IETF 92 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 92 報告会, 2015年4月24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
- IETFでの活動 (2004~)
  - 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 (互換性部分を担当)
  - draft-fujiwara-dnsop-ds-query-increase(2013/6~)
  - draft-fujiwara-dnsop-poisoning-measures (2014/7)
  - draft-ietf-dnsop-dns-terminology (2014/11~)
  - draft-fujiwara-dnsop-nsec3-aggressiveuse (2015/3~)

DNSを扱ったWG/BOF

- DNS関連WG/BOF
  - dnsop　　DNS運用ガイドラインの作成
  - dprive　　DNS通信路の暗号化
  - dane　　DNS(SEC)にTLSの証明書を載せる
  - dnssd　　DNS-SD (RFC 6763)の拡張
- DNSの話題があったWG
  - homenet　　家のネットワーク
  - v6ops　　IPv6 operations
- IETF以外
  - IEPG

dnsop WG (1)

- DNS Operations, DNS運用ガイドラインを作るWG

- 振り返り: 2014年7月のIETF 90
  - DS自動更新と親側のNS/glue自動更新
  - AS112の変更
  - Root Zone Scaling (ルートゾーンの規模増大への対応)
  - DNSSEC Validator requirements
  - IPv6の逆引き再び
- 振り返り: 2014年11月のIETF 91
  - DNS Cookies復活
  - TCPトランスポートについての提案と熱い議論
  - ISPでのIPv6の逆引きドキュメント → 否定的ではない
  - Negative Trust Anchor: DNSSEC検証オフ設定 → 肯定的
  - IETF 91前後、複数のdraftをWG draft化: Root Scaling含む

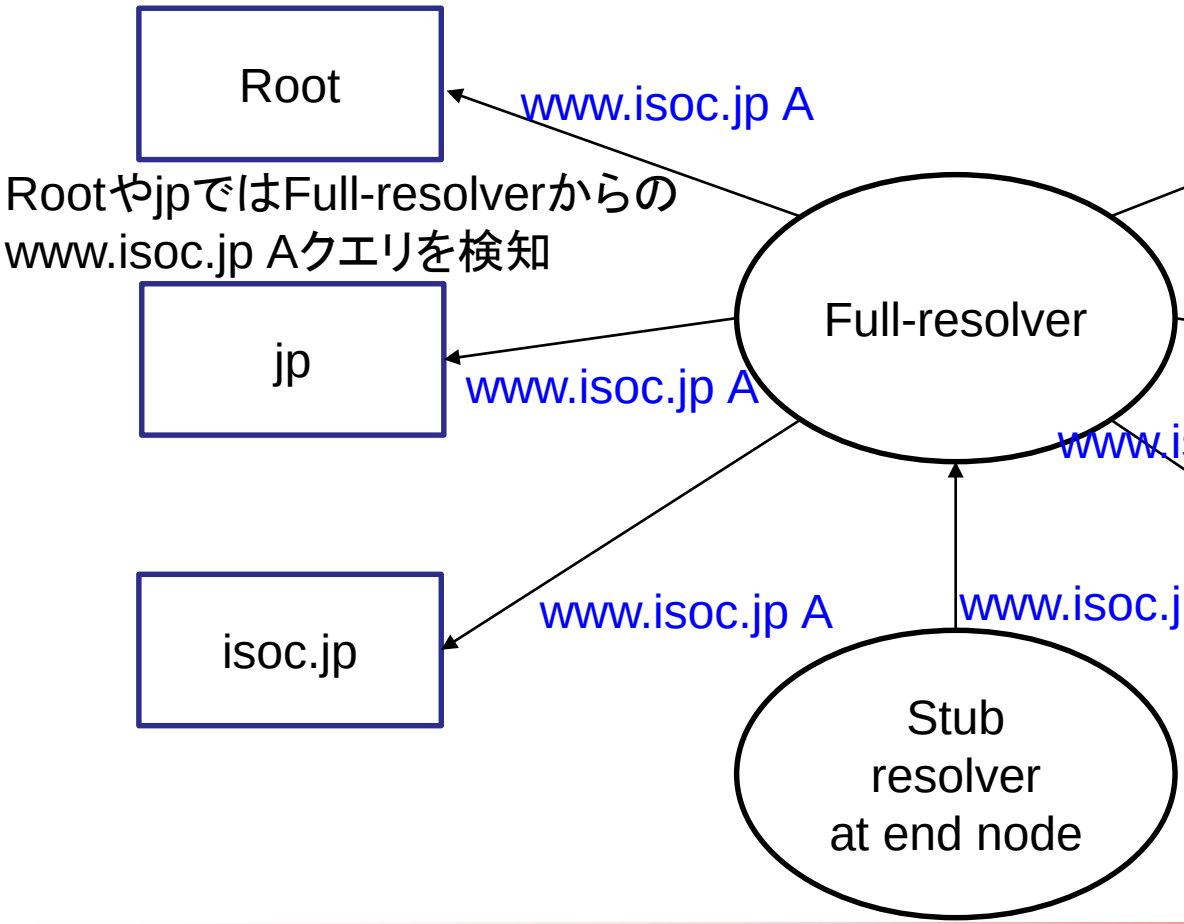
dnsop WG (2)

- draft-ietf-dnsop-qname-minimisation-02, Exp
  - プライバシ向上のため、クエリ情報の漏洩を最小化
  - 現在のフルリゾルバはユーザからのクエリ名、タイプをそのままルートを含む権威DNSサーバに送る
    - ルートやTLDでユーザからのクエリ名、クエリタイプが見える
    - キャッシュ効果により、一部しか見えない
  - そこで、例えばwww.isoc.jp Aを知りたいときに
    - ルートには、TLDのNSクエリ (jp NS)
    - TLDには、登録ドメイン名のNSクエリ (isoc.jp NS)

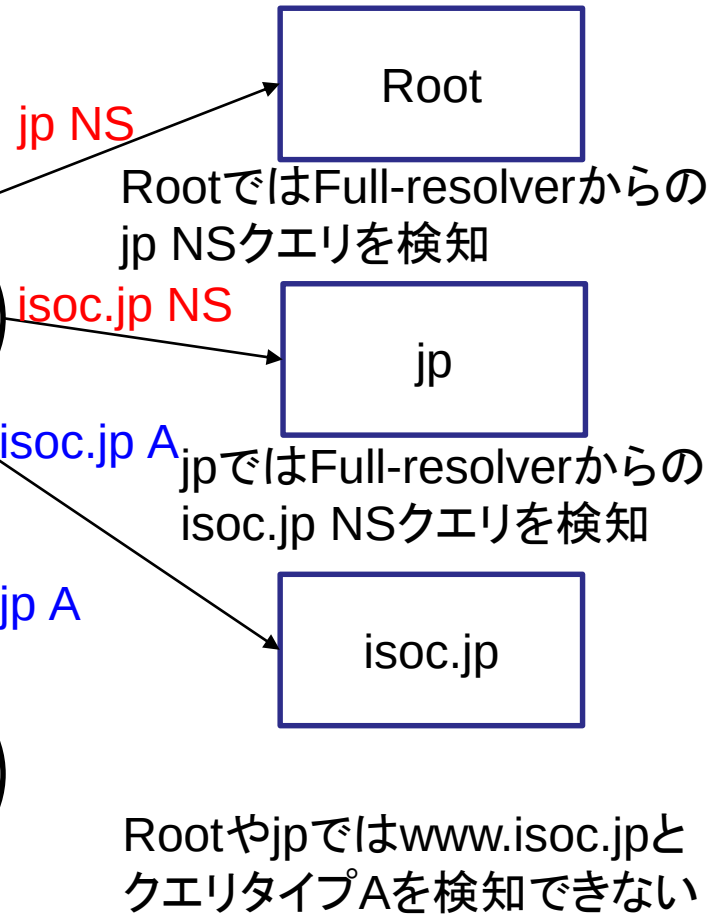
    を送ると、ルート・TLDでユーザクエリの内容が見えない
  - プロトコル違反ではないことの確認と好意的な確認や議論が行なわれ、議論を継続することとなった
  - 実装して使うことは問題ないので実装しましょう

Qname minimisation の例

従来の動作
同じqname qtype



提案手法
最小限の情報



dnsop WG (3)

- draft-ietf-dnsop-root-loopback-01
  - Rootサーバ規模増大対策: localにroot zoneコピー
  - Best Current PracticeかInformationalかという議論の結果、Informationalに (推奨はしない)
  - PowerDNS Recursorの設定方法待ち
- draft-hoffman-dns-terminology-02
  - DNSの用語集
  - Best Current Practice
  - 既存RFCの用語の抽出(矛盾もあり)と、WG mailing listで合意されたものを収録
  - WG draftとし、標準化をすすめることが合意された
  - 4/14にdraft-ietf-dnsop-dns-terminology-00 が投稿

dnsop WG (4)

- draft-ogud-dnsop-acl-metaqueries-00
  - metaqueriesの拒否についての議論(AXFR,ANYなど)
  - もともとはANYに応答したくないということから
    - mail listでDJBがqmailでANYを使った理由をコメント (古い実装のバグの回避など)
  - 無応答, TC=1, REFUSED, NOTIMP, empty(NOERROR), RTYPE=NULL, その他のタイプなどが提案された
  - どの案もDNSSECや既存実装で問題があり、継続
- draft-mekking-mixfr-01: 差分転送の改善提案
  - IXFRの改善提案と複数ゾーンの同時転送の提案
  - IXFRはRRごとに削除・追加だが、RRSetごとに入れ替えや全削除などの操作を提案
  - DNSプロトコルの変更はdnsop WGのチャーター内だが、変更点が大きいので、dpriveのように別のWGを設立することも含めて検討することが提案された

dnsop WG (5)

- TLDの予約関連
  - .onion: draft-appelbaum-dnsop-onion-tld
    - Torでは[証明書のハッシュ].onionを識別子としている
    - 3万程度の.onion識別子が存在
    - 2015年10月までに.onionが予約されないと存在しないTLDの証明書として扱われ、既存の.onion証明書は無効化
    - 2015年10月までに.onionがほしい
  - .alt: draft-wkumari-dnsop-alt-tld
    - TLDの予約の替わりに.alt以下のドメイン名を使用する提案
  - 結論は出ず、5月にInterim meeting予定(電話会議)
  - 予約だけではルートサーバにクエリが漏れるので、AS112と同様に委任するとよいといったコメントあり

dnsop WG (6)

- draft-fujiwara-dnsop-nsec-aggressiveuse-00
  - NSEC RRを用いてランダムサブドメイン名攻撃(いわゆる水責め攻撃)に対抗するという提案
    - com IN NSEC communityは、comからcommunityの間にラベルがないことを証明するため、キャッシュ内のNSECを積極的に使用する提案
    - ランダムサブドメイン名攻撃では、(random).example.comというクエリ名のため、NSECでランダムラベルの不存在を示すことができる
  - 加藤朗さんと藤原による提案で、RFC 4035をほんの少し改造
  - 気がついている人はいて、実装している人もいる
  - 提案に対して、有用だと思う人はいるようで継続

dprive WG (1)

- DNS PRIVate Exchange (dprive) WG
- スタブリゾルバとフルリゾルバの間の通信をTLSで暗号化するプロトコルを策定するWG

- 振り返り: 2014年11月のIETF 91
  - 2014年10月17日に設立
  - 最初の頭だし
  - 複数の提案
    - ポート53+STARTTLSのようなコマンド
    - ポート443
    - 443、53以外
    - DNS (JSON, binary, base64) over HTTPS
  - 懸念事項:Middle box(CPEやFirewall)を通るか

dprive WG (2)

- 複数の提案がある状況は同じ
  - draft-hallambaker-privatedns-01
    - DNS (JSON) over HTTPS
  - draft-hzhwm-dprive-start-tls-for-dns
    - 二つの提案(別ポート案とSTARTTLS案)をマージ
    - DNS protocol (TCP)をTLSで暗号化
    - まず、新ポート番号でTLSを試し、
    - 次にTCPポート53に、TLS OK (TO) bit1, RD=0, “STARTTLS” CH TXTクエリを送り、TLSモードに変更
  - draft-wijngaards-dnsop-confidentialdns
    - 独自の暗号化、ENCRYPT RR

dprive WG (3)

- 三提案のうちどれがいいかという議論
  - Milestone: Mar 2015　　WG selects one or more primary protocol directions
- draft-hzhwm-dprive-start-tls-for-dns (DNS over TLS)方式が好まれる
  - DNSプロトコル(TCP)をそのまま使用
  - TLSをそのまま使用
- 基本的には議論を継続する
  - ただし締切あり: Jul 2015 WG LC on primary protocol directions

dane WG (1)

- DNSにTLSの証明書を載せるWG

- 振り返り: 2014年3月のIETF 89
  - 今後: プロトコルが完成したらWGを閉じるか？
- 振り返り: 2014年7月のIETF 90
  - DANE SMTP, DANE SRV: 議論完了
  - DANE OpenPGP, S/MIME:まとまらず、継続
  - Raw key format: 継続
  - draft-ietf-dane-ops: BCP → Standards
  - 今後: DANEbisとops、残務を行う
- 振り返り: 2014年11月のIETF 91
  - DANE SMTP, DANE SRV: WGLC完了
  - DANE SMIMEA: 実装案の議論とOpenPGPとのマージ提案
  - DANEの普及に関する議論

dane WG (2)

- OpenPGPKEY: WGLC完了
- Milestoneに対し、半年から一年遅れで延長
- Verisign, Inc.でS/MIMEへの実装を行なっている
  - https://github.com/verisign/smaug
  - https://github.com/verisign/smaug-tbird-plugin (Mozilla Thunderbirdのプラグイン)
- Draft-wiley-paymentassoc-00,
  - Glen Wiley, Verisign
  - 課金情報を扱う提案
  - W3C Web Payments group で活発
  - 興味を持つ人が多い

dane WG (3)

- メールアドレスの扱いについての議論
  - メールアドレスは大文字小文字を区別するが、しない実装も多い
  - DANEラベルを計算するときの大文字小文字の議論
  - 実験的にOPENPGPKEYの標準化を進めることとなった
  - draft-ietf-dane-openpgpkey-03 では、メールアドレスのユーザ部を小文字にしてからハッシュを計算することになった
    - username@domainname のOpenPGPKEYを、
    - L=hex(先頭28octet(sha256(小文字(username))))
    - $L._openpgpkey.domainname IN OPENPGPKEY <base64 publickey>

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

- 振り返り: 7月のIETF 90
  - Requirements: 完了
  - プロトコルの実装はハイブリッドプロキシー
  - 脅威モデル: 最初の話題提供
- 振り返り: 11月のIETF 91
  - Long Lived Queries復活: pollingによらずに、クライアントに登録情報の変更を通知する仕組み？
  - 脅威モデル: 継続
  - 実装案: ハイブリッドプロキシー

dnssd (2)

- Requirements: 現在RFC Editor queue
- DNS Push: draft-ietf-dnssd-push-00
  - LLQ is dead:LLQを理解しなくてよくなった
  - DNS Updateを用いる方式に変更
- 実装案 draft-ietf-dnssd-hybrid-00
  - 進展が見られない
  - 実装についての要求仕様とユースケースの議論
  - 通常のDNSとの関連が決まっていない
- 脅威モデル
  - 追記されたが、Hybrid proxyの話があっていない？
- 感想:まだ時間がかかりそうである

homenet

- 家のネットワーク
- draft-mglt-homenet-front-end-naming-delegation
  - 家の情報をDNSに出す仕組みで、家でhidden masterを動かし、ISPにゾーン転送してDNSSEC署名してISPのDNSサーバで公開
  - NOTIFYやゾーン転送の詳細が追記された
- draft-mglt-homenet-naming-architecture-dhc-options-03
  - DHCPにhybrid proxyなどの情報を伝えるオプションを追加する提案
    - OPTION_PUBLIC_KEY, OPTION_DNS_ZONE_TEMPLATE, OPTION_NAME_SERVER_SET, OPTION_REVERSE_NAME_SERVER_SET
- 複雑

v6ops

- IPv6 Operations

- IPv6 Loopback Prefix
  - There is no place like ::1
  - ::1以外のloopbackアドレスがほしいという提案
  - Use casesの質問で、loopback addressに複数のDNSサーバを動かしたいからという回答
  - いまでも、::2/128, ::3/128などをloopback interfaceに設定すると使用可能であるが、公式に使用したいという意図があったようである

IEPG

- DNS関連が4件中2件
- Use of ECDSA, Geoff Huston @ APNIC
  - RSAよりECDSAのほうがRRSIGが小さくなるため、ECDSAを普及させたい
  - ECDSAでのDNSSEC検証対応状況
    - Google Adsを使い、エンドユーザにRSAとECDSAで署名されたドメイン名を検証させた
    - RSAは約25%が対応、ECDSAは約20%
    - ECDSAが普及しない原因の推定(OpenSSLの対応が遅かった)
- EDNS Compliance, Francis Dupont @ ISC
  - BIND 9.10で実装したSIT (DNS Cookie) を試したところ、EDNS0に関する通信エラーが発生
  - EDNS0の実装エラーが原因で、分類して報告
  - IETF dnsop WGでもMark Andrewsが同じ報告をした

参考

- http://www.ietf.org/
  - 過去のIETFミーティングの資料、議事録あり
- http://www.iepg.org/
  - IEPGミーティングの資料
- .onion
  - ICANN Name Collision関連
  - CA/Browser Forum