IETF 93 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 93 報告会, 2015年8月27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/ドメイン名を扱った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
  - dbound　　Public Suffix List の後継
- IETF以外
  - IEPG

- 個人的興味 (範囲外)

dnsop WG (1)

- DNS Operations, DNS運用ガイドラインを作るWG

- 振り返り: 2014年11月のIETF 91
  - DNS Cookies復活, TCPトランスポート, ISPでのIPv6の逆引き, Negative Trust Anchor
  - IETF 91前後、複数のdraftをWG draft化
- 振り返り: 2015年3月のIETF 92
  - qname-minimisation, root-loopback, dns-terminology, acl-metaqueries, 差分転送の改善, TLDの予約(.onion), nsec-aggressiveuse
- IETF 93の概要
  - IETF 93前に複数の案件をIESGに提出、WGLC実施
    - 上記下線項目
  - そのため、新しめの提案を先に扱い、その後でもめている案件(TLD予約)を扱った

dnsop WG (2)

- draft-ietf-dnsop-dnssec-key-timing
  - DNSSECでのキーロールオーバータイミングなどについての問題点を示したもので、Informational
  - 発行直前のAUTH48で半年放置されている
- draft-ietf-dnsop-negative-trust-anchors
  - DNSSEC検証を無効にするドメイン名の設定
  - BIND 9, Unbound, Nominum Vantioの設定例
    - BIND 9: 公開gitのmasterには実装済 (9.11 ?)
    - Unbound 1.5.4には実装済
  - RFC Ed Queue: 近いうちに発行の見込み

dnsop WG (3)

- draft-ietf-dnsop-root-loopback
  - loopbackにルートゾーンのコピーを置く提案でInformational
  - 2015/6/28 IESG提出/AD Evaluation
    → 7/28~8/11 IETF Last call
- draft-ietf-dnsop-dns-terminology
  - DNS関連の用語集
  - 2015/6/28 IESG提出/AD Evaluation
    → 7/28~8/11 IETF Last call, 現在アップデート中
    John Klensinから大規模で有用な提案あり
- draft-ietf-dnsop-onion-tld
  - .onion TLDを予約する提案でProposed Standard
  - .altなどの各種提案があったが、証明書/CABF的な期限のため急ぎ進めた
  - 7/14~8/11 IETF Last call

dnsop WG (4)

- draft-ietf-dnsop-cookies
  - 7/2~7/16にWGLCだったが、Reviewerが少なくIETF 93時にReview要請があった
- draft-ietf-dnsop-qname-minimisation
  - プライバシー向上のため、クエリ情報の漏洩を最小化
  - IETF 93前にWGLC完了
  - IESGへの提出直前

- ここまでがステータス報告　(実際には10分)

dnsop WG (5)

- TCPトランスポートに関する提案
  - DNS Transport over TCP - Implementation Requirements, draft-ietf-dnsop-5966bis-02
    - DNS over TCPの仕様と、性能条件を規定する提案(明確化)
    - RFC 1123ではUDP firstだが、UDPまたはTCPと再定義
      → dprive WGと関連あり
    - TCP接続の再使用、タイムアウト、複数のクエリの同時送信やTCP Fast Openなどを明確化
    - 議論:長期生存するTCP接続の懸念　(BGPとの類似性)
  - edns-tcp-keepalive EDNS0 Option
    - draft-ietf-dnsop-edns-tcp-keepalive
    - TCP接続のタイムアウトを指定するEDNS0オプション
      - 指定時間、クエリがなければTCPを閉じてよい (100ms単位)
    - TCPを張りっぱなしで複数のクエリを処理させることを想定
  - 基本的には議論を継続して進める

dnsop WG (6)

- draft-fujiwara-dnsop-nsec-aggressiveuse-01
  - 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 commbankは、comからcommbank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は (random).example.comというクエリ名のため、NSECでクエリ名の不存在を示すことができる
  - 加藤朗さんと藤原の共著
  - 甘いところが多く、まだ問題点はあるが、継続
    - CD (Checking Disabled) bit が 1だとDNSSEC検証を無効にするため、(キャッシュ済の)NSEC RRを使用できないという問題
    - RFC 2308 (NCACHE) に、完全一致だけを使用すると書かれているという問題
    - DNS/DNSSECの本質にかかわるところなので、注意がいる

dnsop WG (7)

- トラストアンカー管理の提案
  - DNSSEC Trust Anchor Publication
    - draft-jabley-dnssec-trust-anchor-11 (00は2010年)
    - 2010年にルートのトラストアンカーを配布した方法をまとめたもので、IANAからファイルを取得し、検証し、トラストアンカーとして使用する手順を示している
    - RFC 5011(トラストアンカー自動更新)について議論されたが、進展なし？
  - Simplified Updates of DNS Security Trust Anchors
    - draft-wkumari-dnsop-trust-management
    - トラストアンカー自動更新の新手法の提案 (TDS RR)
    - RFC 5011やTALINKと同じではないかと指摘された

dnsop WG (8)

- On No, Not More NameSpace Discussions
  - .onion以外のTLD予約に関するセッション
  - P2Pなどで使用されるTLDの予約提案
    - bit (NameCoin), i2p (local database only)
    - gnu (GNU Name system), zkey (GNS zone key)
    - exit (Tor exit node), tor, carrot
  - Design Team設立
    - RFC 6761によるTLD予約の問題点の指摘と解決のためのDesign Team設立と、そこへの入力が紹介
    - 名前空間とDNSの違いや、ICANNとの調整、ポリシーなど問題が多い
    - 議論が紛糾するので、WGと分離
  - 決めたRFC/ルールに従うべきといったコメントなどがあったが、結論は出ていない

dbound WG

- Domain Boundaries WG / ドメイン境界
- Public Suffix List (PSL)の後継を考えるWG
  - PSLはCookieの取り扱い判定で使用されているもので、Mozilla Foundationがメインテナンスしている
  - 巨大なテキストの順序付きリストで、上から順にパターンマッチ
    - 使用例に複雑な地域型JPドメイン名
- 主な議題は Define the problem で結論出ず
- 用途案
  - Cookieの判定
  - 証明書発行の判定 (組織とドメイン名)
  - ワイルドカード証明書の発行判定
  - メールアドレスからのDMARCドメイン名抽出
    - 現在はPSLについて書かれていない
  - 二つのドメイン名が同じ管理下にあるか判定

dane WG (1)

- DNSにTLSの証明書を載せるWG

- 振り返り: IETF 90
  - SMTP, SRV 議論完了
  - DANE OpenPGP, S/MIME:まとまらず、継続
- 振り返り: IETF 91
  - 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
- 振り返り: IETF 92
  - OpenPGPKEY: WGLC完了
  - SMIMEA実装の紹介
  - 課金情報を扱う提案
  - メールアドレスの扱いについての議論
    - hex(先頭28バイト(sha256(小文字(username))))._openpgpkey.dom

dane WG (2)

- Plan
  - SMIMEA: IETF 94までにWGLC
  - そのあとWGを完了
- DNSSEC auth chain extension, draft-shore-tls-dnssec-chain-extension-01
  - TLSを拡張し、クライアントから要求があればTLSA RRと、ルートからTLSA RRの検証に必要とされるすべてのDS, DNSKEYをTLSでクライアントに送るもの
    - _443._tcp.www.example.com TLSA
    - example.com DNSKEY/RRSIG, example.com DS/RRSIG
    - com DNSKEY/RRSIG, com DS/RRSIG, . DNSKEY/RRSIG
  - DNSクエリなしでルートからTLSAを検証可能
    - IETFハッカソンで実装したとのこと
    - TLSデータが3000バイト程度増える
  - レイヤーバイオレーションの指摘や、chain queryでできることなどが指摘され、不評であった

dane WG (3)

- メールアドレスの扱いについての議論
  - OpenPGPKEYとSMIMEAでの統一が必要
  - OpenPGPKEYでは、hex(先頭28バイト(sha256(小文字(user name)))) という提案が優勢だった
  - 今回は、user nameのbase32とハッシュについて議論が行なわれた
    - DNSは大文字小文字の区別をしない、a-z0-9 36文字→base32
  - base32がよいという雰囲気(ラフコンセンサス)であった
  - 終了後、DNSのラベルには63バイトの制限があるので、63*5ビットのデータしか扱えないことをチェアに聞いてみたところ、複数のラベルを使えばよいと指摘された
    - 例えば40バイトから78バイトのuser nameの場合
    - base32(user name 残り).base32(user name 前半39バイト)._openpgpkey.domainname IN OPENPGPKEY ….
    - 筋が悪いのでまだまだ続きそう

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
  - 複数の提案: ポート53+STARTTLS, DNS over HTTPS
  - 懸念事項:Middle box(CPEやFirewall)を通るか
- 振り返り: 2015年3月のIETF 92
  - 複数の提案のうち、別ポート案とSTARTTLS案をマージしたものが好まれた

dprive WG (2)

- DNS over DTLS, draft-ietf-dprive-dnsodtls
  - DNS over TLSと同じ別ポートを使用可能
  - Downgrade attackへの懸念が示された
  - 継続
- TLS for DNS, draft-ietf-dprive-start-tls-for-dns
  - 実装あり: Unbound, ldns/drill, digit, getdns
  - 別ポート案、併用案などとの比較が必要で議論を継続

dprive (3)

- EDNS Padding Option
  - データサイズが固定されている場合、暗号文を見て原文を推定できる可能性があるため、原文にランダムサイズのpaddingを追加する提案
  - TLS 1.3ではpaddingオプションがあることや、EDNS0で規定するとDoSの原因になること、壊れたDNSサーバは誤動作する可能性があることなどが指摘された
  - 今後、EDNS0 optionとuse caseの二つのドラフトを書くとのこと
    - draft-mayrhofer-edns0-padding-01

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: 2014年11月のIETF 91
  - Long Lived Queries復活
  - 脅威モデル: 継続
  - 実装案: ハイブリッドプロキシー
- 振り返り: 2015年3月のIETF 92
  - Requirements: 現在RFC Editor queue
  - DNS Push: LLQの代わりにDNS Updateに変更
  - 実装案: ハイブリッドプロキシーだが、進展が見られない
  - 脅威モデル: ハイブリッドプロキシーの話があっていない？

dnssd (2)

- RFC 7558 Requirements for DNS-SD 発行
- 現在Milestoneに対して半年遅れ

- Interoperation of Labels Between mDNS and DNS
  - DNSとmDNSでラベルの扱いが違う問題
    - DNSはASCIIのみ (A-label), mDNSはUTF-8そのまま
    - 国際化ドメイン名を理解していない人が多く発散気味
- DNS Push Notifications
  - Reviewerが少ないので判断できない
  - 使いたいと思っている人が少ない？
- Threat model / 脅威モデル
  - まだ記述不足

dnssd (3)

- 実装報告
  - Homenet WG関連で実装
    - draft-ietf-homenet-hybrid-proxy-zeroconf-00
  - RHEL/Ubuntu/Debian/FreeBSDなどで作れる
  - Apple mDNS responderをベースに作ったとのこと
  - さっさと標準化してくれたら実装するという人は多い

homenet

- 家のネットワーク
- draft-ietf-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-ietf-homenet-naming-architecture-dhc-options-02
  - 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
- WGLC が近い

IEPG (1)

- DNS関連が5件中4件
- Deploying New DNSSEC Algorithms, Dan York @ ISOC
  - 新しいアルゴリズムを普及させたいが問題がある
  - RSASHA1が多いのでECDSAなどの新しいアルゴリズムを広めたい
- Visualisation of RIPE Atlas Probes for root dns deployment and routing policies, Ray Bellis@ISC
  - F-Rootへ到達するクエリをRIPE Atlasを用いて評価
  - パロアルトでpeerしている複数の巨大ASのために、各地のAnycast nodeよりもパロアルトが優先される問題の指摘
  - アムステルダムなどのノードも広域に使われる
  - 結果として、200ms以上の遅延のところが日本やEU, USにもある

IEPG (2)

- Infrastructure GeoLoc, Robert Kisteleki@RIPE
  - RIPE NCCでOpenIPMapというGeoIP相当のものを作っているので貢献してほしい
  - https://marmot.ripe.net/openipmap/
- Data Driven Evaluation of root/TLD node placement, Frank Scalzo@Verisign
  - DITL data をもとにrootの配置を把握
  - 地域別のquery source IP addressと量
  - クエリごとの距離などを示されている

IEPG (3)

- The Yeti DNS project, and where we are with it, Shane Kerr @ BII (Beijing Internet Institute)
  - 雪男のロゴと、BIIの巨大なロゴ
  - IPv6 onlyのalternate rootを作って、DNSに関する研究を行うプロジェクト
  - One upon a time at WIDE Camp, Davey Song and Paul Vixie were wondering if ….
  - 主な参加組織: BII, WIDE, TISF(=Paul Vixie)
  - Shaneが、ことあるごとに「WIDE Projectが…」と発言していたことが興味深い
  - いろいろな懸念をコメントされる人が多かった

その他のWG (範囲外)

- mif WG (Multiple Interfaces)
  - 複数のインターフェースから得た設定情報 (DHCP, Route advertisement, PPP) を分けて扱う
    - インターフェースごとにIP/IPv6 address, default route, DNS情報
  - Socket Interfaceを拡張し、socketごとにアドレス、default route、DNS情報を変更
    - setsockopt()でIP_PVDを設定
    - socket(), bind(), listen(), accept(), connect()も変更
    - 当然、kernelも複数のrouting tableを持つ
    - 楽しそうです
- 6man (IPv6 Maintenance)
  - 複数ISPからアドレスを受けるとSource address routing必須
    - 複数のRAを聞くと複数のdefault routeを受け取るが、hostは1つしか使わない
    - 普通のISPは、自分が顧客に割り当てたアドレスからのパケット以外を捨てるというフィルタをすでに実装している
  - Host requirementsを変更するかどうかという議論に
  - draft-baker-6man-multi-homed-host
  - 楽しそうです

参考

- www.ietf.org
  - 過去のIETFミーティングの資料、議事録あり
- www.iepg.org
  - IEPGミーティングの資料