Oracle Database Security Assessment Tool ご紹介

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/

データベースセキュリティナビ

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

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。

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

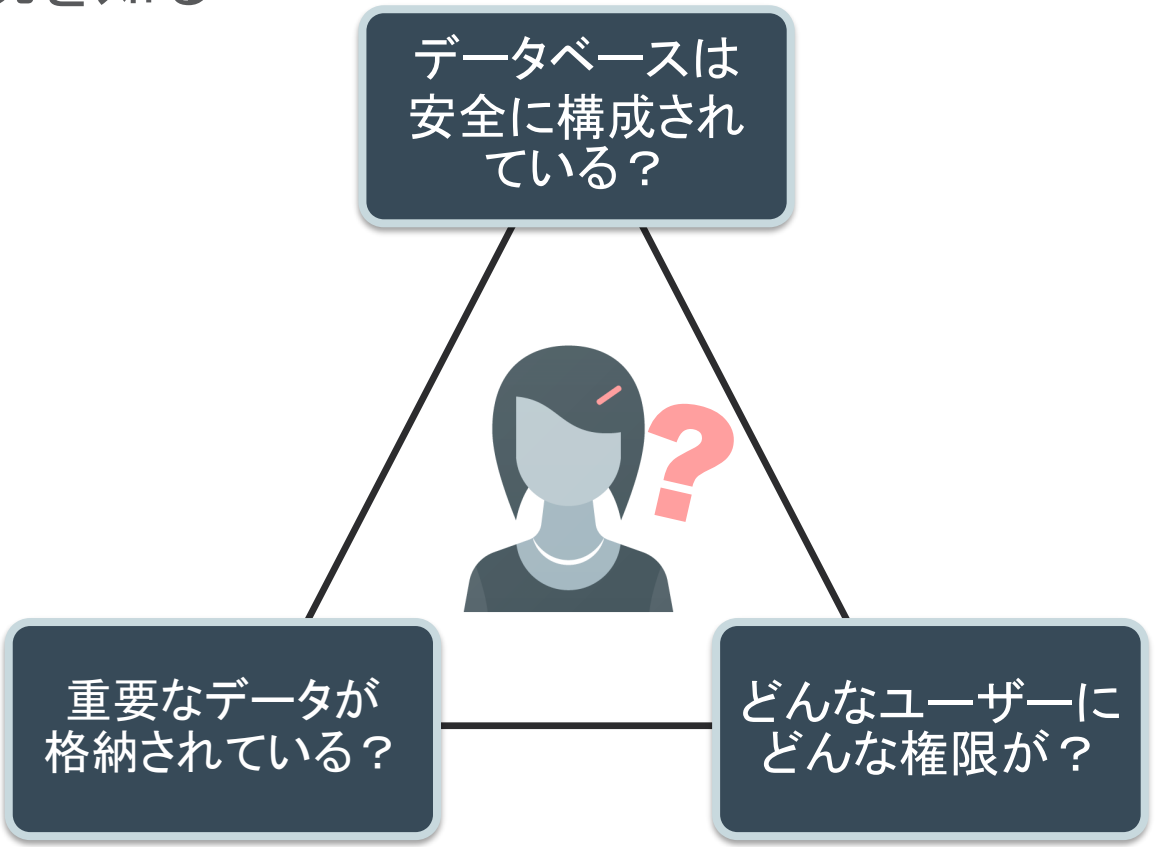
Oracle Database Security Assessment Tool

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 DBSAT2.0 新機能
- 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



(*) 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

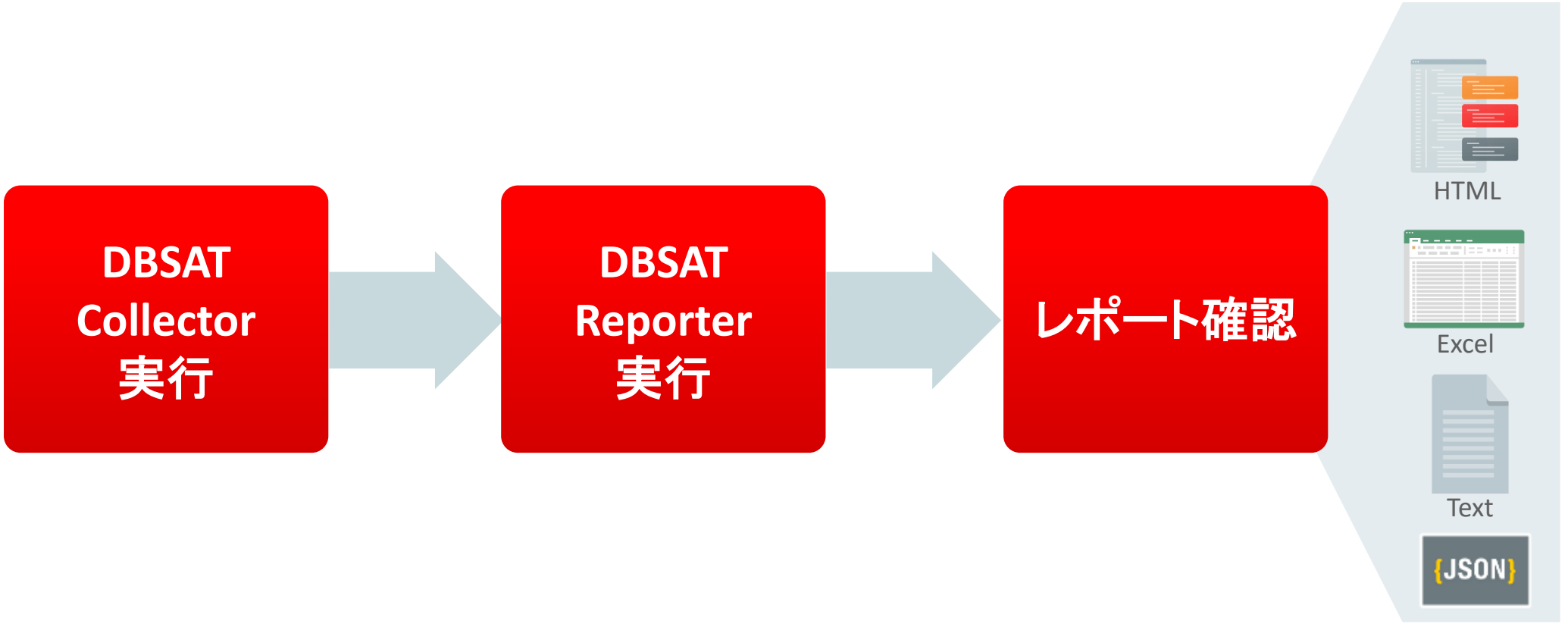
1. **セキュリティ構成状況**
   - データの暗号化
   - 監査ポリシー
   - ファイングレインアクセスコントロール
   - データベースとリスナーの構成
   - OSファイルパーミッション
   - セキュリティパッチ
2. **ユーザーと権限**
   - ユーザーアカウント、権限、ロール
3. **重要なデータ** DBSAT2.0 新機能
   - 種類、場所、数

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

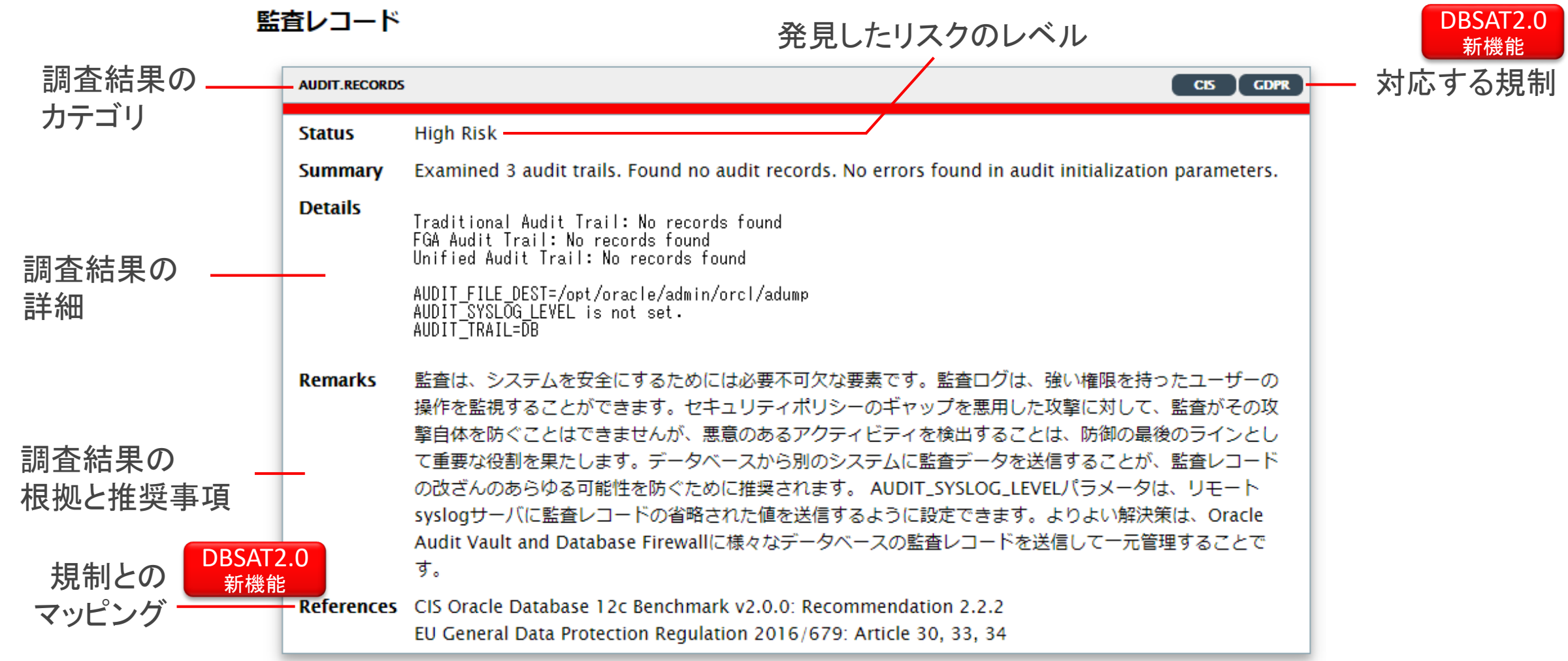
アセスメントレポート

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



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

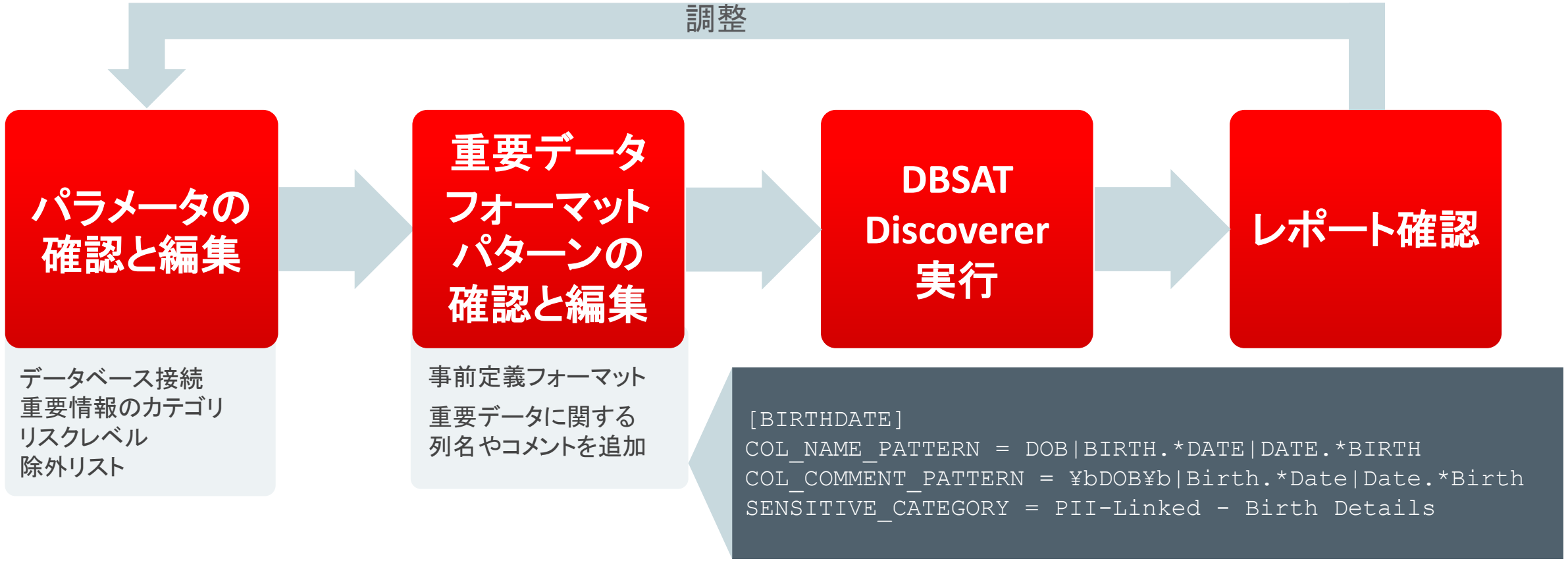
お客様の声

- 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

DBSAT2.0
新機能

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？



DBSAT2.0
新機能

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**

* 重要データか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_AD	--	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

日本語ページ作成中

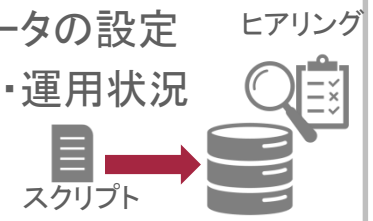
データベース・セキュリティ・アセスメント・サービス

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

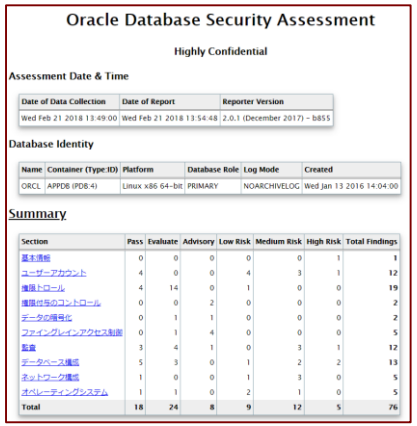
1. 対象システムを選定し、スクリプトとヒアリングで、現在の状況を確認
2. 発見したリスクをリストし、可視化
3. リスクの大きさと対策実施のコストから実施優先順位をご提案
4. 優先対策事項のご提案

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



2 発見したリスクの一覧



Oracle Database Security Assessment

Highly Confidential

Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Wed Feb 21 2018 13:49:00	Wed Feb 21 2018 13:54:48	2.0.1 (December 2017) - b855

Database Identity

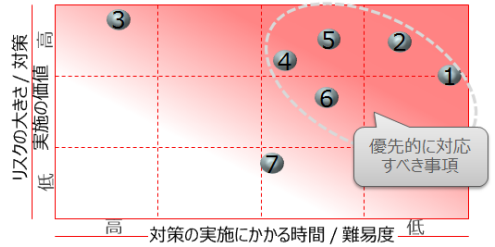
Name	Container (Type:ID)	Platform	Database Role	Log Mode	Created
ORCL	APPDB (PDB:4)	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Wed Jan 13 2016 14:04:00

Summary

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
権限とロール	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

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	アクセスパスの制限
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



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	追加の製品導入なく可能なセキュリティ対策の実施	
②	重要なデータの暗号化	OSファイルやネットワークからのデータ漏洩防止	
④	職務分掌と最小権限の原則の実施	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	アクセスパスの制限	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	
⑥	アクティビティの監査・監視	操作の監査を優先実施	将来的に不正操作の検知

Integrated Cloud

Applications & Platform Services