≪「**報告書詳細版**」は巻末の付録USBメモリに収録しています≫

第22部

DNS extension and operation environment（概要版）

石原 知洋、関谷 勇司

第１章　はじめに

DNS WGでは、DNSにおける実装上や運用上の問題点に関して、情報共有とそれを解決するための活動を行っている。秋のWIDE研究会においてミーティングを開催し、DNSに関するホットトピックについて情報交換を行った。本報告書では、これらのミーティングにおいて発表、議論がなされた事項についてまとめる。

第２章　2019年WIDE春合宿での議論まとめ

2019年9月のWIDE秋合宿において、DNS WGのミーティングを開催した。このミーティングでは、下記の事項について発表と議論が行われた。

2.1　UDP第一フラグメント便乗攻撃の概要と対策案

JPRSの藤原氏より、UDP第一フラグメント便乗攻撃の概要と対策について発表があった。UDP第一フラグメント便乗攻撃は、UDP通信において発生するフラグメントを悪用しDNSのキャッシュ汚染攻撃をおこなうものである。

本発表ではこちらの対策として、UDP payloadのサイズを1220に限定させることにより、IPv6の最低MTUである1280を上回らないようにしてフラグメントを抑制しつつ、フラグメントしたパケットを破棄する、などのいくつかの対抗策が提案された。

第３章　2019年WIDE秋合宿での議論まとめ

2019年9月のWIDE秋合宿において、DNS WGのミーティングを開催した。このミーティングでは、以下の事項に関して発表と議論が行われた。

3.1　フラグメント回避のためのDNSおよびRFC8085でのUDP利用ガイドライン

JPRSの藤原氏より、春合宿で発表があったUDP第一フラグメント便乗攻撃の対策について発表があった。現在、RFC8085ではUDPフラグメンテーションの悪用を防ぐため、UDPのペイロードサイズ選択について規定されている。しかし、RFC8085はUDP全般について書かれた仕様であり、DNSについては一例として触れられているのみである。したがって、DNSの挙動についてRFC8085に従って更新すべきである、との提案があった。

本提案はdraft-fujiwara-dnsop-avoid-fragmentationとしてIETFのdnsopで標準化に向けて議論がおこなわれている。

3.2　DITLデータを用いたルートサーバへ問い合わせを送るホストの解析

JPRSの藤原氏より、ルートネームサーバ上で取得されたトラフィックデータを用いた、ルートネームサーバに対してDNSクエリを送信するDNSホストの、実装および設定などの推定について、発表があった。

解析にり得られた、いくつかの攻撃に見えるトラフィックや、問題が発生しているとみられるDNSサーバホストについて、誤設定や実装の問題などの動作推定について紹介があった。

3.3　DNSのIPv6対応とIPv6の普及状況

JPRSの藤原氏より、DNSにおけるIPv6の普及状況について、JPのゾーンファイルと、Alexaから公開されている人気ドメイン上位の名前に実際に名前解決を実施し得られ

た返答を解析した結果について発表があった。

IPv6トランスポートでの問い合わは全体の14%、およびAAAAレコードの問い合わせは20%と年々増加傾向にある。また、登録レコードベースでも増加がみられるが、JPに登録されているIPv6レコード数よりもAlexaの人気ドメインに見られるような世界的なサイトの方がより多くIPv6対応がされているという現状が説明された。