IETF 87 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 87 報告会, 2013年9月5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
  - dane DNSを利用した証明書の配送・正当性検証
  - dnssdext Bonjourの拡張 (WG前)

Bonjourは、米国およびその他の国で登録されたApple Inc.の商標です。

- DNSの話題があったWG
  - 6man IPv6 Maintenance
  - homenet Home Network
  - apparea Application Area Open Meeting
  - saag Security Area Open Meeting

*はIETF 87では会議なし

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

dnsext WG (DNS Extensions)

- DNSプロトコルを拡張するWG
  - dnsind WGとdnssec WGの活動を引き継ぎ、1999年12月に開始
  - 2008年まで主にDNSSECプロトコルを開発
  - 2010年にRootと複数のTLDがDNSSECの運用を開始し、活動がほぼ完了
- 残務を完了し、2013年7月24日に完了
  - ただし、メーリングリストは継続して使用可能
  - dnsext@ietf.org
  - SPFリソースレコードの問題についての活発な議論が行われた (2013/8/20~28)
  - 新しいWGを作るかどうかという話も出ている

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
  - 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

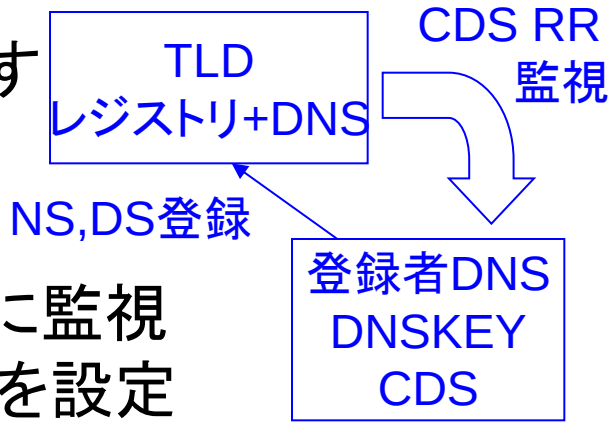
- 90分の時間枠に以下のAgendaがあり、WG Updatesだけで時間が終わった
- WG Updates (最近の話題)
  - AS112 Discussion - Omniscient and DNAME (20 min)
  - DNSSEC Child Delegation (20 min)
  - DNS Cache Mechanism (15 min)
- 過去のドキュメントのアップデート
- New Business (新しい話題)
  - DNS Server Diagnostics
- Any Other Business (時間があれば)
  - draft-deng-pcp-ddns
  - DNSSEC Roadblock Avoidance
  - Root Zone KSK Roll
  - (draft-fujiwara-dnsop-ds-query-increased)

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を用いてIP Anycastのテストベッドとして利用
- 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変化に追従するのは困難
- 提案が二つ
  - 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
- 結論: 両方を検討する (DNAME → Omniscient)

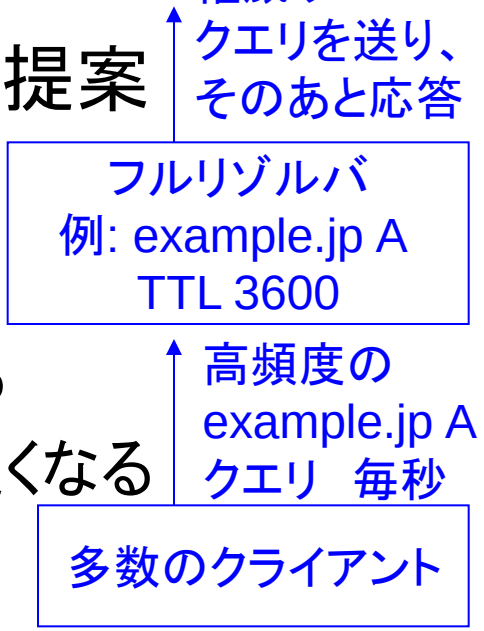
dnsop: Child Delegation

- DNSSECで、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レジストリが運用することが想定
- 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を得て、レジストリDBとTLDゾーンを書き換える
- 二つの提案
  - 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
- 結論
  - 提案の一元化なども議論されたが、結論は出ず、継続
  - 参加者の関心は高い



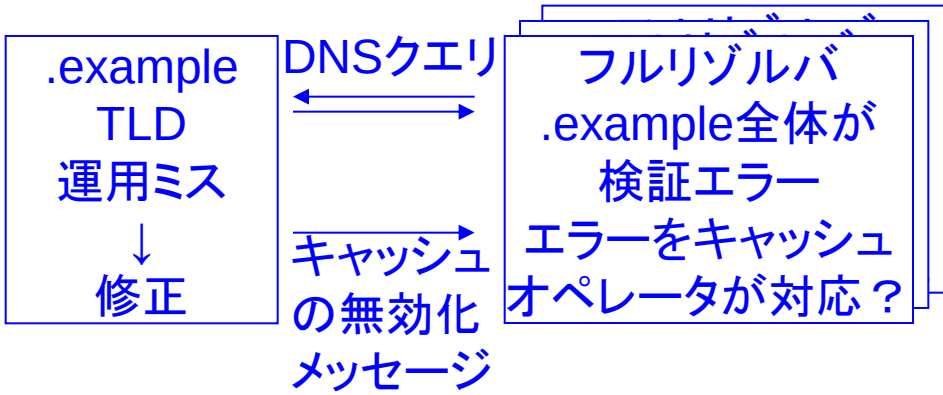
dnsop: キャッシュ方法の改善

- フルリゾルバでのキャッシュ方法の改善提案
- 問題の指摘
  - キャッシュにあれば低遅延で応答できる
  - TTL時間後の最初のクエリは時間がかかる
  - 忙しい名前はTTLごとに定期的に応答が遅くなる
- 提案
  - クライアントからのクエリがあったときに、キャッシュ内のTTLの残り時間が2以下であれば、応答と再クエリを行う
- 結論
  - 権威DNSサーバへの負荷の増大が懸念されたが、計測結果を元に評価して判断することとなった



dnsop: キャッシュの無効化提案

- 問題の指摘
  - DNSSECの運用ミスによるTLD全体や有名サイトが見えなくなる事故の際に、フルリゾルバのキャッシュの一部の無効化を自動化したい
- 提案
  - フルリゾルバにDNS NOTIFYを送ることで、そのゾーンに関するキャッシュを無効化 (DNS FLUSH)
  - 権威DNSサーバから送る
  - TSIGで守る



- 結論
  - 問題は重要な課題であるのでWGで議論を継続する
  - 提案手法はよくないという意見が主流

dane WG (1)

(DNS-based Authentication of Named Entities)

- ドメイン名と公開鍵証明書を対応づけるプロトコル
  - DNSSECを前提に、サーバ証明書をDNSにのせる
  - 2010年12月に開始(Root,TLDのDNSSEC対応後)
- 現在までの成果
  - RFC 6394: Use Cases and Requirements
  - RFC 6698: The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA
- 標準化されたプロトコルをDANE TLSAと呼ぶ
- 使うためには
  - サーバ側: 自己署名証明書の内容をTLSA RRに書く
  - クライアント側: ブラウザやアプリケーションを拡張する

dane WG (2)

- IETF 85,86ではミーティング非開催
- IETF 87ではミーティング開催
- Agenda
  - DANE TLSA実装と運用ガイド
  - DANE TLSAによるSMTP Security
  - DANEとDNSでの用語について
  - www.ietf.orgへのTLSA RRの追加提案
- 結論
  - DNSの専門家二人による、DANE TLSAの使い方の解説
  - www.ietf.org, @ietf.org への導入提案には賛否あったが、そのうち実現されると思われる

dnssdext BoF (1)

- 概要
  - Apple Inc.のBonjour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の後継
  - 名前を変えて再挑戦を図ったもの
- Bonjour
  - Apple Inc.が開発したプロトコルで、OS Xで実装
  - 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
  - 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)

dnssdext BoF (2)

- 経緯
  - IETF 85 mdnsext BoFのあと目立った動きがなかった
  - その後の議論は主にhomenet WGで行われた。
  - homenet WGでは、multicast DNSで家庭内の名前解決をすることを考えている
- 議論と結果
  - プリンタの共有や、公開プリンタへのアクセスが例としてとりあげられた
  - 必要だと思っている人は多い
  - ドキュメントを書いたり、レビューするという人が多かった
- IETF 87後の状況
  - WG Charter案が議論されている
  - 近いうちにWG設立が見込まれる

homenet WG

- 家庭内ネットワークをIPv6で作るWG
  - IETF Chair Jari Arkkoさんの自宅の問題を解決
  - http://www.arkko.com/publications/miracle2011_homenet_arkko.pdf 14ページ
- 家庭内ネットワークでの名前解決
  - 家の中の名前解決はmulticast DNSの拡張
  - 外へのアクセスは通常のDNS
  - 名前ごとに解決手段を変えるHybrid DNS Proxyを作成することが提案された
    - .homeならmulticast DNS, それ以外は普通のDNS
  - 例示されたTLD (.home) への懸念が示された
  - OpenWRTやLinuxでの実装について報告された

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
- 提案: IPv6フラグメントヘッダの廃止
  - IPv6では、フラグメントをしない
  - 影響があるプロトコルとしてDNSSECとSIITが提示
- 議論と結論
  - DNSSECは依存していないというコメントあり (TCP)
  - DeprecateよりもSHOULD NOT useがよい
  - 肯定的に継続して議論するという雰囲気
- DNSへの影響
  - 従来UDPメッセージサイズの上限値として、1220を必須、4000を推奨としていたが、1220を推奨することになる
  - TCPのクエリが増加する可能性 (サーバ増強など)

apparea (Application Area Open Meeting)

- アプリケーションの立場でDNSの拡張
- DNS extension language
  - DNSサーバソフトウェアの変更をしないで新しいRRタイプを追加する言語の提案で、DNSサーバの設定ファイルか、DNSにタイプの設定を書くことが想定されている
- ドメイン名の管理境界についての議論
  - たとえばCookieの有効範囲など (Public Suffix List)

- IETF 87後に、チェアからappareaでDNSに関する話題を扱うべきかという問い合わせがあり、数人が賛意を示していた (反対はなし)

saag (Security Area Open Meeting)

- DNSへの攻撃と対策についての話題が出た
- DNS Cache-Poisoning:
  New Vulnerabilities and Implications
  という発表があった
  - IP fragmentの後半を予測して攻撃するとのこと
  - 9月4日になってdns-operations mailing listで対策の話が盛り上がっている
  - udp-size 1220上限案や、フラグメントを使わない(DFビットをセット) など

まとめ

- IETF 85報告では、DNS関連の活動は低調と書いたが、IETF 87では非常に活発であった

- DNS以外のWGで、DNSの動作に影響を与えるプロトコル拡張が提案されることがあるので、多くのWGを確認しておく必要がある
  - 6man, homenet, appareaなど