

**ORACLE®**

# Oracle Database Security Assessment Tool 2.1

ハッカーに先を越される前に  
自社のセキュリティ態勢を把握する

Pedro Lopes  
製品マネージャー  
Oracle Databaseセキュリティ  
2019年3月1日



# データー もっとも貴重な資産

運転免許証番号、パスポート番号、  
納税者ID、健康保険被保険者番号、…

クレジット/デビット・カード番号、  
暗証番号、SSN、年齢、名前、誕生日、…



# 進化する規制の現状

- EU一般データ保護規則 (EU GDPR)
- クレジット・カード業界のデータ・セキュリティ基準 (PCI DSS)
- 米国サーベンス・オクスリー法 (SOX)
- HIPAA/HITECH
- 多数の侵害通知法



# 誰が自社のデータを狙っているのか?



国家

犯罪者

ハクティビスト

内部関係者

元従業員

詮索好き

個人データ  
財務データ  
企業秘密  
規制データ

顧客



競合企業

# 進化する攻撃ツールとテクニック

盗んだ資格証明

フィッシング

バッファ・  
オーバーフロー

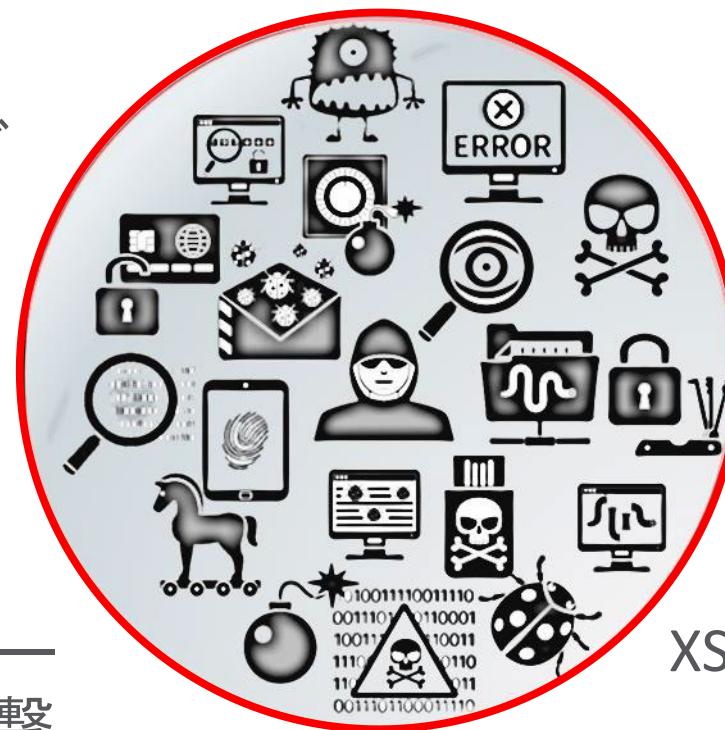
アプリケー  
ション攻撃

SQLインジェクション

権限昇格

XSS攻撃

パッチ未適用のシステム



# 思考の類似

## 攻撃者 vs データの所有者



内部関係者/部外者

オープン・ポート  
データベースSID  
既知のユーザー  
一般的なパスワード  
暗号化されたデータ  
特権ユーザーに  
対する監査  
データベースの  
バージョン  
既知の脆弱性  
有名なパッケージ・アプリ



# 開始点と探索対象



機密データはどこにあるのか?  
ユーザーはだれで、そのエンタイトルメントは  
何か?どんな制御機能を使用できるか?  
使用中のデータベースはセキュアに構成されているか?

データベース・セキュリティ・チームは存在するか?  
知識はどうか?分析時間はどうか?



# お試しください

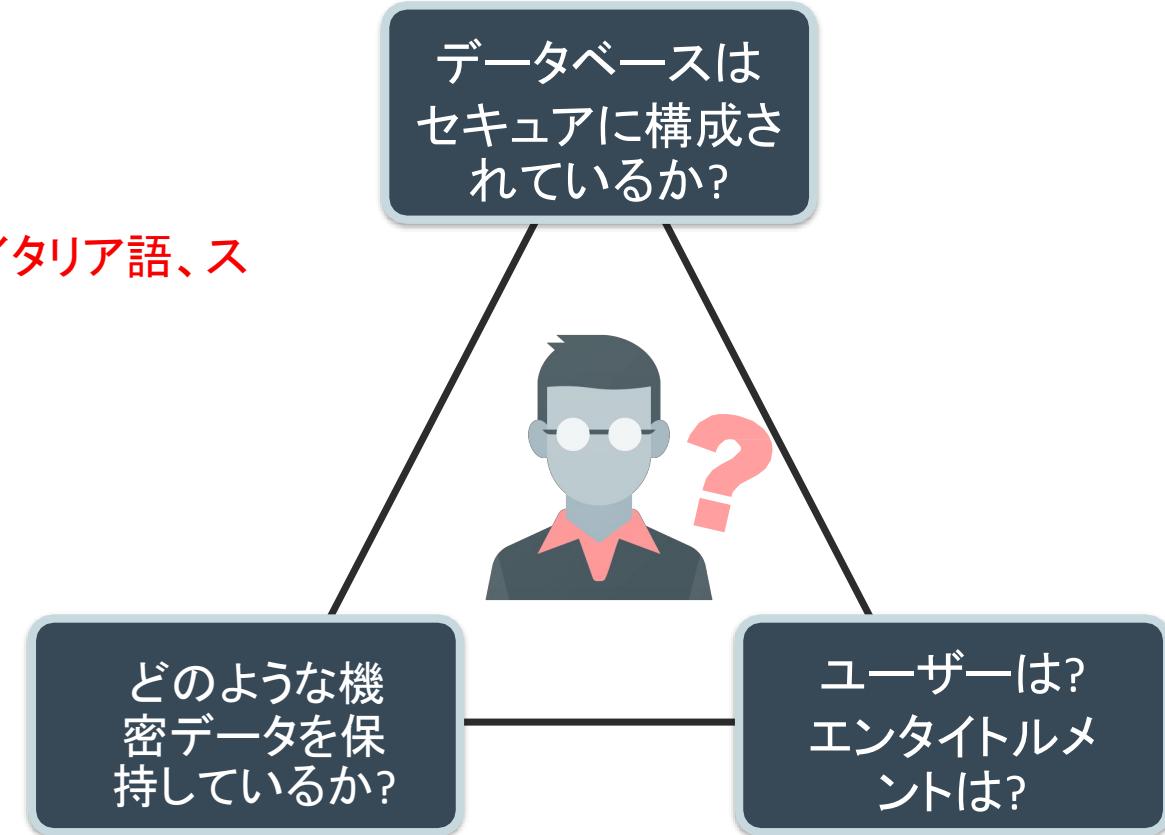
Oracle Database Security Assessment Tool



# Oracle Databaseセキュリティ評価ツール(DBSAT)

ハッカーに先を越される前に自社のセキュリティ態勢を把握する

- ・ 自社のデータベースの安全性(脆弱性)を把握する
  - 全体的なセキュリティの現状を報告する
  - ユーザー、エンタイトルメント、リスクについて調べる
  - 機密データを英語、**ドイツ語、オランダ語、フランス語、イタリア語、スペイン語、ポルトガル語**\*で検索
- ・ 実用的な評価レポート
  - サマリーと詳細情報
  - 優先順位付けされた推奨事項
  - EU GDPRおよびCISベンチマーク、**STIG**\*との紐付け
- ・ スタンドアロンの軽量なツール：迅速で、簡単
- ・ 現在Oracleをご使用のお客様に**無償提供**



\* 2.1の新機能

# Oracle DBSATのチェック対象は?

## 1. セキュリティ構成

- ・データ暗号化
- ・監査ポリシー
- ・ファイングレイン・アクセス制御
- ・データベースとリスナーの構成
- ・OSファイル権限
- ・セキュリティ・パッチ

## 2. ユーザーとエンタitlement

- ・ユーザー・アカウント、権限、ロール

## 3. 機密データ

- ・どのような種類か、どこにあるか、  
どれほどあるか



Oracle Database 10g  
以降が対象

## 2.0.1 DBSATの新機能

- CISベンチマークの推奨事項への参照
- GDPRの条項/備考への参照
- 他のツールとの統合に使用できるJSON出力
- 機密データ検出機能の導入
  - 英語のパターン・ファイルが標準で付属
  - カスタマイズ可能

## 2.0.2 DBSATの新機能

7月に導入

- Discovererとデータベース・サーバーのSSLチャネル経由での接続をサポート
- Exadata Express Cloud ServiceおよびAutonomous Data Warehouseでの機密データの検出
- 検出された機密データ列をAudit Vault and Database Firewallにインポートして新しいデータ・プライバシー・レポートを作成可能

The screenshot shows the Oracle Audit Vault Server interface. The top navigation bar includes Home, Secured Targets, Reports (which is selected), Policy, Settings, and Logout. The version is listed as 12.2.0.8.0. The user is logged in as 'avauditor'. The main menu on the left has sections for BUILT-IN REPORTS (Activity Reports, Summary Reports, Compliance Reports, Specialized Reports), CUSTOM REPORTS (PDF/XLS Reports, Saved Interactive Reports), REPORT WORKFLOW (Report Schedules, Generated Reports), and QUICK LINKS (Payment C, Gramm-Le, Health Ins, Sarbanes-, Data Prote, Reports b). The 'Compliance Reports' link under BUILT-IN REPORTS is highlighted. The central area displays 'Data Privacy Reports' with a message to associate Secured Target(s) with a Compliance Category. It lists four categories: Sensitive Data (Details of sensitive data), Access Rights to Sensitive Data (User's access rights to sensitive data), Activity on Sensitive Data (Activity on sensitive data by all users), and Activity on Sensitive Data by Privileged Users (Activity on sensitive data by privileged users). Below this is a 'Sensitive Data' table titled 'Secured Target Name : target2'. The table has columns for Sensitive Schema Name, Target Type, Target Object, Column Name, and Sensitive Type. The data is as follows:

Sensitive Schema Name	Target Type	Target Object	Column Name	Sensitive Type
SCOTT	TABLE	CCDATA	CREDIT_CARD_NUMBER	CREDIT_CARD_NUMBER
SCOTT	TABLE	CREDITCARD	CREDIT_CARD_NUMBER	CREDIT_CARD_NUMBER
SCOTT	TABLE	TEST	CREDIT_CARD_NUMBER	CREDIT_CARD_NUMBER
SCOTT	TABLE	CCDATA	EMAIL_ID	EMAIL_ID
SCOTT	TABLE	CCDATA	IP_ADDRESS	IP_ADDRESS
SCOTT	TABLE	CCDATA	ISBN_10	ISBN_10
SCOTT	TABLE	CCDATA	ISBN_13	ISBN_10
SCOTT	TABLE	CCDATA	NATIONAL_INSURANCE_NUMBER	NATIONAL_INSURANCE_NUMBER
SCOTT	TABLE	CCDATA	SOCIAL_INSURANCE_NUMBER	NATIONAL_INSURANCE_NUMBER
SCOTT	TABLE	CCDATA	PHONE_NUMBER	PHONE_NUMBER
SCOTT	TABLE	CCDATA	SOCIAL_SECURITY_NUMBER	SOCIAL_INSURANCE_NUMBER
SCOTT	TABLE	CCDATA	UNIVERSAL_PRODUCT_CODE	UNIVERSAL_PRODUCT_CODE

## 2.1.0 DBSATの新機能

- STIGルールの強調表示
- パスワード・ファイル、グローバル名、インスタンス名、RMANバックアップ等に対する新しい評価結果
- 直接付与されたシステム権限の特定の簡素化
  - (D)マークで明示
- Oracle Database 18c、19cおよびAutonomous Databasesに対する動作保証
- ドイツ語、オランダ語、フランス語、スペイン語、イタリア語、ポルトガル語に対応した機密情報パターン・ファイルが付属
- 新しい機密タイプ、カテゴリ、サブカテゴリ
- 機密データのカテゴリをリスク・レベルでグループ化
- リスク・レベルに応じた注釈および推奨される制御をレポートに掲載



# 操作方法

Oracle Database Security Assessment Tool



# ダウンロードして3ステップを実行するだけ

## 1. ダウンロード

<https://www.oracle.com/jp/database/technologies/security/dbsat.html>

## 2. データベース・セキュリティ評価レポート入手

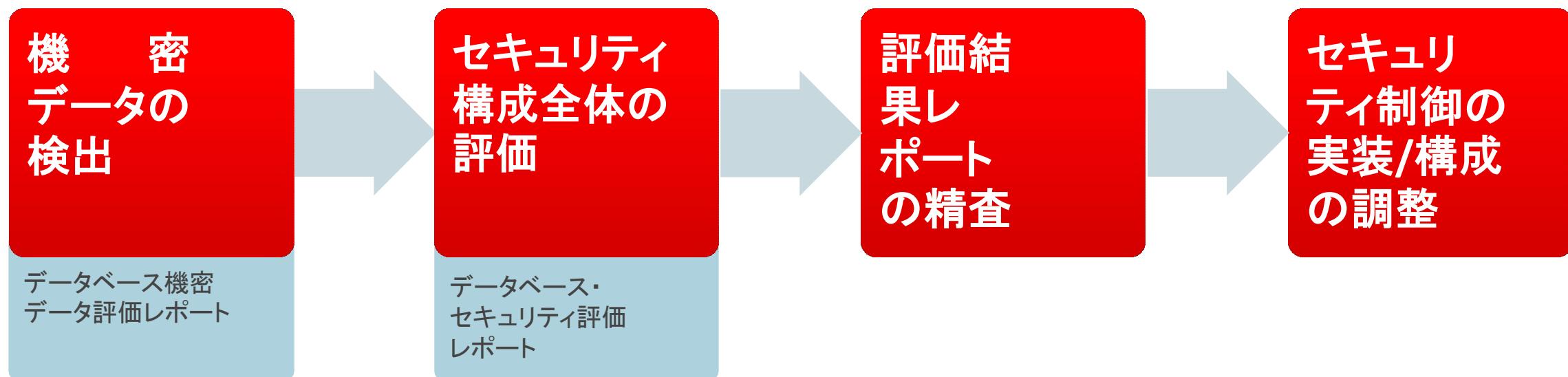
- DBSAT Collectorを実行
- DBSAT Reporterを実行

## 3. データベース機密データ評価レポート入手

- DBSAT Discovererを実行

# 例：データ・プライバシーへの取組みを 進めるための評価フロー・ステップ

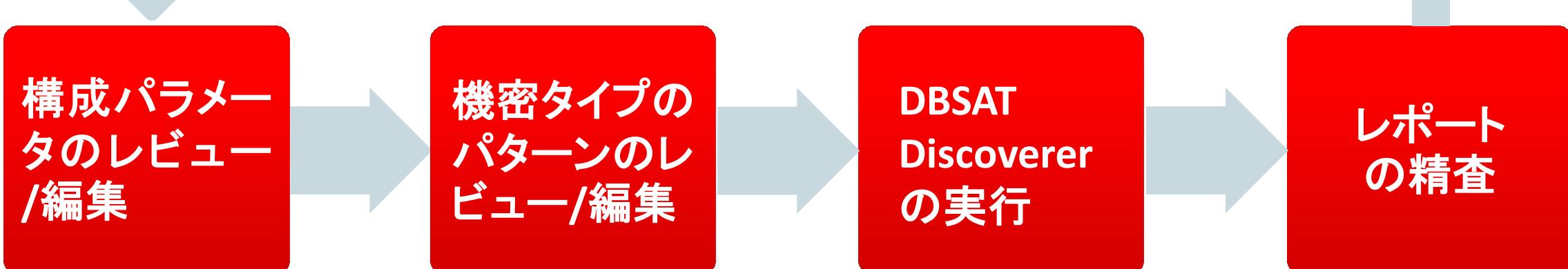
## 検出から推奨事項まで



# 機密データの検出

何を、どこに、どのくらい持っているかを把握する

より細かく調整



データベース接続 機密  
カテゴリリスク・レベル  
適用/除外リスト

機密タイプの  
パターンのレ  
ビュー/編集

追加設定不要なタイプ  
列の名前/コメント検索用  
に独自のタイプを追加

DBSAT  
Discoverer  
の実行

レポート  
の精査

```
[DATE OF BIRTH]  
COL_NAME_PATTERN = DOB$|BIRTH.? (DT|DATE) | (DT|DATE).*BIRTH  
COL_COMMENT_PATTERN = ¥bDOB¥b|BIRTH.?DATE|DATE.*BIRTH  
SENSITIVE_CATEGORY = Biographic Info - Extended PII
```

# レポート:どのような機密データを、 どのくらい保持しているか?

## 機密データの状況

カスタマイズ  
可能なカテゴリ

Sensitive Category	# Sensitive Tables	# Sensitive Columns	# Sensitive Rows
BIOGRAPHIC INFO – ADDRESS	7	18	244
FINANCIAL INFO – CARD DATA	2	2	256
HEALTH INFO – PROVIDER DATA	1	1	149
IDENTIFICATION INFO – PERSONAL IDS	3	3	356
IDENTIFICATION INFO – PUBLIC IDS	3	12	321
IT INFO – USER DATA	1	1	149
JOB INFO – COMPENSATION DATA	7	10	527
JOB INFO – EMPLOYEE DATA	12	25	569
JOB INFO – ORG DATA	7	8	412
<b>TOTAL</b>	<b>21*</b>	<b>80</b>	<b>989**</b>

\* 機密データが含まれる一意の表数  
\*\* 機密データが含まれる一意の行数

# レポート: 推奨される制御

## Security for Environments with High Value Data: Detective plus Strong Preventive Controls

Highly sensitive and regulated data should be protected from privileged users, and from users without a business need for the data. Activity of privileged accounts should be controlled to protect against insider threats, stolen credentials, and human error. Who can access the database and what can be executed should be controlled by establishing a trusted path and applying command rules. Sensitive data should be redacted on application read only screens. A Database Firewall ensures that only approved SQL statements or access by trusted users reaches the database – blocking unknown SQL injection attacks and the use of stolen login credentials.

Recommended controls include:

- Audit all sensitive operations including privileged user activities
- Audit access to application data that bypasses the application
- Encrypt data to prevent out-of-band access
- Mask sensitive data for test and development environments
- Restrict database administrators from accessing highly sensitive data
- Block the use of application login credentials from outside of the application
- Monitor database activity for anomalies
- Detect and prevent SQL Injection attacks
- Evaluate: *Oracle Audit Vault and Database Firewall, Oracle Advanced Security, Oracle Data Masking and Subsetting, Oracle Database Vault*

例

機密情報の操作を監査する データを暗号化する  
テスト/開発時はデータをマスクする

## Tables Detected within Sensitive Category: FINANCIAL INFO – CARD DATA

Risk Level	High Risk
Summary	Found FINANCIAL INFO – CARD DATA within 2 Column(s) in 2 Table(s)
Location	Tables: HCM1.EMP_EXTENDED, HCM1.SUPPLEMENTAL_DATA

# レポート:どのテーブルに、 どれくらいの機密データが含まれているか? 機密情報を含む表のサマリー

Schema	Table Name	Columns	Sensitive Columns	Rows	Sensitive Category
FINACME	COMPANY_DATA	9	4	100	BIOGRAPHIC INFO - ADDRESS, IDENTIFICATION INFO - PERSONAL IDS
HCM1	COUNTRIES	3	1	25	BIOGRAPHIC INFO - ADDRESS
HCM1	DEPARTMENTS	4	1	27	JOB INFO - ORG DATA
HCM1	EMPLOYEES	11	8	107	IDENTIFICATION INFO - PUBLIC IDS, JOB INFO - COMPENSATION DATA, JOB INFO - EMPLOYEE DATA, JOB INFO - ORG DATA
HCM1	EMP_EXTENDED	3	3	107	FINANCIAL INFO - CARD DATA, IDENTIFICATION INFO - PERSONAL IDS, JOB INFO - EMPLOYEE DATA

暗号化 /特権ユーザー・アクセス/プロセッサ制限の候補表?

# レポート: どの列に、 どれくらいの機密データが含まれているか? 機密データのある列の詳細

Schema Name	Table Name	Column Name	Column Comment	Sensitive Category	Sensitive Type	Risk Level
FINACME	COMPANY_DATA	CITY	--	BIOGRAPHIC INFO - ADDRESS	CITY	High Risk
FINACME	COMPANY_DATA	STATE	--	BIOGRAPHIC INFO - ADDRESS	STATE	High Risk
FINACME	COMPANY_DATA	TAX_PAYER_ID	--	IDENTIFICATION INFO - PERSONAL IDS	TAX ID NUMBER (TIN)	High Risk
FINACME	COMPANY_DATA	ZIP	--	BIOGRAPHIC INFO - ADDRESS	POSTAL CODE	High Risk
HCM1	COUNTRIES	COUNTRY_NAME	--	BIOGRAPHIC INFO - ADDRESS	COUNTRY	High Risk
HCM1	DEPARTMENTS	DEPARTMENT_NAME	--	JOB INFO - ORG DATA	DEPARTMENT NAME	Low Risk
HCM1	EMPLOYEES	EMAIL	This is the email ad...	IDENTIFICATION INFO - PUBLIC IDS	EMAIL ADDRESS	High Risk
HCM1	EMPLOYEES	EMPLOYEE_ID	This is the unique e...	JOB INFO - EMPLOYEE DATA	EMPLOYEE ID NUMBER	High Risk
HCM1	EMPLOYEES	FIRST_NAME	--	IDENTIFICATION INFO - PUBLIC IDS	FIRST NAME	High Risk

マスキング、仮名化、監査ポリ  
シーの候補列

# データベース・セキュリティ評価レポート

## セキュリティ構成ステータス、ユーザーとそのエンタイトルメント



# 評価結果の分析

Evaluate、Advisory、Pass、Low Risk、  
Medium Risk、High Riskのいずれか

評価結果の  
カテゴリ

関連する  
可能性が  
ある規制

評価結果の詳細

根拠と推奨事項

規制との  
マッピング

AUDIT.RECORDS

CIS GDPR STIG

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=/u01/app/oracle/rdbms/audit  
AUDIT\_SYSLOG\_LEVEL is not set.  
AUDIT\_TRAIL=DB

Remarks Auditing is an essential component for securing any system. The audit trail allows for monitoring the activities of highly privileged users. For any attack that exploits gaps in other security policies, auditing cannot prevent the attack but it forms the critical last line of defense by detecting the malicious activity. Oracle Database 12c introduced Unified Auditing and this is the recommended auditing mode moving forward (pure Unified Audit mode). It adds several benefits as centralized audit logs in a single audit trail, improved performance, simplified management and security. The AUDIT\_FILE\_DEST controls the OS directory to which the audit trail is written if using AUDIT\_TRAIL=os, xml, or xml\_extended. This directory should be prevented from any unauthorized access. Sending audit data to a remote system is recommended in order to prevent any possible tampering with the audit records. The AUDIT\_SYSLOG\_LEVEL parameter can be set to send an abbreviated version of some audit records to a remote syslog collector. A better solution is to use Oracle Audit Vault and Database Firewall to centrally collect full audit records from multiple databases.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 2.2.2  
EU GDPR 2016/679: Article 30, 33, 34  
Oracle Database 12c STIG v1 r10: Rule SV-75899r1, SV-76111r1, SV-76117r1, SV-76121r1, SV-76123r1, SV-76125r1, SV-76127r1, SV-76129r1, SV-76455r3

# ユースケース：データベースはセキュアに構成されているか？

## 評価結果のサマリー表示、優先度別

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
<a href="#">Basic Information</a>	0	0	0	0	0	1	1
<a href="#">User Accounts</a>	5	0	0	4	2	1	12
<a href="#">Privileges and Roles</a>	5	16	0	0	0	0	21
<a href="#">Authorization Control</a>	0	1	1	0	0	0	2
<a href="#">Fine-Grained Access Control</a>	0	1	4	0	0	0	5
<a href="#">Auditing</a>	0	4	2	0	6	0	12
<a href="#">Encryption</a>	0	1	1	0	0	0	2
<a href="#">Database Configuration</a>	5	3	0	3	2	1	14
<a href="#">Network Configuration</a>	1	1	0	0	3	0	5
<a href="#">Operating System</a>	1	0	0	2	1	1	5
<b>Total</b>	<b>17</b>	<b>27</b>	<b>8</b>	<b>9</b>	<b>14</b>	<b>4</b>	<b>79</b>

# ユースケース: ユーザーとそのエンタイトルメントは? 直接付与されたシステム権限

STIGの強調表示

PRIV.SYSTEM

CIS STIG

Status Evaluate

Summary 1342 grants of system privileges (17 with admin option). 122 Privileges are granted directly.

Details Users directly or indirectly granted each system privilege:

ADMINISTER ANY SQL TUNING SET: DEBRA, OUTSRC\_DBA, SCOTT, SSWADMIN,  
SYSTEM(\*), U1(D), U2(D)(\*), U3(\*)

ADMINISTER DATABASE TRIGGER: DEBRA, OUTSRC\_DBA, SCOTT, SSWADMIN, SYSTEM

ADMINISTER RESOURCE MANAGER: DEBRA, OUTSRC\_DBA, SCOTT, SSWADMIN, SYSTEM

ADMINISTER SQL MANAGEMENT OBJECT: DEBRA, OUTSRC\_DBA, SCOTT, SSWADMIN,

(D) – 直接付与 (\*) – 管理者オプション付き

# ユースケース: ユーザーとそのエンタイトルメントは?

## DBAロール(直接または間接付与)のあるユーザー

PRIV.DBA

CIS

Status Evaluate

Summary 5 grants of DBA role.

Details Grants of DBA role:

DEBRA <- APP\_ROLE: DBA ← 間接的な付与

OUTSRC\_DBA: DBA

SCOTT: DBA

SSWADMIN: DBA

SYSTEM: DBA

Remarks The DBA is a powerful role and can be used to bypass many security controls. It should be granted to a small number of trusted administrators. As a best practice, it is recommended to create custom DBA-like roles with minimum set of privileges that users require to execute their tasks (least privilege principle) and do not grant the DBA role. Privilege Analysis can assist in the task of identifying used/unused privileges and roles. Having different roles with minimum required privileges based on types of operations DBAs execute also helps to achieve Separation of Duties. Furthermore, each trusted user should have an individual account for accountability reasons. Avoid granting the DBA or custom DBA-like powerful roles WITH ADMIN option unless absolutely necessary. Please note that Oracle may add or remove roles and privileges from the DBA role.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 4.4.4

ユーザーDEBRAはロールAPP\_ROLE経由でDBAロールを間接的に付与されている

# 複数のレポート形式

USER.DEFPWD

Status High Risk

Summary Found 2 unlocked user accounts with default password.

Details Users with default password: HR, SCOTT

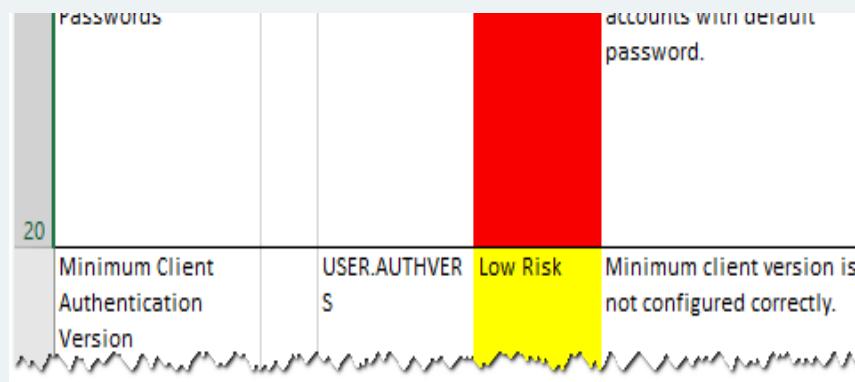
Remarks Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.

References CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2

HTML

```
...
    "severity": 5,
    "title": "Users with Default Passwords",
    "remarks": "Default account passwords for predefined Oracle accounts are well known. Open accounts with default pa
        provide a trivial means of entry for attackers, but well-known passwords should be changed for locked
    "details": "Users with default password: HR, SCOTT\\n",
    "refs": [
        "CIS": "Recommendation 1.2"
    ],
    "type": "finding",
    "id": "USER.DEFPWD",
    "summary": "Found 2 unlocked user accounts with default password."
},
...
}
```

JSON



スプレッドシート

```
205 * Users with Default Passwords *
206 Status: High Risk
207 Summary:
208     Found 2 unlocked user accounts with default password.
209 Details:
210     Users with default password: HR, SCOTT
211 Remarks:
212     Default account passwords for predefined Oracle accounts are well
213     known. Open accounts with default passwords provide a trivial means of
214     entry for attackers, but well-known passwords should be changed for
215     locked accounts as well.
216 References:
217     CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2
218
219
```

テキスト



すぐに始めましょう  
攻撃はすでに始まっています!

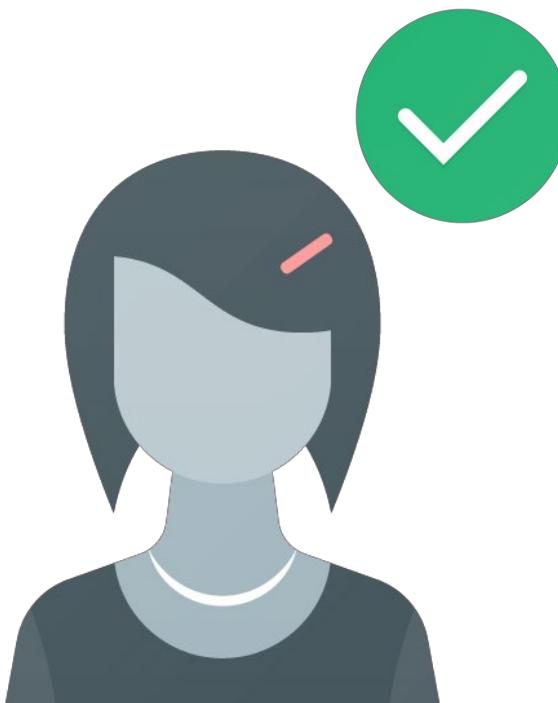
≡ ⊕ ∕ / ⊕ ⊕ ·  
/ ⊕ ≡ / ⊕ ·  
: ≡ ≡ / ⊕ ≡ ≡ :



# インストールと実行が容易

- 下のURLからDBSAT 2.1を今すぐダウンロードする  
<https://www.oracle.com/jp/database/technologies/security/dbsat.html>
- サポート契約が有効なすべてのOracleデータベースのお客様がダウンロード可能
- ターゲットで'dbsat collect'を実行してセキュリティ構成データを収集する
- ターゲットまたは他の場所で‘dbsat report’ を実行する
- ターゲットで‘dbsat discover’ を実行して機密データ・レポートを生成する
- 機密データが含まれるため、生成されたレポートへのアクセスを制限する

# 開始点と探索対象



機密データはどこにあるのか?  
ユーザーはだれで、そのエンタイトルメントは何か?  
どんな制御機能を使用できるか?  
使用中のデータベースはセキュアに構成されているか?

データベース・セキュリティ・チームは存在するか?  
知識はどうか?分析時間はどうか?

# まとめ

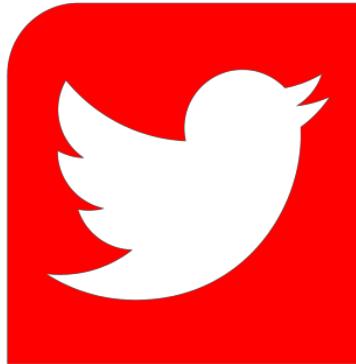
- ハッカーに先を越される前に、データベースの現在のセキュリティ状態を迅速に評価する
- 機密データを特定して、リスクと適切なセキュリティ管理を見極める
  - 英語および**欧州の主要言語**に対応
- 効果が証明されているベスト・プラクティス(**CIS**および**STIG**)を使用して、リスクへの露出を減らす
- EU GDPRや他の規制の順守を推進する
- Oracle Database 10g、11g、12c、18c、19cおよび**Autonomous DB**をサポート
- 追加費用なしで提供
- すぐにデプロイして使用できる

# 今すぐダウンロードしてください

- OTNのページ
- ソーシャル・ネットワークでは#DBSATをご利用ください
- データベース・セキュリティとGDPRホワイト・ペーパー  
<https://go.oracle.com/LP=54366>
- GDPRに関する詳細情報  
[www.oracle.com/goto/gdpr](http://www.oracle.com/goto/gdpr)
- データベース・セキュリティに関する詳細情報  
<http://oracle.com/database/security>

# Q & A

# オラクルの情報を発信しています



/OracleDatabase  
#DBSAT



/OracleSecurity



[blogs.oracle.com/  
SecurityInsideOut](http://blogs.oracle.com/SecurityInsideOut)



Oracle Database Insider



/Oracle/database  
—  
/OracleLearning

[oracle.com/database/security](http://oracle.com/database/security)

[oracle.com/technetwork/database/security](http://oracle.com/technetwork/database/security)

# Integrated Cloud Applications & Platform Services