

# AmazonConnectによる自動電話通知（7.複数連絡先への電話通知〈構築①〉）

AWS



×

ZABBIX

×



## AmazonConnectによる自動電話通知 （7.複数連絡先への電話通知〈構築①〉）

2021.11.12 2021.10.29

[【前回】 AmazonConnectによる自動電話通知（7.複数連絡先への電話通知〈概要〉）](#)[【次回】 AmazonConnectによる自動電話通知（7.複数連絡先への電話通知〈構築②〉）](#)[【簡易版】 AmazonConnectによる自動電話通知（まとめ）](#)

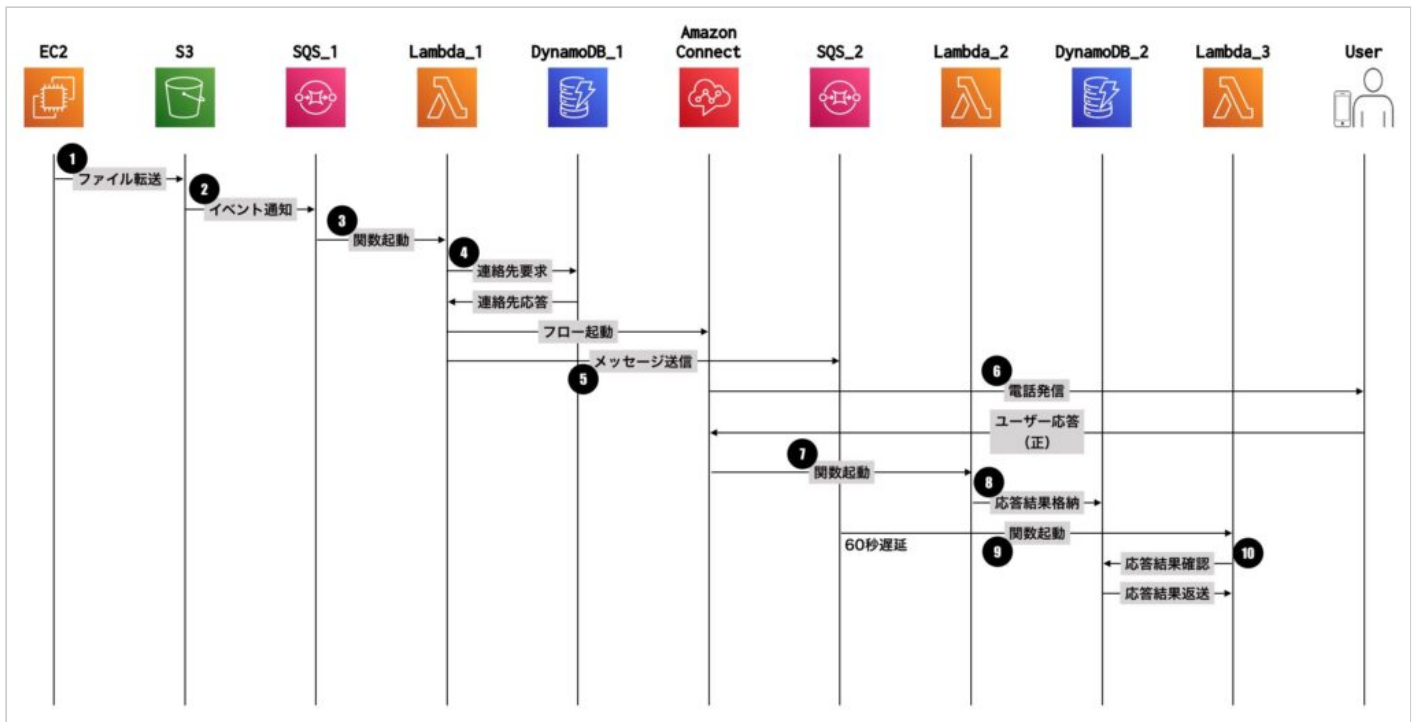
監視サーバーで障害を検知した際に、自動で電話通知できるようにしていきます。ネットワークエンジニアも利用することの多い監視サーバー(Zabbix)で障害検知し、AWS上のAmazonConnectを利用し自動電話を発信します。

今回は下記の条件を満たせるようにAWSの各サービスを利用して自動電話通知の仕組みを導入します。

- 複数の通知先を登録した連絡先リストを持たせる。
- 連絡先リストに優先度(通知順)を設定する。
- 優先度が高い人に最初に電話する。
- 応答が無かった場合、次の優先度の人に順番に電話する。
- 連絡先リストの最後まで電話しても応答が無かった場合、最初に戻って継続する。

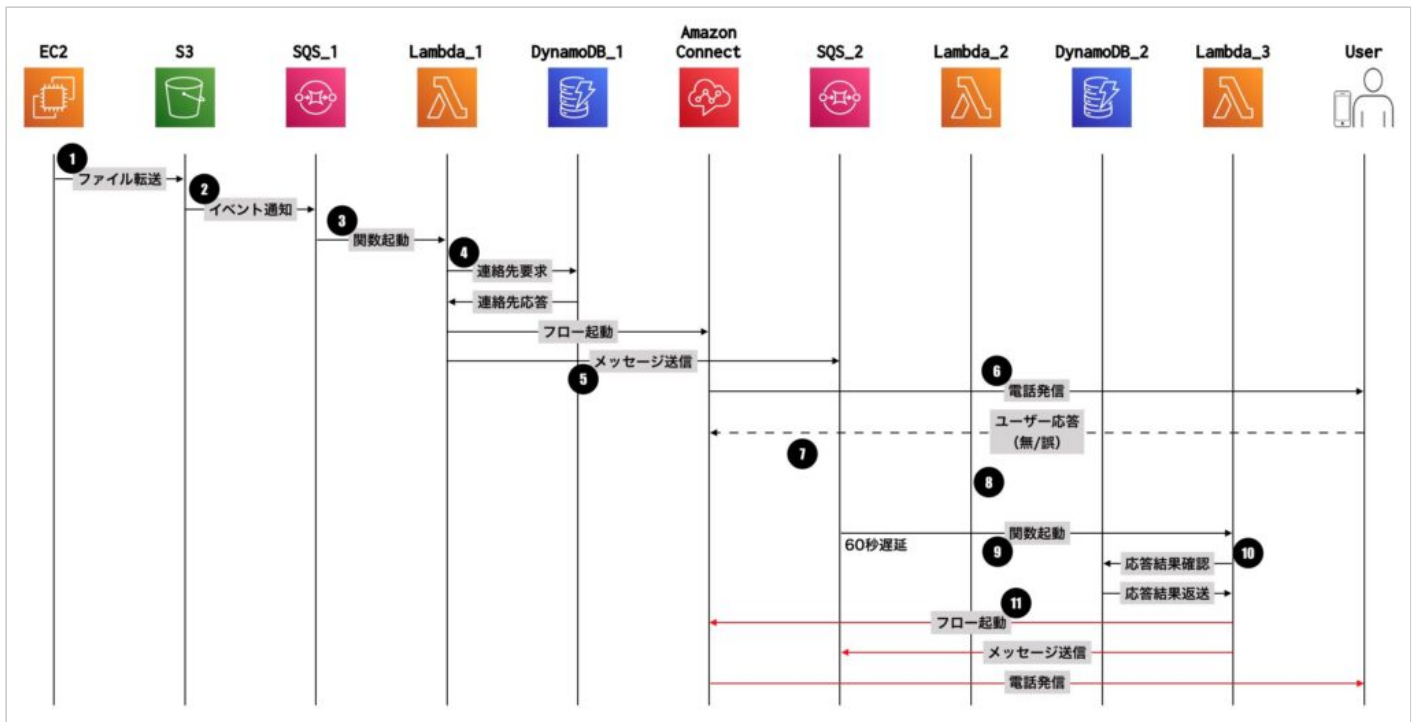
## 自動電話通知フロー

### 電話に応答した場合のフロー



1. EC2上の監視サーバーで障害を検知し、S3へトリガーファイルを格納
2. S3のイベント通知機能で、SQS\_1にメッセージを送信
3. SQS\_1をトリガーとして、Lambda\_1を起動
4. Lambda\_1がDynamoDB\_1から連絡先を取得し、AmazonConnectを起動
5. Lambda\_1がAmazonConnectを起動すると同時に、SQS\_2へメッセージを送信
6. AmazonConnectがユーザーへ自動電話通知を実施
7. ユーザーが正常応答し、AmazonConnectがLambda\_2を起動
8. Lambda\_2が応答結果をDynamoDB\_2に保存(応答OK)
9. 60秒後にSQS\_2をトリガーとしてLambda\_3を起動
10. Lambda\_3がDynamoDB\_2の応答結果を確認(正常応答しているため、何もせずに処理完了)

## 電話に応答しなかった場合のフロー



1. EC2上の監視サーバーで障害を検知し、S3へトリガーファイルを格納
2. S3のイベント通知機能で、SQS\_1にメッセージを送信
3. SQS\_1をトリガーとして、Lambda\_1を起動
4. Lambda\_1がDynamoDB\_1から連絡先を取得し、AmazonConnectを起動
5. Lambda\_1がAmazonConnectを起動すると同時に、SQS\_2へメッセージを送信
6. AmazonConnectがユーザーへ自動電話通知を実施
7. ユーザーが正常応答せず、AmazonConnectがLambda\_2を起動
8. Lambda\_2が応答結果をDynamoDB\_2に保存(応答NG)
9. 60秒後にSQS\_2をトリガーとしてLambda\_3を起動
10. Lambda\_3がDynamoDB\_2の応答結果を確認
11. 正常応答していないため、再度AmazonConnectを起動(以降、5から繰り返し)

## EC2上で監視サーバーを構築

EC2上でのZabbixの構築はこちらを参照してください。

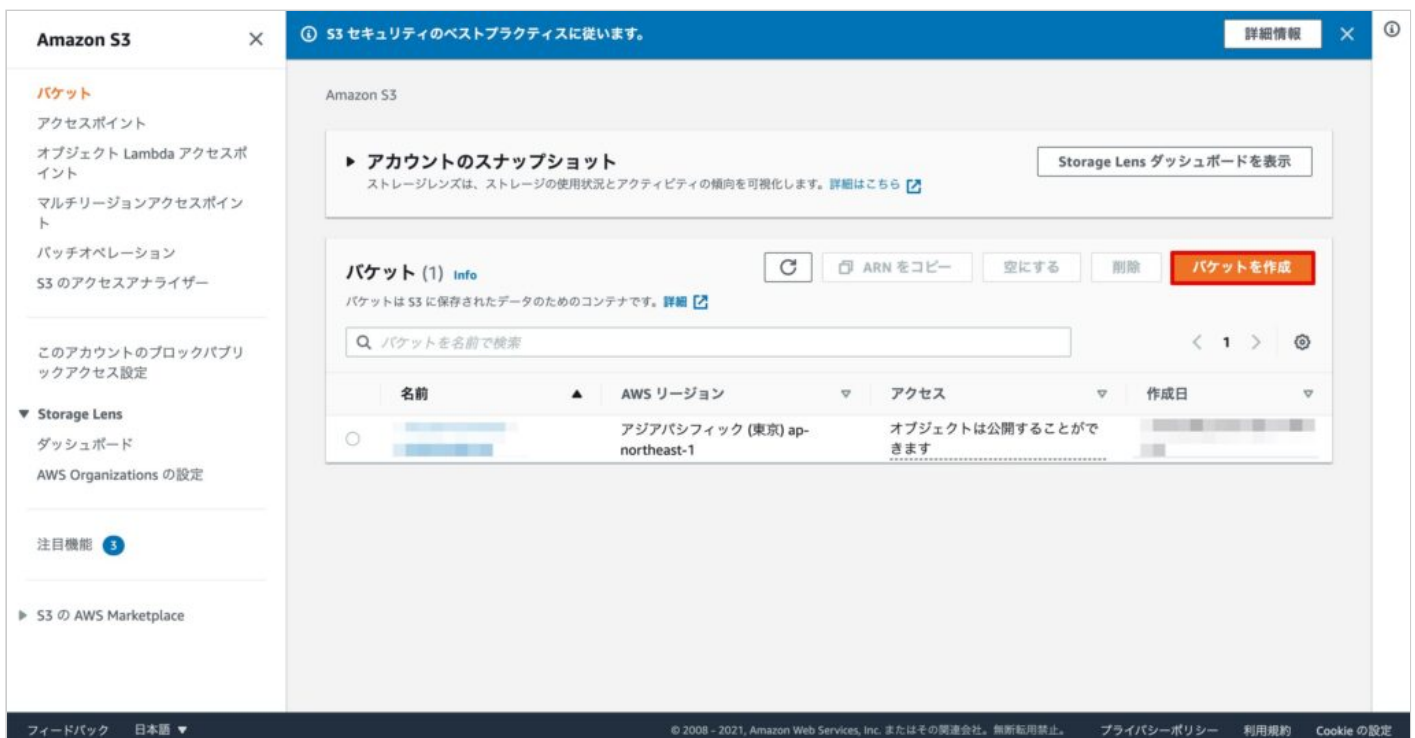
[AWS上での監視サーバー\(Zabbix\)構築](#)

## S3のバケット作成

AWSマネジメントコンソール上で、「s3」を検索します。



「バケットの作成」をクリックします。



バケット名を入力し、それ以外はデフォルトのままで、「バケットを作成」をクリックします。



## 一般的な設定

### バケット名

amazonconnect-alert-notification-bucket

バケット名は一意である必要があり、スペース、または大文字を含めることはできません。バケットの命名規則をご参照ください [🔗](#)

### AWS リージョン

アジアパシフィック (東京) ap-northeast-1

### 既存のバケットから設定をコピー - オプション

次の設定のバケット設定のみがコピーされます。

バケットを選択する

## このバケットのブロックパブリックアクセス設定

パブリックアクセスは、アクセスコントロールリスト (ACL、Access Control List)、バケットポリシー、アクセスポイントポリシー、またはそのすべてを介してバケットとオブジェクトに許可されます。このバケットとそのオブジェクトへの公開アクセスが確実にブロックされるようにするには、[パブリックアクセスをすべてブロック] を有効にします。これらの設定はこのバケットとそのアクセスポイントにのみ適用されます。AWS では [パブリックアクセスをすべてブロック] を有効にすることをお勧めしますが、これらの設定を適用する前に、アプリケーションが公開アクセスなしで正しく機能することをご確認ください。このバケットやオブジェクトへのある程度の公開アクセスが必要な場合は、各ストレージユースケースに合わせて以下にある個々の設定をカスタマイズできます。 [詳細](#) [🔗](#)

### ☒ パブリックアクセスをすべてブロック

この設定をオンにすることは、以下の 4 つの設定をすべてオンにすることと同じです。次の各設定は互いに独立しています。

- ☒ 新しいアクセスコントロールリスト (ACL) を介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする  
S3 は、新しく追加されたバケットまたはオブジェクトに適用されたパブリックアクセス許可をブロックし、既存のバケットおよびオブジェクトに対する新しいパブリックアクセス ACL が作成されないようにします。この設定では、ACL を使用して S3 リソースへのパブリックアクセスを許可する既存のアクセス許可は変更されません。
- ☒ 任意のアクセスコントロールリスト (ACL) を介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする  
S3 はバケットとオブジェクトへのパブリックアクセスを付与するすべての ACL を無視します。
- ☒ 新しいパブリックバケットポリシーまたはアクセスポイントポリシーを介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする  
S3 は、バケットとオブジェクトへのパブリックアクセスを許可する新しいバケットポリシーおよびアクセスポイントポリシーをブロックします。この設定は、S3 リソースへのパブリックアクセスを許可する既存のポリシーを変更しません。
- ☒ 任意のパブリックバケットポリシーまたはアクセスポイントポリシーを介したバケットとオブジェクトへのパブリックアクセスとクロスアカウントアクセスをブロックする  
S3 は、バケットとオブジェクトへのパブリックアクセスを付与するポリシーを使用したバケットまたはアクセスポイントへのパブリックアクセスとクロスアカウントアクセスを無視します。

## バケットのバージョンング

バージョンングは、オブジェクトの複数のバリエーションを同じバケット内に保持する手段です。バージョンングを使用すると、Amazon S3 バケットに格納されているすべてのオブジェクトのすべてのバージョンを保存、取得、復元できます。バージョンングを使用すると、意図しないユーザーアクションと意図しないアプリケーション障害の両方から簡単に復旧できます。 [詳細](#) [🔗](#)

### バケットのバージョンング

- ☒ 無効にする  
☐ 有効にする

## タグ (0) - オプション

バケットにタグ付けすることで、ストレージコストやその他の基準を追跡します。 [詳細](#) [🔗](#)

このバケットに関連付けられたタグはありません。

タグの追加



### デフォルトの暗号化

このバケットに保存された新しいオブジェクトを自動的に暗号化します。 [詳細](#)

サーバー側の暗号化

☒ 無効にする

☐ 有効にする

▶ 詳細設定

📘 バケットを作成したら、バケットにファイルとフォルダをアップロードし、追加のバケット設定を行うことができます。

キャンセル

バケットを作成

フィードバック

日本語 ▼

© 2008 - 2021, Amazon Web Services, Inc. またはそ

バケットが作成されたことを確認します。

#### Amazon S3

- バケット
- アクセスポイント
- オブジェクト Lambda アクセスポイント
- マルチリージョンアクセスポイント
- パッチオペレーション
- S3 のアクセスアナライザー
- このアカウントのブロックパブリックアクセス設定
- Storage Lens
- ダッシュボード
- AWS Organizations の設定
- 注目機能 3
- S3 の AWS Marketplace

#### Amazon S3

▶ アカウントのスナップショット

ストレージレンズは、ストレージの使用状況とアクティビティの傾向を可視化します。 [詳細はこちら](#)

Storage Lens ダッシュボードを表示

バケット (2) Info

バケットは S3 に保存されたデータのコンテナです。 [詳細](#)

🔄 📋 ARN をコピー 空にする 削除 バケットを作成

🔍 バケットを名前検索

名前	AWS リージョン	アクセス	作成日
○ [redacted]	アジアパシフィック (東京) ap-northeast-1	オブジェクトは公開することができます	[redacted]
○ amazonconnect-alert-notification-bucket	アジアパシフィック (東京) ap-northeast-1	非公開のバケットとオブジェクト	[redacted]

フィードバック

日本語 ▼

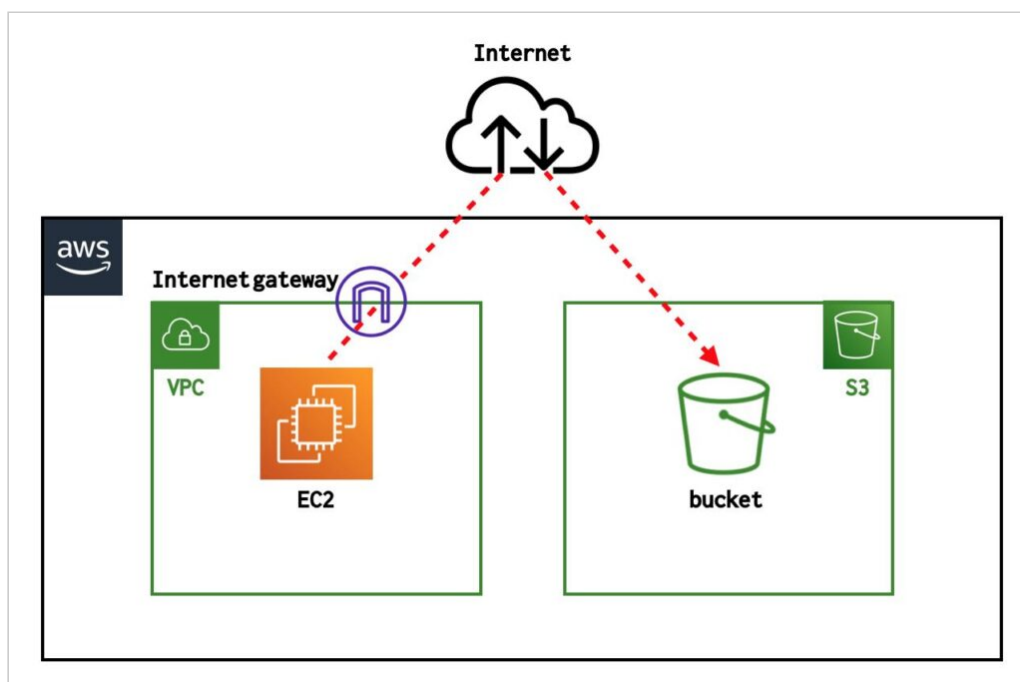
© 2008 - 2021, Amazon Web Services, Inc. またはその関連会社。無断転用禁止。 [プライバシーポリシー](#) [利用規約](#) [Cookie の設定](#)

## S3エンドポイント作成

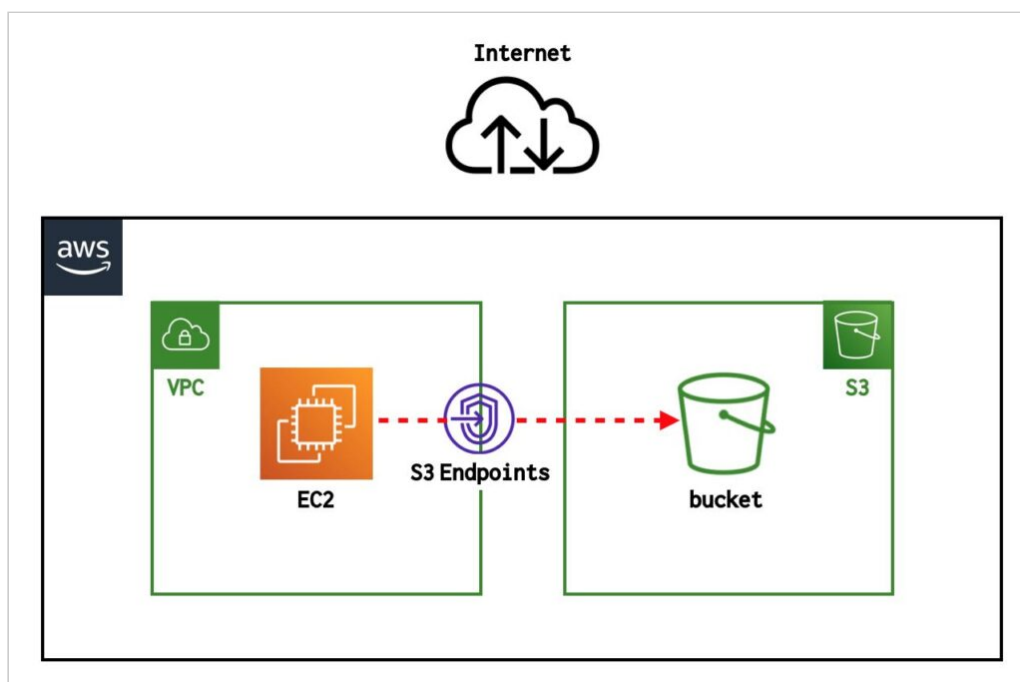
### エンドポイントとは

EC2からS3へトリガーファイルをアップロードする際、デフォルトではインターネットを介した通信となります。S3エンドポイントを作成し、VPCのルートテーブルに追加することでAWS内部での通信が可能となり、セキュリティが向上します。

## デフォルトの通信経路（EC2→S3）

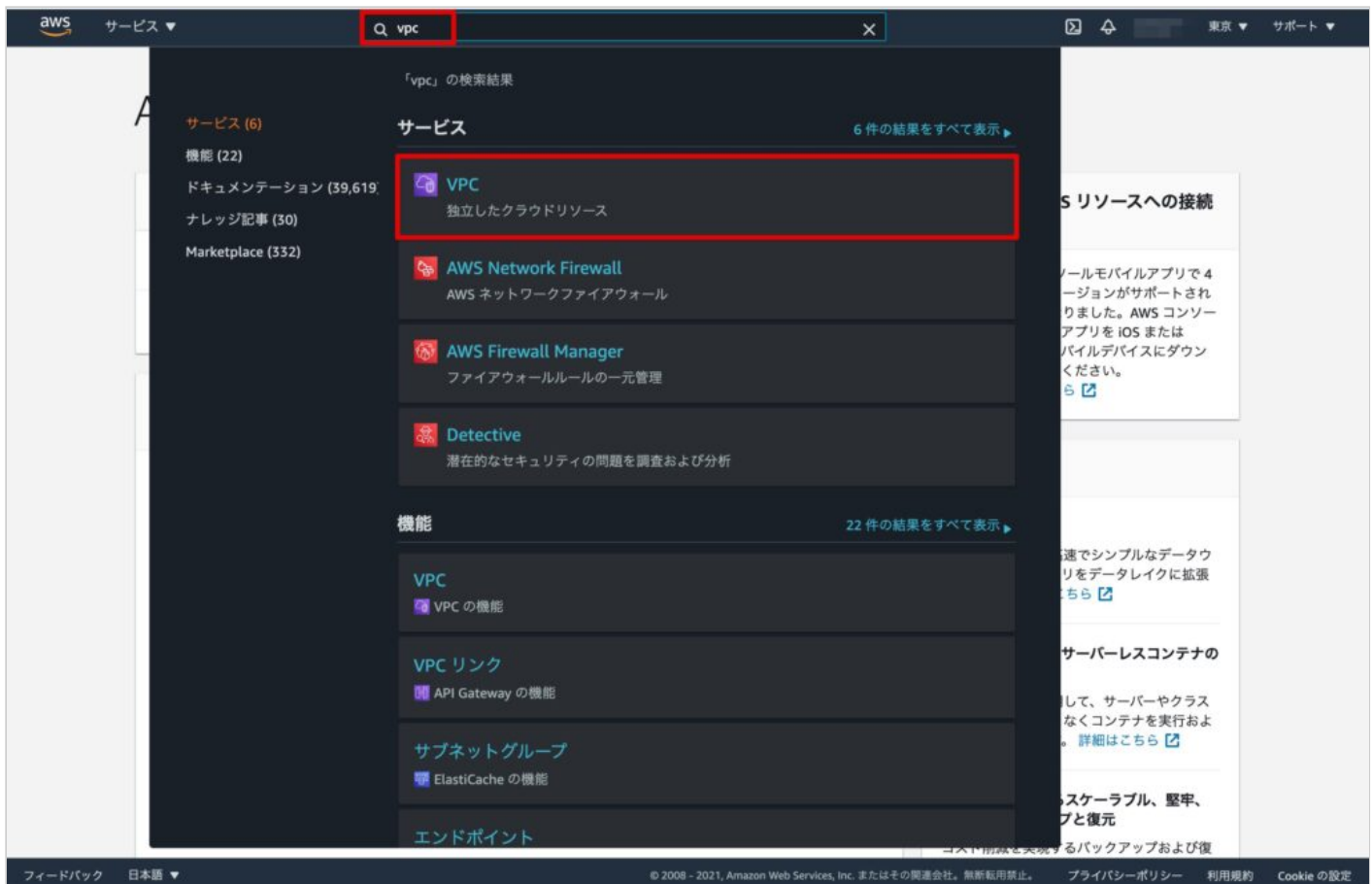


## エンドポイントを利用した通信経路（EC2→S3）



## S3エンドポイントの作成

AWSマネジメントコンソール上で、「vpc」を検索します。



下記の通り選択・入力し、「エンドポイントの作成」をクリックします。

サービスカテゴリ：「AWSサービス」を選択

サービス名：s3で検索し、「com.amazonaws.ap-northeast-1.s3」を選択

VPC：EC2を設置しているVPCを選択

ルートテーブルの設定：チェック

ポリシー：「フルアクセス」を選択



[エンドポイント](#) > エンドポイントの作成

## エンドポイントの作成

VPC エンドポイントを使用して、ご使用の VPC を他のサービスへ安全に接続できます。

インターフェイスエンドポイントには、[PrivateLink](#) が搭載されており、Elastic Network Interface (ENI) をサービス宛てのトラフィックのエントリポイントとして使用します。ゲートウェイエンドポイントは、サービスに対するトラフィックのルートテーブル内のルートのターゲットとして機能します。

- サービスカテゴリ ☒ AWS サービス
- ☐ サービスを名前で検索
  - ☐ ご使用の AWS Marketplace サービス

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

search: s3	フィルターの追加	3 中の 1 ~ 3
サービス名	所有者	タイプ
<input checked="" type="radio"/> com.amazonaws.ap-northeast-1.s3	amazon	Gateway
<input type="radio"/> com.amazonaws.ap-northeast-1.s3	amazon	Interface
<input type="radio"/> com.amazonaws.s3-global.accesspoint	amazon	Interface

VPC\* vpc-xxxxxxxxx ⓘ

ルートテーブルの設定 送信先 (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-xxxxxxxxx ⓘ

ルートテーブル ID	メイン	関連付け
<input checked="" type="checkbox"/> rtb-xxxxxxxxx	はい	2 サブネット



### 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": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

キー (最大 127 文字)

値 (最大 255 文字)

このリソースには現在、タグがありません

タグの追加 残り 50 (最大 50 タグ)

\* 必須

[キャンセル](#)[エンドポイントの作成](#)[フィードバック](#) [日本語](#)

© 2008 - 2021, Amazon Web Services, Inc. またはその関連会社。無断転載禁止。

[プライバシーポリシー](#)[利用規約](#)[Cookie の設定](#)

S3のエンドポイントが作成され、ルートテーブルに紐づいていることを確認します。

The screenshot shows the AWS Management Console interface for the 'Endpoints' section. The left sidebar contains navigation links for VPC, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, Carrier Gateways, DHCP Option Sets, Elastic IP, Managed Prefix Lists, Endpoints, Endpoints Services, NAT Gateways, and Peering Connections. The main content area shows a table of endpoints with columns: Name, Endpoint ID, VPC ID, Service Name, Endpoint Type, Status, and Creation Time. The first endpoint, 'vpce-', is highlighted with a red box. Below the table, the 'Route Tables' tab is selected, showing a table of route tables with columns: Route Table ID, Main, and Attached To. The first route table, 'rtb-', is highlighted with a red box.

The screenshot shows the AWS Management Console interface for the 'Route Tables' section. The left sidebar contains navigation links for VPC, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, Carrier Gateways, DHCP Option Sets, Elastic IP, Managed Prefix Lists, Endpoints, Endpoints Services, NAT Gateways, and Peering Connections. The main content area shows a table of route tables with columns: Route Table ID, Main, and Attached To. The first route table, 'rtb-', is highlighted with a red box.

## EC2からS3バケットへのファイル格納確認

EC2から下記のコマンドを実施し、S3へファイルをアップロードします。※黄色アンダーライン箇所は、作成したS3バケット名を指定してください。

```
touch /tmp/test.txt
aws s3 cp /tmp/test.txt s3://amazonconnect-alert-notification-bucket
```

```
[ec2-user@ip-10-0-0-100 ~]$ touch /tmp/test.txt
[ec2-user@ip-10-0-0-100 ~]$
[ec2-user@ip-10-0-0-100 ~]$ aws s3 cp /tmp/test.txt s3://amazonconnect-alert-
notification-bucket
upload: ../../tmp/test.txt to s3://amazonconnect-alert-notification-
bucket/test.txt
[ec2-user@ip-10-0-0-100 ~]$
```

S3側でファイルがアップロードされたことを確認します。

The screenshot shows the Amazon S3 console interface. On the left is a sidebar with navigation options like 'バケット' (Buckets), 'アクセスポイント' (Access Points), and 'Storage Lens'. The main area displays the 'amazonconnect-alert-notification-bucket'. Under the 'オブジェクト' (Objects) tab, there is a list of objects. A single object, 'test.txt', is listed with a size of 0 B and storage class 'スタンダード' (Standard). The row for 'test.txt' is highlighted with a red border. Above the list are buttons for actions like 'アップロード' (Upload) and 'ダウンロード' (Download). The footer of the console shows copyright information and links to privacy policies.

以上で、AmazonConnectによる自動電話通知（7.複数連絡先への電話通知〈構築①〉）の説明は完了です。