17장 사용자 관리

17.1 데이터베이스 보안을 위한 권한

17.1.1 보안을 위한 데이터베이스 관리자

- 데이터베이스 관리자는 사용자가 데이터베이스의 객체(테이블, 뷰 등)에 대한 특정 권한을 가질 수 있도록 함으로서 다수의 사용자가 데이터베이스에 저장된 정보를 공유하면서도 정보에 대한 보안이 이루어지도록 한다.
- 사용자마다 서로 다른 권한과 롤을 부여함으로서 보안을 설정할 수 있다.

17.1.2 권한의 역할과 종류

- 권한은 사용자가 특정 테이블을 접근할 수 있도록 하거나 해당 테이블에 SQL(SELECT/INSERT/UPDATE/DELETE) 문을 사용할 수 있도록 제한을 두는 것을 말한다.
- 데이터베이스 보안을 위한 권한은 시스템 권한(System Privileges)과 객체 권한(Object Privileges)으로 나뉜다.
- 시스템 권한은 사용자의 생성과 제거, DB 접근 및 각종 객체를 생성할 수 있는 권한 등 주로 DBA에 의해 부여되며 그 권한의 수가 80 가지가 넘기에 대표적인 시스템 권한은 다음과 같다.

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
BACKUP ANY TABLE	임의의 테이블을 백업할 수 있는 권한
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 PROCEDURE	사용자 스키마에서 함수를 생성할 수 있는 권한

17.2 사용자 생성하기

- 오라클 데이터베이스를 설치할 때 자동으로 생성되는 디폴트 사용자 가운데 시스템 권한을 가진 데이터베이스 관리자인 DBA는 SYS, SYSTEM 이다.
- 사용자 계정을 발급 받기 위해서 시스템 권한을 가진 SYSTEM으로 접속해야 한다.

```
-- 형식
CREATE USER USER_NAME IDENTIFIED BY PASSWORD;

-- 예
CREATE USER USER10 IDENTIFIED BY USER10;
ALTER USER SYSTEM IDENTIFIED BY MANAGER;  -- 비밀번호 변경하기
ALTER USER SCOTT IDENTIFIED BY TIGER;
```

[실습] CREATE USER 명령어를 이용한 사용자 생성

- CREATE USER 명령어를 사용하여 사용자명은 USER01 암호는 TIGGER로 사용자를 생성해 보겠

다.

```
CONN SYSTEM/MANAGER
SHOW USER

DROP USER USER01 CASCADE;
CREATE USER USER01 IDENTIFIED BY TIGER;

CONN USER01/TIGER
-- 접속에 실패한다. 사용자에 아무런 권한이 부여되지 않았기 때문이다.
```

[LAB_17_1.SQL]

```
01    CONN SYSTEM/MANAGER
02    SHOW USER
03
04    DROP USER USER01 CASCADE;
05    CREATE USER USER01 IDENTIFIED BY TIGER;
06
07    CONN USER01/TIGER
08    -- 접속에 실패한다. 사용자에 아무런 권한이 부여되지 않았기 때문이다.
```

17.3 권한을 부여하는 GRANT 명령어

■ 사용자에게 시스템 권한 부여하기 위해서는 GRANT 명령어를 사용한다.

```
-- 형식
GRANT PRIVILEGE_NAME, …
TO USER_NAME;
```

[실습] CREATE SESSION 권한 부여하기

■ 새로 생성된 USER01에 데이터베이스에 접속할 수 있는 권한인 CREATE SESSION을 부여한다. 다시 USER01 사용자로 접속을 시도하면 이번에는 데이터베이스에 성공적으로 접속된다.

[LAB_17_2.SQL]

```
01    CONN SYSTEM/MANAGER
02    SHOW USER
03
04    DROP USER USER01 CASCADE;
05    CREATE USER USER01 IDENTIFIED BY TIGER;
06
07    GRANT CREATE SESSION TO USER01;
08
09    CONN USER01/TIGER
```

[실습] CREATE TABLE 권한 부여하기

■ 새롭게 생성된 사용자 계정은 테이블을 생성할 권한을 부여받아야만 CREATE TABLE 명령을 사

용할 수 있다.

[LAB_17_3.SQL]

```
01    DROP TABLE EMP01;
02    CREATE TABLE EMP01(
03    EMPNO NUMBER(4),
04    ENAME VARCHAR2(10),
05    JOB VARCHAR2(9),
06    DEPTNO NUMBER(2)
07    );
08
09    CONN SYSTEM/MANAGER
10    SHOW USER
11
12    GRANT CREATE TABLE, RESOURCE TO USER01;
13
14    CONN USER01/TIGER
15    SHOW USER
16
17    DROP TABLE EMP01;
18    CREATE TABLE EMP01(
19    EMPNO NUMBER(4),
20    ENAME VARCHAR2(10),
21    JOB VARCHAR2(9),
22    DEPTNO NUMBER(2)
23    );
```

17.3.1 테이블 스페이스 확인하기

■ 테이블스페이스(Tablespace)는 디스크 공간을 소비하는 테이블과 뷰 그리고 그 밖의 다른 데이터베이스 객체들이 저장되는 장소이다.

```
CONN SYSTEM/MANAGER
SHOW USER

SELECT USERNAME, DEFAULT_TABLESPACE
FROM DBA_USERS
WHERE USERNAME IN('USER01', 'SCOTT');

-- 테이블 스페이스 쿼터 할당하기
CONN SYSTEM/MANAGER
SHOW USER

ALTER USER USER01
QUOTA 2M ON USERS;

-- CREATE TABLE 생성하기
CONN USER01/TIGER;
SHOW USER;

DROP TABLE EMP01;
CREATE TABLE EMP01(
EMPNO NUMBER(4),
ENAME VARCHAR2(10),
JOB VARCHAR2(9),
DEPTNO NUMBER(2)
);
```

17.3.2 WITH ADMIN OPTION

- 사용자에게 시스템 권한을 WITH ADMIN OPTION과 함께 부여하면 그 사용자는 데이터베이스 관리자가 아닌데도 불구하고 부여받은 시스템 권한을 다른 사용자에게 부여할 수 있는 권한도 함께 부여 받게 된다.

```
-- WITH ADMIN OPTION을 지정하여 권한 부여하기
CONN SYSTEM/MANAGER
SHOW USER

CREATE USER USER02 IDENTIFIED BY TIGER;
GRANT CREATE SESSION TO USER02 WITH ADMIN OPTION;

CONN USER02/TIGER;
SHOW USER;

GRANT CREATE SESSION TO USER01;

-- WITH ADMIN OPTION을 지정하지 않고 권한 부여하기
CONN SYSTEM/MANAGER
SHOW USER

CREATE USER USER03 IDENTIFIED BY TIGER;
GRANT CREATE SESSION TO USER03;

CONN USER03/TIGER;
SHOW USER;

GRANT CREATE SESSION TO USER01;
-- 자기가 받은 권한을 다른 사용자에게 부여할 수 없다.
```

17.4 객체 권한

17.4.1 객체와 권한 설정

- 객체 권한은 특정 객체에 조작을 할 수 있는 권한입니다. 객체의 소유자는 객체에 대한 모든 권한을 가진다.
- 객체 권한은 테이블이나 뷰나 시퀀스나 함수 등과 같은 객체별로 DML문(SELECT, INSERT, DELETE)을 사용할 수 있는 권한을 설정하는 것이다.

```
-- 형식
GRANT PRIVILEGE_NAME [(COLUMN_NAME)] | ALL
ON OBJECT_NAME | ROLE_NAME | PUBLIC
TO USER_NAME;
```

17.4.2 다른 유저의 객체 접근하기

```
CONN USER01/TIGER;
SHOW USER;
SELECT * FROM EMP;  -- 조회할 수 없다.
```

```
-- 테이블 객체에 대한 SELECT 권한 부여하기
CONN SCOTT/TIGER;
SHOW USER;
GRANT SELECT ON EMP TO USER01;

CONN USER01/TIGER;
SHOW USER;
SELECT * FROM SCOTT.EMP;
```

17.4.3 스키마 알아보기

- 스키마(SCHEMA)란 객체를 소유한 사용자명을 의미한다. 객체 명 앞에 소속 사용자명을 기술한다.
- 자신이 소유한 객체를 언급할 때 객체 명 앞에 스키마를 생략할 수 있다.

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

17.4.4 사용자에게 부여된 권한 조회

- 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 때에는 USER_TAB_PRIVS_RECD 데이터 딕셔너리를 조회하면 된다.

```
CONN SCOTT/TIGER
SELECT * FROM USER_TAB_PRIVS_MADE;
SELECT * FROM USER_TAB_PRIVS_RECD;
```

17.4.5 사용자에게서 권한을 뺏기 위한 REVOKE 명령어

- 사용자에게 부여한 객체 권한을 데이터베이스 관리자나 객체 소유자로부터 철회하기 위해서는 REVOKE 명령어를 사용한다.

```
-- 형식
REVOKE {privilege_name | all}
ON object_name
FROM {user_name | role_name | public};

-- 예: 객체 권한 제거하기
SELECT * FROM USER_TAB_PRIVS_MADE;
REVOKE SELECT ON EMP FROM USER01;
SELECT * FROM USER_TAB_PRIVS_MADE;

CONN USER01/TIGER
SELECT * FROM SCOTT.EMP;
```

17.4.6 WITH GRANT OPTION

- 사용자에게 객체 권한을 WITH GRANT OPTION과 함께 부여하면 그 사용자는 그 객체를 접근할 권한을 부여 받으면서 그 권한을 다른 사용자에게 부여 할 수 있는 권한도 함께 부여받게 된다.

```
GRANT SELECT ON SCOTT.EMP TO USER02
WITH GRANT OPTION;

CONN USER02/TIGER;
GRANT SELECT ON SCOTT.EMP TO USER01;
```

[과제] 과제-17-01.TXT

1. 전산실에 새로 입사한 사원에게 새로운 계정을 생성해 주려고 합니다.아래의 요구 사항을 만족하는 SQL문을 각각 작성 하세요 ?
   [요구1] USER명 : woman, 패스워드 : tiger
   [요구2] CREATE SESSION 이라는 시스템 권한을 부여해 줍니다.
   (단, 또 다른 유저에게도 권한을 줄 수 있도록 WITH ADMIN OPTION을 부여합니다).

<정답>

2. user01 계정(비밀번호: tiger)을 생성하고 해당 계정에게 오라클 데이터 베이스에 접속해서, 테이블을 생성할 수 있는 권한을 부여하시오.

<정답>