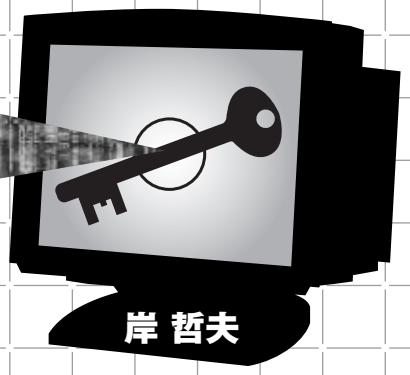
IPsecのインストールとベンチマーク

IPsecによる暗号化通信の実装（後編）



岸 哲夫

本稿では，データ通信の暗号化を行うためのしくみであるIPsecを，Linuxカーネル2.6で利用するための手順について解説する．先月号（2009年1月号，pp.160-165）では暗号通信の必要性とIPsecの概要について説明した．今回はIPsecの接続を実際に試してみる．
（編集部）

リスト1　/boot/grub/grub.conf（変更前）

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol00
#          initrd /initrd-version.img
#boot=/dev/hda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Fedora Core (2.6.22.14-72.fc6)
        root (hd0,0)
        kernel /vmlinuz-2.6.22.14-72.fc6 ro root=/dev/VolGroup00/LogVol00 rhgb
quiet
        initrd /initrd-2.6.22.14-72.fc6.img
title Fedora Core (2.6.18-1.2798.fc6)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-1.2798.fc6 ro root=/dev/VolGroup00/LogVol00 rhgb
quiet
        initrd /initrd-2.6.18-1.2798.fc6.img
[root@localhost grub]#
```

リスト2　/boot/grub/grub.conf（変更後）

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol00
#          initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title SELinux
kernel (hd0,0)/vmlinuz-2.6.18-1.2798.fc6 ro root=/dev/VolGroup00/LogVol00 rhgb
quiet selinux=1 ←追加する
 initrd /initrd-2.6.18-1.2798.fc6.img
```

```
selinux_register_security:  Registering secondary module capability
audit(1227781227.932:2): selinux=0 auid=4294967295
```

図1　非IPsecパソコンでのdmesg

```
selinux_register_security:  Registering secondary module capability
SELinux: initialized (dev selinuxfs, type selinuxfs), uses genfs_contexts
```

図2　IPsecパソコンでのdmesg

1．IPsecのインストール

● IPsecの有効化

IPsecをインストールするためにまずやることは，Linux上でIPsecを有効にして起動することです．最初にLinux起動時のブート・ローダであるGRUBのパラメータを設定します．GRUBの場合，パラメータをgrub.confに追加するだけです．

/boot/grub/grub.confの中身は，**リスト1**のようになっています．変更後は**リスト2**のようになります．selinux=1というパラメータを追加しただけです．

再起動して確認しましょう．非IPsecパソコンは，dmesg¦grep selinuxというコマンドを入力すると，**図1**のようになります．同じく，IPsec設定後のものはdmesg¦grep selinuxというコマンドを入力すると，**図2**のようになります．

今までの説明，カーネル2.6でGRUBにselinux＝1のパラメータを設定した場合です．

再起動した後にgetenforceとコマンドを打鍵すると，非IPsecのパソコンは**図3**のようになります．同じく，IPsecのパソコンは**図4**のようになります．上のパラメータは，/etc/sysconfig/selinuxに記述してあるので，それを変更することもできます（**図5**）．

図3
非IPsecパソコンでのgetenforce

```
[root@localhost ~]# getenforce
Disabled
[root@localhost ~]#
```

図4
IPsecパソコンでのgetenforce

```
[root@localhost ~]# getenforce
Enforcing
[root@localhost ~]#
```

Enforcingになる

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - SELinux is fully disabled.
SELINUX=enforcing
# SELINUXTYPE= type of policy in use. Possible values are:
#       targeted - Only targeted network daemons are protected.
#       strict - Full SELinux protection.
SELINUXTYPE=targeted
```

図5　/etc/sysconfig/selinux

デスクトップ環境としてGNOMEを利用している場合は，メニューのシステム→管理→セキュリティレベルとファイアウォール画面でも変更可能です．

● 試験環境の説明

図6に，試験環境となるFedora8がインストールされたパソコン（サーバとして使用，IPアドレス：192.168.0.29）のcpuinfoを，**図7**にもう1台のFedora8がインストールされたパソコン（クライアント，192.168.0.27）のcpuinfoを示します．クライアントのクロック周波数は700MHzで，10年前の最新型といったところです．組み込み用途では非力なCPUを使うことも多いので，あえて遅めのマシンを利用しています．

● IPsecの設定ファイルの作成

サーバの/etc/sysconfig/network-scripts/ifcfg-ipsec0というファイルを**リスト3**のような内容で作成します．/etc/sysconfig/network-scripts/keys-ipsec0には，**リスト4**のようにpre-sahred keyとしてharahireが入っています．/etc/racoon/racoon.confには**リスト5**のようなパラメータが，/etc/racoon/psk.txtには**リスト6**のようなパラメータが入っています．

もちろん，クライアント側も同じように設定します．宛先のIPアドレスは，サーバ（192.168.0.29）に設定してください．

```
# cat /proc/cpuinfo
processor       : 0
vendor_id       : AuthenticAMD
cpu family      : 6
model           : 8
model name      : AMD Athlon(tm)
stepping        : 0
cpu MHz         : 1252.855
cache size      : 256 KB
fdiv_bug        : no
hlt_bug         : no
f00f_bug        : no
coma_bug        : no
fpu             : yes
fpu_exception   : yes
cpuid level     : 1
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic
mtrr pge mca cmov pat pse36 mmx fxsr sse syscall mmxext
3dnowext 3dnow up ts
bogomips        : 2507.99
```

図6　サーバのcpuinfo

```
# cat /proc/cpuinfo
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 8
model name      : Celeron (Coppermine)
stepping        : 6
cpu MHz         : 701.634
cache size      : 128 KB
fdiv_bug        : no
hlt_bug         : no
f00f_bug        : no
coma_bug        : no
fpu             : yes
fpu_exception   : yes
cpuid level     : 2
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 mtrr
pge mca cmov pat pse36 mmx fxsr sse up
bogomips        : 1404.62
```

図7　クライアントのcpuinfo

リスト3
/etc/sysconfig/network-scripts/ifcfg-ipsec0

```
DST=192.168.0.27
TYPE=IPSEC
ONBOOT=yes
IKE_METHOD=PSK
```

2．IPsecの起動とテスト

● 設定後のIPsecを起動

次のようにコマンドを入力すると，IPsecが起動します．

```
ifup ipsec0
```

起動した後にsetkeyコマンドでIPsecのパラメータを確

リスト4　/etc/sysconfig/network-scripts/keys-ipsec0

```
# cat /etc/sysconfig/network-scripts/keys-ipsec0
IKE_PSK=harahire
#
```