DNSプロトコル変更点の紹介と、脆弱性に焦らないDNS運用

藤原 和典
fujiwara@jprs.co.jp
株式会社日本レジストリサービス (JPRS)

TOPIC講演会, 2017年4月28日

Last update: 2017/4/21 1730 JST

Copyright © 2017 Japan Registry Services Co., Ltd.

自己紹介

- 氏名:　藤原和典
- 個人ページ: http://member.wide.ad.jp/~fujiwara/
- 1991~ WIDEプロジェクト, 現在は"ns.tokyo.wide.ad.jp"のお守り
- 1992~1996: 早稲田大学情報科学研究教育センター助手
  - 早稲田大学のキャンパスネットワーク構築・運用
- 2002~ 株式会社日本レジストリサービス(JPRS)技術研究部
  - 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):メールアドレス国際化
  - RFC 7719 (2015): DNS用語集
  - draft-ietf-dnsop-nsec-aggressiveuse (2015/3~, 現在IESGレビュー中)

Copyright © 2017 Japan Registry Services Co., Ltd.

本日の構成

- DNSプロトコル変更点の紹介
- 脆弱性に焦らないDNS運用

Copyright © 2017 Japan Registry Services Co., Ltd.

DNSプロトコル変更点の紹介

Copyright © 2017 Japan Registry Services Co., Ltd.

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
    - 2017/3/26~31 シカゴにてIETF 98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

Copyright © 2017 Japan Registry Services Co., Ltd.

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、2017年3月完了
- 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

Copyright © 2017 Japan Registry Services Co., Ltd.

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
    - 2016年4月～2017年4月で10本
    - IESG対応中2本
    - WG draft 12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

Copyright © 2017 Japan Registry Services Co., Ltd.

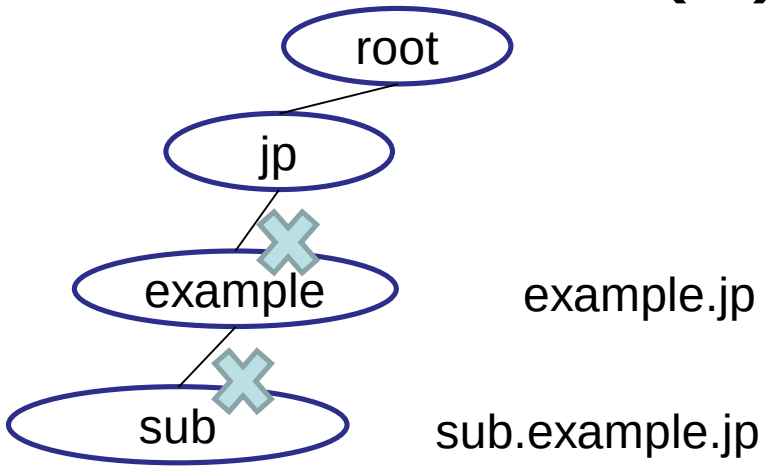
dnsop: DNSプロトコル変更 TCP通信路

- RFC 7766, 2016/3/3
  - DNSでのTCP通信路の要求仕様
  - 目的: DNS over TLSなどでTCP通信路の使用が増えるために改良
  - 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接続で複数クエリを連続して送ること (pipelining)
  - 応答は順不同 (UDPと同じ)
  - TCP接続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 1123 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

Copyright © 2017 Japan Registry Services Co., Ltd.

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
  - 目的: 名前解決時の性能向上



- 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

Copyright © 2017 Japan Registry Services Co., Ltd.

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: 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
  - IESGでレビュー中
  - 著者: 藤原、慶應大学・WIDEプロジェクトの加藤さん、GoogleのWarren Kumariさん
  - 目的: DNSSEC検証時の名前解決の性能向上とDoS耐性向上

Copyright © 2017 Japan Registry Services Co., Ltd.

dnsop: DNSへの機能追加(1) 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

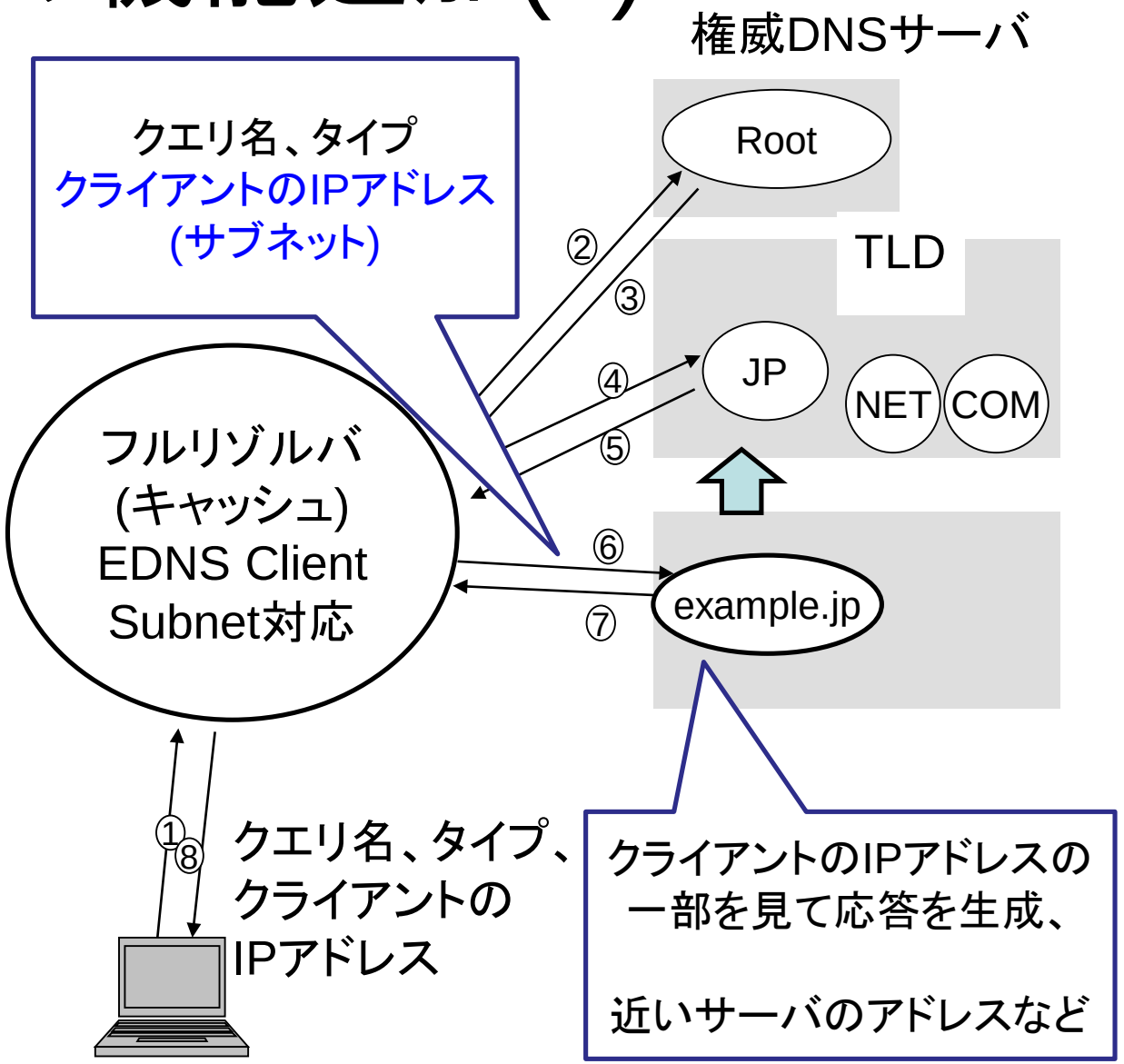
目的

- 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

Copyright © 2017 Japan Registry Services Co., Ltd.

dnsop: DNSへの機能追加(2)

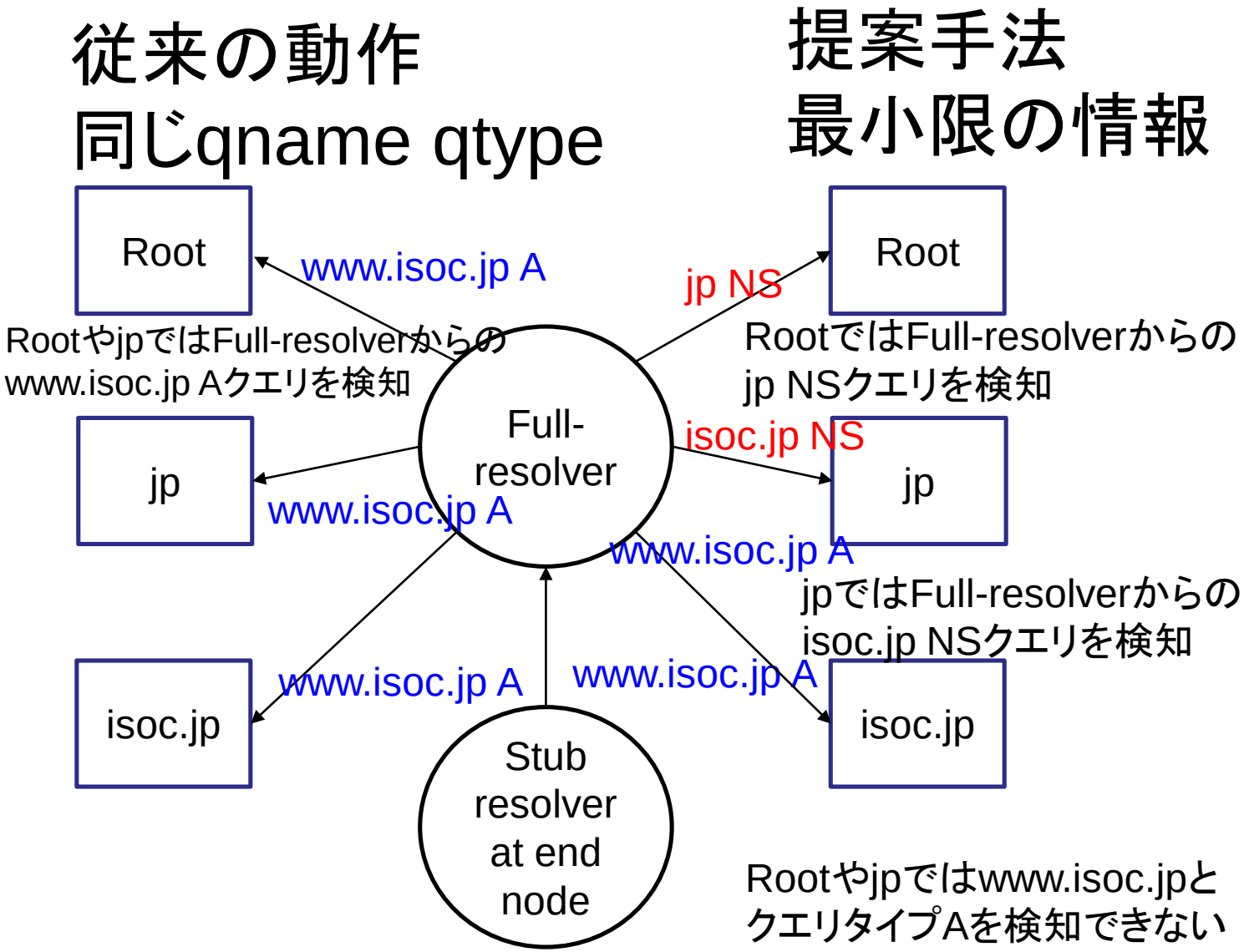
- RFC 7871, 2016/5/20発行
  - EDNS Client subnet
  - Public DNSサービスの利用者がCDNのアドレス制御を使用できるように、クライアントのサブネットアドレスを権威DNSサーバに伝えるEDNS0オプション
  - [address-family] [prefix-length] [prefix]
  - 実装済 (一部のPublic DNS, CDN, Hyper Giants)
  - (クライアントアドレスが漏れる)
  - 目的: Public DNSを使ってもCDNの制御を行なうこと



Copyright © 2017 Japan Registry Services Co., Ltd.

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くなる
  - クエリ名 www.isoc.jp, タイプAを隠蔽
- Knot Resolver, Unboundで実装済



Copyright © 2017 Japan Registry Services Co., Ltd.

dnsop:プロトコルで使用するTLDの予約

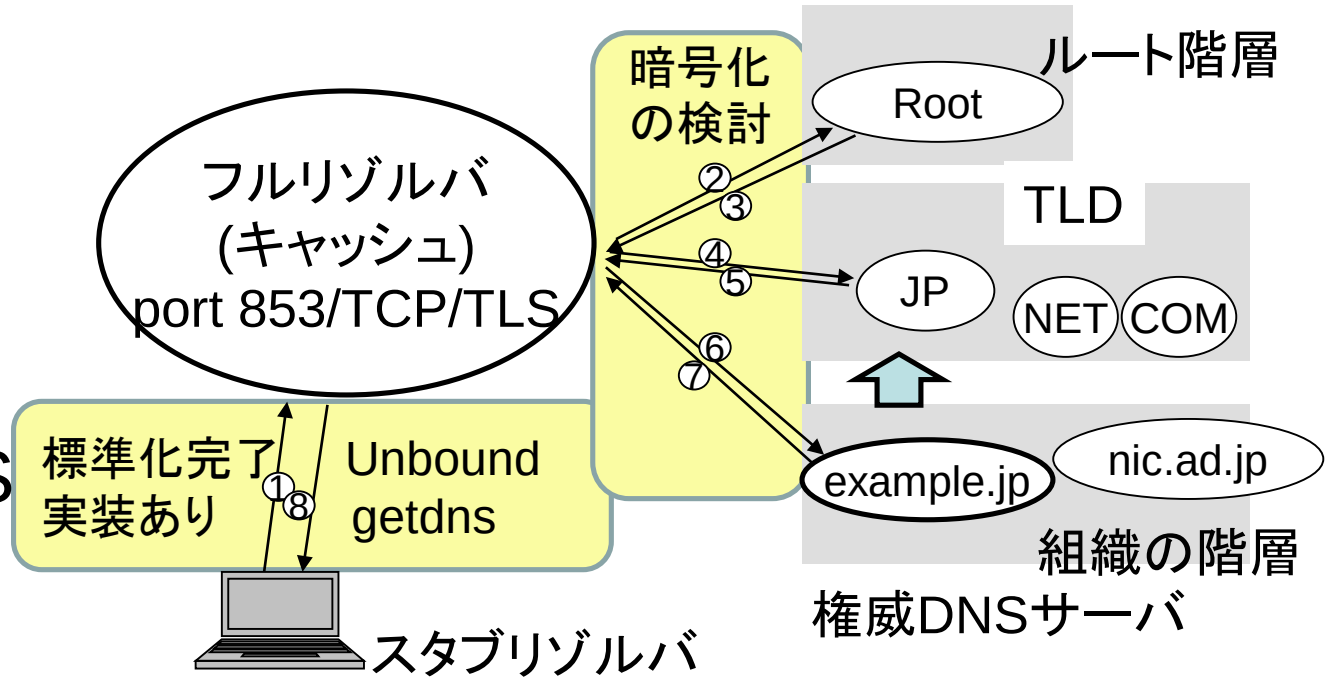
- 歴史
  - Multicast DNS (.local)の標準化はdnsextでは好まれなかった
    - A社のプロトコル
  - dnsext, dnsopとは無関係に標準化
    - IETF Last Callなども通過
    - だれも文句をつけなかった(気付かなかった?)
    - サブマリンRFC?
  - 2013年2月RFC 6761,6762,6763発行
  - RFC 6761 特殊用途で使用するTLDの予約方法を規定
  - RFC 6762 Multicast DNSで.local予約
    - 「A社はタダで.local を手にいれた」という声
- .local の予約がすんなり決まったため、TLD予約の要求が乱立
  - .localの反省でdnsopが取り扱う
  - TLDはICANNの領域であるため、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
- 3/30にIABが.arpaを推奨する声明
  - homenet WGが、".homenet" TLDの予約を希望 → ".home.arpa" に変更

Copyright © 2017 Japan Registry Services Co., Ltd.

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Transport Layer Security(TLS)で暗号化
  - port 853 (TCP)を使用
  - UnboundやgetdnsでDNS over DTLS使用可能
- RFC 8094としてDNS over DTLSが発行された (2017/2/28)
  - port 853 (UDP)を使用

- 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



Copyright © 2017 Japan Registry Services Co., Ltd.

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、標準化を完了し、2017年3月に完了
  - ✓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公開鍵をのせるもの
    hex(先頭28バイト(sha256(localpart)))._openpgpkey.domain IN OPENPGPKEY 公開鍵
    - □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公開鍵を得る
    - □個人証明書をDNSSECで検証
  - ✓SMIMEA RR: S/MIME証明書をのせるもので、RFC発行認可済
  - ✓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

Copyright © 2017 Japan Registry Services Co., Ltd.

dnssd (Extensions for Scalable DNS Service Discovery) WG

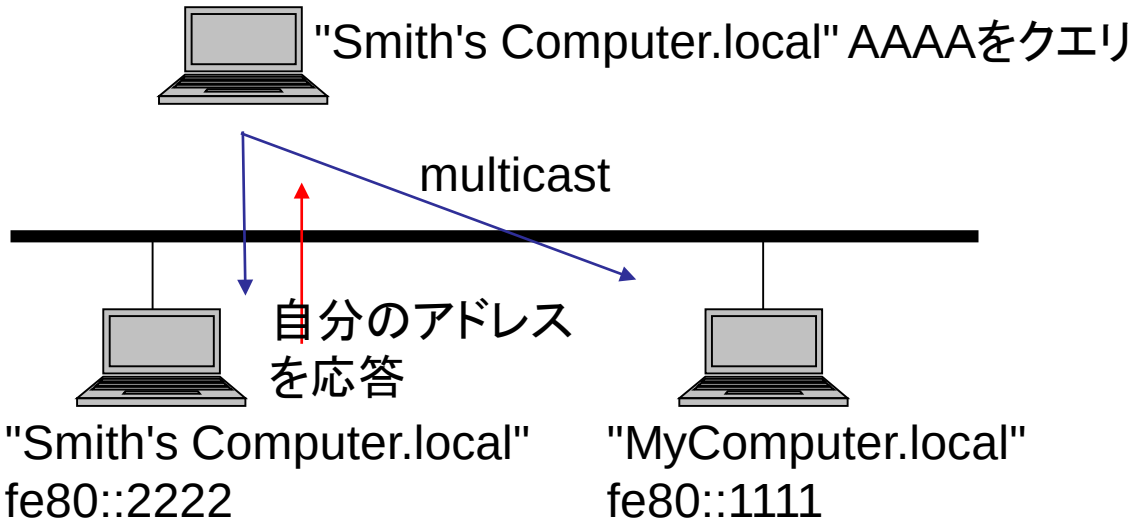
- DNSを使ったサービスディスカバリを作るWG
  - Multicast DNS (RFC 6762, mDNS)とDNS-SD (RFC 6763)をベースに、複数ネットワークセグメントに対応したものを標準化
- status
  - 停滞気味だったが、IETF 97にてこれまでのコメントの反映が報告され、進めることが確認された
  - 主な提案者がMulticast DNSを標準化されたA社の方であり、すでに実装されているとのこと
  - IETF 98では、A社で実装済のプロトコル拡張が紹介された
- Multicast DNS (RFC 6762)
  - link-localでのDNS-likeな名前解決機構
- DNS-SD (RFC 6763)
  - サービスディスカバリ

Copyright © 2017 Japan Registry Services Co., Ltd.

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



Copyright © 2017 Japan Registry Services Co., Ltd.

dnssd: DNS-Based Service Discovery (RFC 6763)

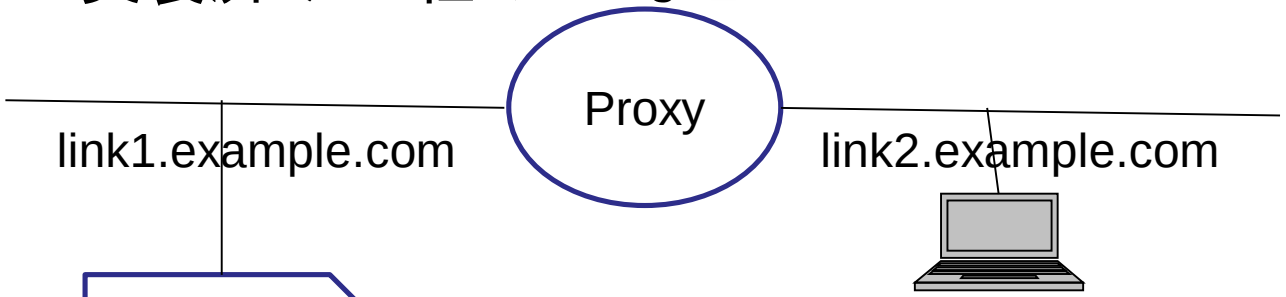
- 構造化されたサービス名
  - <Instance>.<Service>.<Domain>
  - SRVと同じ形式 (_sip._udp.domain)
  - ホスト名と違い、スペースやUTF-8も許可
- サービスの列挙 (enumeration)
  - サービス名に PTRを書き、サービスを列挙
  - _http._tcp.dns-sd.org PTR ¥032*¥032eBay,¥032online¥032auctions._http._tcp.dns-sd.org.
- サービスへのアクセス
  - SRV RRを使用
  - _http._tcp.dns-sd.org. SRV 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
  - ローカルリンクにあるプリンタを使いたいとき
  - _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

    _ipp : Internet Printing Protocol
  - 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

Copyright © 2017 Japan Registry Services Co., Ltd.

dnssd: 提案プロトコル

- draft-ietf-dnssd-hybrid
  - dnssd コアプロトコル
  - mDNSと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

Copyright © 2017 Japan Registry Services Co., Ltd.

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、既に使用可能
  - 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、メールアドレスに対応する証明書を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

Copyright © 2017 Japan Registry Services Co., Ltd.

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

Copyright © 2017 Japan Registry Services Co., Ltd.

脆弱性に焦らないDNS運用

Copyright © 2017 Japan Registry Services Co., Ltd.

よく使用されているDNSソフトウェア

- BIND 9 (named)
- NSD
- Unbound
- Knot DNS
- Knot resolver
- PowerDNS
- PowerDNS recursor
- Microsoft社製品 (Microsoft DNS server)
- Nominum社製品 (Vantio)

Copyright © 2017 Japan Registry Services Co., Ltd.

最近の脆弱性(CVE- Common Vulnerabilities and Exposures)報告数

開発元		ISC	NLnet Labs			PowerDNS.COM BV		CZ.NIC Labs	
ソフトウェア名		BIND 9	NSD	Unbound	Idns	PowerDNS	PowerDNS Recursor	Knot DNS	Knot Resolver
機能		Auth +Resolver +Lib	Auth	Resolver	Lib	Auth	Resolver	Auth	Resolver
CVE 報告数 (同時に複数報告されることあり)	2007	6	0		0	0	0		
	2008	3	0		0	2	2		
	2009	4	1	2	1	0	2		
	2010	9	0	1	0	0	0		
	2011	6	0	2	1	0	0		
	2012	8	2	1	0	1	1	0	
	2013	4	0	0	0	0	0	0	
	2014	5	0	1	1	0	2	0	
	2015	9	0	0	0	4	2	0	
	2016	12	1	0	0	8	3	1	0
	2017	4	0	0	0	0	0	0	0

CVE databaseが更新されず、Reservedのものがあるため、報告数は違う場合がある (特にPowerDNS)

Copyright © 2017 Japan Registry Services Co., Ltd.

2016年1月からのBIND 9(named)脆弱性公開日

- 2016/1/19:　遠隔から停止 (2件, Remotely, High)
- 2016/3/9:　遠隔から停止 (3件, Remotely, High)
- 2016/9/27:　遠隔から停止 (Remotely, High)
- 2016/10/20:　遠隔から停止 (ただし古いパッケージ限定)
- 2016/11/1:　遠隔から停止 (Remotely, High)
- 2017/1/11:　遠隔から停止 (4件, Remotely, High)
- 2017/2/8:　遠隔から停止 (DNS64とRPZの両方使用)
- 2017/4/13:　遠隔から停止 (3件, Remotely, High)
- 最近のものは停止する脆弱性のみ、年に4~6回

Copyright © 2017 Japan Registry Services Co., Ltd.

BIND 9での脆弱性公開後の猶予

- 脆弱性情報そのものやソースコードの差分を読むと容易に再現できるため、公開と同時に攻撃が広まる
  - bin/tests/system/ のシステムテストに過去の落とし方が明記
  - Malformed packet一発で落とせるものはncコマンドで可能

    printf "¥0¥1¥0¥0¥0¥1¥0¥0…." | nc -u IPアドレス 53
- 脆弱性情報公開時刻
  - USの平日業務時間帯 (日本時間で午前4時～8時が多い)
  - USの金曜に公開されると日本では土曜日
- 火曜から土曜の午前中に、すぐに、失敗せずに修正版に入れ替える必要がある → 対応しないと落とされる可能性あり

Copyright © 2017 Japan Registry Services Co., Ltd.

(BIND 9の)脆弱性に焦らないDNS運用

1. 第三者のサービス
2. サポートがしっかりした製品やアプライアンス
3. BIND 9のサポート契約
4. (自前でやる場合)

Copyright © 2017 Japan Registry Services Co., Ltd.

1. 第三者のサービス

- 権威DNSサーバ: DNSサービスを使用
  - 独自開発や、落ちないシステム構成
  - A社、A社、C社、D社、G社、N社など
  - DDoS対策を考えるとおすすめ
  - 1社では1TbpsのDDoSに耐えられない可能性があるので、複数契約して併用するとよい (大手へのDDoSの巻き添えがありうる)
- フルリゾルバ: Public DNS サービスを使用
  - G社とかO社
  - 彼らのIPアドレスをDHCPなどで配布する
  - クエリ名・タイプ・IPアドレスの情報をすべて明け渡すことになる

Copyright © 2017 Japan Registry Services Co., Ltd.

2. 製品やアプライアンス

- Nominum製品

- BIND 9を使うアプライアンスでも、まともな製造者であれば BIND 9のサポートを買っているはずなので、脆弱性情報を事前に入手して、一般公開と同時にアップデートしてくれるはず

Copyright © 2017 Japan Registry Services Co., Ltd.

3. (BIND 9の)サポート契約

- 脆弱性情報の事前提供サービス
  - 3～5日前に情報を得られる
  - www.isc.org → "Support" → "BIND Support" → "Advance Security Notification"
  - 引用: TIME is your most critical tool in Internet Security

Copyright © 2017 Japan Registry Services Co., Ltd.

4. (自前で)脆弱性に焦らないDNS運用

- 脆弱性が少ない実装を使用する
- 複数の実装を組み合わせる (多様性)
  - BIND 9の脆弱性は、侵入されるものは少なく、サービス停止が多い
  - BIND 9とNSD/Unbound同時に脆弱性報告が出ることはほぼない
  - DNSは冗長構成を組みやすいシステムである
  - 複数のDNSサーバのうち一つ止まっても文句を言われない組織向け
  - 全体としてサービスが止まらなければよい
    - すべてのサーバが動いていないと文句をいう人がいる場合は金をかけてください

Copyright © 2017 Japan Registry Services Co., Ltd.

権威DNSサーバ編

- マスターサーバ (プライマリサーバ)
  - BIND 9の便利な機能を使っているのであればそのまま使う
  - 設定手順を変更するのは大変
  - マスターを隠し、ゾーン転送元として使うのがよい (hidden master)
- スレーブサーバ (セカンダリサーバ)
  - BIND 9, NSD, Knot DNSなどを組み合わせる
- 脆弱性が公開されて攻撃を受けると、マスターサーバが停止する可能性があるが、スレーブサーバは稼動を続ける
  - スレーブが生きているので名前解決は可能
  - 落ち着いて対策すればよい
  - 停止の検知はしておくこと

Copyright © 2017 Japan Registry Services Co., Ltd.

権威DNSサーバ構成例

- マスターサーバ: BIND 9
  - BIND 9の脆弱性公表で落とされるかもしれないのでインターネットからは隠しておくとよい (hidden master)
- 自営のセカンダリサーバ
  - BIND 9, NSD, Knot DNS を組み合わせる
  - マスターがBIND 9でhidden master構成にできない場合は、NSDやKnot DNSを使用する
- セカンダリDNSサービス
  - 脆弱性公表と同時に対応する、はず
  - SINETさんも提供

Copyright © 2017 Japan Registry Services Co., Ltd.

例: NSD

- package systemなどからNSDを導入する
- nsd.conf の例 (最小限)

```
server:
        ip-address: 192.0.2.1          # サーバのIPアドレス
remote-control:
        control-enable: yes            # nsd-control-setup
zone:
        name: "example.jp"
        zonefile: "/etc/nsd/slave/example.jp"
        request-xfr: 192.0.2.2 NOKEY  # IPアドレスで指定
        allow-notify: 192.0.2.2 NOKEY # notifyも明示的に指定
```

Copyright © 2017 Japan Registry Services Co., Ltd.

フルリゾルバ編

- 複数の実装(例えば、BIND 9とUnbound)のフルリゾルバを準備しておく
- /etc/resolv.conf や DHCP では普通は複数のフルリゾルバのアドレスを指定するので、用意した複数のフルリゾルバのアドレスを指定する
- 攻撃を受け、BIND 9フルリゾルバが停止しても、Unboundは同時には停止しない
  - 今どきのクライアントは、片方が停止していると、短時間でもう一方に切り替え、遅延を感じないものが多い
- 停止の検知はしておくこと

Copyright © 2017 Japan Registry Services Co., Ltd.

例: Unbound

- package systemなどからUnboundを導入する
- unbound.conf の例

```
server:
        interface: 192.0.2.10    # サーバIPアドレス
        msg-cache-size: 512m  # cache sizeを大きく
        rrset-cache-size: 512m # cache sizeを大きく
        infra-cache-numhosts: 100000 # host cache sizeを大きく
        #auto-trust-anchor-file: "/etc/unbound/root.key" # DNSSEC
remote-control:
        control-enable: yes # unbound-control-setupを実行
```

Copyright © 2017 Japan Registry Services Co., Ltd.

事例: ns.tokyo.wide.ad.jp (1)

- 変更前
  - wide.ad.jpは、すべてのNSがBIND 9
  - ns.tokyoはBIND 9で権威サーバ・フルリゾルバ共存という古い設定
  - wide.ad.jp、関連ドメイン名、逆引き、いくつかの大学・企業のセカンダリ
- 変更計画
  - マスター(ns-wide.wide.ad.jp)と別ISPにあるサーバ(mango.itojun.org)を変更しない
  - ns.tokyoの従来のIPアドレスをフルリゾルバにして、Unboundに変更
    - /etc/resolv.conf に設定してるユーザがそれなりにいたため
  - ns.tokyo.wide.ad.jp に別IPアドレスを割り当てて、NSDに変更

Copyright © 2017 Japan Registry Services Co., Ltd.

事例: ns.tokyo.wide.ad.jp (2)

- 2016/3 開始: 新IPアドレスとVMの用意、NSD起動
- 2016/6~8: 大学・企業のセカンダリのゾーン転送設定変更を依頼、変更完了待ち (この間、BIND 9とNSD両方に転送)
- 2016/9: ns.tokyo.wide.ad.jpのIPアドレス変更(JPレジストリ設定)
  - BIND 9の動くVMからNSDが動いているVMへ
  - 数日待ち
- 2016/9: 従来のIPアドレスをフルリゾルバ専用のUnboundに変更
- 結果
  - BIND 9の脆弱性が悪用されても ns.tokyoは NSDなので wide.ad.jpの名前解決が失敗することは避けられるようにできた
  - マスターサーバの設定変更手順などは変更なし (BIND 9のまま)

Copyright © 2017 Japan Registry Services Co., Ltd.

まとめ

- DNSの運用に疲れたら、サービスの利用を考えましょう

- 自分でやるつもりであれば、複数の実装を組み合わせましょう
  - DNSは冗長構成を組みやすいプロトコルです
  - 今どきのクライアントは優秀です

Copyright © 2017 Japan Registry Services Co., Ltd.

参考資料

- NLnet Labs (NSD, Unbound): www.nlnetlabs.nl
- Knot DNS: www.knot-dns.cz

Copyright © 2017 Japan Registry Services Co., Ltd.