ORACLE

Oracle Database Security Assessment Tool FAQ

ビジネスの機密データと規制対象データを保護することは不可欠です。しかしながらほとんどの組織が、データベースはセキュアに構成されているのか、どのようなユーザーがそのデータベースにアクセスできるのか、また機密データはどこに保存されているのかを把握しきれずにいます。オラクルの多層防御機能の一部であるOracle Database Security Assessment Tool（Oracle DBSAT）は、データベースの構成、運用、実装の領域でリスクを招く恐れがある部分を特定し、リスクを低減するために必要な変更内容と制御方法を提案します。

全般

Oracle Database Security Assessment Tool（Oracle DBSAT）にはおもにどのようなユースケースがありますか。

中心となるユースケースが3つ存在します。データベースがどの程度セキュアに構成されているかを評価し、どのようなユーザーがデータベースにアクセスでき、それらのユーザーはどのような権限を有しているかを判断し、機密データがデータベースのどこに保存されているかを特定します。

Oracle DBSATはどのような仕組みになっていますか。

Oracle DBSATには、Collector、Reporter、Discovererという3つのコンポーネントがあります。Collectorは、すべての関連データをデータベースから収集し、その後Reporterがそのデータを分析し、セキュリティ評価レポートを作成します。Discovererは、データベース内のさまざまな種類の機密データを特定し、機密データ評価レポートを作成するスタンドアロン・モジュールです。

どのような種類のデータが収集および分析されますか。

Oracle DBSATは、以下のカテゴリのデータを収集してレポートを作成します。

- ユーザー・アカウント、特権およびロール
- 認可制御
- ファイングレイン・アクセス制御
- 監査ポリシー
- データ暗号化
- データベース構成
- リスナー構成
- 関連のオペレーティング・システム構成

Oracle DBSAT Discovererは、データベース内の機密データの種類と量を検出するために、列名と列コメントでパターンマッチングを行い、以下のように機密データを分類します。

- 識別情報
- 出自情報
- IT情報
- 財務情報
- 健康情報
- 職歴情報
- 学歴情報

機密データのカテゴリをカスタマイズして、さまざまな要件に対応することができます。

Oracle DBSATを実行すると、パフォーマンスにどのような影響がありますか。

データベースのパフォーマンスに及ぼす影響は、無視できる程度です。Oracle DBSAT CollectorおよびDiscovererは、データベース構成ファイルとオラクルのデータ・ディクショナリ・ビューからのみデータを収集します。アプリケーション・データは参照しません。

Oracle DBSATの実行方法とデータの分析方法を学ぶにはどれほどの時間を要しますか。

Oracle DBSAT自体は、非常に簡単に使用できるコマンドライン・ツールです。ツールの使用方法は、数分で学ぶことができます。わずか10分ほどでインストールからレポート作成まで進むことができます。数千のデータベース・ユーザーが含まれるデータベースは、分析時間が長くなる可能性があります。

クラウドにデプロイされているデータベースでOracle DBSATを実行できますか。

データベースがオンプレミスで実行されているか、Autonomous Databaseで実行されているか、お客様が管理するDatabase Cloud Services（DBCS）で実行されているか、もしくはIaaSにデプロイされたデータベースであるかにかかわらず、Oracle DBSATを使用できます。ただし、他の前提条件が存在するので、ドキュメントを参照してください。複数のデータベースを対象とするサービスとして評価を実行し、ベースライン設定、ずれ、比較、履歴、アラートなどのエンタープライズ機能を利用したい場合は、Data Safeを参照してください。Oracle Data Safeは、セキュリティおよびユーザーの評価機能を提供します。

Autonomous Databaseで実行できますか。

はい。Oracle DBSATは、Oracle Autonomous Data Warehouse Cloud（Oracle ADW）とOracle Autonomous Transaction Processing（Oracle ATP）のデータベースのサーバーレス、専用、またはCloud at Customerデプロイメント・モデルで動作が保証されています。Oracle Autonomous JSON Database（Oracle AJD）での動作も保証されています。

Oracle DBSATではデータベースのタイプに応じて異なる推奨事項が提示されますか。

はい。Oracle DBSATはターゲットの種類を特定し、データベースがオンプレミスで実行されているか、クラウド内で実行されているかの詳細なチェックを実行します。Oracle DBSATは、オンプレミス・データベース、さまざまなAutonomous Database、Base Database Serviceを識別します。これらのターゲットの種類では、該当する場合に、具体的な推奨事項が提示されます。

DBSATコレクタおよびレポータ

Oracle DBSAT Collectorはどのようにして実行できますか。

Collectorは、Oracle Databaseで次のように入力して起動します。

$ dbsat collect <connect_string> <dest-file>

connect_stringは、ターゲット・データベースへの接続文字列です。

dest-fileは、Collectorによって作成される出力ファイルの、拡張子を除いたファイル名です。

以下に、コマンドの例を示します。

$ dbsat collect dbsatusr@orcl dbdata

Oracle DBSAT Collectorはデータベース構成とオペレーティング・システム構成の両方を分析するため、データベース・サーバーが稼働しているホストと同じホストから実行することが推奨されます。

レポートを取得するには、Oracle DBSAT Reporterを実行する必要があります（以下を参照）。

Oracle DBSAT Reporterはどのようにして実行できますか。

Oracle DBSAT Reporterは、Java Runtime Environment（JRE）1.8（jdk8-u172）以降がインストールされているデスクトップやラップトップを含む任意のシステムで実行できます。

$ dbsat report <dest-file>

dest-fileは、Collectorが生成するJSON/zipファイルの（ファイル拡張子を除いた）名前です。Oracle DBSAT Reporterによって作成されるすべてのレポート・ファイルのベースとして同じパス名が使用され、レポート形式（テキスト、HTML、JSON、およびXLS）に該当する接尾辞がそのパス名に付加されます。たとえば、次のように指定します。

$ dbsat report dbdata

評価結果とは何ですか。

Oracle DBSAT Reporterの出力として、複数の評価結果で構成されるデータベース・セキュリティ評価レポートが作成されます。それぞれの評価結果には、データベースのセキュリティ状況を改善するための推奨事項と、さらに詳しく分析を行うための情報が含まれます。また、Oracle DatabaseのSTIGルールとCISベンチマークの推奨事項、EU GDPRの条項/備考の該当部分への参照も必要に応じて含まれます。Oracle DBSATでは、CIS、STIG、またはGDPRのコンプライアンスを調査している場合でも、すべての顧客が従うべきベスト・プラクティスである評価結果の場合、その評価結果をOracle Best Practice（OBP）としてもマークします。

特定の評価結果を抽出すること、複数のレポートを比較すること、複数のデータベースの集約レポートを作成することはできますか。

Oracle DBSAT Reporterでは、JSON形式でレポートが提供されるため、評価結果をさらに処理できます。

Oracle DBSATユーティリティをダウンロードして詳しく分析することもできます。Oracle DBSATユーティリティはPythonで記述された2つのサンプル・プログラムで、評価結果の抽出と2つのJSONレポートの比較ができます。Oracle DBSATユーティリティは、My Oracle Supportからダウンロードできます。

このほか、Oracle Data Safeを利用することも可能です。Data Safeは、ユーザーとセキュリティの評価を含む、包括的なセキュリティ機能セットを提供するデータベース・セキュリティのクラウド・サービスです。Oracle Data Safeのエンタープライズグレードの評価機能では、スケジュールに基づく評価の実行、複数のデータベース評価の実行、セキュリティ・ベースラインの確立、そのベースラインと現在の評価実行のずれを表した比較レポートの取得が可能です。Oracle Data Safeイベント、およびOCIイベントと通知を活用することにより、ずれが生じた際にアラートを受信し、それらのアラートを他のシステムに統合することができます。Oracle Data Safeについて詳しくは、https://www.oracle.com/jp/security/database-security/data-safe/を参照してください。

Oracle Audit Vault and Database Firewall（Oracle AVDF）20.9では、データベース・セキュリティ状況管理が導入されました。Oracle AVDFでは、監査レコードの収集や、監査ポリシー、レポート、およびアラートのプロビジョニングへの対応に加えて、Oracle Database向けのOracle DBSATを統合することによって、エンタープライズには一元化されたセキュリティ評価ソリューションが提供されるようになりました。コンプライアンス・マッピングや推奨事項を備えたフル機能の評価により、組織はすべてのOracle Databaseのセキュリティ状況を一元的に把握できます。Oracle Audit Vault and Database Firewallについて詳しくは、https://www.oracle.com/jp/security/database-security/audit-vault- database-firewall/を参照してください。

Oracle DBSAT Collectorはマルチテナントのプラガブル・データベースで実行できますか。

はい。ただし、Oracle DBSATをルート・コンテナと各PDBで別々に実行する必要があります。

独自のカスタム・セキュリティ評価ルールを追加できますか。

いいえ、Oracle DBSATは、お客様に速やかに価値を提供する迅速で使いやすいツールとして構築されました。Oracle DBSATは、Oracle Database Securityベスト・プラクティスのルールとともに出荷され、必要に応じて、Oracle Database STIGルール、CISベンチマークの推奨事項と関連のEU GDPR条項/備考を提案します。My Oracle Supportへ機能強化リクエストを提出することをお勧めします。オラクルでは、すべての機能強化リクエストについて、新しいルールに追加するかどうかを確認して評価します。Oracle DBSATは、お客様による検出ルール/構成の作成または変更をサポートします。

DBSAT Discoverer

Oracle DBSAT Discovererはどのような仕組みになっていますか。

Oracle DBSAT Discovererは、構成ファイル、機密データの種類を表す1つまたは複数のパターン・ファイル、および列名と列コメントの検索用の正規表現を使用します。Oracle DBSAT Discovererでは、データへのクエリーは実行されず、列名と列コメントに関連付けられたメタデータのみにクエリーが実行されます。

たとえば、“名前”を検索するには、以下を使用できます。

```
[FIRST NAME]
COL_NAME_PATTERN = (^|[_-])(FNAME|(FIRST|GIVEN).*(NAME|NM)|FORE.?(NAME|NM))($|[_-])
COL_COMMENT_PATTERN = (FIRST|GIVEN) NAME|FORENAME
SENSITIVE_CATEGORY = Identification Info - Public IDs
```

Oracle DBSATには、初期構成とパターン・ファイルが付属していますが、お客様がカスタムの機密タイプやカテゴリ/サブカテゴリを追加することも可能です。

より徹底的に機密データの特定に取り組む場合は、Oracle Data Safe Sensitive Data Discoveryを確認することをお勧めします。Data Safeでは、列名と列コメントの分析に加えてデータ自体を検証することで、機密情報をより正確に特定できます。

どのような種類の正規表現が使用されますか。

Oracle DBSAT Discovererでは、拡張正規表現（ERE）をサポートしています。この構文はIEEEによって標準化されており、Javaで一般的に使用されています。

たとえば、(^JOB.*(TITLE|PROFILE|POSITION)$)|^POSITIONは、JOBで始まり（^JOB）、任意の文字（.）がゼロ個以上（*）続き、TITLE、PROFILE、またはPOSITIONで終わる（$）文字列と一致します。または（|）、POSITIONで始まる（^）文字列と一致します。

パターン一致規則はどの程度正確ですか。誤判定をどのように処理したらよいですか。

Oracle DBSATで提供されるルールは、誤判定を減らすために作成されました。しかしながら、Oracle DBSATは列名と列コメントのみを検査するため、誤判定を生成する場合があります。誤判定を減らす1つの方法として、パターン・ファイルを編集し、正規表現を特定のデータ・モデルに合わせて調整する方法が挙げられます。また、除外リスト・ファイルを使用して、スキーマ、表、列を検索対象から除外する方法もあります。CSVレポートには、列の完全な修飾名が含まれるため（Schema.Table.Column）、それらをCSVレポートから除外リスト・ファイルにコピー/ペーストすることで、容易に誤判定を排除できます。

英語以外の言語のデータ・モデルでも、Oracle DBSATで機密データを検索できますか。

Oracle DBSATには、英語で記述された列名とコメントを検索するパターン・ファイルが付属しているほか、オランダ語、フランス語、ドイツ語、ギリシャ語、イタリア語、ポルトガル語、スペイン語に対応したパターン・ファイルのサンプルも付属しています。これにより、英語以外で記述されたデータ・モデルでも機密データの検出を迅速に開始できます。独自のパターン・ファイルを最初から作成するか、または既存のパターン・ファイルをコピーして要件に適応させることができます。

Oracle DBSAT Discovererはどのように実行できますか。

Oracle DBSAT Discovererは、Java Runtime Environment（JRE）1.8（jdk8-u172）以降が実行されているラップトップを含む任意のマシンで実行できます。データベース・サーバーと同じサーバーで実行する必要はありません。

$ dbsat discover –c <config file> <dest-file>

例：

$ dbsat discover –c Discoverer/conf/dbsat.config dbdata

Oracle DBSAT Discovererを実行する前に、Oracle DBSAT Collectorを実行する必要がありますか。

いいえ。Oracle DBSAT Discovererはスタンドアロン・コンポーネントです。Oracle DBSAT CollectorやReporterへの依存性はありません。Oracle DBSAT Collectorを実行するかスキップするかを選択できます。

セキュリティに関する考慮事項

データベースに接続してデータを収集するには、どのような権限が必要ですか。

オラクルの提供するDBAロールを有するデータベース・ユーザー・アカウントには、必要な権限が備わっていますが、最小権限の原則に従うべきです。Oracle DBSATを実行するために必要な最小権限については、ドキュメントを参照してください。さらに、Oracle DBSAT Collectorを実行するOSユーザーには、ORACLE_HOMEおよびTNS_ADMINディレクトリとファイルの読取り権限が必要です。

Oracle DBSATでは、収集された構成データと生成されたレポートをどのように保護しますか。

デフォルトでは、インストール済みのzip/unzipを使用して、Oracle DBSAT出力ファイルが圧縮され、パスワードで保護されます。出力ファイルにはデータベースに関する機密情報が含まれるため、すべての出力ファイルを常に暗号化することを強く推奨します。

本番データベースでOracle DBSATを実行すると、セキュリティ上どのようなリスクがありますか。

Oracle DBSATは構成とメタデータのみを読み取るため、リスクは最小限です。Oracle DBSATによって実行されるすべてのデータベース・アクションは読み取り専用です。

Oracle DBSATは、最小権限で実行して分析に必要なデータを収集することができます。一般的な診断ツールを実行して、コレクタの実行中にOracle DBSATがどのような操作を実行するかを検証できます。Oracle DBSAT Collectorの出力データ（JSON形式）を調べ、どのようなデータが収集されたかを確認することもできます。Oracle DBSATが生成したレポートにはアクセス制限を加える必要があり、Oracle DBSATを実行するために作成されたデータベース・ユーザー・アカウントは使用後に削除またはロックする必要があります。

ダウンロードとインストール

Oracle DBSATはどこでダウンロードできますか。

Oracle DBSATはMy Oracle SupportのDoc ID 2138254.1からダウンロードできます。

Oracle DBSATをインストールするにはどうすればよいですか。

Oracle DBSATはzipファイルとして提供されます。ファイルを解凍するだけです。

$ unzip dbsat.zip –d <directory>

Oracle Databaseのどのバージョンがサポートされていますか。

Oracle DBSATでは、Oracle Database 11.2.0.4から23cまでのリリースがサポートされています。

どのプラットフォームがサポートされていますか。

Oracle DBSATは以下のプラットフォームで実行されます。

- Solaris x64およびSolaris SPARC
- Linux x86-64およびLinux 64ビットARM
- Windows x64
- HP-UX IA（64ビット）
- IBM AIX（64ビット）およびLinux on zSeries（64ビット）

Oracle DBSATは、サポートされるほとんどのOracle Databaseプラットフォームで実行できます。ただし、現在のところOracle DBSAT Collectorは、Windowsプラットフォームで実行されるデータベース・サーバーからはOSデータを収集しません。またリモートで実行した場合もOSデータは収集されません。Unix/Linuxシステムではbashシェルでの実行が必要です。bashシェルが使用できない場合は、インストールするか、bashシェルを搭載したサーバーからリモートでコレクタを実行してください。

Oracle Sales Consulting（SC）、Oracle Consulting Services（OCS）、Oracle Advanced Customer Services（ACS）、または Oracle Customer Success Services（OCSS）が自分の代わりにOracle DBSATをダウンロードして実行することはできますか。

ご自身でOracle DBSATをダウンロードして実行することを推奨します。評価の範囲に応じて、Oracle Sales Consulting、Oracle Consulting Services、またはOracle Advanced Customer Servicesの組織が、Oracle Databaseセキュリティ評価プログラムの実行、データの分析、および修復ステップの優先順位付けを、お客様の環境を考慮に入れてお手伝いします。さらに、Oracle DBSATレポートを補完するためのインタビューを現場で行うことで、お客様をサポートしてデータベース・セキュリティ状況への洞察を深めることができるよう支援します。適切なセキュリティ評価では、技術分析と組織の特性、広範なITエコシステム、導入されているプロセス、規制遵守要件が考慮されます。

製品ライセンスとサポート

Oracle DBSATはどのように配布されていますか。

このツールは、My Oracle Support（MOS）アカウントをお持ちのオラクルのお客様（アクティブなサポート契約のある方）が追加費用なしでダウンロードできます。

Oracle DBSATのバグ報告や改善リクエストはどのように行うことができますか。

MOSポータルを使用して、Oracle DBSATのサービス・リクエスト（SR）を送信してください。

Oracle DBSATのバグ修正はどのように入手できますか。

Oracle DBSATでは、機能拡張とバグ修正を含むアップデートを四半期に1度作成する予定です。そのため、最新リリースがあるかどうかMy Oracle Supportで常に確認することを強くお勧めします。

Oracle DBSATとData Safe

Oracle DBSATとData Safeはどのように関連していますか。

Data Safeは、包括的なセキュリティ機能一式を提供するデータベース・セキュリティのクラウド・サービスです。セキュリティ評価、ユーザー評価、アクティビティ監査、SQL Firewall、機密データの検出、データ・マスキングなどの機能があり、クラウド内またはオンプレミスで実行されるデータベースで動作します。

Oracle DBSATは少数のデータベースについての現在のセキュリティ状態を評価する上で、非常に優れています。Data Safeは、エンタープライズレベルの要件に対応します。Data Safeでは以下の操作を実行できます。

- スケジュール設定した定期的な評価の実行
- データベース・セキュリティのベースラインの設定
- ベースラインとのずれを示した比較レポートの表示
- アラートの受信
- すべての評価実行履歴の表示
- ユーザー評価機能を使用したユーザー・リスクに関するインサイトの提示
- 本番環境以外でのデータ匿名化を要求する企業要件または規制要件への対応、データベース・アクティビティの監視、データベース・セキュリティ状況の評価、機密データの検出を1つの統合コンソールで実行

Oracle Data Safeについて詳しくは、https://www.oracle.com/jp/security/database-security/data-safe/を参照してください。

Oracle DBSATとAudit Vault and Database Firewall

Oracle Audit Vault and Database Firewall（Oracle AVDF）はソフトウェア・アプライアンスで、オンプレミスにデプロイするか、またはMarketplaceイメージを使用してOracle Cloud Infrastructureにデプロイすることができます。Oracle AVDF 20.9にはデータベース・セキュリティ状況管理が導入され、Oracle Database向けの一般的なDatabase Security Assessment Toolを統合することによって、エンタープライズ向けの一元化されたセキュリティ評価ソリューションを提供するようになりました。コンプライアンス・マッピングや推奨事項を備えたフル機能の評価により、組織はすべてのOracle Databaseのセキュリティ状況を一元的に把握できます。Audit Vault and Database Firewallを使用すると、以下が可能になります。

- データベース・セキュリティのベースラインの設定
- ベースラインとのずれを示した比較レポートの表示
- ユーザー・エンタイトルメントに関するインサイトの提示
- データベース・アクティビティの監視を要求する企業要件または規制要件への対応、データベース・セキュリティ状況の評価、SQLインジェクション攻撃の防止

Oracle Audit Vault and Database Firewallについて詳しくは、https://www.oracle.com/jp/security/database-security/audit-vault-database-firewall/を参照してください。

ORACLE

詳細情報

Oracle DBSATに関する詳細情報はどこで入手できますか。

oracle.comのOracle DBSATのページを参照してください。

Oracle Databaseセキュリティ評価プログラムについての詳細情報はどこで入手できますか。

世界中の複数のオラクル・チームが、独自のOracle Databaseセキュリティ評価プログラムを作成しています。詳しくは、オラクルの営業担当者にお問い合わせください。

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