DNS 標準化動向 in IETF 102th

東京大学　総合文化研究科
石原知洋

本日の内容

- DNS プロトコル関連
  - dnsop - DNS 運用のガイドライン等を作成
  - dprive - DNS の通信暗号化

- DNS 応用関連
  - dnssd - DNS Service Discovery(RFC 6763) の拡張
  - homenet- ホームネットワーク(zeroconf + service discovery)
  - Dmarc - （非開催）

- Non-wg BOF / Side meeting
  - Driu

dnsop wg

dnsop

- 他の WG からのお知らせ
  - dnssd が新しいチェアを探している
  - dmarc で WGLC になっているドラフトについて、DNS guys のレビューが欲しい
    - draft-ietf-dmarc-arc-protocol
    - draft-ietf-dmarc-rfc7601bis

WGLC が完了したドラフト

- draft-ietf-dnsop-terminology-bis
  - RFC 7719 DNS Terminology のアップデート
  - 新規用語の収集と、用語定義の変更
- draft-ietf-dnsop-kskroll-sentinel
  - DNSクエリを使って、DNSSEC Validator のトラストアンカーの状況をクライアント側から調べるための仕組み
  - Root KSK Rollover の進行状況を調べるために使用することを想定
- draft-ietf-dnsop-attrleaf
- draft-ietf-dnsop-attrleaf-fix
  - "_プロトコル名" のレジストリを作る提案
  - SRVやTLSA, OpenPGPKEYなどで使用
- draft-ietf-dnsop-isp-ip6rdns
  - ISP で IPv6 の逆引きをどうするかの事例(Informational)

dnsop
ongoing draft / new draft

- draft-ietf-dnsop-algorithm-update
- draft-woodworth-bulk-rr
- draft-huque-dnsop-multi-provider-dnssec
- draft-pwouters-powerbind
- DNS Cookies and their Operational Impacts
- Let's Talk CNAME @ APEX
- dns-ietf-dnsop-wireformat-http
- draft-song-atr-large-resp
- draft-tariq-dnsop-iviptr
- draft-wessels-dns-zone-digest
- draft-kh-dnsop-7706bis

draft-ietf-dnsop-rfc5011-security-considerations Security Considerations for RFC5011 Publishers

- RFC5011 を用いて Trust Anchor のロールオーバーをする際の鍵追加・失効のタイミングについて、数学的な前提をもとに述べたドラフト
- 「This document contains much math and complicated equations」と概要に書いてある

- WGLC に戻り、Informational に変更
- dnsop ML にて追加審議、コメント受付

draft-ietf-dnsop-algorithm-update Algorithm Implementation Requirements and Usage Guidance for DNSSEC

- DNSSEC で使う鍵アルゴリズムの要求およびガイダンス
- RFC6944 を更新
  - 暗号アルゴリズムが名指しで書いてあるので、RFC化後もこれを obsolete する文書が出続けるものと思われる

Algorithm Implementation Requirements and Usage Guidance for DNSSEC（続き）

Number	Mnemonics	DNSSEC Signing	DNSSEC Validation
1	RSAMD5	MUST NOT	MUST NOT
2	DSA	MUST NOT	MUST NOT
5	RSASHA1	NOT RECOMMENDED	MUST
6	DSA-NSEC3-SHA1	MUST NOT	MUST NOT
7	RSASHA1-NSEC3-SHA1	NOT RECOMMENDED	MUST
8	RSASHA256	MUST	MUST
10	RSASHA512	NOT RECOMMENDED	MUST
12	ECC-GOST	MUST NOT	MAY
13	ECDSAP256SHA256	MUST	MUST
14	ECDSAP384SHA384	NOT RECOMMENDED -> MAY（01 で変更）	RECOMMENDED
15	ED25519	RECOMMENDED	RECOMMENDED
16	ED448	MAY	RECOMMENDED

draft-huque-dnsop-multi-provider-dnssec Multi Provider DNSSEC models

- DNS プロバイダ（だいたいにおいてはレジストラが兼ねる）が提供するシステムは自サービスでの単独動作を想定しており、自動署名などはレジストラのシステムに統合されている
- 冗長性確保のために2つ以上のプロバイダで動かすことは少し難しい
- 複数のプロバイダで DNSSEC を運用する場合のベストプラクティス

- 一方で署名して一つは完全なスレーブとして動くモデルと、個々がマスターとして動作し、Inline signing するモデルが提案されている
- 後者の場合、KSK/ZSK の鍵をどのように持つか（シェアするか、各自別々のものを持つか）が3パターン紹介されている

draft-woodworth-bulk-rr
BULK DNS Resource Records

- ホストの逆引きなど、多量のレコードを必要とするものについて、変換ルール形式のレコードを定義する
- BIND などの $GENERATE と似た機能を標準に
  - ただし、$GENERATE のように実際に個々のレコードとして生成せず、あくまでサーバ上では「BULK A 形式のレコード」として保持
  - ゾーン情報をメモリ上に展開するときや、ゾーン転送をするときの転送量に効いてくる

BULK A レコード

```
example.com. 86400 IN BULK A (
        pool-A-[0-255]-[0-255].example.com. 10.55.${1}.${2}
        )
```

draft-woodworth-bulk-rr
議論

- DNSSEC にまつわる問題
  - On-the-Fly Signing しなければならない
- そもそも必要なのか、IPv6 の逆引きなんて登録するのか
- Dynamic Update (RFC2136)使えばいいんじゃない？
  - それが本当に実現可能なら・・・というもっともなコメントも

DNS Cookies and their Operational Impacts

- Willem Toorop , Ondřej Surý の発表
- サーバ実装がマルチベンダであったときのDNS Cookieについて考察
  - DNS Amplifier などに対抗するためには、広く Deploy している必要がある
  - マルチベンダ対応は必須
- 問題点
  - Anycast で複数サーバがある場合
    - 同一 Cookie Secret、同一アルゴリズム、etc…
    - 対応実装、非対応実装
  - さらにそれらが別実装であった場合
  - 各サーバ間での状態の同期

DNS Cookies and their Operational Impacts（続き）

- 対応策
  - DNS Cookie の暗号化アルゴリズムについて規定する
  - SipHash などの暗号化ハッシュの導入
  - それぞれのアルゴリズムに対して Mandatory , Optional などの要求を規定する
  - DNS 運用者に対するガイドラインの整備

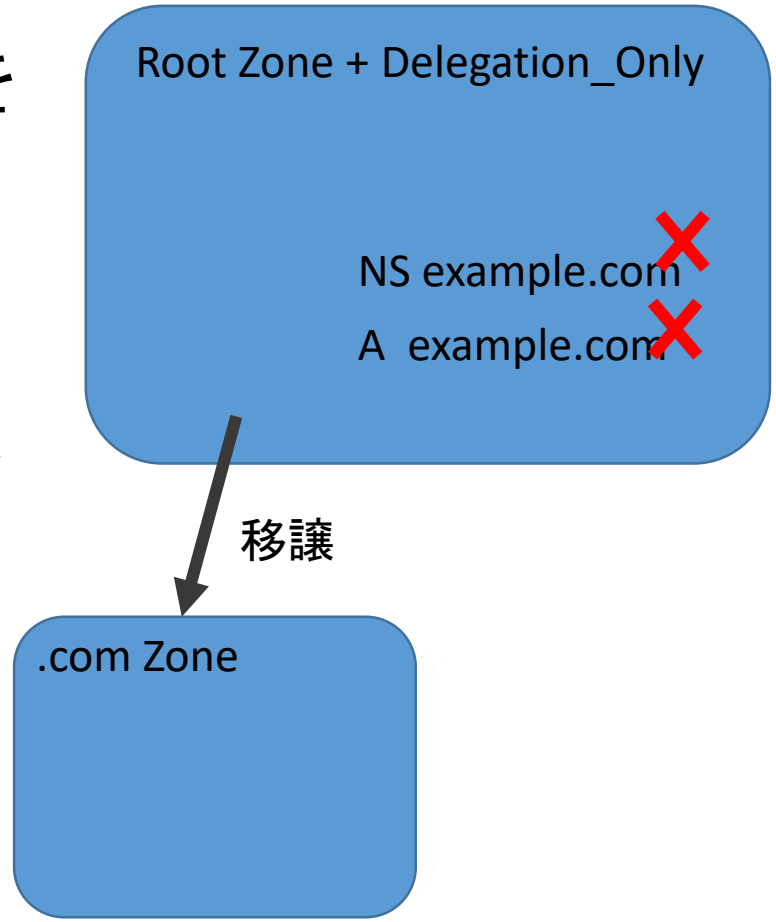
- 議論
  - どの程度の暗号化アルゴリズムを mandatory にするか？
  - 「そもそも TCP 使えばすべてが終わる、UDP を殺して（kill UDP）このような無駄な議論はやめるべき」という過激な意見も
  - （クライアントのトラッキングなど）プライバシーの問題を考える必要があるのでは？
  - 現時点での実装の相互接続性を継続議論、するか DNS Cookie を殺すドラフトを書く

Let's Talk CNAME @ APEX

- Zone APEX に CNAME を使うことについて
  - 本来のプロトコル上は許されない
    （CNAME は他のレコードと共存できない
    ＝ NS Record を持てない
    ＝ Zone APEX ではCNAME は使えない）
- とはいえ、できる DNS プロバイダはいくつもある
- 必要性も理解できなくもない（SRVなど）
- 「使えるところもあるのだから標準にすべき」とまでは言わないが、同じような事ができる「何か」を考え、そこへの移行を考えるべき
- 対応している DNS プロバイダとしていないプロバイダがあるのは困る
  - Amazon AWS で固めてないと動かない、など

The Delegation_Only DNSKEY flag draft-pwouters-powerbind

- DNSKEY に新しい Flag をつけ、「ラベル区切りを超えて署名しない」ことを示す
- 例えば、Root において DNSKEY に Delegation_Only フラグをつけた場合、example.com というような delegation はしない、example.com という名前の A レコードなども（root ゾーンには）持たないということを示す
- Cache Poisoning 対策



draft-song-atr-large-resp
ATR: Additional Truncated Response for Large DNS Response

- IPフラグメンテーションを適切に受信できない場合
- TCPでの再問い合わせを促すため、通常の応答の10ms後に、Truncatoin が起こったことを意味するTCビットがセットされた短い応答を追加で返すようにする提案

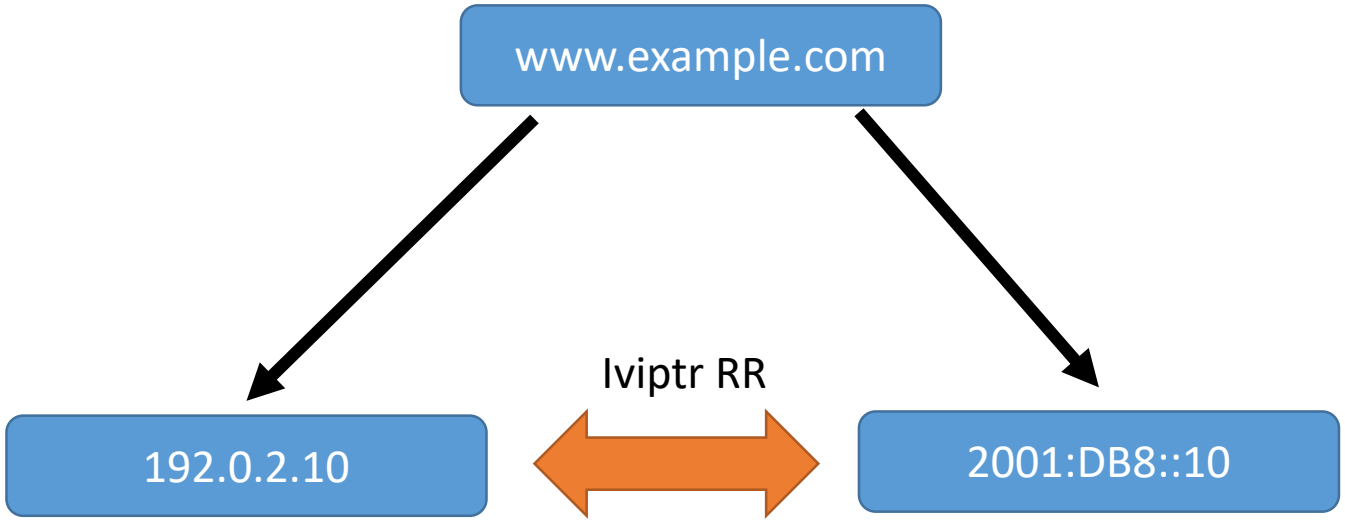
- 議論
  - Implementation の手間に比べて benefit が見えない
  - Amplification Attack がもっとひどいことになるのでは
  - 現時点での wg adoption は無しとの判断

draft-wessels-dns-zone-digest
Message Digest for DNS Zones

- ゾーンファイルのRR「全体」にダイジェストをつけて検証可能にしようという提案
  - Zone Transfer 以外でのゾーン情報の配布、その場合の検証方法
  - 例 : Root ゾーンを Zone Transfer 以外の方法で安全に配布できる
    - Local-root など
- 単なるファイル署名じゃいけないの？
  - 「ゾーンファイル」の形を保ってるとは限らない
  - 署名と対象ファイルを分けたくない
  - 実装に取り込むとnon-DNS の情報は消える、バイナリフォーマットになったり

draft-tariq-dnsop-iviptr
IVIPTR: Resource Record

- あるドメイン名に A と AAAA のリソースレコードがあったときに、A（or AAAA）を引くと、AAAA(or A)を返すレコード
  - v4/v6 のみ＋トランスレータ環境で、名前がない（ブラウザ等に直接IPアドレスを打ち込むような）場合
- 参加者から「必要性がよくわからない、元々を全てドメイン名で扱えばいいのでは？」とのコメント、あまり興味を引かなかった？



dprive WG

dprive

- DNS のプライバシーを扱う
- 以前は DNS over TLS/DTLS を策定していた WG
- 現在は DoT の運用についての BCP などを策定
  - draft-dickinson-dprive-bcp-op
  - draft-bortzmeyer-dprive-rfc7626
  - draft-annee-dprive-oblivious-dns

DNS-over-TLS Measurements with RIPE Atlas Probes

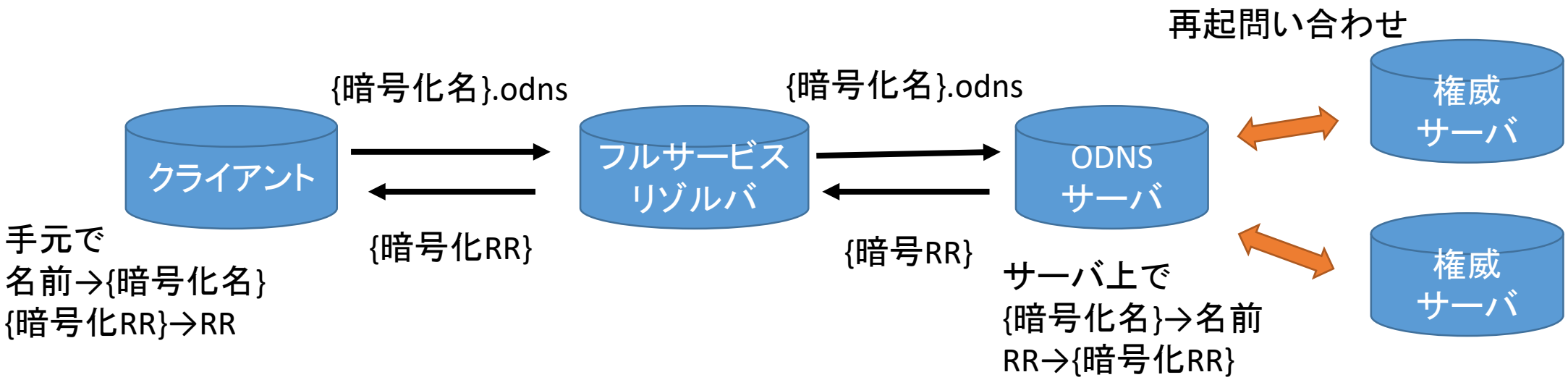
- RIPE Atlas probe で、DNS over TLS の計測対応と測定をおこなった、という発表

draft-dickinson-dprive-bcp-op
draft-bortzmeyer-dprive-rfc7626

- RFC7626 が書かれた当時は DNS over TLS も DNS over HTTPS もなかったが、今は大幅に状況が違う
- ２つのドラフトでセット
  - 考えられる脅威 : RFC7626-bis(このドキュメント）
  - 対応策 : dprive-bcp-op の内容内容
- 変更内容
  - DOT/DOH の内容を追加
  - DNS Payload について追加（特に DNS Cookie の記述など）
  - 暗号化通信に対して考えられる攻撃
  - サーバの認証
- WG Adoption

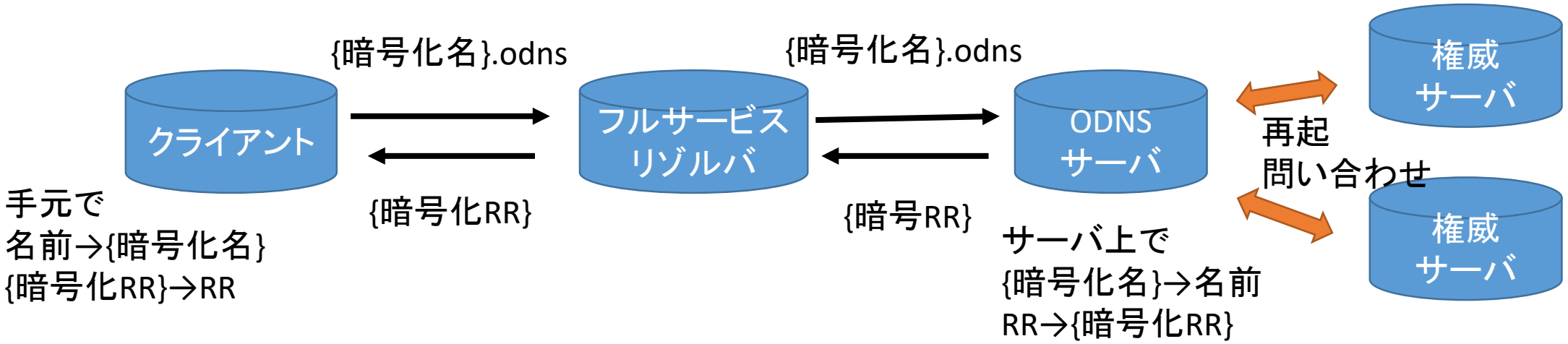
draft-annee-dprive-oblivious-dns
Oblivious DNS

- クライアントが聞きたい名前を {暗号化}.odns という形式でフルサービスリゾルバに聞いて、.odns のサーバ（ODNS Server）再起問い合わせをして名前解決
- フルサービスリゾルバには何を聞いたかわからない
- ODNSサーバには誰が聞いたかわからない



draft-annee-dprive-oblivious-dns Oblivious DNS：続き

- 議論
  - どのような Security Problem を解こうとしている？
    → Security Problem ではなく Privacy Problem
  - EDNS0 では OPT RR を forward する仕様になってない、プロトコルに対する修正が必要
  - ODNS Server が単一障害点にならないだろうか
  - リゾルバでのキャッシュ共有の利点はなくなりそう



driu (non WG)

driu

- DNS Resolver Identification and Use の略
- 議論のための BOF、Non-wg
- 主に DNS over HTTP などの、「どのリゾルバ使うのか」問題について議論
  - 「DNS でプライバシ」と考え始めると、DHCP で配られる Resolver が信じられるはずがない、という議論が始まり悩ましい問題

DHCPv6 DNS THREATS

- DNS クエリのプライバシーを考えたときに、DHCPv6 で設定する DNS はとてもじゃないが使えない
  - サーバが詐称される、結果として、不正な書き換えをされる、モニタされる、など
- どのようにして Resolver DNS を選ぶか、評価するか？
  - Reputation LIST?
- セッションでは、DHCPv6 encapsulating Option を利用してセキュアに DNS Discovery をする方法が提案
  - DHCPv6 Options for private DNS Discovery(draft-pusateri-dhc-dns-driu)

draft- nottingham-doh-digests
Choosing DoH servers from lists by target

- DNS over HTTPS で通信路は暗号化できるが、「どのサーバを選ぶか」という内容は議論されていない
- 一つの信頼できるサーバを予め選んでおく、というのは簡単で安全であるが、寡占によるデメリットが発生しやすい
  - 複数のサーバがオープンに DNS over HTTPS を提供し、それら複数のサーバを「安全に」選択できるメカニズムも提供する、という提案

- そこで、Broom Filter を使って各問い合わせのホスト名からダイジェストを計算し、その DoH サーバに問い合わせを送るか判断する

- 見たこともない人数が質問に並ぶ、という結果に
  - その Broom Filter を誰が作って、それは信じられるのか？など

Where’s my DNS

- DNS over TLS, DNS over HTTPS などの標準化が進み、現状、および今後の名前解決環境について総覧
- Encrypted DNS の pros & cons
  - 利点
    - トラフィックモニタ、DNS詐称、ポートブロッキングに強い（DoH のみ）
  - 欠点
    - Resolver トラフィックが集中することにより、サービス提供者は容易にトラッキングが可能
    - クライアント毎のDNSクエリ情報が外部ネットワークに漏れる

Where’s my DNS （続き）

- 今後のクライアントのスタブリゾルバはどうなっていくのか？
  - 現状のようにOS毎なのか、それともアプリごとになるのか？
    - 基本的に OS の機能アップデートはアプリケーションに比べて遅い、OS ができなければアプリは否応なく自前でやらねばならない
  - リゾルバがアプリごとになった場合、それぞれの DoH/DoT サーバの発見・選択は異なるリスト・方法が使われていくのか？
  - Firefox 62 は DoH を使えるようになる（もしくはデフォルトで？）
  - ユーザにはどのように通知していくのか？ユーザは（どのリゾルバ/DoH サーバを使ってるかについて）知るべきなのか
- 信じられる DoH サーバとは？
  - 唯一すべての問い合わせを知れる存在、どう信頼するのか？
  - アプリベンダはアプリ用に自前の DoH サーバを立てるかもしれない
  - 結局は大きい人たちの寡占になるかも

DNS 応用関連 wg (dnssd, homenet)

dnssd

- DNS を Service Discovery に使う、という標準について議論
- WGLC 済み、IESG
  - draft-ietf-dnsop-session-signal (DNS Stateful Operations)
  - draft-ietf-dnssd-push (DNS Push)
  - draft-ietf-dnssd-hybrid (Discovery Proxy)
- 議論中のドラフト
  - draft-ietf-dnssd-privacy (Privacy Extensions)
  - draft-huitema-dnssd-prireq (Privacy and Security Requirements)
  - draft-huitema-dnssd-privacyscaling (Privacy Scaling Tradeoffs)
  - draft-ietf-dnssd-pairing (Short Authentication Strings)
  - draft-ietf-dnssd-pairing-info (Pairing Design Issues)

dnssd：続き

- やはりここでもプライバシーの問題が出てくる
- 「他人に見えてほしくない」デバイスの問題
- さらに、誰がどんなサービスを Discovery しているかも知られたくもない
- 共有対象鍵を使ったプライバシー保護
  - スケーラビリティの問題が・・・

homenet

- 家庭につなぐネットワーク機器の zeroconf
- サービス提供用ゾーンの Master (Home Network Authority:HNA)を用いたシステムの提案
- いくつかのドラフトが進行中（WGLC に近い物が2つ）

- その後は？
  - Chair から、まだ CPE ベンダが homenet サービス実装しようとすると欠けているパーツがまだたくさんあるのでは、と提案

draft-ietf-homenet-front-end-naming-delegation Outsourcing Home Network Authoritative Naming Service

- 家でサービス発見用ゾーンの Master (Home Network Authority:HNA) を動かし、ISPにゾーン転送してISPのDNSサーバで公開
  - DNSSEC Sign は自前でやっても ISP に頼んでもよい（ただしHNAでやることを推奨はする）
- 外部から名前が引けるようになるので、家のサービスに名前でアクセスが可能
- だいぶ revise されて、そろそろ WGLC
- 実装も進んでいる

その他

IEPG presentation

Resolverless DNS side-meeting

IEPG Meeting

- DNS に関連した発表がいくつか

- old trust-anchors on github
  - github に追いてあるファイルは古い trust-anchor 使っている、その調査

- Dmap: Automating Domain Name Ecosystem Measurements and Applications
  - Registry, DNS, 名前に関連付けられたサービス(HTTP/SMTP等）を包括的に測定する枠組みと、テストケース

Resolverless DNS

- 非公式 meeting
- DNSOP に「以下のことについて議論しよう！」と突発的に案内

- (DNS)リゾルバのない環境が作れるか？それはどのようなものか？という議論
  - 例えば、ゾーンの情報はすべて HTTPS で転送、など
  - 名前の Uniqueness を崩すのではないか？という疑問
  - そこまで頑張っても名前解決の速度が遅ければユーザは（プライバシより）早い方に付いちゃうよ、など

- Resolverless DNS という ML を作り継続審議することに

まとめ

- 少し前までDNSプライバシのプロトコル標準の提案であったが、プロトコル標準が完了し、Deploy フェーズでの Best Current Practice 整備が増加
  - DNS プライバシ運用上の問題を解決する提案

- Driu/Resolverless DNS など、更にその先を見越した提案などがあり、これらの議論を元にさらに新しい提案が出てくる可能性
- 今までのDNSアーキテクチャから大きく変わるのかも？という予感を皆感じている