Oracle® Database

2 日でセキュリティ・ガイド

11*g* リリース 1（11.1）

部品番号 : E05781-03

2008 年 10 月

ORACLE®

Oracle Database 2 日でセキュリティ・ガイド , 11*g* リリース 1（11.1）

部品番号 : E05781-03

Oracle Database 2 Day + Security Guide, 11*g* Release 1 (11.1)

原本部品番号 : B28337-04

原本著者 : Patricia Huey

原本協力者 : Nina Lewis、Paul Needham、Deborah Owens、Ashwini Surpur、Kamal Tbeileh、Mark Townsend、Peter Wahl、Peter M. Wong

目次

4 ユーザー権限の管理

5 ネットワークの保護

6 データの保護

7 データベース・アクティビティの監査

索引

表一覧

はじめに

『Oracle Database 2 日でセキュリティ・ガイド』へようこそ。このマニュアルは、Oracle Database を使用して日常的なセキュリティ・タスクを実行するユーザーを対象としています。

内容は次のとおりです。

対象読者

このマニュアルでは、Oracle Database のセキュリティを管理するために『Oracle Database 2 日でデータベース管理者』で習得したセキュリティの知識についてさらに詳しく説明します。このマニュアルの内容はすべてのプラットフォームに適用されます。プラットフォーム固有の情報については、ご使用のプラットフォームのインストレーション・ガイド、構成ガイドおよびプラットフォーム・ガイドを参照してください。

このマニュアルは次のユーザーを対象としています。

- データベース・セキュリティ管理者のスキルを習得する必要がある Oracle Database 管理者
- セキュリティ管理に関する知識はあるが、Oracle Database の使用は初めてのデータベース管理者

このマニュアルでは、セキュリティに関して包括的には説明しません。セキュリティの詳細は、Oracle Database セキュリティに関するドキュメント・セットを参照してください。このマニュアルでは、Oracle E-Business Suite アプリケーションのセキュリティについては説明しません。Oracle E-Business Suite アプリケーションのセキュリティについては、Oracle E-Business Suite 製品のドキュメントを参照してください。

ドキュメントのアクセシビリティについて

オラクル社は、障害のあるお客様にもオラクル社の製品、サービスおよびサポート・ドキュメントを簡単にご利用いただけることを目標としています。オラクル社のドキュメントには、ユーザーが障害支援技術を使用して情報を利用できる機能が組み込まれています。HTML 形式のドキュメントで用意されており、障害のあるお客様が簡単にアクセスできるようにマークアップされています。標準規格は改善されつつあります。オラクル社はドキュメントをすべてのお客様がご利用できるように、市場をリードする他の技術ベンダーと積極的に連携して技術的な問題に対応しています。オラクル社のアクセシビリティについての詳細情報は、Oracle Accessibility Program の Web サイト http://www.oracle.com/accessibility/ を参照してください。

ドキュメント内のサンプル・コードのアクセシビリティについて

スクリーン・リーダーは、ドキュメント内のサンプル・コードを正確に読めない場合があります。コード表記規則では閉じ括弧だけを行に記述する必要があります。しかし JAWS は括弧だけの行を読まない場合があります。

外部 Web サイトのドキュメントのアクセシビリティについて

このドキュメントにはオラクル社およびその関連会社が所有または管理しない Web サイトへのリンクが含まれている場合があります。オラクル社およびその関連会社は、それらの Web サイトのアクセシビリティに関しての評価や言及は行っておりません。

Oracle サポート・サービスへの TTY アクセス

アメリカ国内では、Oracle サポート・サービスへ 24 時間年中無休でテキスト電話（TTY）アクセスが提供されています。TTY サポートについては、(800)446-2398 にお電話ください。アメリカ国外からの場合は、+1-407-458-2479 にお電話ください。

関連ドキュメント

詳細は、次のリソースを参照してください。

Oracle Database のドキュメント

セキュリティ関連の情報については、Oracle Database のドキュメント・セットの次のマニュアルを参照してください。

- 『Oracle Database 2 日でデータベース管理者』
- 『Oracle Database 管理者ガイド』

- 『Oracle Database セキュリティ・ガイド』
- 『Oracle Database 概要』
- 『Oracle Database リファレンス』
- 『Oracle Database Vault 管理者ガイド』

このマニュアルの多くの例では、Oracle をインストールするときにデフォルトでインストールされるシード・データベースのサンプル・スキーマを使用しています。これらのスキーマの作成方法および使用方法については、『Oracle Database サンプル・スキーマ』を参照してください。

Oracle Technology Network Japan（OTN-J）

リリース・ノート、インストール関連ドキュメント、このマニュアルの更新版、ホワイト・ペーパー、またはその他の関連ドキュメントは、Oracle Technology Network Japan（OTN-J）から無償でダウンロードできます。次の Web サイトを参照してください。

`http://www.oracle.com/technology/global/jp/membership/index.htm/`

メンバーでないユーザーは、次の Web サイトから無償で登録できます。

`http://www.oracle.com/technology/global/jp/membership/index.html`

OTN のセキュリティ固有の情報については、次の Web サイトを参照してください。

`http://www.oracle.com/technology/global/jp/tech/security/index.html`

このマニュアルを含む最新版の Oracle ドキュメントについては、次の Web サイトを参照してください。

`http://www.oracle.com/technology/global/jp/documentation/index.html`

OracleMetaLink

セキュリティ・パッチ、動作保証およびサポート・ナレッジ・ベースについては、次の Oracle*MetaLink* を参照してください。

`https://metalink.oracle.com/`

表記規則

このマニュアルでは次の表記規則を使用します。

規則	意味
太字	太字は、操作に関連する Graphical User Interface 要素、または本文中で定義されている用語および用語集に記載されている用語を示します。
イタリック体	イタリックは、ユーザーが特定の値を指定するプレースホルダ変数を示します。
固定幅フォント	固定幅フォントは、段落内のコマンド、URL、サンプル内のコード、画面に表示されるテキスト、または入力するテキストを示します。

サポートおよびサービス

次の各項に、各サービスに接続するための URL を記載します。

Oracle サポート・サービス

オラクル製品サポートの購入方法、および Oracle サポート・サービスへの連絡方法の詳細は、次の URL を参照してください。

`http://www.oracle.com/lang/jp/support/index.html`

製品マニュアル

製品のマニュアルは、次の URL にあります。

http://www.oracle.com/technology/global/jp/documentation/index.html

研修およびトレーニング

研修に関する情報とスケジュールは、次の URL で入手できます。

http://education.oracle.com/pls/web_prod-plq-dad/db_pages.getpage?page_id=3

その他の情報

オラクル製品やサービスに関するその他の情報については、次の URL から参照してください。

http://www.oracle.com/lang/jp/index.html
http://www.oracle.com/technology/global/jp/index.html

注意： ドキュメント内に記載されている URL や参照ドキュメントには、Oracle Corporation が提供する英語の情報も含まれています。日本語版の情報については、前述の URL を参照してください。

1

Oracle Database セキュリティの概要

この章の内容は次のとおりです。

このマニュアルについて

このマニュアルでは、日常的なデータベース・セキュリティ・タスクの実行方法について説明します。これは、Oracle Database セキュリティの基礎となる概念を理解しやすくすることを目的としています。データベースの保護に必要な、一般的なセキュリティ・タスクの実行方法について学びます。このマニュアルで説明するタスクの完了時に得られる知識は、データの保護、および米国企業改革法（Sarbanes-Oxley Act）などの一般的なコンプライアンス要件の準拠に役立ちます。

このマニュアルで使用している主な管理インタフェースは、Database Console モードの Oracle Enterprise Manager で、Oracle Database で導入されたすべての自己管理機能を装備しています。

この項の内容は次のとおりです。

このマニュアルを使用する前に

このマニュアルを使用する前に、次のことを実行する必要があります。

- 『Oracle Database 2 日でデータベース管理者』をよく理解すること
- 1-3 ページの「データベースを保護するためのツール」で説明している必要な製品およびツールを入手すること

このマニュアルの対象および対象外

このマニュアルはタスク指向です。セキュリティ・タスクを実行する理由とタイミングについて説明することがこのマニュアルの目的です。

必要に応じて、タスクの理解および実行に必要な概要および手順について説明します。このマニュアルでは、Oracle Database のすべての概要を包括的には説明しません。包括的な概要については、『Oracle Database 概要』を参照してください。

また、必要に応じて、セキュリティ・タスクを完了するために必要な Oracle Database の管理手順についても説明します。Oracle Database の基本的な管理タスクについては説明しません。基本的な管理タスクについては、『Oracle Database 2 日でデータベース管理者』を参照してください。また、管理タスクの詳細は、『Oracle Database 管理者ガイド』を参照してください。

また、このマニュアルでは、Oracle Database のすべてのセキュリティ機能に関して、包括的には説明しません。このマニュアルで使用されているツールに類似したコマンドライン機能を提供する API についても説明しません。これらについては、『Oracle Database セキュリティ・ガイド』を参照してください。

一般的なデータベース・セキュリティ・タスク

Oracle Database のデータベース管理者は、セキュリティに関連する次のタスクを実行する必要があります。

- データベースのインストール環境と構成が保護されていることの確認
- セキュアなパスワード・ポリシーの開発、ロールの作成および割当て、当該ユーザーのみへのデータ・アクセスの制限などの、ユーザー・アカウントにおけるセキュリティ面の管理
- ネットワーク接続がセキュアであることの確認
- 機密データの暗号化
- データベースのセキュリティに脆弱性がなく、外部からの侵入を防止していることの確認
- 監査するデータベース・コンポーネントの決定と監査の粒度の決定
- セキュリティ・パッチのダウンロードとインストール

小中規模のデータベース環境では、これらのタスクのみでなく、Oracle ソフトウェアのインストール、データベースの作成、パフォーマンスの監視など、データベース管理者の関連タスクも行う場合があります。大規模な企業環境では、タスクを複数のデータベース管理者で分担し、データベース・セキュリティやデータベースのチューニングなど、それぞれが専門のタスクを担当することがあります。

データベースを保護するためのツール

データベース保護という目的を達成するためには、次の製品、ツールおよびユーティリティが必要です。

- **Oracle Database 11*g* リリース 1（11.1）Enterprise Edition**

  Oracle Database 11*g* リリース 1（11.1）Enterprise Edition は企業クラスのパフォーマンスを持ち、クラスタ・サーバー構成および単一サーバー構成で拡張性および信頼性を備えています。このマニュアルで使用されている多くのセキュリティ機能が含まれています。

- **Oracle Enterprise Manager Database Control**

  Oracle Enterprise Manager は、単一のデータベース・インスタンスまたはクラスタ・データベースに対して管理タスクを実行できる Web アプリケーションです。

- **SQL*Plus**

  SQL*Plus は、SQL および PL/SQL コードを作成し、実行できる開発環境です。これは Oracle Database 11*g* リリース 1（11.1）のインストールに含まれます。

- **Database Configuration Assistant（DBCA）**

  Database Configuration Assistant を使用すると、データベースの作成、構成、削除など、データベースの一般的なタスクを実行できます。このマニュアルでは、DBCA を使用してデフォルト監査を有効にします。

- **Oracle Net Manager**

  Oracle Net Manager を使用すると、Oracle Database でネットワーク関連のタスクを実行できます。このマニュアルでは、Oracle Net Manager を使用してネットワーク暗号化を設定します。

データベースの保護 : ロードマップ

データベースを保護する方法を習得するには、次の一般的な手順を実行します。

1. **Oracle Database のインストール環境と構成を保護します。**

   第 2 章「データベースのインストール環境と構成の保護」のタスクを完了して、Oracle Database のインストール環境へのアクセスを保護します。

2. **サイトに対するユーザー・アカウントを保護します。**

   第 3 章「Oracle Database ユーザー・アカウントの保護」のタスクを完了します。この章は、ユーザー・アカウントの作成方法を習得する『Oracle Database 2 日でデータベース管理者』の内容を踏まえています。ここでは、次の内容を習得できます。

   - ユーザー・アカウントを期限切れにする、ロックする、ロックを解除する方法
   - セキュアなパスワード選択のガイドライン
   - パスワードの変更方法
   - パスワード管理の実施方法
   - Oracle Database 表でのパスワードの暗号化が必要な理由

3. **権限の動作方法を理解します。**

   第 4 章「ユーザー権限の管理」のタスクを完了し、次の内容について習得します。

   - 権限の動作方法
   - 権限付与を慎重に行う必要がある理由
   - データベース・ロールの動作方法
   - セキュア・アプリケーション・ロールの作成方法

4. **ネットワーク間を移動するデータを保護します。**

   第 5 章「ネットワークの保護」のタスクを完了して、クライアント接続の保護方法およびネットワーク暗号化の構成方法を習得します。

5. **機密データを暗号化します。**

   第 6 章「データの保護」のタスクを完了し、次の内容について習得します。

   - データベースの表列および表領域を自動的に暗号化するための透過型データ暗号化の使用方法
   - Oracle Virtual Private Database によるデータ・アクセスの制御方法
   - Oracle Label Security による行レベルのセキュリティの強制方法
   - Oracle Database Vault を使用した機密データへのシステム管理アクセスの制御方法

6. **監査を設定して、データベース・アクティビティを監視します。**

   第 7 章「データベース・アクティビティの監査」のタスクを完了して、標準監査について習得します。

2

データベースのインストール環境と構成の保護

この章の内容は次のとおりです。

データベースのインストール環境と構成の保護について

Oracle Database をインストールした後で、データベースのインストール環境と構成を保護する必要があります。この章では、この保護を行うために一般に使用される方法を説明します。そのすべての方法では、データベース・ファイルの特定の領域への権限を制限します。

Oracle Database は、いくつかのオペレーティング・システムで使用できます。Oracle Database に関する詳細なプラットフォーム固有情報は、次のマニュアルを参照してください。

- 『Oracle Database プラットフォーム・ガイド for Microsoft Windows』
- Oracle Database の管理者リファレンス
- 使用しているプラットフォームの『Oracle Database インストレーション・ガイド』

デフォルトのセキュリティ設定の有効化

新しいデータベースを作成した場合や、既存のデータベースを変更した場合、Database Configuration Assistant（DBCA）の「セキュリティ設定」ウィンドウを使用して、デフォルトのセキュリティ設定を有効または無効にできます。これらの設定を有効にすることをお薦めします。これらの設定では、次のデフォルトのセキュリティ設定が可能です。

- デフォルトの監査設定を有効にします。詳細は、7-5 ページの「セキュリティ関連の SQL 文および権限に対するデフォルト監査の使用」を参照してください。
- 新しいパスワードまたは変更したパスワードの厳しい制約を作成します。新しいパスワードの要件については、3-9 ページの「パスワードの作成要件」を参照してください。
- CREATE EXTERNAL JOB 権限を PUBLIC から削除します。よりセキュリティを強化するために、CREATE EXTERNAL JOB 権限を SYS、データベース管理者、およびこの権限が必要なユーザーにのみ付与します。
- 初期化パラメータ設定を変更します。表 2-1 に、変更された初期化パラメータ設定を示します。

表 2-1 初期化パラメータのデフォルトのセキュリティ設定

設定	前の設定	新しい設定
AUDIT_TRAIL	NONE	DB
O7_DICTIONARY_ACCESSIBILITY	TRUE	FALSE
PASSWORD_GRACE_TIME	UNLIMITED	7
PASSWORD_LOCK_TIME	UNLIMITED	1
PASSWORD_LOGIN_FAILURES	10	10
PASSWORD_LIFE_TIME	UNLIMITED	180
PASSWORD_REUSE_MAX	UNLIMITED	UNLIMITED
PASSWORD_REUSE_TIME	UNLIMITED	UNLIMITED
REMOTE_OS_ROLES	TRUE	FALSE

Database Configuration Assistant を使用してデフォルトのプロファイル・セキュリティ設定を有効にするには、次のようにします。

1. Database Configuration Assistant を起動します。
   - **UNIX:** 端末ウィンドウで次のコマンドを入力します。

     ```
     dbca
     ```

     一般的に、dbca は $ORACLE_HOME/bin ディレクトリにあります。

- **Windows**: **「スタート」**メニューから**「すべてのプログラム」**をクリックします。次に**「Oracle - *ORACLE_HOME*」→「Configuration and Migration Tools」→「Database Configuration Assistant」**の順にクリックします。

  または、次のコマンド・プロンプトで Database Configuration Assistant を起動できます。

  ```
  dbca
  ```

  Windows では一般的に、dbca は *ORACLE_BASE*¥*ORACLE_HOME*¥bin ディレクトリにあります。

2. 「ようこそ」ウィンドウで**「次へ」**をクリックします。

   「操作」ウィンドウが表示されます。

3. **「データベース・オプションの構成」**を選択して、**「次へ」**をクリックします。

   「データベース」ウィンドウが表示されます。

4. 設定するデータベースを選択して、**「次へ」**をクリックします。

   「セキュリティ設定」ウィンドウが表示されます。

5. **「11g のデフォルトの高度セキュリティ設定を維持（推奨）。これらの設定には、監査および新しいデフォルト・パスワード・プロファイルの有効化が含まれます。」**オプションを選択します。

6. **「次へ」**をクリックします。

   「データベース・コンポーネント」ウィンドウが表示されます。

7. 他のオプションを選択してから、**「次へ」**をクリックします。表示される質問に適宜、回答します。

8. **「終了」**をクリックします。

Oracle データ・ディクショナリの保護

ここでは、データ・ディクショナリを保護する方法を説明します。データ・ディクショナリは、スキーマ定義やデフォルト値など、データベースに関する情報を提供する一連のデータベース表です。

この項の内容は次のとおりです。

Oracle データ・ディクショナリについて

Oracle データ・ディクショナリは、データベースに関する情報を提供するデータベース表のセットです。データ・ディクショナリの内容は次のとおりです。

- データベース内のすべてのスキーマ・オブジェクトの定義（表、ビュー、索引、クラスタ、シノニム、順序、プロシージャ、ファンクション、パッケージ、トリガーなど）
- スキーマ・オブジェクトに割り当てられている容量と現在使用されている容量
- 列のデフォルト値
- 整合性制約情報
- Oracle Database ユーザーの名前
- 各ユーザーに付与されている権限とロール
- 様々なスキーマ・オブジェクトをアクセスまたは更新した人物などの監査情報
- その他の一般的なデータベース情報

ある特定のデータベースのデータ・ディクショナリ表およびビューは、そのデータベースの SYSTEM 表領域に格納されます。データ・ディクショナリは、他のデータベース・データと同様に表およびビューで構成されます。ある特定のデータベースのデータ・ディクショナリ表およびビューは、すべてユーザー SYS によって所有されます。SYSDBA 権限を使用してデータベースに接続すると、データ・ディクショナリに対する完全なアクセス権が許可されます。SYSDBA 権限へのアクセスは、パッチ適用やその他の管理操作などの必要な操作のみに限定することをお薦めします。データ・ディクショナリは、すべての Oracle Database の中心です。

データ・ディクショナリには SQL 文を使用してアクセスできます。SYSDBA 権限以外で接続した場合のみデータ・ディクショナリは読取り専用であるため、その表とビューに対して問合せ（SELECT 文）のみを発行できます。データ・ディクショナリのオブジェクトには、ユーザーに公開されないものがあることに注意してください。データ・ディクショナリ・オブジェクトのサブセット（USER_% で始まるオブジェクトなど）は、すべてのデータベース・ユーザーに対して読取り専用として公開されます。『Oracle Database リファレンス』には、データ・ディクショナリに関する情報を検索するために問い合せることのできるデータベース・ビューのリストが記載されています。

例 2-1 に、DICTIONARY ビューを問い合せることでデータ・ディクショナリに固有のデータベース・ビューのリストを検索する方法を示します。

例 2-1 データ・ディクショナリに関連するビューの検索

```
SQLPLUS SYSTEM
Enter password: password
Connected.

SQL> SELECT TABLE_NAME FROM DICTIONARY;
```

データ・ディクショナリ保護の有効化

O7_DICTIONARY_ACCESSIBILITY 初期化パラメータを有効にすることで、データ・ディクショナリを保護できます。このパラメータにより、ANY システム権限を持つユーザーがデータ・ディクショナリ（SYS スキーマ内のオブジェクト）に対してこれらの権限を使用することを防ぎます。

Oracle Database では非常に細かく権限を設定できます。通常 ANY 権限と呼ばれる権限は、このような権限の 1 つであり、一般的にアプリケーション所有者や各データベース管理者にのみ付与されます。たとえば、アプリケーション所有者に DROP ANY TABLE 権限を付与する場合があります。O7_DICTIONARY_ACCESSIBILITY 初期化パラメータを有効にすると、ANY 権限が偶発的または故意に使用されないように、Oracle データ・ディクショナリを保護することができます。

データ・ディクショナリ保護を有効にするには、次のようにします。

1. Oracle Enterprise Manager Database Control（Database Control）を起動します。

   Database Control を起動する手順については、『Oracle Database 2 日でデータベース管理者』を参照してください。

2. SYS としてログインし、SYSDBA 権限で接続します。

   - **ユーザー名**: 管理権限を持つユーザーの名前を入力します。この場合は、SYS と入力します。
   - **パスワード**: ユーザーのパスワードを入力します。
   - **接続モード**: リストから「**SYSDBA**」、「**SYSOPER**」または「**標準**」のいずれかを選択します。この場合は、「**SYSDBA**」を選択します。

   Oracle Enterprise Manager のデータベースのホームページ（データベースのホームページ）が表示されます。

3. 「**サーバー**」をクリックして、「サーバー」サブページを表示します。

4. 「データベース構成」セクションで**「初期化パラメータ」**をクリックします。

   「初期化パラメータ」ページが表示されます。

5. リストで、O7_DICTIONARY_ACCESSIBILITY を検索します。

   「名前」フィールドで O7_（O の文字）を入力し、**「実行」**をクリックします。パラメータ名の最初の数文字を入力できます。この場合、O7_ によって O7_DICTIONARY_ACCESSIBILTY パラメータが表示されます。

   パラメータによっては、「SPFile」サブページの値を変更する必要があります。**「SPFile」**タブをクリックし、「SPFile」サブページを表示します。

6. O7_DICTIONARY_ACCESSIBILTY の値を FALSE に設定します。

7. **「適用」**をクリックします。

8. Oracle Database インスタンスを再起動します。

   a. **「データベース・インスタンス」**リンクをクリックします。

   b. **「ホーム」**をクリックして Database Control のホームページを表示します。

   c. 「一般」で**「停止」**をクリックします。

   d. 資格証明の起動 / 停止ページでは、資格証明を入力します。

      詳細は、『Oracle Database 2 日でデータベース管理者』を参照してください。

   e. 完全に停止した後に、**「起動」**をクリックします。

O7_DICTIONARY_ACCESSIBILTY を FALSE に設定した後は、SELECT ANY DICTIONARY 権限を持つユーザーと、DBA 権限（CONNECT / AS SYSDBA など）の接続を認可されているユーザーのみが、データ・ディクショナリで ANY システム権限を使用できます。O7_DICTIONARY_ACCESSIBILITY パラメータが FALSE に設定されていない場合、DROP ANY TABLE（例）システム権限を持つユーザーはすべて、データ・ディクショナリの要素を削除できます。

注意：

- デフォルトのインストールでは、O7_DICTIONARY_ACCESSIBILITY パラメータは FALSE に設定されます。
- SELECT ANY DICTIONARY 権限は、GRANT ALL PRIVILEGES 文には含まれませんが、ロールを使用して付与できます。ロールについては、4-2 ページの「ユーザーへのロール付与のガイドライン」および『Oracle Database 2 日でデータベース管理者』を参照してください。

Oracle Database へのオペレーティング・システム・アクセスの保護のガイドライン

次のガイドラインに従うことにより、オペレーティング・システム・レベルで Oracle Database へのアクセスを保護できます。

- オペレーティング・システム・ユーザーの数を制限します。
- Oracle Database ホスト（物理コンピュータ）上のオペレーティング・システム・アカウントの権限（管理、root 権限または DBA）を制限します。ユーザーには、そのタスクの実行に必要な、最低限の権限のみを付与します。
- デフォルト・ファイル、Oracle Database ホーム（インストール）ディレクトリおよびそのコンテンツのディレクトリ権限を変更する権限を制限します。認可されたオペレーティング・システム・ユーザーや Oracle 所有者でも、オラクル社からの指示がないかぎり、これらの権限を変更してはいけません。
- シンボリック・リンクを制限します。データベースへのパスやファイルを作成するときに、ファイルおよびパスのいずれの部分も、信頼できないユーザーにより変更可能ではないこ

とを確認します。ファイルおよびパスのすべてのコンポーネントは、データベース管理者または *root* などの信頼できるアカウントにより所有されている必要があります。

この推奨は、データ・ファイル、ログ・ファイル、トレース・ファイル、外部表、BFILE など、すべてのタイプのファイルに適用されます。

ランタイム機能への権限付与のガイドライン

多くの Oracle Database 製品は、Oracle Java Virtual Machine（OJVM）などのランタイム機能を使用します。データベース・ランタイム機能には、すべての権限を割り当てないでください。かわりに、データベースの外部でファイルおよびパッケージを実行する可能性のある機能の明示的なドキュメント・ルート・ファイル・パスに特定の権限を付与します。

次に、個々のファイルが指定される脆弱なランタイム・コールの例を示します。

```
call dbms_java.grant_permission('wsmith',
 'SYS:java.io.FilePermission','filename','read');
```

次に、かわりにディレクトリ・パス（***太字***）を指定する、より適切な（よりセキュアな）ランタイム・コールの例を示します。

```
call dbms_java.grant_permission('wsmith',
 'SYS:java.io.FilePermission','directory_path','read');
```

インストール環境と構成のセキュリティに使用される初期化パラメータ

表 2-2 に、Oracle Database のインストール環境と構成を保護するために設定する初期化パラメータを示します。

表 2-2 インストール環境と構成のセキュリティに使用される初期化パラメータ

初期化パラメータ	デフォルト設定	説明
SEC_RETURN_SERVER_RELEASE_BANNER	FALSE	クライアント接続での製品バージョン情報（リリース番号など）の表示を制御します。侵入者は、データベースのリリース番号を使用して、データベース・ソフトウェアに存在するセキュリティ脆弱性に関する情報を検索できる場合があります。このパラメータを設定することで、詳細な製品バージョンの表示を有効または無効にできます。 このパラメータおよび類似パラメータの詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。このパラメータの詳細は、『Oracle Database リファレンス』を参照してください。
O7_DICTIONARY_ACCESSIBILITY	FALSE	SYSTEM 権限に対する制限を制御します。このパラメータの詳細は、2-4 ページの「データ・ディクショナリ保護の有効化」および『Oracle Database リファレンス』を参照してください。

関連項目： 初期化パラメータの詳細は、『Oracle Database リファレンス』を参照してください。

初期化パラメータ値の変更

ここでは、Database Control を使用して初期化パラメータの値を変更する方法を説明します。使用可能な初期化パラメータの詳細は、『Oracle Database リファレンス』を参照してください。

初期化パラメータ値を変更するには、次のようにします。

1. Database Control を起動します。
2. SYSDBA 権限を持つユーザー SYS としてログインします。
   - **ユーザー名** : SYS
   - **パスワード** : パスワードを入力します。
   - **接続モード** : SYSDBA
3. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
4. 「データベース構成」セクションで**「初期化パラメータ」**をクリックします。

   「初期化パラメータ」ページが表示されます。
5. **「名前」**フィールドに、変更するパラメータの名前を入力し、**「実行」**をクリックします。

   パラメータの最初の数文字を入力できます。たとえば、SEC_RETURN_SERVER_RELEASE_NUMBER パラメータを検索する場合は、SEC_RETURN と入力します。または、パラメータのリストをスクロールして、変更するパラメータを検索できます。

   パラメータによっては、「SPFile」サブページの値を変更する必要があります。**「SPFile」**タブをクリックし、「SPFile」サブページを表示します。
6. **「値」**フィールドで、新しい値を入力するか、リストが存在する場合はリストから選択します。
7. **「適用」**をクリックします。
8. パラメータが静的な場合は、Oracle Database インスタンスを再起動します。

   初期化パラメータが静的かどうかを調べるには、『Oracle Database リファレンス』の説明を確認してください。サマリー表の変更可能設定が「いいえ」の場合は、データベース・インスタンスを再起動する必要があります。

   a. **「データベース・インスタンス」**リンクをクリックします。
   b. **「ホーム」**をクリックして Database Control のホームページを表示します。
   c. 「一般」で**「停止」**をクリックします。
   d. 資格証明の起動 / 停止ページでは、資格証明を入力します。

      詳細は、『Oracle Database 2 日でデータベース管理者』を参照してください。
   e. 完全に停止した後に、**「起動」**をクリックします。

3

Oracle Database ユーザー・アカウントの保護

この章の内容は次のとおりです。

関連項目： ユーザー・アカウントの保護の詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。

Oracle Database ユーザー・アカウントの保護について

多くの方法を使用してデータベース・ユーザー・アカウントを保護できます。たとえば、Oracle Database には、パスワードに対する一連の組込み保護があります。この章では、デフォルトのデータベース・アカウントとパスワードを保護する方法およびデータベース・アカウントの管理方法について説明します。

『Oracle Database 2 日でデータベース管理者』では、ユーザー・アカウントの作成および管理の基礎（ユーザー・ロールの管理方法、管理アカウントの概要、パスワード・ポリシーの作成におけるプロファイルの使用方法など）について説明します。

ユーザー・アカウントを作成した後で、この項の手順を使用し、次の方法に従ってこれらのアカウントをより強力に保護できます。

- **事前定義データベース・アカウントの保護。**Oracle Database のインストール時に、事前定義済のアカウントが作成されます。パスワードを変更することで、これらのアカウントをできるだけ早く保護する必要があります。同じ方法を使用して、通常のユーザー・アカウント、管理アカウント、事前定義のアカウントのいずれであるかにかかわらず、すべてのパスワードを変更できます。このマニュアルでは、最もセキュアなパスワードを作成する方法のガイドラインも示します。
- **データベース・アカウントの管理。**データベース・アカウントを期限切れにしたり、ロックまたはロック解除できます。
- **パスワードの管理。**初期化パラメータなど、Oracle Database で提供されたツールを使用して、パスワードを管理および保護できます。

関連項目：

- ユーザー・アカウントおよび認証の管理の詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。
- Oracle Database のインストール時に作成される事前定義のユーザー・アカウントの詳細は、3-2 ページの「Oracle Database から提供される事前定義されるユーザー・アカウント」を参照してください。

Oracle Database から提供される事前定義されるユーザー・アカウント

Oracle Database をインストールすると、インストール・プロセスにより事前定義されたアカウントのセットが作成されます。これらのアカウントは次のカテゴリにあります。

- 事前定義された管理アカウント
- 事前定義された非管理ユーザー・アカウント
- 事前定義されたサンプル・スキーマ・ユーザー・アカウント

事前定義された管理アカウント

Oracle Database のデフォルトのインストールで、事前定義された管理アカウントのセットが提供されます。これらのアカウントには、SYS スキーマが所有するパッケージの EXECUTE 権限、CREATE ANY TABLE 権限、または ALTER SESSION のような、データベースの領域の管理に必要となる特別な権限を持ちます。管理アカウントのデフォルトの表領域は、SYSTEM か SYSAUX です。

これらのアカウントを無許可アクセスから保護するため、インストール・プロセスにより表 3-1 に示されたアカウントを除く、ほとんどのアカウントが期限切れにされ、ロックされます。データベース管理者は、3-8 ページの「データベース・アカウントの期限切れおよびロック」で説明されているとおりにアカウントのロックを解除し、リセットする責任があります。

表 3-1 に、Oracle Database で提供される管理ユーザー・アカウントを示します。

表 3-1 事前定義された Oracle Database の管理ユーザー・アカウント

ユーザー・アカウント	説明	インストール後のステータス
ANONYMOUS	Oracle XML DB への HTTP アクセスを許可するアカウント。EPG（Embedded PL/SQL Gateway）をデータベースにインストールするときに APEX_PUBLIC_USER アカウントのかわりに使用されます。 EPG は Oracle Database とともに使用される Web サーバーです。動的アプリケーションの作成に必要なインフラストラクチャを提供します。	期限切れおよびロック済
CTXSYS	Oracle Text を管理するためのアカウント。Oracle Text でテキスト問合せアプリケーションおよびドキュメント分類アプリケーションを作成できます。Oracle Text は、テキスト用の索引付け、語とテーマの検索および表示機能を提供します。 『Oracle Text アプリケーション開発者ガイド』を参照してください。	期限切れおよびロック済
DBSNMP	データベースの監視および管理を行うために Oracle Enterprise Manager の Management Agent のコンポーネントによって使用されるアカウント。 『Oracle Enterprise Manager Grid Control インストレーションおよび基本構成』を参照してください。	Open パスワードはインストール時またはデータベースの作成時に作成されます。
EXFSYS	Rules Manager 機能および Expression Filter 機能と関連付けられる EXFSYS スキーマにアクセスするために内部で使用されるアカウント。この機能により複雑な PL/SQL のルールおよび表現を構築できます。EXFSYS には Rules Manager や Expression Filter の DDL、DML、および関連するメタデータが含まれています。 『Oracle Database Rules Manager および Expression Filter 開発者ガイド』を参照してください。	期限切れおよびロック済
LBACSYS	Oracle Label Security (OLS) を管理するためのアカウント。Label Security オプションをインストールするときのみ作成されます。 6-20 ページの「Oracle Label Security による行レベルのセキュリティの強制」および『Oracle Label Security 管理者ガイド』を参照してください。	期限切れおよびロック済
MDSYS	Oracle Spatial および Oracle Multimedia Locator 管理者アカウント。 『Oracle Spatial 開発者ガイド』を参照してください。	期限切れおよびロック済
MGMT_VIEW	Oracle Enterprise Manager Database Control で使用されるアカウント。	Open パスワードはインストール時またはデータベースの作成時にランダムに生成されます。ユーザーがこのパスワードを知る必要はありません。
OLAPSYS	OLAP カタログ（CWMLite）を所有するアカウント。このアカウントは、非推奨となりましたが、下位互換性のために保持されています。	期限切れおよびロック済

表 3-1 事前定義された Oracle Database の管理ユーザー・アカウント（続き）

ユーザー・アカウント	説明	インストール後のステータス
OWBSYS	Oracle Warehouse Builder のリポジトリを管理するためのアカウント。 インストール中にこのアカウントにアクセスし、リポジトリのベース言語を定義し、Warehouse Builder の作業領域とユーザーを定義します。データ・ウェアハウスは問合せおよび分析のために設計されたリレーショナル・データベースまたは多次元データベースです。 『Oracle Warehouse Builder インストレーションおよび管理ガイド』を参照してください。	期限切れおよびロック済
ORDPLUGINS	Oracle Multimedia ユーザー。Oracle およびサード・パーティにより提供されたプラグイン（フォーマット・プラグイン）はこのスキーマにインストールされています。 Oracle Multimedia により Oracle Database で画像、音声、動画、DICOM フォーマットの医療用画像などのオブジェクトや、その他の企業情報と統合された異機種間のメディア・データを格納、管理および取得できます。 『Oracle Multimedia ユーザーズ・ガイド』および『Oracle Multimedia リファレンス』を参照してください。	期限切れおよびロック済
ORDSYS	Oracle Multimedia 管理者アカウント。 『Oracle Multimedia ユーザーズ・ガイド』、『Oracle Multimedia リファレンス』および『Oracle Multimedia DICOM 開発者ガイド』を参照してください。	期限切れおよびロック済
OUTLN	プランの安定性をサポートするアカウント。プランの安定性により、ストアド・アウトラインに実行プランが保存され、特定のデータベースの環境の変更がアプリケーションのパフォーマンス特性に影響するのを防ぎます OUTLN は格納されたストアド・アウトラインに関連付けられたメタデータをメインで管理するロールとして動作します。 『Oracle Database パフォーマンス・チューニング・ガイド』を参照してください。	期限切れおよびロック済
SI_INFORMTN_SCHEMA	SQL/MM Still Image Standard 向けの情報ビューを保存しているアカウント。 『Oracle Multimedia ユーザーズ・ガイド』および『Oracle Multimedia リファレンス』を参照してください。	期限切れおよびロック済
SYS	データベース管理タスクの実行に使用されるアカウント。 『Oracle Database 2 日でデータベース管理者』を参照してください。	Open パスワードはインストール時またはデータベースの作成時に作成されます。
SYSMAN	Oracle Enterprise Manager データベースの管理タスクの実行に使用するアカウント。SYS および SYSTEM のアカウントでもこれらのタスクを実行できます。 『Oracle Enterprise Manager Grid Control インストレーションおよび基本構成』を参照してください。	Open パスワードはインストール時またはデータベースの作成時に作成されます。
SYSTEM	Oracle Database のデフォルトの汎用データベース管理者アカウント。 本番システムでは、データベース管理操作用に汎用 SYSTEM アカウントを使用せずに、個々のデータベース管理者アカウントを作成することをお薦めします。 『Oracle Database 2 日でデータベース管理者』を参照してください。	Open パスワードはインストール時またはデータベースの作成時に作成されます。

表 3-1 事前定義された Oracle Database の管理ユーザー・アカウント（続き）

ユーザー・アカウント	説明	インストール後のステータス
TSMSYS	透過的なセッション移行（Transparent Session Migration: TSM）に使用されるアカウント。	期限切れおよびロック済
WK_TEST	デフォルトのインスタンス（WK_INST）のインスタンス管理者。このアカウントのロックを解除し、このユーザーにパスワードを割り当ててから、管理ツールの「インスタンスの編集」ページを使用して、キャッシュ済のスキーマ・パスワードを更新する必要があります。 Ultra Search は、Oracle Database、その他の ODBC 準拠のデータベース、IMAP メール・サーバー、Web サーバーで管理される HTML ドキュメント、ディスク上のファイルなどの複数のリポジトリに対する統一された検索機能および位置特定機能を提供します。 『Oracle Ultra Search 管理者ガイド』を参照してください。	期限切れおよびロック済
WKSYS	Ultra Search データベースのスーパーユーザー。WKSYS はスーパーユーザー権限を WK_TEST などの他のユーザーに付与できます。すべての Oracle Ultra Search データベース・オブジェクトは、WKSYS スキーマにインストールされます。 『Oracle Ultra Search 管理者ガイド』を参照してください。	期限切れおよびロック済
WKPROXY	Oracle9*i* Application Server Ultra Search の管理アカウント。 『Oracle Ultra Search 管理者ガイド』を参照してください。	期限切れおよびロック済
WMSYS	Oracle Workspace Manager のメタデータ情報の格納に使用されるアカウント。 『Oracle Database Workspace Manager 開発者ガイド』を参照してください。	期限切れおよびロック済
XDB	Oracle XML DB データおよびメタデータの保存に使用されるアカウント。 Oracle XML DB は Oracle Database のデータに対し、パフォーマンスの高い XML の格納および取得を提供します。 『Oracle XML DB 開発者ガイド』を参照してください。	期限切れおよびロック済

事前定義された非管理ユーザー・アカウント

表 3-2 には、Oracle Database をインストールするときに作成されるデフォルトの非管理ユーザー・アカウントがリストされています。非管理ユーザー・アカウントはジョブの実行に最低限必要な権限のみ所有します。デフォルトの表領域は USERS です。

これらのアカウントを無許可アクセスから保護するため、インストール・プロセスにより表 3-2 に示されたアカウントを除く、ほとんどのアカウントがインストール後すぐにロックされ、期限切れになります。データベース管理者は、3-8 ページの「データベース・アカウントの期限切れおよびロック」で説明されているとおりにアカウントのロックを解除し、リセットする責任があります。

表 3-2 事前定義された Oracle Database の非管理ユーザー・アカウント

ユーザー・アカウント	説明	インストール後のステータス
APEX_PUBLIC_USER	Oracle Database Application Express のアカウント。このアカウントはデータベース・アクセス記述子（DAD）でデータベースに接続するために使用する Oracle のスキーマの指定に使用します。 Oracle Application Express は Oracle Database 用の迅速な Web アプリケーション開発ツールです。 『Oracle Database Application Express ユーザーズ・ガイド』を参照してください。	期限切れおよびロック済
DIP	Oracle Label Security とともにインストールされる Oracle Directory Integration and Provisioning（DIP）のアカウント。このプロファイルは Oracle Internet Directory が有効な Oracle Label Security のインストール・プロセスの一部として自動的に作成されます。 『Oracle Label Security 管理者ガイド』を参照してください。	期限切れおよびロック済
FLOWS_30000	Oracle Database Application Express のインストール中に作成されるほとんどのデータベース・オブジェクトを所有するアカウント。オブジェクトには、表、ビュー、トリガー、索引、パッケージなどが含まれます。 『Oracle Database Application Express ユーザーズ・ガイド』を参照してください。	期限切れおよびロック済
FLOWS_FILES	ファイルのアップロードやダウンロードなど modplsql のドキュメント転送に関連する Oracle Database Application のインストール中に作成されるデータベース・オブジェクトを所有するアカウント。オブジェクトには表、ビュー、トリガー、索引、パッケージなどが含まれます。 『Oracle Database Application Express ユーザーズ・ガイド』を参照してください。	期限切れおよびロック済
MDDATA	格納されるジオコーダおよびルーターのデータ用に Oracle Spatial に使用されるスキーマ。 Oracle Spatial は SQL スキーマおよびファンクションを提供し、これにより Oracle Database の Spatial 機能の格納、取得、更新、問合せができます。 『Oracle Spatial 開発者ガイド』を参照してください。	期限切れおよびロック済
ORACLE_OCM	Oracle Configuration Manager と使用するアカウント。この機能により現在の Oracle Database インスタンスの構成情報を Oracle*MetaLink* と関連付けることができます。サービス・リクエストを記録すると、データベース・インスタンスの構成情報と関連付けられます。 使用しているプラットフォームの『Oracle Database インストレーション・ガイド』を参照してください。	期限切れおよびロック済
PUBLIC	PUBLIC ユーザー・グループに使用するアカウント。 インストールにおいてこのアカウントは Oracle Universal Installer によりロックされたり期限切れになることはありません。ステータスは OPEN です。 『Oracle Database セキュリティ・ガイド』を参照してください。	期限切れおよびロック済

表 3-2 事前定義された Oracle Database の非管理ユーザー・アカウント（続き）

ユーザー・アカウント	説明	インストール後のステータス
SPATIAL_CSW_ADMIN_USR	CSW（Catalog Services for the Web）アカウント。このアカウントは Oracle Spatial CSW Cache Manager により、データベースからすべてのレコード・タイプのメタデータとレコード・インスタンスを、キャッシュされたレコード・タイプのメイン・メモリーにロードするために使用されます。 『Oracle Spatial 開発者ガイド』を参照してください。	期限切れおよびロック済
SPATIAL_WFS_ADMIN_USR	WFS（Web Feature Service）アカウント。このアカウントは Oracle Spatial WFS Cache Manager により、データベースからすべての機能タイプのメタデータと機能インスタンスを、キャッシュされた機能タイプのメイン・メモリーにロードするために使用されます。 『Oracle Spatial 開発者ガイド』を参照してください。	期限切れおよびロック済
XS$NULL	セッション内にユーザーが存在しないことを表す内部アカウント。XS$NULL は、ユーザーではないため、Oracle Database インスタンスによってのみアクセスできます。XS$NULL には権限がなく、XS$NULL として認証したり、XS$NULL に認証資格証明を割り当てることはできません。	期限切れおよびロック済

事前定義されたサンプル・スキーマ・ユーザー・アカウント

このマニュアルの例を完了するために実行する必要があるサンプル・スキーマをインストールすると、Oracle Database はサンプル・ユーザー・アカウントのセットを作成します。サンプル・スキーマ・ユーザー・アカウントはすべて非管理アカウントで、表領域は USERS です。

これらのアカウントを無許可アクセスから保護するため、インストール・プロセスによりこれらのアカウントがインストール直後にロックされ、期限切れになります。データベース管理者は、3-8 ページの「データベース・アカウントの期限切れおよびロック」で説明されているとおりにアカウントのロックを解除し、リセットする責任があります。サンプル・スキーマ・アカウントの詳細は『Oracle Database サンプル・スキーマ』を参照してください。

表 3-3 には様々な製品を製造している架空の企業の個別の部門を表すサンプル・スキーマ・ユーザー・アカウントがリストされています。

表 3-3 デフォルトのサンプル・スキーマ・ユーザー・アカウント

ユーザー・アカウント	説明	インストール後のステータス
BI	Oracle サンプル・スキーマに含まれている BI（Business Intelligence）スキーマを所有するアカウント。 『Oracle Warehouse Builder ユーザーズ・ガイド』を参照してください。	期限切れおよびロック済
HR	HR（Human Resources）スキーマを管理するためのアカウント。このスキーマには企業の従業員および施設に関する情報が格納されます。	期限切れおよびロック済
OE	OE（Order Entry）スキーマを管理するためのアカウント。このスキーマには製品のインベントリや、様々なチャネルによる製品の売上が格納されます。	期限切れおよびロック済
PM	PM（Product Media）スキーマを管理するためのアカウント。このスキーマには企業が販売した各製品の説明と詳細情報が含まれます。	期限切れおよびロック済
IX	IX（Information Exchange）スキーマを管理するためのアカウント。このスキーマにより B2B（Business-to-Business）アプリケーションを介した発送が管理されます。	期限切れおよびロック済
SH	SH（Sales）スキーマを管理するためのアカウント。このスキーマにはビジネス上の決断を容易にするビジネス戦略が格納されます。	期限切れおよびロック済

サンプル・スキーマ・アカウントに加えて、Oracle Database では別のサンプル・スキーマ・アカウント（SCOTT）が提供されます。SCOTT スキーマには、表 EMP、DEPT、SALGRADE および BONUS が含まれています。SCOTT アカウントは Oracle Database のドキュメント・セット全体の例で使用されます。Oracle Database をインストールすると、SCOTT アカウントはロックされ、期限が切れます。

データベース・アカウントの期限切れおよびロック

『Oracle Database 2 日でデータベース管理者』では、Database Control を使用してデータベース・アカウントのロックを解除する方法を説明します。また、Database Control を使用して、データベース・アカウントを期限切れにしたり、ロックすることもできます。

ユーザーのパスワードを期限切れにすると、パスワードは存在しなくなります。パスワードを期限切れにしない場合は、そのアカウントのパスワードを変更します。アカウントをロックすると、他のアカウント情報と同じようにユーザー・パスワードも保持されますが、そのアカウントを使用してデータベースにログインするユーザーに対してアカウントが使用不可になります。ロックを解除すると、アカウントは再度使用可能になります。

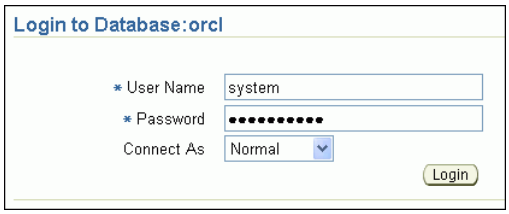
データベース・アカウントの期限切れおよびロックを実行するには、次のようにします。

1. Database Control を起動します。

   Database Control を起動する手順については、『Oracle Database 2 日でデータベース管理者』を参照してください。

2. 管理者権限を使用してログインします。

   次に例を示します。



   データベースのホームページが表示されます。

3. **「サーバー」**をクリックして、「サーバー」サブページを表示します。

4. 「セキュリティ」セクションで**「ユーザー」**をクリックします。

   「ユーザー」ページに、現行のデータベース・インスタンスで作成されたユーザー・アカウントが表示されます。「アカウント・ステータス」列は、アカウントが期限切れか、ロックされているか、オープンかを表します。

5. 「選択」列で期限切れにするアカウントを選択し、**「編集」**をクリックします。

   「ユーザーの編集」ページが表示されます。

6. 次のいずれかの操作を行います。

   - パスワードを期限切れにするには、**「期限切れパスワード」**をクリックします。

     パスワードが期限切れにならないようにするには、**「パスワードの入力」**および**「パスワードの確認」**フィールドに新しいパスワードを入力します。パスワードの要件については、3-9 ページの「パスワードの作成要件」を参照してください。

   - アカウントをロックするには、**「ロック」**を選択します。

7. **「適用」**をクリックします。

パスワードの作成要件

ユーザー・アカウントを作成すると、Oracle Database によって、そのユーザーのデフォルトのパスワード・ポリシーが割り当てられます。パスワード・ポリシーは、最低文字数や有効期限など、パスワードの作成方法に関するルールを定義します。パスワード・ポリシーを使用してパスワードを強化できます。

パスワードは 30 文字以内にする必要があります。ただし、セキュリティを考慮して、次の追加のガイドラインに従います。

- パスワードは 10 ～ 30 文字の英数字で指定します。
- パスワードには、大／小文字および特殊文字を使用します。（詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。）
- パスワードの文字には、データベースのキャラクタ・セットを使用します。これには、アンダースコア（_）、ドル記号（$）およびシャープ記号（#）の文字を含めることができます。
- 実在する単語をパスワードに使用しないでください。

パスワードをさらにセキュアなものにする方法については、『Oracle Database セキュリティ・ガイド』を参照してください。

関連項目：

- ユーザー・パスワードの変更の詳細は、3-9 ページの「デフォルト・パスワードの検索および変更」を参照してください。
- アカウントのロックおよびパスワードの期限切れの詳細は、3-8 ページの「データベース・アカウントの期限切れおよびロック」を参照してください。
- Oracle Database のインストール時に作成される事前定義のユーザー・アカウントの詳細は、3-2 ページの「Oracle Database から提供される事前定義されるユーザー・アカウント」を参照してください。
- パスワード・ポリシーの概要は、『Oracle Database 2 日でデータベース管理者』を参照してください。
- パスワードの管理の詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。

デフォルト・パスワードの検索および変更

Oracle Database では、管理アカウントを含むデータベース・ユーザー・アカウントがデフォルト・パスワードなしでインストールされます。インストール時に、そのアカウント（常に管理アカウント）のパスワードを作成します。作成しない場合は、Oracle Database によって、パスワードが期限切れになった状態でロックされたデフォルト・アカウント（サンプル・スキーマ内のアカウントなど）がインストールされます。

以前のリリースの Oracle Database からアップグレードした場合、デフォルト・パスワードを持つデータベース・アカウントが存在する場合があります。これらのデフォルト・アカウント（HR、OE、SCOTT アカウントなど）は、データベースの作成時に作成されます。

セキュリティは、デフォルトのデータベース・ユーザー・アカウントがインストール後もデフォルト・パスワードを使用していると、最も容易に危険にさらされます。ユーザー・アカウント SCOTT はよく知られているアカウントで侵入されやすい可能性があるため、これが特に当てはまります。デフォルト・パスワードが使用されているアカウントを検索してから、そのパスワードを変更します。

デフォルト・パスワードを検索して変更するには、次のようにします。

1. 管理者権限を使用して SQL*Plus にログインします。

```
SQLPLUS SYSTEM
Enter password: password
```

2. DBA_USERS_WITH_DEFPWD データ・ディクショナリ・ビューから選択します。

   ```
   SELECT * FROM DBA_USERS_WITH_DEFPWD;
   ```

   DBA_USERS_WITH_DEFPWD には、ユーザー・デフォルト・パスワードを持つアカウントが表示されます。次に例を示します。

   ```
   USERNAME
   ------------
   SCOTT
   ```

3. DBA_USERS_WITH_DEFPWD データ・ディクショナリ・ビューに表示されたアカウントのパスワードを変更します。

   たとえば、ユーザー SCOTT のパスワードを変更するには、次のように入力します。

   ```
   PASSWORD SCOTT
   Changing password for SCOTT
   New password: password
   Retype new password: password
   Password changed
   ```

   3-9 ページの「パスワードの作成要件」に示されているガイドラインに従って、*password* をセキュアなパスワードに置き換えます。セキュリティを考慮して、以前のリリースの Oracle Database で使用していたパスワードと同じパスワードは再使用しないでください。

   また、パスワードは、ALTER USER SQL 文を使用して変更することもできます。

   ```
   ALTER USER SCOTT IDENTIFIED BY password;
   ```

管理権限がある場合は、Database Control を使用して、（デフォルトのユーザー・アカウントのパスワードのみでなく）ユーザー・アカウントのパスワードを変更できます。個々のユーザーが Database Control を使用して自分のパスワードを変更することもできます。

Database Control を使用してデータベース・アカウントのパスワードを変更するには、次のようにします。

1. Database Control を起動します。

   Database Control を起動する手順については、『Oracle Database 2 日でデータベース管理者』を参照してください。

2. 管理者のユーザー名とパスワード（SYSTEM など）を入力し、**「ログイン」**をクリックします。

3. **「サーバー」**をクリックして、「サーバー」サブページを表示します。

4. 「セキュリティ」セクションで**「ユーザー」**をクリックします。

   「ユーザー」ページに、現行のデータベース・インスタンスで作成されたユーザー・アカウントが表示されます。「アカウント・ステータス」列は、アカウントが期限切れか、ロックされているか、オープンかを表します。

5. 「選択」列で変更するアカウントを選択し、**「編集」**をクリックします。

   「ユーザーの編集」ページが表示されます。

6. **「パスワードの入力」**および**「パスワードの確認」**フィールドに新しいパスワードを入力します。

7. **「適用」**をクリックします。

関連項目：

- パスワード保護を設定する他の方法については、『Oracle Database セキュリティ・ガイド』を参照してください。
- 3-2 ページの「Oracle Database から提供される事前定義されるユーザー・アカウント」

デフォルト管理ユーザー・パスワードの処理のガイドライン

SYS、SYSTEM、SYSMAN、DBSNMP 管理アカウントでは、同じパスワードを使用することも異なるパスワードを使用することもできますが、各アカウントに別々のパスワードを使用することをお薦めします。どのような Oracle 環境（本番環境もしくはテスト環境）でも、これらの管理者アカウントには強力でセキュアな固有のパスワードを割り当ててください。Database Configuration Assistant を使用して新規データベースを作成する場合は、SYS アカウントおよび SYSTEM アカウントのパスワードを作成する必要があります。

同様に、本番環境では、SYSMAN および DBSNMP を含むすべての管理者アカウントでデフォルト・パスワードを使用しないでください。Oracle Database 11*g* リリース 1（11.1）以上では、デフォルト・パスワードを持つこれらのアカウントはインストールされませんが、以前のリリースの Oracle Database からアップグレードした場合、デフォルト・パスワードを使用するアカウントが存在している可能性があります。これらのアカウントは、3-9 ページの「デフォルト・パスワードの検索および変更」の手順を使用して検索および変更する必要があります。

データベース作成の最後に、Database Configuration Assistant により、SYS および SYSTEM ユーザー・アカウントの新しいパスワードの入力および確認を要求するページが表示されます。

管理ユーザー・パスワードは、インストール後に Database Control を使用して変更できます。パスワード変更の詳細は、3-9 ページの「デフォルト・パスワードの検索および変更」を参照してください。

パスワード管理の強制のガイドライン

すべてのユーザー・パスワードに基本的なパスワード管理ルール（パスワードの長さ、履歴、複雑度など）を適用します。Oracle Database では、デフォルト・プロファイルでパスワード・ポリシーが有効になります。パスワード・ポリシーを作成するためのガイドラインについては、3-9 ページの「パスワードの作成要件」を参照してください。パスワードの管理を実行するために設定する初期化パラメータについては、3-12 ページの表 3-4 を参照してください。

DBA_USERS ビューを問い合せることで、ユーザー・アカウントに関する情報を検索できます。このビューには、パスワードの列が含まれていますが、セキュリティを高めるために、Oracle Database はこの列のデータを暗号化します。DBA_USERS ビューでは、ユーザー・アカウント・ステータス、アカウントがロックされているかどうか、パスワードのバージョンなど、有用な情報が提供されます。DBA_USERS は次のように問い合せることができます。

```
SQLPLUS SYSTEM
Enter password: password
Connected.

SQL> SELECT * FROM DBA_USERS;
```

また、可能な場合は、ネットワーク認証サービス（Kerberos など）、トークン・カード、スマート・カードあるいは X.509 証明書とともに、Oracle Advanced Security（Oracle Database Enterprise Edition のオプション）を使用することをお薦めします。これらのサービスはユーザーの厳密な認証を可能にし、Oracle Database への無許可アクセスに対してより強力な保護を実現します。

関連項目：

- パスワードの管理の詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。
- ユーザーおよびプロファイルに関する情報を検索するために問い合せることができる追加のビューについては、『Oracle Database セキュリティ・ガイド』を参照してください。
- Oracle Database Advanced Security の詳細は、『Oracle Database Advanced Security 管理者ガイド』を参照してください。

ユーザー・アカウントの保護に使用されるパラメータ

表 3-4 に、ユーザー・アカウントを保護するために設定する初期化パラメータおよびプロファイル・パラメータを示します。

表 3-4 ユーザー・アカウント・セキュリティに使用される初期化パラメータおよびプロファイル・パラメータ

パラメータ	デフォルト設定	説明
SEC_CASE_SENSITIVE_LOGON	TRUE	パスワードの大文字と小文字の区別を管理します。TRUE で大文字と小文字の区別が有効になります。FALSE で区別が無効になります。
SEC_MAX_FAILED_LOGIN_ATTEMPTS	デフォルト設定なし	アプリケーションへの接続時にユーザーが失敗できる最大の回数を設定します。
FAILED_LOGIN_ATTEMPTS	10	ユーザー・ログインが何度も失敗した場合に、アカウントがロックされるまでの最大の回数を設定します。 **注意：** SEC_MAX_FAILED_LOGIN_ATTEMPTS 初期化パラメータを使用して、権限のないユーザー（おそらく侵入者）が Oracle Call Interface アプリケーションへのログインを試行する最大回数の制限も設定できます。
PASSWORD_GRACE_TIME	7	パスワードが期限切れになる前に、パスワードを変更する猶予期間の日数を設定します。
PASSWORD_LIFE_TIME	180	現行のパスワードを使用できる日数を設定します。
PASSWORD_LOCK_TIME	1	ログインが指定回数以上失敗した場合にユーザー・アカウントをロックする日数を設定します。
PASSWORD_REUSE_MAX	UNLIMITED	パスワードの再使用が許可される日数を設定します。
PASSWORD_REUSE_TIME	UNLIMITED	現行のパスワードの再使用が許可されるまでに必要なパスワードの変更回数を設定します。

注意： これらのパラメータのほとんどは、ユーザー・プロファイルを作成するために使用できます。ユーザー・プロファイル設定の詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。

初期化パラメータを変更するには、2-7 ページの「初期化パラメータ値の変更」を参照してください。初期化パラメータの詳細は、『Oracle Database リファレンス』および『Oracle Database 管理者ガイド』を参照してください。

4

ユーザー権限の管理

この章の内容は次のとおりです。

関連項目：

- 『Oracle Database セキュリティ・ガイド』
- 『Oracle Label Security 管理者ガイド』

権限管理について

ユーザー権限は、次のように制御できます。

- **個々の権限の付与および取消し。**UPDATE SQL 文を実行する権限など、個々の権限を個々のユーザーまたはユーザーのグループに付与できます。
- **ロールの作成と権限の割当て。**ロールは、ユーザーまたは他のロールに一括で付与する関連権限の名前付きグループです。
- **セキュア・アプリケーション・ロールの作成。**セキュア・アプリケーション・ロールを使用すると、データベース・ロールを有効にできるタイミングを制御する条件を定義できます。たとえば、セキュア・アプリケーション・ロールを使用すると、ユーザー・セッションでデータベース・ロールを有効にするのを許可する前に、そのセッションに関連する IP アドレスをチェックできます。

権限付与のガイドライン

権限は、表の更新や削除などの特定のアクションを実行する権利であるため、データベース・ユーザーに必要以上の権限は付与しないでください。権限の管理の概要は、『Oracle Database 2 日でデータベース管理者』の「ユーザー権限とロールについて」を参照してください。『Oracle Database 2 日でデータベース管理者』では、権限を付与する方法の例も示されています。

つまり、最小権限の原則とは、ユーザーに、効率的かつ簡潔に作業を行うために実際に必要な権限のみを与えることです。最小権限の原則を実践するために、次の制限を可能なかぎり行ってください。

- データベース・ユーザーに付与する SYSTEM 権限と OBJECT 権限の数。
- データベースに SYS 権限で接続するユーザーの数。

たとえば、通常、CREATE ANY TABLE 権限はデータベース管理者権限を持っていないユーザーには付与されません。

PUBLIC ユーザー・グループの権限処理のガイドライン

データベース・サーバーのユーザー・グループ PUBLIC から、不要な権限とロールを削除する必要があります。PUBLIC は Oracle Database ですべてのユーザーに付与されるデフォルト・ロールとして機能します。どのデータベース・ユーザーも、PUBLIC に付与される権限を使用できます。これらの権限には、様々な PL/SQL パッケージでの EXECUTE が含まれ、最小権限のユーザーにより、直接アクセスを許可されていない関数がアクセスおよび実行される可能性があります。

ユーザーへのロール付与のガイドライン

ロールは、ユーザーまたは他のロールに一括して付与する関連権限の名前付きグループです。ロールの管理の基礎については、『Oracle Database 2 日でデータベース管理者』の「ロールの管理」を参照してください。『Oracle Database 2 日でデータベース管理者』の「例 : ロールの作成」も参照してください。

ロールを使用することで、迅速かつ容易にユーザーに権限を付与できます。Oracle Database で定義されているロールを使用することもできますが、必要な権限のみを含む独自のロールを作成すると、より継続的な制御が可能になります。Oracle Database で定義済の CONNECT ロールの権限は変更または削除される可能性があります。このロールには現在、CREATE SESSION 権限しかありません。以前は他に 8 個の権限がありました。

定義したロールに含まれる権限が、特定の職務に必要な権限のみであることを確認します。アプリケーション・ユーザーに既存のロールに含まれるすべての権限が必要ない場合は、適切な権限のみを付与できる別のロールを適用するか、権限をさらに制限するロールを作成して割り当てます。

たとえば、ユーザー SCOTT はよく知られているデフォルトのユーザー・アカウントで、侵入されやすい可能性があるため、このユーザーの権限を厳密に制限する必要があります。CREATE

DBLINK 権限ではあるデータベースから別のデータベースへのアクセスが許可されるため、SCOTT に対するこの権限を削除します。次にユーザーに付与されたロール全体を削除します。これは、ロールによって付与される権限は、個別に削除できないためです。必要な権限のみを含む独自のロールを再作成し、新しいロールをユーザーに付与します。同様に、セキュリティを高めるために、CREATE DBLINK 権限を必要としないすべてのユーザーからこの権限を削除します。

セキュア・アプリケーション・ロールによるアプリケーション・アクセスの制御

セキュア・アプリケーション・ロールは、認可された PL/SQL パッケージによってのみ有効にできるロールです。PL/SQL パッケージ自体は、アプリケーションへのアクセスを制御するために必要なセキュリティ・ポリシーを反映します。

この項の内容は次のとおりです。

セキュア・アプリケーション・ロールについて

セキュア・アプリケーション・ロールは、認可された PL/SQL パッケージによってのみ有効にできるロールです。このパッケージは、アプリケーションへのアクセスを制御する 1 つ以上のセキュリティ・ポリシーを定義します。ロールおよびパッケージは通常、作成者（通常はセキュリティ管理者）のスキーマに作成されます。セキュリティ管理者は、データベースのセキュリティを維持する責任があるデータベース管理者です。

セキュア・アプリケーション・ロールを使用する利点は、ロール自体に付与された権限に加えて、アプリケーション・アクセスにセキュリティの追加レイヤーを作成できることです。セキュア・アプリケーション・ロールを使用すると、パスワードがアプリケーション・ソース・コードに埋め込まれたり表に格納されないため、セキュリティが強化されます。このため、データベースが行う決定はセキュリティ・ポリシーの実装に基づいて行われます。これらの定義はアプリケーションではなくデータベースにまとめて格納されるため、各アプリケーションのポリシーを変更するのではなく、このポリシーを一度に変更します。ポリシーはロールにバインドされているため、データベースに接続しているユーザー数に関係なく、結果は常に同じになります。

セキュア・アプリケーション・ロールには次のコンポーネントがあります。

- **セキュア・アプリケーション・ロール自体。**このロールを作成するには、CREATE ROLE 文を IDENTIFIED USING 句とともに使用して PL/SQL パッケージに関連付けます。次に、一般的にロールに付与する権限をこのロールに付与します。

  このロールをユーザーに直接付与しないでください。この作業は PL/SQL パッケージが行います。ただし、サイトのポリシーがユーザーにロールを付与するものである場合は、ユーザー・アカウントの変更でデフォルトのロールを使用しないかぎり、セキュア・アプリケーション・ロールをユーザーに付与することも可能です。次はその例です。

  ```
  ALTER USER psmith DEFAULT ROLE NONE;
  ```

- **セキュア・アプリケーション・ロールに関連付ける PL/SQL パッケージ、プロシージャまたはファンクション。**PL/SQL パッケージは、データベースへのログインを試行する人物にロールを付与またはロールを拒否する条件を設定します。PL/SQL パッケージ、プロシージャまたはファンクションは、定義者の権限ではなく実行者の権限を使用して作成する必要があります。実行者の権限では、パッケージがアクセスするすべてのオブジェクトに対する EXECUTE 権限がユーザーに与えられます。実行者の権限のプロシージャは現行ユーザー（プロシージャを実行したユーザー）の権限で実行されます。このようなプロシージャは、特定のスキーマにバインドされません。様々なユーザーがこのようなプロシージャを実行でき、集中化されたアプリケーション・ロジックを使用することで複数のユーザーが自身のデータを管理できます。実行者の権限のパッケージを作成するには、プロシージャ・コードの宣言部で AUTHID CURRENT_USER 句を使用します。

ユーザーのロールを有効（または無効）にするために、PL/SQL パッケージには DBMS_SESSION.SET_ROLE コールも含まれている必要があります。

PL/SQL パッケージを作成してから、適切なユーザーにパッケージに対する EXECUTE 権限を付与する必要があります。

- **ユーザーがログオンしたときに PL/SQL パッケージを実行する方法。** PL/SQL パッケージを実行するには、ユーザーがロールによって付与される権限を使用する前に、アプリケーションから直接 PL/SQL パッケージをコールする必要があります。ユーザーがログオンしたときに PL/SQL パッケージを自動的に実行するログオン・トリガーは使用できません。

ユーザーがアプリケーションにログインすると、必要に応じて、パッケージ内のポリシーによるチェックが行われます。チェックを通過したユーザーにはロールが付与され、アプリケーションへのアクセスが許可されます。ユーザーがチェックを通過できない場合、アプリケーションへのアクセスは拒否されます。

チュートリアル : セキュア・アプリケーション・ロールの作成

このチュートリアルでは、2 人のユーザー Matthew Weiss と Winston Taylor が OE.ORDERS 表から情報を取得する場合を説明します。この表へのアクセス権は、EMPLOYEE_ROLE セキュア・アプリケーション・ロールで定義されています。Matthew は Winston のマネージャで、OE.ORDERS 表内の情報にアクセスできます。Winston は情報にアクセスできません。

このチュートリアルでは、次の手順を実行します。

- 手順 1: セキュリティ管理者アカウントを作成する
- 手順 2: このチュートリアルで使用するユーザー・アカウントを作成する
- 手順 3: セキュア・アプリケーション・ロールを作成する
- 手順 4: 参照表を作成する
- 手順 5: PL/SQL プロシージャを作成してセキュア・アプリケーション・ロールを設定する
- 手順 6: Matthew と Winston のプロシージャに EXECUTE 権限を付与する
- 手順 7: EMPLOYEE_ROLE セキュア・アプリケーション・ロールをテストする
- 手順 8: このチュートリアルで使用したコンポーネントを削除する（オプション）

手順 1: セキュリティ管理者アカウントを作成する

セキュリティを強化するためには、システム管理者に職務を割り当てる際に、責務分離の概念を取り入れる必要があります。このマニュアルのチュートリアルでは、sec_admin というセキュリティ管理者アカウントを作成し、使用します。

sec_admin セキュリティ管理者アカウントを作成するには、次のようにします。

1. Database Control を起動します。

   Database Control を起動する手順については、『Oracle Database 2 日でデータベース管理者』を参照してください。

2. 管理者のユーザー名（SYSTEM など）とパスワードを入力し、**「ログイン」**をクリックします。

   データベースのホームページが表示されます。

3. **「サーバー」**をクリックして、「サーバー」サブページを表示します。

4. 「セキュリティ」で、**「ユーザー」**を選択します。

   「ユーザー」ページが表示されます。

5. **「作成」**をクリックします。

   「ユーザーの作成」ページが表示されます。

6. 次の情報を入力します。
   - **名前**: sec_admin
   - **プロファイル**: デフォルト
   - **認証**: パスワード
   - **「パスワードの入力」**および**「パスワードの確認」**: 3-9 ページの「パスワードの作成要件」に示されている要件を満たすパスワードを入力します。
   - **デフォルト表領域**: SYSTEM
   - **一時表領域**: TEMP
   - **ステータス**: ロック解除
7. **「システム権限」**をクリックして、「システム権限」サブページを表示します。
8. **「リストを編集」**をクリックします。

   「システム権限の変更」ページが表示されます。
9. 「使用可能なシステム権限」リストから次の権限を選択し、**「移動」**をクリックして「選択したシステム権限」リストに移動します（複数の権限は [Ctrl] キーを押しながら選択します）。
   - CREATE PROCEDURE
   - CREATE ROLE
   - CREATE SESSION
   - SELECT ANY DICTIONARY
10. **「OK」**をクリックします。
11. 「管理者オプション」では、ボックスを選択しないでください。
12. **「OK」**をクリックします。

手順 2: このチュートリアルで使用するユーザー・アカウントを作成する

Matthew と Winston は、どちらも HR.EMPLOYEES スキーマの従業員のサンプルです。従業員のマネージャ ID や電子メール・アドレスなどの情報を含む列があります。以降でセキュア・アプリケーション・ロールをテストするため、これら 2 人の従業員のユーザー・アカウントを作成する必要があります。

ユーザー・アカウントを作成するには、次のようにします。

1. Database Control で**「データベース・インスタンス」**リンクを選択して、データベースのホームページを表示します。

   Database Control にログインしていない場合、Database Control の起動方法の詳細は『Oracle Database 2 日でデータベース管理者』を参照してください。「ログイン」ページで、管理者のユーザー名（SYSTEM など）およびパスワードを入力し、**「ログイン」**をクリックします。
2. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
3. 「セキュリティ」で、**「ユーザー」**を選択します。

   「ユーザー」ページが表示されます。
4. **「作成」**をクリックします。

   「ユーザーの作成」ページが表示されます。
5. 次の情報を入力します。
   - **名前**: mweiss（Matthew Weiss のユーザー・アカウントを作成するため）
   - **プロファイル**: デフォルト

- **認証**: パスワード
- **「パスワードの入力」**および**「パスワードの確認」**: 3-9 ページの「パスワードの作成要件」に示されている要件を満たすパスワードを入力します。
- **デフォルト表領域**: USERS
- **一時表領域**: TEMP
- **ステータス**: ロック解除

6. **「システム権限」**をクリックして、「システム権限」サブページを表示します。
7. **「リストを編集」**をクリックします。

   「システム権限の変更」ページが表示されます。
8. 「使用可能なシステム権限」リストから CREATE SESSION 権限を選択し、**「移動」**をクリックして「選択したシステム権限」リストに移動します。
9. **「OK」**をクリックします。

   CREATE SESSION がユーザー mweiss のシステム権限としてリストされた状態で「ユーザーの作成」ページが表示されます。
10. CREATE SESSION の「管理者オプション」が選択されていないことを確認し、**「OK」**をクリックします。

    「ユーザー」ページが表示されます。
11. ユーザー・リストから**「MWEISS」**を選択し、次に**「アクション」**リストから**「類似作成」**を選択します。次に**「実行」**をクリックします。
12. 「ユーザーの作成」ページで、次の情報を入力して Winston のユーザー・アカウントを作成します。このアカウントは Matthew のユーザー・アカウントとほぼ同じになります。
    - **名前**: wtaylor
    - **「パスワードの入力」**および**「パスワードの確認」**: 3-9 ページの「パスワードの作成要件」に示されている要件を満たすパスワードを入力します。
13. **「OK」**をクリックします。

    wtaylor に CREATE SESSION 権限を付与する必要はありません。これは、この処理が**「類似作成」**アクションによって実行されているためです。
14. Database Control を終了します。

これで、Matthew Weiss と Winston Taylor の両方にユーザー・アカウントが作成され、同じ権限が与えられました。

手順 3: セキュア・アプリケーション・ロールを作成する

これで、employee_role セキュア・アプリケーション・ロールを作成する準備ができました。これを実行するには、セキュリティ管理者 sec_admin としてログインする必要があります。4-4 ページの「手順 1: セキュリティ管理者アカウントを作成する」に、sec_admin アカウントの作成方法の説明があります。

セキュア・アプリケーション・ロールを作成するには、次のようにします。

1. SQL*Plus を起動し、セキュリティ管理者 sec_admin としてログオンします。

   ```
   SQLPLUS sec_admin
   Enter password: password
   ```

   SQL*Plus が起動し、デフォルトのデータベースに接続してから、プロンプトが表示されます。

   ```
   SQL>
   ```

   SQL*Plus の起動の詳細は、『Oracle Database 2 日でデータベース管理者』を参照してください。

2. 次のセキュア・アプリケーション・ロールを作成します。

```
CREATE ROLE employee_role IDENTIFIED USING sec_roles;
```

IDENTIFIED USING 句では、関連付けられている PL/SQL パッケージ（この場合は sec_roles）内でのみ有効（または無効）にするロールを設定します。この段階では、sec_roles PL/SQL パッケージが存在している必要はありません。

3. ユーザー OE として接続します。

```
CONNECT oe
Enter password: password
```

OE がロックされているというエラー・メッセージが表示された場合は、OE アカウントのロックを解除し、次の文を入力してパスワードをリセットします。セキュリティを考慮して、以前のリリースの Oracle Database で使用していたパスワードと同じパスワードは再使用しないでください。3-9 ページの「パスワードの作成要件」に示されているパスワードのガイドラインに従って、任意のセキュアなパスワードを入力します。

```
CONNECT sys/as sysdba
Enter password: sys_password
PASSWORD OE
Changing password for OE
New password: password
Retype new password: password
Password changed.

CONNECT oe
Enter password: password
```

4. 次の文を入力して、OE.ORDERS 表に対する SELECT 権限を EMPLOYEE_ROLE ロールに付与します。

```
GRANT SELECT ON OE.ORDERS TO employee_role;
```

ユーザーに直接ロールは付与しないでください。ユーザーがセキュリティ・ポリシーの条件を満たしている場合、ロールの付与は PL/SQL パッケージにより行われます。ユーザーに直接ロールを付与する必要がある場合は、ユーザーのロールを無効にする必要があります。これは、パッケージのセキュリティ・ポリシーがチェックを開始する前に、ロールが無効になっている必要があるためです。たとえば、ユーザー wsmith（wsmith にロールが最初に付与されると仮定）のロールを無効にするには、次の文を入力します。

```
ALTER USER wsmith DEFAULT ROLE NONE;
```

手順 4: 参照表を作成する

employee_role ロールを付与するユーザーを決定するプロシージャを作成します。このプロシージャは、マネージャ ID 100 の Steven King に報告を行うマネージャにのみ employee_role を付与します。この情報は HR.EMPLOYEES 表にあります。ただし、この表には給与情報などの機密データが含まれており、また、使用した場合すべてのユーザーがアクセスする必要があるため、このプロシージャでは使用できません。実際にはほとんどの場合に、参照表として既存のアプリケーション表を使用します。このチュートリアルでは、従業員の名前、従業員 ID、マネージャ ID のみを含む独自の参照表を作成します。

HR.HR_VERIFY ルックアップ・テーブルを作成するには、次のようにします。

1. SQL*Plus で、ユーザー HR として接続します。

```
CONNECT hr
Enter password: password
```

HR がロックされているというエラー・メッセージが表示された場合は、そのアカウントのロックを解除し、次の文を入力してパスワードをリセットします。セキュリティを考慮して、以前のリリースの Oracle Database で使用していたパスワードと同じパスワードは再

使用しないでください。3-9 ページの「パスワードの作成要件」に示されているパスワードのガイドラインに従って、任意のセキュアなパスワードを入力します。

```
CONNECT sys/as sysdba
Enter password: password
ALTER USER HR ACCOUNT UNLOCK IDENTIFIED BY password;
CONNECT hr
Enter password: password
```

2. 次の CREATE TABLE SQL 文を入力して参照表を作成します。

```
CREATE table hr_verify AS
SELECT employee_id, first_name, last_name, email, manager_id
FROM employees;
/
```

3. 次の SQL 文を入力して、この表に対する EXECUTE 権限を MWEISS と WTAYLOR に付与します。

```
GRANT SELECT ON hr.hr_verify TO mweiss;
GRANT SELECT ON hr.hr_verify TO wtaylor;
GRANT SELECT ON hr.hr_verify TO sec_admin;
```

手順 5: PL/SQL プロシージャを作成してセキュア・アプリケーション・ロールを設定する

次に、セキュア・アプリケーション・ロールのプロシージャを作成します。多くの場合、プロシージャを格納するパッケージを作成しますが、このチュートリアルは、1 つのセキュア・アプリケーション・ロールのみをテスト（プロシージャで定義）するシンプルなチュートリアルであるため、プロシージャのみを作成します。複数のプロシージャを作成してロールをテストする場合は、パッケージ内にプロシージャを作成します。

PL/SQL パッケージは、SQL 文でアクセスできる関連プロシージャおよびタイプのセットに対する単純で明確なインタフェースを定義します。またパッケージは、コードを再利用可能にし、メンテナンスを簡単にします。セキュア・アプリケーション・ロールに関するここでの利点は、セキュリティ・ポリシーのグループを作成できることです。このポリシー・グループは一緒に使用され、アプリケーションを保護するように設計された堅牢なセキュリティ計画を表します。セキュリティ・ポリシーに違反したユーザー（または潜在的な侵入者）に対して、エラーを記録するための監査チェックをパッケージに追加できます。

セキュア・アプリケーション・ロールのプロシージャを作成するには、次のようにします。

1. SQL*Plus でユーザー sec_admin として接続します。

```
CONNECT sec_admin
Enter password: password
```

2. 次の CREATE PROCEDURE 文を入力してセキュア・アプリケーション・ロールのプロシージャを作成します。

```
1   CREATE OR REPLACE procedure sec_roles AUTHID CURRENT_USER
2    AS
3   v_user varchar2(50);
4   v_manager_id number :=1;
5    BEGIN
6     v_user := lower((sys_context ('userenv','session_user')));
7     SELECT manager_id
8        INTO v_manager_id FROM hr.hr_verify WHERE lower(email)=v_user;
9      IF v_manager_id = 100
10      THEN
11      EXECUTE IMMEDIATE 'SET ROLE employee_role';
12      ELSE NULL;
13     END IF;
14    EXCEPTION
15    WHEN NO_DATA_FOUND THEN v_manager_id:=0;
16   DBMS_OUTPUT.PUT_LINE(v_manager_id);
17  END;
18  /
```

この例では、次のとおりです。

- **1 行目 :** CREATE PROCEDURE 文に、実行者の権限を使用してプロシージャを作成する AUTHID CURRENT_USER 句を追加します。AUTHID CURRENT_USER 句は、現在のユーザーの権限を使用し、実行者の権限を使用してパッケージを作成します。

  パッケージを機能させるには、実行者の権限を使用する必要があります。実行者の権限は、パッケージがアクセスするすべてのオブジェクトに対する EXECUTE 権限をユーザーに与えます。

  実行者の権限のプロシージャ内で有効化されるロールは、プロシージャの終了後も有効なままになります。ただし、ユーザーがセッションを終了すると、ユーザーはセキュア・アプリケーション・ロールに関連付けられた権限を持たなくなります。この場合、残りのセッションのロールを有効にする専用のプロシージャを使用できます。

  ユーザーは、定義者権限のプロシージャ内のセキュリティ・ドメインを変更できないため、セキュア・アプリケーション・ロールは実行者権限のプロシージャ内でのみ有効になります。

  実行者の権限を使用したプロシージャの作成の重要性については、4-3 ページの「セキュア・アプリケーション・ロールについて」を参照してください。

- **3 行目 :** ユーザーのセッション情報を格納する v_user 変数を宣言します。
- **4 行目 :** v_user ユーザーのマネージャ ID を格納する v_manager_id 変数を宣言します。
- **6 行目 :** ユーザー・ログオンのユーザー・セッション情報（この場合は、Matthew または Winston）を取得します。ユーザー・セッション情報を取得するには、SQL ファンクション SYS_CONTEXT をネームスペース属性 USERENV（'userenv'、*session_attribute*）とともに使用して、この情報を v_user 変数に書き込みます。

  このファンクションから返される情報は、ユーザーが認証された方法、クライアントの IP アドレスおよびユーザーがプロキシを介して接続したかどうかを示します。SYS_CONTEXT の詳細は、『Oracle Database SQL 言語リファレンス』を参照してください。

- **7 ～ 8 行目 :** 現行ユーザーのマネージャ ID を取得します。SELECT 文によって、マネージャ ID が v_manager_id 変数にコピーされ、HR.HR_VERIFY 表で現行ユーザーのマネージャ ID がチェックされます。
- **9 から 13 行目 :** IF 条件により、ユーザーに sec_roles ロールを付与すべきかどうかテストされます。この例の場合は、Matthew のマネージャである Steven King（従業員番号は 100）に報告を行うかどうかが条件となります。Matthew のように、King に報

告を行う場合、ユーザーにはセキュア・アプリケーション・ロールが付与されます。報告を行わない場合は、ロールは付与されません。

結果として、Matthew Weiss は Steven King の直属の部下であるためセキュア・アプリケーション・ロールを付与されますが、Winston は Steven King の直属の部下ではないためロールは付与されません。

- **10 ～ 12 行目 :** IF 条件内では、THEN 条件によって SET ROLE 文がすぐに実行され、ロールが付与されます。これが実行されない場合は、ELSE 条件により、権限付与が拒否されます。
- **14 から 15 行目 :** データが検出されない場合は、EXCEPTION 文を使用して v_manager_id を 0 に設定します。
- **16 行目 :** マネージャ ID をバッファにコピーしてすぐに使用できるようにします。

手順 6: Matthew と Winston のプロシージャに EXECUTE 権限を付与する

この段階で、Matthew と Winston は OE.ORDERS 表にアクセスを試行できますが、アクセスはできません。次の手順で、Matthew と Winston に sec_roles プロシージャの EXECUTE 権限を付与します。sec_roles プロシージャは実行できますが、OE.ORDERS 表から選択したときに、アクセスが許可または拒否されます。

sec_roles プロシージャの EXECUTE 権限を付与するには、次のようにします。

- SQL*Plus で、ユーザー sec_admin として次の GRANT SQL 文を入力します。

```
GRANT EXECUTE ON sec_admin.sec_roles TO mweiss;
GRANT EXECUTE ON sec_admin.sec_roles TO wtaylor;
```

手順 7: EMPLOYEE_ROLE セキュア・アプリケーション・ロールをテストする

Matthew と Winston としてログオンし、OE.ORDERS 表にアクセスを試行して、employee_role セキュア・アプリケーション・ロールをテストします。Matthew と Winston がログオンすると、OE.ORDERS 表で SELECT 文を発行する前に、employee_role プロシージャが実行されてロールの検証が行われます。

ユーザー MWEISS として employee_role セキュア・アプリケーション・ロールをテストするには、次のようにします。

1. ユーザー mweiss として接続します。

```
CONNECT mweiss
Enter password: password
```

2. 次の SQL 文を入力して sec_roles プロシージャを実行します。

```
EXEC sec_admin.sec_roles;
```

この文により、現行セッションに対して sec_roles プロシージャが実行されます。

3. OE.ORDERS で次の SELECT 文を実行します。

```
SELECT count(*) FROM oe.orders;
```

Matthew には OE.ORDERS 表へのアクセス権があります。

```
  COUNT(*)
----------
       105
```

次に、Winston がセキュア・アプリケーションにアクセスしようとします。

ユーザー WTAYLOR として employee_role セキュア・アプリケーション・ロールをテストするには、次のようにします。

1. SQL*Plus でユーザー wtaylor として接続します。

```
CONNECT wtaylor
Enter password: password
```

2. 次の SQL 文を入力して sec_roles プロシージャを実行します。

```
EXEC sec_admin.sec_roles;
```

この文により、現行セッションに対して sec_roles プロシージャが実行されます。

3. OE.ORDERS で次の SELECT 文を実行します。

```
SELECT count(*) FROM oe.orders;
```

Winston は Steven King に直接報告を行わないため、OE.ORDERS 表へのアクセス権がありません。SELECT 文を実行した場合でも、ORDERS 表に含まれる実際の注文数はわかりません。

```
ERROR at line 1:
ORA-00942: 表またはビューが存在しません。
```

手順 8: このチュートリアルで使用したコンポーネントを削除する（オプション）

このチュートリアルで作成したコンポーネントを削除します。

コンポーネントを削除するするには、次のようにします。

1. SQL*Plus で、SYSDBA 権限を持つ SYS として接続します。

```
CONNECT SYS/AS SYSDBA
Enter password: password
```

2. 次の DROP 文を入力します。

```
DROP USER mweiss;
DROP USER wtaylor;
```

ユーザー sec_admin は削除しないでください。このマニュアルの以降のチュートリアルで、このユーザーが必要になります。

3. SQL*Plus でユーザー sec_admin として接続します。

```
CONNECT sec_admin
Enter password: password
```

4. 次の DROP SQL 文を入力します。

```
DROP ROLE employee_role;
DROP PROCEDURE sec_roles;
```

5. ユーザー HR として接続してから、HR_VERIFY 表を削除します。

```
CONNECT HR
Enter password: password
DROP TABLE hr_verify;
```

6. SQL*Plus を終了します。

```
EXIT
```

権限セキュリティに使用される初期化パラメータ

表 4-1 に、ユーザー権限を保護するために使用する初期化パラメータを示します。

表 4-1 権限セキュリティに使用される初期化パラメータ

初期化パラメータ	デフォルト設定	説明
O7_DICTIONARY_ACCESSIBILITY	FALSE	SYSTEM 権限に対する制限を制御します。このパラメータの詳細は、2-4 ページの「データ・ディクショナリ保護の有効化」を参照してください。
OS_ROLES	FALSE	Oracle またはオペレーティング・システムが各ユーザー名のロールを識別および管理するかどうかを決定します。
MAX_ENABLED_ROLES	30	他のロールに含まれるロールを含め、ユーザーが有効にできるデータベース・ロールの最大数を指定します。
REMOTE_OS_ROLES	FALSE	オペレーティング・システム・ロールがリモート・クライアントに対して許可されるかどうかを指定します。デフォルト値の FALSE を指定すると、Oracle はリモート・クライアントのロールを識別および管理します。
SQL92_SECURITY	FALSE	UPDATE 文や DELETE 文などを実行するためにユーザーに SELECT オブジェクト権限が付与されている必要があるかどうかを指定します。

初期化パラメータを変更するには、2-7 ページの「初期化パラメータ値の変更」を参照してください。初期化パラメータの詳細は、『Oracle Database リファレンス』および『Oracle Database 管理者ガイド』を参照してください。

5

ネットワークの保護

この章の内容は次のとおりです。

ネットワークの保護について

『Oracle Database 2 日でデータベース管理者』の「ネットワーク環境の構成」および使用しているプラットフォームの『Oracle Database インストレーション・ガイド』の手順に従って、Oracle Database インストール環境へのクライアント接続を構成できます。この章では、ネットワーク上を移動するデータを暗号化する方法を説明し、Oracle Database のネットワーク接続を保護するために従うことのできるガイドラインも示します。

ネットワーク上のクライアント接続の保護

ここでは、クライアント接続のセキュリティを高めて、完全な保護を確保する方法を説明します。SSL の使用は、これらのリストの重要な要素であり、認証と通信の厳密なセキュリティを可能にします。

ガイドラインは次のとおりです。

- クライアント接続保護のガイドライン
- ネットワーク接続の保護のガイドライン

クライアント接続保護のガイドライン

インターネットを介したクライアント・コンピュータの認証には問題が多いため、通常は、かわりにユーザー認証が行われます。この方法により、偽造された IP アドレス、危険にさらされたオペレーティング・システムまたはアプリケーション、偽造または盗用されたクライアント・システム ID がクライアント・システムで使用される問題を回避できます。また、次のガイドラインに従うことで、クライアント接続のセキュリティが向上します。

1. **アクセス制御を効果的に実施して、クライアントを厳密に認証します。**

   デフォルトでは、オペレーティング・システムで認証されたログインのみがセキュア接続で許可され、Oracle Net および共有サーバー構成の使用は拒否されます。デフォルトで行われるこの制限により、リモート・ユーザーがネットワーク接続で他のオペレーティング・システム・ユーザーを装うことが阻止されます。

   初期化パラメータ `REMOTE_OS_AUTHENT` を `TRUE` に設定すると、データベースはセキュアでない接続を介して受信したクライアントのオペレーティング・システムのユーザー名を受け入れ、このユーザー名をアカウント・アクセスで使用します（初期化パラメータを変更するには、2-7 ページの「初期化パラメータ値の変更」を参照してください）。コンピュータなどのクライアントは、オペレーティング・システムの認証を適切に実行していない場合があるため、この機能を使用するとセキュリティが非常に低下します。

   デフォルト設定 `REMOTE_OS_AUTHENT = FALSE` により、よりセキュアな構成が作成され、Oracle Database に接続するクライアントに対してサーバーベースの適切な認証が行われます。

   `REMOTE_OS_AUTHENT` 初期化パラメータのデフォルト設定（`FALSE`）は、変更しないでください。

   このパラメータを `FALSE` に設定しても、ユーザーがリモートから接続できなくなるわけではありません。クライアントがすでに認証されていたとしても、データベースにより標準の認証プロセスが適用されるだけです。

2. **Secure Sockets Layer（SSL）を使用するように接続を構成します。**

   SSL 通信を使用すると、盗聴が困難になり、ユーザーとサーバーの認証に証明書を使用できます。SSL の構成方法は、『Oracle Database Advanced Security 管理者ガイド』を参照してください。

3. **クライアントおよびサーバーの証明書認証を設定します。**

   証明書の管理方法の詳細は、『Oracle Database Advanced Security 管理者ガイド』を参照してください。

4. **システムにアクセスするユーザーを監視します。**

   インターネットを介したクライアント・コンピュータの認証には問題が多いため、かわりにユーザー認証を行います。この方法により、偽造された IP アドレス、ハッキングされたオペレーティング・システムまたはアプリケーション、偽造または盗用されたクライアント・システム ID がクライアント・システムで使用される問題が回避できます。また、次の手順を実行することで、クライアント・コンピュータのセキュリティが向上します。

   a. Secure Sockets Layer（SSL）を使用するように接続を構成します。SSL 通信を使用すると、傍受が困難になります。また、ユーザーおよびサーバー認証で証明書を使用できます。SSL の構成方法については、『Oracle Database Advanced Security 管理者ガイド』を参照してください。

   b. 次のようにして、クライアントおよびサーバーの証明書認証を設定します。

      – 組織は、部署と証明書の発行者により識別します。ユーザーは、識別名と証明書の発行者により識別します。

      – 証明書の期限が切れていないかテストします。

      – 証明書失効リストを監査します。

      証明書の管理方法の詳細は、『Oracle Database Advanced Security 管理者ガイド』を参照してください。

ネットワーク接続の保護のガイドライン

不適切なアクセスまたは変更からネットワークおよびトラフィックを保護することは、ネットワーク・セキュリティにおいて非常に重要です。データが移動するすべての経路を検討し、各経路およびノードに影響を与える脅威を評価します。次に、脅威およびセキュリティが侵害された場合の影響を抑制または排除する手順を実行します。また、監視および監査を実施し、脅威レベルの増加または侵入を検出します。

ネットワーク接続を管理するには、Oracle Net Manager を使用できます。Oracle Net Manager の使用の概要は、『Oracle Database 2 日でデータベース管理者』を参照してください。『Oracle Database Net Services 管理者ガイド』も参照してください。

次の手順を実行して、ネットワーク・セキュリティを強化します。

1. **リスナーのアクティビティを監視します。**

   Oracle Enterprise Manager Database Control を使用してリスナーのアクティビティを監視できます。Database Control のホームページの「一般」で、使用しているリスナーのリンクをクリックします。「リスナー」ページが表示されます。このページには、生成されたアラートのカテゴリ、アラート・メッセージ、アラートがトリガーされた日時などの詳細な情報が含まれています。このページには、リスナーのパフォーマンス統計などの情報も含まれています。

2. **管理者に対して listener.ora ファイルへの書込み権限およびリスナーのパスワードを要求して、オンライン管理を防止します。**

   a. `listener.ora` ファイルで、次の行を追加または変更します。

      ```
      ADMIN_RESTRICTIONS_LISTENER=ON
      ```

   b. `RELOAD` を使用して構成をリロードします。

   c. 次のように、アドレス・リストの第 1 エントリを TCPS プロトコルにして、リスナーの管理に SSL を使用します。

      ```
      LISTENER=
        (DESCRIPTION=
          (ADDRESS_LIST=
            (ADDRESS=
              (PROTOCOL=tcps)
              (HOST = shobeen.us.example.com)
              (PORT = 8281)))
      ```

リモートからリスナーを管理するには、クライアント・コンピュータ上の listener.ora ファイルでリスナーを定義します。たとえば、リスナー USER281 にリモートからアクセスする場合は、次の構成を使用します。

```
user281 =
  (DESCRIPTION =
    (ADDRESS =
      (PROTOCOL = tcps)
      (HOST = shobeen.us.example.com)
      (PORT = 8281))
    )
  )
```

listener.ora のパラメータの詳細は、『Oracle Net Services リファレンス・ガイド』を参照してください。

3. **リスナー・パスワードを設定しないでください。**

   パスワードが listener.ora ファイルに設定されていないことを確認します。オペレーティング・システム認証によってリスナー管理が保護されます。パスワードが設定されていない場合、リモート・リスナー管理は無効です。

4. **複数の NIC カードに関連付けられている複数の IP アドレスがホストにある場合は、リスナーを特定の IP アドレスに設定します。**

   これにより、リスナーはすべての IP アドレスを監視できます。指定した IP アドレスを監視するように制限することもできます。これらのタイプのコンピュータでは、リスナーにすべての IP アドレスを監視させるのではなく、IP アドレスを指定することをお薦めします。特定の IP アドレスの監視に制限することで、リスナー・プロセスから TCP エンドポイントが盗用されることを防止できます。

5. **リスナーの権限を制限して、データベースまたは Oracle サーバーのアドレス空間のファイルを読取り / 書込みできないようにします。**

   この制限により、リスナー（またはエージェントが実行するプロシージャ）によって起動される外部プロシージャ・エージェントに、読取りまたは書込み操作の実行権限が継承されなくなります。この個別のリスナー・プロセスの所有者には、Oracle をインストールした所有者または Oracle インスタンスを実行する所有者（デフォルトの所有者である ORACLE など）は指定しないでください。

   リスナーにおける外部プロシージャの構成の詳細は、『Oracle Database Net Services 管理者ガイド』を参照してください。

6. **インターネットを介してデータを転送する場合は物理アドレスを保護できないため、このデータを保護する必要がある場合は暗号化を使用します。**

   ネットワーク上の Oracle データを保護する方法については、5-5 ページの「ネットワーク暗号化を使用したネットワーク上のデータの保護」を参照してください。ネットワークの暗号化の詳細は、『Oracle Database Advanced Security 管理者ガイド』を参照してください。

7. **ファイアウォールを使用します。**

   内部ユーザーにインターネット・アクセスを許可する場合は、ファイアウォールを適切に配置および構成することで、イントラネットへの外部アクセスを防止できます。

   - データベース・サーバーはファイアウォールの内側に配置してください。Oracle Database ネットワーク・インフラストラクチャである Oracle Net（以前の Net8 および SQL*Net）は、様々なベンダーの各種ファイアウォールをサポートしています。サポートされるプロキシ対応のファイアウォールには、Network Associates の Gauntlet や Axent の Raptor などが含まれます。サポートされるパケット・フィルタ型のファイアウォールには Cisco の PIX Firewall、またサポートされるステートフル・インスペクション・ファイアウォール（より高機能なパケット・フィルタを実装したファイアウォール）には、CheckPoint の Firewall-1 が含まれます。
   - ファイアウォールは、保護するネットワークの外側に配置されている必要があります。

- 安全性が確認されているプロトコル、アプリケーションまたはクライアント / サーバーのソースのみを受け入れるようにファイアウォールを構成します。
- Oracle Connection Manager などの製品を使用し、データベースへの単一のネットワーク接続を介して複数のクライアント・ネットワーク・セッションを多重化します。多重化する際に、送信元、送信先およびホスト名でフィルタ処理できます。この製品により、物理的に保護された端末または既知の IP アドレスのアプリケーション Web サーバーからの接続のみを受け入れるようにできます（IP アドレスは偽造可能なため、IP アドレスのみでフィルタ処理した認証では不十分です）。

8. **Oracle リスナーの不正な管理を防止します。**

   リスナーの詳細は、『Oracle Database Net Services 管理者ガイド』を参照してください。

9. **ネットワーク IP アドレスをチェックします。**

   Oracle Net の有効なノードの確認セキュリティ機能を利用すると、指定の IP アドレスを持つネットワーク・クライアントから Oracle サーバー・プロセスへのアクセスを許可または拒否できます。この機能を使用するには、次の `sqlnet.ora` 構成ファイル・パラメータを設定します。

   ```
   tcp.validnode_checking = YES

   tcp.excluded_nodes = {list of IP addresses}

   tcp.invited_nodes = {list of IP addresses}
   ```

   `tcp.validnode_checking` パラメータで、機能を有効にします。`tcp.excluded_nodes` および `tcp.invited_nodes` パラメータは、特定のクライアント IP アドレスによる Oracle リスナーへの接続の確立を拒否または有効にします。これにより、潜在的なサービス拒否（DoS）攻撃を防ぐことができます。

   Oracle Net Manager を使用して、これらのパラメータを構成できます。詳細は、『Oracle Database Net Services 管理者ガイド』を参照してください。

10. **ネットワーク・トラフィックを暗号化します。**

    可能な場合は、Oracle Advanced Security を使用して、クライアント、データベースおよびアプリケーション・サーバー間のネットワーク・トラフィックを暗号化します。Oracle ネットワーク暗号化の概要は、5-5 ページの「ネットワーク暗号化を使用したネットワーク上のデータの保護」を参照してください。ネットワーク暗号化の詳細は、『Oracle Database Advanced Security 管理者ガイド』を参照してください。

11. **ホスト・オペレーティング・システム（Oracle Database が配置されているシステム）を保護します。**

    オペレーティング・システムの不要なサービスをすべて使用禁止にして、ホスト・オペレーティング・システムを保護します。UNIX および Windows の大部分のサービスは、標準的なデータベース構成では必要ありません。この種のサービスには、FTP、TFTP、TELNET などがあります。使用を禁止している各サービスの UDP ポートと TCP ポートは、両方とも必ず閉じてください。いずれかのポートが使用可能になっていると、オペレーティング・システムが攻撃を受けやすくなります。

ネットワーク暗号化を使用したネットワーク上のデータの保護

情報は、データベース・レベルで暗号化して保護するだけでなく、ネットワークで送受信されるときにも保護する必要があります。

この項の内容は次のとおりです。

関連項目： ネットワーク暗号化の詳細は、『Oracle Database Advanced Security 管理者ガイド』を参照してください。

ネットワーク暗号化について

ネットワーク暗号化とは、クライアントとサーバー間のネットワークを移動するデータを暗号化することです。データベース・レベルだけでなくネットワーク・レベルでもデータを暗号化する必要があるのは、データベースで十分注意して暗号化したデータでもネットワーク・レベルで読み取られる可能性があるためです。たとえば、ネットワークを移動する情報がネットワーク・パケット・スニファを使用して傍受され、ファイルにスプールされて不正に使用される可能性があります。ネットワーク上のデータを暗号化することにより、このようなアクティビティを防止できます。

ネットワーク上のデータを暗号化するには、次のコンポーネントが必要です。

- **暗号化シード。**暗号化シードは、最大 256 文字のランダムな文字列です。ネットワークを移動するデータを暗号化する暗号化キーを生成します。
- **暗号化アルゴリズム。**サポートされるアルゴリズムのタイプ（AES、RC4、DES、3DES）からいずれかを指定します。
- **クライアントまたはサーバーに適用する設定。**サーバーと、サーバーが接続する各クライアントを設定する必要があります。
- **クライアントまたはサーバーが暗号化されたデータを処理する方法。**サーバーとクライアントで、同じ設定を選択する必要があります（オプションが 4 つあります）。
- **暗号化を構成するためのメカニズム。**Oracle Net Manager を使用して暗号化を構成できます。または、`sqlnet.ora` 構成ファイルを編集できます。Oracle Net Manager と `sqlnet.ora` はどちらもデフォルトの Oracle Database インストール環境で使用できます。

ネットワーク暗号化の設定

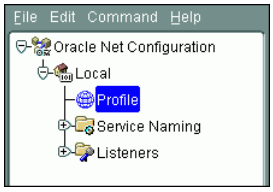
Oracle Net Manager を使用するか、`sqlnet.ora` ファイルを編集して、ネットワーク暗号化を設定できます。このマニュアルでは、Oracle Net Manager を使用してネットワーク暗号化を設定する方法を説明します。

ネットワーク暗号化を設定するには、次のようにします。

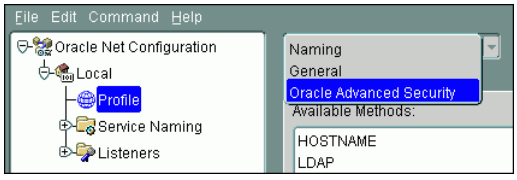
1. サーバー・コンピュータで、Oracle Net Manager を起動します。
   - **UNIX**: `$ORACLE_HOME/bin` から、次のコマンドラインを入力します。

     ```
     netmgr
     ```

   - **Windows**: **「スタート」**メニューから**「すべてのプログラム」**をクリックします。次に**「Oracle - *HOME_NAME*」→「Configuration and Migration Tools」→「Net Manager」**の順にクリックします。
2. Oracle Net Configuration のナビゲーション・ツリーで、**「ローカル」**を拡張してから**「プロファイル」**を選択します。

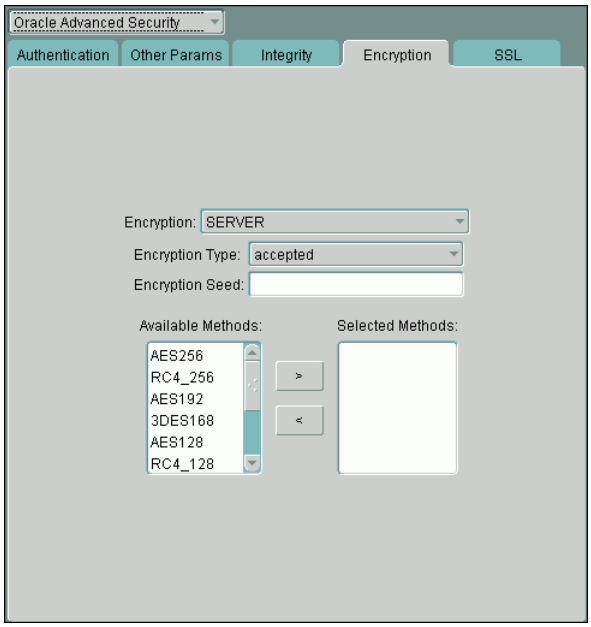


3. リストから**「Oracle Advanced Security」**を選択します。



4. 「Oracle Advanced Security」で、**「暗号化」**タブを選択します。

   「暗号化」設定ペインが表示されます。



5. 次の設定を入力します。

   - **暗号化**: リストから**「SERVER」**を選択して、サーバーにネットワーク暗号化を設定します（クライアント・コンピュータの場合は**「CLIENT」**を選択します）。
   - **暗号化タイプ**: 次の値のいずれかを選択して、暗号化および完全性のネゴシエーションをするときのサーバー（またはクライアント）の動作を指定します。
     - **適用**: 一方の接続側で「必要」または「リクエスト」が指定されており、もう一方の接続側で矛盾のないアルゴリズムが使用可能になっている場合、サービスはアクティブになります。それ以外の場合、サービスはアクティブにはなりません。
     - **拒否**: サービスはアクティブにはなりません。一方の接続側で必要な場合、接続は失敗します。
     - **リクエスト**: 一方の接続側で「適用」、「必要」または「リクエスト」が指定されており、もう一方の接続側で矛盾のないアルゴリズムが使用可能になっている場合、サービスはアクティブになります。それ以外の場合、サービスはアクティブにはなりません。
     - **必要**: サービスはアクティブになります。一方の接続側で「拒否」が指定されている場合、または両立するアルゴリズムがない場合、接続は失敗します。
   - **暗号化シード**: 最大 256 文字のランダムな文字列を入力します。Oracle Database は暗号化シードを使用して暗号化キーを生成します。暗号化または完全性のいずれかが有効な場合は必須です。

     暗号化シード・パラメータの一部にカンマ「,」、右括弧「)」などの特殊文字を使用する場合は、一重引用符で値を囲んでください。
   - **使用可能なメソッド**: 次のアルゴリズムから 1 つ以上を選択し、移動ボタン（>）を使用して「選択メソッド」リストに移動します。「選択メソッド」リストに表示される順番により、ネゴシエーションの優先順位が決まります。つまり、最初に表示されるアルゴリズムが最初に選択されます。
     - **AES256**: Advanced Encryption Standard（AES）。AES はデータ暗号化規格（DES）にかわる暗号化規格として、米国標準技術局（National Institute of Standards and Technology: NIST）で認定されています。ASE256 を使用すると、256 ビットのブロック・サイズを暗号化できます。

- **RC4_256**: Rivest Cipher 4（RC4）。Secure Sockets Layer（SSL）などのプロトコルを保護する、最も一般的に使用されるストリーム暗号です。RC4_256 を使用すると、最大 256 ビットのデータを暗号化できます。
- **AES192**: AES を使用して 192 ビットのブロック・サイズを暗号化できます。
- **3DES168**: 3 キー・オプションによるトリプル DES。3DES168 を使用すると、最大 168 ビットのデータを暗号化できます。
- **AES128**: AES を使用して 128 ビットのブロック・サイズを暗号化できます。
- **RC4_128**: RC4 を使用して最大 128 ビットのデータを暗号化できます。
- **3DES112**: 2 キー（112 ビット）オプションによるトリプル DES を使用できます。
- **DES**: 56 ビットの Data Encryption Standard（DES）キーです。DES は、米国標準技術局（National Institute of Standards and Technology: NIST）の推奨対象ではなくなりました。
- **RC4_40**: RC4 を使用して最大 40 ビットのデータを暗号化できます。
- **DES40**: DES を使用して最大 40 ビットのデータを暗号化できます。

6. 「**ファイル**」メニューから「**ネットワーク構成の保存**」を選択し、次に「**終了**」を選択して Oracle Net Manager を終了します。
7. サーバーに接続するクライアント・コンピュータごとに、これらの手順を繰り返します。

関連項目：

- `sqlnet.ora` ファイルのパラメータを変更してネットワーク暗号化を設定する詳細は、『Oracle Net Services リファレンス・ガイド』を参照してください。
- ネットワークのデータ暗号化の詳細は、『Oracle Database Advanced Security 管理者ガイド』を参照してください。

ネットワーク・セキュリティに使用される初期化パラメータ

表 5-1 に、ユーザー・アカウントを保護するために設定する初期化パラメータを示します。

表 5-1 ネットワーク・セキュリティに使用される初期化パラメータ

初期化パラメータ	デフォルト設定	説明
`OS_AUTHENT_PREFIX`	`OPS$`	データベースへの接続を試行するユーザーを認証するために Oracle Database で使用される接頭辞を指定します。Oracle Database は、このパラメータの値をユーザーのオペレーティング・システム・アカウント名およびパスワードの先頭に連結します。ユーザーが接続リクエストを試行すると、Oracle Database は接頭辞の付いたユーザー名をデータベース内のユーザー名と比較します。 旧バージョンとの下位互換性を保つために、このパラメータのデフォルト値は `OPS$` になっています。ただし、接頭辞の値を "" （null 文字列）に設定して、オペレーティング・システム・アカウント名に接頭辞を追加することを回避できます。

表 5-1 ネットワーク・セキュリティに使用される初期化パラメータ（続き）

初期化パラメータ	デフォルト設定	説明
REMOTE_LISTENER	デフォルト設定なし	Oracle Net リモート・リスナー（つまり、このインスタンスと同じコンピュータで実行されていないリスナー）のアドレスまたはアドレス・リストを解決するネットワーク名を指定します。アドレスまたはアドレス・リストは、tnsnames.ora ファイル、またはシステムで構成されているその他のアドレス・リポジトリで指定されます。
REMOTE_OS_AUTHENT	FALSE	リモート・クライアントが OS_AUTHENT_PREFIX パラメータの値で認証されるかどうかを指定します。
REMOTE_OS_ROLES	FALSE	オペレーティング・システム・ロールがリモート・クライアントに対して許可されるかどうかを指定します。デフォルト値の FALSE を指定すると、Oracle Database はリモート・クライアントのロールを識別および管理します。

初期化パラメータを変更するには、2-7 ページの「初期化パラメータ値の変更」を参照してください。初期化パラメータの詳細は、『Oracle Database リファレンス』および『Oracle Database 管理者ガイド』を参照してください。

6

データの保護

この章の内容は次のとおりです。

データの保護について

Oracle Database には、データを保護する方法が多数用意されています。この章では、サイトでのデータの保護に使用できる次の方法について説明します。

- **透過的データ暗号化。**透過的データ暗号化では、1 つまたは複数のデータベース表列のデータを暗号化したり、表領域全体を暗号化できます。透過的データ暗号化を使用すると、最も迅速かつ容易にデータを暗号化できます。透過的データ暗号化は、Advanced Encryption Standard（AES）および Triple Data Encryption Standard（3DES）アルゴリズムをサポートします。

  ネットワーク上のデータを暗号化することもできます。この方法については 5-5 ページの「ネットワーク暗号化を使用したネットワーク上のデータの保護」を参照してください。

- **Oracle Virtual Private Database（VPD）。**この機能では、データベースに問い合せるすべての SQL 文に対して `WHERE` 句を動的に追加するポリシーを作成し、データへのアクセスを制限します。VPD ポリシーはデータベースの表またはビュー・レベルで作成および管理できます。データベースにアクセスするアプリケーションを変更する必要はありません。

- **Oracle Label Security（OLS）。**この機能では、データベース表を行レベルで保護し、ニーズに応じて、これらの行に異なるセキュリティ・レベルを割り当てます。また、OLS ラベルに基づいてユーザーのセキュリティ認可を作成できます。

- **Oracle Database Vault。**この機能では、データベースに対する管理者のアクセスを制限し、職務分離を適用し、アプリケーション、データベースおよびデータにアクセス可能なユーザー、時間、場所、方法を制御できます。

透過的なデータ暗号化によるデータの透過的な暗号化

透過的データ暗号化により、表領域または 1 つ以上の表の列をすばやく暗号化できます。実装も簡単で、他のタイプのデータベースの暗号化よりも多くの利点があります。

この項の内容は次のとおりです。

機密データの暗号化について

暗号化されたデータを読めるのは受信者のみです。暗号化を使用すると、オフサイトのストレージに送信されたバックアップ・メディアなど、保護されていない可能性のある環境でデータを保護できます。

暗号化されたデータには、次のコンポーネントがあります。

- **データを暗号化するアルゴリズム。**暗号化アルゴリズムは、Oracle Database がデータを暗号化するために使用する計算式です。クリア・テキスト・バージョン（人が読める形式）のデータを、復号化するもう 1 つのアルゴリズムによってのみ解読できる形式に変換します。Oracle Database は、Advanced Encryption Standard（AES）暗号化アルゴリズムなど、業界標準の暗号化アルゴリズムおよびハッシュ・アルゴリズムをいくつかサポートしています。AES は、米国標準技術局（National Institute of Standards and Technology: NIST）により、Data Encryption Standard（DES）にかわるアルゴリズムとして承認されています。

- **データを復号化するアルゴリズム。**復号化アルゴリズムは、暗号化アルゴリズムとは逆のタスクを実行します。データをクリア・テキストに変換します。

- **送信者が使用する暗号化キーと受信者が使用する複合化キー。**データを暗号化するときには、Oracle Database は暗号化アルゴリズムへの入力として暗号化キーおよびクリア・テキ

スト・データを使用します。逆に、データを複合化するときには、アルゴリズムへの入力として複合化キーを使用して、プロセスを逆に実行し、クリア・テキスト・データを取得します。Oracle Database は対称キーを使用してこのタスクを実行します（データの暗号化と複合化の両方で同じキーが使用されます）。暗号化キーはデータ・ディクショナリに格納されます。

データを暗号化するタイミング

多くの場合、コンプライアンス規則を遵守するために機密データを暗号化します。たとえば、クレジット・カード番号、社会保障番号、病歴に関する情報などの機密データは、暗号化する必要があります。

データベース管理者からのデータへのアクセスを制限するため、これまでユーザーはデータの暗号化を求めてきました。しかし問題は暗号化よりも、むしろアクセス制御にあります。Oracle Database Vault を使用してデータベース管理者からアプリケーション・データへのアクセスを制御することで、この問題に対処できます。

多くの場合、クレジット・カード番号や社会保障番号などの機密データは、バックアップ・テープやディスク・ドライバの紛失または盗難時にアクセスされないように暗号化します。近年では、ペイメント・カード産業（PCI）データ・セキュリティ標準や医療保険の相互運用性と説明責任に関する法律（HIPAA）などの業界規制に従って、クレジット・カード情報や医療情報の保護に暗号化がますます使用されています。

> **関連項目：** 格納されたデータの暗号化に関してよくある誤解については、『Oracle Database セキュリティ・ガイド』を参照してください。

透過的データ暗号化の動作

透過的データ暗号化を使用すると、個々の表列もしくは表領域全体を暗号化できます。ユーザーが暗号化された列にデータを挿入すると、透過的データ暗号化により、挿入されたデータが自動的に暗号化されます。ユーザーが列を選択すると、データは自動的に復号化されます。

透過的データ暗号化を使用してデータを暗号化するには、次のコンポーネントを作成します。

- **マスター暗号化キーを格納するウォレット。**ウォレットは、データベースの外にあるバイナリ・ファイル形式の記憶域です。データベースは、マスター暗号化キーの格納にウォレットを使用します。ウォレットは、Enterprise Manager または `ALTER SYSTEM` コマンドを使用して作成できます。ウォレットは、暗号化キーとしてパスワードを使用して暗号化できます。パスワードはウォレットの作成時に作成します。このため、ウォレットのコンテンツ（マスター・キー）へのアクセスは、パスワードを知っているユーザーに制限されます。ウォレットを作成したら、データベースがマスター暗号化キーにアクセスできるように、パスワードを使用してウォレットを開く必要があります。
- **ウォレットの場所。**`sqlnet.ora` ファイルを変更して、ウォレットの場所を指定できます。

ユーザーが暗号化された列にデータを入力すると、Oracle Database により次の手順が実行されます。

1. ウォレットからマスター・キーを取得します。
2. データ・ディクショナリの表の暗号化キーを復号化します。
3. 暗号化キーを使用して、ユーザーが暗号化した列に入力したデータを暗号化します。
4. 暗号化した形式でデータをデータベースに格納します。

ユーザーがデータを選択した場合も、同じようなプロセスが実行されます。Oracle Database によりデータが復号化され、その後、データがクリア・テキスト形式で表示されます。

透過的データ暗号化には、次の利点があります。

- セキュリティ管理者の場合、ストレージ・メディアまたはデータ・ファイルが盗み出された場合にも機密データを保護できます。
- 透過型データ暗号化を実装すると、セキュリティ関連のコンプライアンス要件を遵守できます。

- データを復号化するために、トリガーまたはビューを作成する必要がありません。表から取得されたデータは、データベース・ユーザーに対して透過的に復号化されます。
- データベース・ユーザーは、自身がアクセスしたデータが暗号化された形式で格納されていることを認識する必要がありません。データはデータベース・ユーザーに対して透過的に復号化され、ユーザーがアクションを行う必要はありません。
- 暗号化されたデータを処理するためにアプリケーションを変更する必要がありません。データの暗号化 / 復号化は、データベースにより管理されます。

透過型データ暗号化では、データが暗号化された列から取得されるときおよび暗号化された列に挿入されるときにのみ、パフォーマンスに影響します。暗号化されていない列に関する操作では、パフォーマンスが低下することはありません。これらの列が含まれる表に、暗号化された列が含まれている場合も同様です。暗号化されたデータは、クリア・テキスト・データより多くの記憶域を必要とします。平均的には、1 つの列を暗号化すると、行ごとに 32 バイトから 48 バイトの記憶域が余分に必要になります。

関連項目： 透過型データ暗号化の使用に関する詳細は、『Oracle Database Advanced Security 管理者ガイド』を参照してください。

透過的データ暗号化を使用するためのデータの構成

透過的データ暗号化の使用を開始するには、ウォレットとマスター・キーのセットを作成する必要があります。ウォレットは、他の Oracle Database コンポーネントと共有するデフォルトのデータベース・ウォレットを使用することも、特に透過的データ暗号化で使用される個別のウォレットを使用することもできます。オラクル社では、個別のウォレットを使用してマスター暗号化キーを格納することをお薦めします。このウォレットは、透過的データ暗号化により暗号化されるすべてのデータで使用されます。

次の手順を実行して、透過型データ暗号化を使用するように表列を設定します。

- 手順 1: ウォレットの場所を設定する
- 手順 2: ウォレットを作成する
- 手順 3: ウォレットを開く（または閉じる）
- 手順 4: データを暗号化（または復号化）する

関連項目： 表領域の暗号化の使用に関する詳細は、『Oracle Database Advanced Security 管理者ガイド』を参照してください。

手順 1: ウォレットの場所を設定する

sqlnet.ora ファイルでウォレットに対するディレクトリの場所を指定します。この手順は 1 回のみ実行します。

ウォレットの場所を設定するするには、次のようにします。

1. sqlnet.ora ファイルのバックアップ・コピーを作成します。このファイルのデフォルトの場所は、$ORACLE_HOME/network/admin ディレクトリです。
2. $ORACLE_HOME ディレクトリに、ウォレットを格納するディレクトリを作成します。

   たとえば、C:¥oracle¥product¥11.1.0¥db_1 ディレクトリに ORA_WALLETS という名前のディレクトリを作成します。
3. sqlnet.ora ファイルの最後に、次のコードと同様のコードを追加します。ORA_WALLETS は、ウォレットを格納するディレクトリの名前を表しています。

```
ENCRYPTION_WALLET_LOCATION=
 (SOURCE=
  (METHOD=file)
   (METHOD_DATA=
    (DIRECTORY=C:¥oracle¥product¥11.1.0¥db_1¥ORA_WALLETS)))
```

4. sqlnet.ora ファイルを保存して閉じます。

5. SQL*Plus を起動し、SYS としてログオンし、AS SYSOPER で接続します。

```
SQLPLUS "SYS/AS SYSOPER"
Enter password: password
```

SQL*Plus が起動し、デフォルトのデータベースに接続してから、SQL> プロンプトが表示されます。

SQL*Plus の起動の詳細は、『Oracle Database 2 日でデータベース管理者』を参照してください。

6. 次の SQL 文を入力し、データベースを停止してから再起動します。

```
SHUTDOWN IMMEDIATE
STARTUP
```

手順 2: ウォレットを作成する

ウォレットを作成するには、ALTER SYSTEM SQL 文を使用します。デフォルトでは、それまで使用されたマスター・キーの履歴が Oracle ウォレットに格納されます。これによりマスター・キーを変更でき、また、古いマスター・キーを使用して暗号化されたデータを復号化できます。大 / 小文字が区別されるウォレット・パスワードをデータベース管理者に知らせないことで、職務分離が実現されます。データベース管理者はデータベースを再起動できますが、ウォレットは閉じられており、ウォレット・パスワードを知っているセキュリティ管理者により手動で開かれる必要があります。

ウォレットを作成するには、次のようにします。

1. SQL*Plus で、SYSTEM などの管理権限を持つユーザーまたはセキュリティ管理者として接続します。

次に例を示します。

```
CONNECT SYSTEM
Enter password: password
```

2. 次の ALTER SYSTEM 文を入力します。*password* は、暗号化キーに割り当てるパスワードです。

```
ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY "password";
```

パスワードは二重引用符で囲みます。Oracle Database で作成した他のパスワードと同様に、パスワードはクリア・テキストまたは動的ビューや動的ログには表示されません。

この文により、新しい暗号化キーを使用するウォレットが生成され、このキーがデータの透過的な暗号化の現行のマスター・キーに設定されます。マスター暗号化キーを構成するために公開鍵基盤（PKI）を使用する場合は、証明書 ID を指定します。証明書 ID は、Oracle ウォレットに格納される証明書の固有の ID を含む文字列です。次の構文を使用します。

```
ALTER SYSTEM SET ENCRYPTION KEY certificate_ID IDENTIFIED BY "password";
```

手順 3: ウォレットを開く（または閉じる）

ウォレット・キーを作成した直後は、ウォレットは開かれており、いつでもデータの暗号化を開始できます。ただし、ウォレットを作成した後にデータベースを再起動した場合は、透過的データ暗号化を使用する前に手動でウォレットを開く必要があります。

ウォレットを開くには、次のようにします。

- SQL*Plus で次の ALTER SYSTEM 文を入力します。*password* は、暗号化キーに割り当てたパスワードです。

```
ALTER SYSTEM SET ENCRYPTION WALLET OPEN IDENTIFIED BY "password";
```

ほとんどの場合、ウォレットを閉じるためのセッションが必要がないかぎり、ウォレットは開いたままにしておきます。マスター・キーへのアクセスを無効にし、暗号化された列へのアクセスを防止する場合は、ウォレットを閉じることができます。ただし、暗号化されていないデータは使用可能です。透過的データ暗号化を実行するには、ウォレットが開かれている必要があります。ウォレットを再度開くには、ALTER SYSTEM SET WALLET OPEN IDENTIFIED BY *password* 文を使用します。

ウォレットを閉じるには、次のようにします。

- SQL*Plus で、次の文を入力します。

```
ALTER SYSTEM SET ENCRYPTION WALLET CLOSE;
```

手順 4: データを暗号化（または復号化）する

sqlnet.ora ファイルでウォレットのディレクトリの場所を作成し、ウォレット自体を作成したら、個々の表列もしくは表領域全体のいずれかを暗号化できます。

この項の内容は次のとおりです。

- 表の個々の列の暗号化
- 表領域の暗号化

表の個々の列の暗号化 どの列を暗号化の対象として指定するかは、政府によるセキュリティ規則（カリフォルニア州上院法案 1386）もしくは企業（MasterCard や VISA など）が使用するプライベート標準によって決定します。クレジット・カード番号、社会保障番号、その他の個人情報（PII）はこのカテゴリに分類されます。暗号化が必要な他のデータ（企業秘密、研究結果、従業員の給与、ボーナスなど）は、内部のセキュリティ・ポリシーで定義されます。いつデータを暗号化し、いつ暗号化しないかについては、6-3 ページの「データを暗号化するタイミング」を参照してください。

暗号化する列を選択するには、次のガイドラインに従います。

- **暗号化する列のデータ型をチェックします。**透過型データ暗号化は、次のデータ型をサポートします。

BINARY_FLOAT	NUMBER
BINARY_DOUBLE	NVARCHAR2
CHAR	RAW
DATE	TIMESTAMP
NCHAR	VARCHAR2

- **選択した列が外部キーの一部でないことを確認します。**透過的データ暗号化を使用すると、各表に固有の暗号化キーが作成されます。この暗号化キーはデータベースのデータ・ディクショナリに格納され、外部のマスター・キーによって暗号化されます。暗号化列を外部キーとして使用することはできません。

表の列を暗号化するには次のようにします。

1. 必ずウォレット・キーを作成して開いておきます。

   ウォレット・キーの作成方法については、6-5 ページの「手順 2: ウォレットを作成する」を参照してください。既存のウォレット・キーを開くには、6-5 ページの「手順 3: ウォレットを開く（または閉じる）」を参照してください。

2. Database Control を起動します。

   Database Control を起動する手順については、『Oracle Database 2 日でデータベース管理者』を参照してください。

3. 管理者のユーザー名（SYSTEM またはセキュリティ管理者の名前など）とパスワードを入力し、**「ログイン」**をクリックします。

   データベースのホームページが表示されます。

4. **「スキーマ」**をクリックして「スキーマ」サブページを表示します。

5. 「データベース・オブジェクト」で**「表」**を選択します。

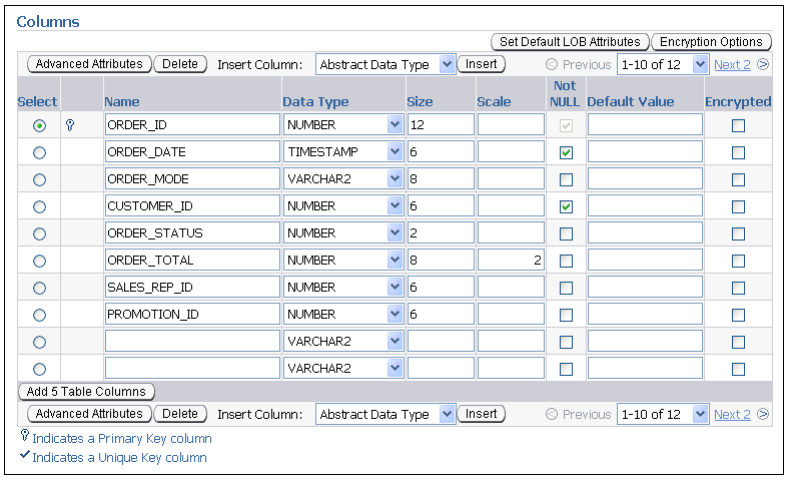
   「表」ページが表示されます。

6. 次のいずれかの操作を行います。

   - 新しい表を作成するには、**「作成」**をクリックしてから表示されたページの質問に回答し、表の作成を開始します。
   - 既存の表を変更するには、スキーマ名を**「スキーマ」**フィールドに、表名を**「オブジェクト名」**フィールドに入力して表名を検索します（パーセント記号（%）ワイルドカード文字を使用して表のグループを検索できます。たとえば、O で始まるすべての表を検索するには、O% を使用します。）。表が「表」ページに示されている場合は、その表を選択して**「編集」**をクリックします。

   「表の作成」または「表の編集」ページで、暗号化オプションを設定できます。

   たとえば、OE.ORDERS 表の列を暗号化する場合、「表の編集」ページは次のように表示されます。



7. 「表の作成」（または「表の編集」）ページで、次の手順を実行します。

   a. 暗号化する列を選択します。

      索引付けされた列や、外部キー制約を使用する列（主キー列または一意キー列）は選択しないでください。これらの列は暗号化できません。これらの列には、名前の左側に鍵またはチェック・マーク・アイコンがあります。

   b. **「暗号化オプション」**をクリックして、「表」ページの暗号化オプションを表示します。

   c. 「暗号化アルゴリズム」リストから次のオプションを選択します。

      - **AES192**: キーの長さを 192 ビットに設定します。AES は「Advanced Encryption Standard」の略です。
      - **3DES168**: キーの長さを 168 ビットに設定します。3DES は「Triple Data Encryption Standard」の略です。
      - **AES128**: キーの長さを 128 ビットに設定します。デフォルトのオプションです。
      - **AES256**: キーの長さを 256 ビットに設定します。

   d. 「キーの生成」で、**「ランダムにキーを生成」**または**「キーの指定」**のどちらかを選択します。**「キーの指定」**を選択した場合は、**「キーの入力」**および**「キーの確認」**フィールドにシード値の文字を入力します。

「ランダムにキーを生成」設定はソルトを有効にします。ソルトは、暗号化されたデータのセキュリティを強化する方法で、暗号化される前のデータに追加されるランダムな文字列です。繰り返されるテキストが、暗号化されたときには異なって表示されます。ソルトによって、攻撃者は、暗号化されたテキストのパターン一致をデータの盗用に使用できなくなります。

e. **「続行」**をクリックして「表の作成」（または「表の編集」）ページに戻ります。

f. **「暗号化」**の下のボックスを選択して、列の暗号化を有効にします。

8. **「続行」**をクリックします。

   表の作成（または「表の編集」）ページが表示されます。

列内の既存のデータおよび将来格納されるデータは、データベース・ファイルに書き込まれるときに暗号化され、認可されたユーザーが選択したときに復号化されます。表の更新時は、読取りアクセスのみが可能です。データ操作言語（DML）文が必要な場合は、オンラインで再定義できます。

表領域の暗号化 新規表領域の作成中に新規表領域を暗号化することはできますが、既存の表領域を暗号化することはできません。回避策として、`CREATE TABLE AS SELECT`、`ALTER TABLE MOVE` を使用するか、または Oracle Data Pump インポートを使用して既存の表領域からデータを取得し、暗号化されている表領域に格納することができます。表領域の作成の詳細は、『Oracle Database 2 日でデータベース管理者』を参照してください。

表領域を暗号化するには、次のようにします。

1. 必ずウォレット・キーを作成して開いておきます。

   ウォレット・キーの作成方法については、6-5 ページの「手順 2: ウォレットを作成する」を参照してください。既存のウォレット・キーを開くには、6-5 ページの「手順 3: ウォレットを開く（または閉じる）」を参照してください。

2. Database Control を起動します。

   Database Control を起動する手順については、『Oracle Database 2 日でデータベース管理者』を参照してください。

3. 管理者のユーザー名（`SYSTEM` またはセキュリティ管理者の名前など）とパスワードを入力し、**「ログイン」**をクリックします。

   データベースのホームページが表示されます。

4. **「サーバー」**をクリックして、「サーバー」サブページを表示します。

5. 「記憶域」で、**「表領域」**をクリックします。

   「表領域」ページが表示されます。

6. **「作成」**をクリックしてから表示されたページの質問に回答し、表領域と必要なデータ・ファイルの作成を開始します。

7. 「表領域の作成」ページで、次のステップを実行します。

   a. 「タイプ」で、「永続」の**「暗号化」**ボックスを選択します。

   b. **「暗号化」**オプションを選択して、「暗号化オプション」ページを表示します。

   c. 「暗号化アルゴリズム」リストから次のオプションを選択します。

      – **AES192**: キーの長さを 192 ビットに設定します。AES は「Advanced Encryption Standard」の略です。

      – **3DES168**: キーの長さを 168 ビットに設定します。3DES は「Triple Data Encryption Standard」の略です。

      – **AES128**: キーの長さを 128 ビットに設定します。デフォルトのオプションです。

      – **AES256**: キーの長さを 256 ビットに設定します。

暗号化アルゴリズムの詳細は、5-6 ページの「ネットワーク暗号化の設定」の手順 5 の「使用可能なメソッド」を参照してください。

d. **「続行」**をクリックします。

「表領域の作成」ページが表示されます。

8. **「OK」**をクリックします。

既存の表領域のリストに新規表領域が表示されます。既存の表領域は暗号化できないことに注意してください。

関連項目：

- 暗号化されている既存の表領域をデータベースに問い合せるには、6-10 ページの「現行のデータベース・インスタンスで暗号化されている表領域のチェック」を参照してください。
- 表領域の暗号化の詳細は、『Oracle Database Advanced Security 管理者ガイド』を参照してください。
- `CREATE TABLESPACE` 文の詳細は、『Oracle Database SQL 言語リファレンス』を参照してください。

既存の暗号化データのチェック

すでに暗号化されているデータについて、データベースに問い合せることができます。暗号化された個々の列、暗号化された列を含む現行のデータベース・インスタンスのすべての表、暗号化されているすべての表領域をチェックできます。

この項の内容は次のとおりです。

- ウォレットが開いているか閉じているかのチェック
- 個々の表の暗号化されている列のチェック
- 現行のデータベース・インスタンスで暗号化されているすべての表列のチェック
- 現行のデータベース・インスタンスで暗号化されている表領域のチェック

ウォレットが開いているか閉じているかのチェック

`V$ENCRYPTION_WALLET` ビューを実行することで、ウォレットが開いているか閉じているかを確認できます。

ウォレットが開いているか閉じているかチェックするには、次のようにします。

- SQL*Plus で、`V$ENCRYPTION_VIEW` ビューを次のように実行します。

```
SELECT * FROM V$ENCRYPTION_WALLET;
```

ウォレット・ステータスが次のように表示されます。

```
WRL_TYPE  WRL_PARAMETER                              STATUS
--------  -----------------------------------------  -------
file      C:\oracle\product\11.1.0\db_1\wallets      OPEN
```

個々の表の暗号化されている列のチェック

SQL*Plus で `DESC`（`DESCRIBE`）文を使用して、データベース表内の暗号化されている列をチェックします。

個々の表の暗号化されている列をチェックするには、次のようにします。

- SQL*Plus で、次の構文を使用して `DESC` 文を実行します。

```
DESC tablename;
```

次に例を示します。

```
DESC OE.ORDER_ITEMS;
```

表スキーマの説明が表示されます。次に例を示します。

```
Name                                      Null?    Type
----------------------------------------- -------- ----------------------------
ORDER_ID                                  NOT NULL NUMBER(12)
LINE_ITEM_ID                              NOT NULL NUMBER(3)
PRODUCT_ID                                NOT NULL NUMBER(6)
UNIT_PRICE                                         NUMBER(8,2)
QUANTITY                                           NUMBER(8) ENCRYPT
```

現行のデータベース・インスタンスで暗号化されているすべての表列のチェック

暗号化されているすべての表列をチェックするには、DBA_ENCRYPTED_COLUMNS ビューを使用します。

現行のデータベース・インスタンスで暗号化されているすべての表列をチェックするには、次のようにします。

- SQL*Plus で、DBA_ENCRYPTED_COLUMNS ビューから選択します。

  次に例を示します。

  ```
  SELECT * FROM DBA_ENCRYPTED_COLUMNS;
  ```

  この SELECT 文によって、Oracle Transparent Data Encryption を使用して暗号化された列を含む、データベースのすべての表および列がリストされます。次に例を示します。

  ```
  OWNER        TABLE_NAME    COLUMN_NAME    ENCRYPTION_ALG     SALT
  -----------  ----------    -----------    ----------------   ----
  OE           CUSTOMERS     INCOME_LEVEL   AES 128 bits key   YES
  OE           UNIT_PRICE    ORADER_ITEMS   AES 128 bits key   YES
  HR           EMPLOYEES     SALARY         AES 192 bits key   YES
  ```

  関連項目： DBA_ENCRYPTED_COLUMNS ビューの詳細は、『Oracle Database リファレンス』を参照してください。

現行のデータベース・インスタンスで暗号化されている表領域のチェック

表 6-1 に、暗号化されている表領域のチェックに使用できるデータ・ディクショナリ・ビューを示します。

表 6-1 暗号化されている表領域のデータ・ディクショナリ・ビュー

データ・ディクショナリ・ビュー	説明

DBA_TABLESPACES	データベース内のすべての表領域が示されます。たとえば、表領域が暗号化されているかどうかを調べるには、次のように入力します。
	`SELECT TABLESPACE_NAME, ENCRYPTED FROM DBA_TABLESPACES`
	
	`TABLESPACE_NAME ENC`
	`------------------------------ ----`
	`SYSTEM NO`
	`SYSAUX NO`
	`UNCOTBS1 NO`
	`TEMP NO`
	`USERS NO`
	`EXAMPLE NO`
	`SECURESPACE YES`

表 6-1 暗号化されている表領域のデータ・ディクショナリ・ビュー（続き）

データ・ディクショナリ・ビュー	説明
USER_TABLESPACES	現在のユーザーがアクセス可能な表領域が示されます。DBA_TABLESPACES と同じ列（PLUGGED_IN 列を除く）が含まれています。

V$ENCRYPTED_TABLESPACE	暗号化されている表領域に関する情報が示されます。次に例を示します。
	`SELECT * FROM V$ENCRYPTED_TABLESPACES;`
	
	`TS# ENCRYPTIONALG ENCRYPTEDTS`
	`---------- -------------- -----------`
	`6 AES128 YES`
	
	このリストには、表領域番号、暗号化アルゴリズム、暗号化が有効か無効かなどが示されます。

関連項目： データ・ディクショナリ・ビューの詳細は、『Oracle Database リファレンス』を参照してください。

Oracle Virtual Private Database によるデータ・アクセスの制御

Oracle Virtual Private Database（VPD）では、ユーザーが実行する任意の SQL 文に WHERE 句を動的に追加することができます。WHERE 句により、ユーザーの資格証明に基づいて、ユーザーがアクセスを許可されているデータがフィルタ処理されます。

この項の内容は次のとおりです。

- Oracle Virtual Private Database について
- チュートリアル : Oracle Virtual Private Database ポリシーの作成

関連項目： Oracle Virtual Private Database の動作については、『Oracle Database セキュリティ・ガイド』を参照してください。

Oracle Virtual Private Database について

Oracle Virtual Private Database（VPD）は、データベースの表またはビュー・レベルの行レベル・セキュリティを提供します。これを拡張して列レベル・セキュリティを提供することもできます。基本的に仮想プライベート・データベースは、仮想プライベート・データベースのセキュリティ・ポリシーの適用対象である表またはビューで使用される、任意の SQL 文に追加的な WHERE 句を挿入します（セキュリティ・ポリシーはデータへのアクセスを許可または阻止する機能です）。WHERE 句では、セキュリティ・ポリシーを通過した資格証明を持つ、すなわち、保護する対象のデータへのアクセス権を持つユーザーのみが許可されます。

Oracle Virtual Private Database のポリシーには次のコンポーネントがあり、通常はセキュリティ管理者のスキーマに作成されます。

- **仮想プライベート・データベースの表に影響する SQL 文に動的 WHERE 句を追加する PL/SQL ファンクション。**たとえば、次の SELECT 文が変換されます。

```
SELECT * FROM orders;
```

この文は次のように変換されます。

```
SELECT * FROM orders
  WHERE SALES_REP_ID = 159;
```

この例では、ユーザーが表示できるのは、販売担当者 159 による注文のみです。この WHERE 句の生成に使用される PL/SQL ファンクションは次のようになります。

```
1    CREATE OR REPLACE FUNCTION auth_orders(
2     schema_var IN VARCHAR2,
3     table_var  IN VARCHAR2
4    )
5    RETURN VARCHAR2
6    IS
7     return_val VARCHAR2 (400);
8    BEGIN
9     return_val := 'SALES_REP_ID = 159';
10    RETURN return_val;
11   END auth_orders;
12   /
```

この例では、次のとおりです。

- **2 ～ 3 行目 :** スキーマ名 OE と表名 ORDERS を格納するパラメータが作成されます。（表に対する 2 番目のパラメータ table_var は、ビューおよびシノニムにも使用できます。）これらの 2 つのパラメータは、常にこの順序で作成されます。つまり、スキーマのパラメータが最初に作成され、その後、表、ビューまたはシノニム・オブジェクトのパラメータが作成されます。ファンクション自体では、OE スキーマ、またはその ORDERS 表は指定されないことに注意してください。作成する仮想プライベート・データベース・ポリシーでは、OE.ORDERS 表の指定にこれらのパラメータが使用されます。
- **5 行目 :** WHERE 述語句に使用される文字列を返します。
- **6 ～ 10 行目 :** WHERE SALES_REP_ID = 159 述語の作成が含まれます。

WHERE 句は、ユーザーのセッション情報（ユーザー ID など）に基づいてユーザー情報をフィルタ処理するよう構成できます。これを行うには、アプリケーション・コンテキストを作成します。アプリケーション・コンテキストは、名前と値のペアです。次はその例です。

```
SELECT * FROM oe.orders
 WHERE sales_rep_id = SYS_CONTEXT('userenv','session_user');
```

この例では、WHERE 句で SYS_CONTEXT PL/SQL ファンクションを使用して、userenv コンテキストによって示されるユーザーのセッション ID（session_user）を取得しています。アプリケーション・コンテキストの詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。

- **パッケージにポリシーを追加する方法。** Database Control または DBMS_RLS.ADD_POLICY 関数を使用して、パッケージにポリシーを追加します。DBMS_RLS PL/SQL パッケージを使用するには、その PL/SQL パッケージに対する EXECUTE 権限を付与される必要があります。ユーザー SYS が DBMS_RLS パッケージを所有しています。

データベース・レベルで行レベルのセキュリティを強制する方法は、アプリケーション・プログラム・レベルでセキュリティを強制した場合に比べて多くのメリットがあります。データを保護する場所であるデータベース自体にセキュリティ・ポリシーを実装できるため、様々な方法でアクセスされた場合でも攻撃を受ける可能性が低くなります。このセキュリティは、ユーザー（侵入者）がどれだけデータへのアクセスを試行しても存在し、強制されます。データベースに接続するすべてのアプリケーションでポリシーを維持する必要はなく、1 箇所（データベース）のみでポリシーを維持できるため、メンテナンス費も低く抑えられます。固有の DML 操作に対してポリシーを作成できるため、非常に柔軟性の高いポリシーを適用できます。

チュートリアル : Oracle Virtual Private Database ポリシーの作成

注文入力データベースの OE の ORDERS 表には次の情報が含まれています。

```
Name                                      Null?    Type
----------------------------------------- -------- ------------------------------
ORDER_ID                                  NOTNULL  NUMBER(12)
ORDER_DATE                                NOTNULL  TIMESTAMP(6) WITH LOCAL TIME ZONE
ORDER_MODE                                         VARCHAR2(8)
CUSTOMER_ID                               NOTNULL  NUMBER(6)
ORDER_STATUS                                       NUMBER(2)
ORDER_TOTAL                                        NUMBER(8,2)
SALES_REP_ID                                       NUMBER(6)
PROMOTION_ID                                       NUMBER(6)
```

表を問い合せる個人に基づいて表へのアクセスを制限すると想定します。たとえば営業担当者は作成された注文のみを確認でき、他の従業員は確認できないようにします。このチュートリアルでは、営業担当者のユーザー・アカウントと財務管理者のアカウントを作成し、ロールに基づいてデータ・アクセスを制限する Oracle Virtual Private Database を作成します。

作成する仮想プライベート・データベース・ポリシーは、PL/SQL ファンクションに関連付けられます。VPD ポリシーは PL/SQL ファンクションまたはプロシージャによって制御されるため、アクセスを制限するポリシーを様々な方法で設計できます。このチュートリアルでは、直属の上司が誰であるかに基づいて従業員のアクセスを制限するファンクションを作成します。このファンクションでは、顧客の ID に基づいて顧客のアクセスが制限されます。

データベース管理者やアプリケーション・アカウントとは別のデータベース・アカウントに VPD ポリシーを格納する場合があります。このチュートリアルでは、4-4 ページの「チュートリアル : セキュア・アプリケーション・ロールの作成」で作成した sec_admin アカウントを使用して VPD ポリシーを作成します。アプリケーション表と VPD ポリシーを分けることで、セキュリティを高めます。

行データの機密性に基づいてアクセスを制限するには、Oracle Label Security（OLS）を使用します。OLS を使用すると、様々なレベルのセキュリティでデータを分類できます。この場合、行内のデータにアクセスできるユーザーをレベルごとに設定できます。この方法では、データのアクセス制御は、ユーザーの権限ではなくデータ自体に焦点が当てられます。詳細は、6-20 ページの「Oracle Label Security による行レベルのセキュリティの強制」を参照してください。

このチュートリアルでは、次の手順を実行します。

- 手順 1: 必要に応じてセキュリティ管理者アカウントを作成する
- 手順 2: セキュリティ管理者アカウントを更新する
- 手順 3: このチュートリアルで使用するユーザー・アカウントを作成する
- 手順 4: F_POLICY_ORDERS ポリシーのファンクションを作成する
- 手順 5: ACCESSCONTROL_ORDERS 仮想プライベート・データベース・ポリシーを作成する
- 手順 6: ACCESSCONTROL_ORDERS 仮想プライベート・データベース・ポリシーをテストする
- 手順 7: このチュートリアルで使用したコンポーネントを削除する（オプション）

手順 1: 必要に応じてセキュリティ管理者アカウントを作成する

4-4 ページの「チュートリアル : セキュア・アプリケーション・ロールの作成」で、チュートリアルで使用するために sec_admin というセキュリティ管理者アカウントを作成しました。このチュートリアルでも、このアカウントを使用できます。まだこのアカウントを作成していない場合は、4-4 ページの「手順 1: セキュリティ管理者アカウントを作成する」の手順を実行して、sec_admin を作成します。

手順 2: セキュリティ管理者アカウントを更新する

sec_admin アカウント・ユーザーには、DBMS_RLS パッケージを使用するための権限が必要です。このパッケージは SYS が所有しているため、このパッケージ権限を sec_admin に付与するには、SYS としてログオンする必要があります。また、sec_admin ユーザーには、OE スキーマの CUSTOMERS 表および HR スキーマの EMPLOYEES 表に対する SELECT 権限も必要です。

sec_admin に DBMS_RLS パッケージを使用する権限を付与するには、次のようにします。

1. Database Control を起動します。

   Database Control を起動する手順については、『Oracle Database 2 日でデータベース管理者』を参照してください。

2. SYS ユーザーとしてログインし、SYSDBA 権限で接続します。

   - **ユーザー名** : SYS
   - **パスワード** : SYS のパスワードを入力します。
   - **接続モード** : SYSDBA

3. **「サーバー」**をクリックして、「サーバー」サブページを表示します。

4. 「セキュリティ」で、**「ユーザー」**を選択します。

   「ユーザー」ページが表示されます。

5. **SEC_ADMIN** を選択して、**「編集」**をクリックします。

   「ユーザーの編集」ページが表示されます。

6. **「オブジェクト権限」**をクリックして「オブジェクト権限」ページを表示します。

7. 「オブジェクト・タイプの選択」リストから**「パッケージ」**を選択し、次に**「追加」**をクリックします。

   「パッケージオブジェクト権限の追加」ページが表示されます。

8. 「パッケージオブジェクトの選択」で SYS.DBMS_RLS と入力し、sec_admin に DBMS_RLS パッケージへのアクセス権を与えます。

9. 「使用可能な権限」で **EXECUTE** を選択し、**「移動」**をクリックして「選択した権限」リストに移動します。

10. **「OK」**をクリックします。

    「ユーザーの編集」ページが表示されます。

11. 「オブジェクト・タイプの選択」リストから**「表」**を選択し、次に**「追加」**をクリックします。

    「表オブジェクト権限の追加」ページが表示されます。

12. **「表オブジェクト」**を選択してから、HR.EMPLOYEES と入力し、sec_admin に HR.EMPLOYEES 表へのアクセス権を付与します。

13. 「使用可能な権限」で**「SELECT」**を選択し、**「移動」**をクリックして「選択した権限」リストに移動します。

14. **「OK」**をクリックします。

    「ユーザーの編集」ページが表示されます。

15. **「適用」**をクリックします。

手順 3: このチュートリアルで使用するユーザー・アカウントを作成する

OE.ORDERS 表へのアクセスを必要とする従業員のための、ユーザー・アカウントを作成する準備ができました。

従業員ユーザー・アカウントを作成するには、次のようにします。

1. Database Control で**「データベース・インスタンス」**リンクの**「ユーザー」**をクリックして、「ユーザー」ページに戻ります。

   「ユーザー」ページが表示されます。

2. **「作成」**をクリックします。

   「ユーザーの作成」ページが表示されます。

3. 次の情報を入力します。

   - **名前 :** LDORAN（Louise Doran のユーザー・アカウントを作成するため）
   - **プロファイル** : デフォルト
   - **認証** : パスワード
   - **「パスワードの入力」**および**「パスワードの確認」**: 3-9 ページの「パスワードの作成要件」に示されている要件を満たすパスワードを入力します。
   - **デフォルト表領域** : USERS
   - **一時表領域** : TEMP
   - **ステータス** : ロック解除

4. **「OK」**をクリックします。

   LDORAN が新しいユーザーとして表示された状態で「ユーザー」ページが表示されます。

5. 「ユーザー」ページで**「LDORAN」**を選択します。

   「ユーザーの編集」ページが表示されます。

6. **「オブジェクト権限」**を選択して、「オブジェクト権限」サブページを表示します。

7. 「オブジェクト・タイプの選択」リストから**「表」**を選択し、次に**「追加」**をクリックします。

   「表オブジェクト権限の追加」ページが表示されます。

8. **「表オブジェクトの選択」**で、次のテキストを入力します。

   ```
   OE.ORDERS
   ```

   このテキストにはスペースを含めないでください。

9. 「使用可能な権限」リストから **SELECT** を選択し、**「移動」**をクリックして「選択した権限」リストに移動します。**「OK」**をクリックします。

   OE.ORDERS の SELECT 権限がリストされた状態で「ユーザーの作成」ページが表示されます。

10. **「適用」**をクリックします。

11. **「LDORAN」**を選択してから、**「アクション」**リストで**「類似作成」**を選択します。次に**「実行」**をクリックします。

    「ユーザーの作成」ページが表示されます。

12. 次の情報を入力します。

    - **名前** : LPOPP（財務管理者の Luis Popp のユーザー・アカウントを作成するため）
    - **「パスワードの入力」**および**「パスワードの確認」**: 3-9 ページの「パスワードの作成要件」に示されている要件を満たすパスワードを入力します。

13. **「OK」**をクリックします。

両方の従業員アカウントが作成され、これらには同じ権限があります。一方が OE.ORDERS 表で SELECT 文を実行すると、すべてのデータを確認できます。

手順 4: F_POLICY_ORDERS ポリシーのファンクションを作成する

f_policy_orders ポリシーは、ORDERS 表に問合せを行うユーザーのフィルタリングに使用される、ポリシーを定義する PL/SQL ファンクションです。ユーザーをフィルタリングするために、ポリシー・ファンクションでは、データベースにログイン中のユーザーに関するセッション情報を取得する SYS_CONTEXT PL/SQL ファンクションが使用されます。

アプリケーション・コンテキストとパッケージを作成するには、次のようにします。

1. Database Control で**「ログアウト」**をクリックし、次に**「ログイン」**をクリックします。
2. ユーザー sec_admin としてログインします。
3. **「スキーマ」**をクリックして「スキーマ」サブページを表示します。
4. 「プログラム」で**「ファンクション」**を選択します。

   「ファンクション」ページが表示されます。
5. **「作成」**をクリックします。

   「ファンクションの作成」ページが表示されます。
6. 次の情報を入力します。
   - **名前**: F_POLICY_ORDERS
   - **スキーマ**: SEC_ADMIN
   - **ソース:** 次のコードを入力し（ただしコード左側の行番号は入力しない）、ログオンしたユーザーが営業担当者かどうかをチェックするファンクションを作成します。

     f_policy_orders ファンクションが、ユーザーのセッション情報を取得する SYS_CONTEXT PL/SQL ファンクションを使用してこれを実行し、sec_admin が SELECT 権限を持つ HR.EMPLOYEES 表にあるユーザーのジョブ ID とこの情報を比較します。

```
1    (schema in varchar2,
2    tab in varchar2)
3    return varchar2
4    as
5     v_job_id   varchar2(20);
6     v_user     varchar2(100);
7     predicate  varchar2(400);
8
9    begin
10    v_job_id  := null;
11    v_user    := null;
12    predicate := '1=2';
13
14   v_user := lower(sys_context('userenv','session_user'));
15
16    select lower(job_id) into v_job_id from hr.employees
17      where lower(email) = v_user;
18
19    if  v_job_id='sa_rep' then
20       predicate := '1=1';
21    else
22       null;
23    end if;
24
25    return predicate;
26
27    exception
28     when no_data_found then
29      null;
30   end;
```

この例では、次のとおりです。

- **1 ～ 2 行目 :** 保護する必要があるスキーマ（schema）と表（tab）のパラメータを定義します。このファンクションは OE.ORDERS 表を指定しません。「手順 5: ACCESSCONTROL_ORDERS 仮想プライベート・データベース・ポリシーを作成する」で作成した ACCESSCONTROL_ORDERS ポリシーによりこれらのパラメータが使用され、OE スキーマと schema 表が指定されます。最初に schema パラメータを作成し、その後に tab パラメータを作成してください。
- **3 行目 :** WHERE 述語句に使用される文字列を返します。この戻り値のデータ型としては VARCHAR2 が常に使用されます。
- **4 から 7 行目 :** ジョブ ID、ログオンしたユーザーのユーザー名、および述語句を格納するよう変数を定義します。
- **9 ～ 25 行目 : 9 行目**の BEGIN 句で開始する WHERE 述語の作成が含まれます。
- **10 から 12 行目 :** v_job_id および v_user 変数を NULL に設定し、predicate 変数を 1=2、つまり誤った値に設定します。この段階では、変数が **16 行目**から始まるテストに通るまで、WHERE 述語は一切生成されません。
- **14 行目 :** SYS_CONTEXT ファンクションを使用してユーザーのセッション情報を取得し、v_user 変数に記述します。
- **16 ～ 23 行目 :** ジョブ ID をログオンしたユーザーと比較して、ユーザーが営業担当者かどうかをチェックします。ログオンしたユーザーのジョブ ID が sa_rep（営業担当者）である場合は、predicate 変数が 1=1 に設定されます。つまりユーザーは営業担当者であることになり、テストに通ります。
- **25 行目 :** WHERE *role_of_user_logging_on* IS "sa_rep" に翻訳される WHERE 述語が返されます。この WHERE 述語は、ユーザー LDORAN と LPOPP が OE.ORDERS 表に対して発行する SELECT 文に追加されます。
- **27 ～ 29 行目 :** 適切な権限を持っていないユーザーがログオンした場合は、EXCEPTION 句が提供されます。

7. 「**OK**」をクリックします。

手順 5: ACCESSCONTROL_ORDERS 仮想プライベート・データベース・ポリシーを作成する

仮想プライベート・データベース・ポリシー・ファンクションの作成が終了したため、仮想プライベート・データベース・ポリシー accesscontrol_orders を作成し、これを ORDERS 表に追加できます。パフォーマンスを向上させるため CONTEXT_SENSITIVE パラメータをポリシーに追加します。これによって、アプリケーション・コンテキストの内容が変わった場合、このケースでは新しいユーザーがログオンした場合のみ、Oracle Database は f_policy_orders ファンクションを実行します。Oracle Database は、ユーザーが ORDERS 表で SQL SELECT 文を実行したときのみポリシーをアクティブにします。INSERT、UPDATE および DELETE 文は権限を付与されていないため、使用できません。

ACCESSCONTROL_ORDERS 仮想プライベート・データベース・ポリシーを作成するには、次のようにします。

1. Database Control で**「データベース・インスタンス」**リンクをクリックして、データベースのホームページを表示します。
2. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
3. 「セキュリティ」セクションで**「仮想プライベート・データベース・ポリシー」**をクリックします。

   「仮想プライベート・データベース・ポリシー」ページが表示されます。
4. **「作成」**をクリックします。

   「ポリシーの作成」ページが表示されます。

5. 「一般」で、次の入力を行います。
   - **ポリシー名**: ACCESSCONTROL_ORDERS
   - **オブジェクト名**: OE.ORDERS
   - **ポリシー・タイプ**:「CONTEXT_SENSITIVE」を選択します。

     最後にカーソルが使用されてからコンテキストが変更されている場合、このタイプは文の実行時にポリシー・ファンクションを再評価します。複数のクライアントが 1 つのデータベース・セッションを共有するセッション・プーリングの場合、クライアント切替え時に中間層でコンテキストをリセットする必要があります。Oracle Database は、このポリシー・タイプのファンクションにより戻された値をキャッシュしません。常に文の解析時にポリシー・ファンクションを実行します。CONTEXT_SENSITIVE ポリシー・タイプは 1 つのオブジェクトのみに適用されます。

     ポリシー・タイプを有効にするには、**「有効」**ボックスを選択します。
6. 「ポリシー・ファンクション」で次の入力を行います。
   - **ポリシー・ファンクション**: ポリシーの述語を生成するファンクション名（この場合は SEC_ADMIN.F_POLICY_ORDERS）を入力します。
   - **長い述語**: このボックスは選択しないでください。

     通常は、32KB までの長さの述語を返すためにこのボックスを選択します。このボックスを選択しないと、Oracle Database は述語を 4000 バイトに制限します。
7. 「強制」で、**「SELECT」**を選択します。
8. **「OK」**をクリックします。

手順 6: ACCESSCONTROL_ORDERS 仮想プライベート・データベース・ポリシーをテストする

この段階では、それぞれのユーザーとしてログオンし、ORDERS 表からのデータの選択を試すことで、accesscontrol_orders ポリシーをテストします。

ACCESSCONTROL_ORDERS ポリシーをテストするには、次のようにします。

1. SQL*Plus を起動します。

   コマンド・プロンプトで、次のコマンドを入力して SQL*Plus を起動し、販売担当者 Louise Doran（ユーザー名は LDORAN）としてログインします。

   ```
   SQLPLUS LDORAN
   Enter password: password
   ```

   SQL*Plus が起動し、デフォルトのデータベースに接続してから、プロンプトが表示されます。

   SQL*Plus の起動の詳細は、『Oracle Database 2 日でデータベース管理者』を参照してください。
2. 次の SELECT 文を入力します。

   ```
   SELECT COUNT(*) FROM OE.ORDERS;
   ```

   Louise に関する次のような結果が表示されます。表示のとおり、Louise は OE.ORDERS 表のすべての注文にアクセスできます。

   ```
   COUNT(*)
   --------
        105
   ```
3. 財務管理者の Luis Popp として接続します。

   ```
   CONNECT LPOPP
   Enter password: password
   ```

4. 次の SELECT 文を入力します。

```
SELECT COUNT(*) FROM OE.ORDERS;
```

Popp 氏は営業担当者ではないので、OE.ORDERS 表のデータへのアクセスがなく、次のような結果が表示されます。

```
COUNT(*)
--------
       0
```

5. SQL*Plus を終了します。

```
EXIT
```

手順 7: このチュートリアルで使用したコンポーネントを削除する（オプション）

このチュートリアルの終了後、使用したデータ構造が不要な場合は削除できます。

sec_admin で作成したデータ構造を削除するには、次のようにします。

1. Database Control で、ユーザー sec_admin としてログインします。
2. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
3. 「セキュリティ」で、**「仮想プライベート・データベース・ポリシー」**を選択します。

   「仮想プライベート・データベース・ポリシー」ページが表示されます。
4. 「検索」で次の情報を入力して、**「実行」**をクリックします。
   - **スキーマ名** : OE
   - **オブジェクト名** : ORDERS
   - **ポリシー名** : %

   作成したポリシーの ACCESSCONTROL_ORDERS が表示されます。
5. **「ACCESSCONTROL_ORDERS」**を選択し、**「削除」**をクリックします。
6. 「確認」ページで**「はい」**をクリックします。

ユーザー・アカウントおよびロールを削除するには、次のようにします。

1. Database Control で**「ログアウト」**をクリックし、次に**「ログイン」**をクリックします。
2. このチュートリアルで使用されるユーザー・アカウントとロールを作成した管理者ユーザーとしてログインします。
3. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
4. 「セキュリティ」で、**「ユーザー」**を選択します。

   「ユーザー」ページが表示されます。
5. 次の各ユーザーを選択し、**「削除」**をクリックしてそれらを削除します。
   - LDORAN
   - LPOPP

   sec_admin は削除しないでください。このマニュアルの以降のチュートリアルで、このアカウントが必要になります。
6. Database Control を終了します。

Oracle Label Security による行レベルのセキュリティの強制

Oracle Label Security（OLS）は、データベース表に行レベルのセキュリティを提供します。セキュリティのレベルを定義する 1 つまたは複数のセキュリティ・ラベルを表のデータ行に割り当てることで、セキュリティを実装できます。

この項の内容は次のとおりです。

Oracle Label Security について

Oracle Label Security を使用すると、データベース表を行レベルで保護でき、ニーズに応じて行を様々なセキュリティ・レベルに割り当てることができます。たとえば、非常に機密性の高いデータを含む行には HIGHLY SENSITIVE というラベルを割り当て、機密性がそれほど高くないデータを含む行には SENSITIVE というラベルを割り当てたりできます。すべてのユーザーがアクセスできる行には PUBLIC というラベルを割り当てます。ラベルは必要なだけ作成でき、使用する環境のセキュリティ要件に適合させることができます。

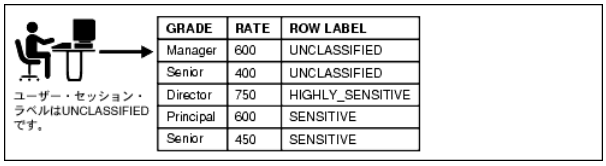
ラベルを作成して割り当てたら、Oracle Label Security を使用して、これらのラベルに基づき特定の行に特定のユーザー認可を割り当てます。以降、Oracle Label Security はデータ行のラベルとユーザーのセキュリティ・クリアランスを自動的に比較し、行のデータにユーザーがアクセスできるかどうかを決定します。

Oracle Label Security ポリシーには次のコンポーネントがあります。

- **ラベル。**データおよびユーザー、ユーザーとプログラム・ユニットの認証のラベルは、保護されている特定のオブジェクトへのアクセスを制御します。ラベルは、次の要素で構成されています。
  - **レベル。**レベルにより、行に割り当てる機密性のタイプが指定されます。たとえば、SENSITIVE や HIGHLY SENSITIVE などです。
  - **コンパートメント。**（オプション）データは、レベルが同じでも、企業内の別々のプロジェクト（たとえば ACME Merger や IT Security など）に属すことができます。コンパートメントはこの例ではプロジェクトのことで、より厳密なアクセス制御を定義できます。コンパートメントは行政環境でよく使用されます。
  - **グループ。**（オプション）グループは、データを所有する組織またはデータにアクセスする組織を識別します。たとえば、UK、US、Asia、Europe などです。グループは商業環境と行政環境の両方で使用され、柔軟性が高いことからコンパートメントのかわりに使用されることもあります。
- **ポリシー。**ポリシーは、ラベル、ルール、認証と関連付けられる名前です。

Oracle Label Security のラベルとポリシーは、Database Control で作成するか、SA_SYSDBA、SA_COMPONENTS、SA_LABEL_ADMIN PL/SQL パッケージを使用して作成できます。PL/SQL パッケージの詳細は、『Oracle Label Security 管理者ガイド』を参照してください。このマニュアルには、Database Control を使用して Oracle Label Security のラベルとポリシーを作成する方法が記載されています。

たとえば、ユーザーがアプリケーション表の SELECT 権限を持っているとします。次の図にあるように、ユーザーが SELECT 文を実行すると、Oracle Label Security は選択された各行を評価して、このユーザーがアクセスできるかどうかを決定します。決定は、セキュリティ管理者がユーザーに割り当てた権限とアクセス・ラベルに基づいて行われます。Oracle Label Security を設定して、UPDATE、DELETE、INSERT 文でもセキュリティ・チェックを行うことができます。



Oracle Label Security のポリシー計画のガイドライン

Oracle Label Security ポリシーを作成する前に、アプリケーション・スキーマにラベルを適用する場所と方法を決定する必要があります。

アプリケーション・データの Oracle Label Security ポリシーを適用する場所と方法を決定するには、次のガイドラインに従います。

1. **アプリケーション・スキーマを分析する。**

   Oracle Label Security ポリシーを適用する必要がある表を特定します。多くの場合、Oracle Label Security ポリシーが必要となるアプリケーションの表は限られています。たとえば、ルックアップ値や定数を格納している表などは、通常セキュリティ・ポリシーで保護する必要はありません。ただし、患者の病歴や従業員の給与などの機密データを含む表は、ポリシーを使用して保護する必要があります。

2. **データ・レベルの使用を分析する。**

   表の特定後、表のデータを評価して、表のセキュリティ・レベルを決定します。分析のこの段階では、ビジネス活動について熟知しているユーザーの意見も参考にしてください。

   データ・レベルはデータの機密性を表します。データ・レベルには、`PUBLIC`、`SENSITIVE`、`HIGHLY SENSITIVE` などがあります。今後、機密性がどう変化するかも考慮する必要があります。そうすることで、強固なラベル定義が作成できます。

   データ・レコードに割り当てられた機密性ラベルのレベル・コンポーネントが、ユーザーのクリアランスより低いレベルの場合、このレコードにアクセスするユーザーにはこの行へのアクセス権が付与されます。

3. **データ・コンパートメントの使用を分析する。**

   データ・コンパートメントは主に、行政環境で使用されます。使用するアプリケーションが商業アプリケーションの場合、多くの場合はデータ・コンパートメントを作成しません。

4. **データ・グループを分析する。**

   データ・グループとデータ・コンパートメントは通常、組織、地域、データ所有者によってデータへのアクセスを制御するために使用されます。たとえば、アプリケーションが販売アプリケーションの場合、国または地域によって販売データへのアクセスを制御できます。

   コンパートメントおよびグループと一緒に機密性ラベルがデータ・レコードに割り当てられた場合、このデータを読み取るユーザーは、データ・ラベル、データ・ラベルのすべてのコンパートメント、機密性ラベル内の少なくとも 1 つのグループのレベルと同等またはそれ以上のレベルのユーザー・クリアランスを持っている必要があります。グループは階層になっているため、データ・ラベルに割り当てられた機密性ラベルの 1 つのグループの親を所有している場合は、そのレコードにもアクセスできます。

5. **ユーザー分布を分析する。**

   ユーザーを複数のユーザー・タイプに分類します。たとえば、通常ユーザー、特権ユーザー、管理ユーザーのいずれかに指定します。ユーザーのカテゴリを作成したら、手順 2 で作成したデータ・レベルと比較します。カテゴリは、手順 1 で実行したスキーマ分析で識別した各表に正確に対応する必要があります。次に、ユーザー分布の組織構造を手順 4 で識別したデータ・グループと比較します。

6. **特権ユーザーと管理ユーザーを確認して、割り当てる Oracle Label Security 認可を決定する。**

   Oracle Label Security には、ユーザーに割り当てることのできる特別な認可が複数あります。多くの場合、通常ユーザーに特別な認可は必要ありません。認可の詳細は、『Oracle Label Security 管理者ガイド』を参照してください。

7. **収集したデータを確認し、ドキュメント化する。**

   この手順は企業全体の連続性を維持するために重要であり、ドキュメントは企業のセキュリティ・ポリシーの一部となります。たとえば、このドキュメントには保護されるアプリケーションのリストとその理由などが含まれます。

チュートリアル : HR.LOCATIONS 表へのセキュリティ・ラベルの適用

このチュートリアルでは、Oracle Label Security を使用する一般的な方法を説明します。ここでは HR.LOCATIONS 表にセキュリティ・ラベルを適用します。ユーザー sking、kpartner、ldoran は、この表内の特定の行に対して、LOCATIONS 表の都市に基づくアクセス権を持っています。

Oracle Label Security を使用して、行データに焦点を当て、データの機密性に基づいて様々なアクセス・レベルを設計することにより、ユーザーによるデータ・アクセスを制限します。ユーザー権限または組織内のユーザーのジョブ・タイトルなどの他の方法に焦点を当ててユーザー・アクセスを制限する必要がある場合、仮想プライベート・データベース・ポリシーとともに使用する PL/SQL ファンクションまたはプロシージャを作成できます。詳細は、6-11 ページの「Oracle Virtual Private Database によるデータ・アクセスの制御」を参照してください。

HR.LOCATIONS のスキーマは次のようになります。

```
Name                                      Null?    Type
----------------------------------------- -------- -------------
LOCATION_ID                               NOT NULL NUMBER(4)
STREET_ADDRESS                                     VARCHAR2(40)
POSTAL_CODE                                        VARCHAR2(12)
CITY                                      NOT NULL VARCHAR2(30)
STATE_PROVINCE                                     VARCHAR2(25)
COUNTRY_ID                                         CHAR(2)
```

次のラベルを適用します。

ラベル	権限
CONFIDENTIAL	ミュンヘン、オックスフォード、ローマに読取りアクセス権を付与します。
SENSITIVE	北京、東京、シンガポールに読取りアクセス権を付与します。
PUBLIC	HR.LOCATIONS 内の他のすべての都市に読取りアクセス権を付与します。

このチュートリアルでは、次の手順を実行します。

- 手順 1: Oracle Label Security をインストールし、ユーザー LBACSYS を有効にする
- 手順 2: Oracle Label Security のチュートリアルで使用する 1 つのロールおよび 3 人のユーザーを作成する
- 手順 3: Oracle Label Security の ACCESS_LOCATIONS ポリシーを作成する
- 手順 4: ACCESS_LOCATIONS ポリシーのレベル・コンポーネントを定義する
- 手順 5: ACCESS_LOCATIONS ポリシーのデータ・ラベルを作成する
- 手順 6: ACCESS_LOCATIONS ポリシーのユーザー認可を作成する
- 手順 7: HR.LOCATIONS 表に ACCESS_LOCATIONS ポリシーを適用する
- 手順 8: HR.LOCATIONS データに ACCESS_LOCATIONS ラベルを追加する
- 手順 9: ACCESS_LOCATIONS ポリシーをテストする
- 手順 10: このチュートリアルで使用したコンポーネントを削除する（オプション）

手順 1: Oracle Label Security をインストールし、ユーザー LBACSYS を有効にする

Oracle Label Security は、Oracle Database のデフォルトのインストールではインストールされませんが、Oracle Database で使用可能な製品の一部です。Oracle Universal Installer を使用して既存のデータベースにインストールし、Database Configuration Assistant（DBCA）を使用

して登録できます。Oracle Label Security では独自のユーザー・アカウント LBACSYS が提供され、このアカウントをインストール後に有効にする必要があります。

- Oracle Label Security のインストール
- Oracle Database での Oracle Label Security の登録
- Oracle Label Security のデフォルトのユーザー・アカウント LBACSYS の有効化

Oracle Label Security のインストール

この手順では、既存のデータベースに Oracle Label Security をインストールする方法を説明します。

Oracle Label Security をインストールするには、次のようにします。

1. Oracle Label Security をインストールする予定のデータベース・インスタンスを停止します。

   SQL*Plus に SYS としてログインし、SYSOPER 権限で接続します。SQL プロンプトで、次のコマンドを入力します。

   ```
   SHUTDOWN IMMEDIATE
   ```

2. SQL*Plus を終了します。

   ```
   EXIT
   ```

3. Oracle Database のプロセスを停止します。

   - **UNIX**: $ORACLE_HOME/bin ディレクトリに移動し、次のコマンドを実行してデータベース・コンソールおよびリスナーを停止します。

     ```
     ./emctl stop dbconsole
     ./lsnrctl stop
     ```

   - **Windows**: Windows のサービス・ツールで、Oracle リスナー、コンソールおよびデータベース・サービスの各サービスを右クリックし、メニューから**「停止」**を選択します。これらのサービス名は Oracle から始まり、データベース・インスタンス名が含まれます。たとえば、データベース・インスタンスが orcl である場合、この名前は次のようになります。

     - OracleDBConsoleorcl
     - OracleJobSchedulerORCL
     - OracleOraDB1g-home1TNSListener
     - OracleServiceORCL

4. インストール・メディアから Oracle Universal Installer を実行します。

   - **UNIX**: 次のコマンドを使用します。

     ```
     /mnt/cdrom/runInstaller
     ```

   - **Windows**: インストール・メディア上の setup.exe ファイルをダブルクリックします。

5. 「インストールする製品の選択」ウィンドウで**「Oracle Database 11g」**を選択し、**「次へ」**をクリックします。

6. **「拡張インストール」**、**「次へ」**の順にクリックします。

   「インストール・タイプの選択」ウィンドウが表示されます。

7. **「カスタム」**、**「次へ」**の順にクリックします。

   ホームの詳細の指定画面が表示されます。

8. Oracle Label Security をインストールする Oracle ベース・ディレクトリおよび Oracle ホーム・ディレクトリを選択します。**「次へ」**をクリックします。

   デフォルトでは、新しい Oracle ホームを作成するよう提案されるため、既存の正しい Oracle ホームを選択する必要があります。その後、システムが最低要件を満たしているかどうかが確認されます。次に、「使用可能な製品コンポーネント」ウィンドウが表示されます。

9. **Oracle Label Security** に該当するボックスを選択します。

   このオプションは、Enterprise Edition のオプションの下にあります。**「Oracle Services For Microsoft Transaction Server」**が選択されていますが、不要な場合はこの選択を解除できます。次に、**「次へ」**をクリックします。

   「サマリー」ウィンドウが表示されます。

10. 選択内容を確認し、**「インストール」**をクリックします。

    進行状況ウィンドウが表示されます。インストールが完了すると、「インストールの終了」ウィンドウが表示されます。

11. **「終了」**、**「はい」**の順にクリックし、終了を確認します。

12. Oracle Label Security をインストールしたデータベース・インスタンスおよびサービスを再起動します。

    - **UNIX**: `$ORACLE_HOME/bin` ディレクトリに移動し、次のコマンドを実行してデータベース・コンソールおよびリスナーを起動します。

      ```
      ./emctl start dbconsole
      ./lsnrctl start
      ```

      SQL*Plus を起動し、データベース・インスタンスを再起動します。

      ```
      SQLPLUS "SYS/AS SYSOPER"
      Enter password: password
      Connected to an idle instance
      SQL> STARTUP
      ```

    - **Windows**: Windows のサービス・ツールで、Oracle リスナー、コンソールおよびデータベース・サービスの各サービスを右クリックし、メニューから**「起動」**を選択します。これらのサービス名は Oracle から始まり、データベース・インスタンス名が含まれます。たとえば、データベース・インスタンスが `orcl` である場合、この名前は次のようになります。

      – OracleDBConsoleorcl

      – OracleJobSchedulerORCL（オプションです。このマニュアルのチュートリアルでは、起動の必要はありません）

      – OracleOraDB1g-home1TNSListener

      – OracleServiceORCL（OracleDBConsole を起動すると、このサービスは起動します）

Oracle Database での Oracle Label Security の登録

インストールが完了したら、Oracle Label Security を Oracle Database に登録する必要があります。

Oracle Label Security を Oracle Database に登録するには、次のようにします。

1. Database Configuration Assistant を起動します。

   - **UNIX:** 端末ウィンドウで次のコマンドを入力します。

     ```
     dbca
     ```

     一般的に、`dbca` は `$ORACLE_HOME/bin` ディレクトリにあります。

- **Windows**: **「スタート」**メニューから**「すべてのプログラム」**をクリックします。次に**「Oracle - *ORACLE_HOME*」→「Configuration and Migration Tools」→「Database Configuration Assistant」**の順にクリックします。

  または、次のコマンド・プロンプトで Database Configuration Assistant を起動できます。

  ```
  dbca
  ```

  Windows では一般的に、dbca は *ORACLE_BASE*¥*ORACLE_HOME*¥bin ディレクトリにあります。

2. 「ようこそ」ページで**「次へ」**をクリックします。

   「操作」ページが表示されます。

3. **「データベース・オプションの構成」**を選択して、**「次へ」**をクリックします。

   「データベース」ページが表示されます。

4. リストから、Oracle Label Security をインストールしたデータベースを選択し、**「次へ」**をクリックします。

   「管理オプション」ページが表示されます。

5. **「Database Control で構成済のデータベースを維持」**を選択します。

   「セキュリティ設定」ページが表示されます。

6. 目的のセキュリティ・オプションを選択し、**「次へ」**をクリックします。

   このリリースの拡張セキュリティ設定を利用することをお薦めします。

   「データベース・コンポーネント」ページが表示されます。

7. **「Oracle Label Security」**を選択し、**「次へ」**をクリックします。

   「接続モード」ページが表示されます。

8. このデータベースの作成時の選択内容に応じて**「専用サーバー・モード」**と**「共有サーバー・モード」**のどちらかを選択し、**「終了」**をクリックし、確認プロンプトで**「OK」**をクリックします。

   Oracle Label Security が登録され、データベース・インスタンスが再起動されます。

9. Database Configuration Assistant を終了します。

Oracle Label Security のデフォルトのユーザー・アカウント LBACSYS の有効化

Oracle Label Security のインストール・プロセスにより、Oracle Label Security 機能を管理するデフォルトのユーザー・アカウント LBACSYS が作成されます。管理者は、このユーザーと同じ権限（SA_SYSDBA、SA_COMPONENTS および SA_LABEL_ADMIN PL/SQL パッケージに対する EXECUTE 権限）を持つユーザーを作成できます。デフォルトでは、LBACYS は、パスワードの期限が切れている、ロックされたアカウントとして作成されます。次の手順では、LBACYS をロック解除し、新しいパスワードを作成します。ユーザー LBACSYS は Database Control を使用して Oracle Label Security ポリシーを作成しているため、SELECT ANY DICTIONARY 権限を LBACSYS に付与する必要があります。

LBACSYS をロック解除するには、新しいパスワードを作成し、SELECT ANY DICTIONARY 権限を付与します。

1. SYSTEM ユーザーとして Database Control にログインします。

   「ログイン」ページで SYSTEM と SYSTEM に割り当てられたパスワードを入力します。**「接続モード」**を**「標準」**に設定します。**「ログイン」**を選択してログインします。

2. **「サーバー」**をクリックして、「サーバー」サブページを表示します。

3. 「セキュリティ」で、**「ユーザー」**を選択します。

   「ユーザー」ページが表示されます。

4. ユーザー LBACSYS を選択します。

   LBACSYS を簡単に検索するには、「オブジェクト名」フィールドに **lba** と入力し、**「実行」**をクリックします。

5. LBACSYS が選択された状態で、**「編集」**をクリックします。

   「ユーザーの編集」ページが表示されます。

6. 「ステータス」の横にある**「ロック解除」**を選択します。

7. **「パスワードの入力」**および**「パスワードの確認」**フィールドで、3-9 ページの「パスワードの作成要件」に従ってセキュアなパスワードを入力します。

   セキュリティを考慮して、以前のリリースの Oracle Database で使用していたパスワードと同じパスワードは使用しないでください。

8. **「システム権限」**をクリックして「ユーザーの編集 : LBACSYS」ページを表示します。

9. **「リストを編集」**をクリックします。

   「システム権限の変更」ページが表示されます。

10. 「使用可能なシステム権限」リストから SELECT ANY DICTIONARY を選択し、**「移動」**をクリックして「選択したシステム権限」リストに移動します。次に**「OK」**をクリックします。

11. **「適用」**をクリックします。

手順 2: Oracle Label Security のチュートリアルで使用する 1 つのロールおよび 3 人のユーザーを作成する

ロールと 3 人のユーザーを作成し、これらのユーザーにロールを付与します。

- ロールの作成
- ユーザーの作成

ロールの作成

emp_role ロールは、これから作成する 3 人のユーザーに必要な権限を付与します。

emp_role ロールを作成するには、次のようにします。

1. Database Control に SYSTEM としてログインしていることを確認します。

   SYSTEM としてログインしていない場合、**「ログアウト」**を選択し、次に**「ログイン」**を選択します。「ログイン」ページで SYSTEM とこのアカウントに割り当てられたパスワードを入力します。**「接続モード」**を**「標準」**に設定します。**「ログイン」**を選択してログインします。

   SYSTEM としてログインしている場合、「データベース・インスタンス」リンクをクリックして、ホームページを表示します。

2. **「スキーマ」**をクリックして「スキーマ」サブページを表示します。

3. 「ユーザーおよび権限」セクションで**「ロール」**をクリックします。

   「ロール」ページが表示されます。

4. **「作成」**をクリックします。

   「ロールの作成」ページが表示されます。

5. **「名前」**フィールドで EMP_ROLE と入力し、「認証」は**「なし」**のままにします。

6. **「オブジェクト権限」**サブページを選択します。

7. 「オブジェクト・タイプの選択」リストから**「表」**を選択し、次に**「追加」**をクリックします。

   「表オブジェクト権限の追加」ページが表示されます。

8. 「表オブジェクトの選択」で HR.LOCATIONS と入力し、HR スキーマの LOCATIONS 表を選択します。次に「使用可能な権限」で、SELECT を「選択した権限」リストに移動します。
9. **「OK」**をクリックして「ロールの作成」ページに戻り、**「OK」**をクリックして「ロール」ページに戻ります。

ユーザーの作成

作成する 3 人のユーザーは、役職に基づき、HR.LOCATIONS 表に対して異なるレベルのアクセス権を持ちます。Steven King（sking）は広報部長で、HR.LOCATIONS 表への完全な読取りアクセス権を持ちます。Karen Partners（kpartner）は販売部マネージャでより制限されたアクセス権を持ち、Louise Doran（ldoran）は販売担当者でアクセス権が最も制限されています。

ユーザーを作成するには、次のようにします。

1. Database Control に SYSTEM としてログインしていることを確認します。

   SYSTEM としてログインしていない場合、**「ログアウト」**を選択し、次に**「ログイン」**を選択します。「ログイン」ページで SYSTEM とこのアカウントに割り当てられたパスワードを入力します。**「接続モード」**を**「標準」**に設定します。**「ログイン」**を選択してログインします。

   SYSTEM としてログインしている場合、「データベース・インスタンス」リンクをクリックして、ホームページを表示します。
2. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
3. 「セキュリティ」セクションで**「ユーザー」**をクリックします。

   「ユーザー」ページが表示されます。
4. **「作成」**をクリックします。

   「ユーザーの作成」ページが表示されます。
5. 次の情報を入力します。
   - **名前**: SKING
   - **プロファイル**: デフォルト
   - **認証**: パスワード
   - **「パスワードの入力」**および**「パスワードの確認」**: 3-9 ページの「パスワードの作成要件」に示されている要件を満たすパスワードを入力します。
   - **デフォルト表領域**: USERS
   - **一時表領域**: TEMP
   - **ロール**: **「ロール」**サブページを選択し、「リストを編集」を選択して emp_role ロールを **sking** に付与します。「使用可能なロール」リストから emp_role を選択し、**「移動」**をクリックして「選択したロール」リストに移動します。**「OK」**をクリックします。「ユーザーの作成」ページで、CONNECT ロールと emp_role ロールの両方で**「デフォルト」**ボックスが選択されていることを確認します。
   - **システム権限**: **「システム権限」**サブページを選択し、**「リストを編集」**をクリックして CREATE SESSION 権限を付与します。sking には ADMIN OPTION オプションを付与しないでください。
6. **「OK」**をクリックします。
7. 「ユーザー」ページで SKING を選択し、「アクション」を**「類似作成」**に設定して**「実行」**をクリックします。

   「ユーザーの作成」ページが表示されます。

8. kpartner および ldoran のアカウントを作成します。

   名前とパスワードを作成します。(3-9 ページの「パスワードの作成要件」を参照してください。) ロールやシステム権限を付与する必要はありません。これらのアカウントのロールおよびシステム権限は、sking アカウントで定義され、自動的に作成されます。

この段階で、同じ権限を持つ 3 人のユーザーが作成されました。これらすべてのユーザーには、HR.LOCATIONS 表に対する SELECT 権限があります。

手順 3: Oracle Label Security の ACCESS_LOCATIONS ポリシーを作成する

ここでは、ACCESS_LOCATIONS ポリシーを作成します。

ACCESS_LOCATIONS ポリシーを作成するには、次のようにします。

1. ユーザー LBACSYS として Database Control にログインします。

   「ログアウト」を選択し、次に**「ログイン」**を選択します。「ログイン」ページで、ユーザー LBACSYS としてログインします。**「接続モード」**を**「標準」**に設定します。**「ログイン」**を選択してログインします。

2. **「サーバー」**をクリックして、「サーバー」サブページを表示します。

3. 「セキュリティ」セクションで**「Oracle Label Security」**をクリックします。

   「Label Security ポリシー」ページが表示されます。

4. **「作成」**をクリックします。

5. 「Label Security ポリシーの作成」ページで、次の情報を入力します。

   - **名前** : ACCESS_LOCATIONS
   - **ラベル列** : OLS_COLUMN

     以降で、表にポリシーを適用するときに、このラベル列が表に追加されます。デフォルトでは、ポリシー・ラベル列のデータ型は NUMBER(10) です。

   - **ラベル列の非表示** : このボックスの選択を解除し、ラベル列が非表示にならないようにします (デフォルトでは選択が解除されています)。

     通常、ラベル列は非表示にしますが、開発段階ではチェックできるように表示しておきます。ポリシーの作成が完了し、使用が開始された後、アプリケーションから見えないようにこの列は非表示にします。

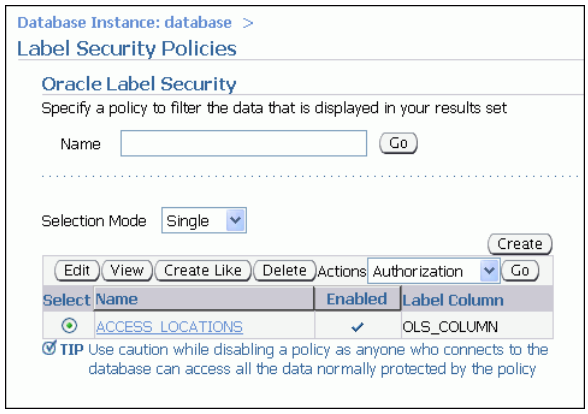
   - **有効** : このボックスを選択し、ポリシーを有効にします (デフォルトでは有効です)。
   - **強制オプション** : **「ポリシー強制の適用」**を選択して、次のオプションを選択します。

     すべての問合せ用 (READ_CONTROL)

     ラベル列の UPDATE 操作にセッションのデフォルト・ラベルを使用 (LABEL_DEFAULT)

6. **「OK」**をクリックします。

   ACCESS_LOCATIONS ポリシーが「Label Security ポリシー」ページに表示されます。



手順 4: ACCESS_LOCATIONS ポリシーのレベル・コンポーネントを定義する

この段階では、ポリシーが作成され、ポリシーの強制オプションが設定されています。次に、ポリシーで使用するラベル・コンポーネントを作成します。

少なくとも、PUBLIC または SENSITIVE など、1 つ以上のレベルを作成し、詳細名、短縮名、機密性レベルを表す数値を定義する必要があります。区分およびグループはオプションです。

レベル数値は、対応するラベルに必要な機密性のレベルを表します。数値は範囲で選択します。この範囲は、セキュリティ・ポリシーでさらにレベルが必要になった場合に拡張できます。たとえば、LOW_SENSITIVITY と HIGH_SENSITIVITY というレベルを追加するには、LOW_SENSITIVITY には 7300、HIGH_SENSITIVITY には 7600 という数値を割り当て、ポリシーにより作成されるセキュリティ・スケールに適合させることができます。通常、番号が大きいほどデータの機密性が高くなります。

コンパートメントは、ラベルが割り当てられたデータの機密性を表す領域を識別し、レベル内のより詳細なレベルを表します。コンパートメントはオプションです。

グループは、データを所有する組織またはデータにアクセスする組織を識別します。グループはデータの配布を制御する際に有用であり、組織的な変更にもタイムリに対応できます。グループはオプションです。

この手順では、レベル・コンポーネントを定義します。レベル・コンポーネントは、ACCESS_LOCATIONS ポリシーで作成する必要がある SENSITIVE、CONFIDENTIAL、PUBLIC ラベルの名前と関係に影響します。

ACCESS_LOCATIONS ポリシーのレベル・コンポーネントを定義するには、次のようにします。

1. 「Label Security ポリシー」ページで **ACCESS_LOCATIONS** ポリシーを選択し、次に**「編集」**を選択します。

   「Label Security ポリシーの編集」ページが表示されます。

2. **「ラベル・コンポーネント」**サブページを選択します。

3. 「レベル」で、**「5 行追加」**をクリックし、次のように詳細名、短縮名および数値タグを入力します（フィールド間を移動するには、[Tab] キーを押します）。

詳細名	短縮名	数値タグ
SENSITIVE	SENS	3000
CONFIDENTIAL	CONF	2000
PUBLIC	PUB	1000

4. **「適用」**をクリックします。

手順 5: ACCESS_LOCATIONS ポリシーのデータ・ラベルを作成する

この手順では、「手順 4: ACCESS_LOCATIONS ポリシーのレベル・コンポーネントを定義する」で作成したポリシーのデータ・ラベルを作成します。データ・ラベルを作成するには、各レベルに数値タグを割り当てる必要があります。以降でポリシーを表に適用したときに、このタグの数値はセキュリティ列に格納されます。タグの数値は、ラベルの機密性とは関係ありません。この数値はポリシーのラベルを識別するためにのみ使用されます。

データ・ラベルを作成するには、次のようにします。

1. **「Label Security ポリシー」**リンクを選択して、「Label Security ポリシー」ページに戻ります。
2. **ACCESS_LOCATIONS** ポリシーを選択します。
3. 「アクション」リストで**「データ・ラベル」**を選択し、次に**「実行」**をクリックします。

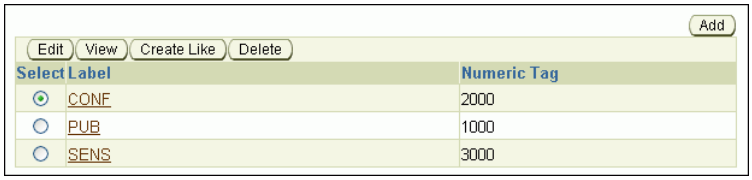
   「データ・ラベル」ページが表示されます。
4. **「追加」**をクリックします。

   「データ・ラベルの作成」ページが表示されます。
5. 次の情報を入力します。
   - **数値タグ**: `1000` と入力します。
   - **レベル**: リストから**「PUB」**を選択します（キーボードを使用してアイテムを選択するには、名前の先頭の文字を入力します。たとえば、`P` と入力して**「PUB」**を選択します）。

6. **「OK」**をクリックします。

   「データ・ラベル」ページにデータ・ラベルが表示されます。
7. もう一度**「追加」**をクリックし、`CONF` レベルのデータ・ラベルを作成します。数値タグは `2000` と入力します。
8. **「OK」**をクリックします。
9. もう一度**「追加」**をクリックし、`SENS` レベルのデータ・ラベルを作成します。数値タグは `3000` と入力します。
10. **「OK」**をクリックします。

    この段階で、「データ・ラベル」ページに `CONF`、`PUB` および `SENS` ラベルが表示されます。



以降で、`HR.LOCATIONS` 表にポリシーを適用したときに、タグの値はセキュリティ列に格納されます。この値は、ラベルの機密性には関係ありません。ポリシーのラベルを識別するために使用されるだけです。

手順 6: ACCESS_LOCATIONS ポリシーのユーザー認可を作成する

次に、ポリシーのユーザー認可を作成します。

ポリシーのユーザー認可を作成するには、次のようにします。

1. **「Label Security ポリシー」**リンクを選択して、「Label Security ポリシー」ページに戻ります。
2. ACCESS_LOCATIONS ポリシーを選択します。
3. 「アクション」リストで**「認可」**を選択し、次に**「実行」**をクリックします。

   「認可」ページが表示されます。
4. **「ユーザーの追加」**をクリックします。

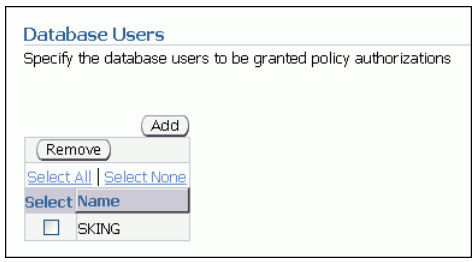
   「ユーザーの追加 : ユーザー」ページが表示されます。
5. 「データベース・ユーザー」で**「追加」**をクリックします。

   「検索と選択 : ユーザー」ページが表示されます。SKING と入力して、**「実行」**をクリックします。

   通常、データベース・ユーザー・アカウントは、たとえば CREATE USER SQL 文を使用してデータベースにすでに作成されています。

   その他のオプションは**「データベース以外のユーザー」**です。アプリケーション・ユーザーの多くは、データベース・ユーザー以外のユーザーとなります。データベース・ユーザー以外のユーザーは、データベース内には存在していません。Oracle Label Security の命名方式に一致し、VARCHAR2(30) の長さのフィールドに適合していれば、どのユーザー名も追加できます。ただし、アプリケーションがデータベースに接続したときに、データベース・ユーザー以外のユーザーに関連するセキュリティ情報は、Oracle Database により自動的には構成されません。この場合、アプリケーションは、Oracle Label Security 関数を呼び出し、データベース・ユーザーではないユーザーのラベル認可を行う必要があります。
6. ユーザー SKING のボックスを選択して、**「選択」**をクリックします。

   「ユーザーの作成」ページにユーザー SKING が表示されます。

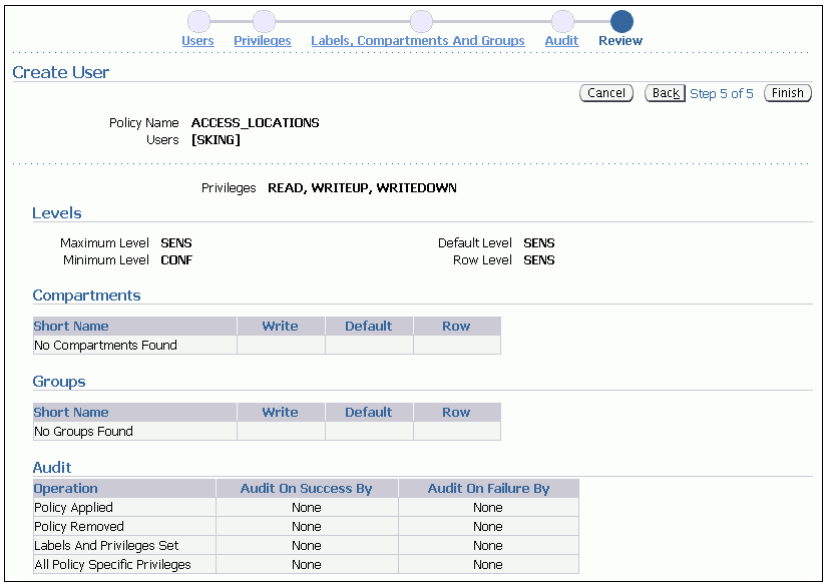


7. **「次へ」**をクリックします。
8. 「権限」ページで、**「次へ」**を選択します。

   ラベル認可を介してポリシーが強制されます。「権限」ページではユーザーによるポリシーのラベル認可をオーバーライド可能にするため、オプションは選択しないでください。
9. ラベル、区分およびグループ・ページで、懐中電灯アイコンを使用して次のフィールドに入力するデータを選択し、ユーザー SKING が HR.LOCATIONS の機密データを読み取れるようにします。
   - **最大レベル** : SENS（SENSITIVE）
   - **最小レベル** : CONF（CONFIDENTIAL）
   - **デフォルト・レベル** : SENS
   - **行レベル** : SENS
10. **「次へ」**をクリックします。

11. 「ユーザーの追加 : 監査」ページの「監査」ペインで、すべての監査の操作が None に設定されていることを確認し、**「次へ」**をクリックします。

    「確認」ページが表示されます。



12. 設定が正しいことを確認し、**「終了」**をクリックします。

    「確認」ページに、選択したすべての認可設定が表示されます。

13. 手順 4 から 12 までを繰り返してユーザー KPARTNER に対して次の認可を作成し、このユーザーが HR.LOCATIONS の機密データおよびパブリック・データを読み取れるようにします。

    - **権限** : 権限は選択しません。
    - **レベル、区分およびグループ** : 4 つすべてのレベルを次のように設定します。
      - **最大レベル** : CONF（CONFIDENTIAL）
      - **最小レベル** : PUB（PUBLIC）
      - **デフォルト・レベル** : CONF
      - **行レベル** : CONF
    - **監査** : すべて「なし」に設定します。

14. ユーザー LDORAN に対して次の認可を作成します。このユーザーは、HR.LOCATIONS のパブリック・データの読取りのみが許可されます。

    - **権限** : 権限は選択しません。
    - **レベル、区分およびグループ** : 4 つすべてのレベルを PUB に設定します。
    - **監査** : すべて「なし」に設定します。

手順 7: HR.LOCATIONS 表に ACCESS_LOCATIONS ポリシーを適用する

次に、HR.LOCATIONS 表にポリシーを適用します。

HR.LOCATIONS 表に ACCESS_LOCATIONS ポリシーを適用するには、次のようにします。

1. **「Label Security ポリシー」**リンクを選択して、「Label Security ポリシー」ページに戻ります。
2. ACCESS_LOCATIONS ポリシーを選択します。

3. 「アクション」リストで**「適用」**を選択し、次に**「実行」**をクリックします。

   「適用」ページが表示されます。

4. **「作成」**をクリックします。

   「表の追加」ページが表示されます。

5. **「表」**フィールドに、HR.LOCATIONS と入力します。

6. **「ポリシー列の非表示」**ボックスが選択されていないことを確認します。

7. **「有効」**ボックスが選択されていることを確認します。

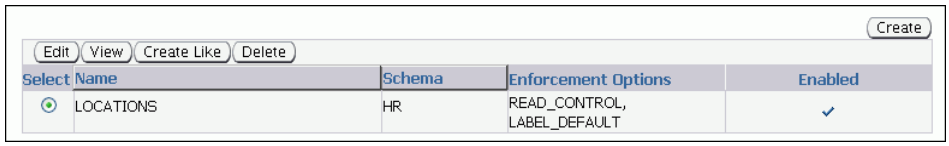
8. 「ポリシー強制オプション」で、**「デフォルトのポリシー強制を使用」**を選択します。

   ACCESS_LOCATIONS のポリシーの強制のデフォルト・オプションは次のとおりです。

   - **すべての問合せ用 (READ_CONTROL)**
   - **ラベル列の更新にセッションのデフォルト・ラベルを使用 (LABEL_DEFAULT)**

9. **「OK」**をクリックします。

   ACCESS_LOCATIONS ポリシーが HR.LOCATIONS 表に適用されます。



手順 8: HR.LOCATIONS データに ACCESS_LOCATIONS ラベルを追加する

ACCESS_LOCATIONS ポリシーを HR.LOCATIONS 表に適用したら、ポリシーのラベルを LOCATIONS の OLS_COLUMN に適用します。ユーザー HR（この表の所有者）がこの操作を行うには、LOCATIONS の非表示の OLS_COLUMN 列にデータ・ラベルを追加する前に、対象の場所への完全なアクセス権を持っている必要があります。

- HR.LOCATIONS 表に対する HR FULL ポリシー権限の付与
- HR.LOCATIONS の OLS_COLUMN 表の更新

HR.LOCATIONS 表に対する HR FULL ポリシー権限の付与

ラベル・セキュリティ管理ユーザー LBACSYS は、必要な権限を HR に付与できます。

ACCESS_LOCATIONS ポリシーへの完全なアクセス権を HR に付与するには、次のようにします。

1. **「Label Security ポリシー」**リンクを選択して、「Label Security ポリシー」ページに戻ります。

2. **ACCESS_LOCATIONS** ポリシーを選択します。

3. 「アクション」リストから**「認可」**を選択し、**「実行」**をクリックします。

   「認可」ページが表示されます。

4. **「ユーザーの追加」**をクリックします。

   「ユーザーの追加」ページが表示されます。

5. 「データベース・ユーザー」で**「追加」**をクリックします。

   「検索と選択」ウィンドウが表示されます。

6. ユーザー HR のボックスを選択して、**「選択」**をクリックします。

   「ユーザーの作成」ページにユーザー HR が表示されます。

7. **「次へ」**をクリックします。

   「権限」手順が表示されます。

8. **「すべてのラベル・セキュリティ・チェックを省略 (FULL)」**権限を選択し、**「次へ」**をクリックします。

   ラベル、区分およびグループ・ページが表示されます。

9. **「次へ」**をクリックします。

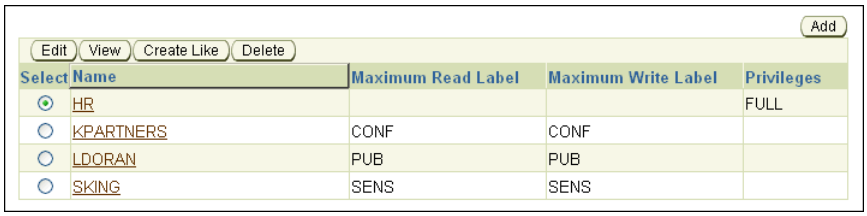
   「監査」手順が表示されます。

10. **「次へ」**をクリックします。

    「確認」手順が表示されます。

11. **「終了」**をクリックします。

    この段階で、HR は他のユーザーとともに「認可」ページにリストされています。



12. Database Control を終了します。

HR.LOCATIONS の OLS_COLUMN 表の更新

この時点で、ユーザー HR は HR.LOCATIONS 表の OLS_COLUMN 列を更新して、CITY 列の都市に基づいて表内の特定の行に割り当てられるデータ・ラベルを追加できます。

HR.LOCATIONS の OLS_COLUMN 表を更新するには、次のようにします。

1. SQL*Plus で、ユーザー HR として接続します。

```
CONNECT HR
Enter password: password
```

   HR としてログインできない場合、このアカウントはロックされているか、期限が切れているため、SYSTEM としてログインしてから、次の文を入力します。*password* は、HR アカウントに適したパスワードに置き換えます。セキュリティを考慮して、以前のリリースの Oracle Database で使用していたパスワードと同じパスワードは再使用しないでください。3-9 ページの「パスワードの作成要件」を参照してください。

```
ALTER USER HR ACCOUNT UNLOCK IDENTIFIED BY password
```

2. 次の UPDATE 文を入力して、北京、東京、シンガポールに SENS ラベルを適用します。

```
UPDATE LOCATIONS
SET ols_column = CHAR_TO_LABEL('ACCESS_LOCATIONS','SENS')
WHERE UPPER(city) IN ('BEIJING', 'TOKYO', 'SINGAPORE');
```

3. 次の UPDATE 文を入力して、ミュンヘン、オックスフォード、ローマに CONF ラベルを適用します。

```
UPDATE LOCATIONS
SET ols_column = CHAR_TO_LABEL('ACCESS_LOCATIONS','CONF')
WHERE UPPER(city) IN ('MUNICH', 'OXFORD', 'ROMA');
```

4. 次の UPDATE 文を入力して、残りの都市に PUB ラベルを適用します。

```
UPDATE LOCATIONS
SET ols_column = CHAR_TO_LABEL('ACCESS_LOCATIONS','PUB')
WHERE ols_column IS NULL;
```

5. 列が更新されたことをチェックするには、次の文を入力します。

```
SELECT LABEL_TO_CHAR (OLS_COLUMN) FROM LOCATIONS;
```

注意： 前述の問合せでラベル列名（OLS_COLUMN）を明示的に使用すると、ラベル列が非表示になっていても表示できます。

ラベル列が非表示であるときに、ラベル列名を明示的に指定しない場合、ラベル列は問合せ結果に表示されません。たとえば、ラベル列が非表示である場合、SELECT * FROM LOCATIONS 問合せを実行しても、ラベル列は表示されません。この機能を使用すると、アプリケーションからラベル列が見えないようにできます。ラベル列が追加される前に設計されたアプリケーションには、ラベル列は認識されず、表示されません。

---

6. ユーザー HR からフルアクセス権を取り消します。

ユーザー HR からフルアクセス権を取り消すには、6-33 ページの「HR.LOCATIONS 表に対する HR FULL ポリシー権限の付与」の手順を参照してください。

手順 9: ACCESS_LOCATIONS ポリシーをテストする

ACCESS_LOCATIONS ポリシーの作成は完了しました。次に、ポリシーをテストします。3 人のユーザーのそれぞれとして SQL*Plus にログインし、HR.LOCATIONS 表で SELECT を実行することで、テストできます。

ACCESS_LOCATIONS ポリシーをテストするには、次のようにします。

1. SQL*Plus でユーザー sking として接続します。

```
CONNECT sking
Enter password: password
```

2. 次のように入力します。

次のコマンドは、読み取りやすいように表の列幅を書式設定します。

```
COL city HEADING City FORMAT a25
COL country_id HEADING Country FORMAT a11
COL Label format a10
```

次に、SELECT 文を次のように入力します。

```
SELECT city, country_id, LABEL_TO_CHAR (OLS_COLUMN)
   AS Label FROM hr.locations ORDER BY ols_column;
```

ユーザー sking は、HR.LOCATIONS 表の 23 行すべてにアクセスできます。アクセスはラベル CONF および SENS が付けられた行に対してのみ認可されていますが、ラベル PUB が付けられた行を読み取ることができます（ただし、書き込むことはできません）。

```
City                      Country     LABEL
------------------------- ----------- ----------
Venice                    IT          PUB
Utrecht                   NL          PUB
Bern                      CH          PUB
Geneva                    CH          PUB
Sao Paulo                 BR          PUB
Stretford                 UK          PUB
Mexico City               MX          PUB
```

```
Hiroshima                 JP          PUB
Southlake                 US          PUB
South San Francisco       US          PUB
South Brunswick           US          PUB
Seattle                   US          PUB
Toronto                   CA          PUB
Whitehorse                CA          PUB
Bombay                    IN          PUB
Sydney                    AU          PUB
London                    UK          PUB
Oxford                    UK          CONF
Munich                    DE          CONF
Roma                      IT          CONF
Singapore                 SG          SENS
Tokyo                     JP          SENS
Beijing                   CN          SENS

23 rows selected.
```

3. ユーザー kpartner と ldoran で、手順 1 と手順 2 を繰り返します。

ユーザー KPARTNER は、ラベル CONF および PUB が付けられた行にアクセスできます。

```
City                      Country     LABEL
------------------------- ----------- ----------
Venice                    IT          PUB
Utrecht                   NL          PUB
Bern                      CH          PUB
Mexico City               MX          PUB
Hiroshima                 JP          PUB
Southlake                 US          PUB
South San Francisco       US          PUB
South Brunswick           US          PUB
Seattle                   US          PUB
Toronto                   CA          PUB
Whitehorse                CA          PUB
Bombay                    IN          PUB
Sydney                    AU          PUB
London                    UK          PUB
Stretford                 UK          PUB
Sao Paulo                 BR          PUB
Geneva                    CH          PUB
Oxford                    UK          CONF
Munich                    DE          CONF
Roma                      IT          CONF

20 rows selected.
```

ユーザー LDORAN は、ラベル PUB が付けられた行にアクセスできます。

```
City                      Country     LABEL
------------------------- ----------- ----------
Venice                    IT          PUB
Hiroshima                 JP          PUB
Southlake                 US          PUB
South San Francisco       US          PUB
South Brunswick           US          PUB
Seattle                   US          PUB
Toronto                   CA          PUB
Whitehorse                CA          PUB
Bombay                    IN          PUB
Sydney                    AU          PUB
London                    UK          PUB
Stretford                 UK          PUB
```

```
Sao Paulo                      BR          PUB
Geneva                         CH          PUB
Bern                           CH          PUB
Utrecht                        NL          PUB
Mexico City                    MX          PUB

17 rows selected.
```

手順 10: このチュートリアルで使用したコンポーネントを削除する（オプション）

このチュートリアルで作成したコンポーネントを削除します。

このチュートリアルで使用したコンポーネントを削除するには、次のようにします。

1. Database Control で、ユーザー SYSTEM として接続します。
2. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
3. 「セキュリティ」セクションで**「ユーザー」**をクリックします。
4. ユーザー kpartner を選択してから、**「削除」**をクリックします。
5. 「確認」ページで**「はい」**をクリックします。
6. ユーザー ldoran と sking で、手順 4 と手順 5 を繰り返します。
7. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
8. **「データベース・インスタンス」**リンクをクリックしてデータベースのホームページに戻ります。
9. 「セキュリティ」セクションで**「ロール」**をクリックします。
10. emp_role ロールを選択し、次に**「編集」**を選択します。
11. 「確認」ダイアログ・ボックスで、**「はい」**をクリックします。
12. Database Control からログアウトし、LABCSYS として再度ログインします。
13. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
14. 「セキュリティ」セクションで**「Oracle Label Security」**をクリックします。
15. 「Label Security ポリシー」ページで、**「名前」**フィールドに ACCESS% と入力して、**「実行」**をクリックします。

16. ACCESS_LOCATIONS が選択されていることを確認し、**「削除」**をクリックします。「確認」ページで、**「はい」**をクリックします。

    ACCESS_LOCATIONS ポリシーを削除すると、HR.LOCATIONS 表から OLS_COLUMN 列も削除されます。

Oracle Database Vault を使用した管理者のアクセスの制御

Oracle Database Vault を使用すると、Oracle Database に対する管理アクセスを制限できます。これによって、内部の脅威に対する保護、コンプライアンス要件の遵守、職務分離の適用など、現在も続く、セキュリティの最も困難な問題に対処できます。

関連項目：『Oracle Database Vault 管理者ガイド』

Oracle Database Vault について

一般的に、Oracle Database 管理者の主な仕事は、データベースのチューニング、アップグレードのインストール、データベースの状態の監視、検出された問題の修復などのタスクを実行することです。Oracle Database のデフォルトのインストールでは、データベース管理者に、ユーザーを作成し、ユーザーのデータにアクセスできる権限が付与されています。セキュリティを考慮すると、このような作業は、必要であると考えられるユーザーだけに制限する必要があります。これを**職務分離**と呼びます。職務を分離することで、データベース管理者は、パフォーマンスのチューニングなど、本来の専門業務に専念することができます。

Oracle Database Vault では Oracle Database への管理者のアクセスが制限されるため、Payment Card Industry（PCI）Data Security Standard（DSS）要件、Sarbanes-Oxley（SOX）Act、European Union（EU）Privacy Directive、Healthcare Insurance Portability and Accountability（HIPAA）Act など、一般的なコンプライアンス要件への遵守が容易になります。これらの規制では、詐称行為、ID の盗用、財政面での不正行為および財政面での不利益をもたらす可能性のある機密情報のアクセス、開示または変更に対する強力な内部制御が必要です。

Oracle Database Vault では、Oracle Database への管理者のアクセスを制限するために次の方法が提供されています。

- **保護対象となるデータベース・スキーマ、オブジェクトおよびロールのグループ分け。**このグループ分けは**レルム**と呼ばれ、レルムのコンポーネントはすべて保護されます。レルムを作成した後に、そのレルムへのアクセスを管理するユーザーを指定します。たとえば、スキーマ内の 1 つの表を対象にしたり、スキーマ全体を対象にしてレルムを作成します。
- **データベース制限をカスタマイズするための PL/SQL 式の作成。ルール**内に式を作成します。1 つのカテゴリにルールが複数ある場合は、ルールを**ルール・セット**にグループ分けします。ルール・セットをレルムに関連付け、レルムに必要と考えられる保護のタイプをさらにカスタマイズすることができます。たとえば、メンテナンス期間（午後 10 ～ 12 時など）におけるデータベースへのアクセスを禁止する場合は、対象となる時間帯だけアクセスを制限するルールを作成できます。
- **ユーザーが使用できる、または使用できない特定の PL/SQL 文の指定。**これは**コマンド・ルール**と呼ばれます。コマンド・ルールを作成して、1 つ以上のデータベース・オブジェクトに影響を与える `SELECT`、`ALTER SYSTEM`、データ定義言語（DDL）およびデータ操作言語（DML）文を保護できます。ルール・セットを関連付けて、コマンド・ルールをさらにカスタマイズすることができます。
- **セッション・ユーザーや IP アドレスなど、Oracle Database Vault が認識および保護できるデータを記録するための属性の定義。**これらの属性は**ファクタ**と呼ばれます。ファクタは、データベースに接続するデータベース・アカウントの認可や、データの可視性および管理性を制限するフィルタ・ロジックの作成などのアクティビティに使用できます。ルール・セットをファクタに関連付けて、ファクタをさらにカスタマイズすることができます。
- **Oracle Database Vault ルールのみによって有効になるセキュア・アプリケーション・ロールの設計。**Oracle Database Vault でセキュア・アプリケーション・ロールを作成した後、これにルール・セットを関連付けます。ルール・セットによって、セキュア・アプリケーション・ロールがいつ、どのように有効または無効になるかが定義されます。

これらのコンポーネントを作成するには、Oracle Database Vault Administrator を使用するか、またはその PL/SQL パッケージを使用します。

チュートリアル : OE スキーマへの管理者のアクセスの制御

OE スキーマには、顧客に許可しているクレジットの上限などの機密情報が格納されている様々な表があります。Order Entry 表には、一般的に、クレジット・カード番号、社会保険番号などの機密情報が格納されています。Payment Card Industry（PCI）Data Security Standards（DSS）によれば、このような種類の情報は、このような情報へのアクセスが仕事上必要な人にのみ制限される必要があります。

このチュートリアルでは、OE スキーマを対象としたレルムを作成し、管理者のアクセスから保護します。ただし、ユーザー SCOTT は OE.CUSTOMERS 表にアクセスする必要があるため、このユーザーがこのデータへのアクセスを続行できるようにする必要があります。

このチュートリアルでは、次の手順を実行します。

- 手順 1: Oracle Database Vault のインストールと登録を行い、そのユーザー・アカウントを有効にする
- 手順 2: OE.CUSTOMERS 表に対する SELECT 権限をユーザー SCOTT に付与する
- 手順 3: ユーザー SYS および SCOTT として OE.CUSTOMERS 表から選択を行う
- 手順 4: OE.CUSTOMERS 表を保護するためにレルムを作成する
- 手順 5: OE Protections レルムをテストする
- 手順 6: このチュートリアルで使用したコンポーネントを削除する（オプション）

手順 1: Oracle Database Vault のインストールと登録を行い、そのユーザー・アカウントを有効にする

この項の内容は次のとおりです。

- Oracle Database Vault のインストール
- Oracle Database Vault の登録
- Database Control へのアクセスの有効化

Oracle Database Vault のインストール

Oracle Database Vault は、Oracle Database のデフォルトのインストールではインストールされませんが、Oracle Database インストール・メディアで利用できる製品に含まれています。インストールは、Oracle Universal Installer を使用し、既存のデータベースに対して行います。

Oracle Database Vault をインストールするには、次のようにします。

1. Oracle Database Vault のインストール先となるデータベース・インスタンスを停止します。

   SQL*Plus に SYS としてログインし、SYSOPER 権限で接続します。SQL プロンプトで、次のコマンドを入力します。

   ```
   SHUTDOWN IMMEDIATE
   ```

2. SQL*Plus を終了します。

   ```
   EXIT
   ```

3. Oracle Database のプロセスを停止します。

   - **UNIX**: $ORACLE_HOME/bin ディレクトリに移動し、次のコマンドを実行してデータベース・コンソールおよびリスナーを停止します。

     ```
     ./emctl stop dbconsole
     ./lsnrctl stop
     ```

   - **Windows**: Windows のサービス・ツールで、Oracle リスナー、コンソールおよびデータベース・サービスの各サービスを右クリックし、メニューから**「停止」**を選択します。これらのサービス名は Oracle から始まり、データベース・インスタンス名が含ま

れます。たとえば、データベース・インスタンスが orcl である場合、この名前は次のようになります。

- OracleDBConsoleorcl
- OracleJobSchedulerORCL
- OracleOraDB1g-home1TNSListener
- OracleServiceORCL

4. インストール・メディアから Oracle Universal Installer を実行します。
   - **UNIX**: 次のコマンドを使用します。

     ```
     /mnt/cdrom/runInstaller
     ```

   - **Windows**: インストール・メディア上の setup.exe ファイルをダブルクリックします。
5. 「インストールする製品の選択」ウィンドウで**「Oracle Database 11g」**を選択し、**「次へ」**をクリックします。
6. **「拡張インストール」**、**「次へ」**の順にクリックします。

   「インストール・タイプの選択」ウィンドウが表示されます。
7. **「カスタム」**、**「次へ」**の順にクリックします。

   ホームの詳細の指定画面が表示されます。
8. Oracle Database Vault をインストールする Oracle ベース・ディレクトリおよび Oracle ホーム・ディレクトリを選択します。**「次へ」**をクリックします。

   デフォルトでは、新しい Oracle ホームを作成するよう提案されるため、既存の正しい Oracle ホームを選択する必要があります。その後、システムが最低要件を満たしているかどうかが確認されます。次に、「使用可能な製品コンポーネント」ウィンドウが表示されます。
9. **Oracle Database Vault オプション**に該当するボックスを選択します。

   このオプションは、Enterprise Edition のオプションの下にあります。Oracle Label Security もインストールする必要があるため、Oracle Universal Installer によって選択されています。**「Oracle Services For Microsoft Transaction Server」**も選択されていますが、不要な場合はこの選択を解除できます。次に、**「次へ」**をクリックします。

   「サマリー」ウィンドウが表示されます。
10. 選択内容を確認し、**「インストール」**をクリックします。

    新しい製品には、Oracle Database Vault J2EE アプリケーション、Oracle Database Vault オプションおよび Oracle Label Security が含まれます。

    「インストール」をクリックした後、進行状況ウィンドウが表示されます。インストールが完了すると、「インストールの終了」ウィンドウが表示されます。
11. **「終了」**、**「はい」**の順にクリックし、終了を確認します。
12. Oracle Database Vault をインストールしたデータベース・インスタンスおよびサービスを再起動します。
    - **UNIX**: $ORACLE_HOME/bin ディレクトリに移動し、次のコマンドを実行してデータベース・コンソールおよびリスナーを起動します。

      ```
      ./emctl start dbconsole
      ./lsnrctl start
      ```

      SQL*Plus を起動し、データベース・インスタンスを再起動します。

      ```
      SQLPLUS "SYS/AS SYSOPER"
      Enter password: password
      Connected to an idle instance
      ```

```
SQL> STARTUP
```

- **Windows**: Windows のサービス・ツールで、Oracle リスナー、コンソールおよびデータベース・サービスの各サービスを右クリックし、メニューから**「起動」**を選択します。これらのサービス名は Oracle から始まり、データベース・インスタンス名が含まれます。たとえば、データベース・インスタンスが `orcl` である場合、この名前は次のようになります。
  - OracleDBConsoleorcl
  - OracleJobSchedulerORCL（オプションです。このマニュアルのチュートリアルでは、起動の必要はありません）
  - OracleOraDB1g-home1TNSListener
  - OracleServiceORCL（OracleDBConsole を起動すると、このサービスは起動します）

Oracle Database Vault の登録

Oracle Database Vault をインストールした後、それをデータベースに登録し、アカウントを作成する必要があります。

Oracle Database Vault を登録するには、次のようにします。

1. Database Configuration Assistant を起動します。
   - **UNIX:** 端末ウィンドウで次のコマンドを入力します。

     ```
     dbca
     ```

     一般的に、`dbca` は `$ORACLE_HOME/bin` ディレクトリにあります。
   - **Windows**:**「スタート」**メニューから**「すべてのプログラム」**をクリックします。次に**「Oracle - *ORACLE_HOME*」→「Configuration and Migration Tools」→「Database Configuration Assistant」**の順にクリックします。

     または、次のコマンド・プロンプトで Database Configuration Assistant を起動できます。

     ```
     dbca
     ```

     Windows では一般的に、`dbca` は *`ORACLE_BASE`*¥*`ORACLE_HOME`*¥`bin` ディレクトリにあります。
2. 「ようこそ」ページで**「次へ」**をクリックします。

   「操作」ページが表示されます。
3. **「データベース・オプションの構成」**を選択して、**「次へ」**をクリックします。

   「データベース」ページが表示されます。
4. リストから、Oracle Database Vault をインストールしたデータベースを選択し、**「次へ」**をクリックします。

   「データベース・コンテンツ」ページが表示されます。
5. **「Oracle Database Vault」を選択し**（インストールされていない場合は**「Oracle Label Security」**も選択し）、**「次へ」**をクリックします。

   Oracle Database Vault がチェックされ、名前がグレーアウトされている場合は、すでに登録されています。

   Oracle Database Vault を選択すると、「Oracle Database Vault 資格証明」ページが表示されます。

6. Database Vault 所有者アカウント（DBVOWNER など）の名前とパスワード、および Database Vault アカウント・マネージャ（DBVACCTMGR など）の名前とパスワードを指定します。

   3-9 ページの「パスワードの作成要件」に示されているパスワードのガイドラインに従って、任意のセキュアなパスワードを入力します。Oracle Database Vault には、追加のパスワード要件があります。これは、不適切なパスワードを作成しようとすると表示されます。

7. **「次へ」**をクリックします。

   「接続モード」ページが表示されます。

8. このデータベースの作成時の選択内容に応じて**「専用サーバー・モード」**と**「共有サーバー・モード」**のどちらかを選択し、**「終了」**をクリックし、確認プロンプトで**「OK」**をクリックします。

   Oracle Database Vault が登録され、データベース・インスタンスが再起動されます。

9. Database Configuration Assistant を終了します。

Database Control へのアクセスの有効化

Database Vault アカウント・マネージャおよび OE アカウントには、Database Control を使用するために SELECT ANY DICTIONARY 権限が必要です。

SELECT ANY DICTIONARY 権限を付与するには、次のようにします。

1. SYS ユーザーとして Database Control にログインします。

   「ログイン」ページで SYS と SYS に割り当てられたパスワードを入力します。**「接続モード」**を **SYSDBA** に設定します。**「ログイン」**を選択してログインします。Database Control の起動方法については、『Oracle Database 2 日でデータベース管理者』を参照してください。

2. **「サーバー」**をクリックして、「サーバー」サブページを表示します。

3. 「セキュリティ」で、**「ユーザー」**を選択します。

   「ユーザー」ページが表示されます。

4. Database Vault アカウント・マネージャのアカウント（DBVACCTMGR）を選択します。

   DBVACCTMGR を簡単に検索するには、**「オブジェクト名」**フィールドに DBV と入力し、**「実行」**をクリックします。

5. DBVACCTMGR が選択された状態で、**「編集」**をクリックします。

   「ユーザーの編集」ページが表示されます。

6. **「システム権限」**をクリックして「ユーザーの編集」ページを表示します。

7. **「リストを編集」**をクリックします。

   「システム権限の変更」ページが表示されます。

8. 「使用可能なシステム権限」リストから SELECT ANY DICTIONARY を選択し、**「移動」**をクリックして「選択したシステム権限」リストに移動します。次に**「OK」**をクリックします。

9. **「適用」**をクリックします。

10. 前述の手順を繰り返し、ユーザー OE にも SELECT ANY DICTIONARY 権限を付与します。

手順 2: OE.CUSTOMERS 表に対する SELECT 権限をユーザー SCOTT に付与する

後でチュートリアルをテストするときに、ユーザー SCOTT は OE.CUSTOMERS 表からの選択を行う必要があります。まず、SCOTT アカウントが有効であることを確認する必要があります。

ユーザー SCOTT を有効にするには、次のようにします。

1. Database Control を起動します。

   Database Control を起動する手順については、『Oracle Database 2 日でデータベース管理者』を参照してください。

2. Oracle Database Vault アカウント・マネージャのアカウントを使用し、**「標準」**として接続します。

   Oracle Database Vault をインストールした後は、管理アカウントを使用してユーザー・アカウントを作成または有効化することはできません。これは、Oracle Database Vault がデフォルトの状態のままでも、管理アカウントに対して職務分離の方針が適用されるためです。この時点から、ユーザー・アカウントを管理するには、Oracle Database Vault アカウント・マネージャのアカウントを使用する必要があります。

   だたし、管理ユーザーには、その業務に必要な権限は付与されたままです。たとえば、システム権限と多数の PL/SQL パッケージを所有するユーザー SYS は、引き続きこれらの権限を他のユーザーに付与できます。

3. **「サーバー」**をクリックして、「サーバー」サブページを表示します。

4. 「セキュリティ」で、**「ユーザー」**を選択します。

   「ユーザー」ページが表示されます。

5. ユーザーのリストから **SCOTT** を選択し、**「編集」**をクリックします。

   「ユーザーの編集」ページが表示されます。

6. 次の設定を入力します。

   - **「パスワードの入力」**および**「パスワードの確認」**: SCOTT アカウントのパスワードのステータスが期限切れである場合は、新しいパスワードを入力します。3-9 ページの「パスワードの作成要件」に示されているパスワードのガイドラインに従って、任意のセキュアなパスワードを入力します。
   - **ステータス**:**「ロック解除」**をクリックします。

7. **「適用」**をクリックします。

8. **「ログアウト」**をクリックします。

ユーザー SCOTT に OE.CUSTOMERS 表に対する SELECT 権限を付与するには、次のようにします。

1. Database Control の「ログイン」ページで、ユーザー OE としてログインします。

   Database Control を起動する手順については、『Oracle Database 2 日でデータベース管理者』を参照してください。

2. **「サーバー」**をクリックして、「サーバー」サブページを表示します。

3. 「セキュリティ」で、**「ユーザー」**を選択します。

   「ユーザー」ページが表示されます。

4. **SCOTT** を選択して、**「編集」**をクリックします。

   「ユーザーの編集」ページが表示されます。

5. 「ユーザーの編集」ページで、**「オブジェクト権限」**サブページを選択します。

   「オブジェクト権限」サブページが表示されます。

6. **「オブジェクト・タイプの選択」**リストから**「表」**を選択し、次に**「追加」**をクリックします。

   「表オブジェクト権限の追加」ページが表示されます。

7. 「表オブジェクトの選択」フィールドで、OE.CUSTOMERS と入力するか、または懐中電灯アイコンを使用してこの表を検索します。

8. 「使用可能な権限」で**「SELECT」**を選択し、**「移動」**をクリックして「選択した権限」に移動します。

9. **「OK」**をクリックします。

   「ユーザーの編集」ページが表示されます。

10. **「適用」**をクリックします。

手順 3: ユーザー SYS および SCOTT として OE.CUSTOMERS 表から選択を行う

この段階では、ユーザー SYS および SCOTT の両者が、OE.CUSTOMERS 表からの選択を行うことができます。これは、SYS は管理権限を所有し、SCOTT はユーザー OE によって付与された明示的な SELECT 権限を所有しているためです。

ユーザー SYS および SCOTT として OE.CUSTOMERS から選択を行うには、次のようにします。

1. SQL*Plus を起動し、SYSDBA 権限を使用してユーザー SYS として接続します。

```
SQLPLUS "SYS/AS SYSDBA"
Enter password: password
Connected.
```

2. 次のように、OE.CUSTOMERS 表から選択を行います。

```
SELECT COUNT(*) FROM OE.CUSTOMERS;
```

   次の出力が表示されます。

```
COUNT(*)
--------
     319
```

3. ユーザー SCOTT として接続し、同じ SELECT 文を実行します。

```
CONNECT SCOTT
Enter password: password
Connected.

SELECT COUNT(*) FROM OE.CUSTOMERS;
```

   次の出力が表示されます。

```
COUNT(*)
--------
     319
```

手順 4: OE.CUSTOMERS 表を保護するためにレルムを作成する

OE.CUSTOMER 表への管理アクセスを制限するには、OE スキーマに対するレルムを作成します。

1. Oracle Database Vault Administrator を起動します。

   ブラウザに、次の URL を入力します。

   https://*host_name*:*port*/dva

host_name は Oracle Database Vault をインストールしたサーバーの名前に、*port* は Oracle Enterprise Manager コンソールの HTTPS ポート番号に置き換えます。ほとんどの場合、サーバーの名前とポート番号は、Database Control で使用しているものと同じです。

Database Vault Administrator を起動できない場合は、これを手動でデプロイする必要があります。詳細は、『Oracle Database Vault 管理者ガイド』を参照してください。

2. 「データベースにログイン」ページで、次の情報を入力します。
   - **ユーザー名**: Oracle Database Vault のインストール時に作成した DV_OWNER アカウントの名前を入力します（DBVOWNER など）。
   - **パスワード**: 入力した名前のユーザーのパスワードを入力します。
   - **ホスト**: Oracle Database Vault をインストールしたコンピュータのホスト名または IP アドレスを入力します（myserver.us.example.com など）。
   - **ポート**: データベースのポート番号を入力します（1521 など）。
   - **SID/ サービス**: データベースの SID（orcl など）またはサービス（myserver.us.example.com など）を入力します。

   データベース・インスタンスの「管理」ページが表示されます。
3. 「Database Vault 機能管理」で、**「レルム」**を選択します。

   「レルム」ページが表示されます。
4. **「作成」**をクリックします。

   「レルムの作成」ページが表示されます。
5. 次の情報を入力します。
   - **名前**: OE Protections
   - **説明**: Realm to protect the OE schema
   - **ステータス**: **「有効」**をクリックします。
   - **監査オプション**: **「失敗時に監査」**を選択します。
6. **「OK」**をクリックします。

   「レルム」ページが表示され、レルムとして OE が示されます。ただし、保護されたオブジェクトまたは認可されたユーザーはまだ存在しません。
7. **OE Protections** レルムを選択し、**「編集」**をクリックします。

   「レルムの編集」ページが表示されます。
8. 「レルム・セキュア・オブジェクト」で、**「作成」**をクリックします。

   「レルム・セキュア・オブジェクトの作成」ページが表示されます。
9. **「オブジェクト所有者」**リストから **OE** を選択します。

   OE は、OE スキーマを所有するアカウントです。OE ユーザーを選択すると、このアカウントで OE スキーマ表を引き続きメンテナンスできます。
10. **「オブジェクト・タイプ」**リストから **TABLE** を選択します。
11. **「オブジェクト名」**フィールドに、OE スキーマ内のすべての表を指定するために % を入力し、**「OK」**をクリックします。

    「レルムの編集」ページが表示されます。
12. **「レルム認可」**で、**「作成」**をクリックします。

    「レルム認可の作成」ページが表示されます。

13. **「権限受領者」**リストから OE を選択し、**「認可タイプ」**を**「所有者」**に設定します。その後で、**「認可ルール・セット」**を **< 未選択 >** に設定します。

    これによって、OE スキーマ内のオブジェクトへのアクセスを管理する OE ユーザーが認可されます。所有者として、OE ユーザーは、レルムで保護されたデータベースのロールの付与または取消し、OE Protections レルムで保護されたオブジェクトのアクセス、操作および作成を実行できます。

    「認可ルール・セット」リストを使用すると、レルムが有効になる時間など、アクセスをさらに制御するルールを選択できます。

14. **「OK」**をクリックして「レルムの編集」ページに戻り、**「OK」**を再びクリックして「レルム」ページに戻ります。

15. **「ログアウト」**をクリックして Oracle Database Vault Administrator を終了します。

手順 5: OE Protections レルムをテストする

OE スキーマを保護するレルムが作成され、テストを実行できるようになりました。データベース・セッションを再び開始する必要はありません。これは、Oracle Database Vault で定義した保護は即時に有効になるためです。

OE Protections レルムをテストするには、次のようにします。

1. SYSDBA 権限を使用してユーザー SYS として SQL*Plus に接続します。

```
CONNECT SYS/AS SYSDBA
Enter password: password
Connected.
```

2. OE.CUSTOMERS 表からの選択を試行します。

```
SELECT COUNT(*) FROM OE.CUSTOMERS;
```

次の出力が表示されます。

```
ERROR at line 1:
ORA-01031: insufficient privileges
```

OE Protections レルムによって、管理ユーザーの OE.CUSTOMERS 表へのアクセスが制限されています。スキーマ全体を保護するように OE Protections レルムを定義したため、管理ユーザーは OE 内の他の表にもアクセスできません。

3. ユーザー SCOTT として接続します。

```
CONNECT SCOTT
Enter password: password
Connected.
```

4. OE.CUSTOMERS 表からの選択を試行します。

```
SELECT COUNT(*) FROM OE.CUSTOMERS;
```

次の出力が表示されます。

```
  COUNT(*)
----------
       319
```

OE Protections レルムはユーザー SCOTT には適用されません。これは、ユーザー OE によって、OE.CUSTOMERS 表に対する SELECT 権限がこのユーザーに明示的に付与されているためです。Oracle Database Vault によって、必要な保護が設定されますが、ユーザーが定義した明示的な権限が上書きされることはありません。SCOTT は、引き続きこの表を問い合せることができます。

5. SQL*Plus を終了します。

```
EXIT
```

手順 6: このチュートリアルで使用したコンポーネントを削除する（オプション）

このチュートリアルの終了後、使用したデータ構造が不要な場合は削除できます。

OE.CUSTOMERS に対する SELECT 権限をユーザー SCOTT から取り消すには、次のようにします。

1. Database Control を起動します。

   Database Control を起動する手順については、『Oracle Database 2 日でデータベース管理者』を参照してください。

2. OE ユーザーとしてログインします。
3. データベースのホームページで、「サーバー」をクリックして「サーバー」サブページを表示します。
4. 「セキュリティ」で、**「ユーザー」**を選択します。

   「ユーザー」ページが表示されます。

5. **SCOTT** を選択して、**「編集」**をクリックします。

   「ユーザーの編集」ページが表示されます。

6. **「オブジェクト権限」**をクリックして「オブジェクト権限」サブページを表示します。
7. OE.CUSTOMERS 表の SELECT オブジェクト権限を選択し、**「削除」**をクリックします。その後で、**「適用」**をクリックします。
8. **「ログアウト」**をクリックします。

SELECT ANY DICTIONARY 権限をユーザー OE から取り消すには、次のようにします。

1. Database Control で**「ログイン」**をクリックします。

   「ログイン」ページが表示されます。

2. ユーザー SYS としてログインし、SYSDBA 権限を使用して接続します。

   Database Control のホームページが表示されます。

3. **「サーバー」**をクリックし、「セキュリティ」リストから**「ユーザー」**を選択します。

   「ユーザー」ページが表示されます。

4. **OE** を選択して、**「編集」**をクリックします。

   「ユーザーの編集」ページが表示されます。

5. **「システム権限」**をクリックしてから**「リストを編集」**をクリックします。

   「システム権限の変更」ページが表示されます。

6. 「選択したシステム権限」リストから **SELECT ANY DICTIONARY** を選択し、**「削除」**をクリックします。その後で、**「OK」**をクリックしてから**「適用」**をクリックします。
7. Database Control を終了します。

OE Protections レルムを削除するには、次のようにします。

1. Oracle Database Vault Administrator を起動します。

   Database Vault Administrator の起動方法については、6-44 ページの「手順 4: OE.CUSTOMERS 表を保護するためにレルムを作成する」の手順 1 を参照してください。

2. Oracle Database Vault のインストール時に作成した DV_OWNER アカウントの名前（DBVOWNER など）を使用してログインします。

   「管理」ページが表示されます。

3. 「Database Vault 機能管理」で、**「レルム」**をクリックします。

   「レルム」ページが表示されます。

4. レルムのリストから **OE Protections** を選択し、**「削除」**をクリックします。その後、「確認」ページで**「はい」**をクリックします。

5. Oracle Database Vault Administrator を終了します。

7

データベース・アクティビティの監査

この章の内容は次のとおりです。

関連項目：

- ユーザーおよびデータベース・アクティビティを監査する他の方法については、『Oracle Database セキュリティ・ガイド』を参照してください。
- 監査の拡張機能を提供する Oracle Audit Vault の詳細は、『Oracle Audit Vault 管理者ガイド』を参照してください。

監査の概要

監査は選択したユーザーのデータベース・アクションの監視と記録です。標準監査を使用して、SQL 文、権限、スキーマ、オブジェクト、ネットワークおよび複数階層アクティビティの監査を行います。標準監査では、初期化パラメータおよび SQL 文 `AUDIT` と `NOAUDIT` を使用して、SQL 文、権限、スキーマ・オブジェクト、およびネットワーク・アクティビティと複数階層アクティビティの監査を行います。

監査が有効かどうかにかかわらず、Oracle Database が常に監査するアクティビティもあります。これらのアクティビティには、管理者権限の接続、データベースの起動、データベースの停止などが含まれます。詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。

監査の別タイプとして、ファイングレイン監査もあります。ファイングレイン監査により、データ・アクセスを、内容に基づき、`value > 1000` などの Boolean 測定を使用して、最も密なレベルで監査できます。ファイングレイン監査では、列へのアクセス、または列内での変更に基づいて、アクティビティを監査できます。Oracle Database にある指定した要素（特定のオブジェクトのコンテンツなど）へのアクセスまたは変更があると監査がトリガーされるようにセキュリティ・ポリシーを作成できます。監査を行う必要がある特定の条件を定義したポリシーを作成できます。たとえば、特定の表の列を監査し、一定期間中のどのタイミングで、誰がアクセスしようとしたかを調べることができます。また、ポリシー違反があった場合にトリガーされるアラートも作成でき、このデータを別の監査ファイルに書き込むことができます。ファイングレイン監査の実行方法は、『Oracle Database セキュリティ・ガイド』を参照してください。

監査の使用目的

監査は、通常次のような目的で使用されます。

- **現行のアクションの今後のアカウンタビリティを有効にします。**

  特定のスキーマ、表、行または影響を受けるコンテンツに対して実行されたアクションも含まれます。

- **アカウンタビリティに基づいて不審なユーザー（もしくは侵入者）による不適切なアクションを阻止します。**

- **不審なアクティビティを調査します。**

  たとえば、ユーザーが表からデータを削除しようとした場合、セキュリティ管理者は、そのデータベースへのすべての接続と、そのデータベースにあるすべての表からの行の削除（成功および失敗）をすべて監査できます。

- **認可されていないユーザーによるアクションを監査人に通知します。**

  たとえば、認可されていないユーザーがデータを変更または削除を実行できるなど、予期した以上の権限を持っている場合に、ユーザー認可を再評価できます。

- **特定のデータベース・アクティビティに関するデータを監視および収集します。**

  たとえば、データベース管理者は、更新された表、実行された論理 I/O 操作の回数、ピーク時に接続していた同時実行ユーザーの数などに関する統計を収集できます。

- **認可またはアクセス制御の実装に関する問題を検出します。**

  たとえば、別の方法で保護されているデータを監査するポリシーを作成します。この場合、データは保護されているため、通常は監査レコードは生成されません。これらのポリシーにより監査レコードが生成された場合は、このデータを保護している別のセキュリティ・コントロールが適切に実装されていないことになります。

- **監査に関するコンプライアンス要件を遵守します。**

  次のような規制には監査に関連する共通の要件があります。

  – 米国企業改革法（Sarbanes-Oxley Act）

- 医療保険の相互運用性と説明責任に関する法律（HIPAA）（Health Insurance Portability and Accountability Act）
- 国際業務を行う銀行の自己資本比率に関する国際統一基準 : 改定版（バーゼル II）（International Convergence of Capital Measurement and Capital Standards: a Revised Framework）
- 日本の個人情報保護法
- 欧州連合のプライバシと電子通信に関する指令（European Union Directive on Privacy and Electronic Communications）

標準監査されたアクティビティが記録される場所

Oracle Database は、監査アクティビティを監査レコードに記録します。監査レコードには、監査された操作、操作を実行したユーザー、操作が実行された日時が記録されます。監査レコードは、**データベース監査証跡**と呼ばれるデータ・ディクショナリ表または**オペレーティング・システム監査証跡**と呼ばれるオペレーティング・システム・ファイルに格納できます。Oracle Database では、不審なアクティビティを追跡するために使用できる一連のデータ・ディクショナリ・ビューも提供されます。これらのビューの詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。

標準監査を使用する場合、Oracle Database では、監査レコードが `DBA_AUDIT_TRAIL`（`sys.aud$` 表）、オペレーティング・システム監査証跡、または標準監査のログ・レコードとファイングレイン監査のログ・レコードを組み合せる `DBA_COMMON_AUDIT_TRAIL` ビューに書き込まれます。

さらに、管理者が実行したアクションは、`syslog` 監査証跡に記録されます。

標準監査による一般的なアクティビティの監査

ここでは、標準監査を使用して SQL 文、権限、スキーマ・オブジェクト、ネットワーク・アクティビティまたは多層アクティビティに対して実行されたアクティビティを監査する方法を説明します。

この項の内容は次のとおりです。

> **関連項目：** 標準監査証跡の管理の詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。

標準監査について

標準監査では、SQL 文、権限、スキーマ・オブジェクトや、ネットワーク・アクティビティまたは多層アクティビティの監査を有効にできます。必要に応じて、特定のスキーマ表に対して監査を実行できます。このタイプの監査を実行するには、Database Control を使用します。

標準監査レコードは、DBA_AUDIT_TRAIL（sys.aud$ 表）、オペレーティング・システム監査証跡、または標準監査のログ・レコードとファイングレイン監査のログ・レコードを組み合せる DBA_COMMON_AUDIT_TRAIL ビューのいずれかに書き込むことができます。

標準監査証跡の有効化または無効化

この項で説明している標準監査を実行する前に、標準監査を有効にする必要があります。標準監査を有効にするときに、データベース監査証跡に監査証跡を作成するか、オペレーティング・システム・ファイルに監査アクティビティを書き込むことができます。オペレーティング・システム・ファイルに書き込む場合は、テキスト形式または XML 形式で監査レコードを作成します。

標準監査証跡を有効または無効にするには、次のようにします。

1. Database Control を起動します。
2. SYS としてログインし、SYSDBA 権限で接続します。
   - **ユーザー名** : SYS
   - **パスワード** : パスワードを入力します。
   - **接続モード** : SYSDBA
3. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
4. 「データベース構成」セクションで**「初期化パラメータ」**をクリックします。

   「初期化パラメータ」ページが表示されます。
5. **「SPFile」**をクリックして「SPFile」サブページを表示します。

   インストールの**「SPFile」**タブが表示されない場合は、サーバー・パラメータ・ファイルを使用して Oracle Database をインストールしなかったということです。次の手順に進みます。
6. **「名前」**フィールドに audit_trail を入力して AUDIT_TRAIL パラメータを検索し、**「実行」**をクリックします。

   AUDIT_ のように、パラメータの最初の数文字を入力できます。または、パラメータのリストをスクロールして、AUDIT_TRAIL パラメータを検索できます。
7. **「値」**フィールドで、次のいずれかの値を選択します。
   - DB: データベース監査を有効にし、すべての監査レコードをデータベース監査証跡（SYS.AUD$）に記録します。ただし、常にオペレーティング・システム監査証跡に書き込まれるレコードは除きます。（この値は、データベースの作成に Database Configuration Assistant を使用した場合のデフォルトです。それ以外の場合のデフォルトは、NONE です。）
   - OS: データベース監査を有効にして、すべての監査レコードをオペレーティング・システム・ファイルに書き込みます。非常に安全なデータベース構成を使用している場合、DoS（サービス拒否）攻撃の可能性を低減できることから、この設定を使用することをお薦めします。また、この設定では、監査証跡の保護も容易になります。監査を行うユーザーがデータベース管理者とは異なる場合は、operating system 設定を使用する必要があります。データベースに格納されたすべての監査情報は、データベース管理者により参照および変更が可能です。

     オペレーティング・システム監査レコード・ファイルの場所を指定するには、AUDIT_FILE_DEST 初期パラメータを設定します。デフォルトのディレクトリは $ORACLE_HOME/rdbms/audit です。

- NONE: 標準監査を無効にします。（この値は、データベースの作成に Database Configuration Assistant 以外の方法を使用した場合のデフォルトです。Database Configuration Assistant を使用した場合のデフォルトは、DB です。）
- DB, EXTENDED: AUDIT_TRAIL=DB 設定のすべてのアクションを実行し、可能な場合は、SYS.AUD$ 表の SQL バインドおよび SQL テキストの CLOB 型の列にデータを移入します（これら 2 つの列は、このパラメータが指定されたときにのみデータが移入されます）。
- XML: オペレーティング・システム監査レコード・ファイルに XML 形式で書き込みます。AuditRecord ノードの、Sql_Text と Sql_Bind 以外のすべての要素をオペレーティング・システム XML 監査ファイルに書き込みます。
- EXTENDED: XML のすべてのアクションを実行し、可能な場合は SYS.AUD$ 表の SQL バインドおよび SQL テキストの CLOB 型の列にデータを移入する XML, EXTENDED を指定します（これらの列は、このパラメータが指定されたときにのみデータが移入されます）。

8. **「適用」**をクリックします。
9. Oracle Database インスタンスを再起動します。
   a. **「データベース・インスタンス」**リンクをクリックします。
   b. **「ホーム」**をクリックして Database Control のホームページを表示します。
   c. 「一般」で**「停止」**をクリックします。
   d. 資格証明の起動 / 停止ページでは、資格証明を入力します。

      詳細は、『Oracle Database 2 日でデータベース管理者』を参照してください。
   e. 完全に停止した後に、**「起動」**をクリックします。

次の点に注意してください。

- オブジェクトの監査に関する変更をした場合は、データベースを再起動する必要はありません。すべての監査をオンまたはオフにするなど、全体に関わる変更を行った場合にのみ、データベースを再起動する必要があります。
- ファイングレイン監査または SYS 監査を有効にする場合、AUDIT_TRAIL を設定する必要はありません（SYS 監査ではシステム管理者のアクティビティが監視されます。詳細は『Oracle Database セキュリティ・ガイド』を参照してください）。ファイングレイン監査の場合は、必要に応じてファイングレイン監査ポリシーを追加および削除し、監視する特定の操作またはオブジェクトに適用します。AUDIT_SYS_OPERATIONS パラメータを使用すると、SYS 監査を有効または無効にできます。

セキュリティ関連の SQL 文および権限に対するデフォルト監査の使用

ここでは、Oracle 推奨の監査パラメータを有効にする方法を説明します。内容は次のとおりです。

デフォルト監査について

新しいデータベースを作成した場合や、既存のデータベースを変更した場合、Database Configuration Assistant（DBCA）の「セキュリティ設定」ウィンドウを使用して、デフォルトのセキュリティ設定を有効または無効にできます。ここでは、DBCA の起動方法およびデフォルトのセキュリティ設定を有効にする方法を説明しています。これらの設定を有効にすると、Oracle Database はセキュリティに関連するいくつかの SQL 文と権限を監査します。また、AUDIT_TRAIL 初期化パラメータが DB に設定されます。別の監査オプション（オペレーティング・システム・ファイルに監査証跡レコードを記述する場合は OS など）に設定することもできます。この場合も、Oracle Database は、デフォルトで監査対象となっている権限を監査します。AUDIT_TRAIL パラメータを NONE に設定して監査を無効にすると、監査は行われません。

Oracle Database は、AUDIT ROLE SQL 文をデフォルトで監査します。デフォルトで監査される権限は、次のとおりです。

```
ALTER ANY PROCEDURE     CREATE ANY LIBRARY        DROP ANY TABLE
ALTER ANY TABLE         CREATE ANY PROCEDURE      DROP PROFILE
ALTER DATABASE          CREATE ANY TABLE          DROP USER
ALTER PROFILE           CREATE EXTERNAL JOB       EXEMPT ACCESS POLICY
ALTER SYSTEM            CREATE PUBLIC DB LINK     GRANT ANY OBJECT PRIVILEGE
ALTER USER              CREATE SESSION            GRANT ANY PRIVILEGE
AUDIT SYSTEM            CREATE USER               GRANT ANY ROLE
CREATE ANY JOB          DROP ANY PROCEDURE
```

また、Oracle Database は、BY ACCESS 句を持つすべての権限と文を監査します。

これらの文および権限の監査がアプリケーションに悪影響を与える可能性がある場合は、Database Configuration Assistant（DBCA）を使用して、この監査を無効にできます。監査を使用するようにアプリケーションを変更したら、これらの文および権限のデフォルト監査を再度有効にできます。

デフォルトで監査を有効にすることをお薦めします。監査は、米国企業改革法（Sarbanes-Oxley Act）で定義されているコンプライアンス要件を満たし、内部からのアクセスを確実に制御できる有効な方法です。監査を実行することでビジネス活動を監視でき、企業のポリシーに反するアクティビティを発見できます。この結果、データベースおよびアプリケーション・ソフトウェアへのアクセスが厳しく制御され、定期的にパッチが確実に適用でき、その場かぎりの変更を防止できます。デフォルトで監査を有効にすると、監査および個人のコンプライアンスに関する監査レコードを生成できます。ただし、監査はデータベースのパフォーマンスに影響する可能性があります。

> **関連項目：** この項で説明している SQL 文および AUDIT_TRAIL 初期化パラメータの詳細は、『Oracle Database SQL 言語リファレンス』を参照してください。

デフォルト監査の有効化

ここでは、Database Configuration Assistant を使用してデフォルト監査を有効にする方法を説明します。

Database Configuration Assistant を使用してデフォルトのプロファイル・セキュリティ設定を有効にするには、次のようにします。

1. Database Configuration Assistant を起動します。
   - **UNIX:** 端末ウィンドウで次のコマンドを入力します。

     ```
     dbca
     ```

     一般的に、dbca は $ORACLE_HOME/bin ディレクトリにあります。
   - **Windows**: **「スタート」**メニューから**「すべてのプログラム」**をクリックします。次に**「Oracle - *ORACLE_HOME*」→「Configuration and Migration Tools」→「Database Configuration Assistant」**の順にクリックします。

     または、次のコマンド・プロンプトで Database Configuration Assistant を起動できます。

     ```
     dbca
     ```

     Windows では一般的に、dbca は *ORACLE_BASE*¥*ORACLE_HOME*¥bin ディレクトリにあります。
2. 「ようこそ」ウィンドウで**「次へ」**をクリックします。

   「操作」ウィンドウが表示されます。

3. リストから**「データベース・オプションの構成」**を選択して、**「次へ」**をクリックします。

   「データベース」ウィンドウが表示されます。

4. リストから、Oracle Label Security をインストールしたデータベースを選択し、**「次へ」**をクリックします。

   「管理オプション」ウィンドウが表示されます。

5. **「Database Control で構成済のデータベースを維持」**を選択します。

   「セキュリティ設定」ページが表示されます。

6. 目的のセキュリティ・オプションを選択し、**「次へ」**をクリックします。

   このリリースの拡張セキュリティ設定を利用することをお薦めします。

   「データベース・コンポーネント」ページが表示されます。

7. **「次へ」**をクリックします。

   「接続モード」ページが表示されます。

8. このデータベースの作成時の選択内容に応じて**「専用サーバー・モード」**と**「共有サーバー・モード」**のどちらかを選択し、**「終了」**をクリックし、確認プロンプトで**「OK」**をクリックします。

個々の SQL 文の監査

監査できる SQL 文は、次のカテゴリに含まれます。

- **DDL 文。**たとえば、表（AUDIT TABLE）の監査を有効にすると、すべての CREATE および DROP TABLE 文が監査されます。

  DML 文。たとえば、SELECT TABLE の監査を有効にすると、表またはビューにかかわらず、すべての SELECT ... FROM TABLE/VIEW 文が監査されます。

文の監査の対象範囲は変更できます。たとえば、すべてのデータベース・ユーザーのアクティビティを監査したり、ユーザーの選択リストのみを監査できます。

> **関連項目：** SQL 文の監査の詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。

個々の権限の監査

権限の監査では、SELECT ANY TABLE など、システム権限を使用する文を監査します。すべてのシステム権限の使用を監査できます。権限の監査では文の監査と同様に、すべてのデータベース・ユーザーのアクティビティを監査することも、指定したリストのアクティビティのみを監査することもできます。SQL 文の監査と同様に、AUDIT 文および NOAUDIT 文を使用することで、権限の監査を有効または無効にできます。また、監査を有効にするには、AUDIT SYSTEM システム権限が必要です。

権限の監査オプションは、対応するシステム権限に一致します。たとえば、DELETE ANY TABLE 権限の使用を監査するオプションは、DELETE ANY TABLE です。次に例を示します。

```
AUDIT DELETE ANY TABLE BY ACCESS WHENEVER NOT SUCCESSFUL;
```

DELETE ANY TABLE 権限の使用の成功および失敗をすべて監査するには、次の文を入力します。

```
AUDIT DELETE ANY TABLE;
```

すべてのデータベース・ユーザーおよび監査対象の個々の文による、すべての表での SELECT、INSERT、DELETE 文の失敗、および EXECUTE PROCEDURE システム権限の使用の失敗をすべて監査するには、次の文を実行します。

```
AUDIT SELECT TABLE, INSERT TABLE, DELETE TABLE, EXECUTE PROCEDURE BY ACCESS WHENEVER
NOT SUCCESSFUL;
```

関連項目： 権限の監査の詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。

多層環境での SQL 文および権限の監査でのプロキシの使用

Database Control の「監査文の追加」ページまたは「監査権限の追加」ページでプロキシを指定すると、多層環境のクライアントのアクティビティを監査できます。多層環境では、Oracle Database はすべての層でクライアントのアイデンティティを保持します。これにより、クライアントのかわりに、中間層アプリケーションにより実行されたアクションを監査できます。

中間層でも、データベース・セッションでユーザーのクライアント ID を設定でき、中間層アプリケーションからユーザー・アクションの監査を有効にできます。ユーザーのクライアント ID は、監査証跡に表示されます。

SQL AUDIT 文を使用して多層環境のクライアントのアクティビティを監査できます。そのためには、AUDIT 文で BY PROXY 句を使用します。

たとえば、クライアント jackson のかわりにプロキシ・アプリケーション・サーバー appserve によって実行された SELECT TABLE 文を監査するには、次のようにします。

```
AUDIT SELECT TABLE BY jackson ON BEHALF OF appserve;
```

ユーザー jackson は、次のように appserve プロキシ・ユーザーを使用して接続できます。

```
CONNECT appserve[jackson]
Enter password: password
```

関連項目： 多層環境での監査の詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。

個々のスキーマ・オブジェクトの監査

スキーマ・オブジェクトの監査では、特定の表の SELECT 文または DELETE 文など、スキーマ・オブジェクト権限により許可されたすべての SELECT 文および DML 文が監査されます。これらの権限を制御する GRANT 文および REVOKE 文も監査されます。

関連項目： スキーマ・オブジェクトの監査の詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。

ネットワーク・アクティビティの監査

AUDIT 文を使用して、ネットワーク・プロトコルの予期しないエラーやネットワーク層で発生した内部エラーを監査できます。ネットワーク監査の対象とならないエラーのタイプは、接続の問題ではなく、複数の原因で発生した可能性があります。考えられる原因として、データベース・エンジニアが単にテスト目的で内部イベントを設定した、などがあげられます。他にも、ネットワークが暗号化の作成または処理に必要な情報を見つけられないなど、暗号化の構成設定の競合などが原因として考えられます。

ネットワークの監査を有効にするには、次のようにします。

1. SQL*Plus を起動し、SYSTEM などの管理者権限で、またはセキュリティ管理者としてログオンします。次に例を示します。

   ```
   SQLPLUS SYSTEM
   Enter password: password
   ```

SQL*Plus が起動し、デフォルトのデータベースに接続してから、プロンプトが表示されます。

SQL*Plus の起動の詳細は、『Oracle Database 2 日でデータベース管理者』を参照してください。

2. 次の文を入力します。

```
AUDIT NETWORK;
```

ネットワークの監査を無効にするには、次の文を入力します。

```
NOAUDIT NETWORK;
```

3. SQL*Plus を終了します。

```
EXIT
```

関連項目： ネットワーク・アクティビティの監査の詳細は、『Oracle Database セキュリティ・ガイド』を参照してください。

チュートリアル : 標準監査証跡の作成

OE.CUSTOMERS 表の SELECT 文を監査する場合を想定します。このチュートリアルでは、標準監査を有効にし、SELECT SQL 文を有効にし、OE.CUSTOMERS 表で SELECT SQL 文を実行してから、その監査ファイルをチェックします。

このチュートリアルでは、次の手順を実行します。

- 手順 1: ログインして標準監査を有効にする
- 手順 2: OE.CUSTOMERS 表の SELECT 文に対する監査を有効にする
- 手順 3: 監査設定をテストする
- 手順 4: このチュートリアルで使用したコンポーネントを削除する（オプション）
- 手順 5: SEC_ADMIN セキュリティ管理者アカウントを削除する

手順 1: ログインして標準監査を有効にする

最初に、ログインして必要ならば標準監査を有効にします。

標準監査を有効にするには、次のようにします。

1. Database Control を起動します。
2. SYS としてログインし、SYSDBA 権限で接続します。
   - **ユーザー名** : SYS
   - **パスワード** : パスワードを入力します。
   - **接続モード** : SYSDBA
3. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
4. 「データベース構成」セクションで**「初期化パラメータ」**をクリックします。

   「初期化パラメータ」ページが表示されます。
5. **「SPFile」**をクリックして「SPFile」サブページを表示します。

   インストールの**「SPFile」**タブが表示されない場合は、サーバー・パラメータ・ファイルを使用して Oracle Database をインストールしなかったということです。次の手順に進みます。

6. **「名前」**フィールドに AUDIT_TRAIL を入力して AUDIT_TRAIL パラメータを検索し、**「実行」**をクリックします。

   AUDIT のように、パラメータの最初の数文字を入力できます。または、パラメータのリストをスクロールして、AUDIT_TRAIL パラメータを検索できます。

7. **「値」**フィールドで、「DB」（データベース）オプションを選択します。

   DB オプションでは、データベース監査を有効にし、すべての監査レコードをデータベース監査証跡（SYS.AUD$）に記録します。ただし、常にオペレーティング・システム監査証跡に書き込まれるレコードは除きます。

8. **「適用」**をクリックします。

9. Oracle Database インスタンスを再起動します。

   a. **「データベース・インスタンス」**リンクをクリックします。

   b. **「ホーム」**をクリックして Database Control のホームページを表示します。

   c. 「一般」で**「停止」**をクリックします。

   d. 資格証明の起動 / 停止ページでは、資格証明を入力します。

      詳細は、『Oracle Database 2 日でデータベース管理者』を参照してください。

   e. 完全に停止した後に、**「起動」**をクリックします。

手順 2: OE.CUSTOMERS 表の SELECT 文に対する監査を有効にする

次に、OE.CUSTOMERS 表の SELECT 文に対する監査を有効にします。

OE.CUSTOMERS 表の SELECT 文の監査を有効にするには、次のようにします。

1. サンプル・ユーザーの sec_admin が存在することを確認します。

   SYSTEM としてログオンし、Database Control のホームページから、**「サーバー」**をクリックすると、「サーバー」サブページが表示されます。「セキュリティ」の下の**「ユーザー」**を選択し、アカウントのリストで sec_admin をチェックします。sec_admin セキュリティ管理者アカウントを作成する方法は、4-4 ページの「手順 1: セキュリティ管理者アカウントを作成する」を参照してください。

2. OE.CUSTOMERS 表での sec_admin SELECT 権限を付与します。

3. ユーザー sec_admin として Database Control にログインします。

4. **「サーバー」**をクリックして、「サーバー」サブページを表示します。

5. 「セキュリティ」セクションで**「ユーザー」**をクリックします。

   監査設定ページが表示されます。

6. **「監査オブジェクト」**サブページを選択します。

7. **「追加」**をクリックします。

   「監査オブジェクトの追加」ページが表示されます。

8. 次の情報を入力します。

   - **オブジェクト・タイプ**:「表」を選択します。
   - **表**: OE.CUSTOMERS と入力します。
   - **監査可能な文**: SELECT を選択し、**「移動」**をクリックして「選択した文」リストに移動します。

9. **「OK」**をクリックします。

10. データベース・インスタンスを停止して、再起動します。

    a. Database Control のページの右上の**「ログアウト」**を選択します。

b. **「ログイン」**をクリックします。

c. 「ログイン」ページで、次の情報を入力します。

ユーザー名 : SYS

パスワード : システム管理者のパスワード

接続モード : SYSDBA

SYSDBA システム権限を使用して、データベースを停止し、再起動します。

d. 「一般」で**「停止」**をクリックします。

e. 資格証明の起動 / 停止ページでは、資格証明を入力します。

詳細は、『Oracle Database 2 日でデータベース管理者』を参照してください。

f. 完全に停止した後に、**「起動」**をクリックします。

g. Database Control を終了します。

手順 3: 監査設定をテストする

この段階では、監査が有効で、OE.CUSTOMERS 表で実行されたすべての SELECT 文が DBA_AUDIT_TRAIL ビューに書き込まれます。次に、監査設定をテストします。

監査設定をテストするには、次のようにします。

1. SQL*Plus を起動し、ユーザー sec_admin として接続します。

```
SQLPLUS sec_admin
Enter password: password
```

2. 次の SELECT 文を入力して監査証跡のアラートを作成します。

```
SELECT COUNT(*) FROM oe.customers;
```

3. 次の文を入力して DBA_AUDIT_TRAIL ビューを表示します。

```
SELECT USERNAME, TIMESTAMP FROM DBA_AUDIT_TRAIL;
```

次のような出力が表示されます。

```
USERNAME          TIMESTAMP
--------------------------
SEC_ADMIN         07-MAY-08
```

4. SQL*Plus を終了します。

```
EXIT
```

手順 4: このチュートリアルで使用したコンポーネントを削除する（オプション）

オプションで、以前に作成した監査設定を削除します。

Database Control で監査設定を削除するには、次のようにします。

1. 管理者権限を使用して、Database Control にログインします。
2. Database Control のホームページに移動します。
3. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
4. 「セキュリティ」セクションで**「ユーザー」**をクリックします。

監査設定ページが表示されます。

5. **「監査オブジェクト」**サブページを選択します。

6. 「スキーマ」に OE と入力します。
7. 「オブジェクト名」に CUSTOMERS と入力します。
8. **「検索」**をクリックします。
9. OE.CUSTOMERS スキーマの横のボックスを選択し、**「削除」**をクリックします。

   「確認」ダイアログ・ボックスが表示されます。
10. **「はい」**を選択します。
11. Database Control を終了します。

AUDIT_TRAIL を元の値に設定するには、次のようにします。

- 7-9 ページの「手順 1: ログインして標準監査を有効にする」の手順に従って SQL*Plus にログインし、AUDIT_TRAIL パラメータを元の値に設定します。次に、データベースを停止してから再起動します。

手順 5: SEC_ADMIN セキュリティ管理者アカウントを削除する

この例は、このガイドの最後の例です。sec_admin 管理者アカウントが不要になった場合は、このアカウントを削除する必要があります。

sec_admin セキュリティ管理者アカウントを削除するには、次のようにします。

1. 管理者権限を使用して、Database Control にログインします。
2. Database Control のホームページに移動します。
3. **「サーバー」**をクリックして、「サーバー」サブページを表示します。
4. 「セキュリティ」セクションで**「ユーザー」**をクリックします。

   「ユーザー」ページが表示されます。
5. **「名前」**フィールドに sec_admin を入力します。
6. **「検索」**をクリックします。
7. sec_admin ユーザー・アカウントの横のボックスを選択し、**「削除」**をクリックします。

   「確認」ダイアログ・ボックスが表示されます。
8. **「はい」**を選択します。
9. Database Control を終了します。

監査のガイドライン

この項の内容は次のとおりです。

- SQL 文および権限のデフォルト監査の使用のガイドライン
- 監査済情報の管理のガイドライン
- 通常のデータベース・アクティビティの監査のガイドライン
- 疑わしいデータベース・アクティビティの監査のガイドライン

SQL 文および権限のデフォルト監査の使用のガイドライン

新しくデータベースを作成すると、選択した一連の SQL 文および権限の監査を有効にすることができます。デフォルト監査を有効にすることを、強くお薦めします。監査は、米国企業改革法（Sarbanes-Oxley Act）で定義されているコンプライアンス要件を満たし、内部からのアクセスを確実に制御できる有効な方法です。デフォルト監査の詳細は、7-5 ページの「セキュリティ関連の SQL 文および権限に対するデフォルト監査の使用」を参照してください。

監査済情報の管理のガイドライン

監査はデータベース・パフォーマンスにあまり影響しませんが、監査するイベントの数はできるだけ制限する必要があります。この制限によって、監査対象の文を実行したときにパフォーマンスの影響が最小限に抑えられ、監査証跡のサイズが最小限になるため、分析と理解が容易になります。

監査方針を立てる際は、次のガイドラインに従います。

1. **監査の目的を評価する**

   監査の目的を理解すると、適切な監査方針を立てることができ、不要な監査を行わずにすみます。

   たとえば、不審なデータベース・アクティビティの調査のために監査を行うと仮定します。この情報のみでは、十分に明確であるとはいえません。どのデータベース・アクティビティが疑わしい、または注意を要するといった具体的な情報が必要です。そのために、たとえば、データベース内の表から許可なくデータが削除されていないかを監査するというように、監査目的を絞り込みます。このような目的を設定すれば、監査の対象となるアクションの種類や、疑わしいアクティビティによって影響を受けるオブジェクトの種類を限定できます。

2. **監査について十分理解する**

   目標とする情報の取得に必要な最小限の文、ユーザーまたはオブジェクトを監査します。これによって、不要な監査情報のために重要な情報の識別が困難になることや、SYSTEM 表領域内の貴重な領域が無駄に消費されることがなくなります。収集が必要なセキュリティ情報の量と、その情報を格納して処理する能力とのバランスを保つ必要があります。

   たとえば、データベース・アクティビティに関する情報を収集するために監査する場合は、追跡するアクティビティの種類を正確に判断した上で、必要な情報を収集するために必要な期間内で、目的のアクティビティのみを監査します。別の例として、各セッションの論理 I/O 情報のみを収集する場合は、オブジェクトを監査しないでください。

通常のデータベース・アクティビティの監査のガイドライン

監査目的が、特定のデータベース・アクティビティに関する履歴情報を収集することである場合は、次のガイドラインに従ってください。

1. **関連のあるアクションのみを監査する**

   不要な監査情報によって重要な情報の識別が困難になることを防ぎ、監査証跡管理の量を削減するために、対象となるデータベース・アクティビティのみ監査します。ファイングレイン監査を使用して特定のアクションを監査できます。『Oracle Database セキュリティ・ガイド』では、ファイングレイン監査が詳細に説明されています。

2. **監査レコードをアーカイブし、監査証跡を削除する**

   必要な情報を収集した後は、目的の監査レコードをアーカイブし、この情報の監査証跡を削除します。

   監査レコードをアーカイブするために、たとえば標準監査証跡では `INSERT INTO table SELECT ... FROM SYS.AUD$ ...` を使用して、通常のデータベース表に関連レコードをコピーできます（ファイングレイン監査レコードは、SYS.FGA_LOG$ 表にあります）。または、監査証跡表をオペレーティング・システム・ファイルにエクスポートできます。『Oracle Database ユーティリティ』では、Oracle Data Pump を使用して表をエクスポートする方法が説明されています。

   監査レコードをパージするには、標準監査レコードを SYS.AUD$ 表から削除し、ファイングレイン監査レコードを SYS.FGA_LOG$ 表から削除します。たとえば、すべての監査レコードを標準監査証跡から削除するには、次の文を入力します。

   ```
   DELETE FROM SYS.AUD$;
   ```

また、emp 表の監査の結果として生成された標準監査証跡からすべての監査レコードを削除するには、次の文を入力します。

```
DELETE FROM SYS.AUD$
     WHERE obj$name='EMP';
```

3. **企業のプライバシ要件に留意する**

   プライバシに関する法規によって、追加のビジネス・プライバシ・ポリシーが必要となる場合があります。プライバシに関する多くの法規では、個人を特定できる情報（PII）へのアクセスを企業で監視する必要があり、このような監視は監査によって実施されます。ビジネス・レベルのプライバシ・ポリシーでは、技術的、法的および企業ポリシーの問題など、データ・アクセスおよびユーザー・アカウンタビリティに関するすべての事項を満たす必要があります。

疑わしいデータベース・アクティビティの監査のガイドライン

監査の目的が疑わしいデータベース・アクティビティを監視することである場合は、次のガイドラインに従います。

1. **一般的な情報を監査してから、特定の情報を監査する**

   疑わしいデータベース・アクティビティの監査を開始する場合、対象となる特定のユーザーまたはスキーマ・オブジェクトについて入手できる情報量が多くないことがあります。したがって、最初は監査オプションをより一般的に設定します。つまり、7-3 ページの「標準監査による一般的なアクティビティの監査」で説明している標準監査オプションを使用して設定します。

   基本的な監査情報を記録および分析した後で、一般的な監査を無効にし、特定のアクションを監査します。『Oracle Database セキュリティ・ガイド』で説明されているファイングレイン監査を使用して、特定のアクションを監査できます。疑わしいデータベース・アクティビティの発生源に関する結論を引き出すのに十分な証拠を収集するまで、このプロセスを継続します。

2. **監査証跡を保護する**

   疑わしいデータベース・アクティビティを監査する場合は、監査情報が監査されずに追加、変更または削除されることのないように、監査証跡を保護します。AUDIT SQL 文を使用して、標準監査証跡を監査します。次に例を示します。

```
SQLPLUS "SYS/AS SYSDBA"
Enter password: password
SQL> AUDIT SELECT ON SYS.AUD$ BY ACCESS;
```

監査に使用される初期化パラメータ

表 7-1 には監査を保護するために使用する初期化パラメータがリストされています。

表 7-1 監査に使用される初期化パラメータ

初期化パラメータ	デフォルト設定	説明
AUDIT_TRAIL	DB	監査を有効または無効にします。詳細は、7-4 ページの「標準監査証跡の有効化または無効化」を参照してください。
AUDIT_FILE_DEST	*ORACLE_BASE*/admin/*ORACLE_SID*/adump または *ORACLE_HOME*/rdbms/audit	AUDIT_TRAIL 初期化パラメータが OS、XML または XML,EXTENDED に設定されている場合に監査証跡が書き込まれるオペレーティング・システム・ディレクトリを指定します。AUDIT_TRAIL 初期化パラメータが XML に設定されている場合、Oracle Database では監査レコードが XML 形式で書き込まれます。 Oracle Database では、必須の監査情報もこの場所に書き込まれ、AUDIT_SYS_OPERATIONS 初期化パラメータが設定されている場合はユーザー SYS の監査レコードが書き込まれます。

表 7-1 監査に使用される初期化パラメータ（続き）

初期化パラメータ	デフォルト設定	説明
AUDIT_SYS_OPERATIONS	FALSE	ユーザー SYS、および SYSDBA または SYSOPER 権限で接続しているユーザーによって発行された操作の監査を有効または無効にします。Oracle Database により、監査レコードがオペレーティング・システムの監査証跡に書き込まれます。さらに、AUDIT_TRAIL 初期化パラメータが XML または XML, EXTENDED に設定されている場合は監査レコードが XML 形式で書き込まれます。 UNIX システムでは、AUDIT_SYSLOG_LEVEL パラメータも設定した場合に、AUDIT_TRAIL パラメータが上書きされます。これにより、SYS 監査レコードは SYSLOG ユーティリティを使用してシステム監査ログに書き込まれます。
AUDIT_SYSLOG_LEVEL	デフォルト設定なし	UNIX システムでは、SYSLOG ユーティリティを使用して SYS および標準 OS 監査レコードをシステム監査ログに書き込みます。

初期化パラメータを変更するには、2-7 ページの「初期化パラメータ値の変更」を参照してください。初期化パラメータの詳細は、『Oracle Database リファレンス』および『Oracle Database 管理者ガイド』を参照してください。

索引

N

O

P

R

S

T

U

V

W

X

あ

え

お

か

き

く

け

ふ

へ

ゆ

ら

り

る

れ

ろ