結託耐性を有した匿名 DNS「μODNS」の開発

～インターネット基盤のプライバシ保護技術～

大学院 情報科学研究科

○准教授　栗原（くりはら） 淳（じゅん）

キーワード　**Domain Name System (DNS), 匿名化, インターネット基盤, インターネットプライバシ**

研究概要

Web ブラウザなどを介したインターネットへのアクセスは、ドメイン名(例: www.u-hyogo.ac.jp)と、インターネット上のサーバ所在地を表す IP アドレス(例: 150.12.2.20)とを紐づける、Domain Name System (DNS) という基盤システムによって支えられている。DNS はインターネットサービスプロバイダや Google らの巨大企業によって提供されることが多く、それらの会社に**ユーザのオンライン行動、即ちプライバシ情報が収集されてしまう**という課題がある(図 1)。特に欧米において、エドワードスノーデンの暴露事件以降、この課題は早急に解決すべきものと注目されている。本研究では、この課題を解決すべく**DNS 匿名化方式「Mutualized Oblivious DNS (μODNS)」を提案・開発し、インターネット上で実装・運用**を行っている(図 2)。μODNS では、複数の「リレー」と呼ばれる中間ノードを準備し、ユーザはそれらをランダムに経由して DNS サーバと通信する。これにより**DNS サーバに対して誰のアクセスかを秘匿したやりとりが可能**になり、プライバシが担保される。加えて、たとえいくつかの**リレーが DNS サーバと結託してユーザプライバシを暴こうとしても、それが不可能となる機構を導入**している。

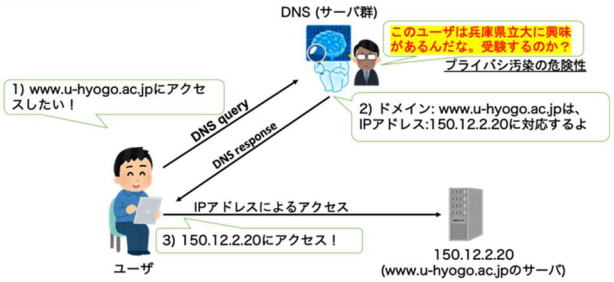

図1: DNSを介したインターネットアクセスとプライバシ問題

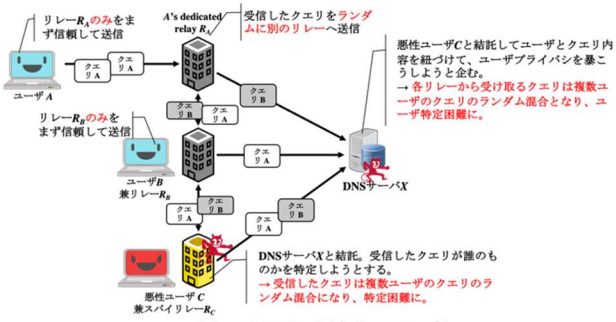

図2: μODNSの匿名化コンセプト

アピールポイント

本研究のトピックである「匿名 DNS」は、米国を中心に 2020 年より研究や標準化が始まったばかりであり、次世代インターネットの重要な技術と認識されている。知る限り、この分野の国内の研究者はまだ筆者以外にはいない。μODNS は、オープンソースプロジェクトとして GitHub 上で開発を進めている。またその概念実装 (Proof-of-Concept) および社会実装として、インターネット上で実験的サービスの運用を行い、その知見を貯めている。

・開発プロジェクト:https://github.com/junkurihara/dnscrypt-proxy-modns
https://github.com/junkurihara/encrypted-dns-server-modns

・実験サービス情報: https://github.com/junkurihara/experimental-resolvers

・発表論文 (コンセプト論文): J. Kurihara and T. Kubo, “Mutualized oblivious DNS (μODNS): Hiding a tree in the wild forest”, 2021.04. https://arxiv.org/abs/2104.13785