

仮想ネットワークの 概要

2023/6/22

仮想ネットワークの概要



仮想ネットワーク 10.0.0.0/16



サブネット 10.0.0.0/24



仮想マシン



ネットワークインターフェースカード(NIC)
プライベートIPアドレス 10.0.0.4



パブリックIPアドレス 11.22.33.44



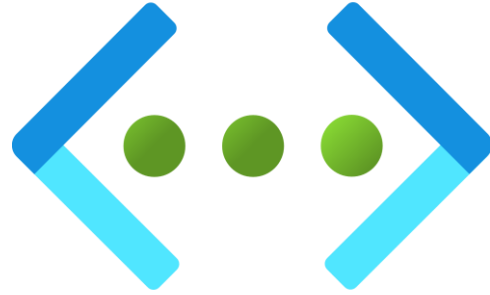
ディスク



ネットワーク
セキュリティ
グループ
(NSG)

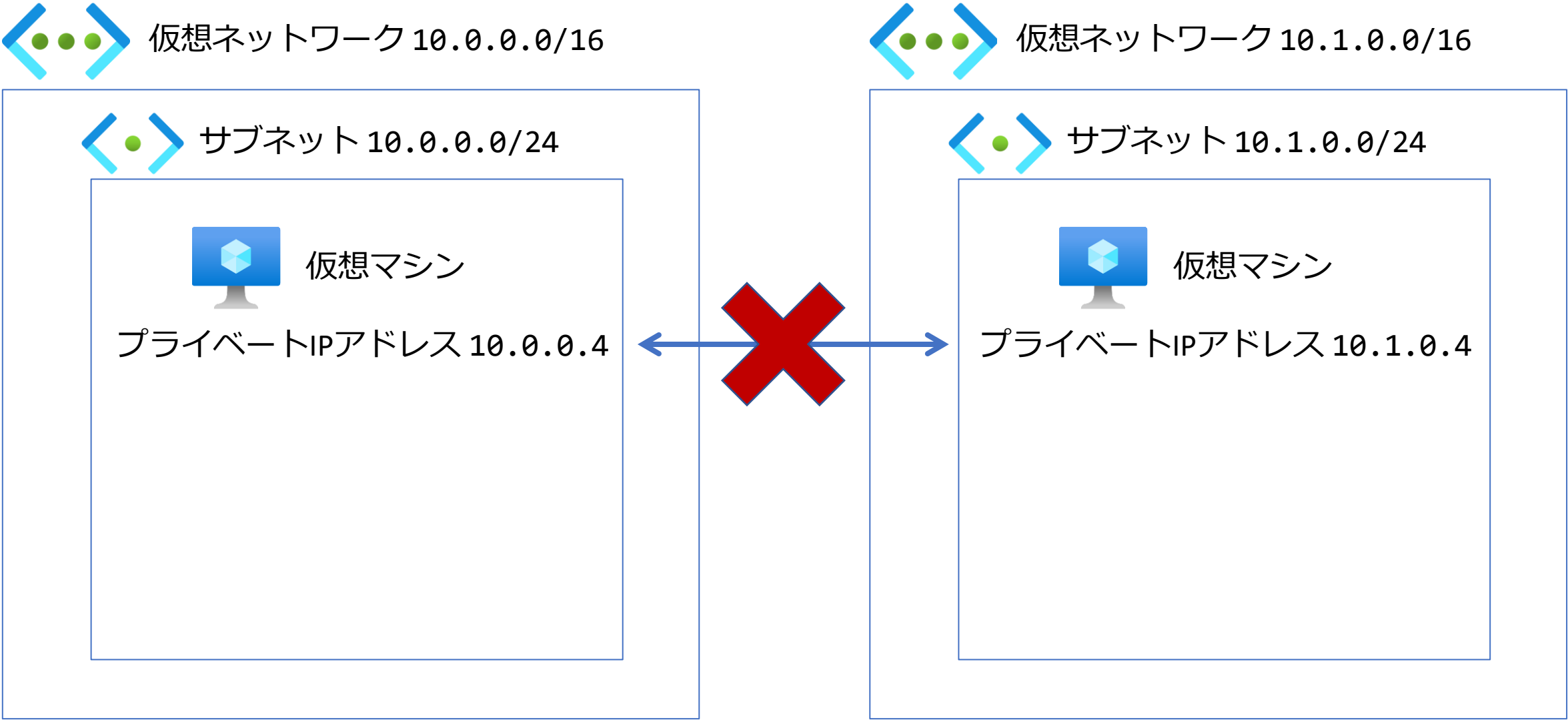


ルートテーブル

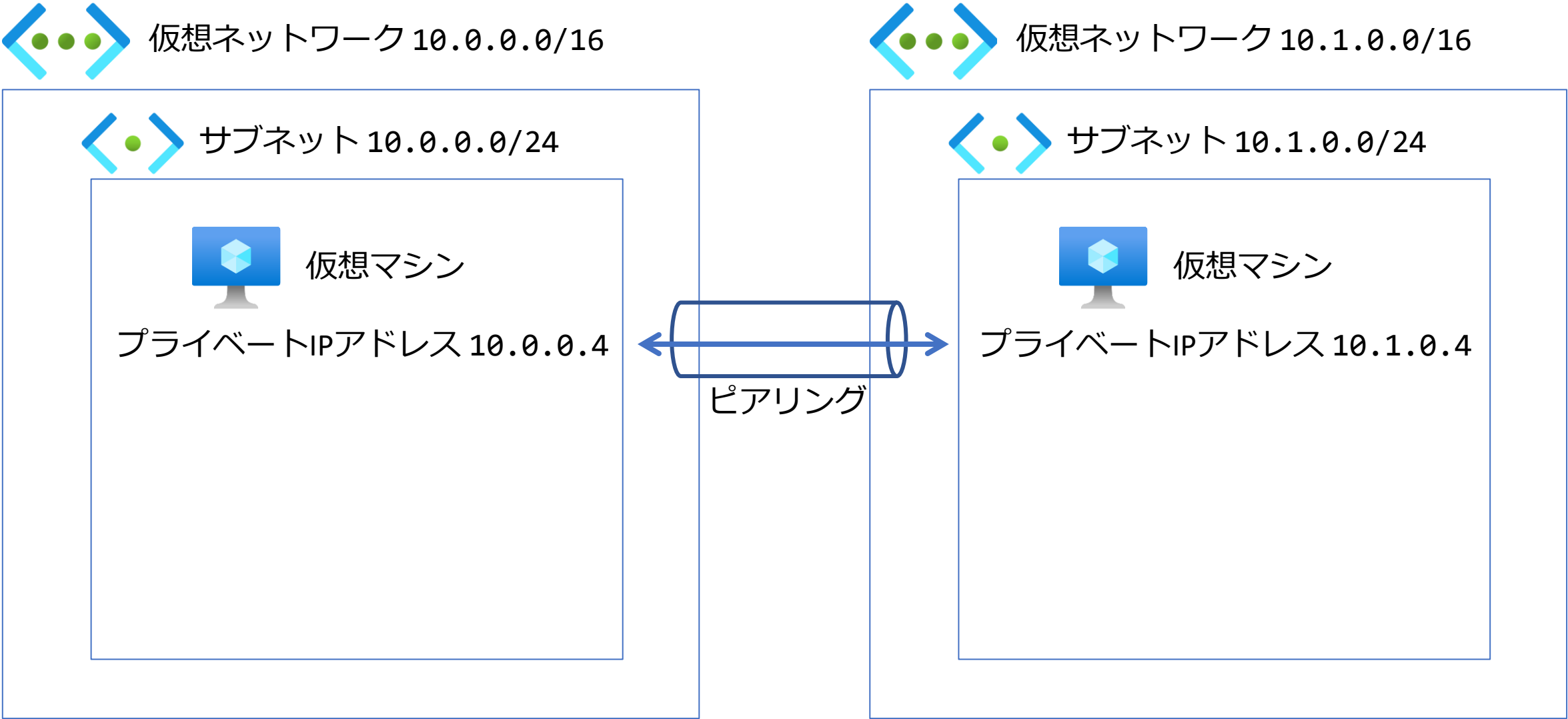


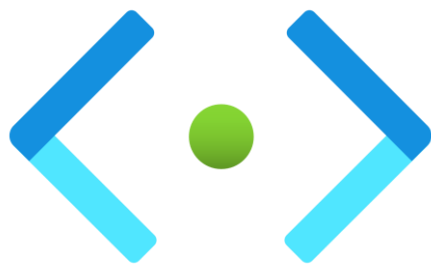
仮想ネットワーク

仮想ネットワークは、仮想マシンなどを運用するためのネットワーク。
異なる仮想ネットワーク同士は、プライベートIPアドレスを使用した直接の通信はできない。



ただし、仮想ネットワーク同士を「ピアリング」で接続すれば、仮想ネットワーク間でのプライベートな通信が可能となる。





サブネット

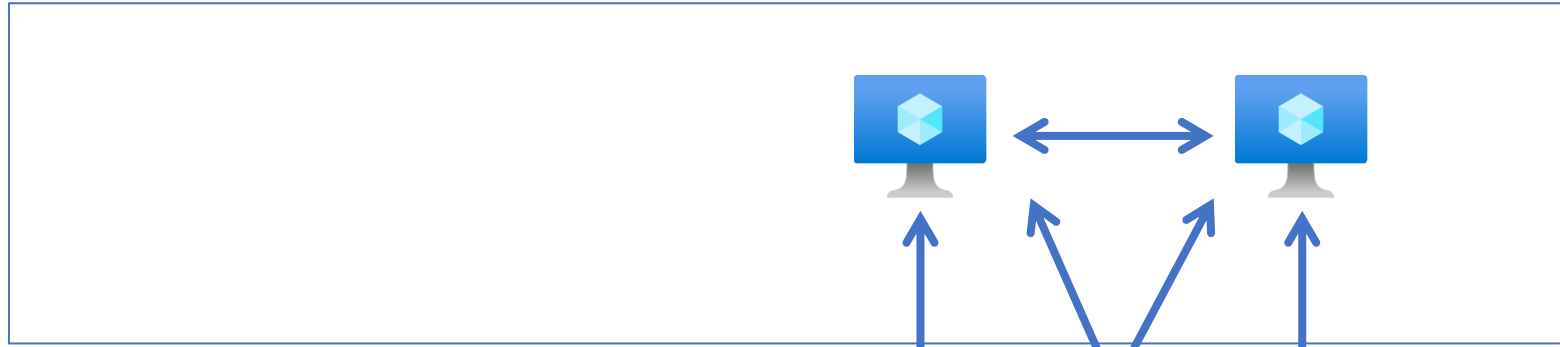
仮想ネットワークの中にサブネットを作成できる。
サブネットには（別の）NSG、ルートテーブルを関連付けできる
VM内のサブネット内のVMは、相互に通信可能。



仮想ネットワーク 10.0.0.0/16



サブネット 10.0.0.0/24



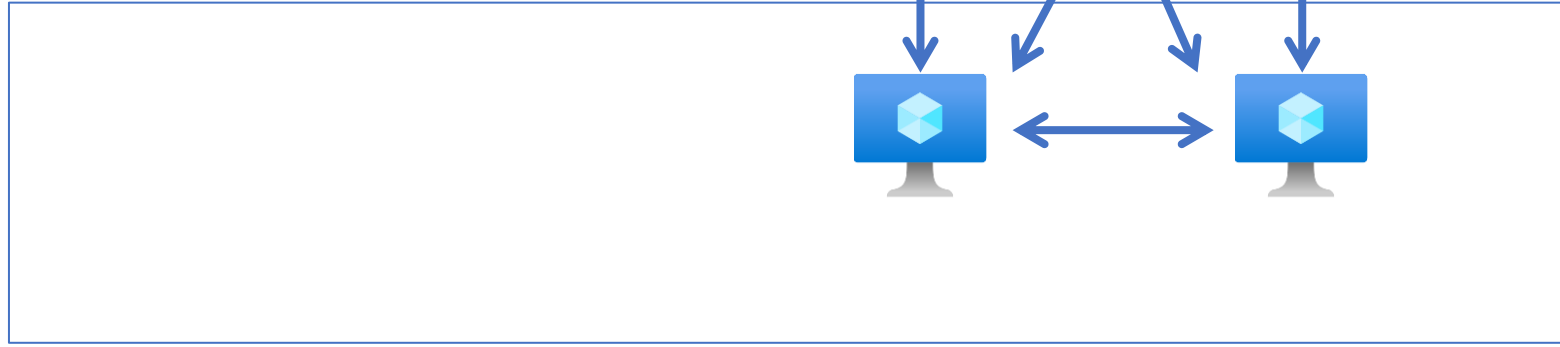
ネットワーク
セキュリティ
グループ
(NSG)



ルートテーブル



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)



ルートテーブル



パブリックIPアドレス

パブリックIPアドレスは、Azureリソースの一種。NICに関連付けされる。インターネットからはこのアドレスを使用してVMにアクセスできる。



仮想ネットワーク 10.0.0.0/16



サブネット 10.0.0.0/24



仮想マシン



ネットワークインターフェースカード(NIC)
プライベートIPアドレス 10.0.0.4



パブリックIPアドレス 11.22.33.44



仮想マシン



ネットワークインターフェースカード(NIC)
プライベートIPアドレス 10.0.0.5



パブリックIPアドレス 55.66.77.88

リソース作成時に
アドレスが割り当てられる

リソース作成時に
アドレスが割り当てられる

プライベートIPアドレス

プライベートIPアドレスは、NICの「IP構成」のプロパティの一部。Azureリソースの一種ではない。サブネット内で仮想マシンが通信する際は、プライベートIPアドレスが使用される。



仮想ネットワーク 10.0.0.0/16



サブネット 10.0.0.0/24



仮想マシン



ネットワークインターフェースカード(NIC)
プライベートIPアドレス 10.0.0.4



パブリックIPアドレス 11.22.33.44



仮想マシン



ネットワークインターフェースカード(NIC)
プライベートIPアドレス 10.0.0.5



パブリックIPアドレス 55.66.77.88

動的（自動）
または 静的（固定）

動的（自動）
または 静的（固定）



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

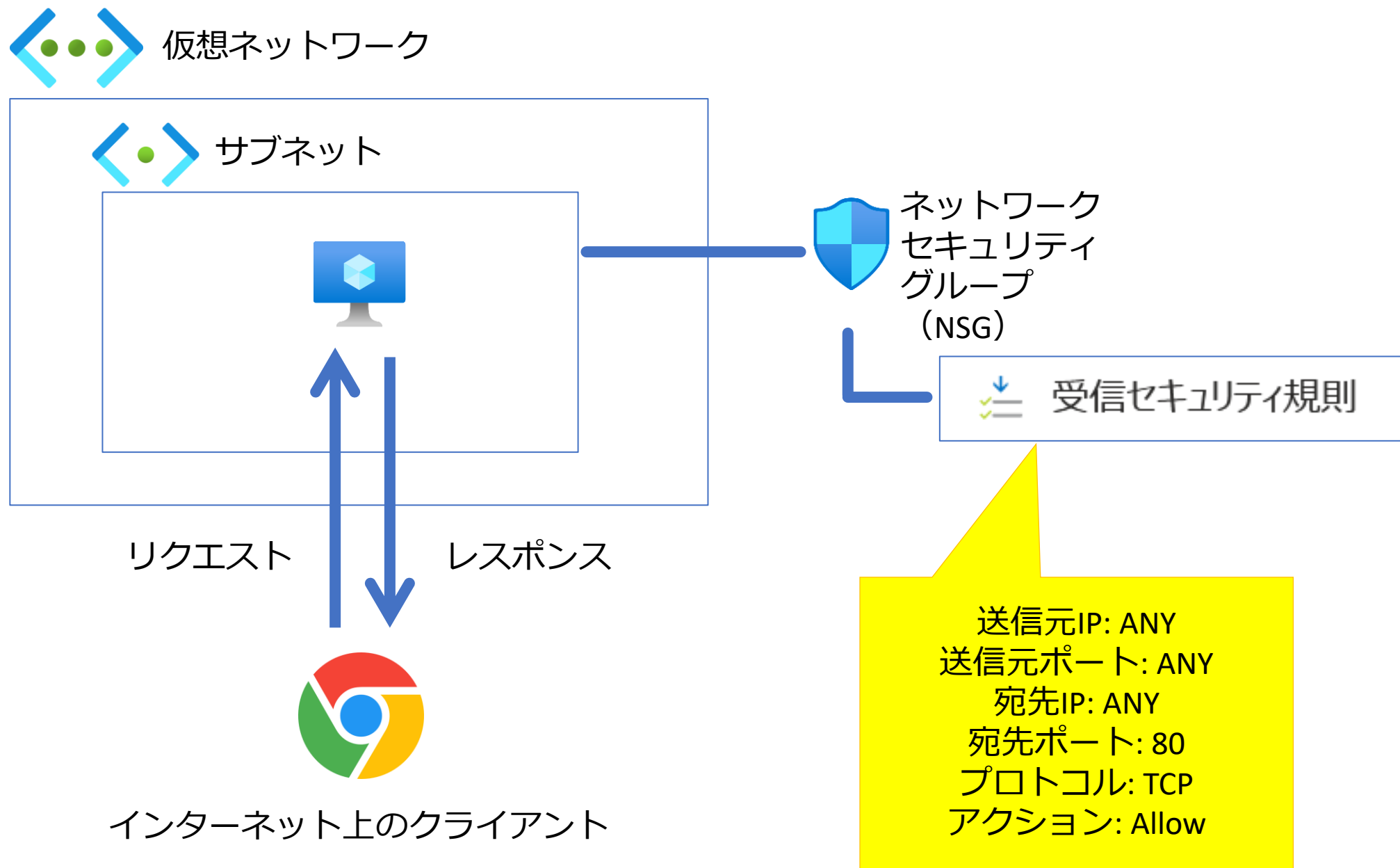
優先度 ↑↓	名前 ↑↓	ポート ↑↓	プロトコル ↑↓	ソース ↑↓	宛先 ↑↓	アクション ↑↓
<input type="checkbox"/> 300	 RDP	3389	TCP	任意	任意	 Allow
<input type="checkbox"/> 310	AllowAnyHTTPInbound	80	TCP	任意	任意	 Allow
<input type="checkbox"/> 65000	AllowVnetInBound	任意	任意	VirtualNetwork	VirtualNetwork	 Allow
<input type="checkbox"/> 65001	AllowAzureLoadBalanc...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

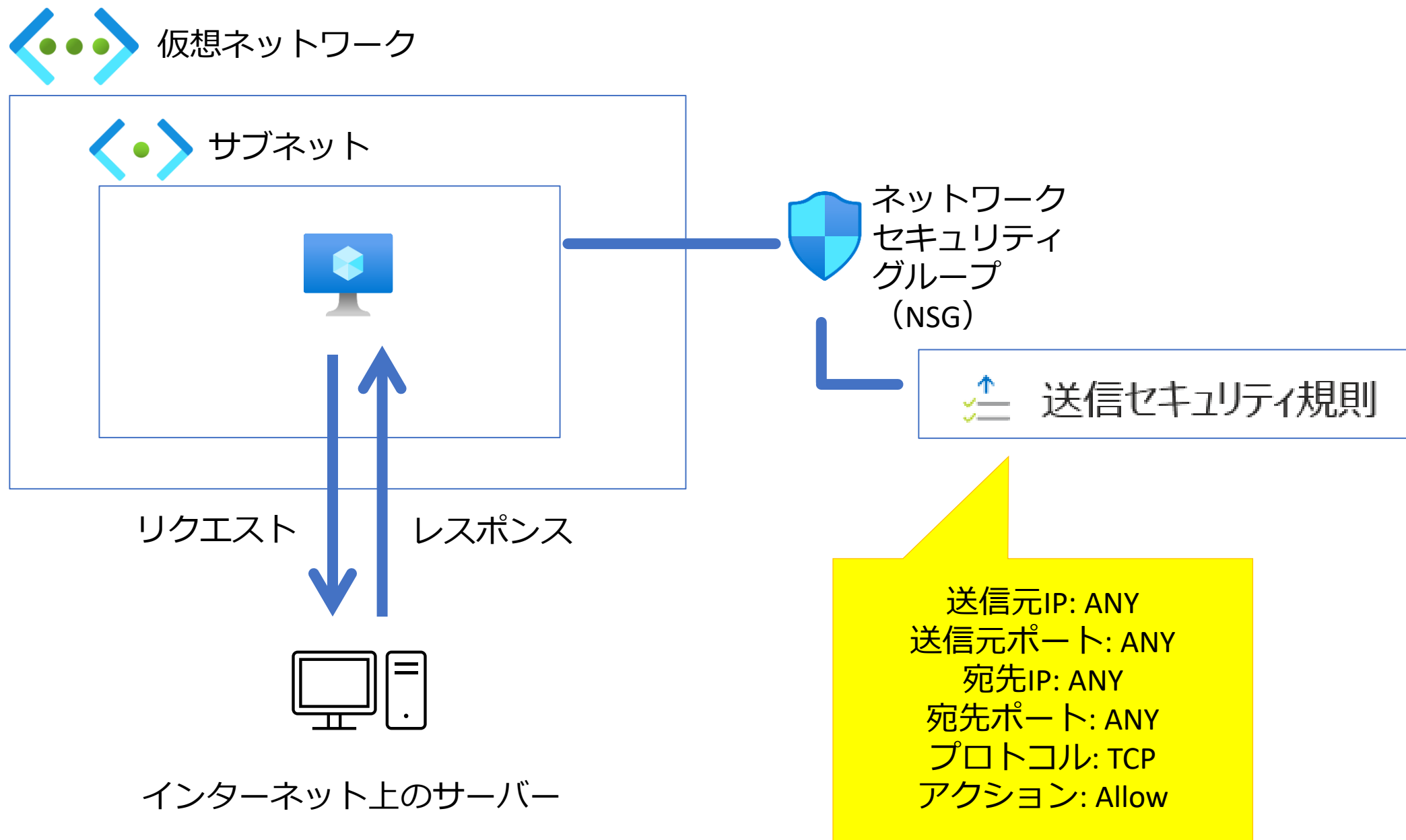
例(2): HTTP(TCP 80)のトラフィック: 優先度310番の規則により、許可される。

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。

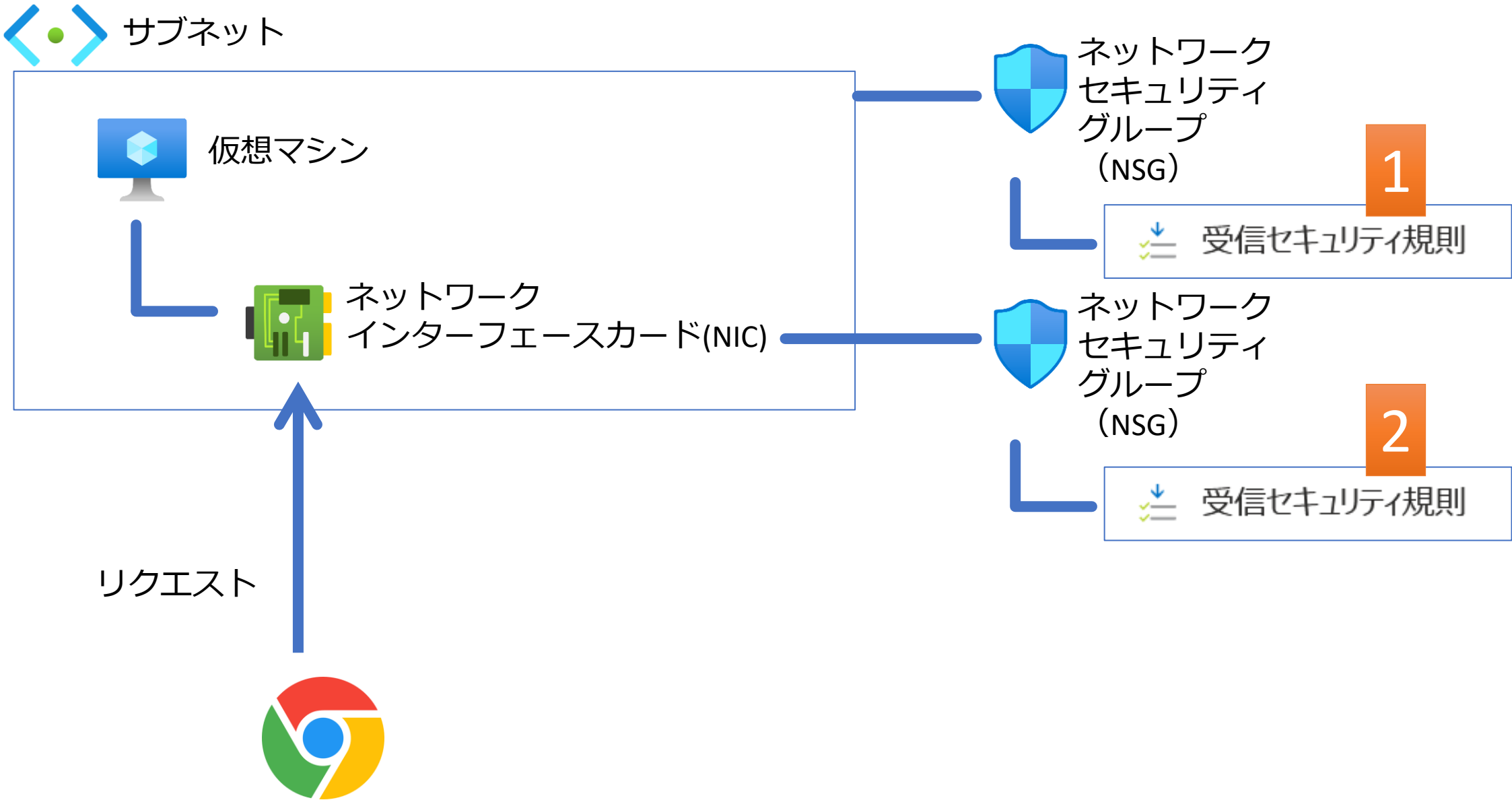
「受信」の例



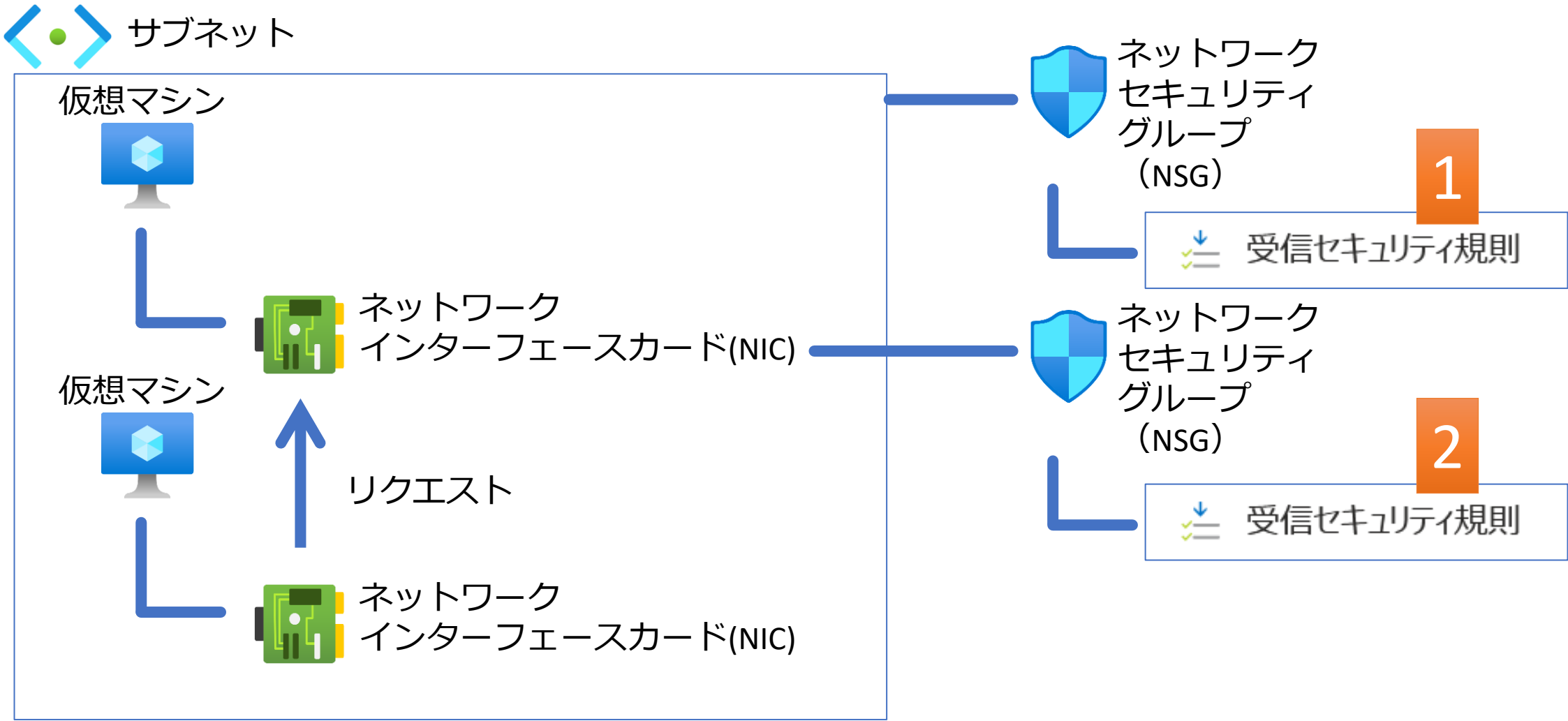
「送信」の例



受信の場合: 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。このプロセスにはサブネット内トラフィックも含まれます。



受信の場合: 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。 **このプロセスにはサブネット内トラフィックも含まれます。**





Azure DNS

「パブリックDNSゾーン」と「プライベートDNSゾーン」



Azure DNS
パブリックDNSゾーン
contoso.com

インターネット上での
名前解決。
※「DNSゾーン」とも

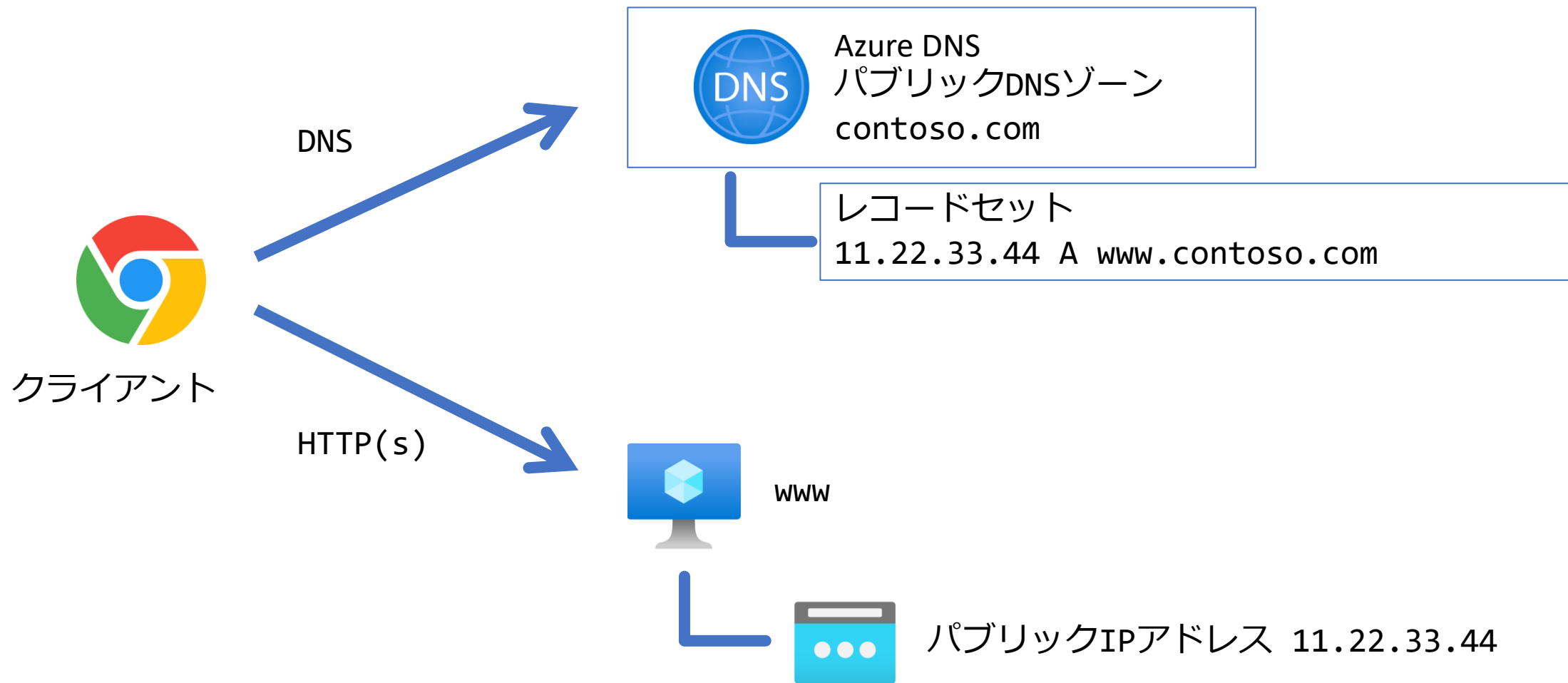


Azure DNS
プライベートDNSゾーン
private.contoso.com

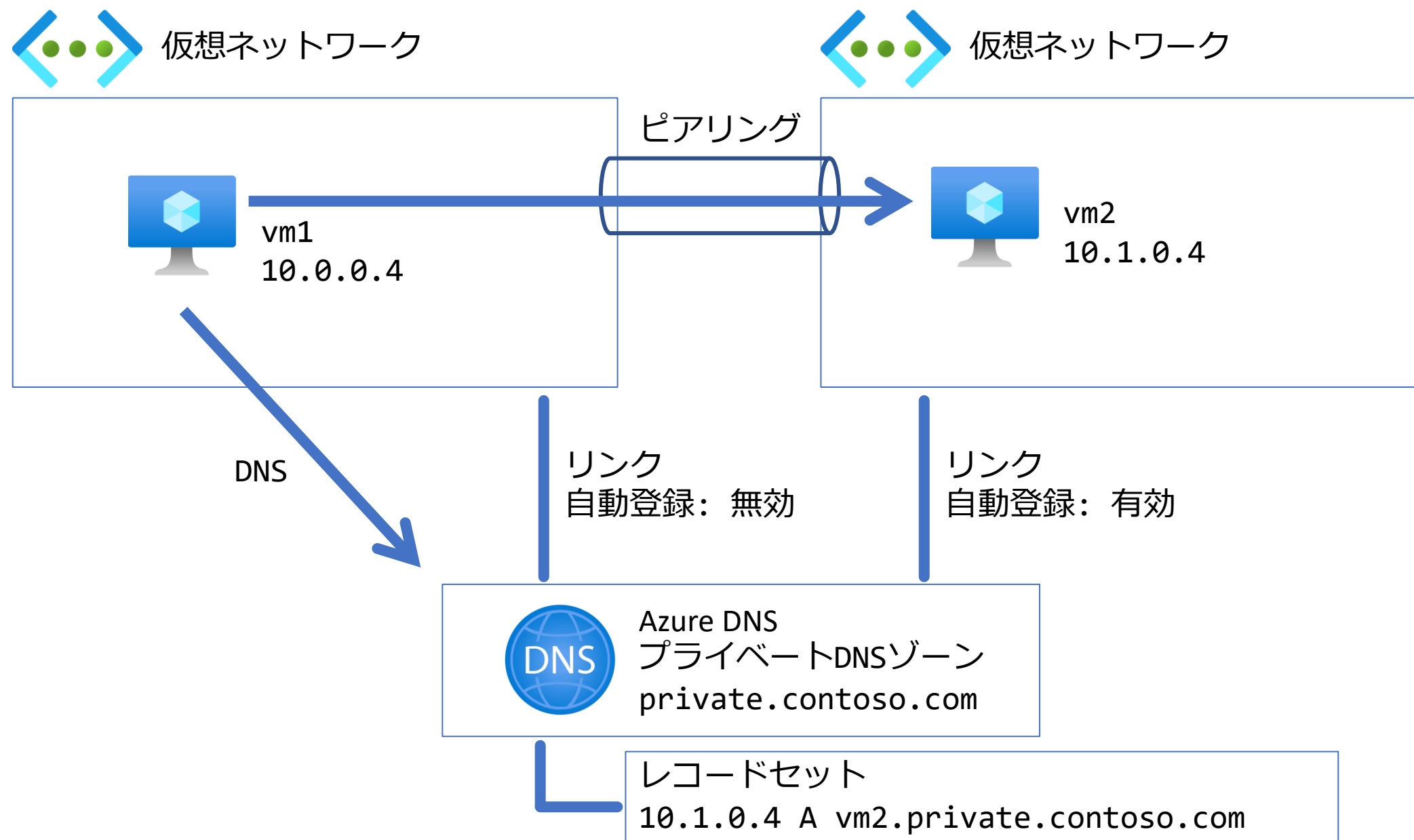
「リンク」したVNet上での
名前解決。

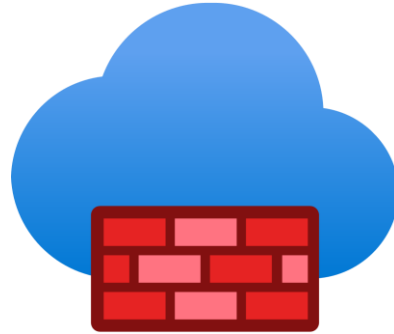


パブリックDNSゾーン



プライベートDNSゾーン





Azure Firewall

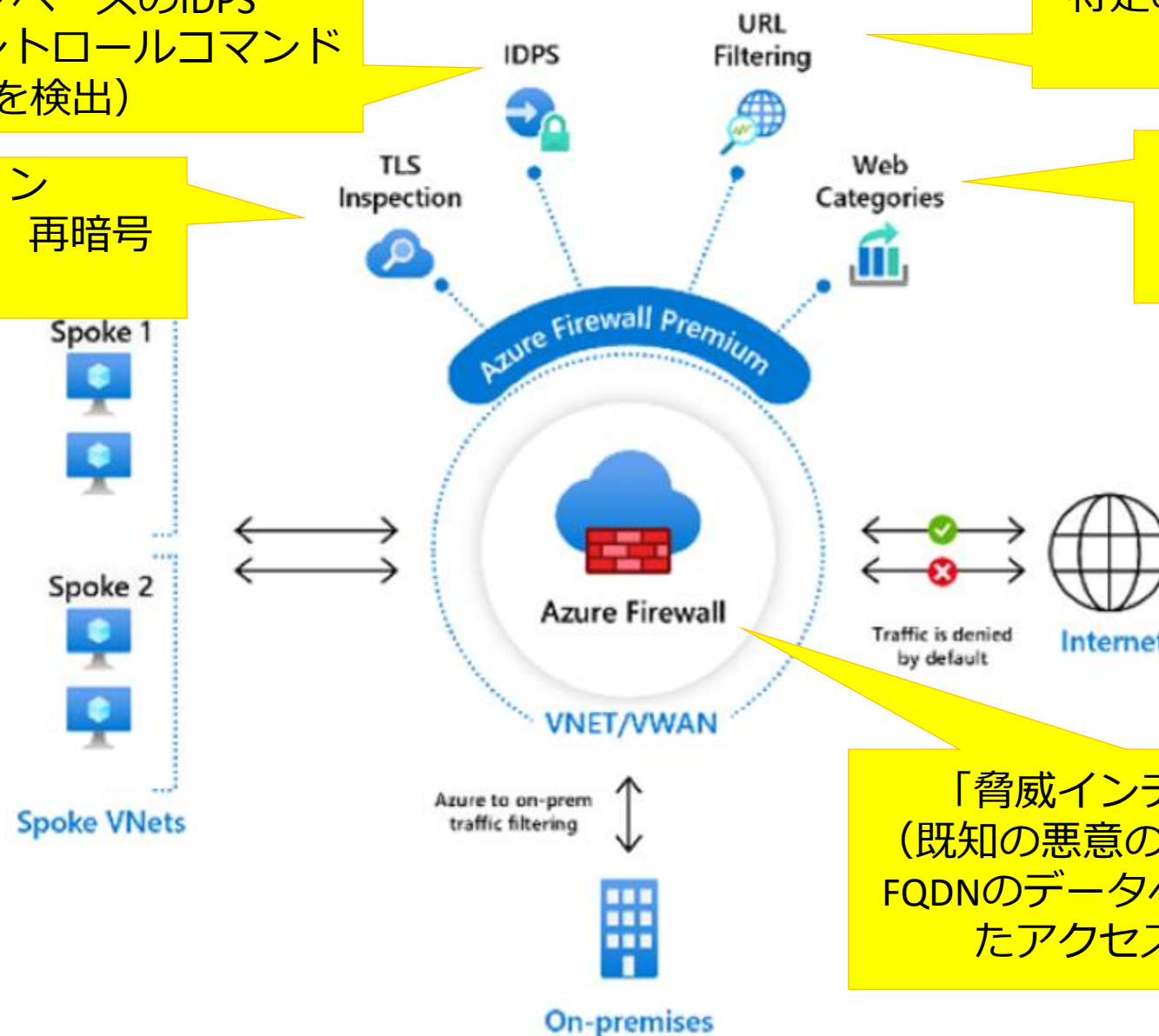
Azure Firewall: 無制限のスケーラビリティを備えた「Firewall as a Service」(FWaaS)

シグネチャベースのIDPS
(ボットのコントロールコマンド
などを検出)

TLSインスペクション
(TLS通信を復号、検査、再暗号
化)

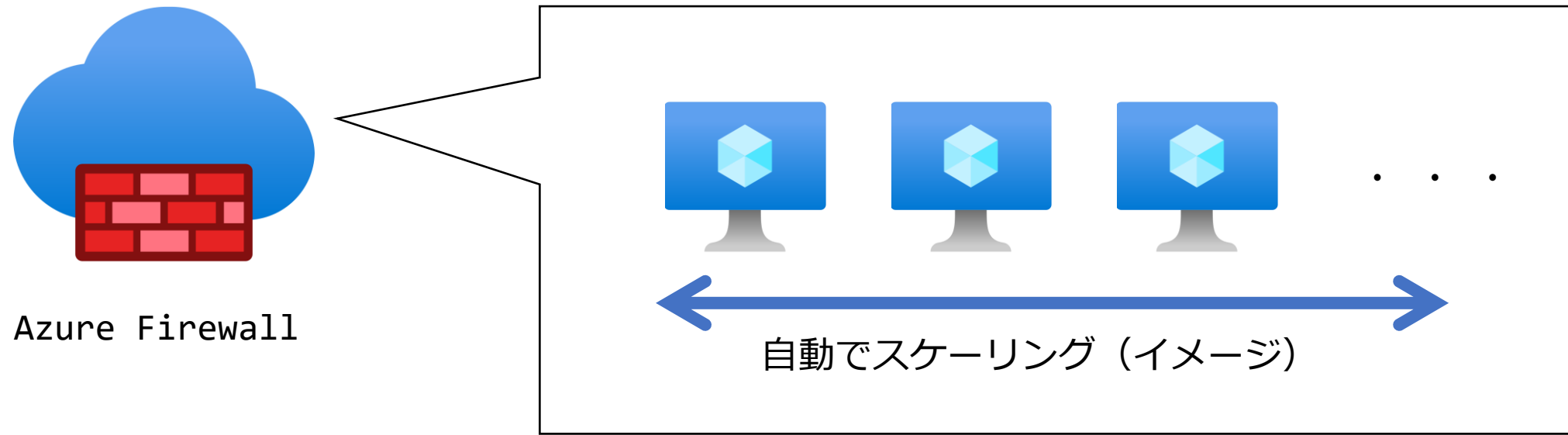
特定のURLへのアクセス
を禁止

特定のWebカテゴリー
(ギャンブル等) へのア
クセスを禁止



「脅威インテリジェンス」
(既知の悪意のあるIPアドレス・
FQDNのデータベース) を使用し
たアクセス制御、警告

Azure Firewall: **無制限のスケーラビリティ**を備えた「Firewall as a Service」(FWaaS)



	Basic	標準	Premium
デプロイメント	デプロイ時間あたり \$0.395	デプロイ時間あたり \$1.25	デプロイ時間あたり \$1.75
データ処理	処理 GB あたり \$0.065	処理 GB あたり \$0.016	処理 GB あたり \$0.016

デプロイされた時間と、処理されたデータ量に比例した料金が発生。
Basicのデプロイメント: 0.395 ドル * 24時間 * 30日 * 140円/ドル ≒ 4万円/月～

インバウンドトラフィックのフィルタリング



仮想ネットワーク



サブネット

※名前は任意



仮想マシン



ルート
テーブル



AzureFirewallSubnet

※この名前である必要がある



Azure Firewall
10.0.1.4

DNAT

Azure FirewallのパブリックIPアドレス
11.22.33.44

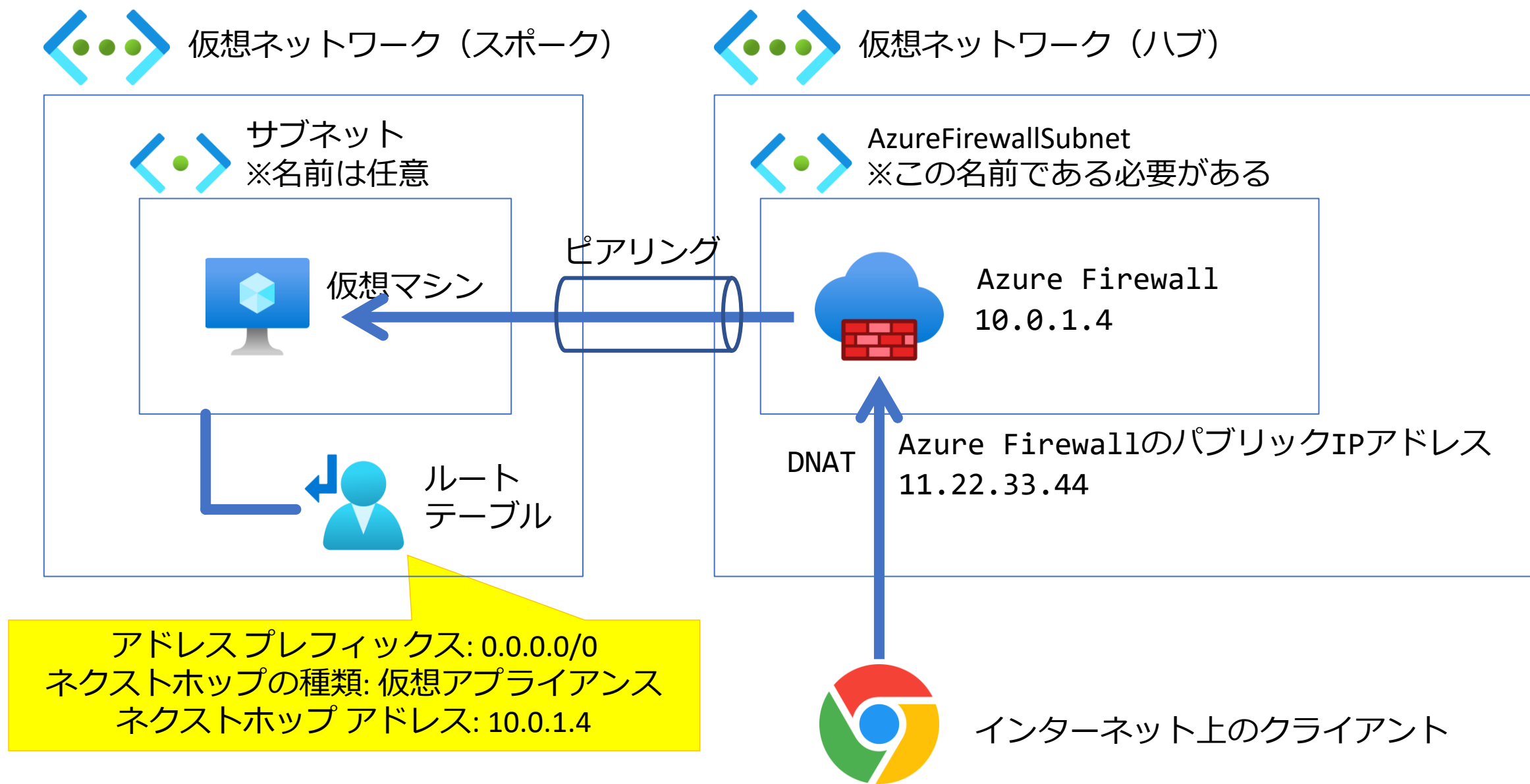


インターネット上のクライアント

アドレスプレフィックス: 0.0.0.0/0
ネクストホップの種類: 仮想アプライアンス
ネクストホップ アドレス: 10.0.1.4

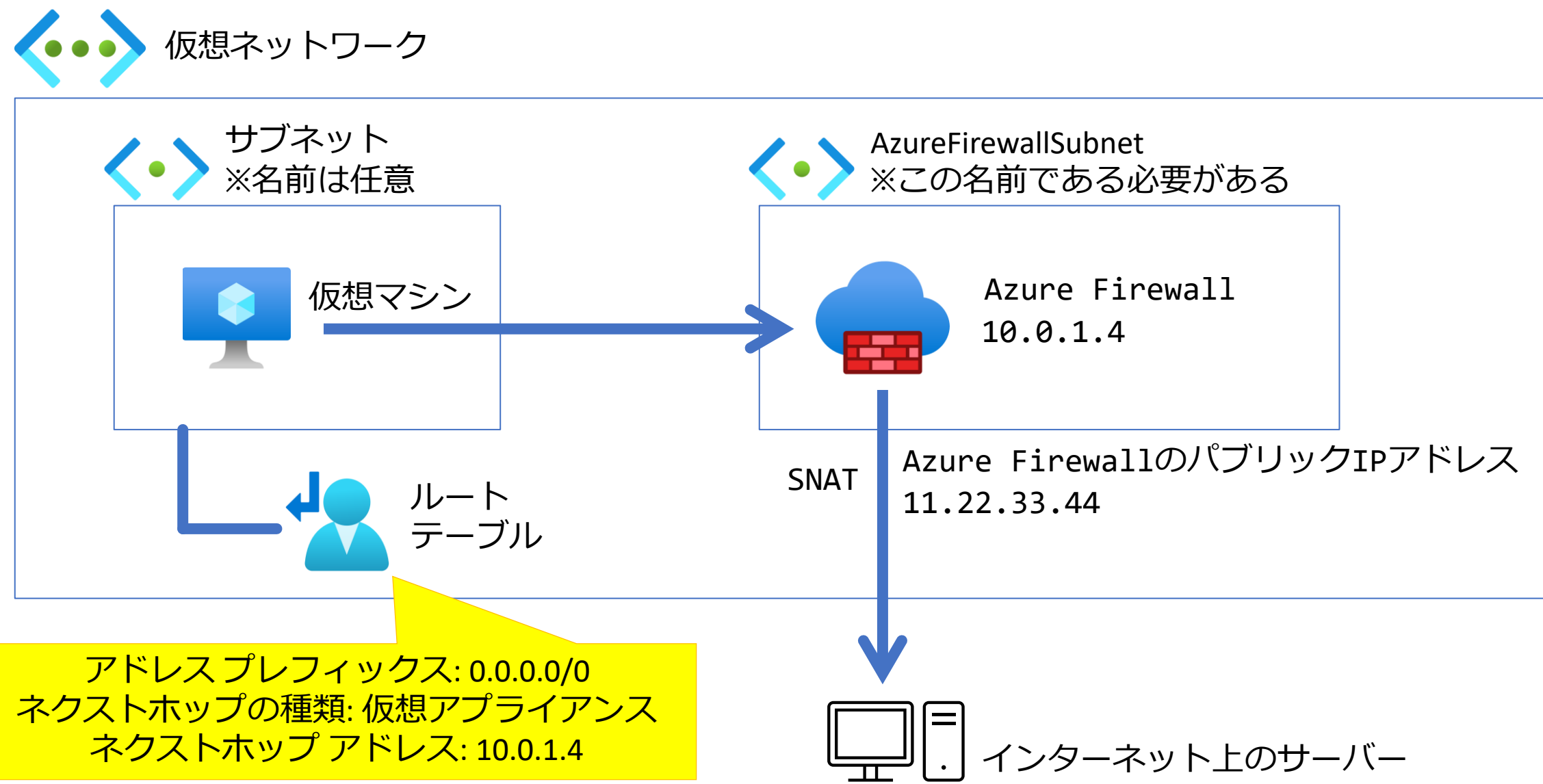
※Azure Firewallは仮想アプライアンスではないが、ルートテーブルの設定上は仮想アプライアンスとする

インバウンドトラフィックのフィルタリング



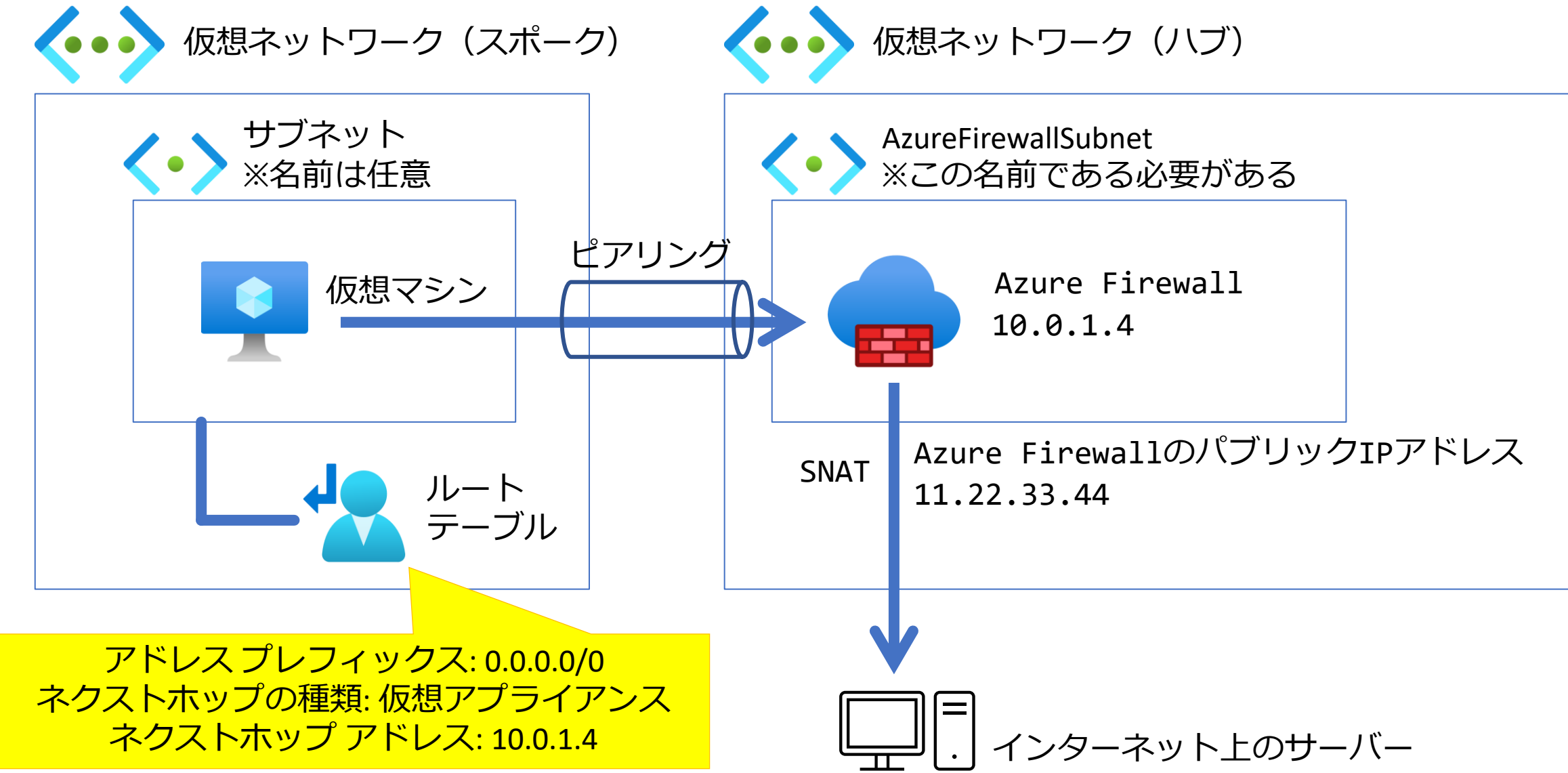
※Azure Firewallは仮想アプライアンスではないが、ルートテーブルの設定上は仮想アプライアンスとする

アウトバウンドトラフィックのフィルタリング ※1つの仮想ネットワークでの運用



※Azure Firewallは仮想アプライアンスではないが、ルートテーブルの設定上は仮想アプライアンスとする

アウトバウンドトラフィックのフィルタリング ※ハブ&スポーク トポロジでの運用



※Azure Firewallは仮想アプライアンスではないが、ルートテーブルの設定上は仮想アプライアンスとする