

SC-5002

補足資料

Microsoft Defender for Cloud の規制コンプライアンス コントロールを使用して Azure のサービスとワークロードをセキュリティで保護する 2

- Defender for Cloud の規制コンプライアンス標準の詳細
- Azure サブスクリプションで Defender for Cloud を有効にする
- Azure portal を使用してネットワーク セキュリティ グループでネットワーク トラフィックをフィルター処理する
- Microsoft Defender for Cloud 用の Log Analytics ワークスペースを作成する
- Log Analytics エージェントを構成して Defender for Cloud のワークスペースと統合する
- Just-In-Time 仮想マシン アクセスについて調べる
- Azure Key Vault のネットワーク設定を構成する

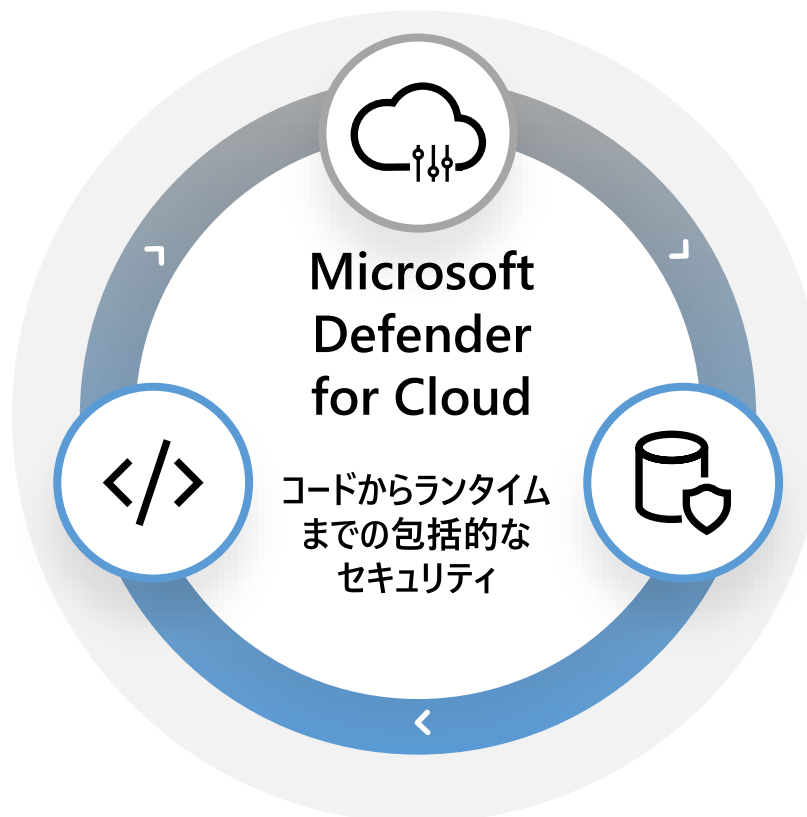
CSPM + CIEM

リスクの継続的な低減

クラウドアプリケーションのライフサイクル全体にわたるコンテキストに応じた
優先順位付けされたセキュリティ態勢管理

AppSec + CI/CDセキュリティ
安全な開発を実現

コードの脆弱性、設定ミス、
シークレットを検出し、
ソフトウェアサプライチェーンを保護



CWP + CDR
**脅威をより迅速に
修復**

統合されたXDRエクスペリエンスで
、クラウドワークロード、データ、APIを
ほぼリアルタイムで検出して対応



Microsoft Defender for Cloud

ポリシー強制 (G: ガバナンス)



推奨事項や規制・コンプライアンスに対して、是正機能（Fix, Remediation）を提供

脆弱性（セキュリティホール）をなくす（CSPM）

- ✓ 推奨事項（Recommendations）
- ✓ クラウドサービスや VM 内の設定などに残っている構成設定上の脆弱性を、修正すべき推奨事項として示す

攻撃（脅威）に気付けるようにする（CWP）

- ! セキュリティ警告（Security alerts）
MDE や ASA（Adaptive Security Appliance）などの各種の攻撃検知システム（センサー）から報告された攻撃を通知する

脆弱性管理（R：リスク管理）

- ★ セキュリティ態勢（Security Posture）
各システム（サブスクリプション）でどの程度セキュリティ対策が行われているかを横並び比較する

規制準拠（C: コンプライアンス）

- 🏛️ 規制コンプライアンス（Regulatory Compliance）
業界標準として定義されている最低限行うべきセキュリティ対策をきちんと行っているかを確認・レポートする

Microsoft Defender for Cloud | 概要

サブスクリプション 'ME-MngEnv841187-naokiabe' を表示しています

検索

サブスクリプション 新機能

表示されている情報が限られています

1
Azure サブスクリプション

セキュリティ態勢

11/11
未割り当て

セキュア スコア

56%
セキュア スコア

セキュリティ体制を調べる>

規制コンプライア

全般

概要

はじめに

推奨事項

攻撃パスの分析

セキュリティ警告

インベントリ

セキュリティグラフ

ブック

コミュニティ

問題の診断と解決

クラウド セキュリティ

セキュリティ態勢

規制コンプライアンス

ワークロード保護

Firewall Manager

DevOps security (preview)

管理

環境設定

セキュリティ ソリューション

ワークフローの自動化

Defender プラン



設定 | Defender プラン

ME-MngEnv841187-naokiabe

検索

保存 自動プロビジョニング - 拡張機能

設定

Defender プラン

電子メールの通知

ワークフローの自動化

連続エクスポート

ポリシー設定

セキュリティポリシー

ガバナンス ルール

すべて有効にする

Cloud Security Posture Management (CSPM)

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, data-aware security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying only for Servers, Databases, and Storage resources at \$5/Billable resource/month. Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

Microsoft Defender for	プラン / 価格	リソースの数	構成	状態
Foundational CSPM	Free 詳細 >		完全に構成済み	<input type="checkbox"/> オン <input type="checkbox"/> オフ
Defender CSPM	\$5/Billable resource/Month, 2023 年 8 月 1 日までは無料 詳細 >	8 resources ^①	完全に構成済み 構成の編集	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ

Cloud Workload Protection (CWP)

Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

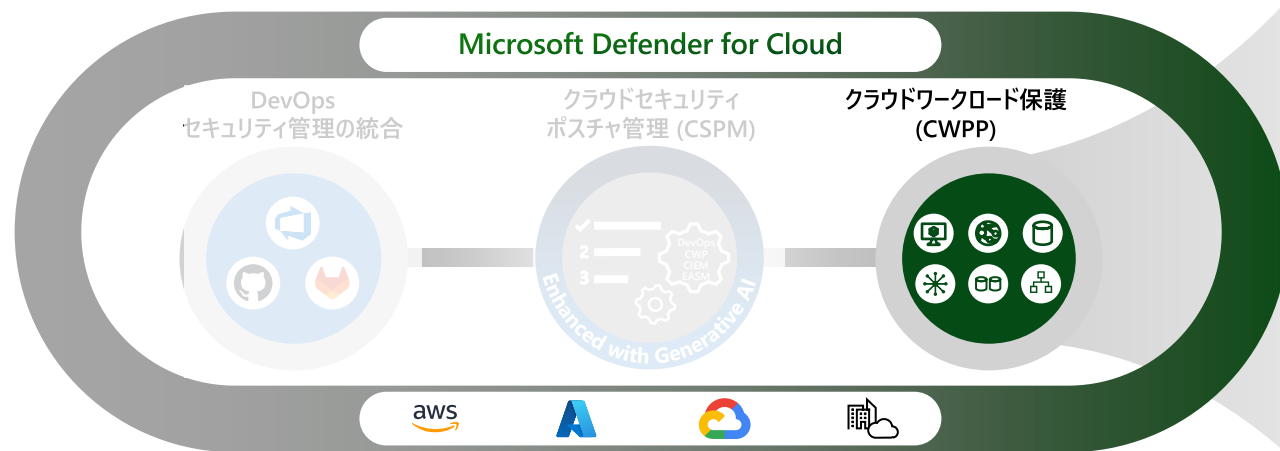
Microsoft Defender for	プラン / 価格	リソースの数	構成	状態
サーバー	プラン 2 (\$15/サーバー/月) ^① プランの変更 >	4 台のサーバー	一部構成済み 構成の編集	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ
App Service	\$15/インスタンス/月 詳細 >	0 個のインスタンス	完全に構成済み	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ
データベース	選択済み: 4 個中 4 個 ^① 種類の選択 >	保護済み: 1 個中 1 個のインスタンス	完全に構成済み 構成の編集	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ
ストレージ	\$10/Storage account/month On-upload malware scanning (\$0.15/GB) ^① 詳細 >	5 個のストレージ アカウント	完全に構成済み 構成の編集	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ
コンテナ	\$7/月あたりの VM コア 詳細 >	0 個のコンテナ レジストリ; 0 個の Kubernetes コア	一部構成済み 構成の編集	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ
Kubernetes (非推奨)	2 ドル/月あたりの VM コア ^①	0 個の Kubernetes コア	完全に構成済み	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ
コンテナ レジストリ (非推奨)	\$0.29/画像	0 個のコンテナ レジストリ	完全に構成済み	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ
Key Vault	0.02 ドル/10K トランザクション 新しいプランが利用可能です	1 個のキー コンテナ	完全に構成済み	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ
Resource Manager	4 ドル/1M のリソース管理操作 新しいプランが利用可能です ^①		完全に構成済み	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ
APIs	無料 (プレビュー) ^① 詳細 >	0 Azure API Management services	Action required ^①	<input checked="" type="checkbox"/> オン <input type="checkbox"/> オフ

CSPM



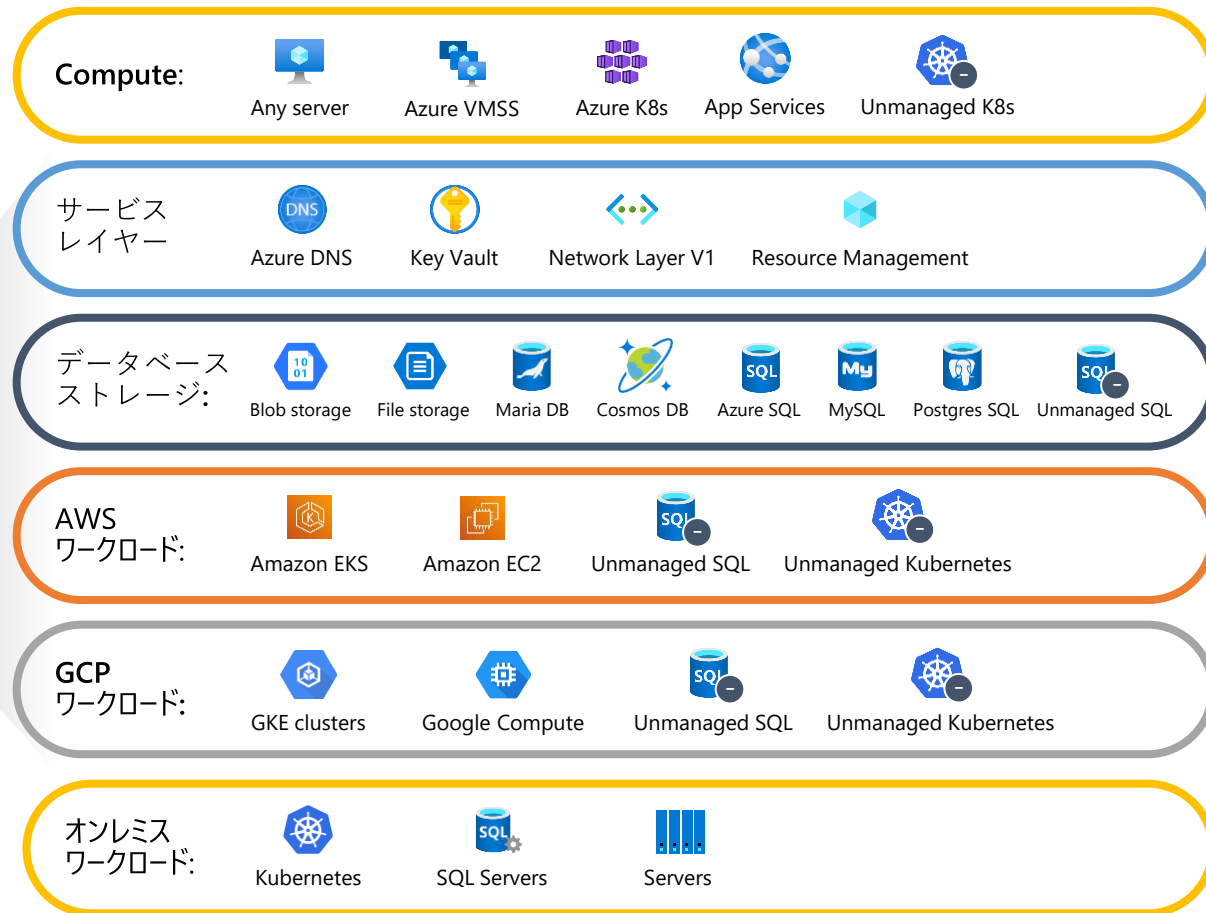
Microsoft Defender for Cloud





Defender シリーズ

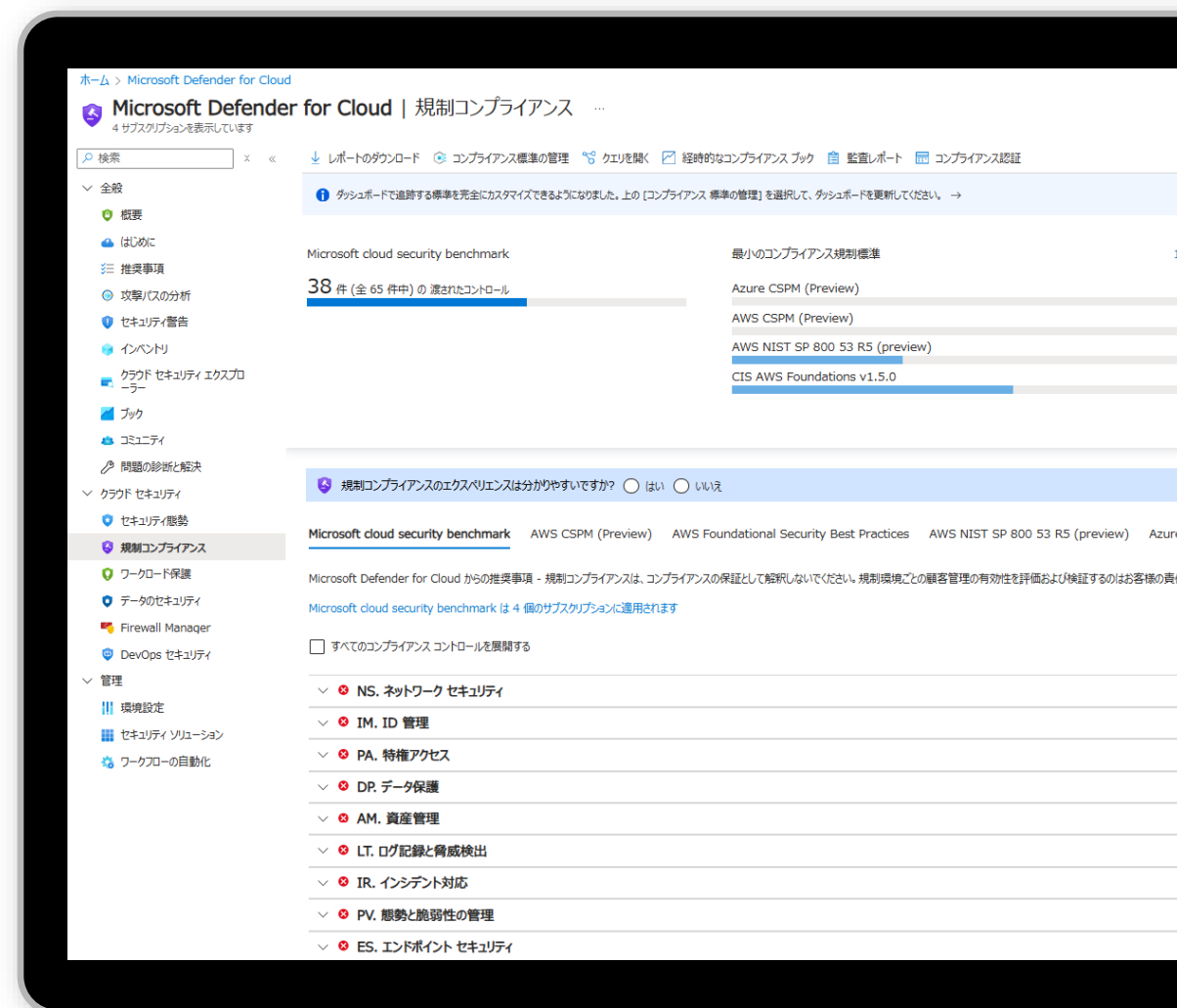
- » Defender for Servers P1 / P2
 - » Defender for Databases
 - » Defender for App Service
 - » Defender for Storage
 - » Defender for Containers
 - » Defender for Key Vault
 - » Defender for Resource Manager
 - » Defender for API
- サーバー保護 (EDR等) 対策
データベースの脆弱性、脅威対策
Web Appサービスの脅威対策
Storage アカウントの脅威対策
AKS,EKS,GKEの脅威対策
Key vaultの振る舞い分析
コントロールプレーンの脅威対策
Azure API Management の脅威対策



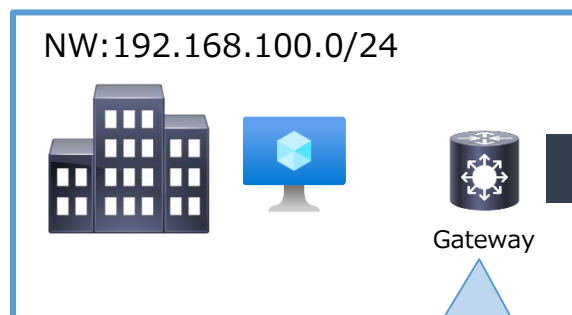
- クラウドリソースの継続的な評価による、コンプライアンス状況の評価と管理
- 業界標準、規制遵守の枠組み、およびベンダーが提供するベンチマークを使用して、セキュリティとコンプライアンスのベストプラクティスを実装する
- 組織固有のニーズに対応するカスタムな推奨事項の作成

幅広い規制コンプライアンスをサポート:

- ✓ CIS
- ✓ PCI
- ✓ NIST
- ✓ SOC
- ✓ ISO
- ✓ HIPAA
- ✓ Local/National compliance standards
- ✓ Microsoft Cloud Security Benchmark
- ✓ AWS Foundational Security best practices



オンプレ拠点



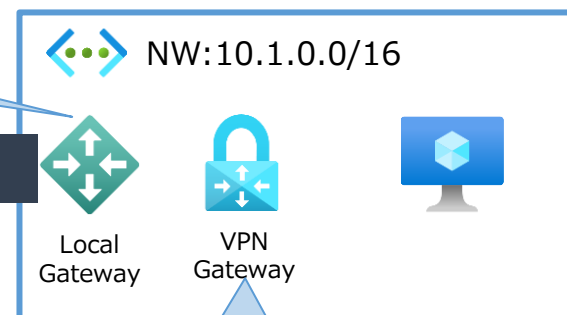
Public IP : YY.YY.YY.YY

S2S接続

オンプレの場合、拠点側のゲートウェイが持つグローバルIPとオンプレ側のアドレス空間をローカルネットワークゲートウェイに指定することで接続できる。

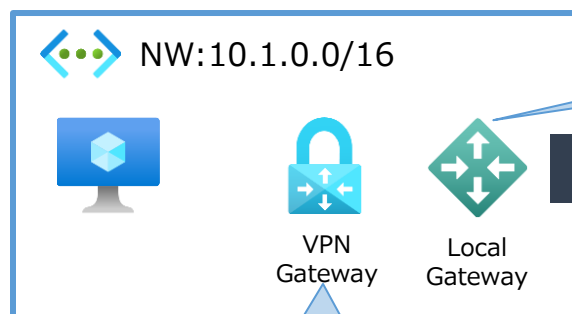
接続先IP : YY.YY.YY.YY
接続先NW : 192.168.100.0/24

Vnet1



Public IP : XX.XX.XX.XX

Vnet1



Public IP : XX.XX.XX.XX

接続先IP : ZZ.ZZ.ZZ.ZZ
接続先NW : 10.2.0.0/16

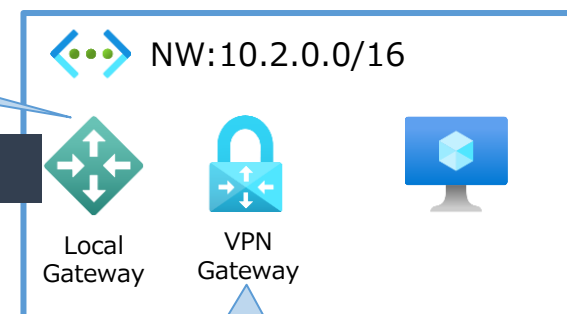
対向NW情報は静的に設定

S2S接続

VNetの場合でも同様に、ローカルネットワークゲートウェイに対向のVNetのVPNゲートウェイのパブリックアドレスと、アドレス空間を指定し、他方のVNetをローカルサイトとしてS2S接続を構築可能。
この接続方法では、接続先のネットワーク情報を静的にしているため、対向VNetのアドレス空間が変更された場合は、手動でローカルネットワークゲートウェイの更新を行う必要がある。

接続先IP : XX.XX.XX.XX
接続先NW : 10.1.0.0/16

Vnet2



Public IP : ZZ.ZZ.ZZ.ZZ

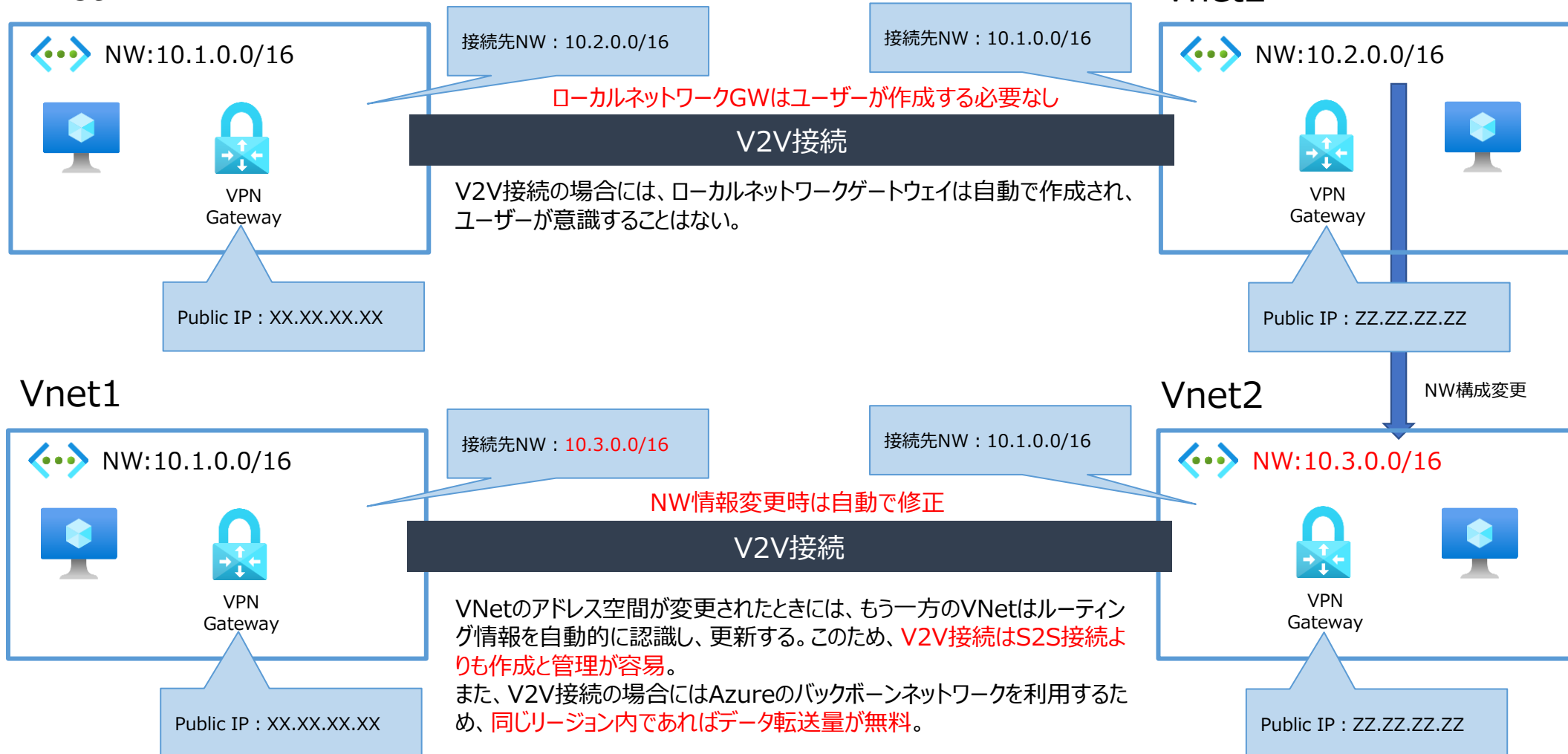
V2V接続 (VNet-to-VNet)

11

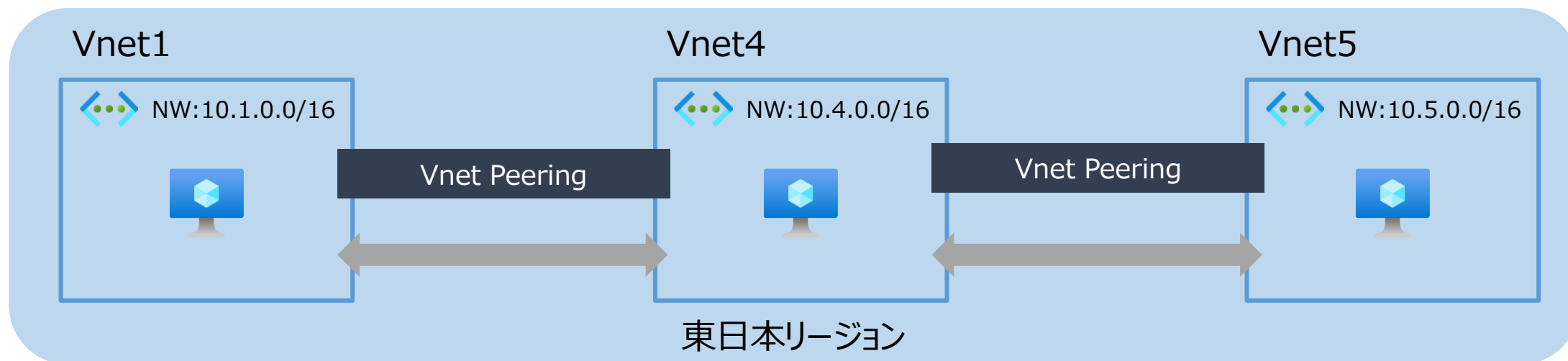
V2V接続はVNet間接続とも呼ばれる。必要なリソースはVPNゲートウェイのみで、実装方法はS2S接続と似ている。どちらの接続もIPsec/IKEのVPNトンネルが確立され、安全な通信機能を提供する。

Vnet1

Vnet2

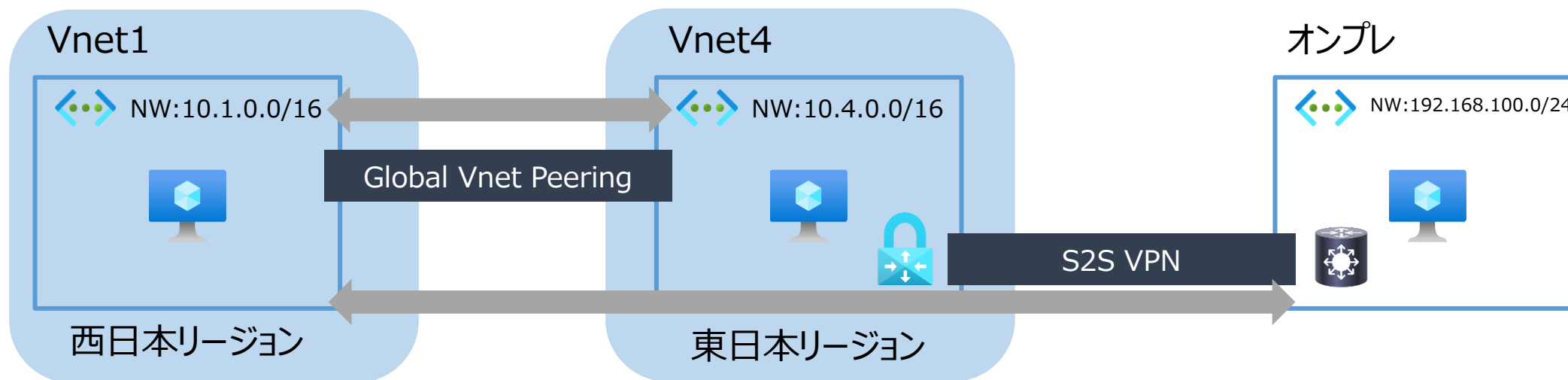


VNetピアリングはVPNゲートウェイを必要とせずVNet同士を接続できる方法。VNet同士での相互通信を実現する。通常VNetピアリングではトラフィックの転送は行わないため、通信したいVNetが複数あるときは個別にピアリングを構成する必要がある。



通信はAzureバックボーンネットワークを利用するため、高速な伝送が可能。V2V接続とは違い、同一リージョン内であっても送受信で料金が発生するが、VPNゲートウェイがボトルネックとならずに高速通信が可能。

グローバルVNetピアリングは異なるリージョンのVNet間を接続できる方式。VNetピアリングと同様でVPNゲートウェイなしで相互接続を構成できる。この場合も通信にはAzureのバックボーンネットワークを利用し、VPNゲートウェイも存在しないため、V2V接続よりも高速な接続が可能。



Vnet1-to-Vnet4

仮想ネットワーク ゲートウェイまたはルート サーバー

☐ この仮想ネットワークのゲートウェイまたはルート サーバーを使用する

☒ リモート仮想ネットワークのゲートウェイまたはルート サーバーを使用する

☐ なし (既定)

Vnet4-to-Vnet1

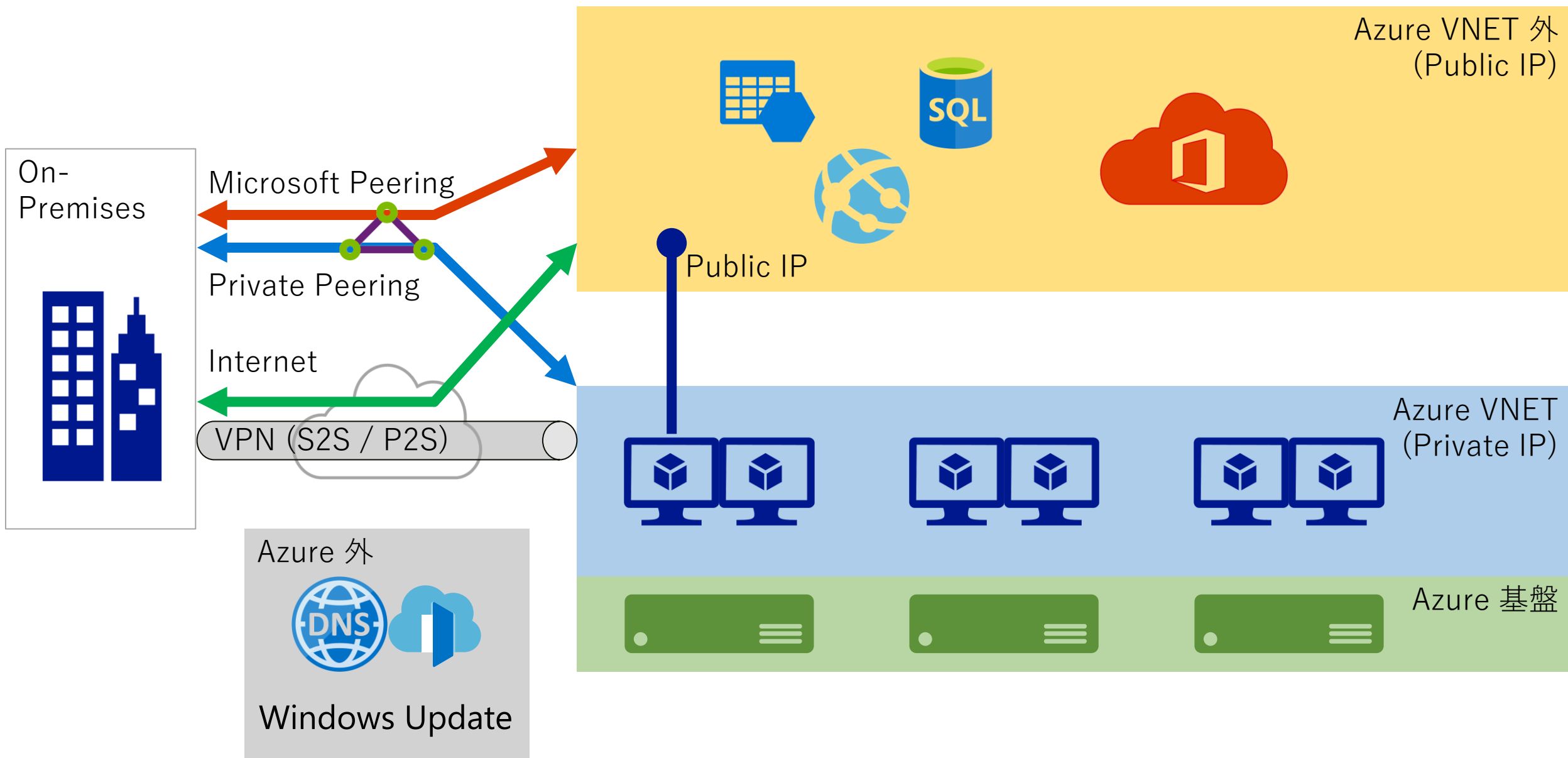
仮想ネットワーク ゲートウェイまたはルート サーバー

☒ この仮想ネットワークのゲートウェイまたはルート サーバーを使用する

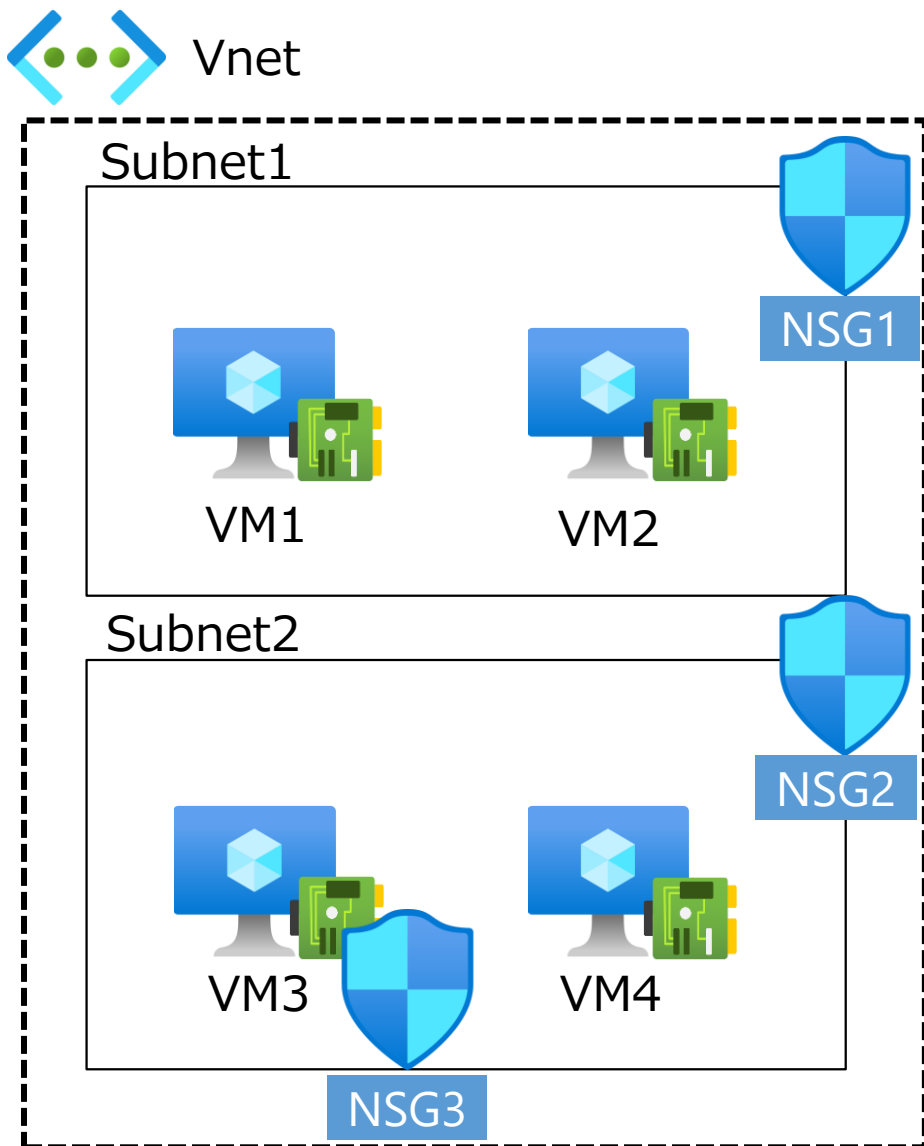
☐ リモート仮想ネットワークのゲートウェイまたはルート サーバーを使用する

☐ なし (既定)

同一リージョン内のVNet同士で構成するVNetピアリングの場合は、どちらかのVNet内にVPNゲートウェイが存在すれば、リモートゲートウェイ転送を有効化する設定を行うことで、トラフィックの転送を行うことができる。以前は異なるリージョン間でのリモートゲートウェイ転送を利用できなかったが、現在は可能。よって、上記構成において、西日本リージョンからオンプレへの通信は可能となる。



NSGまとめ



NSGはSubnet、NICに対して設定できる
→Vnetではない

考え方としては、**VM主体**で受信時はSubnet、NICに割り当てられているNSGを適用する。送信時はNIC、Subnetに割り当てられているNSGを適用する。

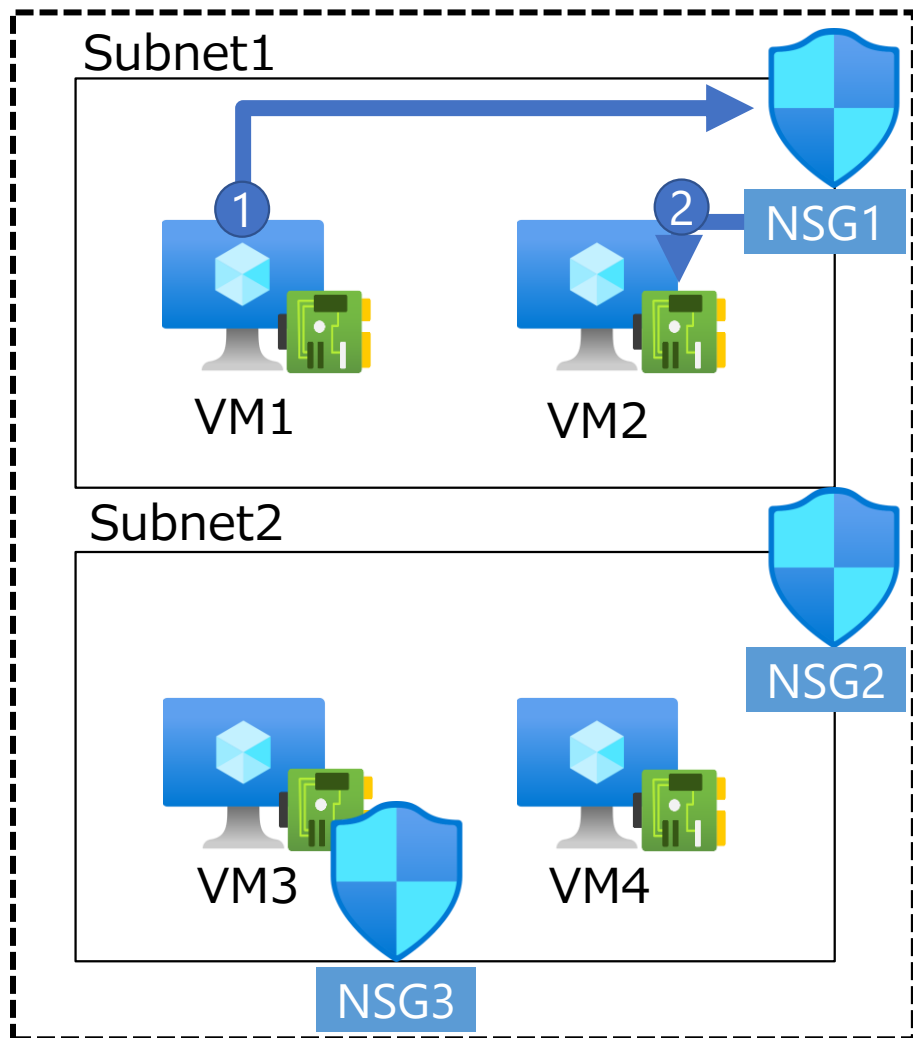
■ 受信トラフィック

受信トラフィックの場合、Azure は、サブネットに関連付けられているネットワーク セキュリティ グループがあれば、まずその規則を処理し、次にネットワーク インターフェイスに関連付けられているネットワーク セキュリティ グループがあれば、その規則を処理します。

■ 送信トラフィック

送信トラフィックの場合、Azure はネットワーク インターフェイスに関連付けられているネットワーク セキュリティ グループがあれば、まずその規則を処理し、次にサブネットに関連付けられているネットワーク セキュリティ グループがあれば、その規則を処理します。

NSGまとめ



VM1 to VM2

①NSG1の送信ルール（Subnet1に紐づいている）

②NSG1の受信ルール（Subnet1に紐づいている）

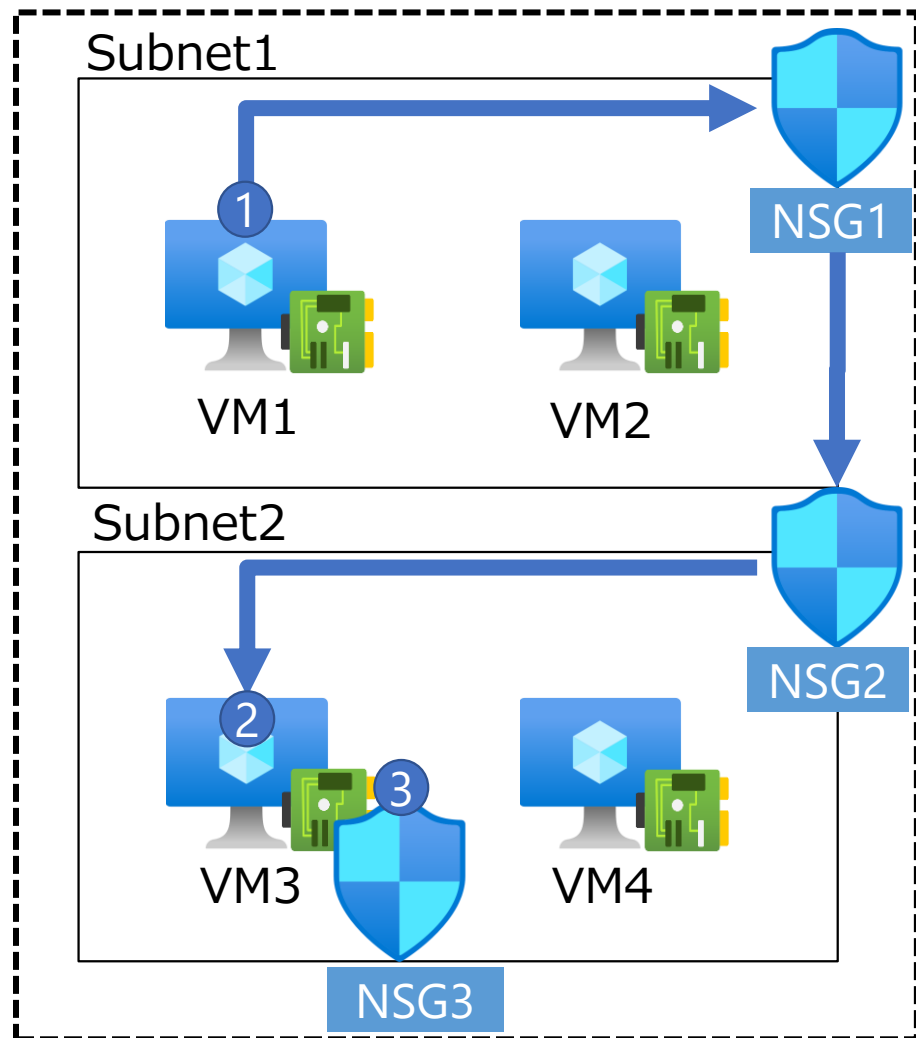
が評価される

→同じサブネット内であれば、隣のサーバにはフリーで繋がるわけではない。デフォルトルールで仮想ネットワーク間の通信は全ポート送受信ともに「許可」設定になっているため自在に接続ができているように見えている。

NSGまとめ



Vnet



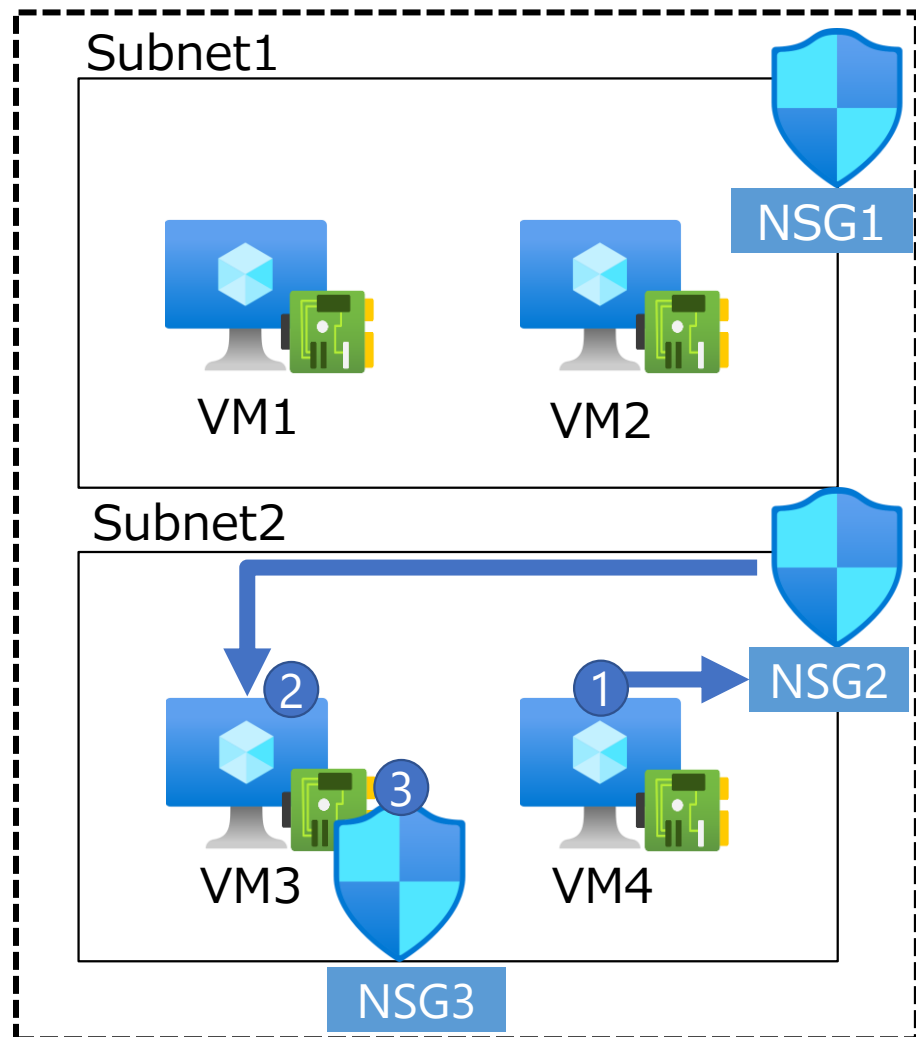
VM1 to VM3

- NSG1の送信ルール (Subnet1に紐づいている)
 - NSG2の受信ルール (Subnet2に紐づいている)
 - NSG3の受信ルール (VM3のNICに紐づいている)
- が評価される

NSGまとめ



Vnet

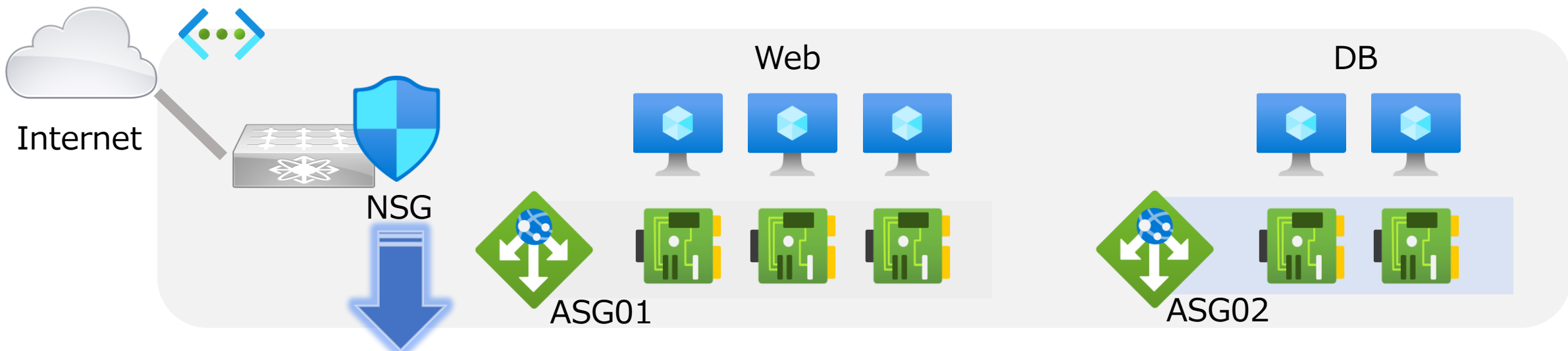


VM4 to VM3

- ①NSG2の送信ルール (Subnet2に紐づいている)
 - ②NSG2の受信ルール (Subnet2に紐づいている)
 - ②NSG3の受信ルール (VM3のNICに紐づいている)
- が評価される

ASGとは

- NSG(ネットワーク セキュリティ グループ)の拡張機能。
- 仮想マシン(NIC)をグループ化する事ができ、NSGの送信元/宛先として適用できる。同じ役割のサーバー同士をグルーピングする事で、アプリケーションの通信パターンに適応したNSG設定が容易になる。
- ※ASGは、同一リージョン内のNICを登録できます。



Source	Destination	Action
Internet	ASG01	Allow
ASG01	ASG02	Allow
Any	Any	Deny

ASGまとめ

- ASGのメリット
 - NSGルールの行数を削減できる
 - 保護対象サーバーが追加された際にも、NSGルールを変更する必要がない
 - 保護対象サーバーのIPアドレスを意識する必要がない
 - マイクロセグメンテーション
- ASGを有効にするための、3つの条件
 1. 保護対象サーバーのNICにASGが適用されている事
 2. 適用したASGが、NSGのルールに適用されている事
 3. NSGが保護対象サーバー上のサブネットに適用されている事

※NICに対し、ASGを複数適用する事が可能

※3つの条件を全て満たした場合のみ、ASGが適用される。

NSG規定ルール

受信セキュリティ規則

優先度	名前	ソース	宛先	サービス	アクション
65000	AllowVnetInBound	VirtualNetwork	VirtualNetwork	任意/任意	Allow
65001	AllowAzureLoadBalancerInBound	AzureLoadBalancer	任意	任意/任意	Allow
65500	DenyAllInBound	任意	任意	任意/任意	Deny

送信セキュリティ規則

優先度	名前	ソース	宛先	サービス	アクション
65000	AllowVnetOutBound	VirtualNetwork	VirtualNetwork	任意/任意	Allow
65001	AllowInternetOutBound	任意	Internet	任意/任意	Allow
65500	DenyAllOutBound	任意	任意	任意/任意	Deny

サービスタグ考察

VirtualNetwork

- 仮想ネットワーク内の同一サブネット
- 仮想ネットワーク内の別サブネット
- 仮想ネットワークピアリングで接続された別仮想ネットワーク
- Site to Site接続された別の仮想ネットワーク(Azure、オンプレ)
- Point to Site接続されたクライアント側PC
- Express Routeによって接続されたオンプレ側ネットワーク
- ホストの仮想 IP アドレス、およびユーザーが定義したルートで使用するアドレス プレフィックス

よってインターネット以外すべてが該当する。安易にVirtualNetworkタグを使って受信規則をフルオープンにしまうと、社内の誰からも、どこからもアクセスできてしまう。

AzureLoadBalancer

Azure インフラストラクチャのロード バランサー。このタグは、Azure の正常性プローブの送信元となるホストの仮想 IP アドレス (168.63.129.16) に変換される。これにはプローブ トラフィックのみが含まれ、バックエンドリソースへの実際のトラフィックは含まれない。Azure Load Balancer を使っていない場合は、この規則をオーバーライドできます。

Internet

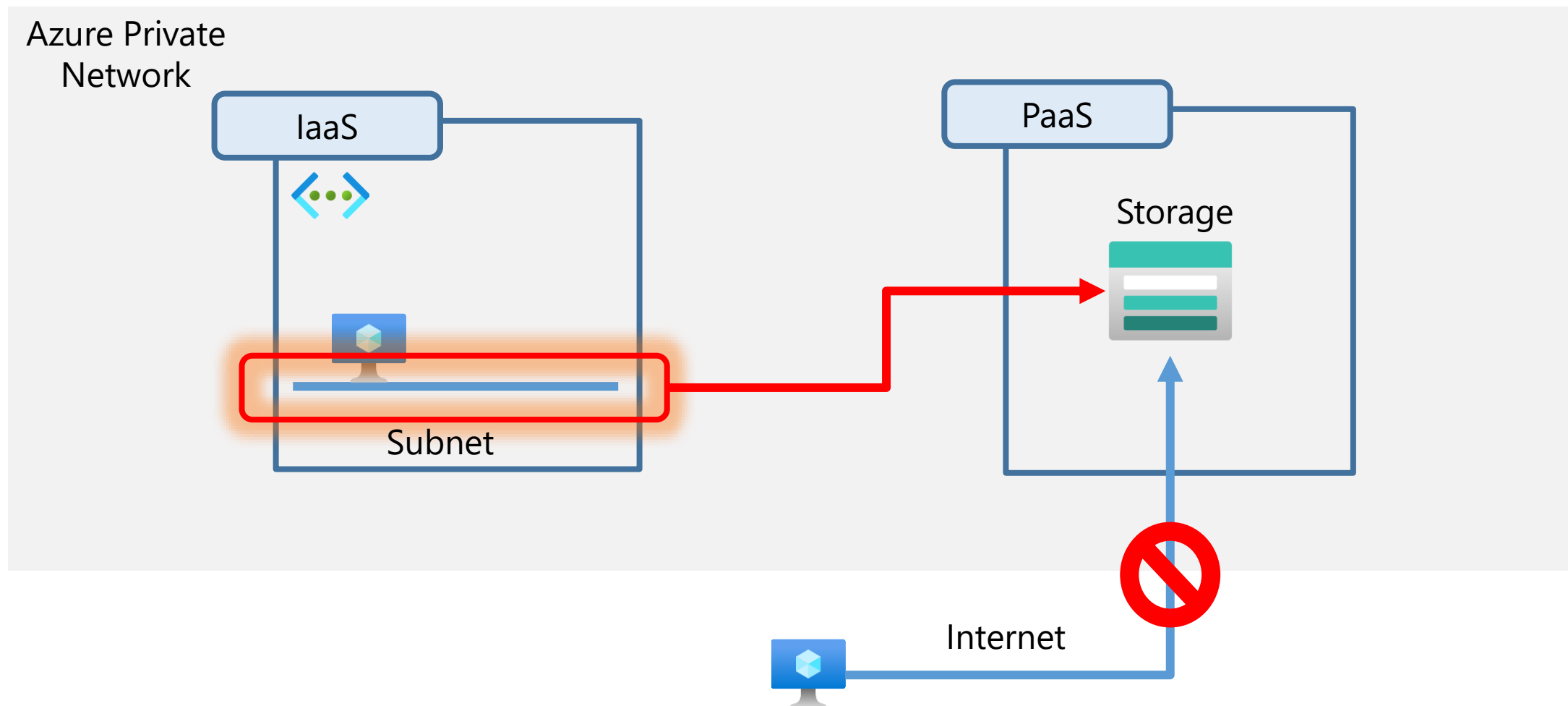
パブリック インターネットによってアクセスできる仮想ネットワークの外部の IP アドレス空間。このアドレス範囲には、**Azure によって所有されているパブリック IP アドレス空間が含まれている。**

送信規則でInternet向けの通信を遮断した場合、以下の事象が発生する。

- 仮想マシンに拡張機能(BGInfoなど)の追加操作をしてもデプロイが正常終了しない
- 仮想マシンの診断機能(Diagnostics)を有効にしてもストレージアカウントに結果が出力されない
- LogAnalyticsが有効なのにログが転送されてこない
- 仮想マシンのバックアップが正常に完了しない

これらは全て仮想マシンのOS内からAzureのPaaSサービス(ストレージアカウント含む)への接続が行えないため発生する。

Azure上の各種PaaS系サービスとの接続を、**仮想ネットワーク(サブネット)からの接続に限定**してしまうセキュリティ機能



- **プライベートエンドポイント**とは、プライベートリンクを実現するための仕組みの一つで、プライベートリンクサービスにプライベートで安全に接続するネットワークインターフェイスを提供する。
- プライベートリンクサービスとは**プライベートリンク**を使用するサービスのことで、Azure Storage や Azure SQL Database などの定義済みのプライベートリンクリソースなどを指す。

