第3章

ユーザーと権限の管理

ここでは、SQL Serverのユーザー管理（ユーザー認証と権限）について記述します。

ユーザー認証

Oracleのユーザー認証では、データベース、オペレーティングシステム、ネットワークのいずれかを選択できますが、推奨はデータベースです。

SQL Serverでは、以下の2種類の認証方法があります。

1. **Windows 認証**
   ユーザーは、Windows NTまたはWindows 2000ユーザーアカウントでログオンします。この時点で認証は終了しており、それ以降はSQL Serverがそのアカウントを信頼し、SQL Serverに接続を許可します。
2. **SQL Server 認証**
   ユーザーはSQL Serverにログインし、SQL Serverが認証を行い、接続を許可します。

認証方法で重要なのは、ユーザー名とパスワードの管理です。この管理をWindows NTあるいはWindows 2000で行うかSQL Serverで行うかを決める必要があります。Oracleでのデータベースによる認証では、プロファイルを使ってパスワードを管理していますが、SQL ServerのWindows認証では、Windows NTあるいはWindows 2000の強固なセキュリティとユーザー管理情報を使えます。さらに、ログオンは1回で終了するのでSQL Serverへの接続が簡単なため、通常はWindows認証を使用したほうがよいでしょう。SQL Server認証は旧バージョンの互換性を保ちたい場合か、Windows NTあるいはWindows 2000にログオンできないユーザーのために使用します。

図3-1は、2つの認証方法の違いを示しています。

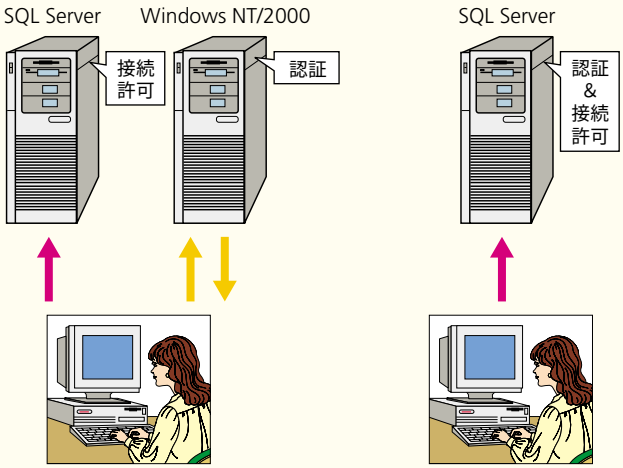

図 3-1
ユーザー認証

SQL Server のインスタンスレベルの認証の設定では、以下の 2 つのいずれかを選択します。

1. 混合モード

Windows 認証、SQL Server 認証のどちらも可能です。

2. Windows 認証モード

Windows 認証のみ可能です。SQL Server 認証はすべて拒否されます。

図 3-2 は、SQL Server Enterprise Manager で認証方法として混合モードを設定しているの画面です。

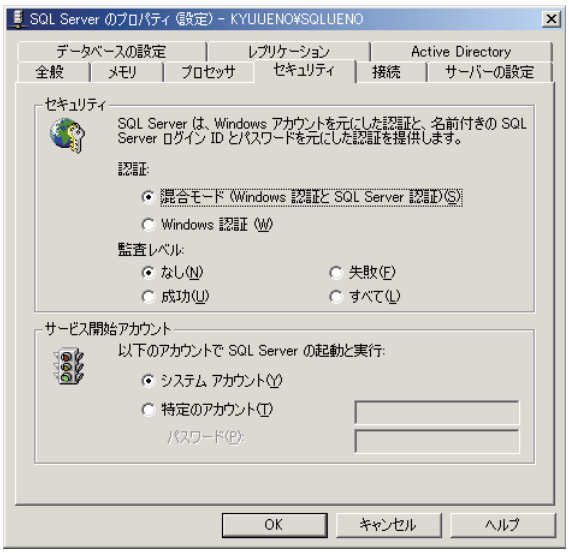

図 3-2
認証の設定
(SQL Server Enterprise Manager)

混合モードに設定した場合は、どちらの認証を使うかはクライアントが接続する際に選択します。図3-3は、クエリアナライザのログイン画面です。認証方法が選択できることがわかります。

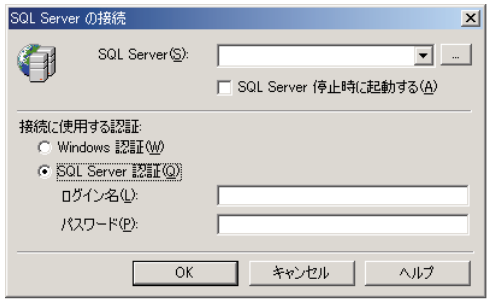

図3-3
クエリアナライザの
ログイン画面

ログインとデータベースユーザー

Oracleでは、インスタンスとデータベースが一対一で対応するため、インスタンスごとにユーザーの設定は1つだけです。

SQL Serverで、データベースオブジェクトを操作するためには、以下の2つのユーザー設定を行う必要があります（図3-4）。

1. **ログイン**
   SQL Serverインスタンスに接続するために必要なユーザー設定です。
2. **データベースユーザー**
   データベースのオブジェクトを操作するための権限を設定するためのユーザーで、データベースごとに設定します。ログインに関連付けられています。

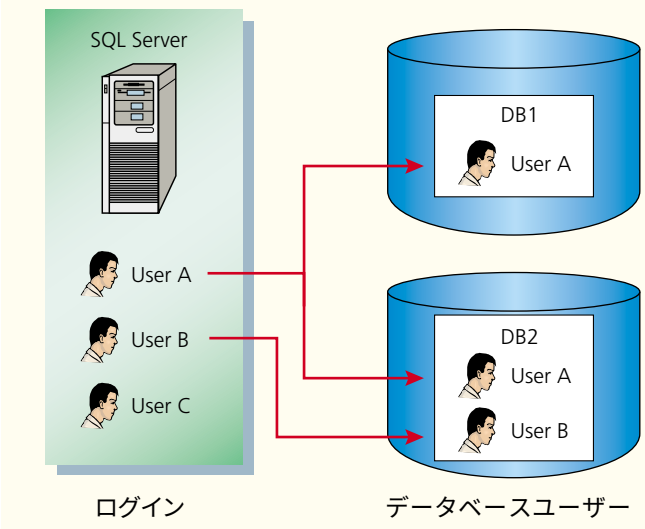

図3-4
ログインとデータベースユーザー

ログインには以下の3種類があります（図3-5）。

1. **SQL Serverログイン**
   SQL Server認証で使用されます。そのため、SQL Serverに各ユーザー名とパスワードの設定を行います。
2. **Windowsユーザーログイン**
   Windowsユーザー認証で使用されます。Windows NTあるいはWindows 2000のユーザーアカウントと関連付けられます。
3. **Windowsグループログイン**
   Windowsユーザー認証で使用されます。Windows NTあるいはWindows 2000のユーザーアカウントが所属するWindowsグループアカウントと関連付けられます。

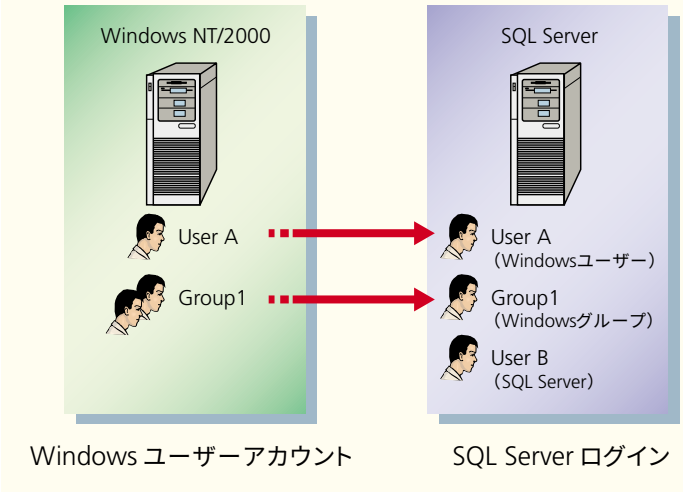

図3-5
ログイン

インストール時に作成される管理用のログインは、以下の2つです。

1. **sa**
   SQL Server認証用の管理者用アカウントで、システムデータベースの所有者です。インストール時に混合モードを選択すると、パスワードを設定できます。Windows認証を設定した場合はログインできません。
2. **BUILTIN\Administrators**
   Windows認証用の管理者アカウントで、Windowsのローカルシステム管理者グループに関連付けられています。

Oracleでユーザーを作成するときは、プロファイルやデフォルト表領域や一時表領域の割り当てなどを行います。

SQL Serverではカレント（既定の）データベースの指定を行います。カレントデータベースとは、ユーザーがログインしたときに最初に接続されるデ

ータベースのことです。ユーザーが接続後に同一インスタンスにあるデータベースをカレントデータベースに変更する場合はUSEコマンドで変更できます。このUSEコマンドは、カレントディレクトリを変更するオペレーティングシステムのCDコマンドと同等に考えると理解しやすくなります。図3-6は、domxドメインのtestuserユーザーアカウントのWindowsユーザーログインを作成する画面です。カレントデータベースはNorthwindです。

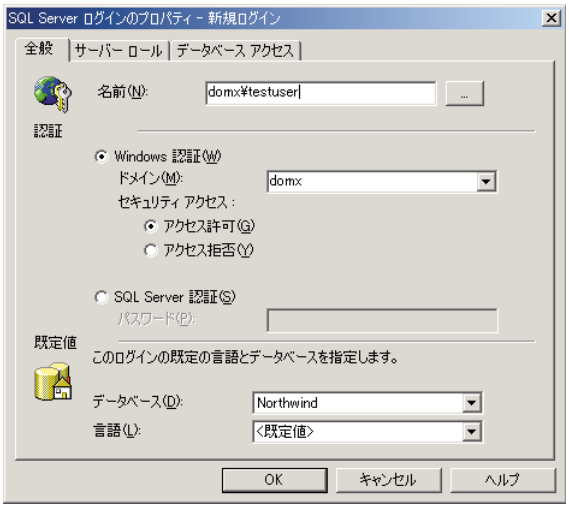

図3-6
ログインの作成
(SQL Server Enterprise Manager)

ログインにカレントデータベースを設定しても接続できるとは限りません。そのデータベースにデータベースユーザーを作成しておく必要があります。データベースユーザーは、そのユーザーが必要とするデータベースごとに作成する必要があります。データベースユーザーは、ログインとの関連付けをするだけで作成できます。

SQL Server Enterprise Managerを使うと、ログイン作成時に同時にデータベースユーザーを作成することも可能です。図3-7では、tesutuserログインをデータベースユーザーとして登録しています。

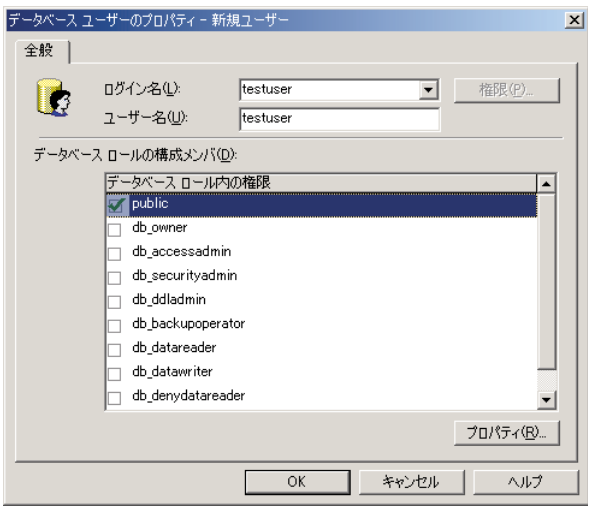

図3-7
データベースユーザーの作成
(SQL Server Enterprise Manager)

データベースを作成すると自動的にdboというデータベースユーザーが作成され、データベースを作成したログインが自動的に関連付けられます。

権限の管理

SQL Serverでは、データベースユーザーに権限を与えることによってデータベースのセキュリティを管理します。権限には、GRANT（許可）、REVOKE（取り消し）、DENY（拒否）の3種類があります。

Oracleの権限の管理は、GRANT（許可）、REVOKE（取り消し）の2種類のコマンドで管理することからわかるように、ユーザーに権限があるかどうかで管理されます。

たとえば、図3-8のように3人のユーザー（USER1、USER2、USER3）と1つのロール（ROLE1）および3つのテーブル（TABLE1、TABLE2、TABLE3）が存在しており、図のように権限が割り当てられている場合、USER1だけTABLE1の権限を割り当てないようにするにはそれぞれ以下の方法で行います。

- Oracleの場合は、USER1からROLE1の権限を取り消し（REVOKE）、USER1をTABLE2、TEBLE3にそれぞれ権限を許可（GRANT）します。あるいは、別のロールを作成し、そのロールにTABLE2とTABLE3の権限を許可し、USER1にそのロールを許可します。
- SQL Serverの場合は、USER1をTABLE1に対して拒否（DENY）します。

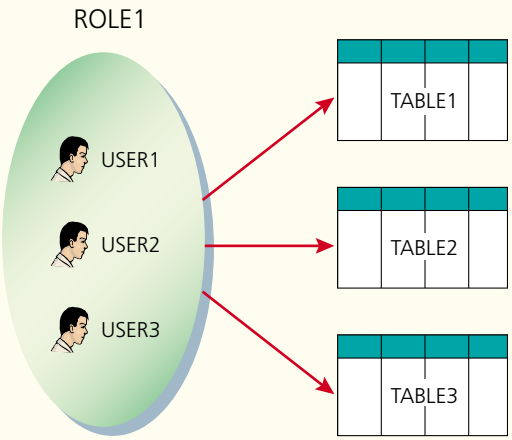

図3-8
権限の例

SQL Serverでは、以下の2つの条件が満たされたときに操作が実行可能となります。

1. ユーザーあるいはそのユーザーの所属するロールに対して1つでも権限が許可（GRANT）されている。

2. ユーザーあるいはそのユーザーの所属するロールに対して1つも拒否（DENY）されていない。

ステートメント権限

Oracleの権限の種類は、システム権限とオブジェクト権限の2種類です。システム権限は管理するためのものであり、オブジェクト権限はオブジェクトのアクセス権をユーザーに割り振るためのものです。

SQL Serverでは、管理用の権限をステートメント権限と呼び、オブジェクト権限はOracleと同様にオブジェクト権限と呼びます。

SQL Serverのステートメント権限は100以上存在します。管理を容易にするため、ユーザーに与えられるステートメント権限は下記の9種類だけです。これらはデータベース単位にそれぞれのデータベースユーザーに割り当てることができます。その他の権限は、管理用に作成されているサーバーロールを使用してまとめてユーザーに割り当てを行います。

- **割り当てを行うことができるステートメント権限**

  CREATE DATABASE（masterデータベースのみに存在）
  CREATE DEFAULT
  CREATE FUNCTION
  CREATE PROCEDURE
  CREATE RULE
  CREATE TABLE
  CREATE VIEW
  BACKUP DATABASE
  BACKUP LOG

図3-9は、masterデータベースのステートメント権限を割り当てている画面です。権限を与えたいデータベースユーザーの行の与えたいステートメント権限のチェックボックスをクリックすると許可（GRANT）したことになります。

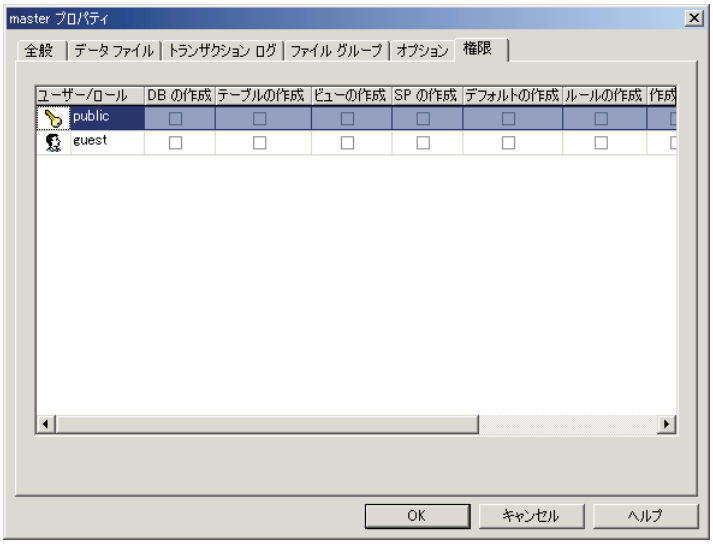

図 3-9
ステートメント権限
（masterデータベースのプロパティ）

次の表は、ステートメント権限がすでに割り当ててある固定サーバーロールの一覧です。管理権限を与えるには、固定サーバーロールをログインに割り当てます。

表：固定サーバーロール

固定サーバーロール	説明
sysadmin	SQL Server上のすべての権限を持っています。Oracleの SYSDBA権限と同様です。
serveradmin	サーバーレベルの設定を実行します。
setupadmin	リンクサーバーの追加および削除を行い、sp_serveroptionなどの一部のシステムストアドプロシージャを実行します。
securityadmin	サーバーのログインを管理します。
processadmin	SQL Serverのインスタンスで実行中のプロセスを管理します。
dbcreator	データベースの作成および変更を行います。
diskadmin	ディスクファイルを管理します。
bulkadmin	BULK INSERTステートメントを実行します。

オブジェクト権限

SQL Serverのオブジェクト権限には、SELECT、INSERT、UPDATE、DELETE、REFERENCES、EXECUTEの6種類があります。これらの権限は、テーブル、列、ビュー、ストアドプロシージャ、関数に割り当てることができます。割り当て可能な組み合わせを、以下の表に示します。

	S	I	U	D	R	E
テーブル	○	○	○	○	○	
列	○		○		○	
ビュー	○	○	○	○	○	
ストアドプロシージャ						○
関数						○

表：オブジェクト権限

※ S＝SELECT　I＝INSERT　U＝UPDATE　D＝DELETE　R＝REFERENCES
E＝EXECUTE

権限を割り当てる場合、列単位で権限を管理することはできますが、パフォーマンスおよび管理コストの観点から、列単位にビューやストアドプロシージャを作成し、権限を管理するようにしてください。

OracleでSYSDBA権限やスキーマ所有者に暗黙的に権限が割り当てられているように、SQL Serverでもsystemadminロール、dboおよびオブジェクト所有者は暗黙的にそれぞれの権限を割り振られています。

ロール

Oracleのロールは権限の集まりです。SQL Serverのロールも同じように考えることができますが、権限の集まりというよりもユーザーをグループ化するものと考えると理解しやすくなります。

たとえば、Oracleで“GRANT A TO B”というSQLステートメントを実行すると、AにもBにもロールを設定することができます。つまり、ロールは権限の集まりなので、権限を許可することも許可されることもできます。SQL ServerではBにしかロールを設定できません。つまり、SQL Serverのロールはユーザーをグループ化したものなので、ロールを許可するという考え方はないのです。

SQL Serverでユーザーあるいはロールにロールを割り当てる場合には、sp_addrolememberストアドプロシージャを使用します。このストアドプロシージャの名前を見てもわかるように、SQL Serverのロールはグループと考えることができます。

ロールの種類

SQL Serverには以下の4種類のロールがあります。

1. **固定サーバーロール**

   この章の「ステートメント権限」を参照してください。

2. **固定データベースロール**

   データベース単位に、管理および操作権限が許可されているロールです。

固定データベースロール	説明
db_owner	データベースでのすべての作業が行えます。
db_accessadmin	データベースユーザーの管理が行えます。
db_datareader	データベース内のすべてのユーザーテーブルのデータを表示できます。
db_datawriter	データベース内のすべてのユーザーテーブルでデータの追加、変更、削除を行えます。
db_ddladmin	データベース内のオブジェクトの追加、変更、削除を行えます。
db_securityadmin	ロールおよびメンバを管理し、データベース内のステートメント権限およびオブジェクト権限を管理できます。
db_backupoperator	データベースをバックアップする権限があります。
db_denydatareader	データベース内のすべてのデータを表示できません。
db_denydatawriter	データベース内のすべてのデータを変更できません。
public	すべてのデータベースユーザーが所属します。

表：固定データベースロール

3. **ユーザー定義データベースロール**

   ユーザーが作成可能なデータベースロールです。SQL ServerのWindows認証でWindowsのグループアカウントを登録した場合は、特に作成する必要はありません。

4. **アプリケーションロール**

   Oracleのロールはパスワードを設定できます。SQL Serverのロールにパスワードを設定する場合はアプリケーションロールを作成します。アプリケーションロールに設定されたパスワードを入力できるアプリケーションあるいはユーザーだけが所属できるロールです。パスワードを設定するには、sp_setapproleシステムストアドプロシージャを使用します。

図3-10は、ユーザー定義データベースロール（標準ロール）あるいはアプリケーションロールを作成する画面です。アプリケーションロールには、パスワードを設定できます。

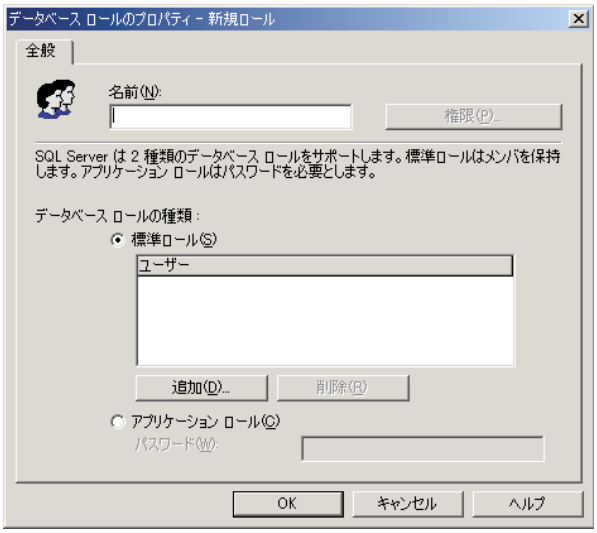

図3-10
ロールの作成画面
(SQL Server Enterprise Manager)

権限の継承

Oracleでは、ユーザーにビューの参照権限やストアドプロシージャの実行権限を与えた場合、ビューのデータを検索（SELECT）するユーザーやストアドプロシージャを実行するユーザーに対しては、ビューやストアドプロシージャを通じて参照するオブジェクトの権限の確認は行われません。これは、SQL Serverでも同様です。

しかし、注意しなければならないことがあります。それは、権限の継承という仕組みです。たとえば、あるビューとそのビューが参照するテーブルが同一の所有者である場合は権限が継承されます（図3-11左）。このとき、テーブルの権限は確認されません。しかし、別の所有者である場合は権限の継承が壊れた状態になり、ビューおよびテーブルの権限が確認されます（図3-11右）。権限の管理を容易にするには、データベース内のオブジェクトはすべてdboユーザーが所有するようにしてください。

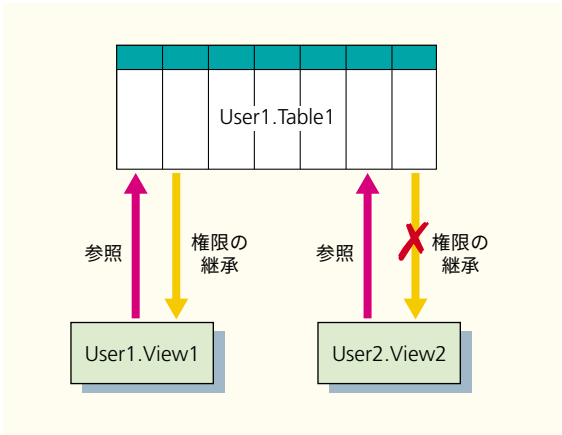

図3-11
権限の継承