

DP-300

Microsoft Azure

SQL ソリューションの管理

Day 2 – (3) セキュリティ

# DP-300 ラーニングパス



コース

Microsoft Azure SQL ソリューションの管理

- 1 Azure データベース管理の概要
- 2 データプラットフォーム リソースの計画と実装
- 3 データベース サービスにセキュリティで保護された環境を実装する
- 4 Azure SQL で運用リソースを監視および最適化する
- 5 Azure SQL でのクエリ パフォーマンスを最適化する
- 6 Azure SQL のデータベース タスクを自動化する
- 7 高可用性とディザスター リカバリーの環境を計画して実装する

2日目



## データベース サービスにセキュリティで保護された環境を実装する

3 時間 • ラーニング パス • 3 モジュール

中級

データ アナリスト

データ エンジニア

データベース管理者

Azure

Azure SQL データベース

SQL Server

認証と認可のための SQL Server ベースのオプションに加え、Azure SQL データベースをセキュリティで保護するための Azure オプションを実装します。暗号化、ファイアウォール、高度な脅威保護について説明します。

# ラーニングパス3

- DB管理者の認証: Entra ID認証、SQL認証、Windows認証
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- ファイアウォール規則
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする

# ラーニングパス3

- DB管理者の認証: Entra ID認証、SQL認証、Windows認証
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- ファイアウォール規則
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする

# データベース管理者の認証（本人確認）

- Azure SQL Database / Azure SQL Database Managed Instanceの場合
  - 「SQL認証」または「Entra認証」を使用
- SQL Server on Azure VMの場合
  - 「SQL認証」または「Windows認証」を使用
  - ※SQL Server 2022以降では「Entra ID認証」も利用可能

<https://learn.microsoft.com/ja-jp/azure/azure-sql/virtual-machines/windows/security-considerations-best-practices?view=azuresql#microsoft-entra-authentication>

<https://learn.microsoft.com/ja-jp/azure/azure-sql/database/logins-create-manage?view=azuresql#authentication-and-authorization>

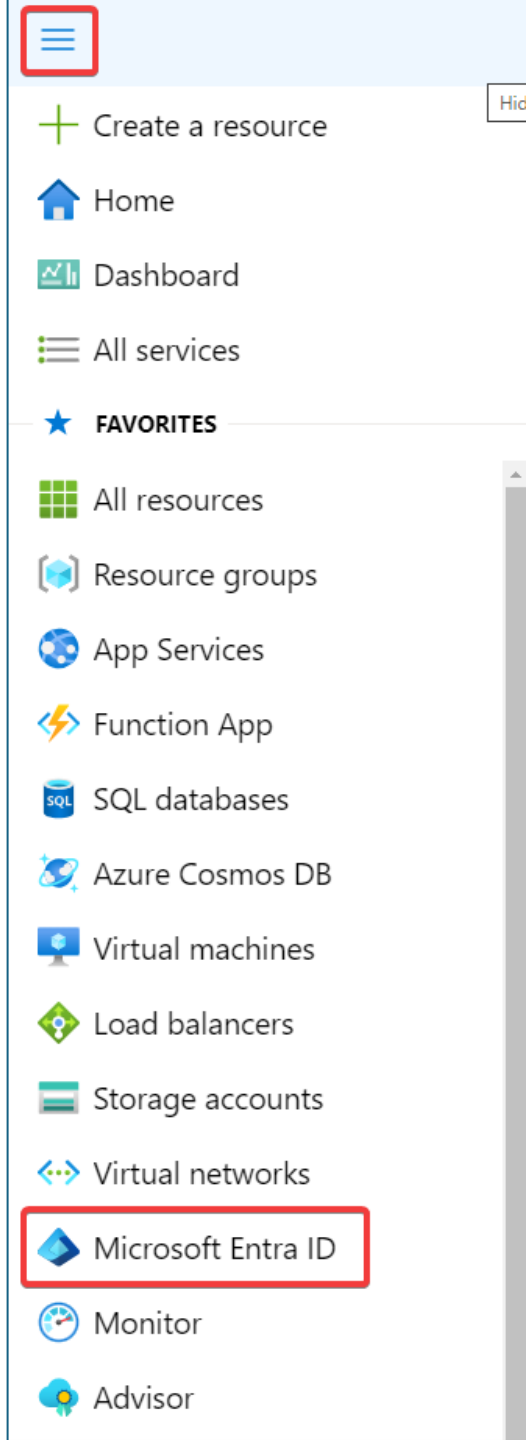
<https://learn.microsoft.com/ja-jp/azure/azure-sql/virtual-machines/windows/ways-to-connect-to-sql?view=azuresql>

# ラーニングパス3

- DB管理者の認証: **Entra ID認証**、SQL認証、Windows認証
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- ファイアウォール規則
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする

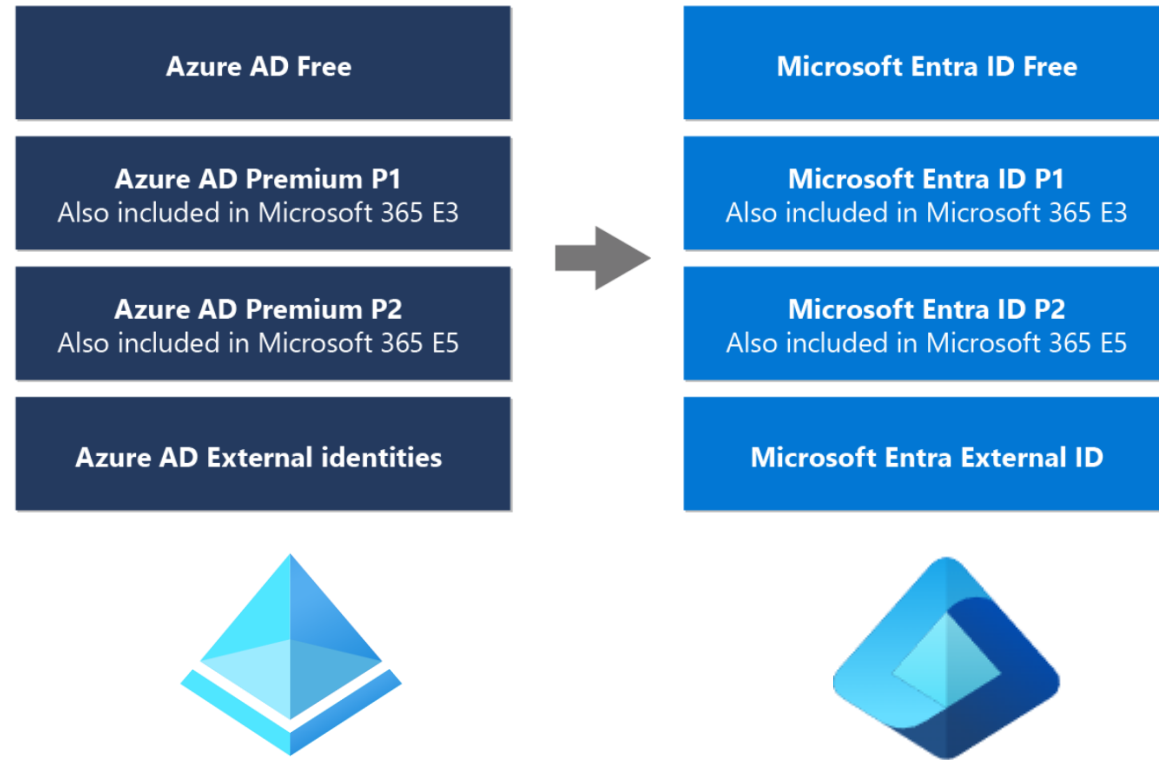


# Microsoft Entra IDとは？ (旧 Azure Active Directory)





2023/7/11～、Azure Active Directory (Azure AD) は「Entra ID」に名称変更（リブランディング）。ただし、機能・料金には変更はない。



旧名称「Azure Active Directory」（Azure AD）は  
新名称「Entra ID」と読み替えてください。

<https://mitomoha.hatenablog.com/entry/2023/08/05/024849>

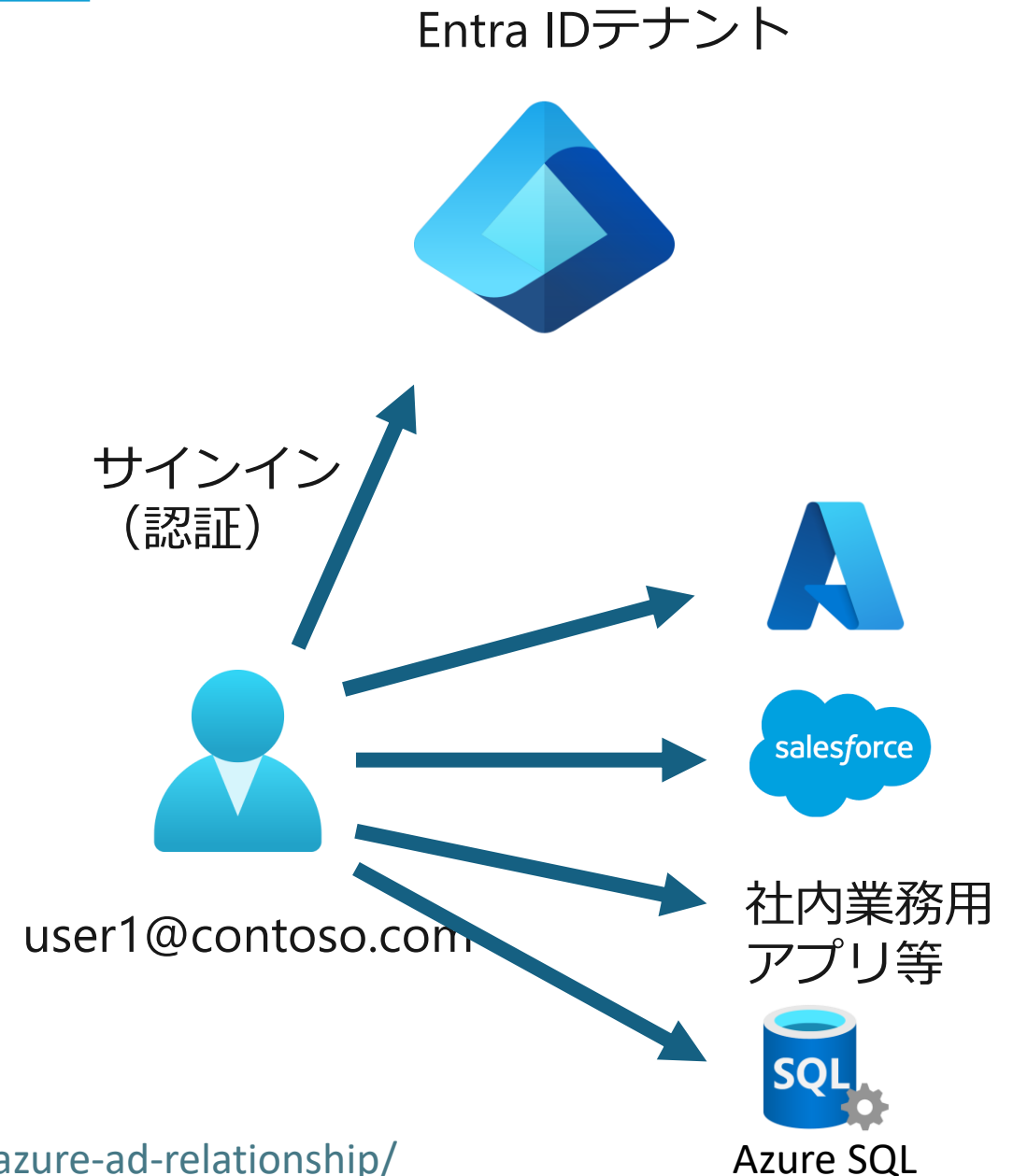
<https://learn.microsoft.com/ja-jp/azure/active-directory/fundamentals/new-name>

<https://news.microsoft.com/ja-jp/2023/07/12/230712-azure-ad-is-becoming-microsoft-entra-id/>

# Microsoft Entra ID とは

Identity and Access  
Management (IAM)

- クラウドベースの「**IDおよびアクセス管理**」サービス
- ユーザーIDなどを一元管理する**認証基盤**
- Microsoft Azure、Microsoft 365などへのサインイン（**ユーザー認証**）で利用される
- サードパーティ製のクラウドアプリ（Salesforce、Dropbox、ServiceNowなど）へのサインインでも利用できる
- ユーザーが開発した独自の業務アプリなどへのサインインでも利用できる
- 一度サインインすれば、いろいろなサービスやアプリにアクセスできる（**シングルサインオン**）



オンプレ資産と  
IDの一元管理



Active Directory  
Domain Service  
(AD DS)



Entra ID  
Connect

ID同期



Entra ID

クラウドベースの  
認証基盤

オンプレの  
アプリへの  
アクセス



Entra ID  
アプリケーション プロキシ



Microsoft Entra  
Domain Services

クラウドへの  
アプリ移行



条件付きアクセス

アプリへの  
アクセス制御

ユーザー  
本人確認



Entra ID  
MFA



セキュリティの  
既定値 (群)

無料のMFA・  
セキュリティ設定

ヘルプデスクの  
コスト削減



セルフサービス  
パスワードリセット



Identity Protection

IDに関する  
リスクを低減

必要な時のみ  
権限を付与



Privileged Identity Management



アクセスレビュー

不要な権限を  
取り除く

権限

# Azure SQLのEntra認証

- Microsoft Entra ID を使用して認証する方式
- Azure SQL Database / Azure SQL Database Managed Instance: 「SQL サーバー」作成時に、認証方式として「Entra認証」を選択し、データベース管理者のユーザーとしてEntra IDユーザーを指定する
- SQL Server on Azure VM: VMの「セキュリティ構成」画面で、認証方式として「Entra認証」を有効化し、データベース管理者のユーザーとしてEntra IDユーザーを指定する
- 接続時、SSMSやAzure portalで「Entra認証」を選択する（このときにまだEntra IDにサインインしていない場合、Webブラウザーが開き、Entra ID認証画面が表示される）

■ Azure SQL Databaseの「SQLサーバー」作成時の、Entra ID認証方式の選択と、Entra IDユーザーの選択

Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

[Home](#) > [SQL databases](#) > [Create SQL Database](#) >

Create SQL Database Server

Microsoft

Authentication

Azure Active Directory (Azure AD) is now Microsoft Entra ID. [Learn more](#)

Select your preferred authentication methods for accessing this server. Create a server admin login and password to access your server with SQL authentication, select only Microsoft Entra authentication [Learn more](#) using an existing Microsoft Entra user, group, or application as Microsoft Entra admin [Learn more](#) , or select both SQL and Microsoft Entra authentication.

Authentication method

☒ Use Microsoft Entra-only authentication

☐ Use both SQL and Microsoft Entra authentication

☐ Use SQL authentication

Set Microsoft Entra admin \*

Not Selected

[Set admin](#)

OK

「Entra ID認証を使用する」を選択

管理者とするEntra IDユーザーを選択

■ SQL Server on Azure VMでの、Entra ID認証方式の有効化と、Entra IDユーザーの選択

SQL

SQL-VM-1

SQL virtual machine

Search

Security

Security Configuration

Microsoft Defender for Cloud

Automation

Tasks (preview)

Help

SQL IaaS Agent Extension Settings

Support + Troubleshooting

Feedback

AZURE KEY VAULT INTEGRATION

Configure your virtual machine to be able to connect to the Azure Key Vault service.

Azure Key Vault integration ☒ Disable ☐ Enable

MICROSOFT ENTRA AUTHENTICATION

Configure Microsoft Entra authentication to SQL Server on this machine. [Learn more](#)

Microsoft Entra Authentication ☐ Disable ☒ Enable

Managed identity type \* 

Please select managed identity type

The selected managed identity has to have one the following permissions. Either:  
- Microsoft Entra Directory Readers role  
OR  
- The following three Microsoft Graph application permission (app roles): User.Read.All, GroupMember.Read.All, and Application.Read.All

<https://learn.microsoft.com/ja-jp/azure/azure-sql/virtual-machines/windows/configure-azure-ad-authentication-for-sql-vm?view=azuresql&tabs=azure-portal#enable-microsoft-entra-authentication>

■ 「Entra ID認証」 による接続の例

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

Copilot

User1-46909853@cl...  
CLOUDSLICE

ホーム > dp300-lab-46909853 | SQL データベース > AdventureWorksLT (dp300-lab-46909853/AdventureWorksLT)

AdventureWorksLT (dp300-lab-46909853/AdventureWorksLT) | クエリ エディター ...

SQL データベース

検索

ログイン

新しいクエリ

クエリを開く

フィードバック

はじめに

概要

アクティビティ ログ

タグ

問題の診断と解決

クエリ エディター (プレビュー)

Fabric でデータベースをミラー化する (プレビュー)

設定

データ管理

統合

Power Platform

セキュリティ

インテリジェント パフォーマンス

Query editor (preview) is a tool to run SQL queries against Azure SQL Database in the Azure portal. It is designed for lightweight querying and object exploration in your database. 詳細とトラブルシューティングについては、[詳細情報](#)

SQL

SQL Database クエリ エディターへようこそ

SQL Server 認証

ログイン \*

sqladmin

パスワード \*

Microsoft Entra の認証

User1-46909853@cloudslice.onmicrosoft.com としてログインしました

または

User1-46909853@cloudslice.onm...

DB管理者のEntraユーザーでAzure portalにサインイン

Entra認証を選択してデータベースに接続

# ラーニングパス3

- DB管理者の認証: Entra ID認証、SQL認証、Windows認証
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- ファイアウォール規則
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする



# SQL認証

- 「SQL Server認証」とも
- 「SQLサーバー」や「SQL Database on VM」の作成時に、データベース管理者のユーザー名とパスワードを設定
- データベース接続時に、そのユーザー名とパスワードを入力

■ Azure SQL Databaseの「SQLサーバー」作成時の管理者ユーザー名（ログイン）・パスワードの設定例

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > SQL データベース > SQL データベースの作成 >

SQL Database サーバーの作成

Microsoft

名前と場所の指定など、この サーバー に必要な設定を入力します。この サーバー が、データベースと同じサブスクリプションとリソース グループに作成されます。

サーバー名 \*

db300-lab-9823742

✓

.database.windows.net

場所 \*

(US) West US 2

▼

認証方法

☐ Microsoft Entra 専用認証を使用する

☐ SQL と Microsoft Entra 認証の両方を使用する

☒ SQL 認証を使用する

サーバー管理者ログイン \*

dp300admin

✓

パスワード \*

.....

✓

パスワードの確認 \*

.....

✓

OK

■ 「SQL認証」を使用した接続の例

SSMS等のツールで「SQL認証」  
を選択し、管理者のユーザー  
名・パスワードを入力

Connection

Recent

Browse

Clear List

sv142533.database.windows.net, <default> (aaaa)

Connection Details

Connection type

Microsoft SQL Server

Server \*

dp300-lab-9287423.database.windows.net

Authentication type

SQL Login

User name \*

dp300admin

Password

.....

☐ Remember password

Database

<Default>

Server group

<Default>

Name (optional)

Advanced...

Connect

Cancel

# ラーニングパス3

- DB管理者の認証: Entra ID認証、SQL認証、**Windows認証**
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- ファイアウォール規則
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする

# Windows認証

- Windows OSのユーザーアカウントを使用して認証する方式
- Azure SQL Database Managed InstanceまたはSQL Server on Azure VMで利用可能
- SQL Server on Azure VMでの利用例
  - Azure VM作成時に、Windows管理者のユーザー名とパスワードを入力する。このユーザーがデータベースの管理者となる
  - データベース管理者は、RDPを使用してVMに接続する。そしてSSMS等でデータベースに接続する際、認証方式として「Windows認証」を選ぶ

■ SQL Server on VMの「Windows認証」の設定例

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Azure SQL > SQL デプロイ オプションを選択する >

仮想マシンの作成 ...

低コスト VM の作成に関するヘルプ

高可用性のために最適化された VM の作成

ユーザー名 \* ⓘ

sqladmin

パスワード \*

.....

パスワードの確認 \*

.....

仮想マシンの作成時に、  
**Windowsの管理者のユーザー名・パスワード**を指定

■ SQL Server on VMの「Windows認証」による接続例

Connect to Server

SQL Server

LoginConnection PropertiesAlways EncryptedAdditional Connection Parameters

Server

Server type:Database Engine

Server name:azureSQLServerV

Authentication:Windows Authentication

User name:azureSQLServerVsqladmin

Password:

☐ Remember password

Connection Security

Encryption:Mandatory

☒ Trust server certificate

Host name in certificate:

Connect

Cancel

Help

Options <<

Windowsにその管理者ユーザーでサインインし、SSMSの「Windows認証」を使用してSQL Serverに接続する

# どの認証方式がよいのか？

- 可能な場合は「Entra認証」を使用することが推奨されている
  - Entra IDでは「MFA」や「条件付きアクセス」、「パスワードレス認証」などの最新の安全な認証機能が提供される
  - 管理者は普段使っているEntra IDを使用してデータベースにサインインでき、追加のパスワードなどを覚える必要がない
- 「SQL認証」と「Windows認証」では、可能な場合は「Windows認証」を使用することが推奨されている
- 「SQL認証」を使用する場合は、ユーザー名・パスワードの漏洩に注意



# ラーニングパス3

- DB管理者の認証: Entra ID認証、SQL認証、Windows認証
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- ファイアウォール規則
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする

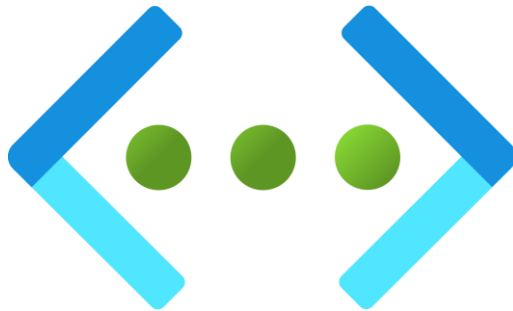
# ラボ3 講師デモ

別紙

# ラーニングパス3

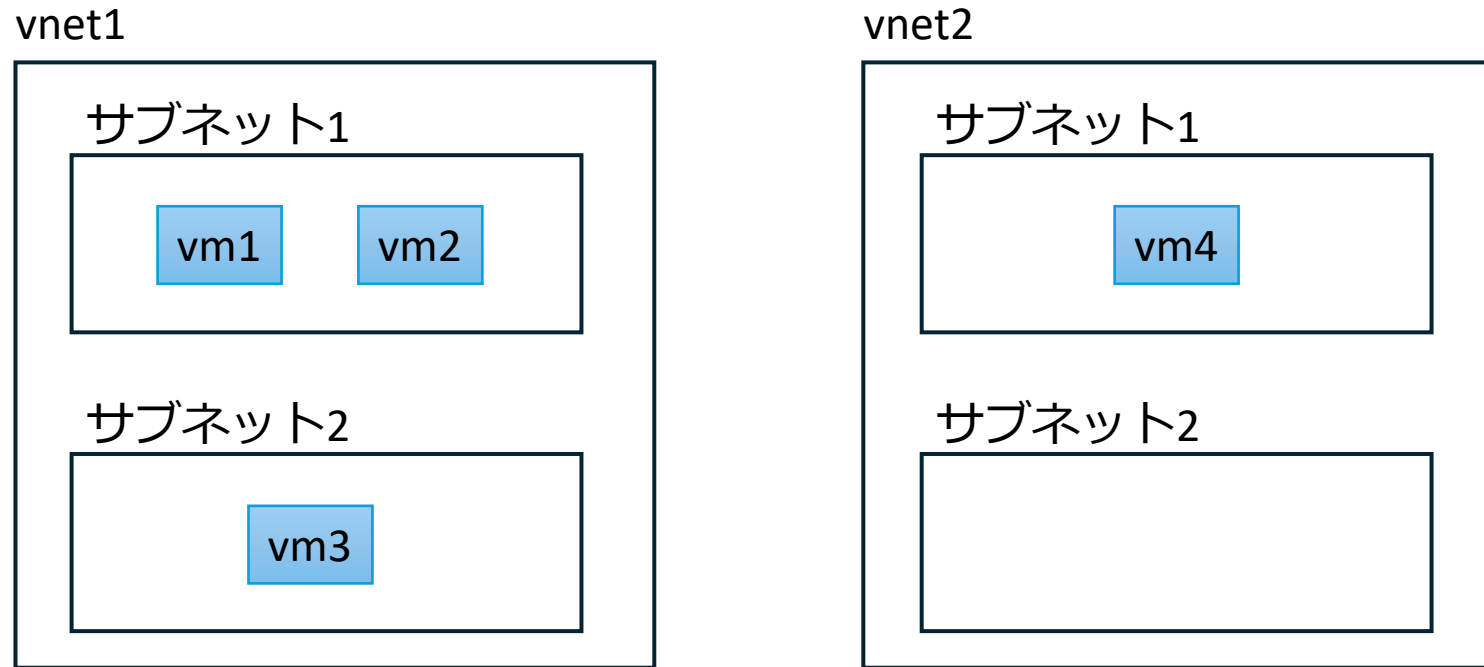
- DB管理者の認証: Entra ID認証、SQL認証、Windows認証
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- ファイアウォール規則
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする

# Azure 仮想ネットワーク



# Azureの仮想ネットワーク (Virtual Network, VNet)

- Azure内に作成されるプライベートなネットワーク
- 各VNetは論理的に分離されている
- VM (Azure仮想マシン)、Azure Firewall、Azure Bastion、Azure Application Gateway、仮想ネットワークゲートウェイなどのリソースはVNetの内部 (サブネット内部) に配置される
- その他の多くのAzureのサービスのリソースはVNetの外部に配置される



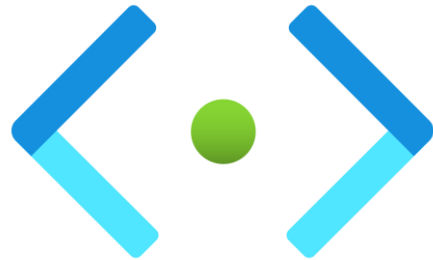
ストレージアカウント

Azure Cosmos DB

Azure Key Vault

Azure OpenAI Service

# サブネット



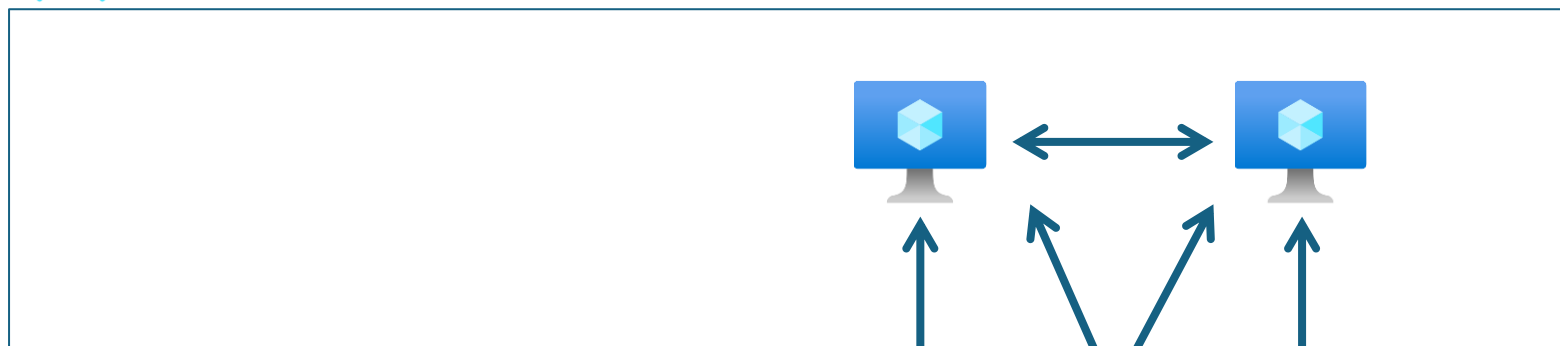
仮想ネットワークの中にサブネットを作成。（パブリック/プライベート、Web/App/DB等）  
VMは、同じVNet内であれば、サブネットを超えて相互に通信可能。  
サブネット(とNIC)にはNSGを関連付けできる



仮想ネットワーク 10.0.0.0/16



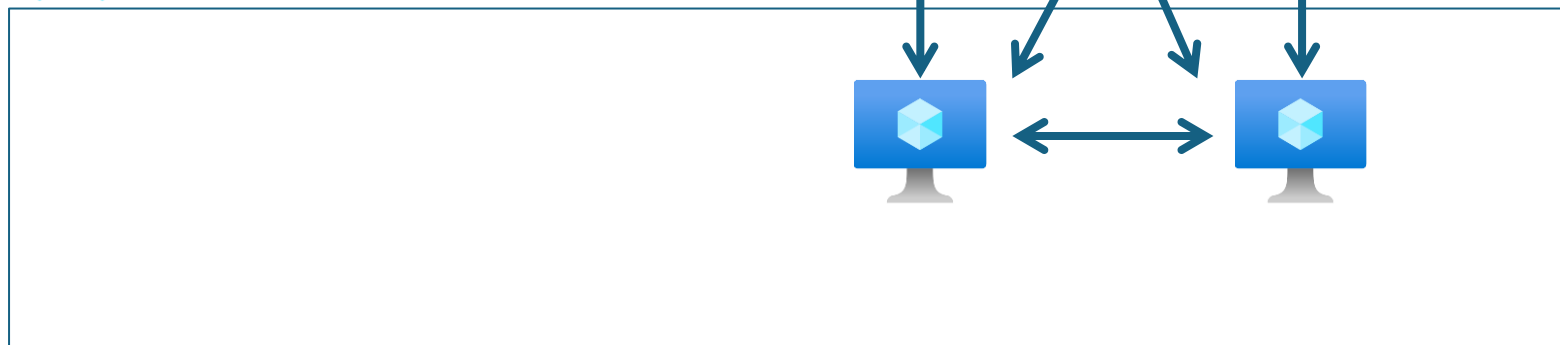
サブネット 10.0.0.0/24



ネットワーク  
セキュリティ  
グループ  
(NSG)



サブネット 10.0.1.0/24



ネットワーク  
セキュリティ  
グループ  
(NSG)



ネットワーク  
セキュリティグループ(NSG)



ネットワークセキュリティグループ (NSG) は、サブネットまたはNICに関連付けが可能。



仮想ネットワーク



サブネット



仮想マシン



ネットワーク  
インターフェースカード(NIC)



ネットワーク  
セキュリティ  
グループ  
(NSG)




ネットワーク  
セキュリティ  
グループ  
(NSG)


NSGには「受信セキュリティ規則」と「送信セキュリティ規則」という規則のリストがある。

優先度 ↑↓	名前 ↑↓	ポート ↑↓	プロトコル ↑↓	ソース ↑↓	宛先 ↑↓	アクション ↑↓
<input type="checkbox"/> 300	 RDP	3389	TCP	任意	任意	 Allow
<input type="checkbox"/> 310	AllowAnyHTTPInbound	80	TCP	任意	任意	 Allow
<input type="checkbox"/> 65000	AllowVnetInBound	任意	任意	VirtualNetwork	VirtualNetwork	 Allow
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	任意	任意	AzureLoadBalancer	任意	 Allow
<input type="checkbox"/> 65500	DenyAllInBound	任意	任意	任意	任意	 Deny



設定


 受信セキュリティ規則

 送信セキュリティ規則

優先度 ↑↓	名前 ↑↓	ポート ↑↓	プロトコル ↑↓	ソース ↑↓	宛先 ↑↓	アクション ↑↓
<input type="checkbox"/> 65000	AllowVnetOutBound	任意	任意	VirtualNetwork	VirtualNetwork	 Allow
<input type="checkbox"/> 65001	AllowInternetOutBound	任意	任意	任意	Internet	 Allow
<input type="checkbox"/> 65500	DenyAllOutBound	任意	任意	任意	任意	 Deny

各規則には「優先度」があり、優先度が高い（数字が小さい）ものから順に評価されていく。  
65000以降のものは組み込みの規則であり、カスタマイズ・削除できない。

評価の順

 受信セキュリティ規則

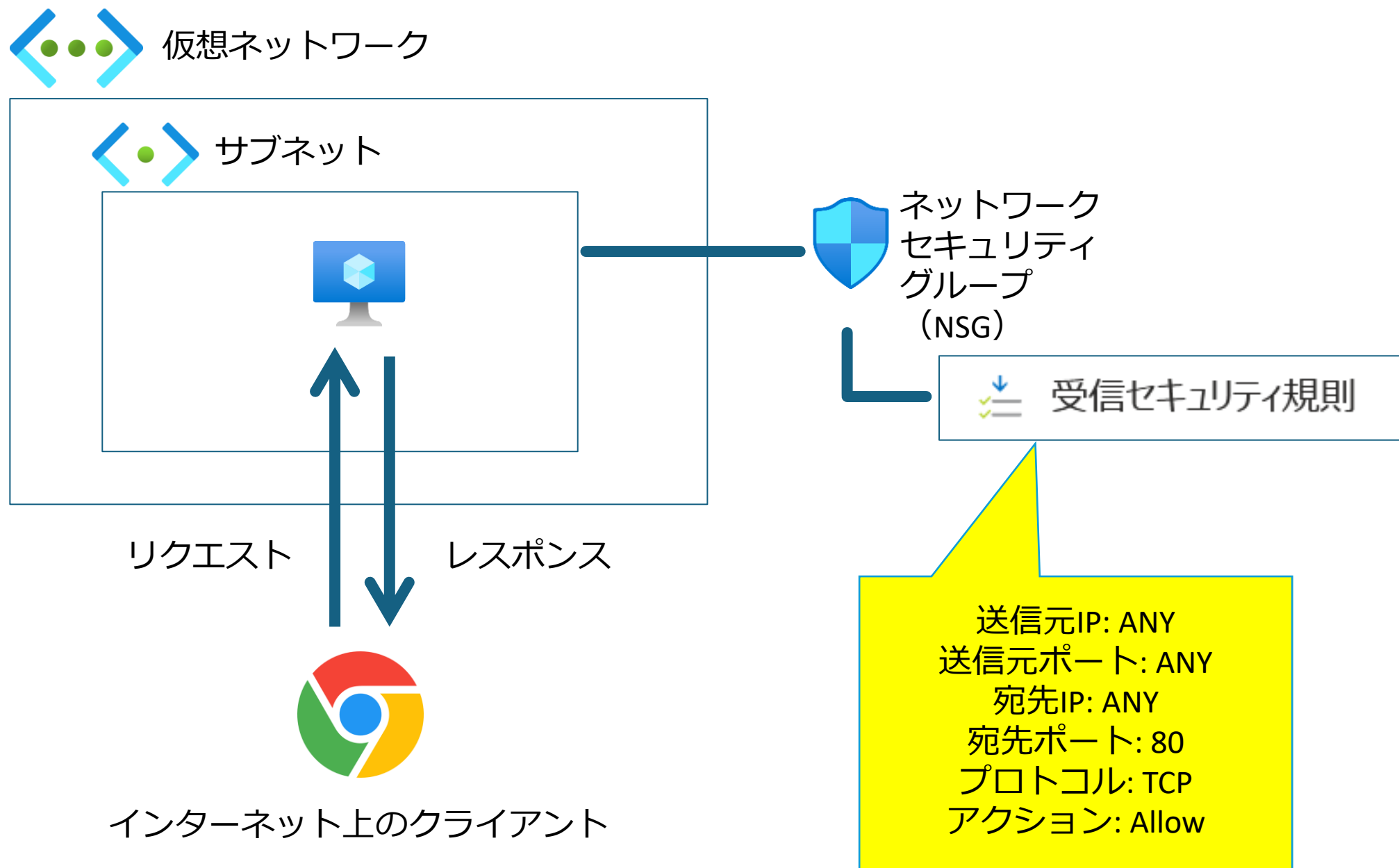
優先度 ↑↓	名前 ↑↓	ポート ↑↓	プロトコル ↑↓	ソース ↑↓	宛先 ↑↓	アクション ↑↓
<input type="checkbox"/> 300	 RDP	3389	TCP	任意	任意	 Allow
<input type="checkbox"/> 310	AllowAnyHTTPInbound	80	TCP	任意	任意	 Allow
<input type="checkbox"/> 65000	AllowVnetInBound	任意	任意	VirtualNetwork	VirtualNetwork	 Allow
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...	任意	任意	AzureLoadBalancer	任意	 Allow
<input type="checkbox"/> 65500	DenyAllInBound	任意	任意	任意	任意	 Deny

例(1): RDP(TCP 3389)のトラフィック: 優先度300番の規則により、許可される。

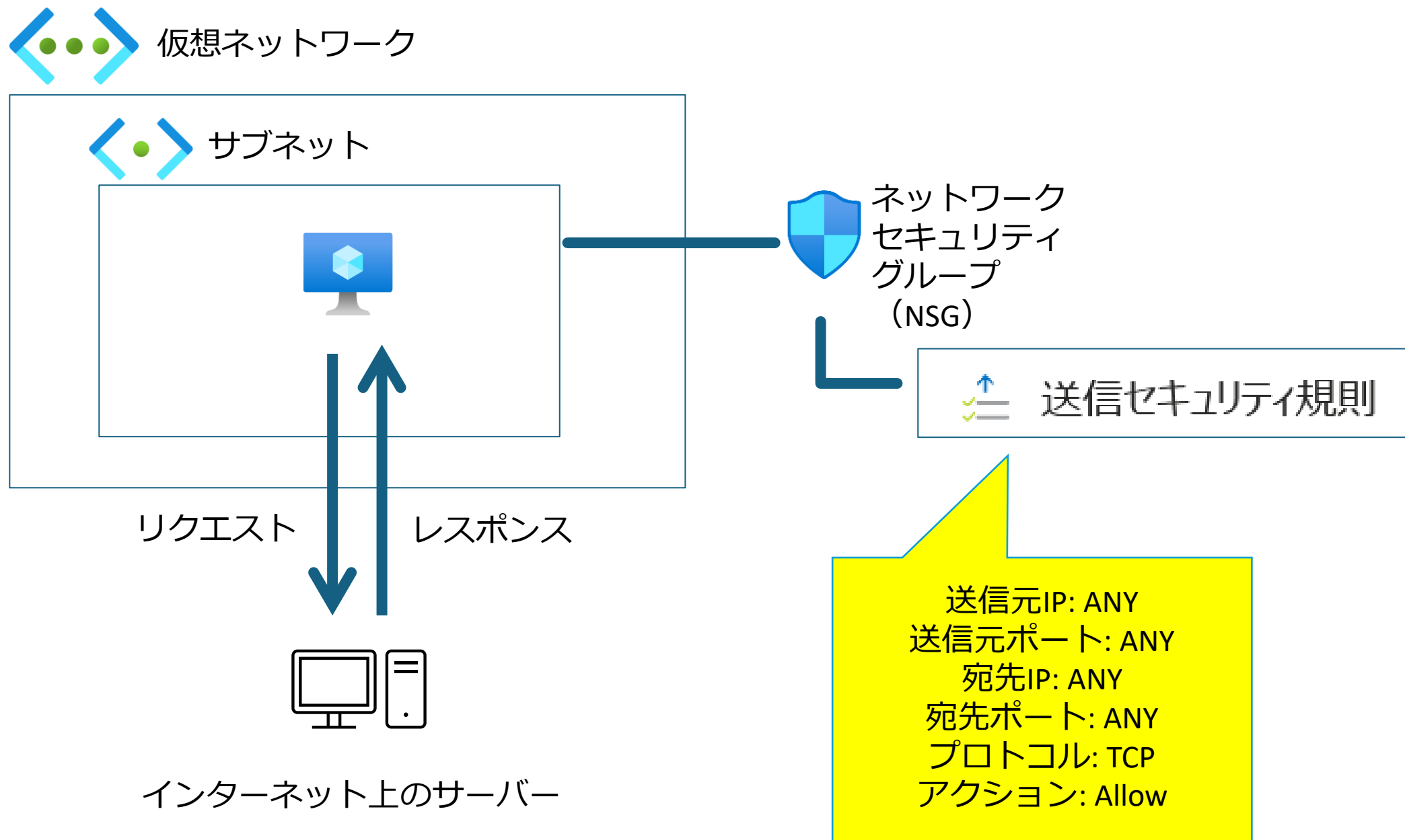
例(2): HTTP(TCP 80)のトラフィック: 優先度310番の規則により、許可される。

例(3): SSH(TCP 22)のトラフィック: 優先度65500番の規則により、拒否される。

# 「受信」の例

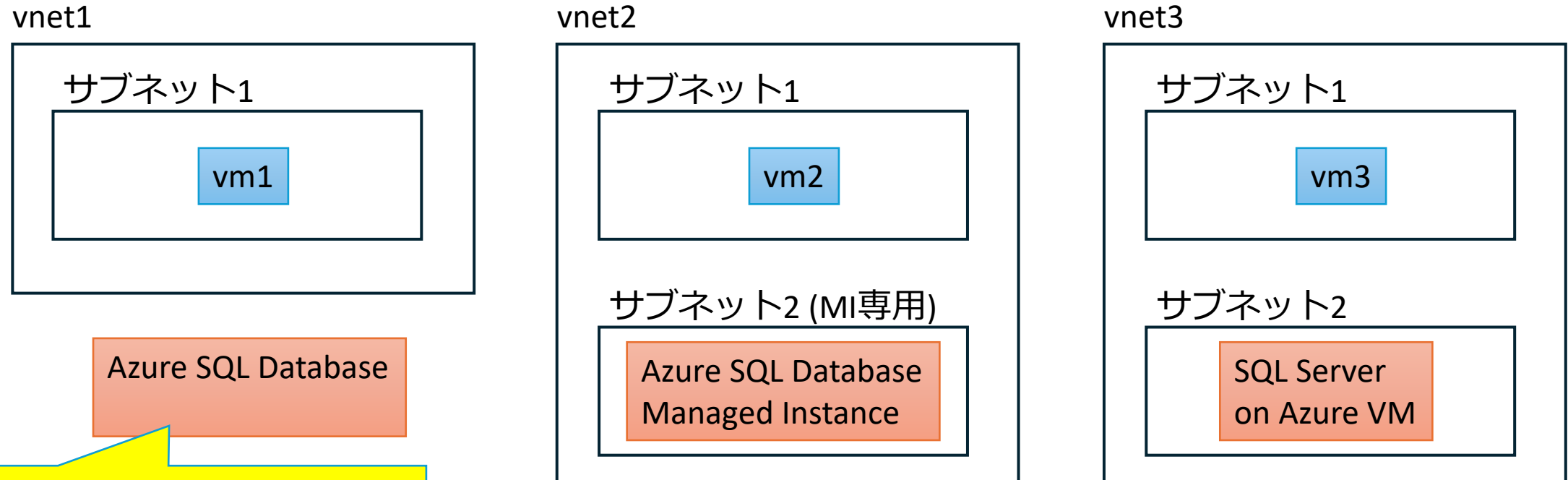


# 「送信」の例



# Azure SQLと仮想ネットワーク

- Azure SQL Database: 仮想ネットワークの**外側**に配置される
- Azure SQL Database Managed InstanceとSQL Server on Azure VM: 仮想ネットワークの**内側**に配置される



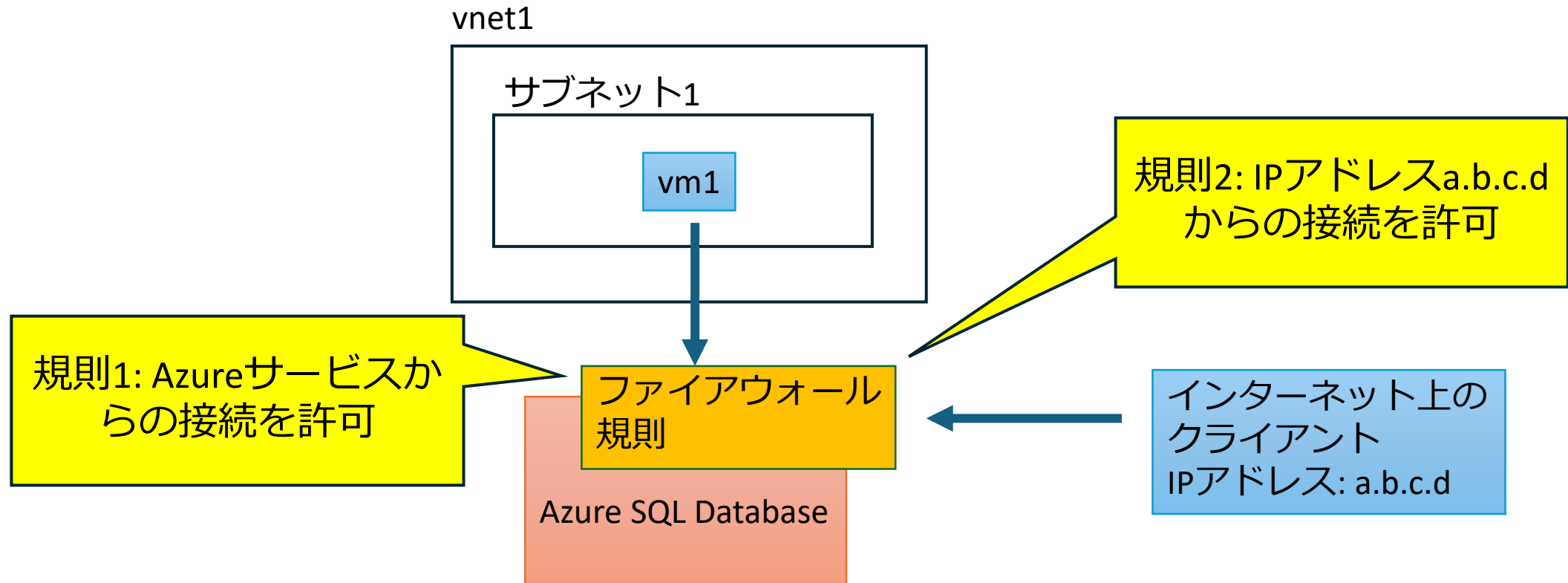
Azure SQL DatabaseはVNet  
の中には配置されない

# ラーニングパス3

- DB管理者の認証: Entra ID認証、SQL認証、Windows認証
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- **ファイアウォール規則**
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする

# Azure SQL Database: 仮想ネットワークの**外側**

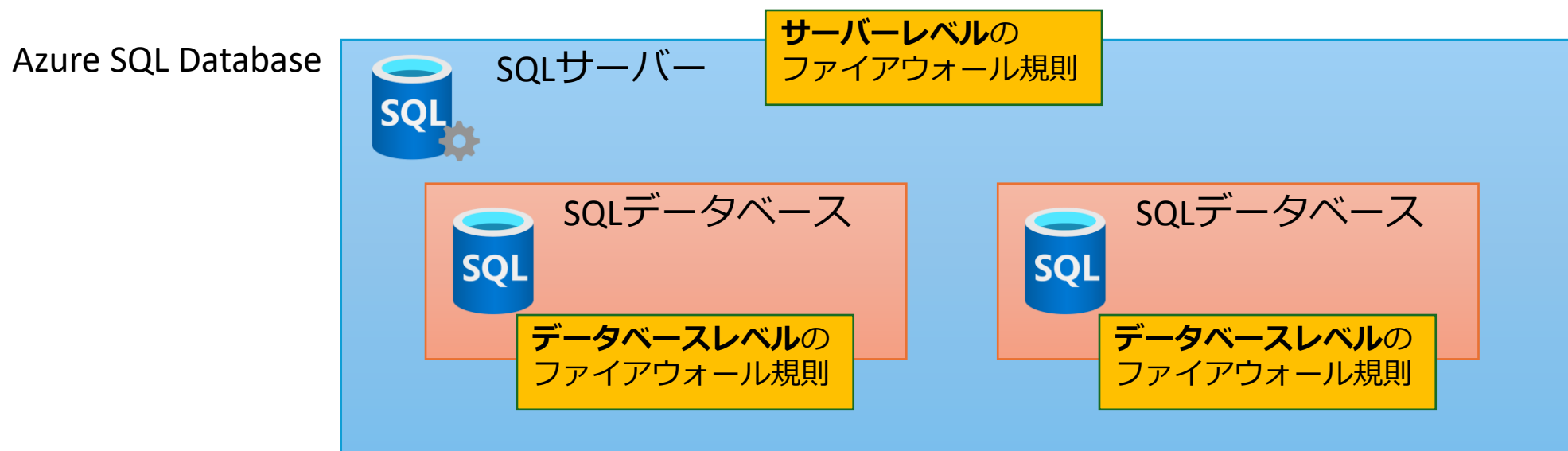
- Azure SQL Databaseでは、適切な「**ファイアウォール規則**」を設定することで、Azure VMなどのAzureサービスや、インターネットからの接続を許可する。
- ※デフォルトでは、すべてのIPアドレスからの接続を拒否



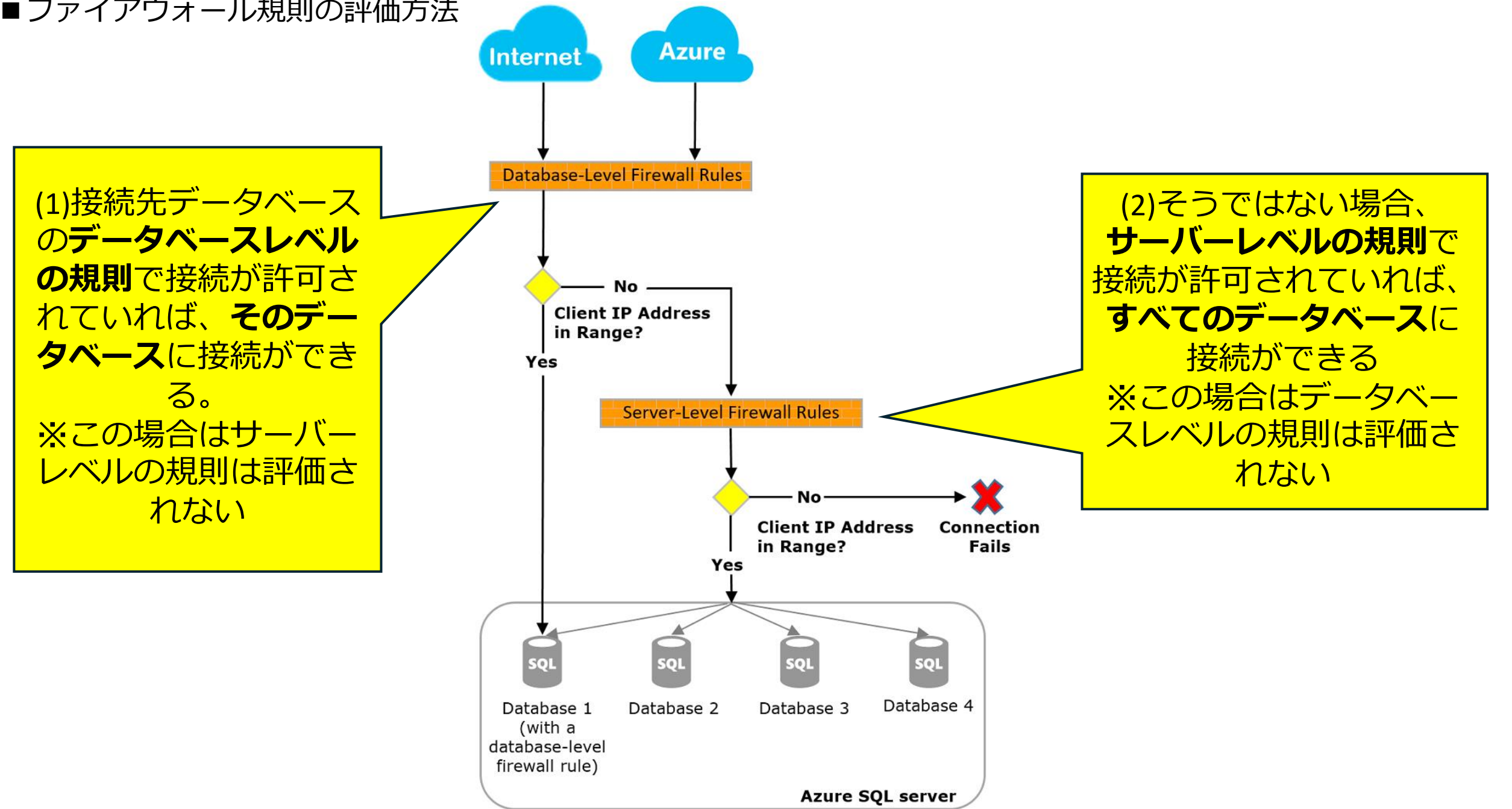


# ファイアウォール規則

- Azure SQL Databaseで利用可能
- 「ファイアウォール規則」は、接続を許可するクライアントのIPアドレスの範囲の指定。
- 例: 11.22.33.100 - 11.22.33.200と指定すると、その範囲のIPアドレスのクライアントから、データベースに接続できる
- 「**サーバーレベル**のファイアウォール規則」と「**データベースレベル**のファイアウォール規則」がある



■ファイアウォール規則の評価方法



■参考: 「特定の」 VNet/サブネットからのみ接続を許可したい場合 (サービスエンドポイント)

mydocsamplesqlserver | Networking

SQL server

Search (Ctrl+ /)

Locks

Data management

Backups

Deleted databases

Failover groups

Import/Export history

Security

Networking

Microsoft Defender for Cloud

Transparent data encryption

Identity

Auditing

Intelligent Performance

Automatic tuning

Recommendations

Feedback

Public accessPrivate accessConnectivity

Public network access

Public Endpoints allow access to this resource through the internet using a public IP address. An application or resource that is granted access with the following requires proper authorization to access this resource. [Learn more](#)

Public network access

☐ Disable

☒ Selected networks

Connections from the IP addresses configured in the Firewall rules

Virtual networks

Allow virtual networks to connect to your resource using service endpoints. [Learn more](#)

+ Add a virtual network rule

Firewall rules

Setting 'Allow Azure services and resources to access this server' to Yes allows communications from the Azure boundary, that may or may not be part of your subscription. [Learn more](#)

Setting 'Add current client IP address' to Yes will add an entry for your client IP address to the Firewall rules

Allow Azure services and resources to access this server \*

No

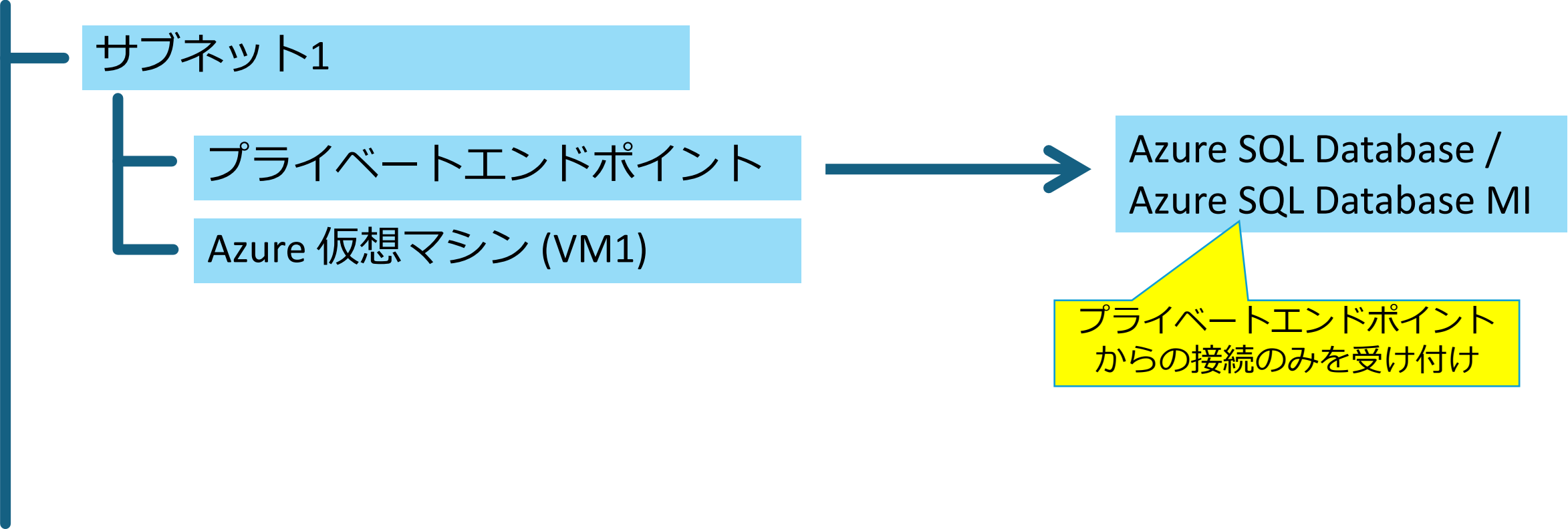
Yes

(1)ネットワーク設定で「選択されたネットワーク」を選び、接続を許可するVNet/サブネットを選択  
※選択されたサブネットには「サービスエンドポイント」が追加される

(2)[Azure サービスおよびリソースにこのサーバーへのアクセスを許可する] を [いいえ] に設定  
※[はい]の場合はすべてのVNet/サブネットからの接続が許可される

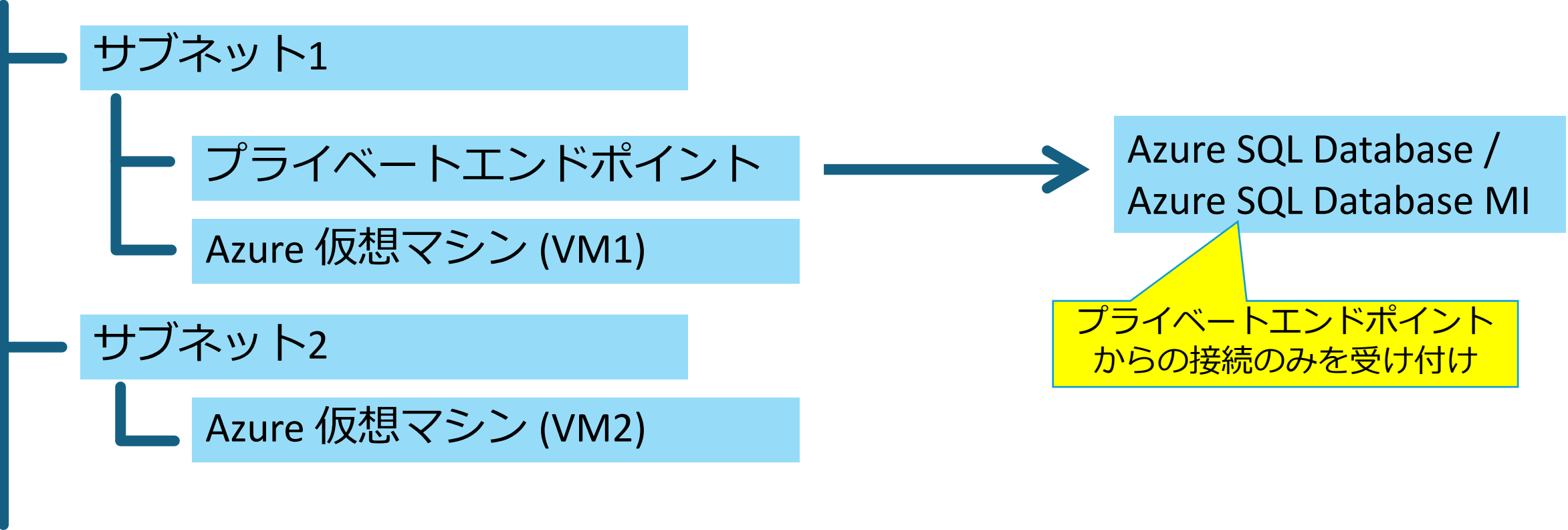
■参考: プライベートエンドポイント接続: さまざまなパターンのプライベート接続をサポート。  
Azure SQL Database: 2018/2/22～ / Azure SQL Database Managed Instance: 2023/8/10～

Azure 仮想ネットワーク(VNet)



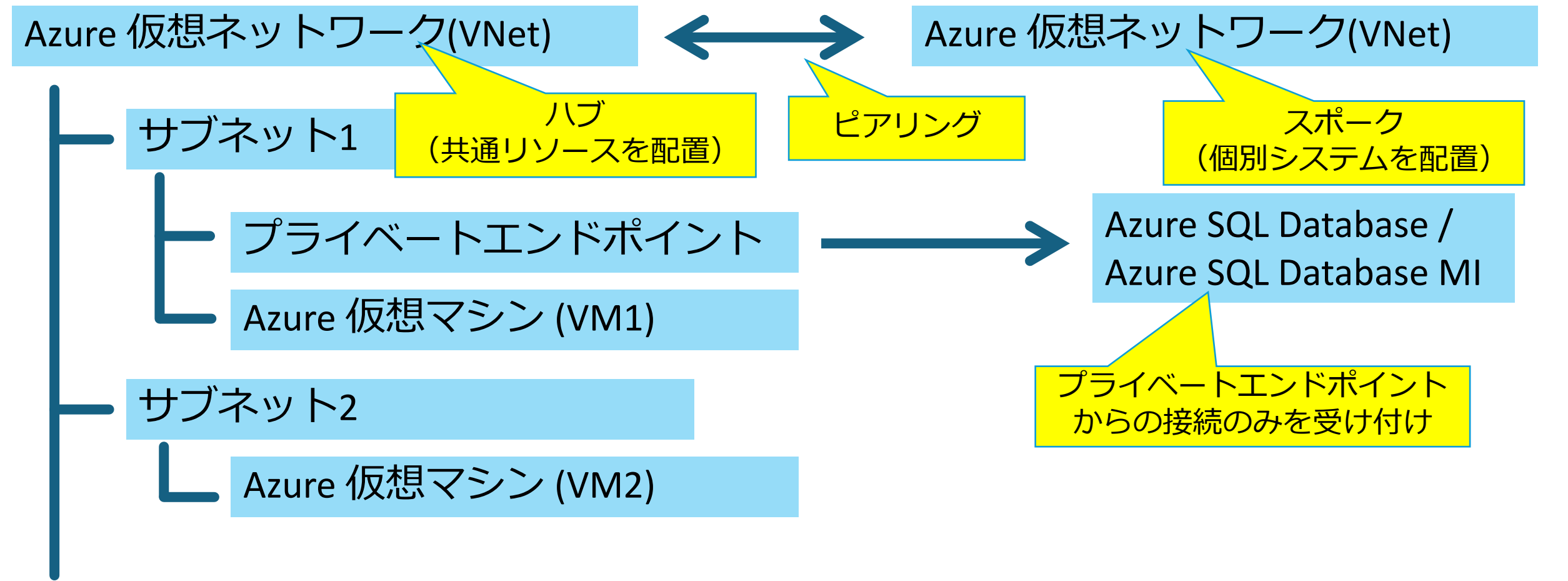
■参考: プライベートエンドポイント接続: さまざまなパターンのプライベート接続をサポート。  
Azure SQL Database: 2018/2/22～ / Azure SQL Database Managed Instance: 2023/8/10～

Azure 仮想ネットワーク(VNet)



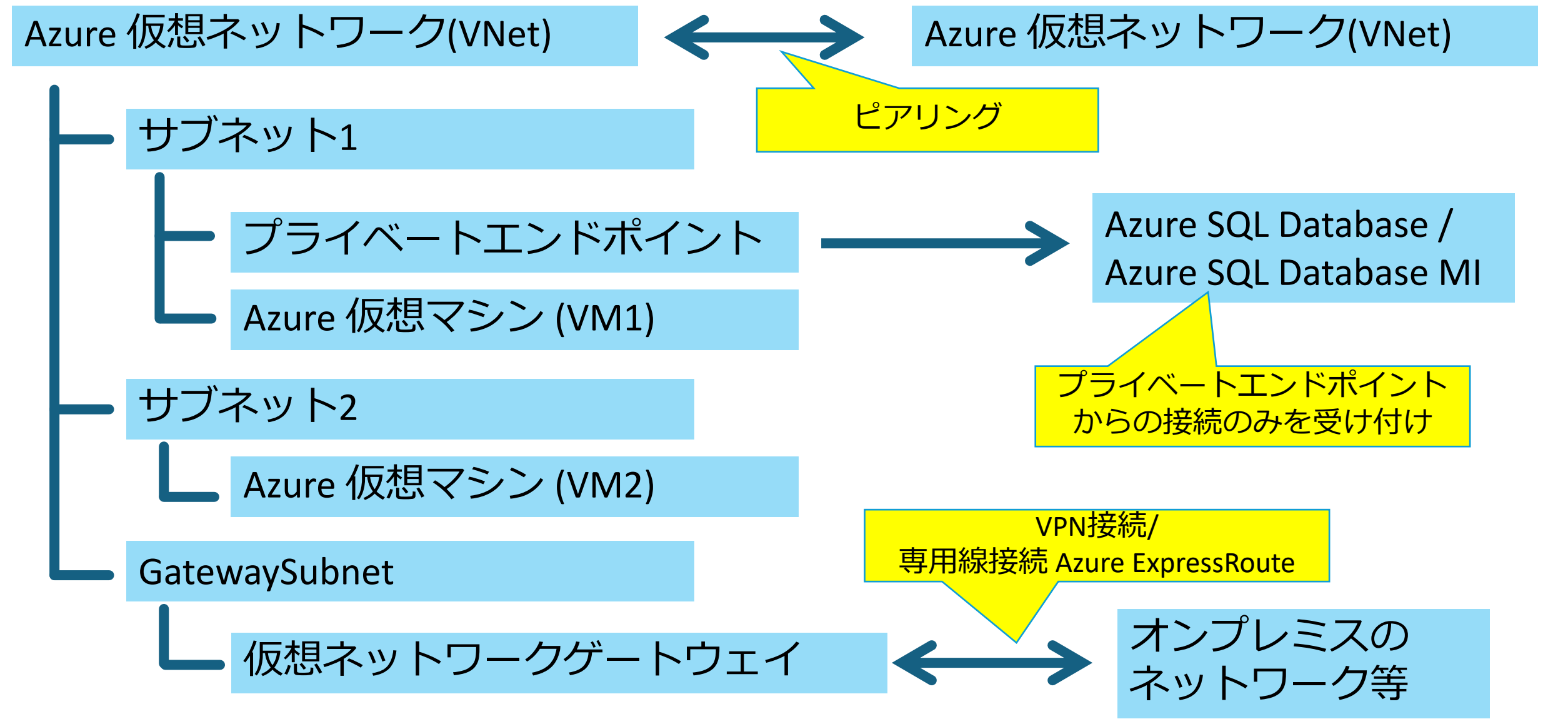
■参考: プライベートエンドポイント接続: さまざまなパターンのプライベート接続をサポート。

Azure SQL Database: 2018/2/22～ / Azure SQL Database Managed Instance: 2023/8/10～

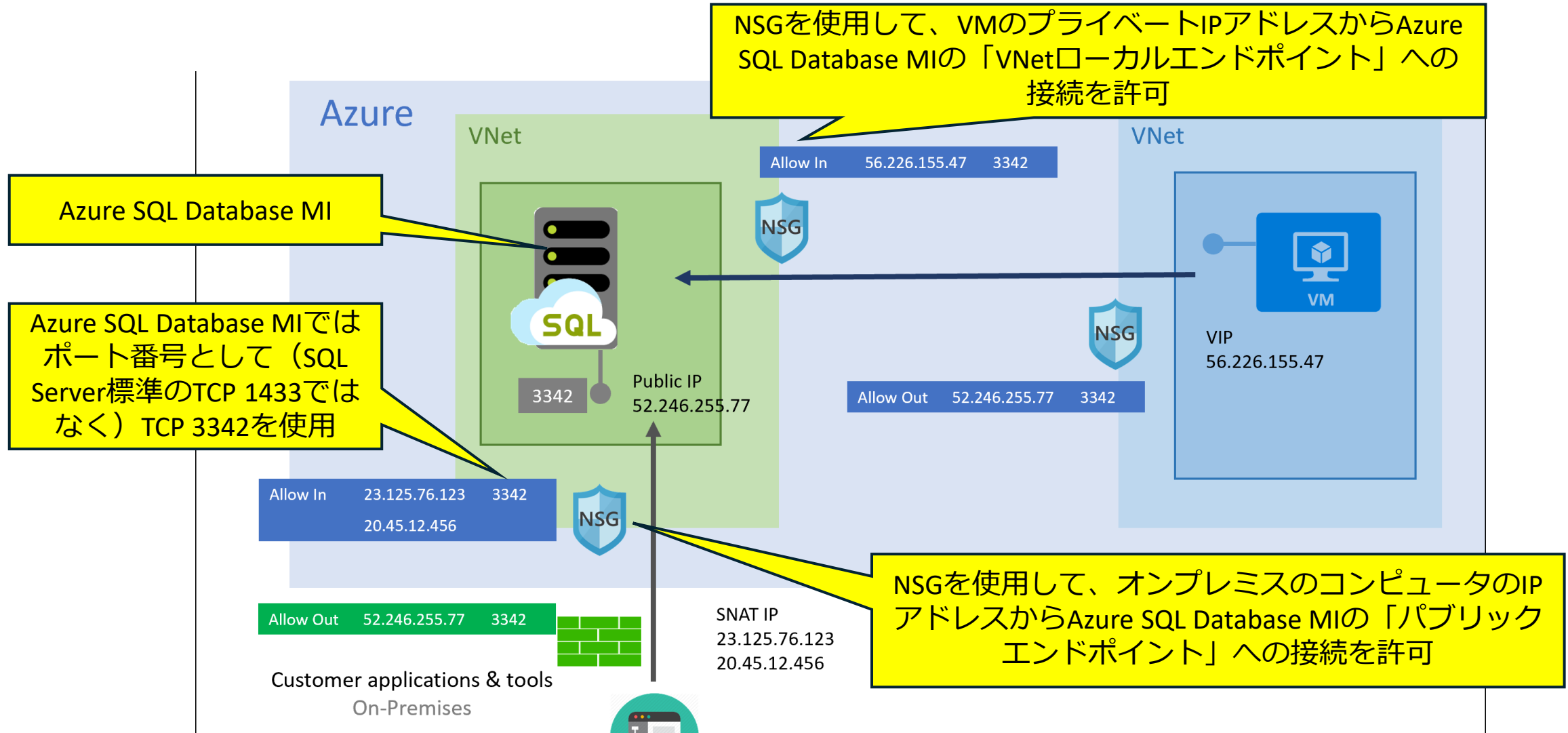


■参考: プライベートエンドポイント接続: さまざまなパターンのプライベート接続をサポート。

Azure SQL Database: 2018/2/22～ / Azure SQL Database Managed Instance: 2023/8/10～



# Azure SQL Database Managed InstanceとSQL Server on VM: 仮想ネットワークの**内側**にあるためNSGを使用して接続を制御





# ラーニングパス3

- DB管理者の認証: Entra ID認証、SQL認証、Windows認証
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- ファイアウォール規則
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする

# ラボ4 講師デモ

別紙

# ラーニングパス3

- DB管理者の認証: Entra ID認証、SQL認証、Windows認証
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- ファイアウォール規則
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする

Microsoft Defender for Cloud



CSPM  
(クラウドセキュリティ態勢管理、「設定ミス」の発見)。無料。  
元「Azure Security Center」

## Microsoft Defender for Cloud



強化されたセキュリティ機能(enhanced security features)

**CSPM**  
(クラウドセキュリティ態勢管理、「設定ミス」の発見)。無料。  
元「Azure Security Center」

**CWPP**  
(クラウドワークロード保護プラットフォーム、VM等の保護)。有料。  
CWP(クラウドワークロード保護)とも。  
元「Azure Defender プラン」

# Microsoft Defender for Cloud



## 強化されたセキュリティ機能(enhanced security features)

### Microsoft Defender for servers

(プラン1: \$5/サーバー/月、プラン2: \$15/サーバー/月)



オンプレ/クラウドの  
Windows/Linux

### Microsoft Defender for SQL

※元Azure SQL  
Data Warehouse

Azure SQL  
Database

Azure SQL Database  
Managed Instance

Azure Synapse  
Analytics

### Microsoft Defender for SQL Server on Machines

SQL Server  
on Azure VM

オンプレVMの  
SQL Server

AWS/GCPのVMの  
SQL Server

CSPM  
(クラウドセキュリティ態勢管理、「設定ミス」の発見)。無料。  
元「Azure Security Center」

CWPP  
(クラウドワークロード保護プラットフォーム、VM等の保護)。有料。  
CWP(クラウドワークロード保護)とも。  
元「Azure Defender プラン」

「強化されたセキュリティ機能」に含まれるプランの1つ。マルチクラウドとオンプレのWindows/Linuxマシンを保護。

「強化されたセキュリティ機能」に含まれるプランの1つ。データベースの脆弱性評価と、脅威に対する保護を提供。

<https://learn.microsoft.com/ja-jp/azure/defender-for-cloud/defender-for-sql-on-machines-overview>

<https://learn.microsoft.com/ja-jp/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1-2>

<https://learn.microsoft.com/ja-jp/azure/defender-for-cloud/defender-for-servers-introduction>

# Microsoft Defender for SQL

- 2020/12/2 一般提供開始
- Azure SQL Database / Azure SQL Database Managed Instance / Azure Synapse Analyticsで利用可
- データベースの潜在的な脆弱性を検出して軽減するのに役立つ
  1. 脆弱性評価: データベースをスキャンして、脆弱性を検出、追跡、修復。
  2. 脅威に対する保護: 詳細なセキュリティ アラートと推奨されるアクションを利用できる
- 有料（\$15/サーバー/月）※最初の30日は無料試用可

# Microsoft Defender for SQL

## 1. 脆弱性評価

- データベースをスキャンして、脆弱性を検出、追跡、修復
- 脆弱性を発見するのに役立つ

## 2. 脅威に対する保護

- 詳細なセキュリティ アラートと推奨されるアクションを利用できる
- SQLインジェクション攻撃、ブルートフォース攻撃などの脅威を検出してアラートを発報
- 脅威を軽減するためのガイダンスが利用できる



# Microsoft Defender for SQL

## 1. 脆弱性評価

攻撃される前の予防

- データベースをスキャンして、脆弱性を検出、追跡、修復
- 脆弱性を発見するのに役立つ

## 2. 脅威に対する保護

実際の攻撃に対する対処

- 詳細なセキュリティ アラートと推奨されるアクションを利用できる
- SQLインジェクション攻撃、ブルートフォース攻撃などの脅威を検出してアラートを発報
- 脅威を軽減するためのガイダンスが利用できる

# ラーニングパス3

- DB管理者の認証: Entra ID認証、SQL認証、Windows認証
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- ファイアウォール規則
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする

# ラボ5(前半) 講師デモ

別紙

# ラーニングパス3

- DB管理者の認証: Entra ID認証、SQL認証、Windows認証
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- ファイアウォール規則
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする

# SQL Information Protection (データベース内の機密データの検出と分類)

- 2018/5/7 一般提供開始
- Azure SQL Database / Azure SQL Database Managed Instance / SQL Server 2012以降で利用可能
- データベースレベルで有効化
- 無料
- **列の名前**に基づき、列の情報種別が決定される。
- パスワード、氏名、電話番号など、機密性の高いデータを含む列をすばやく特定できる。

SQL Server 2012以降が稼働するSQL Server on Azure VMでも利用可能

機密性の高いデータが含まれるデータベースを特定し、保護対策を行うのに役立つ

## Information types

[+ Create information type](#)

### Create and manage information types

Drag information types to order in ascending discovering ranking

 Configure  Move up  Move down  Move to top  Move to bottom  Delete

<input type="checkbox"/>	Information type	State	Associated label	Type
--------------------------	------------------	-------	------------------	------

「データの検出と分類」では、**列の名前**に基づき、列の情報種別が決定される。

たとえば検出パターンに「%password%」と設定すると、**列名にpasswordという文字列が含まれている場合**、その列はパスワードを含む列である、と判断される。

<input type="checkbox"/>	Date Of Birth	Enabled	Confidential - GDPR	Built-in	...
<input type="checkbox"/>	Other	Enabled	Confidential	Built-in	...

[Create new information type](#)

OK

## Configure information type

Enabled

ON

OFF

Display name \*

Description

Associated label

[n/a]

Pattern

Allow numeric

eg. %password%



OK

# ラーニングパス3

- DB管理者の認証: Entra ID認証、SQL認証、Windows認証
  - ラボ3 Entra IDを使用してアクセスを承認する
- 仮想ネットワーク
- ファイアウォール規則
  - ラボ4 Azure SQL Databaseファイアウォール規則を構成する
- Microsoft Defender for Cloud
- Microsoft Defender for SQL
  - ラボ5（前半）Microsoft Defender for SQLを有効にする
- SQL Information Protection (機密データの検出と分類)
  - ラボ5（後半）データ分類を有効にする

# ラボ5(後半) 講師デモ

別紙