

Oracle Label Security

Oracle Label Securityを使用すると、企業や政府機関は、異なるアクセス要件を持つ類似の機密データセット（政府機関の機密データを含む）を、同一のデータベースに統合できます。Oracle Label Securityでは、データの種別とアプリケーション・ユーザーのアクセス・ラベル（セキュリティ・クリアランス）に基づいて、複数レベルのアクセス制御が実装されます。この強力な機能により、機密の研究開発プロジェクト、非公開の財務情報、および複数レベルのセキュリティ要件をOracle Database Enterprise Edition内で実施できます。Oracle Database Enterprise Editionは、Oracle Autonomous DatabaseおよびOracle Exadataクラウド・サービスと、Oracle Base Database ServiceのHigh PerformanceエディションおよびExtreme Performanceエディションの一部として提供されています。

ビジネス上のおもなメリット

- 機密性のレベルが異なるさまざまなデータセットを同一のシステム環境に混在させることができるため、運用コストやストレージ・コストを削減できる
- 開発コストを削減して、クリアランス・レベルに基づいた行レベルのアクセス制御の要件に対応できる
- 複数レベルのセキュリティ、必須のアクセス制御、"Need to know"の原則（知る必要がある人へのみ情報を伝える）に基づくデータへのアクセス管理などのコンプライアンス要件に対して、容易でコスト効率の良い方法を提供できる
- 高度にセキュアな製品に対する政府および商用の要件（Common Criteria認証など）に準拠できる
- 複数のデータとユーザー種別のラベルにより、必須とされるアクセス制御/コンパートメント化の要件のある環境に対応するように最適化できる
- 既存のOracle Enterprise Managerのスキルを活用して、ポリシーを構築してラベルを管理することができる

データの種別

Label Securityは、データのラベルまたは種別をアプリケーション・データに割り当てて、機密データを、機密性がより低いデータとともに同じ表に格納することができます。Label Securityは、アクセスをリクエストしているユーザーのラベルまたはセキュリティ・クリアランスとデータ・ラベルを比較することで、制御を実行します。データ・ラベルは非表示列として表に添付でき、データ・ラベルに基づいてアクセスを仲介することで既存のアプリケーションに透過性を提供しますが、実際のデータ・ラベルをSQL文で返すことはありません。一方、データ・ラベルを明示的に問い合わせることはできますが、問合せ対象の行にユーザーのラベル認可がある場合に限られます。

図1: Label Securityのデータ・ラベル

イベント	場所	ラベル
プレス・リリース	米国	PUBLIC
予算のレビュー	香港	HIGHLY_SENSITIVE:FINANCE:ASIA
カンファレンス	スペイン	PUBLIC
広告プラン	南アフリカ	SENSITIVE::AFRICA
合併協議	米国	HIGHLY_SENSITIVE:MA:USA
従業員向けの発表	グローバル	SENSITIVE
Alphaプロジェクトのレビュー	ブラジル	HIGHLY_SENSITIVE:ALPHA

データ・ラベルは3つの構成要素で構成できます。最初の構成要素は、必須レベルです。レベルの例には、公開、機密、極秘があります。2つ目はオプションで、コンパートメントと呼びます。

追加の特別なアクセス要件を満たすために、複数のコンパートメントをデータ・ラベルに割り当て、使用することができます。たとえば、特別な顧客アカウントを保護するデータ・ラベルには、コンパートメントVIPが含まれることがあります。最後となる3つ目のラベル構成要素はオプションで、グループと呼びます。グループの例には、CEOのオフィス、南北アメリカ、ヨーロッパなどの組織や地域があります。ラベルには常にレベルが含まれ、グループとコンパートメントの数は、ゼロの場合も1以上の場合もあります。

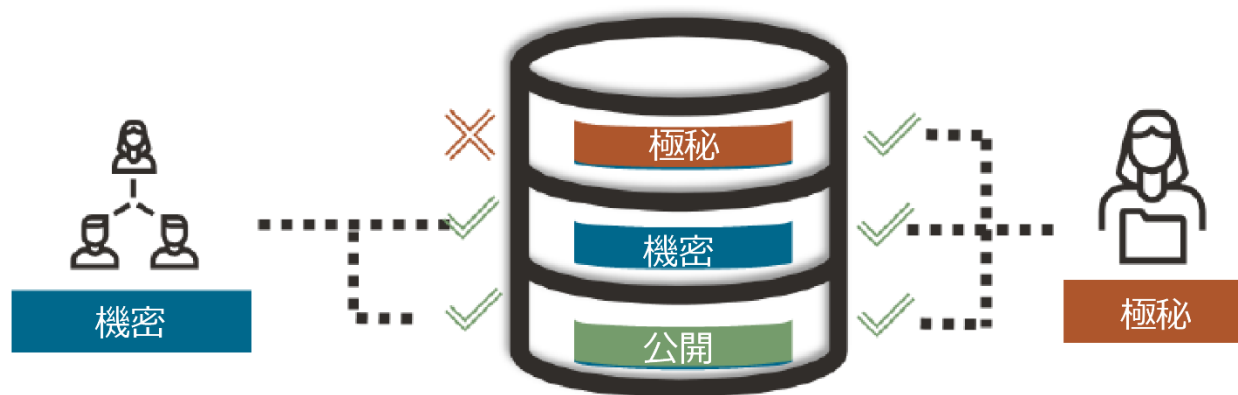
Oracle Label Securityの主な機能

- データのアクセス方法やデータがアクセスされる場所に関係なく、データ・アクセス実施をデータベース内に実装して、アクセス制御ポリシーを実施
- プロキシ認可と組込みアクセス制御ロジックにより、複雑なルールをアプリケーションにコーディングする必要性を排除
- 最小上界（LUB）関数やラベルのマージ関数など、多数のラベル関数を標準で提供
- データ・ラベルの非表示列
- 柔軟できめ細かい実施制御により、READ、UPDATE、INSERT、およびDELETE操作での実施を実現
- FULLやREADなどの権限を割り当てることで、信頼できるストアド・プロシージャを実現
- アプリケーション・ユーザーなどの非データベース・ユーザー、IPアドレス、その他の要素へのラベル認可の割り当てをサポート
- Oracle Database Vaultと統合することで、信頼できるパスの要素としてセキュリティ・ラベルを使用
- Oracle Real Application Securityと統合することで、ラベルをReal Application Securityユーザーに割り当てることが可能

ユーザー・ラベルとアクセス仲介

ユーザー・ラベルは、最大レベルおよび最小レベル、コンパートメント、グループで構成されます。ユーザーがOracle Databaseで認証されると、Label Securityによってそのユーザーのラベルが初期化されます。物理データベース・ユーザーを使用しないアプリケーションの場合、Label Securityはアプリケーションで使用可能な組込みのプロキシ機能を提供し、アプリケーション・ユーザーのIDに基づいてデータ・アクセスを実施できます。Label Securityが提供する柔軟な実施制御により、読取り操作、書込み操作、または両方の操作でアクセス制御が実施されます。アクセスの仲介時に、Label Securityは最初に、ユーザー・レベルと、データ・ラベルに割り当てられたレベルを比較します。2番目に、データ・ラベルに割り当てられたグループのうち少なくとも1つをユーザーが持っていることを確認します。3番目に、データ・ラベルに割り当てられたコンパートメントをすべてユーザーが持っていることを確認します。たとえば、Sensitive:VIP:Executive,CEOのデータ・ラベルの場合、ユーザーは、極秘データおよびVIPコンパートメントへのアクセス権と、ExecutiveまたはCEOのいずれかのグループへのアクセス権を持っている必要があります。

図2 : ユーザー・ラベルとアクセス仲介



データ・ラベルの割当て

データ・ラベルは、機密レベル、ゼロ個以上のコンパートメント、ゼロ個以上のグループからなります。データ・ラベルを作成する前に、有効なラベル構成要素を定義してOracle Databaseデータ・ディクショナリ内に格納します。データ・ラベルは、ラベル付け関数またはユーザーの現在のセッション・ラベルを使用して、表の行に自動的に割り当てることができます。ラベル付け関数により、さまざまなアプリケーションの属性を基にデータ・ラベルを計算できます。また、数値ラベル・タグかchar_to_label関数を使って、INSERT文で実際のラベルを指定することで、ラベルを割り当てることもできます。ストレージ・オーバーヘッドを低く抑えるために、Label Securityは数値タグを使用して各行のデータ・ラベルを表します。label_to_char関数を使用して、数値ラベル・タグをその外部またはテキスト・バージョンに変換します。

Label Securityとデータ・プライバシー規制

欧州連合の一般データ保護規則（EU GDPR）を含む多くのプライバシー規制の下で、データ主体には、組織に対して自身のデータの処理を停止するように要求する権利（処理の制限）があります。このような場合、組織は制御手段を構築して、個々のレコードが継続的に処理されないようにする必要があります。アプリケーション、スキーマ設計、およびアプリケーションのカスタマイズによっては、Label Securityがこのユースケースに適している場合があります。

Label Securityを使用して、セキュリティ関連のメタデータを個々のデータ行に付加することができます。その後、ラベルを使用して、行の処理を続けるかどうかをコントロールできます（アクセス制御）。EU GDPRの適用範囲での別のユースケースは、ラベルを同意管理に使用するというものです。この場合、データ・ラベルにユーザーの同意定義を格納します。EU GDPRにおける消去の権利についても、Label Securityとそのデータ・ラベル付け機能を使用できます。行に“消去対象”とラベル付けするプロセスの後に、データ消去手順によって処理できます。

管理性

ポリシーベースの管理により、データ・ラベル、ユーザー・ラベル、実施オプション、および保護された表を容易に管理できます。同じデータベース内に複数のLabel Securityポリシーを共存させることができます。Oracle Enterprise Managerにより、Label Securityポリシー、データ・ラベル、ユーザー・ラベル、および保護された表を管理できます。

関連製品

Oracle Database 23aiの多層防御ソリューション

- Oracle Data Safe
- Oracle Advanced Security
- Oracle Key Vault
- Oracle Database Vault
- Oracle Data Masking and Subsetting Pack
- Oracle Audit Vault and Database Firewall
- Oracle Database Security Assessment Tool

Connect with us

+1.800.ORACLE1までご連絡いただくか、oracle.comをご覧ください。北米以外の地域では、oracle.com/contactで最寄りの営業所をご確認いただけます。

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2024, Oracle and/or its affiliates.本文書は情報提供のみを目的として提供されており、ここに記載されている内容は予告なく変更されることがあります。本文書は、その内容に誤りがないことを保証するものではなく、また、口頭による明示的保証や法律による黙示的保証を含め、商品性ないし特定目的適合性に関する黙示的保証および条件などのいかなる保証および条件も提供するものではありません。オラクル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。本文書はオラクルの書面による許可を前もって得ることなく、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、Java、MySQLおよびNetSuiteは、Oracle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。