EC2 インスタンスへのセキュアなシェルログインを実現できる AWS Systems Manager(SSM) のセッションマネージャについて、設定方法や利用方法を紹介したいと思います。

セッションマネージャとは

> Session Manager はフルマネージド型 AWS Systems Manager 機能であり、インタラクティブなワンクリックブラウザベースのシェルや AWS Command Line Interface (AWS CLI) を介して Amazon Elastic Compute Cloud (Amazon EC2) インスタンス、オンプレミスインスタンス、および仮想マシン (VM) を管理できます。Session Manager を使用すると、インバウンドポートを開いたり、踏み台ホストを維持したり、SSH キーを管理したりすることなく、監査可能なインスタンスを安全に管理できます。また、Session Manager を使用すると、マネージドインスタンスへの簡単なワンクリックのクロスプラットフォームアクセスをエンドユーザーに提供しつつ、インスタンスへの制御されたアクセス、厳格なセキュリティプラクティス、完全に監査可能なログ (インスタンスアクセスの詳細を含む) が要求される企業ポリシーに簡単に準拠できます。

以上、公式ドキュメントからの抜き出しです
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/session-manager.html

ブラウザ等からシェルログインができるサービスで、従来の SSH と比較して下記のメリットがあります。

・ SSH キー不要
・ セキュリティグループで SSH ポートの開放が不要
・ プライベートサブネットでも踏み台なしでアクセス可能
・ IAM によるアクセス制御が可能
・ ログインのログ、イベントが取得可能（S3、Cloud Watch 等との連携）

EC2 インスタンスのセッティング

セッションマネージャを使うために、EC2 インスタンスの設定でいくつか注意しなければいけない点があります。

IAM ロール

セッションマネージャからインスタンスへの接続を許可するために、`AmazonSSMManagedInstanceCore` という IAM ポリシーを EC2 インスタンスの IAM インスタンスプロファイル (IAM ロール) にアタッチする必要があります。

サブネット

セッションマネージャはパブリックサブネットとプライベートサブネットの両方で利用することができます。
ただし注意が必要なのが、AWS の EC2 や SSM への API アクセスを行うためのアウトバウンド通信が必要という点です。
すなわち、プライベートサブネットの場合は NAT ゲートウェイを用意するか、VPC エンドポイントを利用する必要があります。

この点に関してはクラスメソッドさんの記事で分かりやすく整理されているので参考にしてみてください。
セッションマネージャーのハマりどころをパターンごとに整理してみる

SSM エージェントのインストール

インスタンスに SSM エージェントをインストールする必要があります。
Amazon Linux 系の OS であればデフォルトでインストールされています。

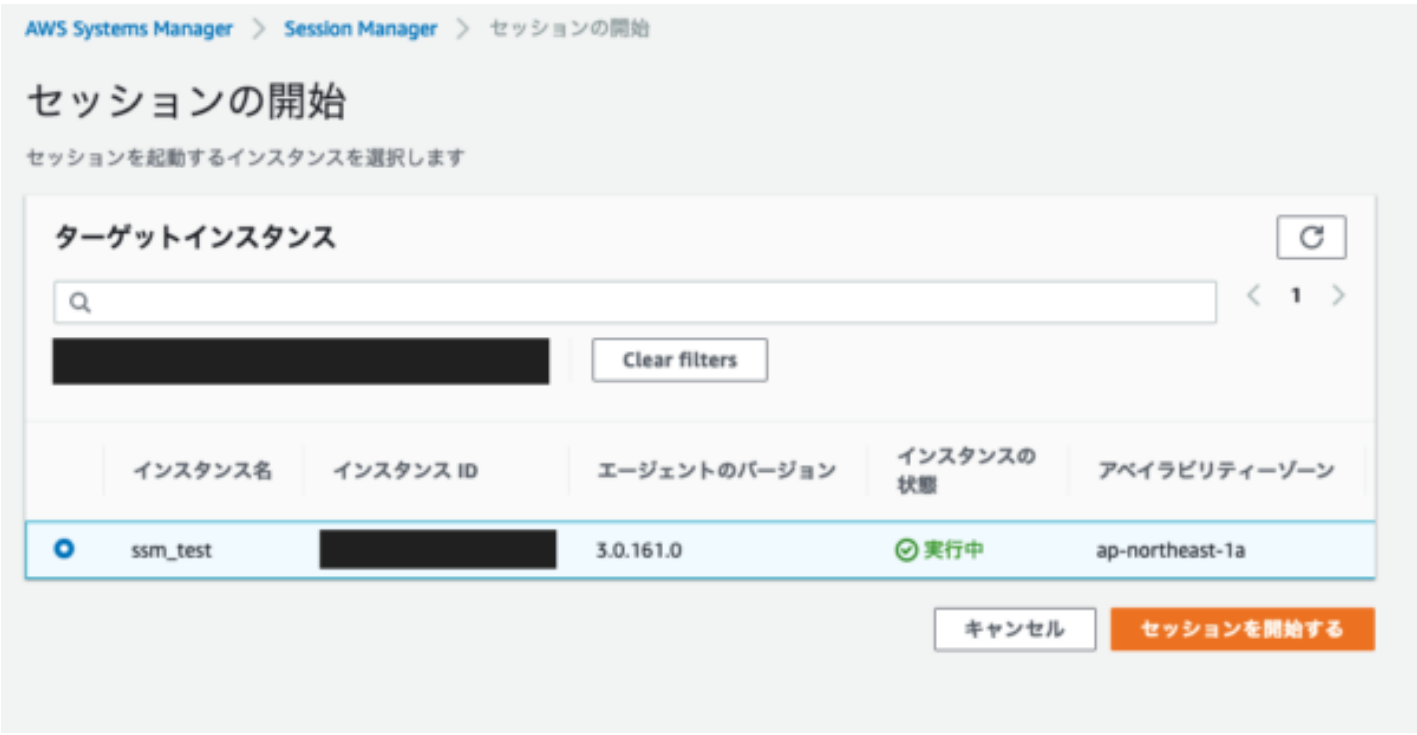
その他 OS でのインストール方法に関しては公式ドキュメントを参照してください。
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/ssm-agent.html

利用方法

AWS コンソールから利用する場合

> **方法 その1**

AWS コンソールにログイン後、「AWS Systems Manager」→「Session Manager」→「セッションの開始」と遷移して、アクセスしたいインスタンスを選択します。



「セッションを開始する」をクリックすると、ブラウザでコンソール画面が表示されます。

方法 その2

実は EC2 のコンソール画面からも接続することができます。
アクセスしたいインスタンスを選択し「接続」をクリックします。

「セッションマネージャ」のタブに移動して「接続」をクリックするとセッションマネージャによる接続が開始されます。

SSH を用いる場合

コンソールからのアクセスの場合、SCP や ポートフォワーディングなどは利用できません。
それらが必要な場合はこちらのSSHを用いる方法が利用できます。

注意点として EC2 インスタンス のキーペアが必要になります。

従来の SSH の場合とは異なり、セキュリティグループで SSH のポートを開放する必要はありません。

準備

（awscli のセットアップは済んでいる前提です）

Session Manager plugin のインストール

awscli からセッションマネージャを利用するために、Session Manager plugin をインストールする必要があります。

mac の場合のインストール手順は下記の通りです。

```
$ curl "https://s3.amazonaws.com/session-manager-downloads/plugin/latest/mac/sessionmanager-bundle.zip" -o "sessionmanager-bundle.zip"
$ unzip sessionmanager-bundle.zip
$ sudo ./sessionmanager-bundle/install -i /usr/local/sessionmanagerplugin -b /usr/local/bin/session-manager-plugin
```

その他の環境におけるインストール手順は公式ドキュメントを参照してください。
https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/session-manager-working-with-install-plugin.html

ssh config の設定

下記設定を ssh config (~/.ssh/config) に追加します。

```
host i-*
  User ec2-user  # amazon linux 系 OS の場合
  ProxyCommand sh -c "aws ssm start-session --target %h --document-name AWS-StartSSHSession --parameters 'portNumber=%p'"
```

参考: https://docs.aws.amazon.com/ja_jp/systems-manager/latest/userguide/session-manager-getting-started-enable-ssh-connections.html

> **接続手順**

接続したい EC2 インスタンスのインスタンスIDを確認します。
下記は awscli を使う場合のコマンド例です。

```
$ aws ec2 describe-instances --region ap-northeast-1 --output=table --filters Name=instance-state-name,Values=running --query 'Reservations[].Instances[]
```

インスタンスID と SSH 鍵を指定して SSH コマンドで接続できます。

```
$ ssh -i <ssh keyのパス> <インスタンスID>
```

まとめ

セッションマネージャによって、セキュリティグループの設定や SSH 鍵の運用などが不要になり、運用管理のコスト削減やセキュリティ向上が期待できます。
是非、試してみてください！