Oracle9*i* for Windows

セキュリティおよびネットワーク統合ガイド

リリース 2（9.2）

2002 年 7 月

部品番号 : J06335-01

ORACLE®

Oracle9*i* for Windows セキュリティおよびネットワーク統合ガイド , リリース 2（9.2）

部品番号 : J06335-01

原本名 ：Oracle9*i* Security and Network Integration Guide, Release 2 (9.2) for Windows

原本部品番号 ：A95492-01

原本著者 ：Craig B. Foch and Herbert Kelly III

原本協力者 ：Toby Close, David Colello, Mark Kennedy, Chithra Ganesh Ramamurthy, Helen Slattery, and Deborah Steiner

目次

2 外部ユーザーおよびロールの管理

3 エンタープライズ・ユーザーおよびロールの管理

4 Oracle Wallet の Windows レジストリへの格納

5 Windows 2000 PKI の統合

A Oracle Net Services の構成

用語集

索引

はじめに

このマニュアルでは、Windows オペレーティング・システム環境で Oracle9*i* のセキュリティ機能およびネットワーク機能を使用するための概要、インストール後の作業、構成および管理情報について説明します。

このマニュアルで説明するのは、Windows NT、Windows 2000、Windows XP および Windows 98 オペレーティング・システムに適用される Oracle9*i* for Windows ソフトウェアの機能のみです。

次の項目について説明します。

対象読者

『Oracle9*i* for Windows セキュリティおよびネットワーク統合ガイド』は、Windows オペレーティング・システム環境で Oracle9*i* のネットワーク、ディレクトリおよびセキュリティの機能を構成または管理するユーザーを対象としています。

このマニュアルは、次のことを前提としています。

- Windows NT または Windows 2000 がコンピュータ・システムにインストールされ、テストされていること
- オブジェクト・リレーショナル・データベース管理の概念に関する知識があること

このマニュアルの構成

このマニュアルは、次のように構成されています。

「Oracle9i for Windows の新機能」

Oracle9*i* リリース 2（9.2）では、大容量メモリー（VLM）構成がサポートされ、新しいコマンドライン・ツールである User Migration Utility が追加されます。Oracle9*i* リリース 1（9.0.1）では、Windows XP Professional のサポート、Windows との拡張された統合、および Database Configuration Assistant と Oracle Internet Directory の管理における改良が行われました。Server Manager および `CONNECT INTERNAL` は、Oracle9*i* リリース 1（9.0.1）からサポートされていません。

第 1 章「Windows 環境におけるデータベース・ユーザーの認証」

この章では、Windows オペレーティング・システム環境における Oracle9*i* データベース・ユーザーの認証について説明します。

第 2 章「外部ユーザーおよびロールの管理」

この章では、外部ユーザーおよびロールの管理について説明します。

第 3 章「エンタープライズ・ユーザーおよびロールの管理」

この章では、エンタープライズ・ユーザーおよびロールの管理について説明します。

第 4 章「Oracle Wallet の Windows レジストリへの格納」

この章では、Windows レジストリにおける Oracle Wallet の格納および取得について説明します。

第 5 章「Windows 2000 PKI の統合」

この章では、Windows オペレーティング・システム環境における、Oracle 公開鍵インフラストラクチャ（PKI）と Windows 2000 PKI（Windows PKI）の統合について説明します。

付録 A「Oracle Net Services の構成」

この付録では、Windows での Oracle Net Services の構成について説明します。Oracle Net Services の一般的な構成の概要は、『Oracle9*i* Net Services 管理者ガイド』を参照してください。

用語集

関連資料

詳細は、次の Oracle マニュアルを参照してください。

- 『Oracle9*i* Database for Windows インストレーション・ガイド』
- 『Oracle9*i* Database for Windows リリース・ノート』
- 『Oracle9*i* Database for Windows 管理者ガイド』
- 『Oracle Advanced Security 管理者ガイド』
- 『Oracle Internet Directory 管理者ガイド』
- 『Oracle Enterprise Manager 管理者ガイド』
- 『Oracle9*i* Net Services 管理者ガイド』
- 『Oracle9*i* データベース新機能』
- 『Oracle8*i* データベース・リファレンス』

リリース・ノート、インストール・ドキュメント、ホワイト・ペーパー、またはその他の関連資料を無償でダウンロードするには、OTN-J（Oracle Technology Network Japan）にアクセスしてください。OTN-J を利用する前に、オンライン登録が必要です。次の URL で登録できます。

`http://otn.oracle.co.jp/membership/`

OTN-J のユーザー名およびパスワードをすでにお持ちの場合は、次の OTN-J の Web サイトのドキュメント・セクションに直接アクセスできます。

`http://otn.oracle.co.jp/document/`

表記規則

ここでは、このマニュアルの本文およびサンプル・コードで使用される表記規則について説明します。表記規則は次の 3 種類です。

- 本文の表記規則
- サンプル・コードの表記規則
- Windows オペレーティング・システムの表記規則

本文の表記規則

本文中では、特定の用語をより簡単に識別できるように、様々な表記規則を使用しています。次の表は、本文中で使用される表記規則とその使用例を説明したものです。

規則	意味	例
太字	太字は、本文中で定義されている用語、または用語集で説明されている用語、あるいはその両方を示します。	この句を指定する場合、**索引構成表**を作成します。
大文字（固定幅）フォント	大文字固定幅フォントは、システムによって指定される要素を示します。これらの要素には、パラメータ、権限、データ型、Recovery Manager のキーワード、SQL のキーワード、SQL*Plus またはユーティリティのコマンド、パッケージ、メソッドの他に、システムで表示される列名、データベースのオブジェクトおよび構造、ユーザー名およびロールがあります。	この句は NUMBER 列に対してのみ指定できます。 BACKUP コマンドを使用して、データベースをバックアップできます。 USER_TABLES データ・ディクショナリ・ビューの TABLE_NAME 列を問い合せます。 DBMS_STATS.GENERATE_STATS プロシージャを使用します。
小文字（固定幅）フォント	小文字固定幅フォントは、実行可能ファイル、ファイル名、ディレクトリ名、およびサンプルのユーザー指定要素を示します。これらの要素には、コンピュータ名およびデータベース名、ネット・サービス名、および接続識別子の他に、ユーザー指定のデータベースのオブジェクトおよび構造、列名、パッケージおよびクラス、ユーザー名およびロール、プログラム・ユニット、およびパラメータ値があります。 **注意：** 一部のプログラム要素には、大文字と小文字の両方が使用されます。これらの要素は、記載されているとおりに入力してください。	sqlplus を入力して、SQL*Plus を開きます。 パスワードは、orapwd ファイルで指定されます。 ¥disk1¥oracle¥dbs ディレクトリのデータ・ファイルと制御ファイルをバックアップします。 department_id、department_name および location_id 列は、hr.departments 表にあります。 QUERY_REWRITE_ENABLED 初期化パラメータを true に設定します。 oe ユーザーとして接続します。 JRepUtil クラスは、これらのメソッドを実装します。

規則	意味	例
小文字イタリック (固定幅) フォント	小文字イタリック固定幅フォントは、プレースホルダまたは変数を示します。	*parallel_clause* を指定できます。 U*old_release*.SQL を実行します。*old_release* は、アップグレード前にインストールしたリリースを表します。

サンプル・コードの表記規則

サンプル・コードは、SQL、PL/SQL、SQL*Plus またはその他のコマンドライン文を示します。これらは固定幅フォントで示され、次の例のように、通常の本文とは区別されています。

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

次の表は、サンプル・コードで使用される表記規則とそれらの使用例を説明したものです。

規則	意味	例
[ ]	大カッコは、1 つ以上のオプション項目を囲みます。大カッコは入力しないでください。	DECIMAL (*digits* [, *precision*])
{ }	中カッコは複数の項目を囲み、そのうちの 1 つが必要であることを示します。中カッコは入力しないでください。	{ENABLE | DISABLE}
|	縦線は、大カッコまたは中カッコ内にある複数のオプションの選択肢を区切るために使用します。オプションの 1 つを入力します。縦線は入力しないでください。	{ENABLE | DISABLE} [COMPRESS | NOCOMPRESS]
...	水平の省略記号は、次のいずれかを示します。	
	■ 例に直接関係のないコードの一部を省略	CREATE TABLE ... AS *subquery*;
	■ コードの一部の繰り返しが可能	SELECT *col1*, *col2*, ... , *coln* FROM employees;
. . .	垂直の省略記号は、例に直接関係のないコードの数行を省略したことを示します。	SQL> SELECT NAME FROM V$DATAFILE; NAME ---------- /fsl/dbs/tbs_01.dbf /fs1/dbs/tbs_02.dbf . . . /fsl/dbs/tbs_09.dbf 9 rows selected.

規則	意味	例
その他の表記規則	大カッコ、中カッコ、縦線および省略記号以外の記号は、示されているとおりに入力してください。	`acctbal NUMBER(11,2);` `acct    CONSTANT NUMBER(4) := 3;`
イタリック	イタリックの文字は、特定の値を指定する必要のあるプレースホルダまたは変数を示します。	`CONNECT SYSTEM/`*`system_password`* `DB_NAME = `*`database_name`*

大文字	大文字は、システムによって指定される要素を示します。ユーザーが定義する語句と区別するために、大文字で示しています。語句が大カッコ内に表示されている場合を除き、記載されているとおりの順序とスペルで入力します。ただし、これらの語句には大文字と小文字の区別がないため、小文字で入力できます。	`SELECT last_name, employee_id FROM employees;`
		`SELECT * FROM USER_TABLES;`
		`DROP TABLE hr.employees;`

小文字	小文字は、ユーザーが指定するプログラム要素を示します。たとえば、小文字は表、列またはファイルの名前を示します。
	注意： 一部のプログラム要素には、大文字と小文字の両方が使用されます。これらの要素は、記載されているとおりに入力してください。
		`SELECT last_name, employee_id FROM employees;`
		`sqlplus hr/hr`
		`CREATE USER mjones IDENTIFIED BY ty3MU9;`

Windows オペレーティング・システムの表記規則

次の表は、Windows オペレーティング・システムの表記規則とその使用例を説明したものです。

規則	意味	例
「スタート」→を選択	プログラムの起動方法。たとえば、Database Configuration Assistant を起動するには、タスクバーの「スタート」ボタンをクリックし、「プログラム」→「Oracle - *HOME_NAME*」→「Configuration and Migration Tools」→「Database Configuration Assistant」を選択します。	「スタート」→「プログラム」→「Oracle - *HOME_NAME*」→「Configuration and Migration Tools」→「Database Configuration Assistant」を選択します。

規則	意味	例
ファイル名およびディレクトリ名	ファイルおよびディレクトリ名には、大文字と小文字の区別がありません。<、>、:、"、/、|、および - の特殊文字は使用できません。特殊文字 ¥ は、引用符に囲まれている場合でも、要素の区切り文字として扱われます。ファイル名が ¥¥ で始まる場合、Windows では汎用命名規則を使用しているものと認識されます。	c:¥winnt"¥"system32 は、C:¥WINNT¥SYSTEM32 と同じです。
C:¥>	現行のハード・ディスク・ドライブの Windows コマンド・プロンプトを示します。コマンド・プロンプトのエスケープ文字は、カレット（^）です。プロンプトは、現在作業中のサブディレクトリを示しています。このマニュアルでは、コマンド・プロンプトと呼びます。	C:¥oracle¥oradata>
特殊文字	特殊文字の円記号（¥）は、Windows コマンド・プロンプトで特殊文字の二重引用符（"）のエスケープ文字として必要な場合があります。カッコおよび特殊文字の一重引用符（'）は、エスケープ文字を必要としません。エスケープ文字および特殊文字の詳細は、Windows オペレーティング・システムのドキュメントを参照してください。	C:¥>exp scott/tiger TABLES=emp QUERY=¥"WHERE job='SALESMAN' and sal<1600¥" C:¥>imp SYSTEM/*password* FROMUSER=scott TABLES=(emp, dept)
HOME_NAME	Oracle ホーム名を示します。 ホーム名は、英数字 16 文字までです。ホーム名で使用できる特殊文字は、アンダースコアのみです。	C:¥> net start Oracle*HOME_NAME*TNSListener

規則	意味	例
ORACLE_HOME および ORACLE_BASE	Oracle8 リリース 8.0 以下のリリースでは、Oracle コンポーネントをインストールすると、サブディレクトリはすべて、最上位の ORACLE_HOME ディレクトリ（デフォルトでは次のとおり）の下に置かれました。 ■ Windows NT の場合は C:¥orant ■ Windows 98 の場合は C:¥orawin98 あるいは、Oracle ホームと呼ばれるディレクトリの下に置かれました。 今回のリリースは、Optimal Flexible Architecture（OFA）に準拠しています。すべてのサブディレクトリが最上位の ORACLE_HOME ディレクトリの下にあるわけではありません。ORACLE_BASE という最上位ディレクトリがあり、デフォルトは C:¥oracle です。コンピュータに最新の Oracle リリースをインストールし、他の Oracle ソフトウェアをインストールしない場合、最初の Oracle ホーム・ディレクトリのデフォルト設定は、C:¥oracle¥ora*nn* です。*nn* は、最新のリリース番号です。Oracle ホーム・ディレクトリは、ORACLE_BASE の直下に置かれます。 このマニュアルでは、ディレクトリ・パスの例は、すべて OFA 表記規則に準拠しています。	%ORACLE_HOME%¥rdbms¥admin ディレクトリに移動します。

Oracle9*i* for Windows の新機能

この項では、Oracle9*i* リリース 2（9.2）の新機能について説明し、追加情報の参照先を示します。現在のリリースに移行するユーザーに役立つよう、前のリリースの新機能情報も記載しています。

次の項では、各リリースの新機能について説明します。

Oracle9*i* リリース 2（9.2）の新機能

次の内容について説明します。

- 大容量メモリー（VLM）のサポート
- User Migration Utility

大容量メモリー（VLM）のサポート

Oracle9*i* for Windows リリース 2（9.2）は、Windows 2000 での大容量メモリー（VLM）構成をサポートします。これにより、Oracle9*i* リリース 2（9.2）は、Windows アプリケーションでこれまで使用可能だった 4 ギガバイト（GB）を超える RAM にアクセスできます。詳細は、『Oracle9*i* Database for Windows スタート・ガイド』の「Windows での Oracle9*i* の拡張性」を参照してください。

User Migration Utility

新しいコマンドライン・ツールである User Migration Utility は、ローカルまたは外部データベース・ユーザーからエンタープライズ・ユーザーへの変換を簡略化します。詳細は、次の関連資料を参照してください。

- 『Oracle9*i* Database for Windows スタート・ガイド』の「データベース・ツールの概要」
- 2-44 ページの「ユーザーの手動による移行」
- 『Oracle Advanced Security 管理者ガイド』の第 16 章

Oracle9*i* リリース 1（9.0.1）の新機能

次の内容について説明します。

- Windows XP のサポート
- Windows との統合
- Database Configuration Assistant の改良
- Oracle Internet Directory 管理の改良
- Windows 2000 での Oracle9i の使用
- CONNECT INTERNAL のサポートの中止
- Server Manager のサポートの中止

Windows XP のサポート

Oracle9*i* for Windows リリース 1（9.0.1.1.1）は、32 ビット・バージョンの Windows XP Professional で動作保証されています。

オラクル社では、様々なプラットフォームでのコンポーネントのサポート情報を提供し、互換性のあるクライアントとデータベースのバージョンをリストし、パッチと対処方法に関する情報を確認しています。次の URL で、最新の情報を参照してください。

```
http://www.oracle.co.jp/
http://support.oracle.co.jp/
```

Windows との統合

Oracle9*i* は、Microsoft Transaction Services および Internet Information Services との拡張された統合をサポートします。Oracle9*i* の PKI およびシングル・サインオン機能は、Windows 2000、Active Directory および Microsoft 証明書ストアとも統合されています。

Windows セキュリティと Oracle9*i* の統合により、レジストリおよび Active Directory で Oracle Wallet をサポートし、Oracle 製品で Microsoft 証明書ストアが使用できるようになります。

Active Directory と Oracle Internet Directory の同期により、Oracle およびサード・パーティ製メタディレクトリ・コンポーネントのスケジューリングおよび構成が集中化されます。

Database Configuration Assistant の改良

Database Configuration Assistant は、テンプレートとして保存されたデータベース定義を含むよう再設計されました。テンプレートで、データベースを生成できます。ユーザーは、新規テンプレートを定義、既存のテンプレートを変更またはオラクル社が提供しているテンプレートを使用できます。Database Configuration Assistant でデータベースを作成する際に、ユーザーは Oracle の新しいサンプル・スキーマを含めることができます。

Oracle Internet Directory 管理の改良

Oracle Internet Directory レプリケーション・サーバーの管理は、新しいレプリケーション・キュー管理および調整ツールの追加によって改良されました。

Windows 2000 での Oracle9*i* の使用

Windows 2000 と Windows NT 4.0 での Oracle9*i* の使用方法には、いくつかの違いがあります。詳細は、『Oracle9*i* Database for Windows スタート・ガイド』の「Windows 2000 での Oracle9*i* の使用」を参照してください。

CONNECT INTERNAL のサポートの中止

CONNECT INTERNAL および CONNECT INTERNAL/PASSWORD は、Oracle9*i* ではサポートされません。かわりに次のものを使用します。

```
CONNECT / AS SYSDBA
CONNECT username/password AS SYSDBA
```

Server Manager のサポートの中止

Server Manager は、Oracle9*i* ではサポートされません。かわりに SQL*Plus を使用します。ほとんどの Server Manager スクリプトは SQL*Plus 環境で動作しますが、変更の必要なスクリプトもあります。

1

Windows 環境におけるデータベース・ユーザーの認証

この章では、Windows オペレーティング・システム環境における Oracle9*i* データベース・ユーザーの認証について説明します。

この章の項目は次のとおりです。

Windows のシステム固有の認証の概要

Oracle9*i* データベースでは、データベース・ユーザーの**認証**に Windows のユーザー・ログイン**資格証明**を使用できます。これには次の利点があります。

- ユーザーは、**ユーザー名**またはパスワードを入力することなく、Oracle9*i* データベースに接続できます。
- Oracle9*i* データベースのユーザー認証およびロール**認可**の情報を、Windows NT または Windows 2000 で一元管理することにより、ユーザー・パスワードまたは**ロール**の情報を Oracle9*i* に格納して管理する必要がなくなります。

（**Oracle Net Services** とともに自動的にインストールされる）Windows のシステム固有の認証アダプタにより、Windows NT または Windows 2000 を介してデータベース・ユーザー認証を行うことができます。これにより、クライアント・コンピュータは Windows NT または Windows 2000 サーバー上の Oracle9*i* データベースに安全に接続できます。その後、サーバーではユーザーによるデータベース・アクションの実行が許可されます。

注意： この章では、Windows NT 4.0 および Windows 2000 環境における Windows のシステム固有の認証方式の使用方法を説明します。SSL プロトコルおよび Oracle Internet Directory の詳細は、『Oracle Advanced Security 管理者ガイド』および『Oracle Internet Directory 管理者ガイド』を参照してください。

Windows の認証プロトコル

Windows のシステム固有の認証アダプタおよび Windows の認証プロトコルにより、Oracle9*i* データベースへのアクセスが可能になります。

- Windows 2000 のデフォルトの認証プロトコルは、Kerberos です。
- Windows NT 4.0 のデフォルトのプロトコルは、NT LAN Manager（NTLM）です。

ユーザーが Windows 2000 環境のコンピュータから、Windows 2000 ドメイン・ユーザーとしてログインする場合、Kerberos が NTS アダプタにより使用される認証機構になります。

その他のすべてのユーザー（ローカル・ユーザー、Windows NT 4.0 ドメイン・ユーザー、Windows 95 および Windows 98 ユーザー）の場合、NTLM が NTS アダプタにより使用される認証機構になります。

スタンドアロンの Windows 2000 または Windows NT 4.0 環境のコンピュータで認証が NTS に設定されている場合は、Windows サービスの NT LM Security Support Provider が開始されていることを確認します。この**サービス**が、スタンドアロンの Windows 2000 または Windows NT 4.0 環境のコンピュータで開始されていない場合、NTS 認証は失敗します。この問題は、Windows 2000 または Windows NT 4.0 をスタンドアロン・モードで稼働している場合にのみ発生します。

クライアント・コンピュータは、Oracle9*i* データベースに接続を試みるときに、認証プロトコルを指定する必要はありません。使用されるプロトコルは、Oracle9*i* データベースによりユーザーに対して完全に透過的に判断されます。唯一の Oracle 側での要件は、クライアントおよびデータベース・サーバーの両方で、次のファイル内のパラメータ SQLNET.AUTHENTICATION_SERVICES に nts が含まれていることです。

```
%ORACLE_HOME%¥network¥admin¥sqlnet.ora
```

インストール後には、これが両方のデフォルト設定になります。Oracle8 リリース 8.0 では、手動でこの値を設定する必要があります。

通常、Oracle9*i* データベースのネットワーク上には、クライアント・コンピュータおよびデータベース・サーバーがあります。このネットワーク上の複数のコンピュータでは、別々のドメインの異なる Windows オペレーティング・システムで、異なるリリースの Oracle ソフトウェアが使用されている場合があります。たとえば、Windows 95 環境にインストールされたリリース 8.0.5 の Oracle クライアントが稼働しており、Windows 2000 ドメイン内の稼働する Windows NT 4.0 環境のコンピュータにインストールされている Oracle9*i* データベースに接続している場合もあります。このようにリリースの異なる組合せが使用されている場合、その認証プロトコルも異なる可能性があります。

Kerberos をデフォルトの認証プロトコルとして使用できるようにするために必要な Oracle ソフトウェアおよび Windows オペレーティング・システムのリリースを、表 1-1 に示します。

表 1-1 Kerberos 認証プロトコルが使用可能なソフトウェア要件

場所	Windows ソフトウェア	Oracle ソフトウェア
クライアント・コンピュータ	Windows NT 4.0 または Windows 2000	Oracle8*i* クライアント以上
データベース・コンピュータ	Windows NT 4.0 または Windows 2000	Oracle8*i* データベース以上
ドメイン	Windows 2000	なし

ネットワーク上で使用される Windows オペレーティング・システムおよび Oracle ソフトウェアのリリースのこれ以外の組合せでは、使用される認証プロトコルはすべて NTLM です。

> **関連資料：** 各認証プロトコルの詳細は、Microsoft Windows のドキュメントを参照してください。

ユーザー認証およびロール認可の方式

この項では、Windows NT 4.0 または Windows 2000 ドメインにおいて、ユーザー・ログイン資格証明が認証される方式、およびデータベース・ロールが認可される方式を説明します。ユーザー認証およびロール認可の定義を表 1-2 に示します。

表 1-2 ユーザー認証およびロール認可の定義

機能	説明	詳細情報の参照先
ユーザー認証	データベースが、ユーザーの Windows ログイン資格証明を使用してユーザーを認証するプロセス	『Oracle9*i* データベース管理者ガイド』
ロール**認可**	割り当てられた一連のロールを認証済のユーザーに対して付与するプロセス	『Oracle9*i* データベース管理者ガイド』

Oracle では、Windows NT 4.0 ドメインにおけるユーザー認証およびロール認可がサポートされています。表 1-3 では、これらの基本的な機能を説明します。

表 1-3 ユーザー認証およびロール認可の基本的な機能

機能	説明
外部ユーザーの認証	ユーザーは、データベースによって Windows ログイン資格証明を使用して認証され、追加のログイン資格証明を要求されることなく Oracle9*i* データベースにアクセスできます。
外部ロールの認可	ロールは、**Windows NT ローカル・グループ**を使用して認可されます。一度**外部ロール**を作成すると、データベース・ユーザーに対してそのロールを付与したり、取り消したりできます。初期化パラメータ `OS_ROLES` は、デフォルトでは `false` に設定されています。外部ロールを認可するには、`OS_ROLES` を `true` に設定する必要があります。

Oracle8*i* リリース 8.1.6 以上では、**エンタープライズ・ユーザー**の認証および**エンタープライズ・ロール**の認可をサポートするよう機能が拡張されています。また、Oracle Internet Directory との統合に加え、Windows 2000 ドメイン内および Active Directory 内で Windows のシステム固有の認証をサポートするよう機能が拡張されています。これらの拡張機能は次の場合にのみ使用可能です。

- Oracle8*i* リリース 8.1.6 以上を構成して、Active Directory とともに使用する場合
- Oracle8*i* リリース 8.1.6 以上のクライアントおよび Oracle8*i* 以上のデータベースを、Windows 2000 ドメインで実行する場合

エンタープライズ・ユーザー認証（またはグローバル・ユーザー認証とも呼ぶ）は、Oracle9*i* データベースが稼働している Windows 2000 ドメインのコンピュータで**レジストリ**・パラメータ `OSAUTH_X509_NAME` を `true` に設定することで使用できます。Windows 2000 ドメインでこのパラメータが `false`（デフォルト）に設定されていると、Oracle9*i*

データベースでは、ユーザーが**外部ユーザー**として認証されます（3-2 ページの「エンタープライズ・ユーザーの認証」を参照）。Windows NT 4.0 ドメインでこのパラメータを `true` に設定しても意味がなく、エンタープライズ・ユーザーは使用できません。

> **関連項目：** レジストリ・パラメータ `OSAUTH_X509_NAME` の使用方法の詳細は、3-2 ページの「エンタープライズ・ユーザーの認証」を参照してください。

使用する認証および認可の方式

表 1-4 では、Oracle9*i* データベース環境に基づいた、ユーザー認証およびロール認可の方式を説明します。

表 1-4 ユーザー認証およびロール認可の方式

方式	データベース環境
エンタープライズ・ユーザーおよびロール	複数のデータベースに多数のユーザーが接続する場合。 エンタープライズ・ユーザーは、複数のデータベース間で同じ識別情報を持ちます。エンタープライズ・ユーザーは、ディレクトリ・サーバーを使用する必要があります。 エンタープライズ・ロールは、ロールが割り当てられたエンタープライズ・ユーザーが地理的に多数の場所に存在しており、複数のデータベースにアクセスする必要がある場合に使用します。各エンタープライズ・ロールは、ディレクトリ内の複数のエンタープライズ・ユーザーに割り当てることができます。エンタープライズ・ロールを使用しない場合は、各データベース・ユーザーに手動でデータベース・ロールを割り当てる必要があります。エンタープライズ・ロールは、ディレクトリ・サーバーを使用する必要があります。
外部ユーザーおよびロール	限定された数のデータベースに少数のユーザーが接続する場合。外部ユーザーは個別に各データベースで作成する必要があり、ディレクトリ・サーバーを使用する必要はありません。 外部ロールも個別に各データベースで作成する必要があり、ディレクトリ・サーバーを使用する必要はありません。外部ロールは、システムの**ローカル・グループ**内のユーザーのグループ・メンバーシップを使用して認可されます。

Active Directory と Oracle9*i* の統合

Active Directory と Oracle9*i* の統合により、オペレーティング・システムのユーザー認証およびロール認可を使用できます。Active Directory と Oracle コンポーネントを統合するには、次のタスクを実行します。

- タスク 1: コンポーネントのインストールおよび構成
- タスク 2: レジストリ・パラメータ OSAUTH_X509_NAME の設定
- タスク 3: Oracle Enterprise Security Manager の起動および使用

注意： オペレーティング・システムのユーザー認証およびロール認可は、Windows 2000 ドメインで実行する場合にのみ使用可能になります。

タスク 1: コンポーネントのインストールおよび構成

インストール前および構成時の問題の詳細は、『Oracle Advanced Security 管理者ガイド』の付録 E および『Oracle9*i* Database for Windows インストレーション・ガイド』を参照してください。

タスク 2: レジストリ・パラメータ OSAUTH_X509_NAME の設定

レジストリ・パラメータ `OSAUTH_X509_NAME` を `true` に設定し、クライアント・ユーザーが X.509 準拠のエンタープライズ・ユーザーとして Oracle9*i* データベースにアクセスできるようにします。Active Directory は、クライアント・ユーザー名の識別およびロールの認可に使用されます。このパラメータの設定は、エンタープライズ・ユーザーおよびロールを使用する場合にのみ必要です。

このパラメータを `false`（デフォルト）に設定すると、クライアント・ユーザーは外部ユーザーとして識別され、ユーザーのロール認可には Oracle9*i* データベースの**データ・ディクショナリ**が使用されます。

レジストリ・パラメータ `OSAUTH_X509_NAME` を設定するには、次のようにします。

1. Oracle9*i* データベースがインストールされているコンピュータに移動します。
2. 「スタート」→「ファイル名を指定して実行」を選択します。
3. 「名前」フィールドに `regedt32` と入力し、「OK」を選択します。

   「レジストリ エディタ」ウィンドウが表示されます。
4. `¥HKEY_LOCAL_MACHINE¥SOFTWARE¥ORACLE¥HOME`*`ID`* に移動します。

   `ID` は編集する Oracle ホームの番号です。

5. レジストリ値 OSAUTH_X509_NAME がある場合は、OSAUTH_X509_NAME をダブルクリックします。

   「文字列エディタ」ダイアログ・ボックスが表示されます。

   該当するレジストリ値がない場合は、REG_EXPAND_SZ のレジストリ値として、OSAUTH_X509_NAME を追加します。

6. [Enter] を押します。
7. 「文字列」フィールドの値を true に設定します。
8. 「OK」をクリックします。
9. 「レジストリ」メニューから「レジストリ エディタの終了」を選択します。

   レジストリ エディタを終了します。

タスク 3: Oracle Enterprise Security Manager の起動および使用

Oracle Enterprise Security Manager は、Oracle Enterprise Manager の統合アプリケーションです。Oracle Enterprise Security Manager を使用して、エンタープライズ・ユーザー、ロールおよびドメインを作成および管理できます。また、エンタープライズ・ユーザーおよびグループにエンタープライズ・ロールを割り当てることもできます。

> **関連資料：** Oracle Enterprise Security Manager の使用方法の詳細は、『Oracle Advanced Security 管理者ガイド』を参照してください。

Oracle Enterprise Security Manager を使用する管理者は、セキュリティ・グループ OracleDBSecurityAdmin のメンバーである必要があります。デフォルトでは、Oracle コンテキストを作成した（つまり、Oracle9*i* データベースを構成して、ディレクトリ・サーバーを使用できるようにした）管理者は、このセキュリティ・グループのメンバーです。Oracle Enterprise Security Manager のすべての機能を使用できるよう認可されるのは、このセキュリティ・グループのメンバーのみです。別のユーザーを手動で追加する場合の詳細は、『Oracle Advanced Security 管理者ガイド』の付録 E を参照してください。

使用する環境に適した認証プロトコルを選択するダイアログ・ボックスにアクセスする場合、「ファイル」メイン・メニューから「Change Directory Connection」を選択します。Active Directory とともに Windows 2000 ドメイン内の Windows NT 4.0 または Windows 2000 環境のコンピュータで Oracle9*i* データベースを実行する場合、「システム固有の認証」を選択します。Oracle Enterprise Security Manager が Windows 2000 ドメイン内で稼働している場合は、自動的に Windows のシステム固有の認証を使用します。

他に使用可能な選択がない場合、「パスワード認証」を選択します。簡易認証は Oracle Internet Directory または Active Directory で使用できますが、安全性は低下します。

Active Directory での Oracle9*i* ディレクトリ・サーバー機能の使用方法

次の項目の詳細は、『Oracle Advanced Security 管理者ガイド』の付録 E を参照してください。

- LDAP および Active Directory の概要
- Oracle9*i* ディレクトリ・サーバー機能
- Active Directory との統合
- Active Directory で Oracle9*i* を使用するための要件
- Active Directory での Oracle9*i* のインストールおよび構成
- 接続のテスト
- Oracle ディレクトリ・オブジェクトのアクセス制御リスト（ACL）の管理
- エンタープライズ・ドメインの作成

インストール時に使用可能になるオペレーティング・システムの認証

Oracle9*i* データベースをインストールすると、ORA_DBA という特別な Windows NT ローカル・グループが作成され（過去のインストールで作成されていない場合）、Windows のユーザー名が自動的に追加されます。ローカル・グループ ORA_DBA のメンバーには、自動的に**SYSDBA 権限**が付与されます。

ORA_DBA のメンバーシップにより、次のことが可能です。

- 次のコマンドを使用し、パスワードなしでローカルの Oracle9*i* データベースに接続できます。

  ```
  CONNECT / AS SYSDBA
  ```

- 次のコマンドを使用し、パスワードなしでリモートの Oracle9*i* データベースに接続できます。

  ```
  CONNECT /@net_service_name AS SYSDBA
  ```

  net_service_name は、リモートの Oracle9*i* データベースの**ネット・サービス名**です。

- ローカル・データベースの起動および停止など、データベース管理手順を実行できます。
- 別の Windows NT ユーザーを ORA_DBA に追加し、そのユーザーに SYSDBA 権限を付与できます。

2

外部ユーザーおよびロールの管理

外部ユーザーおよびロールは、一般に Oracle9*i* データベースの外部のものによって定義されます。Windows 環境では、オペレーティング・システムによって定義されます。

この章では、Oracle Administration Assistant for Windows NT を使用するか、または Oracle コマンドライン・ツール、レジストリ エディタ、および Windows NT のユーザー マネージャを使用した、**外部ユーザー**および**外部ロール**の作成と管理方法について説明します。

注意： どちらの方法でも、Windows 2000 ドメインで外部ユーザーおよびロールを管理できますが、**エンタープライズ・ユーザー**または**エンタープライズ・ロール**の管理には使用できません。エンタープライズ・ユーザーおよびエンタープライズ・ロールの管理に使用できるツールの詳細は、第 3 章「エンタープライズ・ユーザーおよびロールの管理」を参照してください。

この章の項目は次のとおりです。

Oracle Administration Assistant for Windows NT の使用方法

Oracle Administration Assistant for Windows NT は、**Microsoft 管理コンソール**から実行するツールです。このツールを使用すると、Windows オペレーティング・システムで**認証**を行い、パスワードなしで Oracle9*i* データベースにアクセスできる、次の Oracle データベース・ユーザーおよびロールを構成することができます。

- 通常の Windows NT ドメイン・ユーザーおよび**グローバル・グループ**（外部ユーザーとして）
- Windows NT データベース管理者（**SYSDBA 権限**を持つ）
- Windows NT データベース・オペレータ（**SYSOPER** 権限を持つ）

また、Oracle Administration Assistant for Windows NT では、ローカルおよび外部データベース・ロールを作成し、Windows NT ドメイン・ユーザーおよびグローバル・グループに付与できます。

Oracle Administration Assistant for Windows NT を使用すると、次のことを手動で実行する必要はありません。

- データベースの**システム識別子（SID）**および**ロール**と一致する Windows NT **ローカル・グループ**の作成
- これらのローカル・グループへの Windows NT ドメイン・ユーザーの割当て
- SQL*Plus における、`CREATE USER` *`username`* `IDENTIFIED EXTERNALLY` 構文でのユーザー認証

この項では、Oracle Administration Assistant for Windows NT を使用した、次のタスクの実行方法について説明します。

- コンピュータの追加と構成の保存
- コンピュータ上のすべてのデータベースに対する管理者権限の付与
- コンピュータ上のすべてのデータベースに対するオペレータ権限の付与
- データベースへの接続
- データベース認証用パラメータ設定の表示
- 外部 OS ユーザーの作成
- ローカル・データベース・ロールの作成
- 外部 OS ロールの作成
- 単一データベースに対する管理者権限の付与
- 単一データベースに対するオペレータ権限の付与

注意： Oracle Administration Assistant for Windows NT は、Microsoft 管理コンソールから実行できますが、このコンソールは Windows 2000 に組み込まれています。Windows NT 4.0 を使用する場合は、次のいずれかを実行してください。

- Microsoft 管理コンソールを含む、Microsoft Windows NT 4.0 Option Pack をインストール
- Microsoft の Web サイト（`http://www.microsoft.com`）から Microsoft 管理コンソールをダウンロード

リモート・コンピュータの管理

Oracle Administration Assistant for Windows NT を使用して**リモート・コンピュータ**を管理する場合は、そのコンピュータに対して管理者権限を持っている必要があります。Oracle Administration Assistant for Windows NT によって Oracle9*i* データベースで作成されるユーザーの名前には、常に接頭辞としてドメイン名が付けられます。Oracle7 リリース 7*x* 以上のデータベースをリモート管理する場合は、リモート・コンピュータのレジストリ・パラメータ `OSAUTH_PREFIX_DOMAIN` を `true` に設定する必要があります。このパラメータは次のキーにあります。

```
¥HKEY_LOCAL_MACHINE¥SOFTWARE¥ORACLE¥HOME_ID
```

Windows 2000 環境のコンピュータがドメイン・ネーム・システム（DNS）のドメイン名で識別されない場合は、次のエラー・メッセージが表示されます。

```
Calling query w32RegQueries1.7.0.17.0  RegGetValue
Key = HKEY_LOCAL_MACHINE
SubKey = SYSTEM¥CurrentControlSet¥Services¥Tcpip¥Parameters
Value = Domain
Query Exception: GetValueKeyNotFoundException
Query Exception Class: class oracle.sysman.oii.oiil.OiilQueryException
...
```

DNS 名を割り当てるには、次のようにします。

1. 「コントロール パネル」→「システム」→「ネットワーク ID」の「プロパティ」→「詳細」→「このコンピュータのプライマリ DNS サフィックス」を選択します。
2. ドメイン名を入力します（`US.ORACLE.COM` など）。

コンピュータの追加と構成の保存

Oracle Administration Assistant for Windows NT を初めて使用すると、ローカル・コンピュータがナビゲーション・ツリーに追加されます。その後で、他のコンピュータを追加できます。

Microsoft 管理コンソールのツリーにコンピュータを追加するには、次のようにします。

1. 「スタート」→「プログラム」→「Oracle - *HOME_NAME*」→「Configuration and Migration Tools」→「Administration Assistant for Windows NT」を選択します。

   Microsoft 管理コンソールが起動します。

2. 「Oracle Managed Objects」をダブルクリックします。

   「コンピュータ」アイコンが表示されます。

3. 「コンピュータ」を右クリックします。

4. 「新規作成」→「NT コンピュータ」を選択します。

   「コンピュータ追加」ダイアログ・ボックスが表示されます。

5. Oracle データベースがインストールされているコンピュータのドメイン名およびコンピュータ名を指定します。
6. 「OK」をクリックします。
7. 「コンピュータ」をダブルクリックし、追加したコンピュータを表示します。

8. 追加したコンピュータをダブルクリックします。データベース管理者およびオペレータを認証するためのノードがいくつか表示されます。

   「OS データベース管理者 - コンピュータ」ノードでは、コンピュータ上のすべてのデータベース・インスタンスに対する SYSDBA 権限を持つ、オペレーティング・システムで認証されたデータベース管理者を作成します。「OS データベース・オペレータ - コンピュータ」ノードでは、コンピュータ上のすべてのデータベース・インスタンスに対する SYSOPER 権限を持つ、オペレーティング・システムで認証されたデータベース・オペレータを作成します。

9. 「コンソール」メイン・メニューの「上書き保存」をクリックして、コンソール・ファイルに構成を保存します。これにより、コンピュータ上のすべてのインスタンスに対するデータベース管理者およびオペレータを認証できます。

コンピュータ上のすべてのデータベースに対する管理者権限の付与

コンピュータ上のすべてのデータベースに対するデータベース管理者（SYSDBA）権限をデータベース管理者（DBA）に付与するには、次のようにします。

1. 「スタート」→「プログラム」→「Oracle - *HOME_NAME*」→「Configuration and Migration Tools」→「Administration Assistant for Windows NT」を選択します。

   Oracle Administration Assistant for Windows NT が起動します。

2. 「OS データベース管理者 - コンピュータ」を右クリックします。

3. 「追加 / 削除」を選択します。

   「OS データベース管理者 - コンピュータ : *hostname*」ダイアログ・ボックスが表示されます。

4. 「ドメイン」リスト・ボックスで、SYSDBA 権限を付与するユーザーのドメインを選択します。
5. ユーザーを選択します。
6. 「追加」をクリックします。

   ユーザーが「OS データベース管理者 - コンピュータ」ウィンドウに表示されます。
7. 「OK」をクリックします。

コンピュータ上のすべてのデータベースに対するオペレータ権限の付与

コンピュータ上のすべてのデータベースに対するデータベース・オペレータ（SYSOPER）権限を DBA に付与するには、次のようにします。

1. 「スタート」→「プログラム」→「Oracle - *HOME_NAME*」→「Configuration and Migration Tools」→「Administration Assistant for Windows NT」を選択します。

   Oracle Administration Assistant for Windows NT が起動します。

2. 「OS データベース・オペレータ - コンピュータ」を右クリックします。

3. 「追加 / 削除」を選択します。

   「OS データベース・オペレータ - コンピュータ : *hostname*」ダイアログ・ボックスが表示されます。

4. 「ドメイン」リスト・ボックスで、SYSOPER 権限を付与するユーザーのドメインを選択します。
5. ユーザーを選択します。
6. 「追加」をクリックします。

   ユーザーが「OS データベース・オペレータ - コンピュータ」ウィンドウに表示されます。
7. 「OK」をクリックします。

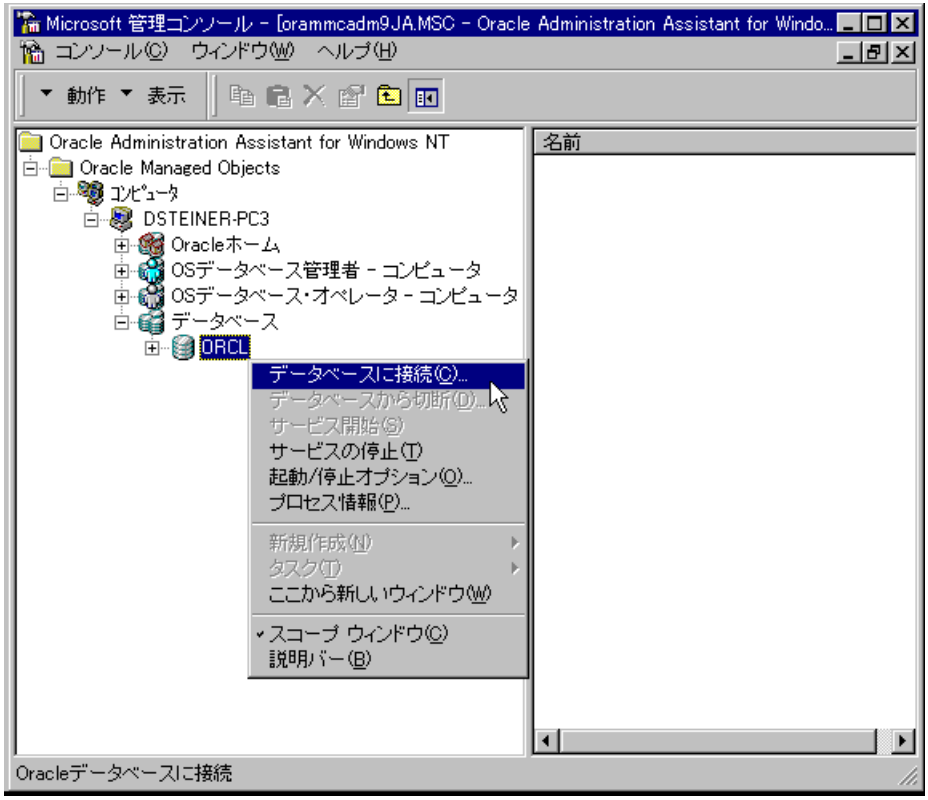
データベースへの接続

Oracle データベースへの接続時に SSL を使用可能にするには、Oracle Wallet Manager で作成された Wallet と同じユーザー・アカウントで **Oracle サービス**および**リスナー**・サービスを開始します。Windows NT の「サービス」ダイアログ・ボックスに表示されるデフォルトのユーザー・アカウントを使用しないでください。Oracle サービスおよびリスナー・サービスがデフォルトのユーザー・アカウントで開始されると、SSL は有効にならず、リスナーは起動しません。SSL のサポートは、Oracle Advanced Security の機能の 1 つです。また、Oracle Wallet Manager も Oracle Advanced Security の機能の 1 つです。

> **関連資料：** SSL サポートの詳細は、『Oracle Advanced Security 管理者ガイド』を参照してください。

データベースに接続するには、次のようにします。

1. Microsoft 管理コンソールのスコープ・ペインで、アクセスするデータベース・インスタンスを右クリックします。次に示す例では、ORCL へ接続します。



2. 「データベースに接続」を選択します。

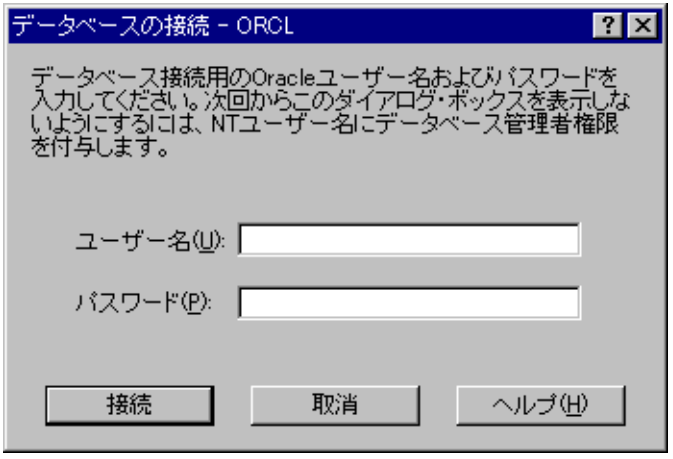
   Oracle データベースに接続すると、インスタンスの下に次のような Windows NT のノードが表示されます。これらのノードが表示されない場合は、そのインスタンスをダブルクリックしてください。

- 外部 OS ユーザー
- ローカル・ロール
- 外部 OS ロール
- OS データベース管理者
- OS データベース・オペレータ

接続に関する問題のトラブルシューティング

ローカル・コンピュータに接続する場合、Oracle Administration Assistant for Windows NT は、最初に Bequeath ネットワーク・プロトコルを使用して、SYSDBA としてデータベースに接続を試みます。リモート・コンピュータに接続する場合、Oracle Administration Assistant for Windows NT は TCP/IP ネットワーク・プロトコル（ポート番号 1521 または非推奨の 1526）で Windows のシステム固有の認証を使用して、SYSDBA としてデータベースに接続を試みます。正常に接続できない場合、1 つ以上のダイアログ・ボックスが表示され、データベースに接続するための情報を入力するよう要求されます。

次に示すダイアログ・ボックスは、Oracle データベースへの接続を試みるときに使用した Windows NT ドメイン・ユーザーが、SYSDBA 権限を持つ認証済のユーザーとして認識されていないために表示されます。データベースにアクセスするには、Oracle **ユーザー名**およびパスワードを入力します。このダイアログ・ボックスを再度表示しないようにするには、ドメイン・ユーザーを Windows NT オペレーティング・システムにより認証されたデータベース管理者として構成します。



次のダイアログ・ボックスは、リモートの Oracle データベースへの接続に TCP/IP ネットワーク・プロトコルを使用していないか、Oracle データベースが稼働していないために表示されます。TCP/IP 以外のプロトコル（たとえば Named Pipes など）を使用すると、リモート接続を試みるたびにこのダイアログ・ボックスが表示されます。

このダイアログ・ボックスを再度表示しないようにするには、TCP/IP プロトコルに変更して、データベースの **Oracle Net Services** リスナーが、デフォルト・ポートの 1521（または非推奨のデフォルト・ポートの 1526）でリスニングするように設定されていることを確認します。プロトコルを変更しないと、このダイアログ・ボックスが毎回表示されます。Oracle データベースが起動していることも確認します。

1. Oracle データベースに接続するための**ネット・サービス名**を入力します。ネット・サービス名は、選択する認証方式にかかわらず入力する必要があります。
2. Oracle ユーザー名およびパスワードを使用してデータベースにアクセスする場合は、「データベース認証」オプションを選択します。このユーザー名およびパスワードは、Oracle データベース内に存在し、SYSDBA 権限を持っている必要があります。
3. 現在ログインしている Windows NT ドメイン・ユーザーとしてデータベースにアクセスする場合は、「SYSDBA としての OS 認証接続」オプションを選択します。このドメイン・ユーザーは、SYSDBA 権限を持つ認証済のユーザーとして Windows NT で認識されている必要があります。認識されていない場合、ログインできません。

注意： Oracle Net Services には、新しい Trace Assistant ツールが用意されています。このツールを使用すると、既存のトレース・ファイル・テキストを読みやすい形式に変換し、接続の問題を診断できます。『Oracle9*i* Net Services 管理者ガイド』の「Trace Assistant を使用したトレース・ファイルの検証」を参照してください。

データベース認証用パラメータ設定の表示

データベース認証用パラメータ設定を表示するには、次のようにします。

1. データベース・インスタンス名を右クリックします。
2. 「プロパティ」を選択します。
3. 「*Instance* のプロパティ」ダイアログ・ボックスが表示され、次のパラメータ値が表示されます。
   - OS_AUTHENT_PREFIX
   - OS_ROLES

OS_AUTHENT_PREFIX は、init.ora ファイルのパラメータで、Windows NT ユーザー名およびパスワードを使用して Oracle データベースに接続を試みる外部ユーザーを認証します。このパラメータの値は、各ユーザーの Windows ユーザー名の先頭に付加されます。

デフォルトでは、このパラメータは Oracle9*i* データベースの作成中になし（""）に設定されます。したがって、frank という Windows ドメイン・ユーザー名は、ユーザー名 frank として認証されます。このパラメータを xyz に設定すると、Windows NT ドメイン・ユーザーの frank は、xyzfrank として認証されます。

OS_ROLES は、init.ora ファイルのパラメータで、true に設定すると、Windows NT オペレーティング・システムでデータベース・ユーザーの**外部ロール**の**認可**を管理できます。デフォルトでは、OS_ROLES は false に設定されています。外部ロールを作成する前に、OS_ROLES を true に設定し、Oracle データベースを再起動する必要があります。OS_ROLES が false に設定されている場合は、Oracle データベースがデータベース・ユーザーに対するロールの付与および取消しを管理します。

OS_ROLES が true に設定された状態で、Windows NT グローバル・グループに外部ロールを割り当てる場合、外部ロールはグローバル・グループ・レベルでのみ付与され、このグローバル・グループ内の個別のユーザー・レベルでは付与されません。つまり、このグローバル・グループ内の個々のユーザーに割り当てられた外部ロールは、後で「*External OS User* のプロパティ」ダイアログ・ボックスの「ロール」タブを使用して取り消したり編集したりすることはできません。このグローバル・グループ（つまり、すべての個別ユーザー）から外部ロールを取り消すには、かわりに「NT グローバル・グループへの外部 OS ロール割当て」ダイアログ・ボックスのフィールドを使用する必要があります。

個々のドメイン・ユーザーに割り当てられた外部ロール、または（OS_ROLES が false の状態で）個々のドメイン・ユーザーまたは Windows NT グローバル・グループに割り当てられた**ローカル・ロール**は、この影響を受けないため、編集または取消しが可能です。

OS_ROLES が true に設定されている場合は、どのデータベース・ユーザーに対してもデータベース内のローカル・ロールを付与できません。Windows NT を介してロールを付与する必要があります。詳細は、2-17 ページの「ローカル・データベース・ロールの作成」および 2-21 ページの「外部 OS ロールの作成」を参照してください。

外部 OS ユーザーの作成

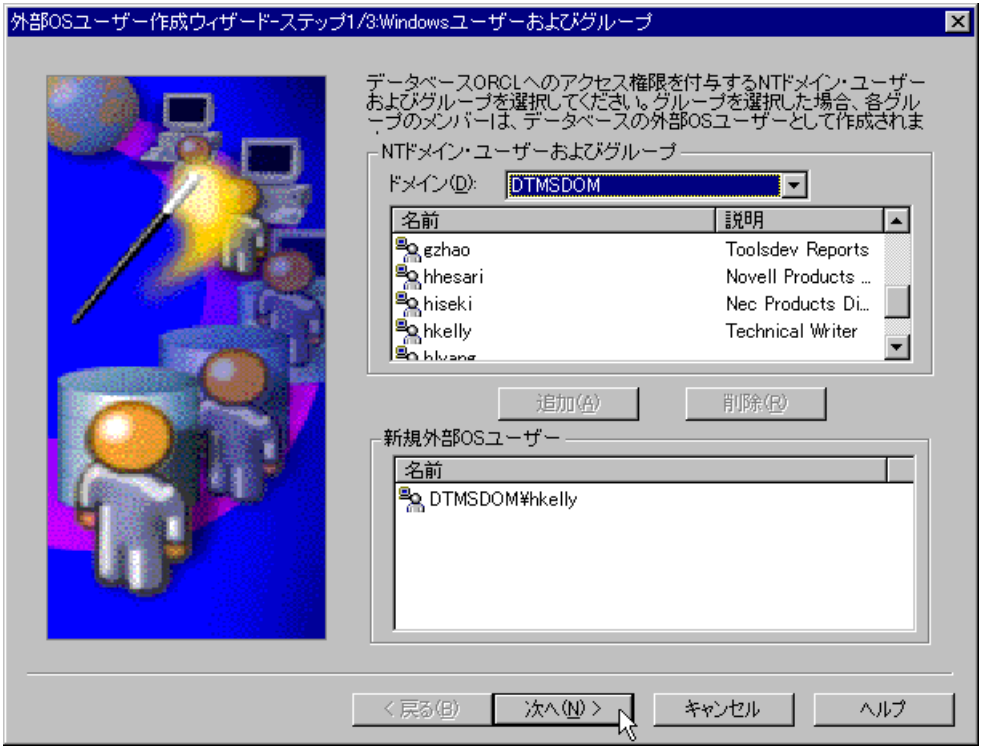
Oracle Administration Assistant for Windows NT の「外部 OS ユーザー」ノードにより、Windows NT ユーザーを認証し、パスワードを要求されずに外部ユーザーとして Oracle データベースにアクセスできます。外部ユーザーは、通常のデータベース・ユーザー（データベース管理者以外）であり、このユーザーに対しては標準のデータベース・ロール（CONNECT および RESOURCE など）を割り当てますが、SYSDBA（データベース管理者）権限または SYSOPER（データベース・オペレータ）権限は割り当てません。

外部 OS ユーザーを作成するには、次のようにします。

1. 2-8 ページの「データベースへの接続」の手順に従って、データベースに接続します。
2. 「外部 OS ユーザー」を右クリックします。コンテキスト・メニューが表示されます。

3. 「作成」を選択します。

   外部 OS ユーザー作成ウィザードが起動し、ウィザードのステップ 1 のダイアログ・ボックスが表示されます。ステップ 1 のダイアログ・ボックスは、「Windows ユーザーおよびグループ」です。



4. 「NT ドメイン・ユーザーおよびグループ」ボックスで、Windows NT ドメイン・ユーザーおよびグローバル・グループが含まれるドメインを選択します。
5. データベースへのアクセス権限を付与する Windows NT ドメイン・ユーザーおよびグローバル・グループを選択します。
6. 「追加」をクリックします。選択されたユーザーおよびグループが「新規外部 OS ユーザー」リスト・ボックスに表示されます。

7. 「次へ」をクリックします。「プロファイルと表領域」ダイアログ・ボックスが表示されます。

8. 「割当てプロファイル」ドロップダウン・リストで、新規外部ユーザー用プロファイルを選択します。プロファイルは、名前の付いたリソース制限のセットです。リソース制限が有効な場合、ユーザーのプロファイルでの定義に基づいて、データベースの使用およびインスタンスのリソースが制限されます。各ユーザーにプロファイルを割り当てることができます。また、特定のプロファイルを持たないすべてのユーザーに対してはデフォルト・プロファイルを割り当てることができます。

9. 「表領域の割当て制限」で、**表領域**をダブルクリックし、表領域の**割当て制限**を設定します。

10. 「次へ」をクリックします。「ロール」ダイアログ・ボックスが表示されます。

11. 「使用可能なロール」で、新規外部ユーザーに付与するデータベース・ロールを選択します。
12. 「付与」をクリックします。
13. 「完了」をクリックします。
14. 詳細を表示する外部ユーザーを右クリックし、「プロパティ」を選択します。

    割り当てられたプロパティが表示されます。

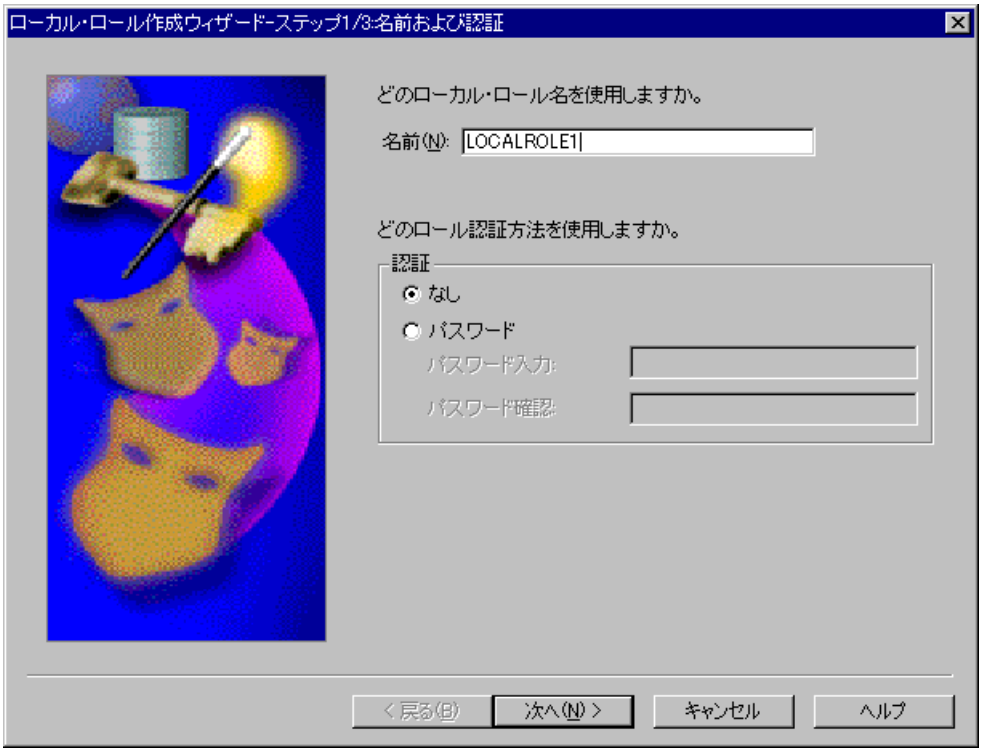
注意： Oracle Administration Assistant for Windows NT を使用した認証で Windows NT グローバル・グループを選択する場合、そのグループに現在含まれるすべてのユーザーが Oracle データベースに追加されます。後で、Windows NT のツールを使用してこの Windows NT グローバル・グループのユーザーを追加または削除しても、その更新は Oracle データベースに反映されません。新規に追加または削除するユーザーは、Oracle Administration Assistant for Windows NT を使用して、Oracle データベースに対して明示的に追加または削除する必要があります。

ローカル・データベース・ロールの作成

Oracle Administration Assistant for Windows NT の「ローカル・ロール」ノードにより、ロールを作成し、そのロールをデータベースで管理できます。一度ローカル・ロールを作成すると、データベース・ユーザーに対してそのロールを付与したり、取り消したりできます。ローカル・データベース・ロールを作成するには、次のようにします。

1. 2-8 ページの「データベースへの接続」の手順に従って、データベースに接続します。
2. ローカル・ロールを作成するデータベースの「ローカル・ロール」を右クリックします。
3. 「作成」を選択します。

   ローカル・ロール作成ウィザードが起動し、ウィザードのステップ 1 のダイアログ・ボックスが表示されます。ステップ 1 のダイアログ・ボックスは、「名前および認証」です。



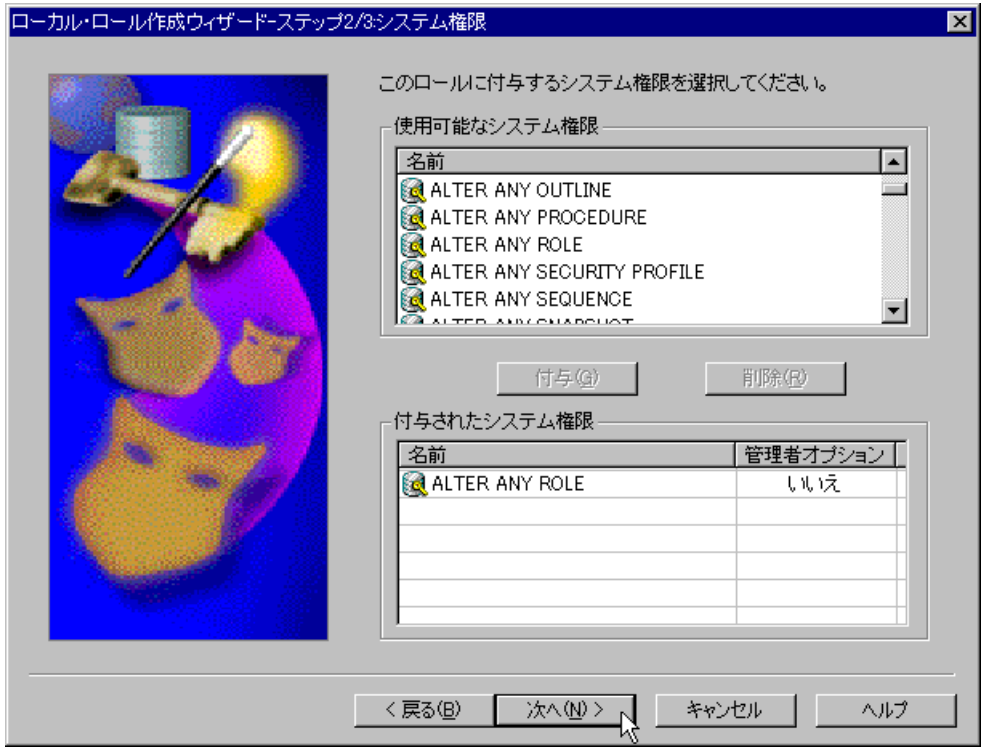
4. 使用するローカル・ロール名を入力します。
5. ユーザーがパスワードを入力せずにこのローカル・ロールを使用できるようにする場合は、「認証」で「なし」を選択します。

   パスワードでこのロールを保護する場合は、「パスワード」を選択します。これらのロールは、SET ROLE コマンドでパスワードを指定した場合にのみ使用できます。詳細は、『Oracle9*i* データベース管理者ガイド』を参照してください。

   このロールで使用するパスワードを入力します。

   確認のためにパスワードを再度入力します。

6. 「次へ」をクリックします。「システム権限」ダイアログ・ボックスが表示されます。



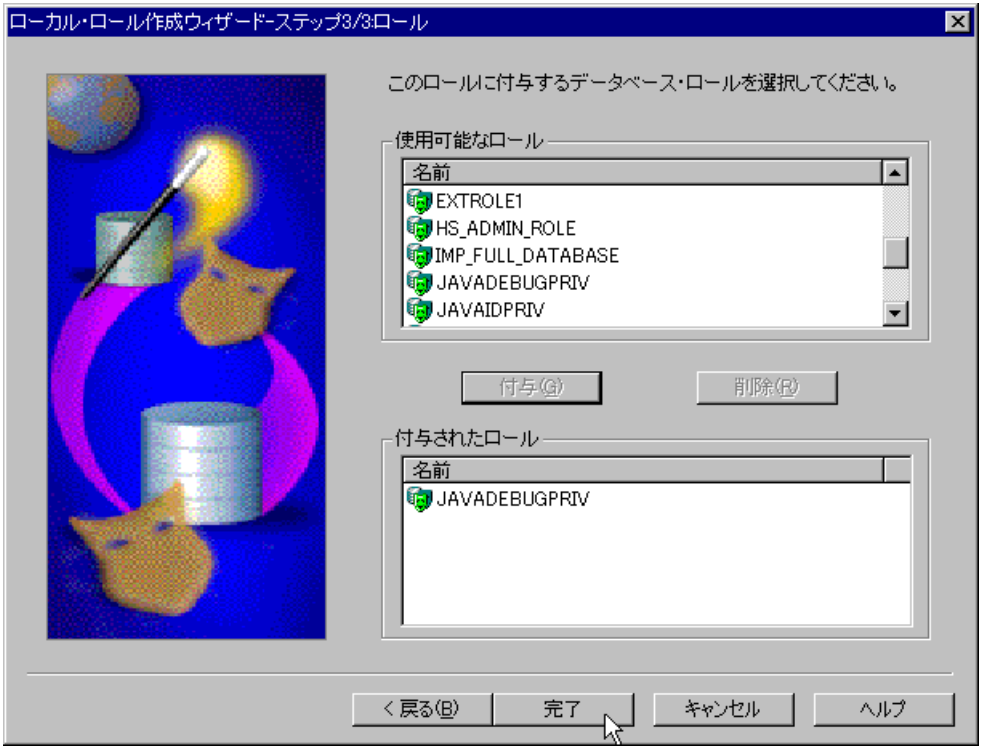
7. 「使用可能なシステム権限」で、ローカル・ロールに割り当てるシステム権限を選択します。

8. 「付与」をクリックして、選択したシステム権限をローカル・ロールに付与します。

   「付与されたシステム権限」フィールドに、ローカル・ロールに付与されたシステム権限のリストが表示されます。システム権限を取り消すには、その権限を選択して「削除」を選択します。

9. このロールに管理者オプションを付与するには、「管理者オプション」列の値をクリックして、リスト・ボックスを表示します。「はい」が選択できます。

10. 「次へ」をクリックします。「ロール」ダイアログ・ボックスが表示されます。



11. 「使用可能なロール」で、ローカル・ロールに割り当てるロールを選択します。ローカル・ロールおよび外部ロールの両方がこのリストに表示されます。

12. 「付与」をクリックして、ロールに選択したロールを付与します。

    「付与されたロール」フィールドに、ロールに付与されたロールのリストが表示されます。ローカル・ロールおよび外部ロールの両方がこのリストに表示されます。ロールを取り消すには、そのロールを選択して「削除」を選択します。

13. 「完了」をクリックします。

外部 OS ロールの作成

Oracle Administration Assistant for Windows NT の「外部 OS ロール」ノードにより、外部ロールを作成し、そのロールを Windows オペレーティング・システムで管理できます。一度外部ロールを作成すると、データベース・ユーザーに対してそのロールを付与したり、取り消したりできます。外部ロールを作成するには、次のようにします。

1. 2-8 ページの「データベースへの接続」の手順に従って、データベースに接続します。
2. 外部ロールを作成するデータベースの「外部 OS ロール」を右クリックします。
3. 「作成」を選択します。

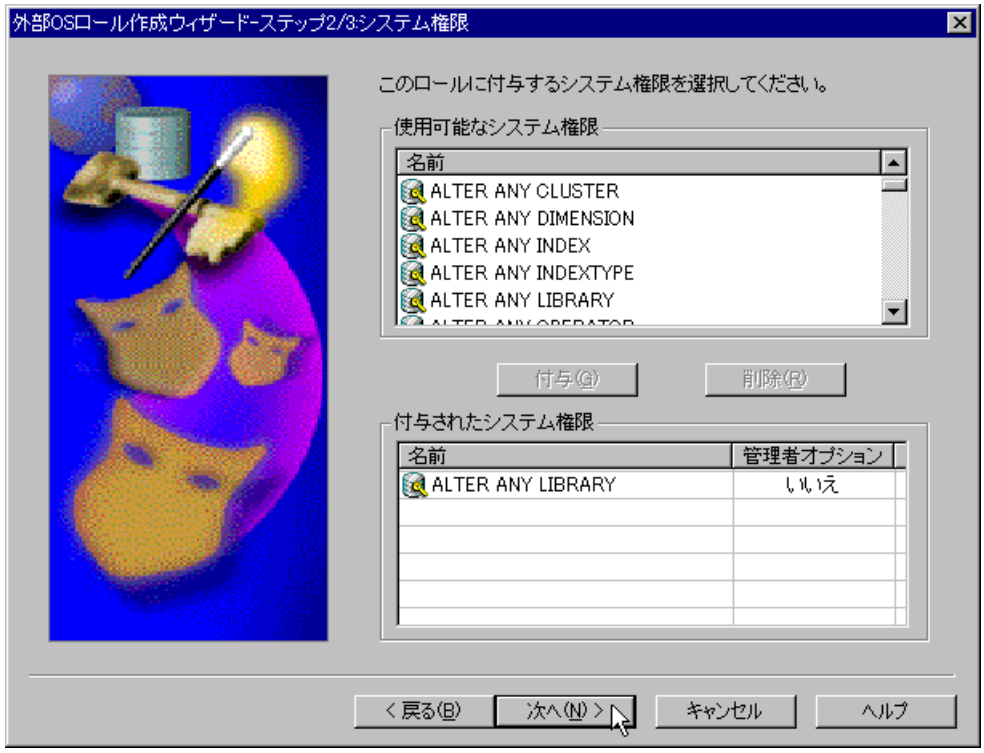
   外部 OS ロール作成ウィザードが起動し、ウィザードのステップ 1 のダイアログ・ボックスが表示されます。ステップ 1 のダイアログ・ボックスは、「名前」です。このダイアログ・ボックスには「認証 : 外部」と表示され、外部ロールのみを作成できることが示されます。

注意 : 外部 OS ロール作成ウィザードは、`init.ora` のパラメータ `OS_ROLES` が `true` に設定されている場合のみ使用できます。`false` に設定されている場合、最初に `true` に変更し、次に Oracle データベースを再起動します。

4. 使用する外部ロール名を入力します。外部ロールは、Windows オペレーティング・システムにより管理されるロールです。

5. 「次へ」をクリックします。

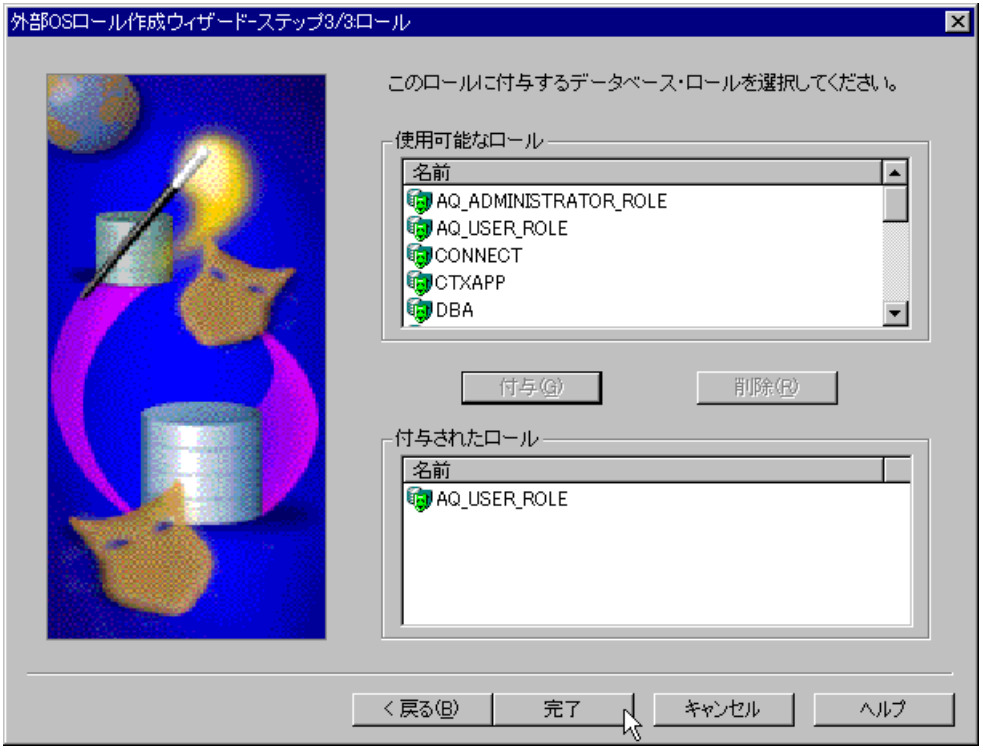
   「システム権限」ダイアログ・ボックスが表示されます。



6. 「使用可能なシステム権限」で、外部ロールに割り当てるシステム権限を選択します。
7. 「付与」を選択して、外部ロールに選択したシステム権限を付与します。
8. 「付与されたシステム権限」フィールドに、外部ロールに付与されたシステム権限のリストが表示されます。システム権限を取り消すには、その権限を選択して「削除」を選択します。
9. このロールに管理者オプションを付与するには、「管理者オプション」列の値をクリックして、リスト・ボックスを表示します。「はい」が選択できます。

10. 「次へ」をクリックします。

    「ロール」ダイアログ・ボックスが表示されます。



11. 「使用可能なロール」で、外部ロールに割り当てるロールを選択します。ローカル・ロールおよび外部ロールの両方がこのリストに表示されます。

12. 「付与」を選択して、外部ロールに選択したロールを付与します。

    「付与されたロール」フィールドに、外部ロールに付与されたロールのリストが表示されます。

13. 「完了」をクリックします。

単一データベースに対する管理者権限の付与

Oracle Administration Assistant for Windows NT の「OS データベース管理者」ノードにより、コンピュータ上の特定のインスタンスに対する SYSDBA 権限を持つ Windows NT ユーザーを認証できます。単一データベースに対する管理者（SYSDBA）権限を付与するには、次のようにします。

1. 2-8 ページの「データベースへの接続」の手順に従って、データベースに接続します。
2. 「OS データベース管理者」を右クリックします。
3. 「追加 / 削除」を選択します。

   「OS データベース管理者 : *instance*」ダイアログ・ボックスが表示されます。次に示す例では、インスタンスは ORCL です。

4. 「NT ドメイン・ユーザーおよびグループ」で、「ドメイン」ドロップダウン・リスト・ボックスから SYSDBA 権限を付与するユーザーのドメインを選択します。
5. ユーザーを選択します。

   ユーザーが「OS データベース管理者」フィールドに表示されます。
6. 「OK」をクリックします。

単一データベースに対するオペレータ権限の付与

Oracle Administration Assistant for Windows NT の「OS データベース・オペレータ」ノードにより、コンピュータ上の特定のインスタンスに対する SYSOPER 権限を持つ Windows NT ユーザーを認証できます。単一データベースに対するオペレータ（SYSOPER）権限を付与するには、次のようにします。

1. 2-8 ページの「データベースへの接続」の手順に従って、データベースに接続します。
2. 「OS データベース・オペレータ」を右クリックします。
3. 「追加 / 削除」を選択します。

   「OS データベース・オペレータ：*instance*」ダイアログ・ボックスが表示されます。次に示す例では、インスタンスは OFS1 です。

4. 「NT ドメイン・ユーザーおよびグループ」で、「ドメイン」ドロップダウン・リスト・ボックスから SYSOPER 権限を付与するユーザーのドメインを選択します。
5. ユーザーを選択します。
6. 「追加」をクリックします。

   ユーザーが「OS データベース・オペレータ」フィールドに表示されます。
7. 「OK」をクリックします。

外部ユーザーおよびロールの手動による管理

Oracle Administration Assistant for Windows NT を使用するかわりに、管理者、オペレータ、ユーザーおよびロールを手動で構成して、オペレーティング・システムに認証させることができます。手動による構成では、Oracle のコマンドライン・ツールを使用して、レジストリを編集し、Windows NT のユーザー マネージャでローカル・グループを作成します。次のものはすべて、Oracle データベースにパスワードなしでアクセスできるように手動で構成することができます。

- 外部 OS ユーザー
- Windows NT データベース管理者（SYSDBA 権限を持つ）
- Windows NT データベース・オペレータ（SYSOPER 権限を持つ）

また、ローカルおよび外部データベース・ロールを手動で作成し、Windows NT ドメイン・ユーザーおよびグローバル・グループに付与できます。

この項では、次の内容について説明します。

注意： 管理者、オペレータ、ユーザーおよびロールを手動で構成して、オペレーティング・システムに認証させる場合は、十分に注意する必要があります。できるかぎり、Oracle Administration Assistant for Windows NT を使用して構成手順を実行してください。

外部 OS ユーザーの手動による作成

この項では、Windows NT を使用して外部 OS ユーザー（データベース管理者以外）を認証し、パスワードなしでデータベースにアクセスできるようにする方法を説明します。Windows NT を使用して外部 OS ユーザーを認証する場合、データベースのユーザー名へのアクセス制限は、Windows NT にのみ依存します。

次の手順では、2 つの Windows NT ユーザー名が認証されます。

- ローカル・ユーザー `frank`
- ドメイン `sales` のドメイン・ユーザー `frank`

ローカル・ユーザー `frank` は、ローカルの Windows NT クライアント・コンピュータにログインし、Oracle9*i* データベースにアクセスします。データベースは、別のコンピュータにあっても構いません。他のコンピュータ上にある他のデータベースおよびリソースにアクセスする場合、ローカル・ユーザーは毎回ユーザー名およびパスワードを入力する必要があります。

ドメイン `sales` のドメイン・ユーザー `frank` は、多数の Windows NT 環境のコンピュータおよびリソースを含み、そのうちの 1 つに Oracle9*i* データベースがある `sales` ドメインにログインします。ドメイン・ユーザーは、ドメインのすべてのリソースに 1 つのユーザー名およびパスワードでアクセスできます。

手順には次の 2 つがあり、作業が実行されるコンピュータにより異なります。

- Oracle9i データベース・サーバーでの外部ユーザー認証タスク
- クライアント・コンピュータでの外部ユーザー認証タスク

Oracle9*i* データベース・サーバーでの外部ユーザー認証タスク

1. パラメータ `OS_AUTHENT_PREFIX` を `init.ora` ファイルに追加します。

   `OS_AUTHENT_PREFIX` の値は、オペレーティング・システムのユーザー名およびパスワードを使用してサーバーに接続を試みる、ローカルまたはドメインのユーザー名に接頭辞として付けられます。この接頭辞付きのユーザー名は、接続要求が試行された場合にデータベース内の Oracle ユーザー名と比較されます。クライアントからサーバーへの安全で信頼性の高い接続を実行するために、Windows のシステム固有の認証方式では、パラメータ `OS_AUTHENT_PREFIX` を使用することをお薦めします。

2. `OS_AUTHENT_PREFIX` の値を設定します。選択肢は次のとおりです。

   - 文字列

     たとえば、`xyz` と指定すると、Windows NT のユーザー名の先頭に、接頭辞として `xyz` が付きます（たとえば、ローカル・ユーザー `frank` は `xyzfrank` になり、ドメイン `sales` のドメイン・ユーザー `frank` は `xyzsales¥frank` になります）。文字列値には、大文字と小文字の区別がありません。

- ""（間にスペースのない 2 つの二重引用符）

  推奨値。この値を使用すると、Windows NT ユーザー名に接頭辞を付ける必要がなくなります（たとえば、ローカル・ユーザー frank は frank になり、ドメイン sales のドメイン・ユーザー frank は sales¥frank になります）。

- 値の指定なし

  OS_AUTHENT_PREFIX に値を指定しないと、デフォルトで OPS$ に設定されます（たとえば、ローカル・ユーザー frank は OPS$frank になり、ドメイン sales のドメイン・ユーザー frank は OPS$sales¥frank になります）。

3. ユーザー マネージャを使用して、frank に対する Windows NT のローカルまたはドメイン・ユーザー名を作成します（適切なユーザーが現在存在しない場合）。詳細は、Windows NT のドキュメントを参照してください。
4. 認証対象がドメイン名付きのユーザーではない場合（ドメイン sales の frank ではなく、単に frank の場合など）のみ、次の手順を実行します。それ以外の場合は、手順 5 に進みます。

   a. コマンド・プロンプトから、レジストリ エディタを起動します。

   ```
   C:¥> regedt32
   ```

   b. ¥HKEY_LOCAL_MACHINE¥SOFTWARE¥ORACLE¥HOME*ID* に移動します。ID は、編集する Oracle ホームの番号です。

   c. 「編集」→「値の追加」を選択します。

   「値の追加」ダイアログ・ボックスが表示されます。

   d. 「値の名前」フィールドに OSAUTH_PREFIX_DOMAIN と入力します。

   e. 「データ タイプ」ドロップダウン・リスト・ボックスで、REG_EXPAND_SZ を選択します。

f. 「OK」をクリックします。

「文字列エディタ」ダイアログ・ボックスが表示されます。

g. 「文字列」フィールドに `true` と入力し、ドメイン・レベルでの認証を可能にします。

ローカル・ユーザー `frank`、`sales` のドメイン・ユーザー `frank`、あるいはその他のドメインのドメイン・ユーザー `frank` など、ネットワーク上に複数の `frank` というユーザー名が存在する場合があります。`true` に設定すると、サーバーではそれぞれが区別されます。`false` に設定すると、ドメインは無視され、ローカル・ユーザー `frank` がオペレーティング・システム・ユーザーのデフォルト値になり、サーバーに返されます。

h. 「OK」をクリックします。

レジストリ エディタによりそのパラメータが追加されます。

i. 「レジストリ」メニューから「レジストリ エディタの終了」を選択します。

レジストリ エディタが終了します。

5. ファイル `sqlnet.ora` のパラメータ `SQLNET.AUTHENTICATION_SERVICES` に、`nts` が含まれていることを確認します。

6. SQL*Plus を起動します。

```
C:¥> sqlplus /NOLOG
```

7. **SYSTEM** データベース管理者（DBA）名でデータベースに接続します。

```
SQL> CONNECT
Enter user-name: SYSTEM/password
```

変更がなければ、`SYSTEM` のパスワードは、デフォルトでは `MANAGER` です。

8. 次のように入力して、ローカル外部ユーザーを作成します。

```
SQL> CREATE USER xyzfrank IDENTIFIED EXTERNALLY;
```

`xyz` は初期化パラメータ `OS_AUTHENT_PREFIX` に対して選択した値です。また、`frank` は Windows NT ローカル・ユーザー名です。

9. 次のように入力して、ローカル外部ユーザーにデータベース・ロールを付与します。

```
SQL> GRANT RESOURCE TO xyzfrank;
SQL> GRANT CONNECT TO xyzfrank;
```

10. 次のように入力して、ドメイン外部ユーザーを作成します。

```
SQL> CREATE USER "XYZSALES¥FRANK" IDENTIFIED EXTERNALLY;
```

XYZ は初期化パラメータ OS_AUTHENT_PREFIX に対して選択した値です。また、SALES¥FRANK はドメイン名および Windows NT ドメイン・ユーザー名です。二重引用符は必須で、構文はすべて英大文字で入力する必要があります。

11. 次のように入力して、ドメイン外部ユーザーにデータベース・ロールを付与します。

```
SQL> GRANT RESOURCE TO "XYZSALES¥FRANK";
SQL> GRANT CONNECT TO "XYZSALES¥FRANK";
```

二重引用符は必須で、構文はすべて英大文字で入力する必要があります。

12. SYSDBA 名でデータベースに接続します。

```
SQL> CONNECT / AS SYSDBA
```

13. データベースを停止します。

```
SQL> SHUTDOWN
```

14. データベースを再起動します。

```
SQL> STARTUP
```

これにより、OS_AUTHENT_PREFIX パラメータ値の変更が有効になります。

クライアント・コンピュータでの外部ユーザー認証タスク

1. Windows NT サーバー上にある同じユーザー名とパスワードで、Windows NT ローカル・ユーザー名またはドメイン・ユーザー名 frank を作成します（適切な名前が現在存在しない場合）。
2. ファイル sqlnet.ora のパラメータ SQLNET.AUTHENTICATION_SERVICES に、nts が含まれていることを確認します。
3. Oracle Net Configuration Assistant を使用して、クライアント・コンピュータから Oracle9*i* データベースがインストールされている Windows NT サーバーへのネットワーク接続を構成します。詳細は、『Oracle9*i* Net Services 管理者ガイド』を参照してください。
4. SQL*Plus を起動します。

```
C:¥> sqlplus /NOLOG
```

5. Windows NT サーバーに接続します。

```
SQL> CONNECT /@connect_identifier
```

connect_identifier は、Oracle9*i* データベースのネット・サービス名です。

Oracle9*i* データベースにより、Windows NT ローカル・ユーザー名またはドメイン・ユーザー名に対応する自動ログイン・ユーザー名が**データ・ディクショナリ**で検索および検証され、xyzfrank または xyzsales¥frank での接続が可能になります。

6. ローカル・ユーザーまたはドメイン・ユーザー frank で Oracle9*i* データベースに接続できたことは、「Oracle9i データベース・サーバーでの外部ユーザー認証タスク」の手順 9 または手順 11 で割り当てられたロールを参照することで確認できます。

```
SQL> SELECT * FROM USER_ROLE_PRIVS;
```

ローカル・ユーザー frank の出力

```
USERNAME                       GRANTED_ROLE                   ADM DEF OS_
------------------------------ ------------------------------ --- --- ---
XYZFRANK                       CONNECT                        NO  YES NO
XYZFRANK                       RESOURCE                       NO  YES NO
2 rows selected.
```

ドメイン・ユーザー frank の出力

```
USERNAME                       GRANTED_ROLE                   ADM DEF OS_
------------------------------ ------------------------------ --- --- ---
XYZSALES¥FRANK                 CONNECT                        NO  YES NO
XYZSALES¥FRANK                 RESOURCE                       NO  YES NO
2 rows selected.
```

Oracle9*i* ユーザー名は、xyzfrank または xyzsales¥frank であるため、xyzfrank または xyzsales¥frank により作成されるすべてのオブジェクト（表、**ビュー**、索引など）には、この名前が接頭辞として付きます。たとえば、別のユーザーが xyzfrank の所有する表 shark を参照するには、次のように入力する必要があります。

```
SQL> SELECT * FROM xyzfrank.shark
```

注意： 自動認証機能は、すべての **Oracle Net** プロトコルでサポートされています。

複数のデータベースに対する管理者権限およびオペレータ権限の手動による付与

この項では、Windows NT により、データベース管理者（SYSDBA）権限およびデータベース・オペレータ（SYSOPER）権限を、データベース管理者に対して付与する方法を説明します。この権限が付与されると、データベース管理者はクライアント・コンピュータから次のコマンドを発行し、パスワードなしで Oracle9*i* データベースに接続できます。

```
CONNECT / AS SYSOPER
CONNECT / AS SYSDBA
```

この機能を使用可能にするには、データベース管理者の Windows NT ローカル・ユーザー名またはドメイン・ユーザー名が、表 2-1 にリストされた Windows NT ローカル・グループのいずれかに属している必要があります。

表 2-1　SYSDBA 権限および SYSOPER 権限を持つ Windows NT ローカル・グループ

ローカル・グループ	権限
ORA_OPER	コンピュータ上のすべてのデータベースに対する SYSOPER 権限
ORA_DBA[1]	コンピュータ上のすべてのデータベースに対する SYSDBA 権限
ORA_*SID*_OPER	単一データベースに対する SYSOPER 権限（*SID* により識別）
ORA_*SID*_DBA	単一データベースに対する SYSDBA 権限（*SID* により識別）

[1] ORA_DBA はインストール中に自動的に作成されます。詳細は、1-8 ページの「インストール時に使用可能になるオペレーティング・システムの認証」を参照してください。

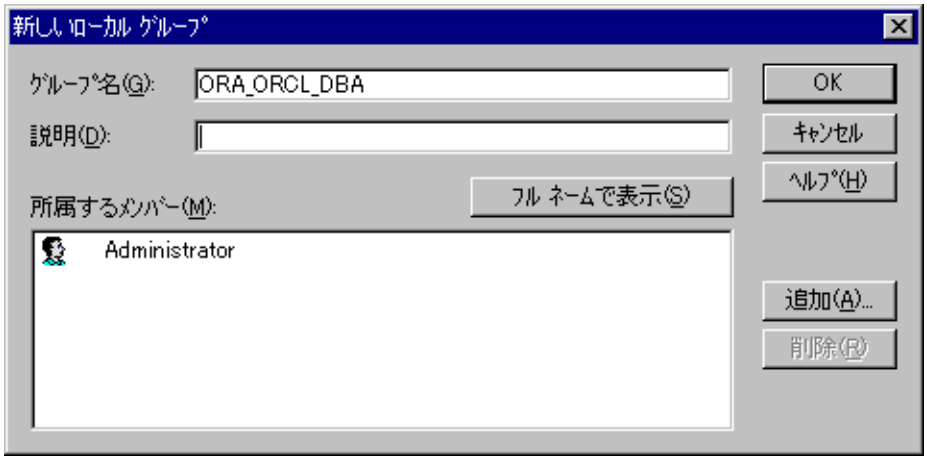
データベース管理者が SYSOPER または SYSDBA としてパスワードなしで接続できるように手動で設定する手順には次の 2 つがあり、作業が実行されるコンピュータにより異なります。

- Oracle9i データベース・サーバーでの SYSDBA または SYSOPER 認証タスク
- クライアント・コンピュータでの SYSDBA または SYSOPER 認証タスク

Oracle9*i* データベース・サーバーでの SYSDBA または SYSOPER 認証タスク

1. Oracle9*i* データベースがインストールされている Windows NT サーバーでユーザー マネージャを開きます。
2. 「ユーザー」メニューから「新しいローカル グループ」を選択します。

   「新しいローカル グループ」ダイアログ・ボックスが表示されます。



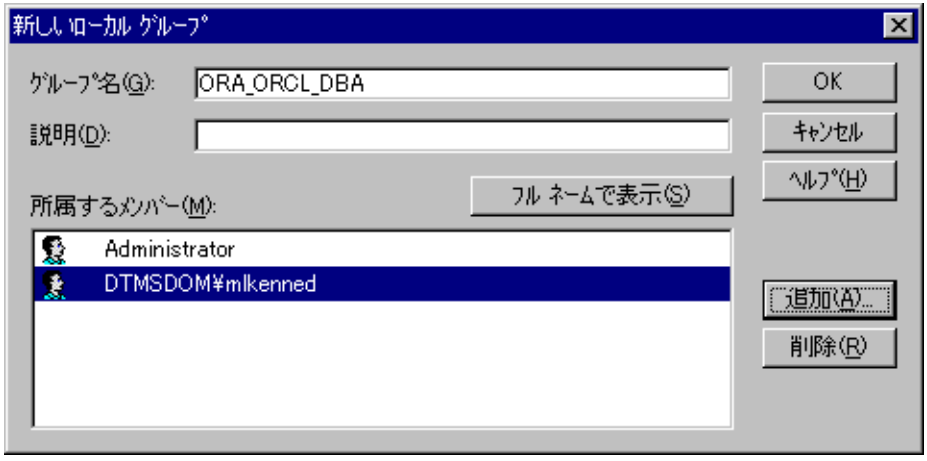
3. 「グループ名」フィールドに新規の Windows NT ローカル・グループに対して選択した名前を入力します。この例では、ORCL という **SID** のデータベースに対する SYSDBA 権限をもつローカル・グループ名を入力します。

4. 「追加」をクリックします。「ユーザーとグループの追加」ダイアログ・ボックスが表示されます。

5. 「名前」フィールドから 1 つ以上の Windows NT ユーザーを選択し、「追加」を選択します。

6. 「OK」をクリックします。

   選択内容が、「新しいローカル グループ」ダイアログ・ボックスの「所属するメンバー」フィールドに追加されます。



7. 「OK」をクリックします。
8. ユーザー マネージャを終了します。
9. ファイル `sqlnet.ora` のパラメータ `SQLNET.AUTHENTICATION_SERVICES` に、`nts` が含まれていることを確認します。
10. コマンド・プロンプトから、レジストリ エディタを起動します。

    ```
    C:¥>regedt32
    ```

11. `¥HKEY_LOCAL_MACHINE¥SOFTWARE¥ORACLE¥HOME`*ID* に移動します。

    ID は編集する Oracle ホームの番号です。

12. パラメータ `OSAUTH_PREFIX_DOMAIN` を `true` に設定します。

クライアント・コンピュータでの SYSDBA または SYSOPER 認証タスク

1. Windows NT サーバー上にある同じユーザー名とパスワードで、Windows NT ローカル・ユーザー名またはドメイン・ユーザー名を作成します（適切なユーザー名が現在存在しない場合）。
2. ファイル sqlnet.ora のパラメータ SQLNET.AUTHENTICATION_SERVICES に、nts が含まれていることを確認します。
3. Oracle Net Configuration Assistant を使用して、クライアント・コンピュータから Oracle9*i* データベースがインストールされている Windows NT サーバーへのネットワーク接続を構成します。詳細は、『Oracle9*i* Net Services 管理者ガイド』を参照してください。
4. SQL*Plus を起動します。

   ```
   C:¥> sqlplus /NOLOG
   ```

5. Oracle9*i* データベースに接続します。

   ```
   SQL> SET INSTANCE net_service_name
   ```

   net_service_name は、Oracle9*i* データベースの Oracle Net ネット・サービス名です。

6. 「Oracle9i データベース・サーバーでの SYSDBA または SYSOPER 認証タスク」の手順 3 で ORA_DBA または ORA_SID_DBA を指定した場合、次のいずれかを入力します。

   ```
   SQL> CONNECT / AS SYSOPER
   SQL> CONNECT / AS SYSDBA
   ```

   手順 3 で ORA_OPER または ORA_*SID*_OPER を指定した場合、次のように入力します。

   ```
   SQL> CONNECT / AS SYSOPER
   ```

   これで、Windows NT サーバーに接続されます。SYSDBA で接続すると、DBA 権限が付与されます。

外部ロールの手動による作成

この項では、Windows NT で Oracle9*i* データベース・ロール（外部ロールとも呼ぶ）をユーザーに直接付与する方法を説明します。Windows NT を使用してユーザーを認証する場合、Windows NT ローカル・グループによりこれらのユーザーに外部ロールを付与できます。ユーザー マネージャを使用して、ユーザーに対して外部ロールの作成、付与または取消しを実行できます。

ユーザーが接続すると、これらのロールに対するすべての権限がアクティブになります。外部ロールを使用する場合、すべてのロールはオペレーティング・システムを介して付与および管理されます。外部ロールおよび Oracle ロールの両方を同時に使用することはできません。

次の例を考えてみます。外部ロールを使用可能にし、ドメイン・ユーザー名 sales¥frank（sales はドメイン名、frank はドメイン・ユーザー名）で Windows NT ドメインにログインします。次に、Oracle データベース・ユーザー scott として、Oracle9*i* データベースに接続します。この場合、sales¥frank に付与されたロールは割り当てられますが、scott に付与されたロールは割り当てられません。

外部ロールを手動で作成する手順には次の 2 つがあり、認証タスクが実行されるコンピュータにより異なります。

- Oracle9i データベース・サーバーでの外部ロール認証タスク
- クライアント・コンピュータでの外部ロール認証タスク

Oracle9*i* データベース・サーバーでの外部ロール認証タスク

1. 初期化パラメータ OS_ROLES を init.ora ファイルに追加します。
2. OS_ROLES を true に設定します。

   デフォルトの設定では、このパラメータは false です。
3. ファイル sqlnet.ora のパラメータ SQLNET.AUTHENTICATION_SERVICES に、nts が含まれていることを確認します。
4. SQL*Plus を起動します。

   ```
   C:¥> sqlplus /NOLOG
   ```
5. Windows NT サーバーに接続します。

   ```
   SQL> CONNECT / AS SYSDBA
   ```
6. 新規のデータベース・ロールを作成します。この新規のロールにはどのような名前でも指定できます。次の例では、DBSALES3 というロール名を使用します。

   ```
   SQL> CREATE ROLE DBSALES3 IDENTIFIED EXTERNALLY;
   ```
7. データベース環境に対応する Oracle ロールを DBSALES3 に付与します。

   ```
   SQL> GRANT DBA TO DBSALES3 WITH ADMIN OPTION;
   SQL> GRANT RESOURCE TO DBSALES3 WITH ADMIN OPTION;
   SQL> GRANT CONNECT TO DBSALES3 WITH ADMIN OPTION;
   ```
8. SYSDBA でデータベースに接続します。

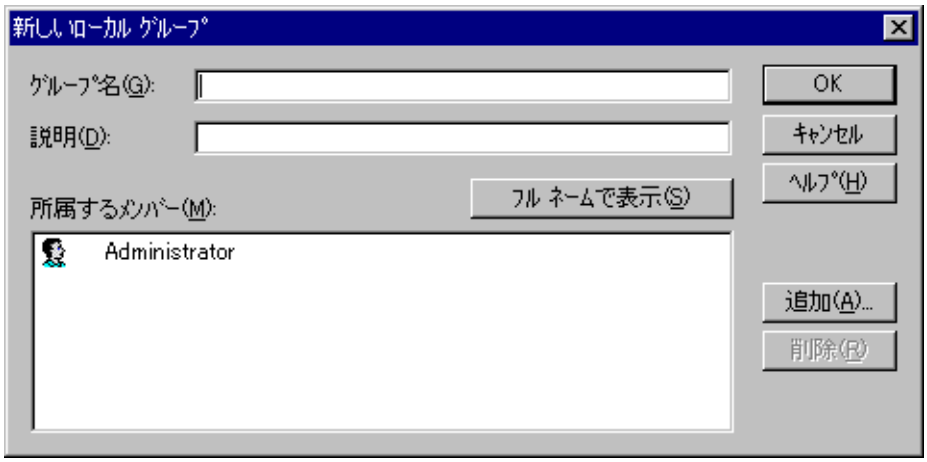
   ```
   SQL> CONNECT / AS SYSDBA
   ```
9. データベースを停止します。

   ```
   SQL> SHUTDOWN
   ```
10. データベースを再起動します。

    ```
    SQL> STARTUP
    ```

11. Windows NT のユーザー マネージャを開きます。
12. 「ユーザー」メニューから「新しいローカル グループ」を選択します。

    「新しいローカル グループ」ダイアログ・ボックスが表示されます。



13. 「グループ名」フィールドに、データベース・ロールに対応する Windows NT ローカル・グループ名を次の構文で入力します。

    ORA_*sid_rolename* [_D] [_A]

    それぞれの要素は次のとおりです。

    - *sid* は、データベース・インスタンスを示します。
    - *rolename* は、付与されるデータベース・ロールを示します。
    - D は、このデータベース・ロールをデータベース・ユーザーのデフォルト・ロールにすることを示します。
    - A は、このデータベース・ロールが ADMIN OPTION を含むことを示します。

    文字 D および A はオプションです。指定する場合は、これらの文字の前にアンダースコアが必要です。

    この例では、ORA_orcl_dbsales3_D と入力します。

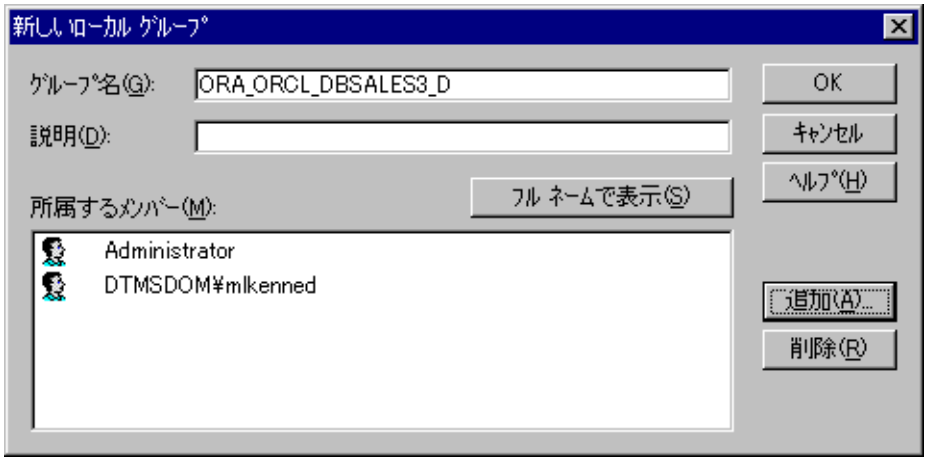
14. 「追加」をクリックします。

「ユーザーとグループの追加」ダイアログ・ボックスが表示されます。

15. 追加する Windows NT ローカル・ユーザー名またはドメイン・ユーザー名を選択し、「追加」をクリックします。

16. 「OK」をクリックします。

選択内容が、「新しいローカル グループ」ダイアログ・ボックスの「所属するメンバー」フィールドに追加されます。



複数のデータベース・ロールを作成し、次の表に示すように、それぞれ異なるオプションで複数の Windows NT グループに付与できます。ORCL インスタンスに接続し、Windows NT により次の 4 つの Windows NT ローカル・グループすべてのメンバーとして認証されたユーザーは、デフォルトで dbsales3 および dbsales4 に関連付けられた権限を付与されます（オプション _D が指定されているためです）。このようなユーザーが最初に dbsales3 または dbsales4 のメンバーとして接続し、SET ROLE コマンドを使用すると、データベース・ロール dbsales1 および dbsales2 にもアクセスできます。ただし、ユーザーが最初にデフォルトのロールで接続せずに、dbsales1 または dbsales2 で接続を試みても、接続できません。また、このようなユーザーは、dbsales2 および dbsales4 をその他のロールに付与できます（オプション _A が指定されているためです）。

データベース・ロール	Windows NT グループ
dbsales1	ORA_ORCL_dbsales1
dbsales2	ORA_ORCL_dbsales2_a
dbsales3	ORA_ORCL_dbsales3_d
dbsales4	ORA_ORCL_dbsales4_da

注意： Oracle9*i* データベースでグループ名がロール名に変換されるとき、名前は大文字に変換されます。

17. 「OK」をクリックします。
18. ユーザー マネージャを終了します。

クライアント・コンピュータでの外部ロール認証タスク

1. Windows NT サーバー上にある同じユーザー名とパスワードで、Windows NT ローカル・ユーザー名またはドメイン・ユーザー名を作成します（適切なユーザー名が現在存在しない場合）。
2. ファイル `sqlnet.ora` のパラメータ `SQLNET.AUTHENTICATION_SERVICES` に、`nts` が含まれていることを確認します。
3. Oracle Net Configuration Assistant を使用して、クライアント・コンピュータから Oracle9*i* データベースへのネットワーク接続を構成します。詳細は、『Oracle9*i* Net Services 管理者ガイド』を参照してください。
4. SQL*Plus を起動します。

   ```
   C:¥> sqlplus /NOLOG
   ```

5. 正しいインスタンスに接続します。

   ```
   SQL> SET INSTANCE connect_identifier
   ```

   connect_identifier は、手順 3 で作成した、Oracle9*i* データベース接続のネット・サービス名です。

6. Oracle9*i* データベースに接続します。

   ```
   SQL> CONNECT scott/tiger AS SYSDBA
   ```

   これで、Net Services を使用して、Oracle ユーザー名 `scott/tiger` で Windows NT サーバーに接続されます。Oracle ユーザー名 `scott` に適用されるロールは、すでにデータベース・ロールにマップされた Windows NT ユーザー名に対して定義されるすべてのロールで構成されます（この例では、`ORA_DBSALES3_D`）。認証された接続で使用可能なすべてのロールは、Windows NT ユーザー名、およびユーザーが属している Oracle 固有の Windows NT ローカル・グループ（`ORA_`*SID*`_DBSALES1` または `ORA_`*SID*`_DBSALES4_DA` など）により決定されます。

注意： OSDBA および OSOPER は、2 つの特別なオペレーティング・システム・グループの汎用名で、オペレーティング・システムの認証を使用する場合にデータベース管理者のログインを制御します。Windows NT では、OSDBA および OSOPER がユーザー マネージャのローカル・グループにマップされます。OSDBA および OSOPER の Windows NT 固有の名前は、2-34 ページの「複数のデータベースに対する管理者権限およびオペレータ権限の手動による付与」に記載しています。OSDBA および OSOPER の詳細は、『Oracle9*i* データベース管理者ガイド』を参照してください。

ユーザーの手動による移行

ローカル・ユーザーまたは外部ユーザーは、User Migration Utility を使用してエンタープライズ・ユーザーに移行できます。データベース・ユーザー・モデルからエンタープライズ・ユーザー・モデルに移行することで、企業の環境における管理、セキュリティおよびユーザビリティの問題への解決策が提供されます。エンタープライズ・ユーザー・モデルでは、すべてのユーザー情報が LDAP ディレクトリ・サービスに移動されるため、次のような利点があります。

- ユーザー情報の一元的な格納および管理
- ユーザー認証の一元管理
- セキュリティの拡張

User Migration Utility はコマンドライン・ツールです。次のような形式の構文です。

```
C:¥ umu parameters
```

User Migration Utility パラメータのリストを取得するには、次のように入力します。

```
C:¥ umu help=yes
```

関連資料： User Migration Utility の詳細は、『Oracle Advanced Security 管理者ガイド』の第 16 章を参照してください。

3

エンタープライズ・ユーザーおよびロールの管理

Oracle Enterprise Security Manager を使用して、エンタープライズ・ユーザー、ロールおよびドメインを作成および管理します。Oracle Enterprise Security Manager は、Oracle Enterprise Manager のコンソールの統合アプリケーションです。Oracle Enterprise Security Manager の使用方法の詳細は、『Oracle Advanced Security 管理者ガイド』を参照してください。

この章の項目は次のとおりです。

注意： Windows 2000 ドメインで**外部ユーザー**および**外部ロール**を管理できますが、この管理には Oracle Enterprise Security Manager は使用できません。外部ユーザーおよび外部ロールを管理する場合に使用可能なツールの詳細は、第 2 章「外部ユーザーおよびロールの管理」を参照してください。

エンタープライズ・ユーザーの認証

エンタープライズ・ユーザーは、ディレクトリ・サーバー（Oracle Internet Directory または Active Directory など）で作成および一元管理されます。複数のデータベースに対するアクセスを可能にするには、エンタープライズ・ユーザーを各データベースで外部ユーザーとして定義する必要があります。

たとえば、`sales` および `marketing` という 2 つのデータベースにアクセスする必要のある**エンタープライズ・ユーザー**（`cn=joe,cn=users,dc=acme,dc=com`）がいるとします。このエンタープライズ・ユーザーは、両方のデータベースで外部ユーザーとして定義する必要があります。

ユーザーのほとんどは、通常、データベースのアプリケーション・スキーマにアクセスするだけですので、独自のスキーマを必要としません。Oracle9*i* では、Oracle Enterprise Security Manager を使用してデータベースに共有**スキーマ**を 1 つ作成し、ディレクトリ・サーバーの複数のエンタープライズ・ユーザーをこの共有スキーマにマップできます。これは、多数のユーザーが同時に 1 つのアプリケーションにアクセスするインターネット環境では特に便利です。1 つの共有スキーマがあれば、ユーザーごとに異なるスキーマを作成する必要はありません。

> **関連資料：** 詳細は、『Oracle Advanced Security 管理者ガイド』を参照してください。

次のような場合、エンタープライズ・ユーザー認証は使用可能です。

- **レジストリ**・パラメータ `OSAUTH_X509_NAME` を `true` に設定する場合。（詳細は、1-6 ページの「Active Directory と Oracle9i の統合」を参照。）
- Windows 2000 ドメインで Oracle9*i* データベースを操作する場合。
- Oracle Enterprise Security Manager を使用する場合。共有スキーマを使用する場合は、Oracle Enterprise Security Manager を使用して、複数のエンタープライズ・ユーザーをこの共有スキーマにマップします。

Kerberos 認証プロトコルは、Windows と Oracle のリリースの組合せが 1-3 ページの表 1-1「Kerberos 認証プロトコルが使用可能なソフトウェア要件」にリストされたものと一致する場合に使用されます。一致しない場合は、NTLM が使用されます。

エンタープライズ・ロールの認可

エンタープライズ・ユーザーには、**エンタープライズ・ロール**が 1 つ割り当てられる場合もありますが、複数割り当てられる場合もあります。エンタープライズ・ロールの**認可**は、Oracle8*i* リリース 8.1.6 以上でサポートされます。エンタープライズ・ロールは、Oracle Enterprise Security Manager を使用してディレクトリ・サーバーに作成される単一の**ロール**です。Oracle Enterprise Security Manager を使用して、複数のデータベースにあるグローバル・ロールおよびグループを、1 つのエンタープライズ・ロールに割り当てます。**グローバル・ロール**は、各 Oracle9*i* データベースで個別に作成する必要があります。

たとえば、エンタープライズ・ユーザーに人事管理データベースのエンタープライズ・ロール HR（グローバル・ロール HR `user` を含む）を割り当てることができます。また、企業情報データベースのグローバル・ロール `employee` を割り当てることもできます。職種が変わった場合、ディレクトリでエンタープライズ・ロールの割当てを変更するだけで、企業全体の複数のデータベースで権限を変更できます。また、管理者は、各ユーザーの権限を個別に更新する必要はなく、エンタープライズ・ロールに機能を追加したり、**権限**を削除したりできます。

エンタープライズ・ロールは、ロールが割り当てられたユーザーが地理的に多数の場所に存在しており、複数のデータベースにアクセスする必要がある場合に使用します。

> **関連資料：** Oracle Enterprise Security Manager を使用してディレクトリ・サーバーにエンタープライズ・ロールを作成および格納する方法の詳細は、『Oracle Advanced Security 管理者ガイド』を参照してください。

エンタープライズ・ユーザーに許可されるアクセス権は、グローバル・ロールに含まれるエンタープライズ・ロールに対して許可されます。

ユーザーは、Windows 2000 **グローバル・グループ**および**ユニバーサル・グループ**に所属できます。Oracle Enterprise Security Manager を使用して、エンタープライズ・ロールにこれらのグループを割り当てることができます。

注意： エンタープライズ・ロールは、ディレクトリ・サーバーにより認可されますが、初期化ファイルのパラメータ `OS_ROLES` を `true` に設定しても（**外部ロール**認可を使用可能にする方法）認可されません。

4

Oracle Wallet の Windows レジストリへの格納

この章では、Windows レジストリにおける Oracle Wallet の格納および取得について説明します。

この章の項目は次のとおりです。

秘密鍵およびトラスト・ポイントの格納

Oracle Wallet では、認証および**暗号化**のために公開鍵アプリケーションで使用される**秘密鍵**、**トラスト・ポイント**および**デジタル証明**が格納されます。Oracle Wallet Manager は、Oracle Wallet を作成および管理します。Oracle Enterprise Login Assistant は、**不明瞭化**された Wallet を作成するために使用します。Oracle 公開鍵アプリケーションでは、認証および暗号化のために不明瞭化された Oracle Wallet を使用します。Oracle Enterprise Login Assistant を使用して各セッションに一度ログインすると、ログアウトするまで、すべてのアプリケーションは同じ不明瞭化された Wallet を使用して**認証**を行います。暗号化および不明瞭化された Oracle Wallet は、ファイル・システムまたは Windows レジストリのユーザー・プロファイル領域に格納できます。

注意： Oracle Wallet Manager、Oracle Enterprise Login Assistant およびこの両方に関連する機能は、Oracle Advanced Security の機能で、Oracle9*i* データベースには含まれないライセンス・オプションです。

ユーザー・プロファイルの格納

Windows 2000 または Windows NT 4.0 のドメインでは、ユーザー・プロファイルはローカル・コンピュータに格納されます。ローカル・ユーザーがログインすると、ローカル・コンピュータのユーザー・プロファイルが、そのコンピュータのレジストリのユーザー・プロファイルにアップロードされます。ユーザーがログアウトすると、ローカル・ファイル・システムに格納されたユーザー・プロファイルが更新され、ドメイン・ユーザーまたはローカル・ユーザーは常に最新バージョンのユーザー・プロファイルを保持できます。

Wallet 格納用レジストリ・パラメータ

ファイル `sqlnet.ora` のパラメータ `WALLET_LOCATION` で、Oracle Wallet をファイル・システムに格納するか、次のレジストリのユーザー・プロファイル領域に格納するかを指定します。

```
¥HKEY_CURRENT_USER¥SOFTWARE¥ORACLE¥WALLETS
```

これにより、暗号化された、または不明瞭化された Oracle Wallet の場所も指定されます。Wallet は、ファイル・システムと同じフォーマットで格納されます。Wallet の機能は、その配置されている場所以外はすべて同じです。

たとえば、次の場所にあるレジストリに Oracle Wallet を格納するとします。

```
¥HKEY_CURRENT_USER¥SOFTWARE¥ORACLE¥WALLETS¥SALESAPP
```

この場合、`WALLET_LOCATION` パラメータは次のようになります。

```
WALLET_LOCATION =  (SOURCE= (METHOD=REG) (METHOD_DATA= (KEY=SALESAPP)))
```

さらに、暗号化された Oracle Wallet は次の場所にあるレジストリに格納されます。

```
¥HKEY_CURRENT_USER¥SOFTWARE¥ORACLE¥WALLETS¥SALESAPP¥EWALLET.P12
```

また、不明瞭化された Oracle Wallet は次の場所に格納されます。

```
¥HKEY_CURRENT_USER¥SOFTWARE¥ORACLE¥WALLETS¥SALESAPP¥CWALLET.SSO
```

Oracle Wallet Manager

Oracle Wallet Manager は、Oracle Wallet を作成および管理します。Oracle Wallet に Windows レジストリを使用する場合、「ファイル」メニューの「Windows レジストリを使用」チェックボックスを選択する必要があります。「Windows レジストリを使用」チェックボックスが選択されている場合、ツールにより、Wallet を開いたり、新規の Wallet を保存するときに既存のキーのリストが表示されます。このリストは、次の場所にあります。

```
¥HKEY_CURRENT_USER¥SOFTWARE¥ORACLE¥WALLETS
```

既存の場所の 1 つを選択するか、新規の場所（レジストリ・キー）の名前を入力できます。たとえば、key1 という名前の新規のキーを入力すると、ツールにより次のレジストリ・キーが作成されます。

```
¥HKEY_CURRENT_USER¥SOFTWARE¥ORACLE¥WALLETS¥KEY1
```

暗号化された Wallet は、次の場所に格納されます。

```
¥HKEY_CURRENT_USER¥SOFTWARE¥ORACLE¥WALLETS¥KEY1¥EWALLET.P12
```

不明瞭化された Wallet は、次の場所に格納されます。

```
¥HKEY_CURRENT_USER¥SOFTWARE¥ORACLE¥WALLETS¥KEY1¥CWALLET.SSO
```

「Windows レジストリを使用」チェックボックスが選択されていない場合、ツールによりローカル・コンピュータのすべての使用可能なドライブおよびディレクトリが表示されます。既存のディレクトリの 1 つを選択するか、新規のディレクトリを入力できます。選択したディレクトリに暗号化された、または不明瞭化された Wallet が格納されます。そのディレクトリがない場合は作成されます。

Oracle Enterprise Login Assistant

Oracle Enterprise Login Assistant を起動すると、最初に、レジストリの次の場所で不明瞭化された Wallet が検索されます。

```
¥HKEY_CURRENT_USER¥SOFTWARE¥ORACLE¥WALLETS¥DEFAULT
```

レジストリで不明瞭化された Wallet が見つからない場合、ファイル・システムの次の場所で不明瞭化された Wallet が検索されます。

```
%USERPROFILE%¥ORACLE¥WALLETS
```

不明瞭化された Wallet がどちらかの場所で見つかると、Oracle Enterprise Login Assistant により自動ログインできたことを伝えるメッセージが返されます。このとき「ログアウト」を選択すると、不明瞭化された Wallet が、見つかった場所（つまり、レジストリまたはファイル・システムのデフォルトの場所）から削除されます。「ログアウト」を選択せずにツールを終了すると、不明瞭化された Wallet は見つかった場所に残ります。

レジストリまたはファイル・システムのデフォルトの場所で不明瞭化された Wallet が見つからない場合、Oracle Enterprise Login Assistant により自動ログインできないことを伝えるメッセージが表示されます。

自動ログインできなくても「ログイン」を選択すれば、Oracle Enterprise Login Assistant では、レジストリの次の場所で暗号化された Wallet が検索されます。

```
¥HKEY_CURRENT_USER¥SOFTWARE¥ORACLE¥WALLETS¥DEFAULT
```

レジストリで暗号化された Wallet が見つからない場合、ローカル・コンピュータのファイル・システムの次の場所で暗号化された Wallet が検索されます。

```
%USERPROFILE%¥ORACLE¥WALLETS
```

暗号化された Wallet がどちらかの場所で見つかると、Wallet のパスワードを入力するように求められます。正しいパスワードを入力すると、暗号化された Wallet が見つかった場所に応じて、不明瞭化された Wallet がレジストリまたはファイル・システムに作成されます。同じセッションで次に「ログアウト」を選択すると、この不明瞭化された Wallet はレジストリまたはファイル・システムから削除されます。「ログアウト」を選択せずに Oracle Enterprise Login Assistant を終了すると、不明瞭化された Wallet は削除されません。

「ログイン」を選択しても、レジストリまたはファイル・システムのデフォルトの場所に暗号化された Wallet が見つからない場合は、Oracle Enterprise Login Assistant によりデフォルトの場所に Oracle Wallet が見つからないことを伝えるメッセージが表示されます。

Wallet Resource Locator

ファイル sqlnet.ora のパラメータ WALLET_LOCATION は拡張され、レジストリに格納された Oracle Wallet をサポートします。WALLET_LOCATION で、Oracle PKI アプリケーションが使用する不明瞭化された Oracle Wallet の場所を指定します。

Windows オペレーティング・システムでは、ファイル sqlnet.ora のパラメータ WALLET_LOCATION に値が指定されていない場合、Oracle PKI アプリケーションにより最初に次のレジストリ・キーで不明瞭化された Wallet が検索されます。

```
¥HKEY_CURRENT_USER¥SOFTWARE¥ORACLE¥WALLETS¥DEFAULT
```

前述の場所で不明瞭化された Wallet が見つからない場合、ローカル・コンピュータのファイル・システムの次の場所で検索が行われます。

```
%USERPROFILE%¥ORACLE¥WALLETS
```

レジストリまたはファイル・システムのデフォルトの場所で不明瞭化された Wallet が見つからない場合、既存の Oracle Wallet が見つからないというエラー・メッセージが表示されます。

5

Windows 2000 PKI の統合

この章では、Windows オペレーティング・システムにおける、Oracle PKI と Windows 2000 PKI との統合について説明します。

この章の項目は次のとおりです。

Oracle PKI

Oracle PKI は、Oracle Enterprise Security Manager、**LDAP** 対応の Oracle Enterprise Manager、Oracle の SSL 認証、Oracle9*i* データベースおよび Oracle Application Server で使用されます。

Oracle PKI には次のコンポーネントが含まれます。

- Oracle Wallet
- Oracle Wallet Manager（OWM）
- Oracle Enterprise Login Assistant

Oracle Wallet では、**暗号化**、**復号化**、**デジタル署名**および検証のために公開鍵アプリケーションで使用される**デジタル証明**、**トラスト・ポイント**および**秘密鍵**が格納されます。Oracle Wallet Manager（OWM）では、デジタル証明を保持する暗号化された Oracle Wallet が作成されます。Oracle Enterprise Login Assistant では、復号化および**不明瞭化**された Oracle Wallet が作成または削除されます。

Windows PKI

この項では、Windows PKI について説明します。

次の内容について説明します。

- Microsoft 証明書ストア
- Microsoft 証明書サービス
- Wallet Resource Locator

注意： Microsoft 証明書ストアとの統合は、Microsoft Enhanced Cryptographic Provider を使用するデジタル証明がある場合にのみ機能します。このような証明書を作成するには、Windows High Encryption Pack をインストールし、Microsoft Enhanced Cryptographic Provider を選択する必要があります。また、同じ鍵の使用（署名および鍵交換）のために使用可能な証明書が複数ある場合、取得された最初の証明書は Oracle SSL に使用されます。

Microsoft 証明書ストア

Microsoft 証明書ストアは、デジタル証明およびそれに関連するプロパティを格納するリポジトリです。Windows 2000 では、デジタル証明および証明書失効リストが、論理ストアおよび物理ストアに格納されます。論理ストアには、物理ストアにある**公開鍵**オブジェクトへのポインタが含まれます。論理ストアにより、各ユーザー、コンピュータまたは**サービス**間で、それらのオブジェクトの複製を格納する必要なく、公開鍵オブジェクトを共有できます。公開鍵オブジェクトは、物理的にローカル・コンピュータの**レジストリ**に格納されますが、一部のユーザー証明書については Active Directory に格納されます。Microsoft により定義される標準システム証明書ストアは、次のとおりです。

- MY または Personal
- CA
- ROOT

MY または Personal は、関連する秘密鍵が使用可能なユーザー証明書を保持します。MY 証明書ストアは、秘密鍵に関連する Cryptographic Service Provider（CSP）を示す証明書プロパティを管理します。アプリケーションは、この情報を使用して、関連する証明書の CSP から秘密鍵を取得します。CA は、発行元または中間**認証局**（CA）証明書を保持します。ROOT は、信頼できるルート CA の自己署名 CA 証明書のみを保持します。

Microsoft 証明書サービス

Microsoft 証明書サービス（MCS）は、次のモジュールで構成されます。

- Server Engine
- Intermediary
- Policy

Server Engine は、すべての証明書要求を処理します。各処理段階においてその他のモジュールと対話し、要求の状態に基づいて適切なアクションが取られていることを確認します。Intermediary モジュールは、クライアントから新規の証明書の要求を受け取り、それを Server Engine に送信します。Policy モジュールには、証明書の発行を制御する一連の規則が含まれます。このモジュールは、必要に応じてアップグレードまたはカスタマイズされる場合があります。

Wallet Resource Locator

Wallet Resource Locator（WRL）により、ファイル sqlnet.ora のパラメータ WALLET_LOCATION が、特定の PKI を識別するよう指定されます。sqlnet.ora のパラメータ WALLET_LOCATION を設定することにより、Oracle Wallet を使用するか、または Microsoft 証明書ストアを使用するかを選択できます。Microsoft 証明書ストアからの**資格証明**を使用するには、sqlnet.ora のパラメータ WALLET_LOCATION を次のように設定します。

```
WALLET_LOCATION = (SOURCE = (METHOD=MCS))
```

Oracle アプリケーションでは、Oracle の SSL 付き TCP/IP プロトコル（TCPS）を使用し、Oracle サーバーに接続します。SSL プロトコルでは、SSL 認証のためにユーザーの Microsoft 証明書ストアからの X.509 証明書およびトラスト・ポイントが使用されます。

A

Oracle Net Services の構成

この付録では、Windows での Oracle Net Services の構成について説明します。Oracle Net Services の構成の詳細は、『Oracle9*i* Net Services 管理者ガイド』を参照してください。

この付録の項目は次のとおりです。

- Oracle Net Services のレジストリ・パラメータおよびサブキーについて
- リスナー要件
- オプションの構成パラメータについて
- 詳細ネットワーク構成

> **関連資料：** Windows 2000 環境の Active Directory と Oracle Net Services の統合については、『Oracle Advanced Security 管理者ガイド』の付録 E を参照してください。

Oracle Net Services のレジストリ・パラメータおよびサブキーについて

レジストリには、Oracle Net Services のパラメータおよびサブキーのエントリが含まれます。Oracle Net Services の構成パラメータを正常に追加または変更するには、そのパラメータの場所および適用される規則を理解する必要があります。

Oracle Net Services のサブキー

サービスに対応するサブキーは、¥HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services に含まれます。インストールされた製品に応じて、Oracle Net Services は次のうちのすべてまたは一部で構成されます。

- Oracle*HOME_NAME*ClientCache
- Oracle*HOME_NAME*CMAdmin
- Oracle*HOME_NAME*CMan
- Oracle*HOME_NAME*TNSListener

各サービスのサブキーには、表 A-1 に示すパラメータが含まれます。

表 A-1 サービス・サブキー・パラメータ

パラメータ	説明
DisplayName	サービス名を指定します。
ImagePath	サービスにより実行される実行可能ファイルの完全修飾パス名、および実行時に実行可能ファイルに渡されるコマンドライン引数を指定します。
ObjectName	ログイン・ユーザー・アカウント、およびサービスがログインする必要のあるコンピュータを指定します。

リスナー要件

Oracle9*i* リリース 2（9.2）では、リスナーはシステムの再起動時に自動的に起動するよう設定されています。すべてのデータベースでそのリスナーのみを使用する場合は、コントロール パネルに表示されている、そのリスナーの Windows NT サービスのみが自動的に開始するよう設定されていることを確認してください。

通常 Windows NT コンピュータで同時に稼働するネット・リスナー・サービスは、1 つのみにするようお薦めします。この単一のリスナーで複数のデータベースをサポートできます。2 つの異なるネット・リスナー・サービスを Windows NT コンピュータ上で同時に稼働させる必要がある場合は、それらが異なる TCP/IP ポート番号でリスニングするよう設定されていることを確認してください。

同じ IP アドレスおよびポートを異なるリスナーに使用した場合でも、2 番目以降のリスナーにバインドの障害は発生しません。Windows NT では、すべてのリスナーが同じ IP アドレスおよびポートでリスニングでき、その結果、リスナーは予測せぬ動作をします。これは、Windows NT オペレーティング・システムにおける TCP/IP 上の問題である可能性が高く、Microsoft 社に報告されました。

オプションの構成パラメータについて

Windows NT および Windows 98 では、次のパラメータが使用できます。

- LOCAL
- TNS_ADMIN
- USE_SHARED_SOCKET

Oracle Net Services では、最初に環境変数としてパラメータをチェックし、その定義された値を使用します。環境変数が定義されていない場合は、レジストリでこれらのパラメータが検索されます。

LOCAL

パラメータ LOCAL を使用すると、接続文字列で接続識別子を指定することなく、Oracle9*i* データベースに接続できます。パラメータ LOCAL の値は、ネット・サービス名などの接続識別子です。たとえば、パラメータ LOCAL が finance として指定されている場合、SQL*Plus から次のコマンドを使用してデータベースに接続できます。

```
SQL> CONNECT scott/tiger
```

次のコマンドは使用しません。

```
SQL> CONNECT scott/tiger@finance
```

Oracle Net Services では、LOCAL が環境変数またはパラメータとしてレジストリに定義されているかをチェックし、finance をサービス名として使用します。このパラメータが存在する場合、Oracle Net Services は LOCAL で指定されたインスタンスに接続します。

TNS_ADMIN

パラメータ TNS_ADMIN を追加すると、Oracle Net Services 構成ファイルのディレクトリ・パスをデフォルトの場所 %ORACLE_HOME%¥network¥admin から変更できます。たとえば、TNS_ADMIN を %ORACLE_HOME%¥test¥admin に設定すると、構成ファイルは %ORACLE_HOME%¥test¥admin から使用されます。

USE_SHARED_SOCKET

パラメータ USE_SHARED_SOCKET を true に設定すると、共有ソケットの使用が可能になります。このパラメータが true に設定されている場合、ネットワーク・リスナーにより、クライアント接続のソケット記述子がデータベース・スレッドに渡されます。その結果、クライアントではデータベース・スレッドに対する新規の接続を確立する必要がなくなり、データベース接続時間が短縮されます。また、すべてのデータベース接続が、ネットワーク・リスナーにより使用されるポート番号を共有するため、サード・パーティのプロキシ・サーバーを設定している場合に役立ちます。

このパラメータは、TCP/IP 環境の専用サーバー・モードでのみ機能します。このパラメータが設定されている場合、リリース 9.0 のリスナーを使用して、Oracle7 リリース 7.*x* データベースを起動することはできません。リスナーと同じ Oracle ホームとは関連付けられていない Oracle データベースの専用サーバーを起動し、共有ソケットを使用可能にするには、両方の Oracle ホームでパラメータ USE_SHARED_SOCKET を設定する必要があります。

詳細ネットワーク構成

次の項では、Windows オペレーティング・システムにおける Oracle Net Services 専用の詳細な構成手順について説明します。

認証方式の構成

Oracle Net Services では、Windows のシステム固有の認証を使用する、Windows オペレーティング・システムの認証方式を提供しています。

Named Pipes プロトコルのセキュリティ構成

サービス Oracle*HOME_NAME*TNSListener に有効なユーザー ID およびパスワードがない場合、ネットワーク・リスナー・サービスは Oracle Names により作成された Named Pipes を開けない可能性があります。

ネットワーク・リスナーのアクセス権を設定するには、次のようにします。

1. 「コントロール パネル」ウィンドウで、「サービス」をダブルクリックします。

   「サービス」ウィンドウが表示されます。

2. 「Oracle*HOME_NAME*TNSListener」サービスをダブルクリックします。

   「サービス」ダイアログ・ボックスが表示されます。

3. 「アカウント」オプションを選択します。次に、横にある「...」オプションを選択します。

   「ユーザーの追加」ダイアログ・ボックスが表示されます。

4. 「名前」リストからログイン ID（ユーザー ID）を選択して、「追加」を選択します。

   ユーザー ID が、「追加する名前」テキスト・ボックスに表示されます。

5. 「OK」をクリックします。

   「サービス」ダイアログ・ボックスが表示され、「アカウント」テキスト・ボックスにユーザー ID が表示されます。

6. 「パスワード」テキスト・ボックスにパスワードを入力します。

7. 「パスワードの確認入力」テキスト・ボックスに同じログイン・パスワードを再入力します。

8. 「OK」をクリックします。

用語集

Active Directory Service Interface（ADSI）

Component Object Model（COM）に基づくクライアント側の製品。ADSI では、Windows 2000、Windows NT、Windows 98 および Windows 95 のクライアント・アプリケーションの Active Directory を含む複数のネットワーク・ディレクトリ・サービスへのアクセスを可能にするディレクトリ・サービス・モデルおよび COM インタフェースのセットが定義されている。ADSI により、アプリケーションは Active Directory と通信できる。

HOME_NAME

ORACLE_HOME の名前を表す。すべての Oracle ホームに一意の *HOME_NAME* がある。

HOME*ID*

製品をインストールする各 Oracle ホーム・ディレクトリの一意のレジストリ・サブキーを表す。あるコンピュータ上の異なる Oracle ホーム・ディレクトリに製品をインストールするたびに、新しい HOME*ID* が作成されて増分される。各 HOME*ID* には、インストールされた Oracle 製品独自の構成パラメータ設定が含まれる。

init.ora

「初期化パラメータ・ファイル」を参照。

LDAP

「**Lightweight Directory Access Protocol（LDAP）**」を参照。

Lightweight Directory Access Protocol（LDAP）

標準的で、拡張可能なディレクトリ・アクセス・プロトコル。LDAP クライアントとサーバーが通信に使用する共通言語。LDAP は、Oracle Internet Directory などの業界標準のディレクトリ製品をサポートする設計規則のフレームワークである。

listener.ora

リスナー名、接続要求を受け入れるためのプロトコル・アドレスおよびリスニングするサービスを識別するリスナーの構成ファイル。

通常、ファイル listener.ora は、Windows オペレーティング・システムの %ORACLE_HOME%¥network¥admin にある。

Microsoft 管理コンソール（Microsoft Management Console）

スナップインと呼ばれる管理ツールのホストとして機能するアプリケーション。Microsoft 管理コンソール自体は、機能を提供しない。

Oracle Net

クライアント・アプリケーションから Oracle データベース・サーバーへのネットワーク・セッションを使用可能にする **Oracle Net Services** のコンポーネント。一度ネットワーク・セッションが確立されると、Oracle Net は、クライアント・アプリケーションおよびデータベース・サーバーのデータ送信手段として機能する。クライアント・アプリケーションとデータベース・サーバー間の接続を確立し、維持する役割の他に、それらの間のメッセージ交換も行う。Oracle Net は、ネットワーク上の各コンピュータにあるため、これらのジョブを実行できる。

Oracle Net Services

分散された異機種間コンピューティング環境においてエンタープライズ・レベルの接続性の解決策を提供する一連のネットワーキング・コンポーネント。Oracle Net Services は、**Oracle Net**、**リスナー**、Oracle Connection Manager、Oracle Net Configuration Assistant および Oracle Net Manager で構成される。

ORACLE_BASE

このマニュアルで ORACLE_BASE と呼ばれる Oracle ベースは、Oracle ディレクトリ・ツリーのルート・ディレクトリである。

ORACLE_HOME

Oracle 製品が動作する環境に対応する。この環境には、インストールされた製品ファイルの場所、製品のバイナリ・ファイルを示す PATH 変数、**レジストリ**・エントリ、ネット・サービス名およびプログラム・グループが含まれる。

Oracle サービス（Oracle service）

Oracle コンポーネントと関連付けられる**サービス**。

SID

「**システム識別子**」を参照。

SYSDBA

ADMIN OPTION および **SYSOPER** システム**権限**とすべてのシステム権限を持つ特別なデータベース管理**ロール**。SYSDBA では、CREATE DATABASE アクションおよび時間ベースの**リカバリ**も許可されている。

SYSOPER

データベース管理者が、STARTUP、SHUTDOWN、ALTER DATABASE OPEN/MOUNT、ALTER DATABASE BACKUP、ARCHIVE LOG および RECOVER を実行することを許可する、特別なデータベース管理**ロール**。RESTRICTED SESSION **権限**も含まれる。

SYSTEM

各データベースに自動的に作成される標準 DBA **ユーザー名**。SYSTEM は、初期パスワード MANAGER で作成される。DBA によってデータベースがメンテナンスされる場合は、ユーザー名 SYSTEM が優先される。

tnsnames.ora

接続記述子を含むファイル。各**接続記述子**は、**ネット・サービス名**にマップされる。すべてのクライアントまたは各クライアントで使用するために、このファイルを集中してメンテナンスすることも、ローカルでメンテナンスすることもできる。通常、このファイルは、Windows NT の %ORACLE_HOME%¥network¥admin にある。

Windows NT グローバル・グループ（Windows NT global group）

グループ独自のドメイン、そのドメイン内のメンバー・サーバーとワークステーション、および信頼できるドメインでのアクセス権および権利が付与されるグループ。これらすべての場所で、**Windows NT ローカル・グループ**のメンバーにもなる。ただし、グローバル・グループには、グループ独自のドメインのユーザー・アカウントしか含めることができない。

Windows NT ローカル・グループ（Windows NT local group）

グループ独自のコンピュータに対するアクセス権および権利、または（ドメインの一部の場合）そのドメインのドメイン・コントローラに対するアクセス権および権利が付与されるグループ。ただし、ローカル・グループには、グループ独自のドメインと信頼できるドメインの両方のユーザー・アカウントおよび **Windows NT グローバル・グループ**を含めることができる。

アラート・ファイル（alert file）

データベース操作中に発生するエラー・メッセージについての重要な情報が含まれているファイル。

暗号化（encryption）

メッセージを、宛先の受信者以外の第三者には読むことができない形式に変換するプロセス。

インスタンス（instance）

実行中の Oracle データベースはすべて、Oracle インスタンスと対応付けられる。データベースをデータベース・サーバー上で起動すると（コンピュータの種類にかかわらず）、Oracle は**システム・グローバル領域（SGA）**と呼ばれるメモリー領域を割り当て、Oracle **プロセス**を起動する。この SGA と Oracle プロセスの組合せをインスタンスと呼ぶ。インスタンスのメモリーおよびプロセスは、対応するデータベースのデータを効率的に管理し、1 名以上のデータベース・ユーザーがデータベースを使用する機能を提供する。

エンタープライズ・ドメイン（enterprise domain）

Oracle9*i* データベース、エンタープライズ・ユーザーおよびエンタープライズ・ロールで構成されるディレクトリ構造。エンタープライズ・ドメインは、共通のディレクトリ・データベースを共有するコンピュータの集合である Windows 2000 ドメインとは異なる。

エンタープライズ・ユーザー（enterprise user）

企業内で固有の識別情報を持つユーザー。エンタープライズ・ユーザーは、**スキーマ**を介して個々のデータベースに接続する。エンタープライズ・ユーザーには、データベースに対するユーザーのアクセス権限を決定する**エンタープライズ・ロール**が割り当てられる。

エンタープライズ・ロール（enterprise role）

複数のデータベースに対するグローバル・ロールが含まれるディレクトリ構造。**エンタープライズ・ユーザー**に付与される。

外部ユーザー（external user）

Windows 2000 または Windows NT オペレーティング・システムにより認証されたユーザー。パスワードの入力を要求されることなく Oracle データベースにアクセスできる。外部ユーザーは、通常のデータベース・ユーザー（データベース管理者以外）で、このユーザーに対しては標準のデータベース・ロール（`CONNECT` および `RESOURCE` など）を割り当て、**SYSDBA**（データベース管理者）**権限**または **SYSOPER**（データベース・オペレータ）権限は割り当てない。

外部ロール（external role）

Windows NT および Windows 2000 オペレーティング・システムにより作成および管理されるロール。一度外部ロールを作成すると、データベース・ユーザーに対してその**ロール**を付与したり、取り消したりできる。外部ロールを作成する前に、**init.ora** のパラメータ `OS_ROLES` を `true` に設定し、Oracle データベースを再起動する必要がある。Windows オペレーティング・システムおよび Oracle データベースの両方を使用して、同時にロールを付与することはできない。

グローバル・グループ（global group）

「**Windows NT グローバル・グループ**」を参照。

グローバル・ロール（global role）

ディレクトリで管理されるが、その権限は 1 つのデータベースに格納されるロール。

権限（privilege）

特定の種類の SQL 文を実行したり、別のユーザーのオブジェクトにアクセスしたりするための権利。

公開鍵（public key）

公開鍵暗号における、一般に公開される鍵。主に**暗号化**に使用されるが、署名の確認にも使用できる。

公開鍵暗号（public key cryptography）

公開鍵暗号は、共有**公開鍵**と**秘密鍵**をペアで使用する、情報の**暗号化**および**復号化**である。これにより、パブリック・ネットワーク上において安全でプライベートな通信ができる。

サービス（service）

レジストリにインストールされ、Windows NT で管理される実行可能な**プロセス**。一度サービスを作成して開始すると、コンピュータにログインしているユーザーがいない場合も、実行できる。

サービス名（service name）

「**ネット・サービス名**」を参照。

資格証明（credentials）

データベースにアクセスするときに使用される**ユーザー名**、パスワードおよび証明書。

システム・グローバル領域（System Global Area: SGA）

Oracle **インスタンス**のデータおよび制御情報が格納される共有メモリー構造のグループ。

システム識別子（system identifier: SID）

Oracle **インスタンス**の一意の名前。Oracle データベースを切り替えるには、ユーザーは SID を指定する必要がある。SID は、**tnsnames.ora** ファイル内の**接続記述子**の CONNECT DATA 部分、あるいは **listener.ora** ファイル内の**ネットワーク・リスナー**の定義に含まれている。

初期化パラメータ・ファイル（initialization parameter file）

データベースおよび**インスタンス**の初期化に必要な情報を含むテキスト・ファイル。ファイル `init.ora` は、Windows オペレーティング・システムのディレクトリ `%ORACLE_BASE%¥admin¥DB_NAME¥pfile` にある。

スキーマ（schema）

オブジェクトの名前付きコレクション。表、**ビュー**、クラスタ、プロシージャおよびパッケージなど、特定のユーザーと関連付けられるもの。

スレッド（thread）

プロセス内の各実行パス。スレッドは、プロセス内のオブジェクトであり、プログラム命令を実行する。スレッドにより、プロセス内における同時実行が可能になる。このため、プロセスはプログラムの異なる部分を異なるプロセッサ上で同時に実行できる。スレッドは、Windows NT 上でスケジュールできる最も基本的なコンポーネントである。

制御ファイル（control file）

データベースの物理構造を記録するファイル。データベース名、関連データベースおよびオンライン REDO ログ・ファイルの名前と場所、データベース作成のタイムスタンプ、現在のログ順序番号およびチェックポイント情報が含まれる。

接続記述子（connect descriptor）

特別にフォーマットされた、ネットワーク接続のための宛先の記述。接続記述子には、宛先**サービス**およびネットワーク・ルート情報が含まれる。宛先サービスは、Oracle9*i* または Oracle8*i* データベースのサービス名、あるいは Oracle8 リリース 8.0 データベースの Oracle**システム識別子**（SID）を使用することにより示される。ネットワーク・ルートは、少なくとも、ネットワーク・アドレスを使用して**リスナー**の場所を示す。

接続識別子（connect identifier）

接続記述子にマップされる、**ネット・サービス名**またはサービス名。ユーザーは、接続する**サービス**に対する**接続文字列**内の接続記述子とともに**ユーザー名**およびパスワードを渡すことによって、接続要求を開始する。たとえば、次のようになる。

```
CONNECT username/password@connect_identifier
```

接続文字列（connect string）

ユーザーが接続する**サービス**に渡す、**ユーザー名**、パスワードおよび**ネット・サービス名**などの情報。たとえば、次のようになる。

```
CONNECT username/password@net_service_name
```

データ・ディクショナリ（data dictionary）

データベースの情報を提供する読取り専用の表のセット。

データベース別名（database alias）

「**ネット・サービス名**」を参照。

デジタル証明（digital certificate）

識別情報を**公開鍵**に安全にバインドする ITU X.509 バージョン 3 規格のデータ構造。証明書は、エンティティの公開鍵が信頼できる識別情報（**認証局**）で署名されたときに作成される。この証明書は、そのエンティティの情報が正しいこと、および公開鍵がそのエンティティに実際に含まれていることを保証する。

デジタル署名（digital signature）

デジタル署名は、**公開鍵**アルゴリズムを使用して、送信者の**秘密鍵**でメッセージに署名すると作成される。デジタル署名によって、文書が信頼できるものであること、別のエンティティで偽造されていないこと、変更されていないこと、送信者によって拒否されないことが保証される。

トラスト・ポイント（trust point）

トラスト・ポイントまたは信頼できる証明書は、一定の信頼度を持つと認定された第三者の識別情報。信頼できる証明書は、エンティティが本物であるという識別情報の確認が行われるときに使用される。信頼する認証局を信頼できる証明書と呼ぶ。複数レベルの信頼できる証明書がある場合、証明連鎖における下位レベルの信頼できる証明書で、それより上のレベルの証明書をすべて再確認する必要はない。

認可（authorization）

ユーザー、プログラムまたは**プロセス**が、オブジェクトまたはオブジェクトのセットにアクセスするために付与されるアクセス権。Oracle では、認可は**ロール**の機能を介して実現される。1 人のユーザーまたはユーザー・グループに、1 つのロールまたはロールのセットを付与できる。ロールはさらに他のロールに付与できる。

認証（authenticate）

コンピュータ・システム内でユーザー、デバイスまたはその他のエンティティの識別情報を検証すること。多くの場合、システム内のリソースへのアクセスを許可するための前提条件となる。

認証局（certificate authority）

ユーザー、データベース、管理者、クライアント、サーバーなどの他のエンティティが本物であることを証明する、信頼できる第三者機関。認証局では、ユーザーの識別情報を検証し、認証局の**秘密鍵**の 1 つを使用して署名した証明書を付与する。

ネット・サービス名（net service name）

データベース・サーバーを識別するためにクライアントが使用する名前。ネット・サービス名は、ポート番号とプロトコルにマップされる。**接続文字列**または**データベース別名**とも呼ばれる。

ネットワーク・サービス（network service）

Oracle アプリケーション・ネットワークでは、サービスはサービス・コンシューマ用のタスクを実行する。たとえば、Oracle Names Server は、クライアントに名前解決サービスを提供する。

ネットワーク・リスナー（network listener）

1 つ以上のプロトコルで 1 つ以上のデータベースへの接続要求をリスニングする、サーバー上のリスナー。「**リスナー**」を参照。

秘密鍵（private key）

公開鍵暗号における秘密鍵。主に**復号化**に使用されるが、**デジタル署名**とともに**暗号化**にも使用される。

ビュー（view）

1 つ以上の表（または他のビュー）の構造およびデータの、選択された表示。

表領域（tablespace）

データベースは、表領域という 1 つ以上の論理記憶単位で構成される。表領域はセグメントという記憶域の論理単位で構成される。セグメントはさらにエクステントで構成される。

フォレスト（forest）

相互に信頼関係を持つ 1 つ以上の Active Directory ツリーのグループ。1 つのフォレストのすべてのツリーは、共通の**スキーマ**、構成およびグローバル・カタログを共有する。フォレストに複数のツリーが含まれる場合、そのツリーは連続する名前空間を形成しない。特定のフォレストのすべてのツリーは、推移性の双方向信頼関係によって相互に信頼する。

復号化（decryption）

暗号化されたメッセージの内容（暗号文）を、元の読取り可能な書式（平文）に戻す変換プロセス。

複数の Oracle ホーム（multiple Oracle homes）

1 台のコンピュータに複数の Oracle ホームを配置する機能。

不明瞭化（obfuscated）

不明瞭化された情報とは、読取り不可能な形式にスクランブルされた情報。スクランブルに使用されたアルゴリズムが不明な場合、スクランブルの解除は非常に難しい。

プロセス（process）

実行可能ファイルを実行できるオペレーティング・システム内のメカニズム。（オペレーティング・システムによっては、ジョブまたはタスクという用語を使用する。）通常、プロセスには実行用のプライベート・メモリー領域がある。Windows NT では、プログラム（Oracle または Microsoft Word など）が実行されるときにプロセスが作成される。実行可能プログラムに加え、すべてのプロセスは少なくとも 1 つの**スレッド**を含む。Oracle マスター・プロセスには、数百のスレッドが含まれる。

マウント（mount）

起動された**インスタンス**とデータベースを関連付けること。

ユーザー名（username）

データベースのオブジェクトに接続してアクセスできる名前。

ユニバーサル・グループ（universal group）

ユニバーサル・グループは、Windows 2000 では使用できるが、Windows NT では使用できない。他のユニバーサル・グループ、**ローカル・グループ**および**グローバル・グループ**など、その他のグループを含めることができる。

リカバリ（recovery）

物理的なバックアップのリストアとは、バックアップを再構築して、Oracle サーバーで使用可能な状態にすることである。リストアされたバックアップのリカバリとは、REDO レコード（つまり、バックアップ後にデータベースに行われた変更の記録）を使用して、バックアップを更新することである。バックアップのリカバリには 2 つの異なる方法がある。REDO データを適用してより最近のバックアップにロールフォワードする方法と、コミットされていないトランザクションに対する変更をすべてロールバックして元の状態に戻す方法である。

リスナー（listener）

サーバーに常駐している**プロセス**。クライアントの着信接続要求をリスニングし、サーバーへのネットワーク通信量を管理する。リスナーは、クライアントがサーバーとのネットワーク・セッションを要求するたびに、実際の要求を受け取る。クライアントの情報がリスナーの情報と一致している場合、リスナーによりサーバーへの接続が許可される。

リモート・コンピュータ（remote computer）

ネットワーク上に存在する、ローカル・コンピュータ以外のコンピュータ。

レジストリ（registry）

コンピュータの構成情報を格納する Windows のリポジトリ。

ローカル・グループ（local group）

「**Windows NT ローカル・グループ**」を参照。

ローカル・ロール（local role）

データベースにより作成および管理されるロール。一度ローカル・ロールを作成すると、データベース・ユーザーに対してその**ロール**を付与したり、取り消したりできる。Windows NT（**外部ロール**管理用）および Oracle データベース（ローカル・ロール管理用）は同時に使用できない。

ロール（role）

関連する権限の名前付きグループ。ユーザーまたは他のロールにロールを付与できる。

割当て制限（quota）

データベース・ユーザーにより使用されるデータベース記憶域の容量などのリソースの制限。データベース管理者は、各 Oracle **ユーザー名**に対して、**表領域**の割当て制限を設定できる。

索引

S

T

U

W

え

お

か

け

こ

し

せ

て

に

ね

は

ひ

ゆ

り

れ

ろ