UNIT 12

권한과 특권

DB2는 운영체제 또는 전문 보안 소프트웨어에서 제공하는 사용자 관리 기능을 이용하여 데이터베이스 접속 시에 사용자 인증을 실행합니다. 인스턴스 수준의 조작을 위한 여러 단계의 권한 체계를 제공하며, GRANT문과 REVOKE문으로 데이터베이스 오브젝트 별 특권을 제어하여 그룹과 사용자의 액세스 유형을 제한합니다.

DB2 9.7 운영자 가이드

Administrator Edition

- 사용자 인증
- SERVER 인증 유형
- CLIENT 인증 유형
- 권한
- 권한별 기능
- 인스턴스 권한 제어 방법
- 데이터베이스 권한 제어 방법
- 특권
- 특권 제어 방법
- 데이터베이스 특권
- 테이블스페이스 특권
- 스키마 특권
- 테이블 특권
- 뷰 특권
- 인덱스 특권
- 패키지 특권
- 루틴 특권
- 시퀀스 특권
- 간접 권한과 특권

TOPIC 12 01 사용자 인증

Point

DB2는 운영체제 또는 보안 소프트웨어의 사용자 관리 기능을 이용합니다. CONNECT문에서 제공된 사용자 ID와 암호를 이들에게 전달하여 유효한 사용자인지를 점검하게 합니다. 기본 인증 방식은 SERVER입니다.

Tip

잘못된 사용자ID 또는 암호를 제공하면, SQL30082N와 이유 "24 " 가 반환되면서 접속이 실패합니다.

Tip

원격 데이터베이스에 접속할 때는 반드시 사용자 ID와 암호를 명시적으로 제공해야 합니다.

Tip

catalog database 명령어에서 데이터베이스별로 인증 방식을 지정할 수 있습니다.

Tip

AUTHENTICATION의 값에 변경하면, 인스턴스를 재기동해야 합니다.

1. 모든 응용프로그램은 데이터베이스에 접속할 때, connect 문을 이용하여 사용자 ID와 암호명을 명시하게 됩니다. 명시한 사용자 ID와 암호명이 유효하지 않으면, 데이터베이스에 대한 접속은 허용되지 않습니다.

```
$ db2 connect to <데이터베이스명> user <사용자명> using <암호명>
```

2. connect 문에서 사용자 ID와 암호를 명시하지 않으면, 현재 세션의 로그인 사용자와 암호명이 사용됩니다.

```
$ db2 connect to <데이터베이스명>
```

3. connect 문에서 제공된 사용자 ID와 암호를 이용하여 OS의 사용자 관리 기능을 요청합니다. 사용자 인증의 방식은 인스턴스 구성 변수인 AUTHENTICATION에 의해 결정되며, 대표적인 인증 방식은 다음과 같습니다.

인 증 방 식	설 명
SERVER	목표 데이터베이스가 존재하는 서버에서 사용자 인증됩니다.
SERVER_ENCRYPT	목표 데이터베이스가 존재하는 서버에서 사용자 인증되며, 사용자 ID와 암호명이 암호화되어 전송됩니다.
CLIENT	연결 시도하는 클라이언트에서 사용자 인증됩니다.
KERBEROS	Kerberos 보안 메커니즘을 사용하여 인증됩니다.
DATA_ENCRYPT	목표 데이터베이스가 존재하는 서버에서 사용자 인증되며, 해당 연결은 데이터 암호화 됩니다.

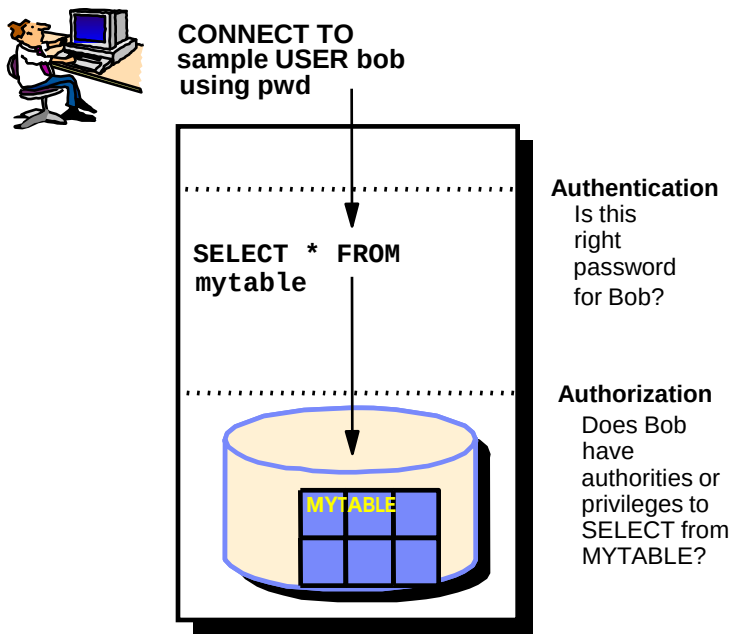

Figure 1201A • • • 사용자 인증과 테이블 액세스 권한

TOPIC 12 02 SERVER 인증 유형

Point

원격 클라이언트에서 데이터베이스 접속 시에 제공된 사용자 ID와 암호는 네트워을 통해서 데이터베이스 서버에 전달되고, 서버의 OS에 의해 사용자 ID와 암호가 점검됩니다. 인스턴스 구성 변수 AUTHENTICATION의 값은 SERVER 입니다.

Tip

SERVER_ENCRYPT 방식을 사용하면, 전달되는 사용자 ID와 암호를 내부적인 암호화 기법으로 변환하여 전송합니다.

Tip

클라이언트에는 사용자 ID가 존재할 필요가 없습니다.

Tip

클라이언트에 동일한 사용자가 존재하고, 암호가 다른 경우에도 점검은 서버에서 이루어지므로 상관이 없습니다.

1 서버의 인스턴스 구성 변수 AUTHENTICATION을 SERVER로 설정합니다.

```
$ db2 get dbm cfg | grep AUTHENTICATION
데이터베이스 관리 프로그램 인증       (AUTHENTICATION) = SERVER
```

2 클라이언트에서 catalog db 명령어를 이용하여 원격 데이터베이스를 등록합니다.

```
C:\> db2 catalog db <원격데이터베이스명> as <데이터베이스별명> at node
    <원격노드명>
C:\> list database directory | find “인증”
인증                                  = SERVER
```

3 클라이언트에서 connect 문을 이용하여 데이터베이스 서버에 접속을 요청하면, 제공된 사용자ID와 암호가 서버로 전송되어 서버의 OS에 의해 점검됩니다. 서버의 OS에 사용자 ID가 존재하고, 암호명이 일치하면 사용자 인증은 성공하여 데이터베이스에 재한 접속이 허용됩니다.

```
C:\> db2 connect to <데이터베이스별명> user <서버의 사용자 ID> using <서버
    의 암호명>
```

4 서버에 제공된 사용자 ID가 존재하지 않거나, 암호명이 일치하지 않으면 사용자 인증은 실패하고 데이터베이스에 대한 접속은 허용되지 않습니다.

```
C:>db2 connect to sample01 user kr001325 using xx
SQL30082N  보안 이유 "24"("USERNAME AND/OR PASSWORD
    INVALID")(으)로 인해 연결
시도에 실패했습니다.  SQLSTATE=08001
```

$ db2 connect to sample user db2user using db2pwd

④ "db2user" 와 "db2pwd" 가 서버에서 유효한 사용자인지 점검합니다.

③ 사용자 ID "db2user" 와 암호 "db2pwd" 가 서버로 전송됩니다.

② 데이터베이스 sample에 사용자 ID "db2user" 와 암호 "db2pwd" 를 이용하여 접속합니다.

① 클라이언트에 사용자 ID "peter" 와 암호 "peterpwd" 를 이용하여 로그온합니다.

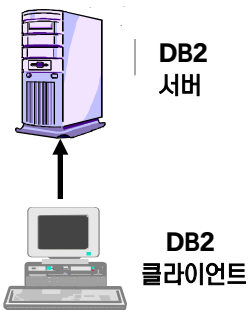

Figure 1202A SERVER 인증

TOPIC 12 03 CLIENT 인증 유형

Point

데이터베이스 접속 시에 제공된 사용자 ID와 암호는 클라이언트의 OS에 의해 점검되고, 인증이 성공하면 사용자 ID를 네트웍을 통해서 데이터베이스 서버에 전달합니다. 인스턴스 구성 변수 AUTHENTICATION의 값은 CLIENT 입니다.

Tip

서버에는 사용자 ID가 존재할 필요가 없습니다.

Tip

서버에 동일한 사용자가 존재하고, 암호가 다른 경우에도 점검은 클라이언트에서 이루어지므로 상관이 없습니다.

1. 서버의 인스턴스 구성 변수 AUTHENTICATION의 값을 CLIENT로 설정합니다.

```
$ db2 update dbm cfg using AUTHENTICATION CLIENT
$ db2stop force
$ db2start
```

2. 클라이언트에서 catalog db 명령어를 이용하여 원격 데이터베이스를 등록합니다.

```
C:\> db2 catalog db <원격데이터베이스명> as <데이터베이스별명> at node
    <원격노드명>
C:\> list database directory | find “인증”
인증                                = CLIENT
```

3. connect 문에서 제공된 사용자ID와 암호는 클라이언트의 OS에 의해 점검됩니다. 클라이언트의 OS에 사용자 ID가 존재하고, 암호명이 일치하면 사용자 인증은 성공하여 데이터베이스에 대한 접속이 허용됩니다. 사용자 ID만 서버로 전송됩니다.

```
C:\> db2 connect to <데이터베이스별명> user <클라이언트의 사용자 ID> using
    <클라이언트의 암호명>
```

4. 제공된 사용자 ID가 클라이언트에 존재하지 않거나, 암호명이 일치하지 않으면 사용자 인증은 실패하고 데이터베이스에 대한 접속은 허용되지 않습니다.

```
C:> db2 connect to <데이터베이스별명> user <클라이언트의 사용자 ID> using
    <잘못된 클라이언트의 암호명>
    SQL30082N  보안 이유 "24"("USERNAME AND/OR PASSWORD
    INVALID")(으)로 인해 연결시도에 실패했습니다.  SQLSTATE=08001
```

$ db2 connect to sample user db2user using db2pwd

⑤ 서버의 사용자 인증은 필요하지 않습니다.

④ 인증이 성공하면, 사용자 ID인 "db2user" 만 서버로 전송됩니다.

③ "db2user" 와 "db2pwd" 가 클라이언트에서 유효한 사용자인지 점검합니다.

② 데이터베이스 sample에 사용자 ID "db2user" 와 암호 "db2pwd" 를 이용하여 접속합니다.

① 클라이언트에 사용자 ID "peter" 와 암호 "peterpwd" 를 이용하여 로그온합니다.

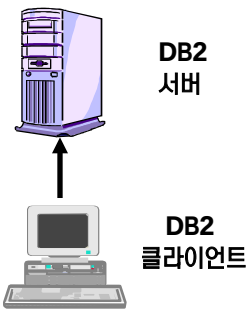

Figure 1203A ··· CLIENT 인증

TOPIC 1204 권한

Point

일련의 DB2 명령어를 실행하거나 데이터베이스를 액세스할 수 있는 능력을 권한이라고 합니다. 권한에는 인스턴스 권한과 데이터베이스 권한으로 분류됩니다.

Tip

상위 권한의 소유자는 하위 권한을 자동으로 소유합니다.

1 인스턴스 권한과 데이터베이스 권한의 체계는 다음과 같이 분류됩니다.

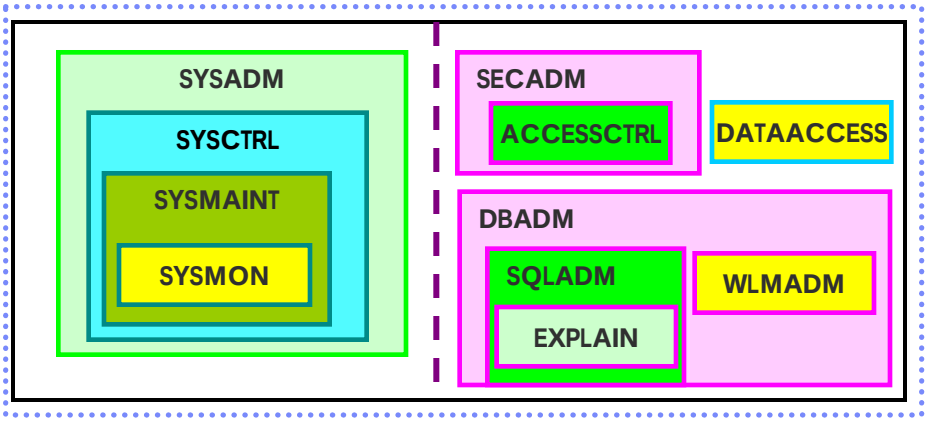

Figure 1204A • • • 인스턴스 권한과 데이터베이스 권한

Tip

인스턴스 권한은 그룹에만 부여되므로 권한 그룹이라고도 합니다.

2 인스턴스 권한은 4가지로 구분됩니다. 인스턴스 구성 변수를 이용하여 OS에 정의된 특정한 그룹 단위로 제어합니다.

권 한	설 명
SYSADM	최고의 인스턴스 권한 그룹으로 인스턴스와 데이터베이스에 대한 모든 유지 보수, 생성, 제거와 연관된 작업을 실행할 수 있습니다. 인스턴스에 존재하는 모든 데이터베이스의 데이터를 직접 액세스할 수 있습니다.
SYSCTRL	인스턴스와 데이터베이스의 유지 보수, 생성, 제거 등과 연관된 명령어를 실행할 수 있으며, 데이터에 대한 직접적인 액세스는 허용되지 않습니다.
SYSMAINT	인스턴스와 데이터베이스의 유지 보수와 관련된 백업 복구 명령어를 실행할 수 있으며, 데이터에 대한 직접적인 액세스는 허용되지 않습니다.
SYSMON	인스턴스 또는 데이터베이스의 시스템 모니터 스냅샷과 연관된 명령어를 실행할 수 있습니다. 데이터에 대한 직접적인 액세스는 허용되지 않습니다.

Tip

9.70이후에는 SYSADM사용자가 더 이상 DBADM권한을 기본으로 보유하지 않습니다. 단, SYSADM권한을 가진 사용자가 데이터베이스를 생성하는 경우에 기존과 동일한 권한을 부여 받을 수 있습니다. 만일 데이터베이스를 생성하지 않은 경우에는 동일한 권한을 가지기 위해서는 SECADM에 의해 DBADM권한을 부여받아야 합니다.

3 데이터베이스 권한은 다음과 같습니다. grant 문과 revoke문을 이용하여 사용자 또는 그룹 단위로 제어할 수 있습니다.

권 한	설 명
SECADM	데이터베이스에 대한 보안 관리자입니다.
DBADM	특정 데이터베이스의 오브젝트에 대한 모든 관리 작업을 할 수 있으며, 해당 데이터베이스의 데이터를 직접 액세스할 수 있습니다.
ACCESSCTRL	ACCESSCTRL, DATAACCESS, DBADM, SECADM 권한 및 감사 루틴에 대한 특권을 제외한 모든 특권과 데이터베이스 권한을 부여/취소 가능합니다.
DATAACCESS	데이터베이스 테이블에 저장된 데이터에 액세스할 수 있도록 허용합니다
SQLADM	SQL문을 모니터하고 조정할 수 있습니다.
WLMADM	워크로드 관리자 역할을 할 수 있습니다. 특히 WLMADM 권한 보유자는 오브젝트 작성 및 삭제, WLM 특권 부여 및 취소, WLM루틴 실행 등을 수행할 수 있습니다.
EXPLAIN	쿼리 계획에 참조된 테이블의 데이터에 액세스할 수 있는 특권 없이 해당 쿼리 계획을 확인할 수 있습니다.

Tip

9.70이후, SECADM은 DBADM 및 SECADM을 포함하여 모든 권한 및 특권을 부여 및 취소할 수 있습니다.

TOPIC 12 05 권한별 기능

Point

SYSADM, SYSCTRL, SYSMAINT, SYSMON 권한은 데이터베이스 시스템과 관련된 명령어를 실행합니다. SYSADM 또는 DBADM, LOAD 권한의 소유자는 데이터베이스와 관련된 명령어를 실행합니다.

Tip

SYSADM, DBADM 권한을 가진 사용자는 데이터베이스에 접속하여 SQL문으로 데이터를 액세스할 수 있습니다.

1 권한별로 실행 가능한 명령어는 다음과 같습니다.

Function	SYSADM	SYSCTRL	SYSMAINT	DBADM
MIGRATE DATABASE	YES			
UPDATE DBM CFG	YES			
GRANT/REVOKE DBADM	YES			
UPDATE db/node/dcs directories	YES	YES		
FORCE USERS OFF SYSTEM	YES	YES		
CREATE/DROP DATABASE	YES	YES		
CREATE/DROP/ALTER TABLE SPACE	YES	YES		
RESTORE TO NEW DATABASE	YES	YES		
UPDATE DB CFG	YES	YES	YES	
BACKUP DATABASE or TABLE SPACE	YES	YES	YES	
RESTORE TO EXISTING DATABASE	YES	YES	YES	
PERFORM ROLLFORWARD RECOVERY	YES	YES	YES	
START/STOP DATABASE INSTANCE	YES	YES	YES	
RESTORE TABLE SPACE	YES	YES	YES	
RUN TRACE	YES	YES	YES	
TAKE DBM or DB SNAPSHOTS	YES	YES	YES	
QUERY TABLE SPACE STATE	YES	YES	YES	YES
UPDATE LOG HISTORY FILES	YES	YES	YES	YES
QUIESCE TABLE SPACE	YES	YES	YES	YES
REORG TABLE	YES	YES	YES	YES
RUN RUNSTATS UTILITY	YES	YES	YES	YES
READ LOG FILES	YES			YES
CREATE/ACTIVATE/DROP EVENT MONITORS	YES			YES

Figure 1205A ··· 권한별로 사용 가능한 명령어

Tip

SYSADM,SYSCTRL,SYSMAINT 권한을 가진 사용자는 SYSMON 권한을 자동으로 소유합니다.

2 SYSMON 권한을 사용하여 사용자는 다음과 같은 명령어를 사용할 수 있습니다

- GET DATABASE MANAGER MONITOR SWITCHES
- GET MONITOR SWITCHES
- GET SNAPSHOT
- LIST ACTIVE DATABASES
- LIST APPLICATIONS
- LIST DCS APPLICATIONS
- RESET MONITOR
- UPDATE MONITOR SWITCHES

Figure 1205B ··· SYSMON 권한으로 가능한 명령어

Tip

SYSADM,DBADM 권한을 가진 사용자는 LOAD 권한을 자동으로 소유합니다.

3 LOAD 권한을 사용하여 사용자는 다음과 같은 명령어를 사용할 수 있습니다

- LOAD
- LIST TABLESPACES
- RUNSTATS
- QUIESCE TABLESPACES FOR TABLE

Figure 1205C ··· LOAD 권한으로 가능한 명령어

TOPIC 12 05 권한별 기능

Point

SYSADM, SYSCTRL, SYSMAINT, SYSMON 권한은 데이터베이스 시스템과 관련된 명령어를 실행합니다. SYSADM 또는 DBADM, LOAD 권한의 소유자는 데이터베이스와 관련된 명령어를 실행합니다.

Tip

SYSADM, DBADM 권한을 가진 사용자는 데이터베이스에 접속하여 SQL문으로 데이터를 액세스할 수 있습니다.

1 권한별로 실행 가능한 명령어는 다음과 같습니다.

Function	SYSADM	SYSCTRL	SYSMAINT	DBADM
MIGRATE DATABASE	YES			
UPDATE DBM CFG	YES			
GRANT/REVOKE DBADM	YES			
UPDATE db/node/dcs directories	YES	YES		
FORCE USERS OFF SYSTEM	YES	YES		
CREATE/DROP DATABASE	YES	YES		
CREATE/DROP/ALTER TABLE SPACE	YES	YES		
RESTORE TO NEW DATABASE	YES	YES		
UPDATE DB CFG	YES	YES	YES	
BACKUP DATABASE or TABLE SPACE	YES	YES	YES	
RESTORE TO EXISTING DATABASE	YES	YES	YES	
PERFORM ROLLFORWARD RECOVERY	YES	YES	YES	
START/STOP DATABASE INSTANCE	YES	YES	YES	
RESTORE TABLE SPACE	YES	YES	YES	
RUN TRACE	YES	YES	YES	
TAKE DBM or DB SNAPSHOTS	YES	YES	YES	
QUERY TABLE SPACE STATE	YES	YES	YES	YES
UPDATE LOG HISTORY FILES	YES	YES	YES	YES
QUIESCE TABLE SPACE	YES	YES	YES	YES
REORG TABLE	YES	YES	YES	YES
RUN RUNSTATS UTILITY	YES	YES	YES	YES
READ LOG FILES	YES			YES
CREATE/ACTIVATE/DROP EVENT MONITORS	YES			YES

Figure 1205A ··· 권한별로 사용 가능한 명령어

Tip

SYSADM,SYSCTRL,SYSMAINT 권한을 가진 사용자는 SYSMON 권한을 자동으로 소유합니다.

2 SYSMON 권한을 사용하여 사용자는 다음과 같은 명령어를 사용할 수 있습니다

- GET DATABASE MANAGER MONITOR SWITCHES
- GET MONITOR SWITCHES
- GET SNAPSHOT
- LIST ACTIVE DATABASES
- LIST APPLICATIONS
- LIST DCS APPLICATIONS
- RESET MONITOR
- UPDATE MONITOR SWITCHES

Figure 1205B ··· SYSMON 권한으로 가능한 명령어

Tip

SYSADM,DBADM 권한을 가진 사용자는 LOAD 권한을 자동으로 소유합니다.

3 LOAD 권한을 사용하여 사용자는 다음과 같은 명령어를 사용할 수 있습니다

- LOAD
- LIST TABLESPACES
- RUNSTATS
- QUIESCE TABLESPACES FOR TABLE

Figure 1205C ··· LOAD 권한으로 가능한 명령어

TOPIC 12 06 인스턴스 권한 제어 방법

Point

시스템 권한은 OS의 그룹에게 부여하므로, 해당 그룹에 속하는 사용자는 모두 동일한 인스턴스 권한을 가지게 됩니다. 인스턴스 구성 변수인 SYSADM_GROUP, SYSCTRL_GROUP, SYSMAINT_GROUP, SYSMON_GROUP으로 제어합니다.

Tip

SYSADM_GROUP 구성 변수에 값이 지정되지 않은 경우에는 인스턴스 사용자의 일차 그룹에 속하는 사용자들이 SYSADM 권한을 가지게 됩니다.

Tip

NULL 은 인스턴스 구성 변수와 데이터베이스 구성 변수의 값을 지정되지 않은 상태로 설정하는 특수한 키워드로 반드시 대문자로 표현합니다.

Tip

지정할 수 있는 그룹명의 최대 길이는 30 글자입니다. 그룹명의 최대 길이는 각 플랫폼에 따라 다를 수 있으며, AIX에서는 8글자까지 가능합니다.

1 SYSADM 권한을 가진 사용자로 로그인합니다.

```
$ login <인스턴스 사용자>
```

2 update dbm cfg 명령어를 이용하여 인스턴스 구성 변수인 SYSADM_GROUP, SYSCTRL_GROUP, SYSMAINT_GROUP, SYSMON_GROUP의 값을 OS에 정의된 <그룹명>으로 지정합니다. 지정한 그룹에 속한 사용자는 간접적으로 권한을 부여 받습니다.

```
$ db2 update dbm cfg using SYSCTRL_GROUP <그룹명>
```

3 update dbm cfg 명령어를 이용하여 인스턴스 구성 변수인 SYSADM_GROUP, SYSCTRL_GROUP, SYSMAINT_GROUP, SYSMON_GROUP의 값을 NULL로 지정하면 기본값으로 복귀하므로, 해당 그룹은 더 이상 인스턴스 권한을 가질 수 없습니다.

```
$ db2 update dbm cfg using SYSCTRL_GROUP NULL
```

4 각 구성 변수의 변경은 인스턴스를 재시작해야 반영됩니다.

```
$ db2stop force
$ db2start
```

5 get dbm cfg 명령어를 이용하여 인스턴스 권한과 관련된 구성 변수의 값을 확인합니다.

```
$ db2 get dbm cfg | grep "_GROUP"
 SYSADM 그룹 이름                (SYSADM_GROUP) = ADMGRP
 SYSCTRL 그룹 이름               (SYSCTRL_GROUP) = CTRLGRP
 SYSMAINT 그룹 이름              (SYSMAINT_GROUP) = MAINTGRP
 SYSMON 그룹 이름                (SYSMON_GROUP) = MOMGRP
```

TOPIC 12-07 데이터베이스 권한 제어 방법

Point

데이터베이스 권한은 OS에 정의된 그룹명 또는 사용자 계정에게 부여됩니다. 그룹에게 권한이 부여되면, 해당 그룹에 속하는 사용자 계정은 모두 동일한 데이터베이스 권한을 가지게 됩니다.

1. SYSADM 권한을 가진 사용자로 데이터베이스에 접속합니다.

```
$ login <인스턴스 사용자>
$ db2 connect to <데이터베이스명>
```

2. grant문으로 DBADM과 LOAD 권한을 사용자에게 부여합니다.

```
$ db2 GRANT DBADM ON DATABASE TO USER <사용자명>
$ db2 GRANT LOAD ON DATABASE TO USER <사용자명>
```

3. grant문으로 DBADM과 LOAD 권한을 그룹에 부여하면, 그룹에 속한 사용자는 간접적으로 권한을 부여 받습니다.

```
$ db2 GRANT DBADM ON DATABASE TO GROUP <그룹명>
$ db2 GRANT LOAD ON DATABASE TO GROUP <그룹명>
```

4. revoke 문으로 DBADM과 LOAD 권한을 제거할 수 있습니다.

```
$ db2 REVOKE DBADM ON DATABASE FROM USER <사용자명>
$ db2 REVOKE LOAD ON DATABASE FROM USER <사용자명>
$ db2 REVOKE DBADM ON DATABASE FROM GROUP <그룹명>
$ db2 REVOKE LOAD ON DATABASE FROM GROUP <그룹명>
```

5. DBADM과 LOAD 권한은 SYSCAT.DBAUTH 뷰를 통해 확인합니다.

```
$ db2 "select grantee, DBADM, LOAD from syscat.dbauth"
```

Tip

DBADM 권한을 부여하면 데이터베이스에 대한 특권인 BINDADD, CONNECT, CREATETAB, CREATE_NOT_FENCED, IMPLICIT_SCHEMA 등이 자동으로 부여됩니다.

Tip

LOAD 권한을 부여 받은 사용자는 실제로 LOAD 유틸리티를 실행할 때, 해당 테이블에 대한 INSERT 권한도 있어야 합니다.

Tip

DBADM 권한을 제거해도 간접적으로 부여받은 데이터베이스에 대한 특권은 자동으로 제거되지 않으므로, 필요시 revoke문으로 명시적으로 제거합니다.

TOPIC 1208 특권

Point

데이터베이스, 테이블스페이스, 스키마, 테이블, 뷰, 인덱스, 패키지, SP, UDF 등의 데이터베이스 오브젝트에 대한 구체적인 SQL 문을 실행할 수 있는 능력을 특권이라고 합니다. grant문과 revoke 문을 이용하여 그룹 또는 사용자별로 특권을 제어합니다.

Tip

오브젝트를 생성한 사용자를 '오브젝트의 소유자' 라고 합니다. 소유자는 DROP문으로 해당 오브젝트를 제거하거나, GRANT문과 REVOKE 문으로 해당 특권을 제어할 수 있는 할 수 있는 CONTROL 특권을 부여받습니다.

1 데이터베이스 오브젝트별 특권의 체계는 다음과 같이 분류됩니다.

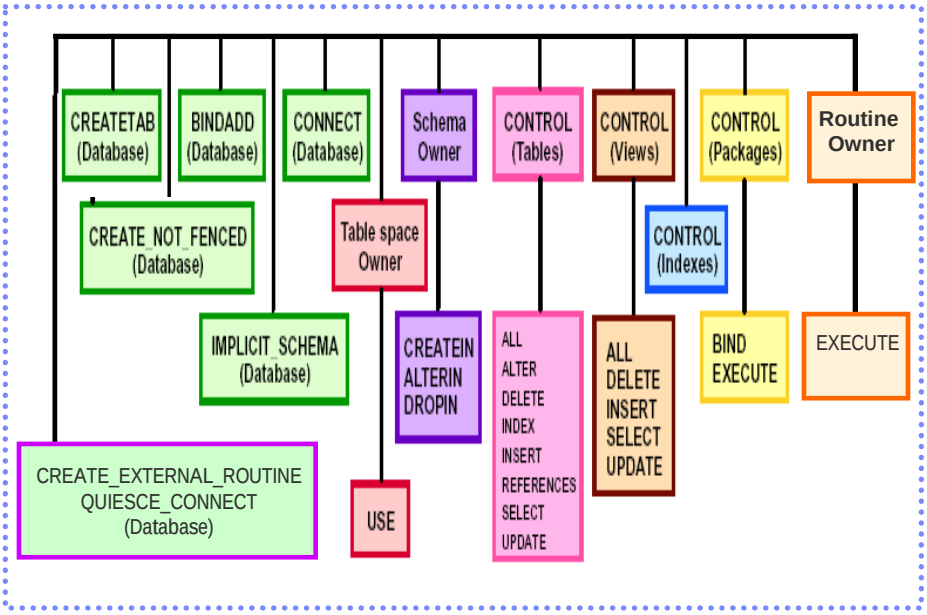

Figure 1208A ••• 데이터베이스 오브젝트별 특권

Tip

그룹에 부여된 특권은 정적 SQL 문을 실행할 때는 적용되지 않습니다. 응용프로그램에 포함된 정적 SQL문을 실행하는 사용자는 해당 SQL문에 대한 명시적인 특권을 가지고 있어야 합니다.

2 오브젝트별로 구체적인 특권명은 다음과 같으며, grant 문과 revoke문을 이용하여 사용자 또는 그룹 단위로 제어할 수 있습니다.

오브젝트	설명
데이터베이스	CONNECT, CREATETAB, IMPLICIT_SCHEMA, BINDADD, CREATE_NOT_FENCED, QUIESCE_CONNECT, CREATE_EXTERNAL_ROUTINE 특권이 있습니다.
테이블스페이스	USE 특권이 있습니다.
스키마	CREATEIN, ALTERIN, DROPIN 특권이 있습니다.
테이블	ALTER, INDEX, SELECT, INSERT, UPDATE, DELETE, REFERENCES 특권이 있습니다.
뷰	SELECT, INSERT, UPDATE, DELETE 특권이 있습니다.
인덱스	CONTROL 등이 있습니다.
패키지	BIND, EXECUTE 특권이 있습니다.
SP, UDF	EXECUTE 특권이 있습니다.
시퀀스	USAGE, ALTER 특권이 있습니다.

TOPIC 12 09 특권 제어 방법

Point

특권은 GRSANT 문과 REVOKE 문을 이용하여 사용자 또는 그룹별로 제어합니다. 특정 그룹에 특권을 부여하면, 해당 그룹에 속하는 사용자 계정은 동일한 특권을 간접적으로 부여받게 됩니다. PUBLIC은 모든 사용자를 의미하는 특별한 키워드입니다.

Tip

DBADM과 LOAD는 특권이 아닌 권한이지만, grant문과 revoke 문으로 제어합니다.

1 특권은 grant 문과 revoke 문으로 제어합니다.

* GRANT/ REVOKE	Database privileges	ON DATABASE	TO/ FROM	USER/ GROUP	userid groupid PUBLIC
	Package privileges	ON PACKAGE package_name			
	Table/view privileges	ON TABLE table/view_name			
	CONTROL	ON INDEX index_name			
	Schema privileges	ON SCHEMA schema_name			
	USE	OF TABLESPACE tablespacename			

* must be SYSADM, DBADM, or have CONTROL on object

Figure 1209A GRANT 문과 REVOKE 문

Tip

GROUP과 USER 키워드는 생략할 수 있지만, 동일한 그룹 ID와 사용자 계정이 존재하는 경우에는 SQLSTATE 56092 가 반환되므로, 명시하는 것이 좋습니다.

2 grant 문으로 OS에 정의된 그룹 또는 사용자에게 특권을 부여합니다.

```
$ db2 grant <특권명> on <오브젝트명> to group <그룹명>
$ db2 grant <특권명> on <오브젝트명> to user <사용자명>
```

Tip

OS 에 존재하지 않는 사용자명을 이용하여 특권을 부여할 수 있지만, 데이터베이스에 접속할 때는 OS에 정의된 사용자명을 이용하여 사용자 인증이 이루어지므로, 실제 운영시에는 의미가 없습니다.

3 한 가지 이상의 특권을 한 개의 grant 문으로 부여할 수 있습니다.

```
$ db2 grant <특권명1>, <특권명2> on <오브젝트명> to user <사용자명>
```

4 모든 사용자에게 권한을 부여하려면 PUBLIC이라는 키워드를 이용합니다.

```
$ db2 grant <특권명> on <오브젝트명> to public
```

Tip

WITH GRANT OPTION 옵션은 package, routine, schema, table, view, table space에만 적용됩니다.

5 WITH GRANT OPTION을 사용하면, 권한을 부여받은 사용자는 다른 사용자에게 부여받은 권한을 전달할 수 있습니다.

```
$ db2 grant <특권명> on <오브젝트명> to user <사용자명> with grant
    option
```

6 revoke 문으로 OS 그룹 또는 사용자에게 특권을 제거합니다.

```
$ db2 revoke <특권명> on <오브젝트명> from user <사용자명>
```

TOPIC 12.10 데이터베이스 특권

Point

CONNECT, CREATETAB, IMPLICIT_SCHEMA, BINDADD, CREATE_NOT_FENCED, QUIESCE_CONNECT, CREATE_EXTERNAL_ROUTINE 등의 특권을 SYSADM, DBADM 사용자가 GRANT 문과 REVOKE 문으로 제어합니다.

Tip

데이블스페이스에 대한 USE 특권과 데이터베이스에 대한 CREATETAB 특권이 모두 있어야 해당 테이블스페이스에 테이블을 생성할 수 있습니다.

Tip

IMPLICIT_SCHEMA 특권의 소유자가 자동으로 생성된 스키마의 소유자는 SYSIBM 이 되고, 스키마에 대한 사용 권한은 모든 사용자에게 부여됩니다.

Tip

DBADM과 BINDADD는 데이터베이스에 대한 특권으로 분류하지 않고, 권한이라고 합니다. 특권과 동일하게 GRANT, REVOKE 문으로 제어합니다.

Tip

WITH GRANT OPTION 은 지원되지 않습니다.

1 데이터베이스에 관한 특권은 다음과 같습니다.

특 권	설 명
CONNECT	접속할 수 있습니다.
BINDADD	새로운 패키지를 생성할 수 있습니다.
CREATETAB	새로운 테이블을 생성할 수 있습니다.
CREATE_NOT_FENCED	'NOT FENCED" 모드의 UDF 또는 SP를 생성할 수 있습니다.
IMPLICIT_SCHEMA	존재하지 않는 스키마명을 이용하여 데이터베이스 오브젝트를 생성하면, 스키마가 생성됩니다.
QUIESCE_CONNECT	데이터베이스가 QUIESCE 모드에 있는 경우에도 접속할 수 있습니다.
CREATE_EXTERNAL_ROUTINE	SQL 프로시저 이외의 외부 소스 프로시저를 생성할 수 있습니다.

2 <특권명>을 지정하여 그룹이나 사용자별로 제어합니다.

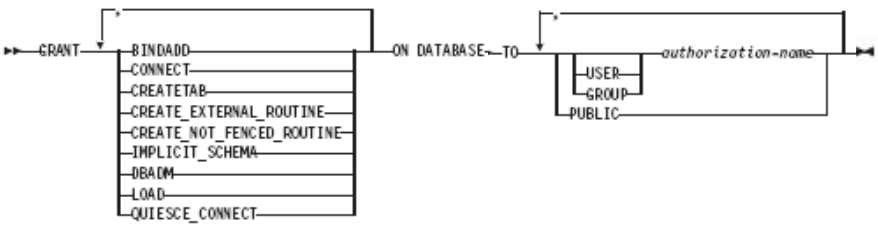

Figure 1210A ••• 데이터베이스 특권을 제어하는 GRANT 문

3 grant 문과 revoke 문으로 그룹 또는 사용자에게 부여합니다.

```
$ db2 grant CONNECT on database to GROUP <그룹명>
$ db2 grant CONNECT on database to USER <사용자명>
$ db2 grant CONNECT on database to PUBLIC
```

4 데이터베이스에 관한 특권은 카탈로그 뷰인 SYSCAT.DBAUTH 를 이용하여 확인합니다.

```
$ db2 "select * from SYSCAT.DBAUTH"
```

TOPIC 12-11 테이블스페이스 특권

Point

사용자는 USE 특권이 있어야 특정 테이블스페이스에 테이블을 생성할 수 있습니다. SYSADM, SYSCTRL 또는 DBADM 권한이 있는 사용자가 GRANT 문과 REVOKE 문으로 제어합니다.

Tip

SYSCATSPACE와 시스템 임시 테이블스페이스는 USE 권한을 부여할 수 없습니다.

Tip

데이터베이스를 생성하면 USERSPACE1에 대한 USE 권한은 모든 사용자에게 부여됩니다.

Tip

테이블스페이스에 대한 USE 특권과 데이터베이스에 대한 CREATETAB 특권이 모두 있어야 해당 테이블스페이스에 테이블을 생성할 수 있습니다.

1 테이블스페이스에 관한 특권은 다음과 같습니다.

특 권	설 명
USE	테이블스페이스에 새로운 테이블을 생성할 수 있습니다.

2 <특권명>과 <테이블스페이스명>을 지정하여 그룹이나 사용자별로 제어합니다.

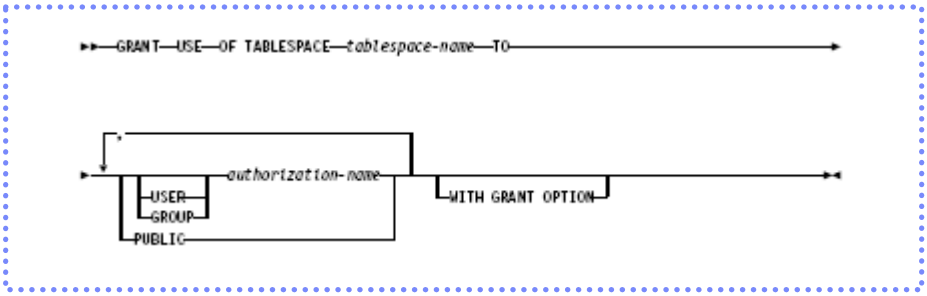

Figure 1211A • • • 테이블스페이스 특권을 제어하는 GRANT 문

3 grant 문과 revoke 문으로 그룹 또는 사용자에게 부여합니다.

```
$ db2 grant USE OF TABLESPACE <테이블스페이스명> to GROUP <그룹명>
$ db2 grant USE OF TABLESPACE <테이블스페이스명> to USER <사용자명>
$ db2 grant USE OF TABLESPACE <테이블스페이스명> to PUBLIC
$ db2 grant USE OF TABLESPACE <테이블스페이스명> to USER <사용자명>
    WITH GRANT OPTION
```

4 테이블스페이스에 관한 특권은 SYSCAT.TBSPACEAUTH 뷰를 이용하여 확인합니다.

```
$ db2 “select * from SYSCAT.TBSPACEAUTH ”
```

TOPIC 12-12 스키마 특권

Point

CREATEIN, ALTERIN, DROPIN 특권이 있습니다. SYSADM 또는 DBADM 권한이 있는 사용자가 데이터베이스에 접속한 후 GRANT 문과 REVOKE 문으로 제어합니다.

Tip

DROPIN 특권은 스키마를 제거할 수 있는 특권이 아닙니다. 스키마는 SYSADM,DBADM 또는 스키마를 생성한 소유자만 제거할 수 있습니다.

1 스키마에 관한 특권은 다음과 같습니다.

특 권	설 명
CREATEIN	특정한 스키마명을 이용하여 새로운 오브젝트를 생성합니다.
ALTERIN	특정한 스키마명을 가진 오브젝트를 변경할 수 있습니다.
DROPIN	특정한 스키마명을 가진 오브젝트를 제거합니다.

2 <특권명>과 <스키마명>을 지정하여 그룹이나 사용자별로 제어합니다.

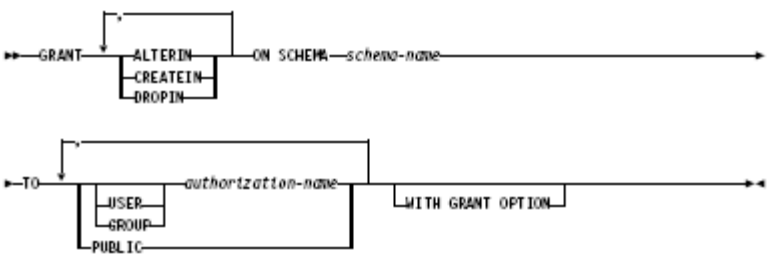

Figure 12-12A ••• 스키마 특권을 제어하는 GRANT 문

3 grant 문과 revoke 문으로 그룹 또는 사용자에게 부여합니다.

```
$ db2 grant ALTERIN on schema <스키마명> to GROUP <그룹명>
$ db2 grant DROPIN on schema <스키마명> to USER <사용자명>
$ db2 grant CREATEIN on schema <스키마명> to PUBLIC
$ db2 grant DROPIN on schema <스키마명> to USER <사용자명> WITH
    GRANT OPTION
```

4 스키마에 관한 특권은 SYSCAT.SCHEMAAUTH 뷰를 이용하여 확인합니다.

```
$ db2 “select * from SYSCAT.SCHEMAAUTH”
```

TOPIC 12 13 테이블 특권

Point

ALL, CONTROL, ALTER, INDEX, SELECT, INSERT, UPDATE, DELETE, REFERENCES 등이 있습니다. SYSADM 또는 DBADM 권한이 있는 사용자가 데이터베이스에 접속한 후 GRANT 문과 REVOKE 문으로 제어합니다.

Tip

REFERENCES 특권과 UPDATE 특권은 컬럼별 지정이 가능합니다.

1 테이블에 관한 특권은 다음과 같습니다.

특 권	설 명
CONTROL	테이블의 소유자는 테이블에 대한 모든 특권을 가집니다. CONTROL 특권을 제외한 모든 특권을 다른 사용자에게 부여할 수 있습니다. 테이블을 제거할 수 있습니다.
ALL	CONTROL 특권을 제외한 모든 특권을 가집니다.
ALTER	기존 테이블에 컬럼 추가,기본키와 고유키 추가, 컬럼 점검 조건을 추가 또는 제거할 수 있고, 트리거를 작성할 수 있습니다.
DELETE	테이블에서 행을 삭제합니다.
INDEX	테이블에 인덱스를 추가합니다.
INSERT	테이블에 행을 추가합니다.
REFERENCES	RI 관계를 정의할 때 parent table 로 사용될 수 있습니다.
SELECT	테이블에서 데이터를 조회할 수 있습니다. export 유틸리티에 사용되는 SELECT문을 요청할 수 있습니다.
UPDATE	테이블의 컬럼값을 변경할 수 있습니다. 특정 컬럼에 대한 UPDATE 특권을 부여할 수도 있습니다.

2 <특권명>과 <테이블명>을 지정하여 그룹이나 사용자별로 제어합니다.

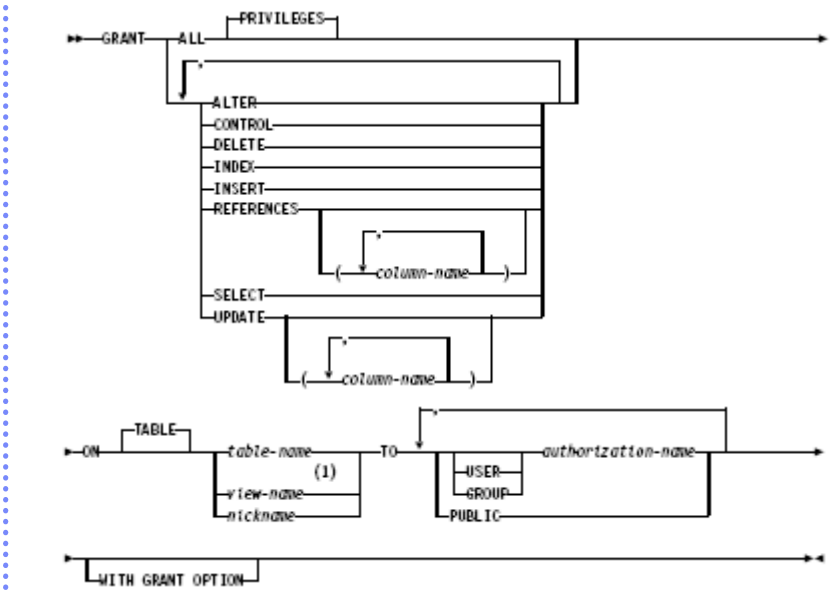

Figure 1213A ••• 테이블과 뷰 특권을 제어하는 GRANT 문

3 테이블에 관한 특권은 SYSCAT.TABAUTH 뷰를 이용하여 확인합니다.

```
$ db2 “select * from SYSCAT.TABAUTH”
```

TOPIC 12.14 뷰 특권

Point

뷰에 대한 특권으로는 ALL, CONTROL, SELECT, INSERT, UPDATE, DELETE 등이 있습니다. SYSADM 또는 DBADM 권한이 있는 사용자가 데이터베이스에 접속한 후 GRANT 문과 REVOKE 문으로 제어합니다.

Tip

뷰의 정의에 사용된 테이블에 대한 특권이 있으면, 뷰에 대한 특권도 자동으로 부여됩니다.

1 뷰에 관한 특권은 다음과 같습니다.

특 권	설 명
CONTROL	뷰의 소유자에게 자동으로 부여되는 특권으로 뷰에 대한 모든 특권을 가집니다. CONTROL 특권을 제외한 모든 특권을 다른 사용자에게 부여할 수 있습니다. 뷰를 제거할 수 있습니다.
ALL	CONTROL 특권을 제외한 모든 특권을 가집니다.
DELETE	뷰에서 행을 삭제합니다.
INSERT	뷰에 행을 추가합니다.
SELECT	뷰에서 데이터를 조회할 수 있습니다. export 유틸리티에 사용되는 SELECT문을 요청할 수 있습니다.
UPDATE	뷰의 컬럼값을 변경할 수 있습니다. 특정 컬럼에 대한 UPDATE 특권을 부여할 수도 있습니다.

2 테이블과 뷰는 동일한 방법으로 grant 문과 revoke 문으로 <특권명>과 <뷰명>을 지정하여 그룹이나 사용자별로 제어합니다.

```
$ db2 grant UPDATE on table <테이블명> to GROUP <그룹명>
$ db2 grant UPDATE (<컬럼명>) on table <테이블명> to USER <사용자명>
$ db2 grant UPDATE on table <테이블명> to USER <사용자명>
$ db2 grant UPDATE on table <테이블명> to USER <사용자명> WITH
    GRANT OPTION
$ db2 grant UPDATE on table <뷰명> to PUBLIC
```

3 뷰에 관한 특권은 SYSCAT.TABAUTH 뷰를 이용하여 확인합니다.

```
$ db2 “select * from SYSCAT.TABAUTH”
```

TOPIC 12.15 인덱스 특권

Point

CONTROL 특권이 있는 사용자는 DROP INDEX 문을 이용하여 해당 인덱스를 제거할 수 있습니다. SYSADM 또는 DBADM 권한이 있는 사용자가 데이터베이스에 접속한 후 GRANT 문과 REVOKE 문으로 제어합니다.

Tip

인덱스에 대한 사용 특권은 필요하지 않습니다. 테이블에 대한 SELECT특권이 있는 경우에는 인덱스도 사용될 수 있습니다.

1 인덱스에 관한 특권은 다음과 같습니다.

특 권	설 명
CONTROL	인덱스의 소유자에게 자동으로 부여되는 특권으로 인덱스를 제거할 수 있습니다.

2 <특권명>과 <인덱스명>을 지정하여 그룹이나 사용자별로 제어합니다.

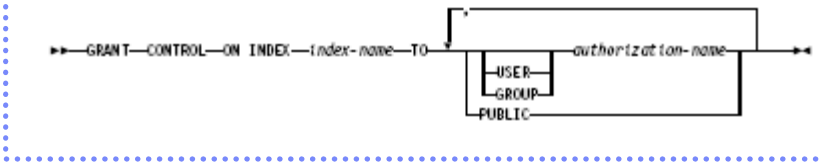

Figure 1215A 인덱스 특권을 제어하는 GRANT 문

Tip

WITH GRANT OPTION 은 지원되지 않습니다.

3 grant 문과 revoke 문으로 그룹이나 사용자별로 제어합니다.

```
$ db2 grant CONTROL on index <인덱스명> to GROUP <그룹명>
$ db2 grant CONTROL on index <인덱스명> to USER <사용자명>
$ db2 grant CONTROL on index <인덱스명> to PUBLIC
```

4 인덱스에 관한 특권은 SYSCAT.INDEXAUTH 뷰를 이용하여 확인합니다.

```
$ db2 “select * from SYSCAT.INDEXAUTH”
```

TOPIC 12.16 패키지 특권

Point

CONTROL, BIND, EXECUTE 특권이 있습니다. SYSADM 또는 DBADM 권한이 있는 사용자가 데이터베이스에 접속한 후 GRANT 문과 REVOKE 문으로 제어합니다.

Tip

패키지는 SQL문에 대한 액세스 플랜을 가지고 있는 데이터베이스 오브젝트로, 시스템 카탈로그에 저장됩니다.

Tip

패키지에 대한 EXECUTE 특권을 부여받으면, 패키지를 실행하는 동안에는 패키지에 포함된 정적 SQL문에 대한 특권을 임시로 가지게 되므로, 해당 SQL문에 대한 명시적인 특권이 없는 사용자도 패키지를 실행할 수 있습니다.

1 패키지에 관한 특권은 다음과 같습니다.

특 권	설 명
CONTROL	패키지의 소유자에게 자동으로 부여되는 특권으로 패키지에 대한 모든 특권을 가집니다. 패키지에 대한 drop, rebind, execute 특권을 가지며, CONTROL 특권을 제외한 모든 특권을 다른 사용자에게 부여할 수 있습니다.
BIND	기존의 패키지를 리바인드할 수 있습니다.
EXECUTE	패키지를 실행할 수 있습니다.

2 <특권명>과 <패키지명>을 지정하여 그룹이나 사용자별로 제어합니다.

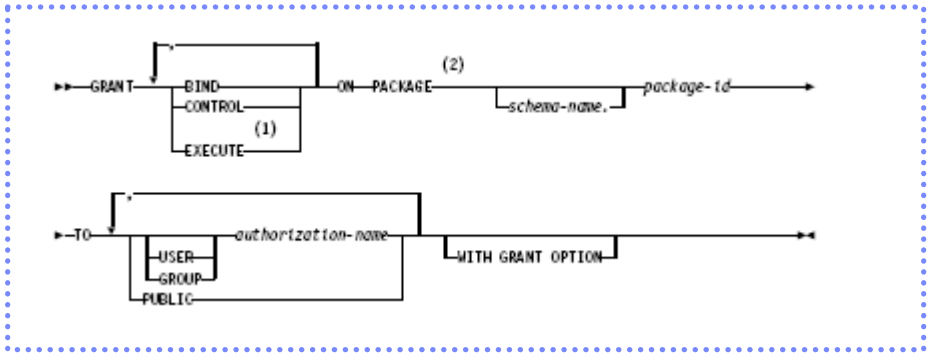

Figure 12.16A ••• 패키지 특권을 제어하는 GRANT 문

2 grant 문과 revoke 문으로 그룹이나 사용자별로 제어합니다.

```
$ db2 grant EXECUTE on package <패키지명> to GROUP <그룹명>
$ db2 grant EXECUTE on package <패키지명> to USER <사용자명>
$ db2 grant EXECUTE on package <패키지명> to PUBLIC
$ db2 grant EXECUTE on package <패키지명> to USER <사용자명> WITH
    GRANT OPTION
```

3 패키지에 관한 특권은 SYSCAT.PACKAGEAUTH 뷰를 이용하여 확인합니다.

```
$ db2 “select * from SYSCAT.PACKAGEAUTH”
```

TOPIC 12.17 루틴 특권

Point

SP(저장 프로시저) 또는 UDF(사용자 정의 함수) 등의 루틴에 대한 특권으로는 EXECUTE 가 있습니다. SYSADM 또는 DBADM 권한이 있는 사용자가 데이터베이스에 접속한 후 GRANT 문과 REVOKE 문으로 제어합니다.

1 UDF 또는 SP 에 관한 특권은 다음과 같습니다.

특 권	설 명
EXECUTE	CALL 문을 이용하여 저장프로시저를 호출하거나, SQL문에서 UDF를 참조할 수 있습니다.

Tip

오버로딩된 UDF 또는 SP인 경우에는 SYSCAT.ROUTINES 뷰에서 고유한 이름인 SPECIFIC 명을 확인하여 사용합니다.

2 <UDF명> 또는 <SP명> 을 지정하여 그룹이나 사용자별로 제어합니다.

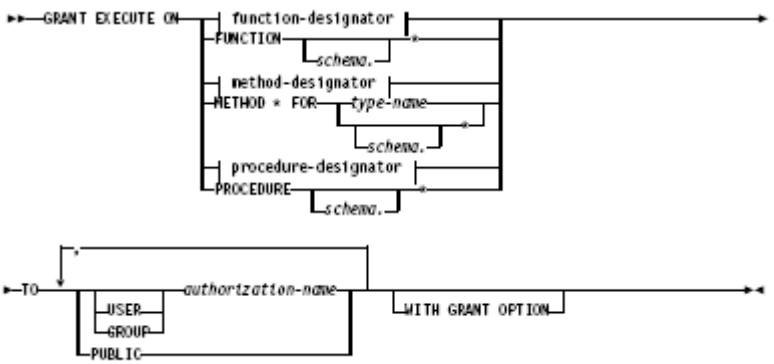

Figure 1217A ••• 루틴 특권을 제어하는 GRANT 문

Tip

<스키마명>.* (asterisk)는 지정한 <스키마명>을 가지는 모든 UDF 또는 SP를 지정하는 특수한 옵션입니다.

3 grant 문과 revoke 문으로 그룹이나 사용자별로 제어합니다.

```
$ db2 grant EXECUTE on FUNCTION <UDF명> to GROUP <그룹명>
$ db2 grant EXECUTE on FUNCTION <UDF명> to USER <사용자명>
$ db2 grant EXECUTE on FUNCTION <UDF명> to PUBLIC
$ db2 grant EXECUTE on FUNCTION <스키마명>.*  to USER <사용자명>
$ db2 grant EXECUTE on FUNCTION <UDF명> to USER <사용자명> WITH
    GRANT OPTION
$ db2 grant EXECUTE on SPECIFIC FUNCTION <UDF에 대한 SPECIFIC명>
    to USER <사용자명>
$ db2 grant EXECUTE on PROCEDURE <SP명> to GROUP <그룹명>
$ db2 grant EXECUTE on PROCEDURE <SP명> to USER <사용자명>
$ db2 grant EXECUTE on PROCEDURE <SP명> to PUBLIC
$ db2 grant EXECUTE on PROCEDURE <스키마명>.* to USER <사용자명>
$ db2 grant EXECUTE on PROCEDURE <SP명> to USER <사용자명> WITH
    GRANT OPTION
$ db2 grant EXECUTE on SPECIFIC PROCEDURE <SP에 대한 SPECIFIC명>
    to USER <사용자명>
```

4 루틴에 관한 특권은 SYSCAT.ROUTINEAUTH 뷰를 이용하여 확인합니다.

```
$ db2 “select * from SYSCAT.ROUTINEAUTH”
```

TOPIC 12 18 시퀀스 특권

Point

ALTER, USAGE 등이 있습니다. SYSADM 또는 DBADM 권한이 있는 사용자 또는 소유자가 데이터베이스에 접속한 후 GRANT 문과 REVOKE 문으로 제어합니다.

1 시퀀스에 관한 특권은 다음과 같습니다.

특 권	설 명
USAGE	시퀀스에 대한 NEXTVAL과 PREVVAL 표현식을 사용할 수 있습니다.
ALTER	ALTER SEQUENCE 문을 이용하여 시퀀스의 정의를 변경할 수 있습니다.

2 <특권명>과 <시퀀스명> 을 지정하여 그룹이나 사용자별로 제어합니다.

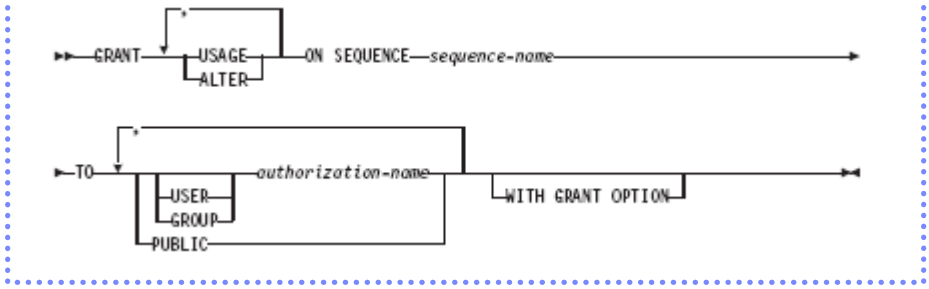

Figure 1218A ••• 시퀀스 특권을 제어하는 GRANT 문

2 grant 문과 revoke 문으로 그룹이나 사용자별로 제어합니다.

```
$ db2 grant USAGE on sequence <시퀀스명> to GROUP <그룹명>
$ db2 grant USAGE on sequence <시퀀스명> to USER <사용자명>
$ db2 grant USAGE on sequence <시퀀스명> to PUBLIC
$ db2 grant USAGE on sequence <시퀀스명> to USER <사용자명> WITH
    GRANT OPTION
```

3 시퀀스에 관한 특권은 SYSCAT.SEQUENCEAUTH 뷰를 이용하여 확인합니다.

```
$ db2 “select * from SYSCAT.SEQUENCEAUTH”
```

TOPIC 12-19 간접 권한과 특권

Point

사용자 또는 그룹이 GRANT 문을 통하지 않고 부여 받은 권한과 특권입니다. 정적 SQL문을 제외한 모든 환경에서 직접 부여 받은 경우와 동일하게 사용할 수 있습니다.

Tip

간접적으로 부여받은 권한과 특권은 revoke 명령어를 이용하여 명시적으로 제거할 때까지 유지됩니다.

Tip

실제 운영 환경에서는 revoke 문을 이용하여 기본적으로 부여된 모든 간접 특권을 제거하고, grant 문을 이용하여 필요한 특권을 다시 제어하도록 합니다.

Tip

명시적인 특권이 없으므로 동일한 SQL문을 패키지의 외부에서 직접 실행할 수는 없습니다.

1 데이터베이스를 생성한 사용자는 해당 데이터베이스에 대한 DBADM 권한을 가지게 됩니다.

```
$ db2 create db <데이터베이스명>
$ db2 “select * from syscat.abauth”
```

2 데이터베이스를 생성하면 간접적으로 다음의 특권이 PUBLIC에게 부여됩니다.

대 상	특 권
데이터베이스	CONNECT, CREATETAB, BINDADD, IMPLICIT_SCHEMA 특권
USERSPACE1 테이블스페이스	USE 특권
시스템 카탈로그 테이블	SELECT 특권
기본 패키지	BIND, EXECUTE 특권
SYSFUN 스키마를 가진 함수	EXECUTE WITH GRANT 특권

3 DBADM 권한을 부여받은 그룹 또는 사용자는 간접적으로 데이터베이스에 대한 모든 특권을 부여받습니다.

```
$ db2 connect to <데이터베이스명>
$ db2 grant DBADM on database to user <사용자명>
$ db2 “select * from syscat.abauth"| grep –i <사용자명>
```

4 테이블, 인덱스, 패키지 등의 데이터베이스 오브젝트를 생성한 사용자는 오브젝트의 소유자로서 CONTROL 특권을 가지게 됩니다.

```
$ db2 connect to <데이터베이스명>
$ db2 "create table <테이블명> (<컬럼명> <데이터유형명>)"
$ db2 “select * from syscat.tabauth” | grep –i <사용자명>
```

5 패키지에 대한 EXECUTE 특권을 부여받으면, 패키지를 실행하는 동안에는 패키지에 포함된 정적 SQL문에 대한 특권을 임시로 가지게 되므로, 해당 SQL문에 대한 명시적인 특권이 없는 사용자도 패키지를 실행할 때는 해당 SQL문을 실행할 수 있습니다.

```
$ db2 connect to <데이터베이스명>
$ db2 grant execute on package <패키지명> to user <사용자명>
$ db2 “select * from syscat.packageauth” | grep –i <사용자명>
```