11. 보안과 권한 관리

01. 보안

조직에서 허가한 사용자만 데이터베이스에 접근할 수 있도록 통제하여 보안을 유지하는 것 중요

- 물리적 환경에 대한 보안 : 자연 재해 등으로부터 보호
- 권한 관리를 통한 보안 : 권한이 없는 사용자로부터 보호, 계정이 발급된 사용자만 접근 허용
- 운영 관리를 통한 보안 : 권한이 있는 사용자로 부터 보호, 데이터 무결성을 위반하지 않도록 올바른 제약조건 정의

02. 권한 관리

· DBMS는 계정이 발급된 사용자가 로그인에 성공했을 경우에만 데이터베이스에 접근 허용 (접근제어)

→ 데이터베이스 관리자가 계정 생성 & 삭제

· 사용자별로 데이터베이스 사용 범위와 수행 가능한 작업 제한, 허용된 권한 내에서만 데이터베이스 사용 (권한확인)

· 일반적으로 객체를 생성한 사용자만 사용 권한 소유 → 다른 사용자도 필요에 따라 접근 가능해야 한다 → SQL문을 이용해 사용 권한 부여

① 권한의 부여

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

(객체: 테이블)

(권한: UPDATE, DELETE, INSERT, SELECT, REFERENCES)

· WITH GRANT OPTION : 권한을 부여받은 사용자가 자신이 부여받은 권한을 다른 사용자에게 부여 가능

ex) 고객 테이블에 대한 삽입과 삭제 권한을 모든 사용자에게 부여 ⇒ GRANT INSERT, DELETE ON 고객 TO PUBLIC;

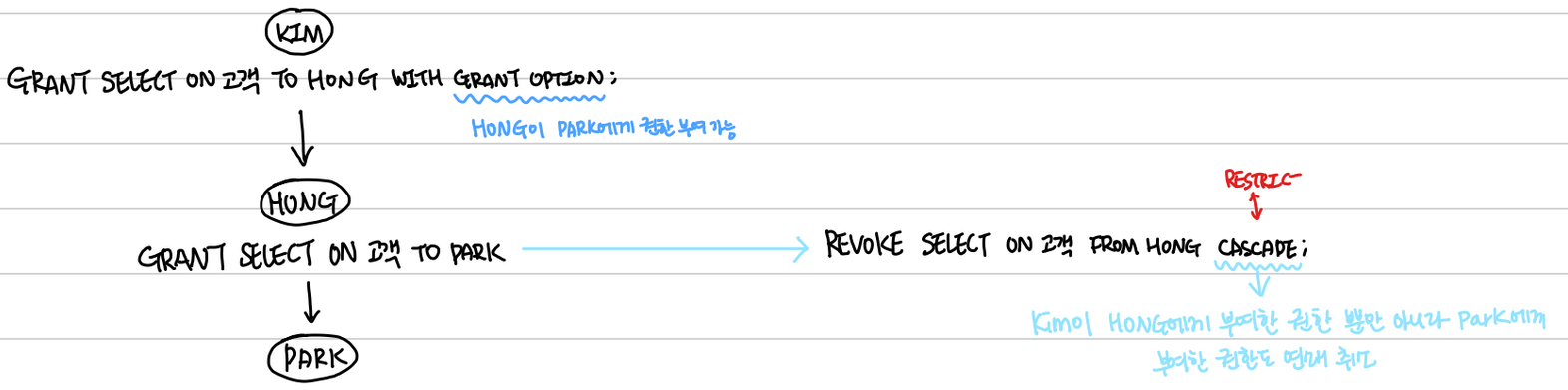
· 객체는 소유자가, 시스템 권한은 DBMS가 권한 부여 → GRANT 사용

(시스템 권한 → 데이터베이스 관리와 관련된 작업 (DDL과 관련된 작업))

② 권한의 취소

REVOKE 권한 ON 객체 FROM 사용자 CASCADE | RESTRICT

ex)



③ 역할의 부여와 취소

· 여러 사용자들에게 동일한 권한들을 부여&취소 → 역할 활용

· 역할은 여러 권한을 그룹으로 묶어놓은 것

생성 ↓ 설정 ↓ 부여 ↓ 취소 ↓ 삭제

CREATE ROLE 롤이름;	ex) CREATE ROLE role_1;	
GRANT 권한 ON 객체 TO 롤이름;	ex) GRANT SELECT, INSERT, DELETE ON 고객 TO role_1;	⇒
GRANT 롤이름 TO 사용자;	ex) GRANT role_1 TO HONG;	
REVOKE 롤명 FROM 사용자;	ex) REVOKE role_1 FROM HONG;	
DROP ROLE 롤이름;	ex) DROP ROLE role_1;