IETF 89 報告
DNSプライバシ、DNS関連

藤原 和典
<fujiwara@jprs.co.jp>
株式会社日本レジストリサービス (JPRS)
IETF 89 報告会, 2014年4月11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)
  技術研究部
- 業務内容:DNS関連の研究・開発
- 活動
  - qmail IPv6対応、tcp wrapper風のものの試作(1997頃)
  - DNSSECの事前検討 (2002~2010)
  - DNS関係のトラフィック解析など (2005~)
  - IETFでの標準化活動 (2004~)
    - DNS関連WG（dnsext, dnsop）における議論に参加
    - enum WG RFCs: 5483 6116
    - eai WG RFCs: 5504 5825 6856 6857
    - draft-fujiwara-dnsop-ds-query-increase

DNSを扱ったWG/BoF

- DNS関連WG
  - dnsop　　DNS運用ガイドラインの作成
  - dnssd　　DNS-SD (RFC 6763)の拡張
  - dane　　DNS(SEC)にTLSの証明書を載せる
- DNS関連の新規テーマ (BoF)
  - dnse　　秘密保持のためにDNSクエリを暗号化
  - dbound　　Public Suffix Listの次を考える
- DNSの話題があったWG
  - apparea　　Application area
  - homenet　　家のネットワーク

- 本日の内容: DNSプライバシの話を中心に

DNSプライバシ: 経緯

- 2013年6月のスノーデン氏の暴露事件のあと、IETFでは各種プロトコルを盗聴から守ることが検討されてきた
  - perpass mailing listで議論、draft提案
- DNSクエリは暗号化されていない
  - DNSSECは署名のみ
- DNSサーバ運用者はDNSクエリの中身を見ることができる
- 第三者が通信路をタップして中身を見ることができる
- という背景で、DNSからの情報の流出を止めることを考えるBoFが開催されたようです。

dnse BoF

- Encryption of DNS requests for confidentiality BOF
  - 秘密保持のためにDNSリクエストを暗号化
- チェア
  - インターネットエリアディレクタ のBrian Haberman氏
- 目的
  - dnsop WGへの問題提示
  - DNS運用者と実装者の興味の把握
  - DNSクエリの秘密保持についての議論
- 議論の流れ
  - 問題点の提示
  - 解決案の提示
  - 議論

DNSプライバシ: 問題点

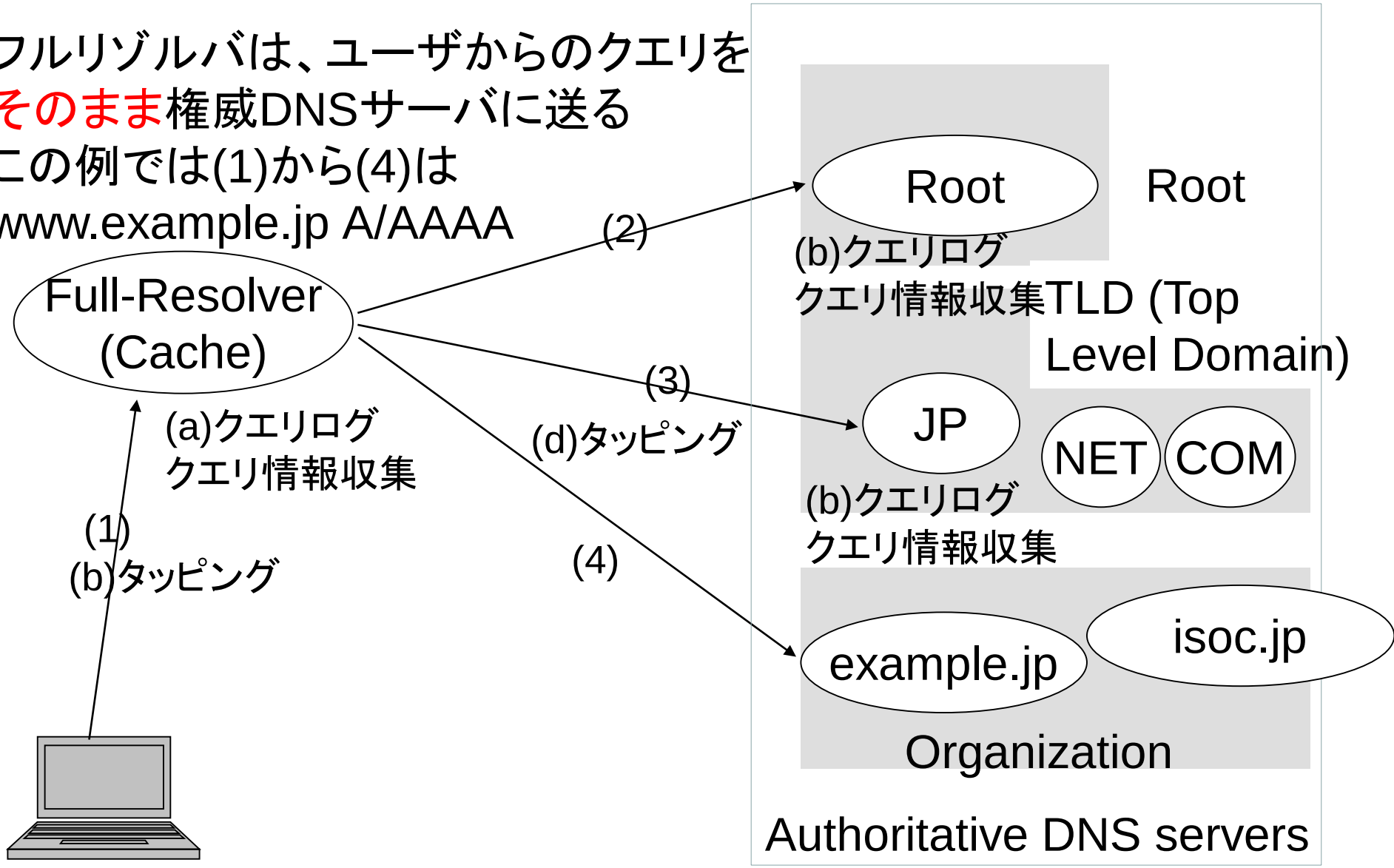
- 問題点の提示 (Problem Statement)
  - draft-bortzmeyer-perpass-dns-privacy-01
  - draft-bortzmeyer-dnsop-dns-privacy-01
  - draft-koch-perpass-dns-confidentiality-00

- DNSクエリ情報収集と懸念、問題点の提示
  - DNSには暗号化の仕組みがない
  - RootやTLDでも細かいクエリ名が見える
    - _bittrrent-tracker._tcp.example.jp
      (あるアドレスがbittrrentを使用しているという情報が漏れている)
    - _kerberos._tcp.dc._msdcs.subdomain.example.jp
      (Active Directoryを使っているという情報が漏れている)

- クエリ情報の使用例
  - malwareの判定: クライアントからのクエリを監視し、malwareが使う名前を検索していれば影響されていると判断するなど

復習:DNSの動作とクエリ情報

フルリゾルバは、ユーザからのクエリを
そのまま権威DNSサーバに送る
この例では(1)から(4)は
www.example.jp A/AAAA



復習:DNSクエリ情報が持つ情報

取れるデータ
フルリゾルバのIPアドレス
時刻、クエリ名、クエリタイプ
ある組織/ISPのユーザが、いつ、なにを見ようとしたかがわかる
キャッシュにより取れるデータは限られる

Full-Resolver (Cache)

(a)クエリログ
クエリ情報収集

(b)タッピング

(1)

(3)

(d)タッピング

(4)

Root

Root

(b)クエリログ
クエリ情報収集

TLD (Top Level Domain)

JP

NET

COM

(b)クエリログ
クエリ情報収集

example.jp

isoc.jp

Organization

thoritative DNS servers

取れるデータ
クライアントのIPアドレス
時刻、クエリ名、クエリタイプ
だれが、いつ、なにを見ようとしたかがわかる
すべてのデータをとれる

(0)enter http://v

参考: DNSクエリ情報収集活動

- Root
  - 年に一度、50時間、ルートサーバなどのクエリ情報を収集
  - 研究やRootの運用に使用 (name collisionの評価など)
- JP
  - Rootと同じタイミングなどで、全JP DNSのクエリ情報を収集
  - [AG].DNS.JPクエリログを2004年から継続して収集
  - 研究やJPの運用に使用 (IPv6/DNSSECなどの普及度など)
- フルリゾルバ
  - 大学などで、組織内向けに提供しているフルリゾルバのクエリ情報を収集し、研究に使用
  - Google Public DNS
    - IPアドレスだけ集め、24時間で消すと以下に書かれている
    - https://developers.google.com/speed/public-dns/faq?hl=ja#privacy
- その他
  - 国レベルでのパケットキャプチャと書き換え

DNS通信の暗号化提案(1)

- IETFで標準化したプロトコルを使って暗号化
  - IPsecとDTLS
  - IPsecは困難
    - 拡張ヘッダが通らない、クライアントの鍵も必要
  - DTLS(Datagram Transport Layer Security)
    - TLSの機能をUDPで使えるようにしたもの
    - RFC 6347
- 具体的な案
  - DNSサーバにサーバ証明書を持たせ
  - (httpsのように)
  - TCPのDNSクエリをTLSで暗号化
  - UDPのDNSクエリをDTLSで暗号化

DNS通信の暗号化提案(2)

- 既存のものを使う提案(DNSCurve, DNSCrypto)
  - (IETFで標準化したプロトコルではないので不評)
- DNSCurve
  - Daniel J. Bernstein氏がデザインしたDNSの暗号拡張で楕円暗号を用い、公開鍵をDNSサーバ名に埋め込む
  - フルリゾルバと権威サーバの通信を暗号化
  - 例: example.com. IN NS uz5bcx1nh80x1r17q653jf3guywz7cmyh5jv0qjz0unm56lq7rpj8l.example.com. (wikipediaより引用)
- DNSCrypto
  - クライアントとフルリゾルバの間でDNS専用のVPNを張る仕組み
  - OpenDNSなどが対応
- 他に二つの提案あり

dnse BoFの結論

- 要件定義(Requirements)が必要である
- 新しいプロトコルを策定した場合、プロトコルの普及に懸念がある
- 興味をもつ人が多いことは確認された
- dnsop WGとの連携が必要である

- 結果として、dnsop WGの枠を追加して、DNSプライバシについて議論することになった (dnse BoFの二日後の夕方に開催)

DNSプライバシ (dnsop)

- 新しい解決案の提案
  - GoogleのQUICをトランスポートに使う
    - UDPの上にTCP+TLS相当の機能をのせたもの
    - 一往復で鍵交換できるとのこと
    - DNSサーバにサーバ証明書が必要
- クエリの送り方の議論
  - フルリゾルバから権威DNSサーバにはクライアントからのクエリを送るが、短くして送ると漏れる情報が減る
    (例:rootにはTLDだけ、jpにはexample.jpだけ)
- 結論: まだ議論が必要である
- 興味を持つ人は多いため、dnsopメーリングリストとは別にdns-privacyというメーリングリストを作る

DNSプライバシ:IETF 89後の動き

- 3/17に dns-privacy@ietf.org が作成
  - https://www.ietf.org/mailman/listinfo/dns-privacy
  - 3/19から議論が始まっている
- Dnsop WGのチャータに、DNSプロトコルの小規模な拡張を行うことが提案されている

- 今後も継続して議論されていくと考えられる
  - まずは要件定義とアイデアの検討

DNSプライバシに関する感想

- 盗聴暴露事件からの動きが性急すぎ、簡単なところから対応しようという動きが見える
  - 暗号化の実装は難しくない (普及は困難だけど)

- DNSサーバでのクエリデータ取得について
  - 意見はあまりなかった
  - 権威DNSサーバはデータを提供しているのでWebサーバのアクセスログと同じではないか
    - 漏れる情報を減らす方法はある
  - フルリゾルバは通信を媒介する？
    - 組織内のフルリゾルバは組織内で決めればよいはず
    - 他者のサービスを使う場合は、各国の法律と約款に注意

DNSプライバシ以外

dnsop WG (DNS Operations)

- DNS運用ガイドラインを作るWG

- 特に新しい結論はなく、議論を継続することになった
  - 従来からの議題でWGLCに向けて進めるもの
    - AS112 (プライベートアドレスの逆引きなど)をDNAMEで
    - DS/NS/グルーの自動更新
  - ドメイン名に似た名前空間の話題
    - p2pサービスで使われる.gnuや.orangeの予約を提案
    - 3提案: .localのように予約、.altにまとめる、気にしない
    - 課題: .localや.homeには大量にクエリが来ている
      これらと同じことが起こりうるという指摘

dnsop WG (続き)

- チャーター更新
  - DNSプロトコルのアップデートを追加したいという人はいる
  - 最新の更新案でDNSプロトコルの拡張が追加された
- 活動再開、レビューアを募集したもの
  - DNSの応答サイズ
  - プライミング (ルートサーバ情報の取得・更新の仕組み)
- getdns API
  - Paul Hoffman氏が提案され、複数の人が参加
  - Version 0.1.0が2014年2月にリリース
  - http://getdnsapi.net/
  - libldns + libunbound + libexpat + libidn をもとに必要な機能を作りこんだとのこと
  - appareaでも紹介

dnssd WG (Extensions for Scalable DNS Service Discovery)

- DNSを使ったサービスディスカバリを作るWG
  - DNS-SD (RFC 6763)をベースに、複数ネットワークセグメントに対応したものを標準化する

- Requirementはほぼ合意された
- 最初の候補を考える時期になってきた
  - mDNSのブリッジ
  - 通常のDNSとマルチキャストDNSの複合プロキシ
    - 検索時は、DNSとmDNSの両方を検索
    - mDNSで登録された名前をDNSにどう展開するか
  - 家電機器などの情報をDNSに出すことへの懸念
  - 複雑さを増すことへの懸念など
  - WG参加者の理解は深まった

dane WG

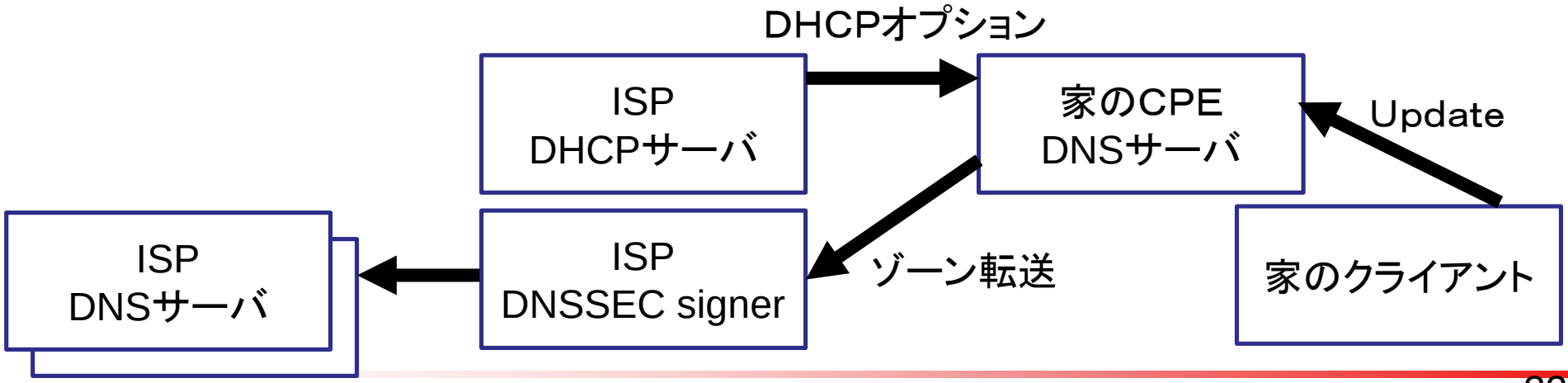
- DNSにTLSの証明書を載せるWG
- 今回の議題
  - WGの今後: プロトコルが完成したら閉じるか？
    - 個々のプロトコルへの実装のサポートが必要というコメントがあったが、継続して議論
  - SMTP, SIP, XMPPなどへの適用した場合の深い話が議論された
    - 実装が進み、曖昧な点、間違いの指摘が進んだ
    - SMTPでは、TLSA RRがない場合にフォールバックして暗号化しないで送るのは危険であるといった指摘など
  - OpenPGPへの適用について
    - メールアドレスの正規化についての問題点が指摘された
    - メールアドレスのローカルパート(ユーザ名部)は大文字小文字区別されることになっているため

dbound BoF (Domain Boundaries)

- Public Suffix Listの仕組みを改善する活動
  - 目的: WGを作り、標準化を完了できるかを判断すること
- Public Suffix List
  - Webブラウザでクッキーを扱う時に、ドメイン名境界を判断する必要がある
  - 現在は固定のリストで管理されており、一部のブラウザに埋め込まれている　https://publicsuffix.org/
  - 2014/4/8現在 8181行のテキストファイル(うちjp 1756行)
- 議論
  - DNSを使った実装などが提案され、議論された
- 結論
  - 結論が出ず、チェアが “not comfortable” と感想を述べ、次のBoFを準備する人を募集した

homenet

- draft-mglt-homenet-dnssec-validator-dhc-options-01
  - 要求: 宅内のホスト情報をインターネットに出したい
  - 提案: 家庭のCPEがhidden masterで、ISPのDNSサーバに転送してDNSSEC署名し、ISPが権威DNSサーバを動かすという提案
  - マルチホームのときにどうするかという質問や、
  - 家のゾーンは自分のものだから、自分でDNSSEC署名したいという主張があった



参考

- http://www.ietf.org/meeting/proceedings.html
  - 過去のIETFミーティングの資料、議事録あり
- https://www.dns-oarc.net/oarc/data/ditl
  - Rootの情報収集と、データへのアクセス方法
- https://publicsuffix.org/
  - Public Suffix List