jail 仮想 OS 技術による管理者教育環境の構築

総合情報基盤センター　布村 紀男
nori2@cns.toyama-u.ac.jp

受講者全員に管理者権限を与えたサーバ演習を行うために、受講者１人１人にサーバを準備するのは、コストや場所的な問題もあって現実的ではない。一方、受講者全員がノートパソコンなどを持っており、管理者権限をあらかじめ有しているのであれば悩むことはないことであるが、それを強制できないのが現状である。そういった問題の解決策のひとつとして、複数台数のサーバを準備することなく、１台のサーバ上に複数の仮想サーバを構築する技術を検討した。本稿では、FreeBSD でサポートされている jail 仮想 OS 技術を使った事例について紹介いたします。

１　はじめに

2004 年度後期より、「情報通信ネットワーク演習」を担当することになった。受講者数は、当初、十数人程度だということだったので、４人１組ぐらいのグループ構成でサーバ１台を提供し、小規模ネットワーク、サーバ構築、管理、運用を含めたより実践的なネットワーク演習を予定していた。その予想に反して、受講者数は 30 人を越えたため、相当数のハードウェアの準備はできなくなり、仕方なく、総合情報基盤センター3F の端末室の PC を使用した演習を行うことになった。

3F の端末室は、ネットワークの設定などは、管理者権限でなくては行えないようになっている。一般ユーザでは、設定されている内容を表示はできるが、変更することはできないと言った状況である。まして、サーバソフトウェアのインストールはできない。何とか管理者権限を受講者各自に与え、しかもサーバ環境を提供する方向を検討した。まず、思い浮かんだのは、各自が持っている PC を持ち込み、設定をしてもらう。しかし、現実的には、自分専用の PC ではなかったり、持ち込み PC に対するセキュリティの保証はできないので、これは今回はあきらめざるを得なかった。また、Knoppix,FreeSBIE といった LiveCD を利用する方法が考えられる。しかし、この方法は CD ブートできる環境がないと利用はできない。センター3F の端末室は、CD ブートできる環境ではないので、これも選択肢から消去ということになりました。いろいろと悩んだあげく最終的に、自分の勉強も兼ねて、FreeBSD で実装されている jail による仮想サーバを構築することにした。

２　jail とは、

jail 環境は、１つの IP アドレスを持つネットワーク的に独立したホストとして機能させることができ、１台のマシン上で複数のサーバホストを稼動することができます。

UNIX 系の OS には、昔から chroot というコマンドがあります。chroot コマンドを使用することにより、ルートディレクトリを変更してコマンドを実行できます。コマンドを任意のディレクトリの下に閉じ込めてファイルへのアクセスを制限することができます。jail は、この chroot 機能を拡張して、ネットワーク機能を隔離できるようにした FreeBSD に実装されている仕組みです。似たような仮想サーバを作る技術として、Linux の User Mode Linux(UML)や商用製品では、VMware などがあります。ただし、それらの仮想 OS 技術とは異なり、プロセス自体はホストマシンのカーネルによって動作するため、仮想マシンとして動作する OS は FreeBSD に限られてしまいます。

演習環境の仮想サーバは、同一 OS であっても問題ないと考えたので、jail による複数の仮想サーバを構築することにしました。

３　jail 環境の構築

jail 環境の概念図を図-1 に示します。
今回は予算がなかったので５万円の手作り PC を使って、PC-UNIX サーバに仕立てました。

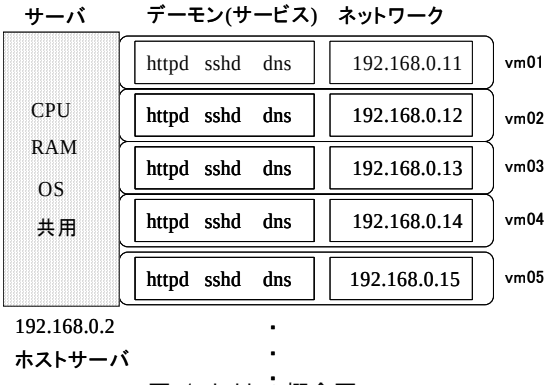

図-1 jail の概念図

3.1 jail 環境作成のシステム構成

◇ハードウェアおよびソフトウェアの仕様

1) ハードウェア

CPU: Celeron D 2.6GHz

メモリ: 512MB

HDD: 120GB

ネットワークインターフェース

100Base-TX

2)ソフトウェア

OS: FreeBSD 5.3

Web サーバ: Apache1.3.33

SSH サーバ: OpenSSH 3.9

テキストエディタ: pico

◇ネットワーク構成

1) IP アドレス

(ホスト環境)192.168.0.2

(jail 環境) 192.168.0.11～ 192.168.0.46

2)サブネットマスク 255.255.255.0

192.168.0.1

3) ゲートウェイ 192.168.0.1

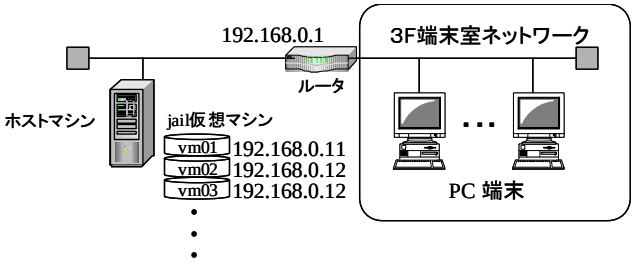

図-２ネットワーク構成図

3.2 jail 環境作成

標準的な jail 環境の作り方は、オンラインマニュアル jail(8)に構築方法が説明されているので、それを参考にして作業を行った。手動で 35 人分の jail 環境を作成するのは、効率が悪いので、以下のスクリプト (mkjail.sh) を準備して 35 個の jail 環境を作成した。ホスト名は vm01～vm35 としました。

```
#!/bin/sh
for i in `cat num.txt`
do
  JDIR=/home/vm$i
  cd /usr/src
  mkdir -p $JDIR
  make world DESTDIR=$JDIR
  cd /usr/src/etc
  make distribution DESTDIR=$JDIR
  mount_devfs devfs $JDIR/dev
  cd $JDIR
  ln -sf dev/null kernel
  mkdir $JDIR/stand
  cp /stand/sysinstall $JDIR/stand/
done
```

リスト-1 mkjail.sh

num.txt の中身は、

```
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
31 32 33 34 35
```

である。ユーザ登録は、受講者 35 人分を

```
ユーザ名:パスワード
```

の:区切りのファイルを作成し、リスト-2 のシェルスクリプトにより登録を行った。

3.3 jail 環境設定

作成された jail 環境を整備するため、以下に示す作業を行う必要がある。(リスト-3 参照)

1)空の/etc/fstab を作成

※起動時のメッセージを抑制するため

2)jai 環境/etc/rc.conf を作成

※リスト-4 参照

3)/etc/resolv.conf の設定

※仮想ＯＳ内から名前解決ができるように

4)root パスワードの定義

※仮想ＯＳ内から管理者を定義するため

5)タイムゾーンを定義する

※仮想ＯＳ内のタイムゾーンを定義するため

6)必要プログラムの導入

※(エディタ pico,インストーラ)

```
#!/bin/sh
PW=/usr/sbin/pw
UHOME=/home
SKEL=/etc/skel/*
while read LINE ; do
  LOGIN=`echo $LINE|cut -f 1 -d :`
  PASSWD=`echo $LINE|cut -f 2 -d :`
  HOMEDIR=$UHOME/$LOGIN
  echo -n creating $LOGIN :
  echo $PASSWD|$PW useradd $LOGIN -h0
  RETVAL=$?
  if [ $RETVAL -eq 0 ]; then
    mkdir -p 0755 $HOMEDIR && ¥
    cp -r $SKEL $HOMEDIR/ && ¥
    chown -R $LOGIN:$LOGIN $HOMEDIR && ¥
    echo OK
  else
    echo NG ($RETVAL)
    exit $RETVAL
  fi
done
exit 0
```

リスト-2 ユーザ登録スクリプト

```
#!/bin/sh
for i in `cat num.txt`; do
# JDIR is jail directory
JDIR=/home/vm$i
cp /etc/resolv.conf $JDIR/etc/
cp /etc/hosts $JDIR/etc/
cp -Rp /usr/share/zoneinfo/Asia/
Tokyo $JDIR/etc/localtime
touch $JDIR/etc/fstab
cp -p /root/rc.conf.jail
$JDIR/etc/rc.conf
cp /root/pkg_apache/* $JDIR/root/
mkdir $JDIR/usr/local/bin
cp -p /usr/local/bin/pico
$JDIR/usr/local/bin/
done
```

リスト-3 jail 環境設定

```
  network_interfaces=""
  portmap_enable="NO"
  inetd_enable="NO"
  syslogd_flags="-ss"
  sshd_enable="YES"
  sendmail_enable="NONE"
```

リスト-4 jail 環境の/etc/rc.conf

3.4 jail 仮想 OS の起動と停止

jail 内の proc ファイル、デバイスファイルのマウントを行った後,jail コマンドで起動を行う (図-3)。

```
# mount_devfs devfs /home/vm36/dev
# mount -t procfs proc /home/vm36/proc
# jail /home/vm36 vm36 192.168.0.46
 /bin/sh /etc/rc
```

図-3 jail 環境内でのシェル起動

```
Loading configuration files.
vm36
Setting hostname: vm36.
ln: /dev/log: Operation not permitted
Starting syslogd.
ELF ldconfig path: /lib /usr/lib
 /usr/lib/compat /usr/local/lib
out ldconfig path: /usr/lib/aout
/usr/lib/compat/aout
Starting local daemons:.
Updating motd.
Starting sshd.
Starting cron.
Local package initialization:
```

図-4 jail 起動時の状況

```
#!/bin/sh
for i in `cat num.txt`
do
  mount_devfs devfs /home/vm$i/dev
  mount -t procfs proc /home/vm$i/proc
  echo "vm$i mount"
  sleep 1
done
```

リスト-5 proc,デバイスファイルマウントスクリプト

jail 仮想 OS の起動プロセスは、ホスト環境から jls コマンドで確認できます（図-5)。

```
# jls
JID  IPAddress  Hostname  Path
1  192.168.0.46    vm36   /home/vm36
```

図-5 jls コマンド

jail 仮想 OS の停止は、killall コマンドに-j オプション プロセス ID を指定して行います。

```
# killall -j 1
```

図-6 killall コマンドによる停止

４　jail 環境への各ユーザのリモートログイン

実際の授業では、30 名が同時にホスト環境へ SSH でログインしただけで、メモリ、CPU の負荷が増大したため、１５人ずつ作業してもらうことにしました。ホスト環境から再度、各 jail 環境に SSH でログインして、Web サーバプログラムのインストール・設定、起動、テストを行いました。Web サーバの動作確認は、ホスト環境より telnet コマンドによる確認と w3m というテキストベースの web ブラウザで表示を確認してもらいました。受講者には、ホスト環境と仮想環境である jail 環境の違いを認識してもらえず、戸惑うこともありましたが、何とか演習を行うことができました。

```
> ssh nuno@vm36
Password:
Welcome to FreeBSD!
> hostname
vm36
> su -
Password:
vm36# hostname
vm36
```

図-7 ホスト環境から jail 環境への SSH ログイン

５　まとめ

・FreeBSD の jail 仮想 OS を使ってサーバ管理者教育環境の構築を試みた。

・今回は、ホスト環境を１台しか準備できなかったが、１５人程度であれば jail 仮想 OS 上で、実習が行えることがわかった。

```
vm36# ps ax |more
  PID  TT  STAT      TIME COMMAND
 5145  ??  SsJ    0:00.00 /usr/sbin/syslogd -ss
 5197  ??  IsJ    0:00.00 /usr/sbin/sshd
 5204  ??  IsJ    0:00.00 /usr/sbin/cron -s
 5219  ??  IsJ    0:00.03 sshd: nuno [priv] (sshd)
 5222  ??  RJ     0:00.02 sshd: nuno@ttyp1 (sshd)
 5223  p1  SsJ    0:00.02 -tcsh (tcsh)
 5227  p1  SJ     0:00.01 su -
 5228  p1  SJ     0:00.02 -su (csh)
 5231  p1  R+J    0:00.00 ps ax
 5232  p1  S+J    0:00.00 more
```

図-8 jail 環境での Web サーバ設定確認と起動

```
vm36# /usr/local/sbin/apachectl configtest
Syntax OK
vm36# /usr/local/sbin/apachectl start
/usr/local/sbin/apachectl start: httpd
started
```

図 9 jail 環境での Web サーバ設定確認と起動

６　さいごに

今回、事前の動作確認を十分に行えなかったことが第１の反省点です。１台のサーバに複数の jail 仮想 OS を構築し、これに 30 人程度の管理者教育用環境を提供するという、当初は無謀な試みだったと思ったが、実際にはなんとか演習を遂行できた。時間の都合上、検証できなかったが User Mode Linux(UML)も使って１台で複数仮想ＯＳ環境を作り、管理者権限を与えた場合も３０人程度の教室規模で全員が一斉に使うと、今回の場合と同様にホストマシンのスペックを考慮しないと、ホストマシンに過度の負荷がかかることが予想されるので、負荷が集中しないように時間をずらして使用するなどの工夫が必要になるだろう。

７　参考文献

[1] 第 3 特集「仮想環境によるシステム構築術」
UNIX USER　2003 年 10 月号

[2] 中満英生「FreeBSD でサーバを作ろう」（インストールから要塞化まで）
FreeBSD Expert 2004 p136-p144

[3] おおつねまさふみ「Expert な jail 環境構築のポイント」
FreeBSD Expert 2005 p77-p86