IETF 103 報告　DNS関連
その他の話題など

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 103 報告会, 2018年12月14日

自己紹介

- 氏名:　　藤原和典
- 勤務先:　株式会社日本レジストリサービス (JPRS)
- 業務内容:DNS関連の研究・開発
- IETF: Active WG: dnsop,　Past WG: enum, eai
  - https://datatracker.ietf.org/person/kazunori%20fujiwara
  - 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 8499)
  - RFC 8198: DNSSECを用いた名前解決の性能向上
- その他
  - Internet Week 2018 プログラム委員
  - RSSAC Caucus
- 個人ページ: http://member.wide.ad.jp/~fujiwara/

DNS関連WG/BOF/ミーティング

- 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 → 直前キャンセル
  - ~~dane　　DNS(SEC)にTLSの証明書~~　完了
  - doh　　DNS Over HTTPS → やることは終わったので非開催
  - dnssd　　DNS-SD (RFC 6763)の拡張
  - homenet　　Home Networking
  - その他のDNS関連RFC
- Side meeting
  - Resolverless-DNS side meeting
  - KSK Rollover side meeting
- DNS関連以外
  - Fragmentation, トランスポートとPath MTU Discoveryの議論
- IETF以外
  - IEPG

概要 1

- dnsop: DNS運用ガイドライン、プロトコル修正
  - RFC発行ペースが鈍化？、2018年は1本 (RFC Editor Queueに6本)
  - serve-staleとanameは実装先行で、標準化は実装を追いかけている
- dprive: DNS通信路の暗号化
  - 初期目標であるスタブからフルリゾルバの暗号化を完了して中休み
  - フルリゾルバから権威サーバまでの暗号化を始める予定が直前キャンセル
  - 12/10にInterim meeting実施、権威サーバまでの暗号化に取り組む
- doh: DNS over HTTPS
  - 2017/9/15設立、2018年4月に完了するという目標設定だったが、2018/10/19にRFC 8484 DNS Queries over HTTPS (DoH)を発行
  - 非開催

概要 2

- dnssd: DNS-SD (RFC 6763)の拡張
  - コアプロトコルの一部(Hybrid Proxy)は完了してRFC Editor Queueに
  - プライバシー提案をまたやりなおし、今後一つの方法に注力見込み
- homenet: Home networking
  - 名前解決機能はローカルはmDNS / dnssd, それ以外はISPのフルリゾルバを使うこととなった
  - 市場に受け入れられるhomenetにするにはどうすればよいかという反省
- その他のDNS関連RFC
  - RFC 8324, 2018/2/27, John KlensinのDNS再構築と置き換えの提案
  - RFC 8427, 2018/7/23, Representing DNS Messages in JSON
  - RFC 8483, 2018/10/19, Yeti DNS Testbed 報告書

概要 3

- IETF 103ではSide meetingという形式のミーティングが開催
  - Resolverless DNS side meeting
    - システムで設定されたリゾルバ以外からDNS情報を得る仕組みの議論
  - KSK Rollover side-meeting
    - ICANNのPaul HoffmanがKSK Rolloverについての意見を集めた
  - 6man/tsvwg Path MTU Discovery Discussion side meeting
    - IPv6プロトコル開発者たちが、IPv6プロトコルの大規模な変更を楽しそうに議論していた。ヘッダの再利用とかICMPv6の追加、ルータの変更など
- IEPG meeting: DNS 2件、ルーティング 2件
  - RPKI origin validationを 1 hop で使えば十分であるとのこと

詳細

dnsop (DNS Operations) WG

- DNS運用ガイドラインを作るWG、プロトコル微修正も扱う

- 2018年に発行したRFC 1本
  - RFC 8501: Reverse DNS in IPv6 for Internet Service Providers
    - 2018/11/28発行, Informational
    - ISPが顧客に提供しているIPv6アドレスの逆引きの提供方法を示す
      - しない(不存在), Wildcard(*), 動的な登録(Update, DHCPv6), 機械的な自動生成

- RFC Editor Queneに6本 (うちAUTH48 3本)

dnsop (2)

- 発行直前のDraft (未発行でAUTH48のもの)
  - RFC 8482: draft-ietf-dnsop-refuse-any, RFC 8499待ち
    - タイプANYクエリに一つのRRSetを返すことを推奨
  - RFC 8499: DNS Terminology, AUTH48 2018/11/8
    - DNS用語集　RFC 7719の更新、RFC 2308をUpdateするため、BCP
    - ドメイン名、名前空間、内部名(in-domain, sibling) などの詳細化
  - RFC 8509, draft-ietf-dnsop-kskroll-sentinel-17, AUTH48 2018/12/13
    - DNSSEC Validatorのトラストアンカーを、クライアントから知る方法
    - root-key-sentinel-is-ta-<key-tag>.<dom> A/AAAA
      - domドメイン名のトラストアンカーとしてkey-tagを設定しているときにこのクエリを受けとると設定してあるA/AAAAを返し、違う場合はSERVFAIL
    - root-key-sentinel-not-ta-<key-tag>.<dom> A/AAAA
      - トラストアンカーとしてkey-tagを設定していないときにこのクエリを受けとると設定してあるA/AAAAを返し、違う場合はSERVFAIL

dnsop (3)

- RFC Editor’s Queue (IESGに発行承認済)
  - draft-ietf-dnsop-attrleaf-16, 2018/11/26
  - draft-ietf-dnsop-attrleaf-fix-07, 2018/11/26
    - prefixed name _label のレジストリを作るもの

      タイプ　ラベル名　定義しているRFC

      例: TXT　_dmarc　RFC7489
  - draft-ietf-dnsop-session-signal, 2018/12/7
    - dnssd WGで使用するstateful operation
    - 新しい OPCODE (6), 新しいTLV(type-length-value)データ形式
    - DNS over TCP (TLS)通信路で、つなぎっぱなしで、サーバ側からもデータを送り付けることができる仕組み
    - IESG Reviewで大規模なDISCUSSをつけられていたが、12/7に発行承認

dnsop (4)

- IESGでレビュー中
  - draft-ietf-dnsop-dns-capture-format
    - CBORデータフォーマットを用い、Query/Responseの組を効率よく蓄積するデータ形式
    - IESGからは多くの微修正を求められている
    - 12/12 更新版の-10が出たため、IANA Review後に発行承認の見込み

dnsop (5)

- IETF 103 dnsop WG で議論が行われたもの
  - draft-ietf-dnsop-serve-stale → dnsop (6)
  - draft-ietf-dnsop-aname → dnsop (7)
  - draft-ietf-dnsop-rfc7816bis: QNAME minimization: EXP→STD進める
  - draft-ietf-dnsop-7706bis: Local root
    - Resolverにroot zoneを直接与えることも含むという意見があった。他の方法があるという意見もあった。規模などの議論あり、継続
    - ICANN用語では Hyper local (root)
  - draft-mayrhofer-did-dns
    - Decentralized Identifier (W3C-DID) をDNSに載せる提案、紹介のみ
  - draft-hoffman-dns-special-labels: IANAに特殊なラベルのレジストリ
    - “.” “xn--, “_ラベル”, “root-key-sentinel-*”　　重要だが退屈な仕事というコメント
  - draft-lhotka-dnsop-iana-class-type-yang: YANG type, YANG class
    - YANGで定義されることでサーバー設定APIなどを作りやすくなると期待

dnsop (6)

- draft-ietf-dnsop-serve-stale-02
  - 権威サーバが応答しない時にキャッシュに存在した古い(stale)データを応答
    - DoS時などに権威サーバから応答が得られず、応答を返せないよりは、古い、期限切れのものでも応答があるほうがましという考え
    - Akamai, Unbound, Knot Resolver, BIND 9, Resolver serviceなどで実装されているが、細かい動作が異なる
    - 現在、推奨するTTL値などが未定、draftには細かいところが書かれていない
    - 提案: 古い応答を返すまでの時間1.8秒、TTL値を30、一週間までのデータを返す
  - ミーティング時には、総論賛成、細かいところにコメント
    - iOS 12に似た機能を実装したとのこと
    - Stale状況をEDNSオプションで応答する部分やTTL値、タイマーなどで議論
  - 継続: 実装が広まっているので時間はかかるが標準化される見込み

dnsop (7)

- draft-ietf-dnsop-aname
  - ゾーン頂点にCNAMEを書いてCDNに向けたいという要求
    - ゾーン頂点には NS, SOAがあるのでCNAMEを書けない
  - ゾーン頂点にA/AAAA RRの別名を定義できるANAME RRを定義
    - example.com IN ANAME example.com.CDN.example.net.
    - もともとの提案は権威サーバがANAME先を名前解決してA/AAAA返す
    - CDN事業者が提供する権威サーバではこの機能をすでに提供している(ALIAS RR)
    - 現在は、DNS Updateで登録することも考えられている
  - IETF 103での議論
    - CNAME + DNAME を委任の代わりに書くと大体うごく → 普通のドメイン名は委任のみ
    - “_https._tcp.ドメイン名”にSRVを書き、ブラウザはそれを使うことにすれば解決するが、ワイルドカードドメイン名を使えない（ _https._tcp.*.example.com は不可能)
    - ブラウザベンダーはSRV方式を嫌っている
  - 結論: 解決しないといけない問題であるため、議論を継続

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暗号化するプロトコルを策定するWG
- スタブリゾルバとフルリゾルバの間については完了
  - RFC 7858, 2016/5, DNS over TLS
  - RFC 8310, 2018/3/21, Usage Profiles for DNS over TLS and DNS over DTLS
    - DNS over TLSの使い方についてのドキュメント
    - Opportunistic, Strict
  - RFC 8467, 2018/10/12, Padding Policies for Extension Mechanisms for DNS (EDNS(0))
    - TLS通信を見て中身を推定されないようにPaddingする場合のやりかた
    - Maximum-length, random-length, random-block-length

dprive WG (2)

- 今後、フルリゾルバと権威サーバの間の通信の暗号化の議論を進めることになっていた
- IETF 103では、直前キャンセル
- 12/10 1600-1800 (UTC)にInterim meeting
  - 11/27に召集 → short noticeだという不満など
  - 招集後にIETF 103のキャンセル理由の説明があり、論点整理などが終わっていなかったためとのこと
  - 12/8に示されたDPRIVE Phase 2 Milestones and Requirements
    - https://trac.ietf.org/trac/dprive/wiki/DPriveStage2
    - 関連するプロトコルとして、Confidential DNS と DNSCurve
    - ユーザ、オペレータ、実装者それぞれの視点でのユースケースなど

dprive WG (3)

- 12/10 1600-1740 (UTC): Interim meeting (WebEx)
  - 20名ほどが参加
  - DPRIVE Phase 2 Milestones and Requirements の解説と質疑
  - 議論
    - Resolverは順に多くの権威サーバにTLSで接続すると時間がかかること
    - TLSではないプロトコルを考慮してもよいこと
    - DNS over TLSのシグナリングをするかしないか
    - DNSCurveのようなネームサーバ名に意味を持たせるなどの案
    - サーバ証明書をどうするか？ TLSAか？
  - 結論: 問題点をまとめて、進める (draftを書くこと)

doh WG: DNS Over HTTPS WG

- DNS over HTTPS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 DNS over HTTPS を標準化する
- 目標: 2018年4月にDNS over HTTPSの仕様をIESGに提出
- 2018/10/19にRFC 8484 DNS Queries over HTTPSを発行 → 非開催
  - DNSワイヤフォーマットのデータをHTTPSで通信
  - GETではbase64エンコード、POSTではbinaryのまま

    :method = GET
    :scheme = https
    :authority = dnsserver.example.net
    :path = /dns-query?dns=AAABAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAAQAB
    :accept = application/dns-message

dnssd WG (1)

- 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
  - Multicast DNS (RFC 6762), 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
  - 一言でいえば、Apple社のOSでのプリンタなどの発見を複数セグメントに拡張するもので、機器の一覧として大学や企業全体の機材を選べるようにするもの
- 現在の状況 (コアプロトコルはできた、プライバシーを作りたい)
  - コアプロトコル Discovery Proxy for Multicast DNS-Based Service Discovery (draft-ietf-dnssd-hybrid-08) が発行承認され、RFC Editor Queue で、draft-ietf-dnsop-session-signal を待っている状態
    - Normative referenceとしてしまったことが問題
    - Appleはすでに実装しているとのこと

dnssd WG (2)

- IETF 103での議論
  - 実装報告: Discovery proxy + DNS Pushを実装している
    - Github, apple.comなどで公開、IETF Hackathonへ参加してほしいとのこと
  - mDNS Privacy
    - 現在のMulticast DNSでは、すべての機器の名前とアドレスが見える
      - 無条件でMulticastに答えるし、名前を聞かれたら答える
    - 個人のデバイスは、持ち主だけが見えるようにしたい
    - ここ2年ほど議論が続いているが進展なし
    - 共有鍵とかグループ内の公開鍵などでmDNSメッセージを暗号化するという複数案が示されたが、どの方法も欠点あり
    - WiFiはmulticastが苦手なので、個人の端末情報も(なんらかの方法で)暗号化してサーバに登録し、解読方法を知っている端末だけが名前解決できる方法を進めることになった
    - draft-ietf-dnssd-privacyが更新される見込み

homenet WG (1)

- Home Networking
- (2代前のIETF Chair、Jari Arkko氏の)家のネットワーク

- 現状
  - Homenet Control Protocol (RFC 7788), ルーティング (Babel) などは決まった
  - 名前解決まわりがまだ複雑だったので simple naming提案

homenet WG (2)

- IETF 103での議論
  - Homenet Naming Architecture
    - draft-ietf-home-simple-naming
    - ローカルはmDNS / dnssd, それ以外はISPのフルリゾルバを使う
    - mif WG/intareaのPvDの考慮あり
    - 複数のISP契約がある場合に対応できないという強い指摘があった
  - Market Resistance to Homenet
    - 市場に受け入れられるhomenetにするにはどうすればよいか
    - 複雑なhomenetにしなくても、L2で組めばいいんじゃないか
    - 使えないものを作ってしまったんじゃないかという反省

その他のDNS関連RFC (1)

- RFC 8427, 2018/7/23, Representing DNS Messages in JSON
  - JSONでDNSメッセージを表現する方法を規定
  - Individual submission
  - DNS over HTTPSの部分は規定していない
  - RDATAは16進で、使いにくい
    - { "NAME": "example.com.","TYPE": 1, "CLASS": 1,"TTL": 3600,"RDATAHEX": "C000AA01" }
  - Google Public DNSのJSONは違う (独自方式)
    - curl https://dns.google.com/resolve?name=internetweek.jp

    → {"Status": 0,"TC": false,"RD": true,"RA": true,"AD": true,"CD": false,"Question":[{"name": "internetweek.jp.","type": 1}],"Answer":[{"name": "internetweek.jp.","type": 1,"TTL": 286,"data": "192.41.192.146"}]}

その他のDNS関連RFC (2)

- RFC 8324, 2018/2/27, DNS Privacy, Authorization, Special Uses, Encoding, Characters, Matching, and Root Structure: Time for Another Look
  - John Klensinからの、DNSの再構築と置き換えの提案
- RFC 8483, 2018/10/19, Yeti DNS Testbed
  - Yeti Projectの報告書
  - 著者は、BIIの人たち、WIDEの加藤さん、Paul Vixie、Shane Kerr
  - Yeti rootは実験用のAlternate root (IPv6のroot serverを21)
  - IANA Root zoneからDNSKEY/RRSIG/ルートサーバ情報を削除して、Yeti RootのNS, AAAAを追加、Yeti Root DNSKEYで署名

Resolverless-DNS side meeting

- IETF 103では、Side meetingという非公式なミーティングが開催
  - 中継なし、資料置き場なし、minutesなし？
- resolverless-dns@ietf.org　WGではないメーリングリストあり
  - Handling of DNS information obtained from sources other than configured resolvers
  - システムで設定されたリゾルバ以外からDNS情報を得る仕組みの議論
  - ブラウザでのページロード時間を短くしたいという目的で、HTTPSでDNS情報を事前に送り付けて名前解決時間を短くしたい
  - DNSSECの署名検証に必要なデータすべてを送られれば信用できる
    - rootからのDS, DNSKEY, 目的のRRSetとそれらのRRSIG一式
  - CDNの負荷分散/EDNS Client Subnetとの兼ね合い、プライバシーとの兼ね合い、Happy Eyeballなどが議論された

KSK Rollover side-meeting

- ICANNのPaul Hoffmanがコミュニティからの意見を集める場として開催
- https://mm.icann.org/mailman/listinfo/ksk-rollover
  - ksk-rollover@icann.org
- 発言したい人が意見を述べるのみ
  - KSK Rollverの必要性の質問には、HSMとの答え
  - 頻繁なRollverの提案 (年1度程度)
  - アルゴリズムの変更提案
  - 各種調査の必要性
  - ブラウザはみんな自動更新にしているのになぜDNSSEC validatorは自動更新にしない人がいるのかという問いかけ
  - リゾルバオペレータとやりとりするチャネルの話
  - …

DNS以外

draft-ietf-intarea-frag-fragile-02

- IP Fragmentation Considered Fragile
  - Author: Ron Bonica, Fred Baker, Geoff Huston, Bob Hinden, Ole Troan, Fernando Gont
  - Fragmentすると上位のプロトコルヘッダがみえないため、stateless middle boxesは扱えない (stateful inspectionする高価な機器は大丈夫)
  - Recommendation
    - アプリケーションはFragmentationに依存するべきではない
    - Middle boxはFragmentation対応のstatefulな処理を行うこと
    - (もともとFragmentationを捨てようという主張だったのに、弱い、IETFではありがち)
  - IETF 103での議論
    - UDP Fragmentationの紹介 → IP Fragmentationいらなくなって幸せ
    - Path MTU Discoveryの議論
    - TCPでもFragmentationすることがあるので、MSSの調整などが必要
    - POSIXなどのインターフェースを拡張して制御したい
  - DNSの話題なし: DNSでもFragmentionは危険 (second fragment attack)

IPv6でのFragmentation (1)

- draft-troan-6man-pmtu-solution-space
  - Path MTU discovery improvements at the network layer?
  - ICMPv6 Packet Too Big (PTB)がフィルタされてしまうため、Path MTU Discoveryがうまく動かない
  - 改善案
    - #1 Path MTU Discoveryをトランスポート層に組み込む (RFC 4821など)
    - #2 なにもしない
    - #3 In-Path fragmentation …. IPv4のように経路上でfragmention ルータ変更
    - #4 固定MTU 1280
    - #5 Truncation … 経路上のルータでは切り詰めてTC=1で送る　　ルータ変更
    - #6 Recording … MTUを記録する新しいICMPv6を定義　　ルータ変更
  - 6man: 議論が必要、継続
  - tsvwg: 議論は盛り上がるが結論出ず、TCP MSS clampingは必要

IPv6でのFragmentation (2)

- 6man/tsvwg Path MTU Discovery Discussion side meeting
  - 提案者は Bob Hinden (IPv6/Path MTU Discovery v6 RFC Author)
  - 金曜日 1000-1200 2時間、15人ほど、広い部屋の一番前だけ
  - 6manとtsvwgの重鎮たちがv6の仕様を変更する気まんまんな議論
    - IPv6のことしか考えていない人たち
    - v6ヘッダの再利用しようぜ！
    - ルータ変えようぜ！ (ICMPv6での記録, Truncation, In-path fragment)
    - プロトコル変えてもIncremental Deploymentできるから大丈夫！
  - おもしろかったのでずっと聞いていたら最後に何かいえといわれ、つい、「いまさらルータを変えるのはよくないと思う」と言ってしまった

IEPG (1)

- IEPGは、IETFの日曜日の非公式な集まり
  - www.iepg.org
  - ルーティング 2件、DNS 2件
- How Stuff Works: DNS Upstream Server Selection
  - Benno Overeinder, NLNet Labs
  - Unboundのサーバ選択アルゴリズムの紹介
- Measuring the KSK Roller Derby
  - Geoff Huston, APNIC
  - KSK Rolloverでの鍵の切り替わりの報告
- Weaponizing BGP Using Communities, Randy Bush, IIJ
  - BGP Communityは強力なので、注意深く使うこと
- Routing Security Roadmap, Job Snijders, NTT Communications

IEPG (2)

- Routing Security Roadmap
  - Job Snijders, NTT Communications
  - 今後のRouting Security
  - RPKI origin validationは、BGPSEC Path Validationがないと使えない

  → Densely peer with each other

  大手事業者は同じところに機材を置いているからできる

  path validation for 1 hop

  Perhaps “1 hop” already is good enough

  # ということは全ASがフルメッシュでpeerしてRPKIすればいい？

Questions and comments ?