보안

물리적 환경에 대한 보안

권한 관리를 통한 보안 (권한이 없는 사용자로부터 DB보호)

- 접근이 허락된 사용자만 DB 사용가능
- 사용 범위를 제한해야함

운영 관리를 통한 보안 (무결성 유지를 위해 권한 있는 사용자로부터 DB보호)

- 접근이 허락된 사용자가 DB를 사용하다 무결성 위반할 수 있음
- 올바른 제약조건 정의, 통제해야함

권한 관리

- DB 관리자는 DB 보안을 위해 모든 권한을 가지고 있음
- 일반적으로 자신이 사용한 객체에 대해 접근할 수 있음

⇒ SQL문을 이용해 다른 사람에게 자신이 생성한 객체에 대한 사용권한을 부여·취소할 수 있음

- 권한 관리
  - 객체권한
    - 권한 부여
    - 권한 취소
  - 역할
    - 역할 생성
    - 역할에 대한 권한 부여
    - 역할 부여

권한 부여 (테이블과 관련) GRANT

GRANT 권한 ON 객체 TO 사용자 [WITH GRANT OPTION];

권한 ↓
insert. delete. update. select.

객체 (테이블)

[WITH GRANT OPTION] ↓
권한을 부여받은 사용자는 자신이 부여받은 권한을 다른 사용자에게 부여가능

references: 해당 권한을 부여받으면 테이블의 기본키를 참조하는 외래키를 자신의 테이블에 포함할 수 있음.

권한( )
└→ 여기에 특정 속성을 나열하여 일부 속성만 권한 부여 할 수 있음

특정 객체에 권한을 부여할 수 있지만, → 객체의 "소유자"가 부여

시스템 권한도 부여 가능(create table, create view 등 DDL)

↳ DB 관리자가 부여

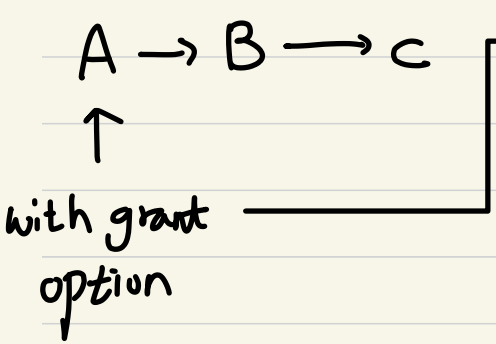
=> GRANT 사용

객체지정 필요X

ex) grant create table to [사용자]

권한 취소 REVOKE

REVOKE 권한 ON 객체 FROM 사용자 CASCADE | RESTRICT;



→ A가 B에게 권한을 부여, B가 C에게 권한을 부여한 상황

CASCADE: A가 B의 권한을 취소하면 C권한도 취소

RESTRICT : B권한만 취소하고 C권한은 취소하지 않음

역할의 부여와 취소

역할

· 여러 권한을 하나의 "역할"로 묶어서 "많은 권한을 부여하기 위해"
복잡한 GRANT 문을 간결하게 도와주는 기능

1) 역할 생성 (DB 관리자 주체)

CREATE ROLE a; a라는 역할 생성

2) 역할에 권한 부여

(상품 테이블 소유자가 주체)

GRANT SELECT, INSERT ON 상품 TO a;

→상품 테이블에서 검색, 삽입이 가능한 권한을 a역할에 부여

3) 역할을 사용자에게 부여

→ 이때 해당 역할이 권한 변경을 하게 되면 역할이 부여된 "모든 사용자"가 변경된 권한을 부여받는다

```
GRANT a TO [사용자];
```

DB 관리자 주체

4) 사용자에게 부여된 역할 취소 (DB 관리자 주체)

```
REVOKE a FROM [사용자];
```

5) 롤 삭제 (DB 관리자 주체)

```
DROP ROLE a;
```

→ 역할이 속해있던 모든 사용자는 권한이 취소됨