DNSとblocking
anti-blocking要素技術
(みえてしまう要素技術)

藤原 和典
fujiwara@jprs.co.jp
株式会社日本レジストリサービス (JPRS)

Internet Week 2018, DNS Day
2018年11月29日

自己紹介

- 氏名:　藤原和典
- 勤務先: 株式会社日本レジストリサービス (JPRS)
- 業務内容:DNS関連の研究・開発
  - RFC 5483 6116 (2004~2011):ENUMプロトコル
  - RFC 5504 5825 6856 6857(2005~2013):メールアドレスの国際化
  - RFC 7719: DNS Terminology → terminology-bis
  - RFC 8198: DNSSECを用いた名前解決の性能向上
  - Internet Week 2018 プログラム委員

- 個人ページ: http://member.wide.ad.jp/~fujiwara/

普段の生活環境 (自宅)

- フレッツネクスト + ISP契約 (固定アドレス, 半固定アドレス)
- 自宅内になんでもサーバ: フルサービスリゾルバ
- 自宅内の名前解決には自前のフルサービスリゾルバ使用

- ところで、DNS BlockingはISPで行われている

- あれ？　Blockingを回避している？　(無意識の回避？)

普段の生活環境 (出張時、外出時)

- 海外出張時でも日本国内限定サービスを使いたい
  - 動画配信系全般, D社のゲーム
- 手元のネットワークが信用できない
  - 公衆WiFi, 会議場WiFi では第三者がパケットキャプチャする
    - NANOGミーティングでは、平文の通信なんか使うなということで、平文telnetのパスワードを公開していた
  - 某国の金盾

- 回避策: 日本までVPN, SSH, リモートデスクトップ(rdp)
- 筆者の対策: 自宅までssh, http* over ssh, rdp over ssh
- IPアドレス限定対策と盗聴対策のつもりが、anti-blocking？

対象とするDNS Blocking

- ISPが利用者に提供しているフルサービスリゾルバで実施している、特定のドメイン名を問い合わせると別のサイトに誘導するサービス
  - 安心ネットづくり促進協議会のブロッキングの仕組み
    - https://www.good-net.jp/blocking/mechanism/

- 金盾のような中間者攻撃は対象としない
  - ユーザがどこに問い合わせても、特定の名前には変な応答が戻る
  - ルートサーバへの問い合わせにも変な応答が戻る
  - 対策は、安全な国へのVPN/ssh (tunneling)

Anti-DNS blocking のためには

- DNS BlockingしているISPのフルサービスリゾルバ(DNSサーバ)を使わなければよい

- IPアドレスでのアクセス: http://192.0.2.1/files/illegalpic001.jpg
  - (Webサーバが名前ベースのバーチャルホストしていたらアクセスできない)
- hostsファイルへの追加
  - /etc/hosts, C:¥Windows¥System32¥drivers¥etc¥hosts など
  - IPアドレス　ホスト名　　例: 192.0.2.1 www.example.com
- 別のフルサービスリゾルバ（DNSサーバ)の使用
  - Public resolver (DNS) service: 8.8.8.8 9.9.9.9 1.1.1.1など
  - 自前でフルサービスリゾルバを動作: 企業や、自宅のサーバ
- 別の通信手段の使用: Tor, HTTP Proxy, VPN

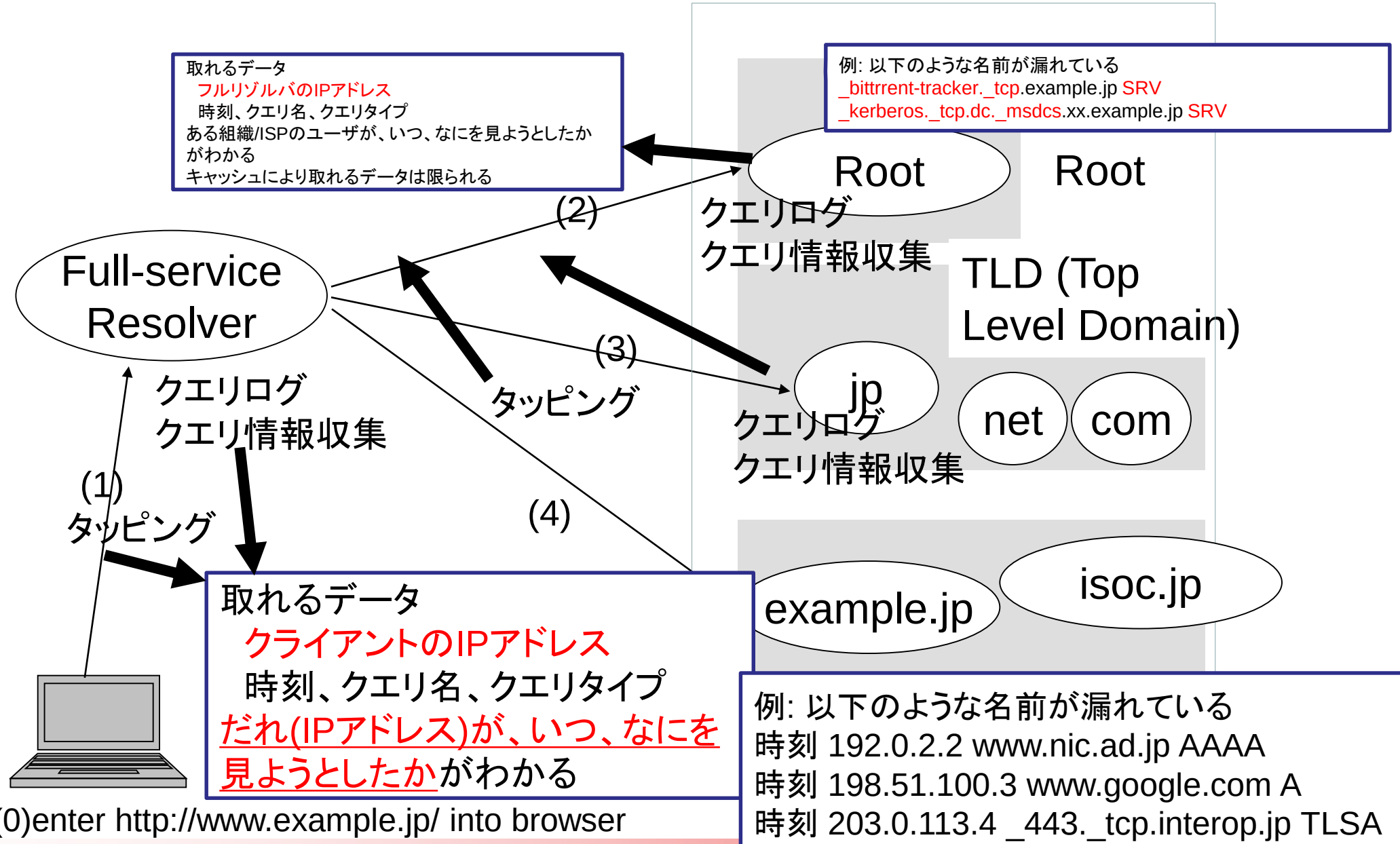
(Anti-blockingに使える)
DNSプライバシーを守る要素技術

- DNS over TLS (DoT)
  - 端末からフルサービスリゾルバの通信をTLSで保護

- DNS over HTTPS (DoH)
  - 端末からフルサービスリゾルバの通信をHTTPSで保護
  - IETFで標準化中の方式
  - 独自方式

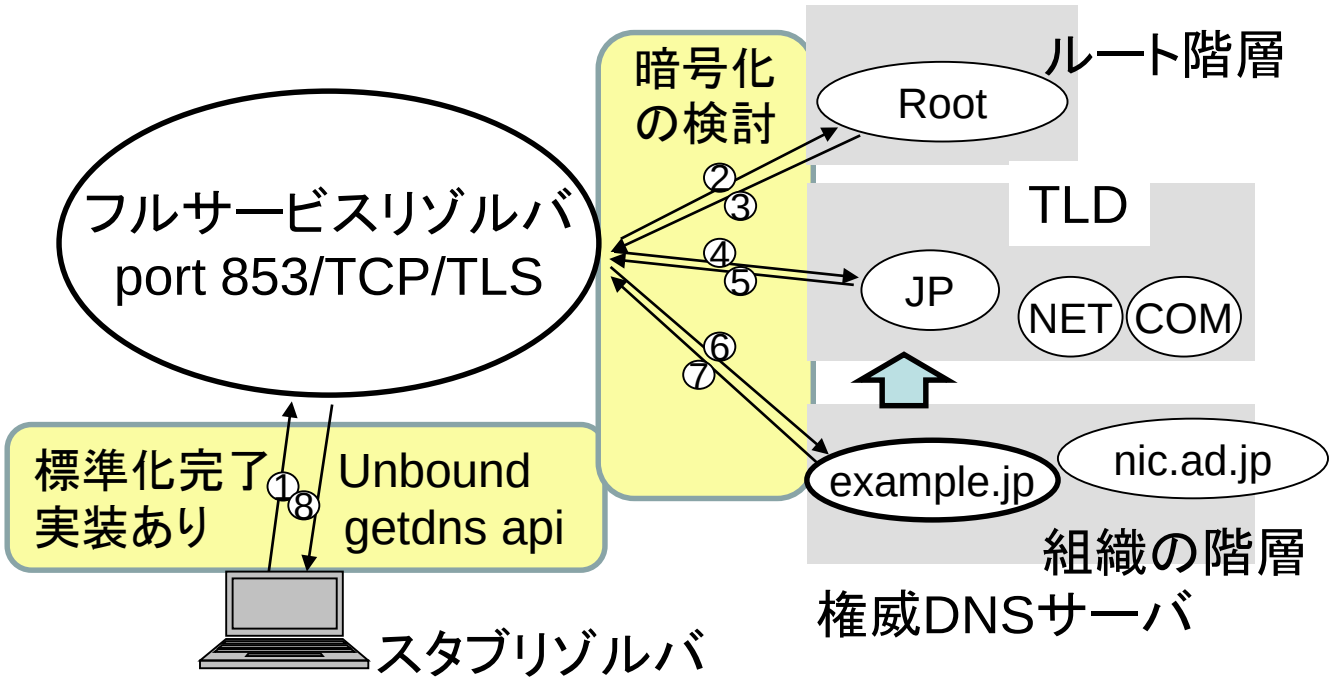
  - DNS over HTTPSなら通常のWebの通信と区別できないので、DNS over TLSよりも区別しづらく、ブロックされにくい

プライバシーの懸念



DNS over TLS (DoT)

- RFC 7858 (DNS over TLS) 2016/5/17発行
  - DNSクエリをTCPで行い、さらにTransport Layer Security(TLS)で暗号化
  - TCP port 853 を使用
  - Unboundやgetdns apiで使用可能
- RFC 8094: DNS over DTLS
  - Datagram Transport Layer Security
  - UDP port 853



DNS over HTTPS (DoH)

- RFC 8484
  - DNS Queries over HTTPS (DoH)
  - DNSワイヤフォーマットのデータをHTTPSで通信
  - GETではbase64エンコード、POSTではbinaryのまま
    - :method = GET
    - :scheme = https
    - :authority = dnsserver.example.net
    - :path = /dns-query?dns=AAABAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAAQAB
    - accept = application/dns-message
- 独自方式
  - あるURLにアクセスすると名前解決結果が(独自JSONで)得られる
  - https://dns.google.com/resolve?name=internetweek.jp

→ {"Status": 0,"TC": false,"RD": true,"RA": true,"AD": true,"CD": false,"Question":[{"name": "internetweek.jp.","type": 1}],"Answer":[{"name": "internetweek.jp.","type": 1,"TTL": 286,"data": "192.41.192.146"}]}

具体的なanti-blocking設定方法

- Windows 10
- MacOS
- Android
- iOS
- Firefox

- *BSD, Linux など: 省略 / 自前で名前解決すればよい

Windows10

- コントロールパネル → ネットワークとインターネット → ネットワーク接続
  - 使っているネットワークインターフェースのプロパティを開く
  - 「インターネットプロトコルバージョン4」のプロパティを開く
  - 「IPアドレスの設定」を変更しない
    - 「IPアドレスを自動的に取得する」のまま変更しない
  - 「次のDNSサーバのアドレスを使う」 を指定

    8.8.8.8, 9.9.9.9, 1.1.1.1 など使いたいものを指定する

  - 「インターネットプロトコルバージョン6」も同様に変更する
    - Public DNSなどのIPv6アドレスを指定

MacOS

- システム環境設定 → ネットワーク → インターフェース指定 → 詳細 → DNS
- フルサービスリゾルバのアドレスを指定する
  - 8.8.8.8, 9.9.9.9, 1.1.1.1 など使いたいものを指定する

Android

- DNS設定だけ変更してVPNを張らないというVPN”アプリ”
- “DNSスイッチ”, “DNS Changer”など多数
  - フルサービスリゾルバを変更
- “1.1.1.1: Faster & Safer Internet” (Cloudflare)
  - フルサービスリゾルバをCloudflare DNS (1.1.1.1など)に変更
- “Intra” (Jigsaw Operations LLC)
  - 名前解決にDNS over HTTPSを使用させる
  - Google, Cloudflare またはそれ以外のDoHサービスを指定できる
  - ソースコードも公開: https://github.com/Jigsaw-Code/Intra
- Android 9.0 は DNS over TLS 対応 とのこと
  - プライベートDNSという項目で、ホスト名で指定するそうです

iOS

- WiFiの設定でフルサービスリゾルバのアドレスを設定可能
- “1.1.1.1: Faster & Safer Internet” (Cloudflare)
  - 1.1.1.1を設定できるようです
- “DNS Override” という”アプリ”でリゾルバアドレスを設定できるようです

Firefox

- ~~https://wiki.mozilla.org/Trusted_Recursive_Resolver~~
- ~~URL欄に about:config と入力し、動作保証外となる設定変更を行う~~
- ~~network.trr.mode を検索して、3 にする~~
- ~~network.trr.uri を検索して、DNS over HTTPSサーバを指定~~
- ネットワーク設定の接続設定
  - ☑DNS over HTTPSを有効にする(B)
  - URL(U): [https://mozilla.cloudflare-dns.com/dns-query]

anti-blocking技術の懸念点

- 第三者が運用するリゾルバサービス (Public DNS service)
  - いつ(時刻)、だれ(IPアドレス)が、なに(クエリ名、クエリタイプなど)を見ようとしたかを事業者に知られる
  - プライバシーポリシーを信用するかどうか (信じる者は救われる？)
  - 有名なので、狙われることもある (トルコでの8.8.8.8ハイジャック)

- Tor: 仕組みを理解してから使うこと
- VPN: VPN先が安全か？ Blockingしていないか？
- HTTP Proxy: 仕組みを理解して、自分で動かして使うこと
  - 第三者が提供するProxyの場合は情報を取られることに留意