

JAWS DAYS 2021

セキュリティグループって何？

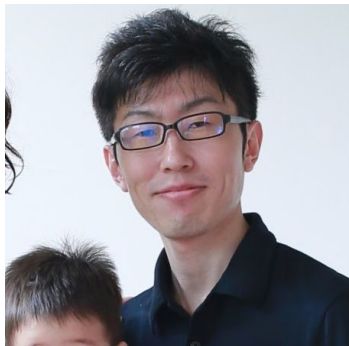
使い方を基礎から学ぼう！

---

JAWS-UG 初心者支部

# 自己紹介

---



- 山原 崇史
- JAWS-UG初心者支部 運営メンバー
- 某Web系企業のSRE
- Twitter : @shonansurvivors



# 本日のゴール

---

- AWSの仮想ファイアウォールであるセキュリティグループを使って、任意の通信を許可/拒否できるようになる

# ハンズオン全体の流れ

---

1. ハンズオン用の環境を構築する
2. ハンズオン用環境の構成図の解説
3. 各ケースに沿ったセキュリティグループを作成、使用してみる
  - a. IPアドレスを限定せず、Webサービスを利用させるケース
  - b. 特定のIPアドレスに対してのみ、Webサービスを利用させるケース
  - c. 特定のリソース同士を相互に通信可能とさせるケース
4. ハンズオン用環境を削除する

ハンズオン用の環境を構築する

# ハンズオン用環境構築の流れ

---

1. CloudShellの起動
2. CloudFormation用ファイルのダウンロード
3. CloudFormationの実行

# CloudShellの起動 - 目的 -

---

本ハンズオン用の環境構築では、GitやAWS CLIというものを使用します。

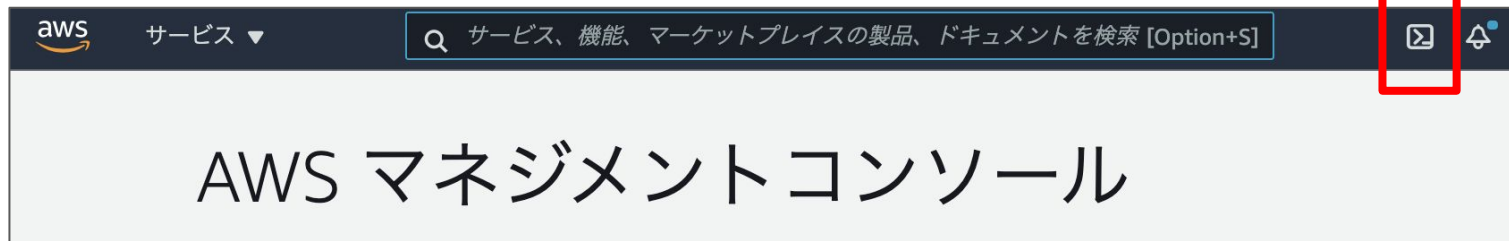
GitやAWS CLIは、準備をすればお手元のPC(WindowsやMac)でも使用することはできます。

しかし、本ハンズオンでは、受講者のみなさんがPC環境の差異を理由につまずくことの無いよう、AWSのCloudShellを利用することにします。

CloudShellはブラウザから利用可能で、GitやAWS CLIがインストール済みとなっています。

# [作業]CloudShellの起動

- マネジメントコンソール(以下、マネコン)へのログイン
  - 以下のURLから、ご自身のAWSアカウントにログインしてください
    - <https://xxxxxxxxxxxxx.signin.aws.amazon.com/console>
    - xxxxxxxxxxxxxxxxの部分は、ご自身のアカウントID (12桁) またはアカウントエイリアスとなります。
- CloudShellの起動
  - 画面右上に表示されている、以下のマークをクリックし、CloudShellを起動してください





# CloudFormationの実行 – 目的 –

---

CloudFormationは、所定の形式のファイルを読み込み、その内容に従ってAWSの各種リソースを自動で作成してくれる、AWSのサービスです。

本ハンズオンではCloudFormation用のファイルを別途用意してありますので、これを使ってAWS上に環境を構築します。

# [作業]CloudFormationの実行 1/2

---

- CloudFormation用ファイルのダウンロード
  - ここでは、GitHub上に存在する本ハンズオン用のCloudFormation用ファイルをダウンロードします。
  - CloudShellの画面に、以下コマンドを貼り付けてエンターキーを押してください。

```
git clone https://github.com/shonansurvivors/security-group-hands-on.git
```

# [作業]CloudFormationの実行 2/2

---

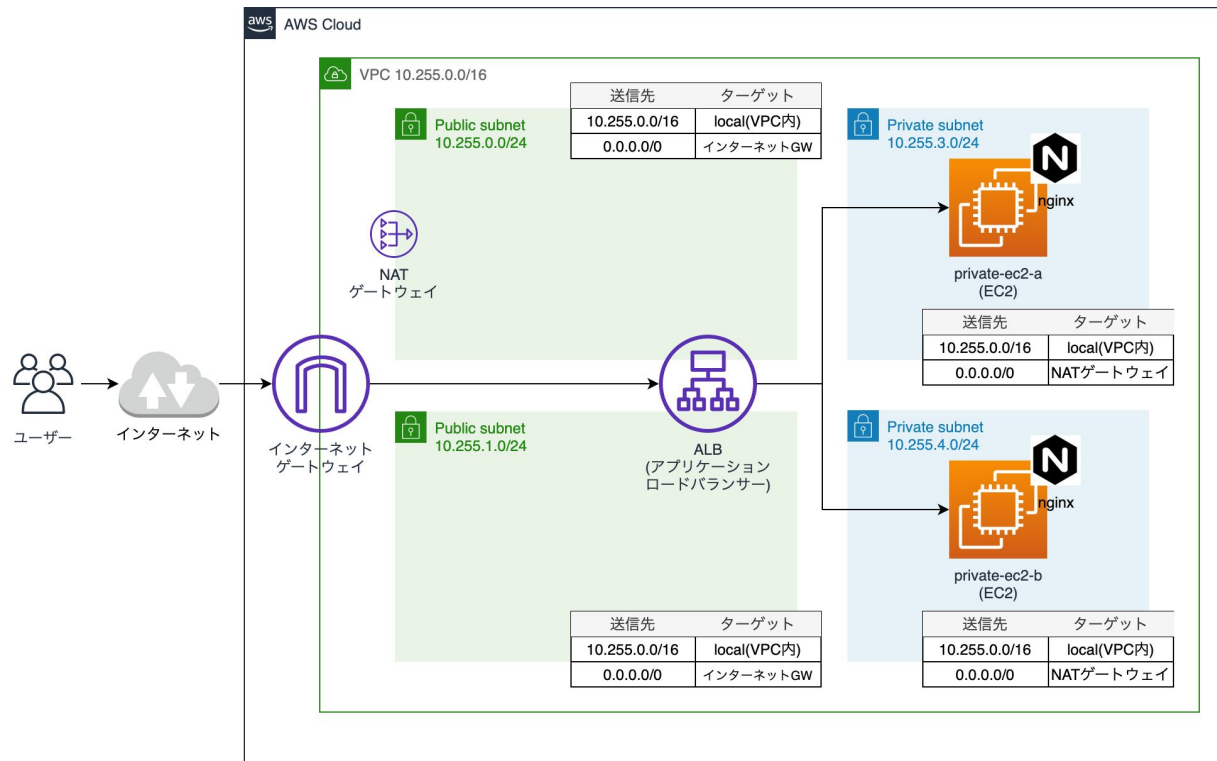
- CloudFormationの実行
  - ここでは、先ほどダウンロードしたファイルを使って、ハンズオン用の環境を構築します。
  - CloudShellの画面に、以下コマンドを貼り付けてエンターキーを押してください。

```
aws cloudformation create-stack --stack-name jaws-sg --template-body file://security-group-hands-on/cloudformation.yml
```

- 環境構築が完了するまで4～5分程度かかるので、その間に解説を先に進めます。

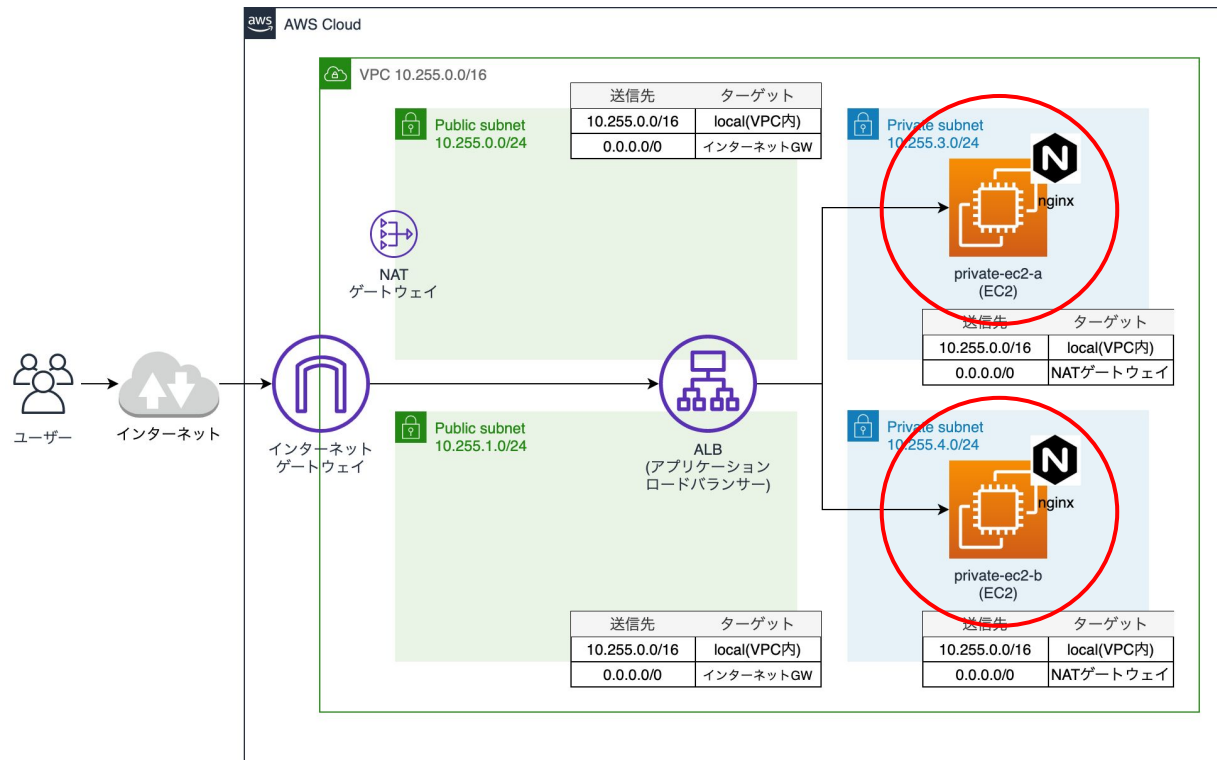
# ハンズオン用環境の構成図の解説

# 構成図解説 1/5



こちらが、今回のハンズオンで使用する環境の構成図です。

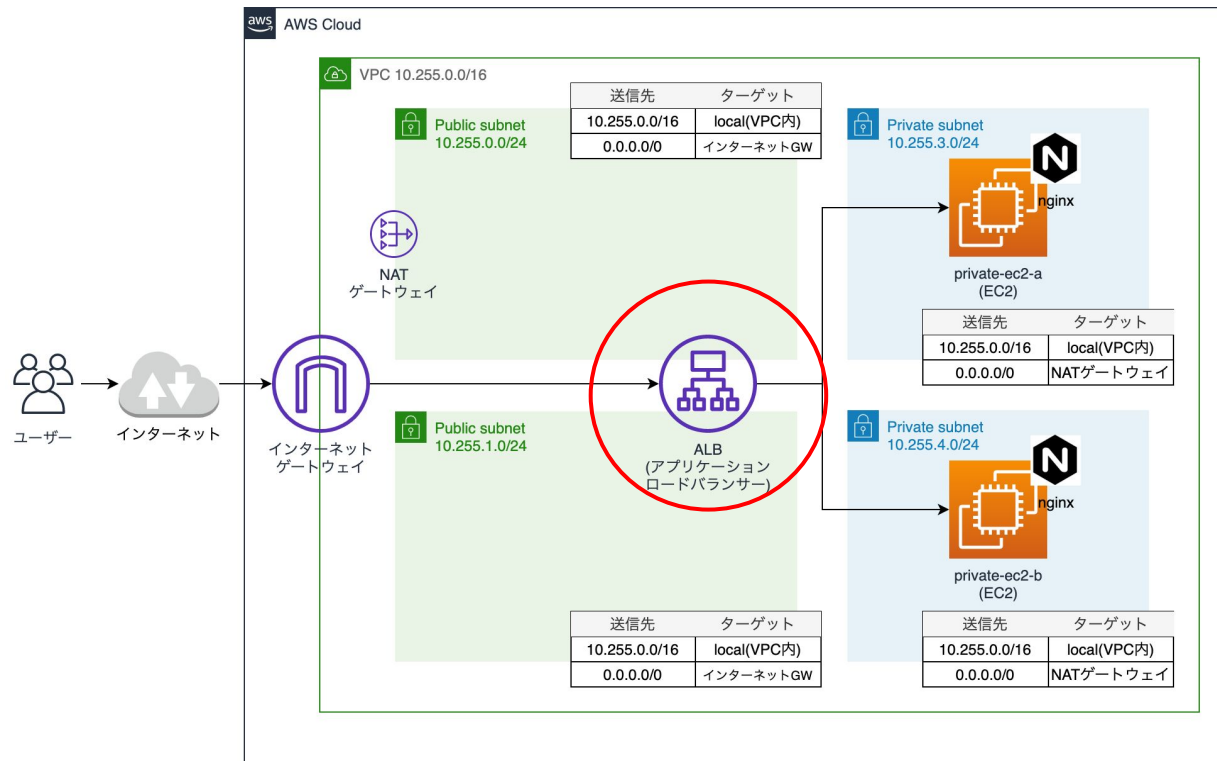
# 構成図解説 2/5



この2台のEC2はWebサーバーの役割を持ちます。

「Hello JAWS!」という内容の画面を表示するように設定済みです。

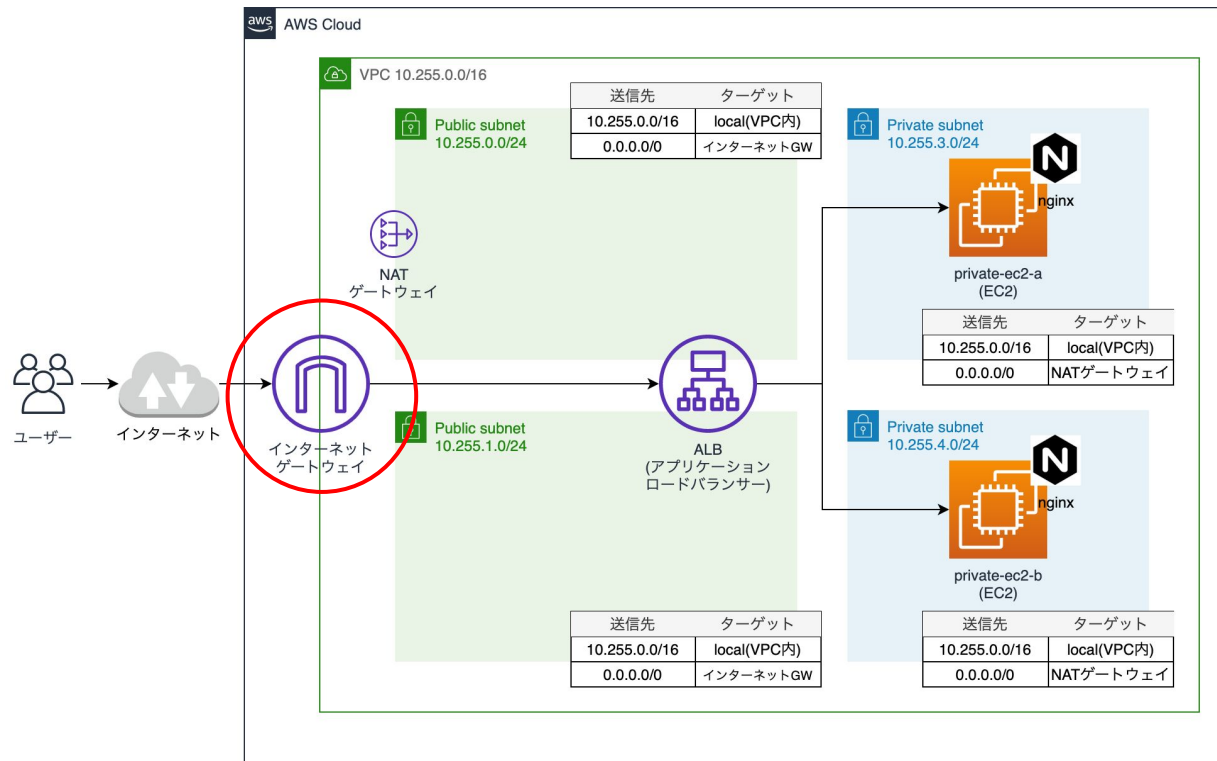
# 構成図解説 3/5



2台のEC2の手前にあるのはALB(アプリケーションロードバランサー)です。

ユーザーからのアクセスを2台のEC2に振り分け(負荷分散)します。

# 構成図解説 4/5

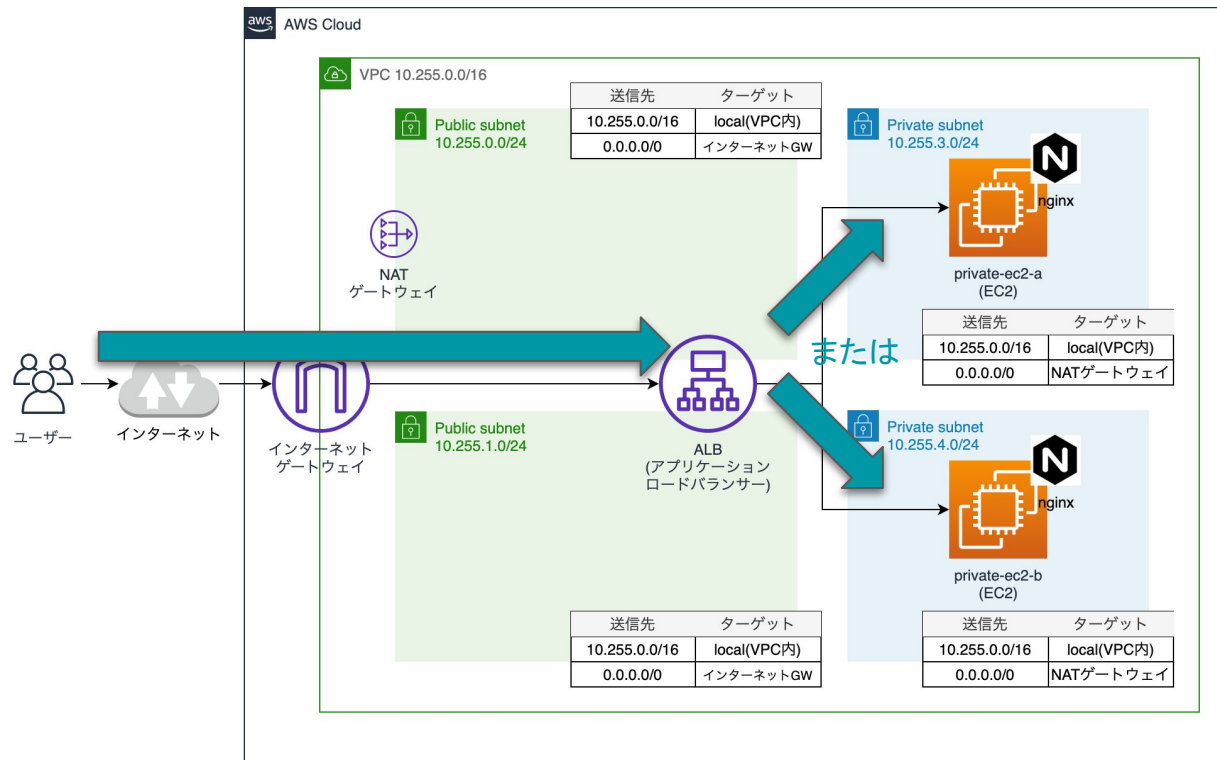


ALBの手前にあるのはインターネットゲートウェイです。

インターネットとの通信の出入り口となります。



# 構成図解説 5/5



つまり、ユーザーのブラウザからALBにアクセスすると、どちらかのEC2が返却する「Hello JAWS!」が表示されることになります。

各ケースに沿った  
セキュリティグループを作成、  
使用してみる

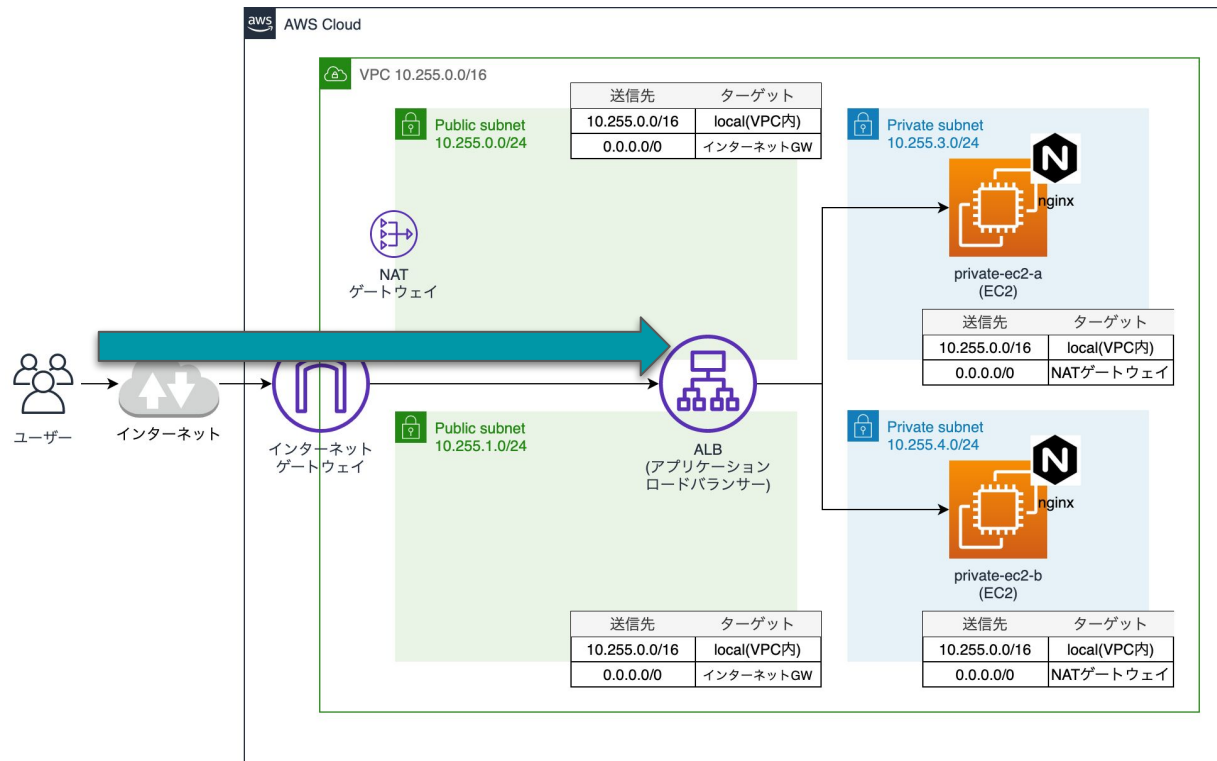
# ケース1

---

IPアドレスを限定せず、誰でもWebサービスにアクセス(HTTP通信)できる



# 構成図によるケース1の解説

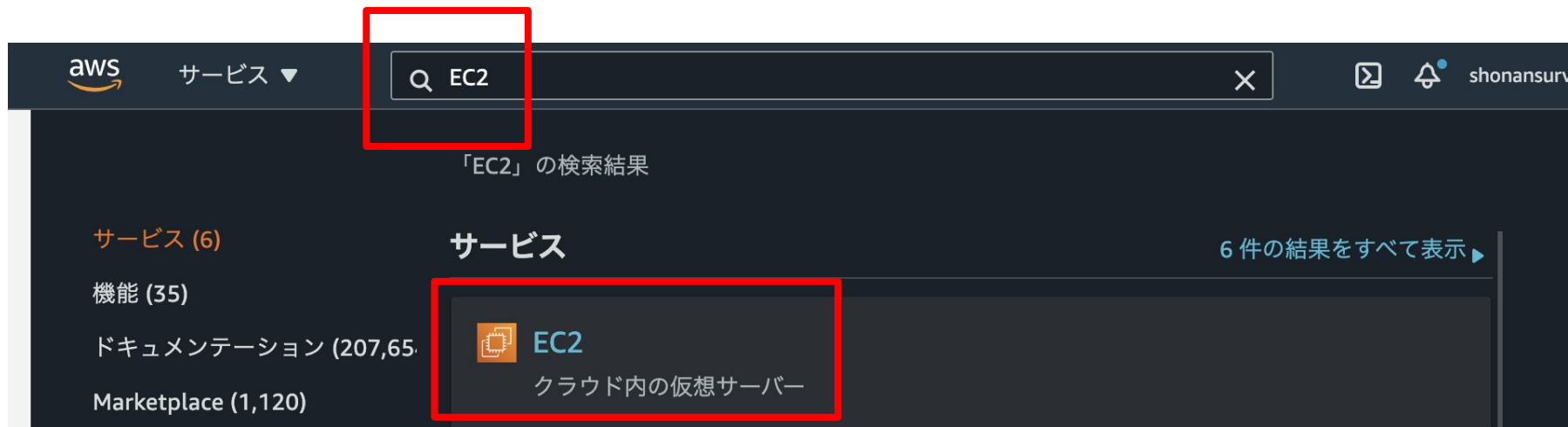


「Hello JAWS!」を表示するためにブラウザでALBにアクセスします。

ALBにアクセスするには、ALBのDNS名をブラウザのアドレスバーに入力します。

# [作業]ALBのDNS名を調べる 1/3

- マネコンの検索欄にEC2と入力し、EC2を選んでください  
(ALBはEC2の画面に存在します)。



# [作業]ALBのDNS名を調べる 2/3

- EC2ダッシュボード画面から、ロードバランサーを選択してください。



The screenshot displays the AWS Management Console's EC2 Resources page. On the left, a navigation sidebar lists various EC2-related features, with 'インスタンス' (Instances) expanded. The main content area, titled 'リソース' (Resources), shows a summary of resources in the 'アジアパシフィック (東京)' (Asia Pacific (Tokyo)) region. A table lists the following resources:

Resource Type	Count
実行中のインスタンス (Running Instances)	3
インスタンス (すべての状態) (Instances (all states))	3
スナップショット (Snapshots)	0
プレースメントグループ (Placement Groups)	0
ロードバランサー (Load Balancers)	1
Elastic IP	1
キーペア (Key Pairs)	4
セキュリティグループ (Security Groups)	5
ボリューム (Volumes)	3
専有ホスト (Dedicated Hosts)	0

The 'ロードバランサー' (Load Balancers) row is highlighted with a red rectangular box. Below the table, a blue information banner states: 'AWS Launch Wizard for SQL Server を使用すると、Microsoft SQL Server Always On 可用性グループのサイズ調整、設定、デプロイを簡単に行うことができます。詳細はこちら' (Using AWS Launch Wizard for SQL Server, you can easily adjust the size, configure, and deploy Microsoft SQL Server Always On availability groups. See details here).

# [作業]ALBのDNS名を調べる 3/3

- `jaws-sg-alb`という名前のALBの説明タブにDNS名が表示されています。
- これをコピーしてください。

ロードバランサーの作成 アクション ▼

タグや属性によるフィルター、またはキーワードによる検索

名前	DNS 名	状態	VPC ID	アベイラビリティーゾーン
jaws-sg-alb	jaws-sg-alb-308871413.ap-n...	active	vpc-032d78cb399acc563	ap-northeast-1c, ap-northeast-1a

ロードバランサー: jaws-sg-alb

説明 リスナー モニタリング 統合サービス タグ

基本的な設定

名前 jaws-sg-alb

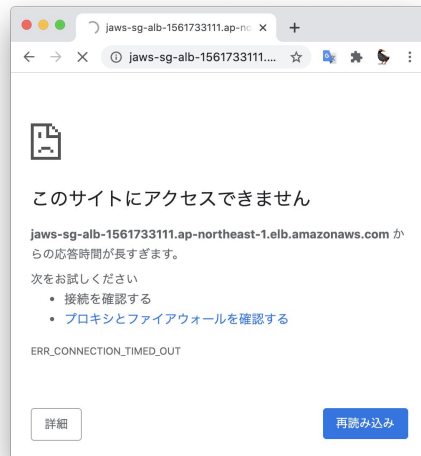
ARN arn:aws:elasticloadbalancing:ap-northeast-1: [redacted]:loadbalancer/app/jaws-sg-alb/54baa63618002dba

DNS 名 jaws-sg-alb-308871413.ap-northeast-1.elb.amazonaws.com (A レコード)

ここをクリックするとコピーできます

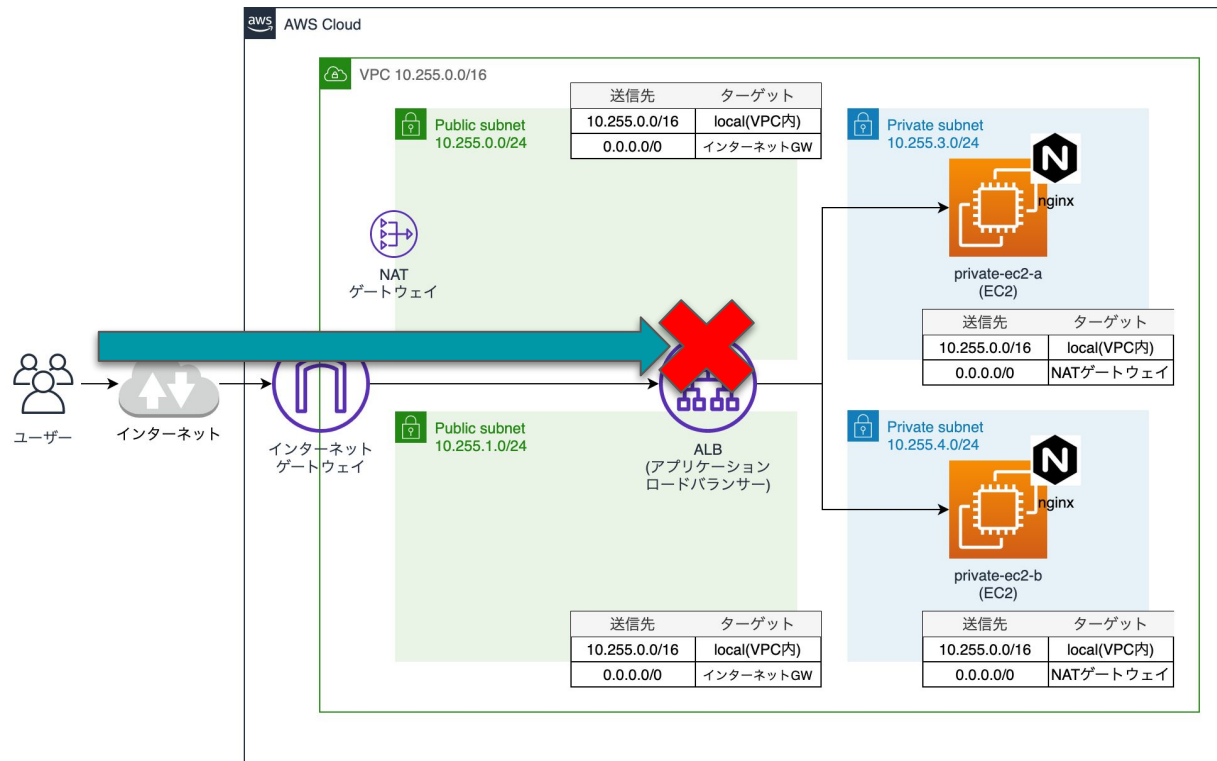
# [作業]ALBにアクセスする

- マネコンが表示されているタブとは別のタブで、アドレスバーにALBのDNS名 + /jaws.htmlと入力してください
  - 例 : `aws-sg-alb-0123456789.ap-northeast-1.elb.amazonaws.com/jaws.html`
- しかし、ブラウザには何も表示されないはずです
- このURLにはハンズオンで繰り返しアクセスするので画面は閉じずにそのままにしておいてください





# アクセスできない理由

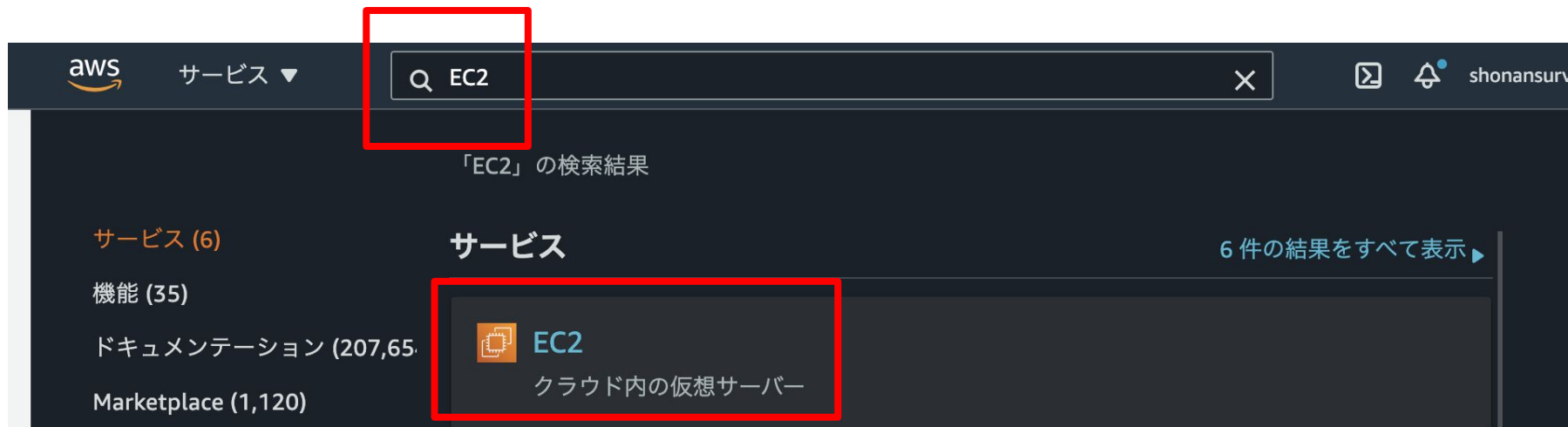


アクセスできない理由は、ALBのセキュリティグループが、インターネットからの通信を拒否しているためです。

この通信を許可するセキュリティグループを作成します。

# [作業]セキュリティグループを作成する 1/7

- マネコンの検索欄にEC2と入力し、EC2を選んでください  
(セキュリティグループはEC2またはVPCの画面で作成できます)。



# [作業]セキュリティグループを作成する 2/7

- EC2ダッシュボード画面から、**セキュリティグループ**を選択してください。

The screenshot shows the AWS Management Console EC2 Dashboard. On the left is a navigation menu with options like 'New EC2 Experience', 'EC2 ダッシュボード', 'イベント', 'タグ', '制限', '▼ インスタンス', 'インスタンス', 'インスタンスタイプ', 'テンプレートの起動', 'スポットリクエスト', 'Savings Plans', 'リザーブドインスタンス', '専有ホスト', and 'キャパシティの予約'. The main area is titled 'リソース' (Resources) and shows a summary of EC2 resources in the 'ap-northeast-1' region. A table lists the following resources and their counts:

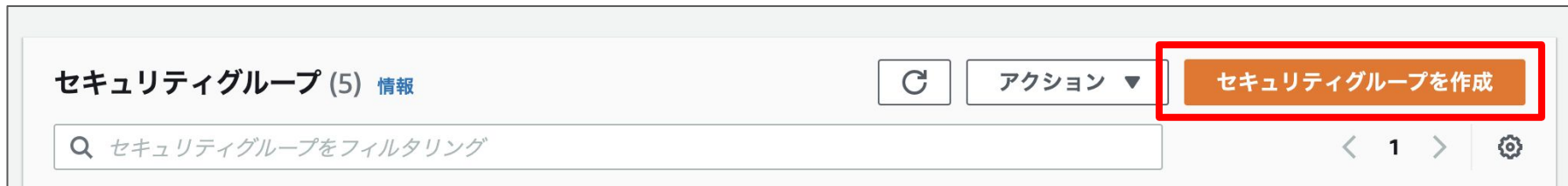
Resource	Count
実行中のインスタンス	3
インスタンス (すべての状態)	3
スナップショット	0
プレイズメントグループ	0
ロードバランサー	1
Elastic IP	1
キーペア	4
<b>セキュリティグループ</b>	<b>5</b>
ボリューム	3
専有ホスト	0

The 'セキュリティグループ' (Security Groups) row is highlighted with a red rectangular box. Below the table, there is a blue information box with the text: 'AWS Launch Wizard for SQL Server を使用すると、Microsoft SQL Server Always On 可用性グループのサイズ調整、設定、デプロイを簡単に行うことができます。詳細はこちら'.

# [作業]セキュリティグループを作成する 3/7

---

- 右上のセキュリティグループを作成ボタンを押してください。



# [作業]セキュリティグループを作成する 4/7

### 基本的な詳細

セキュリティグループ名 情報

jaws-sg-web

作成後に名前を編集することはできません。

説明 情報

jaws-sg-web

VPC 情報

vpc-011ed5e5a25f9d2ac (jaws-sg-vpc)

### インバウンドルール 情報

このセキュリティグループにはインバウン

ルールを追加

1. セキュリティグループ名と説明欄は何でも良いのですが、それぞれ `jaws-sg-web` と入力してください
2. VPCは、`jaws-sg-vpc` を選んでください
3. インバウンドルールのパネルの **ルールを追加** ボタンを押してください

# [作業]セキュリティグループを作成する 5/7

1. **タイプ**欄では許可する通信の種類を指定します。

ここでは**HTTP**を選択してください。

2. **ソース**欄では許可するIPアドレスの範囲を指定します。

ここでは**0.0.0.0/0**を選択してください。これは全IPアドレスを意味します。

**インバウンドルール** 情報

タイプ 情報	プロトコル 情報	ポート範囲 情報	ソース 情報	説明 - オプション 情報
<div>HTTP ▼</div>	TCP	80	<div>カスタム ▼<div>Q0.0.0.0/0 X</div></div>	<div></div> <div>削除</div>

# [作業]セキュリティグループを作成する 6/7

---

- 前ページまでの入力が終わったら、右下のセキュリティグループを作成ボタンを押してください。

キャンセル

セキュリティグループを作成

# [作業]セキュリティグループを作成する 7/7

- 以下のような画面が表示されればセキュリティグループの作成は完了です

🕒 セキュリティグループ (sg-0be633adf5b2b9cc9 | jaws-sg-web) が正常に作成されました

▶ 詳細

EC2 > セキュリティグループ > sg-0be633adf5b2b9cc9 - jaws-sg-web

sg-0be633adf5b2b9cc9 - jaws-sg-web アクション ▼

詳細

セキュリティグループ名 🔗 jaws-sg-web	セキュリティグループ ID 🔗 sg-0be633adf5b2b9cc9	説明 🔗 jaws-sg-web	VPC ID 🔗 vpc-011ed5e5a25f9d2ac 🔗
所有者 🔗 [REDACTED]	インバウンドルールカウント 1 アクセス許可エントリ	アウトバウンドルールカウント 1 アクセス許可エントリ	

インバウンドルール    アウトバウンドルール    タグ

インバウンドルール インバウンドルールを編集

タイプ	プロトコル	ポート範囲	ソース	説明 - オプション
HTTP	TCP	80	0.0.0.0/0	-



# [作業]セキュリティグループを付ける 1/3

1. 左側のメニューの上部のEC2ダッシュボードを押してください
2. 次にロードバランサーを選択してください

The screenshot shows the AWS Management Console interface. On the left, the 'New EC2 Experience' header is visible, followed by a list of navigation items. The 'EC2 ダッシュボード' (EC2 Dashboard) item is highlighted with a red box. Below it, the 'インスタンス' (Instances) section is expanded, showing various instance-related options. On the right, the 'リソース' (Resources) section displays a summary of EC2 resources in the 'アジアパシフィック (東京)' (Asia Pacific (Tokyo)) region. A table lists the following resources:

Resource	Count
実行中のインスタンス (Running Instances)	3
インスタンス (すべての状態) (Instances (all states))	3
スナップショット (Snapshots)	0
プレースメントグループ (Placement Groups)	0
ロードバランサー (Load Balancers)	1
Elastic IP	1
キーペア (Key Pairs)	4
セキュリティグループ (Security Groups)	5
ボリューム (Volumes)	3
専用ホスト (Dedicated Hosts)	0

The 'ロードバランサー' (Load Balancers) item is highlighted with a red box, indicating the next step in the task.

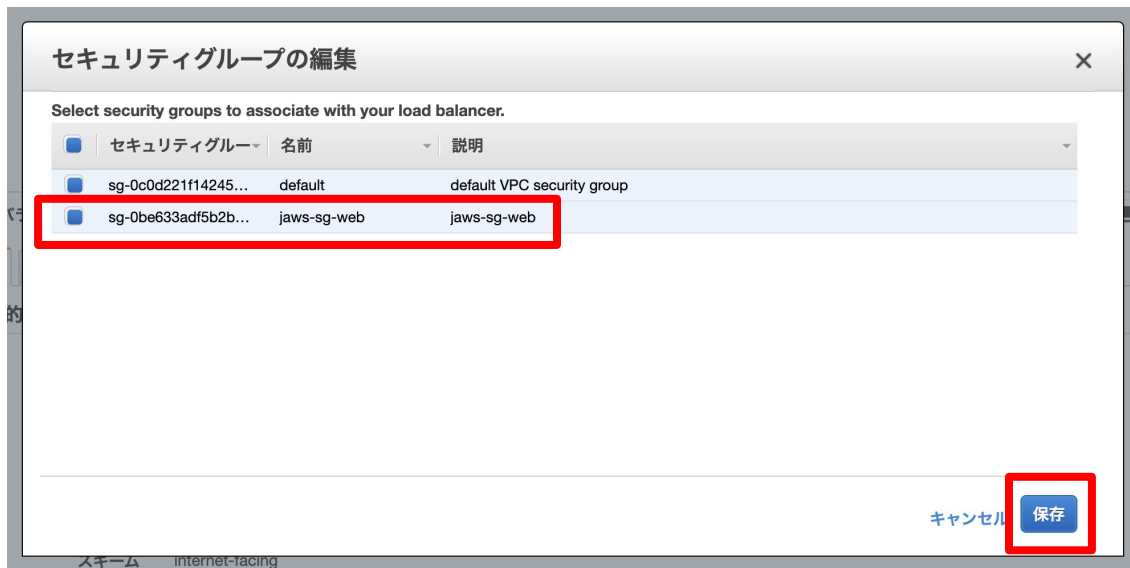
# [作業]セキュリティグループを付ける 2/3

- `jaws-sg-alb`という名前のALBが選択された状態で、アクションボタンを押し、セキュリティグループの編集を選択してください



# [作業]セキュリティグループを付ける 3/3

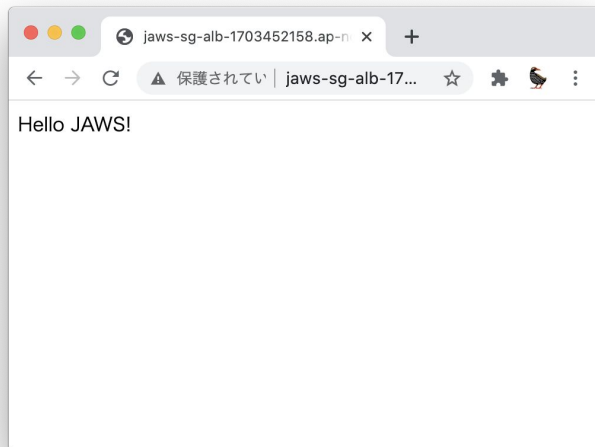
1. `jaws-sg-web`のチェックボックスにチェックを入れてください
2. 次に保存ボタンを選択してください



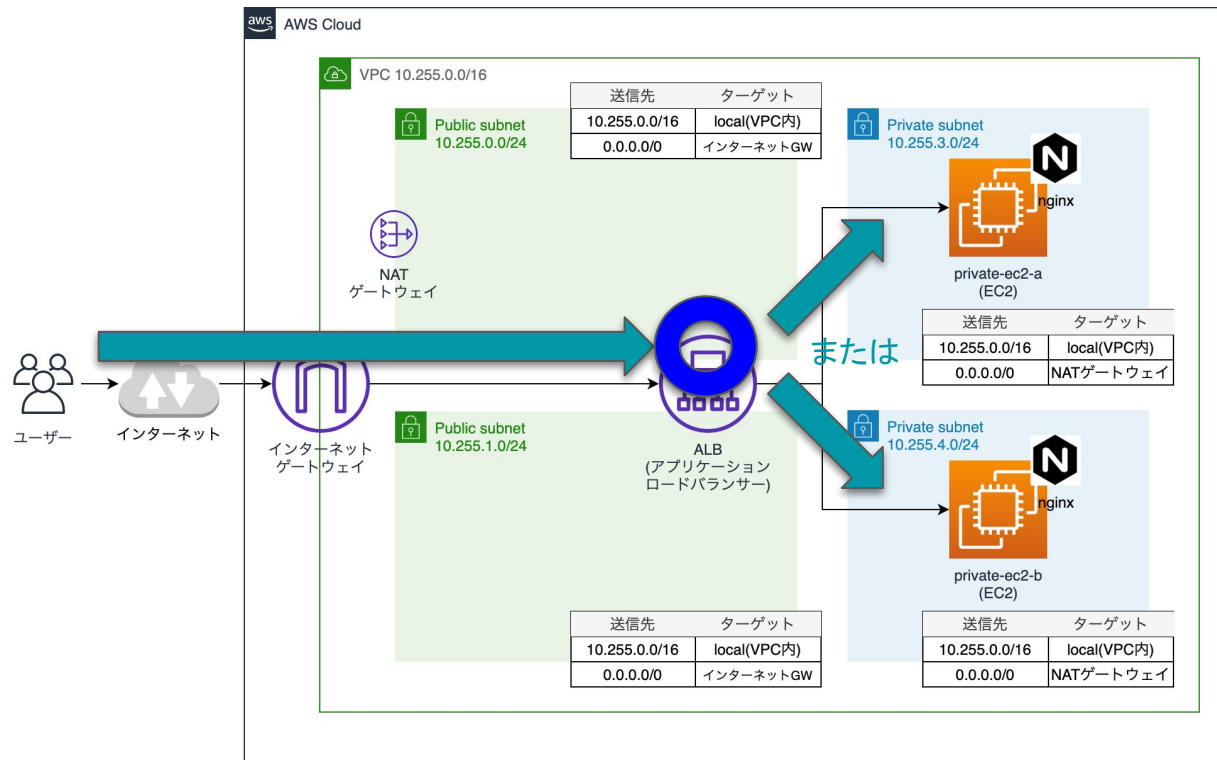
# [作業]ALBにアクセスする

---

- 再びブラウザでALBのDNS名 + `/jaws.html`にアクセスしてください
  - 例 : `aws-sg-alb-0123456789.ap-northeast-1.elb.amazonaws.com/jaws.html`
- 以下のようにHello JAWS!と表示されれば成功です

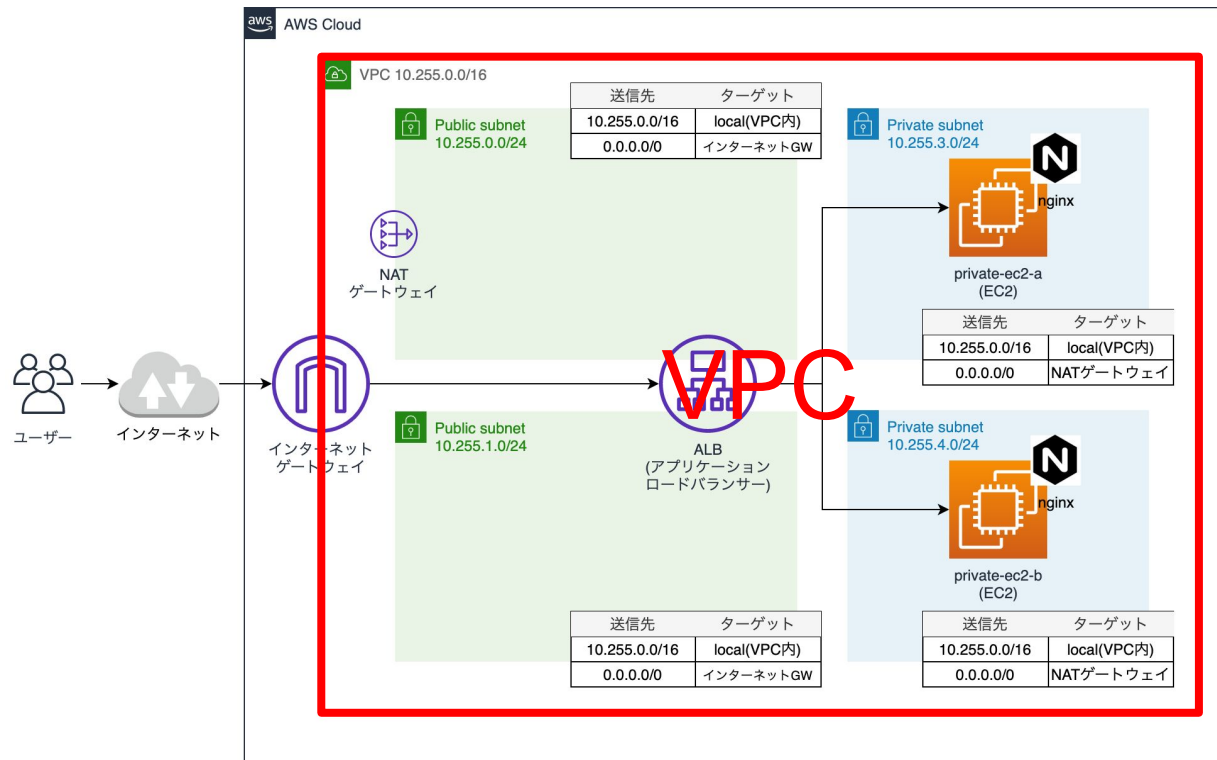


# アクセスできた理由



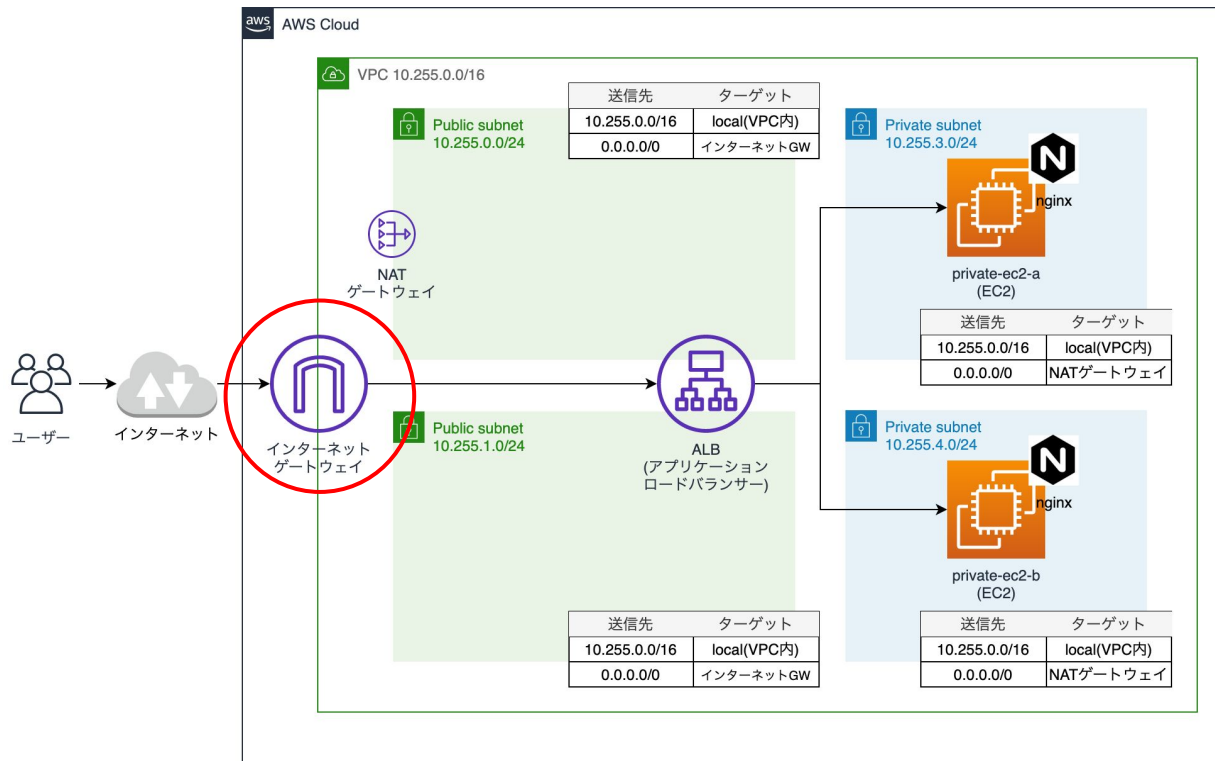
ALBのセキュリティグループが全てのIPアドレスからのHTTP通信を許可するようになったため、「Hello JAWS!」が表示されるようになりました。

# セキュリティグループ以外に必要な条件 1/4



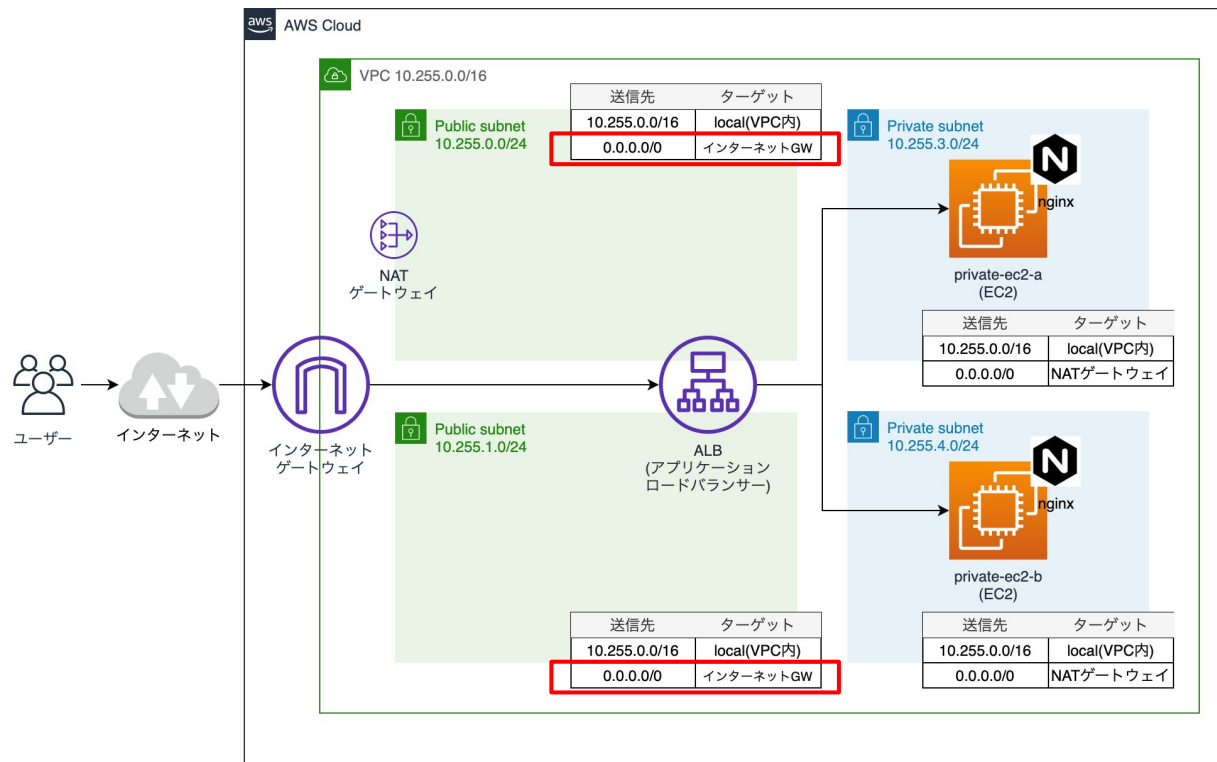
なお、VPC内のリソース (ALBやEC2など)が、インターネットからの通信を受け付けるためには、**セキュリティグループ以外**にも設定が必要なものがあります

# セキュリティグループ以外に必要な条件 2/4



VPCに、インターネット  
ゲートウェイが設置されて  
いること

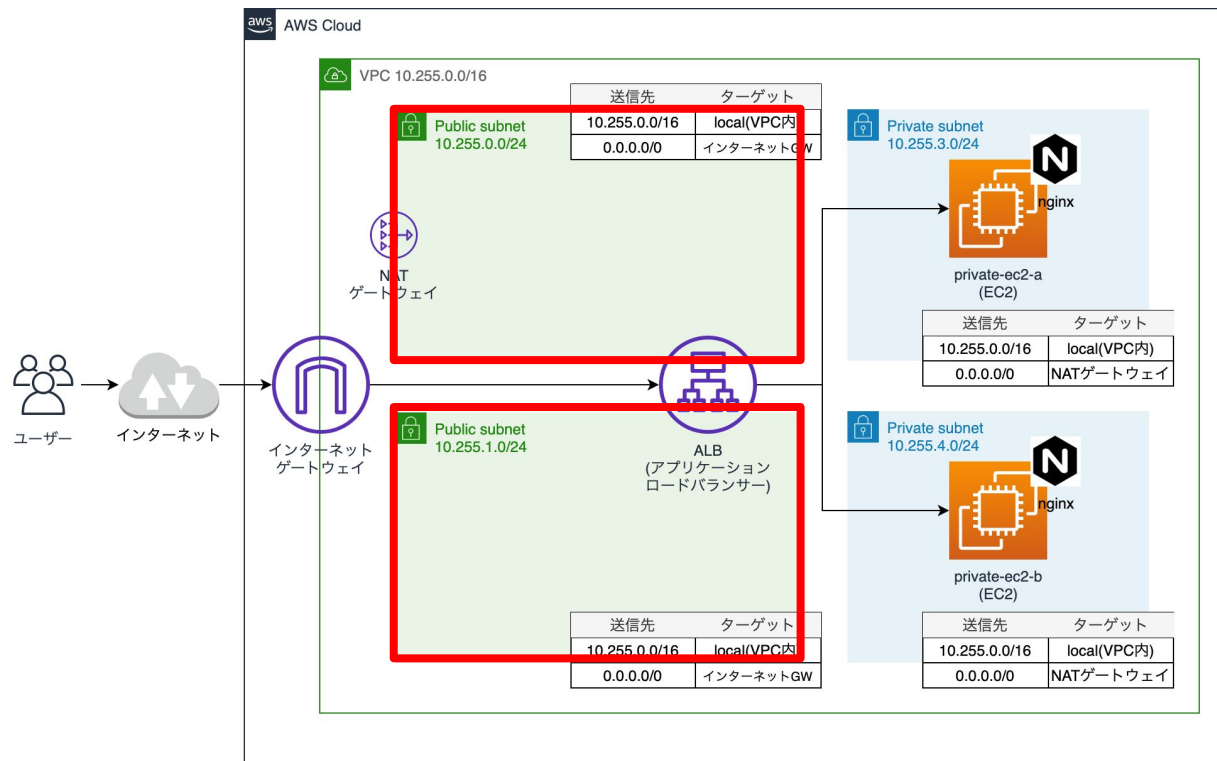
# セキュリティグループ以外に必要な条件 3/4



リソース(今回でいうとALB)の属するサブネットのルートテーブルにおいて、VPC外のIPアドレスに対する通信の向き先がインターネットゲートウェイになっていること



# セキュリティグループ以外に必要な条件 4/4



リソース(今回でいうとALB)の属するサブネットと関連付けられているネットワークACLにおいて、VPC外との通信が拒否されていないこと

# インターネットからの通信受付に必要な条件

---

ハンズオン環境構築用のCloudFormationであらかじめ設定済み

- ✓ VPCに、インターネットゲートウェイを設置
- ✓ ルートテーブルにおいて、VPC外のIPアドレスに対する通信の向き先がインターネットゲートウェイとなっている
- ✓ ネットワークACLにおいて、VPC外との通信を許可(AWSのデフォルト設定)

本ハンズオンで、みなさん自身で設定したこと

- ✓ セキュリティグループにおいて、VPC外のIPアドレスからの通信を許可

ケース1 終了

# ケース2

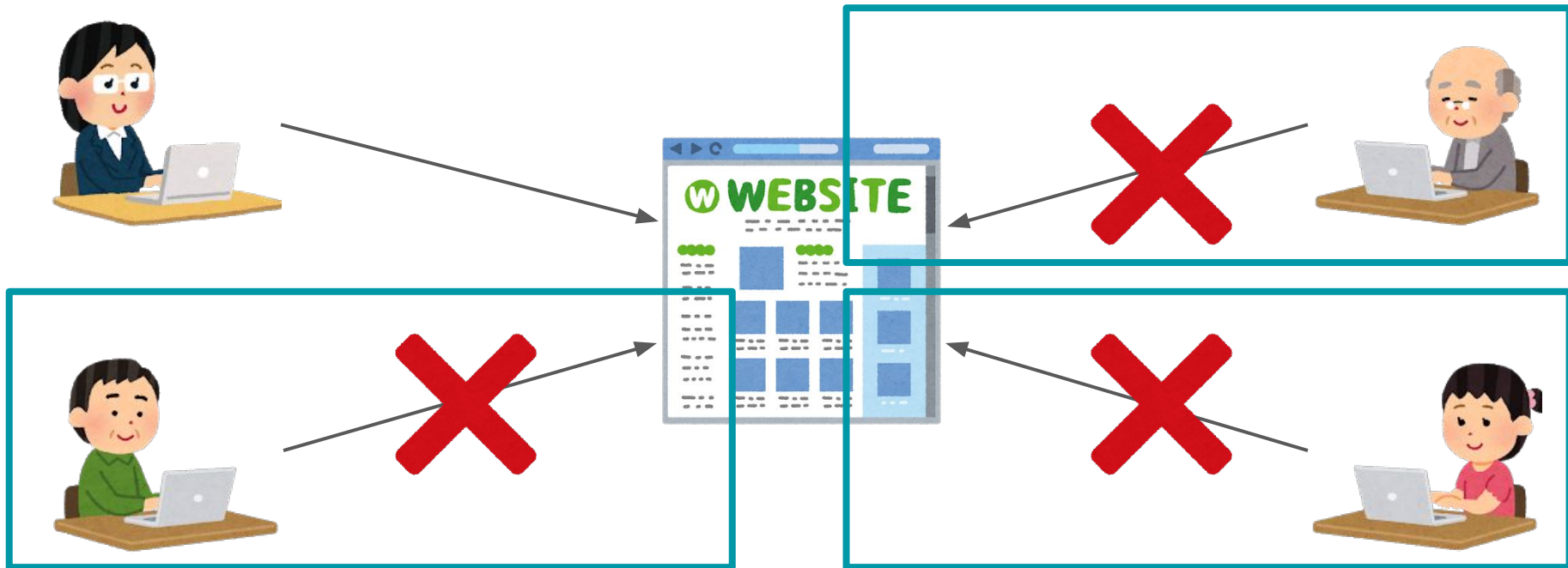
特定のIPアドレスからのみ、Webサービスにアクセス(HTTP通信)できる



社内関係者だけをアクセスさせたいサイトや、  
開発者だけをアクセスさせたい検証用サイトなどを想定

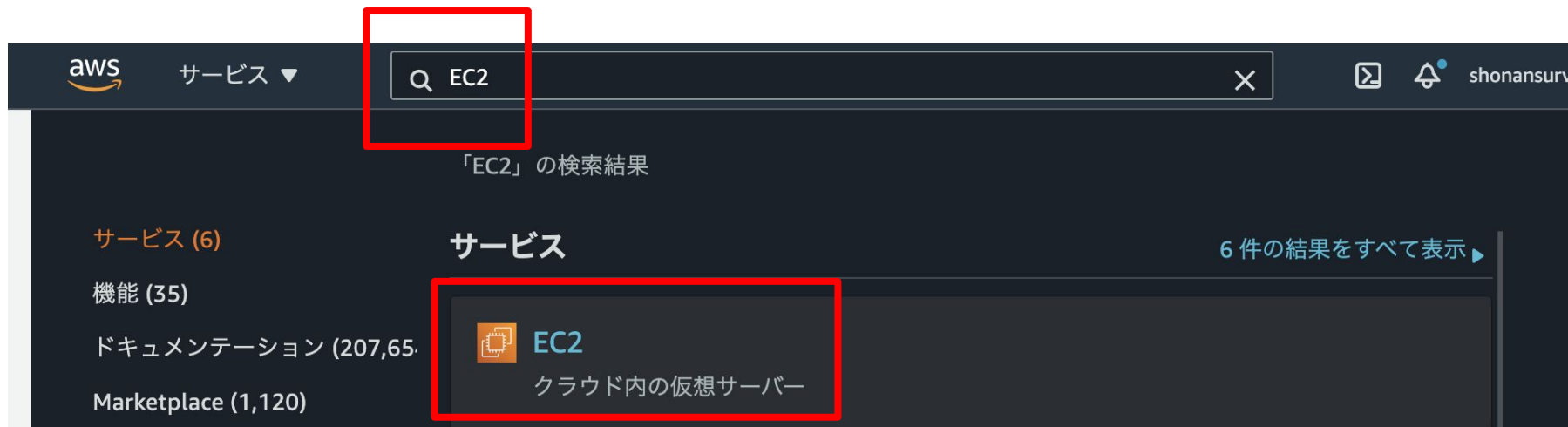
# ケース2 前編

まず最初は、アクセスできない側を体験することになります



# [作業]セキュリティグループ設定変更 1/5

- マネコンの検索欄にEC2と入力し、EC2を選んでください  
(セキュリティグループはEC2またはVPCの画面にあります)。



# [作業]セキュリティグループ設定変更 2/5

- EC2ダッシュボード画面から、**セキュリティグループ**を選択してください。

The screenshot shows the AWS Management Console EC2 Dashboard. The left sidebar contains navigation links: 'New EC2 Experience', 'EC2 ダッシュボード', 'イベント', 'タグ', '制限', '▼ インスタンス', 'インスタンス', 'インスタンスタイプ', 'テンプレートの起動', 'スポットリクエスト', 'Savings Plans', 'リザーブドインスタンス', '専有ホスト', and 'キャパシティの予約'. The main content area is titled 'リソース' (Resources) and shows a summary of resources in the 'アジアパシフィック (東京) リージョン' (Asia Pacific (Tokyo) Region). A table lists the following resources and their counts:

Resource	Count
実行中のインスタンス	3
インスタンス (すべての状態)	3
スナップショット	0
プレースメントグループ	0
ロードバランサー	1
Elastic IP	1
キーペア	4
<b>セキュリティグループ</b>	<b>5</b>
ボリューム	3
専有ホスト	0

The 'セキュリティグループ' row is highlighted with a red box. Below the table, there is a notification about the 'AWS Launch Wizard for SQL Server'.

# [作業]セキュリティグループ設定変更 3/5

1. `jaws-sg-web`のチェックボックスにチェックを入れてください
2. 右上のアクションを押し、インバウンドルールを編集を選択してください

セキュリティグループ (1/3) 情報

Q セキュリティグループをフィルタリング

	Name	セキュリティグループ...	セキュリティグループ名		説明
<input type="checkbox"/>	-	sg-0035fec59d25d523e	default		default V
<input type="checkbox"/>	-	sg-036c4aa666b453b39	default		default V
<input checked="" type="checkbox"/>	-	sg-0b4afb27eb4ace3e2	jaws-sg-web	vpc-057a79b02c818acc4	jaws-sg-v

アクション ▲

- 詳細を表示
- インバウンドルールを編集
- アウトバウンドルールを編集
- タグを管理
- 古いルールを管理

セキュリティグループを作成



# [作業]セキュリティグループ設定変更 4/5

1. まず、0.0.0.0/0のバツボタンを押して削除してください

インバウンドルール 情報

タイプ 情報	プロトコル 情報	ポート範囲 情報	ソース 情報	説明 - オプション 情報
HTTP ▼	TCP	80	カスタム ▼ 0.0.0.0/0 ×	<input type="text"/>

削除

2. 次に、適当なIPアドレスとして、192.0.2.1/32を入力してください

タイプ 情報

プロトコル 情報

ポート範囲 情報

ソース 情報

説明 - オプション 情報

HTTP ▼	TCP	80	カスタム ▼ Q 192.0.2.1/32 ×	<input type="text"/>
--------	-----	----	----------------------------	----------------------

ルールを追加

CIDR ブロック

192.0.2.1/32

削除

# [作業]セキュリティグループ設定変更 5/5

- 前ページまでの入力が終わったら、右下のルールを保存ボタンを押してください

タイプ 情報

HTTP ▼

プロトコル 情報

TCP

ポート範囲 情報

80

ソース 情報

カスタム ▼

Q

192.0.2.1/32 X

説明 - オプション 情報

削除

ルールを追加

⚠ 注意: 既存のルールを編集すると、編集したルールが削除されて、新しい詳細を含む新しいルールが作成されます。これにより、そのルールに依存するトラフィックは、新しいルールが作成されるまで非常に短時間切断されます。

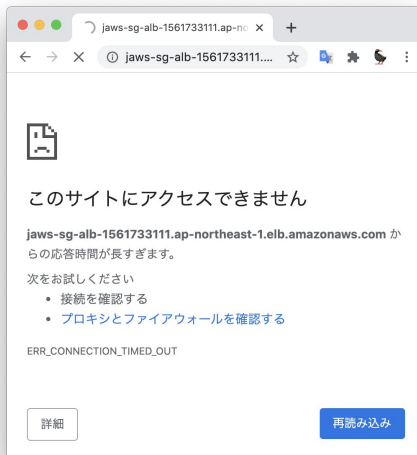
キャンセル

変更をプレビュー

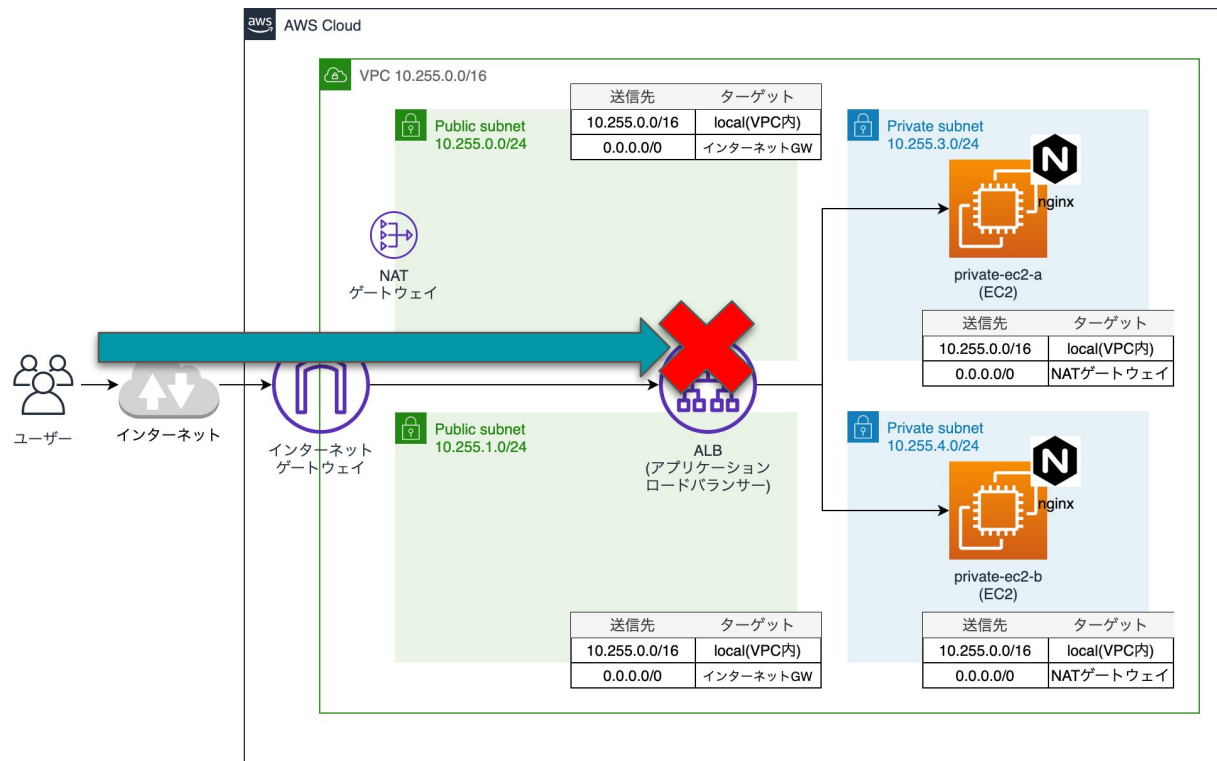
ルールを保存

# [作業]ALBにアクセスする

- ブラウザでALBのDNS名 + /jaws.htmlにアクセスしてください
  - 例 : `jaws-sg-alb-0123456789.ap-northeast-1.elb.amazonaws.com/jaws.html`
- しかし、ブラウザには何も表示されないはずです



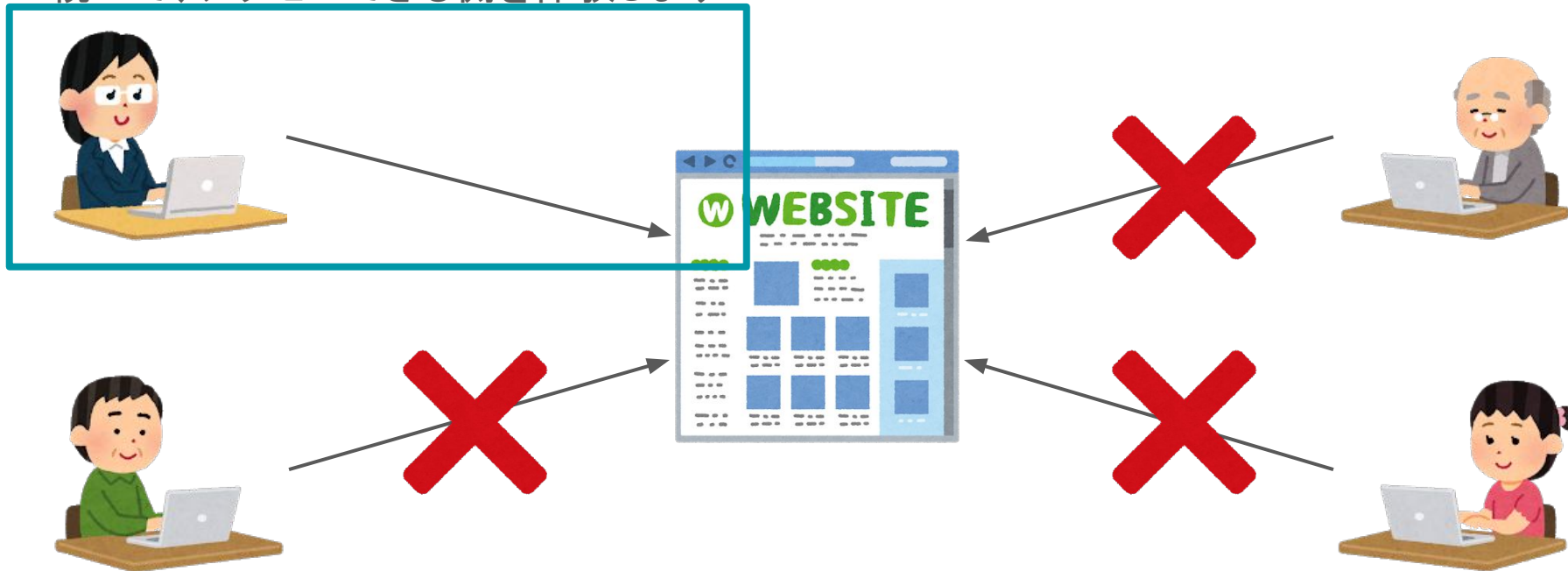
# アクセスできない理由



アクセスできない理由は、ALBのセキュリティグループが「皆さんのPCがインターネットと通信する時に使用されているIPアドレス」からのHTTP通信を拒否するようになったためです

## ケース2 後編

続いて、アクセスできる側を体験します



# [作業]セキュリティグループ設定変更 1/3

1. `jaws-sg-web`のチェックボックスにチェックを入れてください
2. 右上のアクションを押し、インバウンドルールを編集を選択してください

セキュリティグループ (1/3) 情報

Q セキュリティグループをフィルタリング

	Name	セキュリティグループ...	セキュリティグループ名		説明
<input type="checkbox"/>	-	sg-0035fec59d25d523e	default		default V
<input type="checkbox"/>	-	sg-036c4aa666b453b39	default		default V
<input checked="" type="checkbox"/>	-	sg-0b4afb27eb4ace3e2	jaws-sg-web	vpc-057a79b02c818acc4	jaws-sg-v

アクション ▲

- 詳細を表示
- インバウンドルールを編集
- アウトバウンドルールを編集
- タグを管理
- 古いルールを管理

セキュリティグループを作成

# [作業]セキュリティグループ設定変更 2/3

1. まず、192.0.2.1/32の**バツボタン**を押して削除してください

タイプ 情報	プロトコル 情報	ポート範囲 情報	ソース 情報	説明 - オプション 情報
HTTP ▼	TCP	80	カスタム ▼	Q
192.0.2.1/32 ×				削除

2. 次に**マイIP**を選択してください。

タイプ 情報	プロトコル 情報	ポート範囲 情報	ソース 情報	説明 - オプション 情報
HTTP ▼	TCP	80	カスタム ▲	Q
カスタム				削除
任意の場所				
マイ IP				

ルールを追加

# [作業]セキュリティグループ設定変更 3/3

- マイIPを選択すると「あなたのPCがインターネットと通信する時に使用されているIPアドレス」が自動入力されます
- そのままルールを保存ボタンを押してください

タイプ 情報    プロトコル 情報    ポート範囲 情報    ソース 情報    説明 - オプション 情報

HTTP    TCP    80    カスタム    🔍    削除

あなたのIPアドレス

ルールを追加

⚠️ 注意: 既存のルールを編集すると、編集したルールが削除されて、新しい詳細を含む新しいルールが作成されます。これにより、そのルールに依存するトラフィックは、新しいルールが作成されるまで非常に短時間切断されます。

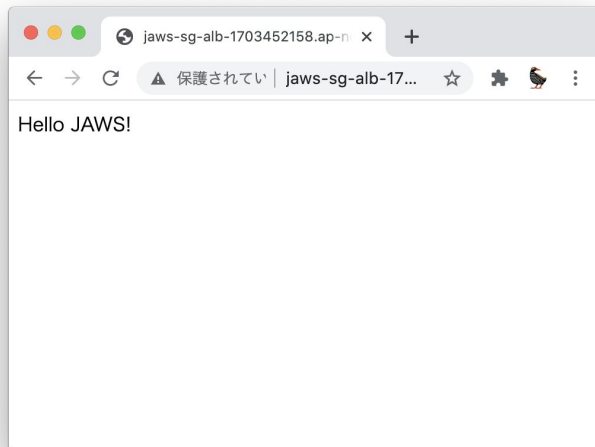
キャンセル    変更をプレビュー    **ルールを保存**



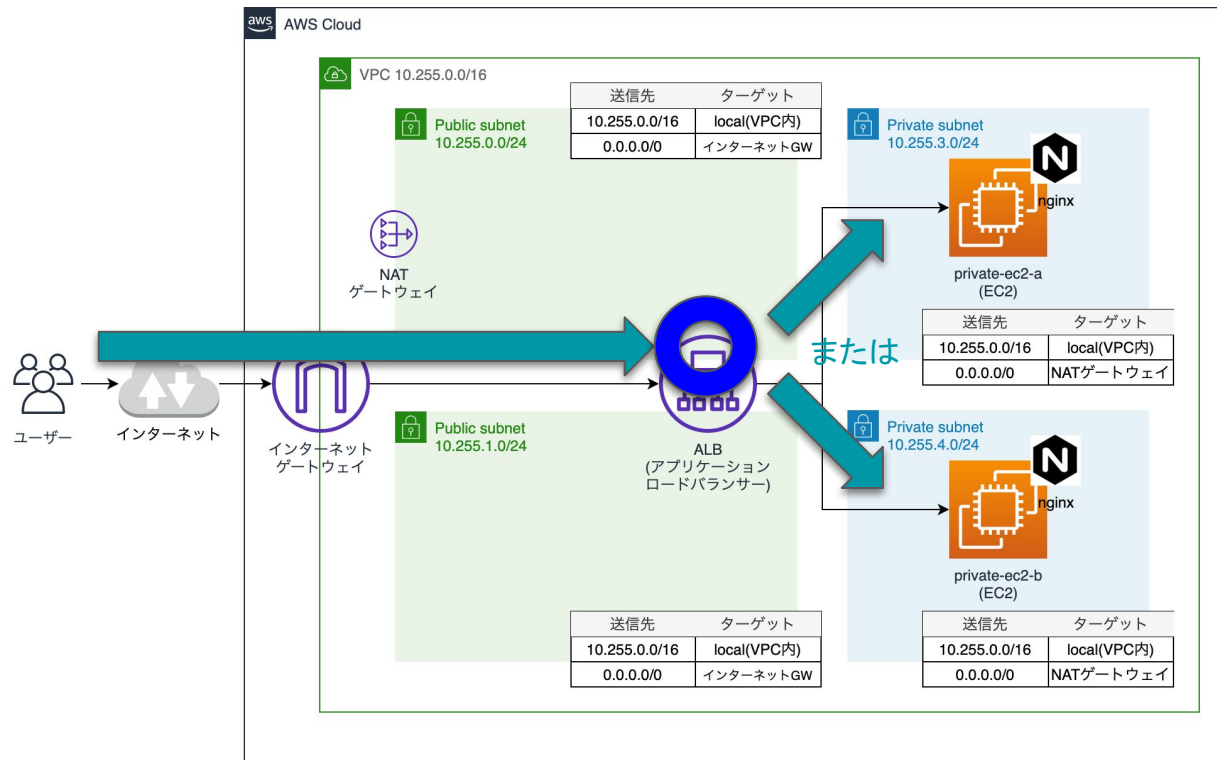
# [作業]ALBにアクセスする

---

- ブラウザでALBのDNS名 + /jaws.htmlにアクセスしてください
  - 例 : `jaws-sg-alb-0123456789.ap-northeast-1.elb.amazonaws.com/jaws.html`
- 以下のようにHello JAWS!と表示されれば成功です



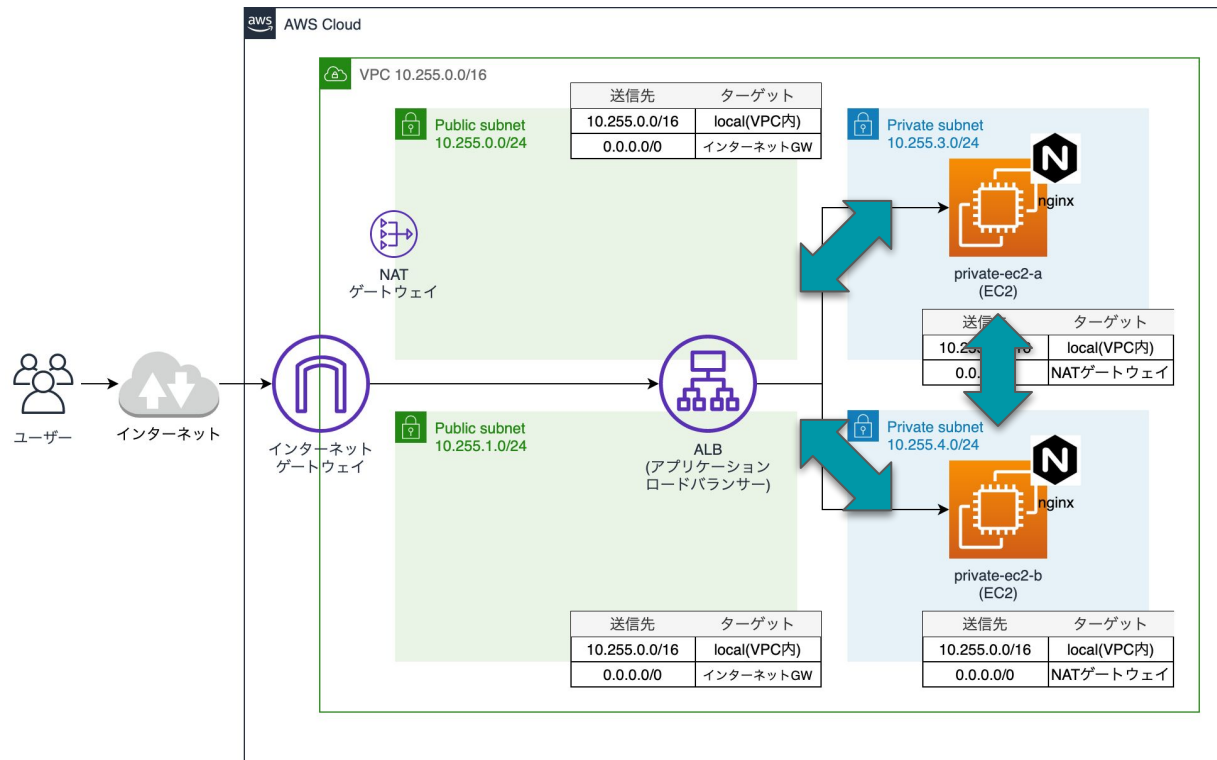
# アクセスできた理由



ALBのセキュリティグループが「あなたのPCがインターネットと通信する時に使用されているIPアドレス」からのHTTP通信を許可するようになったため「Hello JAWS!」が表示されるようになりました。

ケース2 終了

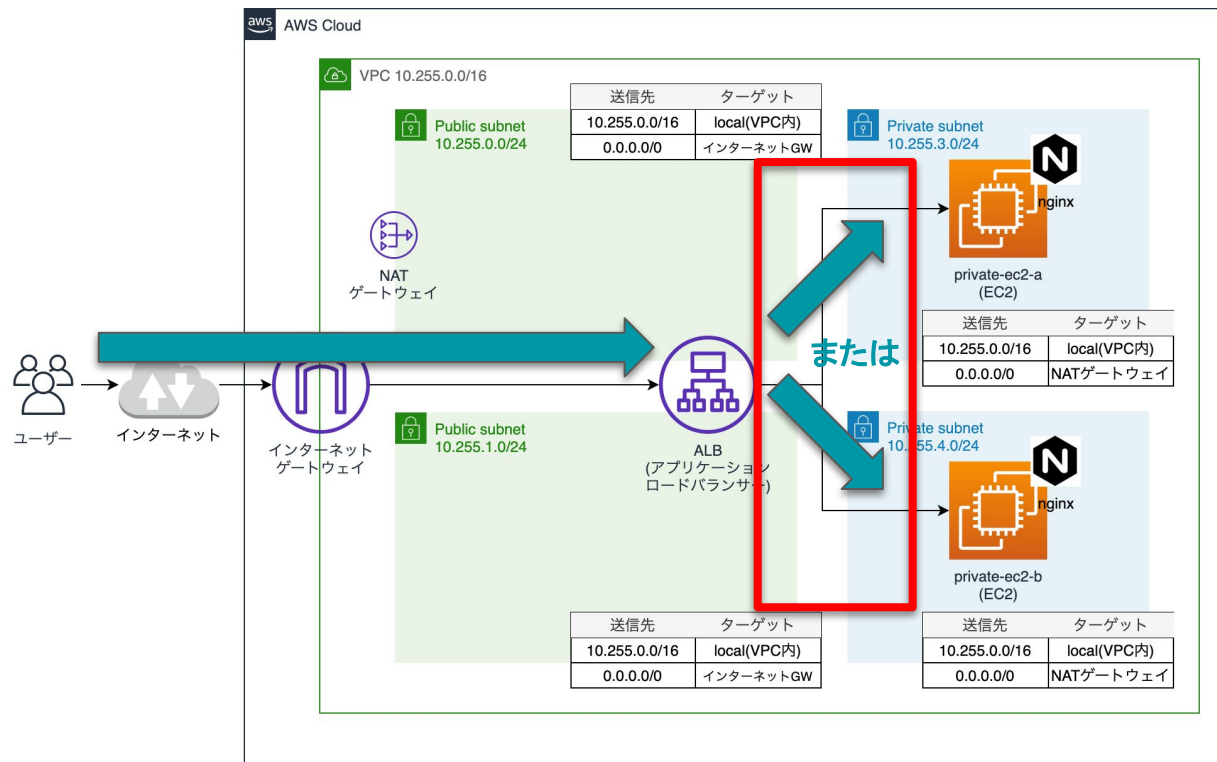
# ケース3



特定のリソース同士を、相互に通信可能とする

ケース3はもう実現済みです。  
何故そうなっているのか、  
設定を確認していきましょう。

# ALBからEC2への通信について



ALBからは、2台あるEC2  
それぞれに通信が可能と  
なっています。

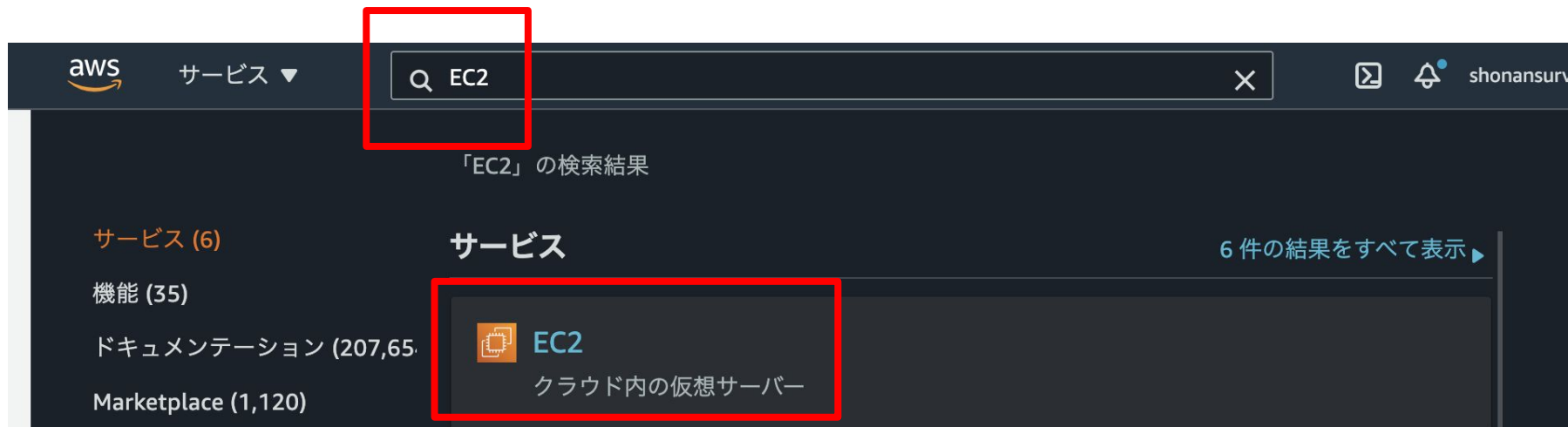
通信を受ける側のEC2の  
セキュリティグループはど  
うなっているのでしょ  
うか？

確認してみます。

# [作業]EC2のセキュリティグループ確認 1/7

- まず、EC2の設定を確認します。

そのために、マネコンの検索欄にEC2と入力し、EC2を選んでください。



# [作業]EC2のセキュリティグループ確認 2/7

- EC2ダッシュボード画面から、**実行中のインスタンス**を選択してください。

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with options like 'New EC2 Experience', 'EC2 ダッシュボード', 'イベント', 'タグ', '制限', '▼ インスタンス', 'インスタンス', 'インスタンスタイプ', 'テンプレートの起動', 'スポットリクエスト', 'Savings Plans', 'リザーブドインスタンス', '専有ホスト', and 'キャパシティの予約'. The main content area is titled 'リソース' (Resources) and shows a summary of EC2 resources in the 'アジアパシフィック (東京) リージョン'. A table lists the following resources:

リソース	数
実行中のインスタンス	3
インスタンス (すべての状態)	3
スナップショット	0
プレースメントグループ	0
ロードバランサー	1
Elastic IP	1
キーペア	4
セキュリティグループ	5
ボリューム	3
専有ホスト	0






A red rectangular box highlights the '実行中のインスタンス' (Running Instances) row in the table. Below the table, there is a blue information box with a message about the AWS Launch Wizard for SQL Server.

AWS Launch Wizard for SQL Server を使用すると、Microsoft SQL Server Always On 可用性グループのサイズ調整、設定、デプロイを簡単に行うことができます。詳細はこちら



# [作業]EC2のセキュリティグループ確認 3/7

- まず、`jaws-sg-private-ec2-a`にチェックを入れてください。

	Name	▼	インスタンス ID	インスタンス...	▼
<input type="checkbox"/>	jaws-sg-private-ec2-b		i-0f294716eed772cb9	✔ 実行中	 
<input checked="" type="checkbox"/>	jaws-sg-private-ec2-a		i-0759af8846a0c516d	✔ 実行中	 

# [作業]EC2のセキュリティグループ確認 3/7

- 次にセキュリティタブを選択し、表示されているセキュリティグループのIDをクリックしてください。

これが、このEC2に付けられているセキュリティグループとなります。

The screenshot shows the AWS Management Console interface for an EC2 instance. At the top, there is a table with columns: Name, インスタンス ID, and インスタンス... . The table lists two security groups: 'jaws-sg-private-ec2-b' and 'jaws-sg-private-ec2-a'. The second group is selected with a checkmark. Below the table, the instance details for 'i-0759af8846a0c516d (jaws-sg-private-ec2-a)' are shown. The 'セキュリティ' tab is selected and highlighted with a red box. Below this, the 'セキュリティの詳細' section shows the 'IAM ロール' as '-' and the 'セキュリティグループ' as 'sg-0146d4b24939266d5 (default)', which is also highlighted with a red box. A red arrow points from the 'セキュリティ' tab to the highlighted security group ID.

	Name	インスタンス ID	インスタンス...
<input type="checkbox"/>	jaws-sg-private-ec2-b	i-0f294716eed772cb9	実行中
<input checked="" type="checkbox"/>	jaws-sg-private-ec2-a	i-0759af8846a0c516d	実行中

インスタンス: i-0759af8846a0c516d (jaws-sg-private-ec2-a)

詳細 **セキュリティ** ネットワーキング ストレージ ステータスチェック モニタリング

▼ セキュリティの詳細

IAM ロール  
-

セキュリティグループ  
sg-0146d4b24939266d5 (default)

所有者 ID  
[Redacted]

# [作業]EC2のセキュリティグループ確認 4/7

- `jaws-sg-private-ec2-a`に付けられているセキュリティグループの情報が表示されます。なお、セキュリティグループの名前は`default`です。

sg-0146d4b24939266d5 - default

アクション ▼

詳細

セキュリティグループ名 default	セキュリティグループ ID sg-0146d4b24939266d5	説明 default VPC security group	VPC ID vpc-079c60b81ec2e751c
所有者 [ユーザーアイコン]	インバウンドルールカウント 1 アクセス許可エントリ	アウトバウンドルールカウント 1 アクセス許可エントリ	

インバウンドルール

アウトバウンドルール

タグ

インバウンドルール

インバウンドルールを編集

タイプ	プロトコル	ポート範囲	ソース	説明 - オプション
すべてのトラフィック	すべて	すべて	sg-0146d4b24939266d5 (default)	-

# [作業]EC2のセキュリティグループ確認 5/7

- インバウンドルールでは、**タイプ**が**すべてのトラフィック**となっており、HTTPに限らず、全ての通信種類が許可されています。

sg-0146d4b24939266d5 - default

アクション ▼

詳細

セキュリティグループ名 default	セキュリティグループ ID sg-0146d4b24939266d5	説明 default VPC security group	VPC ID vpc-079c60b81ec2e751c
所有者 [ユーザーアイコン]	インバウンドルールカウント 1 アクセス許可エントリ	アウトバウンドルールカウント 1 アクセス許可エントリ	

インバウンドルール

アウトバウンドルール

タグ

インバウンドルール

インバウンドルールを編集

タイプ	プロトコル	ポート範囲	ソース	説明 - オプション
すべてのトラフィック	すべて	すべて	sg-0146d4b24939266d5 (default)	-

# [作業]EC2のセキュリティグループ確認 6/7

- ソース欄には許可するアクセス元を指定しますが、IPアドレスではなく、セキュリティグループのIDが表示されています。

sg-0146d4b24939266d5 - default

アクション ▼

詳細

セキュリティグループ名 default	セキュリティグループ ID sg-0146d4b24939266d5	説明 default VPC security group	VPC ID vpc-079c60b81ec2e751c
所有者 [ユーザーアイコン]	インバウンドルールカウント 1 アクセス許可エントリ	アウトバウンドルールカウント 1 アクセス許可エントリ	

インバウンドルール

アウトバウンドルール

タグ

インバウンドルール

インバウンドルールを編集

タイプ	プロトコル	ポート範囲	ソース	説明 - オプション
すべてのトラフィック	すべて	すべて	sg-0146d4b24939266d5 (default)	-

# [作業]EC2のセキュリティグループ確認 7/7

- ソース欄に表示されているセキュリティグループのIDは、このセキュリティグループ自身のIDです。

sg-0146d4b24939266d5 - default

アクション ▼

詳細

セキュリティグループ名 default	セキュリティグループ ID sg-0146d4b24939266d5	説明 default VPC security group	VPC ID vpc-079c60b81ec2e751c
所有者 [ユーザー名]	インバウンドルールカウント 1 アクセス許可エントリ	アウトバウンドルールカウント 1 アクセス許可エントリ	

インバウンドルール    アウトバウンドルール    タグ

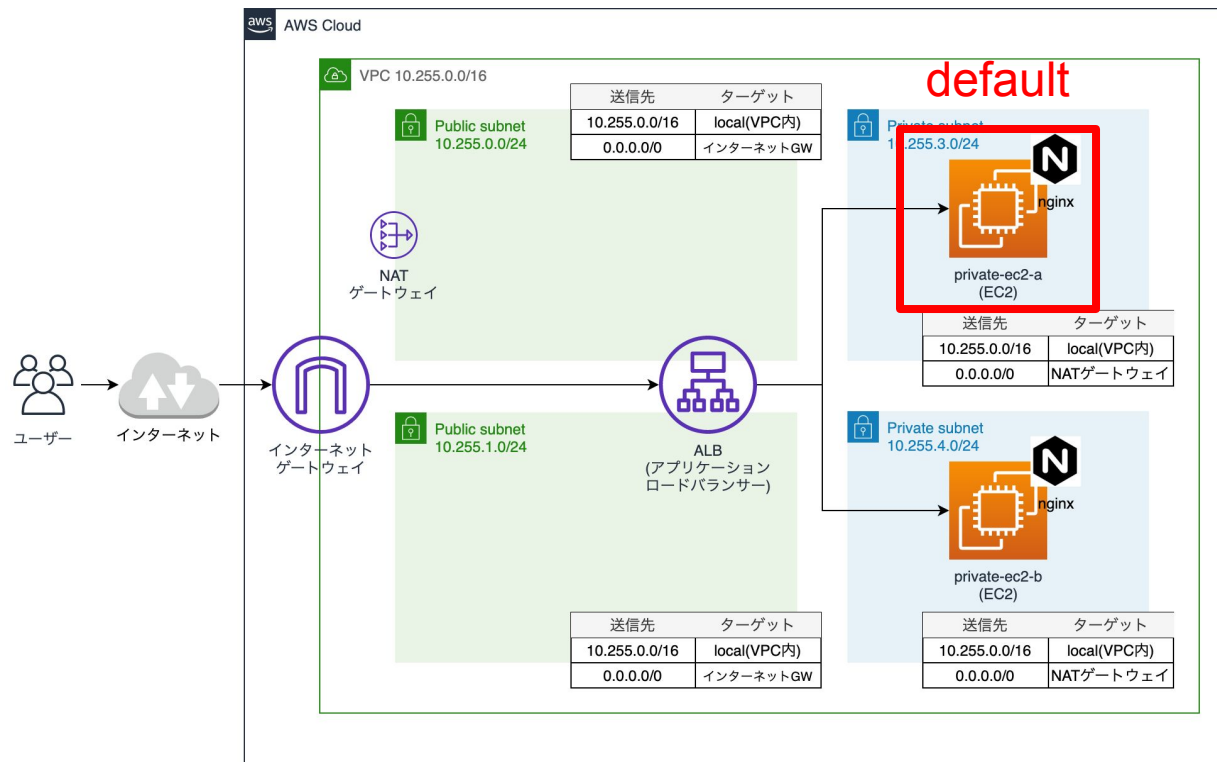
インバウンドルール

タイプ	プロトコル	ポート範囲	ソース	説明 - オプション
すべてのトラフィック	すべて	すべて	sg-0146d4b24939266d5 (default)	-

インバウンドルールを編集

それって、つまりどういうこと？

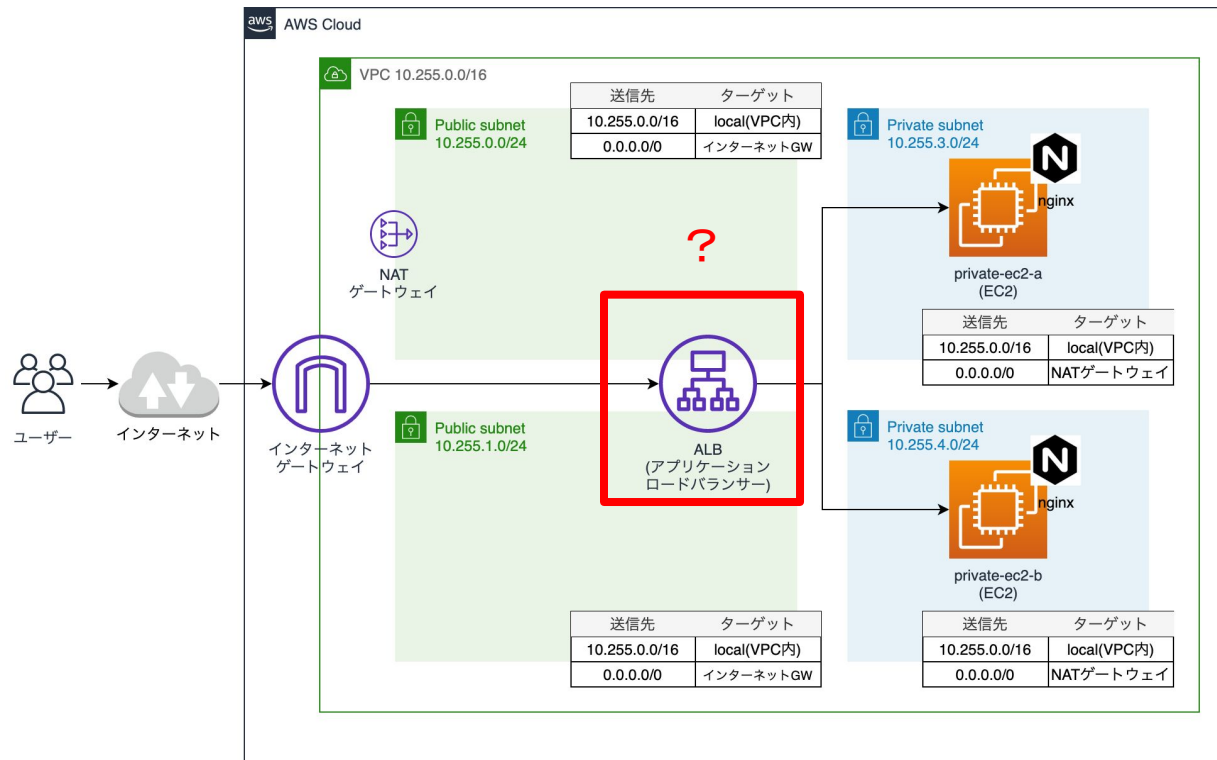
# EC2のセキュリティグループの解説



private-ec2-aにはdefault  
という名前のセキュリティ  
グループが付けられてい  
ますが、同じセキュリティ  
グループが付けられてい  
る他のリソースと通信でき  
ることになります。



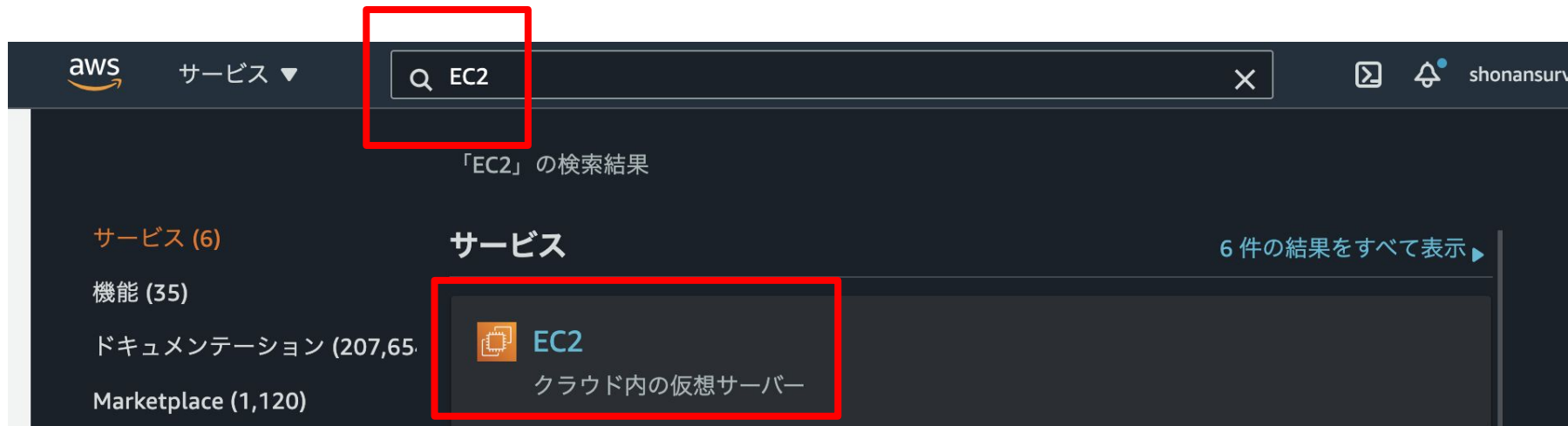
# ALBのセキュリティグループについて



続いて、ALBのセキュリティグループがどうなっているか確認します。

# [作業]ALBのセキュリティグループ確認 1/4

- マネコンの検索欄にEC2と入力し、EC2を選んでください  
(ALBはEC2の画面に存在します)。



# [作業]ALBのセキュリティグループ確認 2/4

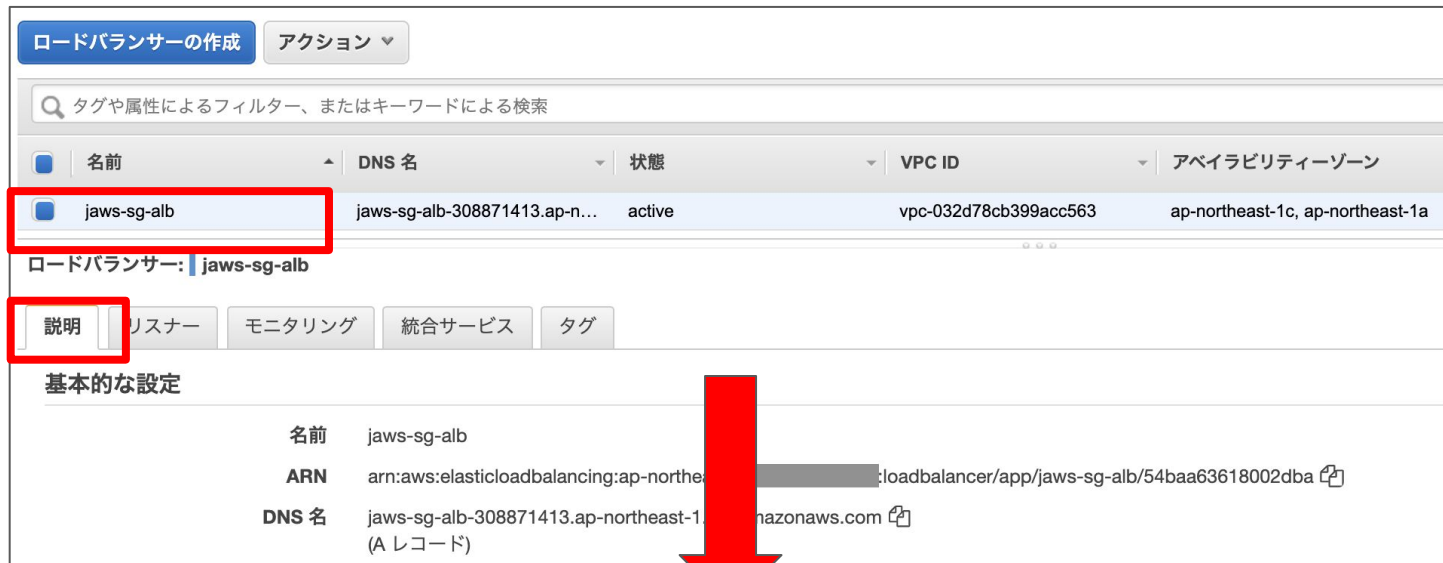
- EC2ダッシュボード画面から、ロードバランサーを選択してください。

The screenshot shows the AWS Management Console EC2 Dashboard. On the left is a navigation menu with options like 'EC2 ダッシュボード', 'イベント', 'タグ', '制限', 'インスタンス', 'インスタンスタイプ', 'テンプレートの起動', 'スポットリクエスト', 'Savings Plans', 'リザーブドインスタンス', '専有ホスト', and 'キャパシティの予約'. The main area is titled 'リソース' (Resources) and shows a table of EC2 resources in the 'アジアパシフィック (東京)' region. The table has two columns: resource name and count. The 'ロードバランサー' (Load Balancers) row is highlighted with a red box, showing a count of 1. Other resources include '実行中のインスタンス' (3), 'インスタンス (すべての状態)' (3), 'スナップショット' (0), 'プレイズメントグループ' (0), 'Elastic IP' (1), 'キーペア' (4), 'セキュリティグループ' (5), 'ボリューム' (3), and '専有ホスト' (0). A notification banner at the bottom mentions 'AWS Launch Wizard for SQL Server'.

リソース	数
実行中のインスタンス	3
インスタンス (すべての状態)	3
スナップショット	0
プレイズメントグループ	0
ロードバランサー	1
Elastic IP	1
キーペア	4
セキュリティグループ	5
ボリューム	3
専有ホスト	0

# [作業]ALBのセキュリティグループ確認 3/4

- `jaws-sg-alb`という名前のALBが選択された状態で、  
説明タブの下の方を見てみてください。



ロードバランサーの作成 アクション ▼

タグや属性によるフィルター、またはキーワードによる検索

名前	DNS 名	状態	VPC ID	アベイラビリティゾーン
jaws-sg-alb	jaws-sg-alb-308871413.ap-n...	active	vpc-032d78cb399acc563	ap-northeast-1c, ap-northeast-1a

ロードバランサー: jaws-sg-alb

説明 リスナー モニタリング 統合サービス タグ

基本的な設定

名前	jaws-sg-alb
ARN	arn:aws:elasticloadbalancing:ap-northeast-1:123456789012:loadbalancer/app/jaws-sg-alb/54baa63618002dba
DNS 名	jaws-sg-alb-308871413.ap-northeast-1.amazonaws.com (A レコード)

# [作業]ALBのセキュリティグループ確認 4/4

- `jaws-sg-alb`には`default`という名前のセキュリティグループが付いています
- これは、`private-ec2-a`に付いていたものと同じセキュリティグループです

## セキュリティ

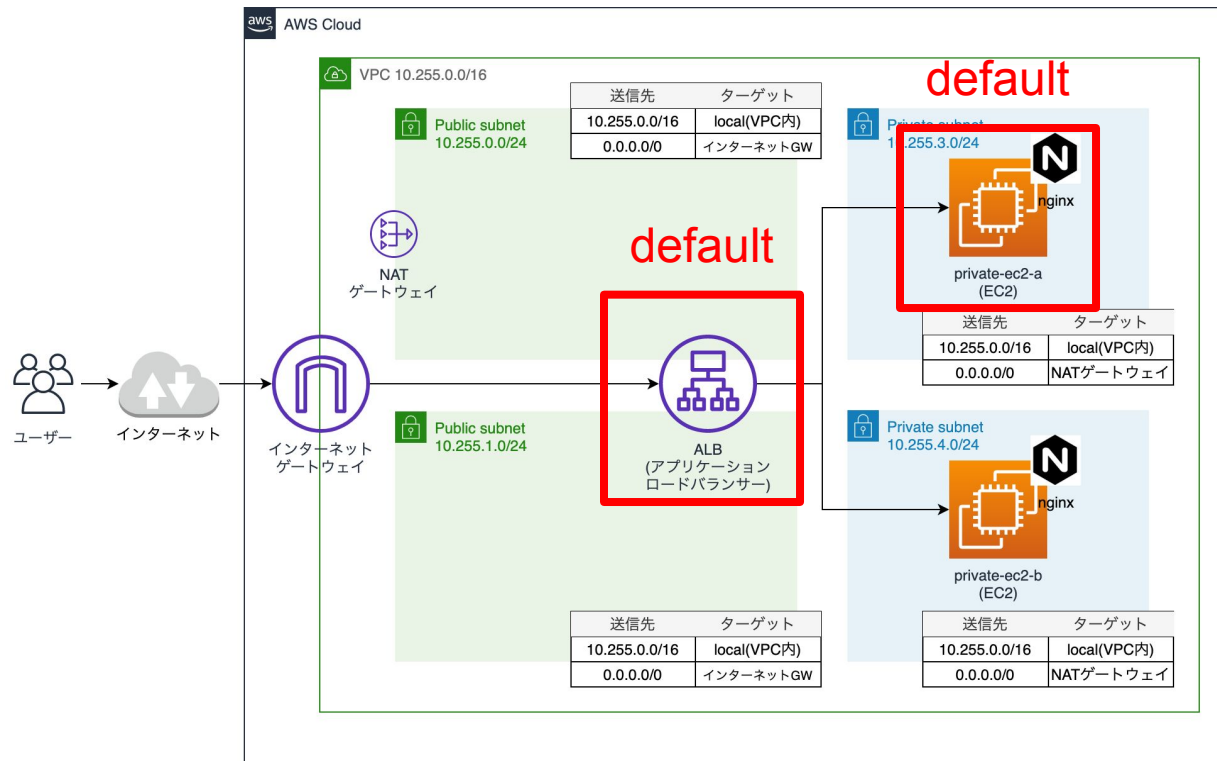
### セキュリティグループ

`sg-0146d4b24939266d5`, **default**  
• default VPC security group

`sg-025534746c6ba10c8`, **jaws-sg-web**  
• jaws-sg-web

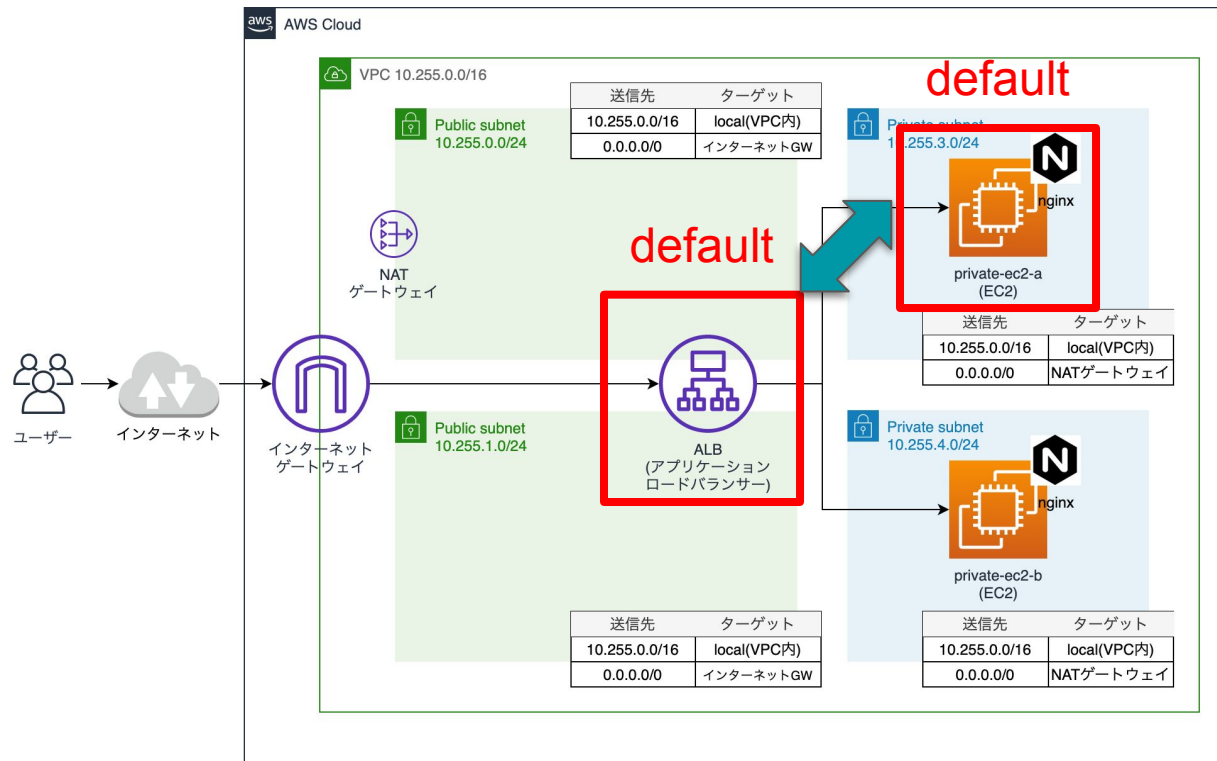
セキュリティグループの編集

# EC2とALBのセキュリティグループ解説 1/3



private-ec2-aと、ALBには、同じセキュリティグループが付けられていました。

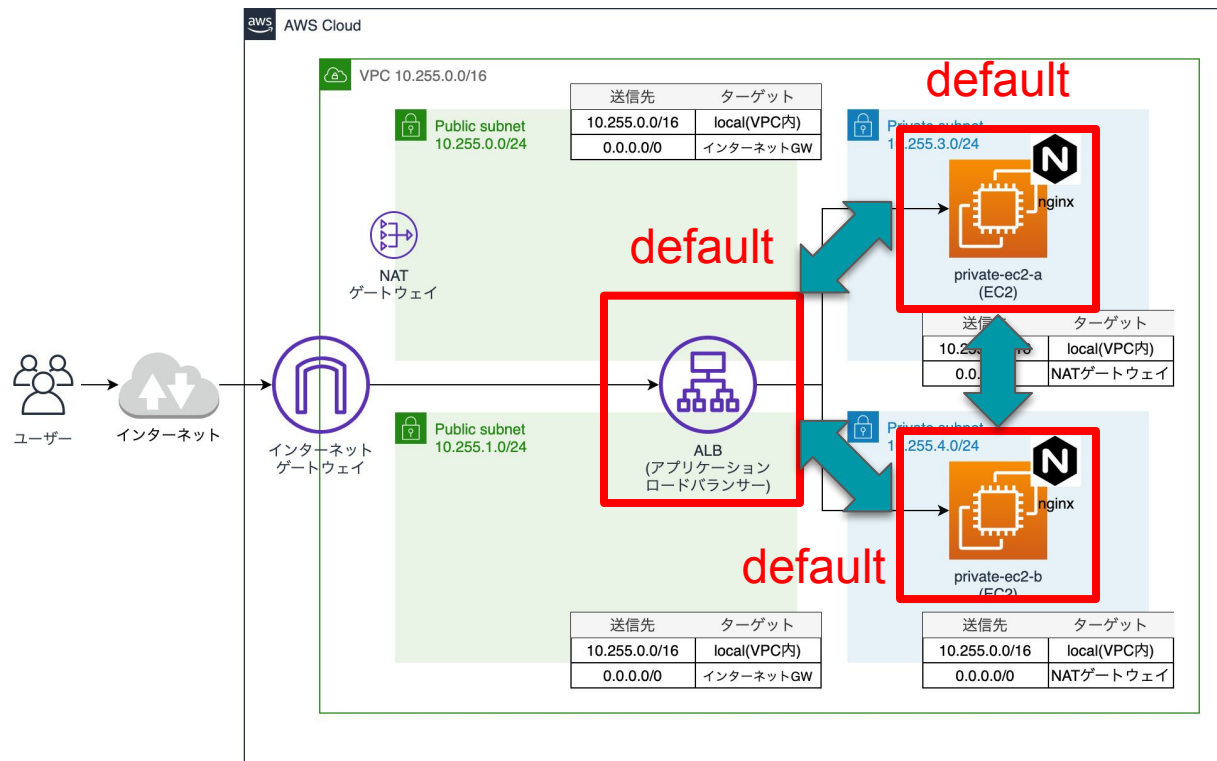
# EC2とALBのセキュリティグループ解説 2/3



そして、このセキュリティグループは、アクセス許可元として自分自身のセキュリティグループIDが指定されています。

つまり、private-ec2-aとALBは相互に通信が可能となっています。

# EC2とALBのセキュリティグループ解説 3/3



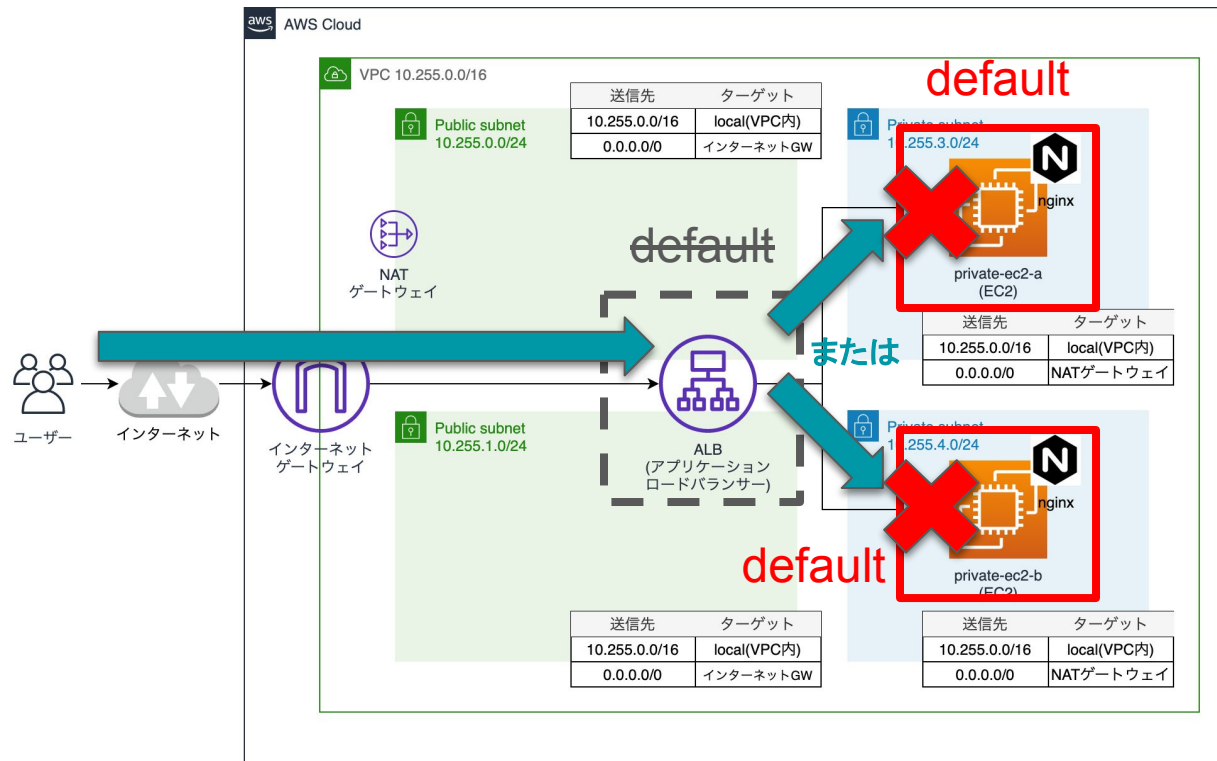
ちなみにprivate-ec2-bにも同じセキュリティグループが付けられています。

よって、VPC内のリソースは相互に通信可能となっています(AWSのデフォルト設定)。



本当にそうなのか確認してみる

# ケース3 後編

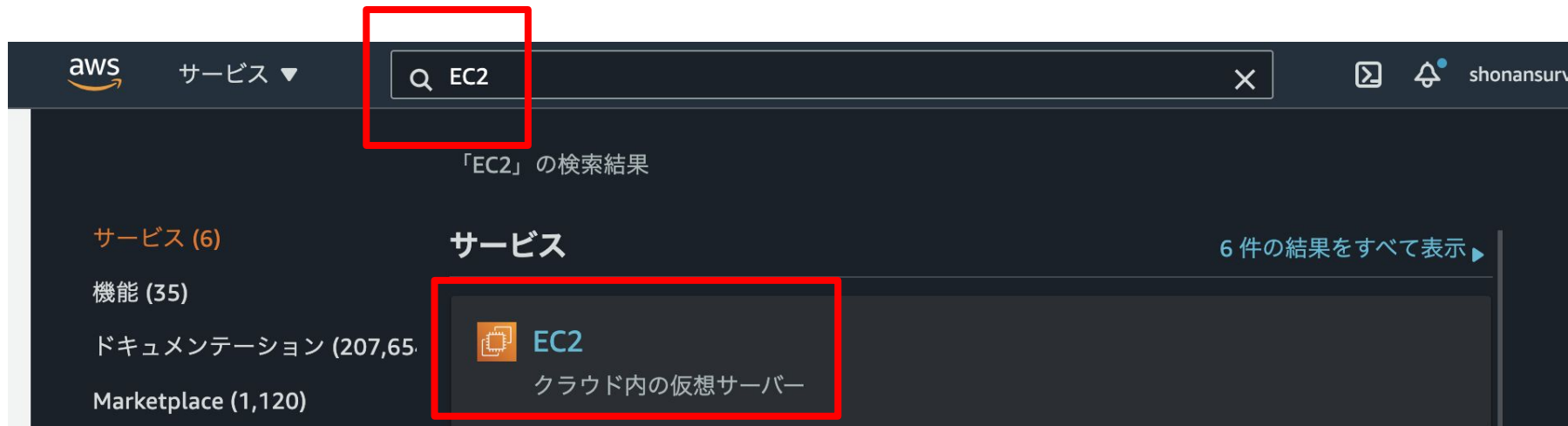


ALBに付けられている  
defaultのセキュリティグ  
ループを外してみます。

すると、EC2はALBからの  
通信を受け付けず、「Hello  
JAWS!」が表示されなくな  
るはずです。

# [作業]セキュリティグループを外す 1/4

- マネコンの検索欄にEC2と入力し、EC2を選んでください  
(ALBはEC2の画面に存在します)。



# [作業]セキュリティグループを外す 2/4

1. 左側のメニューの上部のEC2ダッシュボードを押してください
2. 次にロードバランサーを選択してください

The screenshot shows the AWS Management Console interface. On the left, the navigation menu is visible with the 'EC2 ダッシュボード' (EC2 Dashboard) item highlighted with a red box. The main content area displays the 'リソース' (Resources) page, which lists various EC2 resources. The 'ロードバランサー' (Load Balancer) item is highlighted with a red box. The resources listed are:

Resource	Count
実行中のインスタンス	3
インスタンス (すべての状態)	3
スナップショット	0
プレースメントグループ	0
ロードバランサー	1
Elastic IP	1
キーペア	4
セキュリティグループ	5
ボリューム	3
専用ホスト	0

# [作業]セキュリティグループを外す 3/4

- `jaws-sg-alb`という名前のALBが選択された状態で、アクションボタンを押し、セキュリティグループの編集を選択してください



# [作業]セキュリティグループを外す 4/4

1. defaultのチェックボックスのチェックを外してください
2. 次に保存ボタンを選択してください

セキュリティグループの編集

Select security groups to associate with your load balancer.

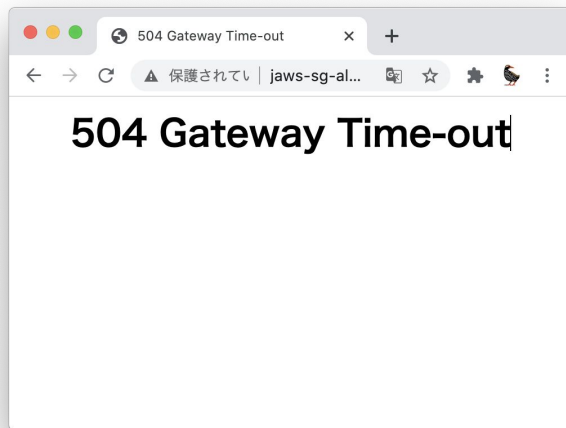
<input type="checkbox"/>	セキュリティグループ	名前	説明
<input type="checkbox"/>	sg-0146d4b249392...	default	default VPC security group
<input checked="" type="checkbox"/>	sg-025534746c6ba...	jaws-sg-web	jaws-sg-web

キャンセル 保存

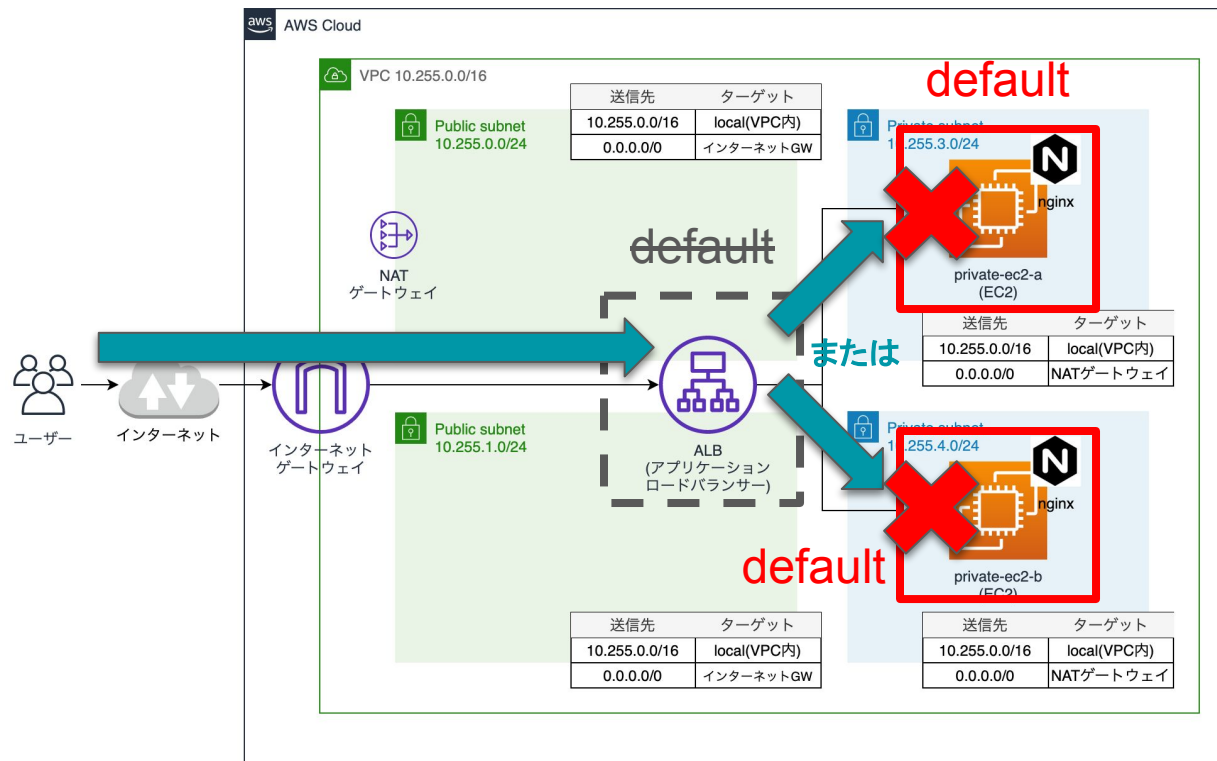
# [作業]ALBにアクセスする

---

- ブラウザでALBのDNS名 + /jaws.htmlにアクセスしてください
  - 例 : `jaws-sg-alb-0123456789.ap-northeast-1.elb.amazonaws.com/jaws.html`
- 「Hello JAWS!」が表示されなければ、想定通りです



# アクセスできない理由



ALBに付けられている  
defaultのセキュリティグ  
ループを外したことで、  
EC2はALBからの通信を  
受け付けず、  
「Hello JAWS!」が表示され  
なくなりました。



ケース3 終了

# ハンズオン全体まとめ

---

- セキュリティグループは、仮想のファイアウォール機能
- インバウンドルールにおいて、アクセスを許可する通信を指定できる
- タイプ欄では許可する通信の種類を指定する
  - HTTPと指定すればHTTPを許可
  - すべてのトラフィックと指定すれば全ての通信種類を許可
- ソース欄では許可する通信元を指定する
  - 0.0.0.0/0と指定すれば、インターネットなどVPC外からの通信を許可
  - xxx.xxx.xxx.xxx/32と指定すれば、IPアドレスxxx.xxx.xxx.xxxからの通信を許可
  - セキュリティグループIDを指定すれば、そのセキュリティグループが付けられた他のリソースからの通信を許可

ハンズオン用環境を削除する

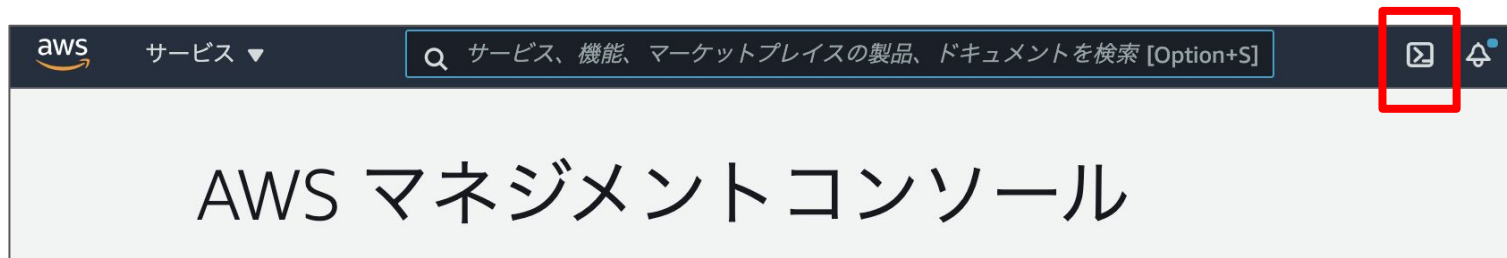
# ハンズオン用環境削除の流れ

---

1. CloudShellの起動
2. CloudFormation(以下、CFn)で構築した環境の削除の開始
3. セキュリティグループ `jaws-sg-web` の削除
4. CFnで構築した環境が削除されたことを確認

# [作業]CFnで構築した環境の削除開始

- (もしCloudShellの画面を閉じていたら)CloudShellの起動
  - 画面右上に表示されている、以下のマークをクリックし、CloudShellを起動してください

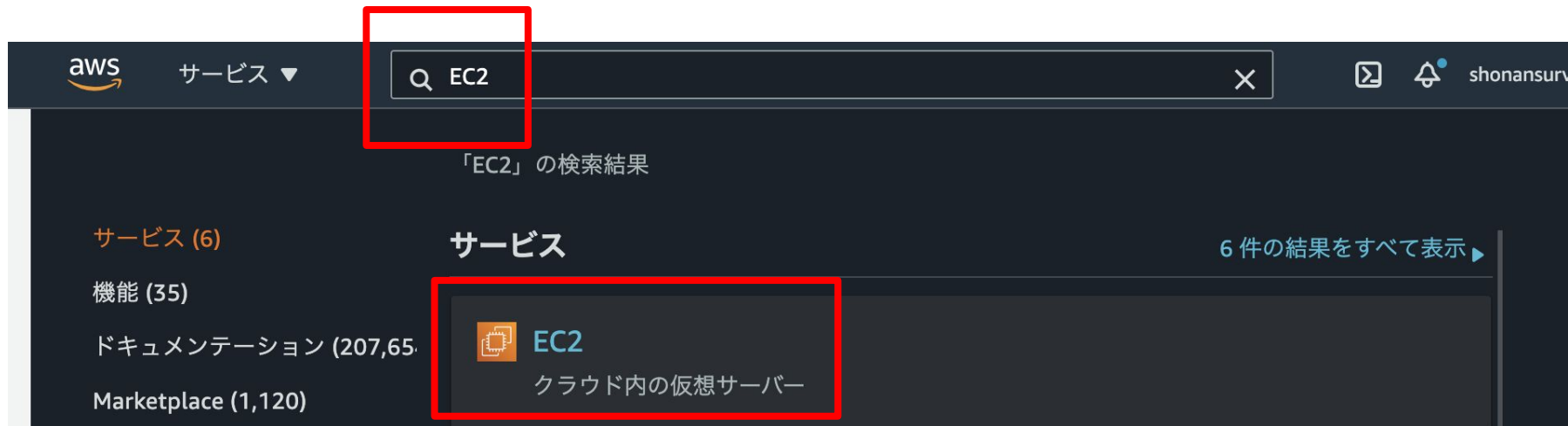


- CloudShellの画面に以下コマンドを貼り付けてエンターキーを押してください

```
aws cloudformation delete-stack --stack-name jaws-sg
```

# [作業]セキュリティグループを削除する 1/4

- マネコンの検索欄にEC2と入力し、EC2を選んでください  
(セキュリティグループはEC2またはVPCの画面で作成できます)。



# [作業]セキュリティグループを削除する 2/4

- EC2ダッシュボード画面から、**セキュリティグループ**を選択してください。

The screenshot shows the AWS Management Console EC2 Dashboard. The left sidebar contains navigation links: 'New EC2 Experience', 'EC2 ダッシュボード', 'イベント', 'タグ', '制限', '▼ インスタンス', 'インスタンス', 'インスタンスタイプ', 'テンプレートの起動', 'スポットリクエスト', 'Savings Plans', 'リザーブドインスタンス', '専有ホスト', and 'キャパシティの予約'. The main content area is titled 'リソース' (Resources) and shows a summary of EC2 resources in the 'ap-northeast-1' region. A table lists the following resources and their counts:

Resource	Count
実行中のインスタンス	3
インスタンス (すべての状態)	3
スナップショット	0
プレースメントグループ	0
ロードバランサー	1
Elastic IP	1
キーペア	4
<b>セキュリティグループ</b>	<b>5</b>
ボリューム	3
専有ホスト	0

The 'セキュリティグループ' row is highlighted with a red box. Below the table, there is a notification about the 'AWS Launch Wizard for SQL Server'.

# [作業]セキュリティグループを削除する 3/4

- `jaws-sg-web`のチェックボックスにチェックを入れてください
- 右上のアクションを押し、下の方にあるセキュリティグループを削除を選択してください

セキュリティグループ (1/3) 情報

Q セキュリティグループをフィルタリング

	Name	セキュリティグループ...	セキュリティグループ名	
<input type="checkbox"/>	-	sg-0146d4b24939266d5	default	
<input checked="" type="checkbox"/>	-	sg-025534746c6ba10c8	jaws-sg-web	
<input type="checkbox"/>	-	sg-036c4aa666b453b39	default	

アクション

- タグを管理
- 古いルールを管理
- 新しいセキュリティグループにコピー
- セキュリティグループを削除



# [作業]セキュリティグループを削除する 4/4

- 以下の画面が表示されたら、削除ボタンを選択してください。

セキュリティグループを削除

×

このセキュリティグループを削除してよろしいですか?

- sg-025534746c6ba10c8 - jaws-sg-web

キャンセル

削除

(もしこのような画面が表示されない場合は、数秒待ってから前のページの手順をもう一度試してみてください)

# [作業]CFn構築環境が削除されたことを確認

---

- CloudShellの画面に以下コマンドを貼り付けてエンターキーを押してください

```
aws cloudformation describe-stacks --stack-name jaws-sg
```

- 以下のようにjaws-sg does not existと表示されれば削除は成功しています

```
An error occurred (ValidationError) when calling the DescribeStacks operation: Stack with id jaws-sg does not exist
```

お疲れさまでした！