

# デュアルスタック時代の AWSクラウド活用

## IPv6環境構築の勘所とベストプラクティス

### 菊地 信明

アマゾン ウェブ サービス ジャパン合同会社  
技術統括本部 ネットワークリユージョン本部  
シニアソリューションアーキテクト  
ネットワークスペシャリスト



# 自己紹介

名前：菊地 信明（きくち のぶあき）

所属：アマゾン ウェブ サービス ジャパン合同会社  
サービス&テクノロジー事業統括本部  
ネットワークソリューション本部  
シニアソリューションアーキテクト ネットワークスペシャリスト



経歴：通信キャリア- ホスティングやマネージドFWのサポートを経験  
鉄道系IT子会社- 設計・開発・運用に従事  
AWSサポート- AWS Direct Connect/AWS VPNをサポート

好きなAWSサービス：

AWS Direct Connect, AWS Transit Gateway, AWS VPN



# Program

## 1.はじめに

- ◆ 本セッションのゴール
- ◆ IPv4/IPv6デュアルスタックの現状と課題

## 2.クラウドのIPv6ネットワーク設計の基本

- ◆ デュアルスタック環境の基本概念
- ◆ IPv6アドレス プライベートとパブリックの使い分け

## 3.IPv6環境構築のベストプラクティス

- ◆ サブネット設計とアドレス割り当て最適化
- ◆ ロードバランサーやCDNを用いた可用性

## 4.IPv6環境における注意点と対策

- ◆ デュアルスタック環境特有の考慮事項
- ◆ 運用管理とセキュリティの実践

## 5.まとめ

- ◆ クラウドを活用した移行戦略のポイント

# 1. はじめに



# 本セッションのゴール



# 本セッションのゴール

- AWSクラウドを利用した際のアドレス設計について理解する
- IPv4アドレスとIPv6アドレスを併用する場合のポイントについて学ぶ
- ハイブリッド環境を運用する際のヒントを得る
- クラウドを利用した次世代ネットワークの実現方法のコツをつかむ

## 解説・お話ししないこと

- IPv4/IPv6アドレスの基本的なこと
- ネットワーク技術の基本的な用語
- プロトコルの詳細

# IPv4/IPv6デュアルスタックの 現状と課題



# なぜ『今』IPv6なの？

IPv4アドレスだけでうまくいっている方たちむけ、以下のようなおところあたりありませんか？

## 1. 知らないうちに直面している制約

- A) プライベートIPv4アドレスの重複を気にしながらネットワーク設計
- B) 最小限のIPv4 CIDRアサインで、制限のある構成

## 2. 見えにくくなっているコスト

- A) プライベートIPv4アドレス重複のためにNATやProxy機能を追加
- B) 仕方なく夜間・休日にプライベートIPv4アドレスリナンバー祭り
- C) パブリックIPv4アドレスの値段高騰

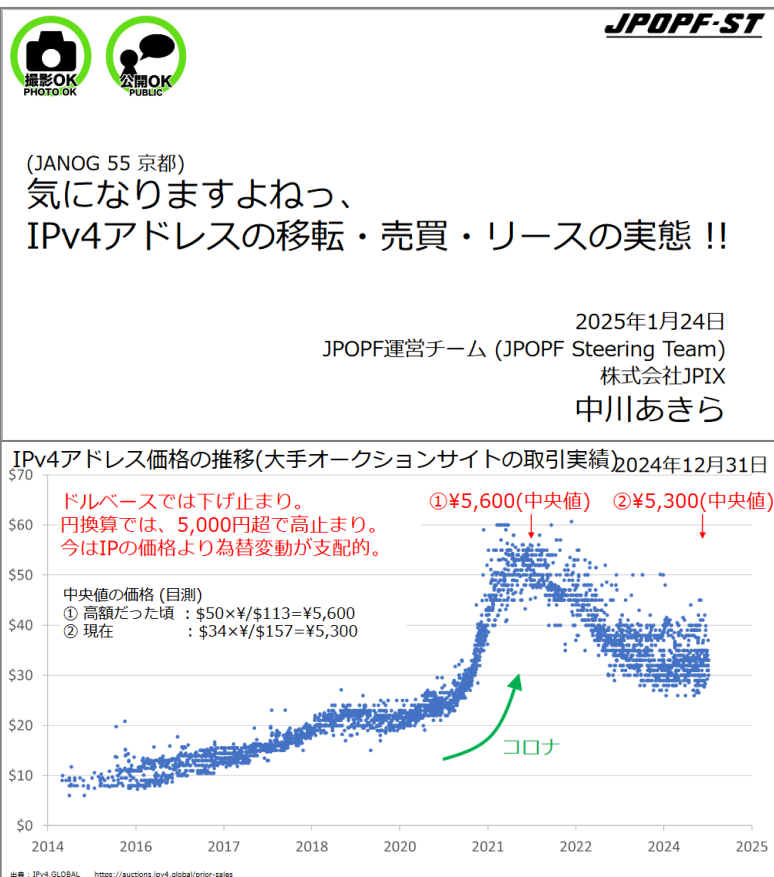
## 3. 将来的なビジネスリスク

- A) 会社の統廃合で得られるはずのシステム共有メリット、結果的にコスト増
- B) ネットワークをつなげるたびに、パズルのようなプライベートIPv4アドレス設計

# IPv4の現状

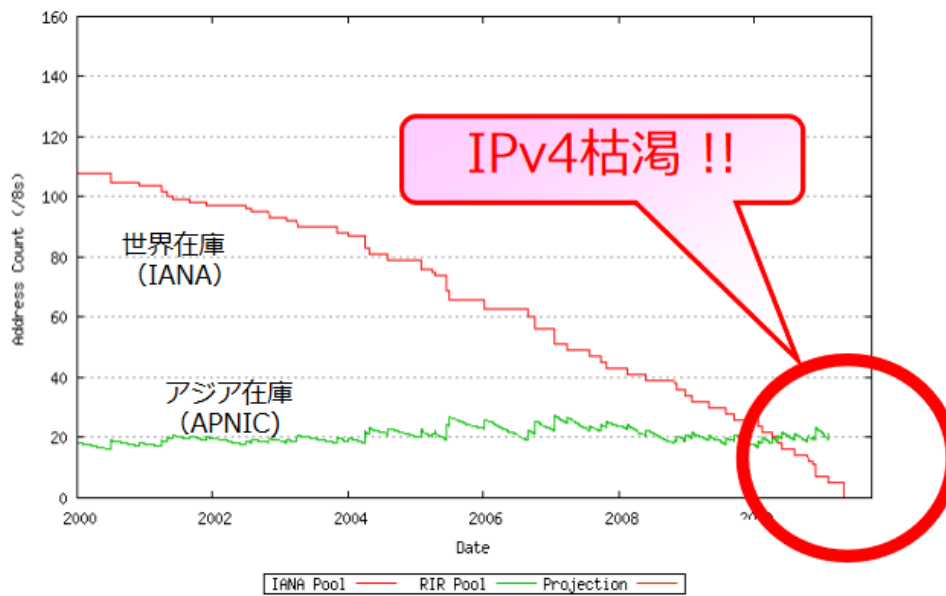
パブリックIPv4アドレスは、すでに枯渇、調達コストも高止まり

JANOG 55 京都「気になりますよねっ、IPv4アドレスの移転・売買・リースの実態 !!」中川 あきらさんの発表より抜粋



## IPv4 アドレスの枯渇

2011年に通常分配の在庫が枯渇して、14年間も経ちました。



**JPOPF-ST**



# クラウド事業者もパブリックIPv4アドレス有料化

AWSでは、2024年2月からパブリックIPv4アドレスに新料金体系を適用し、IPv4アドレス利用の再検討を呼びかけ、IPv6採用を推奨

Amazon Web Services ブログ

## 新着情報 – パブリック IPv4 アドレスの利用に対する新しい料金体系を発表 / Amazon VPC IP Address Manager が Public IP Insights の提供を開始

by Yuya Sudo | on 30 7月 2023 | in [Amazon EC2](#), [Announcements](#), [Launch](#), [News](#) | [Permalink](#) | [Share](#)

AWS は、パブリック IPv4 アドレスの利用に対して新しい料金体系を導入します。2024 年 2 月 1 日より、特定のサービスに割り当てられているかどうかに関わらず、すべてのパブリック IPv4 アドレスの利用に対して 1 IP アドレスあたり 0.005 USD/時間 が課金されます（アカウントに払い出されているものの、どの EC2 インスタンスにも割り当てられていないパブリック IPv4 アドレスに関しては、すでに課金が適用されています）。

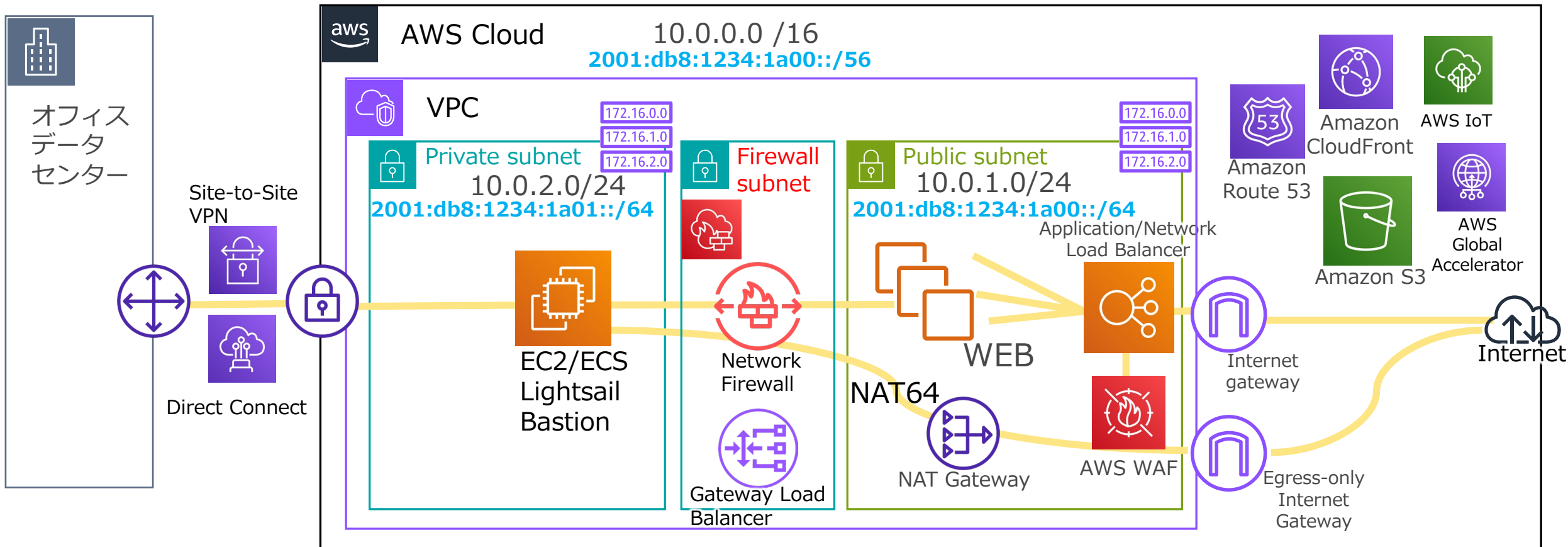
### パブリック IPv4 アドレスの新しい料金体系

IPv4 アドレスはますます希少な資源となっており、パブリック IPv4 アドレスを取得するためのコストは、過去 5 年間で 300% 以上上昇しています。この新しい料金体系の導入は、私たち自身のコストを反映したものであり、また、パブリック IPv4 アドレスの使用を節約し、モダナイゼーションおよび IPv4 アドレスの保全策として IPv6 の採用を奨励することを意図しています。



# AWSクラウドにおけるIPv6の現状

VPC、EC2、ELB、Network Firewall、CloudFront、WAF、Route53、Global AcceleratorなどがIPv6対応



Egress-only Internet Gateway(EIGW) を利用して  
IPv6においてもプライベート利用が可能

**上記のような構成をIPv4/IPv6デュアルスタックで構築可能**

# コンセプト : IPv6 in Amazon VPC (Virtual Private Cloud)

IPv4が基本、希望者はIPv6は追加利用可能

**VPC :**

いずれかを選択

{ IPv4のみ  
デュアルスタック

| お使いの VPC (2) 情報          |               |                       |               |                         |
|--------------------------|---------------|-----------------------|---------------|-------------------------|
| Q VPC をフィルタリング           |               |                       |               |                         |
| <input type="checkbox"/> | Name ▲        | VPC ID ▼              | IPv4 CIDR ▼   | IPv6 CIDR ▼             |
| <input type="checkbox"/> | Default VPC   | vpc-66042901          | 172.31.0.0/16 | –                       |
| <input type="checkbox"/> | IPv6 Demo-vpc | vpc-051a77767380b425c | 192.0.2.0/24  | 2406:da14:583:8000::/56 |

**サブネット :**

いずれかを選択

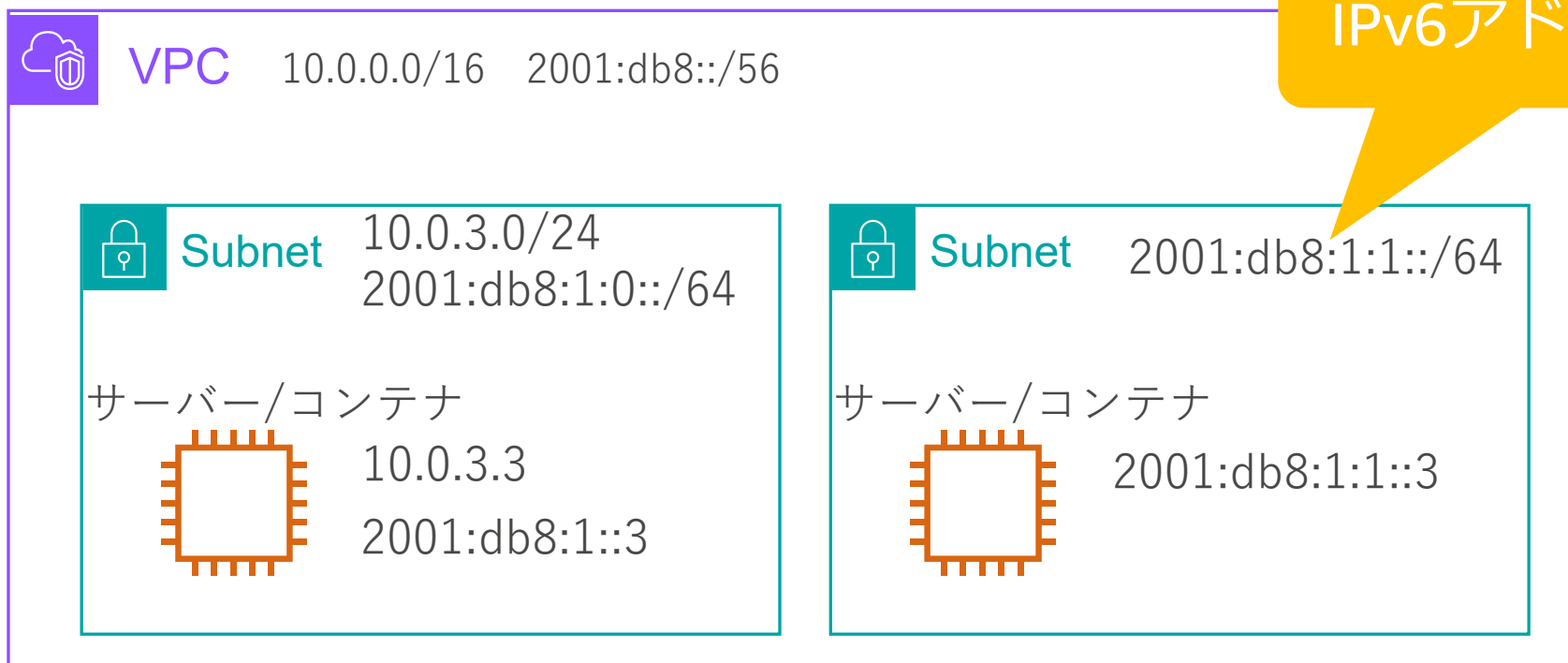
{ デュアルスタック  
IPv4のみ  
IPv6のみ

| サブネット (6) 情報             |                   |                          |               |                         |
|--------------------------|-------------------|--------------------------|---------------|-------------------------|
| Q サブネットをフィルター            |                   |                          |               |                         |
| <input type="checkbox"/> | Name ▲            | サブネット ID ▼               | IPv4 CIDR ▼   | IPv6 CIDR ▼             |
| <input type="checkbox"/> | Dual-Stack Subnet | subnet-0f5205edd0fee12d3 | 192.0.2.0/28  | 2406:da14:583:8000::/64 |
| <input type="checkbox"/> | IPv4-only Subnet  | subnet-0e5af15f00731c361 | 192.0.2.16/28 | –                       |
| <input type="checkbox"/> | IPv6-only Subnet  | subnet-0cc88fbdf481cc9bc | –             | 2406:da14:583:8001::/64 |

# VPC上でのIPv6利用時の課題

IPv6を有効化した場合には、VPC自体はデュアルスタック

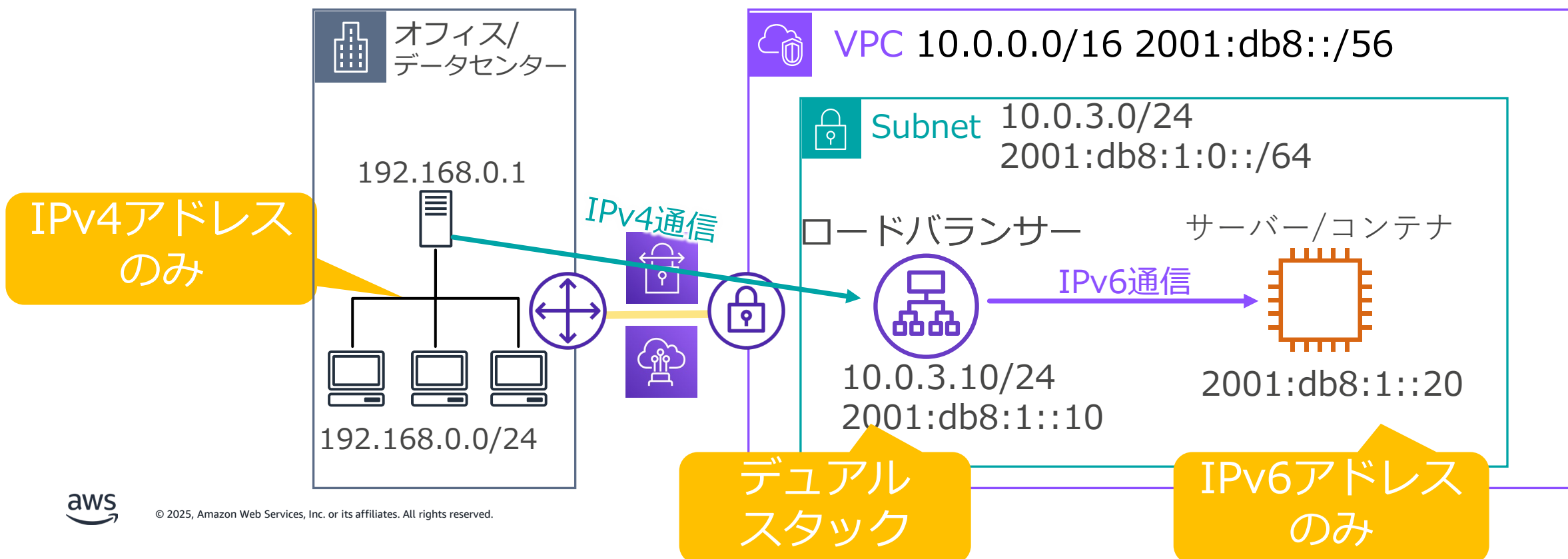
- 要否にかかわらず、IPv4アドレスのアサインが必須
- 持ち込んだIPv6アドレスも利用できる。(BYOIPv6 JPNICを含む)
- 要件に応じて、IPv6のみのサブネットを作ること也有可能



# VPC上でのIPv6利用時の課題

基本的なサービス・リソース間通信については、ほぼ問題になることはない

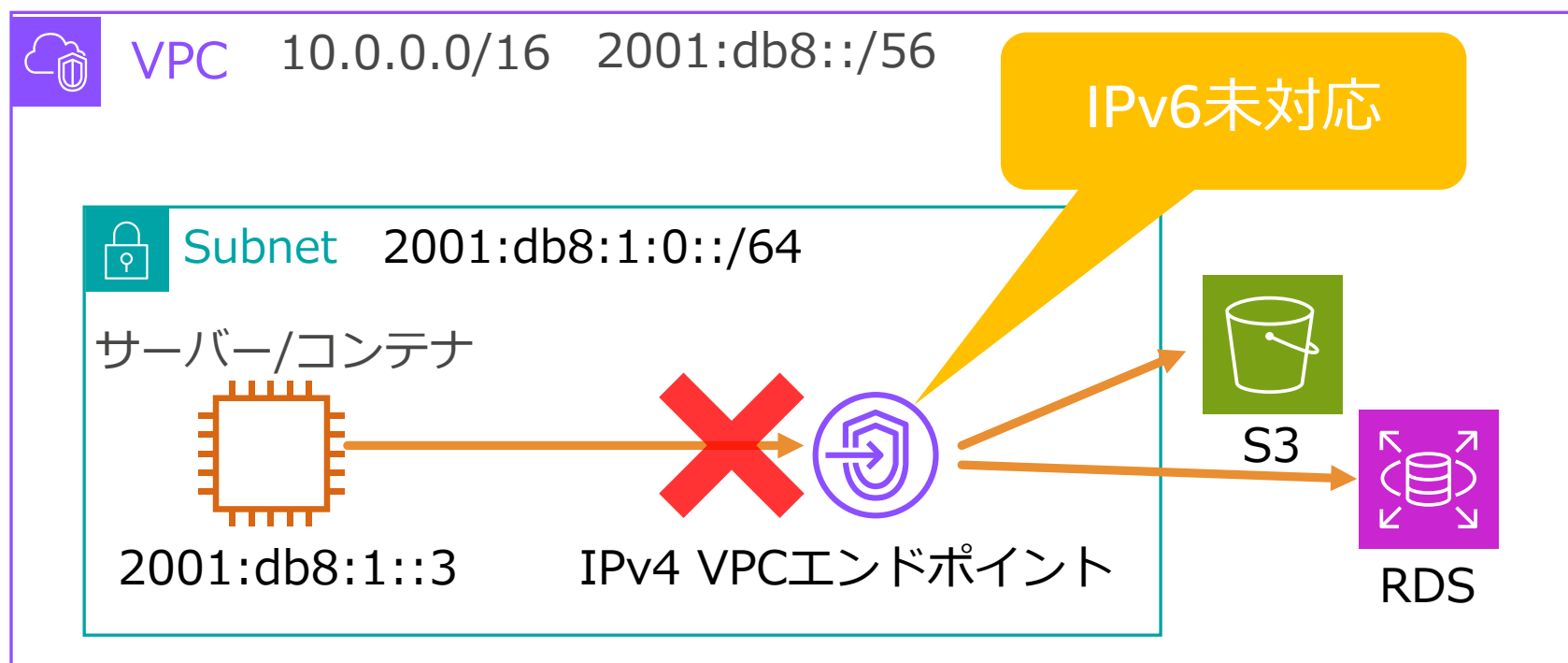
- クラウド上で完結する通信であれば、無料でIPv6化が可能
- オンプレミスから直接通信する際、オンプレミスホストがIPv6アドレスに未対応
- オンプレミスルーターでNAT46を実現するか、ロードバランサーなどで変換



# 未対応サービスの確認

先進的なユーザーによるAWSクラウド利用時に注意

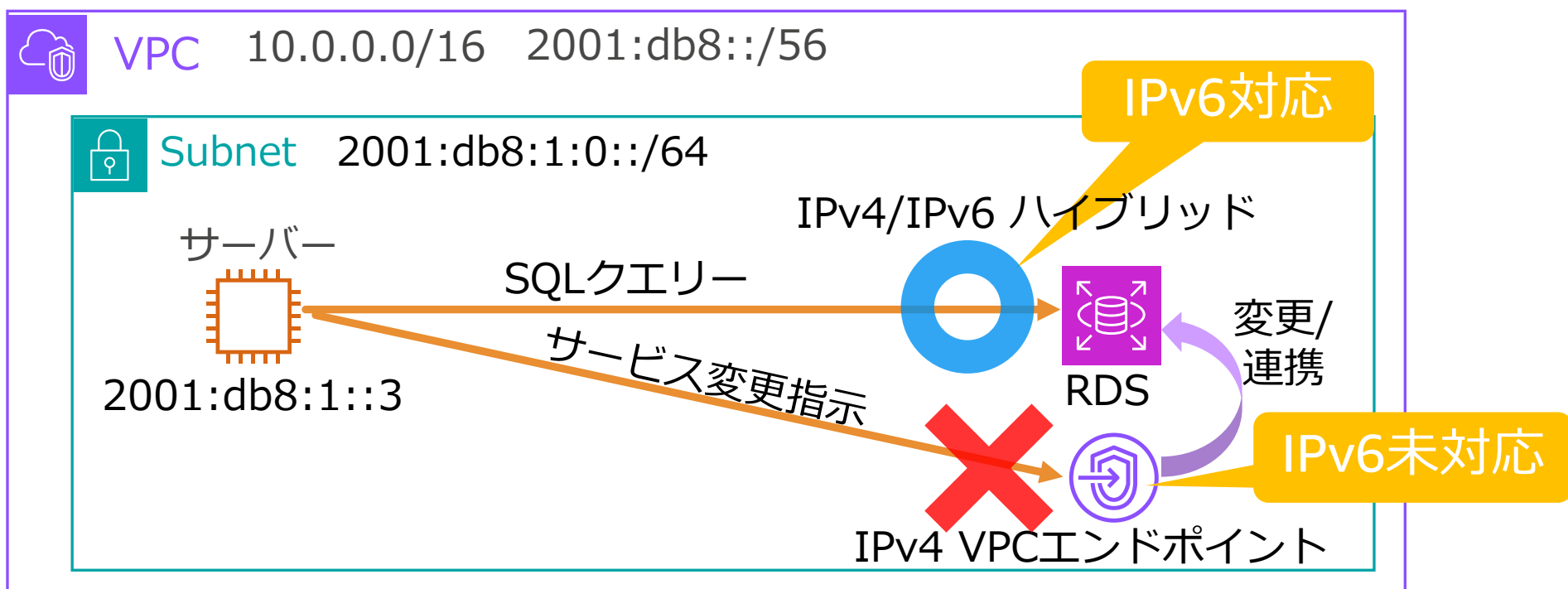
- VPCエンドポイントと呼ぶ、AWSマネージドサービス操作の入り口となる機能が未対応の場合
- デュアルスタックや、IPv4～IPv6を変換する等の対策が必要



# 未対応サービスの確認（続き）

未対応の通信は何か？

- クラウドを利用するうえで、どの機能がIPv6を利用できないのか、確認が必要
  - ✓ データ通信がIPv6未対応の場合
  - ✓ サービス・リソースに対する変更指示通信がIPv6未対応の場合



# 公式ドキュメント：IPv6をサポートするAWSサービス

[https://docs.aws.amazon.com/ja\\_jp/vpc/latest/userguide/aws-ipv6-support.html](https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/aws-ipv6-support.html)

## IPv6 をサポートするサービス

次のテーブルは、デュアルスタックのサポート、IPv6 のみのサポート、および IPv6 をサポートする AWS のサービスを一覧しています。この表は、IPv6 の追加サポートがリリースされたときに更新されます。サービスが IPv6 をサポートする方法についての情報は、そのサービス用のドキュメントを参照してください。

| サービス名                             | デュアルスタックサポート | IPv6 のみサポート | パブリックエンドポイントの IPv6 サポート | プライベートエンドポイントの IPv6 サポート <sup>1</sup> |
|-----------------------------------|--------------|-------------|-------------------------|---------------------------------------|
| AWS Amplify                       | ✅ はい         | ❌ いいえ       | ✅ はい                    |                                       |
| Amazon API Gateway                | ✅ はい         | ❌ いいえ       | ✅ はい                    | ✅ はい                                  |
| AWS App Mesh                      | ✅ はい         | ✅ はい        | ✅ はい                    | ❌ いいえ                                 |
| AWS AppConfig                     | ✅ はい         | ❌ いいえ       | ✅ はい                    | ✅ はい                                  |
| AWS Application Discovery Service | ✅ はい         | ❌ いいえ       | ✅ はい                    | ✅ はい                                  |
| Application Recovery Controller   | ✅ はい         | ❌ いいえ       | ✅ はい                    |                                       |

## 2.クラウドのIPv6ネットワーク 設計の基本



# デュアルスタック環境の 基本概念



# 仮想サーバー：EC2インスタンス内部の見え方

## デュアルスタック環境でのipコマンド実行例

IPv4  
Address

IPv6  
Address

IPv6 Address  
(Link Local)

```
[ssm-user@ip-192-0-2-9 ~]$ ip address show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq s
link/ether 06:ac:c9:f3:35:6d brd ff:ff:ff:ff:ff:ff
inet 192.0.2.9/28 brd 192.0.2.15 scope global dynamic eth0
    valid_lft 2716sec preferred_lft 2716sec
inet6 2406:da14:583:8000:c19d:ed54:2ab6:6e12/128 scope glo
    valid_lft 410sec preferred_lft 100sec
inet6 fe80::4ac:c9ff:fef3:356d/64 scope link
    valid_lft forever preferred_lft forever
```

# 仮想サーバー：EC2インスタンス内部の見え方

## IPv6 Only環境でのipコマンド実行例

IPv4 Address  
(Link Local)

IPv6 Address

IPv6 Address  
(Link Local)

```
[ssm-user@i-0af95398c621af394 ~]$ ip address show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq s
    link/ether 06:8a:f6:a2:51:bd brd ff:ff:ff:ff:ff:ff
    inet 169.254.110.48/32 scope global dynamic eth0
        valid_lft 2128sec preferred_lft 2128sec
    inet6 2406:da14:583:8001:8bf6:9041:f2ed:33c3/128 scope glo
        valid_lft 407sec preferred_lft 97sec
    inet6 fe80::48a:f6ff:fea2:51bd/64 scope link
        valid_lft forever preferred_lft forever
```

# ルートテーブル、セキュリティグループ

IPv6もIPv4も同様に設定、動作する

仮想サーバー（EC2インスタンス）上では、DHCPから取得したデフォルトルートを採用、VPC機能で提供されるルートテーブルで制御する

## ルートテーブルの例

| 送信先                     | ターゲット                 | ステータス  |
|-------------------------|-----------------------|--------|
| 172.16.0.0/24           | local                 | active |
| 2406:da14:4d1:6800::/56 | local                 | active |
| 0.0.0.0/0               | igw-05d751013e99ca39e | active |
| ::/0                    | igw-05d751013e99ca39e | active |

## セキュリティグループの例

| Type        | Protocol | Port Range | Source      |
|-------------|----------|------------|-------------|
| ALL UDP     | UDP (17) | ALL        | sg-84b760ed |
| ALL Traffic | ALL      | ALL        | 0.0.0.0/0   |
| ALL Traffic | ALL      | ALL        | ::/0        |

# DNSリソースレコード登録

Amazon Route 53 : ホストゾーンを提供するDNSサービスで管理

- 同じホスト名で、IPv4、IPv6の両方をアクセスさせる設計、もしくは、ホスト名を分けて管理する設計等
- 同じホスト名の場合には、A RecordとAAAA Record(クワッドエーレコード)を併記する

## リソースレコード登録の例

| <input type="checkbox"/> | レコード名 ▼           | タ... ▼ | ルーテ... ▼ | 差別... ▼ | 値/トラフィックのルーティング先 ▼                                                                                 |
|--------------------------|-------------------|--------|----------|---------|----------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | example.co.jp     | NS     | シンプル     | -       | ns-1536.awsdns-00.co.uk.<br>ns-0.awsdns-00.com.<br>ns-1024.awsdns-00.org.<br>ns-512.awsdns-00.net. |
| <input type="checkbox"/> | example.co.jp     | SOA    | シンプル     | -       | ns-1536.awsdns-00.co.uk. awsdns-hostmaster                                                         |
| <input type="checkbox"/> | www.example.co.jp | A      | シンプル     | -       | 192.168.20.100                                                                                     |
| <input type="checkbox"/> | www.example.co.jp | AAAA   | シンプル     | -       | 2406:da14:d2:c310:48ab:109a:65ba:9fae                                                              |

# IPv6アドレス プライベートとパブリック の使い分け

# IPv6グローバルユニキャストアドレス(GUA)

- IPv6を有効にしたVPCではグローバルユニキャストアドレス(GUA)をアサイン可能
  - IPv6アドレスは、Amazonから割り当てられるか、お客様が持ち込んだIPv6アドレス(BYOIPv6)を利用
- それぞれのインスタンスはGUAが付与される
- 1 : 1 のNATは不要
- Egress Only Internet Gatewayによりアウトバウンド方向のみをトリガーとしたインターネットへ接続可能

# IPv6ユニークローカルアドレス(ULA)

- Amazon VPC IP Address Manager (IPAM) ではユニークローカルアドレス(ULA)をVPCにアサイン可能
  - AWS内のみで利用する、プライベートなIPv6アドレスの役割
- GUAと使い分けすることで、IPv4に近い論理構成が可能
- インターネットへ接続する際には、別のサブネットにGUAを配置し、そちらを経由する

# 3. IPv6環境設計の ベストプラクティス

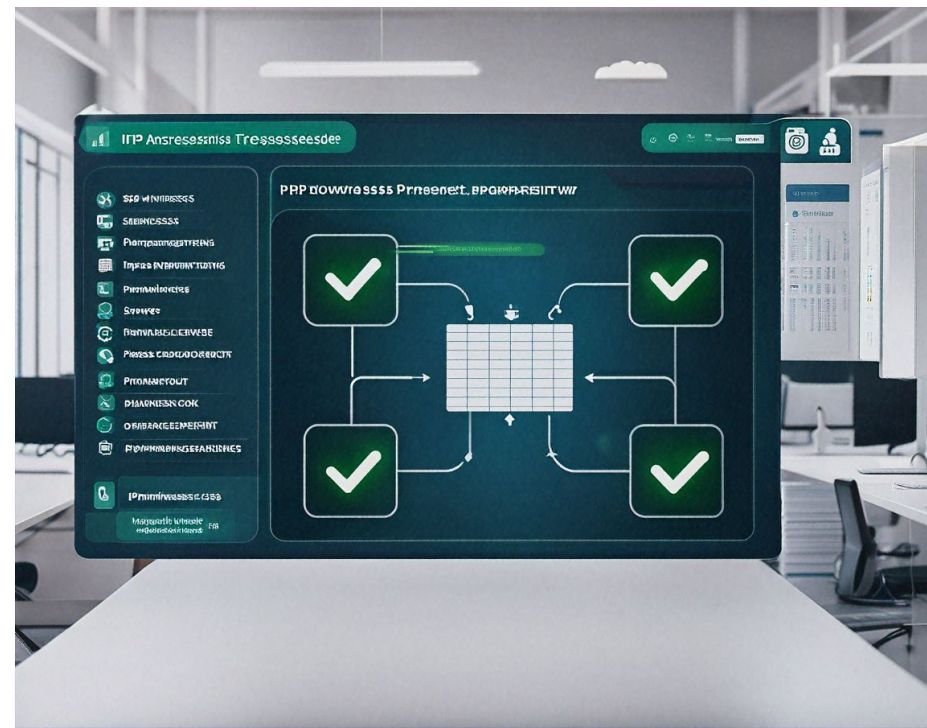


# サブネット設計とアドレス 割り当て最適化



# IPアドレス管理

- オンプレミスと複数契約・アカウントにまたがるクラウドへの割り当てが必要
- よくあるスプレッドシートの管理では重複アサインや残りのアドレス帯把握に限界
- 管理ツールの導入が理想

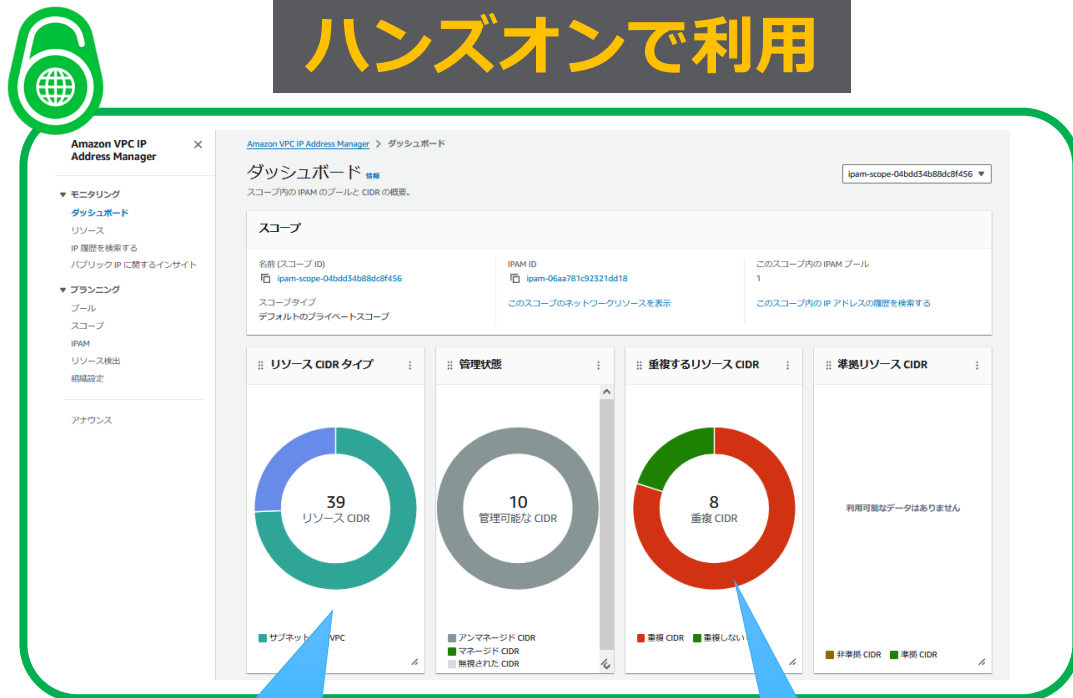


# Amazon VPC IP Address Manager (IPAM)



AWS CloudとオンプレミスのIPを管理

## ハンズオンで利用



IPの利用率を  
ダッシュボードで表示

重複利用し  
ているIPを  
可視化

## 特徴 [\(https://docs.aws.amazon.com/ja\\_jp/vpc/latest/ipam/\)](https://docs.aws.amazon.com/ja_jp/vpc/latest/ipam/)

- IP アドレス空間をルーティングドメインとセキュリティドメインに整理する
- 使用中の IP アドレス空間を監視し、空間を使用しているリソースをビジネスルールに照らし合わせて監視する
- 特定のビジネスルールを使用してCIDRをVPCに自動的に割り当てる

任意のIPv4/IPv6アドレスをBYOIPできる

## 価格体系 [\(http://aws.amazon.com/jp/vpc/pricing/\)](http://aws.amazon.com/jp/vpc/pricing/)

- IPAM 無料利用枠：BYOIP v4 および v6)と、Amazonが提供する連続したIPv6アドレスを管理
- IPAM アドバンスドティア：複数リージョンまたはアカウントを管理

# 既存のIPv4リソースのハイブリッド化

- すでにIPv4のみで設定された環境をハイブリッドに移行するときのステップは3つ
  - ① Amazon Virtual Private Cloud(VPC)にIPv6 CIDRを追加
  - ② VPC内のサブネットにIPv6 CIDRを追加
  - ③ 仮想サーバー(EC2インスタンス等)にIPv6を追加

# ① VPCにIPv6 CIDRを追加

- IPv4 CIDR割り当て済みのVPCに対し、AWS提供またはユーザー持ち込み(BYOIPv6)のIPv6 CIDRを追加割り当てする

**CIDR の編集** 情報  
VPC の CIDR ブロックを追加または削除します。

**IPv4 CIDR** 情報  
CIDR | ステータス  
172.31.0.0/16 | ✔ Associated

[新しい IPv4 CIDR を追加](#)

**IPv6 CIDR** 情報  
CIDR (ネットワークボーダーグループ) | プール  
VPC に関連付けられた IPv6 CIDR

[新しい IPv6 CIDR を追加](#)

**IPv6 CIDR を追加**

**IPv6 CIDR ブロック**

☐ IPAM 割り当ての IPv6 CIDR ブロック

☒ Amazon 提供の IPv6 CIDR ブロック

☐ IPv6 CIDR 所有 (ユーザー所有)

**ネットワークボーダーグループ**  
ネットワークボーダーグループは、IPv4 および IPv6 IP アドレスがアドレスグループです。この VPC のすべてのアベイラビリティゾーンは、このグループを使用します。

us-east-1

**IPv6 CIDR の編集** 情報  
VPC の CIDR ブロックを追加または削除します。

**IPv4 CIDR** 情報  
CIDR | ステータス | 削除  
172.31.0.0/16 | ✔ Associated | [削除](#)

[新しい IPv4 CIDR を追加](#)

**IPv6 CIDR** 情報  
CIDR (ネットワークボーダーグループ) | プール | アドレス属性 | ステータス | 削除  
2600:1f10:4541:3d00::/56 (us-east-1) | Amazon | パブリック | ✔ Associated | [削除](#)

[新しい IPv6 CIDR を追加](#)

[閉じる](#)

## ②VPC内のサブネットにIPv6を追加

- IPv4 CIDR割り当て済みのサブネットに、VPCのIPv6 CIDRの範囲からIPv6 CIDRを追加で割り当てる

The screenshot displays the AWS Management Console interface for editing IPv6 CIDR blocks. On the left, the 'IPv6 CIDR の編集' (Edit IPv6 CIDR) page shows details for a VPC (vpc-3b04515c) and a subnet (subnet-c634d39d). The 'サブネットの CIDR ブロック' (Subnet CIDR Blocks) section indicates that no IPv6 CIDR blocks are currently associated with the subnet, with a button 'IPv6 CIDR を追加' (Add IPv6 CIDR) and a note '残り 1 個' (1 remaining).

An overlay window titled 'サブネットの CIDR ブロック' (Subnet CIDR Blocks) is shown in the foreground. It displays the 'VPC CIDR ブロック' (VPC CIDR Block) as '2600:1f10:4541:3d00::/56'. Below this, the 'サブネットの CIDR ブロック' (Subnet CIDR Block) section shows a new block '2600:1f10:4541:3d00::/64' being added, with a note '18.4Q IPs'. Navigation arrows and a '削除' (Delete) button are visible. At the bottom, there is a button 'IPv6 CIDR を追加' (Add IPv6 CIDR) and a note '残り 0 個' (0 remaining).

### ③仮想サーバー(EC2インスタンス等)にIPv6を追加

- IPv4 Address割り当て済みインスタンスのeth0に、サブネットのIPv6 CIDRの範囲からIPv6 Addressを追加で割り当てる

**IP アドレスの管理** 情報  
インスタンスのネットワークインターフェイスへの/からの IPv4 および IPv6 アドレスの割り当て/割り当て解除を行います。

**IP アドレス**  
インスタンス ID  
i-0438f0270e87cf931 (MyServer)

① このインスタンスに追加のパブリック IPv4 アドレスを割り当てるには、Elastic IP アドレスをそのネットワークインターフェイスに関連付ける必要があります。

▼ eth0: eni-07299f0ccb8ca9fd9 - 172.31.16.0/20

**IPv4 アドレス**  
プライベート IP アドレス: 172.31.29.137  
パブリック IP アドレス:   
割り当て解除

新しい IP アドレスの割り当て

**IPv6 アドレス**  
IP アドレスが存在しません

新しい IP アドレスの割り当て

**IPv6 アドレス**  
IPv6 アドレス  
自動割り当て  
元に戻す  
新しい IP アドレスの割り当て

▼ IP アドレス 情報

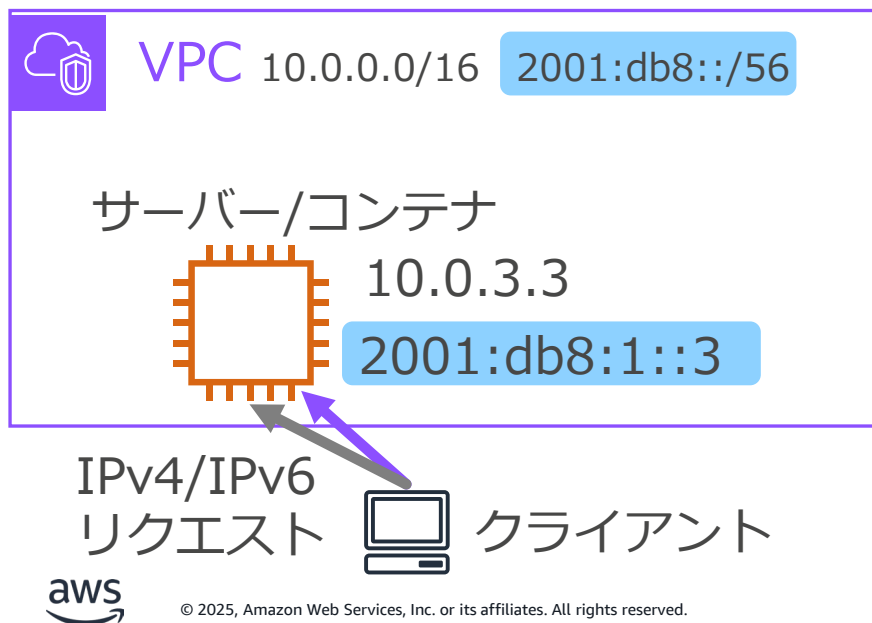
| パブリック IPv4 アドレス | プライベート IPv4 アドレス | IPv6 アドレス                               |
|-----------------|------------------|-----------------------------------------|
| -               | 172.31.29.137    | 2600:1f10:4541:3d00:1a56:b54a:81dc:2bc7 |

まずは、  
IPv4とIPv6の  
ハイブリッドから始める

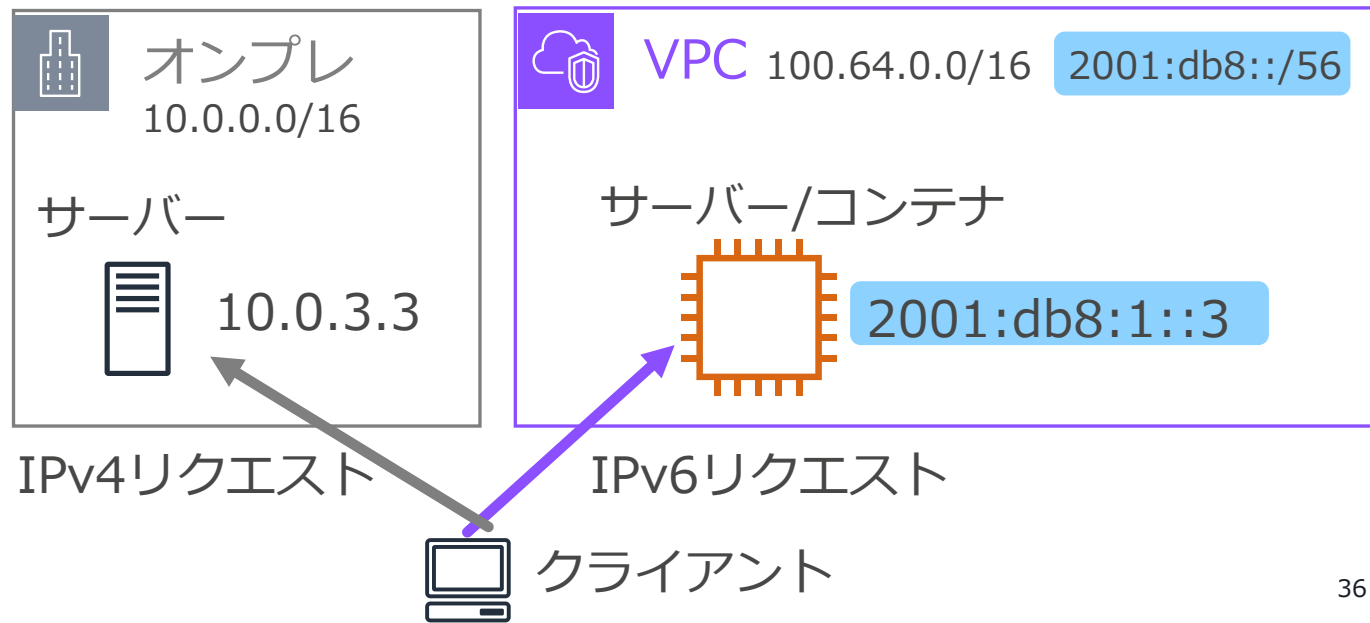
# まずはハイブリッド

- 現行のIPv4システムに、IPv6を追加するアプローチ
  - A) システムの更新タイミングで、クラウド上でハイブリッド構成を作ってみる
  - B) 既存のIPv4構成をオンプレミスで維持したまま、IPv6対応サイトをクラウド上に構築する

## A) クラウド上でハイブリッド



## B) オンプレミスとクラウドで役割分担したハイブリッド



# ロードバランサーや CDNを用いた可用性

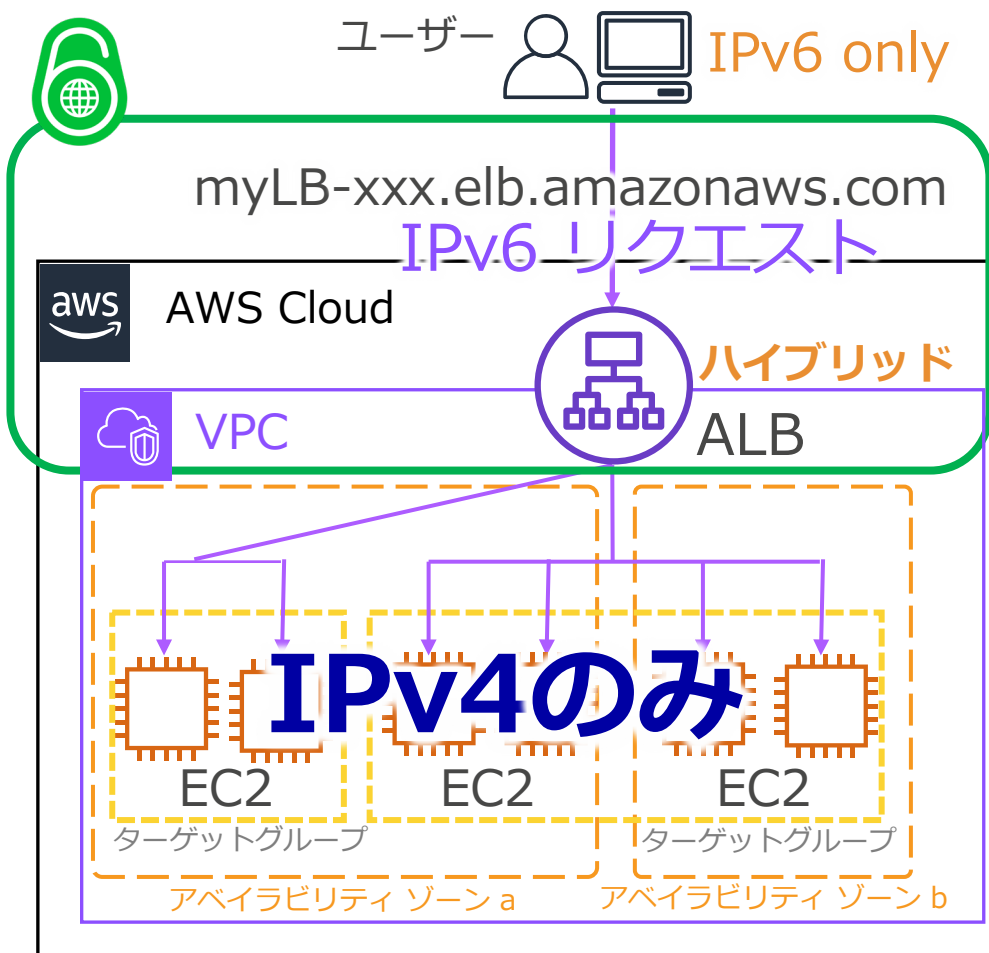


# 動いているサーバーに 変更を加えられないとき

# Application Load Balancer (ALB) **ハンズオンで利用**



レイヤー7のコンテンツベースのロードバランサー



## 特徴 [\(https://aws.amazon.com/elasticloadbalancing/applicationloadbalancer/\)](https://aws.amazon.com/elasticloadbalancing/applicationloadbalancer/)

- レイヤー7のコンテンツベースで、ターゲットグループに対してルーティング
- コンテナベースのアプリケーションのサポート
- WebSocket, HTTP/2, IPv6, AWS WAF をサポート
- 複数のアベイラビリティゾーンに跨って、高レベルの耐障害性を実現
- ALB自体が自動的にキャパシティを増減
- IPv6 Targetに対応 **Update!!**

## 価格体系

[\(https://aws.amazon.com/jp/elasticloadbalancing/applicationloadbalancer/pricing/\)](https://aws.amazon.com/jp/elasticloadbalancing/applicationloadbalancer/pricing/)

- ALBの起動時間
- Load Balancer Capacity Units (LCU)の使用量



# Amazon CloudFront



マネージドCDN(Content Delivery Network)サービス



## 特徴 [\(http://aws.amazon.com/jp/cloudfront/\)](http://aws.amazon.com/jp/cloudfront/)

- 簡単にサイトの高速化が実現できると共に、サーバの負荷も軽減
- 様々な規模のアクセスを処理することが可能
- 世界450箇所以上のPOP
- IPv4で構成されたオリジンをIPv6で公開可能

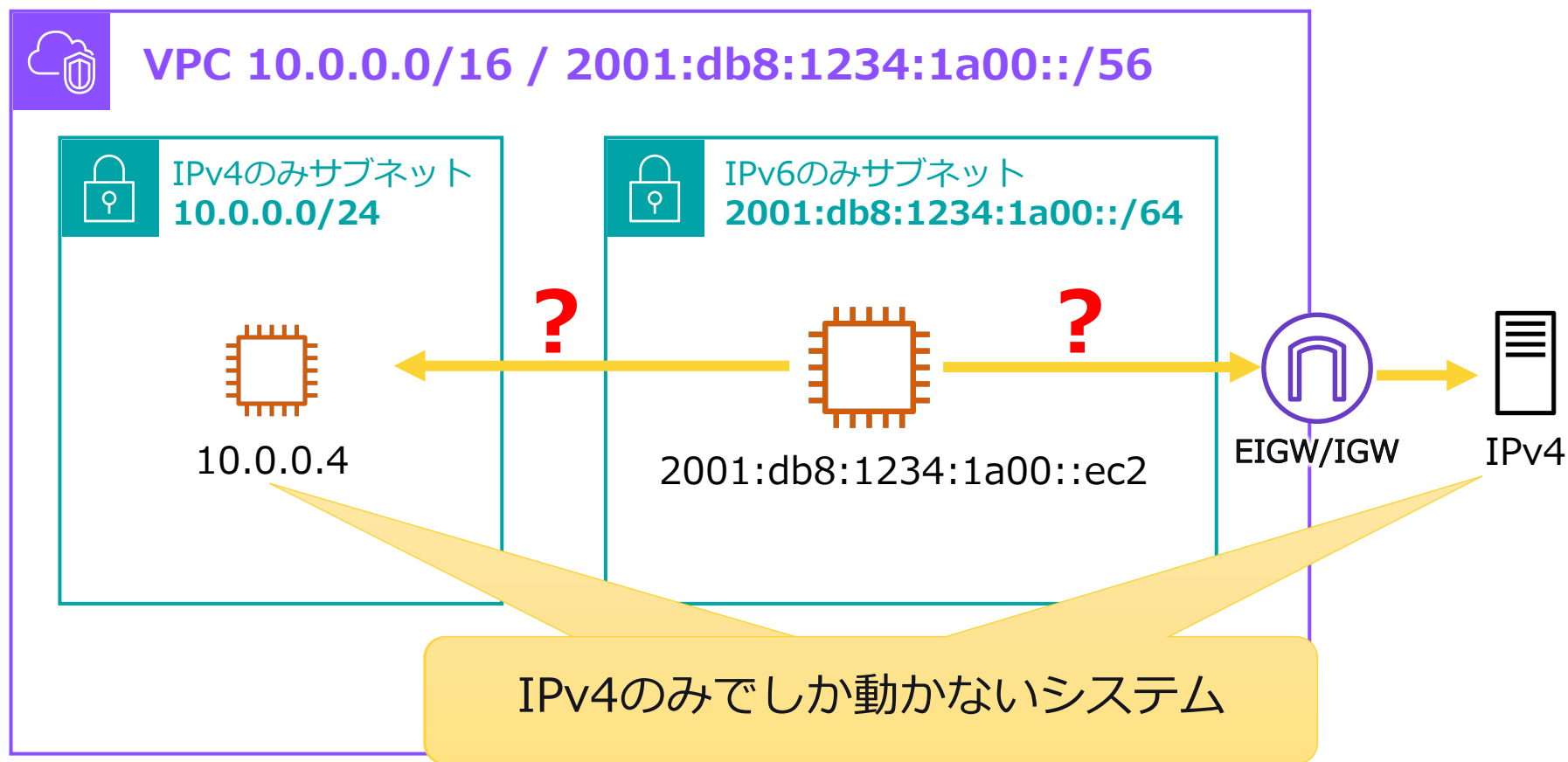
## 価格体系 [\(http://aws.amazon.com/jp/cloudfront/pricing/\)](http://aws.amazon.com/jp/cloudfront/pricing/)

- データ転送量(OUT)
- HTTP/HTTPSリクエスト数
- (利用する場合)SSL独自証明書 など
- 無料枠：1か月あたり最大1TB のデータ転送

# 通信先のシステムが IPv6未対応のとき

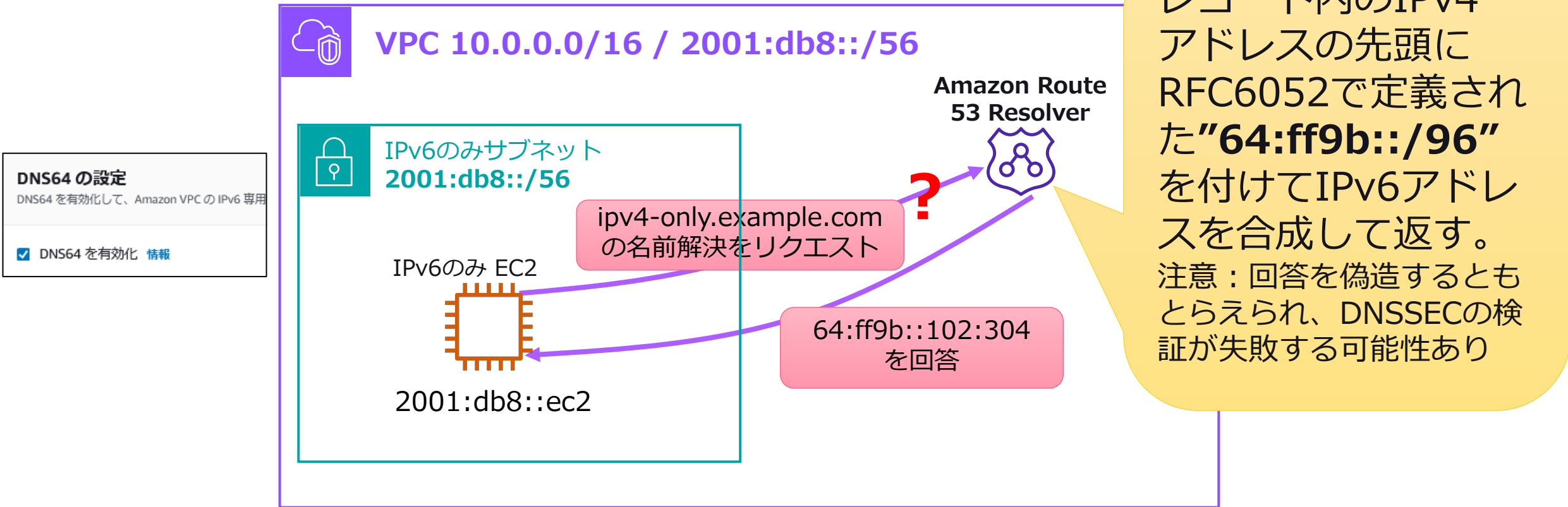
# DNS64/NAT64

ホストがIPv6のみの場合、相手に合わせて通信する必要性あり



# DNS64の動き

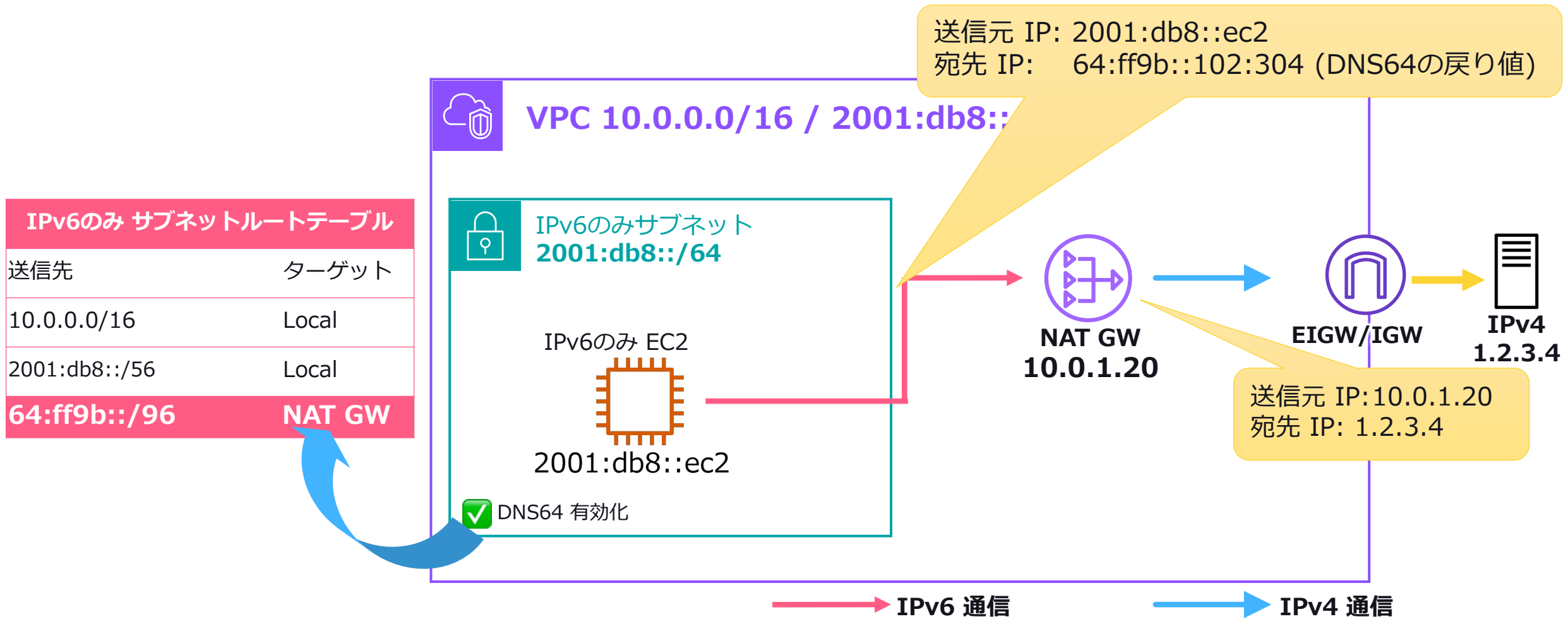
VPCで『DNS64』機能を有効かすると・・・



|                       | Type | Value       | Amazon Route 53 Resolverの戻り値 |
|-----------------------|------|-------------|------------------------------|
| ipv4-only.example.com | A    | 1.2.3.4     | 64:ff9b::102:304             |
| ipv6-only.example.com | AAAA | 2001:db8::1 | 2001:db8::1                  |

# NAT64の動き

通信相手がIPv4のみを持つ場合に有効



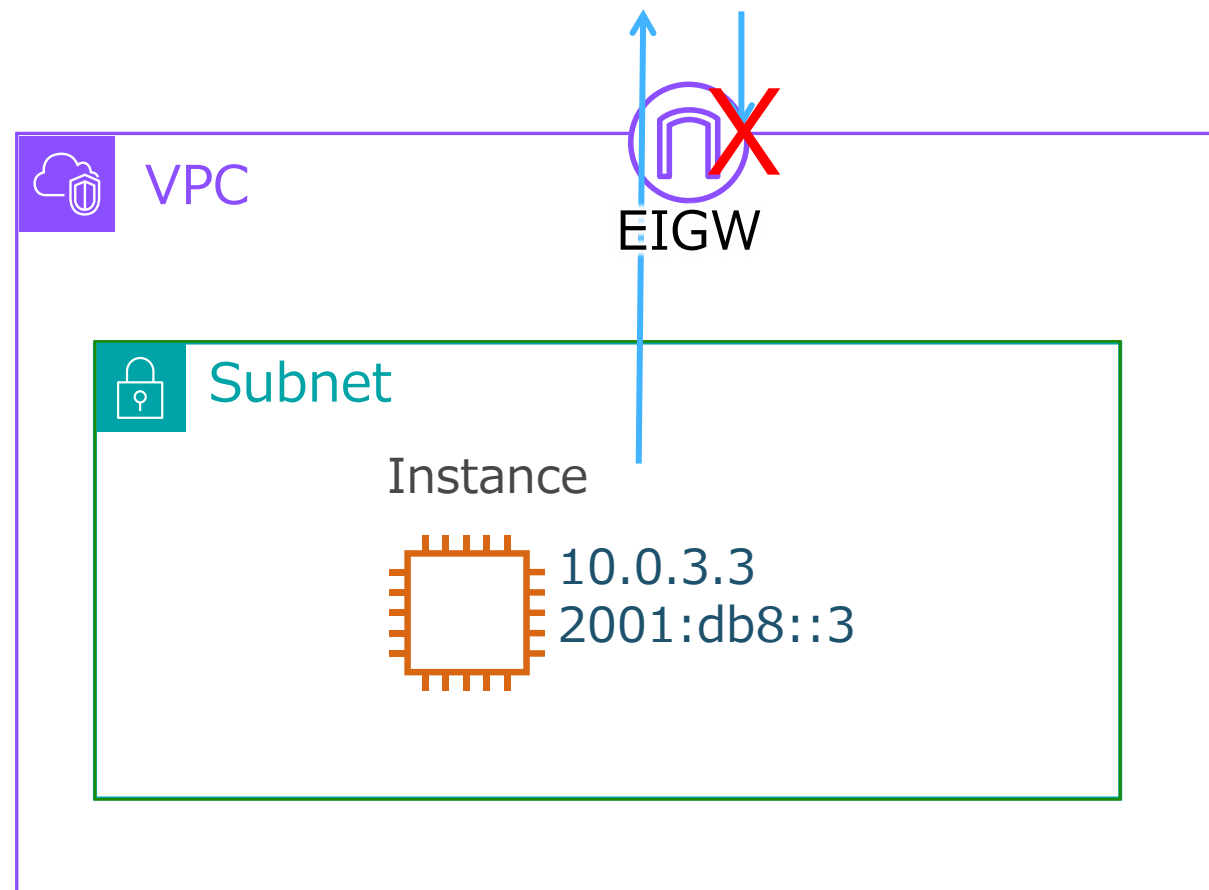
# Egress-only Internet Gateway (EIGW)

IPv6通信はアウトバウンドのみ可能にしたい場合

- IPv6経由でアウトバウンドに限定したインターネットアクセスを提供
- IPv4通信に影響を与えない
- コスト負担なし
- パフォーマンスや可用性の制限はない

## ルートテーブルの例

| 送信先                     | ターゲット                 | ステータス  |
|-------------------------|-----------------------|--------|
| 172.16.0.0/24           | local                 | active |
| 2406:da14:4d1:6800::/56 | local                 | active |
| 0.0.0.0/0               | igw-05d751013e99ca39e | active |
| ::/0                    | eigw-abcd123456789efg | tive   |



# 4. IPv6環境における 注意点と対策



# デュアルスタック環境特有の 考慮事項



# デュアルスタック環境特有の考慮事項

IPv6とIPv4は別のネットワーク環境であることを理解する

- 2つのネットワークについて、それぞれ設計・設定・管理・運用が必要となる。
- 個別のセキュリティ設定が必要、フィルタリングも別に設定する。
- ルートテーブル、ゲートウェイは別途設定する。
- 各ゲートウェイの機能は、双方向でどのような制御が必要かを確認する。
- 名前解決についても考慮し、DNSリソースレコードにおいて、Aレコード、AAAAレコードの両方を管理する。

# デュアルスタックのWebサイトを公開する際の考慮

- IPv4とIPv6のデュアルスタックでサービスを提供する場合、どちらのIPアドレスを利用するのか、最終的にはアクセス元環境に依存する。
- Happy Eyeballs ver.2 (RFC8305) では、IPv6を優先する仕様。しかし、すべての環境・ウェブブラウザでこの通り動作するとは限らない。

参考：

Internet Week ショーケースin 広島

世界で進むIPv4の品質劣化とIPv6の導入、ところで企業のIPv6対応は？

<https://www.nic.ad.jp/sc-hiroshima/program/nakagawa.pdf#page=15>

- 最近では、IPスタックを使い分ける他の概念も出てきている。
- 影響しそうな機構：Windows AD、Proxy、URLフィルタ、ウイルスチェック等

# 運用管理とセキュリティの 実践



# IPv6通信を考慮したログ管理/運用

## 1. ログフォーマットの対応

- A) IPv6アドレスは128ビットと長いため、独自スクリプトなどで、ログフォーマットがIPv6アドレスを適切に処理できることを確認
- B) CloudWatchやVPCフローログなどのログ設定でフォーマットの"protocol"と"type"フィールドを確認

| フィールド               | 内容                                   |
|---------------------|--------------------------------------|
| version             | 3                                    |
| account-id          | 384767312456                         |
| interface-id        | eni-0b62d5e000e412345                |
| srcaddr             | 2001:db8:85a3:8d3:1319:8a2e:370:7348 |
| dstaddr             | 2001:db8:85a3:8d3:1319:8a2e:370:7347 |
| srcport             | 50565                                |
| dstport             | 80                                   |
| protocol            | 6                                    |
| packets             | 7                                    |
| bytes               | 751                                  |
| start               | 1573704396                           |
| end                 | 1573704455                           |
| action              | ACCEPT                               |
| log-status          | OK                                   |
| vpc-id              | vpc-0af48868ceeb12345                |
| subnet-id           | subnet-02ab634d2e4c12345             |
| instance-id         | i-0a998a68301112345                  |
| tcp-flags           | 3                                    |
| type                | IPv6                                 |
| pkt-srcaddr         | 2001:db8:85a3:8d3:1319:8a2e:370:7348 |
| pkt-dstaddr         | 2001:db8:85a3:8d3:1319:8a2e:370:7347 |
| region              | ap-northeast-1                       |
| az-id               | apne1-az1                            |
| sublocation-type    | -                                    |
| sublocation-id      | -                                    |
| pkt-src-aws-service | ROUTE53_HEALTHCHECKS                 |
| pkt-dst-aws-service | EC2                                  |
| flow-direction      | ingress                              |
| traffic-path        | 6                                    |



# IPv6通信を考慮したログ管理/運用（続き）

## 2. キュリティ対応

- A) 通常はIPv6特有の攻撃パターンも意識するが、AWSクラウドではマルチキャストアドレスに非対応なので、過度にICMPv6対策をする必要はない
  - 標準的なAWS VPC環境では、マルチキャストは非サポート
  - Transit Gatewayのマルチキャスト機能は、現時点でIPv4のみをサポート
- B) AWSマネージドサービス(AWS Configなど)のマネージドルールで、IPv6トラフィックが監視対象となることを確認、カスタムルールでは修正が必要な場合もある

## 3. ログ保存容量・保存期間・分析環境

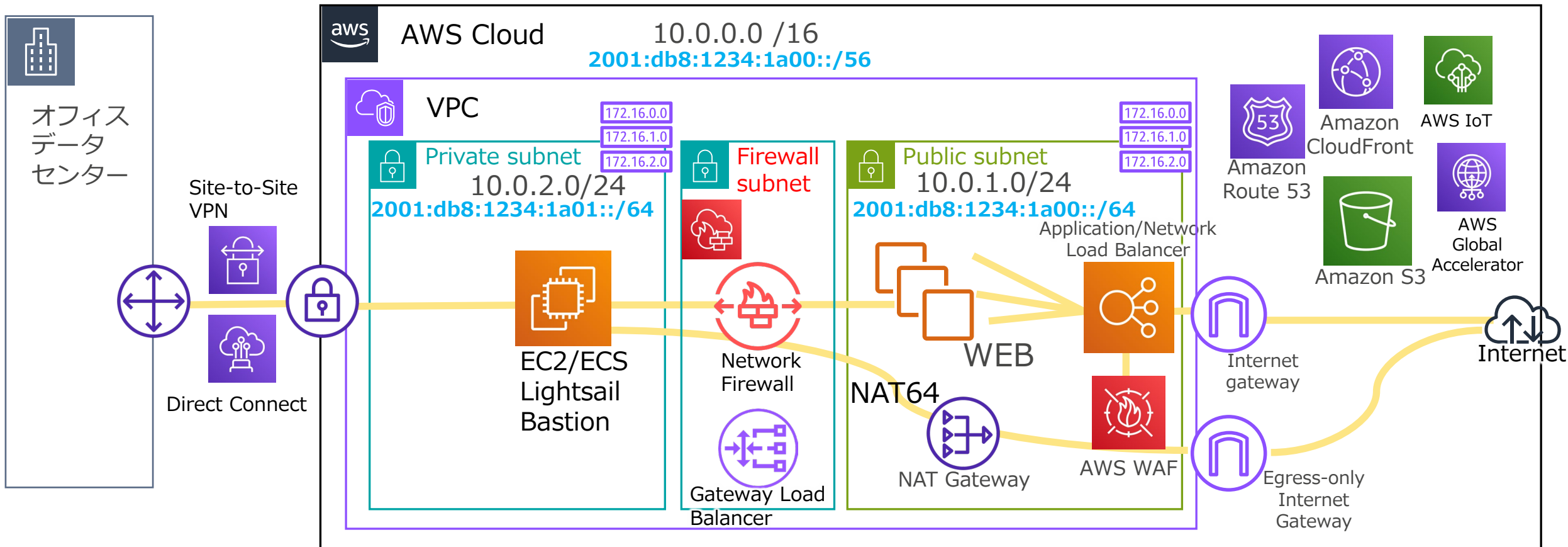
- A) マネージド・独自の分析ツールでIPv6アドレスを適切に処理可能かを確認
- B) ストレージへの保存形式をIPv6と同一にするか、分別するか等検討

# 5.まとめ



# IPv6の現状（再掲）

VPC、EC2、ELB、Network Firewall、CloudFront、WAF、Route53、Global AcceleratorなどがIPv6対応



Egress-only Internet Gateway(EIGW) を利用して  
IPv6においてもプライベート利用が可能

上記のような構成をIPv4/IPv6デュアルスタックで構築可能

# まとめ

- 今後、いつまでもIPv4アドレスで拡張できるとは限らない
- 早くからIPv6利用のノウハウを溜めておくことも有用
- クラウドなら検証環境で気軽にトライ＆エラーができ、低リスクで新しいことが始められる
- 既存の環境との併用も可能

# IPv6の利用ドキュメントもご用意してあります

[https://docs.aws.amazon.com/ja\\_jp/vpc/latest/userguide/get-started-ipv6.html](https://docs.aws.amazon.com/ja_jp/vpc/latest/userguide/get-started-ipv6.html)

<https://aws.amazon.com/jp/blogs/networking-and-content-delivery/dual-stack-ipv6-architectures-for-aws-and-hybrid-networks/>

<https://aws.amazon.com/jp/vpc/ipv6/>

Amazon VPC での IPv6 の使用開始

PDF | RSS

次のステップで  
成する方法につ  
この演習を完了

- IPv6 CIDR  
VPC を作成  
上の必要に  
は、インタ  
ネットです
- 特定のポー  
タンスに作
- サブネット  
をインスタ  
ンススタンス

aws

お問い合わせ サポート 日本語 アカウント コンソールにサインイン

製品 ソリューション 料金 ドキュメント 学ば パートナーネットワーク AWS Marketplace カスタマーサポート イベント

Amazon VPC 概要 特徴 料金 開始方法 リソース よくある質問

製品 / ネットワークとコンテンツ配信 / Amazon VPC

## IPv6

IPv6 でアプリケーションのスケールを実現する

AWS PrivateLink が IPv6 のサポートを開始

IPv6 の使用は年々増加しており、多くの新しいネットワーク構成でデフォルトになりつつあります。IPv6 のリーダーになることで、最新のネットワーク上でアプリケーションを管理および配信できます。AWS では、エンドツーエンドの IPv6 接続を活用するグローバル環境を設計およびデプロイできます。デュアルスタックおよび IPv6 専用仮想ネットワーク環境でアプリケーションをホストし、IPv6 を介して Amazon VPC 全体およびインターネットとの間の接続を提供できます。AWS では 2011 年から IPv6 をサポートしており、2021 年現在、IPv6 専用サブネットや EC2 インスタンスなどの IPv6 専用機能、IPv6 から IPv4 への変換をサポートする NAT ゲートウェイ、IPv6 をターゲットとする Elastic Load Balancer、Amazon EKS の IPv6 サポートなどを備えています。これらの機能により、既存の IPv4 ワークロードとの下位互換性を維持しながら、IPv6 で高度にスケーラブルなアーキテクチャを構築することにより、ビジネスの成果を実現できます。

### 利点

**シンプルなアーキテクチャとコスト削減**

AWS での IPv6 は、変換メカニズムの必要性を最小限に抑えることで、ウェブアーキテクチャを簡素化します。また、プライベート IPv4 アドレスを使用して複雑なアーキテクチャを構築し、制約のあるパブリック IPv4 アドレスを回避する必要性がなくなります。

**IPv4 空間の制限を超えてスケールする**

AWS でのアプリケーションのスケールリングは、VPC 内の IPv4 アドレスの数によって制限されなくなりました。IPv6 を使用することで、管理しやすい連続した IP 範囲をマイクロサービ스에割り当てることができ、VPC 内のアプリケーションを事実上無制限にスケールリングできます。

**グローバルな到達可能性を拡大する**

インターネットに接続するデバイスが急増しており、その多くが IPv6 アドレスを使用するようになっています。AWS 上のアプリケーションを IPv6 互換にすることで、エンドツーエンドのネイティブ IPv6 を実行できるようになりました。

IPv6 on AWS

Best practices for adopting and designing IPv6-based networks on AWS

October 26, 2021



# Thank you!

菊地 信明

アマゾン ウェブ サービス ジャパン合同会社  
シニア ソリューション アーキテクト  
ネットワーク スペシャリスト



# 【参考】 個別サービスの対応状況



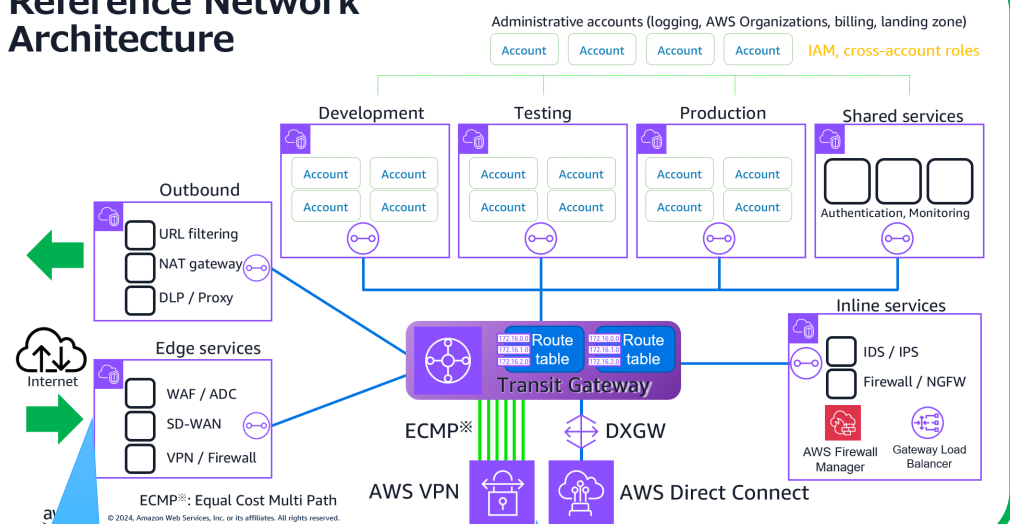
# Amazon VPC (Virtual Private Cloud)



仮想プライベートクラウドサービス

ハンズオンで利用

## Reference Network Architecture



インターネット  
ゲートウェイ

VPN  
or  
専用線

## 特徴

(<http://aws.amazon.com/jp/vpc/>)

- AWS上にプライベートネットワークを構築
- AWSと既存環境のハイブリッド構成を実現
- きめ細かいネットワーク設定が可能

BYOIPv6に対応

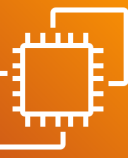
## 価格体系

(<http://aws.amazon.com/jp/vpc/pricing/>)

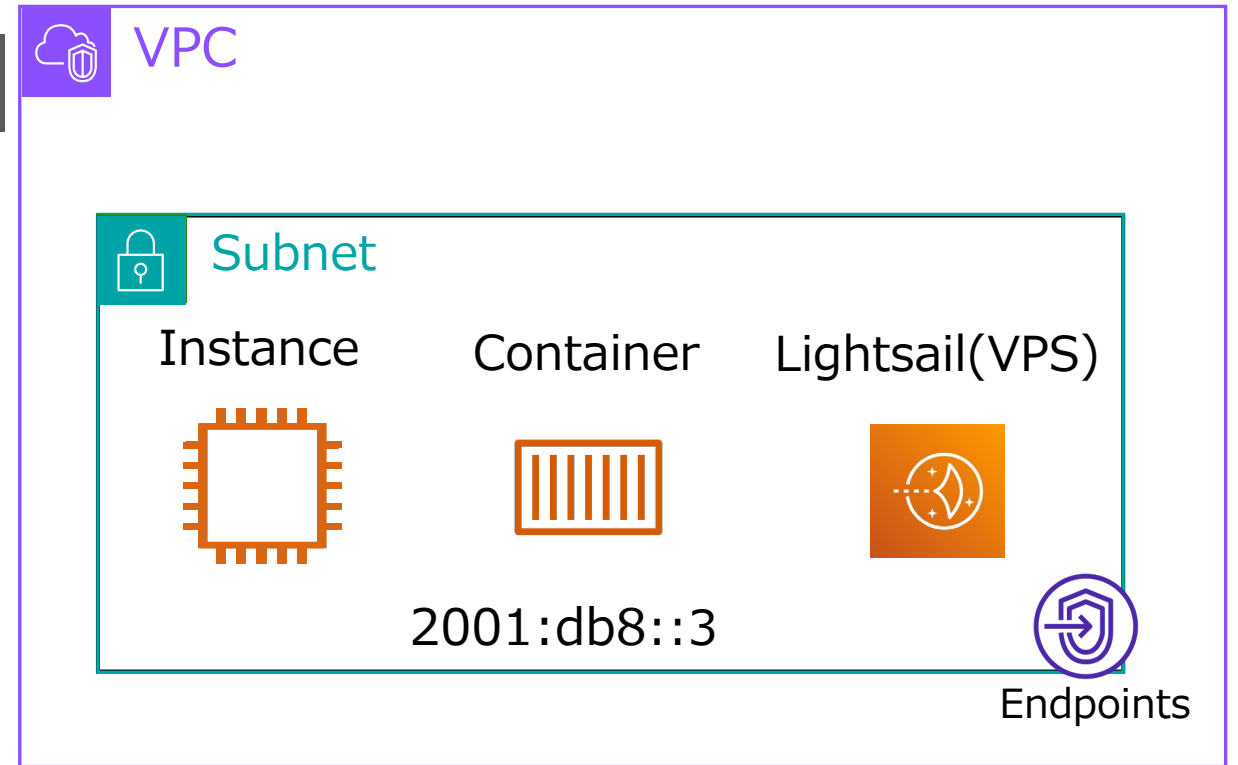
- VPCの利用は無料



# コンピュートリソース



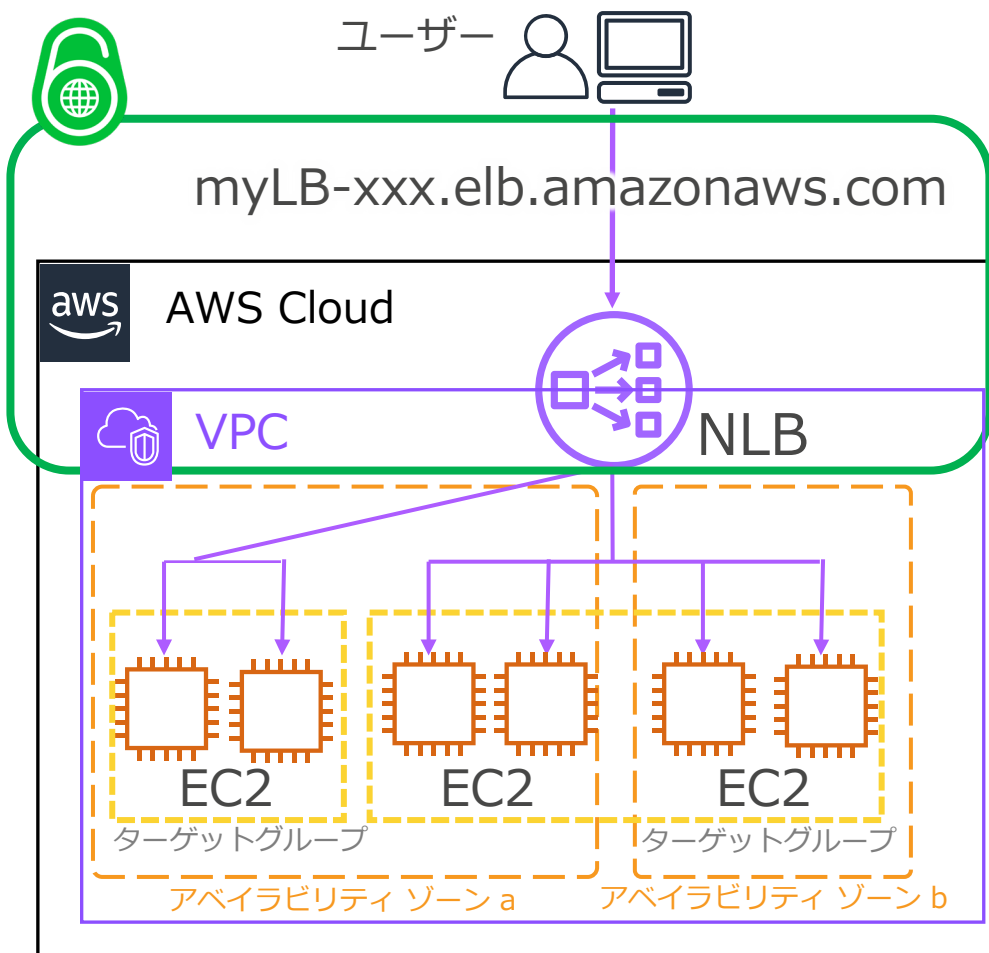
- 三種類のコンピュートリソースが対応
  - 仮想マシン(EC2) **ハンズオンで利用**
  - コンテナ(ECS)
  - VPS(Lightsail)
- APIコールを行うVPC EndpointもIPv6に対応



# Network Load Balancer (NLB)



レイヤー4のコネクションベースのロードバランサー



**特徴** (<https://aws.amazon.com/jp/elasticloadbalancing/network-load-balancer/>)

- TCP、UDP(L4)のバランサーとして機能
- TCPがIPv6対応
- 固定IPアドレス: AZ毎に1つ、既に持っているEIPも利用可能
- 送信元IPアドレスの保持: X-Forwarded-ForやProxy Protocolが不要
- 暖気なしに急激なスパイクにも対応可能
- SSLオフロード

**価格体系** (<https://aws.amazon.com/elasticloadbalancing/pricing/>)

- NLBの起動時間
- Load Balancer Capacity Units (LCU)の使用量

# Gateway Load Balancer (GWLBE)



L3ゲートウェイとL4ロードバランサの機能を兼ね備えた新タイプのロードバランサ

## 特徴

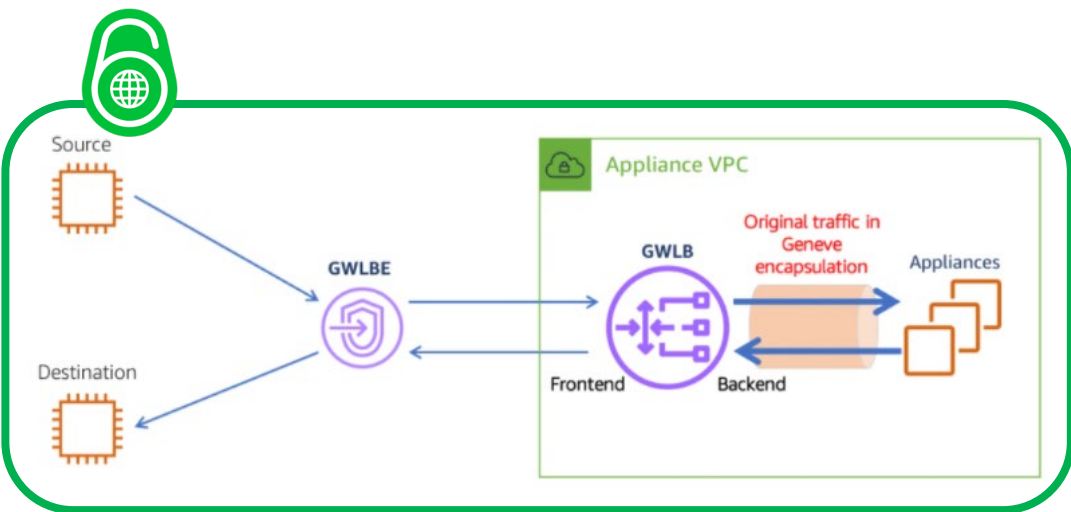
(<https://aws.amazon.com/jp/elasticloadbalancing/gateway-load-balancer/>)

- Gateway Load Balancerエンドポイント(GWLBE)に入るトラフィックをGWLBへ配送し、アプライアンスが稼働するEC2へ転送
- ネットワークトラフィックに対して透過型
- サードパーティアプライアンスのAZ冗長に活用
- 送信元/送信先IPアドレスの保持
- 急激なスパイクにも対応可能

## 価格体系

(<https://aws.amazon.com/elasticloadbalancing/pricing/>)

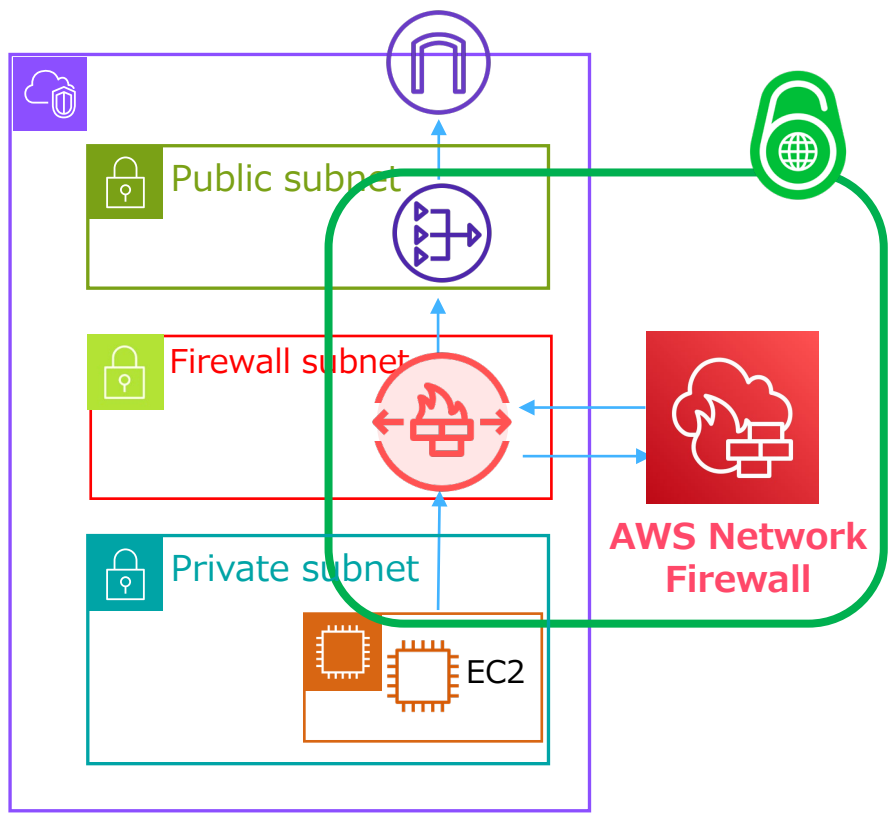
- NLBの起動時間
- Load Balancer Capacity Units (LCU)の使用量
- Gateway Load Balancerエンドポイントの利用料としてPrivateLinkの利用料が加算



# AWS Network Firewall (ANF)



VPCのサブネットに配置するマネージドファイアウォールサービス



## 特徴 (<https://aws.amazon.com/jp/network-firewall/>)

- 100 Gbpsまでスケールアウト
- AWSマネージドルールの他、サードパーティ製ルールの利用も可能
- StatelessとStatefulルール組み合わせによりトラフィックを制御する
- Domain Listによるフィルタリングが可能
- オープンソースのSuricata互換形式のルールを利用可能
- Transit Gatewayの専用アタッチメントに対応

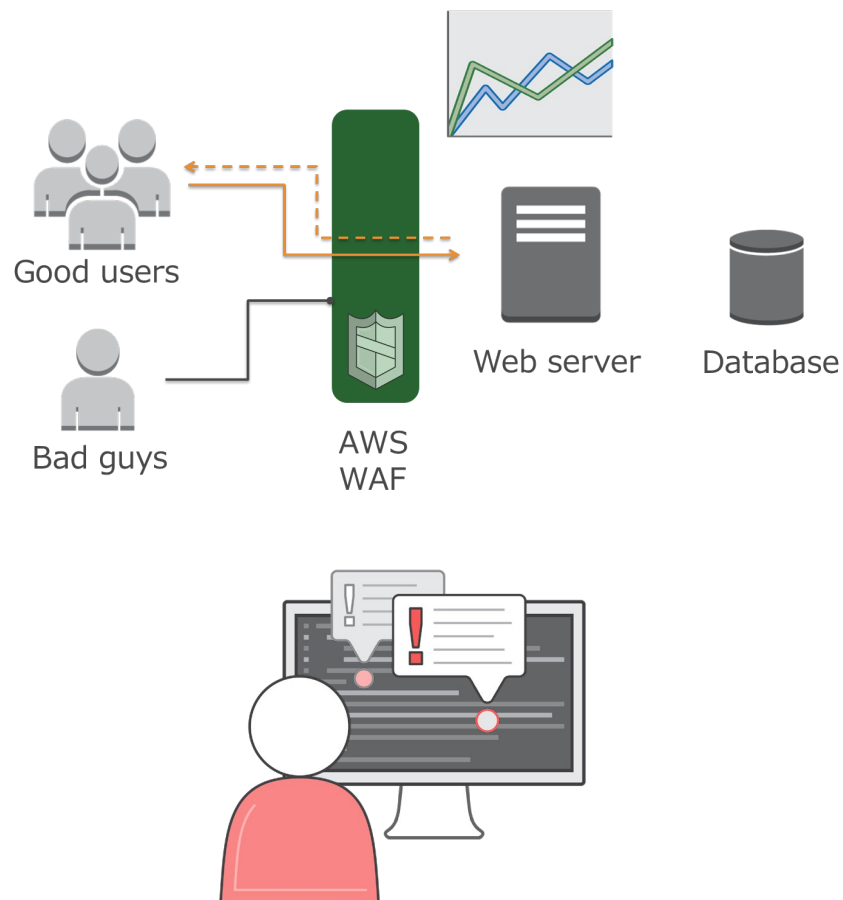
## 価格体系 (<https://aws.amazon.com/elasticloadbalancing/pricing/>)

- Endpointの起動時間
- Network Firewallのデータ処理料
- NAT Gateway(NGW)と併用した場合、NGWの利用料を免除

# AWS WAF(Web Application Firewall)



AWSが提供するウェブアプリケーションファイアウォール



## 特徴 [\(https://aws.amazon.com/jp/waf/\)](https://aws.amazon.com/jp/waf/)

- カスタムルールによるアクセス制御を実現
- SQLインジェクションやXSS攻撃などへの対応が可能。APIを利用した動的なルールの変更もサポート



CloudFrontとALB(Application Load Balancer)、APIGWで利用できる

## 価格体系 [\(https://aws.amazon.com/jp/waf/pricing/\)](https://aws.amazon.com/jp/waf/pricing/)

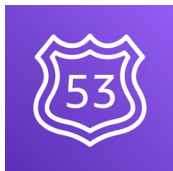
- ウェブACLの数とルール数
- リクエスト数

# Amazon Route 53 **ハンズオンで利用**



高い可用性と豊富な機能を提供するフルマネージドな権威DNS

## Route53の特徴的な機能



- 各ネームサーバは冗長化され世界中に分散配置。
- IP Anycast
- ヘルスチェック/DNSフェイルオーバー
- 重み付けラウンドロビン
- レイテンシーベースルーティング
- ジオルーティング
- ドメイン取得と管理
- AAAA, Query in IPv6
- DNSSEC
- DNS64

## 特徴 (<http://aws.amazon.com/jp/route53/>)

- 高い可用性：Amazon Route53は世界中に配置されたサーバーによって、非常に高い可用性を提供
- 多様な機能：管理ホストに対するヘルスチェックや様々なアルゴリズムによるラウンドロビンなど、柔軟なアプリケーションの運用を助ける機能が豊富
- アプリケーションの内部DNSとしても利用可能

## 価格体系 (<http://aws.amazon.com/jp/route53/pricing/>)

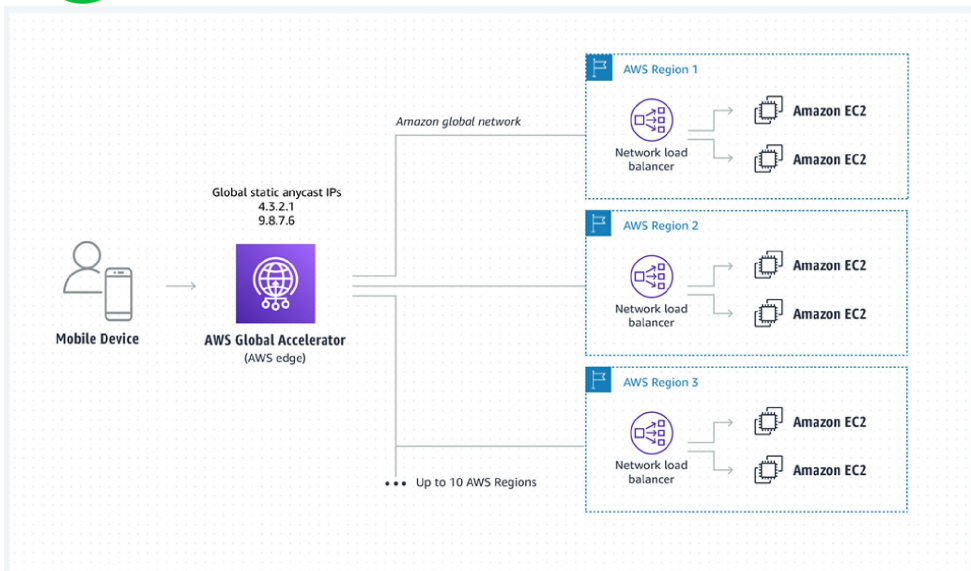
- 非常に低価格なのが特徴。
- ホストするゾーンあたり 0.5USD/月
- 標準クエリ: 10億クエリあたり0.4USD



# AWS Global Accelerator



IPv6トラフィックをデュアルスタックのApplication Load Balancer エンドポイントにルーティング



## 特徴 (<https://aws.amazon.com/jp/global-accelerator>)

- パフォーマンス向上：AWのグローバルネットワークインフラを利用して、ユーザーのトラフィックのパフォーマンスを最大 60% 向上させるネットワーキングサービス
- マルチリージョン対応：マルチリージョンアプリケーション向けの、簡素化した回復力のあるトラフィックルーティング
- 固定IP要件：IPv4/6でそれぞれ2つの静的 IP を提供

## 価格体系 (<https://aws.amazon.com/jp/global-accelerator/pricing/>)

- 固定料金とプレミアムデータ転送料金で構成
- アクセラレーターあたり18 USD/月
- データ転送料：送信元/先リージョン毎に定義