DNSプロトコルの変化

東京大学総合文化研究科

石原知洋

ここ最近の DNS プロトコル変化のホットトピック

- DNSSEC - 普及フェーズの議論
- UDP Fragmentation 対策
- DNS プライバシーの議論
  - DoH/DoT と運用やアプリケーションの議論

DNSSEC

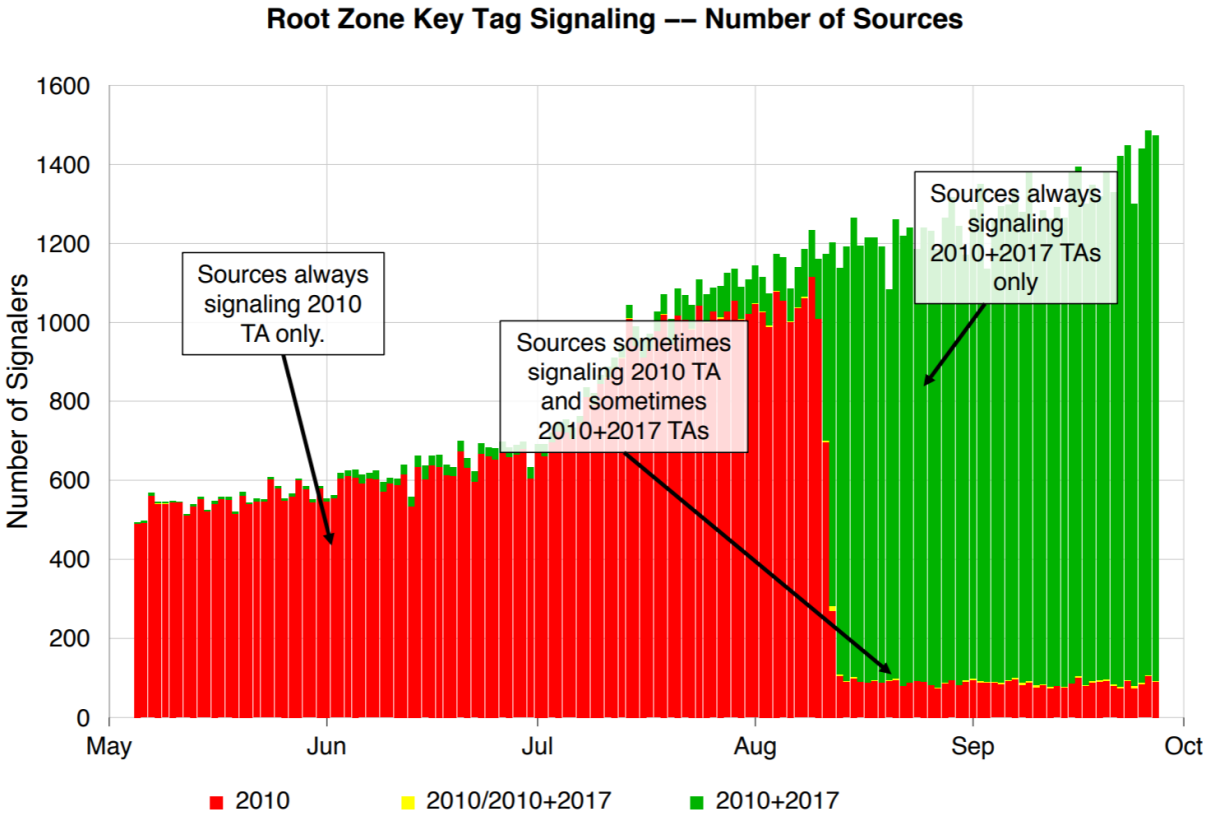
- DNSSEC は deploy を加速するフェーズへ
- Deploy 過程で見つかった様々な問題を議論
- 検証エラーの問題
  - どのように見つけるか？
  - 見つけたときにどうするか

DNSSEC 関連のRFC・ドラフト

- RFC
  - RFC8145 – Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)
  - RFC8198 – Aggressive Use of DNSSEC-Validated Cache
  - RFC8509 – A Root Key Trust Anchor Sentinel for DNSSEC
  - RFC8624 – Algorithm Implementation Requirements and Usage Guidance for DNSSEC
- ドラフト
  - DNS Extended Error(draft-wkumari-dnsop-extended-error)
  - Multi Signer DNSSEC models(draft-ietf-dnsop-multi-provider-dnssec)
  - Moving DNSSEC Lookaside Validation (DLV) to Histric Status (draft-ietf-dnsop-obsolete-dlv)
  - Responsibility for Authoritative DNS and DNSSEC Mistakes (draft-livingood-dnsop-auth-dnssec-mistakes)
  - In Case of DNSSEC Validation Failures, Do Not Change Resolvers (draft-livingood-dnsop-dont-switch-resolvers)
  - Operational recommendations for management of DNSSEC Validator (draft-mglt-dnsop-dnssec-validator-requirements)

KSK Rollover等による鍵変更の状況確認

- RFC8145 – Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)
  - Resolver が EDNS(0) により、Trust Anchor の鍵のバージョンを通知
  - Authoritative Server 側が鍵の普及状況を確認できる
- RFC8509 – A Root Key Trust Anchor Sentinel for DNSSEC
  - ユーザや第三者機関が Resolver が使っている鍵を確認できる



出典：A Look at RFC 8145 Trust Anchor Signaling for the 2017 KSK Rollover
Duane Wessels, DNS-OARC 26 San Jose, CA

新しいエラー情報
Extended DNS Error(EDE)
(draft-wkumari-dnsop-extended-error)

- DNS の status code は数種類しかない
  - NXDOMAIN, SERVFAIL, REFUSED, FORMERR, …
- 特に問題となるのは ServFail
  - （何かが原因で）DNSSEC で失敗すると ServFail, Lame Delegation で ServFail, Authoritative が reload 中で ServFail, etc..
  - とにかく「ServFail」しか言わないので、なぜそうなったか分からない
- というわけで、EDNS0 拡張を用いて新しいエラーを定義

EDE の一覧

- 0 : Other
- 1 : Unsupported DNSKEY Algorithm
- 2 : Unsupported DS Digest Type
- 3 : Stale Answer
- 4 : Forged Answer
- 5 : DNSSEC Indeterminate
- 6 : DNSSEC Bogus
- 7 : Signature Expired
- 8 : Signature Not Yet Valid
- 9 : DNSKEY Missing
- 10 : RRSIGs Missing
- 11 : No Zone Key Bit Set
- 12 : NSEC Missing
- 13 : Cached Error
- 14 : Not Ready
- 15 : Blocked
- 16 : Censored
- 17 : Filtered
- 18 : Prohibited
- 19 : Stale NXDOMAIN Answer
- 20 : Not Authoritative
- 21 : Not Supported
- 22 : No Reachable Authority
- 23 : Network Error
- 24 : Invalid Data

Operational recommendations for management of DNSSEC Validator (draft-mglt-dnsop-dnssec-validator-requirements)

- DNSSEC Resolver のオペレータ（DRO）に対する、安全なDNSSEC validation を行う Resolver を運用するためのガイドライン (Recommendation)
- (ネガティブ)トラストアンカーの運用や、PC の時刻の取り扱いなど、Resolver 起動時・実行中・イベントへの対応の３つのカテゴリにわけて推奨動作を規定
  - 起動時の TA のスクリーニングに失敗したら Resolver を立ち上げない、など

その他 DNSSEC 関連の話題

- IEPG での発表など
  - Detecting DNSSEC Validation Failure at Authoritative Servers
    - JPRS 米谷さんと NII 福田さんの研究発表
    - RIPE Atlas を用いて、世界中から DNSSEC Validation を行いその成否を確認
  - old trust-anchors on github
  - github に追いてあるファイルが古い trust anchor を使っているか調査

フラグメンテーションの議論

- 特にCache Poisoningで問題となるUDP Fragmentationの議論
  - 第二Fragmentを偽装したキャッシュポイズニング攻撃が容易
  - Fragmentを通さないネットワーク機器(Firewallなど)があると、名前解決が困難、または時間がかかる
- Avoid IP fragmentation in DNS(draft-fujiwara-dnsop-avoid-fragmentation)
  - Resolver のEDNS0 Requester のUDPペイロードサイズと、Authoritative の EDNS0 Responder の最大ペイロードサイズを実際のpath MTUの値(からIP ヘッダ・UDPヘッダ分を除いたもの)か、1220から1400の間の値へ
  - IP_DONTFRAG/IPV6_DONTFRAGを付けて Fragment を抑制
  - これらを超える場合には TC bit を付けて返し、TCP への Fall back を要求
  - Resolver はすべての Fragmentation を無視して捨ててよい

プライバシーの議論(1)

- IETF88から始まったプライバシーに対する脅威の議論
  - RFC7258: Pervasive Monitoring Is an Attack
- 2014年に dprive wg 開始
  - DNS トランスポートの暗号化により、これらの脅威に対抗

- まずは足回りであるプロトコルの暗号化
  - EDNS(0) padding Option（RFC7830)
  - DNS over TLS (DoT)（RFC 7858）
  - DNS over DTLS（RFC8094）
  - DNS Queries over HTTPS (DoH) (RFC 8484)

プライバシーの議論(2)
クライアント・アプリケーションの動作

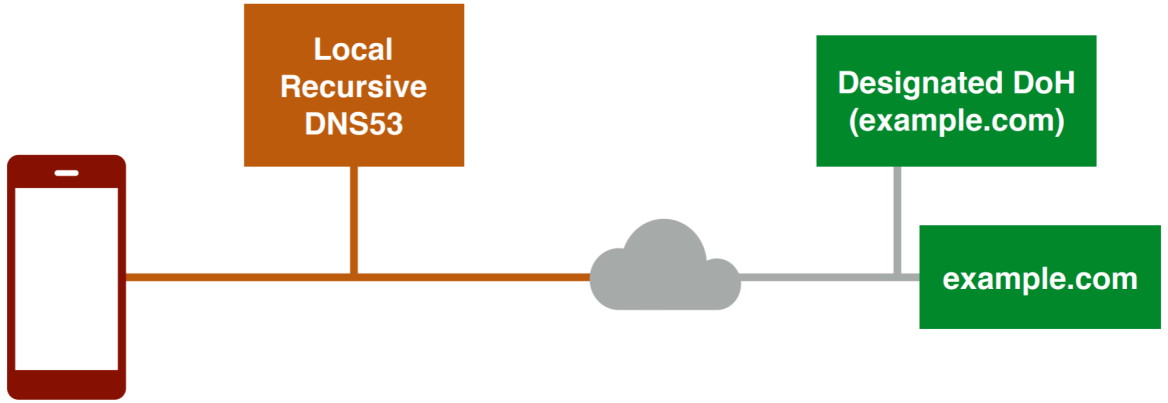
- 先ほどのプロトコルは通信方式を定めているが、どの Resolver を選択するかは仕様の範囲外
- 実際にクライアントはどの (Encrypted) Resolver を使うのか、という話題に話がシフト

プライバシーの議論(3)
クライアントの設定・動作についてのドラフト

- DNS Resolver Information Self-publication
- DNS Resolver Information: "doh"
- DNS Resolver-Based Policy Detection Domain
- Adaptive DNS: Improving Privacy of Name Resolution
- A Bootstrapping Procedure to Discover and Authenticate DNS-over-(D)TLS and DNS-over-HTTPS Servers
- Selecting Resolvers from a Set of Distributed DNS Resolvers
- DNS over HTTP resolver announcement Using DHCP or Router Advertisements
- Indication of Local DNS Privacy Service During User Access
- Client DNS Filtering Profile Request
- DNS over HTTPS (DoH) Considerations for Operator Networks
- A privacy analysis on DoH deployment
- Centralized DNS over HTTPS (DoH) Implementation Issues and Risks
- Centralised Architectures in Internet Infrastructure

Adaptive DNS: Improving Privacy of Name Resolution (draft-pauly-dprive-adaptive-dns-privacy)

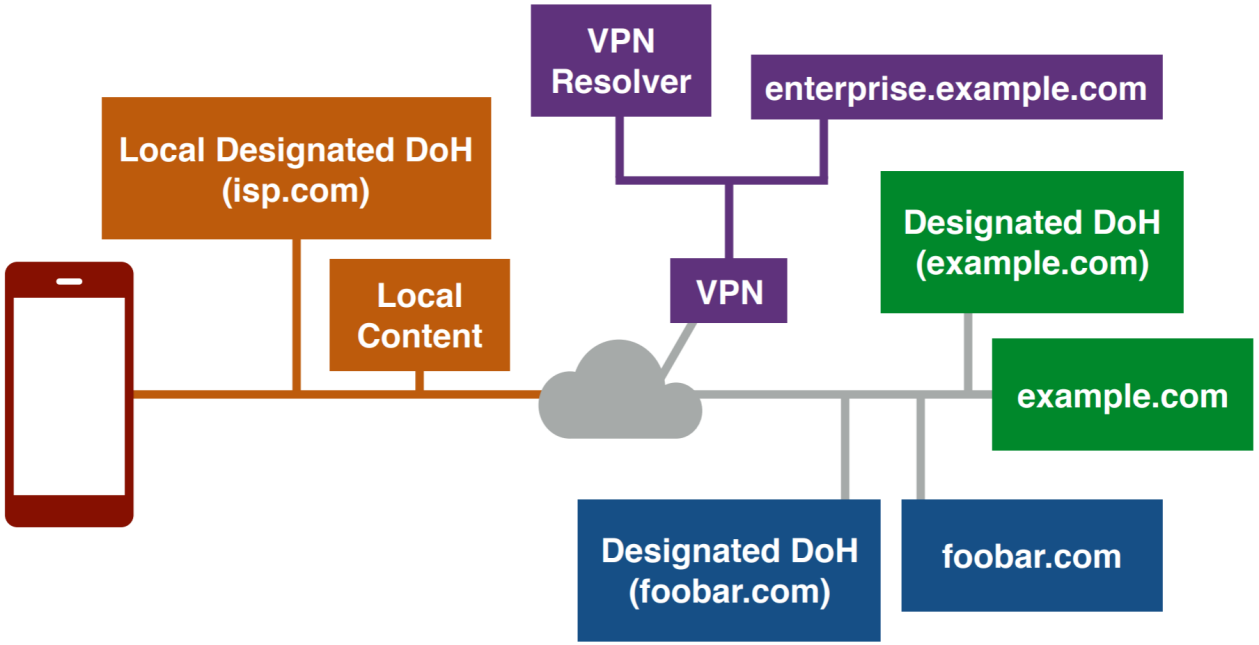
- クライアントが対象ドメインごとに「専用の」Resolverを選択する提案
- HTTPSSVC レコードで、対象となるドメインのResolverを取得
  - この時はネットワークから得た Resolver を使い、DNSSEC 検証



出典：https://datatracker.ietf.org/meeting/106/materials/slides-106-abcd-adaptive-dns-privacy
Tommy Pauly, Chris Wood, Eric Kinnear, Patrick McManus ABCD IETF 106, November 2019, Singapore

Adaptive DNS: Improving Privacy of Name Resolution (draft-pauly-dprive-adaptive-dns-privacy)

- Resolver ごとに優先順位を付けて利用
  - VPN Resolver
  - Homenet などで指定されたローカル Resolver(後述)
  - 指定された DoH Resolver
  - Oblibious DoH Resolver (後述)
  - ネットワークから得た Resolver



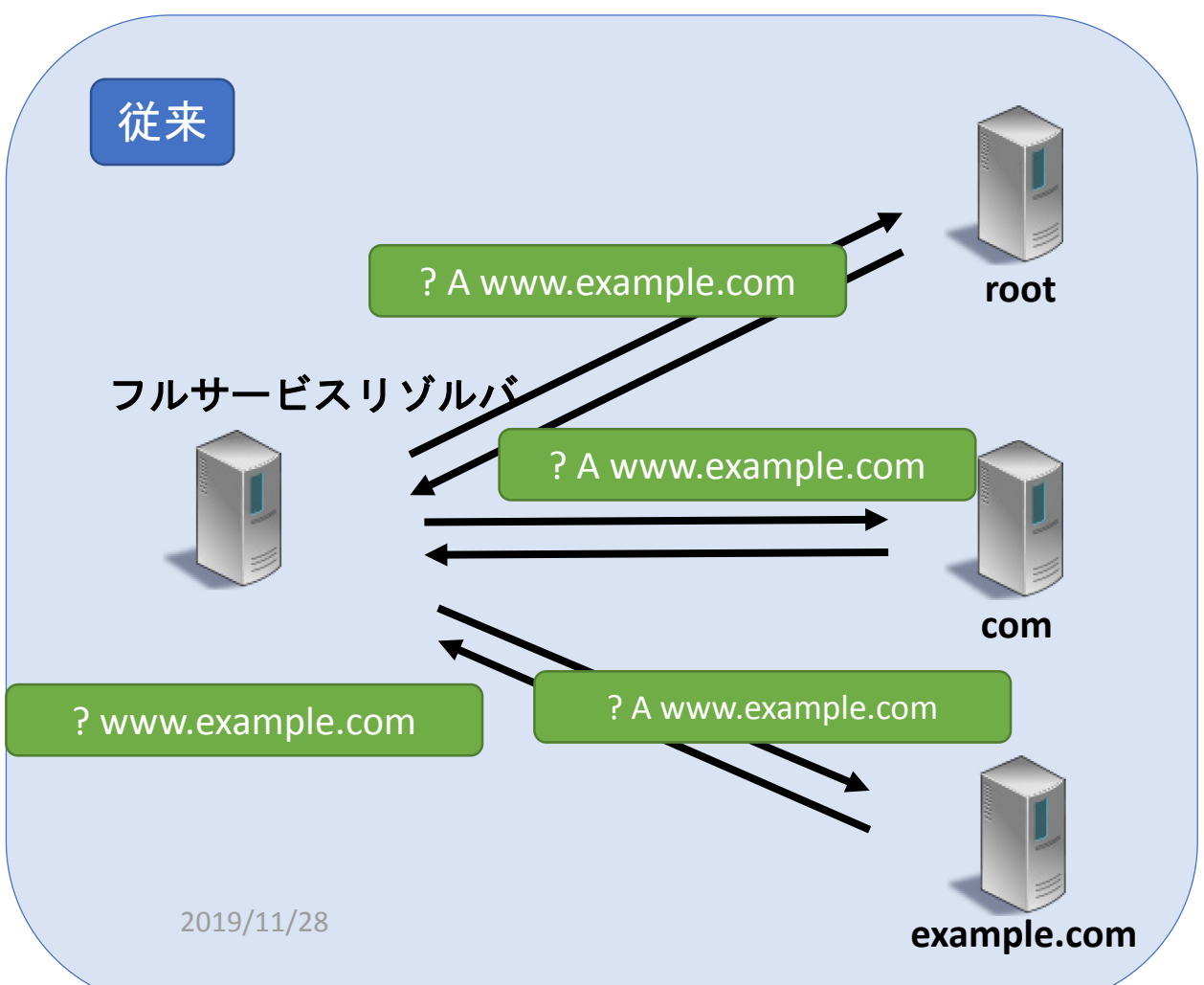
出典：https://datatracker.ietf.org/meeting/106/materials/slides-106-abcd-adaptive-dns-privacy
Tommy Pauly, Chris Wood, Eric Kinnear, Patrick McManus ABCD IETF 106, November 2019, Singapore

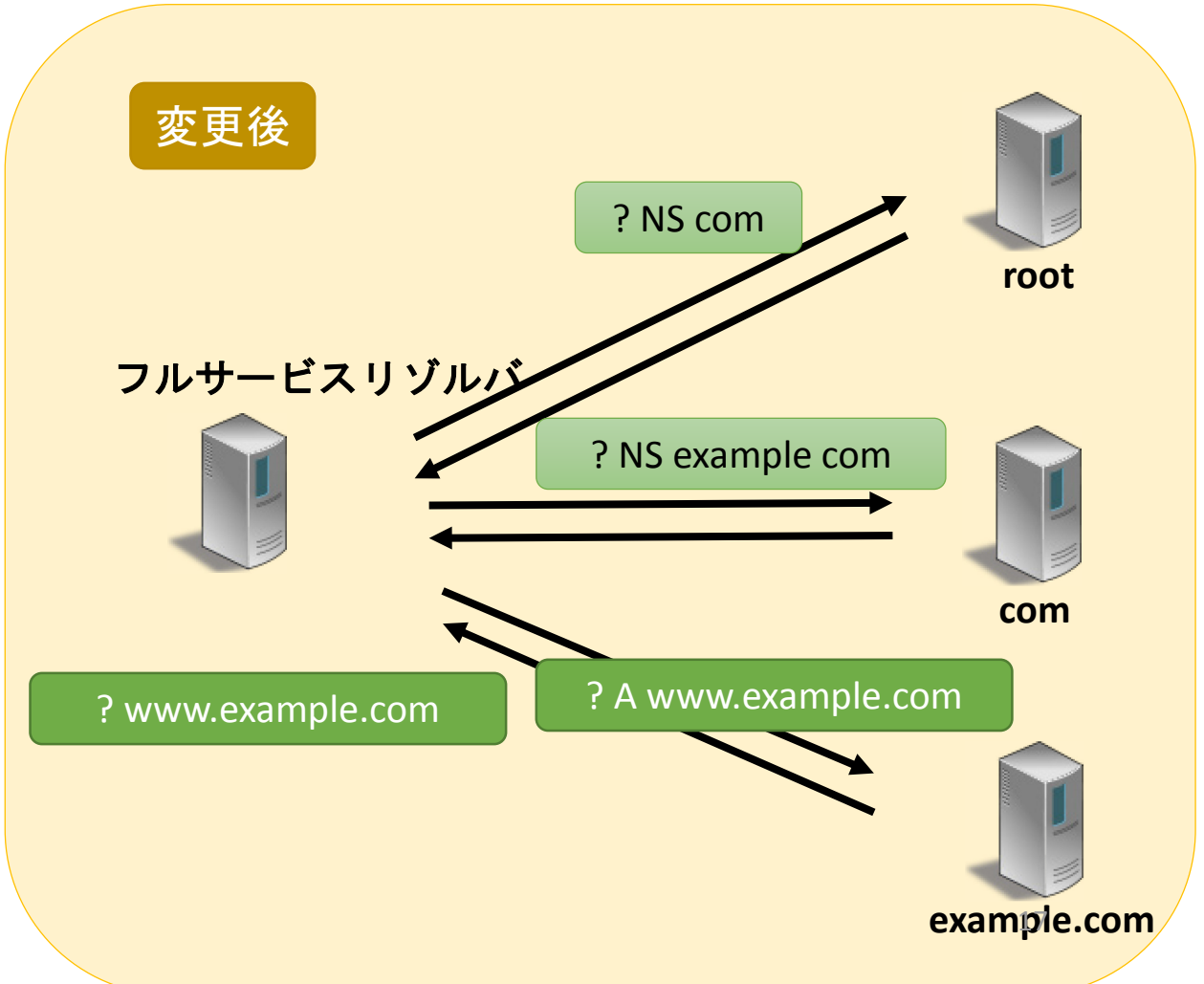
プライバシーの議論(4)
dprive フェーズ2

- 当初の dprive ではクライアントの stub resolver と full service resolver 間の通信にフォーカス
- それらの標準化が終わり、フェーズ２として full service resolver と Authoritative Server 間の通信の暗号化に議論が発展している
  - DNS Privacy Requirements for Exchanges between Recursive Resolvers and Authoritative Servers(draft-lmo-dprive-phase2-requirements)
  - Root も対応か、という話もあるが、Root へは Qname minimization さえすれば大した情報は漏洩しないのでは、という反論もある
- Oblivious DNS など、間に proxy を入れることでさらに Privacy を向上する仕組みなども提案されている

Qname Minimization(RFC7816)

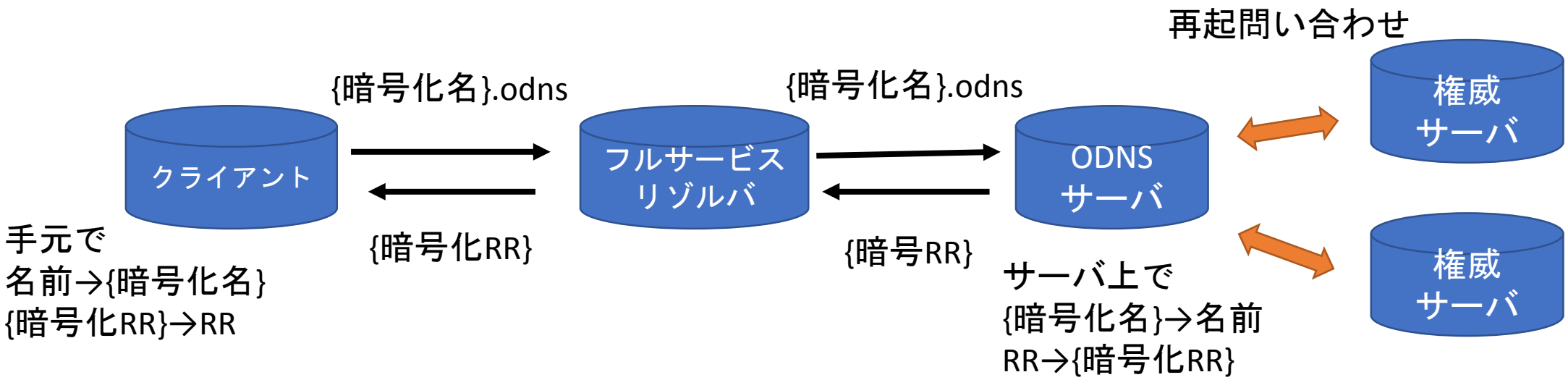
- 権威サーバに送られる情報を最小化





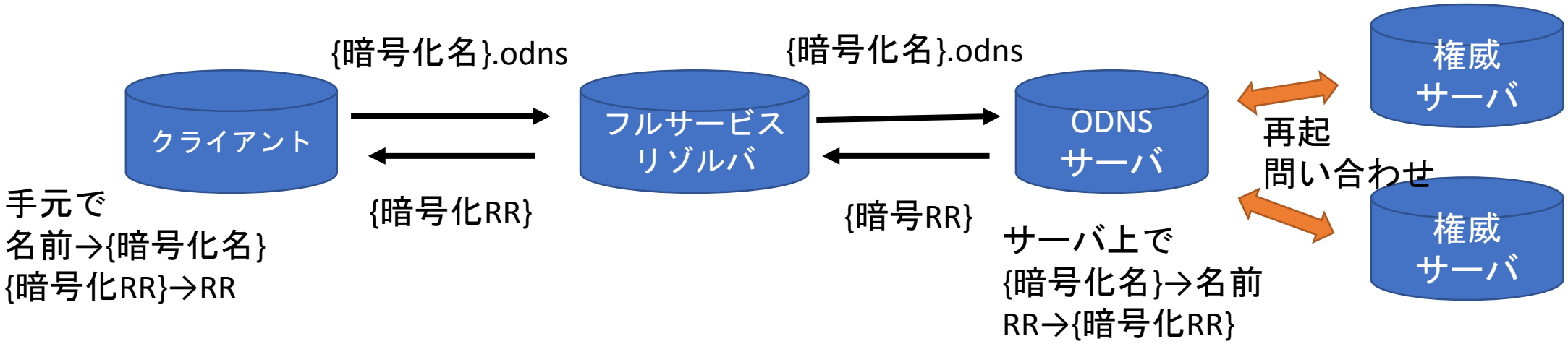
draft-annee-dprive-oblivious-dns
Oblivious DNS

- 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
  - 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
- DoH に対応した Oblibious DoH という提案もおこなわれている



DoH/DoT とアプリケーションのその他の議論

- Mozilla Canary Domain
  - Mozilla Firefox の独自拡張（標準化するかは未定）
  - DNS ベースでの Contents Filter がかかっている際に、DoH を使わないようにアプリケーションへ通知
  - 特有のドメイン名[use-application-dns.net]を引くことで、その環境で DoH を使わないことが指定されているかどうか判断
  - ネットワーク管理者は RPZ などを使いこのドメインを書き換える

IETF でアプリケーションの暗号化 DNS運用を論じる side meeting / BOF

- DNS Resolver Identification and Use(DRIU)
  - Side meeting
- Application Doing DNS(ADD)
  - BoF
- Application Behavior Considering DNS(ABCD)
  - BoF
  - WG 化の Charter などについて議論

その他、DNS プロトコルへの変更提案

- Interoperable Domain Name System (DNS) Server Cookies(draft-ietf-dnsop-server-cookies)
  - DNS cookie の生成アルゴリズム標準化
  - Primary/secondary 間で異なる実装の場合にも問題ないように
- DNS TIMEOUT Resource Record(draft-pusateri-dnsop-update-timeout)
  - DNSレコードの Dynamic Update 時の Lifetime の情報をレコード化し、secondary や、キャッシュと共有
  - TIMEOUT RR は時間が切れて本体の RR を消したら自分も消える
- Serving Stale Data to Improve DNS Resiliency(draft-ietf-dnsop-serve-stale)
  - Resolver のキャッシュが切れて再問合せが発生した際に名前解決ができなかった場合、キャッシュ切れの元データをクライアントに返す提案

dnssd

- DNS を Service Discovery に使う、という標準について議論
- ドラフト
  - draft-ietf-dnssd-prireq (Privacy and Security Requirements)
  - draft-ietf-dnssd-push (DNS Push)
  - draft-ietf-dnssd-hybrid (Discovery Proxy)
  - draft-ietf-dnssd-srp (Service Registration Protocol for DNS-Based Service Discovery)

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 を目的とした WG
- Special-Use Domain 'home.arpa.'(RFC 8375)
  - Homenet のサービス用ドメイン
  - 家庭内などのローカル環境での利用を想定、グローバルユニークではない
- Outsourcing Home Network Authoritative Naming Service(draft-ietf-homenet-front-end-naming-delegation)
  - 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
  - 家庭内とクラウドにネームサーバを配置し同期(暗号化チャネルで）
  - 外部接続が切れても homenet 内の名前解決が可能
- その他、いくつかのドラフトが進行中

まとめ

- DNS インフラのセキュリティ（真正性としての DNSSEC、秘匿性としての DoH/DoT）についての議論
- 標準化、実装も進んでおり、普及・運用についての議論が進みつつある
- 世間的にも、Firefox が Cloudflare の DoH サーバをデフォルトにしたり、Microsoft が DoH に対応します！と表明したり
  大きな変化がみられる