

Oracle Database Security Assessment Tool 紹介

日本オラクル株式会社

データベースセキュリティ情報の紹介

今さら？ 今こそ！ データベースセキュリティ

<http://www.atmarkit.co.jp/ait/series/6445/>

@IT > 今さら？ 今こそ！ データベースセキュリティ

今さら？ 今こそ！ データベースセキュリティ

本連載では、データベースセキュリティの「考え方」と「必要な対策」をおさらいし、Oracle Databaseを軸にした「具体的な実装方法」や「Tips」を紹介していきます。



いいね! 0 シェア ツイート B!ブックマーク 0 G+



今さら？ 今こそ！ データベースセキュリティ (2) :

なぜ、データベースセキュリティが必要か——企業の対策率「たった20%」の現状

本連載では、データベースセキュリティの「考え方」と「必要な対策」をおさらいし、Oracle Databaseを軸にした「具体的な実装方法」や「Tips」を紹介していきます。今回は、あらためて「なぜ、データベースセキュリティが必要なのか」を説明します。

【福田知彦，日本オラクル株式会社】(2017年6月29日)



今さら？ 今こそ！ データベースセキュリティ (1) :

なぜ、今「データベースセキュリティ」なのか——安全なデータベースに必要な「5つ」の基本

本連載では、データベースセキュリティの「考え方」と「必要な対策」をおさらいし、Oracle Databaseを軸にした「具体的な実装方法」や「Tips」を紹介していきます。初回は、「データベースセキュリティの基本的な考え方」を解説します。

データベースセキュリティナビ

<https://blogs.oracle.com/sec/>



データベース・セキュリティナビ



Oracle Databaseのセキュリティパッチ

オラクルではセキュリティ修正を含む累積パッチを四半期ごとにCritical Patch Updateとして定期的に提供しています。脆弱性をついた攻撃が発生したときには、これとは別に緊急の個別パッチがでることもありますが、基本的には四半期ごとの累積パッチを適用することで既知の脆弱性への対策ができていく最新の状態を保つことができます。最近のコンプライアンス要件でも、ソフトウェアを最新の状態に保つことが求められています。「個人情報の保護に関する法律についてのガイドライン(通則編)」では、講じなければならない措置として「(3) 外部からの不正アクセス等の防止」があり、実現のための手法として「機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする」とあります。「PCI DSS」では、「要件: 6.2」で「すべてのシステムコンポーネントとソフトウェアに、ベンダ提供のセキュリティパッチがインストールされ、既知の脆弱性から保護されている。重要なセキュリティパッチは、リリース後1カ月以内にインストールする」とあります。また...

Thursday, July 13, 2017 | DBSec | [Read More](#)

オラクル・セキュリティお客様活用事例 (データベース・セキュリティ)

顧客事例/ニュースリリースとして発表させていただいたお客様及びメディア掲載いただいたお客様の事例をご紹介します(五十音順)。SBIトレードウィンデック(Advanced Security, Database Vault and Database Firewall)事例(PDF) エディオン(Advanced Security)事例(PDF) 性能向上は当然、コストも大幅削減、エディオンが「約1200店舗の業務をリアルタイムにサステナブルデータベース基

以下の事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント(確約)するものではないため、購買決定を行う際の判断材料になさらないで下さい。

オラクル製品に関して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。

Oracleは、米国オラクル・コーポレーション及びその子会社、関連会社の米国及びその他の国における登録商標または商標です。他社名又は製品名は、それぞれ各社の商標である場合があります。

データベース管理者の悩み

情報漏えい事件はなくならないし、法律やコンプライアンス要件もいろいろあるけれども。。



データベースは安全に構成されている？
重要なデータはどこにある？
重要なデータに誰がアクセスできる？
どんなセキュリティ設定やポリシーがある？

データベースセキュリティ担当者はいる？
何がセキュリティホールか知っている？
まずやらなきゃいけないことは何？
どんなスキルが必要？

そこで

Oracle Database Security Assessment Tool

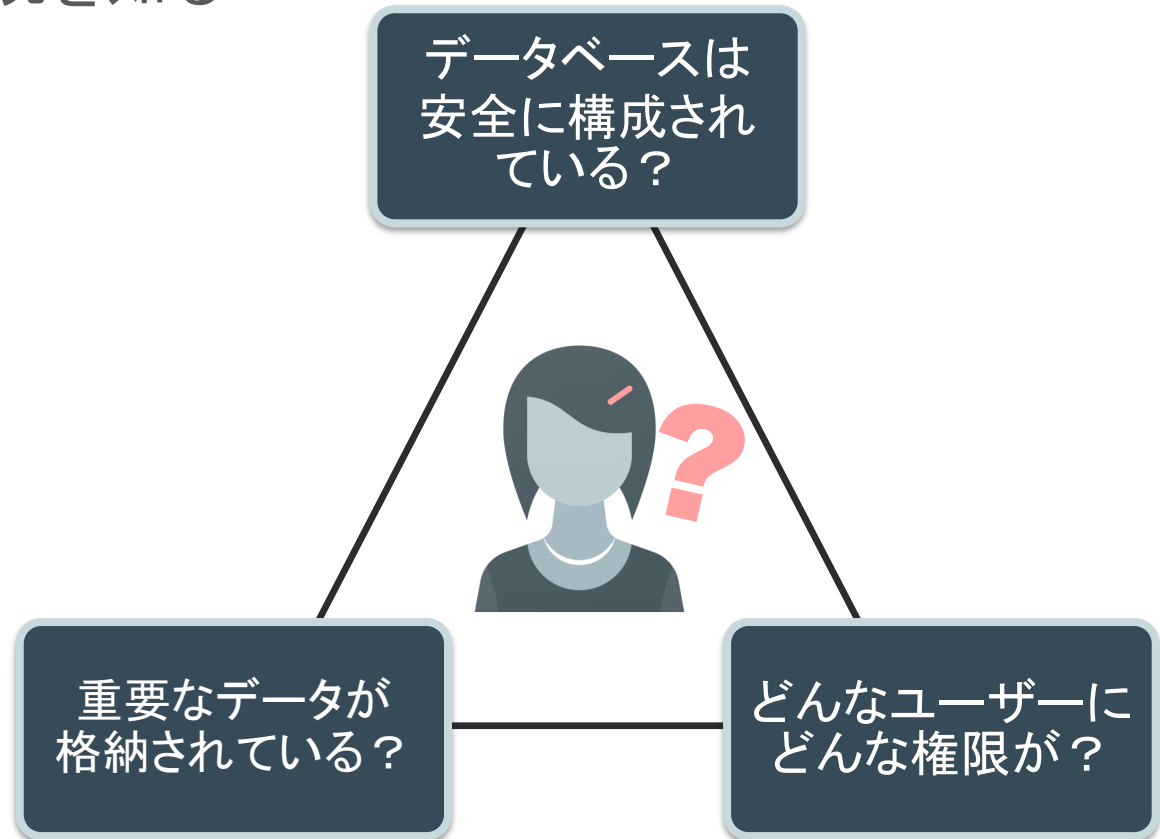
2018年1月 Version 2.0.1 公開

Oracle Database Security Assessment Tool (DBSAT)

攻撃者より先にデータベースのセキュリティ状況を知る

- データベースが安全(でない)ことを見える化
 - セキュリティ状況概要レポート
 - ユーザー、権限付与状況、リスクを理解
 - 重要なデータをリスト化
- すぐに使えるアセスメントレポート
 - 概要および詳細情報
 - 優先順位付けられた推奨事項
 - EU GDPRやCIS Benchmark(*)とのマッピング
- すぐに簡単に実行できる独立型のツール
- すべてのオラクルユーザーが**無料**で利用可能

DBSAT2.0
新機能



(*) CIS(Center for Internet Security)が作成した
安全なOracle Database構成のベストプラクティス

DBSATの確認項目

1. セキュリティ構成状況

- データの暗号化
- 監査ポリシー
- ファイングレインアクセスコントロール
- データベースとリスナーの構成
- OSファイルパーミッション
- セキュリティパッチ

2. ユーザーと権限

- ユーザーアカウント、権限、ロール

3. 重要なデータ

DBSAT2.0
新機能

- 種類、場所、数

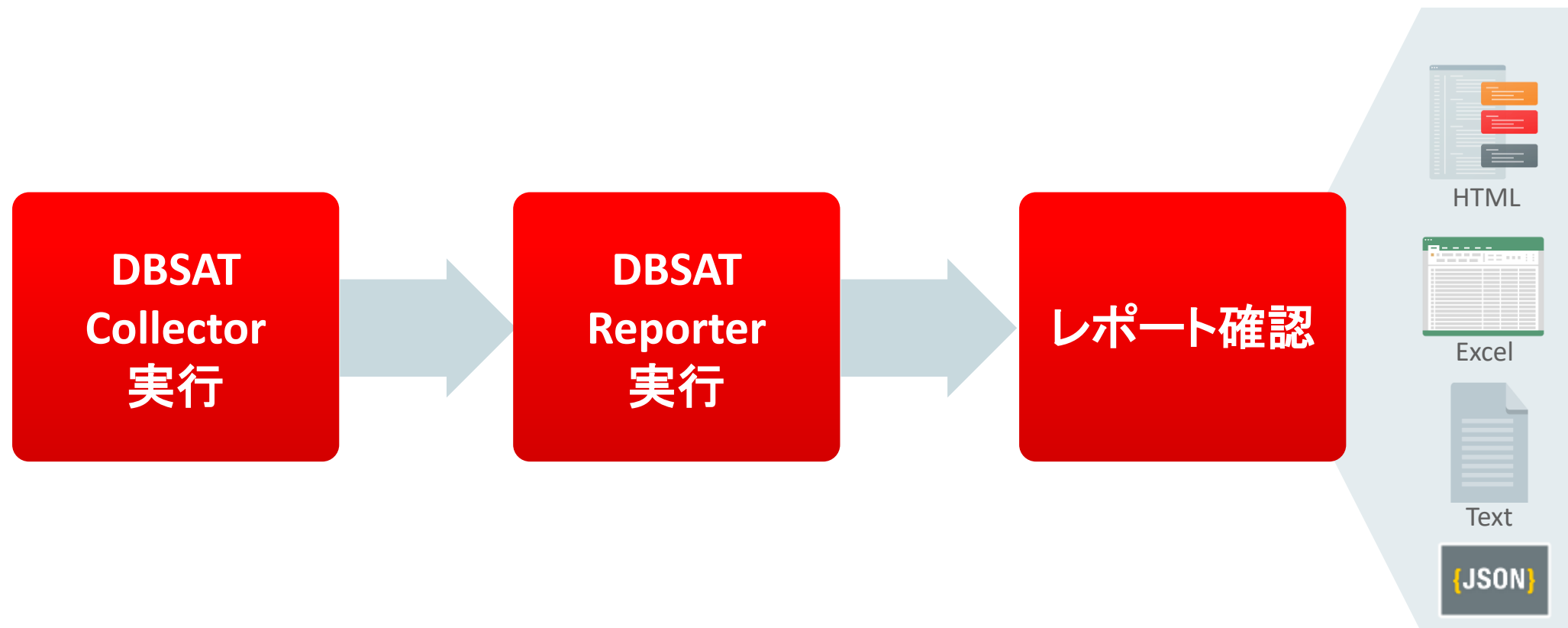


Oracle Databases 10g以降に対応

データディクショナリへの検索とOSファイル、パッチ確認のみで
ユーザーデータへのアクセスはありません

アセスメントレポート

セキュリティ構成状況、ユーザーと権限付与状況など



出力されるレポートは英語ですが、
日本オラクルで日本語化サービスを提供します

調査結果例

監査レコード

発見したリスクのレベル

DBSAT2.0
新機能

対応する規制

調査結果の
カテゴリ

調査結果の
詳細

調査結果の
根拠と推奨事項

規制との
マッピング

DBSAT2.0
新機能

AUDIT.RECORDS	
Status	High Risk
Summary	Examined 3 audit trails. Found no audit records. No errors found in audit initialization parameters.
Details	Traditional Audit Trail: No records found FGA Audit Trail: No records found Unified Audit Trail: No records found AUDIT_FILE_DEST=/opt/oracle/admin/orcl/adump AUDIT_SYSLOG_LEVEL is not set. AUDIT_TRAIL=DB
Remarks	監査は、システムを安全にするためには必要不可欠な要素です。監査ログは、強い権限を持ったユーザーの操作を監視することができます。セキュリティポリシーのギャップを悪用した攻撃に対して、監査がその攻撃自体を防ぐことはできませんが、悪意のあるアクティビティを検出することは、防御の最後のラインとして重要な役割を果たします。データベースから別のシステムに監査データを送信することが、監査レコードの改ざんのあらゆる可能性を防ぐために推奨されます。AUDIT_SYSLOG_LEVELパラメータは、リモートsyslogサーバに監査レコードの省略された値を送信するように設定できます。よりよい解決策は、Oracle Audit Vault and Database Firewallに様々なデータベースの監査レコードを送信して一元管理することです。
References	CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 2.2.2 EU General Data Protection Regulation 2016/679: Article 30, 33, 34

Use Case: データベースは安全に構成されているか？

優先付けられた調査結果のサマリー

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
基本情報	0	0	0	0	0	1	1
ユーザーアカウント	4	0	0	4	3	1	12
権限トロール	4	14	0	1	0	0	19
権限付与のコントロール	0	0	2	0	0	0	2
データの暗号化	0	1	1	0	0	0	2
ファイングレインアクセス制御	0	1	4	0	0	0	5
監査	3	4	1	0	3	1	12
データベース構成	5	3	0	1	2	2	13
ネットワーク構成	1	0	0	1	3	0	5
オペレーティングシステム	1	1	0	2	1	0	5
Total	18	24	8	9	12	5	76

Use Case: ユーザーと権限付与状況の確認

DBAロールを付与されているのは誰か？

DBAロール

PRIV.DBA		CIS
Status	Evaluate	
Summary	3 grants of DBA role.	
Details	Grants of DBA role: MASK: DBA PUKU <- MYDBA: DBA SYSTEM: DBA	
Remarks	DBAロールは非常に強力で多くのセキュリティ保護をバイパスすることができます。信用できる少数の管理者に対して付与するべきです。その上にそれぞれの信頼できるユーザには、説明責任を持たせるために個々のアカウントを持つようにする必要があります。同様にほかの強力なロールと同様に、本当に必要がない限りはDBAロールをWITH ADMINオプションで付与することを避けます。	
References	CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 4.4.4	

間接的な権限付与

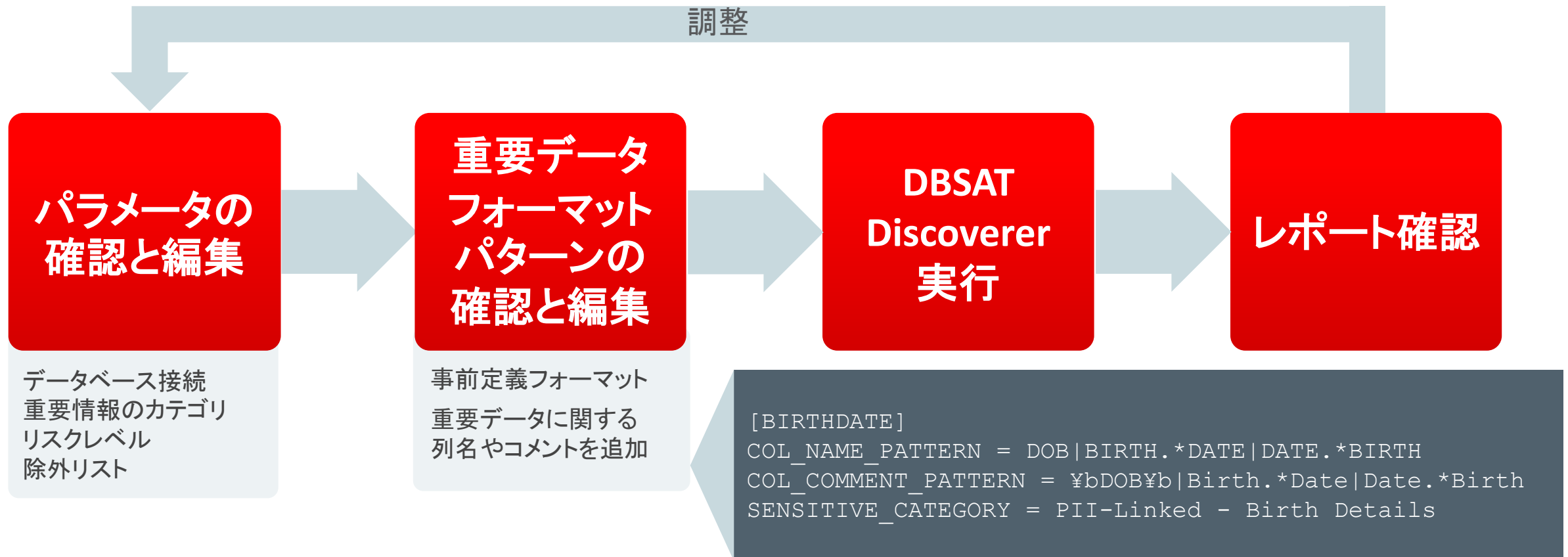
PUKUユーザーは
MYDBAロール経由で
DBAロールが
付与されている

お客様の声

- ベンダーに聞いても「大丈夫です」としか言われていなかったが、対策状況が可視化できた事が非常によかった
- 境界防御に偏った対策をしていて、データベースでの対策ができていない事がよく分かった
- 設定ミスで強力な権限を与えたまま残っていたアカウントが発見できた
- 製品を買わなくても設定で直せる点も多いのは非常によい
- データベースでのセキュリティ対策を今後進めていきたい

Use Case: 重要なデータのリスト化

どのようなデータがどこにどれくらいあるのか？



Report: どのような重要なデータをどのくらい持っているか

重要データの概況サマリー

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
JOB DATA	7	18	906
PII	7	22	2968
PII – ADDRESS	8	23	1859
PII – IT DATA	5	5	357
PII-LINKED	1	2	319
PII-LINKED – BIRTH DETAILS	1	1	1105
TOTAL	19*	71	3552**

* 重要データが格納されている表の(重複しない)数

** 重要データが格納されている列の(重複しない)数

表のサマリー

Schema	Table Name	Columns	Sensitive Columns	Rows	Sensitive Category
APP_A	APP_USER	3	1	496	PII – IT DATA
APP_A	CUSTOMERS	14	8	7	PII, PII – ADDRESS
APP_A	LINKED_DATA	6	4	500	PII-LINKED, PII-LINKED – BIRTH DETAILS
APP_A	PERSONAL_DATA	9	7	500	PII, PII – ADDRESS, PII – IDS
GENEVIS	EMP	24	4	14	JOB DATA
HR	JOBS	8	3	19	JOB DATA
HR	LOCATIONS	12	6	23	PII – ADDRESS, PII – IT DATA
HR	SUPPLEMENTAL_DATA	6	4	149	FINANCIAL DATA – PCI, JOB DATA, PII – IDS, PII – IT DATA

重要なデータが格納された列の詳細

Schema Name	Table Name	Column Name	Column Comment	Sensitive Category	Sensitive Type
APP_A	APP_USER	PWD	--	PII – IT DATA	PASSWORD
APP_A	CUSTOMERS	CUST_EMAIL	--	PII	EMAIL
APP_A	CUSTOMERS	CUST_FIRST_NAME	--	PII	FIRST_NAME
APP_A	CUSTOMERS	CUST_STREET_ADDRESS	--	PII – ADDRESS	STREET
APP_A	CUSTOMERS	PHONE_NUMBER1	--	PII	PHONE

いますぐダウンロード可能

<http://www.oracle.com/technetwork/database/security/dbsat/>

もしくは

DBSAT



で検索

Oracle
Database Security
Assessment Tool

With data breaches growing every day along with the evolving set of data protection and privacy regulations, protecting business sensitive and regulated data is mission critical. However, knowing whether the database is securely configured, who can access it, and where sensitive personal data resides is a challenge for most organizations. As part of Oracle's defense in depth capabilities, the Oracle Database Security Assessment Tool (DBSAT) helps identify areas where your database configuration, operation, or implementation introduces risks and recommends changes and controls to mitigate those risks.

[Data Sheet: Oracle Database Security Assessment Tool](#)

[FAQ: Oracle Database Security Assessment Tool](#)

日本語ページ作成中

データベース・セキュリティ・アセスメント・サービス

スクリプトとヒアリングをもとにリスクを可視化し、推奨する対策と優先順位をご提案



1

現在の状況をスクリプトとヒアリングで確認

- ・ロールや特権の設定状況
- ・暗号化、アクセス制御状況
- ・DBの初期パラメータの設定
- ・アカウントの設定・運用状況
- ・監査の設定状況
- ・ネットワーク構成

ヒアリング

スクリプト

2

発見したリスクの一覧

Oracle Database Security Assessment

Highly Confidential

Assessment Date & Time

Database Identity

Summary

発見された代表的なリスク

セキュアなシステム構成

アカウント管理

アクセス制御

機密性保護

監査と監視

3

対策実施の優先順位のご提案

① ベストプラクティスに準拠した設定・運用

② 重要なデータの暗号化

③ 共有アカウントの原則廃止

④ 職務分掌と最小権限の原則の実施

⑤ アクセスバスの制限

⑥ アクティビティの監査・監視

⑦ パッチ適用およびアップグレード計画の策定

リスクの大きさ / 対策実施の価値

優先的に対応すべき事項

4

優先対策事項のご提案と推奨対策実施による効果の可視化

① ベストプラクティスに準拠した設定・運用

② 重要なデータの暗号化

④ 職務分掌と最小権限の原則の実施

追加の製品導入なく可能なセキュリティ対策の実施

OSファイルやネットワークからのデータ漏洩防止

データベースの権限の見直しと共有アカウント使用時の多要素認証

⑤ アクセスバスの制限

⑥ アクティビティの監査・監視

データベースにアクセスできる経路を限定することで脅威の発生の可能性を最小化

操作の監査を優先実施

将来的に不正操作の検知

ORACLE

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

16

Integrated Cloud

Applications & Platform Services