14-3. 특수 접근 권한 관리

특수 접근 권한

- 리눅스의 권한은 소유자, 소유그룹, 나머지 사용자의 3부류로 나뉘며 각각 파일에 대한 권한을 읽기, 쓰기, 실행의 3가지로 나타낸다.
- 관리자의 입장에서 시스템의 모든 상황을 고려해야 하기 때문에 이러한 권한 외에 몇가지 특수한 권한을 사용하여 시스템 관리의 효율성을 높인다.
- umask 값을 출력하면 숫자가 4자리로 출력되는데, 3자리 이외의 나머지 1자리가 바로 특수 접근 권한을 나타낸다.
- umask 0022에서 맨 앞자리 숫자가 0이면 일반적인 접근 권한이지미나 이 숫자가 1, 2, 4이면 특수 접근 권한을 설정할 것이다.
- 특수 권한은 **SetUID, SetGID, Sticky Bit**가 있다.

특수 권한	절대 모드 표현
SetUID	4000
SetGID	2000
Sticky Bit	1000

SetUID

- **실행 파일에 적용된다.**
- **특정 파일이 실행되는 동안, 실행한 사용자의 권한이 아닌 해당 파일의 소유자 권한으로 파일을 실행한다.**
- SetUID를 적용할 경우 일반 허가권에 4000 추가한다.
- 적용되면 소유자의 허가권 값에 실행권한에 x가 아닌 s로 명시된다.

passwd

- SetUID가 부여된 대표적 명령어이다.
- passwd를 변경하는 과정에서 /etc/shadow 파일의 내용을 읽거나 쓸 수 있어야 변경한 패스워드를 기록할 수 있기 때문에 passwd 파일에는 SetUID가 걸려 있고 소유주가 root로 설정되어 있다.
- **ls -l /usr/bin/passwd**

SetGID

- **실행 파일과 디렉터리에 적용된다.**
- **실행하려는 파일의 소유 그룹 권한으로 파일을 실행한다.**
- SetGID 적용할 경우 일반 허가권에 2000 추가한다.

- 적용되면 소유그룹의 허가권 값에 실행권한 x가 아닌 s로 명시된다.

디렉터리에 적용될 경우

- **명시된 디렉터리 하위에 생성되는 디렉터리는 동일한 SetGID 권한을 가진다.**
- 시스템에 어떠한 사용자가 SetGID 권한이 부여된 디렉터리 내에서 디렉터리를 생성하더라도 SetGID 권한이 적용된 디렉터리와 동일한 그룹 소유주가 된다.

Sticky Bit

- **디렉터리에 적용되는 권한이다.**
- 모든 사용자는 읽고, 쓰고 삭제가 가능
- **단, 삭제는 오로지 소유자와 관리자만 가능**
- Sticky Bit를 적용할 경우 일반 허가권에 1000 추가
- 적용되면 Other의 허가권 값에 실행권한에 x가 아닌 **t**로 명시
- **대표적인 Sticky Bit가 적용된 디렉터리는 /tmp와 /var/tmp가 있다**
- **보통 공용 디렉터리에 적용**

➢ 특수 접근 권한 설정의 오류

- 특수 권한을 설정하는 파일이나 디렉터리 모두 실행 권한을 가지고 있어야 한다.
- 만약 실행 권한이 없는 파일에 SetUID나 SetGID를 설정하면 s가 아니라 S로 표시된다.
- 또한 디렉터리에 실행 권한이 없는데 Sticky Bit를 설정하면 T로 표시된다.