



Amazon Route 53

～導入編～

Katsuhisa Takahashi

Solutions Architect

2023/05

自己紹介

名前：高橋 克久

所属：

技術統括本部 エンタープライズ技術本部

東日本エリアの電力業界のお客様ご支援を担当



好きなAWSサービス：

AWS Transit Gateway, Amazon Route 53, Amazon SageMaker

本セミナーの対象者

これから AWS を用いたシステムのネットワーク設計を担当される方

Amazon Route 53 の全体像と必要な DNS の基礎を学習されたい方

本セミナーでお話ししないこと

- Amazon Route 53 各機能の詳細な設定方法
- 詳細については、AWS BlackBelt Online Seminar Amazon Route 53 Hosted Zone 編 と Resolver 編 をご視聴ください

アジェンダ

1. Amazon Route 53 概要
2. Amazon Route 53 インフラストラクチャ
3. Amazon Route 53 の機能
4. Amazon Route 53 機能の理解に必要な DNS の基礎知識
 - ドメイン名の基礎
 - ネームサーバーの基礎
 - 名前解決の基礎
5. まとめ



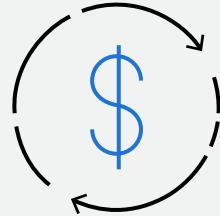
Amazon Route 53 概要

Amazon Route 53 の特徴

可用性が高く、コスト効率に優れた DNS Webサービス



高速な名前解決



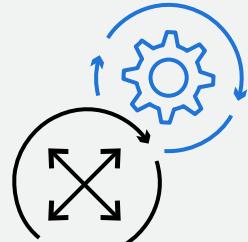
高いコスト効率



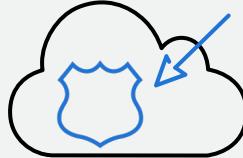
セキュア



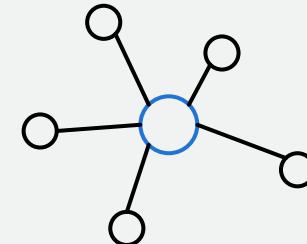
高可用性



100 % SLA



ドメイン名の購入と移管



AWS サービス連携

Amazon Route 53 の機能

AWS サービスとネイティブ連携する 3 つの機能を提供



ドメイン名の登録



権威 DNS サービス



DNS リゾルバー



Resolver



Resolver DNS Firewall

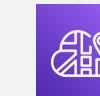
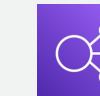
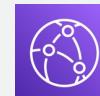
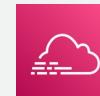
Disaster recovery



Application Recovery
Controller



AWS サービスとの統合

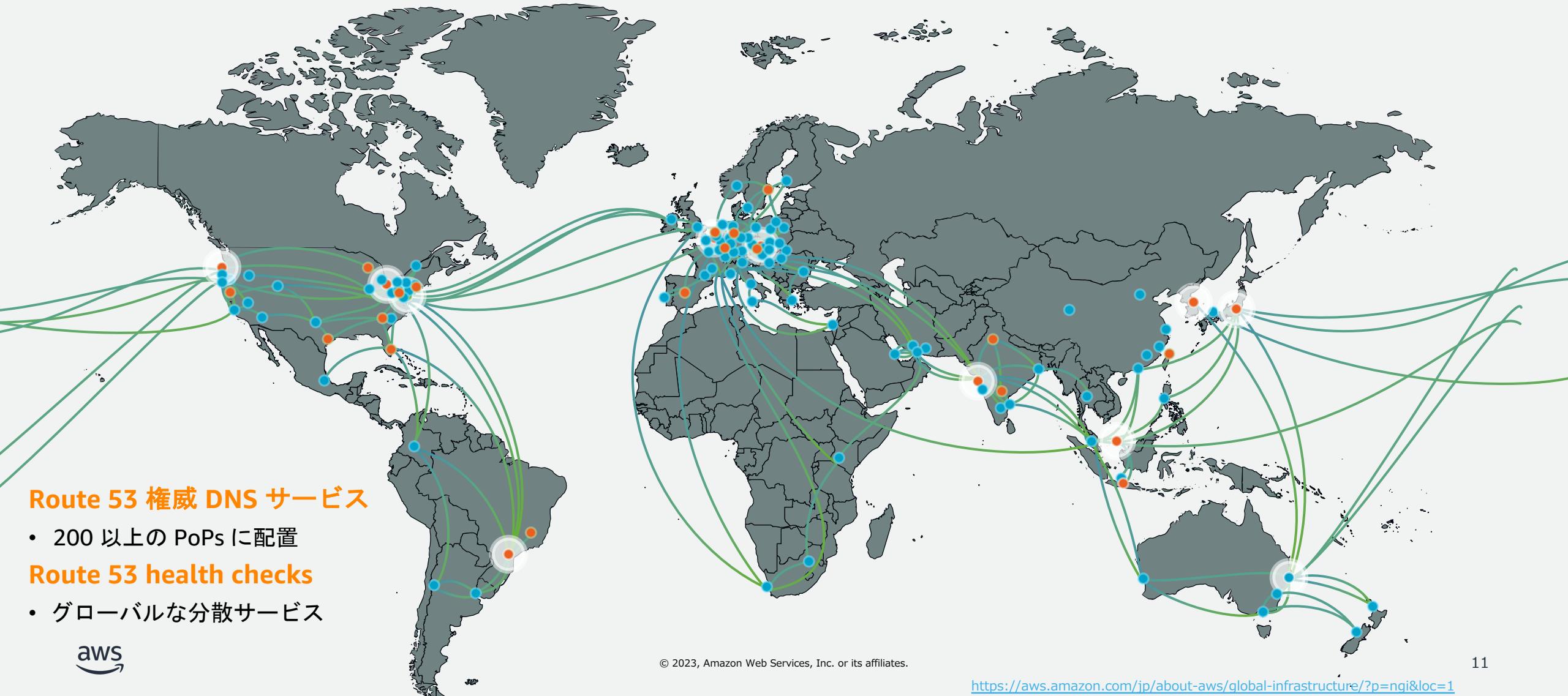


Amazon Route 53 インフラストラクチャ



AWS グローバルインフラストラクチャ

Amazon Route 53 は Edge Location から全世界へサービスを提供



コントロールプレーンとデータプレーン

*“Control plane” and “data plane” are terms of art from networking,
but we use them all over the place within AWS.*

[Amazon Route 53 concepts - Amazon Route 53](#)
[Static stability using Availability Zones \(amazon.com\)](#)



コントロールプレーンとデータプレーン

分散システムのトレードオフのため機能ごとに求められる性能要件に応じた分離設計を採用



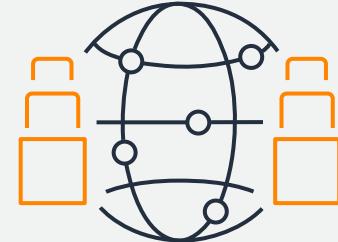
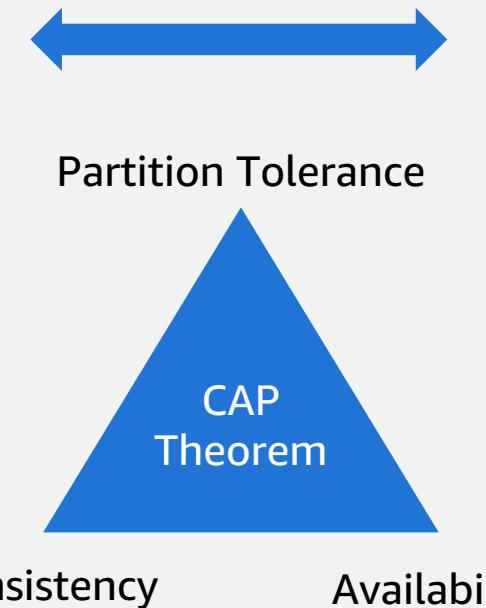
コントロールプレーン

データの一貫性を重視した設計

主に CRUD 操作を実装
AWS ではリソースの設定に利用

(e.g. DNS レコード変更,
ChangeResourceRecordSets)

Route 53 では us-east-1/us-west-2 に配置



データプレーン

データの可用性を重視した設計

設定ではなくサービスを
提供するコンポーネント

(e.g. DNS クエリ応答)

Route 53 ではグローバルに分散

Amazon Route 53 のコントロールプレーンとデータプレーンの機能

<https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/route-53-concepts.html>

	権威 DNS	ヘルスチェック	リゾルバー	ドメイン登録
コントロール プレーン	<u>機能:</u> Route 53 コンソール API <u>Location:</u> us-east-1	<u>機能:</u> Route 53 コンソール API (ヘルスチェックの CRUD 操作) <u>Location:</u> us-east-1	<u>機能:</u> Route 53 コンソール API (VPC 設定、リゾルバー ルール設定、クエリロギ ングポリシー設定、DNS Firewall ポリシー設定) <u>Location:</u> リージョンごと	<u>機能:</u> Route 53 コンソール API (ドメイン登録) <u>Location:</u> us-east-1
データ プレーン	<u>機能</u> 権威 DNS サービス <u>Location:</u> グローバルに分散	<u>機能:</u> ヘルスチェック Public/Private DNS サー ビスへの集約結果の送信 <u>Location:</u> グローバルに分散	<u>機能:</u> DNS フォワーディング DNS 再帰クエリ <u>Location:</u> リージョンごと	なし



SLA 100 %



AWS の他のサービスも
DNS に依存



複数のお客様のゾーンを
ホスティングすることによる
DDoS 対策の重要性



全てのお客様に低成本で
サービスを提供する必要性

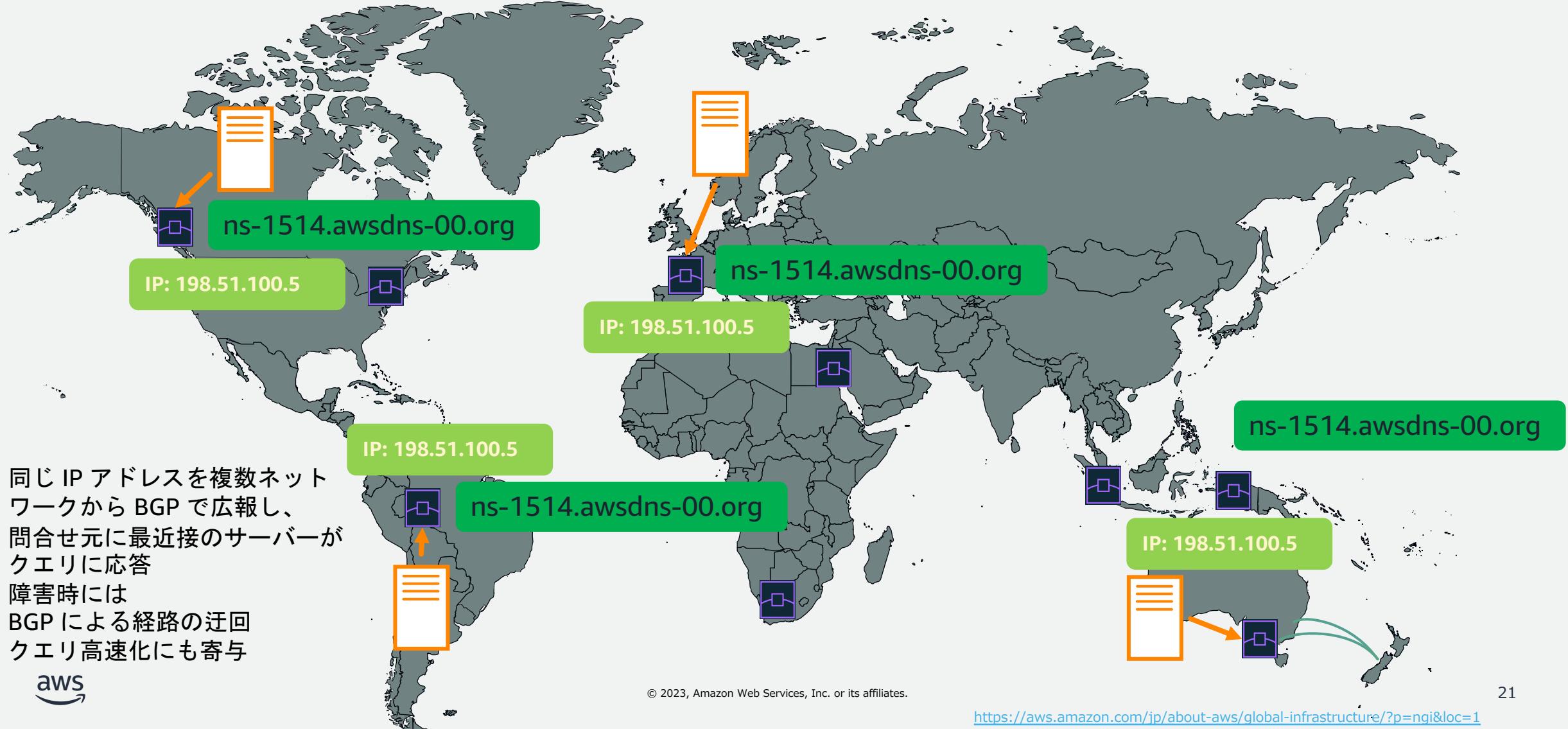
➤ Amazon Route 53 では 権威 DNS サービスのデータプレーンの可用性設計目標を 100 % に設定

https://aws.amazon.com/route53/sla/?nc1=h_ls

<https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/appendix-a-designed-for-availability-for-select-aws-services.html>

SLA 100 % のための設計 – IP Anycast

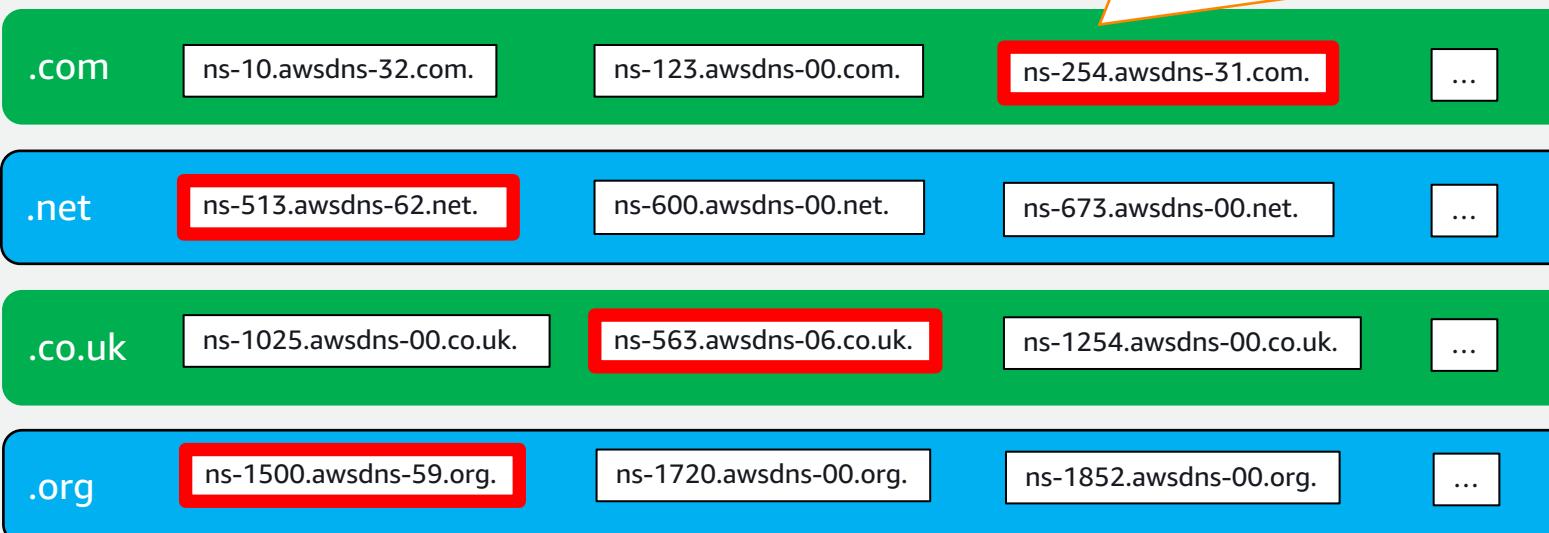
IP Anycast により最も近くのネームサーバーが DNS クエリに応答、障害時は別サーバーへ経路切り替え



SLA 100 % のための設計 – name server stripes

ゾーン間で重複しない4つのTLDを割り当てて障害の影響を分離

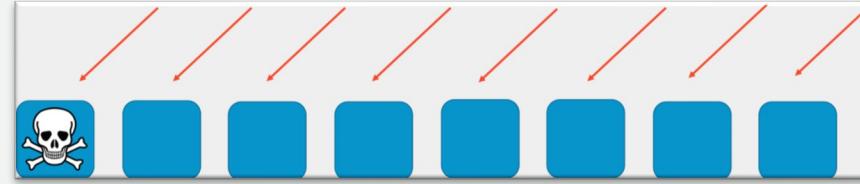
Stripe : 1つのTLDでホストされる全てのネームサーバーの集合
各 Stripe は数千のネームサーバーを持つ



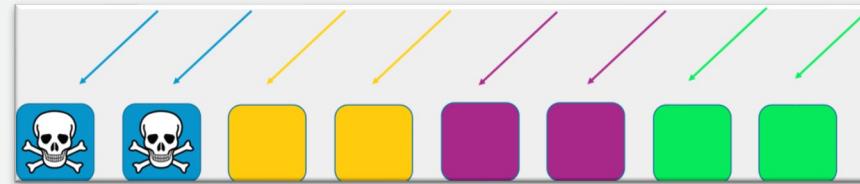
- 各 Stripe から 1 つずつネームサーバーが割り当てられる
- 割り当てられた 4 つのネームサーバーが他のゾーンに割り当てられた 4 つのネームサーバーと完全に一致することはない

SLA 100 % のための設計 – Shuffle Sharding

シャーディングによる機器障害影響の局所化とシャッフルによるテナント間での障害の拡大を防止



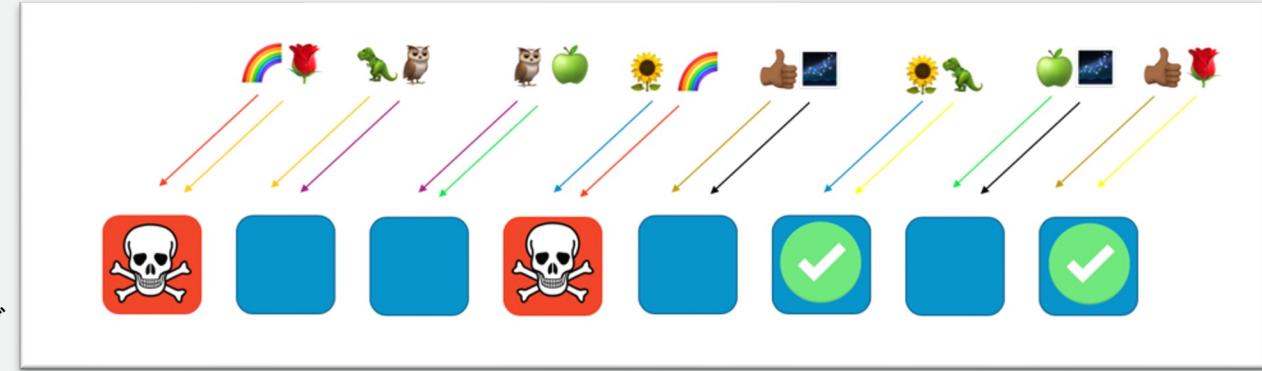
DNS クエリに対応するワーカーがクエリに均等に対応する場合、DDoS など大量リクエストの攻撃の影響は時間と共に影響が拡大してしまう



シャーディングにより、ドメインごとにリソースを分割する、など対策を講じることで、障害の影響範囲を分離することができる

しかし、同じシャードに属するクライアントには影響が伝播してしまう

シャッフル
シャーディング



障害影響の分離のために、シャードをランダムにワーカーへ割り当てることで、異なるシャードが共有するネームサーバーを 2 つ以内にとどめる

あるお客様ドメインが攻撃されると、4 つのネームサーバーのトラフィックは急増するものの、ネームサーバーを共有する別のお客様ドメインは別のネームサーバーも割り当てられているため、影響は及ばない

<https://aws.amazon.com/jp/builders-library/workload-isolation-using-shuffle-sharding/>

Amazon Route 53 Infrastructure まとめ

- Amazon Route 53 は AWS の 200 以上の PoP にホストされている
- DNS は他の AWS サービスが依存するサービスであるため SLA を 100 % 設定し、可用性設計目標を 100 % と定めている（権威 DNS サーバーのデータプレーン）
- 可用性設計目標 100 % とする関連技術を紹介
 - IP Anycast
 - Name server stripes
 - Shuffle Sharding

Amazon Route 53 の機能

Amazon Route 53 ドメイン登録

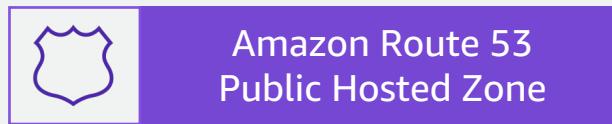
- Amazon Route 53 はリセラーとしてドメイン登録が可能
 - レジストラは Gandi SAS、Mesh Digital Limited、Amazon Registrar, Inc
 - https://aws.amazon.com/route53/domain-registration-agreement/?nc1=h_ls
- 他のレジストラから Amazon Route 53 下での管理に移管、その逆も可能
- 登録ドメインのプライバシー保護が利用可能



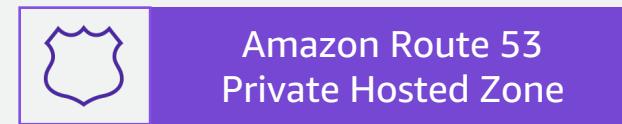
- ドメイン登録料金は[ドキュメント](#)をご参照ください

Amazon Route 53 Hosted Zone

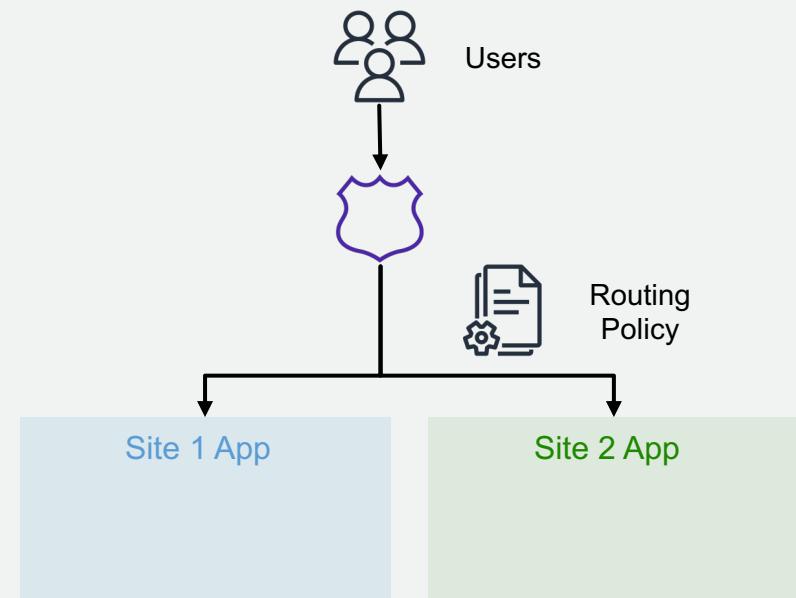
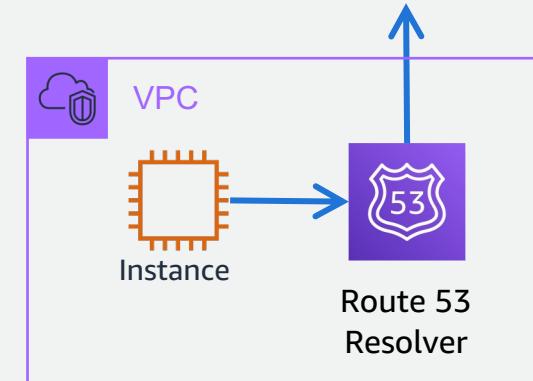
- ・ ネームサーバーと Global Server Load Balancing (GSLB) を提供するマネージドサービス
- ・ AWS による拡張である Alias レコードを利用した AWS リソースへのルーティングが可能
- ・ ルーティングポリシーによる複数種類の広域負荷分散や Blue-Green デプロイが可能
- ・ Public/Private Hosted Zone を併用することでスプリットビュー DNS が構成可能



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

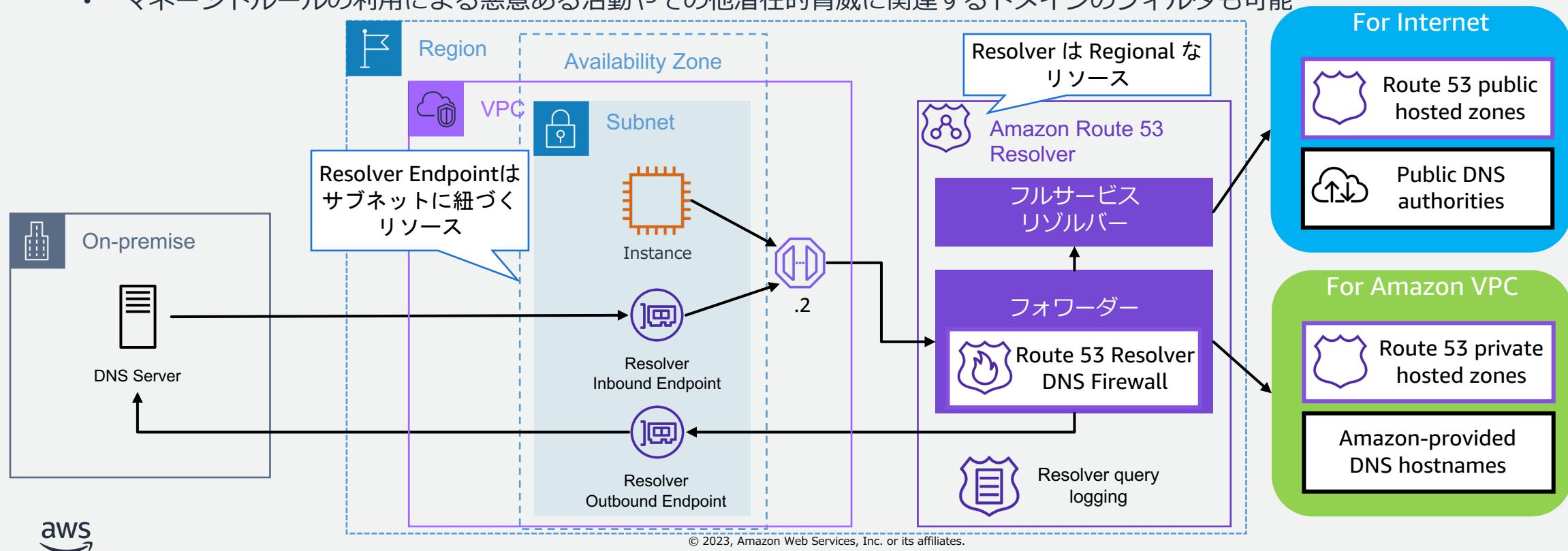


1つもしくは複数の VPC プライベートネットワーク内の
DNS ドメインのレコードを管理するコンテナ



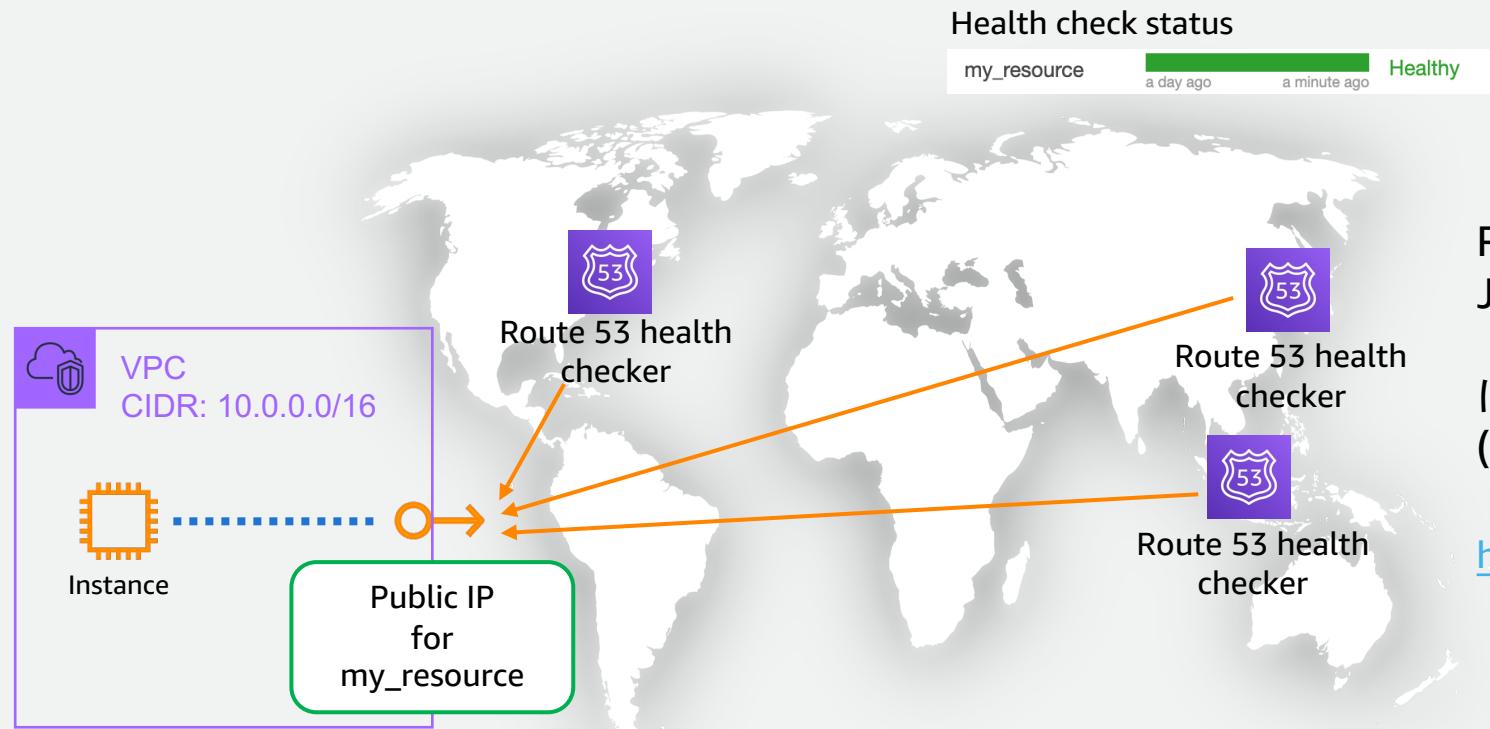
Amazon Route 53 Resolver (別名: AmazonProvidedDNS, VPC+2 Resolver)

- VPC 内リソースおよびオンプレミスリソースからの再帰的問い合わせを解決する(フルサービスリゾルバー)サービス
- VPC内リソースからの問い合わせを解決する VPC + 2 Resolver とオンプレミス環境との名前解決の連携を行う Resover Endpoint からなる
- VPC からのアウトバウンド DNS クエリのフィルタリングを行う Resolver DNS Firewall
 - マネジドルールの利用による悪意ある活動やその他潜在的脅威に関するドメインのフィルタも可能



Amazon Route 53 Health check

- Edge location 上のサーバーからヘルスチェックを実施できる
- エンドポイント、計算結果、Amazon CloudWatch アラームなど複数種類のヘルスチェックが可能
- フェールセーフ設計によりヘルスチェックの不備時にもシステム稼働を持続させる仕組み



Route 53 ヘルスチェッカーは以下リンクの JSON 中で
“service”: “ROUTE53_HEALTHCHECKS”
に記載の IP アドレスから発信される
(適宜ファイアウォールにルール設定)

<https://ip-ranges.amazonaws.com/ip-ranges.json>

Amazon Route 53 – AWS Service 統合の例



Amazon Route 53 機能まとめ

- Amazon Route 53 を利用したドメイン登録が可能
- Amazon Route 53 Hosted Zone はネームサーバー機能と DNS ルーティングを担う
- Amazon Route 53 Resolver はフルサービスリゾルバー機能を提供する
- Amazon Route 53 health check ではお客様のサービスを AWS のグローバルなネットワークから監視可能
- Amazon Route 53 では AWS サービスと連携したさまざまな機能をご提供

Amazon Route 53 機能の理解に必要な DNS 基礎知識



ドメイン名の基礎

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.

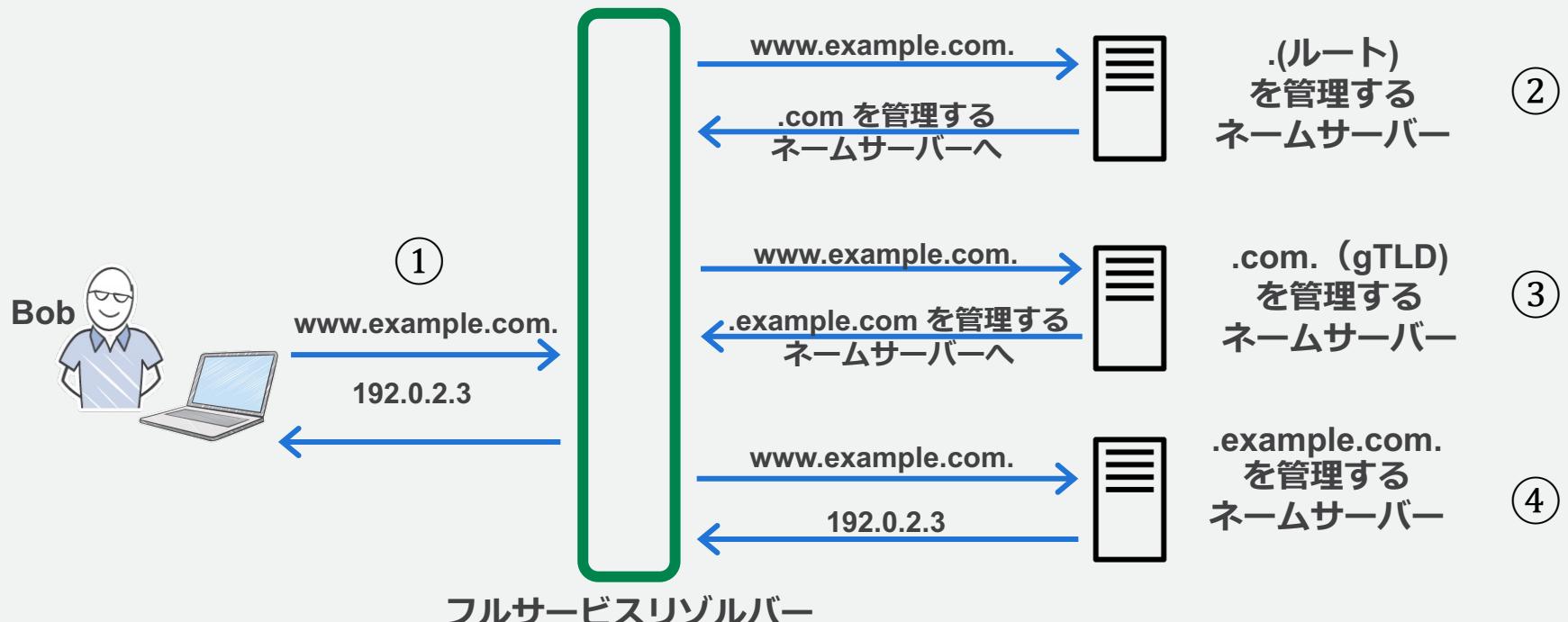
※ルートは「.」で表されるため、狭義の意味での FQDN を表記する際には、末尾の「.」まで含めて表記する

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 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



ドメイン名の登録

- ・インターネットで任意のドメイン名を利用するには登録が必要
- ・ドメイン名には種類があり、管理主体や属性によって、誰でも登録できるものや、特定の条件が存在するものがある

分野別トップレベルドメイン (gTLD: generic TLD)

たとえば

.com	登録されていないものは誰でも登録できる
.net	登録されていないものは誰でも登録できる
.org	登録されていないものは誰でも登録できる
.gov	米国政府機関のみ登録できる

国コードトップレベルドメイン (ccTLD: country code TLD)

たとえば

.jp	登録されていないものは誰でも登録できる
.co.jp	日本国内で登記を行っている会社のみ登録できる

ドメイン名登録の全体像

レジストラント
登録者

レジストラ
登録取次事業者

レジストリ
登録管理機関

ドメイン名を登録し、使用する
ユーザー

レジストリと契約し、ドメイン
名登録の窓口となる事業者

TLD を管理する主体、
TLD のネームサーバーと 登録情
報のデータベースである
WHOIS を提供



レジストラントは
リセラーを介してレジストラと
やり取りする場合もある

操作

コントロール
パネル

レジストラ
管理システム

連携

WHOIS

WHOIS
データベース

同期



TLD
ネームサーバー

WHOIS データベース

- レジストリがインターネットに提供するドメイン名の登録情報を参照可能なデータベース
 - 登録者情報
 - ネームサーバー情報
 - ドメインの状態など
- プライバシー保護機能により、WHOIS を介してインターネットにユーザー情報を公開せずにドメイン名の登録ができるサービスを提供するレジストラやリセラーもある

ICANN LOOKUP

Registration data lookup tool

Enter a domain name or an Internet number resource (IP Network or ASN) [Frequently Asked Questions \(FAQ\)](#)

Domain Information

Name: EXAMPLE.COM

Registry Domain ID: 2336799_DOMAIN_COM-VRSN

Domain Status:

[clientDeleteProhibited](#)
[clientTransferProhibited](#)
[clientUpdateProhibited](#)

Nameservers:

A.IANA-SERVERS.NET
B.IANA-SERVERS.NET

Dates

Registry Expiration: 2023-08-13 04:00:00 UTC

Updated: 2022-08-14 07:01:31 UTC

Created: 1995-08-14 04:00:00 UTC

<https://lookup.icann.org/en/lookup>

ドメイン名管理者が認識しておきたいトラブル事象

- ドメイン名ハイジャック
 - 登録情報の書き換え、ネームサーバーの侵害などによる乗っ取り
- スラミング
 - ドメイン名移転スキームの悪用による所有権乗っ取り
- ドロップキャッチング
 - 更新漏れ、あるいは廃止したドメインを第三者が取得し利用

ドメイン名のトラブルを避けるためにできること

- レジストラ/レジストリからの連絡を見逃さない
 - 連絡窓口情報 (Point of Contact) の適正化
 - 対応体制、手順の整備
- いわゆるレジストリロック/レジストラロックの活用
 - 登録情報変更やドメイン名の移転、廃止を制限する機能
 - 提供主体によって機能提供の有無や、その内容が異なる
- 多要素認証など、レジストラが提供するコントロールパネルの認証強化
- ドメイン名を手放す際には、第三者の手に渡った際の影響を考慮する

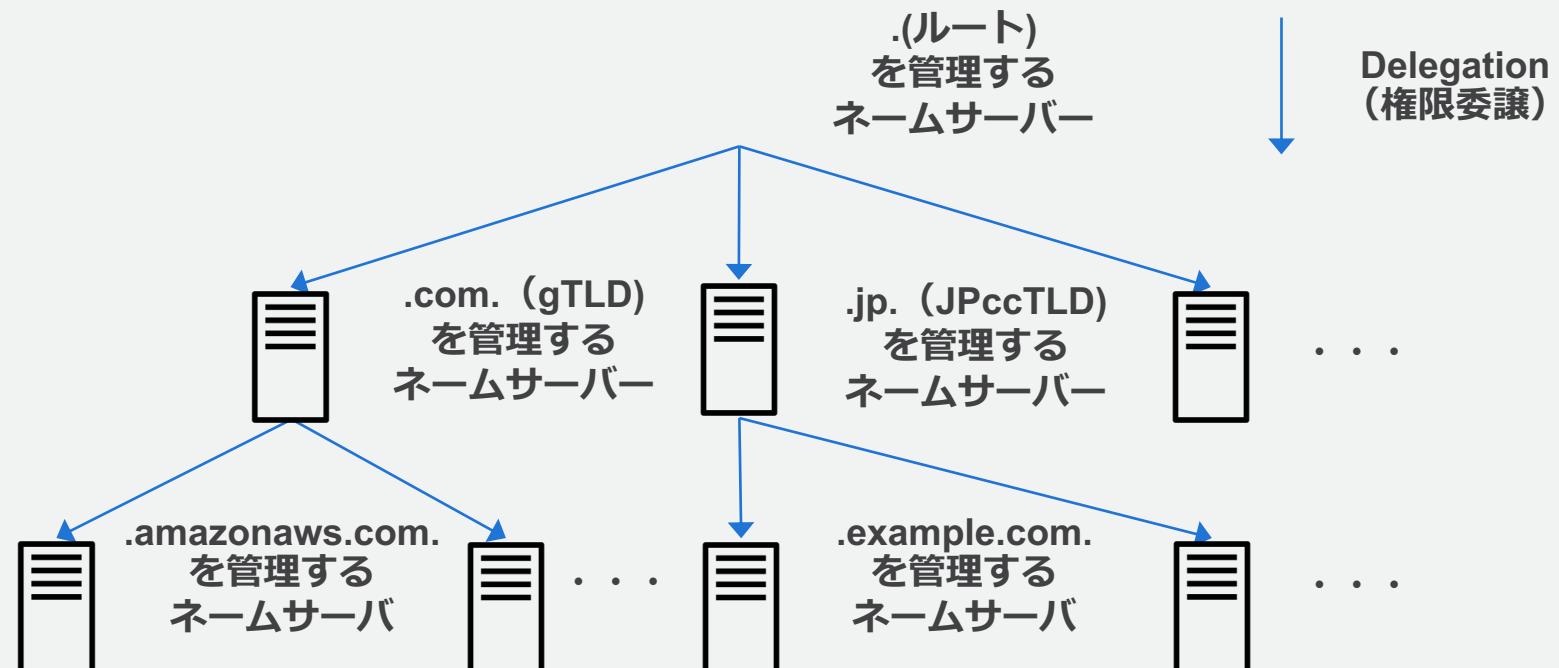
ドメイン名の基礎 まとめ

- ・ インターネットで任意のドメイン名を利用するには登録が必要
- ・ ドメイン名登録に関わる「レジストリ」「レジストラ」「レジストラント」
- ・ 登録情報を公開する WHOIS データベース
- ・ 登録可能なドメインは用途やレジストラによって異なる、全てのドメインを誰もが取得可能なわけではない
- ・ ドメイン名にまつわるトラブルと、避けるための取り組み

ネームサーバーの基礎

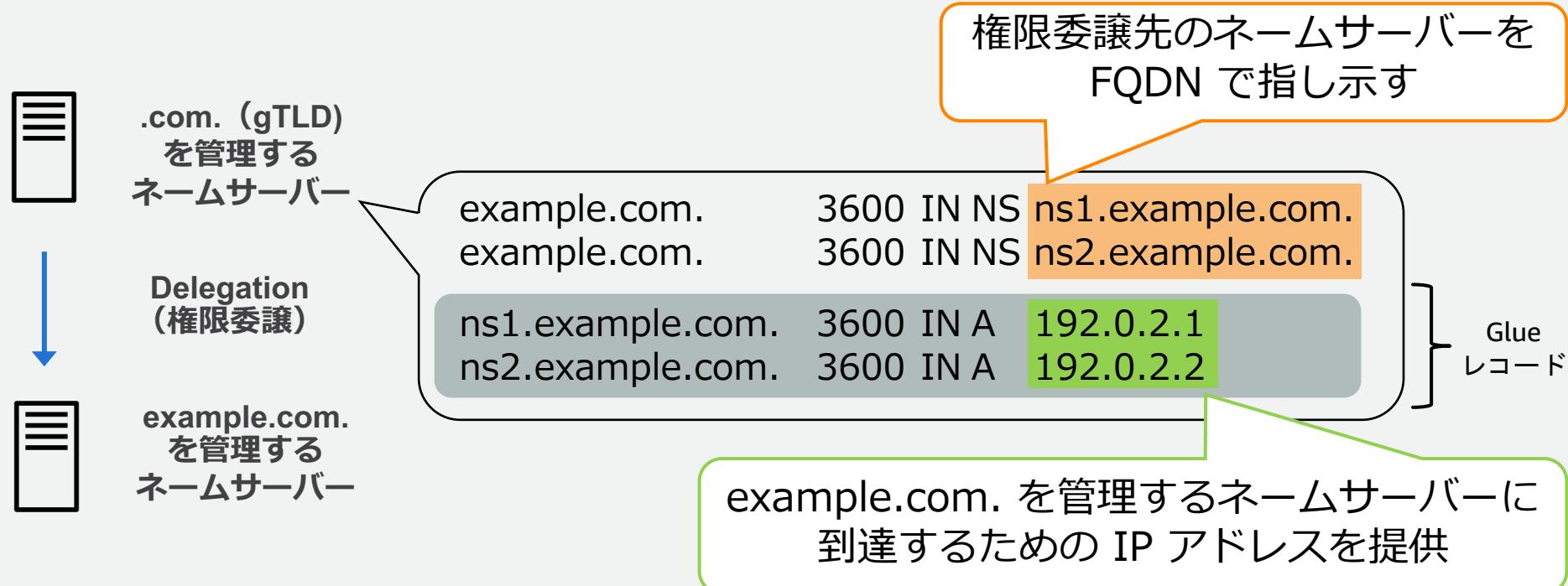
ネームサーバー(権威 DNS サーバー/Authoritative Server)

- .(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サーバー
- 権限委譲元を「親ゾーン」、権限委譲先を「子ゾーン」と呼ぶ



権限移譲 (Delegation)

- 親ゾーンから子ゾーンのネームサーバーを FQDN で指示することで権限を委譲
- 子ゾーンのネームサーバーの FQDN が、子ゾーンで管理されている場合、親ゾーンの返答にその IP アドレスも含めて指示する (Glue レコード)
- DNS クエリのループを回避



リソースレコードと RRSet

- RR (リソースレコード) は 5 つのフィールドを持ち、NAME、CLASS、TYPE の 3 つ組み合わせが問い合わせのキーとなる
- 同じ NAME、CLASS、TYPE を持ち RDATA が異なる RR の集合を RRSet と呼ぶ
- ネームサーバーは問い合わせに対して RRSet 単位で応答する

NAME	TTL	CLASS	TYPE	RDATA	
www.example.com.	3600	IN	A	192.0.2.3	RRSet
service.example.com.	3600	IN	A	192.0.2.11	RRSet
service.example.com.	3600	IN	A	192.0.2.12	RRSet
example.com.	3600	IN	MX	10 mx1.example.com.	RRSet
example.com.	3600	IN	MX	20 mx2.example.com.	RRSet

※本資料ではRRをゾーンファイル形式（RFC1034, RFC1035）に倣って記載

ネットワーク・プロトコルを指定する CLASS

- ・ インターネット・プロトコル (IP)以外のネットワーク・プロトコルでの利用を想定し、DNS の仕様上定義されているもの
- ・ 今日のインターネットにおいて、IN 以外が使われることは通常ない

No.	CLASS	Description
1	IN	for the Internet
2	CS	for the CSNET
3	CH	for the CHAOS
4	HS	for Hesiod [Dyer 87]

<https://en.wikipedia.org/wiki/CSNET>

<https://en.wikipedia.org/wiki/Chaosnet>

[https://en.wikipedia.org/wiki/Hesiod_\(name_service\)](https://en.wikipedia.org/wiki/Hesiod_(name_service))

用途に応じたリソースレコードタイプ

代表的なリソースレコードタイプ

RR TYPE	概要
SOA	DNS 構成用【後述】
NS	DNS 構成用【後述】
A	IPv4 アドレスを応答【後述】
AAAA	IPv6 アドレスを応答【後述】
CNAME	Canonical NAME（正式名）を応答【後述】
PTR	IP アドレスから FQDN の逆引きを応答【後述】
MX	当該ドメインのメールサーバーの FQDN を応答
TXT	任意の文字列を応答、多用途に利用される
SRV	任意のサービスのサーバーの FQDN を応答

ゾーンの起点と管理情報を示す SOA レコード

- ・ ゾーンの管理主体であること、権威であることを宣言 (Start Of Authority)
- ・ ゾーンには Zone Apex (サブドメインを含まないドメイン名) の名前の SOA レコードが必ず必要
- ・ ゾーンの管理に関する情報 (管理者メールアドレス、シリアル番号など) や、ゾーンが応答する RRSet の動作に関する設定が含まれる

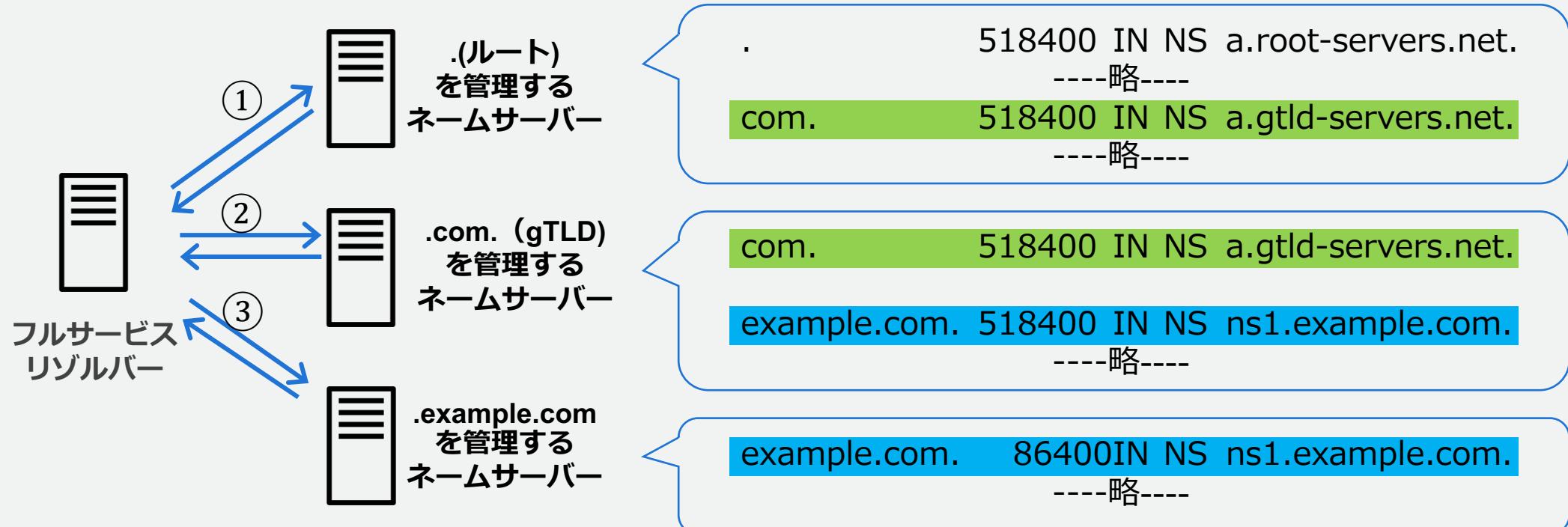
example.com. ゾーン

example.com.	3600	IN	SOA	ns.icann.org.	noc.dns.icann.org.
				2019101513	7200 3600 1209600 3600

スペースで区切られたパラメータの
ひとつひとつが意味を持つ

ネームサーバーを指示する NS レコード

- ゾーンを管理するネームサーバーの FQDN を指示する
- ゾーン自身と、その親ゾーンの両方に定義
- 親ゾーンから取得した値は、子ゾーンの値で上書きされる



ホストアドレスを示す A/AAAA レコード

- FQDN に対応する IP アドレスを応答する
 - IPv4 アドレスを応答する A レコード
 - IPv6 アドレスを応答する AAAA レコード

www.example.com.	3600	IN	A	192.0.2.3
www.example.com.	3600	IN	AAAA	2001:0DB8::1

名前解決を置き換える CNAME レコード

- CNAME が定義されている場合、名前解決を CNAME が指定する名前に置き換えて継続することを要求する
- ホスト名に別名を付ける手段として使われることが多い
- どのようなレコードタイプの問い合わせに対しても、CNAME を応答する

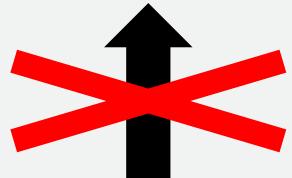
info.example.com.	3600	IN	CNAME	www.example.com.
www.example.com.	3600	IN	A	192.0.2.3

CNAME レコードの制約と Zone Apex

- ある名前で CNAME レコードタイプを定義すると、同一の名前で他のリソースレコードを定義できない
- ゾーンには Zone Apex (サブドメインを含まないドメイン名) の SOA/NS レコードタイプが必要なため、Zone Apex には CNAME を定義できない

example.com ゾーン				
example.com.	3600	IN	SOA	--省略--
example.com.	3600	IN	NS	ns.example.com.
ns.example.com.	3600	IN	NS	192.0.2.1
www.example.com	3600	IN	A	192.0.2.3

example.com. の SOA と NS が存在するため、example.com. に CNAME を定義し、Zone Apex でサービスをホストできない



追加

【補足】

Amazon Route 53 ではエイリアスレコード機能により、制約を回避し Zone Apex でサービスをホストできる

example.com.	3600	IN	CNAME	www.example.com.
--------------	------	----	-------	------------------

IP アドレスから FQDN を逆引きする PTR レコード

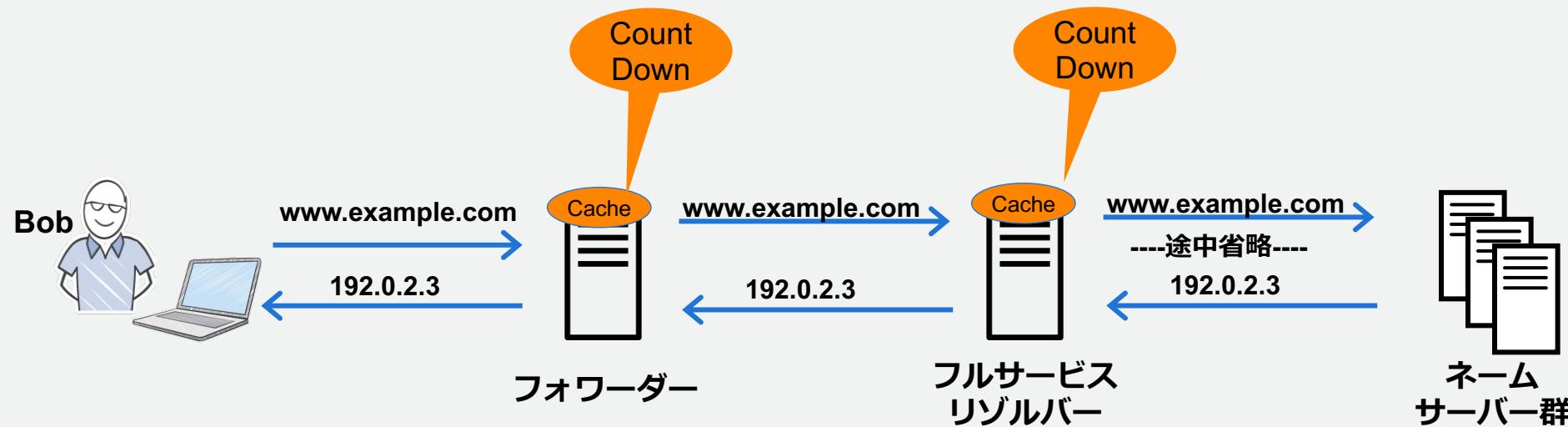
- IP アドレスをオクテット (8bit) 単位に区切り、「.」で区切って逆に並べ、`in-addr.arpa` を付与した名前をキーに問い合わせを行う

例)

- いくつかのサービスでは、動作に逆引き名の登録を必要とする

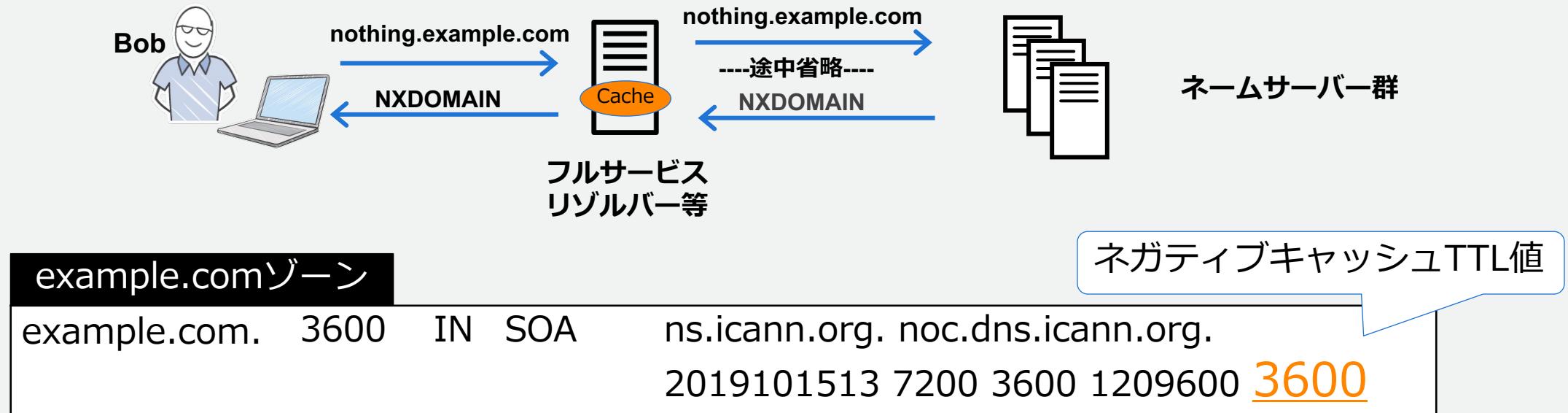
キャッシュ時間を定める TTL

- フルサービスリゾルバーや、フォワーダーなどで保持されるキャッシュの時間を定めるパラメータ
- TTL 値はキャッシュに残す義務を示すのではなく、残せる限界時間を指定
- キャッシュは保持する主体でカウントダウンをしており、キャッシュを用いて応答する際にはそのタイミングの値を利用する



NXDOMAIN とネガティブキャッシュ

- 存在しない RRSet を問い合わせると不存在応答（NXDOMAIN）を応答
- 不存在応答（NXDOMAIN）のキャッシュはネガティブキャッシュ※と呼ばれ、SOA レコードのネガティブキャッシュ TTL 値の期間キャッシュされる



※ネガティブキャッシュの対象は不存在応答（NXDOMAIN）のみ、それ以外の応答（SERVFAILなど）は対象外のためキャッシュされず都度問い合わせが行われる

名前解決の基礎

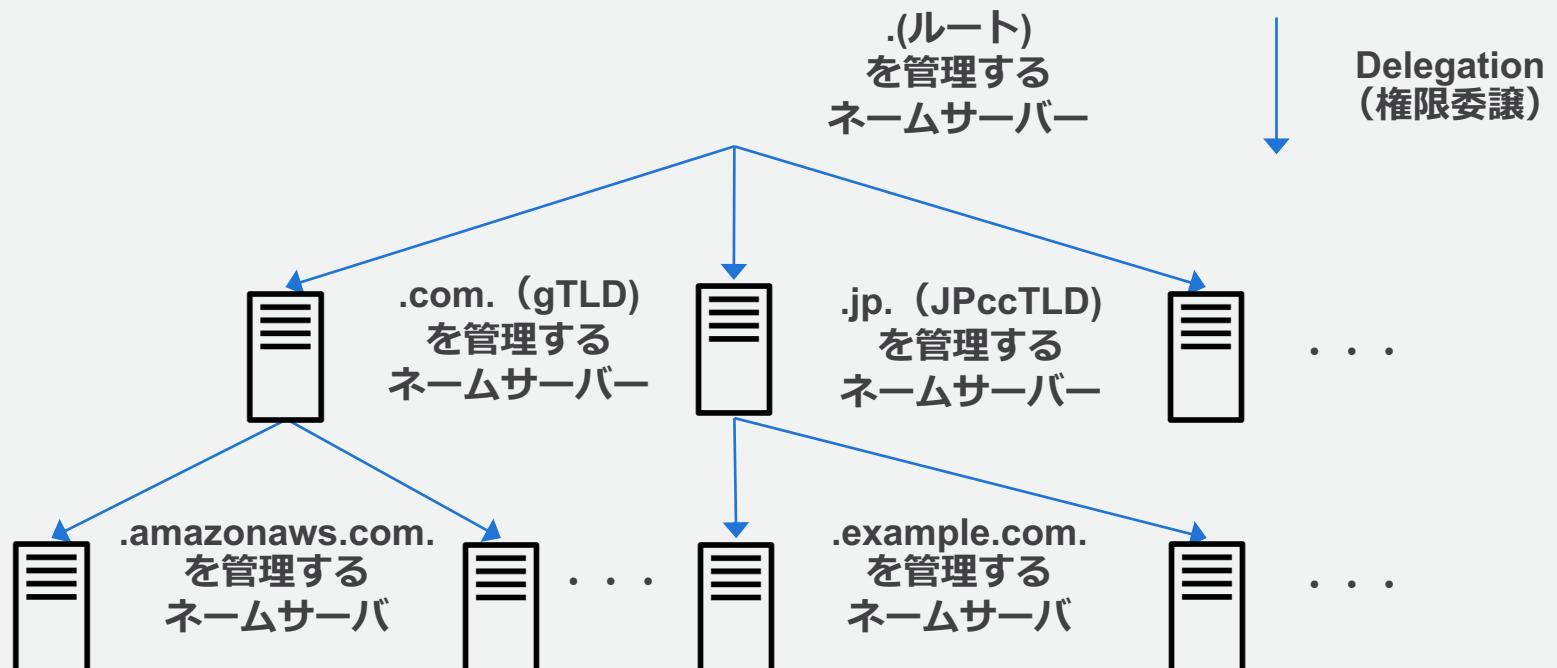
DNS サーバー

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 (キャッシュ DNS サーバー)
- ③ スタブリゾルバー / Stub Resolver
- ④ フォワーダー / Forwarder

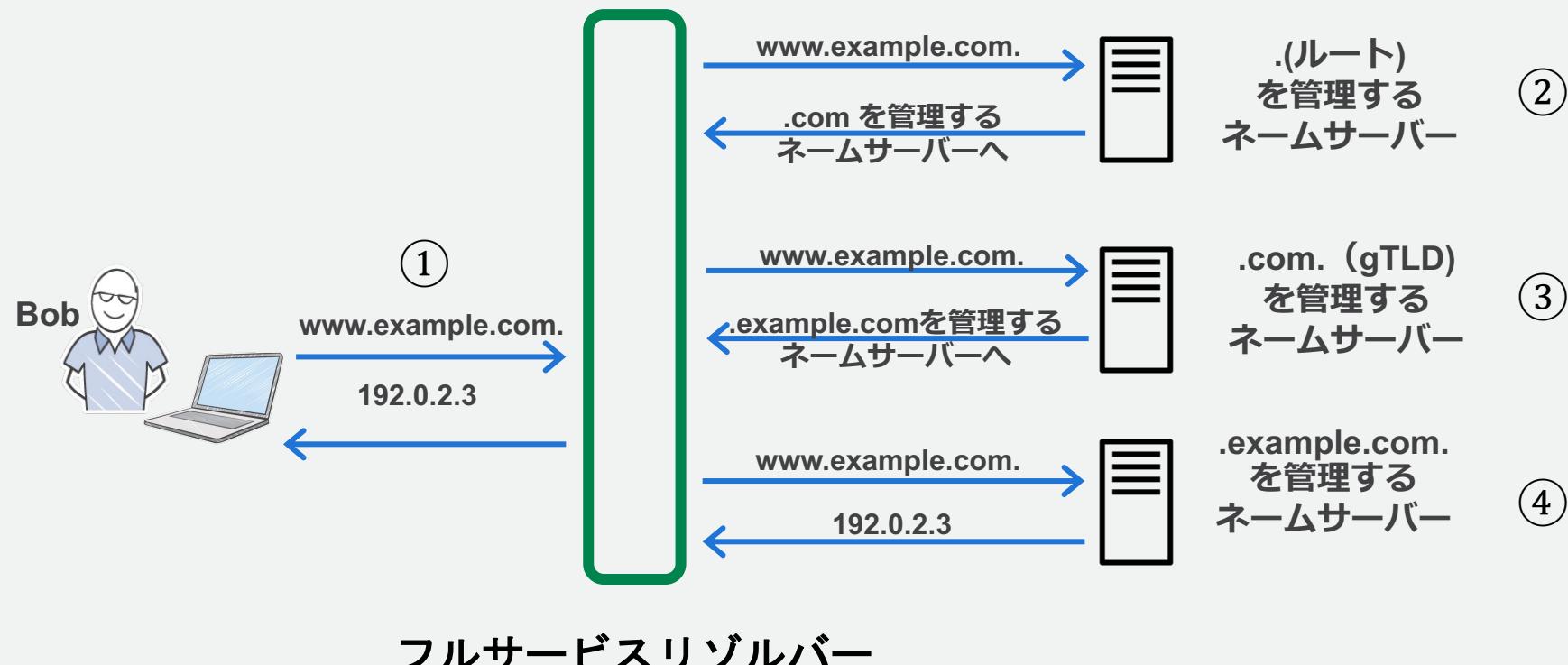
(再掲)ネームサーバー(権威 DNS サーバー/Authoritative Server)

- .(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サーバー
- 権限委譲元を「親ゾーン」、権限委譲先を「子ゾーン」と呼ぶ



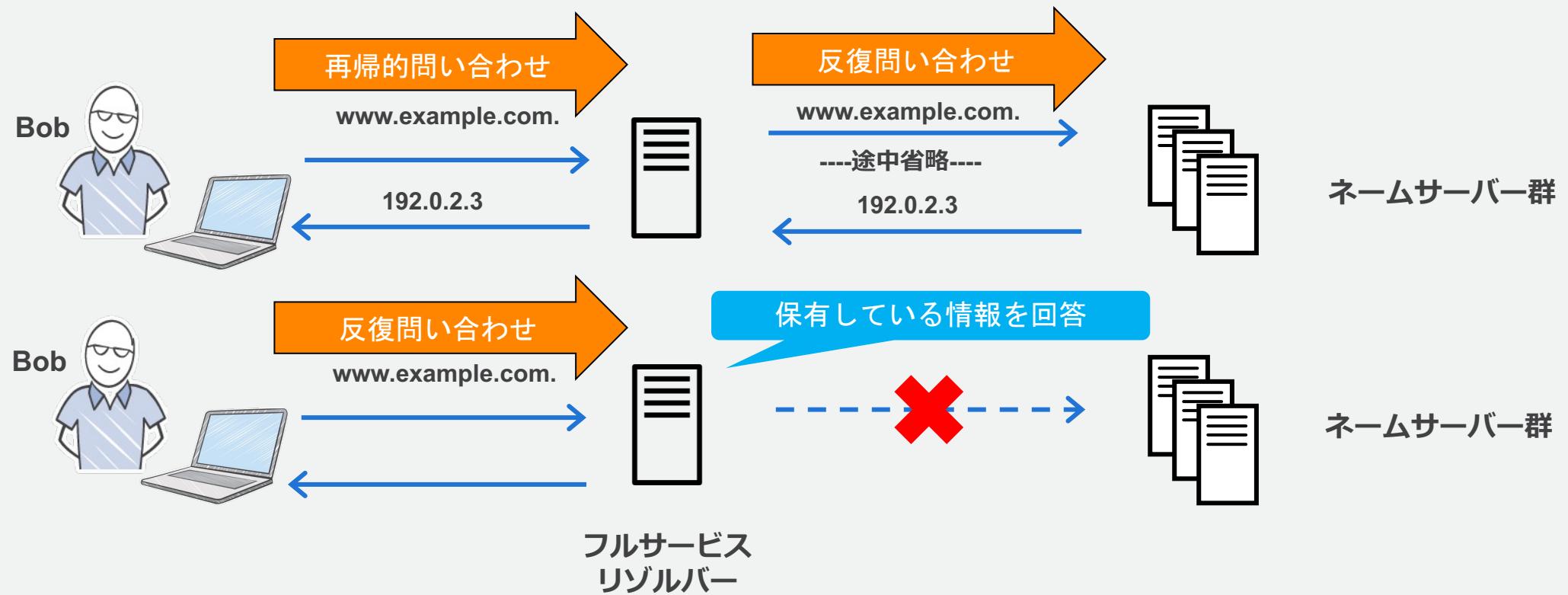
フルサービスリゾルバー(キャッシュ DNS サーバー)

- .(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



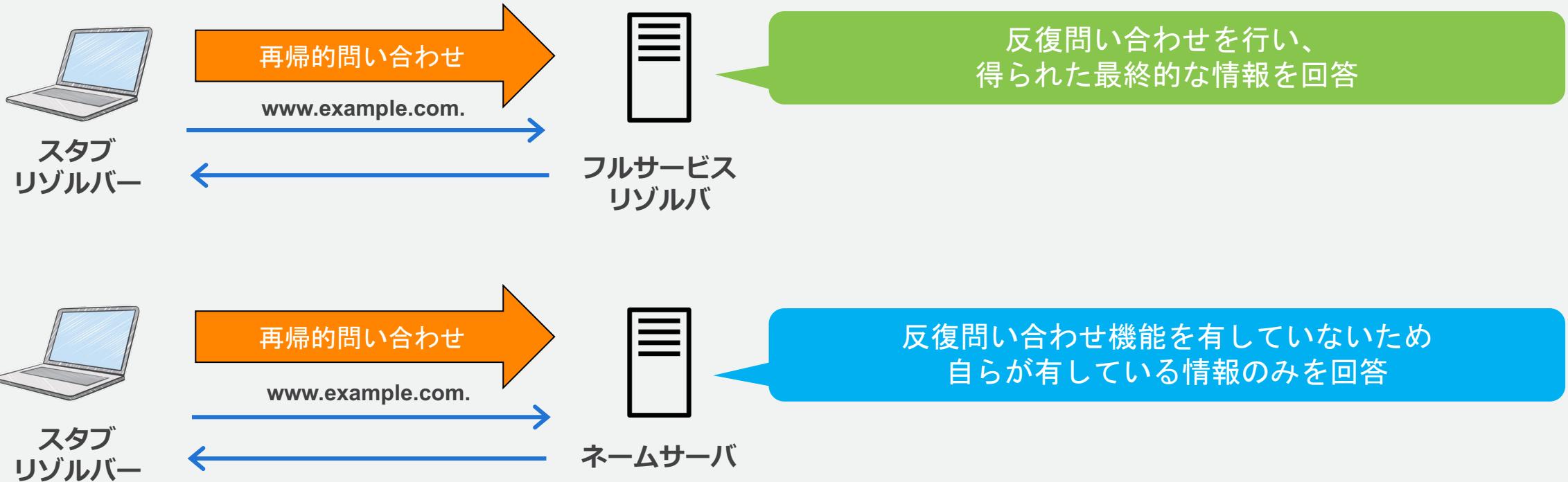
再帰問い合わせと反復問い合わせ

- 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



スタブリゾルバー

- 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

Preferred DNS server:

192 . 0 . 2 . 2

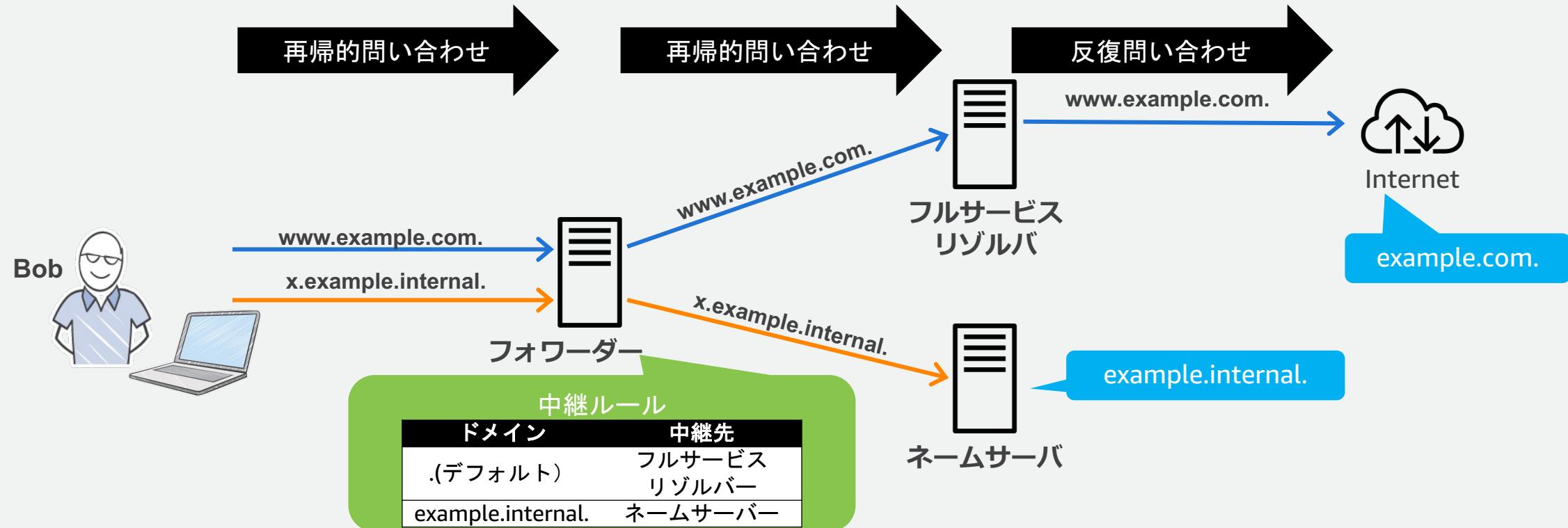
Alternate DNS server:

198 . 51 . 100 . 2

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

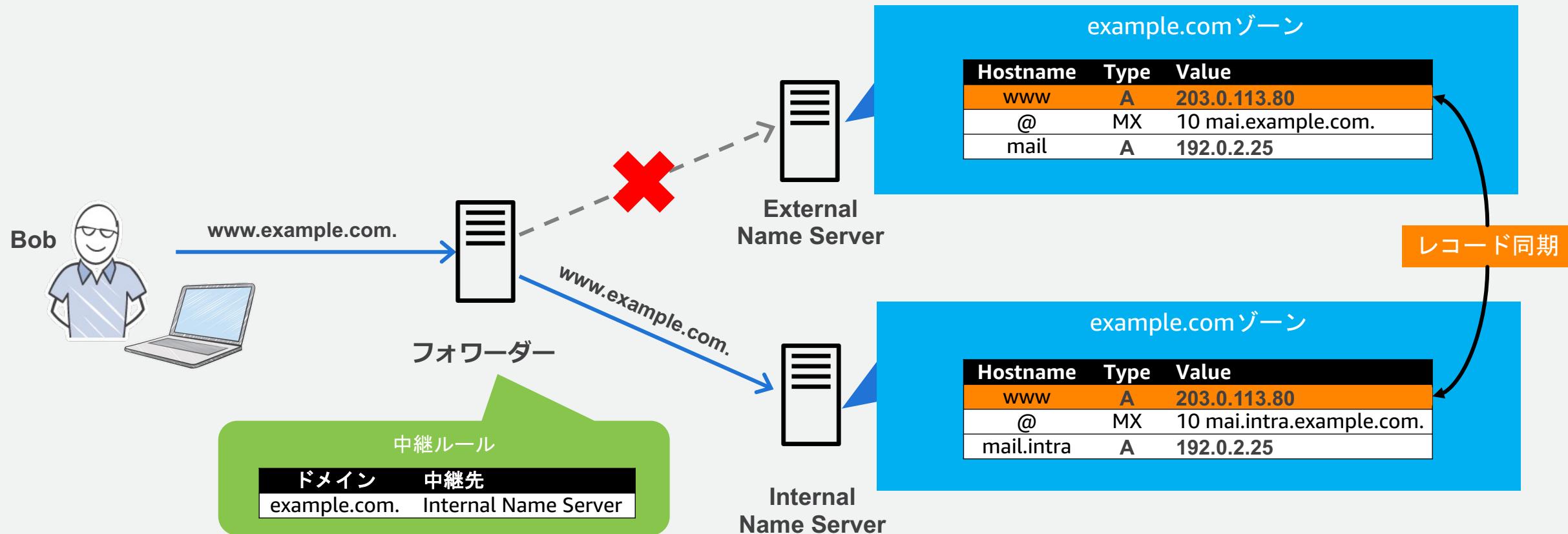
フォワーダー

- 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



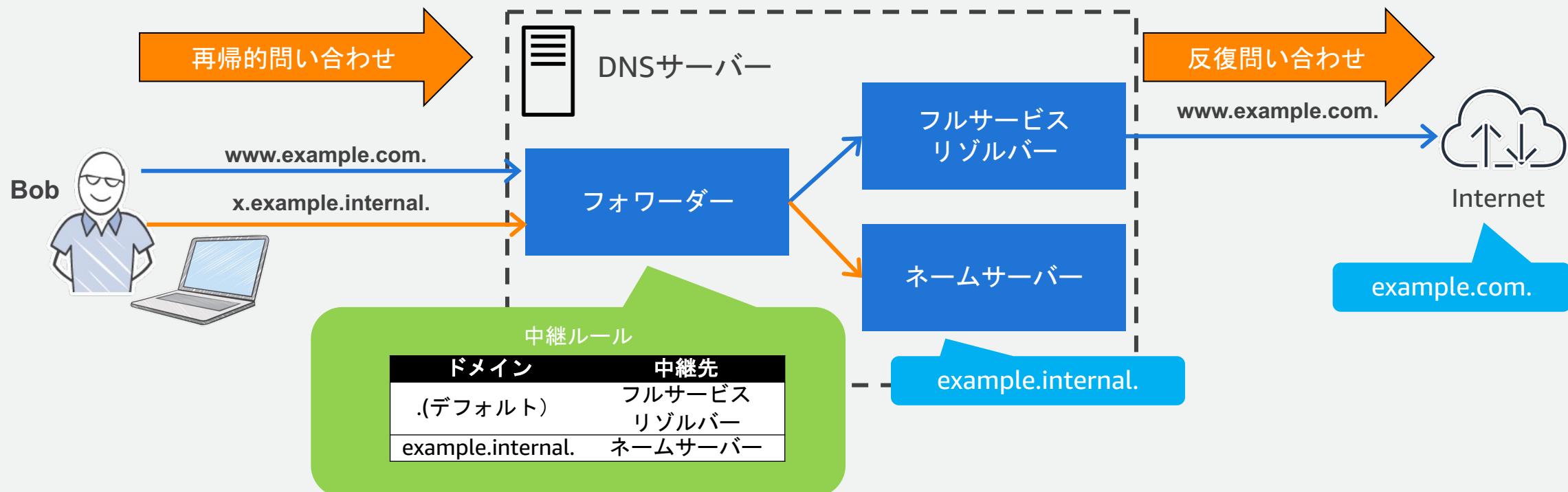
フォワーダーの制約

- 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 DNS サーバー基本構成

- ・ 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探っていることが多い



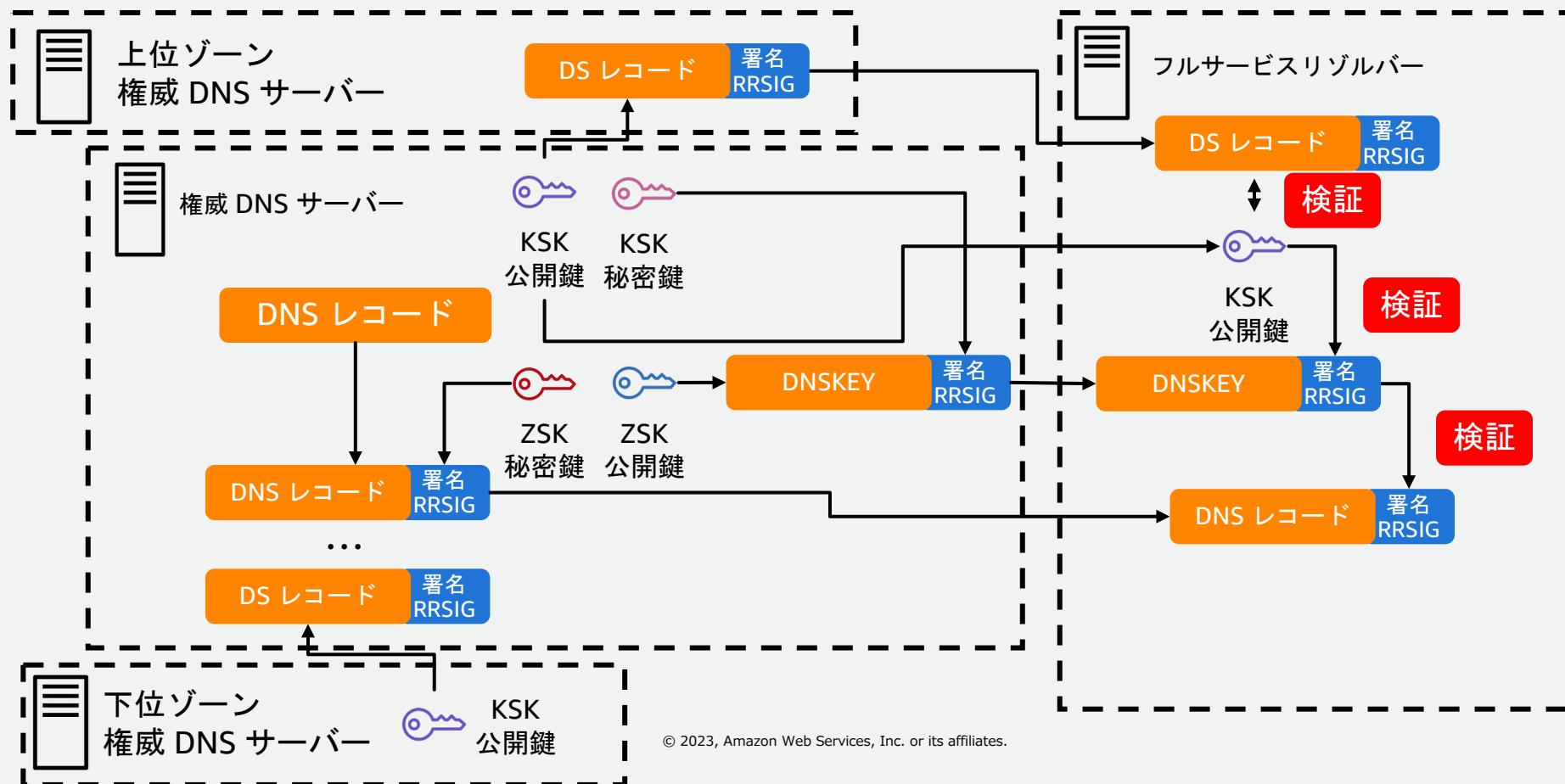
EDNS0 と EDNS Client Subnet 拡張

- EDNS0 は RFC 6891 で定義された DNS プロトコルの拡張
 - 512 バイトの DNS メッセージサイズを超えて様々な拡張機能を追加する
- EDNS Client Subnet: クライアントのアドレスブロックを権威サーバーに通知する技術
 - パブリック DNS リゾルバーの普及により、エンドユーザーとリゾルバーは必ずしも同じ地理的に近いわけではなくなつた
 - 位置情報に関する DNS ルーティングでエンドユーザーの位置推定の精度改善などに利用される



DNSSEC

- 応答に公開鍵暗号方式による署名を付与することで DNS の応答偽造を防ぐ技術
- ゾーンに署名する ZSK(Zone Signing Key) とゾーンの公開鍵に署名する KSK(Key Signing Key) の 2 種の鍵を利用
- RRSet の署名は RRSIG レコード、ZSK 公開鍵は DNSKEY レコード、KSK 公開鍵は信頼の連鎖を確立するために上位ドメインの DS レコードとして登録し公開する



名前解決の基礎 まとめ

- DNS サーバーの 4 つの機能と制約
 1. ネームサーバー (権威 DNS サーバー)
 2. フルサービスリゾルバー (キャッシュ DNS サーバー)
 3. スタブリゾルバー
 4. フォワーダー
- DNS クエリの種類
 1. 再帰的問合せ
 2. 反復問合せ
- レコードを構成する5つの要素と用途に応じたリソースレコードタイプ
- CNAME レコードタイプの制約と Zone Apex
- 正常応答のキャッシュ、不存在応答 (NXDOMAIN) のネガティブキャッシュ
- EDNS0 による DNS 拡張と DNSSEC

まとめ



まとめ

- Amazon Route 53 概要をインフラストラクチャとサービスの機能面からご紹介しました
- Amazon Route 53 の機能の理解のための DNS の基礎についておさらいしました
- 機能詳細については、Hosted Zone 編、Resolver 編をご視聴ください

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 5 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!



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



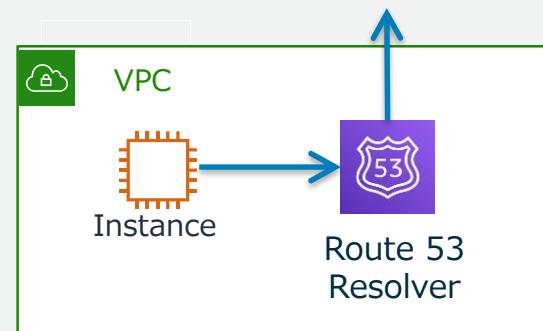
Amazon Route 53
Public Hosted Zone

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



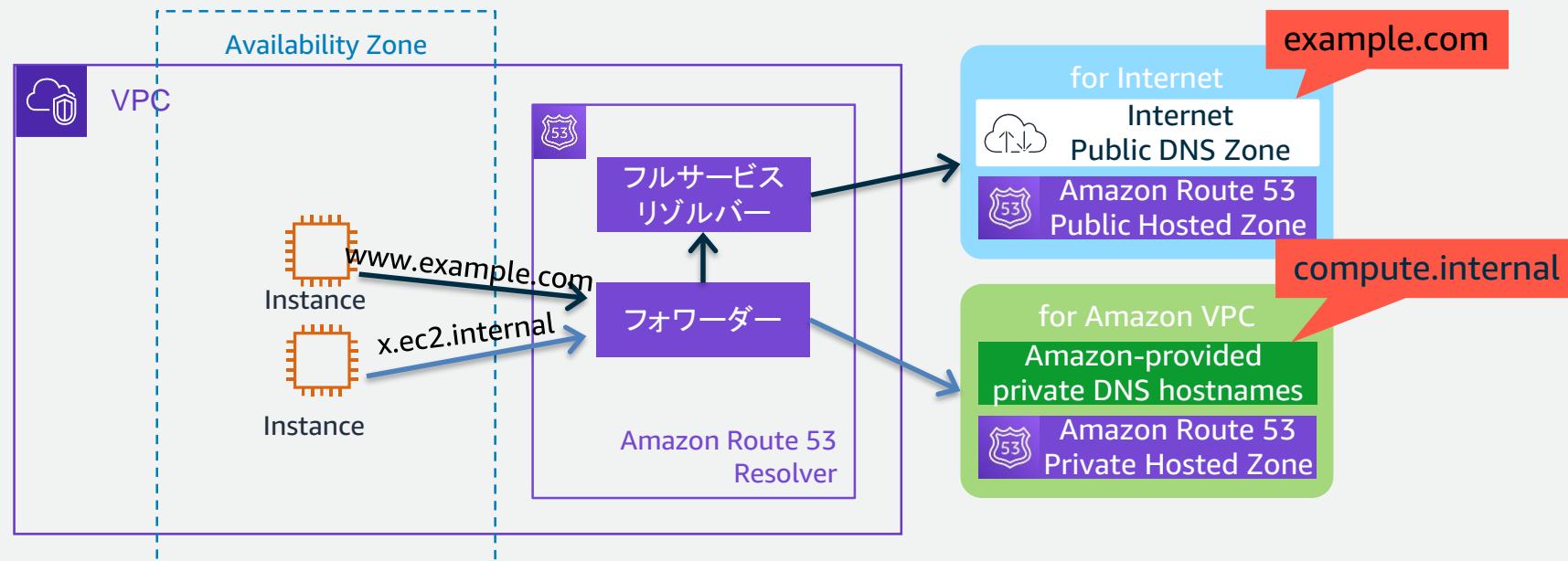
Amazon Route 53
Private Hosted Zone

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

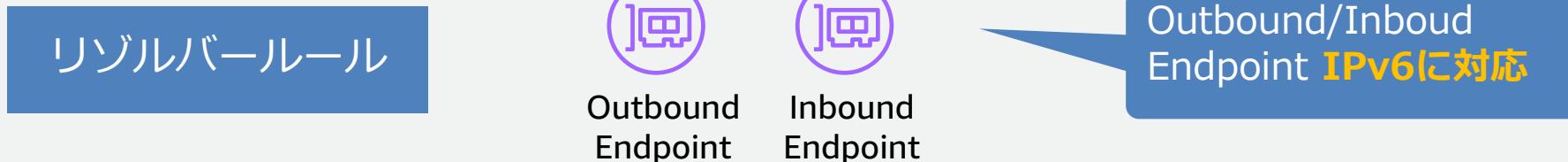
- VPCに標準で備わるDNSサーバー(フォワーダー + フルサービスリゾルバー)
 - VPC+2のIPアドレスでアクセス可能
例：VPCのCIDRが 10.0.0.0/16 の場合、10.0.0.2 でアクセス
- 以前「.2 Resolver」「Amazon Provided DNS」と呼ばれていたものを改称



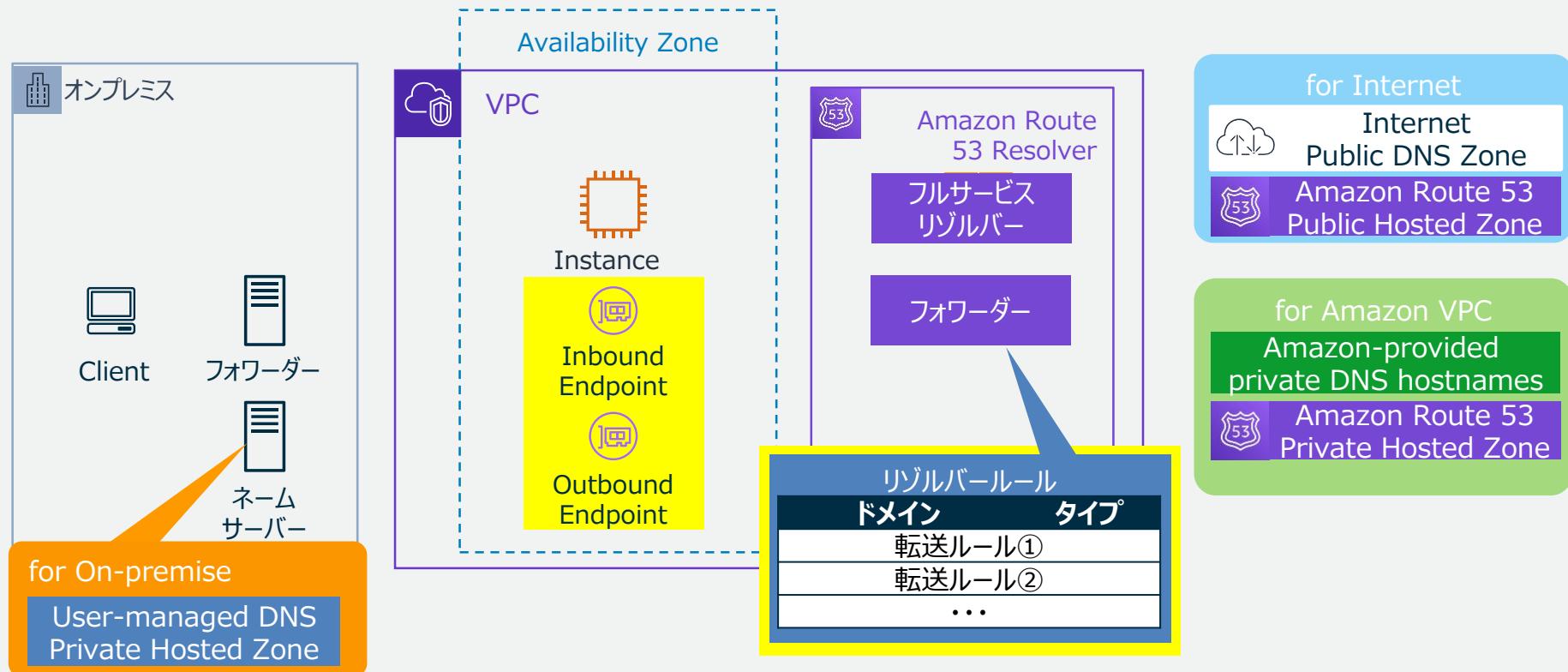
Amazon Route 53 Resolver for Hybrid Clouds

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

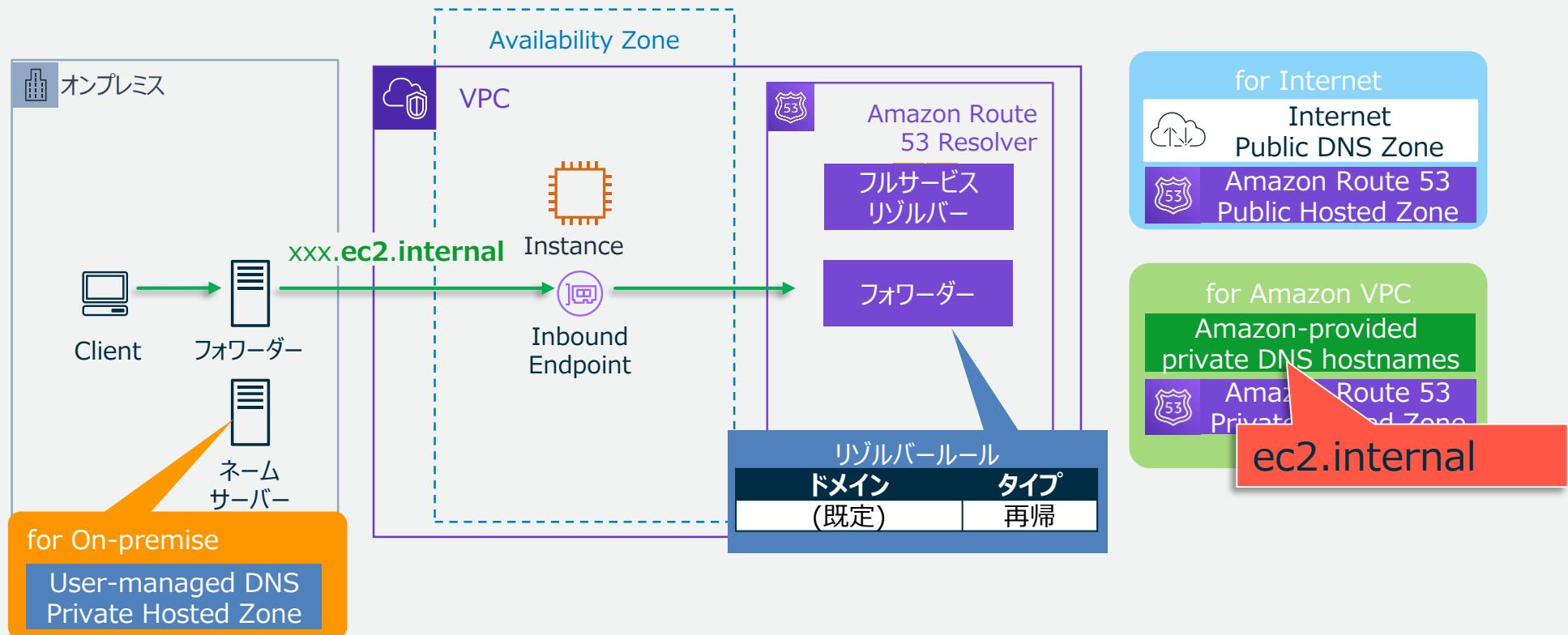


Route 53 Resolver for Hybrid Clouds Overview



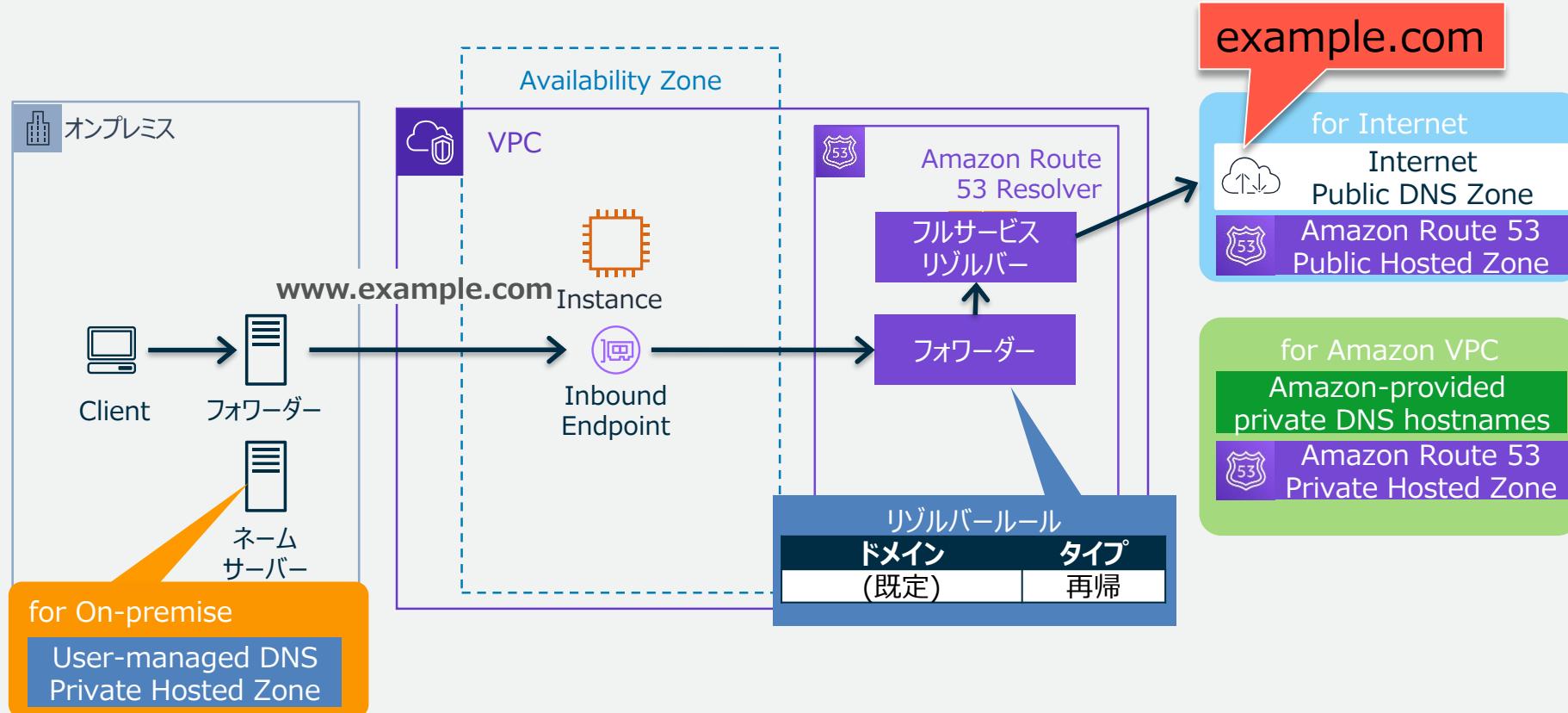
ユースケース①

オンプレミスからVPC向けゾーンの名前解決



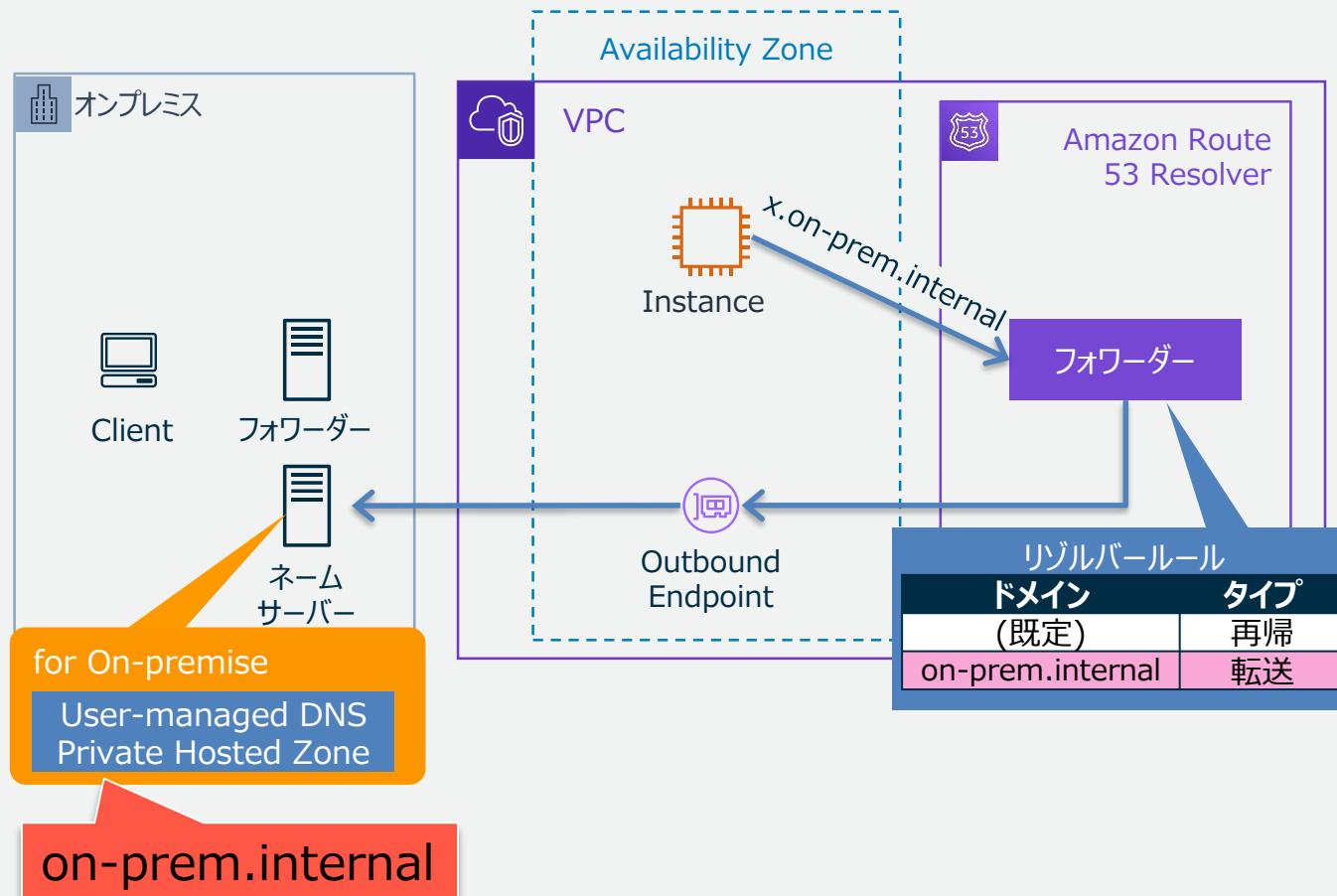
ユースケース②

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



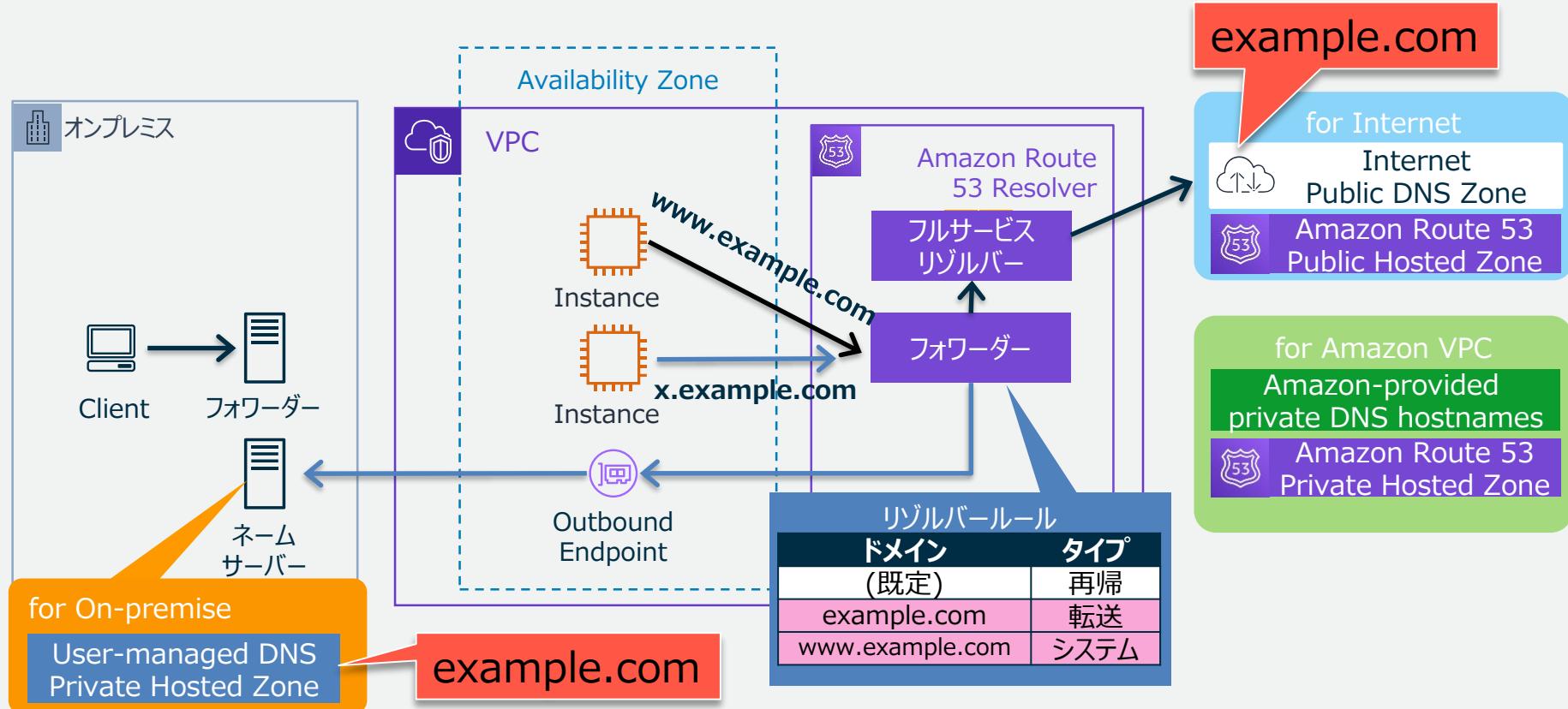
ユースケース③

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 リゾルバー自身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とするルールタイプ。

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



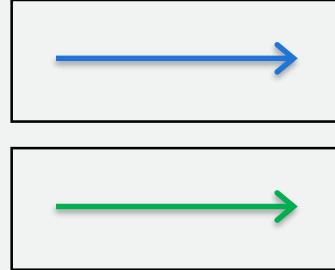
Route53 Resolver の逆引きDNSルールの上書きが可能

【参考】自動定義されたシステムルール

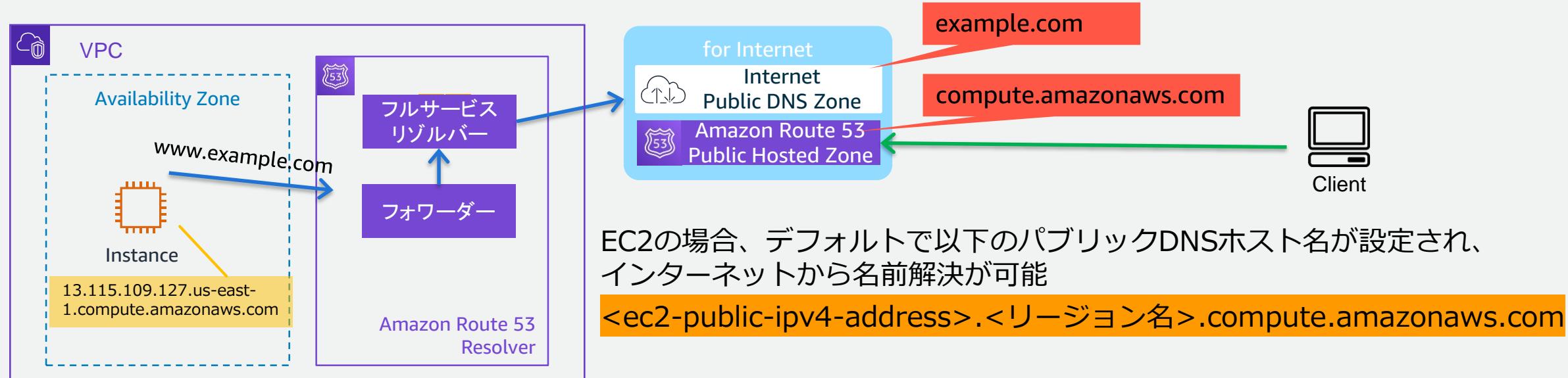
https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-autodefined-rules

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



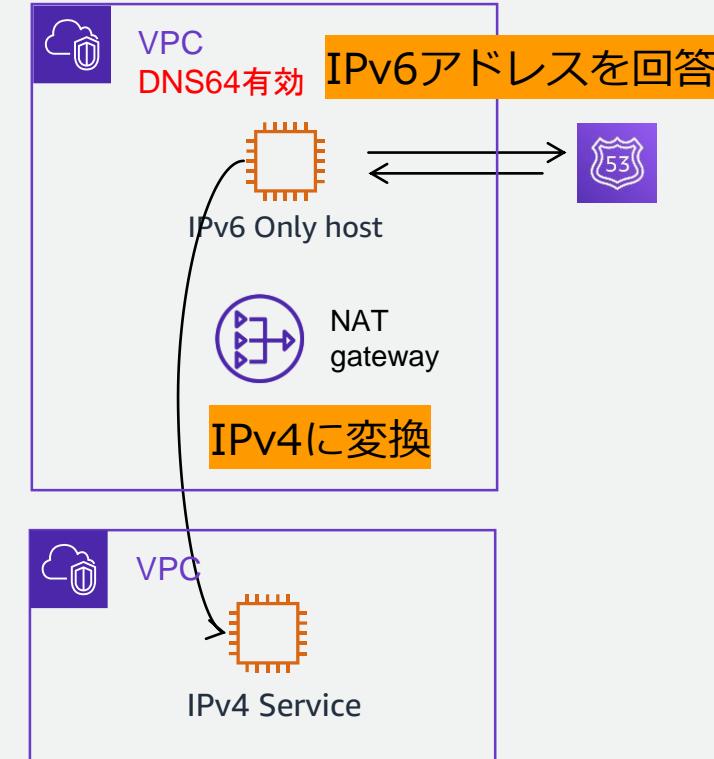
- EC2からインターネットに公開されたドメインへの名前解決
(AWS→インターネット)
- インターネットからEC2のパブリックDNSホスト名の名前解決
(インターネット→AWS)



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ヶ月だと…

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

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)}



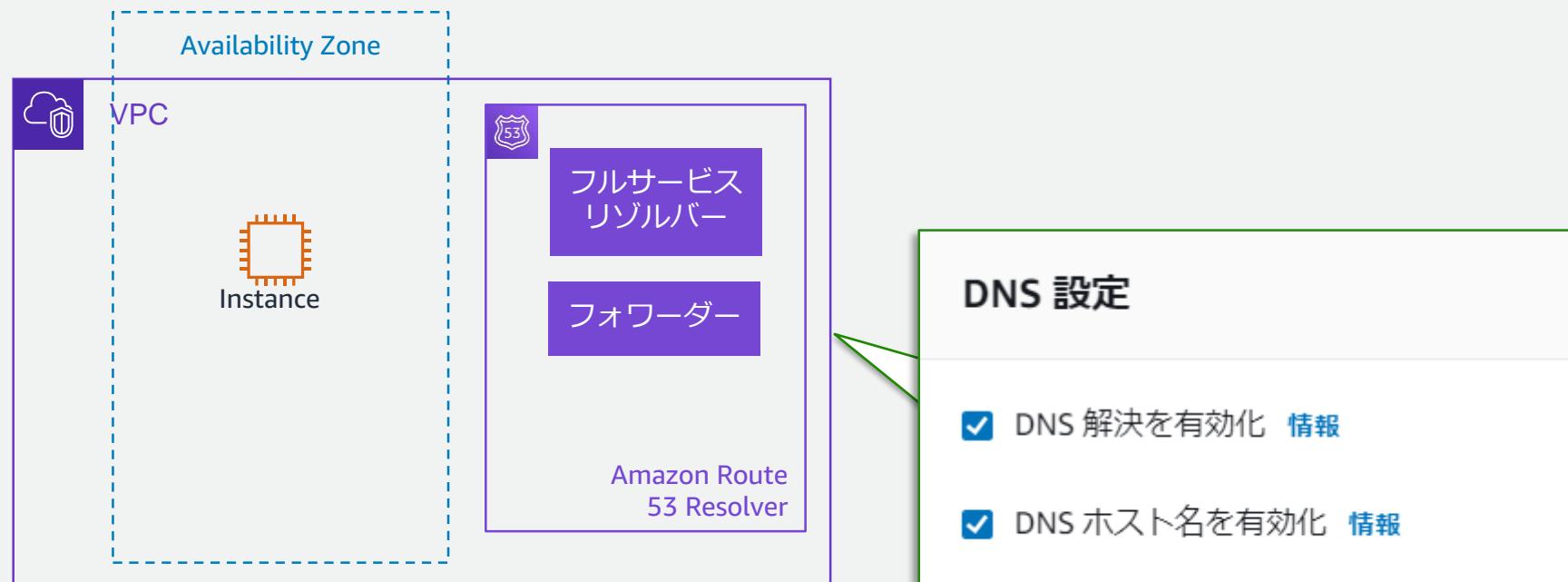
Amazon
Route 53 Resolver
for Hybrid Clouds

- 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

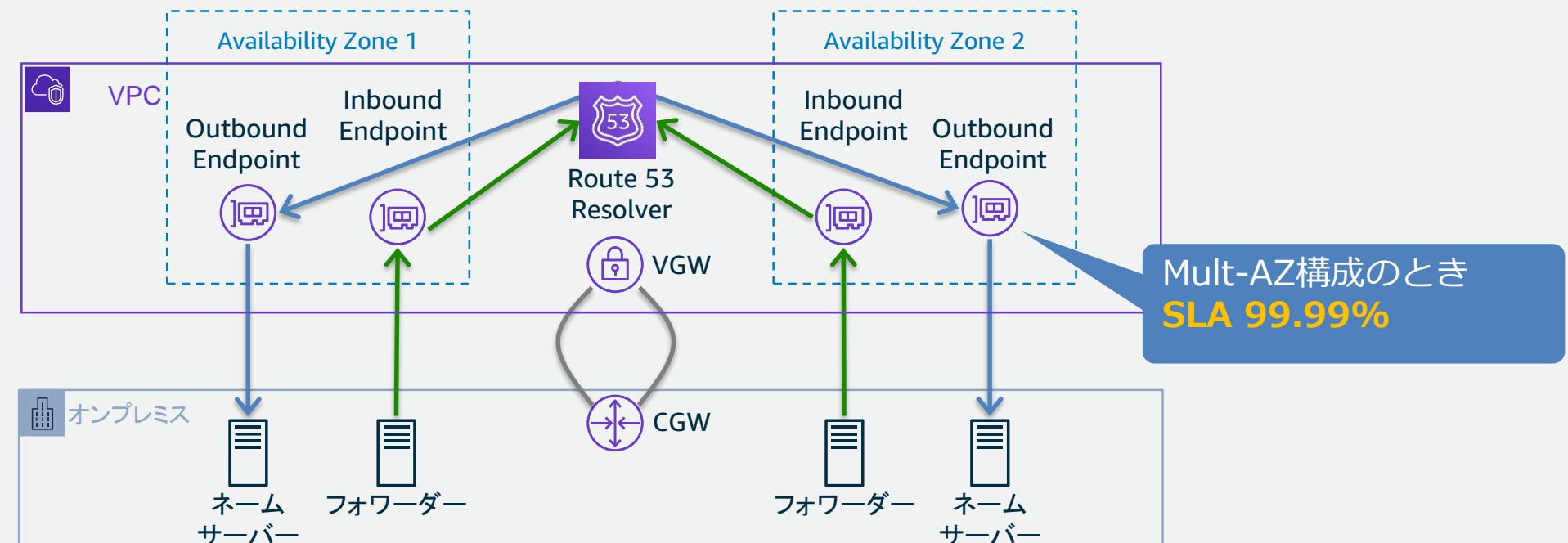
- VPC作成時にデフォルトで有効、必要な場合はVPC毎に有効/無効に設定可能
- IPアドレス設定はDHCPで自動的に配布される



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



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リ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 X

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タを使用します。

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ут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

エンドポイント名は最大 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。エントリの作成後は、この値を変更することはできません。

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ーゾーンで 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ーゾーンのアドレスを追加できます。

▼ IP アドレス #1

アベイラビリティーゾーン 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ーゾーン

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。

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.

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。

エンドポイント名は最大 64 文字です。有効な文字は、a~z、A~Z、0~9、スペース、_ (フロントドット) です。

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。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。

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ーゾーンで 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ーゾーンのアドレスを追加できます。

▼ IP アドレス #1

アベイラビリティーゾーン [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ーゾーンです。

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。リゾ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、この値を変更することはできません。

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 (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

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

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

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

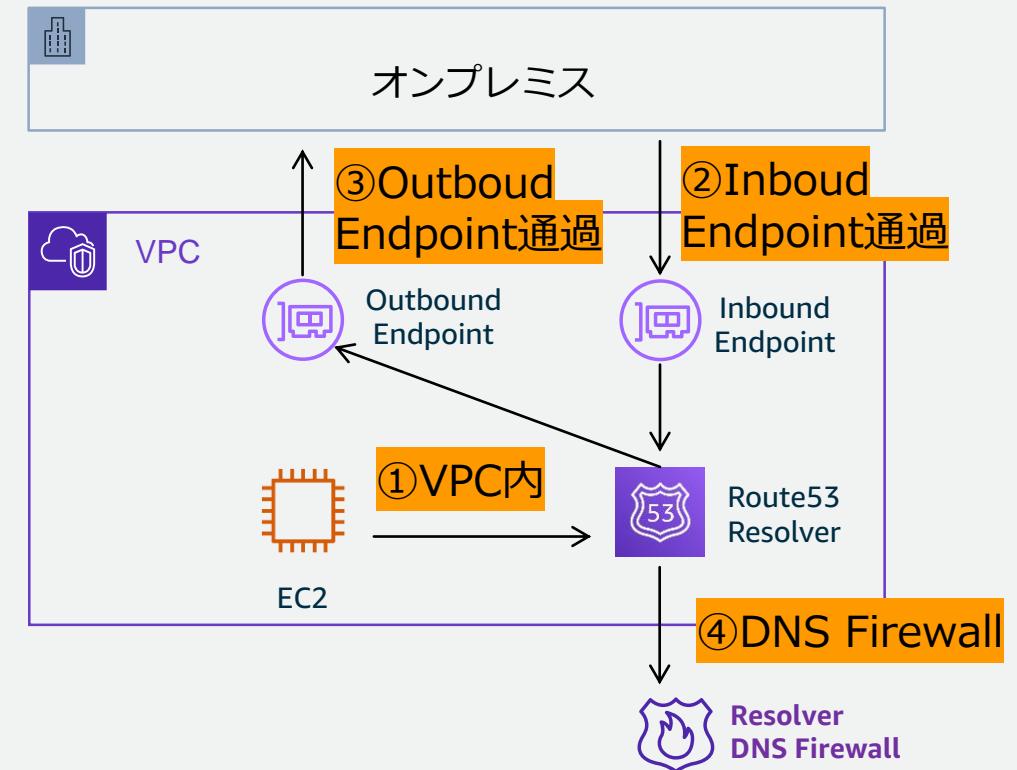
- Amazon Route 53 Resolverは通常そのまま利用可能
- Amazon Route 53 Resolver for Hybrid Clouds構成時の考慮ポイント
 - 各コンポーネントの冗長化を強く推奨、SPOFを作らない(Availability Zone / 回線 / サーバーなど)
 - エンドポイントには管理の必要性に応じてIPアドレスを指定
 - 転送ルールの共有はResource Access Managerで一元管理
- テストとトラブルシューティング
 - 実際にエンドポイントに対して問い合わせを試行する
 - 出力情報やオプションが豊富なdigコマンド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

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

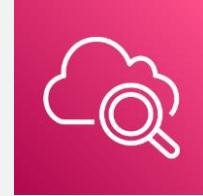


例：EC2のプライベートIPv4DNSの名前解決

```
{  
    "version": "1.100000",  
    "account_id": "xxxxxxxxxxxxxx",  
    "region": "us-east-1",  
    "vpc_id": "vpc-000a00aaa0000a0a",  
    "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"  
    }  
}
```

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

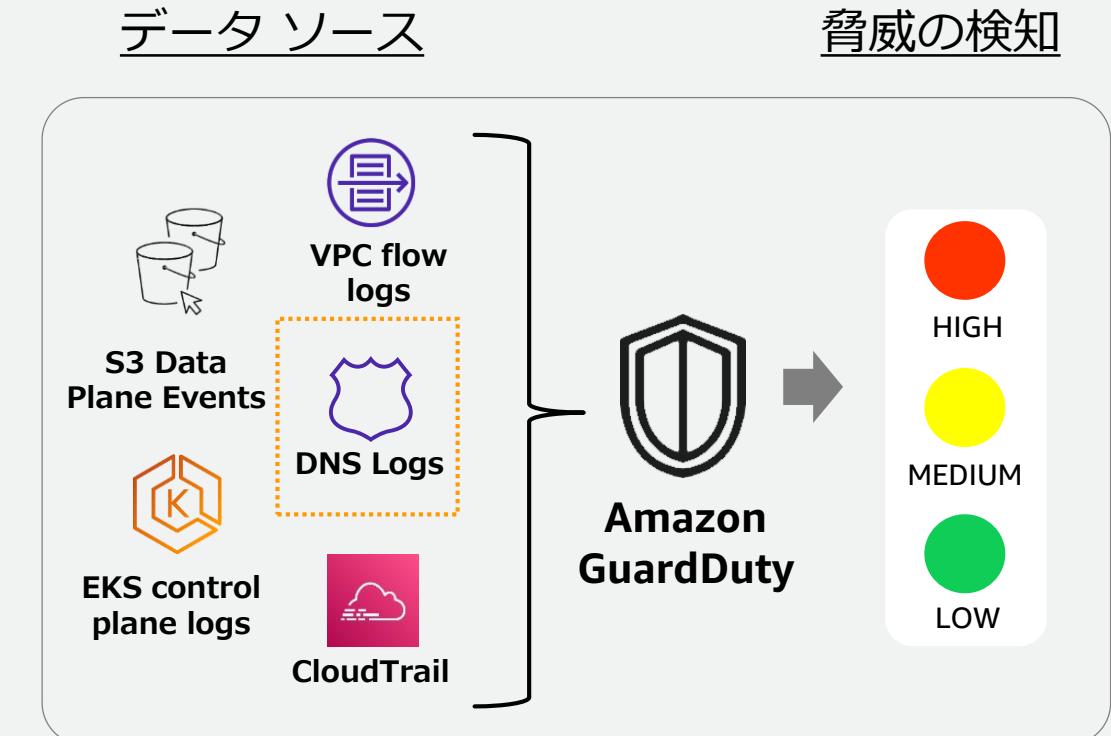
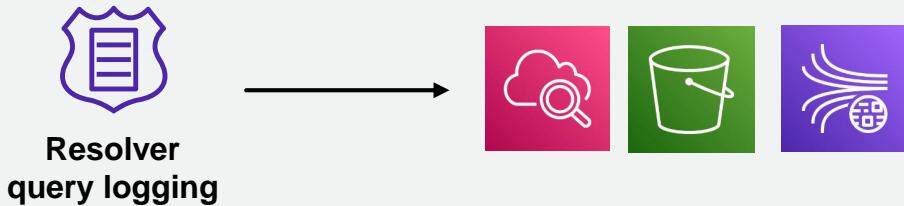


Kinesis Data Firehose の配信ストリーム

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

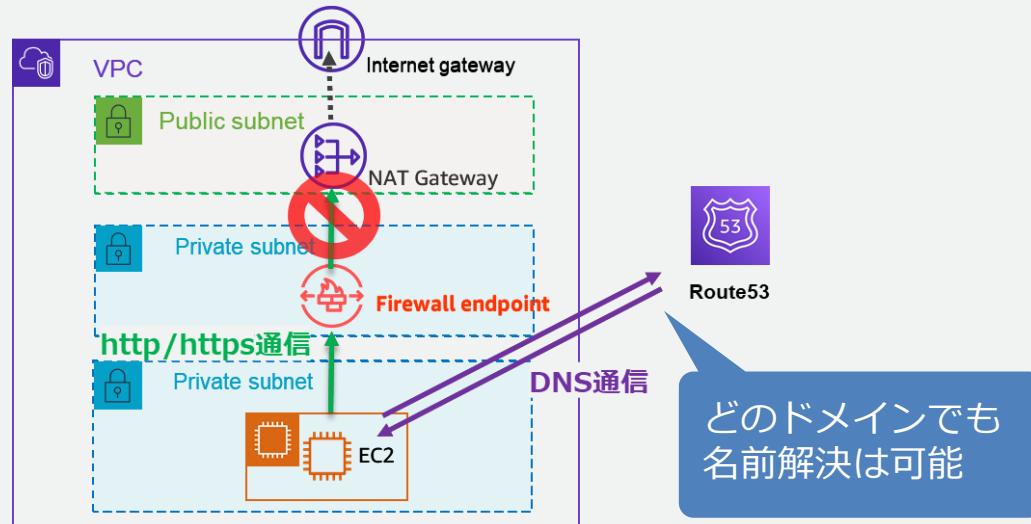


AWS Network Firewall との違い



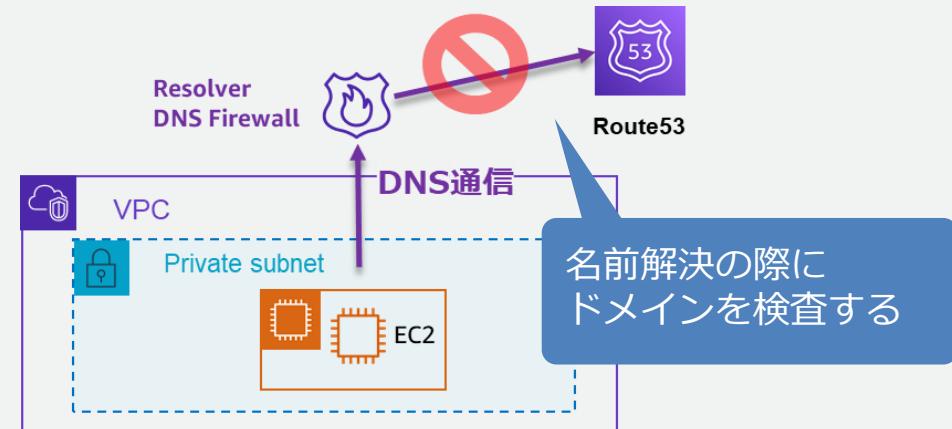
Network Firewall ドメインのフィルタリング

- 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

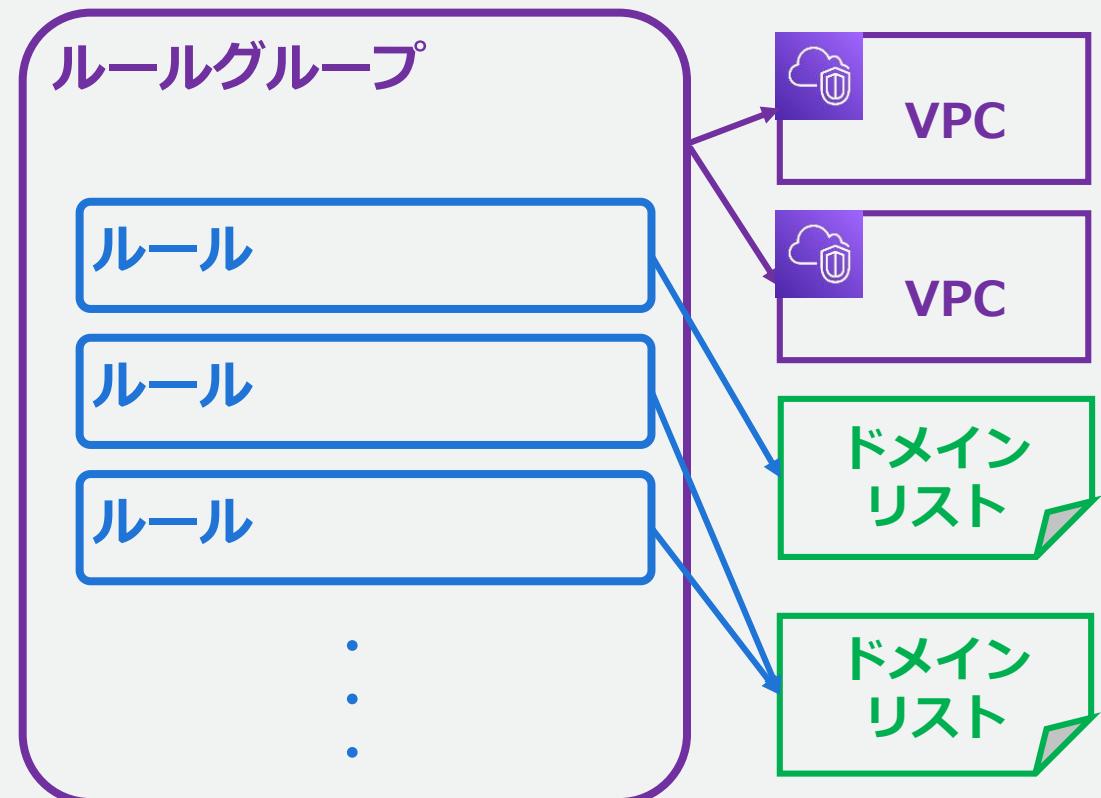


DNS Firewall の設定

DNS Firewall を使用するためには
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

The screenshot shows the 'Domain list builder' interface. At the top, it says 'Domain list name' followed by a text input field containing 'MyList'. Below this, a note states: 'The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -(hyphen), and _(underscore).'. There is also a radio button labeled 'Switch to bulk upload'. Below these, a section titled 'Enter one domain per line' contains a text area with two entries: 'example.com' and 'sample.com'.

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)				
<input type="text"/> Search				
Name	Action	Priority	Domain list	
Rule-01	ALLOW	1	rslvr-fdl-15f4860b1ad54ead (AWSManagedDomainsAggregateThreatList)	Edit Delete
Rule-02	ALLOW	2	rslvr-fdl-2c46f2ecbfec4dcc (AWSManagedDomainsMalwareDomainList)	Edit Delete
Rule-03	ALLOW	3	rslvr-fdl-aa970e9eb1ca4777 (AWSManagedDomainsBotnetCommandandControlDomainList)	Edit Delete
Rule-04	ALLOW	4	rslvr-fdl-b5f3953a7fe24d01 (AWSManagedDomainsGlobalThreatList)	Edit Delete

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

Set rule priority - optional [Info](#)

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

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

Rule priority
Move rules up or down to change the evaluation order.

▲ Move up **▼ Move down**

後に実行

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
MyRuleGroup	rslvr-frg-964...	Associated	2	Not shared

Rules	VPCs associated	Tags
Associated VPCs (2)		

ID	Name	Number of associated rule groups	Association ID
vpc-0a7f0591b83f4ab58	rgassoc-vpc-0a7f0591b83f4ab58-rslvr-frg-964306d798241b	-	rslvr-frgassoc-704910cdc9f54
vpc-060eb775c5c3bed...	rgassoc-vpc-060eb775c5c3bed7a-rslvr-frg-964306d79824...	-	rslvr-frgassoc-a89e068eeed44

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、リゾルバーが 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

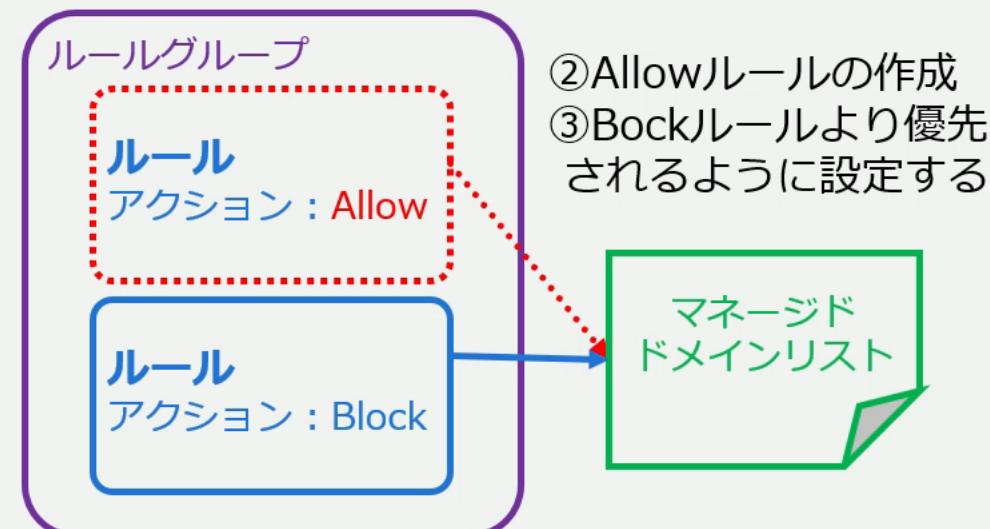
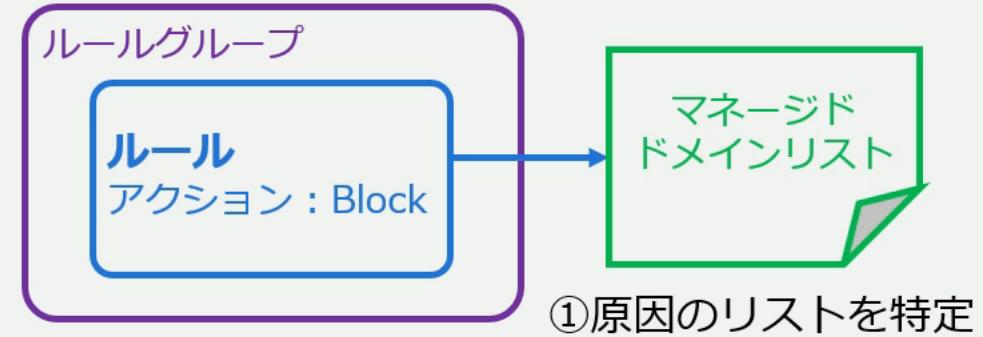
- フェイルオープン
 - DNS Firewallから応答がないDNSクエリは全て通過させる
 - セキュリティよりも可用性を優先

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

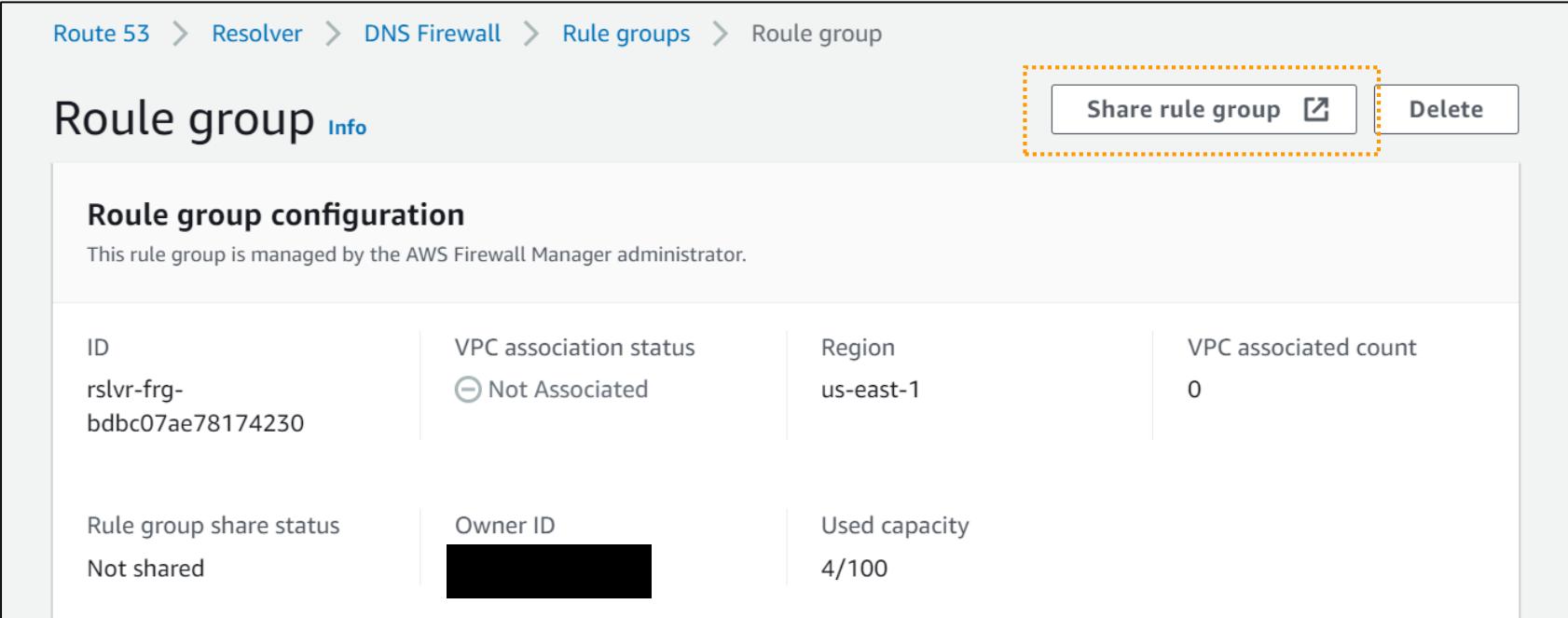
- ① ブロックしているルールの特定
 - Resolver ログを確認し、誤検出の原因となるルールグループとマネージドドメインリストを特定
- ② Blockされたクエリを明示的に許可するルールを追加
- ③ 追加したルールが優先されるように設定
 - ルールグループ内で新しいルールの優先度の値を①のマネージドリストを使用しているルールの数値より小さく設定する

➡ 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



The screenshot shows the AWS Route 53 Resolver interface, specifically the DNS Firewall section. The navigation path is: Route 53 > Resolver > DNS Firewall > Rule groups > Rule group. The main title is "Rule group" with an "Info" link. On the right, there are two buttons: "Share rule group" with a copy icon and "Delete". A yellow dashed box highlights the "Share rule group" button. Below the title, it says "Rule group configuration" and "This rule group is managed by the AWS Firewall Manager administrator." The table contains the following data:

ID	VPC association status	Region	VPC associated count
rslvr-frg-bdbc07ae78174230	Not Associated	us-east-1	0

Rule group share status	Owner ID	Used capacity
Not shared	[REDACTED]	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」](#)



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=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



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。



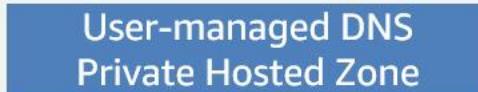
Amazon-provided
private DNS hostnames

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。



Amazon Route 53

Hosted zone 編

Amine Tei (丁 亞峰)

Solutions Architect
2023/05

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



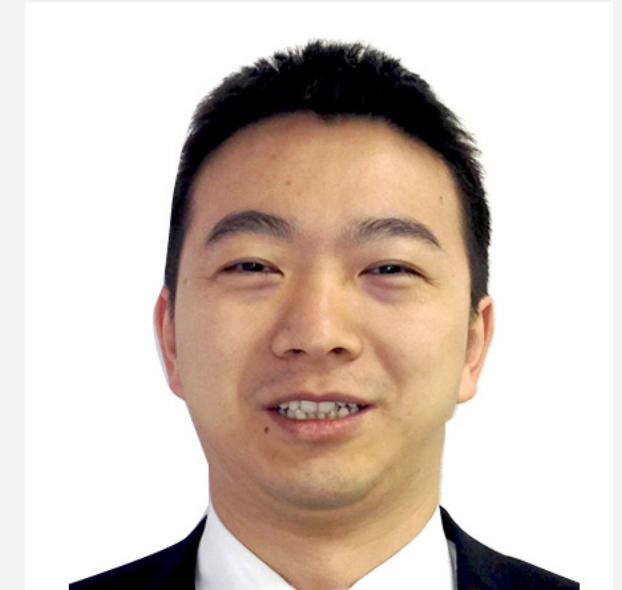
内容についての注意点

- 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)

自己紹介

名前：丁 亜峰

所属：アマゾンウェブサービスジャパン合同会社
西日本担当ソリューションアーキテクト



経歴：SaaS会社にてインフラエンジニアとして活動（大阪）

好きなAWSサービス：

AWS Transit Gateway, AWS サポート, AWS IoTサービス

本セミナーの対象者

- これからAmazon Route 53 を利用される予定の方
- オンプレミス-AWS環境のDNSの設計・実装を担当される方
- AWSのネットワーク設計を担当されている方

Agenda

1. Amazon Route 53 ドメインの登録
2. Amazon Route 53 Hosted Zone
3. トラフィックルーティング
4. ドメイン移行とテスト、トラブルシューティング
5. まとめ

Agenda

1. Amazon Route 53 ドメインの登録
2. Amazon Route 53 Hosted Zone
3. トラフィックルーティング
4. ドメイン移行とテスト、トラブルシューティング
5. まとめ

ドメインのレジストラ Amazon Route 53 ドメインの登録



Amazon Route 53にて新しいドメインを登録

- サポートされるドメイン 2023/4時点
 - 汎用トップレベルドメイン (gTLD)
 - 273 gTLD (.com .net .org など)
 - 地理的トップレベルドメイン (ccTLD)
 - 62 ccTLD (.uk .au .ca .de など)
 - Route 53 レジストラは、Amazon Registrar, Inc. と Gandi のいずれか
- 信頼性の高いTLDを利用
 - プロダクトなど可用性が求められるユースケース

Amazon Route 53 に登録できる最上位ドメイン

https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/registrar-tld-list.html

Amazon Route 53にて新しいドメインを登録

① ドメイン名の選択

.com - \$13.00 チェック

ドメイン名を登録するには、使用可能なものの検索から開始します。ドメイン名の最初の部分 (example.com の example など) を入力し、拡張子 (.com や .org など) を選択して、[チェック] をクリックします。ドメインが使用可能かどうか、および他の拡張子で取得できるかどうかお知らせします。[詳細はこちら](#)

② 1 ドメインのお問い合わせ詳細

登録者、管理者、および技術的な連絡先の詳細を以下に入力します。特に指定されない限り、すべてのフィールドが必須です。[詳細はこちら](#)

登録者、管理者、および技術的な連絡先はすべて同じです: いいえ いいえ

登録者の連絡先

連絡先のタイプ	会社
名	Domain
姓	Registr
会社名	company
Eメール	company@example.com
電話	+44 1234567 国コードと電話番号を入力します
住所 1	50 Asdf 住所: 私営地
住所 2	Osaka フアード、部屋、部署、ビル、階など
国/地域	Japan
都道府県	都道府県は必須ではありません
市区町村	
郵便番号	

プライバシーの保護

連絡先タイプが会社の場合:

- プライバシー保護により、.com ドメインの一部の連絡先詳細が非表示になります。

有効化 無効化

③ 連絡先の詳細の確認

次の連絡先情報が正しいことを確認します。購入を完了すると、ショッピングカートのすべてのドメインに対してこの情報が使用されます。

登録者の連絡先	管理者の連絡先	テクニカル担当者
Domain Registr company company@example.com +44.1234567 50 Asdf Osaka Suiat 100-0002 JP プライバシー保護済み	Domain Registr company company@example.com +44.1234567 50 Asdf Osaka Suiat 100-0002 JP プライバシー保護済み	Domain Registr company company@example.com +44.1234567 50 Asdf Osaka Suiat 100-0002 JP プライバシー保護済み

新しいドメインの DNS の管理

新しいドメインの DNS のサービスとして簡単に Route 53 を使用するため、自動的にホストゾーンが作成されます。これは、ドメインのトラフィックをルーティングする方法 (たとえば Amazon EC2 インスタンスにルーティングする) についての情報を保存する場所です。ここでドメインを使用しない場合は、ホストゾーンを削除できます。お客様のドメインを使用する場合、ホストゾーンおよびそのドメインに対して当社が受け取る DNS ケリについては、Route 53 の料金がかかります。詳細については、[Amazon Route 53 料金表](#) を参照してください。

ドメインを自動的に更新しますか?

ユーザーは、登録したドメイン名を 1 年間所有します。ドメイン名の登録を更新しない場合は期限切れとなり、他のユーザーがそのドメイン名を登録できるようになります。毎年、自動的に更新することによって、ドメイン名を確実に保持することができます。ドメイン名更新のコストはお使いの AWS アカウントに請求されます。Route 53 コンソールを使用して、いつでも自動更新を有効または無効にできます。詳細については、[ドメイン登録の更新](#) を参照してください。

有効化 無効化

規約

Amazon Route 53 では、AWS アカウントを使用してドメイン名を登録し、移管することができます。ただし、AWS はドメイン名レジストラではないため、レジストラソシエイトが登録および移管サービスを行います。AWS を通じてドメイン名を購入する場合、当社レジストラソシエイトがドメインを登録します。ドメインのレジストラは、指定された登録者の連絡先と定期的に連絡を取って連絡先の詳細を確認し、登録を更新します。

AWS ドメイン名の登録契約 を読んで同意します

[キャンセル](#) [戻る](#) [注文を完了](#)

Amazon Route 53にて新しいドメインを登録

The screenshot shows the AWS Route 53 'Registered domains' page. On the left, a sidebar lists various services: Dashboard, Hosted zones, Health checks, IP-based routing, CIDR collections, Traffic flow, Traffic policies, Policy records, Domains, Registered domains (which is selected and highlighted in orange), Pending requests, Resolver, VPCs, and Inbound endpoints. The main content area displays a single registered domain. At the top of this section are three buttons: 'Edit contacts', 'Manage DNS', and 'Delete domain'. Below these are several domain details:

Domain	Transfer lock	Authorization code	Name servers
[Redacted]	Disabled (enable)	Get code	ns-526.awsdns-01.net ns-439.awsdns-54.com ns-1152.awsdns-16.org ns-1562.awsdns-03.co.uk Add or edit name servers
Registration date 2022-10-14	Domain name status code	addPeriod ok	
Expiration date 2023-10-14 (extend)	Tag	View and manage tags for your domains using Tag editor	
Auto renew Enabled (disable)			

Below this, there are sections for 'Registrant contact' (Verified, Domain Registrar: reinvent-net206@, Address: 60 Holborn Viaduct, London, London EC1A 2FD, GB), 'Administrative contact' (Domain Registrar: reinvent-net206@, Address: 60 Holborn Viaduct, London, London EC1A 2FD, GB), and 'Technical contact' (Domain Registrar: reinvent-net206@, Address: 60 Holborn Viaduct, London, London EC1A 2FD, GB). A red circle highlights the 'Name servers' section, and a red arrow points from the explanatory text below to the 'Add or edit name servers' link.

新しいドメインの ネームサーバとして簡単に Route 53 を使用するため、自動的にホストゾーン（後述）が作成され、ドメインのトラフィックをルーティングする方法（後述）についての情報を保存する場所。

ドメインを移管



- 1** • 現在のレジストラでドメインをロック解除する
• ドメインを新しいレジストラに移管
- 2** • AWSへ移管する場合:
 - ネームサーバーが割り当てられる
 - Route 53 Public Hosted Zone が作成される

Amazon Route 53 ヘドメインを移管

- TLD一覧に含まれているドメインの移管は可能
- 移管時に現レジストラより認証コードが必要となる場合がある
 - TLD の「Route 53 への移管に必要な認証コード」をご参照

Route 53 へのドメインの移管

別のレジストラから Route 53 に 1 つまたは複数のドメイン登録を移管できます。続行する前に、以下の操作を実行します。

- ドメインが移管可能であることを確認します。 [最上位ドメインの移管要件](#) を参照してください。
- 移管するドメインごとに、 [Route 53 へのドメイン登録移管](#) の最初の 4 つのステップを実行します。

最大 5 つのドメインを移管するには、各ドメイン名を以下に入力できます。

5 つを超えるドメインを移管する場合は、 [複数のドメインの Route 53 への移管ページ](#) を使用できます。

.com - \$13.00

▼

チェック

別のレジストラから Route 53 にドメインの登録を移管できます。 [詳細はこちら](#)

https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/domain-register-values-specify.html

Route 53 Architecture – Name server ストライブ

.com

ns-10.awsdns-32.com.

ns-123.awsdns-00.com.

ns-321.awsdns-02.com.

...

.net

ns-513.awsdns-62.net.

ns-600.awsdns-00.net.

ns-673.awsdns-00.net.

...

.co.uk

ns-1025.awsdns-00.co.uk.

ns-1090.awsdns-00.co.uk.

ns-1254.awsdns-00.co.uk.

...

.org

ns-1514.awsdns-00.org.

ns-1720.awsdns-00.org.

ns-1852.awsdns-00.org.

...

example.com

4つの独立したコントロールプレーン
1つのドメインにストライブ内の4つのネームサーバー
を割り当てる。



Amazon Builders' Library

シャッフルシャーディングを使ったワークロードの分離

アーキテクチャ | レベル 400

新しいコンテンツの通知を受け取りますか？

更新を受け取る

[記事の内容](#)

はじめに

[DNS ホスティングの対応開始](#)

[DDoS 攻撃への対処](#)

[シャッフルシャーディングとは？](#)

[Amazon Route 53 とシャッフルシャーディング](#)

[まとめ](#)

[ハンズオンラボ](#)

Colm MacCárthaigh 著

[PDF](#)[Kindle](#)

現在では、世界でも最も大きいビジネスやほとんどの著名なウェブサイトをホスティングしている Amazon Route 53 ですが、その立ち上がり時期においては、はるかに控え目なものでした。

DNS ホスティングの対応開始

AWS のサービス開始後、さほど長い時間が経過する前に、AWS のお客様からは、Amazon Simple Storage Service (S3)、Amazon CloudFront、Elastic Load Balancing のサービスをドメインのルートで使用して、「www.amazon.com」だけでなく「amazon.com」というドメイン名も使いたいという要望がありました。

これは、一見簡単なことに思えます。しかし、1980 年代に決定された DNS プロトコルの設計思想が、これを見た目より困難にしているのです。DNS には、CNAME と呼ばれる機能があり、所有者はドメインの一部のホスティングを他のプロバイダーに任せられるようになっています。しかしこの機能は、ドメインのルートやトップレベルでは使えません。先に書いたような要望に答えるには、お客様のドメインを、当社が実際にホスティングしなければならないのです。当社でお客様ドメインをホスティングすると、Amazon S3、Amazon CloudFront、Elastic Load Balancing などに対し、その時点のいかなる IP アドレスのセットでも返す事が可能です。こういったサービスは拡張し続けており IP アドレスも追加され続けています。つまり、ユーザーの方ご自身で、ドメイン定義の中に容易にハードコードできるようなものではありません。

<https://aws.amazon.com/jp/builders-library/workload-isolation-using-shuffle-sharding/>



Agenda

1. Amazon Route 53 ドメインの登録
2. Amazon Route 53 Hosted Zone
3. トラフィックルーティング
4. ドメイン移行とテスト、トラブルシューティング
5. まとめ



ドメインのDNS サービス Amazon Route 53 Hosted Zone



Amazon Route 53 Hosted Zone の特徴

信頼性

- 冗長化されたロケーション
- SLA設定

使いやすさ

- フルマネージドサービス
- トラフィックフロー
- CLI/APIでの操作
- 数分で利用開始など

高速

- 全世界で動作するAnycastネットワーク
- 変更を高速伝播

経済性

- 安価
- 使用した分だけの課金

AWS サービスと の統合

- エイリアスレコード
- IAM
- CloudWatchメトリクス
- CloudTrail
- など

柔軟性

- 重みづけラウンドロビン
- レイテンシベース
- DNSフェイルオーバー
- 位置情報ルーティングなど

Public Hosted Zone と Private Hosted Zone

Public hosted zone

- インターネット向けリソースへのルート
- インターネットからのリゾルバー
- インターネットにアクセス可能なネームサーバー
- 親ゾーンから委任できる
- サブドメインの委任をサポートする
- グローバルルーティングポリシー
- DNSSEC コンフィギュレーション

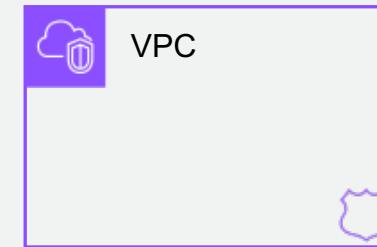
Private hosted zone

- VPC リソースへのルーティング
- VPC (またはオンプレミスネットワーク) から名前解決
- 転送ルールとエンドポイントを使用してアクセス可能
- クロスアカウントで共有、複数VPC間で共有
- 委任をサポートしていません

Route 53 リゾルバー (VPC+2) との統合



Internet

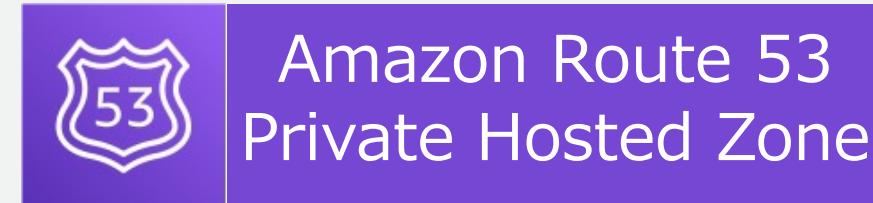


Public Hosted Zone と Private Hosted Zone

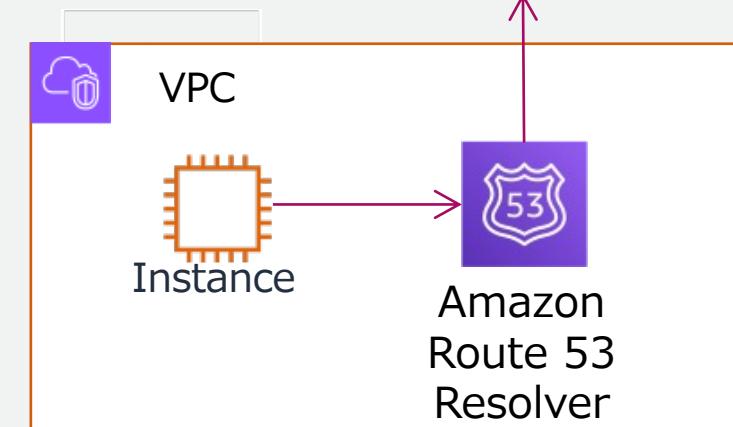
- 特定のVPCからの問い合わせと、それ以外からの問い合わせを識別し、異なる応答を返す
- スプリットビュー DNS /スプリットホライズン DNSを構成できる



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



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 Hosted Zoneでできること

- フルマネージドのネームサーバー
- ヘルスチェック & DNS フェイルオーバー
- トラフィックルーティング

Hosted Zone = ネームサーバー

- Hosted Zoneでドメイン名のリソースレコードを管理
- Amazon Route 53 は、作成したHosted Zoneごとに、ネームサーバー (NS) レコードと Start of Authority (SOA) レコードを自動的に作成する

レコード (2) 情報					
Automatic モードは最適なフィルタ結果に最適化された現在の検索動作です。モードを変更するには、[設定] に移動します。					
	レコード名	タイプ	ルーティングポリシー	差別...	TTL (秒)
<input type="checkbox"/>	sample.com	NS	シンプル	-	いいえ
<input type="checkbox"/>	sample.com	SOA	シンプル	-	いいえ

↑↑↑ 原則としてこれらのレコードを変更しないでください

値/トラフィックのルート...
ns-1783.awsdns-30.co.uk.
ns-1334.awsdns-38.org.
ns-890.awsdns-47.net.
ns-114.awsdns-14.com.
ns-1783.awsdns-30.co.uk. a...
172800
ns-1783.awsdns-30.co.uk. a...
900

1つのHosted ZoneにネームサーバーのFQDNを4つ割り当て、4つのトップレベルドメイン (*.com, *.org, *.net, *.co.uk) にまたがる

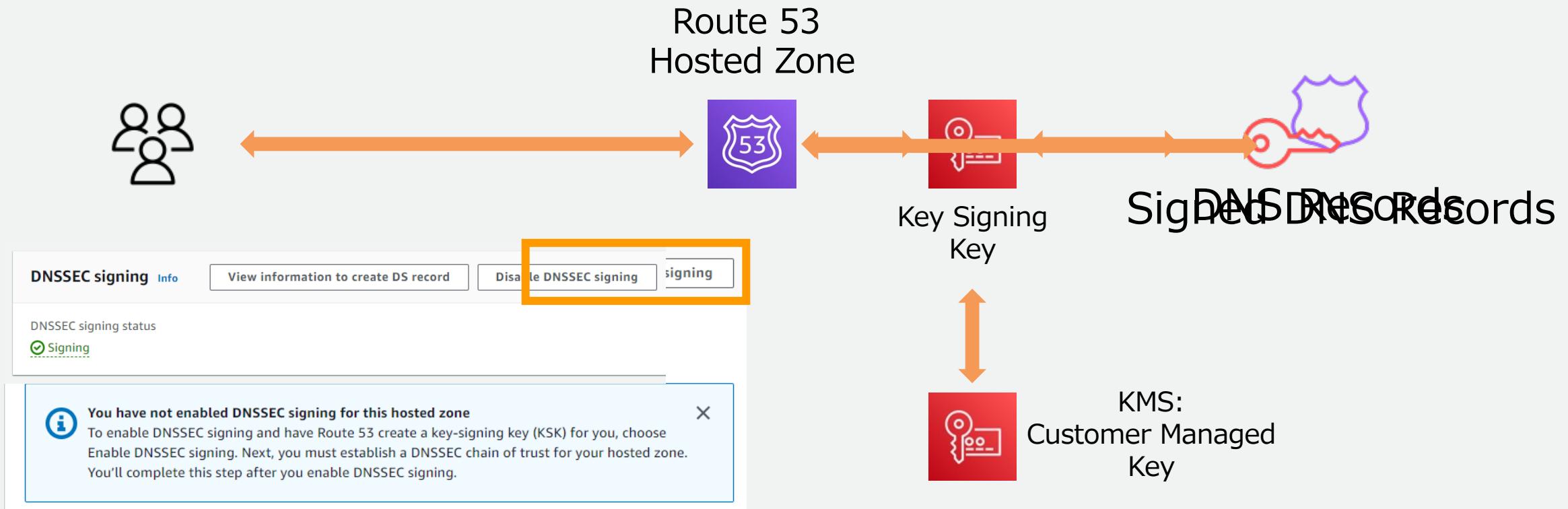
Amazon Route 53 サービスレベルアグリーメント
<https://aws.amazon.com/jp/route53/sla/>

Amazon Route 53 IPv6 support



- IPv6 エンドツーエンドのDNS
- IPv6 フォワード (AAAA) およびリバース (PTR) DNS レコードのサポート
- Route 53 ヘルスチェックは IPv6 エンドポイントのモニタリングをサポート

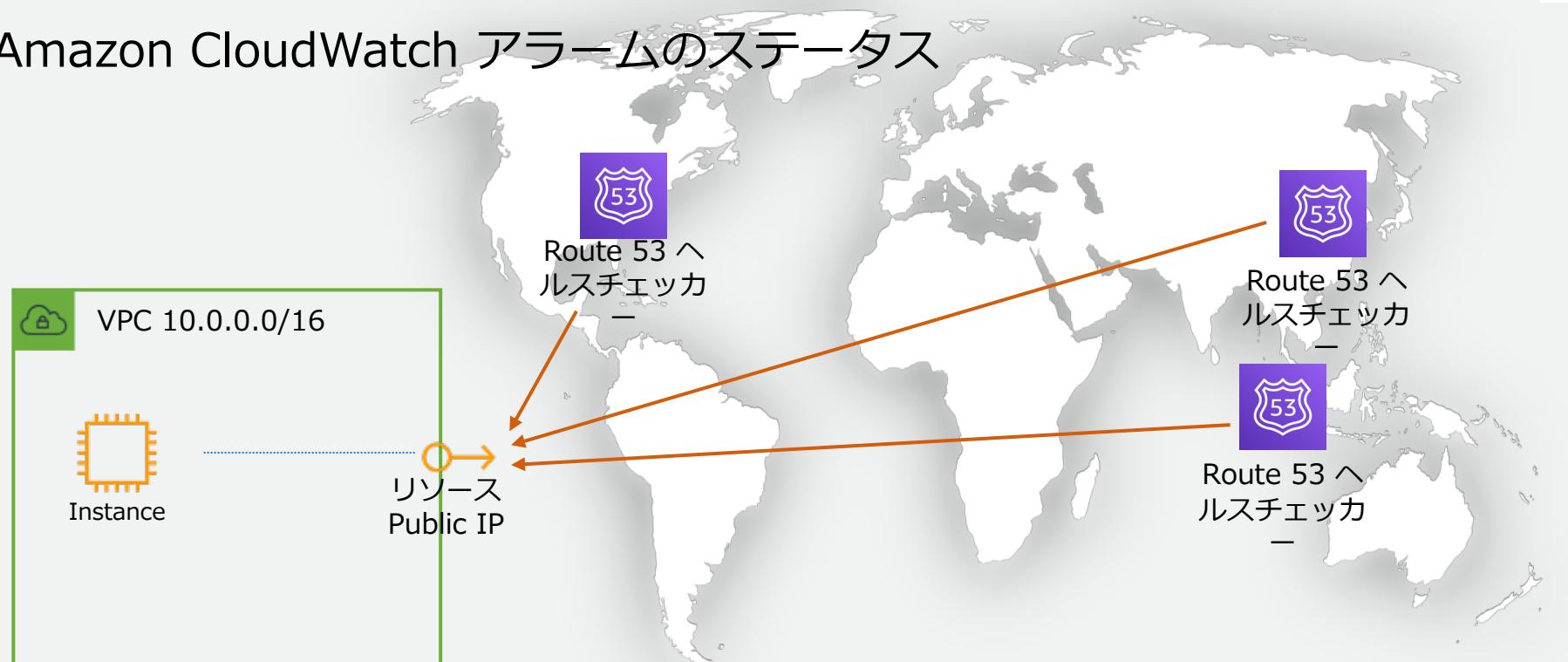
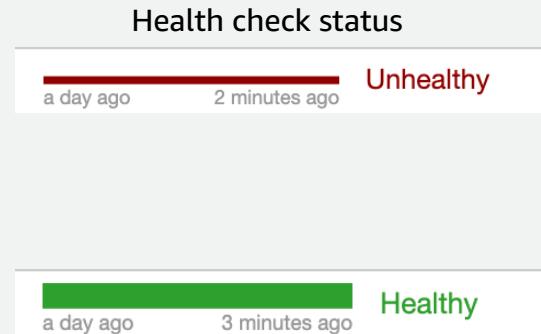
Amazon Route 53 での DNSSEC 署名



DNS 応答が Amazon Route 53 から送信され、DNS リゾルバーは改ざんされていないことを検証
DNSSEC 署名を使用すると、ホストゾーンへのすべての応答は、公開キー暗号化を使用して署名される

Amazon Route 53 ヘルスチェックとアラート

- ・ 指定されたリソースのヘルスチェック
- ・ その他のヘルスチェックのステータス
- ・ Amazon CloudWatch アラームのステータス



Route 53 よく利用されるレコードタイプ

- *ALIAS* – CNAMEを応答せず、最終的に必要とするレコードデータのみを応答
- *A Record* – IPv4 アドレスを応答
- *AAAA Record* – IPv6 アドレスを応答
- *CNAME Record* – *Canonical NAME* (正式名)を応答
- *MX Record* – 該当ドメインのメールサーバーのFQDNを応答
- *NS Record* – Hosted Zoneで指定されたネームサーバー
- *DS Records* – DNSSEC 委任レコードの指定に使用される

エイリアスレコード

- 問い合わせ元にCNAMEを応答せず、最終的に必要とするレコードデータのみを応答するAmazon Route 53固有の拡張機能
- CNAMEを利用しないことで、**Zone Apex**(サブドメインを含まないドメイン名)でサービスをホスト可能とする(例：<https://example.com>)
※エイリアスレコードの詳細な仕様はドキュメントを参照してください

CNAMEを用いた名前解決の応答例

www.example.com.	60	IN	CNAME	www-a.example.com.
www-a.example.com.	60	IN	CNAME	xxxx.cloudfront.net.
xxxx.cloudfront.net.	60	IN	A	192.0.2.3

最終的に必要とするレコードデータ

エイリアスを用いた名前解決の応答例

www.example.com.	60	IN	A	192.0.2.3
------------------	----	----	---	-----------

Agenda

1. Amazon Route 53 ドメインの登録
2. Amazon Route 53 Hosted Zone
3. トラフィックルーティング
4. ドメイン移行とテスト、トラブルシューティング
5. まとめ



トラフィックルーティング

トラフィックルーティング

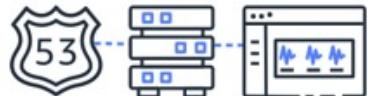
- DNSの応答をカスタマイズすることで、クライアントからのトラフィックをより適したリソースにルーティングする機能
- レコードの作成時に、Amazon Route 53 がクエリに応答する方法を決定するルーティングポリシーを選択

トラフィックルーティングポリシー

Amazon Route 53が提供するルーティングポリシー

- シンプルルーティング

すべてのクライアントが同じレスポンスを受信するようにする場合に使用します。



- フェイルオーバー

あるリソースが正常な場合にはそのリソースにトラフィックをルーティングし、そのリソースに異常がある場合には別のリソースにトラフィックをルーティングするときに使用します。



- 加重

同じジョブを実行する複数のリソースがあり、各リソース（例：2つ以上のEC2インスタンス）へのトラフィックの割合を指定する場合に使用します。



- レイテンシー

複数のAWSリージョンにリソースがあり、レイテンシーが最適なリージョンにトラフィックをルーティングする場合に使用します。



- IP ベース

CIDR表記でIPアドレス範囲の場所にトラフィックをルーティングするために使用します。



- 複数値回答

Route 53がDNSのクエリに対し、ランダムに選択された最大8つの正常なレコードを返すようにする場合に使用します。



- 位置情報

ユーザーの場所に基づいてトラフィックをルーティングする場合に使用します。



ルーティングポリシーの選択 - Amazon Route 53

https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/routing-policy.html



ルーティングポリシー：シンプル

- 従来のDNSと同様に、静的なマッピングによりルーティングが決定される
- 複数の値を 1 つのレコードに指定すると、すべての値をランダムな順序で応答（いわゆるDNSラウンドロビン）
- プライベートホストゾーンのレコードに使用可能

レコードセットの設定

名前	タイプ	値
www.example.com.	A	192.0.2.11 192.0.2.12 192.0.2.13

応答

名前	TTL	Type	Value
www.example.com.	60	IN	A 192.0.2.13
www.example.com.	60	IN	A 192.0.2.11
www.example.com.	60	IN	A 192.0.2.12

応答順序は都度ランダム



ルーティングポリシー：フェイルオーバー

- ヘルスチェックの結果に基づいて利用可能なリソースのみを応答する
- アクティブ / アクティブおよびアクティブ / スタンバイ構成を実現
- フェイルオーバー条件は、**複数のヘルスチェック結果**を結合するなどのカスタマイズが可能
- プライベートホストゾーンのレコードに使用可能

具体的なユースケース

複数リージョンにまたがるシステムで冗長構成

災害発生時にリージョン間でフェイルオーバー

障害時に、S3にホスティングした静的ウェブサイトのSorry Pageを表示

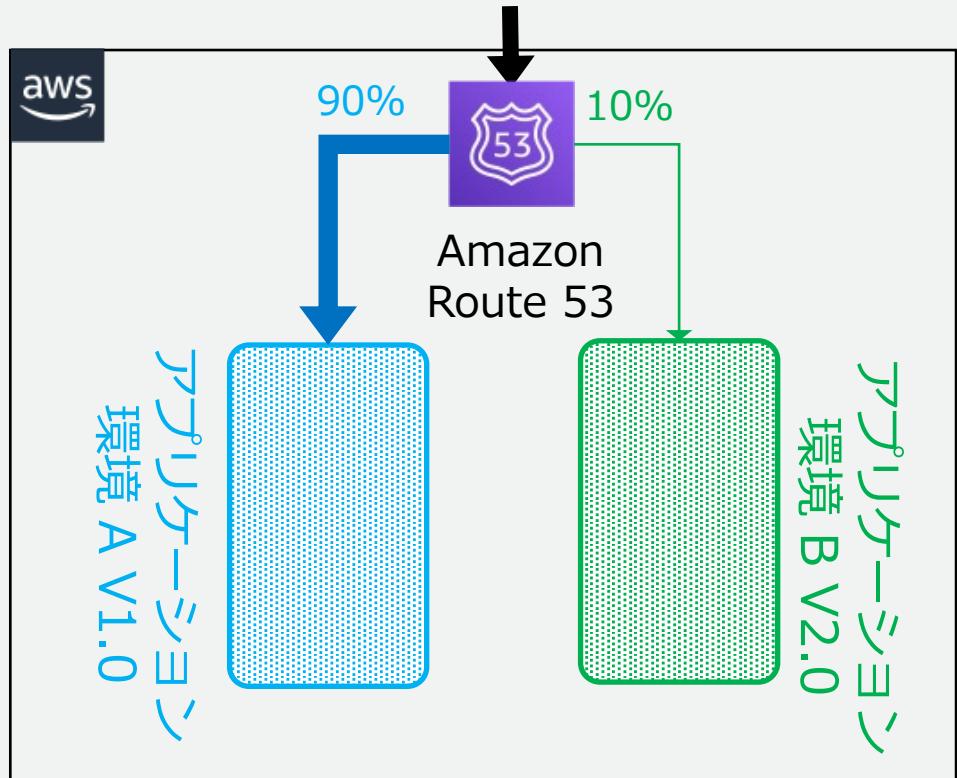


ルーティングポリシー：加重

- ・ 指定した比率で複数のリソースにトラフィックをルーティングする
- ・ より重み付けの高いリソースにより多くルーティングされる
- ・ プライベートホストゾーンのレコードに使用可能

具体的なユースケース

- ・ A/Bテスト、新しいバージョンのテスト
- ・ 段階的な移行(Blue/Greenデプロイ)
- ・ サーバー毎に性能の偏りがある場合の負荷平準化



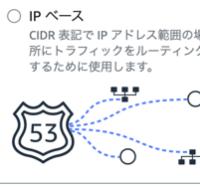


ルーティングポリシー：レイテンシー

- 複数の AWS リージョンでアプリケーションがホストされている場合、**ネットワークレイテンシー**が最も低い AWS リージョンのリソースを応答
- 一定期間中に実行されたレイテンシーの測定値に基づいており、時間の経過と共に変化する場合がある
- プライベートホストゾーンのレコードに使用可能

具体的なユースケース

ネットワークレイテンシーが最も低いリクエストを処理することで、ユーザーのパフォーマンスを向上させる



ルーティングポリシー：IPベース

- ユーザー IP からエンドポイントにマッピングする形で Route 53 にデータをアップロードする
- IP 範囲の管理とリソースレコードセット (RRSet) への関連付け

具体的なユースケース

- 特定の ISP から特定のエンドポイントにエンドユーザーをルーティング
 - 例：グローバルな動画コンテンツプロバイダーが、特定の ISP からのエンドユーザーをルーティング
- 位置情報ルーティングなど既存の Route 53 ルーティングタイプにオーバーライドを追加



ルーティングポリシー：複数値回答

- 最大 8 つのランダムに選択された正常なレコードで DNS クエリに応答
- 各リソースが正常かどうかを確認し、正常なリソースの値のみを応答
- 応答をキャッシュされた後にリソースが使用できなくなった場合にも、クライアントは応答内の別の IP アドレスを利用できる

これはロードバランサーに置き換わるものではありませんが、正常であることが確認できる複数の IP アドレスを返すことにより、DNS を使用してアベイラビリティーとロードバランシングを向上させることができる



ルーティングポリシー：位置情報

- ・ クライアントの位置情報に基づいて、DNSクエリに応答する
- ・ 特定の地域・国からのDNSクエリに対して、特定のアドレスを応答する
- ・ プライベートホストゾーンのレコードに使用可能。大陸別、国別、米国の州別に指定する

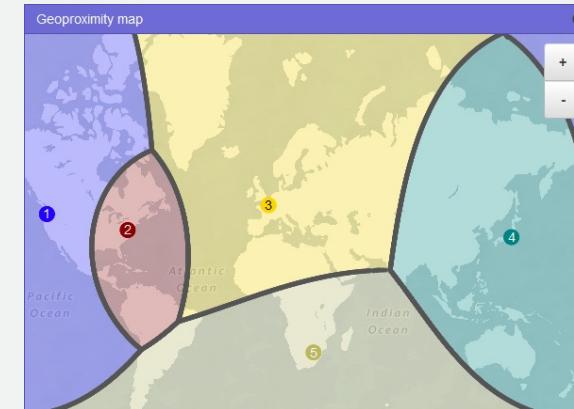
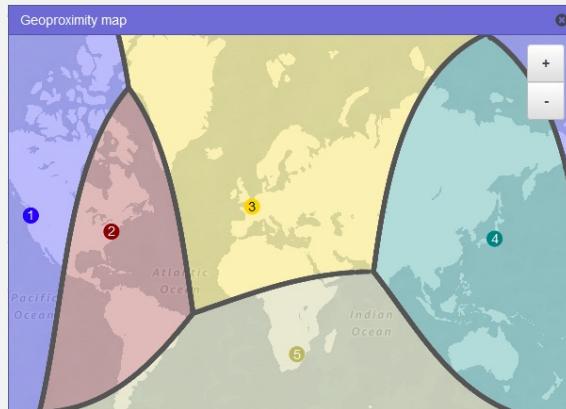
具体的なユースケース

クライアントの地域により適切な言語でコンテンツを提供

コンテンツのディストリビューションをライセンス許可した市場のみに制限する

ルーティングポリシー：地理的近接性

- ユーザーとリソースの地理的場所に基づいてDNSクエリに応答する
EDNS0 を使用してユーザーの場所を推定、EDNS0 の edns-client-subnet 拡張をサポート
- バイアスの値を指定して特定のリソースにルーティングするトラフィックの量を変更する
- 地理的近接性ルーティングを使用するには、トラフィックフロー（後述）を使用する必要がある

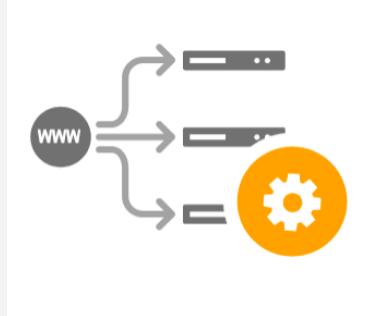


プライベートホストゾーンのレコードに使用できません。

https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/routing-policy-geoproximity.html

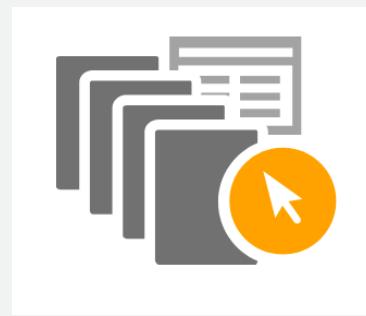
トラフィックフロー

ポリシーベースのトラフィックルーティングを、簡単に作成・管理できる機能



ビジュアルエディタ

直観的なビジュアルエディタを使用して複雑な設定を作成し、これをトラフィックポリシーとして保存。



トラフィック ポリシーバージョン

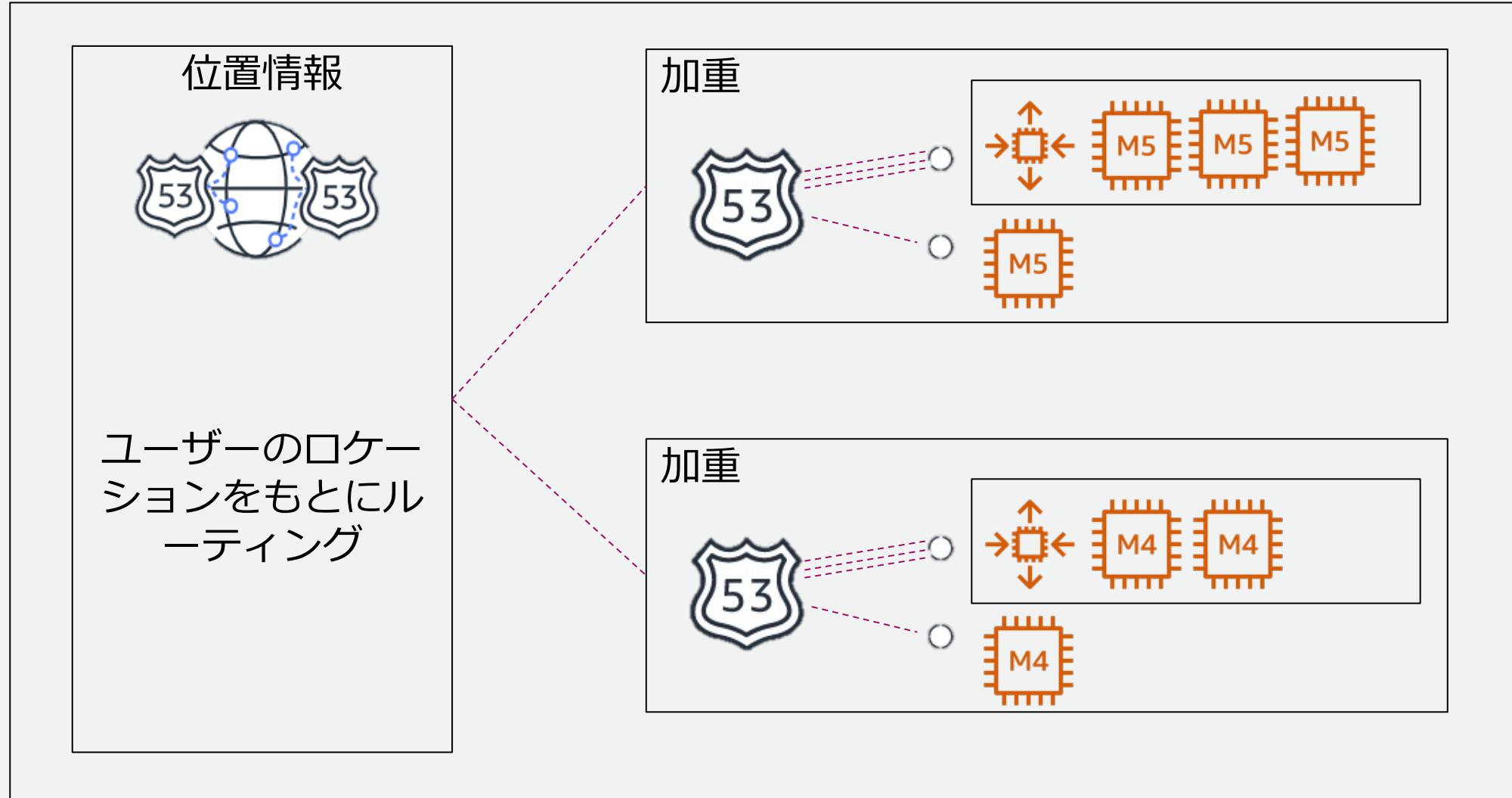
1つのトラフィックポリシーの複数のバージョンを作成して、バージョニングを使用してアップデートの適用あるいは不適用を行う。



ポリシーレコード

ポリシーレコードを作成して、トラフィックポリシーをドメインあるいはサブドメイン名に関連付ける。

Route 53 高度なトラフィックポリシー



さらなる応用

- Amazon Route 53 では、AWS CLIやAWS SDKやAWS CDKを用いてゾーンやレコードの操作が可能
- Amazon Route 53が機能として備えていないロジックをユーザーが作成し、実装することが比較的容易
- AWS Lambdaはこれらロジックの実行環境として良い選択肢



Agenda

1. Amazon Route 53 ドメインの登録
2. Amazon Route 53 Hosted Zone
3. トラフィックルーティング
4. ドメイン移行とテスト、トラブルシューティング
5. まとめ



移行とテスト、トラブルシューティング



ネームサーバーの移行

- 適切な手順に則って作業すれば移行は難しくない
- 陥りがちな移行トラブルを未然に防ぐため、下記ドキュメントの熟読を推奨

DNSサーバーの引っ越し～トラブル発生を未然に防ぐ手順とポイント～,
株式会社日本レジストリサービス, 2015
<https://jprs.jp/related-info/guide/019.pdf>

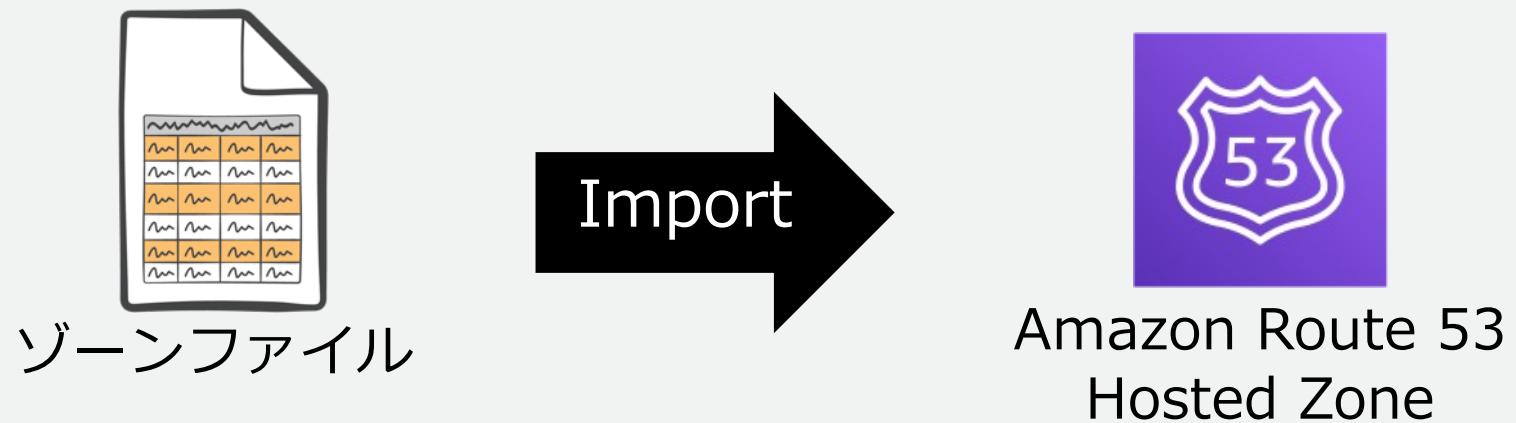
ネームサーバーをAmazon Route 53に移行する際の代表的なタスク

- Amazon Route 53 Hosted Zone を構成する
- ネームサーバーに関連するリソースレコードのTTLを短縮する
- DNSSEC を無効にする
- 親ゾーンと子ゾーンでDelegation(権限委譲) の設定を変更する
- 旧ネームサーバーの廃止、DNSSEC を有効にする



Amazon Route 53 Hosted Zoneを構成する

- RFC1034, 1035形式のゾーンファイルをインポートしてHosted Zoneを構成できる
- \$GENERATEなど一部仕様はサポートしていない、必要に応じて AWS CLI / AWS SDKを利用



TTL の短縮

- ・ 作業開始前に該当するTTL 値の短縮が可能な場合
 - ・ネームサーバーの切り替えに要する時間を短縮できる
 - ・万が一、移行作業に失敗した場合の「切り戻し」の時間も短縮される
- ・ 移行作業、切り戻しの時間を考慮し60秒～3600秒程度に短縮することが多い

example.com.	86400	IN	NS	ns1.example.com.
ns1.example.com.	3600	IN	A	192.0.2.1

あるいは

短縮

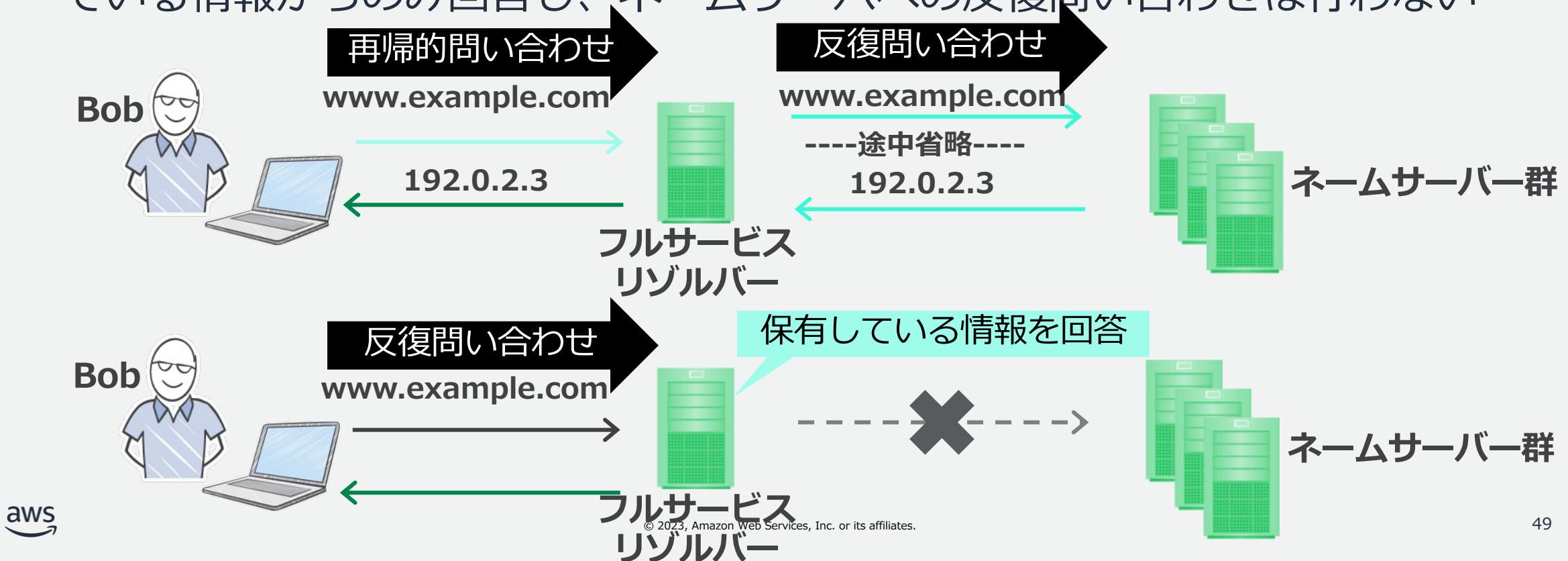
ns1.example.com.	300	IN	A	192.0.2.1
example.com.	300	IN	NS	ns1.example.com.

テストとトラブルシューティング

- ネームサーバーやフルサービスリゾルバー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)
- 原因はどこか? ドメインか? ネームサーバー (Hosted Zone) か? フルサービスリゾルバーのキャッシュか? を特定する
 - キャッシュの有無、再帰的問い合わせと反復問い合わせを識別しながら試行すると問題箇所を特定しやすい
 - 出力情報やオプションが豊富な dig コマンドが有用

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、問い合わせ先に名前解決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からのみ回答し、ネームサーバへの反復問い合わせは行わない



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 @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

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 192.0.2.3

;; 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つた
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>



複数地点からの確認

- ・ インターネット上の複数のフルサービスリゾルバーから確認を行うことで、移行後の正常性確認を確実にできる
- ・ Public DNSの活用は、これを手軽に行うための選択肢のひとつ



【参考】Public DNS Server List
<https://public-dns.info/>

Amazon Route 53 DNS のベストプラクティス

DNS フェイルオーバーとアプリの回復にデータプレーン機能を使用

Route 53 のデータプレーンは、グローバルに分散されて、重大なイベント中でも 100% の可用性と機能性を実現するように設計されている

DNS レコードの TTL 値の選択

レイテンシーと信頼性、および変化に対する応答性と間のトレードオフ。

DNS の委任

DNS で複数のレベルのサブドメインを委任する場合、常に親ゾーンから委任することが重要

DNS レスポンスのサイズ

大きなシングルレスポンスの作成は避ける。

ほかのはドキュメントをご参照ください。

https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/best-practices-dns.html

© 2023, Amazon Web Services, Inc. or its affiliates.



Agenda

1. Amazon Route 53 ドメインの登録
2. Amazon Route 53 Hosted Zone
3. トラフィックルーティング
4. ドメイン移行とテスト、トラブルシューティング
5. まとめ



まとめ



まとめ

Amazon Route 53 にてドメイン新規登録、移管とDNSのネームサーバー機能を提供するAmazon Route 53 Hosted Zoneについて解説しました。

本資料に関するお問い合わせ・ご感想

技術的な内容に関しては、有料のAWSサポート窓口へ
お問い合わせください

<https://aws.amazon.com/jp/premiumsupport/>

料金面でのお問い合わせに関しては、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）

<https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service>

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください



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



その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

<https://aws.amazon.com/jp/events/>

ハンズオンコンテンツ

<https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/>

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

<https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html>



Thank you!