

## 3주차 1차시 권한 관리

### 【학습목표】

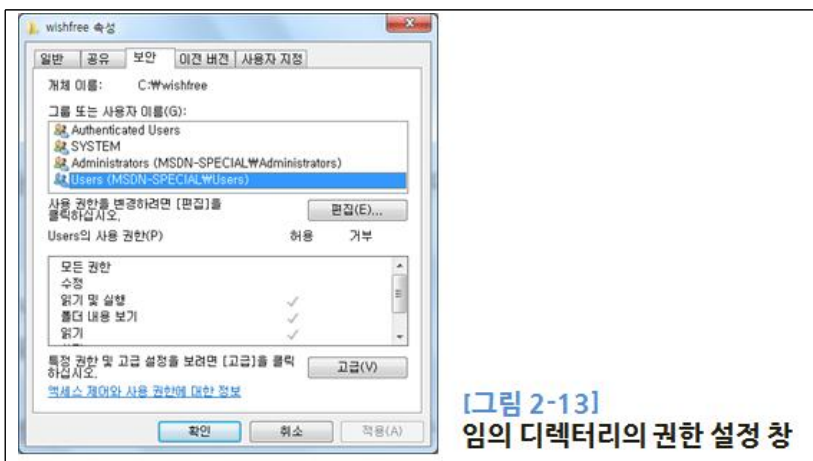
1. 권한관리의 개념을 설명할 수 있다.
2. 운영체제, 데이터베이스, 응용 프로그램에 대한 권한 관리를 구분할 수 있다.

### 학습내용1 : 운영체제의 권한 관리

#### 1. 윈도우의 권한 관리

##### 1) NTFS 권한의 종류

- ① 모든 권한 : 디렉터리에 대한 접근 권한과 소유권을 변경할 수 있으며, 하위에 있는 디렉터리와 파일을 삭제할 수 있음
- ② 수정 :
  - 디렉터리를 삭제할 수 있음
  - 읽기 및 실행과 쓰기 권한이 주어진 것과 같음
- ③ 읽기 및 실행 : 읽기를 수행할 수 있으며, 디렉터리나 파일을 옮길 수 있음
- ④ 디렉터리 내용 보기 : 디렉터리 내의 파일이나 디렉터리의 이름을 볼 수 있음
- ⑤ 읽기 : 디렉터리의 내용을 읽기만 할 수 있음
- ⑥ 쓰기 : 해당 디렉터리에 하위 디렉터리와 파일을 생성할 수 있으며, 소유권이나 접근 권한의 설정 내용을 확인할 수 있음



2) 윈도우의 6가지 권한은 다음과 같은 규칙이 적용됨

- ① 접근 권한은 누적됨
- ② 파일에 대한 접근 권한이 디렉터리에 대한 접근 권한보다 우선
- ③ '허용'보다 '거부'가 우선

## 2. 유닉스의 권한 관리

drw-r-xr-x 117 root root 12288 Jul 28 06:42 etc

①                      ②           ③

1 - rw- r-- r--

① ② ③ ④

- ① 파일 및 디렉터리의 종류이다. -표시는 일반 파일을, d 표시는 디렉터리를, l 표시는 링크(Link)를 나타냄
- ② 파일 및 디렉터리 소유자의 권한
- ③ 파일 및 디렉터리 그룹의 권한
- ④ 해당 파일 및 디렉터리 소유자도 그룹도 아닌 제3의 사용자에게 대한 권한

- 유닉스는 읽기(r: read), 쓰기(w: write), 실행(x : execute)과 같은 세 가지 권한을 부여
- 권한은 숫자로도 표현할 수 있음. 읽기는 4, 쓰기는 2, 실행은 1로 바꾸어 각 권한 세트별로 합치는 것
- rw- r-x r-x = 42- 4-1 4-1 → 655

2 파일에 대한 소유자

3 파일에 대한 그룹

## 학습내용2 : 데이터베이스의 권한 관리

### 1. 질의문에 대한 권한 권리

#### ① DDL

- DDL(Data Definition Language)은 데이터 구조를 정의하는 질의문
- 데이터베이스를 처음 생성하고 개발할 때 주로 사용하고 운영 중에는 거의 사용하지 않음

CREATE	데이터베이스 객체를 생성함
DROP	데이터베이스 객체를 삭제함
ALTER	기존의 데이터베이스 객체를 다시 정의함

#### ② DML

- DML(Data Manipulation Language)은 데이터베이스의 운영 및 사용과 관련해 가장 많이 사용하는 질의문
- 데이터의 검색과 수정 등을 처리

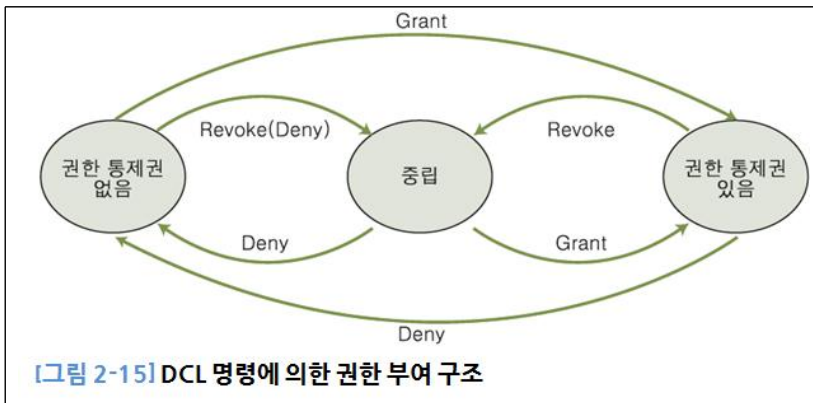
SELECT	사용자가 테이블이나 뷰의 내용을 읽고 선택함
INSERT	데이터베이스 객체에 데이터를 입력함
UPDATE	기존 데이터베이스 객체에 있는 데이터를 수정함
DELETE	데이터베이스 객체에 있는 데이터를 삭제함

#### ③ DCL

- DCL(Data Control Language)은 권한 관리를 위한 질의문

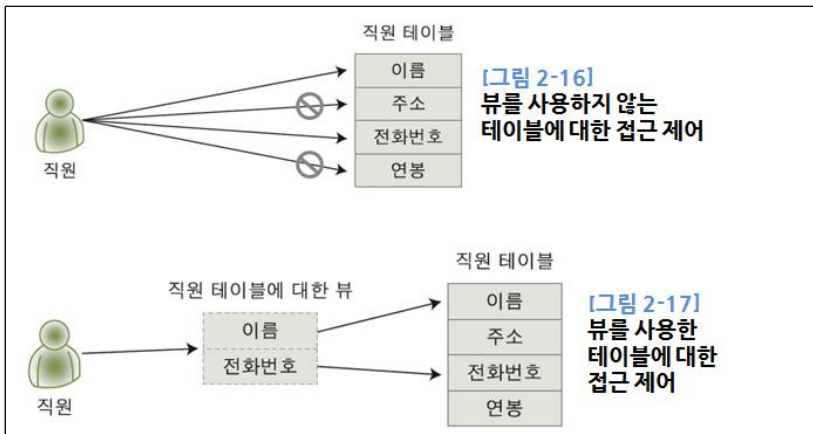
GRANT	데이터베이스 객체에 권한을 부여함
DENY	사용자에게 해당 권한을 금지함
REVOKE	이미 부여된 데이터베이스 객체의 권한을 취소함

1) DDL과 DML은 DCL에 의해 허용(Grant) 또는 거부(Deny)됨



## 2. 뷰에 대한 권한 관리

- 뷰 : 각 사용자에게 대해 참조 테이블의 각 열에 대한 권한을 설정하는 것이 불편해서 만든 가상 테이블



## 학습내용3 : 응용 프로그램의 권한 관리

- 응용 프로그램은 응용 프로그램 내의 권한보다 응용 프로그램 자체의 실행 권한이 더 중요함
- 응용 프로그램은 자신을 실행한 계정의 권한을 물려받음
- 응용 프로그램이 보안상에 문제가 있는 취약한 프로그램일 때 해당 프로그램을 실행한 계정의 권한이 악용되는 문제가 발생
  - 윈도우의 IIS에서는 그 실행 프로세스 권한을 별도로 만들어 사용
  - 유닉스에서는 nobody와 같이 제한된 계정 권한을 사용

## 【학습정리】

1. 권한관리는 운영체제의 경우 디렉터리 및 하위 디렉터리에 대한 접근 권한과 소유권을 변경 등을 처리한다.
2. 권한관리의 응용에는 운영체제 권한관리, 데이터베이스 권한관리, 응용프로그램 권한관리 등이 있다.