

오픈소스프로그래밍

Dong-Geol Choi

Information and Communication Engineering

Hanbat National University



파일 접근 권한 관리하기



목차

1. 파일의 속성
2. 파일의 접근 권한
3. 기호를 이용한 파일 접근 권한 변경
4. 숫자를 이용한 파일 접근 권한 변경
5. 기본 접근 권한의 설정



학습목표

- 파일의 속성과 접근 권한의 개념을 이해한다.
- 접근 권한을 변경하는 방법을 익힌다.
- 접근 권한을 상속하고 초기에 설정하는 방법을 익힌다.



01. 파일의 속성

❖ 다중 사용자 시스템의 특징

- 여러 사람이 하나의 시스템 사용
- 다른 사람이 내 파일을 읽거나 수정, 삭제 할 수 없도록 보안 필요
- 다른 사용자의 무단 접근으로부터 자신의 파일을 보호하는 기능으로 파일에 접근 권한을 부여하여 권한 만큼만 파일을 사용

❖ 파일의 속성

- 파일 종류
- 파일 접근 권한
- 하드 링크 개수
- 파일 소유자의 사용자 이름
- 파일이 속한 그룹 이름
- 파일 크기
- 파일의 마지막 수정 일시



01. 파일의 속성

❖ 파일의 속성

- 유닉스에서 파일을 관리하기 위해 저장하는 정보들
- `ls -l` 명령으로 파일 속성을 확인할 수 있음

```
root@d649e90df62b:/workspace/test# ls -l
total 4
-rw-r--r-- 1 root root 6 Apr 16 06:58 test.txt
```

표 6-1 파일의 속성

| 번호 | 속성 값 | 의미 |
|----|--------------|-------------------------------|
| 1 | - | 파일 종류(- : 일반 파일, d : 디렉토리) |
| 2 | rw-r--r-- | 파일을 읽고, 쓰고, 실행할 수 있는 접근 권한 표시 |
| 3 | 1 | 하드 링크 수 |
| 4 | root | 파일 소유자의 로그인 ID |
| 5 | root | 파일 소유자의 그룹 이름 |
| 6 | 6 | 파일의 크기(바이트 단위) |
| 7 | Apr 16 06:58 | 파일이 마지막으로 수정된 일시 |
| 8 | test.txt | 파일명 |



01. 파일의 속성

❖ 파일의 속성

▪ 파일 종류

| 문자 | 파일 유형 |
|----|--------------------------|
| - | 일반 (정규) 파일 |
| d | 디렉토리 파일 |
| b | 블록 단위로 읽고 쓰는 블록 장치 특수 파일 |
| c | 문자 단위로 읽고 쓰는 문자 장치 특수 파일 |
| l | 심볼릭 링크 파일 |
| p | 파이프 |
| s | 소켓 |

file 파일명

```
user1@Solaris11:~/Unix/ch6$ mkdir temp
user1@Solaris11:~/Unix/ch6$ file first.dat temp
first.dat:      ascii text
temp:          directory
user1@Solaris11:~/Unix/ch6$
```



01. 파일의 속성

❖ 파일의 속성

- 파일이 속한 그룹 이름

groups [사용자명]

사용자명 지정한 경우

-> 인자로 지정한 사용자가 속한 그룹 이름 출력

인자가 없으면

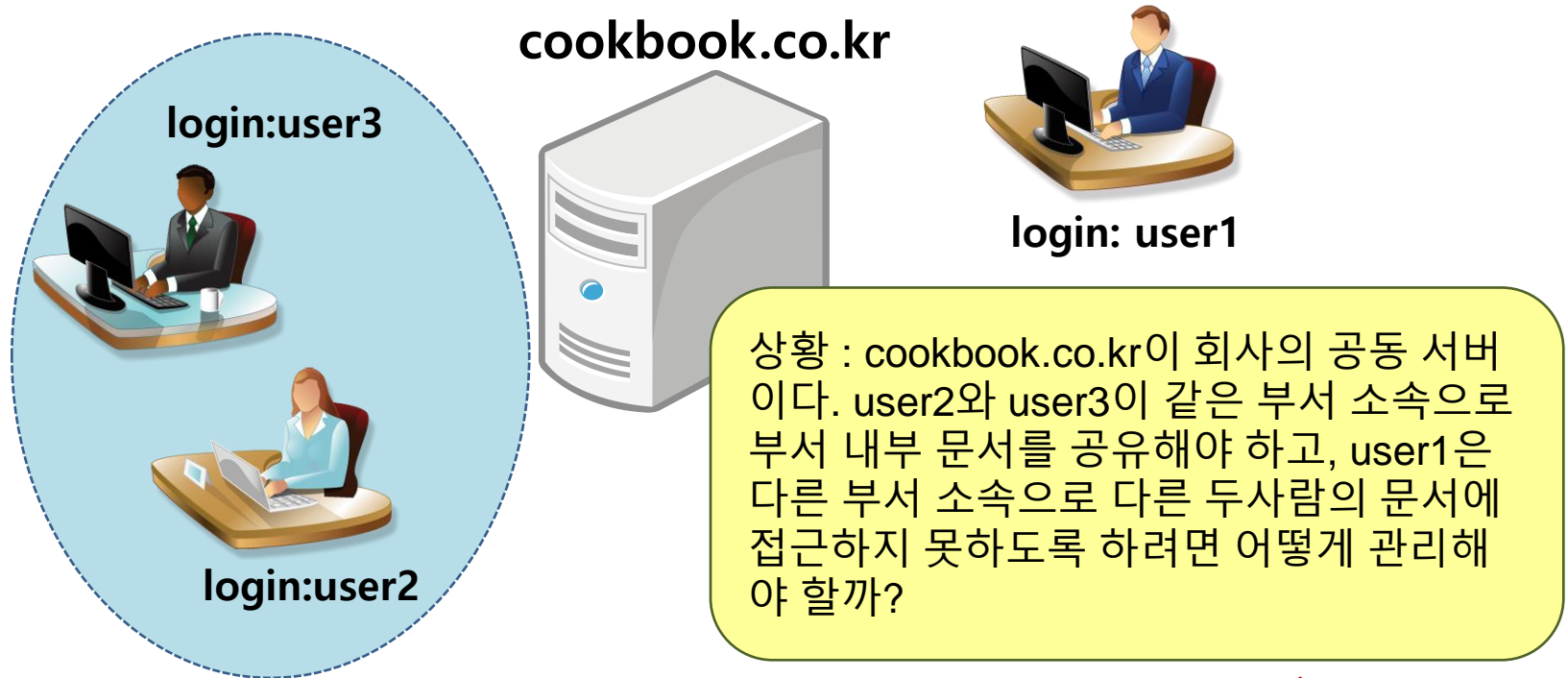
-> 자신이 속한 그룹 이름 출력

```
user1@Solaris11:~/Unix/ch6$ groups
staff
user1@Solaris11:~/Unix/ch6$ groups root
root other bin sys adm mail tty lp daemon
user1@Solaris11:~/Unix/ch6$
```



02. 파일의 접근 권한

- ❖ 파일을 읽고, 쓰고, 실행할 수 있는 권한
- ❖ 다중 사용자 시스템의 가장 기본적인 보안 기능



➡ 접근 권한



02. 파일의 접근 권한

❖ 유닉스의 사용자 카테고리

- **소유자**
 - 일반적으로 파일을 생성한 사용자. 명령을 통해 변경할 수도 있음
- **그룹**
 - 파일과 동일한 그룹에 속한 사용자들.
 - 파일이 속한 그룹?
 - 일반적으로 파일을 생성한 사용자의 기본 그룹
 - 상위 디렉토리에 특수한 권한(setgid)이 부여된 경우 다른 그룹으로 지정
 - 명령을 이용하여 변경 가능
- **기타 사용자**
 - 소유자나 그룹 카테고리에 속하지 않은 모든 사용자들

❖ 접근 권한은 카테고리 별로 다르게 부여



02. 파일의 접근 권한

❖ 기본 권한

- 읽기(r), 쓰기(w), 실행(x)
- 파일의 종류에 따라 의미 다름

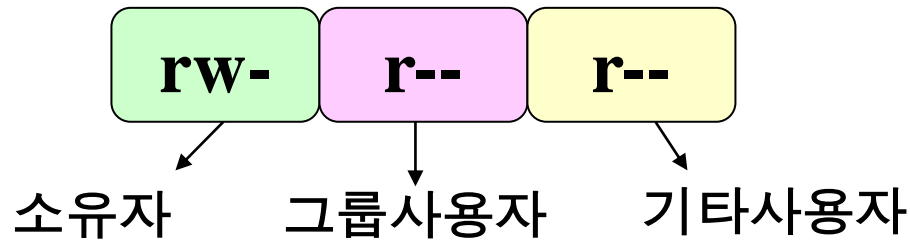
표 6-2 파일과 디렉토리의 접근 권한

| 권한 | 파일 | 디렉토리 |
|----|--|--|
| 읽기 | 파일을 읽거나 복사할 수 있다. | ls 명령으로 디렉토리 목록을 볼 수 있다 (ls 명령의 옵션은 실행 권한이 있어야 사용할 수 있다). |
| 쓰기 | 파일을 수정, 이동, 삭제할 수 있다 (디렉토리에 쓰기 권한이 있어야 한다). | 파일을 생성하거나 삭제할 수 있다. |
| 실행 | 파일을 실행할 수 있다(셸 스크립트나 실행 파일의 경우). | cd 명령의 사용이 가능하다. 파일을 디렉토리로 이동하거나 복사할 수 있다. |



02. 파일의 접근 권한

❖ 접근 권한 표기 방법



❖ 문자의 의미

- r: 읽기 허가, w: 쓰기 허가, x: 실행 허가, -: 허가 취소

❖ 다양한 사용 권한 조합

표 6-3 다양한 접근 권한 조합의 예

| 접근 권한 | 의미 |
|-----------|--|
| rw-r--r-- | 소유자는 읽기·쓰기·실행 권한을 모두 갖고, 그룹과 기타 사용자는 읽기와 실행 권한만 가짐 |
| r--r--r-- | 소유자, 그룹, 기타 사용자 모두 읽기와 실행 권한만 가짐 |
| rw----- | 소유자만 읽기·쓰기 권한을 갖고, 그룹과 기타 사용자는 아무 권한도 없음 |
| rw-rw-rw- | 소유자와 그룹, 기타 사용자 모두 읽기와 쓰기 권한을 갖고 있음 |
| rw-rw-rwx | 소유자, 그룹, 기타 사용자 모두 읽기·쓰기·실행 권한을 갖고 있음 |
| rw----- | 소유자만 읽기·쓰기·실행 권한을 갖고, 그룹과 기타 사용자는 아무 권한도 없음 |



03. 기호를 이용한 파일 접근 권한 변경

chmod [옵션] 모드 파일명

- ❖ 자신이 소유한 파일의 사용 권한을 변경
- ❖ 옵션
 - -R : 하위 디렉토리까지 모두 변경
- ❖ 모드
 - 변경할 사용 권한 표시
 - 종류 : 기호 모드, 8진수 모드



03. 기호를 이용한 파일 접근 권한 변경

❖ 기호 모드를 이용한 권한 변경

기호모드

chmod

사용자카테고리

연산자

권한

파일명

u+w, u-x
g+x, g-wx
o=rwx, go-wx
a=rwx

| 사용자 카테고리 | 의 미 |
|-------------|---------------|
| u | 소유자 |
| g | 그룹 |
| o | 기타사용자 |
| a | 모든 사용자(u+g+o) |

| 연산자 기호 | 의 미 |
|--------|--------------------|
| + | 허가권 부여 |
| - | 허가권 제거 |
| = | 특정 사용자에게 허가권 지정 |

| 권한 기호 | 의 미 |
|-------|-------|
| r | 읽기 허가 |
| w | 쓰기 허가 |
| x | 실행 허가 |



03. 기호를 이용한 파일 접근 권한 변경

❖ 사용법

```
$ ls -l first.dat
-rw-r--r-- 1 user1 staff 183 May  9 23:11 first.dat
$ chmod u-w first.dat
$ ls -l first.dat
-r--r--r-- 1 user1 staff 183 May  9 23:11 first.dat
$ chmod g+wx first.dat
$ ls -l first.dat
-r--rwxr-- 1 user1 staff 183 May  9 23:11 first.dat*
$ chmod o+x first.dat
$ ls -l first.dat
-r--rwxr-x 1 user1 staff 183 May  9 23:11 first.dat*
$ chmod go-x first.dat
$ ls -l first.dat
-r--rw-r-- 1 user1 staff 183 May  9 23:11 first.dat
$ chmod a+x first.dat
$ ls -l first.dat
-r-xrwxr-x 1 user1 staff 183 May  9 23:11 first.dat*
$ chmod u+w, g-w first.dat
$ ls -l first.dat
-rwxr-xr-x 1 user1 staff 183 May  9 23:11 first.dat*
```



[실습 4-1] 기호 모드로 파일 권한 변경하기

1. 실습용 디렉토리 만들기

```
OpenSSH SSH client
user1@Solaris11:~/Unix/ch6$ mkdir Practice
user1@Solaris11:~/Unix/ch6$ cd Practice
user1@Solaris11:~/Unix/ch6/Practice$
```

2. 파일 권한 확인하기

```
OpenSSH SSH client
user1@Solaris11:~/Unix/ch6/Practice$ cp /etc/hosts .
user1@Solaris11:~/Unix/ch6/Practice$ ls -l
total 2
-rw-r--r--  1 user1  staff    193 Jun 20 14:00 hosts
user1@Solaris11:~/Unix/ch6/Practice$
```



[실습 4-1] 기호 모드로 파일 권한 변경하기

3. 소유자 권한 변경하기

```
OpenSSH SSH client
user1@Solaris11:~/Unix/ch6/Practice$ chmod u+w hosts
user1@Solaris11:~/Unix/ch6/Practice$ ls -l
total 2
-rw-r--r--  1 user1    staff      193 Jun 20 14:00 hosts
user1@Solaris11:~/Unix/ch6/Practice$
```

4. 그룹 및 기타 사용자 권한 변경하기

```
OpenSSH SSH client
user1@Solaris11:~/Unix/ch6/Practice$ chmod go+w hosts
user1@Solaris11:~/Unix/ch6/Practice$ ls -l
total 2
-rw-rw-rw-  1 user1    staff      193 Jun 20 14:00 hosts
user1@Solaris11:~/Unix/ch6/Practice$
```



[실습 4-1] 기호 모드로 파일 권한 변경하기

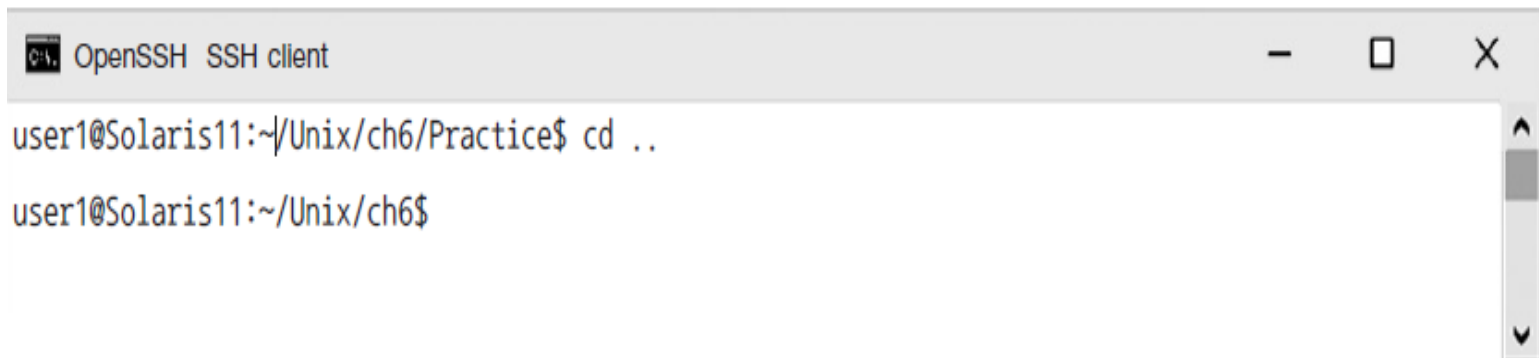
5. 권한 제거하기



A terminal window titled "OpenSSH SSH client" showing a user performing file permission changes. The user runs `chmod go-rw hosts` to remove write and execute permissions for group and others on the `hosts` file. Then, they run `ls -l` to verify the permissions, which are now `-rw-----`. The terminal output is as follows:

```
user1@Solaris11:~/Unix/ch6/Practice$ chmod go-rw hosts
user1@Solaris11:~/Unix/ch6/Practice$ ls -l
total 2
-rw----- 1 user1  staff    193 Jun 20 14:00 hosts
user1@Solaris11:~/Unix/ch6/Practice$
```

6. 디렉토리 위치 변경하기



A terminal window titled "OpenSSH SSH client" showing a user changing the current directory. The user runs `cd ..` to move up one directory level from `~/Unix/ch6/Practice` to `~/Unix/ch6`. The terminal output is as follows:

```
user1@Solaris11:~/Unix/ch6/Practice$ cd ..
user1@Solaris11:~/Unix/ch6$
```



04. 숫자를 이용한 파일 접근 권한 변경

❖ 숫자 모드

- 숫자를 이용하여 접근 권한 표현
- 모든 카테고리의 접근 권한을 동시에 조정할 때 기호모드보다 편리
- 각 카테고리 별로 접근 권한을 하나의 8진수로 표현
- 3개의 8진수를 사용하여 전체 접근 권한 표기

❖ 표시 방법

| | 소유자 | 그룹 | 기타사용자 | |
|-----------|-----|-----|-------|-----|
| ① 사용권한 | rWX | r-X | r-X | |
| ② 2진수로 대체 | 111 | 101 | 101 | 2진수 |
| | | | | ↓ |
| ③ 8진수로 변환 | 7 | 5 | 5 | 8진수 |

권한이
있으면 1,
없으면 0
으로 표시



04. 숫자를 이용한 파일 접근 권한 변경

❖ 진법?

- 수를 표시하는 방법 중 하나
- 수를 표현하는데 0 ~ p-1까지 p개의 기호를 사용하면 p진법이라 한다
- 위치에 따라 값을 다르게 보는 위치적 기수법을 사용함

▪ 10진수

- 자리 값이 올라감에 따라 값이 10배씩 커짐
- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 등 10개의 문자로 수 표현

▪ 2진수

- 자리 값이 올라감에 따라 값이 두배 씩 커짐
- 0, 1 두 개의 문자로 수 표현

▪ 8진수

- 자리 값에 올라감에 따라 값이 8배씩 커짐
- 0, 1, 2, 3, 4, 5, 6, 7 등 8개의 문자로 수 표현

2진수

1 1 1

8/10진수

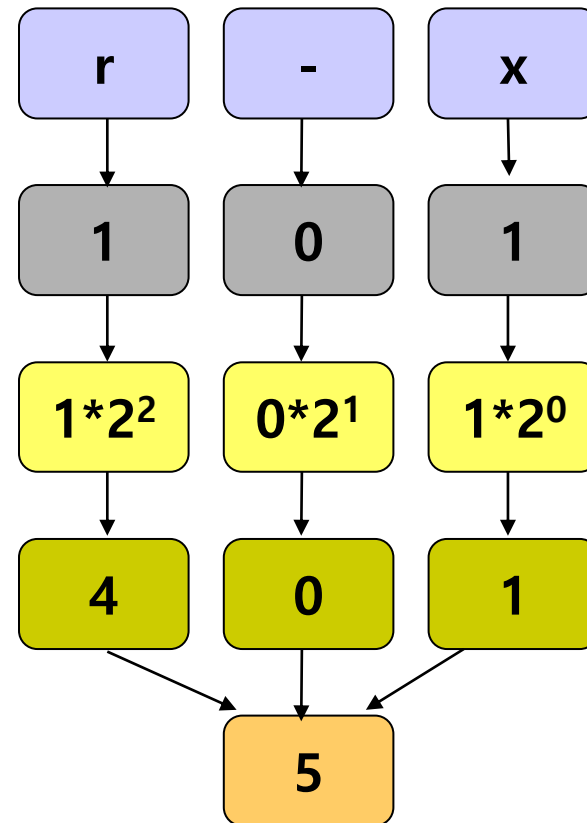
2^2 2^1 1



04. 숫자를 이용한 파일 접근 권한 변경

❖ 사용 권한의 8진수 변환 과정

- 1) 사용 권한
- 2) 2진수로 대체
- 3) 2진수 계산
- 4) 계산 결과 합산
- 5) 8진수 권한 값



04. 숫자를 이용한 파일 접근 권한 변경

❖ 접근 권한과 8진수의 대응 관계

| 기호 | 숫자(2진수) | 숫자(8진수) | 의미 |
|-----|------------|---------|------------|
| rwX | 111→ 4+2+1 | 7 | 읽기, 쓰기, 실행 |
| rw- | 110→4+2+0 | 6 | 읽기, 쓰기 |
| r-X | 101→4+0+1 | 5 | 읽기, 실행 |
| r-- | 100→4+0+0 | 4 | 읽기 |
| -wX | 011→0+2+1 | 3 | 쓰기, 실행 |
| -w- | 010→0+2+0 | 2 | 쓰기 |
| --X | 001→0+0+1 | 1 | 실행 |
| --- | 000→0+0+0 | 0 | 권한이 없음 |



04. 숫자를 이용한 파일 접근 권한 변경

❖ 8진수로 표현한 접근 권한

| 사용 권한 | 8진수 모드값 |
|-----------|---------|
| rwXrwxrwx | 777 |
| rwXr-xr-x | 755 |
| rw-rw-rw- | 666 |
| r-xr-xr-x | 555 |
| rw-r--r-- | 644 |
| rwX----- | 700 |
| rw-r----- | 740 |
| r----- | 400 |
| ----- | 000 |



04. 숫자를 이용한 파일 접근 권한 변경

❖ 숫자 모드를 이용한 접근 권한 변경

숫자모드

chmod

소유자
8진수

그룹
8진수

기타
8진수

파일명

```
(1) chmod 444 first.dat
(2) chmod 474 first.dat
(3) chmod 475 first.dat
(4) chmod 464 first.dat
(5) chmod 575 first.dat
(6) chmod 755 first.dat
(7) chmod 700 first.dat
```

```
(1) 444 = r--r--r--
(2) 474 = r--rwxr--
(3) 475 = r--rwxr-x
(4) 464 = r--rw-r--
(5) 575 = r-xrwxr-x
(6) 755 = rwxr-xr-x
(7) 700 = rwx-----
```



[실습 4-2] 숫자 모드로 파일 권한 변경하기

1. 파일 권한 확인하기

```
OpenSSH SSH client
user1@Solaris11:~/Unix/ch6$ cd Practice
/export/home/user1/Unix/ch6/Practice
user1@Solaris11:~/Unix/ch6/Practice$ ls
hosts
user1@Solaris11:~/Unix/ch6/Practice$ rm hosts
user1@Solaris11:~/Unix/ch6/Practice$ cp /etc/hosts .
user1@Solaris11:~/Unix/ch6/Practice$ ls -l
total 1
-rw-r--r--  1 user1    staff      193 Jun 20 14:18 hosts
user1@Solaris11:~/Unix/ch6/Practice$
```

2. 그룹과 기타 사용자 권한 변경하기

```
OpenSSH SSH client
user1@Solaris11:~/Unix/ch6/Practice$ chmod 666 hosts
user1@Solaris11:~/Unix/ch6/Practice$ ls -l
total 2
-rw-rw-rw-  1 user1    staff      193 Jun 20 14:18 hosts
user1@Solaris11:~/Unix/ch6/Practice$
```



[실습 4-2] 숫자 모드로 파일 권한 변경하기

3. 권한 제거하기

```
OpenSSH SSH client
user1@Solaris11:~/Unix/ch6/Practice$ chmod 400 hosts
user1@Solaris11:~/Unix/ch6/Practice$ ls -l
total 2
-r----- 1 user1  staff   193 Jun 20 14:18 hosts
user1@Solaris11:~/Unix/ch6/Practice$
```

3. 디렉토리 위치 변경하기

```
OpenSSH SSH client
user1@Solaris11:~/Unix/ch6/Practice$ cd ..
user1@Solaris11:~/Unix/ch6$
```



05. 기본 접근 권한의 설정

❖ 기본 접근 권한

- 유닉스에서 새로운 파일이나 디렉토리를 만들 때 부여되는 접근 권한

| 파 일 | 기본 접근 허가권 |
|------------------------------------|-----------|
| 실행할 수 없는 일반 파일 (문서 편집기로 생성한 파일) | 666 |
| 실행할 수 있는 일반 파일 | 777 |
| 디렉토리 | 777 |



05. 기본 접근 권한의 설정

umask [마스크값]

❖ 기본 접근권한을 출력하거나 변경

❖ 마스크 값

- 파일이나 디렉토리 생성시 부여하지 않을 권한 지정
- 이 값을 지정하면 지정한 마스크를 이용하여 기본 접근권한 지정
- 지정하지 않으면 현재 설정된 마스크값 출력

❖ 사용예

```
user1@Solaris11:~/Unix/ch6$ umask 077
user1@Solaris11:~/Unix/ch6$ umask
0077
user1@Solaris11:~/Unix/ch6$
```



❖ 마스크

- ❖ 마스크를 이용한 접근 권한 생성

- | | 일반 파일 | 디렉토리 |
|--------------|------------------|------------------|
| 1) 최대권한 | rw-rw-rw- | rw-rw-rw- |
| 2) 2진수 표현 | 110110110(666) | 111111111(777) |
| 3) 마스크값(022) | <u>000010010</u> | <u>000010010</u> |
| 4) XOR 결과 | 110100100(644) | 111101101(755) |

(XOR : 두 값이 같으면 0, 다르면 1)



05. 기본 접근 권한의 설정

❖ 간단한 계산 방법

| | | |
|--------------|-----------|-----|
| 1) 최대권한 | rw-rw-rw- | 666 |
| 2) 마스크값(022) | ----w--w- | 022 |
| 3) 뺄셈결과 | rw-r--r-- | 644 |

❖ 대표적 마스크 값

- 기본사용 권한 **XOR** 마스크

표 6-8 마스크 값 목록

| 마스크 값 | 일반 파일 적용결과 | 디렉토리 적용결과 | 의미 |
|-------|---------------|--------------|-----------------------------------|
| 022 | 644 | 755 | 그룹과 기타 사용자의 쓰기 권한 제거 |
| 077 | 600 | 700 | 그룹과 기타 사용자의 접근 권한 모두 제거 |
| 027 | 640 | 750 | 그룹의 쓰기 권한 제거, 기타 사용자의 접근 권한 모두 제거 |



[실습 4-3] 기본 접근 권한 변경하기

1. 기본 접근 권한 수정하기

```
OpenSSH SSH client
user1@Solaris11:~/Unix/ch6$ umask 022
user1@Solaris11:~/Unix/ch6$ umask
0022
user1@Solaris11:~/Unix/ch6$ cd Practice
/export/home/user1/Unix/ch6/Practice
user1@Solaris11:~/Unix/ch6/Practice$
```

2. 파일과 디렉토리를 생성해 권한 확인하기

```
OpenSSH SSH client
user1@Solaris11:~/Unix/ch6/Practice$ mkdir utmp
user1@Solaris11:~/Unix/ch6/Practice$ touch utest
user1@Solaris11:~/Unix/ch6/Practice$ ls -l
total 6
-r----- 1 user1  staff  193 Jun 20 14:18 hosts
-rw-r--r-- 1 user1  staff   0 Jun 20 14:48 utest
drwxr-xr-x 2 user1  staff   2 Jun 20 14:48 utmp/
user1@Solaris11:~/Unix/ch6/Practice$
```



[실습 4-3] 기본 접근 권한 변경하기

3. 기본 접근 권한 변경하기

```
OpenSSH SSH client
user1@Solaris11:~/Unix/ch6/Practice$ umask 027
user1@Solaris11:~/Unix/ch6/Practice$ umask
0027
user1@Solaris11:~/Unix/ch6/Practice$
```

4. 변경된 접근 권한의 적용을 확인하기

```
OpenSSH SSH client
user1@Solaris11:~/Unix/ch6/Practice$ mkdir utmp2
user1@Solaris11:~/Unix/ch6/Practice$ touch utest2
user1@Solaris11:~/Unix/ch6/Practice$ ls -l
total 10
-r----- 1 user1  staff      193 Jun 20 14:18 hosts
-rw-r--r-- 1 user1  staff         0 Jun 20 14:48 utest
-rw-r----- 1 user1  staff         0 Jun 20 14:49 utest2
drwxr-xr-x 2 user1  staff        2 Jun 20 14:48 utmp/
drwxr-x--- 2 user1  staff        2 Jun 20 14:48 utmp2/
user1@Solaris11:~/Unix/ch6/Practice$
```



[실습 4-3] 기본 접근 권한 변경하기

5. 디렉토리 위치 변경하기

A terminal window titled "OpenSSH SSH client" with standard window controls. It shows a user at a Solaris11 machine in the directory ~/Unix/ch6/Practice. The user enters the command "cd .." to move up one directory level. The prompt then changes to ~/Unix/ch6\$.

```
user1@Solaris11:~/Unix/ch6/Practice$ cd ..  
user1@Solaris11:~/Unix/ch6$
```

