Oracle9*i*

セキュリティ概要

リリース 2（9.2）

2002 年 7 月

部品番号：J06253-01

ORACLE®

Oracle9*i* セキュリティ概要 , リリース 2（9.2）

部品番号：J06253-01

原本名：Oracle9*i* Security Overview, Release 2 (9.2)

原本部品番号：A96582-01

原本著者：Jeff Levinger

原本協力者：Rita Moran, Kristy Browder, Mary Ann Davidson, John Heimann, Paul Needham, David Saslav, Uppili Srinivasan, Mike Cowan, Sudha Iyer, Richard Smith, Deborah Steiner, Daniel Wong, Valarie Moore

目次

5 保護ディレクトリの使用と配置

6 エンタープライズ・ユーザーのセキュリティの管理

7 監査によるシステム・セキュリティの監視

索引

はじめに

このマニュアルでは、インターネット環境におけるデータ・セキュリティの基本的な概念、基本的なデータ・セキュリティ要件およびデータの整合性やプライバシを脅かすリスクについて説明します。また、システム・セキュリティに貢献する豊富なテクノロジについても、数章にわたって説明します。最後に、これらのテクノロジを実装する Oracle の機能および製品を紹介します。

これらの製品によって、システムのすべての無防備な領域へのアクセスを制御できます。また、ユーザーと管理者は、実施されているセキュリティ計画を危険にさらすことなく各自のタスクを実行できます。

この項の内容は、次のとおりです。

対象読者

このマニュアルは、次のタスクを担当するデータベース管理者（DBA）、アプリケーション・プログラマ、セキュリティ管理者、システム・オペレータおよびその他の Oracle ユーザーを対象としています。

- アプリケーションのセキュリティ要件の分析
- セキュリティ・ポリシーの作成
- セキュリティ・テクノロジの実装
- エンタープライズ・ユーザーのセキュリティの管理

このマニュアルの内容は、データベースとネットワーキングの概念について全般的な知識を持っていることを前提としています。

このマニュアルの構成

このマニュアルでは、インターネット環境におけるシステム・セキュリティの基本的な概念、今日の主要なデータ・セキュリティ上のリスクとその対応に使用できる業界標準テクノロジの概要、さらにこれらのセキュリティ・テクノロジの実装に使用できるようにきめ細かく統合されている Oracle 製品パッケージについて説明します。

第 I 部 : セキュリティ要求

第 I 部では、データの整合性とプライバシに対するセキュリティ上の多様なリスクについて説明します。

第 1 章「データ・セキュリティ要求」

この章では、データ・セキュリティの基本的な概念と、データおよびシステムの保護を必要とする脅威について概要を説明します。

第 II 部 : セキュリティ・リスクに対する技術的なソリューション

第 II 部では、データ・セキュリティ要求を満たすために使用可能なテクノロジについて説明します。

第 2 章「データベース内のデータの保護」

この章では、データベース・セキュリティの基本要素について説明します。

第 3 章「ネットワーク環境でのデータの保護」

この章では、ネットワーク経由で転送中のデータを保護する方法について説明します。ネットワーク・アクセス制御、暗号化、Secure Sockets Layer（SSL）およびファイアウォールと、3 層環境におけるセキュリティを取り上げます。

第 4 章「データベースに対するユーザーの認証」

この章では、データベース、アプリケーションおよびネットワーク・ユーザーの識別情報の検証に使用可能な、多様なテクノロジについて説明します。

第 5 章「保護ディレクトリの使用と配置」

ディレクトリを使用すると、ユーザー関連の情報を単一のディレクトリに一元的に格納して管理できるというメリットがあります。この章では、このようなディレクトリを保護する方法と、ディレクトリを使用してアクセスを制御する方法について説明します。

第 6 章「エンタープライズ・ユーザーのセキュリティの管理」

この章では、エンタープライズ・ユーザー管理機能の構成要素について説明します。

第 7 章「監査によるシステム・セキュリティの監視」

この章では、セキュリティ・ポリシーの有効性の監視に使用可能なテクノロジについて説明します。

第 8 章「セキュリティに対する公開鍵インフラストラクチャによるアプローチ」

この章では、セキュリティに対する公開鍵インフラストラクチャ（PKI）アプローチを紹介します。PKI のコンポーネントと、PKI が業界標準となった理由を説明します。

第 III 部 : Oracle9*i* のセキュリティ製品

第 III 部では、データ・セキュリティ要件を満たすことのできる、Oracle セキュリティ製品パッケージについて説明します。

第 9 章「Oracle9i のセキュリティ製品および機能」

この章では、Oracle9*i* で使用できる主なセキュリティ関連製品と、各製品により第 II 部で説明した各種セキュリティ・テクノロジがどのように実装されるかについて説明します。

関連文書

詳細は、次の Oracle マニュアルを参照してください。

- 『Oracle9*i* データベース概要』
- 『Oracle9*i* アプリケーション開発者ガイド ー 基礎編』
- 『Oracle9*i* データベース管理者ガイド』
- 『Oracle Advanced Security 管理者ガイド』
- 『Oracle Internet Directory 管理者ガイド』
- 『Oracle Label Security 管理者ガイド』
- 『Oracle9*i* Net Services 管理者ガイド』
- 『Oracle9*i*AS Single Sign-On 管理者ガイド』
- 『Oracle9*i* Java 開発者ガイド』
- 『Oracle9*i* JDBC 開発者ガイドおよびリファレンス』
- 『Oracle Enterprise Manager 概要』

マニュアル・セットに含まれるマニュアルの多くでは、Oracle のインストール時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。これらのスキーマがどのように作成されているか、およびその使用方法については、『Oracle9*i* サンプル・スキーマ』を参照してください。

リリース・ノート、インストレーション・マニュアル、ホワイト・ペーパー、またはその他の関連文書は、OTN-J（Oracle Technology Network Japan）に接続すれば、無償でダウンロードできます。OTN-J を使用するには、オンラインでの登録が必要です。次の URL で登録できます。

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

OTN-J のユーザー名とパスワードを取得済みであれば、次の OTN-J Web サイトの文書セクションに直接接続できます。

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

表記規則

このマニュアル・セットの本文とコード例に使用されている表記規則について説明します。

本文の表記規則

本文中には、特別な用語が一目でわかるように様々な表記規則が使用されています。次の表は、本文の表記規則と使用例を示しています。

規則	意味	例
太字	太字は、本文中に定義されている用語または用語集に含まれている用語、あるいはその両方を示します。	この句を指定する場合は、**索引構成表**を作成します。
固定幅フォントの大文字	固定幅フォントの大文字は、システムにより指定される要素を示します。この要素には、パラメータ、権限、データ型、Recovery Manager キーワード、SQL キーワード、SQL*Plus またはユーティリティ・コマンド、パッケージとメソッドの他、システム指定の列名、データベース・オブジェクトと構造体、ユーザー名、およびロールがあります。	この句は、NUMBER 列に対してのみ指定できます。 BACKUP コマンドを使用すると、データベースのバックアップを作成できます。 USER_TABLES データ・ディクショナリ・ビューの TABLE_NAME 列を問い合せます。 DBMS_STATS.GENERATE_STATS プロシージャを使用します。
固定幅フォントの小文字	固定幅フォントの小文字は、実行可能ファイル、ファイル名、ディレクトリ名およびサンプルのユーザー指定要素を示します。この要素には、コンピュータ名とデータベース名、ネット・サービス名、接続識別子の他、ユーザー指定のデータベース・オブジェクトと構造体、列名、パッケージとクラス、ユーザー名とロール、プログラム・ユニット、およびパラメータ値があります。 **注意：**一部のプログラム要素には、大文字と小文字の両方が使用されます。この場合は、記載されているとおりに入力してください。	sqlplus と入力して SQL*Plus をオープンします。 パスワードは orapwd ファイルに指定されています。 データ・ファイルと制御ファイルのバックアップを /disk1/oracle/dbs ディレクトリに作成します。 department_id、department_name および location_id の各列は、hr.departments 表にあります。 初期化パラメータ QUERY_REWRITE_ENABLED を true に設定します。 oe ユーザーで接続します。 これらのメソッドは JRepUtil クラスに実装されます。

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

コード例の表記規則

コード例は、SQL、PL/SQL、SQL*Plus または他のコマンドラインを示します。次のように、固定幅フォントで、通常の本文とは区別して記載されています。

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

次の表は、コード例の記載上の表記規則と使用例を示しています。

規則	意味	例
[ ]	大カッコで囲まれている項目は、1 つ以上のオプションの項目を示します。大カッコ自体は入力しないでください。	DECIMAL (*digits* [, *precision*])
{ }	中カッコで囲まれている項目は、そのうちの 1 つのみが必要であることを示します。中カッコ自体は入力しないでください。	{ENABLE | DISABLE}
|	縦線は、大カッコまたは中カッコ内の複数の選択肢を区切るために使用します。オプションのうち 1 つを入力します。縦線自体は入力しないでください。	{ENABLE | DISABLE} [COMPRESS | NOCOMPRESS]
...	水平の省略記号は、次のどちらかを示します。 ■ 例に直接関係のないコード部分が省略されていること。 ■ コードの一部が繰り返し可能であること。	CREATE TABLE ... AS *subquery*; SELECT *col1*, *col2*, ..., *coln* FROM employees;
. . .	垂直の省略記号は、例に直接関係のない数行のコードが省略されていることを示します。	
その他の表記	大カッコ、中カッコ、縦線および省略記号以外の記号は、示されているとおりに入力してください。	acctbal NUMBER(11,2); acct CONSTANT NUMBER(4) := 3;

規則	意味	例
イタリック	イタリックの文字は、特定の値を指定する必要のあるプレースホルダまたは変数を示します。	`CONNECT SYSTEM/`*`system_password`* `DB_NAME = `*`database_name`

大文字	大文字は、システムにより提供される要素を示します。これらの用語は、ユーザー定義用語と区別するために大文字で記載されています。大カッコで囲まれている場合を除き、記載されているとおりの順序とスペルで入力してください。ただし、この種の用語は大 / 小文字区別がないため、小文字でも入力できます。	`SELECT last_name, employee_id FROM employees;`
		`SELECT * FROM USER_TABLES;`
		`DROP TABLE hr.employees;`

小文字	小文字は、ユーザー指定のプログラム要素を示します。たとえば、表名、列名またはファイル名を示します。
	注意：一部のプログラム要素には、大文字と小文字の両方が使用されます。この場合は、記載されているとおりに入力してください。
		`SELECT last_name, employee_id FROM employees;`
		`sqlplus hr/hr`
		`CREATE USER mjones IDENTIFIED BY ty3MU9;`

第 I 部

セキュリティ要求

第 I 部では、データの整合性とプライバシに対するセキュリティ上の多様なリスクについて説明します。

1

データ・セキュリティ要求

この章では、データ・セキュリティ要件の概要を説明し、対応を必要とするデータ・セキュリティ上のリスクのあらゆる側面を検証します。また、セキュリティ上のリスクと、現在使用可能なデータ保護のテクノロジの種類を関連付けるマトリックスを示します。この章は、次の項で構成されています。

注意： このマニュアルのセキュリティ・テクノロジの概要では、問題をできるかぎりテクノロジの実装方法から独立して記載しています。ただし、一部のテクノロジは、Oracle 製品にのみ用意されています。その場合は、Oracle ソリューションの観点から概念を説明しています。

Oracle のセキュリティ・ソリューションの詳細は、第 9 章「Oracle9i のセキュリティ製品および機能」を参照してください。

トップ・セキュリティに関する通説

データ・セキュリティの分野では誤った考え方が数多くあり、人々が非効率的なセキュリティ・ソリューションを設計する原因となっています。最も明らかなセキュリティ上の通説には、次のようなものがあります。

- 通説 : セキュリティに対する最大の脅威はハッカーです。

  実際には、データ消失のうち 80% は内部の関係者によるものです。

- 通説 : 暗号化によってデータが保護されます。

  実際には、暗号化はあくまでもデータ保護アプローチの 1 つです。セキュリティにはアクセス制御、データ整合性、システムの可用性および監査も必要です。

- 通説 : ファイアウォールによってデータが保護されます。

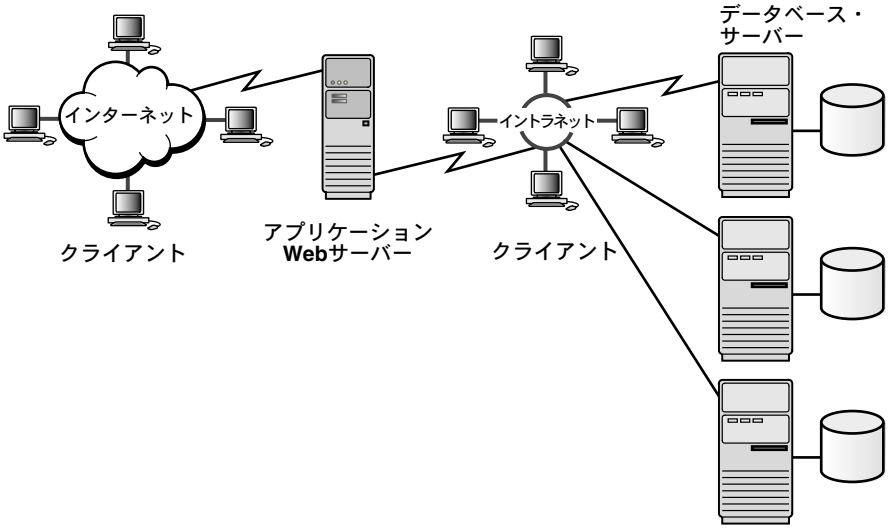
  実際には、インターネットへの侵入のうち 40% は、ファイアウォールがあるにもかかわらず発生したものです。

真にデータを保護するセキュリティ・ソリューションを設計するには、サイトに関連するセキュリティ要件と、現時点でデータに対する脅威となっている範囲を理解する必要があります。

システム・セキュリティの多数のディメンションの理解

インターネット環境では、貴重で重要なデータに対するリスクが従来よりも大きくなっています。図 1-1 に、データ・セキュリティ計画に組み込む必要のある複雑なコンピューティング環境の概要を示します。

図 1-1 データ・セキュリティ・ニーズの適用範囲



管理者はデータベースとそれが常駐するサーバーの保護、内部データベース・ユーザーの権限の管理と保護、データベースにアクセスする E-Commerce カスタマの機密性の保証を行う必要があります。インターネットは絶えず成長を続けており、ネットワーク経由でやりとりされるデータに対する脅威も飛躍的に増大しています。

複雑なコンピューティング・システムのあらゆる要素を保護するには、多数のディメンションでセキュリティ上の問題に対応する必要があります。表 1-1 の説明を参照してください。

表 1-1 データ・セキュリティのディメンション

ディメンション	セキュリティの問題
物理	コンピュータは、無許可ユーザーがアクセスできないように物理的に保護する必要があります。これは、安全な物理環境に置く必要があることを意味します。
人員	サイトでのシステム管理とデータ・セキュリティの担当者は、信頼できるユーザーである必要があります。採用を決定する前に、データベース管理者の経歴調査が必要となる場合があります。
手順	システムの操作に使用する手順は、信頼できるデータを保証するものである必要があります。たとえば、あるスタッフがデータベースのバックアップを担当するとします。その唯一の役割は、データベースを確実に稼働させることです。別のスタッフは、給与計算や売上データに関するアプリケーション・レポートの生成を担当する場合があります。その役割は、データを検査して整合性を確認することです。データ管理におけるユーザーの機能的な役割を分けた方が良い場合があります。
技術	データの格納、アクセス、操作および送信は、特定の情報制御ポリシーを施行するテクノロジで保護する必要があります。

データに対する特定のセキュリティ・リスクを慎重に検討し、採用するソリューションが実際に問題に適合しているかどうかを確認してください。技術ソリューションでは不適切な場合があります。たとえば、従業員が一時的に席を離れなければならない場合があります。技術ソリューションでは、このような物理的な問題は解決できません。作業環境を保護する必要があります。

基本的なデータ・セキュリティ要件

次の各項では、テクノロジで保証する必要のある基本的なセキュリティの標準について説明します。

- 機密保護
- 整合性
- 可用性

機密保護

保護システムによりデータの機密保護が保証されます。つまり、各ユーザーは想定されているデータのみを見ることができます。機密保護には、次の各項で説明するように異なる側面があります

- 通信のプライバシ
- 重要データの安全な格納
- 認証を受けたユーザー
- 細分化されたアクセス制御

通信のプライバシ

データ通信のプライバシを保護するには、どうすればよいでしょうか。プライバシは、きわめて広範囲の概念です。個人の場合は、健康、職歴および信用記録など、機密情報の流布を制御する機能が関連します。ビジネスの世界では、プライバシには取引上の機密、製品やプロセスに関する独自情報、競争力に関する分析、マーケティングや販売計画などが関連する場合があります。政府の場合、プライバシには人口統計情報を収集して分析する一方で、多数の市民の機密性を保護する機能などの問題が関連します。さらに、国家の利害に影響する機密を維持する機能も必要になります。

重要データの安全な格納

データを収集後に機密を保証するには、どうすればよいでしょうか。入力された機密データの整合性とプライバシを、データベースとそれが常駐するサーバー上で保護する必要があります。

認証を受けたユーザー

データを参照する権限を持ったユーザーと組織を指定するには、どうすればよいでしょうか。認証は、信頼するユーザーや組織に関する決定を実装する手段です。認証方式により、システム・ユーザーの個別性、つまり、ユーザーが他人を装っているのではなく、主張どおりの人間であることを保証することを目的としています。

細分化されたアクセス制御

特定のユーザーが参照する必要のあるデータの量はどの程度でしょうか。アクセス制御は、データへのアクセスが部分的に可能となるように、データベースの各部を遮断する機能です。人事部門の担当者は emp 表へのアクセスが必要ですが、会社全体の給与情報へのアクセスは許可しないようにする必要があります。アクセス制御の細分化により、データベースの特定の表、ビュー、行および列に対して異なるデータ・アクセス・レベルを設定できます。

認証、認可およびアクセス制御の違いに注意してください。認証は、ユーザーの識別情報がチェックされるプロセスです。ユーザーは認証を受けるときに、権限が付与されたアプリケーション・ユーザーとして確認されます。認可は、ユーザーの権限が確認されるプロセスです。アクセス制御は、アプリケーションの物理データに対するユーザーのアクセスを、権限に基づいて制限するプロセスです。この 3 つは、分散システムでは重要な問題です。たとえば、JAUSTEN がデータベースへのアクセスを試みた場合、認証により有効なユーザーとして識別されます。認可では、プロジェクト・マネージャ権限でデータベースに接続する権利があるかどうかが確認されます。アクセス制御により、JAUSTEN のユーザー・セッションではプロジェクト・マネージャ権限が施行されます。

整合性

保護システムにより、システム内のデータが有効であることが保証されます。データ整合性は、データベースに存在する間やネットワーク経由で送信される間に、データが削除や損傷から保護されていることを意味します。整合性には、次のような側面があります。

- システム権限とオブジェクト権限により、認可されたユーザー以外はデータを変更できないように、アプリケーションの表とシステム・コマンドへのアクセスが制御されます。
- 参照整合性は、定義済みのルールに従ってデータベース内の値間で有効な関係を保つ機能です。
- データベースは、データを破損させるように設計されたウィルスから保護する必要があります。
- ネットワーク通信は、削除、破損および盗聴から保護する必要があります。

可用性

保護システムにより、データは認可されたユーザーが即座に使用可能になります。DoS 攻撃は、許可されたユーザーが必要なときにシステムにアクセスし、使用するのを妨害する攻撃です。システムの可用性には、次のように様々な側面があります。

表 1-2 システム可用性に関する側面

可用性の側面	説明
抵抗	保護システムは、使用不能になるような状況または意図的な攻撃に対して防御するように設計する必要があります。たとえば、データベースにはリソース集中型の問合せを禁止する機能が必要です。ユーザー・プロファイルでは、特定のユーザーが消費できるリソースを定義し、制限する必要があります。これにより、ユーザーによる過大なメモリー消費やプロセス消費から（悪意によるものかどうかを問わず）システムを保護し、他のユーザーの作業を妨げません。
拡張性	システム・パフォーマンスは、サービスを要求するユーザー数やプロセス数に関係なく十分であることが必要です。
柔軟性	管理者には、全ユーザーを十分に管理できる手段が必要です。たとえば、そのためにディレクトリを使用する方法があります。
使用しやすさ	セキュリティ実装自体により、有効なユーザーの作業が制限されないようにする必要があります。

インターネット環境でのセキュリティ要件

インターネット環境でのデータ・セキュリティの領域は、次の各項で説明するような方法で拡大しています。

インターネットのメリットとデメリット

情報は、E-Business の根幹です。インターネットにより、顧客、仕入先、従業員およびパートナは必要なビジネス情報に必要な時点でアクセスでき、ビジネスにおける情報の使用効率が高まります。顧客は Web を使用して発注できるため、納品までの所要期間が短縮され、エラーも減少します。また、仕入先や物流センターは受注の時点から関与できるため、在庫が削減、または不要となり、従業員は業務情報を適切なタイミングで取得できます。また、インターネットにより、仕入先の場合はオンライン入札、顧客の場合はオンライン・オークションなど、まったく新しい価格設定メカニズムが可能になります。このようなインターネット対応サービスは、いずれもコストの削減につながり、さらに間接費の削減、規模の拡大、効率の向上などをもたらします。E-Business の最大のメリットは、情報へのアクセス・コストが削減され、多数の人々が適切なタイミングで貴重な情報にアクセスできることです。

E-Business のメリットは、データ・アクセスの直接性に関連するセキュリティ要求により相殺されます。仲介者の除外（ディストリビュータ、卸売業者および小売業者の取引連鎖からの排除）は、仲介者による情報のセキュリティも除外することになります。ユーザー・コミュニティは、イントラネット経由でデータにアクセスする信頼できる既知のユーザーで構成された小規模グループから、インターネット経由でデータにアクセスする大量のユーザーへと拡張されます。プロバイダとデータ交換を管理するアプリケーションでは、ユーザーや顧客によるセキュリティ要件が特に厳密であり、矛盾する場合もありますが、必要なコミュニティ間で保護データを共有できます。

ビジネス・システムをインターネットに置くことで効率の向上とコストの削減という面では無限の機会が得られますが、潜在的なリスクも無限になります。インターネットにより、正当なユーザーのみでなく、ハッカーや不満を抱いている従業員、犯罪者および企業スパイも、より重要なデータにより広範囲にアクセスできるようになります。

データ・アクセスの増加

インターネットによる E-Business の主なメリットの 1 つは、直接性にあります。電話や郵送で受け取った受注の入力など、従来は従業員が行っている中間的な情報処理ステップは、E-Business のプロセスからは削除されます。従業員ではなく、従来の会社という境界の外にいるユーザー（顧客、仕入先およびパートナなど）は、関連するビジネス情報にオンラインで直接、即時にアクセスできます。

従来のオフィス環境では、重要なビジネス情報へのアクセスは従業員経由で行われていました。従業員が常に信頼できるとはかぎりませんが、少なくとも従業員として識別されており、重要データへのアクセスは職務により制限され、アクセスは物理的制御と手順による制御で規定されています。セキュリティ・ポリシーに反して重要情報を社外に流す従業員は、懲戒処分の対象になる場合があります。したがって、懲戒の脅威は無認可アクセスの防止に役立ちます。

ビジネス情報にインターネット経由でアクセスできるようにすると、その情報にアクセスできるユーザー数は大幅に増加します。ビジネスがインターネットに移行すると、環境も激変します。会社は、自社システムにアクセスするユーザー（多くの場合は従業員ですが）に関してほとんど知らないか、何も知らない場合もあります。ユーザーが誰であるかがわかっていても、企業が情報に対する自社のポリシーに反したアクセスを阻止するのは困難です。したがって、企業は重要情報へのアクセスを管理し、その情報への無認可アクセスを発生前に防止することが重要になります。

有益なデータの増加

E-Business では、ビジネス情報に従来の会社の外側からアクセスできるようにすることのみでなく、ユーザーに最新で最良の情報を必要なタイミングで使用可能にすることが重要になります。たとえば、企業は仕入先に対して連結された受注情報への直接アクセスを許可することで、操作を簡素化して間接費を削減できます。これにより、仕入先に対する発注内容を必要なタイミングで正確に取得して、在庫を削減できます。また、データ交換によるオンライン入札など、新しい価格設定テクノロジを活用し、仕入先から最も有利な価格を取得したり、顧客に最適価格を提供できます。

ビジネス・システム経由の情報の流れを簡素化することで、ユーザーはシステムから適切な情報を取得できます。従来、外部のパートナ、仕入先または顧客からのデータは、しばしば非効率的なメカニズムを通じてシステムに入力されており、そのためにエラーや遅延が生じがちでした。たとえば、多くの企業は大量の受注を電話、文書またはファックスで受け入れ、この情報をスタッフや営業担当が入力していました。電子データ交換メカニズムは存在していましたが、通常は独自のものであり、企業の内部データ・インフラストラクチャと統合するのは困難でした。現在では、企業が他社や消費者にビジネス情報をインターネット経由で直接送受信することを許可していれば、より適切な時期に正確で有益な情報を、従来のデータ・チャネルを使用した場合よりも低コストで取得できます。

従来は、情報がビジネス・システムに入力されると、通常は区分化されていました。営業、製造、物流および財務など、社内の各部門がメンテナンスする情報は別個に保存され、通常は物理的に切り離されているため「情報の島」と呼ばれる、互換性のないデータベースやアプリケーションで処理されていました。このことが、各部門が必要な時点で情報を交換した

り、重役がビジネスの最新で正確な状態を判断することを困難にし、企業が手持ちの情報を十分に活用する妨げとなっていました。そこで、企業は、情報の島をできるかぎりリンクして連結すれば、ユーザーがより適切な情報を取得して、その情報からより多くのメリットを得られるようになることに気づいたのです。これにより、情報はさらに有益になります。

正当なユーザーが使用可能なデータの価値を高めると、通常は侵入者にとっても価値が高まります。このため、そのデータに対する無認可アクセスから得られる潜在的な見返りも大きくなり、データが破損すればビジネスが受ける損害も大きくなる可能性があります。つまり、E-Business システムの効率が高まるほど、無認可アクセスから保護する必要性も高くなります。

ユーザー・コミュニティの拡大

インターネット経由でビジネス・システムにアクセスできるユーザー・コミュニティの規模が変化すれば、そのシステムに対するリスクが増大するのみでなく、リスクに対応するために配置するソリューションも制約を受けることになります。インターネットにより、セキュリティ・メカニズムの拡張性、メカニズムの管理、および標準的で相互運用可能なものにする必要性が生じます。

拡張性

インターネット対応システムのセキュリティ・メカニズムでは、インターネット対応でないシステムに比べると、はるかに大規模なユーザー・コミュニティをサポートする必要があります。従来は、最大のエンタープライズ・システムでも一般にサポートされるユーザーは数千程度でしたが、多くのインターネット対応システムでは数百万のユーザーがサポートされます。

管理性

各ユーザーにアクセス先のシステムごとにアカウントとパスワードを付与するなど、ユーザーを識別してアクセスを管理する従来のメカニズムは、インターネット環境では実際的ではない場合があります。システム管理者が各システム上でユーザーごとに別個のアカウントを管理することは、すぐに困難で高コストの作業になります。

相互運用性

企業がシステムのすべてのコンポーネントを所有して制御する従来のエンタープライズ・システムとは異なり、インターネット対応の E-Business システムは、顧客、仕入先、パートナなど、他のユーザーが所有および制御するシステムとデータを交換する必要があります。したがって、E-Business システムに配置されているセキュリティ・メカニズムは、他のシステムと相互に運用できるように業界標準に準拠し、柔軟性と相互運用性を備えていることが必要です。また、Thin クライアントをサポートし、複数層アーキテクチャで動作する必要があります。

管理対象システムとデータ交換

ホストによる管理に関する主なセキュリティ要求は、様々な管理対象ユーザー・コミュニティからのデータの分離状態を保つことです。そのためには、管理対象となるコミュニティごとに物理的に別個のシステムを作成するのが最も単純な方法です。このアプローチのデメリットは、管理対象となるユーザー・コミュニティごとに別個のコンピュータを用意し、ソフトウェアを別個にインストール、管理および構成する必要があることです。これでは、ホスト会社にとってはコスト面でほとんどメリットがありません。

いくつかの要因により、ホスト・サービス・プロバイダにとってのコストを大幅に削減できます。たとえば、複数のユーザー・コミュニティによる単一のハードウェアおよびソフトウェア・インスタンスの共有を可能にするメカニズム、様々なユーザー・コミュニティのデータを分離するメカニズム、ホスト・プロバイダ用に単一の管理インタフェースを提供する方法などがあります。

データ交換には、データ分離とデータ共有の両面で要件があります。たとえば、データ交換では、仕入先の入札を他の仕入先が参照できないように保ち、入札を要求したエンティティはすべての入札を評価できるようにする必要があります。また、組織のグループがデータを選択的に共有したり、入札への参加などの作業は共同で行えるように、目的によるコミュニティもサポートできます。

データ・セキュリティのリスク

データの整合性とプライバシは、無認可ユーザー、ネットワーク上でリスニング中の外部ソースおよび情報を漏らしている内部ユーザーなどによるリスクにさらされています。この項では、リスクを伴う状況と、データを危険にさらす恐れのある攻撃について説明します。

- データの改ざん
- 盗聴とデータの盗難
- ユーザー ID の偽造
- パスワード関連の脅威
- 表と列への無認可アクセス
- データ行への無認可アクセス
- アカウンタビリティの欠落
- 複雑なユーザー管理要件

データの改ざん

通信のプライバシは、送信中にデータを変更または参照できないことを保証する上で不可欠です。分散環境では、悪意のある第三者がサイト間を移動する間にデータを改ざんし、コンピュータ犯罪を起こす可能性があります。

データ変更アタックの場合は、ネットワーク上の無認可ユーザーが送信中のデータを傍受し、その一部を変更してから再送する恐れがあります。この一例が、銀行のトランザクションの金額を $100 から $10,000 に変更する行為です。

再実行アタックの場合は、有効なデータ・セット全体がネットワークに繰り返し挿入されます。たとえば、有効な $100 の銀行口座振替トランザクションが 1000 回も反復される場合などです。

盗聴とデータの盗難

クレジット・カード番号などの情報が盗まれないように、データを安全に格納し、送信する必要があります。

インターネットおよび Wide Area Network（WAN）環境では、公共の通信業者とプライベート・ネットワーク所有者の両方が、しばしばネットワークの各部を非保護の通信線、きわめて無防備なマイクロ波や衛星リンク、または多数のサーバーを通じて転送しています。このような状況では、貴重なデータを関心のある人が誰でも参照できるようになっています。ビルや大学構内の Local Area Network（LAN）環境では、物理配線に触れることのできる内部関係者が、他人のデータを参照できる可能性があります。ネットワーク Sniffer をインストールして、ネットワークの通信を簡単に盗聴できます。また、パケット Sniffer は、ユーザー名とパスワードを探して盗み取るように設計できます。

ユーザー ID の偽造

接続しているユーザーを知る必要があります。分散環境では、ユーザーが ID を偽造して重要情報へのアクセスを取得する可能性が高くなります。クライアント B からサーバー A に接続しているユーザー Pat が、本当に Pat であるかどうかを確認するにはどうすればよいでしょうか。

また、犯罪者が接続をハイジャックする恐れもあります。クライアント B とサーバー A が主張どおり B および A であることを確認するにはどうすればよいでしょうか。サーバー A の人事システムからサーバー B の給与システムに送られるトランザクションが送信中に傍受され、かわりにサーバー B を装った端末に転送される恐れがあります。

ID の盗難は、インターネット環境における個人に対する最大の脅威の 1 つになりつつあります。犯罪者は、ユーザーのクレジット・カード番号を盗み取り、そのアカウントで買い物をしようと試みます。また、当座預金番号や運転免許証番号などを盗み取り、他人の名前でクレジット口座を開設することもあります。

否認防止という機能がないことも ID の問題です。ユーザーのデジタル署名は正しく保護されているでしょうか。ハッカーが他人のデジタル署名を盗み取った場合、そのプライベート

な署名キーを使用してなされた行為に対する責任がデジタル署名を盗まれたユーザーに課される場合があります。

パスワード関連の脅威

大型システムの場合、ユーザーは使用する様々なアプリケーションとサービスについて複数のパスワードを覚える必要があります。たとえば、開発者はワークステーション上の開発アプリケーション、電子メール送信用の PC、テスト、バグのレポート、構成管理用の複数のコンピュータまたはイントラネット・サイトへのアクセス権を持っている場合があります。

通常、ユーザーは複数のパスワードを管理するという問題に次のように複数の方法で対処しています。

- 名前、架空の文字または辞書に載っている単語など、推測しやすいパスワードを選択する場合があります。このようなパスワードはいずれもディクショナリ・アタックに対して無防備です。
- すべてのマシンまたは Web サイトに共通になるように、パスワードを標準化する方法を選択する場合もあります。この場合は、パスワードが危険にさらされた場合に、他のユーザーに知られる危険性が大きくなります。また、既知のパスワードに若干のバリエーションを持たせたパスワードを使用する場合もありますが、これは元のパスワードから簡単に導き出すことができます。
- 複雑なパスワードを使用するユーザーは、それを攻撃者が簡単に見つけられる場所にメモしていたり、単に忘れてしまう場合があります。このため、管理コストとサポート作業が増大します。

このような方法は、いずれもパスワードの機密性とサービスの可用性を危険にさらすことになります。さらに、複数のユーザー・アカウントとパスワードを管理する作業は複雑で、時間がかかり、しかも高コストです。

表と列への無認可アクセス

データベースに機密の表が含まれていたり、表に機密の列が含まれている場合があります。その場合は、データベースへのアクセスを認可されているユーザー全員が直接は使用できないようにする必要があります。また、データを列レベルで保護できるようにする必要があります。

データ行への無認可アクセス

特定のデータ行に機密情報が含まれており、表へのアクセスが認可されているユーザーが直接は使用できないようにする必要が生じる場合があります。

アクセス制御の細分化、つまり、データ自体の機密保護を施行する手段が必要です。たとえば、共有環境では、企業は自社データへのアクセスのみが必要で、顧客が参照できるのはその注文のみにする必要があります。必要な区画化がアプリケーションにより追加されるのではなく、データに施行されていれば、ユーザーはバイパスできません。

したがって、システムには柔軟性、つまり、対象が顧客であるか従業員であるかに応じて異なるセキュリティ・ポリシーをサポートする機能が必要です。たとえば、従業員（より多くのデータを参照できるユーザー）には、顧客の場合よりも厳密な認証を要求できます。また、従業員にはすべての顧客レコードの参照を許可する一方で、顧客が参照できるのは各自のレコードのみにすることもできます。

アカウンタビリティの欠落

システム管理者がユーザーのアクティビティを追跡できなければ、ユーザーは各自のアクションについて責任を持つことができません。そこで、データを誰がどのように操作しているかを監視するために、信頼性の高い手段が必要です。

複雑なユーザー管理要件

通常、システムでは数千～数十万のユーザーをサポートする必要があるため、拡張可能であることが必要です。このような大規模環境では、ユーザー・アカウントとパスワードの管理に伴う負荷により、システムがエラーや攻撃に対して無防備になります。信頼性の高いセキュリティを実現するには、ユーザーが実際には誰であるかを、アプリケーションのすべての層で知る必要があります。

複数層システム

この問題は、複数層システムでは特に複雑になります。この場合やほとんどのパッケージ・アプリケーションでは、代表的なセキュリティ・モデルは「単一の大型アプリケーションのユーザー」です。このモデルでは、ユーザーはアプリケーションに接続し、アプリケーション（またはアプリケーション・サーバー）が単一のユーザーでデータベースにログオンします。全員に完全なアクセス権が提供され、監査はなく、無制限の権限が付与されます。このモデルの場合、データはリスクにさらされます。特にインターネットでは、Web サーバーやアプリケーション・サーバーはファイアウォールに依存しているため、リスクがあります。ファイアウォールは、一般に侵入に対しては無防備です。

複数システムのセキュリティ管理のスケール変更

数十万のユーザーを管理することは、単一システムの場合にも困難です。この負荷は、複数システムでセキュリティを管理する必要がある場合にはさらに複雑になります。

セキュリティ管理の拡張要求を満たすには、業界標準に基づくディレクトリを使用して、複数のアプリケーションおよびデータベース間でユーザーと権限を一元的に管理できるようにする必要があります。これにより、システム管理コストを削減し、ビジネスの効率を向上させることができます。

さらに、複数のアプリケーション・サブスクライバ用に別個のデータベースを作成して構築するのは、アプリケーション・サービス・プロバイダにとって費用効率の高いモデルであるとは言えません。技術的には可能ですが、サブスクライバごとに別個のデータベースを構築するモデルは短期間のうちに管理不能になります。成功を収めるには、単一のアプリケーション・インストレーションで複数の企業を集結し、一元的に管理できるようにする必要があります。

セキュリティ・リスクとソリューションのマトリックス

表 1-3 に、セキュリティ・リスク、それに対処するテクノロジおよび対応する Oracle 製品の関係を示します。

表 1-3 セキュリティ・リスクとソリューションのマトリックス

問題	ソリューション	セキュリティ・テクノロジ	Oracle の製品と機能
無認可ユーザー	ユーザーの識別	認証	Oracle9*i* Standard Edition および Oracle9*i* Enterprise Edition: パスワード、パスワード管理 Oracle Advanced Security: トークン、スマート・カード、Kerberos など PKI: X.509 証明書

表 1-3 セキュリティ・リスクとソリューションのマトリックス（続き）

問題	ソリューション	セキュリティ・テクノロジ	Oracle の製品と機能
データへの無認可アクセス	データへのアクセス制限	アクセス制御	Oracle9*i* Standard Edition Oracle9*i* Enterprise Edition: 仮想プライベート・データベース機能
	動的問合せの変更	ファイングレイン・アクセス・コントロール	Oracle9*i* Enterprise Edition: 仮想プライベート・データベース機能
	データ行および列へのアクセス制限	ラベル・ベースのアクセス制御	Oracle Label Security
	データの暗号化	データ暗号化	Oracle9*i* Standard Edition および Oracle9*i* Enterprise Edition
	権限の制限	権限の管理	Oracle9*i* Standard Edition: ロール、権限 Oracle9*i* Enterprise Edition: 保護アプリケーション・ロール Oracle Advanced Security: エンタープライズ・ロール
通信の盗聴	ネットワークの保護	ネットワーク暗号化	Oracle Advanced Security: 暗号化 Secure Sockets Layer
データの破損	ネットワークの保護	データ整合性	Oracle Advanced Security: チェックサム PKI: チェックサム（SSL に付属）
サービスの拒否	リソースへのアクセス制御	可用性	Oracle9*i* Standard Edition および Oracle9*i* Enterprise Edition: ユーザー・プロファイル
ユーザーにとっての複雑さ	パスワード数の制限	シングル・サインオン	Oracle Advanced Security: Kerberos、DCE、エンタープライズ・ユーザーのセキュリティ Login Server: Web ベースの SSO
管理者にとっての複雑さ	管理の一元化	エンタープライズ・ユーザー・セキュリティ	Oracle Advanced Security: ディレクトリの統合 Oracle Internet Directory

表 1-3 セキュリティ・リスクとソリューションのマトリックス（続き）

問題	ソリューション	セキュリティ・テクノロジ	Oracle の製品と機能
アカウンタビリティの欠落	ユーザー・アクションの監視	監査	Oracle9*i* Standard Edition: 監査 Oracle9*i* Enterprise Edition: 標準監査、ファイングレイン監査
データへの過大に広範囲なアクセス	動的問合せの変更	ファイングレイン・アクセス・コントロール	Oracle9*i* Enterprise Edition: 仮想プライベート・データベース Oracle Label Security
多すぎるアカウント数	管理の一元化	ディレクトリ・サービス、LDAP 準拠のディレクトリ・サービス	Oracle Internet Directory
オペレーティング・システムへの侵入	重要データの暗号化	格納されたデータの暗号化	Oracle9*i* Standard Edition および Oracle9*i* Enterprise Edition: データ暗号化

システム・セキュリティ・チーム

複雑なデータ・セキュリティ・システムでは、スタッフ・チームが特定のサイトでのセキュリティを確保する必要があります。表 1-4 に、関連する管理者のタイプを示します。

表 1-4 システム・セキュリティ・チーム

スタッフ	職責
ユーザー	正当な目的へのシステムの使用、アクセス権を付与されている重要データの保護およびパスワードの安全管理を担当します。
データベース管理者	データベース・ユーザーの作成と管理、システム権限とオブジェクト権限の付与およびユーザーに対するローカル・ロールの割当てを担当します。
オペレーティング・システム管理者	オペレーティング・システムの基礎となるセキュリティのメンテナンスを担当します。
ネットワーク管理者	送信中のデータのセキュリティ確保を担当します。
アプリケーション管理者	セキュリティを確保できる方法でアプリケーションを配置する作業を担当します。
トラステッド・アプリケーション管理者	トラステッド・アプリケーションのユーザーおよび関連権限の作成と管理を担当します。
エンタープライズ・セキュリティ・マネージャ	ディレクトリのセキュリティのメンテナンスと、一元化されたエンタープライズ・ユーザーのセキュリティの実装を担当します。

第 II 部

セキュリティ・リスクに対する技術的ソリューション

第 II 部では、データ・セキュリティ要求を満たすために使用可能なテクノロジについて説明します。

- 第 2 章「データベース内のデータの保護」
- 第 3 章「ネットワーク環境でのデータの保護」
- 第 4 章「データベースに対するユーザーの認証」
- 第 5 章「保護ディレクトリの使用と配置」
- 第 6 章「エンタープライズ・ユーザーのセキュリティの管理」
- 第 7 章「監査によるシステム・セキュリティの監視」
- 第 8 章「セキュリティに対する公開鍵インフラストラクチャによるアプローチ」

2

データベース内のデータの保護

どの様なコンピュータ・システムでもデータは様々な箇所で無防備になっており、それを保護するために多数のセキュリティ手法と各種の機能を採用できます。この章では、サーバーに常駐するメモリー、ファイルおよびプロセスを保護できるセキュリティ機能を系統的に紹介します。この章は、次の項で構成されています。

注意： このマニュアルのセキュリティ・テクノロジの概要では、問題をできるかぎりテクノロジの実装方法から独立して記載しています。ただし、一部のテクノロジは、Oracle 製品にのみ用意されています。その場合は、Oracle ソリューションの観点から概念を説明しています。

Oracle のセキュリティ・ソリューションの詳細は、第 III 部の「Oracle9i のセキュリティ製品」を参照してください。

データベース・セキュリティ概念の概要

機密保護、整合性および可用性は、データベース・セキュリティの品質証明であると言えます。つまり、データにアクセスする権利を持っているのは誰か、すべてのデータのうち、特定のユーザーにアクセスを許可する必要があるのはどの部分か、権限を持つユーザーに対して実行を許可する必要があるのはどんなデータ操作か、権限を持つユーザーは必要なときに有効なデータにアクセスできるかなどです。

認可は、オブジェクトまたはオブジェクト・セットにアクセスできるように、ユーザー、プログラムまたはプロセスに付与される許可です。ユーザーに付与されるデータ・アクセスのタイプには、読取り専用と読取り / 書込みがあります。権限により、ユーザーがデータに対して実行できるデータ操作言語（DML）操作を指定します。

この章では、これらの事項とデータベース・セキュリティの他の基本的な概念について説明します。

システム権限とオブジェクト権限

権限は、表を問い合せるための許可など、指定したオブジェクトに規定された方法でアクセスするための許可です。権限は、ユーザーに対し、他のユーザー（管理者）の裁量で付与されます。また、特定のユーザーに権限を付与することで、データベースへの接続（セッションの作成）、各自のスキーマでの表の作成、他のユーザーの表からの行の選択または他のユーザーのストアド・プロシージャの実行を許可できます。

次の各項では、データベース内の権限を次の 2 つのカテゴリに分けて説明します。

- システム権限
- スキーマ・オブジェクト権限

関連項目： 9-4 ページ「権限」

システム権限

システム権限により、ユーザーはシステム単位の特定のアクションや、特定タイプのスキーマ・オブジェクトに対する特定のアクションを実行できます。たとえば、表領域を作成するための権限や、データベース内の任意の表から行を削除するための権限は、システム権限です。多くのシステム権限はきわめて強力なため、使用できるのは管理者とアプリケーション開発者に限られています。

スキーマ・オブジェクト権限

データへのアクセスは、ほとんどの場合はデータベース自体または特定の表へのアクセス・レベルで制御されます。スキーマ・オブジェクト権限により、ユーザーは特定のスキーマ・オブジェクトに対して特定のアクションを実行できます。たとえば、特定の表の行を削除するための権限は、オブジェクト権限です。

表に対するスキーマ・オブジェクト権限があれば、データ操作言語（DML）およびデータ・ディクショナリ言語（DDL）の操作のレベルで表のセキュリティを確保することが可能です。たとえば、管理者は個々のユーザーに対して、表またはビューに対する DELETE、INSERT、SELECT および UPDATE といった各 DML 操作を使用するための権限や、表に対して DDL 操作を実行するための ALTER、INDEX および REFERENCES 権限を付与できます。

権限は列レベルで指定できます。表に対するユーザーの INSERT および UPDATE 権限を、表の個々の列に限定できます。同様に、権限を行レベルで指定することも可能です。表に対するユーザーの SELECT、INSERT、UPDATE および DELETE の各権限を、表の特定の行に限定できます。

一般的なルールとして、オブジェクト権限はそのオブジェクトの所有者によってのみ付与されます。ただし、所有者は、特定ユーザーに他のユーザーへの権限付与の権限を指定することもできます。スキーマ内のオブジェクトに関するアクションの全範囲に及ぶ権限は、通常、デフォルトで管理者に付与されます。管理者は、この完全セットを他のユーザーに委譲できます。つまり、ユーザーやグループに対する付与や取消しを選択的に行うことができます。特に、管理者は GRANT ANY OBJECT PRIVILEGE に対する権限をアプリケーション開発者または DBA に付与できます。この権限を付与することで、開発者は直面するセキュリティ構成作業を容易に行い、DBA は発生したアクセス制御の問題を解決しやすくなります。

システム権限とオブジェクト権限の管理

ユーザーが有効なユーザー名とパスワードを入力できるかということを、データベースまたは特定のデータベース表にアクセスするための最初の認証レベルとして使用できます。次の各項では、システム権限とオブジェクト権限の厳密な管理に使用できる他の手法を説明します。

- ロールを使用した権限の管理
- ストアド・プロシージャを使用した権限の管理
- ネットワーク機能を使用した権限の管理
- ビューを使用した権限の管理

ロールを使用した権限の管理

ロール・メカニズムは認可を与えるために使用することができます。1 人のユーザーまたはユーザー・グループに、1 つのロールまたはロールのグループを付与できます。また、1 つのロールに他のロールを付与することもできます。管理者が各種のロールを定義すると、アクセス権限の管理がはるかに簡単になります。

この項の内容は、次のとおりです。

- データベースのロール
- グローバル・ロール
- エンタープライズ・ロール
- 保護アプリケーション・ロール

関連項目： 9-4 ページ「ロール」

データベースのロール

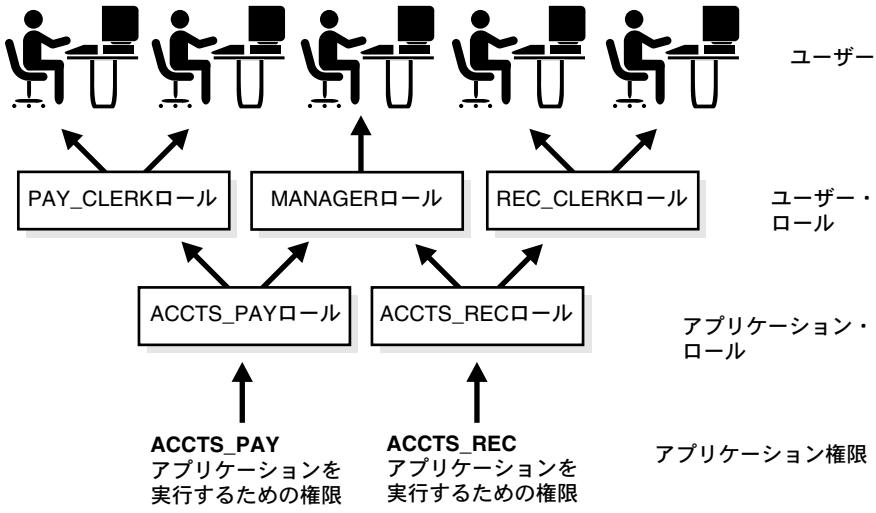
権限により、ユーザーはデータベースのデータに対しアクセスや変更が行えます。データベースのロールは、ユーザーまたは他のロールに付与される、特定のジョブに関連した権限の名前付きグループです。ロールにより権限の管理がより簡単で適切なものになるため、通常は権限を特定のユーザーではなくロールに付与します。ユーザーに付与されているロールを選択的に有効または無効にすることができます。これにより、特定の状況でのユーザーの権限を特定の方法で制御できます。たとえば、ロールの使用はパスワードで保護できます。アプリケーションを、適切なパスワードが入力された場合にロールを有効にするように作成できます。これによって、パスワードを知らないユーザーは、ロールを有効にできなくなります。

次のロールのプロパティにより、権限管理が簡単になります。

- 権限付与の削減。データベース管理者は、同じ権限セットを多数のユーザーに対して明示的に付与するのではなく、関連ユーザー・グループに対する権限をロールに付与し、そのロールをグループの各メンバーに付与できます。
- 動的な権限管理。グループの権限を変更する必要がある場合は、ロールの権限を変更するのみですみます。グループのロールを付与されていたすべてのユーザーのセキュリティ・ドメインには、ロールの変更内容が自動的に反映されます。
- 権限の選択的可用性。ユーザーに付与されているロールを選択的に有効（使用可能）または無効（使用不可）にすることができます。これにより、特定の状況でのユーザーの権限を特定の方法で制御できます。
- アプリケーションの検出。データベース・アプリケーションは、ユーザーがアプリケーションの使用を試みた時点で、ロールを選択的、自動的に有効または無効にするように設計できます。

各種レベルのロールと権限を使用すると、アクセス制御をさらに細分化し、図 2-1 のように最小限の権限という原則に従うことができます。この図の各個人に付与されるのは、それぞれのジョブの実行に必要な権限のみです。

図 2-1 ロールの共通使用



グローバル・ロール

グローバル・ロールは、エンタープライズ・ユーザー・セキュリティのコンポーネントの 1 つです。このロールは単一のデータベースにのみ適用されますが、エンタープライズ・ディレクトリに定義されているエンタープライズ・ロールに付与できます。グローバル・ロールはディレクトリ内で管理されますが、その権限は単一データベース、つまり、ロールが定義されているデータベースに含まれています。

グローバル・ロールは、権限とロールを付与することでデータベース内でローカルに定義しますが、実際に他のユーザーやデータベース内の他のロールにグローバル・ロールを付与することはできません。エンタープライズ・ユーザーがデータベースへの接続を試みると、そのユーザーに対応付けられたグローバル・ロールを取得するために、ディレクトリに問合せが行われます。

エンタープライズ・ロール

エンタープライズ・ロールは、複数のデータベース上のグローバル・ロールを含むことのできるディレクトリ構造であり、エンタープライズ・ユーザーに付与できます。エンタープライズ・ロールを LDAP ベースのディレクトリ・サービスに格納して管理すると、認可など、ユーザー関連情報の管理を一元化できます。

たとえば、エンタープライズ・ロール `clerk` には、人事管理データベースに対して一意の権限を持つグローバル・ロール `hrclerk` と、給与計算データベースに対して一意の権限を持つ `analyst` ロールを含めることができます。

エンタープライズ・ロールでは、1 人以上のエンタープライズ・ユーザーに対して権限の付与または取消しができます。たとえば、エンタープライズ・ロール `clerk` を、同じジョブを担当する多数のエンタープライズ・ユーザーに付与できます。この情報はディレクトリ内で保護され、ユーザーの管理、およびそのロールの付与および取消しができるのは管理者のみです。

ユーザーには、エンタープライズ・ロールの他に、データベース内でのローカル・ロールおよび権限を付与できます。

関連項目： 第 6 章「エンタープライズ・ユーザーのセキュリティの管理」

保護アプリケーション・ロール

長期的なセキュリティの問題となっていたのは、ユーザーによるデータへのアクセス方法を制限し、ユーザーがアプリケーション・ロジックをバイパスしてデータに直接アクセスできないようにすることでした。たとえば、Web ベースのアプリケーションでは、ユーザーがデータベースに認識されていても、データへの直接アクセスを許可しない方がよい場合があります。従来は、データへのアクセスに使用されるアプリケーションの妥当性を安全にチェックする手段がなかったため、これはきわめて解決が困難なセキュリティ上の問題でした。たとえば、悪意のあるユーザーが、有効な人事管理アプリケーションであるかのように見えるプログラムを記述する可能性がありました。

この問題に対処する方法の 1 つは、保護アプリケーション・ロール、つまりパッケージにより実装されるロールを使用することです。パッケージでは必要な妥当性チェックを実行し、ユーザーがデータベース内でロールに付与されている権限を実行する前に、該当する条件が満たされているかどうかを確認できます。データベースでは、それが適切なアクセス条件を決定するロールを実装する唯一のトラステッド・パッケージであることが保証されます。

保護アプリケーション・ロールはアプリケーションにより使用され、アプリケーションのみによって有効化され、パスワードは不要です。

関連項目： 9-19 ページ「保護アプリケーション・ロール」

ストアド・プロシージャを使用した権限の管理

ストアド・プロシージャを通じて、ユーザーが実行できるデータベース操作を制限できます。定義者権限で実行するプロシージャおよびファンクションを通じてのみ、データへのアクセスを許可できます。たとえば、ユーザーに、表を更新するプロシージャへのアクセス権を付与し、表自体へのアクセス権は付与しないという方法があります。ユーザーがプロシージャをコールすると、そのプロシージャは所有者の権限で実行されます。プロシージャの実行権限のみを持つ（ただし、基礎となる表の問合せ、更新または削除を行う権限は持たない）ユーザーは、そのプロシージャをコールできますが、それ以外の方法では表のデータを操作できません。

関連項目： 9-5 ページ「ビュー、ストアド・プログラム・ユニット、トリガー」

ネットワーク機能を使用した権限の管理

データベースのロールを外部サービス（DCE グループや RADIUS 認可など）にマップし、すべてのネットワーク・リソースの権限を一元的に管理できます。データベースは、ネットワーク・リソースの 1 個にすぎません。

関連項目：

- 第 3 章「ネットワーク環境でのデータの保護」
- 9-49 ページ「Oracle Net Services」

ビューを使用した権限の管理

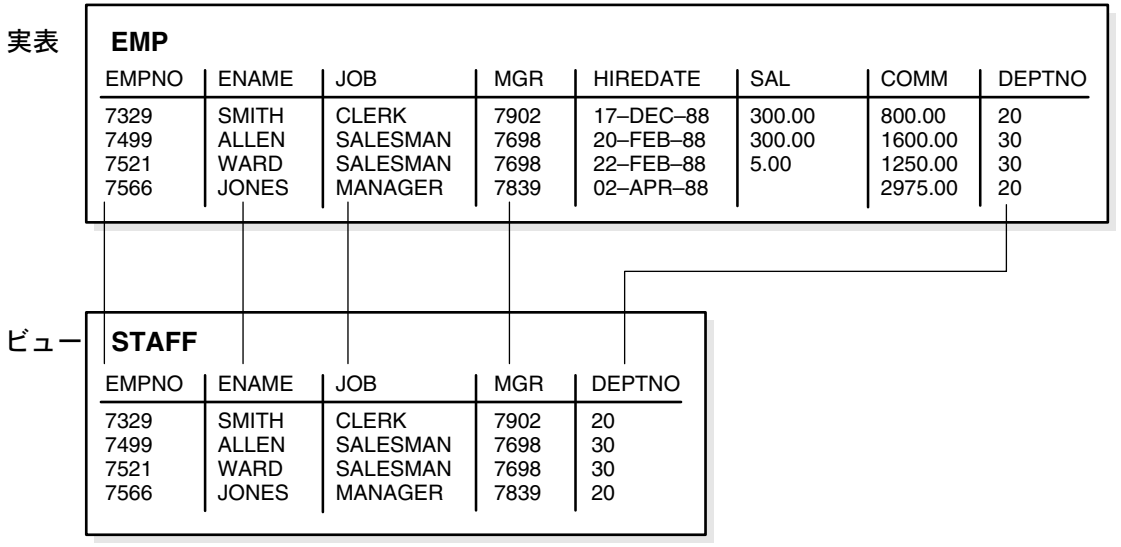
ユーザーに特定の表に対する権限を付与するのではなく、表のビューへのアクセス権を付与できます。ビューにより、さらに 2 つのセキュリティ・レベルが追加されます。

- ビューを使用すると、アクセスを実表のうち選択した列のみに限定できます。
- また、表内の情報について値ベースのセキュリティを提供できます。したがって、ビューの定義の WHERE 句で表示できるのは、実表のうち選択した行のみとなります。

ビューを使用するために必要となるのは、ビュー自体に対する適切な権限のみです。ユーザーに、ビューの基礎となるベース・オブジェクトに対する権限を付与する必要はありません。

図 2-2 に、実表 emp から導出されたビュー staff の例を示します。このビューには、実表のうち 5 列のみが表示されていることに注意してください。

図 2-2 ビューの例



関連項目： 9-5 ページ「ビュー、ストアド・プログラム・ユニット、トリガー」

行レベルのセキュリティ

さらに単位の小さいデータ・アクセスは、行レベルのアクセスです。データを持つ表であれば、その特定の行へのアクセスを従業員が所属する部門、職責や職位または他の重要な要因などを考慮して設定できます。従来、行レベルのセキュリティの実装には複合ビューと動的ビューが使用されていました。しかし、この問題に対しては他に 2 つの効果的なアプローチがあります。1 つは仮想プライベート・データベース（VPD）で、行レベルのセキュリティの独自実装を作成します。もう 1 つはラベル・ベースのアクセス制御で、既存の VPD ポリシーを目的に合せてカスタマイズします。この項では、これらのアプローチについて説明します。

- 複合ビューと動的ビュー
- アプリケーションのクエリー・リライト : 仮想プライベート・データベース
- ラベル・ベースのアクセス制御

複合ビューと動的ビュー

複合ビューと動的ビューは、行レベルのセキュリティに対する従来のアプローチです。複合ビューを定義する場合は、アプリケーション設計者が独自のユーザー・セキュリティ表を作成し、アプリケーション・ユーザーの名前に基づいてアプリケーション表を新規のセキュリティ表と結合します。通常、このアプローチには多数の複合ビュー定義が必要であり、セキュリティ要件の変化に応じたメンテナンスが必要となります。もう 1 つのアプローチは、動的ビューを作成することです。このアプローチでは、動的 DDL 実行ユーティリティを使用し、アプリケーション・ユーザーの識別情報に基づいて新規のビュー定義を定義します。ただし、動的ビューは高コストで時間もかかります。

アプリケーションのクエリー・リライト : 仮想プライベート・データベース

仮想プライベート・データベースには、パッケージで定義し、表、ビューまたはシノニムに対応付けたセキュリティ・ポリシーに基づいて、問合せ文を変更する機能があります。また、データ駆動型かつコンテキスト依存型かつ行ベースのファイングレイン・アクセス・コントロールを提供しています。これは、ミッション・クリティカルなリソースを顧客やパートナに公開する 3 層システムを構築するうえで、重要なテクノロジです。

関連項目： 9-12 ページ「Oracle9i の仮想プライベート・データベース」

ラベル・ベースのアクセス制御

ラベル・ベースのアクセス制御を使用すると、組織はデータ行に機密性ラベルを割り当て、そのラベルに基づいてデータへのアクセスを制御し、データが適切な機密性ラベルでマークされることを保証できます。この最もわかりやすい例は、米国などの政府が採用しているセキュリティ分類システムです。このモデルでは、情報の機密性レベルに基づいて、CONFIDENTIAL、SECRET または TOP SECRET など、階層形式の分類ラベルがデータに割り当てられます。また、NATO や CRYPTO など、公式のセキュリティ区分も定義され、データに割り当てられています。特定レベル（SECRET など）のラベルが付いたデータへのアクセスは、そのレベル以上のアクセス権を付与されているユーザーに限定されます。特定区分（CONFIDENTIAL NATO など）のデータへのアクセスは、該当レベルへのアクセス権と問題の区分への明示的なアクセス許可が付与されているユーザーに限定されます。

通常、E-Business にはラベル・データ分類システムはありませんが、ほぼ常にデータ・ラベル付けの要件を伴っています。たとえば、E-Business では、社内秘情報と公開情報を区別している場合があります。また、一部の社内秘情報は機密情報公開契約や他の法的文書に基づいてパートナと共有可能にする一方、他の情報へのアクセスは社内の特定グループ（財務部門や営業部門など）に限定できます。ラベル付きのデータを管理する機能が備わっていれば、E-Business では適切な保護データ・アクセス・レベルで適切なユーザーに適切な情報を提供するという大きなメリットが得られます。

関連項目： 9-42 ページ「Oracle Label Security」

サーバー上でのデータの暗号化

暗号化は、権限を持つユーザー以外は理解できないようにデータをエンコーディングする手法です。ただし、データを保護するには暗号化のみでは十分ではありません。データベース内のデータを保護するには、アクセス制御、データ整合性、暗号化および監査などの方法があります。この項の内容は次のとおりです。

- 格納されているデータの選択的暗号化
- 業界標準の暗号化アルゴリズム

格納されているデータの選択的暗号化

ある種のアプリケーションでは、追加のセキュリティ措置としてデータを暗号化するように決定する場合があります。データ・セキュリティのほとんどの問題は適切な認証およびアクセス制御により処理でき、適切に識別され、権限が付与されたユーザーのみがデータにアクセスできることを保証できます。ただし、データベース管理者はすべての権限を持っているため、通常、データベース内のデータをデータベース管理者によるアクセスからは保護できません。同様に、組織ではサード・パーティによって格納されたバックアップ・ファイルなど、オフラインで格納された機密データの保護が問題になる場合があります。侵入者がデータベースに物理的に格納されているデータにアクセスできないようにガードする必要があります。

暗号化は効率的なアクセス制御の代替策ではありませんが、データベースに格納する前に機密データを選択的に暗号化することで、追加のセキュリティ対策を得ることができます。特に機密性が高く、保証付きの暗号化を必要とする情報には、クレジット・カード番号、厳密なプライバシ保護法を持つ国における身分証明書番号、工業上の数式のような取引上の機密などがあります。ユーザーがデータベースではなくアプリケーションに対して認証されるアプリケーションでは、暗号化も使用してアプリケーション・ユーザーのパスワードや Cookie を保護できます。

業界標準の暗号化アルゴリズム

業界標準の多数の暗号化アルゴリズムは、サーバー上のデータの暗号化と復号化に役立ちます。最も普及しているのは、次の 2 つです。

データ暗号化規格（DES）	データのプライバシについて業界標準に準拠した暗号化を提供します。
Triple-DES（3DES）暗号化	メッセージ・データは DES アルゴリズムを利用して 3 回暗号化されます。

RC4 暗号化アルゴリズムはストリーム暗号であるため、データベースでの暗号化には適していないことに注意してください。ネットワークでの暗号化には役立ちます。

関連項目：

- 3-4 ページ「暗号化アルゴリズム」
- 9-20 ページ「データベースでの Java セキュリティ実装」
- 9-49 ページ「Oracle Net Services」

データベースの整合性メカニズム

データベースの整合性により、データベース内のデータが正確で一貫性を持っていることが保証されます。データベースの整合性メカニズムは、システムの整合性をサポートするメカニズムと、リレーショナル・データベースの整合性プロパティ（エンティティの整合性、参照整合性、トランザクション整合性およびビジネス・ルールなど）を施行するメカニズムに分けることができます。

従来のシステム整合性の場合は、システムに挿入されたデータが実際に取り出されるときの内容と同一であることを保証します。また、権限が付与されていないユーザーは、データの変更や削除を禁止されます。

データベースでは、データがデータベース管理者またはアプリケーション開発者によって決定された特定のビジネス・ルールに準拠していることを保証する必要があります。たとえば、ビジネス・ルールでは、emp 表内の従業員は salary 列の値の 20% を超える昇給を受け取ることができないと規定されているとします。この整合性ルールへの違反を試みる insert 文または update 文は、失敗する必要があります。整合性制約とデータベース・トリガーを使用すると、データベースのデータ整合性ルールを管理できます。

参照整合性は、表の列または列セットに対して定義されたルールが、関連する表の値（参照値）と一致するようにします。また、参照整合性には、参照先のデータに対してどのようなタイプのデータ操作を許可するか、およびその操作の結果として依存値がどのような影響を受けるかについて指示するルールが含まれています。参照整合性ルールを使用すると、このような関係を持たせることができます。

関連項目： 9-2 ページ「整合性」

システム可用性の要因

データ・セキュリティでは、権限を持つユーザーが必要に応じてデータにアクセスできることも必要です。可用性は、通常はサービスの継続性とみなされ、データベースが 1 日 24 時間、1 週 7 日間を通じて使用可能であることを保証するものです。ただし、可用性にはセキュリティという側面もあります。たとえば、ユーザーが他のユーザーに対して可用性を拒否するためにシステム・リソースを操作できるとすれば、それはセキュリティ違反となります。これは**サービスの拒否**と呼ばれます。

システム可用性は、次のような要因により保護できます。

表 2-1 システム可用性の要因

要因	説明
記憶域割当て制限	管理者が、デフォルト表領域、一時表領域および表領域割当て制限を含め、各ユーザーに対してデータベースに割り当てられているディスク領域の使用を指示し、制限できるようにします。
リソース制限	各ユーザーには、ユーザーが確立できる同時セッション数、ユーザー・セッションに使用可能な CPU 処理時間、ユーザーが使用可能な論理 I/O の量など、そのユーザーが使用可能なシステム・リソースを制限するプロファイルを割り当てる必要があります。
ホット・バックアップ	データは、予期しないデータ消失やアプリケーション・エラーに備えた保護対策としてコピーする必要があります。オリジナル・データが失われても、バックアップを使用して再構成できます。
攻撃に対する抵抗	ソフトウェアは、保護コーディング規格に従って記述する必要があります。
保護構成	システムは、悪意のある侵入者が利用できるような無防備さを露呈しないような方法でセットアップする必要があります。
パラレル・システム	クラスタを使用すると、キュー・データに対する可用性の高いアクセスを保証できます。キューはデータベース表を使用して実装できます。インスタンス障害が発生した場合は、そのインスタンスで管理されているメッセージを、障害を起こしていないインスタンスの 1 つで即時に処理できます。

関連項目： 9-5 ページ「高可用性」

保護構成

最後に、データ・セキュリティを保証するために採用するテクニックは、データベース管理者が適切なセキュリティに従っていなければ無駄になります。たとえば、DBA は常に次のことに注意する必要があります。

- パブリック・アカウントの権限の取消し
- 使用していないアカウントのロック
- インストール後のデフォルト・パスワードの変更
- 適切な許可の設定。権限を管理するためにロールを実装できますが、オペレーティング・システムで許可が適切に設定されていなければ、セキュリティ上の抜け穴になる恐れがあります。

関連項目：

- 『Oracle9*i* データベース管理者ガイド』
- 『Oracle9*i* アプリケーション開発者ガイド ー 基礎編』

3

ネットワーク環境でのデータの保護

この章では、ネットワーク経由で転送中のデータを保護する方法について説明します。この章は、次の項で構成されています。

- ネットワーク環境におけるデータ保護の概要
- 送信中のデータの保護
- 3 層システムでのセキュリティの保証

ネットワーク環境におけるデータ保護の概要

セキュリティの問題は、ネットワーク環境ではさらに複雑になります。ネットワークへのアクセスが制御されていることと、データがネットワーク経由の転送中に攻撃に対して無防備にならないことを保証する必要があります。データの暗号化を行うためには様々なテクノロジを利用可能ですので、そのプライバシと整合性を保証するのに役立ちます。この種のテクノロジでは、次のことが保証されます。

- データの機密性が保たれること。
- データを変更できないこと。
- データを再生できないこと。
- 失われたパケットを検出できること。

複数層システムが関係している場合は、ネットワーク・アクセスがさらに複雑になります。ユーザーは中間層からネットワークにアクセスできますが、その場合にデータベースで認識されるのは中間層のみで、個々のユーザーの認可は失われることがあります。機密性を保証するには、中間層からアクセスしている実際のユーザーをデータベースで識別できる必要があります。

関連項目：

- 9-24 ページ「Oracle Advanced Security のネットワーク・セキュリティ・サービス」
- 9-25 ページ「Oracle Advanced Security のデータ整合性機能」
- 9-49 ページ「Oracle Net Services」

送信中のデータの保護

次の各項では、送信中のデータのプライバシと整合性を保証するために使用可能なテクノロジについて説明します。

- ネットワーク内でのアクセスの制御
- ネットワーク送信用のデータの暗号化
- Secure Sockets Layer（SSL）プロトコル
- ファイアウォール

ネットワーク内でのアクセスの制御

この項では、ネットワーク内でのアクセスを制御する様々な方法について説明します。

中間層の接続管理

きわめて大規模なユーザー人口の接続を管理する中間層を構成できます。多数のユーザーをサポートするために、Oracle Connection Manager の複数インスタンスを構成できます。この製品では、データベースへの単一のネットワーク接続を通じて複数のクライアントのネットワーク・セッションが多重化され、接続の総数が増加します。

ソース、宛先およびホスト名にフィルタを適用することもできます。これにより、物理的な保護端末または既知の IP アドレスを持つアプリケーション Web サーバーからのみ接続されることを保証できます（IP アドレスのみでは、偽装できるため認証には不十分です）。この方法では、IP アドレスの `foo` から `payroll` のホスト `bar` への接続を許可できます。

関連項目： 9-50 ページ「Oracle Connection Manager」

システム固有のネットワーク機能（有効なノードのチェック）

機密データベースの場合は、ネットワーク上の特定のポイントからのみ接続されるように保証する必要があります。たとえば、会社は、ユーザー `jausten` は職場でのみ給与計算データベースにアクセスできるというセキュリティ・ポリシーを設定できます。

関連項目： 9-53 ページ「Oracle Net Services での有効なノードのチェック」

データベースにより施行されるネットワーク・アクセス

仮想プライベート・データベース（または保護アプリケーション・ロール）を使用して、特定のネットワーク・ノードからデータベースへのアクセスを制限することもできます。IP アドレスは偽装される恐れがあるため、ユーザーの主要な認証または認可方法として使用しないように注意してください。ただし、IP アドレスは、他の方法で権限が付与されているユーザーについてデータへのアクセスを制限する補助的手段として使用できます。たとえば、ユーザー Jane は `emp` 表へのアクセス権を持っていますが、会社の方針では Jane が社内イントラネット内にいない場合は、人事管理部門の特定のサブネットからであっても、従業員データへのアクセスを許可しないように指示できます。

関連項目：

- 9-12 ページ「Oracle9i の仮想プライベート・データベース」
- 9-54 ページ「データベースにより施行される VPD ネットワーク・アクセス」

ネットワーク送信用のデータの暗号化

イントラネットまたはインターネットを通じて転送される機密データは、暗号化によって保護できます。暗号化は、情報を復号鍵がなければ読めない形式に変換する処理です。暗号化は、復号鍵がなければ数学的に解読することは不可能になるため、強力なセキュリティ・メカニズムです。

たとえば、インターネットによる購入者が、保護された方式でクレジット・カードを使用して会社の製品を購入することを希望しているとします。購入者のクレジット・カード番号は、暗号鍵で暗号化されます。暗号化されたクレジット・カード番号は、ネットワーク経由でデータベースに送信されます。暗号化によりメッセージがスクランブルされ、受信者以外は誰も読み取れなくなります。サーバーでは、メッセージが復号鍵を使用して復号化され、クレジット・カード番号が読み取られます。

暗号化されたデータの機密性は、通信の送信側と受信側の間で共有される秘密鍵の存在に依存しているため注意してください。このような秘密鍵を提供してメンテナンスする作業は、キー管理と呼ばれます。マルチユーザー環境では、安全にキーを配布するのが困難な場合があり、この問題を解決するために公開鍵暗号が発明されました。

暗号化では、クライアントからの送信と中間層からの送信を含め、データベースとの通信すべてを取り扱う必要があります。また、データベースへのすべてのプロトコルを保護する必要があります。

暗号化アルゴリズム

表 3-1 に、業界標準となっているデータの暗号化と復号化に関する暗号化アルゴリズムを示します。

表 3-1 暗号化アルゴリズム

アルゴリズム	特性
RSA Data Security RC4	データ・プライバシのための高速な暗号化が可能です。各セッションに一意のランダムに生成される秘密鍵を使用することで、すべてのデータ値、SQL 文およびストアド・プロシージャ・コールとその結果など、ネットワークの通信量全体が完全に保護対策の対象となります。クライアントまたはサーバー、あるいはその両方が、データが保護されていることを保証するために暗号化モジュールの使用を要求できます。
データ暗号化規格（DES）	対称鍵暗号を使用してネットワーク通信を保護します。金融機関や他の多数の機関には、DES が必要です。

表 3-1 暗号化アルゴリズム（続き）

アルゴリズム	特性
Triple-DES（3DES）暗号化	メッセージ・データが DES アルゴリズムで 3 回暗号化されます。3DES は高度なメッセージ・セキュリティを提供します。ただし、暗号化を実行するプロセッサの速度に依存するというパフォーマンス上のデメリットを伴います。通常、3DES の場合は、標準的な DES アルゴリズムに比べると、データ・ブロックの暗号化に 3 倍の時間が必要です。

関連項目：

- 2-11 ページ「格納されているデータの選択的暗号化」
- 9-24 ページ「Oracle Advanced Security のネットワーク・セキュリティ・サービス」

データ整合性チェック

暗号化に加えて、データの改ざんやパケットの再送がないことを保証できる整合性アルゴリズムがあります。データベースでは、このようなアルゴリズムを使用してデータ・ブロックの破損を検出できます。表 3-2 に、業界標準の整合性アルゴリズムを示します。

表 3-2 整合性アルゴリズム

アルゴリズム	特性
MD5 チェックサム	ハッシングと順序付けを通じてデータ整合性を提供し、データがネットワーク経由での送信中に変更されたり盗まれないことを保証します。
Secure Hash Algorithm（SHA）	MD5 に似ていますが、より大きなメッセージ・ダイジェストを生成して、より高度なセキュリティを提供します。

Secure Sockets Layer（SSL）プロトコル

Secure Sockets Layer（SSL）プロトコルは、Netscape 社によって開発され、ネットワーク・トランスポート層のセキュリティに関して業界で受け入れられている標準です。SSL は、現在使用可能なすべての Web サーバーと Web ブラウザでサポートされます。また、LDAP や IMAP など、他のプロトコルが受け入れられるというメリットもあります。SSL プロトコルは、公開鍵インフラストラクチャ（PKI）で認証、データ暗号化およびデータ整合性を提供します。

SSL は、3 層システムの層間で交換されるユーザー・データの保護という問題に対応します。強力で標準ベースの暗号化および整合性アルゴリズムを提供することで、SSL はシステム開発者およびユーザーに対してインターネット上でデータが危険にさらされないことを保証します。クライアントをサーバーに対してのみ認証するパスワード・ベースの認証とは異なり、SSL はクライアントに対してサーバーを、サーバーに対してクライアントを認証できます。ユーザーは通常、サーバーにクレジット・カード番号などの機密情報を提供する前に、アプリケーション Web サーバーの識別情報を認証するように要求するため、これは Web ベースの 3 層システムを構築する場合に役立つ機能です。

関連項目：

- 8-5 ページ「Secure Sockets Layer 認証と X.509v3 デジタル証明書」
- 9-26 ページ「Secure Sockets Layer（SSL）の暗号化機能」
- 9-31 ページ「Oracle Advanced Security での Secure Sockets Layer（SSL）認証」

ファイアウォール

ネットワーク・インフラストラクチャの潜在的な弱点を排除するために、複雑な復号化や再暗号化を行わずに、プロトコル間でデータを渡すように選択できます。これを安全に行うには、ネットワーク・プロトコルの境界をまたがってデータを安全に転送するなんらかの手段が必要になります。

インターネットでは、社内イントラネットを広範囲のパブリック・ネットワークに接続できます。この機能はビジネスに大きなメリットをもたらしますが、データやコンピュータ・システムも危険にさらされることになります。システムのプライバシと整合性を保護する方法の 1 つは、パブリック・ネットワークとイントラネットの間にファイアウォールを設けることです。

ファイアウォールは、ネットワーク上の単一の制御ポイントであり、認可されていないクライアントがサーバーに到達するのを防止するために使用されます。また、フィルタとして機能し、権限を持たないネットワーク・ユーザーがイントラネットを使用できないように排除します。そのために、送信されるデータのパケットの内容に基づいてアクセス制御を施行し、個々のプロトコルやアプリケーションに対する攻撃から保護できます。ファイアウォールはルールベースです。ファイアウォールには、接続できるクライアントと接続できないクライアントを定義するルールのリストがあります。クライアントのホスト名または IP 名をルールと比較して、クライアントにアクセス権を付与するかどうかを決定できます。

関連項目： 9-51 ページ「Oracle Net Services によるファイアウォールのサポート」

3 層システムでのセキュリティの保証

次の各項では、複数層システムにおけるセキュリティの問題について説明します。

- 3 層のセキュリティを保証するためのプロキシ認証
- Java Database Connectivity（JDBC）

3 層のセキュリティを保証するためのプロキシ認証

3 層システムの重要なセキュリティ機能は、中間層からデータベースに認証済みユーザーの識別情報をプロキシする機能です。この機能は *n* 層認証とも呼ばれ、実際に中間層を通じてデータベースにアクセスしているユーザーを識別できます。ユーザーとマシンは、データベース・パスワードまたは他の資格証明を使用して認証され、別個のデータベース接続によるオーバーヘッドは生じません。また、権限を持たないユーザーが中間層経由でインターネット上のサーバーにあるデータにアクセスできないことを確実にすることで、サーバー上のデータが保護されます。アカウンタビリティは、誰がアプリケーションでどんな操作を行ったかをトレースできるように、中間層を通じてアプリケーションにログオンしたユーザーを追跡することで保証されます。拡張性は、エンタープライズ・ユーザーのサポートの導入を通じてさらに改善されます。

関連項目：

- 4-8 ページ「プロキシ認証および認可」
- 9-8 ページ「Oracle9i でのプロキシ認証」

Java Database Connectivity（JDBC）

Java を使用して 3 層環境でデータを安全に送信できます。Java はインターネット用の言語であり、OLAP アプリケーションにも採用されています。アプリケーション開発者は、Java を使用してアプリケーションとアプレットをビルドします。Java はオブジェクト指向でプラットフォームに依存しないネットワーク・ベースの保護言語であり、アプリケーション開発者が選択する言語として C++ と Visual Basic よりも急速に利用が増加しつつあります。

JDBC（Java Database Connectivity）は業界標準の API（Applications Program Interface）であり、Java プログラムでは SQL 文を Oracle などのオブジェクト・リレーショナル・データベースに送信できます。JDBC により、中間層サーバーはユーザー用の軽量セッションを確立し、クライアント・ユーザーのかわりにデータベースにアクセスできます。

したがって、Java アプレットは保護チャネルを通じてデータを送信できます。JavaServer Pages（JSP）を使用すると、中間層サーバーからデータベースへの保護接続を確立できます。これにより、次の理由でセキュリティが強化されます。

- 各プロトコルを保護できます。
- JDBC-Oracle Call Interface と Thin クライアントをサポートできます。
- 2 層と 3 層のアーキテクチャをサポートできます。

Java のセキュリティおよびネゴシエート・アルゴリズムを実装するには、次の 2 つの方法があります。

- JDBC クライアント・アプリケーションにハード・コーディングします。
- システム固有のネットワーク暗号と同様に構成します。

JDBC Oracle Call Interface ドライバ

JDBC Oracle Call Interface（JDBC OCI）ドライバは、クライアント側に Oracle クライアントをインストールすると使用できるようになります。

JDBC Thin ドライバ

JDBC Thin ドライバは、Java ソケットを使用してデータベース・サーバーに直接接続するタイプ 4（100% Pure Java）のドライバです。これは Java Net と呼ばれ、Oracle Net の軽量 Java 実装です。

Thin ドライバには、クライアント側の Oracle ソフトウェアは不要です。サーバー側には TCP/IP リスナーが必要です。このドライバを、Web ブラウザにダウンロードされる標準の Oracle Net リスナーの Java アプレットに使用してください。Thin ドライバは自己完結型ですが、Java ソケットをオープンするため、ソケットをサポートするブラウザでなければ実行できません。

関連項目： 9-27 ページ「Oracle Advanced Security の Java 暗号化機能」

4

データベースに対するユーザーの認証

ユーザー ID の認証は、分散環境では必須です。認証がなければ、ネットワークやデータベースのセキュリティの信頼性は低くなります。この章は、次の項で構成されています。

ユーザー認証の概要

基本的なセキュリティ要件は、ユーザーを認識することです。つまり、最初にユーザーを識別しなければ、その権限やアクセス権を決定できません。データに対するアクションを監査できるように、ユーザーを認識する必要があります。

ユーザーは、データベース・セッションの作成を許可される前に、様々な方法で認証を受けるようにできます。データベース認証の場合は、データベースでユーザーの識別と認証の両方を実行できるようにユーザーを定義できます。外部認証の場合は、オペレーティング・システムまたはネットワーク・サービスにより認証が実行されるように、ユーザーを定義できます。また、Secure Sockets Layer（SSL）により認証されるようにユーザーを定義することもできます。エンタープライズ・ユーザーの場合は、ディレクトリを使用し、エンタープライズ・ロールを通じてデータベースへのアクセス権を付与できます。さらに、中間層サーバー経由の接続を許可するユーザーを指定できます。中間層サーバーでは、ユーザー ID が認証され、それを前提としてそのユーザーの特定のロールの有効化が許可されます。これは、プロキシ認証と呼ばれます。

認証用のパスワード

パスワードは、基本的な認証形式の 1 つです。ユーザーは、データベースの無認可使用を防ぐために、接続の確立時に適切なパスワードを入力する必要があります。この方法では、データベースへの接続を試みるユーザーを、そのデータベースに格納されている情報を使用して認証できます。パスワードは、ユーザーの作成時に割り当てられます。データベースでは、ユーザーのパスワードをデータ・ディクショナリに暗号化形式で格納できます。ユーザーは割り当てられたパスワードをいつでも変更できます。

パスワードに依存するデータベース・セキュリティ・システムでは、パスワードを常に秘密にする必要があります。ただし、パスワードは盗まれたり、忘れたり、悪用される危険性があります。次のように多数の手順により基本的なパスワード機能を強化し、データベース・セキュリティを厳密に制御できます。

- データベース管理者とセキュリティ管理者は、ユーザー・プロファイルを通じてパスワード管理ポリシーを制御できます。
- データベース管理者は、パスワードの最小長など、パスワードの複雑さに関する標準を設定できます。
- パスワードには、辞書にないワードを使用する必要があります。氏名や生年月日は使用しないでください。
- パスワードには、一定期間後に期限切れになるようにタイムアウトを設定できます。これにより、ユーザーは値を定期的に変更することが必要になります。
- パスワードの再利用を一定期間は禁止できます。
- 特定のユーザーのログイン失敗回数が指定した回数を超えた場合に、サーバーではそのユーザーのアカウントを自動的にロックできます。

厳密認証

中央の機能にネットワークのすべてのメンバー（サーバーに対してクライアント、サーバーに対してサーバー、クライアントとサーバーの両方に対してユーザー）を認証させるのは、ネットワーク上のノードが識別情報を偽装する脅威に効果的に対応する方法の 1 つです。2 つの要素による認証を使用して、厳密認証を設定することもできます。つまり、ユーザーが知っている情報（PIN など）と、ユーザーが持っているもの（トークン・カードなど）の組合せです。

厳密認証には、次のように重要なメリットがあります。

- スマート・カード、Kerberos またはオペレーティング・システムなど、使用可能な認証メカニズムの選択肢が豊富です。
- Kerberos や DCE など、多数のネットワーク認証サービスでシングル・サインオンがサポートされています。つまり、ユーザーが覚えるパスワードが少なくてすみます。
- すでに認証になんらかの外部メカニズムを使用している場合は、そのメカニズムをデータベースでも使用すれば、管理上のオーバーヘッドを削減できる場合があります。

この項では、分散環境で使用できる次の厳密認証方式について説明します。

- Kerberos および CyberSafe
- RADIUS
- トークン・カード
- スマート・カード
- 分散コンピューティング環境（DCE）
- バイオメトリック
- PKI および証明書ベースの認証

関連項目： 9-3 ページ「Oracle9i における認証とアクセス制御」

Kerberos および CyberSafe

Kerberos は、マサチューセッツ工科大学が作成した信頼度の高いサード・パーティ認証システムであり、インターネット上で無償で提供されています。

Kerberos は共有シークレットを使用します。サード・パーティが安定していると想定して、シングル・サインオン機能、パスワード集中格納、データベース・リンク認証、拡張 PC セキュリティを提供します。これは、Kerberos 認証サーバー経由、または民間の Kerberos ベース認証サーバーである CyberSafe ActiveTrust 経由で行われます。

Kerberos によるシングル・サインオンには多数のメリットがあります。単一の集中的なパスワード・ストアのみですむため、管理上のオーバーヘッドが削減され、ユーザーはパスワードを 1 つ覚えるのみですみます。また、ネットワーク・アクセス時間を制御でき、DES 暗号化と CRC-32 整合性を使用して無認可アクセスやパケットの再生から保護できます。さらに、現行ユーザーのデータベース・リンクを使用可能にします。Kerberos 対応のデータベースでは、Kerberos ユーザーが Kerberos を通じてシングル・サインオンで接続できるように、クライアントの識別情報を次のデータベースに伝播させることができます。

CyberSafe は Kerberos の市販バージョンであり、CyberSafe ActiveTrust サーバーのサポートなど、特定の付加機能とサポートが追加されています。CyberSafe によりセキュリティが一元化され、シングル・サインオンが可能になります。Kerberos と同様に、CyberSafe もパスワード・ベースですが、認証メカニズムははるかに強力です。

関連項目： 9-32 ページ「Oracle Advanced Security と Kerberos および CyberSafe」

RADIUS

RADIUS（Remote Authentication Dial-In User Service）プロトコルは、認証ベンダーによって共通の通信方式として採用されている業界標準プロトコルです。RADIUS には、クライアントと認証サーバー間のユーザー認証、認可および課金の機能があります。ユーザーによるネットワークへのリモート・アクセスの使用を許可している組織の多くは、RADIUS を使用しています。RADIUS は業界で広範囲に受け入れられており、柔軟性があり、使用しやすいようにすべてのユーザー情報を集中化でき、ユーザー管理コストを削減できるため、企業は RADIUS を採用しています。認証プロセス全体がユーザーからは、シームレスで透過的に行われます。

関連項目： 9-32 ページ「Oracle Advanced Security と RADIUS」

トークン・カード

トークン・カードは、ユーザーをデータベースに対して認証する 2 つの要素によって認証する方式を提供します。アクセス権を取得するには、ユーザーは物理的なカードを所有し、パスワードを知っている必要があります。

トークン・カード（SecurID または他の RADIUS 準拠のカード）により、複数の異なるメカニズムを通じて利便性を改善できます。一部のトークン・カードは、認証サービスと同期化されているワンタイム・パスワードを動的に表示します。サーバーは認証サービスと連絡を取り合うことによって、トークン・カードが提供するパスワードをいつでも検証できます。キーパッド付きで、要求 / 応答に基づいて機能するトークン・カードもあります。この場合は、サーバーが要求（番号）を提供し、ユーザーがその番号をトークン・カードに入力します。そして、トークン・カードは応答（要求から暗号的に導出される別の番号）を提供し、それをユーザーが入力してサーバーに送信します。

表 4-1 に、トークン・カードのメリットを示します。

表 4-1 トークン・カードのメリット

メリット	説明
厳密認証	犯罪者がユーザーを装うには、トークン・カードとその操作に必要な個人識別番号（PIN）を入手する必要があります。これを 2 つの要素による認証と呼びます。
使用しやすさ	ユーザーは、複数のパスワードを覚えるかわりに 1 つの PIN を覚えるのみですみます。
簡単なパスワード管理	複数のパスワードではなく単一のトークン・カードが使用されるため、パスワード管理が簡単です。
アカウンタビリティの明確化	トークン・カードの認証メカニズムは強力なため、ユーザーはアクションの責任が明確になります。

関連項目： 9-33 ページ「Oracle Advanced Security とトークン・カード」

スマート・カード

RADIUS 準拠のスマート・カードは、クレジット・カードに似たハードウェア・デバイスです。メモリーとプロセッサが組み込まれており、クライアント・ワークステーションにあるスマート・カード・リーダーによって読み取られます。表 4-2 に、スマート・カードのメリットを示します。

表 4-2 スマート・カードのメリット

メリット	説明
セキュリティの強化	スマート・カードは 2 つの要素による認証を行います。スマート・カードはロックでき、ロックを解除できるのは、カードを所有していて、適切な個人識別番号（PIN）を知っているユーザーのみです。
パフォーマンスの改善	一部の洗練されたスマート・カードには、ハードウェア・ベースの暗号化チップが組み込まれており、ソフトウェア・ベースの実装よりもスループットが高くなります。スマート・カードにはユーザー名も格納できます。
すべてのワークステーションからのアクセス可能性	ユーザーがログインするときには、スマート・カードをハードウェア・デバイスに挿入します。これにより、カードが読み取られ、PIN など、カードに必要な認証情報の入力を求めるプロンプトが表示されます。ユーザーが適切な認証情報を入力すると、スマート・カードにより他に必要な認証情報が生成されて入力されます。
メモリー	スマート・カードにはメモリーが組み込まれているため、暗号鍵、ユーザーの秘密鍵およびデジタル証明書などを格納できます。

関連項目： 9-33 ページ「Oracle Advanced Security とスマート・カード」

分散コンピューティング環境（DCE）

Open Software Foundation（OSF）からの分散コンピューティング環境（DCE）は、複数のシステム間で動作して分散環境を提供する、統合ネットワーク・サービスの集合です。ネットワーク・サービスには、リモート・プロシージャ・コール（RPC）、ディレクトリ・サービス、セキュリティ・サービス、スレッド、分散ファイル・サービス、ディスクレス・サポートおよび分散タイム・サービスなどが含まれます。

DCE は、分散アプリケーション、オペレーティング・システムおよびネットワーク・サービス間のミドルウェアであり、クライアント / サーバー・コンピューティング・モデルに基づいています。DCE が提供するサービスとツールを使用すると、ユーザーは異機種環境にまたがって動作する分散アプリケーションを作成、使用およびメンテナンスできます。

関連項目： 9-33 ページ「Oracle Advanced Security と分散コンピューティング環境（DCE）」

バイオメトリック

バイオメトリック・ソリューションは、厳密認証を達成するもう 1 つの手段です。このアプローチでは、個人を識別して認証するために指紋や音声などの物理特性が使用されます。

関連項目： 9-33 ページ「Oracle Advanced Security とバイオメトリック認証」

PKI および証明書ベースの認証

公開鍵インフラストラクチャ（PKI）は、安全な情報交換を保証するために使用できる、業界標準のプロシージャとポリシーのセットです。暗号化方式とアクセス制御、およびユーザーの認証に使用できるデジタル証明書の形式によるセキュリティ資格証明を提供します。

関連項目：

- 8-4 ページ「保護証明書 : PKI における証明書ベースの認証」
- 9-37 ページ「Oracle Advanced Security の PKI 実装」

プロキシ認証および認可

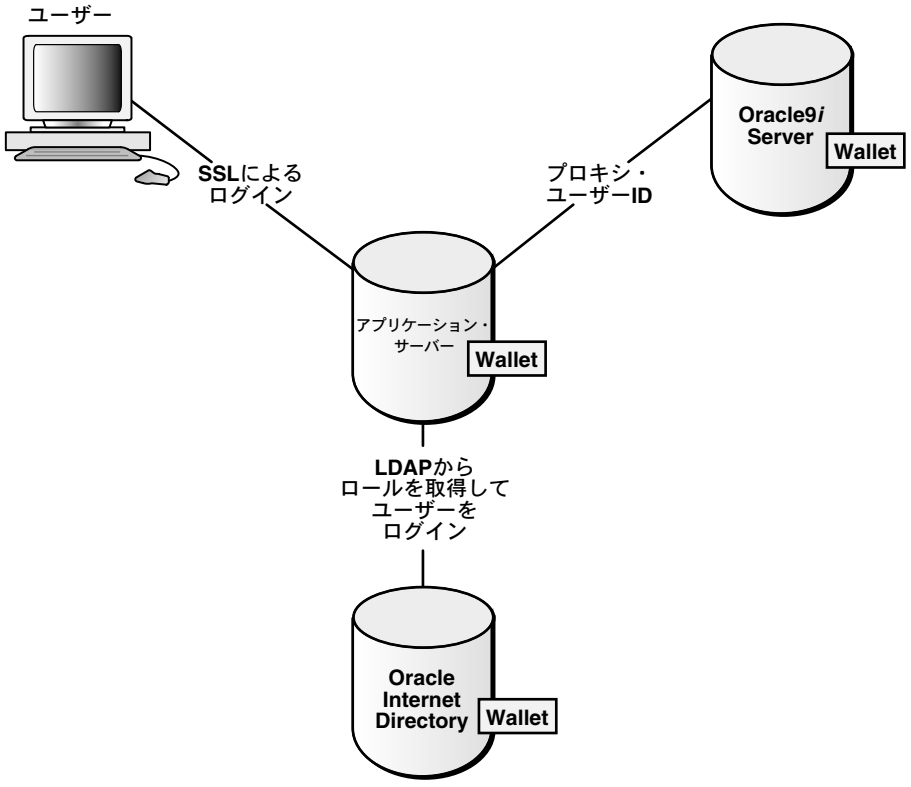
トランザクション処理モニターなどの複数層環境では、すべての層を通じてクライアントの識別情報と権限を保ち、クライアントのかわりに実行されたアクションを監査して、中間層アプリケーションのセキュリティを制御する必要があります。これは、プロキシ認証を使用すれば可能です。たとえば、この機能により、Web アプリケーション（プロキシとも呼ばれます）を使用している個人の識別情報を、アプリケーション経由でデータベース・サーバーに渡すことができます。これにより、次のようなことが可能となります。

- アプリケーションでは、ユーザーの証明書を場合によってはデータベース・サーバーに渡して、その妥当性をチェックできます。
- データベース管理者は、特定のアプリケーション経由でデータベース・サーバーへアクセスを許可されるユーザーを規制できます。
- 管理者は、特定のユーザーのかわりに機能しているアプリケーションのアクションを監査できます。

各中間層には、特定のユーザー・セットを認証し、それにかわって特定のロール・セットを使用して動作する機能を委譲できるため、プロキシ認証では中間層サーバーの限定的な信頼モデルがサポートされ、権限が付与されているすべての中間層による問題を回避できます。また、信頼度の高い中間層（会社のファイアウォール内にある中間層など）には、信頼度の低い中間層（ファイアウォールの外部にあるため、より危険にさらされやすい中間層など）よりも多くの権限を付与できます。さらに、中間層とユーザーの識別情報が軽量ユーザー・セッション経由でデータベースに渡されるため、この機能により 3 層システムにおけるユーザー・アクションの監査が簡単になり、アカウンタビリティが向上します。

図 4-1 に、複数層環境での認証を示します。

図 4-1 複数層環境でのプロキシ認証



プロキシ認証では、潜在的に次のユーザーをサポートできます。

- データベース・ユーザー
- エンタープライズ・ユーザー
- データベースに認識されないアプリケーション・ユーザー

中間層のメリットの 1 つは接続プーリングです。接続プーリングにより、複数のユーザーが別個の接続を必要とせずに単一のデータベース・サーバーにアクセスできます。このような環境では、接続の設定と解除をきわめて迅速に行える必要があります。また、軽量セッションが重要になります。この種の軽量セッションにより、各ユーザーはデータベース・パスワードで認証を受けることができ、別個のデータベース接続によるオーバーヘッドは発生せず、実際のユーザーの識別情報は中間層を通じて保たれます。

関連項目：

- 3-7 ページ「3 層のセキュリティを保証するためのプロキシ認証」
- 9-8 ページ「Oracle9i でのプロキシ認証」

シングル・サインオン

通常、イントラネット・ユーザーは、作業中にアクセスする必要のある各サーバーに対して自分自身を認証するために、別個のパスワードを使用するように要求されます。ただし、複数のパスワードを使用することには、いくつかの問題があります。ユーザーが様々なパスワードを記憶していることは困難であり、不適切なパスワードを選択したり、目立つ場所に書き留める傾向があります。管理者は、各サーバーで別個のパスワード・データベースを追跡する必要があります。パスワードが常にネットワーク経由で頻繁に送信され、この事実から生じる潜在的なセキュリティの問題に対応する必要があります。

シングル・サインオン（SSO）により、このような問題はなくなります。ユーザーは、単一のパスワードを使用して様々なサーバーにログインし、アクセス権限が付与されているすべてのサーバーへの認証済みアクセスを取得できます。これにより、複数のパスワードを使用する必要がなくなります。また、システム管理者にとっては、ユーザーのアカウントとパスワードの管理作業が簡素化されます。

次の各項で説明するように、SSO は異なった方法で実装できます。

- サーバー・ベースのシングル・サインオン
- 中間層のシングル・サインオン

サーバー・ベースのシングル・サインオン

集中化されたディレクトリ・サーバーを使用してユーザー、管理およびセキュリティ情報を格納できます。これにより、管理者は一箇所、つまりディレクトリで情報を変更するのみですみます。この集中化により管理コストが削減され、企業の安全性が高まります。

ディレクトリ・サーバーを使用して、ユーザー・アカウント、ユーザー・ロールおよびパスワード情報を一元化できます。データベース・サーバーは、ディレクトリに格納されている情報を使用してユーザーを認証します。認証されたユーザーは、エンタープライズ・ユーザー・セキュリティを使用するように構成されたデータベースにアクセスできます。

中間層のシングル・サインオン

Oracle9*i*AS Single Sign-On Server は Oracle9*i* Infrastructure の一部で、Web ベースのシングル・サインオンと、従来型アプリケーションとの統合を提供します。シングル・サインオンを使用すると、ユーザーは単一の厳密なユーザー名 / パスワード・アカウントをメンテナンスするのみで、全社のすべての Web アプリケーションにアクセスできます。

Oracle9*i*AS Single Sign-On と統合されているアプリケーションは、ユーザー認証プロセスを安全に委譲できます。これによりパスワード・ルール、反復的なログイン失敗に基づくアカウントのロックアウトおよび監査が施行されます。また、ローカル認証の他に、LDAP やデータベース・ユーザー・リポジトリなどの外部リポジトリを使用して、ユーザーを認証する機能も用意されています。

ユーザーがシングル・サインオンを使用してアプリケーションへのアクセスを初めて試みると、サーバーでは次の処理が実行されます。

- ユーザー名とパスワードを使用してユーザーが認証されます。
- クライアントの識別情報がシングル・サインオン対応アプリケーションに渡されます。
- 認証対象のクライアントが、暗号化されたログイン Cookie でマークされます。

以降のログインでは、ログイン Cookie によりユーザーの識別情報がシングル・サインオンを提供するサーバーに渡され、認証がすでに実行済みであることが示されます。

関連項目：

- 9-34 ページ「Oracle Advanced Security でのシングル・サインオンの実装」
- 9-56 ページ「Oracle9i Application Server でのシングル・サインオン」

5

保護ディレクトリの使用と配置

ID、証明書および他の属性など、ユーザー情報の格納と管理をディレクトリに集中化すると、セキュリティ上の多数のメリットが得られます。この章では、ディレクトリを保護する方法と、ディレクトリを使用してアクセスを制御する方法について説明します。

関連項目：

- 第 6 章「エンタープライズ・ユーザーのセキュリティの管理」
- 9-44 ページ「Oracle Internet Directory」

概要

今日の管理者は、複雑なユーザー情報を管理し、絶えず最新で安全な状態を保つ必要があります。これらのタスクはいずれも、企業内でテクノロジの使用が増大し、ユーザーがよく変更されるようになるにつれて重要な課題となります。たとえば、典型的な企業では、各ユーザーが様々なデータベースに複数のアカウントを持っている場合があります。これは、ユーザーにとってはパスワードが多すぎて覚えきれず、管理者にとってはアカウントが多すぎて管理しきれないことを意味します。そのため、ユーザーはパスワードをメモしたり、覚えやすい（したがって他人も推測しやすい）パスワードにしたり、すべてのアカウントに同じパスワードを選択する結果となっています。

管理者は、ユーザーごとに複数のアカウントを管理する必要があります。その結果、ユーザー管理にかなりのリソースを費やしています。ユーザー名、ユーザーのオフィスの所在地と電話番号、システム権限など、複数のアプリケーションで使用する共通の情報は、通常は社内で断片化されており、データの重複、不整合および管理コストの増大を招いています。

また、セキュリティの問題もあります。たとえば、ユーザーが退職したりジョブが変わった場合は、古くなったり使用しなくなったアカウントや権限が誤用されないように、その日のうちに権限を変更する必要があります。ただし、大企業では、ユーザー・アカウントとパスワードが複数のデータベースに分散されており、管理者は適切なセキュリティに必要とされているほど迅速にはすべての変更を行うことができません。

エンタープライズ・ユーザーのセキュリティ管理では、このようなユーザー、管理およびセキュリティの要求に対応する必要があります。最善の方法は、ユーザー関連情報の格納と管理を、Oracle Internet Directory のような LDAP 準拠のディレクトリ・サービスに集中化することです。これにより、従業員のジョブが変わった場合も、管理者は一箇所、つまりディレクトリ内で情報を変更するのみですみます。この集中化により管理コストが削減され、企業の安全性が高まります。

LDAP による共有情報の集中化

今日、ネットワーク情報は複数のシステムに複数のディレクトリ形式で格納されています。インターネット・コンピューティングや新たな E-Business テクノロジによって新たな要件が発生し、すべてのデータとリソースの管理および構成の基盤として機能する共通リポジトリ・インフラストラクチャのニーズが高まっています。このような共通のインフラストラクチャにより、異機種ネットワーク上のリソースを管理および構成するコストが削減されます。

Lightweight Directory Access Protocol（LDAP）テクノロジは、当初はミシガン大学で開発されました。現在では、業界標準として受け入れられており、多様な実装で使用できます。

LDAP 準拠のディレクトリ・サーバーのサポートにより、分散ネットワークの管理と構成を集中化できます。ディレクトリはデータベース・ネットワーク・コンポーネント、ユーザーと会社のポリシー、ユーザー認証とセキュリティに関するすべてのデータの中央リポジトリとして機能できるため、クライアント側とサーバー側でローカライズされていた tnsnames.ora ファイルが置き換えられます。

LDAP 準拠のディレクトリは、多数の強力な情報保護機能を提供できます。

表 5-1 LDAP 準拠のディレクトリのセキュリティ機能

機能	用途
データ整合性	パスワードを含め、データが送信中に変更、削除または再生されないことを保証します。
データ・プライバシ	公開鍵暗号を使用して、データが送信中に不適切に検出されないことを保証します。公開鍵暗号の場合は、メッセージの送信側が受信側の公開鍵でメッセージを暗号化します。配信されたメッセージは、受信側の秘密鍵で復号化されます。
パスワード保護	パスワードはハッシュ値として格納され、侵入者は読むことも復号化することもできないことが保証されます。
パスワード・ポリシーの管理	ディレクトリでユーザーとアカウントのポリシー管理を集中化できます。
認証	ユーザー、ホストおよびクライアントの識別情報の妥当性が適切にチェックされることが保証されます。
認可	ユーザーが権限を付与されている情報のみを読取りまたは更新することが保証されます。

セキュリティ・ディレクトリの統合によるこれらのメリットをすべて得るには、最初にディレクトリ自体が安全かどうかを確認する必要があります。これには、次のことが必要です。

- ユーザーおよび管理者側のディレクトリへの保護接続
- ディレクトリ自体でのアクセス制御

ディレクトリを保護した後は、社内または管理対象となる環境の他のアプリケーションは、これらの機能をすべて活用できます。管理の委譲にディレクトリを使用し、アプリケーションのメタデータへのアクセスを制御できます。

関連項目： 3-6 ページ「Secure Sockets Layer（SSL）プロトコル」

ディレクトリの保護

この項では、ディレクトリ内でアクセスを制御する方法について説明します。

- ユーザーのディレクトリ認証
- ディレクトリでのパスワード保護
- ディレクトリを使用したユーザー認証

ユーザーのディレクトリ認証

認証は、ディレクトリ・サーバーがディレクトリに接続するユーザーの真の識別情報を設定するプロセスです。ユーザー、ホストおよびクライアントの識別情報を検証するために、ディレクトリでは次のように様々な認証オプションを提供できます。

表 5-2 ディレクトリ認証オプション

オプション	説明
匿名認証	ユーザーは、ログイン時に「ユーザー名」フィールドと「パスワード」フィールドをブランクにするのみですみます。各匿名ユーザーは、匿名ユーザー用に指定された権限を行使します。
簡易認証	クライアントは、ネットワークでの送信時に暗号化されない識別名とパスワードを使用し、ディレクトリに対して自己認証を行います。
Secure Sockets Layer（SSL）を使用した認証	信頼できる認証局から発行された証明書を交換して認証できます。
中間層を介する認証	RADIUS サーバーや LDAP セルフ・サービス・サーブレットなどの中間層を介して認証できます。この場合、プロキシ・ユーザーはエンド・ユーザーのかわりにディレクトリ操作を実行します。

関連項目： 第 4 章「データベースに対するユーザーの認証」

ディレクトリでのパスワード保護

Oracle Internet Directory では、パスワードを一方向ハッシュ値として格納することで保護できます。パスワードがハッシュされていれば、悪意を持ったユーザーは読むことも復号化することもできないため、このアプローチはパスワードをクリア・テキストまたは暗号化された値として格納するアプローチよりも安全です。

ディレクトリ・サーバーに対する認証中に、ユーザーはパスワードをクリア・テキストとして入力します。ディレクトリ・サーバーでは、このユーザー・パスワードが指定のハッシング・アルゴリズムを使用してハッシュされてから、格納されているハッシュ済みパスワードと比較して検証されます。ハッシュされたパスワード値が一致すると、サーバーによりユーザーが認証されます。

次のハッシング方式から 1 つを選択できます。

表 5-3 ハッシング・アルゴリズム

ハッシング方式	説明
MD4	デフォルトのハッシング方式。MD4 は、128 ビットのハッシュまたはメッセージ・ダイジェスト値を生成する一方向ハッシュ関数です。
MD5	MD4 の、より複雑な改良版。
SHA	Secure Hash Algorithm の略で、MD5 より長い 160 ビットのハッシュを生成します。MD5 よりも若干遅いですが、メッセージ・ダイジェスト値が大きくなることで、強力な衝突や反転攻撃に対してより強力に保護できます。
UNIX Crypt	UNIX ハッシング・アルゴリズム。
ハッシュなし	パスワードはハッシュされません。

関連項目： 3-4 ページ「ネットワーク送信用のデータの暗号化」

ディレクトリを使用したユーザー認証

認可は、ユーザーが権限を付与されている情報のみを読取りまたは更新することを保証するプロセスです。ディレクトリ・セッション中にディレクトリ操作が試みられると、ディレクトリ・サーバーによりユーザーがその操作の実行に必要な権限を持っているかどうかが確認されます。ユーザーが必要な権限を持っていなければ、ディレクトリ・サーバーでは操作が禁止されます。このメカニズムを通じて、ディレクトリ・サーバーでは、ディレクトリ・データがディレクトリ・ユーザーによる権限のない操作から保護されます。

管理対象の環境で実行中のアプリケーションでは、次のディレクトリ・アクセス制御機能を使用できます。

表 5-4 ディレクトリ・アクセス制御機能

機能	説明
模範的なアクセス制御	サービス・プロバイダは、個々のオブジェクトごとにポリシーを記述するかわりに、ディレクトリ・オブジェクトのコレクションについてアクセス制御リスト（ACL）を指定できます。この機能により、特に多数のオブジェクトが同一または類似のポリシーにより制御される大規模ディレクトリでは、アクセス制御の管理が簡素化されます。
階層形式のアクセス制御管理モデル	サービス・プロバイダは、ディレクトリ管理をサブスクライバに委譲できます。サブスクライバは、必要に応じてさらに委譲できます。
委譲されたドメインに関する管理のオーバーライド制御	サービス・プロバイダは、意図しないアカウントのロックアウトや不測のセキュリティ・リスクについて、診断を実行してリカバリできます。
アクセス制御エンティティの動的評価	サブツリー管理者は、サブジェクトとオブジェクトの両方を、そのネームスペースおよびディレクトリ内の他のオブジェクトとの対応付けに基づいて識別できます。たとえば、あるサブスクライバ・サブツリーの管理者は、ユーザーの給与属性の更新をそのユーザーの上司にのみ許可できます。別のサブスクライバ・サブツリーの管理者は、給与属性に関して異なるポリシーを設定して施行できます。

ディレクトリ・ベースのアプリケーション・セキュリティ

エンタープライズ環境や管理対象となる環境では、LDAP 準拠のディレクトリの機能を使用して、アプリケーションのメタデータ、つまりアプリケーションの動作やアクセスできるユーザーを制御する情報へのアクセスを制御できます。

ディレクトリのアクセス制御ポリシーは LDAP 属性として格納されるため、それを変更できるユーザーを制御するメタポリシーを設定できます。これにより、グローバル管理者は、管理対象環境にあるアプリケーションの管理者など、特定のサブツリーの管理者に権限を割り当てることができます。同様に、部門の管理者に、その部門内のアプリケーションのメタデータへのアクセスを委譲することもできます。これにより、部門管理者はその部門のアプリケーションへのアクセスを制御できるようになります。このようにして、アクセス制御をユーザー・レベルと管理者レベルという 2 つのレベルで実装できます。

この項の内容は次のとおりです。

ユーザーの認可

ディレクトリにはアクセス制御ポリシーが格納され、それを外部アプリケーションが読み取って施行します。ユーザーがアプリケーションを使用して操作を試みると、アプリケーションではユーザーが操作を実行するための適正な認可を持っているかどうかが検証されます。

管理者の認可

ディレクトリは、すべてのアプリケーション固有のアクセス制御ポリシーに関する信頼度の高い管理ポイントとして機能します。特定のアプリケーションのアクセス制御ポリシーを管理できるユーザーを制御するために、これらのアプリケーションについてディレクトリ・レベルでアクセス制御ポリシーを設定できます。これにより、ユーザーがアプリケーション固有のアクセス制御ポリシーの変更を試みると、ディレクトリではユーザーがその変更を行うための適正な認可を持っているかどうかが検証されます。

図 5-1 に、管理対象環境におけるディレクトリのアクセス制御とアプリケーション固有のアクセス制御メカニズムの関係を示します。

図 5-1 ディレクトリ・ベースのアプリケーション・セキュリティのための管理の委譲

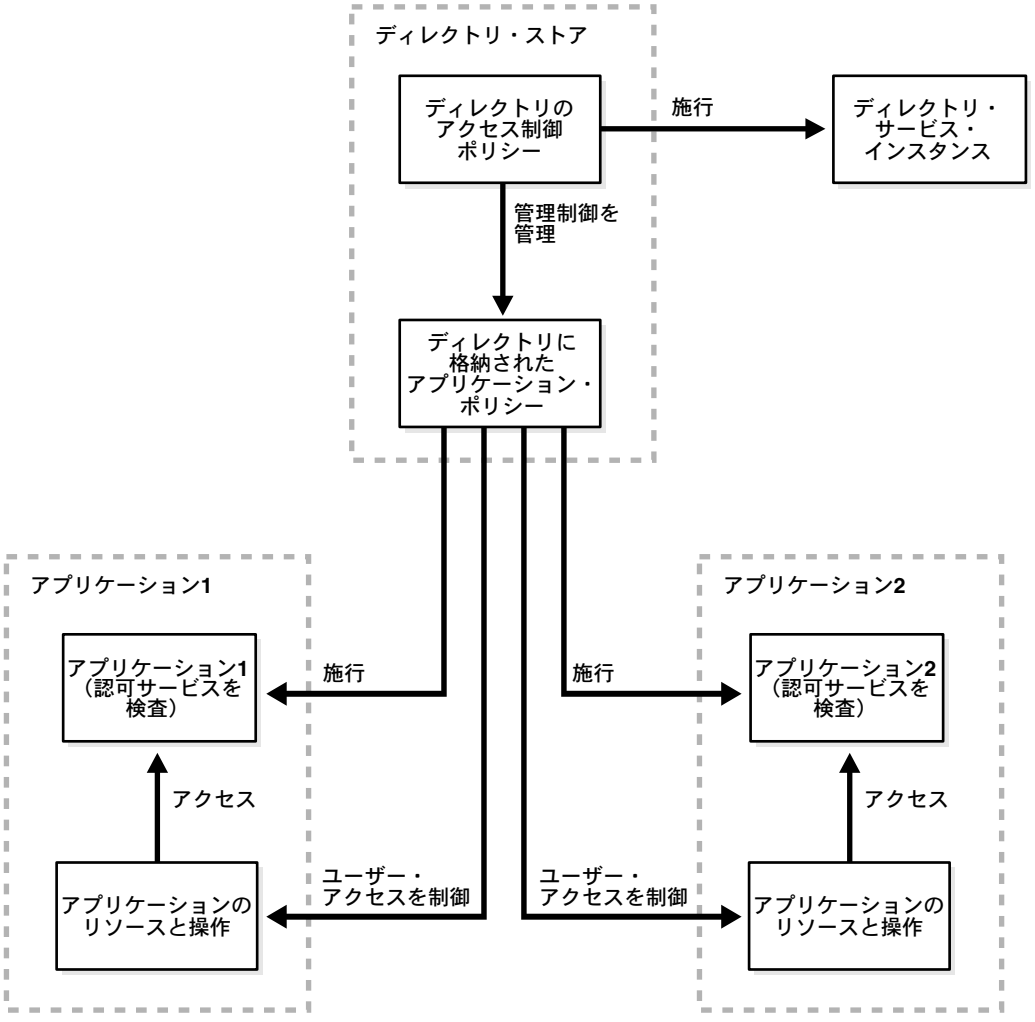


図 5-2 に、各種ドメインと、ディレクトリ内で対応付けられているロールを示します。

図 5-2 管理対象環境におけるディレクトリのドメインとロール

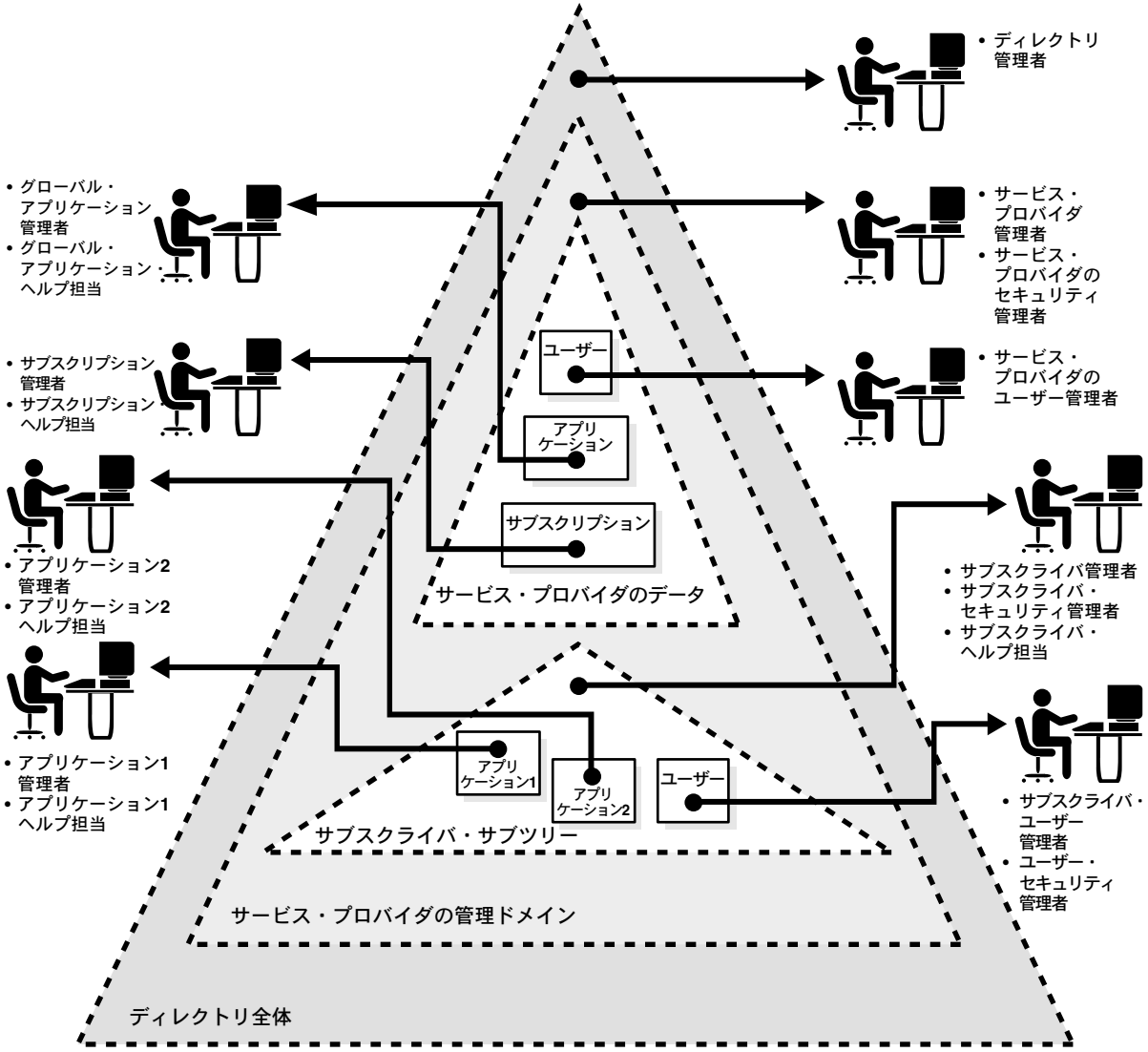


図 5-2 では、それぞれの三角形はディレクトリ情報ツリー（DIT）の一部を表しています。

- 最も外側の三角形は、ディレクトリ全体を表します。ディレクトリ管理者は、ディレクトリ全体にまたがる権限を持っています。
- 最も外側の三角形のすぐ内側には、もう 1 つ三角形があり、これはサービス・プロバイダの管理ドメインを表します。この部分では、新規エントリを追加する権限がサービス・プロバイダの管理者に委譲されます。
- サービス・プロバイダの管理ドメインの内側では、ディレクトリ情報の所有権に基づいて権限をさらに委譲できます。たとえば、情報が特定のサブスクライバに固有のものか、サービス・プロバイダに対してグローバルであるかに応じて委譲できます。

図 5-2 は、ディレクトリ内で表される単一のサブスクライバのみを示しています。実際には複数のサブスクライバがあり、それぞれが他のサブスクライバからの保護を必要とする独自ドメインを持っています。このモデルの保護ドメインの一部を次に示します。

- ディレクトリ全体
- サービス・プロバイダの管理ドメイン
- サービス・プロバイダ固有のディレクトリ情報ツリー
- サブスクライバ固有のサブツリー
- ディレクトリ内のアプリケーション固有のフットプリント
- ユーザー固有の情報

ディレクトリでの管理ロール

前項で示した保護ドメインは、3 タイプのロールでサポートされます。これらのロールにより、サービス・プロバイダやサブスクライバは必要に応じてアクセス制御をカスタマイズできます。

表 5-5 ディレクトリでの管理ロール

ロール	機能
グローバル管理ロール	このタイプのロールには、ディレクトリ全体にまたがるアクティビティを実行する権利があります。
サブスクライバ固有のロール	このタイプのロールは、サブスクライバ固有のディレクトリ・ツリーに制限されています。
アプリケーション固有のロール	ディレクトリ対応アプリケーションを管理する場合は、ディレクトリ内でアプリケーション固有のすべてのロールとなる必要はありません。ただし、ディレクトリのフットプリントに直接影響するロールとなる場合、アプリケーションでは前述の委譲モデルに関するリコメンデーションに従うことをお薦めします。これにより、アプリケーションではディレクトリ固有の権限をユーザーに付与するときに、ディレクトリ・ベースの委譲モデルを活用できます。

6

エンタープライズ・ユーザーのセキュリティの管理

この章では、エンタープライズ・ユーザー管理機能の構成要素について説明します。

- 概要
- エンタープライズ権限の管理
- 共有スキーマ
- パスワード認証を受けたエンタープライズ・ユーザー
- エンタープライズ・ロール
- 複数層の認証および認可
- シングル・サインオン

関連項目：

- 第 5 章「保護ディレクトリの使用と配置」
- 9-44 ページ「Oracle Internet Directory」

概要

ほとんどの組織は、E-Business であるかどうかを問わずユーザー管理の面で困難な障害に直面しています。通常、組織内のユーザーが持っているユーザー・アカウントが多すぎるために、Web ベースのセルフ・サービス・アプリケーションの成長による問題が悪化しています。ユーザーは隔週で新しいユーザー・アカウントとパスワードを覚えることになります。データ・アクセスとアカウンタビリティをユーザー別にしようと考える組織は、ユーザーがアクセスする各データベースでユーザーを管理するという悪夢を望んでいるわけではありません。

この問題は、Web が直面する E-Business アプリケーションの場合は複雑になります。ミッション・クリティカルなシステムをパートナや顧客に公開している組織は、パートナがアクセスする各データベース内でパートナごとにアカウントを作成しようとは考えませんが、各パートナの権限とアカウンタビリティに対する必要性は大きいものです。このようなニーズを満たすには、強力なエンタープライズ・ユーザー管理ツールが必要になります。

エンタープライズ権限の管理

3 層システムを含めて、あらゆる分散システムが本来抱えている問題は、共通のアプリケーション情報が通常は社内で断片化されており、データの重複、不整合および管理コストの増大を招いていることです。ディレクトリを参照する Oracle 製品やサード・パーティ製品は増える一方ですが、これはエンタープライズ情報を社内の複数のシステムで使用可能にするために最適のメカニズムであるためです。また、ディレクトリにより、組織は仮想プライベート・ネットワーク経由などのインターネット経由で、特定タイプの情報にアクセスしたり共有できます。ディレクトリの使用は、最近の Lightweight Directory Access Protocol（LDAP）の成長によって加速されてきました。

ディレクトリへの格納について共通に示される特定タイプのエンタープライズ情報が、権限およびアクセス制御情報です。ロールで表されるユーザー権限と、オブジェクトにアクセスできるユーザーが指定されているアクセス制御リスト（ACL）で表されるオブジェクト制約を、ディレクトリに格納できます。

特定ユーザーの権限やアクセス属性を指定するディレクトリ情報は、権限なしで変更されると、ユーザーに対して権限やアクセス権が無認可で付与または拒否される恐れがあるため機密です。企業内のこの情報をメンテナンスするディレクトリでは、ディレクトリ内でメンテナンスされている権限やアクセス情報を変更できるのが、権限を持つシステム・セキュリティ管理者のみであることを保証する必要があります。

関連項目：

- 9-48 ページ「Oracle Internet Directory によるエンタープライズ・ユーザー管理の編成方法」
- 9-35 ページ「Oracle Advanced Security のエンタープライズ・ユーザー・セキュリティ機能」

共有スキーマ

共有スキーマは、識別情報が中央の LDAP リポジトリでメンテナンスされている非スキーマ依存のデータベース・ユーザーです。非スキーマ依存ユーザーがデータベースに接続すると、データベースはディレクトリに問い合せて、そのユーザーが登録されているかどうかを判断し、登録されている場合はそのユーザーをマップする必要のあるデータベース・スキーマと、そのユーザーが取得する必要のあるロールを判断します。

たとえば、あるアプリケーションのユーザー数が 500 人で、それぞれが社内の複数のデータベース・サーバー上のデータにアクセスする必要があるとします。Oracle9*i* では、各データベース上で 500 の異なるユーザー・アカウントをメンテナンスするかわりに、システム管理者が各データベース上で適切な権限を指定した単一の共有スキーマ（HR アプリケーションの場合は HRAPPUSER など）を作成してから、Oracle Internet Directory 内で 500 のエンタープライズ・ユーザーを作成できます。これらのユーザーが特定のデータベースに接続すると、そのデータベース上の適切なスキーマ（HRAPPUSER など）にマップされ、スキーマに対応付けられている権限と、ディレクトリ内で付与されたロールに対応付けられている追加の権限を継承します。これらのユーザーは共通スキーマを共有しますが、個々の非スキーマ依存ユーザーの識別情報はデータベースによりセッションと対応付けられ、アクセス制御や監査の目的で使用されます。LDAP 内で作成されたこれらのユーザー・アカウントは、複数のアプリケーション内でも使用できます。

共有スキーマ・ユーザー機能には、多数のメリットがあります。社内のユーザー管理に関連する管理上の負荷が軽減され、従来よりはるかに大規模なユーザー・コミュニティを効率的に管理できます。また、中間層でもディレクトリ内のユーザー識別情報と権限の管理がサポートされていれば、複数層システムの層にまたがるユーザー・アカウントと権限の管理を統合するメカニズムを提供できます。このようなシステムでは、新規のユーザーとその権限をディレクトリに登録してから、アクセスを必要とする社内の中間層とデータベースへの適切なアクセス権を付与できます。将来は、新規ユーザーが Web サーバーに自己登録でき、Web サーバーでこれらのユーザーのエントリをディレクトリに作成して、関連する該当データベース内の情報へのアクセス権を付与できるような、3 層システム（Web ストアフロントなど）の構築が可能になります。

関連項目：

- 9-36 ページ「Oracle Advanced Security の共有スキーマ」
- 9-48 ページ「Oracle Internet Directory での共有スキーマ」

パスワード認証を受けたエンタープライズ・ユーザー

処理のオーバーヘッドと管理に伴う負荷を軽減するために、エンタープライズ・ユーザーにはパスワード・ベースの認証を使用することをお薦めします。また、エンタープライズ・ユーザーは、必要に応じて単一のエンタープライズ・ユーザー名とパスワードを使用し、複数のデータベースに接続できるようにする必要があります。この機能は、複数のアプリケーションにアクセスする大規模なユーザー・コミュニティに特に役立ちます。

関連項目： 9-35 ページ「Oracle Advanced Security のエンタープライズ・ユーザー・セキュリティ機能」

エンタープライズ・ロール

ユーザー関連情報の管理を LDAP 準拠のディレクトリ・サービスに集中化していれば、エンタープライズ・ロールを格納して管理し、データベースに対するエンタープライズ・ユーザーのアクセス権限を決定できます。エンタープライズ・ロールは、複数のデータベース上のグローバル・ロールを含むディレクトリ構造であり、エンタープライズ・ユーザーに付与できます。

複数層の認証および認可

トランザクション処理モニターのように大規模な中間層を使用するアプリケーションでは、中間層に接続しているクライアントの識別情報を保てることが重要になります。クライアントの識別情報と権限は、すべての層で保持して監査する必要があります。

シングル・サインオン

社内イントラネットの典型的なユーザーは、多数のクライアント・アプリケーションへのアクセス権を持っています。この種のユーザーは、アクセスするアプリケーションごとにユーザー名とパスワードを覚える必要があります。ユーザーにとって、ユーザー名とパスワードの多数の組合せを覚えて、異なるアプリケーションにアクセスするたびに認証を受けるための再入力をする必要があるのは、非効率的です。このため、ユーザーは、アクセス権が付与されているすべてのアプリケーションについて、ユーザー名とパスワードを 1 つのみ保持する傾向があります。通常、このようなフレームワーク内ではハッカーが多数の攻撃ポイントを選択できるため、適切なセキュリティとしては望ましくありません。

アプリケーションにとっては、このようなフレームワークでは各ユーザーのユーザー名とパスワード・ストアをメンテナンスする必要があります。このため、ユーザーのロールと権限（全社単位で付与されている場合があります）に関して転送可能な情報が欠落し、パスワード・ストアが冗長になり、アプリケーション間の通信がなくなります。

シングル・サインオン・テクノロジを使用すると、ユーザーは一意のユーザー名とパスワードを一度入力するのみですみます。入力したユーザー名とパスワードは、その後は多数の異なるクライアント・アプリケーションに対してユーザーを自動的に認証するために使用され、ユーザー名やパスワードの再入力は不要になります。ユーザーのロールと権限は、アクセス先となるアプリケーションで適切な権限が付与されるように、アプリケーション間で伝播されます。

関連項目： 9-34 ページ「Oracle Advanced Security でのシングル・サインオンの実装」

7

監査によるシステム・セキュリティの監視

監査は、セキュリティ・ポリシーの有効性を監視する手段であり、システム・セキュリティの重要な側面です。この章の内容は次のとおりです。

概要

セキュリティ・ポリシーでは、ユーザーがアクションの責任を明確にできるように、システム・アクティビティのレコードをメンテナンスする必要があります。監査により、権限を持たないユーザーによる、他の方法では防止できない動作を阻止できます。特に、権限を持つシステム・ユーザーがその権限を悪用しないことを保証する場合に役立ちます。

ファイングレイン監査は、ユーザーによるデータ・アクセス権限の悪用の「早期警報システム」や、データベース自体の侵入検出システムとして役立てることができます。

基本的な監査要件

この項では、セキュリティ監視の基本的な要件について説明します。

- 確実で包括的な監査
- 効果的な監査
- カスタマイズ可能な監査

確実で包括的な監査

強力な監査機能により、データベース・アクティビティを文別、システム権限の使用別、オブジェクト別またはユーザー別に監査できます。アクティビティは、データベースに対するすべてのユーザー接続全般として、または表を作成する特定のユーザーに限定して監査できます。また、成功した操作のみ、または失敗した操作のみを監査することもできます。たとえば、失敗した SELECT 文を監査すると、参照する権限が付与されていないデータを「探っている」ユーザーを捕捉できます。監査証跡レコードは、Oracle9*i* の表に格納したり、管理しやすいように、選択したオペレーティング・システム上のオペレーティング・システム監査証跡と組み合せることができます。Oracle9*i* の表に格納された監査証跡レコードは、非定型問合せまたは適切なアプリケーションやツールを通じて参照できます。監査証跡を個別に格納することによって、企業は、権限を付与されているユーザーによるほとんどのアクションを監査できます。

> **関連項目：** `audit_sys_operations` パラメータについては、『Oracle9*i* データベース管理者ガイド』を参照してください。

効果的な監査

監査は効果的に実装する必要があります。つまり、SQL 文は実行と監査のための解析を、別々にではなく一度に行います。また、監査はサーバー自体の内部に実装され、別個のアドオン・サーバーに実装されないようにします。後者の場合は、実行される文からリモートになることがあります（そのため、ネットワーク・オーバーヘッドが発生します）。このような監査オプションの最小単位と適用範囲により、一般的な監査に多く発生するパフォーマンス上のオーバーヘッドを発生させずに、特定のデータベース・アクティビティを記録して監視できます。また、必要なオプションのみを設定することで、すべての文を途中でキャッチしてログに記録してから、フィルタを適用して対象を取り出すような、すべてをキャッチしては放出する監査方法を回避できます。

カスタマイズ可能な監査

監査レコードには自動的に組み込まれないカスタマイズされた情報を記録するために、トリガーを使用して監査条件と監査レコードの内容をさらにカスタマイズできます。データベース・トリガーは、PL/SQL または Java の文のユーザー定義セットであり、コンパイル済みの形式で格納されます。ユーザーはストアド・プロシージャを明示的に実行しますが、データベース・トリガーは事前に指定したイベントに基づいてデータベース・サーバー内で自動的に実行（または「起動」）されます。トリガーは、INSERT、UPDATE または DELETE 文の前または後に実行するように定義され、その操作が特定の表に対して実行されると、トリガーが自動的に起動します。たとえば、EMP 表にトリガーを定義して、従業員の昇給が 10% を超えた場合に、SALARY の変更前後の値などの指定した情報を含めた監査レコードを生成できます。

関連項目： 9-4 ページ「監査」

拡張可能なファイングレイン監査

ファイングレイン監査により、組織は正当なデータ・アクセス権の悪用を管理者に警告できるように、特定の監査ポリシーを定義できます。

標準的な監査では、権限とオブジェクトを監視し、トリガーを定義して、INSERT、UPDATE および DELETE などの DML 操作を監視できます。これに対して、SELECT 文の監視は、内容に基づいてデータ・アクセスを監視できるファイングレイン監査により容易になります。この方法では、監査条件を指定可能で、環境と問合せ結果に関して、より詳細な情報を取得できます。この追加情報は、監査対象イベントを再構成し、アクセス権の違反があるかどうかを判断するときに役立ちます。また、ユーザーはデータベース監査をバイパスできなくなります。

関連項目： 9-19 ページ「ファイングレイン監査」

複数層アプリケーション環境での監査

多くの 3 層アプリケーションでは、ユーザーが中間層に対して認証されてから、トランザクション処理モニターまたはアプリケーション・サーバーが上位権限を持つユーザーで接続し、すべてのユーザーにかわってすべてのアクティビティを実行します。ただし、中間層で実際のクライアントの識別情報を保持し、中間層を介して「最小権限」を施行できることが重要です。また、中間層によりユーザーのかわりに実行されたアクションを監査する必要があります。ユーザーが中間層経由で接続されているか、データベース・サーバーに直接接続されているかを問わず、ユーザー・アクティビティを監査することでユーザーのアカウンタビリティが強化され、中間層システム全体のセキュリティが強化されます。

関連項目： 9-20 ページ「Oracle による 3 層アプリケーションの監査」

8

セキュリティに対する公開鍵インフラストラクチャによるアプローチ

公開鍵インフラストラクチャ（PKI）は、安全な情報交換を確立する一連のポリシーと手順です。この章では、PKI の構成要素と、PKI がセキュリティ実装に対する業界標準アプローチとなった理由を説明します。

概要

この項では、公開鍵インフラストラクチャ（PKI）の基本概念について説明します。

PKI のセキュリティ機能

PKI は、セキュリティの根幹を提供することにより保護 E-Commerce やインターネットのセキュリティ基礎となっています。

認証	ユーザーとマシンの識別情報を検証する認証の重要性は、組織がインターネットへの門戸を開いている場合に決定的になります。厳密認証メカニズムにより、ユーザーとマシンが主張どおりのエンティティであることが保証されます。
暗号化	暗号化アルゴリズムは、通信を保護し、コンピュータ間で送信されるデータのプライバシを保証するために使用されます。
否認防止	PKI を使用すると、デジタル署名を通じて否認防止を提供できます。これにより、特定のユーザーが特定の時刻に特定の操作を実行したことが証明されます。

これらの要素の組合せにより、E-Commerce を配置する安全で切れ目のない環境と、社内イントラネットからインターネット・ベースの E-Business アプリケーションに至るまで、すべてのタイプの電子取引を作成できる、信頼度の高い環境が提供されます。

PKI の構成要素

公開鍵インフラストラクチャの主な構成要素は次のとおりです。

デジタル証明書	信頼できるサード・パーティにより発行される、ユーザーとマシンを識別するためのデジタル「識別情報」。Wallet またはディレクトリに安全に格納できます。
公開鍵と秘密鍵	秘密鍵および数学的に関連付けられた公開鍵に基づいて、安全な通信のための PKI の基礎を形成します。
Secure Sockets Layer（SSL）	インターネット標準の保護プロトコル。
認証局（CA）	デジタル証明書の信頼度の高い、独立系プロバイダです。

その他、PKI の配置を可能にする重要な要素には、証明書とキーのセキュアな格納、証明書を要求する管理ツール、Wallet へのアクセスとユーザーの管理、証明書の中央リポジトリとして機能するディレクトリ・サービスなどがあります。

PKI アプローチのメリット

セキュリティに対する PKI アプローチは、他のすべてのセキュリティ・テクノロジにかわるものではなく、セキュリティ達成のための代替手段です。PKI は、次のメリットにより、インターネットと E-Commerce アプリケーションの保護に関して業界標準となってきています。

- PKI は業界標準に準拠したテクノロジです。
- 信頼できるプロバイダを選択できます。
- 高度な拡張性を備えています。ユーザーは自分の証明書をメンテナンスし、認証局はクライアントとサーバー間のデータ交換にのみ関与します。つまり、サード・パーティの認証サーバーをオンラインにする必要はありません。したがって、PKI を使用してサポートできるユーザー数にも制限はありません。
- PKI では信頼関係を委譲できます。つまり、認識され信頼できる認証局から証明書を取得したユーザーは、そのサーバーに初めて接続するときにサーバーに対して自己認証でき、事前にシステムに登録する必要がありません。
- PKI は明らかなシングル・サインオン・サービスではありませんが、シングル・サインオンが可能になるような方法で実装できます。

公開鍵暗号と公開鍵 / 秘密鍵のペア

公開鍵暗号では、安全な方法による通信を希望するエンティティは、特定のセキュリティ資格証明を持つことになります。これはセキュリティ資格証明のコレクションであり、Wallet に格納されます。セキュリティ資格証明は、公開鍵と秘密鍵のペア、「ユーザー」証明書、証明連鎖および「信頼できる」証明書で構成されています。

暗号化されたデータのセキュリティは、通常、通信の送信側と受信側の間で共有される秘密鍵の存在に依存します。このような秘密鍵を提供して配布する作業は、キー管理と呼ばれます。マルチユーザー環境では、秘密鍵を安全に配布するのが困難な場合があり、この問題を解決するために公開鍵暗号が発明されました。

公開鍵暗号は、保護秘密鍵のペアに基づいています。各鍵（ペアの一方）によって暗号化された情報を復号化できるのは、対応する鍵（ペアの他方）のみです。鍵のペアは次のとおりです。

秘密鍵	所有者のみが知っています。
公開鍵	広範囲に配布されますが、所有者にのみ対応付けられています。

暗号化鍵のペアを使用して安全な暗号化チャネルを設定すると、メッセージのプライバシを保証し、メッセージ送信者の信頼度の妥当性をチェックできます。また、鍵のペアのうち秘密鍵の構成要素の整合性を損なわずに、サーバー上または中央ディレクトリ内で公開鍵を広範囲に配布できるという重要なメリットもあります。これにより、公開鍵をシステム内で通信相手ごとに送信する必要がなくなります。

公開鍵システムに参加する各エンティティは、公開鍵と秘密鍵のペアを持つ必要があります。エンティティの公開鍵は、ユーザーの証明書として認証局（CA）から発行されます。これにより、保護情報の送信を希望する他のエンティティは、受信側エンティティの公開鍵を使用して情報を暗号化できます。公開鍵のもう 1 つの用途は、通信の受信側エンティティが送信側の組織の所属を検査することです。

保護証明書 : PKI における証明書ベースの認証

ユーザー ID の設定は分散環境では主な問題ですが、権限をユーザー別に制限するという点ではあまり信頼できません。最も一般的な認証方式として使用されているのはパスワードですが、特に機密性の高いデータの場合は、より厳密な認証サービスを採用する必要があります。この項の内容は次のとおりです。

証明書と認証局

中央の機能にネットワークのすべてのメンバー（サーバーに対してクライアント、サーバーに対してサーバー、クライアントとサーバーの両方に対してユーザー）を認証させるのは、ネットワーク上のノードが識別情報を偽装する脅威に効果的に対応する方法の 1 つです。この方法には、証明書と認証局が関係します。

認証局

認証局（CA）は、ユーザー、データベース、管理者、クライアント、サーバーなど、他のエンティティが主張どおりの存在であることを証明する、信頼できるサード・パーティです。認証局は、ユーザーを証明するときに、そのユーザーの識別情報を検証し、認証局の秘密鍵を使用して署名した証明書を発行します。認証局は独自の証明書と公開鍵を持ち、それが安全にメンテナンスされる秘密鍵とともに発行されます。サーバーとクライアントでは、CA のルート証明書を使用して、認証局が作成した署名を検証します。認証局は証明書サービスを行う外部の会社であったり、企業の MIS 部門などの内部組織である場合があります。

証明書

証明書は、ネットワークへのアクセスを求めるユーザーやデバイスの識別情報を証明する、電子的なパスポートのようなものです。この証明書は、そのエンティティの情報が正しいこと、および公開鍵がそのエンティティに実際に属していることを保証します。証明書は、エンティティの公開鍵が、信頼されている機関（認証局）によって署名されたときに有効となります。証明書の内容は、次のとおりです。

- 証明書のユーザー名
- 有効期限
- 認証局が証明書に割り当てた一意のシリアル番号

- ユーザーの公開鍵
- 証明書に関連する権利と使用についての情報
- 証明書を発行した認証局の名称
- 認証局による署名
- 証明書への署名に使用されたアルゴリズムを識別するアルゴリズム ID

信頼できる証明書はルート鍵証明書とも呼ばれ、通常は証明書の発行に関して信頼されているサード・パーティ・エンティティに属しています。これは安全な方法で取得され、自動署名があるため、運用上、アクセスするたびに信頼性を検査する必要はありません。クライアントまたはサーバーは、エンティティの証明書が既知の信頼できる認証局から発行されたかどうかを検証し、そのエンティティが主張どおりの存在であるかどうかを検査できます。

一般的に、信頼されている認証局によってユーザーの証明書が発行されます。Oracle にはデフォルトで複数の信頼できる証明書が用意されているため、ユーザーが独自にインストールする必要はありません。これらの信頼できる証明書により、サーバーは Wallet に信頼できる証明書のみが格納されているクライアントに対して SSL 認証を実行できます。

クライアントとサーバーは、これらの証明書を使用し、公開鍵暗号を使用して、SSL などの保護サービスにアクセスします。Wallet は、オープン後は位置やタイプを透過的に格納する機能も提供しています。

PKI で使用される認証方式

PKI で一般的に使用されている認証方式は、次のとおりです。

- Secure Sockets Layer 認証と X.509v3 デジタル証明書
- Entrust/PKI 認証

Secure Sockets Layer 認証と X.509v3 デジタル証明書

Secure Sockets Layer（SSL）は、公開鍵インフラストラクチャで認証、データ暗号化およびデータ整合性を提供する業界標準プロトコルです。SSL はインターネット上で広く採用され、ユーザーに確立されたデジタル証明書を提供し、メッセージの盗聴や改ざん、偽造を防止しています。

SSL は、信頼できる認証局によって検証されている証明書の交換を通じて認証を提供します。SSL では、デジタル証明書（X.509 v3）と公開鍵と秘密鍵のペアを使用してユーザーとシステムが認証されます。

最も普及している公開鍵証明書は X.509 フォーマットに準拠しており、X.509 バージョン 3 証明書は現行の業界標準フォーマットとなっています。公開鍵インフラストラクチャは X.509 証明書に依存しており、これはデジタル証明書、または公開鍵認証の場合は公開鍵証明書とも呼ばれます。

X.509v3 デジタル証明書の内容は、次のとおりです。

- 所有者を一意に識別する、証明書所有者の識別名（DN）
- 認証局を一意に識別する、証明書発行者の識別名
- 証明書所有者の公開鍵
- 発行者による署名
- 証明書の有効期間
- 証明書のシリアル番号

SSL プロトコルはユーザーの信頼を得ており、おそらく現在最も普及し認知されている暗号化プロトコルです。

関連項目： 9-31 ページ「Oracle Advanced Security での Secure Sockets Layer（SSL）認証」

Entrust/PKI 認証

Entrust Technologies 社は、Entrust/PKI ソフトウェアを通じて、公開鍵インフラストラクチャ・ソリューションの業界大手プロバイダとなっています。Entrust/PKI には、ユーザーの PKI 証明書を保護する Entrust Profile や、Entrust Technologies 社の認証局製品である Entrust Authority など、多数の製品があります。オラクル社は、Entrust/PKI と統合できるように自社の SSL 実装を変更しています。

Entrust/PKI は、関連するすべての PKI 規格に全面的に準拠しているわけではないため注意してください。

関連項目： 9-31 ページ「Oracle Advanced Security での Entrust/PKI のサポート」

PKI での保護証明書の格納

多くの組織は、ユーザーと認可を LDAP 準拠のディレクトリで別々に管理しています。また、証明書もディレクトリに安全に格納し、ユーザー管理機能を強化できます。

PKI を使用すると、デジタル証明書などの保護証明書を「Wallet」と呼ばれるコンテナに格納できます。Wallet は、SSL に必要なキー、証明書および信頼できる証明書など、認証データの管理に使用される透過的データベースです。Wallet は LDAP 準拠のディレクトリに格納できます。この実装により、ユーザーの集中管理が可能になります。

セキュリティ管理者は、Oracle Wallet Manager などのツールを使用して、サーバー側でセキュリティ資格証明を管理します。Wallet 所有者は、Wallet を使用してクライアント側でセキュリティ資格証明を管理します。

Public Key Certificate Standard #12（PKCS#12）は、保護証明書の格納に関する規格です。

関連項目：

- 5-3 ページ「LDAP による共有情報の集中化」
- 9-38 ページ「Oracle の公開鍵インフラストラクチャ・ベースの認証のコンポーネント」

PKI を使用したシングル・サインオン

シングル・サインオンにより、ユーザーは単一のパスワードで複数のアカウントおよびアプリケーションにアクセスできます。この機能により、ユーザーにとっては複数のパスワードが不要になり、システム管理者にとってはユーザー・アカウントとパスワードの管理が簡素化されます。シングル・サインオンにより、ユーザーは利便性が高まり、セキュリティ管理者は集中管理が可能になります。

すべてのクライアント、アプリケーション・サーバーおよびデータベース・サーバーは相互に自己認証できるため、PKI はネットワークに重要なセキュリティ・インフラストラクチャをもたらします。

関連項目： 9-34 ページ「Oracle Advanced Security でのシングル・サインオンの実装」

PKI を使用したネットワーク・セキュリティ

PKI の実装により、ネットワーク認証が集中化されるのみでなく、ネットワークの通信量を暗号化し、整合性をチェックできます。Secure Sockets Layer は強固な、業界標準に準拠した暗号化技術およびデータ整合性アルゴリズムを提供します。

関連項目：

- 3-4 ページ「ネットワーク送信用のデータの暗号化」
- 9-37 ページ「Oracle Advanced Security の PKI 実装」

第 III 部

Oracle9*i* のセキュリティ製品

第 III 部では、データ・セキュリティ要件を満たすことのできる、Oracle セキュリティ製品パッケージについて説明します。

9

Oracle9*i* のセキュリティ製品および機能

この章では、最新のセキュリティ・テクノロジを使用してデータを保護できる Oracle 製品および特殊機能を紹介します。

- Oracle9i Standard Edition
- Oracle9i Enterprise Edition
- Oracle Advanced Security
- Oracle Label Security
- Oracle Internet Directory
- Oracle Net Services
- Oracle9i Application Server

Oracle9*i* Standard Edition

データベース・セキュリティにより、データベースとそこに格納されたオブジェクトに対するユーザー・アクションを許可または拒否できます。Oracle では、スキーマとセキュリティ・ドメインを使用して、データへのアクセスを制御し、各種データベース・リソースの使用を制限しています。この項では、Oracle9*i* データベース固有の多数のセキュリティ・メカニズムについて説明します。

- 整合性
- Oracle9i における認証とアクセス制御
- 権限
- ロール
- 監査
- ビュー、ストアド・プログラム・ユニット、トリガー
- データ暗号化
- 高可用性
- Oracle9i でのプロキシ認証

これらの機能の詳細は、Oracle9*i* のマニュアルを参照してください。

関連項目：

- 『Oracle9*i* データベース概要』
- 『Oracle9*i* データベース管理者ガイド』

整合性

Oracle9*i* には、データベースの整合性を保証し、トランザクションの並行性とシリアル化の可能性を提供し、データの破損を防止するために、多数のメカニズムが用意されています。強制的なアクセス制御を施行するアクセス制御メカニズムは、権限を持たないユーザーによるデータの変更や削除を防止する目的でも使用されます。

データ整合性

Oracle9*i* は、ISO/ANSI SQL 規格で定義されている宣言エンティティおよび参照整合性制約を使用して、データ整合性を提供します。整合性ルールは表定義の一部として宣言で指定され、トランザクションにより表の行が更新、挿入または削除されるたびに、データベース・サーバーによりチェックされます。このようなルールをサーバーで定義して施行することで、すべてのアプリケーションで一貫して同じルールが確実に適用され、一元的にメンテナンスできることが保証されます。また、サーバー側でルールを施行すると、アプリケーション内でプログラムにより施行する場合に比べてパフォーマンス上のメリットが得られます。

ストアド・プロシージャとトリガーを使用すると、さらに複雑なビジネス・ルールを施行できます。ただし、通常、このようなメカニズムは、エンティティ、参照またはトランザクションの整合性の施行には使用されません。

また、データベースの整合性メカニズムにより、トランザクションのすべてのステップが完全な 1 単位としてコミットされることが保証され、すべての部分がコミットされるか、ロールバックされるかのどちらか一方になります（トランザクションの整合性）。

エンティティの整合性の施行

エンティティの整合性を施行することで、表の各行が主キー列の非 NULL 値で一意に識別されることが保証されます。エンティティ整合性の例として、EMP 表の各従業員番号が一意であることの保証などがあります。

参照整合性

参照整合性制約は、表の行相互の依存性と関係を施行するために使用されます。たとえば、これは EMP 表の従業員の部門番号（外部キー）が DEPT 表に指定された有効な部門（主キー）と一致する必要がある場合に発生します。主キー / 外部キーの関係は、表作成の一部として定義されます。

関連項目： 2-12 ページ「データベースの整合性メカニズム」

Oracle9*i* における認証とアクセス制御

Oracle9*i* には、ユーザー、ホストまたはクライアントの識別情報が適切に認識されるように、ユーザー認証が用意されています。データベースにアクセスするには、ユーザーはそのデータベースの有効なユーザー名と関連パスワードを入力する必要があります。これにより、権限を持たないユーザーによる使用が防止されます。さらに、Oracle9*i* の認証では、ユーザー、プログラムまたはプロセスは、オブジェクトまたはオブジェクト・セットにアクセスするための適切な権限を付与されることが保証されます。

権限を持たないユーザーによるデータベース・ユーザー名の使用を防止するために、Oracle には通常のデータベース・ユーザーを対象として複数の異なる方式によるユーザー検証が用意されています。認証は次の方法で実行できます。

- オペレーティング・システム
- 関連する Oracle データベース

また、Oracle Enterprise Edition では、次の認証モードもサポートされます。

- ユーザーのかわりにトランザクションを実行する中間層アプリケーションの Oracle データベース
- Secure Sockets Layer（SSL）プロトコル
- ネットワーク・サービス（Oracle Advanced Security 経由）

簡素化のために、通常は 1 つの方式ですべてのデータベース・ユーザーが認証されます。ただし、Oracle では、同じデータベース・インスタンス内ですべての方式を使用できます。

関連項目： 第 4 章「データベースに対するユーザーの認証」

権限

Oracle9*i* では、データへのすべてのユーザー・アクセスが権限によって制御されます。また、最小権限の概念がサポートされます。これは、ユーザーに付与する権限は、ジョブの実行に必要な最小数に抑える必要があるとする考え方です。Oracle9*i* では、ユーザーの作成時に自動的には直接的な権限を付与しないことで、この概念を施行しています。列レベルの権限と行レベルの権限の両方がサポートされます。列レベルの権限は直接付与でき、行レベルの権限はプログラムで、または Oracle Label Security を通じて付与できます。Oracle9*i* のシステム権限とオブジェクト権限は高度に細分化されているため、ユーザーには広範囲な権限を付与するのではなく、必要とする特定の権限のみを付与できます。

関連項目： 2-2 ページ「システム権限とオブジェクト権限」

ロール

Oracle9*i* では、ロールが広範囲にサポートされ、管理者はユーザーの権限を最適の状態で管理できます。Oracle9*i* Standard Edition では、次のロールがサポートされます。

- データベースのロール
- グローバル・ロール

Oracle Enterprise Edition では、次のロールもサポートされます。

- エンタープライズ・ロール
- 保護アプリケーション・ロール

関連項目：

- 2-4 ページ「ロールを使用した権限の管理」
- 9-19 ページ「保護アプリケーション・ロール」

監査

Oracle9*i* では、ユーザー・アクションを選択的に監査して、アカウンタビリティを提供できます。監査レコードは、不審なユーザー・アクティビティの識別ツールとしても役立ちます。監査は、ユーザー、文、権限（SELECT など）、およびスキーマ・オブジェクト（SELECT FROM EMP など）のように、様々なレベルで実行できます。

関連項目： 第 7 章「監査によるシステム・セキュリティの監視」

ビュー、ストアド・プログラム・ユニット、トリガー

Oracle9*i* のビューおよびストアド・プログラム・ユニットにより、システムにセキュリティ・レベルを追加できます。ビューでは、表のうち事前に指定した行と列のセットに対するユーザー・アクセスを制限できます。ストアド・プログラム・ユニット（ストアド・プロシージャ、パッケージおよびトリガーなど）は、関連タスク・セットの実行、複雑なセキュリティ認可の施行、特定の DML 操作の制限などの目的で使用できます。

関連項目：

- 2-7 ページ「ストアド・プロシージャを使用した権限の管理」
- 2-8 ページ「ビューを使用した権限の管理」

データ暗号化

他のセキュリティ・テクノロジの中でも、Oracle では強固な業界標準に準拠した暗号化技術を通じて E-Business システムのデータを保護します。Oracle では、Oracle7 以来、Oracle Advanced Security（旧称は「Secure Network Services」、その後「Advanced Networking Option」）を通じて、ネットワーク・データの暗号化をサポートしてきました。Oracle9*i* では、データベース内で暗号化を使用して選択したデータを保護する方法もサポートされます。

選択的なデータ暗号化のニーズに対応するために、Oracle9*i* には格納されているデータを暗号化および復号化するための PL/SQL パッケージが用意されています。このパッケージ DBMS_OBFUSCATION_TOOLKIT では、データ暗号化規格（DES）アルゴリズムを使用したバルク・データ暗号化がサポートされ、DES を使用して暗号化および復号化するためのプロシージャが含まれています。単一の DES に加えて、Oracle の DBMS_OBFUSCATION_TOOLKIT では、市販の最大レベルの暗号化を必要とするユーザーのために、2 キー・モードと 3 キー・モードの両方で Triple-DES（3DES）暗号化をサポートしています。さらに、データ整合性を保証するための MD5 保護暗号化ハッシュと、保護暗号キーを生成するための乱数ジェネレータもサポートされます。

関連項目： 2-10 ページ「サーバー上でのデータの暗号化」

高可用性

リソース制限とユーザー・プロファイル、オンライン・バックアップとリカバリ、およびアドバンスト・レプリケーションなど、Oracle9*i* の複数のメカニズムは、今日のオンライン・トランザクション処理および意思決定支援環境をサポートするために、連続的なデータベース処理を提供し、サービスの拒否を最小限に抑えます。

ユーザー・プロファイル

リソース制限およびユーザー・プロファイル・メカニズムにより、「リソース集中型」の問合せが防止され、特定のユーザーがシステム・リソースを意図的に悪意を持って操作することができなくなります。ユーザー・プロファイルは、管理者が定義してユーザー名に割り当

てるリソース制限のセットです。Oracle9*i* では、ユーザー・プロファイルを使用することで、データベース管理者はユーザーが使用可能な特定のシステム・リソースの量を定義して制限できます。制限できるシステム・リソースは、次のとおりです。

- 合計接続時間と合計アイドル時間
- 合計論理入出力（I/O）量
- ユーザー名別の同時複数セッション数
- メモリー使用量
- サイトで定義した前述の項目の重み付けに基づく複合的なシステム使用

Oracle9*i* では、ユーザー・プロファイルを通じて、他のユーザーに対するサービスを意図せずに、または故意に拒否するようなリソースの占有を防止します。

オンライン・バックアップおよびリカバリ

Oracle9*i* では、確実なオンライン・バックアップおよびリカバリを提供することで、高可用性も保証されます。このため、ミッション・クリティカルなアプリケーションは、これらの必要なアクティビティにより禁止されることがなくなります。データベースのバックアップの作成、管理およびリストアの方法が統合されており、バックアップおよびリカバリ操作の管理が容易になっている一方で、データベースの優れたパフォーマンスと高可用性が保たれています。データベースのバックアップは、トランザクション処理アクティビティのピーク期間中でもオンラインで実行できます。サーバー管理のバックアップおよびリカバリにより、データベース管理者の生産性が向上するのみでなく、バックアップおよびリカバリ・プロセスが簡素化されます。Oracle9*i* のバックアップおよびリカバリでは、一度の操作でデータベース全体とそのサブセットのうちどちらのバックアップを作成するかを選択できます。また、バックアップおよびリストアの自動パラレル化を実行することで、この操作の所要時間を最短に抑えることができます。さらに、バックアップ操作中の出力用およびリストア操作中の入力用に、順次 I/O デバイスもサポートされます。テープによるバックアップも、ベンダー提供のテープ管理システムとともにサポートされます。

アドバンスト・レプリケーション

Oracle9*i* のアドバンスト・レプリケーション機能を使用すると、トランザクション処理データベースから大規模な問合せをオフロードして、システムの可用性を高めることができます。たとえば、データ集中型の問合せが同じ表に対するトランザクションと競合しないように、データを購入する顧客の大きな表をカスタマ・サービス・データベースにレプリケートできます。また、アドバンスト・レプリケーション機能は、ミッション・クリティカルなデータベースの可用性の保護にも役立ちます。たとえば、対称レプリケーションでは、データベース全体をフェイルオーバー・サイトにレプリケートして、プライマリ・サイトがシステム障害やネットワーク障害のために使用不能になった場合に備えることができます。読取りおよび書込みアクセスの両方のアドバンスト・レプリケーションにより、データ整合性が保証されます。リフレッシュ・グループにより、参照整合性、トランザクションの一貫性、関連マスター表の表スナップショットが保たれます。たとえば、顧客、注文および注文明細はすべて関連があるため、1 グループとしてリフレッシュできます。

データのパーティション化

Oracle9*i* でのデータのパーティション化は、Oracle9*i* データベース・サーバーを使用して配置されるアプリケーションの管理性、パフォーマンスおよびスケールを大幅に改善する強力なツールです。また、表のレンジ・パーティション化と、索引に対する複数のパーティション化方法が許可されており、非常に大型のデータベースがサポートされ、管理操作が改善されます。実際には、メディア障害、パフォーマンスのためのアクセス・バランシングおよび表の断片化解消は、パーティション化により障害の影響を軽減したり、高負荷状況で可用性を高めることのできる分野のごく一部にすぎません。

現在、Partitioning Option 付きの Oracle9*i* では、すべての DML 操作がパラレルでサポートされます。また、索引スキャン、表データのエクスポートとインポート、および統計の見積りと計算も、個々のパーティションでパラレルに実行できます。パーティションは、索引を事前に作成しているかどうかにかかわらず、個別にパラレルでロードできます。ロード、バックアップ、リカバリ、統計の計算およびインポートとエクスポートは、すべてパーティションごとにサポートされます。これらの操作は、他のパーティションに対して進行中の操作を妨げずに個別に実行できます。各操作をパーティション単位で実行できるため、真に大幅なパフォーマンス改善を実現できます。

Oracle Real Application Clusters による高可用性

Oracle Real Application Clusters は、ミッション・クリティカルなアプリケーションにきわめて高レベルの可用性を提供します。Real Application Clusters 環境では、Oracle はクラスタ内の複数のシステム上で実行され、単一の共有データベースに同時にアクセスします。システムの 1 つに障害が起きると、正常に稼働しているシステムにより、クラッシュした Oracle インスタンスのリカバリが実行されます。これにより、単純なコールド・クラスタ・フェイルオーバーに比べて可用性と拡張性の両面で大きなメリットが得られます。

- システムの 1 つが障害を起こしても、影響を受けるのはそのユーザーのサブセットのみです。障害は、クラスタ内の他のシステムに接続しているユーザーには影響しません。
- 障害を起こしたシステムのユーザーは、クラスタ内の正常なシステムにフェイルオーバーできます。Oracle サーバーはすでに正常なシステム上で実行されているため、このフェイルオーバーは高速です。フェイルオーバー後のパフォーマンスには、データが正常なシステムのキャッシュにすでにロードされていることによるメリットがあります。
- データベースのユーザーは、障害が発生した場合に使用されるバックアップ・サーバーに事前に接続でき、ユーザーの再接続に伴う遅延が軽減され、リカバリが高速になります。
- すべてのサーバーは通常の操作中はアクティブになっているため、システム・リソースの使用率が適正化され、大きい負荷に耐えることができます。また、このソリューションはスケーラブルです。容量の追加が必要になった場合は、クラスタに新しいサーバーを追加できます。

関連項目： 2-13 ページ「システム可用性の要因」

Oracle9*i* でのプロキシ認証

この項では、Oracle9*i* によるプロキシ認証のサポートについて説明します。

概要

OCI のプロキシ認証機能は、当初は Oracle8*i* でリリースされ、データベース・クライアントでは、単一のデータベース接続で多数の「軽量」ユーザー・セッションをセットアップし、各セッションを異なるデータベース・ユーザーに対応付けることができるようになりました。

Oracle9*i* のプロキシ認証では、クライアントの認証は次のようにサポートされます。

- ユーザーが Oracle9*i* のプロキシ認証にアクセスするときに与えられるデータベース・パスワードを使用
- 識別名または X.509 証明書を使用

Oracle9*i* では、この機能は、特定の中間層の動作を指定のユーザー・セットの代理に限定できるように設計されています。中間層がデータベースに対して自己認証すると、パスワードのようなユーザー固有の認証情報を発行しなくても、そのユーザーのかわりに軽量セッションを確立できます。さらに、Oracle9*i* は、特定の中間層が特定ユーザーのかわりにデータベースで操作する場合に、特定のデータベース・ロールのセットを想定できるように構成できます。つまり、データベースでは、軽量セッションを通じて、あるユーザーのために操作する中間層に付与する権限を決定するときに、中間層の識別情報とクライアント・ユーザー ID の両方が使用されます。

関連項目：

- 3-7 ページ「3 層のセキュリティを保証するためのプロキシ認証」
- 4-8 ページ「プロキシ認証および認可」

追加のプロトコルのサポート

Oracle8*i* では、プロキシ認証機能は Oracle Call Interface（OCI）を使用するデータベースへの通信に制限されていましたが、Oracle9*i* では、この機能がデータベースへの Java Database Connectivity（JDBC）アクセスにも拡張されています。中間層サーバーは JDBC OCI を通じてクライアント・ユーザー用の軽量セッションを確立し、そのユーザーのかわりに Oracle9*i* データベースにアクセスできるようになりました。

拡張された証明書のプロキシ

Oracle8*i* では、パスワードのみで認証されたデータベース・ユーザーのプロキシ認証がサポートされていました。パスワードは、組織のセキュリティ・プリファレンスに応じて、データベースで検証される属性として渡すことができる場合と、そうでない場合がありました。

Oracle9*i* ではプロキシ認証が拡張され、データベースに対する識別名（DN）または完全な X.509 証明書による追加の認証プロキシが含まれるようになっています。これにより、SSL 証明書（X.509 証明書または DN）をユーザーの（認証ではなく）識別のためにデータベースに渡すことができるため、強力な 3 層のセキュリティが提供されます。（SSL は、エンド・ツー・エンド・プロトコルではなく 2 点間プロトコルであるため、複数層を介したユーザーの認証には使用できません。）たとえば、ユーザーは SSL を使用して中間層に認証でき、中間層は証明書から DN を抽出して、その DN（または完全な証明書）をデータベースに渡すことができます。もう 1 つの利点は、DN または証明書を軽量セッションで使用でき、そこに含まれる要素を仮想プライベート・データベースで使用してアクセスを制限できることです。たとえば、組織では、データベースに対するユーザー証明書の組織単位（OU）要素に基づいて、データ・アクセスを制限できます。

データベースでは、DN または証明書を使用して、Oracle Internet Directory、またはエンタープライズ・ユーザーのセキュリティ（Oracle Advanced Security 機能）について証明されている他の LDAP 準拠のディレクトリ内でユーザーを検索できます。プロキシ認証とエンタープライズ・ユーザー・セキュリティの統合により、ユーザー ID をアプリケーションのすべての層でメンテナンスでき、ユーザーをディレクトリ内で一度作成するのみですみます。また、Oracle8*i* とは異なり、エンタープライズ・ユーザー・セキュリティを単なるクライアント / サーバーではなく 3 層アプリケーションで使用できます。

> **関連項目：** 9-35 ページ「パスワード認証を受けたエンタープライズ・ユーザー」

アプリケーション・ユーザーのプロキシ認証

多くのアプリケーションでは、セッション・プーリングを使用して、複数のユーザーにより再利用される多数のセッションが設定されています。このコンテキストでは、「アプリケーション・ユーザー」はデータベースに認識されるユーザーではなく、アプリケーションの中間層に対して認証されるユーザーです。Oracle9*i* では、このタイプのアプリケーション用にアプリケーション・ユーザーのプロキシ認証が導入されています。

このモデルでは、セッションの確立時に中間層からデータベースにクライアント識別子が渡されます。（クライアント識別子は、Cookie や IP アドレスなど、中間層に接続するクライアントを表すものであれば、なんでもかまいません。）アプリケーション・ユーザーを表すクライアント識別子は、ユーザー・セッション情報に使用でき、アプリケーション・コンテキストでも（USERENV ネーミング・コンテキストを使用して）アクセスできます。そのため、アプリケーションでは、アプリケーション・ユーザーがデータベースに認識されない場合にも、仮想プライベート・データベースを使用してユーザー・アクセスを制限できます。アプリケーションではセッションを設定したり再利用でき、その間もセッション中に「アプリケーション・ユーザー」を追跡できます。

JDBC OCI で使用可能なアプリケーション・ユーザーのプロキシ認証には、別個のユーザー・セッション（「軽量」セッションであっても）の設定と管理によるオーバーヘッドを発生させずに接続プーリングが可能になり、ユーザーがデータベースに認識されないアプリケーションでも、仮想プライベート・データベースを利用できるという利点があります。したがって、アプリケーション・ユーザーのプロキシ認証は、ユーザーの拡張性要件を満たしつつユーザー別のデータ・アクセス制御がサポートされるため、数千人のユーザーを伴うE-Business アプリケーションでは特に役立ちます。

Oracle9*i* Enterprise Edition

Oracle9*i* Enterprise Edition は、強力なデータ保護、インターネット規模のセキュリティ、およびアプリケーションとデータ交換にターゲットを絞ったセキュリティ・メカニズムを提供することで、E-Business アプリケーションの構築と配置には理想的なプラットフォームとなっています。Oracle9*i* Standard Edition の強力な機能がすべて組み込まれているのみではありません。この項の内容は次のとおりです。

- インターネット規模のセキュリティ機能
- アプリケーション・セキュリティ
- Oracle9i の仮想プライベート・データベース
- 保護アプリケーション・ロール
- ファイングレイン監査
- Oracle による 3 層アプリケーションの監査
- データベースでの Java セキュリティ実装

これらの機能の詳細は、Oracle9*i* のマニュアル・セットを参照してください。

関連項目：

- 『Oracle9*i* データベース概要』
- 『Oracle9*i* アプリケーション開発者ガイド ― 基礎編』

インターネット規模のセキュリティ機能

E-Business は、顧客、パートナおよび従業員に対して、制御された安全な方法で情報へのアクセスを提供することが重要です。Oracle9*i* では、強力なデータ保護、インターネット規模のセキュリティ、安全なホスティングおよびデータ交換を通じて、E-Business のセキュリティ要求に対処します。

強力なデータ保護

強力なデータ保護により、クライアントからアプリケーション・サーバー、データベース・サーバーへと、アプリケーションの層全体について、適格で包括的なセキュリティが保証されます。

E-Business システムをインターネットに配置するとリスクが増大します。セキュリティ上のリスクを軽減する最善の方法は、単一のメカニズムが障害を起こしても重要な情報が損なわれないように、複数層のセキュリティ・メカニズムを採用することです。これは、強力なデータ保護と呼ばれます。Oracle9*i* では、このメカニズムが仮想プライベート・データベース（VPD）、Oracle Label Security、選択的なデータ暗号化および広範囲の監査を通じて提供されます。

インターネット規模のセキュリティ

インターネット規模のセキュリティにより、ユーザーと権限の管理を、データにアクセスする数十万のユーザーまで拡張できます。Oracle9*i* Enterprise Edition は、ユーザー管理、PKI 統合およびディレクトリ・ベースの権限管理に関する Oracle Advanced Security 機能の基盤です。

セキュリティ・メカニズムは、数千または数百万のユーザーをサポートできるようにインターネット規模まで拡張し、しかも管理できるようにする必要があります。Oracle9*i* には、インターネット規模のアプリケーションを構築できるように調整された多数のセキュリティ機能が用意されています。たとえば、プロキシ認証、Secure Sockets Layer（SSL）などのインターネット規格および関連する公開鍵インフラストラクチャ（PKI）規格、Java セキュリティ、エンタープライズ・ユーザー・セキュリティ・サポートなどがあります。

安全なホスティングおよびデータ交換

安全なホスティングおよびデータ交換により、データ・アクセスを顧客別またはユーザー別に経済的で安全な方法でパーティション化する一方、必要なコミュニティ間で共有されるデータの保護をサポートできます。Oracle9*i* Enterprise Edition は、仮想プライベート・データベース・テクノロジ、公開鍵インフラストラクチャ（PKI）とエンタープライズ・ユーザー・セキュリティに関する Oracle Advanced Security の機能および Oracle Label Security の基盤となっています。

アプリケーション・セキュリティ

データベース・アプリケーションごとに、独自のセキュリティ・ポリシーを設定できます。独自の権限を設定し、アプリケーションの実行時に異なるセキュリティ・レベルを提供する 1 つ以上のデータベース・ロールを使用できます。データベース・ロールは、ユーザー・ロールに付与するか、特定のユーザー名に直接付与できます。

潜在的に SQL 文の（SQL*Plus などのツール経由による）実行が無制限に許されるアプリケーションでは、機密または重要なスキーマ・オブジェクトへの悪意のあるアクセスを防止するセキュリティ・ポリシーを使用できます。これにより、ユーザーが実際にはアプリケーションを使用していないときに、ロールや権限を悪用しないことを保証できます。

Oracle9*i* の仮想プライベート・データベース

Oracle9*i* では、仮想プライベート・データベース（VPD）テクノロジで、行レベルのアクセス制御が提供されます。この機能は Oracle 社からのみ提供されています。また、仮想プライベート・データベース・ツールキットで構築され、ラベル・ベースのアクセス制御を追加する Oracle Label Security 製品もサポートされます。

この項の内容は次のとおりです。

- Oracle8i および Oracle9i での仮想プライベート・データベース
- 仮想プライベート・データベースの機能
- Oracle9i でのアプリケーション・コンテキスト
- アプリケーション・コンテキストによる VPD の活用
- パーティション化されたファイングレイン・アクセス・コントロールによる VPD の活用
- ユーザー・モデルと仮想プライベート・データベース
- Oracle Policy Manager

> **関連項目：** アプリケーション・コンテキスト、ファイングレイン・アクセス・コントロールおよび VPD の詳細は、『Oracle9*i* アプリケーション開発者ガイド ― 基礎編』を参照してください。

Oracle8*i* および Oracle9*i* での仮想プライベート・データベース

Oracle8*i* では、仮想プライベート・データベース（VPD）の導入により、データベース・セキュリティに新しい標準が設定されました。サーバー側で施行されるファイングレイン・アクセス・コントロールと保護アプリケーション・コンテキストにより、複数の顧客とパートナがミッション・クリティカルなデータに対して安全に直接アクセスできます。仮想プライベート・データベースにより、単一のデータベース内でデータ・アクセスをユーザー別または顧客別に制御でき、物理的にデータが分離されることが保証されます。インターネット・アクセスの場合は、仮想プライベート・データベースにより、オンライン・バンキングの顧客に対して自分の注文以外は表示されないことを保証できます。Web ホスティング会社は、

複数企業のデータを同じ Oracle9*i* データベースでメンテナンスし、各社に自社データの参照のみを許可できます。

企業内では、仮想プライベート・データベースによりアプリケーションの配置に伴う所有コストが削減されます。セキュリティは、データにアクセスする各アプリケーションではなくデータベース・サーバー側で一度構築すればすみます。セキュリティは、ユーザーがデータにアクセスする方法に関係なくデータベースにより施行されるため強力です。ユーザーが非定型問合せツールや新規レポート・ライターにアクセスすると、セキュリティのバイパスはなくなります。仮想プライベート・データベースは、管理対象となる Web ベースのアプリケーションを構築する組織や Oracle 自身のためのキーとなるテクノロジです。Oracle SalesOnline.com や Oracle9*i*AS Portal など、複数の Oracle アプリケーションは、VPD を使用してホスティング用のデータ分離を施行しています。

Oracle8*i* では、仮想プライベート・データベース機能によりファイングレイン・アクセス・コントロールとアプリケーション・コンテキストを提供していました。データベース内のデータは、すべてのアプリケーションにまたがって行レベルでセキュリティを提供し、表やビューにセキュリティ・ポリシーを直接連結することで保護されます。

Oracle9*i* では、次のように複数の新しい拡張機能が追加され、仮想プライベート・データベースが拡張されています。

- Oracle Policy Manager。セキュリティ・ポリシーの管理を容易にするツールです。
- パーティション化されたファイングレイン・アクセス・コントロール。複数アプリケーションおよび管理対象環境への VPD の配置を容易にします。
- グローバル・アプリケーション・コンテキスト。アプリケーション・ユーザー・モデルをサポートします。
- シノニムに対する VPD サポート。

関連項目：

- 2-9 ページ「アプリケーションのクエリー・リライト : 仮想プライベート・データベース」
- 3-3 ページ「データベースにより施行されるネットワーク・アクセス」
- 9-18 ページ「Oracle Policy Manager」

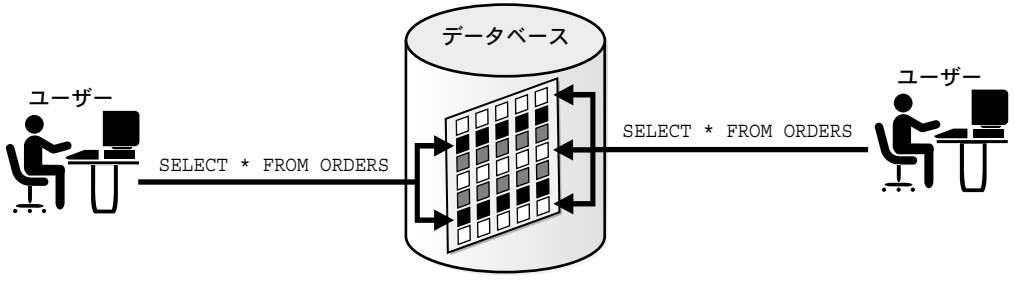
仮想プライベート・データベースの機能

仮想プライベート・データベースは、1 つ以上のセキュリティ・ポリシーを表またはビューに対応付けることで使用可能になります。セキュリティ・ポリシーは、ユーザーが取得できるアクセスやビューのタイプを制約します。セキュリティ・ポリシーが連結されている表に直接または間接的にアクセスすると、データベースはポリシーを実装する関数に問い合せます。ポリシー関数は、述語（WHERE 句）と呼ばれるアクセス条件を戻します。この述語はデータベースによりユーザーの SQL 文に追加されるため、ユーザーによるデータ・アクセスが動的に変更されます。

VPD を実装するには、各 SQL 文に SQL 述語を追加して、その文の行レベルのアクセスを制御するように、ストアド・プロシージャを記述します。次に、セキュリティ・ポリシーは、関数を必要なスキーマと表にリンクします。たとえば、John Doe（部門 10 に所属）が文 SELECT * FROM emp を入力した場合は、VPD を使用して WHERE DEPT = 10 句を追加できます。このように問合せの変更を使用して、特定の行へのデータ・アクセスを制限します。

保護アプリケーション・コンテキストにより、組織、コスト・センター、勘定科目番号、職階など、アプリケーションが重要と判断する属性であれば、事実上あらゆる属性に基づいてアクセス条件を設定できます。たとえば、Web による注文入力システムでは、顧客番号と、ユーザーが顧客であるか販売担当であるかに基づいて、アクセスを施行できます。これにより、顧客は自分の注文状況をオンラインで（ただし、自分の注文についてのみ）参照でき、営業担当は担当する顧客についてのみ複数の注文を参照できます。

図 9-1 仮想プライベート・データベース : 顧客は自分の注文のみを参照



仮想プライベート・データベースにより、ユーザーがデータを取得する方法（アプリケーション、レポート作成ツールまたは SQL*Plus 経由）に関係なく、同じ厳密なアクセス制御ポリシーが施行されることが保証されます。これにより、VPD を使用すると、銀行は顧客が自分の口座のみを参照する（他人の口座を参照しない）ことを保証でき、電話会社は顧客レコードを安全に保護し、人事管理アプリケーションは従業員レコードへのデータ・アクセスに関して複雑なルールをサポートできます。

これらのファイングレイン・アクセス・コントロール機能は、データベース名にシノニムを使用した場合にも適用されます。シノニムにポリシー関数を適用することによって、ビューの作成時に適用されたのと同じ制約を、リソースやプロセスを多くを使用することなく作成できます。ポリシー関数を使用しない場合は、リソースやプロセスがユーザーの数に比例して増加します。

Oracle9*i* でのアプリケーション・コンテキスト

アプリケーション・コンテキストにより、ファイングレイン・アクセス・コントロールの実装が容易になります。関数を使用してセキュリティ・ポリシーを実装し、それをアプリケーションに対応付けることができます。各アプリケーションでは、独自のアプリケーション固有のコンテキストを使用できます。ユーザーがコンテキストを（SQL*Plus 経由などで）任意に変更することは許されません。

アプリケーション・コンテキストでは、アプリケーションに必要な属性に基づく、柔軟なパラメータ・ベースのアクセス制御が許されます。たとえば、人事管理アプリケーションのコンテキスト属性には「職階」、「組織単位」および「国」を使用し、受注管理属性には「顧客番号」と「営業地域」を使用できます。

エンタープライズ・ユーザーのセキュリティには、Oracle Advanced Security が必要なため注意してください。この機能では、Oracle Label Security のラベルと権限もサポートされます。

アプリケーション・コンテキストによる VPD の活用

ほとんどのアプリケーションには、アクセス制限の基準に関する情報が含まれています。たとえば、注文入力アプリケーションの場合は、顧客によるアクセスをその顧客の注文（ORDER_NUMBER）と顧客番号（CUSTOMER_NUMBER）に限定する必要があります。アプリケーション・コンテキストは基礎となるデータベース機能であり、アプリケーションでアクセス制御の施行に使用できる属性を定義し、設定してアクセスできます。ユーザー名、従業員番号、アクセス権が付与されている帳簿および管理階層における職階など、ユーザー属性を安全に格納できます。その情報を後でセッション中に取り出して、ファイングレイン・アクセス・コントロールに使用できます。

アプリケーション・コンテキストを初期化するには、次の 4 つの方法があります。

- ローカルにアクセスするアプリケーション・コンテキスト
- 外部で初期化するアプリケーション・コンテキスト
- グローバルに初期化するアプリケーション・コンテキスト
- グローバルにアクセスするアプリケーション・コンテキスト

ローカルにアクセスするアプリケーション・コンテキスト

アプリケーション・コンテキスト機能は、Oracle8*i* で導入されました。ローカル・データベース環境では、属性値をユーザーのセッション情報から初期化できます。各アプリケーションでは、独自の属性を持つ独自のコンテキストを使用できます。

外部で初期化するアプリケーション・コンテキスト

この機能を使用すると、外部リソースからの属性値の初期化を受け入れる特別なタイプのネームスペースを指定できます。これによりパフォーマンスが強化され、セッション間で属性を自動的に伝播できるようになります。多くのアプリケーションでは、ファイングレイン・アクセス・コントロールに使用される属性が、アクセス制御用のデータベース・メタデータ表に格納されます。たとえば、EMPLOYEES 表には、コスト・センター、タイトル、署名権限、ファイングレイン・アクセス・コントロールに役立つその他の情報を含めることができます。ただし、多くの組織では、ユーザー情報とユーザー管理を、Oracle Internet Directory のような LDAP 準拠のディレクトリに集中化しています。これらの組織は、アクセス制御に使用するユーザー情報も集中化することを希望しています。アプリケーション・コンテキスト属性をディレクトリに格納し、1 人以上のエンタープライズ・ユーザーに割り当てることができます。この情報は、エンタープライズ・ユーザーのログイン時に自動的に取り出して、アプリケーション・コンテキストの初期化に使用できます。

グローバルに初期化するアプリケーション・コンテキスト

この機能はユーザーのアプリケーション・コンテキスト用に集中化された格納場所を提供し、アプリケーションで初期化中にユーザーの識別情報に基づいて、そのユーザーのコンテキストを設定できるようにします。特に、この機能では、Oracle Label Security のラベルと権限もサポートされます。この機能により、管理者にとっては多数のユーザーおよびデータベースのコンテキスト管理がはるかに容易になります。

グローバルに初期化されたアプリケーション・コンテキストでは、Lightweight Directory Access Protocol（LDAP）が使用されます。LDAP には、このアプリケーションが割り当てられているユーザーのリストが格納されます。Oracle9*i* では、エンタープライズ・ユーザーの認証および認可用のディレクトリ・サービスとして、Oracle Internet Directory を使用できます。

グローバルにアクセスするアプリケーション・コンテキスト

グローバル・アプリケーション・コンテキストは、トラステッド・セッション間で共有できます。アプリケーション（特に中間層製品）は、ファイングレイン・アクセス・コントロール・ポリシーを施行するのみでなく、このサポートを使用してアプリケーション属性を安全でグローバルに管理できます。

多くの Web ベース・アプリケーションでは、接続プーリングを使用して高い拡張性を達成し、数十万人のユーザーをサポートしています。このようなアプリケーションでは、ユーザーごとに異なるセッションを持つのではなく、接続が設定されて再利用されます。たとえば、Web ユーザー Jane と Ajit が中間層アプリケーションに接続し、アプリケーションでは両方のユーザーのかわりに使用するデータベース内でセッションが確立されるとします。このアプリケーションは、接続中のユーザー名の切替えを受け持つため、セッションを使用しているユーザーは常に Jane または Ajit のどちらかとなります。

Oracle9*i* の VPD 機能により、ユーザー・セッションごとにアプリケーション・コンテキストを設定するかわりに、複数の接続で 1 つ以上のグローバル・アプリケーション・コンテキストにアクセスできるようになり、接続プーリングが活用されます。グローバル・アプリケーション・コンテキストの柔軟性が向上するため、Web ベースのアプリケーションで仮想

プライベート・データベースを使用できるのみでなく、セッションごとにアプリケーション・コンテキストを設定するかわりに、複数のセッション間で共通のアプリケーション・コンテキストを再利用することによりパフォーマンスも強化されます。

アプリケーション・ユーザーのプロキシ認証をグローバル・アプリケーション・コンテキストと併用すると、E-Business アプリケーションの構築時にさらに柔軟性が高まり、パフォーマンスが向上します。たとえば、ビジネス・パートナに情報を提供する Web ベース・アプリケーションに、使用可能な情報のレベルを表す Gold、Silver および Bronze という 3 タイプのユーザーがいるとします。各ユーザーに個々のアプリケーション・コンテキストで独自セッションを設定させるかわりに、アプリケーションで Gold、Silver または Bronze 用のグローバル・アプリケーション・コンテキストを設定し、クライアント識別子を使用して適切なコンテキストでセッションを指し、適切なタイプのデータを取り出すことができます。アプリケーションでは、3 つのグローバル・コンテキストを一度初期化するのみで、クライアント識別子を使用して適切なアプリケーション・コンテキストにアクセスし、データへのアクセスを制限できます。

パーティション化されたファイングレイン・アクセス・コントロールによる VPD の活用

ファイングレイン・アクセス・コントロールにより、小さな単位レベルのセキュリティ・ポリシーを施行するアプリケーションを構築できます。たとえば、ファイングレイン・アクセス・コントロールを使用すると、Oracle サーバーにアクセスする顧客は自分のアカウントしか参照できず、医者は担当する患者の記録しか参照できず、管理者は部下の記録しか参照できないように制限できます。

アプリケーションによりセキュリティ・ポリシーの施行をパーティション化できるため、VPD の配置が容易になります。たとえば、注文入力アプリケーションと在庫管理アプリケーションの両方が Orders 表にアクセスするとします。注文入力アプリケーションでは顧客番号に基づいてアクセスを制限し、在庫管理アプリケーションでは部品番号に基づいてアクセスを制限しています。この場合は、どちらのアプリケーションがデータにアクセスしているかに応じて、異なるセキュリティ・ポリシーを適用できるように、ファイングレイン・アクセス・コントロールをパーティション化できると便利です。それ以外の場合、この 2 つのアプリケーションの開発者は相互のポリシーに同意する必要がありますが、それが実際的でない場合や同意できない場合があります。そのため、アプリケーションでは、個々のアプリケーションのニーズに基づいて異なるセキュリティ・ポリシーを使用できます。

Oracle9*i* では、ポリシー・グループと駆動側アプリケーション・コンテキストを通じて、仮想プライベート・データベースをパーティション化できます。駆動側アプリケーション・コンテキストでは、どちらのアプリケーションがデータにアクセスしているかが安全に判断され、ポリシー・グループではアプリケーションにより適用されるポリシーの管理が簡単になります。また、Oracle9*i* では、常にデータ・アクセスに適用されるデフォルトのポリシー・グループもサポートされます。たとえば、サブスクライバ ID を使用するアプリケーション・ホスティング用のアプリケーション「striped」では、常にサブスクライバ別にデータ分離が施行されるデフォルト・ポリシー「Subscriber」と、在庫管理および注文入力ベースのアクセス用に、データにアクセスしている特定のアプリケーションに応じて適用される追加のポリシー・グループを使用できます。

ユーザー・モデルと仮想プライベート・データベース

アプリケーションでは様々なユーザー・モデルを使用できますが、ユーザー別にアクセスを制限するには VPD も使用します。Oracle9*i* には、ユーザーがデータベース・ユーザーであるか、データベースに認識されないアプリケーション・ユーザーであるかに関係なく、アプリケーションでファイングレイン・アクセス・コントロールをユーザー別に施行できるように、様々な方法が用意されています。

アプリケーション・ユーザーがデータベース・ユーザーでもあるアプリケーションの場合、VPD の施行は比較的簡単です。ユーザーはデータベースに接続し、アプリケーションではセッションごとにアプリケーション・コンテキストを設定できます。各セッションは異なるユーザー名で開始されるため、「Jane」と「John」に異なるファイングレイン・アクセス・コントロール条件を規程するのも簡単です。また、JDBC OCI の各「軽量」セッションは個別のデータベース・セッションでもあり、独自のアプリケーション・コンテキストを使用できるため、プロキシ認証も使用できます。プロキシ認証はエンタープライズ・ユーザーのセキュリティと統合できるため、ユーザー・ロールを Oracle Internet Directory のみでなく VPD 施行に使用できる他の属性からも取り出すことができます。

単一ユーザー（OneBigApplicationUser など）がすべてのユーザーのかわりにデータベースに接続するアプリケーションの場合も、ユーザー別のファイングレイン・アクセス・コントロールが可能です。アプリケーション開発者は、アプリケーション・ユーザー（「realuser」など）を表すコンテキスト属性を作成できます。すべてのデータベース・セッション（およびすべての監査レコード）は OneBigApplicationUser で開始されますが、各セッションでは誰が「real user」であるかに応じて異なる属性を使用できます。このモデルが最も適切なのは、ユーザー数が限られていて、セッション再利用の要件がないアプリケーションの場合です。もちろん、データベースの観点からは、各セッションは同じデータベース・ユーザーとして作成されるため、ロールやデータベース監査などを使用する機能は前述の理由から大幅に低下します。

Oracle Policy Manager

Oracle9*i* では、Oracle Policy Manager を通じて VPD のポリシーの管理が改善されています。Oracle Policy Manager は、Oracle Enterprise Manager を通じてアクセスされる、使用しやすい Graphical User Interface（GUI）です。開発者は Oracle Policy Manager を使用して、表やビューなどのスキーマ・オブジェクトにセキュリティ・ポリシーを適用したり、アプリケーション・コンテキストを作成できるため、VPD の開発と管理がはるかに簡単になります。また、Oracle Policy Manager は、データにラベル・ベースのアクセスを提供する VPD ベース製品である Oracle Label Security の管理ツールでもあります。つまり、Oracle Label Security は、ファイングレイン・データ・アクセス・コントロールの問題に対する汎用ソリューションです。

関連項目： 9-42 ページ「Oracle Label Security」

保護アプリケーション・ロール

この機能は Oracle9*i* に固有のもので、ユーザー定義の基準に基づいてロールを使用できるようにします。保護アプリケーション・ロールは、パッケージにより実装されるロールです。たとえば、特定の IP アドレスからのみ接続するユーザー、または特定の中間層を介してのみデータベースにアクセスするユーザーによるロールの使用を許可するパッケージを記述できます。

プロキシ認証を使用する 3 層システムの場合、パッケージではユーザー・セッションが中間層により作成されたかどうか、つまり、ユーザーが適切なアプリケーション経由でデータベースにアクセスしているかどうかを検証できます。また、保護アプリケーション・ロールにより、データベースに直接接続しているユーザーは、どのデータにもアクセスできないことが保証されます。さらに、他のセキュリティ条件も規程できます。たとえば、ユーザーは、特に機密性の高い人事データには、インターネットからのアクセスを許可されません。

保護アプリケーション・ロールにより、データベースの固有の厳密な認証とファイングレイン・アクセス・コントロールが拡張され、ユーザーは適切なアクセス条件を満たしていなければ、どんな権限も持つことができなくなります。また、非常に厄介なセキュリティの問題も解決され、安全な Web ベースのアプリケーション・データへのアクセスがサポートされます。

関連項目： 2-6 ページ「保護アプリケーション・ロール」

ファイングレイン監査

Oracle9*i* は、拡張可能なファイングレイン監査の導入により、データベースの既存の確実な最小単位による監査機能として拡張されています。ファイングレイン監査により、組織は監査機能を洗練させて、問題となっている特定のデータ・アクセスを獲得し、識別できます。ファイングレイン監査は、正当なアクセスの悪用を検出するなど、より小さい単位にターゲットをしぼった監査情報を提供するのみでなく、Oracle9*i* データベース自体の侵入検出システムとしても機能できます。

ファイングレイン監査により、組織は監査イベントのトリガーとなるデータ・アクセス条件を指定して監査ポリシーを定義し、柔軟なイベント・ハンドラを使用してトリガー・イベントが発生したことを管理者に通知できます。たとえば、組織は人事管理スタッフには従業員の給与情報へのアクセスを許可し、$500001 以上の給与にアクセスした場合は、そのアクセスを監査できます。監査ポリシー「where SALARY > 500000」は、監査ポリシー・インタフェース（PL/SQL パッケージ DBMS_FGA）を通じて EMPLOYEES 表に適用されます。

実装の柔軟性を高めるために、組織はユーザー定義関数を使用してポリシー条件を決定し、監査に関連する列を識別できます。たとえば、関数では、ユーザーがイントラネット内部でデータにアクセスしているかぎり、すべての給与への無監査アクセスを許可する一方、インターネットからアクセスする場合は役員レベルの給与へのアクセスを監査できます。監査列を使用すると、特定の列が問合せで参照される場合にのみ監査を起動すればよいため、誤った監査レコードや不要な監査レコードのインスタンスを削減できます。たとえば、人事管理スタッフが給与情報のみにアクセスする場合、対応する従業員名も選択しなければ意味がな

いため、組織は従業員名がアクセスされる場合にのみ役員給与へのアクセスを監査すればよいことになります。

監査トリガー・イベントが発生すると、Oracle9*i* はユーザーが監査表で実行した文の正確な SQL テキストと、問合せを実行中のユーザーやタイムスタンプなどの追加情報を獲得します。ファイングレイン監査を LogMiner のような他のデータベース機能と併用すると、ユーザーに戻された正確なレコードを再作成できます。これは、極秘情報を共有する必要があり、それに対して厳密なアカウンタビリティを必要としている組織にとって、特に重要な場合があります。たとえば、国際レベル、連邦レベル、州レベルおよびローカル・レベルの多くの司法機関は、相互に情報を共有することでますます「E-Business」化しつつありますが、重要データなどの機密情報へのアクセスを監査し、誰がどのデータにアクセスしたかを正確に知ることも、これまでになく重要になってきています。

イベント・ハンドラを使用すると、組織は監査トリガー・イベントの処理方法を柔軟に決定できます。監査トリガー・イベントを特別な監査表に書き込んでさらに分析したり、セキュリティ管理者のポケット・ベルをアクティブにすることができます。イベント・ハンドラにより、組織は監査応答を適切なエスカレーション・レベルへと微調整できます。

関連項目： 7-3 ページ「拡張可能なファイングレイン監査」

Oracle による 3 層アプリケーションの監査

Oracle9*i* では、中間層を通じて実際のクライアントの識別情報を保ち、中間層を介して「最小権限」を施行できるのみでなく、中間層によりユーザーのかわりに実行されたアクションも監査できます。Oracle9*i* の監査レコードでは、接続を開始したログイン・ユーザー（つまり中間層）と、かわりにアクションが実行されたユーザーの両方が獲得されます。

関連項目： 7-4 ページ「複数層アプリケーション環境での監査」

データベースでの Java セキュリティ実装

Oracle9*i* では、サーバーに Java セキュリティ実装が含まれています。Java Virtual Machine（JVM）は、コンパイル済み Java バイトコードをプラットフォームのマシン言語に変換し、それを実行する Java インタプリタです。JVM は、クライアント側、ブラウザ内、中間層内、Web 上、Oracle9*i* Application Server などのアプリケーション・サーバー上または Oracle9*i* などのデータベース・サーバー内で動作します。

クラスによる実行

Oracle9*i* の JVM 実装では、クラス内のコードを実行する権利は、クラス自体の実行権限により制御されます。これは、PL/SQL パッケージの実行権限と同じデータベース権限であり、管理方法も同じです。

SecurityManager クラス

Oracle9*i* JVM は、インストール済みのクラス java.lang.SecurityManager で起動します。Oracle9*i* データベースは、Sun 社の Java Development Kit（JDK）リリース 1.2 に準拠しており、このリリースのセキュリティ機能が実装されています。この実装では、許可はデータベース表の内容別に制御されます。通常、表は PL/SQL プロシージャ（および Java メソッド）で管理されます。表を使用すると、ユーザーまたはロールに許可を付与でき、クラスの「コード・ソース」はスキーマにクラスがロードされているユーザーで識別されます。特定の Oracle の許可により、表を更新する権利が制御され、セキュリティが重要な他の操作が実行されます。

関連項目：『Oracle9*i* Java 開発者ガイド』

Oracle Advanced Security

Oracle Advanced Security は、Oracle9*i* 用の付加価値インターネット・セキュリティのまとまりです。その機能は、ネットワーク・セキュリティ・サービス、エンタープライズ・ユーザーのセキュリティおよび公開鍵インフラストラクチャ（PKI）という 3 つのカテゴリに分かれています。この製品の機能については後述します。

- Oracle Advanced Security の概要
- Oracle Advanced Security のネットワーク・セキュリティ・サービス
- Oracle Advanced Security のエンタープライズ・ユーザー・セキュリティ機能
- Oracle Advanced Security の PKI 実装

注意： Oracle Advanced Security リリース 8.1.6 は、米国連邦情報処理標準 140-1（FIPS）に基づいてレベル 2 のセキュリティ・レベルで検証済みです。これは重要な米国政府のセキュリティ査定であり、レベル 2 はソフトウェアの最高レベルです。これにより、Oracle Advanced Security が暗号化に関して厳しい政府基準に準拠していることが外部から立証されたことになります。

Oracle Advanced Security の概要

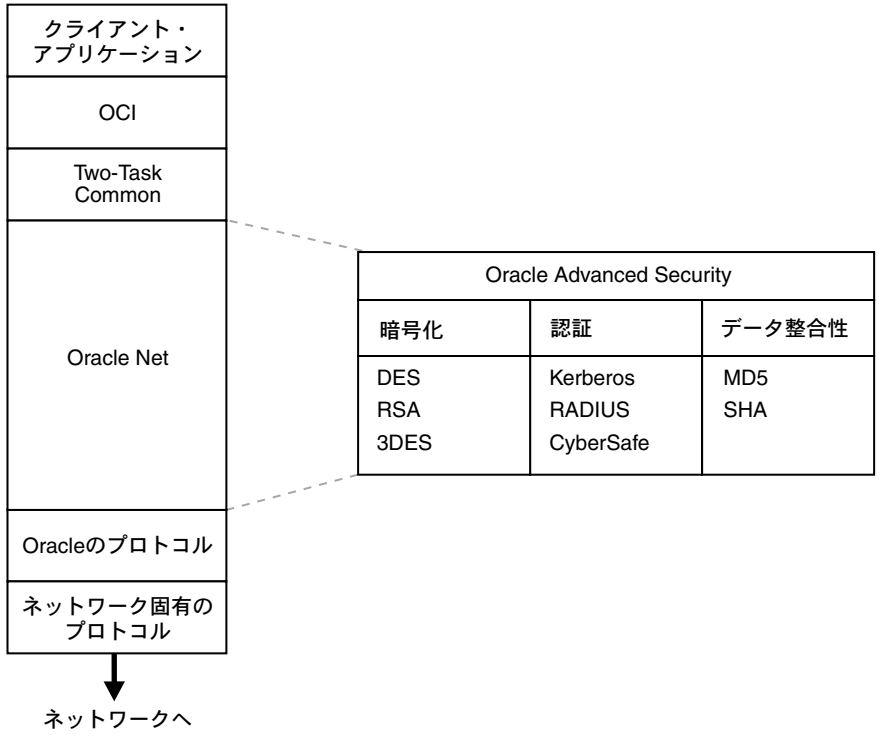
Oracle Advanced Security では、Oracle9*i* 用のセキュリティ・サービスを提供しています。この製品は、Oracle9*i* Enterprise Edition とともに購入できる別売オプションとして提供されます。

- Oracle Advanced Security は、すべてのネットワーク・プロトコルのデータ暗号化と整合性を Oracle データベースに提供します。これには、システム固有の暗号化機能を持つ Oracle Net、Oracle Net/SSL、IIOP/SSL および JDBC Thin クライアント用の Java ベースの暗号化が含まれます。
- この製品は、サード・パーティの認証、認可およびシングル・サインオン・サービスと統合されます。
- 公開鍵インフラストラクチャ（PKI）を統合し、Secure Sockets Layer（SSL）や X.509 バージョン 3 証明書（サード・パーティの証明書サーバーにより提供）などの公開鍵ソリューションをサポートします。Oracle Wallet Manager や Oracle Enterprise Login Assistant などの関連ツールが提供されています。SSL ベースのシングル・サインオンのみでなく、証明書ベースのサーバー間認証およびデータベース・リンクが可能になります。また、Entrust PKI とも統合されます。
- Oracle Advanced Security では、LDAP バージョン 3 準拠のディレクトリ・サーバーを使用してユーザー管理が集中化され、Oracle Enterprise Security Manager によってエンタープライズ・ユーザーとエンタープライズ・ロールが管理されます。ユーザーと認可の格納に関して Oracle Internet Directory を制限付きで使用できるようにし、ロール管理用の Microsoft Active Directory とも統合されます。

Oracle Advanced Security はデフォルトでインストールされますが、Oracle9*i* Enterprise Edition の別売オプションであり、使用する場合は購入する必要があります。このライセンス要件は、セキュリティ機能を Java Beans（IIOP/SSL 経由の EJB）または Oracle Net/SSL によるデータベース・エンタープライズ・ユーザーとの併用を希望している顧客にも影響します。ただし、RDBMS への HTTPS（HTTP/SSL）接続のみは例外で、Oracle Advanced Security のライセンスは不要です。

図 9-2 に、Oracle ネットワーキング環境での Oracle Advanced Security のアーキテクチャを示します。

図 9-2 Oracle ネットワーク環境における Oracle Advanced Security



Oracle Advanced Security では、既存の Oracle Protocol Adapters と同様のアダプタによって認証をサポートしています。

関連項目： Oracle ネットワーク環境でのスタック通信の詳細は、『Oracle9*i* Net Services 管理者ガイド』を参照してください。

Oracle Advanced Security のネットワーク・セキュリティ・サービス

Oracle Advanced Security には、データ送信のプライバシを保護するために、複数の方法が用意されています。

- Oracle Net Services 固有の暗号化
- Oracle Advanced Security のデータ整合性機能
- Secure Sockets Layer（SSL）の暗号化機能
- Oracle Advanced Security の Java 暗号化機能
- Oracle Advanced Security でサポートされる厳密認証方式
- Oracle Advanced Security でのシングル・サインオンの実装

Oracle Net Services 固有の暗号化

Oracle Advanced Security では、送信中に誰もデータを読み取れないように、ネットワークの通信を暗号化することでデータ・プライバシが保証されます。

Oracle Advanced Security には、業界標準の複数の暗号化アルゴリズムとチェックサム・アルゴリズムが用意されており、特定のシステム要件に基づいて選択できます。ネットワークの暗号化方式を選択できるため、各種のデータ転送に様々なセキュリティ・レベルおよびパフォーマンス・レベルを使用できます。

暗号の強度はキー管理に応じて異なるため注意してください。Oracle Advanced Security では、公開鍵に基づく Diffie-Hellman キー折衝アルゴリズムを使用して、暗号化とデータ整合性をもたらすために安全なキーの配布が実行されます。暗号化を使用して暗号化されたデータのセキュリティを保護する場合は、複合キーの影響を最小限に抑えるために、キーを頻繁に変更する必要があります。このため、Oracle Advanced Security のキー管理機能では、セッション・キーがセッションごとに変更されます。Oracle Advanced Security では、Diffie-Hellman Key Exchange は自動的に行われるため、暗号化システムに関連する管理上の問題は発生しません。

Oracle Advanced Security の旧バージョンでは Domestic、Upgrade および Export という 3 つのエディションが用意されており、それぞれ暗号キーの長さが異なっていました。従来は米国版の Domestic エディションでのみ使用可能でしたが、リリース 9.0.1 では、世界中の Oracle ユーザーのために、使用可能な暗号化アルゴリズムとキー長がすべて含まれています。この製品の旧バージョンを配置しているユーザーは、特定の製品リリースの米国版 Domestic エディションを入手できます。

注意： 米国政府は、暗号化製品に関する輸出ガイドラインを緩和しています。それに応じて、オラクル社は Oracle Advanced Security に最も強力な暗号化機能を組み込んで、事実上世界中のすべてのユーザーに出荷できるようになりました。

Oracle Advanced Security には、業界標準のアルゴリズムと暗号の FIPS 準拠の実装が付属しており、暗号化の実装に通常伴う複雑な作業を簡素化できます。次の業界標準の暗号化アルゴリズムがサポートされます。

表 9-1 暗号化アルゴリズム

名前	説明
RSA 暗号化	RSA 暗号化モジュールでは、RSA Security 社の RC4 暗号化アルゴリズムが使用されます。Oracle の最適化された実装は、パフォーマンスの低下を最小限に抑えて高度なセキュリティを提供します。RC4 アルゴリズムの場合、Oracle には 40 ビット、56 ビット、128 ビットおよび 256 ビットの暗号キー長が用意されています。
DES 暗号化	Oracle Advanced Security では、標準的で最適化された 56 ビット・キー暗号化アルゴリズムとともに DES が実装され、下位互換性のために 40 ビット・バージョンである DES40 も提供されます。
Triple-DES 暗号化	Oracle Advanced Security では、Triple-DES（3DES）暗号化もサポートされます。これには 2 キー・バージョンと 3 キー・バージョンがあり、有効なキー長はそれぞれ 112 ビットと 168 ビットです。どちらのバージョンも、暗号ブロック連鎖（CBC）モードで動作します。

Oracle Advanced Security では、キー管理と暗号化の複雑さは管理者とユーザーから隠されています。ユーザーは少数の単純なステップを実行するのみで、Oracle Advanced Security の暗号化を構成できます。Oracle Net Manager の Graphical User Interface（GUI）ツールを使用して暗号化アルゴリズムを選択する方法と、`sqlnet.ora` の 6 つのパラメータを手動で設定する方法があります。構成後の暗号化は、ユーザーに対して透過的です。

Oracle Advanced Security の暗号化に関連するオーバーヘッドはほとんどありません。パフォーマンスは（オペレーティング・システム、選択した暗号化アルゴリズムおよび他の要因に応じて）変動しますが、パフォーマンス・テストでは低下が 10 分の 1 秒程度であることを示しています。

Oracle Advanced Security のデータ整合性機能

Oracle Advanced Security では、順序付きの暗号チェックサムによりデータ整合性が保証されます。データが送信中に変更、削除または再生されていないことを保証するために、Oracle Advanced Security ではオプションで、MD5 アルゴリズムを使用した暗号チェックサムを通じて、暗号で保護されたメッセージ・ダイジェストが生成され、それがネットワーク経由で送信される各パケットに組み込まれます。または、SHA-1 を（SSL とともに）使用することもできます。データ整合性アルゴリズムによるオーバーヘッドの増加はほとんどなく、データ変更アタック、パケットの削除および再生アタックから保護されます。

Secure Sockets Layer（SSL）の暗号化機能

Oracle Advanced Security には、この項で説明するように SSL 暗号化機能が用意されています。

Oracle Advanced Security による SSL のサポート

Oracle Advanced Security の SSL 機能を使用すると、クライアントとサーバー間の通信を保護できます。これには、Oracle Net Services、LDAP、JDBC OCI および IIOP 形式のデータが含まれます。SSL 暗号化は、Oracle Advanced Security でサポートされる固有の Oracle Net Services の暗号化プロトコルの代替手段をユーザーに提供します。SSL のメリットは、インターネットのデファクト・スタンダードとなっており、Oracle Net Services 以外のプロトコルを使用するクライアントで使用できることです。

Oracle Advanced Security の SSL サポートにより、ネットワークの通信が暗号化され、整合性チェックと Oracle クライアントおよびサーバーの認証が実行され、Oracle 環境に公開鍵ベースのシングル・サインオンが取り込まれます。SSL は、認証、暗号化およびデータ整合性タイプのセットである暗号パッケージを使用して、暗号化とデータの整合性を提供します。クライアントとサーバーには、それぞれがサポートする暗号パッケージ（認証用の RSA、暗号化用の 3DES およびデータ整合性用の SHA-1 など）のリストがあります。両者は、接続中にどれを使用するかを折衝します。

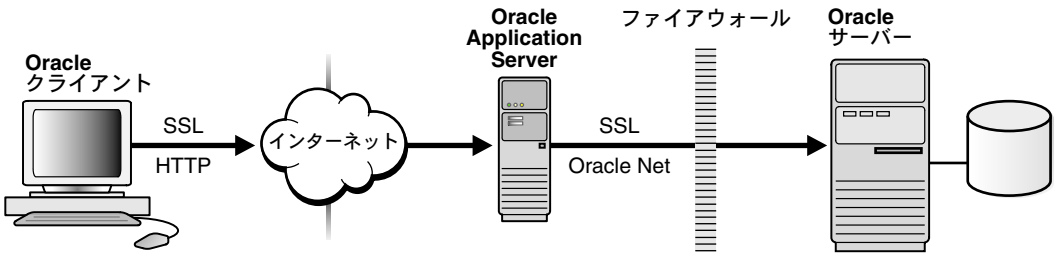
Oracle Advanced Security による SSL でのチェックサム

Oracle Advanced Security の SSL 機能では、MD5 と Secure Hash Algorithm（SHA）を使用できます。SHA は MD5 よりも若干低速ですが、メッセージ・ダイジェスト値が大きくなることで、激しい衝突や反転アタックに対してより強力に保護できます。

Oracle9*i* Application Server の SSL サポート

Oracle9*i* Application Server では、Thin クライアントと Oracle9*i* Application Server 間、および Oracle9*i* Application Server と Oracle9*i* データベース・サーバー間の SSL 暗号化がサポートされます。

図 9-3 SSL によるインターネットと Oracle 通信の保護



関連項目：

- 3-6 ページ「Secure Sockets Layer（SSL）プロトコル」
- 8-5 ページ「Secure Sockets Layer 認証と X.509v3 デジタル証明書」

Oracle Advanced Security の Java 暗号化機能

Sun 社は Java Database Connectivity（JDBC）規格を定義しており、オラクル社はプロバイダとしてこの規格を独自の JDBC ドライバとともに実装し、拡張しています。Oracle には、次の 4 種類の JDBC ドライバが用意されています。

- OCI ライブラリと Oracle Net Services クライアントの最上位に組み込まれた JDBC OCI ドライバ
- アプレットおよびアプリケーション用の JDBC Thin ドライバ（クライアント・インストレーションはなく、最大の移植性を提供）
- ターゲット・データベース内部からリモート Oracle データベースに接続するための JDBC サーバー側 Thin ドライバ
- データベース内部で実行するストアド・プロシージャやファンクションなどのコードためのサーバー側内部ドライバ

JDBC OCI ドライバ

JDBC OCI ドライバは、クライアント側とサーバー側の両方で Oracle Net Services 通信スタック全体を使用するため、既存の Oracle Advanced Security の暗号化メカニズムと認証メカニズムを活用できます。Oracle9*i* では、プロキシ認証が Java Database Connectivity（JDBC OCI）に拡張されており、中間層サーバーはクライアント・ユーザー用の軽量セッションを確立し、そのユーザーのかわりに Oracle9*i* データベースにアクセスできます。

Thin JDBC

Thin JDBC ドライバはインターネット経由で使用されるダウンロード可能なアプレットと併用するように設計されているため、Oracle9*i* には、Thin クライアントで使用できるように Oracle Advanced Security の暗号化および整合性アルゴリズムの 100% の Java 実装が組み込まれています。次のようなメリットにより、Oracle と他のコンポーネントを配置している E-Business では、多様なチャネルを介して様々な情報を安全に送信できます。

- 通信のプライバシのためのデータ暗号化
- データを変更、再生および盗聴から保護するためのデータ整合性チェック
- JDBC Thin クライアントから Oracle9*i* データベースへの保護接続
- 開発者が保護通信チャネルを介してデータを送信するアプレットを構築するための機能
- Oracle9*i* データベースから旧バージョンの Oracle Advanced Security 対応データベースへの保護接続
- JavaServer Pages（JSP）搭載の中間層サーバーから Oracle RDBMS への保護接続

Oracle JDBC Thin ドライバは、認証用の Oracle パスワード・プロトコルを実装します。Oracle Advanced Security の SSL 実装も、RADIUS や Kerberos のようなサード・パーティの認証機能もサポートされません。Oracle JDBC OCI ドライバでは、すべての Oracle Advanced Security 機能がサポートされます。

Oracle Advanced Security では、C で記述されたアルゴリズムを使用して、Oracle Net Services クライアントと Oracle サーバー間の Oracle Net Services の通信が絶えず暗号化され、整合性がチェックされます。Oracle Advanced Security の JDBC Thin 用の Java 実装には、次の暗号化アルゴリズムの Java バージョンが用意されています。

- RC4_256
- RC4_128
- RC4_56
- RC4_40
- DES56
- DES40

事実上すべてのクライアント用の保護接続

サーバー側では、アルゴリズムの折衝とキーの生成が Oracle Advanced Security の Oracle Net Services 暗号化と同様に機能するため、クライアントとサーバーの下位互換性と上位互換性が有効になります。クライアント側では、アルゴリズムの折衝とキーの生成は C ベースの Oracle Advanced Security 暗号化と同じ方法で発生します。クライアントとサーバーは、従来の Oracle Net Services クライアントと同じ方法で暗号化アルゴリズムを折衝し、乱数を生成し、Diffie-Hellman を使用してセッション・キーを交換し、Oracle パスワード・プロトコルを使用します。JDBC Thin には、Pure Java による Oracle Net Services クライアントの

実装全体が含まれています。Oracle Advanced Security の Java 実装には、他の暗号化の実装との一貫性があり、暗号アルゴリズムへのアクセスを防止し、データの二重暗号化やネットワーク経由で渡されるデータの暗号化を不可能にします。ユーザーは、キースペースの変更も暗号化アルゴリズム自体の変更もできません。

関連項目： 3-8 ページ「Java Database Connectivity（JDBC）」

Oracle Java SSL

Oracle Java SSL は、Java Secure Socket Extension（JSSE）の市販グレードの実装です。安全で高速な SSL 実装を作成するために、Oracle Java SSL ではシステム固有のコードを使用して重要なコンポーネントのパフォーマンスを改善します。Oracle Java SSL では、JSSE 仕様に含まれている機能に加えて次の機能がサポートされます。

- 複数の暗号アルゴリズム
- Oracle Wallet Manager を使用した証明書およびキー管理
- 認証など、Oracle Java SSL の最上位に組み込まれたアプリケーションで使用できる SSL 固有のセッション機能

関連項目：『Oracle Advanced Security 管理者ガイド』

Oracle Advanced Security でサポートされる厳密認証方式

Oracle Advanced Security では、複数のサード・パーティの認証サービスを介し、SSL をデジタル証明書と併用して、強化されたユーザー認証が提供されます。これらのオプションの多くでは集中化された認証が使用され、分散環境におけるユーザー、クライアントおよびサーバーの識別情報に高度な信頼性をもたらします。また、トークン・カードなどのテクノロジを統合し、ユーザーの個別性を証明することで拡張された認証を提供します。ユーザー認証は Oracle9*i* の機能であり、Oracle Advanced Security でサポートされる認証方式を使用することで大幅に拡張されます。

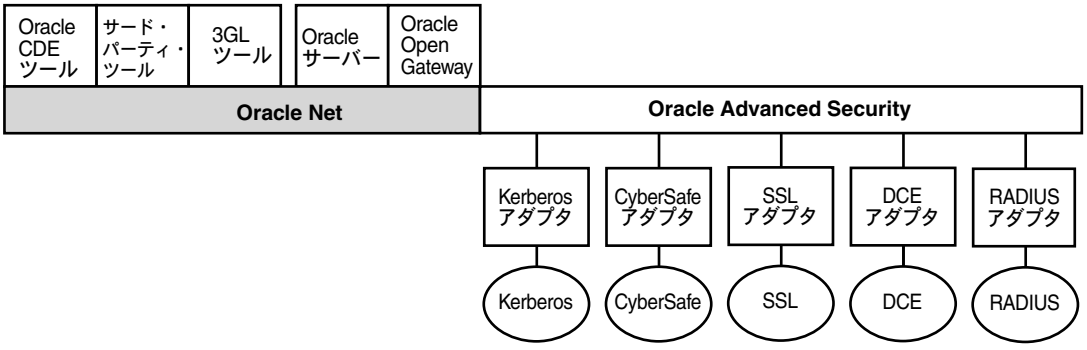
サポートされる認証方式は、次のとおりです。

- Oracle の公開鍵インフラストラクチャ・ベースの認証
  - Oracle Advanced Security での Secure Sockets Layer（SSL）認証
  - Oracle Advanced Security での Entrust/PKI のサポート
  - Oracle Advanced Security での標準的な PKI のサポート
- Oracle Advanced Security と RADIUS
- Oracle Advanced Security と Kerberos および CyberSafe
- Oracle Advanced Security とスマート・カード
- Oracle Advanced Security とトークン・カード

- Oracle Advanced Security とバイオメトリック認証
- Oracle Advanced Security と分散コンピューティング環境（DCE）

図 9-4 に、Oracle Advanced Security の厳密認証コンポーネントの一部を示します。認証アダプタは Oracle Net Services インタフェースの下で統合され、既存のアプリケーションを変更せずに新しい認証システムを透過的に活用できるようにします。

図 9-4　認証アダプタと Oracle Net Services



関連項目： 4-3 ページ「厳密認証」

Oracle の公開鍵インフラストラクチャ・ベースの認証

Oracle には、公開鍵と証明書を使用できるように公開鍵インフラストラクチャ（PKI）が用意されています。この項では、Oracle の PKI 認証機能の概要を説明します。

- Oracle Advanced Security での標準的な PKI のサポート
- Oracle Advanced Security での Secure Sockets Layer（SSL）認証
- Oracle Advanced Security での Entrust/PKI のサポート

Oracle Advanced Security での標準的な PKI のサポート

Oracle9*i* では、証明書要求とインストール用に、標準的な X.509 バージョン 3 証明書および関連 Public Key Certificate Standards（PKCS）がサポートされます。このため、ユーザーはこれらの規格をサポートしている認証局（CA）であれば、どこの証明書でも要求できます。また、ユーザーは選択した CA からの信頼できるルート証明書をインストールでき、サーバーはその CA から発行された証明書を認識して検査できます。オラクル社は VeriSign 社や Baltimore Technologies 社などの PKI サービスおよび製品の大手ベンダーと協力して、CA の信頼できるルートが Oracle9*i* に事前にインストールされ、顧客がこれらのベンダーからの証明書を使用してそのまま Oracle9*i* に対して認証を受けられることを保証しています。

関連項目： 9-37 ページ「Oracle Advanced Security の PKI 実装」

Oracle Advanced Security での Secure Sockets Layer（SSL）認証

Oracle Advanced Security の SSL を使用して次の認証ができます。

- 1 つ以上の Oracle サーバーに対してすべてのクライアントまたはサーバーを認証
- すべてのクライアントに対して単一の Oracle サーバーを認証

Oracle9*i* と同様に、X.509 証明書による匿名、サーバーのみおよびクライアント / サーバー認証がサポートされます。

SSL 機能は、単独で使用しても、Oracle Advanced Security でサポートされる他の認証方式と併用してもかまいません。たとえば、SSL を Kerberos と併用し、SSL で提供される暗号化を Kerberos の認証方式とともに使用できます。

ユーザーと管理者は、Oracle Wallet Manager を使用して SSL 用のデジタル証明書を管理します。Oracle Wallet Manager を使用すると、ユーザーとデータベース管理者は各自の Wallet の内容を制御できます。また、管理者は Wallet を LDAP 準拠のディレクトリ内で一元的に管理できます。Oracle Enterprise Login Assistant は使用しやすいツールであり、エンド・ユーザーが Wallet をオープンして SSL 経由でログインを実行できるように用意されています。このツールにより、ユーザーは認証用の証明書を使用して、シングル・サインオンを単純で透過的に実行できます。Wallet と管理ツールは、証明書、秘密鍵および証明書サーバーに対する要求を安全に格納して管理するために併用されます。

関連項目：

- 8-5 ページ「Secure Sockets Layer 認証と X.509v3 デジタル証明書」
- 9-39 ページ「Oracle Wallet Manager」

Oracle Advanced Security での Entrust/PKI のサポート

Oracle Advanced Security を使用すると、オラクル社と Entrust Technologies 社の顧客は、どちらも Oracle アプリケーションに Entrust ベースのシングル・サインオンを取り込むことができます。Entrust/PKI との統合により、Oracle では広範囲なキー管理、証明書の失効および Entrust の他の機能を必要とする大口顧客に、X.509 ベースのシングル・サインオンを提供する機能が拡張されます。

Oracle Advanced Security では、証明書と秘密鍵の保管、および保護証明書管理のための Entrust のメカニズムである Entrust Profile がサポートされます。Oracle Advanced Security では、Oracle Wallet からユーザーの資格証明（秘密鍵と証明書）にアクセスするかわりに、認証とシングル・サインオンのためにユーザーの Entrust Profile にアクセスできます。Entrust を統合するには、Entrust Authority 5 が必要です。

関連項目： 8-6 ページ「Entrust/PKI 認証」

Oracle Advanced Security と Kerberos および CyberSafe

Oracle Advanced Security による Kerberos および CyberSafe のサポートは、Oracle ユーザーのシングル・サインオンと集中化された認証というメリットをもたらします。

注意： Kerberos 用の Oracle 認証では、データベース・リンク認証（プロキシ認証とも呼ばれます）が提供されます。CyberSafe では、プロキシ認証はサポートされません。

関連項目： 4-4 ページ「Kerberos および CyberSafe」

Oracle Advanced Security と RADIUS

RADIUS（Remote Authentication Dial-In User Service）のサポートは、Oracle の顧客に主に 2 つのメリットをもたらします。第 1 に、トークン・カード、スマート・カードおよび要求 / 応答などの認証テクノロジをサポートできるようになります。第 2 に、Oracle9*i* データベース・サーバーを RADIUS クライアントにすることで既存のシステムに迅速に統合でき、組織がすでに行ったインフラストラクチャと投資を資本化できます。

RADIUS を使用すると、ネットワーク・ユーザーの認証に使用可能な事実上すべてのメカニズムを選択できます。トークン・カードとスマート・カードの多数のメーカーが RADIUS をサポートしており、RADIUS 準拠のデバイスはどれでも Oracle Advanced Security と統合でき、認証プロバイダから要求される変更はほとんどなしに Oracle ユーザーを認証できます。多数の組織がネットワークへのリモート・アクセス用に RADIUS を実装しているため、簡単に Oracle を既存のシステムに統合し、組織がすでに行った投資を活用できます。

サード・パーティの認証ベンダーは、Oracle Advanced Security とともに出荷される Java インタフェース・クラスをカスタマイズして、クライアントの Graphical User Interface（GUI）を実装できます。次のベンダーの製品は、RADIUS インタフェースを使用して Oracle Advanced Security と統合されています。

- ActivCard 社の ActivRadius、ActivCard Gold Tokens および Smart Cards
- Lucent Technologies 社の Radius Server
- RSA ACE/Server。これは RADIUS サーバーであり、SecurID トークンにより RADIUS インタフェースを介して Oracle ユーザーが認証されます。
- SafeWord RADIUS サーバーおよび SafeWord トークンなど、Secure Computing 社の SafeWord 製品。
- Funk Software Steel Belted Radius。サード・パーティの認証ベンダーが認証バックエンドを記述するための API を提供します。

関連項目： 4-4 ページ「RADIUS」

Oracle Advanced Security とトークン・カード

トークン・カード・テクノロジにより、ユーザー認証が拡張されます。Oracle Advanced Security では、RSA の SecurID トークンがサポートされます。このトークンにより、2 つの要素による認証を通じてセキュリティが強化されます。ユーザーは、PIN を知っていることと SecurID 電子トークン・カードを持っていることが要求されます。また、Oracle Advanced Security での RADIUS サポートにより、多様なトークン・カードとの統合が許されます。組織は、権限なしでの使用からネットワークを保護するために使用するトークンを選択できます。

関連項目： 4-5 ページ「トークン・カード」

Oracle Advanced Security とスマート・カード

Oracle Advanced Security は、Oracle ユーザーを認証するために、RADIUS 準拠のスマート・カードと統合されます。スマート・カードは、強力なセキュリティ・デバイスとして一般的になりつつあります。プロセッサが組み込まれているため、動的なパスワードを生成できます。また、メモリーが組み込まれているため、ユーザー名、証明書または医療記録などのデータを格納する場合に役立ちます。スマート・カードは普及しつつあり、ユーザー ID の証明をスマート・カードに依存している組織では、ユーザーが Oracle に接続するとき、認証に使用できます。

関連項目： 4-6 ページ「スマート・カード」

Oracle Advanced Security とバイオメトリック認証

RADIUS をサポートしているバイオメトリック・デバイスのベンダーは、Oracle Advanced Security と統合できます。厳密認証を必要とするクライアントやサーバーに配置されたバイオメトリック・デバイスは、個人の物理特性に基づいてユーザー認証を提供します。

Oracle Advanced Security と分散コンピューティング環境（DCE）

分散コンピューティング環境（DCE）の統合により、ユーザーは Oracle のツール製品やアプリケーションを透過的に使用して、DCE 環境で Oracle9*i* データベースにアクセスできます。Oracle Advanced Security では、Solaris、Windows、HP、AIX など、特定のプラットフォームで OSF の DCE 1.0 がサポートされます。

Oracle ネットワークを一部またはすべての DCE サービスと統合できます。これには、セキュリティ・サービス、認証とシングル・サインオン、集中的な認可管理のための DCE グループへの Oracle ロールのマッピングが含まれます。

関連項目： 4-7 ページ「分散コンピューティング環境（DCE）」

Oracle Advanced Security でのシングル・サインオンの実装

Oracle Advanced Security では、分散環境で保護シングル・サインオン機能がサポートされることにより、複数のパスワードのメンテナンス作業が最小限ですみます。ユーザーは 1 日に一度ログオンすれば、ユーザー名やパスワードを再入力せずに他のサービスに自動的に接続できます。このため、ユーザーは複数のパスワードを覚えたり管理する必要がなくなり、複数のサービスにログインする時間を節約できます。また、システム管理者にとっては、ユーザーのアカウントとパスワードの管理作業が簡素化されます。

集中的な認証により、シングル・サインオンが可能になります。次のように異なる構成がサポートされます。

- サード・パーティ製品とのシングル・サインオン構成
- PKI ベースのシングル・サインオン構成

関連項目：

- 4-10 ページ「シングル・サインオン」
- 8-7 ページ「PKI を使用したシングル・サインオン」
- 9-56 ページ「Oracle9i Application Server でのシングル・サインオン」

サード・パーティ製品とのシングル・サインオン構成

Oracle Advanced Security は、シングル・サインオン機能をサポートするために、複数の異なるテクノロジと統合されています。これには Kerberos、CyberSafe および DCE が含まれます。

PKI ベースのシングル・サインオン構成

Oracle Advanced Security では、LDAP バージョン 3 準拠のディレクトリ・サービスとの統合により、Oracle ユーザー用に SSL ベースのシングル・サインオンと Entrust ベースのシングル・サインオンが用意されています。統合されたディレクトリ・サービスと Oracle PKI 実装の組合せにより、Oracle9*i* データベースでの SSL ベースのシングル・サインオンが有効になります。シングル・サインオンにより、ユーザーが一度認証を受ければ、以降の接続はデジタル証明書を使用して確立できます。

Oracle Advanced Security のエンタープライズ・ユーザー・セキュリティ機能

エンタープライズ・ユーザーのセキュリティ機能は、ユーザー関連情報の格納と管理を LDAP 準拠のディレクトリ・サービスに集中化して、ユーザー、管理およびセキュリティの要求に対処します。このような環境では、従業員のジョブに変更があった場合も、管理者は 1 箇所、つまりディレクトリで情報を変更するのみで、複数のデータベースとシステムを効率的に変更できます。この集中化により、管理コストが大幅に削減され、企業のセキュリティが実質的に改善されます。

このリリースでは、エンタープライズ・ユーザーのセキュリティが拡張されており、3 層環境がサポートされます。Oracle9*i* のプロキシ認証機能により、次が使用可能になっています。

- 複数層を通じたユーザー名とパスワードのプロキシ
- 複数層を通じた X.509 証明書と識別名の証明によるプロキシ

この組合せは、SSL 認証を受けるエンタープライズ・ユーザーとパスワード認証を受けるエンタープライズ・ユーザーの両方に適用されるため注意してください。

この項の内容は次のとおりです。

関連項目：『Oracle9*i* アプリケーション開発者ガイド ― 基礎編』

パスワード認証を受けたエンタープライズ・ユーザー

Oracle Advanced Security では、2 種類のエンタープライズ・ユーザー、つまり、SSL による認証を受けるエンタープライズ・ユーザーと、パスワードで認証を受けるユーザーを使用できます。

SSL 認証を受けたユーザーは、Secure Sockets Layer バージョン 3 経由で業界標準の相互運用可能な X.509 バージョン 3 証明書を使用して、Oracle9*i* へのシングル・サインオンによる利点を得ることができます。

また、Oracle Advanced Security にはエンタープライズ・ユーザー向けにパスワード・ベースの認証も実装されており、クライアント側 Wallet およびほとんどの Secure Sockets Layer（SSL）処理の要件がなくなります。（データベースと Oracle Internet Directory 間の接続を保護するには、従来どおり SSL が必要です。）パスワード認証を受けたエンタープライズ・ユーザーは、LDAP 準拠のディレクトリに安全に格納されている同じパスワードを使用し、複数のデータベースに対して自己認証できます。管理者は、両方のタイプのユーザーを 1 つのディレクトリで管理できます。

処理オーバーヘッドの削減、使用しやすさの向上およびセットアップと管理の簡素化などのメリットがあるため、パスワード認証を受けたエンタープライズ・ユーザーは、複数のアプリケーションにアクセスする大規模なユーザー・コミュニティに特に役立ちます。Oracle Advanced Security では、従来のすべての Oracle クライアント・バージョンについて、パスワード・ベースの認証によるエンタープライズ・ユーザーのログインがサポートされます。また、エンタープライズ・ユーザーは、必要に応じて単一のエンタープライズ・ユーザー名とパスワードを使用し、複数のデータベースに接続できます。

シングル・サインオンを使用すると、ユーザーは一度認証を受けるのみですみます。これに対して、単一パスワード機能の場合、ユーザーは多数の異なるデータベースに同じパスワードを使用できますが、パスワードを何度も入力する必要があります。

関連項目： 6-4 ページ「パスワード認証を受けたエンタープライズ・ユーザー」

エンタープライズ・ユーザー・セキュリティ用のツール

Oracle Advanced Security には、3 つの Graphical User Interface（GUI）が用意されています。これらのツールを使用すると、複数のアプリケーションにアクセスする大規模なユーザー・コミュニティを管理でき、ユーザーによるログインも簡単になります。

- Oracle Enterprise Security Manager
- Oracle Wallet Manager
- Oracle Enterprise Login Assistant

関連項目： 各ツールの詳細は、9-38 ページの「Oracle の公開鍵インフラストラクチャ・ベースの認証のコンポーネント」を参照してください。

Oracle Advanced Security の共有スキーマ

共有スキーマ（旧称は非スキーマ依存ユーザー）を使用すると、複数のエンタープライズ・ユーザーが単一のデータベース・スキーマを共有できます。この方法では、同じユーザーを各データベースに作成する必要がありません。この方法でディレクトリを使用するメリットは、ユーザー・アカウント数が減少することです。アプリケーション開発者は、ユーザー・アカウントを統合し、ユーザー管理の規模をインターネットまで拡張できます。

関連項目： 6-3 ページ「共有スキーマ」

現行ユーザーのデータベース・リンク

Oracle Advanced Security には、SSL 対応データベースおよびエンタープライズ・ユーザー向けに、新しいタイプのデータベース・リンクが用意されています。現行ユーザーのデータベース・リンクを使用すると、ユーザーは次のデータベースにプロシージャ所有者（または接続ユーザー）として接続できます。現行ユーザーは、次のデータベースにあるプロシージャ所有者の表にアクセスできます。

この機能は、サーバー間に SSL 相互認証を提供します。データベースは、アクセス制御などに関して相互を信頼できます。データベース・リンクを使用するには、データベースにエンタープライズ・ユーザーと SSL を実装する必要があります。Distributed_Trust_Admin パッケージで実装された SSL をデータベース・リンクと併用すると、データベース管理者によるファイングレイン・アクセス・コントロールが可能になります。

ディレクトリの統合

Oracle Advanced Security のライセンスには、エンタープライズ・ユーザー、パスワード、Oracle の Wallet およびエンタープライズ・ロールの格納のための Oracle Internet Directory の使用が含まれています。Oracle Internet Directory は、Oracle Advanced Security の他のコンポーネントと連動し、集中化されたユーザー管理および認証を実現します。Oracle Enterprise Security Manager は、ディレクトリにユーザー・エントリを作成し、そのユーザーの認証を管理できるように用意されています。

Oracle Advanced Security では、Microsoft Active Directory もサポートされます。

関連項目：

- 第 6 章「エンタープライズ・ユーザーのセキュリティの管理」
- 9-44 ページ「Oracle Internet Directory」

Oracle Advanced Security の PKI 実装

Oracle にはセキュリティの実装用に様々な選択肢が用意されており、公開鍵インフラストラクチャ（PKI）アプローチはその 1 つにすぎません。PKI は、セキュリティとシングル・サインオンを達成し、Oracle Advanced Security オプションに付加価値をもたらすために生まれた手段です。たとえば、RSA RC4 暗号化を使用するには、システム固有の暗号化コンポーネント用または SSL ベースの暗号化用に Oracle Advanced Security を使用できます。パスワード、スマート・カードおよび X.509 証明書など、様々な認証方式から選択できます。この項の内容は次のとおりです。

- Oracle の公開鍵インフラストラクチャ・ベースの認証のコンポーネント
- PKI の統合と相互運用性
- Oracle の PKI 実装のまとめ

Oracle の公開鍵インフラストラクチャ・ベースの認証のコンポーネント

Oracle9*i* の PKI 実装では、PKI 関連コンポーネントに関する業界標準の仕様に従って安全な情報交換が確立されます。次に説明するように、製品および機能のパッケージ全体が取り込まれます。

Secure Sockets Layer

このプロトコルは、公開鍵暗号を使用して認証、保護セッション・キー管理、暗号化およびデータ整合性を提供します。

Oracle Call Interface

Oracle Call Interface（OCI）および PL/SQL ファンクションは、秘密鍵と証明書を使用してユーザー指定のデータに署名し、信頼できる証明書を使用してデータの署名を検証するために使用されます。

信頼できる証明書

信頼できる証明書は、信頼度の高いサード・パーティによる識別情報です。信頼という言葉は、エンティティが本人であるという識別情報の確認が行われるときに使用されます。一般的に、信頼されている認証局によってユーザーの証明書が発行されます。複数レベルの信頼できる証明書がある場合、証明連鎖における下位レベルの信頼できる証明書は、それより上のレベルの証明書をすべて再検証する必要はありません。Oracle Advanced Security では、信頼できる証明書が VeriSign、RSA、Entrust および GTE CyberTrust から自動的にインストールされます。

X.509 バージョン 3 証明書

この種の証明書は、エンティティの公開鍵が、信頼されている機関（Oracle 外部の信頼されている認証局）によって署名されたときに有効となります。証明書には、ユーザーまたはサービスの識別情報、公開鍵および認証を可能にするために使用される他の情報が含まれています。この証明書は、そのエンティティの情報が正しいこと、および公開鍵がそのエンティティに実際に属していることを保証するものです。証明書は、認証が有効になるように Oracle Wallet にロードされます。

Oracle Wallets

Oracle の Wallet は、認証局でリアルタイムでチェックせずにすむように、証明書および信頼できる証明書が格納され、管理されるコンテナです。これらのデータ構造には、ユーザーの秘密鍵、ユーザー証明書および信頼できる証明書のセット（ユーザーが信頼しているルート証明書のリスト）が安全に格納されます。

Oracle Wallet Manager

セキュリティ管理者が、Oracle クライアントとデータベース・サーバーにおける公開鍵のセキュリティ資格証明の管理に使用する、Java ベースのアプリケーションです。このアプリケーションでは、Oracle Enterprise Login Assistant を使用して開くことのできる Oracle の Wallet が作成されます。

Oracle Wallet Manager では、公開鍵 / 秘密鍵のペアが作成され、ユーザー用の証明書が管理されます。認証局に対して PKCS#10 証明書要求が発行され、証明書が Wallet にインストールされます。VeriSign、RSA および GTE CyberTrust からの信頼できる証明書とともに出荷され、サイト独自の社内認証局を使用できます。

Oracle Enterprise Login Assistant

Oracle Enterprise Login Assistant は Java ベースのツールで、アプリケーションの保護 SSL ベースの通信を有効化または無効化するためにユーザーおよび Wallet を開閉します。このツールには、SSL 認証を受けたユーザー用のシングル・サインオン機能があります。また、クライアント / サーバー環境または 3 層環境では、シングル・サインオンおよび厳密認証というメリットがあります。パスワードで認証を受けるエンタープライズ・ユーザーは、そのパスワードをデータベースまたはディレクトリでのパスワード変更にも使用できます。

Oracle Internet Directory

この LDAP バージョン 3 準拠のディレクトリは Oracle9*i* データベース上に構築され、PKI ベースのシングル・サインオンを有効化できます。X.509 証明書を使用して認証を受けたユーザーについて、セキュリティ属性および権限など、ユーザーおよびシステム構成環境を安全に保護できます。Oracle Internet Directory では属性レベルのアクセス制御が施行され、ディレクトリでは特定の属性に対する読取り、書込みまたは更新権限を、指定した特定ユーザー（企業のセキュリティ管理者など）に限定できます。また、SSL 暗号化を介したディレクトリの問合せおよび応答の保護と認証もサポートされます。

Oracle Enterprise Security Manager

Oracle Enterprise Security Manager は、LDAP ディレクトリ内でエンタープライズ・ユーザーおよびエンタープライズ・ロールを集中的に管理するための Graphical User Interface（GUI）です。データベース管理者は、このツールを使用して次のように様々なタスクを実行できます。

- 新規のエンタープライズ・ドメインの作成。
- エンタープライズ・ドメイン内での登録済みユーザーと公開済みデータベースの割当て。
- エンタープライズ・ドメイン内での個別性のための、データベースに対するエンタープライズ・ロールの付与。これにより、ロールで LDAP がサポートされる場合は、Oracle Internet Directory にロールを格納し、そこから取得できます。また、Oracle スキーマおよび関連アクセス制御リストのインストールがサポートされていれば、他の LDAP バージョン 3 準拠のディレクトリ・サーバーにロールを格納できる場合もあります。

Oracle Enterprise Security Manager は、Oracle Enterprise Manager の外部で起動します。ユーザー数は数万に拡張され、様々なドメインにある数千のデータベースと、各データベースに接続するユーザーを管理できます。

PKI の統合と相互運用性

Oracle9*i* では、次の機能を通じて PKI の統合と相互運用性が拡張されます。

- PKCS #12 サポート
- Oracle Internet Directory に格納された Wallet
- 複数証明書サポート
- 強力な Wallet 暗号化

PKCS #12 サポート

Oracle Advanced Security では、PKCS #12 コンテナに格納された X.509 証明書がサポートされ、Oracle Wallet と Netscape Communicator 4.x や Microsoft Internet Explorer 5.x などのサード・パーティ・アプリケーションとの相互運用が可能になり、オペレーティング・システム間で Wallet を移植できるようになります。既存の PKI 証明書を持つユーザーは、それを PKCS#12 形式でエクスポートして Oracle Wallet Manager で再利用したり、その逆のことができます。したがって、PKCS#12 により相互運用性が向上し、組織にとっては PKI の配置コストの削減となります。

Oracle Internet Directory に格納された Wallet

Oracle Enterprise Security Manager では、ユーザーの Wallet がユーザー登録プロセスの一部として作成されます。この Wallet は、Oracle Internet Directory または他の LDAP 準拠のディレクトリに格納されます。Oracle Wallet Manager では Wallet を LDAP ディレクトリにアップロードし、そこから取り出すことができます。

Wallet を集中化された LDAP 準拠のディレクトリに格納することで、ユーザーのローミングがサポートされ、ユーザーは複数のロケーションやデバイスから各自の証明書にアクセスできます。このため、一貫した信頼度の高いユーザー認証が保証され、Wallet のライフ・サイクル全体で Wallet の集中管理が実現します。

複数証明書サポート

Oracle9*i* では、Oracle Wallet Manager と Oracle Enterprise Login Assistant で Wallet ごとに次のような複数の証明書がサポートされます。

- S/MIME による署名付きの証明書
- S/MIME 暗号化証明書
- コードによる署名付きの証明書

Oracle Wallet Manager では、単一人物のデジタル・エンティティに複数の証明書、つまり複数の秘密鍵のペアを使用することがサポートされます（それぞれの秘密鍵は 1 つの証明書とのみ一致できます）。このため、ユーザーの PKI 証明書が統合され、より安全に管理できます。

強力な Wallet 暗号化

X.509 証明書に関連付けられている秘密鍵は、保護チャネルでの強力な暗号化を必要とします。Oracle9*i* では、DES 暗号化がさらに強力な暗号化アルゴリズムである 3 キーの Triple-DES（3DES）に置き換えられており、Oracle Wallets に優れたセキュリティをもたらします。

Oracle の PKI 実装のまとめ

電子メールや E-Commerce などのアプリケーションを保護するために、公開鍵インフラストラクチャが配置されることが多くなるにつれて、PKI は企業にとって最も重要な投資対象となってきています。すべてのクライアント、アプリケーション・サーバーおよびデータベース・サーバーは相互に自己認証できるため、PKI はネットワークに重要なセキュリティ・インフラストラクチャをもたらします。

SSL は、Oracle Net のみでなく、Internet Inter-ORB Protocol（IIOP）のような他のプロトコルも保護します。Oracle Advanced Security は、Java サポートを利用して IIOP 接続を保護し、Oracle に Thin クライアントと Enterprise JavaBeans（EJB）を処理する機能を与えています。

Oracle Advanced Security で SSL がサポートされることで、クライアント、Web サーバーやアプリケーション・サーバーおよびすべての Oracle9*i* データベース間の保護エンド・ツー・エンド通信のループがクローズすることになります。たとえば、ユーザーが振込みのために金融機関に接続する場合は、パスワードや口座番号などの機密情報を正しいサーバーに提供していることを、確実に検証できる必要があります。SSL および公開鍵認証により、サーバーはその識別情報をユーザーのブラウザに対して検証でき、クライアントはサーバーに対して自己を識別できます。

現在、組織はネットワーク保護のためにアプリケーション・サーバーとファイアウォールを導入しつつあり、接続プロセスは拡張されています。同じ例では、財務情報をファイアウォールで保護された Oracle9*i* データベース・サーバーに格納できます。ユーザーは SSL を使用してデータベースに接続し、インターネット経由でアプリケーション・サーバーに接続します。接続要求はファイアウォール経由で Oracle Net（同じく SSL で保護）を通り、口座情報とともに安全な Oracle9*i* サーバーに渡されます。

証明書では、クライアントがサーバーに対して認証されるのみでなく、サーバーも他のサーバーに対して認証されます。これにより、サーバーの相互認証には保護データベース・リンクが使用され、システム全体のセキュリティが拡張されます。SSL の配置により、データベース・サーバーやアプリケーション・サーバーなど、すべてのクライアントおよびサーバーは、通信先となる他のすべてのマシンやサービスに対して、自己を識別する証明書を持つことになります。

オラクル社が提供する完全なパッケージには、ネットワーク経由で送信されるメッセージの盗聴、改ざんまたは偽造を防止する業界標準に準拠した方式が用意されており、ネットワークおよびイントラネットでクライアントとサーバーのシングル・サインオンと厳密認証を提供します。公開鍵インフラストラクチャは、IT 時代の E-Commerce を保護する手段の基盤です。

Oracle Label Security

Oracle Label Security は Oracle9*i* Enterprise Edition のアドオン・セキュリティ・オプションであり、独自のラベル・ベースのアクセス制御ポリシーをカスタマイズできます。Oracle Policy Manager は、この製品に付属する簡便な Graphical User Interface（GUI）です。

図 9-5 Oracle Label Security

GRADE	RATE	ROW LABEL
Manager	600	UNCLASSIFIED
Senior	400	UNCLASSIFIED
Director	750	HIGHLY_SENSITIVE
Principal	600	SENSITIVE
Senior	450	SENSITIVE

この製品を使用すると、管理者は標準的なアクセス制御では不十分な場合に、アクセス仲介プロセスにラベル・ベースのアクセス制御を追加できます。Oracle Label Security は仮想プライベート・データベース・ツールキットに基づいて構築されており、プログラミングは一切不要です。データベース表の行へのアクセスは、その行に含まれているラベル、各データベース・セッションに対応付けられているラベルおよびセッションに割り当てられた Oracle Label Security 権限に基づいて仲介されます。Oracle Label Security にはデータ・ディクショナリと管理ツールがあり、有効なラベルの作成、ユーザーのラベル認証および権限の設定、表とスキーマに対する生成済み Oracle Label Security ポリシーの適用などに使用できます。

Oracle 仮想プライベート・データベース・ツールキットと Oracle Label Security には、ホスティングとデータ交換用にきわめて有効なメカニズムが用意されています。仮想プライベート・データベースは、データベース内でのファイングレイン・アクセス・コントロールを提供します。また、組織でデータベース表を共有する一方、関係するデータ以外は表示できないように、様々な組織からのデータを単一のデータベース・インスタンス内で分離状態に保つよう構成できます。これはホスティングには理想的です。ホスティング会社のシステム管理者は、管理対象サービスを提供するアプリケーションごとに、単一バージョンをセットアップして構成し、基礎となるアプリケーション表では仮想プライベート・データベースを使用して、管理対象となる顧客ごとに別個の仮想アプリケーション・インスタンスを提供できるためです。これにより、ホスティング関連のコストを大幅に削減できます。ハードウェア、データベースおよびアプリケーション・インスタンスを共有できるため、管理対象とな

るコンピュータごとに物理的に別個のインスタンスが必要な場合に比べると、ハードウェア関連のコストのみでなく、ソフトウェアのインストールと構成に伴うコストも削減されます。

Oracle Label Security は、機密性レベル、アクセス・カテゴリまたはユーザー・グループなどを使用して情報へのアクセスを公式化できるホスティング環境には特に有効です。このような環境では、Oracle Label Security を使用すると、ホスティング会社はラベル・ベースのセキュリティ・ポリシーを定義および管理することが容易になります。Oracle Label Security を使用すると、データ交換の面で特にメリットが得られます。これは、ラベル・ベースのアクセス・ポリシーでは、問題のコミュニティをサポートできるデータ・ラベルに、自動的で管理しやすい「グループ」アクセスが埋め込まれているためです。

また、Oracle Label Security のラベル・ベースのアクセス・ポリシーは、E-Business アプリケーションにアクセスするユーザーのプライバシ要求を施行するにも理想的です。多くの顧客は、プライバシの問題があるため、インターネット経由で商品やサービスを購入することに抵抗を感じています。Oracle Label Security を使用すると、自分のデータを送信先のマーケティング活動に使用されたり、購入データを売られたくないユーザーのために、データに「opt out」（二次目的のための情報提供の拒否）規定を示すラベルを付けることができます。データ・ラベルとユーザーのプライバシ・ポリシーはデータとともに残るため、複数のアプリケーション間でユーザーのプライバシ・プリファレンスを簡単に保護して施行できます。

関連項目：

- 9-18 ページ「Oracle Policy Manager」
- 『Oracle Label Security 管理者ガイド』

Oracle Internet Directory

Oracle Internet Directory は、Oracle9*i* データベース上にアプリケーションとして実装されるディレクトリ・サービスです。分散ユーザーおよびネットワーク・リソースの情報を検索できます。Oracle Internet Directory は、オープンなインターネット規格のディレクトリ・アクセス・プロトコルである Lightweight Directory Access Protocol（LDAP）バージョン 3 に、Oracle9*i* Server が提供する高パフォーマンス、拡張性、耐久性、可用性を組み合せたものです。

Oracle Internet Directory 自体はセキュリティ製品ではなく、エンタープライズ・データを効率的に管理するためのテクノロジです。LDAP ディレクトリのエンタープライズ・ユーザーのセキュリティをサポートすることで、データ・セキュリティに貢献します。

Oracle プラットフォームは、様々な方法で LDAP に対応するように設計されています。Oracle 顧客は厳しいセキュリティ要件を持っているため、タスクに適切な LDAP サーバーの選択肢は限定されます。ほとんどの場合、サポートされる LDAP サーバーは Oracle Internet Directory のみです。

この項の内容は次のとおりです。

- Oracle Internet Directory の概要
- LDAP 準拠
- Oracle Internet Directory によるエンタープライズ・ユーザー管理の編成方法

関連項目：

- 第 5 章「保護ディレクトリの使用と配置」
- 第 6 章「エンタープライズ・ユーザーのセキュリティの管理」
- 『Oracle Internet Directory 管理者ガイド』

Oracle Internet Directory の概要

Oracle Internet Directory は、ディレクトリのアクセス制御を包括的かつ柔軟にサポートします。これには、エントリ・レベル、属性レベルおよび模範的なアクセス制御が含まれ、企業とサービス・プロバイダの特定のニーズを満たせるように多様なセキュリティ・レベルを提供します。管理者は、特定のディレクトリ・オブジェクトまたはディレクトリ・サブツリー全体へのアクセス権を付与したり制御できます。Oracle Internet Directory では、3 つのユーザー認証レベルが実装されます。匿名、パスワード・ベースおよび証明書ベース（認証済みアクセスとデータ・プライバシのための Secure Sockets Layer（SSL）バージョン 3 を使用）の 3 つです。

また、Oracle Internet Directory には多数の強力な機能が用意されており、エンタープライズ環境や管理対象環境で使用して、アプリケーションのメタデータ（アプリケーションの動作とアクセスできるユーザーを制御する情報）へのアクセスを制御できます。そのためには、管理を委譲するためのディレクトリを配置します。この配置により、たとえばグローバル管理者は、部門の管理者に、その部門内のアプリケーションのメタデータへのアクセスを

委譲できます。このような部門管理者は、自部門のアプリケーションへのアクセスを制御できるようになります。

Oracle Internet Directory には、次のように重要なメリットがあります。

表 9-2 Oracle Internet Directory のメリット

メリット	説明
データ整合性	Oracle Internet Directory では、Secure Sockets Layer（SSL）を使用して、データが送信中に変更、削除または再生されていないことが保証されます。SSL では、MD5 アルゴリズムまたは Secure Hash Algorithm（SHA）を使用し、暗号チェックサムを通じて、暗号で保護されるメッセージ・ダイジェストを生成し、それをネットワーク経由で送信される各パケットに挿入できます。
データ・プライバシ	Oracle Internet Directory では、SSL で使用可能な公開鍵暗号化を使用して、データが送信中に検出されないことが保証されます。
パスワード保護	パスワードを保護するために、Oracle Internet Directory ではデフォルトで MD4 アルゴリズムが使用されます。MD4 は、128 ビットのハッシュまたはメッセージ・ダイジェスト値を生成する一方向ハッシュ関数です。

Oracle Internet Directory のコンポーネントは、次のとおりです。

表 9-3 Oracle Internet Directory のコンポーネント

メリット	説明
Oracle Directory Server	ユーザーおよびリソース情報に関するクライアント要求に応答し、TCP/IP 経由で複数層アーキテクチャを直接使用して、その情報を更新します。
Oracle Directory Replication Server	Oracle Directory Server 間で LDAP データをレプリケートします。
Oracle Directory Manager	Graphical User Interface（GUI）管理ツールです。
Oracle のツール製品	多様なコマンドライン管理およびデータ管理ツールです。

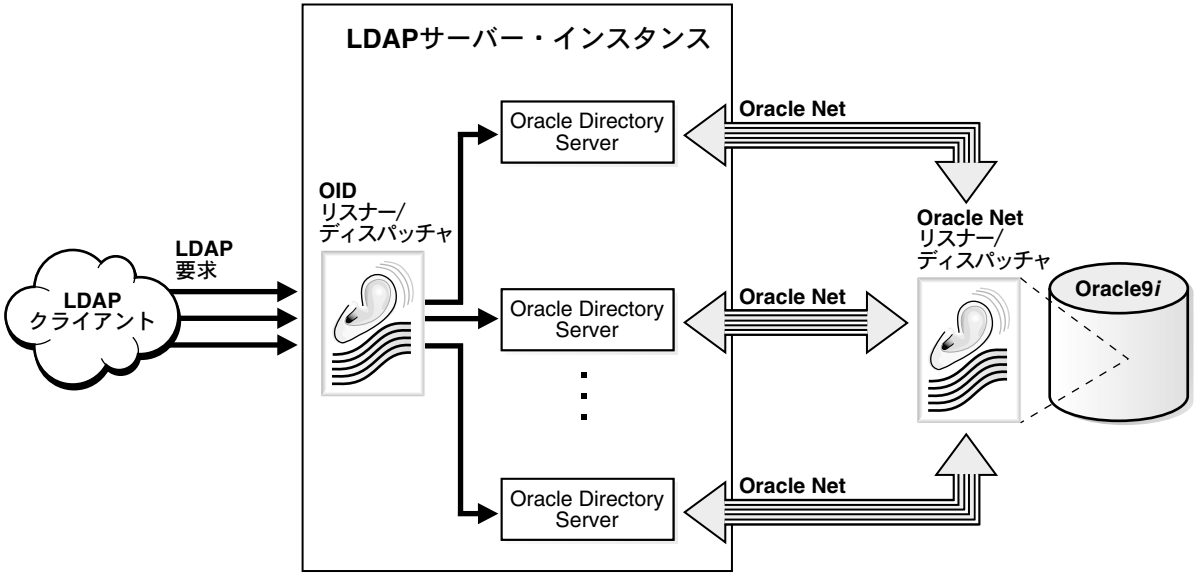
LDAP 準拠

Oracle Internet Directory は、Lightweight Directory Access Protocol（LDAP）に準拠しています。おそらく、Oracle Internet Directory は最もスケーラブルな LDAP ディレクトリです。Oracle9*i* データベースの組込みの拡張性を活用して、数十万のユーザーの管理が簡素化されます。LDAP ネーミングと Oracle Internet Directory の集中化されたディレクトリ・サービスのサポートにより、クライアントには前述のテクノロジに加えて新しい統一されたネーミング・メカニズムが提供されます。

Oracle Internet Directory では、LDAP バージョン 3 が実装されます。これは、ディレクトリ・サービス用の新たなインターネット標準です。従来の ISO X.500 Directory Access Protocol（DAP）規格に準拠していますが大幅に簡素化されており、LDAP の実装は効率的、単純、容易になっています。LDAP は、インターネット中心の「Thin クライアント」アプリケーションでの配置に特に適しています。

各 LDAP ディレクトリ・サーバー・インスタンスは、図 9-6 の構成のようになります。

図 9-6 LDAP サーバー・インスタンスのアーキテクチャ

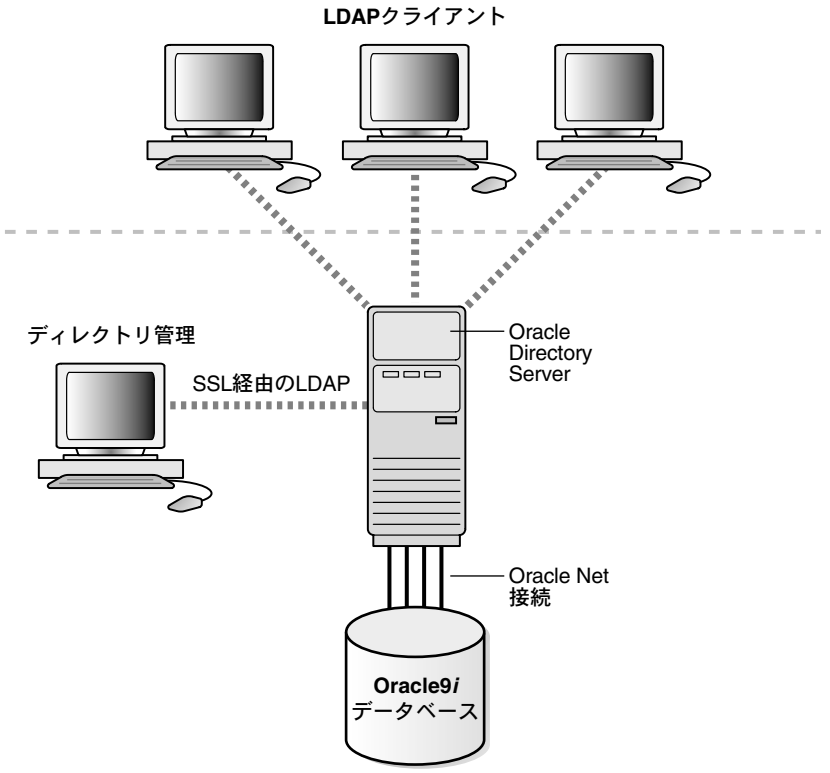


Oracle Advanced Security は、LDAP バージョン 3 準拠のディレクトリと統合できます。Oracle Advanced Security ライセンスにより、ユーザー管理、認可の格納と取出し用に、Oracle Internet Directory を配置することが許可されます。

Oracle Internet Directory の実装方法

Oracle Internet Directory ノードは、Oracle9*i* データベース上で実行されるアプリケーションとして実装されます。Oracle Internet Directory では、同一プラットフォームまたは異なるプラットフォーム上にあるデータベースと通信するために、Oracle のプラットフォームに依存しないデータベース接続ソリューションである Oracle Net Services が使用されます。この関係を図 9-7 に示します。

図 9-7 Oracle Internet Directory のアーキテクチャ



Oracle Internet Directory によるエンタープライズ・ユーザー管理の編成方法

この項では、Oracle Internet Directory によるエンタープライズ・ユーザー管理と共有スキーマについて説明します。

Oracle Internet Directory によるエンタープライズ・ユーザーの管理

Oracle Internet Directory では、属性レベルのアクセス制御と SSL 経由の最適の厳密ユーザー認証がサポートされ、厳密認証を受けたユーザー以外はユーザー権限やアクセスに関するディレクトリ情報を更新できないように構成できます。

エンタープライズ・ロールは集中管理される権限セットであり、Oracle Internet Directory 内、または Oracle のセキュリティ基準を満たす、選択されたパートナからのディレクトリ内でメンテナンスされます。エンタープライズ・ロールにより、ユーザーへの集中化された強力な認可が可能になります。また、管理者は、各ユーザーの認可を個別に更新せずに、エンタープライズ・ロール（複数ユーザーに付与）に機能を追加できます。Oracle Enterprise Security Manager には、集中的にユーザー定義を管理してロールを割り当てるためのツールが用意されており、全社的にユーザー管理コストが削減されます。単一ステーションによる管理には、セキュリティ管理が簡単であれば、組織は全社的に強力なセキュリティを実装できるという利点もあります。

関連項目： 3-6 ページ「Secure Sockets Layer（SSL）プロトコル」

Oracle Internet Directory での共有スキーマ

Oracle Internet Directory では共有スキーマがサポートされます。共有スキーマにより、データベースはユーザー識別情報や権限の管理をディレクトリに委譲でき、ディレクトリが統合されるというメリットが拡張されます。

関連項目： 6-3 ページ「共有スキーマ」

Oracle Net Services

Oracle Net Services は、クライアントと Oracle データベース・サーバーに常駐するソフトウェア層です。クライアント・アプリケーションとサーバー間で、接続の確立とメンテナンス、および業界標準プロトコルを使用したメッセージの交換を受け持ちます。この項の内容は次のとおりです。

関連項目：『Oracle9*i* Net Services 管理者ガイド』

Oracle Net Services のコンポーネント

Oracle Net Services は、Oracle Net、リスナーおよび Oracle Connection Manager で構成されています。この項の内容は次のとおりです。

クライアント側の Oracle Net

クライアント側では、アプリケーションは Oracle Net Client と通信し、接続を確立してメンテナンスします。Oracle Net Client は、TCP/IP のような業界標準ネットワーク・プロトコルで通信できるように、Oracle protocol support を使用して、Oracle データベース・サーバーと通信します。

データベース・サーバー側の Oracle Net

Oracle データベース・サーバー側は、クライアント側と同じです。ネットワーク・プロトコルにより、クライアント要求情報が Oracle protocol support 層に送信され、そこから Oracle Net に送信されます。Oracle Net は Oracle データベース・サーバーと通信し、クライアント要求を処理します。Oracle データベース・サーバー側に固有の操作の 1 つは、リスナーと呼ばれるプロセスを通じて初期接続を受信することです。リスナーは、クライアント要求を受け取ってサーバーに渡します。

Oracle protocol support

Oracle Net では、次の業界標準ネットワーク・プロトコルとの通信に Oracle protocol support が使用されます。

- TCP/IP
- SSL 付き TCP/IP
- Named Pipes

- LU6.2
- VI

Oracle Connection Manager

Oracle Connection Manager は、クライアントや Oracle データベース・サーバーとは別の専用コンピュータに常駐するソフトウェア・コンポーネントであり、データベース・サーバー宛の要求を代行します。また、Oracle Connection Manager は、セッションの多重化、アクセス制御またはプロトコルの変換用にも構成できます。

プロトコル変換

Oracle Connection Manager はプロトコル・コンバータであり、異なるネットワーキング・プロトコルを持つクライアントと Oracle データベース・サーバーが相互に通信できます。Oracle Advanced Security は Oracle Connection Manager により全面的にサポートされ、ネットワーク・プロトコルの境界にまたがって安全なデータ転送を実現します。異なるネットワーク・プロトコルで構成されているクライアントとデータベース・サーバーは、データを相互に安全に共有できます。ネットワーク・インフラストラクチャにおける潜在的な弱点を排除し、最大限のパフォーマンスを得るために、Oracle Connection Manager は暗号化されたデータをプロトコル間で渡します。したがって、復号化してから再び暗号化することによるコストやリスクは発生しません。

アクセス制御

Oracle Connection Manager はアクセス制御フィルタとして、Oracle データベースへのアクセスを制御します。特定のデータベース・サービスやコンピュータへのクライアント・アクセス権を付与または拒否するように構成できます。ソース、宛先およびデータベース・サービス名に関するフィルタ規則を指定すると、特定のクライアントからサーバーへのアクセスを許可または制限できます。

セッションの多重化

セッションの多重化というロールにおいて、Oracle Connection Manager は特定の宛先への単一トランスポート・プロトコルを通じて、複数のセッションを集中化します。これにより、Oracle データベース・サーバーで着信要求に使用される接続エンドポイントが減少し、2 つのプロセス間で複数セッションの維持に必要なリソースに対する需要が減少します。そのため、サーバーで処理できるネットワーク・セッションの合計数を増やすことができます。同時ユーザー数を増やすには、Oracle Connection Manager の複数インスタンスをインストールします。

Oracle Connection Manager をアプリケーション Web サーバーと同じコンピュータで実行すると、アプリケーション Web サーバーでは Oracle Connection Manager を通じて複数のクライアント・セッションをルート指定し、各セッションが Oracle データベース・サーバーに継続的にアクセスすることを保証できます。この機能は、セッションの可用性と応答時間が主要な問題となる Web アプリケーションに特に役立ちます。

Oracle Net Services によるファイアウォールのサポート

ファイアウォールを実装するには、次の 2 つの方法があります。

- イントラネット環境での Oracle Connection Manager を使用したファイアウォール
- インターネット環境での Oracle Net ファイアウォール・プロキシを使用したファイアウォール

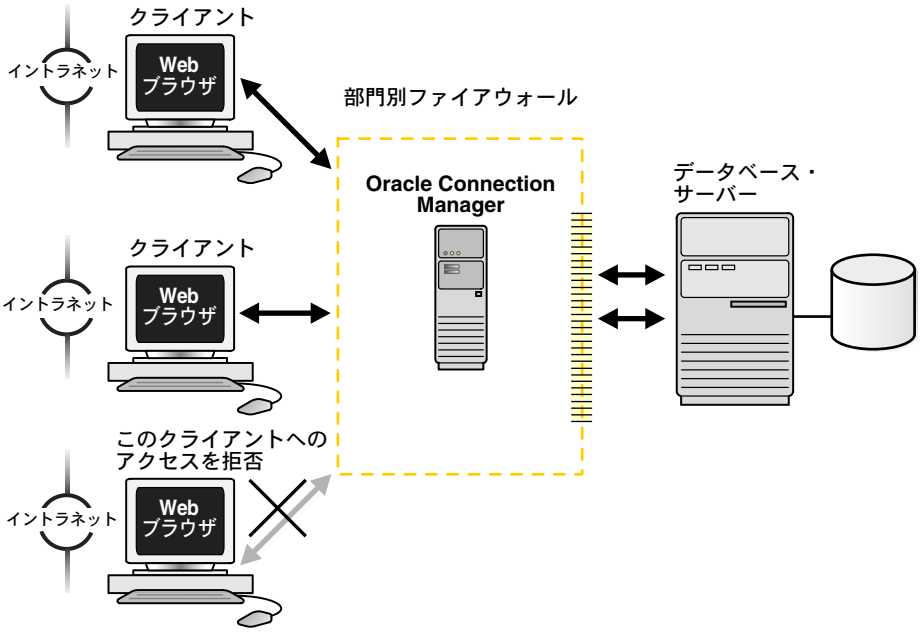
イントラネット環境での Oracle Connection Manager を使用したファイアウォール

Oracle Connection Manager は、イントラネットにファイアウォールとして配置できます。また、特定のデータベース・サービスやコンピュータへのクライアント・アクセス権を付与または拒否するように構成できます。フィルタ規則を指定すると、特定のクライアントからサーバーへのアクセスを、次の基準に基づいて許可または拒否できます。

- クライアントのソース・ホスト名または IP アドレス
- サーバーの接続先ホスト名または IP アドレス
- 接続先データベース・サービス名
- Oracle Advanced Security のクライアントの使用

図 9-8 に、3 つのクライアントと Oracle データベース・サーバーの間に配置された Oracle Connection Manager を示します。Oracle Connection Manager は、最初の 2 つの Web クライアントに対してアクセスを許可し、3 番目の Web クライアントに対してアクセスを拒否するように構成されています。この構成を機能させるには、クライアントに JDBC Thin ドライバが必要です。

図 9-8 Oracle Connection Manager によるイントラネット・ネットワークのアクセス制御

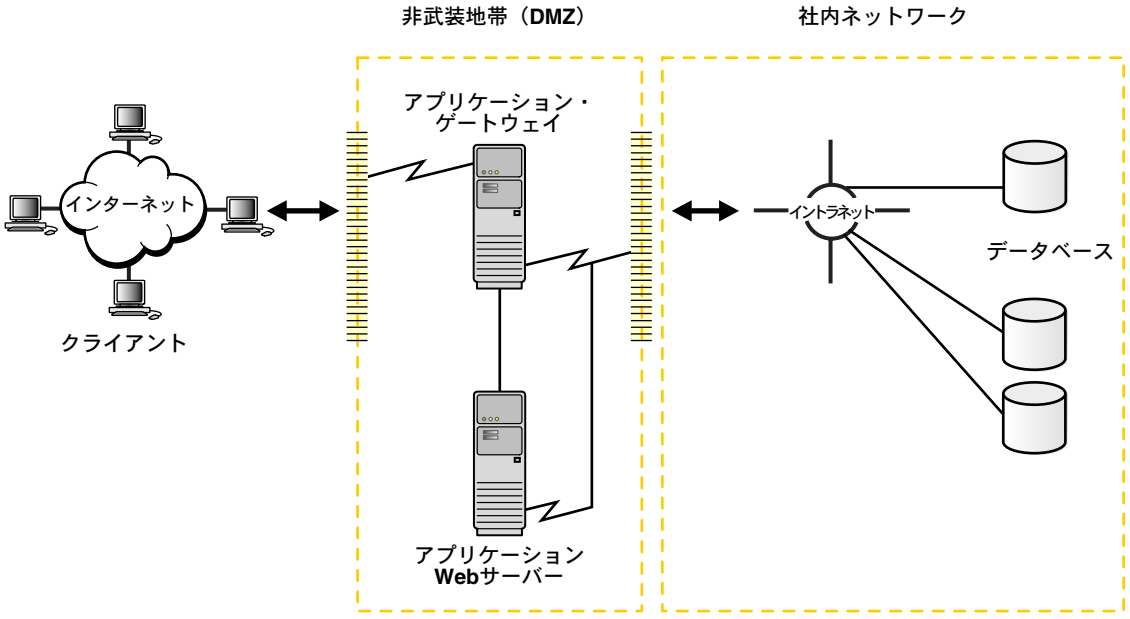


インターネット環境での Oracle Net ファイアウォール・プロキシを使用したファイアウォール

オラクル社はファイアウォール・ベンダーと協力して、サーバー製品に主要なファイアウォール・テクノロジを取り込み、分散データベース・ネットワークの通信をサポートしています。一部のファイアウォール・ベンダーは、Oracle Net ファイアウォール・プロキシと呼ばれるソフトウェア・コンポーネントを通じて、Oracle Connection Manager の機能を提供しています。Oracle Connection Manager ソフトウェアは、アプリケーション・ゲートウェイと呼ばれるホスト・コンピュータで実行されます。

図 9-9 に、内部ネットワークと外部ネットワーク間の通信量を制御し、アクセス制御と監査のための単一チェックポイントを提供するアプリケーション・ゲートウェイを示します。結果として、権限を持たないインターネット・ホストは、社内のデータベースに直接はアクセスできませんが、権限を持つユーザーは社内ネットワーク外部のインターネット・サービスをそのまま使用できます。この機能は、インターネット環境で機密データへのアクセスを制限する上で不可欠です。

図 9-9 アプリケーション・ゲートウェイによるインターネット・ネットワークのアクセス制御



関連項目： 3-6 ページ「ファイアウォール」

Oracle Net Services での有効なノードのチェック

Oracle Connection Manager を使用して有効なノードをチェックするのみでなく、Oracle Net Services のプロトコル固有のパラメータ（TCP.EXCLUDED_NODES および TCP.INVITED_NODES）を使用すると、データベースへのクライアント・アクセス制御を構成できます。また、パラメータ TCP.VALIDNODE_CHECKING を使用すると、TCP.INVITED_NODES および TCP.EXCLUDED_NODES をチェックして、アクセスを許可または拒否するクライアントを決定できます。

関連項目： 3-3 ページ「システム固有のネットワーク機能（有効なノードのチェック）」

データベースにより施行される VPD ネットワーク・アクセス

仮想プライベート・データベース（または保護アプリケーション・ロール）を使用して、特定のネットワーク・ノードからデータベースへのアクセスを制限することもできます。IP アドレスは偽装される恐れがあるため、ユーザーの主要な認証または認可方法として使用しないように注意してください。ただし、IP アドレスは、他の方法で認証されたユーザーによるデータへのアクセスを制限する補助的な修飾子として使用できます。たとえば、ユーザー Jane は EMP 表へのアクセス権を持っていますが、会社の方針では Jane が社内イントラネット内にいない場合は、人事管理部門の特定のサブネットからであっても、EMP データへのアクセスを許可しないように指示できます。

VPD と保護アプリケーション・ロールを使用すると、IP アドレスに基づいてデータへのアクセスを制限できます。VPD の場合、ポリシー関数は、次のような USERENV ネーミング・コンテキストを使用して、クライアント接続の IP アドレスにアクセスできます。

```
SYS_CONTEXT('userenv', 'ip_address')
```

また、データへのアクセスを許可するようにポリシー関数を定義できるのは、IP アドレスが許容値の範囲内（社内イントラネットの内部または人事管理部門用に予約されたアドレスの範囲内など）にある場合のみです。

プロキシ認証の場合、クライアント接続の IP アドレスは軽量セッションを開始したアプリケーション・サーバーの IP アドレスであり、ユーザーにはアプリケーション・サーバー経由でのみデータベースにアクセスするように、効率的に強制できます。特に、VPD ポリシー関数では USERENV ネーミング・コンテキストを使用できます。

```
SYS_CONTEXT('userenv', 'ip_address')
```

これにより、IP アドレスがアプリケーション・サーバーの IP アドレスと一致しなければ、レコードは戻されません。

この場合、ユーザーが適切に認証を受けていれば、データベースへの直接接続が禁止されることはないため注意してください。単に、戻されるレコードが制限されるのみです。valid_node チェックは、データベースの特定の IP アドレスへの接続を直接的に制限するため、ユーザー・アクセスの制限方法として汎用的で優れた方法です。

保護アプリケーション・ロールでも、USERENV ネーミング・コンテキスト（つまり、SYS_CONTEXT('userenv', 'ip_address')）を使用して、特定の IP アドレスから接続する場合にのみロールの有効化を許可できます。

ポリシーはビューで使用でき、ディクショナリ処理をはるかに低コストで実行できます。ポリシーはシノニムでも使用でき、シノニムに依存しているアプリケーションでは VPD を使用して高度なセキュリティを実現できます。

Oracle9*i* Application Server

Oracle9*i* Application Server は、E-Business への進化をサポートするように設計された、信頼度が高く、スケーラブルで安全な中間層アプリケーション・サーバーです。この製品を使用すると、テクノロジ上複雑な、完全な中間層インターネット・インフラストラクチャのアセンブルが管理されます。Oracle9*i* Application Server は、ビジネスとともに拡張できるインフラストラクチャを提供します。小規模から始めて、Web サイトのユーザー数や洗練された機能の増加をサポートできます。

この項では、Oracle9*i* Application Server のセキュリティ機能を紹介します。これには、HTTP Server や Portal など、アプリケーションの開発と配置のための汎用ファイアウォールを提供するコンポーネントや、特定のアプリケーション・サービスや機能を提供するコンポーネントが含まれます。また、HTTP Server や Portal には Oracle9*i* Application Server の汎用セキュリティ機能が実装されるため、そこで提供されるセキュリティ・サービスを重点的に説明します。

- Oracle HTTP Server
- Oracle9iAS Portal
- Oracle9i Application Server でのシングル・サインオン

関連項目： Oracle9*i* Application Server に関する Oracle マニュアルおよび関連ドキュメントを参照してください。

Oracle HTTP Server

Oracle HTTP Server は Apache 準拠の Web サーバーであり、最も普及している Web サーバー製品の中でもオープンなソース Web サーバーです。Oracle HTTP Server では、標準および Oracle 固有の多様な拡張機能（Apache コミュニティでは「mod」と呼ばれています）により Apache が拡張されます。基本的な HTTP リスナー機能のみでなく、静的および動的な Web ページをサポートする機能も用意されています。また、Secure Sockets Layer（SSL）暗号化などのセキュリティ・サービスや、他の Oracle9*i* Application Server コンポーネントおよび Oracle データベースなどの製品との統合機能もあります。

Oracle9*i* Application Server には、包括的なセキュリティ・サービス・セットが用意されています。これには、ユーザーの識別情報に基づいてファイルとサービスへのアクセスを制限または許可する機能が含まれます。ユーザーの識別情報は、基本的な要求 / 応答操作、クライアントが提供する X.509 証明書および IP アドレスやホスト名アドレスを使用して確立されます。機密保護は SSL プロトコルにより提供され、SSL は HTTP Server に対して X.509 証明書を表すためにも使用されます。また、HTTP Server には、侵入試行の検出と解決に必要なロギングなどの機能も用意されています。

Oracle9*i*AS Portal

Oracle9*i*AS Portal は、オラクル社の「エンタープライズ・ポータル」カテゴリに含まれる製品の主要コンポーネントです。これは、インターネット・ポータルがインターネット上のコンテンツへのゲートウェイであるのと同様に、社内イントラネットのビジネス関連情報へのゲートウェイを提供する新たな製品クラスです。

エンタープライズ・ポータルは、既存の市場の連結や拡張を行う点で、オラクル社の論理上のマーケットであり、強力なテクノロジ・ベース、重要なビジネス・システムを管理する広範囲のアプリケーション（ERP/CRM/BI）、アプリケーションをイントラネット上の他のデータストアとまとめるテクノロジを活用するファイアウォール（Oracle9*i*AS Portal）があります。Oracle9*i*AS Portal に組み込まれた機能は、複数の Oracle 製品およびアプリケーション間に共通のフレームワークをもたらします。「ポータル対応」の Oracle 製品を購入したユーザーは、E-Business のニーズや優先順位に従って、他の用途へと少しずつ簡単に拡張できます。

Oracle9*i* Application Server でのシングル・サインオン

Oracle9*i* Application Server の重要なセキュリティ機能が、Web ベース・アプリケーションへのシングル・サインオン（SSO）用にサポートされます。企業が SSO を検討するには、様々な理由があります。たとえば、会社が従業員別、顧客別およびパートナ別に使用できるように配置している Web ベース・アプリケーションの使用量の増大などがあります。SSO を使用しなければ、各ユーザーはアクセス先となるアプリケーションごとに別個の識別情報とパスワードをメンテナンスする必要があります。ユーザーごとに複数のアカウントとパスワードをメンテナンスするのは危険であり、高コストを招きます。この項の内容は次のとおりです。

- Web SSO テクノロジ
- Login Server
- LDAP の統合
- PKI サポート
- 複数層の統合
- Oracle のシングル・サインオンのまとめ

Web SSO テクノロジ

Oracle Web SSO テクノロジは、Web ユーザー用のシングル・サインオンを提供します。これは、複数の Web ベース・アプリケーションにポータル経由でアクセス可能な、Oracle9*i* Application Server の場合のようなポータル環境で動作するように設計されています。

Web SSO では、2 種類のアプリケーションがサポートされます。一方のパートナ・アプリケーションは、SSO フレームワーク内で動作し、ユーザー認証を SSO サービスに依存します。他方の外部アプリケーションは、引き続き独自のユーザー名とパスワードを使用しま

す。Oracle Web SSO アプローチは、パートナ・アプリケーションと Login Server と呼ばれる集中化されたサーバーの両方で作成される Cookie に基づいています。

Login Server

Login Server は、オラクル社の SSO テクノロジの中核部分です。この製品は、Web ベースのシングル・サインオンと、従来型アプリケーションとの統合を提供します。Login Server はシングル・サインオンを使用してユーザーを認証し、その識別情報をパートナ・アプリケーションに安全に渡します。また、ユーザーが特定の期間中（通常は 1 日）に初めてシステムにアクセスするときに、ユーザー名とパスワードの入力を求めるプロンプトを表示し、ユーザーが入力したパスワードを検証します。Login Server の SSO は、Web サーバーによりブラウザ・クライアントに格納された、書式化された情報部分である Cookie を使用します。Cookie により、Web サーバーはクライアント・ユーザーに関する情報を格納し、取り出して、他のステートレス Web 環境でクライアントの状態を効率的にメンテナンスします。Cookie は現行のすべてのブラウザでサポートされますが、ユーザーは無効にすることができます（その場合、Login Server は SSO を提供しません）。

LDAP の統合

Oracle Login Server では、SSO のユーザー名とパスワードを Oracle Internet Directory で検証できます。ユーザーが初期認証の一部として Login Server に SSO ユーザー名およびパスワードを発行すると、Login Server では、そのユーザー名とパスワードを使用して、Oracle Internet Directory に対する LDAP バインドが実行されます。LDAP バインドが成功すると、SSO ユーザー名およびパスワードは検証済みとみなされます。

PKI サポート

多数のアプリケーションで、PKI 認証がパスワードに置き換わりつつあります。Web ベース・アプリケーションでは、通常、PKI 認証は Secure Sockets Layer（SSL）セッション確立の一部として、X.509 証明書の交換を通じて実行されます。証明書を持つユーザーはパスワードを入力せずに複数のアプリケーションに認証できるため、PKI 自体を使用して SSO を提供できます。将来は、ユーザーは PKI を使用して Login Server に対して認証できるようになります。これにより、Login Server でサポートされる Web ベース・アプリケーションと、PKI 対応アプリケーションの両方に、SSO が提供されます。

複数層の統合

Login Server は、Web クライアントから Web サーバーへのアクセス用の SSO を提供します。Web サーバーが 3 層アーキテクチャの中間層として配置され、バックエンド層のデータベースへのアクセスを提供する例が増えてきています。ユーザーが Web アプリケーションにアクセスする場合に、その Web アプリケーションがデータベースへのアクセスを必要とするようであれば、ユーザーはそこに格納されているデータにアクセスするために、データベース・ユーザー名とパスワードを入力しなくても済むようにする必要があります。Login Server では非 Web ベース・アプリケーションはサポートされませんが、Oracle データベースには、3 層アーキテクチャ経由によるデータベースへの保護アクセスをサポートするために特別に設計された機能が組み込まれています。

Oracle のシングル・サインオンのまとめ

SSO に対するオラクル社の計画には、様々なテクノロジが含まれています。Web ベース・アプリケーションの分野は拡大を続けており、オラクル社は Web SSO の提供を目的として特別に設計された SSO フレームワークと Login Server を開発しています。Oracle Web SSO アプローチには多数のメリットがあります。たとえば、ブラウザ・クライアントから、Oracle Applications や Oracle のツール製品などの Web ベース・アプリケーションへの保護 SSO のためのフレームワークを、標準プロトコルを通じて提供します。また、SSO フレームワークを活用するパートナ・アプリケーションと、従来型のサード・パーティ製品サポート用の外部アプリケーションの両方をサポートします。Oracle の中間層 Web ポータル製品である Oracle9*i*AS Portal と適切に統合され、外部ディレクトリにあるユーザー情報の管理や、他の非 Oracle アプリケーションの SSO テクノロジとの統合が可能です。今後は、PKI クライアント認証がサポートされるようになり、多様な Web アプリケーションに対する PKI 認証が使用可能になります。

> **関連項目：** Oracle9*i* Application Server に関する Oracle マニュアルおよび関連ドキュメントを参照してください。

索引

P

R

S

T

U

V

W

X

あ

い

え

か

き

ち

つ

て

と

に

り

れ

ろ