【図解/AWS】インターネットGWとNAT-GWの違い～各メリット、パブリックサブネットとは～

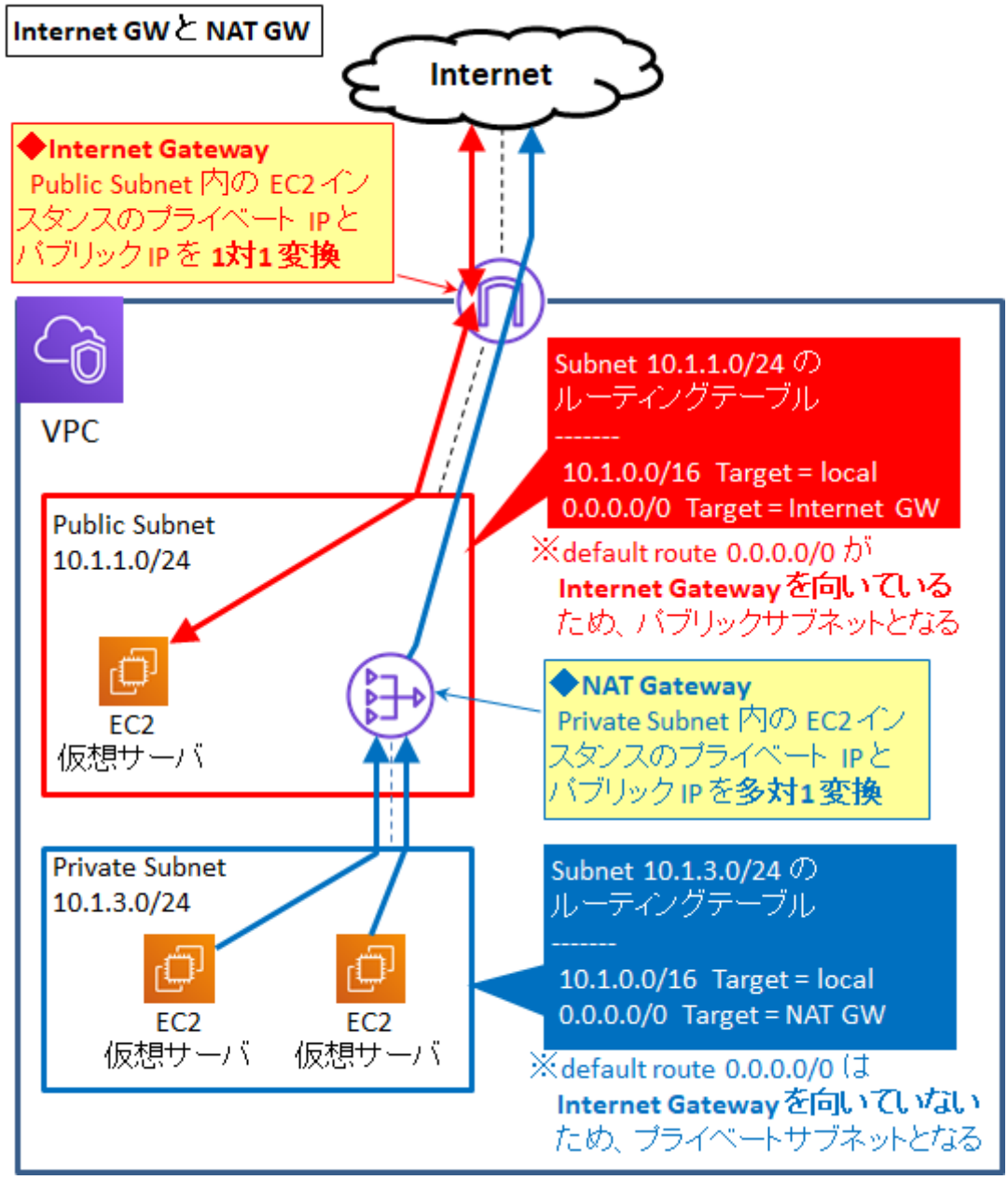
2021.01.21　2019.02.22

インターネットゲートウェイとNAT ゲートウェイの違い

インターネットゲートウェイと NAT ゲートウェイはともに **NAT 機能を提供する、インターネット接続時に利用されるオブジェクト**です。

今回はインターネット gateway と NAT gateway の違いを比較してみました

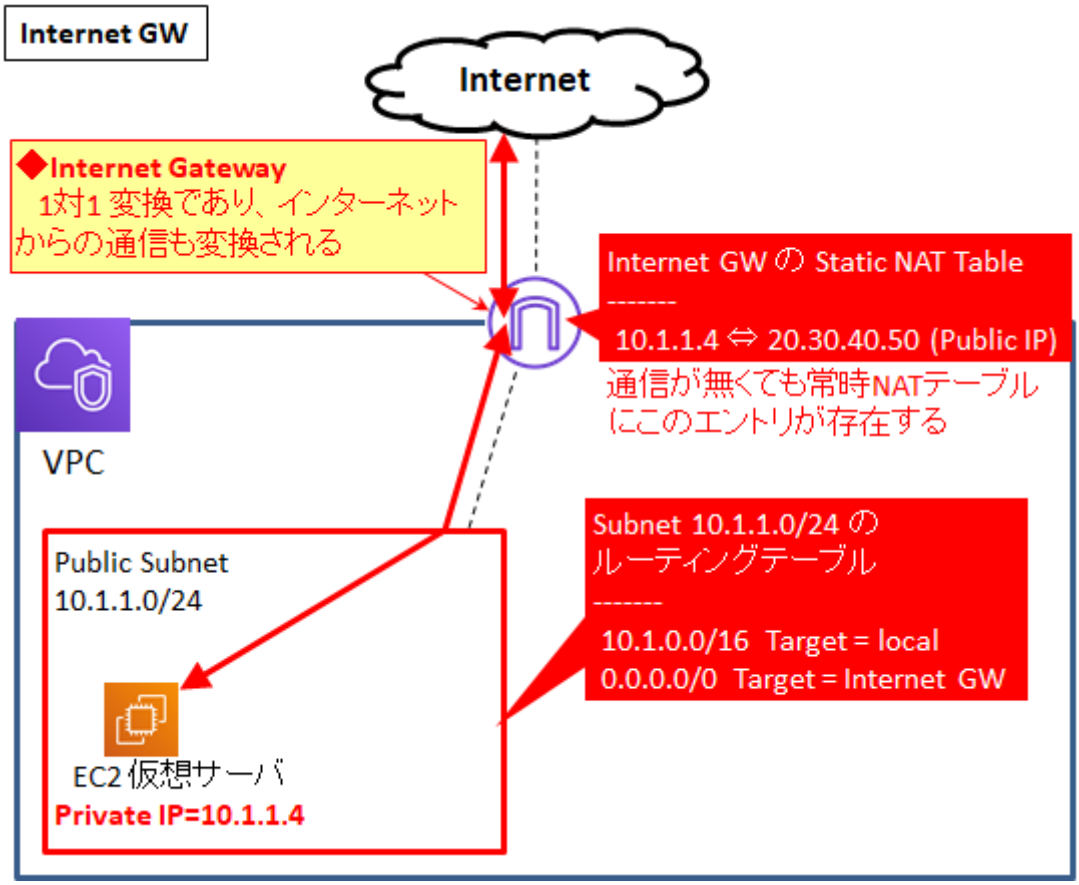
	インターネットGW	NAT GW
主な機能	- NAT - VPC ⇔ インターネット間の接続	- NAT (インターネットとの接続性には インターネットGWが必要)
NATの種類	- Static NAT	- Dynamic NAPT
配置場所	- VPC	- (パブリック)サブネット
速度制限	- 無し	- 5～45 Gbps



インターネットゲートウェイとは

インターネット GW は Static NAT を行います。つまり、パブリック IP を割り当てられた EC2 インスタンス等は、**プライベート IP とパブリック IP が 1 対 1 で変換**されます。

Static NAT の場合、NAT テーブルには通信前から「プライベート IP とパブリック IP の変換ルール」が定義されていますので、EC2 から始まる通信であっても、インターネットのクライアントから始まる通信であっても、IP は変換され、通信が可能です。



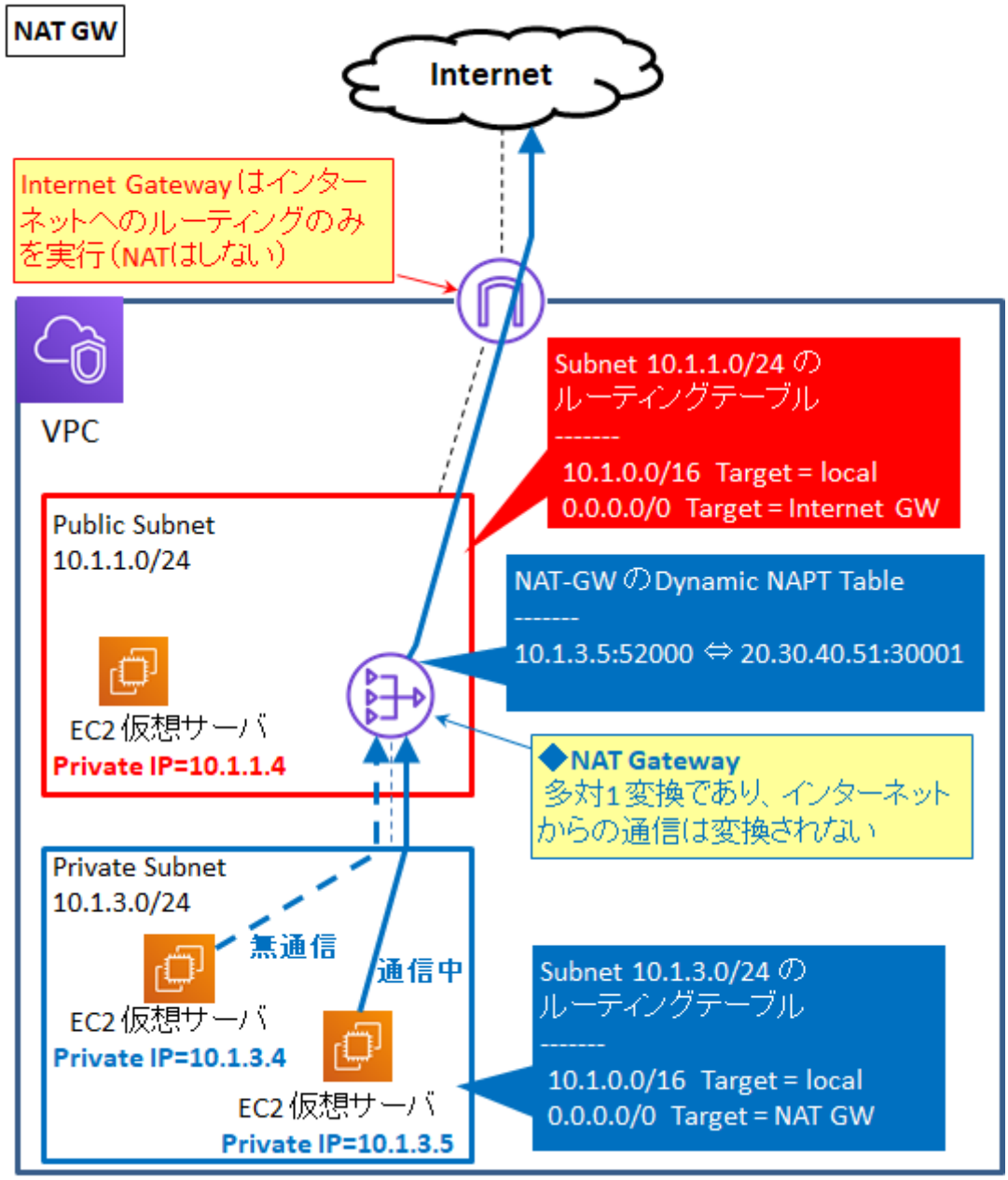
なのでインターネット GW の使い道は主に「インターネットからのアクセス」と「インターネットへのアクセス」の両方を実現することです。

インターネット GW は VPC に配置します。そしてインターネット GW を使いたい EC2 インスタンスは、「デフォルトルート 0.0.0.0/0 のターゲット」として "インターネットGW" を指定しているルーティングテーブルと関連付けられたサブネット（=パブリックサブネット）上に起動する必要があります。

NAT ゲートウェイとは

一方、**NAT-GW はプライベート IP とパブリック IP が多対 1 で変換されます**。複数の EC2 インスタンスから発する通信が、各々のプライベート IP で NAT-GW を通過する際、NAT-GW で 1 つのパブリック IP に変換されます。

ただし、複数のプライベート IP を 1 つのパブリック IP に変換してしまうと、戻りの通信においてどの通信がどのプライベート IP に変換すればいいか一意に定まらなくなってしまうので、TCP/UDP ポート番号も変換することでそれを回避しています。**このような NAT 方式を「動的 NAPT (ナプト)=Dynamic NAPT」と呼びます**。



動的 NAPT では NAT テーブルは初期状態では空です。プライベート IP が入ってきたタイミングで変換と同時に動的に NAT エントリが生成されます。NAT エントリには変換前後の IP:TCP/UDP port (or ICMP) が含まれますので、インターネットからの戻りの通信はそのエントリを使って元の IP:TCP/UDP port (or ICMP) に戻されます。

つまり**インターネットから始まる通信は (NAT エントリが無いので) アクセスできません**。つまり、セキュリティを高めることができる、というメリットがあります。これは一般的な家庭 NAT ルータと同等の動きです。

NAT-GW の使い道は主に「インターネットからはアクセスされたくないけどインターネットへのアクセスは実施したい」というケースです。

なお、NAT-GW だけではインターネットとの接続性がありませんので、NAT-GW は「パブリックサブネット」に配置します。

「パブリックサブネット」とは、デフォルトルートのターゲットが「インターネットGW」となっているルーティングテーブルに関連付けられたサブネットです。

つまり、NAT-GW を使ってインターネットに出ていくためには、インターネット GW は必須ということです。