# Is the DNS dying?

鈴木常彦

## Ⅰ．VISA.CO.JP 問題

「こりゃまずい。とうとう削除されちゃったか…」とつぶやいたのは 5 月 18 日の真夜中でした。翌日に名古屋大学の「計算機と社会」の講義があり，そのネタの確認に DNS で VISA.CO.JP を検索してみたところ，ネームサーバ（escdns01.e-ontap.com）を引き受けていたドメイン E-ONTAP.COM が消滅していたのです。実はこのドメインを運営していた会社は数年前に解散しており，ドメインは長らく放置されていたのです。

E-ONTAP.COM が削除されたあと，誰かに再取得されて以前と同じ名前でネームサーバをあげられてしまえば，VISA.CO.JP が自由に操られてしまいます。DNS 的には正当な VISA.CO.JP のホームページを立ち上げられる可能性もあれば，VISA.CO.JP のメールを横取りされてしまう可能性[1]もあります。

深夜に一刻の猶予もないと思われる状況で，筆者はやむなく E-ONTAP.COM を取得する判断を下し，即座に手続きに入りました。そして発見から 20 分後には E-ONTAP.COM とそれに管理を委譲したままの VISA.CO.JP は私の管理の下に置かれることになったのです。そしてログから判明したのですが，visa.com.cn（VISA チャイナ），visa.com.tw（VISA 台湾），mymoneyskills.co.kr（VISA 韓国），mymoneyskills.com.hk（VISA 香港），visa.com.au（VISA オーストラリア）等，アジアのビザ・インターナショナル関連ドメインも軒並み E-ONTAP.COM の管理下にあったのです。

その後の経緯は省きますが，VISA 関連すべてのドメインの管理権限が私の E-ONTAP.COM からなくなり，とりあえずの解決をみたのは 6 月 2 日未明でした。話の詳細は http://www.e-ontap.com/ を御覧ください。

## Ⅱ．ハイジャック可能なドメイン

その後，類似の問題がないかをまず政府系のドメインから調べ始めたところ，すぐに消防庁を始めとするいくつかのドメインの問題を発見し，IPA へ報告（http://www.e-ontap.com/dns/fdma.html）を行いました。これには政府もあわてて，総務省，経産省（IPA），警察庁から注意喚起文書がだされるに至りました。JP ドメインを管理する組織（レジストリ）である株式会社日本レジストリサービス（通称 JPRS）も，6 月 26 日に「DNS サーバの不適切な管理が引き起こす

1　http://www.e-ontap.com/dns/risk.html

脅威と対策について」[2] という文書を出しました。

JPRS は 8 月から「DNS サーバの不適切な管理による危険性解消のための取り組みを開始」[3] しています。これは，ハイジャックの危険性のあるドメインを調査し，管理者に直接連絡をとるというものだそうです。ただし，調査対象は NS レコード（ドメインの管理権限のある DNS サーバ名）も JP ドメインである JP ドメインに限定されています。

さて，ここで気になるのは，ハイジャックにもつながる不適切な管理の DNS はどれくらいあるのだろうかという点です。残念ながら JPRS は数字を公表してくれません。また JP ドメインのリストは非公開となっているので網羅的調査も行えません。やむなく，あるルートで入手した 51771 ドメインのリストを調査してみました。結果は思ったとおりひどいものでした。

表 1　JP ドメイン健全性調査結果 1 ～危険なドメイン（2005.9.4）

| | | |
|---|---|---|
| DNS が存在しないドメインを NS レコードが指しているドメイン | 140 | 2.8% |
| そのうち即日ハイジャック可能なドメイン | 18 | 0.03% |

即日ハイジャック可能とは，NS レコードの指す先が .COM や .NET や汎用 JP など取得審査のないドメインを指していることで判断しました。ただし，CO.JP や GR.JP なども比較的取得は容易ですのでこの 18 ドメイン以外も安全ではありません。8 月 1 日現在，745381 の JP ドメインが存在しています。18/51771 の割合でハイジャックが可能だとすると，259 のドメインが現在ハイジャック可能な状態にあると推察されることになります。そして 140/51771 の率で考えると，実に 2016 のドメインが危険な状態にあると言えます。

## Ⅲ．ハイジャックだけが問題なのか

ICANN[4] の理事でもある Carl Auerbach が彼のブログに“Is the Internet dying?”というエッセイを書いています。スパムやワームやサーチエンジンなどのノイズが氾濫し，一方でそれらに対抗する不適切な防壁がオープンだったネットをばらばらに分断し，インターネットはもはや瀕死の状態にあるというのが彼の説です。全くそのとおりだと思います。そして不適切に管理されている DNS もまたノイズを撒き散らし，インターネットを死に追いやる手助けをしています。

表 2 に見られるように，前述の 51771 ドメインの調査において，3122（6%）のドメインが問い合わせに応答しないサーバ（Lame Server）を DNS に登録していました。Lame Server は DNS クライアントに多くの問い合わせを強要し，DNS の世界に負荷をかけます。確率的に検索も遅くなります。

驚くのは，日本でトップシェアのレジストラ（DNS 登録事業者）が顧客のセカンダリとして

2　http://jprs.co.jp/topics/050629.html

3　http://jprs.co.jp/press/050804.html

4　The Internet Corporation for Assigned Names and Numbers

提供しているサーバがLame Serverで，351ドメインが影響を受けているということがわかったことです。なぜ誰も苦情を言わないのでしょうか。

表２　JPドメイン健全性調査結果２～問題のあるドメイン（2005.9.4）

| | | |
|---|---|---|
| 応答のないサーバ（Lame Server）をNSレコードが指しているドメイン | 3209 | 6.2% |
| 単なるキャッシュサーバをNSレコードが指しているドメイン | 3471 | 6.7% |
| NSレコードが指すサーバがキャッシュサーバを兼用しているドメイン | 38781 | 75% |

調査結果を見てさらに驚くのは，単なるキャッシュサーバをネームサーバにしているドメインが6.7%もあることです。誰かが再帰検索でキャッシュを注入しないと応答を返しません。信用できない応答をする点ではLame Serverよりたちが悪いと言えるでしょう。

また，DNSサーバにBINDを使っているところが多いせいでしょうが，実に75%のドメインがコンテンツサーバとキャッシュサーバを兼用しています。権威のないデータを応答したり，場合によってはDDoSや毒入れの被害に遭うかも知れないということを知らないのでしょうか。さらに今回の調査項目にはいれていませんが，以下のような問題もよく見受けられます。

- NSレコードのTTLが異常に短い
- NSレコードがCNAMEを指している
- NSレコードがプライベートIPアドレスを指している
- glue Aレコードの IPアドレスが間違っている
- 余計なAdditional Aレコードがついている
- MXレコードがCNAMEを指している
- PTRレコードが適切に設定されていない

## Ⅳ．DNSの構造的問題

### １．技術者不在と杜撰な管理体制

こうしてみてくると，DNSのことをわかっている技術者がいかに少ないか，また技術者がいるとしてもいかに管理システムがお粗末であるかが分かるかとおもいます。問題の露見しているドメインは決して中小零細ばかりではありません。大手コンピュータメーカ，銀行，大手自動車メーカ，大手プロバイダ，政府／行政機関，大学等にも多く問題が見受けられるのは，かなり深刻な状況といわざるをえません。

DNSそのものが技術的に陳腐化しており，今日のネット社会を支えられるものでないことは明白ではあるのですが，問題を生じやすい仕様であっても，それをカバーする技術力と管理能力がもっとあってもよさそうなものなのです。しかし実態は悪い仕様をとことんまで悪く使い込んでいるようにしか見えません。

問題が表面化しないのは，リタンダンシーのおかげでしょうが，潜在的な症状の悪化に気づく能力すら技術者達が失っているからではないでしょうか。先端技術ばかり追いかけているうちに，

足元を支える技術者がいなくなっているという危機的状況にすでに陥っているような気がしてなりません。

表３　問題のあるドメインの種別（2005.9.4）

| 種　別 | 危　険 | Lame | キャッシュ |
|---|---|---|---|
| 政府系（go.jp） | 4 | 41 | 30 |
| 学術系（ac.jp） | 8 | 186 | 126 |
| 市町村（city,town,vill） | 13 | 230 | 224 |
| 企業（co.jp） | 52 | 1286 | 1422 |
| プロバイダ（ne.jp） | 12 | 213 | 196 |

## ２．インターネットガバナンスの問題

管理に問題があるのは，末端のドメインばかりではありません。そもそもレジストラ（ドメイン登録事業者）とレジストリ（TLD のデータベース /DNS を管理する事業者）が厳密な管理をしていれば多くの問題はある程度避けることができます。しかし日本の独占的レジストリである JPRS の管理する JP ドメインの DNS（[a,b,d,e,f].dns.jp）には多くの間違ったレコードが登録され，放置されています。またこれらの DNS の応答には一貫性がありません[5]。

ルートサーバにしても同様です。このことはまだ公表されていませんが，複数のトップレベルドメインに関係するネームサーバの A レコードが間違って登録されていたりします。場合によっては国レベル（トップレベルドメイン）でハイジャックに遭う可能性があるということです。

これまで，ドメインはインターネット社会における自律的組織である ICANN とドメインブローカーたちが管理してきました。しかし ICANN による管理が来年 3 月で契約が切れるのを目前にして，国連が管理すべきだ，いや米国が管理するといった議論が巻き起こり，混沌とした状況になってきています。現状の惨状をどうすればよいか，そして今後どのような管理がなされていくべきか，インターネットコミュニティの人々はもっと関心をもつべきでしょう。

本研究の一部は，文部科学省科学研究費基盤研究（A）「地域学術コンソーシアムにおける e-Learning 地域ハブに関する研究」（課題番号：15200054）の助成を受けて実地されています。

（すずき　つねひこ：中京大学情報科学部）

5　余計な Additional A レコードがついたりつかなかったりする