ORACLE Database

Oracle Database Security Assessment Tool

データ侵害が日々増え続け、データ保護やプライバシーに関する一連の規制が進化し続けている中で、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、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、また機密の個人データはどこに保存されているのかを、ほとんどの組織が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（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、リスクを緩和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（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。

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。

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

ORACLE

- 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

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

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。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。

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。

クラウドにデプロイされているデータベースで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、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、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。

Oracle Autonomous Databaseで実行できますか。

はい。DBSATはOracle Autonomous Data Warehouse Cloud（Oracle ADW）とOracle Autonomous Transaction Processing（Oracle ATP）での動作が保証されています。

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に対して次のように起動します。

```
$ dbsat collect <connect_string> <dest-file>
```

`connect_string`は、ターゲット・データベースに接続するために必要な接続文字列です。

`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。

例：`$ dbsat collect dbsatusr@orcl dbdata`

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。リモートから実行すると、オペレーティング・システムのチェックなど、一部のチェックが省略されます。

Oracle DBSATレポータはどのようにして実行できますか。

DBSAT Reporterは、Python 2.6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によって生成されるJSON/zipファイルの（ファイル拡張子を除いた）名前です。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。

例：`$ dbsat report dbdata`

分析結果とは何ですか。

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。評価結果には、データベースのセキュリティ態勢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が必要に応じて含まれます。

評価結果のみを抽出して複数のレポートを比較することや、複数のデータベースからの集約レポートを結合することはできますか。

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。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。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。DBSAT utilsはMy Oracle Supportからダウンロードできます。

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、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。

独自のカスタム評価ルールを追加できますか。

DBSATの設計センターは、もっとも一般的な問題に対処した、簡易で使いやすいツールです。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。オラクルは、すべての改善リクエストを確認し、将来的なリリースに組み込むことを検討する予定です。

DBSAT Discoverer

DBSAT Discovererはどのような仕組みになっていますか。

DBSAT Discovererは、構成ファイルのほか、機密データの種類を表す1つまたは複数のパターン・ファイルと、列名と列コメントの検索に使用される正規表現を使用します。

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
```

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。

どのような種類の正規表現が使用されますか。

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。

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、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、正規表現を自身のアプリケーション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/ペーストするだけで、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、DBSATで機密データを検索できますか。

はい。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、ヨーロッパの主要言語（オランダ語、フランス語、ドイツ語、イタリア語、ポルトガル語、スペイン語など）に対応したパターン・ファイルも付属しています。

DBSAT Discovererに独自の機密タイプまたはカテゴリを追加できますか。

はい、できます。パターン・ファイルをコピーし、機密タイプ、カテゴリ、および列名と列コメントを検索するための正規表現を追加してください。また、新たなカテゴリは、リスク・レベルとともに構成ファイルに追加する必要があります。有効なリスク・レベルは、Low Risk、Medium Risk、High Riskです。

DBSAT Discovererはどのように実行できますか。

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 config dbdata`

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

いいえ。DBSAT Discovererはスタンドアロン・コンポーネントです。DBSAT CollectorやReporterへの依存性はありません。

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。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。DBSAT Collectorを実行するOSユーザーには、ORACLE_HOMEディレクトリとファイルを読み取ることができる権限が必要です。

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、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。

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。データを収集するDBSAT CollectorのSQLスクリプトをレビューし、実行される処理を確認することができます。DBSAT Collectorの出力データ（JSON形式）を調べ、実際にどのようなデータが収集されているかを確認することもできます。
DBSATが生成したレポートへのアクセスは、制限される必要があります。

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。

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 10.2.0.5から19c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
- Windows x64
- HP-UX IA（64ビット）
- IBM AIXおよびzSeriesベースのLinux

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。

Oracle Sales Consulting（SC）、Oracle Consulting Services、またはAdvanced Customer Services（ACS）が自分の代わりに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DBSATをダウンロードして実行することを推奨します。オラクルのコンサルタントは、データベース・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、お客様の組織の環境を考慮に入れてお手伝いします。さらに、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、お客様がデータベース・セキュリティ態勢への洞察を深めることができるよう支援します。このように、DBSATは最大の価値を提供します。適切なセキュリティ評価では、組織の特性、広範なITシステム、導入されているプロセス、対処すべき規制などが考慮されます。

製品ライセンスとサポート

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がダウンロードできます。

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、DBSATのサービス・リクエスト（SR）を送信してください。

DBSATのバグ修正はどのように入手できますか。

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。最新リリースがあるかどうか常に確認することを強くお勧めします。

その他の情報

Oracle DBSATに関する詳細情報はどこで入手できますか。

oracle.comのページを参照してください。

データベース・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、独自のデータベース・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
Database

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/oracle facebook.com/oracle twitter.com/oracle

Integrated Cloud Applications & Platform Services

ORACLE

Oracle is committed to developing practices and products that help protect the environment