DNS関連情報の入手方法
(+OARC/IETF報告)

藤原 和典
fujiwara@jprs.co.jp
株式会社日本レジストリサービス (JPRS)

Internet Week 2017, DNS Day
2017年11月30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 (2002年に転職してから)
- 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
  - RFC 7719: DNS Terminology → terminology-bis
  - RFC 8198: DNSSECを用いた名前解決の性能向上
  - draft-fujiwara-dnsop-additional-answers-00: 複数応答を返す新提案
- その他
  - Internet Week 2017 プログラム委員

紹介する情報源の種類と主な組織

- 研究: 学会 (ACM, IEEE, IEICE, IPSJ, JSSST, Usenix, …)
- プロトコル作成: IETF
- DNS関連の業界団体: DNS-OARC, dnsops.jp
- オペレータ団体、資源管理組織など
  - APNIC, APRICOT, JANOG, NANOG, RIPE NCC, …
  - ICANN
- DNSソフトウェア: BIND 9, Knot DNS, NSD/Unbound, …
- 企業など: JPNIC, JPRS, Nominum, Verisign, …

情報源ごとの傾向とDNS運用への近さ

1. **DNSソフトウェア**: **新機能、脆弱性、バグ情報、使い方**
2. **DNS関連の団体: DNSだけの時間を過ごせる**
3. **オペレータ団体**: **攻撃、脆弱性、設定ミス**、統計情報
4. **IETF**: プロトコルを作る過程と、結果としての**RFC**
5. ICANN: ポリシー、ccTLD/gTLD全体の動向など
6. 企業など: 自社サービスの宣伝につながるものや、**日本語での情報**
   - ソフトウェアの脆弱性を翻訳して提供している組織あり
7. 学会: 論文になるもの、稀に運用に有用な情報

DNSソフトウェア (1)

- BIND 9 (Internet Systems Consortium)
  - www.isc.org → Open Source → BIND DNS Server → BIND Users mailing list
  - bind-announce@lists.isc.org
    - 脆弱性情報や新規リリース情報
  - bind-users@lists.isc.org
    - 利用者による情報交換 + bind-announce
    - 開発者がよく返事している
    - Assertion failureのlogを送るとみんな慌てる →　bind-bugs に送ること
    - bind-users mailing listを読んでおくと、バグを事前に知ることができる可能性がある

DNSソフトウェア (2)

- NSD (NLnet Labs)
  - www.nlnetlabs.nl → Projects → NSD
  - nsd-users mailing list
  - 開発者がよく返事している
- Unbound (NLnet Labs)
  - www.unbound.net
  - unbound-users mailing list
  - 開発者がよく返事している
- Knot DNS servrer (cz.nic)
  - www.knot-dns.cz → Development にメーリングリスト情報
- Knot Resolver (cz.nic)
  - www.knot-resolver.cz
  - メーリングリストは不明で、Knot DNSのを共用？

DNS関連団体 DNS-OARC

The DNS Operations, Analysis, and Research Center

- www.dns-oarc.net
- 会員制組織
  - それなりの会費
- 年に2度、ワークショップを開催
  - 2日間 (例:0900-1800, 0900-1500)
  - DNSだけ
  - ICANNや、大規模な運用者、実装者のひとが興味深い内容を発表
  - だれでも参加可能 (参加費 $150)
  - 資料とビデオが公開
- 言語は英語
- 公開Mailing list
  - dns-operations@dns-oarc.net
  - だれでも参加可能
  - IETF DNS関係者、TLDオペレータ、ISPのオペレータ、Public DNSなどのオペレータなどが参加
  - KSK Rollover延期やルートサーバのアドレス変更などから、ドメイン名の設定不良の指摘などの軽い話題まで
    - 実名入り
    - 指摘されたら、すぐ治す
  - 最近の話題: new public DNS service 9.9.9.9

オペレータ団体のミーティングなど

- NANOG: North American Network Operators' Group
  - www.nanog.org　　年3回のミーティング、メーリングリスト
- 各地域のネットワークオペレータグループ(NOG)
  - 例: JANOG
- 地域インターネットレジストリ
  - アドレスポリシーと、地域NOG機能
  - RIPE NCC　www.ripe.net　　年3回のミーティング、メーリングリスト
  - APNIC　www.apnic.net　　年2回のミーティング
  - LACNIC　www.lacnic.net
  - AFRINIC　www.afrinic.net
  - ARIN　www.arin.net　　(NOG機能はNANOG)

RIPEミーティング

- RIPE NCCはヨーロッパ中東地域のアドレスレジストリ
- RIPE meetingは、JPOPM+JANOG相当の範囲をカバー
- www.ripe.net → Meetings → RIPE Meetings → Previous RIPE Meetings → RIPE 75 を選び、PRESENTATIONSをクリック
- DNS関連の話題 (RIPE 75)
  - A Curious Case of Broken DNS Responses という発表あり
    - 中東の某国では8.8.8.8の応答が別の応答に書き換えられている
  - Knot Resolver - a modern DNS resolver
    - Knot resolver実装状況の紹介
  - Living on the Edge: (Re)focus DNS Efforts on the End-Points
    - エンドノードでのDNS関連の脆弱性と対策

ICANN

- インターネットの資源管理を行う非営利法人
  - TLDの登録・管理、ルート
  - IPアドレスなどの管理
  - プロトコル番号などの管理
- 年に4回のミーティング
  - 基本的にはポリシー策定
  - DNS運用に関する技術的な話題も取り上げられる
- www.icann.org からたどる
  - 日本語のページも増えている
  - 探しにくい

標準化団体 IETF: Internet Engineering Task Force

- インターネットで使用するプロトコルを作成し、RFCとして発行
- 年3回の会議と公開メーリングリストで議論
  - ドキュメント、資料、Minutesとメーリングリストアーカイブを公開
  - www.ietf.org
- DNS関連は複数のWorking Groupで扱われている
  - dnsop (DNS Operations): DNS運用、DNSプロトコル拡張のhome
  - dprive (DNS Private Exchange): DNSプライバシー
  - dnssd (Extensions for Scalable DNS Service Discovery)
  - doh (DNS over HTTP)

学会 (1)

- 研究者は論文を論文誌に採録されて評価される
- 論文は公開
  - 有料(定期購読か購入:値段はいろいろ648円, 3240円, $15, …)
- 検索は無料
  - “Domain Name System” や “DNS” で論文検索
- 欧米の著者はpdfを個人サイトで公開する傾向がある

  → タイトルと著者名で検索する
- ニュースサイトで話題になってからでも十分

学会 (2)

- IEEE: The Institute of Electrical and Electronics Engineers, Inc.
  - http://ieeexplore.ieee.org
- ACM: Association for Computing Machinery
  - https://dl.acm.org
- USENIX: Advanced Computing Systems Association
  - https://www.usenix.org
- 情報処理学会 (IPSJ)
  - インターネットと運用技術研究会など
- 電子情報通信学会 (IEICE)
  - インターネットアーキテクチャ研究会、情報ネットワーク研究会など
- ソフトウェア科学会 (JSSST)

言語 (英語問題)

- 資料は英語のものが多く、日本語は少ない
  - 「英語の情報しかない」→「英語が読めない」は世界共通
- 国連公用語:中国語、英語、フランス語、ロシア語、スペイン語、アラビア語
- ICANN: English, العربية, Español, Français, Русский, 中文
  - 読める言語はありますか？
  - 最近は日本語のページも増えている
- 英語が読めない？
  - (小)中学校からの英語教育
  - 第二外国語覚えてますか？
  - 「英語でよかった」と思える時　(例: Soltie)
  - 読み書きするしかない　(機械翻訳併用で読み解くなど)

日本語のDNS情報

- 翻訳は二次情報
  - 日本人も読まれたいドキュメントを英語で書く (提案、論文など)
  - 日本語で書くものは世界に通用しなくていいもの
- それでも、日本語で読みたいなら
  - 運用者系: DNSOPS.JP, JANOG
  - 学会系: 情報処理学会、電子情報処理学会、ソフトウェア科学会など
  - 団体・企業: JPNIC, JPRSなど

DNSOPS.JP

- https://dnsops.jp/　日本DNSオペレーターズグループ
- 夏に一日のDNS Summer Day, Internet WeekにBoF開催
- 2017/6/28 DNS Summer Day 2017
  - 災害から考えるDNSと地域インターネットサービス
  - DNSの怪しい伝説を斬る
  - ライトニングトーク
  - BIND卒業できました？
  - 製品・サービスセッション
  - 懇親会
- 本日19時からRoom 0にてBoF開催 → 懇親会

JANOG

- https://www.janog.gr.jp/
- 日本ネットワーク・オペレーターズ・グループ
- 年に2回、ミーティングを開催
- 最近のDNS関連セッション
  - JANOG 40: DNSに関する常識の変化
  - JANOG 39: DNS権威サーバ向けのDDoS攻撃対策をした話～さくらインターネット編～
  - JANOG 38: EDNS-client-subnetってどうよ? 改めRFC7871ってどうよ
  - JANOG 38: Root DNS anycast performance in South Asia & Japan
  - JANOG 37.5: DNS-OARCワークショップ報告 (Root Zone ZSKサイズの変更)
  - JANOG 37: DNS-OARC 2015 注目トピック
  - JANOG 36: GSLBをやってみた ～Designate&PowerDNS～
  - JANOG 36: [LT] Yeti DNS Projects

団体・企業: JPNIC, JPRSなど

- JPNIC 一般社団法人日本ネットワークインフォメーションセンター
  - www.nic.ad.jp → インターネットの技術: IETF, RFC, DNS解説など
    https://www.nic.ad.jp/ja/tech/
  - www.nic.ad.jp → メールマガジン一覧: IETF報告など
    https://www.nic.ad.jp/ja/mailmagazine/backnumber/
- JPRS 株式会社日本レジストリサービス
  - https://jprs.jp/

    DNS関連技術情報, ドメイン名関連会議報告, ドメイン名やDNSの解説, メールマガジン「FROM JPRS」
  - 宣伝になるので書きたくないですが、部屋の外にブースがあります

DNS-OARC Workshop (OARC27) 報告

DNS-OARC Workshop

- OARC 27
  - 2017/9/29, 30 にサンノゼで開催
  - 176人の参加者
    - シリコンバレーの中心なので、参加者が多い
    - ICANNから9, Verisignから10

OARC 27のトピック

- Root KSK Rollover
  - 詳細は省略
  - 2017/9/28：延期の第一報 (dns-operations mailing list)
  - 2017/9/29 0940- VerisignのDuane Wessels氏より、RFC 8145トラストアンカーシグナリングの評価結果が発表され、5%のアドレスが古いトラストアンカーのみであることが報告された
  - 2017/9/29 1800- ICANNのMatt Larson氏より、ICANNでもVerisignからと他のルートサーバのデータを用い、Verisignと同じ評価をして延期を決めたと発表
  - 2017/9/30 1200- ICANNのEdward Lewis氏より、問題点の報告の仕方についての問いかけが行われた (KSK Rolloverと関係か？)

OARC 27 (2)

- RIPE NCCのDaniel Karrenberg氏より、DNS Priming Queries 2017と題してK-rootへ”.” NSクエリを大量に送るアドレスがあることが報告された
  - select * from dns where qname='.' and qtype=2 and dst_port=53;
  - 平均で1時間に1クエリ以上をHyper Activeとして調査
  - 送信元に質問: “What is happening? **Are you under attack?**”
  - キャッシュしたくないのでUnboundのキャッシュを無効しようとcache-min-ttl: 0, cache-max-ttl: 0, rrset-cache-size:0, msg-cache-size: 0
  - すると “.” NS クエリを多数送るようになるとのこと

OARC 27 (3)

- (DNSの)キャッシュヒット率
  - Nominumが収集している多くのフルリゾルバのデータをもとに調査
  - クエリ数が多いほどキャッシュヒット率が高く、忙しいと90%
  - Akamaiのakadns.netはNODATAのときにSOAを追加しないのでネガティブキャッシュが有効に働かないと指摘された

    → Akamaiの人が直すとコメントし、次の営業日に修正された
- BIND 9.12.0でのリファクタリングと性能向上
  - 複雑で巨大な関数を小さく分割して読みやすくした
  - ネームサーバ本体をlibnsというライブラリにしてunittest

IETFでの情報収集と
IETF 100報告

IETFの標準化との付き合い方

- プロトコルに不満のあるひと
  - IETFに参加してください
  - 例: ゾーン頂点にCNAME書きたいひと (http://example.com をCDN)
- DNSを運用するひと
  - RFCが発行され、ソフトウェアに実装されてからで十分
  - Standards, Best Current Practiceを読むこと、他は著者・内容次第
- 最近発行されたRFC
  - 従来の標準の明確化: 用語集やプライミング → 参考に
  - 性能向上, Root KSK Rollover関連 → ソフトウェアのバージョンアップで対応
  - DNSSEC設定・運用を容易にするもの → 仕組みを作る必要あり
  - プライバシー(情報漏洩の最小化や暗号化) → バージョンアップと設定変更

2017年発行のRFC (1)

- RFC 8078, Managing DS Records from the Parent via CDS/CDNSKEY
  - 2017/3/10発行, dnsop WG, Proposed standard
  - DNSオペレータが、レジストラ・レジストリを通さずにDS設定するプロトコル
  - RFC 7344にDS新規追加と、DS削除を追加
  - 新規追加の場合は、別チャネル(登録者へのメールなど)での認証してもよいし、無条件に信用してもよい
- RFC 8109, Initializing a DNS Resolver with Priming Queries
  - 2017/3/15発行, dnsop WG, Best current practice
  - リゾルバがRoot DNSサーバの情報をアップデートする動作について定めたもの (従来から実装されている動作を明確に記述)

2017年発行のRFC (2)

- RFC 8145, Signaling Trust Anchor Knowledge in DNSSEC
  - 2017/4/11発行, dnsop WG, Proposed standard
  - DNSSEC ValidatorがTrust anchorのkeytagを権威サーバに送信
  - Root KSK Rolloverの進捗を調べることが目的
- RFC 8162, Using Secure DNS to Associate Certificates with Domain Names for S/MIME
  - 2017/5/31発行, dane WG, Experimental → 使ってもよい
  - S/MIMEの個人証明書をDNSに登録
  - hex(head28byte(sha256(localpart)))._smimecert.domain IN SMIMEA CertUsage Selector MatchingType 証明書ハッシュなど

2017年発行のRFC (3)

- RFC 8198 Aggressive use of DNSSEC-validated cache
  - 2017/7/25発行, dnsop WG, Proposed Standard
  - DNSSECでは、名前エラーに名前不存在の範囲が添付
  - NSEC/NSEC3のタイプビットマップで存在するタイプを明記
  - loans. NSEC locker. NS DS(loansからlockeの間に名前が存在しない)
  - キャッシュ済のNSEC/NSEC3を利用して、フルリゾルバで名前不存在(NXDOMAIN)、タイプ不存在(NODATA)を生成
  - Google Public DNS, BIND 9.12.0, Knot Resolver 2.0で実装
- RFC 8244, Special-Use Domain Names Problem Statement
  - 2017/10/19発行, Informational
  - ドメイン名に似た識別子で使用されるTLD予約についての問題提起

IETF での情報収集

- www.ietf.org

→ Working Groups → Active Working Groups → WG名

- About: ワーキンググループの概要
  - チェア、メーリングリスト、設立趣意書、予定など
- Documents:現在議論中のドキュメント
- Meetings: 最近の会議の資料、議事録
- List Archive: メーリングリストのアーカイブ

IETF dnsop WGの近況 (1)

- https://datatracker.ietf.org/wg/dnsop/documents/
- Active Internet-Drafts
  - 標準化作業中の提案
  - 例: draft-ietf-dnsop-aname-00
- RFCs
  - dnsop WGで標準化したRFCが時系列に並んでいる
  - 最新は2017年7月発行のRFC 8198
- Related Internet-Drafts
  - WGへ提案され、WGで標準化を進めることが決まる前の提案

IETF dnsop WGの近況 (2)

- メーリングリスト
  - About: https://datatracker.ietf.org/wg/dnsop/about/
    - Mailing List: To subscribe
    - http://www.ietf.org/mailman/listinfo/dnsop
  - https://datatracker.ietf.org/wg/dnsop/archives/
- ミーティングの資料、議事録
  - https://datatracker.ietf.org/wg/dnsop/meetings/
  - Agenda
  - Minutes
  - Materials: Slides, Blue sheets (出席者リスト)

IETF dnsop WGの近況 (3)

- テーマ
  - NSEC5: NSEC3よりよい方式 → 停滞
  - RPZ: Response Policy Zones (DNS firewall) → 停滞
  - attrleaf: _label のレジストリ → 必要だが停滞
  - DNSSECアルゴリズムの更新 → 停滞: 現在はRSASHA1が必須
  - 一つのクエリで複数の応答 → 継続
  - 応答コードの拡張 → 活発
  - DNSSEC関連の要求仕様、明確化など
  - DNSプロトコルの修正 → 問題発覚ごと
  - DNS over HTTP, QUICなど → DNS over HTTP WG設立

IETF 100

- 2017/11/10 ~ 16 にシンガポールで開催

- dnsop WG: 11/13 0930-1200
- dprive WG:開催なし、有志によるサイドミーティング 1時間
- dnssd WG: 11/15 0930-1200
- doh WG: 11/16 1330-1530

IETF 100: dnsop WG

DNS運用ドキュメント作成とプロトコル標準化

- DNS用語集のアップデート (terminology-bis)
  - RFC 7719から用語を追加したが、最近は新規用語の要求が減ったため、2018/1/15にWGLCして確定しようとしている
  - 用語の追加があれば早めに出すことと、レビューの依頼
  - RFC 7719はInformationalのため、Proposed standardを目指す
- RFC 5011 トラストアンカー自動更新のセキュリティ問題
  - RFC 5011の問題で攻撃できるので、修正するもの
  - DNSサーバ実装者とICANNが対応する → バージョンアップ
- DNSエラーコードの拡張
  - DNSSEC Bogus, DNSSEC Indeterminate (不確定), Lame, Prohibited, Too Busy
  - 複数のエンコード案が提示: 一番楽しい時期

IETF 100: dnsop WG (2)

- “localhost”の再定義
  - APIやライブラリがlocalhostを特別扱いすること
  - DNSに存在しない名前で、フルサービスリゾルバはNXDOMAINを返す
- 一つの問い合わせに複数の応答を返す方法の議論
  - AとAAAAを一つのクエリで得たい、など
  - 複数の問い合わせを送る提案と、サーバが応答を追加する案
  - 現在、5つの方式が提案されている
  - 新規提案: 権威サーバが勝手に応答を追加する (MX応答のように)
    - NSEC, NSEC3を追加することでRFC 8198でNODATA, NXDOMAIN生成
  - 5つの提案の比較表 → 活発な議論、継続して議論することとなった

IETF 100: dnsop WG (3)

- クライアントからDNSSEC検証サーバのトラストアンカーを知る方法の提案
  - 特殊な名前 _is-ta-KEYTAG. を問い合わせ、トラストアンカーでなければSERVFAIL
  - KSKロールオーバーの評価のための実装案、まにあうか？
- TSIGの修正
  - RFC 2845に曖昧な点があり、脆弱性が見つかった
  - すすめる方向性、ユーザとしては新しいソフトウェアを使えばよい
- .internal TLDの提案
  - 従来通り、IETFでやるべきでないという意見が強い

IETF 100: dprive WG
DNS通信路の暗号化

- エンドノードからフルリゾルバの間の暗号化、DNS over TLSは完了し、実装も増えてきている
  - Android, iPhone, stubby(Posix, Windows, MacOS)
- 残作業として、TLSの中身の推定対策など (padding)
  - すすめることとなった
- 今後、フルリゾルバから権威サーバへの通信路の暗号化に取り組みたいと考えている人がいる
- 現在のチャーターの目標を達成した
- IETF 101でリチャーターの提案予定

IETF 100: dnssd WG

マルチキャストDNS(Avahi, Apple Bonjour)を大規模に使用する仕組み

- 主な仕様は完成し、リンク間はDiscovery Proxyが書き換えて中継する
  - 管理者がリンク名やProxyの設定を行う
  - 現在はIESGの手続き中で、IETF Last callが終わったところ
  - Hackathonで相互接続試験を行い、動作の確認を行っている
- いくつかの追加仕様が停滞中
- DNS-SD Privacyは複雑で止まりそう
- Apple社の仕様をドキュメントしている

IETF 100: doh WG: DNS over HTTP WG
DNS over HTTPの標準化

- 2017/9/15に設立
  - DNS関連WGやアプリケーション関連エリアで2年ほど議論されてきた
- draft-ietf-doh-dns-over-https-01
  - DNSワイヤフォーマットのデータをHTTPで通信
  - GETではbase64エンコード、POSTではbinaryのまま
  - GET /.well-known/dns-query
?content-type=applicaton/dns-udpwireformat
&body=q80BAAABAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAAQAB
&accept=application/dns-udpwireformat
- 議論など
  - HTTP/2とするか？
  - DNSキャッシュとHTTPキャッシュの扱い
- 問題は少ないため、すぐに決まる可能性あり

Comments ? Questions ?