

dnssec.jp 配下における

DNSSEC テストベッド参加マニュアル

Version 1.2

2006 年 3 月 7 日

JPRS

はじめに

この文書は、JPRS が dnssec.jp 配下で提供する DNSSEC テストベッドに参加するための手順と、実際に DNSSEC 対応の DNS サーバを設定する方法について記述したものです。

この文書では、以下の内容について記述しています。

- ・ DNSSEC 対応のための前提条件
- ・ ゾーンの設定(DNSSEC なし)
- ・ ゾーン DNSSEC 化
- ・ DNSSEC 対応 DNS キャッシュサーバの設定
- ・ レジストリ(登録システム)への登録

この文書中における各種コマンドの実行例では、実行するユーザの権限を以下のようにプロンプトの違いで示しています。

% ... 一般ユーザ権限で実行するコマンド

... スーパーユーザ(root)権限で実行するコマンド

またこの文書では、参加者は BIND を使用した DNS サーバの設定に関する基本的な知識を既に保有していることを想定しています。

1. DNSSEC 対応のための前提条件

DNSSEC 対応 DNS サーバを動作させるためには、DNS サーバを動作させるホストにおいて、以下の条件を満たしている必要があります。

- ・ DNS コンテンツサーバを動作させるホストはインターネットから到達可能であること

DNS コンテンツサーバはインターネット上のすべてのホストから参照可能である必要があります。少なくとも DNS サービスで使用する、TCP ポート 53 および UDP ポート 53 双方への外部からのアクセスが可能である必要があります。

- DNS コンテンツサーバを動作させるホストは固定 IP アドレスを持つこと
DNS コンテンツサーバの情報は上位ゾーンの DNS サーバ(登録システム)に登録する必要があるため、そのための固定 IP アドレスが付与されている必要があります。
- DNS キャッシュサーバを動作させるホストはインターネットに到達可能であること
DNS キャッシュサーバはインターネットに到達可能である必要があります。
- クライアントホストにサービスを提供するための DNS キャッシュサーバを動作させるホストは固定 IP アドレスを持つこと
クライアントホストにサービスを提供するための DNS キャッシュサーバには、そのための固定 IP アドレス(通常、DNS コンテンツサーバとは別の IP アドレスを割り当てる)が付与されている必要があります。

DNSSEC への対応を行うためには、DNSSEC に対応した DNS サーバ(コンテンツサーバおよびキャッシュサーバ)の導入が必要になります。

1.1. BIND(BIND 9)を利用した DNSSEC の設定

以降では、DNSSEC に対応した BIND を使用した、DNSSEC 対応 DNS サーバのセットアップ方法について記述します。なお以下では、FreeBSD 6.0-RELEASE/i386 版における導入を例に記述しますが、Linux 等の他の OS においても基本的な手順は同様です。

BIND のバージョンは、必ず BIND 9.3.0 以降のものを利用してください。それよりバージョン番号の小さいものは、DNSSEC の方式に互換性がないため、本テストベッドに参加することはできません。

また、OS に標準で付属している BIND が BIND 9.3.0 以降のものであっても、生成時に `--with-openssl` オプションが指定されていない場合 DNSSEC を使用することができませんので、OS に付属の BIND を使用してテストベッドに参加する場合、

- (1) BIND 9.3.0 以降のバージョンが導入されていること
- (2) 生成時に `--with-openssl` オプションが設定されていること

の 2 点について、必ず確認するようにしてください。なお FreeBSD 6.0-RELEASE/i386 版では、

- (1) 標準添付の BIND は BIND 9.3.1
- (2) 生成時に `--with-openssl` オプションが設定されている

ため、標準添付の BIND をそのまま使用することができます。

1.2. BIND の導入

OS に付属の BIND よりも新しい最新版の BIND を ports によりインストールする場合、以下のコマンドを順に実行します。

```
# cd /usr/ports/dns/bind9
# make install
```

FreeBSD 6.0R の ports 環境では標準で `--with-openssl` オプションが自動的に指定されるようにデフォルトで設定されていますので、`make` の際にオプションを追加指定する必要はありません。

BIND をソースから生成する場合、BIND 9.3.2 は以下の URL から入手します。

```
ftp://ftp.isc.org/isc/bind9/9.3.2/
```

ソースを入手後、適切な場所でアーカイブを展開します。

```
% tar xzf bind-9.3.2.tar.gz
```

以下の手順によりコンパイル、インストールを行います。DNSSEC を有効にするため、コンパイルの際に `--with-openssl` オプションを指定する必要があります。

```
% ./configure --with-openssl
% make
# make install
```

これで、BIND のインストールは完了です。

2. ゾーンの設定(DNSSEC なし)

DNS コンテンツサーバの設定を行います。

DNSSEC の導入を容易にするため、ここではまず通常の DNS コンテンツサーバ(DNSSEC なし)の設定を行い、次にそれを DNSSEC 対応にするための設定を行う場合を例として説明します。

2.1. 設定の準備

FreeBSD では BIND の設定ファイルは/etc/namedb ディレクトリに作成します。

```
# cd /etc/namedb
```

rndc-confgen コマンドを実行して、rndc コマンドのためのファイル(rndc.conf)を作成します。

```
# rndc-confgen > rndc.conf
```

OS の更新の際に参照されることがあるため、システムに標準で入っている named.conf ファイルを保存しておきます。

```
# cp -p named.conf named.conf.ORG
```

これで、DNS コンテンツサーバの設定の準備ができました。

2.2. named.conf ファイルの作成

まず、vi 等のエディタで named.conf ファイルを作成します。

```
# vi named.conf
```

named.conf ファイルの設定例を付録 1 に示します。

ここでは、付録 1 に示した named.conf の設定内容について、順に説明します。

named.conf 最初の部分は、さきほど作成した rndc.conf のコメントの部分を、コメントをはずした上でそのまま設定します。

```
# Use with the following in named.conf, adjusting the allow list as needed:
```

```

key "rndc-key" {
    algorithm hmac-md5;
    secret "QJ4smILOxisoiY7vK8LS/w==";
};

controls {
    inet 127.0.0.1 port 953
        allow { 127.0.0.1; } keys { "rndc-key"; };
};

```

次に、options で各種オプションを設定し、ログをとるための設定をします。セカンダリサーバを追加設定する場合は、allow-transfer 行と notify 行の設定を適宜変更する必要があります。

```

options {
    directory "/etc/namedb";
    pid-file "/var/run/named/pid";
    recursion no;
    allow-transfer { none; };
    notify no;
};

logging {
    category default { default_syslog; };
};

```

次に、登録したドメイン名に対応するゾーンの設定を行います。ここでは、登録したドメイン名が example.dnssec.jp であった場合の例を記述しています。

```

zone "example.dnssec.jp" {
    type master;
    file "example.dnssec.jp.zone";
};

```

これで、named.conf ファイルの設定は終了です。

2.3. ゾーンファイルの作成

次に、ゾーンファイルの作成を行います。

ここでは、付録 2 に示したゾーンファイルの設定内容について、順に説明します。

ゾーンの ORIGIN、TTL を設定します。

```
$ORIGIN example.dnssec.jp.
```

```
$TTL 300
```

SOA レコードと NS レコードを設定します。

```
@      IN  SOA  ns1.example.dnssec.jp. hostmaster.example.dnssec.jp. (
                                2006030701    ; serial
                                3600          ; refresh
                                900           ; retry
                                1209600       ; expire
                                900           ; minimum
                                )
      IN  NS   ns1.example.dnssec.jp.
```

次に、必要な A レコード等を適宜設定します。

ここでは、www.example.dnssec.jp に対する A レコードを設定する場合の例を記述しています。

```
; sample A records
```

```
www    IN    A      192.168.0.1
```

2.4. 動作確認

次に、DNS コンテンツサーバの動作確認をします。

まず、手動で named を起動します。

```
# /usr/sbin/named -u bind
```

プロセスが正しく起動すること、また起動の際、画面や/var/log/messages ファイルにエラーが出な

いことを確認します。

次に、dig コマンドにより動作確認を行います。IP アドレスとして、設定中の DNS コンテンツサーバの IP アドレスを指定します。

```
# dig +norec -t A www.example.dnssec.jp @IP アドレス
```

下記のような出力が得られれば、コンテンツサーバは正常に設定されています。

```
; <<>> DiG 9.3.1 <<>> +norec -t A www.example.dnssec.jp @サーバの IP アドレ  
ス  
;; global options: printcmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32527  
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0  
  
;; QUESTION SECTION:  
www.example.dnssec.jp. IN      A  
  
;; ANSWER SECTION:  
www.example.dnssec.jp. 86400 IN A 192.168.0.1  
  
;; AUTHORITY SECTION:  
example.dnssec.jp. 86400 IN      NS      ns1.example.dnssec.jp.  
  
;; Query time: 1 msec  
;; SERVER: IP アドレス#53(IP アドレス)  
;; WHEN: Mon Mar 15 02:24:33 2004  
;; MSG SIZE rcvd: 152
```

2.5. 自動起動のための設定

システムの立ち上げの際に、named を自動起動するための設定を行います。
/etc/rc.conf ファイルに以下を追加します。これにより、システム立ち上げの際に named が自動的に起動するようになります。

```
# for named
named_enable="YES"
named_flags="-u bind"
```


3. ゾーンの DNSSEC 化

次に、コンテンツサーバを DNSSEC 対応にするための設定を行います。

3.1. 鍵の作成

現在の DNSSEC では、異なった 2 つの鍵を使用することが推奨されています。一方はゾーンファイルに署名するための鍵(Zone Signing Key: ZSK)で、他方はその鍵に署名するための鍵(Key Signing Key: KSK)です。KSK から生成された DS 情報が親ゾーン(ENUM 登録システム)に登録され、親ゾーンからの信頼連鎖に使用されます。

まず、鍵の作成を行います。鍵は DNSKEY レコードとしてゾーンファイルに読み込ませる必要があるため、`/etc/namedb` ディレクトリで作成する必要があります。

```
# cd /etc/namedb
```

次に、ZSK を作成します。ZSK は更新頻度を上げることを条件に鍵長を短くすることができ、署名にかかる負荷を軽減することができます。ここでは、1024 ビットの鍵を作成します。

```
# dnssec-keygen -a RSASHA1 -b 1024 -n zone example.dnssec.jp.  
Kexample.dnssec.jp.+005+36536
```

KSK を作成します。KSK は高い安全性が必要であるため、鍵長を長くします。ここでは、4096 ビットの鍵を作成します。

```
# dnssec-keygen -a RSASHA1 -b 4096 -n zone example.dnssec.jp.  
Kexample.dnssec.jp.+005+48812
```

3.2. ゾーンファイルに鍵を読み込ませる設定を追加

3.3 で設定したゾーンファイルに、ZSK と KSK を読み込ませるための設定をゾーンファイル内に追加します。

下記のように `$INCLUDE` 文を使うことで、容易に設定することができます。

```
; include ZSK and KSK
```

```
$INCLUDE Kexample.dnssec.jp.+005+36536.key ; ZSK
$INCLUDE Kexample.dnssec.jp.+005+48812.key ; KSK
```

3.3. ゾーンファイルのシリアルドメイン名を更新

ゾーンファイルのシリアル番号を更新します。

```
@      IN SOA ns1.example.dnssec.jp. hostmaster.example.dnssec.jp. (
                2006030702      ; serial   この数字を更新
                3600             ; refresh
                900              ; retry
                1209600          ; expire
                900              ; minimum
        )
      IN NS  ns1.example.dnssec.jp.
```

3.4. ゾーンファイルへの署名

現在の BIND の実装では、ゾーンファイルのファイル名をゾーン名に一致させておくと、署名の操作を簡単に行うことができます。ここでは、シンボリックリンクを作成することで、ファイル名を一致させておきます。

```
# ln -s example.dnssec.jp.zone example.dnssec.jp
```

その後、dnssec-signzone コマンドを使用して、ゾーンファイルの署名を行います。dnssec-signzone -k KSK zonefile ZSK のように、-k オプションで KSK を指定し、ゾーンファイルの後ろに ZSK を指定します。

```
# dnssec-signzone -k Kexample.dnssec.jp.+005+48812.key
example.dnssec.jp Kexample.dnssec.jp.+005+36536.key
example.dnssec.jp.signed
( は継続行)
```

署名が終了すると、ゾーン名.signed という署名済みファイルが作成されます。

3.5. ファイルのリロード

named.conf ファイルを修正し、従来のファイル(ゾーン名.zone)のかわりに署名済みファイル(ゾーン名.signed)をゾーンファイルとして読み込むように設定します。

```
zone "example.dnssec.jp" {
    type master;
    //file "example.dnssec.jp.zone";
    file "example.dnssec.jp.signed";
};
```

BIND の場合、named.conf ファイルの options エントリで dnssec-enable yes; を指定することにより、DNSSEC を明示的に有効にする必要があります。この設定を行っていない場合、DNSSEC が有効とならないため、注意が必要です。

```
options {
    (省略)
    dnssec-enable yes;    この行を追加
};
```

その後、rndc コマンドによりゾーンファイルのリロードを行います。/var/log/messages ファイルにエラーが出力されないことを確認してください。

```
# rndc -c /etc/namedb/rndc.conf reload
server reload successful
```

これにより、ゾーンの DNSSEC 化が完了します。

3.6. 動作の確認

DNSSEC 化の確認は、dig コマンドに+dnssec オプションをつけることで行うことができます。IP アドレスとして、DNS コンテンツサーバの IP アドレスを指定します。

```
# dig +dnssec +nored -t A www.example.dnssec.jp @IP アドレス ( は
継続行)
```

dig コマンドの出力を付録 3 に添付します。付録 3 のような出力が得られれば、コンテンツサーバ

は正常に DNSSEC 対応に設定されています。

4. DNSSEC 対応 DNS キャッシュサーバの設定

次に、DNSSEC 対応キャッシュサーバを設定します。

ここでは、コンテンツサーバとは別のマシン(FreeBSD 6.0-RELEASE/i386)を準備したうえで、そのマシンを DNSSEC 対応キャッシュサーバとして設定する場合を例として説明します。なお DNS コンテンツサーバと同じマシンを DNS キャッシュサーバとして設定する場合にも、一般的に DNS キャッシュサーバが使用する IP アドレス DNS コンテンツサーバのものとは別のものにする必要があることに注意してください。

4.1. 設定の準備

コンテンツサーバの場合と同様に、ディレクトリを移動します。

```
# cd /etc/namedb
```

コンテンツサーバの場合と同様に、`rndc.conf` を作成します。

もしコンテンツサーバと同じマシンでキャッシュサーバを動作させる場合、ファイル名を変える必要があります。

```
# rndc-confgen > rndc.conf
```

システムに標準で入っている `named.conf` ファイルを保存しておきます。

```
# mv named.conf named.conf.ORG
```

4.2. `named.conf` ファイルの作成

`vi` 等のエディタで `named.conf` ファイルを作成します。

```
# vi named.conf
```

キャッシュサーバ用の `named.conf` ファイルの設定例を付録 4 に示します。

ここでは、`named.conf` の設定内容について順を追って説明します。

最初の部分は、さきほど作成した `rndc.conf` のコメントの部分を、コメントをはずした上でそのまま設定します。もしコンテンツサーバと同じマシンでキャッシュサーバを動作させる場合、`rndc` コマンド

が使用するポート番号を変える必要があります。

```
# Use with the following in named.conf, adjusting the allow list as needed:
```

```
key "rndc-key" {
    algorithm hmac-md5;
    secret "QJ4smILOxisoiY7vK8LS/w==";
};

controls {
    inet 127.0.0.1 port 953
        allow { 127.0.0.1; } keys { "rndc-key"; };
};
```

次に、option で各種オプションを設定し、システムログのための設定をします。キャッシュサーバでは、再帰検索(recursion)を有効にする必要があります。

なお DNS コンテンツサーバの場合と同様 DNS キャッシュサーバの場合も、named.conf ファイルの options エントリで dnssec-enable yes; を指定することにより、DNSSEC を明示的に有効にする必要があります。この設定を行っていない場合、DNSSEC が有効にならないため、注意が必要です。

```
options {
    directory "/etc/namedb";
    pid-file "/var/run/named/pid";
    recursion yes;
    allow-transfer { none; };
    notify no;
    dnssec-enable yes;
};

logging {
    category default { default_syslog; };
};
```

次に、ルートサーバのためのヒントファイルと、localhost の逆引きの設定を行います。
(各ファイルの設定内容は省略します)

```

zone "." {
    type hint;
    file "named.root";
};

zone "0.0.127.IN-ADDR.ARPA" {
    type master;
    file "localhost.rev";
};

// RFC 3152
zone
"1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA"
{
    type master;
    file "localhost-v6.rev";
};

```

最後に、trusted keys の設定を行います。

<https://register.etjp.jp/reg/named.conf> にある設定ファイルのサンプルから、trusted-keys の部分 (dnssec.jp および 1.2.0.0.1.8.e164.arpa の行の 2 行)を named.conf ファイルにそのまま、コピー&ペーストします(trusted-keys の内容は実際のものとは異なる場合があります)。

```

trusted-keys { "dnssec.jp." 257 3 5
"AQPfVHjVeqY7c6g0txSuATAhbsF0BF0mirs9yz+CZS7tvSQ96SYABSE8
z1Fv95AfaF7rf3vGPFoNUMfk9/IfGLngwHGVgvggnQsBPvfOm0/mMAGsp
iACJBop9IbvFAFv2JGetO3sCFGsILG75sj0aLbc3e9C1bOrAwlVDVXg3
q3L03QlUsyhAEiMH3px2evOescvk6W8/NL4nTqbYC/+DXF6u0zognxWI
NF60cZBU41oixge4YUEqZKAAKOthU+aiez1WWEeo08Vwfaa1H8qGhqW+
toX1ASYSQiDPQ/JoLEMZQSYt1K5zXZz0BalG6joiedgNMOK7eKBzRPuK
wfurfrsimkVxyeYDf7jtX5dCOsZ+dACnvpV4dG/XbKiHoolpQYqC4nI/
JIm7Ai8APVfwjM5Af/Qs7S2lWrE9Z60KBaEXFSYZAxqdDYiZbIW6Tm91
LWJV+DUcR7mym86NcNKIw7y4qvFaV4XrJxC4zoI7y1Wiw+P0pSBHLwfr
9r9+8khB8Cz1Oha4PIQK1OXEA/MQH3R851UD+oF4mbLOUpbpzzybryDP
kNeS9tYddEo7awm2olSw36fpsF17KTfILe6V3AAcOeDhCxakWEU+VAYK

```

```
qypVAe2vKayxEvTCqizx4z16BhR+Vz4vyyGaLt9sKY6mfeJWTZPP4wUF
5cSc5RnE1EBYhw==" ; };
```

(注: は継続行)

```
trusted-keys { "1.2.0.0.1.8.e164.arpa." 257 3 5
"AQO+z+SCfYvWmBTm/yiRbLmo2ELtUMONDRTSLWg+s2MWtN19JT+4ZGWC
NYEj56KDu2ksaRaQnUJlaG13kEKTGzNkyjtLq4mUfwwJGLHb9piLUfYg
vThqQ4y3e51KDtZnWLOEJSFMjEFialATG1MkK5gCumzI8jhFmrZvlnOs
PErn/BMsl5vAwsIyaHUsWJWxYM6STOZ1+78AqUj6ILkPDqmBkRna4YKK
7FAQkGJzerbFgd/zO4b6Q2JL7HRjNqPRGDdCqNOwVzD3m8XdErhlBAQL
/JDHXF+pBnzUwhj6mKhwbZj0nY2gT/bJaYCD3aQj8sPKDDogFWLeJXE6
sqdsU5wBONh0k7FYpM5Fhoy+brftWkq/Gfp1LqNuRGehEy5ZDQoRbBEh
towaZiEIRZYOGQZe3YIk3j8mZ03p7K8xbGstg4gmF1CRXsFUyDAoDrvW
XXo41VS+c3faqwH7Pmq3K7aS/HOcXMGkUwkTfMEHfbjmyFkLflXmphTl
bJauM9Q3uCmwiIYooagqNzJshGtCvTiwkRi8vtrBWL4giGZQm6SfEyBy
AARXPTdnIsT7a5uKr3ax5J2PPO8VixE8bkVjtfzoom6Di089UZ3KCoON
Vd79MBhzhHRuj3LEmPPX25I6t1x2bXhtIKGpl1sMoSiT3+tvCuJKa7EH
9wrSOZZ1A4KBFQ==" ; };
```

(注: は継続行)

これで、named.conf ファイルの設定は終了です。

その後、コンテンツサーバの場合と同様に、自動起動のための設定を行います。

4.3. DNSSEC 対応キャッシュサーバの動作確認

DNSSEC 対応キャッシュサーバの動作確認は、dig コマンドに+dnssec オプションをつけることで行うことができます。再帰検索を行わせるために、+norec オプションは指定しません。

```
# dig +dnssec -t A www.example.dnssec.jp @IP アドレス
```

「3.6 動作の確認」と同様の出力が得られれば、キャッシュサーバは正常に DNSSEC 対応に設定されています。

4.4. /etc/resolv.conf ファイルの設定

最後に、/etc/resolv.conf ファイルを書き換えることにより、デフォルトサーバを DNSSEC 対応 DNS

キャッシュサーバに切り替えます。

`nameserver` キャッシュサーバの IP アドレス

5. レジストリ(登録システム)への登録

登録システムに、生成した DS セットを登録します。

BIND 9.3.0 ベータ版では、上位ゾーンに登録するための DS セットは、3.4. におけるゾーンファイルへの署名の際に、dsset-ゾーン名(例えば dsset-example.dnssec.jp)というファイル名で作成されています。

DS セットファイルの例を以下に示します。

```
example.dnssec.jp.      IN DS 38306 5 1  
656E7376BA2C0576C4CD0762FB9F6387029290EC
```

(は継続行)

このファイルの内容を登録システムに登録します。

まず、登録システムにおいて、該当するドメイン名を委任するための設定を行います。

登録システム (<https://register.etjp.jp/reg/dnssec.cgi>) の「Enter new domain name」で、希望する dnssec.jp 配下のドメイン名を入力し、enter をクリックします。

ETJP dnssec.jp registry system

[ETJP members page](#) (Japanese only)
[e164.jp Registry system](#)

Your account = [blacked out]

Edit your entry.
You can edit:

[View zonefile](#)

You can register one 'dnssec.jp' subdomain.
enter New domainname

.dnssec.jp. ドメイン名を入力し、
 enter をクリック

[DNSSEC resolver cacheserver's configuration](#)

Copyright (C) JPRS. 2004
All rights reserved.

登録された実験用ドメイン名のリンクをクリックします。

ETJP dnssec.jp registry system

example is added for

[ETJP members page](#)(Japanese only)
[e164.jp Registry system](#)

Your account =

Edit your entry.

You can edit: [example](#) [ここをクリック](#)

[View zonefile](#)

You can register one 'dnssec.jp' subdomain.

enter New domainname

.dnssec.jp

[DNSSEC resolver cacheserver's configuration](#)

Copyright (C) JPRS. 2004

All rights reserved.

編集画面が開きますので、「NS delegation mode」を選択して、enter をクリックします。

etjp dnssec.jp registry

Info: 'example' zonedata will not be generated.

Your account = █████

Edit domain: example

DOMAINNAME: example.dnssec.jp

delete this domain

A/AAAA mode

NS delegation mode ここを選択

Resource Record edit:

delete **A/AAAA** **value**

A AAAA

ここをクリック

[View zonefile](#)

[Return to Top](#)

If you make any changes, click 'enter' button.

If you make changes, zone file will be generated soon.

del = delete mark

Copyright (C) JPRS. 2004

All rights reserved.

ネームサーバ情報の入力画面が開きますので、ネームサーバホスト名、必要なグルーレコード、鍵セットを入力します。

「value」にネームサーバのホスト名を入力し、「glue records:」に必要なグルーレコードを入力します。そのうえで DS セットファイルの内容をそのまま順番にコピー&ペーストして、「enter」をクリックします。

etjp dnssec.jp registry

Info: 'example' zonedata will not be generated.

Your account = 999

Edit domain: example

DOMAINNAME: example.dnssec.jp

delete this domain

A/AAAA mode

NS delegation mode

Resource Record edit:

delete **value**

NS ns1.example.dnssec.jp

ネームサーバのホスト名を入力

glue records:

ns1.example.dnssec.jp. IN A 192.168.0.1

必要な
グルーレコードを入力

DS Resource record for example.dnssec.jp:

delete	KeyTag	Algorithm	Digest Type	Digest
<input type="checkbox"/>		=5	=1	20bytes

DS 38306 5 1 30576C4GD0762F69F6387029290EC

enter をクリック

DS セットファイルの
内容をそのまま順番に入力

[View zonefile](#)

[Return to Top](#)

If you make any changes, click 'enter' button.

If you make changes, zone file will be generated soon.

del = delete mark

Copyright (C) JPRS. 2004

All rights reserved.

これで、登録システムに DS セットが登録され、DNSSEC テストベッドへの参加が完了します。

付録 1 DNS コンテンツサーバ用 named.conf ファイルの例

```
controls {
    inet 127.0.0.1 port 953
        allow { 127.0.0.1; } keys { "rndc-key"; };
};

options {
    directory "/etc/namedb";
    pid-file "/var/run/named/pid";
    recursion no;
    allow-transfer { none; };
    notify no;
    dnssec-enable yes;
};

logging {
    category default { default_syslog; };
};

zone "example.dnssec.jp" {
    type master;
    file "example.dnssec.jp.zone";
};
```

付録2 ゾーンファイルの例

```
$ORIGIN example.dnssec.jp.  
$TTL 86400  
@                IN SOA ns1.example.dnssec.jp.  
hostmaster.example.dnssec.jp. (  
                        2004031501 ; serial  
                        3600      ; refresh  
                        900       ; retry  
                        1209600   ; expire  
                        900       ; minimum  
                        )  
                IN NS  ns1.example.dnssec.jp.  
  
; sample A  
www             IN A   192.168.0.1
```


付録3 dig コマンド出力例

```
; <<>> DiG 9.3.1 <<>> +norec +dnssec -t a www.example.dnssec.jp.
@192.168.0.1
;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 54344
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.example.dnssec.jp.          IN      A

;; ANSWER SECTION:
www.example.dnssec.jp.          300     IN      A          192.168.0.1
www.example.dnssec.jp.          300     IN      RRSIG     A 5 4 60 20040711190204
20040611190204 42407 example.dnssec.jp.
XDqF2mYXMoVDGFAYhUsS6pMmyhknGQZS7gMlBtfilC2q2Te/ZjB7Mp84
vbKQCTfYMeGoETXJbjaluaUIUNjs+qiPdM+4k1jHSnS0CCR/vm1CYnV
gRBXW+yG5mpJlNBCSpSDA+CfX9dDemy5VxC60TfAjUTEiZ2XgV8L6J84 DPk=

;; AUTHORITY SECTION:
example.dnssec.jp.          300     IN      NS         ns1.example.dnssec.jp.
example.dnssec.jp.          300     IN      RRSIG     NS 5 3 60 20040711190204
20040611190204 42407 example.dnssec.jp.
TclmENTUszhpmBo26Q+6Xwkjac8giRmV+5aLqyz94ueDtjT+RZ2rw1YQ
xlgPUZJgmlTMVKCvX89X3i/GDjgWSKvVW09yVLaHODnu45SFGAUT4c
47RE5h6XvaaXFTTWGiYseY/pha9bUW0P2flqsxheyUKrwKnBO+QBXXRF 7Qc=

;; ADDITIONAL SECTION:
ns1.example.dnssec.jp.          300     IN      A          192.168.0.1
ns1.example.dnssec.jp.          300     IN      RRSIG     A 5 4 60 20040711190204
20040611190204 42407 example.dnssec.jp.
MZbM0Nu3d6FLP7rp5NclNptWraExIl61exrdW8wmtHcoEJTWvB3qxQkL
78o0bod1qJeSz+LQ4bp+BY4mlHAK06rK0uC/hDvnxwhL4MSOUcw6xBym
```

Eq80rNo4VCjkLnO8DmpSprUu97Xr+wv/hFYfQh351YSW/YSC+uWfxCwq pp4=
example.dnssec.jp. 300 IN DNSKEY 256 3 5
AQPFAdnNqR1wKEddNww4Yz1wo89QH1/aTibLcG/A5b4o6FxFxSeSgmXrvd
vKNugytJtxp3f1DjIpjt7oThHrj6L83XJgxW+a3fd0AIFU5rOyEuPrK0
QBIYR1P9cVadeu7zefJpD7fzpjn4ZREyQ+M7tyOx1121oFd2uXQ750DG de/S6Q==
example.dnssec.jp. 300 IN DNSKEY 256 3 5
AQOxZRw5HKM5bexLxAWU0X/ROjk0vsHNzx3SSLacmGITgnncFSpt/vtp
Vt7UTQTOFJfrnA7yUVsAVS9AHk9vGHeeUZhpsn/58X34b0+UAYnQQufe
V/UGdJwBPX+x8G2zyrbBCWQ0brgZyHgEUhWBgTXgp4nuMconccG6Q1vp
b7WQ4y7dJjt8p/9raYUVNKP616OR/uIoFU2pamNpAwuvT0n3MnYWPQZ
MJHZMVvBZtuUzIkJjRKCqVmRoqmmGat+u65YYR7JkvpEqbUKVVnpg9fG
qhEG8osUS/bEtsCS+EZ4xpdD9FJGxz5szjbLgS/2PaW08ISYegchXec
wxASJqud2WyIUte3oUpZWfn7j9k1Gjx12VUnJ6cEYBvqi76Zw4rxGfK2
vzT5zK0sJqEgvp0qj6NqrZez4SpPfUmqgcl2BdGGHOJYkDz29dVv0sV
VG2tVxJ4nfQbMDRsZxFlgQ0LE/LMu7cD51IpMkBjUpOEx9g+0qCdrna3
J+1qlq3ehduy7oJrjeS1BucsOojr0x91ScLuHtOXVLkYPMk65BAeNNck
Dl1ikghQ37a9v8ULhjc63KuAgwpsMsntLWdPzz30fYv0JxXn8PKrRjd7
n2XqL/AserJh+RnvTP3SasHYzOhlEpMncWf1Xdfk052jmYg3d547nv68
Kk2qJQkdI7Urfw==
example.dnssec.jp. 300 IN RRSIG DNSKEY 5 3 60 20040711190204
20040611190204 38306 example.dnssec.jp.
Q1Zd21E2mfrEUdKseQYkLaeMrSO+YI4kpyEMFGNHxenCvkh2Zp/ikUFs
7DxGD9XlVTPDh/HnumsheYclRjfpuBw20W5s3pZSOZfzWAV5oWSXVf9m
BvsJMQjxGLgvUlsed6WnNmEcBrIUTvRtVhgFPFMg71dTbiKr3GRGc5Zu
JIIfGUUsealmvRPGPG0AlyDF2IWjMkhD2aeMXIzWnuXWODMiFjDObuLIWO
ZsZAn3AoSEzJk1wMptPNTJwz+X8hZdPwjNyeUMzHhUy3TpbNmXvUA23
y3X0ByFrqP35noolZycrGvZeUcXZuqnESg6MkBTewTqy1X/oL52RbD4b
urH3rH0QHdwWZq0WbP1J+w2jsvVkjC+qBCCKDGGvtj13fhN4AEVZF2aM
AYUYaRgd3m4z/SfD0yBq4v0H8+WQmllPeE5dX6DiRoos3DO5PqwtSXL7
RS3+KGr2t754A/71Lh5I/dhqm3tEutwt2zhuCU75f0MXfkd6o4/PuYrd
IsubN8KBEo9DyzcL8sWVieluj6jboXRHYnCA/+wLX7QYRja4woi9lSjn
df19syYkLXvMsfY05MCzUJDHfJIF9P+XXxxvAAfjvl3OGHtctuXzKFC4
mqXlGnf09hCXWifXhqY/io/yaONqp2kFp3JWm6MSYG1MaaZlgSQkDnDt kse22WBveAY=
example.dnssec.jp. 300 IN RRSIG DNSKEY 5 3 60 20040711190204
20040611190204 42407 example.dnssec.jp.
APbMSKg6Oc7wCBP0/7x0TiDTZJShayiwDh6YTLXHQcshpXDj0m9CXxsg

bNa2WGaaEraOfU+ohhZ4GsDhKqEkloxILLaEeb9azy5PG0aKltW4upmm
SeTy6eGm8Qst2c0KANYD0fN4JFJ97j5OXxnWYedcf5NmQQEDZvCFpj2s s2I=

;; Query time: 1 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Mon Jun 14 21:56:19 2004
;; MSG SIZE rcvd: 2039

付録 4 DNS キャッシュサーバ用 named.conf ファイルの例

```
options {
    directory "/etc/namedb";
    allow-transfer {none;};
    allow-query {127.0.0.1; };
    listen-on {127.0.0.1;};
    listen-on-v6 { none; };
    dnssec-enable yes;
    recursion yes;
    pid-file "/var/run/named/cache.pid";
};

trusted-keys { "dnssec.jp." 257 3 5
"AQPfVHjVeqY7c6g0txSuATaHbsF0BF0mirs9yz+CZS7tvSQ96SYABSE8
z1Fv95AfaF7rf3vGPFoNUMfK9/IfGLngwHGVgvgvgnQsBPvfOm0/mMAGsp
iACJBop9IbvFAFv2JGetO3sCFGsILG75sj0aLbc3e9C1bOrAwlVDVXg3
q3L03QlUsyhaEiMH3px2evOesckv6W8/NL4nTqbYC/+DXF6u0zognxWI
NF60cZBU41oixge4YUEqzKAAK0thU+aiez1WWEeo08VwfaalH8qGhqW+
toX1ASYSQiDPQ/JoLEMZQSYt1K5zXZz0BalG6joiedgNMOK7eKBzRPuK
wfurfrsimkVxyeYDf7jtX5dCOsZ+dACnvpV4dG/XbKiHoolpQYqC4nI/
JIm7Ai8APVfwjM5Af/Qs7S2lWrE9Z60KBaEXFSYZAxqdDYiZbIW6Tm9l
LWJV+DUcR7mym86NcNKIw7y4qvFaV4XrJxC4zoI7y1Wiw+P0pSBHLwfr
9r9+8khB8CzlOha4PIQK1OXEA/MQH3R851UD+oF4mbLOUpbpzzybryDP
kNeS9tYddeo7awm2olSw36fpsF17KTfILe6V3AAcOeDhCxakWEU+VAYK
qypVAe2vKayxEvTCqizx4zl6Bhr+Vz4vyyGaLt9sKY6mfeJWTZPP4wUF
5cSc5RnE1EByhw==" ; };

trusted-keys { "1.2.0.0.1.8.e164.arpa." 257 3 5
"AQO+z+SCfYvWmBTm/yiRbLmo2ELtUMONDRTSLWg+s2MWtN19JT+4ZGWC
NYEj56KDu2ksaRaQnUJlaG13kEKTGzNkyjtLq4mUfwwJGLHb9piLUfYg
vThqQ4y3e5lKDtznWlOEJSFMjEFialATG1MkK5gCumzI8jhFmrZvlnOs
PErn/BMsl5vAwsIyaHUSWJWxYM6STOZ1+78AqUj6ILkPDqmBkRna4YKK
7FAQkGJzerbFgd/zO4b6Q2JL7HRjNqPRGDdCqNOWVzd3m8XdeRh1BAQL
/JDHXF+pBnzUwhj6mKhwbZj0nY2gT/bJaYCD3aQj8sPKDDogFWLeJXE6
sqdsU5wBOnH0k7FYpm5Fhoy+brftWkq/Gfp1LqNuRGehEy5ZDQoRbBEh
towaZiEIRZYOGQZe3YIk3j8mZ03p7K8xbGstg4gmF1CRXsFUyDAoDrvW
```

```
XXo41VS+c3faqwH7Pmq3K7aS/HOCxMGkUwkTfMEHfbjmyFkLf1XmphT1
bJauM9Q3uCmwiIYooagqNzJshGtCvTiwkRi8vtrBWL4giGZQm6SfEyBy
AARXPTdnIsT7a5uKr3ax5J2PPO8VixE8bkVjtfzoom6Di089UZ3KCoON
Vd79MBhzhHRuj3LEmPPX25I6t1x2bXhtIKGp11sMoSiT3+tvCuJKa7EH
9wrSOZZ1A4KBFQ==" ; };
```

```
logging {
    channel log2 {
        file "/var/log/named/cache" versions 10 size 100k;
        print-category yes;
        print-severity yes;
        print-time yes;
    };
    category default      { log2; };
    category general      { log2; };
    category database     { log2; };
    category security     { log2; };
    category config       { log2; };
    category resolver     { log2; };
    category xfer-in      { log2; };
    category xfer-out     { log2; };
    category notify       { log2; };
    category client       { log2; };
    category unmatched   { log2; };
    category network      { log2; };
    category update       { log2; };
    category queries      { log2; };
    category dispatch     { log2; };
    category dnssec       { log2; };
    category lame-servers { log2; };
};

zone "." {
    type hint;
    file "named.root";
};
```

更新履歴

- Version 1.00 Version 1.01 における変更
 - 「1.1 BIND 9.3-snapshot のインストール」の configure 実行時のオプションが誤っていたのを修正
 - ◇ 誤: --enable-openssl
 - ◇ 正: --with-openssl
 - 別ファイルであった付録 1～付録 4 を本文にマージ
- Version 1.01 Version 1.1 における変更
 - BIND 9.3.0 ベータ版への更新に伴う変更
 - ◇ DNS コンテンツサーバ
 - ◇ DNS キャッシュサーバ
 - ◇ レジストリシステム
 - ◇ 各種サンプルファイル
 - ◇ dig コマンドサンプル
- Version 1.1 Version 1.2 における変更
 - BIND 9.3.0 正式版への更新に伴う変更
 - ◇ DNS コンテンツサーバ
 - ◇ DNS キャッシュサーバ
 - ◇ レジストリシステム
 - ◇ 各種サンプルファイル
 - ◇ dig コマンドサンプル
 - FreeBSD 5.2.1R 6.0R への更新に伴う変更
 - ◇ 設定手順
 - ◇ 設定内容
 - 日本 ENUM トライアルによる DNSSEC テストベッド開始に伴う変更
 - ◇ ドメイン名 (e164.jp 1.2.0.0.1.8.e164.arpa)