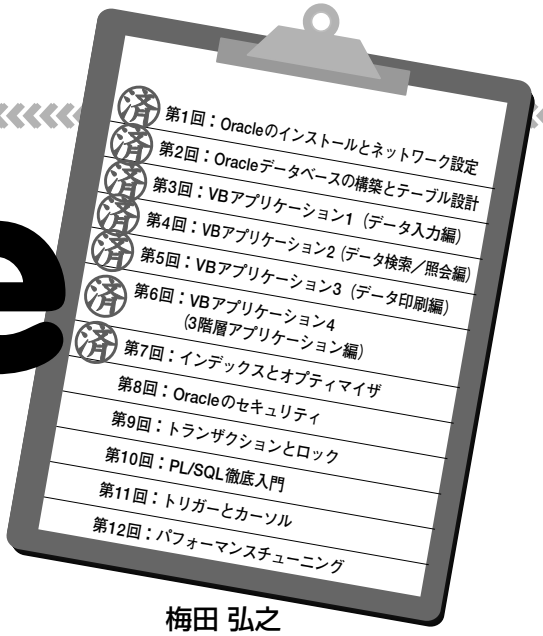
Oracleプログラミング教習所



第8回 Oracleのセキュリティ

梅田 弘之
UMEDA, Hiroyuki

みなさん、「Oracleプログラミング教習所」へようこそ。今回は、VBプログラマがRDBMSを利用する際に知っておかなければならないセキュリティについて学びましょう。RDBMSの役割は、データを蓄積／管理して複数のユーザーで共有利用するものです。そのため、ユーザーごとにデータに対するアクセス権限を設定したり、RDBMS自体を管理、操作する権限をコントロールする必要があります。セキュリティの基本をマスターし、快適なドライビングテクニックを身に付けましょう。

ここでお知らせがあります。11月20日にSQL Serverユーザーグループ（PASSJ）コンファレンスが開催されます[注1]。筆者も、「データベース設計」というテーマでデータモデリングや業務DB設計についてをお話します。参加された方はお気軽に声をかけてください。

1時限目 学科：ユーザー認証とアクセス制御

Oracleのセキュリティには、ユーザー認証やデータに対するアクセス制限、ネットワークの機密保護、第三者認証、データの暗号化、監査など幅広い技術分野に対する対応が用意されています。今回は、その中から基本となるユーザー認証とアクセス制御を理解することにしましょう。

ユーザーとロールとシステム権限

Oracleでは、ユーザーごとにデータベースにアクセスする権限を設定します。Oracleをインストールするとデフォルトで SYSやSYSTEM、SCOTTなどのユーザー名が用意されますが、データベースアプリケーションではこれらのデフォルトユーザー名を使わず、新たに必要なユーザー名を作成して利用します。これまで本連載の講習でも、デフォルトユーザー名であるSYS、SYSTEM以外にユーザー名：「MARKETING」（パスワード：「yosan」）を作成し、Visual Basicで作成したログイン画面（図1）から作成したユーザー名で

本稿で前提となるもの

OS	Windows NT4.0（SP5） Windows 2000（SP3） Windows XP Professional（SP2）
開発環境	Visual Basic 6.0（SP5） Oracle8i/9i

初級　中級　上級

この記事で解説したサンプルプログラムは、付録CD-ROMの¥DMAG¥ORACLEフォルダ以下に収録しています

¥ORACLE06：本連載6回目までに取り上げたVisual Basic 6.0用プロジェクトファイル

注1）参考URL：http://www.sqlpassj.org/conf/default.aspx

図1：Visual Basicアプリケーションからのログオン画面

接続するようにしていましたね。

OracleなどのRDBMSでは、ユーザーにより操作できる機能を制限する必要があります。たとえば、システム管理部門のDatabase Administrator（データベース管理者）の役割を果たす者であればOracleを管理／操作するための権限が必要ですが、一般ユーザーであれば単にアプリケーションを通してデータにアクセスするだけで十分です。このように、ユーザーごとに使用できることをコントロールするために用意された機能が「ロール」と「システム権限」です。

システム権限

システム権限とは、OracleのようなRDBMSを管理／操作するための権限のことです。Oracle9iには図2のようなシステム権限が130種類程度用意されており、これを使い分けてユーザーに対して細かな権限設定ができるようになっています。たとえば「CREATE ANY TABLE」とはテーブルの作成、「DROP USER」はユーザーの削除を行なえるシステム権限です。もしもテーブル作成だけを許可するのであれば「CREATE ANY TABLE」権限だけを付与することになります。

しかし、ユーザーごとにいちいち130種類ものシステム権限を選択して付与するのは大変です。このため、Oracleではユーザーの役割ごとにシステム権限をまとめたロールという機能を用意し、システム権限を細かく付与する代わりにロールを付与するという方式をとっています。

ロール

ロールとはシステム権限の集まりで、Oracle9iでは、15種類のロールがデフォルトで用意されています。たとえばデータベース管理者であればDBAロール（約130種類すべてのシステム権限）をもちますが、データベースに接続するだけであればロール「CONNECT」だけで十分です。ロール「CONNECT」には図2の中の実線で囲んであるような「CREATE TABLE」「CREATE SESSION」などの8つのシステム権限のみが含まれており、テーブルの作成やRDBMSへの接続などが行なえます。

ユーザーには、「ロールを付与」「システム権限を付与」というどちらの方法でも権限付与できるので、自システムのユーザーに与える権限として適当なロールがない場合は、既存ロールに加えてシステム権限を直接付与することも可能です。

しかし、その方法はアクセス権限管理が複雑になるのであまり推奨できません。ロールは、必要に応じて自分で

図2：ユーザーとロールとシステム権限