# AWSサイト間VPNの構築（1.AWSの基本設定）


2021.08.11　2021.08.10

【次回】AWSサイト間VPNの構築（2.AWSのEC2構築）

## AWSサイト間VPN接続とは

VPN(Virtual Private Network)とは、インターネットをはじめとする共用のネットワーク上に仮想的な専用線を構築し、セキュアな通信を実現するための技術です。AWSサイト間VPN(AWS Site-to-Site VPN)は、「ローカル環境(オンプレミス環境等)」と「AWSのVPC」との間でVPNを構築し、相互のLAN同士の通信を可能にします。

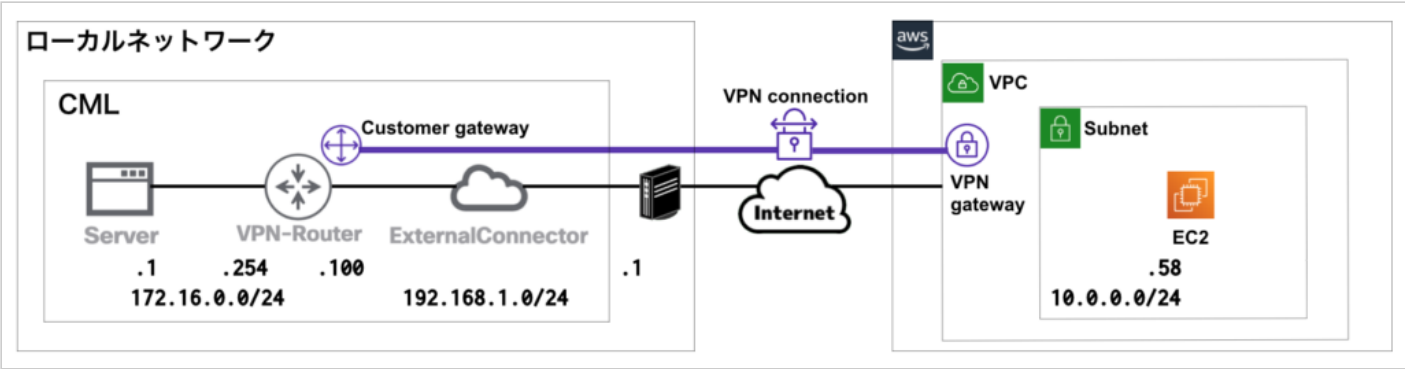
## AWSサイト間VPNの接続料金

AWSのサイト間VPNの接続料金は以下の通りとなっています。(2021年8月現在)
1時間あたり5円程度のため、1日120円ほどで検証環境を構築することが可能です。検証が終わった後は、AWS上のVPN接続を削除することを忘れないようにしましょう。


また、EC2のデータ転送料金が発生しますが、1GBまでは無料となっています。


# ネットワーク構成

下記のネットワーク構成で、CML上のLAN(172.16.0.0/24)とAWSのサブネット(10.0.0.0/24)が直接通信できるようにします。
※Server(172.16.0.1)からEC2(10.0.0.58)にPingによる疎通確認ができるようにしていきます。

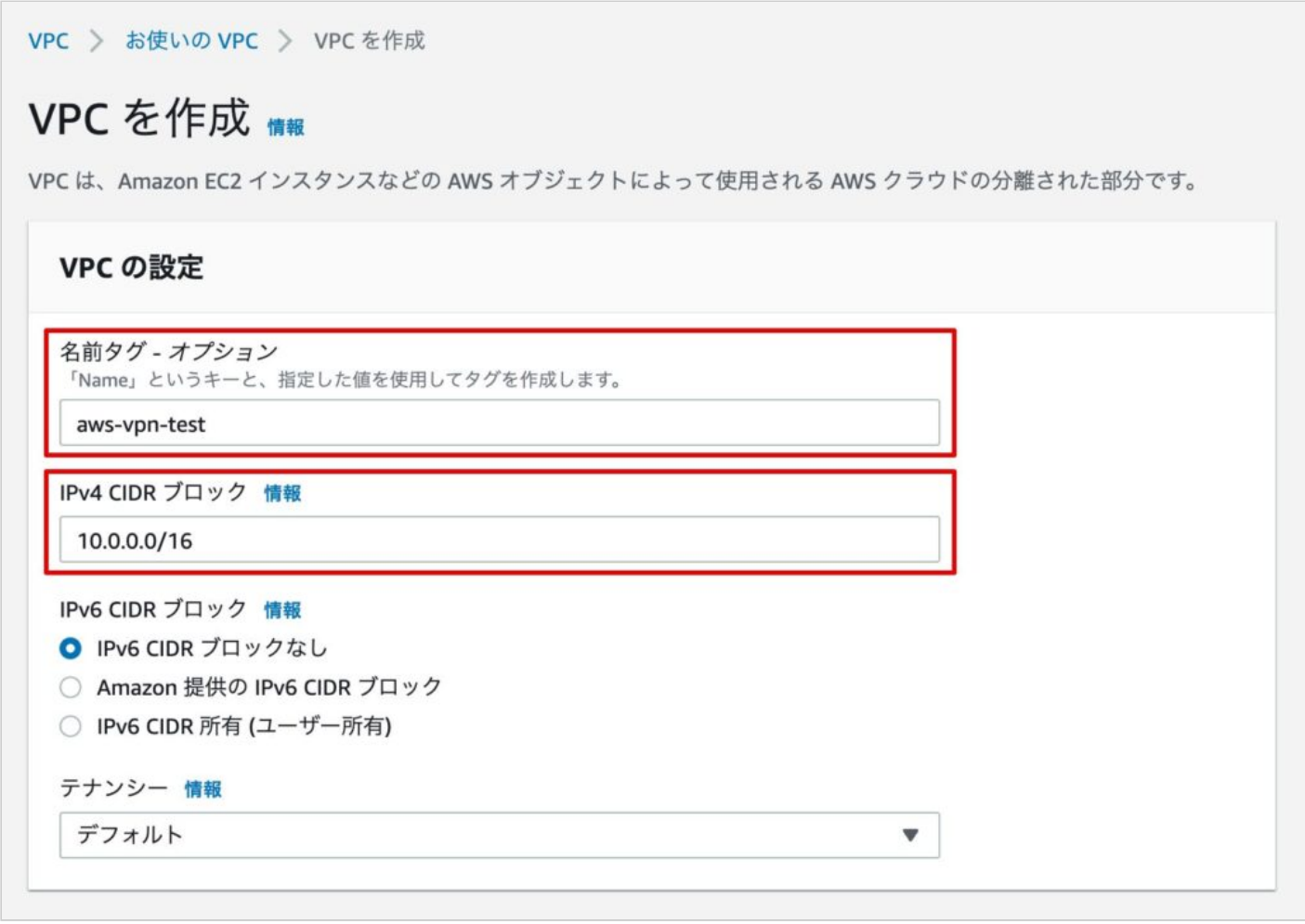



# AWSの基本設定

ここでは、検証用にAWS上で、VPC・インターネットゲートウェイ・ルートテーブル・サブネットを作成/設定していきます。

## VPCの作成

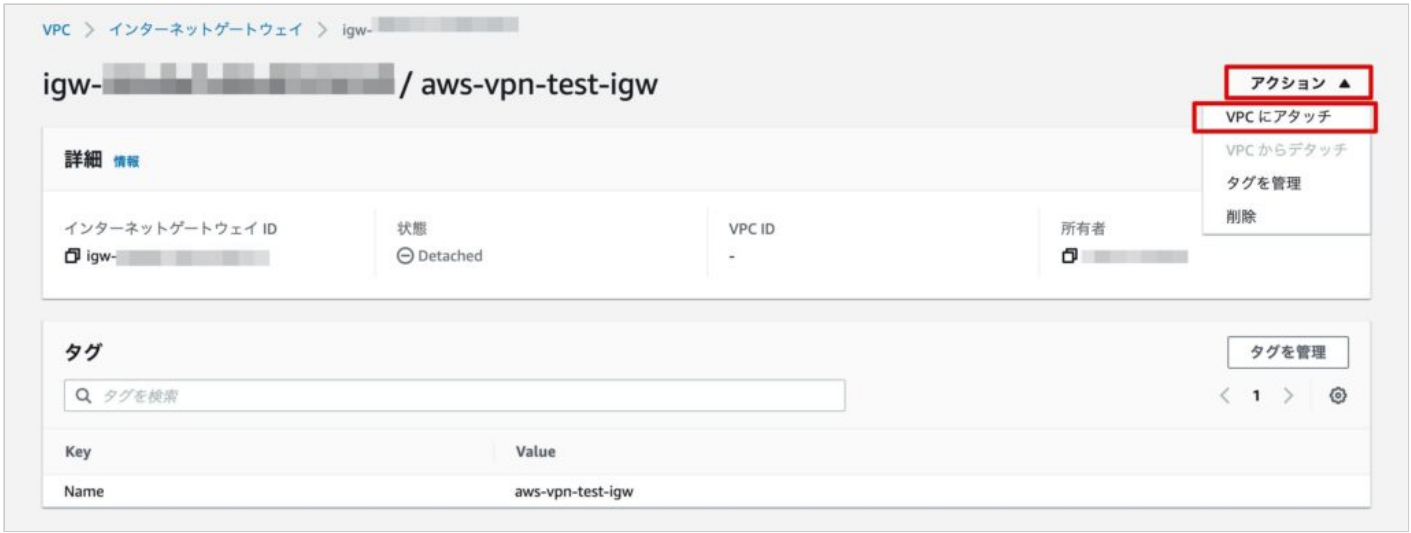
検証用のVPCを作成します。
「aws-vpn-test」という名前で作成し、「10.0.0.0/16」のCIDRブロックを割り当てています。




## インターネットゲートウェイの作成

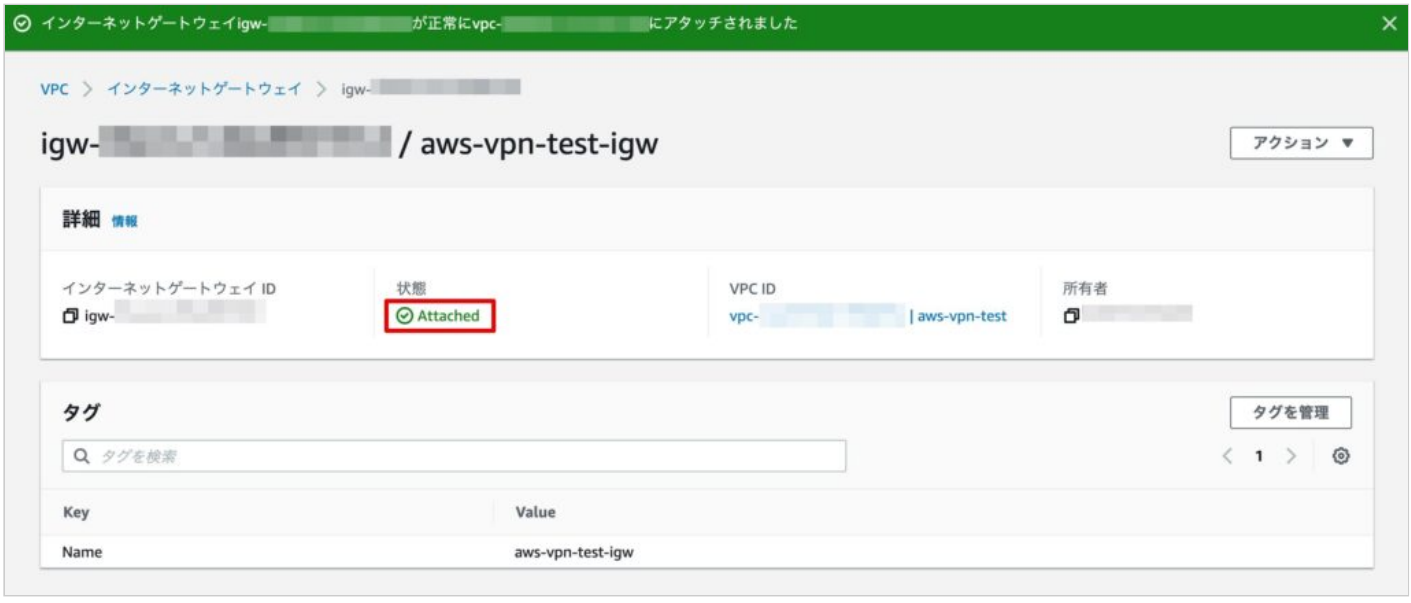
インターネット経由でVPNを構築するため、インターネットゲートウェイを作成します。
「aws-vpn-test-igw」という名前で作成しています。


作成したインターネットゲートウェイをVPCにアタッチします。
「アクション」→「VPCにアタッチ」を選択します。



作成したVPCを選択し、「インターネットゲートウェイのアタッチ」をクリックします。

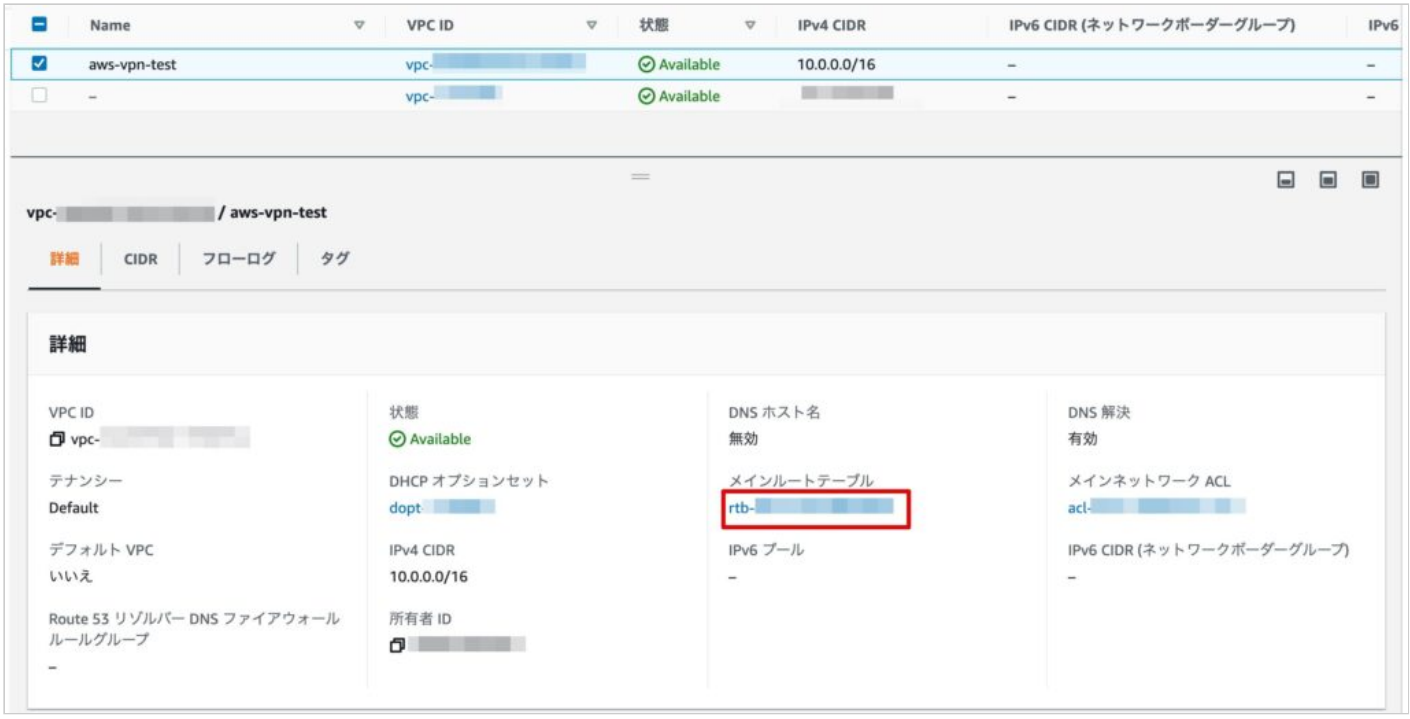

インターネットゲートウェイの状態が「Attached」となれば、VPCへのアタッチは完了です。




## ルートテーブルの設定

VPCのルートテーブルにインターネットゲートウェイを設定します。

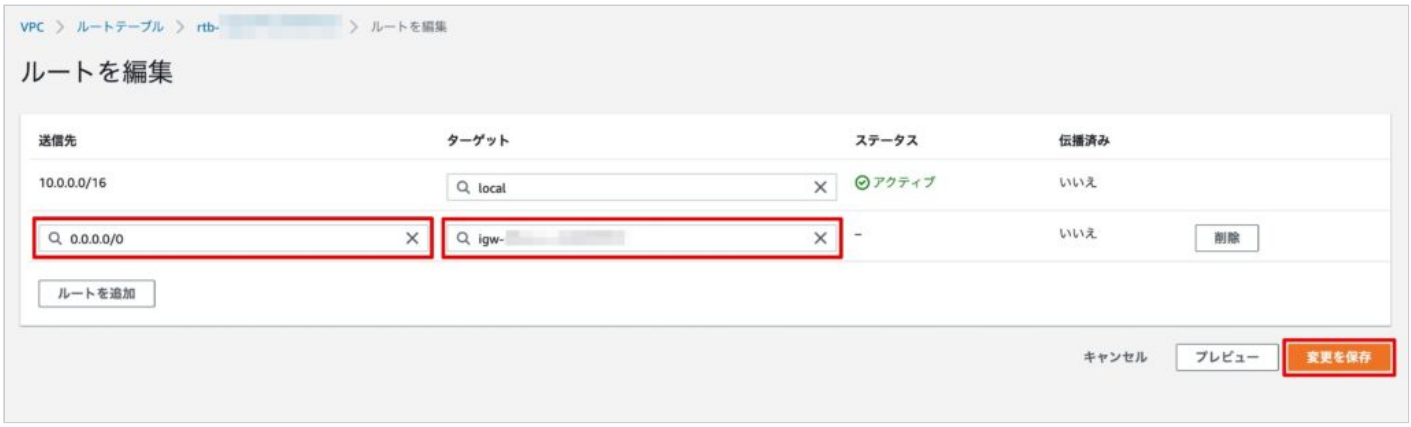
VPCの画面で、メインルートテーブル(rtb-XXXXXXXX)をクリックします。



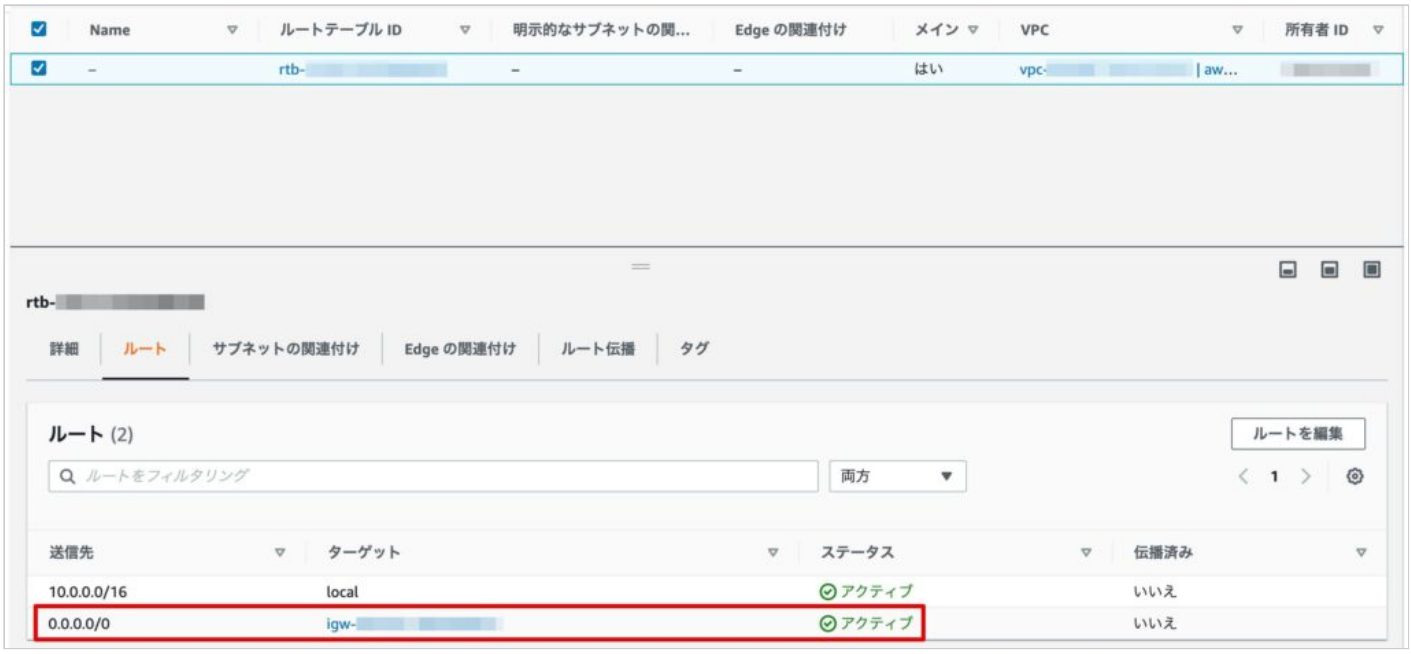

「ルート」タブを選択し、「ルート編集」をクリックします。


「ルートを追加」をクリックします。

送信先に「0.0.0.0/0」、ターゲットに「作成したインターネットゲートウェイ(igw-XXXXXXXX)」を入力し、「変更を保存」をクリックします。




追加したルートが表示されていれば、ルートテーブルの設定は完了です。




## サブネットの作成

EC2を配置するサブネットを作成します。

作成したVPC(aws-vpn-test)を選択します。


「aws-vpn-test-subnet1」という名前で、CIDRブロックは「10.0.0.0/24」を割り当てます。


これで、AWSサイト間VPN接続のためのAWSの基本設定は完了です！