学位論文審査の要旨

博士の専攻分野の名称　博士 (情報科学)　氏名　砂原 悟

審査担当者　主　査　教　授　飯田 勝吉
副　査　特任教授　髙井 昌彰
副　査　教　授　南 弘征

学位論文題名

A Study on DNS Architecture Realizing Institutional Privacy Preservation
（機関プライバシーを実現する DNS アーキテクチャに関する研究）

近年、インターネットは社会基盤として不可欠な存在となっているが、その基盤技術の一つである Domain Name System(DNS) は、設計当初に通信の機密性が十分考慮されていなかった。現在では DNS over TLS(DoT) や DNS over HTTPS(DoH)、DNS over QUIC(DoQ) といった暗号化 DNS プロトコルにより、利用者端末と DNS フルサービスリゾルバ間の通信は保護されつつある。しかし、フルサービスリゾルバと権威 DNS サーバ間の通信は依然として平文であり、組織単位の通信傾向が外部から推測可能な状態にある。大学や企業などの組織において、DNS 問い合わせは内部活動や関心を反映するため、その漏洩は社会的信用や戦略的機密性に重大な影響を及ぼす。このような背景から、DNS 通信全体を対象とした包括的なプライバシー保護が求められている。

既存研究である RFC 9539 では、DNS 通信における機関のプライバシー保護についての方向性が検討されているものの、(1) プライバシー保護を優先したいユーザの意思が DNS フルサービスリゾルバに十分反映されないこと、(2) 既存の DNS 運用との互換性維持が平文通信に依存しており、プライバシー情報が漏洩するという 2 つの課題が存在する。本研究では、最初に課題 (1) に取り組み、次にその取り組みを拡張することで課題 (2) を解決している。

課題 (1) の問題は、DNS 利用者が自身の属する機関のプライバシーを保護したいと考えていたとしても、その意図はフルサービスリゾルバから権威 DNS サーバへの問い合わせ過程には伝達されず、結果としてフルサービスリゾルバと権威 DNS サーバ間の通信に平文が使用され、機関のプライバシーが漏洩してしまうことである。このような構造では機関全体の問い合わせ傾向が外部から観測可能となり、通信経路に攻撃者は活動内容や関心の推測が可能である。

課題 (2) の問題は、フルサービスリゾルバと権威 DNS サーバ間における暗号化通信と平文通信の相互運用性の確保が困難な点である。DNS は長年にわたり平文通信を前提として運用されてきたため、暗号化通信を一律に導入すると、暗号化に未対応の権威 DNS サーバとの通信に支障をきたすことが想定される。一方で、互換性を優先して平文通信を許容すると、機関のプライバシー保護が不完全なものとなる。

本研究では課題 (1) に対し、DoH のリクエストパスによる挙動の拡張を許容している点に着目している。具体的には、フルサービスリゾルバに「プライバシー保護の優先」と「互換性の優先」という 2 つのリクエストパスを用意し、ユーザ側でこれを選択できるようにする。完全暗号化パスを選択した場合、暗号化通信に失敗しても平文には戻らず名前解決を失敗させることで、意図しない情報漏洩を防止する。また、DoH のパス自体が TLS で保護されるため、ユーザの選択 (意思) その

ものが第三者に傍受されるリスクも排除している。実装による評価の結果、ドメイン 1 階層あたりの名前解決時間は 0.27 秒程度であり、証明書検証による負荷はあるものの、実用上の許容範囲内であると論じている。

次に、課題 (2) に取り組むため、親権威サーバが子権威サーバへ委任を行う際の NS レコード自体に「dh-e-(DoH 有効)」などの特定の文字列を接頭辞として付与する手法を提案している。これにより、フルサービスリゾルバはルートヒントファイルや上位サーバからの応答を確認するだけで、初回接続時から平文を一切介さずに暗号化通信を開始することが可能になる。検証環境における評価により、提案手法は SVCB レコードを別途解決する手順を省けるため、RFC 9461 よりも低遅延で効率的な名前解決を実現できることが確認された。このように、DNS の基本的な委任構造を拡張して暗号化情報を共有することで、既存インフラとの互換性を保ちつつ、完全なプライバシー保護と高いパフォーマンスを両立できることを明らかにしている。

これを要するに、著者は、DNS 通信の完全暗号化と委任構造を拡張した効率的な情報共有手法を確立しており、既存インフラとの互換性を維持しつつ、プライバシー保護と通信パフォーマンスを高度に両立させた点は、インターネットのプライバシー保護ならびに次世代セキュアネットワーク基盤の発展に資するものである。よって、著者は北海道大学博士 (情報科学) の学位を授与される資格があるものと認める。