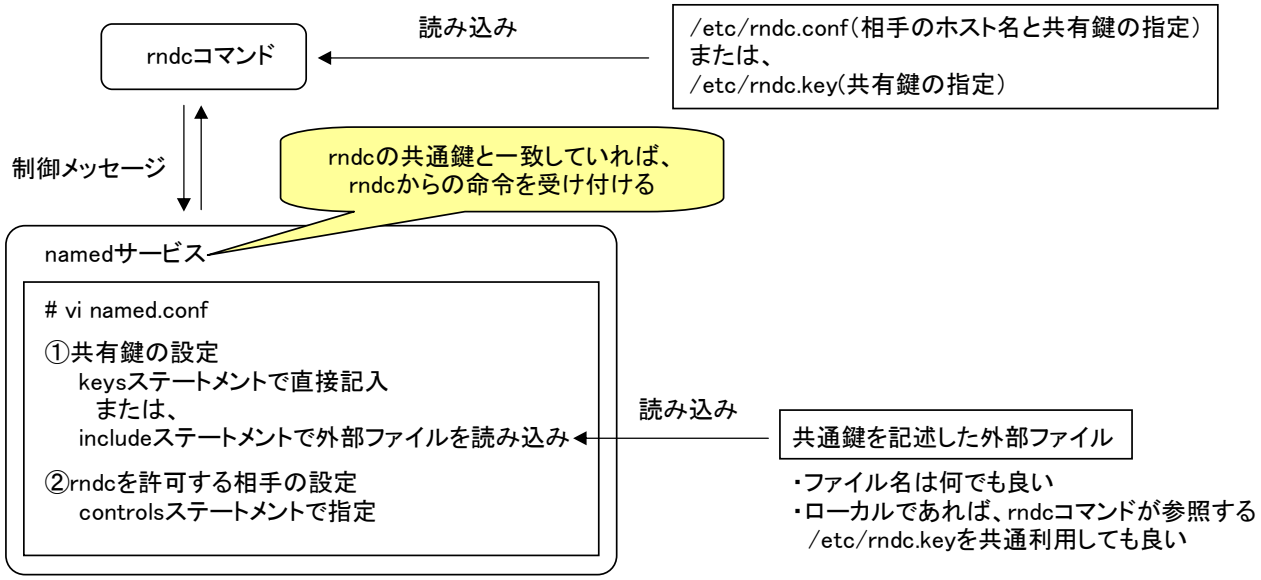
rndc
ローカル上、またはリモート上にあるBIND9を制御するツール

rndcの仕組み



rndcの設定
rndcを利用するためには、rndcコマンドを実行する側とBINDサービスが実行されている側の双方で設定が必要になる

① 共通鍵の作成
BIND付属のrndc-confgenを使用して共通鍵を作成する
作成した共通鍵は、②や③で使用する

[書式]
rndc-confgen オプション

[主なオプション]

-a	共通鍵を新しく作成する　デフォルトでは/etc/rndc.keyに出力
-b ビット数	共通鍵のビット数　　省略時のデフォルトは128bit　512bit推奨
-c 出力ファイル名	省略時は/etc/rndc.keyで作成されるが、別のファイル名としたい場合に使用する
-k 共通鍵名	共通鍵名の指定
-t chrootディレクトリ	chrootディレクトリ配下にもファイルを出力したい場合
-u ユーザ名	chrootディレクトリ配下に出力したファイルの所有者を指定したい場合

[設定例]

```
# rndc-confgen -a -b 512 -k rndctest

# more /etc/rndc.key
key "rndctest" {
        algorithm hmac-md5;
        secret "Ey/2YxEvsIiJ5WwQWzdlDAZ5L1ICSShC6e1QNdQ1
h5jgThMij608OVd38ge7Br/NFE0WnkK1oUB/Ykm63fg16A==";
};

# ls -l /etc/rndc.key
-r-------- 1 root root 141  4月 23 03:58 /etc/rndc.key
```

-cオプション省略時は/etc/rndc.keyに出力
(既存の/etc/rndc.keyを上書き)
ビット数は512bit推奨

```
# rndc-confgen -a -b 512 -c /etc/rndc.key.test
-k keytestdesu -t /var/named/chroot -u named

# ls -l /etc/rndc*
-r-------- 1 root root 113  4月 13 11:03 /etc/rndc.key
-rw------- 1 root root 144  4月 23 03:45 /etc/rndc.key.test

# ls -l /var/named/chroot/etc/rndc.key.test
-rw------- 1 named root 144  4月 23 03:45 /var/named/chroot/etc/rndc.key.test
```

検証のため適当にオプションを追加

-cオプションを使うと既存の/etc/rndc.keyを
上書きすることは無い

chroot配下にも同じものが作成される
-uオプションはchroot配下のファイルに影響している

② rndcコマンドを実行する側の設定

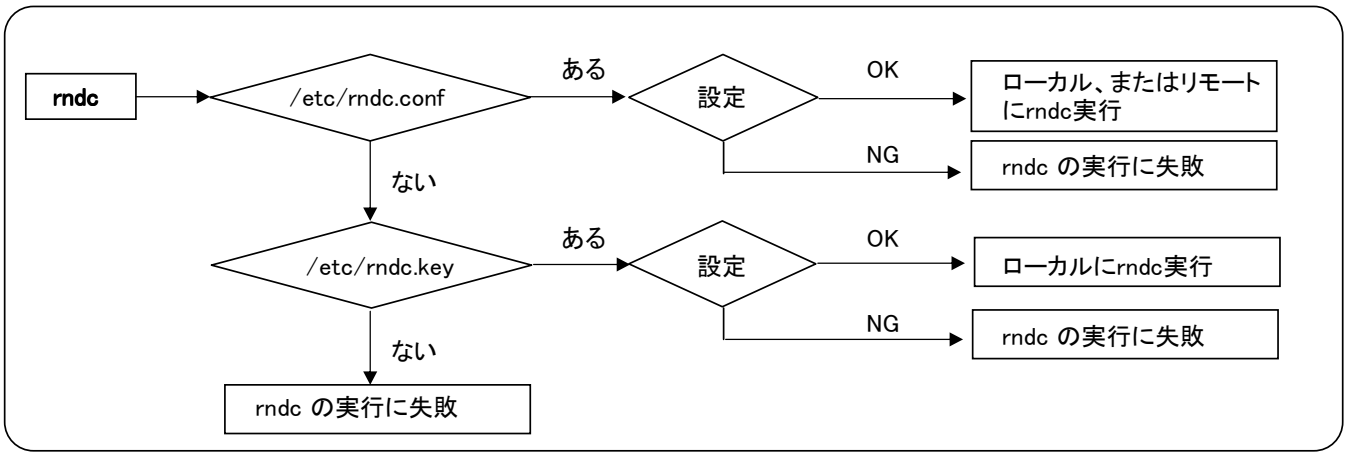
rndcコマンドは、デフォルトで/etc/rndc.confまたは/etc/rndc.keyを参照している
最初に/etc/rndc.confを参照し、「ファイルがない場合は」/etc/rndc.keyを参照する
よって、/etc/rndc.confの設定が誤っている場合は、/etc/rndc.keyが存在していてもrndcに失敗する

/etc/rndc.confにするのか、/etc/rndc.keyにするのかは自由だが、リモート上にあるBINDを制御する場合は、
/etc/rndc.confとすること （ローカル上のBINDの制御であればどちらでも良い）

ファイルのアクセス権はrootのみ読み込みができるように変更をする

rndc実行時のオプションを使うことにより、/etc/rndc.confまたは/etc/rndc.key以外のファイルを使用することもできる

rndcが読み込むファイルの順序



各ファイルで使用するステートメント

/etc/rndc.conf

optionsステートメント	デフォルトで使用する共有鍵名と相手のホスト名を指定する
serverステートメント	デフォルトで指定した相手以外に対してもrndcを実行したい場合は、 serverステートメントを使用して、その相手のホスト名と使用する共有鍵名を指定する serverステートメントを省略した場合は、optionsで指定したデフォルトを対象とする
keyステートメント	共有鍵の設定

/etc/rndc.key

keyステートメント	共有鍵の設定

各ファイルでの書式

[/etc/rndc.confの書式]

```
options {
        default-server デフォルトの相手となるホスト名;
        default-key "デフォルトで使用する共通鍵名";
};

server rndcの対象となるホスト名 {
        key "使用する共通鍵名";
};

key "共通鍵名" {
        algorithm       hmac-md5;
        secret          "ベース64でエンコードされた共通鍵";
};
```

[/etc/rndc.keyの書式]

```
key "共通鍵名" {
        algorithm       hmac-md5;
        secret          "ベース64でエンコードされた共通鍵";
};
```

[/etc/rndc.confの場合の設定例]

# more /etc/rndc.conf 	
options {
　　default-server localhost;
　　default-key "rndckey";
};
 	
server localhost {
　　key "rndckey";
};
 	
key "rndckey" {
　　algorithm　　hmac-md5;
　　secret　　"NWteQWyWZBsI6T9W3srJ7bTPg5
ju3To8rfZj0sd0y3sD9cA7LNxB4sU9KxE7";
};
 	
# ls -l /etc/rndc.conf 	
-r-------- 1 root root 217　4月　7 10:49 /etc/rndc.conf
	optionsステートメントは必須
	
	serverステートメントは任意
	左記の場合だと、optionsと同じ内容なので
	省略しても問題ない
	
	keyステートメントは必須
	
	rootしか読み込みができようにアクセス権を変更する

[/etc/rndc.keyの場合の設定例]

# more /etc/rndc.key 	
key "rndckey" {
　　algorithm　　hmac-md5;
　　secret　　"NWteQWyWZBsI6T9W3srJ7bTPg5
ju3To8rfZj0sd0y3sD9cA7LNxB4sU9KxE7";
};
 	
# ls -l /etc/rndc.key 	
-r-------- 1 root root 217　4月　7 10:49 /etc/rndc.key
	keyステートメントは必須
	
	rootしか読み込みができようにアクセス権を変更する

③ namedサービス側の設定

named.confファイルで、以下の項目の設定を行う

ステートメント

keysステートメント	rndcを使う相手との間で使用する共通鍵の設定 複数設定可能 named.confにkeysステートメントを使ってキーを直接記載せずに、includeステートメントを使って、 外部ファイルに記載したkeysステートメントを読み込む方法もある
controlsステートメント	rndcによる制御を許可する相手と使用する共通鍵を設定 rndcを実行する相手ごとに異なる共通鍵を使用する場合は、複数設定する

[書式]

```
key "共通鍵名" {
　　algorithm　　hmac-md5;
　　secret　　"ベース64でエンコードされた共通鍵";
};

include "外部ファイル名";　　# 外部のファイルを読み込む場合

controls {
 inet nrdcを受け付けるインターフェースアドレス allow { 許可する相手; } keys { "使用する共通鍵名"; };
};
```

[外部ファイルを読み込む場合の設定例]

```
# more named.conf
:
include "/etc/rndc.key";
:
controls {
 inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndckey"; };
};
```

外部からkeyを読み込む場合

この場合はローカル(127.0.0.1)からのみrndcコマンドを受け付ける

```
# more /var/named/chroot/etc/rndc.key
key "rndckey" {
        algorithm       hmac-md5;
        secret          "NWteQWyWZBsI6T9W3srJ7bTPg5
ju3To8rfZj0sd0y3sD9cA7LNxB4sU9KxE7";
};
```

includeで読み込んでいるファイル

```
# ls -l /var/named/chroot/etc/rndc.key
-r-------- 1 named named 113  3月 23 15:22 /var/named/chroot/etc/rndc.key
```

外部ファイルから読み込む場合は、そのファイルはnamedサービスを実行するユーザのみ読み込みができるようにアクセス権を変更する

rndcの設定例

ここではローカルからのrndcのみ許可する設定を説明すると同時に、
rndcコマンドが読み込むファイルとnamedサービスが読み込むファイルが異なることを検証する

rndcが使用するファイルの作成

```
# ls -l /etc/rndc.key
-r-------- 1 root root 77  4月  1 14:01 /etc/rndc.key
```

rndcが使うファイル
rootしか読み込めないようにする
(一般ユーザがrndcを使えないようにする)

```
# more /etc/rndc.key
key "rndc-key" {
        algorithm hmac-md5;
        secret "171UOxgzl3zdljSaTD380Q==";
};
```

内容は共通鍵のみ
こちらの共通鍵名はrndc-keyとした

named.confの設定

```
# view /var/named/chroot/etc/named.conf
:
include "/etc/rndc.key.chroot";
:
:
controls {
 inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndckeys"; };
};
```

chroot環境下なので、実際は
/var/named/chroot/etc/rndc.key.chroot
(ファイル名は何でも良い)

アクセスできるのはローカルシステムのみ
使用する共通鍵名は、rndckeysにした
(/etc/rndc.keyと明確に区別するため)

```
# ls -l /var/named/chroot/etc/rndc.key.chroot
-r-------- 1 named named 77  4月  1 15:05 /var/named/chroot/etc/rndc.key.chroo
```

named.confが読み込むファイル
namedしか読み込めないようにする

```
# more  /var/named/chroot/etc/rndc.key.chroot
key "rndckeys" {
        algorithm hmac-md5;
        secret "171UOxgzl3zdljSaTD380Q==";
};
```

内容は共通鍵のみ
こちらの共通鍵名はrndckeys

rndcの確認

```
    # service named start                                   namedの起動
    named を起動中:                                [  OK  ]

    # rndc status                                           rndcが実行できることを確認
    version: 9.7.3 (Not available.)
    CPUs found: 1
    worker threads: 1
    number of zones: 21
    debug level: 0
    xfers running: 0
    xfers deferred: 0
    soa queries in progress: 0
    query logging is ON
    recursive clients: 0/2900/3000
    tcp clients: 0/100
    server is up and running

    # rndc reload                                           設定の再読み込みもできた
    server reload successful

    # service named stop                                    停止も正常にできた
    named を停止中:                                [  OK  ]  (rndcがおかしい場合は正常に終了できない)
```

リモートのnamedサービスを制御する

192.168.24.54のホスト上で動作するnamedサービスに対して、192.168.24.60からrndcコマンドの実行ができるようにする

192.168.24.54側の設定

```
# vi /var/named/chroot/etc/named.conf

acl localnet {                                              ACLの作成（任意）
        192.168.24.60;                                      ここでは192.168.24.60のみに指定
};

include "/etc/rndc.key.chroot";                             ローカルからのrndc用の設定ファイル

controls {
 inet 127.0.0.1 allow { 127.0.0.1; } keys { "rndckeys"; };
};

key "rndc-test" {                                           新しく追加したkey
        algorithm hmac-md5;                                 共有鍵名は、rndc-test
        secret "TUbsOzfVESkheH8Z2NDEbfEWKQaRt3WeVH7CCr4
AdVUmCuCp1drQPfHtnARtaCW62EZhgmkMJWkALU0XuhVDig==";
};

controls {                                                  localnetからのrndcを許可
 inet 192.168.24.54 allow { localnet; } keys { "rndc-test"; }   使用する共通鍵名は、rndc-test
};


# rndc reload                                               設定の再読み込み



# iptables -I INPUT 14 -s 192.168.24.60 -p tcp --dport 953 -j ACCEPT   192.168.24.60からのTCP953宛パケット
                                                            を許可する
# service iptables save
```

192.168.24.54側の設定

```
# vi /etc/rndc.conf
options {
        default-server localhost;
        default-key "rndckey";
};

server localhost {
        key "rndckey";
};

key "rndckey" {
        algorithm       hmac-md5;
        secret          "NWteQWyWZBsI6T9W3srJ7bTPg5ju3To8rfZ
j0sd0y3sD9cA7LNxB4sU9KxE7";
};

server 192.168.24.54 {
        key "rndckey2";
};

key "rndckey2" {
        algorithm       hmac-md5;
        secret          "TUbsOzfVESkheH8Z2NDEbfEWKQaRt3WeVH7CC
r4AdVUmCuCp1drQPfHtnARtaCW62EZhgmkMJWkALU0XuhVDig==";
};
```

192.168.24.54に対しては、rndckeysを使用

新しく追加したkey

確認

```
# rndc -s 192.168.24.54 status
version: 9.7.3 (Not available.)
CPUs found: 1
worker threads: 1
number of zones: 21
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is ON
recursive clients: 0/2900/3000
tcp clients: 0/100
server is up and running
```

デフォルト以外のホストを対象とするときは、
「-s ホスト名」オプションを使用する

rndc関係のトラブルシューティング

rndcが使用する、共通鍵が記述されたファイル(/etc/rndc.confまたは/etc/rndc.key)が見つからない

```
# rndc status
rndc: neither /etc/rndc.conf nor /etc/rndc.key was found

[ 対応 ]
/etc/rndc.keyまたは/etc/rndc.confを用意する
```

rndcが使用するkeyと対象のnamedサービスが使用するkeyが異なる

```
# rndc status
rndc: connection to remote host closed
This may indicate that the remote server is using an older version of
the command protocol, this host is not authorized to connect,
or the key is invalid.

[ 対応 ]
rndcが使用するkey(/etc/rndc.confまたは/etc/rndc.keyの中)とnamed.confの使用するkey(named.conf内か読み込んで
いる外部ファイル)の共通鍵(鍵名は不一致でも良い)を合わせる
```

rndcの設定がおかしいため、namedサービスが正常に終了できない

# service named stop named を停止中: .....[失敗]. [対応] namedを強制的に終了させ、rndc関係の設定を確認する [解決例] # ps -ef | grep named named 8344 1 0 13:59 ? 00:00:00 /usr/sbin/named -u named -4 -t /var/named/chroot	namedのプロセスを確認
# kill 8344	killコマンドで強制終了
# service named start named を起動中: [OK]	仮にすぐに起動させた場合は、起動するが・・
# service named status named が停止していますが PID ファイルが残っています	status情報がおかしい ここの灰色の部分は 検証のために行ったこと なのでやらないこと
# ps -ef | grep named named 9831 1 0 15:31 ? 00:00:00 /usr/sbin /named -u named -4 -t /var/named/chroot # more /var/run/named.pid 9136	起動中のnamedのプロセス番号と、named.pidに 登録されているプロセス番号が不一致するという 問題が発生する
# service named status rndc: connect failed: 127.0.0.1#953: connection refused named が停止していますが PID ファイルが残っています	killで終了した場合はまずはstatusを確認 rndc：connection～はnamedが停止のためなので無視
# more /var/run/named.pid	PIDファイルの確認（こちらはシンボリックリンク） 中身は空だがファイルは存在する（存在することが問題）
# more /var/named/chroot/var/run/named/named.pid	PIDファイルの確認（こちらは本体） 中身は空だがファイルは存在する（存在することが問題）
# rm /var/named/chroot/var/run/named/named.pid	PIDファイルの削除
# rm /var/run/named.pid rm: remove シンボリックリンク `/var/run/named.pid'? y	同上
# service named status rndc: neither /etc/rndc.conf nor /etc/rndc.key was found named は停止していますがサブシステムがロックされています	（2重起動防止のための）ロックファイルが 残っているのでまだ起動できない
# ls -l /var/lock/subsys/named -rw-r--r-- 1 root root 0 4月 1 13:08 /var/lock/subsys/named	ロックファイルが存在する
# rm /var/lock/subsys/named rm: remove 通常の空ファイル `/var/lock/subsys/named'? y	ロックファイルの削除
# service named status rndc: connect failed: 127.0.0.1#953: connection refused named は停止しています rndcの設定を確認後、namedサービスを起動させる	エラーが出なくなった