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

2025年3月、バージョン23.1

ORACLE

本書の目的

本書は、セキュリティ・リスクを低減し、Oracle Databaseの規制遵守を向上する選択肢を、読者が評価するための支援をすることを目的としています。本書の対象読者は、Oracle Databaseのセキュリティ制御を設計、実装、保守、運用する担当者です。

本書は、多種多様な製品マニュアルによる8,000ページを超えるセキュリティ関連ドキュメントに置き換わるものではありません。そうではなく、セキュリティに重点を置いたデータベース機能、オプション、関連製品を使用すべき理由を説明しています。同じ目的を達成するために使用できる制御が複数ある場合に、読者が適切な制御を選択できるよう支援することに努めています。「付録：ツール — 機能、オプション、製品、パック」には、それらの制御のポイントと、詳細情報を知りたい方向けのドキュメントのリンクが記載されています。

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。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。本文書に記載されている機能の開発、リリース、時期および価格については、弊社の裁量により決定されます。製品アーキテクチャの性質上、本書に記述されているすべての機能を安全に組み込むことができず、コードの不安定化という深刻なリスクを伴う場合があります。

ORACLE

目次

Database Security Assessment Tool（DBSAT）	a
Oracle Data Safe	a
Enterprise Manager Database Lifecycle Management	a
権限分析	a
Oracle Native Network Encryption	a
Transport Layer Security	b
集中管理ユーザー	b
エンタープライズ・ユーザー・セキュリティ	b
従来型監査	b
ファイングレイン監査	b
統合型監査	b
Enterprise Managerデータ検出	b
Oracle Advanced Security	c
Oracle Key Vault	c
SQLファイアウォール	c
Oracle Database Vault	c
Oracle Audit Vault and Database Firewall	c
Oracle Data Masking and Subsetting	c

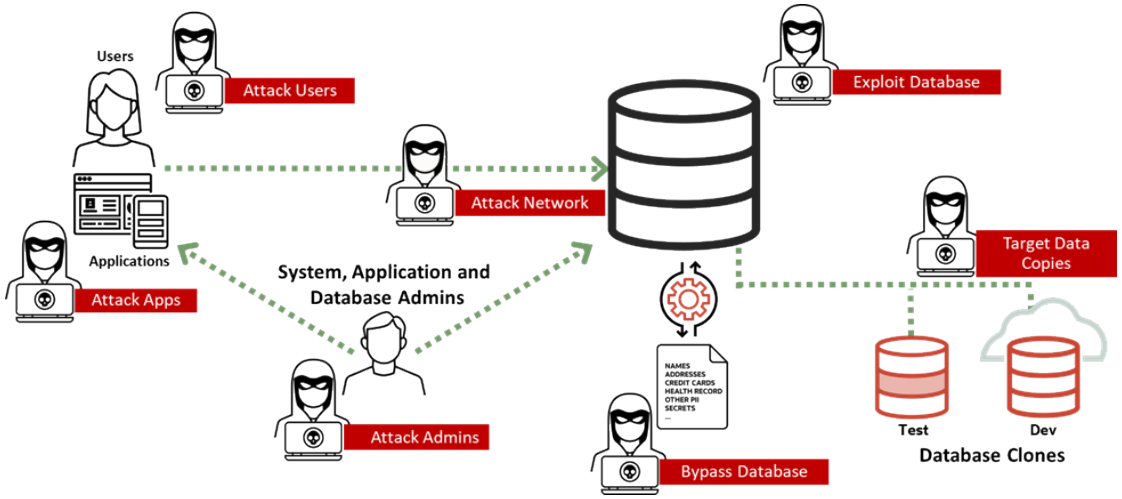
はじめに

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、データ窃盗やランサムウェア攻撃の第一の標的とな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があるのは、以下の2点の必須対応項目があるからです。

- 規制要件 – データ・プライバシーに関する国内法は160を超え（EU一般データ保護規則（GDPR）、インドのデジタル個人データ保護法、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ー原則など）、さらに州政府や地方政府の法規制（カリフォルニア州消費者プライバシー法、ケベック州プライバシー法など）、業界規制（PCI、米国FFIEC、米国HIPAA、EU PSD2、BASELなど）も数多く存在します。各種法規制をすべて記載すると本書の情報は膨大になり、また規制環境は常に変化しているため、そのような一覧はすぐに古くなるでしょう。規制を遵守しない場合、極めて大きい代償を払うことになる可能性があります。これまでの罰金総額は、米国HIPAAで1,600万ドルを超え、EU GDPRでは12億ユーロに達します。
- リスク低減とデータ窃盗の懸念 – 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。毎年、数十億もの個人データ・レコードが盗まれています。この窃盗の経済的な影響は、容易に数兆ドルに上ります。「サイバー犯罪が1つの州であるとすると、世界第3位の経済規模になる」と、*2023*年*1*月に開催された世界経済フォーラム第*53*回年次総会において、アルバニアの*Edi Rama*首相は述べました。

本書では、データベース・セキュリティ計画のためのフレームワークを提示します。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と、組織の機密データに対して適切なレベルの保護を提供できるかを説明します。

また、本書では、データの窃盗（または悪用）の防止を目標とした上で、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く一方、本書で説明するセキュリティ制御は、規制遵守の面でも重要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。



データベースの攻撃ポイント

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について理解するには、まずデータベースが侵害される典型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・アカウントです。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、不正アクセスさ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。
- データベースを完全に迂回するという攻撃手法もあります。攻撃者がデータベースの下層のストレージにアクセスする、データベースのバックアップを盗む、あるいはデータベースのエクスポートを取得するといった手法です。これらの場合、攻撃者はデータベースのアクセス制御と監視の制御を回避できます。迂回攻撃は、ほとんどのランサムウェアの動作原理になっています。単純にストレージからデータベース・ファイルを収集し、そのデータをランサムウェア犯罪組織のサーバーに秘密裏に取り込みます。
- 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。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、管理者はデータベースへのセキュリティ・パッチの適用状況を管理することで、データベースの悪用を防止します。
- ネットワーク境界を突破した攻撃者は、単にネットワーク内に潜み、“興味深い”データを盗聴する場合もあります。このようなネットワーク攻撃は、捕捉され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好都合な標的です。厳密に監視されている可能性が低く、多くの場合は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、攻撃の道筋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、影響、脆弱性、価値を掛け合わせたものです。

- 脅威：誰かがデータの窃盗、破壊、または悪用を試み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）
- 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
- 価値：データにはどのような価値があるか（攻撃者と組織の両者にとって）

脅威や影響を変えることはほぼ不可能ですが、対策を行うことで脆弱性を低減できます。また、非本番用のデータベース・コピーでは、攻撃者にとってのデータの価値を低減できます。

リスクに対してできることは、緩和する、保険をかける、受け入れるという3点のみです。本書では、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。

セキュリティ・ベースラインの確立

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、組織のポリシーとリスク耐性が反映されるべき最低限のセキュリティ・ベースラインが確立されます。データベースのセキュリティ・ベースラインについて考える際は、データを盗む可能性のある者（脅威）、保管するデータの種類（価値）、データの用途（影響）を問わず、すべてのデータベースで脆弱性を低減するために期待されるセキュリティであると考えると良いでしょう。セキュリティ・ベースラインにはわずかな例外（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、その例外が継続して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セキュリティ・ベースライン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。この評価を定期的に繰り返し、承認されたベースラインから逸脱した構成を検出する必要があります。

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、ほとんどのビジネス・ニーズに対応するように構成できます。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。セキュリティ・ベースラインの方針には、最小限のセキュリティ標準を満たした構成を反映する必要があります。セキュアなデータベース構成に関する組織の標準がまだない場合は、Oracle Databaseにつて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、Database Security Assessment Tool（DBSAT）、Oracle Data Safe、Oracle Audit Vault and Database Firewall（Oracle AVDF）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。

どれを選択すべきか

データベースをOracle Cloudサービス（AWS、GCP、Azureで使用するOracle Databaseを含む）として実行する場合は、Oracle Data Safeが無償で使用できるため、明確な選択肢となります。Oracle Data Safeは、オンプレミスなどの他のOracle Databaseでも使用できます（サブスクリプション料金がかかります）。クラウド・サービスの使用を避けたい場合は、Oracle AVDFが有力な選択肢です。調査すべきデータベースが1～2つしかなく、ドリフト検出が不要な場合は、Oracle DBSATが手軽に使用できます。Oracle DBSATはすべてのOracle Databaseに付属しており、My Oracle Supportからダウンロードできます。

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、RADIUS、Oracle Cloud Infrastructure Identity and Access Management（OCI-IAM）トークン、OCI-IAMパスワード、Microsoft Entra ID OAuth2トークン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、適切なパスワード規則を適用するようにします。ほとんどの場合、データベースのパスワード・ポリシーは、組織の標準ポリシーを反映している必要があります。これには、パスワードの長さ、有効期間、複雑さに関する要件が含まれます。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。重要性がやや低いラップトップなどのシステムよりも脆弱なパスワード・ポリシーは、到底受け入れられません。

データベース・サービス・アカウントは、下流のシステムの可用性に影響が及ぶため、場合によってはパスワードを期限切れにする手法は現実的ではありません。その場合は、制御を追加して、アカウントに接続を許可する条件を厳密に制限することで、期限切れにならないパスワードが持つリスクを軽減することを検討してください。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への移行を検討してください。データベースで使用されるもっとも一般的な厳密認証はKerberosです。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します。認証をデータベース外部のActive Directoryに移行すると、認証の一元的制御、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。

別の厳密認証方式としては、Microsoft Entra IDまたはOracle Cloud Infrastructure Identity and Access Management（OCI-IAM）によって発行されるトークンがあります。Entra IDもOCI-IAMも複数の多要素認証パスを提供しています。

MicrosoftはActive Directoryの利用顧客に対して、Entra IDに移行することでID管理インフラストラクチャを刷新することを推奨しています。おそらく今後数年で、Kerberosに代わってトークンがもっとも一般的な厳密認証メカニズムとなる見込みです。

また、RADIUSという厳密認証方式もあります。RADIUSは、古くからある周知の認証方式であり、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受け入れられていることが、近年のRADIUS採用の一因になっています。

さらに、PKI証明書もOracle Databaseの厳密認証に対応しています。証明書ベースの認証は、アプリケーションまたはAPIからデータベースへの接続において頻繁に使用されています。PKI証明書は、米国国防総省の共通アクセス・カード（CAC）、米国政府のPersonal Identity Verification（PIV）カードを含むほとんどのスマートカード認証に使用されている基盤の認証方式でもあります。

どれを選択すべきか

“パスワード以外のどれでも”と言いたいところですが、パスワードはさまざまな欠点があるにもかかわらず、依然として唯一の現実的な選択肢となるケースも一部あります。そのためここでは、パスワードからより厳密な認証方式に移行することが可能ならば、それがリスクを軽減する優れた手段となるとお伝えしておきます。重要なのは、Oracle Databaseには高い柔軟性があることです。Oracle Databaseで使用できない認証サービスはほとんどありません。データベース向けの厳密認証方式としてどれを選択するかは、ほぼ必ず、組織の他の認証ニーズに合わせた選択肢によって決まります。組織でEntra IDを使用している場合、通常はデータベースにもEntra IDを使用するのが合理的です。Oracle Access Manager、Oracle Cloud IAM、またはOktaを基に運用している場合は、おそらくRADIUSを使用してそれらのサービスをデータベースに接続するのが良いでしょう。

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手段であるため、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アカウントによる脅威を低減できます。Oracle Data Safe、Oracle AVDF、Oracle DBSATは、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。Oracle AVDFとOracle Data Safeはいずれも、レポート機能にドリフト検出が追加されており、ユーザーやその権限に対する変更を容易に特定できます。さらに、オラクルは権限分析によって、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。

権限分析で推奨されるプラクティスは、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、ごく稀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（アプリケーションやバッチ・プロセスによって使用されるアカウントなど）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の間で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ための数種のオプションが提供されています。

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強制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強制した場合、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”と見なされますが、クライアントが接続するにはユーザー認証も必要になります。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ます。また、クライアント証明書がユーザーの認証に使用される場合もあります。Oracle Database 23aiはTLS標準の最新バージョンであるTLS 1.3をサポートしています。

どれを選択すべきか

Oracle NNEとTLSのどちらを選択すべきかはユースケースによって異なります。パフォーマンスはおおよそ同程度であるため、選択の根拠にはほぼなりません。使用される暗号化の質は、いずれも強度の面では同程度ですが、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ではほぼ必ずクライアント構成の変更が必要になり、使用される証明書は最終的に期限が切れて保守が必要になります。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。ポスト量子コンピューティング耐性について、特に、あらかじめ盗んで保管しておき将来的に解読を試みようとする攻撃に対して不安がある場合は、TLSを推奨します。

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、おそ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、複数のオプションがあります。どのオプションを選択しても、接続するすべてのデータベースにわたる共通の資格証明を使用して、複数のデータベースのデータベース・アカウントを1か所で管理することになります。以下のようなオプションがあります。

クラウドベースのIDサービス

Oracle Databaseは、Microsoft Entra IDやOracle Identity and Access Management（Oracle IAM）などのクラウドベースのIDサービスをサポートしています。集中管理ユーザーは、Oracle Database 19c以降のデータベース・バージョンでサポートされています。どちらのクラウド・サービスも多要素認証をサポートしており、アプリケーション・サービスとのトークンベースの統合に対応しています。

集中管理ユーザー

集中管理ユーザーは、Oracle DatabaseをMicrosoft Active Directoryに接続するデータベース機能です。データベース・スキーマがActive Directoryのユーザーまたはグループにマッピングされ、データベース・ロールがActive Directoryのグループにマッピングされます。認証は通常、KerberosまたはPKI証明書により行われます。パスワードベースの認証もサポートされますが、推奨されません。集中管理ユーザーは、Oracle Database 18c以降のデータベース・バージョンでサポートされています。

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、集中管理ユーザーと似ていますが、Active DirectoryではなくOracle DirectoryにOracle Databaseを接続します。エンタープライズ・ユーザー・セキュリティは、Oracle Database 9i以降のデータベース・バージョンでサポートされています。エンタープライズ・ユーザー・セキュリティは、引き続き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が、Oracle Database 23aiでは非推奨になっています。

データベース・アクティビティの監査

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。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、調査をサポートし、インシデントの範囲に関する証拠を提供できます。データベース監査により、それらの記録が監査証跡に保持されます。

どのアクティビティを捕捉して監査証跡に保管するかについては、監査ポリシーにより定義します。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、システムに対する負荷が著しく増加することになるため、通常は現実的ではありません。以下は、通常は頻度が低いものの、セキュリティにおいて重視されるアクティビティです。監査のベースラインの一環として、監査ポリシーによってこれらのアクティビティを捕捉する必要があります。

- ユーザー・アカウントの変更（作成、変更、削除）
- 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
- データベースへのログイン（特にログインの失敗）
- 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

Oracle Databaseでは、このベースライン・アクティビティのほとんどを捕捉するよう監査ポリシーが事前に構成されています。そのために、ORA_SECURECONFIGまたはORA_LOGIN_LOGOUTという2つの事前構成ポリシーが存在します。いずれも19c以降のデータベースではデフォルトで有効化されています。そのため、これらのポリシーを誰も無効化していないことの確認だけが必要になります。データベース管理者に対しては、デフォルトでないORA_ALL_TOPLEVEL_ACTIONSポリシーを有効化してください。Data Pumpエクスポートを監査するには、カスタムの監査ポリシーを作成する必要があります。また、ベースラインを超えた厳格な監査ポリシーの場合は、ポリシーから逸脱したデータ・アクセスの試みを捕捉する必要もあります。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により捕捉する必要があります。

Oracle Database 12c以降、従来型監査機能のほかに統合型監査が提供されています。Oracle Database 23aiでは、従来型監査機能のサポートは終了し、統合型監査が唯一の監査機能となっています。

機密データの検出

ほとんどのデータベースでは、セキュリティ・ベースラインを超えてセキュリティを厳格にするかどうかの判断は、データベース内に保管される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となるような規制要件はあるか、あるいは、その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・リスクがあるか、といったことです。一部のデータベースではその答えは明白です。HCM、CRM、または財務用の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。製造現場のランタイム・センサー・データをホストするデータベースの場合は、おそらく追加の保護は必要ありません（データから機密性の高い知的財産が漏洩しない限り）。

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。機密データの検出はそのような場合に効果を発揮します。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。ここで引用符を使用しているのは、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るからです。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。

オラクルは、機密データの検出を支援する4つのツールを提供しています。Database Security Assessment Tool（DBSAT）、Oracle Data Safe、Oracle Audit Vault and Database Firewall（Oracle AVDF）、およびOracle Data Masking and Subsetting Packの一部であるEnterprise Managerデータ検出です。

どれを選択すべきか

Oracle Data Safeを使用できる場合は、これが第一の選択肢です。Oracle 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150種類以上の機密データを検索する機密データの検出機能が提供されます。Oracle 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。

クラウド・サービスの使用に積極的でない、あるいはクラウド・サービスよりも高度な制御を求めている組織では、Oracle AVDFが有力な選択肢です。

すでにOracle Enterprise Managerを使用していて、データ検出機能に必要なライセンスを所有している場合は、Oracle Enterprise Managerも機密データの検出における有力な選択肢です。

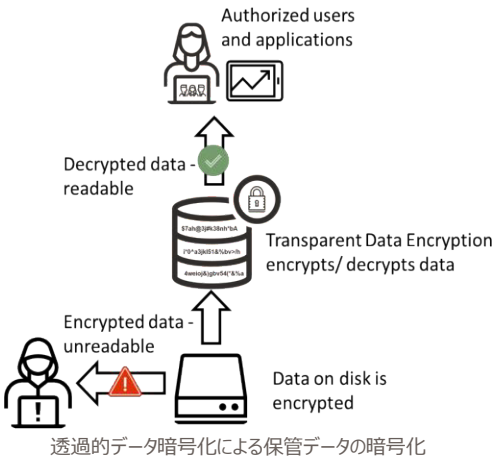
英語以外のデータベースを使用している場合は、DBSATを検討してください。DBSATは、英語以外の言語を使用したスキャニングをサポートするオラクル唯一の機密データ検出ツールです。本書の執筆時点では、DBSATには英語、スペイン語、ドイツ語、ポルトガル語、イタリア語、フランス語、オランダ語、ギリシャ語の検出パターン・ファイルが同梱されています。Oracle Data SafeやEnterprise Managerとは異なり、DBSATは実際には表データをスキャンせず、列名や列コメントを含むメタデータのみをスキャンします。

ベースラインを超えて – Maximum Security Architecture

データベースに潜むリスクに対応するためにベースラインを超えた厳格な保護が必要だと判断した場合は、オラクルのMaximum Security Architecture（Oracle MSA）の検討を始めることになります。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、セキュリティ・ベースラインを拡張し、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。Oracle MSAのさまざまなコンポーネントが、多様な攻撃手段を緩和するために使用されます。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、リスクの低減、セキュリティ向上、規制遵守の強化を行っています。

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、暗号化しておくことで、攻撃者がデータベースAPIを使用せずにデータを直接読む取ることができなくなります。この種の迂回攻撃はアクセス制御を巧妙に回避し、監査レコードの記録をトリガーしないため、絶対に避けるべき最悪の状況です。保管データの暗号化は、セキュリティ・ベースラインよりも厳格な制御としてはもっとも一般的であり、その他の非ベースラインのセキュリティ機能と比較して、多くのオラクルのお客様によって実装されています。また、多くの組織で、保管データの暗号化はベースラインに含まれています。



透過的データ暗号化による保管データの暗号化

また、暗号化は、データ・プライバシー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、通常はデータ保護のための必要な対策が講じら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）というデータベース・オプションの一機能である透過的データ暗号化（TDE）です。

TDEは20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あり、ほとんどのTDEの実装で問題は発生しません。ただし、考慮すべき点がいくつかあります。

架空の問合せではなく実際のデータ・ワークロードに基づいて、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。暗号化により、必ず何らかのパフォーマンス・オーバーヘッドが生じます。より多くの処理を実行するようシステム（特にCPU）に要求するためです。TDEとOracle Advanced Compressionの併用は、そのオーバーヘッドを低減する優れた手段です。Oracle 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中で最強の暗号化を使用してください。本書の執筆時点では、Advanced Encryption Standard（AES）256ビット鍵です。強度の低い暗号化や短い鍵長は、ポスト量子コンピューティングによる影響が懸念されるため、今後は使用しないでください。現在、強度の低い暗号化を使用している場合は、AES256への移行を検討してください。Oracle Database 23aiでは、AES256がデフォルトです。それよりも前のデータベース・バージョンでは、各表領域を手動でAES256に設定するか、データベースのデフォルト・アルゴリズムを変更する初期化パラメータを設定できます。

暗号化がバックアップ・システムに及ぼす影響を必ず考慮してください。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・システムにとって新しいデータと見なされます。そのため、重複排除の対象とならず、最初のうちは必要となるストレージが急増します。時間が経ち、暗号化されていないバックアップが古くなって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。また、暗号化されたデータの圧縮率は低くなる傾向にあるため、暗号化を先に実行するとある程度の圧縮の効果が永久に失われます。前述のOracle Advanced Compressionを使用すれば、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部分の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。

データベースのバックアップとは別に、鍵を確実にバックアップしてください。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、セキュリティを強化するために、信頼の起点として、Oracle 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、管理職務の分離は共通の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。Oracle Database Vaultは、この要件に対応できるデータベース・オプションです。Oracle 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。その他の分離については、Oracle Database Vaultポリシーによって有効化されます。どのレベルのSODが組織にとって適切であるかは、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設定はおそ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。分離される職務としては他に（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、パッチ適用などがあります。組織の状況に合ったモデルを採用し、それでも可能な限り、職務に必要な最小権限のみが付与されたアカウントを使用するよう推進してください。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。Oracle Database Vaultを使用してデータベース管理者による機密データへのアクセスをブロックすることで、不正アクセスされた管理者アカウントが与え得る被害を大幅に低減できます。

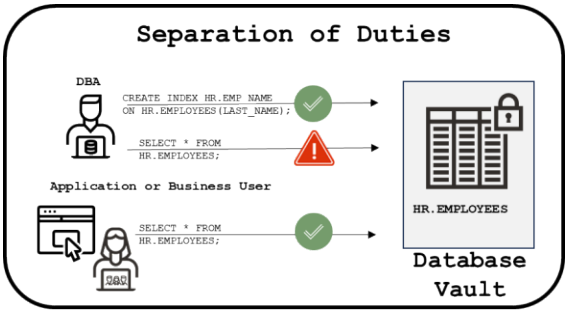


図1：特権ユーザーによるデータへのアクセスを制御

機密データへの信頼パス・アクセスの徹底

データ窃盗において、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っています。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が広がり、アカウントに不正アクセスされるリスクが増加します。Oracle 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

セキュリティ・ベースラインのセクションでは、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まと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 Data SafeとOracle Audit Vault and Database Firewallは両方とも、監査データを収集し、セキュアなデータウェアハウスに配置します。このデータウェアハウスで、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。

どれを選択すべきか

Oracle DatabaseをOracle Cloudサービス（Azure、GCP、またはAWSで使用するOracle Databaseを含む）として実行している場合は、Oracle Data Safeがそれらのサービスに含まれており追加費用はかからないため、明確な解決策となります。Oracle Data Safeは、オンプレミスなどの他のOracle Databaseでも使用できます（サブスクリプション料金がかかります）。

Oracle Databaseクラウド・サービスを使用していない場合や、Oracle DatabaseとOracle以外のデータベースの両方の監査データを収集したい場合は、Oracle Audit Vault and Database Firewallがおそらく最適な選択肢です。Oracle AVDFは、監査証跡を生成するほぼすべてのシステムから監査データを収集できます。

アクティビティの異常の検出とブロック

異常の検出と防止は、データ保護のためのもっとも重要な機能の1つです。データベースは通常、同じタスクを繰り返し実行します。そのため、何か新しいことがあればすべて、無害だと証明されるまでは警戒する必要があります。アカウントが突如これまでとは異なる振る舞いをするようになった場合（新しいプログラム、通常とは異なるOSユーザー名、新しいIPアドレスなど）、そのアカウントが属するユーザーとは別の誰かがそのアカウントを使用している可能性があります。アプリケーションが突如これまでにないSQLコマンドを実行し始めた場合、SQLインジェクションによってすり抜けようとしている可能性があります。

データベースの監査に代わるものはありませんが、監査は一般的に、異常検出にはあまり向いていません。すべてのアクティビティを監査できることは非常に稀だからです（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）。異常を検出するには、すべてのアクティビティを調査する必要があります。オラクルは、データベース・ファイアウォールという別の制御によって監査データを補完することで、このような監査の影響に対処しています。オラクルは2種類のデータベース・ファイアウォールを提供しています。両方とも基本的には同じ機能を提供しており、異常検出タスクへのアプローチも似ています。

1つ目は、Oracle Audit Vault and Database Firewallに搭載される“データベース・ファイアウォール”です。データベース・ファイアウォールはデータベースとは異なるサーバーで稼働し、データベースに送信されるSQLコマンドをネットワーク・レイヤーで監視します。データベース・ファイアウォールはプロキシとして構成できます（その場合、データベース・トラフィックはデータベースに到達する前に、このファイアウォールを通過します）。または、クライアントからデータベース・サーバーに向かってネットワークを横断中のSQLコマンドをネットワークから秘密裏に読み取ることもできます。どちらの構成でも異常検出が可能ですが、異常のブロックに対応しているのはプロキシ構成のみです。

2つ目は、Oracle Database 23aiで新たに導入されたコンポーネントである“SQLファイアウォール”です。SQLファイアウォールはデータベース・カーネルの内部で稼働し、データベースでの受信時にSQLコマンドを調査します。常にトラフィックのデータベースへの到達に合わせて実行され、異常を記録するかブロックするように構成できます。

SQLファイアウォールもデータベース・ファイアウォールも異常検出の問題に対するアプローチは同様です。通常のアクティビティ（どのIPアドレス、OSユーザー名、プログラム、SQLコマンドがデータベースに送信されているか）を学習し、その通常動作に基づいて許可リストを作成します。許可リストの作成後は、単純にその許可リストにないものはすべて異常であり、調査の必要があると見なします。この同じアプローチで、SQLインジェクション攻撃の検出とブロックも容易に実行できます。

機能的には類似しているものの、この2つの制御には大きく異なる部分があります。データベース・ファイアウォールは異種環境に対応し、Oracle Database（すべてのバージョンとエディション）、Oracle MySQL、Microsoft SQL Server、IBM Db2、SAP Sybaseを保護します。SQLファイアウォールはOracle Database 23ai Enterprise Editionのみで動作します。

データベース・ファイアウォールはネットワーク・レイヤーで動作するため、下層のデータベース・セッション・コンテキストにはアクセスしません。そのため、再帰的SQL、新規シノニム、動的に生成されたSQLの影響については把握できません。ネットワークベースの監視は、監査に適した品質のデータは生成しませんが、正常パターンからの逸脱を特定できる十分なデータを生成することに長けています。SQLファイアウォールはデータベース内で動作するため、下層のセッション・コンテキストやデータベース・メタデータに完全にアクセスできます。SQLファイアウォールはシノニム、再帰的SQL、動的SQLを可視化できます。また、SQLファイアウォールはデータベースの一部であるため、攻撃者は別のネットワーク・パスを使用してSQLファイアウォールを“迂回する”ことはできません。SQLファイアウォールによって収集されたポリシー違反データは監査に適した品質であり、SQLファイアウォールのポリシー違反については監査証跡に書き込むこともできます。

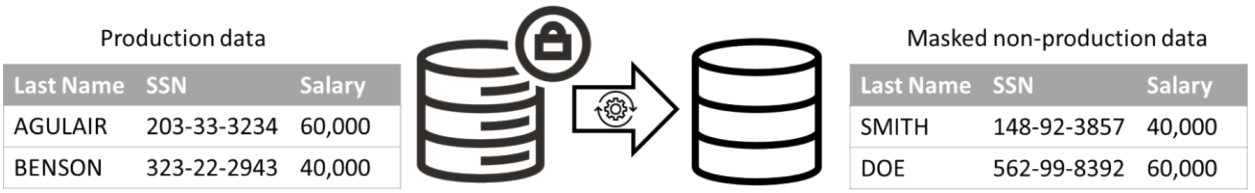
ライセンスの観点では、データベース・ファイアウォール、SQLファイアウォールの両方がOracle AVDFに含まれています。また、SQLファイアウォールはOracle Database Vaultにも含まれています。

どれを選択すべきか

Oracle Database 23aiを使用している場合、通常は新機能のSQLファイアウォールを導入するのが最適です。それよりも前のデータベース・バージョンを使用しているか、Oracle Database以外のデータベースを使用している場合は、データベース・ファイアウォールが適しています。

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架空のデータで作成されている場合は問題ありません。架空の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構築されている場合は、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。機密データを架空の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。

どれを選択すべきか

クラウド・サービスの使用が可能な組織では、ほとんどのケースでOracle Data Safeが最適な選択肢となります。より早く価値を実現でき、かつ本書ですでに説明したOracle Data Safeの他のセキュリティ機能も使用できるためです。セキュリティ制御をオンプレミスで維持したい場合は、Oracle Data Masking and Subsettingが適しています。

リスクベースのアプローチの採用

本書では最初に、すべてのデータベースに適用されるセキュリティ・ベースラインの概念について説明しました。次に、機密データの検出と、システムのリスク・レベルを最小限に抑えるためのベースラインを超えた厳格な制御について説明しました。以下に、いくつかのサンプル・システムと、それに関連するリスク・レベルおよび制御についてまとめます。

システム	リスク・レベル	ベースラインよりも厳格な制御	注釈
人事管理	高	暗号化、鍵管理、職務分離、信頼パス	プライバシーの懸念/規制
財務レポート作成	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
注文のフルフィルメント/出荷/CRM	非常に高い	暗号化、鍵管理、職務分離、信頼パス、異常検出	プライバシーの懸念/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、プライバシーの懸念/規制
テストおよび開発	高	データ・マスキング	システムからの機密データの削除

最初の1歩

本書では多くの内容を扱いましたが、手短に紹介したそれぞれの分野が、専用の書籍1冊の題材にもなり得るものです。これから行うべき作業は気が遠くなるほど膨大になる可能性があります。完璧な実装計画を立てようとして途方もない時間を費やしながら、リスク削減について何も達成できない“分析まひ”に陥る企業は後を絶ちません。特に忘れられないのは、一緒に働きたいと思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

実用に足るシステムに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、運用サポートおよびデータ使用のニーズとの間でバランスを取ることです。通常実施できる最善策は、リスクを少しずつ崩し、組織が耐えることができるレベルにまでリスクを低減することです。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強化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合理的かを判断します。本書の最初にセキュリティのベースライン・レベルの概要を説明しましたが、そのベースラインは貴社にとって合理的でしょうか?合理的である場合は、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、ということを常に意識してください。

最後に

リスクの低減とセキュリティの強化を開始する中で、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、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が保管されているため、嬉々としてその情報を盗み、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向上の一助となり、攻撃が成功する可能性を低減します。貴社のプロジェクトの成功を祈っています。

参考資料

データベースのセキュリティ強化に関する詳細や、作業に優先順位を付け、自社環境にとって最適な制御を選択するために役立つ情報については、以下のリソースを参照してください。

- Oracle Database Security – 概要
- Oracle Database Security – A Technical Primer
- データベース・セキュリティ製品のドキュメント

付録：ツール — 機能、オプション、製品、パック

この種の話題では製品と機能の一覧が欠かせませんが、本書の主要部分では製品と機能の説明を最小限に抑えるよう努めました。以下、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は注意点があります。本書の執筆時点の最新情報を記載していますが、ホワイト・ペーパーは一般的に長く有効である一方、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でドキュメントの最新バージョンを確認してください。ここに示されているリンクでは最小限、検索すべきマニュアル（および通常は章や付録）を把握できます。

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・ユーティリティです。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

Oracle 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や、Oracle Cloud Computeで実行中のOracle Databaseとともに使用できます。Oracle 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搭載されています。Oracle 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、新機能を急速に展開しています（2週間の開発スプリント）。最近の変更内容に関する最新情報については、“What’s New”を参照してください。Oracle Data Safeのドキュメントは、こちらで参照できます。

Enterprise Manager Database Lifecycle Management

Database Lifecycle Managementは、Oracle Enterprise Manager Cloud Controlの管理パックです。Database Lifecycle Management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 Database Lifecycle Management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

Oracle 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（Oracle 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。Oracle 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（EUS）は、Oracle Database Enterprise Editionに含まれるデータベース機能です。EUSは、Oracle Database 8.1（Oracle 8i）で導入されました。EUSを使用すると、Oracle DatabaseをOracleディレクトリ・サービスに接続できます。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。EUS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で導入され、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。現在は統合型監査に置き換わりつつあります。Oracle Database 23ai以降は、従来型監査のサポートは終了しています。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、Oracle 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。

Enterprise Managerデータ検出

データ検出はEnterprise Managerで使用できます。データ検出はデータベースをスキャンして機密データを特定し、Oracle Data Masking and Subsetting（Oracle DMS）、Oracle Audit Vault and Database Firewall（Oracle AVDF）の機密データの監査レポート作成、透過的機密データ保護（TSDP）のポリシー推進に役立ちます。Enterprise Managerデータ検出により、アプリケーション、表、表の列間のリレーションシップ（データ・ディクショナリで宣言されているもの、アプリケーション・メタデータからインポートされたもの、またはユーザーが指定したもののいずれか）の一覧が保存されます。データ検出は機密データのタイプとその関連先の列の情報を保持します。また、データ・サブセット化、データ・マスキングなど、テスト・データをセキュアに生成する目的でテスト・データ運用によって使用されます。Oracle Data Safeと同様に、データ検出は表に含まれるデータをスキャンして機密データを特定します。

データ検出は、Oracle Advanced Security、Oracle Database Vault、Oracle Label Security、Oracle Data Masking and Subsetting、Oracle Audit Vault and Database Firewallに搭載されており、追加費用はかかりません。データ検出は、列間の関係性や機密データが含まれる列など、データベース・スキーマについて把握するために使用できます。データ検出のドキュメントは、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Data Redactionを含むデータベース・オプションです。Oracle 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。Oracle Advanced Securityの透過的データ暗号化のドキュメントは、こちらで参照できます。Oracle Advanced SecurityのData Redaction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。Oracle Key Vaultにより、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・アーキテクチャが実現されます。暗号化鍵の保護に加えて、Oracle Key Vaultは包括的なSSH鍵ガバナンス（データベース・サーバーだけでなくすべてのLinuxサーバーを保護するための重要な機能）、シークレット管理、DBMS_CRYPTO鍵管理など多数の機能を提供しています。Oracle Key Vaultのドキュメントは、こちらで参照できます。

SQLファイアウォール

SQLファイアウォールは、Oracle Database 23aiで新たに導入されたコンポーネントです。SQLインジェクションやその他の異常を検出してブロックするよう設計されています。SQLファイアウォールは、Oracle Database VaultおよびOracle Audit Vault and Database Firewallに含まれています。SQLファイアウォールのドキュメントは、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。Oracle 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。Oracle Database VaultにはSQLファイアウォールが含まれています。Oracle 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、異種環境向けの機能を備えたデータベース・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。Oracle Databaseに対しては、セキュリティ評価、ユーザーに付与された権限の追跡、ドリフト検出、機密データの検出の機能も提供されます。また、Oracle AVDFにはSQLファイアウォールが含まれています。Oracle 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。機密データを架空の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。Oracle Data Masking and Subsettingのドキュメントは、こちらで参照できます。

ORACLE

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