# IETF 88 報告
# 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 88 報告会, 2013年12月20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

# 報告対象WG

- DNS関連WG
  - dnsext*　　DNSプロトコル拡張 (2013年7月に完了)
  - dnsop　　DNS運用ガイドラインの作成
  - dnssd　　DNS-SD (RFC 6763)の拡張

- DNSの話題があったWG (IETF87)
  - 6man　　IPv6 Maintenance

- IEPG (同時開催の別会議)

*はIETF 88では会議なし

# dnsext WG (DNS Extensions)

- DNSプロトコルを拡張するWG
  - 2013年7月24日に完了
  - メーリングリストは継続して使用可能:dnsext@ietf.org
- 2013年8月から12月のメーリングリストの議論
  - SPF RR廃止提案の議論: TXTか独自タイプ(SPF)か
  - プロトコルの不明点の明確化: 不在証明とtype bitmap
  - edns-tcp-chain-query: ひとつのクエリでDNSSEC検証に必要な複数のRRSetを取得する提案
  - Dynamic Updateにゾーンの追加削除機能追加
  - DNSの脆弱性
  - DNAMEは使えるかどうか

# dnsop WG (DNS Operations)

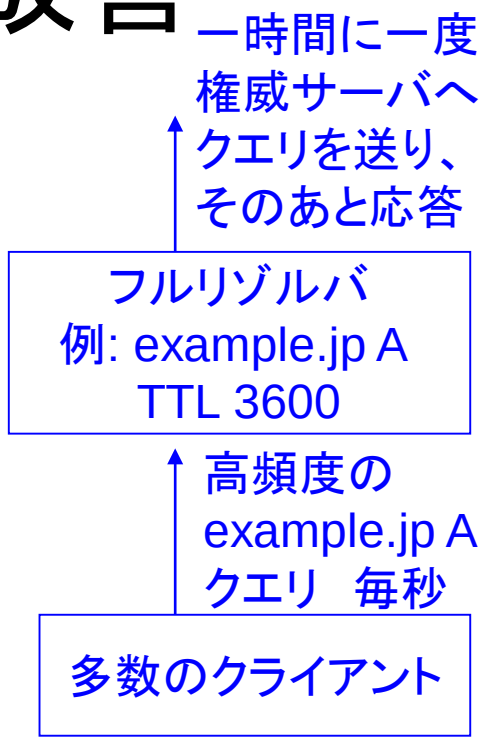
- DNS運用ガイドラインを作るWG
  - DNSSEC運用
  - ルートサーバ、TLDの運用も含む
- 1999年6月に開始
- 現在までの主な成果 (2013/9から変化なし)
  - RFC 2870: ルートDNSサーバ運用の要求条件
  - RFC 3258: DNS Anycast
  - RFC 3901: IPv6 DNSサーバのガイドライン
  - RFC 5358: Reflector Attacksへの対策
  - RFC 6303: Locally Served DNS Zones (プライベートアドレスなどの逆引き)
  - RFC 6781: DNSSEC Operational Practices, Version 2
  - RFC 6841: DNSSECポリシーの枠組みとDPS

# dnsop: Meeting Agenda

- 前回と異なり、90分で予定していたAgendaをしっかりと完了
  - 前回は積み残しあり
- Agenda
  - キャッシュ方式の改善 (継続)
  - Child Delegation / 委任情報(DS)の自動更新 (継続)
  - JPで観測したDSクエリ増大問題
  - PCP to update Dynamic DNS  (PCP WG)
  - AS112 with DNAME (継続)
  - 遠隔地からのキャッシュのフラッシュ (継続)
  - edns-tcp-chain-query (dnsext WGの話題)
  - IPv6マルチキャストアドレスの逆引き
  - IPv6 prefix delegationのアドレスの逆引き登録方法

# dnsop: キャッシュ方法の改善

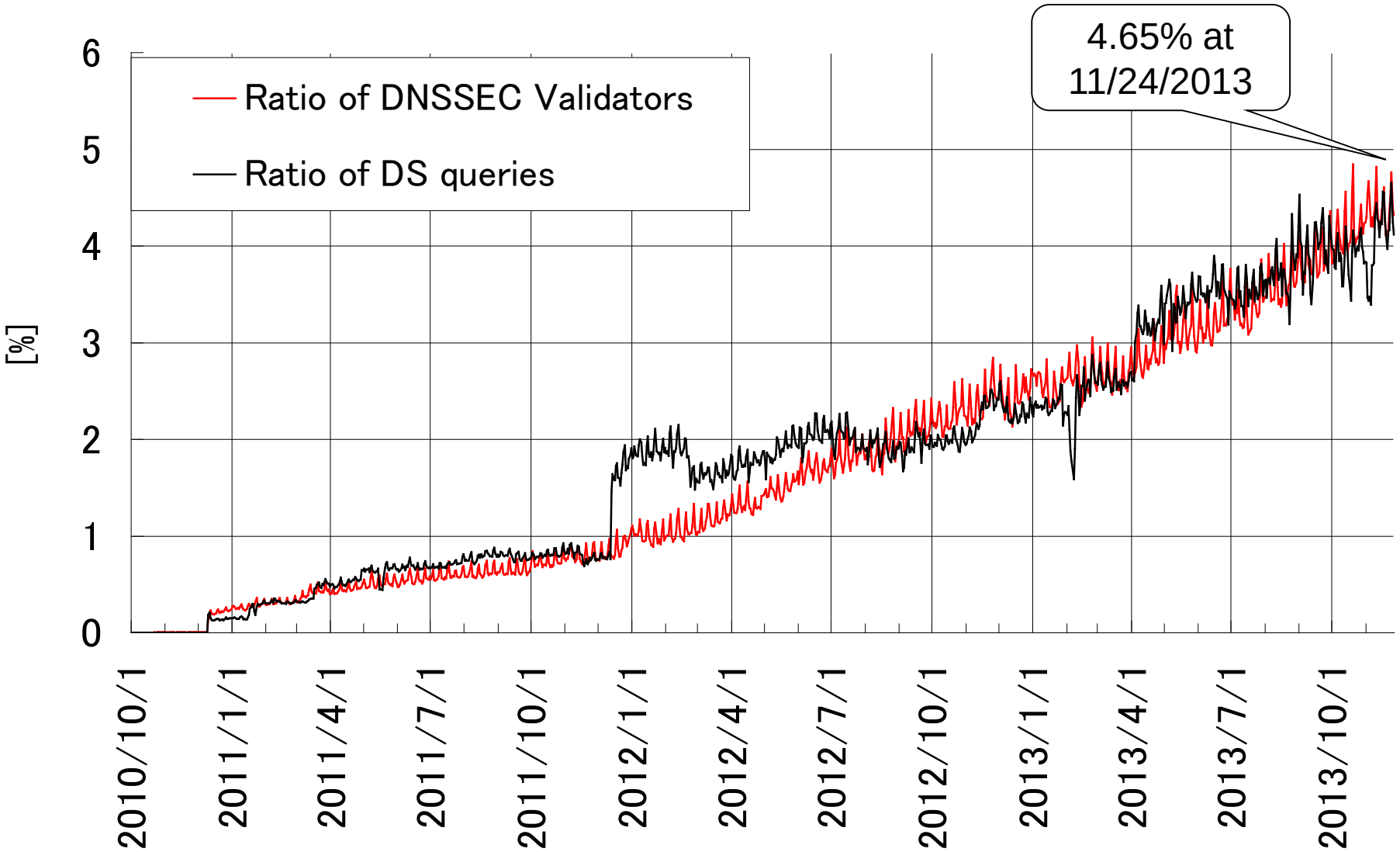
- 問題の指摘と提案 (IETF87)
  - キャッシュにあれば低遅延で応答できる
  - TTL経過後の最初のクエリは時間がかかる
  - 忙しい名前はTTLごとに定期的に遅延増大
  - クライアントからのクエリ時に、キャッシュ内のTTL残りが2以下であれば、応答と再クエリ
  - draft-wkumari-dnsop-hammer-00
- 今回のミーティングの議論
  - Unboundに若干変更して実装し、実データをもとにシミュレーションしたところ、1.5%のクエリがプリフェッチされたが、遅延の改善は大きくなかった
  - いくつかの有名な名前で評価すると違う結果がでるのではないかといった意見が出た
  - 元の提案に今回の結果を追加することとなった



# dnsop: JPで観測したDSクエリ増大

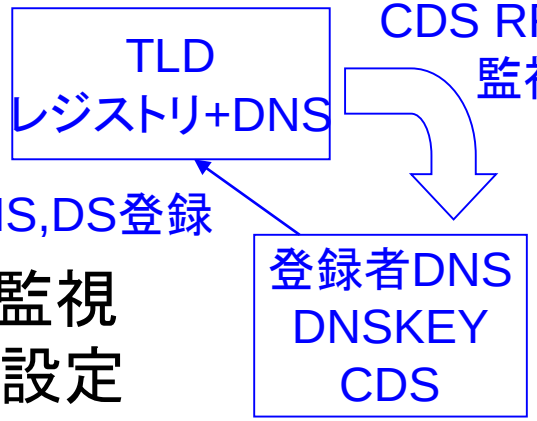
- draft-fujiwara-ds-query-increased
- DNSSEC Validatorと推定されるIPアドレスからJP DNSへ大量のDSクエリが送信されている
- 原因
  - ほとんどの有名なドメイン名がDNSSEC非対応でDSがない
  - 現在のJPのNCACHE TTLは900
  - 有名なドメイン名のA, AAAA TTLはロードバランスなどのために短い
- 結果として、有名ドメイン名のDSクエリを15分ごとに送るアドレスがみられた (忙しいDNSSEC Validator?)
- すべてのフルリゾルバがDNSSEC検証をするようになると、JPへのクエリが最大96倍(86400/900)になる懸念
- よい対策案はないが複数の案を提示
  - DNSSEC署名の普及や、NCACHE TTLを長くする、DSなしを示す新しい方法の提案など
- まだ問題は顕在化していないが、将来のために文書化をしておくことが重要であり、会議中に受けたコメントを反映することとなった

# Ratio of DS queries seen at JP 2 of 7 servers, 24 hours data



# dnsop: 委任情報の自動更新 (1)

- 子ゾーン管理者が親ゾーンに登録するDSの自動更新の提案
  - DNSSECのKSK鍵更新の手間を減らす
  - TLDレジストリによる運用が想定
- 動作
  - TLDは登録者のDNSサーバを定期的に監視
  - 登録者が自ゾーン内にDS更新の合図を設定
  - TLDは登録者ゾーンから新しいDSを入手して、レジストリDBとTLDゾーンを書き換える
- IETF87では二つの提案があり、結論がでなかった
  - DSと同じフォーマットのCDSリソースレコード
  - 複数のRRタイプを指定できるCSYNCリソースレコード



# dnsop: 委任情報の自動更新 (2)

- IETF 88での提案
  - CDSはDSを扱い、CSYNCはNS, グルーのA, AAAAを扱うという双方の提案を両立させる提案が行われた
  - 登録者がレジストラにDynamic Updateを用いてDSなどを更新するという新しい提案があった
    - レジストラはEPPなどの既存のプロトコルを用いてレジストリのDSなど変更する
    - レジストラは登録者にTSIGキーを発行することで、登録者を認証し、情報を安全に受け取る


- IETF88の結論
  - Dynamic Updateを用いた方式についても議論内容に含めた上で、継続して検討することになった

# dnsop:委任情報の自動更新(3)

- dnsop WGは運用ガイドラインを作るWG
  - DNSのプロトコル拡張はスコープ外

- CDS/CSYNCの話題について、プロトコル拡張かという質問があった
  - チェアは、プロトコル拡張は別でやり、CDS/CSYNCを使った場合のオペレーションの議論をしていると回答
  - CDSのタイプはexpert reviewにより、IANAから割り当て済

# dnsop: AS112

- プライベートアドレスの逆引き
  - 有志がDNSサーバを運用 (blackhole-[12].iana.org.)
  - AS112プロジェクト: http://www.as112.net/  48組織
  - AS112はIP Anycastのテストベッドとして利用されている
- 問題の指摘
  - ゾーン数が多い (10, 172.16~172.31, 192.168, …)
  - ゾーン数が変化: 100.64.0.0/10が追加される？
  - すべてのオペレータが即座に変化に追従するのは困難
- IETF87では二つの提案があり、DNAME方式を先にすすめることとなった
  - Omniscient: どんな応答でもエラーを返す専用サーバ
  - DNAME: DNAMEを書き、変換後のゾーン1つを運用
    - empty.as112.arpa
- IETF88では、rfc6304bisとしてWGドキュメントとすることが合意された  draft-ietf-dnsop-as112-dname-00

# dnsop: edns-tcp-chain-query

- draft-wouters-edns-tcp-chain-query-01
- DNSプロトコルの拡張を意図
- ひとつのクエリでDNSSEC検証に必要な情報をまとめて送れるようにするプロトコル拡張の提案
  - クライアントでのDNSSEC検証に必要な情報をまとめて転送 (root, TLD, 組織のNS, DS, DNSKEYやRRSIG)
  - クライアントとフルリゾルバの間を拡張
  - DNSSECの検証で必要なものをまとめて取得するため
  - クライアントの遅延が大きいところで有利
    - DNSSEC検証のためにはルートからのDS, NS, DNSKEYなどの情報がすべて必要で、遅延が大きい環境では取得に非常に時間がかかるため
- 結論
  - 有用だが、さらなる一般化や検討が必要である
    - 過去何度もA, AAAAを同時に取得するといった提案があった
  - どこで標準化するか議論が必要 (dnsopではない)

# dnsop: IETF88後の話題

- DNSでのプライバシ問題について書かれたドキュメントが提案
  - draft-bortzmeyer-perpass-dns-privacy-01
  - 守り方などの議論
- p2p用に6 TLDの予約を要請する提案
  - 著者はGNUやTorの人たちで、IESG承認の文書
  - draft-grothoff-iesg-special-use-p2p-names-01
  - .gnu,.zkey,.onion,.exit,.i2p,.bit
- Chairの交代
  - 8年以上dnsop WGのchairだったPeter Koch氏が退任予定
  - 新チェアを選ぶプロセスが開始

# dnssd WG (1)

- 概要
  - Extensions for Scalable DNS Service Discovery
  - 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
  - IETF 85で開催したmdnsext BoF，IETF 87のdnssdext BoFの結果をうけて2013/10/25にWGが設立された
- DNS-SD (RFC 6763)
  - ローカルネットワークにつないだ機器の名前解決、サービスディスカバリに用いられる
  - Apple Inc.のBonjour, LinuxのAvahi
  - 標準化状況 (IETF 85以後に下線のRFCが発行)
    - RFC 6761: 特殊なドメイン名のためのIANAレジストリ
    - RFC 6762: mDNSプロトコル (.local)
    - RFC 6763: サービスディスカバリ
    - 参考: RFC 4795 Multicast Name Resolution (Microsoft mDNS)

# dnssd WG (2)

- dnssd専用のローカルな名前解決のためのTLDの予約
  - 既存のDNS-SD(RFC 6763)では.localを使用
  - 複数の提案
    - .localを転用する
    - 新しいTLDを予約する
    - TLDではなくSLDを使用する
  - 非常に盛り上がったが、結論は出ず、継続

# dnssd WG (3)

- 要求仕様の議論
  - 提案　draft-lynn-dnssd-requirements-00
    - 同一リンク内からインターネットまでの名前解決に対応すること
    - 使いやすいこと（Usability）
    - スケーラブルであること（Scalability）
    - 段階的な普及、小型デバイスでも動作し、大規模な機器を必要としないといった、普及可能性（Deployability）
    - 使用するにあたっての安全性（Security）
  - 追加: 既存のDNS-SD/mDNSに悪影響を及ぼさないこと

# dnssd WG (4)

- 国際化ドメイン名の表現形式
  - DNS-SD（RFC 6763）ではUTF-8のU-Labelを使用し、エラーの場合はASCIIのA-Labelに変換して再問い合わせ可
    - ○○のコンピュータ.local
  - 通常のDNSでは、ASCIIのA-Labelを使用
    - XN--WGV71A119E.JP (日本語.jp)
  - DNS-SDで使用されるUTF-8のラベルがそのまま通常のDNSに漏れることが懸念される
  - どこかで変換するというアイデアは出されたが、結論はでなかった

# 6man (IPv6 Maintenance)

- IPv6プロトコルの保守、拡張を行うWG
  - DNSに影響を与える提案があった

- IETF 87(前回) フラグメントヘッダの廃止提案があったが、今回は議論されなかった
- Charterが変更され、2014/3までにフラグメントヘッダについての方向性を決めることとなった

# IEPG (1)

- IETFミーティングに先立って日曜の朝に開かれる非公式(informal)な会合で、インターネットの運用についてのテーマを扱う
  - Mailing list: iepg@iepg.org
  - Web: http://www.iepg.org/
- Agenda
  - エクアドルでのRPKIとOrigin Validation
  - Google Public DNSの利用状況調査
  - IPv6インターネットでのフラグメントと拡張ヘッダのサポート状況調査
  - Unboundを用いたDNSデータプリフェッチの実装と評価
  - IANAの特殊アドレスレジストリの改善についての相談？
  - DNSにおける各種セキュリティ機能の検討

# IEPG (2)

- Google Public DNSの利用状況調査
  - APNICのGeoff Huston氏
  - Web広告を用いてクライアントにFlashプログラムを実行させ、クライアントの用いるフルリゾルバを調査
  - 2013年5月時点でその広告をアクセスしたIPアドレス数のうち
    - Google Public DNSのみを使っているものが5.3%
    - Google Public DNSと他を併用しているものが1.9%
  - スノーデン事件以後
    - Google Public DNSのみを使っているものが4%台に減少
    - 併用しているものは、2%台に増加
  - Google Public DNSの国別の利用率なども報告された

# IEPG (3)

- Unboundを用いたDNSデータプリフェッチの実装と評価
  - IETF 87のdnsop WGで提案されたキャッシュ方法の改善をUnboundに実装し、評価したとのこと
  - 発表者: Unboundの開発者 Wouter C.A. Wijngaards氏
  - IEPGでの報告後、dnsop WGでも報告された
  - 変更点
    - TTL 2秒以下のときにプリフェッチから、元TTLの10%以下になっていたらプリフェッチ
    - オリジナルTTLが6以下のときに除外から、9以下のときに除外
  - 評価結果
    - 1.5%のクエリがプリフェッチされた
    - 権威DNSサーバへの問い合わせ状況はごくわずか
    - 応答遅延時間が短いものが増加した
  - 分析ではTTLで指定された時間内に到達した問い合わせ数NとTTLの比率を用いて、N/TTL > 0.1を人気にある名前と定義
  - 人気がある名前に対してDNSデータプリフェッチが有効であることが示された

# IEPG (4)

- DNSにおける各種セキュリティ機能の検討
  - Farsight SecurityのPaul Vixie氏
  - DNSに対する脅威と対策について、コスト面から検討した結果が示された
    - TCPの常用
    - DNS RRLにおけるslipの設定変更
    - ANYレコードに対する対策
  - 攻撃に対する対策はコストがかかる
  - セキュリティは経済（economics）であり、過去から現在、未来になるに従い、徐々に高コストとなっていくと結論づけられた

# まとめ

- DNSの話題は減らないが、dnsextが閉じたため、dnsopでプロトコル拡張まで事実上扱っている状態

- DNS関連のプロトコルについてはdnssd WGが設立された
- DNSそのもののプロトコル拡張を扱うWGが必要にみえる

# 用語解説

- DNS: Domain Name System
  - ドメイン名（例: isoc.jp）とIPアドレスやメールサーバ情報などを対応付ける仕組み

- DNSSEC: DNS Security Extensions
  - 暗号技術(電子署名)を用いてDNS応答が改竄されていないかを受信側で確認できるようにする仕組み