DNS設定駆け込み寺

勘所をしっかり押さえる

第3回

馬場達也

DNSは、インターネットでアプリケーションを使用する場合になくてはならない重要なシステムである。しかし、DNSの運用は難しいため、取り扱いに苦労している管理者も多いことだろう。ここでは、実際にネームサーバ(DNSサーバ)を運用する際に生じるさまざまな疑問に答え、管理者がスムーズにDNSを運用するためのテクニックを紹介する。

Q11 BINDのバージョンを知られないようにしたい

ネームサーバのバージョンが知られると、不正アクセスのためのヒントとして利用されてしまう。これを防ぐために、外部にはネームサーバのバージョンを知られないようにしたい。

A BINDの機能を使用してバージョン情報を隠す

BINDのバージョン番号は攻撃材料を与えることにもなる

BINDでは、デフォルトの状態でサーバを立ち上げると、外部からBINDのバージョンを取得できる。バージョンを知られると、そのネームサーバにどのようなセキュリティホールがあるのかがわかってしまうため、不正アクセスのためのヒントとして利用されてしまう可能性がある。そのような危険を回避するには、BINDのバージョンを知られないようにするのが得策だ。

最初に、BINDのバージョンを取得する方法を紹介しよう。BINDのバージョンを取得するには、ネームサーバに対して、QCLASSとして「CH」、QTYPEとして「T

```
$ dig @192.168.0.2 version.bind. txt chaos

; <<>> DiG 9.2.1 <<>> @192.168.0.2 version.bind. txt chaos
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58996
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.2.1"

;; Query time: 1 msec
;; SERVER: 192.168.0.2#53(192.168.0.2)
;; WHEN: Thu Aug  7 00:15:57 2003
;; MSG SIZE  rcvd: 48
```

BIND 9.2.1を使用していることがわかる

リスト1● digコマンドを使用してBINDのバージョンを取得する

XT」、ドメインとして「version.bind.」を指定して問い合わせを行えばよい。digを使用する場合は、リスト1のようなコマンドを発行する。すると、TXTレコードのデータとしてBINDのバージョンが返ってくる。リスト1の回答からは、問い合わせ先のネームサーバがBIND 9.2.1を利用していることがわかる。

BINDのバージョンを隠すように設定する

BIND 8.2以降では、バージョンの問い合わせを受けてもバージョンを返さないようにするための機能が用意されている。これは、BINDの設定ファイルである「named.conf」ファイルのoptionsステートメント内において「version」サブステートメントを設定することで実現できる。versionサブステートメントでは、バージョンの問い合わせを受けた場合にバージョンの代わりに返答する文字列を指定する。例えば、リスト2のようにversionサブステートメントを設定すると、バージョンの問い合わせを受けた場合に、空のTXTレコードが返るようになる(リスト3)。

このように、versionサブステートメントを使用することによって、BINDのバージョンを隠すことができるようになる。ただし、バージョンを隠すことはできても、この機能を実装しているBIND 8.2以降を使用しているということだけは相手側にわかってしまうので注意しよう。

問い合わせ元によって返答を変えることも可能

また、内部のホストにはバージョンを知らせたいが、外部のホストにはバージョンを知らせたくないという場

```
options {
        version "";
        directory "/var/named/";
};
```

リスト2● versionサブステートメントの設定例。バージョンの問い合わせを受けた際に空のTXTレコードを返す

```
$ dig @192.168.0.2 version.bind. txt chaos

; <<>> DiG 9.2.1 <<>> @192.168.0.2 version.bind. txt chaos
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53671
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     ""

;; Query time: 2 msec
;; SERVER: 192.168.0.2#53(192.168.0.2)
;; WHEN: Thu Aug  7 00:25:28 2003
;; MSG SIZE  rcvd: 43
```

リスト3● versionサブステートメントを設定した場合のバージョンの問い合わせ結果。返されたTXTレコードが空であることがわかる

合もある。この場合には、BINDのビュー機能を使用すればよい。

まず、「named.conf」ファイルの中で、リスト4のようにインターネットクラスのビュー（リスト4では「internet」というビュー名で定義）とカオスネットクラスのビュー（リスト4では「chaosnet」というビュー名で定義）のそれぞれを記述し、通常のゾーンをインターネットクラスのビューの中で定義する。そして、「bindゾーン」をカオスネットクラスのビューの中で定義し、「allow-query」サブステートメントを使用して、内部ホスト以外からの問い合わせを受け付けないように設定する。このbindゾーンのゾーンデータファイルは、リスト5のように設定する。

すると、内部ホストからバージョンを問い合わせた場合は、リスト6のようにbindゾーンで記述したバージョン文字列が返されるが、外部ホストから問い合わせた場合は、リスト7のようにバージョン文字列が返されずに「REFUSED」エラーが返されるようになる。

```
options {
        directory "/var/named/";
};

view internet in {                                          インターネットクラスのビューを定義

        [通常のゾーンを定義する]

};

view chaosnet chaos {                                       カオスネットクラスのビューを定義

        zone "bind" {                                       bindゾーンを定義
                type master;
                file "bind.zone";
                allow-query { 192.168.0.0/24; };            バージョンを返答する内部アドレスを定義
        };

};
```

リスト4● カオスネットクラスのビューの記述例。内部ホスト以外からの問い合わせを受け付けないように設定する

```
$TTL 86400
@       CH      SOA     ns1.example.com.  hostmaster.example.com. (
                                2003081000 ; シリアル番号
                                28800      ; リフレッシュ間隔（秒）
                                7200       ; リトライ間隔（秒）
                                604800     ; ゾーンの有効期間（秒）
                                3600       ; ネガティブキャッシュの有効期間（秒）
                        )
        CH      NS      ns1.example.com.
version CH      TXT     "9.2.1"                             返答するバージョン文字列を記述
```

リスト5● bindゾーンのゾーンデータファイル（bind.zone）の記述例。問い合わせに対して返答するバージョン番号が指定されている

```
$ dig @192.168.0.2 version.bind. txt chaos

; <<>> DiG 9.2.1 <<>> @192.168.0.2 version.bind. txt chaos
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36036
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           86400   CH      TXT     "9.2.1"  ← バージョン番号が返される

;; AUTHORITY SECTION:
bind.                   86400   CH      NS      ns1.example.com.

;; Query time: 1 msec
;; SERVER: 192.168.0.2#53(192.168.0.2)
;; WHEN: Thu Aug  7 00:38:46 2003
;; MSG SIZE  rcvd: 83
```

リスト6● 内部ホストからバージョンを問い合わせた場合にはバージョン文字列が返される

```
$ dig @192.168.0.2 version.bind. txt chaos

; <<>> DiG 9.2.1 <<>> @192.168.0.2 version.bind. txt chaos
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 17136  ← 「REFUSED」エラーが返される
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; Query time: 4 msec
;; SERVER: 192.168.0.2#53(192.168.0.2)
;; WHEN: Thu Aug  7 00:40:43 2003
;; MSG SIZE  rcvd: 30
```

リスト7● 外部ホストからバージョン情報を問い合わせると「REFUSED」エラーが返される

Q12 停止したネームサーバを自動的に再起動させたい

ネームサーバが何らかの原因で停止してしまった場合でも、自動的にネームサーバを起動させ、DNSサービスを継続させたい。

A BIND 9に付属しているnanny.plを利用する

ネームサーバを監視するプログラムがBINDに付属

BIND 9には、ネームサーバ（named）が正常に動作しているかどうかを監視し、正常に動作していない場合には自動的にnamedを再起動させるためのプログラム「nanny.pl」が付属している。nanny.plは、BIND 9のソースプログラムを展開したあとの「contrib/nanny/」ディレクトリに存在する。nanny.plをインストールするには次のようにすればよい。

```
$ tar xzvf bind-9.2.2.tar.gz   ← BINDのソースを展開する
$ cd bind-9.2.2/contrib/nanny/ ← nanny.plが存在するディレクトリに移動
$ su                           ← rootになる
# cp nanny.pl /usr/sbin        ← nanny.plファイルを適当なディレクトリにコピー
# chmod 755 /usr/sbin/nanny.pl ← nanny.plファイルに実行権を与える
```

nanny.plを利用するには、最初に、環境に合わせてファイル中のパラメータを修正する必要がある。Red Hat Linux 9で利用するには、「$pid_file_location」「$dig_program」「$named_program」の各パラメータをリスト8のように修正すればよい。

そして、root権限で次のコマンドを発行する。

```
# /usr/sbin/nanny.pl
```

すると、nanny.plがデーモンとして常駐し、30秒間隔でnamedが正常に動作しているかどうかを監視するようになる。そして、namedが正常に動作していない場合に

```
#!/usr/bin/perl
#
# Copyright (C) 2000, 2001  Internet Software Consortium.
#
# Permission to use, copy, modify, and distribute this software for any
# purpose with or without fee is hereby granted, provided that the above
# copyright notice and this permission notice appear in all copies.
#
# THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM
# DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL
# IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL
# INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT,
# INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING
# FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT,
# NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION
# WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

# $Id: nanny.pl,v 1.8 2001/01/09 21:46:21 bwelling Exp $

# A simple nanny to make sure named stays running.
```

リスト8● 「nanny.pl」ファイルの設定例。「$pid_file_location」「$dig_program」「$named_program」の各パラメータを修正する

```
$pid_file_location = '/var/run/named/named.pid';          namedのPIDファイルを設定
$nameserver_location = 'localhost';
$dig_program = '/usr/bin/dig';                            digコマンドを指定
$named_program =  '/usr/sbin/named -u named';             namedを起動するためのコマンドを指定

fork() && exit();

for (;;) {
        $pid = 0;
        open(FILE, $pid_file_location) || goto restart;
        $pid = <FILE>;
        close(FILE);
        chomp($pid);

        $res = kill 0, $pid;

        goto restart if ($res == 0);

        $dig_command =
               "$dig_program +short . ¥@$nameserver_location > /dev/null";
        $return = system($dig_command);
        goto restart if ($return == 9);

        sleep 30;
        next;

 restart:
        if ($pid != 0) {
                kill 15, $pid;
                sleep 30;
        }
        system ($named_program);
        sleep 120;
}
```

リスト8の続き

は、自動的にnamedを再起動させる。

また、nanny.plは、OS起動時に自動的に実行させるようにするのがよいだろう。Red Hat Linux 9の場合は、上記のコマンドをリスト9のように「/etc/rc.local」ファイルに記述しておくことで、OS起動時に自動的にnanny.plを実行することができる。

```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
/usr/sbin/nanny.pl                                        この行を追加
```

リスト9● OS起動時にnanny.plを自動起動させるための「/etc/rc.local」の記述例

NTTデータ　馬場達也