【Azure Virtual Desktop】サービス概要

2025年7月30日

改訂履歴

版数	発行日	改訂内容
第1版	2025年7月30日	初版発行

本資料の内容は 2025/7/30 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. Azure Virtual Desktop とは
    1. Azure Virtual Desktop とは
    2. Azure Virtual Desktop の利用目的
    3. 他製品との比較
3. Azure Virtual Desktop の特徴
    1. Azure Virtual Desktop の特徴
    2. 特徴① マルチセッション機能
    3. 特徴② スケーラビリティ機能
    4. 特徴③ コントロールプレーンによる基盤機能の統合管理
    5. 特徴④ Microsoft 製品との連携
4. Azure Virtual Desktop の仕組み
    1. 接続フロー
    2. 接続情報のやり取りと接続先の決定プロセス
    3. 認証フロー
5. ライセンスとコスト構成
    1. 必要なライセンス
    2. コスト構成
    3. コスト最適化のポイント
    4. 構築時の考慮ポイント

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	BYOD（Bring Your Own Device）	従業員が私物のデバイス（PC、スマートフォンなど）を業務に利用する運用形態 Azure Virtual Desktop では、企業管理外デバイスから安全に業務環境へアクセスする手段として活用される
2	WAN回線	Wide Area Network（広域ネットワーク）の略称で、地理的に離れた複数のLAN（Local Area Network）を接続して構築される大規模な通信ネットワーク
3	BCP（事業継続計画）対策	災害・障害時でも業務を継続できるようにするための対策 Azure Virtual Desktop は、クラウド上に業務環境を持つため、BCP 対策の一環として有効
4	FSLogix	ユーザーの個別設定やデータを仮想化し、複数ホスト間で一貫したユーザー環境を提供する Microsoft のツール
5	GUI（Graphical User Interface）	画面上のボタンやアイコンを使って、視覚的・直感的に操作できる管理画面のこと
6	PowerShell	Windows やクラウドの設定をスクリプトで自動化できるツール 複数台の仮想マシンをまとめて設定・管理する際に利用される
7	REST API	Web 経由でシステム間の情報取得や操作を行う仕組み Azure Virtual Desktop では管理やモニタリング機能を自動化・外部連携する際に活用される

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
8	VPN （Virtual Private Network）	インターネット上で暗号化された通信を行う仮想的な専用線
9	ゼロトラスト	社内外問わずすべてのアクセスを信頼せずに検証し続けるセキュリティの考え方
10	シングルサインオン（SSO）	一度の認証で複数のクラウド／オンプレサービスへ連続的にアクセス可能にする仕組み
11	多要素認証（MFA）	パスワードに加え、スマートフォン認証アプリ・SMS・生体認証など複数の認証要素を要求する手法
12	AVD クライアント	Azure Virtual Desktop に接続するためのアプリケーション Windows、Web ブラウザなど複数のプラットフォームに対応しており、ユーザーはこのクライアントを通じて仮想デスクトップにアクセスする
13	Azure Portal	Microsoft Azure の各種サービスを管理・構成するための Web ベースの管理ポータル 仮想マシンの作成、ユーザー管理など、Azure Virtual Desktop 環境の構築を視覚的に操作できる
14	Log Analytics	Azure Monitor の機能の一つで、Azure リソースのログデータを収集・分析できるサービス ログを検索・可視化し、トラブルシューティングやパフォーマンス監視に役立つ

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
15	Azure Resource Manager	Azure のインフラ全体を管理・デプロイするためのフレームワーク 仮想マシン、ネットワーク、ストレージなどのリソースをコードとして管理し、構成の自動化や一貫性のある運用を実現する
16	AVD Agent	Azure Virtual Desktop において、セッションホストとして機能する各仮想マシンにインストールされる専用のエージェントソフトウェア ユーザー接続の管理、接続ステータスの報告、セッションの制御などの役割を担う

2. Azure Virtual Desktop とは

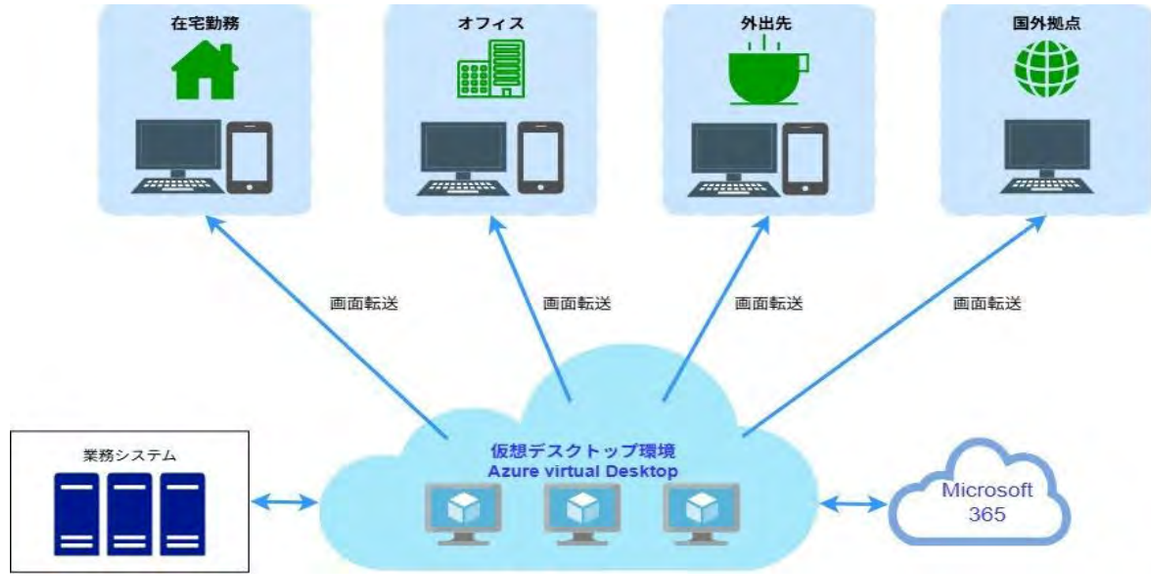
2.1. Azure Virtual Desktop とは

Azure Virtual Desktop（以下、AVD）は、Microsoft Azure 上で提供されるクラウドベースの仮想デスクトップサービスです。クラウド上に Windows のデスクトップ環境を構築し、場所やデバイスを問わず、安全かつ柔軟にアクセスすることができます。

従来のオンプレミス型 VDI では、ゲートウェイや接続ブローカーなど複数のインフラ要素を自社で構築・運用する必要があり、専門知識や運用負荷が大きな課題となっていました。
AVD では、これらのインフラ要素を Microsoft がクラウド上で提供・管理しており、ユーザーは仮想マシンなどの最小限の構成要素のみを管理すればよく、導入・運用の負担を軽減できます。

また、AVD の環境は Microsoft が提供する Azure Portal という管理画面を使って、Web ブラウザ上で作成・設定します。
PowerShell や REST API を使うことで、スクリプトによる一括操作や定期的な処理の自動化が可能です。

Azure Virtual Desktop 概要イメージ



2.2. Azure Virtual Desktop の利用目的

近年、働き方の多様化やサイバーセキュリティの脅威増加により、企業の IT 環境にはこれまで以上に柔軟性と安全性が求められています。

特にテレワークやハイブリッドワークの普及に伴い、従業員が社外からでも業務に支障なくアクセスできる仕組みは不可欠です。

AVD は、こうした企業や組織のニーズに応えるためのソリューションとして、柔軟なアクセス環境と高いセキュリティ、運用効率の向上を実現します。主な利用目的は以下の通りです。

Azure Virtual Desktop の利用目的

■リモートワークの推進

Azure 上に構築された仮想デスクトップ環境は、場所やデバイスを選ばずにアクセス可能です。
従業員は社外からでも社内と同じ業務環境にアクセスでき、働く場所を選ばない柔軟な働き方を実現します。

■開発・テスト環境としての利用

開発やテストに必要な仮想環境を必要な時に構築・削除でき、リソースの無駄を削減できます。複数バージョンの OS やアプリケーションを並行して管理できるほか、セキュアな環境で外部委託先と作業を共有することも容易です。

■教育分野での活用

専門的なソフトウェアやアプリケーションを必要とする教育現場において、AVD は柔軟な学習環境の提供に役立ちます。
BYOD（Bring Your Own Device）を推進しつつ、場所やデバイスに依存しないアクセスを可能にすることで、遠隔授業や自習環境の整備にも活用されています。

■BCP（事業継続計画）対策

災害や緊急事態が発生した際にも、クラウド上の業務環境にアクセスできるため、業務の継続性を確保できます。
オンプレミス環境に依存しない AVD は、BCP 対策として有効な選択肢です。

2.3. 他製品との比較

AVD は、DaaS（Desktop as a Service）と呼ばれるクラウド型仮想デスクトップサービスの一種であり、各 DaaS 製品によって提供機能や連携の柔軟性が異なるため、組織の運用体制に合わせた製品選定が重要です。

■製品を選ぶ基準の例

・パフォーマンスと性能、業務効率を左右する速度や負荷耐性に問題がないか　　・サポート体制、トラブル発生時に迅速な対応が可能か

・従業員数の変動に柔軟に対応できるか

以下は、代表的な DaaS 製品との比較です。

項目 / 製品名	Azure Virtual Desktop	Amazon WorkSpaces	Citrix Virtual Apps and Desktops
Microsoft 製品との親和性	◎ Microsoft 365、Teams、Entra ID とネイティブ統合	△ Microsoft 365 アプリは利用可能だが最適化なし	○ Microsoft 365 との連携は可能（構成次第）
サポート OS	Windows 10/11（マルチセッション対応）、Windows Server	Windows 10/11、Windows Server、一部Linuxも対応	Windows 10/11、Windows Server（マルチセッション対応）、Linux
管理の手軽さ	◎ Microsoft が主要コンポーネントを管理	○ 一部マネージドだが構成はユーザー側で実施	△ 高機能だが構成が複雑、専門知識が必要
スケーリングの柔軟性	◎ 自動スケーリング対応、柔軟な構成が可能	○ スケーリング可能だが手動設定が多い	◎ Citrix Autoscale などによる柔軟なスケーリングが可能

DaaS 製品とは

DaaS（Desktop as a Service）とは、PC のデスクトップ環境を仮想化し、クラウド上で提供するサービスの呼び名です。
一般的なデスクトップ環境は、個々の PC にインストールされた OS やアプリケーションによって構成されており、デスクトップで利用するデータも PC 上に保存されます。DaaS はこれらをクラウド上で提供し、インターネットや WAN 回線経由で利用できるサービスです。

3. Azure Virtual Desktop の特徴

3.1. Azure Virtual Desktop の特徴

AVD の主な特徴として、コスト効率の高い運用、拡張性のある環境構築、統合的な管理、そして Microsoft 製品とのシームレスな連携が挙げられます。
これらにより、柔軟なアクセス環境の提供に加え、セキュリティレベルの統一化と運用管理の簡素化を実現します。

特徴

■ マルチセッション機能
AVD では、Windows 10/11の仮想マシンを複数ユーザーで同時に接続して利用できます。
これにより、1台の仮想マシンを共有して運用できるため、コスト削減や管理工数の軽減が可能です。

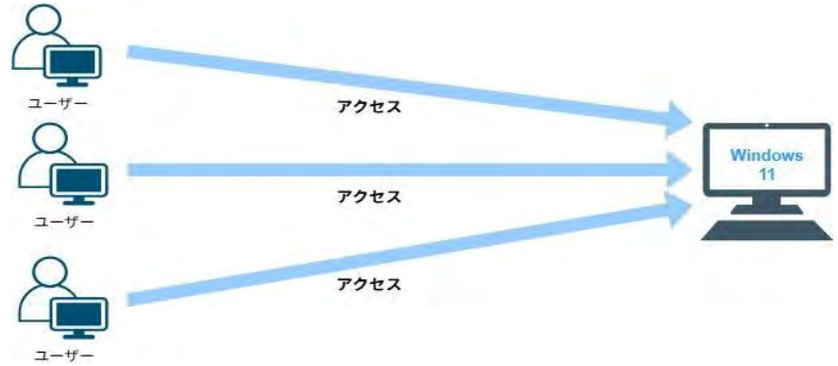
■ スケーラビリティ機能
クラウドの柔軟性を活かし、利用状況に応じて仮想デスクトップ環境を自動的に増減させることができます。
必要な時に必要なリソースを確保しつつ、コスト効率を最適化できます。

■ コントロールプレーンによる基盤機能の統合管理
AVD 環境の接続・認証・管理を担うクラウドベースの管理層です。この機能は Microsoft が Azure 上で提供・運用しており、ユーザー側の負担を軽減します。

■ Microsoft 製品との連携
Microsoft Intune や Microsoft Entra ID などの Microsoft 製品と高い親和性を持ち、シームレスな連携が可能です。特に Microsoft 365 との連携により、ユーザーは使い慣れた環境で効率的に作業できるメリットがあります。

3.2. 特徴① マルチセッション機能

AVD では、1台の仮想デスクトップ環境を複数のユーザーで同時に利用できます。
これにより、従来のように1ユーザーごとに専用の仮想マシンを割り当てる必要がなくなり、サーバー台数や管理の手間を減らすことができます。
また、同じリソースを複数人で共有するため、利用効率が上がり、運用コストの削減につながります。



メリット

■コスト削減
・1台の仮想マシンを複数人で共有できるため、必要な台数を減らし、運用コストを削減できます。

■リソースの効率的な活用
・仮想マシンの CPU やメモリは Windows OS が複数ユーザーの処理を適切に割り当てて柔軟に分配するため、共有リソースを効率的に利用できます。
過剰なリソース消費を防ぐために、管理者はグループポリシーで CPU 使用率の制限やホストプール（複数のセッションホストが属するグループ）の台数・セッション数の上限調整が可能です。

■管理負荷の軽減
・管理対象となる仮想マシンが少なく済むため、設定やメンテナンスにかかる作業負担が軽減されます。

注意点

■パフォーマンスへの影響
・複数ユーザーが1台の仮想マシンを利用するため、リソースを多く使用するユーザーがいる場合、Windows OS の標準的なリソース割り当てだけでは十分に対応できず、他のユーザーの作業に影響が出る可能性があります。

■ユーザーごとのカスタマイズの制限
・共有環境では、基本的に全ユーザーに同一設定が適用されます。
FSLogix を利用すればユーザープロファイルを個別に保持でき、カスタマイズ設定の維持が可能です。

■メンテナンスの計画
・共有環境のため、セキュリティパッチやアップデートは影響範囲を考慮し、適切なタイミングで計画的に実施する必要があります。

3.3. 特徴② スケーラビリティ機能

Azure のスケーリング機能を利用し、仮想マシンの台数やリソースを負荷状況に応じて自動で調整できます。
利用が多いピーク時には自動で仮想マシンを追加し、利用が少ない時間帯には停止・縮退させることで、コスト効率とパフォーマンスの両立を実現します。

スケーラビリティ機能

台数・電源を自動制御（スケールイン/アウト）

利用状況に応じて仮想マシンを自動で追加し、不要な仮想マシンは停止させることで、適切な台数を維持します。

スペック調整（スケールアップ/ダウン）

必要に応じて仮想マシンサイズ（CPU やメモリなど）を手動で変更することができ、パフォーマンス確保のための調整が可能です。

メリット

■効率的なリソース利用
・必要な分だけリソースを増減できるため、無駄を減らしコスト削減につながります。

■業務ニーズへの即応性
・利用状況のピーク時でも、必要なリソースを迅速に確保可能です。

■コストの最適化
・非ピーク時には仮想マシンを縮小・停止することで、運用コストを抑えることが可能です。

注意点

■設定と管理の複雑さ
・スケーリング設定には知識が必要で、最適化が不十分だとリソース不足や過剰消費につながる可能性があります。

■予算管理の難しさ
・従量課金制のため、利用状況をモニタリングし、計画的に管理しないとコストが予想以上に増える可能性があります。

■パフォーマンスの維持
・スケール操作のタイミングによっては、一時的にパフォーマンスが低下するがあります。

3.4. 特徴③ コントロールプレーンによる基盤機能の統合管理

仮想デスクトップ環境を構築する際は、接続、認証、負荷分散などの基盤制御が必要になりますが、これらは複雑で管理負荷も高い領域です。
AVD では、これらの制御機能を「コントロールプレーン」として Microsoft がクラウド上で提供します。

そのため、利用者側は基盤の構築・運用を行う必要がなく、仮想マシンの運用に専念できます。
これにより、導入・運用の負担が軽減され、仮想デスクトップ環境のシンプルな管理が可能になります。

コントロールプレーンの主な機能

機能名	役割	管理者の負担軽減ポイント
接続管理 （接続ブローカー＋負荷分散）	ユーザーの接続要求を最適な仮想マシンに割り当て、セッション管理を自動化	手動での割り当てが不要になる
ユーザー認証	Entra ID による認証結果を受け取り、認証済みユーザーの接続制御を実施	認証基盤の構築・運用が不要になり、Entra ID との統合によりセキュリティも強化される
ゲートウェイ提供 （Web アクセス管理を含む）	インターネット経由で安全に AVD 環境へ接続できる通信経路を提供	VPN の設計・運用が不要になり、外部接続の設計・運用が不要になる
管理 API の提供	Power Shell や REST API 経由で管理操作が可能	GUI に依存せず、自動化やスクリプトによる運用が可能になる
マルチリージョン対応	複数の Azure リージョンにまたがる環境構築が可能	災害対策や地域ごとのパフォーマンス最適化に有効

3.4. 特徴③ コントロールプレーンによる基盤機能の統合管理

メリット

■セキュリティ強化
・Microsoft が提供する認証・接続管理により、ゼロトラストに基づいた高い信頼性と安全性を確保できます。

■運用効率化
・Azure Portal やAPI を通じて AVD 環境を一元管理でき、スクリプトや自動化ツールとの連携も容易です。

■可用性の向上
・コントロールプレーンはマルチリージョン対応で冗長性が高く、障害時にも安定した接続環境を維持できます。

注意点

■Microsoft への依存性
・コントロールプレーンは Microsoft が管理しているため、障害発生時の対応範囲や責任分界を事前に理解しておく必要があります。

■カスタマイズ制限
・コントロールプレーンの動作は Microsoft が制御しており、細かな動作変更や独自設定はできません。

■リージョン選定の重要性
・コントロールプレーンの動作リージョンと仮想マシンの配置が離れている場合、接続遅延の要因となる可能性があります。

AVD におけるコントロールプレーンの役割

AVD のコントロールプレーンは、ユーザーの接続要求を受け付け、認証・ルーティング・負荷分散などの制御をクラウド上で担う中枢機能です。このコントロールプレーンは仮想マシンとは独立して存在し、ユーザーと仮想デスクトップ環境を結ぶ安全な接続経路の入口として機能します。
ユーザーの接続要求はまずコントロールプレーンを経由し、そこで Entra ID による認証、最適なセッションホストの選定、セキュリティ経路の確立が自動的に実行された後、ユーザーは対象の仮想デスクトップ環境へ接続できます。

3.5. 特徴④ Microsoft 製品との連携

仮想デスクトップ導入においては、既存の認証基盤や業務ツールとの統合が不可欠です。
AVD は Microsoft のクラウドサービスとの連携を前提に設計されており、導入後の管理設計や運用をシンプルに保つことができます。

各連携機能は、自動的に有効になるわけではありません。活用するには、ライセンス管理やストレージ構成など事前に適切な設計・構成が必要です。以下に、代表的な Microsoft 製品との連携例をご紹介します。

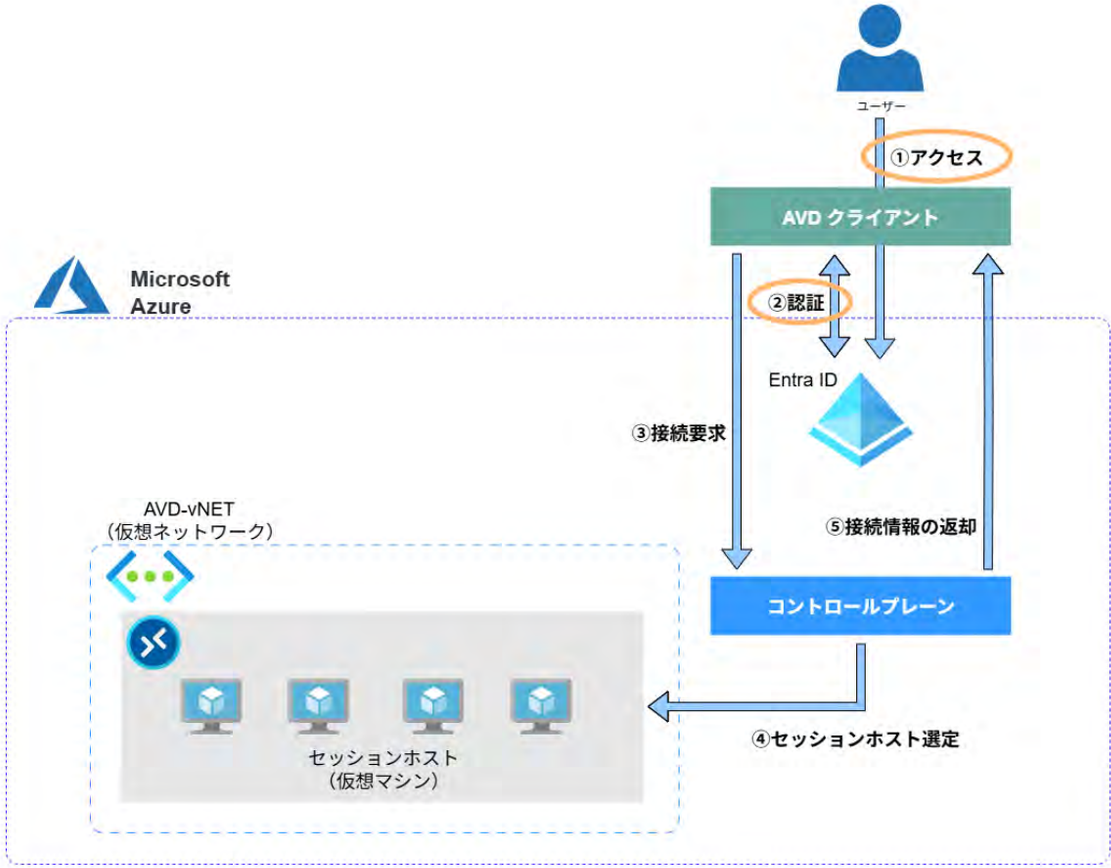
AVD と Microsoft 製品の主な連携例

目的	連携ツール・活用例
業務アプリケーションの統合	・Microsoft 365（Word、Excel、PowerPoint、Outlook など）を仮想デスクトップ上で利用可能 ・一貫した業務環境とデータセキュリティを確保
認証・管理・セキュリティ	・Microsoft Entra ID によるシングルサインオン（SSO）や多要素認証（MFA）に対応 ・Microsoft Intune による端末・アプリのポリシー配布とセキュリティ設定の一元管理 ・Microsoft Defender for Endpoint との連携による高度なセキュリティ対策
ユーザープロファイル管理	・FSLogix を活用し、ユーザーごとのプロファイルデータを効率的に管理 ・ログイン時間の短縮と一貫性のある作業環境を提供
クラウドストレージ・ファイル管理	・OneDrive、SharePoint、Azure Files との連携により、安全なデータ保存と共有が可能 ・場所を問わずアクセスできる柔軟なファイル管理を実現
運用監視・最適化	・Azure Monitor や Log Analytics を活用し、セッションの利用状況やパフォーマンスを可視化

4. Azure Virtual Desktop の仕組み

4.1. 接続フロー

下図は、AVD の基本的な接続の流れです。
クライアントの起動から、認証、コントロールプレーンによる接続制御、セッションホストへの割り当てまで、AVD の接続処理がどう行われるかを整理します。



接続フロー

①アクセス

「AVD クライアント起動と接続要求」

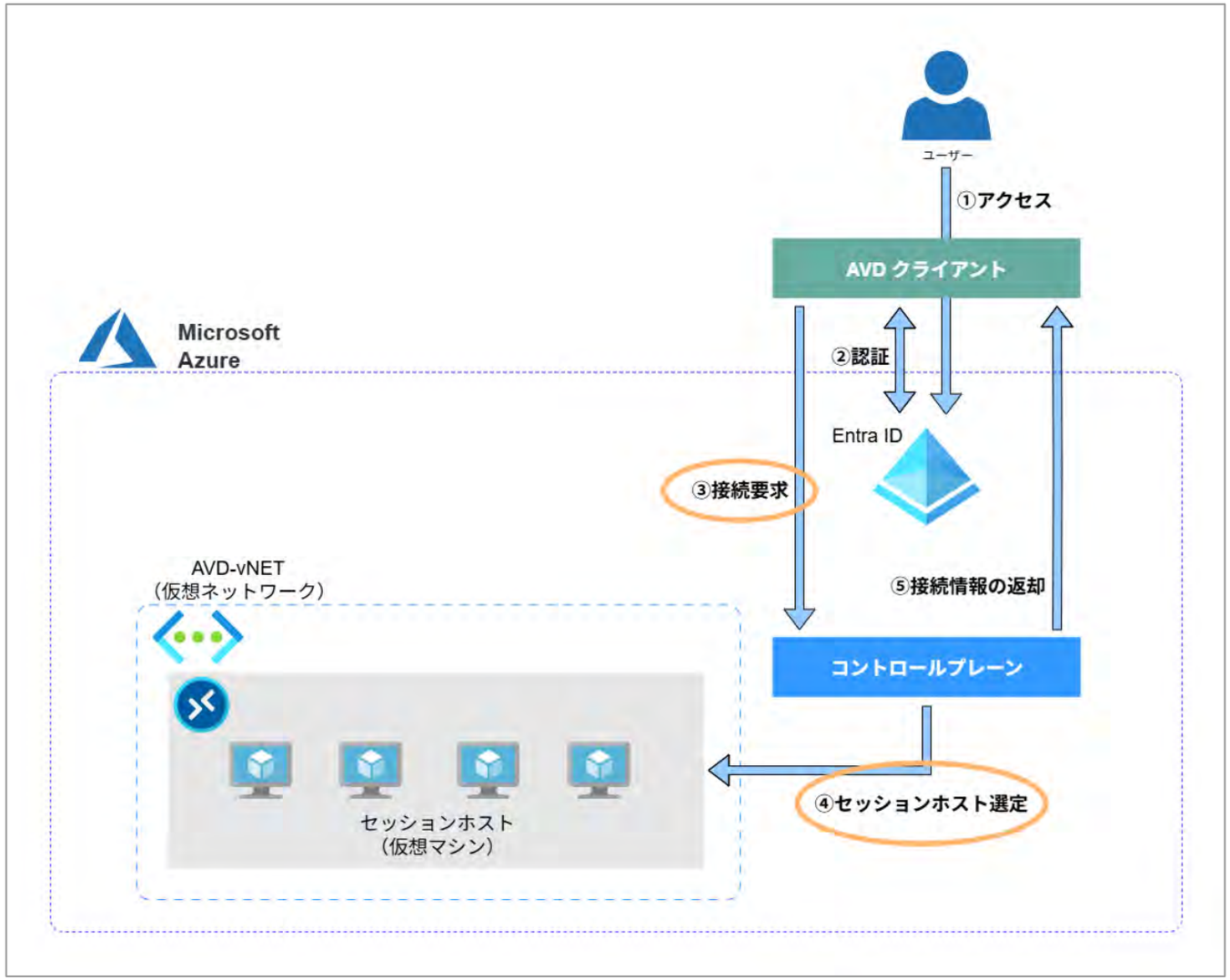
ユーザーは各端末から AVD クライアント（Remote Desktop Client や Web Client）を起動し、接続先の AVD リソース（デスクトップやアプリ）を選択して接続を開始します。

②認証

「Entra ID によるユーザー認証」

AVD クライアントはまず Entra ID に対して認証要求を送信し、ユーザーの ID と、対象の AVD リソースに対するアクセス権限が確認されます。
多要素認証（MFA）が有効化されている場合は、追加認証が求められます。
このプロセスにより、ユーザーが正当な利用者であり、指定されたリソースにアクセスする権限を持っていることが確認されます。

4.1. 接続フロー



接続フロー

③接続要求

「コントロールプレーンへの接続要求送信」

Entra ID による認証が成功すると、AVD クライアントはその認証情報（アクセストークン）を使って、コントロールプレーンに接続要求を送信します。

コントロールプレーンは受け取った認証情報をもとに、ユーザーがどのリソースにアクセスしようとしているか、どの仮想マシンに割り当てるべきかを判断します。

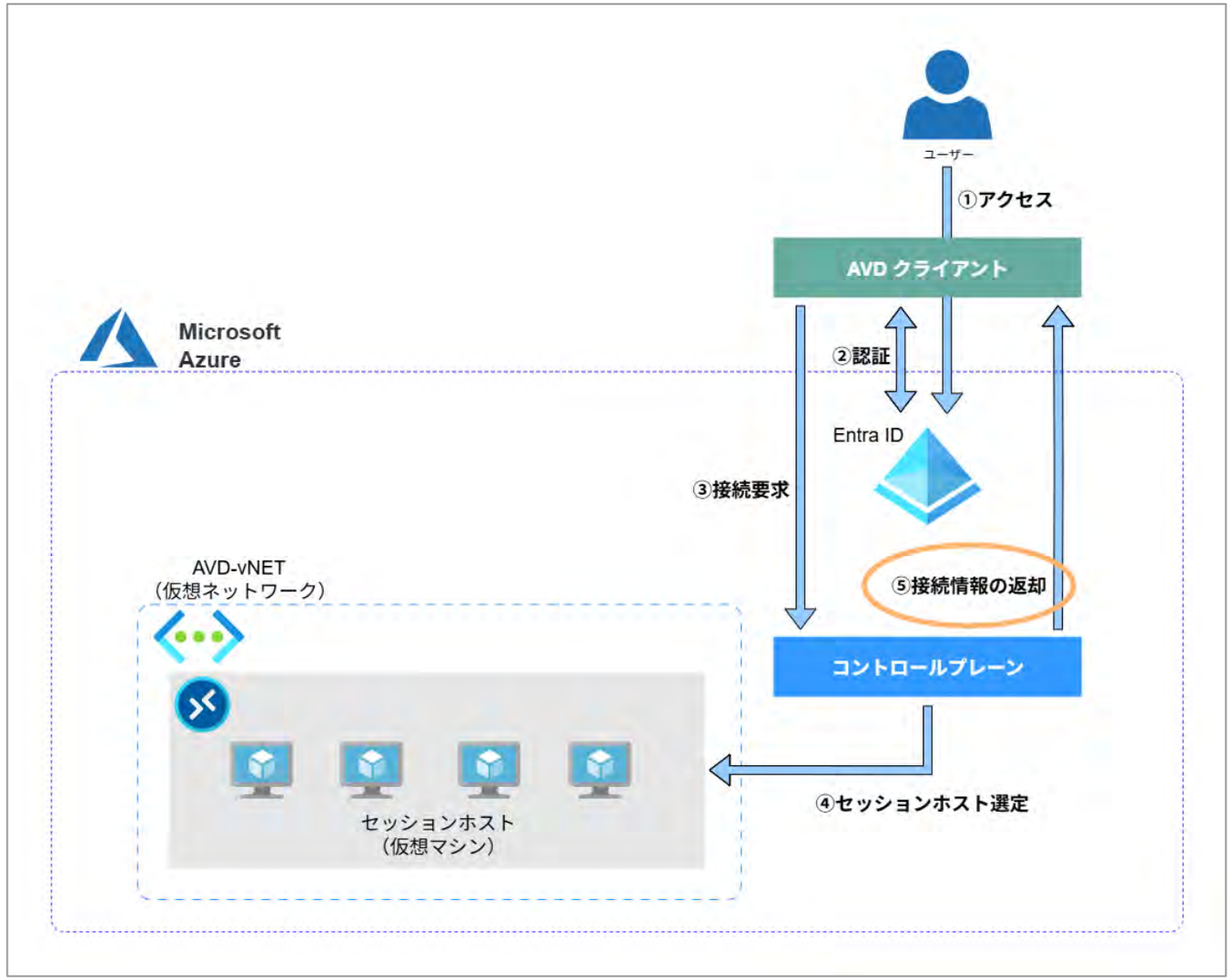
④セッションホスト選定

「セッションホストの確認と選定」

コントロールプレーンは、対象ユーザーが所属するホストプール（複数のセッションホストが属するグループ）を確認し、現在の負荷状況や接続状態に基づいて、最適な仮想マシンを選定します。

これにより、リソースの最適活用と高速な接続が実現されます。

4.1. 接続フロー



接続フロー

⑤接続情報の返却

「接続情報のクライアントへの返却」

コントロールプレーンは選定されたセッションホストの RDP 接続情報（IP アドレス、ポート番号、証明書など）を AVD クライアントに返却します。

これにより、AVD クライアントはどのセッションホストに接続すべきかを認識し、接続準備が整います。

⑤まで接続フローが進むと、ユーザーの画面に仮想デスクトップの Windows 画面が表示されます。

ユーザーは Windows ログイン資格情報を使用して、仮想デスクトップにサインインし、リモート環境での操作が可能になります。

4.2. 接続情報のやり取りと接続先の決定プロセス

前スライドでは、AVD における接続の流れを①～⑤のステップで整理しました。
このスライドでは、その接続処理の裏側でやり取りされている情報や、最適な接続先がどのように決定されるかについて記載します。

AVD では、ユーザーの認証情報は Entra ID から、セッションホストの状態は Azure Resource Manager や AVD Agent から取得されます。
これらの情報をもとに、コントロールプレーンが自動で最適な接続先を判断し、ユーザーは安全に最適な仮想マシンへ接続できる仕組みになっています。

接続情報の提供元と流れ

情報①
セッションホストの構成情報

ホストプールに登録された各セッションホストの仮想マシン情報（IP アドレス、ステータス、割り当て状態など）は、Azure Resource Manager から取得されます。

情報②
セッションホストの稼働状況

各セッションホストには AVD Agent がインストールされており、Azure に対して定期的にハートビートとステータス情報（起動状態、負荷、アクティブセッション数など）を送信します。

情報③
ユーザー認証情報

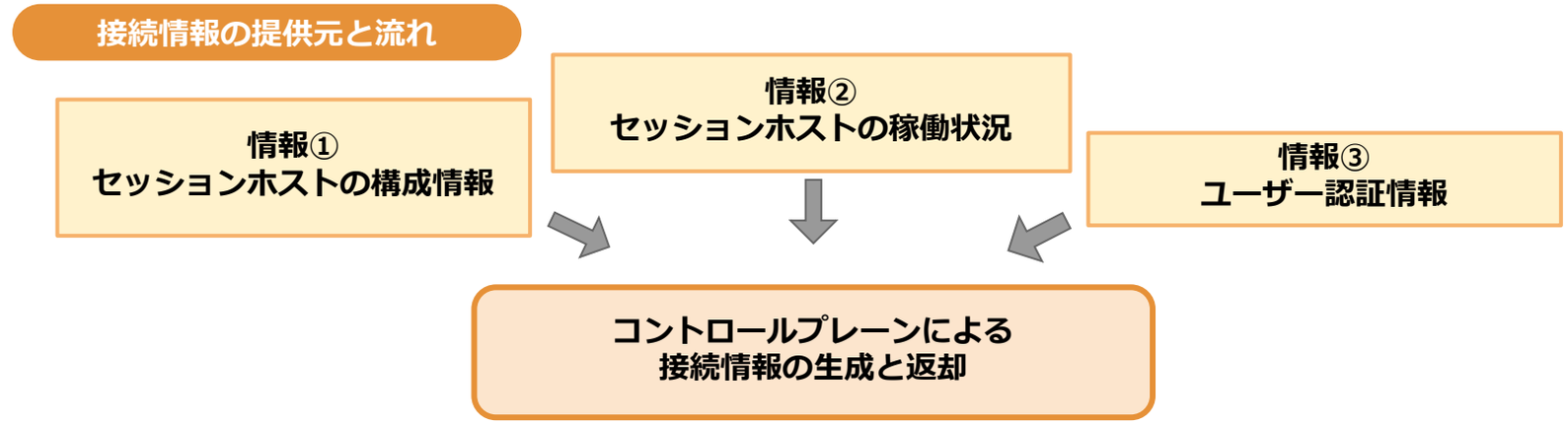
接続を要求するユーザーの認証およびアクセス許可の情報は、Entra ID から取得されます。

コントロールプレーンによる接続情報の生成と返却

①～③の情報をもとに、コントロールプレーンがユーザーに最適なセッションホストを選定します。
接続先ホストが確定したら、その RDP エンドポイント情報を含むトークンをユーザーごとに生成し、AVD クライアントに返却します。

4.2. 接続情報のやり取りと接続先の決定プロセス

再掲



複数候補がある場合の接続先決定方法

上記の流れにより、接続可能なセッションホストが複数存在する場合、コントロールプレーンはホストプールの設定や負荷分散アルゴリズムに基づいて接続先を自動的に決定します。
マルチセッション構成（共有ホストプール）の場合、以下の負荷分散方式が利用されます。

- **Breadth-first（幅優先）**：セッションホスト全体に均等にセッションを分散
- **Depth-first（深度優先）**：1台のセッションホストにセッションを集中させ、上限に達したら次のホストへ割り当て

また、各ホストの同時接続セッション数の上限も考慮され、上限を超えたホストは接続先の候補から除外されます。
これらの制御により、ユーザーはパフォーマンスが安定した最適な仮想デスクトップに接続できます。

4.3. 認証フロー

AVD の接続には、主に以下の2段階の認証があり、それぞれ異なる目的とタイミングで実施されます。

認証の種類

コントロールプレーンの認証（Entra ID）

目的：AVD サービスへのアクセス権を確認するため

・ユーザーが AVD クライアント（Remote Desktop ClientやWeb Client）から接続要求を送信
・Entra ID によってユーザー認証を実施
・認証後、ユーザーはコントロールプレーンへのアクセス権を取得

セッションホストへのログイン認証

目的：仮想マシンへのログイン確認のため

・コントロールプレーンがホストプール内のセッションホストを選定し、ユーザーを指定の仮想マシンに接続
・Windows ログイン資格情報を使用して仮想マシンにログイン

AVD では、ユーザーの接続やセッション管理を制御するためにトークンが利用されます。
これらのトークンは、ユーザーのアクセス権や接続先情報を一時的に保持し、安全かつ効率的な接続を実現するための重要な仕組みです。

主なトークン種類	生成タイミング	用途	有効期限
アクセストークン	ユーザー認証後	AVD クライアントの接続制御 ユーザーが AVD に接続する際、Entra ID による認証後に発行され、AVD のコントロールプレーンへのアクセスに使用される）	～1時間程度
登録キー	セッションホスト登録時	仮想マシンを AVD のホストプールに登録する際に使用	90日 ※仮想マシンを90日以上停止していると、登録キーの証明書の有効期限が切れ、AVD サービスとの接続ができなくなる可能性があります。定期的な仮想マシンの起動により、証明書は自動更新されます。

5. ライセンスとコスト構成

5.1. 必要なライセンス

AVD のライセンス構成

AVD には専用のライセンス製品が存在するわけではなく、Microsoft 365 や Windows ライセンス、Azure リソース利用料などの既存ライセンスを組み合わせて利用するサービスです。加えて、ユーザー認証や運用管理、セキュリティ対策などの観点から、Microsoft の各種クラウドサービスとの連携が推奨されます。
AVD 導入にあたって必要な最低限のライセンス構成を以下に整理します。

ライセンス種類	内容	備考
ユーザーライセンス（Microsoft 365 / Windows ライセンス）	AVD を利用するユーザーに必要な基本ライセンス 以下いずれかのライセンスが必要 ・Microsoft 365 E3/E5 ・Microsoft 365 Business Premium ・Windows 10/11 Enterprise E3/E5	マルチセッション機能を利用するには、Windows Enterprise ライセンスが必要です。
Azure リソース利用料	仮想マシン、ストレージ、ネットワークなどの Azure リソースに対する課金	仮想マシンサイズ・稼働時間・リージョンにより料金が変動するため、コスト最適化にはスケーリング設計が重要です。
Microsoft Entra ID	ユーザー認証、シングルサインオン（SSO）、多要素認証（MFA）などを提供する認証基盤	AVD のユーザー認証は Entra ID を前提としています。Entra ID の高度な機能には Entra ID P1/P2 ライセンスが必要なため、要件に応じたライセンス選定が重要です。

Windows Enterprise ライセンスについて

Windows Pro をベースにしたユーザー単位のサブスクリプションライセンスであり、AVD におけるマルチセッション機能の利用に必要です。
Microsoft 365 E3/E5 や Microsoft 365 Business Premium には、Windows Enterprise ライセンスが含まれているため、これらのライセンスを保有していれば別途 Windows Enterprise ライセンスを購入する必要はありません。詳しくは[Microsoft公式ページ]をご確認ください。

5.2. コスト構成

AVDのコストは主に以下の要素で構成されます。

主なコスト構成の内訳

仮想マシンの利用料	ユーザーが接続する仮想デスクトップのサイズや稼働時間に応じて課金されます。 利用時間帯やユーザー数に応じたスケーリング設計がコストに大きく影響します。
ストレージ費用	OS ディスク、ユーザープロファイル、ログ保存などにかかるストレージ費用が発生します。用途に応じて Premium、Standard、Archive などのストレージ種類を選択できます。
ネットワーク転送量	リージョン間の通信やインターネットアクセスに伴うデータ転送に対して課金される場合があります。Azure 内の通信は無料ですが、外部との通信には費用が発生します。
Entra ID 利用料	ユーザー認証やシングルサインオン（SSO）、多要素認証（MFA）などを提供する Microsoft Entra ID の利用に応じてライセンス費用が発生します。
Intune、Defender などの追加サービス利用料	運用管理やセキュリティ強化のために Intune や Defender for Endpoint などを利用する場合、それぞれに応じた追加費用が発生します。

ポイント

・AVD のコストは「ユーザーライセンス ＋ Azure リソース利用料 ＋ 追加サービス」で構成される
・コストへの影響が大きいのは仮想マシンとストレージの設計 ⇒ コスト構成を把握し適切な構成や設計を行うことで、安定したユーザー体験を維持しながらコスト面でも無駄のない運用が可能になる◎

5.3. コスト最適化のポイント

AVD は、柔軟な構成と高い拡張性を持つ一方、運用方法によってコストが大きく変動する可能性もあります。
特に仮想マシンやストレージなどの Azure リソースは利用状況に応じた従量課金制のため、導入前にコスト構成を把握し、最適化のポイントを押さえておくことが重要です。

AVD の導入効果を最大限に引き出すためには、単にリソースを割り当てるだけでなく、利用パターンに応じた効率的な構成や運用設計が求められます。

AVD の運用コストを抑えた適切な運用には、以下のような工夫が有効です。

コスト最適化のポイント

■ 自動スケーリングの活用
利用時間帯に応じた仮想マシンの起動・停止の自動化により、未使用時間のリソース稼働を抑え、コストを削減。

■ マルチセッションの活用
Windows 10/11 Enterprise のマルチセッション機能を利用し、1台の仮想マシンに複数ユーザーを収容してインフラコストを効率化。

■ ストレージ階層の最適化
使用頻度に応じて Premium、Standard、Archive などのストレージ種別を使い分けることで、不要な高性能ストレージの利用を避け、コストを削減。

■ 監視と分析によるリソースチューニング
Azure Monitor や Log Analytics を活用して、仮想マシンやセッションの利用状況を可視化し過剰なリソース使用を調整することで、無駄なコストを削減。

5.4. 構築時の考慮ポイント

AVD の構築にあたっては、コスト構成に加えて、構築における手動設定と運用フェーズでの自動化機能の住み分けを理解し、ユーザー体験・パフォーマンス・コストのバランスを最適化することが重要です。

構築内容	手動設定	自動化・効率化
ユーザー要件	利用人数や使用アプリの要件を整理	-
ホストプール設計	仮想マシンサイズの選定、ホストプールの個人利用/共有利用の構成、セッションホスト数の調整	スケーラビリティ機能による仮想マシンの台数調整
プロファイル管理	FSLogix の構成、ストレージの設定	一度構成すれば運用はほとんどが自動 ログ取得やバックアップは自動化可能
セキュリティ	Entra ID 連携、MFA 設定など	連携ツールにおける自動化範囲が適用
運用・監視	ログ設定、パフォーマンス監視の構成	Azure Monitor / Log Analytics による自動収集と可視化、アラート通知
コスト管理	ライセンス確認、仮想マシン構成の見直し	運用・監視の自動化による分析と最適化

補足

AVD は、構築は手動・運用は自動が基本であり、初期段階では手動設定が中心となります。ホストプールの設計、仮想マシンのサイズ選定、ネットワークやセキュリティの構成などは、業務要件やユーザー環境に応じて細かく調整する必要があります。

また、ユーザーの業務内容や使用アプリに応じて、仮想マシンのスペックやホストプール構成を調整する必要があります。
例えば、Microsoft 365 や Web ブラウザ中心のライトユーザーと呼ばれる利用では、1つの仮想マシンサイズあたり最大6名程度まで同時利用が可能ですが、動画編集や高解像度画像を多く扱うようなパワーユーザーと呼ばれる利用では、1～2名程度が目安となります。

手動で決めた仮想マシンサイズに基づき、コントロールプレーンが自動的に最大の利用人数を判断し割り振るため、こうした初期設計の精度が、運用の安定や効率化に大きく影響します。