AWS Black Belt Online Seminar

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。

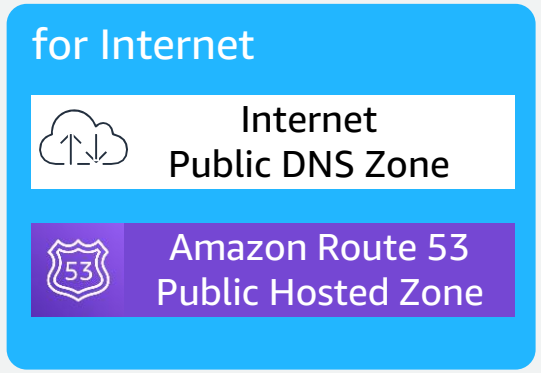
Amazon
Route 53

Amazon
Route 53 Resolver

Amazon
Route 53 Resolver
for Hybrid Clouds

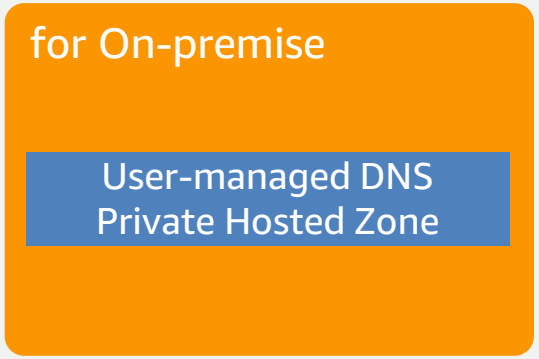
AWSと名前空間（ゾーン）の整理

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



インターネットに公開された
DNSドメインのゾーン

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

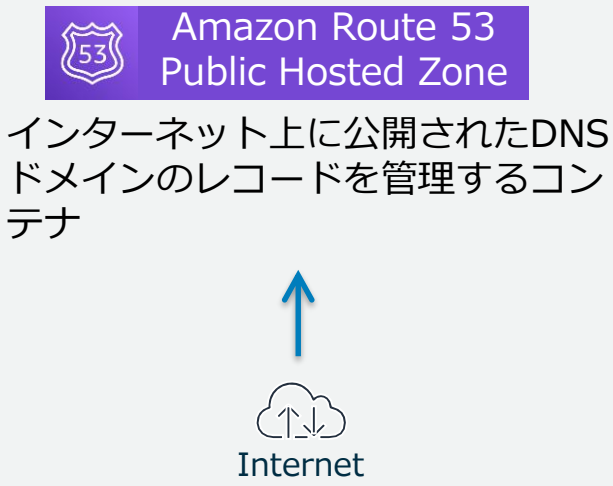


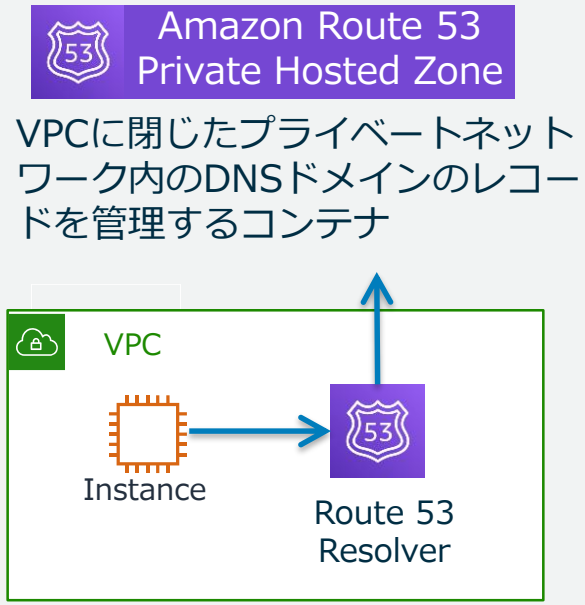
オンプレミス環境に閉じた
プライベートネットワーク内の
DNSドメインのゾーン

【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

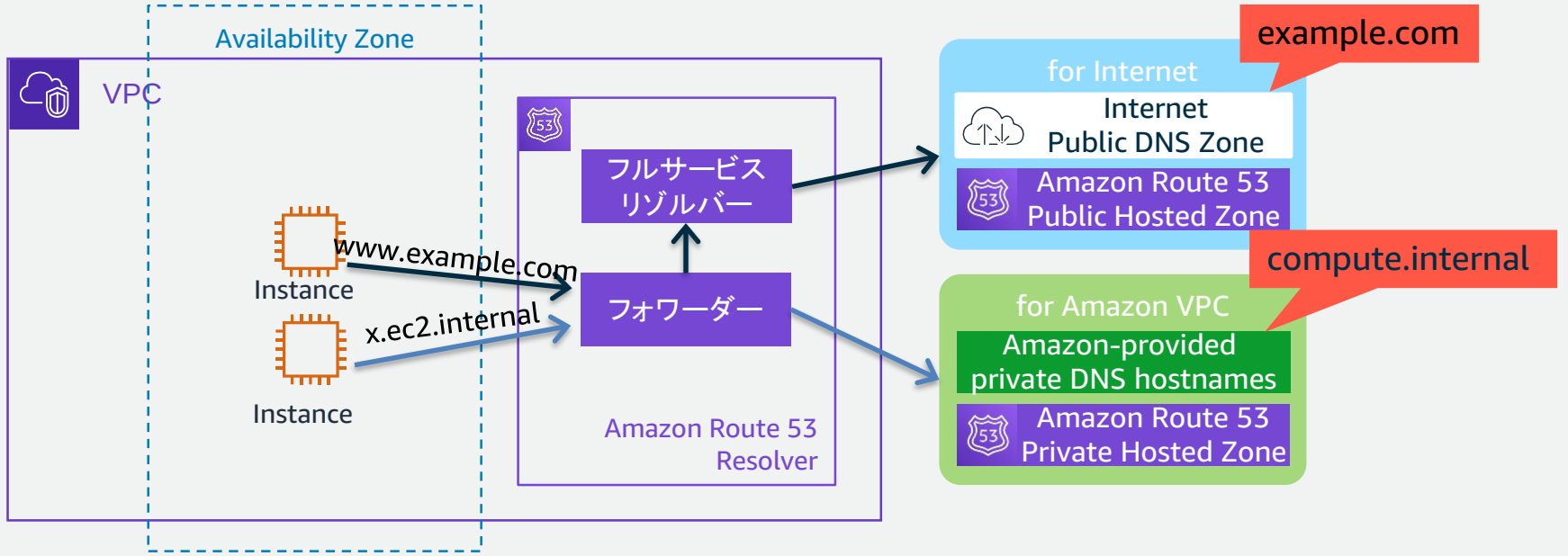




Amazon Route 53 Resolver

- 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

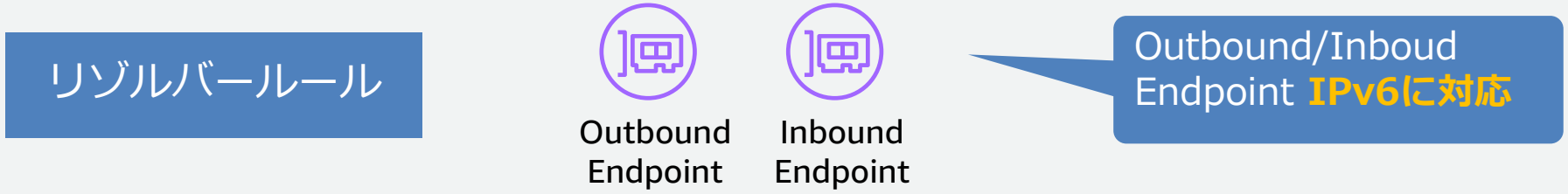


Amazon Route 53 Resolver for Hybrid Clouds

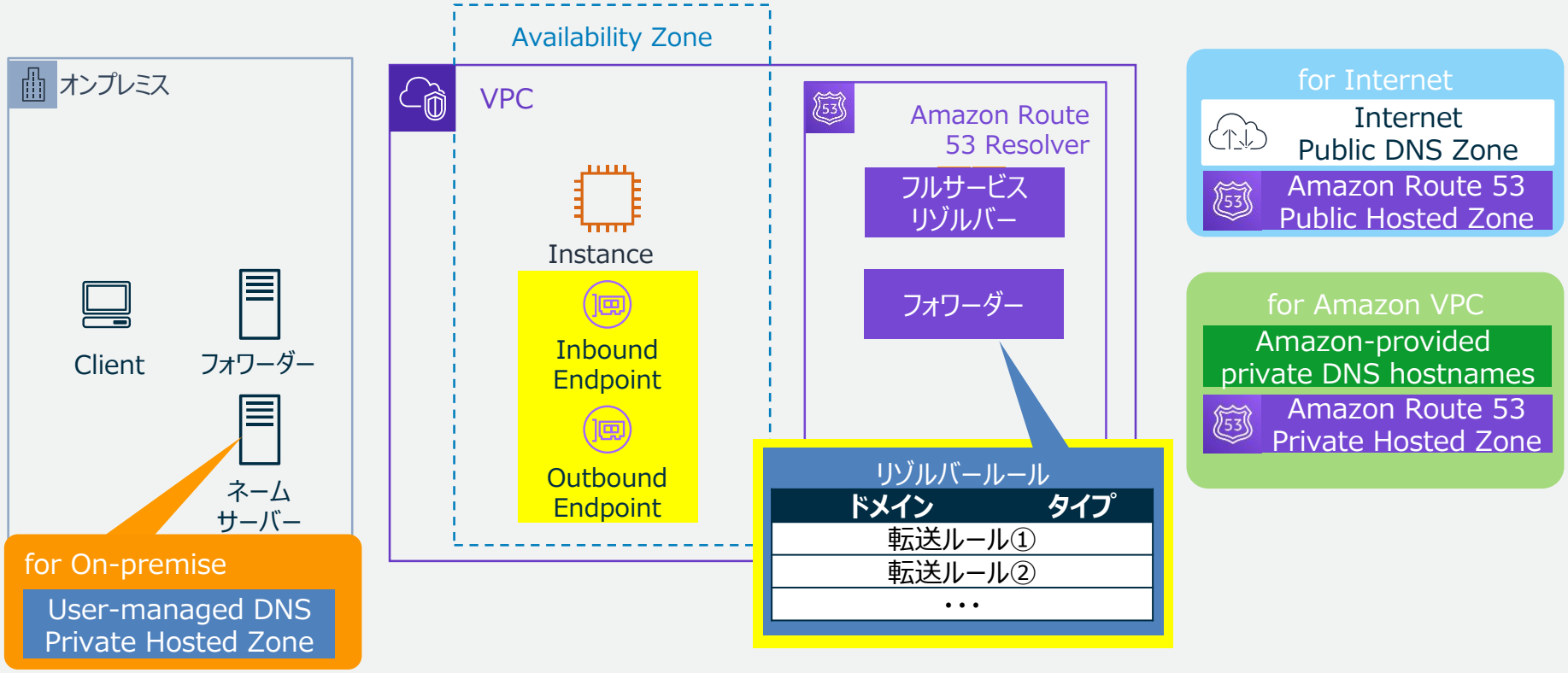
ハイブリッド環境の名前解決の一元化を実現

- 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

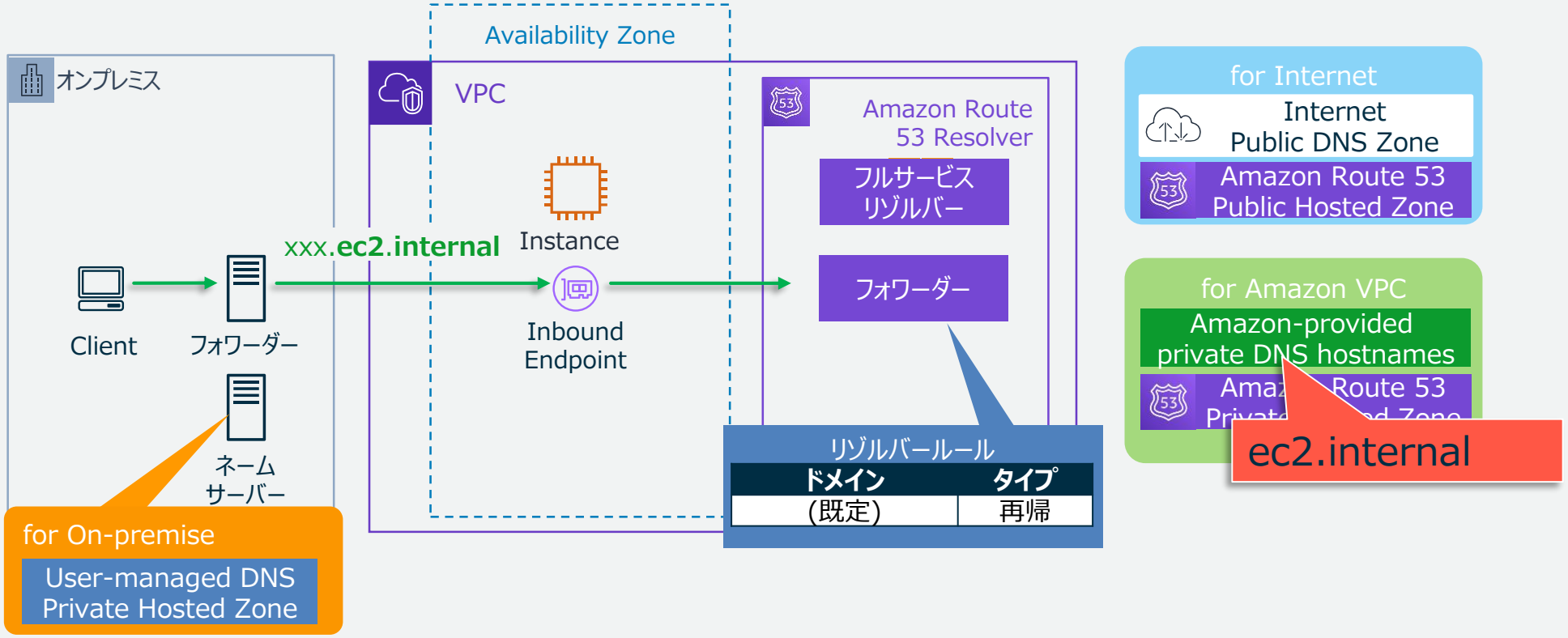


Route 53 Resolver for Hybrid Clouds Overview



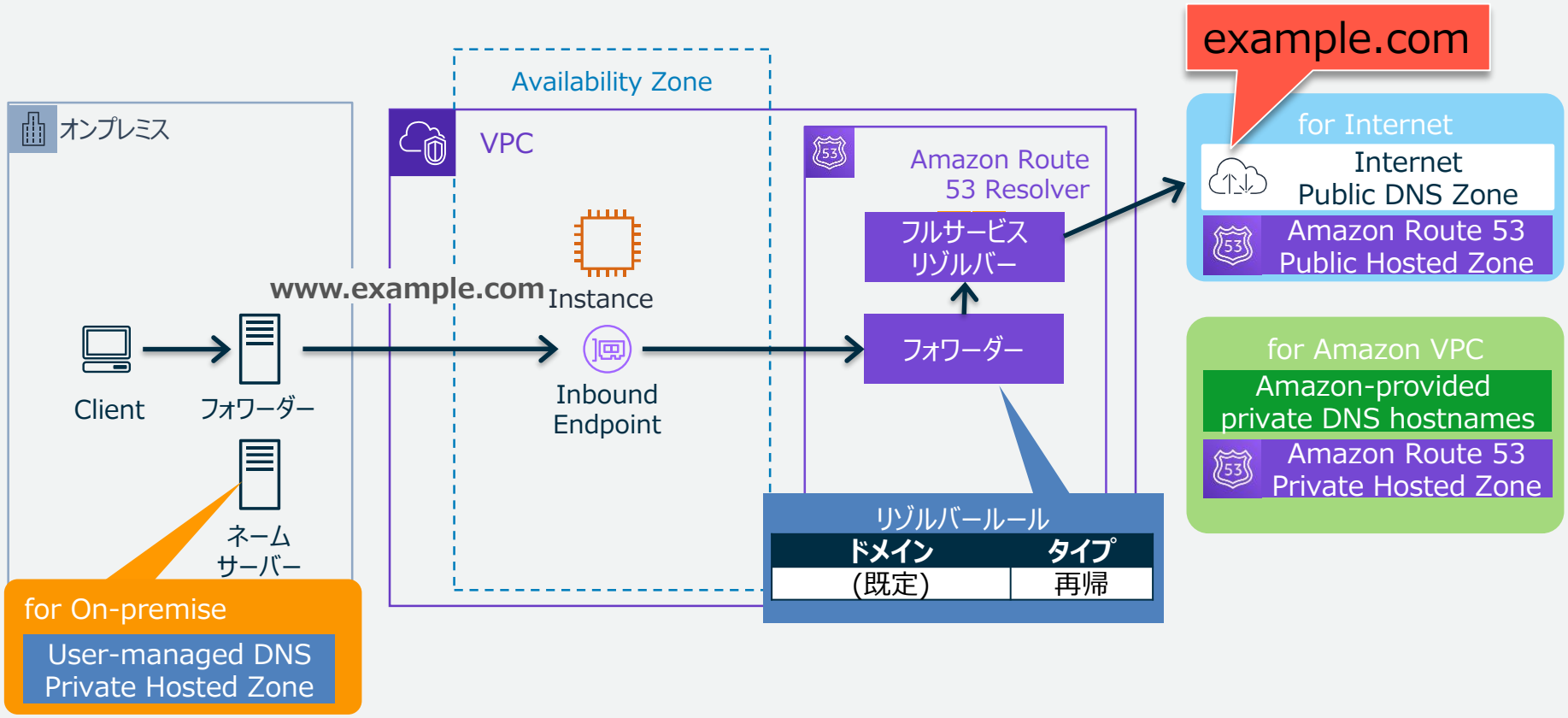
ユースケース①

オンプレミスからVPC向けゾーンの名前解決



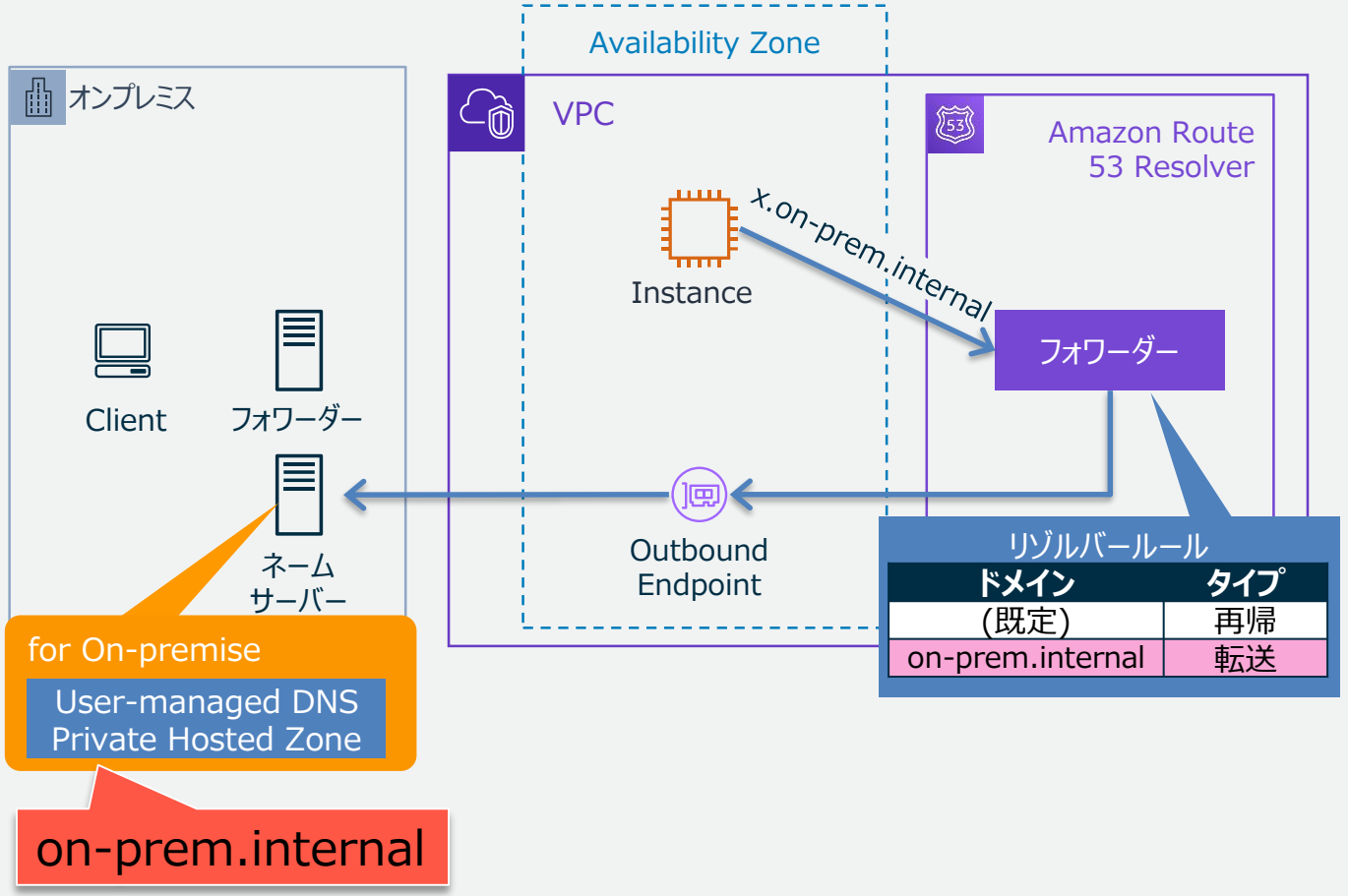
ユースケース②

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



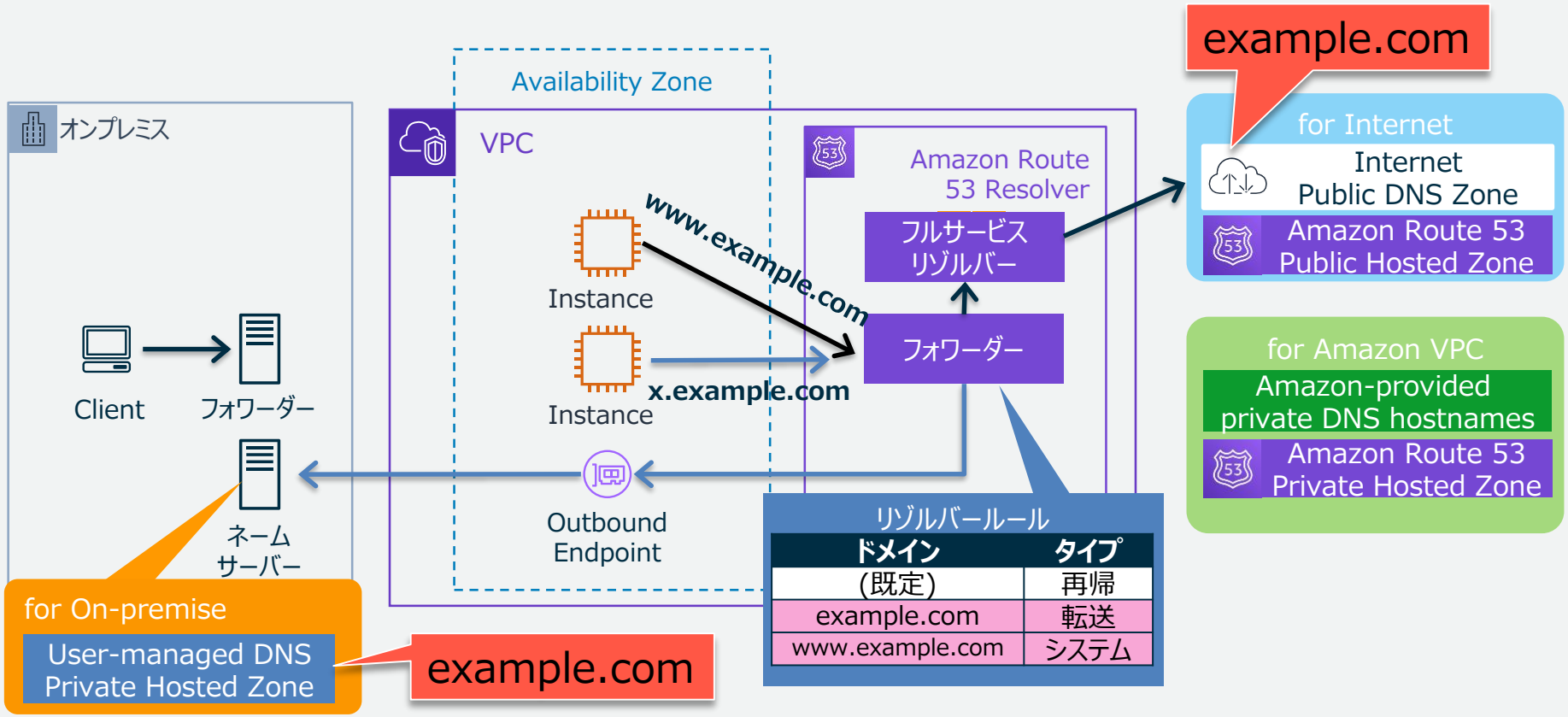
ユースケース③

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

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=ture*

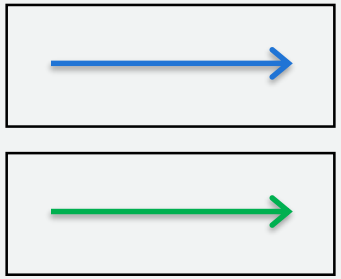
- 以下は自動定義されたシステムルールよりも優先される
  - Route53 プライベートホストゾーンの「PTR」レコード
  - Route53 Resolverの転送ルール

Route53 Resolver の逆引きDNSルールの上書きが可能

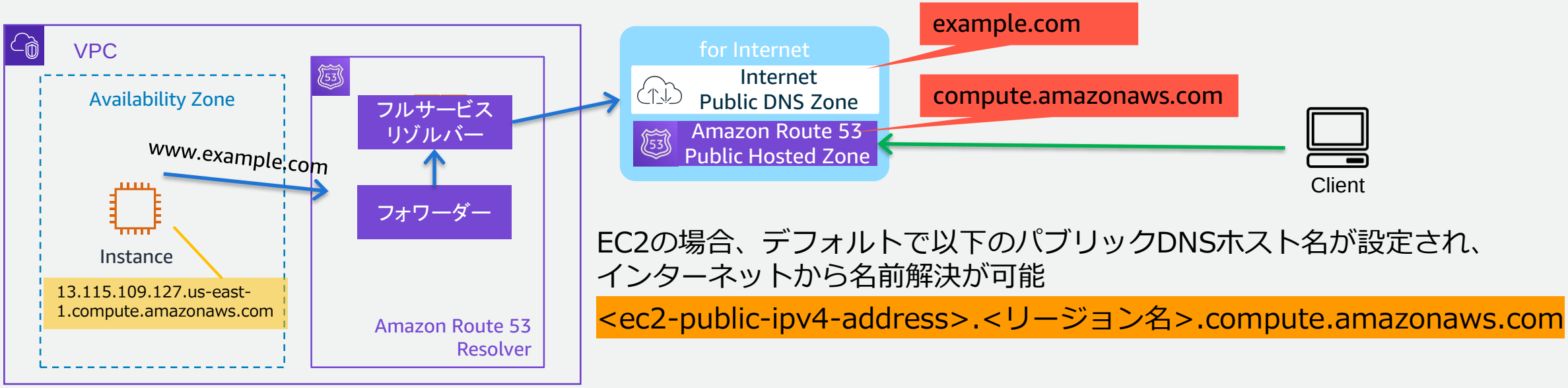
【参考】自動定義されたシステムルール
https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-autodefined-rules

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ホスト名の名前解決（インターネット→AWS）



EC2の場合、デフォルトで以下のパブリックDNSホスト名が設定され、インターネットから名前解決が可能

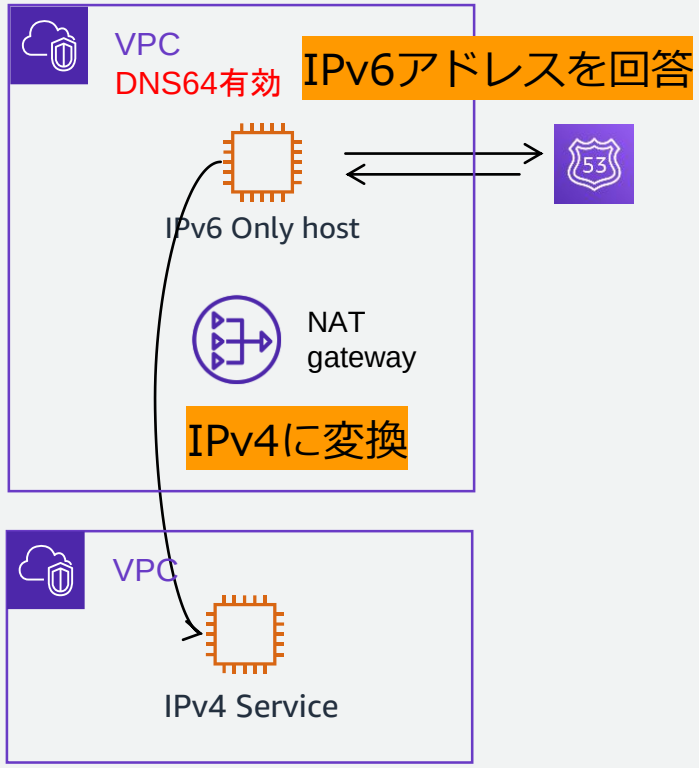
<ec2-public-ipv4-address>.<リージョン名>.compute.amazonaws.com

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ドル * 24時間 * 30日 = 90ドル ≒ 約**12,200**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)

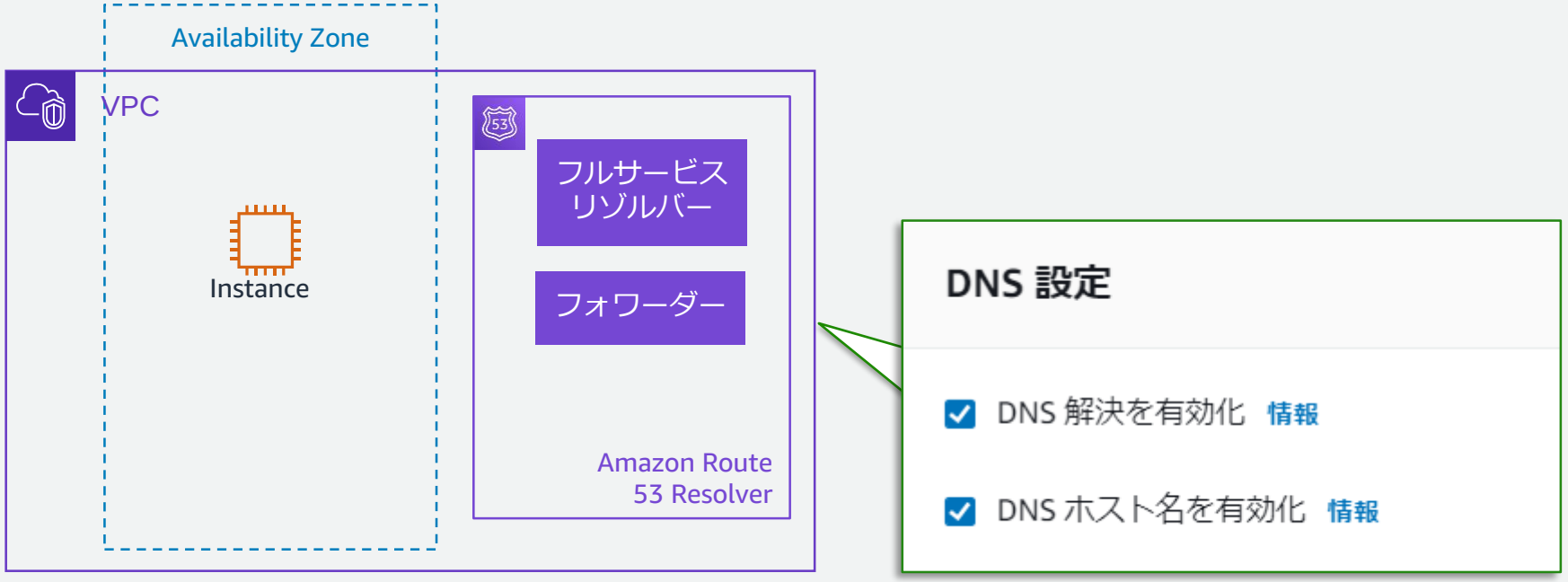
Amazon
Route 53 Resolver
for Hybrid Clouds

- 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

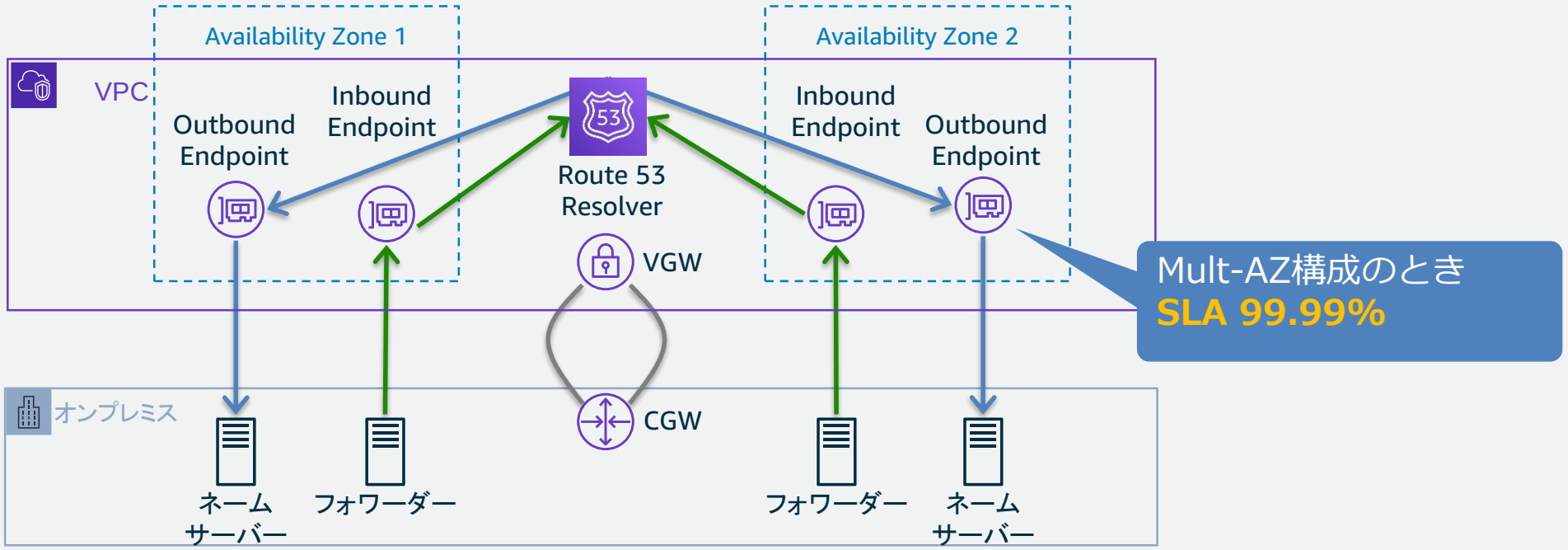
- VPC作成時にデフォルトで有効、必要な場合はVPC毎に有効/無効に設定可能
- IPアドレス設定はDHCPで自動的に配布される



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**

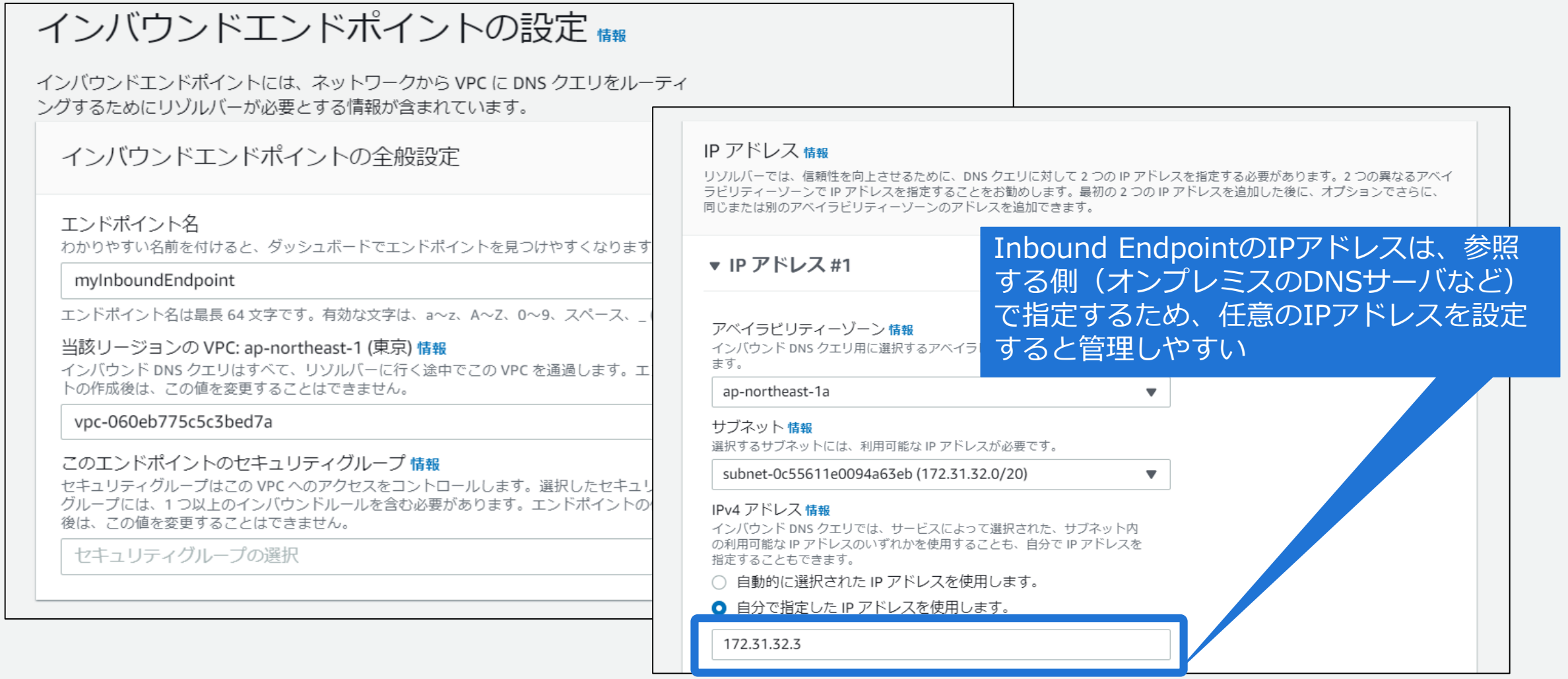
【参考】 Resource Access Manager ユーザーガイド
https://docs.aws.amazon.com/ram/latest/userguide/what-is.html

ここから、具体的な構成手順を見ていきましょう

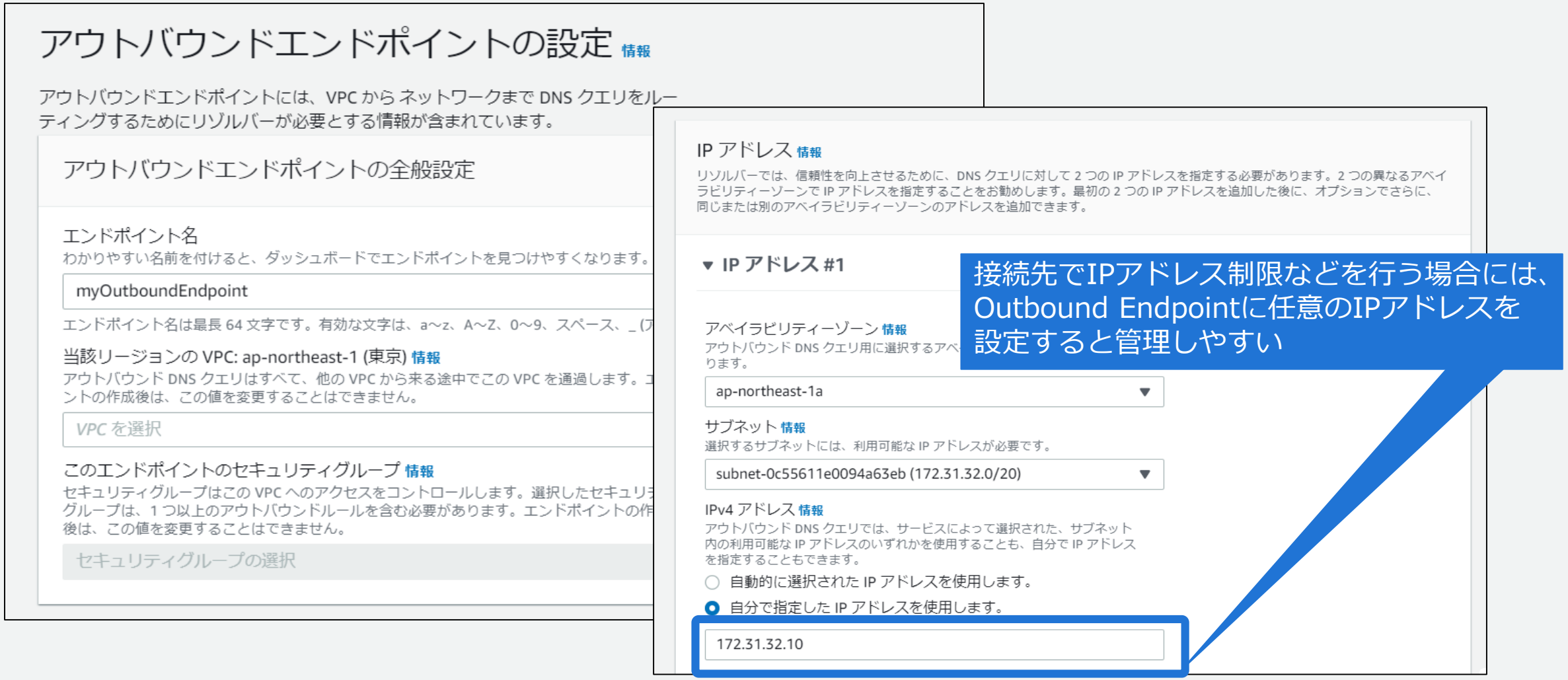
Route 53 Resolver for Hybrid Clouds
Step 1 Get Started

Route 53 Resolver for Hybrid Clouds
Step 2 Choose Endpoints

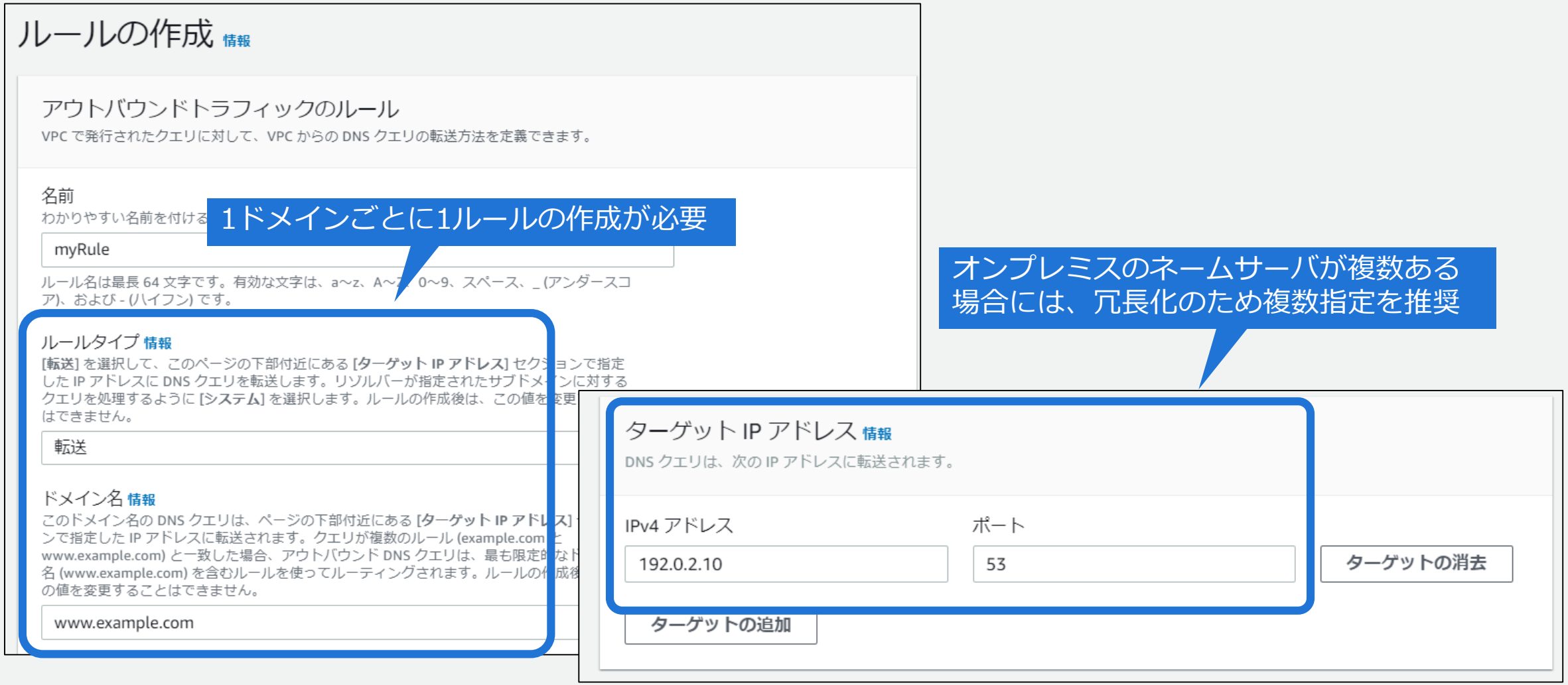
Route 53 Resolver for Hybrid Clouds
Step 3 Configure Inbound Endpoint



Route 53 Resolver for Hybrid Clouds
Step 4 Configure Outbound Endpoint



Route 53 Resolver for Hybrid Clouds
Step 5 Create Rules



テストとトラブルシューティング

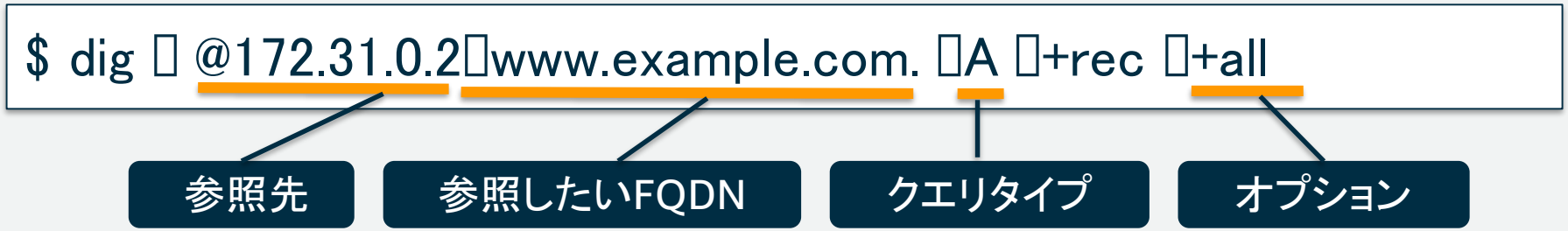
テスト

- 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



- 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出来ます。

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

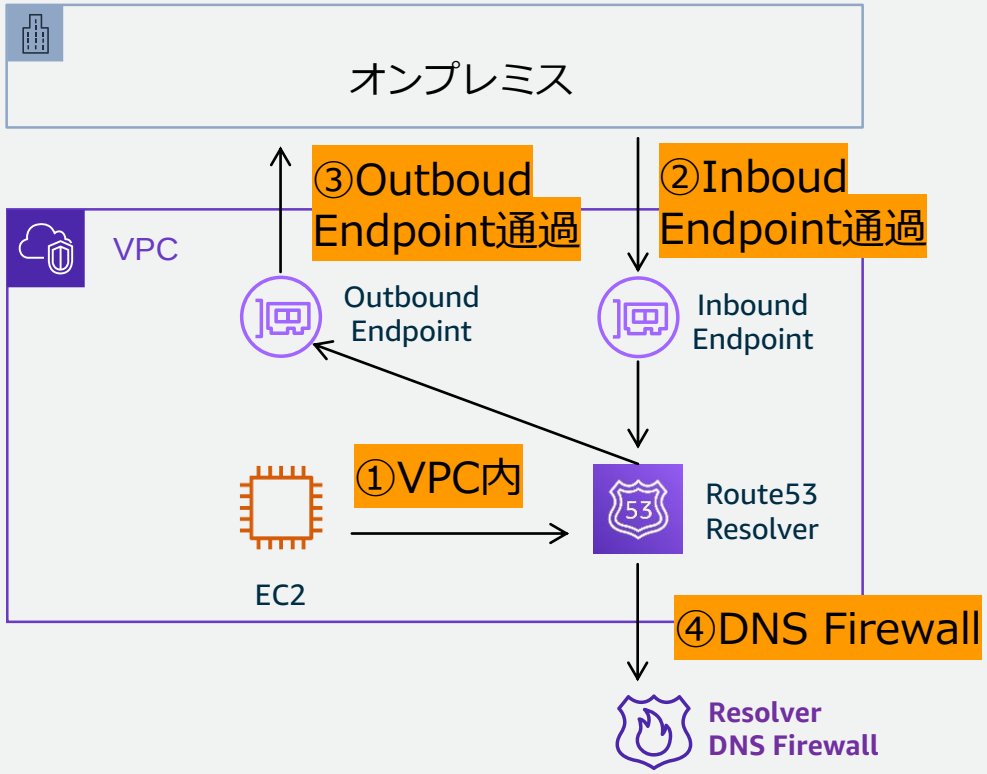
Resolverで、以下のDNSクエリの記録が可能

① 指定VPCで発生するクエリとその応答

② InboudEndpointを通過するオンプレからのクエリ

③ 再帰的なDNS解決にOutboudEndpoint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 クエリに応答して返される 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": “XXXXXXXXXXX”,
    “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

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

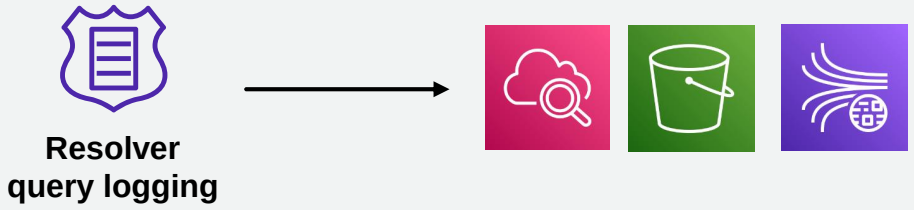
S3バケット

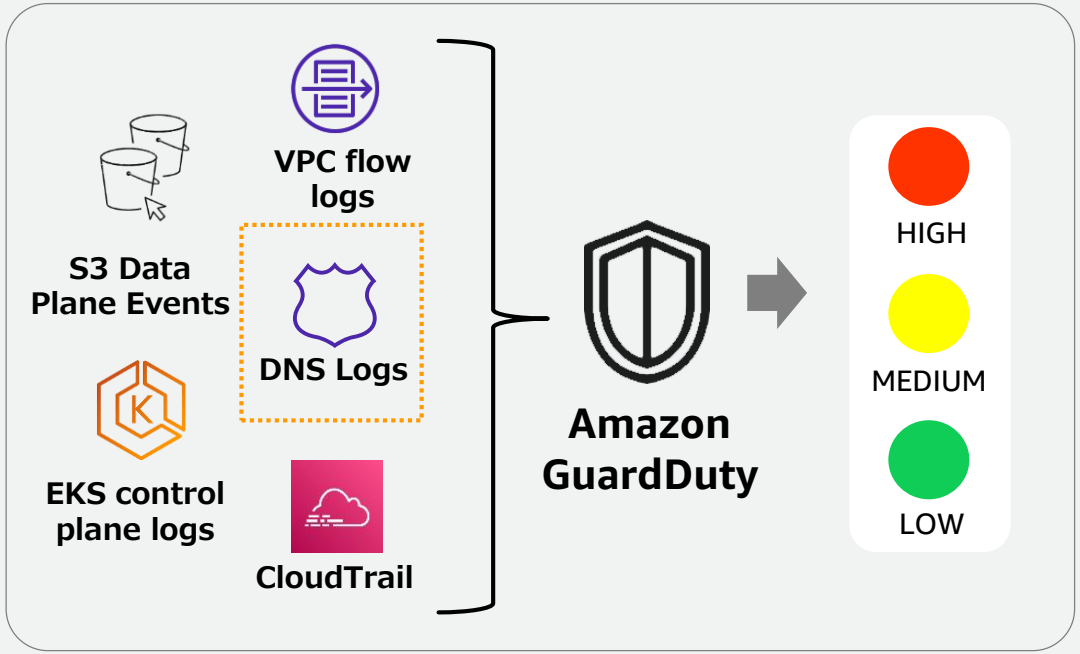
Kinesis Data Firehose の配信ストリーム

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

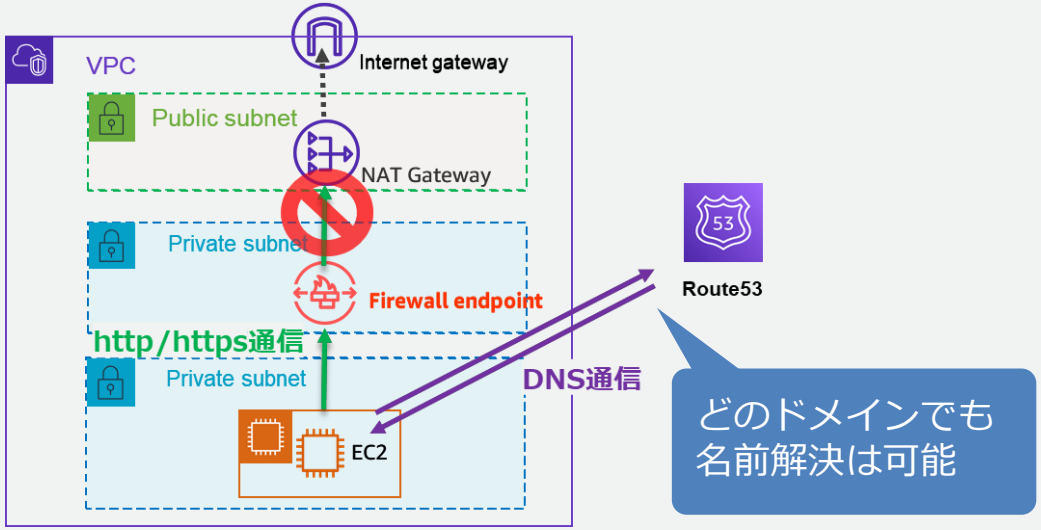
Route 53 Resolver DNS Firewallとは

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

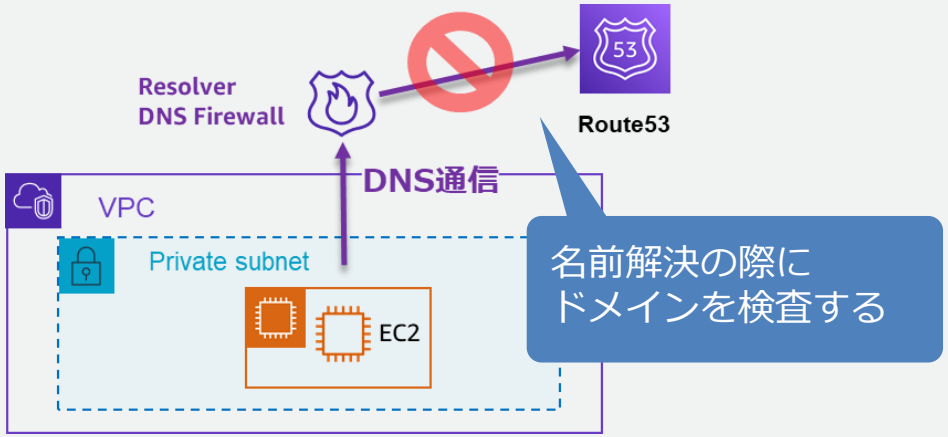
- http/https通信の宛先のドメイン名を検査する
- Firewall Endpointを通過するインバウンド/アウトバウンドが対象



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

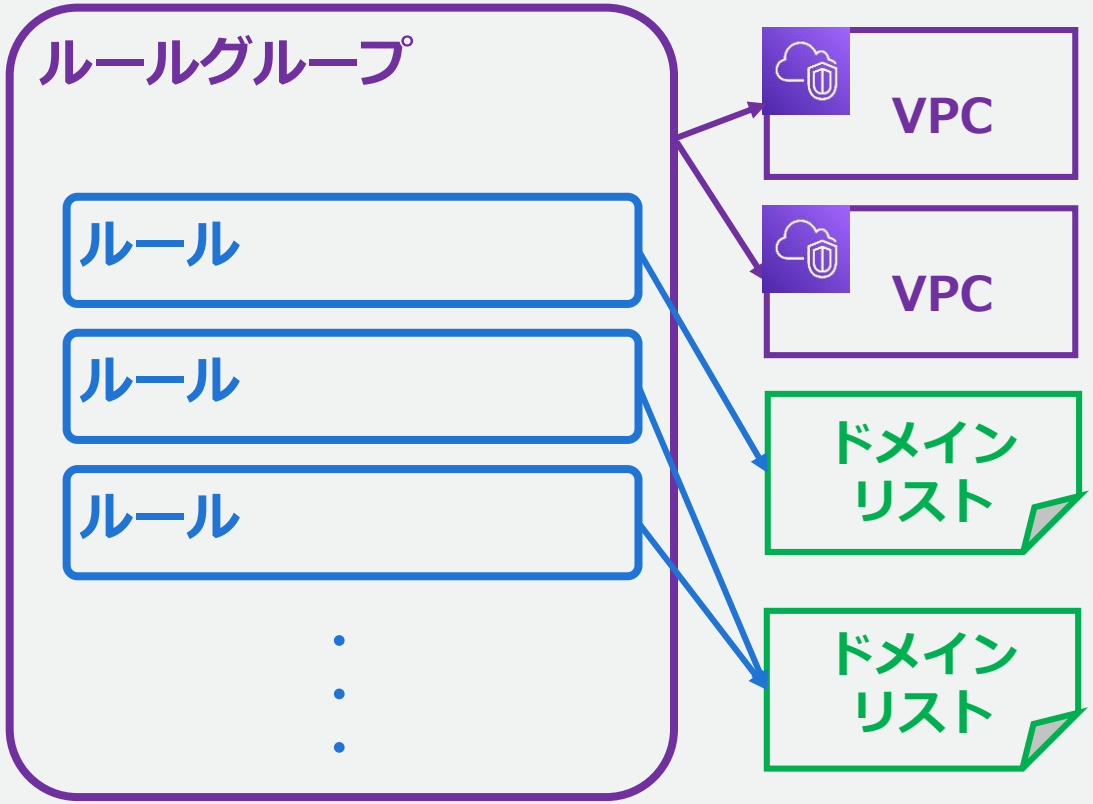


DNS Firewall の設定

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

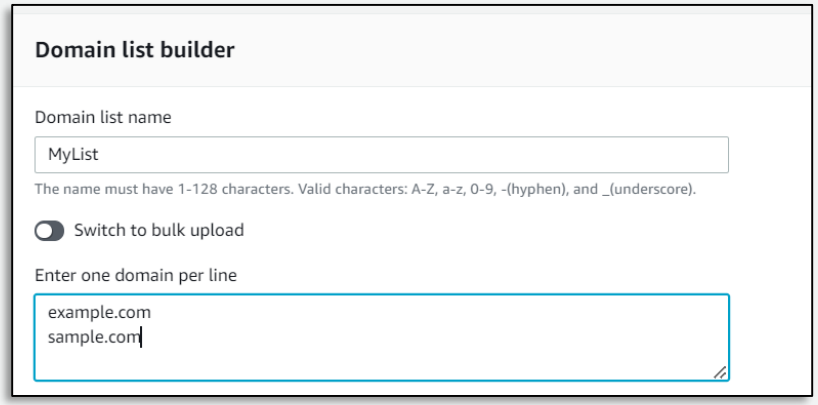


DNS Firewall ドメインリスト

- 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

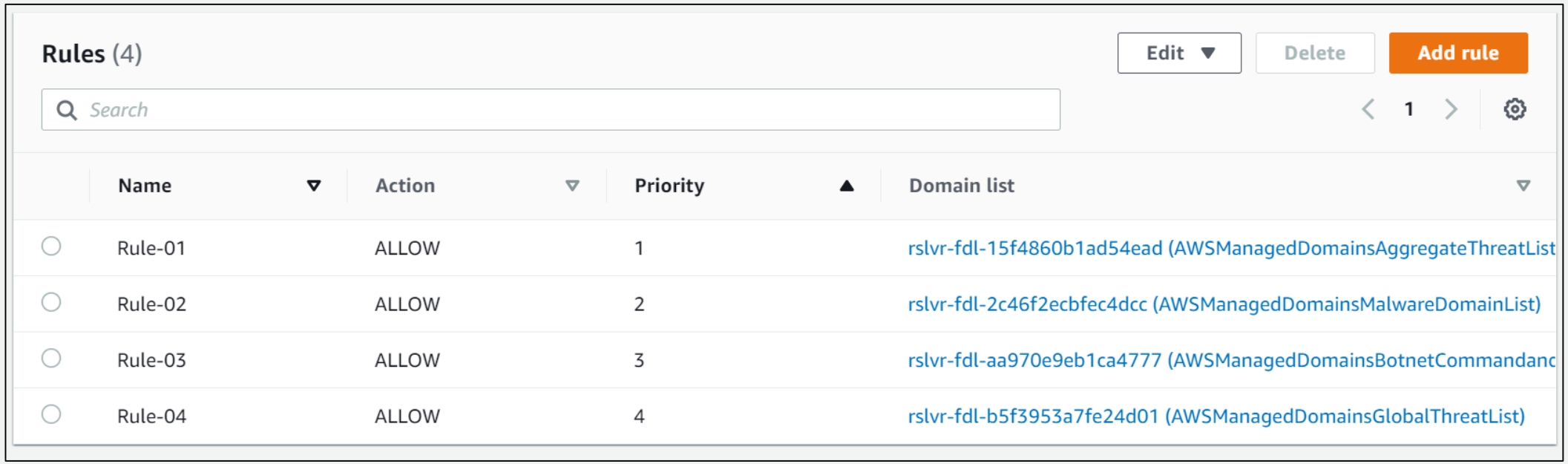


- **AWS マネージドドメインリスト**
  - AWS が作成し管理する
  - 新しい脆弱性と脅威が出現するとリストは自動的に更新される
  - ユーザによる編集、閲覧、ダウンロードは不可

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



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

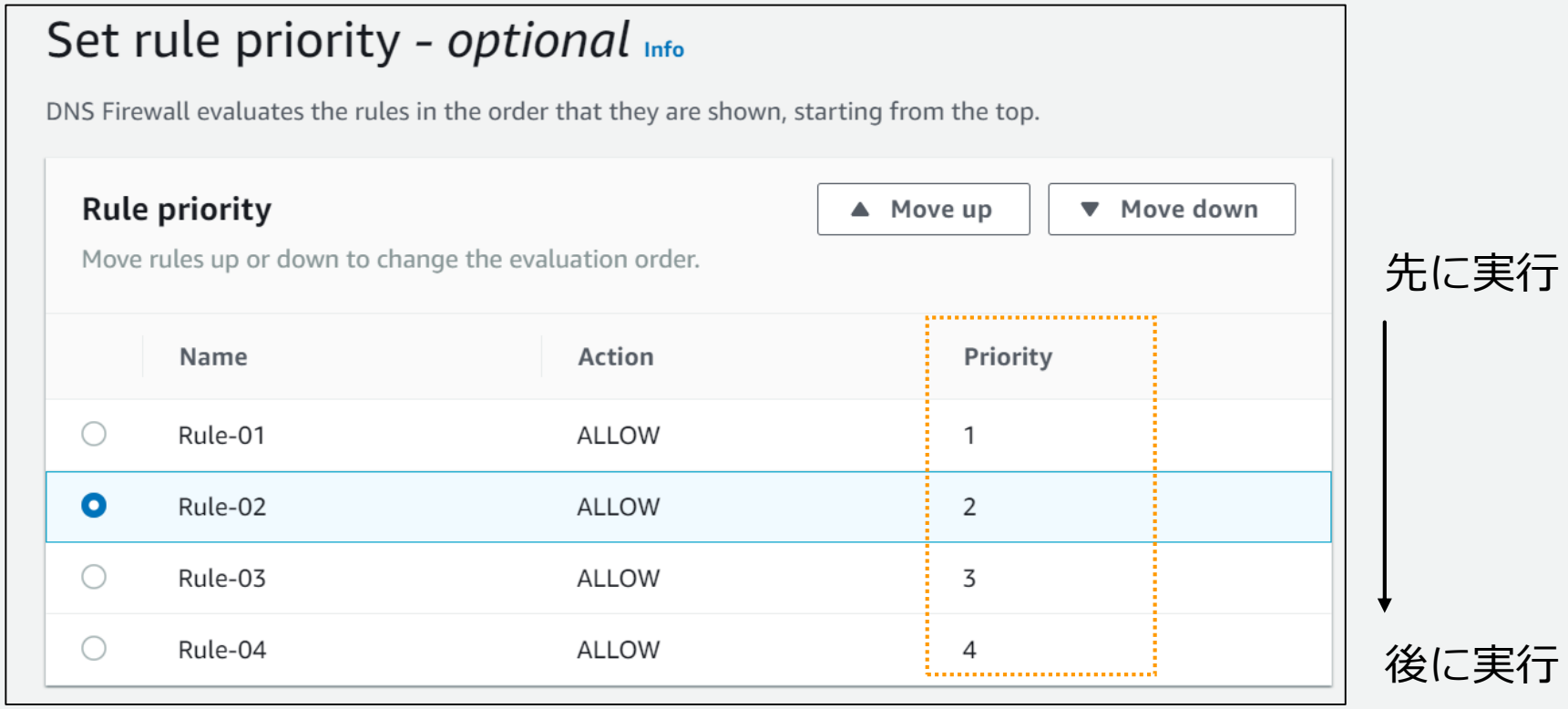
DNS Firewall のBlockアクションについて

- 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を調査することで、
    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

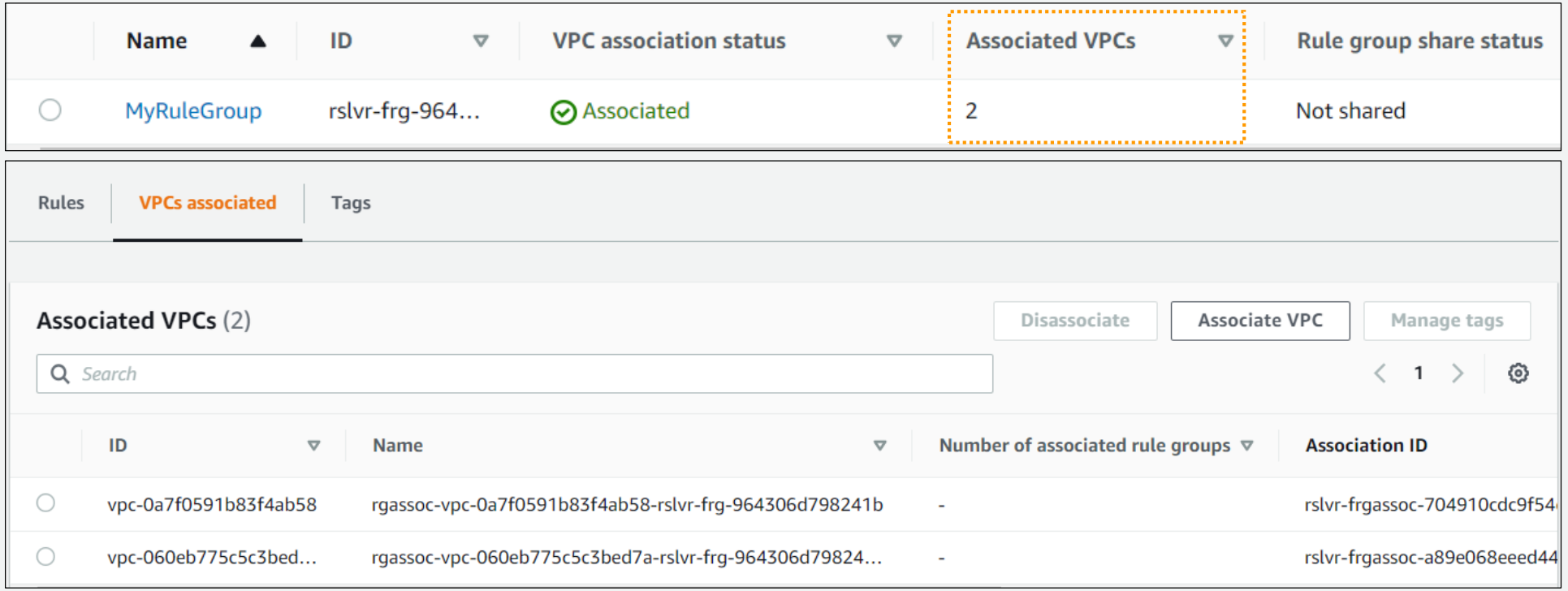
DNS Firewall ルールの優先度

- 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



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



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

- 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定

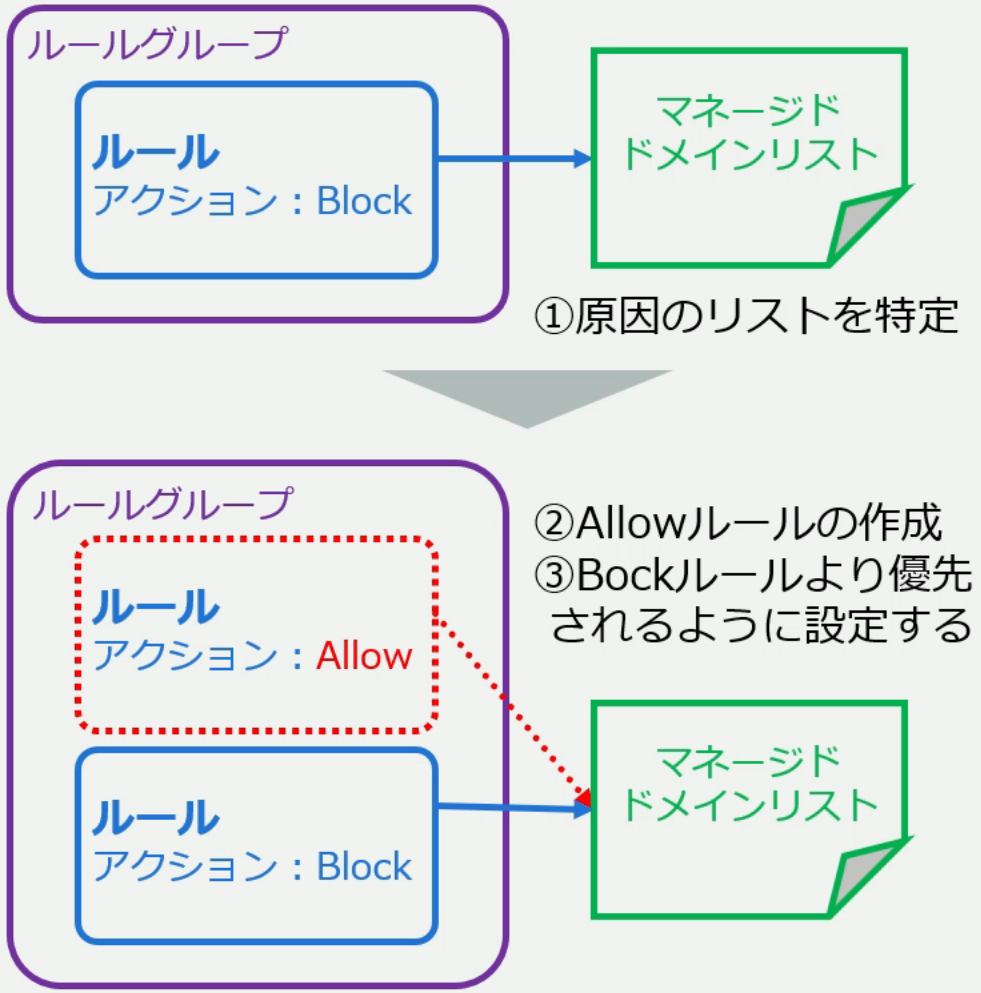
- Resolver ログを確認し、誤検出の原因となっているルールグループとマネージドドメインリストを特定

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

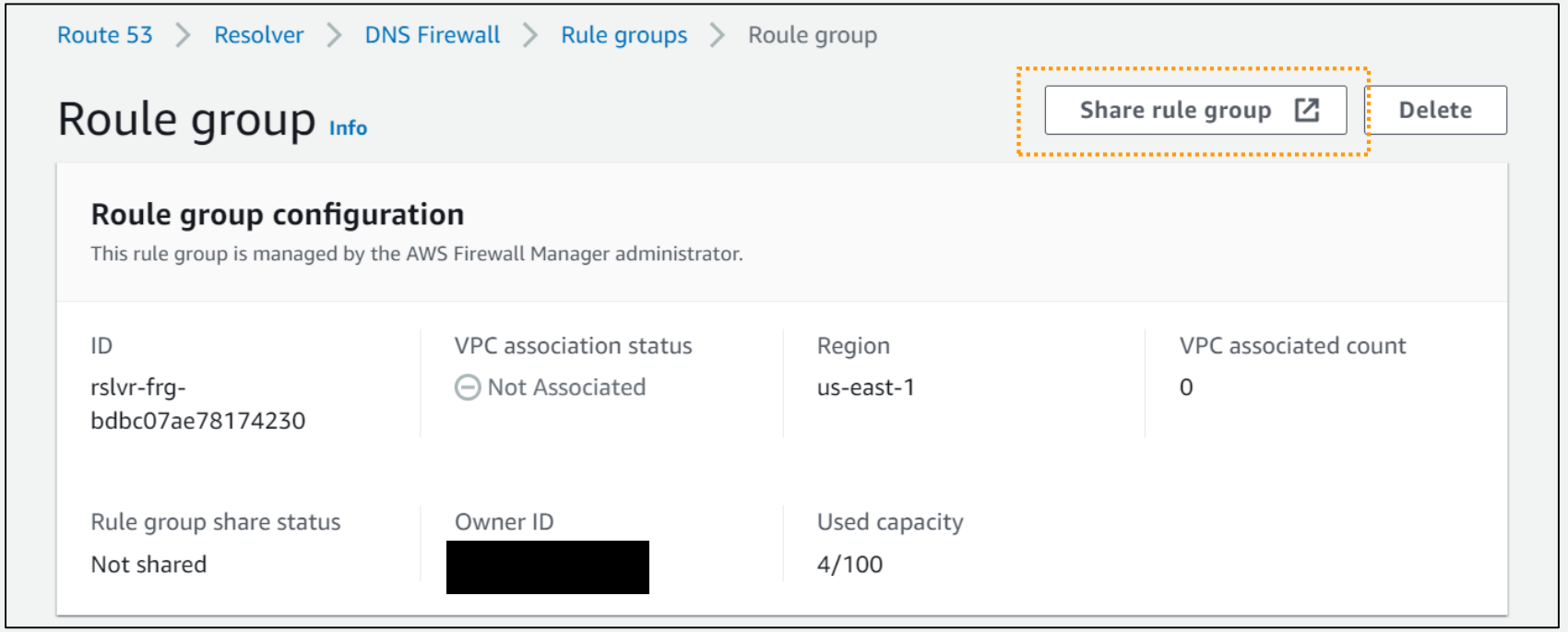
- ルールグループ内で新しいルールの優先度の値を①のマネージドリストを使用しているルールの数値より小さく設定する

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



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」

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/OutboudEndpoint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
  - Nework 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=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY

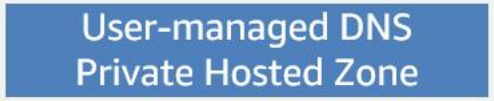
ご感想は Twitter へ！ハッシュタグは以下をご利用ください
#awsblackbelt

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。