DNSのタベ
-セキュリティ・技術的動向に関して-

藤原 和典
<fujiwara@jprs.co.jp>
株式会社日本レジストリサービス (JPRS)
第一回 ISOC-JP 勉強会
2014年7月29日

自己紹介

- 氏名:　　藤原和典
- 個人ページ: http://member.wide.ad.jp/~fujiwara/
- 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(root, jp, 大学)など (2005~)
  - IETFでの標準化活動 (2004~)
    - DNS関連WG（dnsext, dnsop）における提案と議論
    - enum WG RFCs: 5483 6116
    - eai WG RFCs: 5504 5825 6856 6857

本日のテーマ

http://www.isoc.jp/wiki.cgi?page=1st_ISOC_JP_Workshop より引用

- 「DNSのタベ -セキュリティ・技術的動向に関して-」
- DNSは，インターネットの根幹を支えるシステムの一つですが，ここ最近，多くの課題が発覚しています．また，利用方法等，新しい提案も実施されています．この勉強会で，DNSSECの現状等，昨今のDNS関連の課題や，IETFで議論されている最新の技術動向について，藤原さんにご紹介頂き，その後の議論を通じて最近の動向を共有致します．

どのような内容がよいでしょうか？

- IETF 90 速報
- DNSSEC (新規な情報なし)
  - 悪影響 (IEPG資料)
- DNS privacy (IETF 89報告会)
- 最近流行りのDoS攻撃
  - Reflector attacks ()
  - フルリゾルバ (伝聞で紹介可能)
  - 権威DNSサーバ ()
- Cache poisoning (IEPG, JANOG)
- トラフィック解析 (DNS-OARC, IEPG)
  - ルート、JP、大学など

IETF 90 DNS関連 速報

dnsop (1)

- DNS Operations WG
- 3月以降、完了したもの
  - チャーター更新: DNSプロトコルの軽微な修正追加
  - DS自動更新 (rfc editor queue)
    - 対応しているTLDなどでは、子側にCDS, CDNSKEYを書くと、親が子ゾーンを定期的にチェックし、親側のDSを自動的に書き換える
  - 親のNS/glue自動更新 (IESG処理中)
    - 対応しているTLDなどでは、子側にCSYNCを書くと、親が子ゾーンを定期的にチェックし、親側のNSとグルーを自動的に書き換える
  - AS112 DNAMEとrfc6304bis (IESG処理中)
    - プライベートアドレスの逆引きを、DNAMEを使って実装
    - いまは多数のゾーンを管理しないといけないが、empty.as112.arpaゾーンを保持するだけでよくなる

dnsop (2)

- 新規: Scaling root zone
  - draft-wkumari-dnsop-dist-root
    - ルートゾーンを配布するという提案
    - フルリゾルバがルートゾーンを持てば、ルートサーバの負荷が軽くなる
    - 遅滞なく大規模に配布することは困難
    - いまでも、f.root-servers.netのslaveにすると可能
    - ICANNサービス　http://www.dns.icann.org/services/axfr/
  - draft-lee-dnsop-scalingroot
    - Xiaodong Lee (CNNIC), Paul Vixie, Zhiwei Yan
    - いまのroot serversをつぶして作り直そうという提案
    - 不評

dnsop (3)

- DNSSEC Validator requirements
- 変なフルリゾルバの避け方 (ホテルとか)
- 鍵と署名ポリシー
- キャッシュポイズニング対策再び
- IPv6の逆引き再び
- マルチキャストアドレスの逆引きをどうするか

dnssd

- Extensions for Scalable DNS Service Discovery
- Requirementsは完了
  - マルチキャストの電力消費の話を追記
- セキュリティモデル
- プロトコルの実装はハイブリッドプロキシーになりそう
  - 既存のDNSとmDNSをプロキシーする
  - 例: lb._dns-sd._udp.meeting.ietf.org. ptr
  - 例: _pdl-datastream._tcp.meeting.ietf.org. ptr
  - 例: term-printer._pdl-datastream._tcp.meeting.ietf.org srv

IEPG meeting

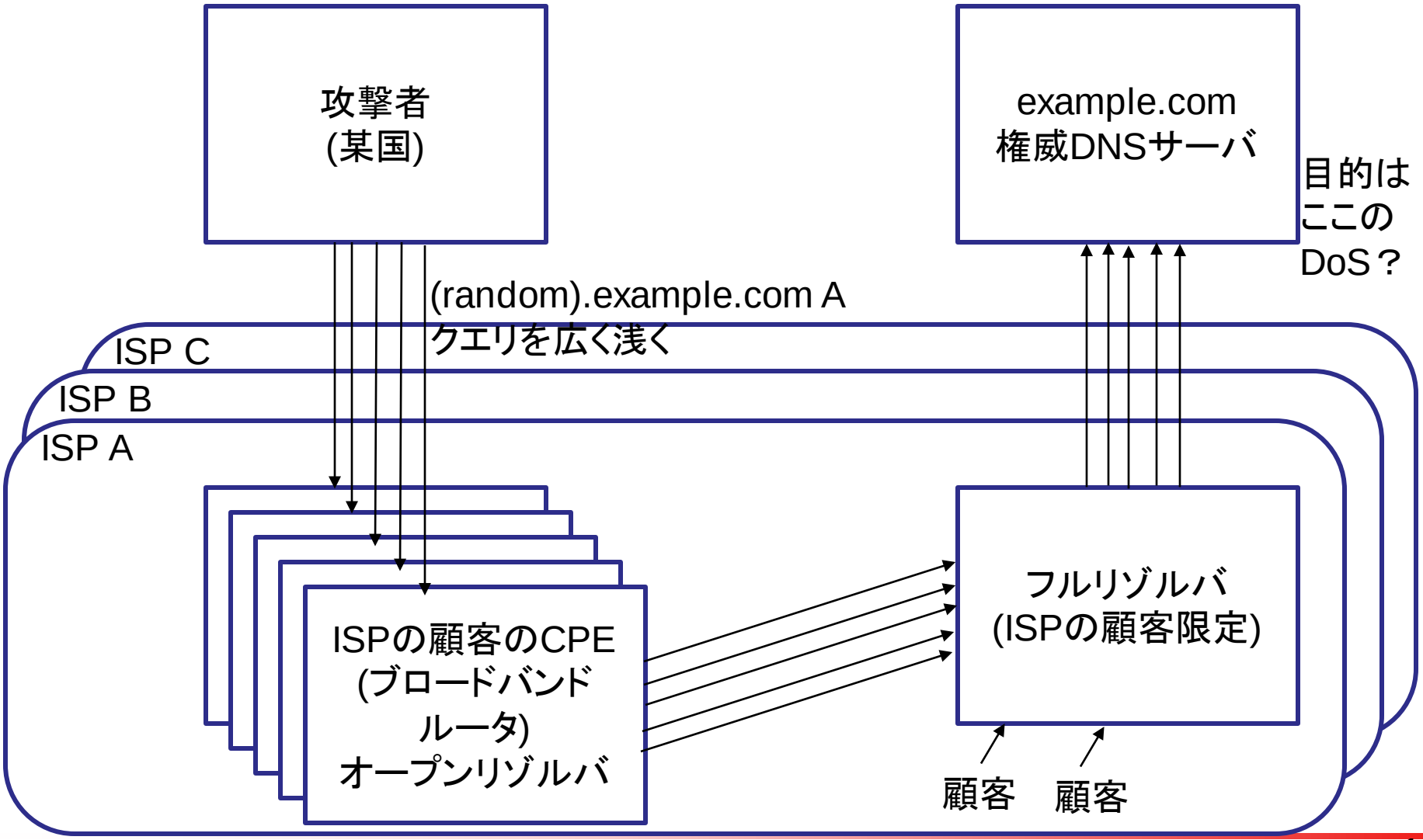
- DNS: what if everyone did it?, Geoff Huston
  - DNSSECの悪影響の話
  - DNSSEC検証の普及度を調べたら、検証しないものが80%
  - DNSSEC検証で200~500msほど名前解決が遅くなる
  - DNSSECでDNSトラフィックは7.5倍
- Redirecting the target domain's nameserver cache poisoning attacks

フルリゾルバへのDoS

DoS: フルリゾルバ

- 伝聞
- 最近某国方面から、CPEのオープンリゾルバ経由でISPのフルリゾルバが攻撃されているらしい
- ランダムプリフィックスをつけたクエリ名
- ランダムということは、キャッシュに存在しないため、権威DNSサーバに問い合わせ
  - キャッシュにないクエリの処理は重い
  - 権威DNSサーバが落ちたり、応答が遅いと処理中のクエリ処理が増える
  - 同時に処理可能なクエリに限界があって、通常のクエリが影響を受ける → クレーム

DoS: フルリゾルバ:図



DoS: フルリゾルバ:対策

- ISPのフルリゾルバでの対策
  - 攻撃されているドメイン名の名前解決を停止
    - ローカルにexample.comゾーンを持たせてエラーにする
    - 副作用としてexample.comの名前解決ができなくなる
  - BIND 9.11にExperimentalな実装が入る見込み
    - IETF 90会場で開催されたISC/BIND users meetingでアイデアの発表があった
    - 応答しなくなったサーバの検知と関連クエリ抑止機能
    - ゾーンごと、クライアントごとの制限機能
    - 確率的にクエリを落とす機能
- CPEのオープンリゾルバ対策
  - 顧客への53/udpのブロック(IP53B)が話題に
  - 追記: 2014/7/22改定のJAIPA「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」に記載があるとのこと