

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。

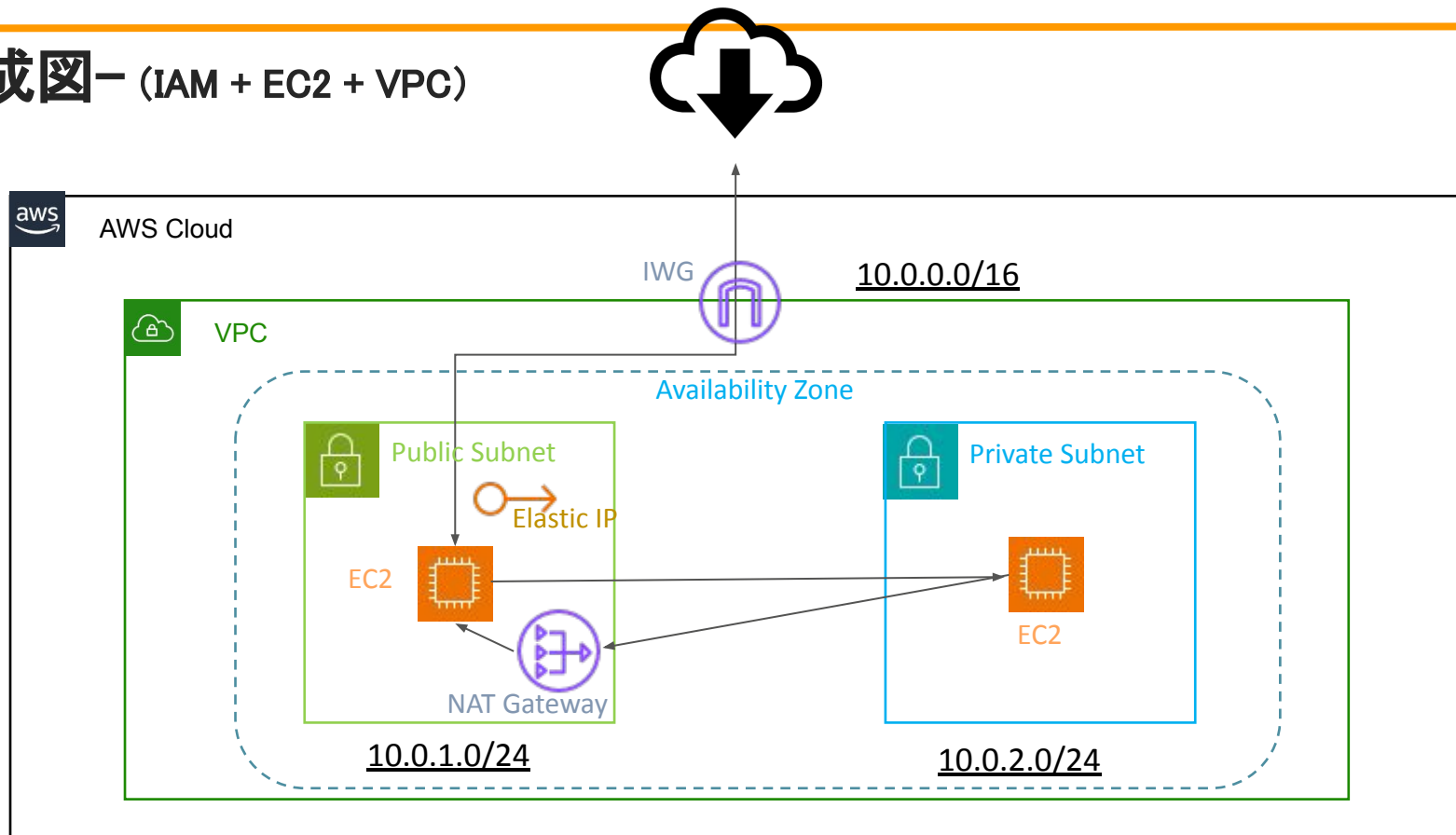
## 2: 設計

### ■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

### VPC の設定

#### 作成するリソース 情報

VPC リソースのみ、または VPC と他のネットワークリソースを作成します。

☐ VPC のみ

☒ VPC など

#### 名前タグの自動生成 情報

Name タグの値を入力します。この値は、VPC 内のすべてのリソースの Name タグを自動生成するのに使用されます。

☒ 自動生成

test

#### IPv4 CIDR ブロック 情報

CIDR 表記を使用して VPC の開始 IP とサイズを決定します。

10.0.0.0/16

65,536 IPs

CIDR ブロックサイズは /16 から /28 の間である必要があります。

## レビュー

### VPC 詳細を表示


AWS 仮想ネットワーク


プロジェクト-vpc

### サブネット (2)

この VPC 内のサブネット

ap-northeast-1a

 プロジェクト-subnet-public1-ap-

 プロジェクト-subnet-private1-ap-

### ルートテーブル (2)

ネットワークトラフィックをリソースにルートする

プロジェクト-rtb-public

プロジェクト-rtb-private1-ap-

### ネットワーク接続 (2)

他のネットワークへの接続

プロジェクト-igw

プロジェクト-nat-public1-ap-

# 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

## i-0a448b534089a3034 (pri\_instace) のインスタンス概要 情報

less than a minute 前に更新済み

### インスタンス ID

i-0a448b534089a3034

### IPv6 アドレス

-

### ホスト名のタイプ

IP 名: ip-10-0-1-239.ap-northeast-1.compute.internal

### プライベートリソースの DNS 名に応答

-

### 自動的に割り当てられた IP アドレス

-

### パブリック IPv4 アドレス

-

### インスタンスの状態

実行中

### プライベート IP DNS 名 (IPv4 のみ)

ip-10-0-1-239.ap-northeast-1.compute.internal

### インスタンスタイプ

t2.micro

### VPC ID

vpc-00d08b2e6b14fb682 (test\_VPC)

接続

インスタンスの状態 ▼

アクション ▼

### プライベート IPv4 アドレス

10.0.1.239

### パブリック IPv4 DNS

-

### Elastic IP アドレス

-

### AWS Compute Optimizer の検出結果

① レコメンデーションについては、AWS Compute Optimizer にオプトインしてください。

### アベイラビリティゾーン (AZ) の数 情報

サブネットをプロビジョニングする AZ の数を選択します。可用性を高めるには、少なくとも 2 つの AZ をお勧めします。

1 2 3

### ▶ AZ のカスタマイズ

### パブリックサブネットの数 情報

VPC に追加するパブリックサブネットの数。インターネット経由でパブリックにアクセス可能にする必要があるウェブアプリケーションには、パブリックサブネットを使用します。

0 1

### プライベートサブネットの数 情報

VPC に追加するプライベートサブネットの数。プライベートサブネットを使用して、パブリックアクセスを必要としないバックエンドリソースを保護します。

0 1 2

### ▶ サブネット CIDR ブロックをカスタマイズ

### 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

ソフトウェアがオンラインインストールされた

#### ▼ キーペア (ログイン) 情報

キーペアを使用してインスタンスに安全を確認してください。

キーペア名 - 必須

test\_key\_pair




# 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をパ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


## 概要

割り振られた IPv4 アドレス  
 54.65.201.14

関連付け ID  
 eipassoc-  
04bba37291d0e56d9


ネットワークインターフェース ID  
[eni-00c0ad394e16d501f](#) 

アドレスプール  
 Amazon

タイプ  
 パブリック IP

範囲  
 VPC

ネットワークインターフェースの所  
有者アカウント ID  
 584791980123


ネットワークボーダーグループ  
 ap-northeast-1

割り当て ID  
 eipalloc-0b8f8c283379251be

関連付けられたインスタンス ID  
-

パブリック DNS  
-

逆引き DNS レコード  
-

プライベート IP アドレス  
 10.0.1.125

NAT ゲートウェイ ID  
[nat-05721469a3767a104](#) (プロジェクト-nat-public1-ap-northeast-1a)

0 1 2

▶ サブネット CIDR ブロックをカスタマイズ

NAT ゲートウェイ (\$) 情報

NAT ゲートウェイを作成するアベイラビリティゾーン (AZ) の数を選択します。NAT ゲートウェイごとに料金が発生することに注意してください。

なし 1 AZ 内 AZ ごとに 1

VPC エンドポイント 情報

エンドポイントは、VPC から S3 に直接アクセスすることで、NAT ゲートウェイの料金を削減し、セキュリティを向上させるのに役立ちます。デフォルトでは、フルアクセスポリシーが使用されます。このポリシーはいつでもカスタマイズできます。

なし S3 ゲートウェイ


### 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

igw-04e77e9dc096fde87 / プロジェクト-igw

#### 詳細 情報

インターネットゲートウェイ ID

 igw-04e77e9dc096fde87

状態

 Attached

VPC ID

[vpc-03787ea1890e521f2](#) | [プロジェクト-vpc](#)

# 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

Elastic IP アドレス: 54.65.156.5

## リソースタイプ

Elastic IP アドレスを関連付けるリソースのタイプを選択します。

- ☒ インスタンス  
☐ ネットワークインターフェイス

⚠ 既に Elastic IP アドレスが関連付けられているインスタンスに Elastic IP アドレスを関連付けると、引き続きアカウントに割り振られたままとなります。[詳細](#)

プライベート IP アドレスが指定されていない場合、Elastic IP アドレスはプライマリプライベート IP

## インスタンス

Q i-082f6f1af4ed83c80

## プライベート IP アドレス

Elastic IP アドレスを関連付けるプライベート IP アドレス。

Q 10.0.1.244

再関連付け

i-082f6f1af4ed83c80 (test-pub-instance) のインスタンス概要 [情報](#)



接続

インスタンスの状態 ▼

アクション ▼

less than a minute 前に更新済み

インスタンス ID

i-082f6f1af4ed83c80

IPv6 アドレス

-

ホスト名のタイプ

IP 名: ip-10-0-1-244.ap-northeast-1.compute.internal

プライベートリソースの DNS 名に応答

-

自動的に割り当てられた IP アドレス

-

パブリック IPv4 アドレス

54.65.156.5 | [オープンアドレス](#)

インスタンスの状態

🟢 実行中

プライベート IP DNS 名 (IPv4 のみ)

ip-10-0-1-244.ap-northeast-1.compute.internal

インスタンスタイプ

t2.micro

VPC ID

vpc-03787ea1890e521f2 (プロジェクト-vnr) [?](#)

プライベート IPv4 アドレス

10.0.1.244

パブリック IPv4 DNS

-

Elastic IP アドレス

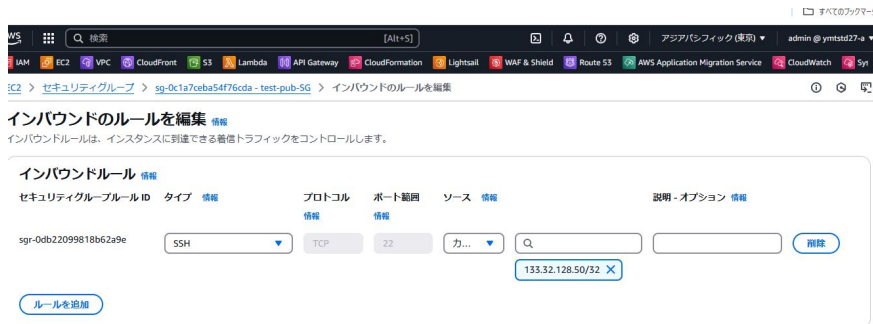
54.65.156.5 [パブリック IP]

AWS Compute Optimizer の検出結果

① レコメンデーションについては、AWS Compute Optimizer に「オプトイン」してください。

# 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

インバウンドのルールを編集

インバウンドルールは、インスタンスに到達できる着信トラフィックをコントロールします。

セキュリティグループルール ID	タイプ	プロトコル	ポート範囲	ソース	説明 - オプション
sg-0f690567a62c8f7e9	カスタム TCP	TCP	10022	カ...	

ルールを追加

キャンセル 変更をプレビュー ルールを保存

アウトバウンドルール

セキュリティグループルール ID	タイプ	プロトコル	ポート範囲	送信先	説明 - オプション
sg-0f4195208e17bffa	すべてのトラフィック	すべて	すべて	カ...	

ルールを追加

宛先が 0.0.0.0/0 または ::0/0 のルールでは、インスタンスは任意の IP v4 または IP v6 アドレスにトラフィックを送信できます。セキュリティグループのルールは制限を厳しくし、特定の宛先の IP アドレスへのトラフィックのみを許可するように設定することをお勧めします。

キャンセル 変更をプレビュー ルールを保存

# 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。

グループに名前を付ける

ユーザーグループ名  
このグループを識別するためのわかりやすい名前?

Operators

最大 128 文字です。英数字と「+','=','\_」文字を

ユーザーをグループに追加 - オ

IAM ユーザーは AWS で作成するエンティティ

検索

ユーザー名

☐ admin

☒ samurai

## アクセス許可を指定 情報

サービス、アクション、リソース、条件を選択してアクセス許可を追加します。JSON エディタを使用してアクセス許可ス

ポリシーエディタ

ビジュアル JSON

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "DenyEC2Termination",  
6       "Effect": "Deny",  
7       "Action": "ec2:TerminateInstances",  
8       "Resource": "*" }  
9   ]  
10 }  
11 }
```

ステータス  
DenyEC2T

アクション  
サービス  
検索

含まれて  
EC2

使用可能

## 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

[illegible]

## 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。

```
ec2-user@ip-10-0-1-239:~  
# $OpenBSD: sshd_config,v 1.104 2021/07/02 05:11:21 dtucker Exp $  
  
# This is the sshd server system-wide configuration file. See  
# sshd_config(5) for more information.  
  
# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin  
  
# The strategy used for options in the default sshd_config shipped with  
# OpenSSH is to specify options with their default value where  
# possible, but leave them commented. Uncommented options override the  
# default value.  
  
# To modify the system-wide sshd configuration, create a *.conf file under  
# /etc/ssh/sshd_config.d/ which will be automatically included below  
Include /etc/ssh/sshd_config.d/*.conf  
  
# If you want to change the port on a SELinux system, you have to tell  
# SELinux about this change.  
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER  
#  
#Port 22  
Port 10022  
#AddressFamily any  
#ListenAddress 0.0.0.0  
#ListenAddress ::  
  
#HostKey /etc/ssh/ssh_host_rsa_key  
#HostKey /etc/ssh/ssh_host_ecdsa_key  
#HostKey /etc/ssh/ssh_host_ed25519_key  
"/etc/ssh/sshd_config" 134L, 3865B
```



## 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

[illegible]

## 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。

```
[ec2-user@ip-10-0-1-244 ~]$ ssh -i test_key_pair.pem ec2-user@10.0.2.15 -p 10022
#
##### Amazon Linux 2023
#####|
###|
###\##/
#####V~!> https://aws.amazon.com/linux/amazon-linux-2023
#####
#####
#####_/_/_/
#####_/_/_/
#####_/_/_/

Last login: Wed Feb 12 02:27:43 2025 from 10.0.1.244
[ec2-user@ip-10-0-2-15 ~]$ ping google.com
^C
[ec2-user@ip-10-0-2-15 ~]$ ping google.co.jp
^C
[ec2-user@ip-10-0-2-15 ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=57 time=2.07 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=57 time=1.68 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=57 time=1.78 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=57 time=1.47 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=57 time=1.49 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=57 time=1.20 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 1.196/1.614/2.073/0.274 ms
[ec2-user@ip-10-0-2-15 ~]$
```

## 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。

