DNS Update: IETF/RFC動向

(あるいはIETF 118 DNS報告)

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 2023 DNS DAY

2023年11月21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 Editor queue)
    - 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
- Internet Week: 2016からプログラム委員

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 118での状況
- IETF/dnsop WGでの2件の特別対応
  - HTTPS/SVCB (RFC 9460)
  - 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11月で43本
    - 年平均5本以上
- 発行されたRFC: 1年で5本
  - 2023/2/14: RFC 9364 DNSSEC BCP
  - 2023/7/ 6: RFC 9432 DNS Catalog Zones
  - 2023/9/14: RFC 9476 .alt TLD
  - 2023/9/30: RFC 9471 Glue Requirements
  - 2023/11/6: RFC 9460 SVCB and HTTPS
- IESG承認済/RFC Editor Queue (2)
  - caching-resolution-failures
  - rfc8499bis: DNS用語集
- IESG Review (3)
  - ~~rfc5933-bis: Use of GOST 2012 in DNSSEC~~
  - avoid-fragmentation
  - zoneversion
  - dns-error-reporting
- Waiting for WG Chair Go-Ahead (1)
  - domain-verification-techniques
- WGLC (2)
  - rfc8109bis (priming)
  - dnssec-bootstrapping
- 議論中のWG drafts (9)
  - qdcount-is-one
  - dnssec-automation
  - generalized-notify
  - compact-denial-of-existence
  - svcb-dane
  - cds-consistency
  - structured-dns-errors
  - dnssec-validator-requirements
  - ns-revalidation

dnsop: 発行されたRFC

- 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

    → 標準化しながら実装が進んでいるので既に使用可能
- RFC 9471: DNS Glue Requirements in Referral
  - 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
- RFC 9476: The .alt Special-Use Top-Level Domain
  - 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
- RFC 9364 DNSSEC BCP
  - DNSSECを実装するために必要なRFCリスト
- RFC 9460: Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)
  - 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
    - サービス名. IN HTTPS SvcPriority TargetName SvcParam（httpsの場合)
    - _scheme.サービス名. IN SVCB SvcPriority TargetName SvcParam (https以外)
    - 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
    - SvcParam ipv4hint=192.2.0.1 ipv6hint=2001:dc8::1
    - hintがあっても、TargetNameのA/AAAAクエリしろ (SHOULD) と書かれていることに注意 (クエリ減らない)

IETF 118 Hackathon: DELEG RR提案

- IETF Hackathonで、DNSをよくするという議論があったらしい
- 委任に新機能を追加したい: 委任に直接IPアドレスを書きDoT/DoQ指定したい
- DELEG RRTYPE提案: SVCB/HTTPSと同じ形式
  - in-domainの委任の場合
    - TargetNameにネームサーバ名
    - ipv4hints, ipv6hintsにIPアドレス
    - transport=dot, doq
    - 例: company1.example. DELEG 1 ns.company1.example. (ipv4hint=192.2.0.1 transport=dot)
  - sibling, unrelated の委任の場合は、SVCBへのALIASを書く
    - company1.example. DELEG 0 ns1.provider1.example.
    - ns1.provider1.example. SVCB 1 ns1.provider1.example. (ipv4hint=… transport=dot)
    - 複数のALIASのDELEG RRで、multi-providerもできる
  - NS, DS, 既存のグルーはそのまま残す (互換性のため)
- 議論はDNS-OARC Mattermost chat serverのDELEG-designチャンネルで継続
- 楽しそう (標準化というか実装までは遠そう)

dnsop WG での議論 (1)

- draft-ietf-dnsop-compact-denial-of-existence
  - 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の2つのNSEC,SOAとRRSIG*3
  - 不存在応答のかわりにNODATA応答を返す
    - NODATAはNSEC*1, SOA, RRSIG*2
    - 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)
    - NXNAMEビットがあると存在しないと読み替える
  - すでにCloudflare,NS1,Amazon Route53が実装、private RR type codeで空の応答を返すらしい
    - 例: dig +norec +dnssec @ns3.cloudflare.com hoge.cloudflare.com aaaa

    cloudflare.com. SOA

    cloudflare.com RRSIG SOA

    hoge.cloudflare.com NSEC ¥000.hoge.cloudflare.com RRSIG NSEC TYPE65283

    hoge.cloudflare.com RRSIG NSEC
  - 曖昧なところや、利点が不明確というコメントがあったが、Cloudflareの権威サーバのCPU timeが減り、パケットサイズが小さくなったとのこと

- rfc5933-bis: Use of GOST 2012 in DNSSEC
  - IESGでのレビューにて、IETFのドキュメントとしてふさわしくないと判断された
  - IETFで扱う暗号はIRTFのCrypto Forum Research Group(CFRG)で公開されたドキュメントに依存しているが、

  GOSTアルゴリズムはIRTFの審査基準に適合せず、(dnsop WGは)代替の分析手段を提供していないのでIETF streamのRFCには不適切

  → Independent Submission に変更
    - IETFの成果ではないRFC
    - (企業独自プロトコルのRFCのような扱い)

  - IRTF の審査基準
    - オープンで査読のある審査プロセス
    - またはIRTF暗号パネルによるレビュー

dnsop WG での議論 (2)

- draft-bash-rfc7958bis
  - DNSSEC Trust Anchor (Rootの公開鍵)の公開方法を定義したRFC 7958の更新
    - https://data.iana.org/root-anchors/root-anchors.xml
    - XML Syntax
    - DS, DNSKEYの取り出し方
  - 主にErrata対応
- draft-ietf-dnsop-qdcount-is-one
  - DNSのクエリセクション数QDCOUNTは0か1
  - DNSSDで2を使うことが指摘された
  - (dnsopでは0か1で進める見込み)
- draft-ietf-dnsop-domain-verification-techniques
  - 議論は続いている
  - Public suffixにトークンドメイン名を書かないこととか
  - 複数のアカウントがある場合のドメイン名
    - _xxxxxxx._foo-challenge.www.example.org TXT
  - draft-ietf-acme-dns-account-challenge の変更
    - _xxxxxxx._acme-challenge.www.example.org TXT
- DNS in Mostly Isolated Networks
  - draft-many-dnsop-dns-isolated-networks
  - 火星・月軌道での名前解決をどうするかという問題提起
  - 火星ローカルは地球と同様に権威サーバ、リゾルバ、トラストアンカー、ルートも必要か？
  - 地球の情報は必要なものだけ事前にコピーしておく？
  - どこで議論するのがよいか？ dnsopは興味を持つか？
  - RFC 8806 local rootで対応すべきといった議論があった
- draft-ietf-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
  - NOTIFY送信先を示す新しいリソースレコードの提案
  - NOTIFY, CDSなんかやめてDNS Updateすればいいといった議論も ↓
- draft-johani-dnsop-delegation-mgmt-via-ddns
  - CDSなどのかわりにDynamic UpdateでTLDのNS, DS, glueを書き換える提案
  - 認証などが考慮されていないことが指摘されていた
  - TLDのDNSサーバへDynamic Updateってすごい

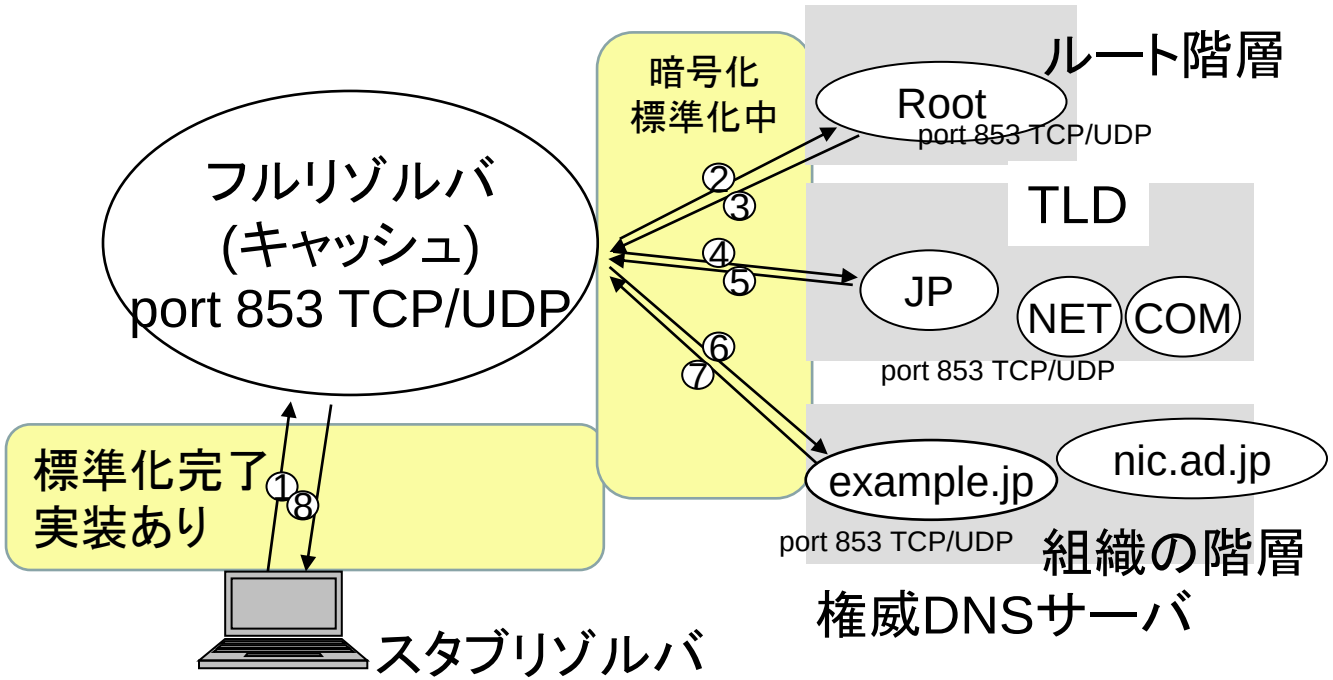
dnsop WG での議論 (3)

- draft-ietf-dnsop-svcb-dane
  - SVCB/HTTPSを使うときのTLSAの書き方
  - ALIASの場合はTargetNameにTLSAを書く
  - example.com. HTTPS 0 xyz.provider.example.
  - xyz.provider.example. HTTPS 1 . alpn=h2,h3 ...
  - _443._tcp.xyz.provider.example. TLSA
  - _443._quic.xyz.provider.example. TLSA
- draft-homburg-dnsop-igadp
  - Authoritative DNS Proxies
  - Authoritativeもcacheするproxyとしたいという提案
  - 似たような実装はあることや、関心がある人はいる
  - 懸念はいっぱい
- draft-peltan-edns-presentation-format
  - RFC 8427 JSONでのDNSメッセージの表現 ではEDNS0が定義されていないので追加する提案
  - RFC 8427はinteroperability testingのためにまとめたのでindependent submissionだという説明があった
  - RFC 8427がIndependent submissionであるので同様にすすめればよいという助言があった
- draft-momoka-dnsop-3901bis
  - RFC 3901
    - すべてのリカーシブネームサーバはIPv4のみかdual stackでないといけない
    - すべてのDNSゾーンは一つ以上のIPv4権威サーバをもたないといけない
  - IPv4アドレスは枯渇したし、RFC 3901はIPv6に厳しいので、以下のように更新する提案
    - すべてのリカーシブネームサーバはdual stackでないといけない
    - すべてのDNSゾーンは一つ以上のIPv4権威サーバとIPv6権威サーバをもたないといけない
  - 概ね好意的
  - IPv6での名前解決の失敗率の懸念の指摘

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 117,118ではミーティングなし

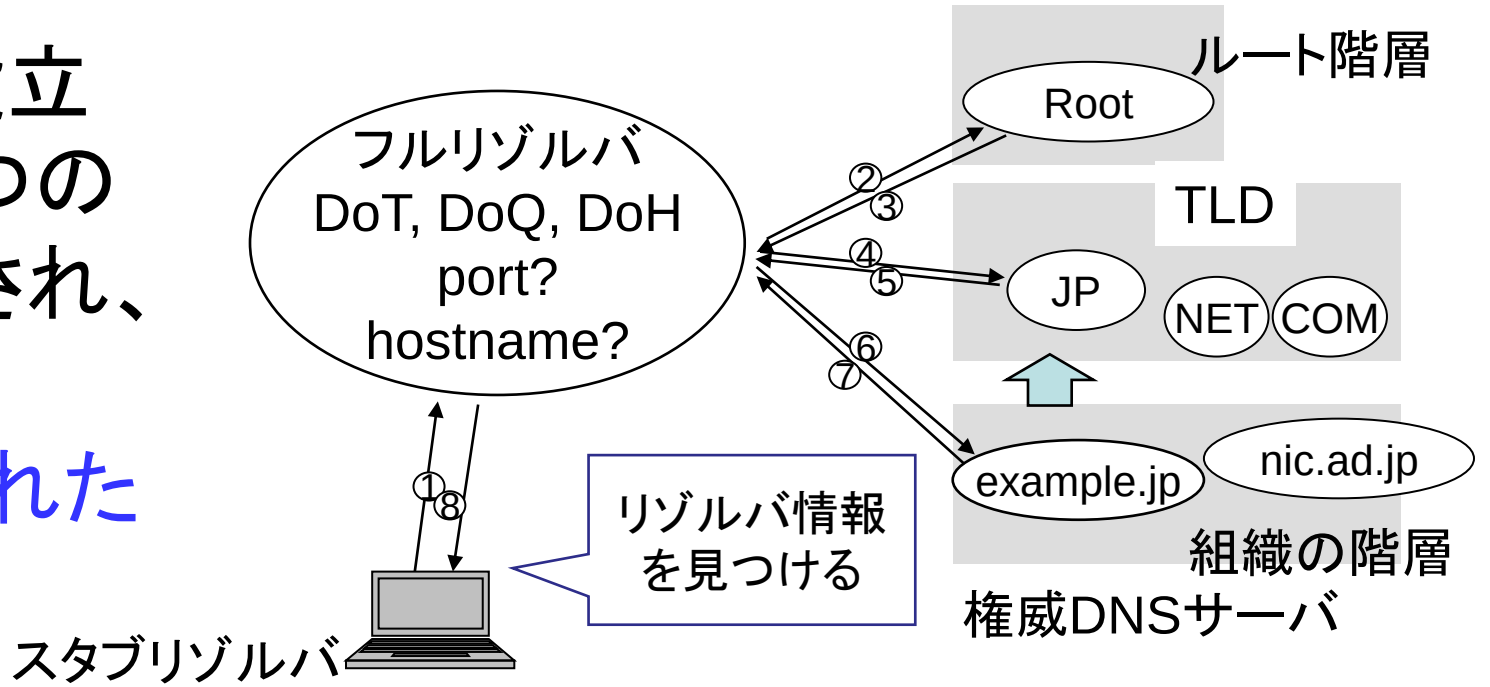


dprive WG の現状 (2023/11)

- 現在の提案: draft-ietf-dprive-unilateral-probing-13
  - 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、2023/10/31 にIESGが発行承認、11/1にRFC Editorが受理 (近いうちにRFC発行見込み)
  - 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、2023/11/6にRFC 9461, 9462, 9463として発行された



add WG: 2023/11/6にRFC発行

- RFC 9461: Service Binding Mapping for DNS Servers
  - SVCBにDNS情報をいれる仕組み
  - _dns.ドメイン名にSVCB　alpnにdot,doq,h2,h3　SvcParamにdohpathを追加
- RFC 9462: 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})
- RFC 9463: 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})

add WG: IETF 118での議論

- draft-ietf-add-split-horizon-authority
  - 内部ドメイン名の認証情報などをProvisioning Domain(PvD)で与える
    - PvDのJSONで“splitDnsClaims”に
      {“resolver”: “resolver17.parent.example.”,
      “parent”: “parent.example.”,
      “subdomains”: [“internal.parent.example.”, …
      “*”], “algorithm”: “SHA384”, “salt”: “001122”}
  - parentに、指定された計算方向で計算したtokenをdraft-ietf-dnsop-domain-verification-techniques の形式で書く
    - 例: resolver17.parent.example._splitdns-challenge.parent.example.
      IN TXT
      "token=6rQ7oOZqdg8qQFRqtxpEhK97mNkgFwzNKTmNOtlxspBscZqUwFZZJDDD-Djetw2MCg"
  - WGLC: 2023/7/26 – 8/17
    - すこしコメントがあって、改版された
    - このまま進む見込み
  - (複雑)
- 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 sig=“署名”
  - RESINFO RR TYPE 261
  - 署名は、リゾルバのTLS証明書で作ると書かれているが、具体的には書かれていない
  - BIND 9で実装しているらしい
  - sigを追加したため、2度目のWGLCをかける予定
- 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！
- IETF 118ハッカソン
  - Raspberry Piをルータとし、DNR(RFC 9463)オプションを追加したDHCPv4サーバとDoHサーバを用意したところ、Windows11 とiOS は期待した動作をしたとのこと
  - Windows11ではregistryのDNRをenableにすること

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
    - IESGからの指摘を3か月放置
  - 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
    - 3か月放置
    - 通常のDNSでも使えそう

dnssd: IETF 117, 118での議論

- draft-ietf-dnssd-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
  - 複雑なのでsimpleにする提案があった
    - SRPと分離するらしい
    - draft待ち
- 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)
  - Apple tvOSに実装されているらしい
  - 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？
    - 細かい実装をして確かめているらしい
  - 今後まだ仕様がかわりそう

dance (DANE Authentication for Network Clients Everywhere) WG

- 証明書または生の公開鍵を使用したTLSクライアント証明書をDANE TLSAで扱えるように拡張するWG
- 2021年9月設立
- 2022/11/8から2本のドキュメントがWGLC
- IETF 118での議論
  - WGLCコメントと今後の修正案の議論
  - AfNIC(.FR)でのLoRaWanでIoT認証にDANE/DANCEを使ったという報告
  - WGの今後の議論
    - 標準化しようとしていたものはほぼ完了
    - デバイスのIDと認証を扱うという提案

- draft-ietf-dance-tls-clientid-02
  - DANE Client IDを扱うTLSの拡張
  - TLSに”dane_clientid”を追加する
  - 値はテキストのドメイン名とする
    - 最後の”.”は除く

- draft-ietf-dance-client-auth-02
  - DANE TLSA RRによるTLSクライアント認証
  - クライアントはドメイン名とTLSクライアント証明書を持つ
    - IPアドレスは固定でなくていい
  - 証明書の”dane_clientid”にクライアントのドメイン名を書く
    - “dane_clientid”を使わないときはSubject Alternative Nameに書く
  - サービスごとのクライアントID
    - _service.[client-domain-name] TLSA
  - IOT Device Identity
    - [devicename]._device.[org-domain-name] TLSA
  - クライアントからサーバへの接続の変更
    - サーバは接続時にTLSクライアント証明書を要求する
    - サーバは”dane_clientid”をみてTLSA RRを取り出す
    - クライアントから得た証明書とTLSA RRを比較、一致したら認証成功

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発行前からブラウザと一部CDNの実装が進んだ
    - Safari, Firefox, Chrome, Cloudflare など
  - 2022/5/22にIESGが発行承認
    - draft-ietf-tls-esni(TLS Encrypted Client Hello)を参照してた
    - 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か月放置された
  - 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/
  - 2023/11/6 RFC 9460として発行

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Best Current Practice提案
    - IPv4 ではDF (Don’t Frag) bitをセットすること (SHOULD)
    - IPv6 ではFragmentしない大きさの応答パケットを作ること (SHOULD)
    - Fragmentされたパケットは捨ててもいい (MAY)
  - 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
  - 主要なソフトウェアが実現できていないものは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IESGに提出
  - 治ってなかったので、 8/26 AD: (temporarily) returning this to the WG
  - IPv4 ではDF (Don’t Frag) bitをセットしてもいい (MAY) と変更
  - 2023/10/13: IESGに提出
  - 2023/10/28: SECDIRから、IPv4でDF bitをセットするのは SHOULD であるべきだろう、とコメントされた (対応案検討中)

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、実装も進んでいる
  - 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、特別対応もある
- 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 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、RFC発行直前
- add WG
  - _dns.resolver.arpa SVCB方式とDHCP, RAの拡張のRFCが発行
  - 実装も進んでいる
- 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
- dance
  - 標準化と実装が進んでいる
- 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、ビデオなど
    - https://datatracker.ietf.org/meeting/118/agenda
  - ワーキングループの情報
    - 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