IETF 95 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 95 報告会, 2016年5月10日

Last update: 2016/5/10 0300

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
    - RFC 7719: DNS Terminology
    - draft-fujiwara-dnsop-nsec3-aggressiveuse (2015/3~)
- 個人的なIETF 95結果:IEPG発表1,dnsopでコメント1
  → Call for adoption

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
  - dbound　　Public Suffix List の後継
  - dnssd　　DNS-SD (RFC 6763)の拡張
  - arcing　　IABによるDNS以外の名前解決のBoF
  - homenet　　Home Networking
- IETF以外
  - IEPG
  - DNS-OARC Workshop

DNS関連報告の概要

概要 1

- dnsop: DNS運用ガイドラインの作成
  - RFCを多数生産中 (IETF 94から5本、RFC Editor Queueに4本)
  - 多数の提案の議論が進められた
  - その場で結論を出さないものが多かった
- dprive: DNS通信路の暗号化
  - DNS over TLSが完了したため、一時間と短め
  - DNS over DTLSを進めるが、DTLSが難しく、reviewerが少ない
- dane: DNS(SEC)にTLSの証明書
  - ほとんどの議論が完了したため、非開催

概要 2

- dbound: Public Suffix List の後継
  - 非開催
  - 進捗が遅いのでADからどうするか問われている
- dnssd: DNS-SD (RFC 6763)の拡張
  - 使いにくいプロトコルになりそうなことがわかってきた
  - さらに、プライバシーということで、限定的に名前を返す提案が出てきて迷走しそう
- homenet: Home networking
  - dnssdのプロトコルが使えないものとなったため、通常のDNSを使用した新しい名前解決アーキテクチャが提案された

概要 3

- arcing: IABによるDNS以外の名前解決についてのBoF
  - dnsopで時間を消費するTLD予約について、IABを中心に解決する方向で意見を集めるBoF
  - インターネットでのDNSとDNS以外の名前解決の解説と、それについての議論が行なわれた
- IEPG: 運用に関する話題を扱うinformalな集まり
  - DNS (5件)とBGP (1件)、アドレス移転(1件)の発表が行なわれた
  - 今回は全体的に低調で、ほとんど質問がなかった
- DNS-OARC Workshop
  - Root zoneのDNSKEY Rolloverについての報告や予定が発表された
  - Root DNS serverなどへのDoSの状況が報告された
  - DNS Privacyについての実装が紹介された

詳細

dnsop (DNS Operations) WG

- DNS運用ガイドラインを作るWG
  – DNSプロトコル拡張を作る機能も含む

- 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
  – 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
- 振り返り: IETF 94でのミーティングの概要
  – .onion以外の特殊用途TLDの予約
  – 多数の新規提案: ordered-answers, maintain-ds, dns-message-checksums, message-fragments, edns-key-tag, DNAME in the Root?, NXDOMAIN

dnsop

- 着実にRFCを発行

2015/11/24　RFC 7706 draft-ietf-dnsop-root-loopback
2015/12/15　RFC 7719 draft-ietf-dnsop-dns-terminology
2016/ 3/ 3　RFC 7766 draft-ietf-dnsop-5966bis
2016/ 3/22　RFC 7816 draft-ietf-dnsop-qname-minimisation
2016/ 4/ 6　RFC 7828 draft-ietf-dnsop-edns-tcp-keepalive

- RFC Editor Queue

2015/12/10　draft-ietf-dnsop-rfc6598-rfc6303
2016/2/24　draft-ietf-dnsop-edns-chain-query
2016/3/30　draft-ietf-dnsop-edns-client-subnet
2016/4/11　draft-ietf-dnsop-cookies

- 現在、IESGでレビュー中のDraftはなし

dnsop (2)

- RFC 7706: draft-ietf-dnsop-root-loopback
  - Informational, 2015/11/24
  - ルートゾーンのコピーをフルリゾルバのloopback interfaceで動かし、ルートへのアクセス時間を短くするアイデア、BIND 9.9, NSD 4/Unbound 1.4, Microsoft Windows Server2012での設定例あり
- RFC 7719: draft-ietf-dnsop-dns-terminology
  - Informational, 2015/12/15
  - DNS用語集
  - 従来のDNS用語を使うだけなら、Terminology sectionでRFC 7719をreferするだけでよい

dnsop (3)

- RFC 7766: draft-ietf-dnsop-5966bis
  - Proposed Standard, 2016/3/3
  - TCP通信路でのDNSの実装要求仕様
  - RFC 1035の明確化、最近の技術の追加など
    - 一つのTCPで複数クエリを連続して送ること
    - 複数のクエリを送った場合に応答は順不同 (UDPと同じ)
    - アイドルタイマーを使ったクローズ
    - TCP Fast Open
- RFC 7828: draft-ietf-dnsop-edns-tcp-keepalive
  - Proposed Standard, 2016/4/6
  - 長期生存するTCPセッションの使用を支援するため、keepalive時間を指定するEDNS0オプション

dnsop (4)

- RFC 7816: draft-ietf-dnsop-qname-minimisation
  - Experimental, 2016/3/22
  - フルリゾルバから権威DNSサーバへのクエリ時のクエリ情報(クエリ名、タイプ)の最小化
  - クエリ名をTLDなどの短い側から小出しにする
  - ルート、TLDなどへ送るクエリのタイプをNSとし、最後に知りたいタイプのクエリを送る
  - (DNSに与える負荷は増大するため、各種低減措置の議論が進む)
  - Unbound 1.5.7やKnot resolverで実装済

dnsop (5)

- RFC Editor Queue (1)
  - draft-ietf-dnsop-rfc6598-rfc6303, Best Current Practice
    - Add 100.64.0.0/10 prefixes to IPv4 Locally-Served DNS Zones Registry
    - 空応答を返すため、フルリゾルバに64ゾーン追加
    - {64..127}.100.in-addr.arpa
  - draft-ietf-dnsop-edns-chain-query, Experimental
    - Validatingスタブリゾルバからフルリゾルバの通信で、クエリ名の検証に必要な情報をまとめて受け取るためのEDNS0オプション
    - EDNS0オプションで指定したドメイン名を検証済として、そこからクエリ名までの検証に必要なDS, DNSKEY, RRSIGをauthority sectionに追加

dnsop (6)

- RFC Editor Queue (2)
  - 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
    - [address-family] [prefix-length] [prefix]
    - 実装済 (Public DNS, CDN, Hyper Giants)
  - draft-ietf-dnsop-cookies, Proposed Standard
    - 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、サーバはレスポンスにコピー
    - 送信したCookieと受信したCookieが異なると異常
    - [client-cookie 8 bytes] [server cookie 8 to 32 bytes]
    - 実装済 (BIND 9.10.0 sit → 9.10.3 draft対応)

dnsop (7)

- IETF 95ミーティングの概要
  - IETF 94からの提案とその後の新規提案を進めるための議論が行なわれた
  - 今回のdnsop WGでは、議題ごとにコメントを受け付け、チェアが感じた雰囲気にしたがってメーリングリストでの議論を進めるという進め方であった
    - Humは、edns-key-tag, dns-delegation-requirements

dnsop (8)

- 議論されたテーマ
  - draft-ietf-dnsop-resolver-priming
  - draft-ietf-dnsop-dnssec-roadblock-avoidance
  - draft-ietf-dnsop-refuse-any
  - draft-ietf-dnsop-maintain-ds
  - draft-ietf-dnsop-nxdomain-cut
  - draft-ietf-dnsop-edns-key-tag
  - DNS over HTTP
  - draft-wkumari-dnsop-cheese-shop vs draft-fujiwara-dnsop-nsec-aggressiveuse
  - draft-wallstrom-dnsop-dns-delegation-requirements
  - draft-ietf-dnssec-algorithm-update
  - draft-sullivan-dns-class-useless
  - draft-vavrusa-dnsop-aaaa-for-free
  - draft-valsorda-dnsop-black-lies
  - .onion以外の特殊用途TLDの予約 (→ arcing BoF)

dnsop (9)

- draft-ietf-dnsop-refuse-any
  - タイプANYクエリを拒否したい(RFC 1035違反)
  - ANYに対して大きな応答を返さないことに変更
  - すべてではなく何かを返せばよい (any != all)
  - ClouldFlareではHINFOを自動生成
  - NSDはMX+A+AAAAを応答

  → **MX+A+AAAAも追記するように指示、議論をみてWGLC**
- draft-ietf-dnsop-maintain-ds
  - DNSSEC設定を、レジストリなしに行う提案で、最初は無条件に信用する (Opportunistic) 提案を含む
  - 懸念点を示されると、**”Send text”**

dnsop (10)

- draft-ietf-dnsop-nxdomain-cut
  - あるドメイン名がNXDOMAIN(名前不存在)の場合、その子孫をすべてNXDOMAINとして扱うという提案
  - 空の非終端ドメイン名の扱いにバグのあるサーバの懸念を示された
  - RFC 1034, 2308の明確化にとどめておくべきであるというコメントもあった
- DNS over HTTP: draft-song-dns-wireformat-http
  - DNSのbinary dataをそのままHTTPで伝達
  - DNSをブロックされた時にport 80/443を使いたい？
  - 関心を持つ人やsupportする人は多い
  - text/jsonが良いと思う人や既存のAPIなどとの親和性に懸念を持つ人がいるため、議論を継続させる見込み

dnsop (11)

- DNSSECの不存在証明の活用
  - draft-fujiwara-dnsop-nsec-aggressiveuse
    - 可能なケースに対応 (NSEC, NSEC3, ドメイン名空間全体)
    - 部分的な実装も考慮
  - draft-wkumari-dnsop-cheese-shop
    - ルートサーバからの応答に限定
    - スコープを狭くして早めに標準化・実装を進める意図
  - 議論の結果、nsec-aggressiveuseのほうが好まれた
    - Chairからのメールの引用: “the sense we received from the room is that the group should move forward with this draft.”
  - 4/10に Call for adoption (WG draftにするか判断するプロセス) を開始、4/25に承認され、現在アップデート中

dnsop (12)

- draft-wallstrom-dnsop-dns-delegation-requirements
  - (DNS設定判定ツールを作るにあたっての)委任についての要求条件をまとめたもの
  - 新しい仕様定義はないのにMUST/SHOULDを多用している点に問題がありそう
  - 継続
- draft-ietf-dnssec-algorithm-update
  - DNSSECで使用するアルゴリズムの優先順位を指定したいという提案
  - 署名と検証にわけ、MUST+/ MUST/ SHOULDなどレベル付け
  - 継続

dnsop (13)

- draft-sullivan-dns-class-useless
  - “IN”以外のクラスは使われていないので、使わないことにする提案
  - CHAOSとHESIODは使用されていたというコメントあり
  - 反対はないが、クラスフィールドを転用できるわけではないので、変化はない
- draft-vavrusa-dnsop-aaaa-for-free
  - A, AAAAを一つのクエリで同時に名前解決する提案で、EDNS0オプションなどのシグナリングを使わず、additional sectionに追加する
  - 従来のクライアントは捨てるだけで無害
  - RRSIGを付けておき、DNSSEC検証すればよい
  - 反対意見や、別の提案などがあり、結論でず

dnsop (14)

- draft-valsorda-dnsop-black-lies
  - Online signing (クエリ処理時に署名) の場合に名前が存在しないことを示すため、空の応答を用いたいという提案
  - 存在応答のほうが小さいため、うれしい
  - 例: missing.filippo.ioが存在しない応答 (RRSIG略)
    - RCODE=NOERROR
    - missing.filippo.io IN NSEC ¥003.missing.filippo.io NSEC RRSIG
  - 従来 (RRSIG略)
    - RCODE=NXDOMAIN
    - filippo.io IN SOA
    - {missing.Filippo.ioの直前} IN NSEC ¥000.missing.Filippo.io NSEC RRSIG
    - {*.Filippo.ioを含む範囲} IN NSEC …
  - 継続

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
- 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
- 振り返り: IETF 94
  - DNS over TLS ほぼ完了、edns paddingほぼ完了、DNS over DTLS継続

dprive (2)

- RFC Editor Queue
  - draft-ietf-drprive-over-tls, Proposed Standard
    - TCP port 853 で待ちうけ、(httpsのように)TLS処理
    - 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
    - サーバ認証プロファイルとしてOpportunistic(認証しない) と 事前設定
  - draft-ietf-dprive-edns0-padding, Proposed Standard
    - 暗号データを守るためのEDNS0 Padding optionの追加

dprive (3)

- ミーティング概要
  - ミーティング時間、一時間のみ
  - ドキュメントステータスの報告
  - DNS over DTLSについての議論
  - サーバ認証プロファイルについての議論
  - TLS 1.3の報告
  - 完了が見えてきたため、短め

dprive (4)

- 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
      IP fragmentationには非対応
  - 前回、DNS over DTLS fragmentationについて提案されたが複雑で合意されそうになかったため、**fragmentationを削除**、IP fragmentationしそうになったら**TC=1**とし、DNS over TLSで再問合せ
    - DF(Don't fragment)ビットを使用？
  - ミーティングでの議論
    - Reviewした人数が少ないため、結論を出せない
    - 多くの人がReviewしたらWGLC予定

dprive (5)

- draft-ietf-dprive-dtls-and-tls-profiles
  - 2016/1/27にWG draftとして採択
  - DNS over (D)TLSの使い方を規定するもの
  - フルリゾルバの証明書の入手手順
    - Opportunistic (証明書を検証せずに暗号機能のみを使用)
    - 事前設定 (サーバのSPKI pinsetを指定)
    - DHCPでDNS-IDを得てDANE(_domain-s.DNS-ID)
    - DANE(_853._udp.server_domain_name)で入手
  - 検証結果による動作
    - 違ったら接続しない、違ったら暗号化をやめる
    - 一致したらDNS over TLSを使用
    - 検証できないときどうするか
  - ミーティングでの議論
    - 内容の確認
    - わかりにくいので利用モデルを追加すること
    - “no privacy”の追加 (TLSを使用しない)

dane WG

- DNS-based Authentication of Named Entities WG
- DNSにTLSの証明書を載せるWG
- Status
  - 2015/10/14にRFC 7671 (Updates), RFC 7672 (DANE SMTP), RFC 7673 (DANE SRV) 発行
  - 残件: OPENPGPKEYとSMIMEA
- 振り返り: IETF 92, 2015/3
  - OPENPGPKEY: WGLC完了→2015/5/23にIESGに提出
  - hex(先頭28バイト(sha256(tolower(localpart)))) ._openpgpkey.dom
- 振り返り: IETF 93, 2015/7
  - OPENPGPKEY変更案: base32(localpart)._openpgpkey.dom
- IETF 94, IETF 95: ミーティング非開催

dane (2)

- draft-ietf-dane-openpgpkey
  - 2015/5/23にIESGに提出 (-03)
  - メールアドレスで迷走していたようである
  - Version 03～10での主な変更点
    - 問題点が多いため、実験に変更 (Status: Experimental)
    - ローカルパートの正規化 (CFWS, “.”の削除, Unicode NFC)
    - hex(先頭28バイト(sha256(localpart)))._openpgpkey.dom
    - ↑ tolower小文字化が削除
  - 2016/4/21 IESG投票 (-10) → 5/2に-12
    - ART AREA のADからのDISCUSS → 5/3にYES → 5/9承認
    - メールアドレスのlocalpartは、US-ASCIIの大文字小文字をプロトコルでは区別するが、実装は区別しないことが多い
    - John.Smith, john.smith など、使用する可能性があるlocalpartすべてから作成したOPENPGPKEY RRを書く必要あり

dbound (Domain Boundaries) WG

- Public Suffix List (PSL)の後継を考えるWG
- Public Suffix List
  - Cookieの取り扱い判定などで使用されている
  - 巨大なテキストの順序付きリスト
  - Mozilla Foundationがメインテナンス
  - https://publicsuffix.org/
- 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
  - IETF 94:何を解決したいかが曖昧であり、結論出ず
- 2016/3/21に担当ADから進捗が見られないので進め方を提案をするようにという厳しいメール
  - IETF 95: 非開催

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: 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
- 振り返り: IETF 94
  - 継続した議論だが若干減速気味

dnssd (2)

- draft-ietf-dnssd-hybrid
  - dnssdをmDNSとDNSのHybrid proxyとして実装
  - リンクごとにドメイン名を設定、ルータなどでproxyを動かす
    - 例: link1.example.com, link2.example.com, …
  - Proxy: <name>.local ⇔ <name>.link1.example.com
    - <name>.link1.example.com PTRクエリを受け取ると、<name>.local PTRクエリをmDNSで送り、応答を書き換えて返す
  - Browse設定を管理者が行なう
    - b._dns-sd._udp.example.com PTR link1.example.com
PTR link2.example.com
…
  - WGLCコメントの紹介が行なわれ、反映後、IESGに提出見込み
  - 使いにくいプロトコルになったと思われている雰囲気あり

dnssd (2)

- draft-ietf-dnssd-push-07
  - DNS Push Notifications
  - DNS/TCPで名前管理サーバに接続し、ゾーン名を指定してSUBSCRIBE (rcode 6)メッセージを送るとSUBSCRIBE
  - 名前管理サーバは、DNS UPDATEのフォーマットでクライアントにゾーン情報の変化を送る
    - 最初は全情報？
- draft-huitema-dnssd-privacy-00
  - Privacy Extensions for DNS-SD
  - プライバシーのために、ホスト名をランダムに、ID類を64bitのハッシュにするという提案
  - 議論を継続
  - (迷走の予感)

Homenet WG

- Home Networking
- (IETF Chairの)家のネットワーク

- 振り返り: IETF 93 (2015/7), IETF 94 (2015/11)
  - Homenetでの名前解決にはdnssdのhybrid proxy使用
  - 家の情報をDNSに出す仕組みが提案されているが停滞
  - 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

homenet (2)
homenetでの名前解決の新提案

- draft-lemon-homenet-naming-architecture
  - dnssd hybrid proxyがhomenetの考えとは違う形でまとまったため、2016/3/21に新提案
  - Ted Lemon, Nominum, Inc.
  - Homenet Naming Databaseで情報管理
    - mDNS browse, snoopで情報収集
    - UPDATEで明示的に登録
  - 複数のname space
    - Global: ISPから指定など (name.example.com)
    - Local: .homenetなどの割り当てを想定
    - Guest？ 客向け
  - 今後継続して議論される見込み
    - ただし、従来のdnssd hybrid proxy案もまだ生きている

homenet (3)

- RFC 7788 Home Networking Control Protocol にErrata指摘
  - 2016/4/23に発行されたRFC 7788に ”.home” TLDをdefaultで使用すると書かれていた
  - ただし、正式な予約手続きは書かれていない
  - dnsop WGでは TLD予約を進めているのに、review processがないことが問題になった
  - とりあえず、2016/4/26にErrataとして”.home”のところを削除する訂正案をdnsop chairが投稿
    - http://www.rfc-editor.org/errata.php

arcing bof

Alternative Resolution Contexts for Internet Naming

- 「インターネットネームのための代替の解決コンテキスト」(by Google翻訳)
- IABによるBOF
  - 現在のIABメンバーにDNS関係者3名 (IAB chair = 元dnsext chair, dnsop chair, DNS Anycast / URIの著者)
  - IABによる発案で、インターネットの新しいアーキテクチャとしての名前空間を考えるもの
  - WGを作るBOFではない
- 発表
  - DNS、ドメイン名の歴史の振り返り
  - 他の名前解決システムの紹介 (nsswitch, p2psip, …)
- 議論
  - Homenetではローカルな名前空間が必要なことなど、活発な議論が行なわれた
  - 次回のIETF 96でWGを作るためのBOFを開くこととなった
- 個人的な希望
  - dnsopでのTLD予約の議論がこちらに移るとうれしい

IEPG

- 運用に関する話題を扱うinformalな集まり
- 7件の発表
  - Stuff seen at ns.icann.org - Roy Arends
  - BGP in 2015 - Geoff Huston
  - Internationalized Domain Name (IDN) query trends seen at JP and Root - Kazounori Fujiwara
  - Continuous Data-driven Analysis of Root Stability (CDAR) - Giovane C. M. Moura
  - Legacy transfers and RPKI Up / Down - Randy Bush
  - EDNS Compliance - Mark Andrews
  - Missing Keytags - Roy Arends

IEPG (2)

- Stuff seen at ns.icann.org
  - ns.icann.orgのクエリ分析
  - int, museum, icann.org, mcast.net, 224~239.in-addr.arpaなどを提供
  - ns.icann.orgのクエリの59%がIP6.INT
  - TPC.INTクエリがまだくる(電話番号のドメイン名)
    - 電話番号からFAXのメールアドレス (ENUMの前身)
- IDN query trends seen at JP and Root
  - JPとRootで見た国際化ドメイン名クエリの傾向
  - JPでは0.2%, Rootでは0.1%がIDNクエリ
  - 2~3%のIPアドレスがIDNクエリを送信
  - 増加傾向はみえるが確実ではない
  - 普及度: IPv6 > DNSSEC >> IDN, 新gTLD ?

IEPG (3)

- Continuous Data-driven Analysis of Root Stability (CDAR)
  - ICANNからの公募により、新gTLDプログラムがRoot DNSの安定に及ぼした影響を評価しはじめた
  - いまのところ、影響がなかった
  - (そもそもクエリ数が非常に少なかった)
- EDNS Compliance
  - EDNS対応状況の把握
- Missing Keytags
  - dnssec-keygenでRSA鍵を作成しても16k個しかできなかった
  - Keytag計算は65535 = 3*5*17*257 の剰余
  - (P*Q) % 3, 5, 17 or 257 will never be 0
  - (P*Q) % 3 has 2 solutions (not 3), %5 -> 4, %17 -> 16, …
  - (P*Q) % 65535 has 2*4*16*256 solutions = 32768
  - Revoke bitを0, 1のパターンを用意するので半分に

DNS-OARC

- DNS Operations Analysis and Research Center
- https://www.dns-oarc.net/
- DNSの運用、解析、研究を行う組織
  - Root DNSサーバのオペレータやTLD、大規模なユーザ組織が参加
  - 毎年50時間、Root DNSサーバのパケットキャプチャ実施
    A Day in the Life of the Internet (DITL)
  - 日本の組織だと、WIDE、JPRSがメンバー
- 年に2度Public Workshopを開催
  - 今回はIETF 95前の木金 2016年3月31日～4月1日

DNS-OARC 2016 Spring Workshop (OARC 24)

- Patron sponsorにNTT Communications (US)
- 参加者: 日本人、日本からの参加者は合計3
- https://www.dns-oarc.net/ のPast workshopsをたどる
- 20件の発表と5件のライトニングトーク
- 内容
  - State of the "DNS privacy" project: running code
  - Unbound QNAME minimisation
  - Knot DNS Resolver
  - Review and analysis of attack traffic against A-root and J-root on November 30 and December 1, 2015
  - Increasing the Root Zone ZSK Size
  - Rolling the Root Key

OARC 24 (2)
DNSプライバシー関連

- State of the "DNS privacy" project: running code
  - 現在の実装状況の報告
- Unbound QNAME minimisation
  - UnboundにQNAME minimisationを実装した
  - 実装時に考えないといけなかったことを発表
  - NSクエリ時にSERVFAILを返すCDN/Load balancer
  - Unbound 1.5.7で実装 (default off)
- Knot DNS Resolver
  - Qname minimisation実装済、default on
  - 近いうちに正式リリース

OARC 24 (3)
ルートサーバへのDoS報告

- Review and analysis of attack traffic against A-root and J-root on November 30 and December 1, 2015
  - 2015/11/30 0650-0928, 2015/12/01 0510-0608 のDDoSをA,Jのデータで分析
  - 10 out of 13 (D,L,M no attack)
  - IPv4 UDP only
  - A,J: 5M queries/sec
  - 895 million source IP addresses, 4739 address sent 100+ queries, top 200 addresses 68%
  - RRL (Response Rate Limiting)で60%の応答を自動的に減らせた
  - 攻撃にパターンがあったため、容易にフィルタできた
  - ということで、RRLの有効性を示せたとのこと

OARC 24 (4)
Root DNSSEC key rollover関連

- Increasing the Root Zone ZSK Size
  - 2016/10/1にRoot zone ZSK sizeを1024bitから2048bitに変更する計画
  - Daune Wessels @ Verisign = Root zone operator
  - 連邦政府的に1024bit RSAの使用を継続しにくいと推定
- Rolling the Root Key
  - ICANNのRoot KSK Design Teamの報告
  - DNSSECのRoot trust anchorを変更する話
  - RFC 5011: Automated Updates of DNS Security (DNSSEC) Trust Anchors を使うとうまくいきそうであるということ
  - 検討結果を2015/12にICANNに報告した
  - 具体的な実行の話ではない

参考

- www.ietf.org
  - 過去のIETFミーティングの資料、議事録あり
- www.rfc-editor.org
  - RFC
- www.iepg.org
  - IEPGミーティングの資料
- www.dns-oarc.net
  - DNS-OARCの情報、Workshop資料