第20部

DNS extension and operation environment

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。2015年は、広域でのルートネームサーバ実験・実証環境であるyetiプロジェクトの実施をおこなった。また、春と秋の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　2017年WIDE春合宿での議論まとめ

2017年3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。

- Status of DNS terminology-bis (日本レジストリサービス　藤原)
- How to retrieve domain name list to research (日本レジストリサービス　藤原)
- Yeti DNS update (慶應義塾大学　加藤)

2.1　Status of DNS terminology-bis (日本レジストリサービス　藤原)

日本レジストリサービスの藤原氏より、IETFで議論中のドラフト、draft-ietf-dnsop-terminology-bis-04について報告があった。本インターネットドラフトはDNSの用語について説明するRFC7719を修正するものである。RFC7719はDNSプロトコルの説明で表記ゆれがあった用語の明確化などがおこなわれていた。本ドラフトでは、RFC7719に対して用語の追加や、定義の変更が提案されている。大きな変更点はドメイン名の定義に関するものであり、DNSのRFCではドメイン名は255文字以下、ラベルは63文字以下と定義されていたが、それらの文字数制限を定義から外している。また、ドメイン名について、DNSで使われるもの、という定義を外し、DNS以外でもドメイン名が使われることを想定したものに変更している。また、新たにグローバルDNS、プライベートDNSというものを定義し、グローバルDNSを従来のDNSにより使われる名前空間、プライベートDNSがドメイン名構造を利用した独自の名前空間として規定した。これらの規定は、Torで利用される .onionや、Active Directoryで利用される .localなどの独自の名前空間を想定したものである。

2.2　How to retrieve domain name list to research (日本レジストリサービス　藤原)

日本レジストリサービスの藤原氏より、研究で利用できるドメイン名リストの取得方法について説明があった。ドメイン名リストは、特定のゾーンにある名前の列挙や、悪性ドメイン名のリスト、アクセス数が多いドメインのリストなど異なる性質の物があり、用途により様々な種類のものが必要となる。RootやTLDなどのドメイン名リストは、学術的用途であれば取得できる場合が多い。また、サービスとして名前を収集している組織・団体があり、それらについても自由に、ないしは契約によりドメイン名リストを取得できる。

2.3　Yeti DNS update (慶應義塾大学　加藤)

慶應義塾大学の加藤氏より、Yeti DNSプロジェクトのアップデートについて説明があった。Yeti DNSプロジェクトは、実際のルートゾーンと同じレコードを持つネームサーバを世界規模で実験運用することで、ルートゾー

ンの運用にかかる様々な知見を得ることが目的である。

今回の発表では、MTUにより発生する問題について報告があった。DNSSECを有効化すると、MTUが1500を超えてしまう場合があるが、特にIPv4の場合には中間機器がフラグメンテーションを正しく処理しないものがあり、問題が発生する場合が見受けられる。EDNS0をサポートしていれば適切なサイズで送信することも可能だが、DNSの実装によってはサポートしておらず、そのような機器を使用した際にはDNSのパケットサイズによっては名前解決が適切にできない場合があることが報告された。

第３章　2016年WIDE秋合宿での議論まとめ

2016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。

- Root KSK Key Rollover (日本レジストリサービス　米谷)
- Webを用いたDNSSEC対応チェック (東京大学　石原)

3.1　KSK Key Rollover (日本レジストリサービス　米谷)

日本レジストリサービスの米谷氏より、Root KSK Key Rolloverの説明と、その影響について報告があった。Root KSK Key Rolloverとは、Rootゾーンで利用されているDNSSECの鍵であるKSKを変更するものであり、すべてのDNSSECバリデータが鍵の変更に追従することが期待されている。本変更による影響としては、バリデータがKSKの変更に対応できず名前が解決できなくなる可能性や、鍵変更プロトコルの仕様上、変更期間は古い鍵と新しい鍵を併せて配るため、パケットサイズが大きくなりMTUを超えることで、途中経路によっては正しく通信ができなくなる可能性が挙げられる。本件については日本レジストリサービスに多くの問い合わせがあったが、問い合わせを行う人の知識レベルがまちまちで苦労をした。今回のような影響範囲が大きいDNSに関する周知をどのようにするかは今後の大きな課題である。

3.2　Webを用いたDNSSEC対応チェック (東京大学　石原)

東京大学の石原より、Webサイトを用いたDNSSEC対応チェック機構について説明と、実験参加者の募集があった。本機構はイメージタグでDNSSECバリデーションに失敗するドメイン名をURLとして埋め込み、さらに読み込み失敗時に別のURLを読み込むように属性を設定することで、いずれのURLにアクセスをしたかでDNSSECのバリデーションをしているかどうかを判断する仕組みである。本システムはWebサイトの一部に埋め込めば動作するため、Webサイトへの配置を協力してくれる参加者の募集をおこなった。また、広告などの有料のサービスを利用して、このような埋め込みHTMLを多く閲覧される場所に配置する方法について議論があった。