第22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　2016年WIDE春合宿での議論まとめ

2016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。

- JP,RootでのIDNクエリの状況(日本レジストリサービス 藤原)
- AXFRの調査(日本レジストリサービス 藤原)
- RIPE Atlas(国立情報学研究所 福田)
- Yeti-DNS Project Update(慶應義塾大学 加藤)
- glibcの脆弱性(CVE-2015-7547)について(日本レジストリサービス 森下)
- DNSパケットフォーマットの話(日本レジストリサービス 藤原)

2.1　JP,RootでのIDNクエリの状況(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、JPドメイン、およびRootドメインにおける国際化ドメインの状況について報告があった。

現在登録されている日本語ドメインについて、現在は140件ほどあり傾向としては均衡状態にある。また、JPおよびRootに寄せられるDNS問い合わせを解析した結果、JPについては８年前に急激に増加して以降、ここ２、３年は微増傾向であり、全体の問い合わせの0.3%ほどが国際化ドメイン名に対する問い合わせとなっている。また、Rootに寄せられる問い合わせについても同様に微増傾向であり、全体の0.1%ほどが国際化ドメイン名に対する問い合わせであった。問い合わせの内訳については、実在するTLDに対する問い合わせはほぼ変わらず、実在しないTLDに対する問い合わせが増加していた。以上より、ブラウザのIDN対応が進んだ結果、IDNクエリは着実に増加していることがわかった。

2.2　AXFRの調査(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AXFR (Asynchronous xfer、全ゾーン転送)によりゾーンの全ての情報が漏洩する問題について説明があった。また、登録されているドメイン名について、ネームサーバがAXFRを許可しているかチェックするツールを開発し、日本レジストリサービスで調査をする予定である旨、報告があった。本調査の結果は日本レジストリサービスのホームページ上で公開されている。

2.3　RIPE Atlas(国立情報学研究所 福田)

国立情報学研究所の福田氏より、RIPEの主導で進められている全世界的な計測プローブシステムAtlasを利用したDNSサーバの計測について報告があった。RIPE Atlasは多数の計測用インターネットノードを世界中の協力機関に設置し、複数地点からのping, traceroute, digなどを実

行して計測するものである。

今回の実験ではDNSSECの署名がされている権威サーバを用意し、その名前を各probeを利用して名前解決をすることで、DNSSECの署名検証の対応状況と挙動の調査をおこなった。

2.4 Yeti-DNS Project Update(慶應義塾大学 加藤)

慶應義塾大学の加藤氏より、Yeti-DNSプロジェクトの中間報告があった。Yeti-DNSプロジェクトは、ルートサーバと同じデータセットを持つ権威サーバを用いて実インターネット上にテストベッドを構築し、Rootに対するさまざまな変更とその影響を調査するものである。

報告では、Yetiに新しく追加された権威サーバの紹介と、現在までに実施された実験について説明があった。実験は、ルートにおけるPriming Responseの増加、ZSKの鍵長増加、ルートゾーンデータ配布元別に複数のZSKによる署名、KSK鍵更新などをおこない、それぞれの場合についてサーバ上でデータ取得をおこない、クライアント、およびサーバに与える影響の調査をおこなった。

また、プロジェクト参加の募集などがおこなわれた。プロジェクトの参加は、サーバ運用者としての参加、テストベッド利用者としての参加があり、特にDNS名前解決機構を持ったブロードバンドルータのベンダなどの参加を期待している。

2.5 glibcの脆弱性(CVE-2015-7547)について(日本レジストリサービス 森下)

2016年2月に注意喚起がおこなわれたglibcの名前解決機能における脆弱性について、日本レジストリサービスの森下氏より報告があった。当該脆弱性はglibcに組み込まれている名前解決機能であるgetaddrinfo()関数に脆弱性があり、glibcを用いてそれらを利用しているOS、ソフトウェアが影響を受けるものである。glibcは多くのlinuxディストリビューションで採用されているが、glibcを利用しないAndroidやiOSなどは本脆弱性の影響をうけない。

攻撃は細工をされたDNS応答をクライアントに返すことでおこなわれる。そのため、クライアント側からの問い合わせに対応する形で、ポート番号等を合わせて送信する必要があるため、通常の環境では攻撃を成立させることは難しい。また、細工された応答はDNSメッセージとしては異常であるため、一般的なフルリゾルバを経由する名前解決において影響を受ける可能性は少ない。

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。

- DNS query trends seen at Root and JP, 14 June, 2016, NANOG 67 DNS Track, Chicago, IL, US.(日本レジストリサービス 藤原)
- IETF 95 報告(日本レジストリサービス 藤原)
- WPAD name collision(日本レジストリサービス 森下)

3.1 DNS query trends seen at Root and JP, 14 June, 2016, NANOG 67 DNS Track, Chicago, IL, US.(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、JP権威サーバ、およびルートネームサーバで定期的に行なわれている一日のトラフィック計測(A Day in the Life of the Internet/DITL)の解析結果について報告があった。

ルートネームサーバについては、問い合わせは継続的な増加傾向にあり、８年前のDITL計測結果と比較すると約5倍の問い合わせ量になっている。また、ごく少数のホストから秒間600を超える大量の問い合わせが発行されていることがわかった。

IPv6に関する問い合わせの量については、AAAAレコードの問い合わせが17%を占めており、少なくないホストがIPv6アドレスの問い合わせを行っていた。また、DNS自体の通信プロトコルがIPv6であるものについては全体の7%となっていた。また、DNSSECに対応しているとみられるリゾルバからの問い合わせは10%程度となっていた。

3.2　IETF 95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、ISOC-JP IETF報告会の資料をもとにIETF95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, dbound, dnssd, homenet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。

3.3　WPAD名前衝突(日本レジストリサービス 森下)

日本レジストリサービスの森下氏より、Webプロキシ探索プロトコルであるWPADで利用されるドメイン名の衝突により発生する脅威について説明があった。

WPADはWindows等で利用されているWebプロキシ探索プロトコルであり、DHCP等で取得されたドメイン名にWPADというラベルのprefixを付けたホストを探索し、そちらをWebプロキシとして自動的に設定する。

本プロトコルは当該ドメイン名が見つからなかった場合、より上位のドメインに問い合わせる(例えばwpad.aaa.example.comが見つからなかった場合、wpad.example.comを探索する)。そのため、悪意をもった人間がドメインツリー上においてこのような問い合わせが発生する場所にWPADというラベルを含むドメイン名を取得することにより、クライアントに対して攻撃者のWebプロキシの情報を送信でき、HTTP通信の情報を詐取することができる。

本脆弱性はWPADのプロトコルに起因するものであるため、対策としてはWPADを利用しない場合にWPADを無効にすることが必要となる。

第４章　おわりに

本年度は大規模なルートネームサーバ実証・実験環境であるyetiプロジェクトにより、さまざまなルートネームサーバの変更に対する知見が得られ、これらの情報はルートネームサーバの運用者に対してフィードバックが行なわれた。DNSワーキンググループは、引き続き実証実験をおこない、またそれらについての議論を活発におこなう場として、来年以降もワーキンググループの活動をすすめていく。