UNIX 및 실습

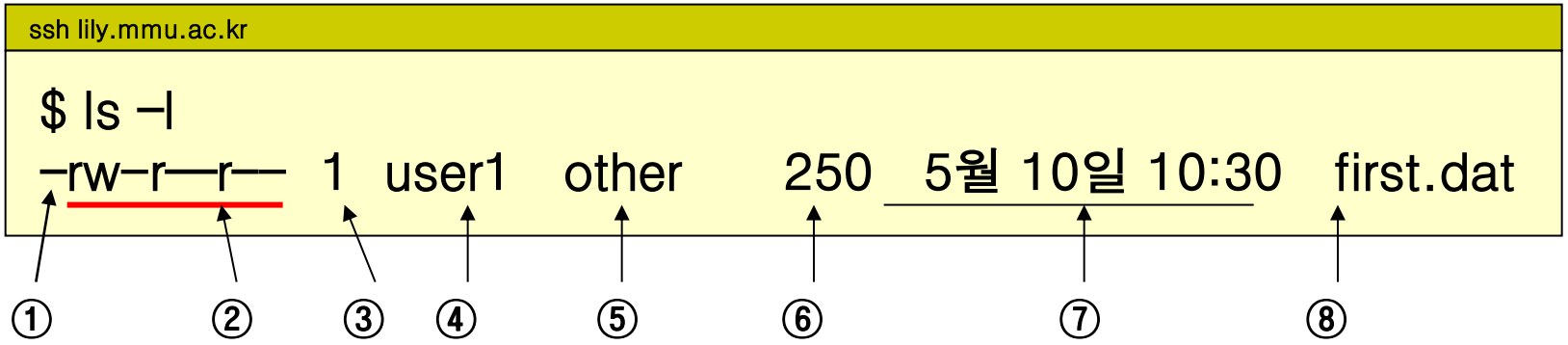
6장. 파일 사용권한 관리하기

6장. 파일 사용 권한 관리하기

- 학습목표
  - 파일의 속성과 사용 권한에 대한 개념을 이해한다.
  - 사용 권한을 변경하는 방법을 익힌다.
  - 사용 권한의 상속과 초기 설정하는 방법을 익힌다.

Section 01 파일의 속성

- ls –l 명령으로 파일과 디렉토리의 속성을 알 수 있다.



번호	값	의 미
①	-	파일 종류 (- : 일반파일, d: 디렉토리)
②	rw-r--r--	파일을 읽고,쓰고,실행할 수 있는 권한 표시
③	1	물리적 연결 개수
④	user1	파일 소유자의 사용자 명
⑤	other	파일 소유자의 그룹명
⑥	250	파일 크기 (바이트 단위)
⑦	5월 10일 10:30	파일이 마지막으로 변경된 시간
⑧	first.dat	파일 명

파일의 종류

- (1)에 나타나는 문자들이 의미하는 파일의 종류

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

파일의 종류

file 파일명

- 지정한 파일의 종류를 알려준다.
- 사용 예

ssh lily.mmu.ac.kr

```
$ file first.dat temp
first.dat:   아스키 텍스트
temp:        디렉토리
$
```

[실습하기] 파일의 종류

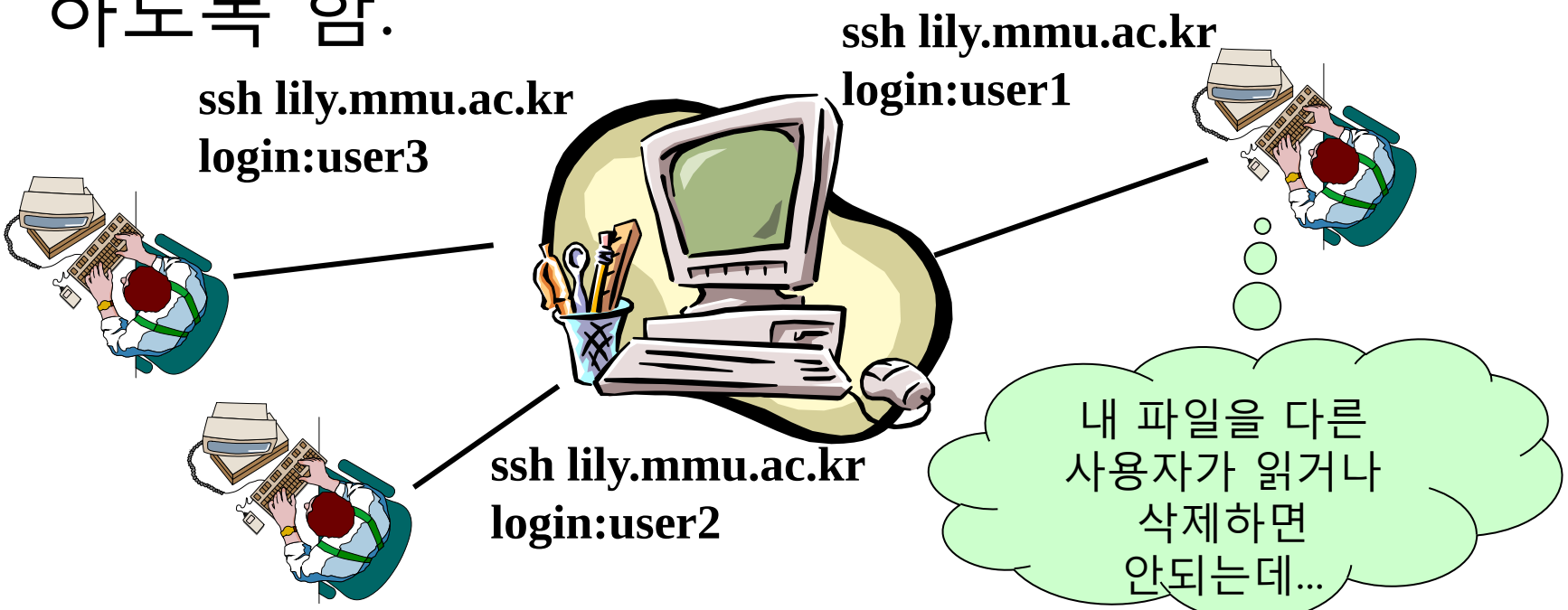
- 실습하기

```
1) cd
2) ls   -l

3) cd   /
4) ls   -l

5) cd  /devices/pseudo
6) ls   -l

7) cd
```

어떤 종류의
파일들이 있나?

Section 02 파일의 사용 권한

- 유닉스시스템에서 사용자 자신의 파일 및 디렉토리를 다른 사용자로부터 보호하기 위해 접근(Access)할 수 있는 권한을 변경하도록 함.



파일사용 권한-사용자 구분

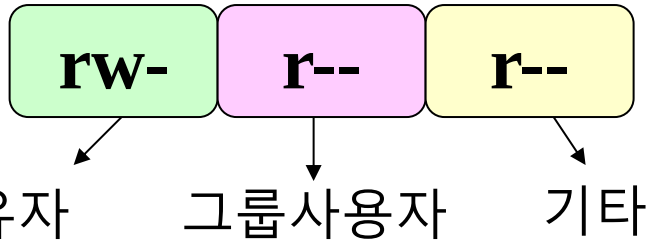
- 유닉스는 사용 권한을 부여하기 위해 사용자를 세 카테고리로 구분하여 적용
- 파일의 소유자, 파일이 속한 그룹, 기타 사용자로 구분

파일사용 권한-사용 권한의 종류

- 사용 권한은 파일 유형에 따라 약간 다르게 해석된다.

모드	일반 파일	디렉토리 파일	특수 파일
읽기 (r)	파일 내용을 읽을 수 있다	디렉토리가 포함하는 파일 목록을 읽을 수 있다	read() 를 사용하여 파일을 읽을 수 있다
쓰기 (w)	파일을 수정/삭제 시킬 수 있다	디렉토리 내에 파일을 생성,삭제할 수 있다	write() 를 사용하여 파일에 쓸 수 있다
실행 (x)	파일을 실행 시킬 수 있다	cd 명령을 이용하여 디렉토리로 이동할 수 있다	아무런 의미가 없다

파일사용 권한-사용 권한 표기방법



- 문자의 의미
  - r: 읽기 허가, w: 쓰기 허가, x:실행 허가, -: 허가 취소
- 다양한 사용 권한 조합

사용 권한	의 미
rwxr-xr-x	소유자는 읽기/쓰기/실행 권한을 모두 가지고 그룹과 기타사용자는 읽기와 실행권한만 가짐
r-xr-xr-x	소유자, 그룹, 기타사용자 모두 읽기와 실행권한만 가짐
rw-------	소유자만 읽기/쓰기 권한을 갖고 그룹과 기타사용자는 아무 권한도 없음
rw-rw-rw-	소유자와 그룹, 기타사용자 모두 읽기와 쓰기 권한을 가지고 있음
rwxrwxrwx	소유자, 그룹, 기타사용자 모두 읽기/쓰기/실행 권한을 가지고 있음
rwx------	소유자만 읽기/쓰기/실행권한을 가지고 있고 그룹과 기타사용자는 아무 권한도 없음

기호를 이용한 파일사용 권한 변경

chmod ［옵션］ 모드 파일명

- 자신이 소유한 파일의 사용 권한을 변경
- 옵션
  - -R : 하위 디렉토리 포함
- 모드
  - 변경할 사용 권한 표시 : 기호 모드, 8진수 모드

기호를 이용한 파일사용 권한 변경

- 기호모드
  - 기호를 이용하여 허가권 변경

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

기호를 이용한 파일사용 권한 변경

- 사용법

```
ssh lily.mmu.ac.kr
(1) chmod  u-w  first.dat
(2) chmod  g+wx first.dat
(3) chmod  go=rw first.dat
(4) chmod  +rwx first.dat
(5) chmod  u=rwx first.dat
```

- 1.소유자의 쓰기 권한 제거
- 2.그룹에 쓰기와 실행권한 부여
- 3.그룹과 기타에 읽기와 쓰기 권한 부여
- 4.소유자는 rwx, 그룹과 기타사용자는 r-x
- 5.소유자에게 rwx 권한 부여

[실습하기] 기호를 이용한 파일사용 권한 변경

```
1) cd Unix/ch6
2) mkdir Practice
3) cd Practice
4) cp /etc/hosts .
5) ls -l
6) chmod u+x hosts
7) chmod go+w hosts
8) chmod go-rw hosts
9) ls -l
```

hosts 파일의
최종 권한은 무엇인가?

[실습하기] 기호를 이용한 파일사용 권한 변경

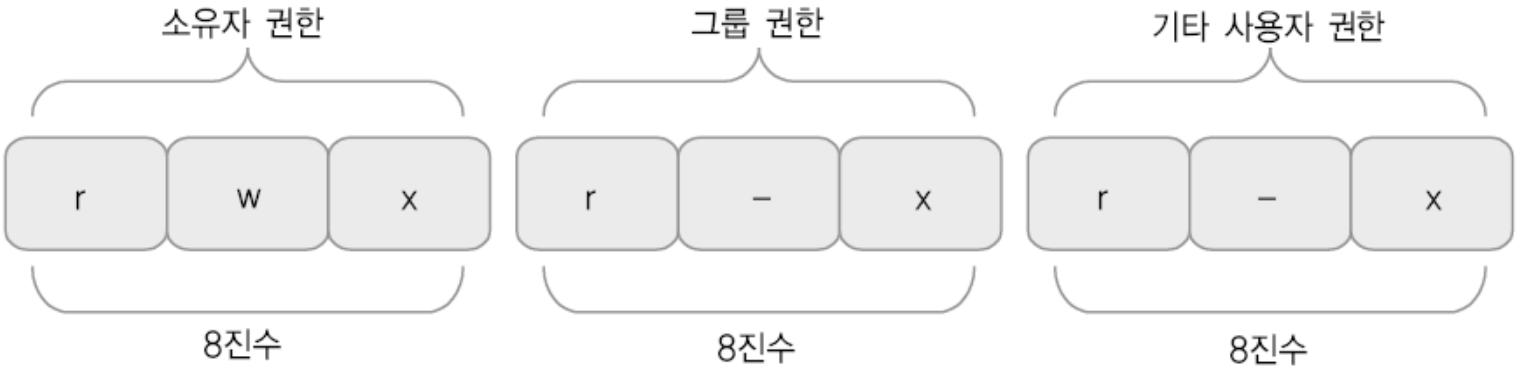
```
1) ls   Unix
2) chmod   u-r   Unix
3) ls Unix
4) cd Unix
5) ls   Unix

6) cd   ..
7) chmod   u+r   Unix
8) ls   Unix
9) chmod   u-x   Unix
10) ls   Unix
11) cd   Unix
12) chmod   u+x   Unix
```

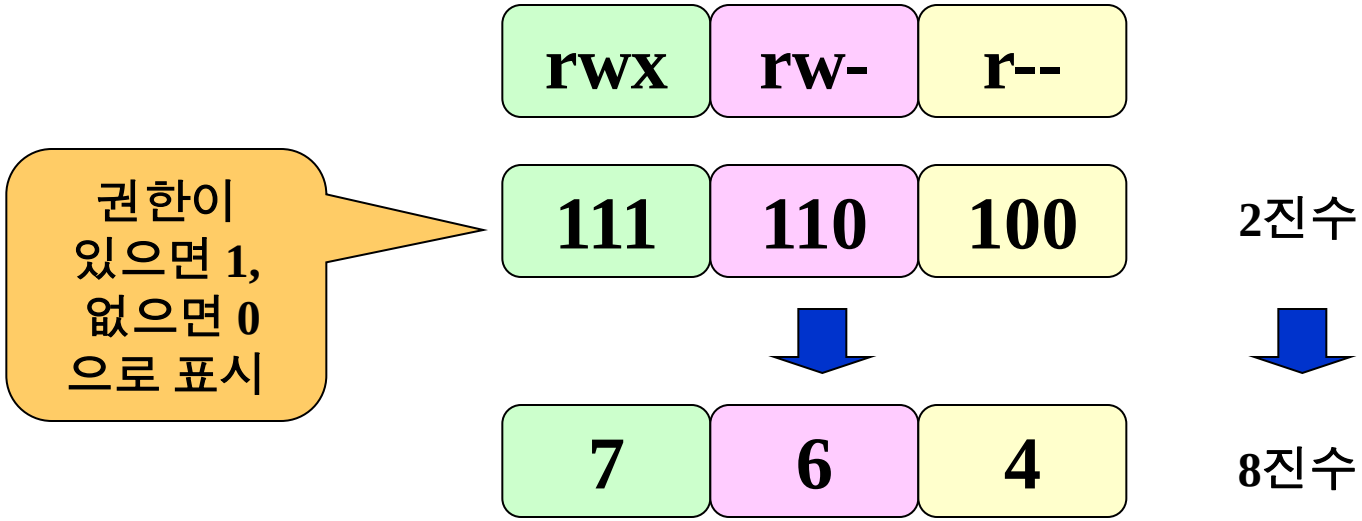
3) ls 명령이 실행되는가?
4) cd 명령이 실행되는가?
5) ls 명령이 실행되는가?

10) ls 명령이 실행되는가?
11) cd 명령이 실행되는가?

Section 04 숫자를 이용한 파일사용 권한 변경

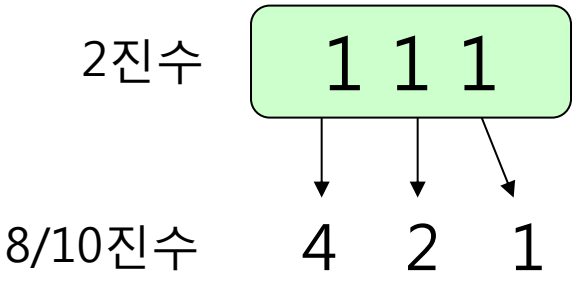
- 숫자모드





숫자를 이용한 파일사용 권한 변경

- 2진수와 8진수
  - 2진수 : 0과 1로 구성 (2는 없다)
  - 8진수 : 0, 1, 2, 3, 4, 5, 6, 7로 구성
  - 10진수 : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9로 구성



10진수의 경우

9 ➡ 10

99 ➡ 100

2진수의 경우

1 ➡ 10

11 ➡ 100

숫자를 이용한 파일사용 권한 변경

- 사용 권한의 8진수 변환과정

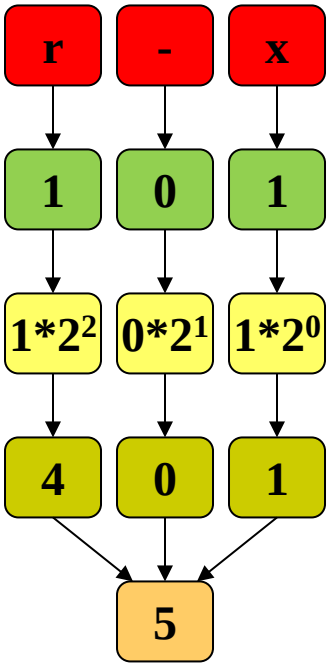
1) 사용 권한

2) 2진수로 대체

3) 2진수 계산

4) 계산 결과 합산

5) 8진수 권한 값



숫자를 이용한 파일사용 권한 변경

- 기호모드와 숫자모드

기호	숫자(2진수)	숫자(8진수)
rwx	111	7
rw-	110	6
r-x	101	5
r--	100	4
-wx	011	3
-w-	010	2
--x	001	1
---	000	0

숫자를 이용한 파일사용 권한 변경

- 8진수로 표현한 사용 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

숫자를 이용한 파일사용 권한 변경

- 사용예

telnet hanbitbook.co.kr
(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------

[실습하기] 숫자를 이용한 파일사용 권한 변경

```
1) cd Practice
2) ls  -l
3) chmod 644 hosts
4) ls -l
5) chmod 666 hosts
6) ls -l
7) chmod 400 hosts
8) ls -l
```

여러 가지 숫자로
바꾸어 봅니다

Section 05 기본사용 권한

- 기본 사용 권한
  - 유닉스에서 새로운 파일이나 디렉토리를 만들 때 적용하는 기본 사용 권한

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

기본사용 권한 설정

umask [마스크값]

- 기본사용 권한을 변경하거나 출력
- 마스크값
  - 마스크 값을 지정하면 지정한 마스크를 이용하여 사용 권한 지정
  - 마스크 값을 지정하지 않으면 현재의 마스크 값을 보여줌.
- 사용예

```
ssh lily.mmu.ac.kr
$ umask
22
$ umask 077
$ umask
77
```

022를 의미
077을 의미

마스크 값의 의미 [1/2]

- 마스크
  - 가리다
  - 사용 권한에서 허용하지 않을 값을 지정
- 마스크를 이용한 사용 권한 생성
  - 기본사용 권한 XOR 마스크

	일반 파일	디렉토리
1) 최대권한	rw-rw-rw-	rwxrwxrwx
2) 2진수 표현	110110110 (666)	111111111 (777)
3) 마스크값(022)	000010010	000010010
4) XOR결과	110100100 (644)	111101101 (755)

(XOR : 두 값이 같으면 0, 다르면 1)

마스크 값의 의미 [2/2]

- 간단한 계산방법

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

마스크 값	실행할 수 없는 일반 파일	실행할 수 있는 일반 파일	디렉토리	의 미
022	644	755	755	소유자는 모두 할 수 있고 그 이외의 사용자는 쓰기 금지
077	600	700	700	소유자 이외는 파일에 접근 금지

[실습하기] 기본사용 권한

```
1) cd
2) cd
   Unix/ch6/Practice
3) umask
4) mkdir utmp
5) touch utest
6) ls -l
7) cd ..
8) umast 027
9) umask
10) mkdir utmp2
11) touch utest2
12) ls -l
```

umask값의 변경에 따라
생성된 디렉토리와 파일
기본 권한을 비교해 본다.

[실습과제]

- 실습 각 단계 화면 캡처하여 pdf 파일로 정리하여 과제 제출 (cms.mmu.ac.kr/bear)
- 제출기한 : 4월 14일 자정