

AZ-104

補足資料

Azure接続のデバイス管理

BYODデバイスの組織での管理

Azure AD 登録 (Azure AD registered)

- 会社で管理されていないデバイス・組織外のデバイスを想定した機能
- PC へのログオン方法は従来と変わらない
(ローカルアカウント or AD アカウント)
- Windows 10 のみ対応
- 主に外部組織のリソースへの SSO を得る場合に利用されるケースが多い

組織で管理されたWindowsデバイスからのアクセスのサポート

Azure AD 参加 (Azure AD joined)

- Windows PC をクラウドのみで管理するパターン。デバイスの情報は Azure AD に保持される
- PC へのログオンは Azure AD の ID で行う (ykodama@microsoft.com など)
- Windows 10のみがこの方式を利用可能
- 既にオンプレミス ADに参加している PC は重ねて Azure AD Joinすることはできない
- PC へのポリシー適用は MDM ツール (Intuneなど) により行われる

ハイブリッド Azure AD 参加 (Hybrid Azure AD joined)

- 既存 Domain Joined 状態はそのままに Azure AD にも登録
- オンプレミス AD の ID を利用して PC にログオン (UPN, sAMAccountName など)
- Windows 7 / 8.1 / 10 に対応
- オンプレ AD と Azure AD 両方にデバイス情報を保持
- PC へのポリシー適用は GPO にて実施

Microsoft Entra ID (Azure Active Directory)

- Azureを利用するにはサブスクリプションが必要
 - リソースの支払いに紐づける
- テナント (Azureを使用する際に作成される利用範囲)
 - サブスクリプションが紐づけられる (サブスクリプションは複数紐づけできる)
- テナントのリソースはAzure階層で構成される
 - Azure階層ではAzure Policy、Azure RBACが使用される
 - Azure階層で構成された内容は下位の階層に継承される
 - Azure階層は「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」

テナントとAzure階層

- Azure AD (テナント)

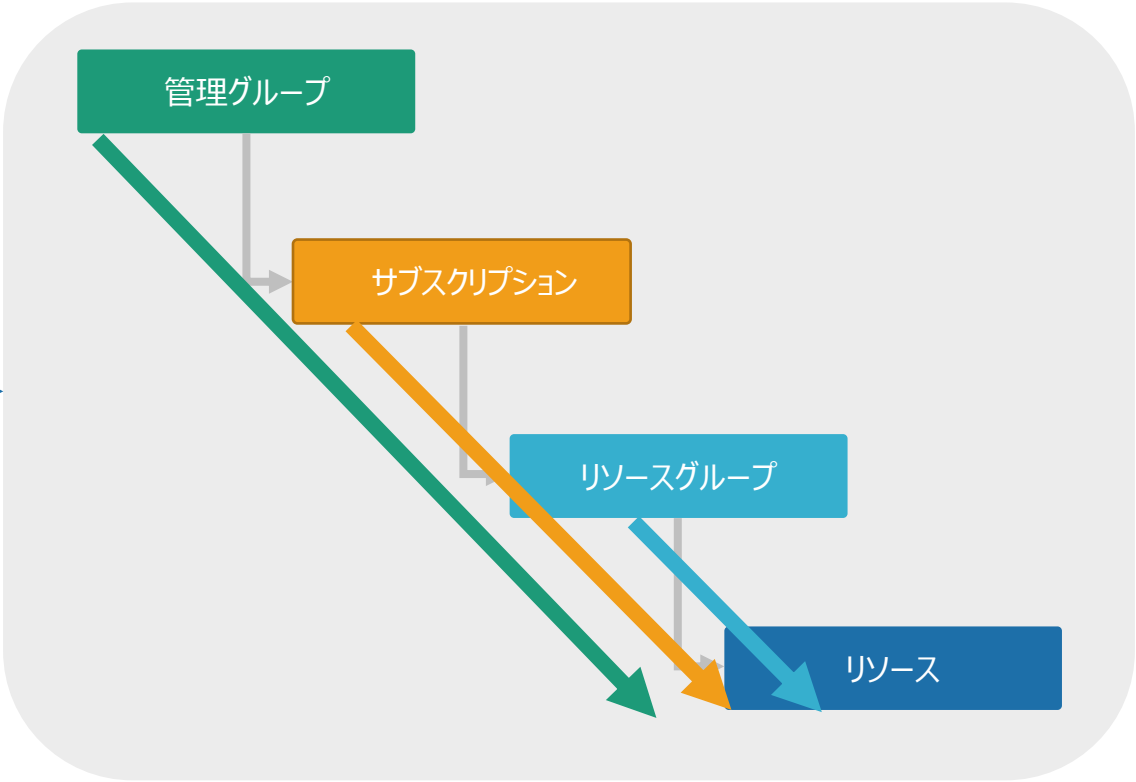
テナント

- Azure AD ロール
 - グローバル管理者
 - セキュリティ管理者

適用範囲はテナント
ロールはAzure AD RBAC
を使用している

- Azure 階層

適用範囲は階層以下に継承
Azure RBAC
Azure Policy
を適用できる



Azure Policy の役割

• リスク

- 将来の不確定な状況
- 脅威（外的要因）×脆弱性（内的要因）
- 外的要因はアンタッチャブルなので、脆弱性を何とかすることができる

• コンプライアンス

日本ではガイドライン、ルールと呼ばれることが多い

- 守るべきルール
- ルールは「脆弱性を減らす」ために存在
- セキュリティベースライン（MCSB）、ISO27001、NIST SP800、HIPPA...

• ガバナンス（守るべき基準・規範 + 守らせる仕組み）

- （改善を目的として）、決められたプロセス、ルールが確実に実施されていることを確認、監視するプロセス

チェックツールや是正ツール、プロセスなどにより構成される（Azure Policyが該当する）
ガードレールと呼ばれることが多い

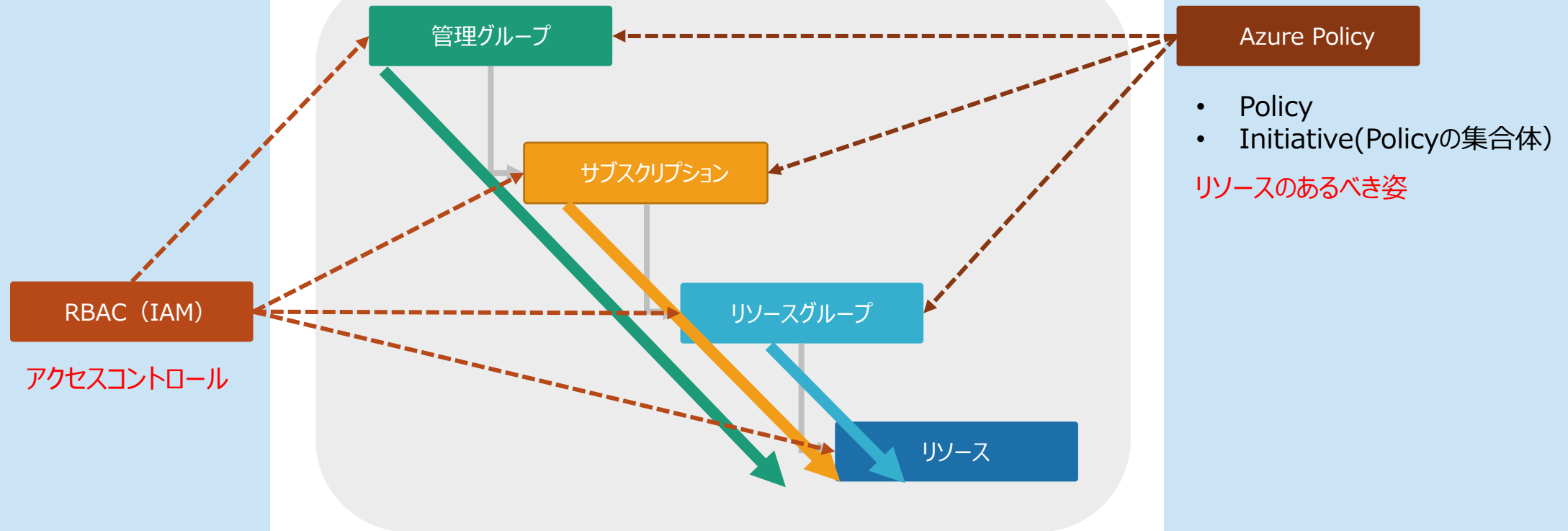
Azure階層とRBACロール

Azure Blueprints

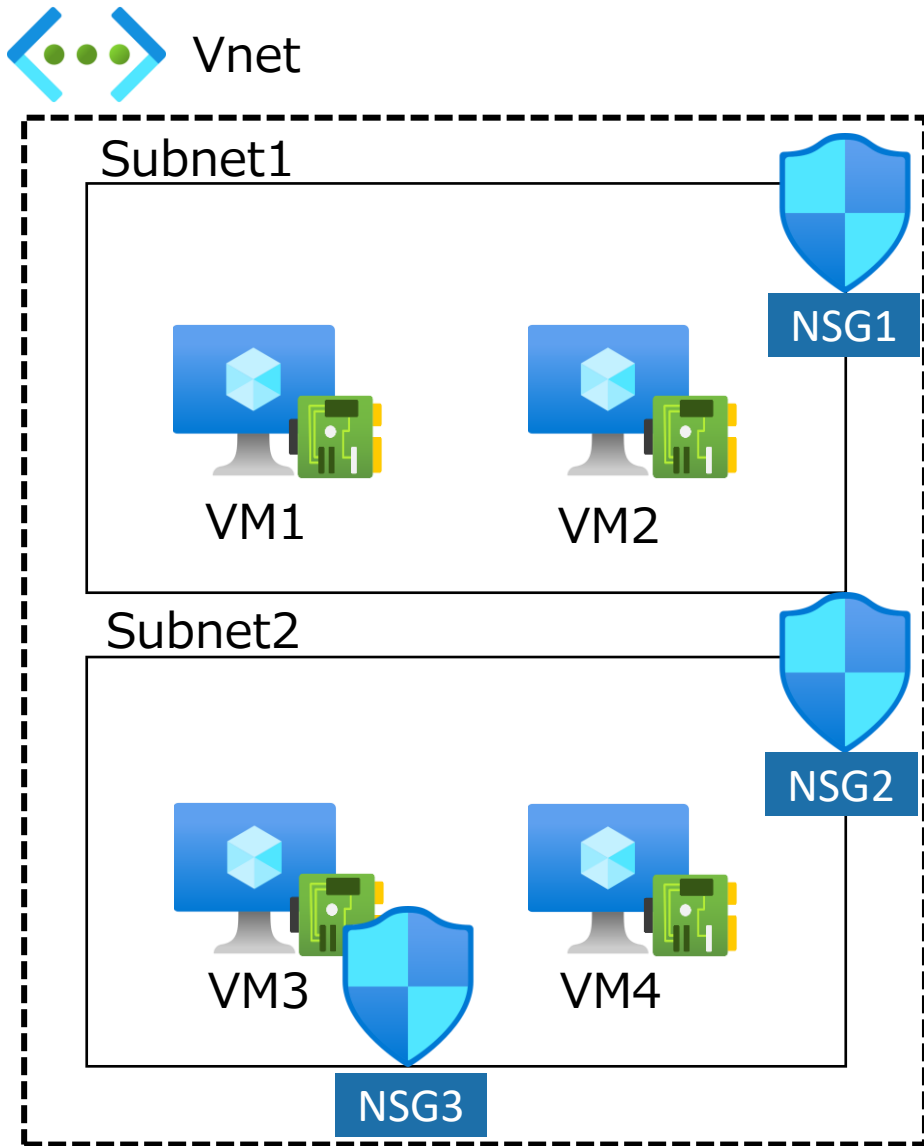
- 組織のコンプライアンス設定可能
- バージョン設定
- RBACの拒否設定

ARM Template

Azureのリソースを定義したJSONファイル



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。

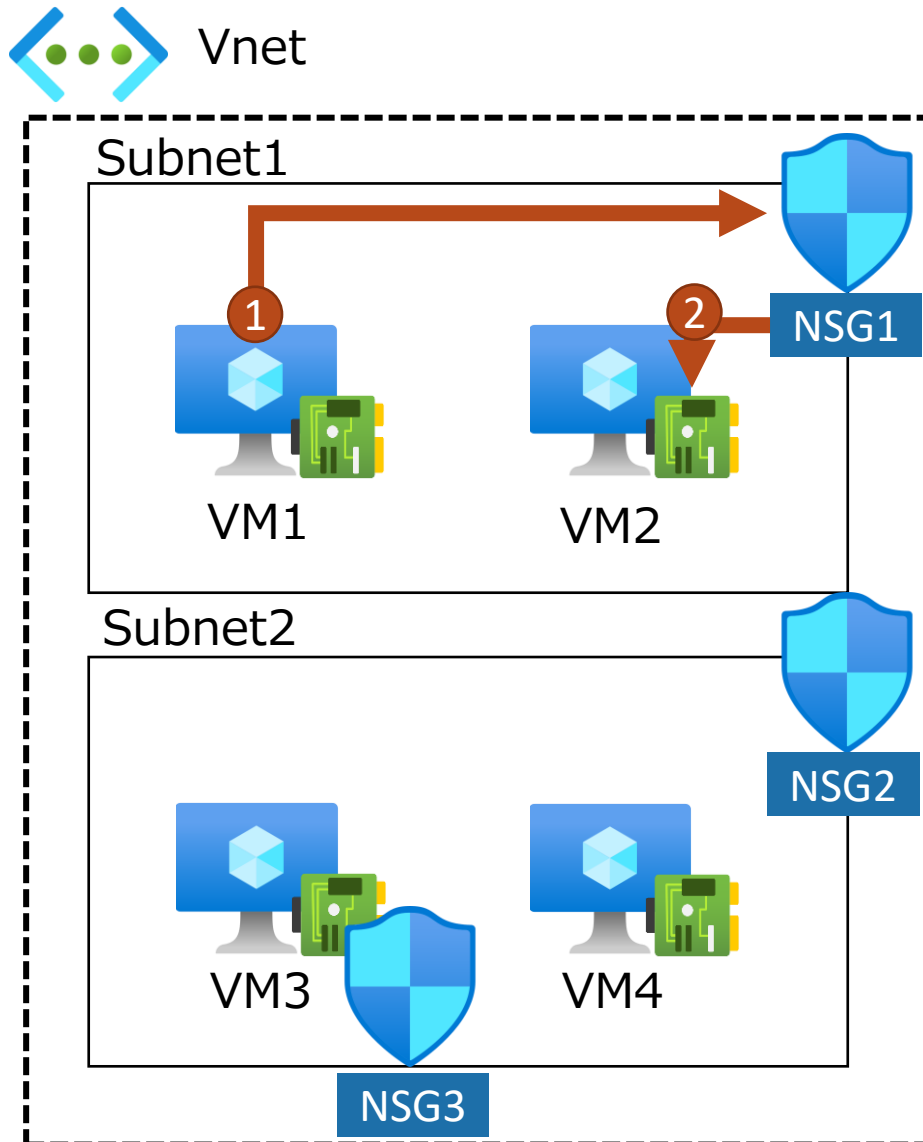
■ 受信トラフィック

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

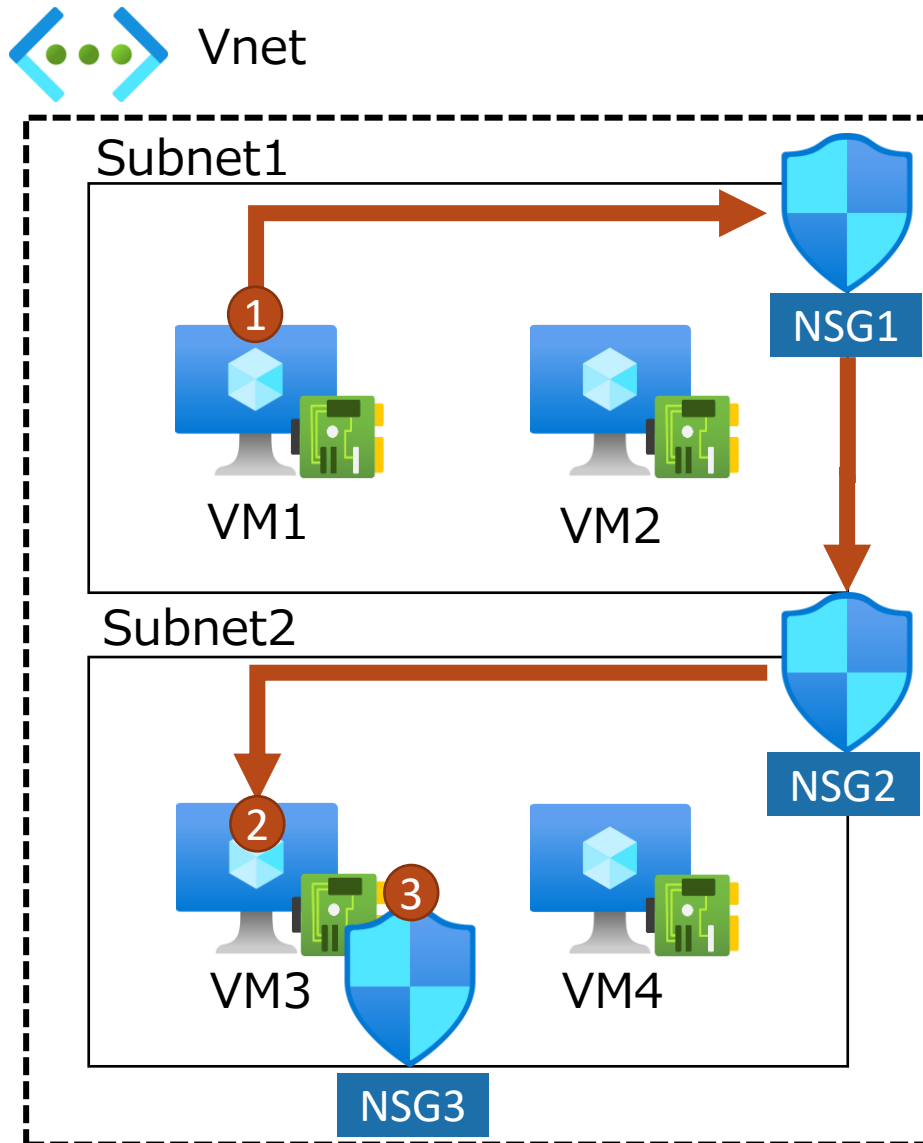
①NSG1の送信ルール（Subnet1に紐づいている）

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。

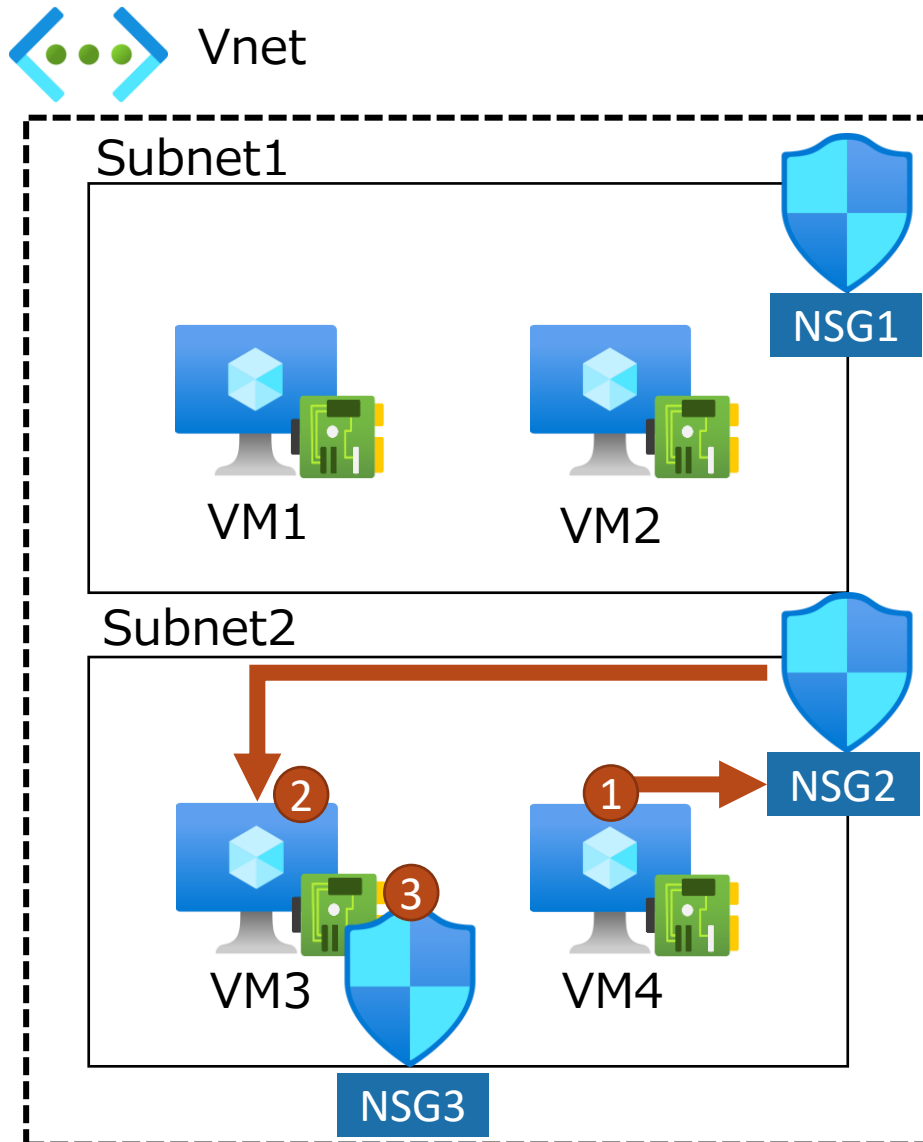
NSGまとめ



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

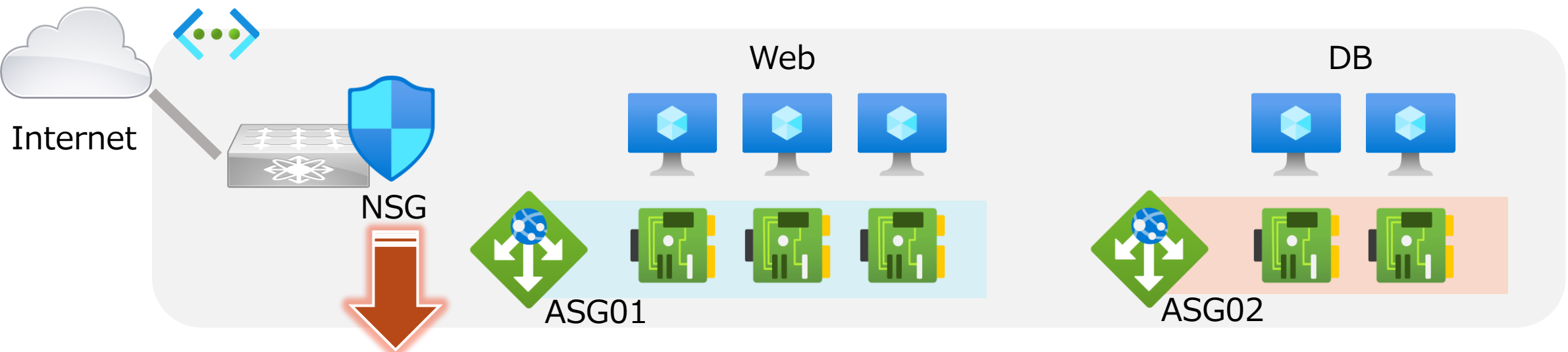


VM4 to VM3

- 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。

VNet接続まとめ

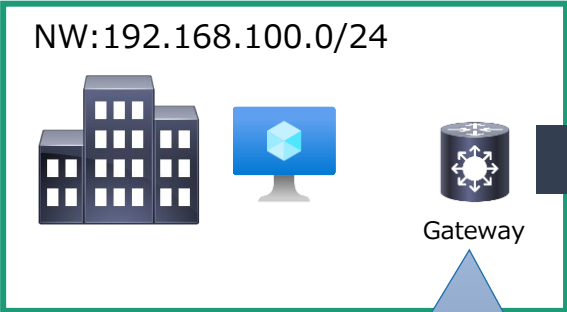
- VNetは独立しており、異なるVNetとは通信できない
- VNet間を接続することで、VNet間の通信ができる
 - Site-to-Site (S2S接続)
 - Vnet-to-Vnet (V2V接続)
 - Vnet ピアリング
 - グローバル Vnet ピアリング

VPN接続の種類

- 安全な拠点間通信を可能にするVPN接続サービスは主に以下の3種類
 - インターネットVPN
 - インターネット上に、仮想のネットワーク環境を構築
 - IP-VPN
 - 通信事業者の閉域IP網を使用して、仮想のネットワークを構築
 - 広域イーサネット
 - 通信事業者の専用回線、あるいは閉域網を利用して仮想のネットワークを構築

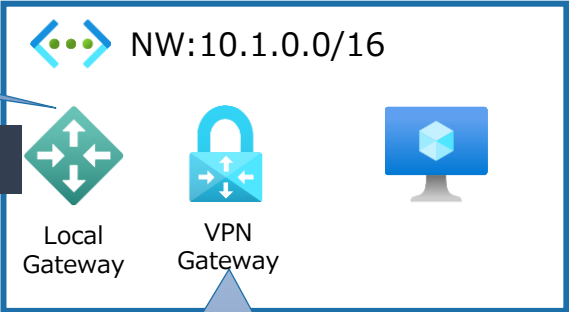
S2S接続 (Site-to-Site)

オンプレ拠点



Public IP : YY.YY.YY.YY

Vnet1



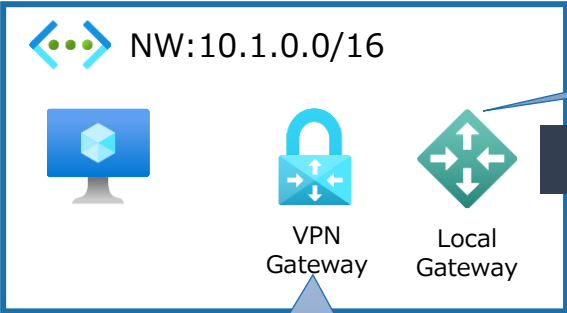
Public IP : XX.XX.XX.XX

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。

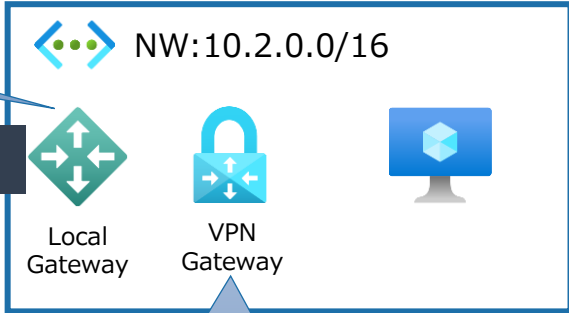
接続先IP : YY.YY.YY.YY
接続先NW : 192.168.100.0/24

Vnet1



Public IP : XX.XX.XX.XX

Vnet2



Public IP : ZZ.ZZ.ZZ.ZZ

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。

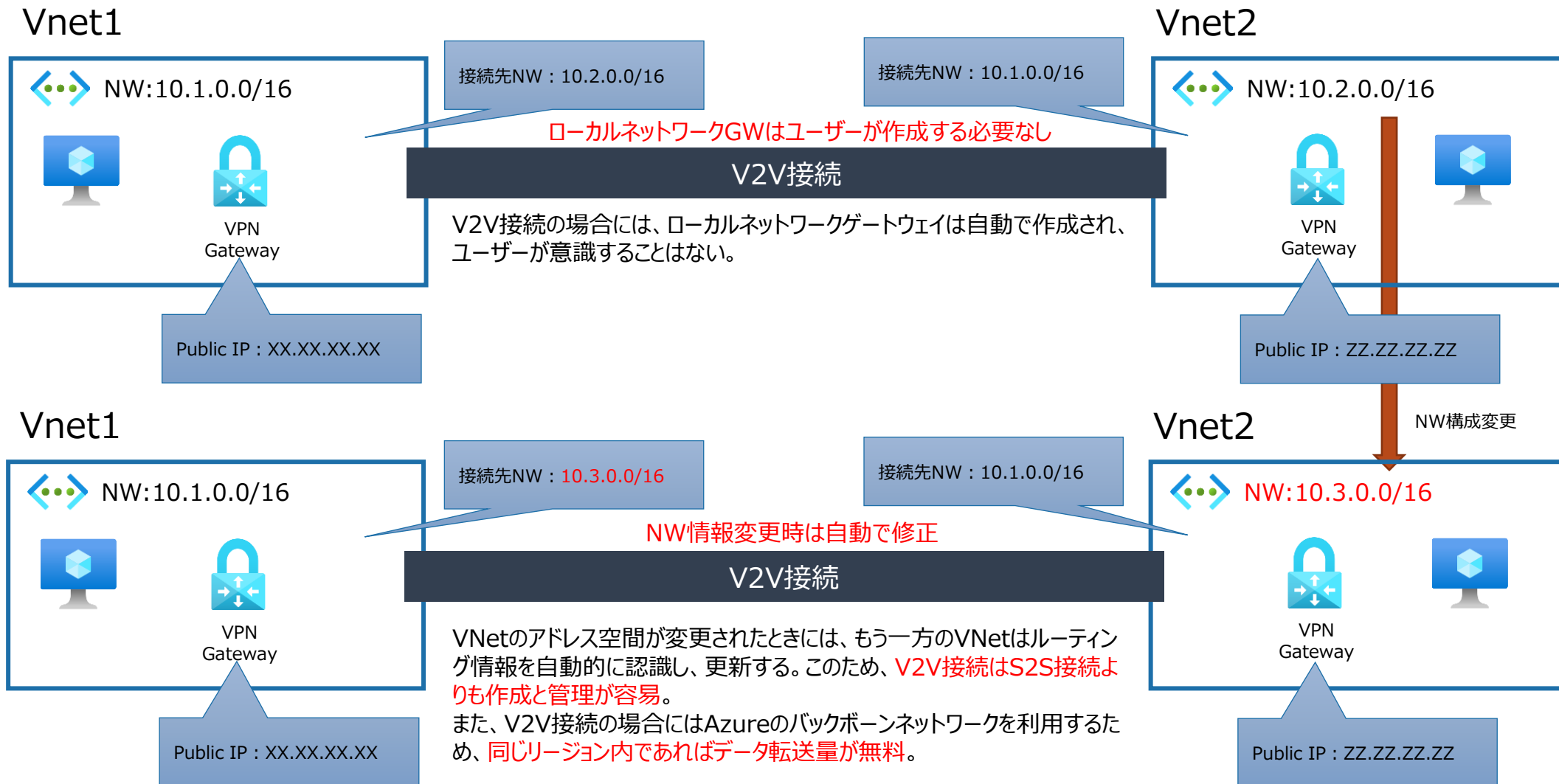
対向NW情報は静的に設定

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

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

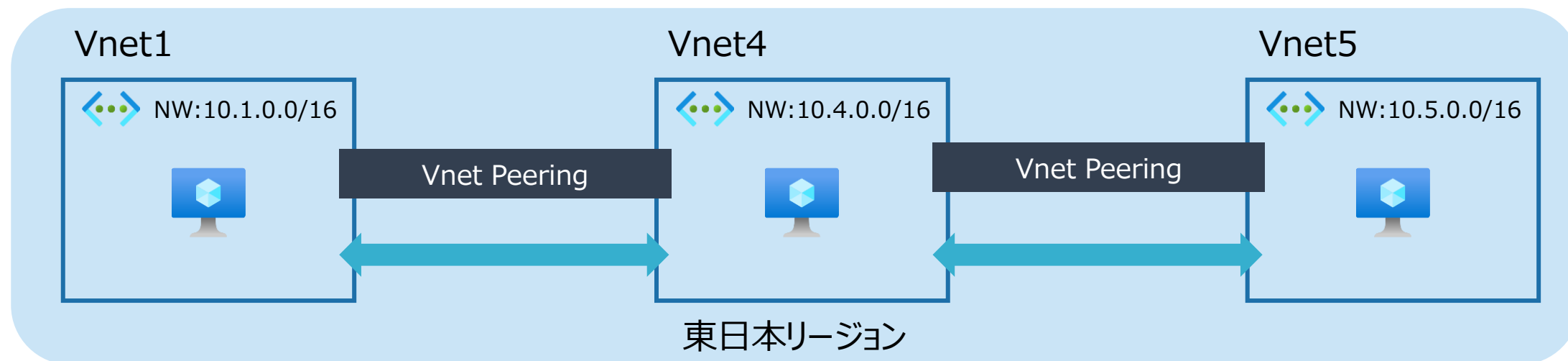
V2V接続 (VNet-to-VNet)

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。



Vnetピアリング

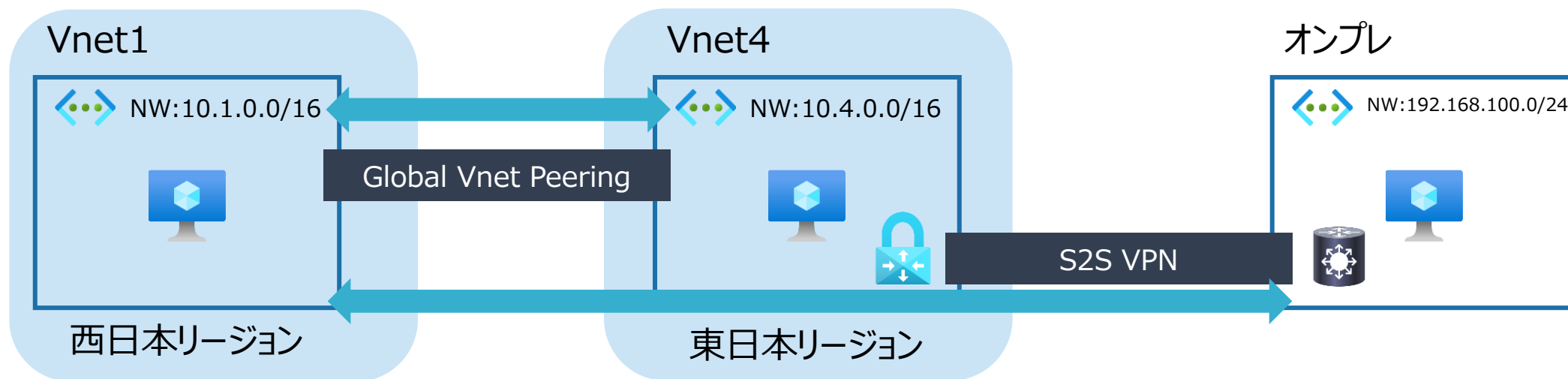
VNetピアリングはVPNゲートウェイを必要とせずVNet同士を接続できる方法。VNet同士での相互通信を実現する。通常VNetピアリングではトラフィックの転送は行わないため、通信したいVNetが複数あるときは個別にピアリングを構成する必要がある。



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

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)

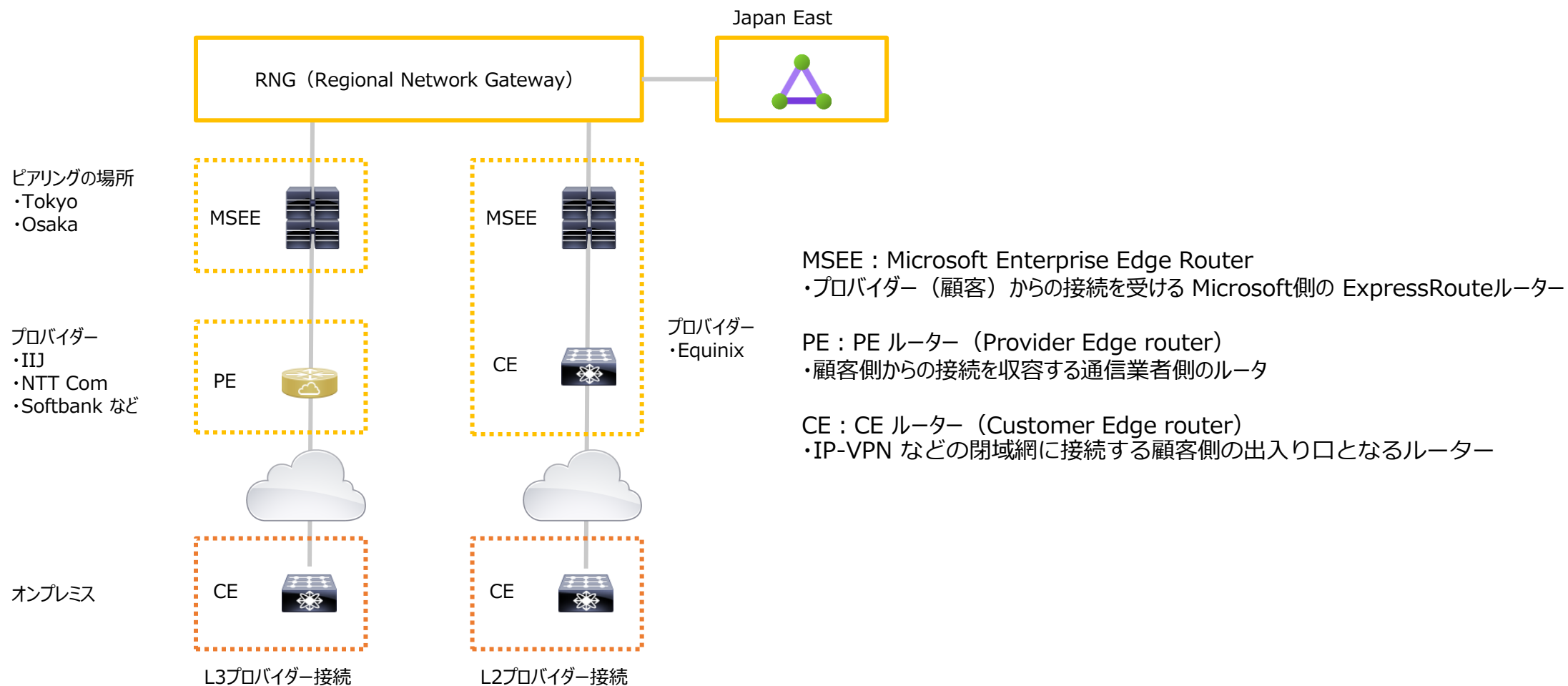
同一リージョン内のVNet同士で構成するVNetピアリングの場合は、どちらかのVNet内にVPNゲートウェイが存在すれば、リモートゲートウェイ転送を有効化する設定を行うことで、トラフィックの転送を行うことができる。以前は異なるリージョン間でのリモートゲートウェイ転送を利用できなかったが、現在は可能。よって、上記構成において、西日本リージョンからオンプレへの通信は可能となる。

ExpressRoute物理構成

L2接続プロバイダー：CEとMSEEを直接接続する構成。CEルータを自身で設定できるので、自由にルーティング設計ができる。

L3接続プロバイダー：CEは、PEと接続するだけでOK。ルーティング設定は、プロバイダーにおまかせできる。

※RNG：リージョン内に複数存在するDCを束ねる地域閉域網。Azureバックボーンへの接続もここを経由して行われる。



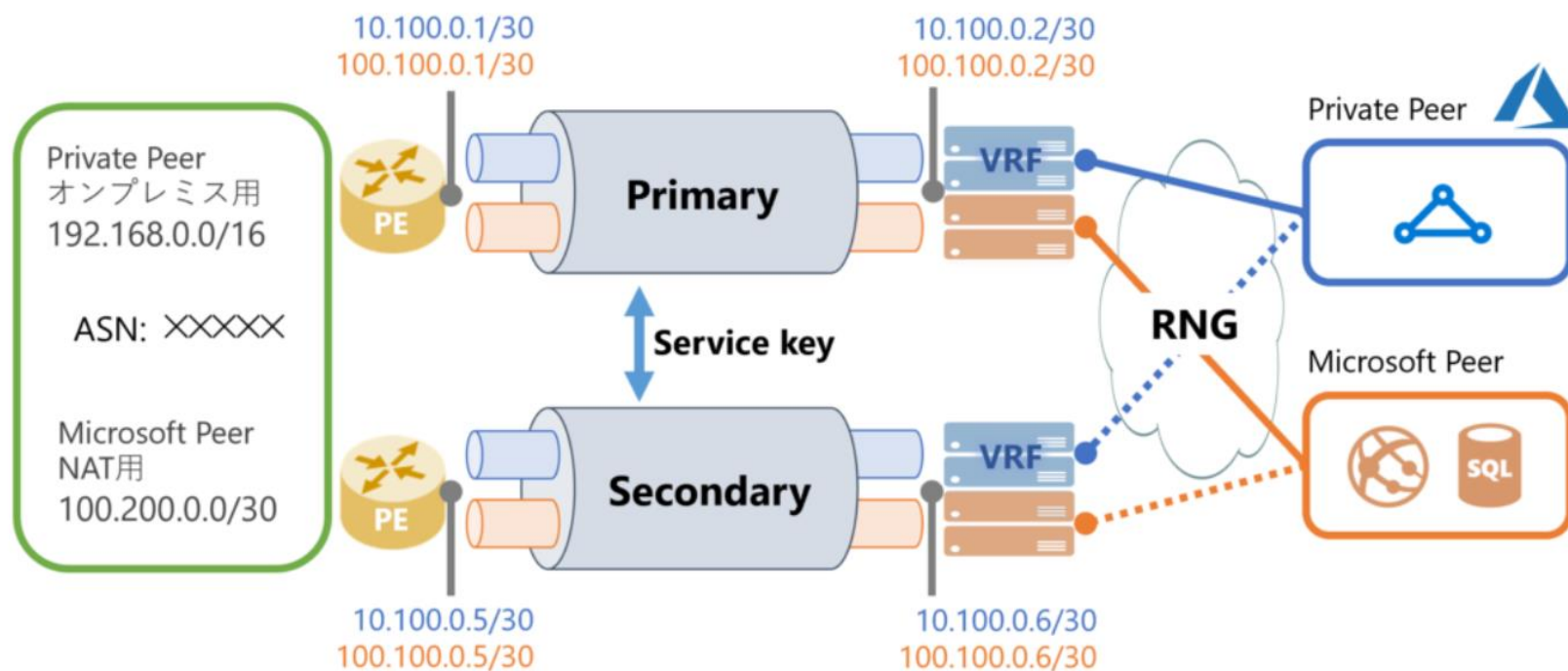
ExpressRoute ピアリング 接続図

Privateピアリング

- ・IaaS環境へ接続。Vnetに接続する際に利用
- ・[/30]のプライベートIPが2つ必要

Microsoftピアリング

- ・PaaS、MSサービス(O365,SharePointなど)に接続する際に利用
- ・[/30]のパブリックIPが2つ、NAT用のパブリックIP[/30]以上が必要
- ・AS番号が必要。プライベートでも可。パブリックASの場合、AS_PATHプリバンドが利用可



オンプレミス～Privateピアリング間の通信

VnetのIPセグメントがオンプレミス ルータに伝播される。
オンプレミスで利用しているプライベートIPのまま、Azure上のVMと通信が可能

オンプレミス→Microsoftピアリング向けの通信

NAT用IPセグメントがMicrosoftピアリングに伝播される。
送信元のプライベートIPをNAT用パブリックIPにてSNAT(PAT)します。

Microsoftピアリング→オンプレミス向けの通信

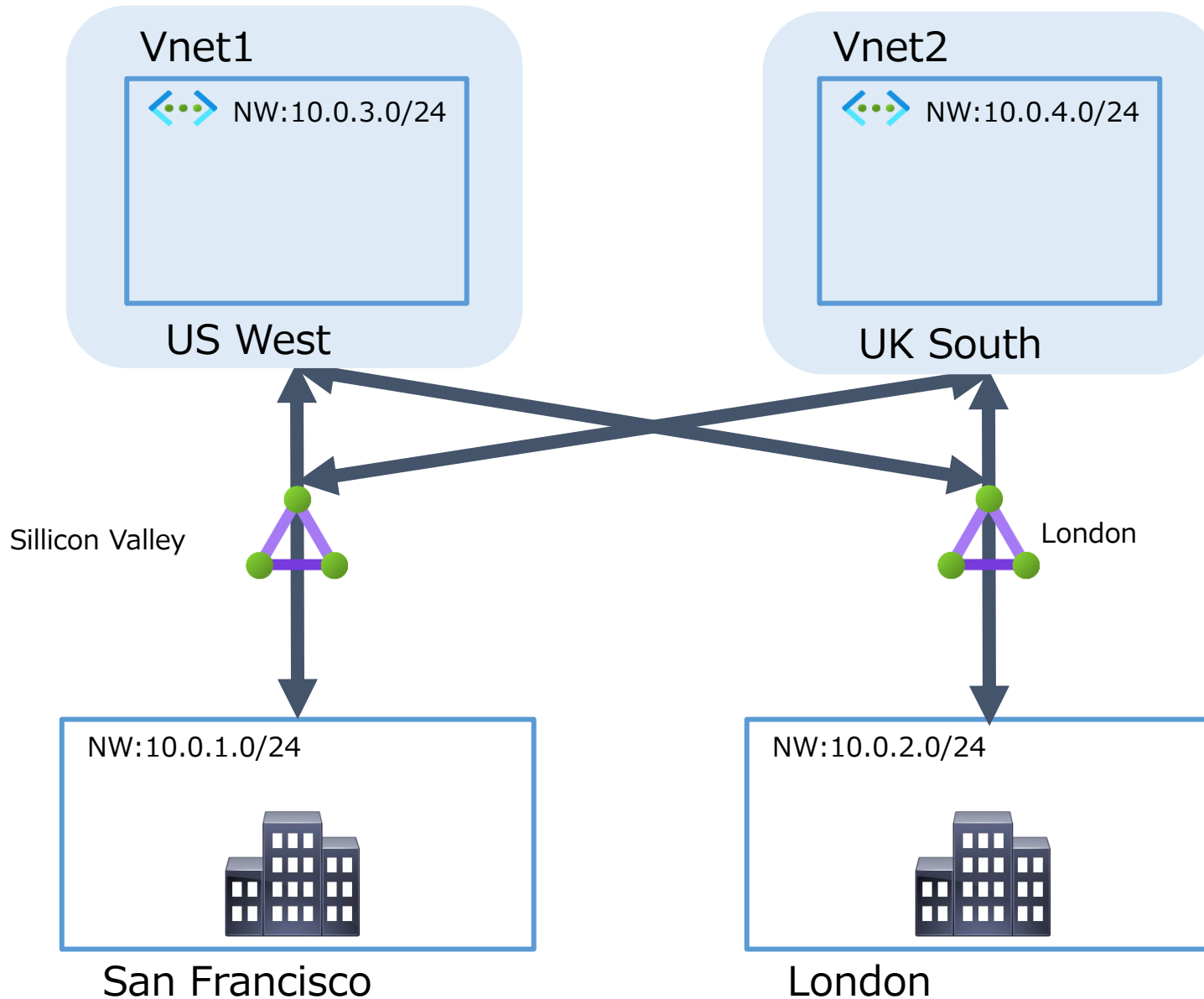
ルートフィルターで指定したパブリックIPがオンプレミス ルータに伝播される。
宛先となるNAT用パブリックIPをIPフォワードでDNATします。

Privateピアリング～Microsoftピアリング間の通信

両方のルートはPEにて集約されるため、PE経由となる。

※強制トンネリング用のデフォルトルートはPEから伝播される。
※強制トンネリングを有効にすると、デフォルトルートがMSEEに変更される。

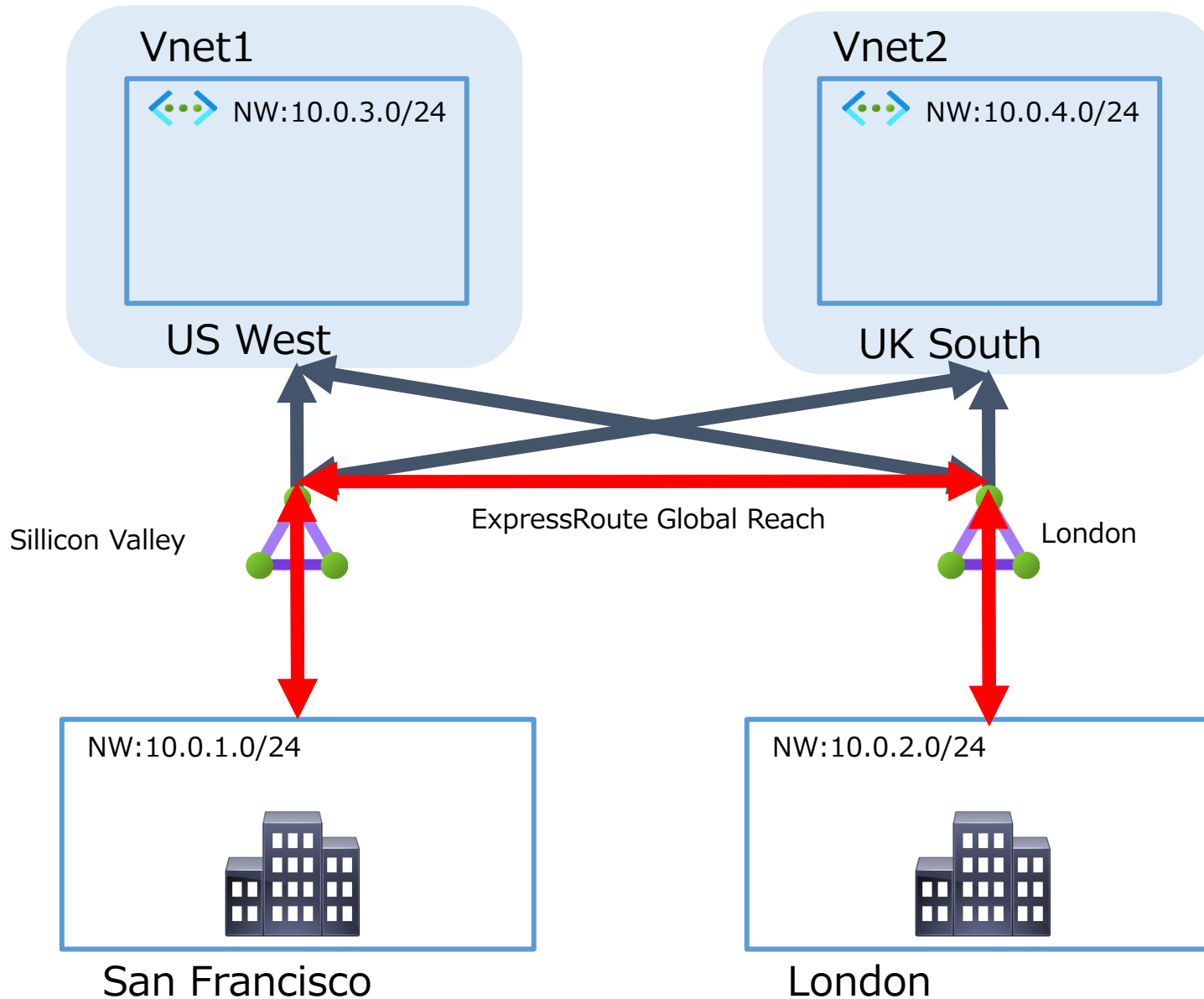
ExpressRoute



サンフランシスコオフィスからVnet1およびVnet2にデータ送信できるが、ロンドンオフィスとは通信できない。

10.0.1.0/24 から 10.0.3.0/24 および 10.0.4.0/24 ネットワークにデータを送信することはできるが、10.0.2.0/24 ネットワークには送信できない。

ExpressRoute Global Reach



ExpressRoute 回線を相互にリンクして、オンプレミス ネットワーク間にプライベート ネットワークを構築できる。
ExpressRoute Global Reach を追加することで、サンフランシスコ オフィス (10.0.1.0/24) が、既存の ExpressRoute 回線と Microsoft のグローバル ネットワークを介してロンドン オフィス (10.0.2.0/24) とデータを直接交換できる。

システムルートに関して

サブネットごとにシステムルートが生成される。

VNet内であれば自由に通信可能。それ以外はインターネットへの接続となる。

No	宛先	ネクストホップ	ネクストホップの説明	補足
1	仮想ネットワーク内	仮想ネットワーク	仮想ネットワーク内のアドレス空間の範囲内でトラフィックをルーティングする	AWSのルートテーブルのデフォルト値と同様
2	0.0.0.0/0	インターネット	仮想ネットワーク内のアドレス以外のあて先はインターネットにルーティングする	Azureサービスが宛先の場合には、インターネットではなくAzureバックボーンネットワークに直接ルーティングする
3	10.0.0.0/8	なし	ルーティングされず、パケットをDrop（破棄）する	
4	192.168.0.0/16	なし	ルーティングされず、パケットをDrop（破棄）する	
5	100.64.0.0/10	なし	ルーティングされず、パケットをDrop（破棄）する	

参考 インターネットアクセス方法

Azure仮想ネットワークにおいてNAT機能は「暗黙的に有効」

No	シナリオ	ロードバランサーまたはパブリックIPのSKU	NATの方式	対応プロトコル
1	インスタンスレベルのパブリックIPアドレスを含む仮想マシン（ロードバランサーあり、またはなし）	Standard、Basic	SNAT（PATは不使用）	TCP、UDP、ICMP、ESP
2	仮想マシンに関連付けられたパブリックロードバランサー	Standard、Basic	ロードバランサーのフロントエンドを使用したPATによるSNAT	TCP、UDP
3	スタンドアロン仮想マシン（ロードバランサーなし、パブリックIPなし）	なし、またはBasic	PATによるSNAT	TCP、UDP

PAT:ポートマスカレードのこと

この機能には上限があり、ポート枯渇や送信元IPが固定されないなどの課題がある。これらの課題を解決する手段として、「NATゲートウェイ」が提供されている

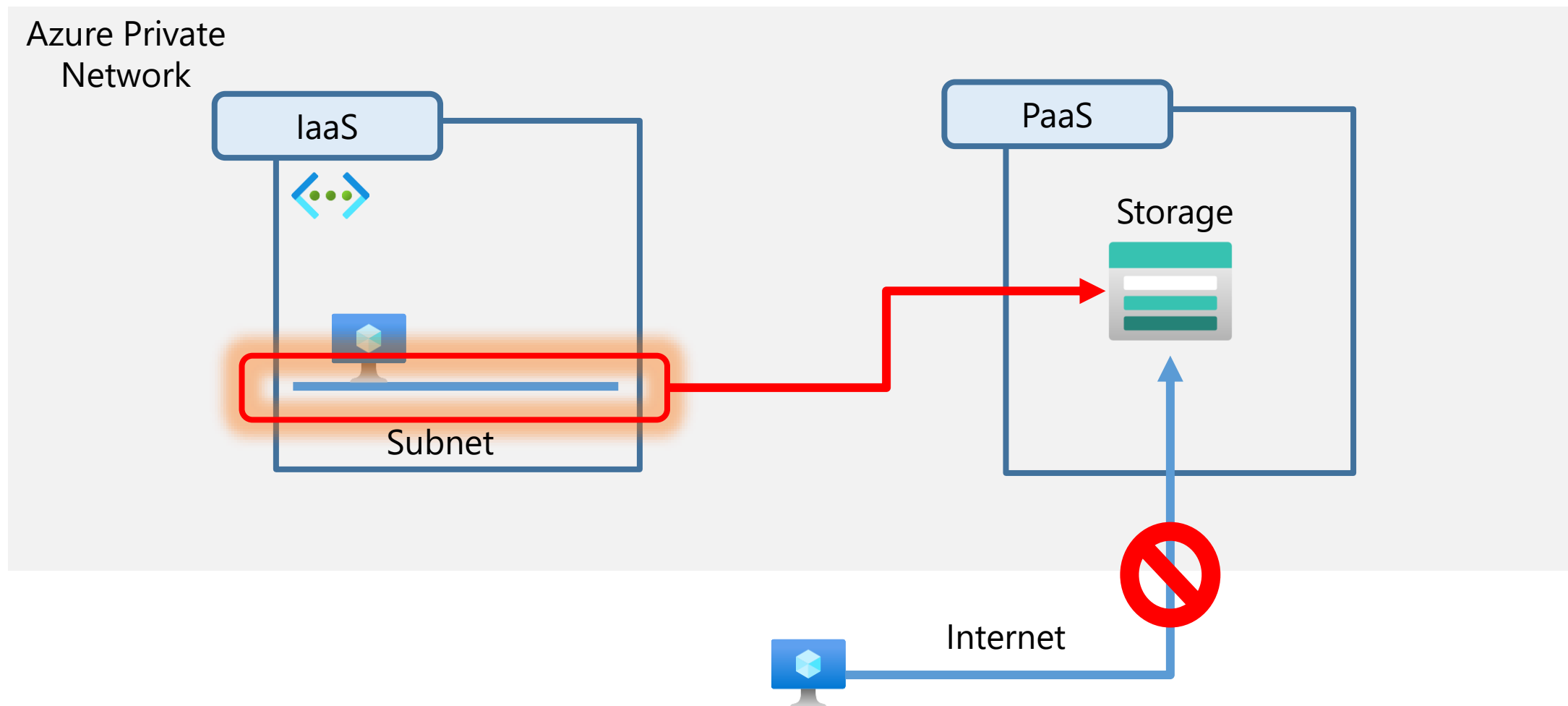
UDR

UDR(User Defined Route)を作成することでシステムルートを上書き可能。イメージ的にはスタティックルートの追加と同じ。利用シーンとしては

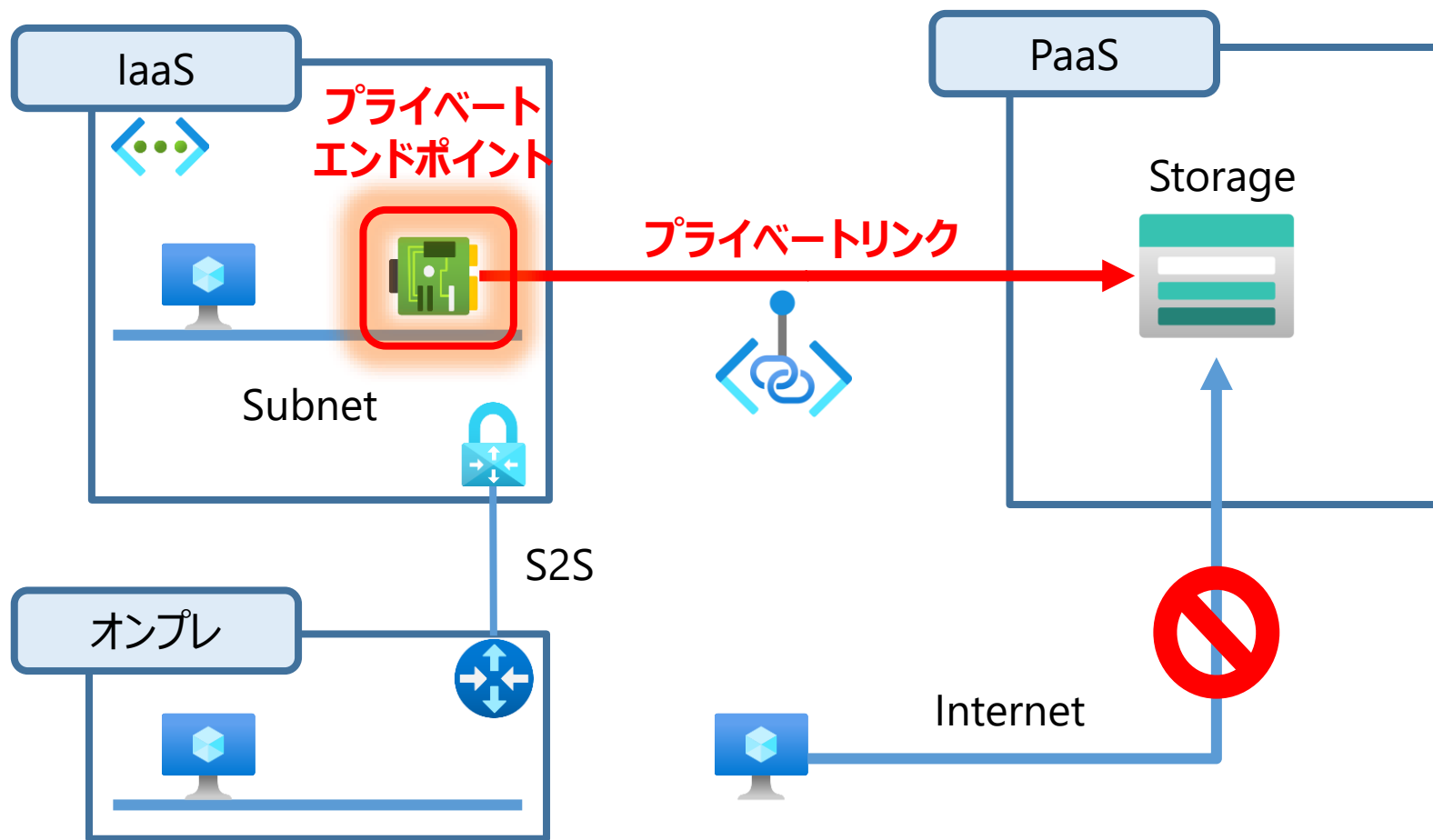
- 仮想アプライアンスを導入した場合
- インターネット通信をオンプレ経由で通信させたい場合
- サブネット間の通信を止めたい場合(NSGでも可)
- 別の仮想ネットワークを経由して通信させたい場合








ネクストホップの種類	説明
仮想ネットワークゲートウェイ	特定のアドレスプレフィックス宛の通信を仮想ネットワークゲートウェイにルーティングする。 仮想ネットワークゲートウェイは種類が「VPN」のものに限る。 種類が「ExpressRoute」の場合には、ExpressRouteではルーティングテーブルでBGPの使用が必須のため、UDRを指定することできない。
仮想ネットワーク	仮想ネットワーク内の既定のルーティング（＝システムルート）を上書きする場合に指定する
インターネット	インターネットに明示的にルーティングする場合に指定する。
仮想アプライアンス	F/WやWAFなどのネットワーク製品の仮想アプライアンスを指定したルーティングにしたい場合、本項目を指定する。
なし	指定した宛先のトラフィックを強制的にDrop（破棄）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

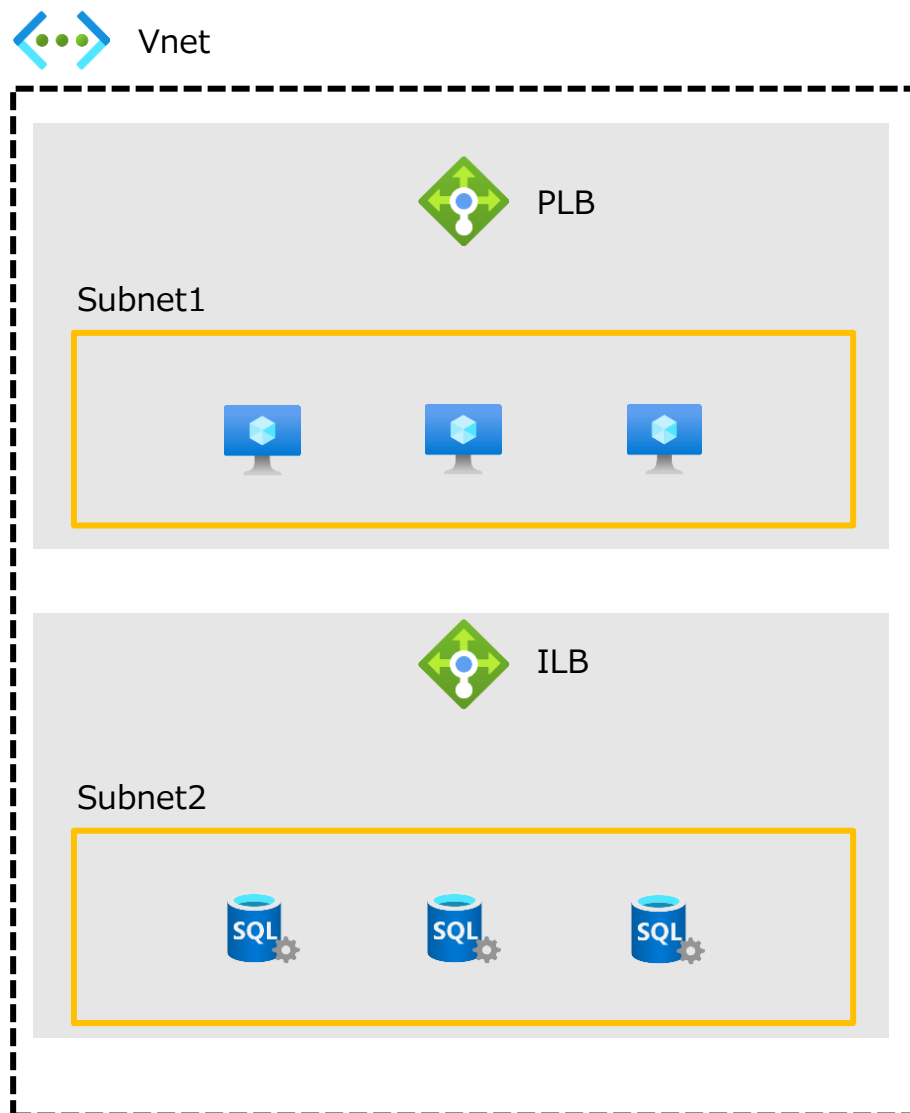


- **プライベートエンドポイント**とは、プライベートリンクを実現するための仕組みの一つで、プライベートリンクサービスにプライベートで安全に接続するネットワークインターフェイスを提供する。
- プライベートリンクサービスとは**プライベートリンク**を使用するサービスのことで、Azure Storage や Azure SQL Database などの定義済みのプライベートリンクリソースなどを指す。



Port	シングルリージョン	マルチリージョン	推奨トラフィックレイヤー
すべてのPort	<div><div>4</div><div>Load Balancer</div></div>	<div><div>7</div><div>Traffic Manager</div></div>	<div>7</div> <div>6</div> <div>5</div> <div>4</div> <div>3</div> <div>2</div> <div>1</div>
80,443	<div><div>7</div><div>Application Gateway</div><div></div></div>	<div><div>7</div><div>Front Door</div><div></div></div>	<div>7</div> <div>6</div> <div>5</div> <div>4</div> <div>3</div> <div>2</div> <div>1</div>

Load balancer の理解



- LBのバックエンドプールは同一仮想ネットワーク内
- インターネット経由でアクセスするLB（Public IPが必要）を**PLB**という
- インターネット経由でアクセスしない（VNet内での通信）LBを**ILB**という
- プール内のインスタンス稼働状況の確認
 - **正常性プローブ**
- セッション維持方法
 - **セッション永続化**

負荷分散装置まとめ

サービス	Azure Load Balancer	Application Gateway	Traffic Manager
テクノロジー	L4	L7	DNS
サポートプロトコル	任意	HTTP,HTTPS,WebSocker	任意（HTTPエンドポイントはエンドポイントの監視に必要）
エンドポイント	Azure VM と Cloud Service のロールインスタンス	任意の Azure 内部 IP アドレス、Public IP アドレス、Azure VM、または Cloud Service	Azure VM、Cloud Service、Azure Web Apps および外部エンドポイント
Vnet	インターネット接続と内部（Vnet）のアプリケーションの両方に使用できる	インターネット接続と内部（Vnet）のアプリケーションの両方に使用できる	インターネットに接続するアプリケーションのみをサポートする
エンドポイントの監視	プローブ経由	プローブ経由	HTTP/HTTPS GET 経由でサポート

Azure Load Balancer VS Application Gateway

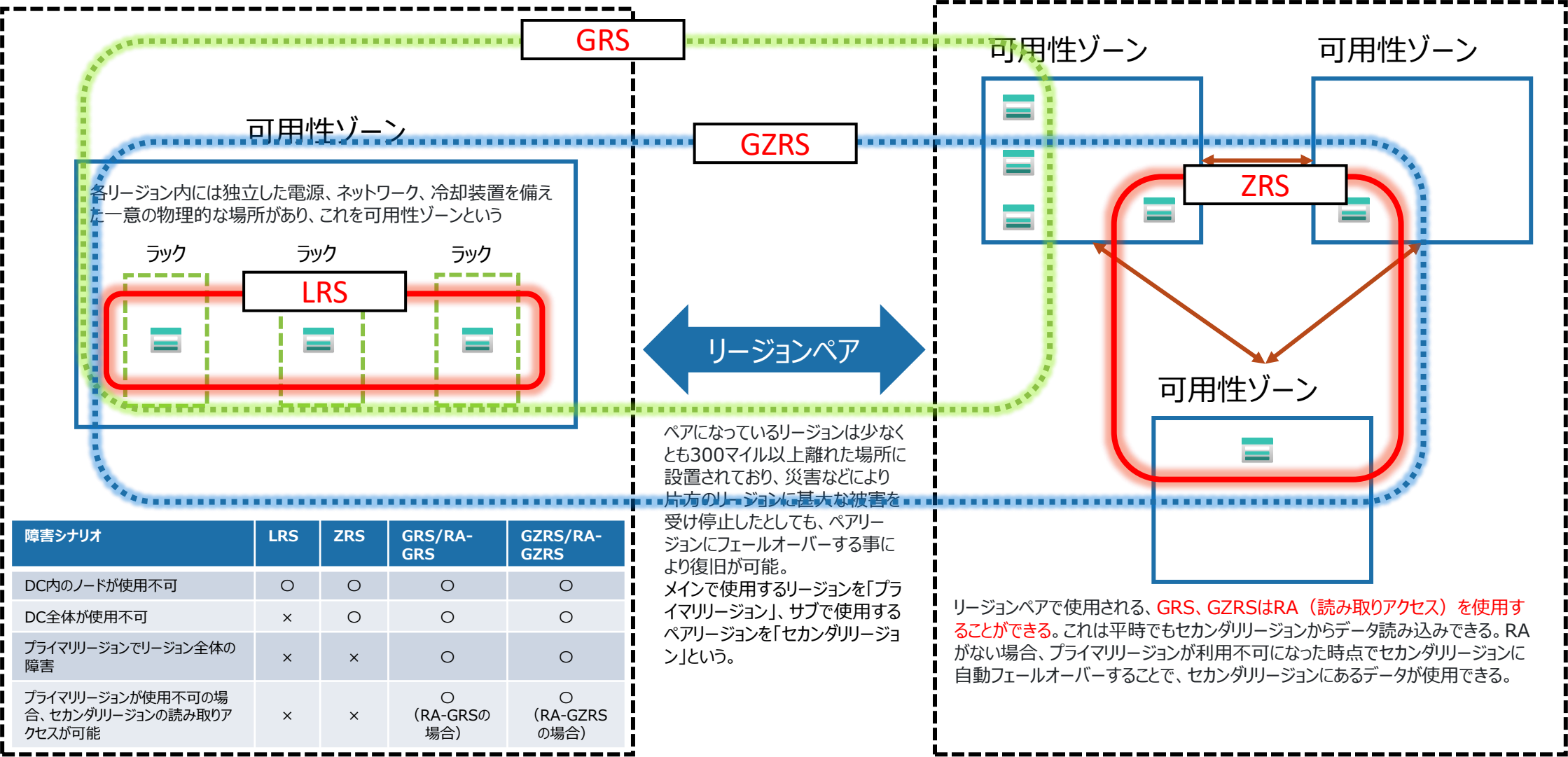
	Azure Load Balancer	Application Gateway
プロトコル	TCP/UDP	HTTP,HTTPS,WebSocket
IP Reservation	○	×
負荷分散モード	5 tuple Hash（発信元 IP、ソースポート、宛先 IP、宛先ポート、プロトコルの種類）	ラウンドロビン、URLに基づくルーティング
負荷分散モード（発信元IP／スティッキーセッション）	セッション アフィニティまたはクライアント IP アフィニティとも呼ばれます。このモードは 2 タプル（ソース IP と接続先 IP）または 3 タプル（ソース IP、接続先 IP、プロトコルの種類）のハッシュを使用	Cookieベースのアフィニティ URLに基づくルーティング
正常性プローブ	既定値：プローブ間隔-15秒。循環から除外：2回連続のエラー。ユーザー定義のプローブサポート	アイドル状態のプローブ間隔30秒。5回連続するライブトラフィック障害またはアイドルモードでの単一のプローブ障害の後に除外。ユーザー定義のプローブをサポート
SSLオフロード	×	○
URLベースのルーティング	×	○
SSLポリシー	×	○

Azure Storage レプリケーション

LRS:Locally redundant storage
ZRS:zone-redundant storage
GRS:geo-redundant storage
GZRS:geo-zone-redundant storage

西日本リージョン

東日本リージョン



ストレージのアクセス層まとめ

ホット

- 他の層と比べてストレージ コストが **高め**だが、アクセス コストが**最も低く**なります。
- 頻繁にアクセスされる**データの格納向け

クール

- ホットストレージ層に比べてストレージコストが**低く**なり、アクセスコストが**高くなり**ます。
- アクセス頻度が低い**データ向け。
- 少なくとも 30 日以上保管されるデータに最適化。

コールド

- クール層に比べてストレージコストが**低く**なり、アクセスコストが**高くなり**ます。
- アクセス頻度が低い**データ向け。
- 少なくとも 90 日以上保管されるデータに最適化。

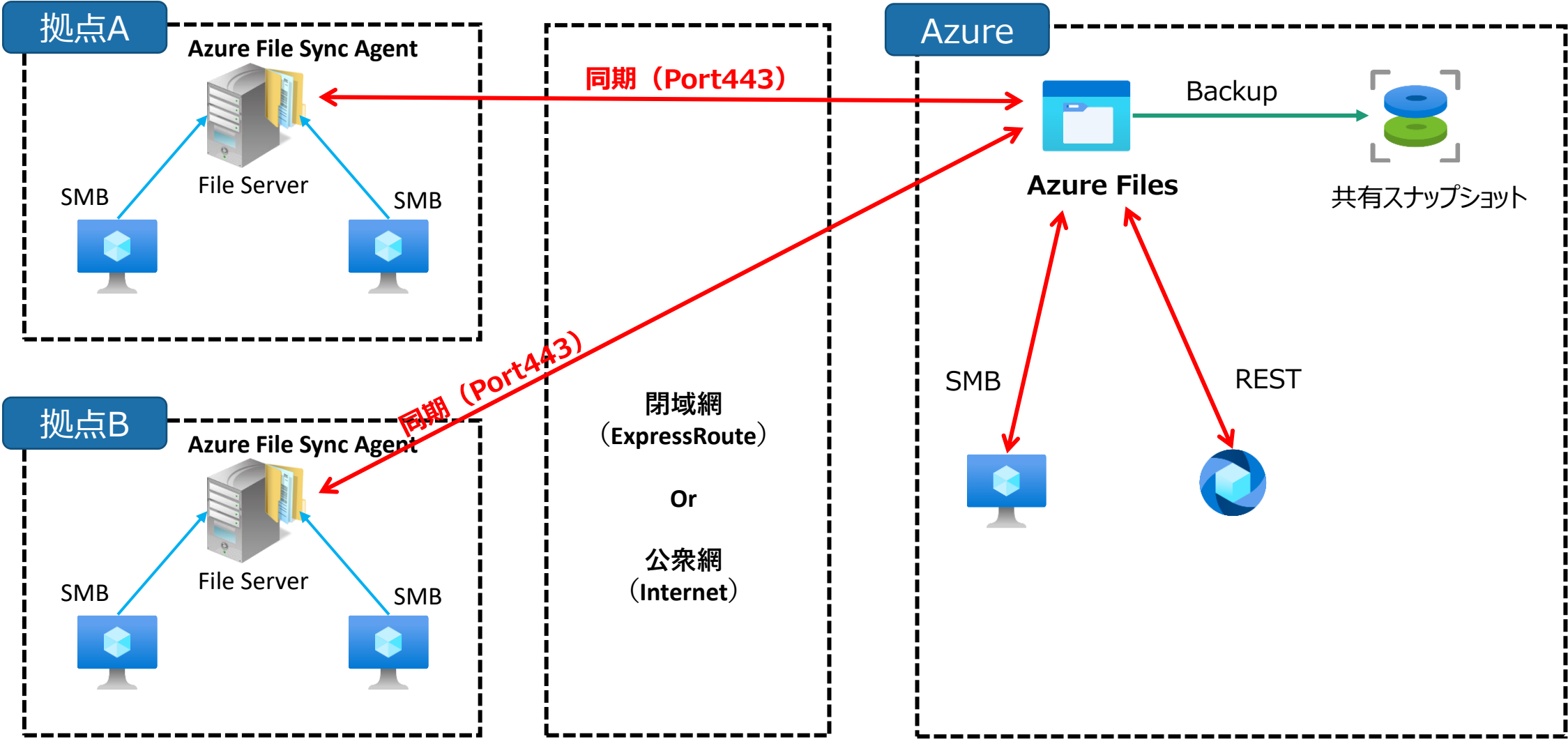
アーカイブ

- ストレージ コストが**最も低く**、他に比べてデータ取得コストが**最も高くなり**ます
- データの読み取り、コピー、上書き、変更を行うことはできない。
- ほとんどアクセスされず、少なくとも 180 日以上保管されるデータ向け。

	ホット	クール	コールド	アーカイブ
可用性	99%	99%	99%	99%
可用性(RA-GRS)	99.99%	99.9%	99.9%	99.9%
ストレージコスト	高い	低い	低い	最も低い
アクセスコスト	低い	高い	高い	最も高い
トランザクションコスト	低い	高い	高い	最も高い
最小ストレージ存続期間	-	30日	90日	180日
待機時間	ミリ秒	ミリ秒	ミリ秒	15時間未満

Azure File Sync ファイルサーバーのクラウドシナリオ例

ポイント：ポート445をFWやGWに対して開ける必要なし



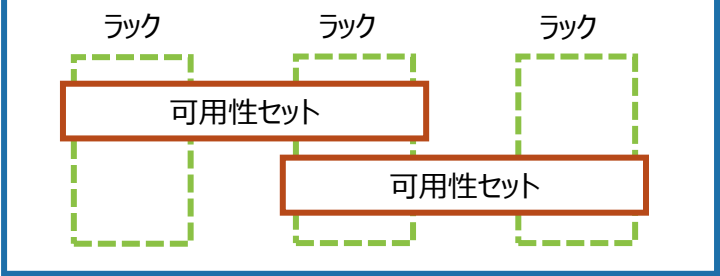
可用性セットと可用性ゾーン

西日本リージョン

「リージョン」とはクラウドサービスにおいて、データセンターを設置している独立した地域の事

可用性ゾーン

各リージョン内には独立した電源、ネットワーク、冷却装置を備えた一意の物理的な場所があり、これを可用性ゾーンという



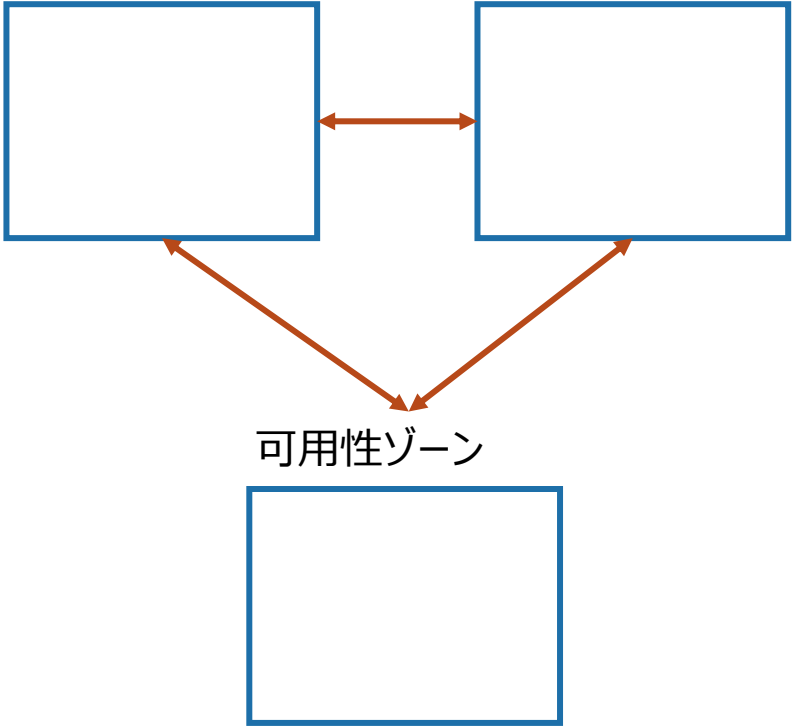
可用性ゾーンはデータセンターそのものの障害によるシステム停止を防ぎ、可用性セットはデータセンター内のサーバーラックやサーバー機の障害からシステムを保護する。

可用性ゾーンを設定した場合の仮想マシンのSLAは99.99%、可用性セットを設定した場合は99.95%です。システム停止許容時間に応じて可用性ゾーンと可用性セットのどちらを設定するかを設計する。

東日本リージョン

可用性ゾーン

可用性ゾーン



ペアになっているリージョンは少なくとも300マイル以上離れた場所に設置されており、災害などにより片方のリージョンに甚大な被害を受け停止したとしても、ペアリージョンにフェールオーバーする事により復旧が可能。メインで使用するリージョンを「プライマリーリージョン」、サブで使用するペアリージョンを「セカンダリーリージョン」という。

SLAとダウンタイム

SLA	週間ダウンタイム	月間ダウンタイム	年間ダウンタイム
99%	1.68 時間	7.2 時間	3.65 日
99.9%	10.1 分	43.2 分	8.76 時間
99.95%	5 分	21.6 分	4.38 時間
99.99%	1.01 分	4.32 分	52.56 分
99.999%	6 秒	25.9 秒	5.26 分

通常、計画されたダウンタイム（メンテナンス）はSLAには含まれません。

可用性セット

- 更新ドメイン内のVMは順番に再起動する
 - デフォルトでは5つの更新ドメインが作成される (MAX20)
 - 一度に一つの更新ドメインが再起動対象
- 障害ドメイン障害ドメインとは、同じ電源やスイッチを共有している範囲
 - サーバーラックのイメージで定義できる範囲は1～3 (MAX3)

Update
Domain
10



Fault
Domain
2



- 可用性セットで14台のVMがある場合、最大のVMダウン数は
 - 更新ドメインは2台
 - 障害ドメインは7台

仮想マシンとスケール セットの違い

- スケール セットは、仮想マシンをベースに構築されます。スケール セットには、アプリケーションの実行とスケーリングを行うための管理レイヤーと自動化レイヤーがあります。代わりに、個別の VM を手動で作成して管理したり、既存のツールを統合して同様のレベルの自動化を構築したりすることもできます。

シナリオ	手動の VM グループ	仮想マシン スケール セット
補助 VM インスタンスの追加	作成、構成、コンプライアンスの遵守が手動プロセス	一元化された構成から自動で作成
トラフィックのバランス調整と分散	Azure ロード バランサーまたはアプリケーション ゲートウェイの作成と構成が手動プロセス	Azure ロード バランサーまたはアプリケーション ゲートウェイの作成と統合を自動で実行可能
高可用性と冗長性	可用性セットの作成、または可用性ゾーンでの VM の分散および追跡が手動	可用性ゾーンまたは可用性セットでの VM インスタンスの自動分散
VM のスケーリング	手動による監視と Azure Automation	ホスト メトリック、ゲスト内メトリック、Application Insights、またはスケジュールに基づいた自動スケーリング

App Service Plan

プランによって、含まれる機能が異なることが重要

含まれる機能

この App Service プランでホストされているすべてのアプリがこれらの機能にアクセスできます:



カスタム ドメイン / SSL

SNI および IP SSL バインドでカスタム ドメインを構成し購入する



自動スケール

最大 20 個のインスタンス。可用性に応じて異なります。



ステージング スロット

運用環境にスワップする前に、テストとデプロイで使用するための最大 20 個のステージング スロットです。



毎日のバックアップ

アプリを毎日 50 回バックアップします。



Traffic Manager

アプリの複数のインスタンス間でトラフィックをルーティングすると、パフォーマンスと可用性が向上します。

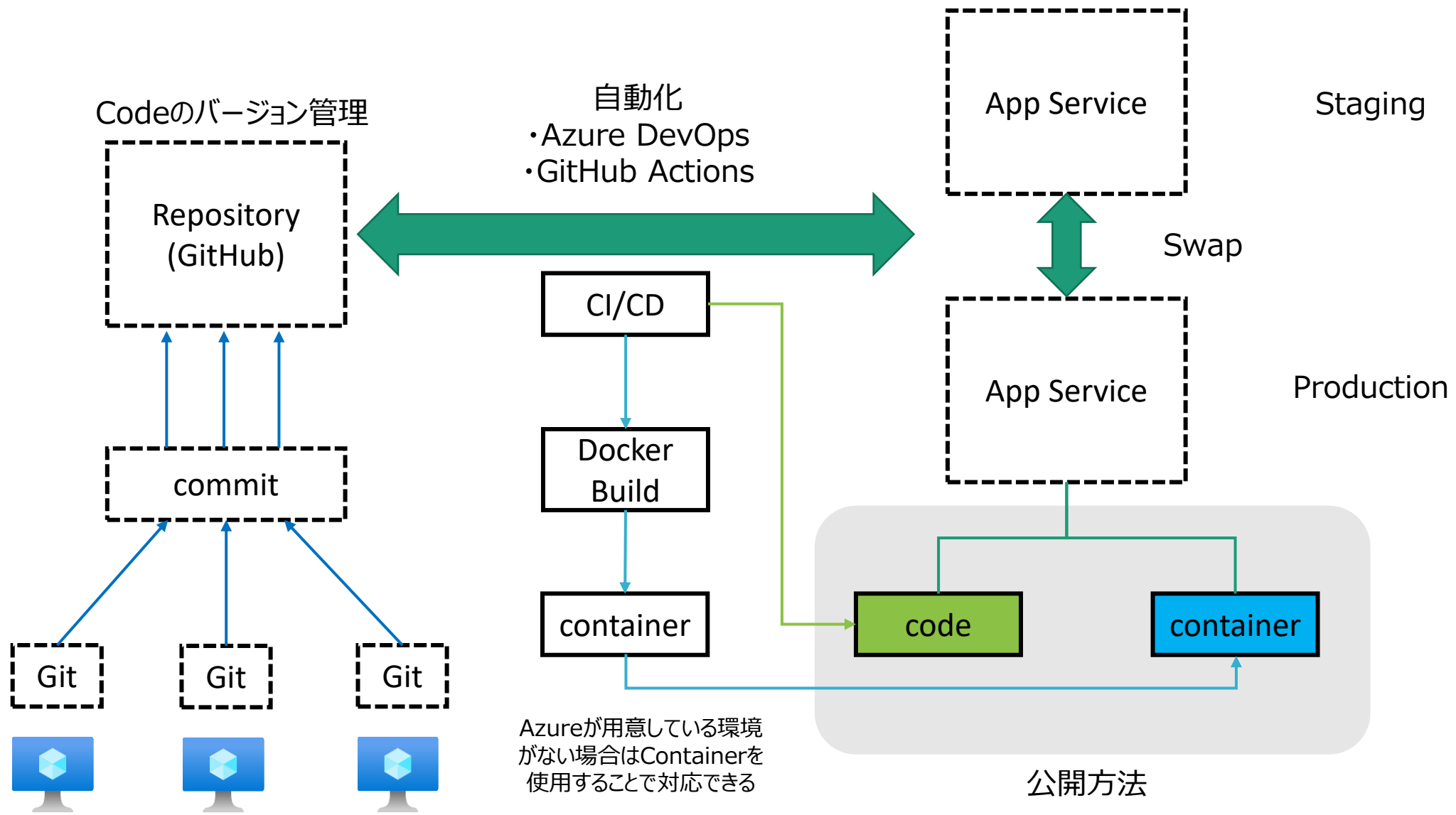
App Service

App Service

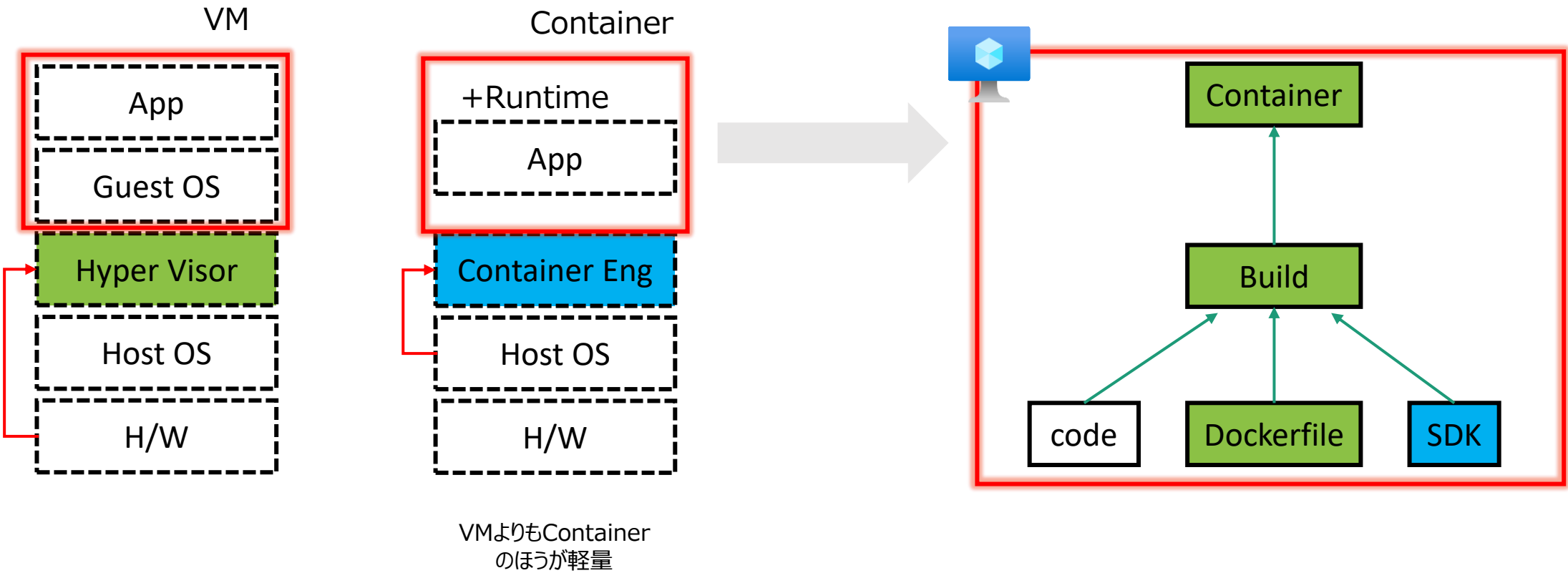
App Service

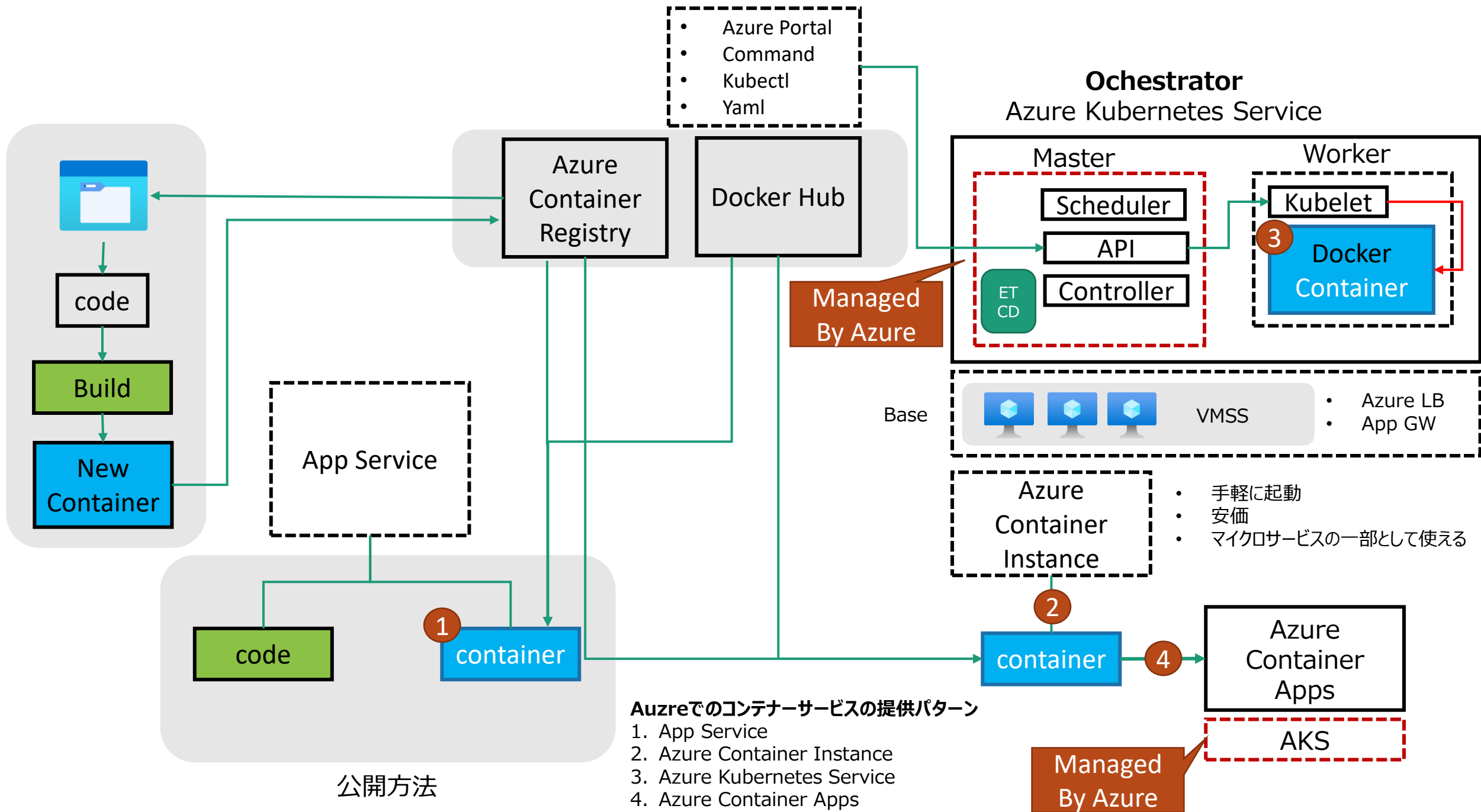
App Service Plan

PaaSでの開発工程



PaaSでの開発工程





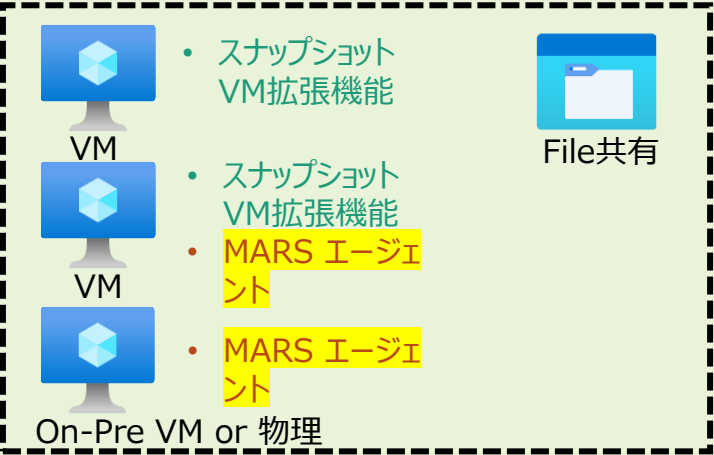
Azure Backup の整理

MARS:Microsoft Azure Recovery Services
MABS:Microsoft Azure Backup Server
DPM:System Center Data Protection Manager

A

Azure or On-pre

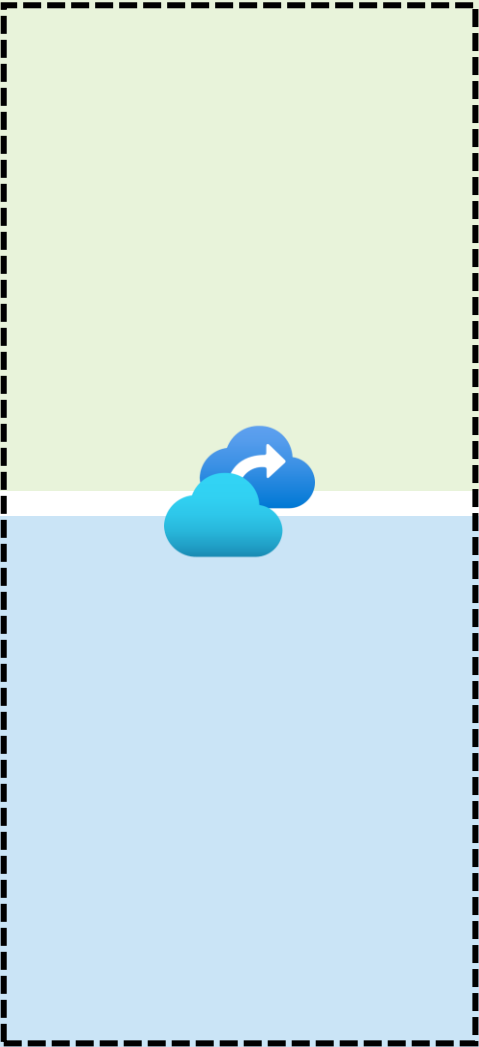
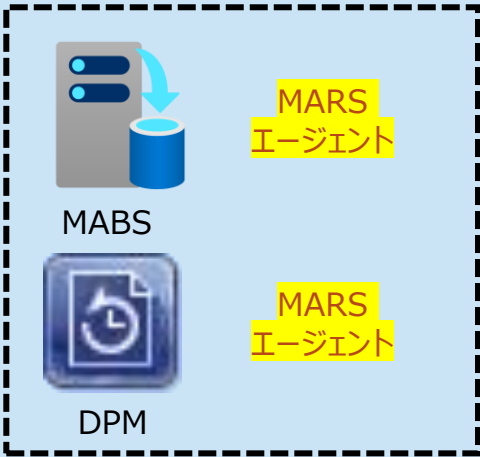
Azure(Recovery Services vault)



B

Azure or On-pre

Azure or On-pre



アラートルールまとめ

対象範囲（何を監視するか）を決める

スコープ選択

- サブスクリプション
- リソースの種類
- 場所

どのような事象に対してアラート設定するかを決める

シグナル選択

- シグナルを選択（仮想マシンのリスタートなど）
- アラートをトリガーするためのロジック設定（イベントレベル、状態、イベント開始者）

アラートに該当する場合、何を行うかを決める

アクション選択

- 新しいアクション グループを選択または作成することにより、アラートルールがトリガーされたときに通知を送信するか、アクションを呼び出します。