一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
IA2022-23(2022-09)

# 完全 DoH 化 DNS アーキテクチャに関する一検討

砂原 悟† 金 勇‡ 飯田 勝吉§

†公立千歳科学技術大学 〒066-8655 北海道千歳市美々 758 番地 65
‡東京工業大学 〒152-8550 東京都目黒区大岡山 2-12-1
§北海道大学 〒060-0808 北海道札幌市北区北 8 条西 5 丁目

E-mail: †s-sunaha@photon.chitose.ac.jp, ‡yongj@gsic.titech.ac.jp , §iida@iic.hokudai.ac.jp

**あらまし** DNS の通信では暗号化を伴わない UDP が主に用いられており、DNS キャッシュポイズニングによる改ざんや盗聴によるプライバシー漏洩の脅威が問題となっている。これらの脅威を緩和するために、DNS トラフィックの暗号化が有効である。現在、IETF によって、クライアントと DNS フルサービスリゾルバ間で暗号化通信を行うために、DNS over HTTPS (DoH)の標準化が行われ、いくつかの Public DNS や ISP などで DoH サービスの提供が始まっている。しかし、DNS フルサービスリゾルバと権威ネームサーバ間は現在も UDP で通信されており、DNS キャッシュポイズニングとプライバシーの保護への対策が十分とは言えない。本研究では、DNS の通信経路を全て DoH で暗号化を行う「完全 DoH 化 DNS アーキテクチャ」の手法を提案する。この手法より、クライアントから DNS フルサービスリゾルバ、そして DNS フルサービスリゾルバから権威ネームサーバ、どちらの区間も DoH による DNS キャッシュポイズニング防止とプライバシー保護が可能となる。
**キーワード** DNS, プライバシー，キャッシュポイズニング攻撃，DoH

# A consideration of DoH-exclusive DNS architecture

Satoru SUNAHARA† Yong JIN‡ and Katsuyoshi IIDA§

†Collaborative Education, Chitose Institute of Science and Technology 758-65 Bibi, Chitose, Hokkaido, 066-8655 Japan
‡Global Scientific Information and Computing Center, Tokyo Institute of Technology 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8550 Japan
§Information Initiative Center, Hokkaido University Kita 8 ,Nishi 5,Kita-ku, Sapporo, Hokkaido 060–0811 Japan

E-mail: †s-sunaha@photon.chitose.ac.jp, ‡yongj@gsic.titech.ac.jp , §iida@iic.hokudai.ac.jp

**Abstract** Conventional DNS communication uses non-encrypted UDP protocol so that DNS cache poisoning attacks and privacy leakage have become critical cyber threats nowadays. To protect private information from falsification and eavesdropping during DNS communication, the IETF has standardized DNS over HTTPS (DoH) protocol and some service providers have started DoH based domain name resolution service. However, the current DoH protocol only supports the DNS communication between client and DNS full-service resolver due to the conventional DNS architecture. Thus, the DNS communication between full-service resolver and DNS authoritative server is still unencrypted, and accordingly the risks of DNS cache poisoning attack and privacy leakage still exist. In this research, we propose a novel DNS authoritative server architecture using DoH(DoH-exclusive DNS architecture), which enhances DoH communication to between DNS full-service resolver and DNS authoritative server. Consequently, we expect to mitigate the risks of DNS cache poisoning attacks and privacy leakage during the whole name resolution process.
**Keywords** DNS, privacy, cache poisoning, and DoH.

## 1. はじめに

Domain Name System (DNS)はインターネットアクセスにおいて重要な基盤サービスであるが、現代においても、DNS フルサービスリゾルバ(キャッシュサーバ)へ偽の DNS 情報を送信し、クライアントからの接続を本来とは異なるサーバに通信させる DNS キャッシュポイズニングアタックや、DNS フルサービスリゾルバと権威ネームサーバ間の通信が盗聴され、クライアントのプライバシー情報が漏洩するといった脅威が存在する[1]。

これらの脅威を緩和するために、Domain Name System Security Extensions (DNSSEC)[2]や DNS over TLS(DoT)[3], DNS over HTTPS (DoH)[4]などが IETF によって標準化された。DNSSEC は主に DNS フルサービスリゾルバと権威ネームサーバ間において、DNS トラフィックのデータ完全性を確認することにより通信経

路でのデータ改竄や通信相手が正しいことを保証する。しかし、通信内容の暗号化はサポートしておらず、プライバシーは保護されていない。一方、改ざんや盗聴行為の脅威を緩和する手法として、DoT や DoH による通信経路の暗号化は一定の効果が見込まれており、Quad9 や Cloudflare, google public DNS などのサービスにおいて運用が始まっている。しかし、DoT や DoH による通信経路の暗号化はクライアント(スタブリゾルバ)から DNS フルサービスリゾルバ間が対象であり、DNS フルサービスリゾルバから権威ネームサーバ間の通信は、現在でも平文が用いられているため、盗聴や改ざんの脅威が存在している。DNS フルサービスリゾルバから権威ネームサーバ間の通信における DNS プライバシー保護を目的として Query Name Minimisation [5]が提案されている。しかし、Query Name Minimisation は最終的にユーザのプライバシー情報を平文で通信してしまうため、根本的な対策とはいえない。したがって、既存の DNS 構成においては、DNS フルサービスリゾルバと権威サーバ間の通信においてプライバシーが完全には保護されていない。そこで本研究では、DNS の通信経路を全て DoH で暗号化を行う「完全 DoH 化 DNS アーキテクチャ」を提案し、既存の DNS キャッシュポイズニングへの対策だけでなく課題となっているプライバシーの保護を実現する。

## 2. 関連研究

### 2.1. DNSSEC

DNSSEC は公開鍵暗号化方式を用いた電子署名を使用して DNS 応答の完全性を保障する仕組みである(図 1)。DNSSEC では、スタブリゾルバあるいは DNS フルサービスリゾルバと権威ネームサーバ間の DNS 通信におけるデータの完全性を保障するために電子署名を利用する。事前準備として、権威ネームサーバ上で鍵ペア(秘密鍵と公開鍵)と秘密鍵を利用した電子署名による DNS レコードのハッシュ値を用意する。権威サーバへ DNSSEC による名前解決のリクエストがあった場合は、DNS レコードとハッシュ値①を秘密鍵で電子署名した情報をクライアントに送信する。データを受け取ったクライアントは権威ネームサーバの公開鍵を用いて電子署名を元のハッシュ値①へ復号化する。また、受け取った DNS レコードのハッシュ値②を計算し、ハッシュ値①と一致するかを検証する。これらの通信は全て平文で行われるため、クライアントのプライバシー (クライアントがリクエストした FQDN) 情報は保護されない。

### 2.2. Query Name Minimisation

Query Name Minimisation は DNS の通信においてプライバシー情報(クライアントがリクエストした FQDN)の通信回数を最小限にし、漏洩リスクの低減を図る仕組みである。Query Name Minimisation による名

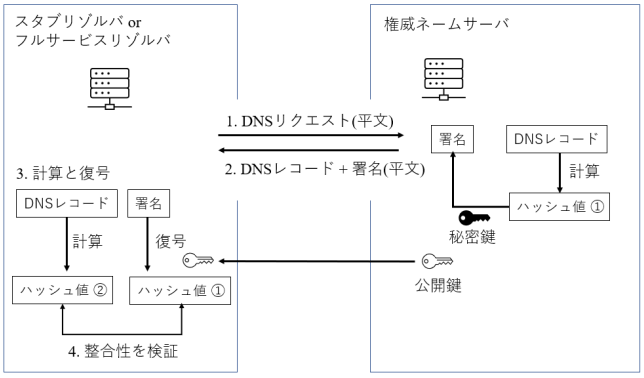


図 1 DNSSEC による応答の完全性を保障する仕組み

前解決の流れを図 2 に簡単に示す。従来の DNS プロトコルでは DNS フルサービスリゾルバから全ての権威ネームサーバに対し、プライバシー情報が含まれた状態で通信されていた。Query Name Minimisation では、プライバシー情報が必要になるまで、通信先の権威ネームサーバには送信しない。しかし最終的には平文でプライバシー情報を含めた通信が発生するため、根本的な解決には至っていない。

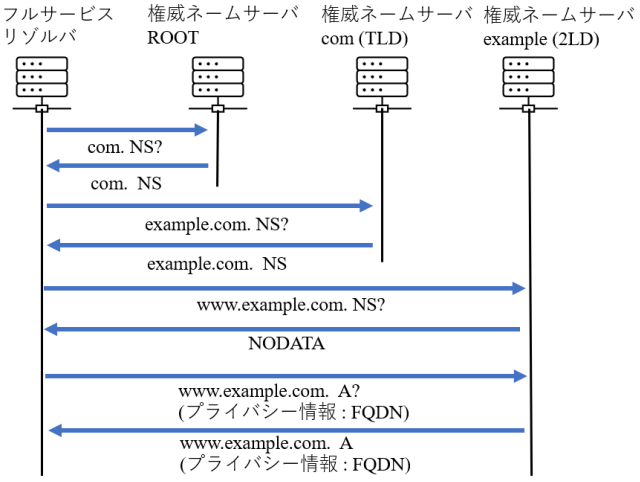


図 2 Query Name Minimisation の通信手順

### 2.3. DoT/DoH

DoT/DoH はプライバシーを保護するために DNS の通信を暗号化する仕組みである。DoT は TCP ポート 853 番が割り当てられており、DNS サーバが TLS 接続手続きを行うことで、通信経路上の暗号化、改ざん防止を行うことが可能である。DoH は TLS 接続の代わりに Web の通信で使用される HTTPS 接続を用いる手法であり、DoT と同程度のプライバシー保護が可能である。DoT/DoH は通信経路の途中でなりすましを行うような改ざんの防止は可能であるが、権威ネームサーバ自体をなりすますような攻撃があった場合は、通信内

容の完全性は保障されない。完全性を保証する場合には DNSSEC などの仕組みと組み合わせる必要がある。DoT/DoH によって暗号化が適用される区間はスタブリゾルバと DNS フルサービスリゾルバ間のみであり、DNS フルサービスリゾルバと権威ネームサーバ間には用いられていないことは課題である。

## 3. 完全 DoH 化 DNS アーキテクチャの提案

現在、世界中で実運用されている DNS サービスの通信における、プライバシー保護の状況を図 2 に示す。スタブリゾルバと DNS フルサービスリゾルバ間の通信はプライバシーの保護が実現できるようになってきているが、DNS フルサービスリゾルバと権威ネームサーバ間の通信はプライバシーが保護されていないという問題が存在する。2 章でも述べた通り、DNSSEC は DNS レコードの完全性を保証するだけであり、プライバシーの保護は行われない。この問題を解決するために、我々は DNS の通信経路を全て DoH で暗号化を行う「完全 DoH 化 DNS アーキテクチャ」を提案する。

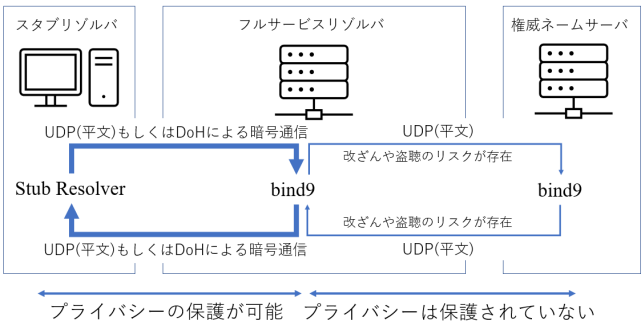


図 2 既存の DNS におけるプライバシーの課題

本研究にて提案する DNS の構成を図 3 に示す。DNS フルサービスリゾルバと権威ネームサーバ間の全ての通信にてプライバシーの保護を行うためには、全ての権威ネームサーバが暗号化をサポートする必要がある。既に主要な DNS サーバソフトウェアである bind9 および Unbound において DoH のサポートが行われるため、権威ネームサーバでは、この機能を有効化するだけでよい。DNS フルサービスリゾルバが各権威ネームサーバと DoH にて通信を行うことで通信経路におけるプライバシーの保護を実現できる。各通信規格と提案手法の完全性及びプライバシー保護の特徴は表 1 の通りである。

## 4. 研究課題

DNS フルサービスリゾルバと権威ネームサーバ間の通信を DoH で暗号化することによって通信経路のプライバシー保護や改ざんを防ぐ効果を期待できる。しかし、権威ネームサーバにおける DoH サービスを実現するためにはいくつかの懸案事項が存在する。

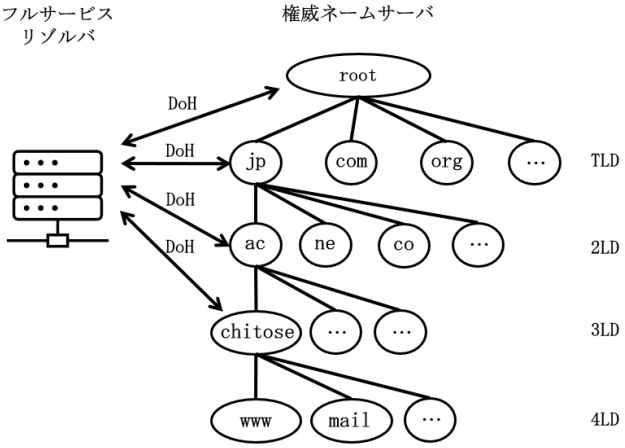


図 3 提案する DNS のアーキテクチャ構成

表 1 各手法の完全性とプライバシー保護の比較

| 手法 | 完全性の保証 | プライバシー保護 | 保護の範囲 |
|---|---|---|---|
| DNSSEC [2] | 保証する | 保護しない | クライアント～権威ネームサーバ |
| DoT [3], DoH [4] | 通信経路のみ保証 | 保護する | クライアント～フルサービスリゾルバ |
| Query Name Minimisation[5] | 保証しない | 通信回数を最小化する | フルサービスリゾルバ～権威ネームサーバ |
| 提案手法 | 通信経路のみ保証 | 保護する | フルサービスリゾルバ～権威ネームサーバ |

### 4.1. 権威ネームサーバへの HTTPS リクエスト

提案手法では、DNS フルサービスリゾルバは名前解決の過程において全ての権威ネームサーバに対して、HTTPS 通信を行う必要がある。この機能は DNS フルサービスリゾルバの DNS ソフトウェア上で実装されていることが望ましいが、現在は実装されていない。したがって、検証を行う場合には UDP のリクエストを HTTPS 通信可能な変換を行う proxy の開発が必要となる。proxy を用いた変換の流れを図 4 に示す。①プライバシー情報を含む通信はスタブリゾルバから DNS フルサービスリゾルバの DNS へ UDP 或いは DoH で送信される。②DNS フルサービスリゾルバの DNS がリクエストに対応する DNS レコードをキャッシュしていない場合は各権威ネームサーバへ UDP のリクエストを送信する。その UDP リクエストをホスト上の proxy で HTTPS に変換し、権威ネームサーバに対してリクエストを行う。③権威ネームサーバの応答を HTTPS で proxy が受け取る④HTTPS の応答を UDP に変換する。⑤スタブリゾルバは DNS フルサービスリゾルバからの応答を UDP 或いは DoH で受け取り、名前解決が完了する。

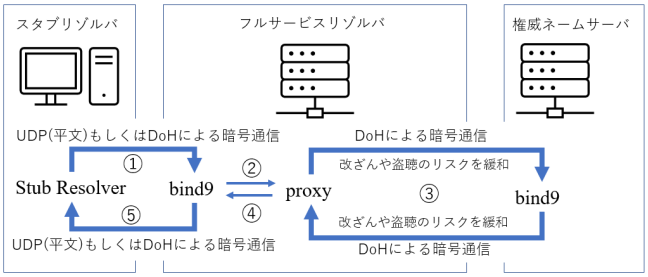


図 4 HTTPS 変換 proxy を用いた通信手順

### 4.2. 機材の負荷や性能への影響

UDP 通信と比較すると DoH 通信はパケットサイズや送受信が増えるため、通信量が増加する。名前解決における UDP 通信と DoH 通信の送受信の比較を図 5 に示す。UDP では 1 往復で完了するが、DoH では TCP 3way handshake や TSL handshake などのオーバヘッドが発生する。また、クライアントと DNS フルサービスリゾルバは 1:1 の通信であることに対し、DNS フルサービスリゾルバと権威ネームサーバの通信は 1:N であるため、通信量や遅延が N 倍以上になる可能性がある。実用化を考えた場合、無線機器や海底ケーブルなどの帯域が DNS のトラフィックで圧迫されないか、応答速度が実用に耐えられるかなど、通信のパフォーマンスを十分に調査し、負荷分散やスケーラビリティについて慎重に検討を行う必要がある。

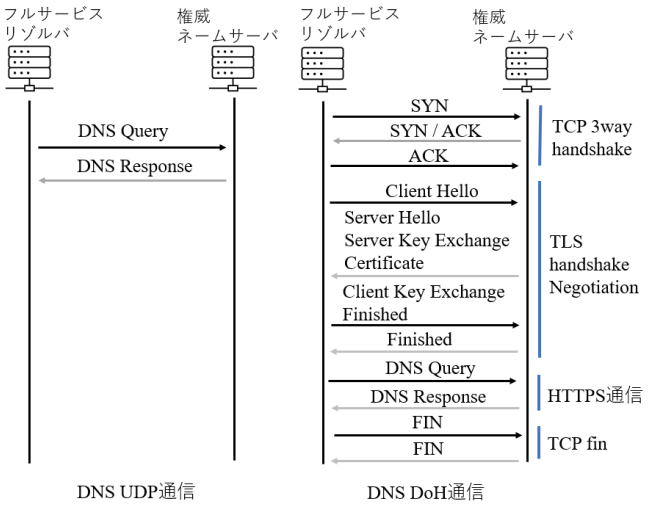


図 5 UDP と DoH の送受信手順の比較

### 4.3. Denial of Services (DoS)攻撃に対する対策

DNS に限らず、Web システムにはサービスの継続を妨害するような DoS 攻撃の脅威が存在する。提案手法では、全ての権威ネームサーバ上で DoH を有効化するため、新たな対策などを必要する可能性がある。DoS 攻撃に対するセキュリティ対策を行う際に、DNS の管理者にどの程度の負担が発生するか考える必要がある。

### 4.4. 既存のセキュリティシステムを回避される問題

スタブリゾルバと DNS フルサービスリゾルバ間の通信に DoH を通信に用いることによって、ISP による DNS ブロッキングや企業・組織のポリシーを回避することができる可能性がある[6]。DNS フルサービスリゾルバと権威ネームサーバ間の通信に DoH を用いることによって既存のセキュリティに与える影響を考慮する必要がある。

## 5. 研究計画

前節で述べた課題を検証するためのデータは実運用している権威ネームサーバから取得できることが望ましい。しかし、提案手法は root を含む全ての権威ネームサーバで DoH を有効にする必要があるため、実現が難しい。そこで本研究では root サーバを含め、いくつかの権威サーバを疑似的に作成し、仮想環境上のデータで分析を行う。権威ネームサーバを実世界と同数用意することも難しいため、ゾーン数や問い合わせの数、種類を増やしながらモデルの構築を試みる。

## 6. おわりに

現在の DNS アーキテクチャでは、DNS フルサービスリゾルバと権威ネームサーバ間において、クライアントのプライバシー情報が保護されていない。我々は、この問題を解決するために、DNS の通信経路を全て DoH で暗号化を行う「完全 DoH 化 DNS アーキテクチャ」の提案を行い、取り組むべき課題について紹介した。今後は計画に基づいて検証を進める予定である。


### 謝辞

本研究の一部は、JSPS 科研費 19K20254 の助成を受けたものです。


### 文　献


[1] C. Deccio and J. Davis, “DNS privacy in practice and preparation,” *Proc. IEEE Int. Conf. emerging Networking EXperiments and Technologies (CoNEXT2019)*, Dec. 2019, pp. 138–143.

[2] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, “DNS Security Introduction and Requirements.” *IETF RFC 4033*, Mar. 2005.

[3] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels and P. Hoffma,. “Specification for DNS over Transport Layer Security (TLS),” *IETF RFC 7858*, May 2016.

[4] P. Hoffman, P. McManus, “DNS Queries over HTTPS (DoH),” *IETF RFC 8484*, Oct. 2018.

[5] S. Bortzmeyer, R. Dolmans and P. Hoffman, “DNS Query Name Minimisation to Improve Privacy.” *IETF RFC 9156*, Nov 2021.

[6] L. Csikor, H. Singh, M. S. Kang, and D. M. Divakaran, “Privacy of DNS-over-HTTPS: Requiem for a Dream?” *Proc. IEEE European Symp. Security & Privacy (EuroS&P2021)*, Sep. 2021, pp. 252–271.