【Microsoft Azure】サービス概要

2025年3月31日

改定履歴

版数	発行日	改訂内容
第1版	2025年3月31日	初版発行

本資料の内容は 2025/3/31 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でご了承ください。

Agenda

1. 前提情報
    1. 本書の目的とゴール
    2. 用語集
2. クラウドコンピューティング
    1. クラウドコンピューティング
    2. クラウドコンピューティングの種類
    3. クラウドサービスの種類
    4. クラウドサービス種類の比較
    5. クラウドサービスにおける責任範囲
    6. 代表的なクラウドコンピューティング サービス
3. Microsoft Azure の基本
    1. Microsoft Azure の特徴
    2. Microsoft Azure の構成要素① 物理インフラストラクチャ
    3. Microsoft Azure の構成要素② 管理インフラストラクチャ
    4. Azure Resource Manager
    5. Microsoft Azure サービスの種類
4. コンピューティングサービス
    1. 仮想マシンとは
    2. コンピューティングサービスの例
5. ネットワークサービス
    1. クラウドネットワークサービスとは
    2. Microsoft Azure ネットワークサービスの種類
    3. Azure Virtual Network（VNet）
    4. VNet の機能① IP アドレスの取得
    5. VNet の機能② サブネット分割
    6. VNet の機能③ 他のネットワークへの接続
    7. Azure サービスエンドポイント
    8. Azure ネットワークセキュリティグループ (NSG)
6. 基本的な Azure 環境構成
    1. 基本的な Azure 環境構成と検討フロー
    2. Azure Bastion

1. 前提情報

1.1. 本書の目的とゴール

目的

Microsoft Azure は幅広いクラウドコンピューティングサービスを数多く提供しており、利用者の要件や設定によって多種多様な活用が可能です。
本資料は Microsoft Azure のサービス概要を把握することを目的とし、そのために必要な関連情報や知識をまとめ提示するものです。

ゴール

本資料を通し、以下の内容を理解できる状態を目指します。

1. **クラウドコンピューティングの基本概念を理解する**
2. **オンプレミスとクラウドネットワークの違いを理解する**
3. **IaaS, PaaS, SaaS の違いを理解し、クラウドサービスにおける責任範囲について認識する**
4. **Microsoft Azure の基本構成要素について理解する**
5. **Microsoft Azure の仮想ネットワーク構築について概要を把握する**

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	アプリケーション	ユーザーが利用するソフトウェアやサービスのこと。例：Webアプリや業務システム。
2	データ	アプリケーションで扱う情報。ファイル、設定、ログ、データベースなどが含まれる。
3	ランタイム	アプリケーションを実行するための環境。例：.NET、Java Runtimeなど。
4	ミドルウェア	OSとアプリケーションの間で動作し、機能を補完するソフトウェア。例：Webサーバーやデータベース管理システム。
5	OS	コンピューターを動かす基本ソフト。例：Windows、Linux。
6	仮想化	1台の物理サーバー上に複数の仮想マシン（VM）を動かす技術。
7	物理サーバー	実際に存在するハードウェアのサーバー。仮想マシンの土台となる。
8	記憶域	データを保存する場所。HDDやSSD、クラウドストレージなどがある。
9	ネットワーク	コンピューター同士をつなげて通信する仕組み。インターネットや社内LANなど。

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
10	従量課金制	使った分だけ料金が発生する仕組み。クラウドでは一般的な料金体系。
11	物理ホスト	仮想マシンを動かす実体のある物理的なコンピューター。
12	物理ネットワーク	ケーブルやスイッチなど、実際に存在する通信インフラ。
13	物理データセンター	サーバーやネットワーク機器を設置する建物や施設。
14	Azure API	Azureの機能をプログラムから操作するためのインターフェース。自動化や連携に利用される。
15	ポート番号（RDP/SSH、HTTPS）	ネットワーク通信で特定のサービスに接続するための入り口番号。代表例として、RDP（リモートデスクトップ）は3389番、SSHは22番、HTTPS通信には443番が使われる。
16	VPN 接続	インターネットを通じて安全に拠点間やクラウドと通信するための技術。
17	ネットワークインターフェース（NIC）	Azureで仮想マシンをネットワークに接続するための重要なコンポーネントで、通信に必要なIPアドレスや設定情報を保持する。複数のNICを追加することでネットワーク分離や冗長化が可能になり、セキュリティグループやパブリックIPアドレスと組み合わせて通信の制御や安全な接続を実現できる。

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
18	インスタンス	アプリケーションが稼働する仮想サーバーのこと。または、仮想サーバーの数やサイズ（CPU数、メモリ容量、ストレージ容量）を指す。クラウドサービス提供元によって意味に多少の違いがあるため注意。
19	冗長構成	障害に備えて、予備のシステムや経路を用意する構成。高可用性を実現する。
20	OSディスク	仮想マシンのオペレーティングシステムをインストールするために使用され、VMの起動に必須。
21	データディスク	アプリケーションデータやログファイルを保存するための追加ストレージで、OSディスクとは別に管理される。データのバックアップや拡張が容易になり、パフォーマンスを向上させることができる。
22	負荷分散	複数のサーバーに処理を分散させ、性能向上や障害対策を行う仕組み。
23	RDP/SSH接続	リモートでVMに接続する方法。RDPはWindows向け、SSHはLinux向け。
24	TLS	インターネット通信を暗号化するプロトコル。WebサイトやAPIの通信を安全に保つ。

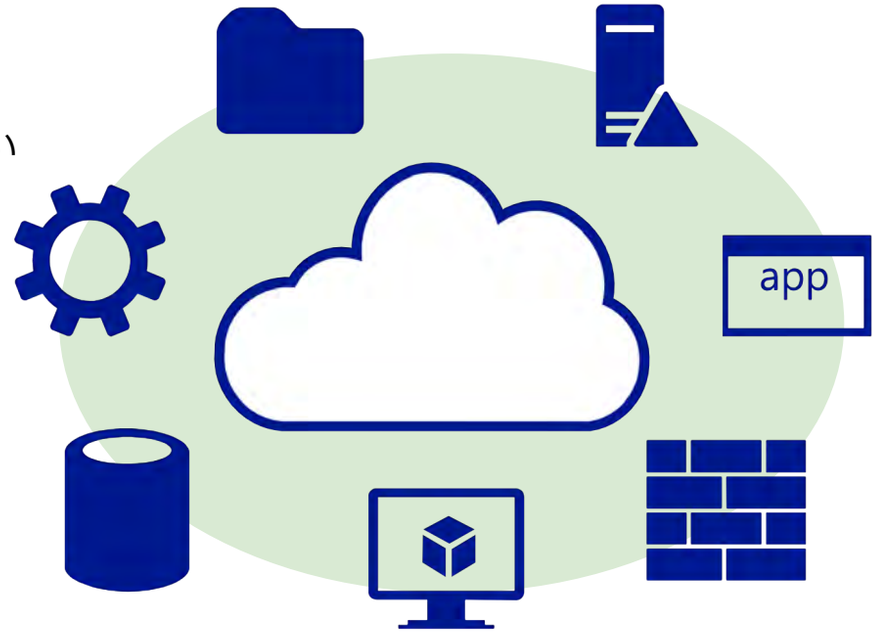
2. クラウドコンピューティング

2.1. クラウドコンピューティング

■クラウド コンピューティングとは
インターネット（クラウド）を経由して、インターネット上のサーバーに存在するコンピューター リソースを利用する仕組みのことです。
クラウドコンピューティングで利用できるリソースにはサーバー、プラットフォーム、ネットワーク、データベース、ストレージ、ソフトウェアなどがあります。クラウドとも呼ばれます。

■クラウド コンピューティングの特徴
・メリット
- ソフトウェア・ハードウェアを自社で購入する必要がないため、初期費用が安い
- サービスの導入から利用開始までが早い
- 導入したサービスの運用・保守管理が不要
- 拡張性が高い
- インターネットが使える環境であればいつでも利用できる

・デメリット
- インターネットが使えない環境では利用できない
- サービス終了の可能性がある



■クラウド コンピューティングサービス導入時の検討事項
導入を考える際、まずは「**クラウド コンピューティングの種類**」と「**クラウド サービスの種類**」を検討する必要があります。
次のページで紹介します。

2.2. クラウドコンピューティングの種類

■クラウド コンピューティングサービス導入時の検討事項①：クラウド コンピューティングの種類
まず、どの環境でクラウド コンピューティングを実装するかを検討します。
それぞれの種類により特徴が異なるため、組織の特性と使う目的に合わせて使い分ける必要があります。

	パブリッククラウド	プライベートクラウド	ハイブリッドクラウド
特徴	- 共有サーバ設備 クラウド サービス プロバイダーが所有・運営するクラウド リソース (サーバーやストレージなど)をインターネット経由で利用	- 専有サーバ設備 ・ホスティング型：クラウド プロバイダーが提供するパブリッククラウド内に、仮想的に専用の領域を確保 ・オンプレミス型：組織内にデータセンターを物理的に配置	- 共有サーバと専有サーバの組み合わせ
利用形態	不特定多数のユーザーが物理的に同じサーバを共用する	特定のユーザーだけが専有サーバを利用する	パブリック型とプライベート型を併用する
メリット	・導入が早く工数が少ない ・サービス提供者が所有・運用するため、メンテナンスが不要	・カスタマイズの自由度が高い ・セキュリティが強固	・用途に応じてパブリック型とプライベート型の長所を活かせる
デメリット	・カスタマイズが難しい ・セキュリティ上のリスクが比較的高い	・導入・運用の手間、工数がかかる	・管理が煩雑 ・パブリックとプライベートの切り分けを行う必要がある
費用	安い	高い	用途に応じて最適化できる

2.2. クラウドコンピューティングの種類

【 プライベートクラウドについての補足 】

前のページで、クラウド コンピューティングの種類には **パブリッククラウド、プライベートクラウド、ハイブリッドクラウド**の 3つがあると記載しました。そのうちの**プライベートクラウド**はさらに「**ホスティング型**」と「**オンプレミス型**」の 2種類に分けられます。

どちらも利用者（組織）が自社専用のクラウド環境を構築・運用できる仕組みですが、異なる特徴を持つため用途に合わせた選択が可能です。

ホスティング型プライベートクラウド

クラウド事業者が提供するパブリッククラウド内で、仮想的に設けた領域を自社専用で利用する形態です。クラウド事業者がインフラの運用管理を行うため、利用者はインフラの運用管理にかかるコスト削減が可能です。

クラウドサービスの環境を占有できるため、ほかの利用者の影響を受けにくく、性能やセキュリティを確保しやすいです。

オンプレミス型プライベートクラウド

自社でシステムの設置場所やサーバーやネットワーク機器などのインフラを用意し、その上にクラウド環境を構築、運用します。

インフラの構築や保守管理も自社で行うためコスト、時間や労力、専門知識を持つ人材が必要になります。

大規模なシステムを持つ、大企業や企業グループなどで活用されています。

【 **オンプレミス** と **オンプレミス型**プライベートクラウドの違い 】

オンプレミスとは、自社内にシステムを構築・運用する従来型のシステム形態です。物理的なサーバーやネットワーク機器などのハードウェアを保有し、運用管理することを指します。

オンプレミス型プライベートクラウドとの違いは、**構築するシステムがクラウド環境として作られるか否か**です。

2.3. クラウドサービスの種類

■クラウド コンピューティングサービス導入時の検討事項②：クラウド サービスの種類
クラウド コンピューティングのサービス種類は大きく「サービスとしてのインフラストラクチャ（IaaS）」、「サービスとしてのプラットフォーム（PaaS）」、「そしてサービスとしてのソフトウェア（SaaS）」で分けられます。
利用者とサービス提供者の役割に違いがあり、組織はリソースの制御レベルによってどのサービスを利用するか選択できます。

オンプレミス	**IaaS**	**PaaS**	**SaaS**
アプリケーション	アプリケーション	アプリケーション	アプリケーション
データ	データ	データ	データ
ランタイム	ランタイム	ランタイム	ランタイム
ミドルウェア	ミドルウェア	ミドルウェア	ミドルウェア
OS	OS	OS	OS
仮想化	仮想化	仮想化	仮想化
物理サーバー	物理サーバー	物理サーバー	物理サーバー
記憶域	記憶域	記憶域	記憶域
ネットワーク	ネットワーク	ネットワーク	ネットワーク

組織 管理領域　サービス提供者管理領域

2.4. クラウドサービス種類の比較

「サービスとしてのインフラストラクチャ（IaaS）」、「サービスとしてのプラットフォーム（PaaS）」、「そしてサービスとしてのソフトウェア（SaaS）」の特徴は以下のように比較できます。

	IaaS	PaaS	SaaS
特徴	インターネット経由でサーバやネットワーク機器などのインフラ部分を提供	インターネット経由でアプリケーションを開発するためのプラットフォームを提供	インターネット経由でアプリケーションやソフトウェアを提供
利用可能なリソース	・仮想サーバや回線などのインフラ設備一式	・サーバなどのハードウェア ・OS	・ソフトウェア ・アプリケーション
メリット	・必要なハードウェアのスペックやOSを自由に選べる ・拡張性が高い	・アプリケーション開発に集中できる ・開発コストや期間を抑えられる	・パッケージのインストールなどの手間が不要 ・サービスを即時導入、利用できる
デメリット	・開発やサーバ管理などの専門知識が必要	・使用言語やOSなど希望する開発環境を自由に選べない	・カスタマイズ性が低い ・サービスを利用するためのOSやハードウェアは自社で用意する必要がある
料金体系	利用時間、ストレージ容量、ネットワークトラフィックなどにもとづく従量課金制が一般的	CPU利用率、ディスク利用率、ネットワーク帯域幅、トランザクションなどにもとづく従量課金制が一般的	利用プランやオプション、利用ID数などにもとづく定額制が一般的

2.5. クラウドサービスにおける責任範囲

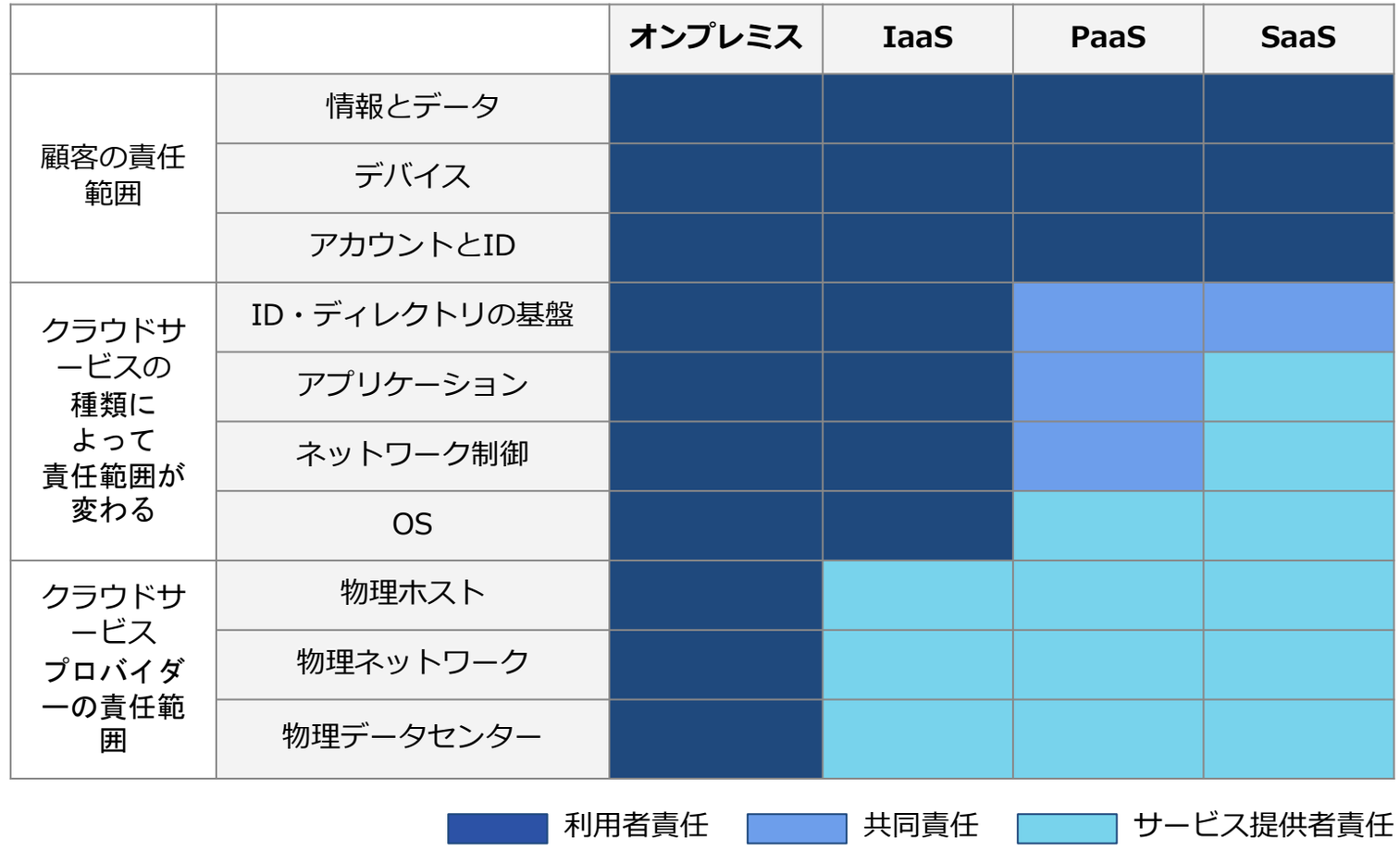
従来のオンプレミス環境ではすべてのリソースやセキュリティを自社で管理していました。
それに対し、クラウドサービスは種類によってそれぞれ提供するサービスの範囲が異なるため、利用者とサービス提供者での管理責任を共有することになります。

利用者とサービス提供者とで誰がどの部分の責任を持つのか定めたものを「**共同責任モデル（責任共有モデル）**」と言います。

クラウドサービスを提供する Microsoft AzureやAWS（Amazon Web Service）、GCP（Google Cloud Platform）などのサービス提供者はそれぞれ責任範囲を明示・公開しています。

右の図は Microsoft社が公開しているモデルで、責任共有モデルに基づく一般的な責任範囲を表したものです。

「IaaS」＜「PaaS」＜「SaaS」とサービス事業者の責任範囲は大きくなり、利用者の責任範囲は小さくなります。ただし、利用者の設定によりシステムの挙動が変わる部分については利用者の責任です。



2.6. 代表的なクラウドコンピューティング サービス

クラウドコンピューティングのサービスのなかで、最大手は以下の3つです。

	提供元	提供サービス数	特徴
Microsoft Azure	Microsoft	200 以上	・Windows や Office など Microsoft 製品との親和性が高い ・Microsoft ライセンスと組み合わせることでコスト削減が可能
AWS （Amazon Web Services）	アマゾン	300 以上	・サービス数が多い ・サービスのカテゴリーが多岐に渡る ・歴史が長く、ナレッジを持つ技術者が豊富
GCP （Google Cloud Platform）	Google	160 以上	・Google サービスと連携可能 ・Google の AI やデータ分析、機械学習を活用できる

各クラウドサービスの提供者によって利用可能なサービスが異なります。また、提供されるサービスは日々拡充・更新されています。
サービスは従量課金制を採用しており、導入する組織が必要なサービスを選択・組み合わせて使用することでコストが発生します。

本資料では Microsoft Azure のサービス概要についてご案内します。

3. Microsoft Azure の基本

3.1. Microsoft Azure の特徴

Microsoft Azure は、Microsoft が提供するクラウドコンピューティングのサービスです。
Microsoft Azure のサービスは大きく**仮想化されたインフラストラクチャーを提供する IaaS のサービス**と、
アプリケーション実行環境を提供する PaaS のサービスで分類できます。

特徴

・クラウドでのサービス提供
全ての機能がクラウド上で提供されるため、ユーザー側ではサーバー確保などの初期導入コストを抑えられます。

・Microsoft 製品との親和性が高い
Microsoft のクラウドプラットフォームであるため、Windows OS、Office 365、Dynamics 365など
Microsoft 製品群とのシームレスに連携できます。

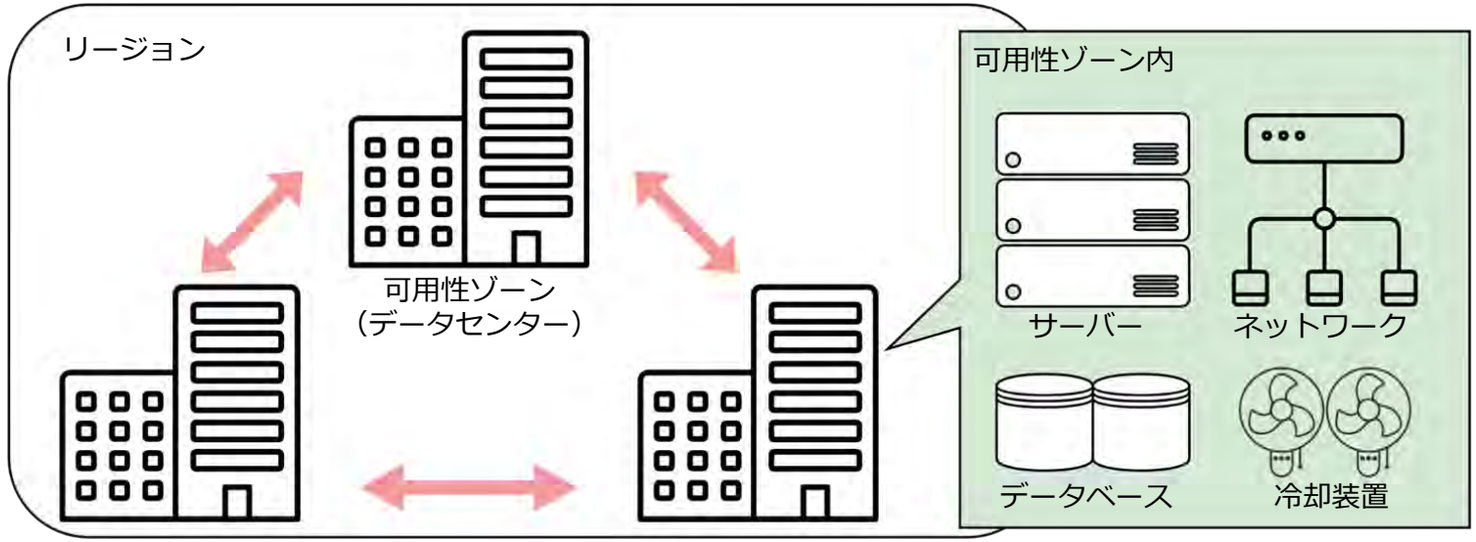
・拡張性・柔軟性が高い
リソースを自由に増減させることができるため、状況に応じて運用を最適化することができます。
また、Microsoft が提供している他のさまざまなアプリケーションやサービスと連携して、組織の状況に合わせた柔軟な活用が可能です。

・ハイブリッドクラウドの実現
オンプレミス環境とクラウドを連携したハイブリッド環境が構築・管理できます。

・障害や災害への対策
世界 60ヵ所の地域にデータセンターがあり、一部の地域で障害・災害などが発生しても、他の地域のサーバーを利用して迅速なサービスの復旧が可能です。

3.2. Microsoft Azure の構成要素① 物理インフラストラクチャ

Microsoft Azure のコア アーキテクチャ コンポーネント（仕組みを支える構成要素）を案内します。

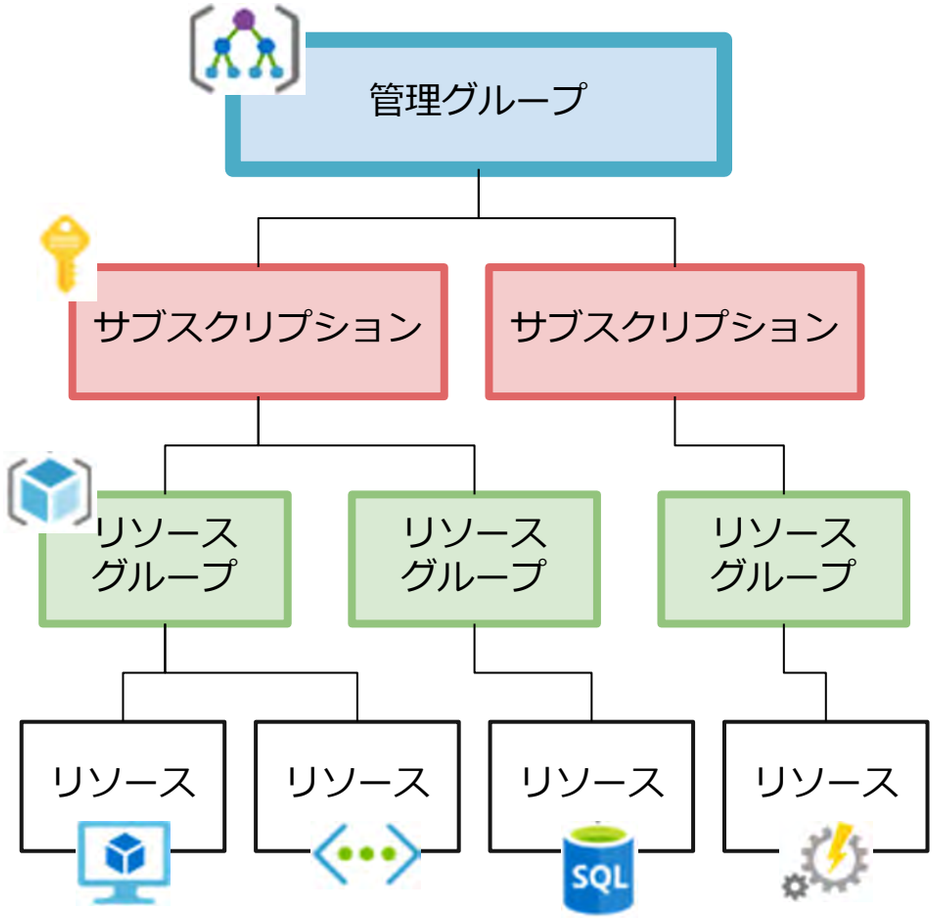


	概要
リージョン	世界に位置する物理的データセンターのグループ。 リソースのデプロイ先とされ、可用性向上のために近いリージョンを利用することが一般的。安定的な使用のために複数のリージョンを活用するケースも多い。 日本国内のリージョンは2つ（東日本リージョン、西日本リージョン）
可用性ゾーン	単一のリージョン内にある、独立したデータセンターのグループ。 独自の電源、冷却、およびネットワークインフラストラクチャを持っており、物理的に分離されているため、リージョン内の一部のインフラストラクチャに障害が発生した場合でも他の可用性ゾーンは影響を受けない。

3.3. Microsoft Azure の構成要素② 管理インフラストラクチャ

Microsoft Azure のコア アーキテクチャ コンポーネント（仕組みを支える構成要素）を案内します。

	概要
リソース	Azure が管理するサービスの要素。 仮想マシンや仮想ネットワーク、ストレージ、データベースなど。
リソースグループ	サブスクリプション内の関連するリソースをまとめて管理するコンテナー。 各リソースは1つのリソースグループに所属できる。
サブスクリプション	Azure のサービスやリソースを利用する際の、課金とアクセス制御の単位。 各リソースは1つのサブスクリプションに関連付けられる。
管理グループ	1つ以上のサブスクリプションに使用するコンテナー。 管理グループ、サブスクリプション、リソース グループ、リソースからなる階層を定義し、アクセス、ポリシー、コンプライアンスを継承し管理できる。

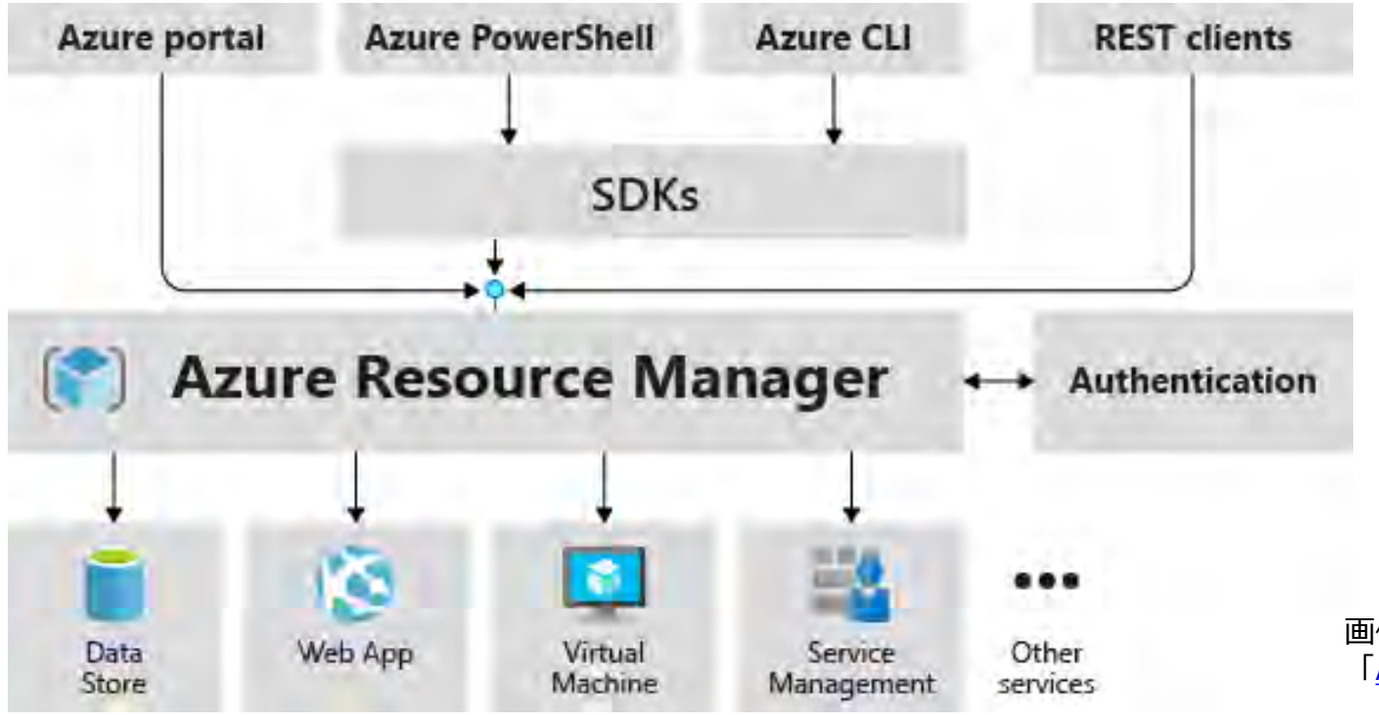


3.4. Azure Resource Manager

Azure のリソースをデプロイ、更新する管理サービスが **Azure Resource Manager** です。

ユーザーが Azure API、ツール、または SDK のいずれかを介して要求を送信すると、Azure Resource Manager が要求を受信します。
要求は、認証および承認された後、適切な Azure サービスに転送されます。すべての要求が同じ API を介して処理されるため、異なるツールでも一貫した結果と機能が得られます。

以下の図は、Azure の要求の中で Resource Manager が果たす役割を示しています。



画像出典：Microsoft ドキュメント
「Azure Resource Manager とは」

3.5. Microsoft Azure サービスの種類

Microsoft Azure はクラウドコンピューティングの領域で200以上のサービスを提供しています。数多くのサービスから組織で必要な機能を選択し利用できます。
以下の表でMicrosoft Azure のサービスのコアサービスを紹介します。

サービスカテゴリー	概要	サービスの例
コンピューティング	仮想マシンやサーバーレスの環境を提供し、アプリケーションの実行やコンテナ管理を行う	・Azure Virtual Machines (VM) ・Azure App Services ・Azure Functions
ネットワーク	ネットワークインフラの設計・管理を行う クラウド内外での安全かつ効率的な通信を可能にする	・Azure Virtual Network (VNet) ・Azure Load Balancer ・Azure VPN Gateway
ストレージ	データの保存、管理、アクセスを行う	・Azure Disk Storage ・Azure Blob Storage ・Azure File Storage
データベース	クラウド上でのデータ保存とアクセスを可能にする	・Azure Cosmos DB ・Azure SQL Database

上記以外にも、**AIと機械学習、分析、IoT、セキュリティ、ID、開発者ツール**などのサービスカテゴリーも提供されています。
次の項で、コアサービスのなかの**コンピューティング**と**ネットワーク**について詳しく紹介します。

4. コンピューティングサービス

4.1. 仮想マシンとは

■仮想マシン（VM, Virtual Machine）とは
物理的なサーバーを通し、仮想環境に擬似的に再現したコンピューターのことです。
一般的にコンピューターは物理的な部品を備わっていますが、仮想マシンはそれらの機能をソフトウェアが担い、仮想化された空間でコンピューターとして機能します。

物理的なコンピューターが1台あれば、その中に複数の仮想マシンを構築することができます。複数の仮想マシンはそれぞれ独立したコンピューターとして利用できます。仮想マシンは物理的なコンピューターとは分離されており、物理的なコンピューターに影響を与えません。

仮想マシンの用途

・アプリケーションのデプロイや動作検証を実施
・開発用サーバーやテストサーバーとして活用
・ベータリリースなどの新しい OS を試験運用
・既存の OS のバックアップ
・組織で使用していない別の OS 環境でソフトウェアやアプリケーションの動きを確認
・ウイルス感染データへのアクセスや古い OS で古いアプリケーションの実行
・負荷の高いアプリケーションの運用　など

仮想マシンの特徴

・メリット
- コスト削減：物理的なコンピューター台数を減らせる
- 拡張性・柔軟性：物理環境より柔軟な構築が可能
- 可用性の向上：バックアップや移植が簡単のため、障害などによるダウンタイムを短縮できる

・デメリット
- 性能の低下：物理サーバーを借用するため性能・処理スピードに制限がある
- 専門性：構築や管理に専門技術が必要

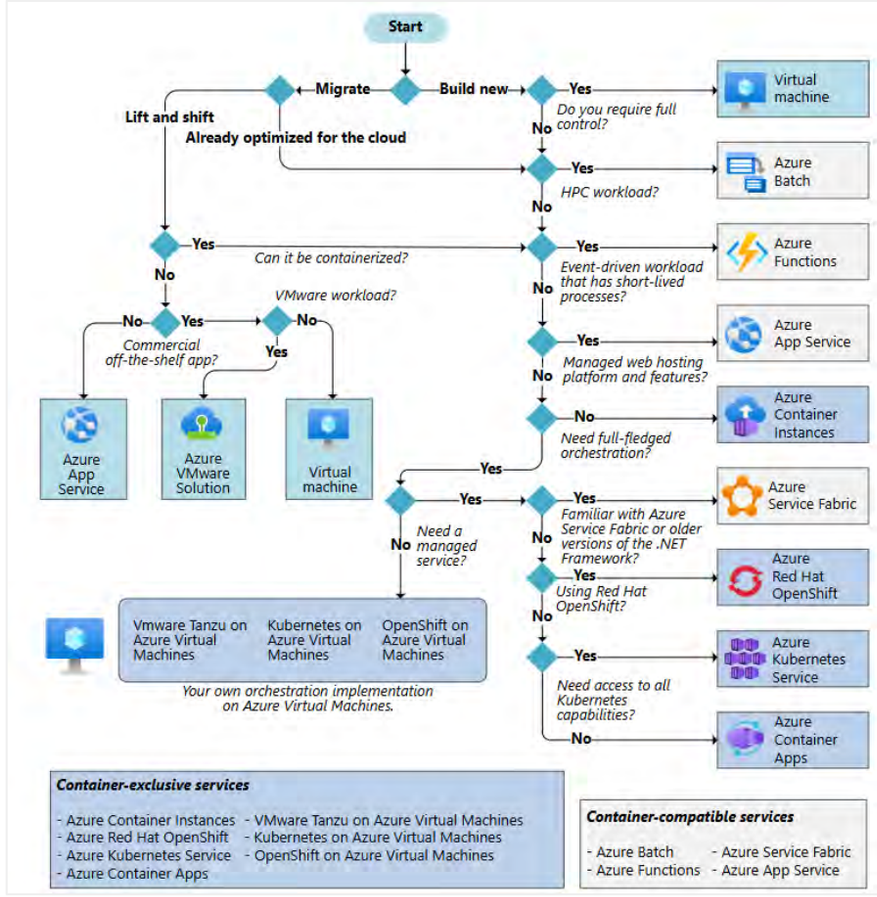
4.2. コンピューティングサービスの例

クラウドサービスの最大手3社はそれぞれ多数のコンピューティングサービスを提供しています。
組織は右の図のように、要件に合わせて利用するサービスを選択できます。

コンピューティングサービスのなかでも IaaS でのサービスが主要サービスとなっており、各社の IaaS における仮想マシンサービスは以下となります。

	サービス名
Microsoft Azure	Azure Virtual Machines
AWS（Amazon Web Services）	Amazon Elastic Compute Cloud（Amazon EC2）
GCP（Google Cloud Platform）	Google Compute Engine（GCE）

仮想マシンはネットワークと通しクラウド上で動作するため、ネットワークの構成が必須になります。次の項で Azure のネットワークサービスについて紹介します。



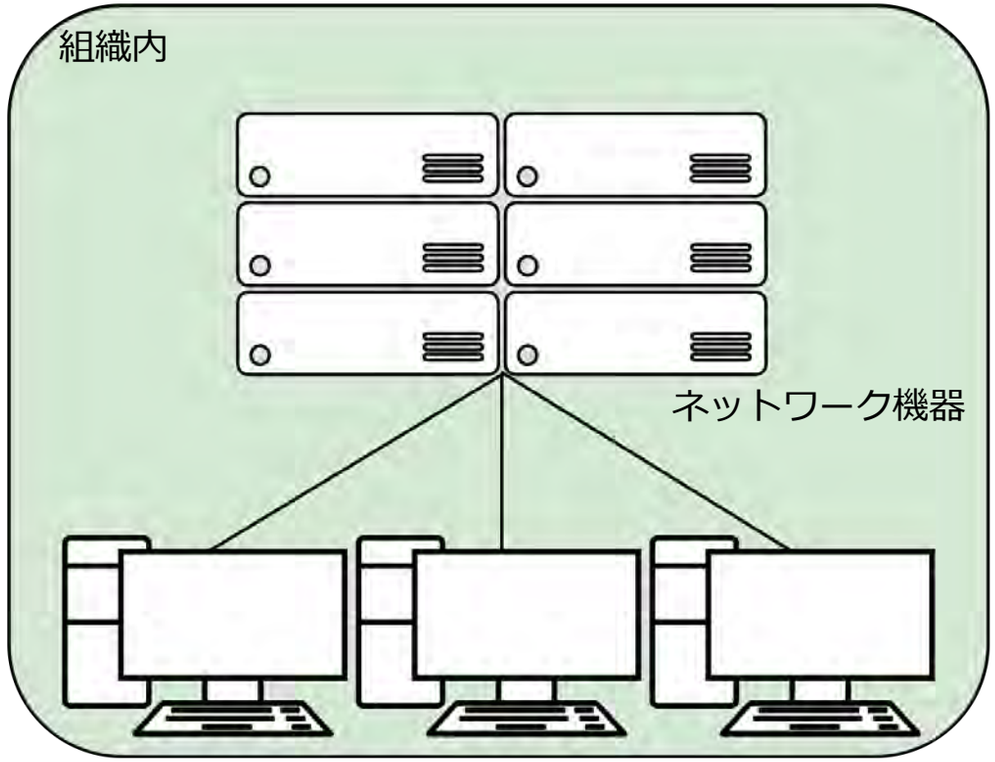
画像出典：Microsoft ドキュメント
「Azure コンピューティング サービスを選択する」

5. ネットワークサービス

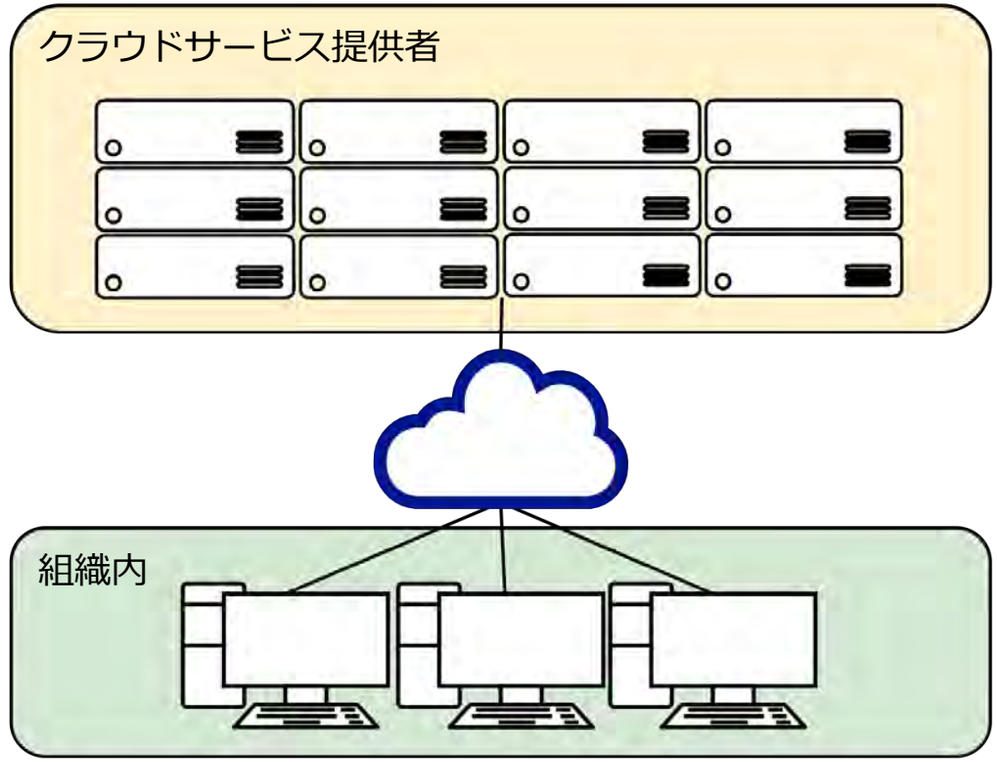
5.1. クラウドネットワークサービスとは

従来のオンプレミス環境でネットワークを構成するには、物理的なネットワーク機器を設置し、物理的な配線を行う必要がありました。そのため高度な知識を持つ人材、運用・管理のためのコストが必要です。

一方、クラウド化された Microsoft Azure の各種ネットワークサービスの場合、迅速かつ簡単にネットワークを構成することができます。



<オンプレミス>



<クラウド>

5.2. Microsoft Azure ネットワークサービスの種類

Microsoft Azure で提供されているネットワークサービスを機能で分類すると以下のようになります。

種類	主な機能	サービスの例
ネットワーク基盤	Azure のリソースにネットワーク接続を提供	・Azure Virtual Network ・Azure Private Link ・Azure NAT Gateway ・Azure DNS ・Azure Bastion
負荷分散とコンテンツ配信	アプリケーションとワークロードの管理、配布、最適化	・Azure Load Balancer ・Azure Application Gateway ・Azure Front Door
ハイブリッド接続	Azure のリソース間の通信をセキュリティで保護	・Azure VPN Gateway ・Azure ExpressRoute ・Azure Virtual WAN
ネットワーク セキュリティ	Web アプリケーションと IaaS サービスを DDoS 攻撃や悪意のあるアクターから保護	・Azure Firewall ・Azure Web Application Firewall
ネットワークの管理と監視	ネットワーク リソースを管理および監視	・Network Watcher ・Azure Network Function Manager

次のページから、Azure ネットワークの基本となるサービスや機能ついて詳細を説明します。

5.3. Azure Virtual Network（VNet）

■Azure Virtual Network（VNet）とは
Azure クラウド上で仮想ネットワークを構築・管理するサービスです。利用者は組織の要件に合わせた仮想ネットワークを自由に構築し、効率的に用途やアクセスレベルが異なるネットワーク空間を設定できます。

構築した仮想ネットワークは他ネットワークと論理的に分離されたプライベートな環境になります。
また、通信のフィルタリング機能を利用し、特定のトラフィックのみを許可または拒否することができます。つまり、送信元のIPアドレスやポート番号に基づいて、ネットワークのセキュリティを強化できます。

Azure Virtual Network の基本的な機能

・パブリック IP アドレス、プライベート IP アドレスの取得
・仮想ネットワーク構築、サブネットの分割
・他のネットワークへの接続

上記を含む、Azure のクラウドネットワークサービスに関わる機能について次のページから説明します。

5.4. VNet の機能① IP アドレスの取得

仮想マシンを VNet に接続することで、仮想マシンにパブリック IP アドレス（グローバル IP アドレス）とプライベート IP アドレス（ローカル IP アドレス）を割り当てることができます。

パブリック IP アドレスとプライベート IP アドレスの特徴を比較すると以下のようになります。

	概要	設定の要否	割り当て範囲	割り当て方法
パブリック IP	インターネット上で公開される IP アドレス	オプション	リージョンのアドレス範囲内	静的・動的
プライベート IP	仮想ネットワーク内での通信用 IP アドレス	必須	サブネットのアドレス範囲内	静的・動的

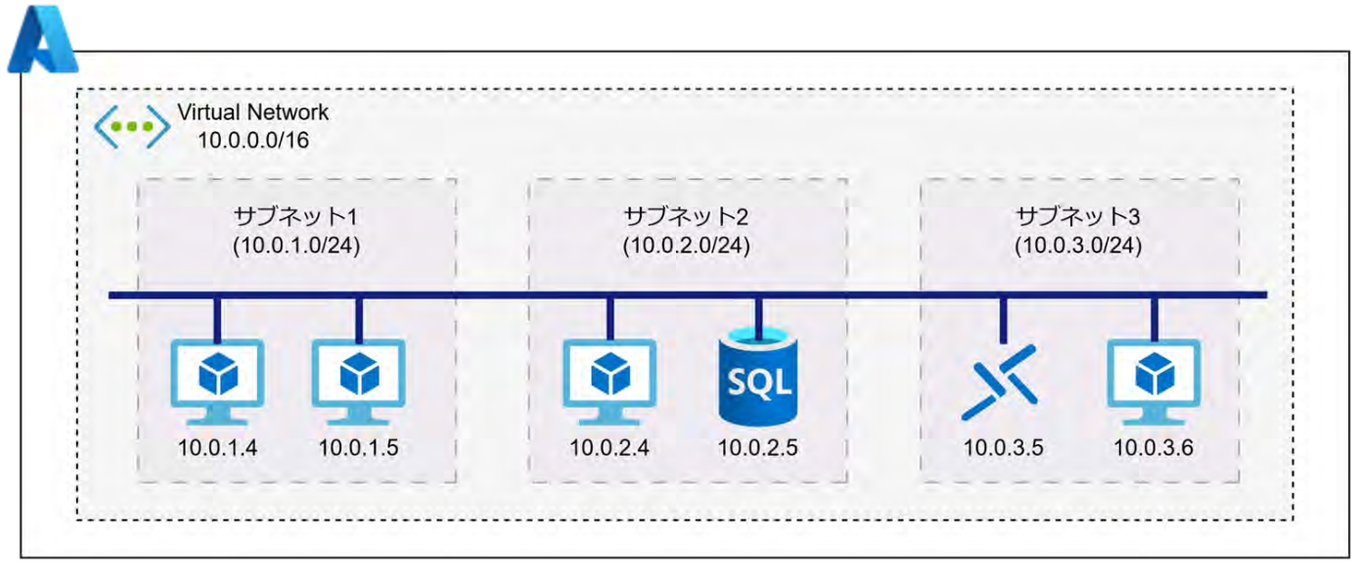
プライベート IP アドレスを使う理由

パブリック IP アドレス（グローバル IP アドレス）はインターネット上で共通し使用されているため、常に枯渇が危惧されています。外部ネットワークと接続しない仮想ネットワーク内ではプライベート IP アドレスを使用することで、IP アドレスを安定的に確保できます。

また、「外部ネットワークとの通信」と「仮想ネットワーク内での通信」で別の IP アドレスを利用することで、仮想ネットワーク内の通信のセキュリティ向上にも繋がります。

5.5. VNet の機能② サブネット分割

VNet には 1つ以上のアドレス空間を割り当て、それぞれのアドレス空間には 1つ以上のサブネットを配置できます。
個々のサブネットのプライベート IP アドレス範囲は VNet が持つアドレス空間から切り出されます。
Azure の各種リソースをサブネット内にデプロイすると、サブネットに紐づくプライベート IP アドレスが割り当てられ、ネットワークへの接続が可能になります。



アドレス空間とは

仮想ネットワーク全体で利用するプライベート IP アドレスの範囲を指します。仮想ネットワークを作成する際にカスタムで指定します。

サブネットとは

VNet の仮想ネットワークを1つ以上のセグメントに分割するもの（サブネットワーク）です。1つの VNet を複数のサブネットに切り分け、用途によって分離することができます。

5.6. VNet の機能③ 他のネットワークへの接続

VNet を通し、他の VNet やオンプレミスなど外部ネットワークへの接続が可能になります。どこに接続する必要があるかにより、必要な通信方式が異なります。

インターネットとの通信

VNet に接続している仮想マシンなどのリソースは、パブリック IP アドレスを設定していない場合でも、デフォルトでインターネットへの送信方向（アウトバウンド）の通信が可能です。(※2025年9月をもってデフォルトアウトバウンド通信は廃止となります)
ただし、デフォルトのままではインターネットからの受信方向（インバウンド）の通信は行えません。インターネットからの接続（インバウンド通信）が必要な場合は、VNet 内のリソースに**パブリック IP アドレス**を設定するか、**パブリックロードバランサー**を割り当てます。

クライアントコンピュータとの通信

個々のクライアント コンピューターから VNet へ通信を行う場合は、**P2S（ポイント対サイト）VPN 接続**で端末と VNet を接続します。
端末上の VPN クライアントから、VPN 内の VPN Gateway へ VPN 接続を要求することで通信ができます。

オンプレミスとの通信

VNet とオンプレミスで通信を行う場合は、**S2S（サイト間）VPN 接続**でオンプレミス環境と VNet を接続します。
仮想ネットワーク上のローカルネットワークゲートウェイにオンプレミスのグローバル IP アドレスとアドレス空間を指定して接続します。
利用にあたっては、オンプレミス側でグローバル IP アドレスと VPN デバイスが必要です。
ほかにも、通信キャリアが提供する閉域網または専用線を介した接続を行う Azure Express Route というサービスが用意されています。

他の VNet との通信

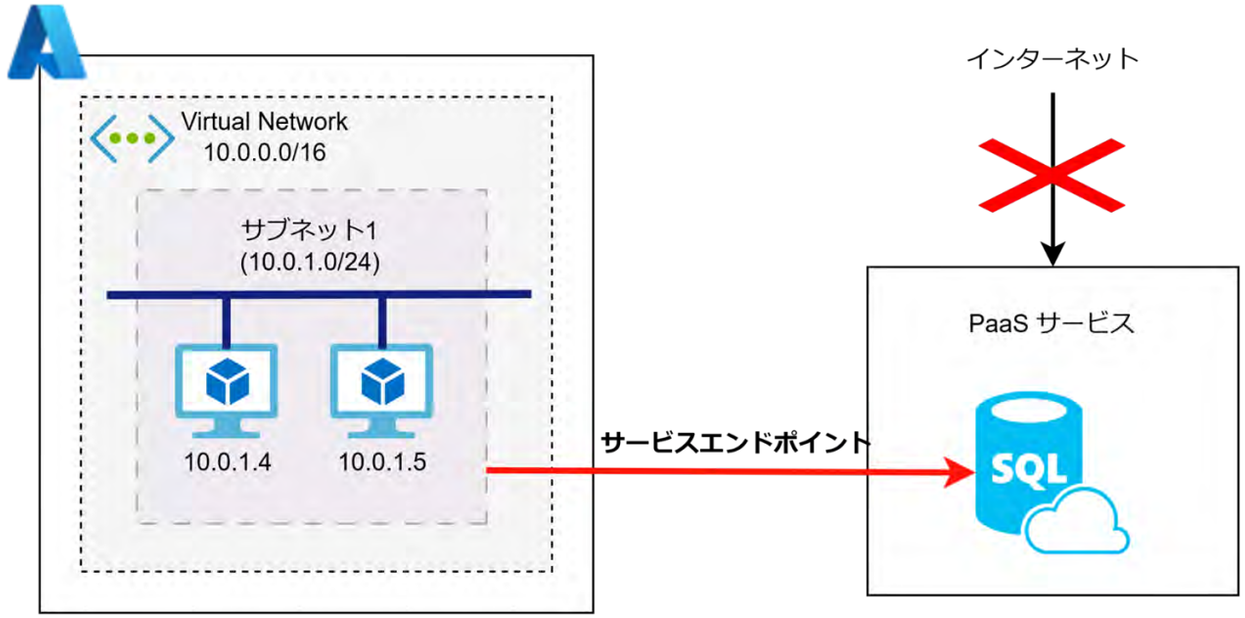
同じ VNet 内のリソースどうしは相互に通信できますが、異なる VNet リソースに接続する際は**S2S（サイト間）VPN 接続**や **VNet ピアリング**を構成して接続します。この場合リージョン間の通信はインターネットに出ることなく、Azure のバックボーンネットワーク経由で行われます。

5.7. Azure サービスエンドポイント

■ Azure サービスエンドポイントとは
仮想ネットワークから Azure の PaaS サービスに接続できるようにする機能です。

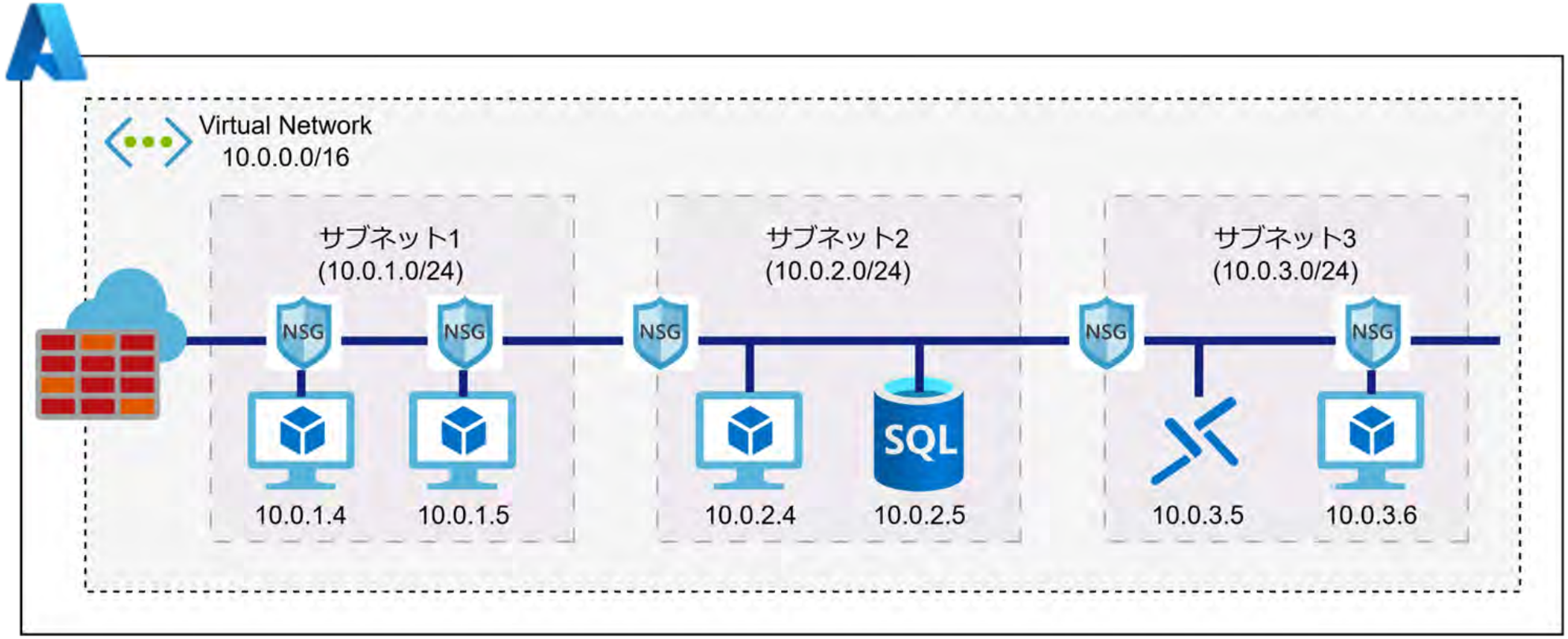
Azure の PaaS サービスは、インターネットからアクセス可能なパブリック IP アドレスを持っています。仮想ネットワークがインターネットへの接続を制限している場合、通常であれば PaaS への接続ができなくなってしまいます。

Azure サービスエンドポイントはこれらの PaaS サービスに対するインターネットからの接続を禁止し、アクセスを VNet 内の特定のサブネットからのみに制限します。PaaS サービスを使いながらも仮想ネットワーク自体はインターネットへの接続を許可しない状態を継続できるため、セキュリティ対策として使用されます。



5.8. Azure ネットワークセキュリティグループ（NSG）

■ Azureネットワークセキュリティグループ（NSG）とは
Azure 仮想ネットワーク上でファイアウォールのように機能するセキュリティサービスで、制御ルールを設定することで VNet 内の Azure リソースへのアクセスを制御します。
VNet のサブネットや仮想マシンのネットワークインターフェース（NIC）に適用でき、リソーストラフィックや仮想マシンの NIC 間の通信を制御します。類似したサービスには Azure Firewall があります。



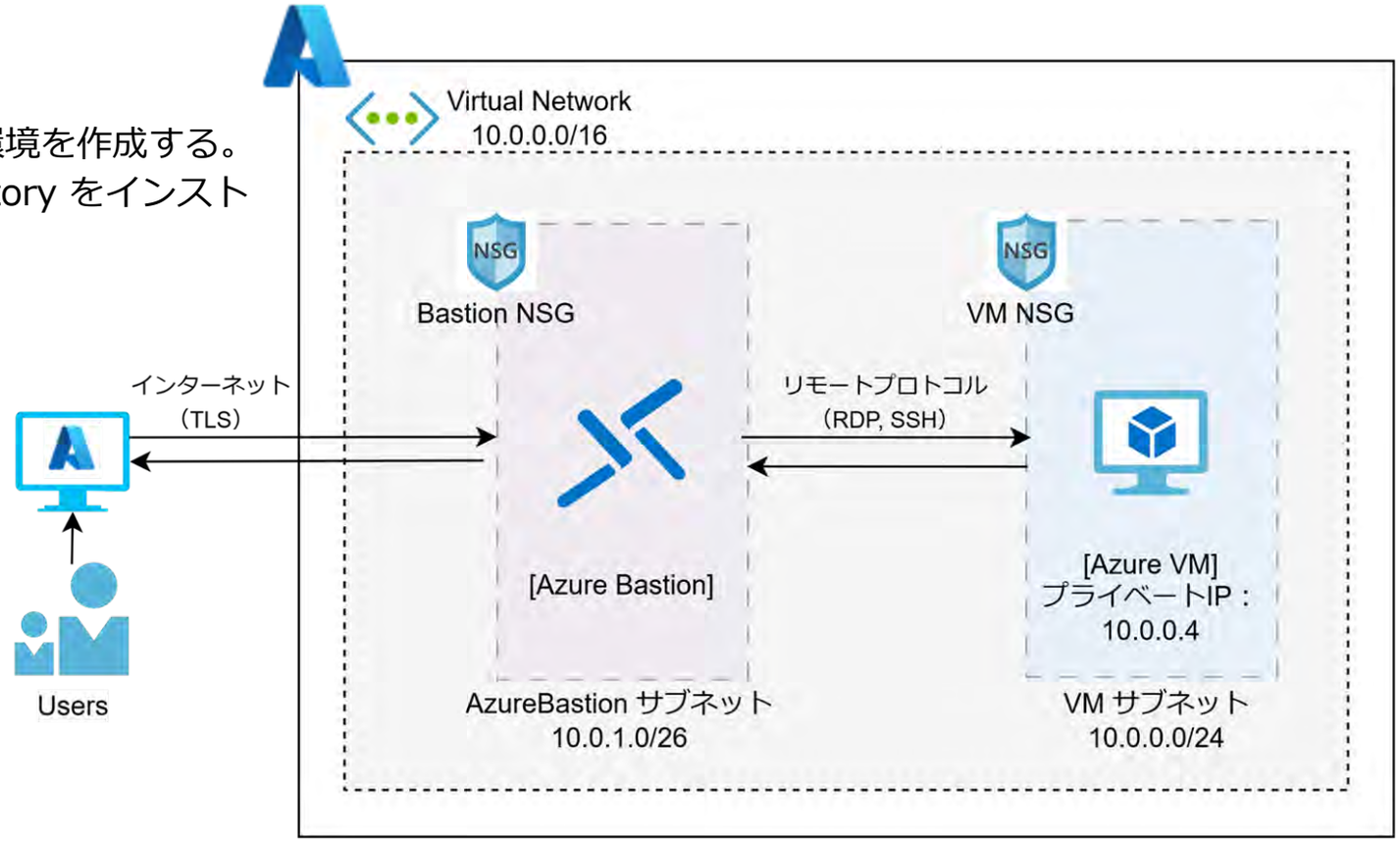
6. 基本的な Azure 環境構成

6.1. 基本的な Azure 環境構成と検討フロー

Azure の仮想ネットワーク環境構築に関する理解を深めるために、基本的な環境構成を例に構成時の検討事項とそのフローを確認します。本資料で説明する Azure の環境は、最終的に以下の構成になります。次のページから、以下の構成に辿り着くまでの検討フローを紹介します。なお、詳細な作成手順および設定値については割愛します。

構成シナリオ

会社の PC から Azure の仮想マシンに接続できる環境を作成する。
仮想マシンの OS は Windows とし、Active Directory をインストールするための環境を構築する。
なお、シンプルで基本的な構成にする。

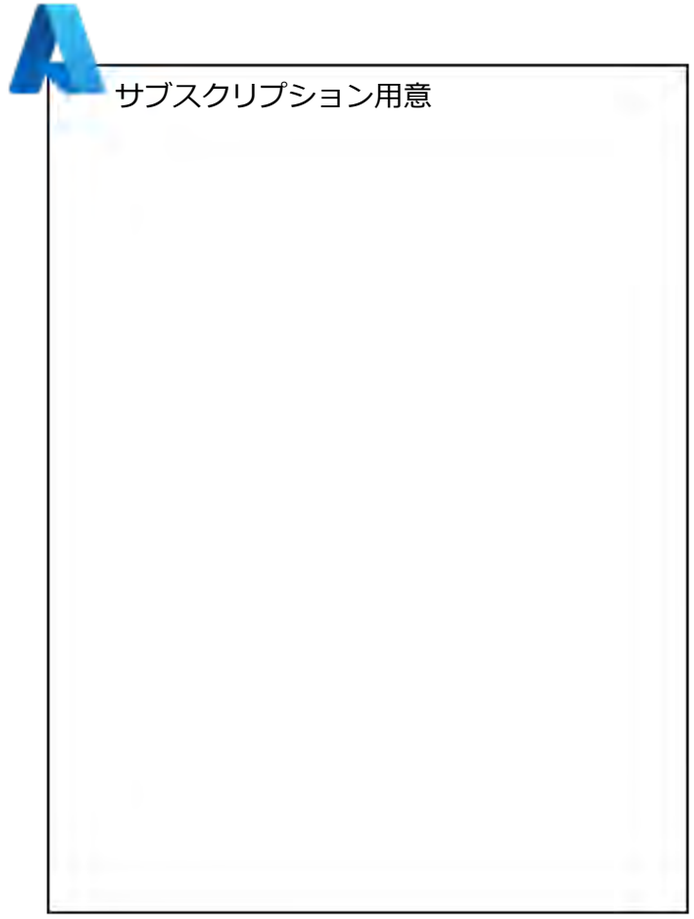


6.1. 基本的な Azure 環境構成と検討フロー

まずは基本的な構成で仮想ネットワークと仮想マシンを作成します。

作成手順

1. Azure ポータル（https://portal.azure.com/）にアクセスし、Azure アカウントでログインを行う
2. リソースグループを作成する
   a. サブスクリプションは既存のもの、または新規で作成する
   b. リソースグループの名称を設定する
   c. リソースグループのリージョンを選択する



検討事項

・サブスクリプション

Azure の課金やアクセス制御の範囲になるため、要件に応じて既存サブスクリプションの利用/新規作成を検討する。

・リージョン

データセンターとの距離によってパフォーマンスに多少の影響がある。
また、リージョンごとに料金が異なる。
必要に応じてマルチリージョンで冗長構成を考慮する。

6.1. 基本的な Azure 環境構成と検討フロー

作成手順

3. 仮想ネットワークを作成する
    a. メニューから「仮想ネットワーク」を選択し作成する
    b. 基本情報
        i. プロジェクトの詳細
        ii. インスタンスの詳細
    c. セキュリティ
    d. IP アドレス
        i. サブネットの追加
    e. タグ
    f. レビューと作成

検討事項

・IP アドレス

- アドレス空間の指定（=仮想ネットワークで使用するプライベート IP アドレスの範囲）

既存の仮想ネットワークやオンプレミスのネットワークと重複しない範囲を選ぶ。また、将来のリソース増加やサブネットの追加を見越して、広めの IP アドレス空間を確保する。（例: /24 で256 IP 確保）

- サブネットの追加

サブネットに配置予定のリソース要件や将来の拡張を考慮し、十分な IP アドレスを確保するとともに未割り当ての範囲も残しておく。

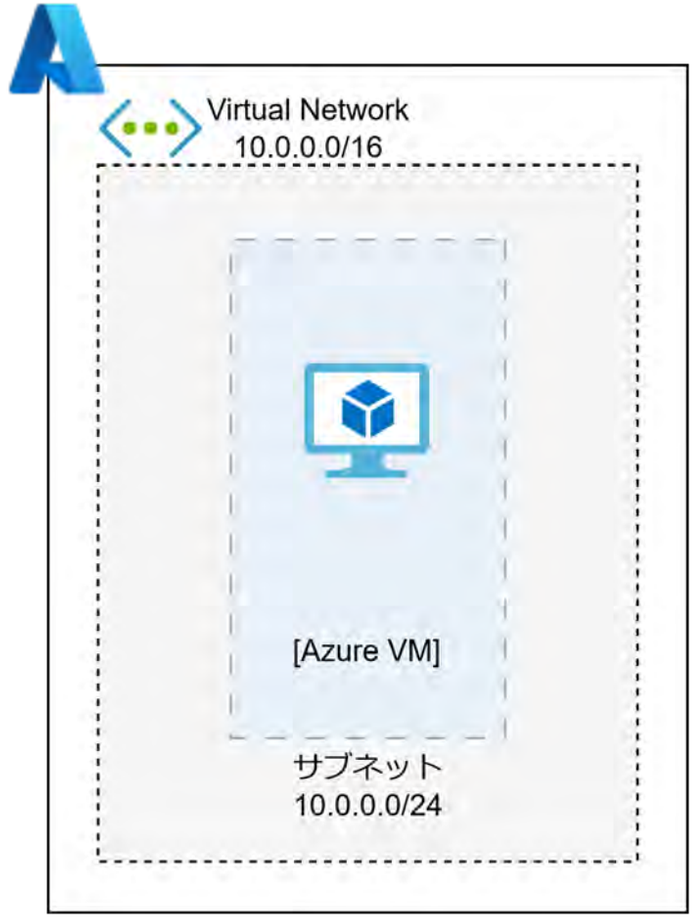
Azure の予約 IP アドレス（最初の4つと最後の1つ）に注意する。

異なるセキュリティ要件を持つリソースを別々のサブネットに分離する。

6.1. 基本的な Azure 環境構成と検討フロー

作成手順

4. リソースグループ内にリソース（仮想マシン）を作成する
    a. Marketplace から「仮想マシン」を選択し作成する
    b. 基本
        i. プロジェクトの詳細
        ii. インスタンスの詳細
        iii. 管理者アカウント
        iv. 受信ポートの規則



検討事項

・インスタンスの詳細

- リージョン

仮想ネットワークはリージョン単位で作成され、異なるリージョンのVMとは直接接続できないため、仮想ネットワークと同様のリージョンを選択する。

- 可用性ゾーン

可用性ゾーンをサポートするリージョンを選択する。

- イメージ

必要な機能や要件を満たす OS、アプリケーションを選択する。

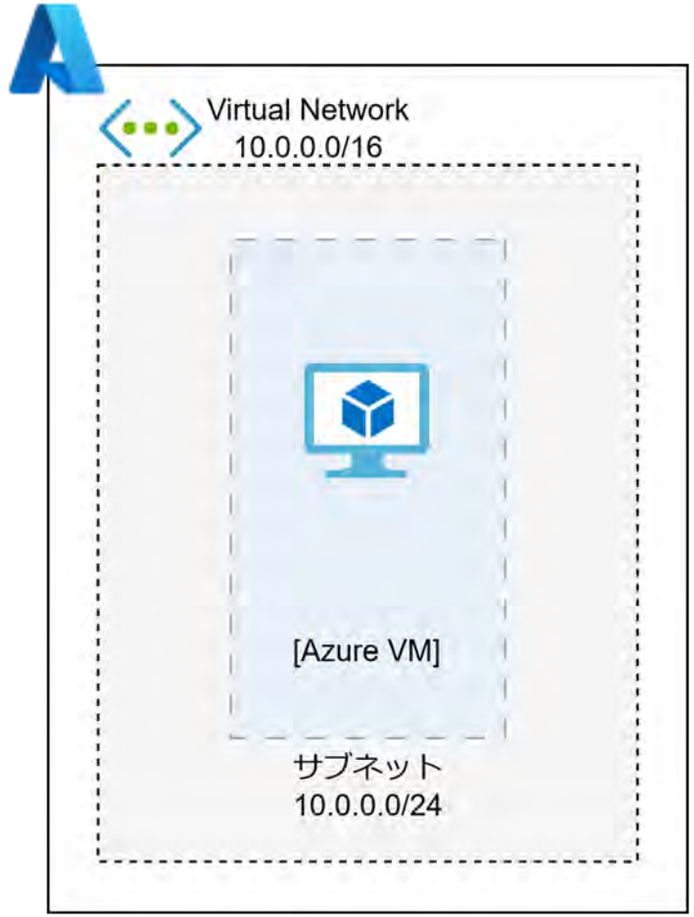
- サイズ

VMのサイズは、ワークロードの要件に適した処理能力、メモリ、記憶域容量などを基に選択する。サイズと OS に基づいて料金が請求される。

6.1. 基本的な Azure 環境構成と検討フロー

作成手順

4. リソースグループ内にリソース（仮想マシン）を作成する
    c. ディスク
        i. VMディスクの暗号化
        ii. OSディスク
        iii. データディスク



検討事項

・ディスク

- OS ディスク

OS システムの起動に必要なディスクで、パフォーマンスやコストに応じた種類と容量を選択する。

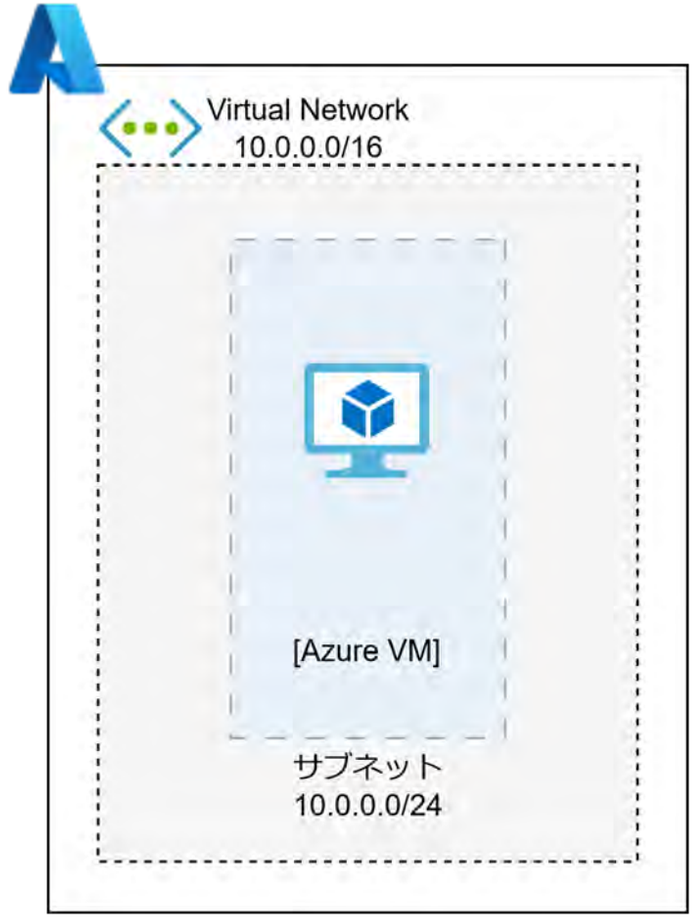
- データディスク

アプリケーションデータやログを保存するためのディスクで、用途に応じた種類・容量を選択する。

6.1. 基本的な Azure 環境構成と検討フロー

作成手順

4. リソースグループ内にリソース（仮想マシン）を作成する
    d. ネットワーク
        i. ネットワークインターフェース
        ii. 負荷分散
    e. 管理
    f. 監視
    g. 詳細
    h. タグ
    i. 確認および作成



検討事項

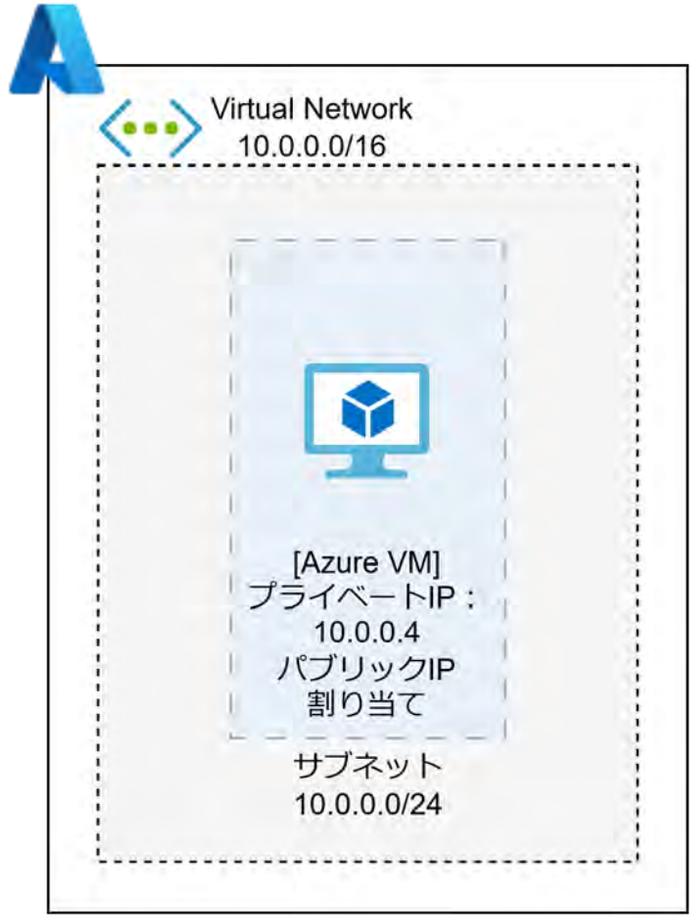
・負荷分散

選択した負荷分散オプションに応じて、VM のトラフィック管理が行われる。

6.1. 基本的な Azure 環境構成と検討フロー

作成手順

4. 仮想マシンへ IP アドレスを割り当てる
    a. 仮想マシンのネットワークインターフェース（NIC）に IP 構成を行う
        i. プライベート IP アドレスの設定
        ii. パブリック IP アドレスの設定
5. RDPを通し、仮想マシンへの接続を確認する



検討事項

構築シナリオに合わせて以下を検討する。

・プライベート IP アドレスの設定（=仮想マシンの通信のために必要な IP アドレスの設定）
Azure Bastion* 経由で RDP 接続を行う場合、NSG や Firewall で許可する IP を明確にするため、割り当てを [静的] にして、プライベート IP アドレスを指定する。
※不要なインターネット公開を防ぐため、パブリック IP は設定不要。
※Azure Bastion については後続で説明

・パブリック IP アドレスの設定
外部ネットワークから VM へ RDP でアクセスする場合は、パブリック IP アドレスを VM に割り当てる。
※ SKU [Basic] は利用不可のため、[Standard] を選択する。

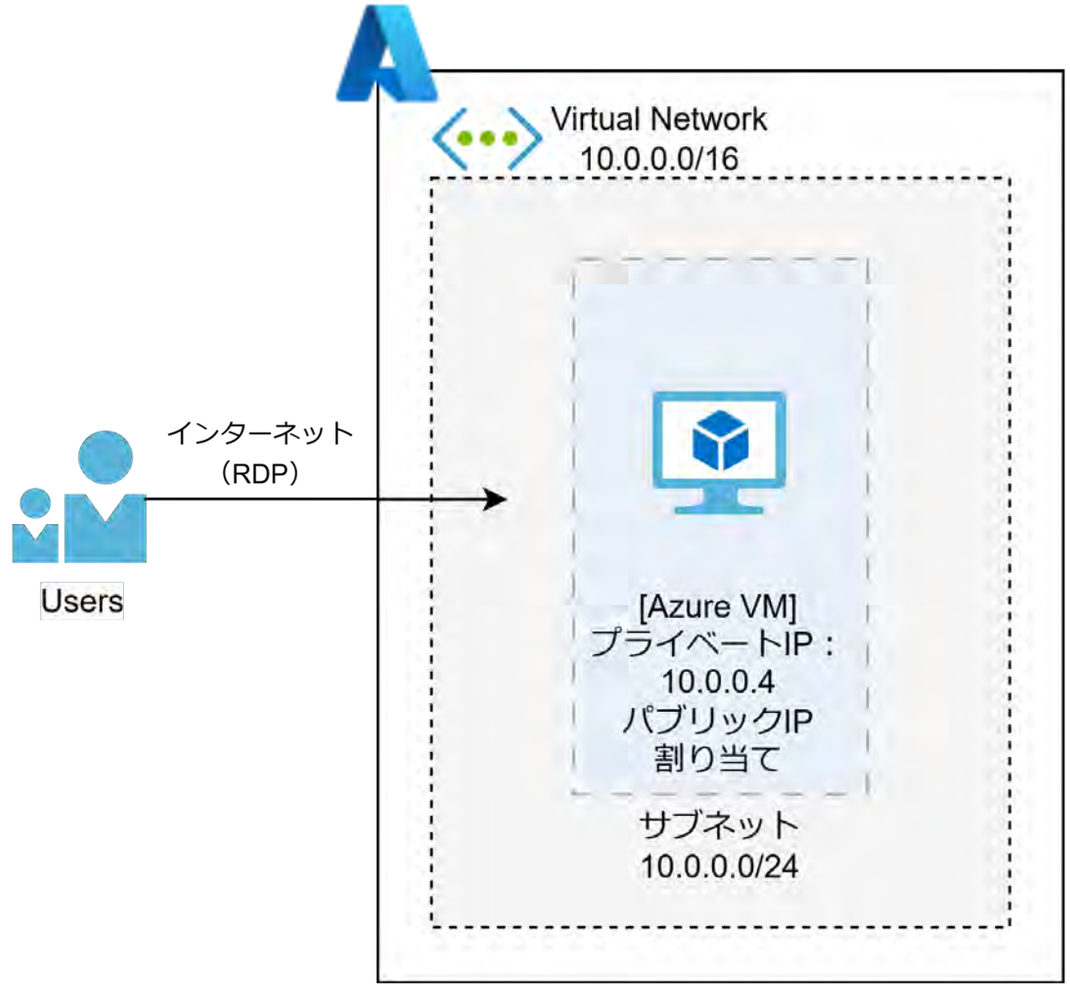
6.1. 基本的な Azure 環境構成と検討フロー

ここまでの作業で、まずは仮想ネットワーク内の仮想マシンへ接続できるようになりました。

■現状の設定
・仮想ネットワーク内に1つのサブネット
・サブネットに仮想マシンを配置
・仮想マシンにパブリック IP アドレス割り当て
・インターネットから RDP を用いり仮想マシンに直接接続
・接続についてセキュリティ対策はなし

このままではインターネットからの攻撃や不正利用が発生する可能性があるため、仮想マシンに安全に接続するためのセキュリティ対策を行う必要があります。

セキュリティを考慮した設定方法は数多くありますが、次のページから以下の 2つを紹介します。
① ネットワークセキュリティグループ（NSG）の設定
② Azure Bastion の利用

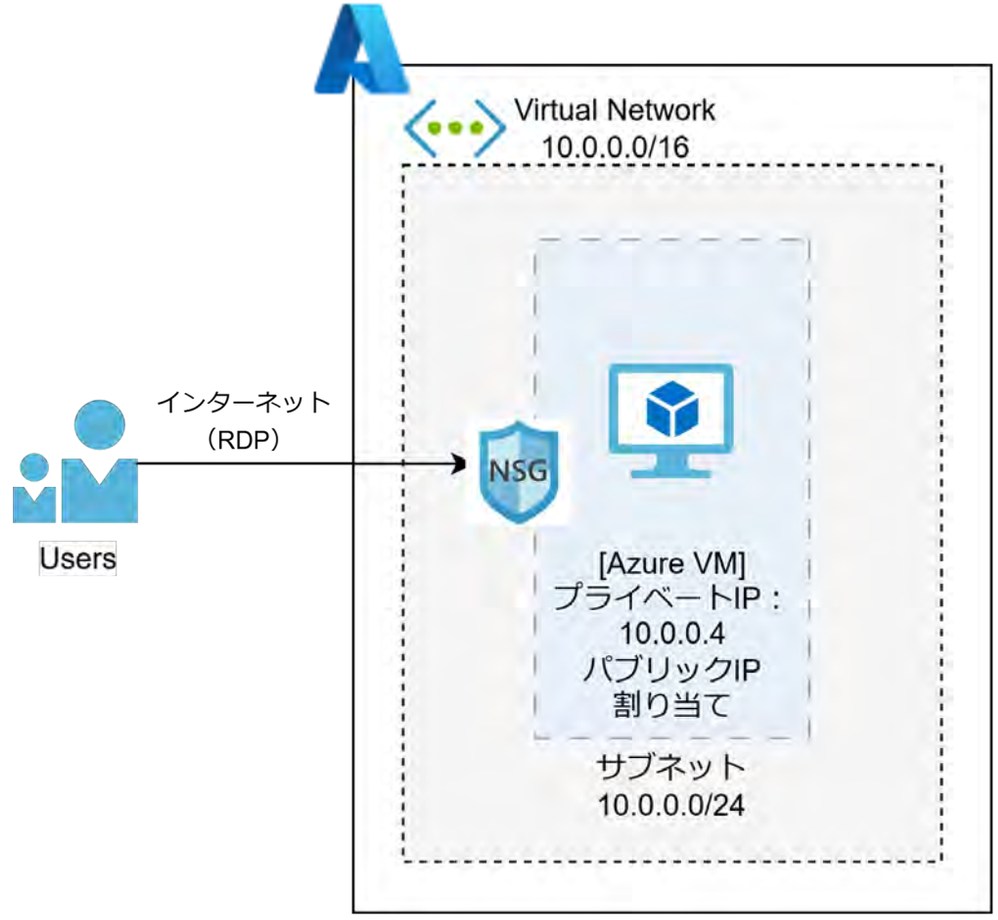


6.1. 基本的な Azure 環境構成と検討フロー

セキュリティ対策　その1：ネットワークセキュリティグループ（NSG）の設定
送信元のパブリック IP アドレスが固定されている（静的）場合、接続する IP アドレスを NSG で絞ることでセキュリティ性を高めることができます。

作成手順

1. NSG を作成する
    a. 基本
        i. プロジェクトの詳細
        ii. インスタンスの詳細
    b. タグ
    c. 確認および作成
2. NSG の受信セキュリティ規則でRDP接続用のルールを作成する
3. NSG とサブネットを関連づける
    a. 仮想ネットワーク
    b. サブネット
4. 指定した IP アドレスから、RDP を通し仮想マシンへの接続を確認する



検討事項

・受信セキュリティ規則 - ソースポート範囲
仮想マシンへ接続する方法を RDP にする場合、RDP を利用できるパブリック IP アドレスを制御する。

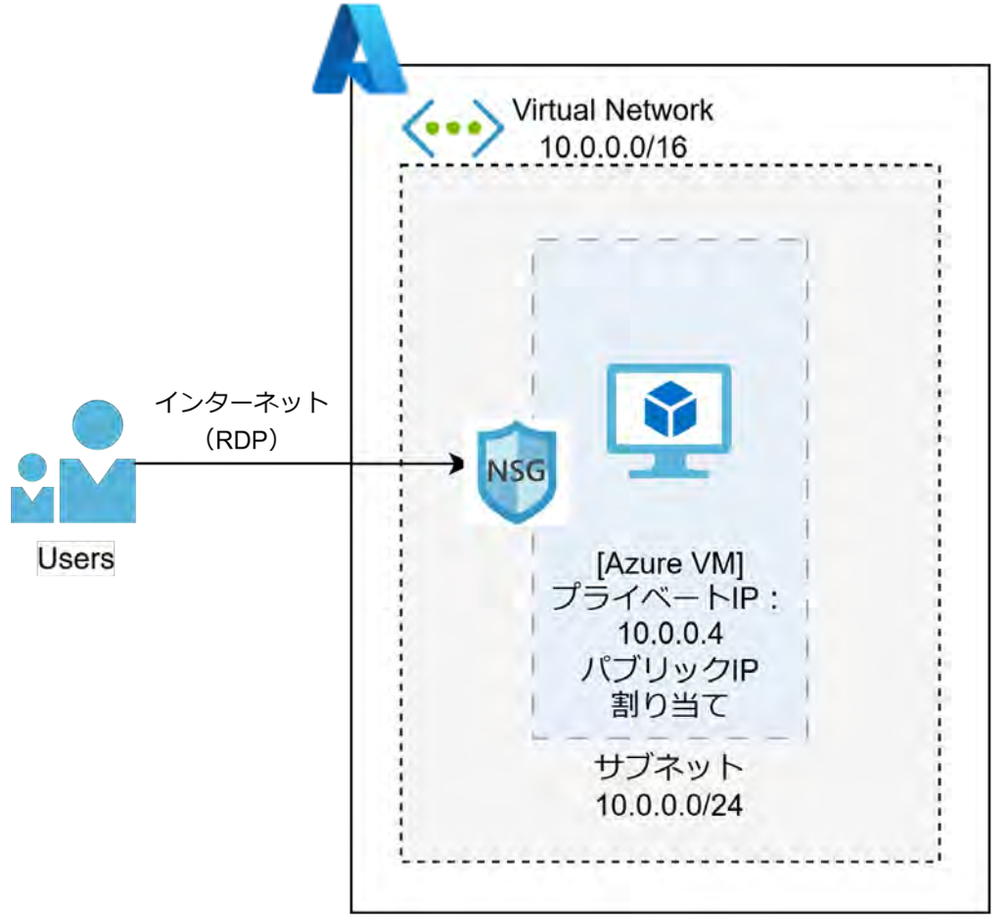
6.1. 基本的な Azure 環境構成と検討フロー

ネットワークセキュリティグループ（NSG）を設定し、アクセスできる IP アドレスを制限するセキュリティ対策を行いました。

■現状の設定
・仮想ネットワーク内に1つのサブネット
・サブネットに仮想マシンを配置
・仮想マシンにパブリック IP アドレス割り当て
・インターネットから RDP を用いり仮想マシンに直接接続
・仮想マシンに接続できるパブリック IP アドレスを NSG を通して制御

NSG は IP アドレスやポート番号などで設定したルールに従って仮想マシンへのアクセスを制御します。このような制御は仮想マシンへのアクセスを**送信元のパブリック IP アドレスが静的**な場合に適しています。
例えば、オフィスのネットワークを利用して仮想マシンにアクセスする場合などです。しかしクラウドにおいてこのような利用は理想的ではありません。

また、仮想マシンにパブリック IP アドレスが割り当てられたこのような環境はインターネットからの攻撃リスクがあり**推奨されません**。
そのため、安全に仮想マシンへアクセスするために次で紹介する Azure Bastion のような踏み台サーバーの機能を用意するのが一般的です。

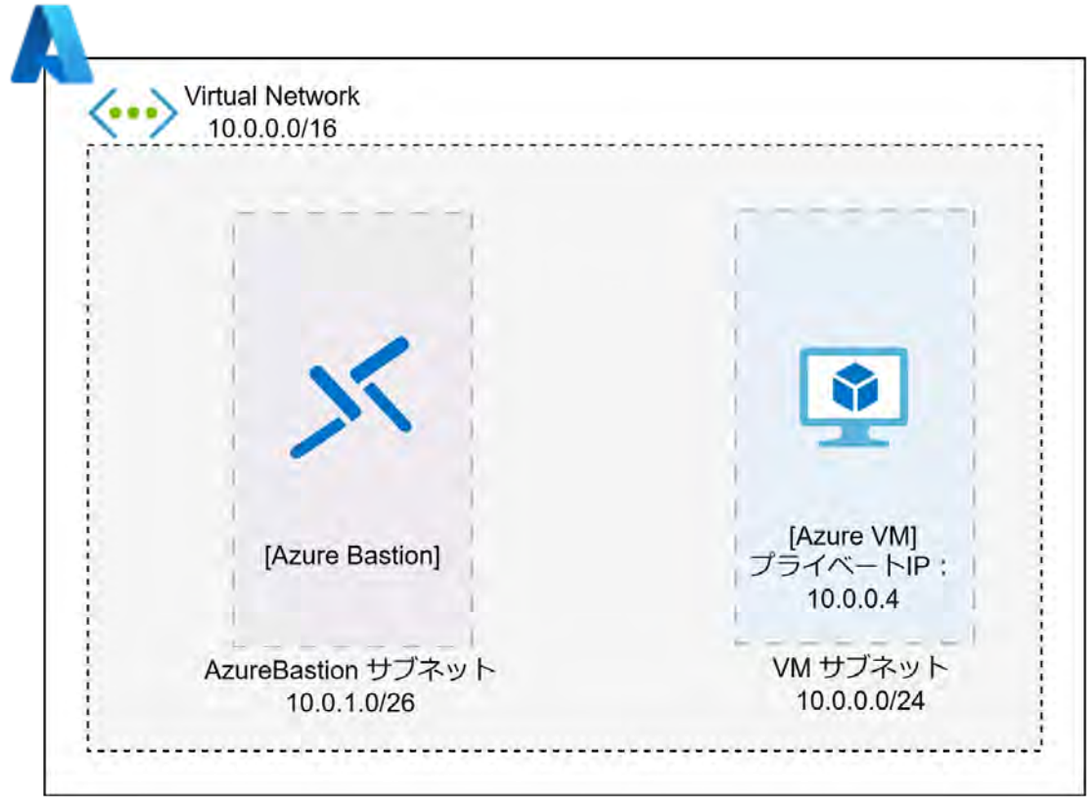


6.1. 基本的な Azure 環境構成と検討フロー

セキュリティ対策　その2：Azure Bastion の利用
仮想マシンのパブリック IP アドレスや RDP/SSHポートを公開せず仮想マシンに接続したい場合に活用できる設定方法です。

作成手順

1. 仮想ネットワーク内に Azure Bastion 専用のサブネットを作成する
    a. サブネットの目的：「Azure Bastion」を指定
    b. IPv4 アドレスの範囲
2. 仮想ネットワーク内にリソース（Bastion）を作成する
    a. 基本
        i. プロジェクトの詳細
        ii. インスタンスの詳細
        iii. 仮想ネットワーク構成
        iv. パブリック IP アドレス
    b. タグ
    c. 確認および作成



検討事項

・インスタンスの詳細 - レベル
Azure Bastion には複数の SKU（サービスレベル）があり、
それぞれ異なる機能を提供するため、要件に応じたレベルを選択する。

6.1. 基本的な Azure 環境構成と検討フロー

作成手順

3. Azure Bastion のサブネットに NSG を作成する
    a. 基本
        i. プロジェクトの詳細
        ii. インスタンスの詳細
    b. タグ
    c. 確認および作成
4. NSG の受信セキュリティ規則にルールを作成する
5. NSG の送信セキュリティ規則にルールを作成する
6. Azure Bastion の NSG とサブネットを関連づける
    a. 仮想ネットワーク
    b. サブネット

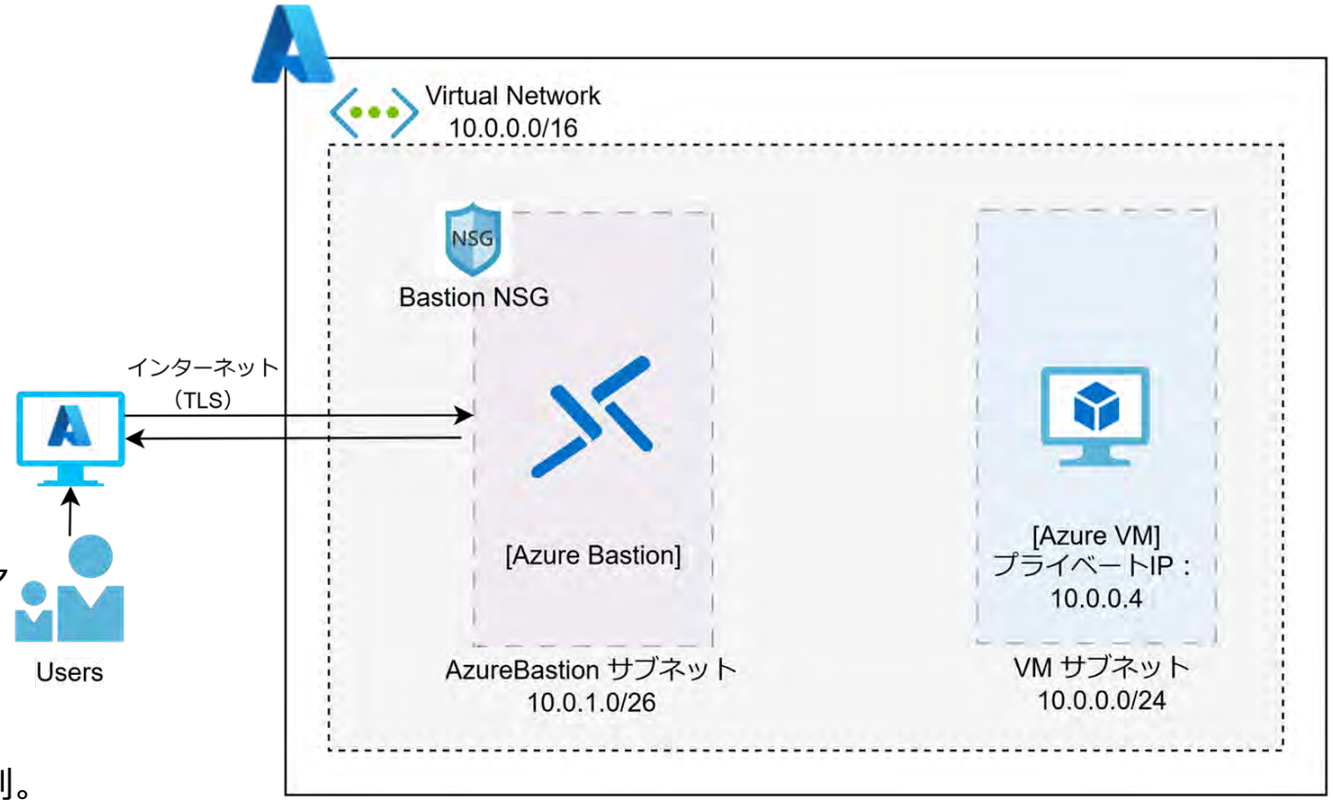
検討事項

・受信セキュリティ規則

Bastion へのユーザーアクセスを許可し、外部からの不正アクセスを防ぐための規則。（例: ポート 443 を許可）
要件に合わせて設定する。

・送信セキュリティ規則

Bastion から VM へ、必要な通信のみを許可するための規則。
（例: ポート 3389 / 22 を許可）
要件に合わせて設定する。

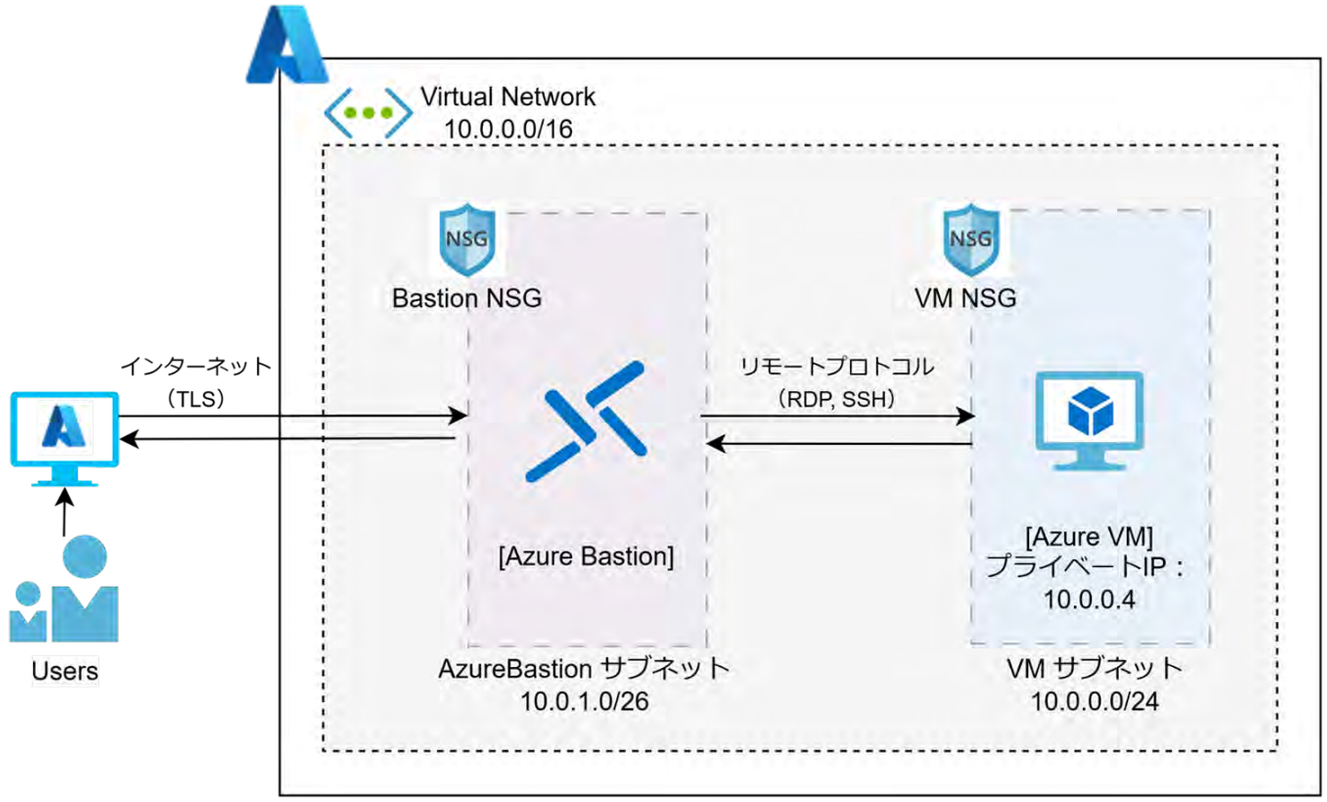


※推奨 NSG 参照：Microsoft ドキュメント
「NSG アクセスと Azure Bastion を使用する」

6.1. 基本的な Azure 環境構成と検討フロー

作成手順

7. 仮想マシン のサブネットに NSG を作成する
    a. 基本
        i. プロジェクトの詳細
        ii. インスタンスの詳細
    b. タグ
    c. 確認および作成
8. NSG の受信セキュリティ規則にルールを作成する
9. NSG の送信セキュリティ規則にルールを作成する
10. 仮想マシンの NSG とサブネットを関連づける
    a. 仮想ネットワーク
    b. サブネット
11. Azure Bastion を通し仮想マシンへの接続を確認する



検討事項

・受信セキュリティ規則

VM への必要な通信を許可し、不正アクセスを防ぐための規則。（例: RDP/SSH やアプリケーション通信）
要件に合わせて設定する。

・送信セキュリティ規則

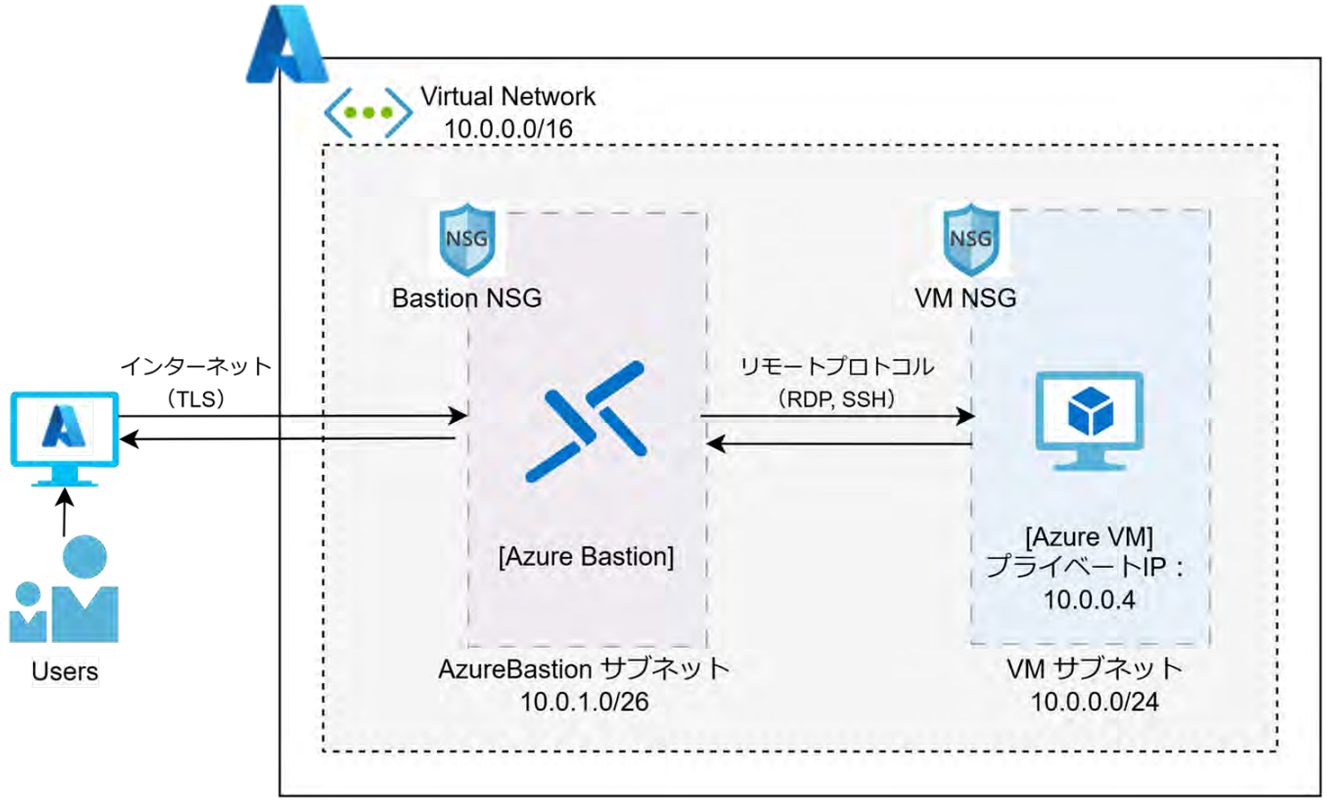
VM から外部リソースへの通信を制御し、必要な通信のみを許可するための規則。要件に合わせて設定する。

6.1. 基本的な Azure 環境構成と検討フロー

ここまでの作業で、安全に仮想ネットワーク内の仮想マシンへ接続できるようになりました。

■現状の設定
・仮想ネットワーク内に2つのサブネット
・各サブネットに仮想マシンと Azure Bastion を配置
・仮想マシンにはプライベート IP アドレスのみ割り当て
・Azure ポータルから仮想マシンに接続
・Azure Bastion が踏み台サーバーの役割をし、Bastion から仮想マシンへ直接接続

Azure Bastion を利用した環境構築は、仮想マシンにパブリック IP アドレスを割り当てたくない場合や、インターネットからの直接アクセスを避けたい場合に有効です。



6.2. Azure Bastion

[6.1. 基本的な Azure 環境構成と検討フロー] にて、仮想マシンに接続する際のセキュリティ向上対策として Azure Bastion を紹介しました。Azure Bastion について説明します。

■Azure Bastion とは
Azure のフル マネージド PaaS サービスで、仮想ネットワークに構築した仮想マシンに安全に接続する機能を提供します。

特徴

・踏み台サーバー（ジャンプサーバー）の役割
Azure ポータルから TLS 経由で（または RDP/SSH を介して）仮想マシンへ直接 RDP/SSH 接続できる

・仮想マシンのパブリック IP アドレスが不要
プライベート IP アドレス経由で接続するため、接続先となる仮想マシンにパブリック IP アドレスを割り当てる必要がない

・セキュリティリスクの軽減
RDP/SSH 接続は TLS で保護され、仮想マシンの ポートを外部に公開しないため、セキュリティリスクの軽減に繋がる

メリット

・デプロイまでかかる時間が短い
・セキュリティ対策
・アクセス元や時間を制限できる
・操作ログを確認できる

デメリット

・サービスの立ち上げに多少の時間を要する
・利用料金が比較的高い