第 XIV 部

DNS extension and operation environment

第 14 部
DNS extension and operation environment

本ドキュメントでは、DNS-WG の 2010 年活動を報告する。

第 1 章　DNS-WG 2010 年の活動

DNS ワーキンググループは、研究会および WIDE 合宿においてミーティングを行い、さまざまな DNS のホットトピックについて議論し、意見交換を行うためのワーキンググループである。

本報告書は、2010 年に開催された DNS ワーキンググループミーティングにおいて発表され、議論された事項をまとめたものである。

第 2 章　2010 年 3 月 WIDE 春合宿における議論のまとめ

2010 年春の WIDE 合宿において、DNS WG のミーティングが開催された。本議事録では、ミーティングにて報告ならびに議論された事項をまとめた。

本ミーティングでの議題は以下の通りである。

- DNS リゾルバのシミュレータモジュールについて
- DNS 計測ツールについて
- BIND9 が無応答になる問題について
- JP DNSSEC 導入に向けての試験
- Deliberately Unvalidatable root Zone (DURZ)
- DNSSEC のパケット増大についての議論

DNS リゾルバのシミュレータモジュールについて

慶應義塾大学の鈴木氏より、ネットワークシミュレーションフレームワークである OMNeT++ のモジュールとして動作する、DNS リゾルバのシミュレータの開発について報告があった。シミュレーションを行う対象としては限定されたドメイン名で、それらのドメイン名の名前解決にかかる時間を測定し、かつ担当する権威サーバの地理位置的な場所をもとに遅延を計算する。これに対して、DNSSEC はどうするのか？ パケットロスレートは反映するのか？ という質問が出た。またプロバイダの方から、シミュレーション用のキャッシュサーバのデータは提供できる、などの意見があった。

DNS 計測ツールについて

JPRS の藤原氏より、DNS の計測・解析や、DNS 実装の検証用のため開発したツール群について紹介があった。各ツールの詳細については以下の通り。

- watchsoa
  ゾーンの SOA レコードをマスターサーバおよびスレーブサーバより定期的に取得し、SOA レコードのシリアルから、ゾーン転送にかかる遅延を記録するツール
- dns_reply
  指定した DNS サーバに対して query を連続で発行し、サーバに負荷をかけるツール
- replyconf
  DNS サーバ上で記録された問い合わせのログより、上記 dns_reply で利用可能な問い合わせのパターンを作成するツール。dns_reply を利用して特定のサーバへの問い合わせを再現することができる。
- replyanalize
  dns_reply のサーバからの応答記録を解析するためのツール

これらのツールの一部は藤原氏のホームページにて公開されている。

BIND9 が無応答になる問題について

引き続き JPRS の藤原氏より、BIND9 が特定の状況下において一定時間応答しなくなる現象について報告があった。BIND9 は全データのゾーン転送（AXFR）を行った際にファイルに対してゾーンデータを書き出すが、その際に一切の問い合わせに応答しない状態になる。例えば jp のサーバの場合一日に一度ずつ AXFR をしているが、そのたびに 5 秒ほど応答ができなくなる。原因としては、BIND9

が応答とディスクの情報が一致することを実装的に担保しているためであり、ジャーナリングを行わない AXFR ではこのような無応答が発生する。ジャーナリングを行う追加したデータのみのゾーン転送（IXFR）ではこの問題が発生しない。本現象は BIND9 の開発元である ISC にバグレポートとして送っている。

これについて、オプションで BIND9 の動作を変えられるようにすれば回避できるのではないか、などの意見が出た。

JP DNSSEC 導入に向けての試験について

JPRS の民田氏より、JP ドメインにおける DNSSEC 導入に向けての試験について報告があった。将来的に JP ドメインに DNSSEC の導入がされるため、JP ドメインの利用者も DNSSEC が利用できるようになるが、そこで DNSSEC の導入によって DNS の管理がどのようにかわるか？ということについて説明があった。トラフィックの増大や、署名検証にかかるリゾルバサーバの負荷増大、署名データによるゾーンデータの増大などがあり、軽い見積もりでメモリが 5〜10 倍必要になる、という予測になる。

Deliberately Unvalidatable root Zone (DURZ)

慶應義塾大学の加藤氏より、ルートネームサーバから問い合わせの応答が来ない場合にどのような影響が出るかを検証するために、ルートゾーンに検証不能な署名データを挿入する実験について報告があった。「検証不能な署名データ」とは、検証可能な署名データと同じサイズを持つが、署名としては正しくなく、検証できないデータのことである。本実験は DNSSEC のルートゾーン導入のためのスケジュールである「インクリメンタル・ロールアウト」の一環であり、DNSSEC 導入による影響を段階的に見積もるために行われている。実験は 1 月下旬より行っており、各ルートにおいて段階的に実施している。結果としては、ルートネームサーバ側から見て大きな変化がなかった。BIND9 において Authority Section のサイズが増大したため、こちらを修正した。本実験は 5 月ぐらいまでに全てのルートネームサーバに対して実施されるため、サイズが大きい DNS パケットを通さない機器があると問題が発生するかもしれないという注意喚起があった。

DNSSEC のパケット増大についての議論

DNSSEC 導入により DNS パケットは増大することが見込まれているが、それについていくつか議論があった。一般的な OS や、プロバイダなどで利用される業務用ネットワーク機器などではパケット増大による影響はでないと予測されているが、ブロードバンドルータなどの家庭内でのネットワーク機器で問題が出る可能性はある。これに対して、現在 JPRS 主導で DNSSEC の検証を行うプロジェクトがあり、家庭用ルータベンダも参加しているとの紹介があった。家庭にすでに配置されているブロードバンドルータが対応できるかどうかについては、テストサーバである DNS-OARC を使う方法、NIC.CZ の名前を問い合わせる方法などが報告された。

サーバ側の対策としては、BIND9 の新しいバージョンで MTU ディスカバリを無効にするオプションをつけ、EDNS0 と MTU サイズで競合する問題について対処をしたことが報告された。

また、Linux では DF bit を立てて送ることがデフォルトになっており、これによってサイズの大きい DNS パケットが問題になることがある。こちらに対してはインターフェースの MTU サイズを下げる、ソケットオプションを変更するなどの対処が考えられるのではないか、などの意見が出た。

第 3 章　2010 年 9 月 WIDE 秋合宿における議論のまとめ

2010 年秋の WIDE 合宿において、DNS WG のミーティングが開催された。本文章では、ミーティングにて報告並びに議論された事項をまとめた。

本ミーティングでの議題は以下の通りである。

- DNSSEC でのハイパースレッディングの利用時のパフォーマンス
- DNS での等価文字の扱い
- DNS RPZ

DNSSEC でのハイパースレッディング利用時のパフォーマンス

JPRS の民田氏より、DNSSEC の署名および検証において Intel のハイパースレッディングを利用し

た場合と、していない場合のパフォーマンス測定について報告があった。

BIND 等を始め、広く利用されている暗号化ライブラリである openssl は、暗号化処理においてその並列度を指定できる。その並列度を変化させながら、RSA の署名・検証、および SHA-1/SHA-256 の署名・検証のパフォーマンスについて測定した。

Intel のハイパースレッディングは、処理中のパイプラインの空きなどを利用して、実際には 1 コアでも、2 以上のスレッドを同時に動作させているのと同じような効果を出すことができる技術である。そのため、CPU コアの数以上のスレッドを並列動作させても、性能向上が期待できる。

実験した結果、RSA の署名および検証についてはハイパースレッディングの効果により、CPU のコア数よりも多いスレッドにした場合にも、ゆるやかな性能向上をし、実コア数の倍程度までのスレッド数まで上昇を確認できた。しかし、SHA-1 および SHA-256 の場合は実コア数で性能は頭打ちになり、スレッドをそれ以上増やすと、ハイパースレッディング利用時には逆にパフォーマンスが低下することがわかった。

この結果に対して、暗号化方式とは直接は関係なく、実装上の問題ではないのか、他のライブラリなどでも試すといいのでは、などの意見が出た。

DNS での等価文字の扱い

JPRS の藤原氏より、DNS での等価文字の取り扱いについて提案があった。

現在、DNS においてさまざまな文字コードを利用可能にする拡張が提案されているが、他の多言語文字コードと同じく等価文字、例えば日本の漢字と中国の簡体字などの取り扱いについて多くの議論が続けられている。

等価文字を扱う場合、何らかの DNS ツリー上のリダイレクト機構が必要である。現在、いくつかのドラフトが考えられており、DNAME リソースレコードや BNAME リソースレコードを利用して等価文字を別の DNS ツリーにリダイレクトし、それらの等価文字を同じように扱う方法が提案されている。

しかし、DNAME/BNAME は自分以下のサブツリーについてリダイレクト可能ではあるが、自分自身のラベルについてリダイレクトできないという問題がある。また、自分自身のリダイレクトのために CNAME を使うことは、RFC2181 で指摘されている問題があるため行えない。

そこで、藤原氏は DNAME/BNAME に変わる擬似リソースレコードである SNAME を提案した。SNAME は擬似リソースレコードのため、ネームサーバ内部の処理のためだけに使われ、実際の DNS プロトコルとして通信される場合は既存のリソースレコードである CNAME に変換される。ネームサーバは寄せられた問い合わせに合わせて等価文字を処理して返答する。

本方式の利点としては、プロトコル上に変更を加えることがなく、かつ旧来のリゾルバや DNSSEC validator も対応ができることが挙げられる。欠点としては、擬似コードを内部的に変換するため問い合わせの内容にあわせて署名を生成しているため、パフォーマンス的に不利なことである。

DNS Response Policy Zones (RPZ) (ISC: Paul Vixie)

ISC の Paul Vixie 氏より、新しいバージョンの BIND9 に搭載される予定の拡張機能である Response Policy Zones (RPZ) について紹介があった。RPZ は、特定のドメイン名について名前解決を行わないことでブロッキングを実現する機能である。ブロッキングを行うドメインについては、内部的に設定することも、メールにおける RBL のように外部のデータベースを利用することも可能である。ブロッキングは NXDOMAIN などを利用して実際に存在しないかのように見せたり、もしくは別の名前を返すことで問題のあるドメインであることを注意喚起する web ページに誘導することも可能である。

現在は BIND に当該機能だけを搭載しており、実際の評価データベースの運用についてはスコープ外としている。

第 4 章　まとめ

今年はルートゾーンおよび JP ゾーンの DNSSEC 署名が行われた、まさに DNSSEC 元年とも言える年であった。そのため、DNSSEC の基幹ゾーン導入に関する内容や、実運用に関する議論、例えば DNSSEC

導入によるサーバおよびネットワークへの影響の見積もり、変化の測定、および運用上で発生した問題点の共有などが活発に行われた。

DNSSEC だけでなく、DNS のブロッキングなどの新しい DNS のセキュリティへのアプローチについても提案があり、大きな議論が行われた。

DNS ワーキンググループは、引き続き DNS のプロトコルや運用、セキュリティなどに関する話題について議論を行える場所として、来年以降もワーキンググループを継続し、ミーティングを開催していく所存である。