

# VPCエンドポイントを試してみた

AWS, EC2, IAM, vpc

vpcエンドポイントのハンズオンを体験したので、概要と作成方法の記録です。

勉強途中のため一部理解が追いついていない部分がありますが、ご了承ください。

## vpcエンドポイントとは

---

vpcエンドポイントは、グローバルIPを持つAWSサービスに対して、vpc内から直接アクセスするための出口のこと。

オンプレだと、専用線で自社サーバと、別地域のサーバやストレージを接続するイメージです。(うん百万かかるのに・・・)

今回は、プライベートサブネット内のインスタンスから、S3へ直接アクセスするための、vpcエンドポイントを作成します。

以下の順に進んでいきますので、よろしくお願いいたします。  
す。

間違っている箇所があればコメントで教えていただけると大変助かります🙏

- 利用環境
- S3の作成
- IAMロールの作成・インスタンスへ割当
- VPCエンドポイントの作成・設定
- 動作確認
- VPCエンドポイントを使用しない場合のS3接続方法
- VPCエンドポイント諸々

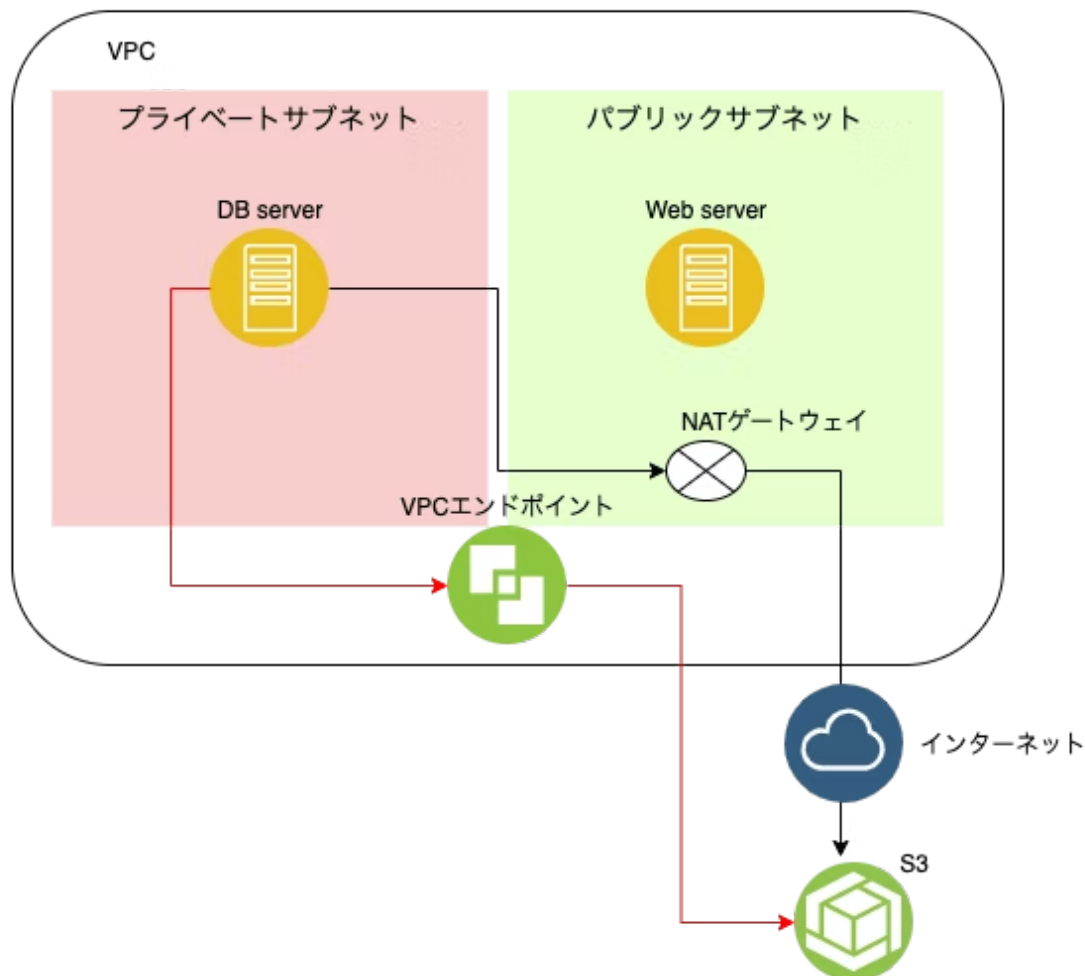
## 利用環境

---

今までに作成したVPCやサブネット、インスタンスをそのまま利用しました。

下図の赤線ルートでS3へアクセスできることが目的です。(黒線はVPCエンドポイントを使用しない場合のアクセス例)

## VPCエンドポイント作成



## S3の作成

今までS3は作成してこなかったため、最初にS3の作成を行います。

AWSマネジメントコンソールから「S3」と検索し、「S3マネジメントコンソール」に移動します。

# AWS マネジメントコンソール

## AWS のサービス

### サービスを検索する

名称、キーワード、頭文字を入力できます。

✕

#### S3

クラウド内のスケーラブルなストレージ

#### S3 Glacier

クラウド内のアーカイブストレージ

#### AWS Snow Family

大容量データの転送

#### AWS Transfer Family

SFTP、FTPS、FTP の完全マネージド型サポート

#### Athena

SQL を使用した [S3](#) でのデータクエリ

#### Amazon Transcribe

強力な音声認識

S3 マネジメントコンソールに移動したら、「バケットの作成」を選択します。

私はいくつかバケットを作成しているのでバケット名が表示されていますが、初回であれば何も表示されません。

Amazon S3

バケット

バッチオペレーション

S3 のアクセスアナライザー

ブロックパブリックアクセス (アカウント設定)

注目機能 2

S3 ストレージクラスを効果的に使用方法について説明します。詳細情報 »

ドキュメント

S3 コンソールのこのバージョンは一時的に復元されていますが、新しい S3 コンソールエクスペリエンスは今後も改善していきます。

S3 バケット

コンソールのご紹介

Q バケット検索

すべてのアクセスタイプ

+ バケットを作成する

パブリックアクセス設定を編集する

空にする

削除

2 バケット

1 リージョン

バケット名	アクセス	リージョン	作成日
<input type="checkbox"/> connect-3dab0aa33890	オブジェクトは公開可能	アジアパシフィック (東京)	6月 25, 2020 11:54:50 午後 GMT+0900
<input type="checkbox"/> vpc20200907	バケットとオブジェクトは非公開	アジアパシフィック (東京)	9月 7, 2020 8:53:53 午後 GMT+0900

S3バケットに名前をつけたら、今回は他に設定をしないので「作成」を選択します。

S3バケット名は一意的な値である必要があるため、日付等を名前の後に付与すると良いようです。

バケットの作成

① 名前とリージョン    ② オプションの設定    ③ アクセス許可の設定    ④ 確認

名前とリージョン

バケット名 ⓘ

vpc20200915

リージョン

アジアパシフィック (東京)

既存のバケットから設定をコピー

バケットを選択する (省略可) 2 バケット

作成    キャンセル    次へ

# IAMロールの作成・インスタンスの割当

続いて、インスタンスがS3へアクセスするためのIAMロールを作成します。

(S3を作成しただけでは使えません!!まずはインスタンスがS3へアクセスできるよう権限設定をします)

AWS マネジメントコンソールから「IAM」と検索し、「IAM マネジメントコンソール」に移動します。

IAM マネジメントコンソールの左ペイン、「ロール」を選択し、「ロールの作成」を選択します。



ユースケースは「EC2」を選択し「次のステップ」を選択します。

## ロールの作成

1

2

3

4

### 信頼されたエンティティの種類を選択

**AWS サービス**

EC2、Lambda、およびその他

**別の AWS アカウント**

お客様またはサードパーティーに属しています

**ウェブ ID**

Cognito または任意の OpenID プロバイダ

**SAML 2.0 フェデレーション**

企業ディレクトリ

AWS のサービスによるアクションの代行を許可します。 [詳細はこちら](#)

### ユースケースの選択

**一般的なユースケース****EC2**

Allows EC2 instances to call AWS services on your behalf.

**Lambda**

Allows Lambda functions to call AWS services on your behalf.

または、サービスを選択してユースケースを表示します

[API Gateway](#)[CodeDeploy](#)[EMR](#)[KMS](#)[Rekognition](#)[AWS Backup](#)[CodeGuru](#)[ElastiCache](#)[Kinesis](#)[RoboMaker](#)[AWS Chatbot](#)[CodeStar Notifications](#)[Elastic Beanstalk](#)[Lake Formation](#)[S3](#)[AWS Marketplace](#)[Comprehend](#)[Elastic Container Service](#)[Lambda](#)[SMS](#)[AWS Support](#)[Config](#)[Elastic Transcoder](#)[Lex](#)[SNS](#)[Amplify](#)[Connect](#)[ElasticLoadBalancing](#)[License Manager](#)[SWF](#)

\* 必須

[キャンセル](#)[次のステップ: アクセス権限](#)

「AmazonS3FullAccess」を選択し、「次のステップ」を選択します。

※ 「ポリシーのフィルタ」で「S3」を入力すると良きです。



## ロールの作成

1

2

3

4

### ▼ Attach アクセス権限ポリシー

新しいロールにアタッチするポリシーを 1 つ以上選択します。

ポリシーの作成



ポリシーのフィルタ ▼

Q S3

5 件の結果を表示中

	ポリシー名 ▼	次として使用
<input type="checkbox"/>	▶ AmazonDMSRedshiftS3Role	なし
<input checked="" type="checkbox"/>	▶ AmazonS3FullAccess	Permissions policy (1)
<input type="checkbox"/>	▶ AmazonS3ReadOnlyAccess	なし
<input type="checkbox"/>	▶ Batch-S3	Permissions policy (1)
<input type="checkbox"/>	▶ QuickSightAccessForS3StorageManagementAnalyticsReadOnly	なし

### ▶ アクセス権限の境界の設定

\* 必須

キャンセル

戻る

次のステップ: タグ

設定しなくても大丈夫ですが、「Name」キーの設定を行いました。

## ロールの作成

1

2

3

4

### タグの追加 (オプション)

IAM タグは、ロール に追加できるキーと値のペアです。タグには、E メールアドレスなどのユーザー情報を含めるか、役職などの説明文とすることができます。タグを使用して、この ロール のアクセスを整理、追跡、制御できます。 [詳細はこちら](#)

キー	値 (オプション)	削除
Name	vpc_to_S3	×
新しいキーを追加		

さらに 49 個のタグを追加できます。

キャンセル

戻る

次のステップ: 確認

「ロール名」、「ロールの説明」を入力し、「ロールの作成」を選択します。

※ロール名は先ほどの「Name」キーと同様の値にしています。ロールの説明は適当でも大丈夫です。

## ロールの作成

1

2

3

4

### 確認

以下に必要な情報を指定してこのロールを見直してから、作成してください。

ロール名\* vpc\_to\_s3

英数字と「+','=','@-」を使用します。最大 64 文字。

ロールの説明 vpc\_to\_s3

最大 1000 文字。英数字と「+','=','@-」を使用します。

信頼されたエンティティ AWS のサービス: ec2.amazonaws.com

ポリシー  AmazonS3FullAccess [外部リンク](#)

アクセス権限の境界 アクセス権限の境界が設定されていません

新しい ロール は次のタグを受け取ります

キー	値
Name	vpc_to_S3

\* 必須

キャンセル

戻る

ロールの作成

ここまでで、S3へのアクセス権を持った、IAMロールの完成です。

続けて、作成したIAMロールをインスタンスへ割り当てます。

「EC2マネジメントコンソール」に移動して、インスタンスを選択後、「アクション」、「インスタンスの設定」、「IAMロールの割り当て/置換」を選択します。

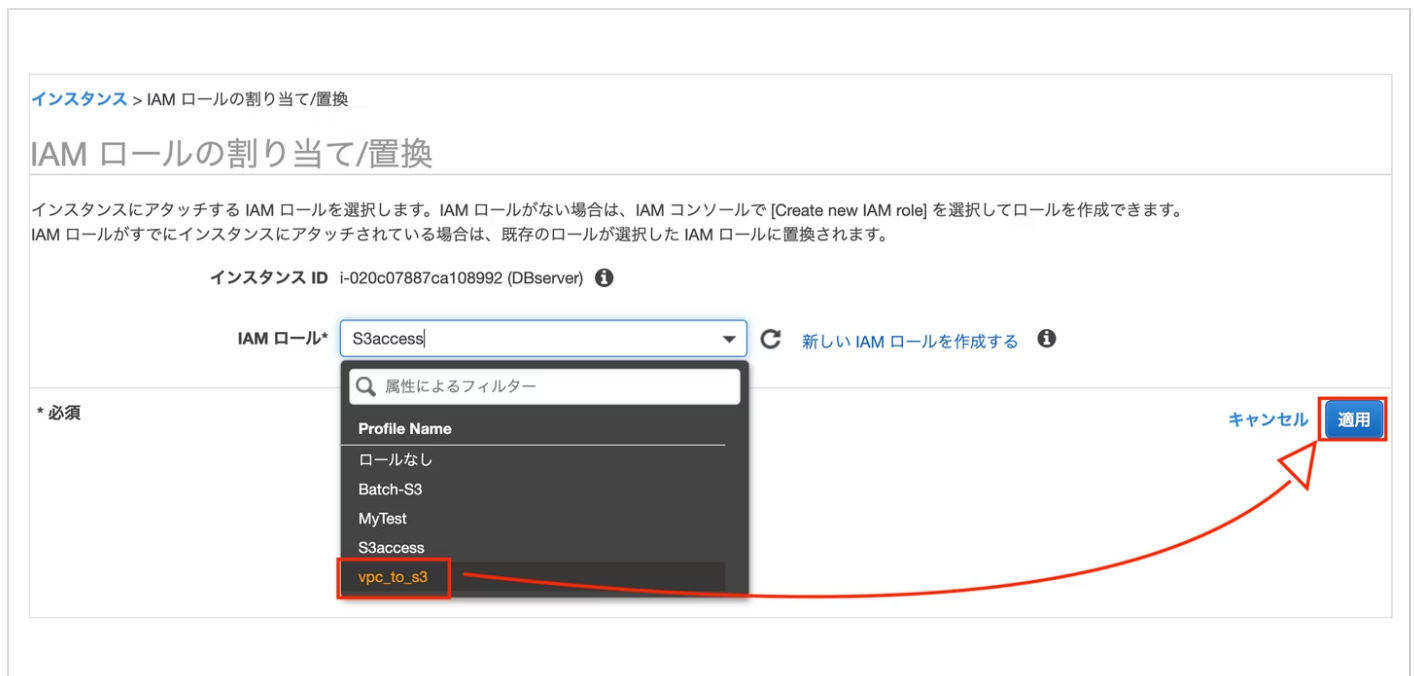
なお、インスタンスが停止していると割り当てに失敗しますので、起動状態をお願いします。

下の画面はインスタンスが停止しているので、この後失敗します。

The screenshot shows the AWS Management Console interface for the 'New EC2 Experience'. On the left, there is a navigation menu with sections like 'EC2 ダッシュボード', 'イベント', 'タグ', '制限', 'インスタンス', 'イメージ', and 'Elastic Block Store'. The main area displays a list of EC2 instances. Two instances are visible: 'DBserver' (ID: i-020c07887ca108992) and 'Webserver' (ID: i-093b66c62...). The 'DBserver' instance is selected, and its details are shown below. The 'Actions' menu is open, and the 'IAM role assignment/swap' option is highlighted. The instance details show it is in a 'stopped' state.

説明	ステータスチェック	モニタリング	タグ
インスタンス ID	i-020c07887ca108992		
インスタンスの状態	stopped		
インスタンスタイプ	t2.micro		
検索中	推奨事項については、AWS Compute Optimizer に最適化してください。 <a href="#">詳細はこちら</a>		
プライベート DNS	ip-10-0-2-10.ap-northeast-1.compute.internal		
プライベート IP	10.0.2.10		
セカンダリプライベート IP			
VPC ID	vpc-07ac761ab7e4c6a1b (VPC_AREA)		
アベイラビリティゾーン	ap-northeast-1d		
セキュリティグループ	DB-SG. インバウンドルールの表示、アウトバウンドルールの表示		
予定されているイベント	-		
AMI ID	amzn2-ami-hvm-2.0.20200406.0-x86_64-gp2 (ami-0f310fed6141e627)		

先ほど作成したロールを選択して、「適用」を選択します。



これでIAMロールに準じたアクセス権限がインスタンスにされたことになります。

今回は、「AmazonS3FullAccess」がインスタンスに付与されたことになります。

また、プライベートサブネット内のインスタンスに割り当てたので、VPCエンドポイントもNATゲートウェイもない今の状態では、S3へは接続できません。

実際にプライベートサブネット内のインスタンスに接続して確認してみます。

```
# 自分のPCから
$ ssh ec2-user@18.177.121.50 -i my-key.pem
```

```
# パブリックサブネットのインスタンスから
[ec2-user@10.0.1.10 ~]$ ssh ec2-user@10.0.2.10 -i DBserver

# プライベートサブネットのインスタンスから
[ec2-user@10.0.2.10 ~]$ aws s3 ls
```

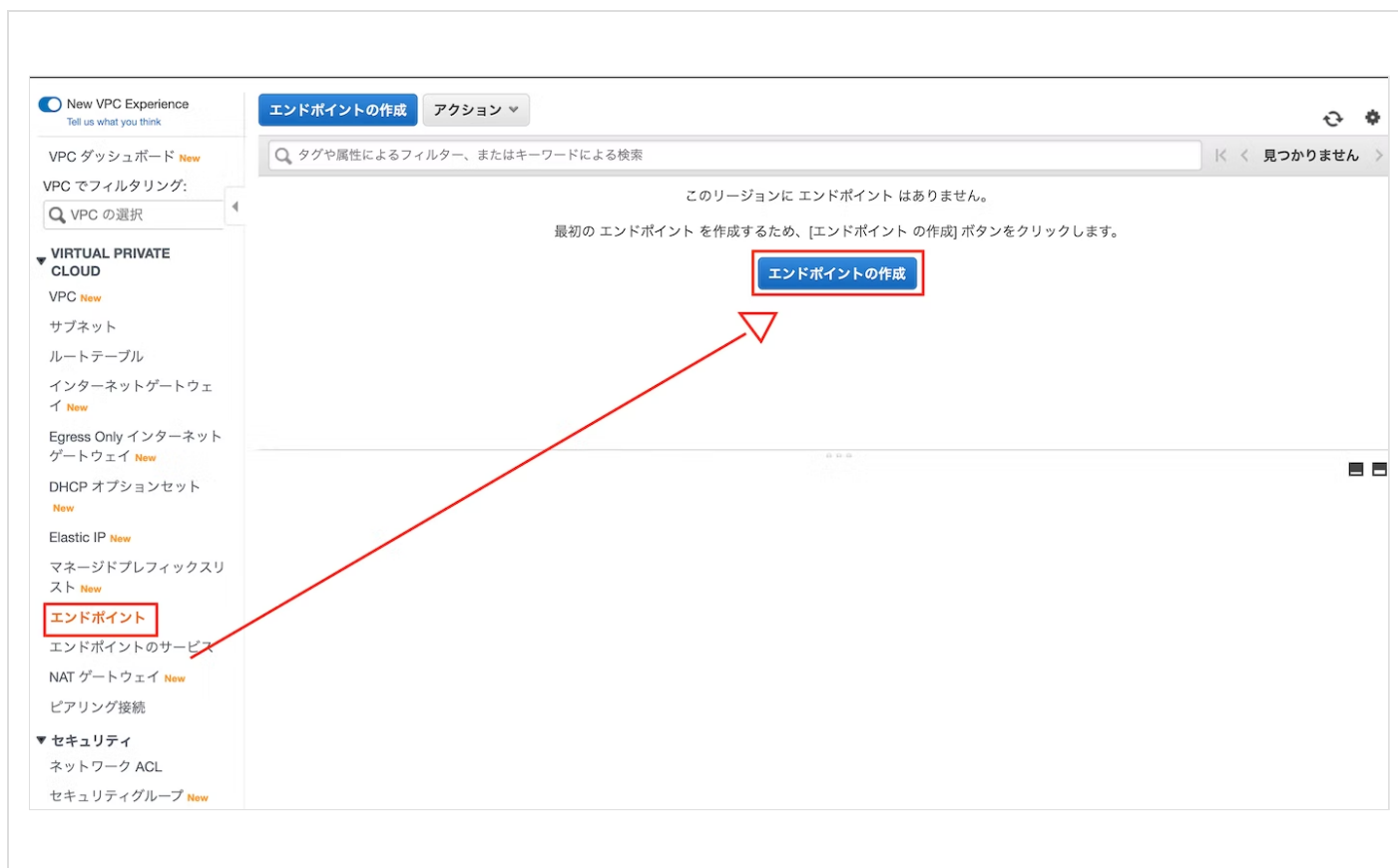
下図のようにプロンプトが戻ってきませんので、「Ctrl」＋「C」でAbortしましょう。

```
https://aws.amazon.com/amazon-linux-2/
26 package(s) needed for security, out of 62 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-2-10 ~]$
[ec2-user@ip-10-0-2-10 ~]$
[ec2-user@ip-10-0-2-10 ~]$
[ec2-user@ip-10-0-2-10 ~]$
[ec2-user@ip-10-0-2-10 ~]$ aws s3 ls
```

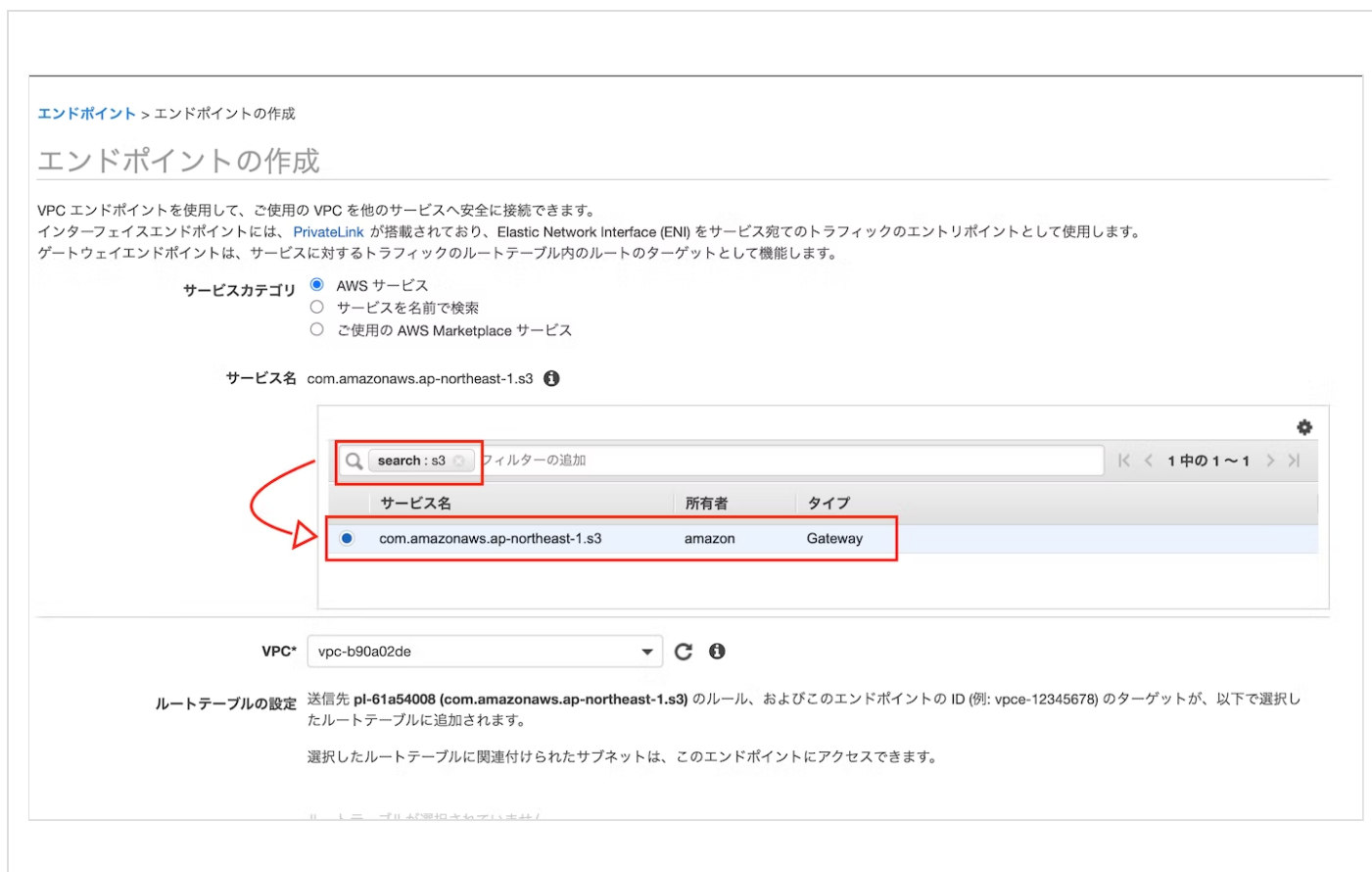
## VPCエンドポイントの作成・設定

続いてVPCエンドポイントを作成します。

VPCダッシュボードから、左ペインの「エンドポイント」を選択します。



「S3」でフィルタをかけて、表示されたサービスを選択します。



vpcは自身で作成したvpcを選択します。

サービス名 com.amazonaws.ap-northeast-1.s3 ⓘ

search : s3 ⓘ フィルターの追加

1 中の 1 ~ 1

サービス名	所有者	タイプ
com.amazonaws.ap-northeast-1.s3	amazon	Gateway

VPC\* vpc-07ac761ab7e4c6a1b ⓘ

ルートテーブルの設定

属性によるフィルター

vpc-b90a02de 172.31.0.0/16 available

vpc-07ac761ab7e4c6a1b 10.0.0.0/16 available VPC\_AREA

エンドポイントの ID (例: vpce-12345678) のターゲットが、以下で選択し  
アクセスできます。

ルートテーブルが選択されていません

ルートテーブル ID	メイン	関連付け
<input type="checkbox"/> rtb-05911150181fdb651	はい	subnet-0afe725925c5ec288   Private_Subnet
<input type="checkbox"/> rtb-09e407f82169416e7	いいえ	subnet-06b4eab6bc3cdf0b3   Public_Subnet

プライベートサブネットに属しているルートテーブルを選択  
します。



ルートテーブルの設定 送信先 **pl-61a54008 (com.amazonaws.ap-northeast-1.s3)** のルール、およびこのエンドポイントの ID (例: vpce-12345678) のターゲットが、以下で選択したルートテーブルに追加されます。

選択したルートテーブルに関連付けられたサブネットは、このエンドポイントにアクセスできます。

rtb-05911150181fdb651

	ルートテーブル ID	メイン	関連付け
<input checked="" type="checkbox"/>	rtb-05911150181fdb651	はい	subnet-0afe725925c5ec288   Private_Subnet
<input type="checkbox"/>	rtb-09e407f82169416e7	いいえ	subnet-06b4eab6bc3cdf0b3   Public_Subnet



#### 警告

エンドポイントを使用する場合、同じリージョンの AWS のサービスにアクセスするために影響を受けるサブネットのインスタンスからのソース IP アドレスは、パブリック IP アドレスではなくプライベート IP アドレスになります。パブリック IP アドレスを使用した、影響を受けるサブネットから AWS のサービスへの既存の接続は、切断される可能性があります。エンドポイントを作成または変更する場合は、重要なタスクが実行中でないことを確認してください。

#### ポリシー\*

- ☒ フルアクセス - VPC 内のすべてのユーザーまたはサービスが、どの AWS アカウントの認証情報を使用しても、この AWS のサービスのすべてのリソースへアクセスすることが可能です。アクセスを可能にするためには、すべてのポリシー (IAM ユーザーポリシー、VPC エンドポイントポリシー、AWS のサービス特有のポリシー (例: Amazon S3 バケットポリシー、S3 ACL ポリシー など)) が、必要な権限を付与する必要があります。

- ☐ カスタム

ポリシーを生成するには、[ポリシー作成ツール](#)を使い、作成されたポリシーを以下に貼り付けてください。

```
{
  "Statement": [
```

ポリシーは変更せず、「エンドポイントの作成」をすると完成です！！

先ほどと同様の手順で確認をしてみると。。。。

```
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-1-10 ~]$ ssh ec2-user@10.0.2.10 -i DBserver.pem
Last login: Thu Sep 17 11:26:03 2020 from 10.0.1.10

  _ _| _ _| _ )
 _| ( _ _ /   Amazon Linux 2 AMI
---| \---|---|

https://aws.amazon.com/amazon-linux-2/
26 package(s) needed for security, out of 62 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-2-10 ~]$ aws s3 ls --region ap-northeast-1
2020-06-25 14:54:51 connect-3dab0aa33890
2020-09-10 10:47:01 vpc20200907
2020-09-15 10:20:39 vpc20200915
[ec2-user@ip-10-0-2-10 ~]$
```

「aws s3 ls」 コマンドで応答が帰ってこなかったため、以下コマンドを使用しています。

```
$ aws s3 ls --region ap-northeast-1
```

## 少し補足

---

VPCエンドポイントには2種類あり、今回使用したのは無料のGateway型です。

Privatelink型は有料だそうです。

名前	実装方法
Gateway型	エンドポイントポリシーをルートテーブルに設定することで直接アクセスする
Privatelink型	サブネットがエンドポイント用のIPを持ち、それをDNSが名前解決することでルーティングする

## 参考文献

---

- [これだけでOK！AWS 認定ソリューションアーキテクト – アソシエイト試験突破講座（SAA-C02試験対応版](#)

- そのトラフィック、NATゲートウェイを通す必要ありますか？適切な経路で不要なデータ処理料金は削減しましょう
- AWSの公式ドキュメント VPCエンドポイント

最後までお付き合いいただきありがとうございました🍵