Subject: Lecture on Operating System Lecture Exercise 11.3
From: IKENOYA Katsutoshi <j05002@ie.u-ryukyu.ac.jp>
Date: Tue, 13 Feb 2007 21:19:25 +0900
To: Shinji KONO <kono@ie.u-ryukyu.ac.jp>

学籍番号：055702B

・修正点

/dev/memを採用していないOSの場合を追加

問題11.3

Unix では、top という命令で他のプロセスに関する情報を得ることができる。
top は、システムの任意のメモリにアクセスすることができる/dev/mem に
アクセスすることによって情報を得ている。
/dev/mem のユーザID，グループIDに関して考察せよ。

lsで/dev/mem，/dev/kmemを見てみた。

```
[j05002@~]% ls -l /dev | grep mem
crw-r----- 1 root kmem 3, 1 Jan 26 00:49 kmem
crw-r----- 1 root kmem 3, 0 Jan 26 00:49 mem
```

/dev/memにアクセスすることによってコンピュータの任意の
メモリアドレスに対して読み書きを行うことができる。
/dev/kmemはカーネルの仮想記憶にアクセスすることができる。
もしこのメモリデバイスにアクセスできるならばシステムの
メモリ上にあるプログラム、データ、ステータス情報などに
アクセス可能となる。そのため普通はrootしか読み書きできず、
またkmemグループは読むことだけしかできない。
しかし、topコマンドは/dev/memにアクセスすることによって情報
を得ている。
ここで、ls で topコマンドと、psコマンドと、suコマンドを見てみた。

```
[j05002@~]% ls -l /usr/bin/top
-rwsr-xr-x   1 root     wheel       83088 Jan 30  2006 /usr/bin/top*
[j05002@~]% ls -l /bin/ps
-rwsr-xr-x   1 root     wheel       31932 Jan 31  2006 /bin/ps*
[j05002@~]% ls -l /usr/bin/su
-r-sr-xr-x   1 root     wheel       19588 Jan 31  2006 /usr/bin/su*
```

結果を見ると、topやpsのグループはwheelになっており、wheelはsuコマン
ドの所有者であるため、スーパーユーザーとなり、/dev/memにアクセスすること
ができる。

また、/dev/memを採用していないOSでは、/proc にある仮想ファイルを読み込ん
で動作する。この場合、 ps は kmem に suid する必要はなく、動作にいかなる
特権も必要としない。
*/proc/*プロセスID/の下にあるファイルにプロセスごとの状態が表示され、psは
この値を見てプロセス状態を表示している。
さらに、top も、 /proc にマウントされたproc ファイルシステムのファイルを
読み込んで動作する。 /proc がマウントされていないと、 top は動作しない。
/etc/toprc によって特権のないユーザーに対して top の利 用をセキュアモー
ドに制限することができる。
システムの設定ファイルはtopによって作成されない。
逆に、ユーザーがこのファイルを手動で作成し、/etc ディレクトリに置く。
以下は/procと、/proc/2287をlsしたときの結果の抜粋である。

```
[j05002@pw002 ~]% ls -l /proc/
省略
```

```
dr-xr-xr-x    3 j05002   y05j            0 Feb 11 15:25 2287/
dr-xr-xr-x    3 j05002   y05j            0 Feb 11 15:25 2288/
dr-xr-xr-x    3 j05002   y05j            0 Feb 11 15:25 2360/
dr-xr-xr-x    3 j05002   y05j            0 Feb 11 15:25 2365/
省略
[j05002@pw002 ~]% ls -l /proc/2287/
ls: /proc/2287/cwd: 許可がありません
ls: /proc/2287/root: 許可がありません
ls: /proc/2287/exe: 許可がありません
合計 0
-r--r--r--    1 root     root            0 Feb 11 15:26 cmdline
lrwxrwxrwx    1 root     root            0 Feb 11 15:26 cwd
-r--------    1 root     root            0 Feb 11 15:26 environ
lrwxrwxrwx    1 root     root            0 Feb 11 15:26 exe
dr-x------    2 root     root            0 Feb 11 15:26 fd/
-r--r--r--    1 root     root            0 Feb 11 15:26 maps
-rw-------    1 root     root            0 Feb 11 15:26 mem
-r--r--r--    1 root     root            0 Feb 11 15:26 mounts
lrwxrwxrwx    1 root     root            0 Feb 11 15:26 root
-r--r--r--    1 root     root            0 Feb 11 15:26 stat
-r--r--r--    1 root     root            0 Feb 11 15:26 statm
-r--r--r--    1 root     root            0 Feb 11 15:26 status
```