DNSとドメイン名に関連した標準化の動向(IETF)
(続)DNSプロトコルの進化 2021

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 2021, DNS Day
2021年11月19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) を紹介した。
- 本日は、2020年11月から1年間の変化を紹介する

DNSプロトコルの標準化を行うWGなど

- IAB (Internet Architecture Board)
  - IETFやインターネット技術全般にわたる方向性を示す
- 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から引き継ぎ
  - 1999年以前に設立
- dprive (DNS Privacte Exchange) WG
  - DNS通信路を暗号化
  - 2016年5月にRFC 7858 DNS over TLS (DoT) を発行
  - ゾーン転送の暗号化を完了
  - 2019年ごろから権威サーバとの通信のDoT/DoQに取り組んでいる
- 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
- 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
  - Apple Bonjourで使っている追加機能の標準化が残る
- 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, 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　青字は変化

IABによる.arpaドメイン名の運用の変更

- RFC 9120: Nameservers for "arpa" Domain
- IABにより、2021年10月に発行
- arpa (Address and Routing Parameter Area) TLDの運用をRootと分離する
  - 内部名の a.ns.arpa, b.ns.arpa, c.ns.arpa … に委任する
- 理由: IETFからのarpaドメイン名の変更提案が、rootの運用に影響するとして通らなかったことがあったため
- 分離する方針のみ書かれていて、計画は書かれていない
  - 今後、移行計画が示されるはず
- 利用者への影響: 影響がないように移行可能

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～2021年11月で33本/6年
    - (2020年11月から1年で5本)
    - RFC Editor queueに2本
    - IESG対応中2本
    - WG draft 10本
- 最近のdnsop WGでのテーマ
  - 標準の明確化と修正
    - DNS用語
    - クエリ名情報漏洩の最小化
    - DNSSECアルゴリズム
    - DNS Cookies, TSIG, NSECなどの修正
  - 新しい要求
    - HTTPS系サービスを提供するための、新しいリソースレコード (SVCB, HTTPS)
  - セキュリティ対策
    - ゾーン情報のダイジェスト
    - 委任情報確認の厳格化
    - Delegation only
    - IP断片化回避

dnsop WG: 2020/11～2021/11のRFC

- RFC 8945, 2020/11/30: Secret Key Transaction Authentication for DNS (TSIG)
  - RFC 2845 TSIG プロトコルの脆弱性修正 (DNSでの共有鍵認証方式)
- RFC 8976, 2021/2/9: Message Digest for DNS Zones (ZONEMD)
  - ゾーン全体の情報のハッシュ値を保持するZONEMD RRを定義 (IW2020で紹介)
  - DNSサーバソフトウェアでの実装が進んでおり、ルートサーバでは将来的に使用される
- RFC 9018, 2021/4/5: Interoperable Domain Name System (DNS) Server Cookies
  - DNS Cookies のうちサーバCookieの相互運用性を改善 (従来は実装依存だった/Anycast困難)
- RFC 9077, 2021/7/22: NSEC and NSEC3: TTLs and Aggressive Use
  - NSEC, NSEC3のTTL値の扱いを改善する標準で、DNSSEC, RFC 5155 (NSEC3), RFC 8198 (不在情報を用いた性能改善) を更新するもの
- RFC 9108, 2021/9/8: YANG Types for DNS Classes and Resource Record Types
  - YANGデータモデルを扱うためにDNSにYANGクラスとYANGタイプを追加
- RFCの欠陥を改善するRFCは、DNSサーバソフトウェアに実装されたら使えばよい

dnsop WGで検討が終わったドキュメント

- HTTPS SVCB リソースレコード
  - 詳細はこのあとのセッションで
  - dnsop WGでの議論は完了し、IESGに提出、レビュー中
  - _dns.サーバ名 SVCB 1 サーバ名 alpn=dot ネームサーバがDoT対応
- draft-ietf-dnsop-rfc7816bis
  - 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
  - RFCとしての発行を承認され、RFC Editorの手続き待ち
- draft-ietf-dnsop-dnssec-iana-cons
  - 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)
    - ロシアの新しいGOST algorithmをInformational RFCにし、実装をMAYとする
    - RSASHA256のように実装がMUSTなものはStandards Trackが必要
  - RFCとしての発行を承認され、RFC Editorの手続き待ち

dnsop WG (現在の議論状況)

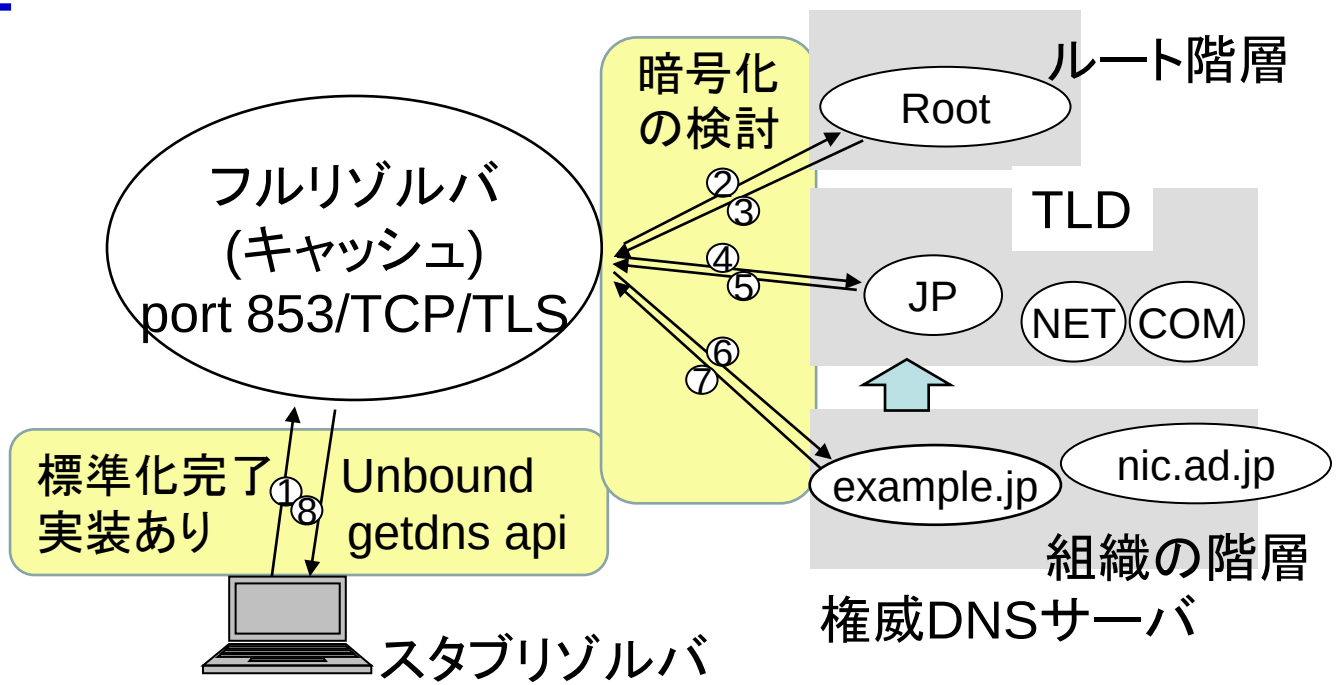
- draft-ietf-dnsop-glue-is-not-optional
  - https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-glue-is-not-optional
  - 委任応答でのグルーはオプションではなく必須情報である
  - NS, DS, RRSIG(DS)だけ応答してグルーが空だと名前解決に失敗することがある
  - グルーがすべて入らなければTC=1 (Truncation)とし、TCPで再問合せ
  - 概ね合意されている
- draft-ietf-dnsop-avoid-fragmentation
  - https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-avoid-fragmentation
  - DNS/UDPでIP断片化(Fragmentation)を使わないようにしようという提案
  - 概ね合意、詳細部分を要修正

dnsop WG IETF 112での議論

- draft-ietf-dnsop-nsec3-guidance: NSEC3パラメータの推奨値の変更
  - https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-nsec3-guidance
  - NSEC3の機能を使っていないならNSECを使うこと
  - 小さいゾーンではOpt-Outをしないこと
  - Iteration を 0 とすること (SHOULD)
  - DNSSEC検証時、Iterationが大きいと検証しないとかエラーにするなど
  - 合意される見込み
- DNSを使ったドメイン名の認証のsurvey報告
  - https://datatracker.ietf.org/doc/html/draft-sahib-domain-verification-techniques-02
  - TXTやCNAMEに指定されたものを追加することでドメイン名の管理権限を持つことを確認する
  - ドメイン認証のサーバ証明書発行などで使用される (例: ACME dns-01認証)
- DNS Catalog Zones
  - https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-dns-catalog-zones
  - セカンダリサーバなどの設定をゾーンファイルに書けるようにする仕組み
  - 複数の実装で設定方式が違っても、同じ仕組みでセカンダリサーバの設定ができるようになる (のでうれしい、というコメントがあった)
  - 著者にDNSソフトウェア実装者が4人いるので、実装が進んでいる。合意される見込み

add (Adaptive DNS Discovery) WG

- DoT, 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
- 設立前から提案されていた二つの実装案は概ね合意されつつあり、WGLC (Working Group Last Call)が近い



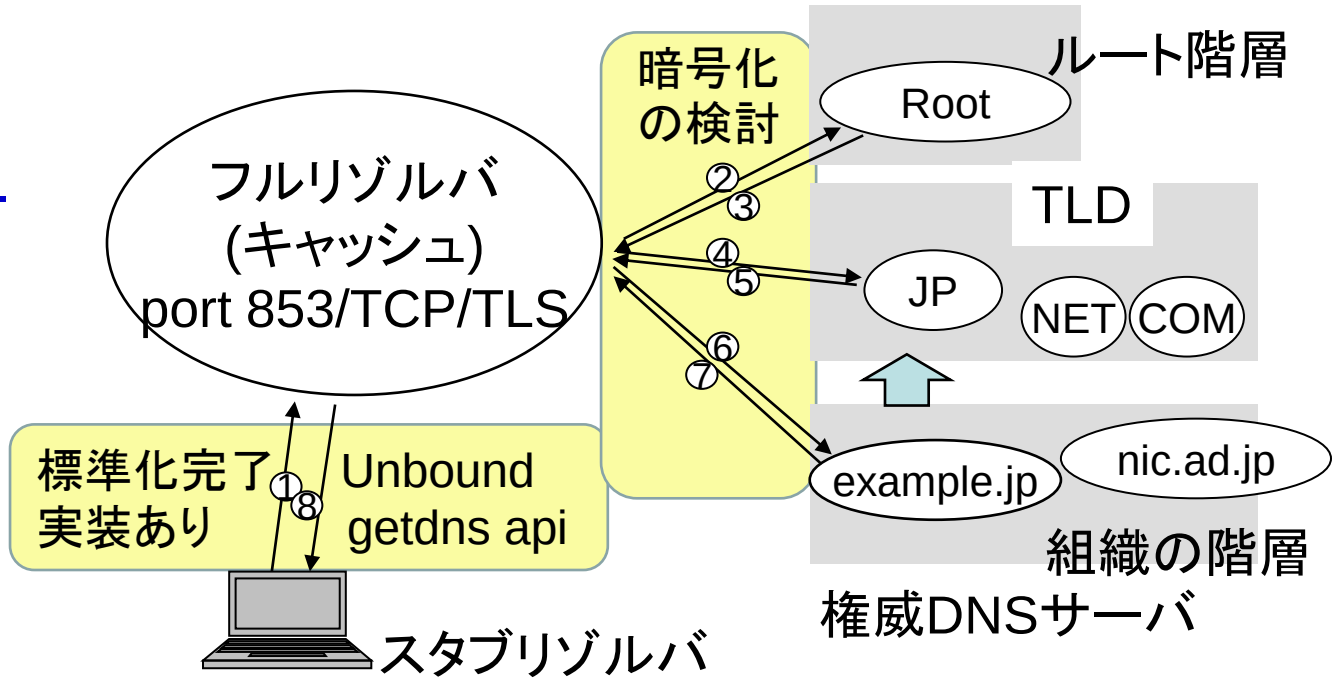
add WG 提案プロトコル

- 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リゾルバ情報を得られる仕組み
  - 例: _dns.resolver.arpa. 7200 IN SVCB 1 doh.example.net (alpn=h2 dohpath=/dns-query{?dns})
  - 例: _dns.resolver.arpa. 7200 IN SVCB 1 dot.example.net (alpn=dot port=8530)
  - クライアントに指定されているリゾルバIPアドレスが知っているものだったら対応するDoT/DoHを使うという実装があったが、それを自動化するもの
- 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), IPv4/v6アドレス, SvcParams
    - SvcParamsは、SVCBと同じでalpn、port、dohpathなどを含む
- この2本は概ね合意されつつあり、近いうちに標準化手続きに入る見込み

dprive (DNS Privacate 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
  - 詳細は本日のDoT/DoH入門参照
- DNS over QUICは継続
- DNS over DTLSは使われていない
  - DNS over DTLSを廃棄して、UDPポート853をDNS over QUICで使う提案
- ゾーン転送をDNS over TLSで行う拡張は完了
  - DNS Zone Transfer-over-TLS
  - サーバ証明書でサーバ名確認など

- 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、IETF 112(2021/11)でも、複数の実装案の議論が継続されている



dprive WG: 2020/11～2021/11のRFC

- RFC 9076, 2021/7/22: DNS Privacy Considerations, Informational
  - 現在のDNSでのプライバシー問題を分析したもの
  - RFC 7626の置き換え
- RFC 9103, 2021/8/23: DNS Zone Transfer over TLS, Proposed Standard
  - ゾーン転送で、DNS over TLS を使用できるようにするもの
  - ゾーン転送を暗号化できる (従来のゾーン転送は平文のみであった)
  - ゾーン転送のアクセス制限に証明書情報を使用できる
  - DNSサーバソフトウェアで実装される見込み、実装されたら使用可能に

dprive WG IETF112での議論 (1)

- DNS over DTLS ではUDPポート853を使うことになっているが、廃棄して、UDPポート853をDNS over QUICに再割り当てしたい
- 権威サーバがDNS over TLSに対応していることを調べる方法
  - 案1: UDP/TCP port 53への接続のかわりに、TCP/853へ接続してみて応答があったらDoTを使う (接続可能情報をキャッシュする)
  - 案2: _dns.ネームサーバ名 SVCB alpn=dot があるとDoTで接続 (h2ならDoH, h3ならDoQ)
    - 案2a: _dns.ネームサーバ名 SVCBを子側に書く → ネームサーバ名の問い合わせが平文となる
    - 案2b: _dns.ネームサーバ名 SVCBを親側に置く
      - 案2b1: 新しいリソースレコードを定義して、権威サーバの動作を変更 (ドメイン名登録、EPP、権威サーバすべて大規模に変更)
      - 案2b2: DSにSVCBの情報をかけるように改造 (DS hack方式)

dprive WG IETF112での議論 (2)

- DS hack方式の主張
  - DSにVERBATIMタイプを追加: Digest dataのところにハッシュではなく、可変長のバイナリデータをそのまま書く
  - バイナリデータとして、”_dns.ネームサーバ名 SVCB” リソースレコードを書く
    - 委任のNSリソースレコードとグルーも書く → 委任情報にも署名を追加
  - EPP, ドメイン名登録, 権威サーバを変更しない
  - DSリソースレコード中に、少し長めのSVCBリソースレコードを含む形となる
  - 名前解決中に得られるDSをみて、DNS over TLS可能であることを識別できる
  - 例

child.example IN NS ns.child.example.
ns.child.example. IN A 192.0.2.53
child.example IN DS <real DS>
child.example IN DS $DSGLUE (_dns.ns, SVCB, [1 ns.child.example. alpn=dot])
child.example IN DS $DSGLUE (., NS, [ns.child.example.])
ns.child.example. IN DS $DSGLUE (ns., A, 192.0.2.53)

- 結論が出るまでまだかかる

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とDNS-SD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
  - 主にApple社のBonjourとAvahiとして実装されているプロトコルをIETFで標準化したプロトコルにするために拡張を行っている
- Multicast DNS (RFC 6762)
- DNS-SD (RFC 6763)
- DNSSDコアプロトコル, 2020/6/22発行
  - RFC 8766 Discovery Proxy / 複数セグメントをProxyで対応
  - RFC 8765 DNS Push Notifications
- RFC 8882: DNSSDプライバシーセキュリティの要求仕様 (2020/9/10発行)

- Apple Bonjourで実装している機能で標準化できてないものを標準化しようとしているが、進みは遅い
  - Multicast DNSの端末がSleep状態でも答えるプロキシー
  - プロキシー耐障害性のための多重化
  - プロキシーへの登録プロトコル
- RFCとして発行したプロトコルや、Apple社の人が提案したドラフトは、まずmacOS, iOS, iPadOSで実装される

その他のDNS関連RFC

- RFC 9102, 2021/8/11発行, TLS DNSSEC Chain Extension, Experimental, Independent submission
  - IETF WG・IAB・IRTF以外で標準化された実験プロトコル
  - DANE TLSAリソースレコードのDNSSEC検証に必要な情報をTLSオプションとして提供するプロトコル
  - TLSで接続すると、DNSSEC検証に必要な情報(DS, DNSKEY, RRSIGなど)をクライアントにまとめて送るので、DNS問い合わせをする必要がなくなるというもの

まとめ

- IABが.arpaの運用方針の変更を示した
- 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の通信路暗号化の標準化は完了し、すでに使用可能
  - ゾーン転送の暗号化は完了
  - フルリゾルバから権威DNSサーバ間の暗号化に取り組んでいる
- add WG
  - DHCP, RAの拡張と_dns.resolver.arpa方式の議論が進んだ
- 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