



AWS-IPv6ハンズオン Advance

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

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
技術統括本部 ネットワークソリューション部
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

- AWSのネットワーク関連サービス
- IPv6対応サービス
- 最近のIPv6関連アップデート
- IPv6環境における注意点

2. IPv6対応ネットワークを作る

- Client VPCの作成
- NAT64/DNS64の設定・動作確認
- IPv6 Only Subnet/Webの作成
- DNSでIPv6をFQDNに登録
- NLBを導入してアクセス先IPアドレスを固定化

3. フォローアップ、QA

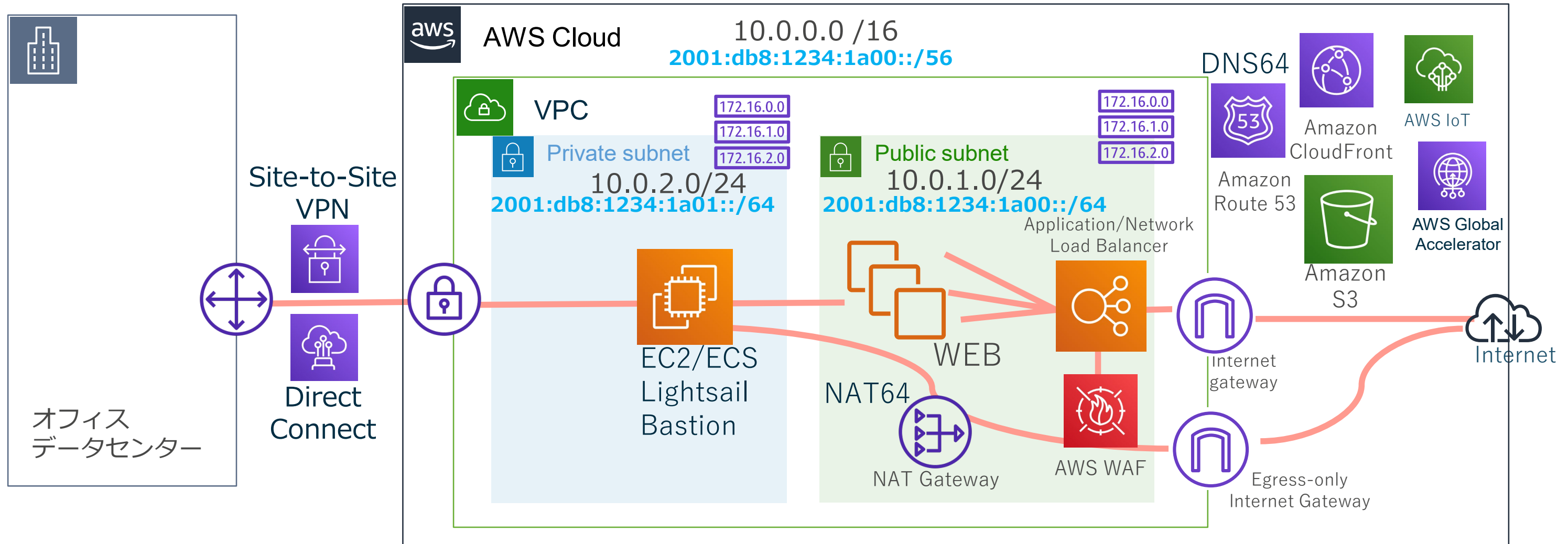
AWSの ネットワーク関連サービス



現在のIPv6対応状況



IPv6の対応 VPC、EC2、ELB、CloudFront、WAF、Route53、Global Accerator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

- IPv4がデフォルト、IPv6 はオプトイン。

VPC：

- IPv4のみ
- デュアルスタック



<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

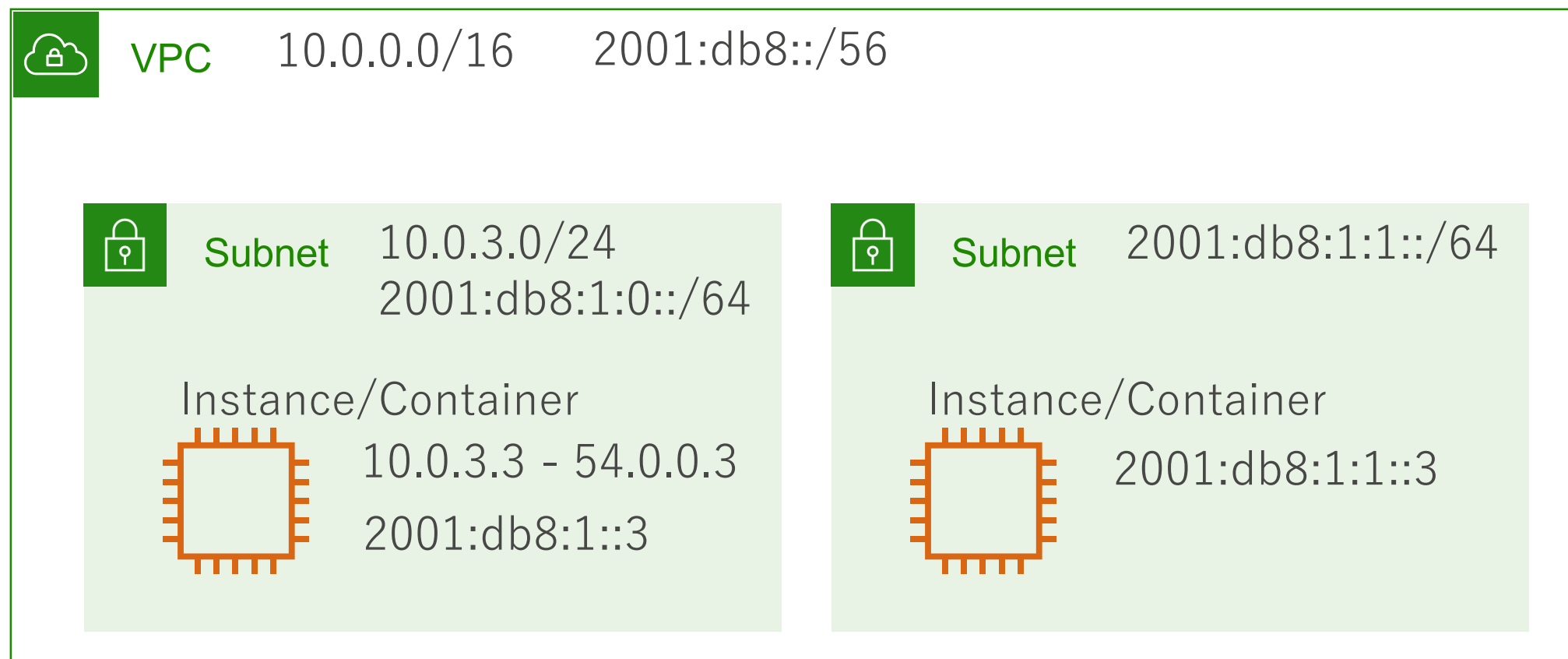
サブネット：

- デュアルスタック
- IPv4のみ
- IPv6のみ

<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

コンセプト : IPv6 in Amazon VPC/Subnet

- IPv6をオプトインし、有効化した場合には、VPC自体はデュアルスタック
- 持ち込んだIPv6アドレスも利用できる。(BYOIPv6)
- 要件に応じて、IPv6のみのサブネットを作ることにも可能



コンセプト：IPv6グローバルユニキャストアドレス

- 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)を使う。
 - 割り当てられるIPv6アドレスは、Amazonから割り当てられるか、持ち込んだIPv6アドレス(BYOIPv6)を使う。
- それぞれのインスタンスはGUAが付与される
- 1：1のNATは存在しない

参考：デュアルスタック環境でのipコマンド実行例

IPv4 Address

IPv6 Address

```
[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
```

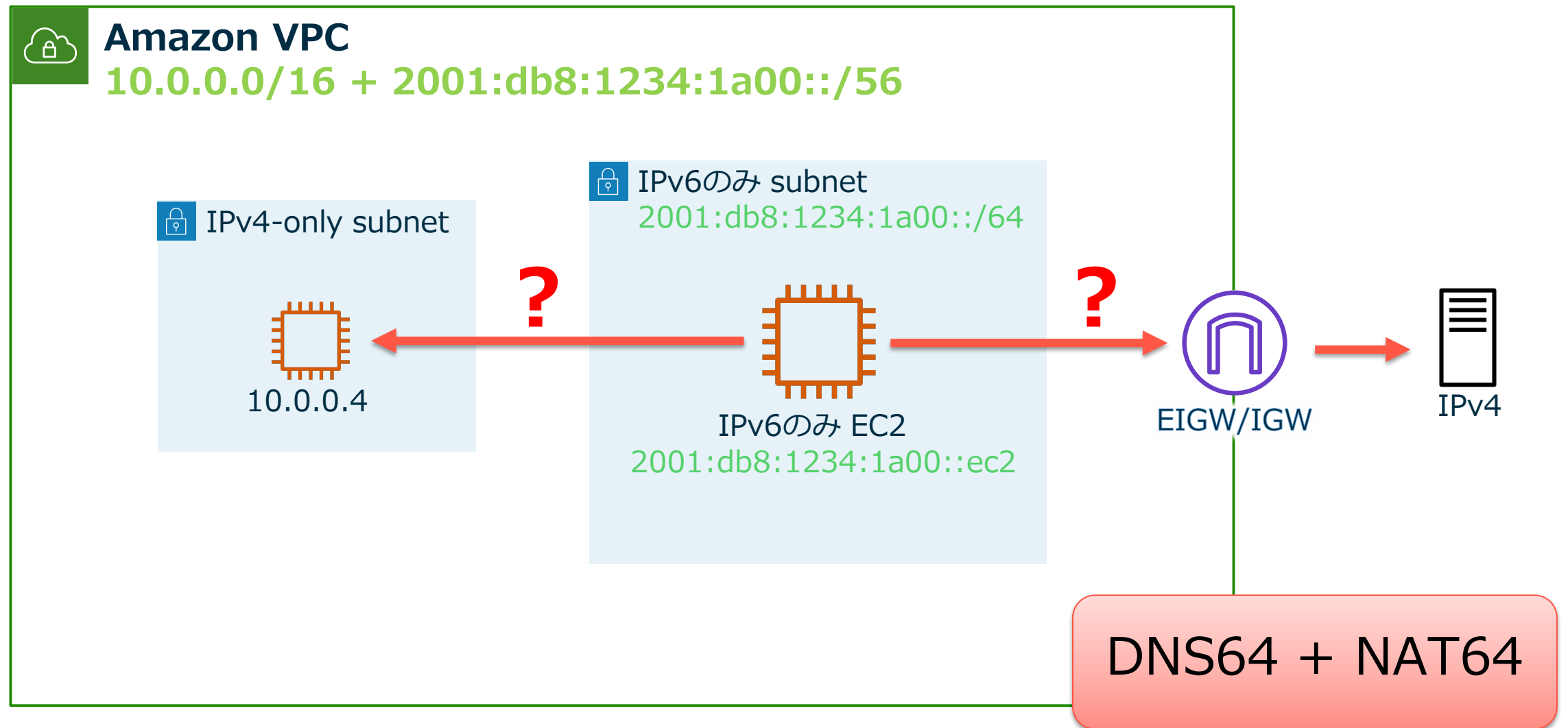
参考 : IPv6 Only環境でのipコマンド実行例

IPv4 Address
(Link Local)

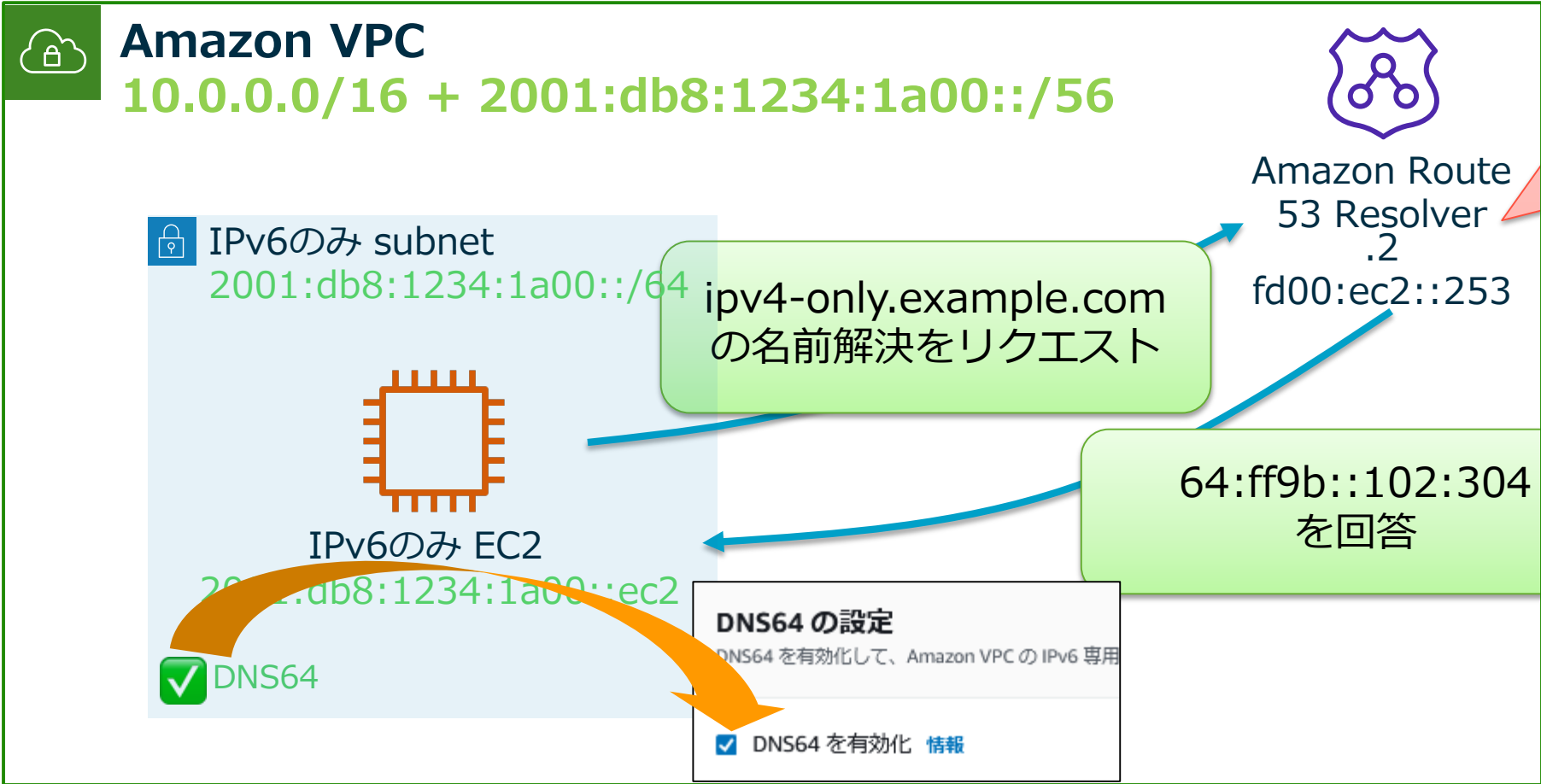
IPv6 Address

```
[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
```

DNS64/NAT64紹介



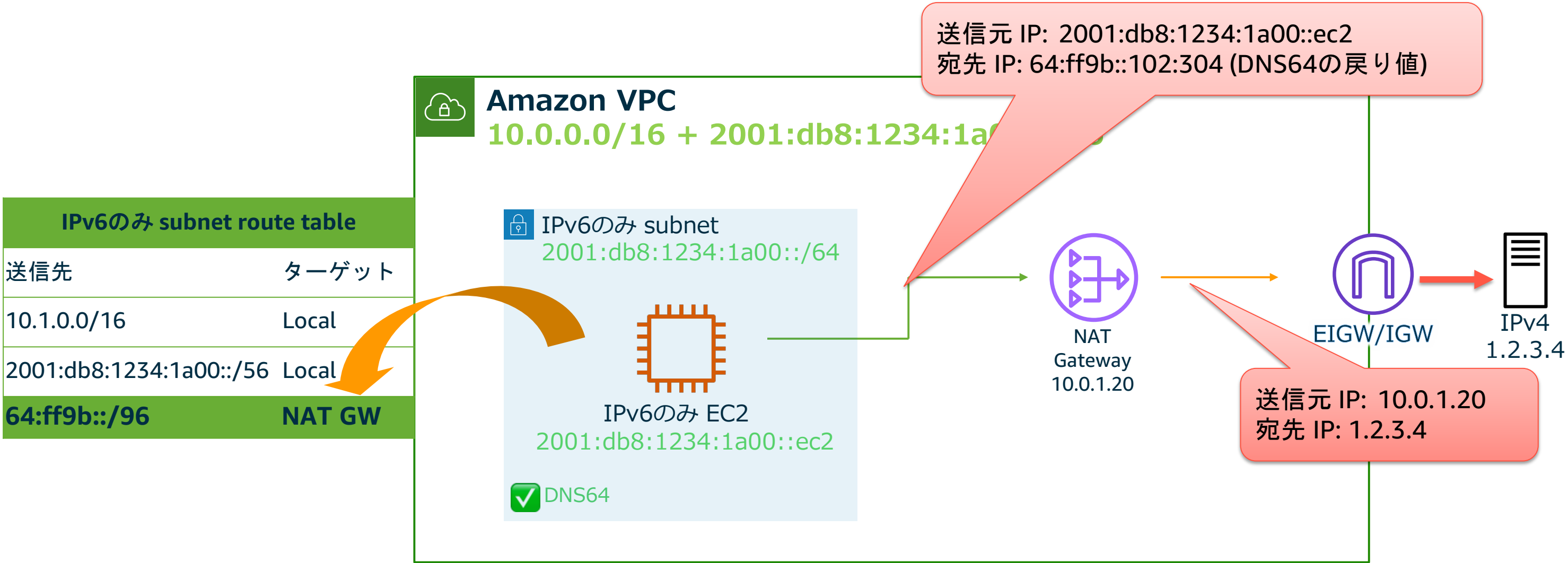
DNS64の動き



レコード内のIPv4アドレスの先頭にRFC6052で定義された"64:ff9b::/96"を付けてIPv6アドレスを合成して返す。

		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



個別サービスの対応状況



Amazon VPC (Virtual Private Cloud)



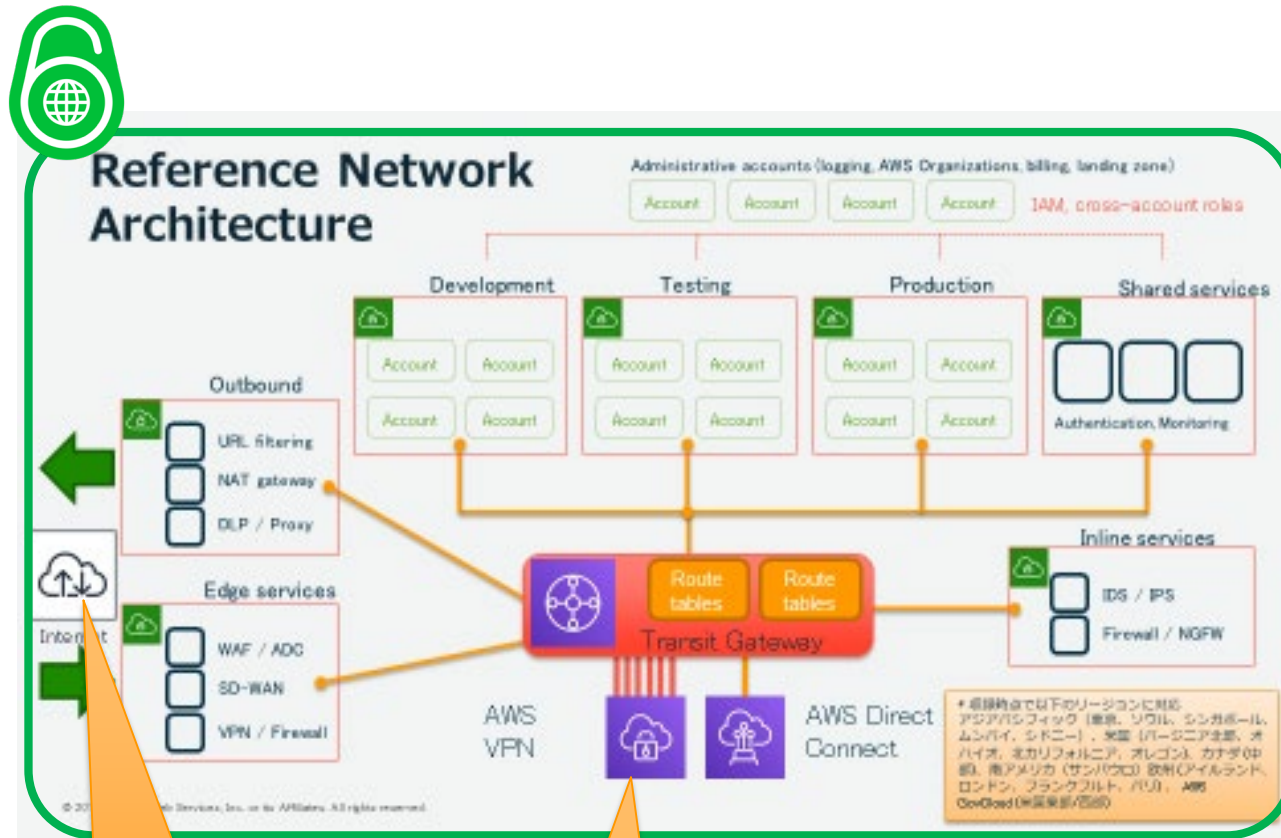
仮想プライベートクラウドサービス **ハンズオンで利用**

特徴 [\(http://aws.amazon.com/jp/vpc/\)](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 [\(http://aws.amazon.com/jp/vpc/pricing/\)](http://aws.amazon.com/jp/vpc/pricing/)

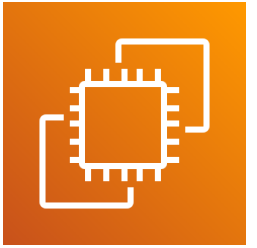
- VPCの利用は無料



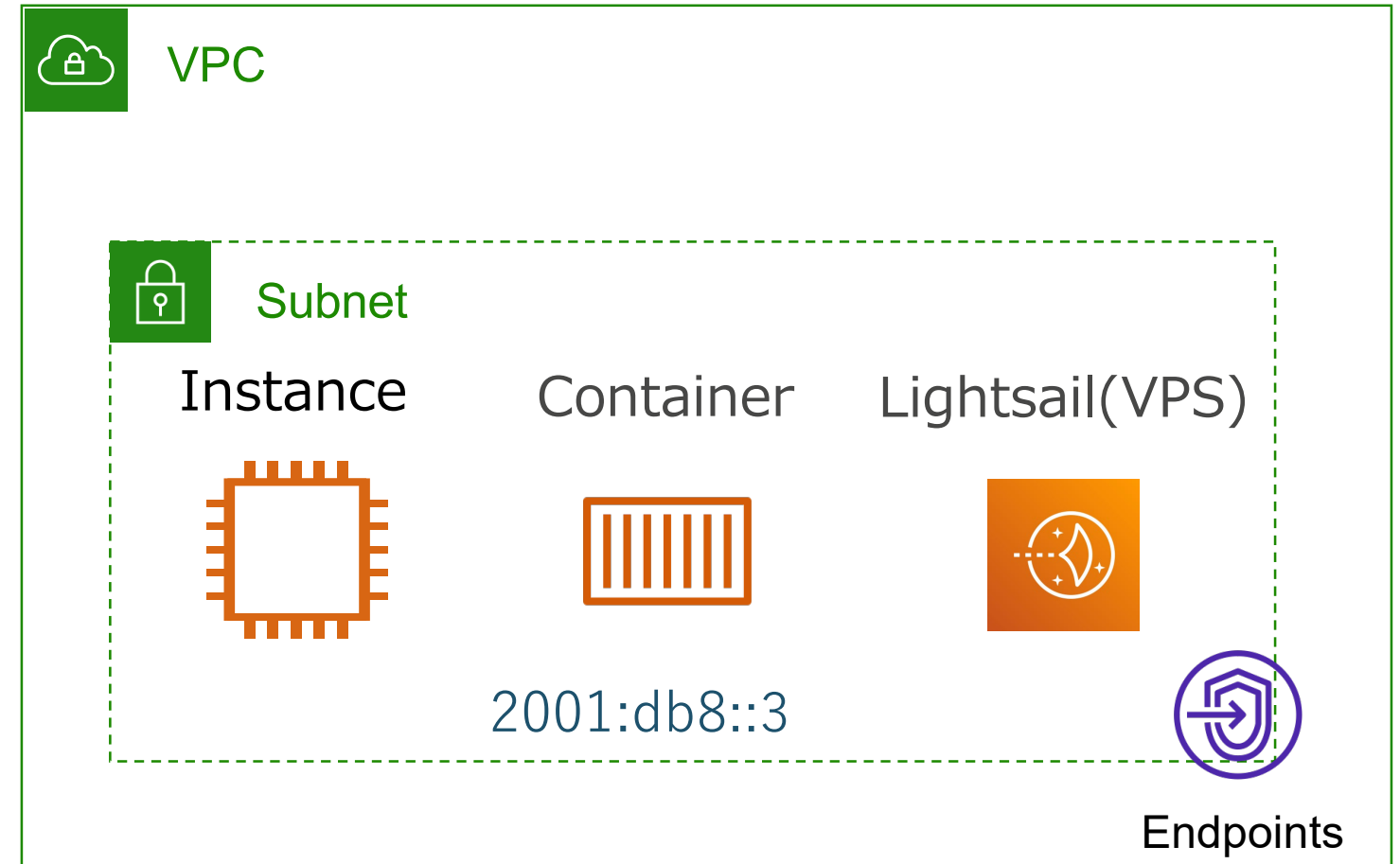
インターネット
ゲートウェイ

VPN
or
専用線

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

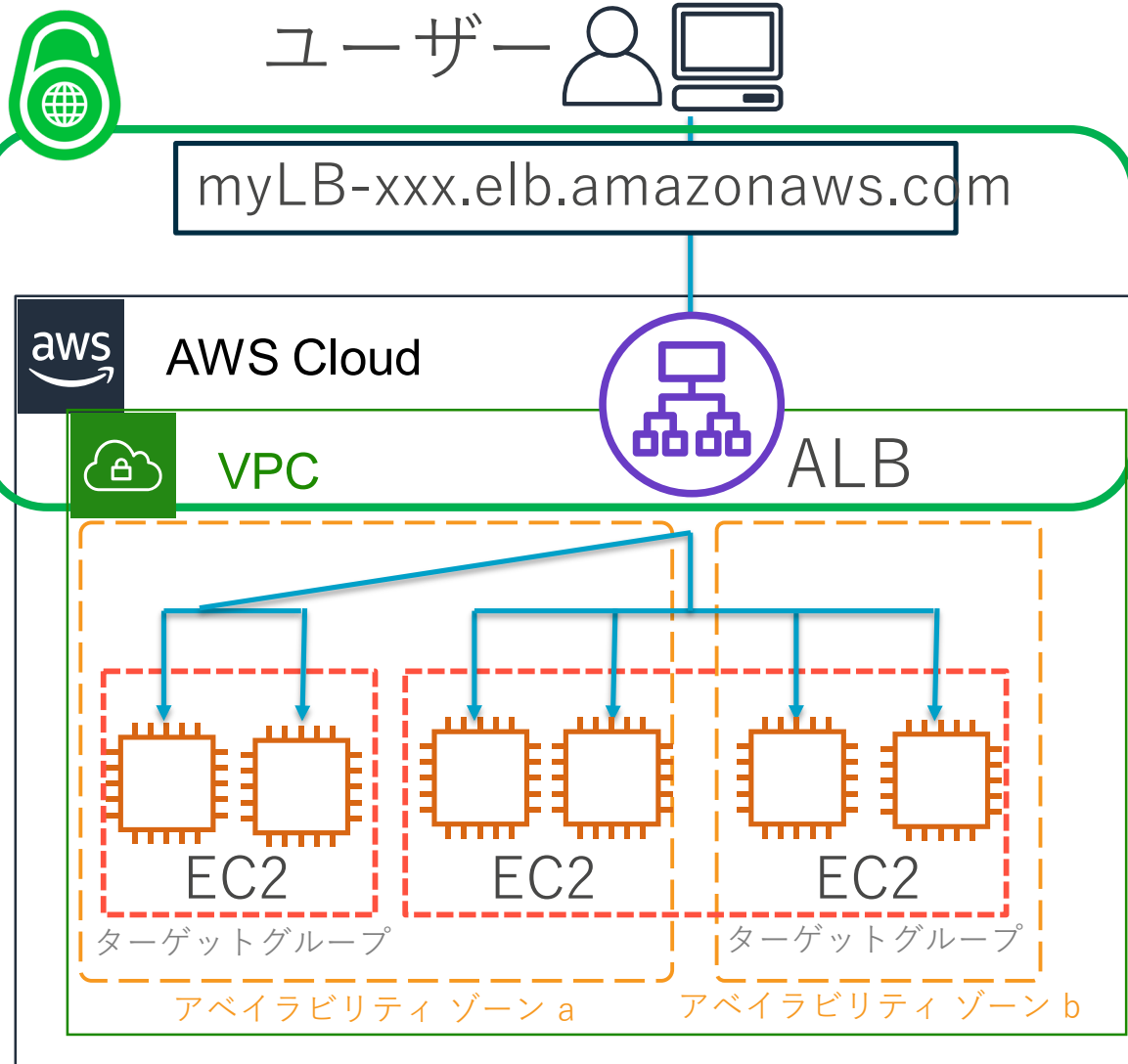


Application Load Balancer (ALB)

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/>)

- 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

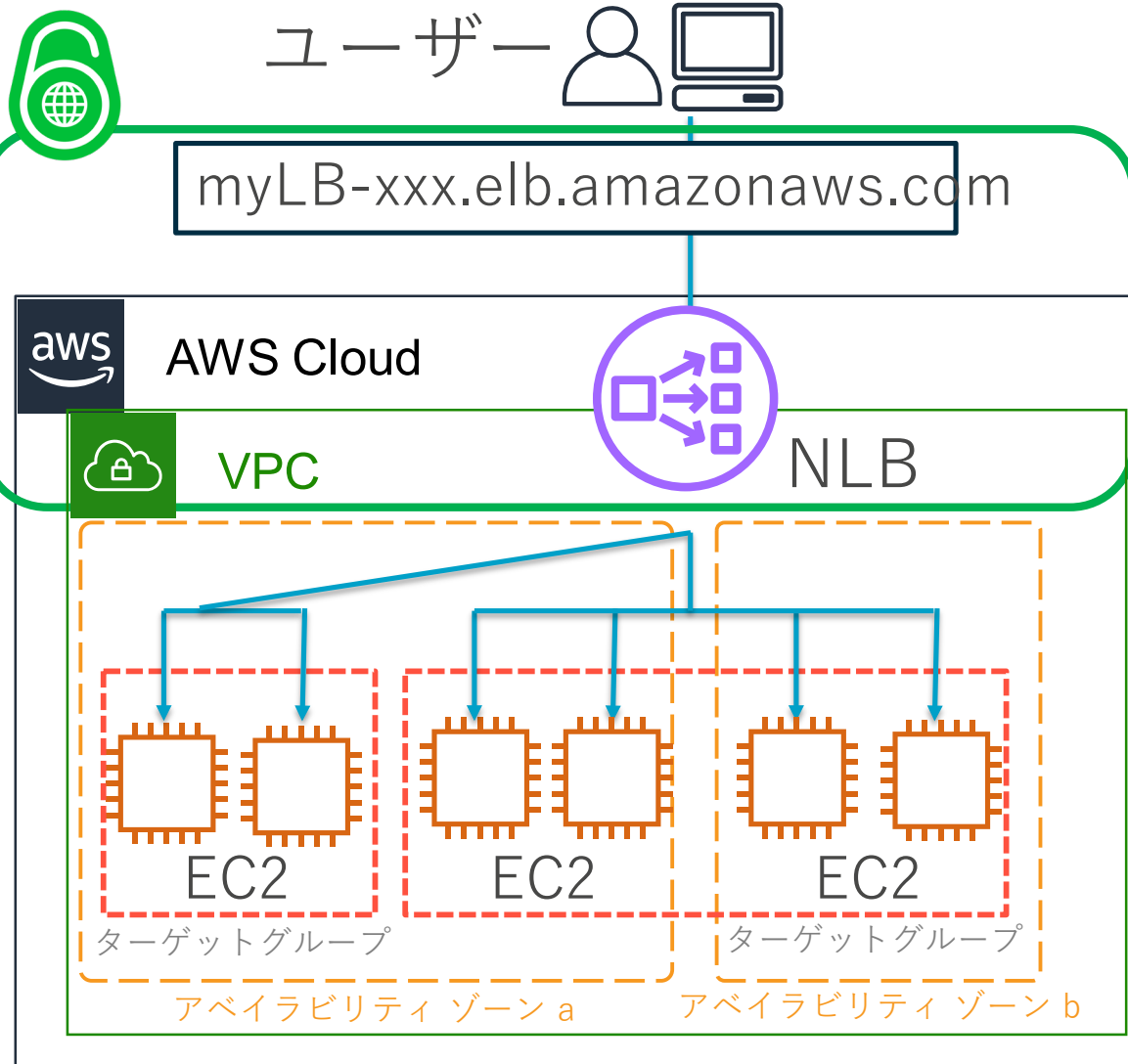
(<https://aws.amazon.com/jp/elasticloadbalancing/applicationloadbalancer/pricing/>)

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

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 [\(https://aws.amazon.com/jp/elasticloadbalancing/network-load-balancer/\)](https://aws.amazon.com/jp/elasticloadbalancing/network-load-balancer/)

- TCP、UDP(L4)のバランサとして機能
 - 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 [\(https://aws.amazon.com/elasticloadbalancing/pricing/\)](https://aws.amazon.com/elasticloadbalancing/pricing/)

- NLB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

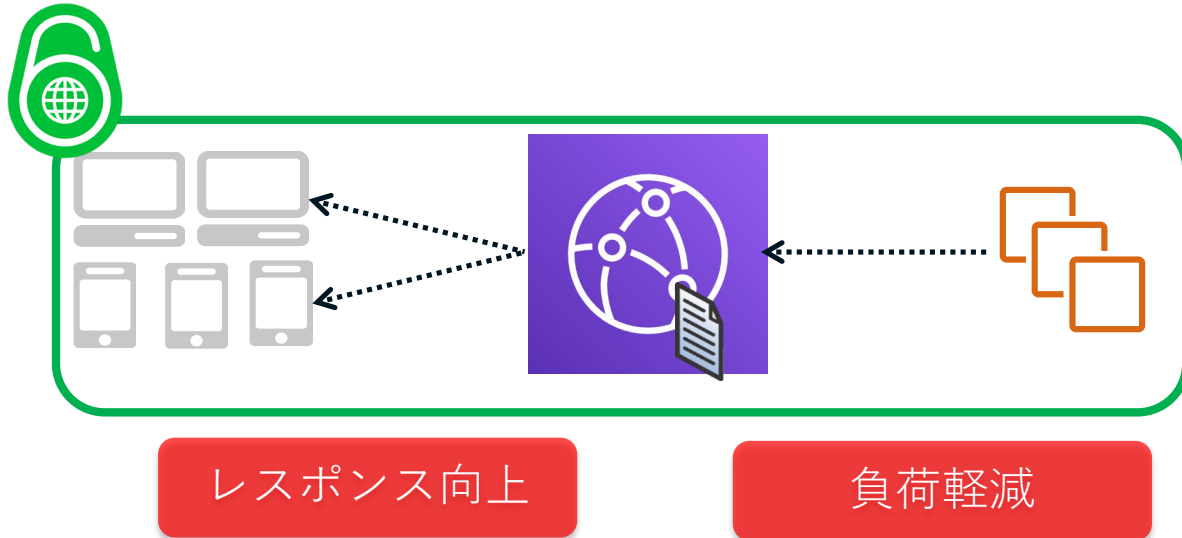
(<http://aws.amazon.com/jp/cloudfront/>)

- 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275箇所以上のPOP

価格体系

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

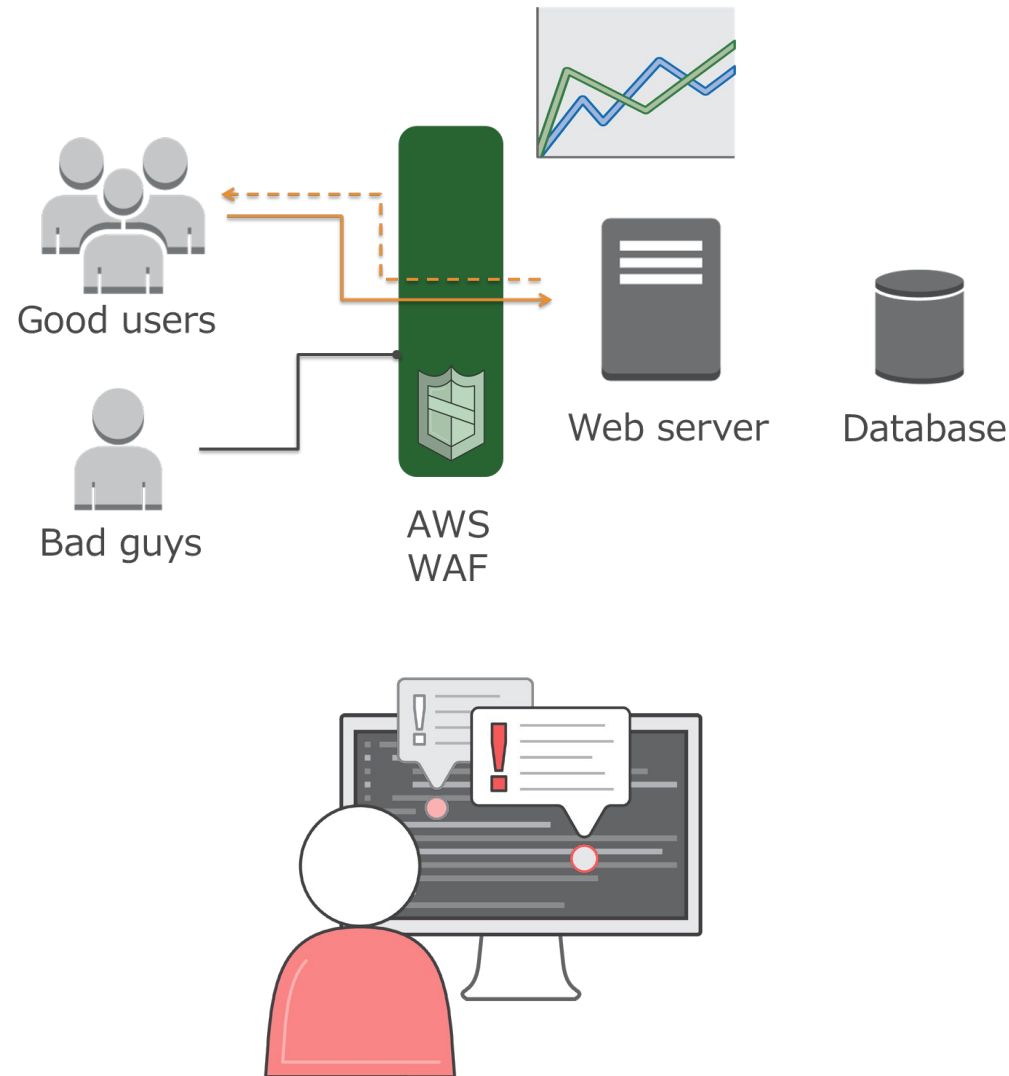
- データ転送量(OUT)
- HTTP/HTTPSリクエスト数
- (利用する場合)SSL独自証明書 など



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/>)

- 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

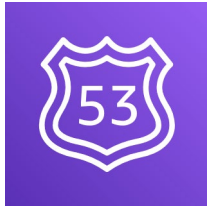
価格体系 (<https://aws.amazon.com/jp/waf/pricing/>)

- ウェブACLの数とルール数
- リクエスト数



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

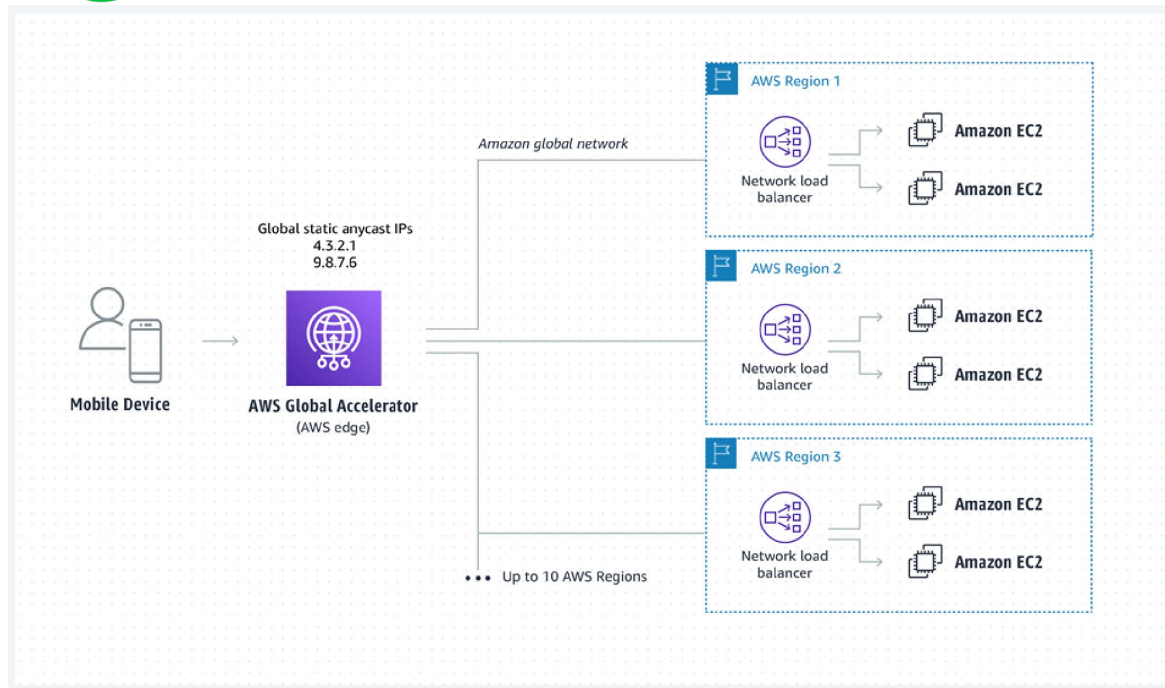
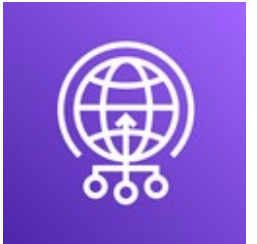
(<http://aws.amazon.com/jp/route53/pricing/>)

- 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

NEW

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：AWS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

IPv6環境を AWS上で利用する上での注意点



IPv6環境をAWS上で利用する上での注意点

- 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）
- ルートテーブル、ゲートウェイは別途設定する。
- 特に、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する。
- 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。

セキュリティグループ、ルートテーブル、NACL

- IPv6もIPv4も同様に設定、動作する

Example Security Group Rules

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

Example Route Table

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

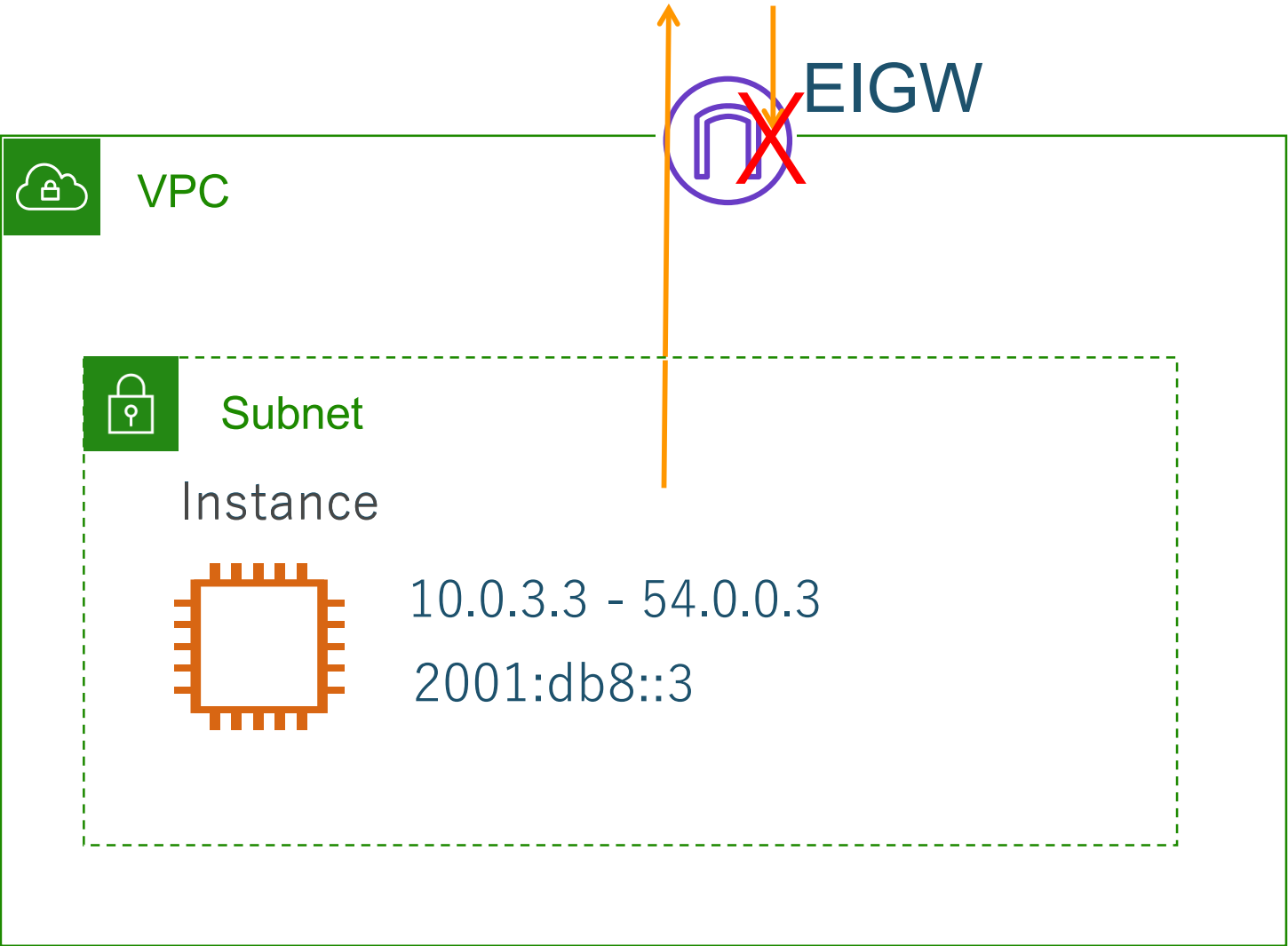
Egress-only Internet Gateway

- IPv6経由でのアウトバウンドに限定したインターネットアクセスのための仮想デバイスを導入
- 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

Example Route Table

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	active

IPv6通信はアウトバウンドのみ可能となる



DNSリソースレコード登録

- 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Quad A（AAAA）を併記する

Example Record

<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. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. 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

デュアルスタックのWebサイトを公開する際の考慮

- 最終的にIPv4とIPv6のどちらを利用して接続するかは、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？

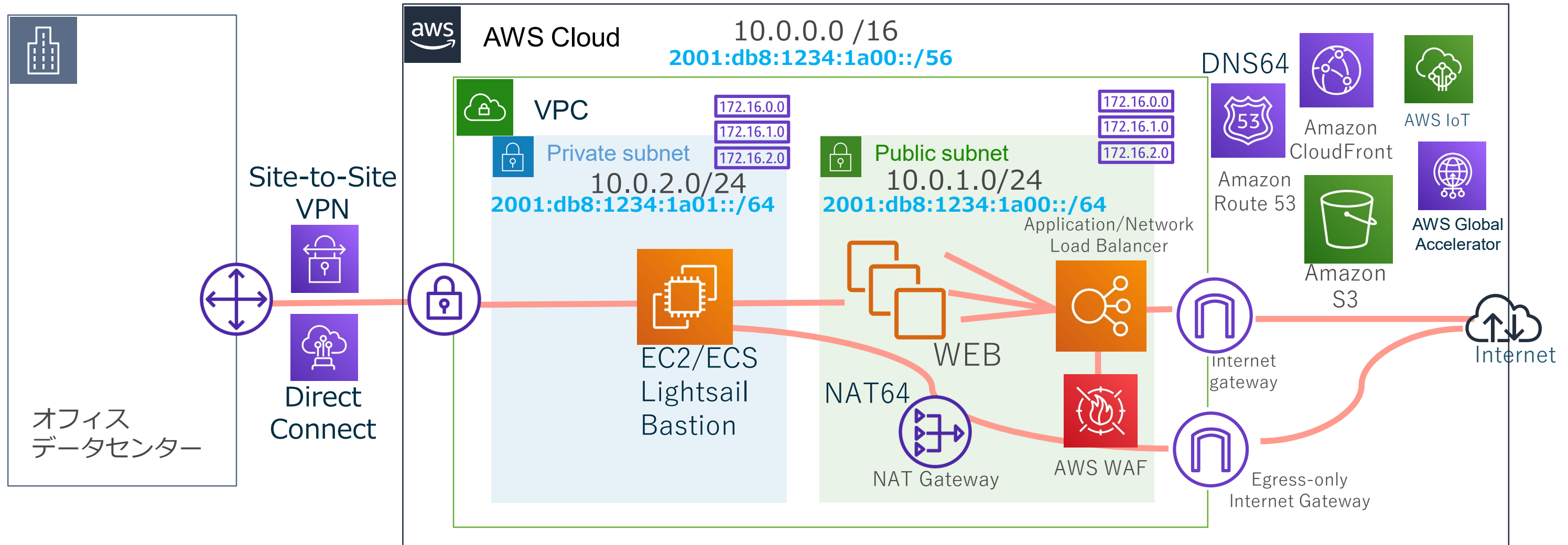
<https://www.nic.ad.jp/sc-hiroshima/program/nakagawa.pdf#page=15>

- 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

まとめ



IPv6の対応 VPC、EC2、ELB、CloudFront、WAF、Route53、Global Accerator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

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

<https://d1.awsstatic.com/whitepapers/IPv6-on-AWS.pdf>



aws このガイド内で検索 日本語 コンソールにサインインする

AWS > ドキュメント > Amazon VPC > ユーザーガイド フィードバック 設定

Amazon Virtual Private Cloud ユーザーガイド

Amazon VPC とは?
Amazon VPC の仕組み

▼ 開始方法

IPv6 の使用開始

- ▶ Amazon VPC コンソールウィザードの設定
- ▶ VPC の例
- ▶ VPC とサブネット
デフォルト VPC とデフォルトサブネット
- ▶ セキュリティ
- ▶ VPC のネットワーキングコンポーネント
- ▶ Amazon EC2 ネットワーキングコンポーネント


Amazon VPC での IPv6 の使用開始

PDF | RSS

次のステップでは、IPv6 アドレス指定をサポートする VPC を作成する方法について説明します。

この演習を完了するには、以下の作業を行います。

- IPv6 CIDR ブロックと 1 つのパブリックサブネットを作成します。サブネットを使うと、インターネットに接続する必要がある場合にグループ化することができます。インターネットゲートウェイを通してインターネットです。
- 特定のポートのみからトラフィックを許可するセキュリティグループを作成します。
- サブネット内に Amazon EC2 インスタンスを起動し、インターネットに接続できるようにします。



aws Contact Us

Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace

Blog Home Category Edition Follow

RELATED POSTS

- Connect Amazon S3 File Gateway using AWS PrivateLink for Amazon S3
- Field Notes: How to Scale Your Networks on Amazon Web Services
- Improving Performance and Reducing Cost Using Availability Zone Affinity
- Protect and manage Dell EMC PowerScale data on Amazon S3
- Automate Networking foundation in multi-account environments


Networking & Content Delivery

Dual-stack IPv6 architectures for AWS and hybrid networks

by Alexandra Huides | on 18 OCT 2021 | in Amazon VPC, Networking & Content Delivery, Technical How-to | Permalink | Share

Introduction

An increasing number of organizations are adopting IPv6 in their environments, driven by the public IPv4 space exhaustion, private IPv4 scarcity, especially within large-scale networks, and the need to provide service availability for IPv6-only clients. An intermediary step in the path to fully supporting IPv6 are dual-stack IPv4/IPv6 designs, which leverage both versions of the IP protocol in parallel.



IPv6 on AWS

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

October 26, 2021

aws



Thank you!