DoH/DoT Update

DNS Summer Day 2020

山口崇徳@IIJ

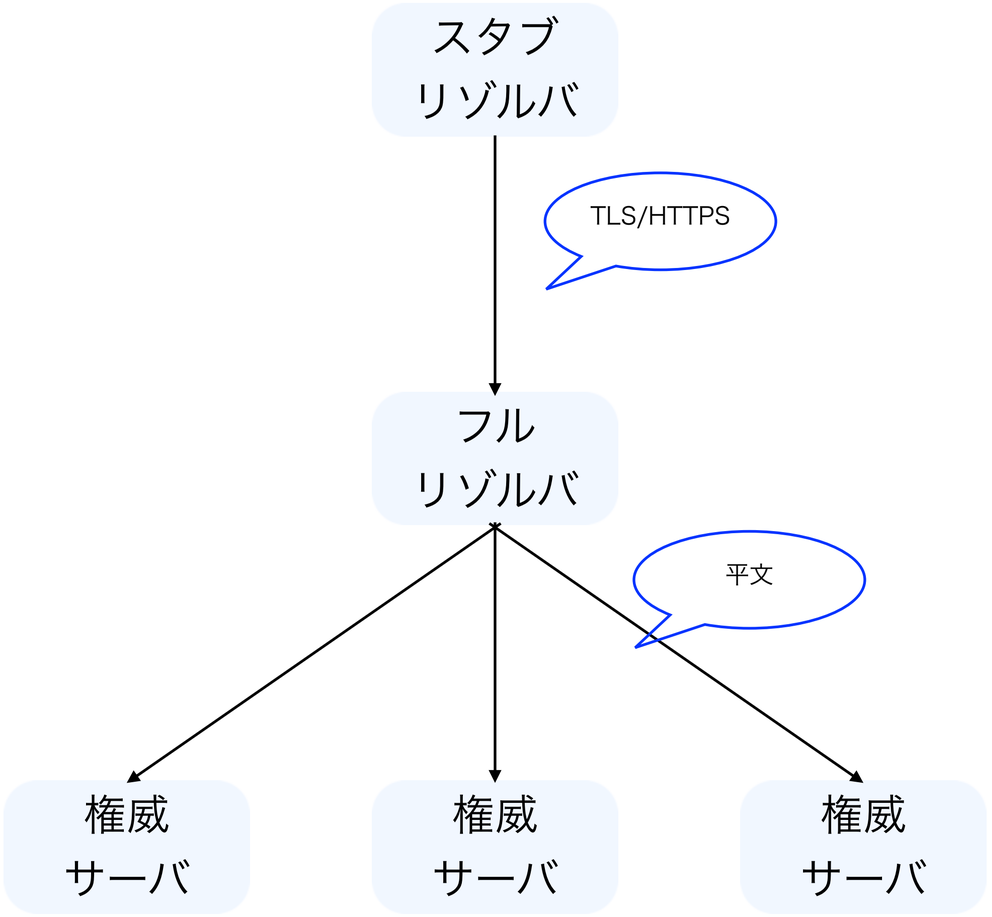
はじめに

- 英語では「でぃーおーえいち」「でぃーおーてぃー」ではなく「どー」「どっと」と発音するようです
  - が、日本人にとっては「でぃーおーえっち」のほうがわかりやすいと思うので、今回もそう喋ります

- ここ数年ほど、DoH/DoTについて発表させてもらう機会が多いし、会社でもいろいろ始めてるけれど、個人的には推進派のつもりはありません

DoH/DoTとは

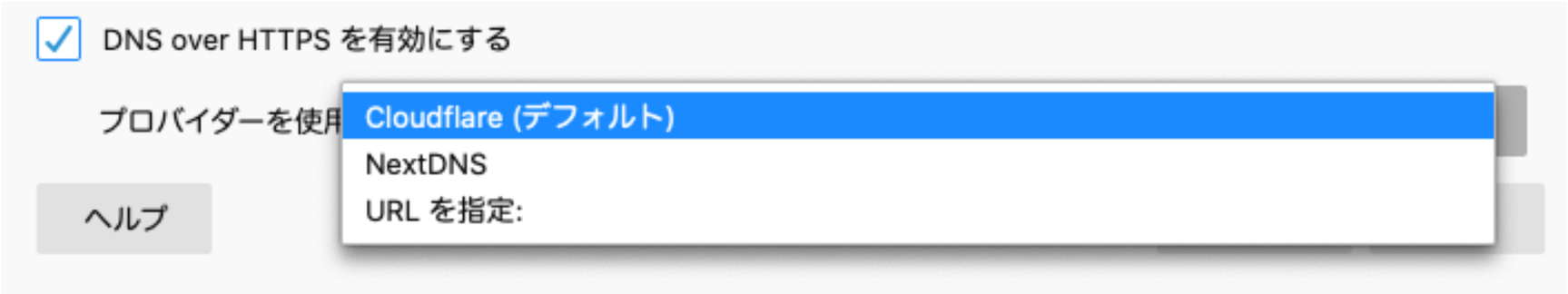
- DNS over HTTPS (RFC8484)
- DNS over TLS (RFC7858)
- スタブ-フルリゾルバ間の暗号化
  - 権威サーバまでのDNSの系全体を暗号化するわけではない
- その他詳細はこちらを
  - https://www.nic.ad.jp/ja/materials/iw/2019/proceedings/d3/d3-yamaguchi.pdf



ブラウザのDoH

Firefox

- Firefox62 (2018/09) でDoHに対応
- 2020/02 からデフォルト有効(米国のみ)
  - https://blog.mozilla.org/blog/2020/02/25/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/
- OSのリゾルバ設定とは無関係に、Firefoxだけで使われるリゾルバを設定する



Firefox
canary domain

- まず、use-application-dns.netを名前解決
  - canary domainと呼ばれる
  - 名前解決失敗またはA/AAAAが空ならばDoHを使わない
- ネットワーク管理者はcanary domainの名前解決をブロックすることで、ユーザにDoHを利用させないようにすることができる
  - canary: カナリア(鳥)、または俗語で密告者の意
- Chrome/Edgeなど他のDoH実装で追随する動きなし

Firefox
DoHは悪党なのか?

- イギリスISP協会がMozillaを2019年の悪党オブザイヤーにノミネート
  - https://www.ispa.org.uk/ispa-announces-finalists-for-2019-internet-heroes-and-villains-trump-and-mozilla-lead-the-way-as-villain-nominees/
  - 他の候補者はEU著作権指令13条、トランプ米大統領
- MozillaではなくISPA UKの方が叩かれ炎上 → ノミネート取り下げ
  - https://www.ispa.org.uk/ispa-withdraws-mozilla-internet-villain-nomination-and-category/
  - 炎上したノミネートよりも取り下げ声明の方に重要な指摘を含んでいる(が、こっちの方はまったく話題にならなかった)

Firefox
ISPA UKの指摘 (1)

1. ユーザによる選択
   - ユーザ自身が選択した設定をないがしろにするべきではない
   - たとえば、すでにDNSによるペアレンタルコントロール等が設定されていた場合、アプリケーションはそれを尊重するべき
2. ユーザによる同意
   - リゾルバ設定を変更する際にはユーザに十分説明し、同意を得るべきである
3. データ保護
   - ローカルデータ保護の要件を満たすべき

Firefox
ISPA UKの指摘 (2)

4. セキュリティ
   - マルウェア保護等、現在のセキュリティポリシーを引き継げるようにするべき
5. online safety
   - 同様にポリシーを引き継げるようにするべき
6. サポート
   - DoHに問題が起きても、ユーザはDoHの提供者ではなくISPに問い合わせるだろうが、ISPでは解決できない
   - アプリケーション提供者が24時間稼動のコールセンターを用意するべき

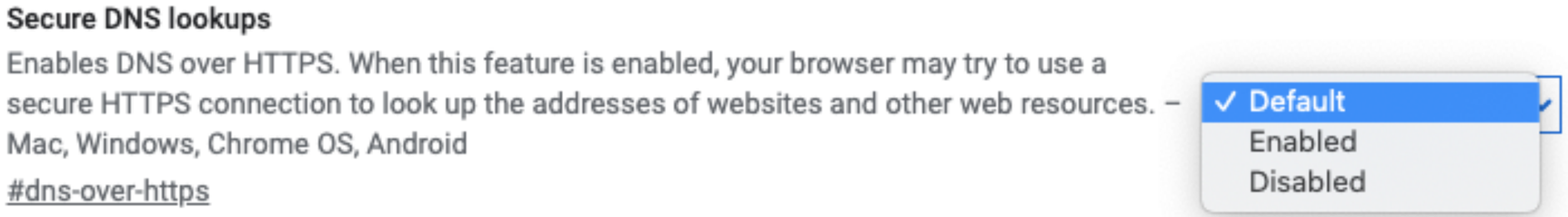
Firefox
なぜ批判されるのか

- DoHを実装したこと自体は批判されていない
- 「OS設定を無視してお仕着せ(cloudflare)を上書き設定する」という方針が批判されている
- ISPA UK以外からの批判意見も同様のものがほとんど

- Umbrella (DNSによるドメインフィルタリングサービス、商用版OpenDNS)はcanary domainをブロッキング
  - https://umbrella.cisco.com/blog/doh-dns-over-https-to-block-or-not-to-block

Chrome

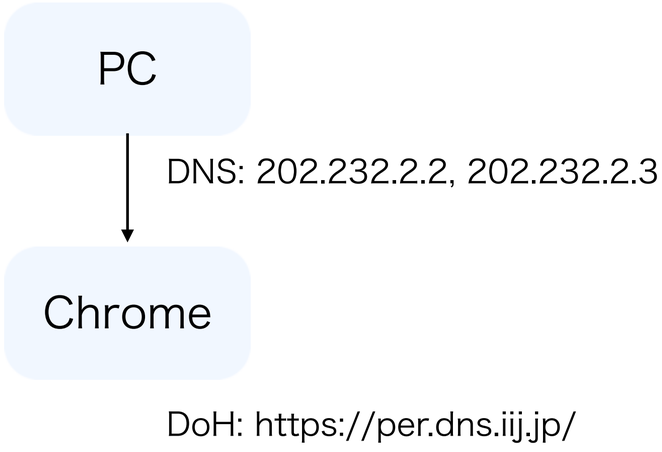
- Chrome79 (2019/12) で実験的にDoH対応
  - 設定はデフォ/有効/無効の選択だけで、DoH URLを入力する欄がない



- Chrome83 (2020/05) で正式対応
  - https://developers-jp.googleblog.com/2020/06/secure-dns.html
  - デフォルトでchrome79の「有効」設定相当で、任意URLを設定することも可能
  - ……らしいが、手元の環境では設定項目が存在しない

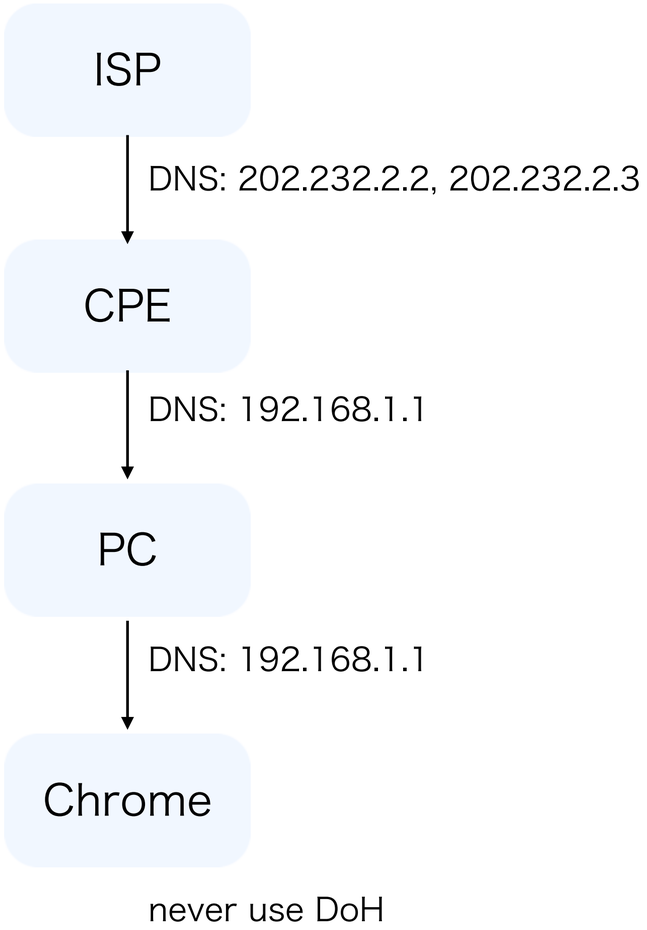
Chrome
Same-Provider Auto-Upgrade (1)

- ChromeはOSに設定されたフルリゾルバがDoHに対応している場合、DoHを使う
  - ブラウザ内にIPアドレスとDoH URLの対応表が静的に組み込まれている
- トランスポートがUDPかDoHかの違いだけ
  - 同一事業者(same provider)が同じポリシーで提供することが前提なので、Firefoxへの批判はChromeには当たらない
- しかし…



Chrome
Same-Provider Auto-Upgrade (2)

- ほとんどのホームルータはDNS forwarder
  - PCに自動設定されるフルリゾルバのアドレスは、ISPが配ってるものではなく、ホームルータのもの
  - ブラウザ組み込みのDoH対応リストに存在しない
  - **ISPがDoHを提供しても、アップグレードされない**
- 自前のDoHサーバを使うためには、Chromeのソースに追加してもらう必要がある
  - あくまで平文からのアップグレードなので、アップグレード元がないDoH専用サーバはそれもできない



Microsoft
Windows/Edge

- EdgeはベースとなっているChromeと同じバージョン(?)で対応済み
  - 開発版ではなく一般向けバージョンですでに利用可能
  - 設定UIはChrome(実験対応版)と同じ
- Windows Insider Programで、アプリではなくOSとしてのDoH対応を実験開始
  - https://techcommunity.microsoft.com/t5/networking-blog/windows-insiders-can-now-test-dns-over-https/ba-p/1381282
  - 現状はレジストリ直接編集や貧弱なCLIコマンドを駆使して設定する必要あり
  - Chromeと同じく、Same-Provider Auto-Upgradeを採用
    - DoH対応リストはレジストリから手動追加可能

Apple
Mac/iOS/Safari

- これまで沈黙を保ってきたが、WWDC2020 (06/22)でついに対応を発表
  - https://developer.apple.com/videos/play/wwdc2020/10047
  - macOS 11.0, iOS 14.0でリリース予定
- システム全体でDoH/DoT両方に対応
  - MDM (Mobile Device Management)による端末集中管理での設定も可能
  - getaddrinfo()のようなPOSIX APIでも暗号化される
- アプリケーションが個別にDoH/DoTを使うAPIも提供

この先どうなるの?

権威サーバの暗号化

- 現在のDoH/DoTはスタブリゾルバ - フルリゾルバ間だけ
- フルリゾルバ - 権威間は従来の平文DNS

- いちおう議論は始まってる
  - dprive WGの”Phase 2”として、かなり本気で取り組むみたい
    - https://tools.ietf.org/html/draft-ietf-dprive-phase2-requirements-00
    - ただし、まだ要件定義の段階で具体的には何も…
  - その他いくつかのの個人ドラフト

DoH/DoT自動設定

- IPアドレスなどネットワーク接続に必要な情報がOSに自動設定される
  - DNSも自動設定される情報のひとつ
  - IPCP (PPP)、DHCP/DHCPv6、RDNSS (IPv6 RA)
- DoH/DoTは自動設定されない
  - Firefoxのようにお仕着せ設定にするか
  - ChromeのようにAuto-Upgradeするか
  - 手作業で設定するか
  - それとも新プロトコルを作ってデプロイするか

DoH/DoT自動設定
Adaptive DNS Discovery WG (add)

- IETFにこのテーマを専門に扱うWGが作られる
  - あれ、あなた以前はApplication Doing DNSと名乗ってませんでした?
- いくつかドラフトが提出されているが、形になるのはだいぶ先になりそう
  - ちゃんとRFCで標準化されるのが先か、どこかのベンダーのやりかたがde facto standardになるのが先か

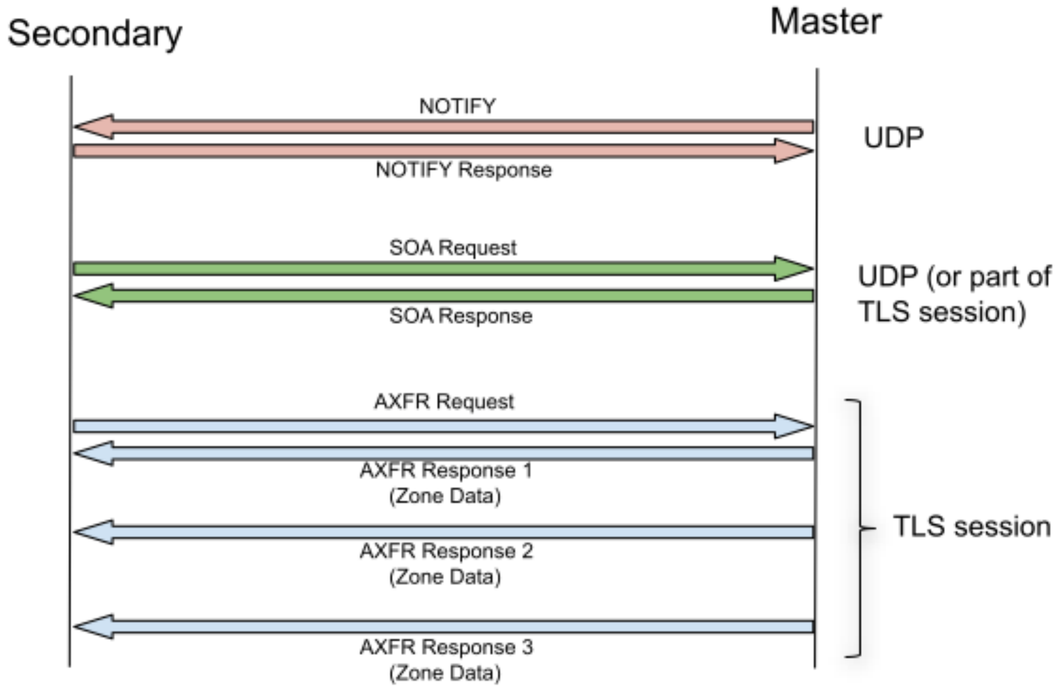
DoTって息してる?

- 最近は目立った動きなし

- DoQも仕様がだいぶ固まってきた
  - https://tools.ietf.org/html/draft-ietf-dprive-dnsoquic-00
  - ますますDoTの存在感が…

XoT
XFR over TLS

- 権威サーバ間のゾーン転送の TLS 化
- AXFR/IXFR → AXoT/IXoT
- dprive WG で検討中
  - https://tools.ietf.org/html/draft-ietf-dprive-xfr-over-tls-01
- ゾーン転送に先立つ NOTIFY/SOA のやりとりまでは TLS にしない方向?
- まだドラフトなので実際どうなるかは謎



https://github.com/hanzhang0116/hzpa-dprive-xfr-over-tls/blob/master/02-draft-svg/AXoT_mechanism_1.svg

とーーとつですが、CDNについて。

CDNとは

- ユーザがコンテンツ配信元から遠いのは効率がよくない
  - 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

DNSによるトラフィックマネジメント

- Anycast
  - 同一のIPアドレスを持った複数の権威サーバを分散配置し、ネットワーク的にもっとも近いDNSサーバにアクセスを誘導する
  - DNS自体の効率化
- GSLB (Global Server Load Balance; GeoDNS)
  - 権威サーバが問い合わせ元IPアドレスによってA/AAAAレコードの応答を変え、ネットワーク的にもっとも近いWebサーバにアクセスを誘導する
  - DNSの次にアクセスされるWebの効率化

DNSによるトラフィックマネジメント

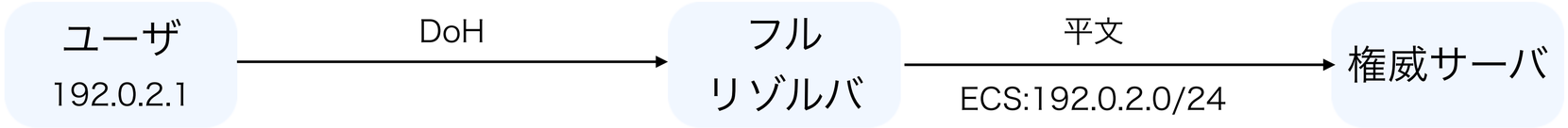
- Anycast
  - 同一のIPアドレスを持った複数の権威サーバを分散配置し、ネットワーク的にもっとも近いDNSサーバにアクセスを誘導する
  - DNS自体の効率化
- GSLB (Global Server Load Balance; GeoDNS)
  - 権威サーバが問い合わせ元IPアドレスによってA/AAAAレコードの応答を変え、ネットワーク的にもっとも近いWebサーバにアクセスを誘導する
  - DNSの次にアクセスされるWebの効率化

GSLBとpublic DNS

- 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
- これまで、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同じネットワーク内
  - CDNの配信効率に影響はない
- が、ユーザがpublic DNSを利用する場合はこれが成り立たない
  - GSLBが誘導するWebサーバがエンドユーザに最適化されたものとはかぎらない
  - 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



- フルリゾルバ - 権威サーバ間は平文DNSが使われる
  - ユーザがDoHで暗号化していても、フルリゾルバ - 権威間で盗聴できてしまう
  - 何のためにDoHを使うの?

public DNSとDoH

- ISPがユーザに対してDoHサービスを提供するメリットがない
  - ISP網内の通信は平文でも外部からの盗聴の危険は小さい
  - 仮にISPがDoHサービスを提供したとしても、自動設定の仕組みがなく、Same-Provider Auto-Upgradeも機能しないため、ほとんど利用されない
- つまり、DoHはほぼpublic DNS専用プロトコル
  - DoHの普及 ≒ public DNSへの集中化・寡占化
  - この方向に進んでしまってほんとうにいいの?

まとめ
まとまらない

- 主要WebブラウザのDoH対応状況
- 今後の方向
  - 権威サーバの暗号化
  - DoH/DoTの自動設定
- CDN、public DNSとの関係