

DNSQC-TF 2002 年度活動報告

1. DNSQC-TF の概要

DNS(Domain Name System) の最も基本的な機能は、論理的な名前空間であるドメイン名と、インターネット上での通信に必要となる IP アドレスの間の対応づけ、つまり名前解決を行うものである。さらに、電子メールの配送に必要となる情報を取得するためにも、DNS が利用されている。このように、インターネット上の様々なサービスは、DNS を利用しているものが殆んどであり、DNS が正常に機能していることが、インターネットの安定運用には不可欠であり、前提条件であると言える。

しかし、最近以下のような状況が見受けられるようになってきている。

- ・ DNS の不安定な動作
- ・ 不必要な DNS パケットの送信/再送
- ・ 不必要なタイムアウト待ち

DNS は、インターネット上の分散化されたデータベースの協調により、その機能が実現されている。つまり、インターネット上の DNS 管理者一人一人が、DNS の設定を適切に行い、安定した運用を心がけなければならない。

しかしながら、DNS 管理者が自分自身の不適切な設定を発見修正することが難しい場合がある。このため、現在の DNS 設定状況を調査分析し、発生しやすい誤りや、問題の解決方法(正しい設定方法)などを公開することで、DNS の安定運用を目指すことを目的に、WIDE プロジェクト、JPRS、JPNIC の共同プロジェクトとして「DNS 運用健全化タスクフォース」を 2002 年 4 月に設立し、活動を開始した。

2. 活動内容

DNSQC-TF は、以下のような項目を掲げ活動を進めている。

- (1) DNS 設定の調査項目の洗い出し
- (2) 調査プログラムの開発
- (3) 調査プログラムを用いたデータの収集
- (4) 収集したデータの分析
- (5) 分析した結果の公開や個別の通知
- (6) DNS の運用に関する広報教育活動（文書作成やセミナー開催）

2002年度は、基本的な技術の開発と現状の調査を行い、分析結果を発表公開することで、DNS 管理者等へのフィードバック(情報提供)を実施した。

- 2002年4月 DNSQC-TF 設立
- 2002年6月 予備調査の実施
- 2002年7月 IEPG での報告「JPNIC Study on DNS misconfiguration」
- 2002年7月 JANOG10 での報告「DNS 運用の健全化に向けて」
- 2002年11月 試行調査の実施
- 2002年12月 IW2002 DNS-Day での報告「DNS 運用健全化タスクフォース」
- 2002年12月 IW2002 IP meeting での報告
「国際化ドメイン名(IDN)と DNS の適切な設定に向けて」
- 2003年1月 本調査の実施
- 2003年1月 JANOG11 での報告「DNS 正引きの実態」
- 2003年3月 IEPG での報告
「DNSQC-TF (DNS Quality Check Task Force) Update」
- 2003年3月 2002年度活動報告(本報告)

3. 調査対象・調査内容について

DNSQC-TF では、DNS 設定状況の実態を把握するために、調査プログラムを作成し分析を実施することとした。

調査対象：JP ドメイン名を対象とした。

調査内容：以下に調査プログラムの仕様を述べる。

調査プログラムの仕様について

本プログラムは perl で作成した。

入力には、調査したいドメイン名のリストを与える。

調査結果(出力)は、ドメイン名ごとのファイルに格納される。

調査方法は、ゾーン転送を使用せず UDP による DNS パケットの応答で得られる情報から DNS 設定状況の確認を行った。

調査項目は、以下の通りである。

- ・委任の設定に関するチェック
 - 親サーバが返す NS RR Set の親サーバ間の一貫性チェック
 - 子サーバが返す NS RR Set の子サーバ間の一貫性チェック
 - 親が返す NS RR Set と子供が返す NS RR Set の一貫性チェック
 - 親が返す NS List の各サーバに当該ドメインの NS RR を問い合わせた際 Authoritative Answer を返すかのチェック
 - ネームサーバの reachability チェック
原因は問わず、UDP port 53 に答えないサーバを検出
 - 全く索けないドメインの検出

- NS RR に関するチェック
 - NS RR に 1 ネームサーバしか設定していない

- SOA RR の各フィールドの値に関するチェック
 - 子ネームサーバ間のシリアル番号の一貫性のチェック
 - シリアル番号のフォーマットのチェック
 - 推奨フォーマットである YYYYMMDDnn であるかのチェック
 - E-MAIL フィールドに @ 文字が入っているかのチェック
 - refresh および retry フィールドの値のチェック

- MX RR に関するチェック項目
 - MX RR に IP address がセットされているかのチェック

- 不正な文字列が含まれているかのチェック
 - NS RR、MX RR、SOA MNAME フィールドに、使用してはいけない文字列が入っているかのチェック

- CNAME に関するチェック
 - NS RR、MX RR のホストに CNAME が定義されている

- non-routable アドレスチェック
 - NS RR、MX RR に定義されているサーバの IP アドレスが以下の non-routable アドレスであるかのチェック
 - IPv4
 - 0.0.0.0/8 - Historical Broadcast
 - 10.0.0.0/8 - RFC 1918 Private Network
 - 127.0.0.0/8 - Loopback
 - 169.254.0.0/16 - Link Local Networks
 - 172.16.0.0/12 - RFC 1918 Private Network
 - 192.0.2.0/24 - TEST-NET
 - 192.168.0.0/16 - RFC 1918 Private Network
 - 224.0.0.0/4 - Class D Multicast
 - 240.0.0.0/5 - Class E Reserved
 - 248.0.0.0/5 - Unallocated
 - 255.255.255.255/32 - Broadcast
 - IPv6
 - Loopback address
 - Link local address
 - Site local address
 - Mapped address

- ネームサーバのバージョンチェック
 - CHAOS TXT version.bind. を問い合わせた結果の取得

4. 調査結果について

DNS 設定状況調査の実施にあたり、予備調査を 2002 年 6 月に、試行調査を 11 月に実施した。この予備調査および試行調査により、調査方法のレビューや調査仕様の実装確認などを行った。

本章では、2003 年 1 月に実施した本調査の結果について報告する。

4.1 ドメイン名種別ごとの分析

表 1: 2003 年 1 月調査結果

	総数	co.jp	or.jp	ne.jp	ad.jp	gr.jp	ac.jp	ed.jp	lg.jp	地域	汎用	日 本 語
エラー率%	37.9	30.2	30.9	43.4	37.0	37.4	41.7	40.1	39.5	50.2	88.4	
badns%	24.6	21.6	25.4	30.8	30.1	26.9	35.7	31.3	32.0	29.9	10.3	
LAMEns%	17.8	11.9	10.5	19.8	11.4	16.2	13.7	18.4	14.0	26.7	79.0	
nsnone%	11.1	5.9	2.8	11.1	4.5	7.7	1.7	3.3	3.4	19.3	79.1	
cnamens%	0.5	0.4	0.6	0.7	0.5	0.6	0.8	2.0	0.7	0.8	0.0	
cnamemx%	3.6	3.8	3.6	3.5	2.2	4.4	3.2	2.9	3.8	3.5	0.2	
badsoa%	0.3	0.3	0.2	0.3	0.0	0.3	0.3	0.8	0.2	0.3	0.0	
private%	0.0	0.0	0.0	0.0	0.2	0.0	0.1	0.0	0.1	0.0	0.0	

すべて、各ドメイン種別内の割合(パーセント)

エラー率	下記いずれかの設定誤りのあるドメインの割合
badns%	レジストりに登録したネームサーバと、ゾーンに書いたものが違う割合
LAMEns%	レジストりに登録したネームサーバがゾーンのデータをもっていない割合
nsnone%	測定時に全くデータを引けなかったゾーンの割合
cnamens%	ゾーンに登録してあるネームサーバが CNAME であるものの割合
cnamemx%	ドメイン名の MX レコードに書かれているホストが CNAME なものの割合
badsoa%	ゾーンの SOA に間違いがあるものの割合
private%	NS, MX レコードのアドレスに private address が混じっているものの割合

表 1 より、JP ドメイン全体の 37.9% のドメインに、不適切な設定があることがわかる。また、項目別に見ると badns が最も多く、全体の 1/4 に誤りがあることがわかる。LAME が次に多く、全体の 17.8% に誤りがある。

badns は、JP DNS に登録されているネームサーバと、実際に各ゾーンで定義されているネームサーバのリストが不一致なものを検出対象としている。各ドメインのネームサーバを変更する場合には、JPRS への登録とゾーン内の定義の両方を変更する必要があるが、どちらか片方を変更し忘れてしまうと、この種の設定誤りになるため、発生しやすい誤りであると考えられる。ネームサーバの登録および変更作業をマニュアル化するなど、設定作業の誤りを発生させないようにすることが重要である。

LAME は、JP DNS に登録されているネームサーバが、実際にはゾーンに関する情報を持っておらず、当該ゾーンのネームサーバとして機能していないものである。この種の設定誤りは、気が付きにくいということが問題である。LAME の場合、一見正しく機能しているように見えるが、応答内容がキャッシュされた古い情報である場合があるため、適切な名前解決が実行できない状態が発生する。このような状況を回避するためには、当該ゾーンのプライマリあるいはセカンダリネームサーバとしての適切な設定を行ったうえで、上位ゾーン(レジストリ)への登録を行う必要があり、これらのネームサーバの IP アドレスが変更になったような場合には、必要となる設定変更作業を確実に実施する必要がある。

最後に、日本語ドメイン名についてであるが、LAME 率が高い(79%)という調査結果が出ている。これは、日本語ドメイン名をまだ使用していないのにもかかわらず、仮のネームサーバを登録してしまっているために発生している状況であると想定される。今後、日本語ドメイン名の稼働率が高まるにつれて解消されて行くであろう。DNSQC-TF としても、改善されるよう働きかけてゆきたい。

5. 国際的な動向

現在、DNS の運用健全化については、地域レジストリ(RIR)や各国の TLD レジストリにおいても、懸案事項の 1 つとなっており対策の検討が進められている。ここでは、各レジストリでの取り組みについて簡単に報告する。

ARIN では、Lame Delegation を検知した場合、電子メール、電話、郵便で連絡を行い、一定期間(30 日)経過しても改善が見られない場合は、DNS の設定を解除するということを始めている。

http://www.arin.net/registration/lame_delegations/

<http://www.apnic.net/meetings/15/sigs/dns/docs/dns-pres-ray-lame-implement.ppt>

APNIC から同様の提案がなされている。

<http://www.apnic.net/meetings/15/sigs/dns/docs/dns-doc-ggm-lame-dns1.doc>

<http://www.apnic.net/meetings/15/sigs/dns/docs/dns-pres-ggm-sweep-lame-dns.ppt>

RIPE NCC では、DNS 設定状況の調査を行っており、以下のような調査結果が公開されている。

<http://www.ripe.net/ripenc/p-services/stats/revdns/zcheck/quality-report.html>

また、いくつかの TLD レジストリにおいても、ARIN に類似した対策の実施が検討されている。特に BR(ブラジル) のレジストリである Registro.br では、ARIN に類似した対策(既に設定されている DNS サーバのチェック)に加え、ネームサーバの登録時に、そのネームサーバが適切に設定されているかどうかを確認し、正しく設定されている場合にのみ登録を受付けている。この結果、運用の健全化が計られているとの報告がなされている。

http://www.potaroo.net/iepg/march-2003/br_lame_iepg_ietf56.pdf

DNS は、一つの国や地域に限定されるものではなく、世界中のユーザに影響を与えることとなるため、国際的に協調を取りながら運用の健全化を進めて行く必要がある。我々、DNSQC-TF の活動状況についても、国際協調の一環として IEPG において以下の報告を行っている。

<http://www.potaroo.net/iepg/july2002/>

<http://www.potaroo.net/iepg/march-2003/>

6. まとめ

2002 年度は、本プロジェクトを立ち上げるとともに、活動項目として掲げた 6 つの項目の内、(1) DNS の設定においてチェックすべき項目の洗い出し 及び (2) チェックを行うツールの開発 を実施することができた。2003 年 1 月 21 日には、BIND の開発者である Paul Vixie 氏 と意見交換を行う機会を設けることができた。このような機会を得ることができたことは、今後調査分析を進めて行くうえで大変有意義であったと感じている。

また、(3)調査プログラムを用いたデータの収集、(4)収集したデータの分析、(5)分析した結果の公開や個別の通知については、開発した調査プログラムを使用して、本調査を 1 度実施し調査結果を発表公開することができた。プロジェクト初年度としては、大きな成果を得られたと感じている。しかしながら、インターネットの安定した運用という最終目標に向けて、DNSQC-TF が取り組むべき課題は多い。今後も定期的に調査を実施し、分析結果を公開するとともに、適切な設定を行うための情報提供などを積極的に実施して行きたいと考えている。特に、ARIN や Registro.br での試みなどを参考にしながら、各ドメインの DNS 管理者に個別に調査結果を伝えるなど、具体的な改善を計って行きたいと考えている。

インターネットは、DNS 管理者一人一人に支えられていると言っても過言ではない。DNSQC-TF の活動趣旨をご理解いただき、より安定したインターネットの運用のためにご協力頂きたい。