フルサービスリゾルバの
反復問い合わせクエリの可視化

2022年6月24日

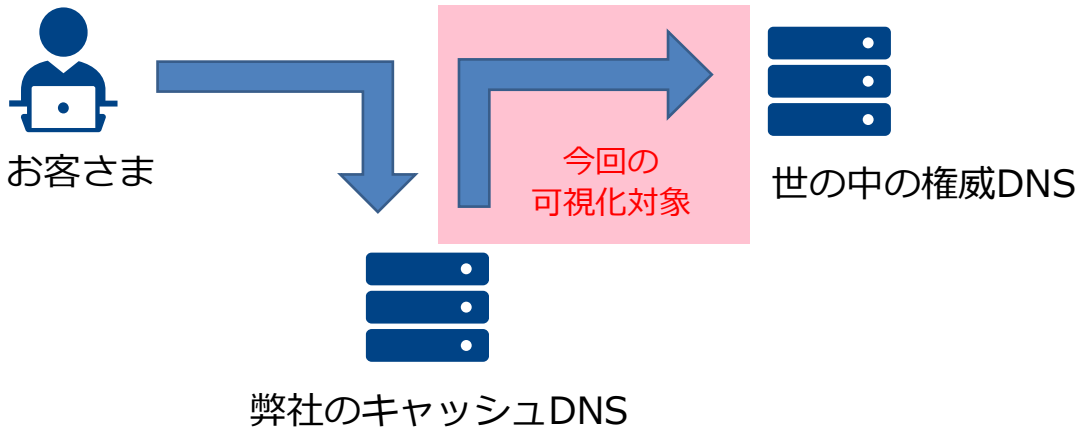
NTTコミュニケーションズ株式会社

小坂　良太

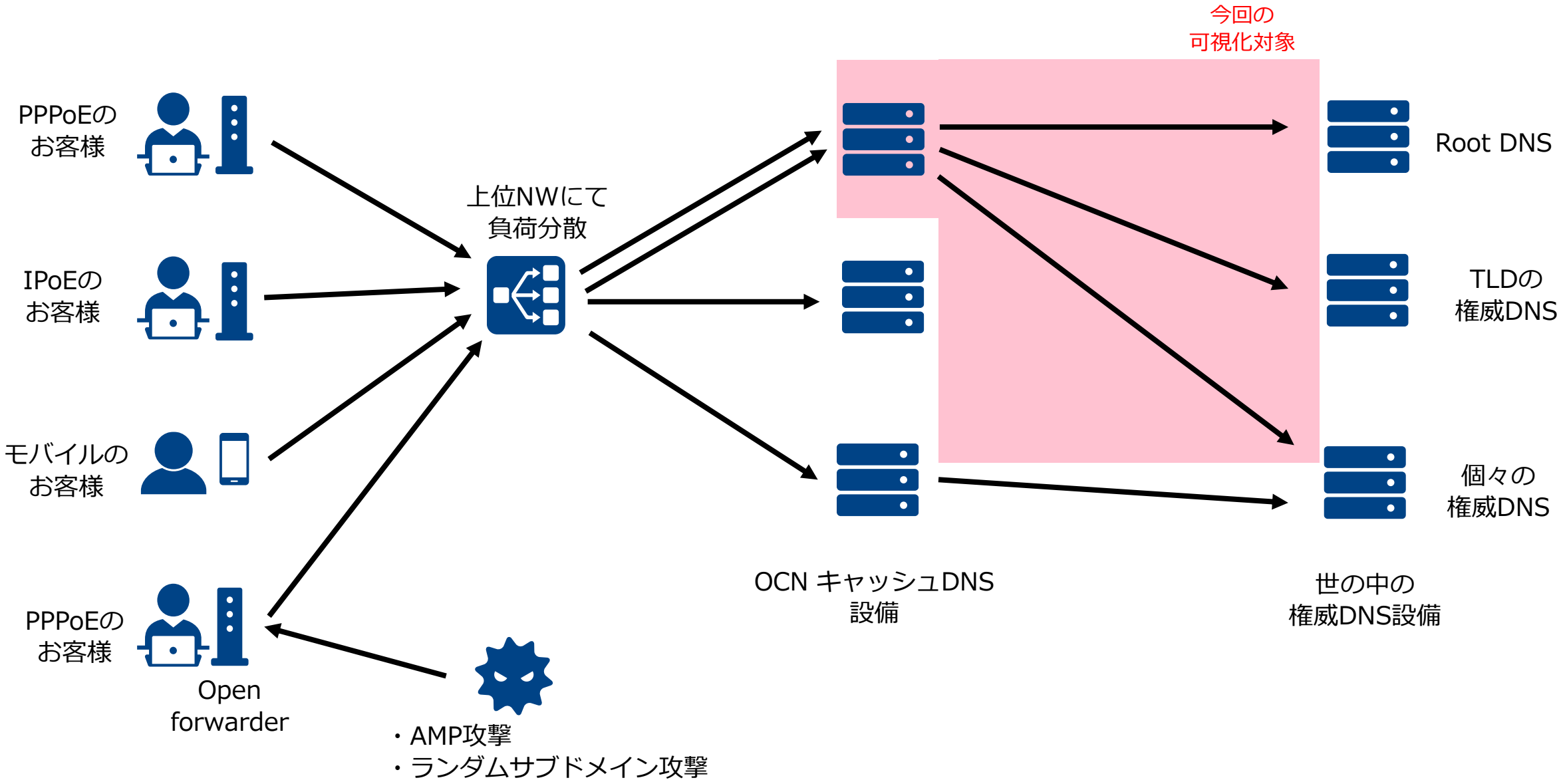
自己紹介

・名前：小坂　良太
・所属：NTTコミュニケーションズ株式会社
・仕事：ISPとして提供しているフルサービスリゾルバ(キャッシュDNS)と
　　権威DNSの設計および開発　(回線サービス名：OCN)

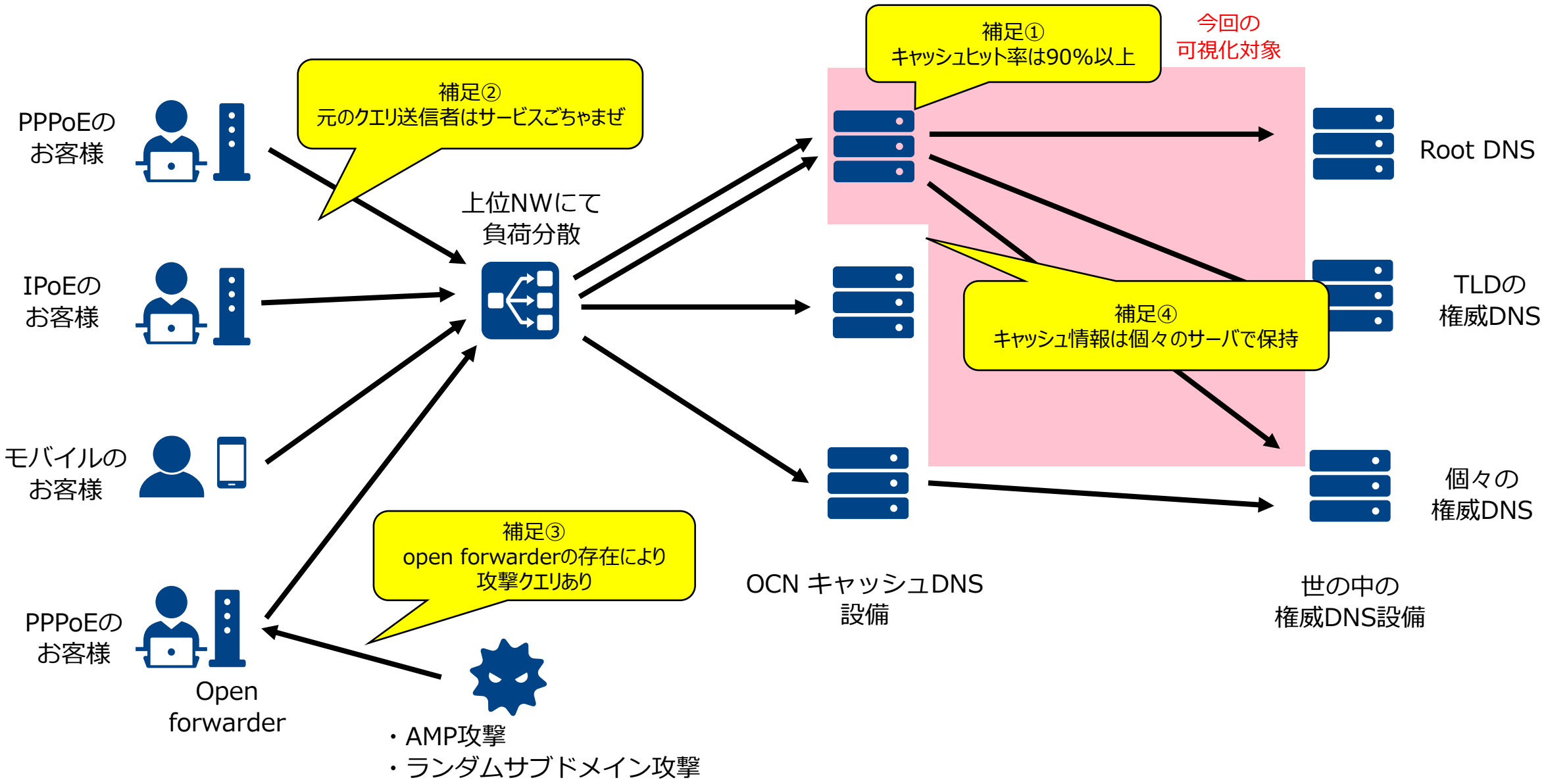
・昨年度の発表内容
- キャッシュDNSのロードバランサーなし構成について　(DNS Summer Day 2021)
- フルサービスリゾルバ利用状況　(Internet Week 2021)
- DNSの可視化検討　(JANOG49 Meeting)



可視化の対象について　～全体像～

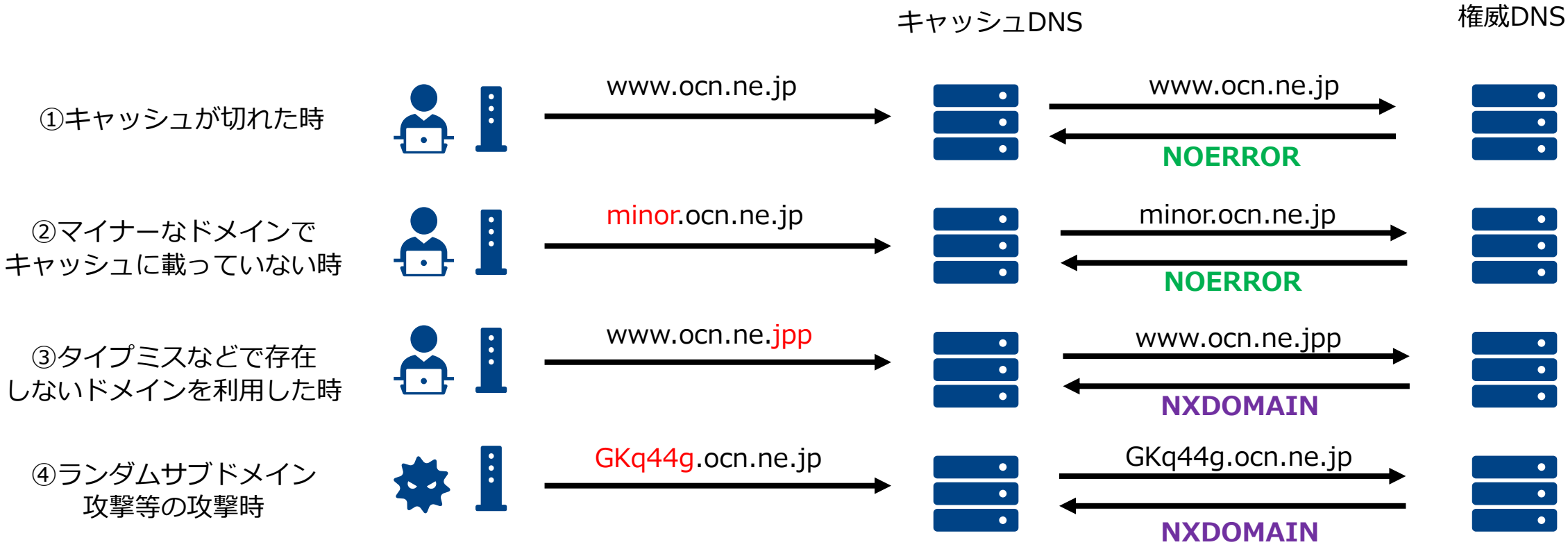


可視化の対象について　～補足～



今回の可視化のモチベーションについて

■反復問い合わせが発生するパターン

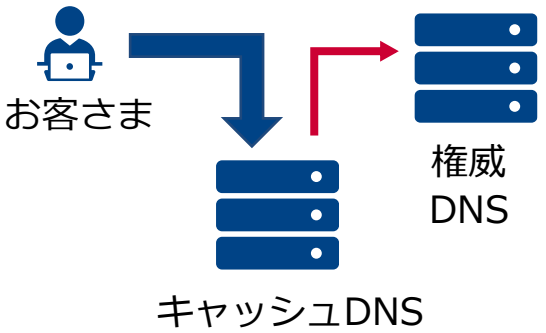


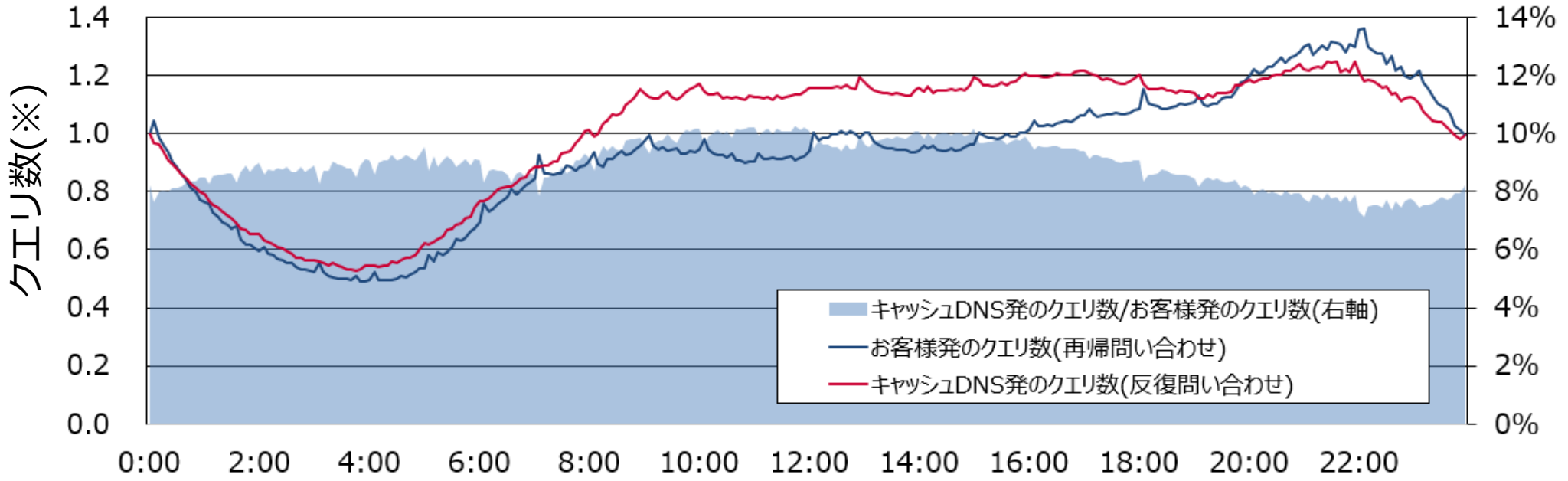
- **NOERROR**と**NXDOMAIN**のレスポンス数を知ることで攻撃クエリの量を把握したい
- root DNS宛のクエリ数を知ることでRFC8806によって負荷がどれだけ下がるかを把握したい

再帰問い合わせと反復問い合わせのクエリ数

●お客様　⇒　　OCNキャッシュDNS宛のクエリと
　OCNキャッシュDNS　⇒　権威DNS宛のクエリをカウント
●お客様発は21～22時にピークがあり、日勤帯と比べるとクエリ数はより非常に多い
●キャッシュDNS発もピーク時間帯は同じだが、日勤帯とそこまで変わらない
　⇒**お客様からのクエリ数がどれだけ多くても反復問い合わせはそこまで増えない**
●比率(右軸)は8～10%程度なのでキャッシュヒット率と比較しても妥当？
　⇒キャッシュミスがあっても1～2回の非再帰問い合わせで名前解決結果が得られる

クエリ数は10:1程度

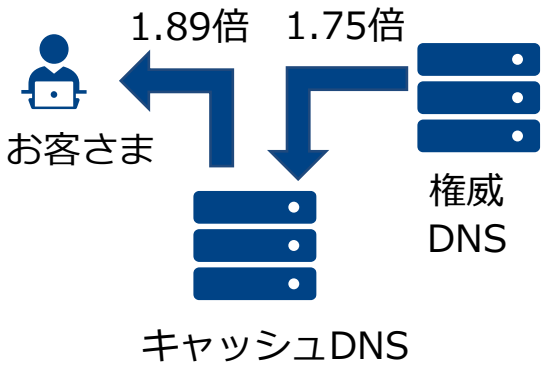


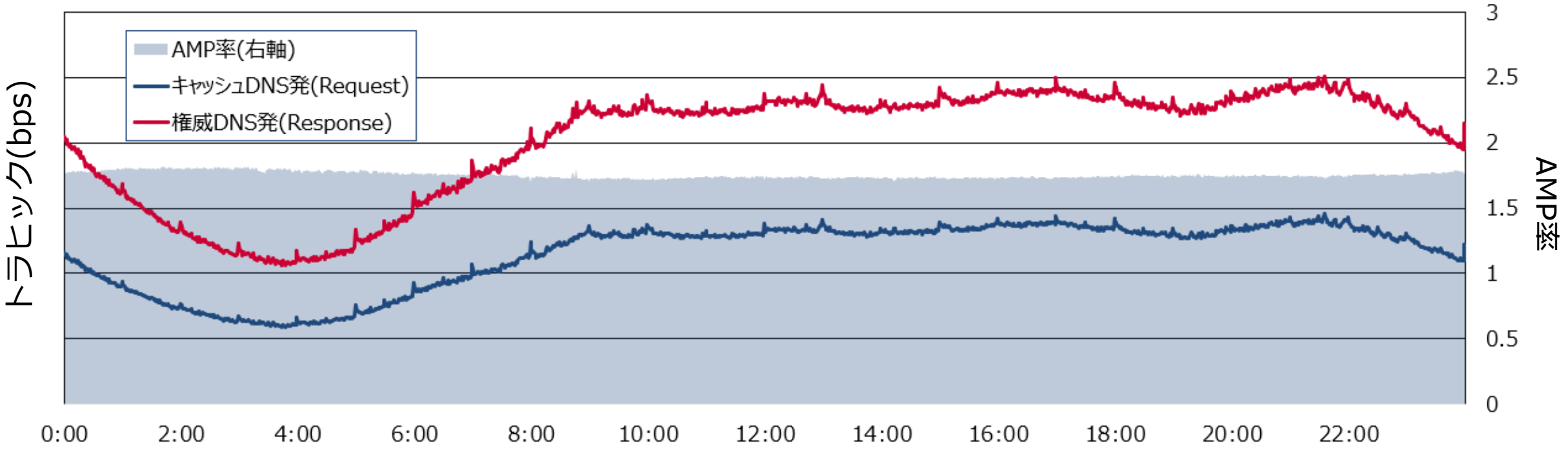


(※)0:00のそれぞのクエリ数を「1」として正規化

反復問い合わせのクエリのAMP率

●OCNキャッシュDNS～権威DNS間のAMP率を測定(bpsから単純計算)
●1日を通して大きな変化はなく約1.75倍
  ✓ お客様～キャッシュDNS間を別途確認した所、約1.89倍
  ✓ 皆が使うドメイン(キャッシュヒットするドメイン) は若干AMP率が高い

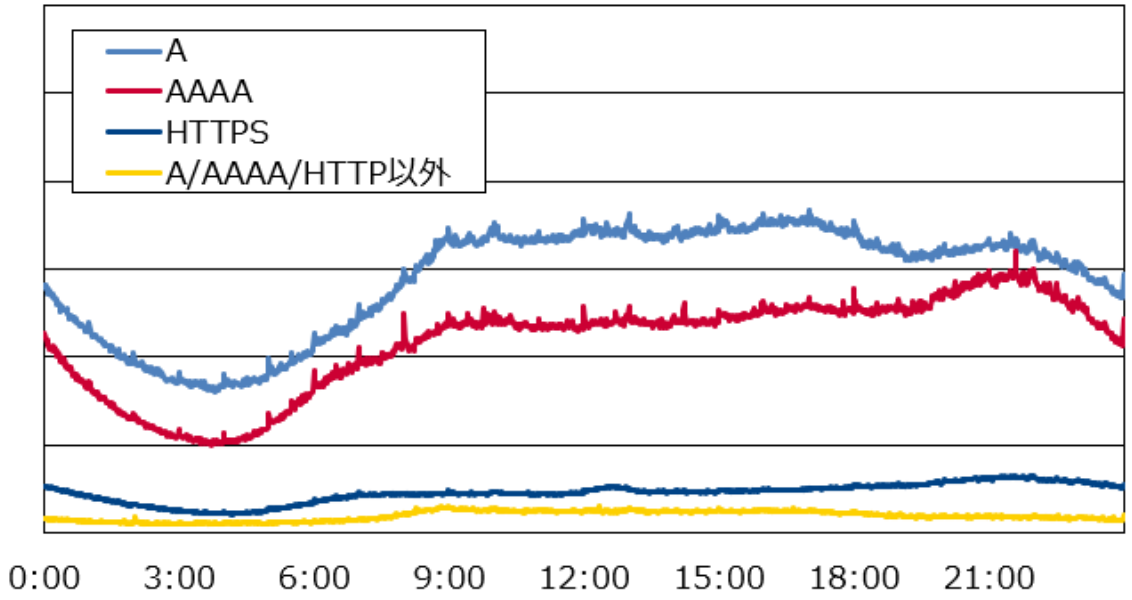




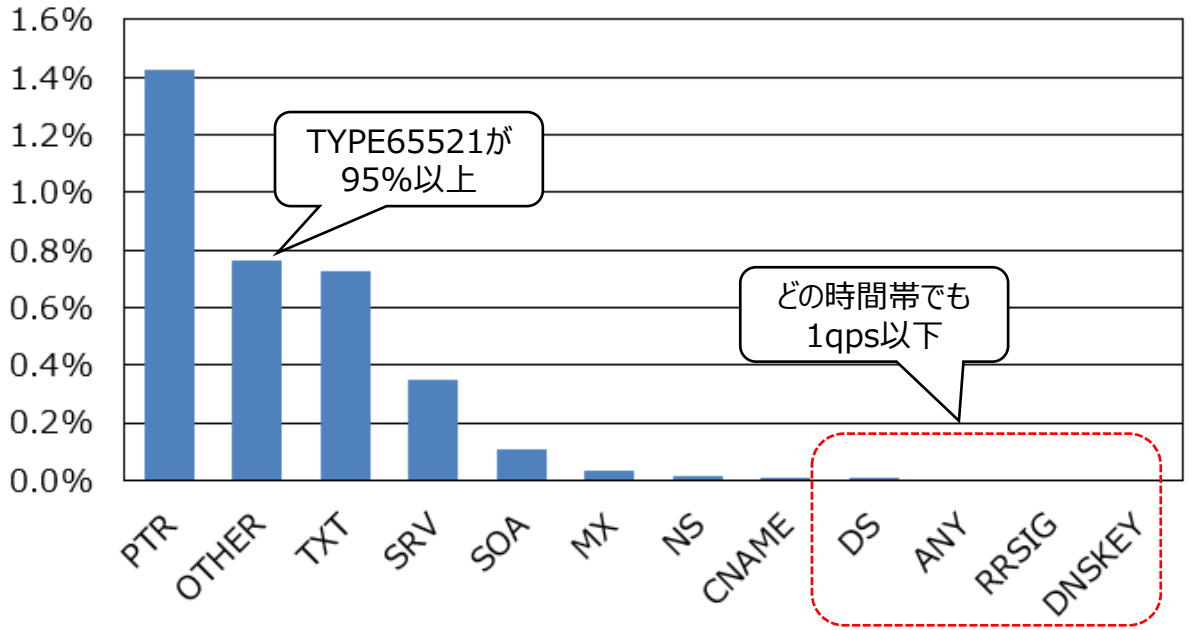
反復問い合わせのクエリタイプ

- A/AAAA/HTTPSレコードで総クエリの96%を占める
  - ✓ Aレコード：50%　AAAAレコード：38%　HTTPSレコード：8%　左記以外：4%
  - ✓ 18:00以降はAレコードに対するクエリ数が減少傾向
- TTLを長く設定されるNSレコードやキャッシュヒットしやすいANYタイプはクエリ数が少ない
- 割り当てがされていないTYPE65521のクエリが意外と多い

■クエリタイプ毎のクエリ数



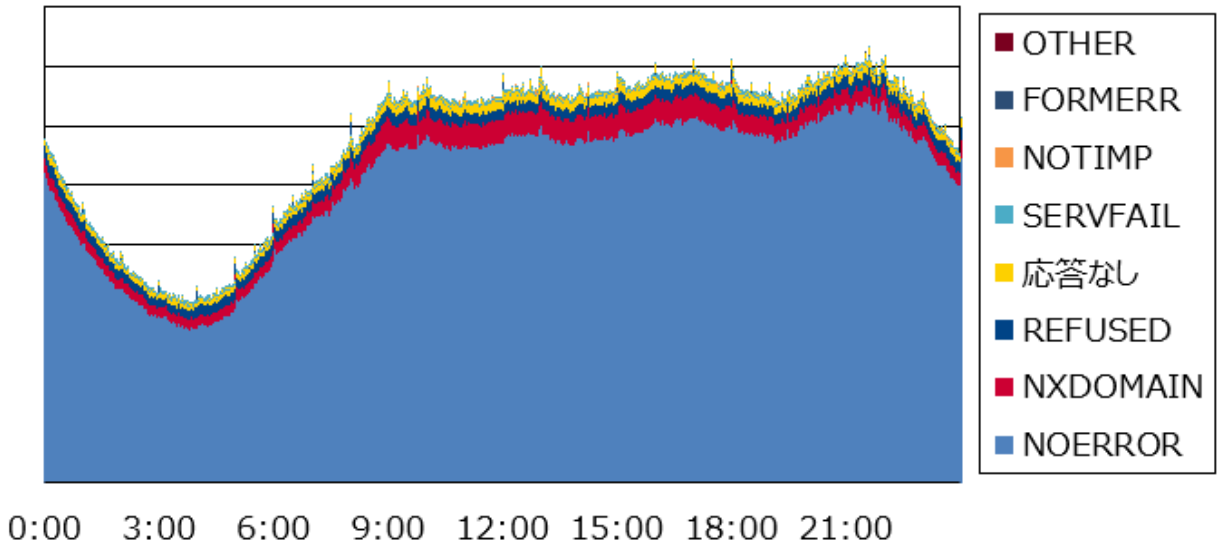
■A/AAAA/HTTPS以外のクエリ数(総クエリに対する割合)



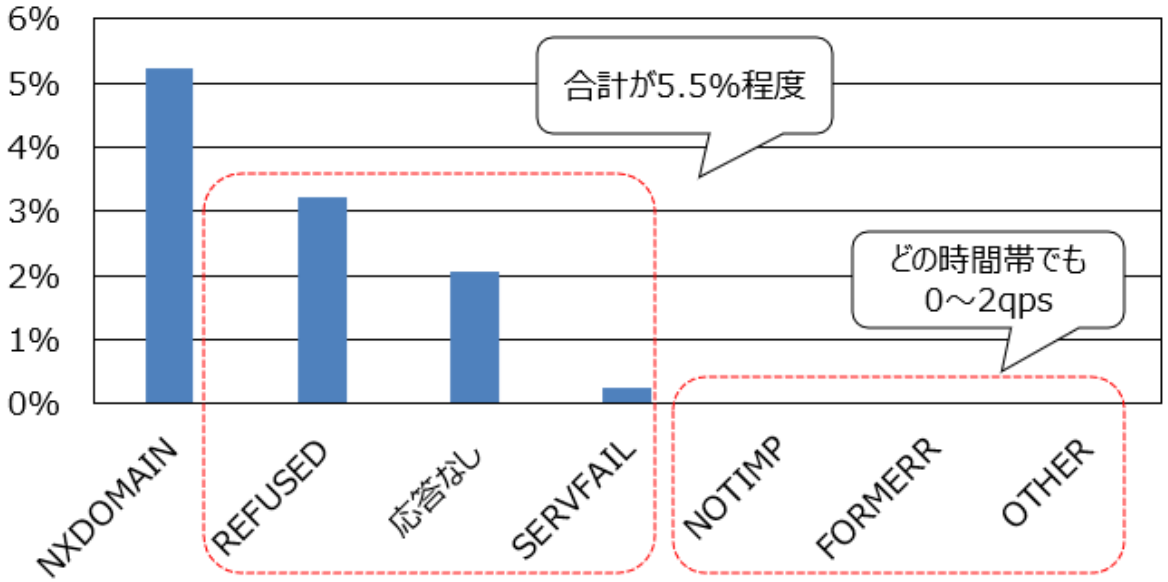
反復問い合わせクエリに対する応答コード

- ●権威DNSからのレスポンスに含まれる応答コードをカウント
  - ✓ また、(レクエスト数－レスポンス数)を『応答なし』の数として集計
- ●NOERRORが89%、NXDOMAINが5%
  - ⇒ランダムサブドメイン攻撃によるクエリ増はあまりない？
  - ⇒TTLの短いドメインが多く、頻繁に権威DNSに聞きに行っている？
- ●REFUSED/SERVFAIL/応答なしの合計が5.5%なのでlame delegationなドメイン(権威DNS)の数は多い

■応答コード毎のレスポンス数(積み上げグラフ)



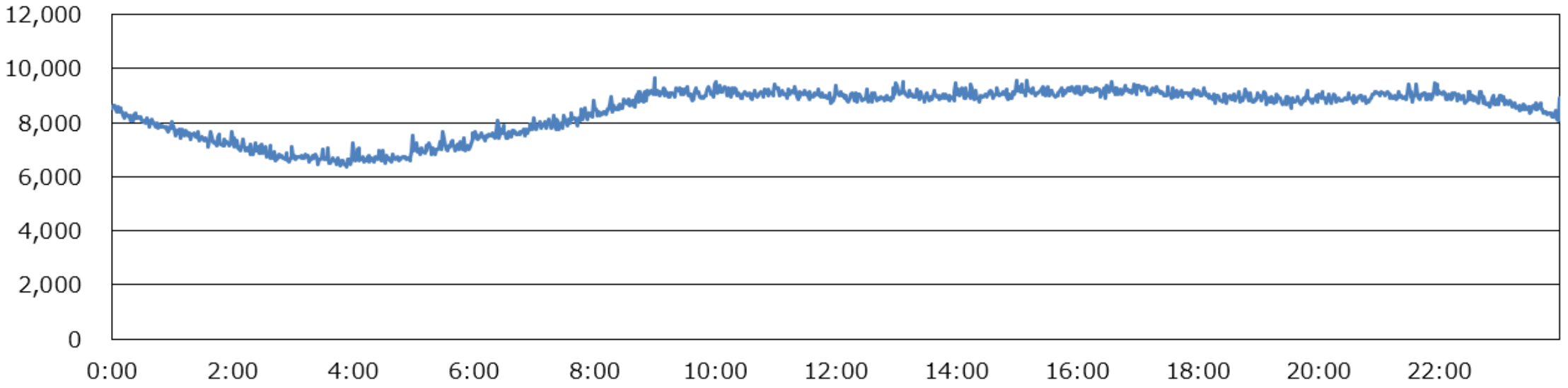
■NOERROR以外のレスポンス数
(総レスポンスに対する割合)



キャッシュDNSから見た権威DNSの数(IP数)

- 1分毎にクエリの送信先(権威DNSのIP)を集計
- 1日を通してのユニークIP数は不明だが、1分毎の場合は最大でも1万IP弱
  - また本集計はキャッシュDNS 1台に対してなので基盤全体で集計するとユニークIPは更に多い
  - 1分間のクエリ数と比較すると1/10以下なので、1分間で同じ権威DNSに何度も問い合わせしている
    ⇒常に何らかのドメインはTTL切れを起こしている＆そのドメイン数はそこそこ多いと推測

■キャッシュDNSから見た宛先IP数

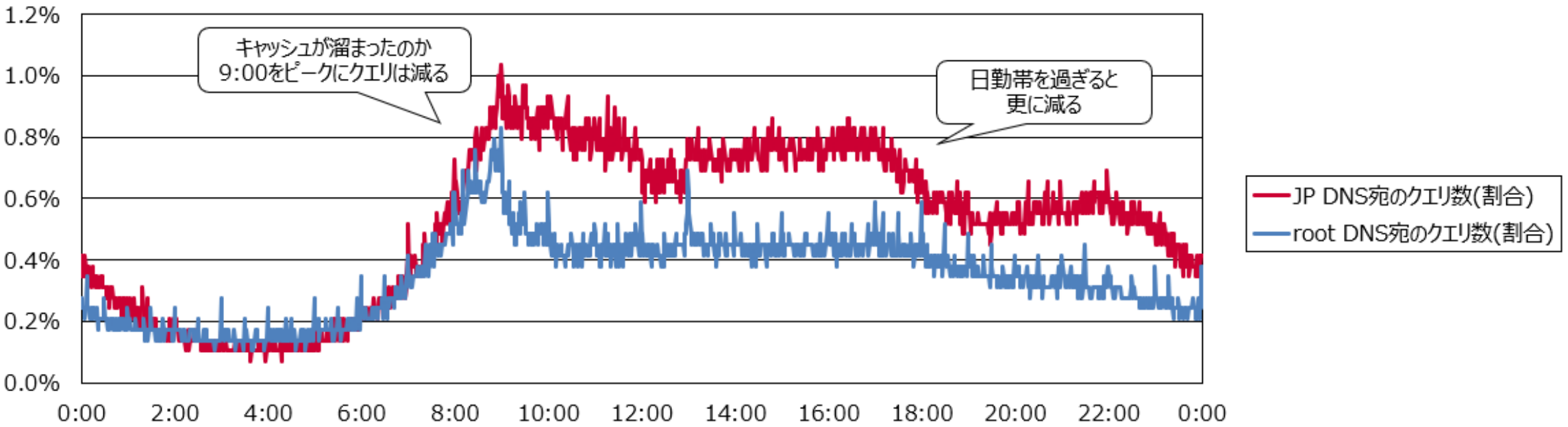


Root DNS及びJP DNSに送信するクエリ数

- Root DNS(a～m.root-servers.net.)およびJP DNS(a～h.dns.jp.)に送信するクエリ数をカウント
- いずれも1日を通して1%以下とクエリ数は非常に少ない(※)
  - キャッシュ(ネガティブキャッシュ含む)がしっかり効いている
  - 本資料p7の通りNOERROR率も高いためやはり攻撃クエリは少なそう
  - RFC8806に従って内部にルートゾーンを保持しても負荷削減効果の方はあまり期待できない

■総クエリ数に占めるRoot DNS及びJP DNSに送信するクエリ数の割合

(※)あくまでキャッシュDNSの視点です
権威DNS運用者からすると塵も積もって山となります



まとめ

・再帰問い合わせと反復問い合わせのクエリ数
⇒ 反復問い合わせのクエリ数はお客様からのクエリ数の約8～10%ほど

・反復問い合わせのクエリのAMP率
⇒ 平均1.75倍と大きくAMPとなるような傾向は見られなかった

・反復問い合わせのクエリタイプ
⇒ A/AAAA/HTTPSがやはり多く、一方でNSやANYは想定より少なかった

・反復問い合わせクエリに対する応答コード
⇒ **NOERRORが89%を占めており、攻撃クエリはあまり見られなかった**
一方でREFUSED/SERVFAIL/応答なしが5%以上と権威DNSの設定ミスは想定より多く見られた

・キャッシュDNSから見た権威DNSの数(IP数)
⇒ クエリ数と比較するとIP数は1/10と少なかった

・ Root DNS及びJP DNSに送信するクエリ数
⇒ キャッシュが効いており、root DNS宛のクエリは少なかった
RFC8806を採用しても負荷を下げる効果は小さいと考えられる