public DNSとプライバシー
DoH/DoTとISPのフルリゾルバ

日本ネットワークイネイブラー株式会社
石田慶樹

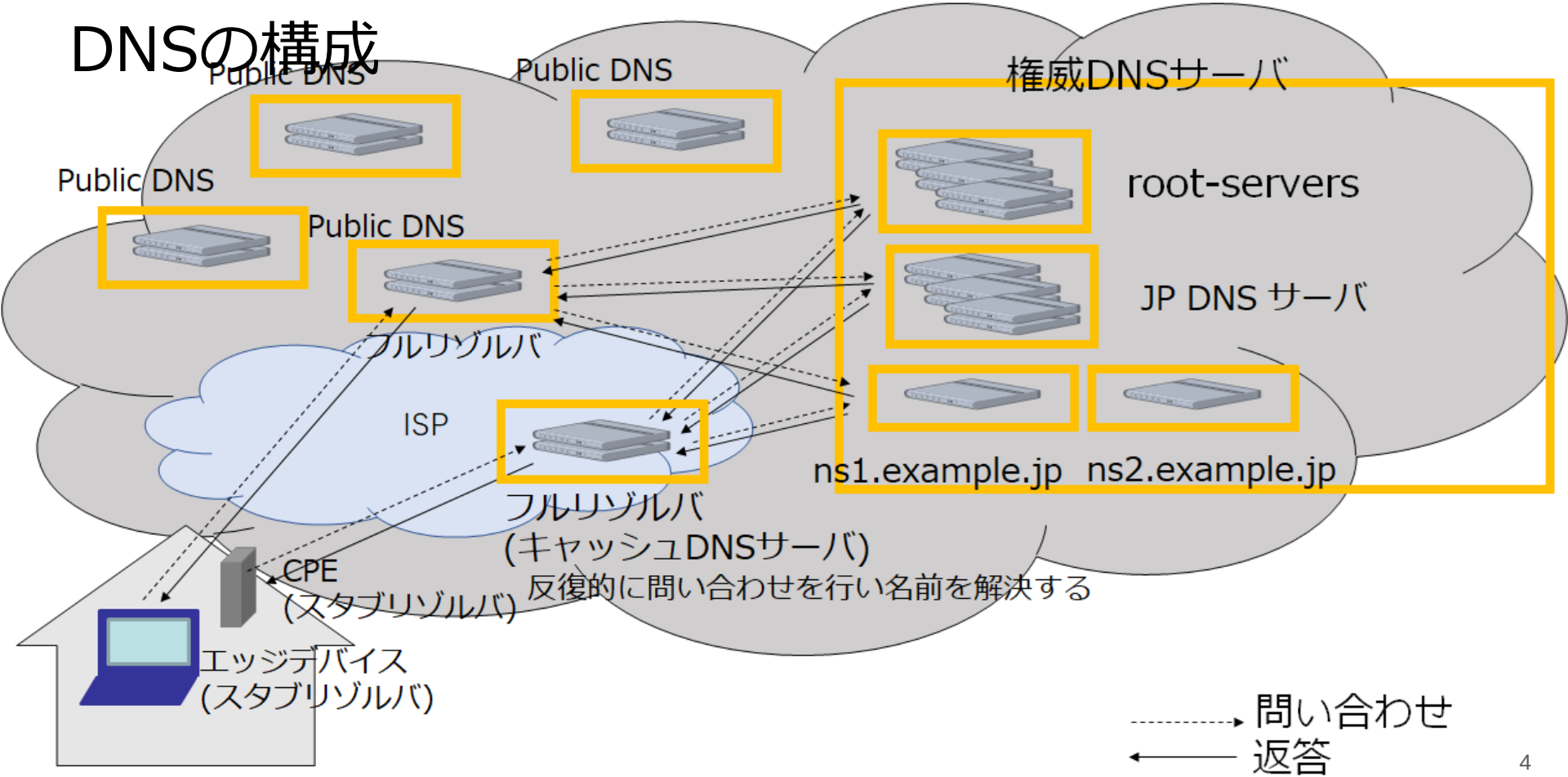
ISPのフルリゾルバとプライバシー

- エンドユーザからのフルリゾルバへの問い合わせも通信の秘密の対象
- プライバシーの観点からも個々の問い合わせについての知得も行わない
- 例外：
  - 児童ポルノブロッキング(緊急避難)
  - マルウェアサイトブロッキング(同意とオプトアウトの提供)

ISPのフルリゾルバとプライバシー

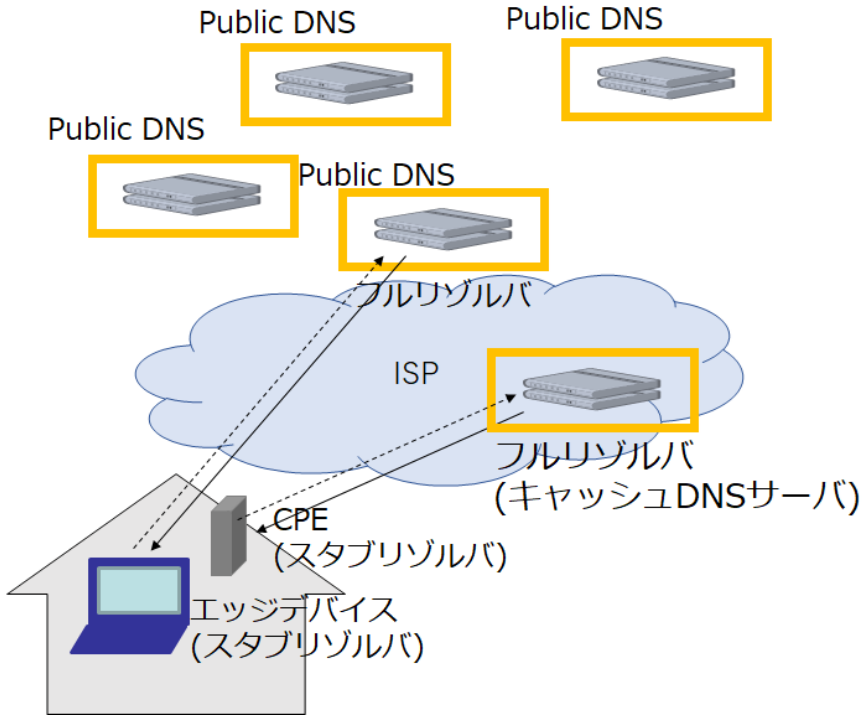
ちょっと脱線：「海賊版サイトブロッキング」問題
「東京高判令和元年10月30日（令和元年（ネ）2753号）」
「本件ブロッキングを実施した場合には、第1 審被告によりユーザーの全通信内容（アクセス先）の検知行為が実行され、このことが日本国憲法2 1 条2 項の通信の秘密の侵害に該当する可能性があることは、第1 審原告が指摘するとおりである。児童ポルノ事案のように、被害児童の心に取り返しのつかない大きな傷を与えるという日本国憲法1 3 条の個人の尊厳、幸福追求の権利にかかわる問題と異なり、著作権のように、逸失利益という日本国憲法2 9 条の財産権（財産上の被害）の問題にとどまる本件のような問題は、通信の秘密を制限するには、より慎重な検討が求められるところではあるが、訴訟費用の負担の問題の結論を左右する問題ではないものというほかはない。」

DNSの構成


Public DNS
Public DNS
Public DNS
Public DNS
権威DNSサーバ
root-servers
JP DNS サーバ
ns1.example.jp
ns2.example.jp
フルリゾルバ
ISP
フルリゾルバ
(キャッシュDNSサーバ)
反復的に問い合わせを行い名前を解決する
CPE
(スタブリゾルバ)
エッジデバイス
(スタブリゾルバ)
問い合わせ
返答

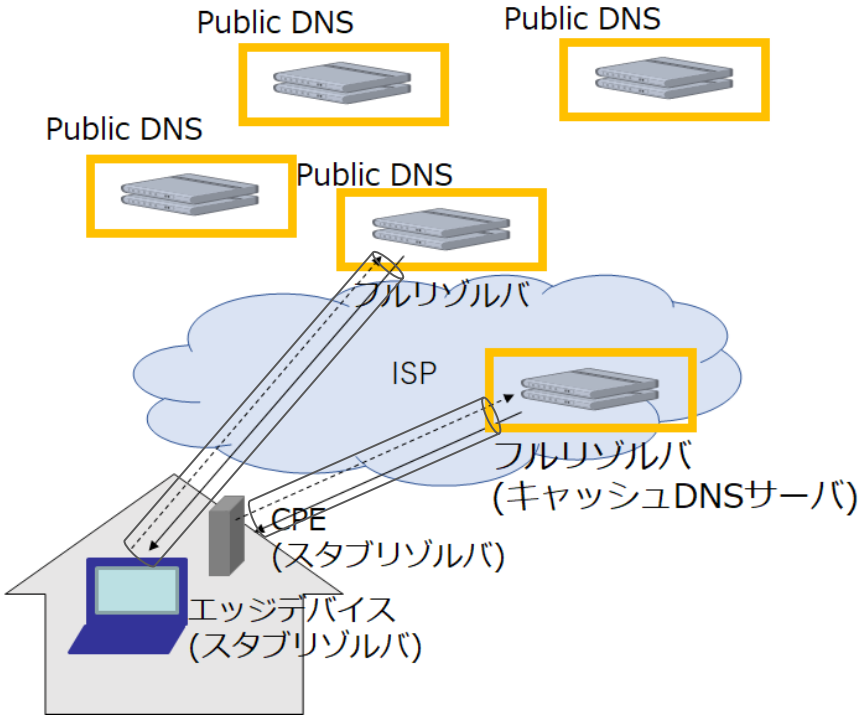
フルリゾルバを運用する立場からの懸念事項

- DoT/DoHによる Public DNS が主流となった場合：
  - フルリゾルバの利用が Public DNS に巻き取られることに関する懸念
  - 自社の利用者に対して DoT/DoH を提供することに関しての懸念



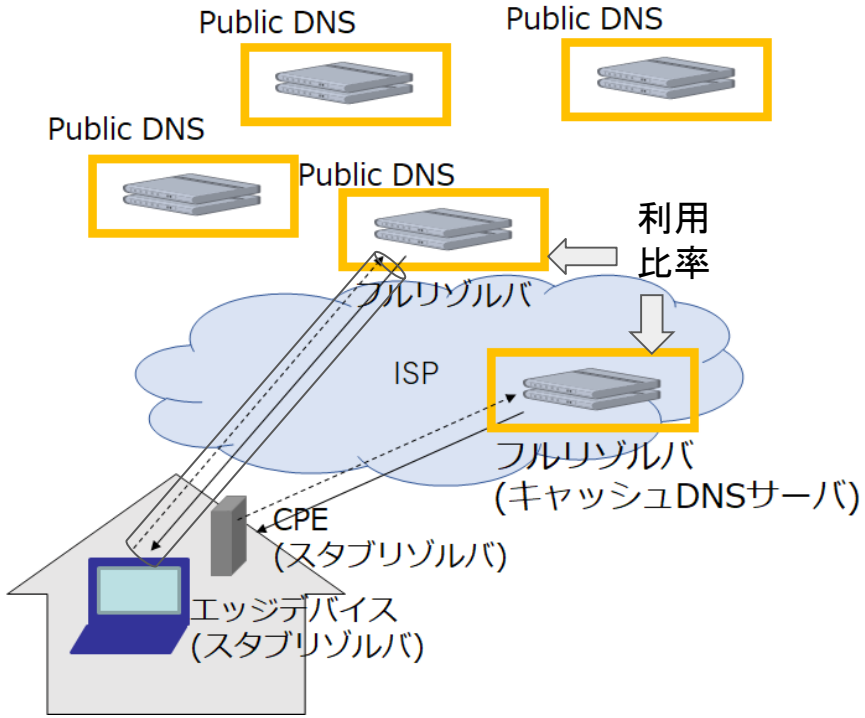
ISPのフルリゾルバ

- DoH/DoT の導入が進んだ場合には、ISP のフルリゾルバでも対応すべき？
  - 対応しない場合
  - 対応する場合



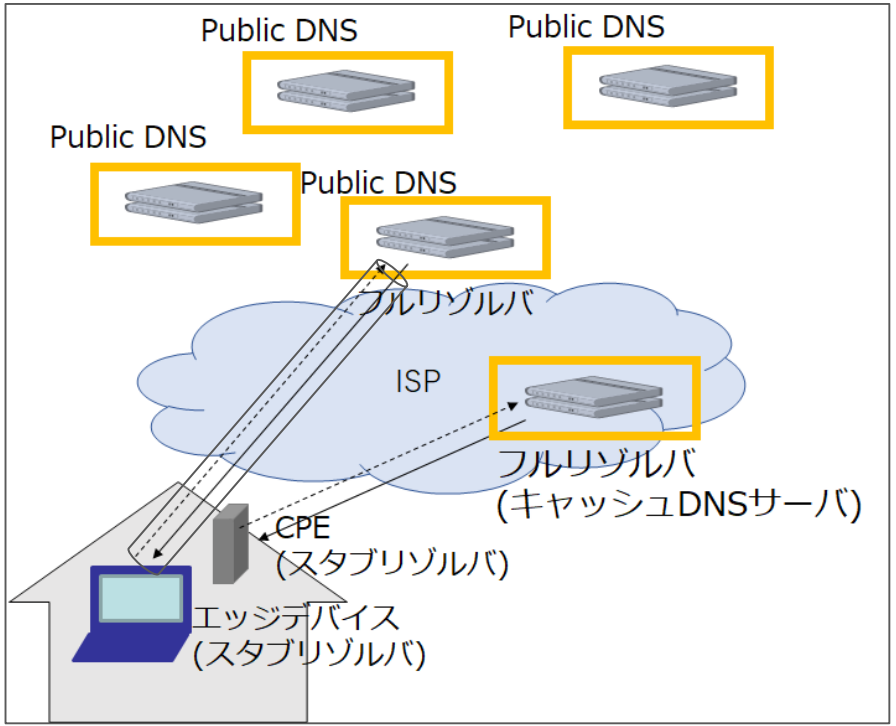
DoH/DoTへ対応しない場合に想定されること

- 完全に Public DNS に巻き取られる
  - ISPはフルリゾルバの運用から解放される(？)
- 一部のみで Public DNS が利用される
  - 様々な問題が発生する可能性



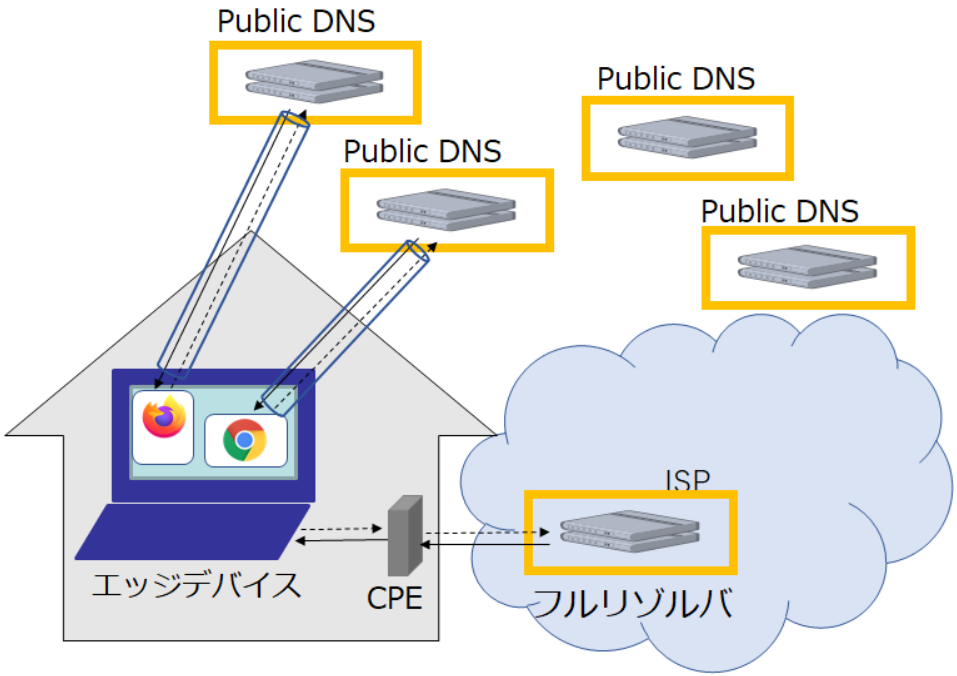
一部のみで Public DNS が利用される

- 想定される問題
  1. 同一ユーザが異種のフルリゾルバを利用することにより発生する不具合
  2. CDN(GSLB)利用の不整合
  3. フルリゾルバの運用管理への影響



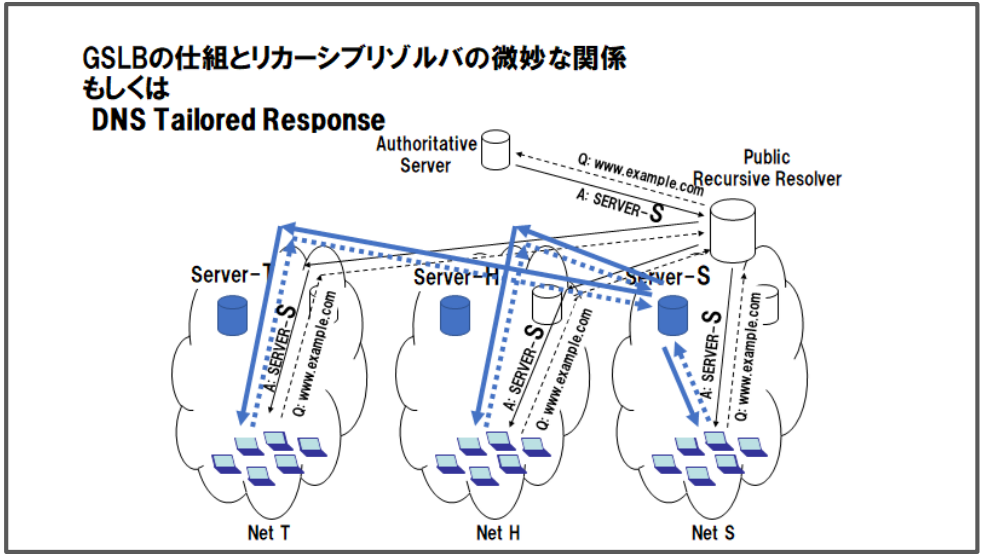
一部のみで Public DNS が利用される

1. 同一ユーザが異種のフルリゾルバを利用することにより発生する不具合
    - 同一のユーザがエッジデバイス毎に異なる複数のフルリゾルバを利用する可能性
    - 同一のエッジデバイス内で異なる複数のフルリゾルバを利用する可能性
    - 名前解決ができない場合の原因の切り分けが困難



一部のみで Public DNS が利用される

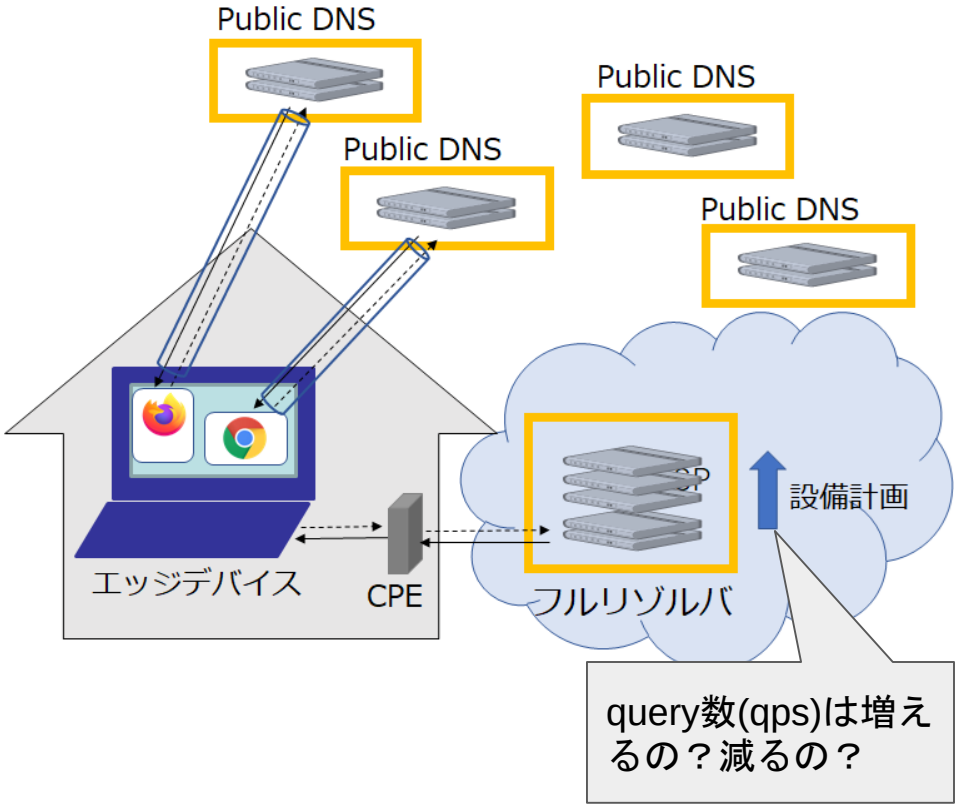
2. CDN(GSLB)利用の不整合
   - DNSによる負荷分散のための配信サーバの選択が最寄りではなくなる
   - 解決するにはPublic DNSとCDNプロバイダへのECS(RFC7871)の実装が必須



JANOG38(2016/07/08)
「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

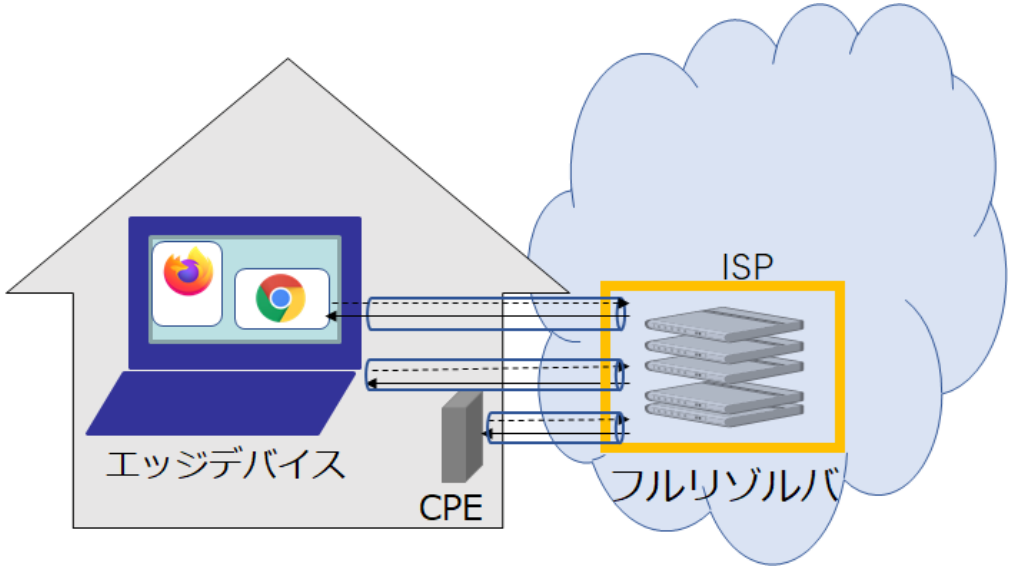
一部のみで Public DNS が利用される

3. フルリゾルバの運用管理への影響
    - フルリゾルバの設備計画(性能設計・収容設計)が困難
    - 接続元のアクセスコントロール



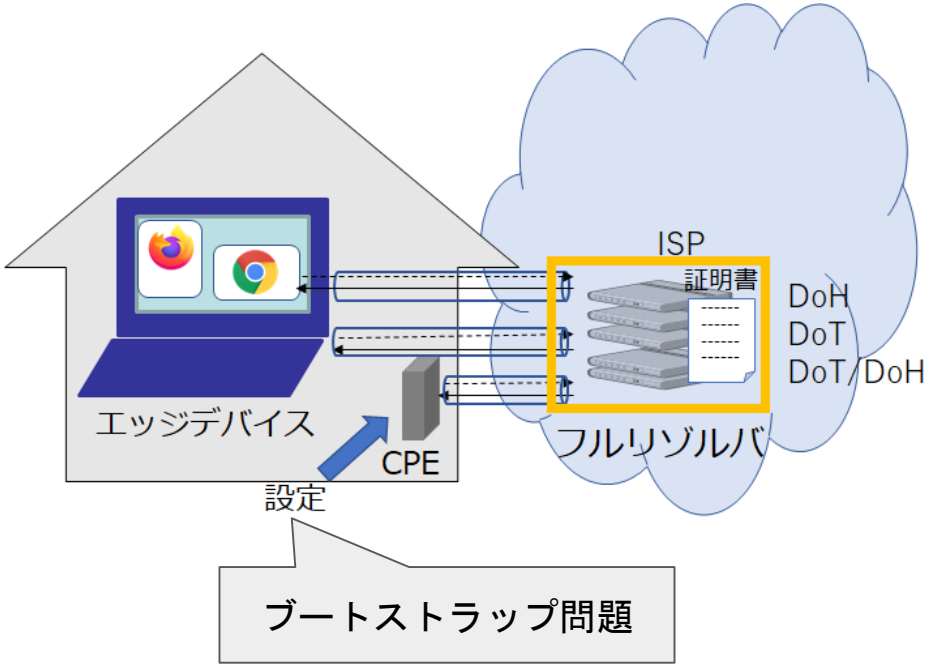
DoH/DoTへ対応する場合

- 提供形態
  - DoH/DoTのクライアント(スタブリゾルバ)は誰か？
    - CPE
    - エッジデバイス(OS)
    - アプリケーション



DoH/DoTへ対応する場合

- DoH/DoTに関わる運用
  - DoH/DoTのいずれかに対応するか or 両方か
  - DoH/DoTに対応するためのシステム構成
  - スタブリゾルバへの設定方法
    - FQDN or IPアドレス
  - DoH/DoTに利用する証明書
    - WebPKIの証明書???



DoH/DoTへ対応する場合

- DoH/DoTに関わる運用
  - 「IIJのDNS暗号化への取り組み」
    https://eng-blog.iij.ad.jp/archives/5298

まとめ

- DoT/DoHは(今のところ)フルリゾルバ・スタブリゾルバ間の暗号化が目的
- ISPは対応／非対応に関わらず大きな問題が発生する可能性が高い
- フルリゾルバの運用はメイルサーバの轍を踏むのか？？？