Oracle Label Security

19c ORACLE Database

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大き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許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。

製品の概要

Oracle Label Security とは何か

Oracle Label Security（OLS）はOracle Enterprise Editionデータベースのセキュリティ・オプションで、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（許可ラベル）のセットとを比較することで、データ行へのアクセスを仲介します。

ORACLE

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統合および保護
- 個人のヘルスケア記録へのアクセスの制限
- 他の部門からの人事データの保護
- 行政と国防を用途とする機密データの保護
- 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。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。アプリケーションを変更する必要はありません。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。

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、Label Security 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、ユーザー許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、3 つのコンポーネントがあります。ラベル・コンポーネント – 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への許可を示します。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ないと、そのレコードにアクセスできません。
- 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、グループ・コンポーネントに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 は列を認識しません。

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、OLS 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。このタイプの OLS と VPD の統合例については、OLS OTN Web ページのホワイト・ペーパーを参照してください。

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、ユーザーが閲覧を許可された値を除き、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

はい。'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、OLS 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、OLS ポリシーを表に適用する必要はありません。この例は、OLS OTN Web ページのホワイト・ペーパーに掲載されています。

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（DAC）で実行されます。起動者が、OLS ユーザー許可（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許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、OLS 権限である'FULL'または'READ'のいずれかが付与されたプロシージャです。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 Database 11g Release 1 以降、Oracle Policy Manager の機能（および他のほとんどのセキュリティ関連の管理ツール）が Oracle Enterprise Manager Cloud Control で利用可能になったため、管理者は OLS ポリシーを最新の便利な統合環境で作成し、管理することができます。

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 の一部であるオプションです。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。さらに、OLS を機密表に適用する前に、いくつかの点を考慮する必要があります。考慮事項については、OLS OTN Web ページにある『Oracle Label Security – Multi-Level Security Implementation』というホワイト・ペーパーを参照してください。

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。また、Oracle Technology Network にあるホワイト・ペーパーと技術リソースで例を示しています。これらの資料では、推奨される実装ガイドラインの一覧が紹介されています。ほとんどの場合、Oracle 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）で無償提供されるセキュリティ・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 のポリシーとユーザー・ラベル（許可）を Oracle Identity Management に一元的に保存することはできるか

エンタープライズ・ユーザー・セキュリティを使って、データベース・ユーザーを Oracle Identity Management に一元的に保存し、管理できるだけでなく、Oracle Label Securityのポリシーとユーザー許可を Oracle Identity Management にも保存し、管理することもできます。これで分散環境におけるポリシー管理が大幅に簡素化され、セキュリティ管理者は、一元管理されている全ユーザーにユーザー許可を自動的に付加できます。

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。

- 本当に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、駆動表を検索します。
- LS 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)OLS 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。
- 製品の OTN Web ページにある Oracle Label Security のホワイト・ペーパーを参照すること。Oracle Label Security を使用する際のパフォーマンスに関する考慮事項が詳細に説明されています。

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

はい、できます。Oracle Label Security は、Oracle Database Vault 内で係数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 Advanced Security Data Redaction とも統合でき、Data Redaction ポリシーでセキュリティ許可を使用できます。

その他の情報

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

Oracle Technology Network（OTN）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、ホワイト・ペーパー、顧客事例、エンドユーザー向け文書、ディスカッション・フォーラムなど、有益な各種情報をオンラインで入手できます。

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

19c ORACLE Database

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/cloudsecurity/db-sec　facebook.com/oracle　twitter.com/oracle

Integrated Cloud Applications & Platform Services

ORACLE