第 XV 部

DNS extension and operation environment

第 15 部
DNS extension and operation environment

第 1 章　DNS ワーキンググループ 2008 年度の活動

DNS ワーキンググループは、主に WIDE 合宿や研究会においてミーティングを開催し、その時点で話題となっている DNS に関する事項を議論し、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、2008 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　2008 年 3 月 WIDE 春合宿における議論のまとめ

2008 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。本章では、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ものである。

本ミーティングでの議題は、以下の通りである。

- IPv6 on Root DNS
- ns-wide
- a.dns.jp 解析

IPv6 on Root DNS（kato@wide.ad.jp）

ルート DNS サーバに対して IPv6 AAAA レコードが追加された。2008 年 2 月 4 日（US 時間）に追加され、どのような影響が各ルート DNS サーバ、とくに M.root-serves.net に対してあったのかの報告が行われた。

AAAA record が追加されたのは A、F、H、J、K、M の 6 つのルート DNS サーバである。M ルート DNS サーバでは、IPv4 : IPv6 の DNS クエリの割合が 16000 : 80 程度であることが確認された。以前からいくつかのルート DNS サーバ運用者は、IPv6 トランスポート対応への準備を進めていたため、とくに大きな障害はなくスタートすることができた。M ルート DNS サーバも 2000 年から試験サーバ運用を開始していたため、何も問題なく運用を開始することができた。

IPv6 クエリの割合は、リゾルバサーバとして利用されている DNS サーバがどれだけ IPv6 トランスポートの到達性を有しているかに影響される。エンドノードが IPv6 対応しているかどうかとは直接関係しているわけではない。

ns-wide（onoe@sm.sony.co.jp）

WIDE Project のリゾルバ DNS サーバである、ns.wide.ad.jp に関しては、以前からオープンリゾルバ問題が指摘されていた。ns.wide はどの IP アドレスからの再帰問い合わせにも応えるように設定されており、これが問題であると日本 DNS オペレーターズグループ（dnsops JP）から指摘を受けていた。

この問題に関して、まずはコンテンツサーバとリゾルバサーバを分割することで対応を行った。以前は同一の DNS サーバ（ns.wide.ad.jp）にて wide.ad.jp ゾーンを受け持つ権威サーバとリゾルバサーバを運用していたが、あらたに ns-wide.wide.ad.jp という DNS サーバを用意し、このサーバに wide.ad.jp ゾーンの権威サーバを移した。実際には同一のサーバを用い、BIND9 の view 機能を利用することによって、権威サーバとリゾルバサーバを分割した。

この対応によって、外から権威サーバとして見える ns-wide.wide.ad.jp はオープンリゾルバサーバとしては機能しなくなったとの報告があった。

a.dns.jp 解析（minmin@jprs.co.jp）

JP zone の権威サーバの 1 つである、a.dns.jp のエニーキャスト運用状況に関しての報告がなされた。具体的には、エニーキャスト拠点からの経路広告を止めたり、拠点からの経路広告に対して AS prepend を行うことで、a.dns.jp の各エニーキャスト拠点へのアクセス変化を計測した。計測ならびに実験自体は 2007 年 2 月に行われたものである。

計測ならびに実験は以下の項目に関して行われた。

(1) 東京拠点のみ AS を 1 個 Prepend した場合と、東京拠点に 2 個かつ大阪拠点に 1 個 Prepend した場合とで同じ挙動を示すか
→ ほぼ同様の結果を示した

(2) ニューヨーク拠点稼働前と稼働後のクエリ比率の計測

	大阪拠点	東京拠点	ニューヨーク拠点
ニューヨーク稼働前	64%	36%	0%
ニューヨーク稼働後	56%	30%	14%

(3) ニューヨーク拠点稼働後、大阪拠点と東京拠点にて AS を 1 個 Prepend

大阪拠点	東京拠点	ニューヨーク拠点
38%	24%	38%

DNS クエリのソース IP アドレスから地理的分布を分析すると、ニューヨーク拠点に来るクエリは、US やロシアからのクエリが多いということが判明した。しかし、その他の国、とくにアジア諸国からは思ったほどニューヨーク拠点にクエリが来ることはなく、ニューヨーク拠点稼働前と同じく大阪拠点へのクエリが多いということが報告された。

以上、今回の DNS ワーキンググループミーティングでは、ルート DNS サーバならびに JP DNS サーバに関する報告ならびに議論が議題の中心となった。一方、学生からの発表等は無かったため、DNS ワーキンググループとして学生が発表できるような環境作りならびに指導を行えればと考えている。

第 3 章　2008 年 9 月 WIDE 秋合宿における議論のまとめ

2008 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。

- 脆弱性対策
- a.dns.jp クエリ統計
- Port randomization
- ゾーンデータ比較手法
- M Root DNS クエリ解析

脆弱性対策（orange@jprs.co.jp）

DNS キャッシュ汚染攻撃を非常に効率的に実行できる手法が発見された。通称 Kaminsky Attack と呼ばれる手法で Dan Kaminsky 氏によって発見された手法である。

対処方法としては、以下のものが考えられると報告があった。

- DNS で用いる UDP のポートのランダマイズ
- ACL による利用者の限定
- Ingress filtering による詐称パケット防御
- 権威 DNS サーバとリゾルバ DNS サーバの分離

しかし、どの対処方法も根本的な対処と言えるものではなく、あくまでも攻撃成功の可能性を下げるための対処方法であることが述べられた。

根本的にはどうすればいいのか、という議論も行われ、やはり DNSSEC を導入することが有効であるとの意見が出された。一方で、DNSSEC は確かに有効な対処方法であるが、すぐに普及するのが難しいことも明らかであるという意見が出された。そのため、

- 疑わしい応答クエリが来たら再度 TCP で聞き直す
- 何度も問い合わせを行い結果を得る

といった、攻撃の成功確率をさらに下げるための手法も研究されており、実際に商用製品に導入されつつあることが報告された。

また、簡単に DNS サーバの脆弱性をチェックできるサイトがあることが紹介された。

- https://www.dns-oarc.net/oarc/services/dnsentropy/
- https://recursive.iana.org/

a.dns.jp クエリ統計（minmin@jprs.co.jp）

a.dns.jp に来る問い合わせクエリのソースポートに関する統計を紹介した。これは前述の Kaminsky Attack に対応したものであり、a.dns.jp に問い合わせを行ってくる DNS サーバがどれだけソースポートランダマイズの対応を行ったかを調査したものである。

ソースポートが偏っている DNS サーバとソースポートがランダマイズされている DNS サーバの比

率の傾向を時系列で示す。

2008/7/7@ 変化が表れ始め、ソースポートランダマイズされたDNSサーバの割合が増え始める

2008/7/23@ ソースポートが偏っているDNSサーバとソースポートがランダマイズされたDNSサーバの比率がほぼ同一となる

2008/7/28@ 偏っているDNSサーバ：ランダマイズされたDNSサーバの比率が2：8となる

しかし、この統計ではあくまでもIPアドレス単位でDNSサーバを見ているため、NATの裏側にDNSサーバがある場合や、そもそもほんの少ししかクエリを送付してこなかったDNSサーバは正確に判定できていない可能性があることが付け加えられた。

次に、何個程度のポート番号を使い回しているDNSサーバ実装が多く見受けられるのかの統計が示された。統計上の特異点として見受けられたのは、8個のポートを使い回す実装、256個のポートを使い回す実装、2000個程度のポートを使い回す実装、40000個程度のポートを使っている実装が見受けられた。DNSサーバの実装の差異により、統計に特異点が出現することが見て取れる結果となった。

Port randomization（jinmei@isc.org）

次に、Kaminsky Attackに対しての対策となる、ポートランダマイズに関する報告と議論が行われた。

Kaminsky Attackに対する対策として、ポートランダマイズはそれなりの効果を発揮する。しかし、順調に攻撃を続けることができるならば、10時間程度で攻撃が成功してしまう。つまり、あくまでも攻撃の成功確率を下げる対処方法であることは前述の通りである。

さらに、DNSサーバがポートランダマイズを実装したとしても、運用状況によっては以下のような問題が発生するとの報告があった。

- NAT問題
  NATの裏側にDNSサーバが存在すると、問い合わせクエリのソースポートはNATのソースポート選択アルゴリズムに依存してしまうため、攻撃されやすくなる場合がある。
- firewall問題
  query-sourceでポート番号を固定することができなくなったため、firewallでの判定条件が増え、firewallの処理が重くなったとの事例もあった。

そこで、ポートランダマイズに代わる対処方法としては、どのような案があるか紹介された。以下にそれをまとめる。

- DNSSEC
  根本的な解決策であるが、普及が必要。
- 問い合わせする名前に対して、大文字小文字を混ぜる
  ほとんどの実装はクライアントの大文字小文字をキープしたまま返事を返す。この特性を利用して、ところどころ大文字を混ぜてクエリを出すことによって、問い合わせクエリのエントロピーを増やすことができるという手法である。しかし、数字のみのドメイン名や短いドメイン名ではエントロピーが増えないため、効果の薄い手法となる。
- 問い合わせの度にソースアドレスを変える
  IPv6を問い合わせのトランスポートとして利用できる場合には、問い合わせの度に下位64 bitを変更して、ソースアドレスを変更して問い合わせを行う。
- 攻撃検知
  問い合わせに対する応答クエリを観測して、攻撃が検知されたらTCPに切り替えるなり、応答を破棄するという手法。しかし、攻撃を検知するための明確な手法は存在しないため、その有用性に疑問が残る。
- TCPによる問い合わせ
  応答クエリを詐称される可能性はぐっと減るが、一方でTCPセッションDoS攻撃が容易に行えてしまうのも事実である。
- キャッシュの上書き禁止
  一部の実装では、後から届いた応答クエリによって以前のキャッシュ内容が上書きされてしまうため、汚染攻撃がやりやすくなる事例が存在した。そのため、キャッシュの上書きを禁止するという提案も存在する。しかし、上書きを禁止するとキャッシュのTTLが切れるまで古い名前を持ち続けるという問題も存在する。
- DNS cookie
  IETFのdnsext WGで提案された仕様で、DNSサーバのcookie情報を持つことで、以前問い合わせたことのあるDNSサーバからの応答であることを確認する手法である。EDNS0のオプションを利用して実現する。しかし、全てのDNS実装が一斉に対応することは不可能であるため、未

知の EDNS0 オプションを無視してくれる DNS 実装の場合には問題ないが、不正なオプションと認識して応答クエリ自体を破棄してしまう DNS 実装が存在した場合には、問題となる。

どの対処方法も普及の速度とその効果の両面から完全なものは存在しないという結論となった。そのため、できる対策から行うのが今できる最善の対処方法であり、まずは DNS 実装のアップデートを行うことが最低限の対策であることが確認された。

ゾーンデータ比較手法（minmin@jprs.co.jp）

DNS マスタサーバとスレーブサーバ間において、転送されたゾーンデータが間違いなく一致することを検証するための手法について提案ならびに意見募集が行われた。

IXFR によってゾーンの更新を行っている場合に、あるタイミングで同期がずれ、ゾーンデータに差異が発生している場合はないか、また差異が発生したまま更新が行われ続けていることはないかを監視する良い手法が欲しい、という提案である。

現状では、一日に一度は AXFR をしてゾーンの中身を比較するという手法にて検証しているという報告があった。他には MD5 のチェックサムにて比較する手法も考えられるとの意見もあった。

M Root DNS クエリ解析（kato@wide.ad.jp）

m.root-servers.net に来る問い合わせクエリに関して、IPv6 トランスポートでの問い合わせクエリと、EDNS0 サポートが有効となっている問い合わせクエリのそれぞれの全体に占める割合が示された。具体的な割合とそのグラフに関しては、本報告書のルート DNS の運用の章にて示す。

結論としては、Kaminsky Attack の対策のために DNS サーバの実装をアップデートする管理者が多かったためか、Kaminsky Attack が公表されたのと時期を同じくして IPv6 トランスポートクエリの割合と EDNS0 サポートクエリの割合が増加したことが報告された。

第 4 章　まとめ

DNS ワーキンググループでの発表の多くは Root DNS や JP DNS に関する統計や分析といったものが多く扱われる。しかし、本年は DNS にとって大きな話題となった、脆弱性に関する問題が公表されたことに関連し、この攻撃に関する発表や議論が多く見受けられた。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に関する話題を扱い、気軽に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。