ORACLE

SQLインジェクションのリスクの軽減

2023年11月、バージョン1.0

公開

ORACLE

本書の目的

本書では、Oracle Database 23c、およびOracle Audit Vault and Database Firewall（Oracle AVDF）20.10の機能および強化された点の概要が説明されています。本書は、Oracle Database 23cまたはOracle AVDF 20.10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。

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。本文書と本文書に含まれる情報は、オラクルの事前の書面による同意なしに、公開、複製、再作成、またはオラクルの外部に配布することはできません。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

エグゼクティブ・サマリー

SQLインジェクションは、もっとも古く、もっとも頻繁に発生するデータベース攻撃パターンの1つです。問題解決のための何年もの研究と努力にもかかわらず、データ主導型Webアプリケーションに悪影響を及ぼしています。Webアプリケーション・ファイアウォール（WAF）を使用したり、アプリケーション・レベルで保護を追加したりといった従来の方法では、SQLインジェクションのリスクを軽減することはできません。Oracle Databaseセキュリティでは、データ主導型Webアプリケーションに対するSQLインジェクションのリスクを軽減するために2つのアプローチを提供します。

1. Oracle Audit Vault and Database Firewall（Oracle AVDF）のネットワークベースのDatabase Firewall
2. Oracle Databaseに組み込まれたOracle SQLファイアウォール

この技術レポートでは、これらのソリューションを活用して構成することで、データ主導型Webアプリケーションに対するSQLインジェクションのリスクを軽減する方法を説明し、ニーズにもっとも合う方法を選択するための戦略を提案します。

ORACLE

目次

はじめに 6

ネットワークベースのDatabase Firewall 7

SQLインジェクションのリスクを軽減するためのDatabase Firewallポリシー 9

データベース・カーネルに常駐するSQLファイアウォール 12

SQLインジェクションのリスクを軽減するためのSQLファイアウォール・ポリシー 13

学習ステージ 13

保護ステージ 14

SQLファイアウォールの管理 15

SYS.DBMS_SQL_FIREWALLパッケージによるSQLファイアウォールの管理 15

Data SafeによるSQLファイアウォールの管理 17

どちらを使用するかを決定：Database FirewallかSQLファイアウォールか 20

まとめ 20

図一覧

図1：SQLインジェクションの攻撃パターン

図2：Oracle AVDFでのネットワークベースの Database Firewall

図3：Database FirewallによるSQLインジェクションのリスクの軽減

図4：Database Firewall：SQLインジェクションの攻撃パターンを検出してアラートを生成するためのポリシー

図5：Database Firewall：セッション・コンテキスト・ルール

図6：Database Firewall：SQL文ルール

図7：Database Firewall：正常なアプリケーションSQLトラフィックのSQLクラスタ・セット

図8：Database Firewall：アプリケーション・サービス・アカウント・プロファイル

図9：Database Firewall：データベース・オブジェクト・ルール

図10：Database Firewall：権限のあるユーザーと機密性の高いオブジェクトを含むグローバル・セット

図11：Oracle Databaseカーネルに組み込まれたSQLファイアウォール

図12：SQLファイアウォールのプロセス・フロー

図13：SQLファイアウォール・ポリシー

図14：SQLファイアウォール・ポリシーの有効化オプション：実施とアクション

図15：Data Safe：SQLファイアウォールのダッシュボード

図16：Data Safe：収集の作成と開始

図17：Data Safe：SQL収集インサイト

図18：Data Safe：許可リストを含むSQLファイアウォール・ポリシー
図19：Data Safe：SQLファイアウォール・ポリシーの有効化
図20：Data Safe：SQLファイアウォール違反（フリート・ビュー）
図21：Data Safe：SQLファイアウォール違反レポートの詳細
図22：Data Safe：潜在的なSQLインジェクション試行時のサンプル電子メール通知

表一覧

表1：Database Firewallのデプロイメント・モード
表2：SYS.DBMS_SQL_FIREWALLパッケージの重要なPL/SQLプロシージャ

はじめに

SQLインジェクションは、2017年以降、Open Web Application Security Project（OWASP）のアプリケーション・セキュリティに対する脅威トップ10のリスト上でもっとも有名な攻撃パターンの1つです。SQLインジェクションでは、データ主導型アプリケーションの入力フィールドまたはパラメータに悪意のあるSQLコードを注入し、アプリケーションをだまして注入されたSQLに応答させます。SQLインジェクション攻撃が成功すると、アプリケーションでデータが公開されたり、アプリケーション開発者が意図しないアクションが発生したりします。

ほとんどの3層アプリケーションは、アプリケーション・サービス・アカウントとしてデータベースに接続します。これは特殊な種類の非ユーザー特権アカウントで、基礎となるデータベースでのアプリケーションSQL問合せの実行や、自動化されたサービスや他のプロセスの実行に使用されます。アプリケーション・サービス・アカウントは、アプリケーションが実行する可能性があるあらゆるアクションを実行するために必要なすべての権限を持つ特権アカウントです。通常は、アプリケーション・スキーマ（すべてのデータを含む）およびプロシージャ全体にアクセスできます。アプリケーション層は、エンドユーザーのIDと認可に基づいて中間層でアクセス制御を実施します。SQLインジェクション攻撃は、アプリケーションの入力フィールドへの悪意のあるコードの挿入、つまり“インジェクション”で構成されます。攻撃により、アプリケーションはインジェクトされたSQLに応答せざるを得ず、アプリケーション・サービス・アカウントが実行の権限を与えられているすべての操作をデータベースに対して実行できるようになります。これは、Webアプリケーションの認証および認可メカニズムを迂回し、アプリケーション・サービス・アカウントの特権アクセスを使用してデータベースの内容を取得するための完璧な手法です。これには、顧客情報、個人データ、企業秘密、知的財産などの機密データへの不正アクセスが含まれます。攻撃者は、SQLインジェクションを使用して、データベース内のレコードを追加、変更、および削除しようとする可能性があります。

SQLインジェクションは、より広範囲にわたる侵害の入口となることがよくあります。攻撃者は、不正アクセスしたデータベースからデータを引き出すだけでなく、内部ネットワーク上の別のホストに横展開する場合があります。SQLインジェクションの脆弱性、攻撃、および手法には多数の種類があります。しかし、それらのすべてに同様の攻撃パターンがあります。

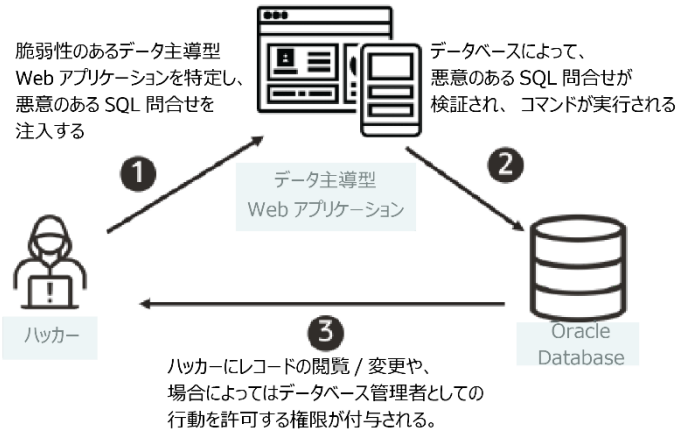

図1：SQLインジェクションの攻撃パターン

SQLインジェクション攻撃を阻止したり軽減したりするのは簡単ではありません。従来のアプローチには、ユーザー認証の向上、最小権限の強化、準備済みステートメントの使用、動的問合せの回避、入力内容の検証の実行など、アプリケーション・レベルの保護が組み込まれています。これらの方法でも保護が強化されるため実践すべきではありますが、開発や構成管理でのわずかなギャップによっても脆弱性が発生する可能性があります。レガシー・アプリケーションの場合は、ソース・コードにアクセスしてSQLインジェクションの脆弱性を修正する必要があります。

WAFは、疑わしい*HTTP*トラフィックがアプリケーションに到達する前にそれを除外することによってSQLインジェクションの試みをブロックするための別の方法です。ほとんどのWAFは、正規表現のパターン・マッチングに依存しています。よくあるSQLインジェクションのペイロードを検出してブロックすることはできる可能性がありますが、ゼロデイ攻撃や複雑なSQLインジェクション攻撃に直面した場合は通常、役に立ちません。WAFでは、インジェクション・ペイロードの実際の内容を評価できず、意思決定時に完全なSQLコンテキストを使用できません。

SQLインジェクション攻撃をブロックするためのもう1つのアプローチは、データベースに処理される前にデータベース・トラフィックをフィルタリングすることです。ここで、データベース・ファイアウォールが関連します。データベース・ファイアウォールは、受信するSQLを分析するための簡潔で効果的な方法を提供することで、インジェクション攻撃を検出し、必要に応じてアラートを生成して、インジェクション攻撃がデータベースに到達するのを阻止します。Oracle Databaseセキュリティでは、データベース・トラフィックをフィルタリングしてSQLインジェクション攻撃のリスクを軽減するために2つのアプローチを提供します。

1. Oracle Audit Vault and Database Firewall（Oracle AVDF）のネットワークベースのDatabase Firewall
2. Oracle Databaseに組み込まれ、Database VaultとOracle AVDF両方の一部であるSQLファイアウォール

他のアプリケーションベースのファイアウォールとは異なり、上記のアプローチはいずれも正規表現のパターン・マッチングに依存しません。代わりに、データベース・ファイアウォールは一般的なアプリケーションSQLトラフィックを学習し、トレーニングされたモデルにSQL文が合致しない場合に拒否したりアラートを生成したりすることができます。

Oracle Database 23cのSQLファイアウォールは、保護をさらにデータに近づけ、実施ポイントをネットワークからデータベース・カーネルに移行しています。データベース・カーネル内で保護を実施することにより、外部のDatabase Firewall経由のデータベース・トラフィックをルーティングする複雑さを回避できます。アプリケーションでこの強力な新しいデータベース・セキュリティ機能を利用することで、SQLインジェクション攻撃のリスクを軽減できます。

これら両方のソリューションによってSQLインジェクションのリスクを軽減する方法を見ていきましょう。ネットワーク・ファイアウォールと組込みファイアウォールは両方とも、次の3つのユースケースに対応できます。

- 認可されたSQL文およびデータベース接続のみにデータベース・アクセスを制限することにより、ゼロデイ攻撃に対するリアルタイムの保護を提供
- SQLインジェクション攻撃、異常なアクセス、資格証明の盗難/乱用リスクの軽減
- 信頼できるデータベース接続パスの適用

ネットワークベースのDatabase Firewall

Oracle AVDFのコンポーネントであるDatabase Firewallはネットワーク上でデータベース防御の最前線として機能し、SQLトラフィックを監視してデータベース・アクセスに期待される動作を実行させる一方、SQLインジェクション、アプリケーション・バイパスなどの悪意のあるアクティビティがデータベースに到達しないように阻止します。1つのDatabase Firewallで、異なるタイプの複数のデータベースを一元的に保護できます。これにより、Oracle、MySQL、Microsoft SQL Server、SAP Sybase、IBM Db2などのエンタープライズ・データベースを監視します。

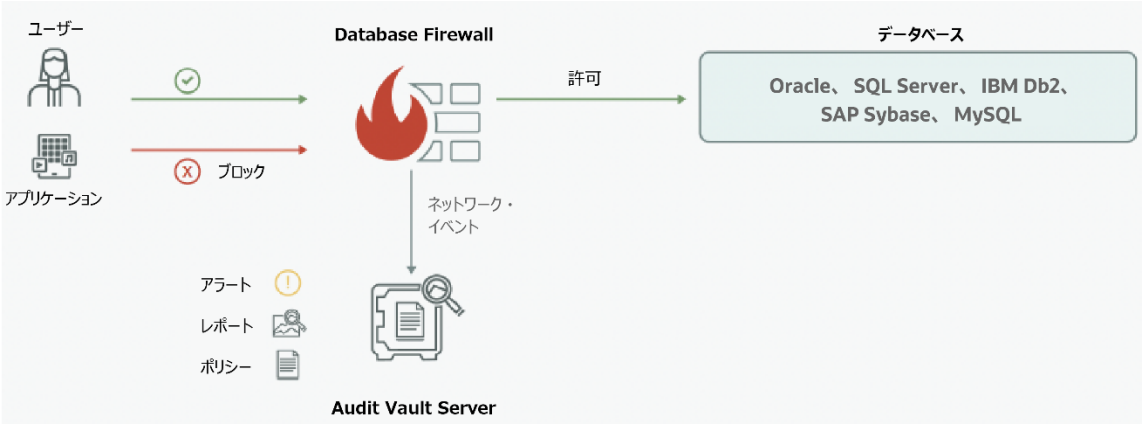

図2：Oracle AVDFでのネットワークベースのDatabase Firewall

Database Firewallは、表1に示すようにさまざまなモードでデプロイできます。

表1：Database Firewallのデプロイメント・モード

モード	詳細	モニタリングまたはブロッキング
プロキシ	リターン・トラフィックを含む、データベース・サーバーへのすべてのトラフィックは、Database Firewall経由でルーティングされます。	• モニタリング • ブロッキング
ホスト監視	ホスト監視はデータベースと同じマシンにデプロイされます。データベースに送信されるSQLトラフィックを取得してから、それをDatabase Firewallにセキュアに転送します。	• モニタリング
帯域外	Database Firewallは、データベースに送信されるネットワーク・トラフィックをリスニングします。データベース・トラフィックのコピーをDatabase Firewallに送信するために、スパン・ポート、ポート・レプリケータなどのいくつかのテクノロジーを使用できます。	• モニタリング

選択するデプロイメント・モードは、潜在的なSQLインジェクション攻撃を検出して監視したいのか、それとも不正なアクティビティをブロックすることで信頼できるアクセス・パターンをデータベースに適用したいのかによって異なります。

攻撃を（ブロックせずに）監視するのみの場合は、ホスト監視モードまたは帯域外モードを使用できます。どちらのモードも、ネットワーク・トラフィックを"スニッフィング"し、Database Firewallのポリシーに違反するSQL文を探すことで機能します。ホスト監視モードでは、データベース・サーバーからのネットワーク・アクティビティをスニッフィングして受信SQLトラフィックを取得し、それをDatabase Firewallに送信して分析できるようにします。帯域外モードでは、SQLトラフィックをネットワークから直接スニッフィングし、Database Firewallに転送します。

不正なSQLトラフィックをブロックするには、プロキシ・モードのデプロイメントを使用して、ファイアウォールと受信SQLトラフィックをインラインにする必要があります。プロキシ・モードは、最初はトラフィックを（ブロックせずに）監視し、不正なアクティビティに対してアラートを生成するのみに設定して実施できます。ファイアウォールのポリシーに確信が持てたら、ブロッキング・モードに切り替えてポリシーを実施し、許可リストにないSQL文や他の不正なアクセスをブロックできます。

Database Firewallは、受信SQLトラフィックを検査し、SQLコマンドへの対応（許可、ログ、アラート、置換、またはブロック）を決定します。ファイアウォールでは、IPアドレス、データベース・ユーザー、OSユーザー、プログラム名、SQL文のカテゴリ、データ定義言語（DDL）、データ操作言語（DML）、およびアクセスされているデータベース表のチェックなどの複数の段階を通じてSQLトラフィックを評価します。

Database Firewallは、許可リストと拒否リストの両方のポリシーをサポートしますが、ほとんどの場合は許可リストを使用することが推奨されます。結局のところ、"不適切な"SQL文の範囲はほぼ無限です。これに対して、アプリケーションが生成すべき文の範囲は、可能性のあるバリエーションの総数のうちの小さなサブセットです。言い換えると、ファイアウォールが通過させるべき内容を記述する方が、ファイアウォールが通過させるべきでない内容をすべて列挙するよりもずっと簡単ということです。

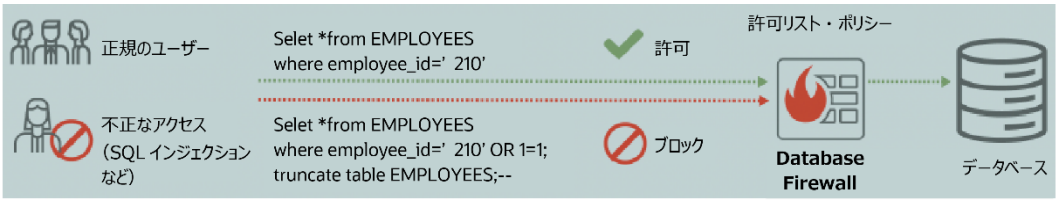

図3：Database FirewallによるSQLインジェクションのリスクの軽減

Database Firewallポリシーに許可リストや許容できるベースラインを構築することで、SQLインジェクションのリスク（多数のゼロデイ攻撃を含む）を軽減する効果的な制御が可能になります。

SQLインジェクションのリスクを軽減するためのDatabase Firewallポリシー

SQLインジェクションのリスクを軽減するための一般的な許可リストのポリシーは次のようになります。

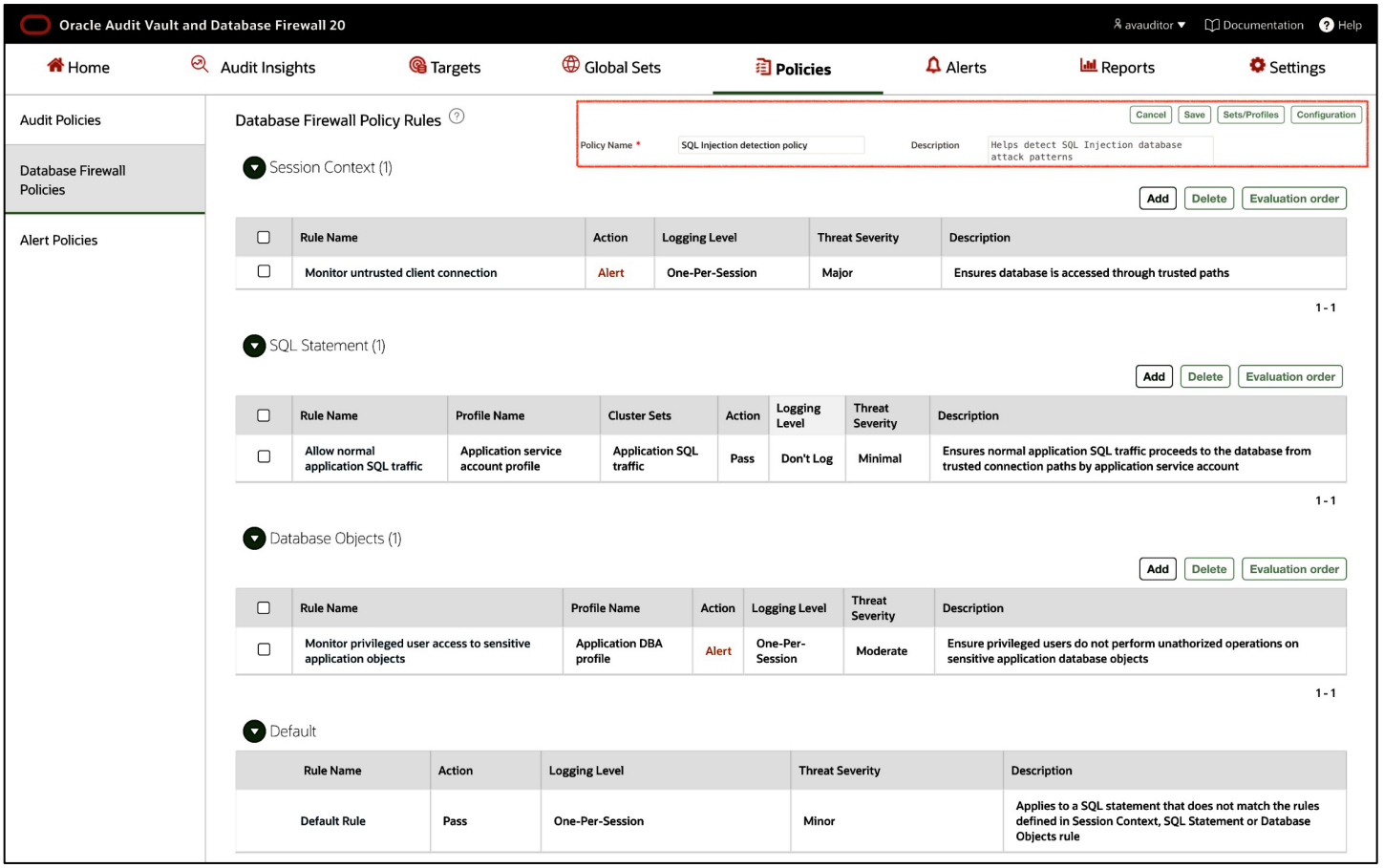

図4：Database Firewall：SQLインジェクションの攻撃パターンを検出してアラートを生成するためのポリシー

Database Firewallポリシーの以下の順次チェック（ルール）を利用して、受信SQLトラフィックがデータベースに送られる前に検査します。

1. 以下のように、セッション・コンテキスト・ルールを使用して、データベース・ユーザー（管理者やアプリケーション・サービス・アカウントなど）が信頼できるアプリケーション・パスを通じてデータベースにアクセスできるようにします。SQLトラフィックの発生元が信頼できないクライアント接続の場合にアラートを生成（またはブロック）します。信頼できるソースからのSQLトラフィックは、次のルールに進んで処理を続けます。

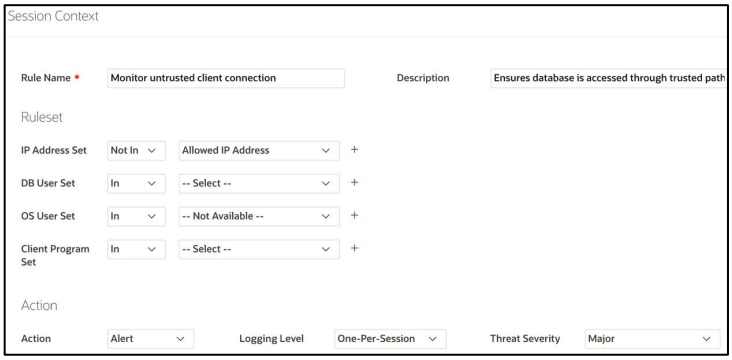

図5：Database Firewall：セッション・コンテキスト・ルール

2. 以下のように、SQL文ルールを使用して、明示的に承認されたSQL文のみが信頼できる接続パスからデータベースに到達できるようにします。残りのSQLトラフィックは、次のルールに進んで処理を続けます。

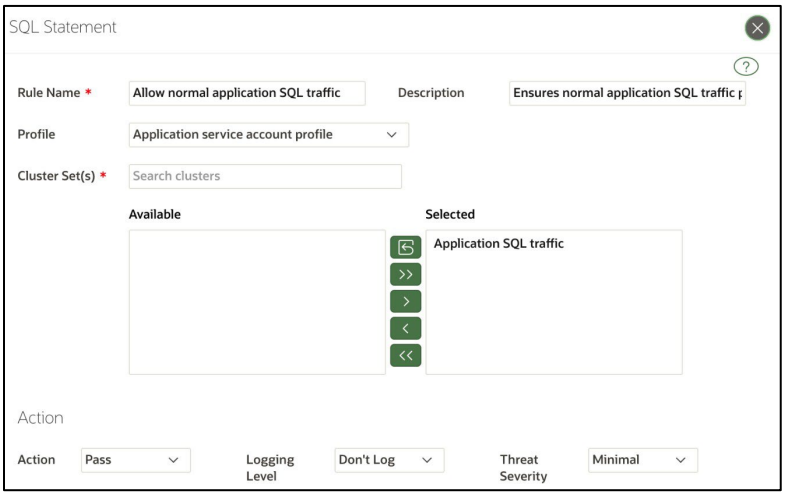

図6：Database Firewall：SQL文ルール

ルールのSQLクラスタ・セットを使用して、承認されたSQL文の許可リストを示します。Database Firewallが、信頼できる接続パスからの認可された正常なSQLトラフィックを学習するようにトレーニングします。Database FirewallによってSQLトラフィックの一意のSQL文がSQLクラスタにグループ化され、以下のようにこれをSQLクラスタ・セットで使用できるようになります。

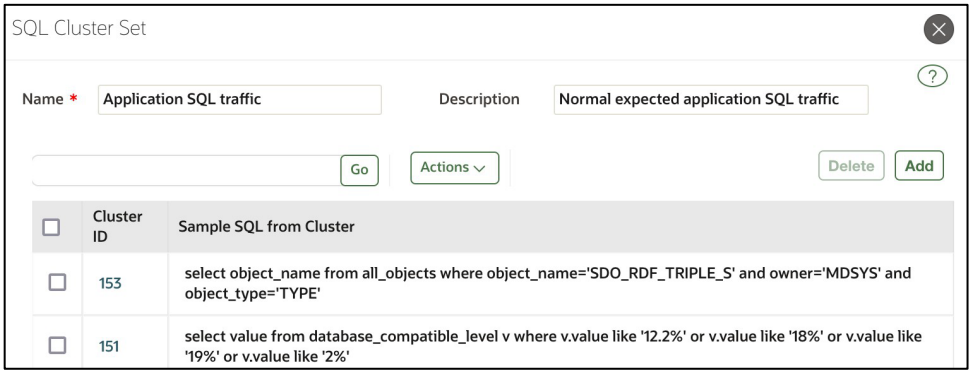

図7：Database Firewall：正常なアプリケーションSQLトラフィックのSQLクラスタ・セット

以下のように、ルールのプロファイルを使用して、信頼できる接続パスからSQLクラスタ・セット内の承認されたSQL文にアクセスするために有効なビジネス上の理由がある、権限のあるデータベース・ユーザーを示します。

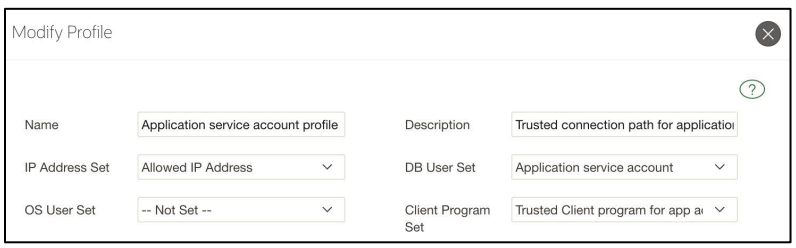

図8：Database Firewall：アプリケーション・サービス・アカウント・プロファイル

3. 以下のように、データベース・オブジェクト・ルールを使用して、権限のあるユーザーがネットワーク経由で機密性の高いアプリケーション・データベース・オブジェクトに対して認可された操作のみを実行できるようにします。権限のあるユーザーによって異常な操作が行われた場合は、アラートを生成（またはブロック）します。残りのSQLトラフィックは、次のルールに進んで処理を続けます。

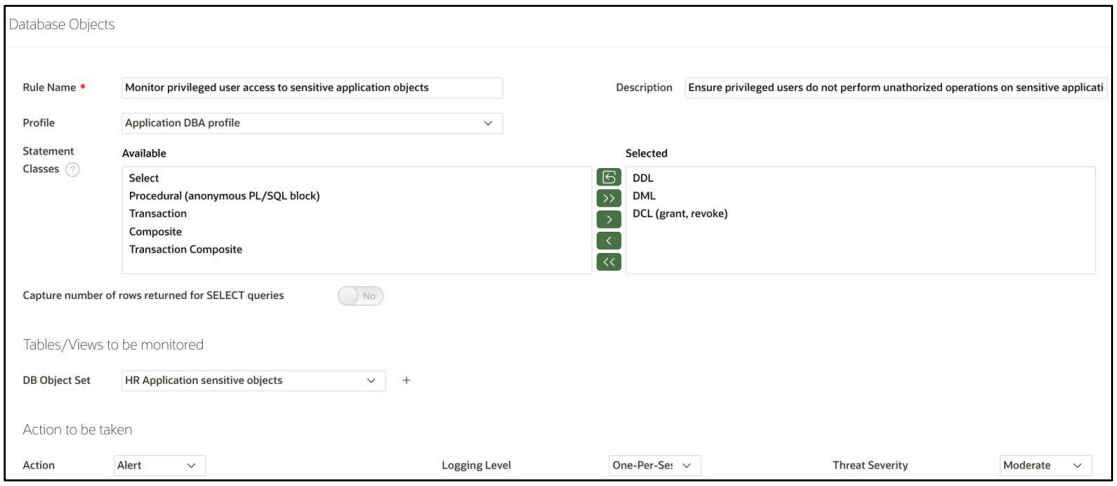

図9：Database Firewall：データベース・オブジェクト・ルール

以下のように、グローバル・セットを利用して権限のあるユーザーと機密データを特定します。データベース・オブジェクト・ルールのプロファイルを使用して、アプリケーションDBAなどの権限のあるユーザーの名前付きセットとその信頼できる接続パスを示します。ルールで検出された機密性の高いオブジェクトの名前付きセットを使用して、アラートの対象にしたい不正な操作を選択します。

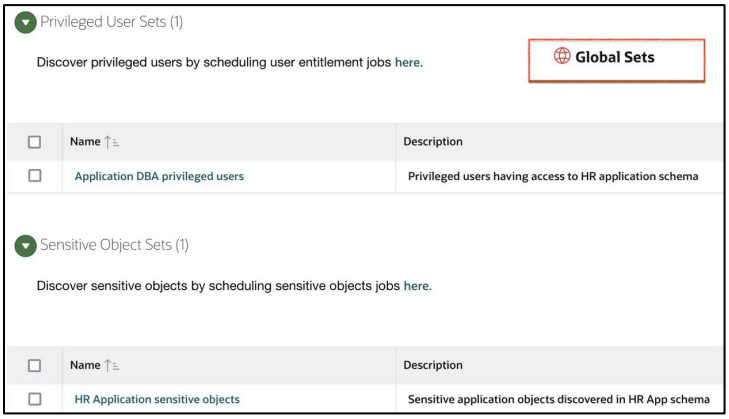

図10：Database Firewall：権限のあるユーザーと機密性の高いオブジェクトを含むグローバル・セット

4. デフォルトのルールを使用して、すべての新規のSQLトラフィックが精査されてからデータベースに進むようにします。新規のSQLトラフィックは、アプリケーションの更新後、新規のユーザーまたはアプリケーションの追加後、または明示的に承認されなかったものの後に発生する場合があります。SQL文はログに記録され、レポートとして表示できます。承認されたSQLベースラインが適切に確立されたら、そのようなトラフィックにアラートを出すようにアクションを切り替える必要があります。

Database Firewallで生じたアラートはAudit Vaultサーバーに送信され、そこでは設定したポリシーに応じて通知がトリガーされます。あらゆるSQLインジェクションの攻撃パターンの発生を検出するためのモニタリング（およびアラートの生成）を考慮してください。十分にトレーニングされたシステム上のセッション・コンテキスト、データベース・オブジェクト、およびデフォルト・ルールでブロッキング・アクションに切り替えて、SQLインジェクションのリスク（ゼロデイ攻撃を含む）へのゼロトレランスおよび予防的戦略を採用することをお勧めします。

データベース・カーネルに常駐するSQLファイアウォール

SQLファイアウォールは、Oracle Database 23cに組み込まれた新機能です。Database Firewallと同様、SQLファイアウォールを使用すると、データ主導型WebアプリケーションへのSQLインジェクションなどのWebアプリケーション攻撃のリスクを軽減できます。Database Firewallとは異なり、SQLファイアウォールでは製品インストールやネットワーク構成を追加する必要がないため、デプロイが大幅に簡素化されます。SQLファイアウォールはOracle Databaseに組み込まれているため、Oracle Database 23c以降でのみ動作します。

SQLファイアウォールはOracle Databaseカーネルの一部分で、データが常駐する場所のより近くで機能するため、制御がバイパスされる可能性がなくなります。SQLファイアウォールは受信するSQL文をすべて検査し、信頼できるデータベース接続パスからの明示的に認可されたSQLのみをデータベースが実行するようにします。SQLファイアウォールは、ローカルであれネットワーク経由であれ、暗号化済みであれ暗号化されていないテキストであれ、あらゆるSQL文を検査できます。正規表現ベースのパターン・マッチングによる保護メカニズムとは異なり、SQL文のエンコーディング、シノニムの参照、または動的に生成されたオブジェクト名の使用によってSQLファイアウォールをバイパスすることはできません。

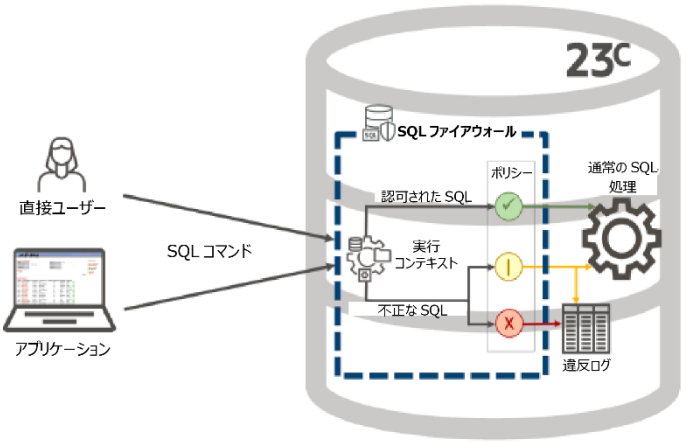

図11：Oracle Databaseカーネルに組み込まれたSQLファイアウォール

Oracle Databaseに組み込まれた他のデータベース・セキュリティ機能がWebアプリケーション攻撃を監視または阻止するためにさまざまなセキュリティ制御を提供する一方で、SQLファイアウォールは、すべての受信SQL文を検査し、認可されたSQLのみを許可する唯一の方法です。SQLファイアウォールは、不正なSQLをログに記録し、データベースで実行されるのをブロックして、Oracle DatabaseへのSQLインジェクション・データベース攻撃に対して高レベルの保護を提供します。

SQLファイアウォールは、信頼できるIPアドレス、オペレーティング・システム・ユーザー名、またはプログラム名から発生していない接続などの異常なアクセス・パターンを観察（またはブロック）することもできるため、データベースへのあらゆるアクセスが信頼できるエンドポイントからのみ行われるようにできます。この機能は、すぐに保護を実行したい場合に役立ちます。同時に、アプリケーション用にSQL文の許可リストを作成します。これには、ファイアウォールを広範囲にわたってトレーニングし、可能性のあるあらゆるSQL文を取得するようにする必要があります。セッション・コンテキスト属性からの許可リスト・ルールは簡単に取得でき、必要に応じて手動で入力できます。

SQLファイアウォールをデータベース内で構築してその実装を合理化することで、パフォーマンス・オーバーヘッドがごくわずかになり、あらゆる本番ワークロードに適するようになります。SQLファイアウォールは、Oracle Database Vaultに含まれています。Oracle AVDFとのSQLファイアウォールの使用も、監視対象のOracle Database向けに提供されています。

SQLインジェクションのリスクを軽減するためのSQLファイアウォール・ポリシー

SQLファイアウォール・ポリシーは、アプリケーション・サービス・アカウントであっても、レポーティング・ユーザーやデータベース管理者などの直接データベース・ユーザーであっても、データベース・アカウント・レベルで機能します。言い換えると、データベース・ユーザー“HR”用に1つのSQLファイアウォール・ポリシーを用意し、データベース・ユーザー“JOE”用に別のSQLファイアウォール・ポリシーを用意するということです。この柔軟性により、データベース管理者またはアプリケーション・サービス・アカウントのいずれかから始めて、データベースの保護レベルを徐々に構築することができます。

各データベース・アカウント用のSQLファイアウォール・ポリシーは、2つの異なる許可リストで構成されます。認可されたSQL文の許可リストと、関連する信頼できるデータベース接続パスの許可リストですSQLファイアウォールの許可リストにより、信頼できるデータベース接続からの認可されたSQL文のみがOracle Database内部での実行を許可されるようにでき、そこに保存されている機密データへの不正なアクセスの試みに対してはアラートの生成またはブロッキングが実行されるようにできます。

データベース・ユーザーの認可されたSQL文と信頼できるデータベース接続パスを取得することによって、SQLファイアウォールをトレーニングします。そのトレーニング・モデルを使用して、取得したSQLアクティビティの許可リストを含むSQLファイアウォール・ポリシーを生成します。その後、SQLファイアウォール・ポリシーを有効化して、潜在的なSQLインジェクション攻撃を阻止または検出します。

SQLファイアウォールは、不正なアクティビティ（許可リストにないもの）を検出すると違反ログ・エントリを生成します。必要に応じて、違反しているSQLトラフィックまたは接続をブロックするようにSQLファイアウォールを構成できます。プロセス・フローを以下に示します。

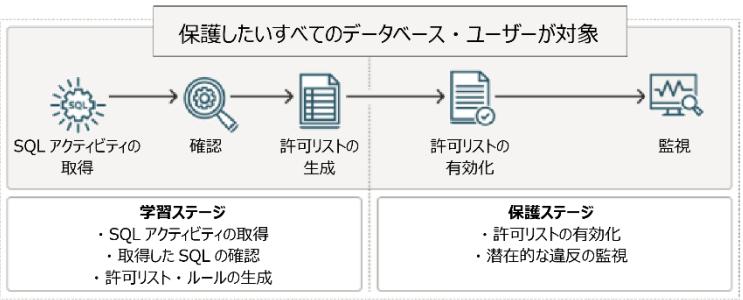

図12：SQLファイアウォールのプロセス・フロー

学習ステージ

SQLアクティビティの取得（収集）：SQLファイアウォールで保護したいすべてのデータベース・アカウントについて、信頼できるデータベース接続パス経由の認可されたSQL文を取得することにより、SQLファイアウォールにデータベース・ユーザーの正常なSQLトラフィックを学習させます。SQLファイアウォールは、以下のカテゴリの情報を取得して、ファイアウォール・ポリシーの許可リストを作成します。

- データベース・セッション情報—クライアントIPアドレス、OSプログラム名、OSユーザー名
- SQLシグネチャによって識別される一意のSQL文
- コンテキスト属性の実行
    - 現在のユーザー
    - SQL問合せの粒度（ユーザーが開始したトップレベルの文、またはPL/SQLプロシージャ内でそれらの代わりに発行されたSQL文）

SQLファイアウォールは、SQLシグネチャを利用して一意のSQL文を識別します。各SQL文は、たとえ同じセッション内で文が複数回実行されたとしても、1セッションあたり1回取得されます。SQL文は、正規化されてデータベース・オブジェクト・リストと連結され、その後、ハッシュされてSQLシグネチャを生成します。

取得（収集）の確認：SQLファイアウォールにより、SQL取得の進捗を監視でき、SQLファイアウォールがアプリケーションSQLトラフィックを完全に学習したことを確認できます。DBA_SQL_FIREWALL_CAPTURE_LOGS（Oracle Data Safe：収集インサイト）を確認し、新規の一意の文を取得しなくなったら収集を停止します。

許可リストを含むファイアウォール・ポリシーの生成：許可されたSQL文および許可されたコンテキストのベースラインを設定する許可リストを含むファイアウォール・ポリシーを生成します。

許可されたSQL文は、<SQLシグネチャ、実行コンテキスト>の一意の組合せペアのコレクションです。ポリシーの許可リストのSQLシグネチャと構文的に似ている構造を含む受信SQL問合せはすべて、対応するランタイム実行コンテキストも許可リストのそれと一致する場合に実行のために渡されます。

許可されたコンテキストは信頼できるデータベース接続パスを表し、クライアントIPアドレス、OSプログラム名、およびOSユーザー名という3つの異なるグループで構成されます。これらにより、データベースへのアクセスが許可リストに定義された信頼できるエンドポイントのみから生じていることを確認できます。許可リストを含むファイアウォール・ポリシーを以下に示します。

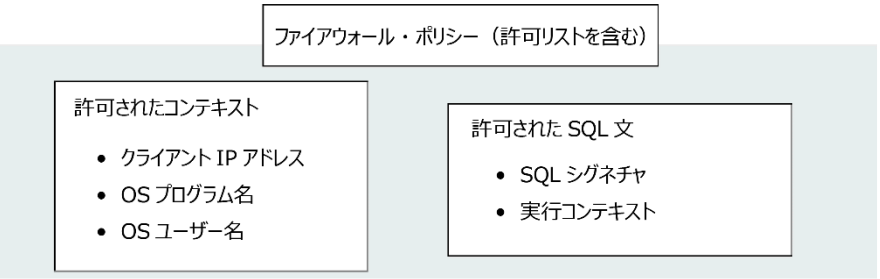

図13：SQLファイアウォール・ポリシー

保護ステージ

ファイアウォール・ポリシーの有効化：生成されたファイアウォール・ポリシーを有効化してデータベース・ユーザーを保護します。ユーザーがデータベースに接続してSQL文を発行すると、SQLファイアウォールによって許可リストへのチェックが実施されます。チェックを実施したい対象が、許可されたコンテキストなのか、許可されたSQL文なのか、またはその両方なのかをSQLファイアウォールに認識させることができます。

受信SQLトラフィックのデータベース接続パスまたはSQL文が、有効化済みで適用済みの許可リストのエントリに一致しない場合は、SQLファイアウォール違反がトリガーされ、このインシデントは違反ログに記録されます。SQLファイアウォールに、SQLファイアウォール違反インシデントにどのように反応すべきか（トラフィックがデータベースに進むのを許可するか、またはブロックするか）を認識させることができます。ブロッキングの場合はORA-47605（SQLファイアウォール違反）が発生し、クライアント接続を中断することなく異常なデータベース・アクセスを阻止します。実施範囲とファイアウォールのアクションの意味について図14に図示します。SQLファイアウォールはすべての違反をログに記録し、必要に応じてデータベース・ユーザーによるアクションの実行をブロックします。

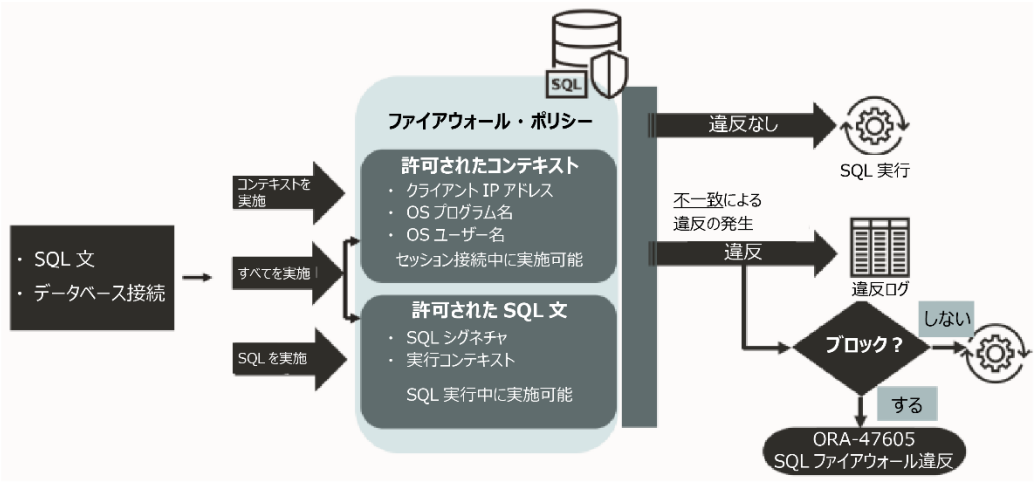

図14：SQLファイアウォール・ポリシーの有効化オプション：実施とアクション

SQLファイアウォールでは、有効化されたファイアウォール・ポリシーの許可リストに新規のSQL文と接続パスを追加できます。これは、ただちに有効になります。

違反の監視：SQLファイアウォールは、SQLファイアウォール・ポリシーの有効化された許可リスト内のエントリに一致しないデータベース接続またはSQLコマンド実行のすべてのシナリオについて、リアルタイムで違反を取り上げてログに記録します。セキュリティ管理者は、SQLファイアウォール違反ログを監視することで、異常の存在を検出できます。Data Safeにより、違反ログを収集し、レポートとして視覚化できます。SQLファイアウォール違反（特にブロックされたもの）を監査することをお勧めします。違反の出現は、SQLインジェクションや資格証明の盗難/乱用などの異常なデータベース・アクセスの試行を示している可能性があります。違反を監査することで、データベースの監査証跡に違反の記録が残り、改ざんを防ぐことができます。

SQLファイアウォールの管理

SQLファイアウォールは、次の2つの方法で管理できます。

- SYS.DBMS_SQL_FIREWALLパッケージのPL/SQLプロシージャ
- Data Safe

SQLファイアウォールを各データベース・インスタンス内で管理したい場合は、SYS.DBMS_SQL_FIREWALLパッケージのPL/SQLプロシージャを使用します。一元的な違反レポート作成、UIベースの管理、または複数のSQLファイアウォールの一元管理を望む場合は、Data Safeを使用します。さらなる自動化と統合のためには、Data Safe REST API、ソフトウェア開発者キット（SDK）、CLI、およびTerraformを使用できます。また、広範なOracle Cloud Infrastructure（OCI）エコシステムを利用して、SQLファイアウォール違反とOCIのアラートおよび通知とを統合することもできます。

SYS.DBMS_SQL_FIREWALLパッケージによるSQLファイアウォールの管理

SYS.DBMS_SQL_FIREWALLのPL/SQLプロシージャを使用すると、SQLファイアウォール構成を管理できます。以下の表は、サンプル・アプリケーション・サービス・アカウントEMPLOYEESEARCH_PRODでSQLファイアウォールを構成するための一般的な操作を示したものです。

表2：SYS.DBMS_SQL_FIREWALLパッケージの重要なPL/SQLプロシージャ

プロシージャ	値
SQLアクティビティの取得（収集）	**DBMS_SQL_FIREWALL.CREATE_CAPTURE** • データベース・ユーザーのSQL取得を作成（および開始）します。 DBMS_SQL_FIREWALL.CREATE_CAPTURE(*'EMPLOYEESEARCH_PROD'*); **DBMS_SQL_FIREWALL.STOP_CAPTURE** • 取得を確認して、取得を停止します。 SELECT * FROM DBA_SQL_FIREWALL_CAPTURE_LOGS WHERE USERNAME = *'EMPLOYEESEARCH_PROD'*; DBMS_SQL_FIREWALL.STOP_CAPTURE(*'EMPLOYEESEARCH_PROD'*);
許可リスト・ルールを含むファイアウォール・ポリシーの生成	**DBMS_SQL_FIREWALL.GENERATE_ALLOW_LIST** • 許可リスト・ルールを含むSQLファイアウォール・ポリシーを生成します。 DBMS_SQL_FIREWALL.GENERATE_ALLOW_LIST(*'EMPLOYEESEARCH_PROD'*); **DBMS_SQL_FIREWALL.ADD_ALLOW_LIST/ DELETE_ALLOWED_CONTEXT** • 許可されたコンテキスト値（すなわち、クライアントIPアドレス、OSプログラム名、OSユーザー名）を変更します。 DBMS_SQL_FIREWALL.ADD_ALLOWED_CONTEXT(USERNAME => *'EMPLOYEESEARCH_PROD'*, CONTEXT_TYPE => *SYS.DBMS_SQL_FIREWALL.IP_ADDRESS*, VALUE => *'10.0.0.0/24'*); **DBMS_SQL_FIREWALL.APPEND_ALLOW_LIST** • 取得ログ/違反ログからのアプリケーション更新に従って新規のSQL文を既存の許可リストに追加します。変更はただちに有効になります。 DBMS_SQL_FIREWALL.APPEND_ALLOW_LIST(*'EMPLOYEESEARCH_PROD'*, *SYS.DBMS_SQL_FIREWALL.CAPTURE_LOG*);
ファイアウォール・ポリシーの有効化	**DBMS_SQL_FIREWALL.ENABLE_ALLOW_LIST** • ユーザー用のSQLファイアウォール・ポリシーを有効化します。変更はただちに有効になります。実施オプション（コンテキスト/SQL文/両方）を選択し、違反のログ記録中に不一致が発生した場合にどのように応答すべきか（許可またはブロック）をSQLファイアウォールに認識させます。 DBMS_SQL_FIREWALL.ENABLE_ALLOW_LIST(USERNAME => *'EMPLOYEESEARCH_PROD'*, ENFORCE => *SYS.DBMS_SQL_FIREWALL.ENFORCE_ALL*, BLOCK => *FALSE*);
許可リストのエクスポート/インポート	**DBMS_SQL_FIREWALL.EXPORT_ALLOW_LIST/ IMPORT_ALLOW_LIST** • データベース・ユーザー用の、許可リストを含むファイアウォール・ポリシーをJSON形式でエクスポート（またはインポート）します。 DBMS_SQL_FIREWALL.EXPORT_ALLOW_LIST(USERNAME => *'EMPLOYEESEARCH_PROD'*, ALLOW_LIST => *PO*

データベース接続やSQL文の実行に不一致のシナリオが発生した場合は常に、SQLファイアウォール違反イベントが生成され、違反ログ（DBA_SQL_FIREWALL_VIOLATIONS）に書き込まれます。SQLファイアウォール・ポリシーがブロッキング・モードで有効化されている場合、クライアントはポリシーによって許可されていないアクションを試みると以下のORAエラーを受信します。

```
ORA-47605 SQL FIREWALL VIOLATION
```

SQLファイアウォール違反を監視するには、2つのオプションがあります。

1. SQLファイアウォール違反ログDBA_SQL_FIREWALL_VIOLATIONSから読み取る。
2. SQLファイアウォールの監査ポリシーを構成してデータベース・ユーザーのSQLファイアウォール違反を監査し、監査証跡UNIFIED_AUDIT_TRAILから読み取る。

```
CREATE AUDIT POLICY EMPSEARCH_APPLICATION_AUDIT_POLICY ACTIONS COMPONENT =
SQL_FIREWALL ALL ON EMPLOYEESEARCH_PROD;

AUDIT POLICY EMPSEARCH_APPLICATION_AUDIT_POLICY;
```

SQLファイアウォールを監査することにより、通常の予想されるアクセス接続パスや承認されたSQL文から外れたユーザーの異常なデータベース・アクティビティを追跡でき、コンプライアンスを示すことができます。SQLファイアウォール違反は、あらゆるコンテキスト情報と共にUNIFIED_AUDIT_TRAILに移入され、既存の監査証跡を利用することでOracle AVDFやData Safeなどのアップストリーム・アプリケーションから監視できます。

Data SafeによるSQLファイアウォールの管理

Data Safeを使用すると、複数のSQLファイアウォールを一元管理でき、以下に示すようにOracleデータベース・フリート全体でSQLファイアウォール違反を包括的に把握できます。SQLファイアウォール管理者は、Data Safeを使用してデータベース・ユーザーのSQLアクティビティを関連するデータベース接続パス（IPアドレス、OSプログラム、OSユーザー）と共に収集でき、収集の進捗状況を監視できます。Data Safeを使用すると、収集したSQLトラフィックからSQLファイアウォール・ポリシーを生成して有効化できます。Data Safeでは、違反ログを自動で収集し、コンソールからSQLファイアウォール違反を監視できます。

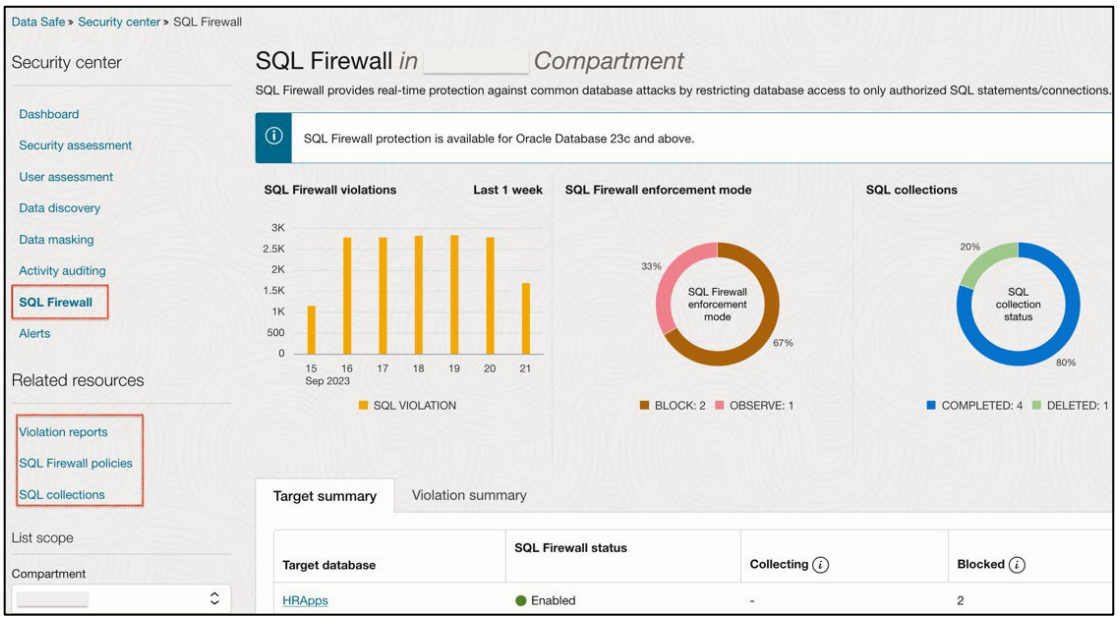

図15：Data Safe：SQLファイアウォールのダッシュボード

ダッシュボードの違反サマリーは、選択した期間にSQLファイアウォールが有効になっているコンパートメント内のすべてのターゲットからのSQLファイアウォール違反の包括的なビューを提供します。ここから違反にドリルダウンして、詳細な分析を行うことができます。SQLファイアウォールによって保護されるデータベース・ユーザーのSQL収集ステータスおよびファイアウォール・ポリシー実施ステータスのサマリーも、データベース環境全体で表示されます。ターゲットのSQLファイアウォール構成はドリルダウン時に変更できます。サンプル・アプリケーション・サービス・アカウントEMPLOYEESEARCH_PRODのSQLファイアウォールを構成するためのData Safeでのワークフローについて見てみましょう。

ここに示すように、ドロップダウン・リストからデータベース・ユーザーを選択して、そのユーザーに認可されたSQLトラフィックの収集を作成して開始します。

収集が開始したら、すべての信頼できるデータベース接続パスからデータベース・ユーザーの予想されるSQLアプリケーション・ワークロードを実行します。

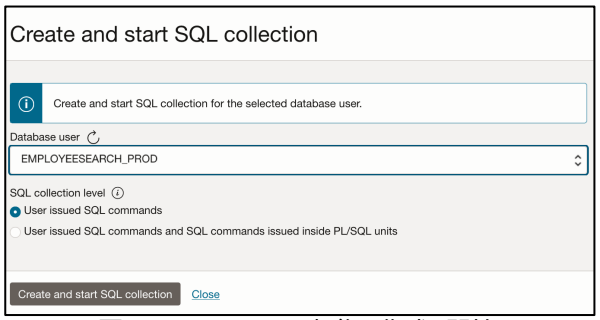

図16：Data Safe：収集の作成と開始

Data Safeでは、SQL収集インサイトを使用してSQL収集の進捗状況を監視できるため、ここに示すように、SQLファイアウォールがSQLアプリケーション・トラフィックを完全に学習したことを確認できます。
一意の新規のSQL文の数がゼロにとどまるまで収集を実行することが最善策です。セッション・コンテキスト属性を使用して、SQLファイアウォールに正常なトラフィック・パターンを学習させることもできます。確認が完了したら、収集を停止してファイアウォール・ポリシーを生成します。

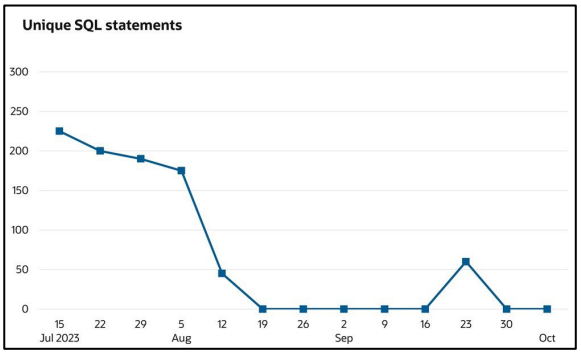

図17：Data Safe：SQL収集インサイト

ここに示すように、SQLファイアウォール・ポリシー内の許可リストの内容（許可されたコンテキストおよび許可されたSQL文）をData Safeで確認できます。
必要に応じて、許可されたコンテキストを変更して、新規のIPアドレス、OSユーザー名、およびOSプログラム名を追加できます。オフライン検証や変更管理のために、許可されたSQL文のレポートと一緒に、それらのSQL文がアクセスしたデータベース・オブジェクトのリストを生成できます

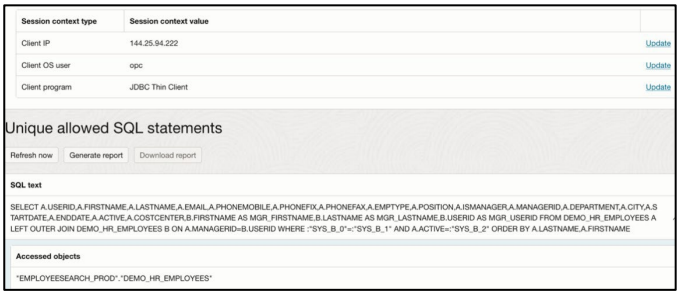

図18：Data Safe：許可リストを含むSQLファイアウォール・ポリシー

ここに示すように、Data Safeでは、実施範囲、ログ記録中のアクション（観察またはブロック）、および監査について適切な値を指定して、SQLファイアウォール・ポリシーをターゲットに対して有効化できます。

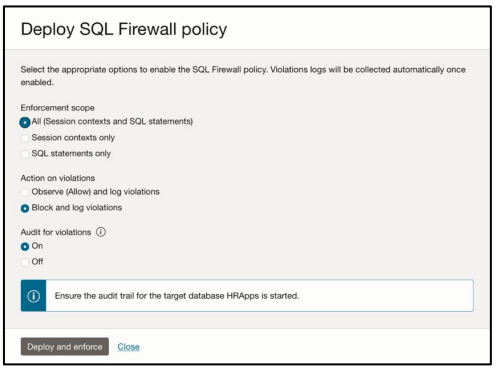

図19：Data Safe：SQLファイアウォール・ポリシーの有効化

SQLファイアウォール・ポリシーが有効化されたら、Data Safeはターゲットの違反ログから自動的に違反を収集し、それらをData Safeのリポジトリに12か月間保存します。Data Safeに保存されたSQLファイアウォール違反は、ここに示すように、データベース・フリート全体のオンライン分析およびレポート作成に使用できます。

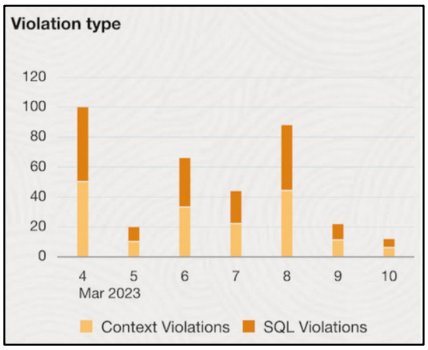

図20：Data Safe：SQLファイアウォール違反（フリート・ビュー）

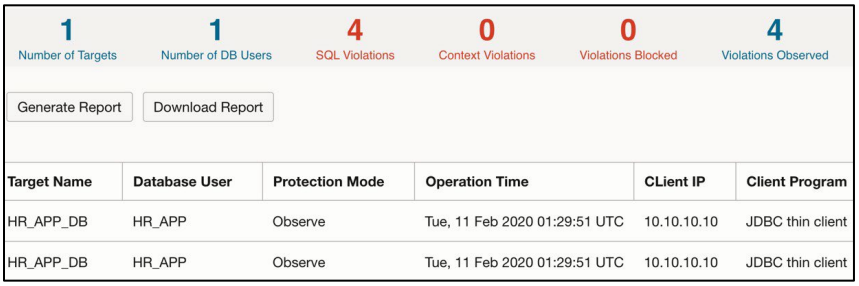

図21：Data Safe：SQLファイアウォール違反レポート

Data Safeでは、監査されたSQLファイアウォール違反にアラートを生成でき、それをさらにOCIイベントなどのより大規模なOCIエコシステムと統合することで、予防的に電子メールで通知したり、SIEMソリューションへ送信したりすることができます。アラートを利用したい場合は、SQLファイアウォール・ポリシーを有効化する際に必ず監査機能をオンにし、ターゲットに対する統合型監査証跡を開始して、監査された違反をData Safeが収集するようにしてください。SQLファイアウォール違反アラート・ポリシーをターゲットに関連付けます。

以下に示すサンプルOCI電子メール通知は、セキュリティ管理者に潜在的なSQLインジェクションの試行を予防的に通知するもので、違反の原因となったクライアント接続やSQLコマンドなどの関連するコンテキストの詳細がすべて含まれています。

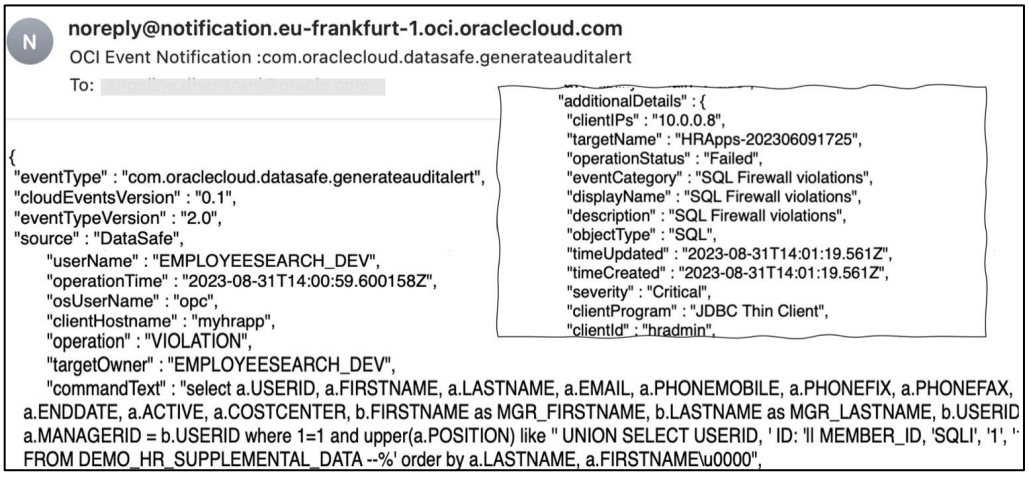

図22：Data Safe：潜在的なSQLインジェクション試行時のサンプル電子メール通知

どちらを使用するかを決定：Database FirewallかSQLファイアウォールか

Database FirewallはネットワークベースのSQLファイアウォールで、Oracle Databaseおよびそれ以外のデータベースの SQLトラフィックを監視できます。サポートされているすべてのバージョンのOracle Database全体で機能します。Oracle Database以外のデータベースや23cより前のOracle Databaseでは、Oracle AVDFのDatabase Firewallが唯一の選択肢です。Oracle Database 23c以降では、2つのオプションのいずれかに決定する場合に、以下の複数の要素を考慮することをお勧めします。

- **パフォーマンスへの影響：**ネットワークベースのDatabase Firewallは、データベース・サーバーのパフォーマンスに影響しません。すべての作業をDatabase Firewallマシン上においてサーバー外で実行するため、RAMも追加のCPUも消費しません。ほとんどのデプロイメント・モードでは、Database Firewallによってパフォーマンス・オーバーヘッドは発生しません。プロキシ・モードでは、Database Firewallによって追加のネットワーク待機時間がわずかに発生します。待機時間の程度は、おもにネットワーク上のDatabase Firewallの位置によって制御されます。SQLファイアウォールによって明らかな待機時間は発生しませんが、1 %～1.5 %を超えない最小限のCPUオーバーヘッドが生じます。
- **デプロイメント・オプション：**Database Firewallは、専用の仮想マシンまたはハードウェア（データベース・サーバーから分離）にデプロイされます。Database Firewallには、プロキシ、ホスト監視、帯域外という複数のデプロイメント・オプションがあります。プロキシは、ブロッキングのユースケースをサポートする唯一のインライン構成ですが、プロキシを使用するにはクライアント側の接続を変更してトラフィックがプロキシ経由でルーティングされるようにする必要があります。SQLファイアウォールはデータベースの一部のため、クライアント側の変更は必要ありません。SQLファイアウォールは、ブロッキングがおもなユースケースであるデプロイメントや、クライアント側の構成を変更することが困難だったり望ましくなかったりする場合に最適なソリューションです。
- **検査の範囲：**Database Firewallは、ネットワーク経由のSQLトラフィックのみを監視できます。ローカルBEQ接続経由のSQLトラフィックは可視化されず、内部のジョブやストアド・プロシージャの実行は認識されません。SQLファイアウォールはデータベースの内部で稼働し、発信元に関係なくすべてのトラフィックを検査します。
- **暗号化されたトラフィックの処理：**暗号化されたSQLトラフィックの処理には、Database Firewallでの追加の構成と処理が必要ですが、SQLファイアウォールへの到達時までにトラフィックはすでに復号化されているため、SQLファイアウォールでの処理はシームレスで単純です。
- **ブロッキングの中断：**ネットワーク上で（Database Firewallを使用して）SQLをブロックすると、各操作はスタンドアロン文として個々に処理されるため、トランザクションが中断される可能性があります。対照的に、SQLファイアウォールはデータベース・トランザクションを把握し、原子性、一貫性、独立性、および永続性を備えています。
- **高可用性：**Database Firewallの高可用性は、クライアントがクライアント接続パラメータに基づいて接続を分散/フェイルオーバーするか、またはサード・パーティのロードバランサを使用することで、冗長なファイアウォールによって提供されます。SQLファイアウォールはOracle Databaseの一部で、Oracle Real Application ClustersやOracle Data Guardなどの高可用性アーキテクチャを利用します。
- **職務の分離：**Database Firewallは、データベース管理者による入力や制御なしでデータベース・トラフィックを監視できます。SQLファイアウォールはOracle Databaseの一部で、データベース管理者と協力してデプロイする必要があります。

まとめ

SQLインジェクションは、データ主導型Webアプリケーションにとってもっとも一般的なデータベース攻撃パターンです。Oracle Databaseに対するリスクを軽減するには、Oracle AVDFのDatabase FirewallまたはOracle DatabaseのSQLファイアウォールを利用します。どちらも、ほとんどのネットワーク・ファイアウォール・ソリューションに一般的に使用されているヒューリスティックな正規表現のパターン・マッチングに依存しません。代わりに、実際のSQLシグネチャを利用してSQL文の許可されたリストを構築します。許可されたSQLをセッション・コンテキストと組み合わせて正常なアプリケーションSQLトラフィックを学習し、リアルタイムで違反を検出してアラート生成またはブロックします。

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