IETF/RFC動向
(続)DNSプロトコルの進化 2022

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 2022, DNS DAY
2022年11月29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
  - Internet Week プログラム委員 (2016～)
- IETFでの活動 (2004~)
  - ENUMプロトコル: RFC 5483 6116
  - メールアドレスの国際化 :RFC 5504 5825 6856 6857
  - DNS関連の問題提起など
    - RFC 7719, 8499: DNS Terminology → rfc8499bis
    - RFC 8198: DNSSECを用いた名前解決の性能向上
    - draft-ietf-dnsop-avoid-fragmentation: DNSでIP断片化を避ける提案

本日の概要

- Internet Week 2020 DNS DAYにてDNSプロトコルの進化 2020 (IETFでの標準化) を紹介し、2021年に変化を紹介した
- 本日は、2021年11月から1年間の変化を紹介する

- DNS関連のRFCが多数発行される見込みであったが、TLS WGが標準化しているTLS ESNI (Encrypted Client Hello) の標準化が遅れており、依存関係にあるRFCの発行が遅れている
  - 依存関係: TLS ESNI← dnsop-svcb-https ← add-svcb-dns, add-ddr ← add-dnr

DNSプロトコルの標準化を行うWGなど

- dnsop (DNS Operations) 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←dnsext WG
  - 1999年以前に設立
- dprive (DNS Private Exchange) WG
  - DNS通信路を暗号化
- dane (DNS-based Authentication of Named Entities) 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
- dance (DANE Authentication for Network Clients Everywhere) WG
  - DANEでTLSクライアント認証するプロトコル
  - 2021年9月設立
- dnssd (Extensions for Scalable DNS Service Discovery) WG
  - .localを使用するMulticast DNS (RFC 6762), DNS-SD (RFC 6763)の拡張
  - 2013年10月設立、コアプロトコルは完了
- doh (DNS over HTTPS) WG
  - 2018年10月にRFC 8484 DoH発行
  - 2020年3月完了、続く議論をadd WGへ
- add (Adaptive DNS Discovery) WG
  - DNSクライアントがDoT, DoQ, DoHサーバを見つける方法を定義する
  - 2020年3月設立
- IETF WG以外からの標準化
  - Independent submission
  - 対応するWGがない場合
- 赤字は完了したWG　青字は報告対象

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1月～2022年11月で38本
      - 年平均5.5本
      - 2021年11月から1年で4本
    - RFC Editor queueに2本
    - IESG対応中2本
    - 議論中のWG draft 13本

- 発行されたRFC
  - 2021/11/18:RFC 9156 qname minimisation
  - 2021/11/30: RFC 9157 DNSSEC algorithm
  - 2022/3/22: RFC 9210 (BCP 235) DNS/TCP
  - 2022/8/11: RFC 9276 (BCP 236) NSEC3
- RFC Editor Queue
  - SVCB/HTTPS
  - DNSSEC BCP
- IESG Review中
  - Use of GOST 2012 in DNSSEC
  - DNS Catalog Zones
- 議論中のもの
  - glue-is-not-optional
  - DNS用語集
  - caching-resolution-failures
  - alt TLD
  - DNS error reporting

dnsop WG: 発行されたRFC

- RFC 9156, 2021/11/18: DNS Query Name Minimisation to Improve Privacy (Proposed Standard)
  - QNAME minimisation (問い合わせ情報の最小化)を標準プロトコルに
  - 従来のRFC 7816はExperimental 実験プロトコルであった
  - 多くのフルサービスリゾルバに実装済
- RFC 9157, 2021/11/30: Revised IANA Considerations for DNSSEC (Proposed Standard)
  - DNSKEY/DSのアルゴリズム追加を Standards TrackではなくRFC required とすることで、Informational でもよいことにする (実装はMAY)
    - 各国政府が決めた暗号をDNSSECで使う場合 (他国では検証すらしなくてよい)
    - 実装がMUSTなものはStandards Trackが必要 (→ 耐量子暗号など)
- RFC 9210 (BCP 235), 2022/3/22: DNS Transport over TCP - Operational Requirements
  - DNSでのTCP通信路についての運用上の要求仕様

RFC 9276: NSEC3パラメータ推奨値の変更

- 2022/8/11, Best Current Practice　すぐにも実装される可能性がある
- 署名側: SHOULD: Iteration 0, SALT 空
  - 必要がなければNSEC3を使わないこと / NSECにすること
  - 0でも1回はSHA1でハッシュするので0で必要十分である
  - NSEC3 Opt-Outは、大きなゾーンで、頻繁に変化し、DSありの委任が少ない場合に使ってよい　(DNSSEC対応ドメイン名が少ないTLDなど)
- 検証側
  - iteration が 0 以外の場合、insecure/SERVFAILを返してよい
    - insecureは、DNSSEC検証せずに名前解決する (ad=0)
  - Extended DNS Errorを返す (value 27)
- TLDでの現在の設定
  - com net shop tokyo　iteration=0 salt=“”
  - org　iteration=0 salt=332539EE7F95C32A
  - jp　iteration=8 salt=49D8ED6F2F

SVCB/HTTPS

- draft-ietf-dnsop-svcb-https: HTTPS/SVCB リソースレコード
  - scheme://サービス名/path の接続情報をSVCB/HTTPS RRに書く
    _scheme.サービス名. IN SVCB SvcPriority TargetName SvcParam
    サービス名. IN HTTPS SvcPriority TargetName SvcParam（httpsの場合）
    - SvcPriority: 0はAliasMode、それ以外はServiceModeで、値は優先度
    - TargetName: AliasModeではCNAME先、ServiceModeではサービスのホスト名
    - SvcParam alpn: dot doq h2 h3
    - SvcParam ech: TLS Encrypted Client Hello 制御パラメータ　（TLS ESNIで定義)
    - SvcParam port: サービスのポート番号
  - dnsop WGでの議論は完了し、IESGレビュー完了
  - IESGレビュー後に1点修正: ループを防ぐ修正
  - RFC発行前ではあるが、ブラウザと一部CDNの実装が進んでいる
    - Safari, Firefox, Cloudflare など
  - TLS ESNIを参照しており、RFC発行まで時間がかかる見込み

dnsop WG: IESG提出済

- draft-ietf-dnsop-dnssec-bcp: DNSSEC BCP
  - 現在のDNSSECを実装するために必要なRFCリスト
  - IESGは発行を承認したがrfc5933bisを参照しているため発行待ち
- draft-ietf-dnsop-rfc5933-bis
  - ロシアのGOST 2012署名アルゴリズムをDNSKEY/DS/RRSIGで用いる
  - DS digest 32バイト (SHA256と同じ), key/sig 512バイト
  - 実装はOPTIONAL
  - IESGがレビュー中
- draft-ietf-dnsop-dns-catalog-zones: DNS Catalog Zones
  - DNS primaryからsecondaryに複数のゾーンの設定を伝えるもの
    - BIND 9のnamed.confのsecondary zone設定など / nsd.conf のゾーン設定など
  - IESGがレビュー中

dnsop WG (現在の議論状況)

- draft-ietf-dnsop-glue-is-not-optional: 委任応答でのグルーの要求仕様
  - グルーの定義と、in-domain glue, sibling glueの定義をこちらで行う
- draft-ietf-dnsop-rfc8499bis: DNS Terminology / DNS用語集の更新
  - 委任, glue, in-domain, sibling の定義をglue-is-not-optionalに移動し、参照
  - in-bailiwick, out-of-bailiwick の定義が消える可能性あり
- draft-ietf-dnsop-avoid-fragmentation: Fragmentation Avoidance in DNS
  - DNS/UDPでIP断片化(Fragmentation)を使わないようにしようという提案
  - dnsop Working Group Last Call を通過して進んでいるといわれているが、まだ
  - LinuxにはIPv4でIP_DFビットをセットする良いAPIがないという指摘
  - 1400/1232といったマジックナンバーについて議論が終わった気がしない

dnsop WG IETF 115での議論

- draft-ietf-dnsop-alt-tld: .alt TLD
  - Tor向け.onionのようなTLD予約を懸念し、.alt TLDの下で対応する提案
  - RFC 6761 Special-Use Domain Nameとしての予約であり、2014年から議論を継続
  - .altの下のセカンドレベルの予約の議論も始まっている
  - 近いうちにWGLCの見込み
- draft-ietf-dnsop-caching-resolution-failures
  - 名前解決中のエラー情報をキャッシュして無駄なクエリを減らす提案
    - SERVFAIL, REFUSED, Timeouts, 委任ループ, CNAMEループ, DNSSEC検証エラー
    - リトライするときに、同じクエリを5秒から、リトライごとに2倍づつの時間待つこと
    - 委任の子側が応答しない場合に、委任の親側の権威サーバに無駄な問い合わせを送らないこと
  - dnsop WGでは好意的だが、しばらく議論を継続する見込み

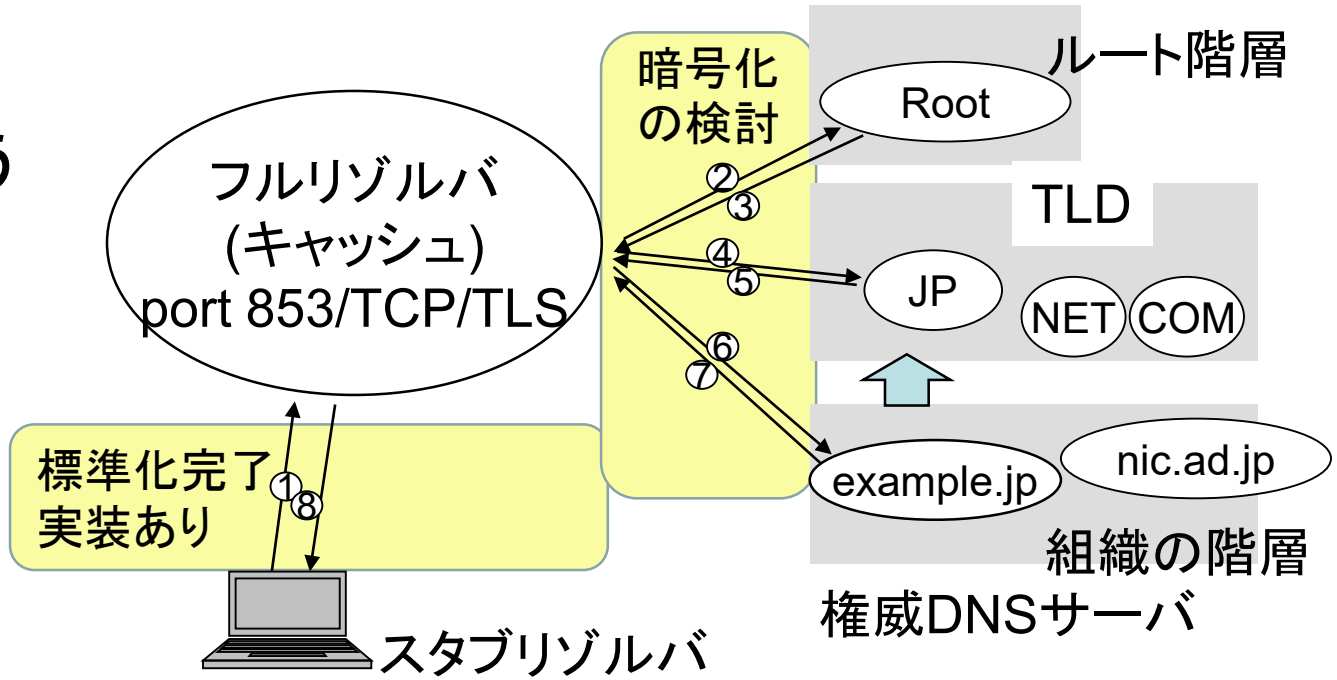
dnsop WG IETF 115での議論

- draft-ietf-dnsop-dns-error-reporting: DNS Error Reporting
  - フルサービスリゾルバから権威サーバにエラーの情報を伝える仕組み
  - 権威サーバの変更: 報告エージェントのドメイン名をEDNS0で応答に追加
  - リゾルバの変更: エラー時にはエラー情報を含むクエリを送信
    - 報告エージェントの情報がある応答を処理中にエラーが出たとき
    - QNAME=_er.エラーコード.QTYPE.QNAME._er.エージェントドメイン名
    - エラーコード: Extended DNS Errors (RFC 8914)
      - 3: Stale Answer, 4:Forged Answer, 6 DNSSEC Bogus, 7:署名失効, 8:署名無効
      - 9 DNSKEYなし 12:NSECなし 15:Blocked　など
    - QTYPE=NULL
    - 例: _er.7.1.broken.test._er.a01.reporting-agent.example NULL
  - エージェントドメイン名の権威サーバでクエリログを取得すれば、エージェントオプションを追加した権威サーバからの応答が関連する名前解決でエラーが起きたことがわかる
  - IETF Hackathonで複数の権威サーバ、リゾルバに実装され、実装経験がdraftにフィードバックされている: NULLからTXTにするなど

dprive (DNS Private Exchange) WG

- DNSの通信をTLSで暗号化
- 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 over DTLSは使われていない →廃棄して853/UDPを転用
- ゾーン転送をDNS over TLSで行う拡張は完了 (2021)
  - DNS Zone Transfer-over-TLS
  - サーバ証明書でサーバ名確認など
- 2022/5/11 UDPポート853を使うDNS over QUIC標準化完了

- 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、議論が続いている。



dprive WG: 2021/11～2022/11のRFC

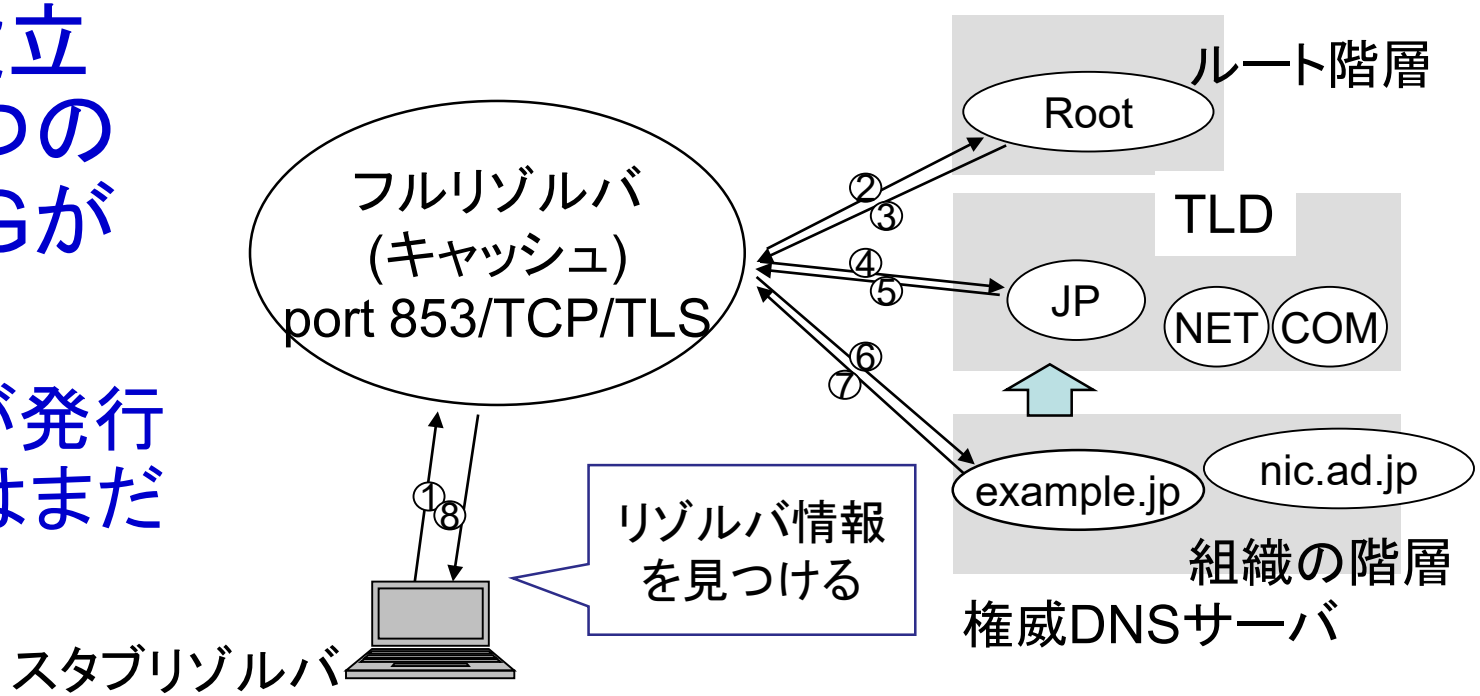
- RFC 9250, 2022/5/11: DNS over Dedicated QUIC Connections
  - TCP通信路形式のDNSプロトコルをUDP port 853のQUIC接続で通す
    - 2オクテット(network byte order)のパケット長と、DNSパケットを送る
  - DNS over TLS (DoT) と同じ使い方

dprive WG IETF113-115での議論

- 2021年に議論されていたDS, SVCBに権威サーバのDoT/DoQ/DoH情報を入れるという提案が破棄された
  - 子側に書くと、ネームサーバ名情報が洩れる
  - 親側に入れるには現在のDNS/DNSSECを大規模に変更する必要あり
- 現在の提案: draft-ietf-dprive-unilateral-probing-02
  - Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS : リカーシブサーバから権威サーバへの暗号通信の一方的な日和見的な実装
  - 対応する権威サーバは、port 853でDoT、DoQで応答すること (SHOULD)
  - 名前解決時に権威サーバへDoT/DoQ接続し、接続できなければ通常のUDP/TCP port 53で問い合わせる
  - DoT/DoQで接続できた・できないという情報をキャッシュしておく
  - 証明書検証はしない (検証失敗でも拒否してはならない (MUST NOT))
  - PowerDNS が実装 (powerdns_recursor と powerdns.com の権威サーバ)
    - 例: dig +tls @pdns-public-ns1.powerdns.com. powerdns.com NS
  - 現在は別の実装を待っている状態で、複数の実装があれば、自信をもって進められる
  - 2023年1月にWGLCをかけ、決めようとしている

add (Adaptive DNS Discovery) WG

- DoT, DoQ, DoHサーバ情報を見つける方法を標準化するWG
- 2020年3月に設立
- 次のページで説明する設立前から提案されていた2つの実装案は合意され、IESGが発行承認した
  - 参照するSVCB/HTTPSが発行されないため、RFC発行はまだ先
- 現在は、企業内などのsplit horizon DNSなどへの対応を議論中



add WG 提案プロトコル

- draft-ietf-add-svcb-dns: SVCBにDNS情報をいれる仕組み
  - _dns.ドメイン名にSVCB　　alpn=dot,doq,h2,h3　SvcParamにdohpathを追加
- draft-ietf-add-ddr: Discovery of Designated Resolvers
  - 従来のリゾルバに、_dns.resolver.arpa SVCBを問い合わせると、DoT/DoH/DoQリゾルバ情報を得られる仕組み

  _dns.resolver.arpa. 7200 IN SVCB 1 dot.example.net (alpn=dot,doq port=853)

  _dns.resolver.arpa. 7200 IN SVCB 1 doh.example.net (alpn=h2,h3 dohpath=/dns-query{?dns})
- draft-ietf-add-dnr: DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)
  - DHCPv6, DHCPv4, IPv6 RAに、Encrypted DNS optionを追加
  - authentication-domain-name (証明書ドメイン名), IPアドレス
  - SvcParams (alpn=dot,doh,h2,h3 ech=<ESNIで定義> dohpath=/dns-query{?dns})
- これら3本はIESGで発行承認された
  - IANAがEncrypted DNS (DNR) optionの値を割り当てたため、実装可能
- TLS ESNI, SVCB/HTTPSを参照しており、RFC発行まで時間がかかる見込み

その他のDNS、ドメイン名関連RFC

- RFC 9233, 2022/3/31: Internationalized Domain Names for Applications 2008 (IDNA2008) and Unicode 12.0.0
  - Unicode 6.0.0時のIDNA2008をUnicode 12.0.0対応にする変更点
  - Standards Track
- RFC 9230, 2022/6/8: Oblivious DNS over HTTPS
  - クライアントでクエリを暗号化し、proxy経由で送信元を秘匿するもの
  - Experimental 実験プロトコル、著者の所属はApple, Fastly, Cloudflare
- RFC 9267, 2022/728: Common Implementation Anti-Patterns Related to Domain Name System (DNS)
  - DNS実装時に間違いやすい点を紹介
  - IETF外からのsubmissionで、Informational

まとめ

- dnsop WG
  - 従来のRFCの問題点解決、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
  - DNSソフトウェア開発者、ブラウザ開発者、CDNなどの開発者が多数集まっている
- dprive WG
  - クライアントからフルリゾルバ間、ゾーン転送の通信路暗号化の標準化は完了し、すでに使用可能
  - DNS over QUICが利用可能に
  - フルリゾルバから権威DNSサーバ間の暗号化を進めており、できるところから暗号化するというプロトコルを進めている
- add WG
  - DHCP, RAの拡張と_dns.resolver.arpa方式の議論は完了したが、RFCの発行はまだ
- dnssd
  - Multicast DNSを複数セグメントで使用する拡張が標準化された
  - さらなる機能追加は停滞中
- IETF
  - 既存プロトコルの問題点の指摘や新しい提案は歓迎される

参考

- www.ietf.org → datatracker.ietf.org
  - IETFミーティングの資料、議事録
  - ワーキングループの情報
    - 標準化したRFCへのリンク
    - 議論中のdraftへのリンクや状態
    - メーリングリストアーカイブ
- www.rfc-editor.org
  - RFC