

# ORACLE LABEL SECURITY



## 主な機能と利点



- 機密性ラベルを使用した透過的な行レベルのアクセス制御
- Oracle Database Vault との統合
- ポリシー・ベースの管理モデルにより、同一のデータベース内に複数のポリシーが共存可能
- 非表示列により、既存のアプリケーションSQL に対する完全な透過性を実現
- 政府や防衛機関にマルチレベルのセキュリティを実装
- 情報セキュリティにおける国際評価基準 (Common Criteria) EAL4+の評価
- Oracle8i Database Enterprise Edition 以降で使用可能な Oracle Database 11g Enterprise Edition の Security Option

Oracle Label Security は、機密性ラベルの使用により、Oracle データベースでの透過的な行レベルのアクセス制御を可能にします。Oracle Database Vault と組み合わせて使用することにより、機密性ラベルは複数要素の認可で使用する際の強力な要素となり、規制順守要件への対応を支援します。Oracle Label Security は柔軟性と適応性が非常に高い、業界で最も高度なラベル・ベースのアクセス制御製品です。ポリシー・ベースの管理によって、機密性ラベルおよびユーザー・ラベル認可の管理が容易になります。

## 機密データの保護

Oracle Label Security は、データの機密性ラベルとユーザー・ラベル認可を比較することにより、アプリケーション・データへのアクセスを透過的に制御できます。

Oracle Enterprise Manager を使用して、セキュリティ管理者はデータの機密性ラベルを定義し、ユーザーにラベル認可を割り当てます。これには、個人ユーザーがアクセスできる最大の機密性ラベルが含まれます。セキュリティ管理者は、ラベル・セキュリティ

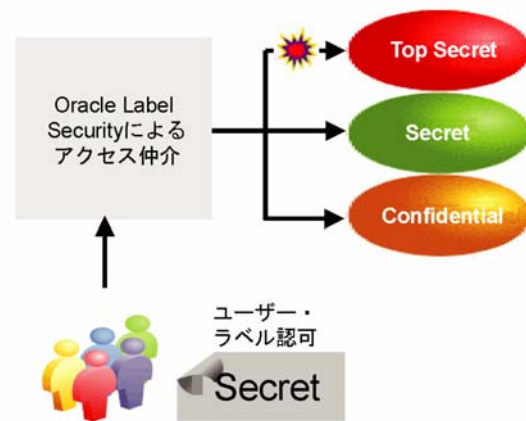


図1 : Oracle Label Security の概要

ティ・ポリシーを1つ以上のアプリケーション表に適用できます。一度適用されると、Oracle Label Security は、ユーザー・ラベル認可をデータに割り当てられた機密性ラベルと比較することで、アプリケーション・データへのアクセスを透過的に仲介します。ユーザー・ラベル認可がデータの機密性ラベルと等しいかあるいは大きい場合のみ、データへのアクセスが許可されます。データの機密性ラベルは、3つのコンポーネントで構成されます。必須の階層レベル、ゼロ以上の水平型コンパートメント、およびゼロ以上の親子グループです。たとえば、機密性ラベル `Secret:ProjectAthens:ExecOnly` は、レベル `Secret`、コンパートメント `ProjectAthens`、およびグループ `ExecOnly` で構成されます。多くの組織はレベル・コンポーネントのみを使用します。

## Oracle Database Vault との統合

Oracle Database Vault と組み合わせて使用することにより、機密性ラベルは複数要素の認可で使用する際の強力な要素となり、規制順守要件への対応を支援します。たとえば、ユーザー・ラベル認可を Oracle Database Vault のコマンド・ルールで使用することによって、データベース、SQL コマンド、およびアプリケーション表へのアクセスを制御できます。この強力な新しい機能によって、Oracle Label Security の概念は従来の行レベルのアクセス制御にとどまらず、データベースおよびアプリケーション・レベルでの仲介に拡張されます。

## ORACLE LABEL SECURITY

関連製品：

以下の製品は、セキュリティ、プライバシー、および規制要件を満たすための追加のセキュリティを提供します。

- Oracle Database Vault
  - DBA および特権ユーザーからのアプリケーション・データの保護
  - アプリケーションおよびデータベースへの透過的なアクセス制御
  - データベースの変更に対する保護
- Oracle Advanced Security
  - アプリケーションの SQL コードを変更しない透過的なデータの暗号化
  - AES 256 のサポート
  - 厳密認証
  - ネットワークの暗号化
- Oracle Secure Backup
  - テープのバックアップ時のデータベースおよびファイル・システム・データの暗号化
  - Oracle Recovery Manager (RMAN) との統合および 256 ビット AES までのサポート

## 柔軟性および適応性

Oracle Label Security は、行レベルでのアクセス制御に複数の適用オプションを提供します。ポリシーは、読取り操作のみ、更新操作のみ、またはその両方に適用できます。ユーザー・ラベル認可には、最大の読取りラベル、デフォルトの書き込みラベル、およびデフォルトのセッション・ラベルが含まれます。最大の読取りラベルは、ユーザーがアクセスできる最大のデータ機密性ラベルを指定します。デフォルトの書き込みラベルは、ユーザーが挿入するデータに割り当てられるデフォルトのデータ機密性ラベルです。デフォルトのセッション・ラベルは、ユーザーがデータベースに接続する際に所有するデフォルトの機密性ラベルです。これは、最大の読取りラベルに等しいか、それよりも小さい必要があります。ユーザー・ラベル認可に関係なく、読取り操作または更新操作のためにすべてのデータへのアクセスを許可する特別な認可を、ユーザーおよびストアド・プロシージャに付与できます。特別な認可は、パッチ適用やメンテナンスといった目的に有用です。Oracle Label Security のプロファイル・アクセス認可によって、1 つの大規模なユーザー・アプリケーションに対するプロキシ機能が提供されており、これによって主要アプリケーション・ユーザーはアプリケーション・ユーザーのラベル認可を引き受けることができます。SQL の述語である 'where' 句は、いずれかの Oracle Label Security ポリシーに任意で追加でき、機密性ラベルの範囲外までアクセス制御を拡張します。ラベル認可は、非データベース・ユーザーに付与できることに注意してください。このモデルは、一般的なアプリケーション・アーキテクチャをサポートします。

## 簡素化された管理性

Oracle Label Security は、使いやすいポリシー・ベースの管理モデルを提供します。

ポリシーは、機密性ラベル、ラベル認可、および任意で保護されるオブジェクトの論理コンテナです。同一のデータベースに複数のポリシーが共存しています。任意で Oracle Identity Management と統合することにより、ポリシーおよびユーザー・ラベル認可の集中管理が可能になります。

Oracle Enterprise Manager の Oracle Label Security コンソールに加えて、包括的な Oracle Label Security API が提供されます。



Copyright 2007, Oracle. All Rights Reserved.

本文書は情報提供のみを目的として提供されており、ここに記載される内容は予告なく変更されることがあります。本文書は一切間違いがないことを保証するものではなく、さらに、口述による明示または法律による黙示を問わず、特定の目的に対する商品性もしくは適合性についての黙示的な保証を含み、いかなる他の保証や条件も提供するものではありません。オラクル社は本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクル社の書面による許可を得て得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

Oracle は米国 Oracle Corporation およびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。