実践で学ぶ

一歩進んだサーバー構築・運用術

written by 仙石 浩明

第2回 ネーム・サーバー(前編)

ドメイン・ネーム・システム(DNS)は,インターネットの根幹を支えるシステムです。DNSを理解することはインターネット・サーバーの運用に欠かせません。連載第2回目の今回は,ネーム・サーバーの2つの種類とセキュリティに配慮したネーム・サーバーの構築について解説します。

社宅から賃貸マンションへ引っ越しました*1。社宅に4年も住んでいたので荷物の多さは覚悟していたのですが,後から後からガラクタが発掘され,引っ越し前日に徹夜をしても結局すべての荷作りは終わりませんでした。引っ越し業者の冷たい視線の中,段ボール箱にどんどんガラクタを投げ入れて,どうにか搬出完了までには大部分のこん包が済みましたが,運び損なってしまったものもかなりあり,後で社宅とマンション間を車で何往復もして運ぶ羽目に陥りました。

話をややこしくしたのは,OCNエコノミーの移転です。当初のもくろみでは,ネットワーク関係をすべて引っ越し先のマンションで再構築して,DNSの伝播*2が完了した後,現在のOCNエコノミーを解約して,引っ越ししようと思っていたのですが,OCNエコノミーは申し込みから開通まで1カ月もかかるということで,引っ越しの方が先になってしまったのです。

つまり,引っ越し作業中も社宅でサーバーを動かし続ける必要があるわけですが,部屋中に電話線やらEthernetケーブルが張り巡らせてある状態で引っ越し作業ができるはずはないので,サーバー,ルーター,TA(Terminal Adapter),電話等のネットワーク関係を部屋の片隅の半畳程度の部分に再構築し,作業中絶対にこの部分には近付かないよう*3引っ越し業者の方にお願いすることにしました*4。

ところが,半畳程度の部分と言っても元々狭い部屋ですからそんなスペースはありません。スペースを作るにはまず食器棚を移動する必要があるのですが,それには食器をこん包しなければなりません。しかし食器をこん包してしまっては生活できませんから,この作業は引っ越し前日に行うほかありません。

問題はもう1つありました。電話線がたんす等の重量物の裏を通っていて,しかもたんすで隠れている部分で壁にしっかり固定してあったので,たんすを動かさない限りは電話線の張り直しができなかったのです。結局,電話線を(ショートしないよう気を付けながら)切断して,はんだでつなぎ直すはめに陥りました*5。

大変なドメイン登録

引っ越し先でOCNエコノミーが開通したら,次に問題になるのはドメイン登録業者*6への変更申請です。GCD*7の場合,多数のドメインを収容していますから,申請を出すだけでも結構大変です。さらに今回の場合,引っ越し元の社宅の明け渡し期限があるのですが,ドメイン登録業者によっては変更が完了するまで数日かかる*8ので,期限までに変更が完了できるのかドキドキします。

私の場合は,既に登録済のドメインの情報

＊1 家賃が約10倍になりましたので,果たして生活できるのか心配です。
＊2 IPアドレス等のネーム・サーバーのデータの変更がインターネット全体に伝わること。通常1日程度で完了しますが,確実を期すには1週間程度必要です。
＊3 サーバーのスイッチに触れるだけで電源が落ちてしまうので要注意なのです。
＊4 サーバーが落ちること無く搬出が無事完了して,ほっとしていたら引っ越し業者が社宅を出るときブレーカを落とそうとしたので焦りました。
＊5 こんなことやってるから,徹夜してもこん包作業が終わらなかったのでしょうね。
＊6 例えば*.jpはJPNIC,*.com,*.org,*.netはNetwork Solutions, Inc.等。
＊7 前回説明したように,OCNエコノミーの費用の一部を賄うため,会員を募って作った任意団体のことです。GCDはGreatest Common Divisor(最大公約数)の略です。はるか昔,私がNIFTY-Serve(現,@nifty)の会員だったころの私のハンドルに由来します。
＊8 JPNICの場合,申請がDNSへ反映されるまで約1日,Network Solutions, Inc.の場合で4〜5日かかるようです。

を変更したのですが，これから常時接続しようとする人の場合は，ドメイン登録業者に新規ドメインの登録依頼をすることになります。いずれにせよドメイン登録業者に申請を行う必要があるわけですから，まずこのドメイン登録について説明しましょう。

ドメイン・ネーム・システム（DNS）

ドメイン登録業者が何をするのか理解するには，まずDNS（ドメイン・ネーム・システム）を理解する必要があります。DNSはインターネット全体に分散するデータベース・システムで，ドメイン名やホスト名からIPアドレスなどを検索したり，逆にIPアドレスからホスト名を検索したりすることができます。例えば，ホスト名「ns.gcd.org」のIPアドレスを調べたい場合は，nslookupコマンドを実行すると，「210.145.125.162」であることが分かります（**図1**）。では，nslookupはどうやってIPアドレスを調べたのでしょうか?

nslookupは，まず/etc/resolv.confファイルに書いてあるネーム・サーバーへ問い合わせます。私のマシン（asao.gcd.org）の/etc/resolv.confは**図2**のようになっています。

「nameserver 0.0.0.0」と書いてあるので，nslookupはまずnslookupが実行されたマシン（asao.gcd.org）上のネーム・サーバーへ問い合わせます。問い合わせを受けたネーム・サーバーの動作には以下の2つの場合があります。

(1)ネーム・サーバーがns.gcd.orgのIPアドレスを知っている場合，知っているIPアドレスをnslookupへ返します。

(2)ネーム・サーバーがns.gcd.orgのIPアドレスを知らない場合，他のネーム・サーバーへ問い合わせ，回答が返ってきたらそれをnslookupへ返します。

今回の場合，asao.gcd.org上のネーム・サーバーはgcd.orgドメインのすべてのホスト名のIPアドレスを知っていますから，(1)の場合に該当します。単に知っているIPアドレスをそのまま返すだけですから，単純ですね。では知らない場合はどうなるでしょうか。例えば，**図3**の例のように知らないホスト名への問い合わせがあると，ネーム・サーバーは他のネー

```
% nslookup ns.gcd.org. ↵
Server:  asao.gcd.org
Address:  0.0.0.0

Name:    ns.gcd.org
Address:  210.145.125.162
```

↵このマークで改行

図1　nslookupコマンドでネーム・サーバーへ問い合わせ
ネーム・サーバーへの問い合わせを行うコマンドがnslookupです。

```
search gcd.org
nameserver 0.0.0.0
nameserver 203.139.160.74
```

図2　/etc/resolv.confの設定
/etc/resolv.confファイルで使用するネーム・サーバーを指定します。

```
% nslookup dns.cybird.ne.jp. ↵
Server:  asao.gcd.org
Address:  0.0.0.0

Name:    dns.cybird.ne.jp
Address:  210.156.250.253
```

図3　他のネーム・サーバーへの問い合わせ
自分の知らない情報を他のネーム・サーバーに問い合わせて解決している例です。

```
% nslookup -q=ns . ↵
Server:  asao.gcd.org
Address:  0.0.0.0

Non-authoritative answer:
(root)     nameserver = L.ROOT-SERVERS.NET
(root)     nameserver = M.ROOT-SERVERS.NET
(root)     nameserver = I.ROOT-SERVERS.NET
(root)     nameserver = E.ROOT-SERVERS.NET
(root)     nameserver = D.ROOT-SERVERS.NET
(root)     nameserver = A.ROOT-SERVERS.NET
(root)     nameserver = H.ROOT-SERVERS.NET
(root)     nameserver = C.ROOT-SERVERS.NET
(root)     nameserver = G.ROOT-SERVERS.NET
(root)     nameserver = F.ROOT-SERVERS.NET
(root)     nameserver = B.ROOT-SERVERS.NET
(root)     nameserver = J.ROOT-SERVERS.NET
(root)     nameserver = K.ROOT-SERVERS.NET

Authoritative answers can be found from:
L.ROOT-SERVERS.NET      internet address = 198.32.64.12
M.ROOT-SERVERS.NET      internet address = 202.12.27.33
I.ROOT-SERVERS.NET      internet address = 192.36.148.17
E.ROOT-SERVERS.NET      internet address = 192.203.230.10
D.ROOT-SERVERS.NET      internet address = 128.8.10.90
A.ROOT-SERVERS.NET      internet address = 198.41.0.4
H.ROOT-SERVERS.NET      internet address = 128.63.2.53
C.ROOT-SERVERS.NET      internet address = 192.33.4.12
G.ROOT-SERVERS.NET      internet address = 192.112.36.4
F.ROOT-SERVERS.NET      internet address = 192.5.5.241
B.ROOT-SERVERS.NET      internet address = 128.9.0.107
J.ROOT-SERVERS.NET      internet address = 198.41.0.10
K.ROOT-SERVERS.NET      internet address = 193.0.14.129
```

図4　nslookupコマンドでルート・サーバーの一覧を得る
ルート・サーバーは，インターネットでのDNS情報の問い合わせ窓口です。

ム・サーバーへ問い合わせるのですが，やみくもに問い合わせても回答が得られるとは限りません*9。そこで，最初に問い合わせるべきネーム・サーバーが決まっています。この，最初の窓口的ネーム・サーバーのことを，ルート（root）・サーバー*10と呼びます。

ルート・サーバー

ルート・サーバーの一覧を得るには，**図4**のようにnslookupを実行します。実行結果のうち，a.root-servers.netからm.root-servers.netまでの13個のネーム・サーバーがルート・サーバーです。ルート・サーバーは全世界からの問い合わせに迅速に回答できるように，13個もあって，それぞれインターネットの要所に配置されています。

試しに，m.root-servers.net（日本に配置されています）に対して問い合わせてみましょう。問い合わせ先を設定するにはnslookupの会話モード（「>」のプロンプト）で「server サーバー名」と指定します。問い合わせを行うと，このルート・サーバーは**図5**のように返事をします。つまり，ルート・サーバーは「dns.cybird.ne.jpのIPアドレスなんて知らないけど，*.jpだったらdns0.spin.ad.jpなどのネーム・サーバーに問い合わせてみては」と言っているわけです。

インターネットに接続しているホストの数は極めて多く，ルート・サーバーがインターネットの全ホストのIPアドレスを記憶することは到底不可能です。そこで，ドメインごとに他のネーム・サーバーへ管理権限を委譲しています（**図6**）。この例で言えば，末尾がjpで終わるドメインの管理を「dns0.spin.ad.jp」などへ委譲しているわけです。

というわけで，dns0.spin.ad.jpに問い合わせてみましょう。nslookupコマンドの会話モードで続けて**図7**のように入力します。結果を

*9　下手な鉄砲数打ちゃあたる式で問い合わせまくられたら迷惑ですね。
*10　世の中には，ルート（route）・サーバーというのもあるので，カタカナで書くと紛らわしいです。

```
% nslookup ⏎
Default Server:  asao.gcd.org
Address:  0.0.0.0

> server m.root-servers.net ⏎
Default Server:  m.root-servers.net
Address:  202.12.27.33

> dns.cybird.ne.jp. ⏎
Server:  m.root-servers.net
Address:  202.12.27.33

Name:    dns.cybird.ne.jp
Served by:
- DNS0.SPIN.AD.JP
    165.76.0.98
      JP
- NS-JP.SINET.AD.JP
    150.100.2.3
      JP
- NS.WIDE.AD.JP
    203.178.136.63
      JP
- NS0.IIJ.AD.JP
    202.232.2.34
      JP
- NS0.NIC.AD.JP
    202.12.30.131
      JP
- NS-JP.NTT.NET
    210.175.162.226
      JP
```

図5　ルート・サーバーへの問い合わせ
ネーム・サーバーを指定して問い合わせを行うには，nslookupコマンドの会話モードを利用します。

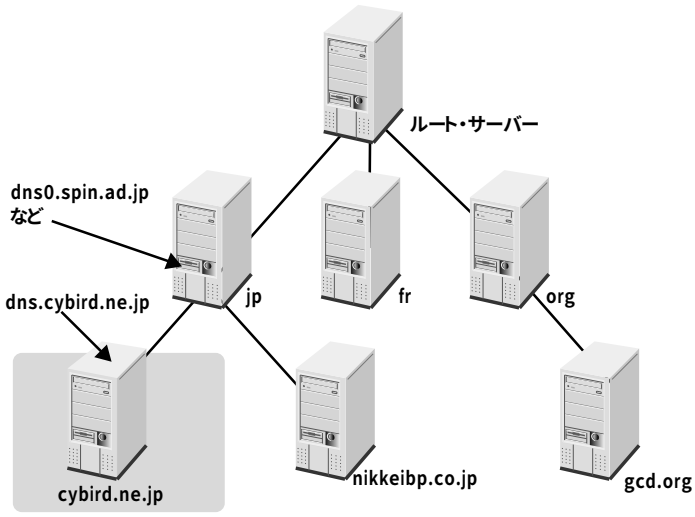

図6　ネーム・サーバーの管理権限委譲モデル
管理権限を委譲されたネーム・サーバーは，そのドメイン内の情報について責任を持ちます。

```
> server dns0.spin.ad.jp ⏎
Default Server:  dns0.spin.ad.jp
Address:  165.76.0.98

> dns.cybird.ne.jp.
Server:  dns0.spin.ad.jp
Address:  165.76.0.98

Non-authoritative answer:
Name:    dns.cybird.ne.jp
Address:  210.156.250.253
```

図7　目的のIPアドレスが得られる
管理権限を持つネーム・サーバーへの問い合わせで，目的の情報が得られました。

見ると分かるように，めでたくdns.cybird.ne.jpのIPアドレス「210.156.250.253」が得られました。ここで，回答の前に「Non-authoritative answer:」と出力されていることに注意してください。直訳すれば「信頼すべき筋からの回答ではない」という意味になります。

信頼すべき筋

これは，dns0.spin.ad.jpが以前dns.cybird.ne.jpのIPアドレスを他のネーム・サーバーに問い合わせたことがあって，その時の結果を覚えていたので，（新たに問い合わせすることなく）覚えていた内容をそのまま返した，ということを意味します。もしかするとこの瞬間にはdns.cybird.ne.jpのIPアドレスが変化しているかも知れないので，信頼できる回答ではない，と言っているわけです。

このような，一度問い合わせたときの結果を覚えておく仕掛けを一般に「キャッシュ」と呼びますが，キャッシュによってDNSは特定のネーム・サーバーに負荷が集中することを防いでいます。キャッシュされた情報だというだけの意味ですから，信頼すべき筋からの回答ではなくても全く問題はありませんが，ここでは実験として信頼すべき筋（ネーム・サーバー）を調べてみましょう。それには検索対象をネーム・サーバーに設定して（set type=ns），問い合わせます（**図8**）。

「Authoritative answers can be found from: cybird.ne.jp」という出力が得られています。これを直訳すれば「信頼すべき回答はcybird.ne.jpのネーム・サーバーから得られる」となります。

そこでまずは，cybird.ne.jpのネーム・サーバーを調べましょう（**図9**）。またもや「Non-authoritative answer:」という答えですが，信頼すべき筋が「dns.cybird.ne.jp」と「ns.ipro.ad.jp」であることが分かりました。つまり，dns0.spin.ad.jpはcybird.ne.jpドメインに関する管理権限を，「dns.cybird.ne.jp」と「ns.ipro.ad.jp」に委譲しているわけです。

権限を持つネーム・サーバーが分かったので，検索対象をIPアドレスに戻して（set type=a），dns.cybird.ne.jpに問い合わせてみます（**図10**）[*11]。これで，めでたく信頼すべき情報「210.156.250.253」が得られました。

さて，DNSの仕掛けが一通り分かったところで，ドメイン登録業者の話に戻ります。ドメイン登録業者が何をするかというと，一言で言えばドメインの管理権限を委譲してくれるのです。

例えば私がgcd.orgドメインを登録するときは，まずgcd.orgドメインに関する問い合わせに答えることができるネーム・サーバーを立ち上げます。そしてネーム・サーバーのホスト名（ns.gcd.org）とIPアドレス（210.145.125.162）をドメイン登録業者へ申請します。

するとドメイン登録業者は，gcd.orgドメインに関する管理権限をns.gcd.orgへ委譲してくれるのです。この結果，ルート・サーバーにgcd.orgに関する問い合わせが届くと，管理権限委譲の連鎖をたどって最終的にns.gcd.orgに対して問い合わせが行われます。

逆に言えばルート・サーバーと管理権限委譲の連鎖によってつながっていなくてもよいの

```
> set type=ns ↵
> dns.cybird.ne.jp. ↵
Server:  dns0.spin.ad.jp
Address:  165.76.0.98

Authoritative answers can be found from:
cybird.ne.jp
        origin = dns.cybird.ne.jp
        mail addr = root.dns.cybird.ne.jp
        serial = 20000126
        refresh = 1800 (30M)
        retry   = 900 (15M)
        expire  = 3600000 (5w6d16h)
        minimum ttl = 1800 (30M)
```

図8　信頼できるネーム・サーバーの検索
どのネーム・サーバーから信頼できる回答が得られるのかを調べています。

```
> cybird.ne.jp. ↵
Server:  dns0.spin.ad.jp
Address:  165.76.0.98

Non-authoritative answer:
cybird.ne.jp     nameserver = dns.cybird.ne.jp
cybird.ne.jp     nameserver = ns.ipro.ad.jp

Authoritative answers can be found from:
dns.cybird.ne.jp internet address = 210.156.250.253
ns.ipro.ad.jp            internet address = 203.179.10.4
```

図9　cybird.ne.jpのネーム・サーバーを調査
dns0.spin.ad.jpはcybird.ne.jpドメインに関する管理権限を，「dns.cybird.ne.jp」と「ns.ipro.ad.jp」に委譲しています。

```
> set type=a ↵
> server dns.cybird.ne.jp. ↵
Default Server:  dns.cybird.ne.jp
Address:  210.156.250.253

> dns.cybird.ne.jp. ↵
Server:  dns.cybird.ne.jp
Address:  210.156.250.253

Name:    dns.cybird.ne.jp
Address:  210.156.250.253
```

図10　信頼すべき情報の入手
権限を持つネーム・サーバーから，信頼すべき情報「210.156.250.253」が得られました。

*11　dns.cybird.ne.jpのIPアドレスを，当のdns.cybird.ne.jpに問い合わせているのですから，ちょっと間抜けな話ですね。これもひとえに「信頼すべき情報」を得るためです。
*12　alternic.netのように組織をこえて利用可能な独自ルート・サーバーもありました。

なら，ドメイン登録業者に申請する必要はありません。組織内で独自のルート・サーバー*12を立ち上げる場合などがこれに当たります。

とは言っても，ドメイン登録業者への申請は，Webで簡単にできますから，常時接続環境を持っていて，独自ドメインをまだ持っていない人はぜひ申請してみて下さい。大抵の業者が，ネーム・サーバーのホスト名とIPアドレス，それに管理者の名前とメール・アドレスと住所・電話番号をWebで送信するだけで済みます*13。

つい先日，新興のドメイン登録業者*14を使ってsengoku.orgドメインを取得してみたのですが，初めて利用したにもかかわらず，申請完了まで数分*15しかかかりませんでした。

ネーム・サーバーの2つのタイプ

さて，ドメイン・ネーム・システムの仕掛けを一通り紹介しましたが，ネーム・サーバーには2つのタイプがあることに気付かれましたか。

1つは/etc/resolv.confに登録できるネーム・サーバーで，nslookup等のクライアントから問い合わせがあると，他のネーム・サーバーに問い合わせて結果をクライアントへ返してくれるタイプです。

もう1つは，答えを知っている問い合わせに対しては答えてくれるけれど，知らない場合は，どこどこへ聞けと冷たく言い放つタイプです。このタイプは自分から他のネーム・サーバーへ問い合わせようとはしません。問い合わせませんから結果を覚えておくためのキャッシュも必要ありません。前述した例で言えば，ルート・サーバーがこのタイプに当たります。

ここでは便宜上，前者のタイプをクライアント型ネーム・サーバー，後者をサーバー専業型ネーム・サーバーと呼ぶことにします。

常時接続環境で独自のドメインを持とうとするとき，どちらのタイプのネーム・サーバーを立ち上げるべきでしょうか。クライアント型ネーム・サーバーもネーム・サーバーですから，答えを知っている問い合わせに対しては答えてくれます。つまりサーバー専業型ネーム・サーバーの動作を完全に含んでいます。したがってクライアント型ネーム・サーバーを立ち上げておけば間違い無いように思われます。実際，ネーム・サーバーに関する記事等では，クライアント型ネーム・サーバーの立ち上げ方法しか解説していないものがほとんどです。

ところが，セキュリティの観点から言うと，クライアント型ネーム・サーバーはあまり好ましいものではありません。クライアント型ネーム・サーバーは，他のネーム・サーバーに問い合わせた時に得られた結果をキャッシュに記憶しますが，問い合わせ先のネーム・サーバーが間違った結果を返したらどうなるでしょうか。

そうなると間違ったデータをキャッシュに記憶してしまい，同様の問い合わせがあると，その間違ったデータを返してしまうようになります。実際，故意に間違ったデータを送りつけ

＊13　クレジット・カードを持っていれば支払いまでWebでできます。残念ながら*.jpドメインの登録を行うJPNICは，あまり簡単ではありません。ドメイン登録にあたって印鑑登録証明書などの身元を証明する書類が必要になります。しかも登録料をJPNICへ直接支払うことはできず，JPNIC会員が代行して支払う仕組みになっています。

＊14　CSL GmbH（http://joker.com/）を利用しました。CSL GmbHは，正確に言うと登録業者というよりは，CORE（Internet COuncil of REgistrars）の再販業者です。年間登録料が12ユーロと，Network Solutions Inc. のような老舗のドメイン登録業者（年間35米ドル）と比べると大変安くなっています。ちなみにJPNICは，NTT（JPNIC会員）経由で支払う場合で年間5000円です。

＊15　約款を熟読する場合は，もう少し必要かも知れません。

```
asao:/home/sengoku % nslookup mucho.gcd.org. ↵
Server:  asao.gcd.org
Address:  0.0.0.0

Name:    mucho.gcd.org
Address:  210.145.125.161

asao:/home/sengoku % nslookup 210.145.125.161 ↵
Server:  asao.gcd.org
Address:  0.0.0.0

Name:    mucho.gcd.org
Address:  210.145.125.161
Aliases:  161.125.145.210.in-addr.arpa
```

(a)

```
cabernet:/home/sengoku % nslookup mucho.gcd.org. ↵
Server:  merlot.cybird.co.jp
Address:  10.0.0.6

*** merlot.cybird.co.jp can't find mucho.gcd.org.:
Non-existent host/domain

cabernet:/home/sengoku % nslookup 210.145.125.161 ↵
Server:  merlot.cybird.co.jp
Address:  10.0.0.6

*** merlot.cybird.co.jp can't find 210.145.125.161:
Non-existent host/domain

cabernet:/home/sengoku % nslookup www.gcd.org. ↵
Server:  merlot.cybird.co.jp
Address:  10.0.0.6

Name:    asao.gcd.org
Address:  210.145.125.162
Aliases:  www.gcd.org
```

(b)

図11　内部からのみDNS情報を得られる
GCD内部では，mucho.gcd.orgというホスト名を引くことができる（a）。しかし外部からは，mucho.gcd.orgに関する情報は得られないようになっています（b）。

ておいて，ホスト名を詐称する攻撃方法が知られています。

また，クライアント型ネーム・サーバーは，ドメインに関する問い合わせを受け取ると，そのドメインのネーム・サーバーに対して問い合わせることになり，いわば外部からの要求の「言いなり」になっています。攻撃者側から見ると攻撃のための便利な道具と言えます。

いずれにせよ，クライアント型ネーム・サーバーは，サーバー専業型ネーム・サーバーに比べると，問い合わせを行う分動作が複雑ですから，セキュリティ・ホールが入り込む余地が多いわけです。サーバー専業型ネーム・サーバーで十分であればクライアント型ネーム・サーバーを立ち上げるべきではありません。

では，クライアント型ネーム・サーバーが必要となるのはどんな場合でしょうか。それはnslookupをはじめとするクライアントが直接問い合わせる可能性があるネーム・サーバーということになります。つまり/etc/resolv.confやWindows98等の「DNS設定」に登録するネーム・サーバーは，クライアント型ネーム・サーバーでなければなりません。つまり組織内部で使うネーム・サーバーです。プロバイダがユーザーに対して提供するネーム・サーバーも，クライアント型ネーム・サーバーです。クライアント型ネーム・サーバーは，先ほど紹介したような攻撃から守るために，組織外部から勝手にアクセスされないよう，ファイアウオール等で守っておく必要があります。

一方，組織外部からの問い合わせに対しては，自組織に関する問い合わせに対してだけ答えれば十分ですから，サーバー専業型ネーム・サーバーで構わないことになります。第三者のドメインに関する問い合わせに対しては「知らない」と突っぱねればいいのです。余計なサービスをしてセキュリティを犠牲にすべきではありません。

まとめると，組織内部で使うためにクライアント型ネーム・サーバーを立ち上げ，組織外部に対しては，サーバー専業型ネーム・サーバーを立ち上げるようにすれば良いことになります。

このように，内部と外部，それぞれに対してネーム・サーバーを立ち上げると，組織外部に公開したくないホスト名をいんぺい（隠蔽）できる，というメリットもあります。

例えばGCD内部では，mucho.gcd.orgというホスト名を引くことができますし，逆にIPアドレス210.145.125.161からmucho.gcd.orgを得ることもできます（**図11(a)**）。

しかし，mucho.gcd.orgは外部からアクセスする必要が全く無いマシンです[*16]。したがって外部向けのネーム・サーバーには登録してありません。このため，GCDの外部（以下の例ではcybird.co.jp）では，mucho.gcd.orgを引くことはできませんし，逆にIPアドレスから引くこともできません。もちろん外部に公開しているwww.gcd.orgならば検索できます（**図11(b)**）。

組織外部向けと内部向けの2つのIPアドレスを持っているマシンの場合，外部向けネーム・サーバーと内部向けのネーム・サーバーに異なるIPアドレスを付けることもできます。例えば，asao.gcd.orgはGCD内部と外部ではIPアドレスが異なります。内部ではプライベート・アドレス192.168.1.1（**図12(a)**）ですが，外部から見ると，グローバル・アドレス210.145.125.162（**図12(b)**）です。

＊　　＊　　＊

次回は，今回の内容を踏まえて，ネーム・サーバーの実際の構築法を紹介します。連載第1回で紹介したように，GCDのゲートウエイはマシン1台だけで，しかもNICは1枚しかありません。このゲートウエイでGCDの内部向けと外部向けのネーム・サーバーを立ち上げ，しかもセキュリティに配慮した構築法を解説します。

＊16　外部からのアクセスは一切禁止しています。

```
asao:/home/sengoku % nslookup asao.gcd.org. ↵
Server:  asao.gcd.org
Address:  0.0.0.0

Name:    asao.gcd.org
Address:  192.168.1.1

asao:/home/sengoku % nslookup 192.168.1.1 ↵
Server:  asao.gcd.org
Address:  0.0.0.0

Name:    asao.gcd.org
Address:  192.168.1.1
```

(a)

```
cabernet:/home/sengoku % nslookup asao.gcd.org. ↵
Server:  merlot.cybird.co.jp
Address:  10.0.0.6

Name:    asao.gcd.org
Address:  210.145.125.162

cabernet:/home/sengoku % nslookup 210.145.125.162 ↵
Server:  merlot.cybird.co.jp
Address:  10.0.0.6

Name:    asao.gcd.org
Address:  210.145.125.162
Aliases:  162.125.145.210.in-addr.arpa
```

(b)

図12　内部と外部とでIPアドレスが違うホストも設定可能
内部ではプライベート・アドレス(a)，外部ではグローバル・アドレス(b)を持つホストの例です。