



このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください

[AWS Black Belt Online Seminar] Amazon Route 53 Hosted Zone

サービスカットシリーズ

Security Solutions Architect 中島 智広

2019/11/05

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>



自己紹介

中島 智広 (Tomohiro Nakashima)

AWS Security Solutions Architect

お客様のセキュリティの取り組みを
AWSアーキテクチャの視点からご支援



Background

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

好きなAWSサービス

Amazon Route 53 / Amazon Route 53 Resolver

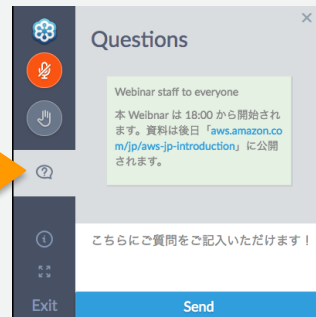
AWS Black Belt Online Seminar とは

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

質問を投げることができます！

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

- ① 吹き出しをクリック
- ② 質問を入力
- ③ Sendをクリック



Twitter ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では2019年11月5日時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(<http://aws.amazon.com>)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっています。日本居住者のお客様が東京リージョンを使用する場合、別途消費税をご請求させていただきます。
- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

ご案内：Amazon Route 53は全2回でお届けしています

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

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

本日の内容

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

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

ご案内：Amazon Route 53 Resolver 資料と映像

Amazon Web Services ブログ

[AWS Black Belt Online Seminar] Amazon Route 53 Resolver 資料及び QA 公開

by AWS Japan Staff | on 18 OCT 2019 | in [Amazon Route 53, Webinars](#) | [Permalink](#) | [Share](#)

先日 (2019/10/16) 開催しました AWS Black Belt Online Seminar 「Amazon Route 53 Resolver」の資料を公開しました。当日、参加者の皆様から頂いた QA の一部についても共有しております。



<https://aws.amazon.com/jp/blogs/news/webinar-bb-amazon-route-53-resolver-2019/>

本セミナーの概要

DNSのネームサーバー機能を提供するAmazon Route 53 Hosted Zoneの活用について解説します。

その前提となるドメイン名、ネームサーバーの基本についても解説し、DNS全体の理解を深めます。

Agenda

1. ドメイン名の基本
2. ネームサーバーの基本
3. Amazon Route 53 Hosted Zoneの基本
4. 移行とテスト、トラブルシューティングの基本

1. ドメイン名の基本

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>



ホスト名とFQDN（完全修飾ドメイン名）

ホスト名

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

例)

www1

FQDN（完全修飾ドメイン名）

サブドメインからトップレベルドメインまで完全に指定されたホスト名

例)

www1.sub.example.com.

ip-private-ipv4-address.ec2.internal.

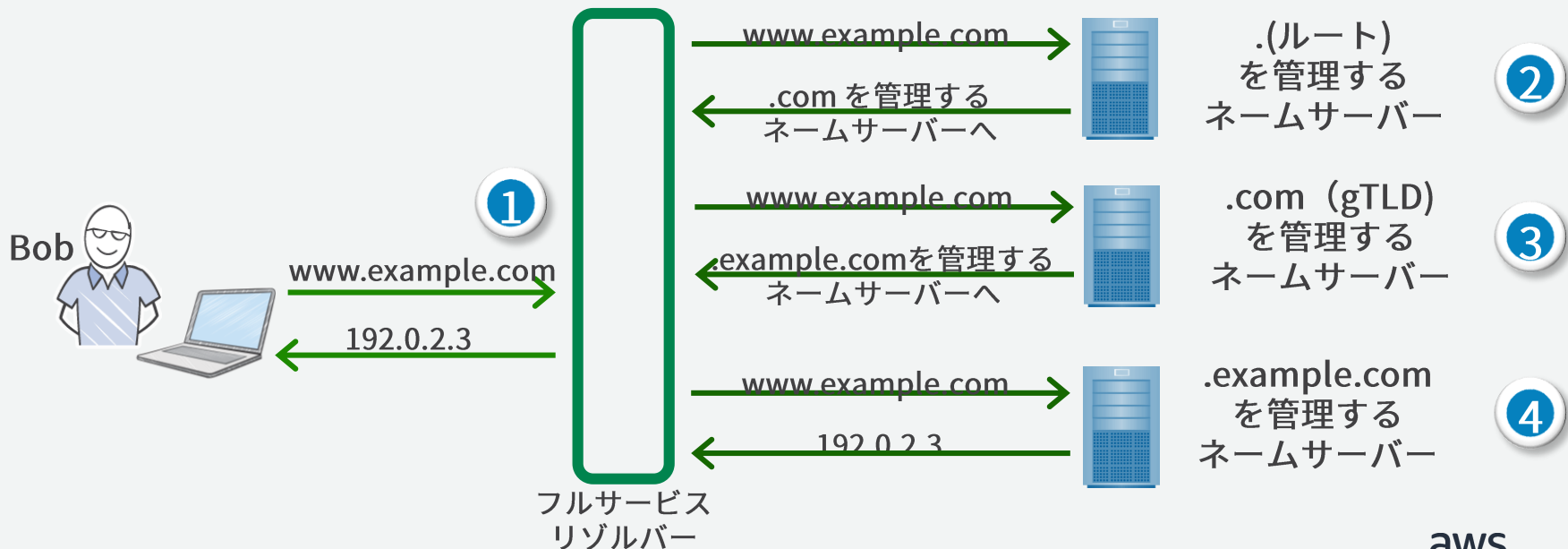
※ルートは「.」で表されるため、狭義の意味でのFQDNを表記する際には、末尾の「.」まで含めて表記する

ノードが一意に識別されることを前提にしていない相対的な名前

特定のドメイン名空間において、ノードを一意に識別が可能な名前

DNS (Domain Name System)

- FQDN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	
.org	
.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

コントロール
パネル

レジストラ
管理システム

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WHOISを提供

WHOIS

WHOIS
データベース

同期

TLD
ネームサーバー

操作

連携

WHOISデータベース

ドメイン名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

Domain Name Registration Data Lookup

Enter a domain name

[Frequently Asked Questions \(FAQ\)](#)

Lookup

By submitting any personal data, I acknowledge and agree that the personal data submitted by me will be processed in accordance with the ICANN [Privacy Policy](#), and agree to abide by the website [Terms of Service](#) and the [Domain Name Registration Data Lookup Terms of Use](#).

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: 2020-08-13 04:00:00 UTC

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

<https://lookup.icann.org/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

ドメイン名の基本 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

【ご案内】 Amazon Route 53 を用いたドメイン登録

- Amazon Route 53のマネジメントコンソールを用いてドメイン登録が可能

ドメインの登録

使用可能なドメインを見つけて登録するか、Route 53 に **既存のドメイン** を移管します。

ドメイン名の入力 .com - \$12.00 チェック

- Amazon Route 53 で登録できるドメイン
https://docs.aws.amazon.com/ja_jp/Route53/latest/DeveloperGuide/registrar-tld-list.html
- レジストラは、Amazon Registrar, Inc. と Gandi
- 追加を希望する TLD を提案するには、[Amazon Route 53 Domain Registration フォーラム](#) でコメントを入力してください。

Agenda

1. ドメイン名の基本
2. **ネームサーバーの基本**
3. Amazon Route 53 Hosted Zone
4. 移行とテスト、トラブルシューティング

2. ネームサーバーの基本

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



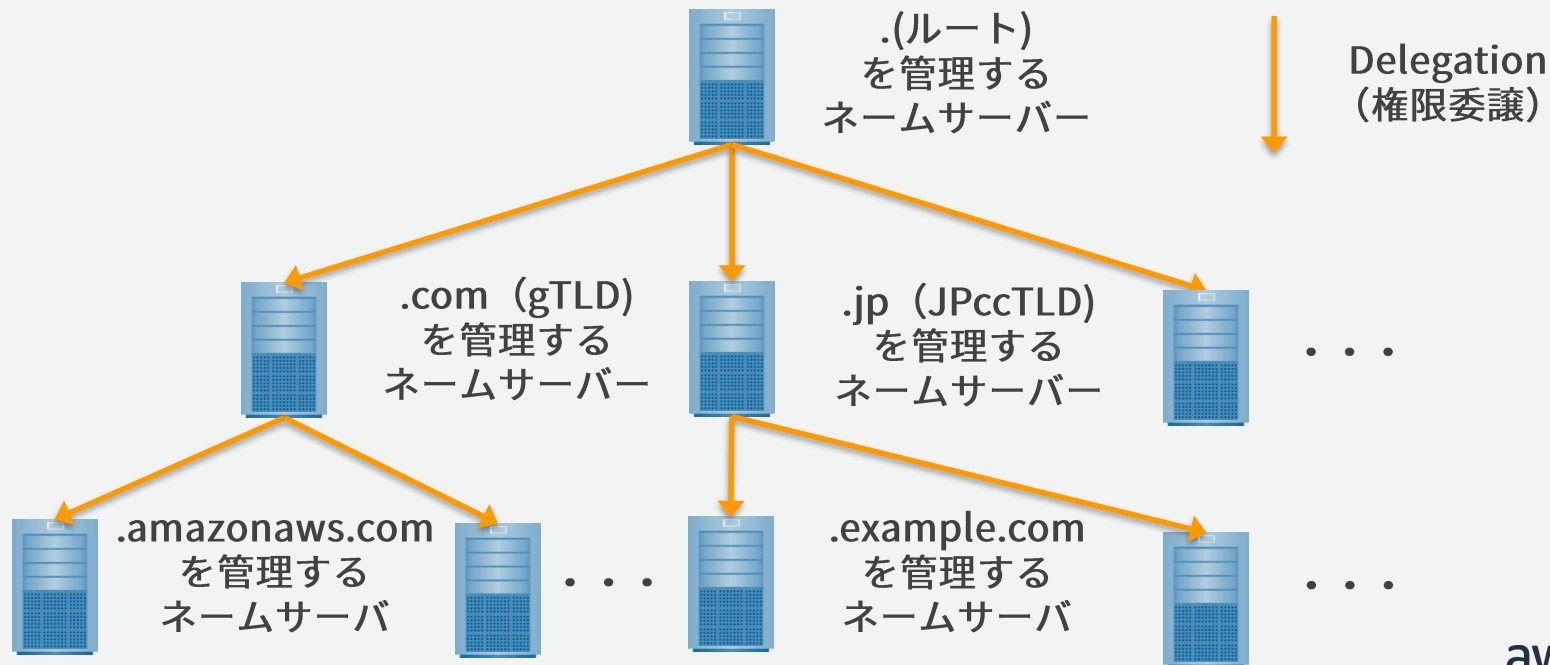
過去資料

<https://amzn.to/JPArchive>



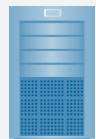
ネームサーバ / Name Server

- .(ルート) を起点に全てのFQDNを探索できるように構成された分散データベース、およびそれを成すひとつひとつのサーバ
- 権限委譲元を「親ゾーン」、権限委譲先を「子ゾーン」と呼ぶ



Delegation (権限委譲)

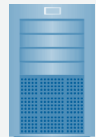
- 親ゾーンから子ゾーンのネームサーバーをFQDNで指し示すことで権限を委譲
- 子ゾーンのネームサーバーのFQDNが、子ゾーンで管理されている場合、親ゾーンの返答にそのIPアドレスも含めて指し示す (a.k.a. Glueレコード)



.com (gTLD)
を管理する
ネームサーバー



Delegation
(権限委譲)



example.com
を管理する
ネームサーバー

権限委譲先のネームサーバーを
FQDNで指し示す

example.com.	3600	IN	NS	ns1.example.com.	
example.com.	3600	IN	NS	ns2.example.com.	
ns1.example.com.	3600	IN	A	192.0.2.1	Glue
ns2.example.com.	3600	IN	A	192.0.2.2	レコード

example.comを管理するネームサーバーに
到達するためのIPアドレスを提供

RR(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をもち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	
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.	

※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レコードタイプ

- ゾーンの実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
- ゾーンの実管理に関する情報 (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

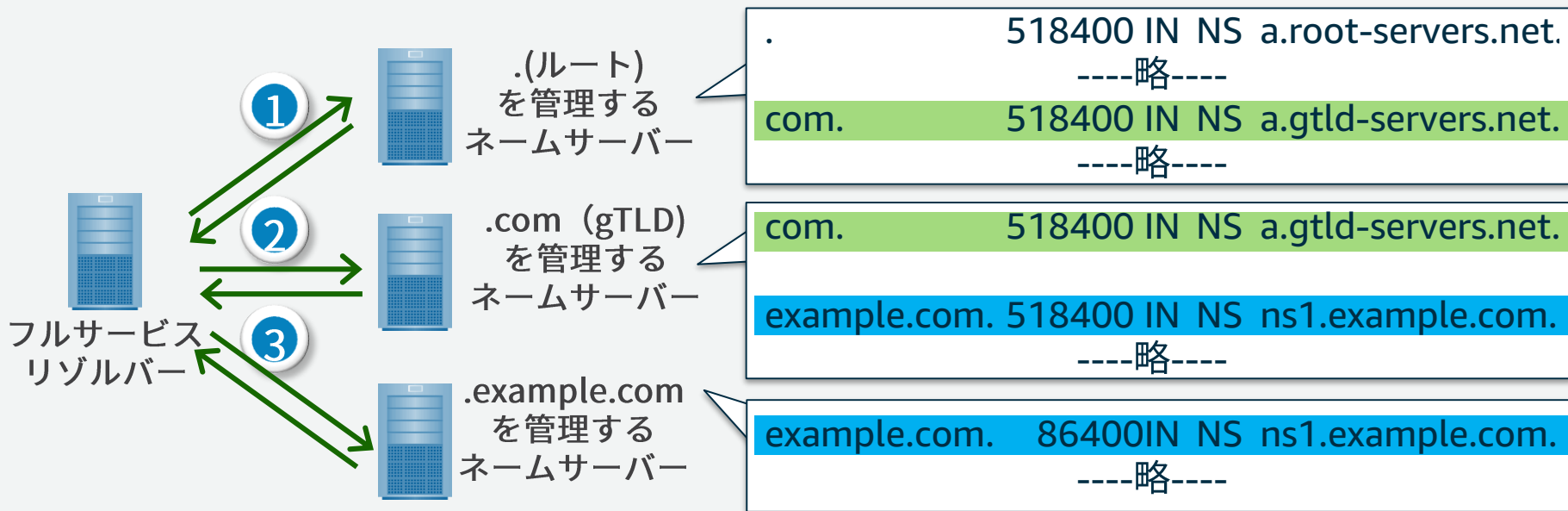
example.comゾーン

```
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し示すNSレコードタイプ

- 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レコードタイプ

- 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レコードタイプ

- 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レコードタイプの制約とZone Apex

- ある名前前で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	
example.com.	3600	IN	NS	ns.example.com.
ns.example.com.	3600	IN	NS	192.0.2.1
www.example.com	3600	IN	A	

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

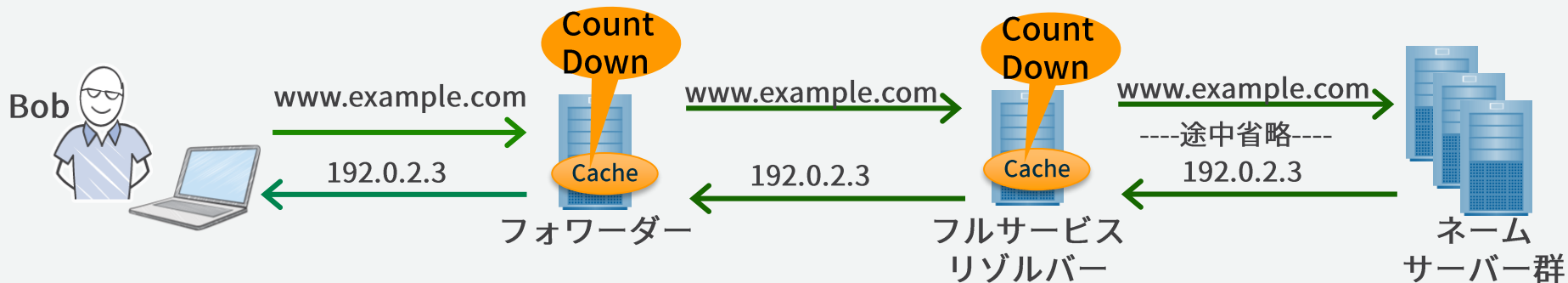
【補足】 Amazon Route 53ではエイリアスレコード機能により、制約を回避しZone Apexでサービスをホストできる

追加

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

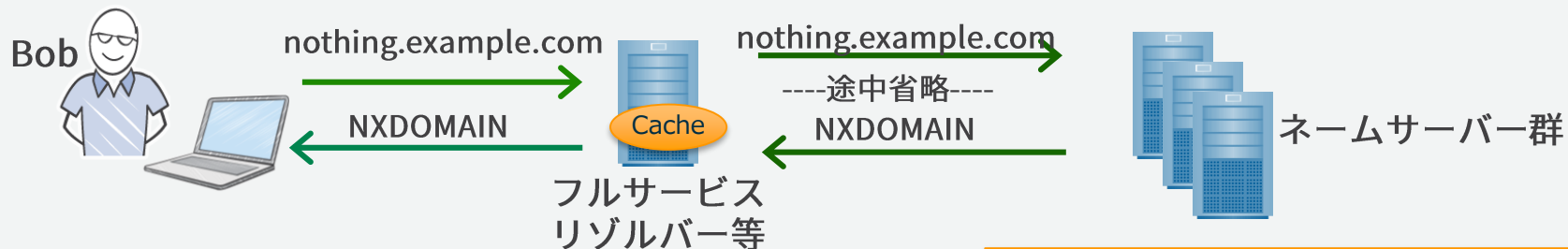
キャッシュ時間を定めるTTL

- 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き、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



不存在応答 (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

ネームサーバーまとめ

- .(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
- NSレコードとGlueによる、親ゾーンから子ゾーンへの権限委譲の仕組み
- レコードを構成する5つの要素 (NAME、TTL、CLASS、TYPE、RDATA)
- 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

Agenda

1. ドメイン名の基本
2. ネームサーバーの基本
3. Amazon Route 53 Hosted Zone
4. 移行とテスト、トラブルシューティング

3. Amazon Route 53 Hosted Zone

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>



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
- 変更の高速伝播

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

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
- トラフィックルーティング
- ヘルスチェック & DNS フェイルオーバー

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
 - 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
- ↑↑↑原則としてこれらのレコードを変更しないでください↑↑↑

<input type="checkbox"/>	名前	タイプ	値
<input type="checkbox"/>	example.com.	NS	ns-1536.awsdns-00.co.uk.
			ns-0.awsdns-00.com.
			ns-1024.awsdns-00.org.
			ns-512.awsdns-00.net.
<input type="checkbox"/>	example.com.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amaz

Amazon Route 53 サービスレベルアグリーメント

<https://aws.amazon.com/jp/route53/sla/>

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



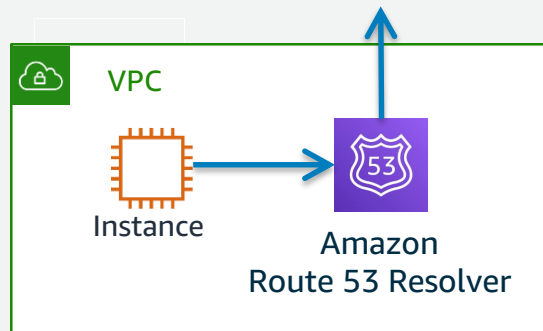
Amazon Route 53
Public Hosted Zone

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



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>)

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
------------------	----	----	---	-----------

※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

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

Amazon Route 53が提供するルーティングポリシー

- | | |
|------------|----------|
| ① シンプル | ⑤ レイテンシー |
| ② 加重 | ⑥ 位置情報 |
| ③ フェイルオーバー | ⑦ 物理的近接性 |
| ④ 複数回答 | |

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①：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）

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

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

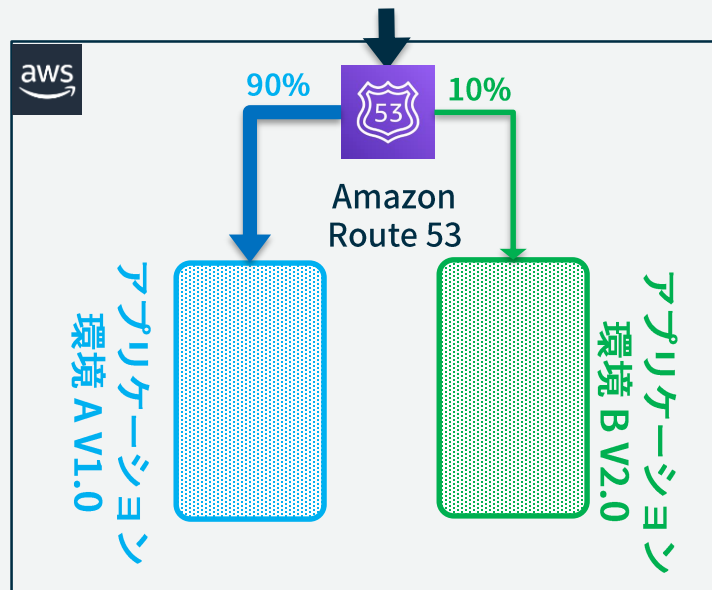
応答順序は
都度ランダム

ルーティングポリシー②：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

具体的なユースケース

- A/B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③：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/パッシブ構成を実現
- 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



ヘルスチェック



フェイルオーバー

具体的なユースケース

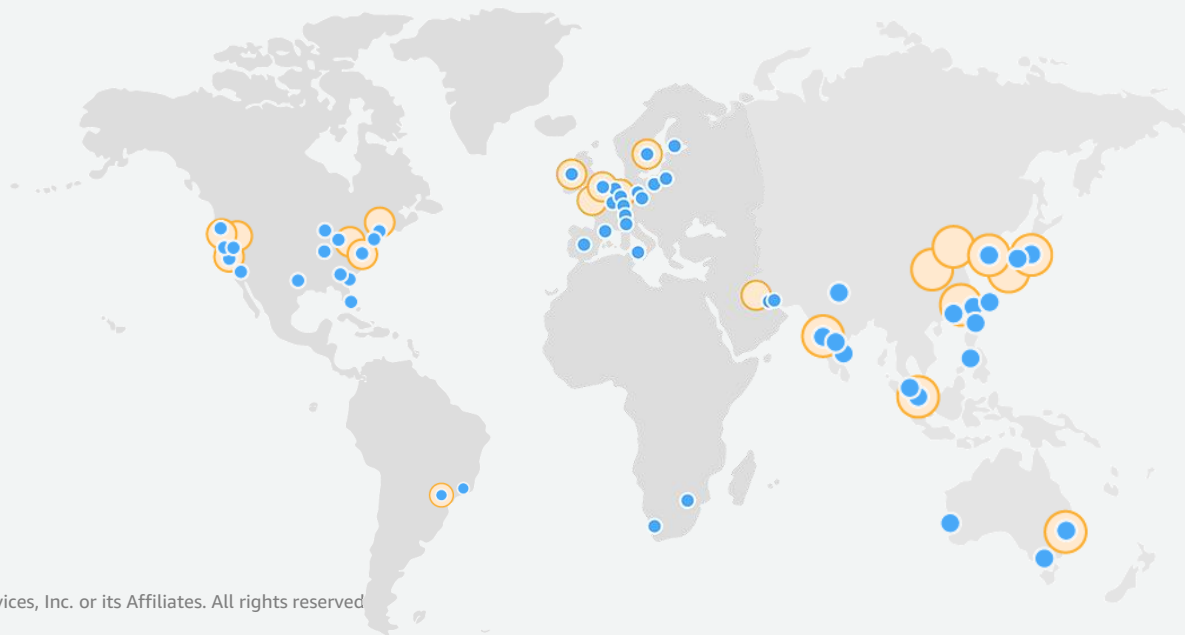
- 複数リージョンにまたがるシステムで冗長構成
- 災害発生時にリージョン間でフェイルオーバー
- 障害時に、S3静的ウェブサイトホスティングのSorry Pageを表示

ルーティングポリシー④：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

ルーティングポリシー⑤：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ります



ルーティングポリシー⑥：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

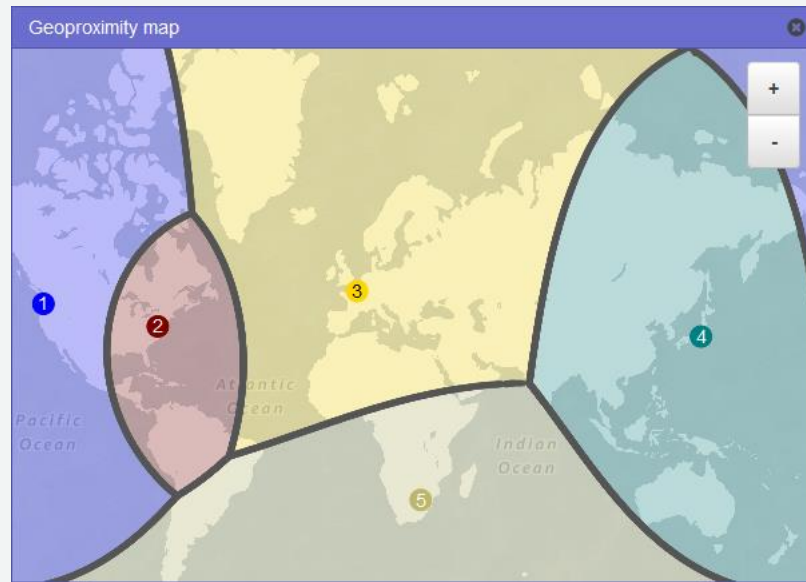
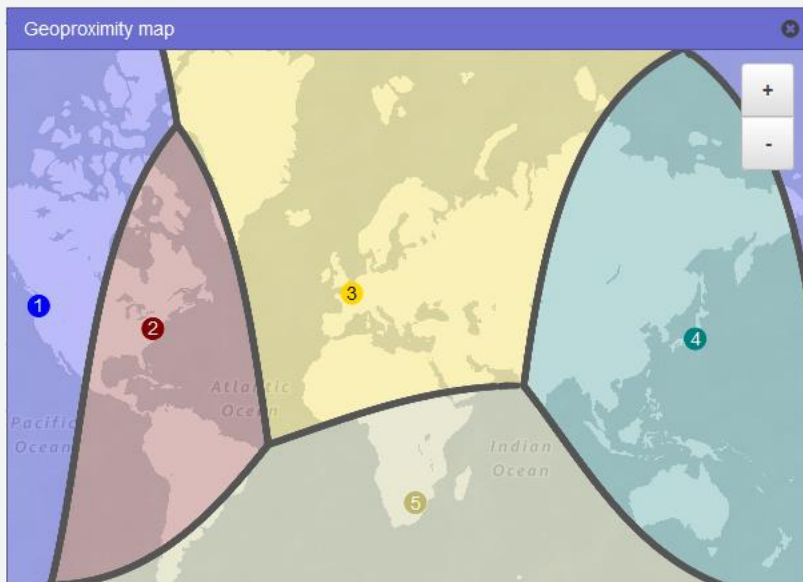


具体的なユースケース

- 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

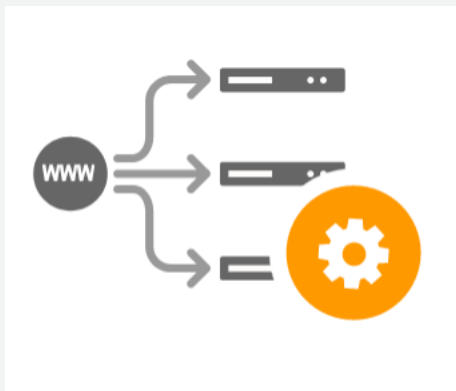
ルーティングポリシー⑦：物理的近接性

- 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
- 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



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します。



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、バージョン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います。

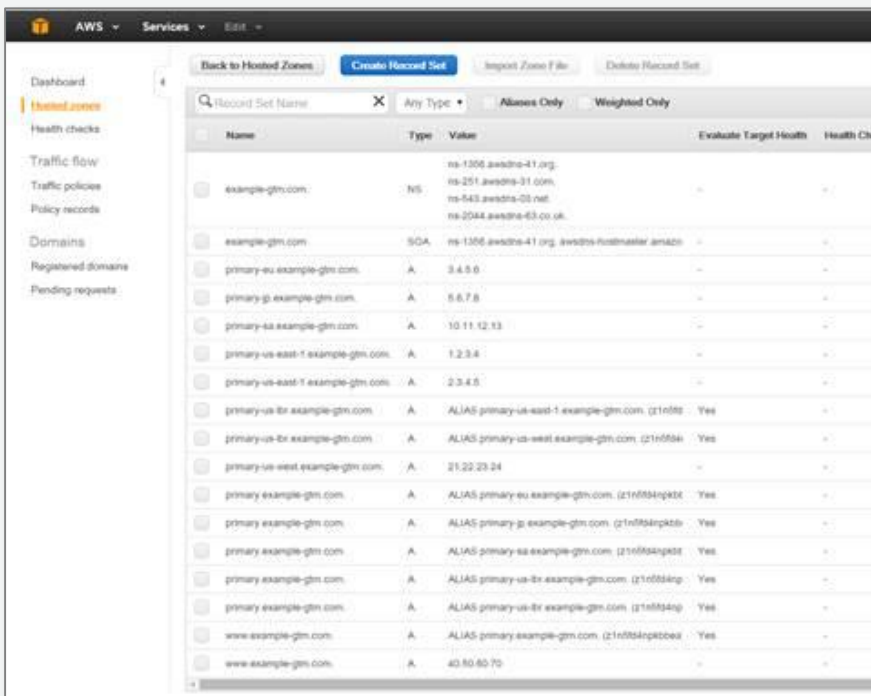


ポリシーレコード

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ます。

トラフィックフローのベネフィット

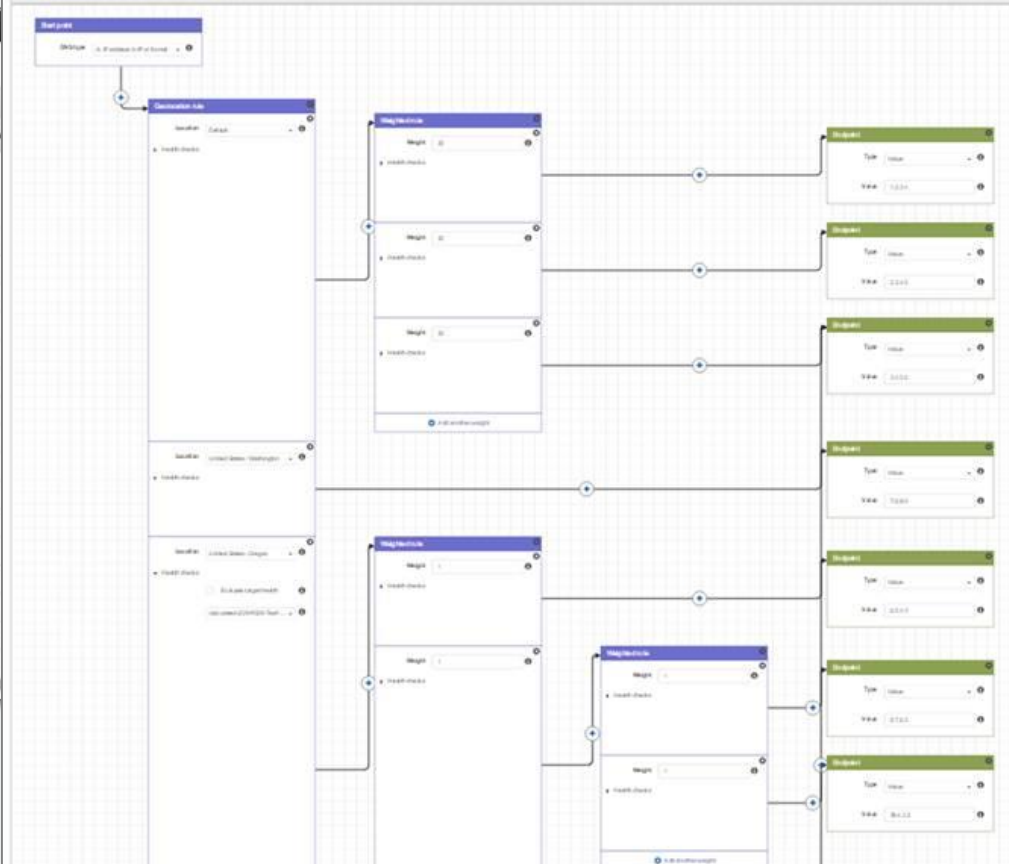
トラフィックフローを用いない設定



The screenshot shows the AWS Route 53 console. The left sidebar contains navigation options: Dashboard, Health checks, Traffic flow, Traffic policies, Policy records, Domains, Registered domains, and Pending requests. The main area displays a table of hosted zones and records.

Name	Type	Value	Evaluate Target Health	Health Check
example-gtm.com.	NS	ns-1266.awdns-41.org. ns-251.awdns-31.com. ns-543.awdns-03.net. ns-2044.awdns-63.co.uk.	-	-
example-gtm.com.	SOA	ns-1266.awdns-41.org. awdns-hostmaster.amazon.com.	-	-
primary-eu.example-gtm.com.	A	3.4.5.0	-	-
primary-g.example-gtm.com.	A	5.6.7.8	-	-
primary-sa.example-gtm.com.	A	10.11.12.13	-	-
primary-us-east-1.example-gtm.com.	A	1.2.3.4	-	-
primary-us-east-1.example-gtm.com.	A	2.3.4.5	-	-
primary-us-ftr.example-gtm.com.	A	ALIAS primary-us-east-1.example-gtm.com. (Z1N054K9K8C)	Yes	-
primary-us-ftr.example-gtm.com.	A	ALIAS primary-us-west.example-gtm.com. (Z1N054K9K8C)	Yes	-
primary-us-west.example-gtm.com.	A	21.22.23.24	-	-
primary.example-gtm.com.	A	ALIAS primary-eu.example-gtm.com. (Z1N054K9K8C)	Yes	-
primary.example-gtm.com.	A	ALIAS primary-g.example-gtm.com. (Z1N054K9K8C)	Yes	-
primary.example-gtm.com.	A	ALIAS primary-sa.example-gtm.com. (Z1N054K9K8C)	Yes	-
primary.example-gtm.com.	A	ALIAS primary-us-ftr.example-gtm.com. (Z1N054K9K8C)	Yes	-
primary.example-gtm.com.	A	ALIAS primary-us-east-1.example-gtm.com. (Z1N054K9K8C)	Yes	-
www.example-gtm.com.	A	ALIAS primary.example-gtm.com. (Z1N054K9K8C)	Yes	-
www.example-gtm.com.	A	40.80.60.70	-	-

トラフィックフローを用いた設定



さらなる応用

- Amazon Route 53 では、AWS CLIやAWS SDK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



Amazon Route 53 Hosted Zoneのまとめ

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
- 変更の高速伝播

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

Agenda

1. ドメイン名の基本
2. ネームサーバーの基本
3. Amazon Route 53 Hosted Zone
4. 移行とテスト、トラブルシューティング

4.移行とテスト、トラブルシューティング

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>



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

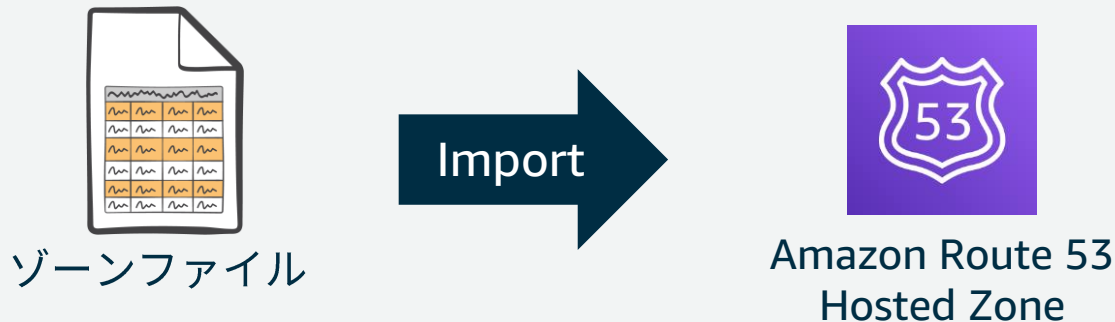
<https://jprs.jp/related-info/guide/019.pdf>

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

1. Amazon Route 53 Hosted Zoneを構成する
2. 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
3. 親ゾーンと子ゾーンでDelegation(権限委譲) の設定を変更する
4. 旧ネームサーバーの廃止

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

短縮

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

あるいは

example.com.	300	IN	NS	ns1.example.com.
--------------	-----	----	----	------------------

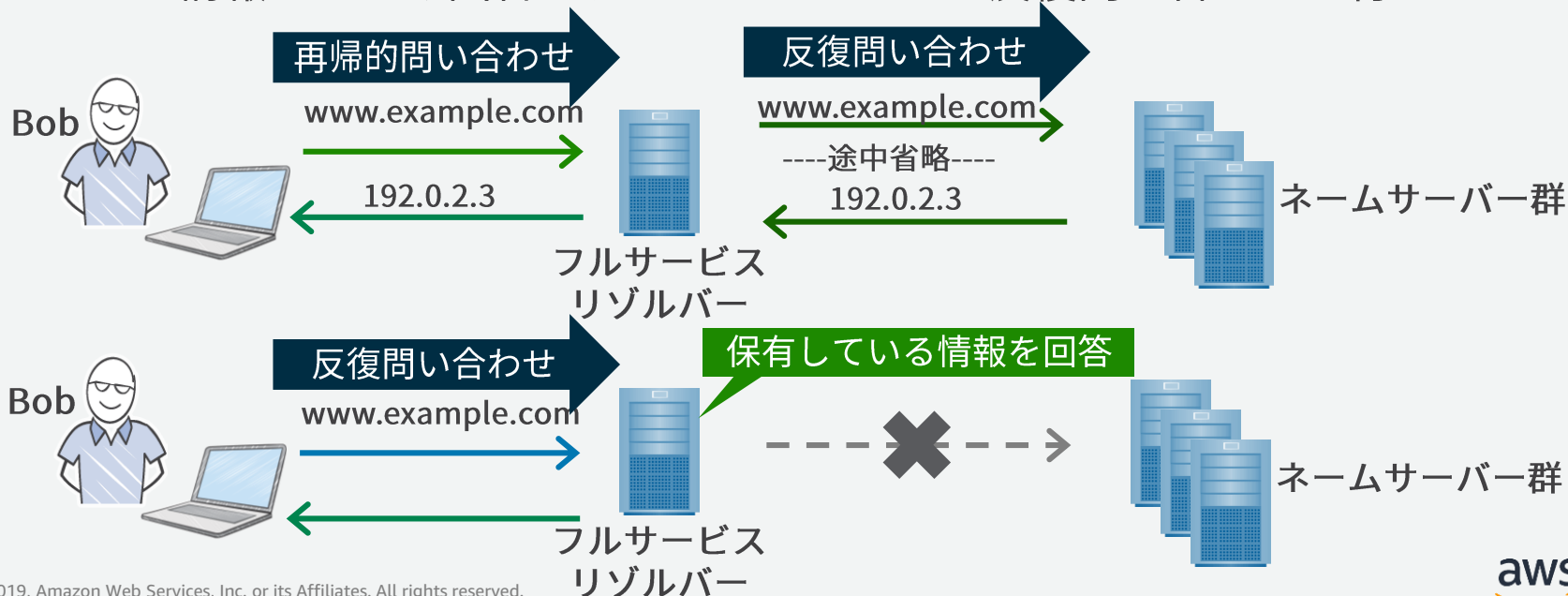
テストとトラブルシューティング

- 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

```
$ 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
```

特に注目

Header

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

```
;; QUESTION SECTION:  
;www.example.com. IN A
```

Question

```
;; ANSWER SECTION:  
www.example.com. 60 IN A 192.0.2.3
```

Answer

```
;; 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
```

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>

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/>

まとめ

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>



本セミナーのまとめ

DNSのネームサーバー機能を提供するAmazon Route 53 Hosted Zoneの活用について解説しました。

その前提となるドメイン名、ネームサーバーの基本についても解説し、DNS全体の理解を深めました。

改めてのご案内：Amazon Route 53は全2回でお届けしました

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

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

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

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

改めてのご案内：Amazon Route 53 Resolver 資料と映像

Amazon Web Services ブログ

[AWS Black Belt Online Seminar] Amazon Route 53 Resolver 資料及び QA 公開

by AWS Japan Staff | on 18 OCT 2019 | in Amazon Route 53, Webinars | Permalink | Share

先日 (2019/10/16) 開催しました AWS Black Belt Online Seminar 「Amazon Route 53 Resolver」の資料を公開しました。当日、参加者の皆様から頂いた QA の一部についても共有しております。



<https://aws.amazon.com/jp/blogs/news/webinar-bb-amazon-route-53-resolver-2019/>

Q&A

質問を投げることができます！

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

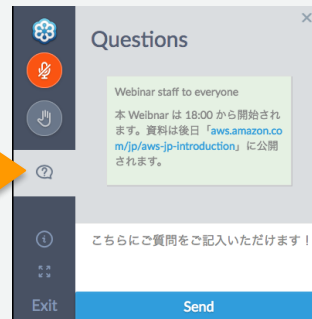
- ① 吹き出しをクリック
- ② 質問を入力
- ③ Sendをクリック

回答はAWS Japan Blog

「<https://aws.amazon.com/jp/blogs/news/>」にて

後日掲載します。

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



AWS の日本語資料の場所「AWS 資料」で検索



The screenshot shows the AWS Japanese website header with the AWS logo, navigation links for '製品', 'ソリューション', '料金', 'ドキュメント', '学習', 'パートナー', 'AWS Marketplace', and 'その他', and a search icon. A '日本語' dropdown menu is visible. A prominent orange button says 'コンソールにサインイン'. The main heading is 'AWS クラウドサービス活用資料集トップ'. Below it is a paragraph in Japanese: 'アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)' At the bottom, there are four buttons: 'AWS Webinar お申込 >', 'AWS 初心者向け >', '業種・ソリューション別資料 >', and 'サービス別資料 >'.

aws

日本担当チームへお問い合わせ サポート 日本語 ▼ アカウント ▼ コンソールにサインイン

製品 ソリューション 料金 ドキュメント 学習 パートナー AWS Marketplace その他 🔍

AWS クラウドサービス活用資料集トップ

アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

AWS Webinar お申込 > AWS 初心者向け > 業種・ソリューション別資料 > サービス別資料 >

<https://amzn.to/JPArchive>

AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

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

- 申込みはイベント告知サイトから
(<https://aws.amazon.com/jp/about-aws/events/>)

AWS イベント

で[検索]



AWS Well-Architected



ご視聴ありがとうございました

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>

