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。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　2018年WIDE秋合宿での議論まとめ

2018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。

- IETF102 DNS関連BOFまとめ（東京大学 石原）
- draft-ietf-dnsop-terminology-bis-13の報告（日本レジストリサービス 藤原）
- 複数リソースレコードによるDNS応答への実装の対応状況について（日本レジストリサービス 藤原）

2.1　IETF102 DNS関連BOFまとめ

東京大学の石原より、IETF102におけるDNSに関連したワーキンググループその他での議論について、報告があった。現在、IETFでは主にDNSのプライバシーについての議論が活発におこなわれており、特に最近RFC化されたDNS通信の暗号化手法であるDNS over HTTPSの運用に関する議論がホットトピックとなっている。

DNS over HTTPSを使用するにあたりどのリゾルバを利用するかについては、DNS over HTTPSのコアプロトコル仕様ではスコープ外となっており、その部分について運用方法および（自動ないし手動の）設定方法についてワーキンググループおよびワーキンググループ外のミーティング等でさまざまな提案がおこなわれている。

その他のトピックとしては、DNSSECで使用する鍵プロトコルの更新、DNS Cookieの運用における影響などが議論された。

2.2　draft-ietf-dnsop-terminology-bis-13の報告（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-13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2015年に発表されたRFCであり、DNSプロトコルの説明において、表記ゆれがあった用語の明確化などがおこなわれた。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。本ドラフトはinformationalとして標準化に向けてIETFで継続的に議論が行われている。ドラフトは8月にIETF Last Callがおこなわれ、現在はRFC化に向けてRFC Editorの作業待ちの状態である。

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。また、ゾーン委譲の種類についても

ゾーン内名前による委譲、ゾーン外名前による委譲などについて分類して定義をおこなっている。

2.3 Evaluation and consideration of multiple responses（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、RFC8198などの、いくつか提案されている複数のリソースレコードによるDNS応答を返す方式の、現在での権威サーバおよびフルサービスリゾルバでの実装・対応状況の評価について、発表があった。

評価は権威サーバについては単純に複数リソースレコードによる応答が返ってくるクエリを送り、複数のリソースレコードによる応答が戻ってくるかを調べる。フルサービスリゾルバについては、フルサービスリゾルバに対して、一回目の問い合わせで複数リソースレコードによる応答が帰ってくる形のクエリを送り、間をおいて二回目の問い合わせで複数リソースレコードに含まれているレコードのクエリを送る。その時の問い合せにかかった時間を計測し、早い時間で戻ってくれば一回目の問い合わせに含まれていたレコードをキャッシュしていた、すなわち複数リソースレコードによる応答に対応していると推測する。

調査の結果、BIND9およびGoogle Public DNSは複数リソースレコードによる応答に対応しておらず、UnbountおよびKnot ResolverはNSECレコードが追加されていた場合のみ受け付けた。PowerDNS RecursorはAdditional Sectionの追加リソースレコードは受け付けず、Answer Sectionに追加されたA/AAAAリソースレコードについては受け付けた。多くのフルサービスリゾルバ実装が追加リソースレコードを受け付けないのは、キャッシュ汚染攻撃による影響を防ぐためと推測される。