



Windows 10

Anniversary Update
法人向けカタログ

第 1 版 (2016 年 8 月)

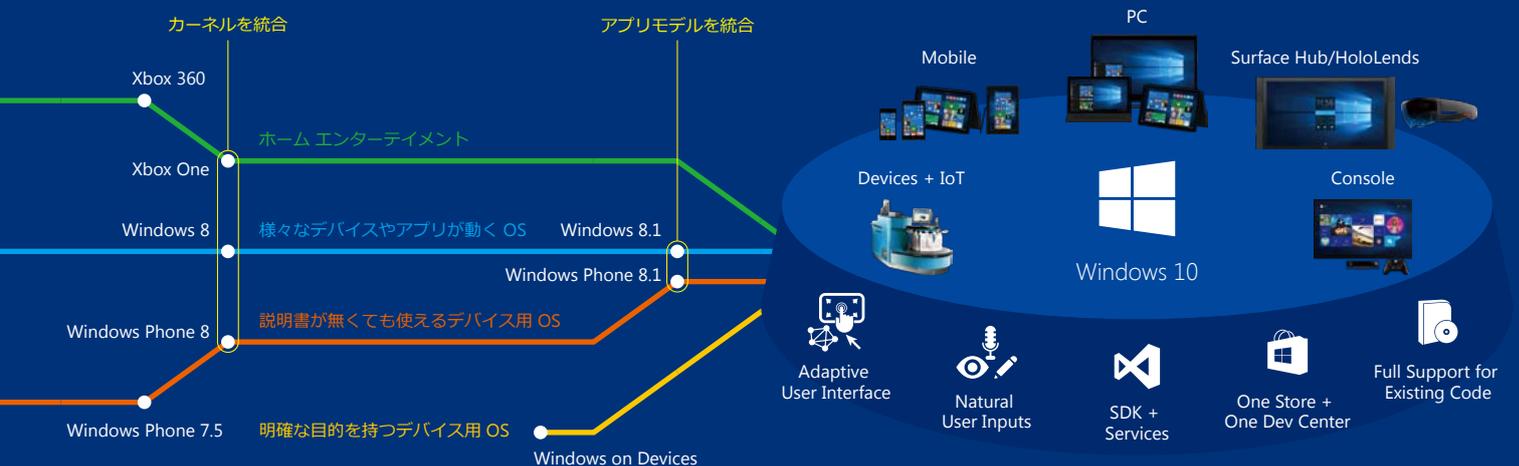
あなたのビジネスをアップグレード

One Core, One Windows

急成長を遂げたモバイルとクラウドの世界。マイクロソフトも新しい時代にあわせて、トランスフォーメーション(変革)を進めています。「すべての机と家庭にコンピュータを」というマイクロソフト創立時の目標を受け継ぎ、企業や組織、個人が、より多くのこと、素晴らしいことを実現するためのお手伝いをする、それが Windows のビジョンです。

Windows 10 では、すべてのクライアント オペレーティング システム (OS) を共通化。モバイル、クラウド、デバイスを有機的につなぎ、画期的なエクスペリエンス (体験) を提供し、どのデバイスを手にしていても、ユーザーはシームレスな体験をすることができます。

Windows 10 では、これからも Windows as a Service (サービスとしての Windows) として、選ばれ、愛される Windows となるために、継続的な進化をご提供し続けます。



企業で Windows 10 を活用する 5 つのメリット

最新のセキュリティ脅威に対抗できる
プラットフォーム

日々の作業を、もっと効率的に、
もっとスマートに

触れてみたくなるほどに、
革新的なデバイス

クラウド時代の
クライアント管理機能を提供

すべてのデバイスに、
いつでも最適な Windows を

多層防御に加えて、侵入後の対策も行えるコンピューティング環境を

Windows 10 では、4 つの分野 (デバイスによる保護、マルウェア対策、ID の保護、データの保護) におけるセキュリティ機能を追加。組織の情報を多層的に防御できるプラットフォームを提供してきました。一方で、セキュリティ脅威は日々進化。より侵入する能力の高い攻撃も発生しており、まったく新しい種類の攻撃には防御策が間に合わないため、侵入者への対策も防御と同じように重要と言われる時代になっています。

マイクロソフトでは、このようなセキュリティ脅威にも対応できる OS として Windows 10 Anniversary Update (ビルド番号 1607) をリリース。Pre-Breach (防御策) の一層の強化はもちろん、Post-Breach (侵入後の対策) も行える新機能を追加しています。条件付きアクセス制御では、多要素認証によりユーザーのなりすましからビジネス データへのアクセスを防御。さらに、Windows Defender Advanced Threat Protection では、デバイスの挙動を監視することにより、侵入を即座に検知。マイクロソフトが持つ膨大なセキュリティ対策のノウハウを活用して、侵入ケースごとに適切な対応を行うことができます。

また、Windows as a Service として、防御策にも最新機能を常に提供。Pre-Breach と Post-Breach のどちらにも対応できる、より信頼性の高い OS として進化を続けています。



- Windows Defender Advanced Threat Protection
 - Windows Hello
 - Windows Information Protection
 - Device Guard
 - Credential Guard
 - Windows Defender/SmartScreen
 - リモートワイプ
 - BitLocker/BitLocker to GO
 - ロックダウン
- 4 ページ
-
- Microsoft IME
 - Windows Ink
 - 使い慣れたスタートメニュー
 - ユニバーサル アプリ
 - Cortana
 - Microsoft Edge
- 6 ページ
-
- デスクトップ/ノート
 - タブレット
 - 2 in 1 デバイス
 - Surface Hub
 - Microsoft HoloLens
 - Windows Holographic
 - Windows 10 Mobile
 - Continuum
- 7 ページ
-
- Azure Active Directory Join
 - Microsoft Intune
 - モバイル デバイス管理 (MDM)
 - Windows Server 2016 AD FS
 - 条件付きアクセス制御
 - Windows Store for Business
- 8 ページ
-
- Windows as a Service
 - Windows Insider Program
 - Windows Update for Business
 - Windows Server Update Services
 - System Center Configuration Manager
 - インプレース アップグレード
 - Windows ICD ツール
 - Windows Upgrade Analytics Service
- 9 ページ

最新のセキュリティ脅威に対抗できるプラットフォーム

最新で高度な攻撃に対処するためのクラウドベースのセキュリティ対策

最近のサイバー攻撃は様々な方法で組織のネットワーク内への侵入を試みます。現在のセキュリティ対策 (マルウェアからの攻撃を防ぐ対策) では防ぎきれないこともあります。また、攻撃の内容を見てもネットワークの破壊や情報漏洩などによって組織の信頼を失墜させる、特定の組織を標的とした攻撃がほとんどで、1 インシデントあたり平均 1,200 万ドルのコストがかかっています。Windows Defender Advanced Threat Protection (WDATP) は、世界最大規模のセンサー群から収集される情報と、マイクロソフトの社内エキスパートやセキュリティ パートナーから成る専門家チームが提供する情報を活用。マイクロソフトが持つ包括的な脅威へのインテリジェンスをベースとした攻撃検知機能をクラウドベースのサービスとして提供し、クライアント端末への悪意のある攻撃の検出、調査を行います。

OS ビルドインのサービスで情報収集

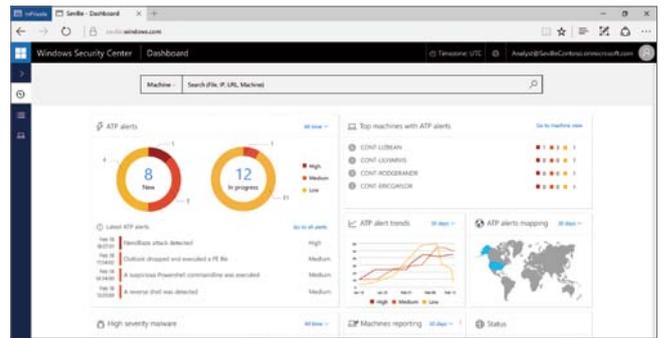
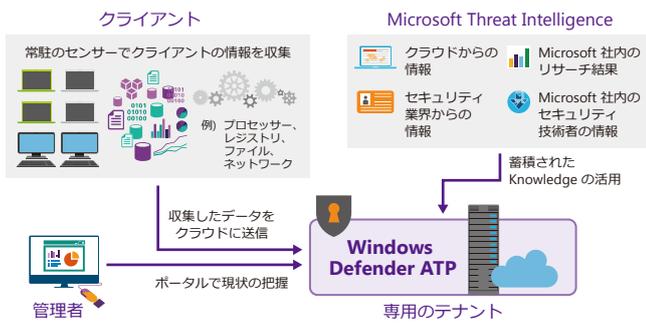
Windows 10 1607 に標準で含まれるサービスを利用して、デバイスの情報だけでなく、稼働中のプロセス情報やネットワークコネクションの情報を収集。脅威の検出に必要な情報を随時クラウド上のテナントにアップロードし、解析を実施します。

クラウドでデータ分析し、脅威を検出、対処方法を提示

デバイスから送信されたデータをクラウド上で分析し、攻撃の挙動や兆候をすばやく検知。管理者ポータルにアラートを表示すると共に、マイクロソフトのノウハウを基にした対処方法を提示します。アラート検出前後の詳細な挙動も時系列に表示、攻撃の内容の把握も可能です。攻撃による影響が拡大しないようにサポートします。

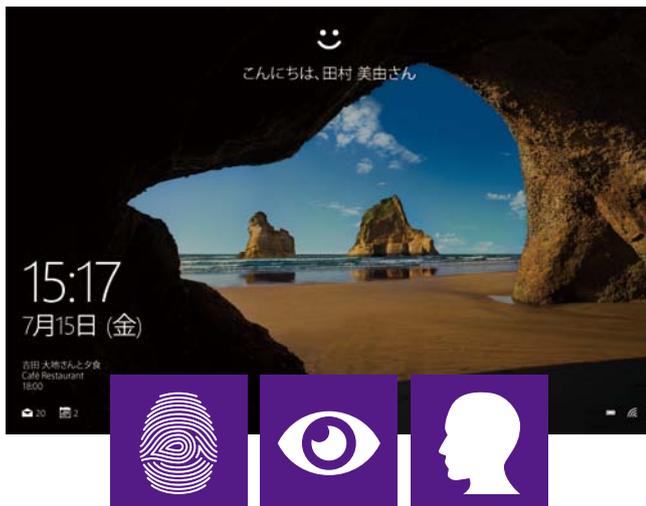
ビッグデータをもとに新たな脅威の検出にも対応

10 億台を超えるデバイスからの情報、2.5 兆のインデックス化された URL、6 億件のオンライン評価データなど、マイクロソフトが蓄積する膨大なセキュリティ情報をもとに分析サービスを提供。クライアントの挙動を監視し、新たな脅威にさらされているデバイスもすばやく検知します。



生体認証 Web でも利用可能に、Windows Hello

Windows Hello は、顔、虹彩、指紋でユーザーを認証し、パスワードを入力することなくサインインできる、生体認証セキュリティ。OS レベルでユーザーを認証するため、アドインも不要です。Windows 10 1607 では、ストア アプリや Microsoft Edge でも Windows Hello が利用可能に。カメラで顔を認識させたり、指紋センサーにタッチしたりするだけで、資格情報が必要となる企業アプリや Web サイトへのセキュアにアクセスできます。ポリシーや MDM で詳細項目の設定も可能です。



企業・組織のデータを自動的に暗号化して保護

BYOD やモバイルが浸透した現在のビジネス環境において企業データを保護するには、システム レベルで識別し暗号化することが重要です。Windows Information Protection (WIP) では、企業データと個人データを識別して格納。Microsoft Intune などの モバイルデバイス管理ソリューションからポリシーを設定し、企業データと個人用アプリとのやり取りをブロックしたり、監査したりすることができます。クラウドサービスを企業の領域として指定することも可能。クラウドから取得したデータを企業データとして安全に扱うことが可能になります。



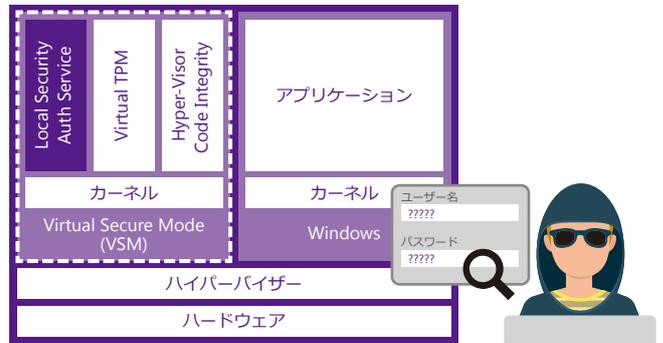
Device Guard で悪意のあるアプリの侵入をブロック

Device Guard は、未知のマルウェアの侵入など、新しい脅威に対抗する高度な保護機能です。Device Guard を有効にすると、マイクロソフトおよび組織により信頼された証明書で署名されたアプリだけを実行できます。メールに添付された未知の実行ファイルなど、ユーザーのデバイスで悪意のあるアプリが実行される可能性をなくします。



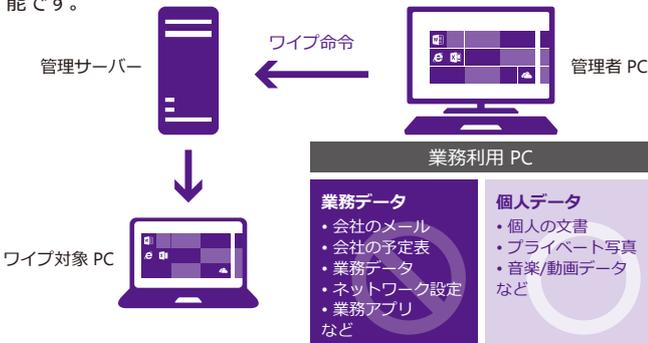
基幹業務アプリの資格情報を安全なコンテナで保護

Windows 10 では Credential Guard により、セキュリティで保護された領域に資格情報を隔離。OS の実行領域とは異なる場所に保管することで、資格情報の不正な抽出を遮断。万が一の不正アクセス時にも被害を最小限に留めます。



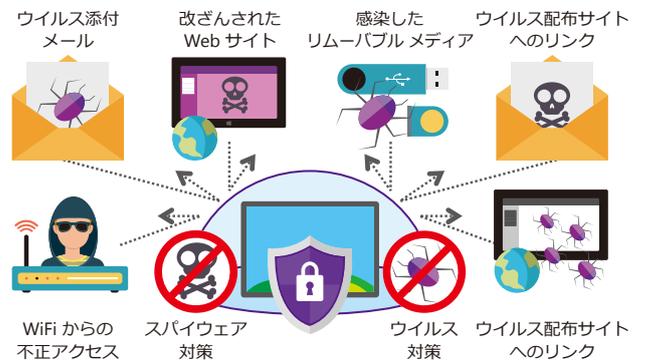
端末紛失時はリモート ワイプで業務データの漏えいを防止

万が一デバイスを紛失した際には Windows Information Protection で保護された業務データなどをリモート ワイプ。VPN の設定や電子証明書なども消去できます。また、部分的に情報をワイプする セレクティブ ワイプだけでなく、フルワイプのメッセージにも対応。リモートから工場出荷時の状態に戻すことができます。機能の利用には、Microsoft Intune などの MDM ソリューションと連携により利用可能です。



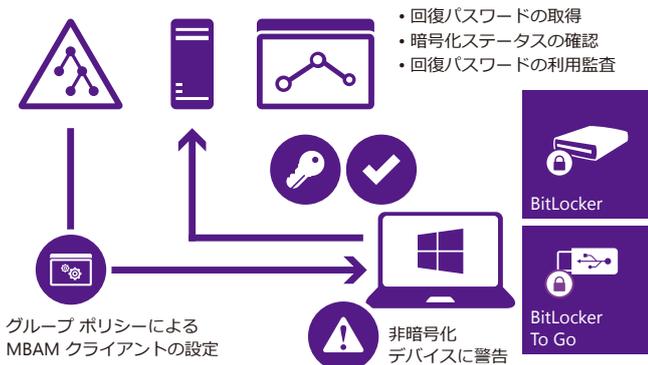
実行中も悪意のある攻撃からデバイスを防御

Windows 10 では、疑わしいアプリやファイルの実行を OS レベルで防止。疑わしいファイルのダウンロードは、Windows Defender が検知し、ワンクリックで除去。SmartScreen フィルターでは、疑わしいサイトへのアクセスだけでなく、疑わしいアプリが実行されないように監視します。



BitLocker による最先端のディスク暗号化ソリューション

デバイスの OS 領域および、データ保存領域全体を BitLocker により暗号化。ディスクの使用領域だけを暗号化でき、暗号処理時間の短縮が可能。グループ ポリシーにより暗号化された外部媒体にだけデータを保存するよう制御が行えるほか、管理ツールでプロビジョニングを行い、保護の徹底を実現できます。



作業に不必要な機能とアプリをロックダウン

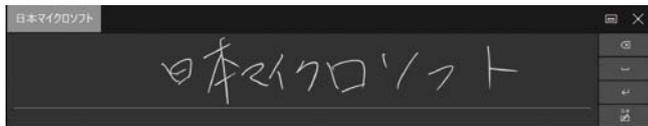
デバイス管理ポリシーを使用すると、特定の機能やアプリだけを利用できるようにユーザー エクスペリエンスをコントロールできます。例えば、空港のキオスク端末にはチェックイン用のアプリだけが表示されているように、学生やタスクワーカーのデバイスには、必要なアプリだけが実行できます。



日々の作業を、もっと効率的に、もっとスマートに

旬な用語にも対応、どんどん使いやすくなる日本語入力 (IME)

Windows 10 ではアップデートを重ねるごとにIMEの使いやすさと入力精度が向上。たとえば「きょう」と入力すると、日付と認識して西暦や和暦の日付を変換候補に表示。クラウド候補を利用することで最新の流行語にも迅速に対応します。入力履歴を保存しないプライベートモードも搭載。ペンによる手書き入力は文字数に制限がなくなり、認識精度も向上しており、より使いやすくなりました。



あらゆる作業で手書きを活用できる、Windows Ink

Windows Ink ワークスペースを活用すれば、付箋紙にメモを書いてリマインダーを作成したり、スケッチパッドに定規を使って描画したり、画面キャプチャに手書きコメントを追加したりできるようになります。Windows Inkは、OfficeやMicrosoft Edge、マップなどのアプリにも対応。APIを提供しているため、企業アプリにペンを活用したシナリオを実装する敷居が格段に低くなっています。



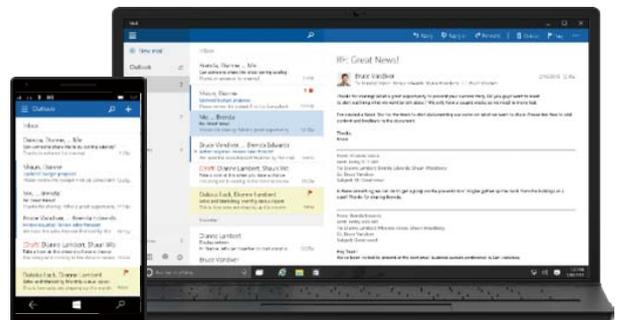
今まで以上に使いやすく、手に馴染む操作感

Windows 10のスタートメニューでは、メニューの左側にWindows 7と同じようにアプリの一覧が、右側にWindows 8のスタート画面でおなじみのライブタイルが並ぶ構造になっており、高さや幅は自由に変更できます。Windows 7ユーザーもWindows 8ユーザーも違和感なく使い始められます。



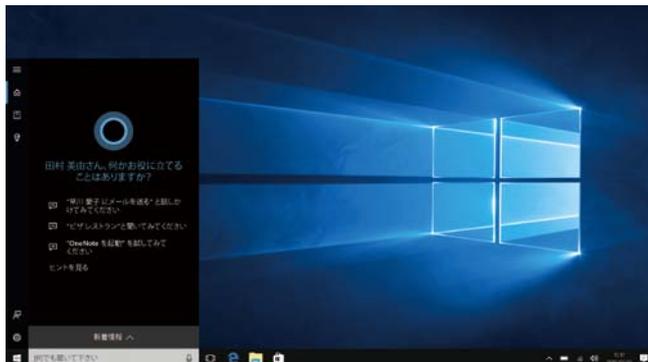
すべてのWindows 10でそのまま活用できる、Windows ユニバーサル アプリ

Windows ユニバーサル アプリなら、デバイスの種類を問わず使えるので、いつのアプリをPC、タブレット、スマートフォンへと展開できます。その好例が新しいOutlook。利用するデバイスにあわせて、画面をシームレスにスケールします。組織では、基幹業務アプリを1つ作成するだけで、あらゆるデバイスで実行することができます。



仕事でもプライベートでも賢いパートナー、Cortana

画面ロック中でも「コルタナさん」と呼びかければ利用できるようになったパーソナルアシスタント、Cortanaの日本語の音声により自然になりました。電車の遅延情報、ポンドやオンスの単位変換、為替情報、地震情報、フライト情報などに対応し、さらなる成長を続けています。OneDrive for Businessも検索対象に設定できます。



より軽量化にしながら、拡張も可能になった、Microsoft Edge

Web標準サポートと高速なブラウジングが特長のMicrosoft Edgeは、さらなる軽量化を実現。Windowsストアから拡張機能の追加も可能になりました。広告のブロック、Webページの自動翻訳、マウスのジェスチャーによるブラウジングなどの機能がすでに提供されており、ユーザーの用途に応じて拡張できます。



触れてみたくなるほどに、革新的なデバイス

働き方に合わせ、最も生産性の高いデバイスを選択可能

Windows 10 では、使い慣れたマウスやキーボードはもちろん、タッチ操作やペン入力などの入力方法もネイティブでサポート。デスクトップ、ノート、タブレット、XBOX などのデバイスをラインアップしており、スマートフォンや大画面端末、レンズ デバイスなども提供しております。Windows 10 IoT Enterprise は、産業デバイスのために特定の機能だけに制限することも可能。あなたの働き方に最もフィットする Windows をご選択いただけます。



コラボレーションに特化した大画面デバイス Surface Hub

Surface Hub は、Windows 10 を搭載した大画面デバイスです。ホワイトボードやディスプレイとしてだけでなく、Skype for Business を活用したリモート会議、ユニバーサル Windows アプリを活用した業務利用など、人と人とのコラボレーションの在り方、働き方を革新します。



現実世界にホログラムを重ね合わせる、 Microsoft HoloLens*

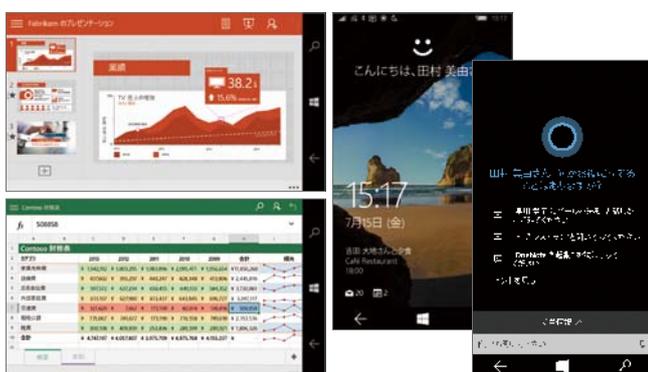
* 北米市場のみリリース (2016年8月現在)

Windows 10 を搭載した世界初のホログラフィック コンピューティングです。Windows Holographic プラットフォームにより、実際に見える物体とホログラムを重ねて表示する Mixed Reality を実現。設計図面の立体化、共有データの視覚化、トレーニングや共同作業など、組織や企業内での活用が期待されています。



Windows 10 Mobile 搭載の 豊富なスマートフォンをラインアップ

ビジネスに最適な Windows スマートフォンを豊富にラインアップ。Cortana、Microsoft Edge、Windows Hello などの機能は共通して使えるほか、Office Mobile をプリインストールしています。Windows ユニバーサル アプリなら、PC にもスマートフォンにも展開できます。



スマートフォンを PC のように使う、Continuum

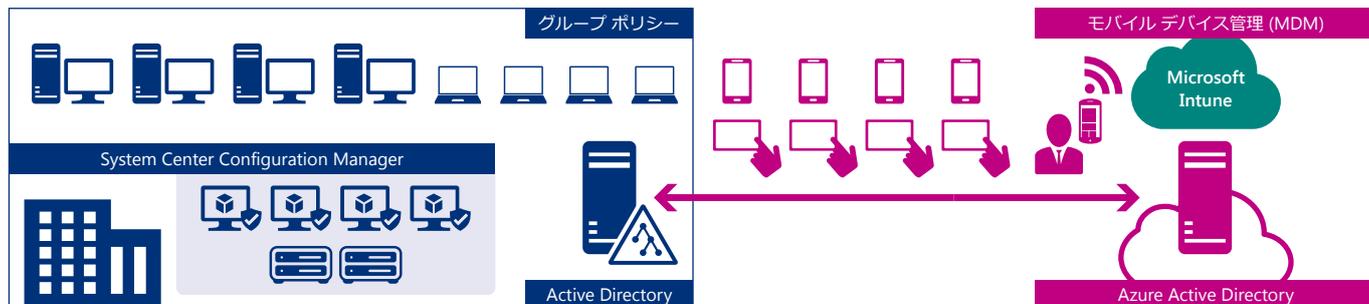
Windows 10 Mobile にモニターやキーボードを接続すると、スマートフォンをまるで PC のように活用できます。Continuum は、出力先のモニターに合わせて画面を調整。単に拡大表示するのではなく、パソコンと同じようにユニバーサル アプリを使用できます。



クラウド時代のクライアント管理機能を提供

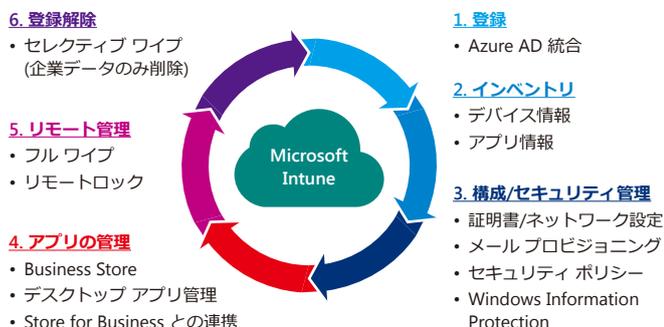
組織に接続するすべてのデバイスと ID を効率よく管理できるよう、幅広い選択肢を提供

社員のワークスタイルにあわせて、ID およびデバイス管理に豊富なオプションを提供。ID 管理では、Azure Active Directory の ID を使用して Windows にサインインできます。Azure AD は Windows Hello for Business による認証も可能。生体認証や PIN を使用した、クラウドサービスへのシングルサインオン環境を構築できます。デバイス管理では、グループポリシーと System Center を継続的にサポート。組織ネットワークに頻繁に接続するデバイスは、既存の管理基盤をそのまま活用できます。モバイルデバイスや BYOD (個人所有端末の業務利用) には、高度なモバイルデバイス管理 (MDM) ソリューションを提供。Azure AD のデバイス登録機能とも連携し、条件付きアクセス、Windows Information Protection のポリシーの設定、ストアの制御、VPN 構成やリモートワイブなどをサポートします。



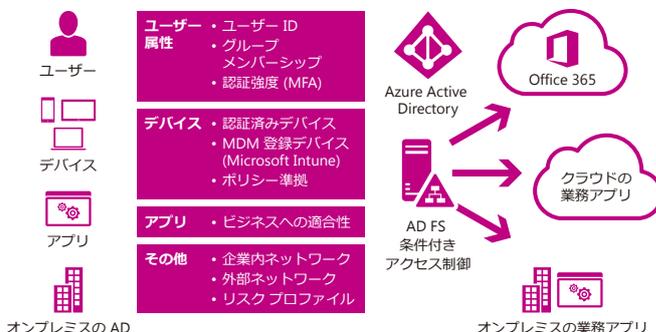
組織の管理ライフサイクルですべてのデバイスを管理

PC、スマートフォン、そして Microsoft Surface Hub や BYOD デバイスまで、すべてのデバイスに OMA-DM ベースの管理プラットフォームを提供。Microsoft Intune では、デバイスの登録から、セキュリティポリシーの展開、アプリの管理、リモートアシスタンスまで、デバイスの管理ライフサイクルを包括的にサポートします。



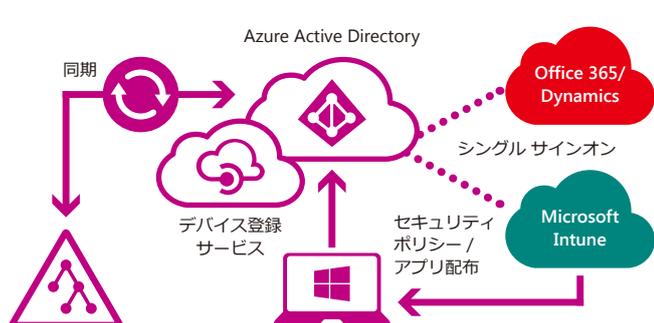
クラウドにもオンプレミスにも認証済みデバイスだけを接続

Windows Server 2016 AD FS では、条件付きアクセスを設定できます。準拠されたデバイスのみ、クラウドアプリやオンプレミスの業務アプリへのアクセスを許可したり、ドメインに参加していないデバイスに MFA (多要素認証) を強制したりすることが可能。デバイス属性に合わせて、アクセスを制御できます。



Azure AD Join でクラウドサービスをシームレスに活用

Windows 10 では、Azure Active Directory も登録先のドメインとして選択できます。Azure AD アカウントを使用して Windows にサインインすると、Office 365 のクラウドアプリや、デスクトップ上の Office アプリ、Windows ストア、Azure に展開されたアプリなどのクラウドサービスにシングルサインオンすることができます。



業務アプリの配信に Windows Store for Business

Windows Store for Business では、管理者が指定した Windows のストアアプリや、自社開発のユニバーサル Windows アプリを配信できます。Azure AD アカウントを利用して、ユーザーごとに配信可能なアプリを設定することも可能。自社アプリのアップデートの配信基盤としても活用できます。



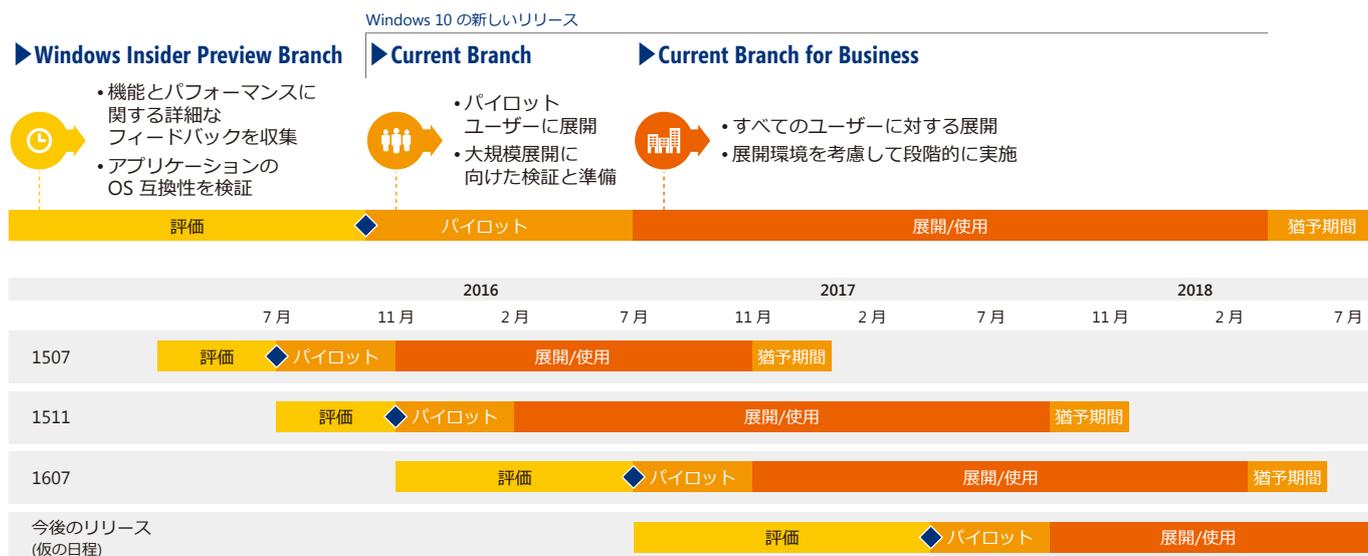
すべてのデバイスに、いつでも最適な Windows を

求められている機能を提供し続ける、 Windows as a Service

Windows 10 は "Windows as a Service" (WaaS: サービスとしての Windows) として、常に進化を続けます。以前のように、メジャーバージョンアップを待つことなく、より短い周期で最新機能を入手できます。進化するセキュリティ脅威への迅速な対応が求められる業務使用のデバイスには、最新のイノベーションを含んだアップデートを年 2 回程度の間隔でタイムリーに提供。専門性が高く、簡単にアップグレードができないミッション クリティカル システムには、セキュリティ パッチとバグフィックスだけを提供することも可能です。エンタープライズ向けには、リリースが 2 段階で行われるため、パイロット展開実施後に本格的な展開を行う運用にも適しています。

Windows Insider Program の参加 で最新機能を配信前に評価可能に

組織でソフトウェア評価を担当される方は、Windows Insider Program にご参加いただくことで、最新機能をユーザーに先駆けて検証できます。Windows Insider Release Preview というリングも用意されており、Current Branch のビルドに対するセキュリティ更新、ドライバー更新、アプリ更新だけを早期に評価することができます。



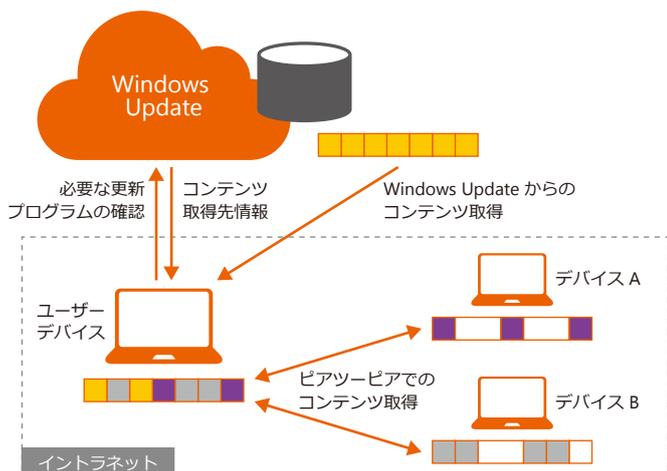
最適な更新を、最適なタイミングと、最適な手法で配信

組織はさまざまな展開手法を利用して、サービスとして随時提供される Windows 機能を最適な方法でユーザーに配布できます。Windows Update (WU) for Business では、クラウドからの配信スケジュールを組織のポリシーに合わせて管理できます。ユーザーが社内の配信サーバーに接続できる場合には、Windows Server Update Services (WSUS) を活用。さらに、アプリ配信や他のデバイスも含めた統合管理を行う場合には、System Center Configuration Manager (SCCM) が利用できます。SCCM および WSUS では BranchCache に対応するほか、WU for Business でもピアツーピアのコンテンツ配信が可能。組織内で一斉更新が行われる際のトラフィックを大幅に軽減できます。

ニーズに合わせた展開オプションを提供

Windows の展開作業は大幅に簡素化。現在、利用中の Windows 7、Windows 8.1 のデバイスにはインプレース アップグレードにより、ワイプすることなく展開。新規に導入したデバイスには、Windows イメージングおよび構成デザイナー (ICD) ツールで構成のカスタマイズとプロビジョニングを効率化。また、新しく追加された Windows Upgrade Analytics Service を使うことで、組織が保有する Windows 7、Windows 8.1 の PC やアプリの情報を収集し、アップグレードに関する課題などを事前に確認できます。

Windows Upgrade Analytics Service



Windows 10 のエディション

Windows 10 は、デスクトップ/ノート/タブレット向けに 4 つのエディション、スマートフォン/モバイル端末向けに 2 つのエディション、および産業機器/IoT デバイス向けに 3 つのエディションを提供しており、エディションによって利用できる機能が異なります。法人のお客様のデスクトップ/ノート/タブレットには、ビジネス向け機能を提供する Windows 10 Pro、または、組織のポリシーにあわせた管理と展開が行える Windows 10 Enterprise をお勧めします。



デスクトップ/ノート/タブレット向け



スマートフォン/モバイル端末向け



産業機器/IoT デバイス向け

Windows 10 Home コンシューマー、BYOD 向け	Windows 10 Pro 中小企業向け	Windows 10 Enterprise 中堅/大企業向け	Windows 10 Education 教育機関向け
---	---------------------------------	--	---------------------------------------

Windows 10 Mobile すべてのモバイル	Windows 10 Mobile Enterprise 企業でのモバイル シナリオ
--------------------------------------	--

Windows 10 IoT Core 低コスト デバイス	Windows 10 IoT Mobile Enterprise ハンドヘルド等のモバイル デバイス	Windows 10 IoT Enterprise 産業デバイス
---	--	--

ビジネス エクスペリエンス

	Home	Pro	Enterprise	Education
▼ 生産性とユーザー エクスペリエンス				
Continuum for phones ^{*1}	●	●	●	●
Cortana ^{*2}	●	●	●	●
Windows Ink ^{*3}	●	●	●	●
スタートメニューとライブ タイル	●	●	●	●
タブレット モード	●	●	●	●
音声、ペン、タッチ、ジェスチャー ^{*4}	●	●	●	●
Microsoft Edge	●	●	●	●
▼ 管理と展開				
グループ ポリシー		●	●	●
モバイル デバイス管理 (MDM) ^{*5}	●	●	●	●
DirectAccess			●	●
AppLocker			●	●
Azure Active Directory の Enterprise State Roaming ^{*6}		●	●	●
Windows Store for Business ^{*7}		●	●	●
Assigned Access		●	●	●
ユーザー エクスペリエンスの管理			●	●
Dynamic Provisioning		●	●	●
Microsoft Application Virtualization (App-V) ^{*8}			●	●
Microsoft User Environment Virtualization (UE-V)			●	●
Windows Update	●	●	●	●
Windows Update for Business		●	●	●
PC 設定の共有		●	●	●
テストの実施		●	●	●
▼ セキュリティ				
Windows Hello ^{*9}	●	●	●	●
Windows Hello Companion Devices ^{*10}	●	●	●	●
Windows Information Protection ^{*11}		●	●	●
デバイスの暗号化 ^{*12}	●	●	●	●
BitLocker ^{*13}		●	●	●
Credential Guard ^{*14}		●	●	●
Device Guard		●	●	●
Trusted Boot	●	●	●	●
Windows Device Health Attestation service ^{*15}	●	●	●	●
▼ ビジネス向け機能				
ドメイン参加		●	●	●
Azure Active Directory 参加とクラウドでホストされているアプリへのシングル サインオン ^{*16}		●	●	●
Internet Explorer エンタープライズ モード (EMIE)		●	●	●
リモート デスクトップ		●	●	●
Client Hyper-V		●	●	●
Windows to Go		●	●	●
BranchCache		●	●	●

^{*1} Continuum 対応の携帯端末のみ。外部モニターでの HDMI 入力のサポートが必要です。アプリのエクスペリエンスは異なります。Continuum 互換のアクセサリ (別売) が必要な場合があります。
^{*2} Cortana が使用できない市場があります。エクスペリエンスは地域およびデバイスにより異なる場合があります。Education エディションでは Cortana は使用できません。
^{*3} タッチ対応のタブレットまたは PC が必要です。
^{*4} ハードウェア依存 (ペンは別売である場合があります)。
^{*5} Home SKU では、一部の MDM 機能が使用できません。MDM を使用するには、Microsoft Intune やその他のサードパーティ製ソリューション (別売) などの MDM 製品が必要です。
^{*6} Azure Active Directory のサブスクリプションが必要です。
^{*7} 使用できない市場があります。機能とアプリは、市場およびデバイスにより異なる場合があります。
^{*8} App-V Server (Windows 10 アセスメント & デプロイメントキットの一部として無償提供) または System Center Configuration Manager (別売) のいずれかが必要です。
^{*9} Windows Hello を使用するには、生体認証ハードウェア (指紋リーダーや IR センサーなどの生体認証センサー) が必要です。Windows Hello 資格情報/キーのハードウェアベースの保護には、TPM 1.2 以上が必要です。TPM が存在しない場合、または構成されていない場合、資格情報/キーの保護はソフトウェアベースで行われます。

モバイル エクスペリエンス

	Mobile	Mobile Enterprise
▼ 生産性とユーザー エクスペリエンス		
スタート画面とアクション センターのカスタマイズ	●	●
音声、タッチ、ジェスチャー	●	●
Continuum for phones ^{*17}	●	●
Cortana ^{*18}	●	●
Microsoft Edge の読み取りビューと PDF リーダー	●	●
Outlook メール、カレンダー、Office、OneDrive for Business のプレインストール	●	●
リモート デスクトップ	●	●
▼ 管理と展開		
モバイル デバイス管理 (MDM)	●	●
条件付きアクセス	●	●
Windows Store for Business	●	●
LOB アプリのサイド ローディング	20 までの署名されたアプリ	無制限の署名されたアプリ
AppLocker	●	●
Dynamic Provisioning	●	●
Assigned Access	●	●
IoT デバイスのバックグラウンド アプリ	●	●
更新の管理	●	●
Current Branch for Business	●	●
テレメトリ設定の制御	●	●
▼ セキュリティ		
Trusted Boot	●	●
ハードウェアベースの Credential Protection	●	●
BitLocker	●	●
Windows Hello ^{*19}	●	●
Windows Hello コンパニオン デバイス ^{*20}	●	●
生体認証のサポート	●	●
Azure Active Directory 参加とクラウドでホストされているアプリへのシングル サインオン	●	●
Windows Information Protection ^{*21}	●	●
企業データの分離と暗号化	●	●
Device Guard	●	●
アプリからの VPN 接続	●	●
FIPS 140 およびセキュリティ評価基準 (CC) 取得 ^{*22}	●	●

^{*10} コンパニオン デバイスは、Bluetooth 経由で Windows 10 PC とペアリングする必要があります。Windows Hello 資格情報を維持したままローミングを行うことのできる Windows Hello コンパニオン デバイスを使用するには、Windows 10 Pro または Enterprise エディションを実行する Windows PC にサインインする必要があります。
^{*11} 以前は Enterprise Data Protection (EDP) と呼ばれていた Windows Information Protection を使用するには、Mobile Device Management (MDM) または System Center Configuration Manager のいずれかを使用して設定を管理する必要があります。Active Directory を使用する場合は、管理が容易になりますが、Active Directory の使用は必須ではありません。
^{*12} InstantGo またはデバイス暗号化 (HCK デスト) に合格したデバイスが必要です。
^{*13} TPM ベースのキー保護には TPM 1.2 以上が必要です。
^{*14} セキュアブート (Trusted Boot) 対応の UEFI 2.3.1 以降が必要です。Intel VT-x、AMD-V、SLAT などの仮想拡張機能が有効である必要があります。デバイスの正常性を確認するには、Windows の x64 バージョン、Intel Vt d や AMD-Vi などの IO/MMU、BIOS ロックダウン、TPM 2.0 が推奨されます (TPM が存在しない場合はソフトウェアが使用されます)。
^{*15} Windows Device Health Attestation Service は、MDM ソリューション (Microsoft Intune など) およびその他の管理システム (SCCM) などでも実現する条件付きアクセス シナリオで使用できます。
^{*16} Azure Active Directory のサブスクリプションが必要です。
^{*17} Continuum 対応の携帯端末のみ。外部モニターでの HDMI 入力のサポートが必要です。アプリのエクスペリエンスは異なります。Continuum 互換のアクセサリ (別売) が必要な場合があります。
^{*18} Cortana が使用できない市場があります。エクスペリエンスは地域およびデバイスにより異なる場合があります。
^{*19} Windows Hello 資格情報/キーのハードウェアベースの保護には、TPM 1.2 以上が必要です。TPM が存在しない場合、または構成されていない場合、資格情報/キーの保護はソフトウェアベースで行われます。
^{*20} コンパニオン デバイスは、Bluetooth 経由で Windows 10 PC とペアリングする必要があります。Windows Hello 資格情報を維持したままローミングを行うことのできる Windows Hello コンパニオン デバイスを使用するには、Windows 10 Pro または Enterprise エディションを実行する Windows PC にサインインする必要があります。
^{*21} Windows Information Protection (以前の名称は Enterprise Data Protection (EDP)) を使用するには、Mobile Device Management (MDM) または System Center Configuration Manager のいずれかを使用して設定を管理する必要があります。Active Directory を使用する場合は、管理が容易になりますが、Active Directory の使用は必須ではありません。
^{*22} マイクロソフトは、Lumia 950、950 XL、550、635 上で実行する Windows 10 Mobile において Common Criteria 証明を取得しています。これは、お客様に対して、セキュリティ制御および暗号化機能が適切に実装されていることを保証するものです。

ライセンス

ボリューム ライセンスとは、お客様の組織の規模やパソコン台数に合わせて、購入が可能なライセンス プログラムです。大量のパッケージ製品を保有、管理する必要がなく、コストダウンが図れます。ボリューム ライセンスでは、Windows 10 Pro のアップグレード ライセンスが購入いただけます。Windows 10 Enterprise E3 (旧名称 Windows Enterprise with Software Assurance) または Windows 10 Enterprise E5 ライセンスを購入いただくと、Windows 10 Enterprise Edition ソフトウェア アシユアランスの特典をご利用いただくことができ、デスクトップ環境の管理ソリューション Microsoft Desktop Optimization Pack for Software Assurance (MDOP) の使用権が得られます。Windows 10 Enterprise E5 をご購入いただくと、E3 の全ての特典に加えて Windows Defender Advanced Threat Protection (ATP) をご利用いただくことができます。

Windows 10 Enterprise E3/E5 で利用できる機能

Windows 10 Enterprise E3				Windows 10 Enterprise E5 [NEW]
Enterprise Edition の機能 <ul style="list-style-type: none"> UX コントロールとロックダウン機能 Credential Guard グループ ポリシー /MDM によるテレメリーの制御 Device Guard DirectAccess Windows to Go AppLocker BranchCache Microsoft User Experience Virtualization (UE-V) [NEW] Microsoft Application Virtualization (App-V) [NEW] 	MDOP による仮想化、管理、リストア <ul style="list-style-type: none"> Microsoft BitLocker Administration & Monitoring (MBAM) Microsoft Advanced Group Policy Management (AGPM) Microsoft Diagnostics and Recovery Toolset (DaRT) 	展開と利用に関する柔軟性 <ul style="list-style-type: none"> Long Term Servicing Branch (10 年間サポート) の利用 サービシング モデルの混在 <ul style="list-style-type: none"> - Current Branch - Current Branch for Business - Long Term Servicing Branch 	バージョン利用権と特典とサポート <ul style="list-style-type: none"> 将来と過去の LTSB バージョン利用 Windows To Go 使用权 Virtualization rights 24x7 延長ホットフィックスサポート トレーニング パウチャーと e-learning TechNet 特典 	より高度な攻撃への対応 <ul style="list-style-type: none"> Windows Defender Advanced Threat Protection [NEW]
・将来的にリリースされる Windows 10 Enterprise に特化した新機能の利用が可能				

ユーザー単位で購入できるライセンス

Windows 10 Enterprise E3、Windows Enterprise E5 および Windows VDA では、ユーザー単位で購入できる新しいライセンス モデルも提供しています。デバイス数がユーザー数を超えている環境では、デバイス単位で購入するよりもお得になり、デバイスの入れ替えも柔軟に行えます。

これまでのデバイス単位のライセンスがお得になるケース

- Windows 10 Enterprise E3 per Device
- Windows 10 Enterprise E5 per Device
- Windows VDA per Device

新しいユーザー単位のライセンスがお得になるケース

- Windows 10 Enterprise E3 per User
- Windows 10 Enterprise E5 per User
- Windows VDA per User

	Windows 10 Enterprise E3/E5 per Device	Windows 10 Enterprise E3/E5 per User	Windows VDA per Device	Windows VDA per User
ライセンス モデル	デバイスごと	プライマリー ユーザごと、デバイスの制限なし	デバイスごと	プライマリー ユーザごと、デバイスの制限なし
必要要件	すべてのデバイスに Windows Pro 必要	プライマリー デバイスのみ Windows Pro 必要	デバイスごとに VDAライセンスが必要	デバイスのライセンスは必要なし
Enterprise のローカル インストール	単一デバイスのみ	Windows 7/8/8.1/10 Pro 搭載 デバイスすべて、もしくは 10.1 インチ以下の Windows タブレット	デバイスごとに VDAライセンスが必要	Windows 7/8/8.1/10 Pro 搭載 デバイスすべて、もしくは 10.1 インチ以下の Windows タブレット
VDI	単一デバイスのみで利用可能	すべてのデバイスで利用可能	単一デバイスのみで利用可能	すべてのデバイスで利用可能
MDOP	デバイスごとに SA が必要	すべてのデバイスが対象	デバイスごとに VDA が必要	すべてのデバイスが対象
Mobile Enterprise	—	8 インチ以下のすべてのデバイスが対象	—	8 インチ以下のすべてのデバイスが対象

サービシング モデルとライセンス

Windows as a Service では、組織のデバイス利用方法にあわせて 3 つのアップデート方法が利用できます。固定化モデル (LTSB) を利用するには、Windows 10 Enterprise または Windows 10 Education が必要です。

最新化モデル (CB)

- Home
- Pro
- Enterprise ^{※1}
- Education ^{※1}

企業向け最新化モデル (CBB)

- Pro
- Enterprise ^{※1}
- Education ^{※1}

固定化モデル (LTSB)

- Enterprise ^{※2}
- Education ^{※2}

^{※1} Enterprise と Education を最新化モデルで利用するには、Windows SA が必要 ^{※2} Windows SA を失効した場合、現時点の LTSB の継続使用権限とダウンロード権を保有

ボリューム ライセンスのご購入方法やソフトウェア アシユアランスの詳細については、こちらの URL をご確認ください。	http://www.microsoft.com/japan/licensing/
製品のサポートに関しては、プロダクト サポート ライフサイクルの Web サイトをご確認ください。	http://support.microsoft.com/lifecycle/

システム要件

プロセッサ	1 GHz 以上のプロセッサまたは SoC
メモリ	新規: 2 GB アップグレード: 1 GB
ハードディスクの空き領域	16 GB (32 ビット) または 20 GB (64 ビット)
グラフィックス カード	DirectX 9 以上 (WDDM 1.0 ドライバー)
ディスプレイ (画面解像度)	800 x 600 以上
追加要件	特定の機能を使用するための追加要件については、ホームページをご確認ください。 https://www.microsoft.com/en-us/windows/windows-10-specifications

エディション別のアップグレード

お使いの Windows に類似するエディションの Windows 10 にアップグレードできます。たとえば、Windows 7 Professional をお使いの場合は、Windows 10 Pro にアップグレードできます。

Windows 7		Windows 8	
アップグレード前	アップグレード後	アップグレード前	アップグレード後
Windows 7 Starter	Windows 10 Home	Windows 8.1 ^{※1}	Windows 10 Home
Windows 7 Home Premium			
Windows 7 Professional	Windows 10 Pro	Windows 8.1 Pro	Windows 10 Pro
Windows 7 Ultimate			
		Windows Phone 8.1 ^{※2}	Windows 10 Mobile

※1 特定の国に向けた Windows 8.1 エディションや Windows 8.1 Single Language、Windows 8.1 with Bing にも適用されます。

※2 Windows Phone 8.1 デバイスについては、デバイスの製造元、携帯電話会社、通信事業者によっては Windows 10 にアップグレードできない場合があります。アップグレードの可否は、OEM や携帯電話会社、通信事業者のサイトをご確認ください。

 Windows 10 に関する最新情報は、
<https://www.microsoft.com/ja-jp/windowsforbusiness> をご覧ください。

●記載されている、会社名、製品名、ロゴ等は、各社の登録商標または商標です。●製品の仕様は、予告なく変更することがあります。予めご了承ください。

製品に関するお問い合わせは、次のインフォメーションをご利用ください。

- インターネット ホームページ <http://www.microsoft.com/ja-jp/>
- マイクロソフト カスタマー インフォメーションセンター 0120-41-6755 (9:00~17:30 土日祝日、弊社指定休業日を除きます)
- マイクロソフト ボリューム ライセンス コールセンター 0120-737-565 (9:00~17:30 土日祝日、弊社指定休業日を除きます)

※電話番号のおかけ間違いにご注意ください。

ご購入に関するお問い合わせは、マイクロソフト認定パートナーへ。

- マイクロソフト認定パートナー <http://www.microsoft.com/ja-jp/partner/>



日本マイクロソフト株式会社

〒108-0075 東京都港区港南 2-16-3 品川ランドセントラルタワー