課題演習 No.1
(IAM + EC2 + VPC)

課題演習1（IAM + EC2 + VPC）

目的：

ある会社が社内システムをオンプレミス環境からAWS環境への移行を
計画している。
機密データが格納されている社内システムなのでインターネットからの直接アクセスはできないようにしたい。
その中で社内システムのメンテナンスも実施したいが、VPNやDirectConnectは準備やコストで負担が大きいため、コストを掛けずにセキュアな方法で社内システムへのアクセスを実現したい。

1：要件

■以下の要件でインフラを構築してください。

1. コストを最小限に抑えるために、冗長構成は不要である。
2. 社内システム用のEC2はインターネットからのアクセスをできないようにしたい。EC2からのインターネットへのアクセスはOSパッチ適用のため、許可したい。
3. 2.のEC2にセキュアにアクセスできるサーバーを作成したい。またこの3.で作成されるサーバーは外部からSSH接続できるようにし、サーバーのIPアドレスは固定にしたい。(3.のアドレスのみ2.のサーバーへアクセス可能にする)
4. 社内システム用のEC2もSSH接続を可能にしたい。セキュリティ強化として、社内システムへのSSH接続時はポート番号を別のものにしたい。
(ポート番号は**10022**に指定)
5. 運用者用アカウントを作成し、そのIAMユーザーにはEC2の削除(終了)をさせないように権限設定したい。今後もアカウントは増える予定で、追加時の権限設定の手間を軽減させたい。

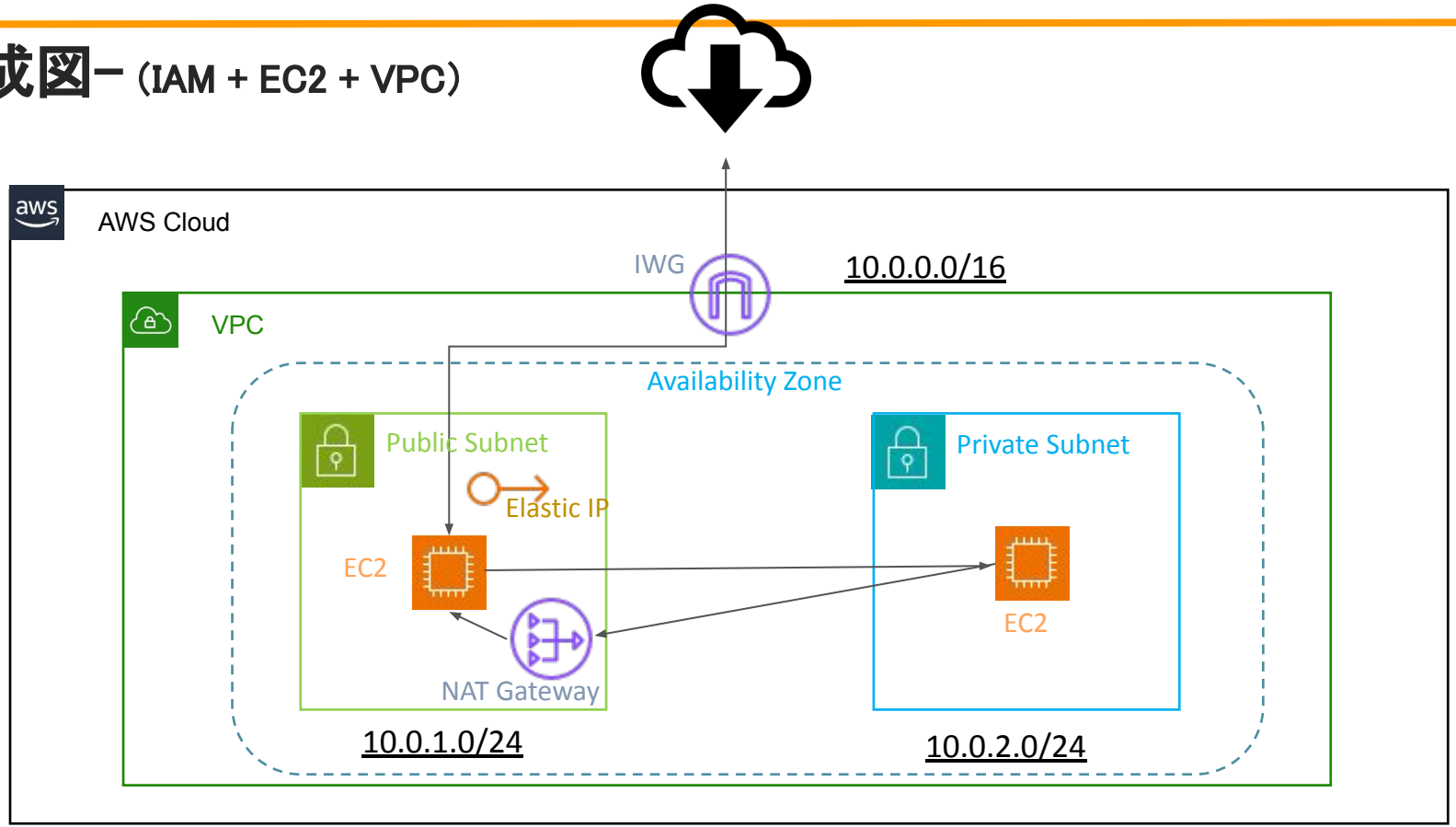
2：設計

■要件に対しての仕様(解決策)

No	要件	仕様(解決策)
1	コストを最小限に抑えるために、冗長構成も不要である。	シングル構成でコスト最小限に抑える。
2	社内システム用のEC2はインターネットからのアクセスをできないようにしたい。 ソフトのアップデートはできるように設定したい。	プライベートサブネット内にEC2を設定してインターネットからのアクセスをできないようにする。 パブリックサブネット内にNATGatewayを設定し社内システムへのインバウンドを制限。 社内システムから踏み台サーバーを経由してインターネットへSSH接続、ソフトのアップデートは可能。
3	踏み台サーバーへのアクセス時のIPアドレスを固定にしたい。また社内システム用EC2へのSSH接続を可能にする。	踏み台サーバーへElasticIPでIPアドレスを固定。 セキュリティグループの設定をしSSH接続可能。
4	セキュリティ強化の為、社内システムへのSSH接続時はポート番号を別のものにしたい。 (ポート番号は10022に指定)	踏み台サーバーから社内システムへのSSH接続のポート番号は10022に設定。
5	運用者用アカウントを作成し、そのIAMユーザーにはEC2の削除(終了)をさせないように権限設定したい。 今後もアカウントは増える予定で、追加時の権限設定の手間を軽減させたい。	IAMグループを作成してEC2を削除をさせないポリシーをアタッチ、新規ユーザーを作成してIAMグループ内に追加制御する。

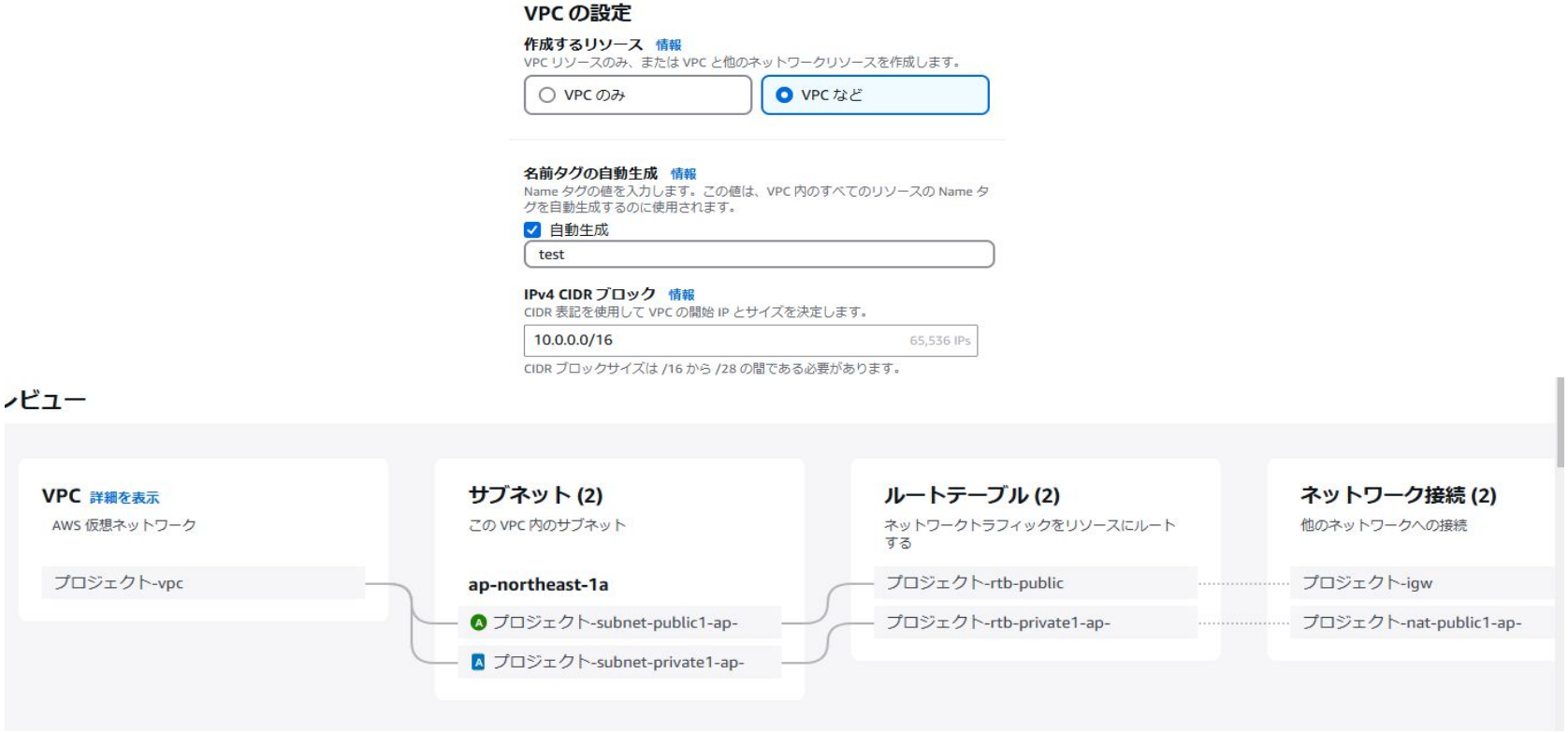
2：設計

−構成図− (IAM + EC2 + VPC)



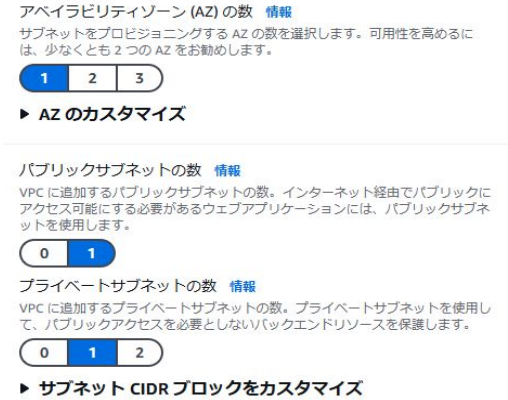
3：構築（実装）

① シングルインスタンスでコスト最小化



3：構築（実装）

② 社内システム用のEC2はインターネットからのアクセスをできないようにプライベートサブネット内に社内システムを構築。
※VPC作成時にVPCなどを選択時に同時に構築

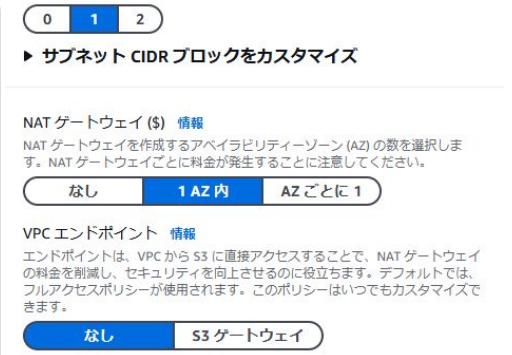


3：構築（実装）

② パブリックインスタンス起動時にキーペアを作成
プライベートインスタンス起動時にも同様のキーペアを選択
キーペアをダウンロードしてローカルPCからインスタンスへログイン
する際に使用

3：構築（実装）

② 社内システムへのインバウンドのトラフィック制御の為に
NATGatewayをバブリックサブネットへ構築
※VPC作成時にVPCなどを選択時に同時に構築

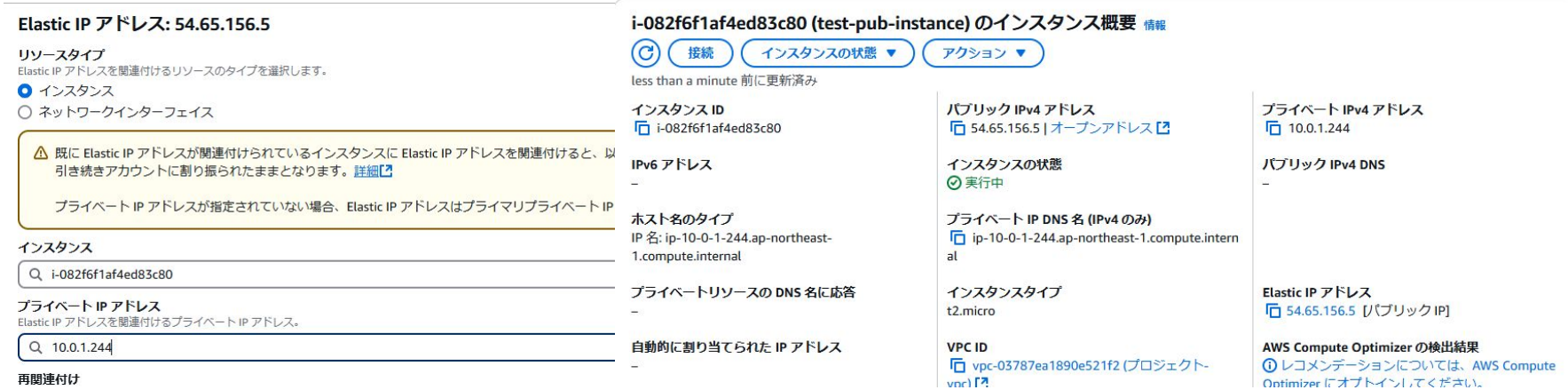


3：構築（実装）

② ソフトウェアのアップデートができるようにIGWをVPCにアタッチ
※VPC作成時にVPCなどを選択時にIGWを同時に構築

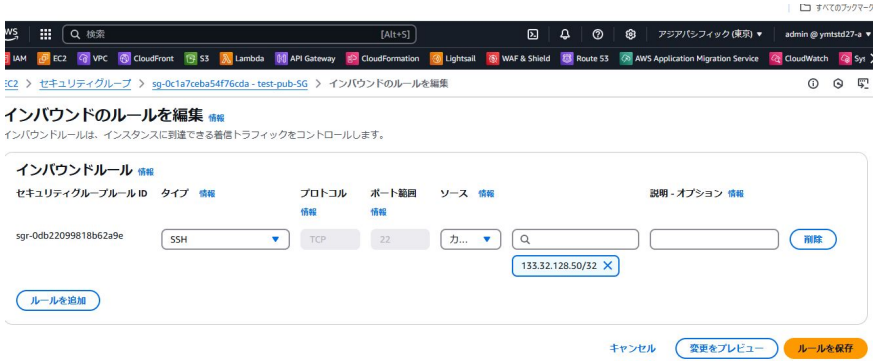
3：構築（実装）

③　踏み台サーバーへElasticIPでIPアドレスを固定。
※VPC作成時にVPCなどを選択時に同時に構築、アタッチ



3：構築（実装）

③　セキュリティグループを設定をしSSH接続可能。
④　踏み台サーバーから社内システムへのSSH接続のポート番号は10022に設定。
パブリックインスタンス用のセキュリティーグループ

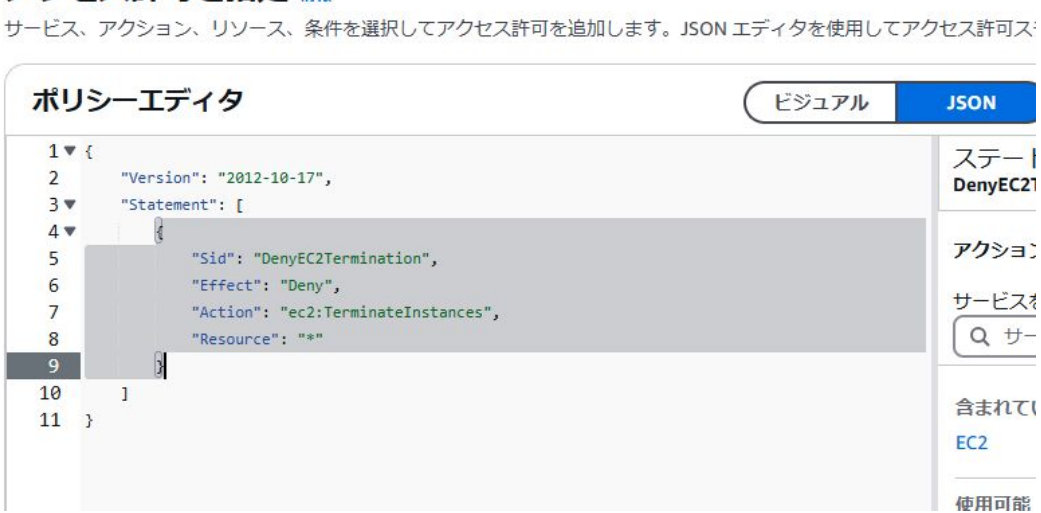


3：構築（実装）

③　セキュリティグループを設定をしSSH接続可能。
④　踏み台サーバーから社内システムへのSSH接続のポート番号は10022に設定。
プライベートインスタンス用のセキュリティーグループ

3：構築（実装）

⑤ IAMグループを作成して運用者アカウントにはEC2を
削除をさせないポリシーをアタッチして、制御する。
アカウントの増加を考慮して、追加時の権限設定の手間を軽減させる。

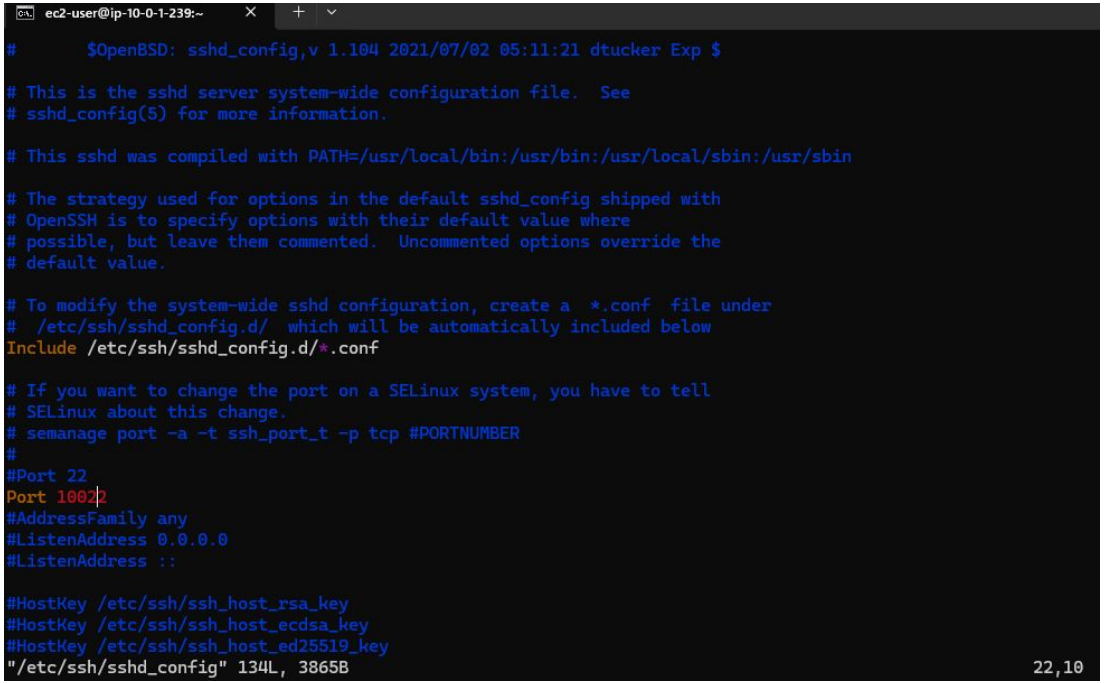


4：テスト結果（検証）

① ローカルPCにダウンロードしたキーペアをscpコマンドで
インスタンスへ転送し、sshコマンドでパブリックインスタンスへの
ログインを確認

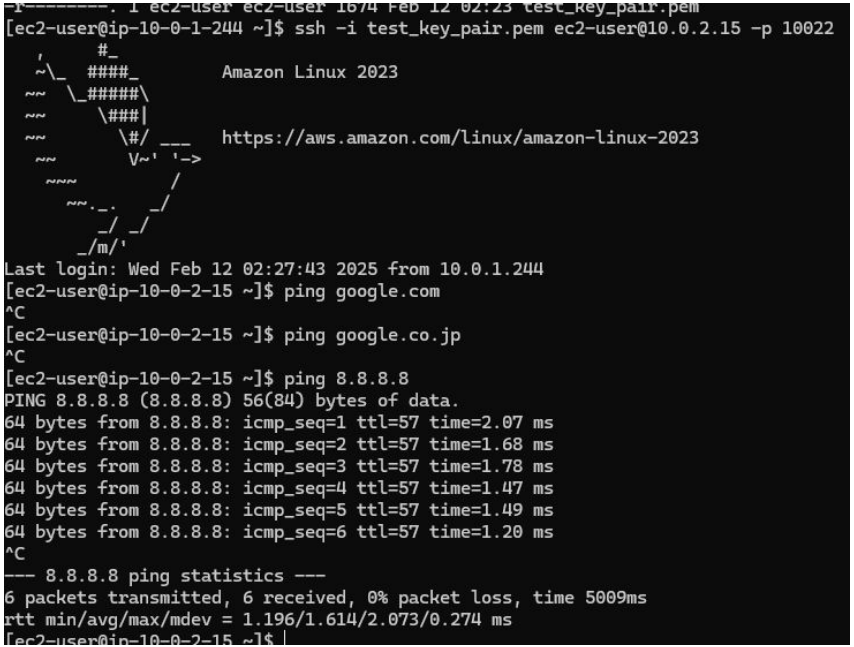
4：テスト結果（検証）

② 社内システムのセキュリティグループのインバウンドルールを
カスタムTCP、ポート番号10022に設定。



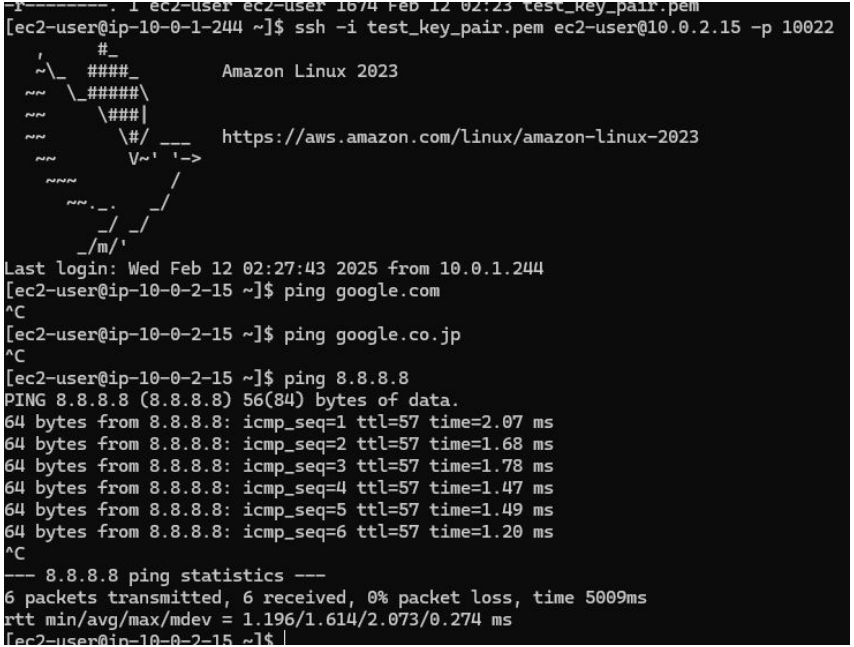
4：テスト結果（検証）

③ プライベートインスタンスのインバウンドのポート番号を10022へ
変更後、パブリックインスタンスから社内システムへログインを確認



4：テスト結果（検証）

④　踏み台サーバーから社内システムへ、社内システムからインターネットへの通信可能を確認。



4：テスト結果（検証）

⑤　運用者アカウントをユーザーグループへ追加をしEC2の削除を実行不可の応答を確認。