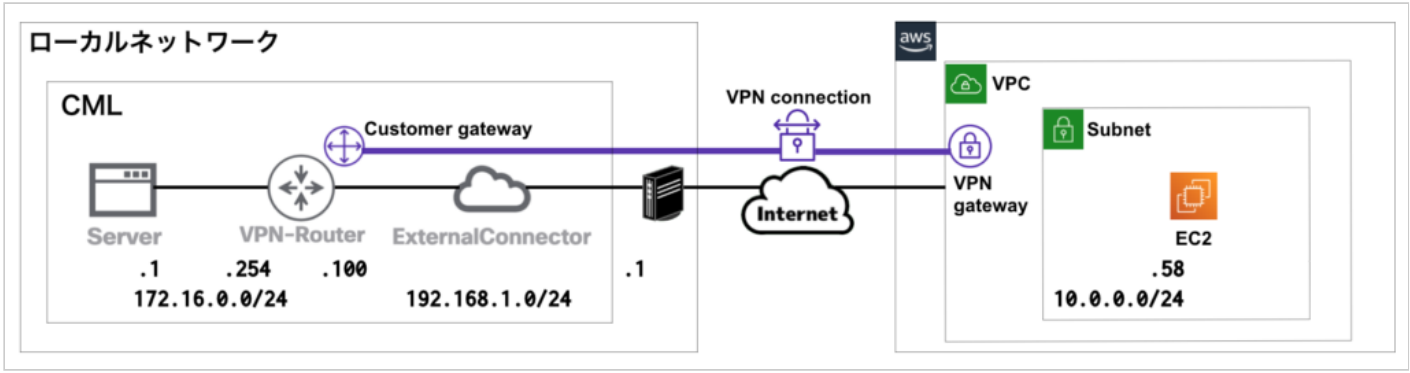
AWSサイト間VPNの構築（2.AWSのEC2構築）

2021.08.31　2021.08.11

【前回】AWSサイト間VPNの構築（1.AWSの基本設定）
【次回】AWSサイト間VPNの構築（3.AWSのVPN構築）

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。



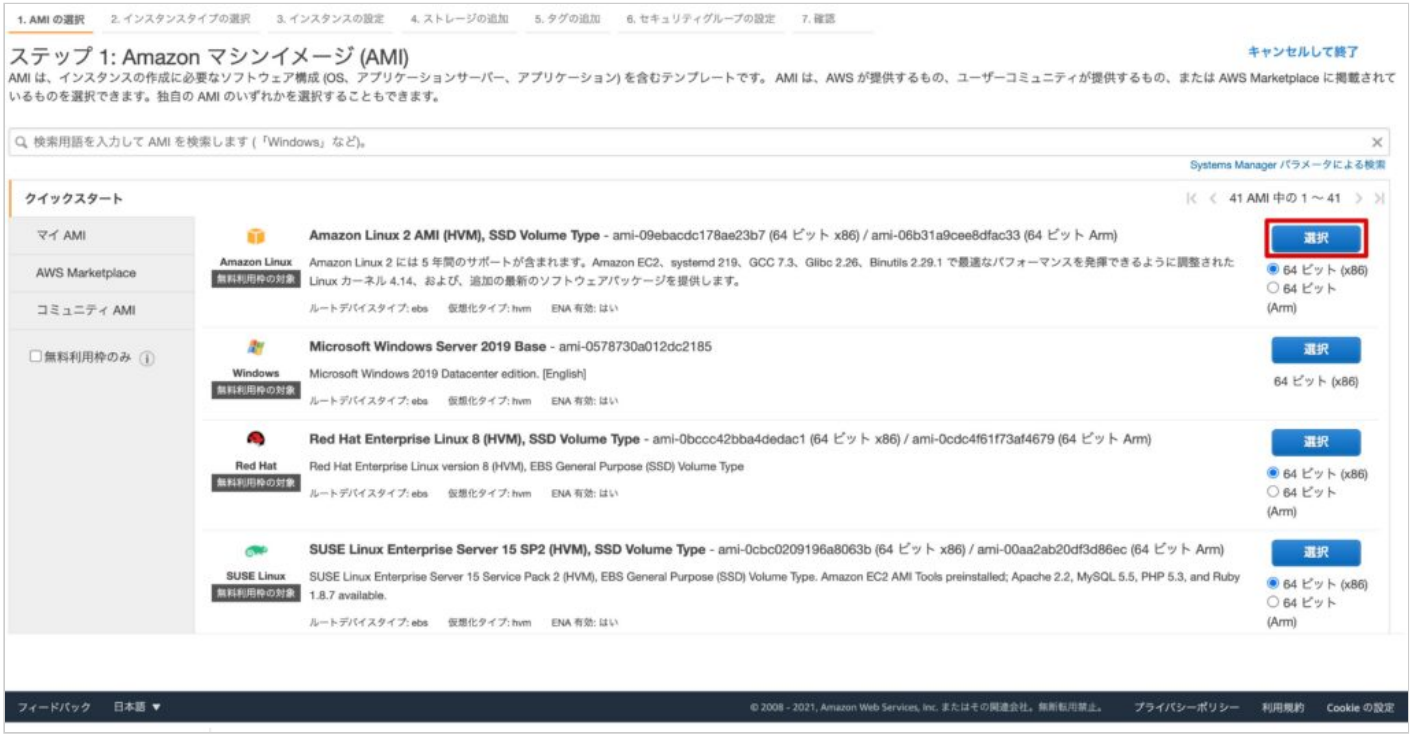
EC2構築

疎通先となるAWSのEC2を構築します。

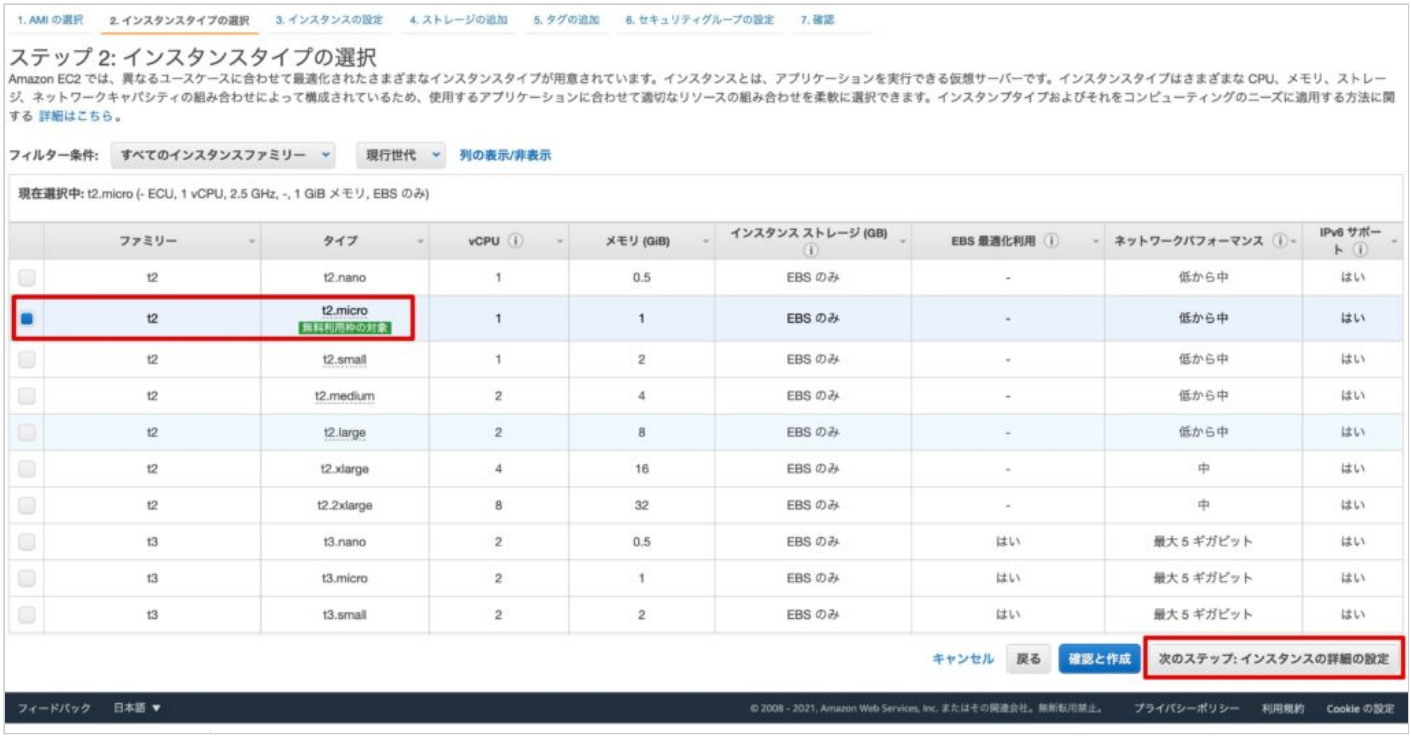
インスタンスの起動

EC2のトップ画面から「インスタンスの起動」をクリックします。

マシンイメージを選択します。ここでは、無料利用枠の対象となる「Amazon Linux」を選択しています。



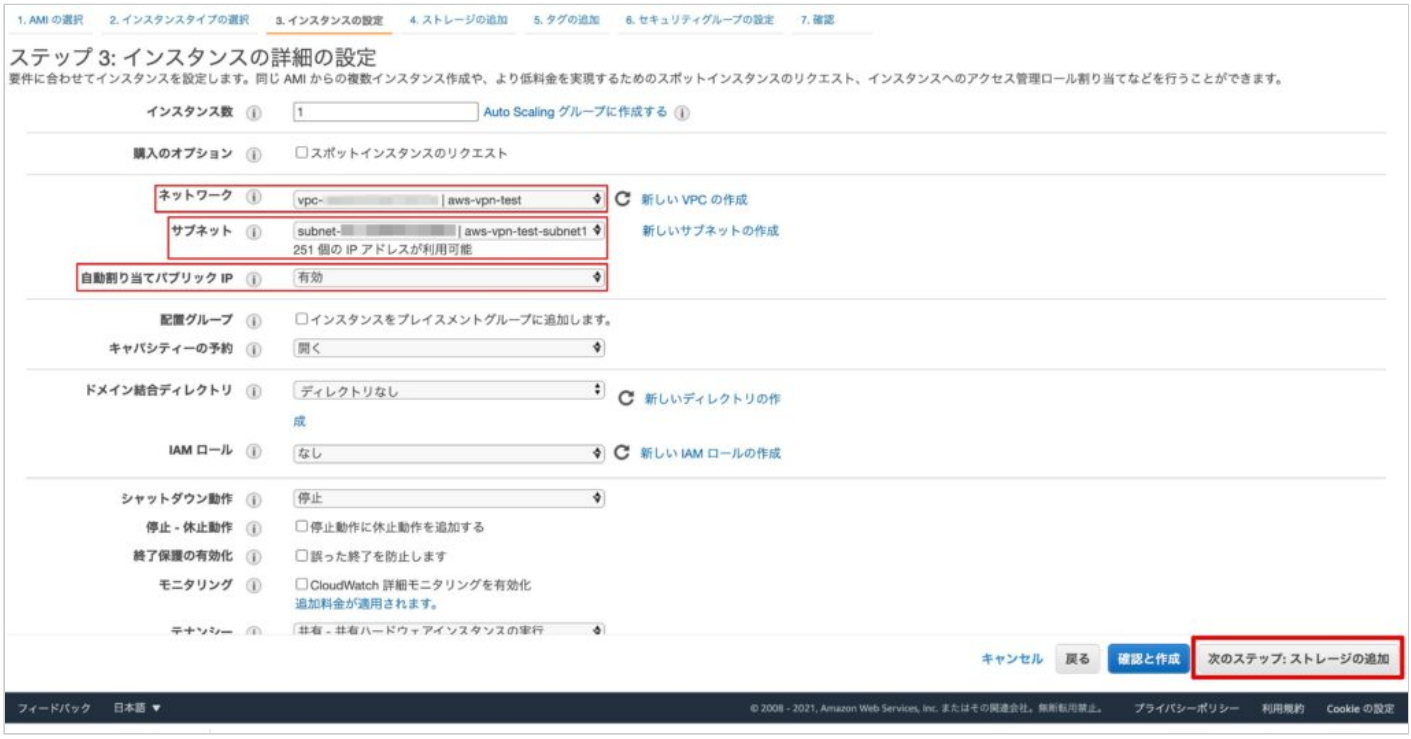
インスタンスタイプを選択します。ここでは無料利用枠の対象となる「t2.micro」を選択しています。



インスタンスの詳細を設定します。

ネットワークとサブネットは、前回作成したものを選択します。

自動割り当てパブリックIPは「有効」を選択します。



ストレージの設定は変更不要です。

タグの追加も変更不要です。

セキュリティグループの設定に関しては、デフォルトで「0.0.0.0/0(全てのIPアドレス)」からのSSHアクセスが許可されているため、自身のネットワークからのみアクセス可能となるように設定を変更します。

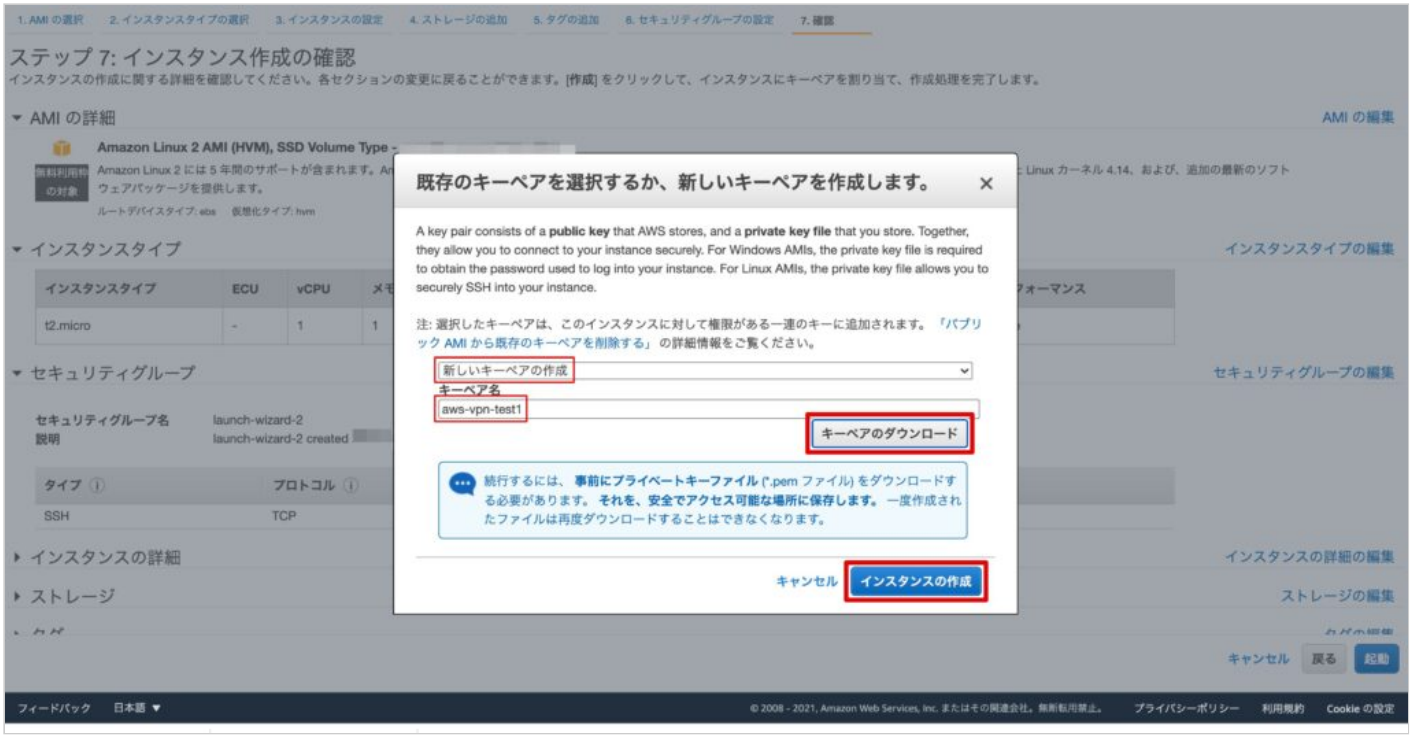
まず、自身が利用しているグローバルIPアドレスを確認します。

ここではCMANのIPアドレス確認ページで確認しています。

ソースに「確認したグローバルIPアドレス」を入力します。サブネットマスクは”/32"で大丈夫です。

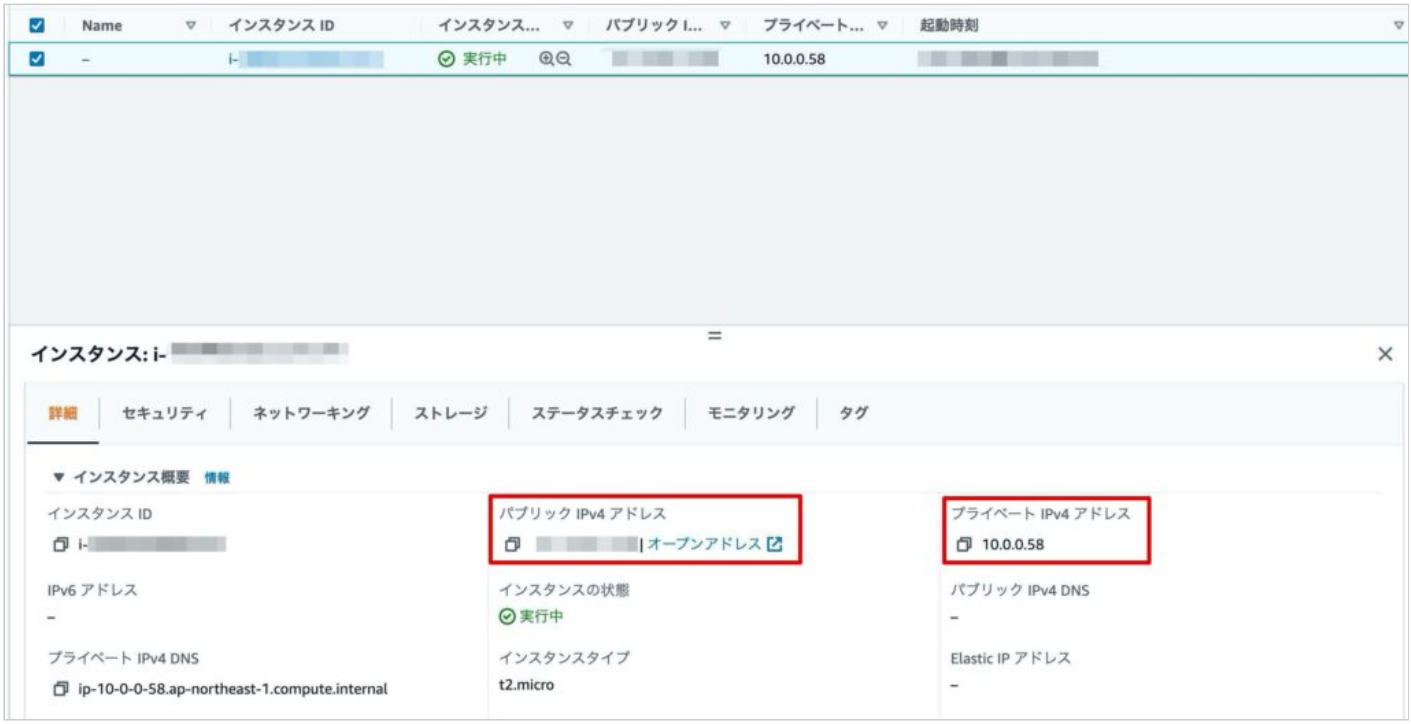
入力内容を確認し、「起動」をクリックします。

EC2にアクセスするためのキーペアを作成し、ダウンロードします。
「新しいキーペアの作成」を選択し、キーペア名は「aws-vpn-test1」としています。
キーペアをダウンロードし、「インスタンスの作成」をクリックします。



作成されたインスタンスを確認します。

※パブリックIPv4アドレスとプライベートIPv4アドレスが付与されていることを確認します。

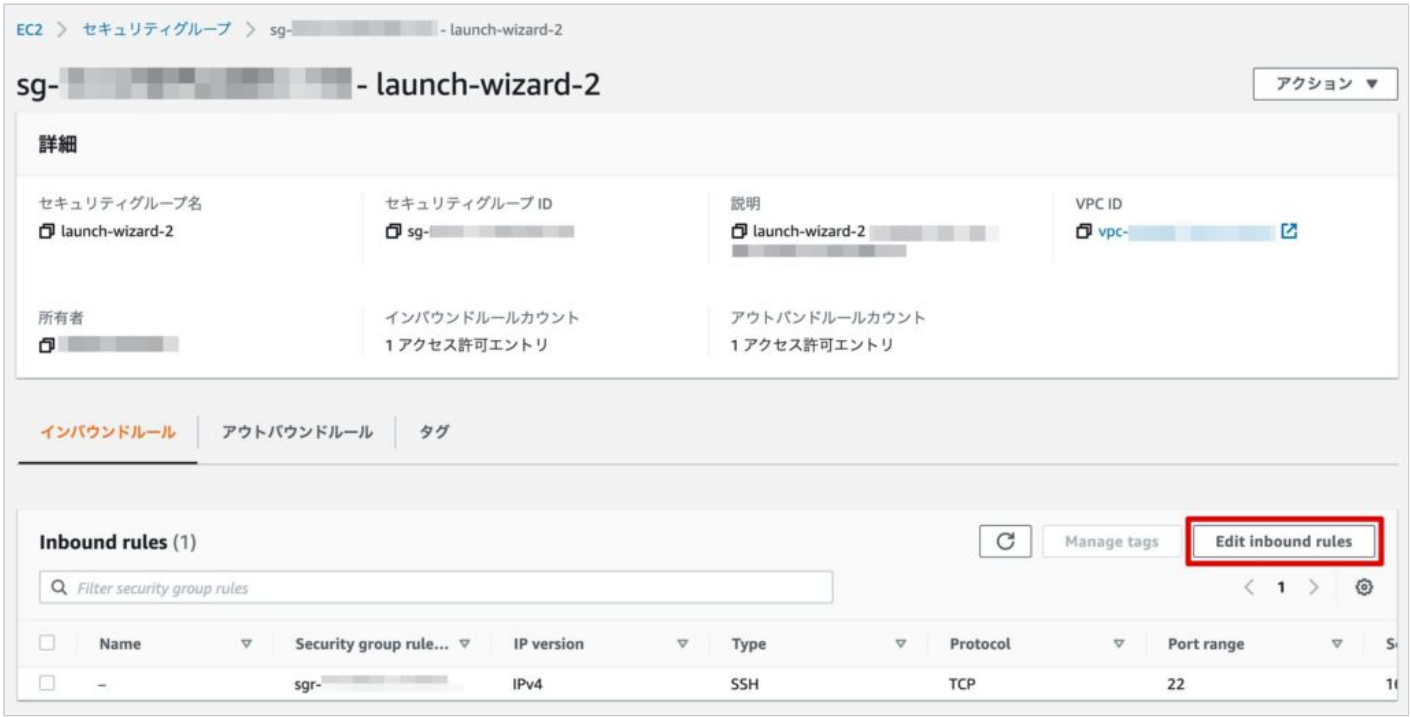


セキュリティグループの追加設定

CML環境からのアクセスを許可するために、セキュリティグループの追加設定を行います。

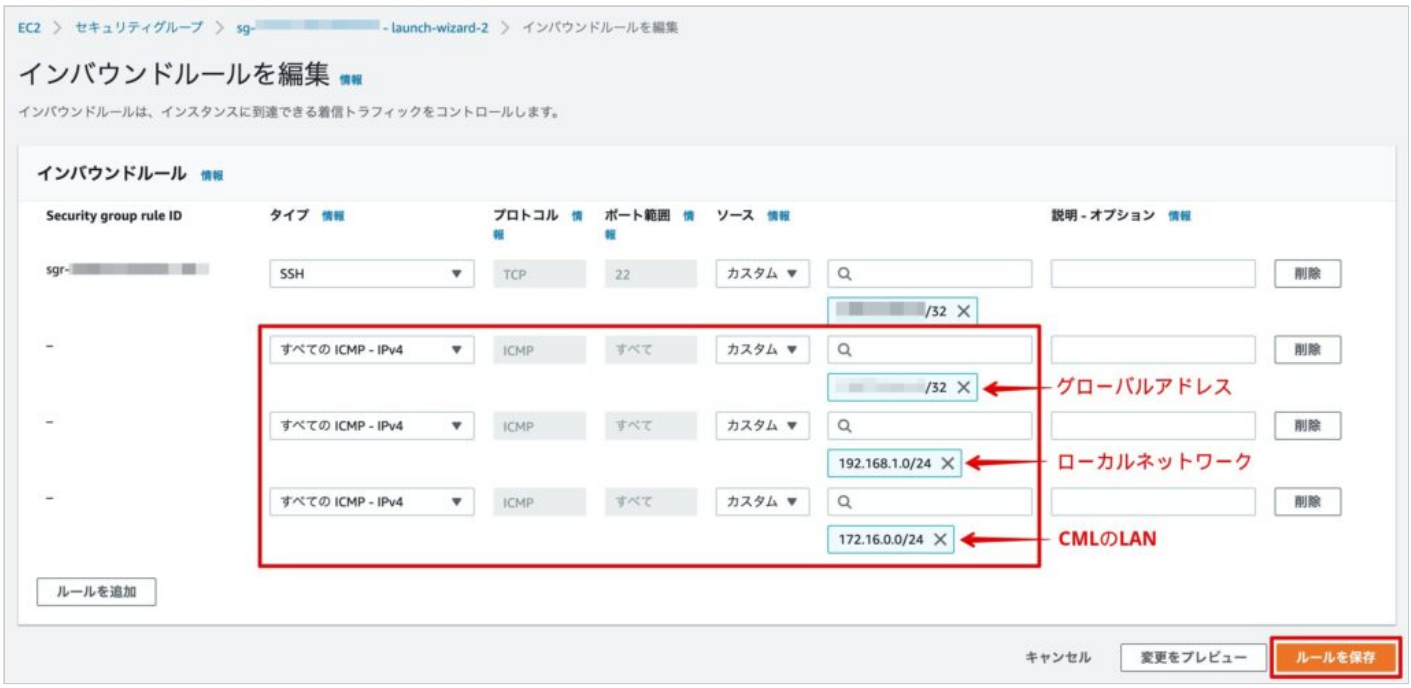
「セキュリティ」タブから「セキュリティグループ」をクリックします。

「Edit inbound rules」をクリックします。

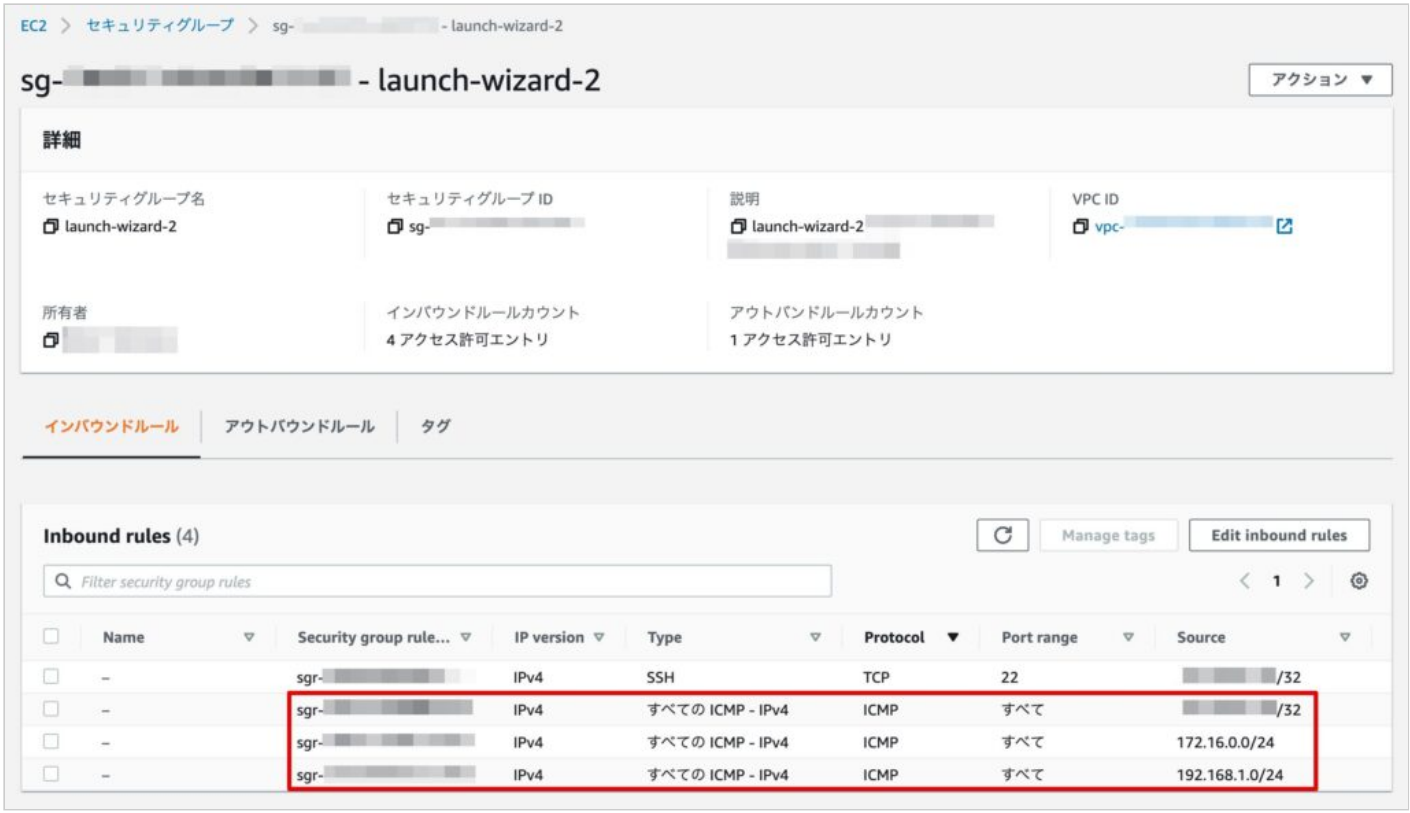


「ルールを追加」をクリックします。

グローバルアドレス、ローカルネットワーク(192.168.1.0/24)、CMLのLAN(172.16.0.0/24)からのICMP通信を許可します。



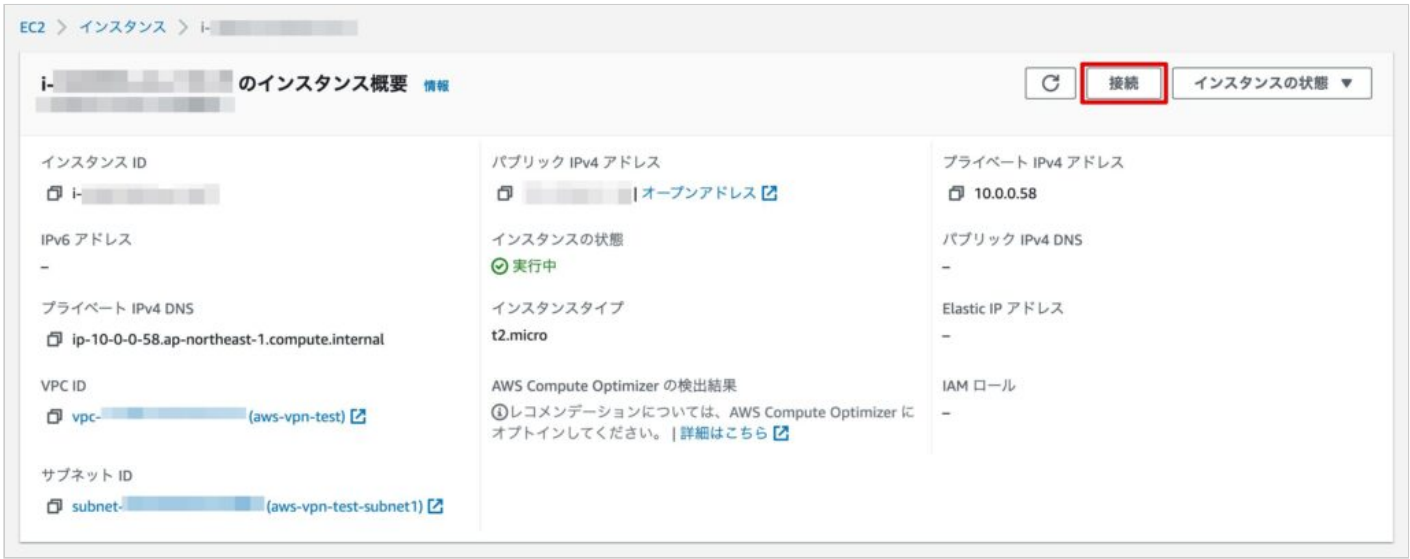
インバウンドルールに追加されていることを確認します。



EC2への接続確認

起動したEC2への接続を確認していきます。
※ここでは、MACのTerminalを利用し接続していきます。

インスタンスの画面から「接続」をクリックします。



「SSHクライアント」タブを選択し、アクセス方法を確認します。

ダウンロードしてキーペアを確認します。

```
[Terminal[AWS]:
[Terminal[AWS]: ls -l
total 8
-rw-r--r--@ 1                    1700                aws-vpn-test1.pem
[Terminal[AWS]:
```

このままSSH接続を試みると、キーペアのアクセス権が不適切というメッセージが表示され接続できません。

```
[Terminal[AWS]:
[Terminal[AWS]: ssh -i "aws-vpn-test1.pem" ec2-user@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'aws-vpn-test1.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "aws-vpn-test1.pem": bad permissions
ec2-user@                : Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[Terminal[AWS]:
```

AWSの接続説明にある通り、アクセス権を変更します。

```
[Terminal[AWS]:
[Terminal[AWS]: chmod 400 aws-vpn-test1.pem
[Terminal[AWS]:
```

アクセス権が変更されたことを確認します。

```
[Terminal[AWS]: ls -l
 total 8
 -r--------@ 1                1700              aws-vpn-test1.pem
[Terminal[AWS]:
```

再度SSH接続を試みると、EC2へ接続できました。

```
[Terminal[AWS]:
[Terminal[AWS]: ssh -i "aws-vpn-test1.pem" ec2-user@

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

 https://aws.amazon.com/amazon-linux-2/
 4 package(s) needed for security, out of 16 available
 Run "sudo yum update" to apply all updates.
[[ec2-user@ip-10-0-0-58 ~]$
```

これで、AWSサイト間VPN接続のためのEC2構築は完了です！