IETF 100 報告
DNS関連
注文: doh, dnssdを中心に

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 100 報告会, 2017年12月15日

自己紹介

- Active WG: **dnsop**,　Past WG: enum, eai
- RFC 8198, Aggressive use of DNSSEC-validated cache, 2017/7/25発行
  - Authors: **Kazunori Fujiwara**, Akira Kato, Warren Kumari
  - キャッシュされた(検証された)NSEC/NSEC3を利用して不存在応答を生成
  - トラフィック・負荷を大きくしたDNSSECを用いてトラフィック削減、性能向上
  - NSEC例：something**.local** クエリに次のNSEC RRが添付される

    loans. NSEC **locker.** NS DS RRSIG NSEC(loansからlockerに名前なし)
  - 実装: Google Public DNS, BIND 9.12.0, Knot Resolver 2.0
- RFC 7719, DNS Terminology → draft-ietf-dnsop-terminology-bis
  - Authors: Paul Hoffman, Andrew Sullivan, **Kazunori Fujiwara**
  - DNS用語を収集、定義を更新するもの: domain name, qnameなど更新

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
  - dane　　DNS(SEC)にTLSの証明書 → 完了
  - **doh　　DNS Over HTTPS**
  - **dnssd　　DNS-SD (RFC 6763)の拡張**
  - homenet　　Home Networking

- 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、2017年は4本
  - 多数の案件: 用語集の更新, KSK rollover関連の修正と提案, エラーコード拡張, localhost, DNS proxy情報, 複数応答, TSIG修正, .internal TLD
- dprive: DNS通信路の暗号化
  - 非開催で、サイドミーティングとして夜に1時間議論
  - 実装紹介、残draft、IETF 101でのリチャータ
- 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

概要 2

- dnssd: DNS-SD (RFC 6763)の拡張
  - 順調に標準化作業が進展(遅延)中
  - Apple社で実装しているプロトコル拡張が紹介され、draftとして紹介
  - プライバシー提案は複雑になったため、脅威の考察からやり直し
- homenet: Home networking
  - 主なプロトコルが決まり、限定されたものとなった
  - 名前解決機能はdnssdベースの簡易なものとなったが、dnssd WGの標準との差異の議論は先送り？

詳細

doh WG, dnssd WGのみ

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
- 標準化対象: draft-ietf-doh-dns-over-https
- 背景
  - DNS, DNS over TLSは通信路(middlebox)が通さない場合がある
    - http(s)なら何でも通る → IPアドレスを含むURLで指定か？
  - Webアプリケーションは、同じ通信路で名前解決したい

doh WG (2)

- draft-ietf-doh-dns-over-https (DNS over HTTPS)
  - 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
  - GET /.well-known/dns-query?
    content-type=application/dns-udpwireformat&　　(01→02で削除)
    body=q80BAAABAAAAAAAAA3d3dwdleGFtcGxlA2NvbQAAAQAB&
    accept=application/dns-udpwireformat
  - 将来的には、application/simpledns+json も標準化
- 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
- 議論が必要な部分は少ないため、すぐに決まる可能性あり

dnssd WG

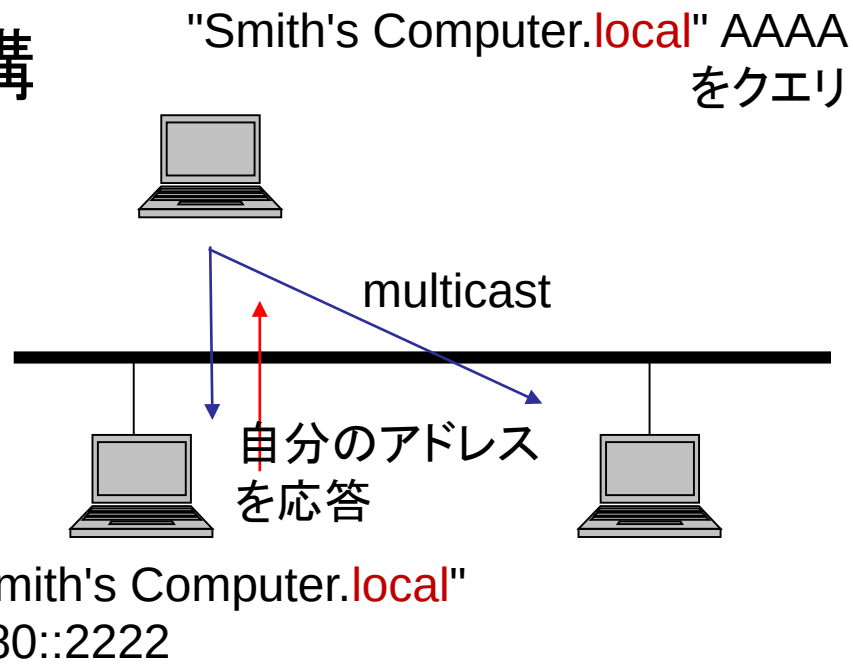
- Extensions for Scalable DNS Service Discovery
- DNSを使ったサービスディスカバリを作るWG
  - DNS-SD (RFC 6763)をベースに、複数ネットワークセグメントに対応したものを標準化する
  - 一言でいえば、Apple社のOSでのプリンタなどの発見を複数セグメントに拡張するもの
  - 印刷しようとするとプリンタの一覧が表示され、プリンタを選んで印刷できるが、そのときに大学や企業全体のプリンタを選びたい
- dnssdコアプロトコルの実装状況
  - Apple社のOSにはすでに実装されている？　追認？

dnssd WG: 進捗状況

- 2013年10月設立 (IETF 88ごろ)
- IETF 88~91: 要求仕様の議論からHybrid Proxy案
- 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 95,96: Hybrid Proxy未更新,Privacy,Push
- IETF 97: Hybrid Proxy更新/名前変更,Privacy, Push
- IETF 98,99: Discovery Proxy更新,Privacy複雑,関連draft
- IETF 100: Discovery Proxy IESG提出,Privacyやり直し,他

おさらい: Multicast DNS (mDNS,RFC 6762)

- Apple Bonjour (←AppleTalkの機能) や Avahi
  - Avahi - Service Discovery for Linux using mDNS/DNS-SD -- compatible with Bonjour
- 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つ
- .local TLDを用いることでDNSと共存
  - MyComputer.local
  - スペース ' 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
- 自分が答えるべき名前のクエリを受け取ると応答



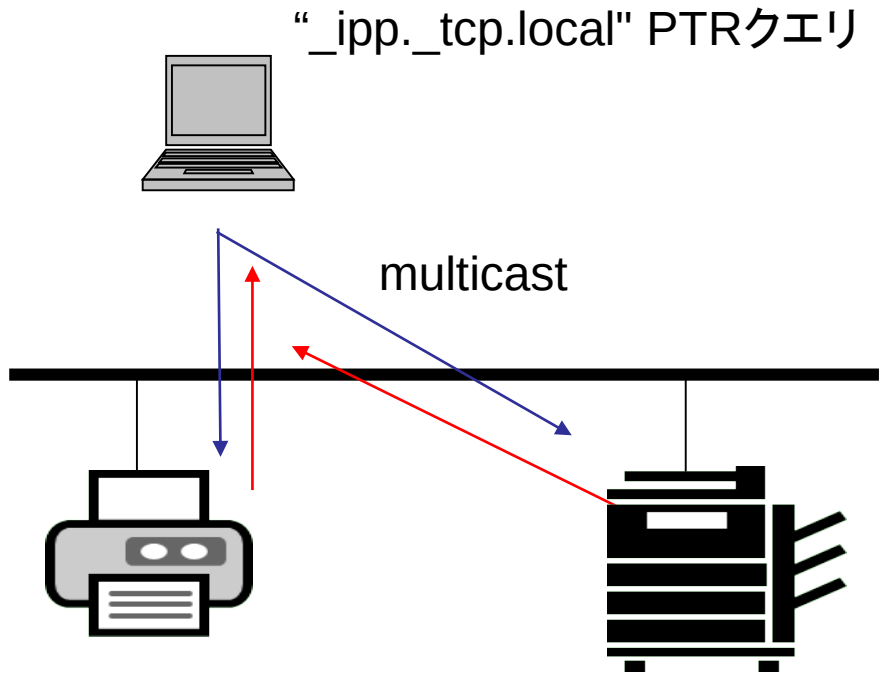
おさらい: DNS-SD (RFC 6763)

- DNS-Based Service Discovery
- 構造化されたサービス名
  - <Instance>.<Service>.<Domain>
  - dns-sd.org の http サービスは、_http._tcp.dns-sd.org
- サービス名に PTRを複数書き列挙
  - dns-sd.org の http サービスは、_http._tcp.dns-sd.org PTR に列挙する

  例: _http._tcp.dns-sd.org PTR eBayAuctions._http._tcp.dns-sd.org.
- サービスへのアクセスにSRV RR
  - eBayAuctions._http._tcp.dns-sd.org. SRV 0 100 80 auc.dns-sd.org.
- 特殊用途の名前: {b,db,r,dr,lb}._dns-sd._udp.<Domain>
  - b._dns-sd._udp.domain PTR: ブラウズすべきドメイン名のリスト

おさらい: Multicast DNSでのDNS-SD

- Multicast DNSでのDNS-SD
  - Domain = .local
  - プリンタは、_ipp
  1. 印刷したい！
  2. _ipp._tcp.local PTRクエリを送ると複数のプリンタが応答 (mDNS)
     - _ipp._tcp.local PTR color._ipp._tcp.local
     - _ipp._tcp.local PTR mono._ipp._tcp.local
  3. User Interfaceで両方を表示
  4. color._ipp._tcp.localを選ぶと、color._ipp._tcp.local SRVクエリを送り、プリンタ情報を得る
     - プリンタ名(→IPアドレス)とポート番号
  5. プリンタに接続

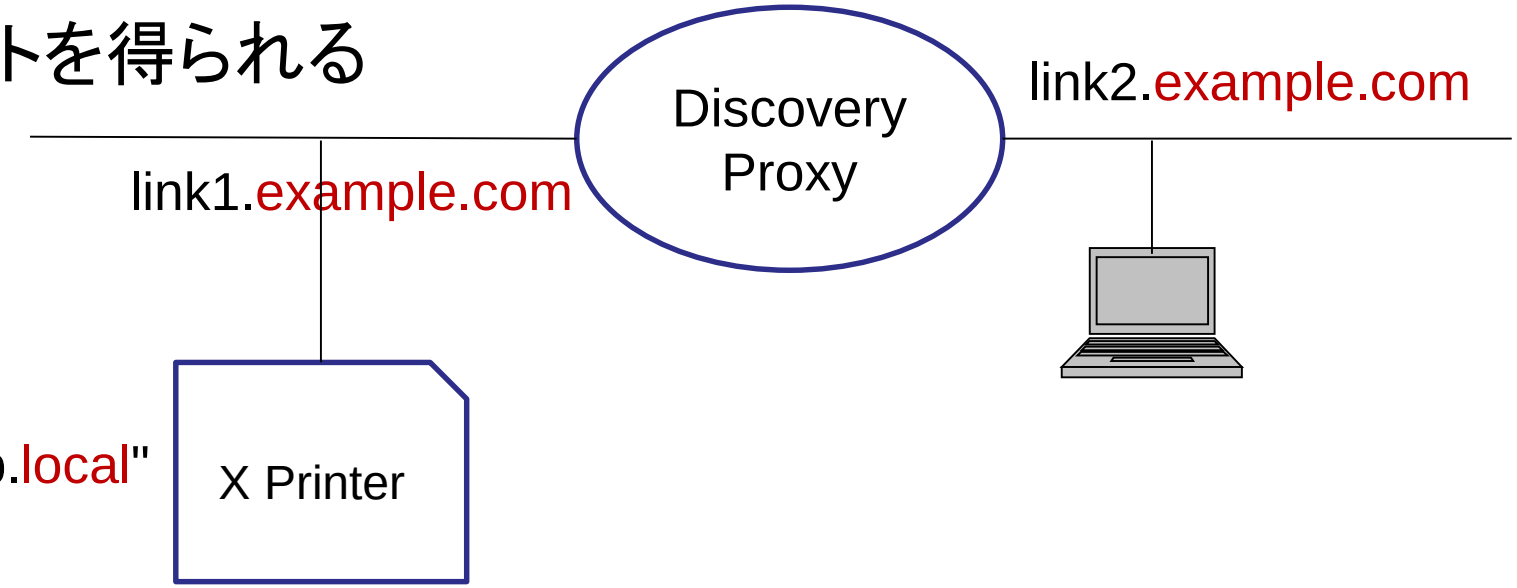


dnssd: 提案プロトコル (1)

- draft-ietf-dnssd-hybrid
  - dnssd コアプロトコル
  - DNSとMulticast DNSのProxyとして実装
  - リンクごとにドメイン名を設定、ルータでDiscovery proxyを動かす
    - 例: link1.example.com
    1. Discovery proxyが<name>.link1.example.comクエリを受け取ると
    2. link1.example.comリンクでmDNSの<name>.localクエリを送り
    3. <name>.link1.example.comからの応答として返す
  - ブラウズ設定を管理者が行っておく
    - b._dns-sd._udp.example.com　PTR link1.example.com
      PTR link2.example.com
  - Multicast DNSのノードは変更しない

dnssd: 提案プロトコル (2)

1. PCで、プリンタを使いたい
2. ブラウズ: b._dns-sd._udp.example.com PTR→ link1, link2がある
3. PCが_ipp._tcp.link1.example.com SRVクエリを送る
4. Discovery Proxyが_ipp._tcp.local SRVクエリに変換して問い合わせ、_ipp._tcp.link1.example.comからの応答に書き換えて応答
5. SRV応答のホスト名を名前解決する
6. プリンタのアドレス、ポートを得られる



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

dnssd: IETF 100 (1)

- コアプロトコル (Discovery Proxy)
  - 2017/9/15にIESGに提出、IESGメンバーからDISCUSS要修正
  - 最低限の仕様はできそうである
- homenet WGでの使用
  - draft-ietf-homenet-simple-naming
  - homenetには管理者がいないのでリンク名の自動設定が必要
  - dnssd Discovery Proxy を改造した提案だがdraft中に “?” が残る
  - <name>.<自動生成リンク名>.home.arpa
  - 決まりそうにない?

dnssd: IETF 100 (2)

- dnssd privacy
  - Multicast DNSにはプライバシーがない
    - ブラウズすると、すべてのノード名が見えるはず
  - 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ようにする提案があったが、複雑すぎて今回は議論されていない
  - 脅威の考察からやりなおし
    - Apple AirDrop (WiFiでの2者間通信?) などを例
- dnssd WGまとめ
  - 順調に標準化作業が進展(遅延)中で、コアプロトコルは1年以内に発行見込み
  - プライバシーはやり直し、homenetでの使用も時間がかかるか？

Questions and comments ?