[DNS関連WG報告]

add WG

IETF107報告会

2020年5月11日

米谷嘉朗

<yoshiro.yoneya@jprs.co.jp>

もくじ

- 背景
- DoHの影響
- DoHの熱い議論(おさらい)
- add WGの目的(概要)
- IETF107 add WGの概要
- 気にすべきこと(私見)
- Q&A

背景(1/2)

- DNSプライバシーの需要拡大
  - DNSパケットは暗号化されていない
  - パケットキャプチャできれば利用者の行動がわかってしまう
  - 2014年9月にdprive WGがINTエリアで設立され、スタブリゾルバとフルリゾルバ間のDNSパケット暗号化方式の標準化が始まった
- DNS over TLS (RFC 7858)
  - 2016年5月にDNSパケットの送受信(トランスポート)をTLS上で行うプロトコル(DoT)が標準化された
    - DTLS上で行うプロトコルは2017年2月にExperimentalでRFC化された(RFC 8094)

背景(2/2)

- DNS over HTTPS (RFC 8484)
  - 2017年9月に、DNSトランスポートをHTTPS上で行いたいという需要に基づきdprive WGとは別のdoh WGがARTエリアで設立された
  - 2018年10月に、DNSパケットの送受信をHTTPS上で行うプロトコル(DoH)が標準化された
- 似て非なる2つの暗号化DNSプロトコルが出来上がった
  - DoTに比べ、DoHは圧倒的に使いやすかった
    - 主要なパブリックDNSではDoHの応答にRFC 8427で標準化されたJSON形式もサポートした
  - アプリケーションレベルですぐに実装された
    - 特に主要なブラウザが素早く対応もしくは対応表明した

DoHの影響(1/3)

- 誰がどうやってDoHサーバを選択するか
  - 伝統的なDNS(Do53)やDoTはシステム管理者やISPがフルリゾルバを指定し、利用者のOSはそれを使う
  - DoHはアプリケーションが独自にDoHサーバを指定でき、システム(OS側)に設定されたフルリゾルバは使わない
    - DoHサーバをIPアドレスで書かない場合にどうやってブートストラップするか

⇒DoHサーバの選択をアプリケーションに委ねてよいのか？

DoHの影響(2/3)

- 適切なDoHサーバをどうやって使わせるか
  - DoHはフルリゾルバによる利用者保護(不適切コンテンツフィルタリングなど)をバイパスでき、ローカルな(ビューで分けられたなどの)名前解決に失敗する
    - 国や地域によっては法律や条例で不適切コンテンツフィルタリングを要請している

⇒システム管理者や利用者の意向は反映できないのか？

DoHの影響(3/3)

- DoHサーバに情報が集中するのではないか
  - DoHサーバの多くはパブリックDNSで提供されている

  ⇒DoHを使うことでパブリックDNSに利用者のDNS問い合わせ情報が集中してよいのか？

DoHの熱い議論(おさらい)

- 過去のIETF報告会で既に取り上げられているので詳細は省略します
  - IETF102報告会「DNS関連の標準化動向」(driuの章)
  - IETF103報告会「DNS関連その他の話題など」(Resolverless-DNS side meetingの章)
  - IETF104報告会「DNSいったいDoHするの？～とあるプロトコル改変に関わる考察～」(全章)
  - IETF105報告会「DNS over HTTPS at IETF 105」(全章)
  - IETF106報告会「ABCD」(全章)

add WG設立までの歴史(1/2)

- DNS Resolver Identification and Use (driu) BoF (IETF102)
  - どのフルリゾルバを選択するかを議論
- Resolverless DNS ML (Jul 2018) & Resolverless-DNS Side Meeting (IETF103)
  - システムのフルリゾルバを使わずにDNS情報を得る仕組みを議論
- Various issues raised in the DoH context Side Meeting (IETF104)
  - 利用者、システム管理者、アプリケーション開発者それぞれの視点からDoHの課題洗い出し

add WG設立までの歴史(2/2)

- add ML (Apr 2019) & add BoF (IETF105)
  - Applications Doing DNS
  - DoHの議論を深化
- abcd BoF (IETF106)
  - Application Behavior Considering DNS
  - RFC 8484発行後に提起されたDoHに関する課題解決のためのWG設立を目的
- add WG (Feb 2020) ← *New!*
  - Adaptive DNS Discovery
  - INTエリア

add WGの目的(概要)

【参考：JPRSメルマガ(FROM JPRS 増刊号vol.189)】

- add WG
  - INTエリア
  - さまざまなネットワーク環境(パブリック・プライベート・VPNなど)においてDNSクライアントがフルリゾルバを発見・選択するための技術的な仕組みを標準化することが目的
  - クライアントもしくはサーバへの推奨ポリシー作成はスコープ外
  - マイルストーンは(まだ)定義されていない

IETF107 add WGの概要(1/3)

【参考:JPRSメルマガ(FROM JPRS 増刊号vol.189)】

- IETF107 add WGで取り上げられた提案(1/2)
  - Selecting Resolvers from a Set of Distributed DNS Resolvers
    - draft-arkko-abcd-distributed-resolver-selection
    - 利用するフルリゾルバを分散させてプライバシー情報の集中を避ける提案
  - Adaptive DNS: Improving Privacy of Name Resolution
    - discovery-selection directions
    - フルリゾルバの発見方式と、そのフルリゾルバに関する情報を得る方式の提案
  - DNS-over-HTTPS and DNS-over-TLS Server Discovery and Deployment Considerations for Home Networks
    - draft-btw-add-home
    - ローカルネットワークやホームネットワークでDoT/DoHサーバを発見する方式の提案

IETF107 add WGの概要(2/3)

【参考:JPRSメルマガ(FROM JPRS 増刊号vol.189)】

- IETF107 add WGで取り上げられた提案(2/2)
  - DNS Server Selection: DNS Server Information with Assertion Token
    - draft-reddy-add-server-policy-selection
    - フルリゾルバのポリシーを注釈(annotation)できるようにする仕組みの提案
    - ポリシーの内容は関知しない
  - DNS Resolver Discovery Protocol (DRDP)
    - draft-mglt-add-rdp
    - DNSリゾルバ発見プロトコルDRDPの提案

IETF107 add WGの概要(3/3)

【参考:JPRSメルマガ(FROM JPRS 増刊号vol.189)】

- IETF107 add WGで寄せられたコメント
  - プライバシーを強化したフルリゾルバの発見プロトコルを作るのか
  - 最初に原則(principle)と要求条件(requirements)をまとめるべきだ

気にすべきこと(私見)(1/2)

- 組織のフルリゾルバ運用者
  - 組織内ネットワーク利用者が参照するフルリゾルバをどうやって制御するか

  ⇒名前解決の失敗トラブルを切り分けられるようにしたい
- ISPのフルリゾルバ運用者
  - 利用者保護機構(DNSフィルタリングなど)をバイパスした利用者をどうやって識別するか

  ⇒利用者からの苦情を免責したい
- アプリケーション開発者
  - どうやって利用者にとって最適なフルリゾルバを選択させるか

  ⇒利用者に丸投げしたくない

気にすべきこと(私見)(2/2)

- 一般利用者
  - これまで通りどのフルリゾルバを使用しているかは意識したくない
  ⇒アプリごとに名前解決結果が異なるのは止めて欲しい
- IETF参加者
  - ポリシーを議論し始めると収束しない
  ⇒本当はそこを一番解決したい

⇒立場によって対立している意見もあります。DoHが気になる人はIETF add WGをフォローし、適切なタイミングで必要なコメントをしていきましょう

Q&A

【参考】

用語集

用語	
サイドミーティング Side meeting	IETF期間中に会場内で開催される非公式なミーティングで、IETFが会議室を提供してくれるもの
BoF	IETF期間中に開催される、WG設立もしくは意見収集を目的とした公式なミーティング
DoT	DNSのクエリ(問い合わせ)とレスポンス(応答)をTLS上で行う方式を規定したもの(RFC 7858)で、従来のport53/{udp,tcp}ではなく853/tcpを使う
DoH	DNSのクエリ(問い合わせ)とレスポンス(応答)をHTTPS上で行う方式を規定したもの(RFC 8484)で、443/tcpを使う
Do53	従来のDNSのことで、DoTおよびDoHとはトランスポートが異なる(従来のport53を使う)ことを明示的に区別する際に用いられることが多い
フルリゾルバ	インターネット利用者の端末やアプリケーションがインターネットサービスにアクセスする際、そのアドレスの名前解決を行うDNSサーバのこと