ORACLE

リスク・レベルに基づく データベース・セキュリティ

Oracle Databaseを保護するための実践的なアプローチ

2020年4月 | バージョン20.01

目的

このテクニカル・ホワイト・ペーパーでは、Oracle Databaseの保護の概要について説明します。機能、オプション、無償で提供される製品についても説明します。本書は、セキュリティ・リスクを低減し、お使いのOracle Databaseの規制遵守を向上するための選択肢を評価できるよう支援することを目的としています。

対象読者

本書は、Oracle Databaseのセキュリティ制御を設計、実装、保守、または操作する責任を担うユーザーを対象としています。

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

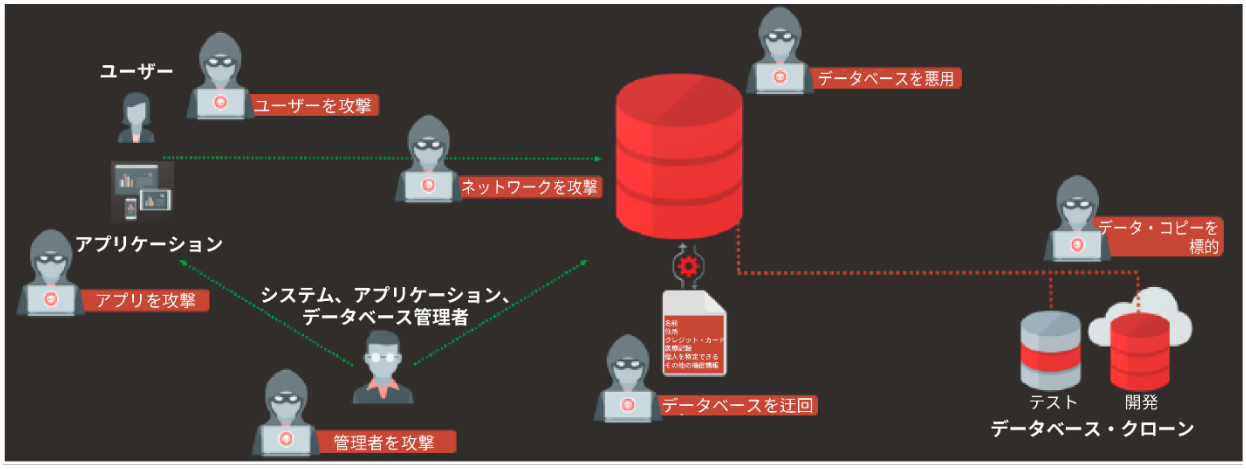
Oracle Databaseには世界のリレーショナル・データの大部分が保管されており、これには、データ窃盗の第一の標的である機密データも含まれます。そのような機密データを窃盗や悪用から保護する必要があります。組織がデータを保護する必要性は、以下の主要な2つの必須事項によって後押しされています。

- 規制要件 – データ・プライバシを管理する国内法は117を超え（EU一般データ保護規則（GDPR）、カナダの個人情報保護および電子文書法、日本の個人情報保護法、オーストラリアのプライバシ原則、ブラジルの個人情報保護法など）、さらに州政府や地方政府の法令や規制（カリフォルニア州消費者プライバシ法、ケベック州プライバシ法など）、業界規制（PCI、米国FFIEC、米国HIPAA、EU PSD2、BASELなど）が非常に数多く存在します。さまざまな法令や規制をすべて記載すると、本書は非常に長くなり、またそのような一覧は、ほぼすぐに古い情報になるでしょう。規制を遵守しない代償は極めて大きい可能性があります。米国HIPAAの過去3年間の罰金は8,700万ドルを超え、EU GDPRの個別の罰金は2億ユーロに達します。
- データ窃盗の懸念 – データには価値があり、データ窃盗者は多くの時間を費やしてデータを盗みます。残念なことに、窃盗は頻繁に成功します。毎年、数十億もの個人データ・レコードが盗まれ、数千ものデータ侵害が明らかになっています。この窃盗の経済的な影響は計り知れず、容易に数兆ドルに上ります。

本書では、データの窃盗（または悪用）の防止と極めて密接にかかわる、リスクの低減に重点を置きます。リスクの低減に重点を置きますが、ここで説明する制御は、規制遵守で不可欠な役割を果たします。結局のところ、データ・セキュリティを重視するほとんどの規制は、リスク管理の試みなのです。

データを保護すべき理由が分かりましたので、Oracle Databaseを保護する方法についてお話しします。どのような機能、オプション、製品があり、それらをどのように組み合わせることで、各自の機密データに適切なレベルの保護を提供できるかを説明します。

本書は製品ドキュメントの代わりとなるものではありません。使用されているコード・サンプルはすべて、例証のみを目的としています。複数のデータベース機能、オプション、関連製品の使用について説明していきます。さらなる情報をお求めの方のために、「付録：**ツール – 機能、オプション、製品、パック**」に、それらの製品についての重要な情報をリンクとともに記載しています。



Oracle Databaseの攻撃ポイント

データベースはどのように侵害されるか

データベースを保護する方法をより深く理解するために、まずデータベースが侵害される一般的な方法について考える必要があります。

- データベース侵害のもっとも一般的な攻撃ポイントは、有効なデータベース・アカウントから開始されます。DBAアカウントやアプリケーション・サービス・アカウントのほか、エンドユーザーのアカウントさえも、そのような攻撃ポイントになる可能性があります。データベースから盗まれたほとんどのデータは、盗まれた有効なアカウントや、ポリシーに違反する方法で使用されている有効なアカウントから外部に流出します。
- もう1つの一般的な攻撃手法は、データベースの完全な迂回です。攻撃者がデータベースの下層のストレージにアクセスできる場合、データベースのバックアップを盗むことができる場合、あるいはデータベースのエクスポートを取得できる場合、攻撃者はデータベースのアクセスと監視の制御を回避できます。
- Oracle Autonomous Databaseクラウド・サービスのいずれかを使用している場合を除いて、ユーザーはデータベース・セキュリティ・パッチのアプリケーションを管理することで、データベースの悪用を防止しています。攻撃者は、パッチが適用されていない脆弱性を見つけようと、データベースと下層のオペレーティング・システムで既知の欠陥を徹底的に探します。
- ネットワーク境界を突破した攻撃者は、ネットワーク内に潜み、“興味深い”データを盗聴します。このようなネットワーク攻撃は、捕まる可能性が低いため魅力的です。
- これらの攻撃はすべて、本番データベースに対して行われる可能性がありますが、テストや開発のために頻繁に作成される本番データベースのコピーも、恰好の標的となります。実際、データベースの非本番用コピーはより恰好の標的です。厳密に監視されている可能性が低く、本番環境で使用されるセキュリティ制御が欠如しているためです。同じデータであれば、データベースのどのコピーであるかは重要ではありません。

単にこのような攻撃のいずれかを防ぐソリューションを使用しても、攻撃者は別の弱点に向かうだけであることに留意してください。データを完全に保護するには、攻撃への道をすべて閉ざす必要があります。

リスクとは

リスクは、脅威、価値、脆弱性、および影響によって作り出されます。

- 脅威：誰かがデータを盗む、破壊する、または悪用することを試みる可能性がどの程度あるか
- 価値：データには、攻撃者と貴社の両者にとってどのような価値があるか
- 脆弱性：データはどの程度危険にさらされているか。データを侵害しようとする試みが成功する可能性がどの程度あるか
- 影響：侵害によって組織はどの程度の損害を被るか（罰金、機会損失のコスト、顧客の信頼損失などの観点から）

脅威や影響に影響を与えることはほぼ不可能ですが、取組みを行うことで脆弱性を低減できます。非本番用のデータベース・コピーでは、データの価値を低減できる場合があります。リスクに対して行うことができるのは、緩和する、保険をかける、受け入れるという3点のみです。ここでは、リスクを緩和し、受け入れることができるレベルにまで低減することに重点を置きます。

基本セキュリティの確立

それぞれのデータベースに実装すべき一定の制御があります。そのような制御によって、最低限の基本セキュリティが生成されます。この基本セキュリティは、組織のポリシーとリスク耐性を反映している必要があります。データベースの基本セキュリティについて考える際は、保管するデータの種類やデータベースの用途を問わず、これがすべてのデータベースに求めるセキュリティであると考えると良いでしょう。

基本セキュリティにはわずかな例外（ある場合）のみが適用されるべきであり、仮に例外がある場合は、その例外がまだ有効であることを確認するために定期的にレビューする必要があります。以下は、当社がデータベースのすべての基本セキュリティに含まれるべきであると考える手順と制御です。

データベースの評価

変更を加える前に、データベースを評価して現在のセキュリティ状態を把握すると良いでしょう。データベース構成、基本的なセキュリティ・ポリシー、ユーザーに与えられた権限、パスワード・ポリシーを確認します。データベースをスキャンして機密データを検索し、このデータベースにはどのような保護を追加するのが適切であるかを把握します。

データベース構成の検証

データベースのセキュリティ評価を実施し、初期化パラメータ、リスナー設定、適用されていないセキュリティ・パッチなどを確認します。Oracle Databaseは極めて柔軟性があり、数百ものパラメータによって、ほぼどのようなビジネス・ニーズも満たすことができるように構成できます。いくつかのパラメータにより、データベースのセキュリティ・リスク・レベルが変わります。リスク削減のベスト・プラクティスに従わない構成の設定に注意を払うことが重要です。セキュリティ評価を使用して、不要なリスクを生み出す構成の選択を特定し、可能な場合はシステムを再構成してそのリスクを排除します。基本セキュリティの状態が、最低限のセキュリティ標準に対応する構成を反映していなければなりません。セキュアなデータベース構成の組織的な標準がまだない場合は、Oracle Database向けのCenter for Internet Security（CIS）ベンチマークの構成、または米国国防情報システム局（DISA）のSecure Technical Implementation Guide（STIG）のいずれかを採用することを検討してください。オラクルは、Oracle Database Security Assessment Tool（Oracle DBSAT）、Oracle Data Safe、Oracle Enterprise Managerのライフサイクル管理など、データベースのセキュリティ評価に役立つ複数のツールを提供しています。これら3つのツールはすべて、結果をCISベンチマークおよびSTIGにマッピングします。

ユーザー認証の確認

Oracle Databaseでは、ユーザー名とパスワード、PKI証明書、Kerberos、およびRADIUSによる認証がサポートされます。もっとも一般的な認証方式は、依然として、シンプルなユーザー名とパスワードです。

データベース・アカウントがまだパスワードで認証されている場合、適切なパスワードのプラクティスを実装するようにします。ほとんどの場合、データベースのパスワード・ポリシーは、パスワードの長さ、寿命、複雑性の要件が設定された貴社の標準ポリシーを反映していなければなりません。Oracle Databaseは機密情報が保管されたビジネスクリティカルなシステムです。ラップトップなどの重要性が低いシステムで許可するよりも脆弱なパスワード・ポリシーを容認する理由があるでしょうか?

下流で可用性に影響が及ぶため、通常はパスワードを期限切れにするのが実用的でないデータベース・サービス・アカウントでは、アカウントに接続を許可する方法を厳密に制限する制御を追加することで、期限切れにならないパスワードのリスクを軽減することを検討してください。この種の緩和策については、本書の後半でアクセス制御を説明する際に詳しく述べます。一定の回数ログインに失敗したアカウントをロックするのも良いプラクティスであり、パスワードの総当り攻撃が成功する可能性を低減します。

インタラクティブなデータベース・アカウントには厳密認証を検討してください。もっとも一般的な厳密認証は、通常はMicrosoft Active Directoryドメイン・コントローラをKerberos鍵配布センターとして使用するKerberosです。認証をデータベース外部のActive Directoryに移行すると、認証トークンの一元的制御、Windowsデスクトップを使用したシングル・サインオン、単一の操作ですべてのデータベースのデータベース・ログインを無効化できる機能など、複数のメリットを享受できます。

あまり一般的でないものの、急速に普及している厳密認証方式はRADIUSです。RADIUSは、広く知られている古い認証方式であり、Oracle Databaseで10年以上サポートされています。Oracle Identity Cloud ServiceやOktaといったクラウドベースの認証サービスでも採用されていることから、その採用が近年後押しされています。

ユーザーに与えられた権限

不正アクセスされたアカウントはデータベース侵害のもっとも一般的なソースであるため、割り当てられた権限を確認し不要な権限をすべて削除することで、不正アクセスされた場合にそれらのアカウントが引き起こす脅威を低減します。Data SafeとOracle DBSATはどちらも、アカウントに付与されている権限のレポートを作成することで、ユーザーに与えられた権限のレビューを支援します。さらに、オラクルは*権限分析*を提供することで、アカウントが実際に*使用している*権限を評価できるよう支援しています。アプリケーション・アカウントに必要な権限を把握することは重要です。割り当てられたタスクを完了するために必要な権限のみを持つアカウントを推進する中で、取り消す候補となる権限を特定するのに役立つためです。

権限分析の良いプラクティスは、取り消す候補となる権限とロールを特定し、それらの権限とロールの使用を一定期間監査することで、たまに必要になる権限を誤って取り消さないようにすることです。非ユーザー・アカウント（アプリケーション・アカウント、バッチ・プロセスなど）では、権限の取消しに注意を払うことが特に重要です。

転送中データの暗号化

データは、データベースとデータベース・クライアントまたはアプリケーションとの間のネットワークを横断する際にリスクにさらされます。熟練の攻撃者は、ネットワーク・トラフィックを頻繁に監視し、機密データを盗聴します。このような受動的攻撃は、攻撃者がデータベースやデータベース・サーバーへの侵入を試みないため、検出が極めて困難です。

幸いにも、Oracle Databaseでは転送中のデータを暗号化する複数のオプションが提供されます。

Oracle Native Network Encryption

Oracle Native Network Encryption（Oracle NNE）は、転送中のデータを暗号化するもっとも簡単な方法です。データベースのネットワーク構成ファイル（sqlnet.ora）に1行追加する必要がありますが、ほとんどの場合はデータベース・クライアントの変更は不要です。Oracle Databaseは、暗号化をリクエストまたは要求することができます。データベースが暗号化をリクエストした場合、暗号化をサポートするクライアントは自動的に暗号化をデフォルトで使用し、暗号化をサポートしないクライアントは非暗号化接続に戻されます。データベースが暗号化を要求した場合、暗号化をサポートしないクライアントは接続できなくなります。暗号化接続では、相互にサポートされる最強の暗号化アルゴリズム（通常はAES-256）が使用されます。

Transport Layer Security

Transport Layer Security（TLS）も転送中のデータを暗号化します。Oracle NNEとは異なり、TLSではデータベース・サーバーの証明書が必要であり、データベース・クライアントの証明書も使用できます。サーバーのみが証明書を使用する場合、接続は“サーバー認証済み”と見なされ、クライアントは接続に引き続きユーザー認証が必要です。データベース・クライアントも証明書を発行した場合、接続は相互に認証され、クライアント証明書がユーザーの認証に使用されます。

Oracle NNEとTLS、どちらが適切か

どちらが適切かはユースケースによって異なります。使用される暗号化の質は、いずれも同等の強度ですが、TLSでは暗号化にサーバー認証が追加されるほか、TLSはクライアントの認証にも使用できます。TLSは、ほとんどのセキュリティ・チームが熟知する業界標準のプロトコルです。ただし、TLSではほぼ常にクライアント構成の変更が必要であり、最終的に期限が切れて保守が必要になる証明書が使用されます。Oracle NNEは設定が容易で、クライアントの変更が必要になることはほとんどありません。運用効率がもっとも重要な場合は、一般的にOracle NNEが使用されています。極めて高いセキュリティ・レベルが求められる場合は、（そのために運用効率の面である程度妥協することになったとしても）TLSがもっとも一般的な選択肢です。

データベース・ユーザーおよびロールの管理

データベース・ユーザーおよびロールは、データベース内でローカルに管理できます。LDAPディレクトリで一元管理することもできます。データベースに接続するユーザーが少なく、接続するデータベースも少ない場合は、恐らくローカルなユーザー管理が最適な選択肢です。多数のデータベース・ユーザーがいる場合、または多様なデータベースを数多く管理している場合は、ユーザーを一元管理する方が良いでしょう。データベース・ユーザーの一元管理には、次の2つのオプションがあります。

集中管理ユーザー

集中管理ユーザーは、Microsoft Active Directoryのユーザーまたはグループにマッピングされたデータベース・スキーマと、Active Directoryのグループにマッピングされたデータベース・ロールを使用して、Oracle DatabaseをActive Directoryに接続します。認証はパスワード、PKI証明書、またはKerberosを使用して行うことができ、その中ではKerberos認証がもっともよく使用される認証方式です。Active Directory環境での侵入性がもっとも低いためです。集中管理ユーザーは、Oracle Database 18c以降でサポートされます。集中管理ユーザーを使用すると、接続されたすべてのデータベースに共通する資格証明を使用して、単一の場所（Active Directory）で複数のデータベースのデータベース・アカウントを管理できます。

エンタープライズ・ユーザー・セキュリティ

エンタープライズ・ユーザー・セキュリティは、Oracle Internet Directoryのユーザーまたは組織単位にマッピングされたデータベース・スキーマと、Internet Directoryのグループにマッピングされたデータベース・ロールを使用して、Oracle DatabaseをInternet Directoryに接続します。認証はパスワード、PKI証明書、またはKerberosを使用して行うことができ、その中ではパスワード認証がもっともよく使用される認証方式です。多くの場合、Oracle DirectoryはMicrosoft Active Directoryのプロキシとして機能しますが、その場合は、Kerberosがもっともよく使用される認証方式です。エンタープライズ・ユーザー・セキュリティは、現行のすべてのデータベース・バージョンでサポートされます。エンタープライズ・ユーザー・セキュリティを使用すると、接続されたすべてのデータベースに共通する資格証明を使用して、単一の場所（Oracle Internet Directory）で複数のデータベースのデータベース・アカウントを管理できます。

ユーザー・アクティビティの監査

データベースの監査には、通常は次の3つの目的があります。

- セキュリティ・インシデント後のフォレンジック調査をサポートするために、データベース・アクティビティの記録を提供する
- 開発と運用をサポートするために、データベース・アクティビティの記録を提供する
- セキュリティ侵害を阻止および防止するために、アクセス異常を特定する

セキュリティ・インシデント後は、何が起き、誰がそれを行い、どこから攻撃され、いつどのように攻撃が発生し、どのようなデータが影響を受けたかを特定する必要があります。監査証跡はインシデント後の調査で極めて重要な役割を果たします。データベースへのログイン、ユーザーへの変更、データベース・オブジェクトの変更、機密データへのアクセスなどの記録を保持することで、このような調査をサポートし、インシデント範囲の証拠を提供できます。

データベースの開発と運用には、何が発生したか、すなわち誰がデータベースをシャットダウンし、いつ表が削除され、いつアプリケーション・サービス・アカウントが正常な認証を停止したかという記録が頻繁に必要となります。監査証跡は、トラブルシューティングや根本原因の分析において大いに役立つ可能性があります。幸いにも、通常は、フォレンジック調査をサポートするために必要な監査ルールと同じもので十分に開発と運用をサポートできます。

異常検出とインシデント防止は、もっとも求められる監査目的の1つです。異常検出とインシデント防止については、本書の後半で、基本セキュリティを超えたMaximum Security Architectureについて説明する際に詳しく説明します。

Oracle Databaseでは、従来型監査、統合型監査、ファイングレイン監査など、ユーザー・アクティビティを監査するための豊富な機能一式が提供されます。監査は、次のセキュリティ目標に役立ちます。

- インシデント後の調査における支援
- コンプライアンス・レポートのサポート
- システム使用における異常検出

監査は常に、パフォーマンスとストレージにある程度の影響を与えるため、監査ポリシーでは、収集される監査データの価値を考慮する必要があります。“すべてを監査する”ことは、システムに著しい負荷をさらに課すことになるため、通常は実用的ではありません。次のアクティビティは、通常は頻度が低いものの、セキュリティにおける価値が高いアクティビティです。監査ポリシーでは、基本的な監査の一環としてこのようなアクティビティを捕える必要があります。

- ユーザー・アカウントの変更（作成、変更、削除）
- データベースへのログイン（特にログインの失敗）
- 権限およびロールの付与
- データベース・オブジェクト（表、ビュー、データベース・リンク、ストアド・プロシージャなど）の作成、変更、削除
- データベース管理者のすべてのアクション
- データベースのエクスポートとバックアップ

基本セキュリティを超える監査ポリシーでは、ポリシーから外れたデータ・アクセスの試みを捕える必要があります。たとえば、アプリケーション外部からのデータ・アクセスがポリシーで許可されない場合、ポリシーを迂回する試みを監査で捕える必要があります。

お使いのデータベース・バージョンが統合型監査をサポートしている場合は、監査ポリシーを作成する際は統合型監査を第一の選択肢にする必要があります。統合型監査では、監査ポリシーが必要なデータのみを捕えることに集中できるようにする機能など、従来型監査と比較して著しい利点が提供されます。Oracle Databaseには、特別な設定なしに一般的な監査要件を満たすことができる数多くの統合型監査ポリシーが用意されています。統合型監査は、Oracle Database 12.1以降で利用できます。

機密データの検出

ほとんどのデータベースでは、基本セキュリティを超えるかどうかの決定は、データベース内に保管されたデータによって決まります。追加のセキュリティ対策が必要な規制要件がありますか?データには、追加のセキュリティ制御への投資を正当化するようなビジネス・リスクがありますか?一部のデータベースではその答えは明白です。HCMデータベースやCRMデータベースの場合は、機密性の高い個人データが保管されていることが分かっているため、しかるべき対応を取ることができます。製造工場のフロアのランタイム・センサー・データをホストするデータベースの場合は、恐らく追加の保護は必要ありません（データから機密の知的財産が漏洩されない限り）。

それ以外のデータベースでは、適切な保護レベルが分からない可能性があります。機密データの検出が役立つのはそのような場合です。機密データの検出では、データベースをスキャンして機密データの“タイプ”を検索します。この“タイプ”は、データベースの話題でよく用いられるCHAR、NUMBER、BLOBといったデータタイプとは異なります。

これは、電子メール・アドレス、納税者ID、アカウント番号などの“タイプ”です。機密データの検出では、どのタイプのデータが、どの程度データベースにあるかを知らせてくれます。この情報を使用して、データベースに含まれるリスクやそのようなリスクを緩和するために必要な保護について、データに基づき決断を下すことができます。

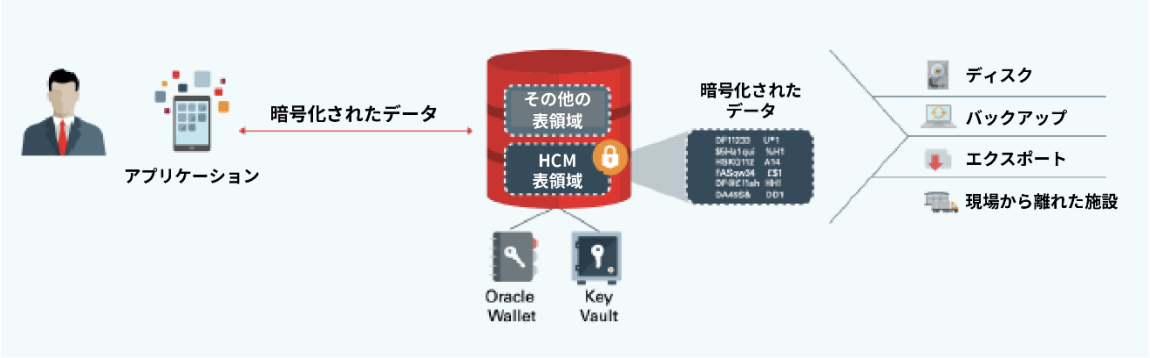
オラクルでは、機密データの検出を支援する3つのツールを提供しています。Database Security Assessment Tool、Data Safe、およびOracle Data Masking and Subsetting Packの一部であるEnterprise Managerアプリケーション・データ・モデル（ADM）です。Data Safeを使用できる場合は、Data Safeが第一の選択肢です。Data Safeでは、データベース・メタデータ（列名と列コメント）と表内の実際のデータをスキャンして125種類以上の機密データを検索する機密データ検出が提供されます。Data Safeの機密データ形式ライブラリは拡張可能なため、組織または地域の独自のデータ・パターンまたはそれに類似するものを作成して容易にモデル化することができます。

すでにOracle Enterprise Managerを使用しており、ADMの必要なライセンスを所有している場合は、ADMも機密データの検出における良い選択肢です。

英語以外のデータベースを使用している場合は、Oracle DBSATを検討してください。Oracle DBSATは、さまざまな言語のスキャニングをサポートするオラクル唯一の機密データ検出ツールです。本書の執筆時点では、Oracle DBSATには英語、スペイン語、ドイツ語、ポルトガル語、イタリア語、フランス語、オランダ語、ギリシャ語の検出パターン・ファイルが同梱されています。Data SafeやADMとは異なり、Oracle DBSATは実際には表データをスキャンせず、列名や列コメントを含むメタデータのみをスキャンします。

基本を超えて – Maximum Security Architecture

Oracle Maximum Security Architecture（Oracle MSA）は、データベース・セキュリティに多層防御手段を適用することで、基本セキュリティを拡張し、機密データを保管するシステムや規制上の制約の対象となるシステムのリスクをさらに低減します。さまざまな攻撃手段を緩和するために、Oracle MSAのさまざまなコンポーネントが使用されます。Oracle MSAのすべての機能が使用されるデータベースは非常に少なく、機密データを保管するほとんどのデータベースでは、Oracle MSAの1つまたは複数のコンポーネントを使用することでリスクが低減され、セキュリティが向上し、規制遵守が強化されます。



透過的データ暗号化による保管データの暗号化

保管データの暗号化

保管データの暗号化により、データベースが迂回されるリスクが軽減されます。攻撃者が下層のデータベース記憶域、データベース・バックアップ、またはデータベース・エクスポートにアクセスしても、暗号化によって、攻撃者がデータベースAPIを使用せずにデータを直接読み取ることが防止されます。この種の迂回攻撃は、アクセス制御を迂回し、監査レコードをトリガーしません。これは最悪の事例であり、回避することが不可欠です。暗号化は、データ・プライバシ規制とデータ保護規制における一般的な要件です。データが暗号化されていない場合、通常は、データを保護するための必要な作業が実施されていないと見なされます。オラクルの第一の暗号化ソリューションは、Oracle Advanced Security（Oracle ASO）の機能である透過的データ暗号化です。

透過的データ暗号化（TDE）は、基本セキュリティを超えるもっとも一般的な制御であり、他の基本セキュリティ以外の機能よりも多くのオラクルのお客様によって実装されています。多くの組織では、TDEは基本セキュリティの一部です。Oracle Cloudがその良い例です。オラクルは、暗号化されていないお客様のデータをホストするリスクを負うことを望んでいないため、Oracle CloudではTDEはデフォルトで使用されます。ほとんどのTDEの実装ではトラブルは発生しません。TDEは10年以上にわたって、非常に多くのお客様のもとで正常に稼働している成熟した機能です。ただし、考慮すべき点がいくつかあります。

人工的な問合せではなく、実際のデータ・ワークロードで独自のパフォーマンス・ベンチマークを実施してください。本番システムへの影響を正確に判断するには、実際のワークロードを使用することが重要です。暗号化は、常に何らかのパフォーマンス・オーバーヘッドを生じさせます。より多くの処理をシステム（特にCPU）に求めているためです。TDEをOracle Advanced Compressionと組み合わせると、そのオーバーヘッドを低減する素晴らしい方法になります。Advanced Compressionによって、復号化が必要なデータ・ブロック数が削減されるためです。

表領域の暗号化は、ほとんどのワークロードで、列レベルの暗号化よりもパフォーマンスが優れている傾向にあります。表領域の暗号化を使用すると、機密データの列を暗号化するのを忘れたり、機密データを含むべきでない列に機密データが挿入されたりする可能性が低くなります。お使いのデータベース・バージョンでサポートされる最強の暗号化を使用してください。本書の執筆時点では、最強の暗号化はAdvanced Encryption Standard（AES）256ビット鍵です。低いレベルの暗号化と短い鍵長を使用すると、パフォーマンスへの影響は若干少なくなりますが、ほとんどの場合はその違いは大きくありません。

暗号化がバックアップ・システムに及ぼす影響を考慮することを忘れないでください。大半の最新バックアップ・ストレージでは、バックアップが圧縮され、重複排除されます。データベースが最初に暗号化されると、暗号化されたデータ・ブロックはすべて、ストレージ・システムから新規と見なされるため、重複排除は行われず、当初はストレージ要件が急増します。時間が経ち、暗号化されていないバックアップが古くなりシステムから削除されると、重複排除が正常なレベルに戻ります。暗号化されたデータは適切に圧縮されない傾向にあります。そのため暗号化されたデータを圧縮すると、圧縮の一部が永久に失われます。前述のAdvanced Compressionでは、データは暗号化される前に圧縮されるため、そのような影響を緩和できます。暗号化がバックアップ・ストレージに及ぼすこの影響は、透過的データ暗号化のデプロイメント計画でもっともよく見過ごされる領域の1つです。

暗号化鍵の管理と保護

保管データの暗号化には永続鍵が必要であり、暗号化のセキュリティは、暗号化鍵のセキュリティと同等です。透過的データ暗号化には、自動鍵管理機能が搭載されています。またOracle Key Vaultでは、Oracle Real Application ClustersやOracle Data Guardといった高度なデータ・アーキテクチャをサポートするために、セキュアな鍵ストレージ、一元的な管理、セキュアな鍵配布が提供されます。

お使いの鍵が（データベースのバックアップとは別に）バックアップされていることを確認してください。鍵のストレージには、デフォルトのOracle Walletではなく、Oracle Key Vaultを使用してください。また、セキュリティを向上するために、信頼の起点として、Key Vaultをハードウェア・セキュリティ・モジュール（HSM）とつなぐことを検討してください。

職務分離の徹底

機密データを保管するデータベースでは、管理職務の分離は一般的なセキュリティ目標です。アカウントを作成し、認証資格証明を管理できる管理者は、データへのアクセス権を付与できません。データ管理者には、ユーザーを作成する権限やユーザーの資格証明を変更する権限はありません。Database Vaultが有効化されている場合、ユーザー・アカウント管理に職務分離（SOD）がデフォルトで実装されます。

どのレベルのSODが組織に適切であるかは、システムやシステム内のデータの機密性だけでなく、多くの要因に基づきます。組織のDBAが1人だけの場合は、複雑なSOD設定は恐らくあまり重要ではありません。一方、組織に数十人または数百人のDBAがいる場合は、管理者アカウントが不正アクセスされた際の被害を限定するために、職務をさらに分離すると良いでしょう。その他にも（思いつくあらゆる組み合わせとして）、バックアップとリカバリの管理、パフォーマンス管理、データ統合、セキュリティ管理、データ管理、パッチ適用などで職務が分離されています。貴社の状況に適切なモデルを採用してください。ただし、可能な限り、職務に必要な最小権限のみが付与されたアカウントの使用を推進してください。DBAが専門化されている場合は、DBAは汎用のDBAロールに含まれる権限を持つべきではありません。各自の職務に合った権限を持つ必要があります。

機密データへの管理者アクセスの制御

データベース管理者アカウントはハッカーの恰好の標的の1つであり、大半のデータベース侵害では、不正アクセスされた資格証明が使用されます。そのため、不正アクセスされたデータベース管理者アカウントは組織に危険を及ぼす可能性があります。幸いにも、データベース管理者は機密データや、そもそもアプリケーション・データにアクセスする必要はほとんどありません。Database Vaultを使用してデータベース管理者の機密データへのアクセスをブロックすると、不正アクセスされた管理者アカウントが与える得る被害の量を大幅に低減できます。

機密データへの信頼パス・アクセスの徹底

データ窃盗では、アプリケーションが機密データにアクセスするために使用するサービス・アカウントへの不正アクセスは、DBAアカウントへの不正アクセスと同じくらい有効な方法です。アプリケーション・サービス・アカウントは、通常、データへの完全なアクセス権を持ちます。そして多くの場合、アプリケーション・サービス・アカウントの資格証明は、運用に悪影響を及ぼさずに更新することが困難です。そのため、資格証明が広く拡散され（特に開発者チームやDevOpsチーム内で）、アカウントが悪用される可能性や、アカウントに不正アクセスされるリスクが増加する可能性が高まります。Database Vaultを使用してこれらのアプリケーション・サービス・アカウントをロックダウンすることで、アプリケーション・サーバーのオペレーティング・システム・ユーザーとして起動され、アプリケーション・サーバー・プログラムを実行しているアプリケーション・サーバーのみに、アカウントの使用を制限できます。複数の要素を用いて、アプリケーション・サービス・アカウントの使用をこの信頼パスに制限し、攻撃者や詮索好きなチーム・メンバーがアカウントを悪用する機会を排除してください。

監査データの一元管理

基本セキュリティのセクションでは、監査データを使用してフォレンジックと運用の両調査をサポートできることを説明しました。個々のデータベースの監査データは、単純なSQL問合せを使用して手作業で分析できますが、複数のデータベースがある場合は、それらのデータベースから監査データを収集して中央のリポジトリに集める方がより実用的です。そうすることで、そのリポジトリで容易にデータを分析し、レポートを作成できます。加えて、統合型監査にまだ切り替えていない場合は特に、特権ユーザーの資格証明を持つ攻撃者が、ローカルに保管された監査データを変更または削除できる可能性があります。

Oracle Audit Vault and Database Firewallは、Oracle Database（およびOracle MySQL、Microsoft SQL Server、IBM DB2、PostgreSQL、MongoDB、SAP Sybaseをはじめとする他の多くのデータベース）から監査データを収集し、その監査データをマネージド・データウェアハウスに配置します。マネージド・データウェアハウスでは、データのレビュー、分析、レポート作成、および（必要に応じて）アラート生成を行うことができます。

異常検出のためのデータベース・アクティビティの監視

異常検出とインシデント防止は、もっとも求められる監査目的の1つです。調査をサポートするために使用する監査証跡と同じものが、進行中の攻撃を検出するために、あるいはデータベースへのアクセスが成功する前の早期の段階で攻撃を検出するために使用されている可能性があります。監査機能は、複数のログイン試行の失敗や新規ユーザー・アカウントの不正な作成など、異常なアクティビティが発生した場合にユーザーに通知する必要があります。

データベースの監査に代わるものはありませんが、監査は通常、もっとも基本的な異常検出以外にはあまり適していません。すべてのアクティビティを監査できることは非常にまれだからです（すべてのアクティビティを監査した場合のパフォーマンスへの影響は大きく、すべての監査レコードを保持するために必要なストレージも膨大です）。高度な異常検出とは、すべてのアクティビティを調査する必要があることを意味しています。オラクルは、ネットワークベースのアクティビティ監視によって監査データを補足することで、監査の制限に対処しています。監視と監査は複数の点において異なります。監視ではセッション・コンテキストは使用されず、下層のデータベース・メタデータにアクセスすることもありません。ネットワークベースの監視では、監査と同じ品質のデータは提供されませんが、ネットワーク監視は、通常のパターンからの逸脱を発見できる十分なデータを提供することに長けています。新しいクライアント・プログラムを使用してデータベースにアクセスしているユーザーがいる、初めて見るOSユーザーとして接続しているユーザーがいる、アプリケーションの通常パターンとは異なるSQL文を突然発行し始めたアプリケーションがあるなどの状況はすべて、ネットワークベースの監視が発見を得意とする異常です。

Oracle Audit Vault and Database Firewallではネットワーク監視が実行されるため、ユーザーは正常なデータベース・アクティビティのプロファイルを迅速に作成して、その基準から逸脱した異常を検出し始めることができます。本来のデータベース監査とネットワークベースの監視を組み合わせることで、データベース・アクティビティの全体像を掴むことができます。

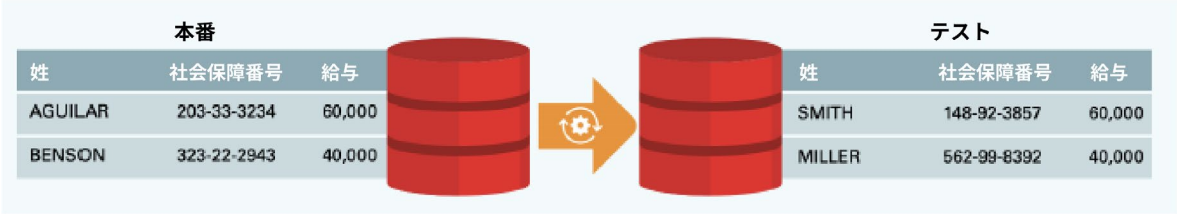
異常の防止

単に異常を監視するのではなく、異常が発生するのを防止する方が理にかなっているシステムもあります。そのようなシステムでは、疑わしいアクティビティや、正規のアクティビティをブロックしている可能性があるアクティビティを防ぐために意識的な選択を行います。この種の制御は、機密性が極めて高いシステムや、保管されるデータ以外の要因のためにリスク・レベルが極めて高いシステムに通常は適用されます。

Oracle Audit Vault and Database Firewallを使用すると、ファイアウォールがデータベース・トラフィックに従って配置されている場合に異常をブロックできます。アクティビティは、データベースに到達する前にファイアウォールを実際に*通過*しなければならなくなります。

機密データの最小化 – 非本番データベースのリスク排除

これまでは、データ・アクセスの制限と監視という制御について説明してきましたが、そのような制限がシステムの目的にそぐわない場合があります。その良い例は、非本番用のテスト・システムや開発システムです。元々そのようなシステムは、アクセス制御があまり厳格でなく、運用方法にばらつきがある傾向にあります。非本番データベースが人工的なデータで作成されている場合は問題ありません。人工的なデータにはリスクがないためです。しかしながら、本番システムをただクローニングする一般的なプラクティスを使用して非本番システムが作成されている場合は、本番システムと同じリスクが伴うため、セキュリティ・インシデントが発生する可能性が高まります。



データ・マスキングを使用して非本番データベース・コピーの機密データを最小限に抑える

このような本番システムの非本番用コピーでは、機密データをマスキングする手法をとるのが適切です。機密データを人工的な値と置き換えてデータの機密性を取り除きつつ、テストや開発に適した環境を提供する手法です。マスキングは本書で説明した他の制御とは異なり、リスクを緩和しません。リスクを実際に排除します。オラクルは、データのマスキングのためにOracle Data SafeとOracle Enterprise Manager Data Masking and Subsettingという2つのソリューションを提供しています。どちらのソリューションを使用しても、機密データを検出し、参照整合性制約を特定し、データをマスキングしてセキュリティ・リスクを排除できます。お使いのアーキテクチャに適したソリューションを選択してください。

リスクベースのアプローチの採用

最初に、すべてのデータベースに適用される基本セキュリティの概念について説明し、次に、機密データの検出と、システムのリスク・レベルを基に基本セキュリティを超える制御を使用することについて説明しました。以下は、いくつかのサンプル・システムと、関連付けられたリスク・レベルと制御です。

システム	リスク・レベル	基本セキュリティを超える制御	注釈
人事管理	高	暗号化、鍵管理、職務分離、信頼パス	プライバシの懸念/規制
財務レポート	高	暗号化、鍵管理、職務分離	米国サーベンス・オクスリー法または類似の法律
顧客管理	非常に高い	暗号化、鍵管理、職務分離、信頼パス、異常検出	プライバシの懸念/規制
注文のフルフィルメント/出荷	非常に高い	暗号化、鍵管理、職務分離、信頼パス、異常検出	プライバシの懸念/規制
Webストア	非常に高い	暗号化、鍵管理、職務分離、信頼パス、異常防止	インターネットからアクセスできるアプリケーション、プライバシの懸念/規制
バグ・データベース/ソース・コード	もっとも高い	暗号化、鍵管理、職務分離、信頼パス、異常防止	知的財産
テストおよび開発	高	データ・マスキング	これらのシステムから機密データを削除

まずはここから

本書では多くの内容を扱いましたが、手短に紹介した各領域については、専用のホワイト・ペーパーで扱われている場合があります。行うべき作業は気が遠くなるほどの量になる可能性があります。当社は複数の企業が、完璧な実装計画を立てようとして膨大な時間を費やしながらも、リスク削減について何も達成できない「分析まひ」に陥るのを見てきました。特に忘れられないのは、一緒に働きたいと願うような素晴らしいお客様が、その分析フェーズに費やした約6か月の間に侵害に遭い、情報が大規模に公開されたことです。その結果、侵害コストが1億7,500万ドル以上に上り、同社は著しい混乱に陥りました。そのような落とし穴を避ける助けとなることを願って、以下を提案します。

何らかの対策を取る

実用のシステムには完璧なセキュリティは存在しません。必要なのは、データ保護の推進と、運用サポートとデータ使用のニーズとの間のバランスを取ることです。通常実施できる最善策は、貴社が耐えることができるレベルにリスクが低減されるまで、リスクを少しずつ崩すことです。上述のセキュリティ制御のいずれも、リスクの低減に役立ち、“受け入れることができるリスク”のレベルに貴社を近づけてくれるはずです。

まずは、本書で最初に説明したように、システムと構成の評価によってセキュリティを向上する対策を始めることが賢明でしょう。現在の状態を認識し、どのような状態になりたいかを決定します。どの制御を採用するのがもっとも理にかなっているかを判断します。本書の最初の部分でセキュリティの基本レベルの概要を説明しましたが、この基本セキュリティは貴社の理にかなっていますか?理にかなっている場合はそのセキュリティを採用し、メンテナンス期間中にシステムに適用し始めます。機密性が高いことを認識しているシステムがある場合は、まずそのようなシステムに重点的に取り組みます。今日排除するリスクは、明日攻撃者に悪用されるリスクかもしれないことを忘れないでください。

最後に

リスクの低減とセキュリティの向上を開始する中で、組織の硬直化に直面することはほぼ確実ですが、やる気をなくしてはいけません。現状を受け入れ続けるリスクは高すぎます。技術的な実装に集中できるよう、貴社のセキュリティ・グループの支援を取り付けてください。セキュリティ・グループには、計画を支援し、この取組みをまとめるリソースがあるかもしれません。

初心を忘れないでください。データベースには極めて価値の高い情報の一部が保管されているため、喜んでその情報を盗み、その情報から利益を得ようとする人は必ずいます。本書で概説した各制御は、システムのセキュリティを向上する一助となり、攻撃が成功する可能性を低減します。プロジェクトの成功を祈っています。

付録：ツール – 機能、オプション、製品、パック

このような内容を説明するには、製品と機能の一覧が欠かせませんが、製品と機能については、本書の主要部分では最小限に抑えるよう努めました。以下は、本書で触れたさまざまな機能、オプション、製品、およびパックを、ドキュメントへのリンクとともに一覧表示しています。各機能は本書で触れた順序で紹介しています。ドキュメントへのリンクについて、一点考慮しておいてください。これらは本書の執筆時点の最新情報ですが、ホワイト・ペーパーはどちらかというと長期的に有効である一方、データベースのバージョンとドキュメントは流動的で頻繁に更新されます。docs.oracle.comを確認し、ドキュメントの最新バージョンを見つけてください。ここで提供されるリンクによって、少なくとも検索すべきマニュアル（および通常は章や付録）が分かります。

Oracle Database Security Assessment Tool（Oracle DBSAT）

Oracle DBSATは、データベース・サポートに含まれるスタンドアロン・ユーティリティであり、セキュリティ評価、ユーザー評価、機密データの検出に役立ちます。Oracle DBSATの使用に追加費用は発生しません。Oracle DBSATは、サポートされるすべてのオペレーティング・システム上の、サポートされるOracle Databaseのすべてのバージョンで使用でき、オンプレミスまたはクラウド（Oracle Cloud以外のクラウドも含む）のデータベースで実行できます。本ユーティリティは、My Oracle Supportからダウンロードできます。ツールのダウンロードについて詳しくは、MOS Note 2138254.1を参照してください。Oracle DBSATのドキュメントは、こちらで参照できます。

Oracle Data Safe

Data Safeは、Oracle Database as a Service製品に含まれるOracle Cloudサービスであり、オンプレミスのデータベースとOracle Cloud Computeで実行中のOracle Databaseとともに使用できます。Data Safeには、セキュリティ評価、ユーザー評価、機密データの検出、機密データのマスキング、統合型監査ポリシーの制御、監査データの検索、レポート作成、アラート生成など、複数のデータベース・セキュリティ機能が含まれています。Data Safeはオラクルの最新のデータベース・セキュリティ・サービスであり、新機能によって急速に進化しています（2週間の開発スプリント）。最近の変更の最新情報については、“What’s New in Oracle Data Safe”を参照してください。Data Safeのドキュメントは、こちらで参照できます。

Oracle Enterprise Managerデータベース・ライフサイクル管理

データベース・ライフサイクル管理は、Oracle Enterprise Manager Cloud Controlの管理パックです。データベース・ライフサイクル管理は、構成管理など、データベースのライフサイクルを管理するためのさまざまな機能を提供しており、セキュリティ評価において重要な役割を果たすことができます。Enterprise Managerデータベース・ライフサイクル管理を使用した構成管理について詳しくは、こちらを参照してください。

権限分析

権限分析は、Standard Editionを除くすべてのデータベースとデータベース・サービスに含まれるデータベース機能です。ユーザー評価、とりわけユーザー・アカウントに付与されているものの使用されていない権限の特定に役立ちます。権限分析は、Oracle Database 12c Release 1で導入されました。権限分析のドキュメントは、こちらで参照できます。

Oracle Native Network Encryption

Native Network Encryption（Oracle NNE）は、Oracle Autonomous Databaseを除くすべてのデータベースとデータベース・サービスに含まれるデータベース機能です（Autonomous DatabaseではOracle NNEではなくTLSが使用されます）。Oracle NNEは、データベースとデータベース・クライアントまたはアプリケーションとの間を移動するデータを暗号化します。Oracle NNEのドキュメントは、こちらで参照できます。

Transport Layer Security

Transport Layer Security（TLS）は、すべてのデータベースとデータベース・サービスに含まれるデータベース機能です。Autonomous Databaseではデフォルトで構成されます。TLSは、データベースとデータベース・クライアントまたはアプリケーションとの間を移動するデータを暗号化します。TLSのドキュメントは、こちらで参照できます。

集中管理ユーザー

集中管理ユーザー（CMU）は、Oracle Database Enterprise Editionに含まれるデータベース機能です。CMUは、Oracle Database 18cで導入されました。CMUを使用すると、Oracle DatabaseをMicrosoft Active Directoryに直接接続できます。CMUでは、ユーザーはActive Directoryで作成され、データベース・スキーマにマッピングされます。必要に応じて、データベース・ロールをActive Directoryグループと関連付け、データベース・ロールのメンバーシップをActive Directoryグループのメンバーシップによって制御できます。CMUのドキュメントは、こちらで参照できます。

エンタープライズ・ユーザー・セキュリティ

エンタープライズ・ユーザー・セキュリティ（Oracle EUS）は、Oracle Database Enterprise Editionに含まれるデータベース機能です。Oracle EUSは、Oracle Database 8.1（Oracle 8i）で導入されました。Oracle EUSを使用すると、Oracle DatabaseをOracle Internet Directoryに接続できます。Oracle EUSでは、ユーザーはInternet Directoryで作成され、データベース・スキーマは、LDAPの組織単位のユーザーまたはユーザーのコレクションにマッピングされます。データベース・ロールをInternet Directoryグループと関連付け、データベース・ロールのメンバーシップをLDAPグループのメンバーシップによって制御できます。Oracle EUSのドキュメントは、こちらで参照できます。Internet Directoryのドキュメントは、こちらで参照できます。

従来型監査

従来型監査は最初にOracle Database 7に導入され、Oracle Database 12cがリリースされるまでは、Oracle Databaseの主要な監査方式でした。従来型監査は、統合型監査に置き換わりつつあります。従来型監査は、Oracle Database 20c以降は非推奨となり、Oracle Database 22cで廃止されます。従来型監査のドキュメントは、こちらで参照できます。

ファイングレイン監査

ファイングレイン監査は、Oracle Database 9.0（9i Release 1）で導入されました。ファイングレイン（きめ細かい）という名前からも分かるように、従来型監査よりも焦点を絞った、列に基づく監査ポリシーが可能です。ファイングレイン監査では、特定の条件が真と判断された場合のみ監査レコードが生成される条件付き監査の概念も導入されました。ファイングレイン監査のドキュメントは、こちらで参照できます。

統合型監査

統合型監査は、Oracle Database 12.1（12c Release 1）で導入されました。統合型監査は、監査レコードを単一のロケーションに集約することで、Database Vault、Oracle Label Security、Oracle Data Pump、Oracle SQL*Loader、Oracle Recovery Manager（Oracle RMAN）、ファイングレイン監査の監査データを、統合型監査ポリシーから生成された監査レコードと結合します。従来型監査とは異なり、統合型監査ポリシーは条件付きの場合があり、トップレベル文のみを監査することを選択する場合があります。また、デフォルトの監査証跡にないコンテキスト情報を含むように拡張できます。統合型監査のドキュメントは、こちらで参照できます。

Oracle Enterprise Managerアプリケーション・データ・モデル

Enterprise Managerアプリケーション・データ・モデル（ADM）は、Enterprise Manager Cloud Controlで利用できます。ADMは、データベースをスキャンして機密情報を検索します。また、Data Masking and Subsetting（Oracle DMS）、Oracle Audit Vault and Database Firewall（Oracle AVDF）の機密データ監査レポート作成、および透過的機密データ保護（TSDP）ポリシーの推進に役立ちます。Enterprise Managerアプリケーション・データ・モデルには、アプリケーション、表、およびデータ・ディクショナリで宣言された表の列、アプリケーション・メタデータからインポートされた表の列、あるいはユーザーが指定した表の列間のリレーションシップの一覧が保管されます。ADMでは、機密データタイプとそれに関連する列が保守されます。ADMは、テスト・データを安全に作成するためのデータのサブセット化やデータのマスキングといったテスト・データ操作によって使用されます。Oracle DBSATとは異なり、ADMは表内に含まれるデータをスキャンして機密データを見つけます。

ADMは、Oracle Advanced Security、Oracle Database Vault、Oracle Label Security、Oracle Data Masking and Subsetting、およびOracle Audit Vault and Database Firewallに無償で含まれています。列同士のリレーションシップや、どの列に機密データが含まれるかなど、データベースの1つまたは複数のスキーマを把握するためにADMを使用してください。ADMのドキュメントは、こちらで参照できます。

Oracle Advanced Security

Oracle Advanced Security（ASO）は、透過的データ暗号化、Oracle RMANバックアップ暗号化、Data Pumpエクスポート暗号化、暗号化されたOracle Database File System（Oracle DBFS）、暗号化されたSecureFile LOB、およびOracle Data Redactionを含むデータベース・オプションです。
Advanced Securityは、もっとも古いデータベース・オプションの1つであり、その起源はOracle 7で導入されたOracle Advanced Networking Optionにまで遡ります。Advanced Securityのドキュメントは、こちらで参照できます。

Oracle Key Vault

Oracle Key Vaultは、オラクルのインフラストラクチャをサポートする鍵管理システムであり、透過的データ暗号化とともに使用されるように最適化されています。Key Vaultでは、暗号化鍵への継続的なアクセスと、フォルトトレラントなマルチマスター・クラスタ・アーキテクチャが提供されます。Key Vaultのドキュメントは、こちらで参照できます。

Oracle Database Vault

Oracle Database Vaultは、高度なアクセス制御機能を提供するデータベース・オプションです。Database Vaultが一般的に使用されるのは、職務の分離を徹底するため、機密データへの管理者のアクセスをブロックするため、およびデータへの信頼パスのアクセスを徹底するためです。Database Vaultのドキュメントは、こちらで参照できます。

Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall（Oracle AVDF）は、異種の機能を使用したデータベース・アクティビティ監視機能であり、Oracle Database、Oracle MySQL、Microsoft SQL Server、PostgreSQL、MongoDB、IBM DB2、およびSAP Sybaseに対応しています。Audit Vault and Database Firewallのドキュメントは、こちらで参照できます。

Oracle Data Masking and Subsetting

Oracle Data Masking and Subsetting（Oracle DMS）は、Oracle Enterprise Managerの管理パックです。機密データを人工的なデータに置き換えることで、データベースからリスクを排除します。Oracle DMSは、データベースのサブセット（元のデータの一部のみを含む小規模なコピー）を作成するために使用することもできます。Data Masking and Subsettingのドキュメントは、こちらで参照できます。

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

2020年5月

Database Security Product Management、Russ Lowenthal