ORACLE

Oracle Label Security

Oracle Label Securityは、機密性に基づいてデータを分類することで行レベルのアクセス制御を実行し、許可された情報のみにユーザーがアクセスできるようにします。これにより、組織は機密性レベルが異なるデータを単一のデータベース内にセキュアに格納でき、運用コストやストレージ・コストを削減できます。

[1.0]

本書の目的

本書では、最新のOracle Label Securityリリースの機能の概要と強化された点が説明されています。本書は、Oracle Label Securityの予防的防御を使用することのビジネス上の利点について評価し、データ・セキュリティ・プロジェクトおよびITプロジェクトを計画立案するのに役立ちます。

免責事項

本文書には、ソフトウェアや印刷物など、いかなる形式のものも含め、オラクルの独占的な所有物である占有情報が含まれます。この機密文書へのアクセスと使用は、締結および遵守に同意したOracle Software License and Service Agreementの諸条件に従うものとします。本文書は、ライセンス契約の一部ではありません。また、オラクル、オラクルの子会社または関連会社との契約に組み込むことはできません。

本書は情報提供のみを目的としており、記載した製品機能の実装およびアップグレードの計画を支援することのみを意図しています。マテリアルやコード、機能の提供をコミットメント（確約）するものではなく、購買を決定する際の判断材料にするものでもありません。本書に記載されている機能の開発、リリースおよび時期については、オラクルの裁量により決定されます。

ORACLE

目次

はじめに

オラクルは、過去40年以上にわたり、機密情報を保護することのできる革新的なデータ・セキュリティ・ソリューションの構築において業界をリードしてきました。Oracle Label Securityは、セキュリティに対するオラクルの多層防御アプローチの一部であり、データ種別に基づいてデータ・アクセスを制御する業界の最先端ソリューションです。このテクノロジーは、米国政府、軍事、および諜報機関の標準を満たすように設計されましたが、Oracle Label Securityはユーザー・データを分離する必要性のある商業組織にも適用できます。政府組織と商業組織のいずれも、Oracle Label Securityを使用して複数のデータベースを統合することで、運用コストを削減してデータ分析と意思決定を簡素化できます。政府機関は、データ種別の基準を整合させてから、Oracle Label Securityを使用して機関内でデータを共有します。営利企業では、Oracle Label Securityを使用して異なる国のデータを分離することで、さまざまな国籍のユーザーがデータにアクセスし、ローカルのプライバシー要件およびコンプライアンス要件にアクセスできるようにします。その他の企業では、各グループが閲覧できるデータを制限する必要がある、子会社や小売店の同様のデータベースを統合しています。Oracle Label Securityは、ベクター・データとともに使用することで、許可されたデータ行のみに検索を制限できます。Oracle Label Securityには、それらを含む類似のユースケースを実現するための機能が標準で組み込まれています。

Oracle Label Securityでは、データの機密性ラベル（このドキュメントでは以下データ・ラベル）およびユーザー・ラベル認可（以下ユーザー・ラベル）に基づいてアクセスを仲介します。Oracle Label Securityは、Oracle Databaseの一部として、Common Criteria for Information Technology Security Evaluation（情報技術セキュリティ評価の共通基準）（ISO15408）に従って常に評価されています。Oracle Label Securityは、APIコールまたはOracle Enterprise Managerを使用して簡単に管理できます。

Oracle Label Securityの概念

データ統合、プライバシおよびコンプライアンスに関係する新しいセキュリティ要件に組織が取り組むようになるにつれて、アプリケーションによる機密データへのアクセスをよりきめ細かく制御することの必要性が高まり、重要性が増しています。機密性の高いデータ（プロジェクト、HR、財務）ごとに別々のデータベースを保持すると、コストがかさみ、管理上の不要なオーバーヘッドが発生します。一方、データベースを統合することは、別々のデータベースからの機密性の高いデータを1つのシステムに結合することを意味する場合があります。Oracle Label Securityには、データ・ラベルまたはデータ種別をデータにタグ付けする機能があります。この機能によりデータベースでは、各ユーザーに適切なデータを識別し、セキュリティ管理を実施することができます。データには、機密性の程度（別名レベル）をラベル付けすることも可能です。たとえば、政府および防衛機関のアプリケーションでは、Unclassified、Secret、またはTop Secretなどでデータにラベル付けします。一方、医療アプリケーションでは、Public、Confidential、またはHighly Restrictedなどでデータにラベル付けします。

Oracle Label Securityでは、データの種別ラベルをユーザーのアクセス認可と比較することによってアクセス制御を実施します。アクセス認可は、標準のデータベース権限およびロールを拡張した機能と考えることができます。たとえば、一般的なデータベースの操作は、アプリケーション表でユーザーまたはロールに対してGRANT the SELECT権限を実行することです。この権限がある場合、ユーザーやロールは表のすべての行を選択できます。機密性の高いデータ行へのアクセスを制限するには、次の2つを実行する必要があります。第一に、機密性が高いと考えられるデータがどれなのかを認識することです。第二に、ユーザーのアクセス認可を認識することが必要です。Oracle Label Securityでは、データ種別ラベルを定義し、アクセス認可をユーザーに割り当て、データ種別ラベルをデータに割り当て、アクセス制御を実施する機能によってこの問題を解決します。歴史的に、この機能を実現するための設計手法は、データベースのビュー、トリガー、および参照表に基づいています。しかし、このアプローチでは、アプリケーションの広範な変更が必要とされ、実装の一貫性を維持することができませんでした。Oracle Label Securityは、データベース内のアプリケーション・レイヤーの下位で組み込まれて適用され、これによりセキュリティが強化されて、アプリケーションのビューおよびトリガーの必要性がなくなります。こうして、独自のセキュリティ・モデルが必要とされるのが一般的なレポート・ツールやビジネス・インテリジェンス・ツールなど、データに接続するすべてのアプリケーションでアクセス権が適用されます。

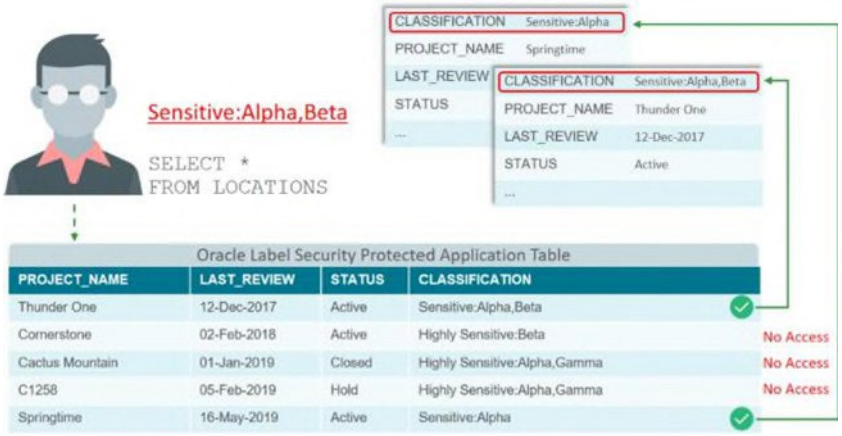

図1：Oracle Label Securityでは、ユーザー・ラベルとデータ・ラベルを利用してデータ・アクセスを制御する。

Oracle Label Securityは確立されたオラクル製品で、簡単な要件から複雑な要件まで対応できます。Oracle Label Securityのデプロイを成功させるには、他の高度なセキュリティ製品と同様、正しい分析と計画が鍵になります。以下の手順は、Oracle Label Securityをデプロイする場合の基本的なガイドラインを示しています。この実装は、Oracle Enterprise ManagerまたはOracle Label Security APIを使用して実行します。まずはサンプルのデモ表で作業を開始し、データ・ラベルによってアクセス制御を仲介する仕組みと、Oracle Label Securityに組み込まれているさまざまな実施オプションについての理解を深めることをお勧めします。

Oracle Label Securityの実装手順

手順
このホワイト・ペーパーで推奨されているデータ分析手順を実行する
Oracle Label Securityポリシーを作成する
レベル、コンパートメント、およびグループなどの必要なデータ・ラベル・コンポーネントを定義する
ユーザー・ラベル（最大、最小、デフォルト）をプロビジョニングする
すでに定義済みのコンポーネント（レベル、コンパートメント、グループ）を使用してポリシーのデータ・ラベルを作成する
ポリシーをアプリケーション表に適用する （いったん適用されると、特別な権限が付与されない限り、データにはアクセスできなくなります）
適切なデータ・ラベルを付けてレガシー・データを更新する

このホワイト・ペーパーでは、製品内部の中核コンポーネント（データ・ラベル、ユーザー・ラベル）に焦点を当て、それからポリシーおよびデータ分析手順について説明します。

データ・ラベルと保護されたオブジェクト

データ・ラベルのコンポーネントには、レベル、コンパートメントおよびグループなどがあります。これらのコンポーネントは、データ・ラベルを作成して、データベース・タイプまたはアプリケーション・タイプのユーザーにユーザー・ラベルを割り当てるために使用されます。レベルは、機密度の高い順に並んでいます。
コンパートメントは独立しており、指定されたレベル内でデータを分離するために使用されます。グループは、指定されたレベル内でデータを組織単位で分離するために使用されます。グループには、継承関係、つまり親子階層関係を含めることができ、親グループへアクセスすることで子グループにアクセスできます。任意のデータ・ラベルには必ず、1つ以上のレベル、0個以上のコンパートメント、および0個以上のグループが含まれます。コンパートメントまたはグループのみを使用するデプロイメントでは、ユーザー・ラベルまたはデータ・ラベルに単一のデフォルト・レベルを作成する必要があります。

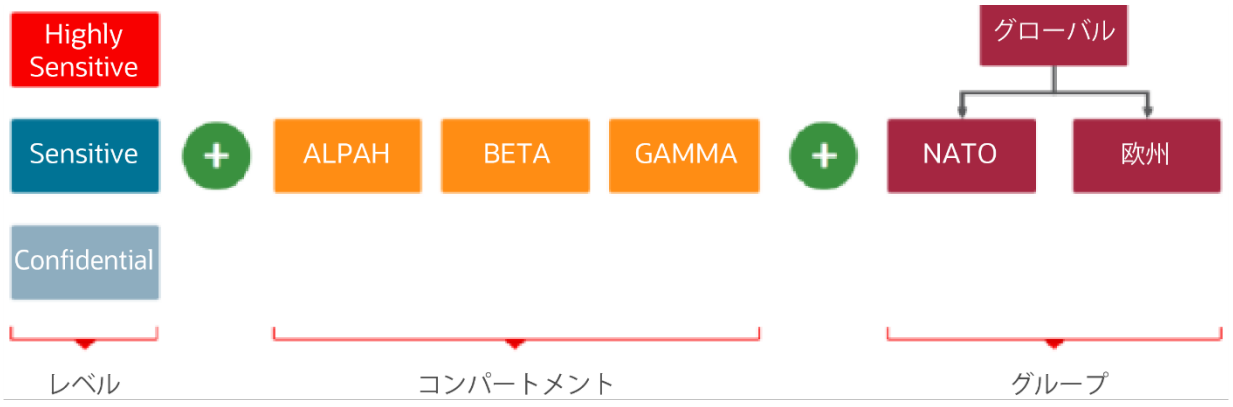

図2：Oracle Label Securityのデータ・レベルには、レベル、コンパートメントおよびグループなどがある。

Oracle Label Security - データ・ラベルのコンポーネント

ラベル・コンポーネント	説明
レベル	レベルは、データの機密性の程度を示すコンポーネントです。 各データ・ラベルとユーザー・ラベルには、必ず1つのレベルが指定されています。 組織では、Confidential、SensitiveおよびHighly Sensitiveなどのレベルを定義できます。組織でレベルを使用する必要がない場合でも、単一のデフォルト・レベルを定義する必要があります。
コンパートメント	コンパートメントは任意のコンポーネントで、互いに独立しています。通常は、データをコンパートメント化するため、1つ以上のコンパートメントが定義されています。コンパートメントは、特定の種類のデータ、知識領域、地理、またはHR、財務、経理などの特定の承認を必要とするプロジェクトで定義可能です。
グループ	グループは任意のコンポーネントであり、各グループに親子関係（階層）を含めることができる点を除いてコンパートメントによく似ています。グループは、フランスとポルトガルを子グループに持つ欧州や、米国とカナダを子グループに持つ北米など、組織構造や地域別にデータを分離するためにもっとも多く使用されます

業種固有のポリシーとデータ・ラベルの例

業種	レベル	コンパートメント	グループ
政府および防衛機関	Confidential Secret Top Secret	統合援助作戦　国境警備局	NATO 国土安全保障省
警察	レベル1 レベル2 レベル3	内政　麻薬取締り	地方管轄、FBI、司法省
人事管理	Confidential Sensitive Highly Sensitive	PII データ調査	グローバル 北米 カナダ、米国 EMEA、 フランス、ポルトガル、 ドイツ LATAM メキシコ、ブラジル、 アルゼンチン
保健医療	Public　Confidential	患者　医師	ラボ、技術者、医療助手
小売財務	デフォルト*	なし	各店舗、国、地域、財務グループ

研究開発	デフォルト*	プロジェクト	プロジェクト・メンバー、 プロジェクト・リード、 財務部門、法律部門

* レベルは、このユースケースのアクセス権を判断するために使用されることはありませんが、デフォルト・レベルを1つ設定する必要があります。

データ・ラベルの使用

組織のデータ・ラベルの要件を決定することは、Oracle Label Securityのデプロイ計画においてもっとも重要な最初の手順です。これは、情報を保護するために必要なレベル、コンパートメント、またはグループを決定することを意味します。一般に、データ・ラベルの要件を決定するということは、アプリケーションを分析し、Oracle Label Securityで保護する予定の表を識別することを意味します。このための最適な方法は、アプリケーション・スキーマについての知識を持つアプリケーション管理者または開発者が実行することです。ほとんどの場合に、アプリケーション表のごく一部のみでOracle Label Securityポリシーが必要とされます。候補となる表が特定されたら、それらの表に含まれるデータを評価する必要があります。データ分析者、またはデータについて把握しているユーザーが必要になる場合もあります。また、将来的なアプリケーション・データについても考慮することが推奨されます。これにより、堅牢な初期ラベル・コンポーネント・セットが作成されます。

1つのOracle Label Securityポリシーには、最大で9999のレベル、コンパートメント、およびグループを含めることができます。ただし、多くの商業組織ではデフォルト・レベルを1つだけ使用するのに対し、政府または防衛機関の実装では2つから5つのレベルを使用します。

データ・ラベルのテキストベースの表現では、コロンとカンマを使用してコンポーネントを区切ります。たとえば、データ・ラベル[Sensitive:Alpha,Beta:UK]には、レベル（Sensitive）、2つのコンパートメント（AlphaとBeta）、および1つのグループ（UK）が含まれています。データ・ラベル[Default::US]には、Defaultと呼ばれる1つの必須レベルとUSグループが含まれています。

Oracle Label Securityの内部では、データ・ラベルごとにラベル・タグと呼ばれる数値識別子が使用されます。ラベル・タグは、データ・ラベルの作成時に設定されます。ラベル・タグは、ポリシーの作成時に管理者によって定義される保護された列の各行に格納されます。管理者は、その列を表示列または非表示列としてアプリケーション表に追加することができます。列を非表示列として追加すると、SQL文において列名が修飾されなかったために、既存のselect、insert、またはupdate文の実行に失敗する可能性が一切排除されます。Oracle Label Securityのポリシー列は、Oracle Label Securityポリシーを適用するより前からアプリケーション表に存在している可能性があることを認識しておくことは重要です。この点を利用するには、アプリケーション表の列データ・タイプの番号を（10）にする必要があります。これにより、Oracle Label Securityのポリシー列を組み込んでアプリケーションを設計できるようになります。

ラベル・コンポーネントの必要なユーザー認可

ラベル・コンポーネント	説明
レベル	ユーザーは、そのレベル以上へのアクセスが許可されている必要があります。たとえば、“Sensitive”というラベルのデータにアクセスする場合、そのユーザーは最低でも"Sensitive"レベルへのアクセスが許可されている必要があります。レベルに割り当てられている数字によりランキングが決まります。
コンパートメント	ユーザーは、データ・ラベルに含まれるすべてのコンパートメントに対してアクセスが許可されている必要があります。たとえば、“Sensitive:Alpha,Beta”というラベルのデータにアクセスする場合、そのユーザーは最低でも"Sensitive"レベルと“Alphおよび“Beta”コンパートメントへのアクセスが許可されている必要があります。レベルとは異なり、コンパートメントに割り当てられている番号には、内部関数を使用するときの複数のコンパートメントの表示順を決めること以外に意味はありません。

グループ	ユーザーは、データ・ラベルに含まれるグループの少なくとも1つへの、または親グループへのアクセスが許可されている必要があります。たとえば、“Default::Canada”というラベルのデータにアクセスする場合、そのユーザーはDefaultレベルとCanadaグループへのアクセスが許可されている必要があります。ただし、Canadaグループの親はNorth Americaグループなので、North America Regionグループもそのデータにアクセスできます。ラベルのレベル、コンパートメントおよびグループの各セクションは、コロンで区切られています。レベルとは異なり、グループに割り当てられている番号には、label_to_char関数や類似の関数を使用する場合の複数グループの表示順を決めること以外に意味はありません。

アプリケーションにエンティティ・リレーションシップ（ER）図がある場合は、その図にエンティティ別のデータ・ラベルの範囲をアノテーションとして付加すると便利です。

ユーザー・ラベル

ユーザー・ラベルにより、データ・ラベルによって保護された情報にユーザーがアクセスできるかどうかが決まります。ユーザー・ラベルは、最小と最大のレベル、デフォルト・レベル、行レベルで構成されています。また、ユーザー・ラベルには、コンパートメントとグループを含めることもできます。たとえばユーザーには、最大レベルとしてSensitiveを、最小レベルとしてPublicを割り当てることが可能です。データベース・ユーザーには、ユーザーがデータベースに接続されるときに初期化されるデフォルト・ラベルもあります。このラベルは、アクティブ・セッション・ラベルと呼ばれることもあります。セッション・ラベルは、コンパートメントとグループを組み合わせた単なるユーザーの現在レベルです。セッション・ラベルは、接続のためにラベルを変更するルールに基づいているユーザー・ラベルとは異なる場合があります。たとえば、ユーザーのユーザー・ラベルの一部としてHighly Sensitiveレベルが割り当てられているとしても、接続がVPNを介したリモート・セッションである場合には、セッション・ラベルがSensitiveレベルに制限されます。

アプリケーション・ユーザーがOracle Label Securityによって保護されているアプリケーション表にアクセスできるようにするには、まず、セキュリティ管理者がOracle Label Securityのユーザー・ラベルを設定しておく必要があります。データベースに複数のポリシーが存在する場合は、ポリシーごとに別々のユーザー認可を設定する必要があります。

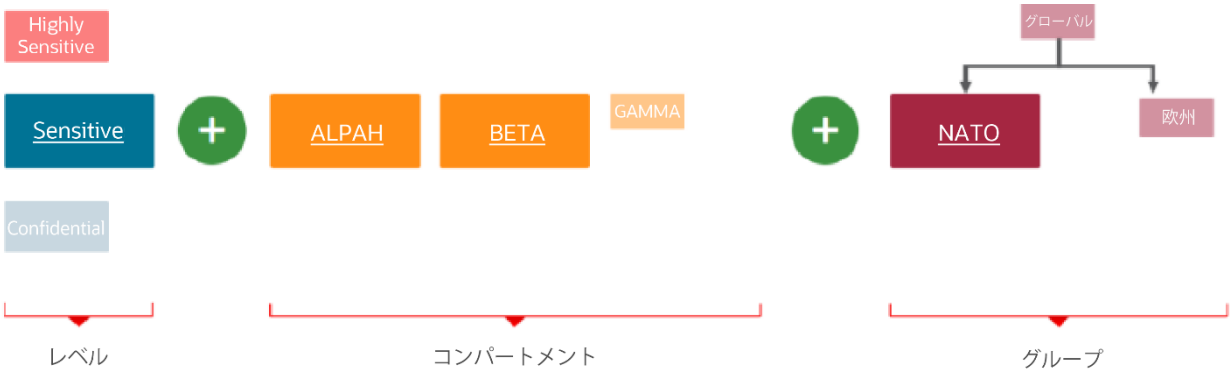

図3：ユーザー・ラベルのコンポーネントには、レベル、コンパートメントおよびグループなどがある

ラベル戦略

ラベル戦略を定義するには、ユーザーのさまざまなロールと責任について理解している必要があります。たとえばユーザーは、分析者、高権限ユーザー、管理ユーザーなどに指定されています。さまざまなロールおよび責任について理解するには、マネージャーやセキュリティ管理者の支援も必要になることがあります。ユーザーを1つ以上のロールまたは機能領域に区分した後は、データ・ラベルの要件とユーザー・ラベルの要件を比較することも必要です。前述のそれぞれの表で、これらのラベルが正しく対応している必要があります。このステップは、アクセス権を持っているユーザーが誰もいない機密性ラベルがデータに割り当てられないようにするのに重要です。言い換えると、そのユーザー・ラベルが原因となって、アプリケーション・ユーザーが特定の職責を実行するのに必要な情報にアクセスできなくなります。最悪の場合は、どのユーザーもアクセスできないデータ・ラベルがデータに割り当てられ、そのデータが事実上完全に隠されてしまいます。

Oracle Label Securityのサンプル認可分析

表	データ	ユーザー			
		C	S	S:A:US	S:A,B:US,UK
資産	C::UK	アクセスなし	アクセスなし	アクセスなし	**アクセスあり**
プロジェクト	C	**アクセスあり**	**アクセスあり**	**アクセスあり**	**アクセスあり**
	S	アクセスなし	アクセス	**アクセスあり**	**アクセスあり**
	S:A:US	アクセスなし	アクセスなし	**アクセスあり**	**アクセスあり**
	S:B:UK	アクセスなし	アクセスなし	アクセスなし	**アクセスあり**
	S:A,B:US	アクセスなし	アクセスなし	アクセスなし	**アクセスあり**

レビューおよびドキュメント

実装担当者は、収集した情報をレビューおよび文書化する必要があります。情報には、保護される必要があるアプリケーション表の一覧、その理由、およびラベルのコンポーネントとその意味の一覧を含めてください。この情報は、Oracle Database Vaultのレルムまたはコマンド・ルール、Oracle Data Redactionポリシー、Oracle Data Masking定義、および表領域暗号化などの他のセキュリティ管理機能を適用する場合にも有用です。このドキュメントは、エンタープライズ・セキュリティ・ポリシーの一部であり、機密情報とみなして安全に保管する必要があります。

ラベル・セキュリティ管理

インストールの指針

Oracle Databaseでは、Oracle Label Securityはデフォルトでインストールされますが、有効化されていません。Oracle Label Securityは、Oracle Database Configuration Assistant（Oracle DBCA）またはコマンドラインを使用して構成および有効化できます。ドキュメントに示す手順に沿って、Oracle Label Securityポリシー、レベル、コンパートメント、およびグループを作成します。

Oracle Label Securityポリシーを作成する予定のプラガブル・データベース（PDB）でOracle Label Securityを有効化します。Oracle Label Securityはデータ・ディレクトリ・オブジェクトを保護するように設計されていないため、ルート・コンパートメントにポリシーを作成することはできません。

ユーザーおよびロールの管理

LBACSYSアカウントには、Oracle Label Securityのポリシー、データ・ラベル、保護されたオブジェクト、実施設定およびユーザー・セキュリティ認可を保存するデータ・ディクショナリが含まれています。LBACSYSは、Label Based Access Control SYSを意味します。Oracle 19c以降、LBACSYSは、オラクルが提供する他のアカウントと同様、スキーマのみのアカウントとして構成されます。Oracle Label Securityを使用する場合、データベース・セキュリティ・オフィサーは、ALTER USERコマンドを実行してLBACSYSにパスワードを提供し、Oracle Label Security管理者がアカウントにアクセスして名前付きユーザーにLBACロールを付与できるようにする必要があります。Oracle Label Security管理者によってロールの付与が完了したら、データベース・セキュリティ・オフィサーは、ALTER USERを再実行して、LBACSYSをスキーマのみのアカウントに返すことができます。LBACSYSは共有アカウントであり、エンドユーザーを正しく監査できないため、オラクルでは、Oracle Label Securityの管理にLBACSYSを使用しないようお勧めします。LBAC_DBAデータベース・ロールを、Oracle Label Securityを日々の使用のために管理する信頼のおけるユーザーに付与することをお薦めします。

LBACSYSに保存されている情報へのアクセスは、ポリシー固有のルールとデータベース・ビューによって制御されます。固有ポリシーの管理は、Oracle Label Securityの固有データベース・ロールを使用し、特定の管理パッケージに権限を付与することによって、許可された個々のユーザーに委任することができます。LBACSYSアカウントでは、Oracle Label Securityに関連付けられているメタデータを保持することに加えて、数十のプロシージャと関数が保持されます。

Oracle Label Securityでは、委任管理が可能です。Oracle Label Securityポリシー"POLICYNAME"を作成すると、新しいデータベース・ロールPOLICYNAME_DBAも作成されます。このロールは、ポリシーのラベル・コンポーネントとラベル認可を管理するために使用でき、ポリシーの管理を担当する名前付きユーザーに付与される必要があります。

Oracle Label Securityの実施の非適用

Oracle Label Securityのポリシーを使用する場合は、以下の例外事項を理解しておくことが重要です。**Oracle Label Securityの実施の非適用**

例外	説明
SYSオブジェクト	Oracle Label Securityポリシーは、SYSスキーマ内のオブジェクトに適用できません。
SYSDBAロール	Oracle Label Securityポリシーは、AS SYSDBAロールで接続するユーザーには適用されません。
DIRECTパス・エクスポート	Oracle Label Securityポリシーは、DIRECTパス・エクスポート時には適用されません。
EXEMPT ACCESS POLICY	Oracle Label Securityのポリシーは、Oracle DatabaseのEXEMPT ACCESS POLICY権限が直接、またはデータベース・ロールを介して付与されているユーザーには適用されません。

信頼できるストアド・プロシージャ

信頼できるストアド・プログラム・ユニットは、標準のプロシージャ、関数、またはパッケージが作成されるのと同じ方法で作成されます。プログラム・ユニットは、Oracle Label Securityの権限が付与されると信頼できるようになります。ユーザーに付与されるOracle Label Securityの権限は、信頼できるストアド・プロシージャに付与することもできます。そうすることで、ストアド・プロシージャの実行コンテキスト内のデータへのアクセスを有効にすることができます。ただし、ストアド・プロシージャまたは関数を呼び出すことによってユーザーが直接アクセスすることはできません。

Oracle Label SecurityおよびOracle Database Vaultの機能

Oracle Label Securityの多くの関数は、Oracle Database Vaultルール・セット内で使用して、ユーザーがデータベース内で特定の運用タスクを実行できるかどうかを判別することもできます。Database Vaultでラベルを使用することは、純粋なデータ種別の外部にあるセキュリティ認可の代替ユースケースで、これにより職務機能をよりきめ細かに区別することができます。

Oracle Label SecurityおよびVirtual Private Databaseの機能

Oracle Label Securityを使用すると、ポリシーがアプリケーション表に適用されるときに非定型の制限のある'where'句または'condition'句を追加することもできます。この'where'句は、アクセス権を決定するためにデータ・ラベルとともに使用され、Oracle Virtual Private Database（VPD）ポリシーの作成機能に似た使いやすくてシンプルな機能を提供します。'where'句は、Oracle Label Securityポリシーに付加されます。そのため、純粋なOracle VPDを実装する場合とは異なり、別個のPL/SQLパッケージを作成する必要はありません。

Oracle Label Securityとデータ改訂ポリシー

Oracle Label Securityは、データ改訂とともに使用して、改訂ポリシーが適用されるかどうかを判断するのに役立ちます。たとえば、Oracle Label Securityのユーザー・セッション・ラベルによって改訂済みデータまたは未改訂データへのアクセスが許可される場合に、データ改訂ポリシーを適用できます。

ベスト・プラクティス

アプリケーション・ユーザーのデータベース・ユーザーへのマッピング

Oracle Label Securityでは、1つのデータベース・アカウントを使用してデータベースに接続する"n-tier"アプリケーションを含め、一般的なアプリケーション・アーキテクチャがサポートされています。これを実行するために、Oracle Label Securityでは、データベース・スキーマ・ユーザーではなくアプリケーション・ユーザーに基づいてセッション・ラベルを設定できます。アプリケーション・ユーザーのセッション・ラベルは、データベース・ユーザーのセッション・ラベルまたはサブセットと同じです。たとえば、アプリケーション・ユーザーは、複数のコンパートメントとグループではなく、1つのコンパートメントと1つのグループにアクセス権があります。

既存のデータへのラベル付け

データ・ラベルが既存のデータのラベル・タグに移入されていない場合、アプリケーション表にOracle Label Securityポリシーが適用されると、どの行も表示されません。これは、ラベル・タグ・フィールドがNULLになるからです。任意で、初期データのラベル付けを担当する管理者にLabel Securityの認可FULLを付与することができます。これによりその管理者は、データ・ラベルに関係なくすべての行を表示し、すべての既存のデータ行へのラベル付けが正しく行われるようにすることができます。

以下に、データ・ラベルを既存のデータへ適用する方法を示します。

1. SQL UPDATE文により、現在のユーザーのセッション・ラベルに基づいて制御される表のラベル・タグを移入します。
2. 必要とされるセッション・ラベルを含むデータベース・ユーザーを使用して、データを含む表を移入します。Oracle Label Securityによって制御される表にアクティブ・ポリシーが含まれる場合は、セッション・ラベルはロード時にデータに適用されます。Oracle Data Pumpをこの方法で使用して、データを他のデータベースからインポートすることもできます。
3. PL/SQLファンクションを書き込み、データの特性とセッションのコンテクストに基づいて行へラベル付けします。

パフォーマンスに関する考慮事項

すべてのアプリケーションにとって、パフォーマンスは重要です。新しい機能を既存のアプリケーションに追加する場合は、慎重に計画して適正評価を行い、パフォーマンスへの影響を最小限にする必要があります。Oracle Label Securityでは、アクセスを許可する前に各行にセキュリティ・チェックを実施し、ログイン認証時に追加セキュリティ・コンテキストを初期化します。遅延の長さは、Oracleポリシーの数と定義されているラベル・コンポーネントの数に応じて決まります。パフォーマンスは、以下を含むさまざまなファクタに応じて決まります。

- 設定されているOracle Label Securityポリシーの数
- Oracle Label Securityによって保護される表の数とサイズ
- 使用したOracle Label Securityの実施オプション
- 既存または新規のアプリケーションPL/SQLロジックの複雑さ

Oracle Label Securityポリシーを必要とする表を特定することは、実装前分析に不可欠な部分です。表のすべての行に常にアクセスがある場合、データ・ラベルを割り当てるLabel Securityポリシーを各行に適用することは推奨されておらず、おそらく冗長になります。Label Securityポリシーの適用先を慎重に考慮することにより、このテクノロジーを有効に使用できます。所定の要件に対応する場合、場合によっては、データ・ラベルを各行に割り当てるよりもOracle Databaseの他のセキュリティ機能を使用する方が適切です。たとえば、すべての行が常にアクセスされている場合、Oracle Database Vaultを使用して、いつ、どこで、なぜ、どのように表がアクセスされているのかを管理するほうが、すべての行にラベル付けするよりも効率的です。各セキュリティ・チェックの追加により、機能に関係なくパフォーマンス・オーバーヘッドが増加します。

オラクルでは、関連付けられたラベル・タグを定義し、データ・ラベルのレベルに関連付けられた範囲内に入るようにすることもお勧めします。たとえば、ConfidentialレベルとSensitiveレベルが2つのコンパートメントAlphaおよびBetaと一緒に定義されているとします。Confidentialに関連付けられている数は5000で、Sensitiveに関連付けられている数は10000です。有効なデータ・ラベルが定義される場合、ConfidentialレベルとコンパートメントAlphaおよびBetaに関連付けられたラベル・タグは、5000と10000の間の数になります。たとえば、データ・ラベルConfidential:Alphaのラベル・タグは5050に、データ・ラベルSensitive:Alpha,Betaのラベル・タグは10055になります。

Oracle PartitioningをOracle Label Securityと一緒に使用し、データ種別に基づいてデータを物理的にパーティション化することができます。たとえば、Highly Sensitive種別のデータは、Sensitive種別のデータとは別個のパーティションに格納できます。

パーティション化にはパーティション・プルーニングによるパフォーマンス上の利点もあり、Oracle Label Securityでは、ユーザーのセキュリティ認可の外部に存在するデータをすばやくスキップすることができます。パーティション化は、データウェアハウス環境で広く使用され、パーティション・エリミネーションを通じて問合せ最適化を提供する大規模な表に適用されており、Oracle Label Securityもこれを利用できます。Oracle Label Securityは、ユーザーのラベル外のパーティションに存在するデータをすばやくスキップします。

既存のコンポジット索引は、Oracle Label Securityによって追加されたポリシー列を含めるように変更可能です。これにより、複合問合せのパフォーマンスを実質的に向上させることができます。

いずれかのユーザーまたはストアド・プロシージャがすべてのデータにアクセスする必要がある場合は、そのユーザーまたはストアド・プロシージャに、Oracle Label Security固有のREAD権限またはFULL権限を付与することが推奨されます。これにより、オーバーヘッドを減らし、パフォーマンスを高めることができます。

LABEL DEFAULT実施ポリシー・オプションを使用すると、新規データにラベル付けする際のパフォーマンスのオーバーヘッドが最小になります。

アプリケーションの使用量に応じて、Oracle Label Securityによってアプリケーション表に追加される列でビットマップ索引を作成することを検討してください。通常、データ行の数と比較した一意のラベルの割合は低くなります。ビットマップ索引によってデータ・ロードの速度が低下しますが、select文でのパフォーマンスは向上します。

まとめ

データ種別は、need-to-know（知るべき人に限定）の原則を適用し、機密データを安全に統合する場合に重要です。従来、機密データは物理的に別個のシステムに保存されてきました。しかし、この方法だと、詳細な分析やビジネス・インテリジェンスを実行する能力が制限されます。

Oracle Label Securityは、業界で最先端の柔軟なデータ種別ソリューションです。ポリシー・ベースのアーキテクチャを採用するOracle Label Securityにより、データ・ラベルの定義、セキュリティ・ラベルの割当て、およびOracle Database内のアプリケーション表の保護を行うことができ、機密性のレベルが異なるさまざまなデータセットが同じデータベース内に存在できるようにすることによって、運用コストとストレージ・コストを削減できます。Oracle Label Securityポリシーにより、医療から司法および防衛機関に至る実質的にすべての業界のカスタム・データ・ラベルを定義し、アプリケーションの開発または再コーディングのコストを削減して、認可レベルに基づいた行レベルのアクセス制御の要件を満たすことができます。柔軟な実施オプションにより、コンプライアンスと規制のさまざまな要件を満たすようにアクセス制御を微調整できます。

Oracle Enterprise Managerでは、Oracle Label Securityポリシーを管理できます。Oracle Label Securityは、International Common Criteriaに従って独立評価されており、安全性の高い製品に対する政府および商業上の要件に準拠しています。

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