第 XIII 部

DNS extension and operation environment

第 13 部
DNS extension and operation environment

本ドキュメントは、DNS-WG の 2009 年活動報告である。

第 1 章　DNS-WG 2009 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、2009 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　2009 年 3 月 WIDE 春合宿における議論のまとめ

2009 年春の WIDE 合宿において、DNS ワーキンググループ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。

本ミーティングの議題は以下の通りである。

- On the Fly IPv6 Reverse DNS Server
- DO=1 クエリの増加原因について

2.1 On the Fly IPv6 Reverse DNS Server

JPRS の民田氏より、IPv6 の逆引きレコードをクエリ到達時に動的に生成するネームサーバの考え方の報告があり、JPRS の藤原氏より実装についての報告があった。IPv6 の逆引きレコードは、広いアドレス空間とステートレスなアドレッシング方法から静的に設定することが困難なため、サーバなどを除くほとんどのホストで IPv6 の逆引きは設定されていない。そこで本プログラムは、IPv6 アドレスのプレフィックス部分だけに着目し、下位のアドレス部分は一定のルールで変換してやることにより動的に逆引きレコードの生成を行う。

このサーバプログラムは perl で実装されており、現状では秒間 1000 クエリに対応できる。また、C 言語などで書き直すことによりさらにパフォーマンスは向上することが期待される。

2.2 DO=1 クエリの増加原因について

JPRS の藤原氏より、DO bit（DNSSEC OK フラグ）がセットされたクエリが増加しているとの報告があった。増加は、

- `A.DNS.JP G.DNS.JP`（JP ゾーンの権威サーバ）
- `ns.tokyo.wide.ad.jp`（wide ゾーンの権威サーバ）
- 藤原氏が個人的に所有しているドメインのサーバ

の 3 箇所で観測された。DO bit がセットされていると、DNSSEC で署名されているゾーンは署名をレスポンスに入れることになる。増加原因を調べるため、いくつかのリゾルバ実装のソースおよび挙動を観察したところ、BIND（9.3 から 9.6）、Unbound（1.0.0 から 1.2.0）および Windows 2008 R2 において必ず DO bit を立ててクエリを送信することがわかった。

これらの挙動についてであるが、RFC によれば「DNSSEC に対応したリゾルバは必ず DO bit をセットしなければならない」となっており、その記述に準拠していると考えられる。

これらリゾルバの挙動による影響だが、多くのリゾルバが DO bit をつけているため、ゾーンに DNSSEC の署名をした場合、署名をしてない場合に比べて数倍以上のトラフィックが必要になると推測される。そのため、DNSSEC を有効にする場合はそれらに対応できるネットワークおよび計算機資源が必要になると考えられる。

第 3 章　2009 年 9 月 WIDE 秋合宿における議論のまとめ

2009 年秋の WIDE 合宿において、DNS ワーキンググループ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。

本ミーティングの議題は以下の通りである。

- BIND 10 の紹介
- BIND9 の脆弱性報告：ANY UPDATE
- DNS Message API
- 名前をロンゲストマッチするアルゴリズムについての考察

3.1 BIND 10 の紹介

ISC の神明氏より、ISC で開発が始まった BIND9 の後継バージョンである BIND10 の報告があった。

BIND10 は古くなった BIND9 の設計を全て見直し、全く新しい設計で開発が行われている。全体をモジュール化しコンパクトにまとめ、各部分を他のソフトウェアに再利用可能な形にしている。また、BIND9 で散見されたクラッシュを低減するように工夫がされている。クラスタ化にも対応し、それぞれのクラスタノードで設定情報を共有できる。

BIND10 の開発は 2009 年 4 月 1 日にはじまり、いくつかの TLD がスポンサーについている。また、従来の BIND の開発体制とは異なり、オープン環境での開発を積極的に行い、常時開発中のソースコードを閲覧可能にしている。また、開発者用のメーリングリストもオープンにしており、広く開発へのコミットを求める体制でプロジェクトを進めている。

3.2 BIND9 の脆弱性報告：ANY UPDATE

JPRS の民田氏より、BIND9 の脆弱性に関する報告があった。

現在まで（9 月時点）の BIND9 の実装は TYPE が ANY だった場合の UPDATE の扱いに問題があり、対策のされていない BIND9 のバージョンで、1) マスターゾーンの設定がある、もしくは 2) localhost とその逆引きゾーンの設定を持っている場合においてサーバをクラッシュさせる DoS 脆弱性がある。

また、本脆弱性について camp のデモ展示（屋台村）において実演を行っている。現在のところバージョンアップ以外の対処法は無く、BIND 上でアクセスコントロールをかけても回避することができない。

3.3 DNS Message API

ISC の神明氏より、先ほど報告のあった BIND10 の開発に関連して、BIND10 の一部として開発されている再利用可能な DNS API コンポーネントについて説明があった。旧来の DNS ライブラリとしては BIND9 由来の libdns が存在するが、ドキュメントが無くインターフェースもあまり使いやすいものとは言い難かった。そこで BIND10 では C++ をベースに、より使いやすく、かつパフォーマンスも従来どおりに良いクラスライブラリを開発している。

また、ドキュメンテーションに関しても専属のスタッフを置き、いままでのドキュメント不足を解消する体制で行っている。

これに関して、Wire Format のデータをどのようにストアすべきか、DNSSEC 用のメソッドが追加されるべきか、それぞれのクラスのドメイン分けをどのようにするか、国際化ドメイン名の対応はどうするか、などの議論が行われた。

3.4 名前をロンゲストマッチするアルゴリズムについての考察

ISC の神明氏より、ネームサーバの実装において名前のロンゲストマッチを行うアルゴリズムについて発表があった。現在 BIND9 は赤黒木を使い名前のロンゲストマッチを実現しているが、もし名前が十分に短いのならばラディックス木の方が効率がよいのではないか、という提案がなされた。

これに対し、1 文字ずつマッチを行うとコストが高いので、8 文字ずつマッチするアルゴリズムはどうか、ラディックス木を使う実例としては経路選択があるが、そちらの実装を参考にしてはどうか、などの意見が出された。

第 4 章　セキュリティを考慮した名前解決エージェントの設計と実装

Domain Name System（DNS）は、インターネットで広く一般的に利用されている名前解決システムであり、インターネット上におけるアプリケーションの利用に先立ち、ホスト名から IP アドレスへの変換を行っている。しかし近年、DNS に関する攻撃がいくつか報告されている。その代表的なものが DNS spoofing である。DNS の名前解決を詐称することで、正規の IP アドレスとは異なったアドレスを攻撃対象に与え、正規の通信相手に成りすまして通信

を誘導することが可能となってしまう。この問題への対策のためにDNSSECが考案されたが、運用コストなどの問題から普及しているとはいいがたい。そこで本研究では、DNSSECを利用できない環境であってもDNS spoofingに対抗できるDNS名前解決方式を提案した。また、提案に基づいたプロトタイプ実装を行い、攻撃に対する効果に関して評価を行った。本研究で提案した方式により、DNSSECが普及していない現状であっても、クライアントにDNS spoofingからの保護を提供することが可能になった。

なお、この研究成果は、2009年3月に発行された情報処理学会論文誌「柔らかなサービスを支えるインターネット技術/分散システム運用管理技術」特集号に発表・掲載されている。(文献[105]参照)。

第5章　まとめ

昨年はKaminsky Attackの発表の影響もあり、DNS脆弱性についての議論が多く行われた。今年もそれに続き脆弱性関連の報告などが多く行われた。また、DNSSECのクライアント側の対応が増加しているという報告もあり、DNS脆弱性への脅威に対応してDNSSECが普及し始めつつあると考えられる。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。