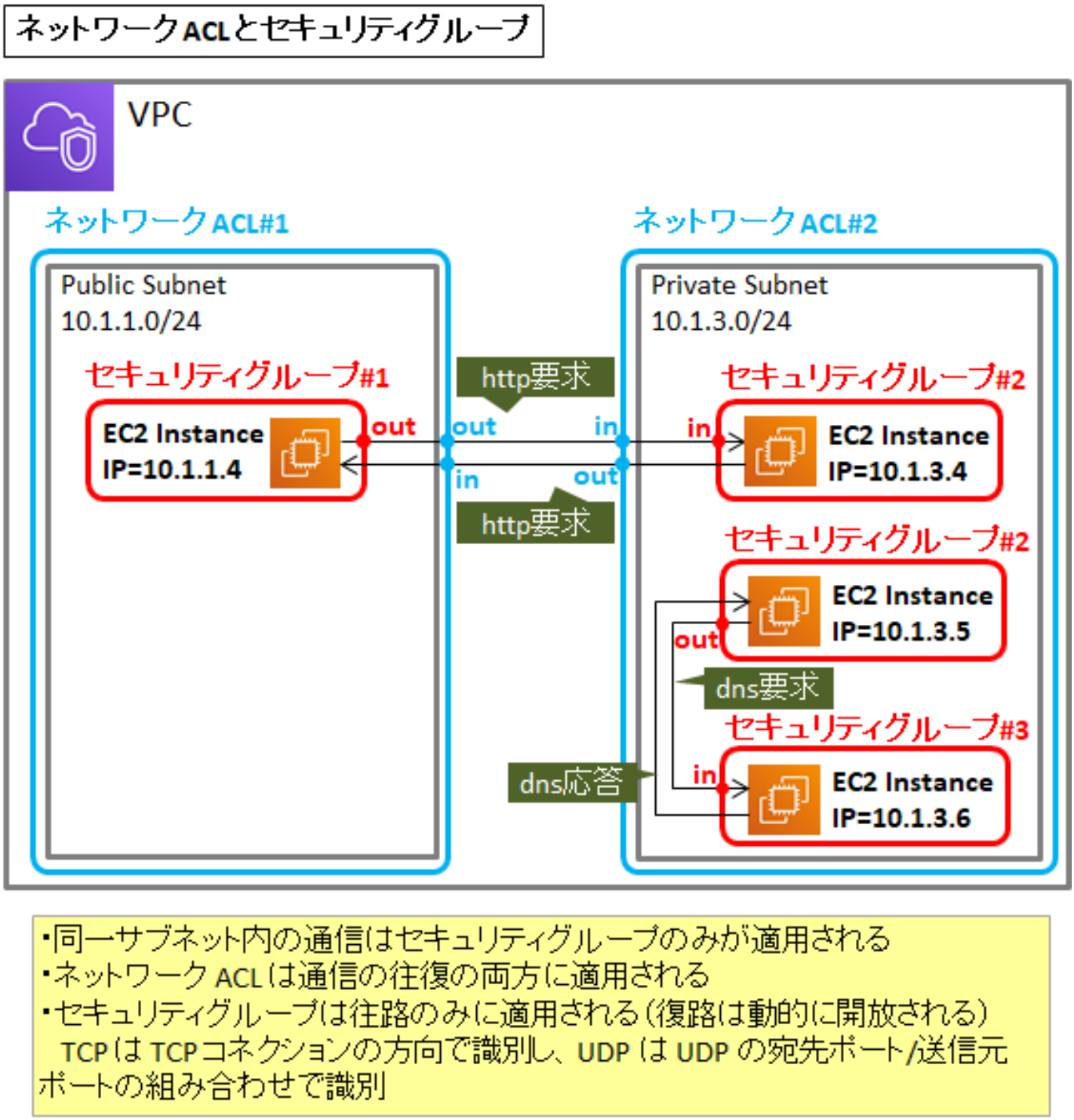
【図解/AWS】ネットワークACLとセキュリティグループの違いと優先度、復路の制御について～

2020.08.01　2019.04.08

ネットワーク ACL とセキュリティグループはどちらも **NW レベル(IP, TCP/UDP レベル) で通信を許可 or 拒否する仕組み**です。この記事ではこの2つの違いや優先度を解説していきます。

ネットワーク ACL とセキュリティグループの違い

ネットワーク ACL はサブネットに適用され、セキュリティグループは EC2 等のインスタンスにセットされます。以下の図ではその様子を表しています。ネットワークACLで制御されるタイミングを青丸、セキュリティグループで制御されるタイミングを赤丸で示しています。



図にある通り、**ネットワーク ACL は通信の往復の両方に適用**されますが、**セキュリティグループは往路のみに適用**されます。復路については動的に許可（開放）されます。

往路と復路の識別は、TCP の場合は TCP コネクションの方向で識別し、UDP の場合は擬似コネクションという形で、UDP の宛先ポート/送信元ポートの組み合わせで識別します。このような復路を動的に許可する仕組みを「ステートフル・インスペクション」と呼びます。ステートフルとステートレスは使うレイヤーによって具体的な意味合いが異なります。詳細については以下を参照下さい。

【初心者向け】ステートフル(Stateful)とステートレス(Stateless)の違い,IPv6やAWSでの考え方

ステートフルとステートレスの違いは気が利く奴か否か ステートフルとは、状況に

よ...

milestone-of-se.nesuke.com 2020.03.09

ネットワークACLとセキュリティグループの機能比較を以下に示します。

	ネットワークACL	セキュリティグループ
主な機能	サブネット間を跨ぐ通信のアクセス制御	サーバ(EC2等)との通信のアクセス制御
State	ステートレス(通信の復路も検査)	ステートフル(通信の復路は動的に許可)
ルール	許可・拒否のどちらかを指定可能	許可ルールのみを指定可能
方向	in と out で個別にルール設定可	in と out で個別にルール設定可

優先度について

先ほどの図から分かる通り、ネットワークACLとセキュリティグループでどちらのルールが優先というのは無いです。2つとも設定されている場合は、両方で許可されていないと通信できません。

評価の順番について

AWS 公式ページの比較表ではネットワークACLのルールの評価の順序性については、

> トラフィックを許可するかどうかを決めるときに、順番にルールを処理します

とあり、セキュリティグループのルールの評価については、

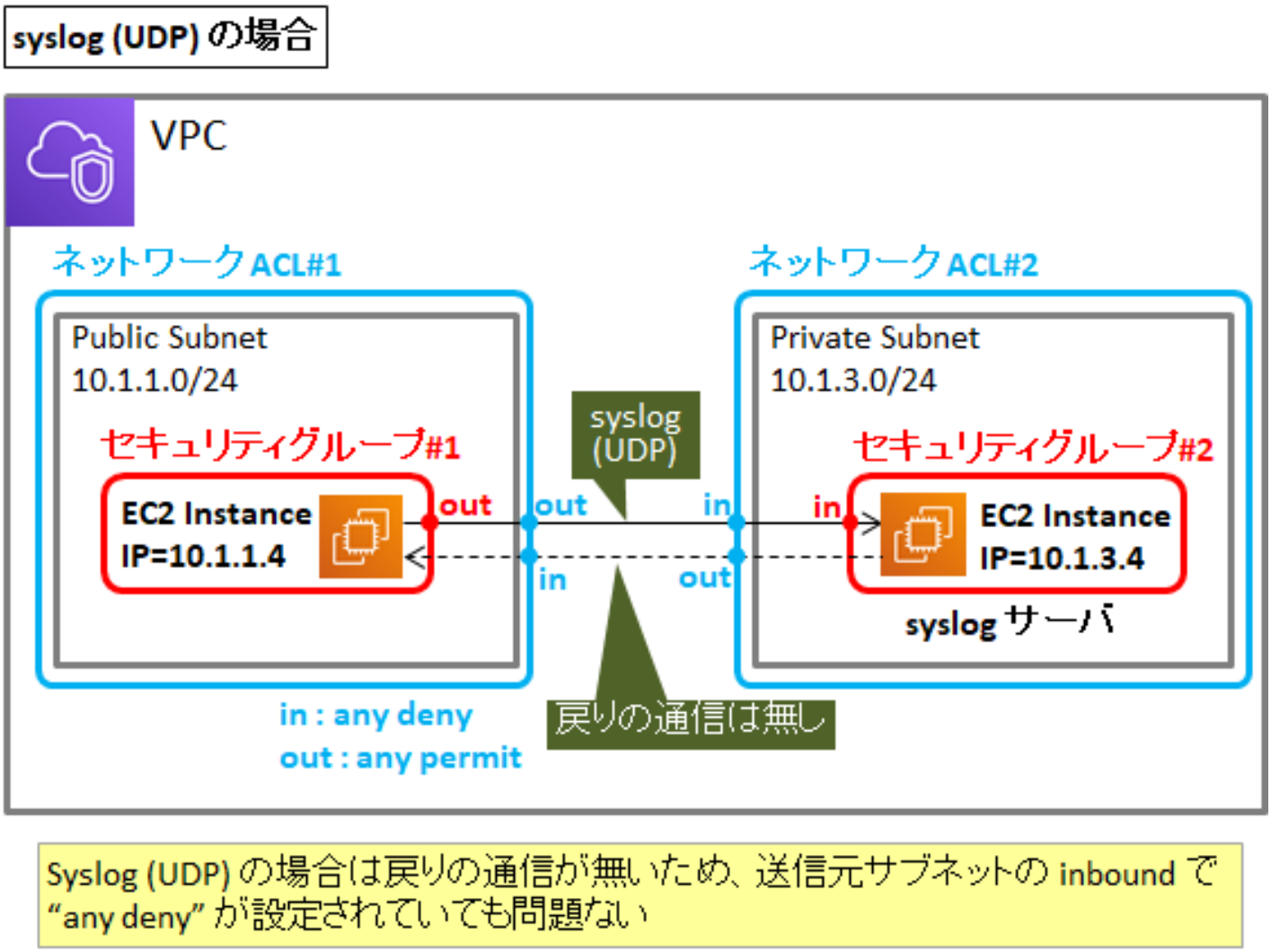
> トラフィックを許可するかどうかを決める前に、すべてのルールを評価します

と記載されていますが、セキュリティグループは許可ルールのみを指定し、最後は暗黙の Deny なので、（ネットワークACLと同じように）上から順番にルールを評価した場合と同じ結果になります。（なぜこのような書き方をしたのかは不明）

ネットワークACLの復路の許可ルールの必要性について

「セキュリティグループについては復路の許可設定が不要」であることを先ほど説明しましたが、ネットワークACLは基本的には復路の通信を考慮し、その許可設定をする必要があります。

ただし、一部のプロトコルはそもそも復路の通信が無いので、その場合は考慮不要です。具体的なプロトコルでいえば、syslog (UDP), SNMP trap, netflow/sflow 等です。



Syslog (UDP) の場合は戻りの通信が無いため、送信元サブネットの inbound で “any deny” が設定されていても問題ない

syslog は TCP を使えるものも多いので、TCP の場合は (TCP ack を返すので) 戻りの許可が必要ですが、UDP の場合は一方的に送るだけなので考慮不要です。

また、SNMP のMIB のポーリング (UDP:161) については往復しますが、Trap については一方通行です（inform という仕組みを使う場合は往復します)。