[AWS Black Belt Online Seminar] Amazon Route 53 Resolver

サービスカットシリーズ

Security Solutions Architect 中島 智広
2019/10/16

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

自己紹介

中島　智広（Tomohiro Nakashima）

AWS Security Solutions Architect
お客様のセキュリティの取り組みを
AWSアーキテクチャの視点からご支援

Background

DNSのセキュリティや運用技術の普及啓蒙に取り組む
日本DNSオペレーターズグループ（DNSOPS.JP）の運営メンバー

好きなAWSサービス

Amazon Route 53 / Amazon Route 53 Resolver

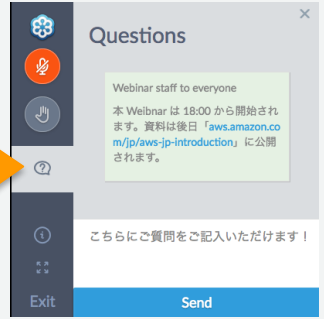
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾン ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
  お答えできませんのでご了承下さい

① 吹き出しをクリック
② 質問を入力
③ Sendをクリック



Twitter 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2019年10月16日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。最新の情報はAWS公式ウェブサイト(http://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が東京リージョンを使用する場合、別途消費税をご請求させていただきます。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

ご案内：Amazon Route 53は全2回でお届けします

本日の内容

Amazon Route 53 Resolver 10/16 (水) 18:00-19:00

はじめにDNSの基本を解説し、Amazon Route 53 Resolverの機能である、Route 53 Resolver Endpoints、Conditional Forwarding Rulesを用いてハイブリッド環境の名前解決を最適化する手法を学びます。

Amazon Route 53 Hosted Zone 11/5 (火) 12:00-13:00

ネームサーバー機能を提供するAmazon Route 53のHosted Zoneについて解説します。インターネットに名前解決を提供するパブリックホストゾーン、VPC内に限定して名前解決を提供するプライベートホストゾーンを中心にAmazon Route 53の活用法を学びます。

aws

本セミナーの概要

DNS(Domain Name System)の基本をおさらいした後、

Amazon Route 53 Resolverの活用方法を取り上げます。

1. DNSの基本
2. AWSが提供するDNSサービスと機能
3. Amazon Route 53 Resolverの構成

1. DNSの基本

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

ホスト名とFQDN（完全修飾ドメイン名）

ホスト名
サーバや端末に付けられた名前、「相対ドメイン名」「不完全なドメイン名」とも呼ばれる

例）
www1

FQDN（完全修飾ドメイン名）
サブドメインからトップレベルドメインまで完全に指定されたホスト名

例）
www1.sub.example.com.
ip-*private-ipv4-address*.ec2.internal.

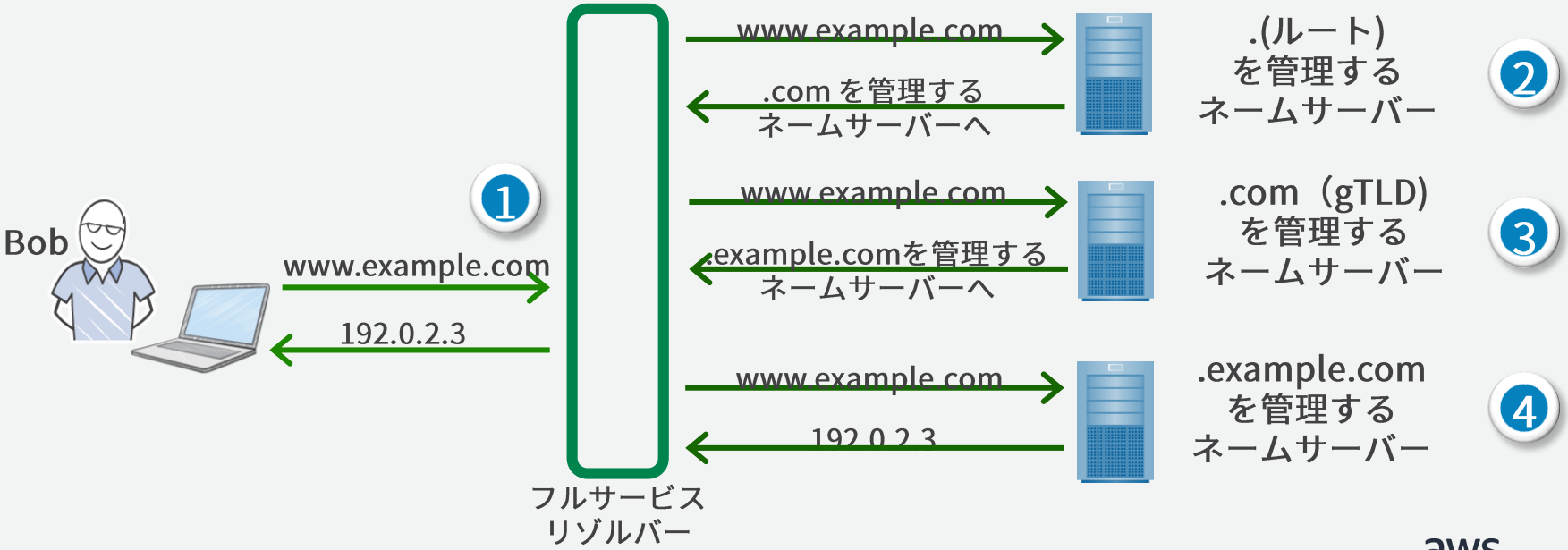
※ルートは「.」で表されるため、 狭義の意味でのFQDNを表記する際には、末尾の「.」まで含めて表記する

ノードが一意に識別されることを前提にしていない相対的な名前

特定のドメイン名空間において、ノードを一意に識別が可能な名前

DNS (Domain Name System)

- FQDNをキーに対応するIPアドレスなどの情報を取得する仕組み
- DNSから情報取得することを「名前解決（Name Resolution）」と呼ぶ
- 各ネームサーバが管理する名前空間を「ゾーン（Zone)」と呼ぶ



DNSサーバーとは何か？

DNSを構成するサーバーはシンプルに「DNSサーバー」と呼ばれることが多いが、実際には以下の4つの異なる機能を持つ実装である。

① ネームサーバ ー/ Name Server

② フルサービスリゾルバー/Full Service Resolver

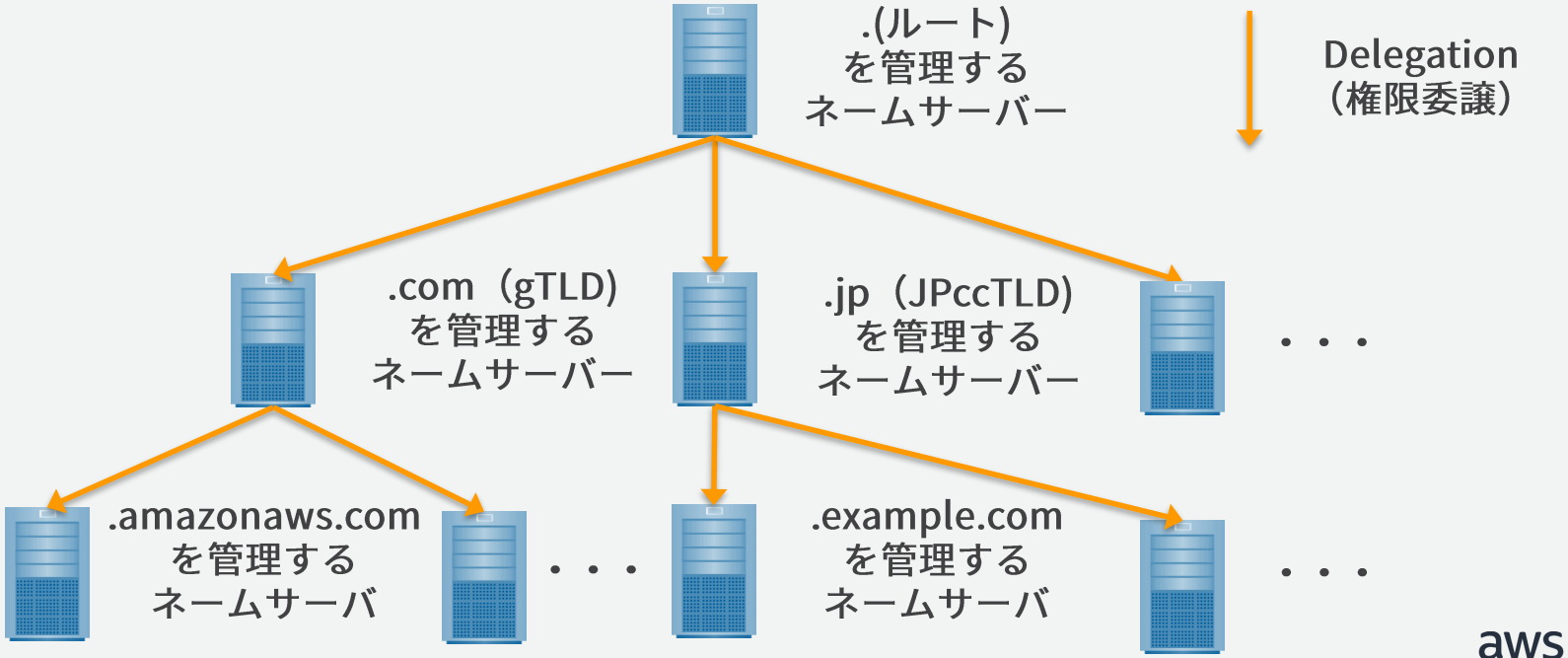
③ スタブリゾルバー/ Stub Resolver

④ フォワーダー / Forwarder

本セミナーではDNSの理解のため、4つを区別をしながら説明してきます。

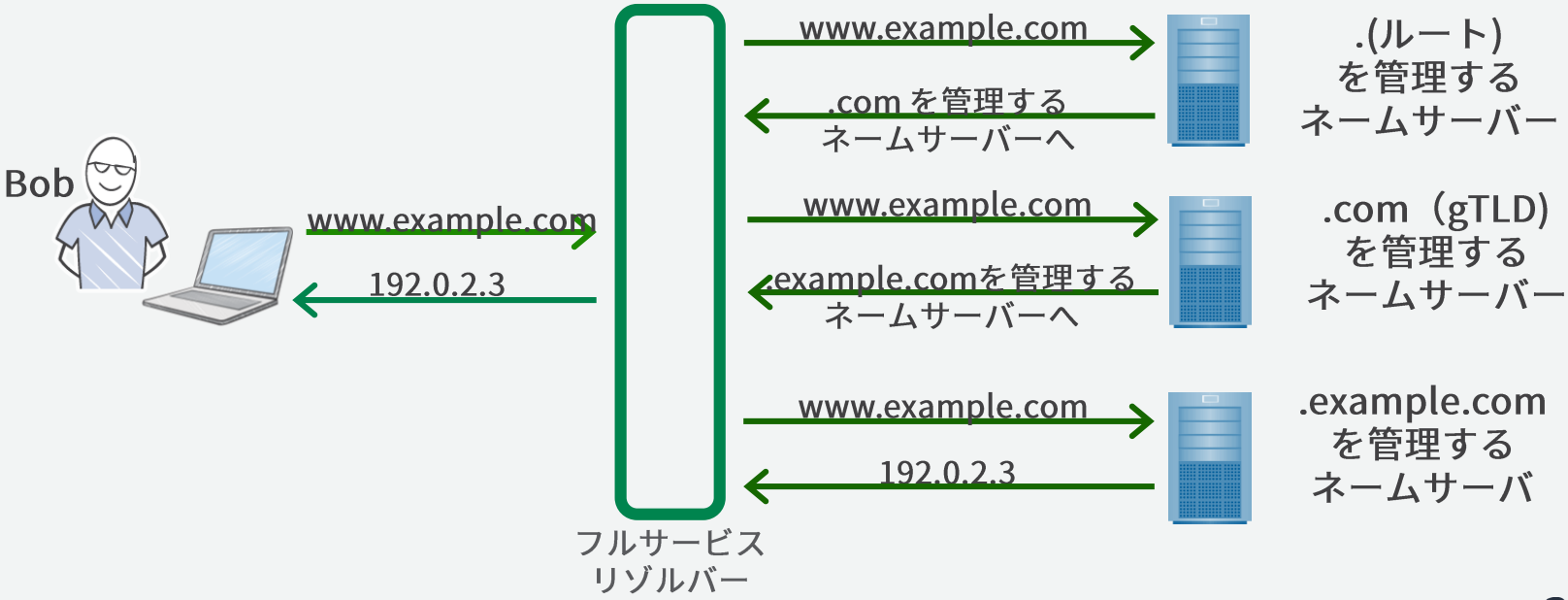
①ネームサーバ / Name Server

- .(ルート）を起点に全てのFQDNを探索できるように構成された
  分散データベース、およびそれを成すひとつひとつのネームサーバー
- 権威DNSサーバ / Authoritative Serverと表現される場合もある



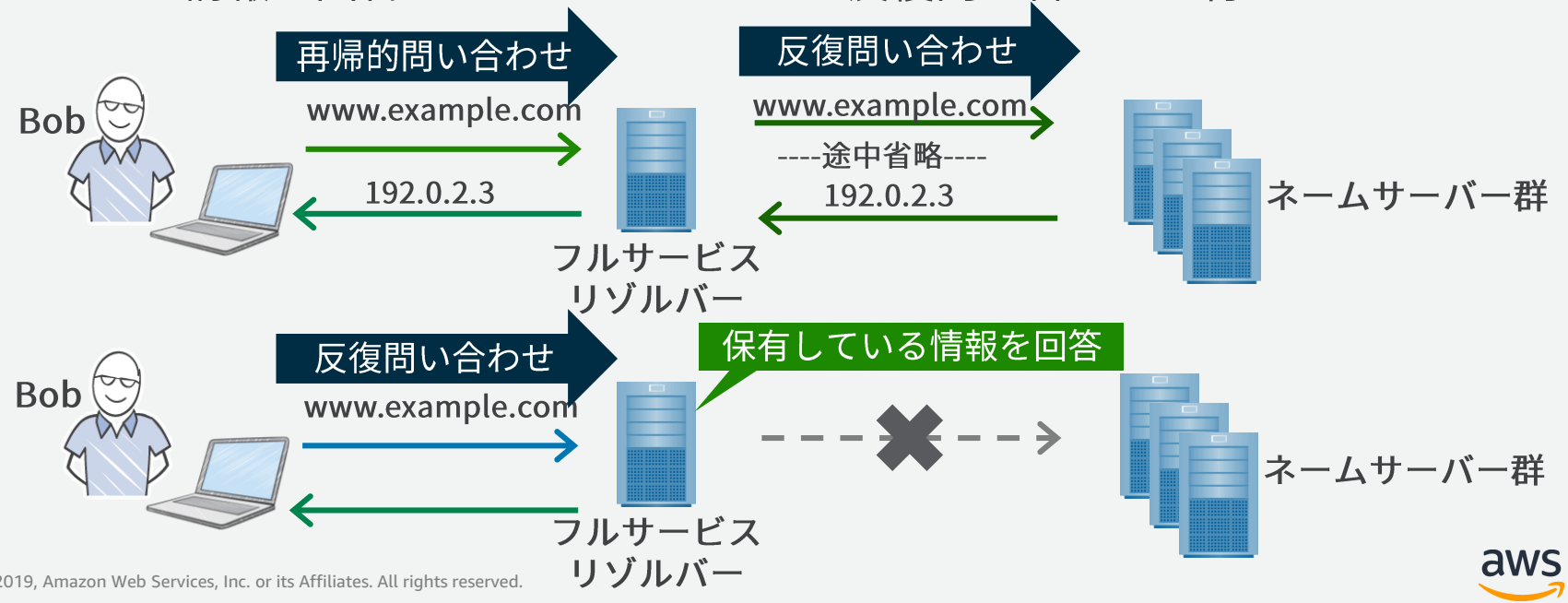
②フルサービスリゾルバ/ Full Service Resolver

- .(ルート）から順にネームサーバに問い合わせ、得られた回答を問い合わせ元に返す機能を有するサーバー実装
- 効率化のため所定の期間（TTL）キャッシュを保持する



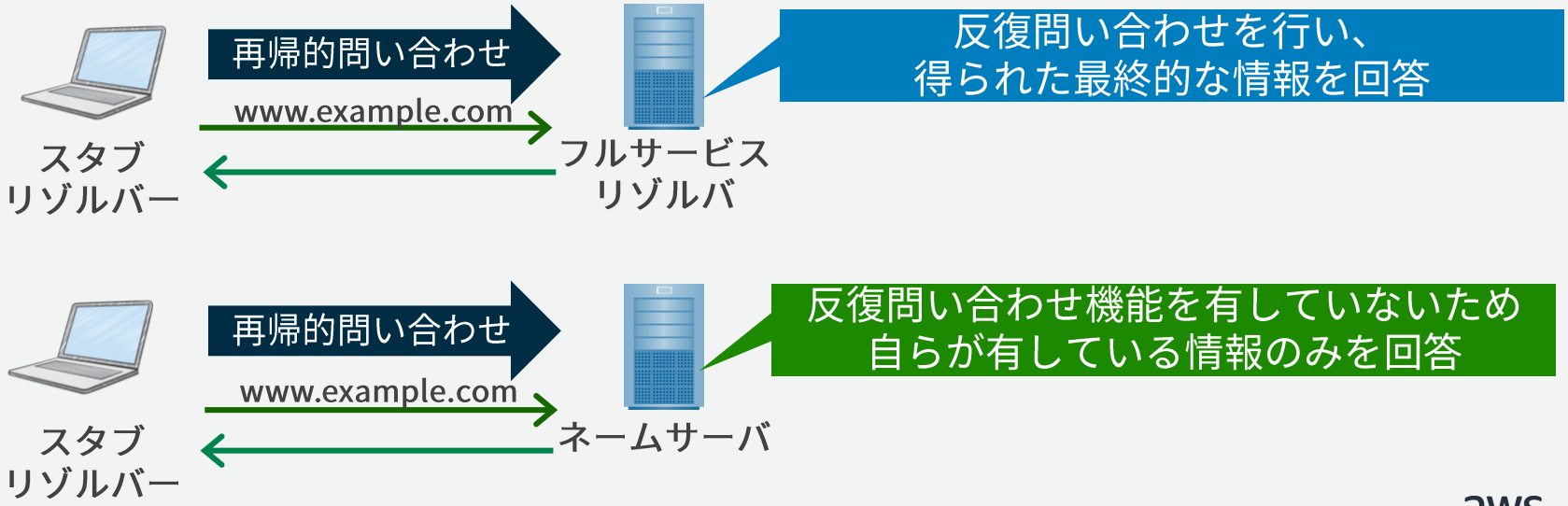
再帰的問い合わせと反復問い合わせ

- 反復問い合わせは、自らがネームサーバを辿る際に行う問い合わせ
- 再帰的問い合わせは、問い合わせ先に反復問い合わせを依頼する問い合わせ
- フルサービスリゾルバーが反復問い合わせを受け取った場合、自らが保有している情報を回答し、ネームサーバへの反復問い合わせは行わない



③スタブリゾルバー/Stub Resolver

- 一般にはOSに組み込まれたDNSクライアント実装
- .(ルート）からネームサーバを辿る反復問い合わせの機能を持たないため、常に再帰的問い合わせを行う
- キャッシュの有無は実装に依存



スタブリゾルバー/Stub Resolverの制約

複数のDNSサーバーに対し、ドメイン毎に振り分けたり、同時に利用したりする機能は有していない

Amazon Linux（libresolv）
/etc/resolv.conf

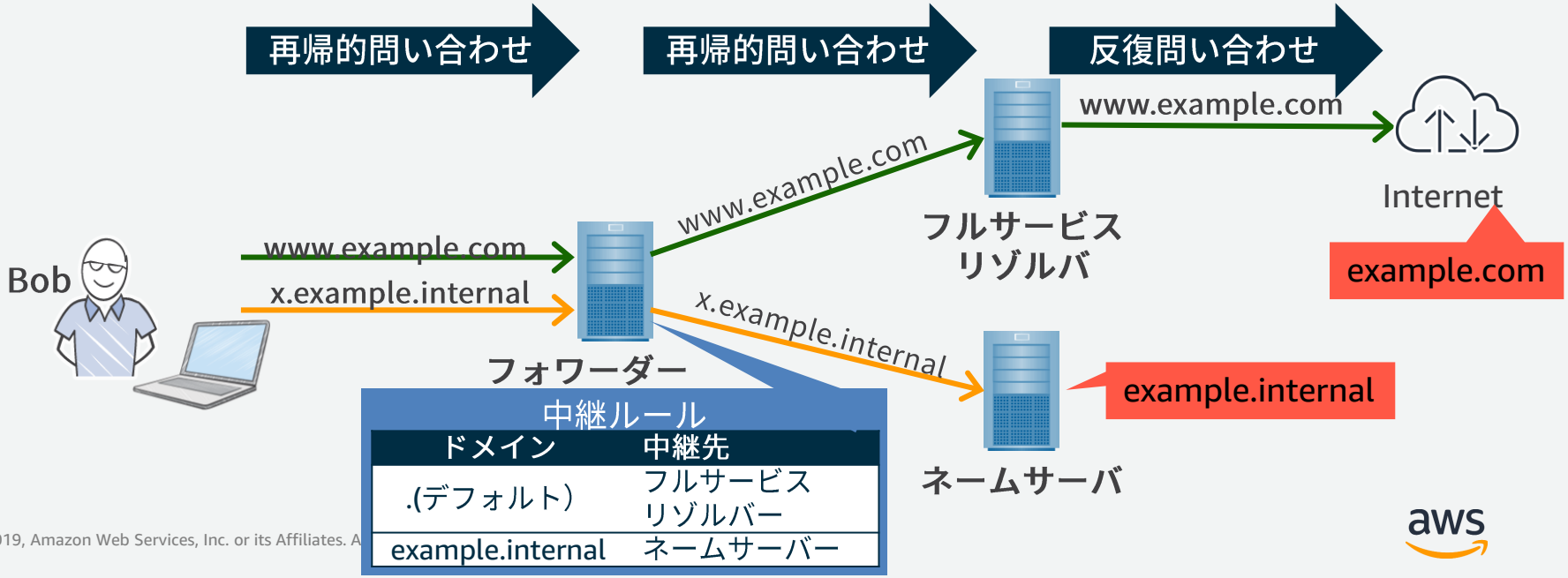
```
options timeout:2 attempts:5
search example.internal
nameserver 192.0.2.2
nameserver 198.51.100.2
```

Windows (Windows DNS Client)
ネットワークインターフェイスの設定

サーバーを複数指定するのは障害時のフォールバックのため、
名前解決に失敗した場合、順に問い合わせをしていく

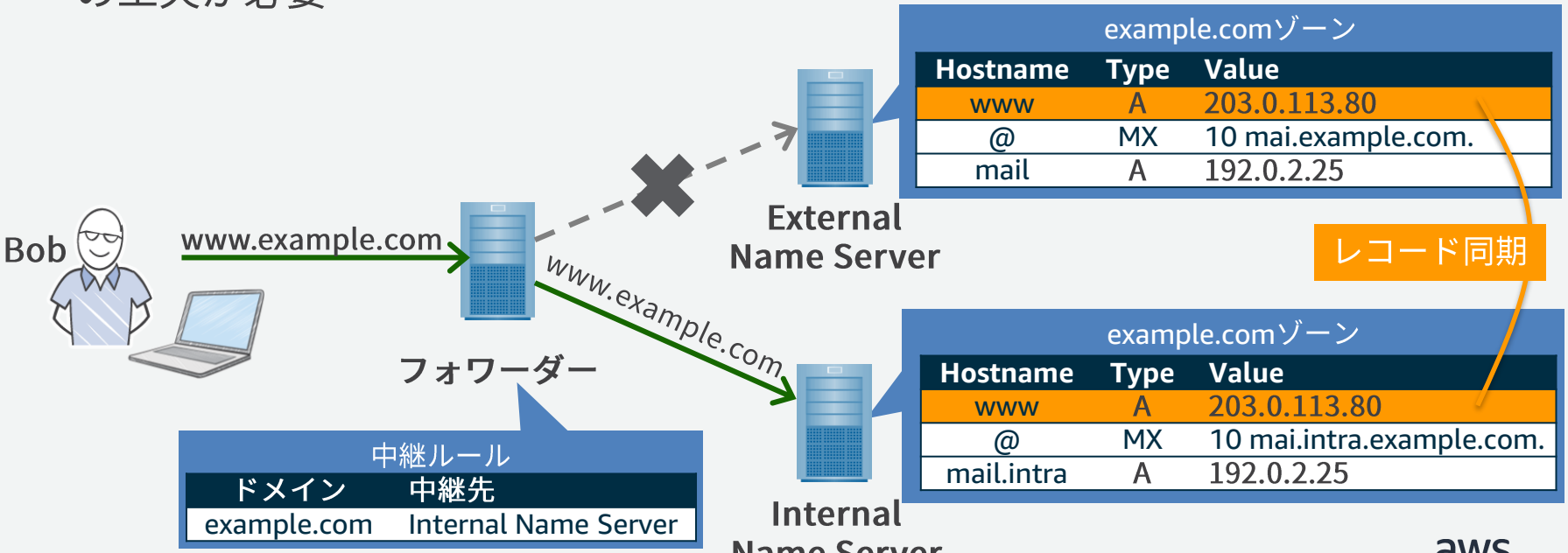
④フォワーダー/Forwarder

- 受け取った問い合わせを、ルールに基づいて中継する実装
- .(ルート）からネームサーバを辿る反復問い合わせの機能を持たないため、常に再帰的問い合わせを行う
- 効率化のため所定の期間（TTL）キャッシュを保持する



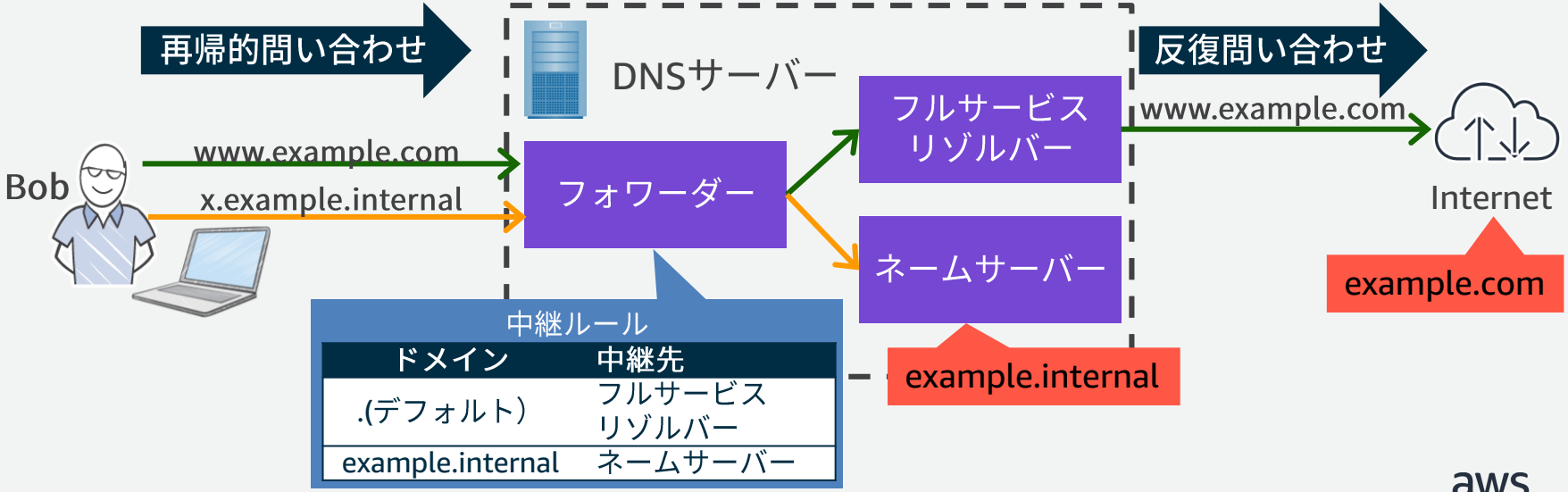
フォワーダー/Forwarderの制約

- インターネット向けネームサーバーと内部ネットワーク向けネームサーバーで同じドメイン名を利用している場合に両方を参照することができない
- ドメインやホスト名を分ける、必要なデータ（レコード）を同期させるなどの工夫が必要



企業ネットワークのよくあるDNSサーバー構成

- フォワーダー、フルサービスリゾルバー、ネームサーバーが同居して、1つのDNSサーバを構成
- 著名なDNSサーバー実装のいくつかは、これら複数の機能を有しているため、管理者が意図せずこのような構成を採っていることが多い



DNSの基本まとめ

- DNSサーバの4つの機能や制約を理解する
    - ① ネームサーバ ー/ Name Server
    - ② フルサービスリゾルバー/Full Service Resolver
    - ③ スタブリゾルバー/ Stub Resolver
    - ④ フォワーダー / Forwarder

- 問い合わせの違いを理解する
    - ① 再帰的問い合わせ
    - ② 反復問い合わせ

- 企業ネットワークのよくあるDNSサーバー構成を理解する

2. AWSが提供するDNSサービスと機能

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

AWSが提供するDNSサービスと機能

本セミナーでは以下のサービスが有する代表的な機能に絞ってご紹介します。

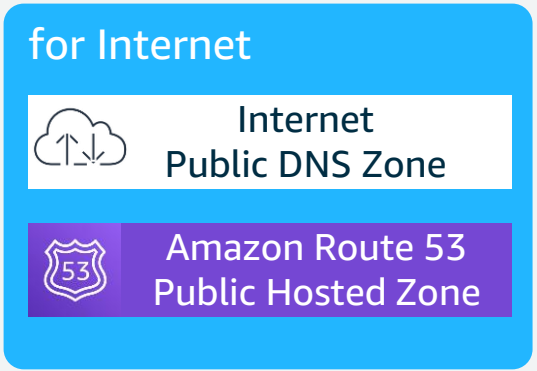
Amazon
Route 53

Amazon
Route 53 Resolver

Amazon
Route 53 Resolver
for Hybrid Clouds

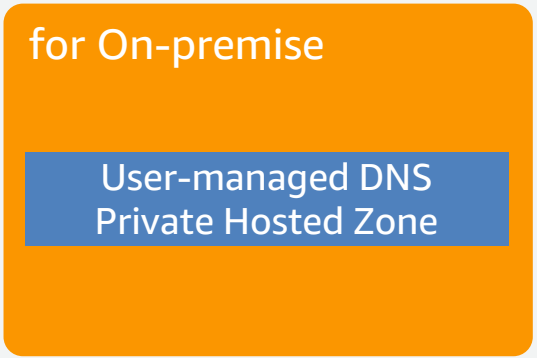
AWSと名前空間（ゾーン）の整理

AWSのユーザー、コンポーネントはさまざまな名前空間（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）

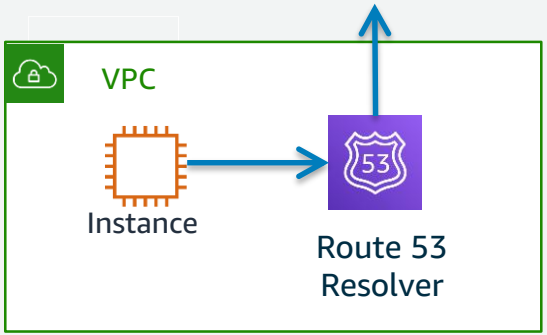
- ネームサーバをマネージドで提供するサービス
- 特定のVPCからの問い合わせと、それ以外からの問い合わせを識別し、異なる応答を返すことができる

Amazon Route 53
Public Hosted Zone

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

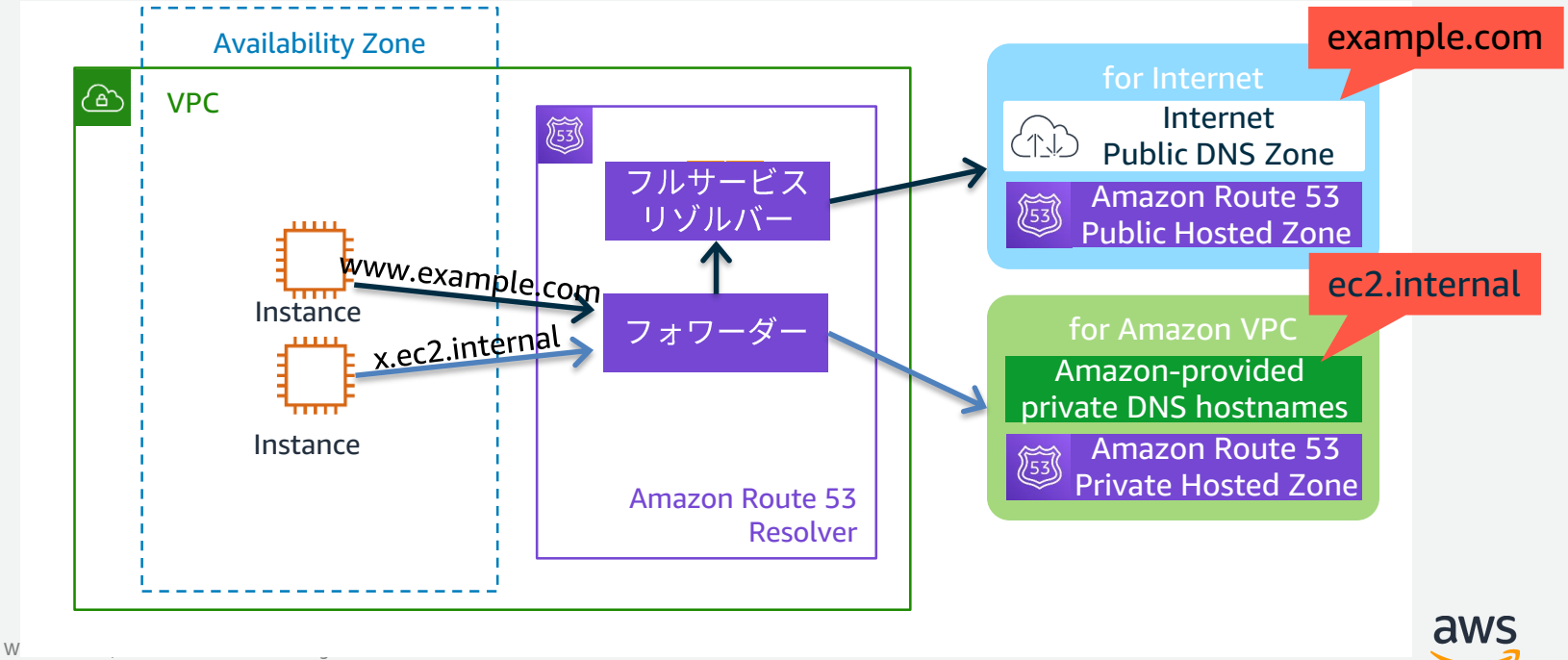
Amazon Route 53
Private Hosted Zone

VPCに閉じたプライベートネットワーク内のDNSドメインのレコードを管理するコンテナ



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



Amazon Route 53 Resolver for Hybrid Clouds

- ハイブリッド環境での名前解決を一元化するRoute 53 Resolverの拡張機能、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ている場合に、双方のゾーンを併用した名前解決

- 以下の新しいコンポーネントから構成

Outbound Endpoint

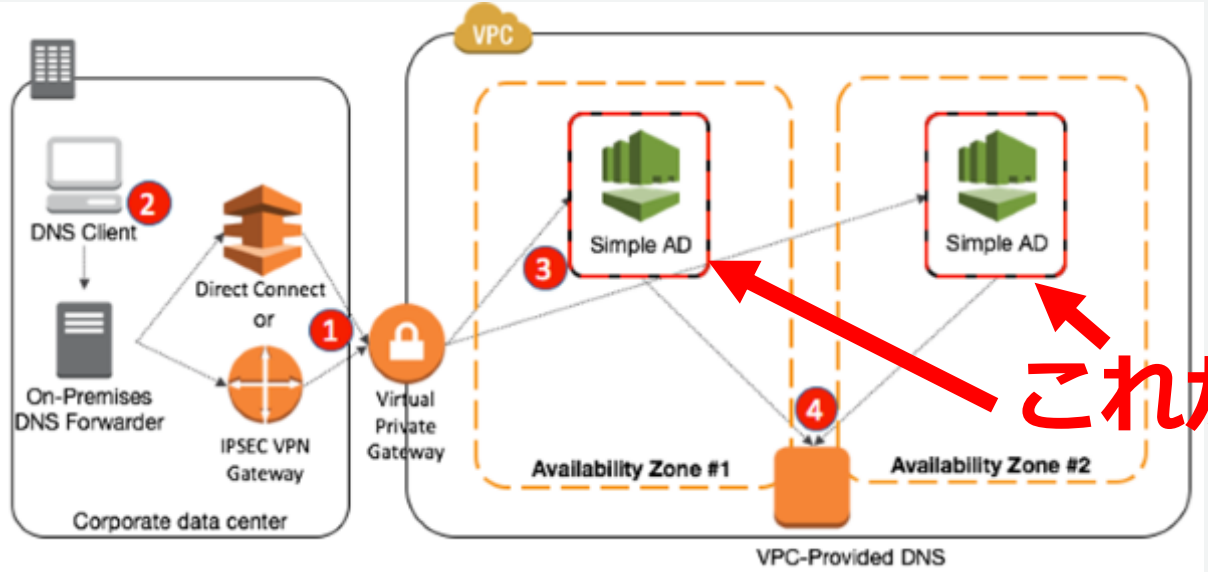
Inbound Endpoint

リゾルバールール

aws

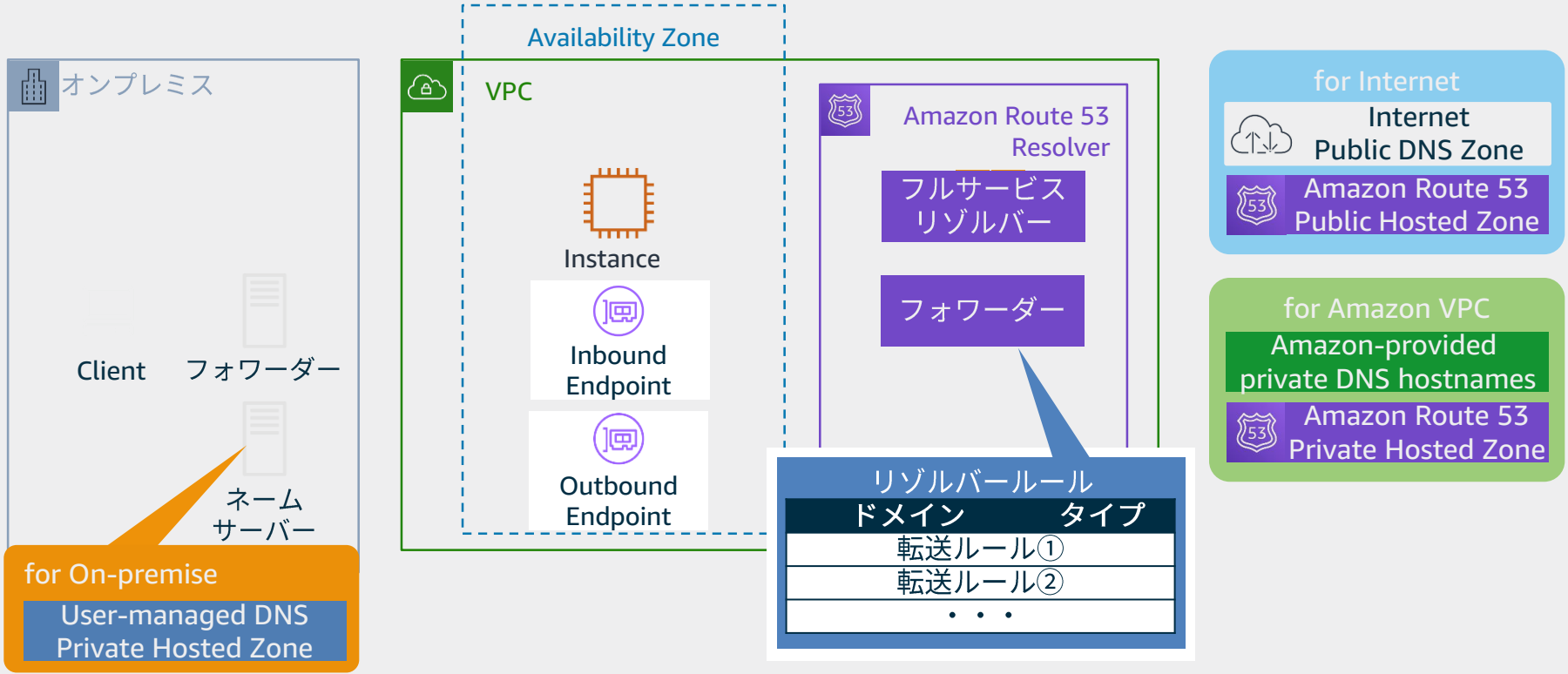
Amazon Route 53 Resolver for Hybrid Clouds以前

前頁に挙げたユースケースを実現するには以下が必要でした
①VPC上にフォワーダーを構築する
②DNSの参照先を構築したフォワーダーに変更する



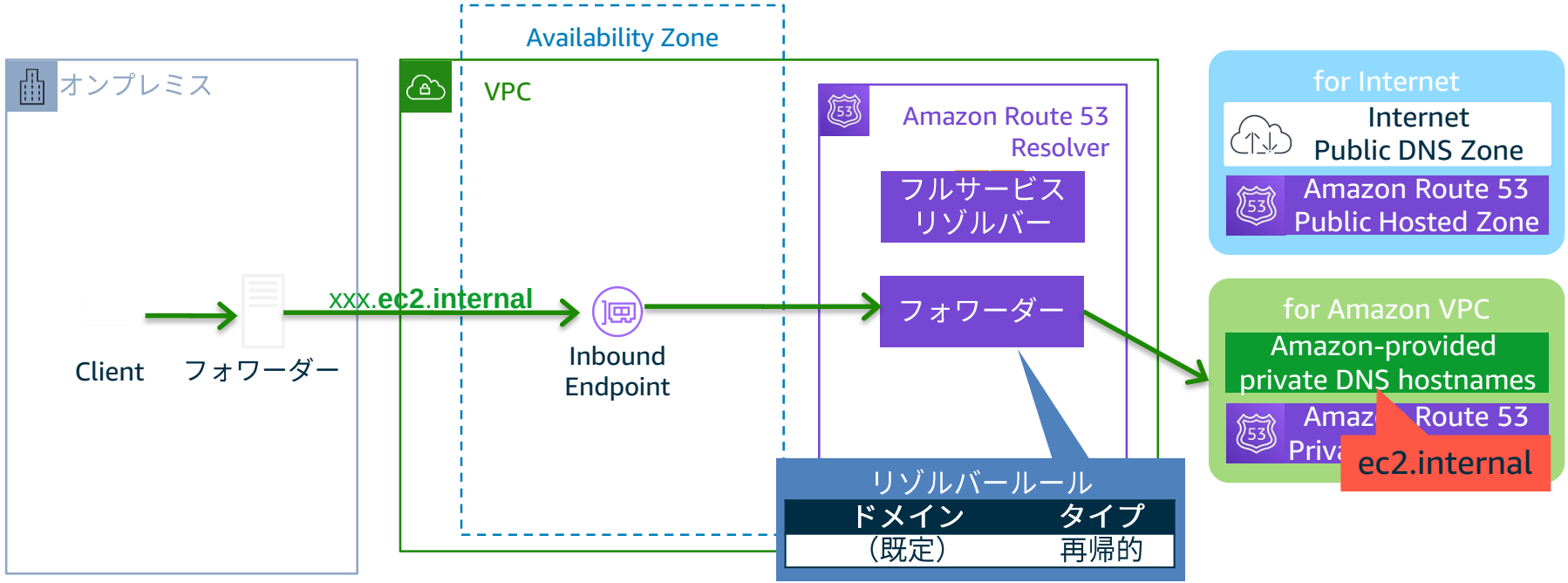
【参考】 https://aws.amazon.com/jp/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-using-aws-directory-service-and-amazon-route-53/

Route 53 Resolver for Hybrid Clouds Overview



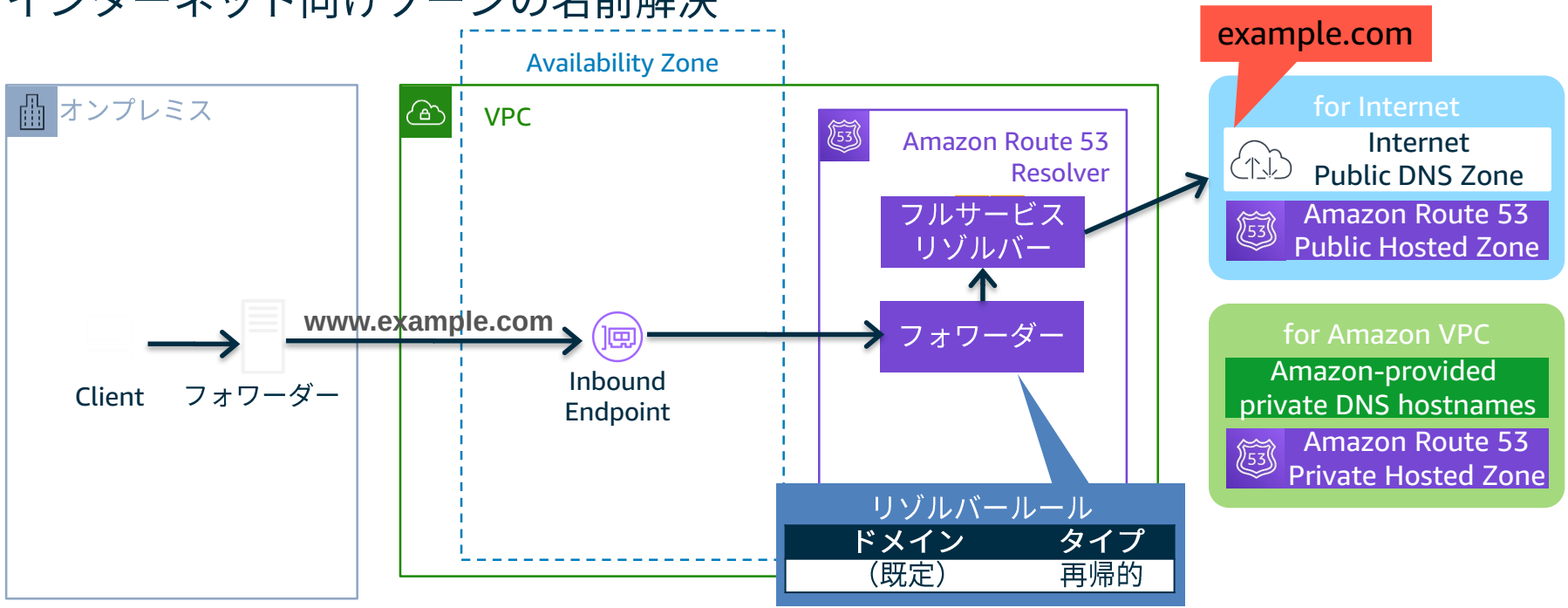
Route 53 Resolver for Hybrid Clouds ユースケース①

オンプレミスからVPC向けゾーンの名前解決



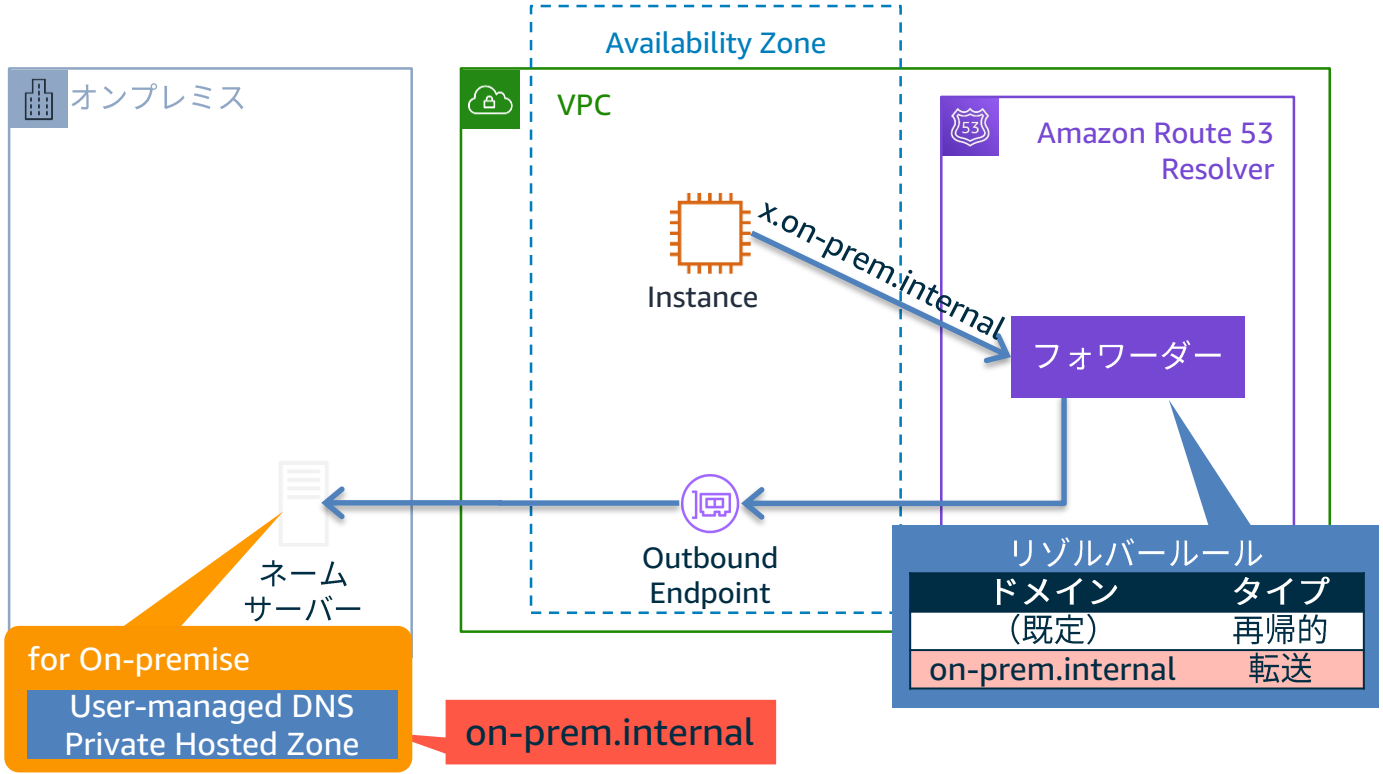
Route 53 Resolver for Hybrid Clouds ユースケース②

オンプレミス環境からAmazon Route 53 Resolverを用いて
インターネット向けゾーンの名前解決



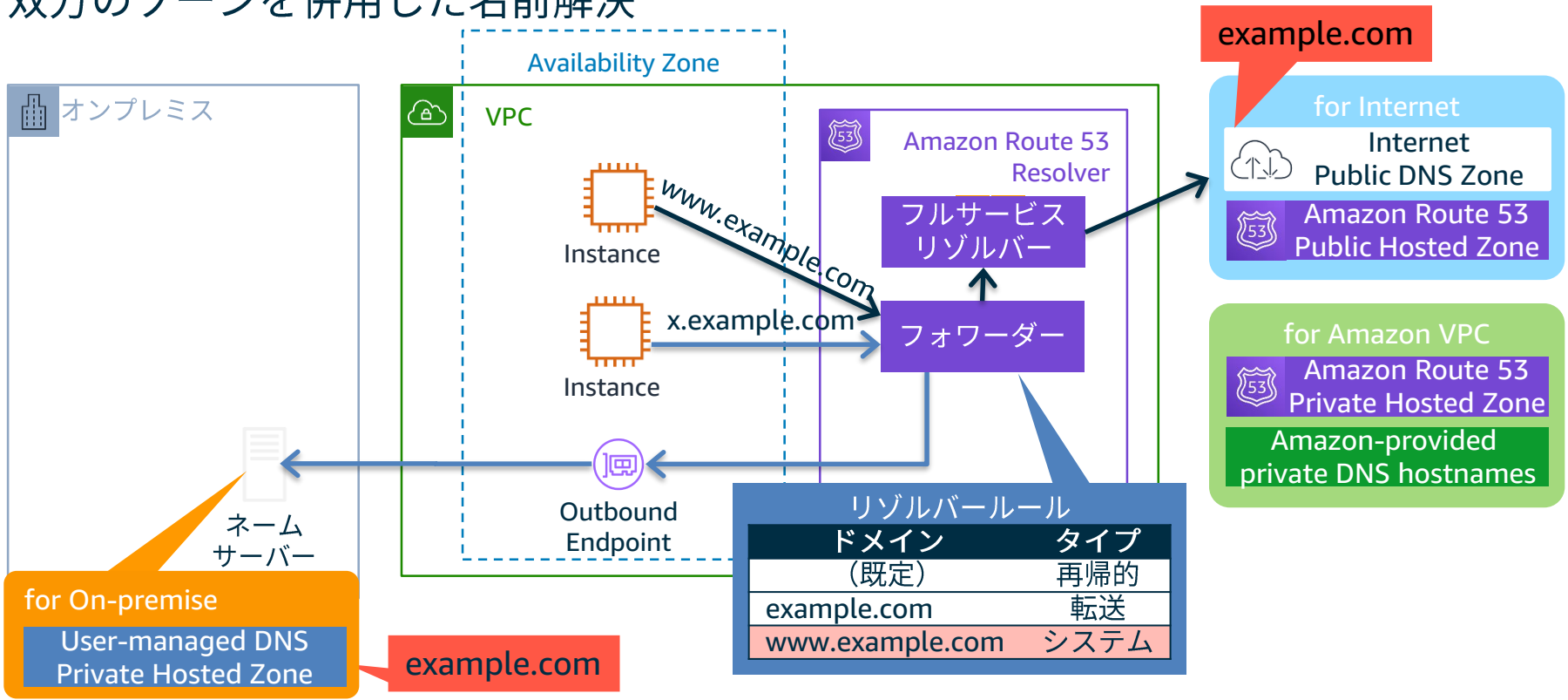
Route 53 Resolver for Hybrid Clouds ユースケース③

VPCからオンプレミス向けゾーンの名前解決



Route 53 Resolver for Hybrid Clouds ユースケース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ている場合に、
双方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

料金（2019/10/16 時点）

Route 53 Resolver

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

Route 53 Resolver for Hybrid Clouds

- エンドポイントの使用には、１時間につき0.125ドルのElastic Network Interfaces (ENIs)の料金が発生
- 条件付き転送規定（転送ルール）またはエンドポイントで処理されるDNSクエリは、最初の10億回までは百万回毎に0.40ドル、その後は百万回毎に0.20ドル

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)
- 「.2 Resolver」
  「Amazon Provided DNS」から改称

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

※

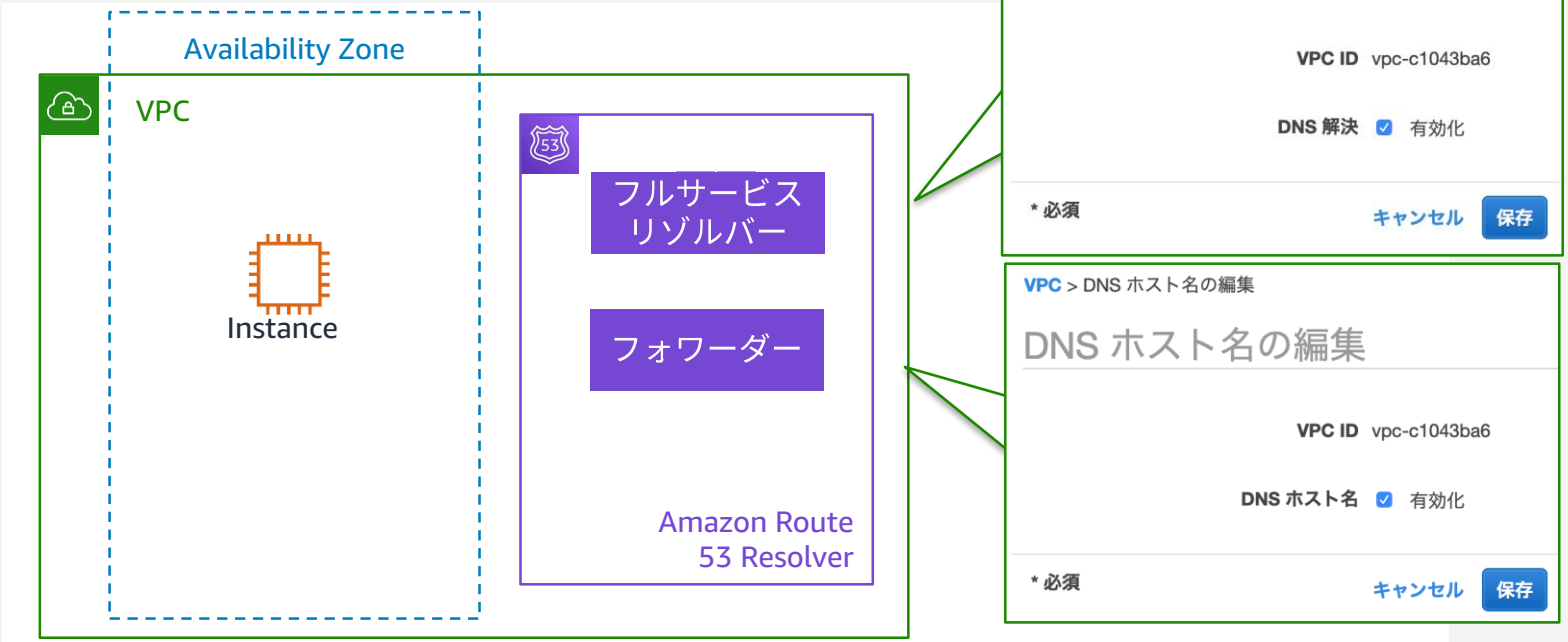
3. Amazon Route 53 Resolverの構成

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

Amazon Route 53 Resolver

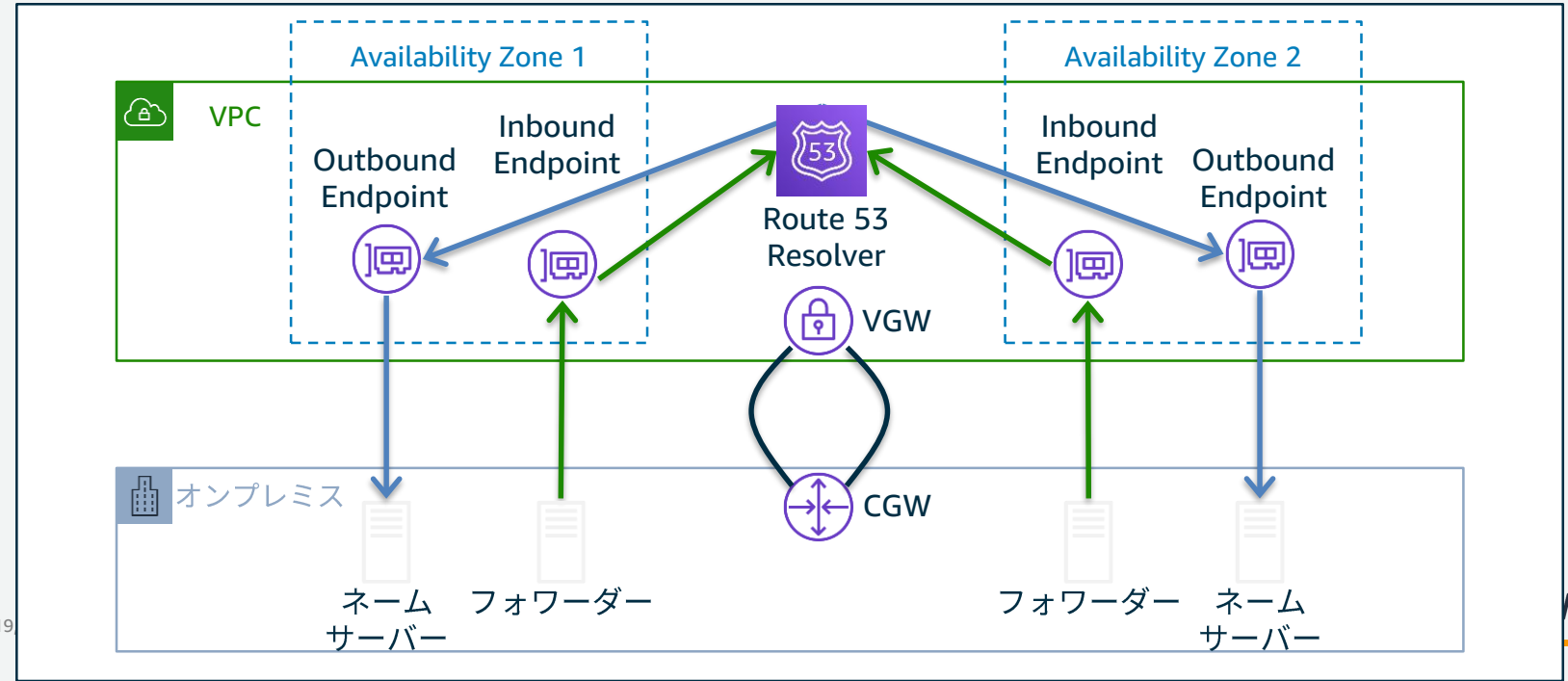
- VPC作成時にデフォルトで有効、必要な場合はVPC毎に有効/無効に設定可能
- IPアドレス設定はDHCPで自動的に配布される



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りがちであることに注意

- 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。

Route 53 Resolver for Hybrid Clouds
転送ルールの共有と共有ルールの使用

1 つの AWS アカウントで作成した転送ルールを他の AWS アカウントと共有できます。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。

次の点に注意してください。

- 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 > リゾルバー

Route 53 リゾルバーへようこそ

Route 53 リゾルバーは、リージョンのサービスで、VPC とネットワークの間の DNS クエリをルーティングさせます。

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

Route 53 リゾルバエンドポイントは、AWS 無料利用枠に含まれていません。詳細については、「Amazon Route 53 料金表」をご参照ください。

エンドポイントの設定

Route 53 Resolver for Hybrid Clouds
Step 2 Choose Endpoints

Route 53 > リゾルバー > エンドポイントの設定

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 Info

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。

基本的な設定

DNS クエリの方向 Info
(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

aws

Route 53 Resolver for Hybrid Clouds
Step 3 Configure Inbound Endpoint

Inbound EndpointのIPアドレスは、参照する側のサーバに設定するため、自分で指定したIPアドレスを使用すると管理しやすい

Route 53 Resolver for Hybrid Clouds
Step 4 Configure Outbound Endpoint

接続先でIPアドレス制限などを行う場合には、Outbound Endpointに自分で指定したIPアドレスを割り振ると管理しやすい

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

aws

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

aws

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

まとめ

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

本セミナーの概要

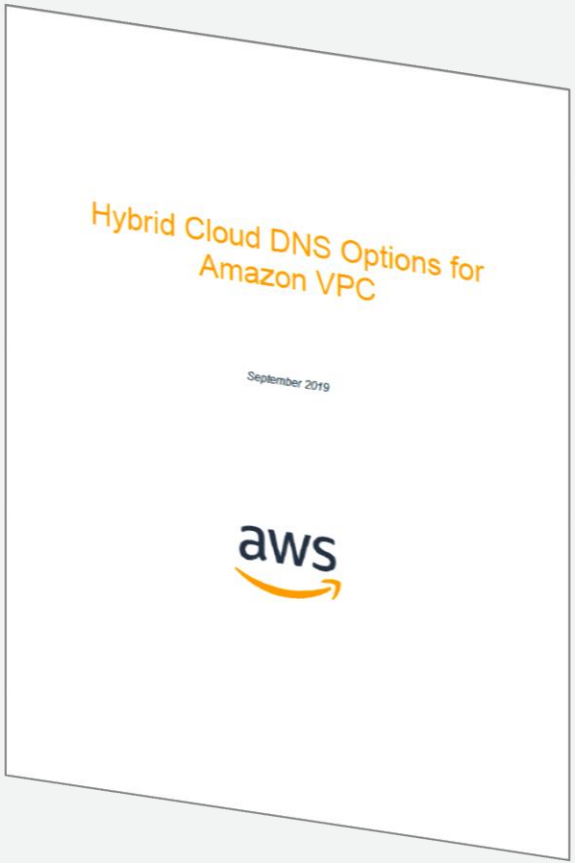
DNS(Domain Name System)の基本をおさらいした後、

Amazon Route 53 Resolverの活用方法を取り上げました。

1. DNSの基本
2. AWSが提供するDNSサービスと機能
3. Amazon Route 53 Resolverの構成

より進んだ設計のために

ホワイトペーパー
「Hybrid Cloud DNS Options for Amazon VPC」



最新の2019年9月改訂版では、
Route 53 Resolver for Hybrid Cloudsを用いた
構成がベストプラクティスに盛り込まれました。

【参考】Hybrid Cloud DNS Options for Amazon VPC
https://d1.awsstatic.com/whitepapers/hybrid-cloud-dns-options-for-vpc.pdf

aws

改めてのご案内：Amazon Route 53は全2回でお届けします

Amazon Route 53 Resolver 10/16 (水) 18:00-19:00

はじめにDNSの基本を解説し、Amazon Route 53 Resolverの機能である、Route 53 Resolver Endpoints、Conditional Forwarding Rulesを用いてハイブリッド環境の名前解決を最適化する手法を学びます。

Coming Soon !

Amazon Route 53 Hosted Zone 11/5 (火) 12:00-13:00

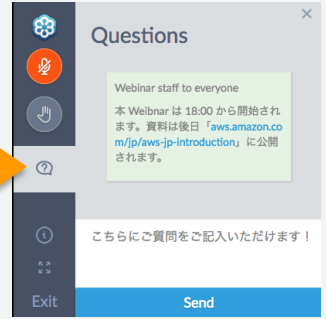
ネームサーバー機能を提供するAmazon Route 53のHosted Zoneについて解説します。インターネットに名前解決を提供するパブリックホストゾーン、VPC内に限定して名前解決を提供するプライベートホストゾーンを中心にAmazon Route 53の活用法を学びます。

aws

Q&A

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
  お答えできませんのでご了承下さい



回答はAWS Japan Blog
「https://aws.amazon.com/jp/blogs/news/」にて
後日掲載します。

ご質問のほか、こういった内容を追加してほしい、と言ったご意見も
お待ちしております。

AWS の日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に対策などを相談することも可能

- 申込みはイベント告知サイトから

  (https://aws.amazon.com/jp/about-aws/events/)

AWS イベント で[検索]

ご視聴ありがとうございました

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

【付録】名前空間（ゾーン）概要説明

 Internet Public DNS Zone	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。
 Amazon Route 53 Public Hosted Zone	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。
Amazon-provided private DNS hostnames	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。
 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。
User-managed DNS Private Hosted Zone	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。

aws