ORACLE

Oracle Label Security

よくある質問

[1.0]

データ統合、プライバシー、コンプライアンスに関わ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、機密データへのアクセスをよりきめ細かく制御することの重要性が増しています。機密性の高い顧客データ向けに専用のデータベースを維持すると、コストがかさみ、不要な管理オーバーヘッドが発生します。ただし、データベースを統合すれば、複数の場所に格納された機密性の高い財務、HR、医療、またはプロジェクトのデータを1つのデータベースに統合して、コストを削減し、管理を容易にし、スケーラビリティを改善できることがあります。Oracle Label Securityには、データ・ラベルやデータ種別によってデータにタグを付ける機能があるため、データベースでは、ユーザーまたはロールにどのデータへの権限が許可されているのかを最初から把握でき、セキュリティを犠牲にすることなく、さまざまなソースからのデータをより広範なデータセットとして、同一の表に統合することができます。

機密データへのアクセスは、データ・ラベルと要求元ユーザーのラベルまたはアクセス認可を比較することで制御されます。ユーザー・ラベルまたはアクセス認可は、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。Oracle Label Securityは、アプリケーション・レイヤーの下位で、データベース内で一元的に適用され、これによりセキュリティが強化されて、複雑なアプリケーション・ビューが不要になります。

本書では、リリース23aiの機能と強化された点の概要が説明されています。本書は、23aiへのアップグレードに関するビジネス上の利点の評価と、説明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目的としています。

製品の概要

Oracle Label Securityとは何か

Oracle Label Securityは、Oracle Database Enterprise Editionのセキュリティ・オプションです。アプリケーション表のデータ行に添付されたラベル（機密ラベル）とユーザー・ラベル（認可ラベル）のセットを比較することで、データ行へのアクセスを仲介します。Oracle Label Securityは、Oracle Autonomous Databaseと、Oracle Cloud Infrastructure（OCI）データベースのHigh PerformanceおよびExtreme Performanceエディションにも搭載されています。

どのような業界がOracle Label Securityを検討すべきか

機密ラベルは、実質的にどの業界でも何らかの形で使用されています。そのような業界には、医療、法執行機関、エネルギー、小売、国家安全保障、軍需産業が含まれます。ラベルの使用例は次のとおりです。

- 支店、フランチャイズ、地域別のデータの分離
- 行政によってプライバシーが厳しく規制された複数の国々の顧客を抱えている金融会社
- R&Dの機密プロジェクトのデータの統合および保護
- 個人のヘルスケア記録へのアクセスを、医療行為を直接行う専門家のみに制限
- 企業の他部門からの人事データの保護
- 行政と国防での用途における、ユーザーの認可レベルに基づく機密データの保護
- 米国務省の国際武器取引規則（ITAR）への準拠
- マルチテナントのSaaSアプリケーションでの複数の顧客のサポート
- EU GDPRの下でのデータ処理の制限、合意の追跡、消去の権利に関するリクエストの処理

Oracle Label Securityは企業のセキュリティ・ニーズにどのように対処できるのか

Oracle Label Securityを使用すると、データにラベルを付け、細かい粒度でアクセスを制限できます。複数の組織、会社、またはユーザーが1つのアプリケーションを共有している場合に特に役立ちます。アプリケーションを変更することなく、機密ラベルを使用して、組織内のデータのサブセットにアプリケーション・ユーザーを制限できます。データ・プライバシーは消費者にとって重要であり、厳格な規制措置が継続的に制定されています。Oracle Label Securityを使用すると、データに対してプライバシー・ポリシーを実装して、必要最小限の人だけにアクセスを制限できます。

ORACLE

コンポーネントと機能

Oracle Label Securityのおもなコンポーネントは何か

Oracle Label Securityはアプリケーション・ユーザーに対し、行レベルのデータ・アクセス制御を実行します。各ユーザーと各データ・レコードには関連するセキュリティ・ラベルが付いていることから、ラベル・セキュリティと呼ばれています。

ユーザー・ラベルは3つのコンポーネント、つまり1つのレベル、ゼロ個以上のコンパートメント、ゼロ個以上のグループで構成されています。このラベルは、ユーザー認可の一部として割り当てられ、ユーザーが変更することはできません。

セッション・ラベルも同じ3つのコンポーネントで構成されており、ユーザーが確立したセッションに基づくユーザー・ラベルとは別物です。たとえば、ユーザーにTop Secretレベルのコンポーネントがあっても、Secretワークステーションからログインすると、セッション・ラベルのレベルはSecretになります。

データ・セキュリティ・ラベルには、ユーザー・ラベルおよびセッション・ラベルと同じコンポーネントがあります。3つのラベル・コンポーネントは、レベル、コンパートメント、およびグループです。

- **レベル**は、データの機密レベル、および機密データにアクセスするためのユーザーに対する認可を示します。そのレコードにアクセスするには、ユーザー（およびセッション）のレベルがデータのレベルと同じかそれ以上である必要があります。
- データはゼロ個以上の**コンパートメント**の一部であることがあります。ユーザーがレコードを問題なく取得するには、ユーザー/セッション・ラベルには、そのレコード・データ・ラベルが持つすべてのコンパートメントが含まれている必要があります。たとえば、データ・ラベルのコンパートメントがA、B、Cである場合、そのデータ・レコードにアクセスするには、セッション・ラベルに少なくともA、B、Cが含まれていなければなりません。
- データには、ゼロ個以上の**グループ**が含まれていることがあります。そのデータ・レコードにアクセスするには、ユーザー/セッションのラベルに、データ・レコードのグループと一致する1つ以上のグループが含まれている必要があります。たとえば、データ・レコードにBoston、Chicago、New Yorkのグループがある場合、セッション・ラベルにBoston（または他の2つのグループの1つ）さえあれば、そのデータにアクセスできます。
- 保護されたオブジェクトとは、ラベル付きのレコードが入っている表です。
- Oracle Label Securityのポリシーは、ユーザー・ラベル、データ・ラベル、および保護されたオブジェクトの組み合わせです。

Oracle Label Securityは、列レベルのアクセス制御に対応しているか

いいえ。Oracle Label Securityポリシーは列に対して機能しません。ただし、列を識別する仮想プライベート・データベース（VPD）ポリシーは、Oracle Label Securityユーザー・ラベルを評価することで、特定の列へのアクセスを判断できます。

特定の列（'機密性の高い'列）が、保護された表へのSQL文の一部である場合にだけアクティブになるように、VPDポリシーを作成することができます。'列の機密性'がオンになると、VPDは、ユーザーが閲覧を許可された機密性の高い列の情報を含んだ行だけを返すか、すべての行を返します。後者の場合、ユーザーがアクセス可能な値を除き、機密性の高い列のセルはすべて空です。

保護アプリケーション・ロールをOracle Label Securityに基づいて設定できるか

'set role'コマンドを実行するかどうかを決定するプロシージャは、Oracle Label Securityユーザー・ラベルを評価することができます。この場合、行ラベルはこのソリューションの一部ではないため、Oracle Label Securityポリシーを表に適用する必要はありません。

トラステッド・ストアド・プログラム・ユニットとは何か

ストアド・プロシージャ、ファンクション、およびパッケージは、定義者のシステムとオブジェクトの権限（任意アクセス制御（DAC））で実行されます。起動者が、Oracle Label Securityユーザー認可（ラベル）を持つユーザーである場合、プロシージャは、定義者のDAC権限と起動者のセキュリティ認可の組み合わせで実行されます。

トラステッド・ストアド・プロシージャは、Oracle Label Security権限である'FULL'または'READ'のいずれかが付与されています。トラステッド・ストアド・プログラム・ユニットが実行されると、有効なポリシー権限は、ユーザーの権限とプログラム・ユニットの権限を併せて起動します。

Oracle Label Securityで利用できる管理ツールはあるか

Oracle Enterprise Manager Cloud Controlは、便利で統合された環境でOracle Label Securityポリシーを作成して管理できます。

導入と管理

Oracle Label Securityはどこで入手できるのか

Oracle Label Securityは、Oracle Database Enterprise Editionのオプションです。Oracle Label Securityはデータベースの一部としてインストールされるので、あとは有効にするだけです。

Oracle Label Securityを使ってすべての表を保護するべきか

オラクルが提供する従来の任意アクセス制御（DAC）オブジェクトの権限であるSELECT、INSERT、UPDATE、DELETEに、データベース・ロールとストアド・プロシージャを組み合わせれば、ほとんどの表には十分です。Oracle Label Securityポリシーは、もっとも機密性の高い表に対してのみ適用する必要があります。

Oracle Label Securityの使用と機密ラベルの定義に関するガイドラインはあるか

はい、包括的なLabel Security Administrator's Guideをオンラインで提供しています。ほとんどの場合、Oracle Database Enterprise Edition（システムとオブジェクトの権限、データベース・ロール、保護アプリケーション・ロール）に搭載のセキュリティ・メカニズムがあれば、セキュリティ要件への対処には十分です。Oracle Label Securityは、個々の行レベルでセキュリティが必要な場合に検討してください。

Oracle Label Securityのアクセス制御ポリシーを適用した後、アプリケーションのパフォーマンスをどのように維持すればよいか

以下のベスト・プラクティスを参考にしてください。

- 保護が必要な表だけに機密ラベルを適用すること。複数の表を結合して機密データを取得する場合は、駆動表に機密ラベルを適用すること。
- Oracle Label Securityポリシーをスキーマに適用しないこと。
- 通常、各種データ種別ラベルの数は少ししかありません。表の大半がREAD操作に使用されている場合、（非表示の）Oracle Label Security列に対してビットマップ索引を作成し、この索引をその表の既存の索引に追加してみてください。

Oracle Label SecurityをOracle Database Vault、Real Application Security、Data Redactionと一緒に使用できるか

はい。Oracle Label Securityは、Oracle Database Vault内でファクタとして使用するユーザー・ラベルを提供でき、セキュリティ・ラベルをReal Application Securityユーザーに割り当てることができます。また、Oracle Label Securityは、Oracle Data Redactionとも統合でき、改訂ポリシーでセキュリティ認可を使用できます。

Oracle Label Securityを使用して、問合せで選択されるベクター行を制限できるか

はい。データ・ラベルは、ベクター型を含む行に適用できます。たとえば、生成AIモデルを構築する際、検索拡張生成中に検索されるデータ・サンプルをラベルによって制限できます。

詳細情報

Oracle Label Securityに関する詳細情報はどこで入手できるか

オラクルWebサイトのOracle Label Securityのページから、詳しい情報を参照してください。データシート、技術レポート、エンドユーザー向け文書など、さまざまな役立つ情報をオンラインで入手できます。

https://www.oracle.com/security/database-security/label-security/

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