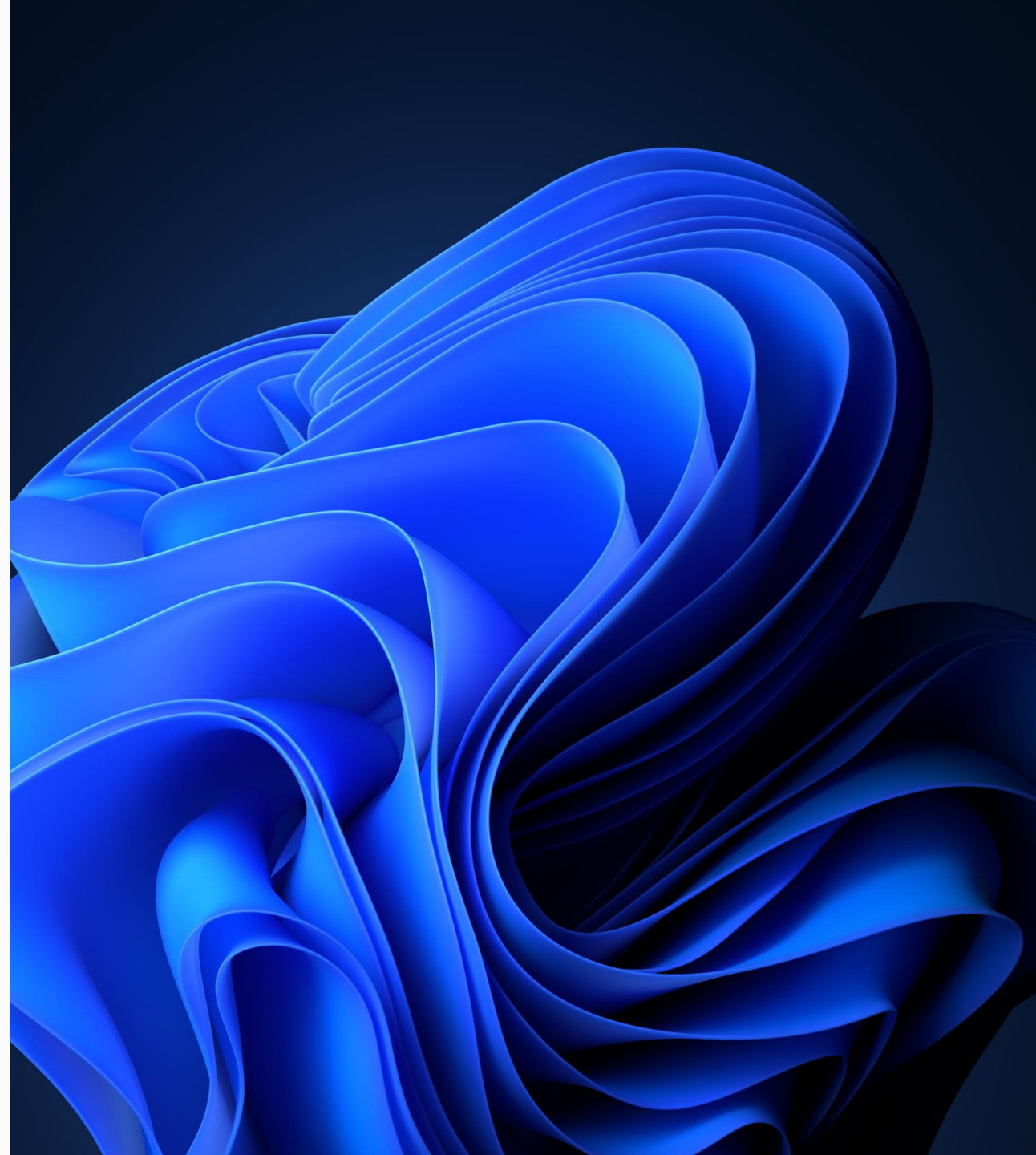




そう、ハイブリッドワークを支える すべてがそろっている Windows 11 ならね

日本マイクロソフト株式会社
パートナー事業本部
パートナーテクノロジーストラテジスト
黒田 衛  [LinkedIn](#)



株式会社ソフトクリエイト

×

Microsoft



Copyright © SOFTCREATE CORP. All Rights Reserved.

Microsoft アワードを受賞されている信頼のあるパートナー

Microsoft Partner of the Year Awards 4年連続受賞！

※「2021 Microsoft Partner of the Year Awards」ファイナリストを含む

Microsoft アワード 受賞歴

2019年	「Microsoft Japan Partner of the Year 2019」特別賞
2020年	「Microsoft Japan Partner of the Year 2020」Retail アワード
2021年	「2021 Microsoft Partner of the Year Awards」ファイナリスト
2022年	「Microsoft Japan Partner of the Year 2022」Retail & Customer Goodsアワード



2021年 アワード受賞

「2021 Microsoft Partner of the Year Awards」ファイナリスト

世界100カ国以上、4,400超の企業がエントリーする中で、
Modern Workplace for SMB 部門のファイナリストに選出されました。

World
Award



▶受賞内容

中堅中小顧客のワークスペース変革を
サポートする事業に大幅かつ持続可能な
成長を遂げたパートナーに授与されます。

2022年 アワード受賞

「Microsoft Japan Partner of the Year 2022」Retail & Customer Goodsアワード

日本マイクロソフトがパートナー企業を対象に、優れた実績を
収めた企業を選出するプログラムで4年連続の受賞となります。

Japan
Award



▶受賞内容

ソフトクリエイトのグループ企業である
visumo社と「visumo on Azure」を共同開発し、
小売市場の企業に対してビジネス成長を実現しました。

自社導入で蓄えたノウハウをお客様に還元しています

Microsoftの事例サイトに掲載中



2021年3月23日

印刷



リモートワークの一般化は、企業の情報システム担当者に対して、大きな業務変革を迫っています。社内のITデバイスを保守するだけでなく、従業員の自宅ネットワークや私物PCをいかに効率的に、そしてセキュアに運用していくのか。これまでとはまったく違うインフラ構築が必要となっているのです。

こうした状況下でソフトクリエイイトは、Microsoft 365 E5 の導入によりゼロトラストセキュリティを実現しました。強固なセキュリティ基盤を築いたことによって、同社では、事業部門の自発的なDX (Digital Transformation) が次々と巻き起こっています。

リモートワーク環境下では、新たなセキュリティの構築が急務だった

主に中堅中小企業の「情報システム部門」に必要なあらゆるサービスを提供しているソフトクリエイイト。PCの調達から、サーバーやクラウドの運用、セキュリティの構築、アプリの保守まで、情シスの機能を総合的に請け負っています。

そんな同社も、新型コロナウイルス感染症 (COVID-19) の流行によって、「急ごしらえ」でリモートワーク環境を構築した企業が増え、セキュリティの構築が急務となった。

お客様
株式会社ソフトクリエイイト (SOFTCREATE CORP.)

製品とサービス
Azure Active Directory
FastTrack for Microsoft 365
Microsoft 365 E5
Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint

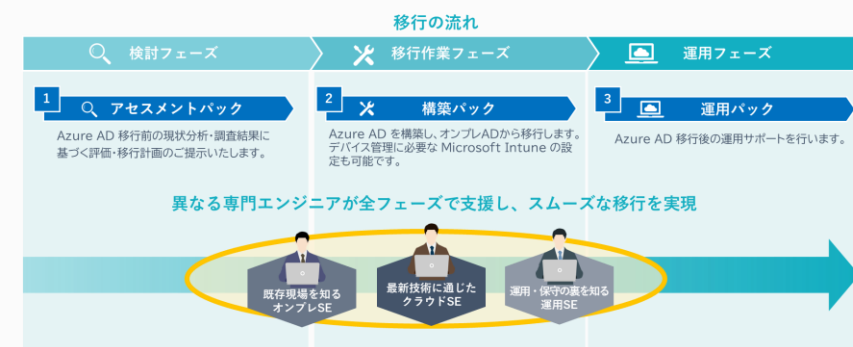


自社運用の経験・ノウハウをサービス化



AzureAD 移行支援サービス

最短距離で AzureAD の利用を可能にするフルマネージドサービス
「設計」「構築」「運用」すべてのフェーズでお客様の要望に応じ、最適な移行を一気通貫で支援いたします。



AzureAD 移行支援サービスの特徴

『クライアントインフラ移行』にフォーカスし、膨大なクライアント作業を最小化



独自スクリプトで自動化し手順書を削減

分かりやすい手順書で問い合わせを削減

利活用を促進するユーザーコミュニティ「ソフクリ365倶楽部」



会員数 **1,500名** 超え！

続々と協賛企業が参画。
お客様に有益な情報を発信し続けます。

トレーニング コンテンツ

- 毎月更新！Teamsマニュアル提供
- 毎月開催！オンライントレーニング
- PowerAppsトレーニング動画提供

利活用情報

- メルマガ「365倶楽部通信」
- 活用の参考になる事例公開
- 倶楽部会員様用専用Webサイト

さらに**Premium 会員** (ソフトクリエイイトよりMicrosoft CSPをご契約中のお客様) になると・・・

Teams コミュニティ

- 会員様同士のコミュニティへの参加
- 最新情報や検証情報、運用マニュアルの公開
- Premium会員限定のセミナー/イベント



どなたでも**Webから**会員登録ができます！



ハイブリッドワークのトレンド

働き方や働く場所の変化



73%

の社員が柔軟なリモートワークの
選択肢を求めていると回答



67%

の従業員がより多くの人との
コラボレーションを望んでいる



80%

の管理職はより柔軟な在宅勤務
制度を期待しています

Sources:

1. "The Work Trend Index" survey was conducted by an independent research firm, Edelman Data x Intelligence, among 31,092 full-time employed or self-employed workers across 31 markets between January 12, 2021 to January 25, 2021.

労働力や組織のニーズの変化



リモートと
ハイブリッドワーク



柔軟性のある
労働力



組織の拡大と
変化



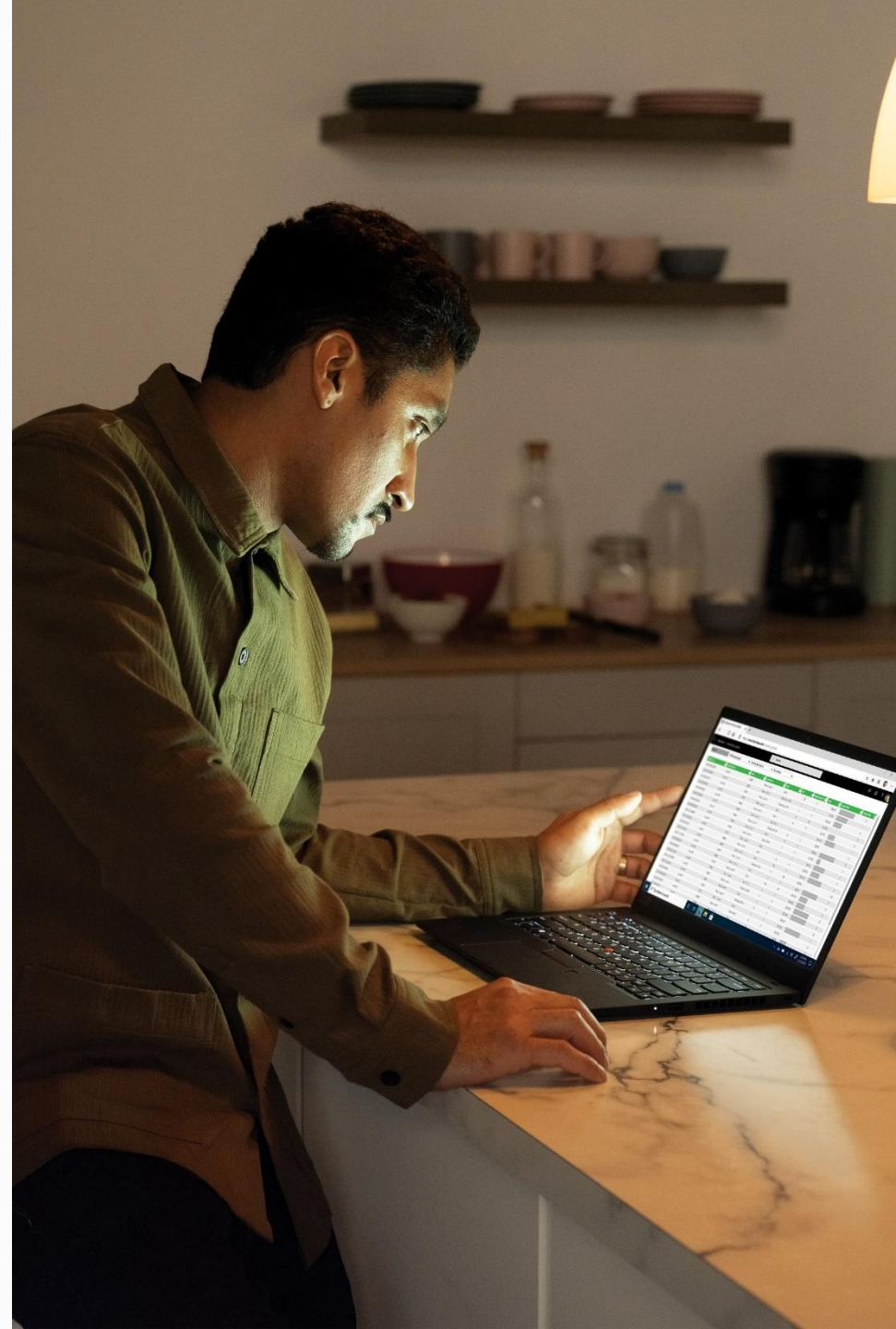
Bring your own
PC (BYOPC)



セキュリティと
コンプライアンス



大規模かつ
特殊なワークロード



在宅勤務



リモートワーク



ハイブリッドワーク

事情に応じて「家」でお仕事

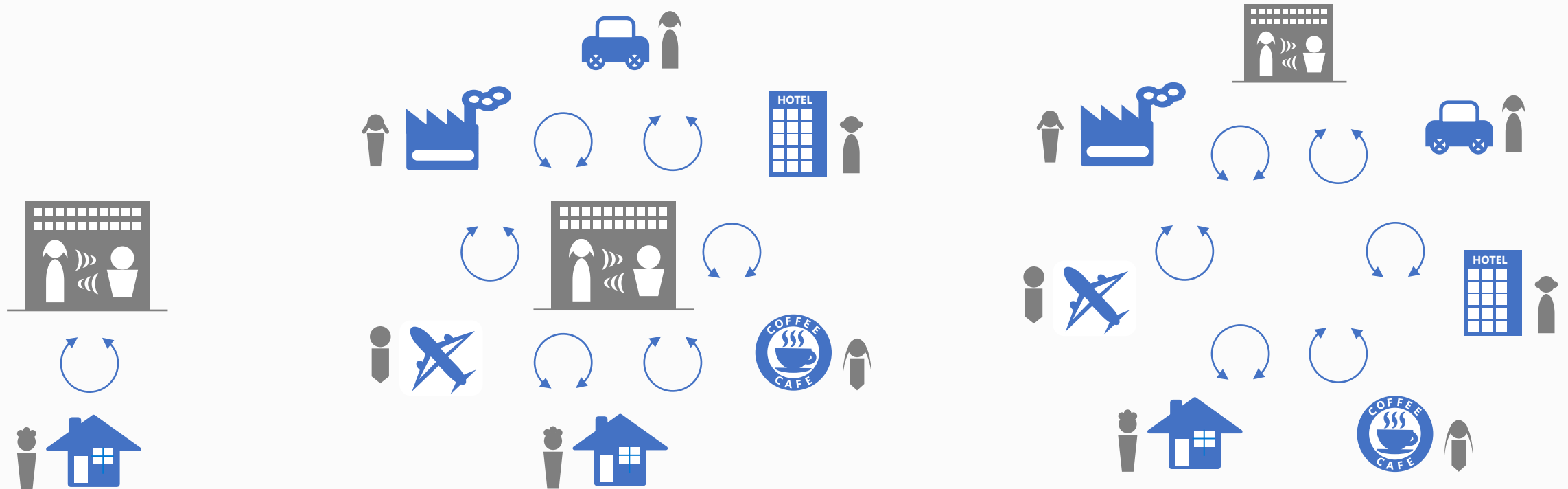
「オフィス」を基軸にどこでもお仕事

「オフィス」は選択肢の並列な1つ

福利厚生の一部

重要な企業戦略

企業戦略 & “真”の働き方の多様性へ



ハイブリッドワークは、新しい機会と新しい挑戦を生み出します



オンボーディングとプロビジョニング

従業員、ベンダー、委託業者が様々なデバイスや場所で使用できるようにするためのゼロタッチのアプローチ。

事業継続性

職場の状況の変化に迅速に対応し、マイナスの影響を軽減し、チャンスを掴む。

セキュリティと規制

生産性を犠牲にすることなく、複雑化するコンプライアンスに対応しながら、組織や顧客のデータを保護する。

ハイブリッドワークのためにデザイン

働く人にパワーを。ITに一貫性を。すべてのユーザーに安全を。

Windows 11



生産性

シンプルでパワフルなユーザーエクスペリエンスが、生産性と集中力を向上します。



コラボレーション

Microsoft Teams と統合することで、よりスマートなコラボレーションが可能になります。



一貫性

アプリの互換性とクラウドによる管理が、導入を容易にします。



安全性

データを保護し、どこからでも安全にアクセスできる「ゼロトラスト」の準備が整っています。

選択肢

従業員1人1人に満足していただき、長く働いていただくことに適したデバイス



Windows 11 紹介



1. Windows 11 の概要
2. Windows 11 の管理インフラ
3. Windows 11 の展開
4. Windows 11 の設定
5. Windows 11 のセキュリティ

生産性が上がる シンプルでモダンな UI

Windows 11の UI は、満足してお使い頂けるよう**大切なことにより集中**できるようにデザインされています

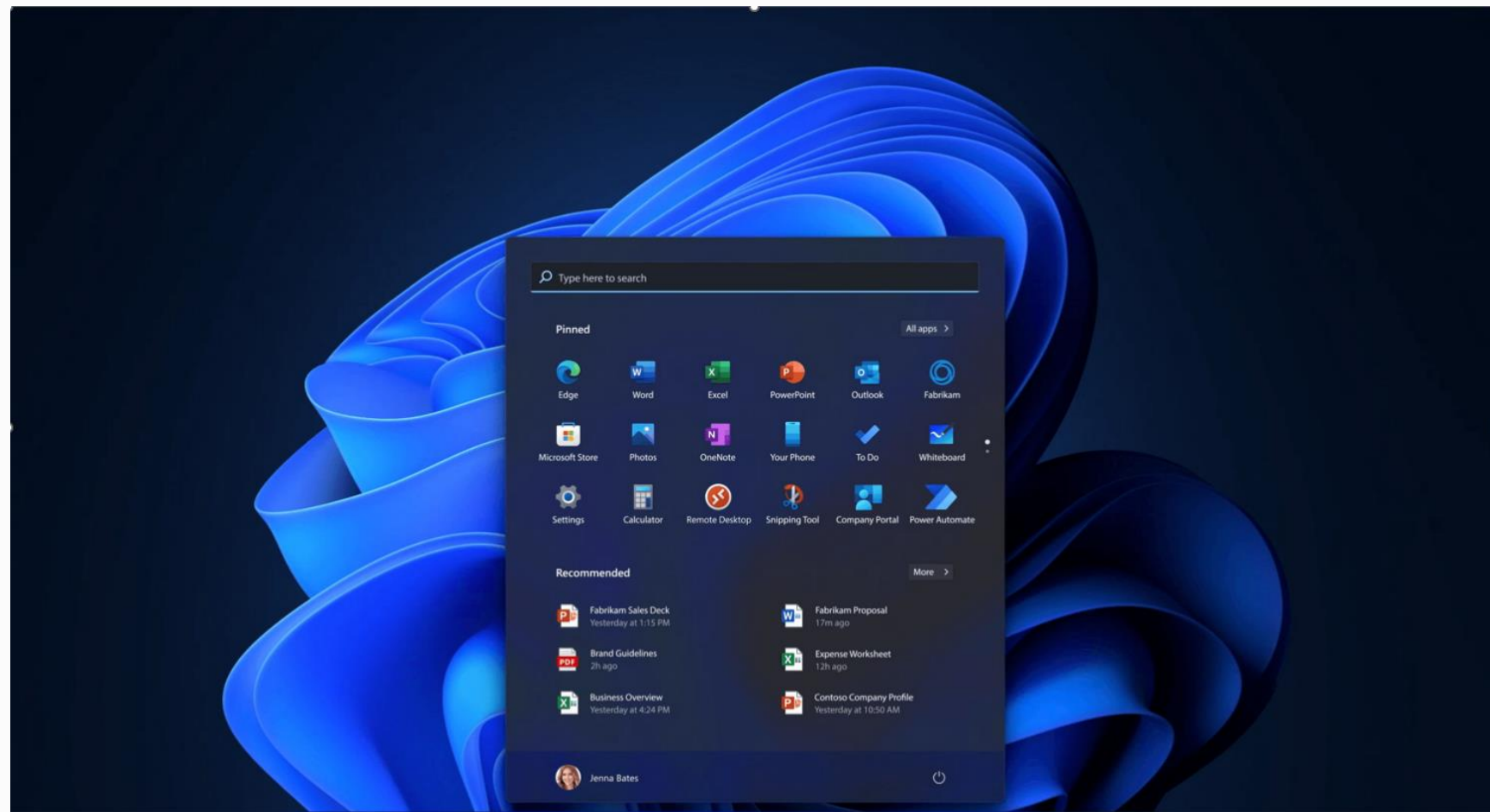
快適性 - 目的の操作を迅速かつ直観的に、集中して正確に実行できる

シンプル - 柔らかく、すっきりとしたデザインは、温かみと親しみが感じられる

パーソナル - ユーザーそれぞれに合わせたカスタマイズ性

一貫性 - OS から、アプリまで、すべてがシームレスに連動

使いやすい - 操作を学習する必要がないため、導入後、すぐに作業を開始できる

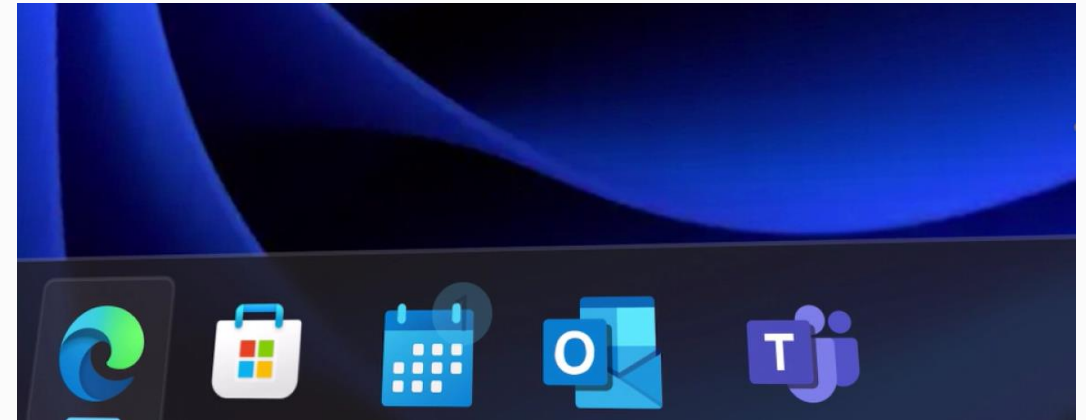
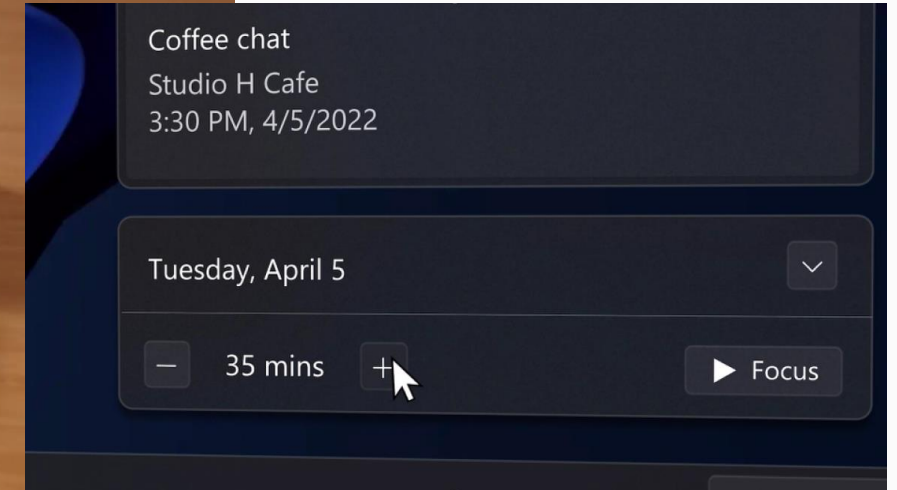


集中モード

集中力を保つ

集中したいときに、気が散る要因となる通知を無効化できる**集中モード**は**応答不可**と**フォーカス**へと機能強化。既定では特定の条件下で自動的に有効になるように設定

タスクバーから**フォーカス時間の調整**や**延長**が可能



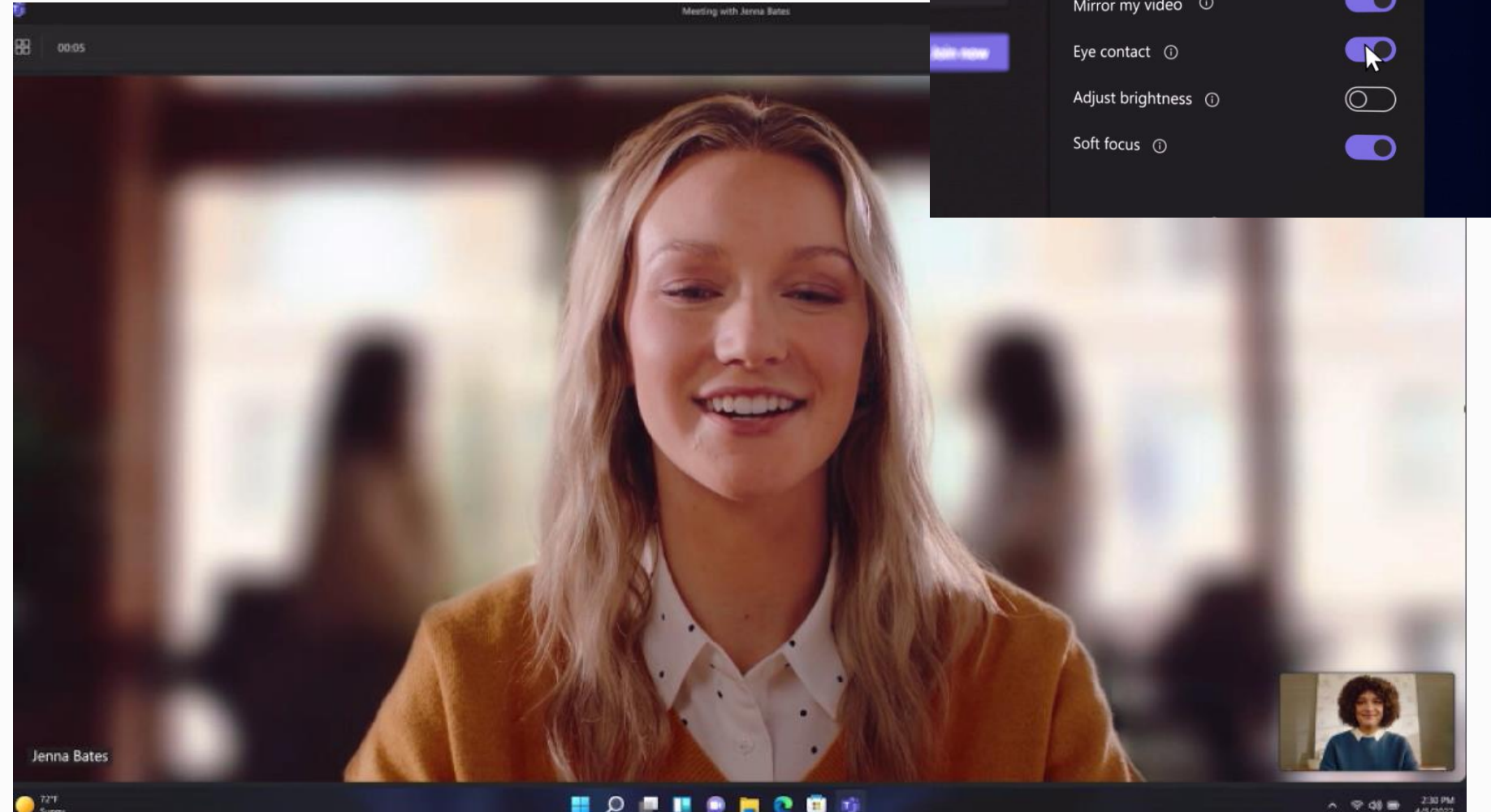
インクルーシブな会議

オンライン会議にAIを活用することで音声と映像が明瞭に

オンラインの会議でのコミュニケーションでは、映像と音声の品質が極めて重要です

会話を文字に変換するライブ キャプションに加えて、**周囲のノイズの抑制**、メモを読んだり別のモニターをみているときの**視線補正**、高精度な背景ぼかしをサポート

デバイスの前を歩き回っても**人物を追尾***し続けることで、どこからでもクリアな音声を届けられる



*デバイスでの NPU（ニューラル プロセッシングユニット）のサポートが必要です。

リリース前の製品に関する情報は一般向け提供開始前に変更となる可能性があります。マイクロソフトは本資料の情報について、明示または黙示を問わず、いかなる責任も負わないものとします。

Windows 11 と Windows 365 の連携

ローカル PC とクラウド PC をシームレスにつなぐ

Windows 365 との連携を強化し、
ローカルとクラウドの境界をなくす

Windows 365 Switch

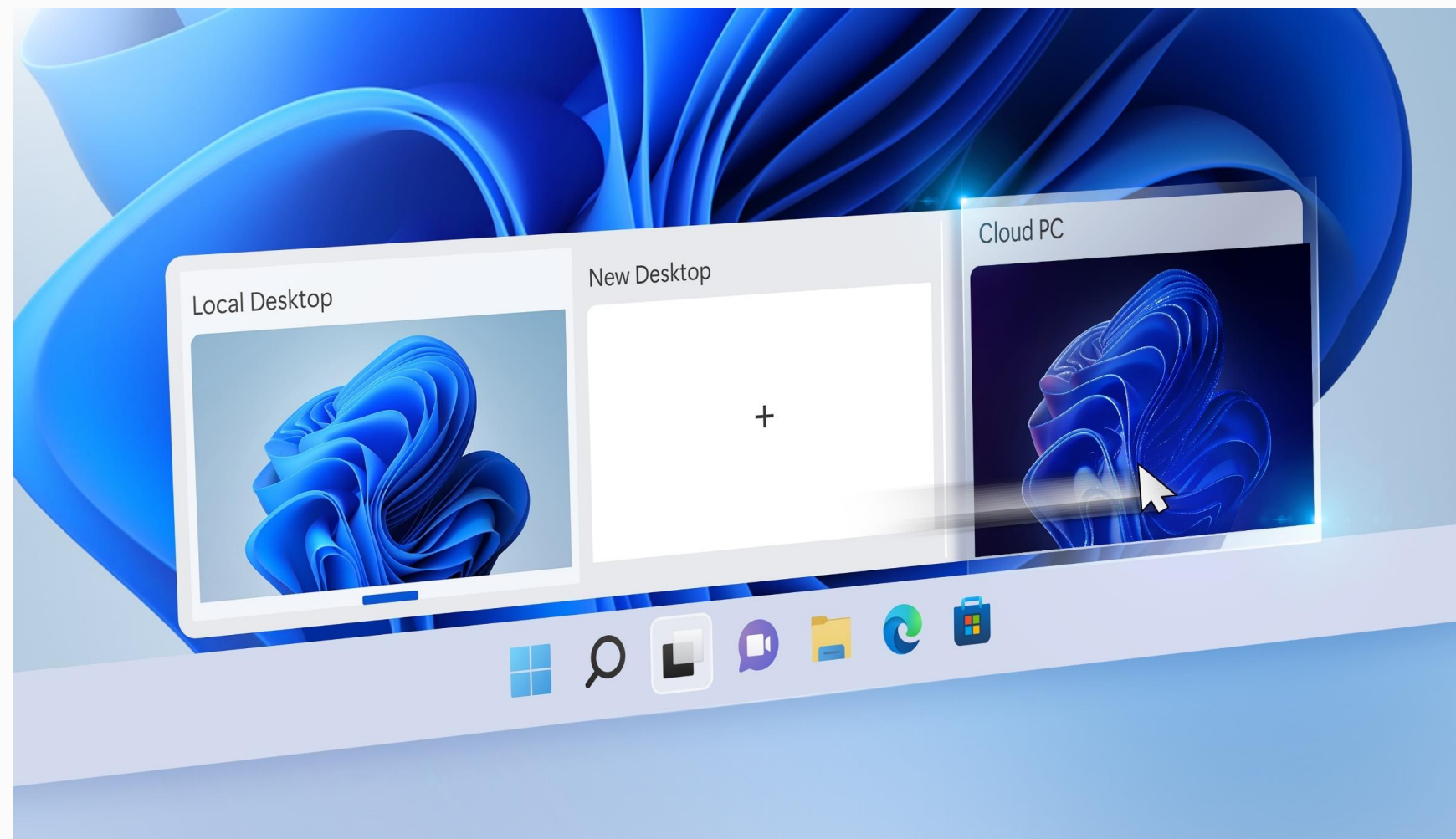
タスクビューから仮想デスクトップを
切り替えるのと同じようにWindows
365に切り替える

Windows 365 Boot

Windows 11 デバイスで直接
Windows 365 クラウド PC を起動

Windows 365 Offline

ネットワークへの接続が切断された
場合でも、途切れることなく作業を
継続。オンラインに復帰したら自動的
に同期を開始



Windows 11 の更新とサポート期間



更新プログラム※

年に 2 回の機能更新

月に 1 回の品質更新

サポート期間

Pro / Home : 18 カ月

Enterprise / Education : 30 カ月(秋)



更新プログラム※

年に 1 回の機能更新

月に 1 回の品質更新

サポート期間

Pro / Home : 24 カ月

Enterprise / Education : 36 カ月

ライフサイクルに関する FAQ - Windows | Microsoft Docs

<https://docs.microsoft.com/ja-jp/lifecycle/faq/windows>

※ 問題や緊急性により、複数回リリースされる場合もあります

Windows 11 ハードウェア要件

プロセッサ：

1 GHz 以上のスピードで 2 つ以上のコアを搭載し [互換性のある 64 ビットプロセッサ](#) または SoC

RAM:

4 GB 以上

ストレージ：

64 GB 以上。

※ 更新プログラムをダウンロードして特定の機能を有効にするには、追加の記憶領域が必要になる場合があります。

グラフィックス カード：

WDDM 2.0 ドライバーを搭載し、DirectX 12 以降と互換性があること。

システム ファームウェア:

UEFI、セキュア ブート対応

TPM：

[トラステッド プラットフォーム モジュール](#) (TPM) バージョン 2.0

ディスプレイ：

高解像度 (720p) ディスプレイ、9 インチ以上のモニター、カラー チャネルあたり 8 ビット

インターネット接続：

更新プログラムを実行し、一部の機能をダウンロードして使用するには、インターネット接続が必要です。

※ Windows 11 Home Edition では、初回使用時にデバイスのセットアップを完了するには、インターネット接続と Microsoft アカウントが必要です。

システム ファームウェア:

UEFI、セキュア ブート対応

Windows 11 の要件 | Microsoft Docs

<https://docs.microsoft.com/ja-jp/windows/whats-new/windows-11-requirements>

Windows 10 アプリは
Windows 11 で動作
App Assure によって支援

App Assure は、必要に応じてアプリケーションの問題を修正するための支援サービス。
<https://www.microsoft.com/ja-jp/fasttrack/microsoft-365/app-assure>

837,699

評価されたアプリの数

99.6%

アプリケーションの
互換性率

90 M

ブロックされていない
エンドポイント

44 M

ヘルプデスクコールの
防止（推定）

\$7.6 B

推定される顧客の
コスト削減

AppAssureプログラムの結果と影響

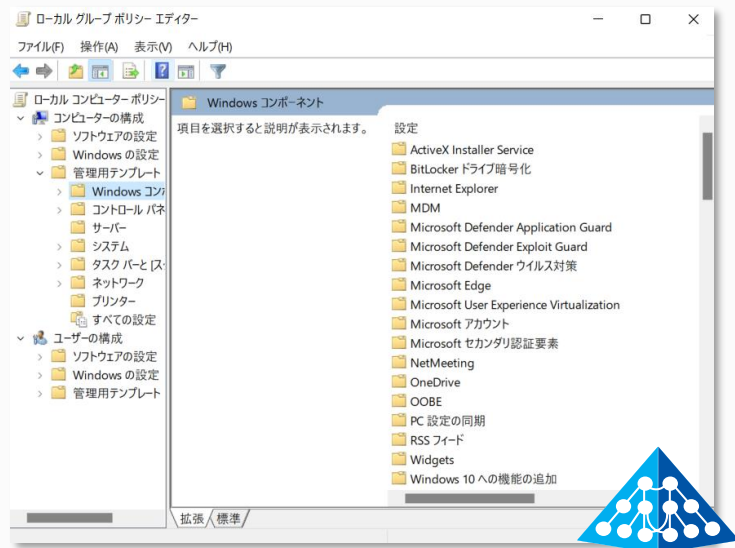
もし懸念がある場合は、**Test Base for Microsoft 365**（プレビュー）を使用して、ビジネスクリティカルなアプリをテストすることも可能。
<https://www.microsoft.com/en-us/testbase>



1. Windows 11 の概要
2. Windows 11 の管理インフラ
3. Windows 11 の展開
4. Windows 11 の設定
5. Windows 11 のセキュリティ

Windows 11 の管理インフラ

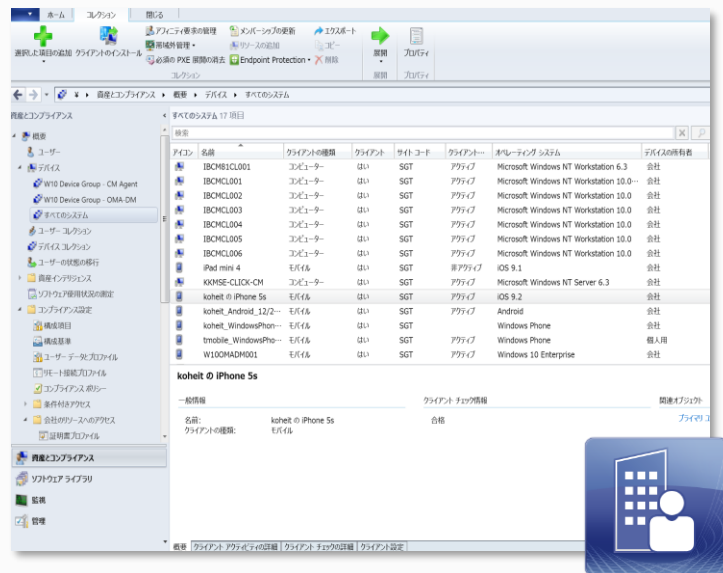
オンプレミス



Active Directory

グループ ポリシーによる設定管理

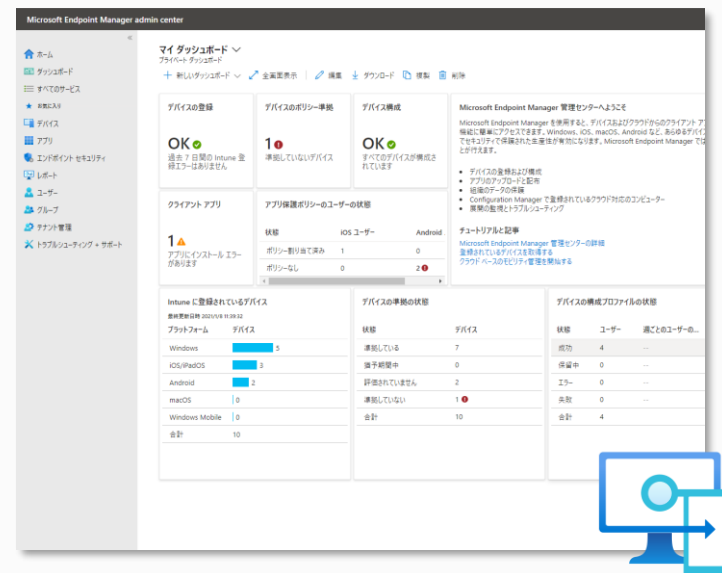
ハイブリッド可能



Configuration Manager
(MECM)

MECM クライアントによる設定管理

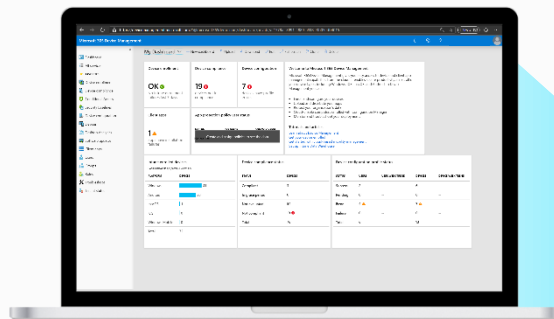
クラウド



Microsoft Intune

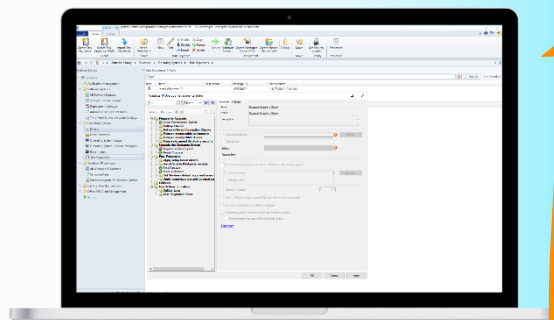
MDM ポリシーによる設定管理

Microsoft Intune



クラウド インフラストラクチャ
モビリティ管理
PC 管理
セキュリティ管理者

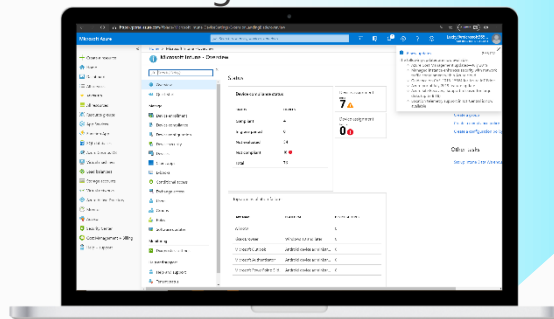
Configuration Manager



“System Center” の一部から、
“Microsoft Endpoint Manager” の一部に
変更になりました

インテリジェントエッジ
オンプレミスの PC 管理

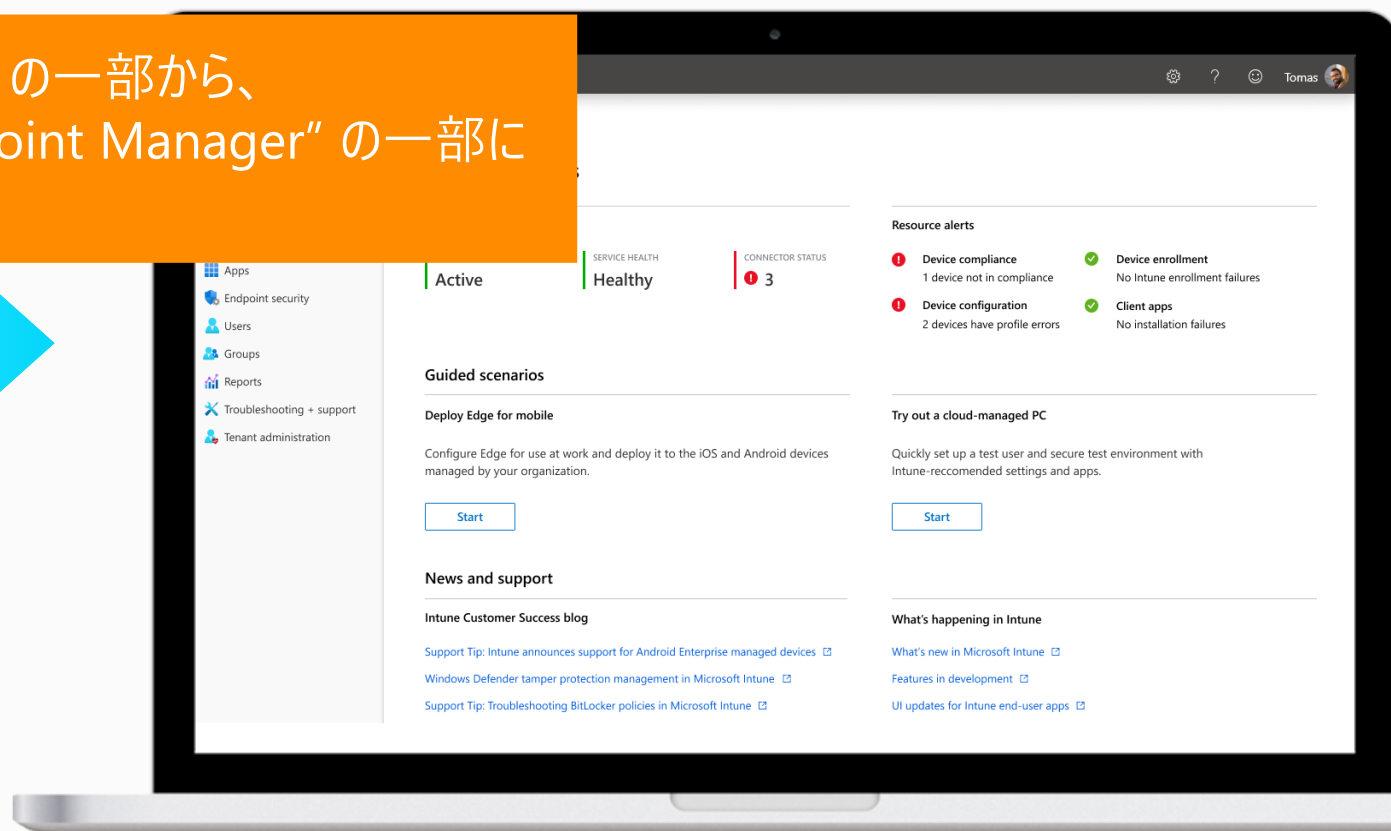
Other Endpoint
Management Tools



Desktop Analytics
AutoPilot などなど

IT管理者が自社のすべてのエンドポイントを把握し、
アクションを起こすための統合ソリューション

Microsoft Endpoint Manager



<https://endpoint.microsoft.com/>

Microsoft Endpoint Configuration Manager

オンプレミス型 - クライアント PC の統合管理

クライアントの管理

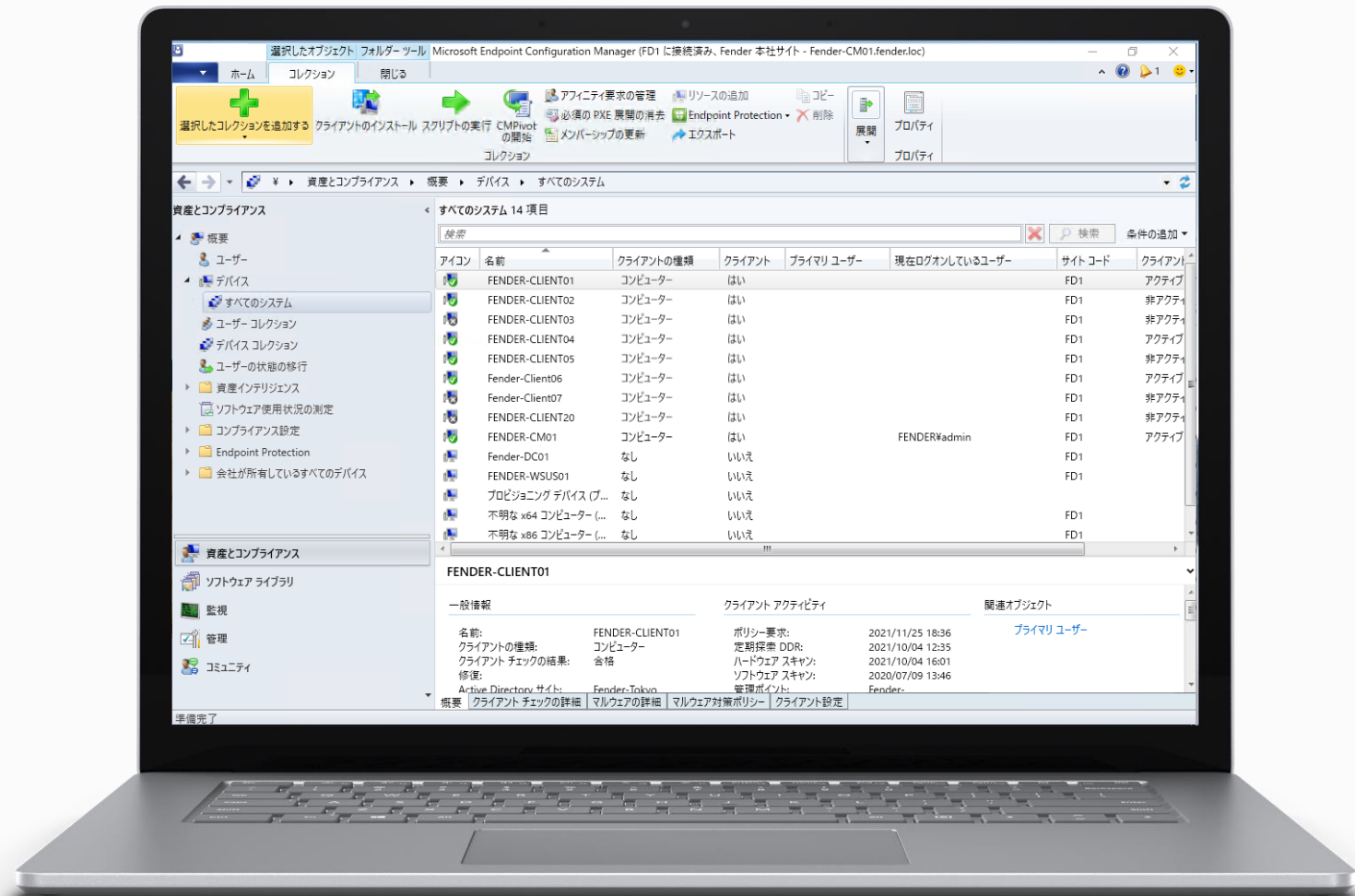
ハードウェアの構成やソフトウェアの情報などを収集
クライアントに対してのポリシーや設定を実施

アプリケーション / 更新プログラムの配布

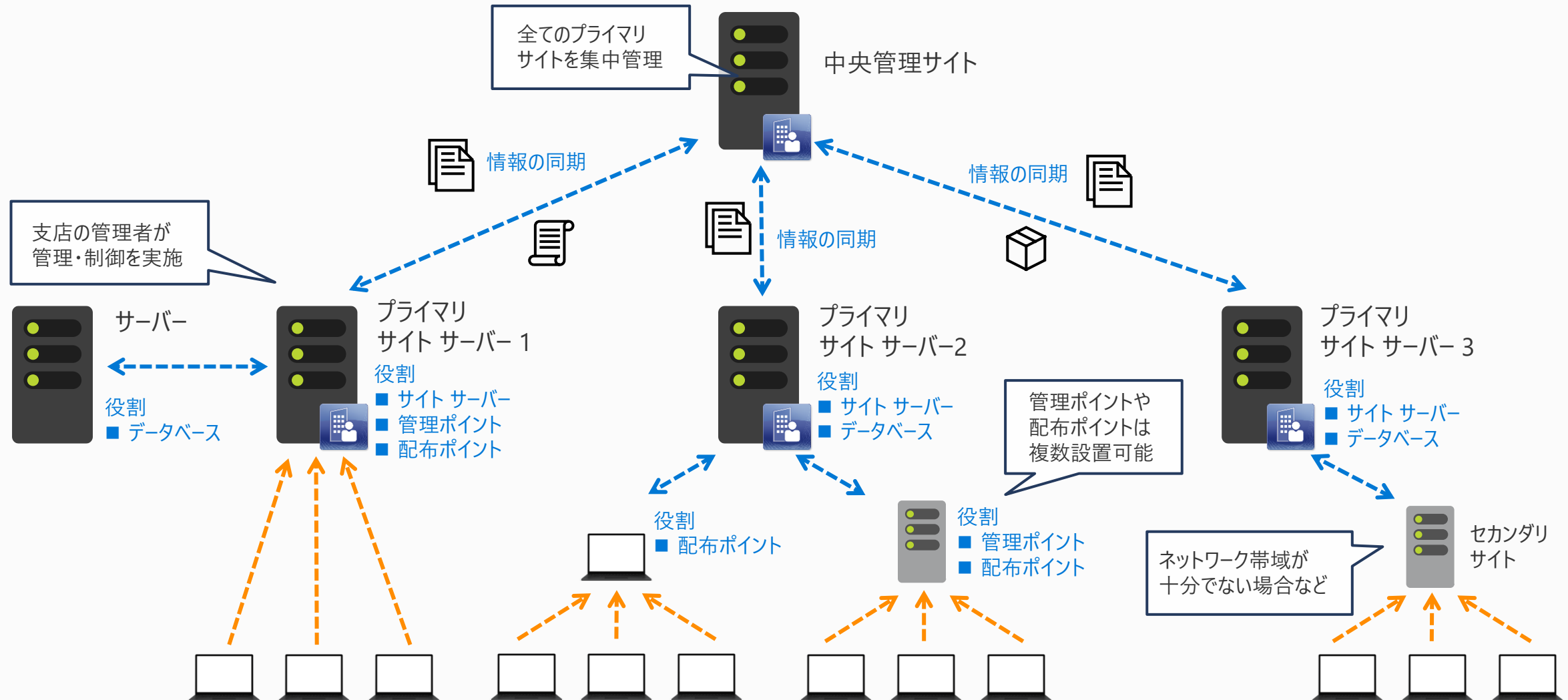
アプリケーション、ソフトウェア更新プログラムを
効率よく負荷を分散して配布をすることが可能
オペレーティング システムの安全でスケーラブルな展開

豊富なオプション機能

各種レポートの確認、コンプライアンス設定、
Microsoft Defender ウイルス対策の管理、
リモート ツールやクライアントへのアクションなど、
クライアント管理に必要な機能を利用可能



制限があるオンプレミス環境に対し柔軟な構成が可能



Microsoft Intune

クラウド型 – モバイル デバイス/アプリ管理 (MDM/MAM) サービス

モバイルデバイスの管理 (MDM)

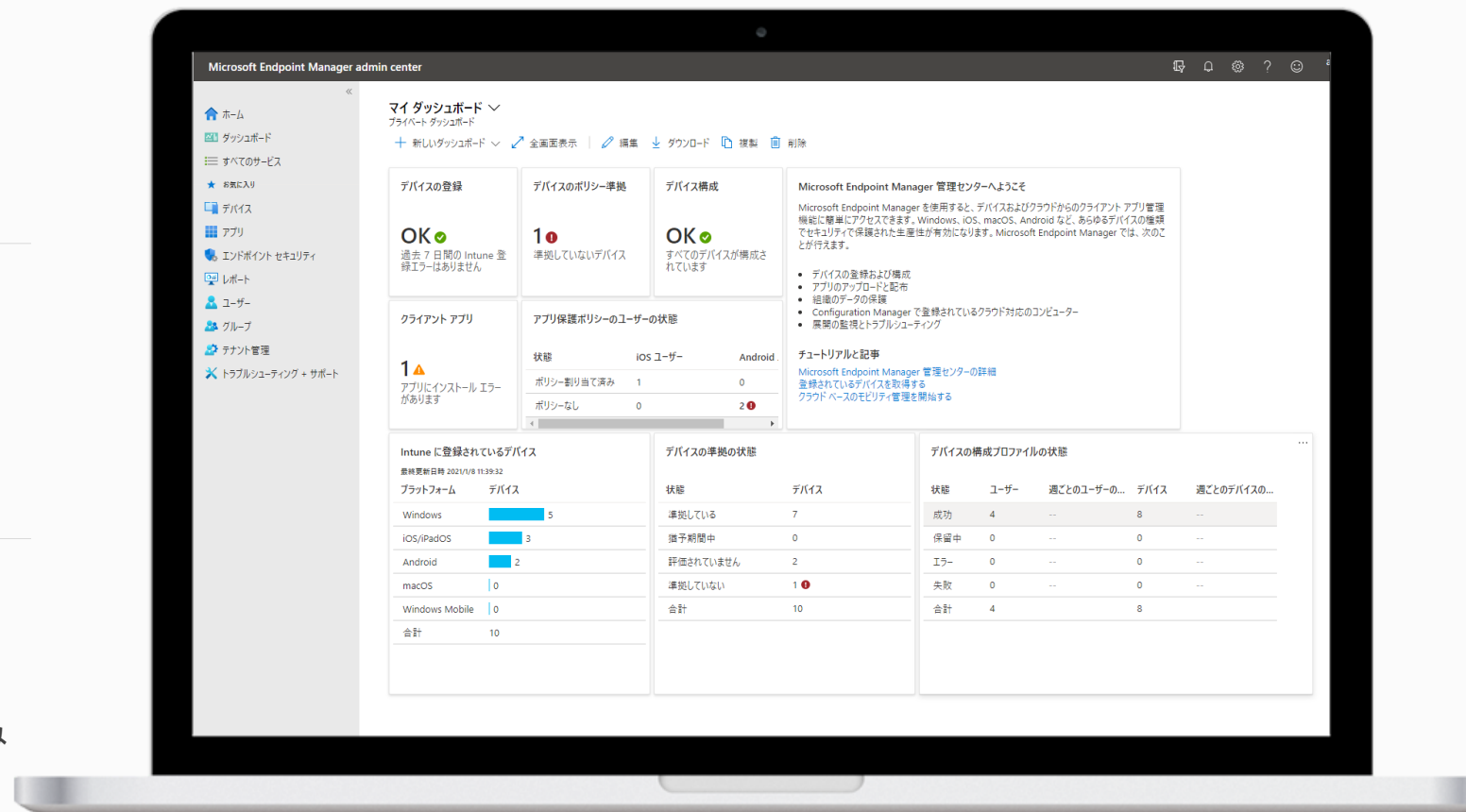
Windows 10/11 や iOS, Android を一元管理
管理下のデバイスに対する、ポリシーの一括設定や
ワイプや端末の探索などのアクションが可能

アプリの管理 (MAM)

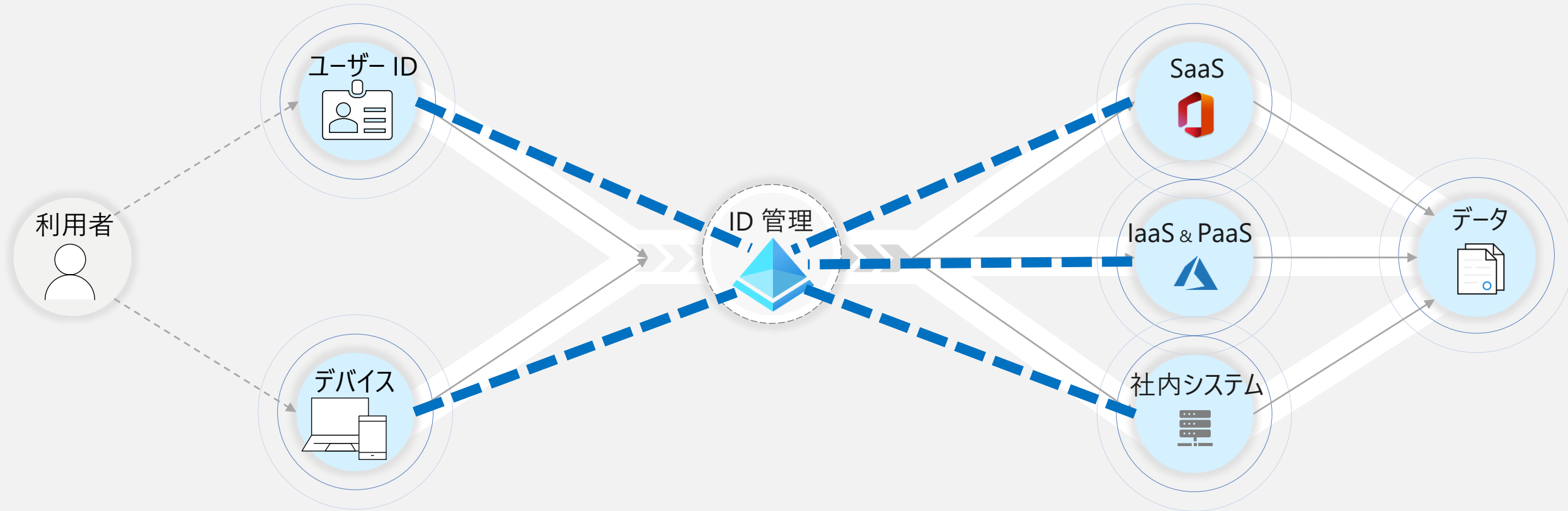
端末やユーザーに応じたアプリの配布・設定が可能
またアプリ保護ポリシー対応アプリであれば、
さらに厳密にセキュリティ設定を行うことが可能

クラウドサービスとの連携 (アクセス制御等)

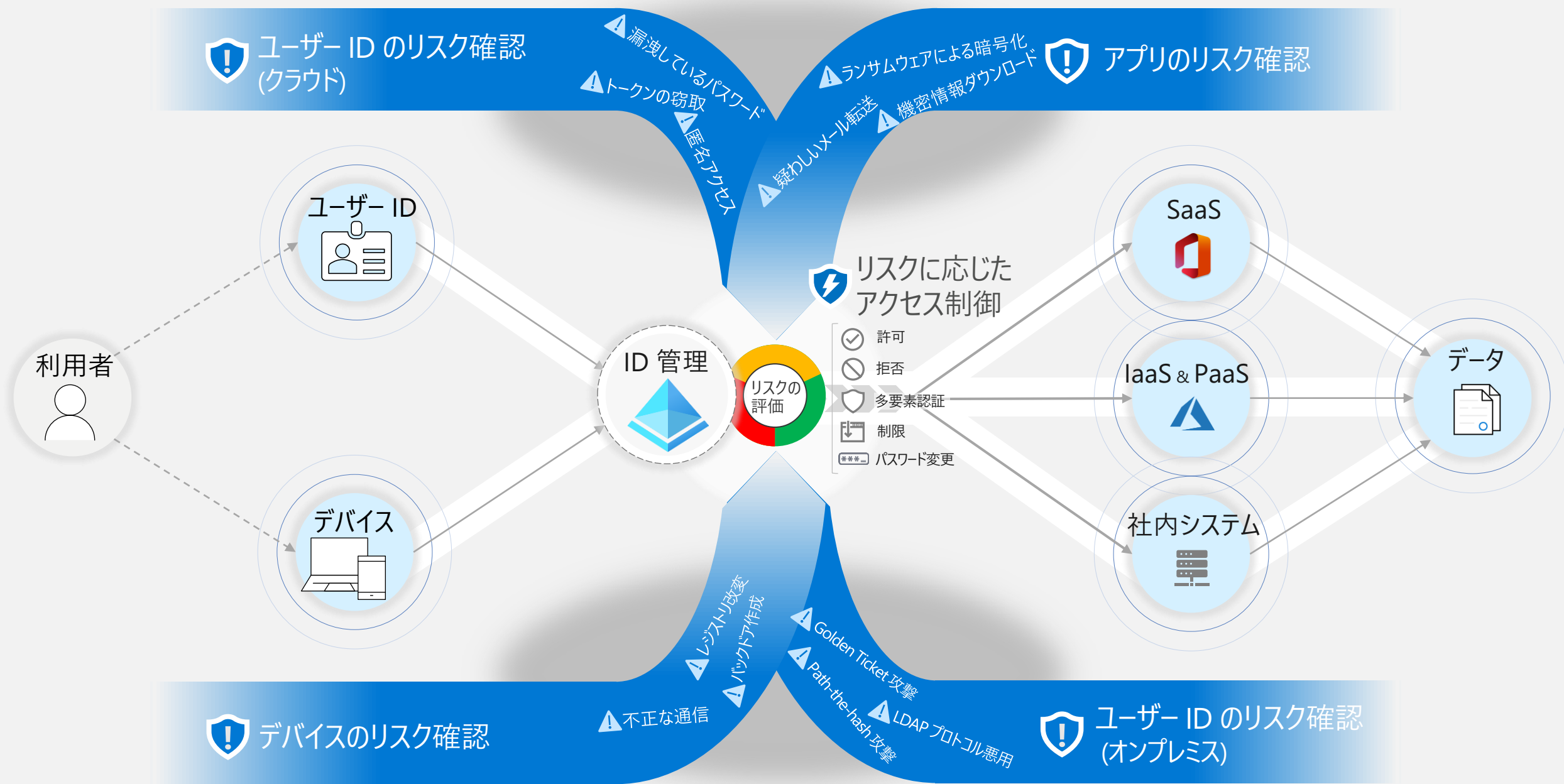
Azure AD の条件付きアクセスと連携し、
管理されたデバイスやポリシーに準拠したデバイスのみ
アクセス可能といったような制御が可能



Microsoft のゼロトラスト → 管理・保護するものを明確にする (ID ベース)



ID ベースのゼロトラスト → 決して信頼せず、常に検証する



条件付きアクセス - 様々な条件でアクセスを制御

条件付きアクセスと多要素認証で ID を保護

例えば、
Intune に登録された
Windows 11（最新バージョン）のみ
Office 365 を使用可



✓ 承認された場所

✓ 承認されたデバイス

✓ 承認された OS

⚠ 危険なデバイス

⚠ 危険な ID

✓ 許可

⊘ ブロック

🛡 多要素認証

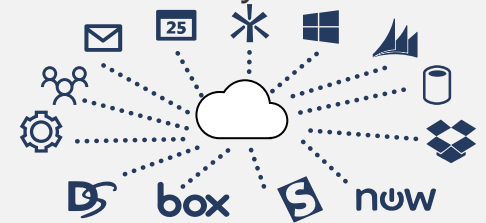
📄 ダウンロード制限等

マイクロソフトクラウド

Azure

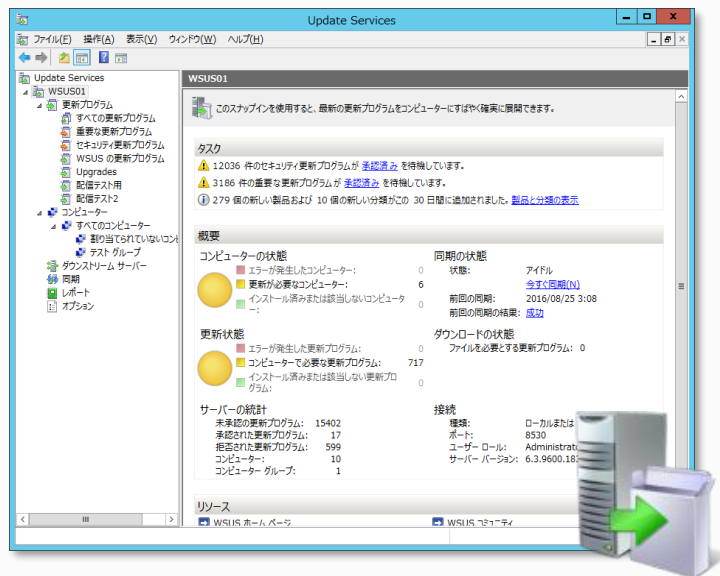
Office 365

3rd Party SaaS アプリ



Windows 11 の「更新プログラム」の管理

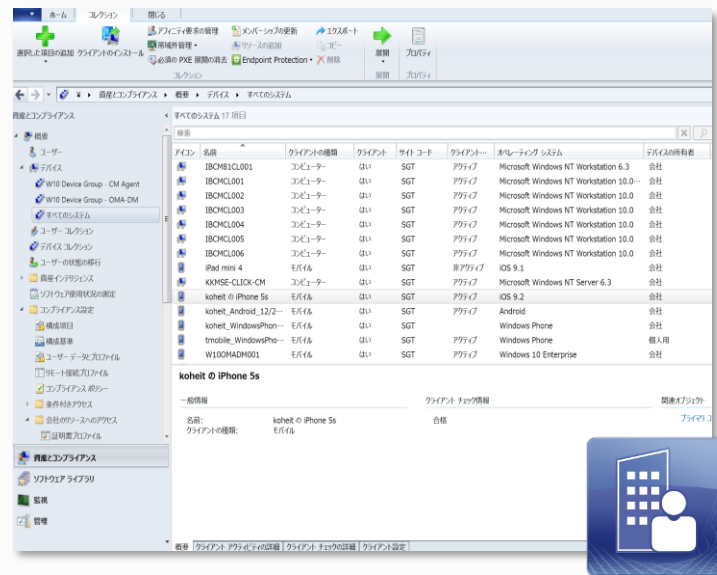
オンプレミス



Windows Update Server Service (WSUS)

- Windows Server の標準機能
- Windows Server 利用のライセンス
- 管理者によって配布プログラムを選択

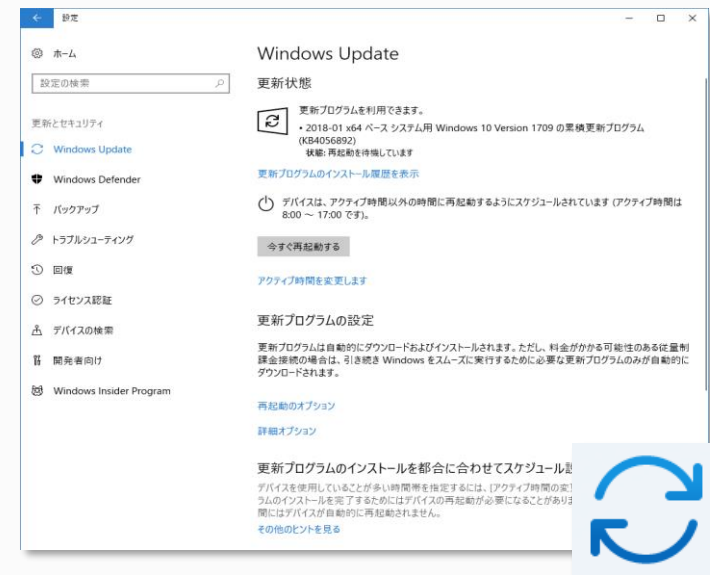
ハイブリッド可能



Configuration Manager (MECM)

- サーバー設置型の PC 管理製品
- 別途 MECM 用ライセンスが必要
- 管理者によって詳細な制御が可能

クラウド



Windows Update for Business (WUfB)

- インターネット上の Windows Update を利用
- 無償にて利用が可能
- 管理者によってアップデート タイミングを制御



1. Windows 11 の概要
2. Windows 11 の管理インフラ
3. Windows 11 の展開
4. Windows 11 の設定
5. Windows 11 のセキュリティ

Windows 11 の展開手法

Windows 11 ではどちらも選択可能

従来型

- コストは高いが、いくつかのシナリオでは有効
- 既存もしくは新しいデバイスに対するイメージでのアプローチ
- ドライバのインストール、アプリケーションの再インストール、データと設定の復元が必要

モダン型

- イメージングなし
- 新しいデバイスを生産的に使用できるように変換する
- 労力を削減し、コストを削減
- OEM によって提供されている、既にチューニングされた Windows 11 インストールを活用する

Windows 11 の展開手法

従来型

ワイプ & ロード

一般的な企業プロセス

- データ・設定のキャプチャー
- カスタム OS イメージの展開
- ドライブの注入
- アプリのインストール
- データ・設定のリストア

どのシナリオでも利用可能

インプレース アップグレード

Windows に任せる

- データ・設定の保存
- アプリ・ドライバーの保存
- 標準 OS イメージのインストール
- 全てのリストア

既存の Windows デバイス

モダン型

プロビジョニング

新しいデバイス向け新機能

- 企業用デバイスに変身
- 企業アプリの追加
- 企業設定の追加

オフライン シナリオ向け

Autopilot

クラウド展開の新機能

- 自動で企業用デバイスに変身
- クラウド環境のフル活用
- 管理もクラウド環境を想定

クラウド管理向け

オンプレミス



- Windows Server の標準機能
- Windows Server 利用のライセンス
- 管理者によって配布プログラムを選択

ハイブリッド可能



- サーバー設置型の PC 管理製品
- 別途 **MECM** 用ライセンスが必要
- 管理者によって詳細な制御が可能

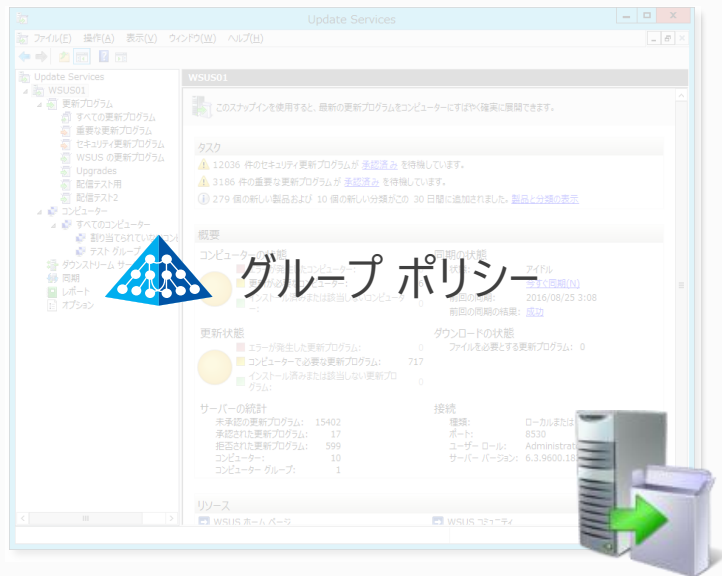
クラウド



- インターネット上の Windows Update を利用
- 無償にて利用が可能
- 管理者によってアップデート タイミングを制御

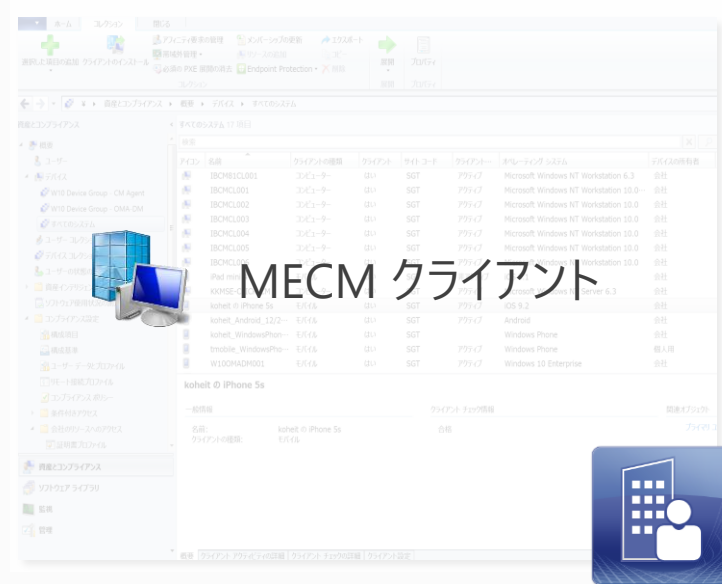
アップデート取得動作の制御方法

それぞれを動作させるためのクライアントの一般的な設定方法



Windows Update Server Service (WSUS)

グループ ポリシーによる設定が一般的
Microsoft Intune による設定も可能



Microsoft Endpoint Configuration Manager (MECM)

MECM の設定項目により設定が一般的
MECM の管理機能によって配布を行う



Windows Update for Business (WUfB)

Intune の MDM による構成
もしくはグループ ポリシーを利用して設定する



Windows Update Server Service (WSUS) の設定

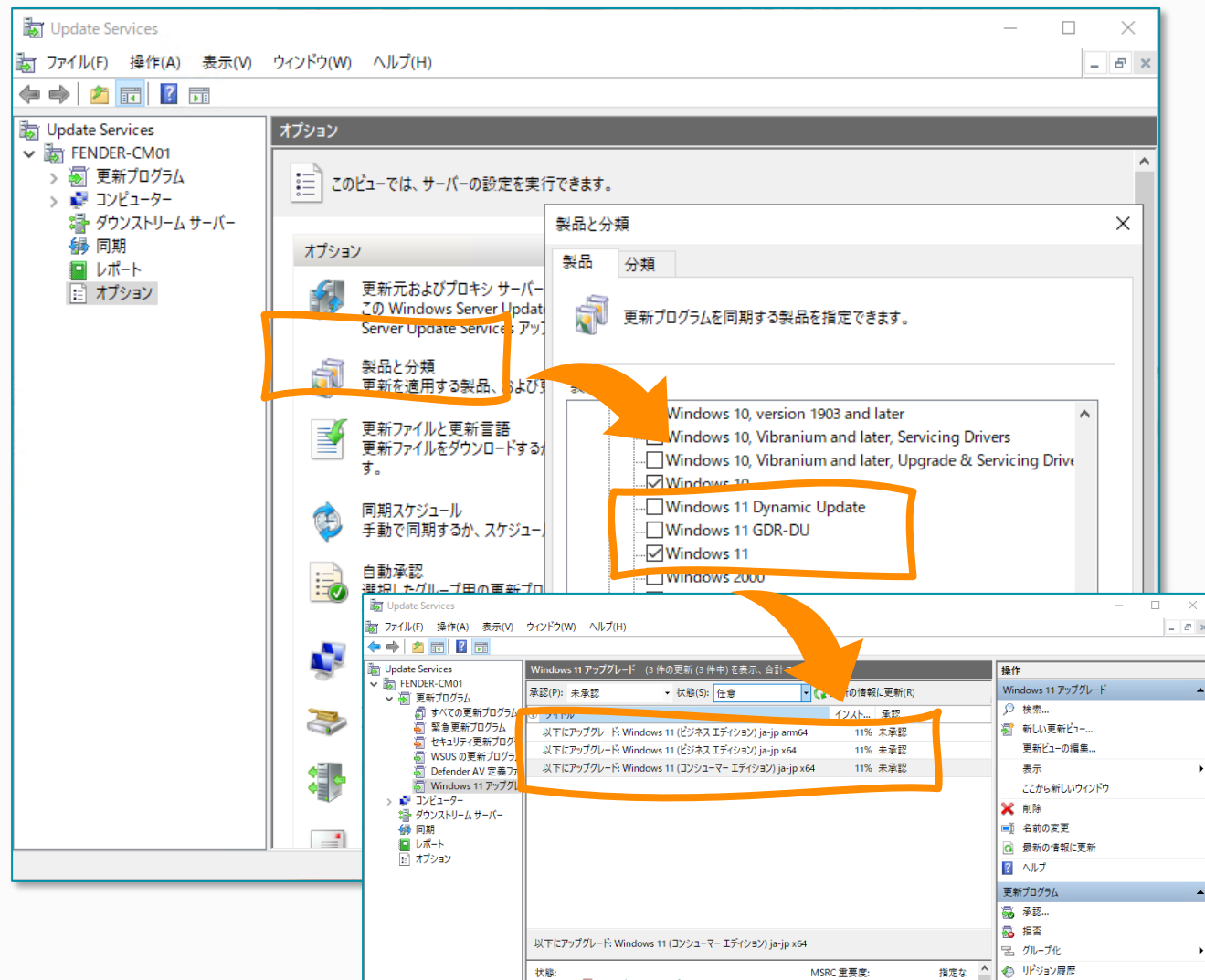
関連するプログラムを同期することで
アップグレード対象となるクライアントに対して
Windows 11 の配布が可能

1. [オプション] より [製品と分類] を選択
2. [製品] タブより「Windows 11」を選択
3. [分類] タブより「Upgrades」を選択
4. 同期を実行後、以下のプログラムを承認

[以下にアップグレード Windows 11 xxx エディション]

Windows 11 の準備

<https://docs.microsoft.com/ja-jp/windows/whats-new/windows-11-prepare>





Configuration Manager (MECM) の設定

ソフトウェア更新ポイントの機能を利用して、アップグレード対象となるクライアントに対して Windows 11 の配布が可能

1. [管理] - [サイト] - [サイト コンポーネントの構成] より [ソフトウェア更新ポイント] を選択
2. [製品] タブより「Windows 11」を選択
3. [分類] タブより「Upgrades」を選択
4. 同期を実行後、以下のプログラムを展開設定

[以下にアップグレード Windows 11 xxx エディション]

Windows 11 の準備

<https://docs.microsoft.com/ja-jp/windows/whats-new/windows-11-prepare>

The screenshot shows the MECM console with the following steps highlighted by orange arrows and boxes:

- Step 1:** In the left-hand navigation pane, the path **管理 > サイト > サイト コンポーネントの構成** is selected, and **ソフトウェア更新ポイント** is chosen from the list.
- Step 2:** In the **製品** (Products) tab, **Windows 11** is selected.
- Step 3:** In the **分類** (Classification) tab, **Upgrades** is selected.
- Step 4:** The main pane shows a list of Windows 11 upgrade programs. The following table represents the data shown in the screenshot:

アイコン	タイトル	アーキテクチャ	アイディ	必須	インストール済み	準備率 (%)
[Icon]	以下にアップグレード: Windows 11 (コンシューマー エディション) ja-jp x64	x64	3-2973	0	0	11
[Icon]	以下にアップグレード: Windows 11 (ビジネス エディション) ja-jp arm64	arm64	3-2973	0	0	11
[Icon]	以下にアップグレード: Windows 11 (ビジネス エディション) ja-jp x64	x64	3-2973	0	0	11



Microsoft Intune の設定

機能更新プログラム ポリシーを設定することで、
Windows Update for Business を利用可能
任意のタイミングで展開をコントロール

※ 本機能の利用には Windows E3 相当のライセンスが必要

※ 本機能とは別でカスタムポリシーにて WSUS の指定も可能

※ 上記ライセンスをお持ちでない場合は [更新リンク] から設定頂くことも可能

1. [デバイス] - [Windows] を選択
2. [Windows 10 以降向け機能更新プログラム] を選択
3. 「プロファイルの作成」をクリック
4. 「展開する機能更新プログラム」より展開する
Windows のバージョンを指定

Windows 11 の準備

<https://docs.microsoft.com/ja-jp/windows/whats-new/windows-11-prepare>

Microsoft Endpoint Manager admin center

ホーム > デバイス > Windows >

機能の更新プログラムの展開を作成する

機能の更新プログラムの展開

1 デプロイの設定 2 割り当て 3 確認および作成

Enable Windows Health Monitoring and select Windows Update scope to get detailed device states and errors. [詳細情報](#)

名前 * Windows 11 の展開 ✓

説明

機能展開設定

展開する機能更新プログラム ① Windows 11 ▼

この機能更新プログラムを選択して展開すると、(1) 該当する Windows ライセンスがボリューム ライセンスで購入されたか、(2) 組織をバインドする権限を持ち、関連する Microsoft ソフトウェア ライセンス条項 (<https://go.microsoft.com/fwlink/?linkid=2171206>) を受け入れているデバイスにこのオペレーティング システムを適用することに同意したものと見なされます。

前へ 次へ

Windows Update for Business の設定 - グループ ポリシー

グループ ポリシーでは以下の項目を設定することで
Windows Update によるアップグレードの管理が可能

※ 製品バージョンの指定には 2004 以降、ターゲットの指定には 1803 以降が必要
※ 上記バージョンに加え Windows の 2021 年 9 月以降の更新プログラムが必要

[コンピューターの構成]

- [管理用テンプレート]
- [Windows コンポーネント]
- [Windows Update]
- [Windows Update から提供される更新プログラムの管理]
- [ターゲット機能更新プログラムのバージョンを選択する]

グループ ポリシー Windows としてビジネス向け更新プログラムを構成する -
Windows Deployment | Microsoft Docs

<https://docs.microsoft.com/ja-jp/windows/deployment/update/waas-wufb-group-policy>

ターゲット機能更新プログラムのバージョンを選択する

ターゲット機能更新プログラムのバージョンを選択する

前の設定(P) 次の設定(N)

☐ 未構成(C) コメント:

☒ 有効(E)

☐ 無効(D)

サポートされるバージョン: Windows Server 2016 以降または Windows 10 以降

オプション:

どの Windows 製品のバージョンから機能更新プログラムを受け取りますか? 例: Windows 10

Windows 11

機能更新プログラムのターゲット バージョン

21H2

ヘルプ:

Windows Update の対象バージョンのページに記載されている通りに製品とバージョンを入力してください。

aka.ms/WindowsTargetVersioninfo

デバイスは、以降のスキャンで製品とバージョンを更新するよう Windows に要求します。

対象の製品を入力して [OK] または [適用] をクリックすると、aka.ms/WindowsTargetVersioninfo にある Microsoft ソフトウェアライセンス条項に同意したとみなされます。組織がソフトウェアのライセンスを提供している場合、その組織に義務を負わせる権限があることを認めたことになります。

無効な値を入力した場合、その値をサポートされている製品とバージョンの値に修正するまで、現在のバージョンが維持されます。

OK キャンセル 適用(A)

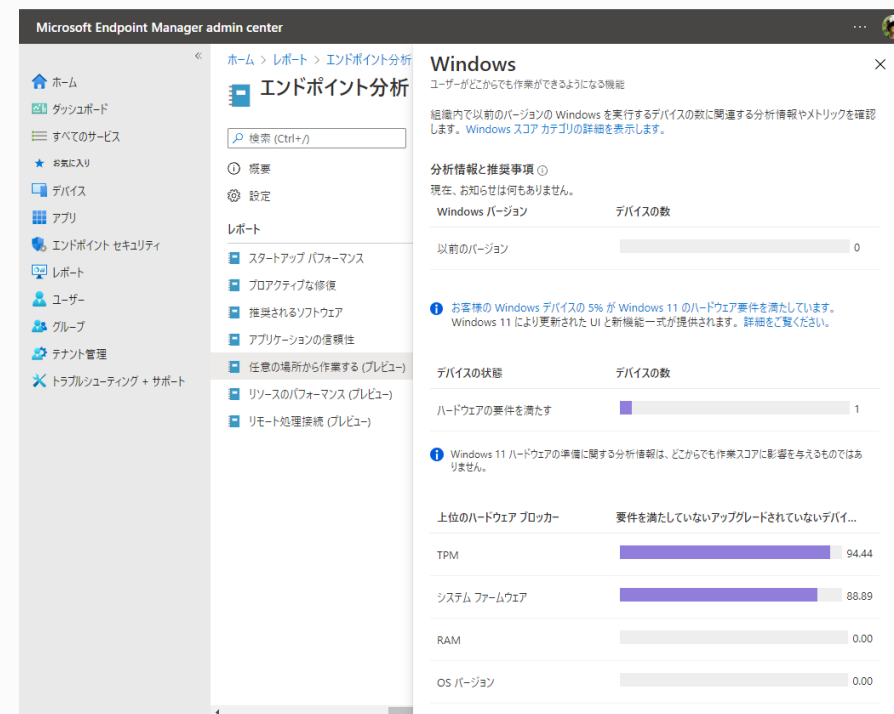
グループ ポリシー エディター

Windows 11 へのデバイスの準備状況を把握



Update Compliance

Windows の更新プログラムの監視ができるクラウド サービス



エンドポイント分析

Microsoft Endpoint Manager で利用できる分析レポート

Windows 11 の展開に役立つツール

<https://blogs.windows.com/japan/2021/10/12/tools-to-support-windows-11-deployment/>

Windows 11 の展開手法

従来型

ワイプ & ロード

一般的な企業プロセス

- データ・設定のキャプチャー
- カスタム OS イメージの展開
- ドライブの注入
- アプリのインストール
- データ・設定のリストア

どのシナリオでも利用可能

インプレース アップグレード

Windows に任せる

- データ・設定の保存
- アプリ・ドライバーの保存
- 標準 OS イメージのインストール
- 全てのリストア

既存の Windows デバイス

モダン型

プロビジョニング

新しいデバイス向け新機能

- 企業用デバイスに変身
- 企業アプリの追加
- 企業設定の追加

オフライン シナリオ向け

Autopilot

クラウド展開の新機能

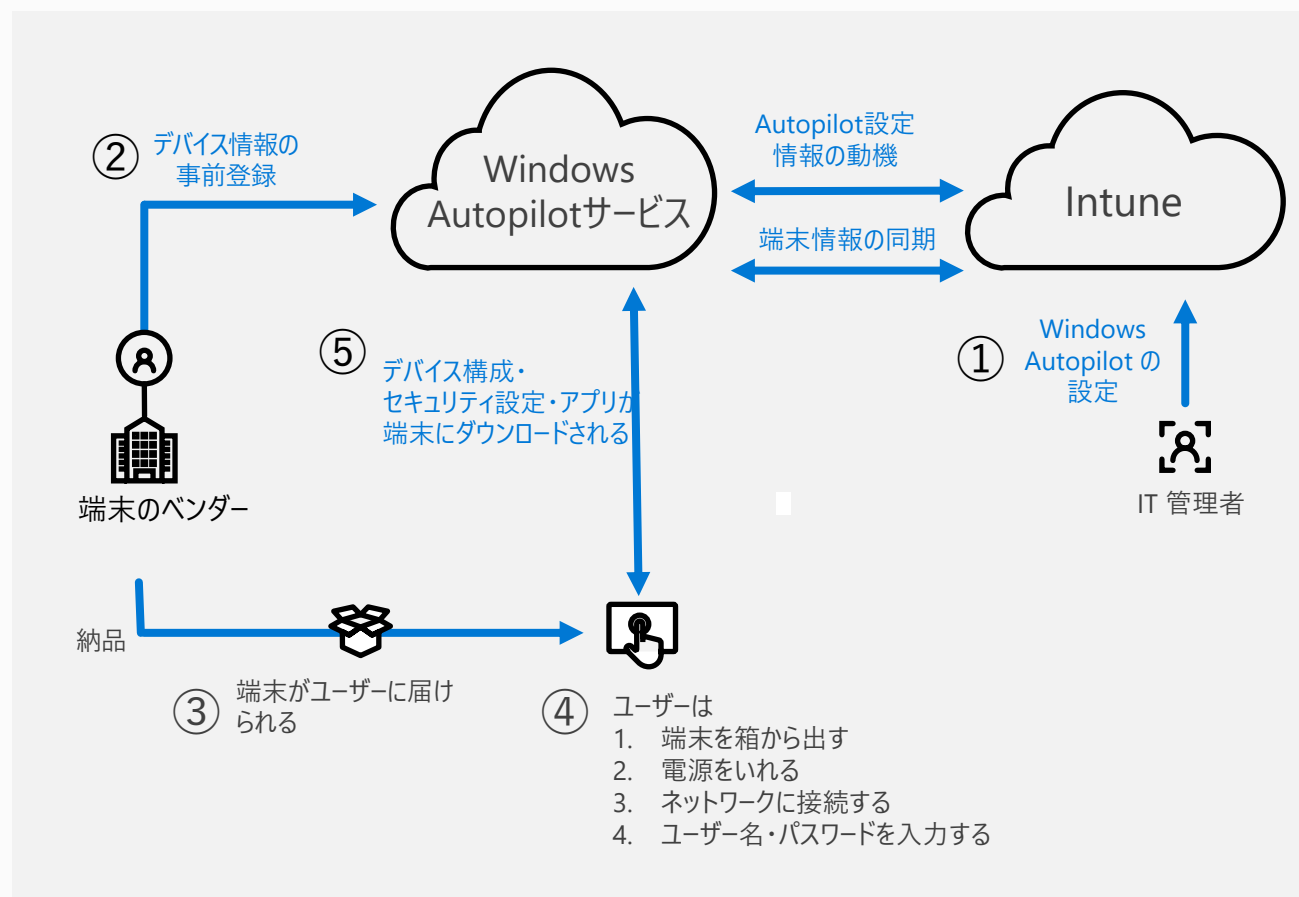
- 自動で企業用デバイスに変身
- クラウド環境のフル活用
- 管理もクラウド環境を想定

クラウド管理向け

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
- CM 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

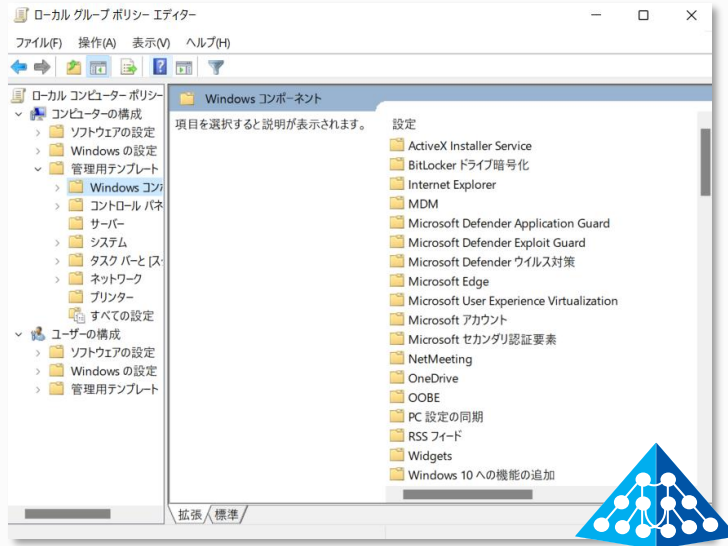




1. Windows 11 の概要
2. Windows 11 の管理インフラ
3. Windows 11 の展開
4. Windows 11 の設定
5. Windows 11 のセキュリティ

Windows 11 の「設定」

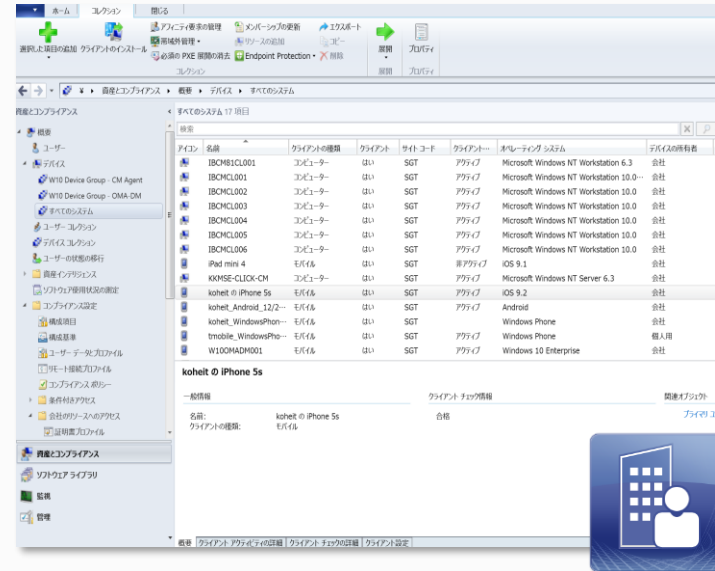
オンプレミス



Active Directory

グループ ポリシーによる設定管理

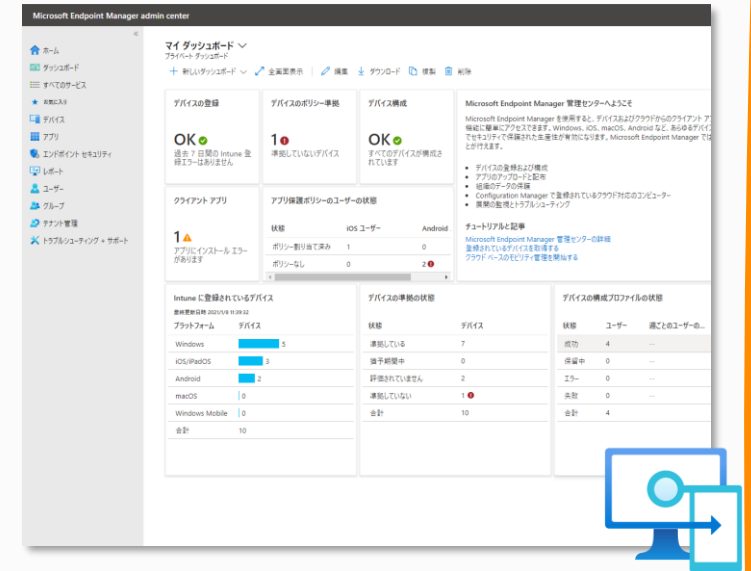
ハイブリッド可能



Configuration Manager
(MECM)

MECM クライアントによる設定管理

クラウド



Microsoft Intune

MDM ポリシーによる設定管理

Microsoft Intune による Windows 11 の設定

主な構成設定(構成プロファイル)の例

Endpoint保護...BitLocker暗号化、Windows Defender設定など

Identity保護...Windows Hello for Business設定など

各種資源配布...証明書配布、VPN設定、Wifi設定など

各種デバイス制限...各種デバイスの禁止設定、設定メニュー非表示など

Windowsアップデート設定...配信の最適化オプションなど

キオスクモード設定...表示アプリの制限、全画面表示の強制など

ファームウェア設定...DFCIファームウェア設定など(*Surface端末のみ)

構成プロファイルはデバイスやグループに配信して適用

プロファイルの作成

Intune 管理コンソールの設定イメージ

Endpoint Protection ①

Identity Protection ①

Microsoft Defender for Endpoint (W

PKCS のインポートされた証明書 ①

PKCS 証明書 ①

SCEP 証明書 ①

VPN ①

Wi-Fi ①

Windows の正常性の監視 ①

エディションのアップグレードおよびモードの切

カスタム ①

キオスク ①

セキュリティで保護された評価 (教育) ①

デバイスのファームウェア構成インターフェイス

デバイスの制限 ①

デバイスの制限 (Windows 10 Team) ①

ドメインへの参加 ①

ネットワーク境界 ①

管理用テンプレート

Endpoint Protection ...

Windows 10 以降

Windows 暗号化

Windows の設定 ①

デバイスの暗号化 ①

メモリーカードの暗号化 (モバイルのみ) ①

BitLocker の基本設定 ①

他のディスクの暗号化に対する警告 ①

Azure AD 参加中の暗号化の有効化を標準
ユーザーに許可する ①

暗号化方法の構成 ①

オペレーティング システム ドライブの暗号化 ①

固定データドライブの暗号化 ①

リムーバブル データドライブの暗号化 ①

BitLocker OS ドライブの設定 ①

起動時の追加認証 ①

互換性のない TPM チップでの BitLocker ①

必要

構成されていません

必要

構成されていません

ブロック

構成されていません

許可

構成されていません

有効にする

構成されていません

XTS-AES 128 ビット

XTS-AES 128 ビット

AES-CBC 128 ビット

必要

構成されていません

ブロック

構成されていません

これまで以上に多くの モバイル デバイス管理

クラウドとクラウド接続管理により、
増大するリモート ワーカーをサポートし、
オンプレミス接続の必要性をなくします。

MDM で使用できるグループ ポリシー
設定が増えたため、モダン管理への移行
がより簡単になりました。デバイス構成
設定カタログが更新され、かつては
MDM で構成できなかった 1,400 以上
の設定がリストアップされました。

Home > Devices > Create profile ...
Windows 10 and later - Settings catalog (preview)

1 Basics 2 Configuration settings 3 Assignments 4 Scope tags 5 Review + create

Settings catalog
With the settings catalog, you can choose which settings you want to configure. Click on Add settings to browse or search the catalog for the settings you want to configure.
[Learn more](#)

+ Add settings ⓘ

Settings picker
Use commas "," among search terms to lookup settings by their keywords
Search for a setting Search

+ Add filter

Browse by category

- Above Lock
- Accounts
- Administrative Templates
 - Control Panel
 - Add or Remove Programs
 - Display
 - Personalization
 - Printers
 - Programs
 - Regional and Language Options
 - User Accounts

11 settings in "Add or Remove Programs" subcategory [Select all these settings](#)

Setting name
☐ Go directly to Components Wizard (User)
☐ Hide Add - Remove Windows Components page (User)
☐ Hide Add New Programs page (User)
☐ Hide Change or Remove Programs page (User)
☐ Hide the "Add a program from CD-ROM or floppy disk" option (User)
☐ Hide the "Add programs from Microsoft" option (User)
☐ Hide the "Add programs from your network" option (User)
☐ Hide the Set Program Access and Defaults page (User)
☐ Remove Add or Remove Programs (User)
☐ Remove Support Information (User)
☐ Specify default category for Add New Programs (User)

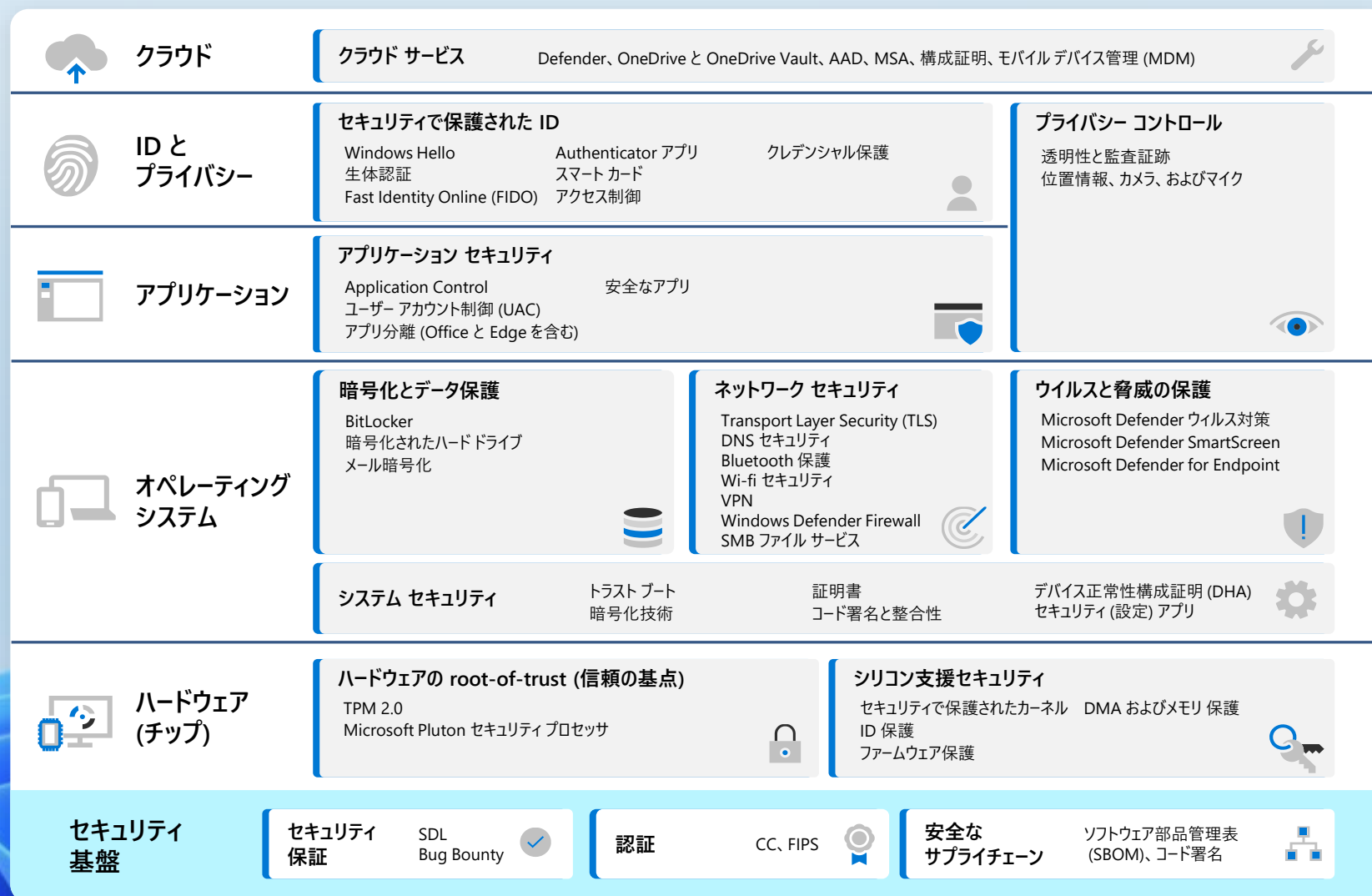
Previous Next



1. Windows 11 の概要
2. Windows 11 の管理インフラ
3. Windows 11 の展開
4. Windows 11 の設定
5. Windows 11 のセキュリティ

標準搭載のセキュリティ

ゼロトラスト
セキュリティモデルへの
移行を推進



ハードウェア概要

ハードウェアの root-of-trust とシリコン支援セキュリティの強力な組み合わせを通じて、Windows 11 はすぐに利用できる組み込みのハードウェア保護を提供します。

ファームウェアの読み込み時に**システムの整合性を保護し、維持**します。

TPM 2.0 を使用した Windows Hello や BitLocker などの機能によって**セキュリティを強化**します。

仮想化ベースのセキュリティ (VBS) を使用して、**コードの整合性と重要な情報を保護**します。

**クラウド**

クラウド サービス
Defender、OneDrive と OneDrive Vault、AAD、MSA、構成証明、モバイル デバイス管理 (MDM)

**ID とプライバシー**

セキュリティで保護された ID
Windows Hello
生体認証
Fast Identity Online (FIDO)

Authenticator アプリ
スマート カード
アクセス制御

クレデンシャル保護

プライバシー コントロール
透明性と監査証跡
位置情報、カメラ、およびマイク

**アプリケーション**

アプリケーション セキュリティ
Application Control
ユーザー アカウント制御 (UAC)
アプリ分離 (Office と Edge を含む)

安全なアプリ

暗号化とデータ保護
BitLocker
暗号化されたハードドライブ
メール暗号化



ネットワーク セキュリティ
Transport Layer Security (TLS)
DNS セキュリティ
Bluetooth 保護
Wi-fi セキュリティ
VPN
Windows Defender Firewall
SMB ファイル サービス



ウイルスと脅威の保護
Microsoft Defender ウィルス対策
Microsoft Defender SmartScreen
Microsoft Defender for Endpoint



システム セキュリティ
トラスト ブート
暗号化技術

証明書
コード署名と整合性

デバイス正常性構成証明 (DHA)
セキュリティ (設定) アプリ



**ハードウェア (チップ)**

ハードウェアの root-of-trust (信頼の基点)
TPM 2.0
Microsoft Pluton セキュリティ プロセッサ



シリコン支援セキュリティ
セキュリティで保護されたカーネル
DMA およびメモリ 保護
ID 保護
ファームウェア保護



セキュリティ 基盤

セキュリティ 保証
SDL
Bug Bounty



認証
CC、FIPS



安全な サプライチェーン
ソフトウェア部品管理表 (SBOM)、コード署名



オペレーティング システム概要

Windows 11 では、ハードウェアとソフトウェアが連携してオペレーティング システムを保護します。

BitLocker¹ および Windows 情報保護² で高度な暗号化を使用して、データの紛失や盗難のリスクを低減します。

複数の保護レイヤーでネットワーク セキュリティを強化します。

ウイルスやその他の脅威に対するインテリジェントな保護を提供します。

強力なシステム セキュリティにより、資格情報、コードの整合性、およびネットワーク アクセスが保護されます。



1. TPM 2.0 が必要です。
2. Windows 情報保護では、設定を管理するためにモバイル デバイス管理 (MDM) または System Center Configuration Manager が必要です。これらの製品は別売りです。Active Directory により管理が容易になりますが、必須ではありません。

アプリケーション概要

ユーザーの安全と生産性を維持するために、Windows 11 は重要なデータとコードの整合性をアプリケーション セキュリティで多層防御します。

Windows Application Control により、IT 担当者が **Windows デバイス上で実行するアプリケーションやドライバーを制御**できます。

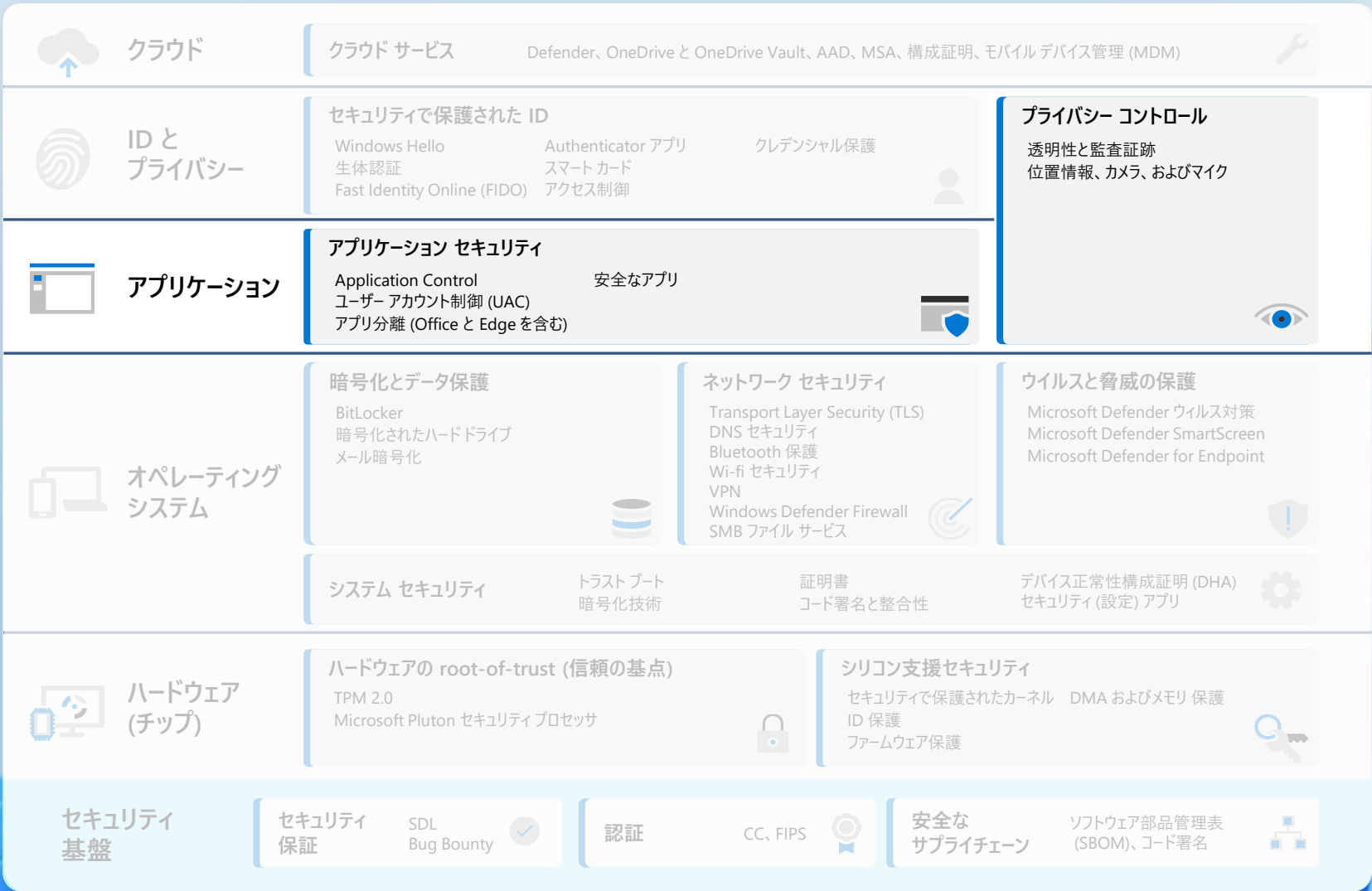
Microsoft Defender Application Guard¹ を使用して、**仮想コンテナ上で Web サイトや Office ファイルを安全に実行**します。

マルウェアが管理者権限を取得するのを防ぎ、PC に変更を加えることを防ぎます。

仮想コンテナでユニバーサル Windows プラットフォーム アプリを実行して、**ファイル システムとレジストリを保護**します。

開発者がゼロからセキュリティを構築することが可能になります。

1. Application Guard を有効化するのに必要なハードウェアを OEM が供給



ID とプライバシー概要

Windows 11 では、パスワードレスのセキュリティにより、デバイスからクラウドまでの安全なシングルサインオンが改善されています。特徴は次の通りです。

Microsoft Authenticator アプリ、Windows Hello for Business、セキュリティキー、または確認コードによって**多要素認証**が有効化されます。

Microsoft 365 を含む**アプリやサービスにシングルサインオン**できます。

ハードウェアで支援されたセキュリティにより、**生体認証データが保護**されます。

USB 生体認証キー、NFC、BLE* など、固有のビジネスニーズに応じて **FIDO2 セキュリティキーやフォームファクタを選択**できます。

* NFC=Near Field Communication, BLE = Bluetooth Low Energy

**クラウド**

クラウド サービス
Defender、OneDrive と OneDrive Vault、AAD、MSA、構成証明、モバイル デバイス管理 (MDM)

**ID とプライバシー**

セキュリティで保護された ID
Windows Hello 生体認証
Fast Identity Online (FIDO)

Authenticator アプリ
スマートカード
アクセス制御

クレデンシャル保護



プライバシー コントロール
透明性と監査証跡
位置情報、カメラ、およびマイク

**アプリケーション**

アプリケーション セキュリティ
Application Control
ユーザー アカウント制御 (UAC)
アプリ分離 (Office と Edge を含む)

安全なアプリ



**オペレーティングシステム**

暗号化とデータ保護
BitLocker
暗号化されたハードドライブ
メール暗号化



ネットワーク セキュリティ
Transport Layer Security (TLS)
DNS セキュリティ
Bluetooth 保護
Wi-fi セキュリティ
VPN
Windows Defender Firewall
SMB ファイル サービス



ウイルスと脅威の保護
Microsoft Defender ウィルス対策
Microsoft Defender SmartScreen
Microsoft Defender for Endpoint



システム セキュリティ

トラスト ブート
暗号化技術

証明書
コード署名と整合性

デバイス正常性構成証明 (DHA)
セキュリティ (設定) アプリ



**ハードウェア (チップ)**

ハードウェアの root-of-trust (信頼の基点)
TPM 2.0
Microsoft Pluton セキュリティ プロセッサ



シリコン支援セキュリティ
セキュリティで保護されたカーネル
DMA およびメモリ 保護
ID 保護
ファームウェア保護



セキュリティ基盤

セキュリティ保証

SDL
Bug Bounty



認証
CC、FIPS



安全なサプライチェーン
ソフトウェア部品管理表 (SBOM)、コード署名



クラウド管理概要

Windows 11 は Microsoft クラウド サービスと連携して、組織がマルチクラウド セキュリティ インフラストラクチャを強化し、ハイブリッド クラウド ワークロードを保護し、アクセス制御と脅威の軽減を図りながら、機密情報を保護することを可能にします。

OneDrive Vault を含む Microsoft OneDrive を使って、**ファイルをクラウドに保存して保護**します。¹

どこからでもアプリやサービスへの**セキュアなアクセス、ID 管理、シングル サインオン**を提供します。²

Microsoft Intune で**セキュリティ コンプライアンスと条件付きアクセスを強制**します。^{1,2}

Microsoft Azure 構成証明を使用して、ネットワークに接続する**デバイスの健全性と安全性を確保**します。

1. 別売りです。
2. 別売りの Azure Active Directory が必要です。

クラウド

クラウド サービスDefender、OneDrive と OneDrive Vault、AAD、MSA、構成証明、モバイル デバイス管理 (MDM)

 ID とプライバシー	セキュリティで保護された ID Windows Hello 生体認証 Fast Identity Online (FIDO) Authenticator アプリ スマート カード アクセス制御 クレデンシャル保護		 プライバシー コントロール 透明性と監査証跡 位置情報、カメラ、およびマイク
	 アプリケーション アプリケーション セキュリティ Application Control ユーザー アカウント制御 (UAC) アプリ分離 (Office と Edge を含む) 安全なアプリ		
 オペレーティングシステム	暗号化とデータ保護 BitLocker 暗号化されたハードドライブ メール暗号化	ネットワーク セキュリティ Transport Layer Security (TLS) DNS セキュリティ Bluetooth 保護 Wi-fi セキュリティ VPN Windows Defender Firewall SMB ファイル サービス	ウイルスと脅威の保護 Microsoft Defender ウィルス対策 Microsoft Defender SmartScreen Microsoft Defender for Endpoint
	システム セキュリティ トラスト ブート 暗号化技術	証明書 コード署名と整合性	デバイス正常性構成証明 (DHA) セキュリティ (設定) アプリ
 ハードウェア (チップ)	ハードウェアの root-of-trust (信頼の基点) TPM 2.0 Microsoft Pluton セキュリティ プロセッサ		シリコン支援セキュリティ セキュリティで保護されたカーネル DMA およびメモリ 保護 ID 保護 ファームウェア保護
	セキュリティ 基盤 セキュリティ 保証 SDL Bug Bounty		認証 CC、FIPS
		安全な サプライチェーン ソフトウェア部品管理表 (SBOM)、コード署名	

1. 別売りです。
2. 別売りの Azure Active Directory が必要です。

エンドポイントのモダン化に向けたロードマップ

ID とアクセス、デバイスとアプリ管理、ゼロトラスト



リモート/ハイブリッド ワーカー向けの
エンドポイントの展開と保護

フロントライン ワーカーのエンドポイント
エクスペリエンスを向上

次世代のエンドポイント資産を再構築



ID とアクセス

クラウド ID とパスワードレス サインイン
条件付きアクセス
Microsoft Defender for Identity



クラウド ファイルとサービス

Exchange、SharePoint、OneDrive および Teams
Microsoft Defender for Cloud Apps
Microsoft Defender for Office 365



モダン デバイス

Windows、iOS および Android
Surface および Secured-core PC
HoloLens、Surface Hub およびその他のデバイス



ご紹介した
ポイント



エンドポイント セキュリティ

ハードウェアの root-of-trust (信頼の基点)
クラウドで管理されたファームウェア
Windows Hello for Business (WHfB)
Microsoft Defender for Endpoint



仮想化されたエンドポイント

Windows 365
Azure Virtual Desktop



エンドポイント サービス

Windows Update for Business (WUfB)
M365 アプリ月次エンタープライズ チャンネル



Microsoft Managed Devices

Device management
Security monitoring



デバイス管理

Windows Autopilot
構成、アプリおよびポリシー
デバイスの正常性およびコンプライアンス
エンドポイント分析
共同管理

ご紹介した
ポイント



ゼロトラスト

ID	アプリ
エンドポイント	インフラ
データ	ネットワーク

ご紹介した
ポイント

Thank you



© Microsoft Corporation. All rights reserved.

本資料は情報提供のみを目的としており、本資料に記載されている情報は、本資料作成時点でのマイクロソフトの見解を示したものです。状況等の変化により内容は変更される場合があります。本資料に特別条件等が提示されている場合、かかる条件等は、貴社との有効な契約を通じて決定されます。

それまでは、正式に確定するものではありません。従って、本資料の記載内容とは異なる場合があります。また、本資料に記載されている価格はいずれも、別段の表記がない限り、参考価格となります。貴社の最終的な購入価格は、貴社のリセラー様により決定されます。

マイクロソフトは、本資料の情報に対して明示的、黙示的または法的な、いかなる保証も行いません。