L-014

DNS の危機的状況
The Critical Situation of DNS

鈴木　常彦
Tsunehiko SUZUKI

中京大学情報理工学部[*1]
School of Information Science and Technology, Chukyo University
tss@sist.chukyo-u.ac.jp

本論文は、日本に於ける DNS の運用が如何に不適切で危険な状態にあるかを明らかにするための調査報告である。2005 年にクレジットカード会社や省庁のドメインに不適切な設定があったことが大きなニュースになったにも関わらず、その後過去約 2 年間の追跡調査において状況の改善は進んでいない。さらに、8 割を超える DNS サーバが DDoS 攻撃 (Distributed Denial of Service Attack) の増幅器として利用される可能性があることも判明した。このような状況にあるインターネットはその完全性、可用性において高いリスクに晒されており、非常に脆弱な状態にあると認識せざるを得ない。
キーワード ：DNS，lame, DNS amp, DDoS, domain hijack

1　はじめに

2005 年 5 月 18 日、筆者は VISA.CO.JP の権威あるネームサーバが用いているドメイン E-ONTAP.COM が登録抹消され、誰でも新規に取得可能となったことに気づき、緊急避難としてこれを取得した。これは筆者が VISA.CO.JP の DNS レコードを自由に設定できる状況に置かれたことを意味する。その後、同様の危険な状況が一部の省庁のドメインにも生じていたことなどから一時大きな騒動となり、省庁から注意喚起文書が出されるなどした。詳しい経緯は http://www.e-ontap.com/summary/ を参照されたい。

本報告はこれらの事件以降 2 年間に渡り、筆者の手元にあった約 5 万件の JP ドメインリストを用いて、その運用状態を継続的に調査してきた結果をまとめたものである。調査は以下の項目からなる。

a) Lame Server(無応答と無権威) の有無
b) ハイジャック可能性
c) 短い TTL(毒入れ脆弱性)
d) DDoS 対策の有無

[*1] 〒470–0393 豊田市貝津町床立 101

2　調査方法と結果

調査はリストの各ドメイン毎に以下の動作をする自作プログラムを作成し、2005 年 8 月 29 日から 2007 年 4 月 22 日までの間、随時動作させて蓄積したデータを分析して行った。

1. TLD(Top Level Domain) に登録された当該ドメインの NS レコードを非再帰検索
2. 1 で得られたネームサーバ (=NS レコード) それぞれに当該ドメインの NS レコードを非再帰検索しその応答を記録
3. 2 の結果に 1 には無かった NS レコードが含まれていれば、そのネームサーバに対しても当該ドメインの NS レコードを非再帰検索しその応答を記録
4. 1 と 2,3 の結果を照合し矛盾を抽出

なお、リストに乗っているドメインの数は当初 52,014 であったが、途中 2,320 のドメインが登録削除となり、最後の調査時点では 49,694 である。途中のドメイン追加は行っていない。

2.1　Lame Server の有無

調査方法に示した手順でリストアップされたネームサーバのうち、応答が無かったものを抽出した。また、応答があっても AA(Authoritative Answer)

フラグが付いていない権威のない応答についても抽出を行った。なお、権威の無い応答は、DNS キャッシュサーバをコンテンツサーバとして運用している場合などに生ずる。これらは一般に Lame Server あるいは Lame Delegation と呼ばれ、DNS には運用上完全性が欠如していることを示しているとともに、DNS リゾルバに無駄な問い合わせを強いるものとなっている。

これら Lame Server を含むドメインの数を観測日ごとに時系列でプロットしたものが図 1 である。図 1 から Lame Server を含むドメインの数が減少していないことがわかる。

2007 年 4 月 22 日のデータでは、無応答のサーバを含むドメインが 3,196/49,694 で 6%、権威無し応答のサーバを含むドメインが 3,382/49,694 で 7%、合計 6,578/49,694 ドメイン、13% が Lame Server であった。これは、JPRS の 2003 年の調査報告 [2] での 14.2% というデータと較べても、状況が全く改善がなされていないことを意味している。

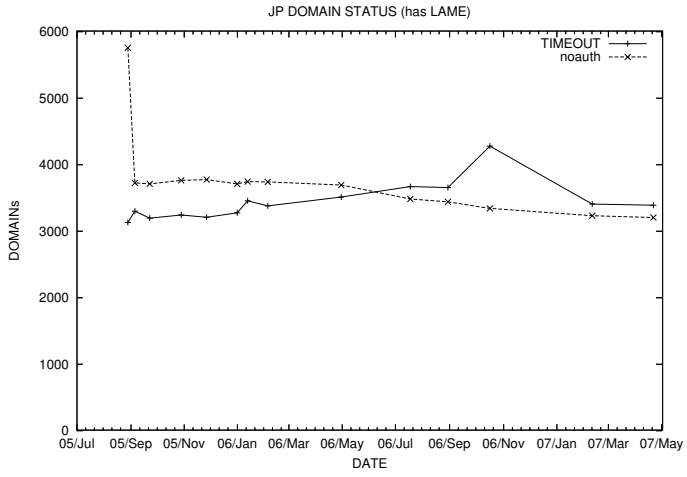

図 1　Lame Server を持つドメイン

2.2　ハイジャックの可能性

Lame Server として得られたネームサーバの中には、そのネームサーバのドメイン自体が存在しなくなっているものがある。例えば、

example.jp NS ns.example.com

example.jp NS ns.example.jp

となっているにも関わらず、ns.example.com を com に問い合わせたとき NXDOMAIN が返るようなケースである。これは最悪の場合、example.com の登録抹消後に、第三者による再取得とともに example.jp が自由に設定されうる。つまり、正規の手続きを踏んだ（しかし example.jp の所有者は気づかないままの）ドメインハイジャックが可能な状態であることを意味する。

このようにネームサーバが TLD において NXDOMAIN を返すドメインは、2007 年 4 月 22 日の時点で 87 ドメイン発見された。2005 年からの推移を図 2 に示す。

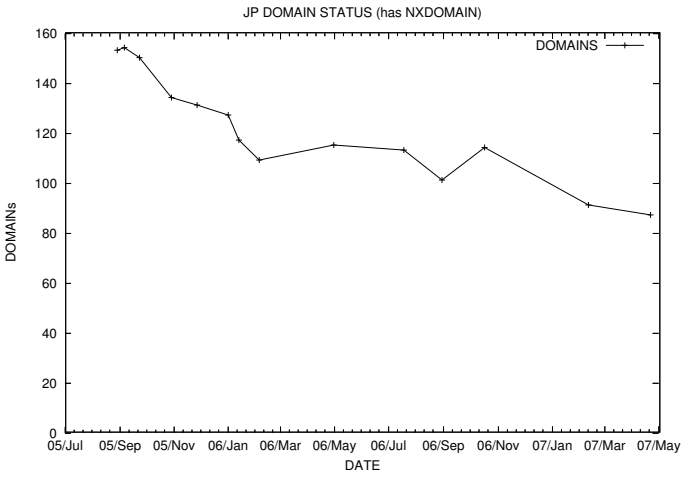

図 2　NXDOMAIN を NS に持つドメイン

2006 年 1 月から JP のレジストリである JPRS が、JP のネームサーバ内において存在しない JP ドメインのレコードを削除する行動に出てくれたため、問題のあるドメインが多少減少したが、その後、グラフは水平となり移譲先に数多く残る問題は大部分が放置されたまま推移している。なお、今年になって 2 割程度の減少傾向が見られるが理由は未調査である。

2.3　短い TTL

民田の報告 [3] が示すように、短い TTL(Time To Live) を持つ DNS レコードは、その問い合わせを行うキャッシュサーバにとって容易に偽の応答（＝毒入れ）を受け入れうる要因となる。この件の調査についてはより広範囲で詳細な民田の報告を参照されたいが、筆者の 2007 年 4 月 22 日の調査においては、110,192 の NS レコード中、600 秒以下の TTL を持つものは 7,472 レコード、7% 存在した。(民田の報告では 9%)

2.4　DDoS 対策の有無

本研究での調査対象は DNS のコンテンツサーバである。これらは DNS キャッシュサーバと兼用してはいけない。兼用すると権威あるデータと権威のないキャッシュデータが混在し、種々の問題を引き

起こす。しかしながら DNS サーバの実装として広く普及している BIND に関する解説や設定例の多くが、この間違った運用を拡大再生産し、多くの問題を引き起こしている。

従来は、権威のないデータの提示や毒入れの危険性など、影響が限定的な問題としてとらえられてきた。しかし、最近は DNS キャッシュサーバが DDoS の増幅器として用いられる危険性が大きな問題となってきており、キャッシュを兼用しているコンテンツサーバは格好の踏台になることが指摘 [4] されている。

この 2 年間の観察において、応答に RA(Recursion Available) のフラグを付けてきたネームサーバ（= キャッシュサーバである可能性大) を有するドメインの数をプロットしたものが図 3 である。技術的観点からはサーバ数（後述）をプロットすべきであるが、ここでは問題の認識を問うためにドメイン数としている。至近のデータで、33,280/49,694 ドメイン、67% がキャッシュサーバ兼用を容認しているドメインである。また、2007 年 4 月 22 日の調査では

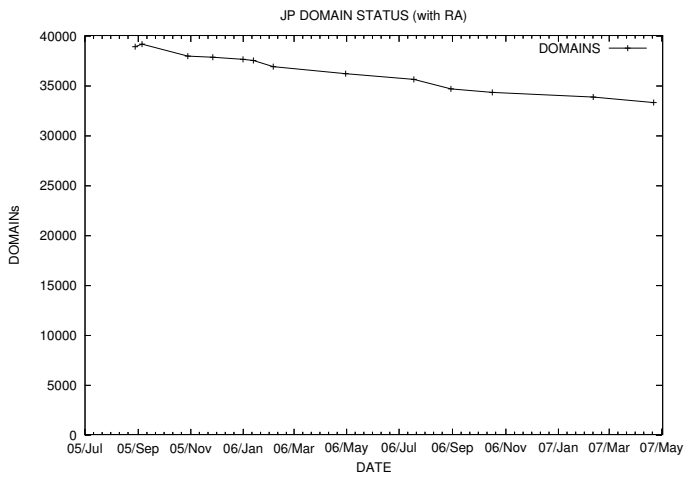

図 3　キャッシュ兼用の NS を持つドメイン

それぞれのサーバのキャッシュ応答を直接確認した。方法の詳細はセキュリティ上の観点から記述しないが、キャッシュにヒットする確率が十分高いデータを再帰検索したものであり、毒入れのような行為は行っていない。

この結果、応答／問い合わせの増幅率が 1 より大きかったサーバは、24,214 サーバ中、20,091 サーバ、つまり 83% ものコンテンツサーバが 1 を超える増幅率でキャッシュを応答する DNS amplifier (以下 DNS AMP) として機能することが判明した。

DNS AMP の増幅率は通常で 25 倍、EDNS0 で 200 倍程度まで可能であり、のべ 100Mbps 程度の問い合わせからでも少なくとも約 2.5Gbps、未調査の条件 (EDNS0 の応答) が成立すると、最大 20Gbps のトラフィックを生む計算が成り立つ。

また、AMP となるキャッシュサーバが 1 台 10Mbps のスループットを生むとすると、今回判明した 20,091 台だけでも、ボットなどからの大量の query により最大 200Gbps のトラフィックが生み出せることになる。

3　考察

本報告でわかるように DNS は壊滅寸前と言ってもいい状況にある。改善も遅々として進まない。DNS に関する正しい知識を持った技術者が、現場にはほとんどいないと見て間違いない。また基盤技術の重要性を理解し、現状を危惧できる経営者もやはりほとんどいないと見て間違いない。

DNS AMP 以外の手法も含め、DDoS の根本対策は詐称 IP アドレスをネットワーク境界でフィルターする Ingress/Egress Filter (RFC2827) しかないが、普及率は不明であるが十分な状況でないことは多くの攻撃事例が示している。

そもそもインターネットは誰もその信頼性を保証していない。個々のサイトの信頼性に依存するのみであるが、根幹の DNS がこのような状況ではインターネットをインフラとして利用することなど到底できるものではない。技術的な対策はすでに提示されている。しかし個々のサイトの管理者、利用者が問題に気づかない限りはどうにもならないのである。インターネットに対する意識が今問われている。

参考文献

[1] 鈴木常彦, “What’s VISA Problem”, 2005 http://www.e-ontap.com/summary/.

[2] DNSQC-TF, “DNSQC-TF 活動報告 (2) (「Internet Week 2003 DNS DAY」での発表資料)”, 2007 http://jprs.jp/tech/material/IW2003-DNS-DAY-dnsqc-tf-fujiwara.pdf.

[3] 民田雅人, “これでいいのか TTL - 短い DNS TTL のリスクを考える”, 2007 http://www.janog.gr.jp/meeting/janog19/files/DNS_Minda.pdf.

[4] JPRS, “DNS の再帰的な問合せを使った DDoS 攻撃の対策について”, 2007 http://jprs.jp/tech/notice/2006-03-29-dns-cache-server.html.