데이터베이스

- 순서 : Ch10-1 데이터베이스 보안을 위한 권한 실습
- 학기 : 2018학년도 2학기
- 학과 : 가천대학교 컴퓨터공학과 2학년
- 교수 : 박양재

데이터베이스

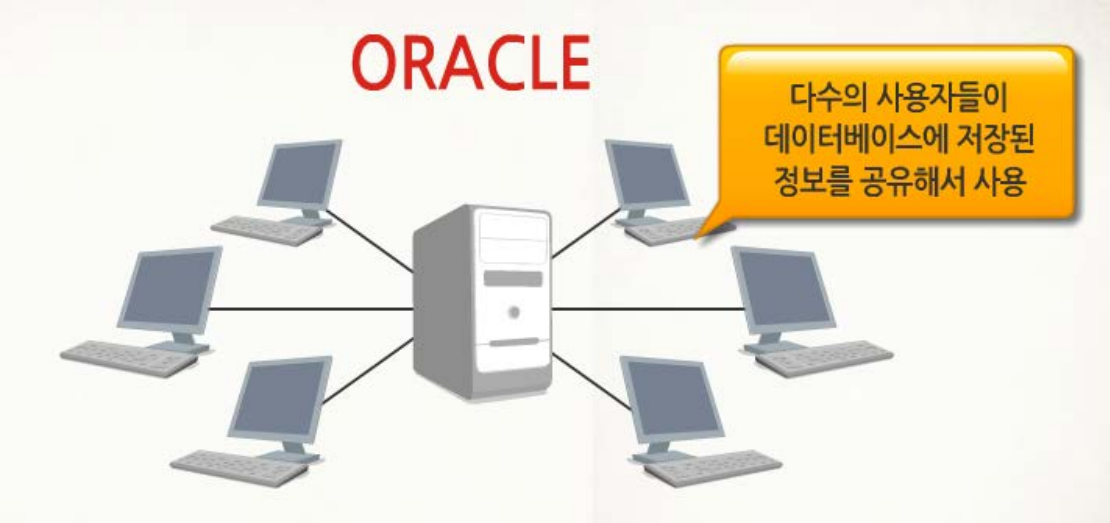
- 목차

10-1장. 데이터베이스 보안을 위한 권한

❑ 데이터베이스 보안을 위한 권한

✓ 오라클은 다수의 사용자들이 데이터베이스에 저장된 정보를 공유해서 사용한다.

✓ 하지만 정보의 유출이나 불법적인 접근을 방지하기 위해 보안을 위한 데이터베이스 관리자가 있어야 한다.



10-1장. 데이터베이스 보안을 위한 권한

- 데이터베이스 관리자
  - ✓ 사용자가 데이터베이스의 객체(테이블, 뷰 등)에 대한 특정 권한을 가질 수 있도록 한다.
  - ✓ 다수의 사용자가 데이터베이스에 저장된 정보를 공유하면서도 정보에 대한 보안이 이루어지도록 한다.
  - ✓ 데이터베이스에 접근하기 위해서는 사용자가 이름과 암호를 입력해서 로그인 인증을 받아야 한다.
  - ✓ 사용자마다 서로 다른 권한을 부여함으로써 보안을 설정한다.
- 권한
  - ✓ 사용자가 특정 테이블에 접근할 수 있도록 하거나, 해당 테이블에 SQL문(SELECT/INSERT/UPDATE/DELETE)을 사용할 수 있도록 제한을 두는 것이다.
  - ✓ 데이터베이스를 위한 권한은 시스템 권한과 객체 권한으로 나뉜다.
    - 시스템 권한(System Privileges) : 사용자의 생성과 제거, DB 접근 및 각종 객체를 생성할 수 있는 권한 등 주로 DBA에 의해 부여
    - 객체 권한(Object Privileges) : 객체를 조작할 수 있는 권한

10-1장. 데이터베이스 보안을 위한 권한

❑데이터베이스 관리자 가 소유하고 있는 시스템 권한

시스템 권한	기능
CREATE USER	새롭게 사용자를 생성하는 권한
DROP USER	사용자를 삭제하는 권한
DROP ANY TABLE	임의의 테이블을 삭제할 수 있는 권한
QUERY REWRITE	함수 기반 인덱스를 생성하는 권한
BACK UP ANY TABLE	임의의 테이블을 백업할 수 있는 권한

❑ 데이터베이스를 관리하는 권한으로 시스템 관리자가 사용자에게 부여하는 권한

시스템 권한	기능
CREATE SESSION	데이터베이스에 접속할 수 있는 권한
CREATE TABLE	사용자 스키마에서 테이블을 생성할 수 있는 권한
CREATE VIEW	사용자 스키마에서 뷰를 생성할 수 있는 권한
CREATE SEQUENCE	사용자 스키마에서 시퀀스를 생성할 수 있는 권한
CREATE RPOCEDURE	사용자 스키마에서 함수를 생성할 수 있는 권한

10-1장. 데이터베이스 보안을 위한 권한

❑ 객체 권한

- ✓ 특정 객체에 조작을 할 수 있는 권한이다.
- ✓ 객체의 소유자는 객체에 대한 모든 권한을 가진다.
- ✓ 다음은 객체와 권할 설정할 수 있는 명령어를 맴핑 시켜 놓은 표이다.

권한	TABLE	VIEW	SEQUENCE	PROCEDURE
ALTER	V		V	
DELETE	V	V		V
EXECUTE				V
INDEX	V			
INSERT	V	V		
REFERENCES	V			
SELECT	V	V		
UPDATE	V	V		

10-1장. 데이터베이스 보안을 위한 권한

❑ 예제 : 새롭게 생성한 USEREDU 사용자로 EMP 테이블의 내용을 조회하는 경우

```
SQL> CONN USEREDU/TIGER;
연결되었습니다.
SQL> SELECT * FROM EMP;
SELECT * FROM EMP
              *
1행에 오류:
ORA-00942: 테이블 또는 뷰가 존재하지 않습니다
```

❑ 특정 객체에 대한 권한은 그 객체를 만든 사용자에게만 주어진다. EMP 테이블은 SCOTT 사용자 소유의 테이블이기에 SCOTT 사용자로 로그인해서 USEREDU 사용자가 테이블 객체 EMP를 조회할 수 있도록 권한을 부여해야 한다.

❑ 예 1) SCOTT 사용자로 접속한다.

SQL> CONN SCOTT/TIGER;
SQL> SHOW USER;

10-1장. 데이터베이스 보안을 위한 권한

- 예 2) SCOTT 사용자 소유의 EMP 테이블을 조회할 수 있는 SELECT 권한을 USEREDU 사용자에게 부여한다.

```
SQL> GRANT SELECT ON EMP TO USEREDU;

권한이 부여되었습니다.
```

- 예 3) 권한이 부여 되었다면 다시 USEREDU 사용자로 로그인하여 EMP 테이블에 접속한다.

```
SQL> CONN USEREDU/TIGER;
연결되었습니다.
SQL> SHOW USER;
USER은 "USEREDU"입니다
SQL> SELECT * FROM EMP;
SELECT * FROM EMP
              *
1행에 오류:
ORA-00942: 테이블 또는 뷰가 존재하지 않습니다
```

- 권한 부여가 되었는데도 USEREDU 사용자가 EMP 테이블 객체를 조회할 수 없다는 것을 확인할 수 있다. 그 이유는 객체의 소유자를 지정하지 않았기 때문이다.

10-1장. 데이터베이스 보안을 위한 권한

❑ 예 4) EMP 앞에 해당 테이블의 소유주인 SCOTT 계정을 기록한다.

SQL> SELECT * FROM SCOTT.EMP;

```
SQL> SELECT * FROM SCOTT.EMP;

     EMPNO ENAME      JOB              MGR HIREDATE         SAL       COMM     DEPTNO
---------- ---------- --------- ---------- -------- ---------- ---------- ----------
      7369 SMITH      CLERK           7902 80/12/17        800                    20
      7499 ALLEN      SALESMAN        7698 81/02/20       1600        300         30
      7521 WARD       SALESMAN        7698 81/02/22       1250        500         30
      7566 JONES      MANAGER         7839 81/04/02       2975                    20
      7654 MARTIN     SALESMAN        7698 81/09/28       1250       1400         30
      7698 BLAKE      MANAGER         7839 81/05/01       2850                    30
      7782 CLARK      MANAGER         7839 81/06/09       2450                    10
      7788 SCOTT      ANALYST         7566 87/04/19       3000                    20
      7839 KING       PRESIDENT            81/11/17       5000                    10
      7844 TURNER     SALESMAN        7698 81/09/08       1500          0         30
      7876 ADAMS      CLERK           7788 87/05/23       1100                    20
      7900 JAMES      CLERK           7698 81/12/03        950                    30
      7902 FORD       ANALYST         7566 81/12/03       3000                    20
      7934 MILLER     CLERK           7782 82/01/23       1300                    10
```

● 자신이 소유한 객체가 아닌 경우에는 그 객체를 소유한 사용자명을 반드시 기술해야 한다.

10-1장. 데이터베이스 보안을 위한 권한)

- 사용자에게 부여된 권한은 어떻게 조회해야 할까?
  - ✓ 사용자 권한과 관련된 데이터 딕셔너리 중에서 USER_TAB_PRIVS_MADE 데이터 딕셔너리는 **현재 사용자가 다른 사용자에게 부여한 권한 정보를 알려준다**
  - ✓ 만일 **자신에게 부여된 사용자 권한을 알고 싶을 때는 USER_TAB_PRIVS_RECD 데이터 딕셔너리를 조회하면 된다.

- 예) USEREDU 와 SCOTT 사용자가 부여한 권한과 부여된 권한이다.
  - ✓ SQL> CONN USEREDU/TIGER;
  - ✓ SQL> COL OWNER FORMAT A10;
  - ✓ SQL> COL TABLE_NAME FORMAT A10;
  - ✓ SQL> SELECT * FROM USER_TAB_PRIVS_MADE;
  - ✓ SQL> SELECT * FROM USER_TAB_PRIVS_RECD;

```
SQL> CONN USEREDU/TIGER;
연결되었습니다.
SQL> COL OWNER FORMAT A10;
SQL> COL TABLE_NAME FORMAT A10;
SQL> SELECT * FROM USER_TAB_PRIVS_MADE;

선택된 레코드가 없습니다.

SQL> SELECT * FROM USER_TAB_PRIVS_RECD;

OWNER      TABLE_NAME GRANTOR                        PRIVILEGE                                GRA HIE
---------- ---------- ------------------------------ ---------------------------------------- --- ---
SCOTT      EMP        SCOTT                          SELECT                                   NO  NO
```

10-1장. 데이터베이스 보안을 위한 권한

❑ 예) USEREDU 와 SCOTT 사용자가 부여한 권한과 부여된 권한이다.

- SQL> CONN SCOTT/[사용자 암호];
- SQL> COL OWNER FORMAT A10;
- SQL> COL TABLE_NAME FORMAT A10;
- SQL> COL GRANTEE FORMAT A10;
- SQL> COL GRANTOR FORMAT A10;
- SQL> SELECT * FROM USER_TAB_PRIVS_MADE;
- SQL> SELECT * FROM USER_TAB_PRIVS_RECD;

```
SQL> CONN SCOTT/1234
연결되었습니다.
SQL> COL OWNER FORMAT A10;
SQL> COL TABLE_NAME FORMAT A10;
SQL> COL GRANTEE FORMAT A10;
SQL> COL GRANTOR FORMAT A10;
SQL> SELECT * FROM USER_TAB_PRIVS_MADE;

GRANTEE    TABLE_NAME GRANTOR    PRIVILEGE                                GRA HIE
---------- ---------- ---------- ---------------------------------------- --- ---
USEREDU    EMP        SCOTT      SELECT                                   NO  NO

SQL> SELECT * FROM USER_TAB_PRIVS_RECD;

선택된 레코드가 없습니다.
```

10-1장. 데이터베이스 보안을 위한 권한

- REVOKE
  - ✓ 사용자에게 부여한 객체 권한을 데이터베이스 관리자나 객체 소유자로부터 회수하기 위한 명령어이다.
- 예 1) SCOTT 사용자로 접속하여 SELECT 권한을 절회하기 전에 SCOTT 게정에 설정된 권한을 확인한다.

```
SQL> SELECT * FROM USER_TAB_PRIVS_MADE;

GRANTEE    TABLE_NAME GRANTOR    PRIVILEGE                                GRA HIE
---------- ---------- ---------- ---------------------------------------- --- ---
USEREDU    EMP        SCOTT      SELECT                                   NO  NO
```

- 예 2) USEREDU 사용자에게 부여된 EMP 테이블에 대한 SELECT 권한을 철회한다.

```
SQL> REVOKE SELECT ON EMP FROM USEREDU;

권한이 취소되었습니다.
```

10-1장. 데이터베이스 보안을 위한 권한

- REVOKE
  - ✓ 사용자에게 부여한 객체 권한을 데이터베이스 관리자나 객체 소유자로부터 회수하기 위한 명령어이다.
- 예 3) 권한이 취소되면 데이터 딕셔너리에 존재했던 객체 권한 정보도 함께 사라진다.

```
SQL> SELECT * FROM USER_TAB_PRIVS_MADE;

선택된 레코드가 없습니다.
```

- 예 4) USEREDU 사용자 계정으로 로그인해서 SCOTT 사용자의 EMP 테이블을 사용할 수 없음을 확인한다.

```
SQL> CONN USEREDU/TIGER;
연결되었습니다.
SQL> SELECT * FROM SCOTT.EMP;
SELECT * FROM SCOTT.EMP
                   *
1행에 오류:
ORA-00942: 테이블 또는 뷰가 존재하지 않습니다
```