学 位 論 文 内 容 の 要 旨

博士の専攻分野の名称　博士（情報科学）　氏名　砂原 悟

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）

This study aims to realize comprehensive privacy protection in DNS communications, which are indispensable to modern Internet infrastructure, with a particular focus on realizing institutional privacy as its ultimate goal. Traditional DNS operates using plaintext communication. Consequently, if an attacker is present on the communication path between an end terminal and a full-service resolver, there is a risk that ”end-user privacy” may be compromised, including information such as which users performed name resolution queries, when those queries were issued, and the specific domain names involved. To protect end-user privacy, encrypted DNS communication protocols such as DNS over TLS, DNS over HTTPS, and DNS over QUIC have been standardized. DNS communication from a full-service resolver to authoritative DNS servers was traditionally considered to pose no privacy concerns, since the source IP address corresponds to the full-service resolver rather than the end user. However, DNS traffic generated by full-service resolvers operated by organizations contains information about Institutional activities, which constitutes ”Institutional privacy.” If sensitive categories of information (such as religion, political, harassment, discrimination activities, etc.) are leaked from DNS communication, the institution may be exposed to loss of confidence threats.

To address challenges, this study proposes two novel and integrated mechanisms to realize full-path DNS encryption. First, by leveraging the extensibility of DoH request paths, such as paths indicating dns-full-encryption or dns-udp-compatibility, we establish a mechanism that allows end users’ privacy preferences to be reflected in resolver operational behavior. This enables user-intent-based control over resolver actions, including whether fallback to plaintext communication is permitted when encrypted communication is unavailable. Second, we introduce a method of embedding, as a prefix, information about the encrypted pro-

tocols supported by child authoritative DNS servers into delegation NS records. With this approach, resolvers can directly obtain protocol information from root hint files or delegation NS records, thereby initiating encrypted communication securely and efficiently without relying on plaintext SVCB record queries as in RFC 9461 or redundant plaintext exchanges as in RFC 9539.

The effectiveness and practical performance of the proposed architecture were validated through the implementation of a prototype system and comparative performance evaluations against existing standards. In particular, the proposed method enables encrypted protocol discovery while completely avoiding privacy leakage due to plaintext traffic. Compared with RFC 9461, it demonstrates superior and more stable performance characteristics in terms of name resolution latency, average response time, and queries per second (QPS). Furthermore, we identify server certificate verification at the resolver as the primary source of performance overhead, providing a clear direction for future optimization.

Overall, this study overcomes the limitations of conventional DNS encryption approaches in both privacy and performance, and realizes institutional privacy protection across the entire DNS resolution path.