ネットワークセキュリティ演習

2回 ファイルシステムのセキュリティ

i-node情報を得る

```
$ df -i
Filesystem       Inodes  IUsed    IFree IUse% Mounted on
/dev/nvme0n1p2 15237120 300087 14937033    2% /
#                                          消費量２%
# testというファイルに対して
$ ls -li
11281969 -rw-rw-r-- 1 cafe cafe    0  9月 30 20:29 test
# inode番号

$ stat test
  Size: 0             Blocks: 0          IO Block: 4096
Device: 10302h/66306d   Inode: 11281969    Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/    cafe)   Gid: ( 1000/    cafe)
Access: 2018-09-30 20:29:36.844532115 +0900
Modify: 2018-09-30 20:29:36.844532115 +0900
Change: 2018-09-30 20:30:14.012683244 +0900
```

LinuxのユーザIDとグループID

```
# 私は誰？
$ whoami
kindai
# ユーザ情報の表示
# id ユーザ名

# id kindai
uid=1000(kindai) gid=1000(kindai)
```

ユーザやグループの追加と削除

```
# ユーザの追加（ホームディレクトリも作成）
# $ sudo adduser ユーザ名
$ sudo adduser user1

ユーザー `user1' を追加しています...
新しいグループ `user2' (1002) を追加しています...
新しいユーザー `user1' (1001) をグループ `user2' に追加しています...
ホームディレクトリ `/home/user1' を作成しています...
`/etc/skel' からファイルをコピーしています...
新しい UNIX パスワードを入力してください:
新しい UNIX パスワードを再入力してください:
passwd: パスワードは正しく更新されました
user2 のユーザ情報を変更中
新しい値を入力してください。標準設定値を使うならリターンを押してください
    フルネーム []:
    部屋番号 []:
    職場電話番号 []:
    自宅電話番号 []:
    その他 []:
以上で正しいですか? [Y/n]

#  ユーザの削除
# $ sudo deluser ユーザ名
$ sudo deluser user1

# グループの追加
# $ sudo addgroup グループ名
$ sudo addgroup group1


# グループの削除
# $ sudo delgroup グループ名
$ sudo delgroup group1
```

ユーザ情報の修正

```
# ユーザに副グループを追加
# $ sudo usermod –aG グループ名　ユーザ名
$ sudo adduser user2
$ sudo addgroup group2
$ sudo usermod -aG group2 user2

# ユーザにプライマリグループを変更
# $ sudo usermod -g グループ名　ユーザ名
$ sudo addgroup joho
$ sudo usermod -g joho user2

# 修正の確認
$ id user2
```

ファイルのパーミッションの変更

```
# 新規ファイルの作成
$ touch test
$ ls -l test
-rw-rw-r-- 1 kindai kindai    0 10月  1 00:14 test

$ chmod 775 test

$ ls -l test
-rwxrwxr-x 1 kindai kindai    0 10月  1 00:14 test
```

passwd コマンド

```
# ユーザがパスワードを設定する／変更する
$ passwd
kindai 用にパスワードを変更中
現在の UNIX パスワード:
新しい UNIX パスワードを入力してください:
```

/etc/passwd ファイル

```
# passwd ファイルのパーミッションの確認
$ ls -l /etc/passwd
-rw-r--r-- 1 root root 2555  9月  3 16:51 /etc/passwd
```

passwdコマンドのパーミッションの確認

```
$ $ which passwd
/usr/bin/passwd
cafe@techcafe:~$ ls -l /usr/bin/passwd
-rwsr-xr-x 1 root root 59640  1月 26  2018 /usr/bin/passwd
```

ファイルの所有者やグループの変更　chown コマンド

```
# chown ユーザ名:グループ名　ファイル名／ディレクトリ名

$ sudo chown nobody: test
$ ls -l test
-rwxrwxr-x 1 nobody nogroup 0 10月  1 00:14 test
```

ユーザの切り替えと復帰

```
$ sudo adduser fujio
# パスワードなどの入力

$ su fujio

# ユーザを切り替える

$ exit

# もとのユーザに戻る
```

ファイルシステムのアクセス制御の実験

確認事項

1. 実験環境の準備（ユーザとグループの作成）
2. ファイルのパーミッションによるアクセス制御
3. ディレクトリのパーミッションによるアクセス制御
4. Stickyビットによる削除権限の制限
5. umaskによる新規ファイルのパーミッションの確認
6. 後始末

手順１ 実験環境の準備

1. ユーザーをつくる

学生（2）、教員（2）、一般人（1）

```
$ sudo adduser gakusei1
$ sudo adduser gakusei2
$ sudo adduser kyoin1
$ sudo adduser kyoin2
$ sudo adduser ippanjin

# 確認
$ id gakusei1
$ id gakusei2
$ id kyoin1
$ id kyoin2
$ id ippanjin
```

2. グループをつくる

   学生、教員、管理者

```
$ sudo addgroup student
$ sudo addgroup teacher
$ sudo addgroup manager
```

3. ユーザのプライマリグループを設定する

   学生（2）、教員（2)

```
$ sudo usermod -g student gakusei1
$ sudo usermod -g student gakusei2
$ sudo usermod -g teacher kyoin1
$ sudo usermod -g teacher kyoin2
```

4. ディレクトリをつくる

   - 学生用
   - 教員用
   - 管理者用
   - 共用（だれもが書き込める）

```
$ cd /tmp
# 演習用のディレクトリを作成する
$ mkdir enshu
$ cd enshu
$ mkdir for_students
$ mkdir for_teachers
$ mkdir for_managers
$ mkdir for_public

#確認
$ ls -l
```

グループ所有者の変更

```
$ sudo chown :studet for_students
$ sudo chown :teacher for_teachers
$ sudo chown :manager for_managers

#確認
$ ls -l
```

手順２ファイルのパーミッションによるアクセス制御

プライマリグループによるアクセス制御の実験

1. kyoin1（教員）でファイルの作成

   （kyoin1 にユーザ切り替え）

```
$ su kyoin1

# ユーザが切り替わる
```

2. パーミッションの設定

   （教員グループのみ読み書き可） seisekiファイルの作成

```
$ cd /tmp/enshu/for_teachers
$ touch seiseki
# エディターでseisekiファイルを修正
$ nano seiseki

# yamasaki 60

$ ls -l seiseki
$ chmod 660 seiseki

#確認
$ cat seiseki
```

3. gausei1（学生）でログインし、seiseki ファイルにアクセス

   別ウィンドウ

```
$ su gakusei

$ cd /tmp/enshu/for_teachers

#確認
$ cat seiseki

# アクセスできないことを確認
```