第26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　2015年WIDE春合宿での議論まとめ

2015年3月WIDE春合宿では、Farsight Security社のPaul Vixie博士とBeijing Internet Institute社のDavey Song博士を招き、DNS Workshopを開催した。本Workshopにおいて両氏より大規模な実験用ルートネームサーバテストベッドの提案が行われ、Workshop内での議論の成果として、Yetiプロジェクトの立ち上げが行われた。Yetiプロジェクトの詳細な説明については、「第５部 特集5 YETI - A Live Root-DNSTestbed」を参照のこと。

第３章　2015年WIDE秋合宿での議論まとめ

2015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。

- ランダムサブドメイン攻撃への対抗策 (JPRS藤原)
- IETF93報告 (JPRS 藤原)

主としてIETFのdnsopワーキンググループにおいてのDNS標準化活動の報告と、それらについて議論がおこなわれた。

3.1　ランダムサブドメイン攻撃への対抗策 (JPRS藤原)

JPRSの藤原氏より、最近増加しているランダムな文字列をラベルとして付加したクエリに対する対抗策の提案と、当該提案のIETFにおける標準化活動について報告がおこなわれた。

ランダムサブドメインは、DNSキャッシュ汚染攻撃の一種であるカミンスキー型攻撃や、DNS権威サーバに対するDDoS攻撃であるDNS水責め攻撃に使われる。毎回異なる名前を生成してDNS問い合わせを繰り返すことにより、キャッシュによるトラフィック軽減が行なわれず、結果としてDNSキャッシュ汚染攻撃の機会を増加させたり、DNS権威サーバに対する負荷を増加させサービス不能攻撃をおこなうことが可能となる。

本提案では、DNSSECにおいてレコードの不在証明に使用するNSEC3レコードをキャッシュサーバ上で利用することにより、キャッシュサーバ側で不在が証明できるレコードについて、外部に再帰問い合わせを行なわず、問い合わせを行ったクライアントに対して即座にレコード不在を返答する。

この方式により、ランダムな文字列を負荷されたDNS問い合わせについても、多くの部分をキャッシュサーバ上のみで完結させることができ、攻撃時にDNS権威サーバに対する負荷を軽減することが可能となる。

本提案はインターネットドラフトとしてIETFのdnsopワーキンググループにて提案されており、現在はワーキ

ングループドラフトにするための議論をおこなっている。

3.2 IETF93報告 (JPRS 藤原)

JPRSの藤原氏より、ISOC-JP IETF報告会の資料をもとにIETF93におけるDNS関連のWGについての報告が行なわれた。報告をおこなったWGはdnsop、dprive、dane、dnssdとなる。本報告によって紹介されたインターネットドラフトについて、提案者本人からの解説もあり、当該インターネットドラフトについての議論も併せておこなわれた。

第４章　おわりに

本年度はDNSワーキンググループでの議論を元に、大規模なルートネームサーバ実証・実験環境であるyetiプロジェクトの立ち上げが行なわれた。yetiプロジェクトは近く行なわれる予定であるDNSSECルート鍵更新による影響の見積もりや、ルートネームサーバの様々な運用形態についての知見を得ることが期待できる。DNSワーキンググループでは、yetiプロジェクトで得られた知見を元に、より活発な議論をすすめていく。