IETF 94 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 94 報告会, 2015年12月8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)
  - DNS関連の問題提起など
    - draft-ietf-dnsop-dns-terminology (2014/11~, AUTH48)
    - draft-fujiwara-dnsop-nsec3-aggressiveuse (2015/3~)
- 一言: IETF 94から今日までの変化が大きい

DNS関連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 (非開催)
  - dbound　　Public Suffix List の後継
  - dnssd　　DNS-SD (RFC 6763)の拡張
- IETF以外
  - IEPG
- DNSを扱ったWG (のうちで見たもの)
  - mif　　Multiple Interfaces
  - homenet　　Home Networking
- ドメイン名
  - lager　　Label Generation Rules (説明できないので対象外)

dnsop (DNS Operations) WG

- 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
- 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
- 振り返り: 2015年7月のIETF 93
  - 多数のdraftが完了し、status report多数
  - TCPトランスポートに関する議論
  - nsec-aggressiveuse
  - トラストアンカー管理の議論
  - .onion以外のTLD予約の話題はDesign Teamに分離

dnsop (2)

- RFC 発行 (1)
  - RFC 7583: DNSSEC Key Timing
    - Informational, 2015/10/21
    - DNSSECでの鍵更新のタイミングについて考察
  - RFC 7646: Negative Trust Anchors
    - Informational, 2015/10/21
    - DNSSEC検証を無効にするドメイン名の設定
    - BIND 9, Unbound, Vantioで実装済
  - RFC 7686: .onion TLD
    - Proposed Standard, 2015/10/23

dnsop (3)

- RFC 発行 (2)
  - RFC 7706: Decreasing Access Time to Root Servers by Running One on Loopback
    - Informational, 2015/11/25
    - ルートゾーンのコピーをfull-service resolverに置く
- RFC Editor Queue
  - draft-ietf-dnsop-dns-terminology
    - Informational, RFC 7719
    - DNS用語集
    - 11/30からAUTH48で最終チェック中

dnsop (4)

- IESGで作業中のもの (1)
  - draft-ietf-dnsop-qname-minimisation, Experimental
    - プライバシー向上のため、クエリ情報の漏洩を最小化
    - IETF Last Call: 11/9～11/23 → コメント反映待ち
  - draft-ietf-dnsop-rfc6598-rfc6303-05, BCP
    - Add 100.64.0.0/10 prefixes to IPv4 Locally-Served DNS Zones Registry
    - IETF Last Call: 11/9~11/23 → 12/7にIESG通過(approved)
  - draft-ietf-dnsop-edns-tcp-keepalive, Proposed Standard
    - DNS/TCPでのkeepalive時間を設定するEDNS0オプション
    - IETF Last Call: 11/16~11/30 → コメント反映待ち
  - draft-ietf-dnsop-5966bis-04, Internet Standard
    - DNS Transport over TCP - Implementation Requirements
    - IETF Last call 11/23~12/7

dnsop (5)

- IESGで作業中のもの (2)
  - draft-ietf-dnsop-cookies, Proposed Standard
    - IETF Last call 11/30~12/14
    - Domain Name System (DNS) Cookies
    - DNS/UDPの攻撃耐性を上げるために、クエリ側で64ビットのCookieを添付し、サーバはレスポンスに同じものをコピー
    - 送信したCookieと受信したCookieが異なっていると異常
  - draft-ietf-dnsop-edns-client-subnet, Informational
    - Public DNSサービスの利用者がCDNのアドレス制御を使用できるように、クライアントのサブネットアドレスを権威DNSサーバに伝えるEDNS0オプション
    - 2015/12/7~12/21 IETF Last Call
  - draft-ietf-dnsop-edns-chain-query, Proposed Standard
    - 2015/11/28 Publication Requested

dnsop (6)

- RFC 7686 The ".onion" Special-Use Domain Name
  - Torで使用している特殊用途ドメイン名として.onionを予約
  - Tor以外での使用, 登録, 設定を禁止
  - 名前解決API, Library, Resolversは.onionを特別扱いして、Tor処理を行うこと(MUST)
    - Torを知らなければエラーとし、名前解決をしないこと
    - .localも特別扱い(RFC 6762, SHOULD)
    - すべてのOSのlibcなどを変更する必要がある？
  - Caching DNS Servers (full-service resolvers)では.onionの名前解決をしないこと (SHOULD NOT)
    - ルートに情報が漏れるため
    - Private addressのゾーンと同じ空のzone設定
  - Operatorは.onionを他用途で設定しない (MUST NOT)

dnsop (7)

- IETF 94でのミーティングの概要
  - これまでの仕事の多くがIESGに提出完了
  - 多くのdraftがWGドラフト候補(candidate)に
    - dnsext WGが対応していたDNSプロトコルの拡張が多い
  - .onion以外の特殊用途TLDの予約
  - 複数の新規提案
    - draft-jabley-dnsop-ordered-answers
    - draft-ogud-dnsop-maintain-ds
    - draft-muks-dnsop-dns-message-checksums
    - draft-muks-dns-message-fragments
    - draft-wessels-edns-key-tag
    - DNAME in the Root?
    - NXDOMAIN means NXDOMAIN

dnsop (8)

- .onion以外のTLD予約について
  - 現在、予約提案が6 (bit, i2p, gnu, zkey, exit, alt)
  - IABとIESGが、dnsopに問題解決を期待している
  - IETF 93で設立されたDesign Teamからの報告
    - draft-adpkja-dnsop-special-names-problem-00
      - Alain Durand, Peter Koch, Joe Abley のイニシャル6文字
    - 現在の状況を把握し、透明な手順を提案する
    - DNSだけではなく、URIのプロトコル識別子(http)などの拡張などを含めた提案などもあり (http-onion://foo/)
    - 選択肢 (予約をやめる, alt TLD, ICANNとのプロセスを作る, 別の識別子, その他)
  - IETF Chairが、IESGで決めることではなくCommunityで議論すべきことであると発言
  - 多数のコメントをDesign Teamがまとめ、継続

dnsop (9)

- .onion以外のTLD予約について (続報)
  - 2015/11/30にICANNから公開されたFinal Report
    - Mitigating the Risk of DNS Namespace Collisions Final Report by JAS Global Advisors
    - https://www.icann.org/news/announcement-2-2015-11-30-en
    - 6ページにRECOMMENDATION summary
    - RECOMMENDATION 1: The TLDs .corp, .home, and .mail be referred to the Internet Engineering Task Force (IETF) for potential RFC 1918 like protection/treatment
  - .corp, .home, .mail もIETFで予約すべきであるとコンサルタントが言っている
  - さてどうなることやら

dnsop (10)

- WG draftとしての採択手順
  - candidate for WG adoption(採択候補)というステータスが追加された
  - Call for adoption 2 weeks
  - Supportという人がいれば採択
- WG draftとして新規採択 (1)
  - draft-ietf-dnsop-refuse-any, 2015/11/4
    - タイプANYのクエリを拒否したいが、RFC 1035に反する
    - ANYに対して大きな応答を返さないという目的に変更
    - ANYの利用目的はdebug,疑わしい最適化,誤解,amp
    - すべてではなく何かを返せばよい (any != all)
    - 応答の自動生成ではHINFOを返すとよいという提案
    - ミーティングでも強いサポートあり

dnsop (11)

- WG draftとして新規採択 (2)
  - draft-ietf-dnsop-dns-no-response-issue, 2015/11/28
    - DNSサーバ無応答問題の分類、評価方法と対策
    - 知らないパケットを捨てるfirewall、TCPのフィルタ、実装ミスなどが原因
    - 2013年5月から提案され、評価結果も公表されていた
    - Call for adoption: 2015/11/12~11/26 → 11/26 adopted
  - draft-wessels-edns-key-tag
    - ValidatorがTrust anchorのkeytagを送信するEDNS0オプションの提案
    - ゾーンの管理者がDNSSEC Trust anchorのロールオーバーの進捗を調べることが目的
    - Call for adoption: 2015/11/28~12/7 → 12/5 adopted

dnsop (12)

- WG draftとして採択候補 (1)
  - draft-ogud-dnsop-maintain-ds
    - CDSでのDS自動更新ではDNSSEC検証できるCDSがあったときにDSを更新するため、最初の登録と削除は不可能
    - DNSSEC設定を、レジストリなしに行う提案
    - 最初は無条件に信用する (Opportunistic) 提案あり
    - Call for adoption 2015/11/28~12/12
  - draft-bortzmeyer-dnsop-nxdomain-cut
    - ミーティング時にはアイデアスライドだけであったもの
    - あるドメイン名がNXDOMAIN(名前不存在)だと、その子孫のドメイン名はすべてNXDOMAINとして扱うという提案
    - draft-vixie-dnsext-resimprove (リゾルバ改良提案)の一項目
    - Call for adoption: 2015/12/5~12/19

dnsop (13)

- WG draftとして採択候補 (2)
  - draft-muks-dnsop-dns-message-checksums, 2015/10/31
    - 攻撃耐性を上げるためにチェックサムを追加
    - Cookieなど他の手段があるため、ミーティングでは不評
  - draft-jabley-dnsop-ordered-answers, 2015/10/31
    - RRSetの順序をそろえる提案で、ミーティングでは不評
  - draft-fujiwara-dnsop-nsec-aggressiveuse, 2015/10/31
    - ミーティングでは触れられなかった
  - draft-fanf-dnsop-rfc2317bis, 2015/11/12
    - Classless IN-ADDR.ARPA delegation and dynamic reverse DNS UPDATE
    - IPv4逆引きDNSの設定についてのRFC 2317のアップデート

dnsop (14)

- WG draftとして採択候補 (3)
  - draft-crocker-dns-attrleaf, 2015/12/2
    - DNS Scoped Data Through '_Underscore' Attribute Leaves
    - IANAにUnderscore names registryを設置する提案
    - dnsop で議論されていなかったが、突然採択候補になった
    - 2006年6月から提案されているドキュメント
    - これまで_sip, _tcp, _udpなどを集中管理していなかったため
- その他
  - DNAME in root
    - .local へのクエリが非常に多いので、それらをAS 112と同様にrootにDNAMEを書くとよいという提案
    - .onionや.exampleなども同様
    - → draftを書くようにという提案があった
    - Rootに漏れていた情報がAS112に漏れるという懸念あり

dprive WG

- 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: 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: IETF 92
  - 別ポート案とSTARTTLS案のマージが好まれた
- 振り返り: IETF 93
  - DNS over TLS継続、DNS over DTLS新規, EDNS Padding新規

dprive (2)

- RFC 7626 DNS Privacy Considerations
  - 2015/8/26 発行
- ミーティング概要
  - DNS over TLSについての報告と確認
  - DNS over DTLSの複雑さについての理解
  - DS,DNSKEYのようなものを使って暗号化するというアイデアの発表があったが、second DTLSはいらないといわれ、不評であった

dprive (3)

- draft-ietf-dprive-dns-over-tls: DNS over TLS
- 概要
  - TCP port 853 で待ちうけ、(httpsのように)TLS処理
    - 複雑なSTARTTLSは消えた
  - DNS over TCP のデータをTLS上に流す
    - 2オクテットのデータ長 + UDP DNSパケットと同じもの
  - TLS/TCPの接続を切らず、張りっぱなしで複数のクエリを処理すること
  - サーバの認証については現在は2種類
    - Opportunistic(認証しない) と 事前設定
- ステータス
  - 2015/10/22~11/12 WG Last Call
  - IETF 94でサーバの認証プロファイルを分離することとなったため、若干遅れそうだが、方向性は合意された
  - 12/7に発行された-02で、サーバの認証プロファイルの追加は他のドキュメントを参照するという記述が追加

dprive (4)

- DNS over TLS実装
  - Unbound: フルリゾルバ
    - Version 1.4.14 から
    - 設定方法 (マニュアルより)

    (ssl-port: 853)

    ssl-service-key: <file> TLS秘密鍵ファイル

    ssl-service-pem: <file>　　TLS公開鍵ファイル

    ssl-upstream: no　Forwarder動作時にTLSで接続
  - getdns api: DNSクライアントライブラリ
    - Version 0.3.0 で入ったようにみえる
  - その他パッチあり
  - TLS(SSL)アクセラレータと既存実装でも実現可能

dprive (5)

- DNS over DTLS, draft-ietf-dprive-dnsodtls
  - UDP port 853を使用し、DTLSのデータとしてDNSを運ぶプロトコル
  - DTLS = RFC 6347 Datagram Transport Layer Security
  - ミーティングでの議論
    - DTLSにはFragmentationの仕組みがないので、そのうえにFragmentationを作る必要があり、複雑さを増すことが理解された
    - DNS層| fragmentation層 | DTLS層 | UDP層 | IP層
    - 複雑そうなので、DNS over TLSだけとなる可能性あり

dprive (6)

- draft-ietf-edns0-padding
  - 暗号データを守るためのEDNS0 Padding
  - Call for adoption: 2015/11/3~11/17
  - WG draftとして採択

dane WG

- DNS-based Authentication of Named Entities WG
- DNSにTLSの証明書を載せるWG

- 振り返り: IETF 90, 2014/7
  - SMTP, SRV 議論完了
- 振り返り: IETF 91, 2014/11
  - DANE SMIMEA: 実装案の議論とOpenPGPとのマージ提案
- 振り返り: IETF 92, 2015/3
  - OpenPGPKEY: WGLC完了
  - 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
- 振り返り: IETF 93, 2015/7
  - DNSSEC auth chain extension
  - メールアドレスの扱いについての議論
    - base32(user name)._openpgpkey.dom

dane (2)

- ミーティング非開催
- 2015/10/14にRFC発行 (proposed standard)
  - RFC 7671: DANE Protocol: Updates and Operational Guidance
  - RFC 7672: SMTP Security via Opportunistic DANE TLS
  - RFC 7673: Using DANE TLSA Records with SRV Records
- draft-ietf-dane-openpgpkey-06
  - 10/19からWaiting for Writeup::AD Followup
  - メールアドレスで迷走か？
  - SMIMEAも停止中

dbound (Domain Boundaries) WG

- 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
    - https://publicsuffix.org/
  - 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
- 振り返り
  - IETF 91:WG設立の合意
  - IETF 93:主な議題はDefine the problemで結論出ず
    - 用途案:Cookie, 証明書発行, ワイルドカード証明書, DMARCドメイン名抽出

dbound (2)

- IETF 94では90分間の議論が行なわれた
- 活発な議論が行なわれたが、何を解決したいかがあいまいであり、結論が出なかった
- draft-deccio-dbound-organizational-domain-policy
  - ドメイン名の管理情報をDNSに置く新提案
  - <内部ドメイン名>._odup.<組織ドメイン名> TXTに各種制約を書くという提案
  - ドメイン名が与えられると、すべての”.”区切りに”_odup”ラベルを追加し、TXTを調べること
    - 内部ドメイン名の上位ドメイン名を調べること
  - ラベル数がn個の場合、n(n-1)/2のTXTクエリが必要

dnssd (Extensions for Scalable DNS Service Discovery) WG

- 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: IETF 91
  - Long Lived Queries,脅威モデル
  - ハイブリッドプロキシー
- 振り返り: IETF 92
  - DNS Push: LLQの代わりにDNS Updateに変更
- 振り返り: IETF 93
  - 基本的には継続した議論
  - DNSとmDNSでラベルの扱いが違う問題
  - Push Notifications, 脅威モデル, 実装の紹介

dnssd (2)

- ミーティングの雰囲気は若干減速気味
  - homenetで使いたいので実装している
  - dnssdを変形したプロトコルの提案
    - IoT関連の名前解決のため業界団体が動き始めた
- draft-ietf-dnssd-hybrid
  - dnssdをmDNSとDNSのHybrid proxyとして実装
  - 近いうちにWGLCの予定だが未実施
- DNS Push Notifixations
  - mDNSに名前を登録するプロトコル
  - DNS Updateをベースに新しく作成された
  - Hybrid proxyとの整合性が取れているか確認が必要
- draft-ietf-dnssd-mdns-dns-interop
  - mDNSとDNSのラベルの整合性
  - WGLCは完了して、近いうちにIESGに提出見込み

mif (Multiple Interfaces) WG

- 複数のインターフェースを使い分けるプロトコル
- RFC 7556: Multiple Provisioning Domain Architecture
  - 各i/fの設定情報をProvisioning Domain (PvD)とし、複数を使い分けることができるアーキテクチャ
- MIF using reverse DNS, draft-stenberg-mif-mpvd-dns
  - _pvd.逆引きドメイン名 PTR にPvD設定情報のドメイン名
  - PvD設定情報ドメイン名のTXTに設定情報
  - 設定情報には、回線の情報や、提供されるアプリケーションの情報、DNSサーバの情報など

例:

_pvd.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.2.3.4.5.6.7.8.8.b.d.0.1.0.0.2.ip6.arpa PTR iptv.foo.example.

iptv.foo.example TXT “n=Foo IPTV” “s” “6=2001:db8::/64” “r=dns-iptv.foo.example”

Connection to Foo IPTV, no-internet, access to 2001:db8::/64 only, use dns-iptv.foo.example as Recursive DNS

homenet (Home Networking) WG

- 家の情報をDNSに出す仕組みが提案されているが停滞気味
  - draft-ietf-homenet-front-end-naming-delegation
    - 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
  - draft-ietf-homenet-naming-architecture-dhc-options
    - DHCPにhybrid proxyなどの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(IETF 93) → IETF 94後も未実施

IEPG

- 若干低調気味であり、研究発表が多い
- Comparing IPv4/IPv6 measurements from RIPE Atlas
- Big data based security applications
  - .NLの新規登録ドメイン名に、毎日200クエリ程度のクエリがあり、フィッシング用だったものがあった
  - 普通のドメイン名は登録直後のクエリは少ない
  - HadoopHDFS+SQLを用い、52TBのpcap dataをhadoop 4ノードでSQLで3.5分で検索可能
  - 検出したら画面を保存しておき、あとで判断
- DNS over TCP - what might it look like
  - Comcastのデータを用いてDNS over TCPの負荷を評価
- 招待講演: How a router actually works…
  - NANOG 65での講演

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