AWS Black Belt Online Seminar

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

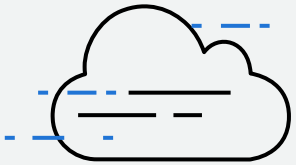
Amazon Route 53 の特徴

可用性が高く、コスト効率に優れた DNS Webサービス

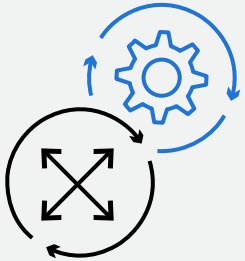
高速な名前解決

高いコスト効率

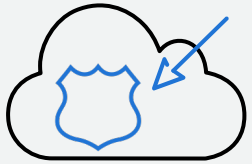
セキュア



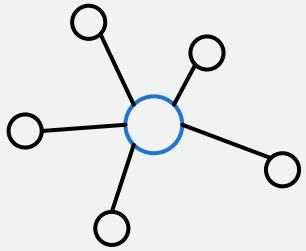
高可用性



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

Hosted Zone

DNS リゾルバー

Resolver

Resolver DNS Firewall

Disaster recovery

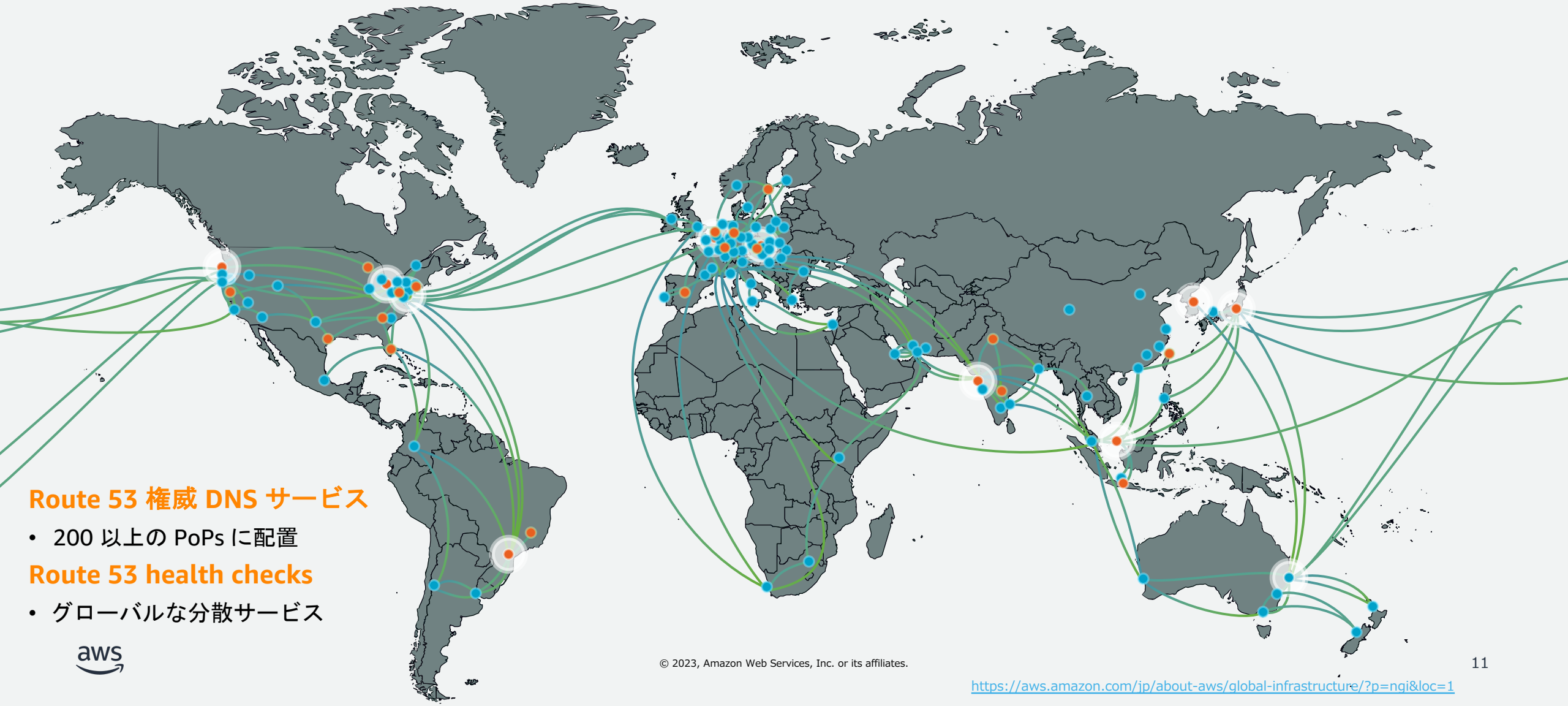
Application Recovery Controller

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



Route 53 権威 DNS サービス

- 200 以上の PoPs に配置

Route 53 health checks

- グローバルな分散サービス

https://aws.amazon.com/jp/about-aws/global-infrastructure/?p=ngi&loc=1

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

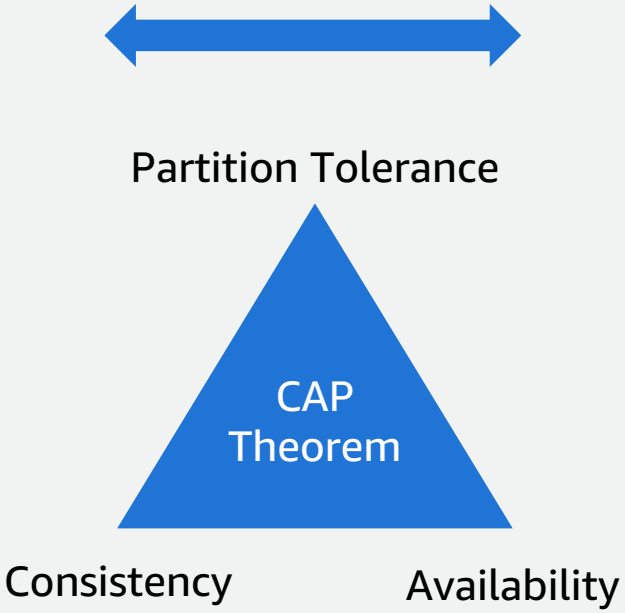
コントロールプレーン

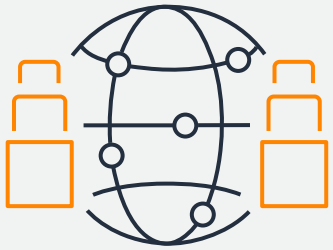
データの一貫性を重視した設計

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)

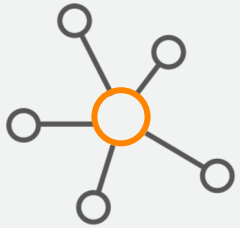
Route 53 ではグローバルに分散

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	機能: Route 53 コンソール API Location: us-east-1	機能: Route 53 コンソール API (ヘルスチェックの CRUD 操作) Location: us-east-1	機能: 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) Location: リージョンごと	機能: Route 53 コンソール API (ドメイン登録) Location: us-east-1
データプレーン	機能 権威 DNS サービス Location: グローバルに分散	機能: ヘルスチェック Public/Private DNS サービスへの集約結果の送信 Location: グローバルに分散	機能: DNS フォワーディング DNS 再帰クエリ Location: 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

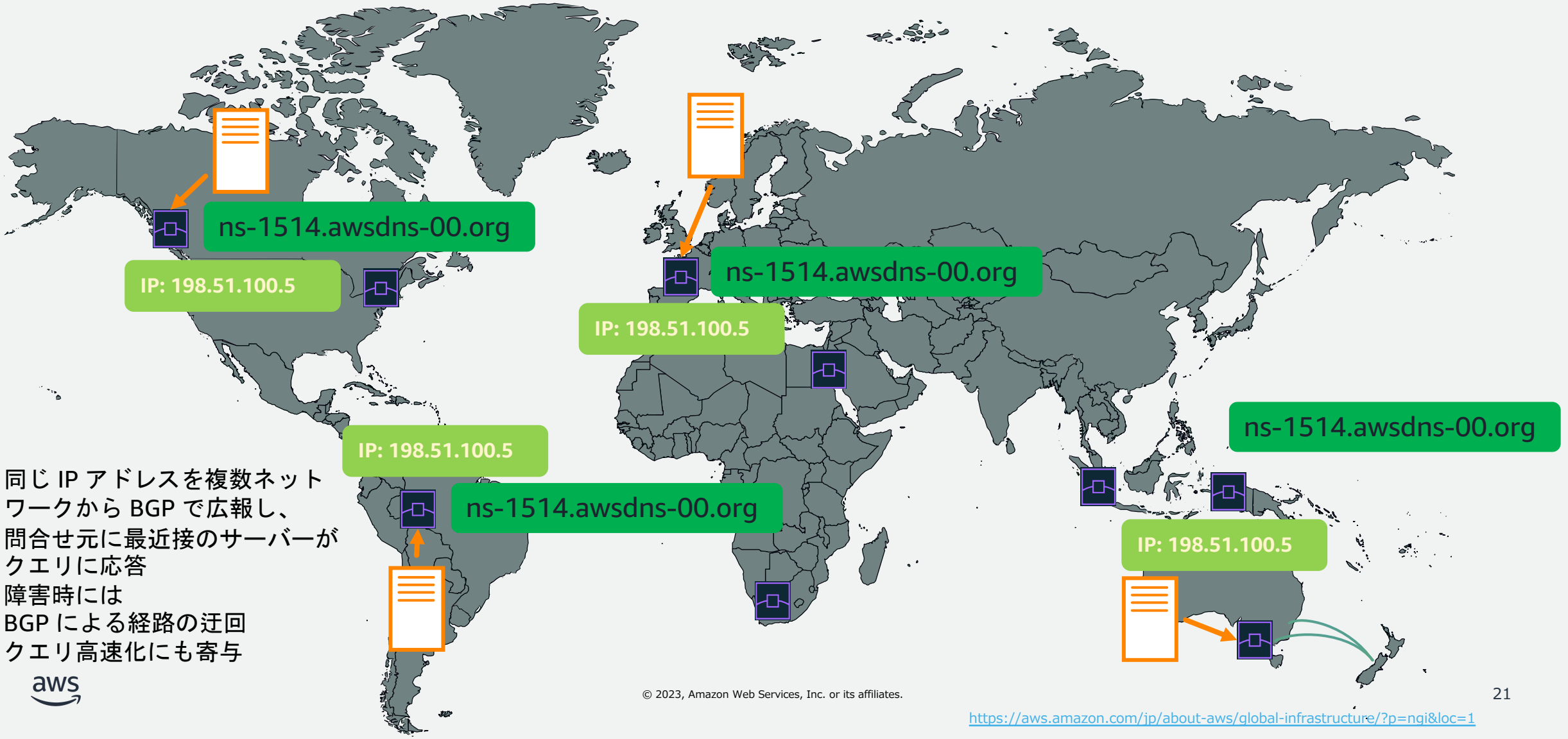
全てのお客様に低コストで
サービスを提供する必要性

➢ 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



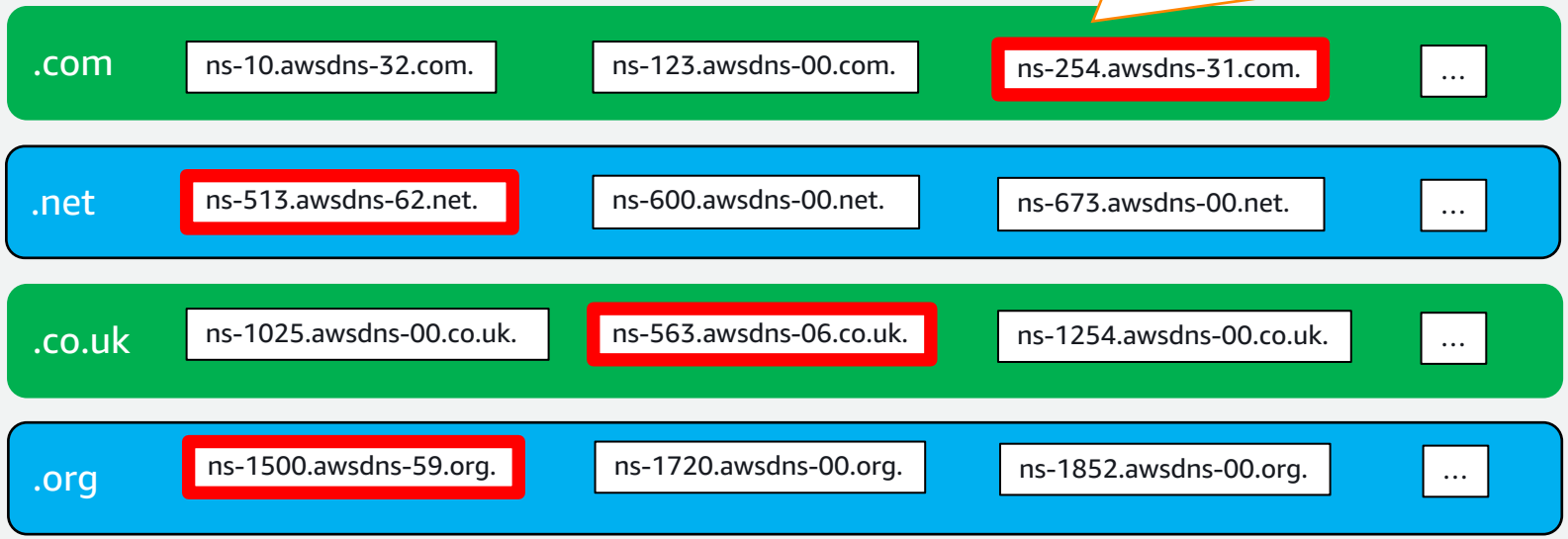
- 同じ IP アドレスを複数ネットワークから BGP で広報し、問合せ元に最近接のサーバーがクエリに応答
- 障害時には BGP による経路の迂回
- クエリ高速化にも寄与

https://aws.amazon.com/jp/about-aws/global-infrastructure/?p=ngi&loc=1

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



example.com

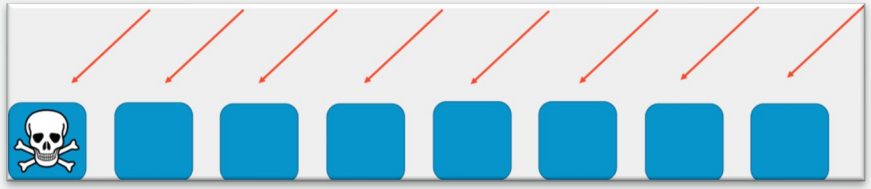
レコード名	値/トラフィックのルーテ...	TTL (秒)
example.com	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.	172800
example.com	ns-1536.awsdns-00.co.uk. a...	900

- 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

https://aws.amazon.com/jp/blogs/architecture/a-case-study-in-global-fault-isolation/

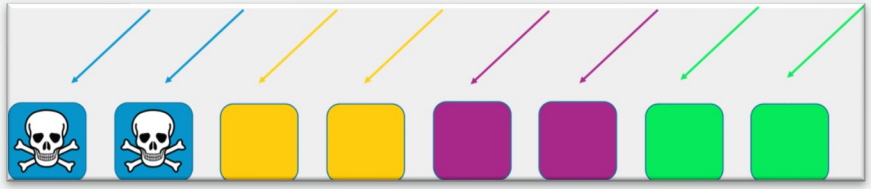
SLA 100 % のための設計 – Shuffle Sharding

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



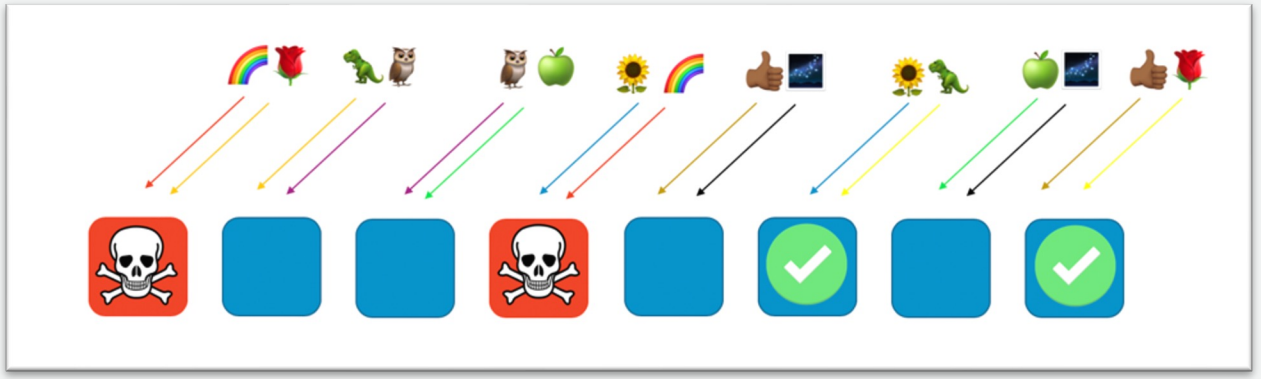
DNS クエリに対応するワーカーがクエリに均等に対応する場合、DDoS など大量リクエストの攻撃の影響は時間と共に影響が拡大してしまう

シャーディング



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 % とする関連技術をご紹介
  - IP Anycast
  - Name server stripes
  - Shuffle Sharding

Amazon Route 53 の機能

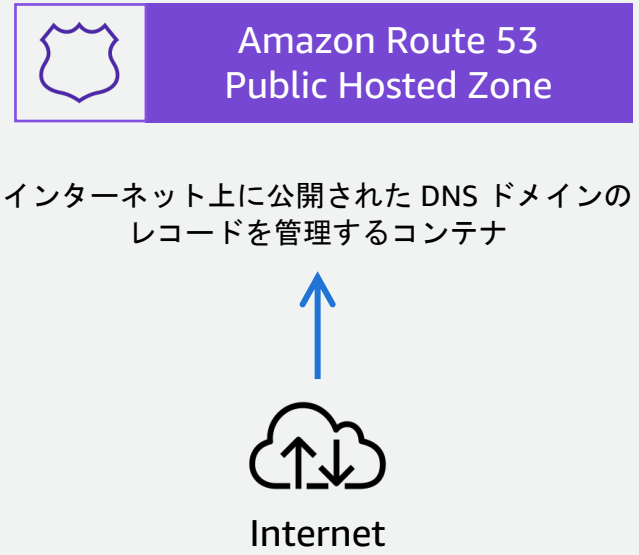
Amazon Route 53 ドメイン登録

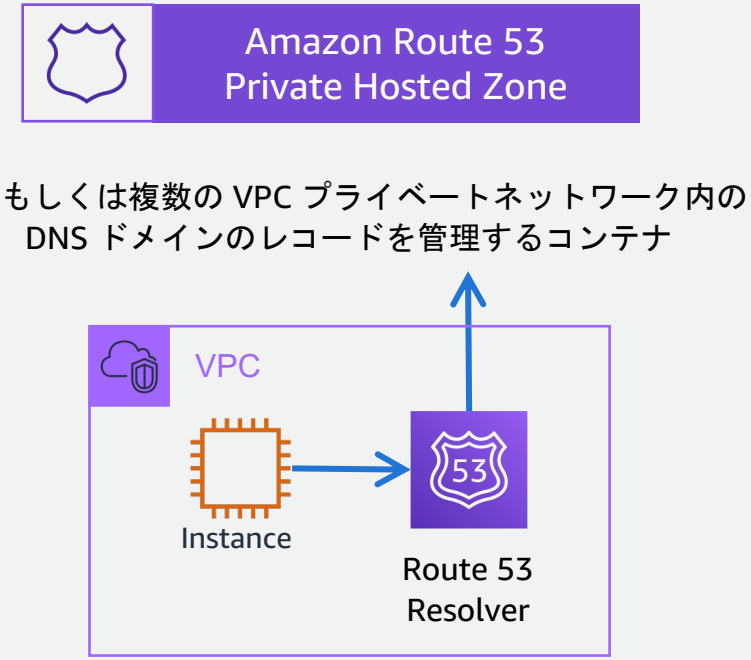
- Amazon Route 53 はリセラーとしてドメイン登録が可能
  - レジストラは Gandi SAS、Mesh Digital Limited、Amazon Registrar, Inc
  - https://aws.amazon.com/route53/domain-registration-agreement/?nc1=h_ls
- 他のレジストラから Amazon Route 53 下での管理に移管、その逆も可能
- 登録ドメインのプライバシー保護が利用可能

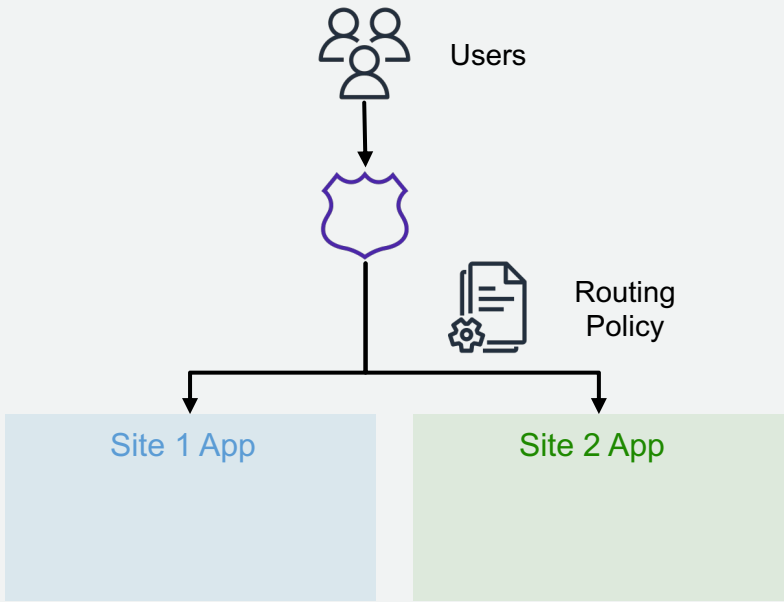
- ドメイン登録料金はドキュメントをご参照ください

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

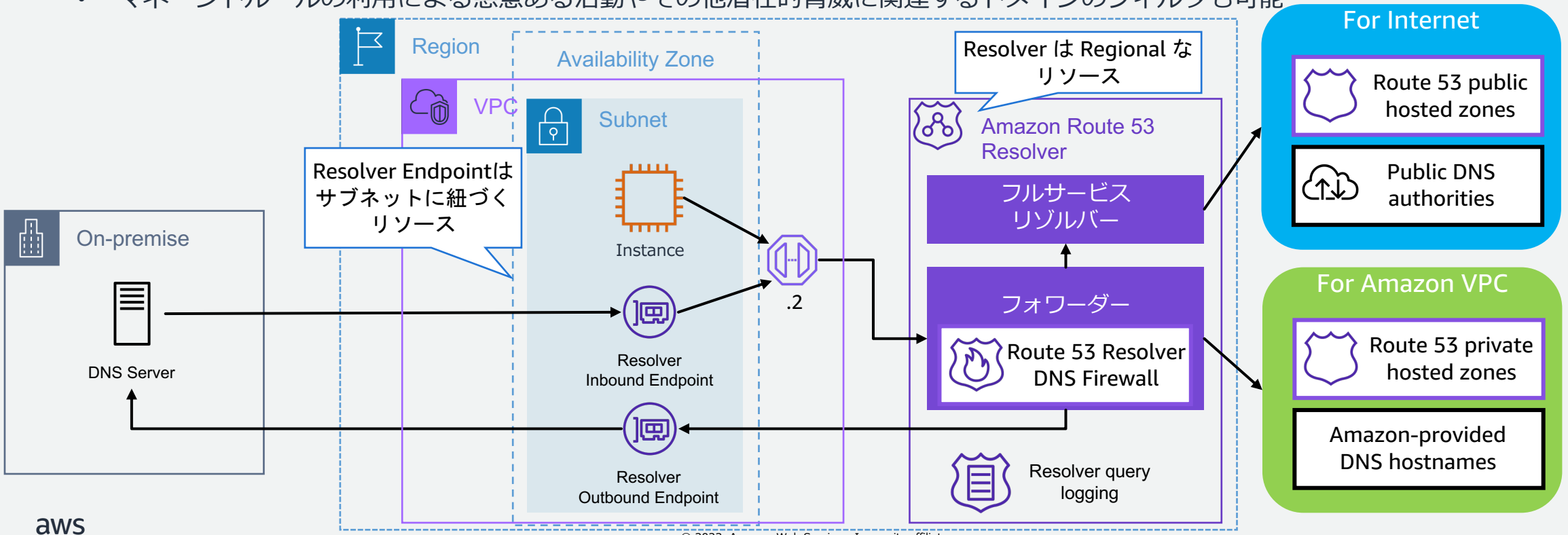






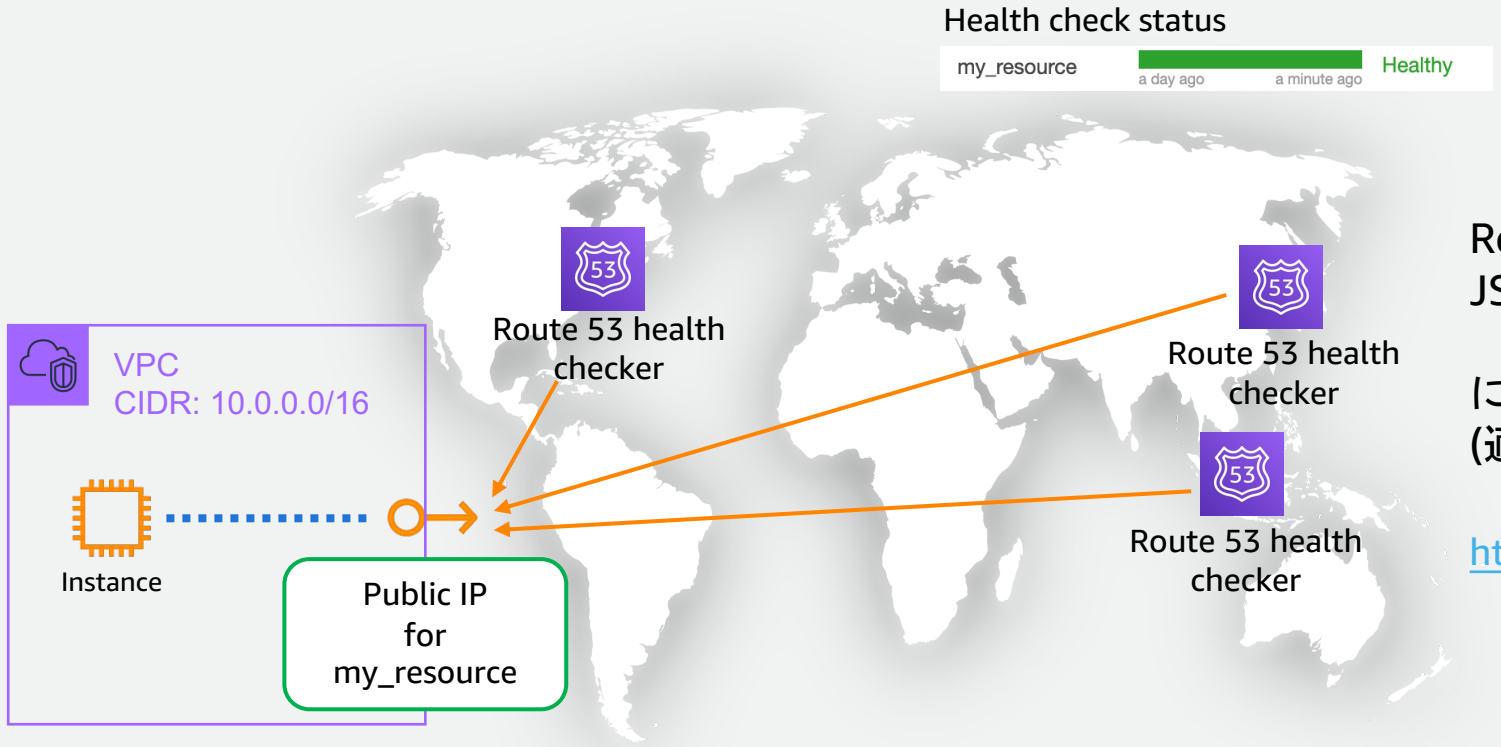
Amazon Route 53 Resolver (別名: AmazonProvidedDNS, VPC+2 Resolver)

- 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
  - マネー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連するドメインのフィルタも可能



Amazon Route 53 Health check

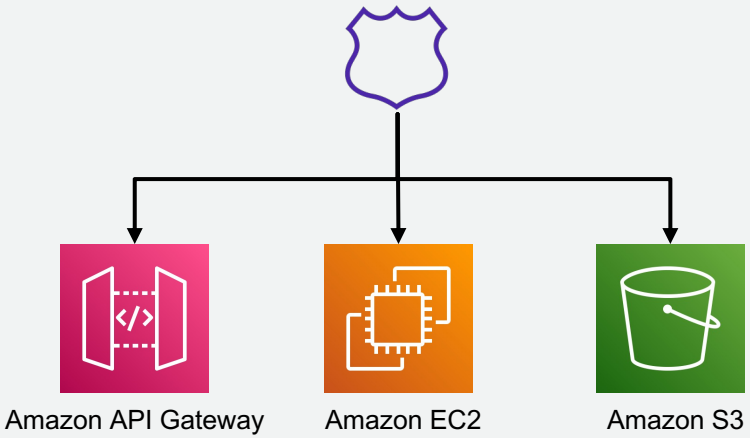
- Edge location 上のサーバーからヘルスチェックを実施できる
- エンドポイント、計算結果、Amazon CloudWatch アラームなど複数種類のヘルスチェックが可能
- フェールセーフ設計によりヘルスチェックの不備時にもシステム稼働を持続させる仕組み



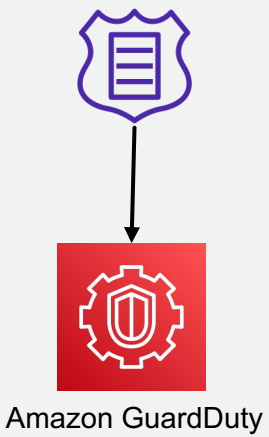
Route 53 ヘルスチェッカーは以下リンクの JSON 中で
“service”: “ROUTE53_HEALTHCHECKS”
に記載の IP アドレスから発信される
(適宜ファイアウォールにルール設定)

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

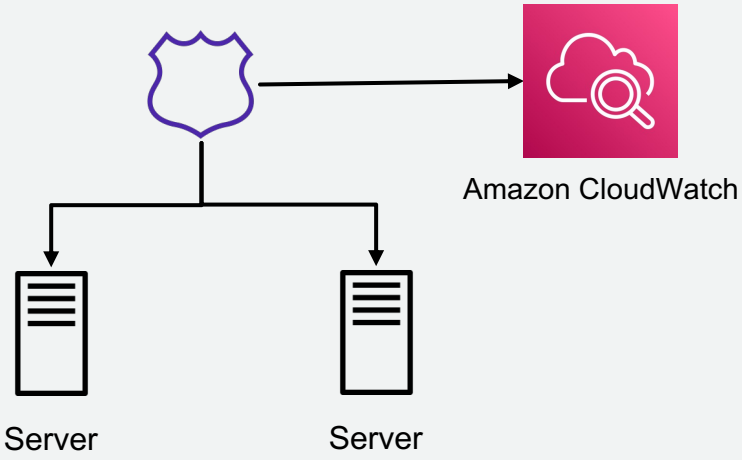
Amazon Route 53 – AWS Service 統合の例



Alias レコードによる
AWS リソースへの
ルーティング



セキュリティサービス連携
による脅威検知



CloudWatch 連携による
柔軟なヘルスチェック

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.

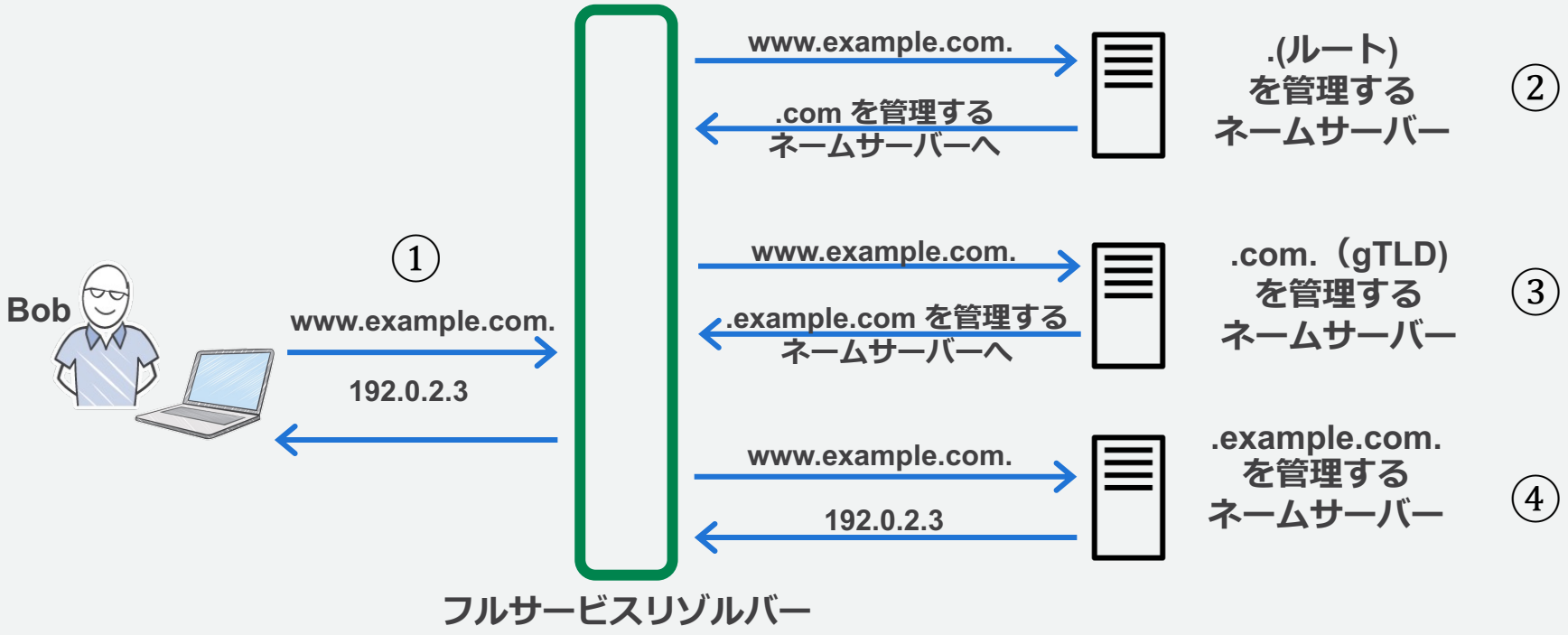
※ルートは「.」で表されるため、 狭義の意味での FQDN を表記する際には、末尾の「.」まで含めて表記する

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 .net .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

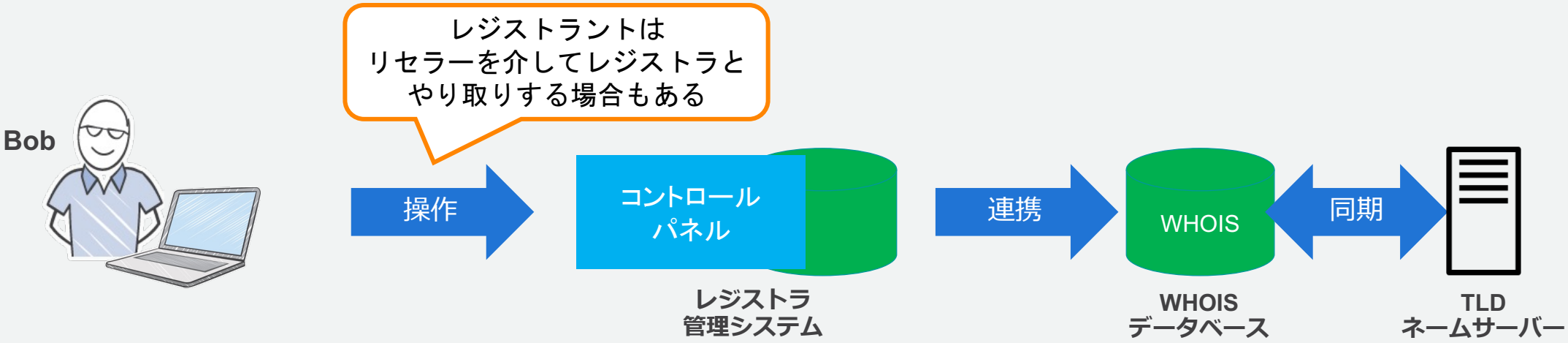
ドメイン名を登録し、使用するユーザー

レジストラ
登録取次事業者

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

レジストリ
登録管理機関

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

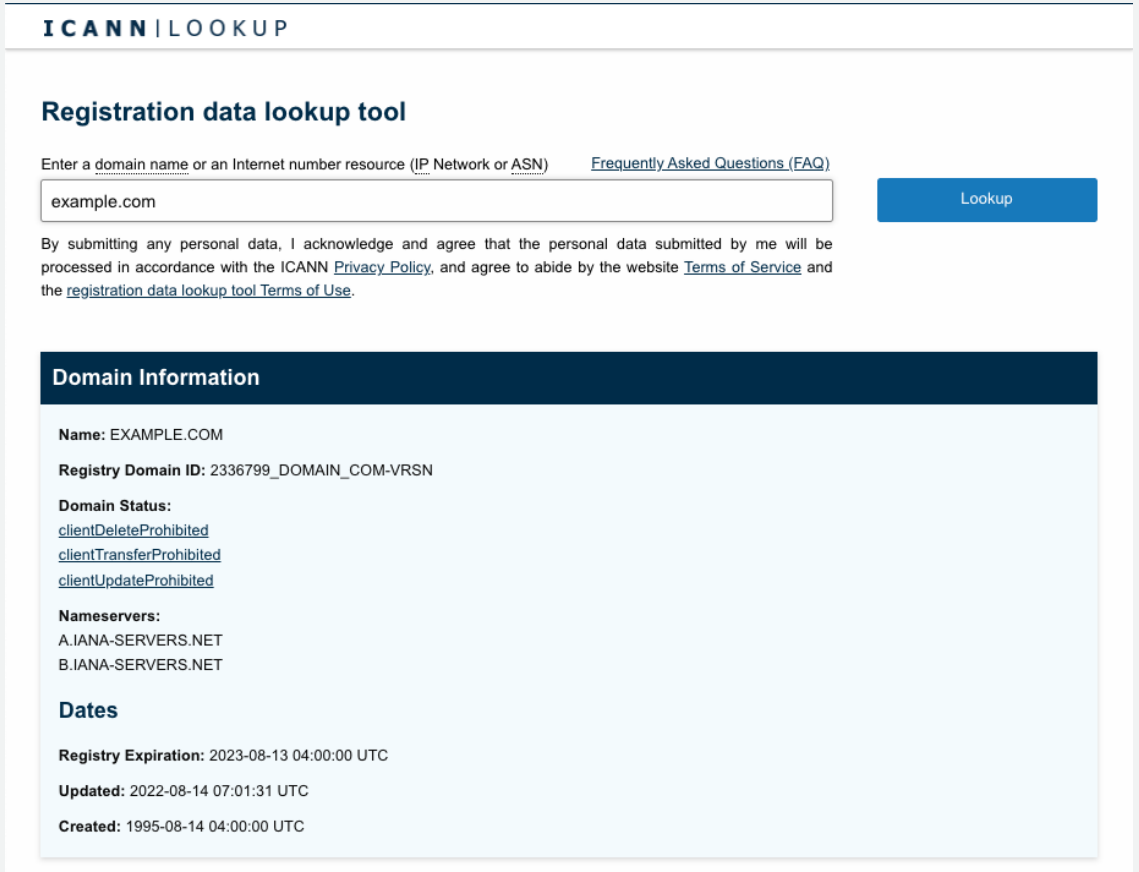


WHOIS データベース

- 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



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

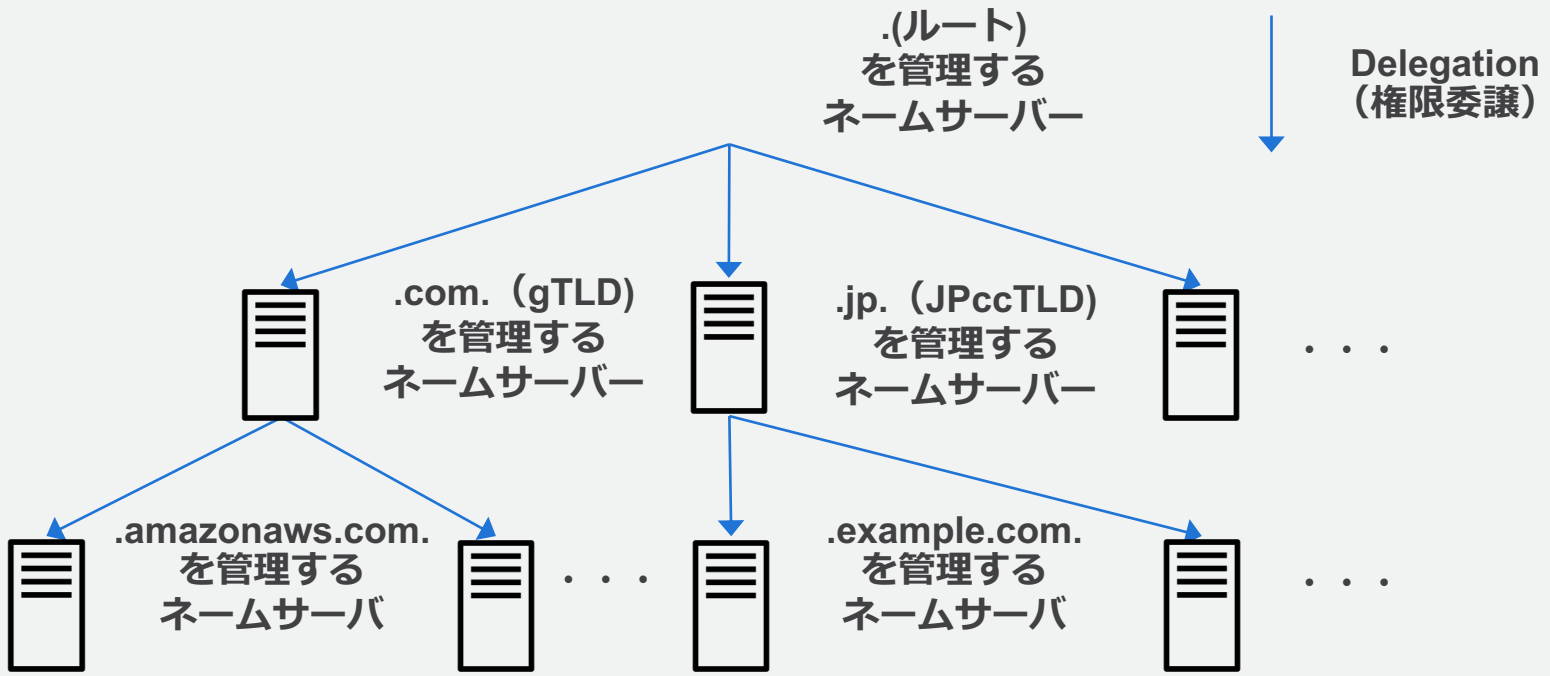
ドメイン名の基礎 まとめ

- 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

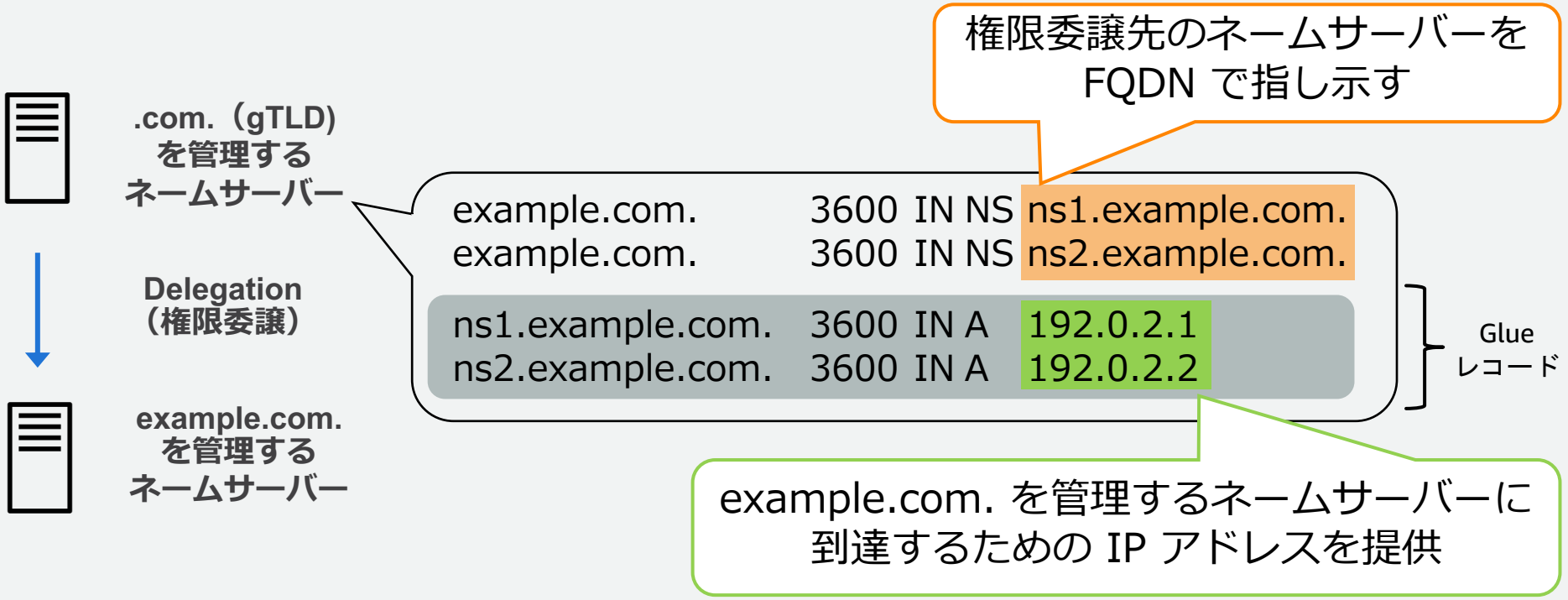
ネームサーバー(権威 DNS サーバー/Authoritative Server)

- .(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 で指し示すことで権限を委譲
- 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し示す（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	
example.com.	3600	IN	MX	10 mx1.example.com.	RRSet
example.com.	3600	IN	MX	20 mx2.example.com.	

※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)

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
- ゾーンの管理に関わる情報（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 の動作に関わる設定が含まれる

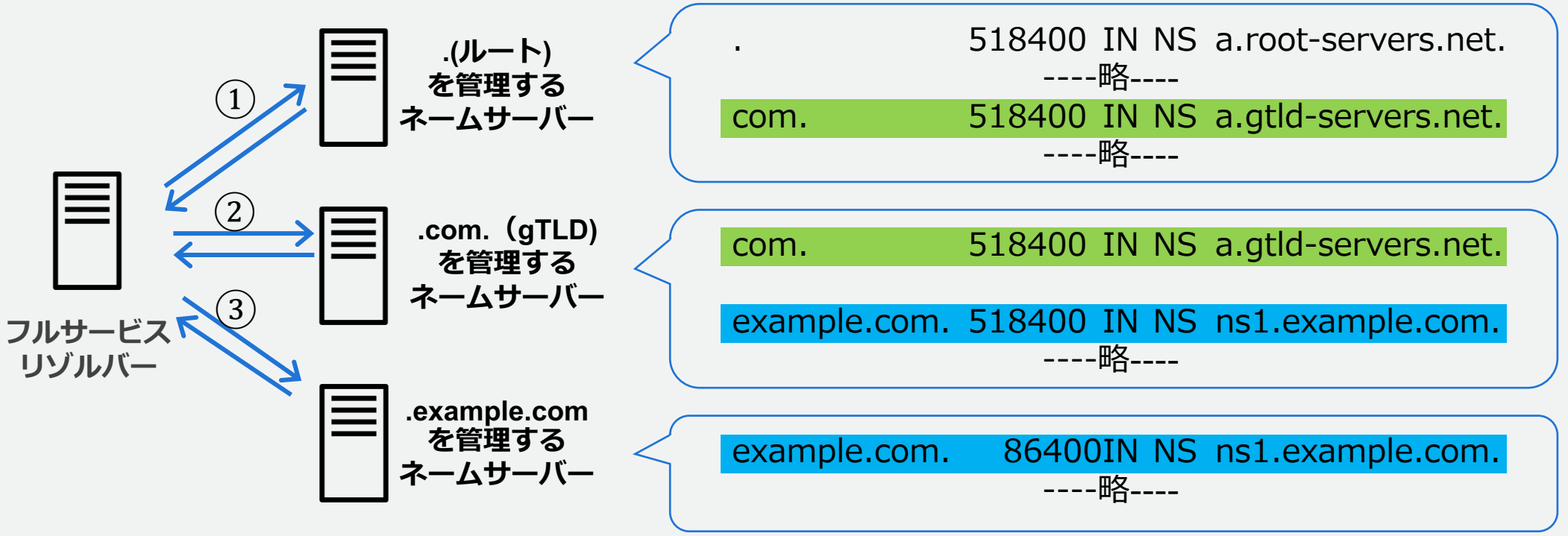
example.com. ゾーン

```
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し示す NS レコード

- ゾーンを管理するネームサーバーの FQDN を指し示す
- 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

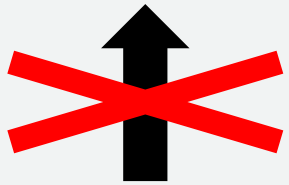
CNAME レコードの制約と Zone Apex

- 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)

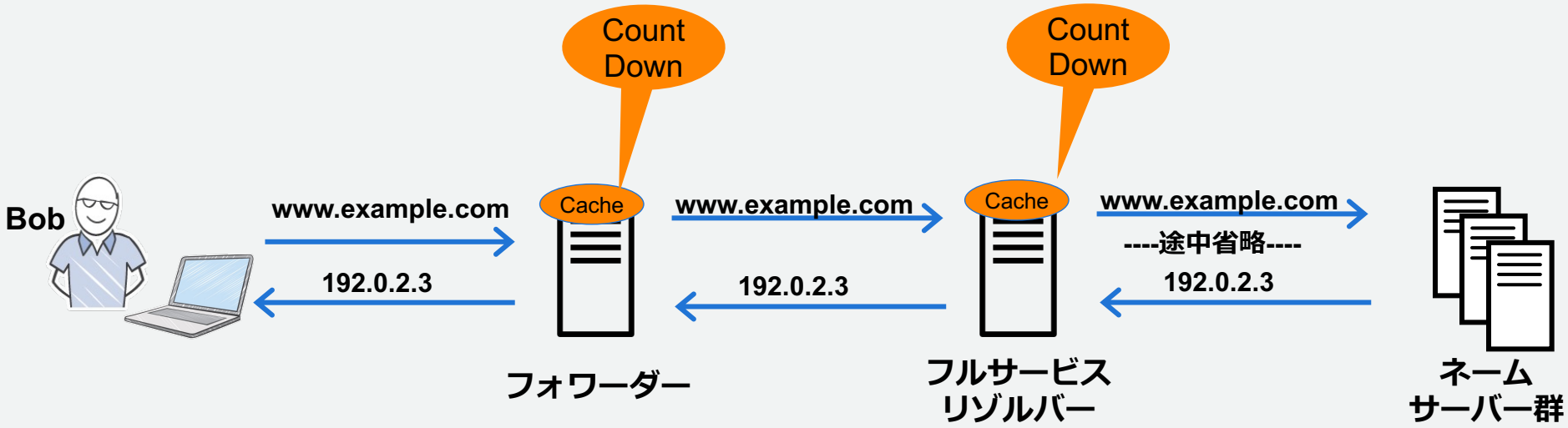
192.0.2.3 を逆引きする名前	3.2.0.192.in-addr.arpa.
2001:0DB8::1 を逆引きする名前	1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 .0.0.0.8.b.d.0.1.0.0.2.ip6.arpa

- 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

3.2.0.192.in-addr.arpa.	3600	IN	PTR	www.example.com.
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa.	3600	IN	PTR	www.example.com.

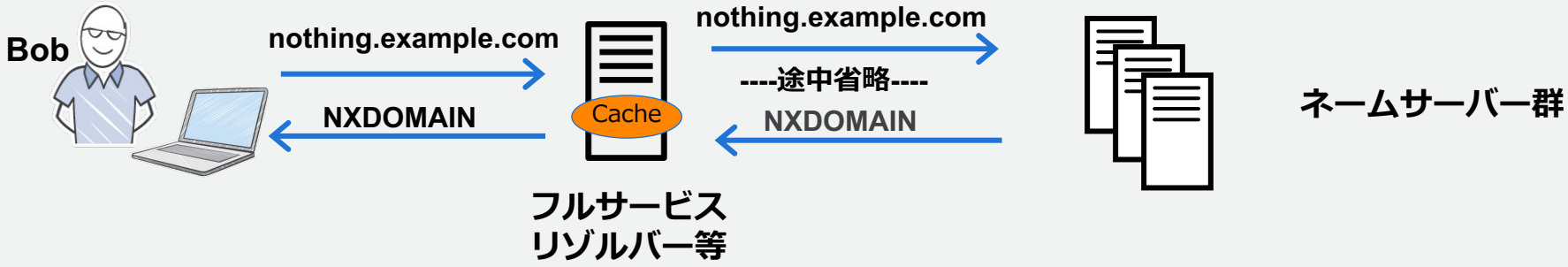
キャッシュ時間を定める TTL

- 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無く、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



example.comゾーン

ネガティブキャッシュTTL値

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

※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

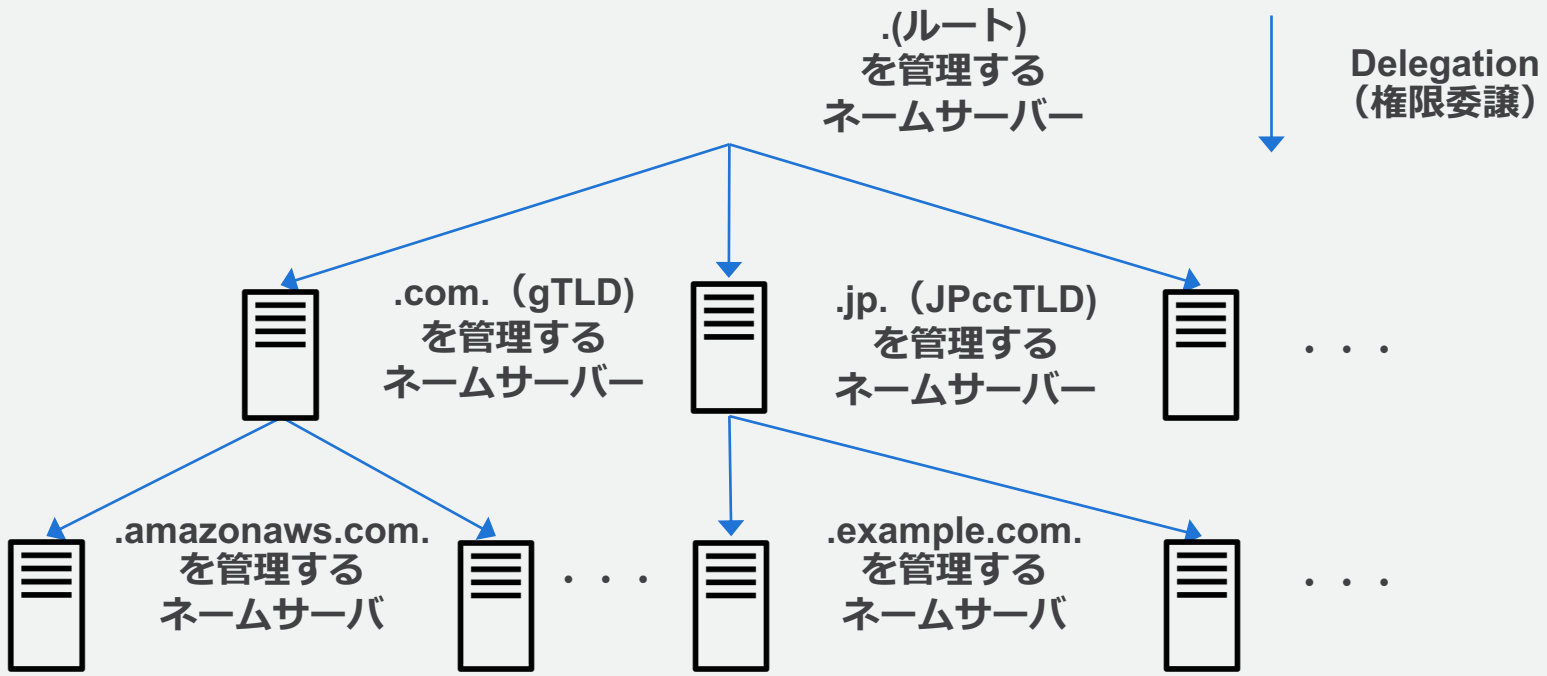
② フルサービスリゾルバー/ Full Service Resolver (キャッシュ DNS サーバー)

③ スタブリゾルバー/ Stub Resolver

④ フォワーダー / Forwarder

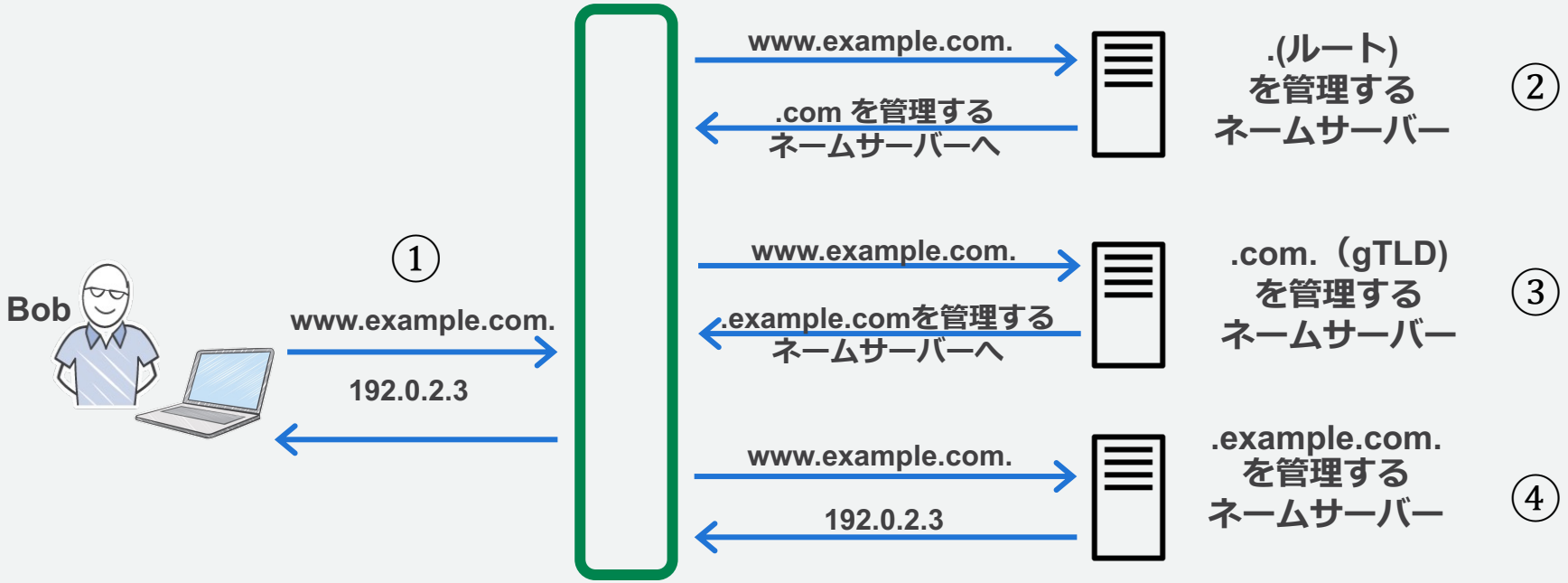
(再掲)ネームサーバー(権威 DNS サーバー/Authoritative Server)

- .(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)

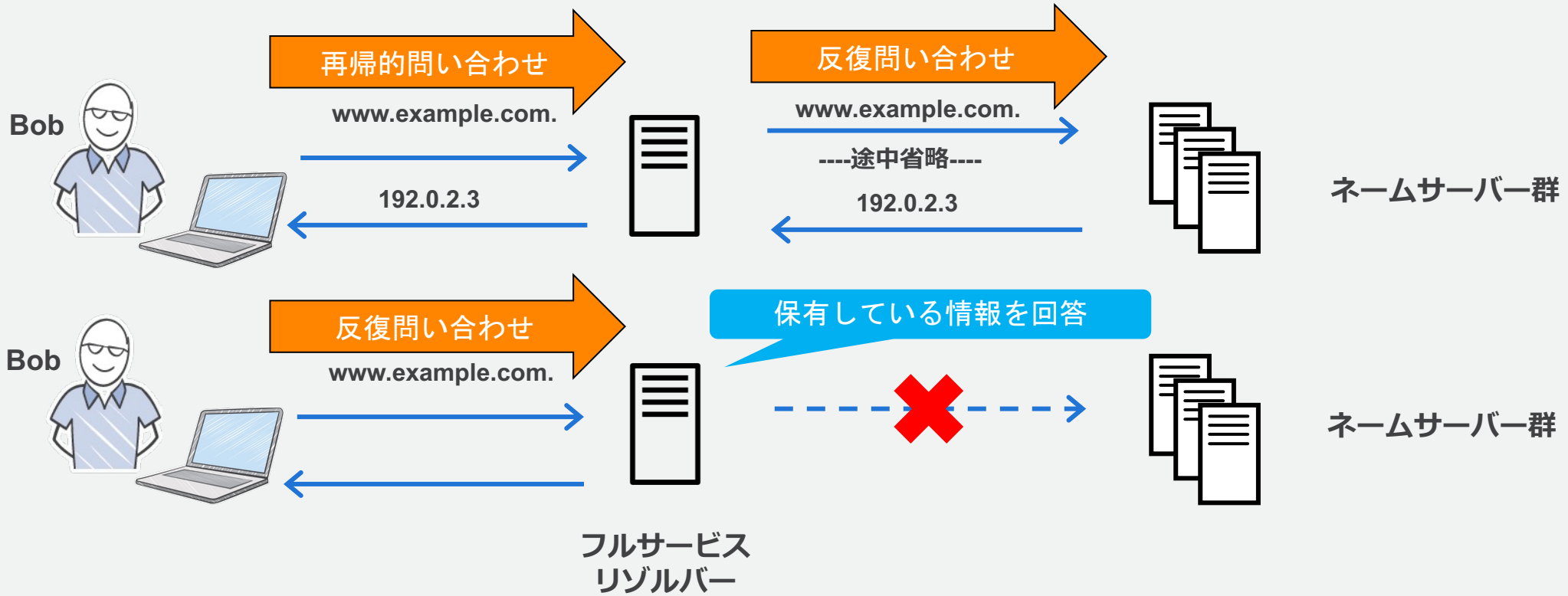
- .(ルート）から順にネームサーバに問い合わせ、得られた回答を問い合わせ元に返す機能を有するサーバー実装
- 効率化のため所定の期間（TTL）キャッシュを保持する



フルサービスリゾルバー

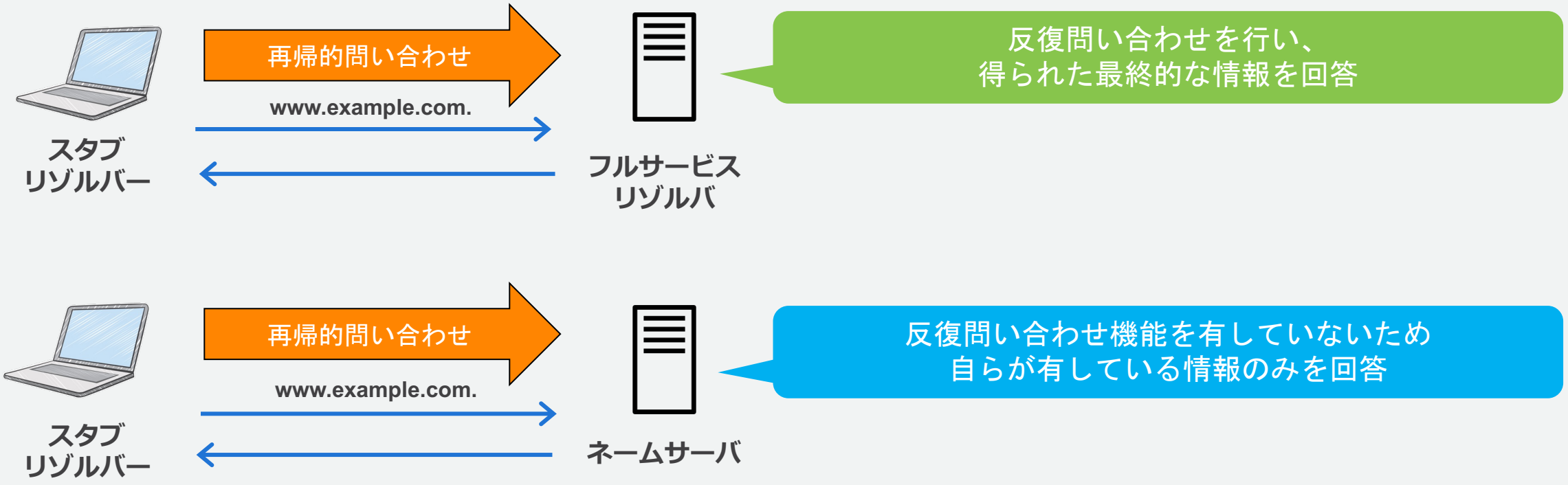
再帰問い合わせと反復問い合わせ

- 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



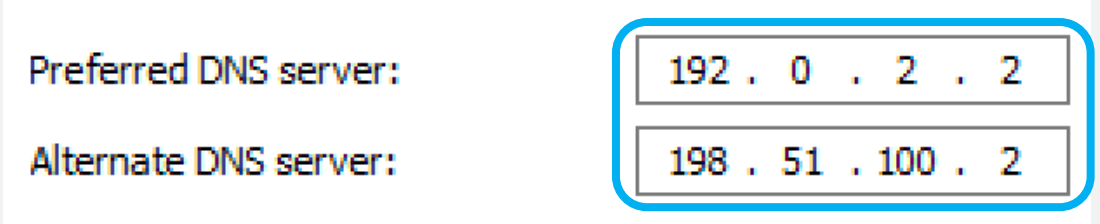
スタブリゾルバーの制約

- 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
```

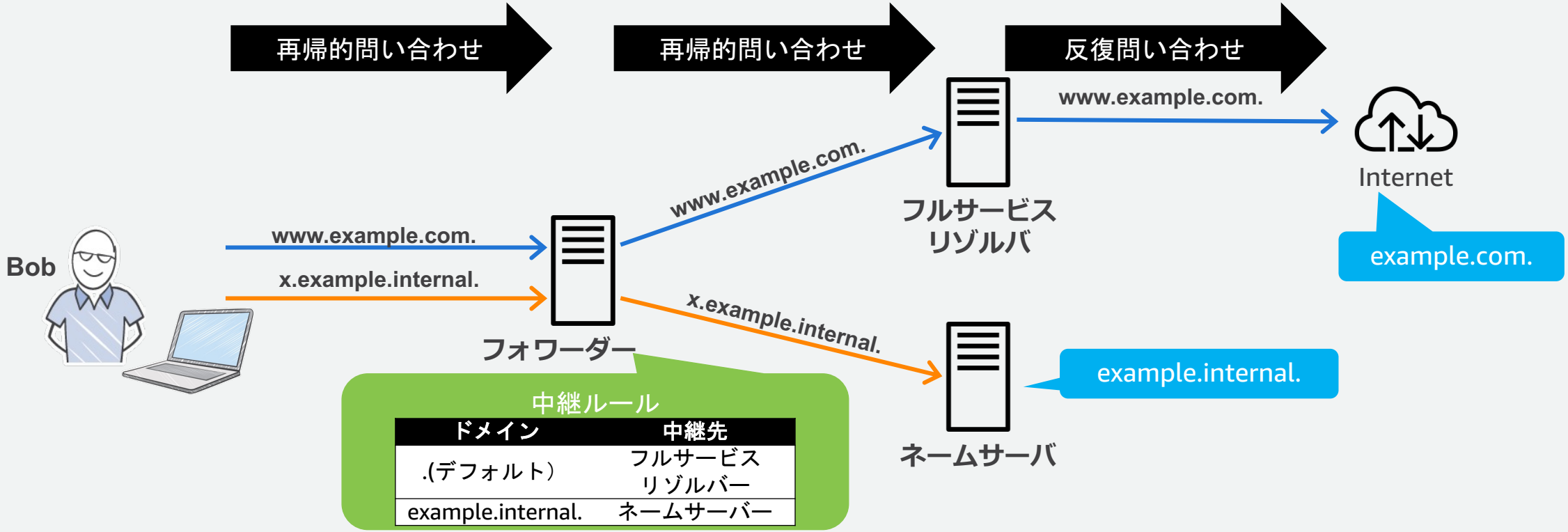
Windows (Windows DNS Client)
ネットワークインターフェイスの設定



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

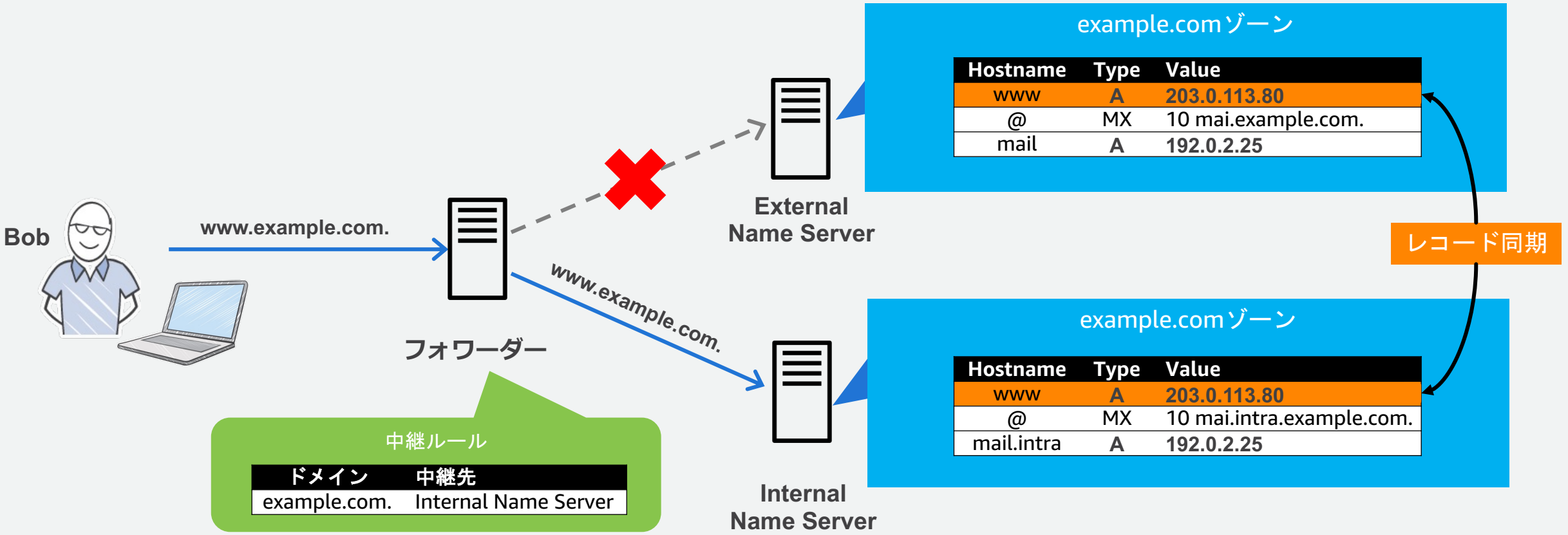
フォワーダー

- 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



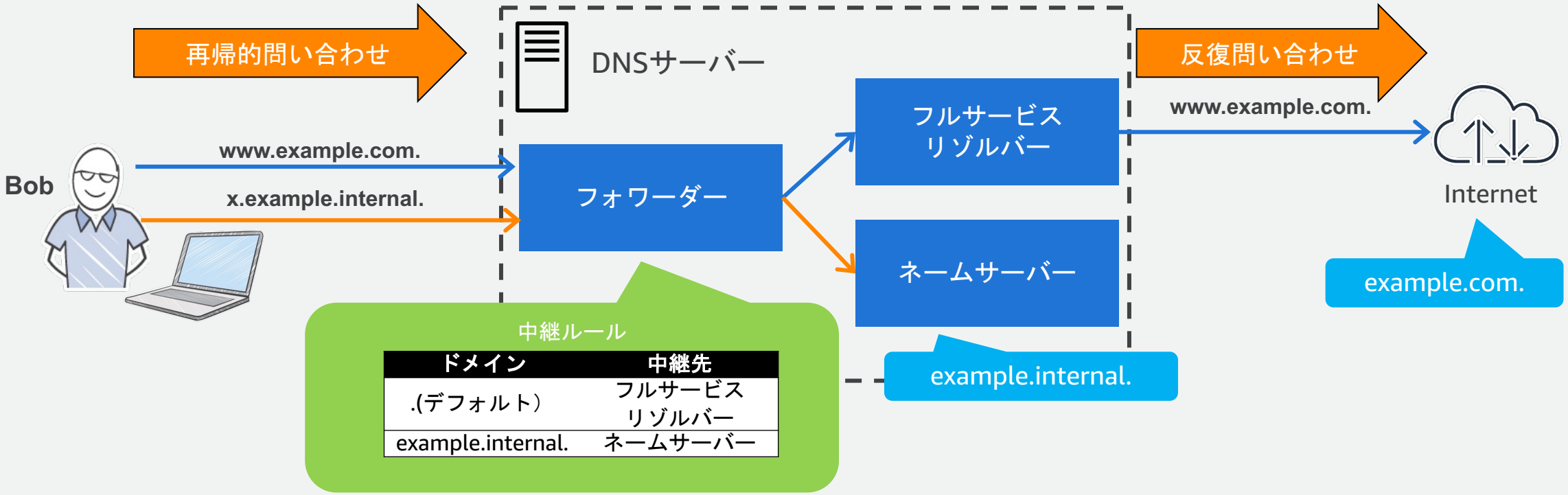
フォワーダーの制約

- 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



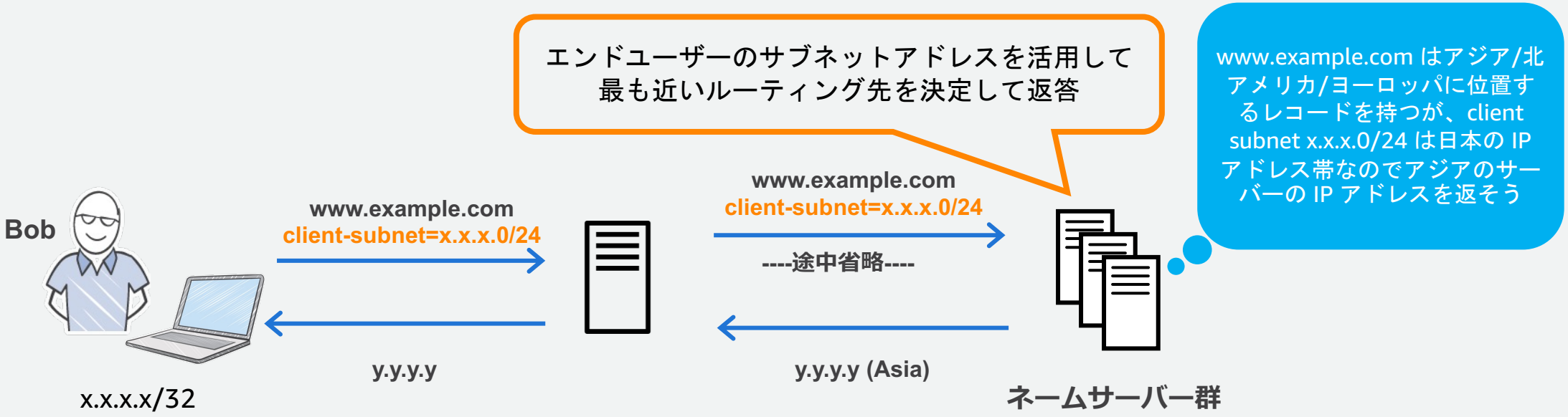
企業ネットワークの DNS サーバー基本構成

- 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採っていることが多い



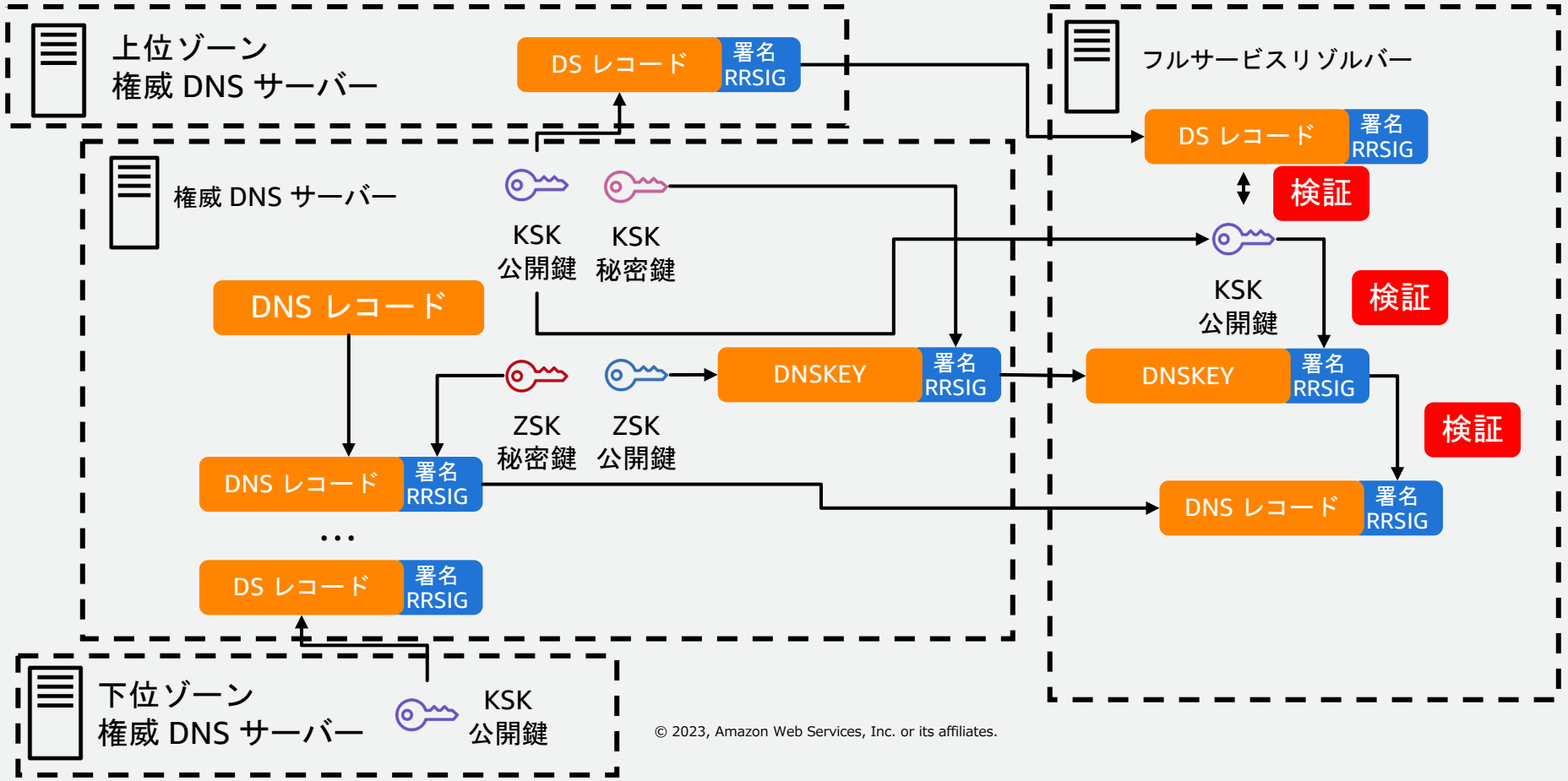
EDNS0 と EDNS Client Subnet 拡張

- 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った
  - 位置情報に関連する 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!