18장 데이터베이스 롤 권한 제어

18.1 롤의 정의와 종류

18.1.1 롤의 정의

- 롤은 사용자에게 보다 효율적으로 권한을 부여할 수 있도록 여러 개의 권한을 묶어 놓은 것이라고 생각하면 된다.

- 사용자를 생성했으면 그 사용자에게 각종 권한을 부여해야만 생성된 사용자가 데이터베이스를 사용할 수 있다.

- 데이터베이스의 접속 권한(CREATE SESSION), 테이블 생성 권한(CREATE TABLE), 테이블 수정(UPDATE), 삭제(DELETE), 조회(SELECT) 등과 같은 권한은 사용자에게 기본적으로 필요한 권한들인데 사용자를 생성할 때마다 일일이 이러한 권한을 부여하는 것은 번거롭다.

- 이 때문에 다수의 사용자에게 공통적으로 필요한 권한들을 롤에 하나의 그룹으로 묶어두고 사용자에게는 특정 롤에 대한 권한 부여를 함으로서 간단하게 권한 부여를 할 수 있도록 한다.

- 또한 여러 사용자에게 부여된 권한을 수정하고 싶을 때에도 일일이 사용자마다 권한을 수정하지 않고 롤만 수정하면 그 롤에 대한 권한 부여를 한 사용자들의 권한이 자동 수정된다. 이 밖에 롤을 활성화 비활성화 함으로서 일시적으로 권한을 부여했다 철회할 수 있으므로 사용자 관리를 간편하고 효율적으로 할 수 있다.

18.1.2 사전에 정의된 롤의 종류

- 롤은 오라클 데이터베이스를 설치하면 기본적으로 제공되는 사전 정의된 롤과 사용자가 정의한 롤로 구분된다. 다음과 사전 정의된 시스템에서 제공해주는 롤이다.

- CONNECT 롤
  - 사용자가 데이터베이스에 접속 가능하도록 하기 위해서 다음과 같이 가장 기본적인 시스템 권한 8가지를 묶어 놓았다.
  - ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW

- RESOURCE 롤
  - 사용자가 객체(테이블, 뷰, 인덱스)를 생성할 수 있도록 하기 위해서 시스템 권한을 묶어 놓았다.
  - CREATE CLUSTER, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER

- DBA 롤
  - 사용자들이 소유한 데이터베이스객체를 관리하고 사용자들을 작성하고 변경하고 제거할 수 있도록 하는 모든 권한을 가진다. 즉, 시스템 자원을 무제한적으로 사용하며 시스템 관리에 필요한 모든 권한을 부여할 수 있는 강력한 권한을 보유한 롤이다.

[실습] 롤 부여하기

- 일반적으로 데이터베이스 관리자는 새로운 사용자를 생성할 때 CONNECT롤과 RESOURCE롤을 부

여한다. USER04 사용자를 생성하여 CONNECT롤과 RESOURCE롤을 부여해 보겠다.

[LAB_18_1.SQL] 롤 부여하기

```
01    CONN SYSTEM/MANAGER
02    DROP USER USER04 CASCADE;
03    CREATE USER USER04 IDENTIFIED BY TIGER;
04    CONN USER04/TIGER
05
06    CONN SYSTEM/MANAGER
07    GRANT CONNECT, RESOURCE TO USER04;
08    CONN USER04/TIGER
```

18.1.3 롤 관련 데이터 딕셔너리

■ 데이터 딕셔너리를 통해서 부여된 권한에 대한 정보를 확인할 수 있다.

```
SELECT * FROM DICT WHERE TABLE_NAME LIKE '%ROLE%';

CONN USER04/TIGER
SELECT * FROM USER_ROLE_PRIVS;
```

딕셔너리 명	설 명
ORLE_SYS_PRIVS	롤에 부여된 시스템 권한 정보
ROLE_TAB_PRIVS	롤에 부여된 테이블 관련 권한 정보
USER_ROLE_PRIVS	접근 가능한 롤 정보
USER_TAB_PRIVS_MADE	해당 사용자 소유의 오브젝트에 대한 오브젝트 권한 정보
USER_TAB_PRIVS_RECD	사용자에게 부여된 오브젝트 권한 정보
USER_COL_PRIVS_MADE	사용자 소유의 오브젝트 중 칼럼에 부여된 오브젝트 권한 정보
USER_COL_PRIVS_REDC	사용자에게 부여된 특정 칼럼에 대한 오브젝트 권한 정보

18.2 사용자 롤 정의

■ 사용자는 CREATE ROLE 명령어로 다음 형식에 따라 롤을 생성해야 한다.

```
-- 형식
CREATE ROLE ROLE_NAME;
GRANT PRIVILEGE_NAME TO ROLE_NAME;
```

[실습] 롤 생성하여 시스템 권한 할당하기

■ 롤을 생성하여 할당하는 시스템 권한을 할당해 보겠다.

```
CONN SYSTEM/MANAGER
CREATE ROLE MROLE;

GRANT CREATE SESSION, CREATE TABLE, CREATE VIEW TO MROLE;

DROP USER USER05 CASCADE;
CREATE USER USER05 IDENTIFIED BY TIGER;
```

```
GRANT MROLE TO USER05;

CONN USER05/TIGER
SELECT * FROM USER_ROLE_PRIVS;
```

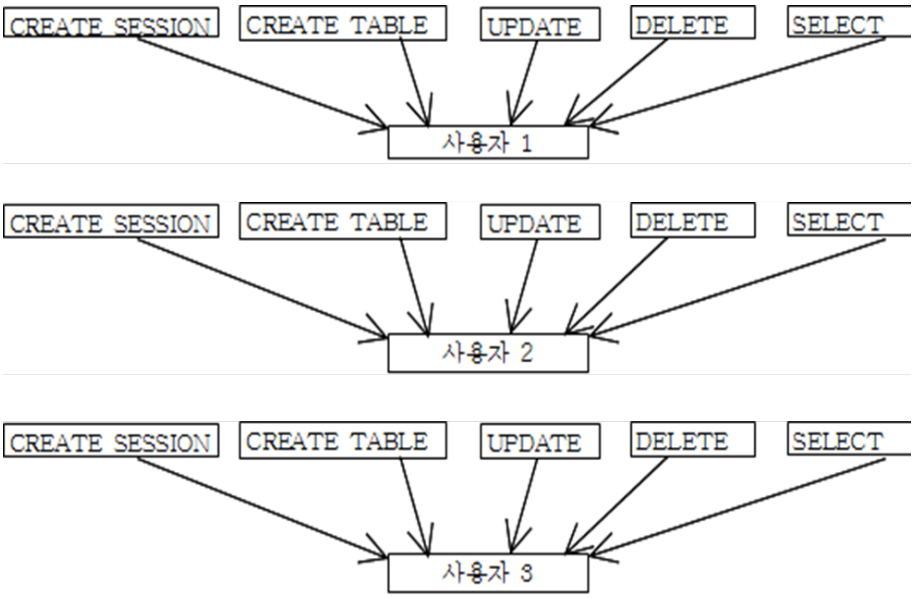
18.3 롤 회수하기

■ 롤을 회수하기 위해 DROP ROLE 명령어를 사용한다.

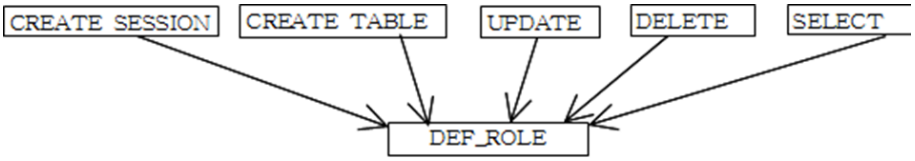
```
-- 형식
REVOKE ROLE_NAME FROM USER_NAME;
```

18.4 롤의 장점

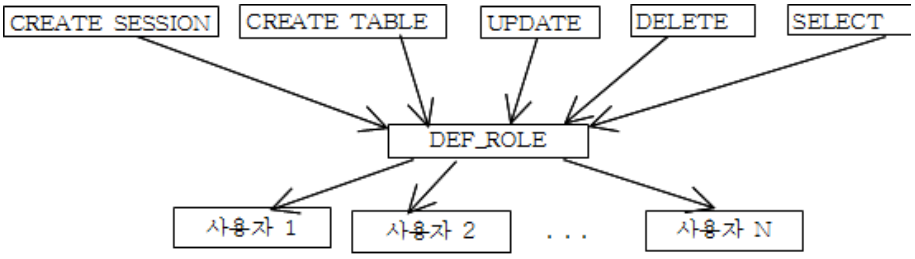
■ 시스템권한이나 객체 권한을 사용자마다 일일이 부여하게 되면 번거롭다.



■ 이러한 단점을 롤로 보안할 수 있다. 우선 롤에 시스템 권한과 객체 권한을 부여한다.



■ 그런 후에 롤을 사용자에 대해 권한 부여함으로서 작업을 간소화할 수 있다.



[실습] 디폴트 롤을 생성하여 여러 사용자에게 부여하기

- 롤에 시스템 권한과 객체 권한을 부여한 후에 사용자에게 롤에 대한 권한을 부여하여 작업을 간소화해 보겠다.

```
CONN SYSTEM/MANAGER
CREATE ROLE DEF_ROLE;

GRANT CREATE SESSION TO DEF_ROLE;
GRANT CREATE TABLE TO DEF_ROLE;

CONN SCOTT/TIGER
GRANT UPDATE ON EMP TO DEF_ROLE;
GRANT DELETE ON EMP TO DEF_ROLE;
GRANT SELECT ON EMP TO DEF_ROLE;

CONN SYSTEM/MANAGER
CREATE USER USERA1 IDENTIFIED BY A1234;
CREATE USER USERA2 IDENTIFIED BY A1234;
CREATE USER USERA3 IDENTIFIED BY A1234;

SHOW USER
GRANT DEF_ROLE TO USERA1;
GRANT DEF_ROLE TO USERA2;
GRANT DEF_ROLE TO USERA3;

SHOW USER
SELECT * FROM ROLE_SYS_PRIVS WHERE ROLE='DEF_ROLE';
SELECT * FROM ROLE_TAB_PRIVS WHERE ROLE='DEF_ROLE';
```