

RubyKaigi 2023での セキュアなDNSリゾルバの運用

— DoT/DoHとDDR —

Kasumi Hanazuki <hanazuki@kmc.gr.jp>

花月かすみ

- @京大マイコンクラブ(KMC)
- Rubyとインターネットがすき
- RubyKaigi NOC
 - 2017 広島
 - 2018 仙台
 - 2019 福岡
 - 2020 松本(中止)
 - 2022 津
 - 2023 松本
 - 2024 那覇(予定)



RubyKaigi

プログラミング言語Rubyと処理系の国際会議

- 地方巡業
- 参加者: 約1,200人
- 有志で会場Wi-Fiを構築・運用
 - アクセスポイント: 約50台
 - 同時接続: 約1,300台^(peak)
 - DNS(フルサービス): 530 qps^(peak), 370 qps^(mean)

(数字はRubyKaigi 2023実績)

京大マイコンクラブ(KMC) / AS59128

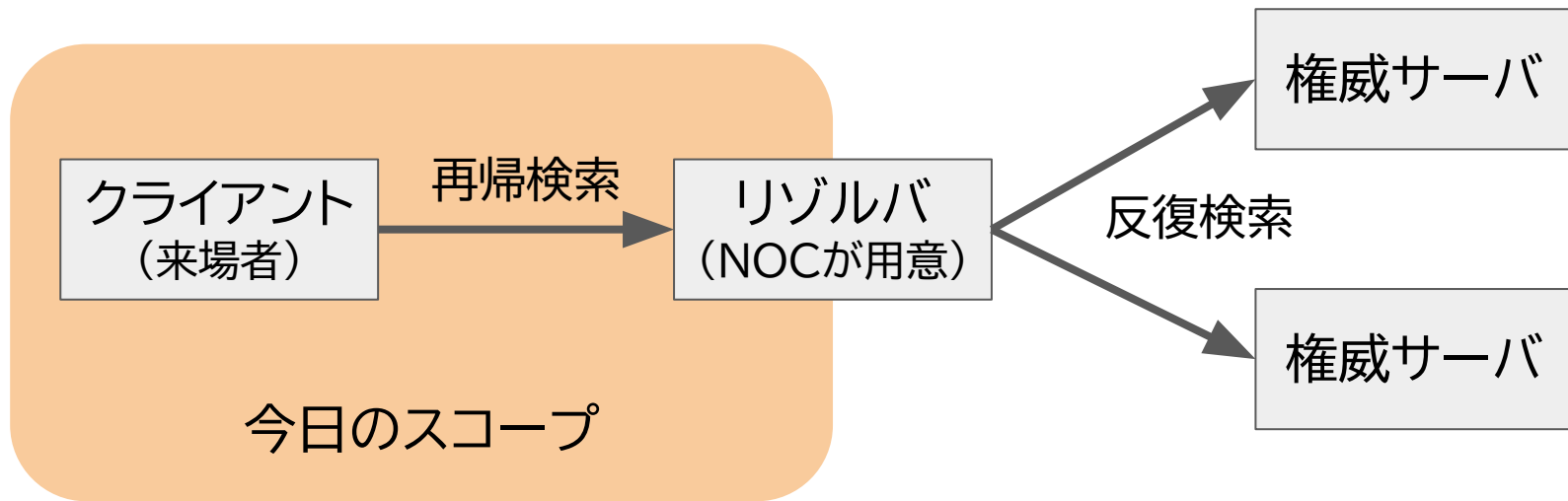
京都大学のマイコン(パソコン)なんでもサークル

- 1977: 設立
- 1991: PIアドレス割当(歴史的PI)
- 2016: AS運用開始
 - 上流: AS20473, AS59105, AS59103
- 2022-23:
RubyKaigiにインターネット接続を提供

DNSと暗号化DNS

DNSのしくみ

クライアントはリゾルバを通してドメインを検索する



公衆Wi-Fiの盗聴・改竄可能性

- WPA2 Personalは事前共有鍵(PSK)が公知の場合、盗聴・改竄に対して脆弱
- 転がしてあるケーブルは抜ける



平文DNSが
流れている！

暗号化DNSプロトコル

主要OS・
ブラウザに
実装済み

- DNS over TLS (DoT)
 - TLSで暗号化
- DNS over HTTPS (DoH)
 - 通例, HTTP/2またはHTTP/3が使われる
 - どちらもマルチストリームを実現するプロトコルで, クエリに対してレスポンスを順不同に返せる
 - TLSで暗号化

DNSから暗号化DNSへ

DNSから暗号化DNSへ

クライアントが暗号化DNSを使うように
自動構成するしくみが必要

- 従来のDHCPやIPv6 RA (RDNSS)は
リゾルバのIPアドレスのみクライアントに伝える
→ リゾルバがどのような暗号化に対応しているか分からない

日和見暗号化 (Opportunistic Encryption)

リゾルバが対応していそうなら、
クライアントが勝手に暗号化プロトコルにアップグレード

- 853/tcpにTLS接続してみて、
 - 接続できれば暗号化通信をする
 - 接続できなければ平文通信にフォールバック
- DoHへのアップグレードは難しい
 - HTTPのパスが分からないため

Android 9+
(2018-08)

systemd 239+
(2018-01)
Disabled by default

Adaptive DNS Discovery

クライアントを暗号化プロトコルに明示的に誘導する

- DNR (RFC 9462)
 - DHCPやIPv6 RAを拡張してクライアントに暗号化リゾルバを紹介する
- DDR (RFC 9463)
 - リゾルバとクライアントの間で暗号化プロトコルをネゴシエーションする

Windows Insider
25982
(先月出た)

macOS* 13+
iOS/iPadOS 16+
(2022-10)

Discovery of Designated Resolvers (DDR)

- 初期状態: クライアントは「非暗号化リゾルバのIPアドレス」だけ知っている
- リゾルバは特殊用途ドメイン名“resolver.arpa.”で自身の対応プロトコルを公開する
 - “arpa.”の権威サーバが答えるわけではない
- クライアントはこの情報をもとに接続プロトコルを選ぶ

サービスバインディング・レコード

_dns.resolver.arpa.

IN SVCB 1 resolver.rubykaigi.net. (

優先度

alpn="h3,h2"

対応プロトコル

dohpath="/dns-query{?dns}")

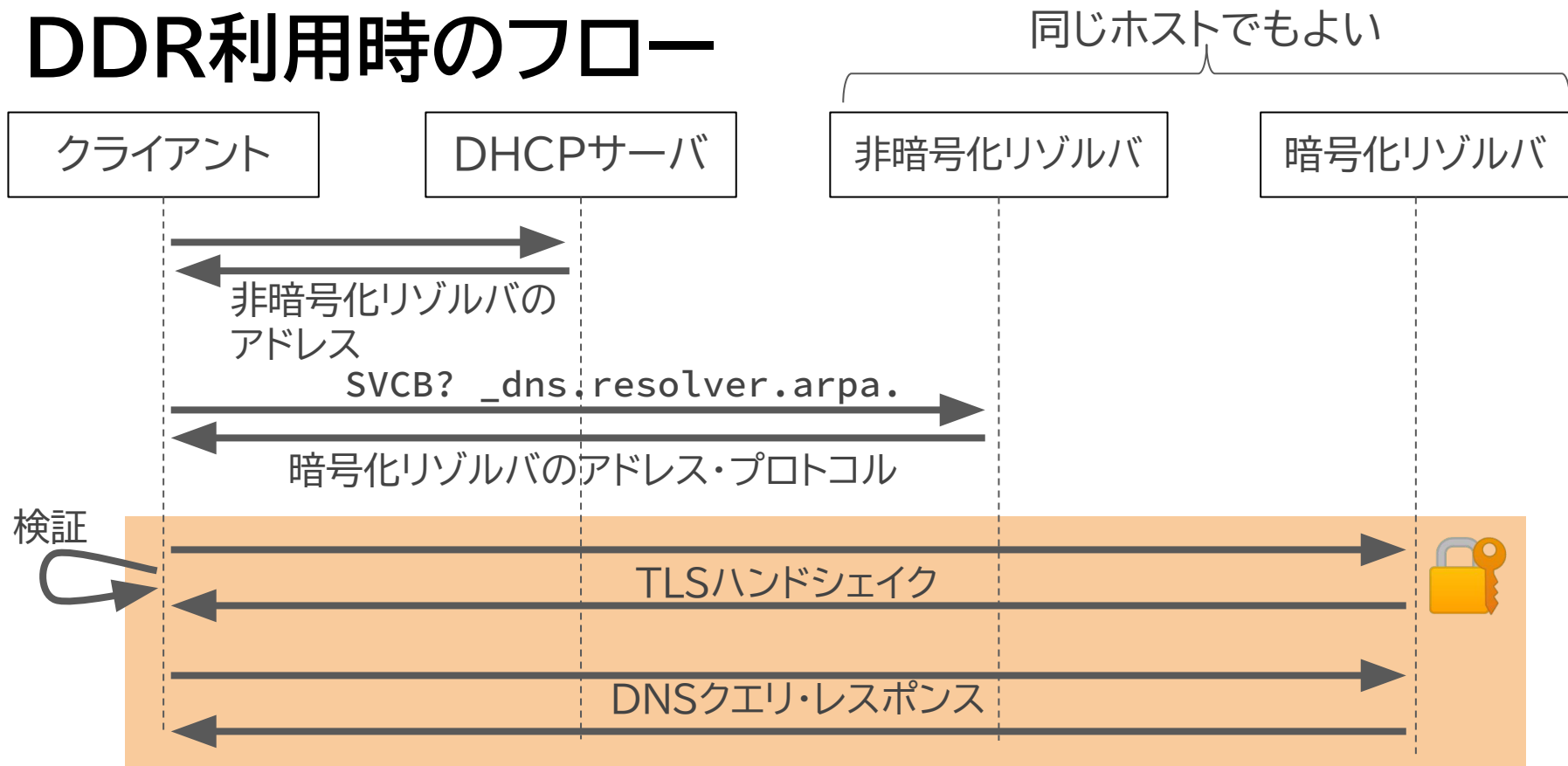
IN SVCB 2 resolver.rubykaigi.net. (

alpn="dot")

パラメータで
DoHのパスを指定

ターゲット
A/AAAAを引くと
暗号化リゾルバの
アドレスが分かる

DDR利用時のフロー



暗号化リゾルバの検証

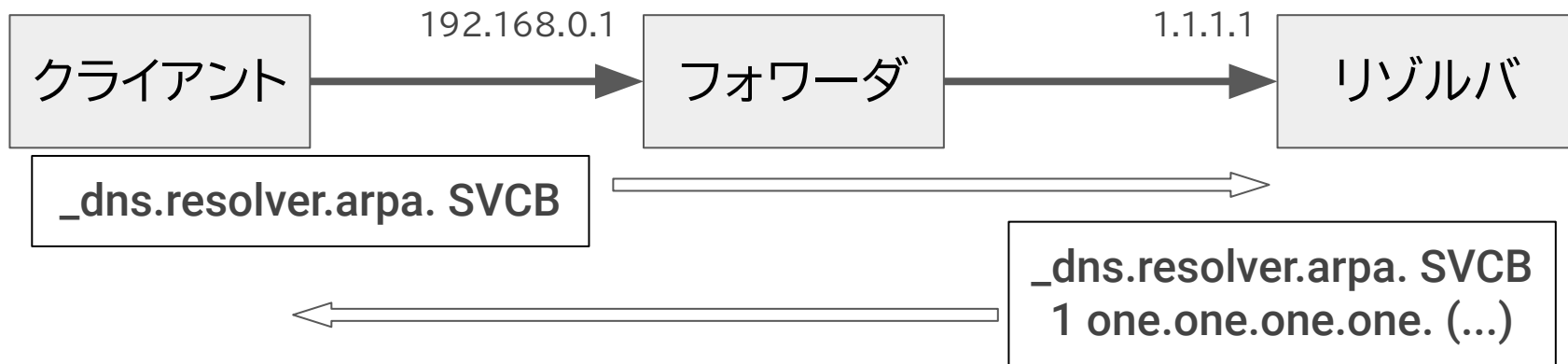
SVCBで知った暗号化リゾルバを信頼して利用する条件

- Verified Discovery
 - a. 証明書がトラストアンカーまで遡って検証可能
 - b. 証明書のSANが「非暗号化リゾルバのアドレス」を含む
- Opportunistic Discovery
 - a. 「非暗号化リゾルバのアドレス」がプライベートアドレス
 - b. 「非暗号化リゾルバのアドレス」と「暗号化リゾルバのアドレス」が一致

Appleデバイスには
実装されていない？
追試おねがいします

中間にDNSフォワーダがある場合

- 非暗号化リゾルバのアドレス \neq サーバ証明書のSAN
→ Verified Discoveryではアップグレードされない
- 非暗号化リゾルバのアドレス \neq 暗号化リゾルバのアドレス
→ Opportunistic Discoveryでもアップグレードされない



DDRの限界

- 防げる攻撃
 - パッシブな盗聴
 - 正規のリゾルバへのなりすまし(Verified Discoveryの場合)
- 防げない攻撃
 - SVCBクエリを妨害して平文通信へダウングレード
 - 経路ハイジャックでCAを騙して証明書を不正取得
 - 野良DHCP
 - ハニーポットWi-Fi

多層防御が必要

RubyKaigi 2023での 暗号化DNSの実装

RubyKaigi 2023のリゾルバ

AppleデバイスにDDRが実装されたと知り^[WWDC]
DNSを暗号化する実験を思いつく

- DoT, DoH (HTTP/2, HTTP/3)
- DDR(2023-05当時ドラフト)
- ~~DNR~~(当時まだオプション番号が未割り当て・クライアント実装がない)

[WWDC]: <https://developer.apple.com/videos/play/wwdc2022/10079/>

使用したサーバソフトウェア

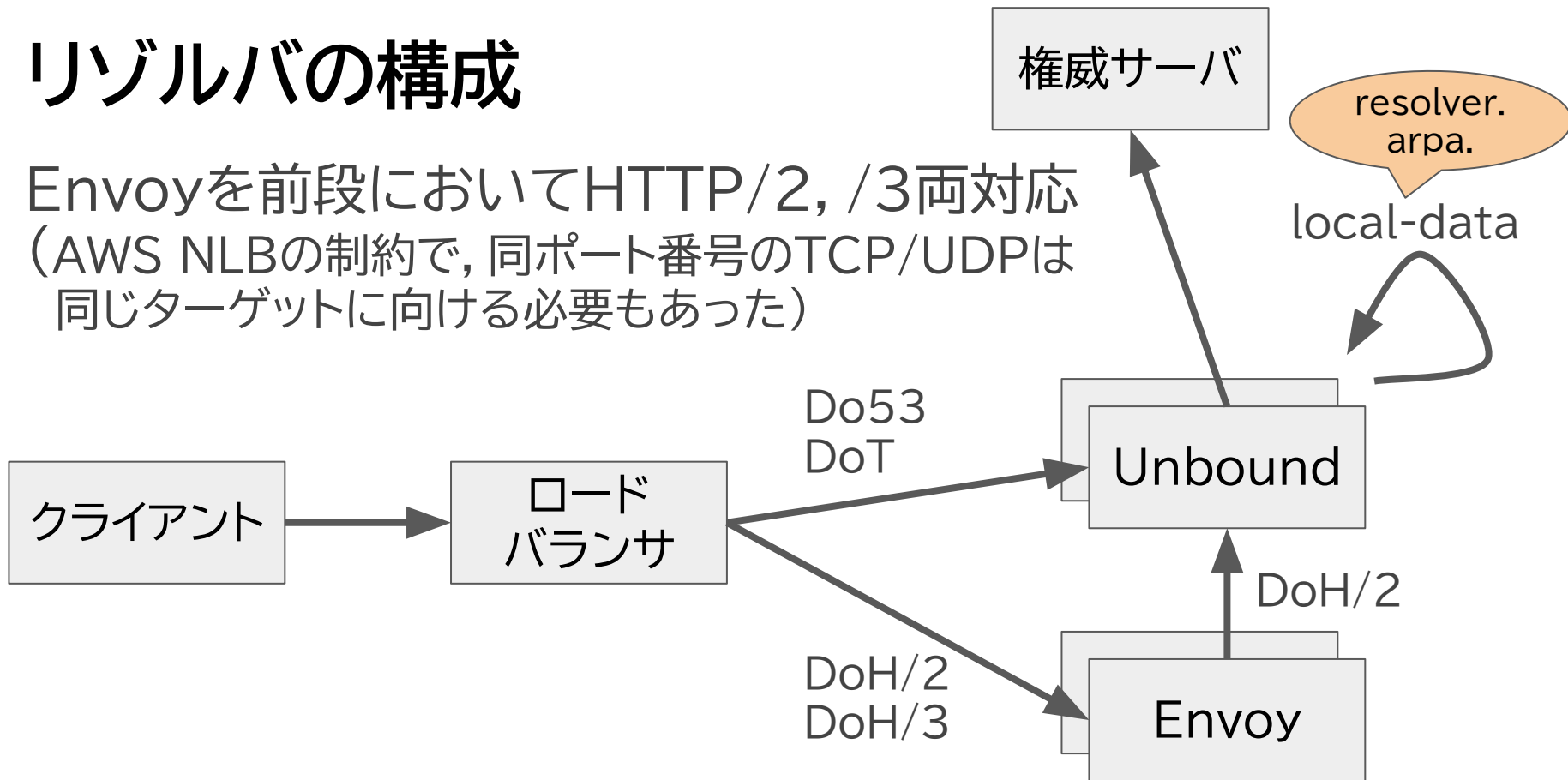
- Unbound
 - DoTとDoH/2に対応するDNSリゾルバ
 - DNSリゾルバとして折り紙付き
 - 一方, DoHは?
 - Ubuntu 22.04に含まれるv1.13.1では壊れていた
(最新版では修正済)
- Envoy
 - HTTP/2と/3に対応するHTTPプロキシ・ロードバランサ
 - 巨大トラフィックを捌く実績あり

まだ枯れてなさそう...

汎用コンポーネントを
使えるHTTPの旨味

リゾルバの構成

Envoyを前段においてHTTP/2, /3両対応
(AWS NLBの制約で, 同ポート番号のTCP/UDPは
同じターゲットに向ける必要もあった)



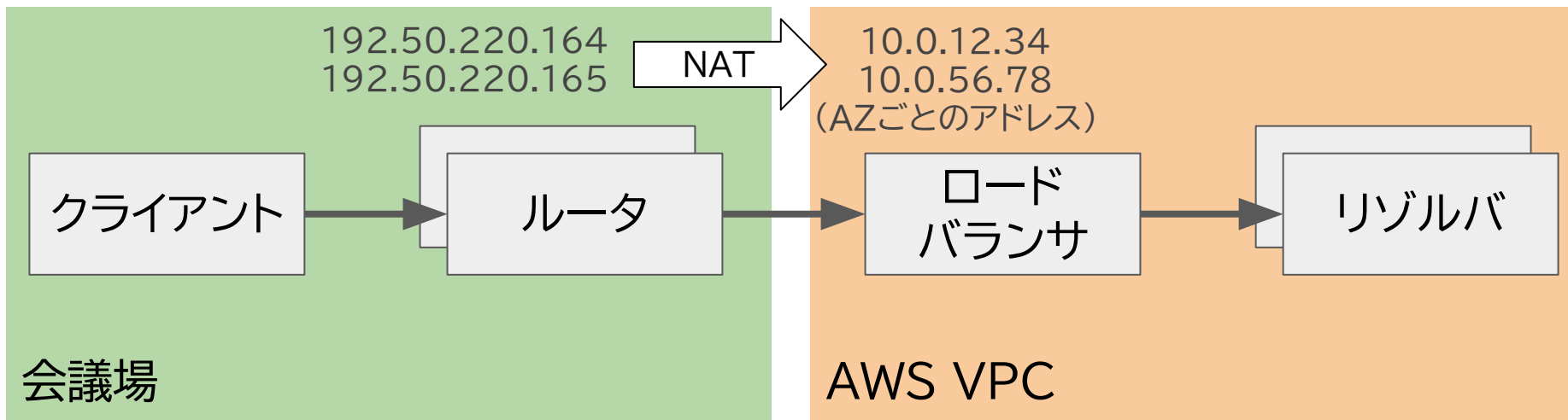
リゾルバのTLSサーバ証明書

DDR対応には、subjectAltName SANにIPアドレスを含むサーバ証明書が必要
また、PKIで検証できる必要がある

- パブリックCAはパブリックIPのSANのみ証明する
→ リゾルバはパブリックIPアドレスで運用する必要
(リゾルバ自体はインターネットから到達可能でなくともよい)
- 社内環境等では、プライベートCAを使って
プライベートIPアドレスで運用可能？(未検証)

パブリックIPアドレスでリゾルバを運用

会場ルータでパブリック→プライベートのNATをしていた



RubyKaigi 2023での実験結果

1/3から1/2のトランザクションを暗号化

30分ごとに集計した
プロトコル別のクエリ割合

Matzのキーノートを
PCで実況？

PCを閉じて
スマホを使っている？

プロトコル	講演中	昼休憩
平文	62%	43%
DoT	6%	9%
DoH/2	30%	46%
DoH/3	3%	3%

Android

macOS/iOS

macOS/iOSが
たまにHTTP/3を
使う(詳細不明)

Day1

10:30-11:00

Day1

12:30-13:00

DoTが少ないような

同時に802.1X認証の実験もしていた

- Androidは選択肢の多いフォームの入力を要求
→ 難しかったのではないか(予想)
- Google製以外の端末でも初期設定でOE有効になっている？
(未調査)

rktmp

EAP method

PEAP

Phase 2 authentication

MSCHAPV2

CA certificate

Use system certificates

Online certificate status

Do not verify

Domain

radius.rubykaigi.net

Identity

rubykaigi

Anonymous identity

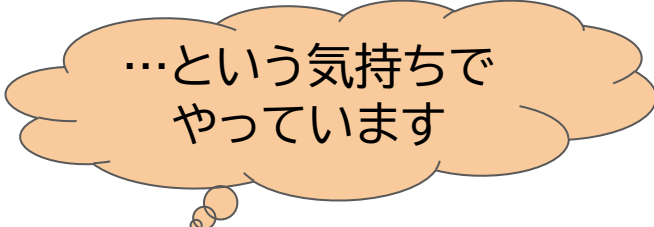
Password

.....

おわりに

それって意味あるの？

公衆Wi-Fiにおいて…

A thought bubble with an orange gradient and a black outline, containing the text "...という気持ちで やっています".

…という気持ちで
やっています

- (プライバシーを気にする)管理者:
 - 利用者を守るために暗号化リゾルバを提供したい
 - 特定の第三者(公衆DNS)に情報を横流ししたくない
- (プライバシーを気にする)利用者:
 - そもそも管理者は攻撃者と同じくらい信用できない
→ 大手の公衆DNSを使う

それって意味あるの？ ②

ご意見・ご感想
うかがいたいです

- オフィスLAN
 - 利用者と管理者の利害は一致しているはず？
- 商用ISP
 - リゾルバから見た直接のクライアントはCPE(ルータ)？
→ 対応はまだまだ先？
 - TLS化の計算負荷は大きい？

Acknowledgement

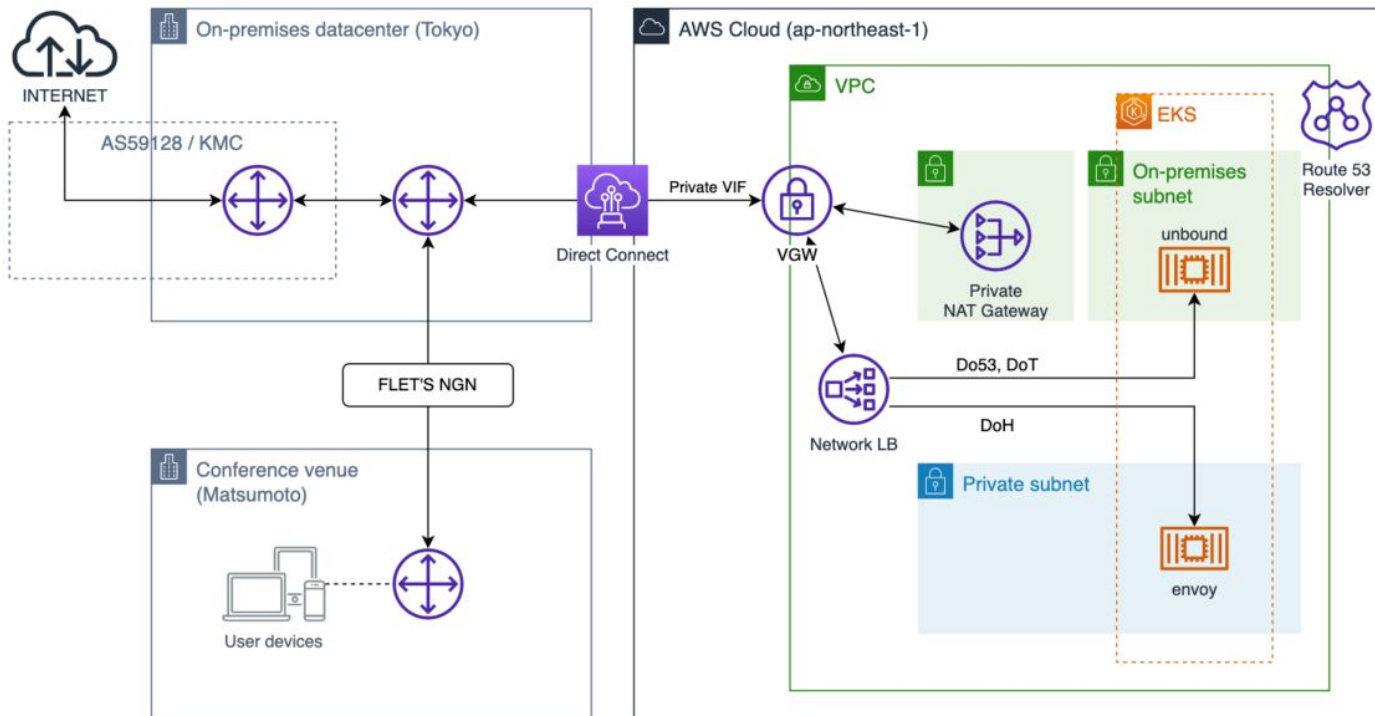
- @sorah, RubyKaigi Organizer & NOC Lead
 - L1-L4設計, L2-L4構築, その他すべて
- NOCチームメイトのみなさん
 - L1構築, ブログ記事・発表資料のレビュー
- RubyKaigiスポンサー各社

関連記事

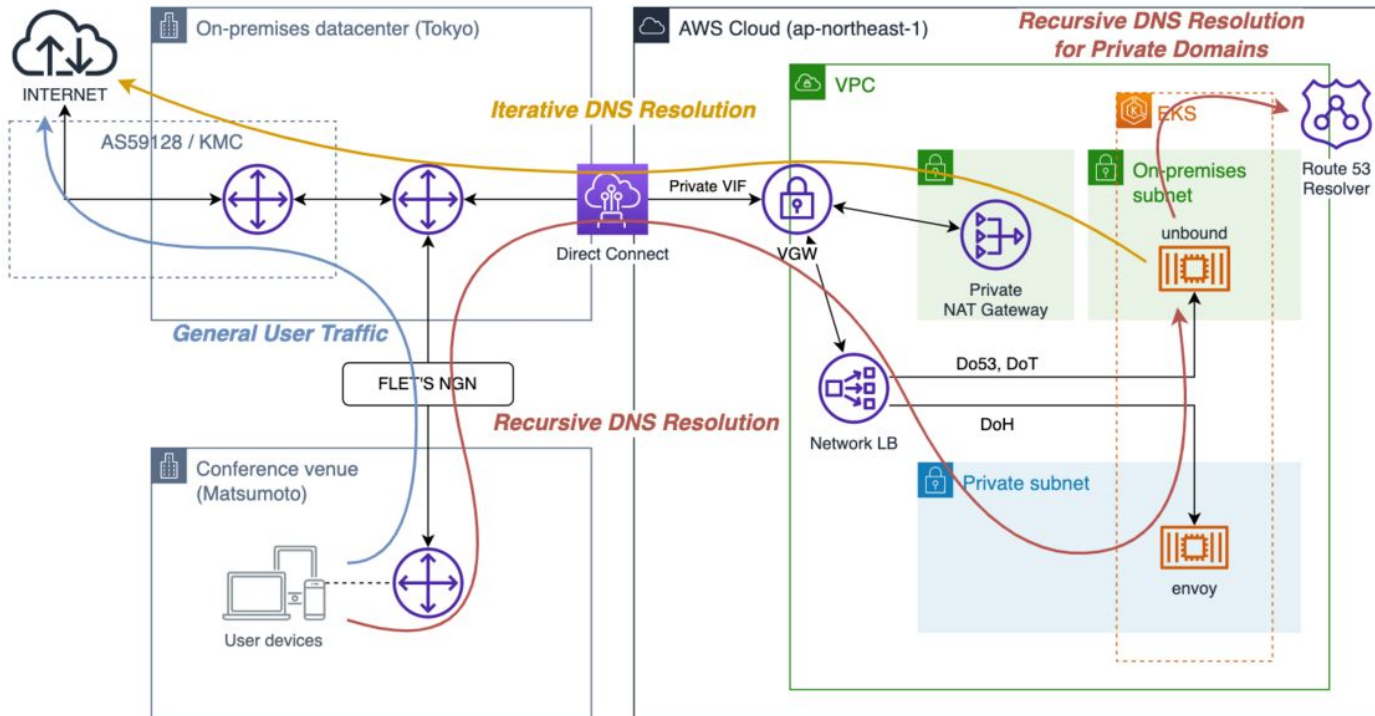
- RubyKaigi 2023でのセキュアなDNSリゾルバの運用
— DNS-over-HTTPSとDDR (@hanazuki)
 - <https://blog.kmc.gr.jp/entry/2023/05/10/165300>
- RubyKaigi 2023 Wi-Fi: 足回り徹底解説 (@sorah)
 - <https://techlife.cookpad.com/entry/2023/05/31/113000>
- ソースコード
 - <https://github.com/ruby-no-kai/rubykaigi-nw>

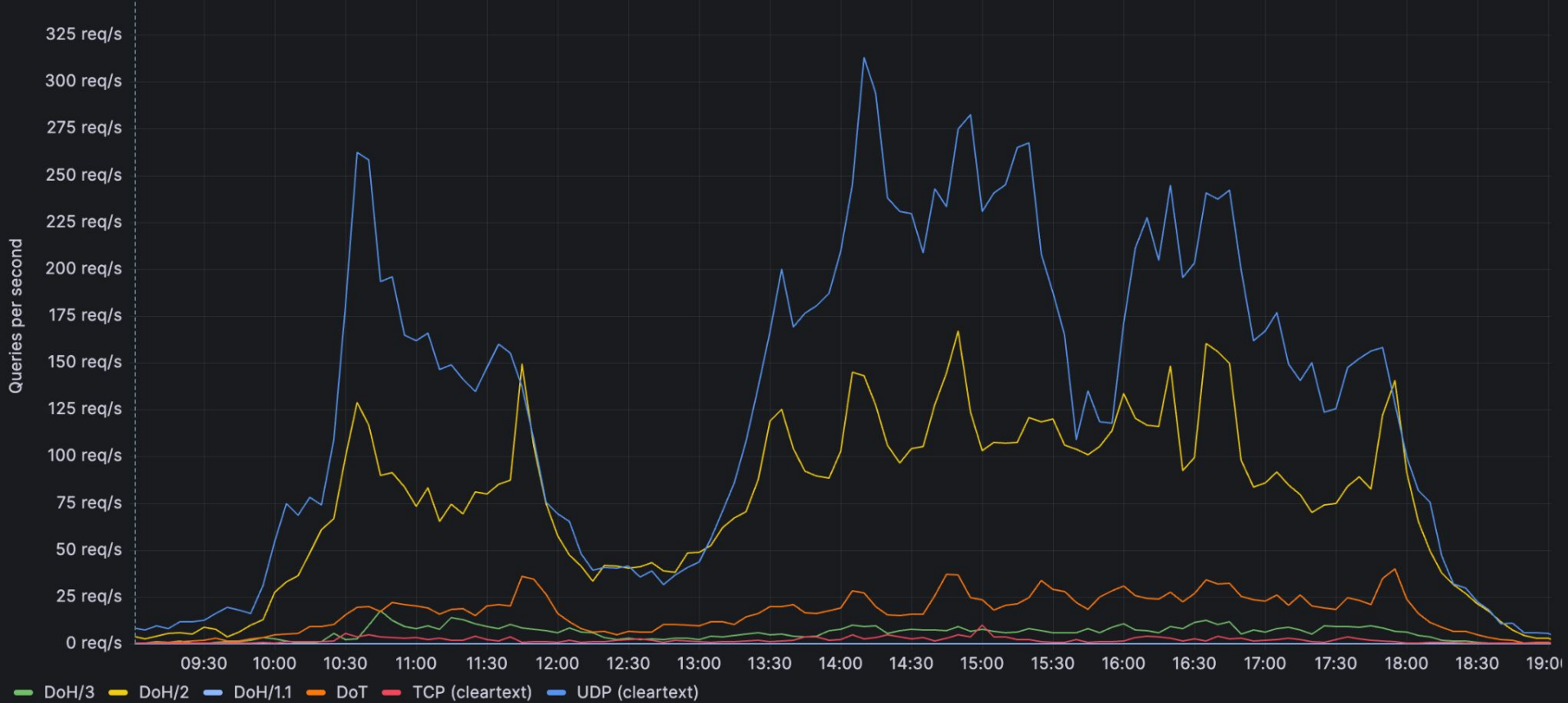
おまけ

RubyKaigi 2023ネットワークの概略



RubyKaigi 2023ネットワークの概略





クエリ数: 平文UDP(青) vs DoH/2(黄) vs DoT(橙)

[Grafana](#)