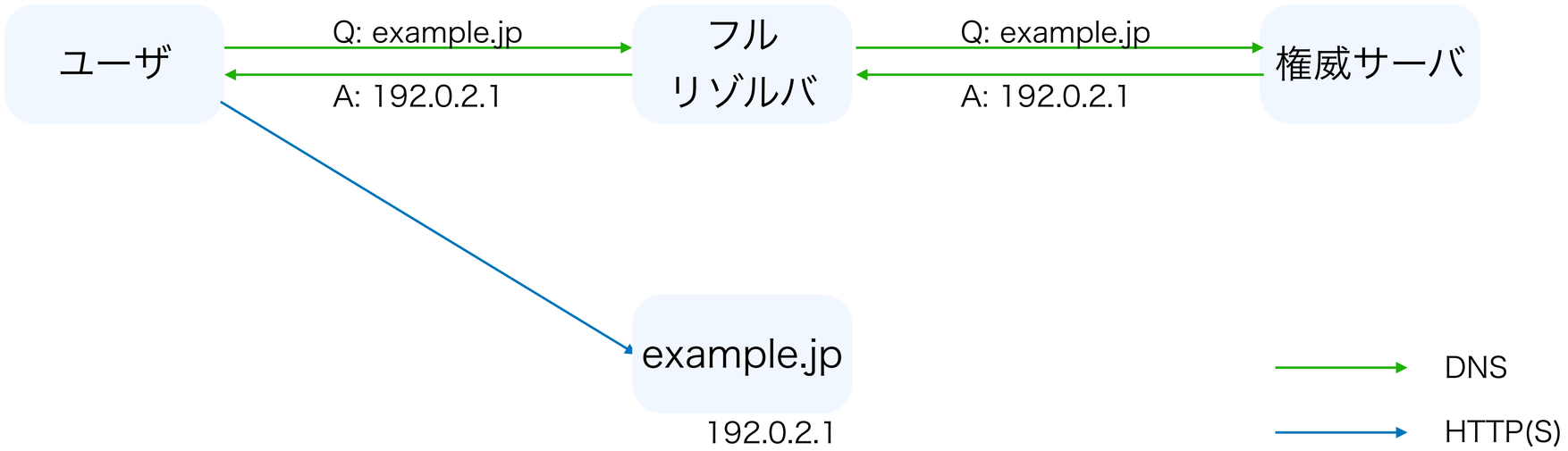
EDNS Client Subnetってどうよ

2020/08/27 JANOG46

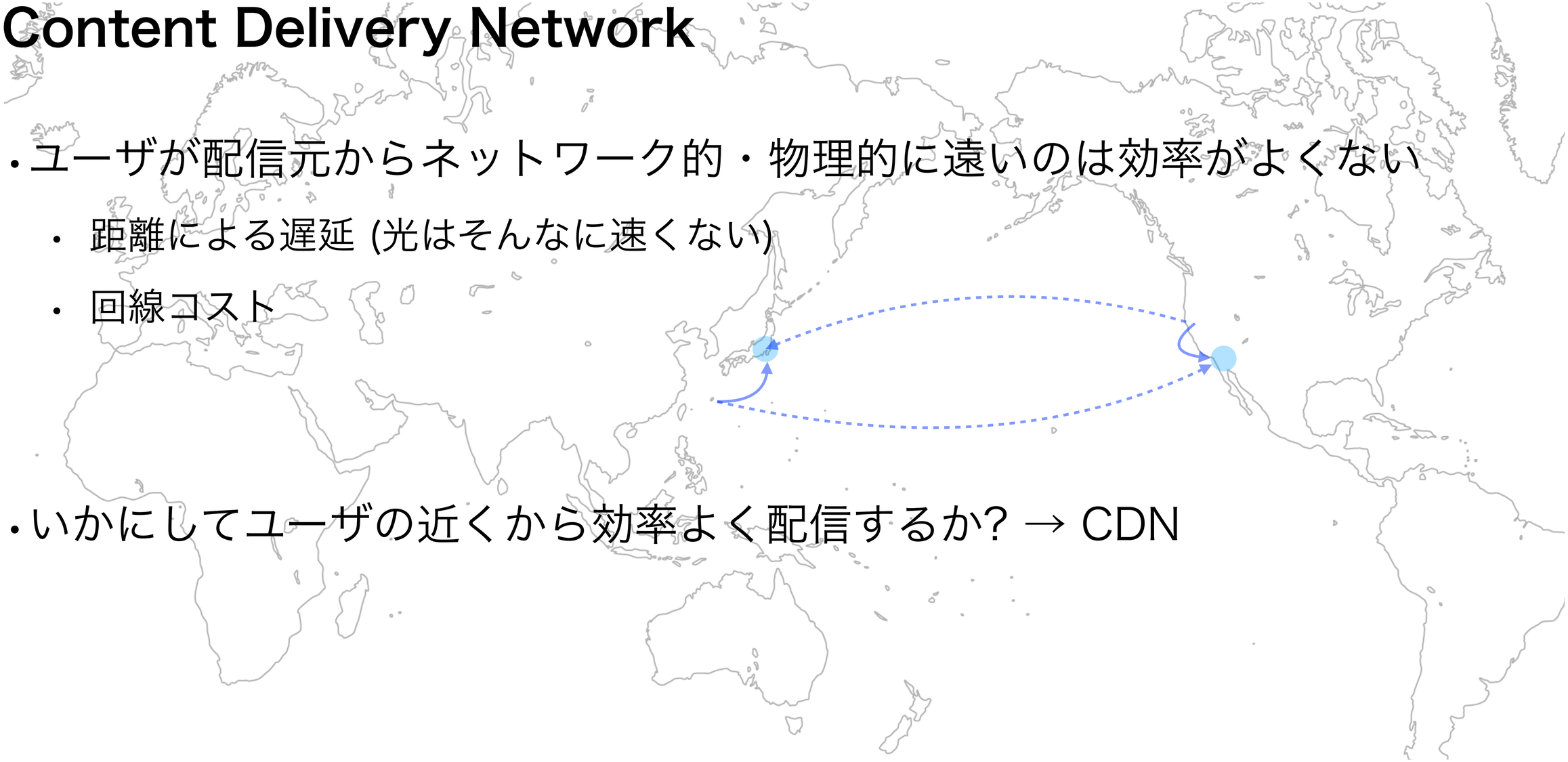
IIJ 山口崇徳

Webサーバにアクセスされるまで



CDN
Content Delivery Network

- ユーザが配信元からネットワーク的・物理的に遠いのは効率がよくない
  - 距離による遅延 (光はそんなに速くない)
  - 回線コスト



- いかにしてユーザの近くから効率よく配信するか? → CDN

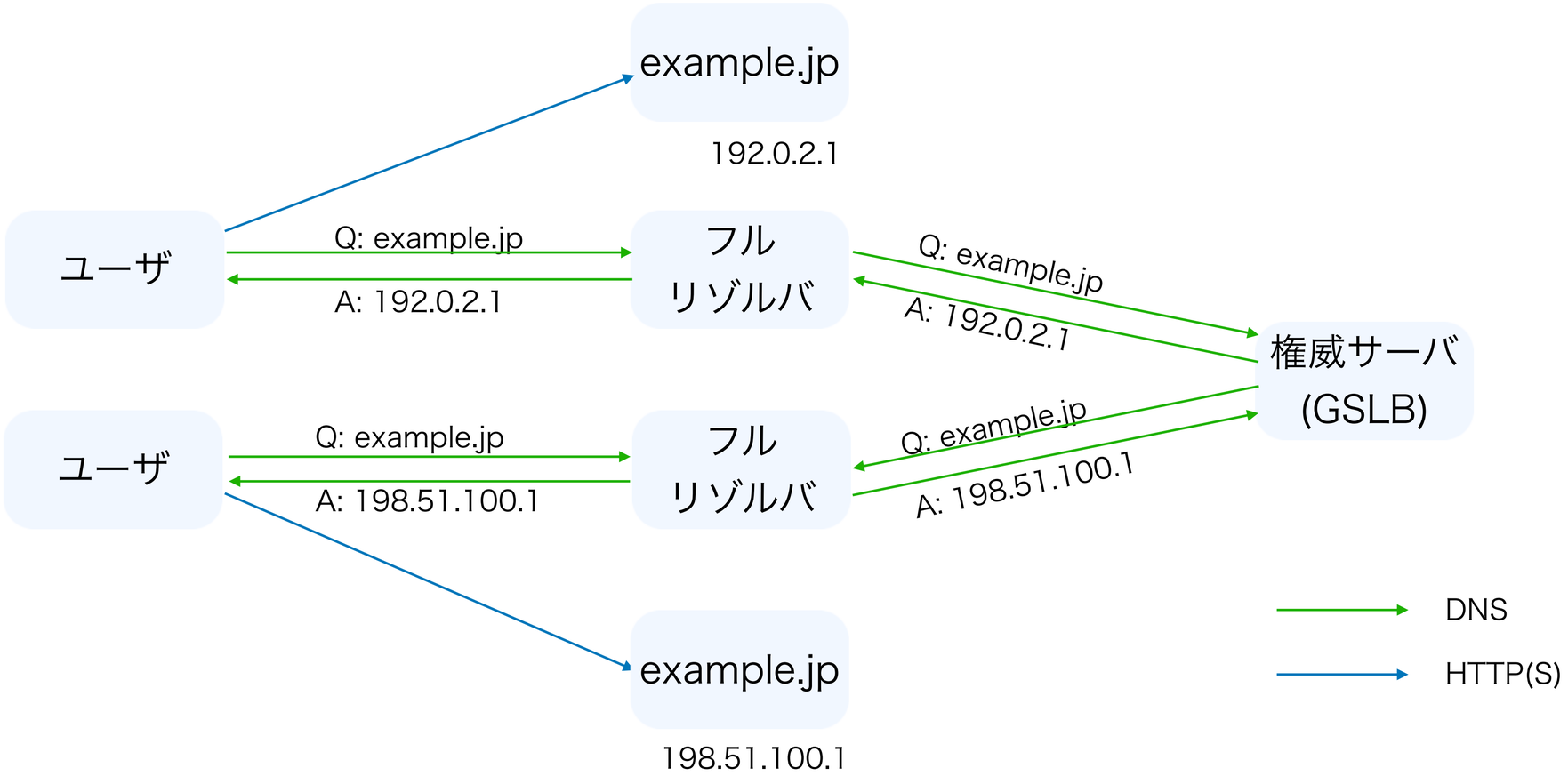
CDNの効率化戦略

- GSLB (Global Server Load Balance; GeoDNS)
  - 異なるIPアドレスを持った多数のサーバを分散配置し、権威DNSサーバが問い合わせ元IPアドレスによって応答を変えることで、ネットワーク的にもっとも近いエッジサーバにアクセスを誘導する
- Anycast
  - 同一のIPアドレスを持った多数のサーバを分散配置し、経路制御によりネットワーク的にもっとも近い権威DNSサーバ、エッジサーバにアクセスを誘導する

CDNの効率化戦略

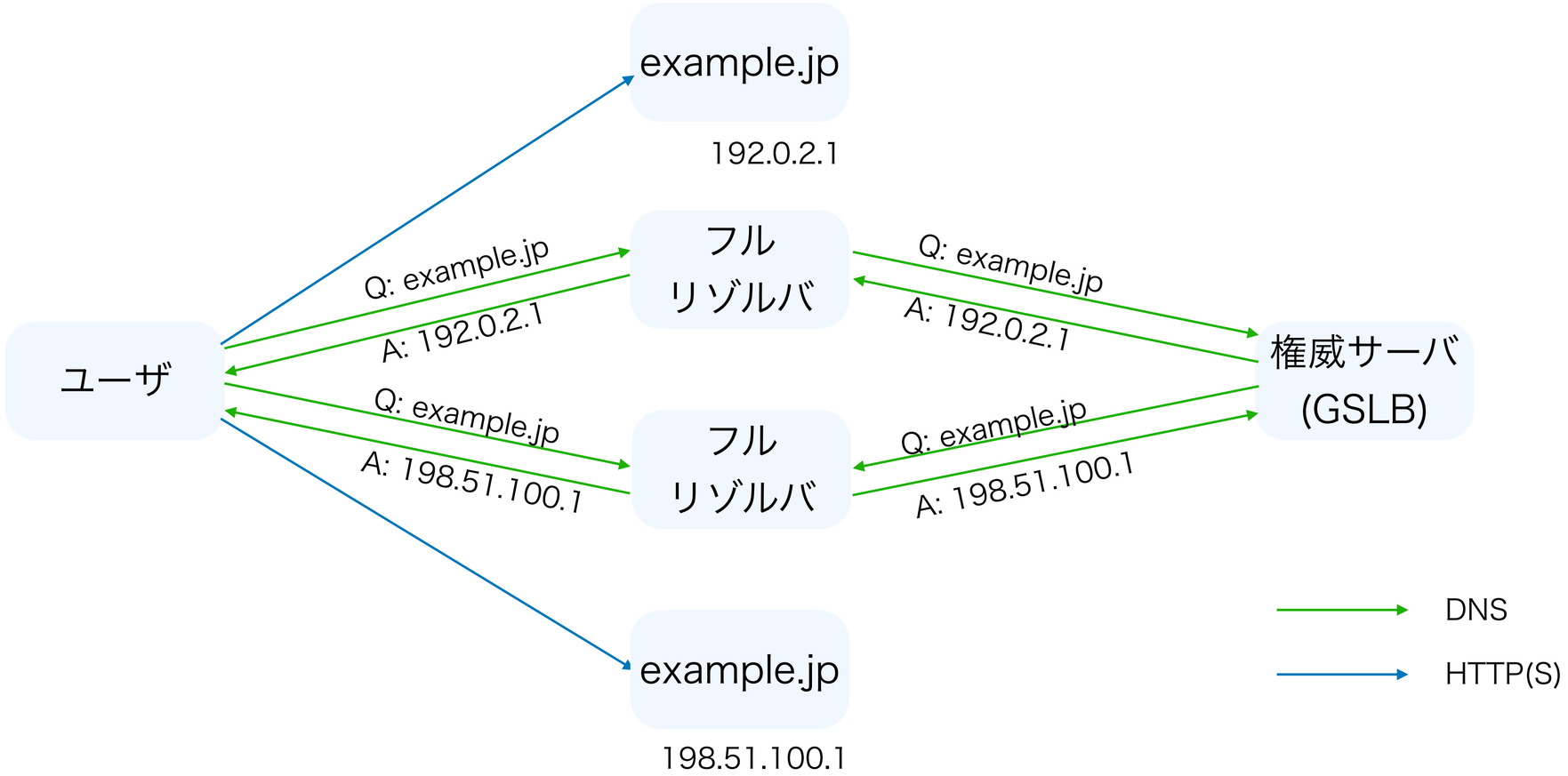
- GSLB (Global Server Load Balance; GeoDNS)
  - 異なるIPアドレスを持った多数のサーバを分散配置し、権威DNSサーバが問い合わせ元IPアドレスによって応答を変えることで、ネットワーク的にもっとも近いエッジサーバにアクセスを誘導する
- Anycast
  - 同一のIPアドレスを持った多数のサーバを分散配置し、経路制御によりネットワーク的にもっとも近い権威DNSサーバ、エッジサーバにアクセスを誘導する

Webサーバにアクセスされるまで
GSLB対応版(1)



- ユーザにとって最適なサーバにアクセスを誘導する

Webサーバにアクセスされるまで
GSLB対応版(2)



- 同じユーザでも利用するフルリゾルバが異なるとアクセスするWebサーバも変わってしまう

GSLBとpublic DNS (1)

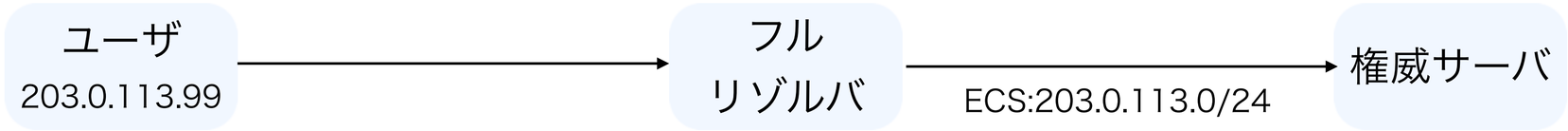
- 権威サーバへの問い合わせ元IPアドレス = フルリゾルバのIPアドレス
  - Webにアクセスしようとするエンドユーザの IPアドレスではない
- 従来、ユーザはISPが提供するフルリゾルバを使うことがほとんどだった
  - フルリゾルバとユーザはほとんどの場合同一AS内
  - 権威サーバがフルリゾルバのIPアドレスを元にエッジサーバを判断しても、CDNの効率に影響はない
- が、ユーザがpublic DNSを利用する場合は…

GSLBとpublic DNS (2)

- 多くの場合、public DNSはAnycastしている
  - ユーザとpublic DNSの間はネットワーク的に近くなる
- public DNSのIPアドレスを元にエッジサーバが決定された場合、
  - ユーザが国内にサーバを持つpublic DNSとCDNにアクセスするなら、国内で通信が完結する → それほど効率は落ちない
  - が、ユーザと同一のAS内にCDNのエッジサーバがある場合でも、別ASのエッジサーバに誘導されることは珍しくない → 最適とはかぎらない
    - CDNにアクセスするユーザだけでなく、ISPにとってもトランジット費用などでデメリット

ECS
RFC7871 EDNS Client Subnet

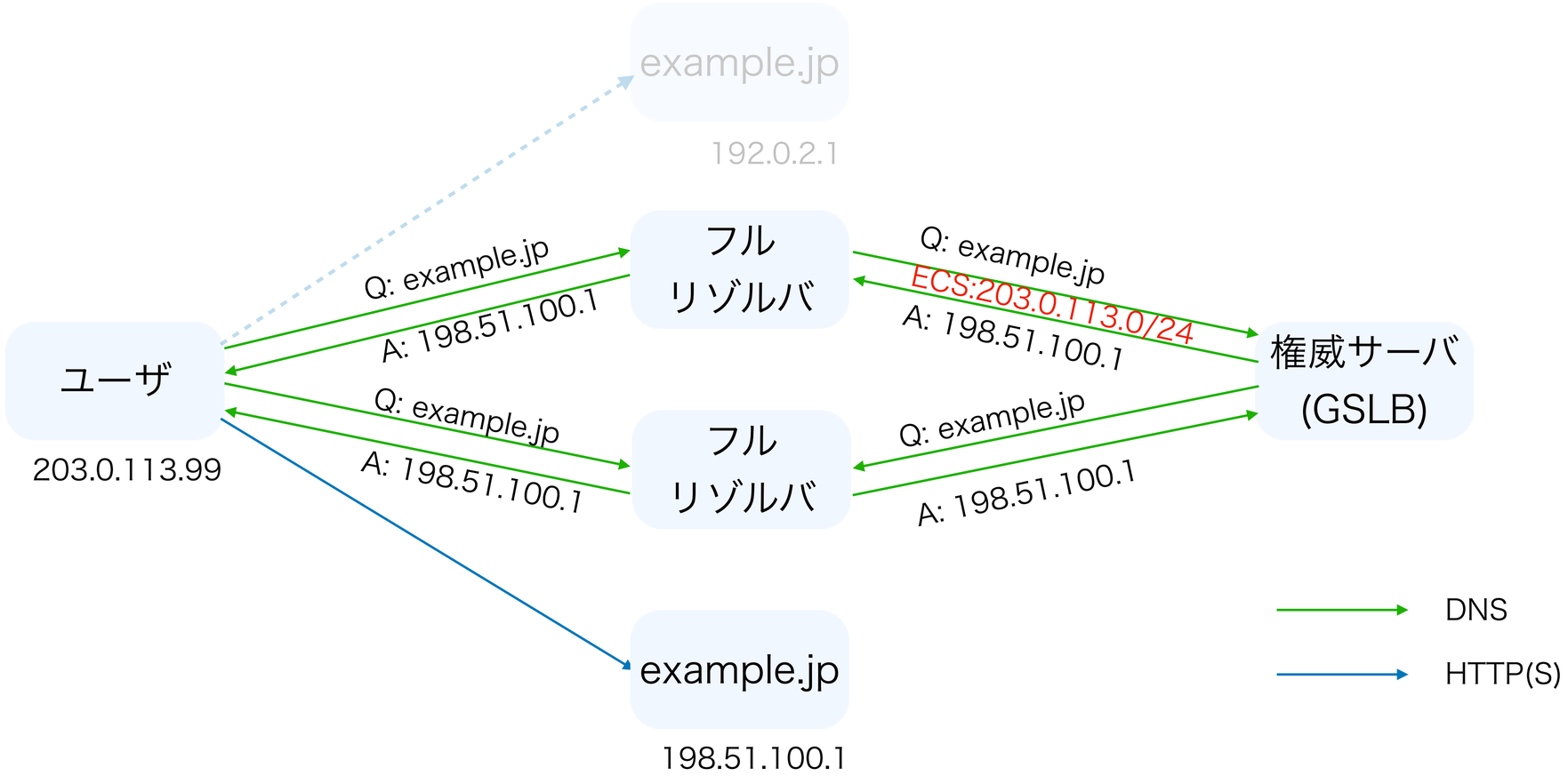
- フルリゾルバは、エンドユーザのIPアドレス(を/24程度に丸めたもの)を権威サーバに伝える



- GSLBは問い合わせ元ではなく、ECSの情報を元に応答するA/AAAAを変える

- 注: Amazon ECS (Elastic Container Service) とは**何の関係もありません**

Webサーバにアクセスされるまで
ECS対応版



・ECSにより、フルリゾルバではなくユーザのIPアドレスによってアクセスを誘導する

JANOG38 (2016年) 当時の ECS

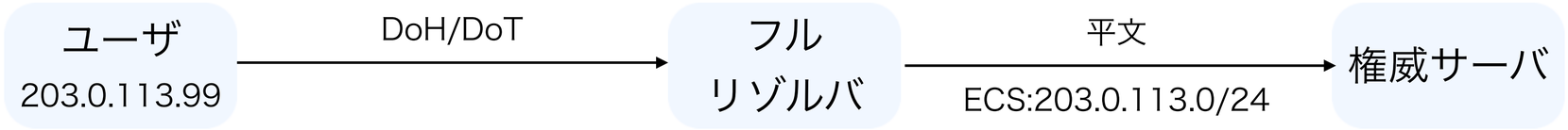
- JANOG38 EDNS-client-subnetってどうよ? 改めRFC7871ってどうよ
  - https://www.janog.gr.jp/meeting/janog38/program/edns.html
- draft から RFC に標準化されたばかり
- 大手事業者ではすでに使われていたが、あまり知られてはいなかった
- 「どうよ?」と問いかける段階

JANOG38から4年

- 対応する事業者(CDN、public DNS)はそれほど増えていない
  - ECSを必要とする事業者の多くはRFCになる前のdraft時点ですでに対応済み
- オープンソース実装での対応が進む
  - 権威: Knot、PowerDNS、(BINDは対応していたが9.16で削除)
  - フルリゾルバ: BIND、Unbound、PowerDNS Recursor
- ECSに起因するトラブル
- 新しいDNSの使い方

ECSのプライバシー

- 権威サーバはECSによりこれまで得られなかったユーザの情報を入手できる
- DoH/DoT: ユーザ-フルリゾルバ間の名前解決の暗号化
  - フルリゾルバと権威サーバの間は従来の平文のまま



- せっかく暗号化したのに、ECS情報が載る経路が平文ではユーザのプライバシーを守ったことになるの?
  - RFC7871ではフルリゾルバにECSを付与させないようユーザがopt-outする方法も用意されているが、一般的なスタブリゾルバではそれが実装されておらず、opt-outできない

1.1.1.1 vs archive.today

- 2018年5月ごろ(?)からcloudflareの1.1.1.1を利用しているユーザが archive.today (いわゆる魚拓サービス)にアクセスできなくなる
  - 1.1.1.1は2018/4/1リリースなので、ほぼサービス開始直後から
- 原因: ECSの解釈の違い
  - 1.1.1.1はユーザのプライバシーを守るという名目で、クエリにECSを付与しない
    - https://developers.cloudflare.com/1.1.1.1/nitty-gritty-details
  - archive.today 曰く、“consider ECS-less requests from Cloudflare as invalid”
    - https://twitter.com/archiveis/status/1018691421182791680

アプリケーション独自の名前解決
Application Doing DNS

- OS本来の仕組みを使わない、アプリケーションによる独自の名前解決
  - 一部のWebブラウザによるDoHでの名前解決など
- 特定ドメインの名前解決をアプリが直接権威DNSサーバに問い合わせるような実装であれば、権威サーバはECSがなくてもユーザのIPアドレスがわかる

- macOS11/iOS14で追加される予定のAPIを使うとこれを実現できるらしい
  - https://developer.apple.com/videos/play/wwdc2020/10047
  - どの程度一般的になる? Windows/Android は追従する?

AnycastによるCDN

- AnycastはTCPなどステートフルな通信には向いていないと言われていた
  - セッションの確立後に経路が変わると通信できなくなる
- が、Anycastでコンテンツ配信するCDNも珍しくなくなってきた
  - Cloudflare、Google Cloud CDN、Fastlyなど
  - 新しめのCDNサービスだとむしろAnycastの方が優勢?
- Anycast CDNは、エッジサーバへの経路制御だけでユーザを最適なノードに誘導できる
  - DNS (ECS)に頼る必要がない

CDNの効率化戦略

- エッジサーバの配置を頑張る
- 権威DNSサーバの動的応答を頑張る ← ここでECSが必要
- IXやprivate peerで頑張る
- 経路広報を頑張る

- CDNの方法によって頑張りどころの優先度が異なる
  - GSLB方式は権威DNSをかなり頑張る必要があって、ECSが非常に重要
  - Anycast方式はDNSが頑張らないので、他のところをより頑張る必要がある

ECSってどうよ?

- CDNからのコンテンツ配信において、ECSがないと効率が落ちることがある
  - DNSベースでトラフィックマネジメントしているCDN事業者
- ECSのプライバシー
- アプリケーション独自の名前解決はこれまで以上に一般的になる?
- そもそもコンテンツ配信もAnycastしているCDN屋さんであればECSは不要

- ECSってどうよ?