特集3 ここがポイント! Oracle DB 開発

Oracle meets .NET

第1回

アクセスするユーザーを制限するには

アクセス制御を極める

大田 浩
OTA, Hiroshi
日本オラクル株式会社
Oracle Direct テクニカルサービス部

Level

1 2 3 **4** 5

Technology Tools

- [x] Visual Basic
- [x] Visual C#
- [ ] Visual C++
- [ ] SQL Server
- [x] Oracle
- [ ] Access
- [ ] ASP.NET
- [x] Other:
  - Visual Studio .NET 2003
  - Oracle Data Provider for .NET

Samples

はじめに

.NETとOracleをつなぐためのミドルウェアとして、Oracle社から提供されているOracle Data Provider for .NET（以下ODP.NET）というミドルウェアがあります。このODP.NETを使用してアプリケーションを開発することにより、Oracleの機能をフルに利用したアプリケーション開発が可能になります。本稿では、このODP.NETを利用して、Oracle固有の機能を活用したアプリケーション開発手法について説明します。第1回目となる今回は、「アクセス制御」について説明します。

個人情報漏洩問題などが多発している昨今、アプリケーションを開発する際に、単に要求された機能を実装したアプリケーションを開発すればよいという時代は終わりました。アプリケーションを開発する際には、事前にセキュリティ面について十分に考慮し設計してから開発を行なう必要があります。

システム全体から見た場合、セキュリティについていろいろ考慮することがありますが、今回はアクセス制御に焦点を絞って説明します。

アクセス制御

データベースセキュリティの基本は、共有して利用するデータベースユーザーを廃止、もしくは削減し、ユーザーに必要最小限の権限を付与することです。これにより、データ変更の権限を付与していないユーザーがデータにアクセスしたり変更を加えたりする可能性は格段に低くなります。アクセス制御は、表1のようにユーザーの属性と情報の機密レベルを組み合わせてアクセス制御のマトリックスを作成し、データベースユーザーを定義するところからはじめます。これらのユーザーにどのような権限を付与するかによって、データベースへのアクセスを制限することが可能になります。

近年、内部の者による情報の漏洩事件が頻発していますが、アクセスしてよい情報を限定し、それ以外の情報を取得できないようアクセス制御を厳密

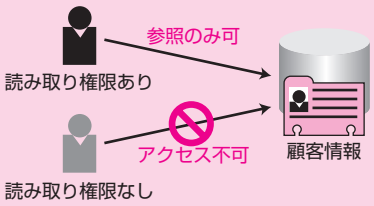
表1：アクセス制御ポリシーの策定

	顧客データ			経理データ		
	低	中	高	低	中	高
営業担当役員	○	○	○	△	△	△
営業本部長	○	○	○	△	△	△
営業部長	○	○	△	△	△	×
営業課長	○	△	×	△	×	×
営業部一般社員	○	×	×	×	×	×
経理担当役員	△	△	△	○	○	○
経理本部長	△	△	△	○	○	○
経理部長	△	△	×	○	○	△
経理課長	△	×	×	○	△	×
経理部一般社員	×	×	×	○	×	×

データの機密レベル 低：機密性 低　中：機密性 中　高：機密性 高

アクセス権限 ○：読み取り、書き込み可能　△：読み取り可能　×：アクセス不可

図1：テーブルに対して権限を設定



に行なうことで回避可能な事件もあります。情報漏洩が起きてしまうと大変な損害が生じます。アクセス制御はリスクを軽減させることができる重要な対策です。

以後は、アクセス制御を考慮したASP.NETのWebアプリケーションをどのように実装するかについて、説明してゆきます。

アクセス制御の実装方法

アクセス制御の具体的な実装方法として、主に以下の3つの手法があります。

- 表単位のアクセス制御
- ビューを使ったアクセス制御
- 行レベルのアクセス制御

それぞれ詳細を見てゆきましょう。

表単位のアクセス制御

アクセス制御をする最も簡単な方法は、テーブルへのアクセス権限による制御です。データベースのユーザーごとに、読み取りの権限や変更の権限を付与して、そのデータを見てはいけないユーザーにはなにも権限を与えず、読み取りのみ可能にするユーザーには読み取り権限を付与する、といった方法です（図1）。

表単位でアクセス権限を設定している場合、ある表に対して読み取り権限を付与するだけで、その表全体を参照できてしまいます。そこで、たとえば人事情報を格納している表の場合は、部署ごとに表を分け、表単位のアクセス権の設定でも対応できます。

しかしこの方法では、ひとつの表を複数に分割しなければなりませんし、アプリケーションの作りなども煩雑になるので、データの持ち方として好ましくありません。そのような場合に考えられるのは、ビューを使ったアクセス制御です。

ビューを使ったアクセス制御

ビューを使ったアクセス制御は、元の表に対して必要な情報のみ参照可能なビューを作成しておき、そのビューに対してのみアクセス権限を付与するという方法です（図2）。ビューへのアクセスは実態としてはSELECT文であり、実データを持ちません。この方法を使えば実データはひとつの表にまとめてすべて格納されているのでデータの持ち方としても問題ありません。また、ユーザーごとにビューを用意すれば、ユーザーごとに異なる結果を見せることも可能です。

ただし、ビューを使用したアクセス制御はユーザー数とビューの数が増え

図2：ビューによるアクセス制御