

IP アドレス（補足）と DNS について

平成 15 年 8 月 22 日

1 グローバルアドレスとプライベートアドレス

各マシンをネットワーク上で識別するための番号である IP アドレスにはグローバルアドレスとプライベートアドレスの 2 種類がある。インターネットに直接接続されている場合、世界中で唯一の番号（インターネットの管理団体が重複しないように割り当てる）が割り振られ、この場合の IP アドレスをグローバルアドレスという。これに対し、直接外部と接続されていない研究室 LAN などの内部ネットワークでは、内部だけで通用する IP アドレスをシステム管理者が自由に割り振ることができる。この IP アドレスをプライベートアドレスという。実際には以下のようにプライベートアドレスとして使用していいアドレスの範囲が決められているので、この範囲内で自由に割り当てることができる。

（プライベートアドレスの範囲）

10.0.0.0~10.255.255.255

172.16.0.0~172.31.255.255

192.168.0.0~192.168.255.255

研究室の場合、192.168.0.? を 3 階の内部マシン、192.168.33.? を 4 階の内部マシンのプライベートアドレスとして使用している。また、外部に接続されたマシン（minako, madoka, hatsune, yoda, ami など）では、133.5.18.? というグローバルアドレスが割り当てられている。プライベートアドレスは内部ネットワークでのみ有効な IP アドレスであるため、外部と通信する際は、NAT などにより、プライベートアドレスをグローバルアドレスに変換する必要がある。

2 ドメイン

インターネット上のホストにアクセスする時には、IP アドレスによって相手のホストを指定しなければならないが、実際にはユーザが分かりやすい名前（www.db.is.kyushu-u.ac.jp など）を指定することによってアクセスを行う。www.db.is.kyushu-u.ac.jp の場合、最初の www がホスト名で、ドメイン名は、db,is,kyushu-u,ac,jp の5つのラベルがある。ドメイン名には、次の5つのドメインが含まれる。

```
db.is.kyushu-u.ac.jp
is.kyushu-u.ac.jp
kyushu-u.ac.jp
ac.jp
jp
```

これらのドメインは階層構造をなして（図1）、木構造の最上位にルートドメインがあり、ドメイン名はルートに向かうように列挙し、ラベル間を”.”で区切って記述する。

3 DNS(Domain Name System)

ホスト名にドメイン名をつけることによってネットワーク上のマシンを一意に識別することが可能であるが、このままではコンピュータが理解できないので、ホスト名とIPアドレスの変換を行う必要がある。通常はホスト名をIPアドレスに変換するテーブルは/etc/hostsに作られる。小規模なLANでは、各マシンごとにテーブルを作成して管理するといったこともできるが、ホストの更新を行う度に各マシンのテーブルを更新する必要があり、マシンの数が多いと大変である。また別の方法として、テーブルをある1つ（または少数）のマシンに作り、他のマシンはそのマシンに必要な応じて問い合わせるといった方法もあるが、インターネットなどの世界規模の膨大なホスト数をもつネットワークでは、サーバの負担が増大し、情報の管理も難しくなる。これを解決する方法として設計された方法がDNSである。DNSでは、ホスト名の管理を各ドメインごとに分散させて行うことができ、サーバマシンの負担を減らすことができる。

3.1 ネームサーバ

DNSのサービスを提供するサーバをネームサーバといい、各ドメインにはDNSサーバが置かれ、ホスト名とIPアドレスの対応関係を管理する。各DNSサーバは自分が管理しているゾーンの情報（1つ下の階層のIPアドレスとホ

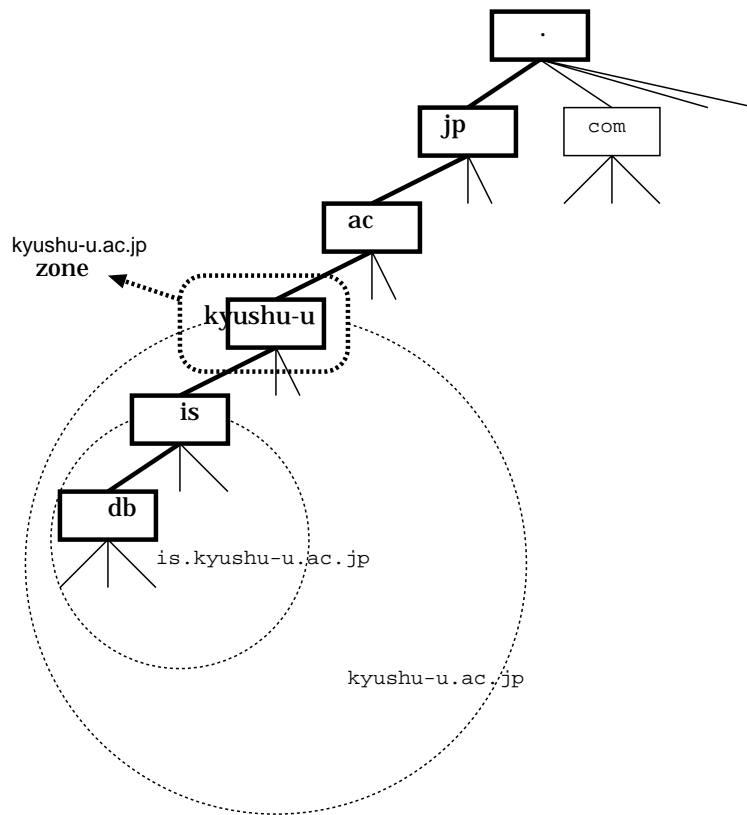


図 1: ドメインの階層構造

スト名)のみをデータベースに格納している。ネームサーバのゾーン (zone) とは、ドメイン名空間の自分が管理している情報の範囲 (図 1) を表す。牧之内研究室では、DNS サーバは `minako.db.is.kyushu-u.ac.jp` になっている。また、3 階内部では、`yoda.db.is.kyushu-u.ac.jp` (=luke.4f.db.is.kyushu-u.ac.jp)、4 階内部では `ami.db.is.kyushu-u.ac.jp` (=yumi.4f.db.is.kyushu-u.ac.jp) がそれぞれ DNS サーバとなっている。なお、「4f」とあるのは内部ネットという意味である (4 階という意味では無い)。

ネームサーバに接続してサービスを利用するクライアントをリゾルバという。リゾルバから変換要求を受けたネームサーバはまず検索対象が自分の管理しているデータベースに登録してあるか調べ、あれば、それを結果として返し、なければ、インターネット上の別のネームサーバに問い合わせを行う。ネームサーバには、プライマリサーバとセカンダリサーバがある。

- **プライマリサーバ**
属するドメインの情報を保持し、それを管理する。自分が管理している情報に対する他のネームサーバからの問い合わせに答える。通常ドメイン内には、1つのプライマリサーバが置かれる。
- **セカンダリサーバ**
プライマリサーバがダウンしたり、アクセスの集中により問い合わせに応じることができない場合にプライマリサーバの代わりとなる。情報はプライマリサーバと定期的に通信を行って、ネットワーク経由で転送される。

3.2 DNS 関連設定ファイル

DNS のサービスを提供する代表的なソフトウェアは BIND (Berkeley Internet Name Domain) である。BIND の設定ファイルは通常 `/etc` 以下に置かれる。

- **ネームサーバ (yoda,ami) の設定ファイル**

- **コンフィギュレーションファイル**

ネームサーバが起動するとき、最初に読み込まれるファイル `/etc/named.conf` というファイルにデータファイルの場所やファイル名などを記述する。

– データファイル

実際にホスト名と IP アドレスの対応を記述したファイルで、ゾーンデータファイルとリバース（逆引き）データファイルがある。

* ゾーンデータファイル

ネームサーバが管理するホストのホスト名を IP アドレスに対応させる。ホスト名 → IP アドレスの変換を正引きという。3 階の場合 yoda の /etc/namedb/4f.zone, 4 階の場合 ami の /etc/namedb/4f.zone がゾーンファイルになる。以下のように 1 行の最初にホスト名を記述し、最後に対応する IP アドレスを記述する。CNAME は別名を表す。

```
luke IN A 192.168.33.1
akari IN A 192.168.33.17
yoda IN CNAME luke
```

* 逆引きデータファイル

ネームサーバが管理するホストの IP アドレスをホスト名に対応させる。IP アドレス → ホスト名の変換を逆引きという。3 階の場合 yoda の /etc/namedb/4f.rev, 4 階の場合 ami の /etc/namedb/4f.rev が逆引きデータファイルになる。以下のように 1 行の最初に IP アドレス（ネットワーク番号は省略可）を記述し、最後にホスト名を記述する。

```
1 IN PTR luke.4f.db.is.kyushu-u.ac.jp.
17 IN PTR akari.4f.db.is.kyushu-u.ac.jp.
```

– ルートキャッシュファイル

ネームサーバはリゾルバから問い合わせを受けたときに、自分の管理しているドメインについてであれば、データファイルを調べて答えを返すが、自分が管理していないドメインについての問い合わせがあった場合、ルートキャッシュファイルを参照し、そこに書いてあるサーバに問い合わせを行う。ルートキャッシュファイルには、全世界のネームサーバを管理しているルートサーバの IP アドレスとホスト名を記述する。/etc/namedb/named.root というファイルがルートキャッシュファイルである。

- リゾルバ(各マシン)の設定ファイル

ネームサーバのサービスを利用するクライアントであるリゾルバに関しては、リゾルバとなるホストの/etc/resolv.conf というファイルで設定する。このファイルには、自分の属するドメイン名と、問い合わせを行うネームサーバの IP アドレスを指定する。ネームサーバは複数指定してすることができる。

```
domain 4f.db.is.kyushu-u.ac.jp
search 4f.db.is.kyushu-u.ac.jp db.is.kyushu-u.ac.jp
nameserver 192.168.33.1      # yoda/luke
nameserver 133.5.18.160    # minako
```

4 実習

各自のマシンの IP アドレスやホスト名は、OS をインストールした後でマシン ami,yoda の設定ファイル

(/etc/namedb/xxxx.[zone,rev])や自分のマシンの/etc/resolv.conf にすでに追加しているので設定することはないが、これらのファイルを ami や yoda にログインして確認してみる。また、自分のマシンで nslookup コマンドを使って、設定ファイルに記述してある通りに指定したホスト名から IP アドレスが得られることを確認する。minako の場合、設定ファイルは/usr/named 以下にある。