IETF 91 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 91 報告会, 2014年12月19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年~2011年):ENUMプロトコル
  - RFC 5504 5825 6856 6857 (2005年~2013年)
    - 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~)
    - JPでのDSクエリ増大問題
  - draft-fujiwara-dnsop-poisoning-measures (2014/7)
    - キャッシュポイズニング対策
  - draft-hoffman-dns-terminology (2014/11~)
    - DNSでの用語解説

DNSを扱ったWG/BOF

- DNS関連WG/BOF
  - dprive　　DNS通信路の暗号化
  - 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
  - dbound　　ドメイン境界 (非公式)
- DNSの話題があったWG
  - homenet　　家のネットワーク
- IETF以外
  - IEPG
- その他
  - Workshop on DNS Future Root Service Architecture

dprive WG (1)

- DNS PRIVate Exchange (dprive) WG設立
  - 2014年10月17日に設立認可
  - Chairs
    - Tim Wicinski (dnsop chair)
    - Warren Kumari (dane, IEPG chair)
  - スタブリゾルバとフルリゾルバの間の通信をTLS(Transport Layer Security)で暗号化する
  - 前提として、フルリゾルバを信用
  - フルリゾルバと権威DNSサーバの間のプロトコルの変更はしない

dprive WG (2)

- 複数の提案
  - DNS/TCPをそのままTLS (16ビットのデータ長 + binaryのDNSデータ)
    - ポート53+STARTTLS (SMTP/POP3のようにコマンドで格上げ)
    - ポート443
    - 443、53以外
  - DNS (JSON format) over HTTPS
  - DNS (BinaryをASCII encode) over HTTPS
- 懸念事項:Middle box (CPEやFirewall)
  - Port 443でhttpsなら通るという主張
  - Firewallが知らないプロトコルは止められる可能性あり

dnsop WG (1)

- DNS Operations, DNS運用ガイドラインを作るWG
- ふりかえり: 3月のIETF 89
  - 継続ものと、チャーター更新
  - 最新の更新案でDNSプロトコルの拡張が追加された
  - DNSE BoF、DNSプライバシについて取り扱う → dprive WG
- ふりかえり: 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
  - 鍵と署名ポリシー
  - IPv6の逆引き再び → 継続
  - マルチキャストアドレスの逆引きをどうするか

dnsop WG (2)

- DNS Cookies復活
  - Cache poisoning対策の一つ
  - draft-eastlake-dnsext-cookies-05
  - 2008年にexpireしていたものを復活、WG docへ
  - BIND 9.10のSIT(Source Identity Token)と連携
    - ただし、フォーマットは違う (SITにはerror codeがない)
- TCPトランスポートについての提案と熱い議論
  - Server side close
  - TCP fast open
  - Query pipelining
- 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

dnsop WG (3)

- IETF 91前後、複数のdraftをWG draft化
  - 10/27 draft-ietf-dnsop-qname-minimisation-00
    - 権威DNSサーバに送るクエリ名を短くしてプライバシ強化
  - 11/16 draft-ietf-dnsop-edns-client-subnet
    - Public DNSを使ってもDNSを使用したロードバランスが動く仕組み
  - 11/30 draft-ietf-dnsop-cookies-00
    - DNS Cookies (攻撃耐性の強化)
  - 11/30 draft-ietf-dnsop-root-loopback
    - ループバックインターフェースでrootサーバのコピーを動かす
    - ルートの規模拡大の話の続き
  - 12/04 draft-ietf-dnsop-5966bis-00
    - DNS Transport over TCP - Implementation Requirements
  - 12/15 draft-ietf-dnsop-negative-trust-anchors-00
    - Definition and Use of DNSSEC Negative Trust Anchors

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

- ふりかえり: 3月のIETF 89
  - Requirements: ほぼ合意
  - 最初の候補:DNSとmDNSの複合プロキシー
    - 検索時は、DNSとmDNSの双方を検索
    - mDNSで登録された名前をDNSにどう展開するか
- ふりかえり: 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

dnssd (2)

- draft-sekar-dns-llq-01: DNS Long-Lived Queries
  - 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？
  - ドキュメントのアップデートを含めて継続
  - ただし、プロトコル提案にはマージされている
- 脅威モデル: draft-rafiee-dnssd-mdns-threatmodel-01
  - mDNSの話は入ったが、実装案のハイブリッドプロキシーの話は入っていない　→　継続
- 実装案 = ハイブリッドプロキシー
  - 既存のDNSとmDNSをプロキシーする
  - draft-ietf-dnssd-hybrid-00として、WG draftになった
  - 細かいところのアップデートと、LLQ追加
  - DoS対策としてrate limitを追加
  - 継続し、メーリングリストでコンセンサスを得る予定

.home TLD

- 新gTLDプログラムで10組織が提案するも、Name Collisionより”high risk”と評価され無期限保留中
- IETF 91 にて、Stuart Cheshire氏がhomenet向けに使いたいと提案
  - Stuart Cheshire氏はRFC 6762で.localを予約した人
  - homenet WGではdnssd WGの仕事と指摘
  - dnssd WGでは質問程度
  - Mailing listでは、arpaの下ならIETFから提案しやすいといったコメント
  - ICANNの領域にはかかわりたくないという雰囲気
- TLDの予約の話は、IETFでは嫌われる
  - TLDはICANNの仕事で、IETFの仕事ではないという認識
  - TLDはICANN(周辺の人)の商品であるという意識

dane WG (1)

- DNSにTLSの証明書を載せるWG

- ふりかえり: 3月のIETF 89
  - WGの今後: プロトコルが完成したら閉じるか？
  - SMTP, SIP, XMPPへ適用した場合の深い話が議論
  - OpenPGPへの適用について
- ふりかえり: 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

dane WG (2)

- DANE SMTP, DANE SRV
  - WGLC: 11/12-12/4　いくつかコメントあり、完了
- DANE SMIMEA
  - localpart@domainnameのユーザのS/MIME公開鍵を以下のドメイン名のSMIMEA RRに置く
  - sha224(localpart)._smimecert.domainname IN SMIMEA 0 0 1 d2abde240d7cd3ee6b4b28c54df034b9 7983a1d16e8a410e4561cb106618e971)
  - SMIMEA RRのワイヤフォーマットはTLSAと同じ
  - OpenPGPとのマージが必要であるという結論
  - VerisignLabsの人が実装
    - Thunderbird + getdns api

dane WG (3)

- DANEの普及に関する議論
  - ISOCのDan York氏
  - http://www.tlsa.info/
    - 330+ SMTPサーバ, 229 JabberサーバがTLSA
  - IETF内で普及推進活動をするか外でやるか？
  - 各国での取り組みとか、本を書くとか、いろいろなアイデアが議論されるが、、、
  - 結論でず、各ドキュメントの議論に
- 2014/12/2にInterim meeting
  - 14名,1時間, WebEx+Jabber
  - SMIMEAの使い方について、ユーザの公開鍵の入手法が議論された
  - 結論: 追加のユースケースをmailing listに送ること
  - 署名と暗号化を分ける提案
    - *._sign._smimecert.domain と *._encr._smimecert.domain

dbound BoF

- Domain Boundaries BoF / ドメイン境界
- Public Suffix Listの後継を考えるグループ
- 今回は非公式なside meetingとして開催
- 複数の境界
  - Private.Public … public suffix listが考えるもの
  - Private.Private … 組織内の境界 (大学の学部とか)
  - Public.Private … co.ukとukの境界？ ukはprivate
  - Public.Public … jp.comとcomの境界？
- ユースケース:cookie, DMARC, SSL証明書
- 結論
  - 興味を持つ人が多いのでWGを設立する
  - ミーティング後、Charterの議論が続く

IEPG

- 今回はIPv6やルーティングの話題中心
  - IPv6 Extension Headers in the Real World v3.0
  - prefix+AS-Origin
  - The 512K route thing
  - Experience with IPv6 path probing - draft-naderi-ipv6-probing-00
  - Update on Operators Survey
- DNS関連
  - Fully synthesised DNSSEC signed zones
    - APNICが自ゾーンのDNSSECで問題をかかえており、Google Adsでzoneをわけないといけないとのこと
    - 75万ゾーンあって、reloadに時間がかかる
    - 専用のDNSサーバを試作したらしい？
    - https://github.com/raybellis/apnic

その他

Workshop on DNS Future Root Service Architecture

Location: Hong Kong, HK

Venue: The Mira Hotel (Kowloon district)

Date: December 8-9, 2014

Hosted by: ISOC-HK

Sponsors: ZDNS/BII and CNNIC

Co-chairs: Warren Kumari and Paul Vixie

- 録画
  - https://www.youtube.com/watch?v=cMKvI-Hk7Uw
  - https://www.youtube.com/watch?v=Nr9StRxasHc
- 提案ドキュメント
  1. draft-wkumari-dnsop-root-loopback-01
  2. draft-lee-dnsop-scalingroot-00

会議の結果

- 現地参加者は約30人
- ビデオは公開されているが資料は公開されていない
  - ビデオに写っている範囲で公開
- 参加していたIETF dnsop WG chairは、この会議はIETFに提案されたInternet draftを参照しているが、dnsop WGとは関係ないと強く指摘
- 中継動画によると、
  - 技術的な内容に限定
  - 政治色は薄い (中継のため、言えないことは言わなかったような雰囲気)
  - 今後議論を続け、IETF dnsop WGに提案する
  - CNNICによるクルージングに感謝の言葉など

draft-lee-dnsop-scalingroot

- How to scale the DNS root system?
- 著者
  - Xiaodong Lee (CNNIC CEO兼CTO)
  - Paul Vixie (Farsight Security)
  - Zhiwei Yan (CNNIC)
- ルートゾーンはICANN/IANA管理
- ルートサーバの名前・アドレスをAnycastアドレスの組に改組して、階層的に配置するという提案
  - 国ごととか、地域ごとなど
  - いまのroot serversをつぶして作り直そうという提案
  - 完全に再割り当てと、一部のルートを変更するという2案
- よく考えられてはいるが、、、不評 (2014/7 IETF 90にて)
  - 政治的意図を感じた人が多かった？

draft-wkumari-dnsop-root-loopback

- Decreasing Access Time to Root Servers by Running One on Loopback
- 著者
  - Warren Kumari, Ed.
  - Paul Hoffman
- ローカルにルートのデータを持つ権威DNSサーバを動かし、フルリゾルバからルート向けはそこに向けるという提案、設定例あり
- 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り、応答速度が向上する
- 2014/11/30にIETF dnsop WGのWG draftに
  - draft-ietf-dnsop-root-loopback
  - Paul Vixie提案にWGとして対抗？

ルートサーバを変更するWorkaround

- Paul Vixie氏による解説
- Alternate rootの作り方
  1. IANA/ICANNからRoot zoneをとってくる
  2. 委任情報の取り出し (NS, DS, glue)
     - . NS, . SOA, . DNSKEY, NSEC, RRSIG, ルートサーバ情報 ([a-m].root-servers.net)を削除
  3. (検閲/編集)
  4. 自分の. SOA, . NS, . DNSKEY, Rootサーバリストを追加、自分の秘密鍵で署名
  5. Internallyに配布 (root hint, trust anchor)

  – 明らかだけど、これまでだれも書かなかった
- 13ルートサーバのアドレスの経路をハイジャック
- 企業や閉域網で使用例あり (国単位も考えらえる)

Zone signature

- Paul Hoffmanによる新提案
- ゾーン転送の正しさを証明するSignatureをゾーン内に追加するもの
- 動的に変化する巨大ゾーンでは困難そう

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

- Workshop on DNS Future Root Service Architecture
  - https://www.youtube.com/watch?v=cMKvI-Hk7Uw
  - https://www.youtube.com/watch?v=Nr9StRxasHc