IETF Update: DNS関連

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 2025
2025年11月26日

自己紹介

- 氏名:　　藤原和典　　博士(工学)
- 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)　システム部
- 業務内容:DNS関連の研究・開発
- IETFでの活動 (2002~)
  - 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, 9499: DNS Terminology (BCP)
    - RFC 8198: DNSSECを用いた名前解決の性能向上 (Proposed Standard)
    - RFC 9715: DNSでIP断片化を避ける提案 (Informational)
    - draft-fujiwara-dnsop-dns-upper-limit-values: 上限値をつける提案

本日の内容

- 2024年11月から1年のDNS関連RFC
- DNS関連WG (dnsop, deleg, add, dnssd)の1年の動向
  - IETF 124 (2025/11)の動向
- スライドにはたくさん書きましたが、全部を紹介している時間はないので青いところを中心に紹介します

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
- deleg (DNS Delegation) WG
  - DNS委任の改良を行う
- dprive (DNS Private Exchange) WG
  - DNS通信路を暗号化
  - 2025/7/11 conclusion (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
- 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
- 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
- dconn (Domain Connect) WG
  - ドメイン名を指定するとDNSプロバイダやサービスプロバイダ(メール, Web)などを簡単に自動設定できるDomain Connect protocolを標準化する
  - 2025/9/30設立
- IETF WG以外からのRFC発行
  - Independent submission
  - 対応するWGがない場合
- 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
  - DNSそのものを扱う唯一の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～2025年11月で54本
    - 年平均5.5本
  - IESG Reviewまでいくとdnsop WGではほとんど話題にならなくなる
  - DNS運用とプロトコル標準化を分離する議論が開始 (dnsext WG機能の分離)
- 発行されたRFC: 1年で5本
  - RFC 9718, RFC 9715, RFC 9609, RFC 9824, RFC 9859

- dnsop WG関連RFC (1)
  - 2024/12/4: RFC 9563 on SM2 Digital Signature Algorithm for DNSSEC
    - Digest Type: SM3 (6)
    - Algorithm: SM2SM3 (17)
- RFC Editor Queue (3)
  - must-not-sha1
  - rfc8624-bis
  - must-not-ecc-gost
- IESG Review (1)
  - cds-consistency
- Waiting for WG Chair Go-Ahead (1)
  - domain-verification-techniques
- WGLC (1):
  - ns-revalidation
- 議論中のWG drafts (8)
  - rfc3901bis, grease, ds-automation, integration
  - expired: svcb-dane, structured-dns-errors, dnssec-automation, dnssec-validator-requirements

dnsop: 発行されたRFC 1/2

- 2025/1/24: RFC 9718 on DNSSEC Trust Anchor Publication for the Root Zone
  - RFC 7958 DNSSEC Trust Anchor Publication for the Root Zone の置き換え
  - Root Trust Anchor (RootのDNSKEYと対応するDS) の公開方法を規定
  - https://data.iana.org/root-anchors/root-anchors.xml
  - XML schema
- 2025/1/27: RFC 9715 on IP Fragmentation Avoidance in DNS over UDP
  - DNS/UDPでIP Fragmentationを避けるBest Current Practiceを目指した提案だったが Informational に変更
  - IP_DFビットをセットすればいい、1400オクテット以下にするなど
  - 現時点で可能な対策として、フルサービスリゾルバ手前のFirewall機能でFragmentされたパケットを捨てると安全になるという記述を追記
- 2025/2/11: BCP 209, RFC 9609 on Initializing a DNS Resolver with Priming Queries
  - フルサービスリゾルバがルートサーバ情報を更新するPrimingの定義
  - RFC 8109 on Initializing a DNS Resolver with Priming Queries の置き換え
  - RFC番号がちょうど1500ずれていることに注意 (RFC Editorの裁量の範囲)
  - 細かい修正と追記
  - TTL切れによる再Priming時には、設定されている古いリストではなく、直前のPrimingで得た最新のルートサーバリストのサーバに問い合わせること
  - Rogue (偽) root name serverの影響を追記

dnsop: 発行されたRFC 2/2

- 2025/9/18: RFC 9824 on Compact Denial of Existence in DNSSEC
  - クエリごとの動的な署名生成での応答改善の仕組み
  - NXDOMAIN応答にはクエリ名を含む範囲とワイルドカードの不存在を示す2つのNSEC,SOA,3つのRRSIGを返す必要があり、応答サイズが大きくなる
  - 不存在応答のかわりにNODATA応答を返す (NSEC,SOA,RRSIG*2)
  - NXNAME RR (type 128) (NSEC type bitmapで使用) NXNAMEがあると存在しないと読み替え
  - 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 TYPE128
    - hoge.cloudflare.com RRSIG NSEC
- 2025/9/28: RFC 9859 on Generalized DNS Notifications
  - CDS自動更新の改良: DNS NOTIFYを一般化し、(子側の)CDS変更の通知をできるようにする
  - DSYNC RRを定義: type 66, DSYNC RRtype(CDS/CDNSKEY) NOTIFY ポート番号 送信先
  - 例: example TLD でCDSの自動更新を使い、Generalized Notifyを受け取る場合
  - *._dsync.example. IN DSYNC CDS NOTIFY port notify-destination.nic.example.
  - label.exampleゾーンのCDSを変更したら、label._dsync.example. DSYNCを問い合わせる
  - この応答を解釈し、notify-destination.nic.example の指定されたポート番号 port にNOTIFYを送る
  - example zone のCDSスキャナは label.example. CDSを問い合わせ、CDSを用いてDSを更新

IETF 124 dnsop WG での議論 1/2

- draft-ietf-dnsop-3901bis-06: DNS IPv6 Transport Operational Guidelines
  - すべてのDNSゾーンはIPv4, IPv6どちらでも権威サーバを動かす
  - すべてのリゾルバはIPv4, IPv6どちらでも名前解決する
  - おおむね好意的
- draft-ietf-dnsop-ds-automation: Operational Recommendations for DS Automation
  - CDS/CDNSKEY自動更新の細かい残務
  - Registry/Registrarがやるべきこと
  - CDSでの自動更新は登録者に通知されないといけない
    - Humans (domains holders) should be notified according to preferences established with registry/registrar
- draft-crocker-dnsop-dnssec-algorithm-lifecycle-02
  - DNSSECアルゴリズムのライフサイクル管理の文書化
  - RFC 1の著者、Steve Crocker 登場
  - Experimental→Adopted→Available→Mainstream→Phaseout→Deprecated→Obsolete
  - IETF/dnsop, IANA Registry, IRTF CFRG など、どこで進めるべきかといった議論があった
- draft-wkumari-dnsop-localroot-bcp: Making LocalRoot a Best Current Practice
  - RFC 7706 → RFC 8806 Running a Root Server Local to a Resolver (Informational)
  - ルートのコピーをフルサービスリゾルバに持たせてルートへのクエリを減らす案をBest Current Practiceにする
  - 大規模なルートゾーンの配布を誰がやるかという問題はあるが、CDN (Google)を使うという案があるらしい

IETF 124 dnsop WG での議論 2/2

- draft-johani-dnsop-transport-signaling-02: Authoritative DNS Transport Signaling
  - 委任の親側のグルーとしてSVCBを追加し、DoT/DoQできることを示す提案
  - _dns.ns.dnsprovider.net. SVCB 1 . “alpn=dot,doq,do53”
  - DELEGの進みが遅すぎて対案を出したようだが、現在のDNSへの変更が大きすぎるので否定的
- draft-jabley-dnsop-zone-cut-to-nowhere: Signalling a Zone Cut to Nowhere in the DNS
  - 委任が存在しないことを示すために NS . (MX 0 . = not accept mailだからNSも同じようにしたい)
  - 名前解決エラーになるのでクエリが増える懸念が示された
- draft-arends-dnsop-delext: DNS Protocol Modifications for Delegation Extensions
  - DELEGのための準備として委任用のタイプを複数用意する
- draft-huque-dnsop-multi-alg-rules: Multiple Algorithm Rules in DNSSEC
  - みんなが使わないといけないUNIVERSAL algorithmを便利にしよう、それ以外を不便にしようという提案
- draft-davids-forsalereg: for-sale Underscored & Globally Scoped DNS Node Name
  - _for-sale TXT "v=FORSALE1;ftxt=call or mail“
  - 販売用のドメイン名を示すラベルを用意したい
- draft-sheth-pqc-dnssec-strategy: Post Quantum Cryptography Strategy for DNS
  - 耐量子暗号をDNSSECに用いる話のまとめ

deleg (DNS Delegation) WG

- dnsop WGから派生
- DNSの委任を改良するプロトコルを作るWG
  - 新しいトランスポート(DoT, DoQなど)とサーバ証明書の情報を追加する
  - DNSプロバイダへの委任の簡略化
- IETF 119 (2024/3)にWorking Group結成BoF
- 要求仕様
  - ドメイン名登録モデルを壊さない, DNS/ソフトウェアとの互換性
  - DNSSECで委任を安全にできること (いまは親側NS, glueは署名なし)
  - 既存のNS+glueから徐々に新方式に移行できること
  - DNSプロバイダ簡単設定 (複数)
- IETF 122 (2025/3)にて、複数提案のうち元祖DELEG案に近いものを選定
  - 議論が発散したため、まずは委任の置き換え/併存部分のみを進めることとなった
    - DNSSEC (DS方式) は変更なし
    - DoT/DoQ指定(alpn=do53,dot,doq)やサーバ証明書(tlsa=証明書Hash)は削除

現在のDELEG案: draft-ietf-deleg-05

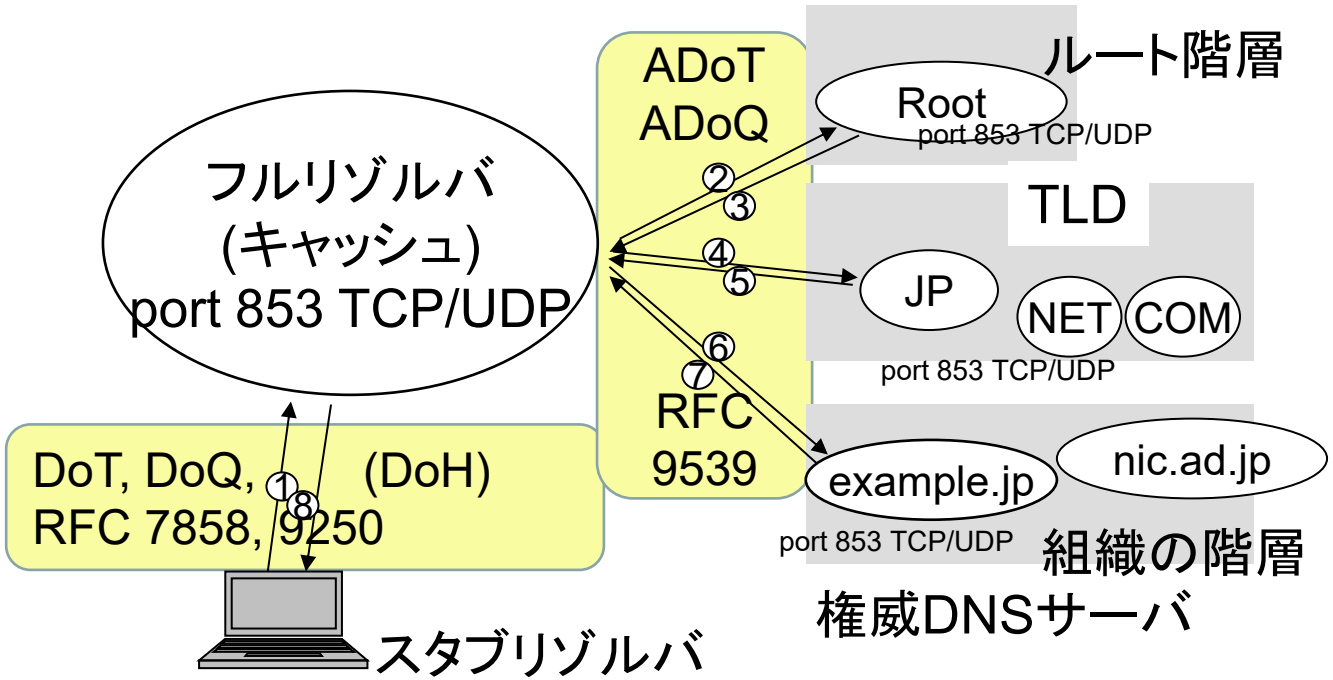
- IETF 123 (2025/7)の結果、02 → 03 でDELEG RRフォーマットをSVCBから変更
- DELEG RRのデータはkey=valueフィールドのみ　RDATA=(key, length, value)
- 現在書かれているKey (3種類それぞれ排他)
  - server-ipv4=IPv4アドレス(リスト) server-ipv6=IPv6アドレス(リスト)　(両方あってもよい)
  - server-name=<ネームサーバ名(リスト)> (名前解決しなければならない)
  - Include-delegi=<DELEGIを指すドメイン名リスト> : DNSプロバイダ指定
- in-domainの委任だった場合
  - server-ipv4, server-ipv6 でIPアドレスのみ指定 (server-nameを書いてはならない)
  - 例: example.com. DELEG server-ipv4=192.0.2.53,192.0.2.54 server-ipv6=2001:db8::53
- sibling, unrelatedの委任だった場合
  - server-name で委任先サーバ名だけ書く (siblingでつく可能性のあったGlue排除)
  - 例: example.com. DELEG server-name=ns1.example.net.,ns2.example.org.
- DELEG RRは親側にあるが署名する (DSのように)
- NS, DS, 既存のグルーはそのまま残す (互換性のため)
- EDNS0 Header FlagsにDEビットを追加、DE=1の場合のみDELEG RRを返す
  - DE=0の場合は既存のNS + Glueを返す

NS方式からの改良は、DELEG RRの署名と、親子にNS,A/AAAAがあることの解消のみ

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)
- 2024/2/29 RFC 9539 Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS 発行
  - 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 (Experimental)

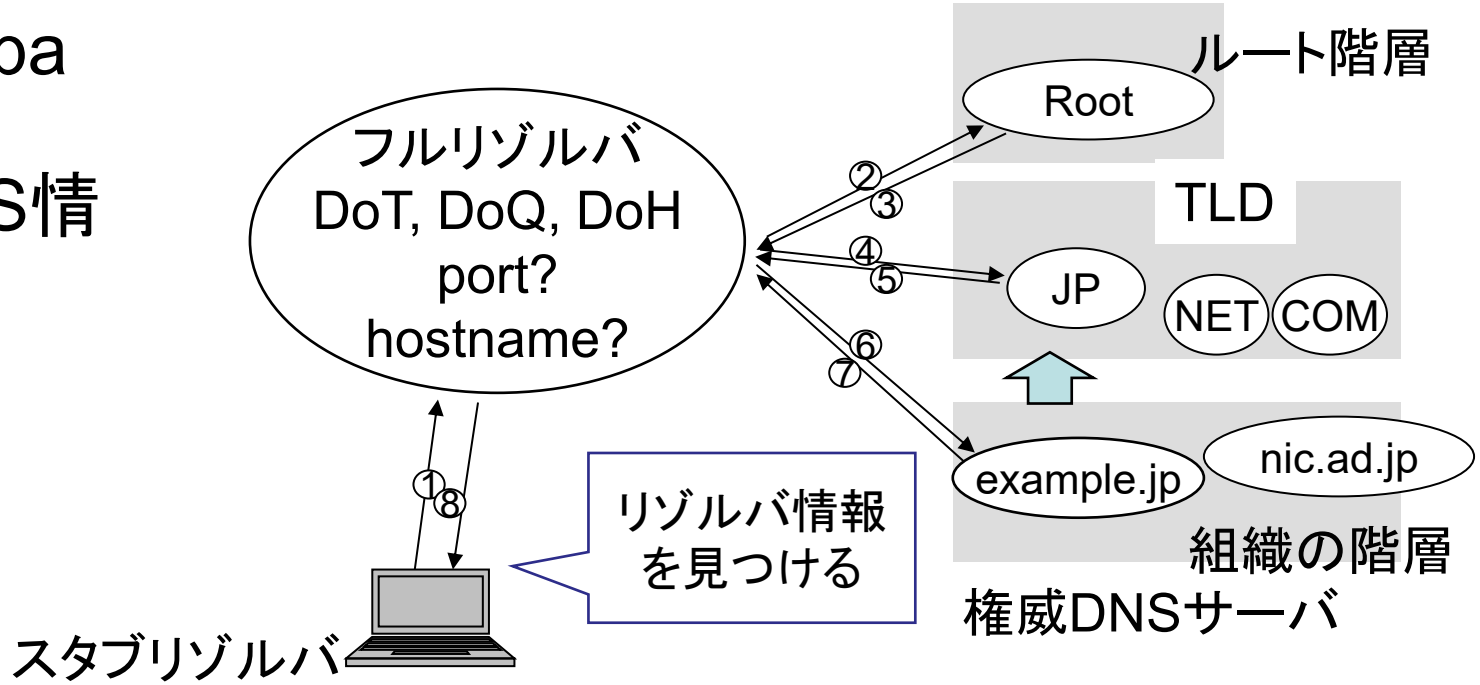
- 2025/7/11: Conclusion of dprive WG (完了)
- ADoT/ADoQを望む有志が動いた
  - IETF 123 (2025/7) にてADoT/ADoQ Deployment Initiative side-meeting開催
  - RIPE 91 (2025/10)にてADoT/ADoQ Deployment Collaboration BoF開催



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
- RFC 9461: SVCBにDNS情報を記述 (alpn=dot,doq サーバ名 dohpath)
- RFC 9462: _dns.resolver.arpa SVCBにDNS情報
- RFC 9463: DHCP, RAにDNS情報
- RFC 9660: DNS Resolver Information

- RFC発行: 2025/1/28, RFC 9704
- 残務: draft-ietf-add-encrypted-dns-server-redirection
  - Encrypted DNS Server Redirection
  - 安全に別のリゾルバにリダイレクトする
- add WGを完了させる提案あり



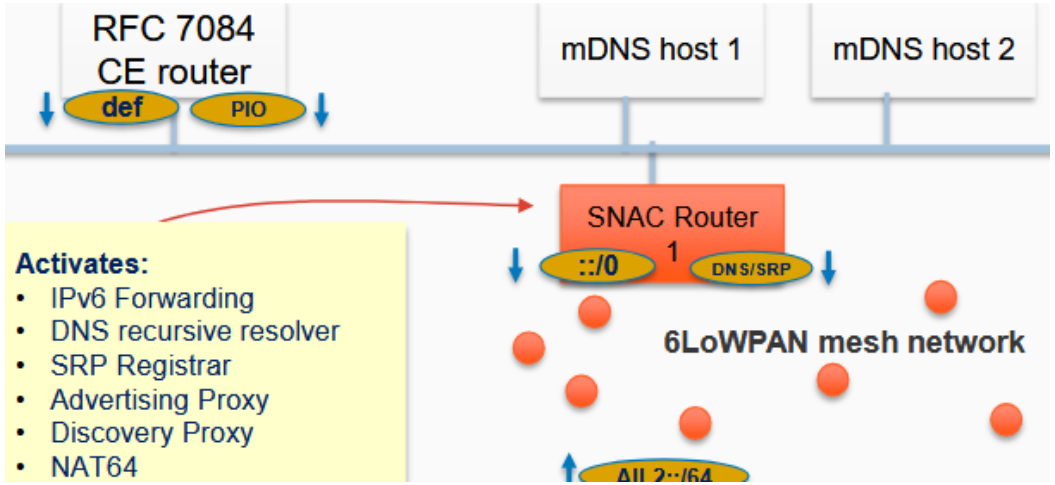
add WG: 発行されたRFC

- 2025/1/28, RFC 9704 Establishing Local DNS Authority in Validated Split-Horizon Environments
  - 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domain-verification-techniques の形式で書く
    - 例: resolver17.parent.example._splitdns-challenge.parent.example. IN TXT "token=6rQ7oOZqdg8qQFRqtxpEh…….”

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
  - Apple社のBonjourとAvahiのプロトコルを拡張し、IETFで標準化する
- DNSSDコアプロトコル, 2020/6/22発行
  - RFC 8766 Discovery Proxy
  - RFC 8765 DNS Push Notifications
- 現在
  - ホームネットワーク向けの(Open)ThreadでmDNSとdnssd protocolが採用されたようである (OpenThreadのAPIにSRP)
    - https://openthread.io/reference
  - IETF snac WG (Stub Network Auto Configuration for IPv6)
    - snac WGではApple社のひとたちが中心となり、dnssd (SRP)と6LoWPANを組み合わせたIoTルータの標準化を進めている

- 2025/6/11 RFC発行
  - RFC 9664 on An EDNS(0) Option to Negotiate Leases on DNS Updates
  - RFC 9665 on Service Registration Protocol for DNS-Based Service Discovery (SRP)
  - どちらの著者もApple社の二人
    - 一人はRFC 6761, 6762, 6763 (mDNS = Bonjour)の著者
    - RFC 8766, RFC 8765 も一人は同一著者



IETF 124 snac WGスライドより引用
https://datatracker.ietf.org/meeting/124/materials/slides-124-snac-snac-simple-multi-ail-situations-00

dnssd: 発行されたRFC

- 2025/6/11: RFC 9664 on An EDNS(0) Option to Negotiate Leases on DNS Updates
  - DNS Updateに秒単位の有効期間を追加するUPDATE-LEASE 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
  - 普通のDNSでも使えるとうれしいかも
- 2025/6/11: RFC 9665 on Service Registration Protocol for DNS-Based Service Discovery
  - Multicast DNS + dnssd で .local でできるサービス検索などを別のドメイン名で通常のport 53 DNSを使ってできるようにする仕組み
  - ドメイン名は別途指定するか、”default.service.arpa.” (特に6LoWPANの場合)
  - (制約付きの) DNS Update と権威DNSサーバの組み合わせ
  - DNS Updateでホスト名とIPアドレスA/AAAA、サービスSRV、リストPTRの対応の登録を受け付け、通常のUnicast DNSで応答する
  - 登録する名前は multicast DNSと同様に、先に名前を登録したものが優先
  - _dnssd-srp._tcp.default.service.arpa SRVにSRPサーバ情報、ここにDNS Updateする
  - 登録した名前を他者に変更されないようにするためにSIG(0)を用い、登録時にKEY RRも追加
  - 登録した名前は2時間ほど使用でき、expire前に再登録を行う (その時にSIG(0)を確認される)

dnssd WG: IETF 124

- draft-ietf-dnssd-tsr
  - Multicast DNS conflict resolution using the TSR EDNS option
- draft-ietf-dnssd-advertising-proxy
- draft-tlmk-infra-dnssd
  - Providing DNSSD Service on Infrastructure
  - Multicast (DNS)はWiFiの帯域を消費するので避けたいらしい→SRP
- draft-michel-srp-remove-all
  - ThreadとMatterはSRPの重要な利用ケースとのこと
  - IPv6 prefixがかわるとSRPの登録をし直す必要あり
  - 登録し直すのは大変なのでSRPを全部消すというEDNS0オプションを提案
- draft-eastlake-dnsop-rfc2931bis-sigzero: SIG(0) bis
  - SRPでSIG(0)を使うのでSIG(0)を使いやすくしたいという提案

dconn (Domain Connect) WG

- ドメイン名を指定するとDNSプロバイダやサービスプロバイダ(メール, Web)などを自動設定できるDomain Connect protocolを標準化する
- 2025/9/30設立
- 解決したい課題
  - MS O365を設定する場合、6ステップの作業が必要で、7～15のDNSエントリを書き、16のヘルプサイトをみないといけなかった。
  - 簡単に自前ドメイン名を登録し、メールサービスなどと連携できるようにするとドメイン名がもっと売れる
- draft-kowalik-domainconnect-02: Domain Connect Protocol - DNS provisioning between Services and DNS Providers
  - サービスとDNSプロバイダのあいだのDNS設定を簡略化するDomain Connect Protocol
  - Registrar、DNSプロバイダ、サービスプロバイダ(メール、Web)のサービスをまとめて設定するプロトコル
  - 各社のサービス仕様をTemplateとしてまとめ、自動化したい
  - 現在、Pythonで実装していて、GoDaddy, IONOS, Cloudflare, Squarespace Domains, Wordpress.com, Presk, O365, Google Workplace, Apple Cloud+, Weebly などに対応しているらしい

その他のWGが発行したDNS関連RFC

- 2025/3/31: RFC 9726, BCP 241 on Operational Considerations for Use of DNS in Internet of Things (IoT) Devices
  - IETF opsawg で標準化、Best Current Practice

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
  - 新しい提案は、関心が高ければ標準化が進む
- deleg WG
  - DNSの委任部分の大改造を行うWG
  - 慎重に要求仕様の検討を行っている
  - 慎重すぎてうれしさはあとまわし
- dprive WG
  - ADoT/ADoQはExperimental
  - すべての標準化を完了した
  - WGの活動は完了したが、有志がADoT/ADoQ推進を試みている
- add WG
  - _dns.resolver.arpa SVCB方式とDHCP, RAの拡張のRFCが発行
  - リゾルバ情報やSplit DNSの標準化完了
- 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
  - Unicast DNSでの使用も標準化進展
  - IoTデバイス向けの名前解決に採用

IETFでは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/124/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