ORACLE

Oracle Label Security

Oracle Label Securityでは、データを行レベルで種別化してアクセス制御を適用し、許可されているデータ以外へのユーザー・アクセスを制限します。そのため、機密性のレベルが異なるデータを同じデータベースに混在させることが可能になり、運用コストやストレージ・コストを抑制できます。

2020年6月11日

本書の目的

本書では、Oracle Label Securityの最新リリースの機能および機能強化について概要を説明します。本書は、Oracle Label Securityの予防措置機能を使用する場合のビジネス・メリットを評価したり、データ・セキュリティ/ITプロジェクトを計画立案したり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なさらないでください。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、弊社の裁量により決定されます。

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の政府、軍隊、ならびに諜報機関の各標準に対応するように設計されていますが、Oracle Label Securityはユーザーに対してデータ分離要件を持つ商業組織にも適しています。政府機関と商業組織の両方が、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ながらデータ分析と意思決定を簡素化しています。
政府機関では、使用する複数のデータ種別標準を調整してから、Oracle Label Securityを使用して機関全体でデータを共有しています。商業組織では、Oracle Label Securityを使用してデータをさまざまな国から分離することで、さまざまな国のユーザーがデータにアクセスし、地域のプライバシ要件やコンプライアンス要件に対応できるようにしています。その他の会社では、子会社や小売店の類似するデータベースを統合しており、各グループが閲覧できるデータを制限する必要があります。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（このドキュメントでは以下ユーザー・ラベル）に基づいてアクセスを仲介します。Oracle Label Securityは、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Oracle Databaseの一部として評価されています。Oracle Label Securityは、API呼出しまたはOracle Enterprise Managerを使用して容易に管理できます。
Oracle Label SecurityはOracle Database Enterprise Editionで使用可能なオプションであり、Oracle Database Cloud ServiceのHigh Performance EditionとExtreme Performance Edition、Autonomous Cloud Database、およびOracle Exadata Cloud Serviceに組み込まれています。

Oracle Label Securityの概要

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、機密データへのアプリケーション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場合、別々のデータベース内の機密データを1つのシステムに結合することが必要になることがあります。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、本質的にユーザーごと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。データに機密性の程度（レベルと呼ばれる）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、Top Secretなどでデータにラベル付けされますが、医療アプリケーションでは、Public、Confidential、Restricted、Highly Restrictedなどでデータにラベル付けされます。

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、ごく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 selectを実行することです。この権限によって、ユーザーまたはロールは表内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つのことが行われる必要があります。まず、機密性が高いと見なされるデータはどれなのかをデータベースが認識する必要があります。次に、ユーザーのアクセス認可をデータベースが認識する必要があります。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。従来、この種の機能を実現するために使用されてきた設計手法は、データベースのビュー、トリガー、および検索テーブルに基づいています。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、アプリケーション間で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は組込みであり、データベース内のアプリケーション・レイヤーの下位で適用されるため、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が必要なくなります。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。

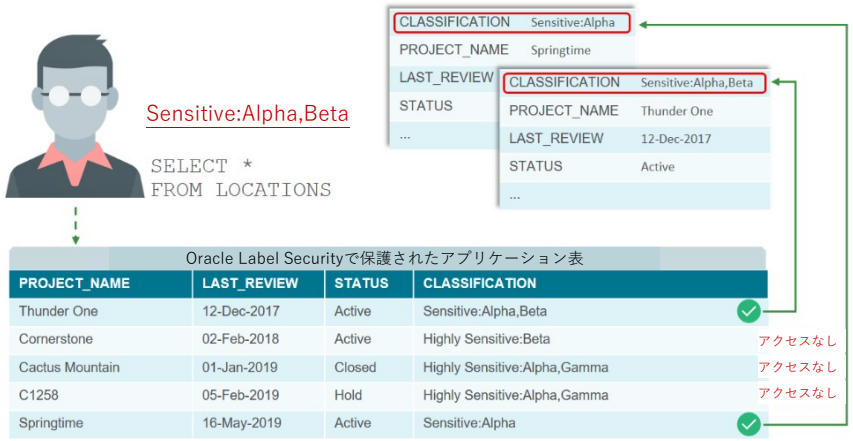

図1：Oracle Label Securityでは、ユーザー・ラベルとデータ・ラベルを利用してデータ・アクセスを制御

Oracle Label Securityは成熟した製品であり、単純な要件から複雑な要件まで対処できます。他の高度なセキュリティ製品と同様に、Oracle Label Securityのデプロイメントを成功させるためには、適切な分析と計画が重要です。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。実装を実行するには、Oracle Enterprise ManagerまたはOracle Label Security APIを使用します。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、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
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 （適用すると、特別な権限がユーザーに付与されない限り、データに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、コア・コンポーネント（データ・ラベル、ユーザー・ラベル）を説明してから、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・コンポーネントには、レベル、コンパートメント、およびグループがあります。これらのコンポーネントを使用して、データ・ラベルを作成したり、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・ラベルを割り当てたりします。レベルは、機密性の高いものから機密性の低いものへの順になっています。
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。グループでは、継承された関係または複数の親子階層関係を使用でき、親グループにアクセスできれば、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関連付けられています。コンパートメントのみまたはグループのみを使用するデプロイの場合は、デフォルトのレベルを1つ作成して、ユーザー・ラベルまたはデータ・ラベルに使用する必要があります。

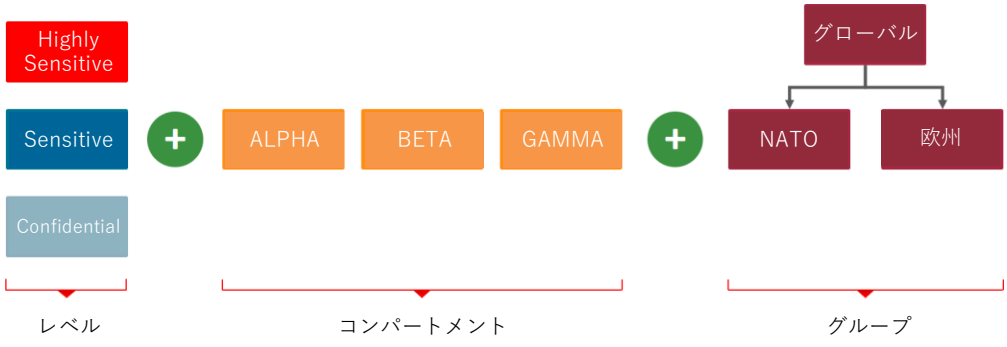

図2. Oracle Label Securityのデータ・レベルには、レベル、コンパートメント、およびグループがある

Oracle Label Security - データ・ラベル・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・ラベルおよびユーザー・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。組織で複数のレベルを必要としない場合は、デフォルトのレベルを1つ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あり、相互に独立しています。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、地域、またはプロジェクト（人事、財務、経理などの特定の承認を必要とする）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、グループごとに親子関係（階層）を設定できること以外は、コンパートメントによく似ています。グループは、組織構造別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。たとえば、EUで子グループとしてフランスとポルトガルを使用したり、北米で子グループとして米国とカナダを使用したりできます。

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	砂漠の嵐作戦 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 南米、メキシコ、ブラジル、アルゼンチン
医療	Confidential Public	患者 医師	Lab_Technician Medical_Assistant
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、1つ設定する必要があります。

データ・ラベルの使用

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は、組織のデータ・ラベルの要件を決定することです。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、および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の支援を得ることです。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。候補となる表を特定したら、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。データ分析者や、データについて把握しているユーザーの支援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のレベルと、最大で9999個の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。

テキストベースのデータ・ラベル表示では、コロンとカンマを使用して複数の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かどうかを選択できます。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文、insert文、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。

コンパートメント、グループ、またはその両方を使用するかどうかを決定するときには、必要なユーザー認可に関して違いを理解しておくことが重要です。

ラベル・コンポーネントに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、そのレベル以上に対して認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"レベルに対して認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認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、"Alpha"および"Beta"の両方のコンパートメントに対して認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つに対して、または親グループに対して認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グループに対して認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グループもそのデータにアクセスできます。ラベルでは、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が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関連（ER）ダイアグラムがある場合は、そのダイアグラムに各エンティティのデータ・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・ラベルによって、データ・ラベルで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。

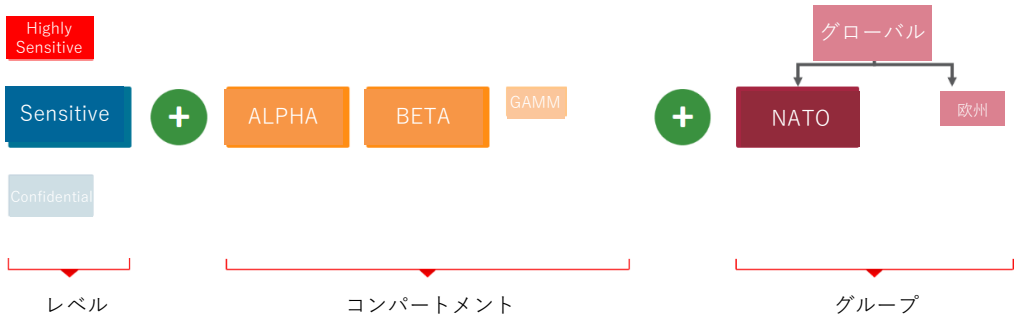

図3：ユーザー・ラベル・コンポーネントには、レベル、コンパートメント、およびグループがある

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るのを防止するために重要です。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

TABLE	DATA	USER			
		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**
	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	**アクセスあり**	**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**

レビューおよび文書化

収集した情報を実装担当者がレビューおよび文書化することは重要です。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のポリシー、Oracle Data Maskingの定義、表領域暗号化などの他のセキュリティ制御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な場所に保管する必要があります。

Oracle Label Securityの管理

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、構成や有効化は行われません。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。ドキュメントに記載されている手順に従って、Oracle Label Securityのポリシー、レベル、コンパートメント、およびグループを作成する必要があります。

マルチテナント環境を使用する場合は、Oracle Label Securityのポリシーを作成するプラガブル・データベース（PDB）でのみOracle Label Securityを有効化します。Oracle Label Securityはデータ・ディクショナリ・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、適用設定、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。オラクル提供の他のアカウントと同様に、Oracle 19c以降、LBACSYSはスキーマ限定アカウントとして構成されます。Oracle Label Securityを使用する場合、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、データベース・セキュリティ担当者はALTER USERコマンドを実行してLBACSYSにパスワードを指定する必要があります。Oracle Label Security管理者がロールの付与を完了したら、データベース・セキュリティ担当者はALTER USERをもう一度実行してLBACSYSをスキーマ限定アカウントにすることができます。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。日常的な使用には、Oracle Label Securityを管理する信頼できるユーザーにLBAC_DBAデータベース・ロールを付与することをお勧めします。

LBACSYSに保存されている情報へのアクセスは、ポリシー固有のロ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、認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も保持されます。

委任管理は、Oracle Label Securityを使用して実行可能です。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。このロールを、ポリシー・ラベル・コンポーネントおよびラベル認可の管理に使用できます。また、このロールは、ポリシーの管理を担当する名前付きユーザーに付与する必要があります。

Oracle Label Securityの適用除外

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の適用除外

例外	説明
SYSオブジェクト	Label Securityのポリシーは、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	Label Securityのポリシーは、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	Label Securityのポリシーは、DIRECTパス・エクスポート時には適用されません。
EXEMPT ACCESS POLICY	Label Securityのポリシーは、Oracle DatabaseのEXEMPT ACCESS POLICY権限が直接に付与されているユーザー、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。

トラステッド・ストアド・プロシージャ

トラステッド・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トラステッドになります。ユーザーに付与できるOracle Label Security権限を、トラステッド・ストアド・プロシージャに付与することもできます。これにより、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し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Database Vaultの機能

データベース内でユーザーが特定の運用タスクを実行できるかどうかを判別するために、Oracle Label Securityのさまざまな関数をOracle Database Vaultルール・セット内で使用できます。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には、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'句を追加する機能もあります。この'where'句は、アクセス権を決定するためにデータ・ラベルと併せて使用され、Oracle Virtual Private Database（Oracle 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のポリシーに付加されるため、純粋なOracle VPD実装の場合とは異なり、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およびData Redactionのポリシー

Oracle Label SecurityをData Redactionと一緒に使用でき、改訂ポリシーが適用されるかどうかを判別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・ラベルで改訂済みデータまたは未改定データへのアクセスが許可されている場合に、Data Redactionのポリシーを適用できます。

Oracle Identity Managementの統合

Oracle Label Securityは、Oracle Internet Directoryと統合することができます。この機能により、ポリシー定義、データ・ラベルおよびユーザー・ラベル認可の一元管理を実現しています。Oracle Label SecurityとOracle Internet Directoryの統合の詳細については、Oracle Label Security管理者ガイドを参照してください。

ベスト・プラクティス

データベース・ユーザーへのアプリケーション・ユーザーのマッピング

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層"の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。これを行うために、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・ラベルを、データベース・ユーザーのセッション・ラベルまたはそのサブセットと同じにできます。たとえば、複数のコンパートメントおよびグループにアクセスする代わりに、アプリケーション・ユーザーは1つのコンパートメントおよび1つのグループにアクセスできます。

既存データのラベル付け

既存データのラベル・タグにデータ・ラベルが移入されていない場合、Oracle Label Securityのポリシーがアプリケーション表に適用されると、どの行も表示されなくなります。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、既存データにデータ・ラベルを適用する方法を示します。

1. SQL UPDATE文を使用し、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. 必要なセッション・ラベルを持つデータベース・ユーザーを使用して、表にデータを移入します。Oracle Label Securityによって制御される表にアクティブなポリシーがある場合、データのロード時にデータにセッション・ラベルが適用されます。Oracle Data Pumpをこの方法で使用して、他のデータベースからデータをインポートすることもできます。
3. データの特性やセッションのコンテキストに基づいて行にラベル付けするように、PL/SQLファンクションを記述します。

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、慎重に計画を行って、パフォーマンスへの影響を最小限にするように適正評価を行う必要があります。Oracle Label Securityでは、アクセスの許可前およびログイン認証時に、各行にセキュリティ・チェックが適用されて、追加のセキュリティ・コンテキストが初期化されます。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。パフォーマンスのオーバーヘッドは、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

Label Securityポリシーを必要とする表を特定することは、事前分析の重要な部分です。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る場合は、Oracle Database Vaultを使用して表アクセスの時間、場所、理由、および方法を制御する方が、すべての行にラベル付けするよりも効率的な可能性があります。使用する機能に関係なく、実行される追加のセキュリティ・チェックごとに、パフォーマンスのオーバーヘッドが追加されます。

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・エリミネーションによって問合せが最適化されるため、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たり、大規模な表に適用されたりしています。Oracle Label Securityで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。

新規データにラベル付けする場合、LABEL DEFAULT適用ポリシー・オプションを使用すると、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。

結論

データ種別は、need-to-know（知るべき人に限定）の原則を適用する場合だけでなく、機密データを安全に統合する場合にも重要な役割を果たします。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 Label Securityのポリシー管理は、Oracle Enterprise Managerを使用して実行でき、Oracle Internet Directoryとの統合により一元化されたエンタープライズ管理を実現できます。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。

オラクルの情報を発信しています

+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

Oracle Label Security
2020年6月