歴史の一幕

WIDEプロジェクト/ソニー株式会社
尾上 淳

3系列のDNS

2012年6月のWorld IPv6 Launchに合わせて、「閉域網」と「インターネット」の混在に起因する、DNSのAAAAフィルタリングが話題になっています。これで思い起こされるのは、日本のインターネットの初期、1989年から1995年まで運用されていた「3系列のDNS」といわれる設定です。

日本のネットワークがインターネットにつながり始めた1989年、DNSをどう設定すべきか数人で頭を悩ませていました。そもそもそれまでは、国内ではネームサーバは使われておらず、組織内のホストはhostsファイルをコピーしたり、NIS（Network Information Service）を使うのが一般的でした。そしてメールはモデムによるダイアルアップ接続で、UUCP（Unix to Unix Copy Protocol）を用いたバケツリレー方式で転送していたのです。ルーティングテーブルのようなメール転送ルールを、各組織の管理者がそれぞれ設定していました。

そんな中、国内の組織が専用線で接続され始め、その一部が海外と接続することで、日本にも「インターネット」がやってくることになりました。管理者の違う組織を接続するので、分散管理の仕組みとしてDNSは必須です。設定に関するドキュメントもほとんどないまま、試行錯誤を繰り返しました。当時、海外接続線はWIDEプロジェクトやTISN（Todai International Science Network：東京大学理学部国際理学ネットワーク）など、いくつかのグループが研究教育用に引いたものしかなく、それらのグループに参加していない一般の組織が使えるようなインターネット接続がまだなかったのです。そのため、海外のサイトから国内組織を検索したときには、従来通りInetClub（KDD研究所によって運用されていた国際科学技術通信網利用クラブ）による、モデム経由のメール転送が行われるようにしなければなりません。逆に、国内接続しかできない組織は、ルートDNSサーバにも到達できないので、別途国内専用のルートDNSサーバを用意する必要がありました。さらに、インターネットにも接続できる国内組織の場合は、この二つを両方見て適宜使い分けなければなりません。そうしないと、例えば国内組織あてのメールがインターネット経由で海外回りになってしまい、メールが遅延するだけでなく余分な通信費用がかかってしまうことになります。

インターネット接続のある組織からは、「せっかく専用線を引いているのだから、早くインターネット経由でメールのやり取りをしたい」と催促がきます。けれど、DNS設定としては国内接続のみの組織のことも考えないといけませんし、ネットニュース等で海外の経験者に相談しても、「インターネットとの接続性がない環境ではDNSは使えないよ」という回答しかもらえない、そんな状況でした。当時唯一のDNSソフトウェアだったBINDの設定を片っ端から試して、どうにか最小の設定コストで運用できないものかと試行錯誤してみたのです。

ようやくたどりついた解決策（というか回避策）が「3系列のDNS」と呼ばれる設定です（図）。各組織の情報として、国内向けDNSサーバ、海外向けDNSサーバをそれぞれ登録します。インターネット接続のある組織の場合は、この二つは共用できます。インターネット接続がない組織の場合は、海外向けは登録しないか、InetClubへの転送設定のみ登録することになります。そして、これら二つのレコードをマージするDNSサーバをいくつか立ち上げておいて、インターネット接続できる組織はマージサーバをforwardersとして指定するというものです。逆引きも同様に設定します。この複雑怪奇な設定を丁寧に解説したTISNの高田広章氏（当時東京大学、現在名古屋大学）の「ネームサーバとその設定について」というドキュメント（http://www.nic.ad.jp/doc/jpnic-00396.html）は、日本のDNS設定のバイブルとして長く参照されました。

ところでDNSというのは、もともとどこから検索しても同じ答えが得られて、得られた情報の解釈はクライアントが行うというのが特徴です。そのため、キャッシュした情報をそのまま使い回しても問題なく、インターネット中に管理を分散してもちゃんと動作する、奇跡の広域分散データベースと呼ばれたりするわけです。ところが3系列DNSの設定では、国内から/国外からなど問い合わせ元によって得られるべきデータが違うという、トリッキーな運用になっています。本当にこれで良いのかという不安はありました。が、他に妙案もなく、1991年にJNIC（のちのJPNIC）が誕生し、登録データベースから自動でDNSレコードを生成するようになっても、構造そのものは変化なく運用され続けていました。

そんな中、とうとう恐れていた問題が起こりました。1994年の末に、海外のサイト管理者から「突然DNSが引けなくなった。自分のところに日本のサーバがキャッシュされていて、日本のホストしか参照できない。これは意図的な設定なのか。」というメールがやってきました。意図的な設定……だったのですが、先方は実際に困っているわけです。実際にはこの問題はBINDのキャッシュ汚染バグによって発生したわけで、当時の最新バージョンでは、警告を吐くだけで汚染しないように修正されていました。しかし、日本がそのような独自の設定をしているのが直接の原因なわけですから、原因を取り除くべきだという声は強いものでした。まだ広く使われている古いBINDの実装に国内サーバの情報が紛れ込んでしまうと、DNS全体に日本のホストしか登録されていない状態になってしまう可能性もあります。さすがに影響範囲も重要性も大きすぎるだろうということで、JPNIC DNS WGの加藤朗氏（当時東京大学、現在慶應義塾大学）と高田氏が中心となり、急遽3系列の見直しを検討しました。商用のインターネットサービスも既に始まっており、ちょうどその年にJUNET協会、InetClubも終了し、インターネット接続のない国内接続のみの組織はかなり少なくなっていましたし、統合しても大きな問題はなかろう、という見込みもありました。こうして1995年5月に、5年余り運用された3系列のDNSというトリッキーな設定は幕を閉じました。

現在のDNSはセキュリティの観点から、補助情報でキャッシュが汚染されないように、DNSソフトウェアの実装にも細心の注意が払われています。またCDNを中心に、問い合わせ元に応じて、より近い位置のサーバのアドレスを返すなどの運用も一般的になっています。それでもやはり、万一情報が紛れ込んでしまっても問題が起きないようになっているだろうか、ということは気になります。ローカルハックが必要な時期はあるのですが、インターネットの大前提であるグローバルな接続性を実現する努力は、続けないといけないのだと思います。

図：3系列のDNS