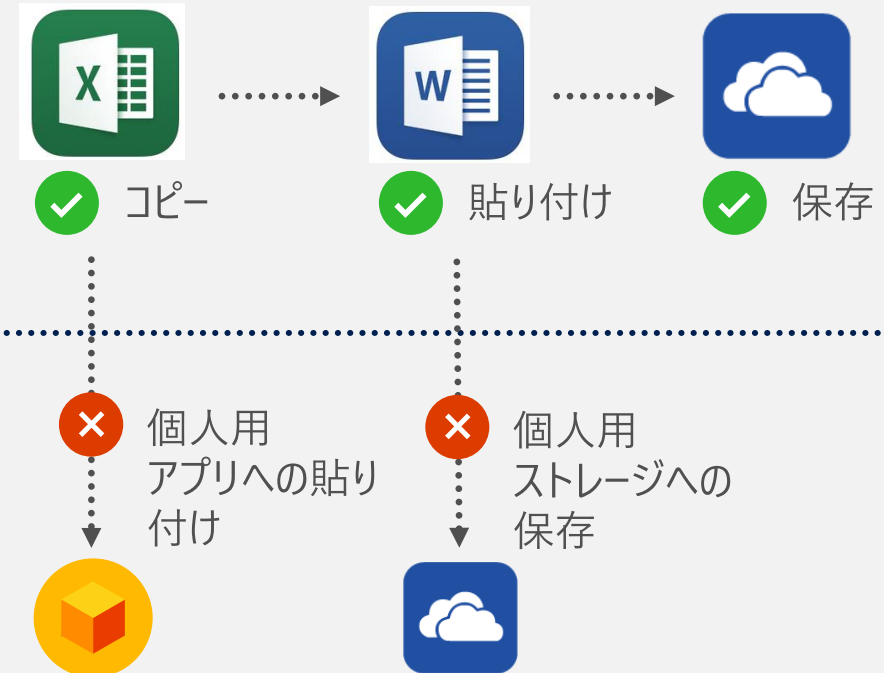
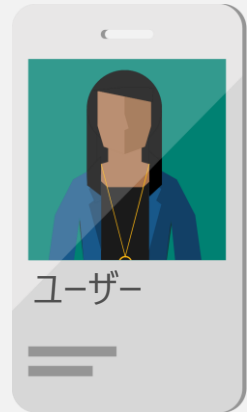


アプリレベルの
セレクトティブワイプを実施

モバイル アプリケーションの管理 (データの分離)



モバイル アプリケーションの管理 (操作の制御)



▶ Intune の管理対象アプリと非管理対象アプリ間でのコピー/切り取り/貼り付け/保存などの操作を制限することで、企業データの漏洩を防ぎつつ生産性を最大化

セレクトティブ ワイプ



その他、設定できる主なポリシー

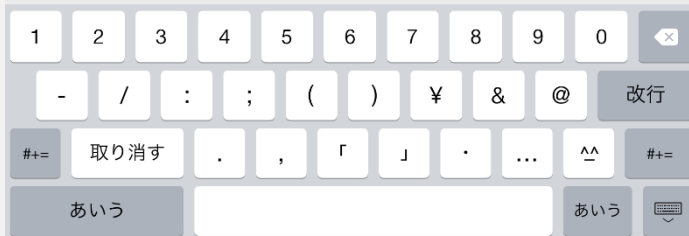
PIN の要求 (iOS は指紋もOK)



会社によって管理されています

PIN を入力してください

[PIN をお忘れですか?](#)



OS / アプリの最低バージョン指定

最低限の iOS オペレーティング システムを必要とします ⓘ

はい いいえ

iOS オペレーティング システム

0.0

最低限の iOS オペレーティング システムを必要とします (警告のみ) ⓘ

はい いいえ

iOS オペレーティング システム

10.0

最低限のアプリ バージョンを必要とします ⓘ

はい いいえ

アプリ バージョン

1.5.6

最低限のアプリ バージョンを必要とします (警告のみ) ⓘ

はい いいえ

アプリ バージョン

15.1.1

その他

- 印刷の無効
- iTunes / iCloud へのバックアップ禁止
- 連絡先の同期を無効
- 長期間利用していないアプリのデータのワイプ
- アプリ内のリンクを開く際に MAM のブラウザ (Intune Managed Browser) に限定

管理対象アプリ

- ▶ Microsoft Office アプリ (Office アプリを MAM で管理できるのは Intune だけ)
- ▶ Adobe, Box など 3rd Party アプリも対応拡大中



Intune mobile application gallery : <https://www.microsoft.com/en-us/cloud-platform/microsoft-intune-apps>

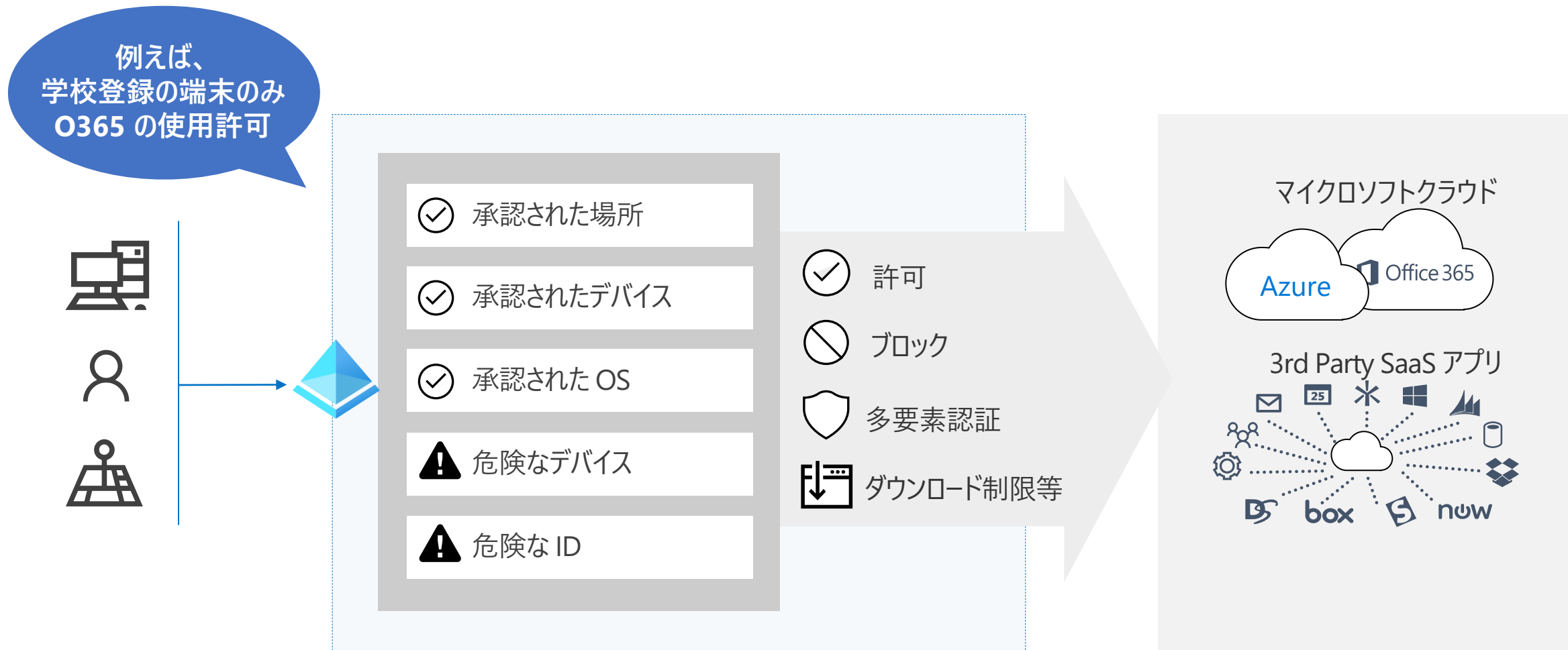


Intune for Education 条件付きアクセス

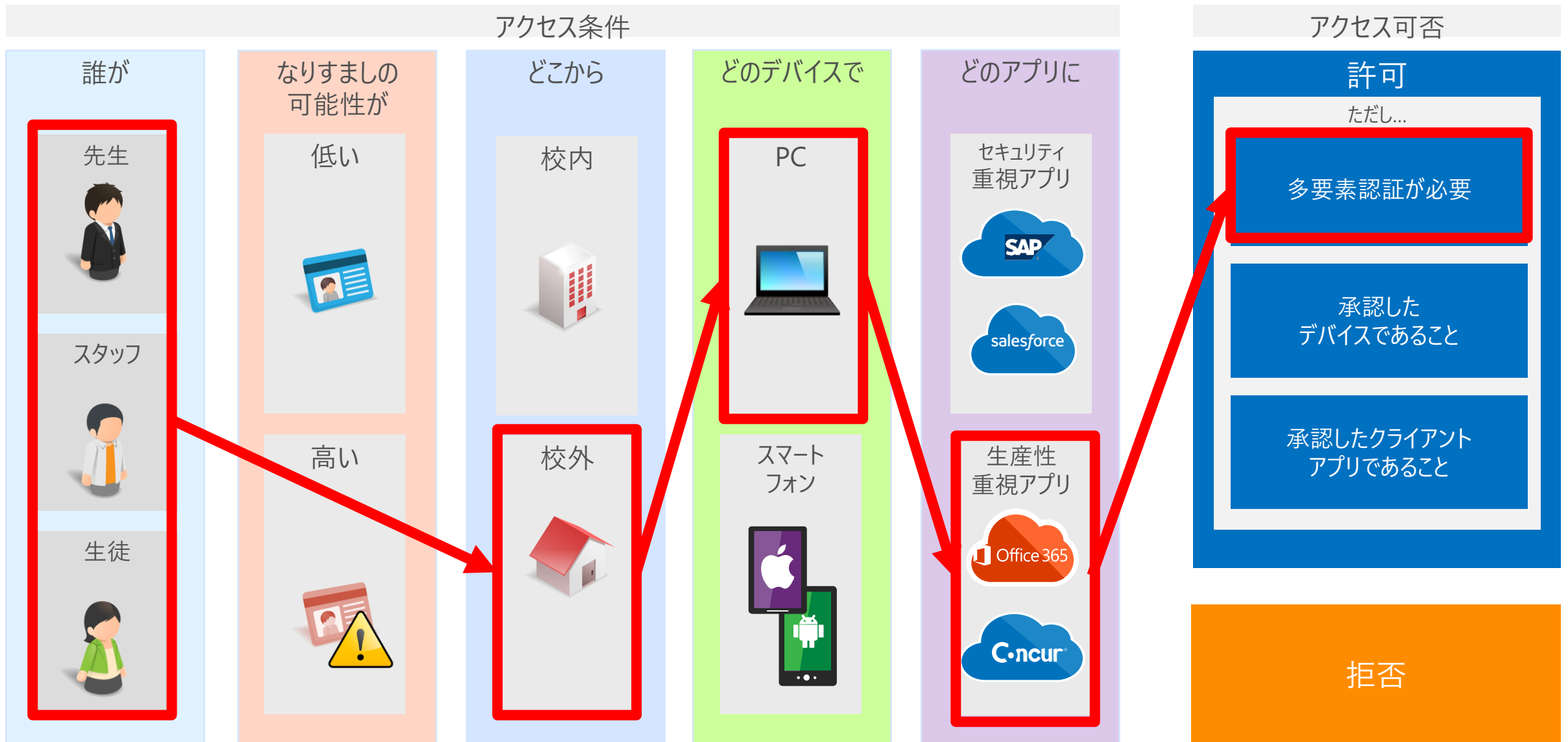
※ Azure AD Premium Plan 1 もしくは Microsoft 365 A3 / A5 が必要です。

様々な条件でアプリケーションへのアクセスを制御

Azure Active Directory 条件付きアクセス

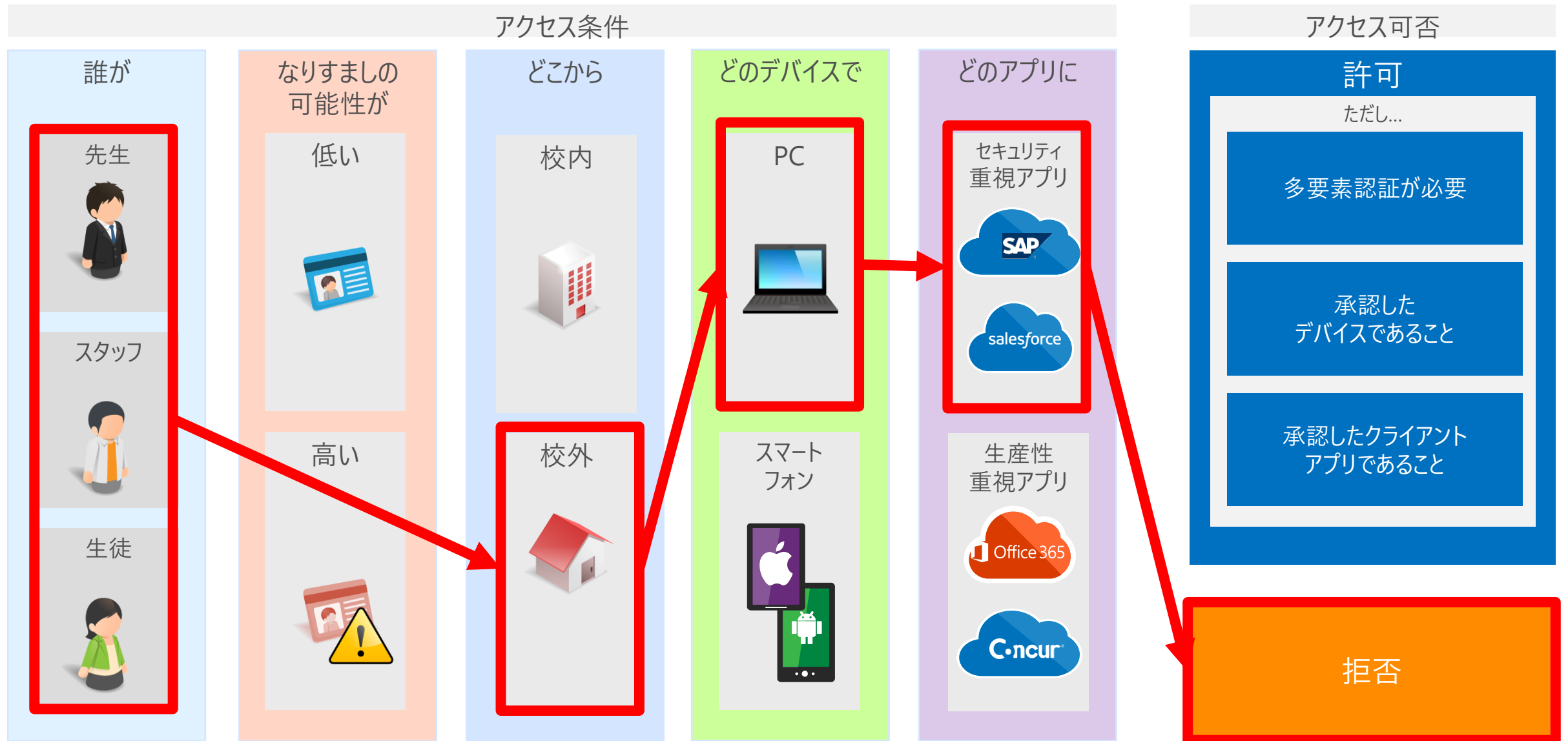


条件付きアクセス：ポリシーの例 – 校外では多要素認証

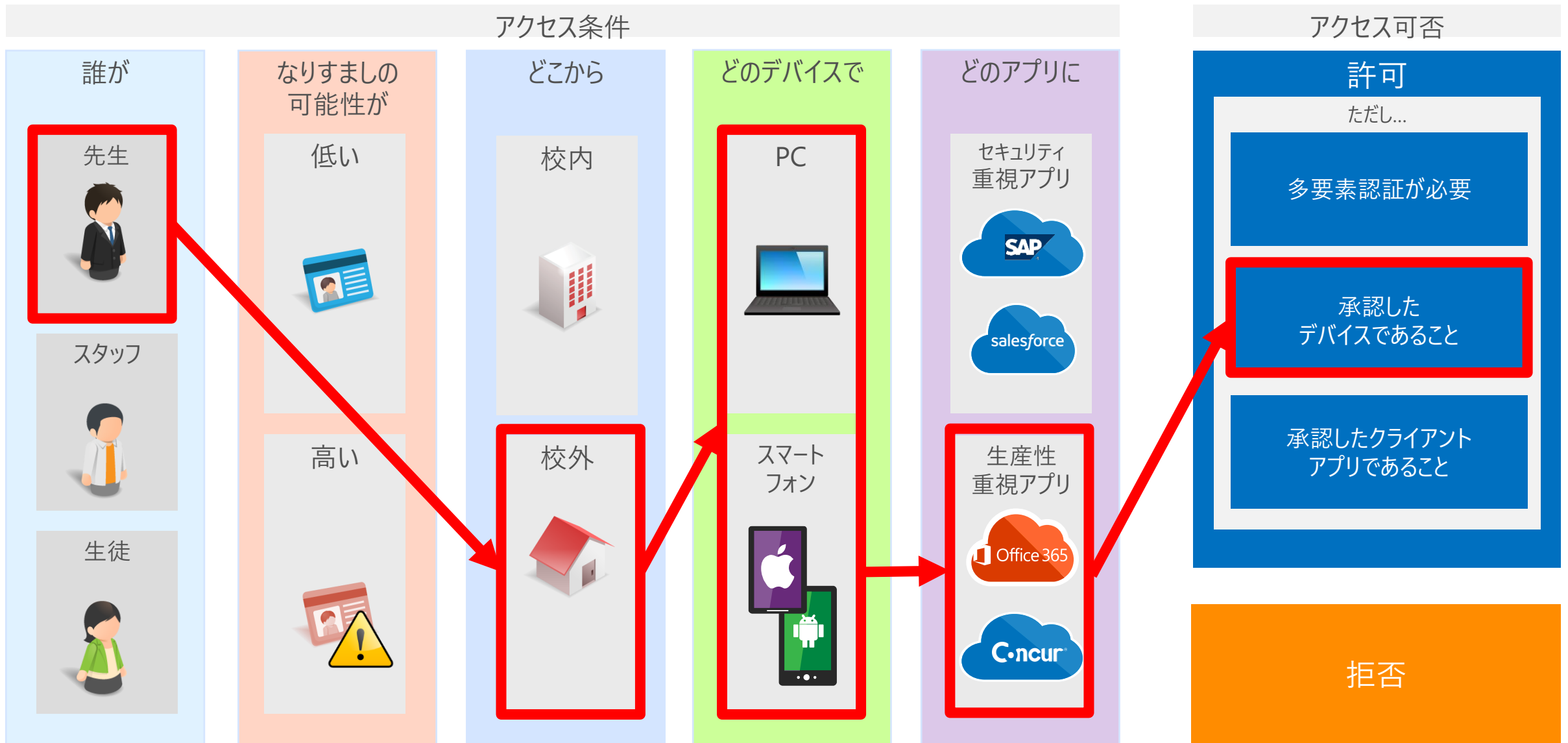


※ Office 365 では、アクセスを完全に制御するには ADFS との組み合わせが必要になる場合があります

条件付きアクセス：ポリシーの例 - 支給端末のみ許可



条件付きアクセス：ポリシーの例 - 支給スマートフォンのみ許可



支給デバイスのみアクセスを許可する仕組み

クラウドサービスへアクセスしてくるデバイス (モバイル、PC) の管理状態を確認

