前回の報告と同じ内容の部分

IETF 98 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 98 報告会, 2017年5月12日
Last update: 2017/5/12 1322 JST

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 → terminology-bis
    - draft-ietf-dnsop-nsec-aggressiveuse (2015/3~)
    - draft-fujiwara-dnsop-resolver-update (2016/10~)
- 個人的なIETF 98結果
  - 共著者による報告1件, chairによる報告1件

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 → 非開催
  - dane　　DNS(SEC)にTLSの証明書 → 非開催
  - dnssd　　DNS-SD (RFC 6763)の拡張
  - homenet　　Home Networking

- IETF以外
  - IEPG

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を多数発行中 (IETF 97から4、IESGに1)
  - 多数の提案の議論が進められた
- dprive: DNS通信路の暗号化
  - 目標をほぼ完了したため、非開催
    - IETF 99で開催予定 (おそらく目標の再設定)
  - RFC 8094 DNS over DTLS発行
- dane: DNS(SEC)にTLSの証明書
  - 目標をほぼ完了したため、非開催
  - 残件: SMIMEAがIESGに提出、3/20に発行承認
  - 2017/3/21に完了 (Conclusion)

概要 2

- dnssd: DNS-SD (RFC 6763)の拡張
  - 順調に標準化作業が進展中
  - 今後の標準化テーマとして、Apple社で実装しているプロトコルが紹介
  - プライバシー提案の議論
- homenet: Home networking
  - 名前解決機能の提案が大規模に変更され、dnssd WGベースの簡易なものになった
  - .home → .homenet → .home.arpa

概要 3

- dbound: Domain Boundaries
  - Public Suffix Listの後継を作ろうとしていたWG
  - 2017/4/24 合意を形成できず、closed
  - "DBOUND WG failed to reach consensus on any specific proposal(s) to express domain relationships in DNS. The WG is thus being closed."
- IEPG: 運用に関する話題を扱うinformalな集まり
  - サーバ証明書(Let's Encrypt), DNS, BGP, IPv6の4件の発表が行なわれた

DNS関連WGの今後

- 特定のプロトコルを作成するためのWGは、目標を達成すると完了して閉じる
  - dane WGは完了 (Conclusion)
  - dprive WGは新しい目標を設定する見込み
    - 権威サーバへのクエリの暗号化
  - dboundは目標に進めず、閉鎖 (closed)
  - dnssdは進展中 (残件多数)
- dnsop WGの目標は今後発生する問題を含むため、完了しない
  - DNSの運用にかかわる問題 (現在及び将来)
  - DNSに関する問題を議論する場
    - Charter: "Serve as a home for drafts that document the problem space around existing or new DNS issues"

詳細

前回の報告と同じ内容の部分

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
  - https://tools.ietf.org/wg/dnsop/
- 振り返り: IETF 95
  - 新規: DNS over HTTP, delegation requirements, dnssec-algorithm-update, class-useless, aaaa-for-free, black-lies
- 振り返り: IETF 96
  - 継続: terminology-bis, nsec-aggressiveuse, TLD予約新規提案
  - 新規: session-signal, bulk-rr, 一つのリクエストで複数クエリ・応答
- 振り返り: IETF 97
  - 継続: terminology-bis, session-signal
  - 新規: ipv4only.arpa, dns-delegation-requirements, dns-capture-format, resolver-update, transferring-automated-dnssec-zones, ccompanying-questions, dns-catalog-zones, deploying-dnssec-crypto-algs

dnsop (2)

- 着実にRFCを発行 (draft-ietf-dnsop-を省略)
  - 2016/11/28 RFC 8027 roadblock-avoidance
  - 2017/3/10 RFC 8078 maintain-ds
  - 2017/3/15 RFC 8109 resolver-priming
  - 2017/4/11 RFC 8145 edns-key-tag
- IESGでレビュー中
  - 2017/3/2 draft-ietf-dnsop-nsec-aggressiveuse IESG提出
  - 2017/4/10 draft-ietf-dnsop-sutld-ps-03 IESG提出
- 関連RFC
  - 2017/2/14 RFC 8080 Edwards-Curve Digital Security Algorithm (EdDSA) for DNSSEC

dnsop (3)

- RFC 8027, BCP 207, 2016/11/28発行
  - draft-ietf-dnsop-dnssec-roadblock-avoidance
  - Best Current Practice
  - “Host Validator”がDNSSEC検証できるかどうかを判定する
  - ホテルのネットワークやmiddle boxの悪影響を避ける目的
  - 2014/3/7 dnsop WG draft 00
  - 2016/5/26 IESG提出、9/7 IESG通過

dnsop (4)

- RFC 8078, 2017/3/10発行
  - draft-ietf-dnsop-maintain-ds
  - RFC 7344 CDS/CDNSKEYをInformationalからStandards trackに変更
    - DNSSEC設定を、レジストリを通さずに行う提案
  - DS新規追加と、DS削除を追加
    - DNSオペレータが、レジストラ・レジストリを通さずにDNSSECのDS設定をしたいという要求より
  - 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
  - 2016/6/21 IESG提出
  - 2016/9/28 IESG Evaluation - Defer　延期
    - RFC 7344をStandards trackに変更する手続きの問題
  - 2017/1/9 RFC Editorに送付

dnsop (5)

- RFC 8109, 2017/3/15発行
  - draft-ietf-dnsop-resolver-priming
  - 2016/8/4-8/19 WGLC
  - 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たこと)
  - WGLCコメントでSecurity Considerationにon-path attackerからの攻撃について追記(DNSSECで防御)
  - 2016/9/18 IESG提出
  - 2016/12/8 Approved-announcement to be sent::Point Raised - writeup needed
    IESGからの指摘を反映したら承認するという状態
  - 2016/12/23, 24に更新
  - 2017/1/30にIESGが発行承認、RFC Editorへ

dnsop (6)

- RFC 8145, 2017/4/11発行
  - draft-ietf-edns-key-tag
  - DNSSEC 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Trust anchorのロールオーバーの進捗を調べることが目的
  - 2016/12/14にIESGに提出
  - 2017/2/21に発行承認、RFC Editorへ

dnsop (7)

- RFC 8080, 2017/2/14発行
  - Edwards-Curve Digital Security Algorithm (EdDSA) for DNSSEC
  - curdle WGで標準化したもの
    - CURves, Deprecating and a Little more Encryption
    - IRTF CFRG (Crypto Forum Research Group)が作った暗号をIETFの標準プロトコルに組み込み、古い暗号を廃止するWG
    - DNSSEC, PKI, SSH, XML, JSONなどを対象
  - エドワーズ曲線デジタル署名アルゴリズムの二つ、Ed25519とEd448を用いたDNSSECの署名アルゴリズム(15,16)を定義
    - Ed25519はDaniel Julius Bernstein教授らが開発したため、政府の関与がない (⇔ECDSAはNIST.GOVが開発)
    - Ed448はMike Hamburg氏
  - RSAよりも鍵長と署名長が小さいことが期待される

dnsop (8)

- draft-ietf-dnsop-nsec-aggressiveuse
  - DNSSECでは、名前エラーに名前不存在の範囲が添付
  - 例: rootにfoo.localクエリを送ると
    - loans. IN NSEC locker. NS DS …
    - loansからlockerの間に名前が存在しない
  - キャッシュ済の不存在証明(DNSSEC)を利用してフルリゾルバで名前不存在を生成するという提案
  - draft-wkumari-dnsop-cheese-shop をマージ
    - ルートサーバからの応答に限定
  - 著者にWarren Kumari氏を追加
    - Native speaker, 有識者(対抗ドラフトの著者)
  - Google Public DNSで、rootに適用した結果を発表
    - Googleではもうonにしたらしい
  - 2017/3/2にIESGに提出, 3/13~3/27 IETF Last Call
  - 2017/5/25 IESG TelechatのAgendaに

dnsop (9)

- draft-ietf-dnsop-sutld-ps-03
  - Special-Use Domain Names Problem Statement
  - 2014年ごろから議論されているプロトコルで使用するTLDを予約することについての問題提起
  - 2017/4/10にIESGに提出

dnsop (10)

- IETF 98ミーティングの概要
  - IETF 97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。
  - Chairからの報告
    - nsec-aggressiveuse: IESGに提出、IETF Last Call Ends
    - edns-key-tag: RFC Editor queue
  - 継続提案 current working group business
    - terminology-bis
    - dns-capture-format
    - attrleaf
    - bulk-rr
    - DNSSEC Algorithm Updates
  - 新規提案 new working group business
    - nsec5
    - dns-tcp-requirements

dnsop (11)

- draft-ietf-dnsop-terminology-bis
  - RFC 7719 DNS Terminology のアップデート
  - 新規用語の収集と、用語定義の変更
  - draft-ietf-dnsop-terminology-bis-05
    - 新規用語の収集: Wildcard, DNSSECなどの用語
    - Domain name の定義の変更
      - ドメイン名予約の議論を受け、DNS以外も含む
      - Label: 0文字以上のバイト列でドメイン名の一部
      - Domain name: 1以上のラベルから構成される順序つきリスト
      - 従来の定義はGlobal DNSのドメイン名に移動
      - ミーティングではコメントなし、新規用語提案だけ

dnsop (12)

- draft-vcelak-nsec5: NSEC5, DNSSEC Authenticated Denial of Existence
  - NSEC: 名前が存在する範囲で不存在証明
  - NSEC3: ドメイン名のハッシュの範囲で不存在証明
    - NSEC3ではゾーン情報を収集できてしまうという主張があり、時々改善の提案が行なわれている
  - NSEC5 = NSEC3のSHA1のかわりに、Verifiable Random Function (VRF)を用いる提案
    - VRFはECDSAベースのHashの一つで、Hash作成用とVerify用の二つのKeyを用いるため、解読されないというもの(draft-goldbe-vrf-00)
  - 必要性への疑問(NSEC3で十分である)、実装や普及コストなどの問題がコメントされた
    - ドメイン名は公開情報である
    - 多くのTLDでリスト公開 (com, net, se, nu, 新gTLD)

dnsop (13)

- draft-ietf-dnsop-dns-capture-format
  - C-DNS: A DNS Packet Capture Format
  - CBOR形式でDNS packet capture dataを保存する
    - RFC 7049 Concise Binary Object Representation (CBOR)
    - 同じものをreferenceに変換するため、pcap formatより小さい
  - IETF 97後にWG itemとなった
    - 2016/12/6: draft-ietf-dnsop-dns-capture-format
  - 現状の発表が行なわれ、サポートするコメント複数

dnsop (14)

- draft-ietf-dnsop-attrleaf
  - "_プロトコル名" のレジストリを作る提案
  - SRVやTLSA, OpenPGPKEYなどで使用
    - _sip, _443, _25, _opengpkey, _smimecert
  - RFC 2782 SRV標準化当時はIANAレジストリが必要ではなかったが、現在は多くのプロトコルが使用するようになったため、レジストリが必要になったという背景がコメントされた

dnsop (15)

- draft-woodworth-bulk-rr
  - $GENERATEの一般化のような提案で、権威DNSサーバで正規表現もどきを使って応答を作成する提案
  - 例: *.55.10.in-addr.arpa. 86400 IN BULK PTR ([0-255].[0-255].55.10.in-addr.arpa. pool-A-${1}-${2}.example.com.)
    - 逆引きの自動生成で、x.y.55.10.in-addr.arpa PTRクエリに対してpool-A-x-y.example.com を返す
  - 会場からのコメント
    - Knot DNSには同じ機能があるので好みであるとか
    - 複雑すぎるというコメントがあった

dnsop (16)

- DNSSEC署名アルゴリズムの更新
  - draft-wouters-sury-dnsop-algorithm-update
  - draft-arends-dnsop-dnssec-algorithm-update
  - 従来は必須だったRSASHA1の優先順位を落とし、RSASHA256を必須にするという提案
  - EdDSA, ECDSAなどを普及させたい意見もあり
  - Best Current PracticeのRFCとする方向へ進みそうである

dnsop (17)

- draft-kristoff-dnsop-dns-tcp-requirements
  - DNS Transport over TCP - Operational Requirements
  - TCP通信路を用いたDNSを普及させる提案
    - RFC 7766では不足という主張
  - サポートする人はいる

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
  - IETF 95: 完了が見え、1時間と短め
    - RFC 7858 DNS over TLS発行 → 使用可能に
  - IETF 97: 使い方と、WGの今後の議論
- IETF 98では非開催
  - 初期の目標を完了
  - IETF 99では開催予定 (目標の再設定の議論?)

dprive (2)

- RFC 8094, 2017/2/28発行
  - 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
  - 2016/8/16に提出された-10で、Standards trackからExperimentalに変更 (実装がないため)
  - 2016/10/5 IESGに提出
  - 2016/12/12 IESG投票中

dprive (3)

- draft-ietf-dprive-dtls-and-tls-profiles
  - DNS over TLSの使い方についてのドキュメント
  - opportunistic(日和見)が失敗した場合の議論
  - 端末からフルリゾルバの実装に必要なものを示すこと
  - 2017/1/24にIESGに提出、2/16-3/2 IETF Last Call
- draft-ietf-dprive-padding-policy
  - EDNS0 paddingの使い方の提案で、クエリ名長などを推定しにくくするもの
  - 実装のためには研究などが必要である
  - 強いサポートあり
  - 2016/12/5にWG draftになった

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
  - RFC 7929 OPENPGPKEY, 2016/8/5発行
  - 残件: SMIMEA 2017/4/29 AUTH48/発行直前
- IETF 94, IETF 95, IETF 96, IETF 97: ミーティング非開催
- 2017/3/21完了(Conclusion)

dane (2)

- 残るドキュメント: draft-ietf-dane-smime
  - 2016/7/9-25 WGLC (-11 → -12)
  - OPENPGPKEYのIESG Reviewを受け、SMIMEも同じように変更
    - 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
    - アスキーの大文字小文字などのVariantは別の所有者名
  - 2017/3/20 RFC発行承認 (RFC Editor queue)
  - 2017/4/29 AUTH48 (著者の承認待ち) RFC 8162

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: Hybrid Proxy
  - IETF 92: LLQの代わりに Update
  - IETF 93: 基本的には継続した議論
  - IETF 94: 継続した議論だが若干減速気味
  - IETF 95: Hybrid Proxy未更新、Privacy, Push
  - IETF 96: Hybrid Proxy未更新、Privacy, Push
  - IETF 97: Hybrid Proxy更新、名前変更、Privacy, Push

dnssd (2)

- dnssdプロトコルの利用イメージ
  - 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
  - 印刷しようとするとプリンタの一覧が表示され、プリンタを選んで印刷できるが、そのときに大学や企業全体のプリンタを選べるようになる
- dnssdコアプロトコルの実装状況
  - Apple社のOSにはすでに実装されているとのこと

dnssd (3)

- IETF 98での議論
  - コアプロトコル (Discovery Proxy)はほぼ完了
  - Push Notification: WGLC完了、コメント反映前
  - Apple社で実装している多数のProxyの紹介と、標準化の提案
  - プライバシー拡張
  - 大学や大規模な企業への展開
  - Stateful Multi-Link DNS Service Discovery
    - IoT向けの機能拡張提案 (core WG関係)

dnssd (4)

- draft-ietf-dnssd-hybrid (dnssdのコアプロトコル)
  - Discovery Proxy and Advertising proxy
  - WGでは合意完了、IESGに提出する準備を行う
- draft-ietf-dnssd-push: 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
  - 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
  - Session定義をdnsopに委任: draft-ietf-dnsop-session
  - WGLC完了: WGLCコメントを反映するように指示

dnssd (5)

- Apple社実装済みプロトコルの紹介と、標準化提案
  - DNS-SD Roadmap
    - 10枚目　https://www.ietf.org/proceedings/98/slides/slides-98-dnssd-dns-sd-next-steps-00.pdf
  - Advertising Proxy
    - 6LoWPANなどでnon-local deviceの名前解決をサポート
  - Sleep Proxy
    - DNS Updateで登録して、寝ている機器がアクセスされたらWake up on LAN magic packetで起こす (Apple TVなど？)
  - Discovery Broker
    - 複数のdiscovery proxyにつないで名前解決を行う
  - Zone Stitching
    - 複数のリンク間の名前が重ならないようにする機構
  - いくつかのプロトコルに興味を持つ人がいたため、Internet-Draftとして提案することとなった

dnssd (6)

- draft-ietf-dnssd-privacy-01, Privacy Extensions for DNS-SD
  - プライバシー保護のために、許可したペア間だけで名前解決できる提案
  - 2016/10/27: WG draftに
  - 前回(00)より簡素化された提案
  - <nonce>:32bit時刻の上位24ビット:256秒ごとに変化
  - proof = SHA256(<nonce>|<pairing key>)
  - Instance Name = BASE64(<nonce>|<proof>)
  - <instance i>._pds._tcp.local SRVクエリをmulticast
  - <pairing key>を知らないと情報を得られない
  - まだ複雑

homenet WG

- Home Networking
- (元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
  - ISPが家のゾーンをDNSSEC署名、DNSサーバ提供
  - DHCPにhybrid proxyなどのオプションを追加する提案
- 振り返り: IETF 95 (2016/4)
  - homenetでの名前解決の新提案
  - Name spaceの議論: Global, Local, Guest (客向け)
- 振り返り: IETF 96 (2016/7)
  - RFC 7788で.home, homenetでの名前解決の議論
- 振り返り: IETF 97 (2016/11)
  - ".hometnet" 提案, 名前解決

homenet (2)

- TLD予約が進展
  - ミーティング時には議論が進まず
  - 3/30にIABが.arpaを推奨する声明
    - "Internet Architecture Board statement on the registration of special use names in the ARPA domain"
  - IETF 98 後に ".home.arpa" 提案
  - .home → .homenet → .home.arpa

homenet (3)

- 名前解決の新提案
  - 簡略化: "All stateful stuff and security is gone."
  - multicast DNSを使い、リンク間ではDNSSD採用
  - リンク名は機械生成でuglyな(醜い)もの
    - Homenet control protocol (HNCP)で設定
  - Discovery proxyをすこし直し、リンク名をみせない
  - 名前が衝突したらDiscovery proxyがリンク名を追加

  - (筋は悪くないが、DNS-SDを変更するのが難点？)
  - use caseから考えるべきといったコメントあり
  - ただし、以前の ISPが家のゾーンを管理する複雑な提案は死んだわけではない

IEPG

- 運用に関する話題を扱うinformalな集まり
- 4件の発表 (DNS関連 1)
  - No domain left behind: is Let's Encrypt democratizing encryption? - Giovane C. M. Moura, SIDN
    - Let's Encryptのbulk issuingがうまくいっていて3 hosting providersで47%のドメイン名
  - The DNS Violations project - Ondřej Surý, NIC.CZ
  - BGP in 2016 - Geoff Huston, APNIC.
    - 経路数の伸びの紹介など (Mostly Harmless)
  - IPv6 Prefix Length Consideration - Job Snijders, NTT
    - AS 2914では/127 22%, /126 52%, /64 23%とのこと

IEPG: The DNS Violations project

- The DNS Horror Show by Ondřej Surý, NIC.CZ
- DNSを脅かす実装エラーを実名で紹介
- 目的: 実装ミスを理解すること、DNSを良くすること、知識を共有すること、問題を避けること
- 共通の問題
  - CDNでの独自実装に問題が見られることが多い
  - パケットのあとにGarbage(ゴミ)がつく
  - 大文字小文字問題
  - 非終端名に対するエラーの間違い
  - EDNS0の実装ミス
  - DNSSECの実装ミス
- 議論
  - 実名公表には賛否両論、「DNS Police !」
  - ドキュメントをまとめることや、Test suiteの必要性がコメントされた

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.iab.org
  - IABからの声明