IETF 117
DNSに関連する最新動向

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 117 報告会, 2023年8月28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~)
  - 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
- 個人的なIETF 117成果
  - WG chairにより、draft 2本のステータスが報告された (IETF 117後IESGへ提出)
- IETF 報告会への参加は2017年 (IETF 98)から6年ぶり

本日の概要

- DNS関連WGの報告
  - dnsop, dprive, add, dnssd WGのここ1年ほどの動向とIETF 117での状況
- IETF/dnsop WGでの2件の特別対応
  - HTTPS/SVCB
  - Fragmentation Avoidance in DNS

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
  - 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
  - RFCを着実に発行中
    - 2016年1月～2023年8月で40本
    - 年平均5.2本
- 発行されたRFC: 1年で3本
  - 2022/8/11: RFC 9276 (BCP 236) Guidance for NSEC3 Parameter Settings
  - 2023/2/14: RFC 9364 (BCP 237) DNSSEC BCP
  - 2023/7/6: RFC 9432 DNS Catalog Zones
- IESG承認済/RFC Editor Queue (3)
  - SVCB/HTTPS
  - glue-is-not-optional
  - alt TLD
- IESG Review (4)
  - rfc5933-bis: Use of GOST 2012 in DNSSEC
  - caching-resolution-failures
  - rfc8499bis: DNS用語集
  - avoid-fragmentation
- WG Consensus (3) / IESG提出準備中
  - zoneversion
  - dns-error-reporting
  - domain-verification-techniques
- 議論中のWG drafts (8)
  - cds-consistency
  - structured-dns-errors
  - dnssec-bootstrapping
  - dnssec-validator-requirements
  - svcb-dane
  - rfc8109bis (Priming)
  - compact-denial-of-existence
  - ns-revalidation

dnsop: RFC, RFC Editor Queue

- RFC 9276 Guidance for NSEC3 Parameter Settings
  - NSEC3パラメータ推奨値の変更
  - 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
    - NSEC3 Opt-OutはTLDなどでは使ってよい
  - 検証側: iteration が 0 以外の場合、insecure/SERVFAILを返してよい
- RFC 9364 DNSSEC BCP
  - DNSSECを実装するために必要なRFCリスト
- RFC 9432 DNS Catalog Zones
  - DNS primaryからsecondaryに複数のゾーンの設定を伝えるもの
    - 権威サーバで、secondary zoneなどの自動設定を行える機能
    - 著者にPowerDNS, CZ.NIC, NLnet Labs, ISCの人々

    → 標準化しながら実装が進んでいるので既に使用可能
- draft-ietf-dnsop-svcb-https
  - HTTPS/SVCB リソースレコードの定義
  - 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）
    - TargetName: AliasModeではCNAME先 (SvcPriority=0)、ServiceModeではサービスのホスト名
    - SvcParam alpn: dot doq h2 h3
    - SvcParam port: サービスのポート番号
- draft-ietf-dnsop-glue-is-not-optional
  - 委任応答でのグルーの要求仕様
  - in-domain glueすべて入らないとTC=1
- draft-ietf-dnsop-alt-tld
  - DNS以外の名前空間でドメイン名を使う場合に、alt TLDの下に名前空間を作れるようにするもの

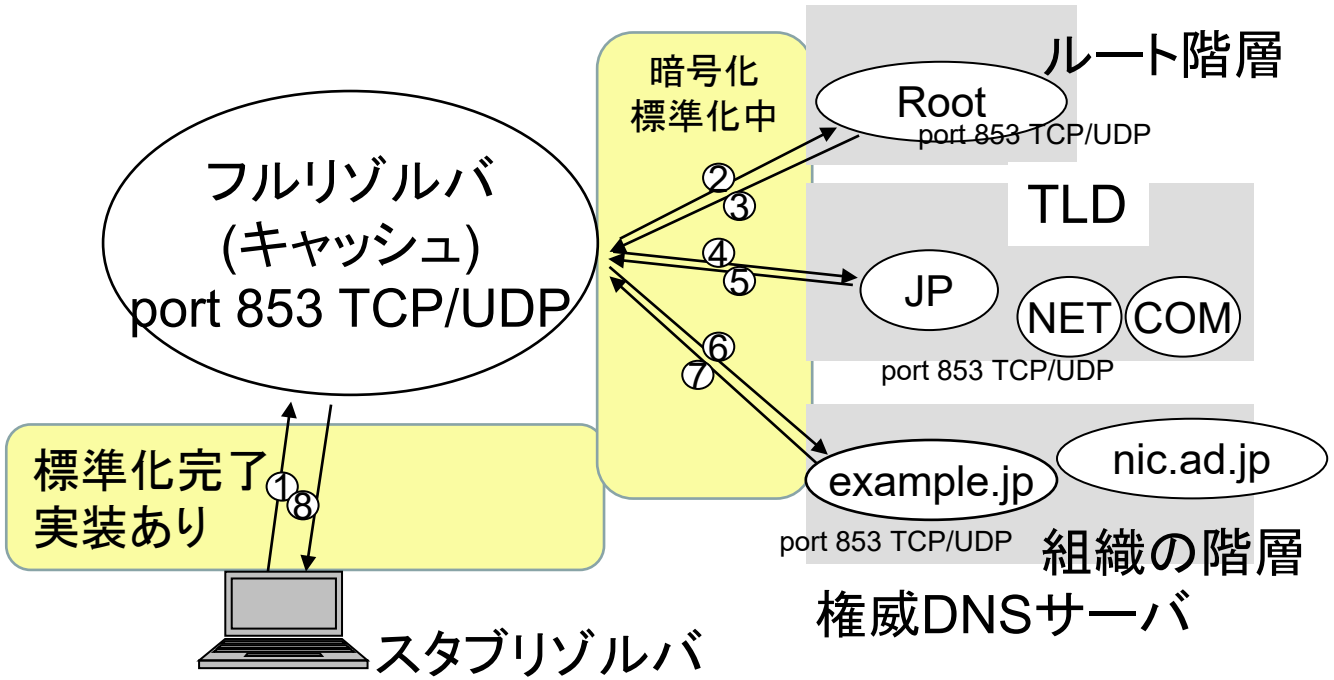
dnsop WG IETF 117での議論

- draft-ietf-dnsop-cds-consistency
  - CDS/CDNSKEY/CSYNC RRでの親側の自動更新を行う場合に、子側の権威サーバすべてからの応答が一致する場合に更新する
  - IETF 117: CSYNCについての記述の不備が指摘され、そのあとドラフトが更新された
- draft-ietf-dnsop-compact-denial-of-existence
  - DNSSECでのNXDOMAIN応答には、クエリ名を含む範囲とワイルドカードを含む範囲を示す2つのNSEC(3) RRとRRSIGが必要
  - ドメイン名が存在しない応答を示すNXNAME RRの提案 (NSEC type bitmapだけで使用)
  - 動的な署名生成時にクエリ名のNSEC RRにNXNAMEビットを立て、NSEC+RRSIG一組返す
    - DNSSEC検証としては名前は存在するが、NXNAMEビットがあるとDNS的には名前が存在しないと読み替える
  - IETF 117: DNSSEC標準との矛盾や解釈できるリゾルバを示す方法がいると指摘があり、今後まだ内容が変わりそうである
- draft-bash-rfc7958bis
  - DNSSEC Trust Anchr (Rootの公開鍵)の公開方法を定義したRFC 7958の更新
  - Erratum対応
- draft-bellis-dnsop-qdcount-is-one
  - DNSのクエリセクション数QDCOUNTは0か1
  - IETF 117: DNS cookieで0を使うことや、DNSSD実装の一部で2を使うことが指摘された
- draft-grubto-dnsop-dns-out-of-protocol-signalling
  - Anycast DNSサーバの運用のためにDNSサーバの管理やBGPとの連携をまとめて管理する仕組み
  - IETF 117: DNSに固有の問題かという議論があった (他のプロトコルにも使える)
- draft-thomassen-dnsop-generalized-dns-notify
  - CDS/CSYNC を実装する場合は、DSを変更する機能を持つ組織が定期的にスキャンする必要があるが、スキャンは大変なので、CDSをいれたらNOTIFYを送るという提案
  - IETF 117: 結論はでず、議論を継続する
- draft-huque-dnsop-multi-alg-rules
  - DNSSEC [RFC 4035]では、ゾーンはDS RRのアルゴリズムで署名されている必要がある
  - KSK, ZSKのアルゴリズムが違っていても許容する提案
  - IETF 117: Needs to be solved / 問題解決が必要

dprive (DNS Private Exchange) WG

- DNSの通信をTLSで暗号化
- 2014年10月に設立
- 2016/5/7: RFC 7858
  - DNS over TLS (DoT)
  - TCP port 853
- 2022/5/11: RFC 9250
  - DNS over Dedicated QUIC Connections (DoQ)
  - UDP port 853
- 2021/8/24: RFC 9103
  - DNS Zone Transfer over TLS (XoT)
  - ゾーン転送をDNS over TLSで行う
  - 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が開始された
- 標準化手続きが進んだためIETF 117ではミーティングなし

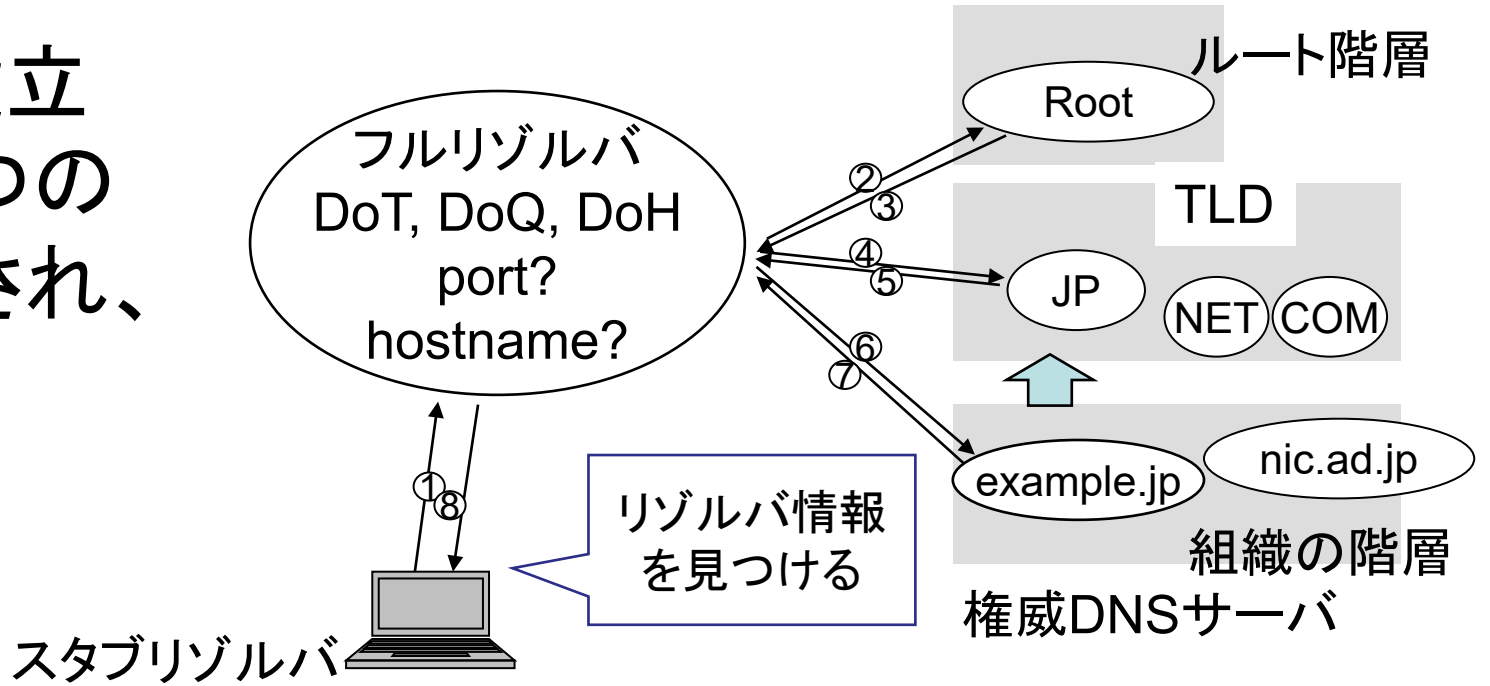


dprive WG の現状 (2023/8)

- 現在の提案: draft-ietf-dprive-unilateral-probing-11
  - Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS
  - フルサービスリゾル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))
  - Experimental (実験) プロトコルとしての標準化
  - dprive WG での議論は完了し、IESGに提出された
    - 2023/8/28 までの IETF Last Call
  - 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

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(3 drafts)は合意され、IESGが発行承認した



add WG: IESGが発行承認 / RFC Editor

- 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 (DDR)
  - 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 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
  - すでにAppleのデバイスがクエリを出しているという噂

add WG: IETF 117での議論

- draft-ietf-add-resolver-info
  - リゾルバ情報をRESINFO RRに書く
  - 例: resolver.example.net. 7200 IN RESINFO qnamemin exterr=15,16,17 infourl=https://resolver.example.com/guide
  - WGLC: 2023/7/26 – 8/17
    →コメントなし、Passed (8/15)
- draft-ietf-add-split-horizon-authority
  - 内部ドメイン名の認証情報/ DS相当の情報などをDHCPやProvisioning Domain(PvD)で与える
    - PvDのJSONで“splitDnsClaims”に
      - “resolver”
      - “parent”
      - “subdomains”
      - “algorithm”
      - “salt”
    - 複雑
  - WGLC: 2023/7/26 – 8/17
    → コメントなし、Passed (8/15)

- draft-reddy-add-delegated-credentials
  - CPEでEncrypted DNS forwarderを動かし、CPEの証明書をACMEのような仕組みで受け取る
    - CPEでTLSをほどく！
  - DNRの変更に言及
    - いまさら？

dnssd (Extensions for Scalable DNS Service Discovery) WG

- DNSサービスディスカバリを作るWG
  - Multicast DNS(RFC 6762)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させる
  - 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
- 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
- 2020/9/10, RFC 8882 DNSSDプライバシーセキュリティの要求仕様
- 現在は、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

- IESG作業中
  - draft-ietf-dnssd-srp
    - Multicast DNSの端末がSleep状態でも答えるプロキシー
  - draft-ietf-dnssd-update-lease
    - DNS Updateに秒単位の有効期間を追加するEDNS0オプション
    - 登録時の有効期間が切れると自動的に削除
    - IESGを条件付き通過
    - 通常のDNSでも使えそう

dnssd: IETF 117での議論

- draft-sctl-advertising-proxy
  - Multicast DNSの情報をSRPでDNSに提供するもの
  - SRPからの情報を集めてゾーン情報とし、権威サーバとして動作する
  - デバイスが同じ固有名の場合の議論などが行われた
- draft-ietf-dnssd-srp-replication
  - SRPの多重化のための複製
  - Hot standbyや負荷分散の議論など

- draft-tllq-tsr
  - Multicast DNS conflict resolution using the Time Since Received (TSR) RR
  - Multicast DNSなどで複数の機器から同じ名前での登録がある場合の解決策の議論
    - printer.localなど
    - あとから登録したものがprinter-2.localになる
  - Time Since Received RRを定義して、登録されてからの時間(秒)を返す
  - 名前の競合時には後で登録されたものを採用する(TSRが小さいもの)
  - 以下のような議論があった
    - マルチキャストをブロックするWiFi AP
    - 従来は先着優先であったこと
    - IPv4, IPv6でも同じ名前が競合すること
      - IPv4とIPv6で別の名前になる？

IETF dnsop WGでの特別対応: 1

- draft-ietf-dnsop-svcb-https: HTTPS/SVCBリソースレコード
  - 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, Chrome, Cloudflare など
  - 2022/5/22にIESGが発行承認
    - draft-ietf-tls-esni(TLS Encrypted Client Hello)を参照しているが、TLS WGはdraftのまま実装経験を積んでいくようで、しばらくRFCにならない見込み
    - RFC EditorのところでMISSREF (参照するドラフトがまだ)という状態で8か月放置
  - 2023/2/23: 担当Area Directorが、draftをRFC Editorからdnsop WGに差し戻し、draft-ietf-tls-esniへの参照を外して標準化しなおすことを提案
  - 2023/3/11: 参照を削除した -12 提出
  - 2023/3/11-18: Additional Working Group Last Call
  - 2023/3/18: IESGへ再提出 → IETF Last call → IESG評価
  - 2023/4/17: IESGが発行承認
  - 2023/5/2 からRFC Editorが作業中
  - https://datatracker.ietf.org/doc/draft-ietf-dnsop-svcb-https/history/

IETF dnsop WGでの特別対応: 2

- draft-ietf-dnsop-avoid-fragmentation: Fragmentation Avoidance in DNS
  - Author: 藤原とPaul Vixie
  - DNSで、IP Fragmentationを使うのをやめましょうという提案
    - IPv4 ではDF (Don't Frag) bitをセットすること
    - IPv6 ではFragmentしない大きさの応答パケットを作ること
    - Fragmentされたパケットは捨ててもいい
  - Best Current Practiceを目指している
  - Working Group Last Callなどを経て、2023/1/24にIESGに発行申請
  - ところが、そのあとdnsop WG mailing listにて、いまのOS実装ではDFビットとIPv4 Path MTU Discoveryの動作を制御できないので、現在のほとんどすべてのDNSサーバソフトウェア実装がDFビットを立てていないという指摘があった
  - その結果、Best "Current" Practiceではないだろうということとなり、2023/2/3にIESGからdnsop WGに差し戻しとなった
  - Dnsop WG chairs, 担当ADの指示の通りにテキストを追加
  - 8/16にdnsop WG chairsがIESGに提出
  - 8/26 AD: (temporarily) returning this to the WG

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
  - 担当ADのWarren KumariがDNSにも詳しいため、特別対応された
- 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 TLS/QUIC, ゾーン転送
  - 権威サーバへのDoT/DoQでの問い合わせは実験プロトコルとして合意され、発行手続きが開始
- 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
  - 残るプロトコル拡張がゆっくりではあるが進んでいる
- 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

参考資料

- www.ietf.org → datatracker.ietf.org
  - IETFミーティングの資料、議事録
    - https://datatracker.ietf.org/meeting/117/agenda
  - ワーキンググループの情報
    - https://datatracker.ietf.org/wg/
    - 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