【Azure Virtual Desktop】ネットワーク概要

2026年5月28日

改訂履歴

版数	発行日	改訂内容
第1版	2026年5月28日	初版発行

本資料の内容は 2026/5/28 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. 本資料の目的
    2. 用語集
2. 背景・基本概念
    1. SaaS 型サービスとしての AVD の位置づけ
    2. Azure Virtual Desktop におけるネットワーク前提
    3. コントロールプレーンとデータプレーンの責任分界点
    4. 従来型 VDI とのネットワーク比較まとめ
3. Azure Virtual Desktop ネットワークの仕組み
    1. クライアント接続順序
    2. 利用されるポート・プロトコルと暗号化
4. 導入・構成パターン別ネットワーク設計
    1. Microsoft Entra ID のみのクラウド完結構成の場合
    2. Entra Connect 利用のハイブリッド構成の場合
    3. VPN・ExpressRoute 利用構成の場合
5. 設計・構成・設定時の考慮事項
    1. 配置：VNet・サブネット 設計の考え方
    2. 経路：NSG・UDR・NAT Gateway 設計の判断軸
    3. 解決：DNS・名前解決の設計注意点
6. 設計判断の軸
    1.提案・要件定義フェーズで必ず確認すべき事項

1. 前提情報

1.1. 本書の目的

目的

本資料は、Azure Virtual Desktop におけるネットワーク構成の考え方と仕組みを理解することを目的としています。
SaaS 型サービスとしての AVD の特性や、顧客管理領域の責任分界点を整理しながら、インバウンド不要・アウトバウンド必須の設計を解説します。あわせて、構成パターン別の設計ポイントを示し、導入検討や設計判断の指針を提供します。

1.2. 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	SaaS	インターネット経由で提供され、利用者がインフラを管理せずに使えるソフトウェアの形態。
2	コントロールプレーン	Azure Virtual Desktop において、ユーザー認証、接続管理、セッション割り当てなどを Azure 上で集中管理する Microsoft 管理の制御基盤。
3	VDI	サーバー上の仮想デスクトップをネットワーク越しに利用する仕組み。
4	オンプレミス	自社施設内にサーバーやネットワーク機器を設置して運用する形態。
5	接続ブローカー	ユーザーの接続要求を受けて適切な仮想マシンやセッションホストに振り分ける役割。
6	RDP Gateway	インターネット経由でも安全にRDP（Remote Desktop Protocol）接続を中継するサーバー。
7	基盤コンポーネント	システムやサービスを構成する土台となる基本要素の集合。
8	VM	物理サーバー上に作られる、OSを含めて独立動作する仮想的なコンピューター。本資料ではAzure上で提供される仮想マシンを指す。
9	セッションホスト	複数ユーザーのリモートデスクトップセッションを実行するサーバー。
10	インバウンド通信	外部ネットワークから内部システムへ入ってくる通信。

1.2. 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	アウトバウンド通信	内部ネットワークから外部ネットワークへ出ていく通信。
12	DMZ	外部と内部の両方から分離し、公開サーバーを配置するための中間ネットワーク領域。
13	多要素認証（MFA）	Microsoft Entra ID において、パスワードに加えてスマートフォン通知やワンタイムコードなどを使い、ユーザーの本人確認を強化する認証方式。
14	メタ情報	データそのものの内容ではなく、作成日時や所有者などデータを説明する情報。
15	フィード	Azure Virtual Desktop において、ユーザーが利用可能な仮想デスクトップやリモートアプリの一覧をクライアントに配信する情報。
16	RDP	ネットワーク越しに別のコンピューターを遠隔操作するためのプロトコル。
17	AVD エージェント	Azure Virtual Desktop のセッションホストにインストールされ、Azure と通信するためのソフトウェア。
18	プロトコル	コンピューター同士が通信する際の手順やルールを定めた規約。
19	Entra ID 認証	Microsoft Entra ID を使ってユーザーの本人確認を行うクラウドベースの認証方式。
20	PoC	新しい技術や構成が実現可能かを小規模で検証するための試行。

1.2. 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	オンプレミス AD	自社環境に構築された Active Directory によるユーザーや端末の管理基盤。
22	セキュリティ要件	システムを安全に運用するために満たすべき条件やルール。
23	FW	通信を許可・遮断することでネットワークを保護する仕組み。Firewallの略。
24	ExpressRoute	オンプレミス環境と Azure を専用回線で直接接続するサービス。
25	VPN	インターネット上に仮想的な専用回線を作り、安全に通信する仕組み。
26	DNS	ドメイン名を IP アドレスに変換する仕組み。
27	BYOD	個人所有の端末を業務利用する運用形態。
28	Hub-Spoke 構成	中央の Hub ネットワークに複数の Spoke ネットワークを接続する設計。
29	ピアリング	仮想ネットワーク同士を直接接続して通信可能にする仕組み。
30	NIC	仮想マシンや物理マシンに割り当てられるネットワーク接続用のインターフェース。

1.2. 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
31	DNS フォワーディング	Azure やオンプレミス環境において、解決できない名前解決要求を別の DNS サーバーへ転送する仕組み。

2. 背景・基本概念

2.1. SaaS 型サービスとしての AVD の位置づけ

Azure Virtual Desktop（以後、AVD）は SaaS として提供される仮想デスクトップサービスです。
接続制御や認証、通信の管理は Microsoft が管理するコントロールプレーンで実施されます。
そのため、従来 VDI のように接続基盤を自社で構築する必要がなく、ネットワーク設計の前提が大きく異なります。

Azure Virtual Desktop とは

✓ 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
✓ ネットワーク設計は、セッションホストを配置する Azure 仮想ネットワークを中心

従来の VDI

従来の VDI（オンプレミス型）では、ユーザー接続を実現するために、接続ブローカーや Gateway などの**基盤コンポーネントを自社で構築・運用する必要があります。(構築型)**

これらの構成要素は、接続制御や負荷分散、外部からのアクセス経路の確保などを担っており、設計・構築・運用のすべてを利用者側で対応する必要があります。

AVD

AVD では、接続ブローカーや認証（Entra ID）などの
ユーザー接続に必要な基盤コンポーネントを、
Microsoft がクラウド上の「コントロールプレーン」として提供・運用しています。(サービス利用型)

そのため、利用者はこれらの基盤を自ら構築・運用する必要がなく、セッションホスト（VM）など最小限のリソース管理に専念することが可能です。

接続基盤の役割分担の違い

観点	従来のVDI	AVD
接続基盤	自社で構築	Microsoft が提供
運用対象	全て	VM中心
接続制御	自社	サービス側中心

AVD の概要について詳しくは→ 【Azure Virtual Desktop】サービス概要

2.2. Azure Virtual Desktop におけるネットワーク前提

AVD は、従来の VDI とは異なる接続モデルを採用しており、ネットワーク設計における前提条件も大きく異なります。
本ページでは、AVD における接続の成立方法と、それに基づくネットワーク設計の前提について整理します。

AVD の接続の制御（認証など）はサービス側で行われる

AVD では、従来の VDI のようにユーザーが FW や VPN を通じて社内ネットワークへ直接接続し、セッションホストに到達するのではなく、Microsoft が提供するコントロールプレーン（認証・接続制御）を経由して、セッションホストへの接続が成立します。

このコントロールプレーンでは、ユーザー認証や接続制御、接続先のセッションホストの選定が行われており、接続の許可・制御はネットワーク機器ではなく、コントロールプレーンによって論理的に制御される構造となっています。

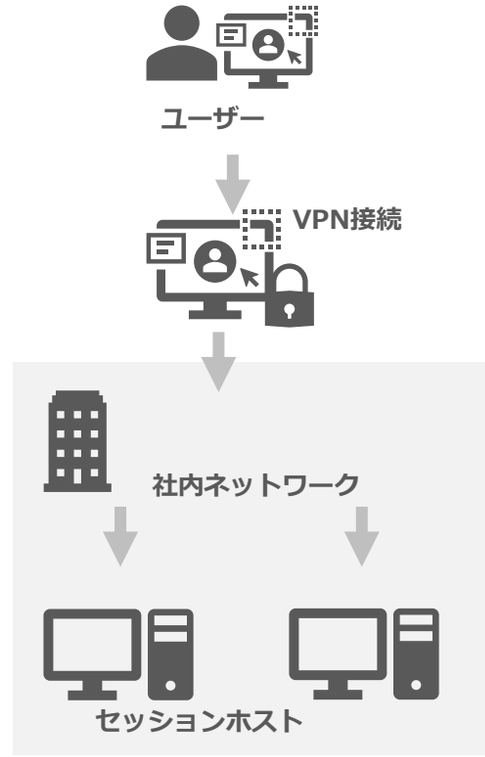
そのため、外部からのインバウンド通信を前提としない設計となり、コントロールプレーンや関連サービスへのアウトバウンド通信が可能となるようネットワーク設計を行う必要があります。

注意点

AVD の接続は Entra ID による認証を前提としていますが、条件付きアクセスの設定により、VPN 接続が必要となる場合があります。

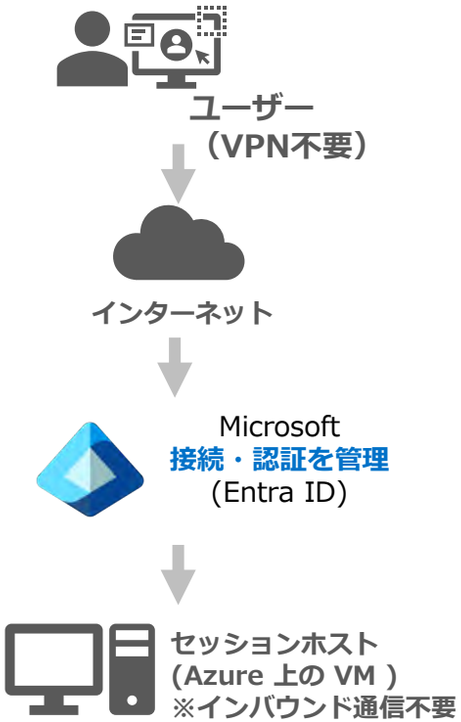
従来のVDI

前提：インバウンド通信必須



AVD

前提：アウトバウンド通信



2.3. コントロールプレーンとデータプレーンの責任分界点

AVD では、データプレーン（実行・通信）を利用者が管理し、コントロールプレーン（認証・接続制御）を Microsoft が管理する形で責任分界が明確に分かれています。

責任分離型のSaaS構成

AVD は SaaS として提供されますが、認証や接続制御は Microsoft が担う一方で、セッションホストやネットワークは利用者側で管理する必要があります。
このように、責任が分担されたハイブリッドな責任モデルである点が特徴です。

データプレーンにおけるネットワーク構成は、利用者が管理

接続制御は Microsoft のコントロールプレーンで実施されますが、VNet や NSG、UDR、DNS といったネットワークおよび業務通信の制御は利用者側の責任となります。
そのため、AVD においてもネットワーク設計が重要となります。

	従来VDI	AVD データプレーン	AVD コントロールプレーン
ユーザー・データ	■	■	■
デバイス	■	■	■
VM	■	■	-
OS	■	■	-
ネットワーク	■	■	□
ID / 認証	■	-	□
接続制御	■	-	□
物理基盤	■	□	□

■ 利用者責任　□ サービス提供者責任

まとめ

接続制御はMicrosoftが担い、**通信制御**と**通信経路**は利用者の責任で設計する必要があります。

2.4. 従来型 VDI とのネットワーク比較まとめ

従来の VDI では、ユーザーがセッションホストに到達するために、VPN 接続や RDP Gateway（DMZ 配置）などを用いて、社内ネットワークへ接続させる必要がありました。一方 AVD では、ユーザー接続は Microsoft が提供するコントロールプレーン（認証・接続制御）で仲介されるため、ユーザーを社内ネットワークに入れることなく、セッションホストへの接続が成立します。
以下の表では2章で説明した従来型 VDI とのネットワーク比較を表にまとめています。

観点	従来型 VDI	AVD
接続方式	社内へ接続	Microsoft 経由
ネットワーク設計	インバウンド中心	アウトバウンド中心
接続制御	自社実装	Microsoft 提供
セッションホストに繋がるまで	VPN や RDP Gateway（DMZ 配置）などの構成 必要	Microsoft がコントロールプレーンとして提供

3. Azure Virtual Desktop
ネットワークの仕組み

3.1. クライアント接続順序

AVD の接続は「認証 → 情報取得 → 制御 → セッション」の4段階で成立しています。
接続は、単一の通信だけでは成立しません。いずれかの通信が遮断されると、接続処理全体が成立しなくなる特徴があります。

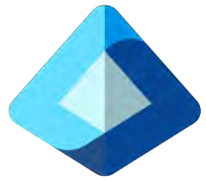
1. Entra ID 認証

ユーザーは AVD クライアントを起動し、Entra ID に対して認証を行う。

✓ユーザーの資格情報の検証

✓多要素認証（MFA）の実施（設定されている場合）

✓利用可能なリソースへのアクセス権の確認



2. リソース情報取得

AVD クライアントは「フィード」と呼ばれる情報取得処理を実施する。

✓ユーザーが利用可能なデスクトップ／アプリ一覧を取得

✓接続可能な AVD リソースのメタ情報を取得

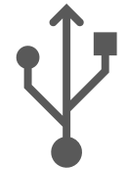
3. 接続制御

AVD クライアントは AVD コントロールプレーンに接続要求を送信する。

✓接続要求の検証および制御

✓使用可能なセッションホストの選定

✓接続先情報（RDP 情報）の生成



4. セッション確立

最終的に指定されたセッションホストへのセッションを確立する。

✓実際のセッション（RDPベース）の確立

✓ユーザーのログイン

✓業務環境の利用開始

※セッションホストは AVD エージェントにより事前にコントロールプレーンへ登録されています

3.2. 利用されるポート・プロトコルと暗号化

AVD の通信は、基本的にインターネット上で安全に接続できるよう設計されており、すべての通信は暗号化されたプロトコルで構成されています。一方で、業務用途によって必要な通信は大きく変化します。

基本となる通信プロトコル（固定）

AVD の接続においては、以下の通信が基本となります。

● **HTTPS（制御通信）…TCP 443**

すべての制御通信のベースとなるプロトコルであり、以下で利用される。

✓ Entra ID 認証
✓ フィード 取得
✓ コントロールプレーン通信

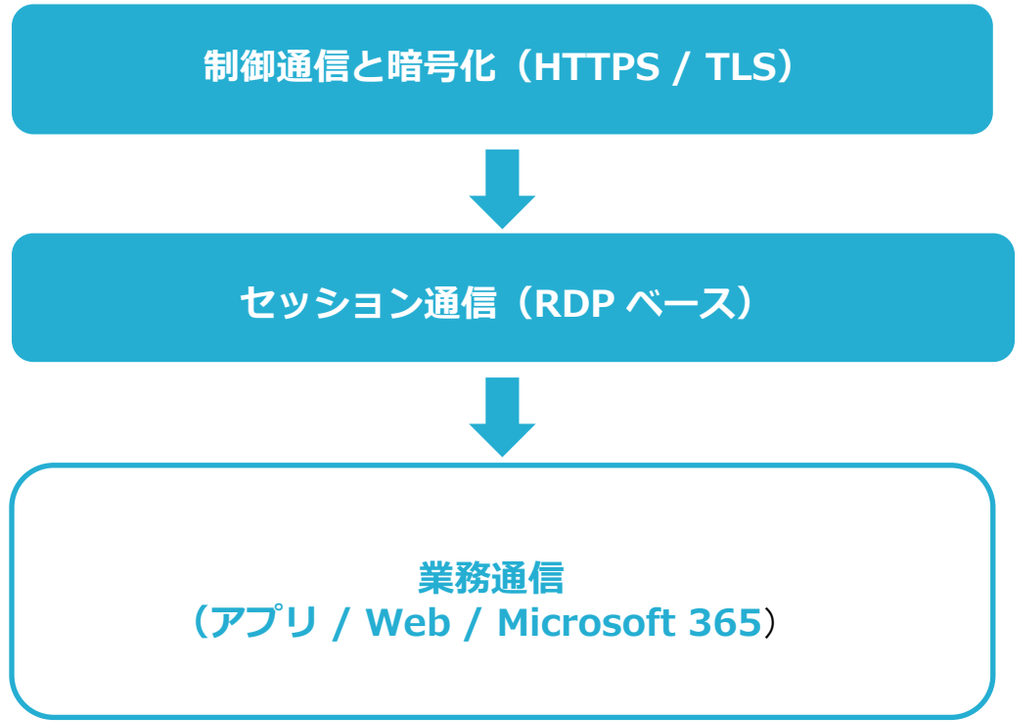
● **TLS（暗号化）**

通信内容を保護するための暗号化プロトコルであり、以下のすべてが暗号化される

✓ 認証情報
✓ 接続情報
✓ セッション情報

● **RDP ベースのセッション通信**

セッションホストとの通信は、**RDP をベースとしたプロトコル**により実現されます。
この通信は TLS により暗号化された形で提供されるため、セッション内で扱われる画面情報や操作内容も保護されます。



3.2. 利用されるポート・プロトコルと暗号化

本ページでは、AVD の通信を役割ごとに分類し、どの通信が設計の対象となるかを明確にします。

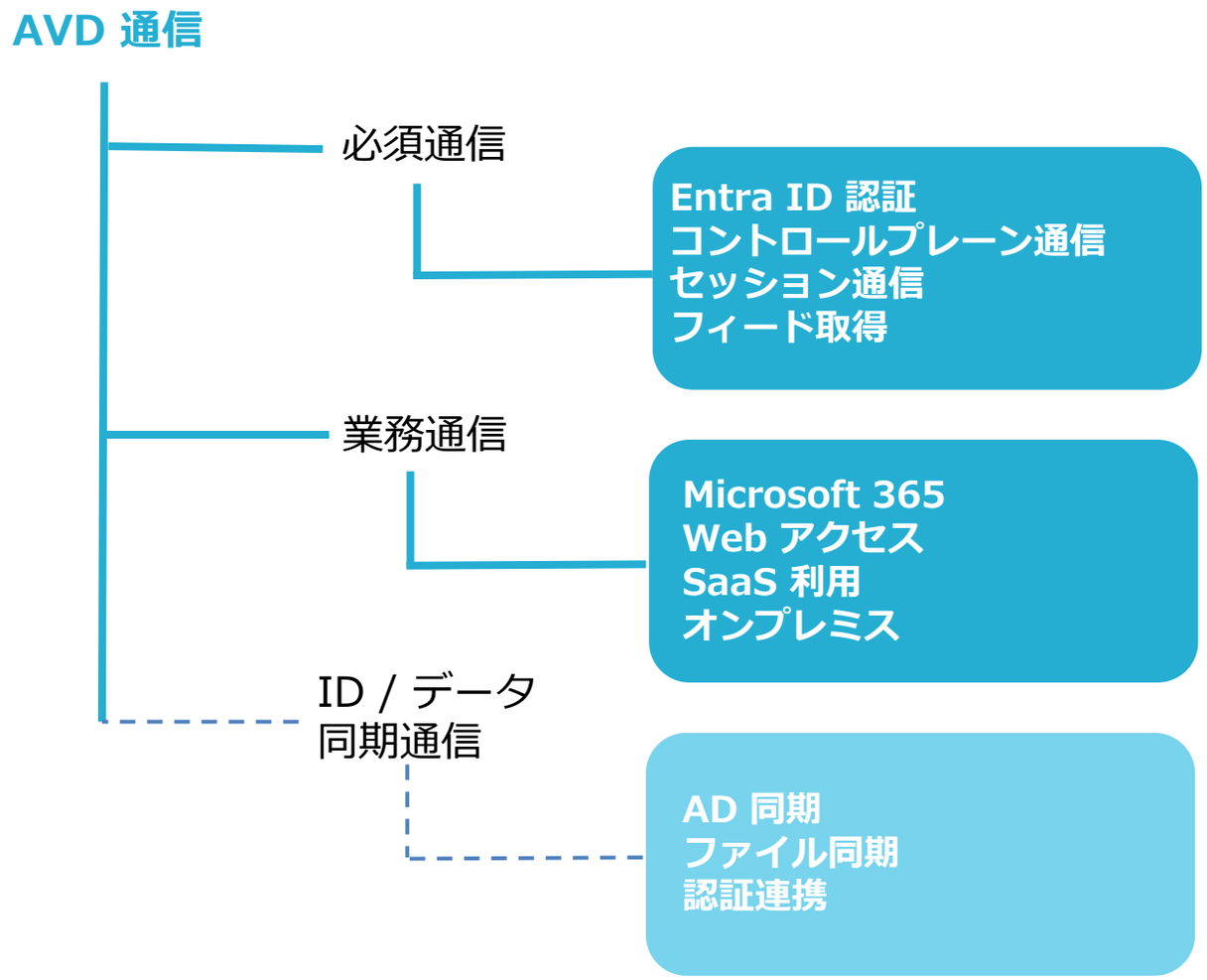
通信の分類（設計に関わる重要概念）

AVD の通信は大きく3つに分けられます。

●必須通信（停止すると接続不可）
✓ Entra ID 認証
✓ コントロールプレーン通信
✓ セッション通信
✓ フィードバック取得

●業務通信（要件依存）→設計の対象
✓ Microsoft 365 など
✓ Web アクセス
✓ SaaS 利用
✓ オンプレミス

●ID / データ同期通信（ハイブリッド時のみ）
→設計の対象
✓ AD 同期
✓ ファイル同期
✓ 認証連携



4. 導入・構成パターン別ネットワーク設計

4.1. Microsoft Entra ID のみのクラウド完結構成の場合

本章では、AVD のネットワーク設計を構成パターン別に整理します。
利用するサービスや連携要件に応じて必要な通信が異なるため、各構成における通信の特徴を把握し、設計判断に活用できる形でそれぞれ整理します。

設計判断ポイント

最小限の通信許可で成立するシンプル構成

- ✓ インバウンド通信は原則不要
- ✓ アウトバウンド通信を許可すれば成立
- ✓ 細かい通信制御を行わなくても構成が成立する

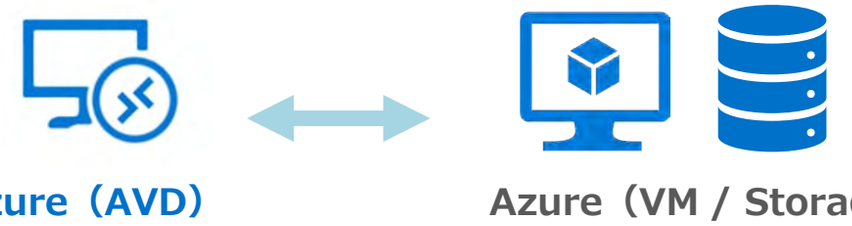
必要な通信の種類

- ✓ Entra ID 認証通信
- ✓ コントロールプレーン通信
- ✓ セッション通信（AVD接続）
- ✓ Microsoft 365通信（Outlook / OneDrive 等）

どのような人向けの構成か

- ✓ PoC / 小規模 / 新規導入向け
- ✓ オンプレミス環境を利用しないケース
- ✓ 最小構成で AVD を利用したいケース

成立する通信モデル例



オンプレミス環境を利用しない

4.2. Entra Connect 利用時のハイブリッド構成の場合

Entra Connect 利用のハイブリッド構成時の場合について説明します。

設計判断ポイント

業務要件によってオンプレミス通信が増える構成

- ✓ AVD のための通信ではない
- ✓ 「同期・認証のための通信」が増える
- ✓ オンプレミス起因の通信がボトルネックになる

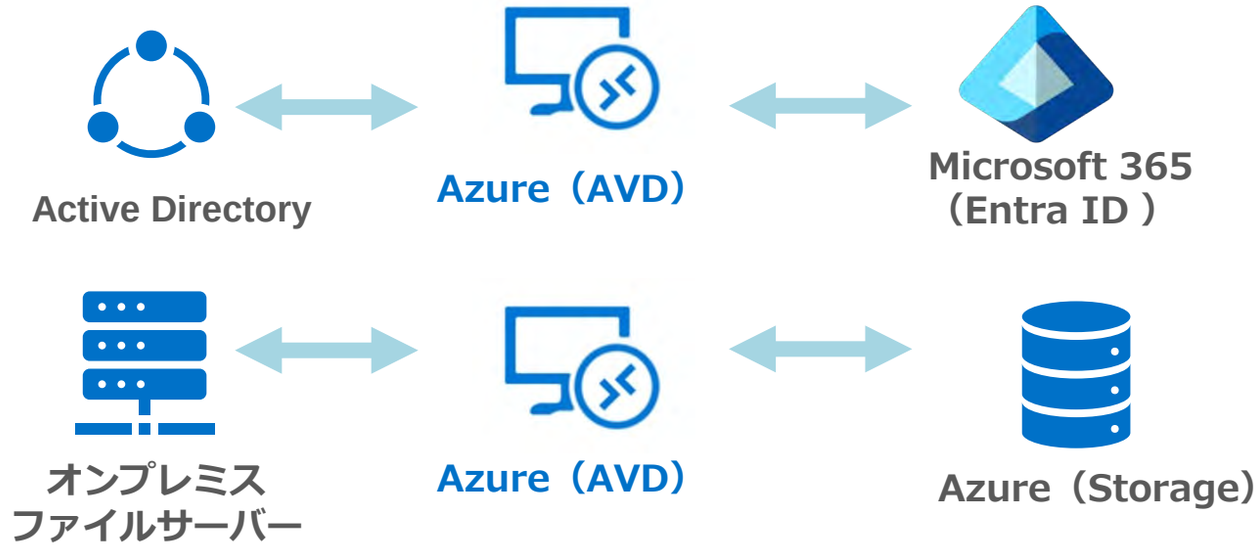
必要な通信の種類

- ✓ ID同期通信（Entra Connect）
- ✓ 認証通信（オンプレミス連携の場合）
- ✓ ファイル同期通信（File Sync 等）
- ✓ セッション → オンプレミスアクセス通信

どのような人向けの構成か

- ✓ オンプレミス AD を継続利用したいケース
- ✓ 既存ファイルサーバーと連携したいケース
- ✓ ID・データをハイブリッドで統合したいケース

成立する通信モデル例



4.3. VPN ・ ExpressRoute 利用構成の場合

VPN ・ ExpressRoute 利用構成の場合について説明します。

設計判断ポイント

通信ごとに扱いを変える設計

- ✓ この通信は VPN 通す？通さない？
- ✓ この通信は社内ポリシー適用する？
- ✓ この通信はインターネットへ直接の接続？

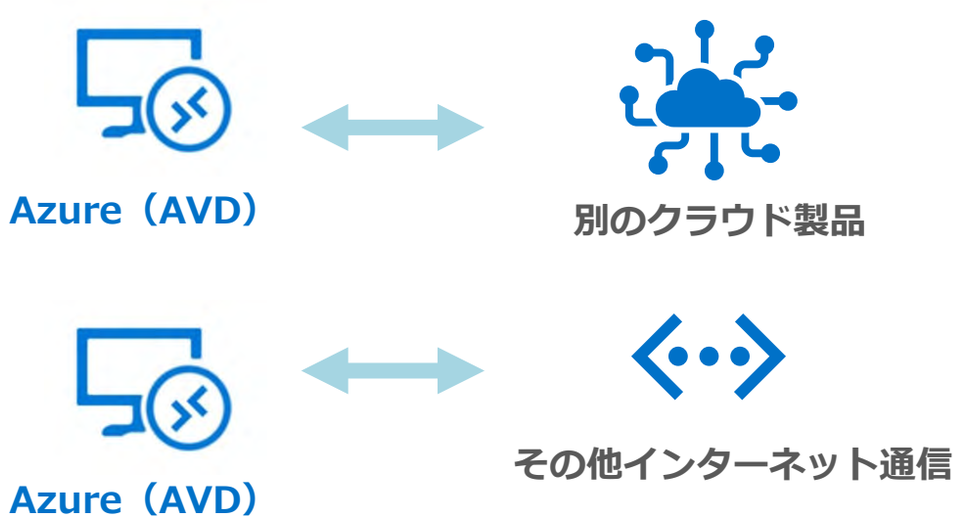
必要な通信の種類

- ✓ AVD 通信認証
- ✓ 接続制御通信 / セッション通信
- ✓ 業務通信
- ✓ メール通信（例：Outlook）
- ✓ Web アクセス
- ✓ 社内システム通信
- ✓ 外部 SaaS 通信　など

どのような人向けの構成か

- ✓ セキュリティ要件が高いケース
- ✓ 環境通信制御を厳密に行いたいケース
- ✓ クラウドと社内ネットワークを統合して制御したいケース

成立する通信モデル例



各通信について VPN Gateway で設定している会社のネットワークポリシーの適用対象とするかどうかを考える必要がある

5. 設計・構成・設定時の考慮事項

5.1. 配置：VNet ・サブネット設計の考え方

本章では、AVD のネットワークの設計・構成・設定時に考慮すべき事項について、「配置」「経路」「名前解決」の観点からそれぞれ整理します。
VNet / サブネット 設計では、接続先の種類と通信の制御レベルに応じて配置を決定します。
本ページではまず、その際に判断軸となる「配置」の考え方について紹介します。

接続先の種類

**接続先の種類に応じて、
必要となるネットワーク構成
および通信経路を判断**

この判断は、必要な通信の種類や経路設計、ネットワーク構成の複雑さに大きく影響します。

■ **クラウド完結（4.1）**
✓通信は Azure / Microsoft 365 内で完結
✓シンプルな構成で成立

■ **ハイブリッド構成 （4.2）**
✓ VPN / ExpressRoute による接続が必要
✓ DNS や認証連携の設計が重要

■ **他クラウド・インターネット制御あり（4.3）**
✓通信の制御（FW など）が必要
✓経路設計が重要

ネットワーク分離の必要性

**AVD 環境を専用の VNet として分離するか、
既存の VNet に統合するかの判断**

この判断は、セキュリティ要件・影響範囲・運用分離の観点に大きく影響します。

■**AVD 専用 VNet とする場合**
✓他システムとの分離が容易で、
影響範囲を限定可能
✓検証環境や PoC、小規模導入に適する

■**既存 VNet に統合する場合**
✓業務システムとの連携がシンプル
✓既存ネットワークポリシーで適用可能

ポイント
分離するか統合するかにより、セキュリティ境界と通信設計の複雑さが決まる

運用主体・ネットワークチーム分離

**ネットワークの管理主体や運用単位に応じて、
VNet およびサブネットの
分離粒度や配置を判断**

この判断は、運用効率や管理責任の分界、構成の分離粒度に大きく影響します。

■**サブスクリプションが分離されている場合**
✓ Vnet も分離される傾向
✓ ピアリングや Hub-Spoke 構成が前提

■**ネットワーク管理チームとシステム管理チームが分離されている場合**
✓ Hub-Spoke 構成が採用されやすい
✓ ポリシー統制を重視した設計

**技術要件だけでなく、
運用体制も重要な要素となります。**

5.2. 経路：NSG・UDR・NAT Gateway 設計の判断軸

ネットワーク設計では、どの通信（3.2）をどの経路で、その範囲まで制御するかを決めます。
その際に判断軸となる「経路」について紹介します。

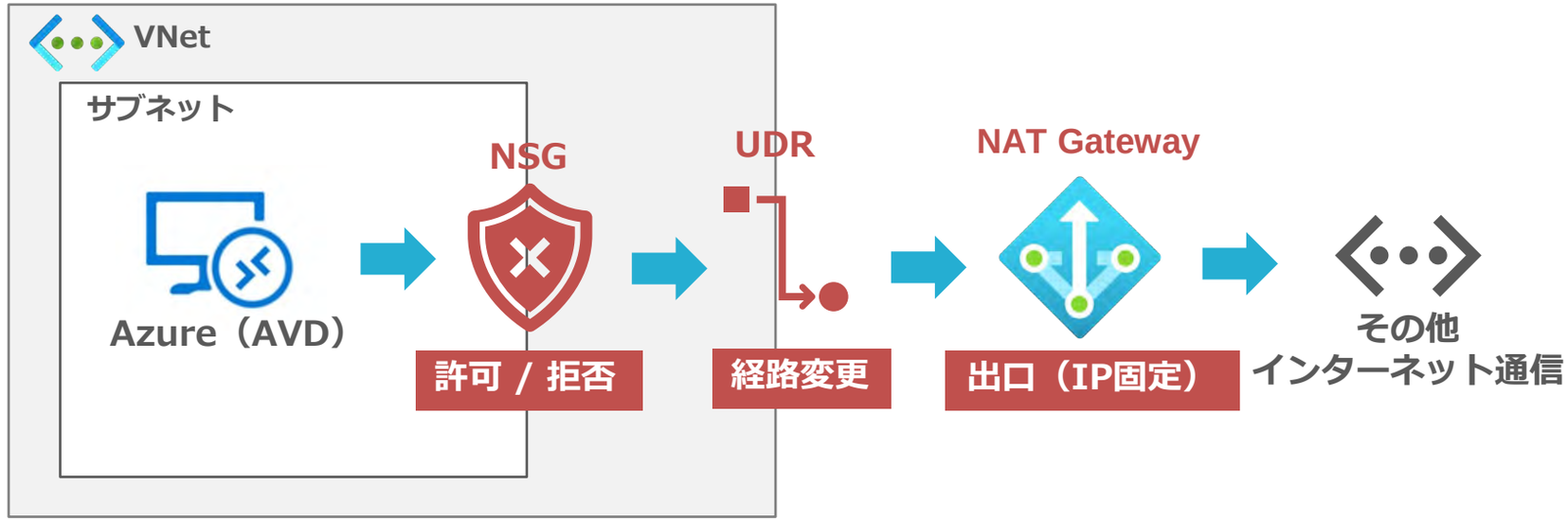
NSG・UDR・ NAT Gateway の役割

NSG の役割
- ✓ サブネット／NIC 単位で通信を許可・拒否
- ✓ AVD 必須通信を遮断すると接続自体が成立しない
- ✓ 業務通信を制御する主なポイント

UDR の役割
- ✓ 通信経路の制御
- ✓ VPN / FW 経由の強制
- ✓ 通信をどこへ流すか決める

NAT Gatewayの役割
- ✓ アウトバウンド通信のIP固定
- ✓ インターネット接続の管理ポイント

■ AVD からその他インターネット通信へ、制御付きで接続する構成図例



推奨されない設計パターン

- ✗ セッションホストの RDP をインターネットに公開する構成：不適切
- ✗ AVD の必須通信を NSG で制限する構成：通信不可になる
- ✗ すべての通信を VPN 経由とする構成：遅延・輻輳

5.3. 解決：DNS・名前解決の設計注意点

DNS・名前解決の設計は、通信の前提となる重要な要素であり、設計ミスは接続不良や認証エラーの原因となります。
本ページでは、AVD 環境における「名前解決」の設計上の注意点を整理します。

設計上の注意点

名前解決経路の統一

不整合の発生を防ぐため、参照する DNS サーバーを明確にし、すべての名前解決が一貫した経路で実行されるよう設計する。

Azure / オンプレミス DNS の使い分け

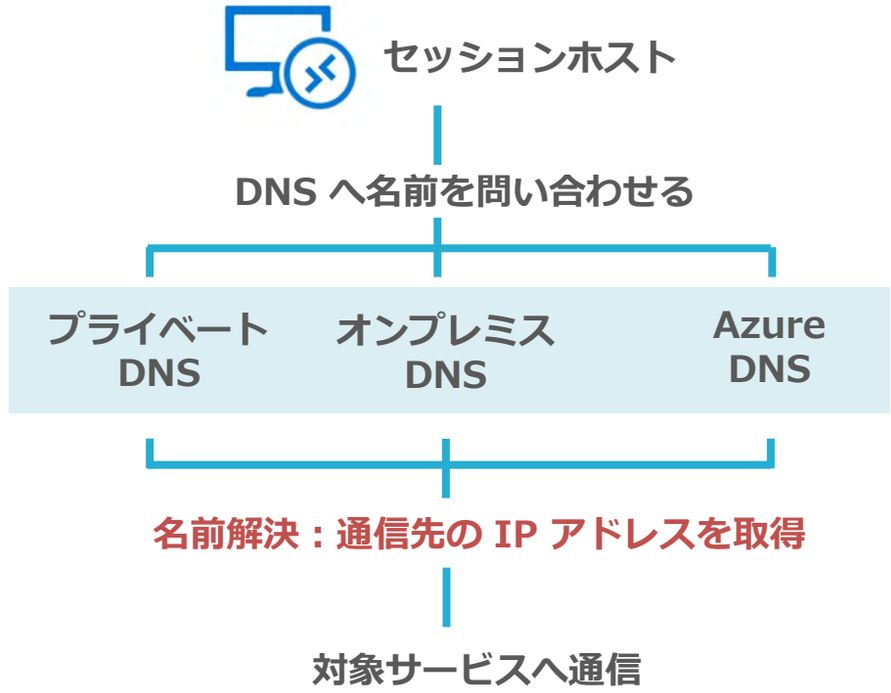
Azure 標準 DNS、オンプレミス DNS、プライベート DNS を適切に役割分担する。

ハイブリッド構成時の DNS 設計

オンプレミス環境と連携する場合、DNS フォワーディングや参照経路を設計する。

よくあるトラブル

症状	原因
ドメイン参加できない	AD DNS 未参照
ログインが遅い	ドメインコントローラー解決不可
ファイルサーバに接続できない	名前解決の不一致
アプリに接続できない	プライベート DNS 未設定



ポイント

名前解決の経路が統一されていないと通信は成立しません

6. 設計判断の軸

6.1. 提案・要件定義フェーズで必ず確認すべき事項

本章では、提案・要件定義フェーズにおいて要件の分解に必要となる事項を紹介します。

■「どこから」（ユーザーの接続元）

質問
- 社内ネットワーク？
- 社外インターネット？
- 海外拠点？
- BYOD 利用？

影響する設計
- NSG / UDR 設計
- VPN / インターネット経路
- 通信制御ポリシー

■「何と連携」（通信先の整理）

質問
- Microsoft 365？
  （Exchange / SharePoint）
- オンプレミス AD？
- ファイルサーバー？
- 他クラウド / SaaS？

影響する設計
- 必須/業務通信
- ハイブリッド構成
- DNS 設計

■「どこまで閉じたいか」（制御レベル）

質問
- インターネット自由利用？
- 業務通信だけ許可？
- すべて社内経由？

影響する設計
- VPN
- NSG / UDR
- FW

■「どの通信をどう扱うか」（通信の扱い）

質問
- AVD 必須通信はどこまで許可するか？
- 業務通信はどの経路で通信させるか？
- 特定通信のみ制御対象とするか？

影響する設計
- 接続方式
- セキュリティモデル
- 認証方式