CentOS7

インストール

```
yum install bind-chroot
systemctl enable named-chroot
```

設定

設定ファイル

```
/etc/named.conf
```

実行時は

```
/var/named/chroot/etc
```

に chroot される。

■ named.conf

```
dnssec-enable no;
dnssec-validation no;
```

にしないと、環境によってはうまく動作しないので注意。

```
acl "trust" {
 192.168.0.0/24;
 192.168.1.0/24;
 localhost;
};

options {
        listen-on port 53 { trust; };
        #listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { trust; };
        allow-query-cache { trust; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;
        allow-recursion { trust; };
        forward first;
        #forward only;
        forwarders {
          8.8.8.8;
          8.8.4.4;
        };

        dnssec-enable no;
        dnssec-validation no;

        /* Path to ISC DLV key */
```

```
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named.flets.zones";
```

■ /var/named/chroot/etc/named.flets.zones

```
// フレッツ正引き用
zone "flets" {
        type forward;
        forward only;
        forwarders {
                123.107.190.5;
                123.107.190.6;
        };
};

zone "flets-east.jp" {
        type forward;
        forward only;
        forwarders {
                123.107.190.5;
                123.107.190.6;
        };
};

zone "v4flets-east.jp" {
        type forward;
        forward only;
        forwarders {
                123.107.190.5;
                123.107.190.6;
        };
};

zone "speed.flets-east.jp" {
        type forward;
        forward only;
        forwarders {
                123.107.190.5;
                123.107.190.6;
        };
};


// フレッツ逆引き用
zone "194.210.220.in-addr.arpa" {
        type forward;
        forward only;
        forwarders {
                123.107.190.5;
                123.107.190.6;
        };
};
```

ローカル用のゾーンファイル作成

■参考

http://rina.jpn.ph/rance/index.php?BIND9%E3%81%A7LAN%E5%86%85DNS%E3%82%B5%E3%83%BC%E3%83%90%E3%82%92%E7%AB%8B%E3%81%A6%E3%82%8B

CentOS5

http://www.atmarkit.co.jp/flinux/rensai/bind902/bind902a.html

http://centossrv.com/bind-lan.shtml

設定

以下のファイルを作成する。
必要に応じて書き換えること。

/var/named/chroot/etc/named.conf

```
// generated by named-bootconf.pl

options {
        directory "/var/named";
        /*
         * If there is a firewall between you and nameservers you want
         * to talk to, you might need to uncomment the query-source
         * directive below.  Previous versions of BIND always asked
         * questions using port 53, but BIND 8.1 uses an unprivileged
         * port by default.
         */
        // query-source address * port 53;

        //forward only;
        forward first;
        // プロバイダのＤＮＳと Google Public DNS（障害時用）
        forwarders{
                211.129.14.138;
                211.129.24.47;
                8.8.8.8;
                8.8.4.4;
        };


};

//
// a caching only nameserver config
// rndc で制御可能なホストを指定 (localhost のみ可 )

controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

// キャッシュサーバとしての設定
zone "." IN {
        type hint;
        file "named.ca";
};

// ループバックアドレス正引き用
zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

// ループバックアドレス逆引き用
zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};

// フレッツ正引き用
zone "flets" {
        type forward;
        forward only;
```

```
        forwarders {
                220.210.194.67; // ns1.flets
                220.210.194.68; // ns2.flets
        };
};

// フレッツ逆引き用
zone "194.210.220.in-addr.arpa" {
        type forward;
        forward only;
        forwarders {
                220.210.194.67;
                220.210.194.68;
        };
};

// rndc 秘密鍵の読込みパスを指定
include "/etc/rndc.key";
```

/var/named/chroot/var/named/localhost.zone

```
$TTL    86400
$ORIGIN localhost.
@                       1D IN SOA       @ root (
                                        42              ; serial (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        @
                        1D IN A         127.0.0.1
```

/var/named/chroot/var/named/named.ca

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;
;       last update:    Nov 5, 2002
;       related version of root zone:   2002110501
;
;
; formerly NS.INTERNIC.NET
;
.                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     128.9.0.107
;
; formerly C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
;
; formerly TERP.UMD.EDU
;
.                        3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A     128.8.10.90
;
; formerly NS.NASA.GOV
;
.                        3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000      A     192.203.230.10
;
; formerly NS.ISC.ORG
;
```

```
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
;
; formerly NS.NIC.DDN.MIL
;
.                       3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000      A     192.112.36.4
;
; formerly AOS.ARL.ARMY.MIL
;
.                       3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000      A     128.63.2.53
;
; formerly NIC.NORDU.NET
;
.                       3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     3600000      A     192.36.148.17
;
; operated by VeriSign, Inc.
;
.                       3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.     3600000      A     192.58.128.30
;
; housed in LINX, operated by RIPE NCC
;
.                       3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.     3600000      A     193.0.14.129
;
; operated by IANA
;
.                       3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.     3600000      A     198.32.64.12
;
; housed in Japan, operated by WIDE
;
.                       3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000      A     202.12.27.33
; End of File
```

/var/named/chroot/var/named/named.local

```
$TTL    86400
@       IN      SOA     localhost. root.localhost.  (
                                        1997022700 ; Serial
                                        28800      ; Refresh
                                        14400      ; Retry
                                        3600000    ; Expire
                                        86400 )    ; Minimum
              IN      NS      localhost.

1       IN      PTR     localhost.
```

named.ca の更新

以下のシェルを作成し、/etc/cron.monthly/named.root_update として設置する

```
#!/bin/sh

new=`mktemp`
errors=`mktemp`

dig @a.root-servers.net . ns > $new 2> $errors

if [ $? -eq 0 ]; then
    # sort_new=`mktemp`
    # sort_old=`mktemp`
    # diff_out=`mktemp`
    # sort $new > $sort_new
    # sort /var/named/chroot/var/named/named.ca > $sort_old
    # diff --ignore-matching-lines=^\; $sort_new $sort_old > $diff_out
    # if [ $? -ne 0 ]; then
        # (
         # echo '------------------- old named.root --------------------'
         # cat /var/named/chroot/var/named/named.ca
```

```
            # echo
            # echo '-------------------- new named.root --------------------'
            # cat $new
            # echo '---------------------- difference ----------------------'
            # cat $diff_out
           # ) | mail -s 'named.root updated' root
           cp -f $new /var/named/chroot/var/named/named.ca
           chown named. /var/named/chroot/var/named/named.ca
           chmod 644 /var/named/chroot/var/named/named.ca
           /etc/rc.d/init.d/named restart > /dev/null
       # fi
       # rm -f $sort_new $sort_old $diff_out
   else
       cat $errors | mail -s 'named.root update check error' root
   fi
   rm -f $new $errors
```

forwarders、 forward first、 forward only について

http://hp.vector.co.jp/authors/VA022911/tec/centos/bind15.htm

forwarders を指定すると、自分が master 以外のゾーンは常に自分をセカンダリと認識し、上位 DNS へ問い合わせます。
forward only を指定すると、上位 DNS での問い合わせに失敗した場合、ルートサーバへの問い合わせは実施しません。名前は解決できなかったことになります。
（つまり zone "." のセクションは使用されません）

forwarders を有効にするには

```
recursion yes;
```

が必要。 ルートサーバへ問い合わせするかどうかは、 forward only かどうかで決まる。