前回の報告と同じ内容の部分

IETF 97 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 97 報告会, 2016年12月16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
    - 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 97結果
  - 発表1件, 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
  - dnsbundled　　Bundled domain BoF
  - DNS over HTTP　bar bof

- IETF以外
  - IEPG
  - Yeti DNS 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を多数発行中 (IETF 96から2、IESGに2)
  - 多数の提案の議論が進められた
- dprive: DNS通信路の暗号化
  - ほとんどの標準化が完了し、暗号の使い方についての議論が行なわれた
  - WGの今後についての議論が行なわれ、フルリゾルバと権威DNSサーバの通信の暗号化が提案された
- dane: DNS(SEC)にTLSの証明書
  - 非開催
  - SMIMEAがIESGに提出直前 (2度目のWGLC完了)

概要 2

- dnssd: DNS-SD (RFC 6763)の拡張
  - hybrid proxyドキュメントが更新されて進んだ
  - プライバシー提案が使いにくそう
- homenet: Home networking
  - .homenet TLDの予約を提案
- dnsbundled: Bundled-domain-names(BoF)
  - Bundled-domain-namesは、あるドメイン名を別のドメイン名に完全に対応付ける仕組みで、現在のDNS(DNAME)では実現できない
  - WG設立のためのBoFであったが、設立の合意には至らず、議論を継続

概要 3

- DNS over HTTP Bar BoF
  - HTTP上でDNSプロトコルをそのまま流す提案について、dnsop WGとhttpbis WG有志によるBar Bofを開催するが、結論は出なかった
  - 要求と現在の提案についての理解は進んだ
- IEPG: 運用に関する話題を扱うinformalな集まり
  - DNS (6件)とNATの検知の発表が行なわれた
- Yeti DNS workshop
  - Yeti DNSはRoot DNSに関する研究を行なうalternate root
  - 研究成果を報告された

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 94でのミーティングの概要
  - 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-cut
- 振り返り: IETF 95
  - 多数の案件
  - 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

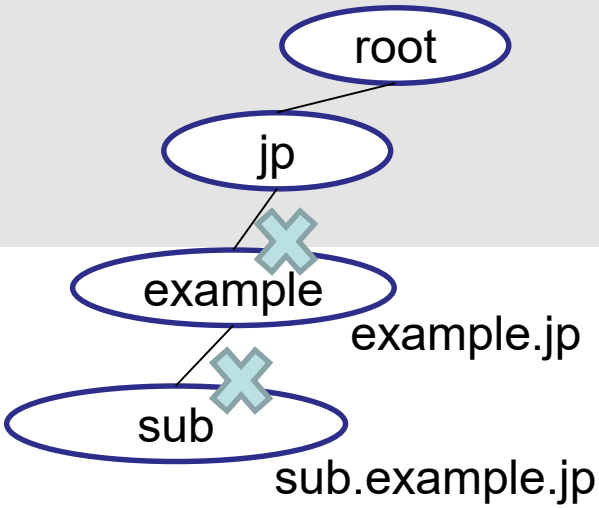
dnsop (2)

- 着実にRFCを発行 (draft-ietf-dnsop-を省略)
  - 2016/11/ 8 RFC 8020 nxdomain-cut
  - 2016/11/28 RFC 8027 dnssec-roadblock-avoidance
- IESGでレビュー中
  - maintain-ds 2016/6/21 IESG提出
  - resolver-priming 2016/9/18 IESG提出
    → 2016/12/1 Approved-announcement to be sent::Point Raised - writeup needed

dnsop (3)

- RFC 8020, 2016/11/8発行
  - draft-ietf-dnsop-nxdomain-cut
  - NXDOMAIN: There Really Is Nothing Underneath
  - リゾルバが名前不存在エラー(NXDOMAIN, Name Error)を受け取った場合にはキャッシュすることとその子孫の名前すべてを存在しない(NXDOMAIN)として扱うこと
  - リゾルバの性能向上
  - Updates RFC 1034, 2308

Random subdomain attack対策に使えるか？
攻撃:(random).example.com
フルリゾルバが攻撃時にルートから再検索する機能を追加するとNXDOMAIN検知できる→負荷増大
example.comの委任をはずすとエラーを返せる→負け



dnsop (4)

- 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 (5)

- draft-ietf-dnsop-maintain-ds-03,
  - 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
  - 2016/10/31 -04提出、いくつかコメント反映
  - 2016/9/28 IESG Evaluation - Defer　延期
    - RFC 7344をStandards trackに変更する手続きの問題

dnsop (6)

- 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

dnsop (7)

- IETF 97ミーティングの概要
  - IETF 96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: 2度目のWGLC予定
    - Special Names (TLD予約): Interim meetingを予定
    - terminology-bis: 毎月更新の予定だったが遅延している
  - 継続提案 current working group business
    - session-signal
  - 新規提案 new working group business

1. ipv4only.arpa
2. dns-delegation-requirements
3. dns-capture-format
4. resolver-update
5. transferring-automated-dnssec-zones
6. accompanying-questions
7. dns-catalog-zones
8. deploying-dnssec-crypto-algs

dnsop (8)

- draft-ietf-dnsop-session-signal
  - DNSにsessionの概念を追加する提案
  - dnssd WGのPUSH提案を複数の提案に分割、DNSへの変更が大きいsessionをdnsop WGで行う提案
  - sessionとは、長生きで双方向通信
    - DNS over TCP, DNS over TLSを想定 (UDP除外)
  - 新Opcode SESSION
  - Format
    - 16bit message ID
    - 16bit: QR, Opcode, Z, Rcode
    - そのあとに、TLV-DATA (QDCOUNTなどなし)
  - Call for adoption 7/22-8/12
    - 合意され、8/14付けでWG draft
    - draft-bellis-* → draft-ietf-dnsop-session-signal
  - いくつかの質問点の確認が行なわれた

dnsop (9)

- draft-cheshire-sudn-ipv4only-dot-arpa
  - RFC 7050 で定義されているipv4only.arpa などを IANA Special Names registryに追加する提案
    - Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis
    - ipv4only.arpa は A のみ、192.0.0.170, 192.0.0.171
    - DNS64の変換結果を見てNAT64で変換するprefixを得る
    - RFC 7050ではRegistry登録を書いていなかった
  - 議論
    - .arpaはIAB担当なので、dnsopで議論する必要はない
    - DNS設定する場合は安定のために長いTTL値を設定する
    - RFC 7050で定義されているため、進める方向

dnsop (10)

- draft-wallstrom-dnsop-dns-delegation-requirements
  - IETF 95
    - (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
  - IETF 97での議論
    - 必要性はあるが、万人が合意できるテスト項目は難しい
    - 継続

dnsop (11)

- draft-dickinson-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
  - 議論
    - 賛成者が多い
  - Call for adoption: WG itemとするか？
    - 2016/11/15-12/1
    - 賛成者多数で、WG itemになった
    - 2016/12/6: draft-ietf-dnsop-dns-capture-format

dnsop (12)

- draft-fujiwara-dnsop-resolver-update
  - 現在の名前解決アルゴリズムは誤りとし、改善を提案
  - RFC 1034の定義
    - zone cut / delegationは親側のNS RRSetが作る
    - 親側のNS(とグルー)は子側ネームサーバへアクセスする全情報を持つ
  - RFC 1034の名前解決アルゴリズム + RFC 2181
    - 親側NS・グルーは、確率的に子側NSとA/AAAAで上書き
  - 提案アルゴリズム
    - 名前解決には、親側のNSとグルーと外部名ネームサーバ名の名前解決結果だけを用いる
    - キャッシュを二つに分離 → Nominumの特許(2003年)の指摘
  - 議論
    - 親側NS, glueだけを使うという点に強い反対意見
    - 親子の違いによる悪影響は問題であるので、解決を望む
    - 親側、子側を分けるならdebugできる仕組みが必要

    → 全く否定されたわけではないので続ける予定

dnsop (13)

- draft-pounsett-transferring-automated-dnssec-zones
  - DNSSECで署名したままのDNSオペレータを移転する際の改善案の提案
  - RFC 6781に書かれた手順の簡略化
  - 議論
    - RFC 6781とこの提案に対してVerisignからIPR Claimがでていることの確認
    - reviewの必要性と議論の継続

dnsop (14)

- draft-yao-dnsop-accompanying-questions
  - 一つのDNSクエリに複数の問い合わせを入れる提案
    - 共著者がPaul Vixieのため、内容はよいが複雑
    - EDNS0オプションにクエリ名・タイプ、フラグ
    - 応答にも、クエリ名・タイプごとにフラグ、ほとんどの応答を表現可能
  - IETF 96での類似提案
    - ミーティング後に、複数応答・複数クエリをどう扱うか議論が行なわれ、しばらくは標準化しないという考えが強かった
  - 議論
    - 必要か？という質問
    - 進めるなら目的とセキュリティ考慮点などの議論が必要
    - 不評気味

dnsop (15)

- draft-muks-dnsop-dns-catalog-zones
  - マスターでのゾーン増減をスレーブに自動的に伝える仕組みの提案
  - DNSサーバの設定変更にゾーン情報を使う
  - master serverでゾーンを追加し、catalog zonesに追加すると、slaveで自動的にゾーンが追加
  - BIND 9.11に実装されている

dnsop (16)

- draft-york-dnsop-deploying-dnssec-crypto-algs
  - (新しいDNSSECアルゴリズム(ECDSA)を普及させたい)
  - 新しいDNSSECアルゴリズムの普及を阻止している構成要素と理由を示している
  - 議論
    - 時間なし
    - おおむね、合意できる現在の状況を示しているだけであるため、進めるかどうかは不明

dnsop (17)

- draft-ietf-dnsop-dns-wireformat-http-00
  - 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？
    - HTTP的に問題ないかhttpbis WGで確認すること
    - 2016/7/11~7/25 Call for adoption → 賛成
    - POSTでbinaryのDNSクエリを送り、応答を待つ
  - IETF 97ではhttpbis WG + dnsop WGでBar BoFを開催

DNS over HTTP Bar BoF

- IETFの会議時間外に、ミーティングルームを使って議論 → (Barじゃない)Bar BoF
  - 40人ほど集まり、狭い部屋が溢れて、床に座る人、立ったままの人多数
  - draft-ietf-dnsop-dns-wireformat-http
    - HTTPをトンネルとして使用
  - draft-hoffman-dns-in-json
    - DNSをjson表現
  - 議論: 非常に活発だが、結論は出ない
    - dane, dpriveの内容も語られて戸惑いあり

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
- 振り返り: IETF 93: DTLS, EDNS Padding新規
- 振り返り: IETF 94: TLS,padding ほぼ完了
  - 振り返り: IETF 95: 完了が見え、1時間と短め
- IETF 96では非開催 (dnsopで実装報告)
  - RFC 7858 DNS over TLS発行 → 使用可能に
  - RFC 7830 EDNS0 Padding発行

dprive (2)

- 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)

- IETF 97ミーティングの概要
  - DNS over (D)TLSの使い方と、WGの今後
  - 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
  - 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

dprive (4)

- WGの今後
  - draft-bortzmeyer-dprive-step-2-01
    - フルリゾルバと権威サーバの間もDNS over (D)TLSにする提案
  - 三択
    - WGを閉じる
    - 1年休憩(sleep)
    - 上記提案を進める
  - 会場の参加者の多くは上記提案を進めることに興味を示した
  - ADから、mailing listで議論を続けるように指示

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など
- IETF 94, IETF 95, IETF 96: ミーティング非開催
- IETF 97: ミーティング非開催

dane (2)

- 残るドキュメント: draft-ietf-dane-smime-14
  - 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
  - 2016/11/14-28 Second WGLC
  - IESG提出の見込み

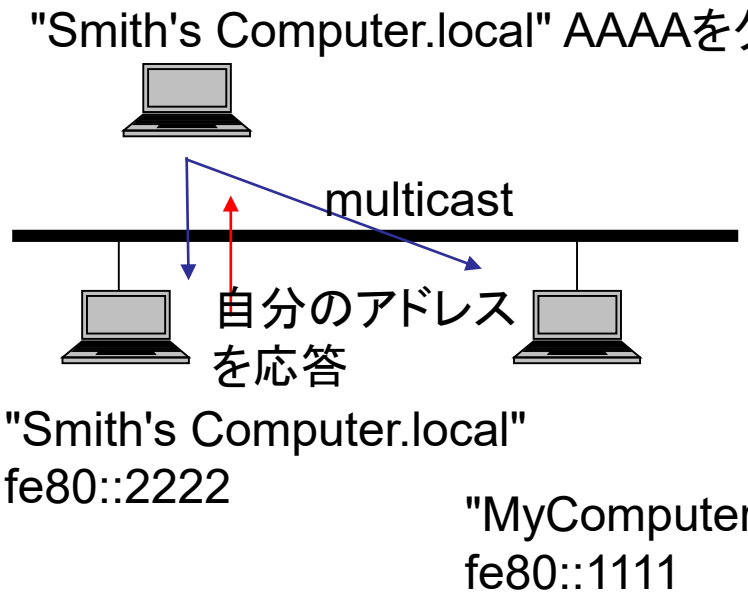
dnssd WG

- 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
- 振り返り: IETF 92: LLQの代わりに Update
- 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
- 振り返り: IETF 95: Hybrid Proxy未更新、Privacy, Push
- 振り返り: IETF 96: Hybrid Proxy未更新、Privacy, Push

dnssd (2): 復習: Multicast DNS (RFC 6762)

- link-localでのDNS-likeな名前解決機構
- 各ノードがラベル一つの名前を持ち、.local TLDを用いることでDNSと共存
  - MyComputer.local
  - スペースや' UTF-8も許容
- 各ノードは、multicastでクエリ
  - 224.0.0.251. ff02::fb　port 5353 UDP
  - パケットフォーマットはDNSと同じ
- 各ノードは、自分のホスト名宛クエリを受け取ると、ホスト名とIPアドレスの対応を応答
- 169.254.0.0/16, fe80::/10の逆引き
- A社のOSや、Avahiが対応
  - Avahi - Service Discovery for Linux using mDNS/DNS-SD -- compatible with Bonjour



dnssd(3) 復習: DNS-Based Service Discovery (RFC 6763)

- 構造化されたサービス名
  - <Instance>.<Service>.<Domain>
  - SRVと同じ形式 (_sip._udp.domain)
  - ホスト名と違い、スペース、UTF-8許可
- サービスの列挙: PTRを列挙
  - _http._tcp.dns-sd.org PTR ¥032*¥032eBay,¥032online¥032auctions._http._tcp.dns-sd.org.
- サービスへのアクセス: SRV
  - _http._tcp.dns-sd.org. SRV 0 100 80 www.dns-sd.org.
- Well known service
  - {b,db,r,dr,lb}._dns-sd._udp.domain
  - b._dns-sd._udp.domain PTR
    - A list of domains recommended for browsing
- Multicast DNSでのDNS-SD
  - domain: .local を使用
  - _ipp._tcp.local PTRクエリに対して、同じリンクにある別の名前を持つ複数のプリンタが応答

    _ipp._tcp.local PTR color._ipp._tcp.local

    _ipp._tcp.local PTR mono._ipp._tcp.local
  - User Interfaceでcolorを選ぶ、

color._ipp._tcp.local 0 0 49152 SRV color.local.

color.local IN A 192.0.2.11

→ 192.0.2.11ポート49152に接続

dnssd (4): 提案プロトコル(1)

- draft-ietf-dnssd-hybrid
  - dnssd コアプロトコル
  - 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
    - 例: link1.local ⇔ link1.example.com

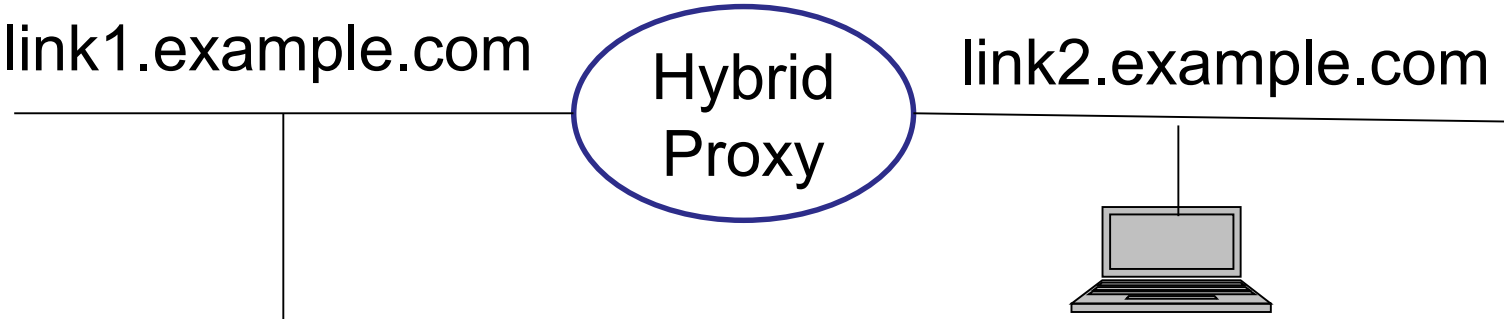
    <name>.link1.example.com PTRクエリを受け取ると、<name>.local PTRクエリをmDNSで送り、応答を書き換えて<name>.link1.example.com応答として返す
  - リンクのリストを事前設定しておく (browse)

b._dns-sd._udp.example.com PTR link1.example.com

b._dns-sd._udp.example.com PTR link2.example.com

  - 実装済み: A社のOSなど

dnssd (5): 提案プロトコル(2)



1. プリンタを使いたい
2. ブラウズ:
   b._dns-sd._udp.example.com
   → link1.example.com, link2.example.comがある
3. _ipp._tcp.link1.example.com を調べる
4. Proxyが_ipp._tcp.localクエリに変換して問い合わせ
5. プリンタ情報を得られる

X Printer

_ipp._tcp.local PTR
"X Printer._ipp._tcp.local"
"X Printer._ipp._tcp.local
SRV ….

dnssd (6)

- IETF 97での議論
  - 建設的に議論が進んだ
- draft-ietf-dnssd-hybrid (dnssdのコアプロトコル)
  - 8ケ月ぶりにアップデート、WGLCコメント反映
  - Hybrid ProxyからDiscovery Proxy and Advertising proxyに名前変更
  - IESGに提出見込み
- 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
  - コメントなく、WGLCが近い

dnssd (7)

- draft-ietf-dnssd-pricacy
  - Privacy Extensions for DNS-SD
  - 2016/10/27: WG draftになった
  - プライバシー保護のために、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
  - 許可したペア間だけで名前解決できるアクセス制限や、encodedな名前を使うことなどが提案された
  - 議論
    - Security Areaのreviewが必要である
    - 事前設定の量についての推定が必要
    - 一対の組から開始できるので、徐々に実装できる
- draft-ietf-dnssd-pairing
  - ペアの組み方のドキュメント
  - 問題提起からデバイスの発見方法、複数の認証(Pin, 押しボタン, 近距離, パスワード)、セキュリティ、ユーザインターフェースまで

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
  - 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
  - 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を仮定した対策
  - homenetでの名前解決の議論

homenet (2)

- draft-ietf-homenet-dot-homenet
  - RFC 7788では ".home" をdefault domain name としていた
  - ".home"は既にrootに漏れていて、ICANN Name collisionで使用不可能であるため、別のドメイン名を使う
  - homenetのdefault domain nameを".homenet" に変更する提案
  - 活発な議論が行なわれ、.homenetの予約に関心を持つ人が多かった
  - 2016/11/18~12/16 WGLC

homenet (3)

- draft-lemon-homenet-naming-architecture
  - homenet naming architecture
  - 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, Local (.homenet想定), Guest
  - 議論
    - DNS情報管理APIの議論 → Web, Netconf ?
    - 家のドメイン名と逆引きをISPに管理させる話で盛り上がる
    - 拡張性を残しつつ、できるところから始めようという提案

      → DNSSDのHybrid Discovery Proxyから始め、
      あとで権威サーバを追加すればよい

dnsbundled BoF

- dnsbundled: Bundled Domains
  - Bundled Domainsは、あるドメイン名を別のドメイン名に完全に対応付ける仕組みで、現在のDNS (DNAME)では実現できない
    - 例: .中国 と .中國
  - WG設立のためのBoF
- 振り返り
  - IETF 96: 昼休みにBar BoF開催、CNNICの提案
- IETF 97: 正式なBoFとして開催

dnsbundled (2)

- 発表
  - 問題提起と解決案の紹介
  - ユースケースの紹介 (CN, TW, GR, CZ, Registrar)
- 議論
  - この問題は、IDNの標準化が進められた2002年にも議論されている
  - 現在の問題提起文書は不十分であり、問題点を明確に定義していない
  - 問題の解決にはDNSの名前解決のみでは不十分であり、インターネット識別子の根本的な作り直しが必要になる
  - 本件においては、DNSのゾーン管理と利用者のアクセスの双方について考慮する必要があるが、この場では対象をゾーン管理に絞るべきである
- 結論
  - WG設立の合意には至らず、メーリングリストで議論を継続

IEPG

- 運用に関する話題を扱うinformalな集まり
- 7件の発表 (DNS関連 6)
  - A demo of DNSDB - Paul Vixie
  - Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event - Moritz Muller
  - DDOS and the DNS- Geoff Huston
  - State of DNSSEC Deployment - 2016 - Dan York
  - PcapParser - tool that reassembles IP fragments and DNS messages from pcaps - Shane Kerr
  - Detecting NAT / NAT-PT - Carlos M. Martinez
  - Aggressive use of NSEC/NSEC3 - Warren Kumari

IEPG (2)

- Anycast vs. DDoS: Evaluating the November 2015 Root DNS Event
  - Moritz Muller
  - 2015年11月のルートサーバへのDDoS攻撃の評価結果
  - 興味深かった点: 攻撃を受けたノードのうちいくつかはBGP経路がなくなり、他の地域のノードに攻撃トラフィックが向かうことが見られた → 経路のFlip

IEPG (3)

- DDOS and the DNS
  - Geoff Huston
  - DNSサーバへのDDoS攻撃への対策
    1. A Bigger Bunker: 物量作戦、太い回線、多数のノードでanycast
    2. Longer TTLs: TTLを長くする
    3. Filter queries: <random> nameをフィルタ
    4. Filter IP addresses:多数の攻撃元アドレスをフィルタ
    5. Use DNSSEC and apply NSEC Aggressive caching
  - draft-ietf-dnsop-nsec-aggressiveuseの宣伝をしてくれた

IEPG (4)

- Aggressive use of NSEC/NSEC3 - Warren Kumari
  - フルリゾルバでキャッシュしているDNSSECの不存在応答を使い、不存在応答を生成して性能向上
    - dig +dnssec Belkin

      beer. 21512 IN NSEC bentley. NS DS RRSIG NSEC

      beerとbentleyの間にはラベルがない
  - CPEのバグで、存在しないTLDのクエリがGoogle Public DNSに多数届き、Rootに漏れた
  - Google Public DNSで実装したところ、Rootへのクエリが激減した
  - Unboundでも実装された

Yeti DNS workshop

- Yeti DNSはRoot DNSに関する研究を行うalternate root
  - IANA rootから委任情報(NS,DS,glue)だけ抽出、独自DNSSECキーと独自ルートサーバリストを追加
- IETF 97の前の日に同じホテルでワークショップを開催
- http://yeti-dns.org/blog.html
- 議題

1. Notes on software construction and reliability for privately signed root zones（Paul Vixie）
2. Invite talk: IDN introduction and current status（Marc Blanchet)
3. Yeti DNS Project status and development (Davey Song)
4. Yeti experiment and findings (Shane Kerr)
5. IPv6 issues in Yeti (Akira Kato)
6. Yeti tools: YmmV and PcapParser (Shane Kerr)
7. Invite talk: Entrada Introduction (Moritz Mueller)
8. Open discussion: Improving Root Name space(Paul Vixie)

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