≪ 巻末の付録USBメモリに追加資料を収録 ≫

第28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。2013年は春と秋のWIDE研究会においてミーティングを開催し、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。

本年度では、DNSSECの本格的な運用が開始したことによる運用上の問題点や知見と、DNS増幅攻撃によるDDoS攻撃関連の報告や調査が多く見られた。

第２章　2013年WIDE春合宿での議論まとめ

2013年3月のWIDE春合宿において、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 RRL (response rate limiting) : (ISC Paul Vixie)
  DNS応答のレートを変更する BIND の新しい機能について報告があった。本機能は権威サーバ上で適用され、DNS増幅攻撃に利用されることを防ぐものである。

- Report of BIND 10 trial in JP(JPRS 藤原)
  BINDの新バージョンであるBIND10の評価報告。いくつかの仕様に準拠していない動作を発見し、報告・改善をおこなった。また、BIND9と比べて通常のクエリ応答速度には問題はなかったが、ゾーン転送の速度で大きく劣っており、まだ単独で運用をおこなうことは難しい状態である。

- Let's make new DNS servers(JPRS 藤原)
  新しいDNSを開発する提案。DNSサーバは権威サーバ、キャッシュサーバなど、その働きによって求められる性質が大きく違い、また規模によっても必要となる要求は変わる。今回の提案ではDNSサーバを機能・規模によりクラス分けし、各DNSサーバに求められる性能と、既存のDNS実装ではカバーしにくいクラスについての分析について議論があった。

- D-RootのIPv4アドレス変更とプライミングの概要 (JPRS 森下)
  Dルートネームサーバの IPアドレス変更に関する報告。IPアドレス変更は2013年1月に行われ、アドレスブロックおよびAS番号も変更となった。旧IPアドレスは半年の間は並行運用されるが、その後は新しいIPアドレスのみに変更になる。ルートネームサーバのIPアドレスは各DNS実装で設定されているため、当該設定ファイルを変更するか、新しいバージョンのDNS実装を利用する必要がある。

第３章　2013年WIDE秋合宿での議論まとめ

また、2013年9月のWIDE秋合宿においても、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。

- Side effect of DNSSEC an increase of DS queries(JPRS 藤原)
  JPゾーンで観測されたDSレコード問い合わせの異常な増加についての報告。DSが存在しないドメインについて、DNSSEC対応クライアントが必ずDSを問い合わせることに起因する。回避策としてダミーDSレコードをゾーンに挿入する方法が提案された。

- An Measurement Study of Open Resolvers(NICT 高野)
オープンリゾルバについての調査報告。すべてのIPアドレスに対して再起付き問い合わせを送り、結果として300万台のDNSサーバと、250万台のオープンリゾルバが発見された。オープンリゾルバは中国・アメリカ・メキシコに多く存在しており、また、多く迷惑メールが送られてくるドメインのアドレスブロックに属しているものが多く見つかった。

- 第一フラグメント便乗攻撃(JPRS 森下)
UDPのフラグメンテーションを利用した新しいDNS詐称攻撃についての報告。DNSのパケット同定に利用するポート番号、DNS IDなどはパケットの先頭部分にしか存在しないため、フラグメンテーションが起こるサイズのDNS応答の場合、通常のパケットより簡単にDNS詐称が可能となってしまう。対策としては、IPの仕様を変えフラグメントされたIPパケットに対してパケットを同定できる情報を埋め込むか、応答パケットにフラグメント位置を予測されないようにランダムな情報を埋め込む方法が提案された。

- DNS on TCP(JAIST 井上)
DNSにTCPを利用した場合の影響についてシミュレーションを行なった結果の報告。通常のTCPを利用した場合、TCPの応答時間はUDPの1.8倍ほどになるが、TCP FastOpenオプションを利用した場合には1.5倍程度に抑えられた。また、TCPマルチプレクサを利用した場合には、1.3倍程度となり、UDPを利用した場合とプロトコル的には大きくは変わらない時間で対応できることが推定された。

第４章　おわりに

2013年度は、大規模ドメインでのDNSSECの運用を通じて得られた知見についていくつか報告があったことと、OpenResolverによる攻撃とその対策についての議論が多く行われた。DNS wgではこれら２点について、今後も重点的に調査および情報交換をおこなっていく。