DNS の運用について

加藤　朗*

2003 年 6 月 2 日

1　はじめに

IP データグラムの送達という点では、DNS はインターネットの重要な基盤とは言えないかも知れない。しかしながら、IPv4 アドレスで資源を指定するのは不便であり、IPv6 アドレスに至っては無理である。従って、名前で資源を指定し、それを解決するシステムである DNS も、インターネットにとって不可欠なサービスになっている。ここでは、UTnet における DNS の運用の問題点について述べる。

2　現状

東京大学では、従来から、u-tokyo.ac.jp というドメイン名を使用している。各部局等が u-tokyo.ac.jp のサブドメインを取得した場合、それに対して名前空間の管理が委任され、つまり、DNS 上では NS レコードおよびそれに対応する A/AAAA レコードが設定されている。

従来は、u-tokyo.ac.jp および東大で使用している主要な IPv4/IPv6 アドレスに対する逆引き zone は 3 台のサーバ ns.nc.u-tokyo.ac.jp、ns2.nc.u-tokyo.ac.jp、ns.s.u-tokyo.ac.jp によって運用されていた。これらのサーバは再帰的な問い合わせにも対応する必要があり、セキュリティ上問題になる可能性がある。そこで、authorized server と再帰的なサービスを分離することを 2002 年 9 月の UTnet Meeting で紹介した：

- ns.nc.u-tokyo.ac.jp, ns2.nc.u-tokyo.ac.jp での再帰的なサービスは継続する。
- 再帰的なサービスを提供しないサーバ群 dns1〜dns3.nc.u-tokyo.ac.jp を用意する。
- 学内の各 zone の secondary は、ns/ns2.nc.u-tokyo.ac.jp から dns1〜dns3.nc.u-tokyo.ac.jp に移行する。

すでに dns1〜dns3.nc.u-tokyo.ac.jp は稼働している。このうち、dns2.nc.u-tokyo.ac.jp に関しては、通常の UTnet とは異なったトポロジ上にあり、UTnet が外部から切断されも DNS のサービスは継続することができる。また、dns1〜dns3.nc.u-tokyo.ac.jp は IPv6 による問い合わせにも対応している。

現行の DNS の運用の問題点として、以下のような事項を挙げることができる。

1. 外部から参照される DNS サーバで再帰サービスを実施しており、セキュリティ上問題がある。
2. DNS の委任が不十分な場合や、一貫していない場合が多く見受けられる。
3. 各部局で稼働している DNS サーバには、セキュリティ上問題があるソフトウェアも多く見受けられる。

3　DNS 運用の問題点

各部局で運用中のサーバ全てに問題があるわけではないが、問題があるサーバあるいはゾーンも少なくない。いくつかの典型的な問題点を記す [1][2]：

1. DNS ソフトウェアにセキュリティ上問題があるバージョンを使用している場合が少なくない。現在、お勧めな BIND は、8.2.6、8.3.4 及び 9.2.2 である。確認には次のように dig コマンドを使用する：
   % dig @*IPaddress* version.bind chaos txt
   最新版のソフトウェアは ftp.isc.org から入手できる。

*kato@wide.ad.jp

2. NS レコードで示されたサーバが、対応するドメインのデータを保持していない場合。これを *lame delegation* というが、いろいろな問題を起こす可能性がある。NS レコードで示された DNS サーバは、必ずそのサブドメインに関する情報を保持していなければならない。
   Lame delegation の有無をチェックするには、
   `% dig @`*IPaddress domain* `soa +norec`
   を実施し、flags に “aa” が含まれるかどうかをチェックする。“aa” がない場合には、その zone を保持していないことが分かる。

3. NS レコードや MX レコードで指し示された名前が CNAME であってはいけない。別名を使いたい場合には CNAME ではなく、アドレスを直接記述する。

4. SOA の最初の引数は primary サーバの FQDN で、最後 “.” の付け忘れに注意。2 つめの引数は管理者のメールアドレスの “@” を “.” に置き換えたもので、やはり最後の “.” の付け忘れに注意。また、このアドレスに送られたメールが正しく管理者に届き、読まれているかどうかも重要になる。UTnet からの連絡は、このアドレスに行うことにしたい。

5. SOA のパラメータが好ましくない場合がある。Refresh は secondary サーバが primary サーバに対して、ゾーンの更新の有無を確認する周期で例えば 86400（1 日）、Retry は例えば 7200、Expire は primary サーバにアクセスできなくてもそのゾーンを保持する上限で 3600000（41 日）、Minimum は negative cache の値を保持する時間で例えば 172800（2 日）ぐらいが適当である。

6. 特に逆引きのゾーンで多く見受けられるのは、PTR レコードの値の最後の “.” がないレコードである。

7. CNAME とそれ以外の種類のレコードが混在している場合がある。CNAME を書いたら、他の種類のレコードを書いてはいけない。

8. ホスト名に使える文字は、A(a)–Z(z)、0–9 および “-” のみである。

4 dns1～dns3.nc.u-tokyo.ac.jp について

従来、学内の各ドメイン（逆引きを含む）の secondary は、ns/ns2.nc.u-tokyo.ac.jp でお引き受けしてきていたが、ns.nc.u-tokyo.ac.jp のみという場合も多く管理上問題があった。そのため、これらのサーバに残っているものはともかく、dns1～dns3.nc.u-tokyo.ac.jp では、一部でお引き受けするのではなく、3 台共通に運用したい。そのため、それぞれの zone は次のいずれかの体系での運用をお願いしたい：

A 各部局等で運用するサーバのみで運用。ただし、複数のサーバが指定されて、実際に運用されている必要がある。

B 各部局等で運用するサーバに加え、dns1～dns3.nc.u-tokyo.ac.jp を 3 台とも指定する。ただし、パケット長の点から、各部局等のサーバは 2 台程度にしておくのが望ましい。

C 各部局等で運用するサーバは zone ファイルに記述せず、dns1～dns3.nc.u-tokyo.ac.jp 3 台のみで運用する。この場合、zone データそのものの生成・管理は、各部局等で運用する DNS サーバでお願いしたい。このサーバは、NS レコードには指定されないが、SOA レコードの最初のパラメータには指定して頂きたい。

D 各部局等では DNS サーバは運用しない。

B・C の場合、u-tokyo.ac.jp 直下のサブドメインに限らず、学科や研究室単位のものを含めて UTnet の DNS サーバで secondary をお引き受けする。

D の場合、

- MX レコードはサブドメインに対するもの 1 つだけ
- www に対する CNAME レコードも 1 つだけ
- 残りは host*nnn* という機械的な名前に対して A レコードを 1 つづつ

という単純な zone に限定して、お引き受けすることを検討しているが、まだ実現していない。

なお、学内の多数の計算機が参照しているため、現在の ns/ns2.nc.u-tokyo.ac.jp は、移行後も引き続き再帰サービスを提供する。ただし、ns.nc.u-tokyo.ac.jp の古いアドレス 130.69.254.252 は既にサービスを停止しているので、このアドレスが resolv.conf に含まれていないことを確認されたい。

移行途中に Lame delegation が発生しない様に、綿密な調整が必要である。そのため、次のような手順でお願いしたい：

1. dns1~dns3.nc.u-tokyo.ac.jp からゾーン転送を可能にする設定をお願いする。具体的には、named.conf に次のような記述を追加されたい：

```
options {
   allow-transfer {
      130.69.0.1;
      133.11.0.1;
      157.82.0.1;
   };
};
```

2. ns/ns2.nc.u-tokyo.ac.jp からの移行、あるいは dns1~dns3.nc.u-tokyo.ac.jp の追加の準備が整ったら、nocstaff@nc.u-tokyo.ac.jp に Subject: DNS で連絡を頂きたい。その際、
   - 移行あるいは追加する zone 名の一覧
   - zone データの転送元のホスト名と IP アドレス

   を連絡して頂きたい。

3. UTnet では dns1~dns3.nc.u-tokyo.ac.jp に設定し、管理者に連絡する。

4. 連絡があった後、ゾーンファイルの NS レコードを、現在の ns.nc.u-tokyo.ac.jp 等から、dns1~dns3.nc.u-tokyo.ac.jp に変更あるいは追加する。この場合、ゾーンファイルの先頭の SOA レコードは、次のようになる：

```
$TTL 86400
@  IN SOA  primary.  admin.  (
                yyyymmddnn ; serial
                86400 ; refresh
                7200 ; retry
                3600000 ; expire
                172800 ) ; minimum
   IN NS   your-primary-server
   IN NS   your-secondary-server
   IN NS   dns1.nc.u-tokyo.ac.jp.
   IN NS   dns2.nc.u-tokyo.ac.jp.
   IN NS   dns3.nc.u-tokyo.ac.jp.
   ...
```

   設定完了後、UTnet に連絡をお願いしたい。先頭の $TTL は bind-9 を使用している場合には必須である。

5. UTnet では、ns/dns2.nc.u-tokyo.ac.jp での設定を解除する。これで移行が完了する。

5 逆引きについて

/24 より小さなアドレス割り当てに関する DNS 逆引きは、RFC2317[3] に記述されているように、CNAME を用いて空間を拡張する方法を使用している。いくつかの方法があるが、UTnet では次のような方法を用いている：

例：133.11.123.192/26 の場合

```
$ORIGIN 123.11.133.in-addr.arpa.
192 IN NS    ns1.xx.u-tokyo.ac.jp.
    IN NS    ns2.xx.u-tokyo.ac.jp.
193 IN CNAME 193.192
194 IN CNAME 194.192
    ...
255 IN CNAME 255.192
```

従って、各 zone は次のようになる：

```
$ORIGIN
192.123.11.133.in-addr.arpa.
193 IN PTR fqdn193.
194 IN PTR fqdn194.
    ...
254 IN PTR fqdn254.
```

6 Software

DNS サーバのソフトウェアには、bind-4/bind-8/bind-9 の他、`djbdns` を始めいろいろな種類がある。それぞれ特徴があるが、現在は、IPv6 でのアクセスを必要とするなら bind-9.2.2、そうでなければ bind-8.3.4 をお勧めする。

その他のバージョンの `bind` はセキュリティ上の問題があるため、使用するべきではない。 また、bind-8.4.0/bind-9.3.0 は開発途上であり、通常の運用には現在はお勧めしない (bind-9.3.0 は `A6` レコードの問い合わせをしないため、安定したら bind-9 系はすべて移行して頂きたいところであるが)。bind の設定に関しては参考文献 [4] を参照されたい。

7 `root.cache`

昨年の 11 月に、Root DNS サーバシステムの強化の一貫として、`j.root-servers.net` の IP アドレスが `192.41.0.10` から `192.58.128.30` に変更になった。bind の場合、Root DNS Server のリストは動的に生成され、`root.cache` はその際に問い合わせを行う候補を示しているに過ぎないため、そのままでも大きな問題は起らないが、この機会に `root.cache` ファイルの更新をお願いしたい。Microsoft 系の DNS サーバは `root.cache` ファイルを Root DNS Server リストとして扱っている模様であり、更新が必要である[1] 。

8 Lame delegation について

Lame delegation があると DNS の名前解決に不要な問い合わせが発生したり、また名前解決に必要以上の時間が掛り、アプリケーションがタイムアウトしてしまうことがある。そのため、IP datagram の配送には問題なくても、プラットフォームによっては `ping` の応答がないように観測されることもある。そのため、Lame delegation が発生しないように DNS を管理していくことが重要である。

そのため、

1. DNS サーバでの zone データは必ず backup を取っておく。別なサーバで cvs repository を設定し、`ssh` でアクセスするのも一案である。
2. DNS サーバの IP アドレスやホスト名は無暗に変更しない。変更する際には、前もって、そのサーバで引き受けている各 zone の管理者および UTnet に連絡して頂きたい。`ns.`*domain*`.u-tokyo.ac.jp` のような名前にするのも手であるが、`CNAME` にしてはいけない。
3. DNS サーバがクラッシュし、代替機の手配に時間が掛る場合には、直ちに UTnet に連絡して頂きたい。zone データが cache されている場合には、そのデータで暫くサービスを継続することができる。

[1] Microsoft Windows Server 2003 は未確認

9 Dynamic Update

Windows では Dynamic Update を用いて DNS の情報を登録しようとする挙動が default で enable になっている。現在の update の頻度はそれほど高くないが、特に RFC1918 アドレス (いわゆる private address) にある場合には、AS112 サーバ (`http://as112.net/`) に update メッセージを送出してしまう。そのため、特に必要がない限り、Dynamic Update を disable しておいた方がよい。

WindowsXP の場合、スタート → 接続 → すべての接続の表示、で表示されるローカルエリア接続を表示する。そしてプロパティ→ インターネットプロトコル (TCP/IP) を選択し、プロパティ→ 詳細設定 → DNS を選択したときの、“この接続のアドレスを DNS に登録する” のチェックを外せばよい。

参考文献

[1] 杜ゆづこ. こけつまろびつ UNIX 27 — DNS チェックリスト —. *Unix Magazine*, Vol. 17, No. 9, pp. 88–99, September 2002.

[2] D. Barr. Common DNS Operational and Configuration Errors. RFC1912, February 1996.

[3] H. Eidnes, G. de Groot, and P. Vixie. Classless IN-ADDR.ARPA delegation, March 1998.

[4] Paul Albitz and Cricket Liu. *DNS and BIND 4th edition*. O'Reilly, 2001.