【Microsoft Windows 365】サービス概要

2025年12月26日

改訂履歴

版数	発行日	改訂内容
第1版	2025年12月26日	初版発行

本資料の内容は 2025/12/26 時点のものです。製品のアップデートにより変更となる場合がございます旨ご了承ください。

Agenda

1. 前提情報
    1. 用語集
2. 背景と課題
    1. クラウドPCが必要とされる背景と課題
    2. クラウドPCとは
    3. Windows 365とは
3. Windows 365の主要な特徴とメリット
    1. Windows 365の主な特徴
    2. 特徴①ユーザー専有型クラウドPC（シングルユーザー設計）
    3. 特徴②フルマネージド型基盤（インフラ管理不要）
    4. 特徴③ Intune を中心とした一元管理
    5. 特徴④ Microsoft 製品とのネイティブ連携
    6. Windows 365 の導入メリットと留意点
4. 接続のステップと利用方法
    1. 事前準備
    2. 接続方法
    3. 接続手順（Windows App）
    4. 接続手順（Webブラウザ）
5. 仮想デスクトップ製品との比較
    1. 仮想デスクトップ製品の全体像
    2. 機能比較
    3. サービス選定ポイント
6. ライセンス
    1. Windows 365のライセンス体系
    2. スペック選択と利用料金の仕組み
    3. 各ライセンスの特徴
    4. ライセンス選定のポイント

1. 前提情報

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	OS	PCやサーバーを動かすための基本ソフトウェア。 Windows や macOS などが該当し、アプリケーションの実行やハードウェアの制御を行う。
2	VDI	サーバー上で仮想デスクトップ環境を構築し、 ユーザーはネットワーク経由でそのデスクトップに接続して利用する仕組み。 自社で基盤構築・運用が必要なケースが多い
3	DaaS（Desktop as a Service）	クラウド上で提供されるデスクトップサービス。 インフラの構築や運用をクラウド事業者が担い、ユーザーはインターネット経由でデスクトップを利用できる。Windows 365 は DaaS に該当
4	SaaS（Software as a Service）	ソフトウェアをクラウドサービスとして提供する形態。 インストール不要で、ブラウザ等から利用可能。 例：Microsoft 365、Teams、Exchange Online。
5	Iaas（Infrastructure as a Service）	サーバー、ネットワーク、ストレージなどのインフラをクラウド上で提供するサービス形態。 OSやアプリケーションの管理は利用者が行う。 例：Azure Virtual Machines。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
6	Intune	Microsoft が提供するクラウド型の端末管理（MDM）サービス。 PCやスマートフォン、クラウドPCに対して セキュリティポリシー、設定、アプリ配布などを行う。
7	マルチセッション	1台の仮想マシンを複数のユーザーで同時利用する仕組み。主に Azure Virtual Desktop（AVD） で利用され、コスト効率に優れるが、ユーザー専有環境ではない。
8	仮想マシン（Virtual Machine）	物理サーバー上にソフトウェアで作成された仮想的なコンピューター。OSをインストールし、通常のPCやサーバーと同様に利用できる。
9	AVD（Azure Virtual Desktop）	Microsoft Azure 上で提供される仮想デスクトップサービス。シングルセッション／マルチセッションの両方に対応し、設計や運用の自由度が高い反面、構築・管理の難易度は高め。
10	仮想ネットワーク（Virtual Network / VNet）	Azure 上に作成する論理的なネットワーク空間。仮想マシンやクラウドPCを配置し、オンプレミス環境との接続や通信制御を行うために利用される。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
11	SSO(Single Sign-On)	一度のサインインで、複数のサービスやアプリケーションを利用できる仕組み。Microsoft Entra ID による認証で、Windows 365 や Microsoft 365 へのシームレスな接続が可能。
12	MFA（Multi-Factor Authentication）	ID・パスワードに加えて、スマートフォン通知やワンタイムパスコードなど複数の要素で本人確認を行う認証方式。不正アクセス対策として重要。
13	Defender for Endpoint	Microsoft が提供するエンドポイントセキュリティサービス。マルウェア対策、脅威検出、侵入後の調査・対応を行い、PCやクラウドPCを含む端末を保護する。
14	ゼロトラスト	社内外を問わず、すべてのアクセスを信頼しないことを前提とするセキュリティの考え方。 ユーザーやデバイスの状態を常に検証し、必要最小限のアクセスのみを許可する。
15	グラフィックアクセラレーション（Graphics Acceleration）	CPUの代わりにGPUを使用して画像処理や描画処理を高速化する技術。 3D描画や動画再生、仮想デスクトップ環境において、表示性能や操作性を向上させる。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
16	回線冗長化	通信が切れないように、複数のインターネット回線を用意しておく仕組み。 1本の回線が障害や混雑で使えなくなっても、別の回線に自動的に切り替わることで、業務システムやクラウドへの接続を継続できる。クラウドPC（Windows 365）やSaaS利用では、インターネット接続が止まると業務ができなくなるため重要な対策。
17	テザリング	スマートフォンの通信回線を使って、PCをインターネットに接続する仕組み。 Wi-FiやUSBでスマホとPCを接続し、スマホのモバイル通信（4G/5G）をPCが利用する。 社内回線や自宅回線が使えない場合のバックアップ回線（簡易な冗長化手段）としてよく使用される。
18	Windows App	Windows 365 や Azure Virtual Desktop などのクラウドPCに接続するためのMicrosoft公式アプリ。 Windows、macOS、iOS、Android、Webブラウザなどから、クラウド上のWindows環境にサインインして利用できる。 従来の「リモートデスクトップアプリ」の後継的な位置づけで、クラウドPCへの標準的な接続手段。
19	PaaS（Platform as a Service）	アプリを動かすための「実行基盤」をクラウドで提供するサービス形態。 OSやサーバー管理はクラウド事業者（Microsoftなど）が担当し、利用者はアプリの開発・運用に集中できる。例：Azure App Service、Azure SQL Database
20	GPO	Windows PC の設定や利用ルールをまとめて制御する仕組み（主にActive Directory環境）。 パスワードポリシー、USB利用制限、デスクトップ設定などを、ユーザーやPCのグループ単位で一括適用できる。Windows 365（Entra ID + Intune 環境）では、GPOの代わりにIntuneの構成プロファイルやセキュリティポリシーが同様の役割を担う。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
21	OU（Organizational Unit：組織単位）	Active Directory 上でユーザー、コンピューター、グループなどのオブジェクトを論理的に分類・管理するための入れ物のことを指す。部署や拠点、役割ごとにオブジェクトを整理し、管理の単位として使用される。 OUを使うことで、以下のような管理が可能になる。 ・特定のOU配下にのみグループポリシー（GPO）を適用する ・管理者権限をOU単位で委任する（例：営業部のPC管理だけを別の管理者に任せる） OUはフォルダーのような階層構造を持ち、組織の構成に合わせて柔軟に設計できる。 これにより、大規模なActive Directory環境でも、セキュリティ設定や運用ルールを効率よく管理できる。

2. 背景と課題

2.1. クラウドPCが必要とされる背景と課題

近年、リモートワークやハイブリッドワークの普及により、
「いつでも・どこでも・同じPC環境で業務ができること」 が、特別なものではなく [前提条件] となりつつあります。
しかし、従来のPC運用や仮想デスクトップ環境では、働き方の変化に十分に追いつけていないケースも少なくありません。

✓ 利用する端末や場所によって、業務環境や操作感が統一されず、生産性に差が生じる

✓ PCや仮想デスクトップの構築・運用に、高度なIT知識や管理負荷が求められる

✓ 人数の増減や短期間の利用など、柔軟なリソース調整に時間とコストがかかる

このように、「環境を用意すること」自体が IT 部門の負担となり、本来注力すべき業務に集中できない という課題が顕在化しています。
こうした課題を解決する手段として登場したのが、PC環境そのものをクラウドから提供する**「クラウドPC」** という考え方です。
クラウドPCは、すぐに使え、場所や端末に依存せず、運用もシンプル なことから、これからの働き方を支える新たな選択肢として注目されています。

2.2.クラウドPCとは

前述の通り、従来のPC運用や仮想デスクトップでは、導入・運用の複雑さや柔軟性の面で課題が顕在化してきました。
こうした課題を解決する考え方として、**PC環境そのものをクラウドから提供する「クラウドPC」** が注目されています。

クラウドPCとは

✓ **OS・アプリ・データを含むPC環境をクラウド上に構築し、インターネット経由で利用する仕組み。**

ユーザーごとに専用のPC環境がクラウド上に用意され、自宅・オフィス・外出先など、どこからでも同じデスクトップ環境にアクセスできます。
端末側にデータを残さない構成が基本となるため、高いセキュリティと管理性を両立できる点も大きな特長です。

特徴

✓ **PC環境を「割り当てる」**

・仮想マシンやネットワークを個別に設計・構築する必要がない
・管理者は、完成済みのPC環境（ライセンス）をユーザーに割り当てるだけ
・仮想化基盤（ホスト、ネットワーク、ストレージ等）の設計や運用を意識せずに利用可能
→従来のVDIに比べ、導入までのハードルが低下

✓ **ユーザーごとに環境が固定され、管理がシンプル**

・基本1ユーザー＝1台のクラウドPCが基本
・ログインのたびに環境初期化/変更されることはない
・障害時も「その人のPC」として切り分けがしやすい

→マルチユーザー前提の運用よりも管理が直感的

✓ **導入・拡張が容易で、利用人数の変動に強い**

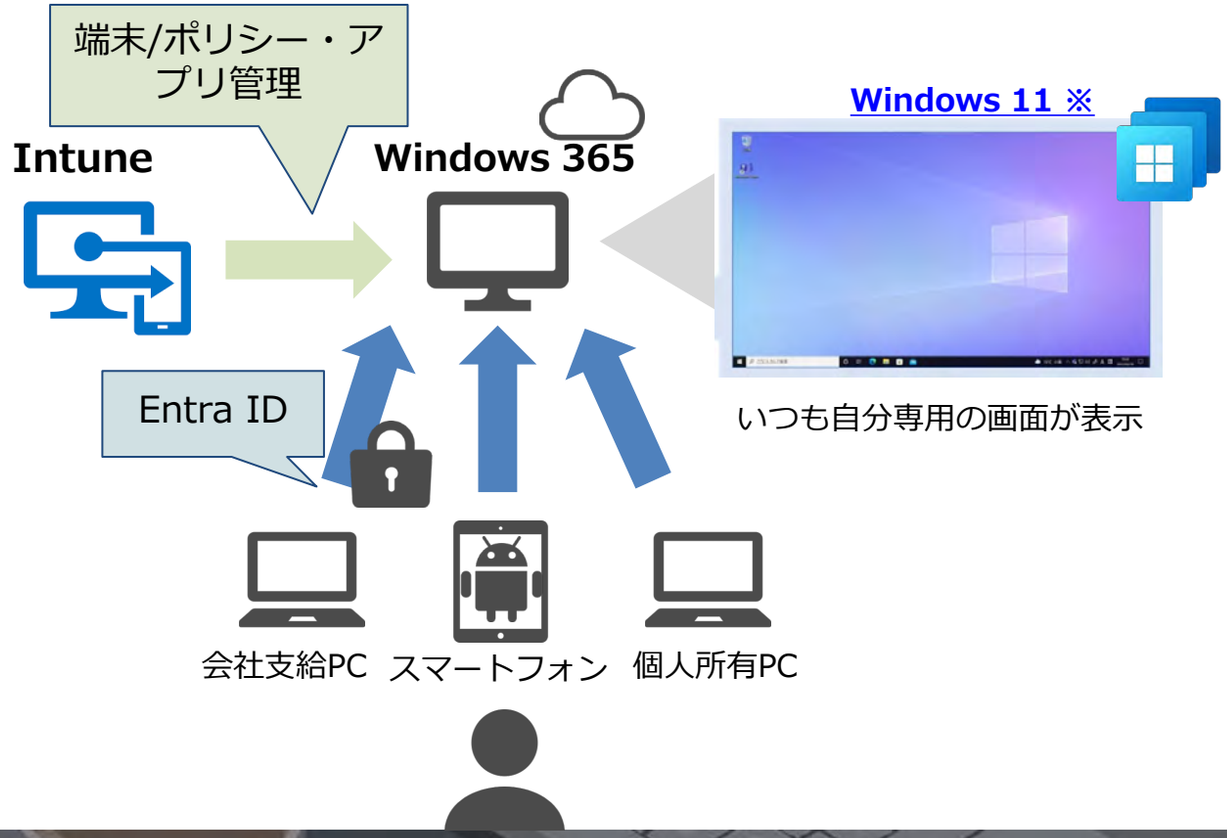
・利用開始・停止をユーザー単位で柔軟に調整可能
・短期間・少人数からでも導入しやすい
・人員増減やプロジェクト単位の利用にも対応

→ビジネスの変化に合わせて、PC環境を早く調整可能

この「クラウドPC」という考え方を、Microsoft がサービスとして提供しているのが**「Windows 365」** です。

2.3. Windows 365とは

Windows 365 は、Microsoft が提供する クラウドPCサービスです。
ユーザーはインターネット経由で、自分専用の Windows 環境にサインインし、業務を行うことができます。クラウド上にユーザーごとの Windows デスクトップを提供する点から、サービスの形態としては DaaS（Desktop as a Service） に分類されます。
一方で、仮想マシンやネットワークの構築・運用を利用者や管理者が行う必要はなく、Microsoft がクラウド上の Windows 環境を一元的に管理・提供します。
このため、Windows 365 は SaaS 型の完全マネージドサービスとして位置づけられています。



認証には Microsoft Entra ID が使用され、クラウドPC は Intune を中心とした管理基盤によって一元管理されます。
利用者の端末には OS やデータを保持せず、処理やデータはクラウド側で完結します。

・利用者は自分専用のクラウド PC にアクセスすることで、**場所や使用するデバイスに依存せず、常に同じ業務環境で作業することができます。**
従来の PC を使う感覚に近い操作性で、クラウド上の Windows を利用できる点が特長です。

・クラウド PC への接続は、**Windows PC に限らず、Mac、iPhone、Android などさまざまなデバイスから可能です。**
（※古い OS やHTML5 非対応ブラウザー、業務利用を想定していない一部デバイスについては適用外となる場合があります。）
Web ブラウザーやアプリを利用して接続します。

2.3. Windows 365とは

補足：Windows 365 で提供される OS について

Windows 365 で提供されるクラウド PC の OS は、2025年12月時点では Windows 11 が標準となっています。
Windows 365 は、Microsoft が提供する最新の Windows 環境をクラウド上で継続的に利用できるサービスとして設計されており、OS の種類やバージョンを利用者が個別に選択する仕組みではありません。
新規に作成されるクラウド PC には、Microsoft が事前に用意・管理している Windows 11 Enterprise の標準OS環境が自動的に適用されます。
OS の更新や将来的なバージョン移行についても Microsoft 側で管理されるため、利用者や管理者は OS のアップグレード作業を意識することなく、常に最新の Windows 環境を利用することができます。

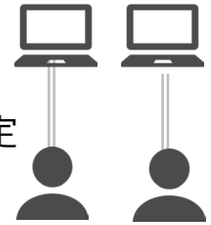
3. Windows 365の主要な特徴とメリット

3.1. Windows 365の主な特徴

Azure 仮想マシン（VM）や Azure Virtual Desktop では、環境設計や運用管理が管理者の役割となります。
Windows 365 では、これらの運用負荷を大幅に軽減し、よりシンプルにクラウドPCを利用できる点が大きな特徴です。

主な特徴

■ ユーザー専有型クラウドPC（シングルユーザー設計）



・1ユーザーにつき1台の専用クラウドPCを割り当て
・他ユーザーの影響を受けにくく、パフォーマンスが安定
・物理PCに近い操作感
・問い合わせ・切り分けが容易

■フルマネージド型基盤（インフラ管理不要）

・VM、ストレージ、可用性設計などは Microsoft が管理
・管理者は Azure 基盤設計を意識する必要がない
・障害切り分け範囲が明確（インフラ層は Microsoft が管理し、管理者は アプリ・ユーザー操作を中心に対応）

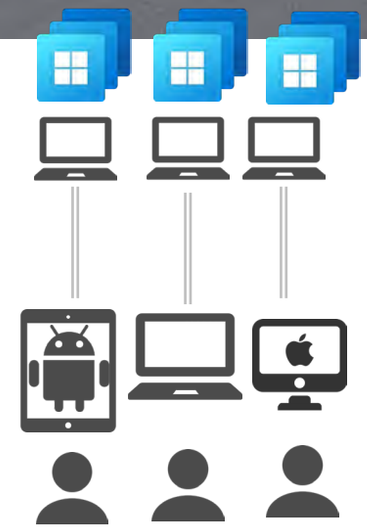
■Intune を中心とした一元管理

・Windows 365 は Intune 管理が前提
・物理PCと同じ管理ポリシーを適用可能
・アプリ配布、構成プロファイル、セキュリティ制御を統一

■Microsoft 製品とのネイティブ連携

・Microsoft Entra ID・Intune・Microsoft 365 を前提とした設計
・認証・アクセス制御・セキュリティを既存環境と同一ルールで適用
・物理PCと同じ管理・運用モデルでクラウドPCを利用可能
・Microsoft 製品群と統合された、シンプルな導入・運用を実現

3.2. 特徴①ユーザー専有型クラウドPC（シングルユーザー設計）



Windows 365 は、**1ユーザーにつき1台の専用クラウドPCを割り当てるシングルユーザー設計**のクラウドPCサービスです。
各ユーザーは、自身専用の Windows 環境を持ち、**他のユーザーと OS やシステムリソースを共有することはありません。**
この設計により、Windows 365 のクラウドPCは、従来の仮想デスクトップのように「複数ユーザーで1つの環境を共有する仕組み」ではなく、**物理PCに近い利用形態で提供されます。**
ユーザーは、自宅・外出先・社内など場所や利用端末を問わず、常に同じ Windows 環境に接続して作業を行うことができます。
また、ユーザー専有型であるため、時間帯や他ユーザーの利用状況による性能低下が起こりにくく、挙動を予測しやすいです。
管理者やサポート担当にとっても、問題発生時の影響範囲がユーザー単位に限定されるため、切り分けや対応をシンプルに行える点が特徴です。

メリット

・他ユーザーの影響を受けない安定したパフォーマンス
セッション競合やリソース奪い合いが発生しない

・トラブルシューティングが容易
ユーザーごとに専用のクラウドPCが割り当てられるため、接続状況やPC状態、操作ログをユーザー単位で確認でき、トラブル発生時の切り分けが容易。

・物理PCに近い運用が可能
管理対象がユーザー専用PCとして分離されているため、物理PCと同様の感覚でユーザー単位の管理・運用が可能。

・AVD（マルチセッション）と比べ、運用設計が簡単
セッション管理や同時接続数を意識する必要がない

注意点

・1ユーザー＝1台のクラウドPCとなるため、マルチセッション構成と比べるとコストが高くなる場合がある
各ユーザーに専用のクラウドPCが割り当てられるため、マルチセッション型の仮想デスクトップのように 複数ユーザーで1台の環境を共有してコストを抑えることはできない

・リソースの集約利用（複数ユーザーでの共有）はできない
繁忙期だけ同時接続ユーザーを増やす、といった使い方には不向き

・ユーザー数に比例してクラウドPC台数が増加（1人1台）
大規模・高密度利用では AVD の方が適しているケースもある

※一部プラン（Frontline）では、利用形態が異なる場合があります。

3.3. 特徴②フルマネージド型基盤（インフラ管理不要）

<Microsoft 管理領域>

・仮想マシン基盤
・ネットワーク
・可用性・保守・更新

<管理者が行う操作>

・ライセンス割り当て

Windows 365 は、**仮想マシンやネットワークなどの基盤部分をMicrosoft が一括して管理・運用するフルマネージド型**のクラウドPCサービスです。**利用者側で仮想マシン（VM）や仮想ネットワーク（VNet）を設計・構築する必要はなく**、クラウドPCの基盤は Microsoft により自動的に用意されます。また、**OS の更新、可用性の確保、基盤の保守や障害対応といったインフラレイヤーの運用は Microsoft が担います**。

管理者は Azure の IaaS 構成や冗長化設計、スケーリング設計などを意識することなく、ユーザーにWindows 365 ライセンスを割り当てるだけで利用を開始できます。このフルマネージド型の設計により、Windows 365 は従来の仮想デスクトップのようなインフラ中心の運用モデルではなく、「PCを管理する感覚」に近いシンプルな運用を実現します。特に、インフラ設計や Azure 運用の専門知識がなくても安定したクラウドPC環境を提供できる点が大きな特徴です。

メリット

・仮想マシンやネットワーク設計が不要
Azure の構成設計や冗長化を意識せずに導入できる

・インフラ運用・保守の負担を大幅に削減
仮想マシン基盤やネットワーク、ストレージ、OS 更新などのインフラ運用・保守は Microsoft が実施する

・導入から利用開始までが非常に短期間
ライセンス割り当て後、自動的にクラウドPCが準備される

・インフラ専門知識がなくても運用可能
情報システム部門やサポート担当の負荷を軽減することができる

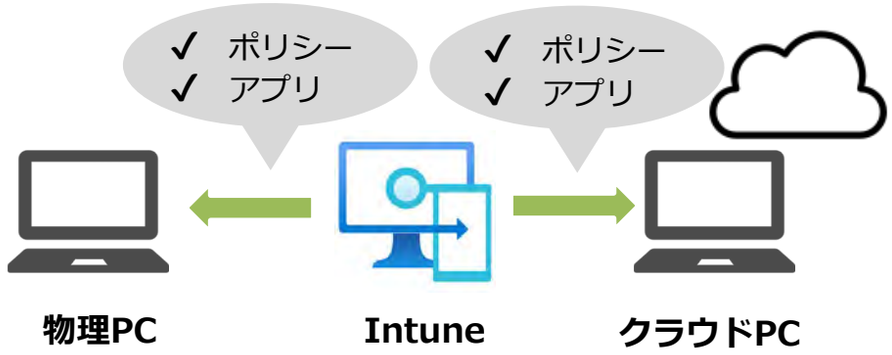
注意点

・基盤構成の自由度は限定的
VM サイズやネットワーク構成を細かくカスタマイズすることはできない

・オンプレミス環境との複雑なネットワーク統合には不向き
特殊なネットワーク要件がある場合は AVD が適するケースもある

・基盤レイヤーの詳細な制御や監視は行えない
インフラレベルでのチューニングが必要な用途には向いていない

3.4. 特徴③ Intune を中心とした一元管理



Windows 365 のクラウドPCは、Microsoft Intune による管理を前提として設計されています。そのため、クラウドPCを特別な仮想デスクトップとして扱うのではなく、**物理PCと同じ「Windows 端末」の一種として管理することが可能**です。
Intune を利用することで、アプリケーション配布、構成プロファイルの適用、セキュリティポリシー設定などを、**物理PCとクラウドPCで共通のルールに基づき一元管理**できます。
このように、Windows 365 はクラウドPCとしての利便性だけでなく、管理のあり方そのものが従来のPC運用とは異なる点も大きな特徴です。次のページにて、Windows 365 が前提としている Intune を中心とした管理モデルについて、従来の GPO 管理との違いを含めて整理します。

メリット

- **物理PCとクラウドPCを同一の管理基盤で運用可能**
  管理ルールや手順を分ける必要がない
- **アプリ配布・設定変更を一元的に実施**
  利用開始後の設定変更や追加対応も容易
- **セキュリティポリシーを統一できる**
  クラウドPC専用の例外ルールを作らずに運用できる
- **管理対象の増加に柔軟に対応**
  ユーザーや端末が増えても管理工数が比例しにくい構成

注意点

- **Intune の導入・運用が前提**
  Intune を利用していない環境では、新たに管理設計が必要
- **従来の GPO 中心の管理とは考え方が異なる**
  Intune は、オンプレミス AD によるGPO 中心の管理とは異なる考え方で設計されています。クラウド前提の管理モデルとなるため、既存の運用ルールやポリシー設計の見直しが必要になる場合があります。
- **Intune の設計品質が運用品質に直結する**
  ポリシー設計が不十分だと、管理が複雑化する可能性がある

3.4. 特徴③ Intune を中心とした一元管理

GPO管理とIntune管理の違いについて

Windows 端末の管理は、これまでオンプレミス Active Directory と GPO を中心とした運用が主流でした。
一方、Windows 365 をはじめとするクラウドPCは、クラウド前提の管理モデルとして設計されており、
従来の GPO 中心の考え方とは異なる管理アプローチが求められます。

■GPO 管理（従来）
オンプレミス Active Directory を前提とした管理方式
OU 構成やポリシーの継承関係を意識した設計・運用が必要

■Intune 管理
クラウド（Microsoft Entra ID）を前提とした管理方式
ユーザーやデバイスに対してポリシーを直接割り当てる考え方

まとめ

Windows 365 では、従来の GPO 管理を「そのまま置き換える」のではなく、
Intune を前提としたクラウド管理の考え方へ運用を整理・見直すことが重要です。
この違いを理解することで、導入時の設計ミスや運用上の混乱を防ぐことができます。

3.4. 特徴③ Intune を中心とした一元管理

管理モデルの違い（自動登録とポリシー適用について）

Windows 365 には、利用規模や管理要件に応じて**Windows 365 Business** と **Windows 365 Enterprise** の2つのプラン が用意されています。これらのプランは、提供されるクラウドPC自体は共通ですが、管理の考え方や管理者が担う役割（管理モデル）に違いがあります。
Windows 365 Business では、クラウドPCは自動的に管理対象として登録され、管理者は複雑な Intune 設計を意識することなく、シンプルに利用を開始できます。
一方、Windows 365 Enterprise では、Microsoft Intune による本格的な端末管理を前提としており、事前に管理ポリシーやプロビジョニングの設計を行うことで、物理PCと同等の管理・運用が可能です。

Windows 365 Business	・クラウドPC作成時に Microsoft 管理の Intune に自動登録 ・シンプルな管理を想定（追加設定は最小限）。具体的に以下のような操作は制限される。 ・独自の詳細な Intune ポリシー設計・カスタマイズ ・条件付きアクセスやプロビジョニングフローの高度設定 ・OS 更新のタイミングや対象ユーザーの細かい制御といった 企業向けの端末管理は行えない。 ・操作可能な管理範囲は Microsoft 管理に限定されており、企業側は Windows 365 管理ポータルからユーザー割り当てやリセットなど簡単な操作のみ行う。 →Intuneは「背景で動く仕組み」として利用されるイメージ ※クラウド PC は自動的にMicrosoft管理の Intune に登録されますが、管理は Microsoft 管理の範囲に限定されており、利用者が Intune ライセンスを保有する必要はありません。
Windows 365 Enterprise	・ポリシー設計や詳細な管理が可能（事前設計が必要） ・既存環境との統合 （既存のIntune/Entra ID環境と統合、ユーザーやグループ、ポリシー設定、条件付きアクセスをクラウドPCに適用、物理PCと同等の運用プロセス・管理ルールで統一可能） →Intuneを「企業が直接操作・運用する管理基盤」として利用するイメージ

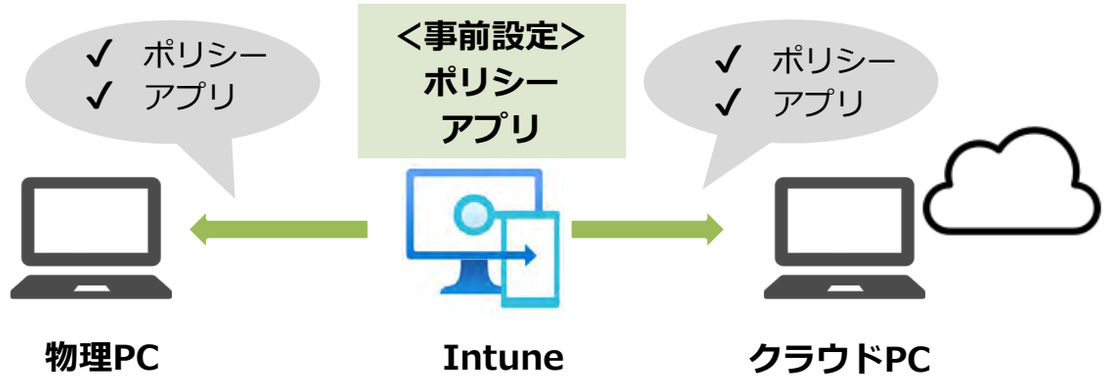
3.4. 特徴③ Intune を中心とした一元管理

自動登録とポリシー適用について

Windows 365 Enterprise では、クラウドPCが自動的に Microsoft Intune に登録され、既存の Entra ID および Intune 環境に統合されます。
これにより、管理者が個別に端末登録や初期セットアップを行う必要はありません。
クラウドPCの運用は、Intune 側で事前に定義したアプリ配布、セキュリティ設定、構成プロファイルなどの各種ポリシーが既存の物理PCと同じ管理ルールのもとで 自動的に適用されます。

※ OS 更新は Microsoft によるフルマネージドが前提ですが、
Intune を利用することで、更新の適用タイミングや対象範囲など、
運用面での制御を行うことが可能です。

※ **Windows 365 Business** では、クラウドPC作成時に Microsoft 管理の Intune に自動登録されます。管理者が行えるのは、クラウドPCの割り当てやリセットなどの基本操作に限定され、アプリ配布やセキュリティポリシー、更新管理は提供されません。
そのため、ソフトのインストールや設定は、各ユーザーがクラウドPC内で個別に行う運用となります。



3.4. 特徴③ Intune を中心とした一元管理

管理モデルの違いと選定ポイント

比較項目	Windows 365 Business	Windows 365 Enterprise
管理対象登録	クラウドPC作成時に自動でMicrosoft 管理のIntune に登録	既存の Intune / Entra ID 環境に統合
管理の複雑さ	シンプルな管理を想定し、追加設定は最小限	詳細なポリシー設計・高度設定が可能
Intune ポリシーの適用	・既定の設定値が適用されるのみ ・カスタマイズは不可	条件付きアクセス、アプリ配布、プロビジョニングフローなど細かく設定可能
OS 更新管理	Microsoft 管理によるフルマネージドが前提	Microsoft 管理＋Intune による運用制御が可能
向いているケース	小～中規模、簡単にクラウドPCを使いたいユーザー向け	大規模、既存環境と統合して統一管理したいユーザー向け

※Frontlineというプランもございますが、管理モデルや仕様が異なるため、ここでは割愛しています。
　Wndows 365のプランについてはこちらのページをご参照ください。

まとめ

・Business はシンプルにすぐ使える環境を提供する一方、カスタマイズや詳細なポリシー設計は制限されます。
・Enterprise は事前設計や管理ルール作成が必要ですが、物理PCと同等の管理運用をクラウドPCでも実現可能です。

3.5. 特徴④ Microsoft 製品とのネイティブ連携

Windows 365 は、Microsoft Entra IDや Microsoft Intune、Microsoft Defender などのMicrosoft クラウドサービスと ネイティブに統合された設計となっており、追加構成や個別連携を行わなくても、Microsoft 365 環境の延長としてそのまま利用できます。

ユーザーは、普段 Microsoft 365 にサインインする際と同じアカウントでWindows 365 にサインインでき、認証・デバイス管理・セキュリティポリシーは 既存の Microsoft 365 / Entra ID / Intune の設定がそのまま適用されます。

そのため、「Windows 365 専用の認証基盤を用意する」、「VDI 用に別の管理ツールやセキュリティ製品を導入する」といった対応は不要で、Microsoft 製品を使っている企業ほど、導入・運用のハードルが低いことが特徴です。

主な連携ポイント

Microsoft Entra ID	・Microsoft 365 と同じ Entra ID アカウントで Windows 365 にサインイン可能（SSO） ・条件付きアクセス、MFA、デバイスベース制御が利用可能
Microsoft Intune	・クラウド PC を Intune で管理（構成プロファイル、アプリ配布、ポリシー適用） ・Windows 365 専用の管理画面を新たに覚える必要がない
Microsoft Defender	・Defender for Endpoint による脅威検知・可視化 ・クラウド PC も物理 PC と同じセキュリティ基準で保護可能
Microsoft 365 アプリとの親和性	・Teams、Outlook、OneDrive などをMicrosoft 365 のデスクトップアプリをインストールして使う前提の設計 ・OneDriveと組み合わせることで、クラウドPC内のユーザーデータを Microsoft クラウド側に集約し、端末へのデータ残留や持ち出しリスクを低減できる

メリット

- **SSO + MFA により、利便性とセキュリティを両立**
- **既存の Microsoft 365 / Intune / Entra ID の知識・設定を流用できる**
- **セキュリティ設計を個別に考えなくても「Microsoft 推奨構成」を取り入れやすい**
- **管理ツールやセキュリティ製品の乱立を防げる**

注意点

- **Microsoft 製品（Entra ID / Intune / Defender）への依存度が高い**
  他社製 ID 管理・MDM を中心に運用している場合はメリットが薄い
- **高度なセキュリティ機能（条件付きアクセス、Defender の一部機能）は別途ライセンス（Entra ID P1/P2、Defender など）が必要**
- **「自由にカスタマイズできる VDI」を求めるケースには不向き**

3.6. Windows 365 の導入メリットと留意点

Windows 365 は、多くの利点を持つ一方で、クラウドPCという特性上、
従来の物理PCやVDIとは異なる考慮点も存在します。本章では、導入によって得られる主なメリットと事前に理解しておくべき注意点を整理します。

メリット

■IT部門（管理者）の運用工数の劇的な削減
・ライセンス割り当てを起点に、数回の操作だけでクラウドPCをプロビジョニングでき、端末配布までのリードタイムを短縮できる
・複雑なVDIインフラの構築・保守が不要となり、Intuneによる物理PCとクラウドPCを一元的に管理できる

■強固なセキュリティとコンプライアンス
・業務データはクラウド上のクラウドPC内にのみ存在し、端末側にデータを残さないため、紛失・盗難時の情報漏えいリスクを低減する
・Microsoft Entra ID や条件付きアクセスと連携し、ゼロトラストの考え方に基づいたアクセス制御が可能
・セキュリティレベルは、条件付きアクセスや Intune ポリシーを用いて、物理 PC と同じ基準で統一管理できる

■ 導入・拡張が容易なライセンスモデル
・ユーザー単位の定額制（サブスクリプション）のため、人数の増減や短期間の利用にも柔軟に対応できる
・派遣社員や期間限定プロジェクトなど、一時的なPC利用にも適している

留意点

■オフライン環境では利用不可
・Windows 365 は常時インターネット接続を前提としたサービス
・ネットワークが利用できない環境では業務が行えないため、回線冗長化やテザリングなどの代替手段を事前に検討する必要あり

■ネットワーク品質への依存
・利用シナリオに応じて必要な帯域が変動
（一般的な業務（Office、Web）：約 1～2 Mbps、 画像が多い操作・高画質表示：5～10 Mbps、Teams 会議・ビデオ利用：10～20 Mbps 程度など）
・Web 会議や動画利用が多い場合は、十分な帯域を確保できる回線環境の整備が重要

■継続的な利用コスト
・定額制（サブスクリプション）のため、長期利用では買い切りより累積額が高くなる場合がある
・長期固定利用の端末が多い場合は、物理PCとのコスト比較が必要

■ カスタマイズ性は限定的
・高度な構成制御や独自要件がある場合は、AVD の検討が適するケースもある

4. 接続のステップと利用方法

4.1. 事前準備

本章ではクラウドPCに接続するための事前準備と、接続方法と実際の操作の流れについて説明します。

事前準備（管理者）

Microsoft Entra ID（ユーザーアカウント）の準備	・クラウドPCを利用するユーザーには、事前に Entra ID 上のユーザーアカウントが必要です
Windows 365 ライセンスの割り当て	・Microsoft管理センターから購入したライセンスを対象ユーザーへ割り当てます。
クラウドPCのプロビジョニング完了確認（Windows 365 ポータル で確認）	・ライセンスをユーザーに割り当てると、Microsoft側でクラウドPCの自動作成（＝※プロビジョニング）が開始されます。（※ライセンス割り当てをきっかけに、Microsoft 側でクラウドPC（Windows 環境）が自動的に作成・初期設定される処理） Windows 365 のクラウドPCが自動作成され、ユーザーが実際に接続・利用できる状態になっていることを確認します。ポータルからクラウドPCが表示されていなかったり、アプリから接続できない場合はプロビジョニングが未完了の可能性があります。
（必要に応じて）条件付きアクセス・MFA の設定	・Microsoft Entra ID の条件付きアクセスを利用することで、多要素認証（MFA）や接続元条件に基づいたアクセス制御を適用できます。
（Enterprise の場合）Intune ポリシーの設定	Windows 365 Enterprise では、作成されたクラウドPCが Intune に自動登録され、管理者が定義した各種ポリシーが適用されます。事前に Intune 側でデバイス構成プロファイルやセキュリティポリシー、アプリ配布設定などを準備しておくことが重要です。

事前準備（作業者）

（アプリ接続の場合）Windows App のインストール	・Windows、macOS、iOS、Android 用の Windows App を事前にインストールします。 ・Microsoft Store や Apple App Store から入手可能で、ブラウザ接続よりも安定した操作性と機能が提供されます。

4.2. 接続方法

接続方法

Windows 365 のクラウドPCは、以下の方法で接続できます。
①Windows App からの接続※(Microsoft社推奨)
②Web ブラウザからの接続
どちらかの接続方法にて利用者が実際に接続を行います。利用者の端末や利用シーンに応じて、接続方法を選択できます。
どちらも共通して、データやアプリはすべてクラウドPC側で処理・保存され、利用端末には原則としてデータを残さないのも特徴です。

①Windows App からの接続

■特徴
・Windows / macOS / iOS / Android / Chromebook に対応した専用アプリによる安定した接続
・マルチディスプレイ、リダイレクト（手元のプリンタ・USB機器等をクラウドPCから利用可能）

■利用シーン例
・社給PCで日常業務として利用
・クラウドPCをメインの業務環境として使う
・高い操作性・パフォーマンスを重視したい

■補足
・端末へのアプリインストールが必要

②Web ブラウザ からの接続

■特徴
・Microsoft Edge / Chrome などのブラウザから即時接続可能
・OSを問わず（Windows / macOS / Chromebook 等）利用可能

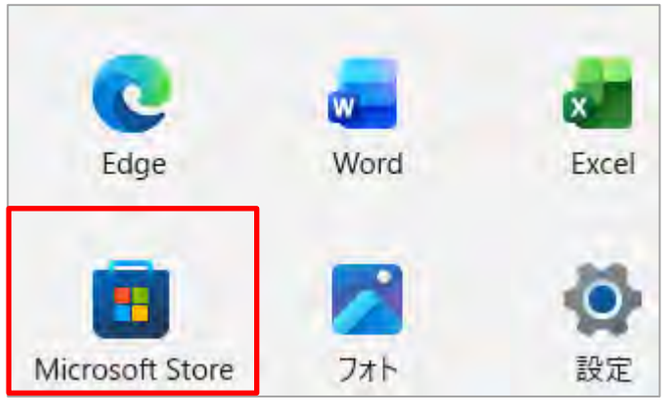
■利用シーン例
・社外や出張先で一時的に利用したい
・個人所有PC（BYOD）や共用PCから利用したい
・端末にアプリをインストールできない環境

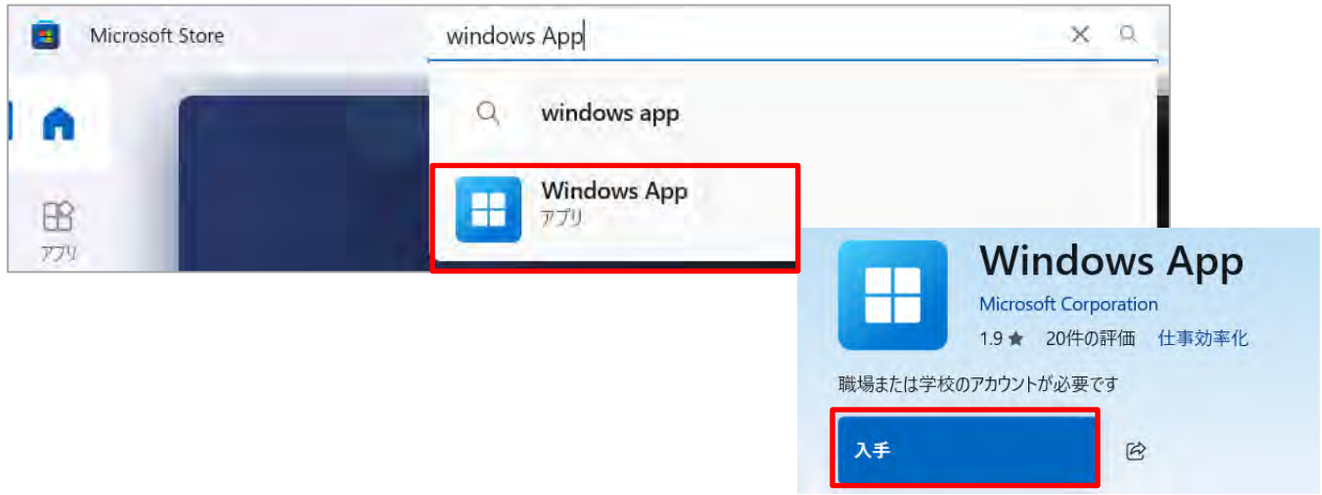
■補足
・ローカルアプリ連携や操作性は、専用アプリより制限される場合あり

※一部画面キャプチャがないものに関しては、文章での記載のみとさせていただいております。

4.3. 接続手順（Windows App ）

①Windows App からの接続手順

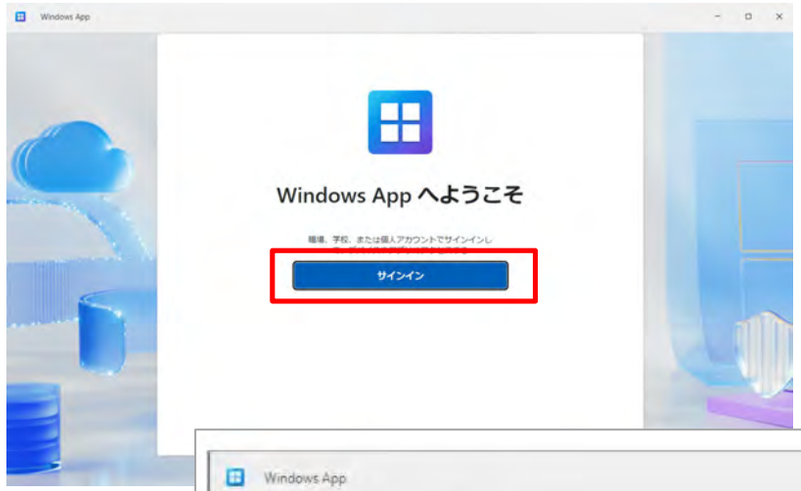


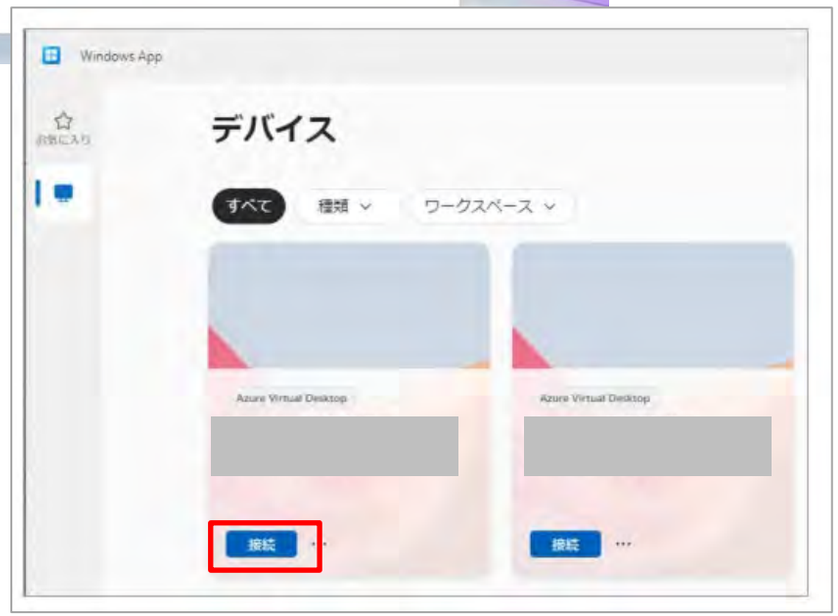


■Windows Appをダウンロード

1. Microsoft Store を開きます。または、Windows端末を利用している場合、デフォルトでインストールされているため検索窓から「Microsoft Store」を検索し選択します。
2. 検索欄に 「Windows App」 と入力し、対象を選択します。
3. 「入手」をクリックし、ダウンロードを行います。

4.3. 接続手順（Windows App ）





■ Windows App を起動

4. スタートメニューからWindows Appを起動します。

■ Microsoft Entra ID でサインイン（認証）

5. サインイン画面が表示されるので以下の情報を入力します。

・メールアドレス
・パスワード

6. MFA（スマホへの通知、コード入力など）を実施します。
（※必要に応じて）

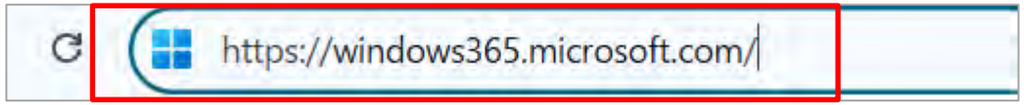
【補足：MFAが要求される条件について】
Windows 365 への接続時には、Microsoft Entra ID に設定された「条件付きアクセス」ポリシーが評価されます。
管理者が MFA を必須とするルールを設定している場合にのみ、接続時に MFAが要求されます。これらのポリシーにより、接続元や端末の状態に応じたアクセス制御が実現されます。

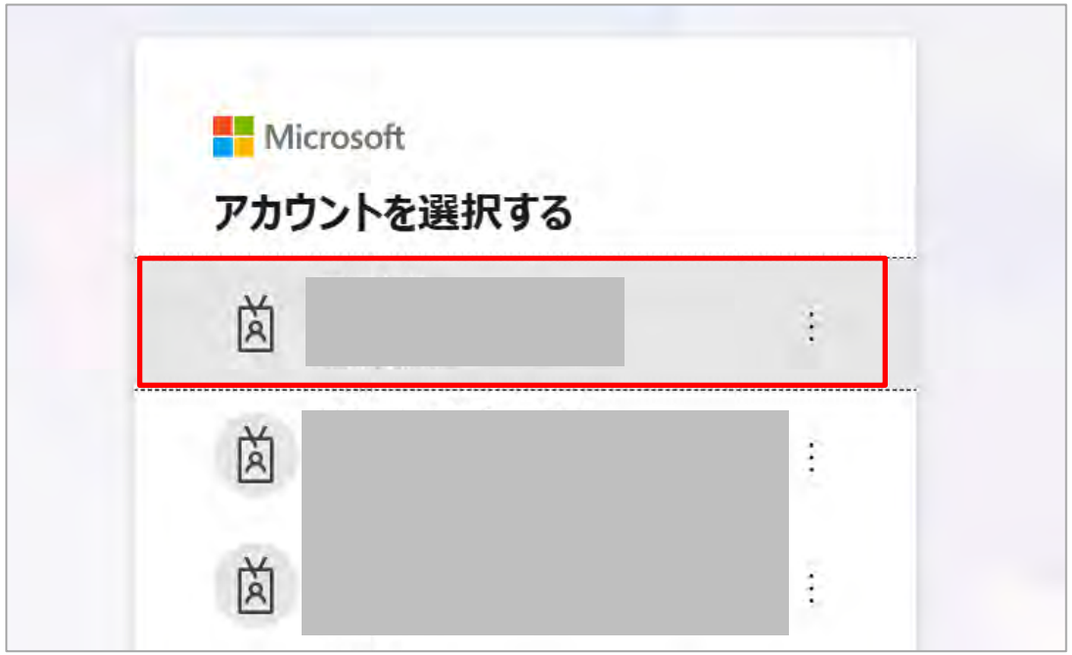
7. 対象のクラウドPCを選択し、「接続」をクリックします。

8. 接続が完了しました。

4.4. 接続手順（Webブラウザ ）

②Web ブラウザ からの接続





■ Webブラウザから接続

1. Windows 365 のライセンスが割り当てられたユーザーで Windows 365 ポータル サイトにアクセスします。

2. サインイン画面が表示されるため、アカウントとパスワードを入力します。
   ここでEntraIDでの認証が発生します。
   Entra ID の条件付きアクセス ポリシーにより、必要に応じて MFAが要求されます。

4.4. 接続手順（Webブラウザ ）

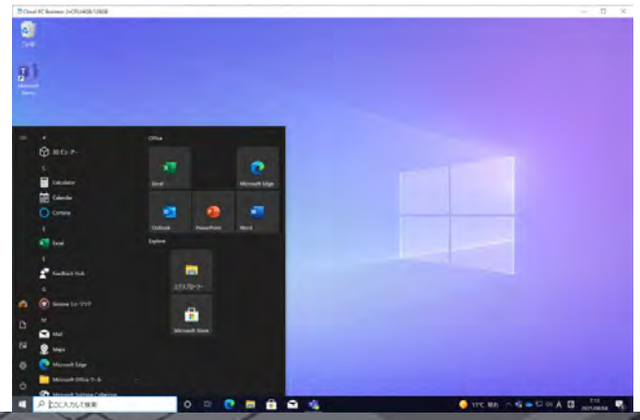
3. [お客様のクラウドPC]に、ライセンスが割り当てられたアクセスできるクラウドPC が表示されます。

4. 「ブラウザーで開く」をクリックします。

4.4. 接続手順（Webブラウザ ）

5. リソースへのアクセスについて表示がでますので、必要に応じて選択し、「許可」をクリックします。
（ブラウザ経由でローカル端末のリソースをクラウドPCにリダイレクトするかどうかをユーザーに確認するためのものです。）

6. [資格情報を入力してください]と表示されましたら、EntraIDの資格情報を入力します。



7. 接続完了しました。

5. 仮想デスクトップ製品との比較

5.1. 仮想デスクトップ製品の全体像

仮想デスクトップサービスは、同じ「クラウド上の Windows 環境」を提供するように見えても、提供形態や設計思想、運用モデルは大きく異なります。本章では、Windows 365、Azure Virtual Desktop（AVD）、Amazon WorkSpaces を対象に、それぞれの特性や向いている利用シーンを整理し、自社の運用体制や利用目的に適したサービスを検討するための比較を行います。

各サービス概要と位置づけ

Windows 365

～PCを割り当てる～

- ✓ Microsoft が提供する クラウドPCサービス
- ✓ ユーザー専有型の Windows 環境をライセンス割り当てのみで利用開始が可能
- ✓ Microsoft 365 / Intune / Entra ID とネイティブ連携

Azure Virtual Desktop（AVD）

～VDIを設計・構築～

- ✓ Azure 上に仮想デスクトップ環境を構築する PaaS型VDI
- ✓ マルチセッション対応による柔軟な構成が可能
- ✓ 高い自由度を持つ一方、設計・運用は管理者責任

Amazon WorkSpaces

～AWS上の仮想デスクトップ～

- ✓ AWS が提供する フルマネージド型仮想デスクトップ
- ✓ Windows / Linux デスクトップをクラウド上に提供
- ✓ AWS 環境と親和性が高く、シンプルな構成で導入可能

5.2. 機能比較

機能・特性比較

項目	Windows 365	AVD	Amazon WorkSpaces
提供形態	クラウドPC（SaaS的）	構築型VDI（PaaS）	マネージドVDI
ユーザー形態	専有（シングルユーザー）	マルチセッション	専有（1ユーザー1インスタンス）
インフラ設計	不要	必要（VM / Vnet / Storage等）	最小限
OS管理	Microsoft	利用者	AWS
管理ツール	Microsoft Intune	Azure ポータル	AWS マネジメントコンソール
認証基盤	Microsoft Entra ID	Microsoft Entra ID	AWS Directory Service
スケーリング	ライセンス単位	構成・設計次第	インスタンス単位
カスタマイズ性	低～中	高	中
運用負荷	非常に低い	高い	中
課金単位	月額制/ユーザー	従量課金（利用リソースによる）	時間制・月額制/ユーザー
初期コスト（作業量・手間の目安）	ほぼ不要	設計・構築が必要	低

まとめ

- ✓ Windows 365 は Microsoft 365 と同じ思想で設計されたクラウドPC
- ✓ AVD は 自由度が高い反面、設計・運用は管理者責任。
- ✓ Amazon WorkSpaces は AWS 環境と親和性の高いマネージド型仮想デスクトップ

5.2. 機能比較

管理責任の範囲と運用負荷の違い

項目	Windows 365	AVD	Amazon WorkSpaces
基盤インフラ運用	Microsoft	利用者	AWS
OS更新・パッチ	Microsoft	利用者	AWS
ネットワーク設計	不要	必要	最小限
障害切り分け範囲	狭い （Microsoft管理範囲が広い）	広い （認証、ネットワーク、VM、アプリなど切り分け対象が多い）	中 （AWS 管理部分と利用者責任部分を明確に切り分けて対応する必要あり）
管理者スキル要求	低	高	中

まとめ

- ✓ Windows 365 は Microsoft が管理する範囲が広く、管理者は 端末・ユーザー管理に集中でき、障害切り分けも比較的シンプルです。
- ✓ AVD は 高い自由度を持つ一方で、設計・運用・トラブル対応は管理者責任となります。障害時は認証、ネットワーク、VM、アプリなど切り分け対象が多く、対応範囲が広くなります。
- ✓ Amazon WorkSpaces は マネージド型ですが、AWS特有の運用知識が必要です。

5.3. サービス選定ポイント

サービス選定ポイント

■Windows 365 が向いているケース
- ✓ PC 管理をシンプルにしたい
- ✓ Microsoft 365 を中心に利用
- ✓ 情シスの運用負荷を最小化したい

■AVDが向いているケース
- ✓ 高度なカスタマイズが必要
- ✓ マルチセッションでコスト最適化
- ✓ Azure を使い慣れた管理体制がある

■Amazon WorkSpacesが向いているケース
- ✓ AWS 基盤を中心に運用
- ✓ シンプルな仮想デスクトップ導入
- ✓ Windows / Linux 混在環境

選択ポイントまとめ

Windows365：シンプルさ重視
ユーザーごとに**専用のクラウドPCを定額で提供**でき、運用がシンプル。
Microsoft 365／Intune との親和性が高く、**PC配布の延長線で導入したい企業**に最適。
設計・運用負荷を抑えたい場合に向いている。

Azure Virtual Desktop（AVD）：柔軟性柔軟性・最適化重視
仮想デスクトップ環境を柔軟に設計・構成できるのが最大の特徴。ユーザー数や利用時間に応じたコスト最適化や高度なカスタマイズが可能。
VDI の設計・運用ノウハウを持つ企業向け。マルチセッションが利用したい場合（3つの中で唯一マルチセッション対応）。

Amazon WorkSpaces（AWS）：AWS 中心のIT環境
AWS 環境との親和性が高く、AWS を中心に利用している企業に適した DaaS。時間課金・月額課金など利用形態に応じた料金選択が可能。
Microsoft 管理基盤（Intune など）との統合は限定的。

6. ライセンス

6.1. Windows 365 のライセンス体系

Windows 365 は、組織の規模や運用形態、IT 管理の要件に合わせて、主に 3 つのライセンス体系を提供しています。
基本はユーザーごとに専用のクラウド PC を提供するモデルで、利用シーン（常時利用か、シフト勤務か）や既存の IT インフラとの親和性に応じて選択します。

Windows 365 Business	Windows 365 Enterprise	Windows 365 Frontline
「手軽に、素早く」導入したい中小規模組織向け IT専門の管理者が不在でも、簡単な操作でクラウドPCの展開が可能です。また、Entra ID 参加を前提としたクラウド完結型の構成です。 **対象規模**： 300ユーザー未満	**「高度な管理と拡張性」を求める大規模組織向け** Entra ID 参加に加え、オンプレミスのADと連携したハイブリッド構成にも対応しています。これにより、クラウドPCを社内ネットワークの一部として利用でき、社内ファイルサーバーや業務システムをそのまま使い続けることが可能です。 **対象規模**： ユーザー数無制限	**「シフト勤務・パートタイム」に特化したコスト最適化モデル** シフト勤務や短時間利用を想定した、利用形態特化型のライセンス。常時利用を前提とする Business / Enterprise を補完する位置づけで、1つのライセンスを最大3名のユーザーで共有（交代制で利用）することで、現場・パートタイムユーザー向けにコスト最適化を目的として利用されます。 **対象規模**： ユーザー数無制限

6.1. Windows 365 のライセンス体系

ライセンスの前提条件

Enterprise /Frontline 利用の際の前提条件

Windows 365 Enterprise / Frontline を利用する場合、 クラウドPCには Enterprise 機能を持つ Windows OS が提供されます。
そのため、Windows 365 ライセンスに加え、Microsoft 365 E3/E5/F3 など Enterprise 機能付きライセンス が必要です。

Business 利用の際の前提条件

Windows 365 Business は、追加の管理基盤ライセンスを必要とせず、Windows 365 Business ライセンスのみで利用可能です。

6.1. Windows 365 のライセンス体系

ネットワークとオンプレミス連携の違い

Windows 365 のクラウドPCは、どこに配置されるかによって「社内ネットワークとの接続方法やアクセスできるリソース」が変わります。プランや運用方針によって、クラウドPCをどのネットワーク上に置くかを選択できます。

① Microsoft 管理ネットワーク

Microsoft が管理するクラウド環境にクラウドPCが配置される方式。

・Azure サブスクリプション不要
・インターネット経由で利用

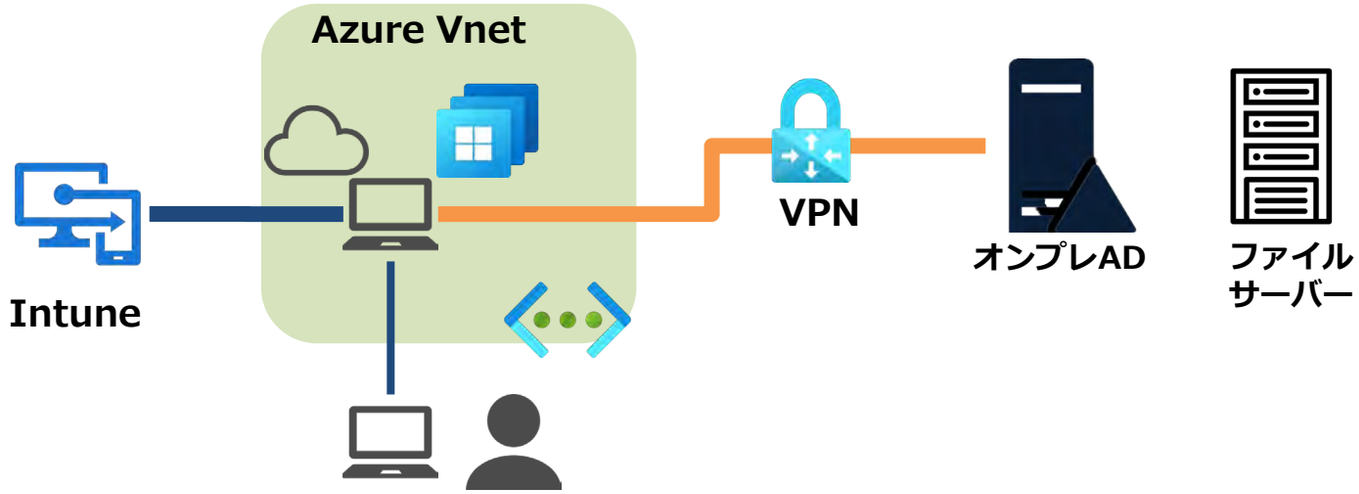
→ Business はこの方式のみ

② ユーザー管理ネットワーク（Azure VNet）

お客様の Azure 仮想ネットワーク内にクラウドPCを配置する方式。

・オンプレミスの AD やファイルサーバーと接続可能
・社内ネットワークの一部としてクラウドPCを利用できる

→ Enterprise / Frontline で利用可能



6.2. スペック選択と利用料金の仕組み

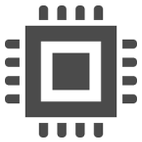
Windows 365の料金は、ライセンスの種類（Business/Enterprise等）に加え、割り当てるクラウドPCのスペック（リソース）によって決定します。

スペックを構成する3つの要素

利用するアプリケーションの負荷に合わせて、以下の組み合わせを選択します。

CPU

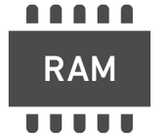
処理速度に影響



- 2 vCPU
- 4 vCPU
- 8 vCPU
- 16 vCPU

メモリ(RAM)

1ユーザーがクラウドPC内で複数のアプリやタブを同時に利用する際の作業のスムーズさに影響



- 4 GB
- 8 GB
- 16 GB
- 32 GB
- 64 GB

ストレージ

保存できるデータ量に影響

- 64 GB
- 128 GB
- 256 GB
- 512 GB
- 1 TB

Windows 365ライセンスの特徴

■定額サブスクリプション制

・Azure仮想デスクトップ（AVD）のような従量課金ではなく、月額固定料金です。起動時間に関わらずコストが一定のため、予算管理が容易です。

・Windows 365 Business および Enterpriseは、1ユーザーあたり1ライセンス/月。
Windows365 Frontlineは3ユーザー1ライセンス/月。

■スペック変更の柔軟性

利用開始後でもスペックを「アップグレード」することが可能です（リサイズ機能）。まずは標準スペック（次のページの、初期設定である基本プランの構成）から開始し、不足があれば変更する運用が推奨されます。

6.3 スペック選択と利用料金の仕組み

基本プラン

Windows 365 Business

Windows 365 Enterprise

Basic	Standard	Premium
2 vCPU 4 GB RAM 128 GB ストレージ	2 vCPU 8 GB RAM 128 GB ストレージ	4 vCPU 16 GB RAM 128 GB ストレージ

オプション/GPU対応

Windows 365 Enterprise

Windows 365 Frontline

Standard	Super	Max
4 vCPU 16 GB RAM 8 GB VRAM 512 GB のストレージ	8 vCPU 56 GB RAM 12 GB VRAM 1 TB のストレージ	16 vCPU 110 GB RAM 16 GB VRAM 1 TB のストレージ

・Windows 365 のライセンスはMicrosoft があらかじめ用意した CPU・メモリ・ストレージ構成の選択肢の中から利用用途に応じたクラウド PC を選択する方式となっています。左記の定義済みの基本プランから選択することもできますが、前ページのスペックから独自の構成を選択することも可能です。

なお、Windows 365 Frontlineは左記のようなプランはなく、スペックから選択する形となっています。

・プランの組み合わせ利用
Windows 365 は、会社（テナント）全体で1つのプランを選ぶ仕組みではなく、ユーザーごとに最適なプランを割り当てるライセンスモデルです。同一のテナント内で、Basic/ Standard などの 複数プランをユーザーごとに混在して割り当てることが可能です。

・Windows 365 Enterprise には、Business と同様の標準プランに加えて、GPU 対応のクラウド PC オプションが提供されています。
基本的なグラフィックアクセラレーションを必要とする作業向けのプランとなり、通常の Cloud PC よりグラフィック性能が強化された構成になっています。

6.4. 各ライセンスの特徴

Windows 365 の各ライセンスは、管理の考え方や利用形態に違いがあります。
Businessはシンプルさを、Enterpriseは高度な統制を、Frontlineは交代制勤務でのコスト最適化を重視した設計となっています。

	Windows365 Business	Windows 365 Enterprise	Windows 365 Frontline	備考
想定ユーザー数	～300ユーザー	制限なし	制限なし	
管理方法（端末管理の考え方）	標準設定中心	Intuneによる高度な管理	Intuneによる管理	Enterprise/Frontline では、Intune を利用して端末ポリシーやアプリ配布などの管理を行います。
オンプレとの接続	不可	可能	可能	クラウド PC を Azure 仮想ネットワークに配置することで、VPN や ExpressRoute を通じてオンプレ環境と接続することは可能
Intuneとの関係	Microsoft 管理の Intune に自動登録（お客様側での管理・設定は不可）	必須（お客様の Intune に登録して管理）	必須（お客様の Intune に登録して管理）	
Entra ID	必須	必須	必須	
同時利用の可否	1ユーザー1ライセンス	1ユーザー1ライセンス	1ライセンスで最大3名 (同時利用は不可)	
費用感※	中（導入コスト最小）	中～高（管理機能重視）	低（ライセンス共有によるコスト最適化）	※ 費用感は、同等の クラウド PC 構成・利用条件を前提とした相対的な目安です。実際の価格は、構成や契約条件により異なります。

6.5. ライセンス選定のポイント

Windows 365は、組織の規模や管理体制、そして「誰がどのように使うか」というワークスタイルに合わせて最適なライセンスを選択できます。

Windows 365 Business

「スピード導入と運用コストの最小化」を優先する場合
・規模： 従業員300名未満の中小規模組織
・管理： 専任のIT管理者が不在、またはデバイス管理に工数をかけたくない
・ニーズ：複雑な設定抜きで、購入後すぐにクラウドPCを利用開始したい
・ネットワーク：既存のオンプレミス資産（Active Directory等）との連携を必要としない

Windows 365 Enterprise

「高度なセキュリティ統制と大規模運用」を優先する場合
規模： 300名以上の組織、または将来的に拡張予定がある
管理： Microsoft Intuneを用いて、物理PCとクラウドPCを一元管理したい
ニーズ： 独自のセキュリティポリシーの適用や、詳細なログ監視を行いたい
ネットワーク： 自社の仮想ネットワーク（VNet）に接続し、社内リソースへ安全にアクセスさせたい

Windows 365 Frontline

「特定業務におけるライセンス効率の最大化」を優先する場合
用途： コールセンター、店舗、製造現場などのシフト制業務
ワークスタイル： 24時間稼働や交代制で、全員が「同時に」接続する必要がない
ニーズ： ユーザー一人ひとりに専用環境を与えつつ、ライセンス費用を最適化したい
条件： Enterprise版と同等の高度なエンドポイント管理（Intune）を前提とする