第106回IETF報告

abcd

木村泰司

一般社団法人 日本ネットワークインフォメーションセンター

概要

- 「Application Behavior Considering DNS」BoF
  - (処理)DoHやDoTが使われるようになると「DNSクライアント」の処理はOSのリゾルバではなくアプリケーションで行われるようになる。
  - (影響)ISPやローカルネットワークのフルリゾルバではなく、どこかのHTTPSで通信するサーバが使われやすくなる。

  - WG策定に向けたBoF
  - ブラウザ実装のトライアルにおいては不確定要素が多く、標準化が必要という意見。
  - 前回のADD BoF以降、様々な議論を盛り込んだ趣意書案。

どのような議論が行われているのか？この先は？

発表者について

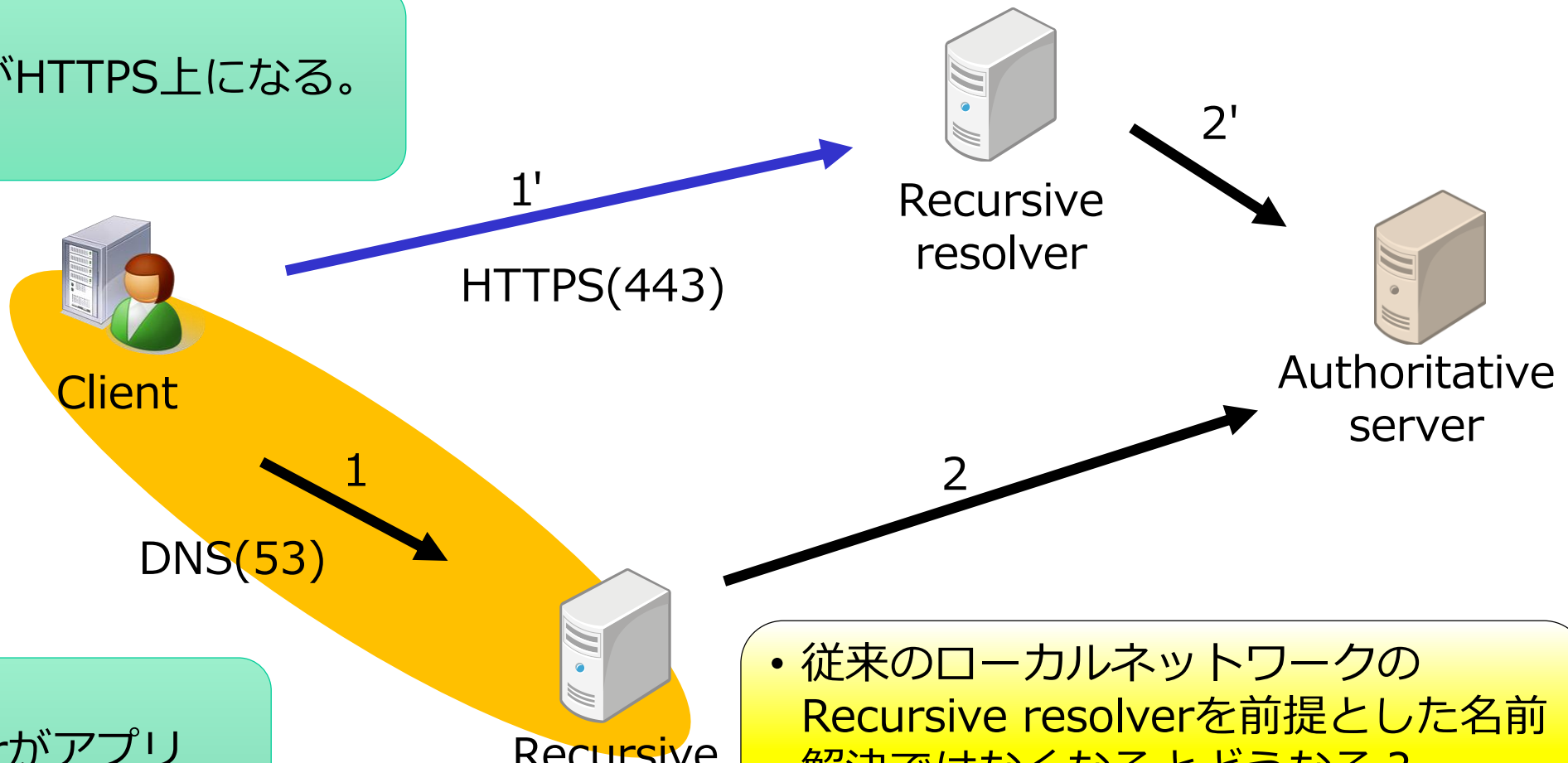
名前	木村泰司
所属	日本ネットワークインフォメーションセンター(JPNIC)
担当	RPKI/認証局/セキュリティ/ 国際動向 IETF, レジストリ
職務	調査/研究/開発/運用/講師/ユーザサポート
関係団体	• セキュリティ・キャンプ講師 • フィッシング対策協議会 技術・制度検討WG • JNSA PKI相互運用技術WG • WIDEプロジェクト

おさらい

DoTとDoH

DoTとDoH - Encrypted DNS(Encrypted transport)

変わること１
DNSトラフィックがHTTPS上になる。
暗号化される。



変わること２
Recursive resolverがアプリケーションによって選択される。

- 従来のローカルネットワークのRecursive resolverを前提とした名前解決ではなくなるとどうなる？
- アプリケーションはどういう仕様に？

時系列(1/3)

- **2013年**
  - 5月, スノーデン氏、PRISMSを公表
  - 11月 IETF88
    - W3C/IAB workshop - STRINT(**Strengthening the Internet Against Pervasive Monitoring**)
    - “**Pervasive Monitoring is an Attack**”, draft-farrell-perpass-attack-00 (RFC7258, 2014)
- **2014年**
  - 9月, dprive WG
    - "Specification for DNS over Transport Layer Security (TLS)", (**RFC7858, 2016**) **# DoT**
- **2015年**
  - 6月, "**DNS over DTLS**" draft-ietf-dprive-dnsodtls-00 (RFC8094, 2017)
  - 7月, IETF93, スノーデン氏、遠隔登場

時系列(2/3)

- **2017年**
  - 4月 "Specification of **DNS over QUIC**" draft-huitema-quic-dnsoquic-00 # current: 07
  - 5月, "DNS Queries over HTTPS", draft-hoffman-dns-over-https-00 (**RFC8484, 2018**) **# DoH**
  - 9月, doh WG
  - 11月, Quad9、DoTをサポート
- **2018年**
  - 4月, Android DoH client アプリ Intra 登場
  - 4月, CloudFlare、パブリックDNSがDoTとDoHをサポート
  - 6月, Firefox、DoHのベータテスト
  - 10月, Quad9、DoHをサポート

時系列(3/3)

- **2019年**
  - 1月, Google パブリックDNSでDoTをサポート
  - Google パブリックDNSでDoH(RFC8484)をサポート

DNS over Transport Layer Security (TLS)

- RFC7858, 2016年
- TCP 853
- 特徴
  - Opportunistic privacy（プライバシーは必須ではない）--- クライアントは**DHCP DNS server option**を使用
  - Out-of-Band Key-Pinned Privacy Profile --- DNSサーバとDNSクライアントの間にトラストの関係が存在している環境を想定
- 認証について (RFC8310)
  - Opportunistic privacy --- 認証に失敗したサーバを使わなくてもよい。
  - Strict Privacy --- **subjectPublicKey Info.(SPKI)とpin setを使用**する。

DNS Queries over HTTPS (DoH)

- RFC8484, 2018
- HTTPS 443
- HTTP リクエスト/レスポンスの仕組みを使ったDNSクエリー
- DoHクライアントにおいてはURIテンプレート(RFC6570)を使って設定
  - http://example.com/search
- DoHサーバは"bootstrap"によりdiscoveryされる。

- **ローカルネットワークの「Recursive resolver」は使われない。**

前回までのあらすじ

DNSの変化に関する議論

- **Centralized DNS over HTTPS (DoH) Implementation Issues and Risks**
  - https://tools.ietf.org/html/draft-livingood-doh-implementation-risks-issues-03
  - DoHの普及によって中心的なDNSサーバができることのリスクなど
- **DNS over HTTPS (DoH) Considerations for Operator Networks**
  - https://tools.ietf.org/html/draft-reid-doh-operator-00
  - 通信事業者に関わるDoHの法律に関連する整理やCDN、captive portalのような仕組みへの影響
- **Recommendations for DNS Privacy Client Applications**
  - https://tools.ietf.org/html/draft-bertola-bcp-doh-clients-00
  - DoHクライアントによるDNSの仕組みなどへの影響

Applications Doing DNS (ADD) BoF (IETF105 モントリオール)

- **DNS in Applications(Mozilla's vision for DNS & apps)**
  - Mozillaにおける考え方。一貫性がなくなったDNSとDNSを使ったコンテンツブロッキングは、オーバーブロッキングなどの懸念など。
- **Google's perspective**
  - リゾルバがおのおののネットワークで提供されていることに、変化を起こそうとしているわけではない。ほか。
- **ブラウザ以外のデバイス(Non-browser apps doing DNS)**
  - トラストアン カーをどのように設定するのか。DoTやDoHをどのように選択するのか、何にフォールバックするのか、といった課題提起。

第105回IETF報告 [第3弾] 「DNSの処理を行うアプリケーション」の話題
https://www.nic.ad.jp/ja/mailmagazine/backnumber/2019/vol1711.html

ABCD

Application Behavior Considering DNS BoF

IETF106 シンガポール, 2019年11月19日 13:30-15:00,

250名以上(!)

アジェンダ

1. **イントロダクションと背景**
   Introduction and background refresher (Chairs)
   - 背景、クライアント実装、サーバの対応状況、ドラフト、議論、議論したい事
2. **canaryドメインでの実験レポート**
   Report on canary domain experience (Andy Grover, Mozilla)
   - DoHサポートした時の実装上の問題、標準化の必要性
3. **アダプティブなDoHの提案の概要**
   Overview of the Adaptive DOH proposal (Tommy Pauly, Apple)
   - ネームサーバを選択する際の複雑さ、議論の必要性
4. **趣意書の議論**
   Charter presentation (Chairs)

イントロダクションと背景

Introduction and background refresher (Chairs)

https://datatracker.ietf.org/meeting/106/materials/slides-106-abcd-chair-slides-00

内容

- (背景) "Encrypted transport"の標準化が進み実装やサーバ対応が進んでいる。クライアント設定に関するドラフト多数。関連するシステムの検討課題や社会的な議論も。
- (議論したい事) WG設立の意義があるか。趣意書を検討する事で利用環境において有益な標準化ができるか。ほか。
  特定のプロトコルのメリットや社会的な議論に関連する主張は扱わない。

"canary"ドメインでの実験レポート

Report on canary domain experience (Andy Grover, Mozilla)

https://datatracker.ietf.org/meeting/106/materials/slides-106-abcd-mozilla-canary-domain

内容

- use-application-dns.netドメインを使った実験
  - DoHをデフォルト
- (サイドエフェクト) ペアレンタルコントロールがある場合に検知してDoHを無効にしなければ。"スプリットホライズン"を避けるには。
- (実装の試み) 特定のドメイン名を除きNXDOMAINの場合などにDoHでない問い合わせ。この辺りの標準化が必要では？

ペアレンタルコントロールと見つけるのは難しそう／use-application-dns.netは.arpaを使っては？

アダプティブなDoHの提案の概要

Overview of the Adaptive DOH proposal (Tommy Pauly, Apple)

https://datatracker.ietf.org/meeting/106/materials/slides-106-abcd-adaptive-dns-privacy

内容

- (検討課題) Encrypted resolverをどう特定するのか？
  設定はどこから／プロトコルの選択
- (検討課題) "ローカルポリシー"をクライアントにどう伝える？
  DHCP/RA？／キャプティブポータルは／問い合わせポリシー
- (検討課題) どう正しいサーバを選択する？
  VPN、ローカルリゾルバ、DoHサーバ、一時的なDoHサーバ...

異なるCDNで提供される同じドメイン名があるときEncryptedSNIで動く？／会社が異なる時に正常に名前解決できる？

WG設立についての議論

- **扱うテーマ**
  - 趣意書案の変更多し(chair)
- **趣意書について**
  - 全体にコンセンサスを得るのは無理(多数)
  - dnsop WGで議論すべき内容も？しかしdnsop WGよりも広い分野の人が集まっている。。
  - 議論しないリストを作るべき。範囲を狭めるべき。
  - WG設立はサポートする。
  - マルウェア検知の観点も必要。
  - MLで議論を。
    → abcd MLで趣意書に関する議論が続いている。

おわり