



# Amazon Route 53 Resolver 編

Maya Yamada

Solutions Architect  
2023/05

# 自己紹介

名前：山田 磨耶 (Yamada Maya)

ポジション：Partner Solution Architect

所属：パブリックセクター 技術統括本部

経歴：前職では日系SIerでシステム開発に従事



# 本セミナーの対象者

- Amazon Route53 Resolver をご利用予定の方
- オンプレミス-AWS環境のDNSの設計・実装を担当される方
- AWSのDNSセキュリティ対策を検討される方

# アジェンダ

1. AWSが提供するDNSサービスと機能
2. Amazon Route 53 Resolverの構成
3. DNSクエリログ
4. Route 53 Resolver DNS Firewall

# 1. AWSが提供する DNSサービスと機能

# AWSが提供するDNSサービスと機能

まずは、AWSが提供するDNSサービスの全体像をご紹介します。



Amazon  
Route 53



Amazon  
Route 53 Resolver



Amazon  
Route 53 Resolver  
for Hybrid Clouds

# AWSと名前空間（ゾーン）の整理

AWSのユーザー、コンポーネントは様々な名前空間（ゾーン）を利用

for Internet



Internet  
Public DNS Zone



Amazon Route 53  
Public Hosted Zone

インターネットに公開された  
DNSドメインのゾーン

for Amazon VPC

Amazon-provided  
private DNS hostnames



Amazon Route 53  
Private Hosted Zone

VPCに閉じたプライベート  
ネットワーク内の  
DNSドメインのゾーン

for On-premise

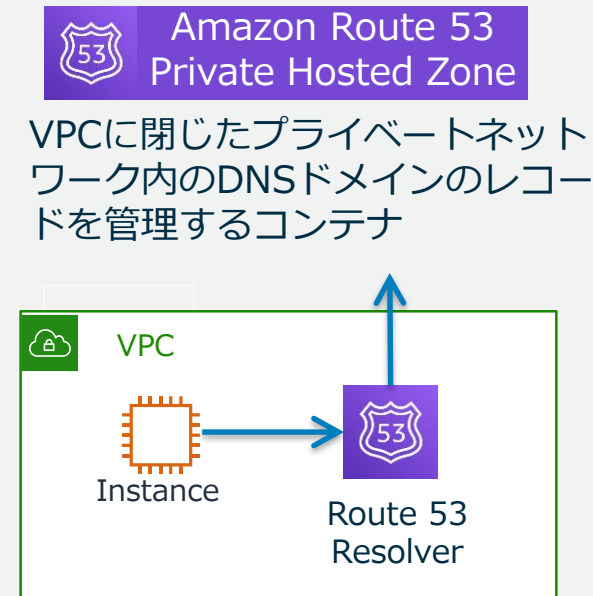
User-managed DNS  
Private Hosted Zone

オンプレミス環境に閉じた  
プライベートネットワーク内の  
DNSドメインのゾーン

【脚注】 各ゾーンの概要説明は末尾に付録として掲載

# Amazon Route 53 (Hosted Zone)

- ネームサーバをマネージドで提供するサービス
- 特定のVPCからの問い合わせと、それ以外からの問い合わせを識別し、異なる応答を返すことができる



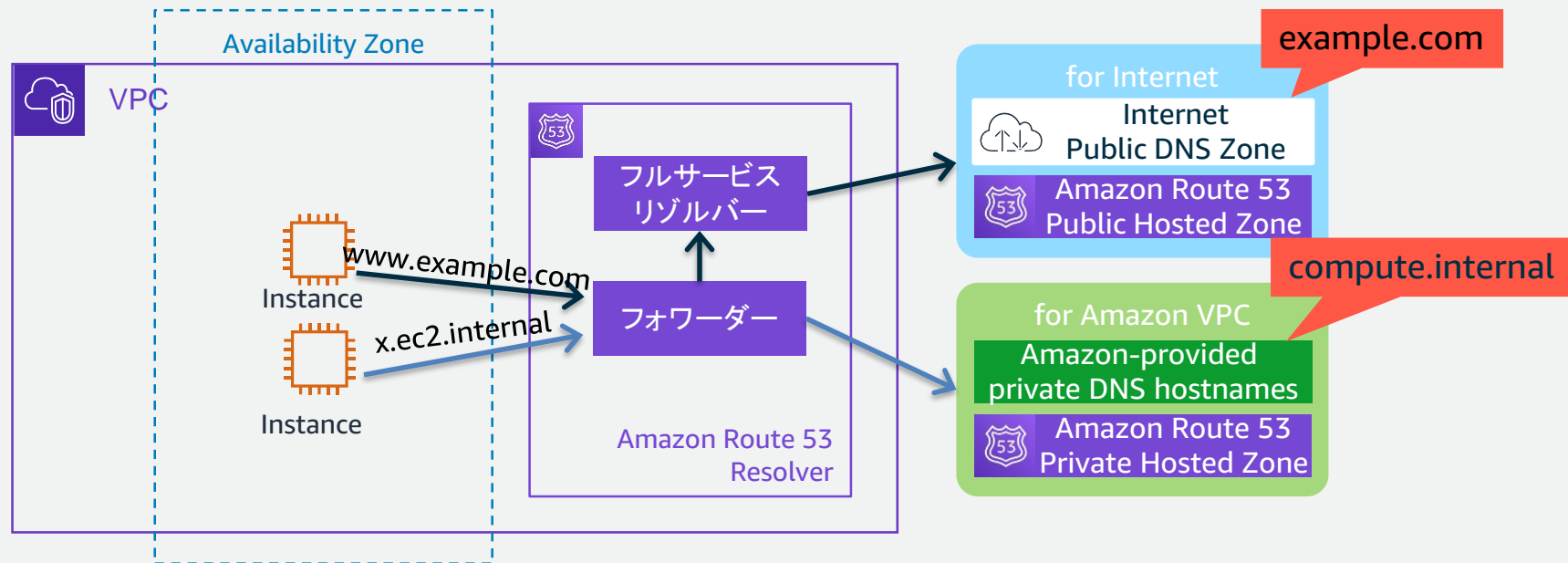


# Amazon Route 53 Resolver

- VPCに標準で備わるDNSサーバー(フォワーダー + フルサービスリゾルバー)
  - VPC+2のIPアドレスでアクセス可能

例：VPCのCIDRが 10.0.0.0/16 の場合、10.0.0.2 でアクセス

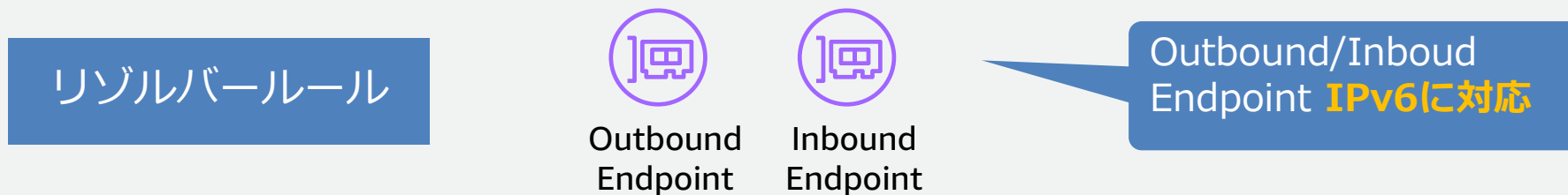
- 以前「.2 Resolver」「Amazon Provided DNS」と呼ばれていたものを改称



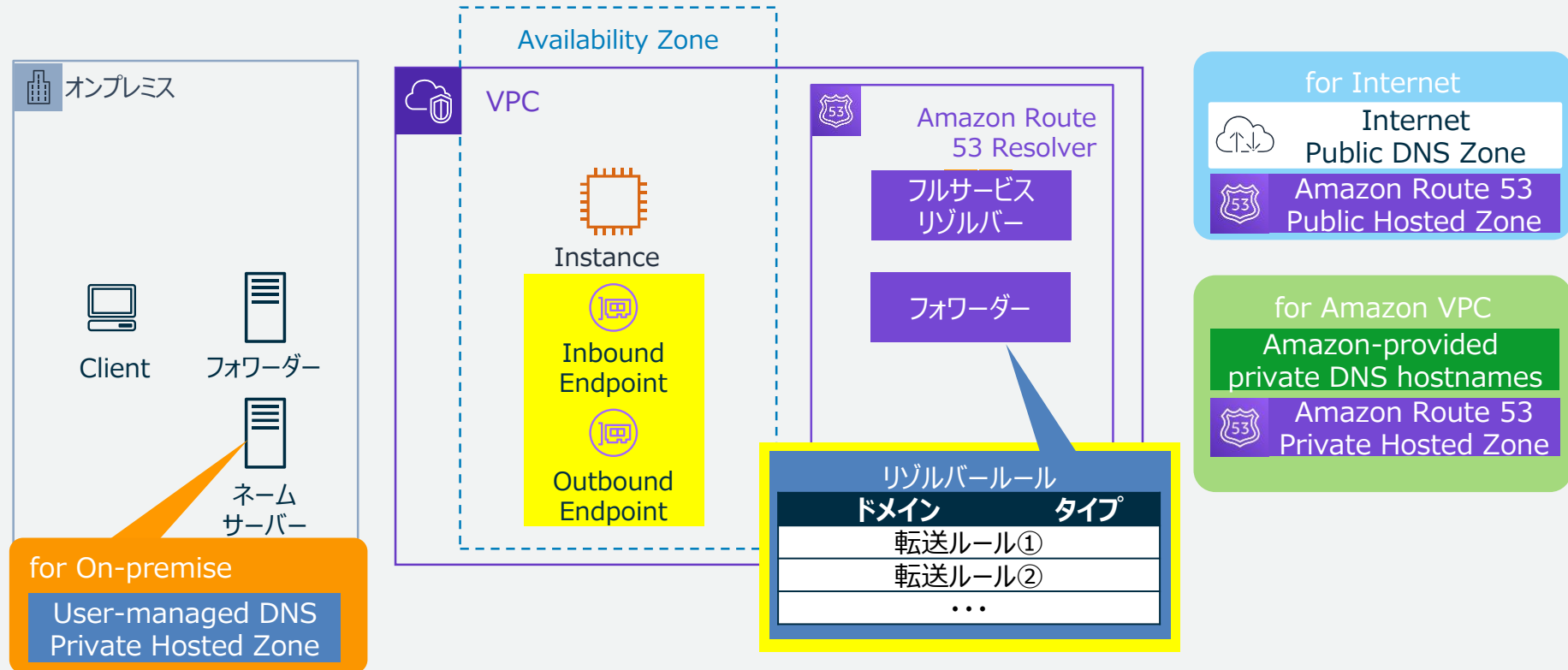
# Amazon Route 53 Resolver for Hybrid Clouds

## ハイブリッド環境の名前解決の一元化を実現

- 以下のユースケースをマネージドサービスで実現する
  - ① オンプレミスからVPC向けゾーンの名前解決
  - ② オンプレミスからインターネット向けゾーンの名前解決
  - ③ VPCからオンプレミス向けゾーンへの名前解決
  - ④ オンプレミスとインターネットで同じドメイン名を利用し、双方のゾーンを併用した名前解決
- コンポーネント

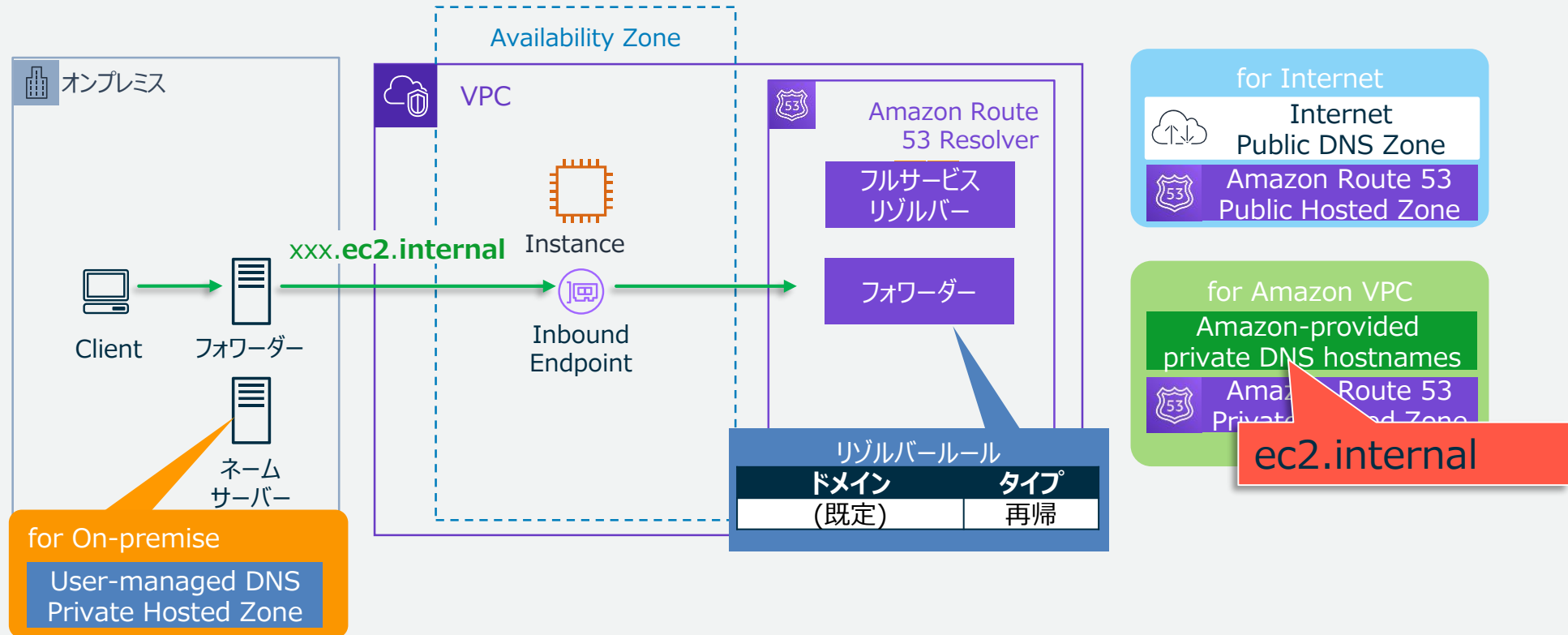


# Route 53 Resolver for Hybrid Clouds Overview



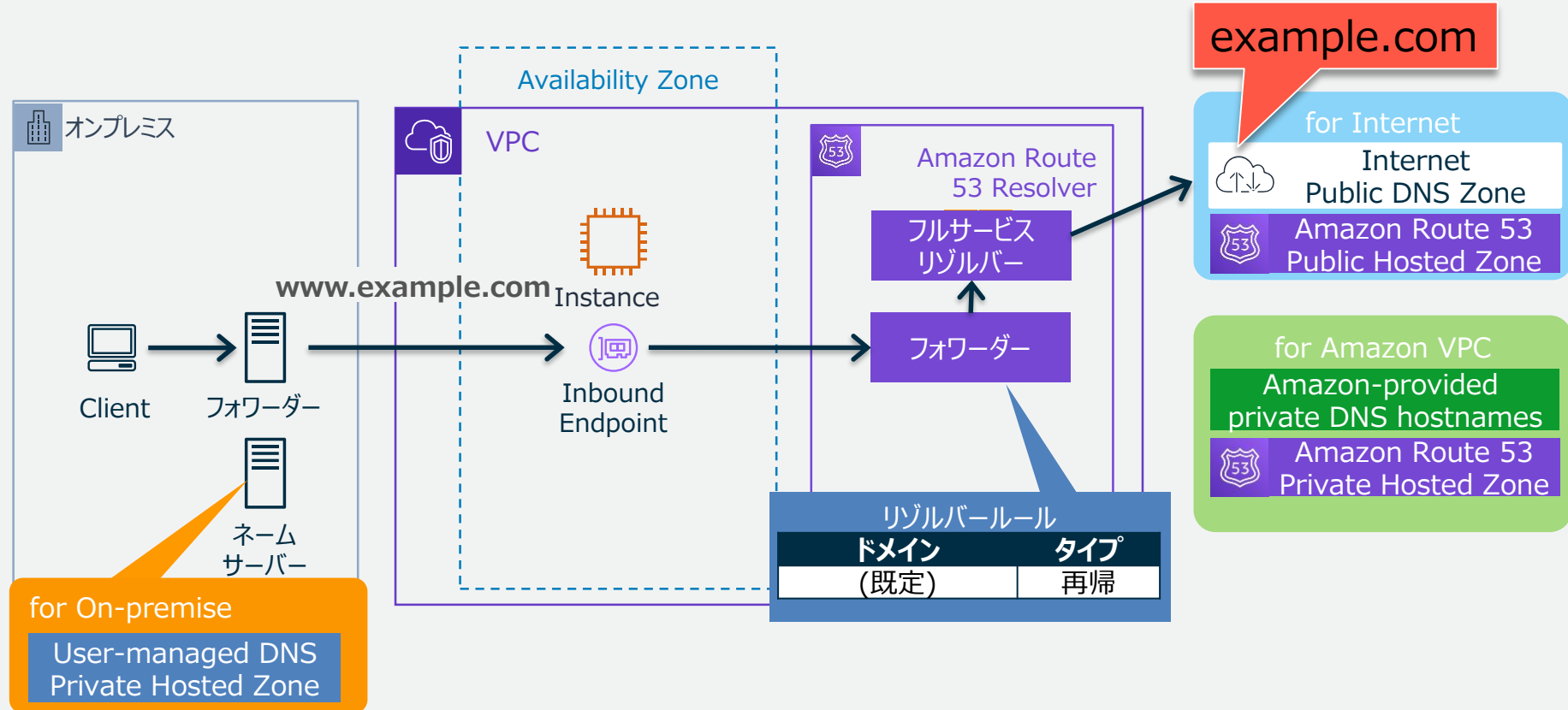
# ユースケース①

## オンプレミスからVPC向けゾーンの名前解決



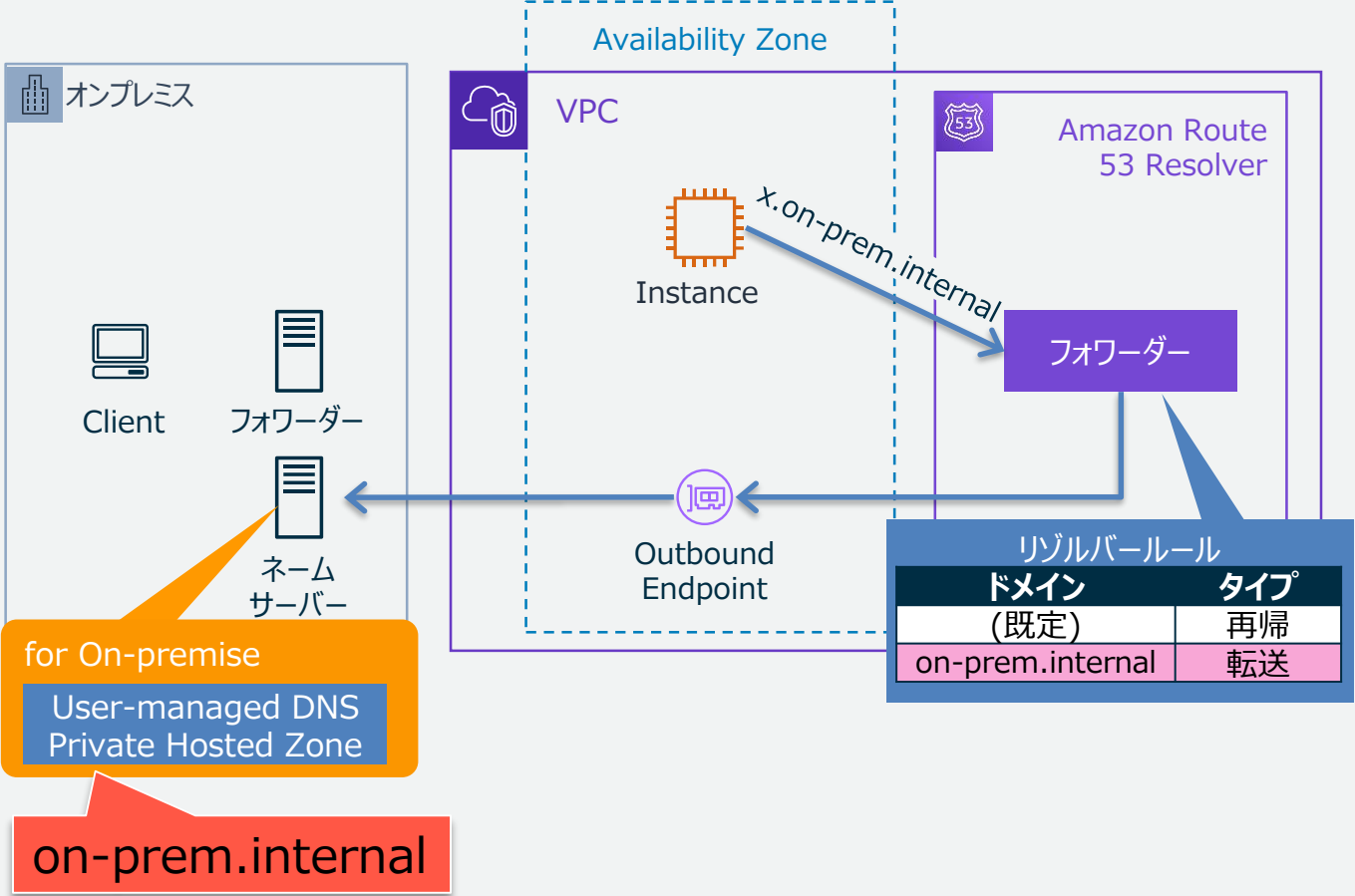
## ユースケース②

### オンプレミス環境からインターネット向けゾーンの名前解決



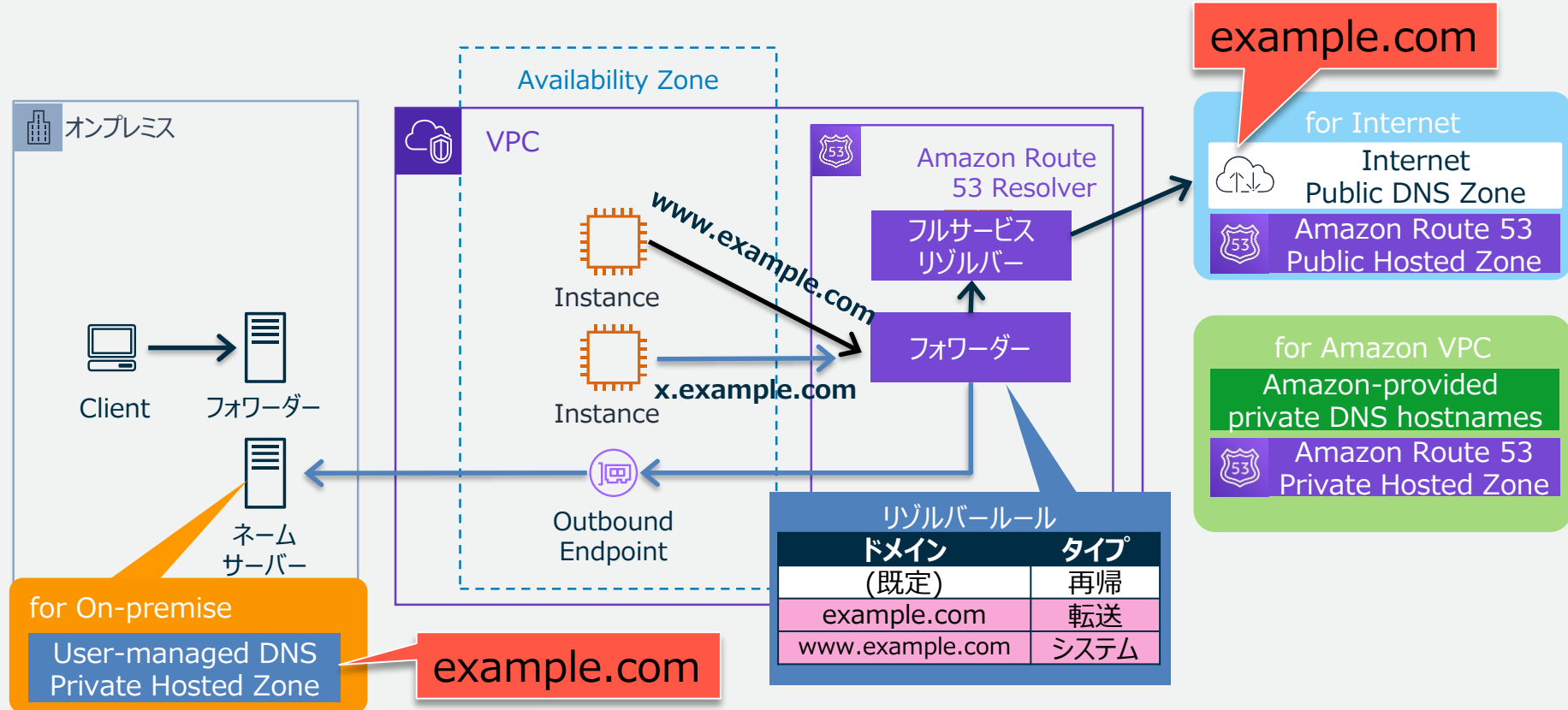
# ユースケース③

## VPCからオンプレミス向けゾーンの名前解決



# ユースケース④

## オンプレミスとインターネットのゾーンを併用した名前解決



# 転送ルールタイプ

どの DNS クエリを Route 53 リゾルバー で別のDNS リゾルバーに転送するか、どのDNSクエリにRoute 53 リゾルバー自体で応答するかをコントロール

## 転送

指定したドメイン名の DNS クエリをネットワークのネームサーバーに転送するルールタイプ。

## システム

リゾルバーが転送ルールで定義されている動作を選択的に上書きするようにするルールタイプ。

## 再帰的

ルールの存在しないドメイン名の再帰リゾルバーとして機能するルールタイプ。  
(既定、削除変更不可)

【参考】 ネットワークへのアウトバウンド DNS クエリの転送

[https://docs.aws.amazon.com/ja\\_jp/Route53/latest/DeveloperGuide/resolver-forwarding-outbound-queries.html](https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/resolver-forwarding-outbound-queries.html)



# VPC内の DNS逆引き

- VPCの設定が以下の場合、Route53 Resolverは逆引きのDNSクエリ向けに自動定義されたシステムルールを自動的に作成する
  - *enableDnsHostnames=true*
  - *enableDnsSupport=true*
- 以下は自動定義されたシステムルールよりも優先される
  - Route53 プライベートホストゾーンの「PTR」レコード
  - Route53 Resolverの転送ルール



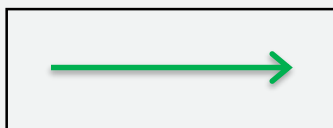
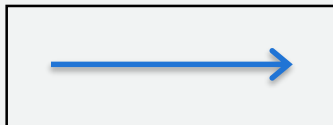
Route53 Resolver の逆引きDNSルールの上書きが可能

【参考】自動定義されたシステムルール

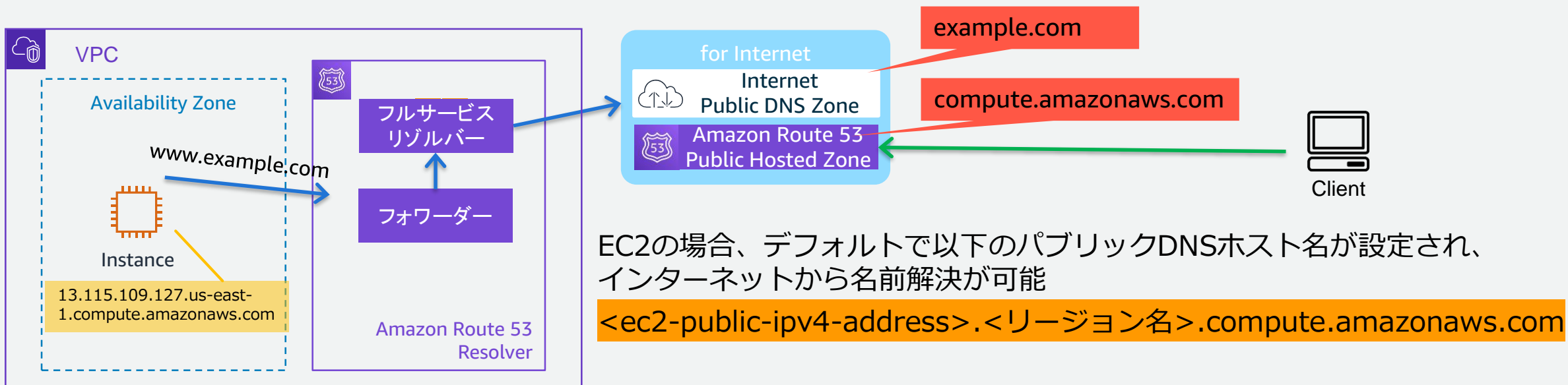
[https://docs.aws.amazon.com/ja\\_jp/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-autodefined-rules](https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-autodefined-rules)

# 注意点：EC2などのAWSリソースの名前解決

以下のような名前解決については、**Inbound/Outbound Endpoint の作成は不要**です



- EC2からインターネットに公開されたドメインへの名前解決（AWS→インターネット）
- インターネットからEC2のパブリックDNSホスト名への名前解決（インターネット→AWS）



# NAT64/DNS64 のサポート

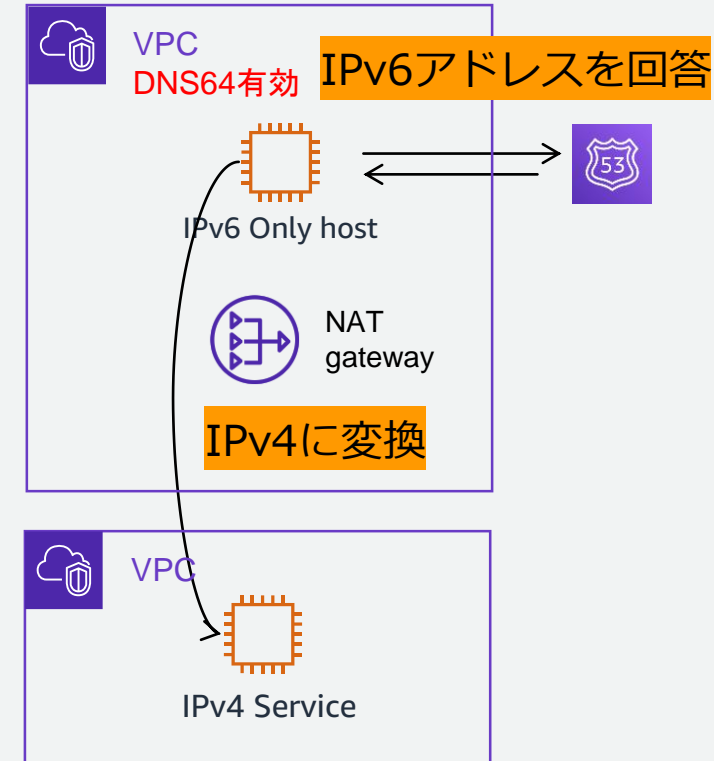
## IPv6 サービスと IPv4 サービス間の通信を実現

- NAT64

- IPv6 から IPv4 へのネットワークアドレス変換を行う
  - ※ IPv4サービスに向かう通信はNAT Gatewayを経由させる
- NAT Gatewayで自動的に機能（設定は不要）

- DNS64

- 名前解決の応答としてIPv6アドレスを返す
  - DNSレコードにIPv6アドレスが存在しない場合は、IPv4アドレスから合成する
- IPv4サービスに接続する全てのサブネットで有効化が必要



# Route 53 Resolver の料金 (2023/5)

- VPC内のインスタンスから発生するDNSクエリは無料
- VPC外からのDNSクエリは受け付けない

# Route 53 Resolver for Hybrid Clouds の料金 (2023/5)

## Inbound/Outboundエンドポイント

- 作成すると0.125ドル/時間の料金が発生

1ヵ月だと…

$0.125 \text{ドル} * 24 \text{時間} * 30 \text{日} = 90 \text{ドル} \div \text{約} \underline{\underline{12,200 \text{円}}}$

## Inbound/Outboundエンドポイントを経由するDNSクエリ

- 最初の10億回まで：百万回毎に0.40ドル
- 10億クエリ超過後：百万回毎に0.20ドル

【Amazon Route 53 料金表】 <https://aws.amazon.com/jp/route53/pricing/>

# AWSが提供するDNSサービスと機能まとめ



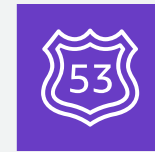
Amazon  
Route 53

- マネージドのネームサーバ
- 特定のVPC向け  
Private Hosted Zone
- インターネットを含む  
特定のVPC以外向け  
Public Hosted Zone



Amazon  
Route 53 Resolver

- Amazon VPCに標準で配備されたDNSサーバー(フォワーダー + フルサービスリゾルバー)



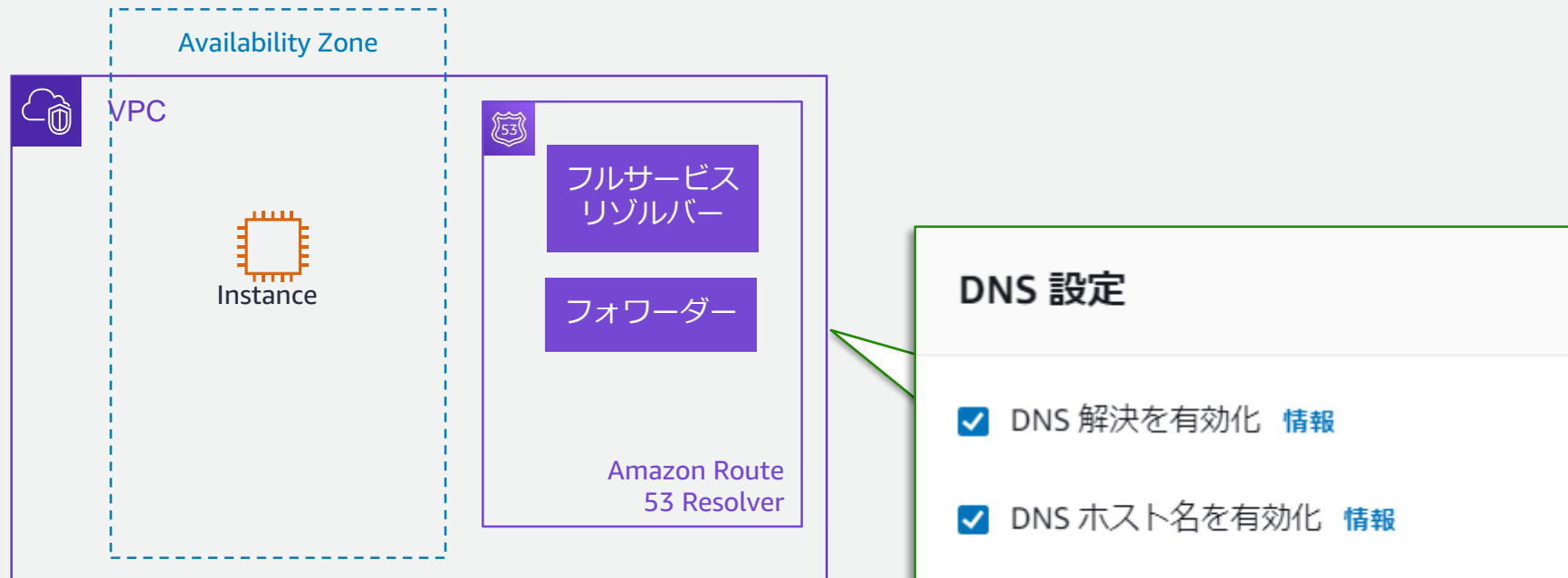
Amazon  
Route 53 Resolver  
for Hybrid Clouds

- ハイブリッド環境の名前解決を一元化する  
Route 53 Resolverの  
拡張機能

## 2. Amazon Route 53 Resolver の構成

# Amazon Route 53 Resolver

- VPC作成時にデフォルトで有効、必要な場合はVPC毎に有効/無効に設定可能
- IPアドレス設定はDHCPで自動的に配布される

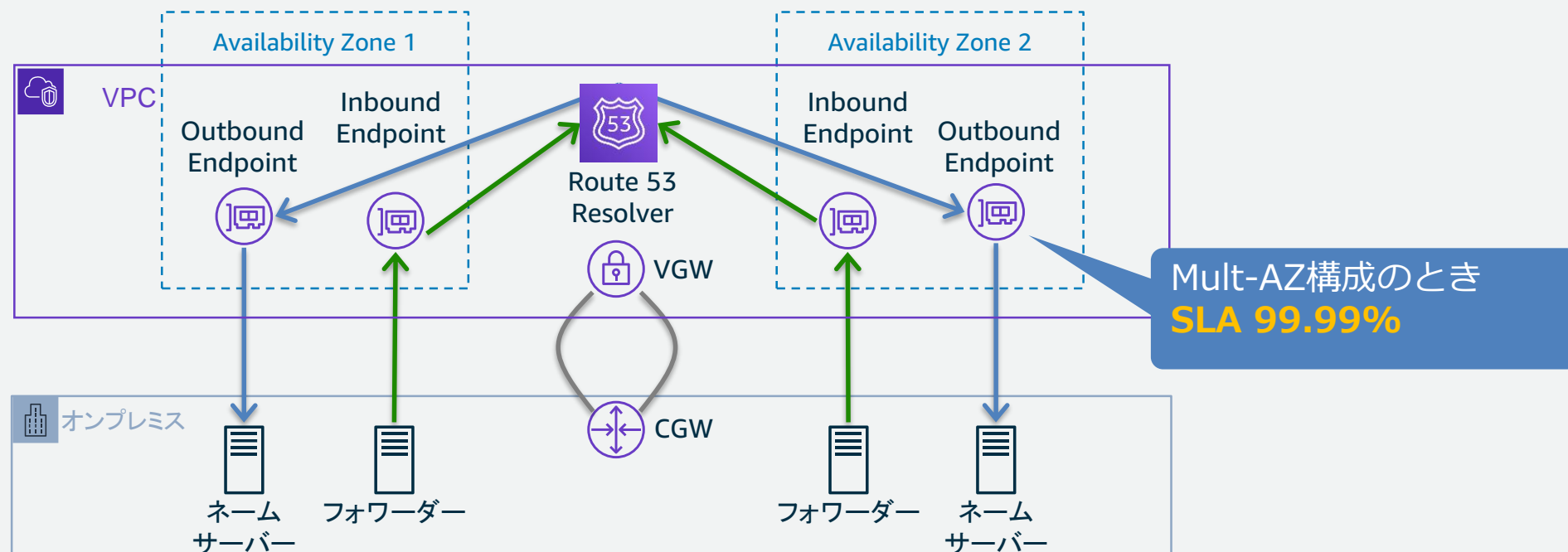




# Route 53 Resolver for Hybrid Clouds 高可用性設計

## 【重要】一般にDNSの障害は影響が広範囲になる傾向がある

- AZ障害を想定し、エンドポイントはMulti-AZ構成を推奨
- AWS Direct ConnectやInternet VPN、オンプレミス側サーバーの冗長化も推奨



# Route 53 Resolver for Hybrid Clouds ネットワークアクセス制御

Endpointの実体はElastic Network Interfaces (ENIs)であるため、仕組み上セキュリティグループの設定が必須、必要に応じて制限を行う

## Inbound Endpointのポリシー例

### インバウンドルール

プロトコル	ポート 範囲	ソース
UDP	53	許可したいアドレス
TCP	53	許可したいアドレス

### アウトバウンドルール

プロトコル	ポート 範囲	送信先
すべて	すべて	0.0.0.0/0

## Outbound Endpointのポリシー例

### インバウンドルール

プロトコル	ポート 範囲	ソース
すべて	すべて	0.0.0.0/0

### アウトバウンドルール

プロトコル	ポート 範囲	送信先
UDP	53	参照先ネームサーバ
TCP	53	参照先ネームサーバ

※制限する場合には、TCP Fallback (RFC 5966) を想定しTCPも許可してください。

# 転送ルールの共有と共有ルールの使用

- 作成した転送ルールは他のAWS アカウントと共有可能
- ルールを共有する場合、Route 53 リゾルバー コンソールは AWS Resource Access Manager と統合されます。Resource Access Manager の詳細については、Resource Access Manager ユーザーガイドを参照してください。
- 次の点に注意
  - **共有ルールと VPC の関連付け**
  - **ルールの削除または共有解除**
  - **ルールに対する制限**
  - **アクセス許可**

【参考】 Resource Access Manager ユーザーガイド  
<https://docs.aws.amazon.com/ram/latest/userguide/what-is.html>

# ここから、具体的な構成手順を見ていきましょう

# Route 53 Resolver for Hybrid Clouds

## Step 1 Get Started

The screenshot shows the Amazon Route 53 Resolver for Hybrid Clouds landing page. The page has a dark blue header with a hamburger menu icon on the left and an information icon on the right. Below the header, the text 'ネットワークとコンテンツ配信' (Network and Content Delivery) is visible. The main heading is 'Amazon Route 53 リゾルバ' (Amazon Route 53 Resolver). Below this, the text 'ネットワークの DNS と簡単に統合できる VPC 用の DNS リゾルバーサービス。' (A DNS resolver service for VPC that can be easily integrated with network DNS.) is displayed. On the right side, there is a white box with the heading '開始する' (Get started). Below this heading, the text '使い始めるには、Amazon VPC に入出入りする DNS クエリのエンドポイントを設定します。' (To get started, set the endpoint for DNS queries entering and leaving Amazon VPC.) is shown. Below this text is an orange button labeled 'エンドポイントの設定' (Set endpoint). Below the white box, there is a section titled '料金' (Pricing).

ネットワークとコンテンツ配信

## Amazon Route 53 リゾルバ

ネットワークの DNS と簡単に統合できる VPC 用の DNS リゾルバーサービス。

### 開始する

使い始めるには、Amazon VPC に入出入りする DNS クエリのエンドポイントを設定します。

エンドポイントの設定

### 料金

# Route 53 Resolver for Hybrid Clouds

## Step 2 Choose Endpoints

ステップ 1

エンドポイントの設定

ステップ 2

インバウンドエンドポイントの設定

ステップ 3

アウトバウンドエンドポイントの設定

ステップ 4

ルールの作成

ステップ 5

確認と作成

### エンドポイントの設定 情報

エンドポイントは、DNS クエリを VPC からネットワークに、ネットワークから VPC に、または双方にルーティングするためにリゾルバーが必要とする情報を提供します。



**ap-northeast-1 (東京) リージョンにサインインしています**  
リージョンを変更するには、右上隅にあるリージョンセレクトアを使用します。



#### 基本的な設定

**DNS クエリの方向 情報**  
(VPC への) インバウンド DNS クエリ、(VPC からの) アウトバウンド DNS クエリ、またはその両方のためのエンドポイントを設定できます。

☒ **インバウンドとアウトバウンド**  
DNS クエリから VPC、VPC から DNS クエリの両方を許可するエンドポイントの設定。  


☐ **インバウンドのみ**  
お使いのネットワークまたは別の VPC から VPC への DNS クエリを許可するエンドポイントの設定。  


☐ **アウトバウンドのみ**  
お使いの VPC から お使いのネットワークまたは別の VPC への DNS クエリを許可するエンドポイントの設定。  


キャンセル

戻る

次へ

# Route 53 Resolver for Hybrid Clouds

## Step 3 Configure Inbound Endpoint

### インバウンドエンドポイントの設定 情報

インバウンドエンドポイントには、ネットワークから VPC に DNS クエリをルーティングするためにリゾルバーが必要とする情報が含まれています。

#### インバウンドエンドポイントの全般設定

##### エンドポイント名

わかりやすい名前を付けると、ダッシュボードでエンドポイントを見つけやすくなります。

myInboundEndpoint

エンドポイント名は最長 64 文字です。有効な文字は、a～z、A～Z、0～9、スペース、\_

##### 当該リージョンの VPC: ap-northeast-1 (東京) 情報

インバウンド DNS クエリはすべて、リゾルバーに行く途中でこの VPC を通過します。エトの作成後は、この値を変更することはできません。

vpc-060eb775c5c3bed7a

##### このエンドポイントのセキュリティグループ 情報

セキュリティグループはこの VPC へのアクセスをコントロールします。選択したセキュリティグループには、1 つ以上のインバウンドルールを含む必要があります。エンドポイントの後は、この値を変更することはできません。

セキュリティグループの選択

#### IP アドレス 情報

リゾルバーでは、信頼性を向上させるために、DNS クエリに対して 2 つの IP アドレスを指定する必要があります。2 つの異なるアベイラビリティゾーンで IP アドレスを指定することをお勧めします。最初の 2 つの IP アドレスを追加した後に、オプションでさらに、同じまたは別のアベイラビリティゾーンのアドレスを追加できます。

##### ▼ IP アドレス #1

##### アベイラビリティゾーン 情報

インバウンド DNS クエリ用に選択するアベイラビリティゾーンを選択します。

ap-northeast-1a

##### サブネット 情報

選択するサブネットには、利用可能な IP アドレスが必要です。

subnet-0c55611e0094a63eb (172.31.32.0/20)

##### IPv4 アドレス 情報

インバウンド DNS クエリでは、サービスによって選択された、サブネット内の利用可能な IP アドレスのいずれかを使用することも、自分で IP アドレスを指定することもできます。

- ☐ 自動的に選択された IP アドレスを使用します。
- ☒ 自分で指定した IP アドレスを使用します。

172.31.32.3

Inbound EndpointのIPアドレスは、参照する側（オンプレミスのDNSサーバなど）で指定するため、任意のIPアドレスを設定すると管理しやすい

# Route 53 Resolver for Hybrid Clouds

## Step 4 Configure Outbound Endpoint

### アウトバウンドエンドポイントの設定 情報

アウトバウンドエンドポイントには、VPC から ネットワーク まで DNS クエリをルーティングするためにリゾルバーが必要とする情報が含まれています。

#### アウトバウンドエンドポイントの全般設定

##### エンドポイント名

わかりやすい名前を付けると、ダッシュボードでエンドポイントを見つけやすくなります。

myOutboundEndpoint

エンドポイント名は最長 64 文字です。有効な文字は、a~z、A~Z、0~9、スペース、\_(7)

##### 当該リージョンの VPC: ap-northeast-1 (東京) 情報

アウトバウンド DNS クエリはすべて、他の VPC から来る途中でこの VPC を通過します。コンソールの作成後は、この値を変更することはできません。

VPC を選択

##### このエンドポイントのセキュリティグループ 情報

セキュリティグループはこの VPC へのアクセスをコントロールします。選択したセキュリティグループは、1 つ以上のアウトバウンドルールを含む必要があります。エンドポイントの作成後は、この値を変更することはできません。

セキュリティグループの選択

#### IP アドレス 情報

リゾルバーでは、信頼性を向上させるために、DNS クエリに対して 2 つの IP アドレスを指定する必要があります。2 つの異なるアベイラビリティゾーンで IP アドレスを指定することをお勧めします。最初の 2 つの IP アドレスを追加した後に、オプションでさらに、同じまたは別のアベイラビリティゾーンのアドレスを追加できます。

##### ▼ IP アドレス #1

##### アベイラビリティゾーン 情報

アウトバウンド DNS クエリ用に選択するアベイラビリティゾーンを選択します。

ap-northeast-1a

##### サブネット 情報

選択するサブネットには、利用可能な IP アドレスが必要です。

subnet-0c55611e0094a63eb (172.31.32.0/20)

##### IPv4 アドレス 情報

アウトバウンド DNS クエリでは、サービスによって選択された、サブネット内の利用可能な IP アドレスのいずれかを使用することも、自分で IP アドレスを指定することもできます。

- ☐ 自動的に選択された IP アドレスを使用します。
- ☒ 自分で指定した IP アドレスを使用します。

172.31.32.10

接続先でIPアドレス制限などを行う場合には、Outbound Endpointに任意のIPアドレスを設定すると管理しやすい



# Route 53 Resolver for Hybrid Clouds

## Step 5 Create Rules

### ルールの作成 情報

#### アウトバウンドトラフィックのルール

VPC で発行されたクエリに対して、VPC からの DNS クエリの転送方法を定義できます。

#### 名前

わかりやすい名前を付ける

1ドメインごとに1ルールの作成が必要

myRule

ルール名は最長 64 文字です。有効な文字は、a~z、A~Z、0~9、スペース、\_ (アンダースコア)、および - (ハイフン) です。

#### ルールタイプ 情報

[転送] を選択して、このページの下部付近にある [ターゲット IP アドレス] セクションで指定した IP アドレスに DNS クエリを転送します。リソルバーが指定されたサブドメインに対するクエリを処理するように [システム] を選択します。ルールの作成後は、この値を変更はできません。

転送

#### ドメイン名 情報

このドメイン名の DNS クエリは、ページの下部付近にある [ターゲット IP アドレス] セクションで指定した IP アドレスに転送されます。クエリが複数のルール (example.com と www.example.com) と一致した場合、アウトバウンド DNS クエリは、最も限定的なドメイン名 (www.example.com) を含むルールを使ってルーティングされます。ルールの作成後は、この値を変更することはできません。

www.example.com

オンプレミスのネームサーバが複数ある場合には、冗長化のため複数指定を推奨

#### ターゲット IP アドレス 情報

DNS クエリは、次の IP アドレスに転送されます。

IPv4 アドレス

192.0.2.10

ポート

53

ターゲットの消去

ターゲットの追加

# テストとトラブルシューティング

## テスト

- 実際にエンドポイントに対して問い合わせを試行する
  - 代表的な疎通確認ツール：dig(主にLinux)/nslookup(主にWindows)

## トラブルシューティング

- 原因はどこか？フォワーダーか？フルサービスリゾルバーか？  
ネームサーバーか？ネットワークか？を特定する
  - 「再帰的問い合わせ」と「反復問い合わせ」を明確に区別して試行すると特定しやすい
  - 出力情報やオプションが豊富なdigコマンドが有用

# digコマンド

```
$ dig @172.31.0.2 www.example.com. A +rec +all
```

参照先

参照したいFQDN

クエリタイプ

オプション

- 引数として「参照したいFQDN」は必須
- そのほかは、省略すると以下の値で補完される
  - 参照先：スタブリゾルバーの参照先（/etc/resolv.confのnameserver）
  - クエリタイプ：A
  - オプション：+rec（再帰的問い合わせ） +all（表示指定を全て有効）

# digコマンド結果

```
$ dig @172.31.0.2 www.example.com
```

```
; <<>> DiG 9.9.4-RedHat-9.9.4-74.amzn2.1.2 <<>>
```

```
www.example.com
```

```
:: global options: +cmd
```

```
:: Got answer:
```

```
:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57031
```

```
:: flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
```

```
ADDITIONAL: 1
```

```
:: OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags;; udp: 4096
```

```
:: QUESTION SECTION:
```

```
;www.example.com. IN A
```

```
:: ANSWER SECTION:
```

```
www.example.com. 60 IN A 192.168.0.1
```

```
:: Query time: 758 msec
```

```
:: SERVER: 172.31.0.2#53(172.31.0.2)
```

```
:: WHEN: 月 10月 14 04:37:26 UTC 2019
```

```
:: MSG SIZE rcvd: 65
```

特に注目

Header

Question

Answer

# Headerから状況を読み解く

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57031
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```

これらはDNSの名前解決で生じている問題を明らかにする有用な情報です。AWSサポートにお問い合わせの際にも、**digコマンドの出力結果**をご提供頂けるとスムーズに原因究明を進めることができます。

status	概要
NOERROR	正常な応答
SERVFAIL	何らかの要因により、DNSサーバーから応答を得られなかった
REFUSED	リクエストが拒否された
NXDOMAIN	リクエストされた名前が存在しない

flags	概要
qr	応答であることを示す
aa	ネームサーバからの応答であることを示す
ra	再帰的問い合わせを受け付けられることを示す
tc	何らかの要因により応答の一部が切り捨てられたことを示す

【参考】 初心者のためのDNS運用入門-トラブル事例とその解決のポイント-, 水野貴史, 株式会社日本レジストリサービス, 2014  
<https://dnsops.jp/event/20140626/dns-beginners-guide2014-mizuno.pdf>

# Amazon Route 53 Resolver の構成 まとめ

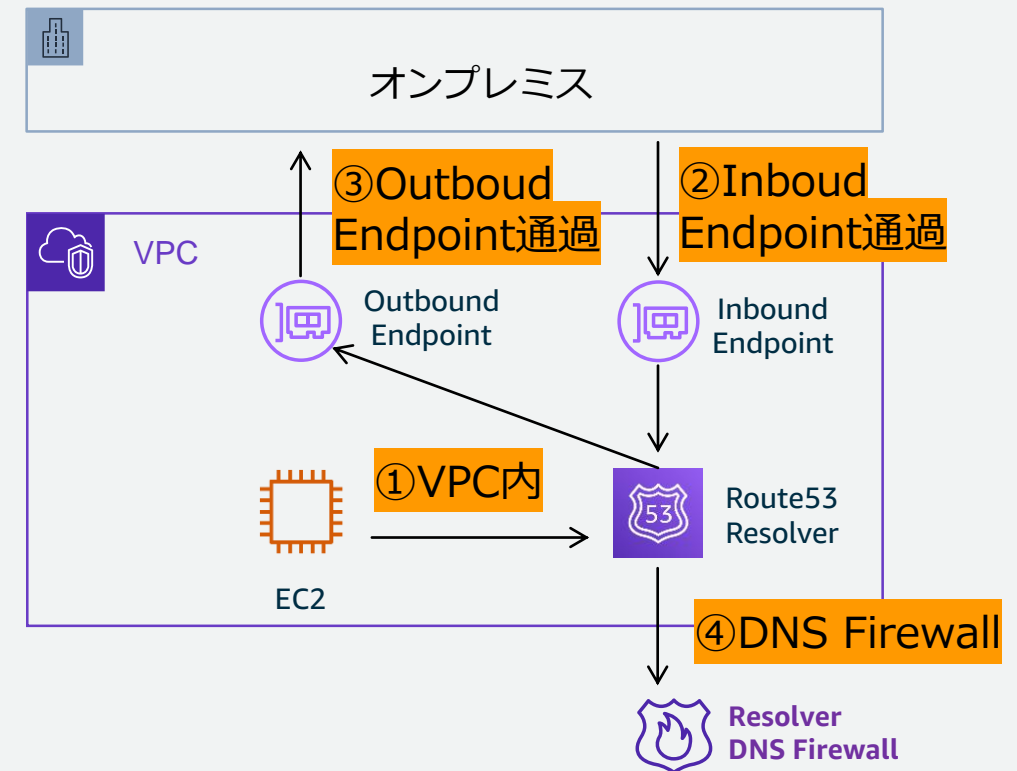
- Amazon Route 53 Resolverは通常そのまま利用可能
- Amazon Route 53 Resolver for Hybrid Clouds構成時の考慮ポイント
  - 各コンポーネントの冗長化を強く推奨、SPOFを作らない  
(Availability Zone / 回線 / サーバーなど)
  - エンドポイントには管理の必要性に応じてIPアドレスを指定
  - 転送ルールの共有はResource Access Managerで一元管理
- テストとトラブルシューティング
  - 実際にエンドポイントに対して問い合わせを試行する
  - 出力情報やオプションが豊富なdigコマンドが有用
  - トラブルシューティング時にはヘッダのstatusとflagsに着目

# 3. DNSクエリのログ記録

# DNSクエリのログ記録

## Resolverで、以下のDNSクエリの記録が可能

- ① 指定VPCで発生するクエリとその応答
- ② InboundEndpointを通過するオンプレからのクエリ
- ③ 再帰的なDNS解決にOutboundEndpointを使用するクエリ
- ④ Route 53 Resolver DNS Firewallによりドメインリストのドメインをブロック/許可/モニタリングするクエリ





# DNSクエリログの内容

## ログに含まれる値

- VPC が作成された AWS リージョン
- クエリの発信元の情報  
(VPC ID、インスタンスのIPアドレス/ID)
- クエリが最初に作成された日時
- リクエストされたDNS 名 (prod.example.com 等)
- DNS レコードタイプ (A や AAAA 等)
- DNS レスポンスコード (NoError や ServFail 等)
- DNS 応答データ  
(DNS クエリに回答して返される IP アドレス等)
- DNS Firewall ルールのアクションに対する応答

例：EC2のプライベートIPv4DNSの名前解決

```
{
  "version": "1.100000",
  "account_id": "XXXXXXXXXXXX",
  "region": "us-east-1",
  "vpc_id": "vpc-000a00aaa00000a0a",
  "query_timestamp": "2023-03-06T06:21:48Z",
  "query_name": "ip-10-0-1-120.us-east-1
                .compute.internal.",
  "query_type": "A",
  "query_class": "IN",
  "rcode": "NOERROR",
  "answers": [
    {
      "Rdata": "10.0.1.120.",
      "Type": "A",
      "Class": "IN"
    }
  ],
  "srcaddr": "10.0.1.120",
  "srcport": "57163",
  "transport": "UDP",
  "srcids": {
    "instance": "i-00a0a0000aa00a0aa"
  }
}
```

Resolver クエリログに表示される値

[https://docs.aws.amazon.com/ja\\_jp/Route53/latest/DeveloperGuide/resolver-query-logs-format.html](https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/resolver-query-logs-format.html)

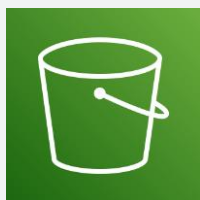


# DNSクエリログの送信先

ログは、以下の AWS リソースのいずれかに送信が可能



CloudWatch Logsのロググループ



S3バケット

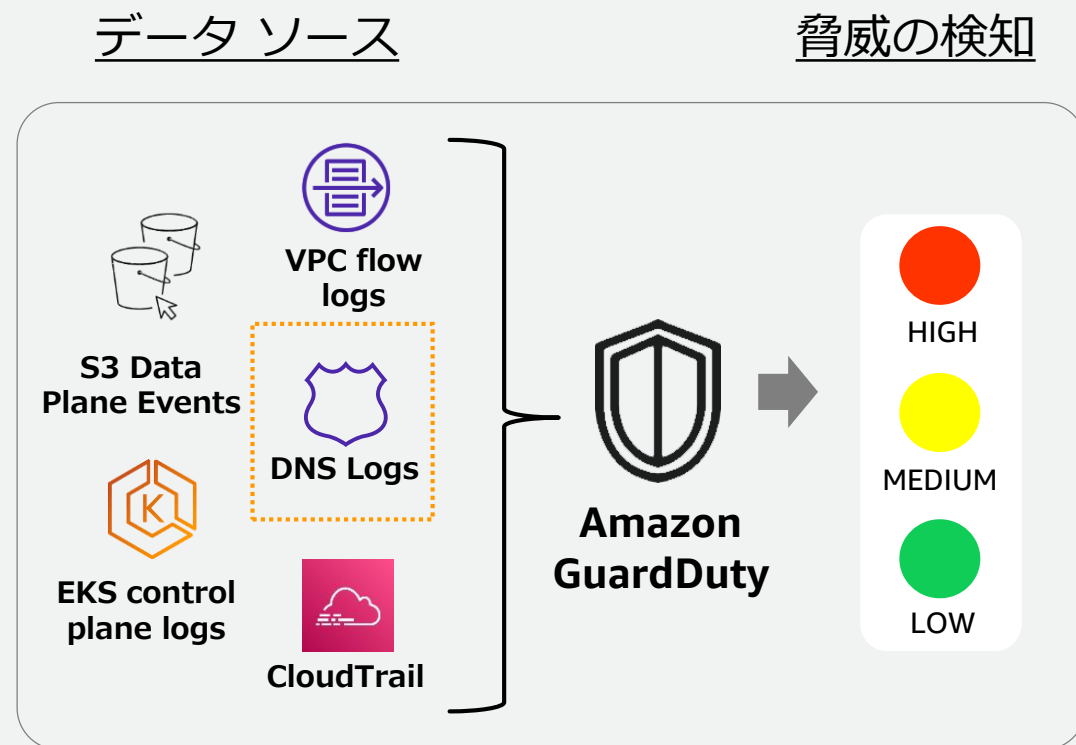
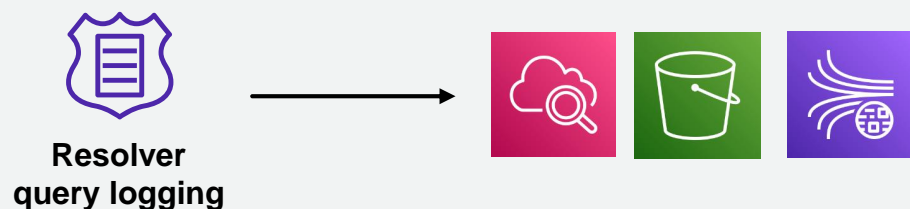


Kinesis Data Firehose の配信ストリーム

# GuardDutyとの連携

GuardDutyを有効化すると、DNSのリクエストとその応答のログが脅威検出の分析に利用される

- EC2インスタンスがAWSのDNSリゾルバーを使用している(デフォルトの設定)場合のみ
- GuardDutyが分析するDNSのログは  
「DNSクエリログ記録」機能によって  
取得されるログとは異なる  
(互いに設定内容が影響しない)



# DNSクエリログの料金 (2023/5)

- クエリログの料金は発生しない
- ログの転送・保管に関しては各サービスに応じて料金が発生

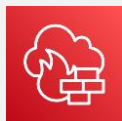
# 4. Route 53 Resolver DNS Firewall

# Route 53 Resolver DNS Firewallとは

お客様のDNSデータ保護を目的に  
VPCのアウトバウンド DNS トラフィックをフィルタリングする

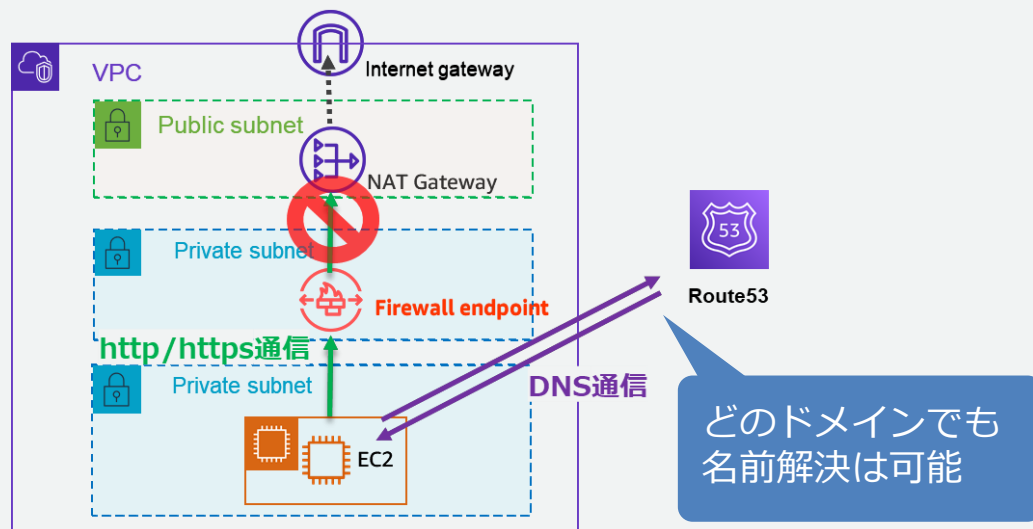


# AWS Network Firewall との違い



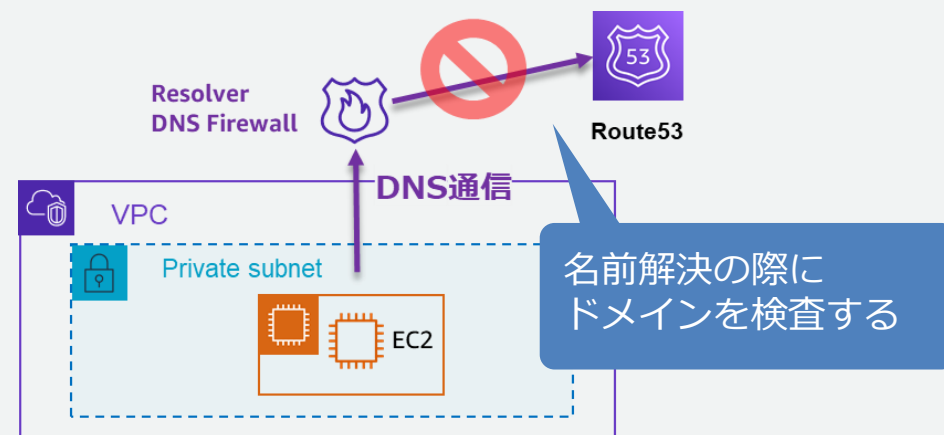
## Network Firewall ドメインのフィルタリング

- http/https通信の宛先のドメイン名を検査する
- Firewall Endpointを通過するインバウンド/アウトバウンドが対象



## DNS Firewall

- DNSクエリに含まれるドメイン名を検査する
  - DNS Firewallを通過するアウトバウンドが対象
- ※ 宛先のIPアドレスによる制御はできない

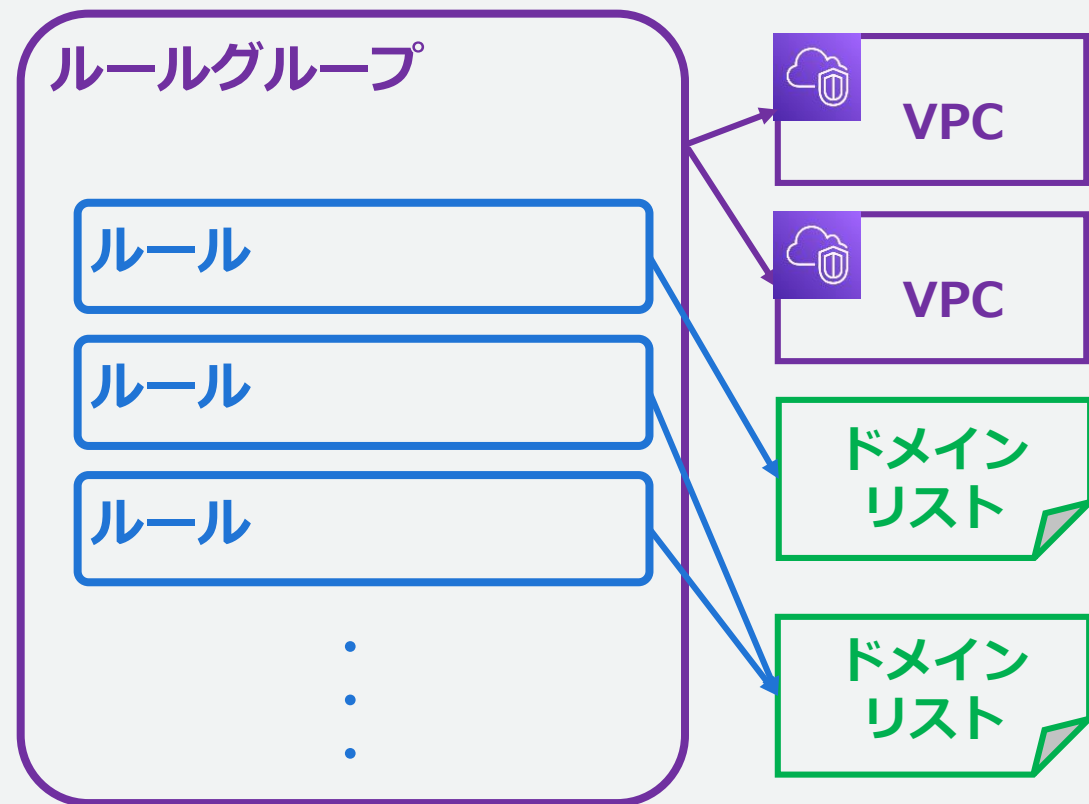


# DNS Firewall の設定

DNS Firewall を使用するために以下の設定を行う

- ドメインリストの作成
- ルールグループの作成
  - ルールの追加
  - ルールの優先度の指定
- ルールグループとVPCの関連付け

## 設定リソースのイメージ





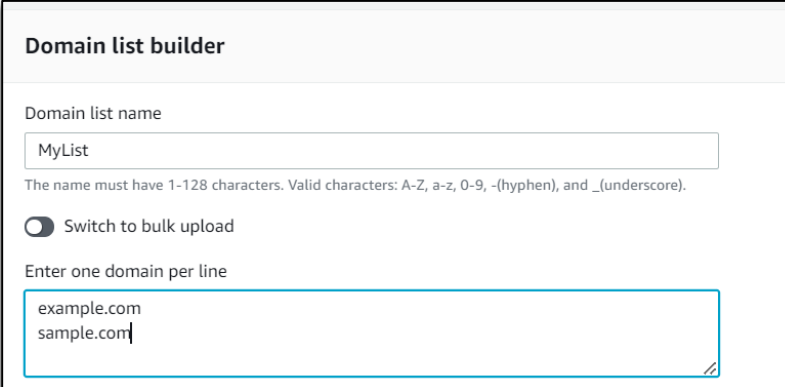
# DNS Firewall ドメインリスト

- DNS Firewall ルールの対象となるドメインを定義する
- 1つのドメインリストを複数のルールによって参照することが可能

## ドメインリストの種類

### • 独自のドメインリスト

- お客様が作成し管理を行う
- ワイルドカードドメイン（\*.example.com など）と完全修飾ドメイン名（FQDN）をサポート

A screenshot of the 'Domain list builder' interface. It features a text input field for 'Domain list name' containing 'MyList'. Below this is a note: 'The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -(hyphen), and \_(underscore)'. There is a radio button labeled 'Switch to bulk upload'. Below that is a text area for 'Enter one domain per line' containing 'example.com' and 'sample.com' on separate lines. A small icon in the bottom right corner of the text area indicates a copy or paste function.

Domain list builder

Domain list name

MyList

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -(hyphen), and \_(underscore).

☐ Switch to bulk upload

Enter one domain per line

example.com  
sample.com

### • AWS マネージドドメインリスト

- AWS が作成し管理する
- 新しい脆弱性と脅威が出現するとリストは自動的に更新される
- ユーザによる編集、閲覧、ダウンロードは不可

# DNS Firewall ルールグループ

- ルールグループを作成し、1つ以上のルールを追加する
- ルールごとに、関連づけるドメインリスト、ドメインリストに一致したときのアクションを指定する

Rules (4)					Edit ▼	Delete	Add rule
<input type="text" value="Search"/>					< 1 > ⚙		
	Name ▼	Action ▼	Priority ▲	Domain list ▼			
<input type="radio"/>	Rule-01	ALLOW	1	<a href="#">rslvr-fdl-15f4860b1ad54ead (AWSManagedDomainsAggregateThreatList)</a>			
<input type="radio"/>	Rule-02	ALLOW	2	<a href="#">rslvr-fdl-2c46f2ecbfec4dcc (AWSManagedDomainsMalwareDomainList)</a>			
<input type="radio"/>	Rule-03	ALLOW	3	<a href="#">rslvr-fdl-aa970e9eb1ca4777 (AWSManagedDomainsBotnetCommandanc</a>			
<input type="radio"/>	Rule-04	ALLOW	4	<a href="#">rslvr-fdl-b5f3953a7fe24d01 (AWSManagedDomainsGlobalThreatList)</a>			

# DNS Firewall ルールグループのアクション

- アクションは以下の3つからいずれかを指定
  - Allow : トラフィックの通過を許可
  - Alert : トラフィックの通過を許可して、Route 53 Resolver ログにクエリのアラートを記録する
  - Block : 目的の送信先への送信をブロックして、Route 53 Resolver ログにそのクエリのブロックアクションを記録する

# DNS Firewall のBlockアクションについて

- Blockアクションを指定した場合は、更にクエリへの応答を指定
  - NODATA : DNSクエリは成功するが利用可能な応答がないことを示す
  - NXDOMAIN : DNSクエリのドメインがないことを示す
  - OVERRIDE : 応答をカスタムする
- Blockアクションを指定する際に、 事前にAlert アクションで影響範囲を確認することが可能
  - アクションを Alert に設定して、ドメインリストをテストする
  - Alert の対象となるクエリの数进行调查することで、  
アクションを Block に設定した場合にブロックされるクエリの数を確認する

# DNS Firewall ルールの優先度

- 優先度（Priority）の値が小さいルールから評価される
- 一致するルールがあればそれより後のルールは評価されない

**Set rule priority - optional** [Info](#)

DNS Firewall evaluates the rules in the order that they are shown, starting from the top.

**Rule priority** ▲ Move up ▼ Move down

Move rules up or down to change the evaluation order.

	Name	Action	Priority
<input type="radio"/>	Rule-01	ALLOW	1
<input checked="" type="radio"/>	Rule-02	ALLOW	2
<input type="radio"/>	Rule-03	ALLOW	3
<input type="radio"/>	Rule-04	ALLOW	4

先に実行



後に実行

# DNS Firewall ルールグループとVPCの関連づけ

- 作成したルールグループをVPCに紐づけたタイミングで、該当のVPCに対して設定したルールが適用される
- ルールグループは複数のVPCと紐づけることが可能

	Name ▲	ID ▼	VPC association status ▼	Associated VPCs ▼	Rule group share status
<input type="radio"/>	MyRuleGroup	rslvr-frg-964...	✓ Associated	2	Not shared

Rules

VPCs associated

Tags

Associated VPCs (2)

Disassociate

Associate VPC

Manage tags

< 1 >

⚙

	ID ▼	Name ▼	Number of associated rule groups ▼	Association ID
<input type="radio"/>	vpc-0a7f0591b83f4ab58	rgassoc-vpc-0a7f0591b83f4ab58-rslvr-frg-964306d798241b	-	rslvr-frgassoc-704910cdc9f54
<input type="radio"/>	vpc-060eb775c5c3bed...	rgassoc-vpc-060eb775c5c3bed7a-rslvr-frg-964306d79824...	-	rslvr-frgassoc-a89e068eed44

# DNS Firewall の障害時の動作

DNS Firewallを設定しているVPCには、以下のいずれかを指定する

- フェイルクローズ

- デフォルトの動作
- DNS Firewallから応答がないDNSクエリを全てブロックする
- 可用性よりもセキュリティを優先

## DNS ファイアウォールフェイルオープン

DNS ファイアウォールに障害が発生した場合や応答がない場合に、リソルバーが DNS クエリを処理する方法を指定します。

☐ この VPC でフェイルオープンを有効化

Status

⊖ 無効

- フェイルオープン

- DNS Firewallから応答がないDNSクエリは全て通過させる
- セキュリティよりも可用性を優先

# DNS Firewall マネージドドメインリストの誤検出について

## マネージドドメインリストによって誤検出でクエリがブロックされた場合

### ① ブロックしているルールの特典

- Resolver ログを確認し、誤検出の原因となっているルールグループとマネージドドメインリストを特定

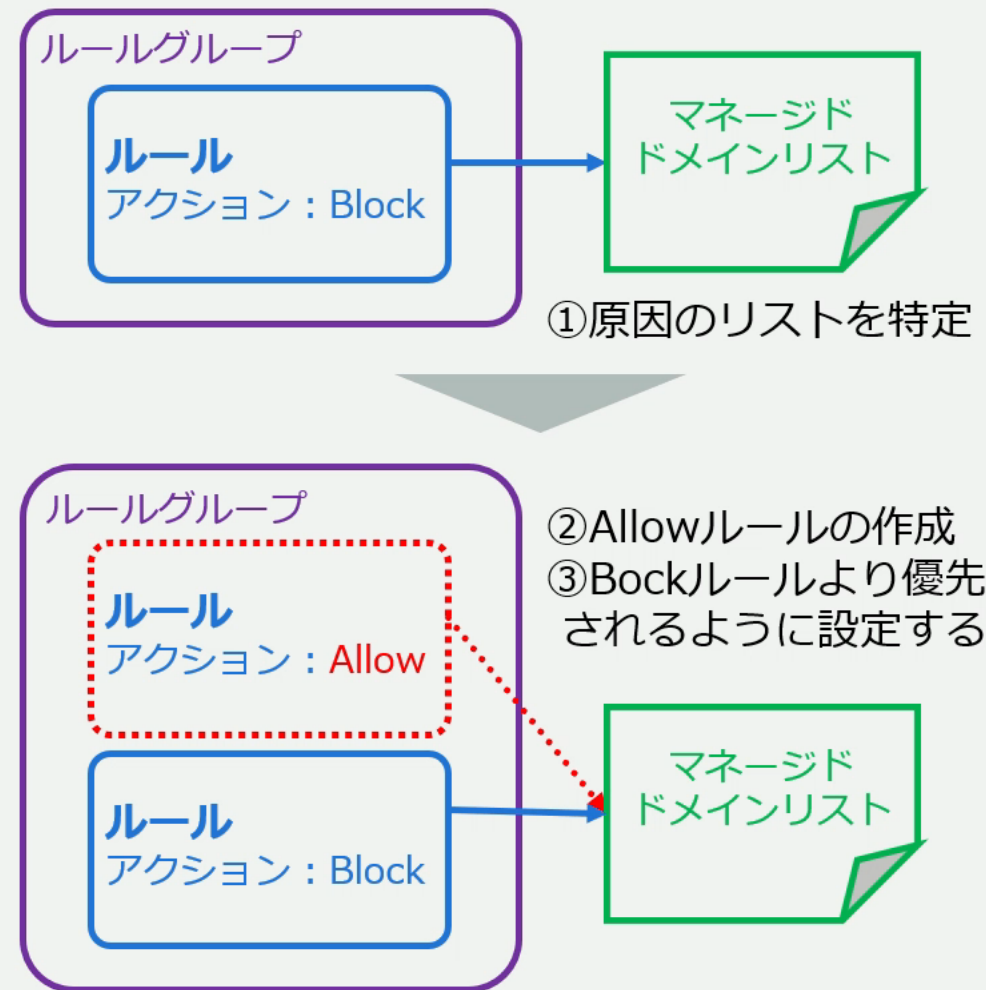
### ② Blockされたクエリを明示的に許可するルールを追加

### ③ 追加したルールが優先されるように設定

- ルールグループ内で新しいルールの優先度の値を①のマネージドリストを使用しているルールの数値より小さく設定する



Blockするルールが実行される前に、  
該当のクエリを許可するルールが実行される





# 複数アカウントでのDNS Firewall の管理

- AWS アカウント間で DNS Firewall ルールグループを共有可能
  - 共有先のアカウントは、AWSアカウントID、OU、組織 のいずれかで指定
  - 他のアカウントを共有するためには、アクション「PutFirewallRuleGroupPolicy」が許可されている必要がある

Route 53 > Resolver > DNS Firewall > Rule groups > Rule group

## Rule group [Info](#)

[Share rule group](#) [Delete](#)

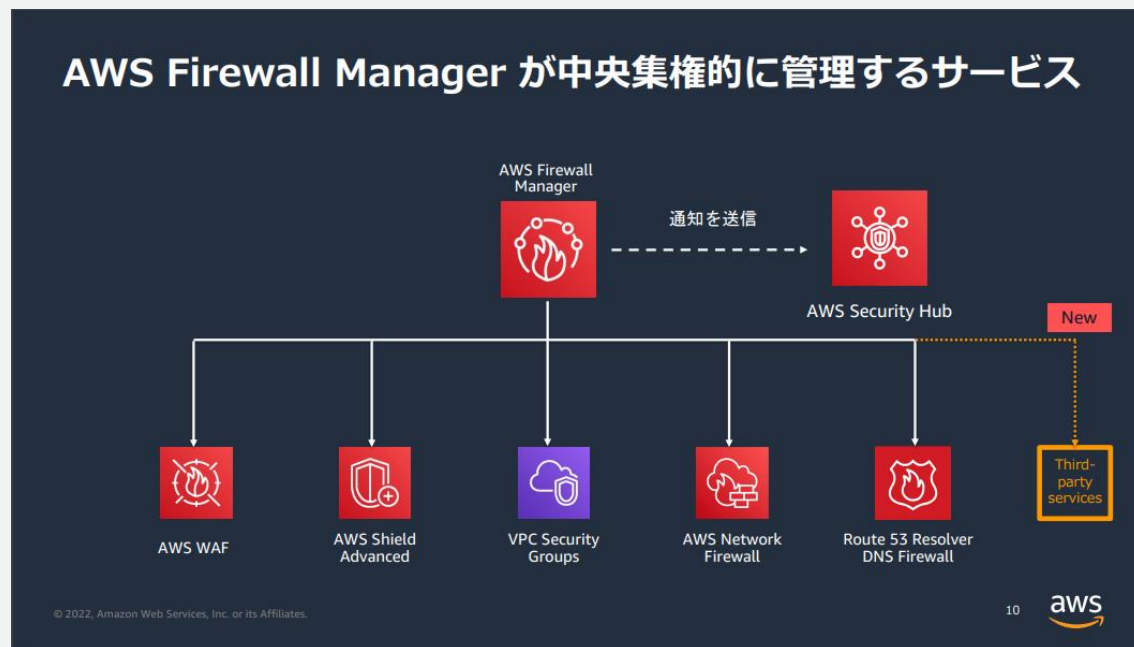
### Rule group configuration

This rule group is managed by the AWS Firewall Manager administrator.

ID rslvr-frg-bdbc07ae78174230	VPC association status ⊖ Not Associated	Region us-east-1	VPC associated count 0
Rule group share status Not shared	Owner ID [REDACTED]	Used capacity 4/100	

# 複数アカウントでのDNS Firewall の管理

- AWS Firewall Managerと連携して、マルチアカウントの一元管理が可能
- AWS Firewall Managerについては以下を参照  
「[AWS Firewall Manager を用いた マルチアカウントでの AWS WAF の管理手法](#)」



**AWS Firewall Manager をはじめるには**

AWS Organizations  
にて全ての機能を有効化

すべての AWS アカウント  
で AWS Config を有効化

Firewall Manager  
管理者を指定

・ AWS Firewall Manager の前提条件 (具体的な設定手順)  
[https://docs.aws.amazon.com/ja\\_jp/waf/latest/developerguide/fms-prereq.html](https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/fms-prereq.html)

© 2022, Amazon Web Services, Inc. or its Affiliates. 17

[https://pages.awscloud.com/rs/112-TZM-766/images/202206\\_AWS\\_Black\\_Belt\\_AWS\\_FirewallManager\\_For\\_AWS\\_WAF.pdf](https://pages.awscloud.com/rs/112-TZM-766/images/202206_AWS_Black_Belt_AWS_FirewallManager_For_AWS_WAF.pdf)

# Route 53 Resolver DNS Firewall 料金 (2023/5)

## ドメイン名の数

- 独自ドメインリストのドメイン名1つにつき、0.0005ドル/月
- 管理されたドメインリストにあるドメイン名には、料金は発生しない

## DNSクエリ

- 最初の10億回まで：百万回毎に0.60 ドル
- 10億クエリ超過後：百万回毎に0.40 ドル
- 以下のクエリが対象
  - ルールグループが関連づけられているVPC内で発生したクエリ
  - Inbound/OutboundEndpointを通過して、ルールグループが関連づけられているVPCに伝達されるクエリ

# Route 53 Resolver DNS Firewall まとめ

- DNSレイヤのセキュリティのためのサービス
  - Network Firewallやその他のセキュリティサービスとは保護するレイヤが異なる
- 使用する際は、ドメインリスト、ルールグループ、VPCとの関連付けを設定する
  - マネージドのドメインリストは無料で、すぐに使い始めることが可能
  - Blockアクションを指定する場合、事前にAlertアクションによる動作確認が可能
  - ルールグループは複数のVPCで利用可能で、他のアカウントとも共有可能なため一元的な管理が可能（Firewall Managerとも連携可能）

# AWS Black Belt Online Seminar とは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWS の技術担当者が、AWS の各サービスやソリューションについてテーマごとに動画を公開します
- 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
  - <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
  - <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBIqY>



ご感想は Twitter へ！ハッシュタグは以下をご利用ください  
#awsblackbelt

# 内容についての注意点

- 本資料では 2023 年 05 月時点のサービス内容および価格についてご説明しています。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます
- 技術的な内容に関しましては、有料の [AWS サポート窓口](#)へお問い合わせください
- 料金面でのお問い合わせに関しましては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)



# Thank you!



# 【付録】 名前空間（ゾーン） 概要説明



インターネット経由で.(root)から辿ることができるゾーン。ユーザーが作成・管理するもののほか、第三者が作成・管理しているものがある。



インターネット上に公開されたDNSドメインのレコードを管理するコンテナ。ユーザーが作成し、ユーザーが管理する。適切に構成することで、インターネット経由で.(root)から辿ることができるゾーンを構成できる。



VPCに閉じたプライベートネットワーク内のDNSドメインのレコードを管理するコンテナ。AWSが生成・管理しユーザーはカスタマイズできない。.ec2.internal/.compute.internal/.amazonaws.comなど。



VPCに閉じたプライベートネットワーク内のDNSドメインのレコードを管理するコンテナ。ユーザーが作成し、ユーザーが管理する。インターネット経由でアクセスすることは出来ない。



プライベートネットワーク内にユーザが構築したネームサーバーで提供される、インターネット経由で.(root)から辿ることは出来ないゾーン。