ORACLE Security

Oracle Data Safeを用いた重要データの保護

統合されたコントロール・センターによる機密データ管理でクラウド・データベースのセキュリティを向上

ホワイト・ペーパー/2019 年 9 月 11 日

ORACLE

免責事項

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。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。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。

機密データをクラウドで保護する必要性の高まり

現在、多くの組織がデータをもっとも価値のある資産の 1 つであると考えています。ただし、データは適切に保護されなければ、すぐに負債となってしまいます。実際のところ、大規模なデータ侵害や、個々のシステムやデータベースへの攻撃についての話題を毎日のように耳にします（補足記事を参照）。プライバシーへの関心が高まるにつれ、組織がユーザー・データを取り扱う方法を示した規制が増えています。これには、欧州連合の一般データ保護規則（GDPR）、米国の医療保険の相互運用性と説明責任に関する法律（HIPAA）、新しいカリフォルニア州消費者プライバシー法（CCPA）、その他の管理機関によるものがあります。これは多額の費用がかかる問題であり、違反に関連する罰金によってその度合いがさらに高まっています。たとえば、Marriott は 9900 万ポンド以上の罰金の支払いを余儀なくされ、British Airways は最近の GDPR 侵害に対する 1 億 8300 万ポンドの罰金に直面しています。

攻撃者は、国民国家のフルタイム従業員、犯罪組織の一員、または単なる詮索好きかもしれませんが、彼らに一つ共通しているのは、セキュリティ戦略の不備を利用する傾向があるということです。ビジネスの運用に大損害を与えるために設計された攻撃もあれば、データを盗むという、より明確な目的に動機付けられた攻撃もあります。通常、データはデータベースに保存されているため、後者の攻撃はハッカーにとって主要なターゲットとなります。

このような外部からの絶え間ない脅威に加え、企業は社内ユーザーからの脅威にも直面しています。故意の場合もあれば、セキュリティ・ソフトウェア構成や関連データについての不注意による誤り、見落とし、見過ごしによる場合もあります。

今日の分散型の作業チームでは、問題を悪化させるだけです。組織は、社内の DevTest チームや外部パートナー組織を含む、さまざまな地域の多様なユーザーを幅広く管理する必要があり、それらすべてに企業データベースへの異なるアクセスレベルが必要です。

意図的な侵害と意図しない侵害の両方を減らすには、企業は機密データを特定し、それを適切に制御して保護し、データベース管理システムでそのデータの使用状況を常時監査する必要があります。ビジネス・リーダーの中には、これらのセキュリティ上の課題のためにデータベースをクラウドへ移動することに不安を抱く人もいますが、機密データを保護する専門知識が社内で不足しているために、事態はますます悪化します。

ニュースに見られるデータ侵害

- 2019 年、Capital One は上位 10 件に入る大規模なデータ侵害について報告しました。そのデータ侵害は、コード共有 Web サイト GitHub にハッキングの詳細が投稿されたのちに発覚しました。
- 2019 年 4 月、米国のおよそ 8000 万世帯に関する個人情報を含む、Microsoft Azure 上でホストされた保護されていないデータベースが vpnMentor によって発見されました。
- 2018 年 2 月、FedEx は、保護されていない Amazon Web Services（AWS）クラウド・ストレージ・サーバー上のデータベースの顧客 119,000 名分の個人情報が不注意によって流出したことに気付きました。この件は Kromtech Security によって発覚し、発覚するまでの 4 年間、情報は保護されていなかったと推定されます。

コンプライアンスのコスト

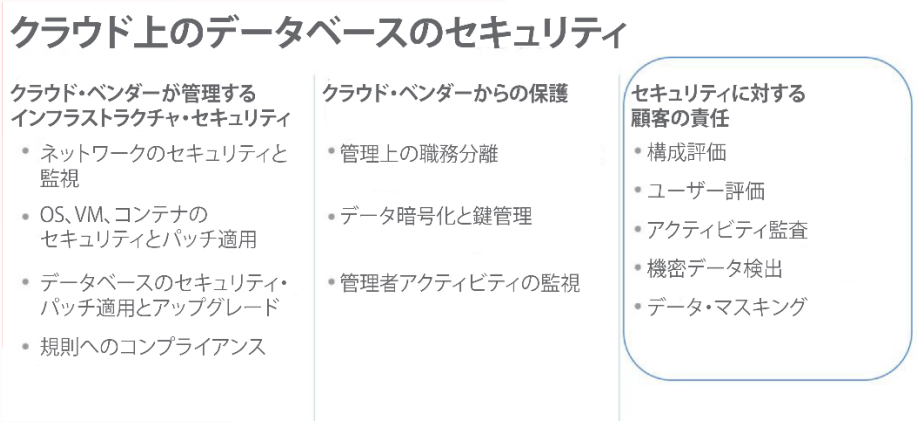
- GDPR による罰金は最大で年間収益の 4 パーセント
- HIPAA による罰金は違反 1 件につき最大で 150 万米ドル

CCPA による罰金は 1 個人あたり 700 ドルに加えて訴訟費用

本書では、クラウド・データベースのデータ・セキュリティを確保する統合された包括的なクラウド・サービスである Oracle Data Safe について説明します。Data Safe は、セキュリティおよびユーザー・リスク評価、ユーザー・アクティビティ監査、機密データ検出、およびデータ・マスキングを通してデータベース保護を支援します。この十分に統合された使いやすいソリューションにより、あらゆる業種のあらゆる規模のクラウド・データベースの顧客が、データベースのセキュリティ要件を非常に簡単に満たすことができます。

Oracle Data Safe でセキュリティを誰にでも使いやすいものに

データとアプリケーションがクラウドへ移動するにつれて、組織の資産を保護する責任は急速に複雑になります。クラウド・サービス・プロバイダがグローバルなインフラストラクチャを保護してクライアント・データベースを社員のアクセスから保護する責任を負う一方で、クラウドの各顧客はそのユーザーとデータを保護するための独自の方法を実装する必要があります。



たとえば、Infrastructure as a Service（IaaS）環境では、クラウド・プロバイダによってクラウド・インフラストラクチャ、オペレーティング・システム、ネットワーク・サービスは保護されますが、データにアクセスするアプリケーションやユーザーは保護されません。組織は、データベースに含まれる機密データの内容と、そのデータにアクセスできるユーザーを決定する責任があります。これは各企業の業界、オペレーション、顧客ベース、およびビジネス目標に固有のものであるため、クラウド・ベンダーが決定できるものではありません。

組織のデータを正しく保護するためには、データの構成方法、データを使用している人、そして各データベースに含まれる機密データのタイプを最初に把握することが必要です。これは、誰が（サンプル・データ、マスクされたデータ、または集計データではなく）本番データにアクセスする必要があるかを追跡し続け、データが不要になったときにそのデータを削除するためのプロセスを整備することも意味します。

Oracle Data Safe はこの多面的なセキュリティ戦略の重要な部分を成しており、ユーザーと構成を保護すると同時に、データ・セキュリティ・コンプライアンス要件を満たすのに役立つ、一連の機能が統合されています。Oracle Data Safe は、クラウドでのデータ・セキュリティ管理を一元的に制御します。

Oracle Data Safeはクラウド・データベース向けの統合されたセキュ リティ・コントロール・センターを提供

Data Safe でデータベース・セキュリティのレベルを向上

- 1 つのまとまった環境からデータベース・セキュリティの完全なビューを取得
- 特別な専門知識は不要、多くの異なるツールをまとめる必要もなし
- インストールやメンテナンスの必要なし

5 つの簡単な手順による機密データへのアクセスの制御

多くの場合、エンタープライズ・データベースには大量の個人情報が含まれており、これはデータを盗んでビジネス・プラクティスを妨害したいハッカーにとって魅力的なターゲットとなります。強力な防御を実装するには、どこに機密データがあり、誰がそのデータにアクセスしているのかを詳しく知る必要があります。さらに、どのようなリスクがユーザーに関係するかを知り、アクティビティを監査できるようにすることが適切なセキュリティ態勢のために重要です。Oracle Data Safe を使用すると、以下の相互に関連する 5 つのコンポーネントによってこれらのタスクを体系的に完了できます：

» セキュリティ評価

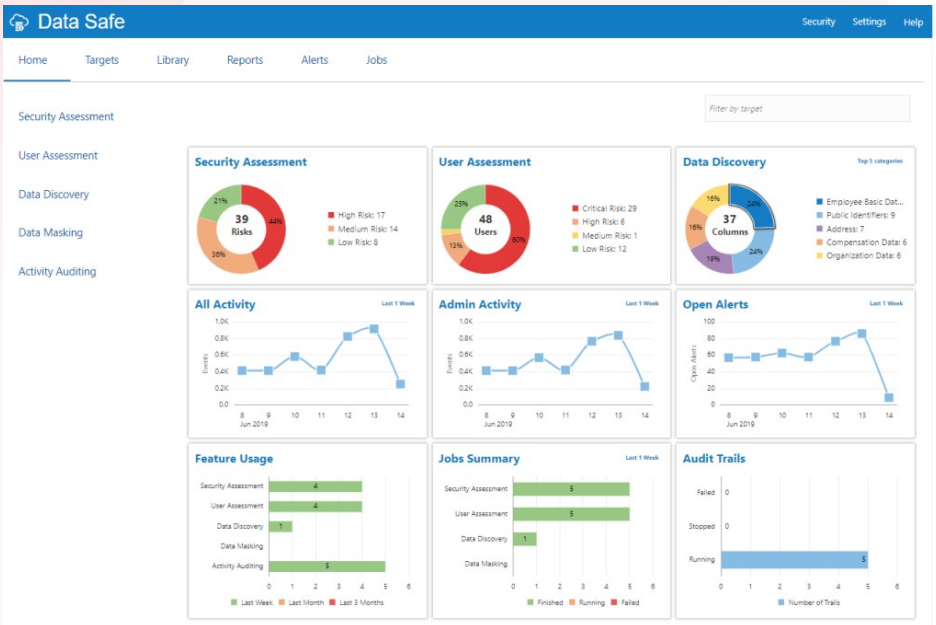
» ユーザー評価

» アクティビティ監査

» データ検出

» データ・マスキング

Oracle Data Safe では、これら 5 つのコンポーネントを統一された使いやすい環境にまとめて置いているため、データを保護するための複数のツールや高いスキルを持ったデータベース・セキュリティの専門家を必要としません。好評を得ているこのサービスは、今日では Oracle Cloud Infrastructure 上のデータベースで使用できます。

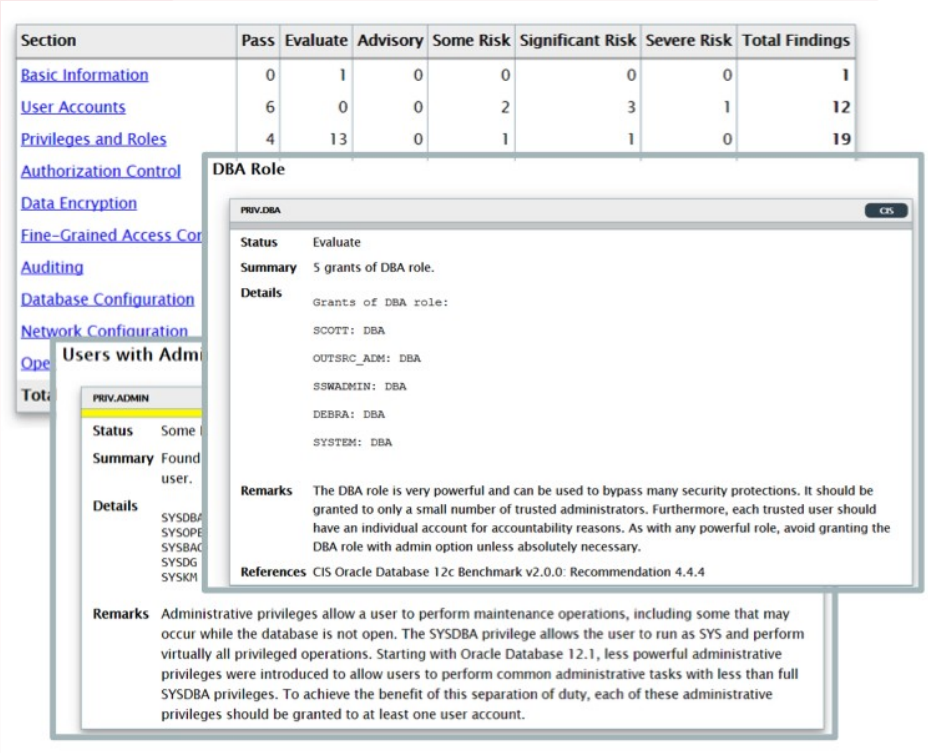


Oracleクラウド・データベース向けの統合されたセキュリティ・コントロール・センター

手順 1：セキュリティ評価

セキュリティ評価は、構成戦略に不備があるかどうかの判断を支援し、それらの不備を修正する方法についての指針を提供します。セキュリティ評価機能によって、セキュリティの脆弱性を特定し、暗号化、監査、およびアクセス制御が実装されていることを検証できます。

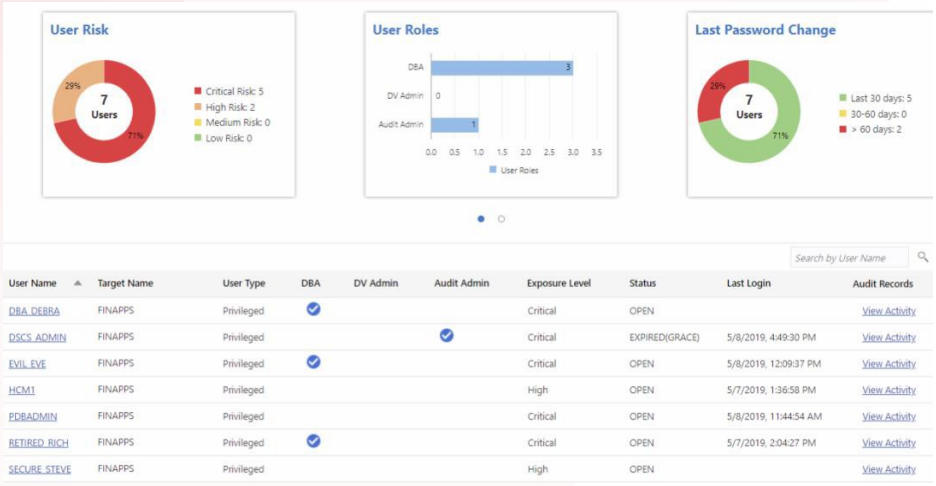
Oracle Cloud Database は、顧客が異なる要件に対応するためにユーザー、権限、およびセキュリティ制御を構成する方法に柔軟性を与えます。たとえば、顧客の機密データを含む本番システム向けに実装されたユーザーおよびセキュリティ制御は、合成テスト・データを含む開発システム向けのセキュリティ制御とは異なることがあります。Oracle Data Safe のセキュリティ評価機能を使用すると、セキュリティ構成パラメータを検証できるため、正しいレベルのセキュリティと制御をアプリケーションごとに実装できます。たとえば、デフォルトのパスワードがいつ使用されているか、ユーザーがいつ必要以上の権限を持っているか、といったことを特定できます。検索結果や推奨事項は、欧州連合の一般データ保護規則（EU GDPR）と Center for Internet Security（CIS）ベンチマークの双方に対応しています。



セキュリティ評価を使用してセキュリティ・パラメータを検証しアプリケーション制御を実装

手順 2：ユーザー評価

Oracle Data Safe に含まれるユーザーの評価および監視機能により、特に特権ユーザーと特権アカウントに関連するリスクを特定できます。これにより、アカウントが侵害されたり、不正を行ったりした場合に大きなリスクをもたらすデータベース・ユーザーを特定できるようになりました。コンテキストこれらのアカウントについては、監視のレベルを上げたり、可能な場合はロールのコンテキスト内で権限を減らしたりすることが必要な場合があります。ユーザー評価レポートにより、ロックまたは削除対象の休眠アカウントを迅速に特定できます。ユーザー評価レポートからアクティビティ監査機能へのリンクにより、ユーザーが実行する監査対象アクティビティが表示されます。



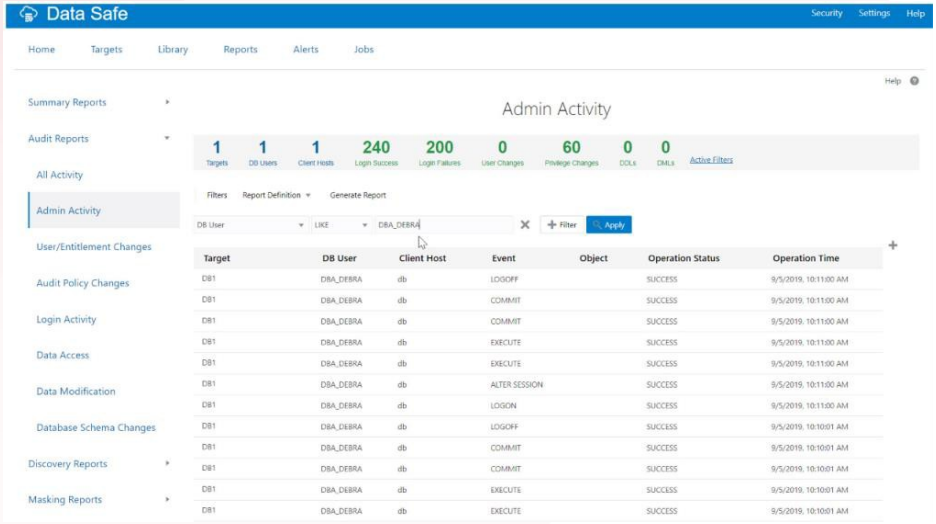
ユーザー評価機能により管理者は特権アカウントの特定と評価が可能

手順 3：アクティビティ監査

Data Safe のアクティビティ監査を使用すると、Oracle Cloud データベース上のユーザー・アクティビティを監視して、業界および規制遵守の要件ごとに監査記録を収集して維持し、異常なアクティビティに対してアラートを起動することができます。機密データの変更、管理者およびユーザーのアクティビティ、および Center for Internet Security が推奨する他のアクティビティを監査できます。アラートを設定できるのは、データベース・パラメータまたは監査ポリシーが変更された場合、管理者による失敗したログインが発生した場合、ユーザー・エンタイトルメントが変更された場合、そしてユーザーが作成または削除された場合です。Oracle Database には事前定義されたポリシーが多数含まれ、そのいずれも Data Safe を通じて数回クリックするだけで有効化できます。

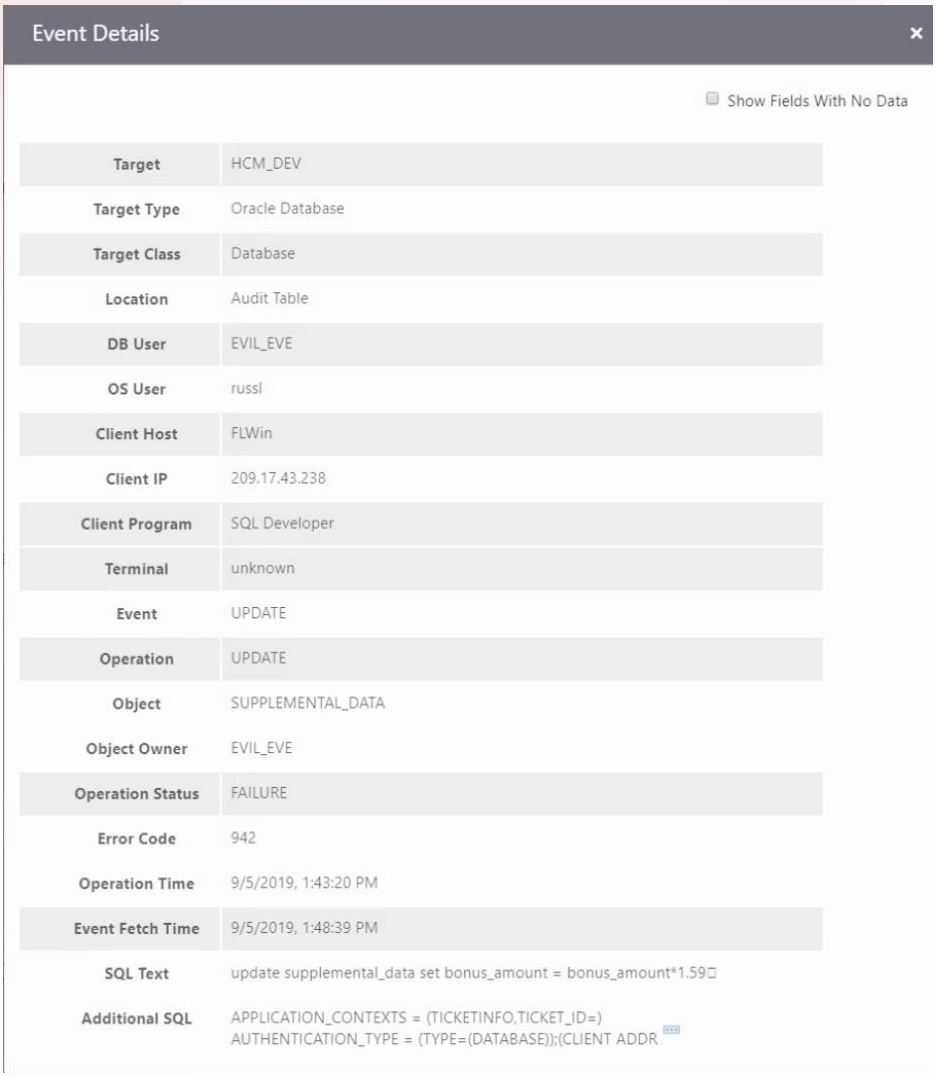
Data Safe ダッシュボード（6 ページを参照）を使用すると、アラートを含むアクティビティの傾向を素早く見つけられます。ダッシュボードでは、監査証跡のステータスをチェックして（監査証跡によって、データベースのどこで監査データを参照すればよいかが Data Safe 上で分かります）、監査アクティビティ全体を閲覧することもできます。

アクティビティ監査レポートには、収集されたイベントおよびアラートのサマリー、すべての監査済みアクティビティ、監査ポリシーの変更、管理者アクティビティ、ログイン・アクティビティ、データベースの問合せ操作、DDL、DML、ユーザーおよびエンタイトルメントの変更などがあります。生成されたアラートを表示させて、フィルタリングして検索することができます。アラートと監査データ・レポートは、どちらもカスタマイズして PDF または XLS 形式で保存またはダウンロードできます。



管理者アクティビティ・レポート

Data Safe のアクティビティ監査は、以下の簡単な 3 段階のプロセスで設定できます：1) 監査するターゲットを選択 2) 収集される監査情報を指定する監査ポリシーをプロビジョニング 3) 監査情報の収集元を Data Safe に伝える監査証跡を作成。



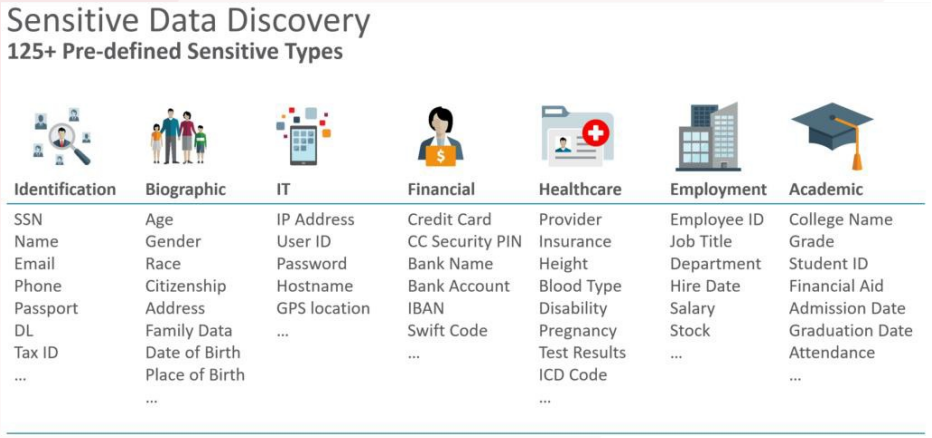
イベントの詳細

設定が完了すると、Data Safe は自動的に監査データを取得し、それをセキュアな Data Safe リポジトリ（削除や変更が行われないよう、監視されるデータベースから分離）に保存します。Data Safe アクティビティ監査で使用できる事前定義されたアラートに基づいて、おもなイベントにアラートを設定できます。インタラクティブなレポートにより、監査データを参照して必要に応じてそれをフィルタリングし、セキュリティ要件やコンプライアンス要件に対応するように定期レポートを作成できます。

自社のデータベースがどれほど安全なのか、どれほどの量の機密データを保有しているのか、それはどこに保存されているのかを実際には把握していない企業が多数あります。

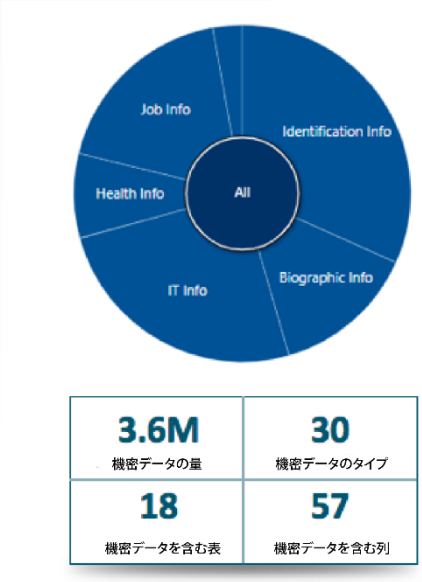
手順 4：データ検出

複数の開発チームが存在し、データが複数のデータベースに分散している状況では、機密データの保存場所をいつも簡単に把握できるとは限りません。データを保護するためには、自社でどのような種類の機密データをどれほどの量保有していて、それがどこに保存されているのかを理解する必要があります。機密データ検出機能を使用すると、保護すべきデータを決定できます。ここでは、PII、IT データ、財務データ、雇用データ、健康データなどの 125 種類以上の機密データを特定して分類できます。



データ検出機能で事前定義されている機密データの種類

個人情報や医療情報など、検出したい機密データのカテゴリを選択できます。また、自社の要件に合致した新しい種類の機密データのカスタム・カテゴリを簡単に定義できます。

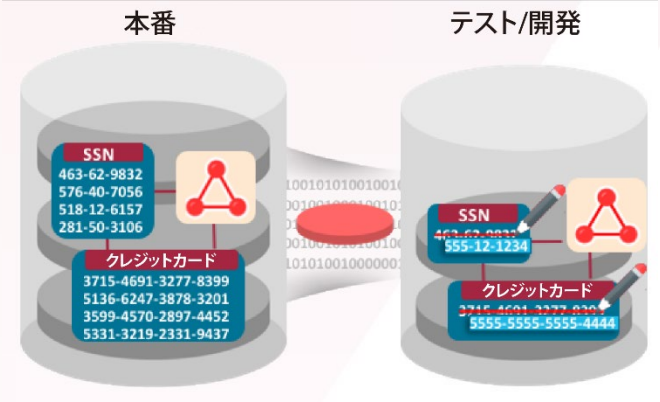


機密データに関するデータ検出レポート

手順 5：データ・マスキング

テスト・チームや開発チームと本番データを共有できることで、実際のデータを通じてアプリケーションの品質を向上させることができます。ただし、本番システムをコピーすると、本番環境ほど十分に保護されていない環境にすべての機密データ（およびそのデータに関連するリスク）が移ってしまいます。その上、クレジットカード番号などの機密データは実際は必要のないものです。ここで、データ・マスキング機能の登場です。データ・マスキング機能は、アプリケーション・データベース内の機密データを架空でありながら現実的な値に置き換えます。そして、それらのデータセットは、アプリケーション開発者、アプリケーション・テスト担当者、およびパートナーと共有できます。これにより、機密データを公開することなしに、現実的なデータセットをアプリケーションのテストおよび開発向けに渡すことができます。データ・マスキングはデータ検出と統合さ

れているため、検出された機密データに対して互換性のあるマスキング形式が自動的に提案されます。Data Safe では、わずか数回のクリックで機密データを検出してマスキングできます。



データ・マスキングは機密データを難読化することでリスクを軽減。

データ・マスキング機能は、シャッフル・マスキング、条件付きマスキング、複合マスキング、SQL 式マスキング、ユーザー定義のマスキング、および他のマスキング形式をサポートし、リレーションの整合性を維持します。

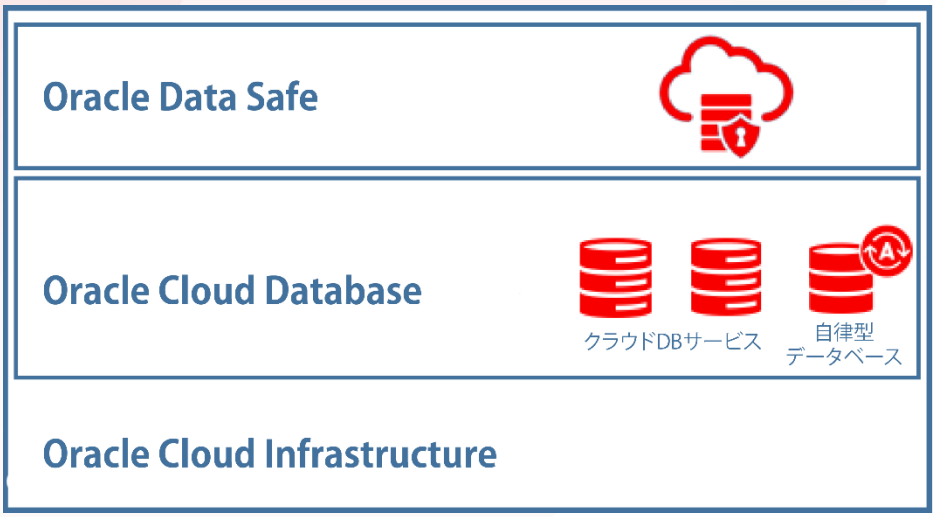
Oracle Data Safe のデータ・マスキング機能は、機密データ検出プロセス中に検出された情報を使用して、社会保障番号、クレジットカード番号、財務データ、給与情報、個人医療情報などを保護するデータ・マスキング・ポリシーを作成します。データ・マスキング機能は、開発、テスト、およびパートナーのデータベース内で、実際のデータを偽装しながらも現実的なデータと置き換え、50 以上の事前定義されたマスキング形式を含みます。

患者の機密データを含む仮説のシナリオ

医療機関が診断のテスト結果を保存するために使用するデータベースについて考えてみましょう。Oracle Data Safe を使用すると、セキュリティ・チームはデータベース構成（パスワード・ポリシー、パラメータ設定、パッチ・レベルなど）を評価して、データベースがベスト・プラクティスに従って構成されていることを確認できます。そして、データベース・ユーザーを迅速に評価して、データに不適切にアクセスした場合にもっともリスクをもたらす権限を持つユーザーを特定し、そのユーザーのデータベース・アクティビティを監視するための監査ポリシーを構成できます。また、機密データ検出機能を使用してデータベースをスキャンし、患者の機密データを含むスキーマ、表、および列を特定できます。テストや開発、またはパートナー向けにデータベースのコピーが作成された場合は、機密データは自動的に現実的な見た目のトライアル・データに置き換えられます。これらはすべて、単一のコンソールからわずか数分で実行できます。

すべてを統合

Data Safe は Oracle Cloud Infrastructure 上で実行され、インフラストラクチャ自体から最新の自己保護型 Oracle Autonomous Database までを網羅する包括的なセキュリティ戦略の重要な部分を成しています。以下の項では、この関係についてさらに詳細に説明します。



Oracle Data SafeとAutonomous DatabaseおよびOracle Cloud Infrastructureとの関係

オラクルは、以下のようなクラウドの顧客のセキュリティに関する多くの重要な懸念に自動的に対処します：

- ネットワークのセキュリティと監視
- OS およびプラットフォームのセキュリティ
- データベースのパッチ適用とアップグレード
- 管理上の職務分離
- デフォルトでのデータ暗号化

Oracle Autonomous Database によるデータベース・セキュリティの向上

Oracle Data Safe は、Oracle Autonomous Database の自己保護機能を拡張し、使用中のデータを保護し、そのデータにアクセスするユーザーを継続的に監視します。オラクルには、データを保護し、DBA の負荷を減らして価値の高いタスク（データの把握や正しい保護と制御の設定など）に集中できるようにするための多岐にわたる戦略があります。

Oracle Autonomous Database に含まれる AI および機械学習テクノロジーにより、外部からの攻撃と悪意のある内部ユーザーの両方からデータベース管理システムを保護します。たとえば、データベースは停止時間なしでセキュリティ・パッチを自動的に適用できます。

Oracle Autonomous Database は、セキュリティ構成の自動的な維持など、データベースの管理やチューニングのタスクを簡略化する革命的なクラウド・サービスです。たとえば、クラスタのノード間でローリング方式で自動でパッチを適用することにより、アプリケーションの停止時間なしに Oracle Autonomous Database 自体を保護します。セキュリティ・パッチは、四半期ごと、または必要に応じて、ファームウェア、オペレーティング・システム、クラスタウェア、およびデータベースに停止時間なしで適用されます。

パッチの適用は、全体の一部に過ぎません。データベースも、暗号化を常時オンにしてそれ自体を保護します。暗号化は、侵害によってハッカーがデータ・ブロックに直接アクセスできる状況でデータを保護します。このプラクティスにより、たとえ機密データを含むデータベース・ファイルがコピーされても、サイバー犯罪者にとっては役に立たなくなります。Oracle Autonomous Database は、送受信中も、保存中も、バックアップされている間も、顧客データを暗号化します。

Oracle Autonomous Database を使用すると、データベース管理者は、データベースのチューニング、パッチ適用、バックアップなどの日常的に繰り返される管理作業から開放され、アプリケーションの管理や機密データのセキュアな維持など、価値の高いタスクに集中できます。

Oracle Cloud Infrastructure による複数層でのセキュリティ

オラクルは、セキュリティの脅威を防止、検知し、迅速に対応するインテリジェントなクラウドベースのプラットフォームによって、今日の複雑なデータベース環境を保護します。たとえば、Oracle Cloud Infrastructure は、堅牢なクラウド・インフラストラクチャに必要な独立性、データ保護、制御、および可視性を顧客に確実に提供するための核となる 7 本の柱に基づいています。オラ

クルの機械学習アルゴリズムは、セキュリティ・オペレーション・センター（SOC）のアクティビティにインテリジェント機能を追加し、クラウド・アクセス・セキュリティ・ブローカ（CASB）によってクラウド・アプリケーションへの脅威が自動で検出されます。エッジでのオラクルのセキュリティ・サービスには、分散型サービス拒否（DDoS）保護、およびインターネットベースの脅威を防ぐ Web アプリケーション・ファイアウォールが含まれます。最終的にオラクルは、24 時間 365 日体制のネットワーク・オペレーション・センター（NOC）の高度に訓練されたスタッフによって、お客様のインフラストラクチャを保護する責任を担います。オラクルのセキュリティに関するテクノロジー、プロセス、およびオペレーションによって、クラウドへ移行するリスク、コスト、および複雑性が軽減されます。オラクルは複数の防御層を備えており、データを保護してサイバー脅威を阻止するコアツーエッジのクラウド・サービスによってサイバー脅威に対抗します。

結論

データベースがクラウドへ移行するにつれて、企業はデータがどのように管理され、アクセスされているか、そして誰がデータを使用しているかを積極的に監視する必要があります。クラウド・プロバイダはお客様のインフラストラクチャとプラットフォーム・サービスを保護しますが、お客様のアプリケーション、ユーザー、そしてデータの保護はお客様次第です。Oracle Data Safe のクラウド・サービスは、構成およびユーザーの評価、コンプライアンスに対応したユーザー・アクティビティの監査、マスキング対象となる機密データの特定など、お客様のセキュリティ・ニーズをすべて統合します。これらをすべて単一のダッシュボードを用いて行うことで、お客様のデータ資産を迅速かつ簡単に保護できます。

Oracle Database セキュリティについて詳しくは、こちらを参照してください：
http://www.oracle.com/database/technologies/security/data-safe.html

ORACLE CORPORATION

World Headquarters

500 Oracle Parkway

Redwood Shores, CA 94065,

海外からのお問い合わせ窓口

電話：+1.650.506.7000

ファクシミリ：+1.650.506.7200USA

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。

Integrated Cloud Applications & Platform Services