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
IA2022-67(2022-12)

［ショートペーパー］IPヘッダ情報からのプライバシー漏洩を防ぐDoHに基づく新たな名前解決機構

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 の通信においてプライバシー情報の保護の重要性が高まっている．現在標準化されている DNS over TLS (DoT) や DNS over HTTPS (DoH) の規格では，DNS の通信を暗号化することによって改ざんや直接漏洩を防ぐことは可能であるが，DNS の通信を暗号化したとしても通信ヘッダの送信元 IP アドレスと送信先 IP アドレスまで隠蔽することはできない．そのため，たとえ DNS の通信が暗号化されていたとしても，送信元のクライアントがどのようなサイトに興味を持っているのかを推測できる可能性がある．本研究では，クライアントから権威 DNS サーバ間の DNS 通信の匿名性を維持し，照会されたドメイン名の推測リスクを軽減させるための手法の提案と手法の検証結果について紹介する．

キーワード　DNS，プライバシー保護，プライバシー漏洩，DoH，IP ヘッダ

[Short Paper] A consideration of DoH-based name resolution architecture for Preventing Privady Leakage from IP Header

Satoru SUNAHARA†, Yong JIN††, and Katsuyoshi IIDA†††

† Chitose Institute of Science and Technology　758–65 Bibi, Chitose, Hokkaido, 066–8655 Japan
†† Tokyo Institute of Technology　2–12–1 Ookayama, Meguro-ku, Tokyo , 152–8550 Japan
††† 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　Privacy preservation on DNS-based name resolution has become one of the important issues in the Internet. DNS over TLS (DoT) and DNS over HTTPS (DoH) which have been standardized by the IETF, can prevent falsification of the DNS traffic and direct leakage in the communication link. However, the DNS traffic encryption cannot hide the source and destination IP addresses from which the queried domain name can be speculated. Therefore, in this paper, we propose a novel DoH-based name resolution architecture to prevent the risk of domain name speculation from the IP header of DNS packet. According to preliminary evaluations, we confirmed that the DNS traffic between end clients and DNS authoritative servers can keep the anonymity and the risk of queried domain name speculation can be significantly mitigated.

Key words　DNS, privacy protection, privacy leak, DoH, IP header

1. はじめに

近年，インターネットの基盤システムである Domain Name System (DNS) の通信においてプライバシーを保護することが重要な課題となっている [1]．従来の DNS 通信では DNS クエリが暗号化されていなかったため，通信経路の途中で「送信元の IP アドレス」と「DNS クエリ」を組み合わせることで，「誰がどのようなサイトにアクセスしようとしているか，興味を持っているか」というプライバシー情報の収集が技術的に可能であった．プライバシー情報の保護を実現するために，DNS 通信の暗号化を行う DNS over TLS (DoT) [2], DNS over HTTPS (DoH) [3] やプライバシー情報を含む DNS クエリの通信頻度を最小化する Query Name Minimization [4] が IETF によって標準化されている．しかしながら，これらの規格によって通信パ

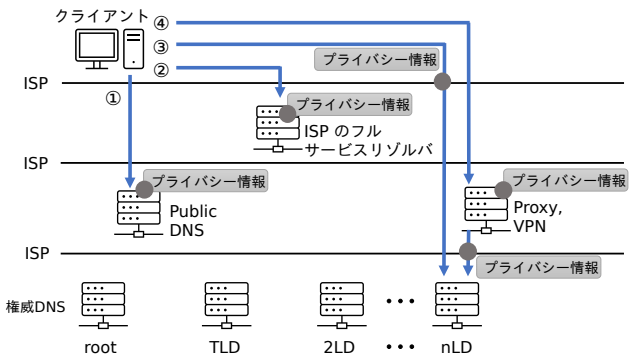

図 1　名前解決の経路上においてプライバシー情報の傍受が可能な例

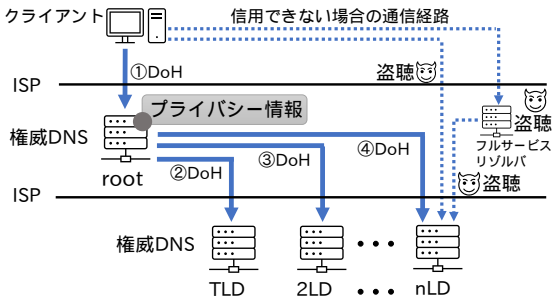

図 2　提案手法の構成

ケットのヘッダまでは暗号化を行うことが実現できていない．パケットのヘッダ情報である「宛先 IP アドレス」から，問い合わせ先の権威 DNS サーバが管理するドメインの情報を推測することが可能であるため，通信経路の途中でクライアントのプライバシー情報が漏洩する可能性がある．具体的な例を図 1 の①〜④に示す．例えば，①クライアントが Public DNS を使用して名前解決を行うと Public DNS の管理者はプライバシー情報を傍受することが可能である．また，②クライアントが ISP のフルサービスリゾルバを使用して名前解決を行う場合も ISP の管理者はプライバシー情報を傍受することが可能である．③外部のフルサービスリゾルバを使用せず，クライアント自身がフルサービスリゾルバを運用する場合においても，ISP の管理者はプライバシー情報を傍受することが可能である．④ ISP の管理者に傍受されないために Proxy や VPN を使う方法も考えられるが，その場合は Proxy や VPN サービスの管理者がプライバシー情報を傍受することが可能である．

2. 提 案 手 法

DNS の通信を暗号化したとしても，ユーザと権威 DNS サーバまでの通信経路において，通信の宛先アドレスからユーザがどのようなドメインやゾーンの情報を参照しようとしているかを傍受および不正利用される可能性がある．通信経路やフルサービスリゾルバは信頼できないが，各権威サーバは信頼ができるという条件において，ユーザのプライバシー情報を保護する手法の構成を図 2 に示す．まず，①クライアントは root 権威サーバへ DoH による暗号通信で名前解決のリクエストを送信する．リクエストを受け取った root 権威サーバは ② TLD, ③ 2LD ･･･④ nLD まで再帰的に名前解決を繰り返し，結果をクライアントに直接返信する．これにより，root 権威 DNS サーバ以外はプライバシー情報を参照できず，通信経路での傍受を防止することが可能となる．なお，root 権威 DNS サーバから各権威サーバの通信ヘッダ情報にはクライアントの送信元アドレスは含まれていないが，通信クエリの情報を通信経路で傍受されることによりクライアントが特定される可能性があるため，通信経路は全て暗号化されていることが望ましい．

3. プロトタイプの実装と機能確認

実証検証のプロトタイプ環境は 1 台の linux サーバと Kernel-based Virtual Machine (KVM) を用いて構築した．検証に用いた VM はクライアント，root 権威 DNS サーバ，TLD 権威 DNS サーバ，2LD 権威 DNS サーバの 4 台である．DNS サーバソフトウェアには ISC bind9 (bind9) を用いた．root サーバから各権威サーバへの問い合わせを行う方法としては，bind9 の再帰問い合わせの設定 (recursion) を有効化するだけでよい．ただし，この設定で運用を開始した場合，Distributed Denial of Service attack (DDoS 攻撃) として不正に利用されてしまう可能性があるため，レートリミットなどの設定を用いた対策も必要となる．また，今回の実証検証には root 権威 DNS サーバから各権威サーバへ DoH で問い合わせする機能が必要である．しかし，現時点では bind9 に DoH で問い合わせを行う機能が実装されていない．そのため，今回の検証では bind9 が出力する UDP のリクエストを DoH に変換する DoH-proxy を用意した．

検証の結果，提案手法においてはクライアントと権威 DNS サーバ間の通信経路からは nLD 向けの通信である情報をパケットヘッダから取得することはできず，また，名前解決の全ての通信においてクエリ情報が暗号化され，クライアントのプライバシー情報が保護されていることが確認できた．通信コストの測定と実用化に向けた検証は今後の課題である．また，今回の実証実験では，root 権威 DNS サーバが再帰問合せを行うように設計したが，今後は各 TLD 権威 DNS サーバまで再帰問合せを行う方法も検討する．

4. 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] A. Khormali, J. Park, H. Alasmary, A. Anwar, M. Saad, D. Mohaisen, “Domain name system security and privacy : A contemporary survey,” *Computer Networks*, vol. 185, 107699, Dec. 2020.

[2] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. Hoffman, “Specification for DNS over transport layer security (TLS),” *IETF RFC7858*, May. 2016.

[3] P. Hoffman, and P. McManus, “DNS queries over HTTPS (DoH),” *IETF RFC8484*, Oct. 2018.

[4] S. Bortzmeyer, “DNS query name minimisation to improve privacy,” *IETF RFC7816*, Mar. 2016.