ch15. 사용자, 권한, 롤 관리

15-1. 사용자 관리

사용자란?

오라클 데이터 베이스에서는 데이터 베이스에 접속하여 데이터를 관리하는 계정을 사용자(USER)로 표현한다.

사용자 관리가 필요한 이유

- 데이터를 활용한 서비스 규모가 크거나 작은 규모의 여러 서비스를 통합한 방식 등 실무에서 사용하는 여러 종류에 서비스는 한 사용자가 관리하기에는 데이터 분량이 너무 방대하거나 구조가 복잡해지는 경우가 많다.
  - ⇒ 따라서, 업무 분할과 효율, 보안을 고려하여 업무에 따라 여러 사용자들을 나눈다.
- 오라클 데이터베이스는 테이블, 인덱스, 뷰 등 여러 객체가 사용자별로 생성되므로 업무별 사용자를 생성한 후에 각 사용자 업무에 맞는 데이터 규조를 만들어 관리하는 방식을 사용할 수 있다.
- 반대로 대표 사용자를 통해 업무에 맞는 데이터 구조를 먼저 정의한 뒤에 사용할 수 있는 데이터 영역을 각 사용자에게 지정해 줄 수도 있다.

데이터베이스 스키마란?

- 데이터베이스에서 데이터 간 관계, 데이터 구조, 제약 조건 등 데이터를 저장 및 관리하기 위해 정의한 데이터베이스 구조의 범위를 스키마 (schema)를 통해 그룹 단위로 분류한다.
- 오라클 데이터베이스에서는 스키마와 사용자를 구별하지 않고 사용하기도 한다.
  - 사용자 : 데이터를 사용 및 관리하기 위해 오라클 데이터베이스에 접속하는 개체
    - ex) SCOTT
  - 스키마 : 오라클 데이터베이스에 접속한 사용자와 연결된 객체

    - ex) SCOTT 이 생성한 테이블, 뷰, 제약 조건, 인덱스, 시퀀스, 동의어 등 데이터베이스에서 SCOTT 계정으로 만든 모든 객체

사용자 생성

오라클 사용자를 생성할 때는 CREATE USER문을 사용한다.

```
CREATE USER 사용자 이름(필수)
IDENTIFIED BY 패스워드(필수)
DEFAULT TABLESPACE 테이블 스페이스 이름(선택)
TEMPORARY TABLESPACE 테이블 스페이스(그룹) 이름(선택)
QUOTA 테이블 스페이스크기 ON 테이블 스페이스 이름(선택)
PROFILE 프로파일 이름(선택)
PASSWORD EXPIRE(선택)
ACCOUNT [LOCK/UNLOCK](선택);
```

- SCOTT계정으로 사용자 생성하기

```
CREATE USER ORCLSTUDY
IDENTIFIED BY ORACLE;
```

- 사용자 생성은 일반적으로 데이터베이스 관리 권한을 가진 사용자가 권한을 가지고 있다.
- 오라클 데이터 베이스를 설치할 때 자동으로 생성된 SYS, SYSTEM이 데이터베이스 관리 권한을 가진 사용자이다.

- SYSTEM 사용자로 접속 후 사용자 생성하기 (SQL*PLUS)

```
$ SQLPLUS SYSTEM/oracle
```

```
$ CREATE USER ORCLSTUDY
   IDENTIFIED BY ORACLE;
```

```
C:₩Users₩kimra>SQLPLUS SYSTEM/oracle

SQL*Plus: Release 11.2.0.1.0 Production on 토 8월 6 22:07:44 2022

Copyright (c) 1982, 2010, Oracle.  All rights reserved.


다음에 접속됨:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> CREATE USER ORCLSTUDY
  2  IDENTIFIED BY ORACLE;

사용자가 생성되었습니다.
```

⇒ 사용자가 생성되긴 했지만 데이터베이스 연결을 위한 권한, 즉 CREATE SESSION 권한을 부여받지
못한 상태.

- SYSTEM 사용자로 접속 후 ORCLSTUDY 사용자에게 권한 부여하기

  `$ CONN SYSTEM/oracle`

  `$ GRANT CREATE SESSION TO ORCLSTUDY`

⇒ ORCLSTUDY 사용자로 데이터베이스에 접속할 수는 있지만 SCOTT계정처럼 테이블을 만들고
데이터를 사용하려면 몇몇 권한이 더 필요한 상태이다.

사용자 정보 조회

사용자 또는 사용자 소유 객체 정보를 얻기 위해 다음과 같이 데이터 사전을 사용할 수 있다.

```
SELECT * FROM ALL_USERS
  WHERE USERNAME = 'ORCLSTUDY';
```

```
SELECT * FROM DBA_USERS
  WHERE USERNAME = 'ORCLSTUDY';
```

```
SELECT * FROM DBA_OBJECTS
  WHERE USERNAME = 'ORCLSTUDY';
```

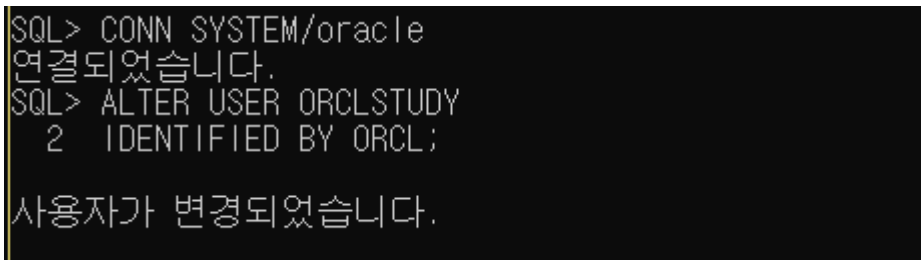
오라클 사용자의 변경과 삭제

오라클 사용자 변경

사용자 정보를 변경할 때에는 ALTER USER문을 사용한다.

- 사용자 정보(패스워드) 변경하기 ORCLSTUDY → ORCL

```
$ ALTER USER ORCLSTUDY
   IDENTIFIED BY ORCL;
```



오라클 사용자 삭제

- DROP USER문을 사용하여 사용자를 삭제한다.
- 삭제하려는 사용자가 다른 곳에서 접속되어 있다면 삭제되지 않는다.

```
$ DROP USER ORCLSTUDY;
```

오라클 사용자와 객체 모두 삭제

사용자 스키마에 객체가 있을 경우에 CASCADE 옵션을 사용하여 사용자와 객체를 모두 삭제할 수 있다.

```
$ DROP USER ORCLSTUDY CASCADE;
```

15-2. 권한 관리

- 데이터를 안전하게 보관하고 특정 데이터에 대해서 관련된 사용자만 데이터를 사용 및 관리할 수 있는 보안 장치가 필요하다
    - 그 첫 번째가 사용자 이름과 페스워드를 통해 데이터 베이스 접속을 허가하는 것이다.
- 하지만, 특정 사용자 정보를 통해 데이터베이스에 접속하는 것만으로 데이터베이스의 모든 데이터를 사용할 수 있다면 여전히 데이터 안전을 보장하기는 어려울 것이다.
- 따라서, 데이터베이스는 접속 사용자에 따라 접근할 수있는 데이터 영역과 권한을 지정해 줄 수 있다.

- 오라클에서의 권한
    - 시스템 권한 *system privilege*
    - 객체 권한 *object privilege*

시스템 권한이란?

- 오라클 데이터베이스의 시스템 권한은 사용자 생성과 정보 수정 및 삭제, 데이터베이스 접근, 오라클 데이터베이스의 여러 자원과 객체 생성 및 관리 등의 권한을 포함한다.
    - 이러한 내용은 데이터베이스 관리 권한이 있는 사용자가 부여될 수 있는 권한이다.

권 한	기 능
CREATE USER	계정 생성 권한
DROP USER	계정 삭제 권한
DROP ANY TABLE	임의 테이블 삭제 권한
CREATE SESSION	데이터베이스 접속 권한
CREATE TABLE	테이블 생성 권한
CREATE VIEW	뷰 생성 권한
CREATE SEQUENCE	시퀀스 생성 권한
CREATE PROCEDURE	함수 생성 권한

시스템 권한 부여

- ORCLSTUDY 사용자에게 CREATE SELSSION 권한을 부여하기

```
$ GRANT CREATE SESSION TO ORCLSTUDY;
```

이처럼 시스템 권한을 부여할 때 다음과 같이 GRANT 문을 사용한다.

```
GRANT [시스템 권한] TO [사용자 이름/롤(ROLE)이름/PUBLIC]
[WITH ADMIN OPTION];
```

[시스템 권한]	오라클 데이터베이스에서 제공하는 시스템 권한을 지정한다. 한 번에 여러 종류의 권한을 부여하려면 쉼표로 구분하여 권한 이름을 여러 개 명시해 주면 된다.(필수)
[사용자 이름/롤(ROLE)이름/PUBLIC]	권한을 부여하려는 대상을 지정한다. 사용자 이름을 지정해 줄 수도 있고, 이후 소개할 롤을 지정할 수도 있다. 여러 사용자 또는 롤에 적용할 경우, 쉼표로 구분한다. PUBLIC은 현재 오라클 데이터베이스의 모든 사용자에게 권한을 부여하겠다는 의미이다.(필수)
[WITH ADMIN OPTION]	현재 GRANT문을 통해 부여 받은 권한을 다른 사용자에게 부여할 수 있는 권한도 함께 부여 받는다. 현재 사용자가 권한이 사라져도, 권한을 재부여한 다른 사용자의 권한은 유지된다.(선택)

- SYSTEM 계정으로 접속하여 사용자 (ORCLSTUDY) 생성하기

```
$ CREATE USER ORCLSTUDY
  IDENTIFIED BY ORACLE;
```

- 사용자 권한 부여하기

```
$ GRANT RESOURCE, CREATE SESSION, CREATE TABLE TO ORCLSTUDY;
```

시스템 권한 취소

- GRANT 명령어로 부여한 권한의 취소는 REVOKE 명령어를 사용한다.

```
REVOKE [시스템 권한] FROM [사용자 이름/롤 이름/ PUBLIC];
```

객체 권한이란?

- 객체 권한은 특정 사용자가 생성한 테이블, 인덱스, 뷰, 시퀀스 등과 관련된 권한이다.
    - 예를 들어, SCOTT 소유 테이블에 ORCLSTUDY 사용자가 SELECT나 INSERT 등의 작업이 가능하도록 허용할 수 있다.

객체 권한

객체 권한	테이블	뷰	시퀀스	프로시저
ALTER	√	√	√	√
DELETE	√	√		
EXECUTE				√
INDEX	√	√		
INSERT	√	√		
REFERENCES	√			
SELECT	√	√	√	
UPDATE	√	√		

ORACLE

16-13

객체 권한 부여

- 객체 권한 부여 역시 GRANT문을 사용한다.

```
GRANT[객체 권한/ALL PREVILEGES]   ... 1
ON[스키마.객체이름]               ... 2
TO[사용자 이름/롤 이름/PUBLIC]    ... 3
[WITH GRANT OPTION];              ... 4
```

1	오라클 데이터베이스에서 제공하는 객체 권한을 지정한다. 한 번에 여러 종류의 권한을 부여하려면 쉽표로 구분하여 권한을 여러 개 명시해 주면 된다. ALL PREVILEGES는 객체의 모든 권한을 부여함을 의미한다.(필수)
2	권한을 부여할 대상 객체를 명시한다.(필수)

3	권한을 부여하려는 대상을 지정한다. 사용자 이름을 지정해 줄 수도 있고, 소개할 롤을 지정할 수도 있다. 여러 사용자 또는 롤에 적용할 경우 쉼표로 구분한다. PUBLIC은 현재 오라클 데이터베이스의 모든 사용자에게 권한을 부여하겠다는 의미이다.
4	현재 GRANT문을 통해 부여받은 권한을 다른 사용자에게 부여할 수 있는 권한도 함께 부여받는다. 현재 권한을 부여 받은 사용자의 권한이 사라지면, 다른 사용자에게 재부여된 권한도 함께 사라진다.

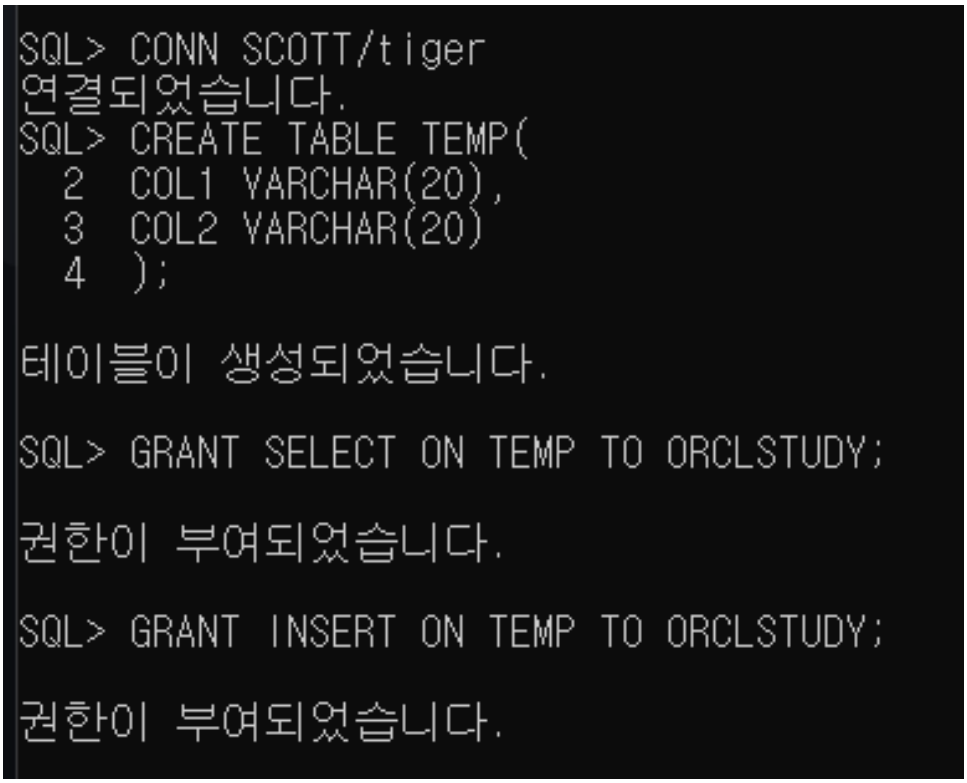
- ORCLSTUDY 사용자에게 TEMP 테이블 권한 부여하기

```
$ CONN SCOTT/tiger
```

```
$ CREATE TABLE TEMP (
    COL1 VARCHAR(20),
    COL2 VARCHAR(20)
 );
```

```
$ GRANT SELECT ON TEMP TO ORCLSTUDY;
```

```
$ GRANT INSERT ON TEMP TO ORCLSTUDY;
```



⇒ SELECT와 INSERT 권한을 두 개의 GRANT문으로 나누어 객체 권한을 부여했다.

- ORCL에게 TEMP 테이블의 여러 권한을 한 번에 부여하기

```
$ GRANT SELECT, INSERT ON TEMP
      TO ORCLSTUDY;
```

```
SQL> GRANT SELECT, INSERT ON TEMP
  2  TO ORCLSTUDY;

권한이 부여되었습니다.
```

- ORCLSTUDY로 사용 권한을 부여받은 TEMP 테이블 사용하기

```
$ CONN ORCLSTUDY/ORACLE
$ SELECT * FROM SCOTT.TEMP;
$ INSERT INTO SCOTT.TEMP VALUES('TEXT', 'FROM ORCLSTUDY');
$ SELECT * FROM SCOTT.TEMP;
```

```
SQL> CONN ORCLSTUDY/ORACLE
연결되었습니다.
SQL> SELECT * FROM SCOTT.TEMP;

선택된 레코드가 없습니다.

SQL> INSERT INTO SCOTT.TEMP VALUES('TEXT', 'FROM ORCLSTUDY');

1 개의 행이 만들어졌습니다.

SQL> SELECT * FROM SCOTT.TEMP;

COL1                 COL2
-------------------- --------------------
TEXT                 FROM ORCLSTUDY
```

객체 권한 취소

객체 권한의 취소도 시스템 권한과 마찬가지로 REVOKE문을 사용한다.

```
REVOKE [객체 권한/ALL PREVILEGES] (필수)
ON [스키마.객체이름] (필수)
```

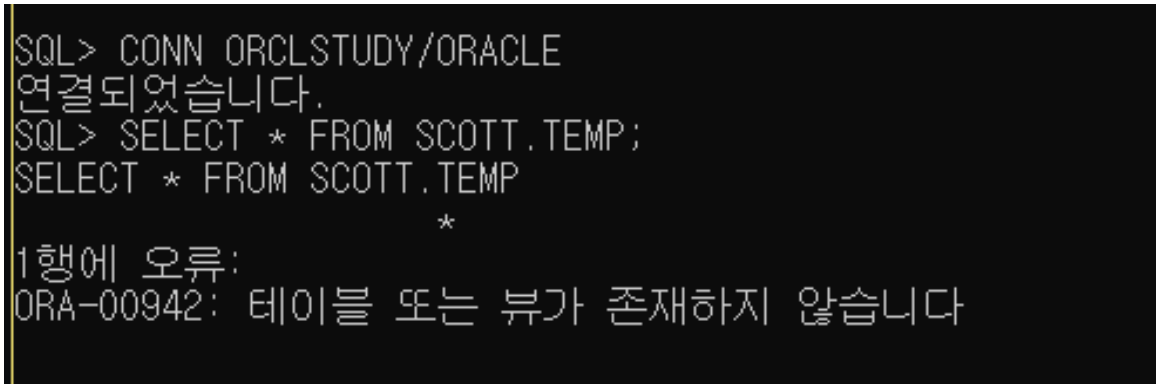
```
FROM [사용자 이름/롤 이름/PUBLIC](필수)
[CASCADE CONSTRAINTS/FORCE](선택);
```

- ORCLSTUDY에 부여된 TEMP테이블 사용 권한 취소하기

```
$ CONN SCOTT/tiger
$ REVOKE SELECT, INSERT ON TEMP FROM ORCLSTUDY;
```

- ORCLSTUDY로 권한 철회된 TEMP 테이블 조회하기 (실패)

```
$ CONN ORCLSTUDY/ORACLE
$ SELECT * FROM SCOTT.TEMP;
```



15-3. 롤 관리

> 롤이란?

- 앞에서 ORCLSTUDY 사용자를 생성하고 여러 가지 권한을 부여하고 취소해보았다.

    - 사용자는 데이터베이스에서 어떤 작업을 진행하기 위해 해당 작업과 관련된 권한을 반드시 부여 받아야 한다.
    - 하지만, 신구 생성자는 아무런 권한이 없으므로 오라클 데이터베이스에서 제공하는 권한을 일일이 부여해 주어야 한다.
    - 이러한 불편한 점을 해결하기 위해 롤(ROLE)을 사용한다.
- 롤은 여러 종류의 권한을 묶어 놓은 그룹을 뜻한다.
    - 롤을 사용하면 여러 권한을 한 번에 부여하고 해제할 수 잇으므로 권한 관리 효율을 높일 수 있다.

⇒ 롤은 오라클 데이터 베이스를 설치할 때 기본으로 제공되는 사전 정의된 롤 *predefined roles* 과
사용자 정의 롤 *user roles* 로 나뉜다.

사전 정의된 롤

1. CONNECT 롤

   사용자가 데이터 베이스에 접속하는 데 필요한 CREATE SESSION 권한을 가지고 있다.

   > 📎 ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE,
   > CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW

2. RESOURCE 롤

   사용자가 테이블, 시퀀스를 비롯한 여러 객체를 생성할 수 있는 기본 시스템 권한을 묶어 놓은 롤이다.

   > 📎 CREATE TRIGGER, CREATE SEQUENCE, CREATE TYPE, CREATE PROCEDURE,
   > CREATE CLUSTER, CREATE OPERATOR, CREATE INDEXTYPE, CREATE TABLE

⇒ 보통 새로운 사용자를 생성하면 CONNEXT 롤과 RESOURCE 롤을 부여하는 경우가 많다.

⇒ CONNECT롤에서 뷰를 생성하는 CREATE VIEW 권한과, 동의어를 생성하는 CREATE SYNONYM
권한이 제외되었기 때문에 뷰와 동의어 생성 권한을 사용자에게 부여하려면,
이 두 권한을 따로 부여해 주어야 한다.

3. DBA 롤

   데이터 베이스를 관리하는 시스템 권한을 대부분 가지고 있으며 매우 강력한 롤이다.

사용자 정의 롤

- 사용자 정의 롤은 필요에 의해 직접 권한을 포함시킨 롤을 뜻한다.
- 다음 절차를 따라 롤을 생성해서 사용할 수 있다.
  1. CREATE ROLE 문으로 롤을 생성합니다.
  2. GRANT 명령어로 생성한 롤에 권한을 포함시킵니다.
  3. GRANT 명령어로 권한이 포함된 롤을 특정 사용자에게 부여합니다.
  4. REVOKE 명령어로 롤을 취소시킵니다.

롤 생성과 권한 포함

- 롤을 생성하려면 데이터 관리 권한이 있는 사용자가 필요하다.

- SYSTEM 계정으로 ROLESTUDY 롤 생성 및 권한 부여하기

```
$ CONN SYSTEM/oracle
$ CREATE ROLE ROLESTUDY;
$ GRANT CONNECT, RESOURCE, CREATE VIEW, CREATE SYNONYM
   TO ROLESTUDY;
```

```
SQL> CONN SYSTEM/oracle
연결되었습니다.
SQL> CREATE ROLE ROLESTUDY;

롤이 생성되었습니다.

SQL> GRANT CONNECT, RESOURCE, CREATE VIEW, CREATE SYNONYM
  2  TO ROLESTUDY;

권한이 부여되었습니다.
```

- ORCLSTUDY 사용자에게 롤(ROLESTUDY) 부여하기

```
$ GRANT ROLESTUDY TO ORCLSTUDY;
```

```
SQL> GRANT ROLESTUDY TO ORCLSTUDY;

권한이 부여되었습니다.
```

부여된 롤과 권한 확인

- ORCLSTUDY 사용자에 현재 부여된 권한과 롤을 확인하려면 USER_SYS_PRIVS, USER_POLE_PRIVS 데이터 사전을 사용하면 된다.
- 데이터 관리 권한을 가진 계정은 DBA_SYS_PRIS, ROLE_PRIVS를 사용해도 된다.

- ORCLSTUDY에 부여된 롤과 권한 확인하기

```
$ CONN ORCLSTUDY/ORACLE
```

```
$ SELECT * FROM USER_SYS_PRIVS;
```

```
$ SELECT * FROM USER_ROLE_PRIVS;
```

```
SQL> CONN ORCLSTUDY/ORACLE
연결되었습니다.
SQL> SELECT * FROM USER_SYS_PRIVS;

USERNAME                       PRIVILEGE                                ADM
------------------------------ ---------------------------------------- ---
ORCLSTUDY                      CREATE TABLE                             NO
ORCLSTUDY                      UNLIMITED TABLESPACE                     NO
ORCLSTUDY                      CREATE SESSION                           NO

SQL> SELECT * FROM USER_ROLE_PRIVS;

USERNAME                       GRANTED_ROLE                   ADM DEF OS_
------------------------------ ------------------------------ --- --- ---
ORCLSTUDY                      RESOURCE                       NO  YES NO
ORCLSTUDY                      ROLESTUDY                      NO  YES NO
```

부여된 롤 취소

GRANT 명령어로 부여한 ROLE을 취소할 때 REVOKE문을 사용한다.

```
$ CONN ORCLSTUDY/ORACLE
$ REVOKE ROLESTUDY FROM ORCLSTUDY;
```

롤 삭제

롤 삭제는 DROP 명령어를 사용한다.

```
$ DROP ROLE ROLESTUDY;
```

Q

1.

```
$ CONN SYSTEM/oracle
$ CREATE USER PREV_HW
   IDENTIFIED BY ORCL;
```

```
$ GRANT CREATE SESSION TO PREV_HW;
```

```
$ SQLPLUS PREV_HW/ORCL
```

```
C:₩Users₩kimra>SQLPLUS PREV_HW/ORCL

SQL*Plus: Release 11.2.0.1.0 Production on 월 8월 8 15:56:53 2022

Copyright (c) 1982, 2010, Oracle.  All rights reserved.


다음에 접속됨:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
```

2.

```
$ CONN SCOTT/tiger
```

```
$ GRANT SELECT ON EMP TO PREV_HW;
$ GRANT SELECT ON DEPT TO PREV_HW;
$ GRANT SELECT ON SALGRADE TO PREV_HW;
```

```
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


     EMPNO ENAME      JOB              MGR HIREDATE         SAL       COMM
```

```
SELECT * FROM SCOTT.DEPT;
```

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

    DEPTNO DNAME          LOC
---------- -------------- -------------
        10 ACCOUNTING     NEW YORK
        20 RESEARCH       DALLAS
        30 SALES          CHICAGO
        40 OPERATIONS     BOSTON
```

```
SELECT * FROM SCOTT.SALGRADE;
```

```
SQL> SELECT * FROM SCOTT.SALGRADE
  2  ;

     GRADE      LOSAL      HISAL
---------- ---------- ----------
         1        700       1200
         2       1201       1400
         3       1401       2000
         4       2001       3000
         5       3001       9999
```

3.

```
$ REVOKE SELECT ON SALGRADE FROM PREV_HW;
```

```
$ CONN PREV_HW/ORCL
$ SELECT * FROM SCOTT.SALGRADE;
```

```
SQL> REVOKE SELECT ON SALGRADE FROM PREV_HW;

권한이 취소되었습니다.

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