最近のIETF事情
(DNS関係)

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 2016, DNS Day
2016年12月1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 (2016/11~)

IETF

- IETF (Internet Engineering Task Force)
  - インターネット標準(RFCなど)を決める団体
- IETFの活動への参加(貢献)
  - ドキュメントを書くこと
  - メーリングリストにメールを書くこと
  - 年三回開催される会議に参加することなど
    - 2016/11/13~18 ソウルにてIETF 97開催
  - だれでも参加可能
  - 原則として個人での参加
- IETFの活動は公開原則
  - メーリングリスト、会議の議事録、音声

DNS関連WG

- dnsext WG
  - DNSプロトコルの拡張
  - 2013年7月に完了、プロトコル拡張機能をdnsopへ
- dnsop WG
  - DNS運用ガイドライン作成
  - DNSプロトコル拡張を作る機能
  - 1999年以前に設立
- 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
  - 2014年10月設立
- dane WG
  - DNS(SEC)にTLSの証明書を載せる
  - 2010年10月設立
- dnssd WG
  - .localを使用するMulticast DNS (RFC 6762), DNS-SD (RFC 6763)の拡張
  - 2013年10月設立
- その他
  - ほかにもDNSやドメイン名に関する活動はあるが、本報告では省略

dnsop (DNS Operations) WG

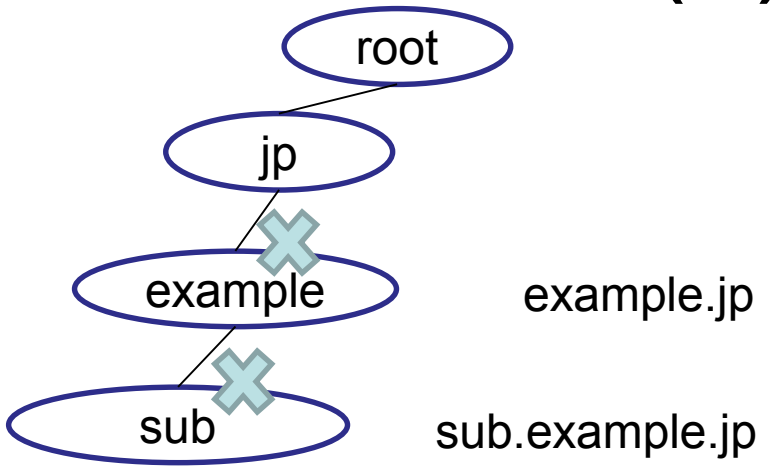
- DNS運用ガイドラインを作るWG
  - DNSプロトコル拡張を作る機能
  - dprive WGはdnsop WGから独立
  - 唯一のDNSそのものを扱うWGとして、ドメイン名全般、DNSプロトコルの話題に関して、IESG, IABなどから意見を求められる
  - 多数の提案を取り扱っている
  - RFCを着実に発行中
    - 2015年11月～2016年11月で10本
    - RFC Editor queueに1本
    - IESG対応中2本
    - WG draft 15本
- 最近のdnsop WGでのテーマ
  - TLD予約 (.localの前例)
  - 標準の明確化と軽微な修正
    - DNS用語
    - TCPトランスポート
    - 応答順序
    - ゾーン情報の要求仕様
  - DNSプライバシー→一部をdprive WG
  - 性能向上
    - ルートへのクエリ数を減らす
    - DNSSECを用いて不存在応答を生成
    - 名前不存在時の性能向上
    - ANY応答の明確化
  - 攻撃対策: DNS Cookie
  - 新しい要求
    - 一つのクエリで複数の応答を得るもの: A/AAAAを同時に得る
    - CDNの制御

dnsop: DNSプロトコル変更 TCP通信路

- RFC 7766, 2016/3/3
  - DNSでのTCP通信路の要求仕様
  - 従来は最初にUDPでクエリを送り、TC=1応答を受け取った場合にTCPで再クエリだったが、最初からTCPで問い合わせてもよくなった
  - 一つのTCPで複数クエリを連続して送ること (応答を待たなくてよい)
  - 複数のクエリを送った場合の応答は順不同 (UDPと同じ)
  - TCPを張りっぱなしでときどきクエリを送るということも可能 (RFC 1035 Section 4.2.2にも既に記載)
  - TCP closeについて明確化
- RFC 2181 Section 6.1.3.2
  - Specifically, a DNS resolver or server that is sending a non-zone-transfer query MUST send a UDP query first.
- RFC 7766での変更
  - Section 5: TCP MAY be used before sending any UDP queries.
- RFC 7828, 2016/4/6
  - The edns-tcp-keepalive EDNS0 Option
  - 通信が流れていないTCPセッションを切るタイムアウト値を伝えるEDNS0オプション

dnsop: 名前不存在の性能向上 (1)

- RFC 8020, 2016/11/8
  - 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
  - Updates RFC 1034, 2308



- 例: フルリゾルバがexample.jpのNXDOMAINを受け取り、キャッシュしている場合に、sub.example.jpクエリを受け取るとNXDOMAINを返してよい

dnsop: 名前不存在の性能向上 (2)

- draft-ietf-dnsop-nsec-aggressiveuse
  - DNSSECでは、名前エラーには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
  - DNSの負荷を増大させたDNSSECを負荷軽減に利用
  - NSEC, NSEC3のタイプビットマップを使ったNODATA応答の生成
  - 実装: Unbound, Google Public DNS
    - Google Public DNSの実装でルートへのクエリが激減したことが報告された
  - 標準化作業中

dnsop: DNSへの機能追加 Cookie

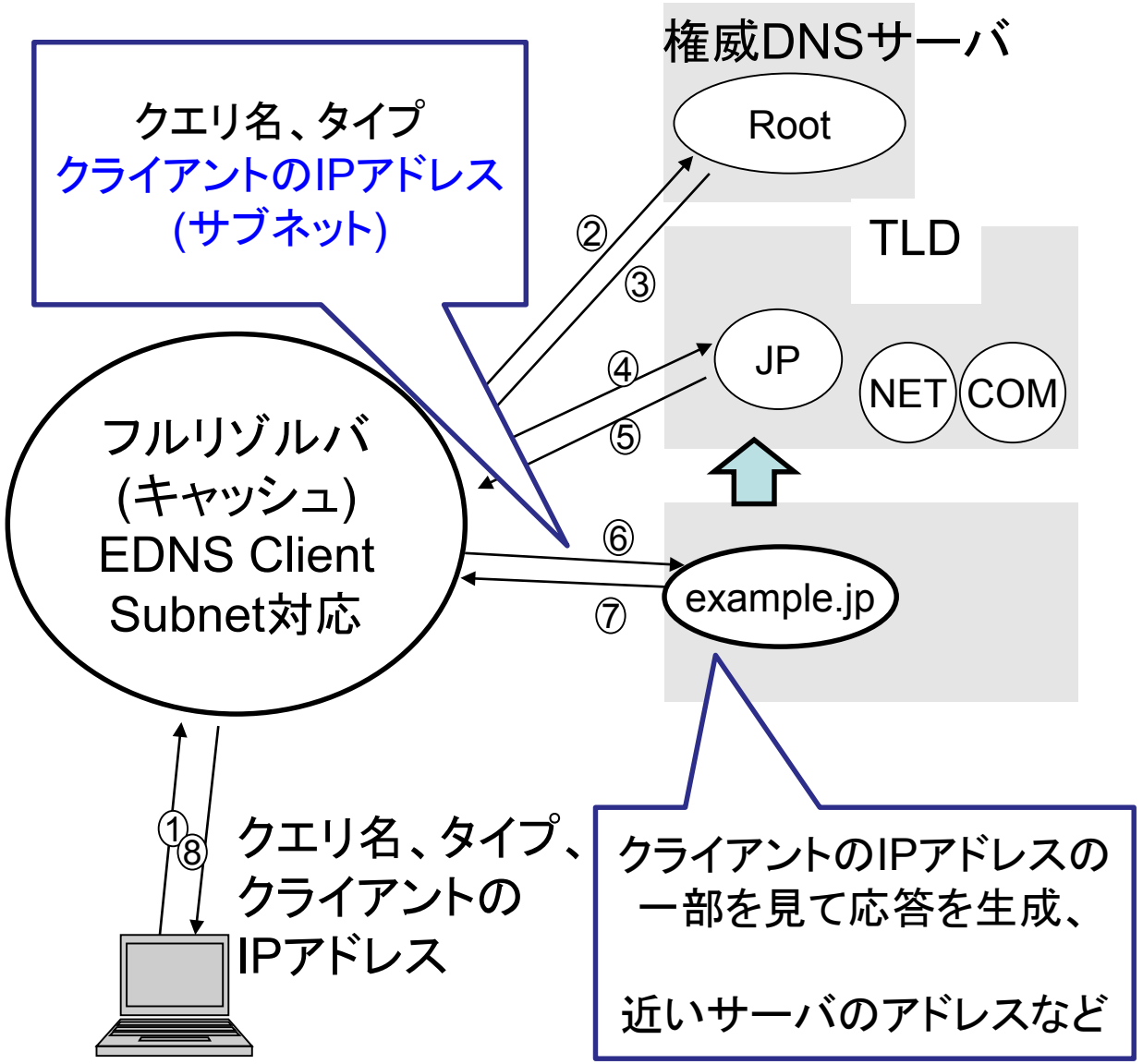
- RFC 7873, 2016/ 5/27発行
  - DNS Cookies
  - DNS/UDPの攻撃耐性を上げるために、クエリ側で64ビットのCookieを添付、サーバはレスポンスにコピー
  - 送信Cookieと受信Cookieが異なると異常
  - [client-cookie 8 bytes]
    [server cookie 8 to 32 bytes]
  - 実装済 BIND 9.10 など

目的

- キャッシュポイズニング対策
- ID 16ビット, ポート番号 16ビットを推定できると、フルリゾルバから権威サーバへのクエリを推定でき、応答を偽造して注入できて、容易にキャッシュポイズニング可能
- そこで新たに64ビット追加
- 96ビットを推定することは困難

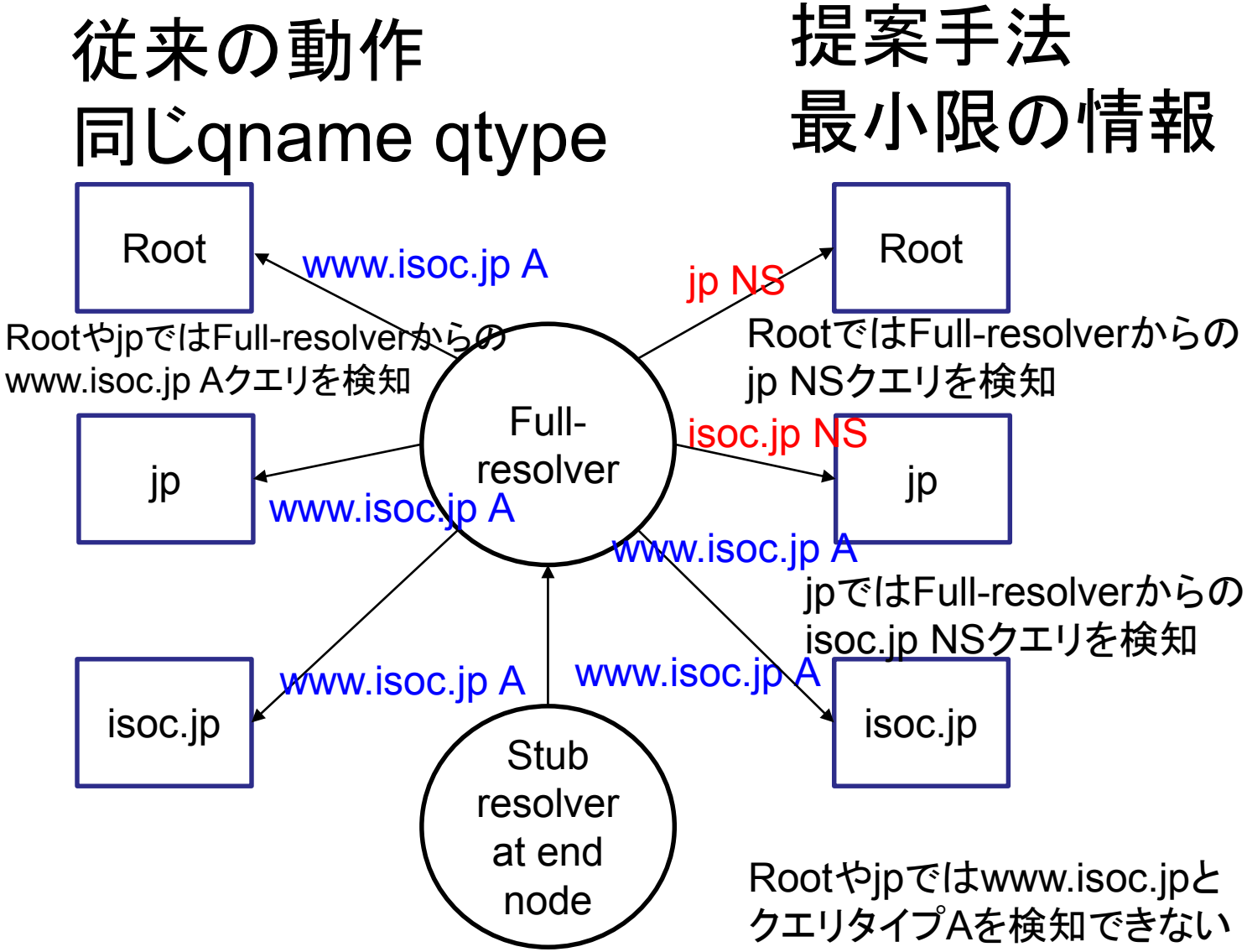
dnsop: DNSへの機能追加

- RFC 7871, 2016/5/20発行
  - EDNS Client subnet
  - 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 (一部のPublic DNS, CDN, Hyper Giants)
  - (クライアントアドレスが漏れる)



dnsop: クエリ情報漏洩最小化

- RFC 7816, 2016/3/22, Experimental RFC
- プライバシー向上のため、クエリ情報の漏洩を最小化
- 現在のフルリゾルバはユーザからのクエリ名、タイプをそのままルートを含む権威DNSサーバに送る
- 例:www.isoc.jp Aを知りたいときに
  - ルートには、TLDのNSクエリ (jp NS)
  - TLDには、登録ドメイン名のNSクエリ (isoc.jp NS)
  - を送ると、ルート・TLDでもとのクエリが見えない
  - クエリ名 www.isoc.jp, タイプAを隠蔽
- Knot Resolver, Unboundで実装済



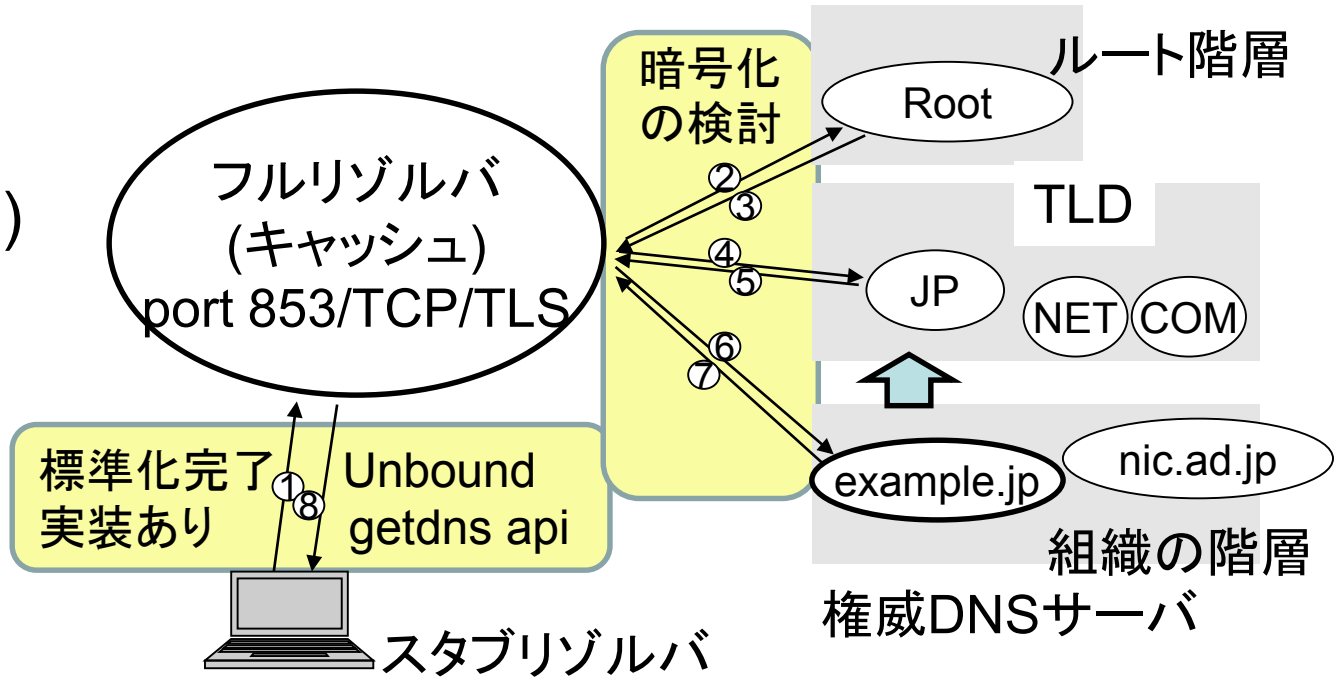
dnsop:プロトコルで使用するTLDの予約

- 歴史
  - Multicast DNS (.local)の標準化はdnsextでは好まれなかった
    - A社のプロトコル
  - dnsext, dnsopとは無関係に標準化
    - IETF Last Callなども通過
    - だれも文句をつけなかった(気付かなかった?)
    - サブマリンRFC?
  - 2013年2月RFC 6761,6762,6763発行
  - RFC 6761 特殊用途で使用するTLDの予約方法を規定
  - RFC 6762 Multicast DNSで.local予約
    - 「A社はタダで.local を手にいれた」という声
- .local の予約がすんなりきまったため、TLD予約の要求が乱立
  - .localの反省でdnsopが取り扱う
  - TLDはICANNの担当であるため、やりたくない
  - ICANNで新gTLDを登録するには金がかかるため、IETFで予約したい
- Torで使用される.onionは広く使用され、発行済み証明書の無効化期限が迫ったため、2015/10/23にRFC 7686で予約
- 現在は、議論のまとめと、複数の解決案の議論が続いている状態
  - .alt TLDに複数の要求をまとめる提案
  - homenet WGが、".homenet" TLDの予約を希望

dprive (DNS Privacate Exchange) WG

- スタブリゾルバとフルサービスリゾルバの間の通信を暗号化
- 2014年10月に設立し、ほぼ完了
- RFC 7858 (DNS over TLS)が発行され、使える状態になった
  - 2016/5/17発行
  - DNSクエリをTCP通信路を用い、さらにTransport Layer Security(TLS)で暗号化
  - port 853を使用
  - Unboundやgetdns apiで使用可能
- DNS over DTLSもIESGに提出

- 今後
  - IETF 97 (2016/11)にて、フルサービスリゾルバから権威サーバ間の通信暗号化の検討を開始することが提案され、参加者に好まれた



dane (DNS-based Authentication of Named Entities) WG

- DNS(SEC)にTLSの証明書をのせるWG
- 2010年10月設立、標準化をほぼ完了
  - ✓RFC 6698: TLSA RR (証明書のハッシュなどをのせるもの)
    - □例: www.example.com サーバ証明書のSHA256ハッシュをのせる場合
      _443._tcp.www.example.com. IN TLSA 0 0 1 d2abde24….618e971
  - ✓RFC 7929: OpenPGPKEY RR: OpenPGP個人証明書をのせるもの
    hex(先頭28バイト(sha256(localpart)))._openpgpkey.domain IN OPENPGPKEY 証明書
    - □例: hugh@example.com のOpenPGP証明書をのせる場合
      c93f1e400f26708f98cb19d936620da35eec8f72e57f9eec01c1afd6._openpgpkey.example.com IN OPENPGPKEY mQCNAzIG[...]
    - □PGP Key serverではなく、メールアドレスに対応するDNSクエリでOpenPGP証明書を得る
    - □個人証明書をDNSSECで検証
  - ✓SMIMEA RR: S/MIME個人証明書をのせるもので、議論中
  - ✓今後ブラウザやメールソフトウェアでの実装が期待される

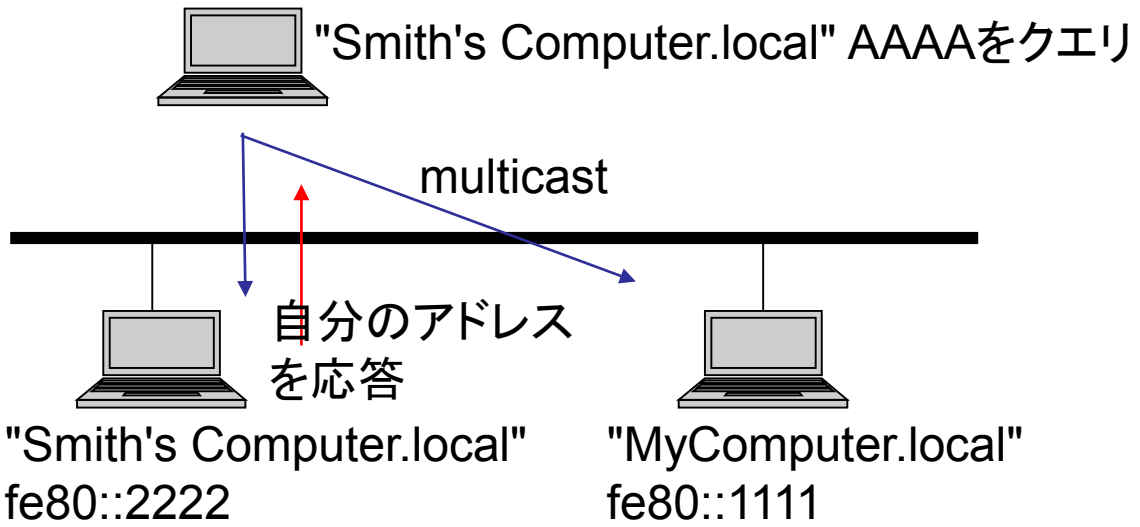
dnssd (Extensions for Scalable DNS Service Discovery) WG

- DNSを使ったサービスディスカバリを作るWG
  - Multicast DNS (RFC 6762, mDNS)と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
- status
  - 停滞気味だったが、IETF 97にてこれまでのコメントの反映が報告され、進めることが確認された
  - 主な提案者がMulticast DNSを標準化されたA社の方であり、すでに実装されているとのこと
- Multicast DNS (RFC 6762)
  - link-localでのDNS-likeな名前解決機構
- DNS-SD (RFC 6763)
  - サービスディスカバリ

dnssd: 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

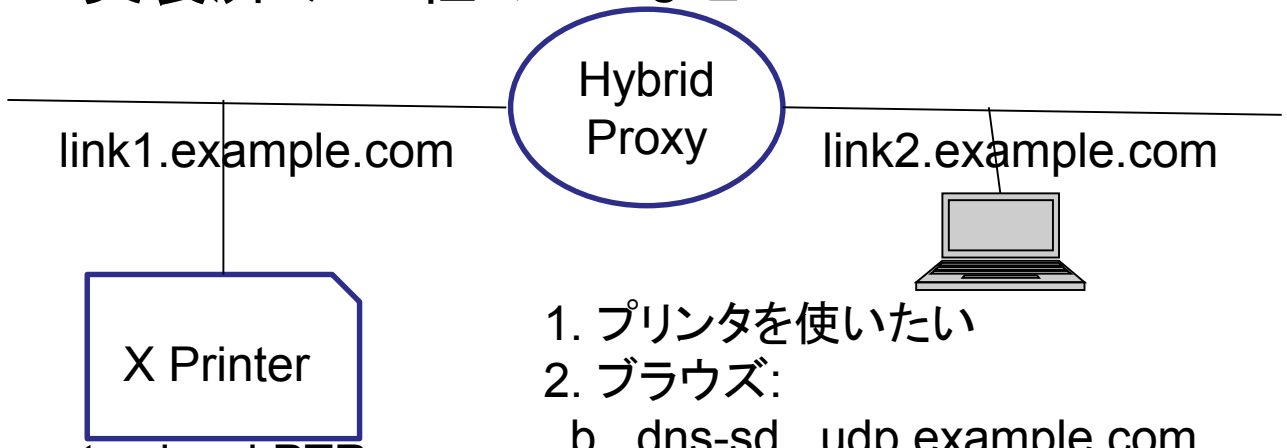


dnssd: DNS-Based Service Discovery (RFC 6763)

- 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、スペースやUTF-8許可
- サービスの列挙 (enumeration)
  - サービス名に PTRを書き、サービスを列挙
  - _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 RRを使用
  - _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
  - _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: 提案プロトコル

- 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を動かす
    - 例: link1.example.com, link2.example.com
    - Proxy 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
  - ブラウズ設定を管理者が行う
    - b._dns-sd._udp.example.com
      PTR link1.example.com
      PTR link2.example.com
  - 実装済み: A社のOSなど



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

1. プリンタを使いたい
2. ブラウズ:
   b._dns-sd._udp.example.com
   → link1, link2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

まとめ

- dnsop WG
  - 名前解決の効率化や攻撃耐性の強化、新機能追加のための拡張が盛んに行なわれ、実装も進む
  - 最初からTCPで問い合わせてもよくなった
- dprive WG
  - クライアントからフルリゾルバ間の通信路暗号化の標準化は完了し、すでに使用可能
  - 今後、フルリゾルバから権威DNSサーバ間の暗号化に取り組む
- dane WG
  - サーバ証明書と、OpenPGPの個人証明書をDNSに載せることができるようになった
  - 今後ブラウザやメールソフトウェアでの実装が期待される
- dnssd
  - Multicast DNSを複数セグメントで使用する拡張が進んでいる
  - A社のOSで実装されている

参考

- www.ietf.org
  - IETFミーティングの資料、議事録
  - メーリングリストアーカイブ
- www.rfc-editor.org
  - RFC