

7.4 権限定義

SQL 言語では、安全保護機能として、表ごとにほかの利用者のアクセスを許すかどうかを制御するための権限機能を提供しています。ここでも、表は、実表だけでなく、ビュー表も含みます。

実表の所有者は、自分の所有する実表にアクセスする権限だけでなく、それらの権限をほかの利用者に付与する権限もち、その表に対する各アクセス権限をほかの利用者に付与することができます。**権限の種類**を次に示します。

▼表 7-6 権限の種類とその意味

権限	意味
SELECT	表 (の列) を検索するための権限
INSERT	表に行 (または列の値) を挿入するための権限
UPDATE	表中の行 (または行の列の値) を更新するための権限
DELETE	表から行を削除するための権限
REFERENCES	外部キーなど制約のために列を参照するための権限

ビュー表の所有者は、自分の所有するビュー表に対する SELECT 権限をもちます。ビュー表が更新可能で、かつビュー定義中で指定した問合せ式中で参照する表、つまり、ビュー表のもととなる表に対する INSERT 権限、UPDATE 権限または DELETE 権限をもつならば、ビュー表に対する INSERT 権限、UPDATE 権限または DELETE 権限をもちます。さらに、そのビュー表のもととなる表に対してもつそれらの権限が付与可能な権限ならば、そのビュー表に対する権限をほかの利用者に付与することができます。

SQL での権限定義の形式は、次のとおりです。

```
GRANT 権限 ON [ TABLE ] 表名
TO 権限受領者 [ , 権限受領者 ]
[ WITH GRANT OPTION ]
```

表名には、権限を付与する対象の表の名前を指定します。

権限の形式は、次のとおりです。

```
ALL PRIVILEGES | 操作 [ , 操作 ] ...
```

ALL PRIVILEGES は、付与可能なすべての権限を意味します。

操作の形式は、次のとおりです。

```
SELECT [ ( 列名 [ , 列名 ] ... ) ]
| INSERT [ ( 列名 [ , 列名 ] ... ) ]
| UPDATE [ ( 列名 [ , 列名 ] ... ) ]
| DELETE
| REFERENCES [ ( 列名 [ , 列名 ] ... ) ]
```

各表に対する操作ごとに、権限を付与することができます。

権限受領者の形式は、次のとおりです。

```
PUBLIC | 認可識別子
```

PUBLIC は、そのデータベースにアクセスできるすべての利用者を意味します。認可識別子は、特定の利用者だけに付与する場合に、付与する各利用者の認可識別子を指定します。

WITH GRANT OPTION は、権限を付与するときに、付与する権限をほかの利用者に付与することも許す場合に指定します。つまり、WITH GRANT OPTION 指定で付与された権限は、付与可能な権限となり、さらに、その他の利用者に付与することができます。

【例 5】

表 7-2 (p.279) の学生表を、認可識別子 user1 の利用者が定義したと仮定します。さらに、SQL を実行する利用者の認可識別子と同じ名前がスキーマ名として暗に想定されるものとします。この場合、ほかの利用者がこの表を参照するためには、スキーマ名 user1 で修飾して、user1.学生という表名で参照します。なお、表を定義した利用者が参照するときには、スキーマ名を省略することが可能で、今までの例では、スキーマ名を省略していました。

学生表を定義した user1 が、その表に対する SELECT 権限を認可識別子 user2 の利用者に付与する SQL の例を示します。

```
GRANT SELECT ON 学生 TO user2
```

このように、SELECT 権限を付与された user2 は、次のとおり、学生表を検索することができます。

```
SELECT * FROM user1.学生
```

しかし、SELECT 権限を付与されていない user3 は、上記のように学生表を検索しようとすると、アクセス規則違反になります。

また、user2 が学生表に行を挿入しようとして、次の SQL を実行する場合を考えます。

```
INSERT INTO user1.学生 VALUES ( 'S06005', '大田垂矢' )
```

user2 は、SELECT 権限しか付与されておらず、INSERT 権限をもたないので、アクセス規則違反になります。

なお、次のように WITH GRANT OPTION を指定して、user1 が user4 に学生表の SELECT 権限を付与する場合を考えます。

```
GRANT SELECT ON 学生 TO user4 WITH GRANT OPTION
```