# DNS Update: IETF/RFC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)

Internet Week 2024 DNS DAY

2024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 (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, 9499: DNS Terminology
    - 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
    - draft-fujiwara-dnsop-dns-upper-limit-values: 上限値をつける提案
- Internet Week: 2016からプログラム委員

Copyright © 2024 Japan Registry Services Co., Ltd.

# 本日の内容

- Internet Week 2023 から1年のDNS関連RFC
- DNS関連WG (dnsop, deleg, dprive, add, dnssd)の1年の動向

Copyright © 2024 Japan Registry Services Co., Ltd.

# 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
- 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
- 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RFC発行
  - Independent submission
  - 対応するWGがない場合
- 青字は報告対象

Copyright © 2024 Japan Registry Services Co., Ltd.

# 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6本
  - 2023/12/22: RFC 9520 Negative Caching of DNS Resolution Failures
  - 2024/3/21: RFC 9499: DNS Terminology
  - 2024/4/26: RFC 9567 DNS Error Reporting
  - 2024/7/16: RFC 9615 Automatic DNSSEC Bootstrapping Using Authenticated Signals from the Zone's Operator
  - 2024/7/24: RFC 9619 QDCOUNT Is (Usually) One
  - 2024/10/11: RFC 9660 The DNS Zone Version (ZONEVERSION) Option

- dnsop WG関連RFC (1)
  - 2024/4/11: RFC 9558: Use of GOST 2012 Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC
- RFC Editor Queue (3+1)
  - avoid-fragmentation
  - rfc8109bis (Priming)
  - rfc7958bis (DNSSEC Trust Anchor Publication)
  - draft-cuiling-dnsop-sm2-alg: 中華人民共和国政府開発のSM2暗号・SM3ハッシュをDNSSECで利用 (AUTH48半年)
- IESG Review (0)
- Waiting for WG Chair Go-Ahead (1)
  - domain-verification-techniques
- Waiting for Write-Up (1)
  - compact-denial-of-existence
- WGLC (1)
  - structured-dns-errors
- 議論中のWG drafts (10)
  - generalized-notify, svcb-dane, cds-consistency, dnssec-validator-requirements, ns-revalidation, rfc8624bis, dnssec-automation, grease, must-not-sha1, must-not-ecc-gost

Copyright © 2024 Japan Registry Services Co., Ltd.

# dnsop: 発行されたRFC 1/2

- 2023/12/22: RFC 9520 Negative Caching of DNS Resolution Failures
  - IW2022で報告
  - フルサービスリゾルバで名前解決失敗の情報をキャッシュし、権威サーバに大量のリトライを送らないようにする規定
  - セカンドレベルの設定間違いや無応答のせいで(com, net) TLDの権威サーバに大量のクエリが来るという問題を解決するため
  - リゾルバは失敗を1秒以上5分以下キャッシュし、その間は同じクエリを同じ権威サーバに送らないこと(MUST)
  - DNSSEC検証エラーをキャッシュすること (MUST)
- 2024/3/21: RFC 9499: DNS Terminology
  - RFC 8499からいくつかの項目を変更、追加
  - 変更: Forwarder, QNAME, Secure Entry Point
  - 委任の関係性でBailiwick廃止、unrelated追加
  - 追加: DoT, DoH, DoQ, Classic DNS, RDoT, ADoT, XoT
- 2024/4/26: RFC 9567 DNS Error Reporting
  - IW2022で報告: QTYPE NULL→TXT
  - 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オプションで応答に追加
  - 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
    - 報告エージェント情報hのついた応答を受け取り、検証エラーになったとき以下のクエリを送る
    - QNAME=_er.Errorcode.QTYPE.QNAME._er.AgentDomain
    - Errorcode: 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
    - QTYPE=TXT
    - 例: _er.7.1.broken.test._er.eporting-agent.example TXT

Copyright © 2024 Japan Registry Services Co., Ltd.

# dnsop: 発行されたRFC 2/2

- 2024/7/16: RFC 9615 Automatic DNSSEC Bootstrapping Using Authenticated Signals from the Zone's Operator
  - CDS/CDNSKEYによるDS自動更新の拡張
  - DNSプロバイダが顧客ドメイン名のDNSSECを運用する場合に、最初のDSがないときにCDSを信頼できるところから得るためにDNSプロバイダのDNSサーバ名以下にCDS/CDNSKEYを書き、Registry/Registrarがそこからcds/cdnskeyを取得する

  _dsboot.顧客ドメイン名._signal.DNSサーバ名. IN CDS

  顧客ドメイン名. IN NS DNSサーバ名.
  - DNSプロバイダは署名済→_dsboot CDSも署名済
  - 顧客ドメイン名の頂点にも同じCDSを書くこと
  - 例:

  _dsboot.example.co.uk._signal.ns1.example.net. IN CDS 12345 13 2 xxxxxxxx

  example.co.uk. IN NS ns1.example.net.

  example.co.uk. IN CDS 12345 13 2 xxxxxxxx
- 2024/7/24: RFC 9619 QDCOUNT Is (Usually) One
  - IW2023で報告
  - Update RFC 1035: OPCODE 0の場合はQDCOUNT≦1
  - OPCODE=0 かつ QDCOUNT>1の場合はFORMERR
- 2024/10/11: RFC 9660 The DNS Zone Version (ZONEVERSION) Option
  - 権威サーバの応答に、応答データのゾーン頂点のドメイン名とSOAシリアル番号などを返すためのEDNSオプション
  - QNAME中のゾーン頂点までのラベル数と、タイプに応じた値を返す
- 2024/4/11: RFC 9558: Use of GOST 2012 Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC
  - IW2023で報告
  - ロシアのGOST 2012署名アルゴリズムをDNSSECで使えるようにするもの
  - Independent Submission (IETFの成果ではないRFC)
  - 実装はOPTIONAL
  - Digest Type 5
  - Algorithm 23 ECC-GOST12

Copyright © 2024 Japan Registry Services Co., Ltd.

# dnsop WG での議論 1/2

- draft-ietf-dnsop-avoid-fragmentation
  - DNS/UDPでIP Fragmentationを避けるBest Current Practiceを目指した提案
  - 2024/3: IESGが、より安全側に倒そうとする
  - 2024/4: DNS実装者(ISC, NLnet Labs, CZ.NIC, PowerDNS) 連名でBCPに反対
  - 2024/5/4 平日なのでミーティングに呼び出し
  - Informational に変更
  - こうすれば安全になるという記述に変更
  - 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
  - 2024/9/26 IESGが発行承認、RFC Editorへ提出
- draft-davies-internal-tld: Top-level Domain for Private Use
  - .internal TLDがICANNによって予約された
  - IETFでもPrivate addressのように認めてほしい

  → ICANNとは距離をとりたい人がそれなり
- draft-ietf-dnsop-rfc8624-bis
  - DNSSECで推奨するアルゴリズムの管理方法を改良
  - 現在はRFC 8624で規定
  - IANA DNSSEC Tableに推奨アルゴリズムの表を作る
  - 項目を追加
    - 署名, 検証に使うアルゴリズム
    - 署名, 検証をソフトウェア実装するアルゴリズム
    - 委任, 検証に使うダイジェストアルゴリズム
    - 委任, 検証をソフトウェア実装するダイジェストアルゴリズム
  - アルゴリズム、項目ごとに MUST, RECOMMENDED, OPTIONAL, MAY, MUST NOT, NOT RECOMMENDED
  - 議論: 署名に使うアルゴリズムを複数MUSTと書くとすべて使わないといけないというふうに読めるので、RECOMMENDEDとする
- draft-ietf-dnsop-must-not-sha1
  - DNSSEC委任・検証でDigestType 1 sha1使用禁止
- draft-ietf-dnsop-must-not-ecc-gost
  - DNSSEC署名・検証でECC-GOST (12)使用禁止
  - RFC 9558 GOST 2012 (アルゴリズム23) とは別

Copyright © 2024 Japan Registry Services Co., Ltd.

# dnsop WG での議論 2/2

- draft-ietf-dnsop-grease
  - Greasing Protocol Extension Points in the DNS
  - GREASE (Generate Random Extensions And Sustain Extensibility)
    - 割り当てられていないプロトコル番号などを定期的に使用
    - Middleboxや欠陥のある実装により使用できないパターンが決まってくるのを防ぐ
    - RFC 8701: Applying GREASE to TLS extensibility
    - RFC 9287: Greasing the QUIC Bit
  - DNSでも、ヘッダフラグ、Type, Class, Opcode, EDNS version, EDNS Opt Codeに使われない値が多数ある
  - テストに使ってよい値を決めておこうという提案

- draft-fujiwara-dnsop-dns-upper-limit-values
  - Upper limit values for DNS
  - DNSには上限値が決められていないパラメータあり
    - RRSet中のResource Record数
      - 委任のNS数、glue A, AAAA数, DS, DNSKEY, RRSIG数
    - CNAME/DNAME連鎖数, 外部名のみの委任の段数
    - DNSパケットサイズ (＜64kB)
  - 多数書くだけで攻撃が成立
    - DS, DNSKEY, RRSIGを多数指定した攻撃がKeyTrap
    - DNS反射攻撃, NS多数書く攻撃、CNAME長い攻撃
  - それぞれに上限値を決めればよいという提案
    - 例:RRSet中のRecord数は root com NSが13なので　≦13
  - 既存実装による上限値
    - BIND 9.18.28: max-records-per-type 100 (RR数上限)
    - Unbound: MAX_VALIDATE_RRSIGS 8 (RRSIG数)
    - Unbound: max-query-restarts 11 (CNAME連鎖数上限)
  - 提案したばかりで、賛否両論、使い方に制限すべきでないという意見もある

Copyright © 2024 Japan Registry Services Co., Ltd.

# 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)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
- IETF 120 (2024/7), IETF 121 (2024/11) に議論

- DELEG RR案があったが、それにとらわれない形で慎重に議論をすすめている
- いまは、要求仕様をすすめている
  - 既存のドメイン名登録モデルを壊さない
  - 既存のDNSとの互換性
  - 既存のDNSソフトウェアに悪影響を与えないこと
  - 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
  - 一つのドメイン名に複数のDNSプロバイダを使えること

Copyright © 2024 Japan Registry Services Co., Ltd.

# 参考: DELEG RR案

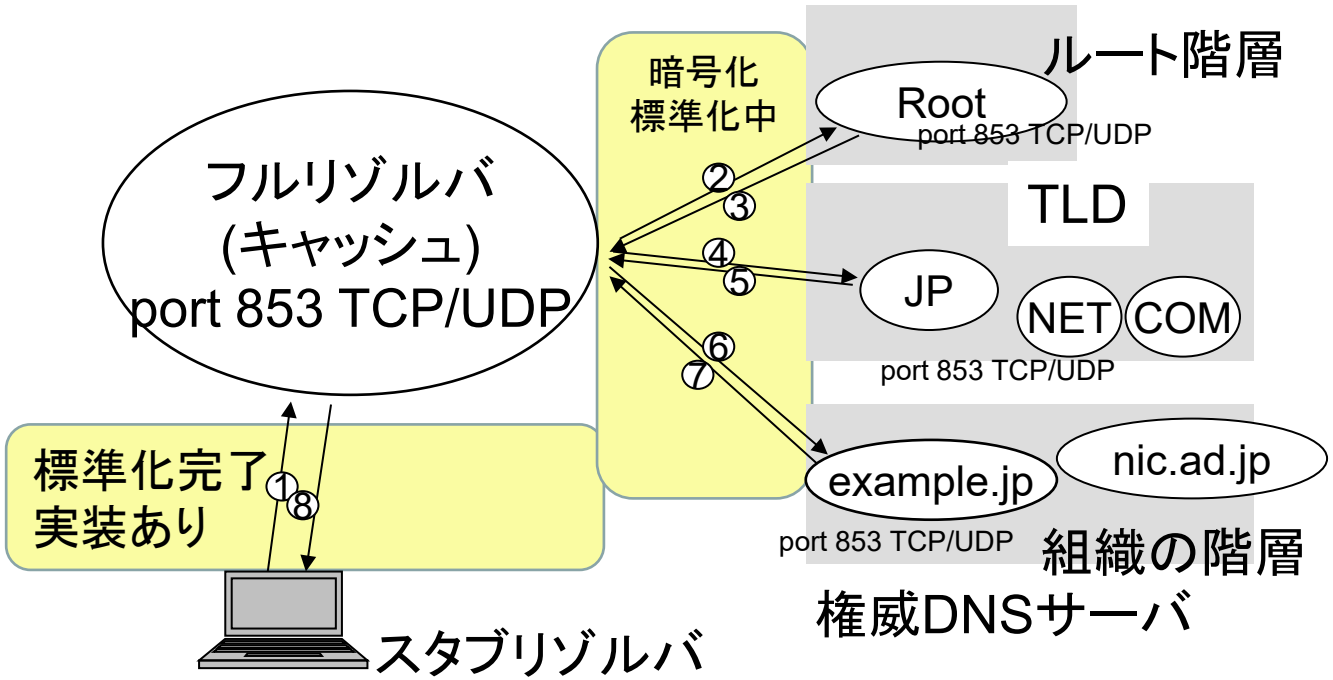
- DELEG RRTYPE提案: SVCB/HTTPSと同じ形式
  - in-domainの委任の場合
    - TargetNameにネームサーバ名
    - ipv4hints, ipv6hintsにIPアドレス
    - transport=dot, doq
    - tlsa= に、DoT/DoQで使う証明書をTLSA Recordの形式で書く
    - 例: company1.example. DELEG 1 ns.company1.example. (ipv4hint=192.2.0.1 transport=dot)
  - sibling, unrelated の委任の場合は、SVCBへのALIASを書く
    - company1.example. DELEG 0 ns1.provider1.example.
      - company1.example. は、provider1のns1.provider1.example. というサーバセットに委任
    - ns1.provider1.example. SVCB 1 ns1.provider1.example. (ipv4hint=… transport=dot)
      - プロバイダ側の設定で ns1.provider1.example. に複数の権威サーバを書ける
    - 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)

Copyright © 2024 Japan Registry Services Co., Ltd.

# 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

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




Copyright © 2024 Japan Registry Services Co., Ltd.

# RFC 9539: Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS

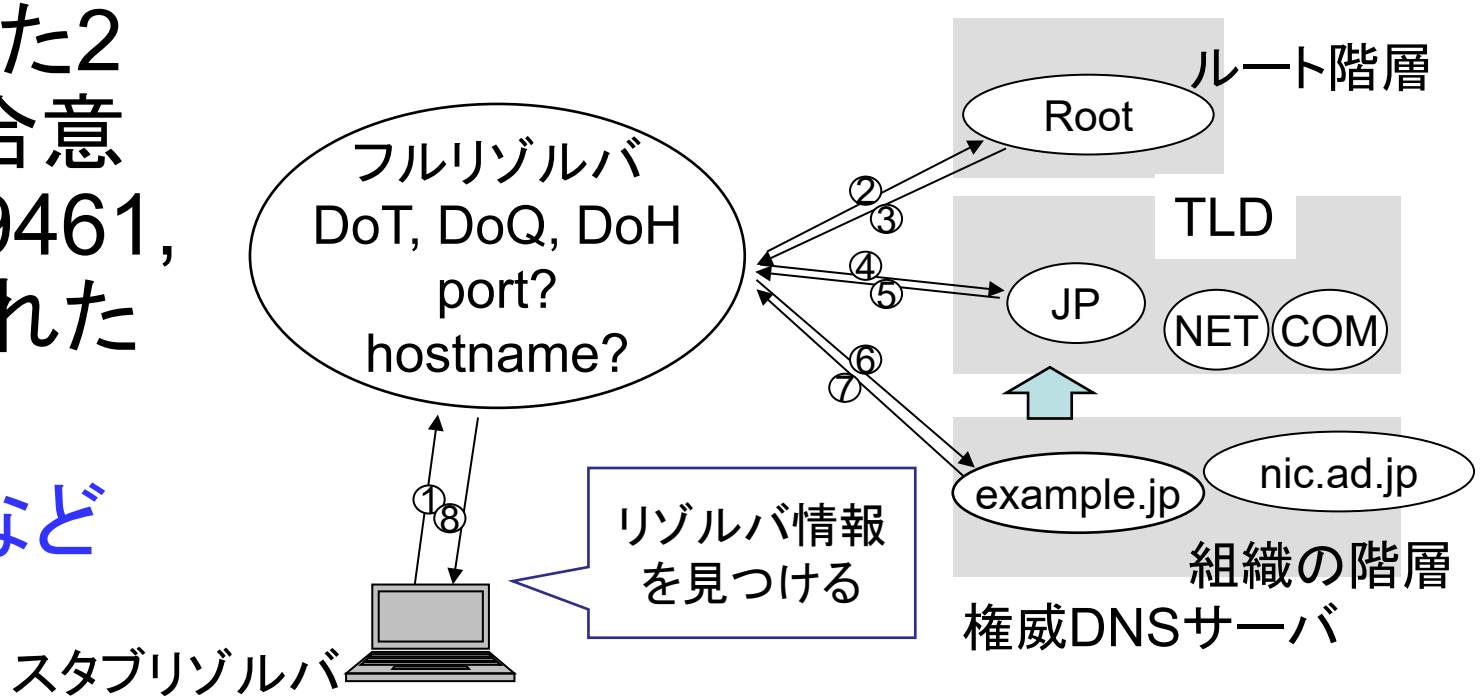
- 2024/2/28に発行された
  - フルサービスリゾルバから権威サーバへの暗号通信の一方的な日和見的な実装
  - 対応する権威サーバは、port 853でDoT、DoQで応答すること (SHOULD)
  - 名前解決時に権威サーバへDoT/DoQ接続し、接続できなければ通常のUDP/TCP port 53で問い合わせる
  - DoT/DoQで接続できた・できないという情報をキャッシュしておく
  - 証明書検証はしない (検証失敗でも拒否してはならない (MUST NOT))
  - Experimental (実験) プロトコルとしての標準化
  - PowerDNSが実装(PowerDNS Recursorとpowerdns.comの権威サーバ)
    - 例: dig +tls @pdns-public-ns1.powerdns.com. powerdns.com NS
- DNS関係者の関心はRFC 9539から DELEG RRに移ったようで、1年間dprive WGの進展はない
  - DELEG RRにDoT/DoQ対応と証明書情報を載せられれば問題が解決するため

Copyright © 2024 Japan Registry Services Co., Ltd.

# 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
- 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
- 2024年にリゾルバ情報(RESINFO)、split DNSなどの標準化も完了

- 機能追加が議論中
  - 他のDNSリゾルバにリダイレクト
  - RESINFOにdns64
  - RESINFO にDNSSEC検証




Copyright © 2024 Japan Registry Services Co., Ltd.

# 参考: add WG: 2023/11/6にRFC発行

- RFC 9461: Service Binding Mapping for DNS Servers
  - SVCBにDNS情報を記述する
  - _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} )

Copyright © 2024 Japan Registry Services Co., Ltd.

# add WG: 発行されたRFCなど

- 2024/6/28: RFC 9606 DNS Resolver Information
  - IW2023で紹介、sigが削除された
  - RFC 9463のauthentication-domain-name (証明書ドメイン名)のRESINFO RRにリゾルバ情報を公開する
  - 例: resolver.example.net. 7200 IN RESINFO qnamemin exterr=15,16,17 infourl=https://resolver.example.com/guide
    - そのリゾルバはqname minimisationに対応している
    - Extended DNS Errors 15,16,17を返す
    - リゾルバの詳細は、infourlに書かれている
  - RESINFO RR TYPE 261
- draft-ietf-add-split-horizon-authority
  - Establishing Local DNS Authority in Validated Split-Horizon Environments
  - IW2023で紹介:曖昧だった部分が書き直された
  - IESGが発行承認し、RFC Editor作業中
  - 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…….”

Copyright © 2024 Japan Registry Services Co., Ltd.

# 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
  - Apple Bonjourで実装している機能で足りないものを標準化しようとしている？
  - 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
- IESG承認済、RFC Editor作業中
  - draft-ietf-dnssd-srp
    - Service Registration Protocol for DNS-Based Service Discovery
    - Multicast DNSの端末がSleep状態でも答えるプロキシー
    - 9/30にAUTH48 (RFC Editorから著者への最終確認)
    - AUTH48で大幅に書き換える必要ができたらしく、WGLCからやり直しになりそう
  - 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
    - 9/30にAUTH48

Copyright © 2024 Japan Registry Services Co., Ltd.

# dnssd: IETF 119-121での議論

- draft-ietf-dnssd-multi-qtypes
  - 一つのクエリで複数のQTYPEを問い合わせるもの
  - 昔dnsop WGで提案され、流れたもの
  - クエリセクションの問い合わせに追加して、複数のタイプをMQTYPE-Query EDNSオプションで与える
  - サーバ側はクエリセクションの問い合わせと同じRCODEの場合だけ、追加されたQTYPEの応答を追加する
  - dnssd WGでのA/AAAA/HTTPSクエリを1パケットで送るという要求に応じて復活
  - QNAMEが違うSRVも同時に問い合わせたいという意見あり (できないけど)
  - 普通のDNSでも使えそう
- その他のドラフトはSRP待ちのようで、あまり進展がない
  - 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
  - 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
  - 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
  - 今後もまだ仕様がかわりそう

Copyright © 2024 Japan Registry Services Co., Ltd.

# 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
- deleg WG
  - DNSの委任部分の大改造を行うWGが動き始めた
  - 慎重に要求仕様の検討を行っている
- 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
  - 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標準化完了
- 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
  - (Open)Thread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

Copyright © 2024 Japan Registry Services Co., Ltd.

# 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/121/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

Copyright © 2024 Japan Registry Services Co., Ltd.