DB内部不正対策WG ソリューション紹介

DB内部不正対策WGメンバー

データベース・セキュリティ取り組みご紹介
～DBセキュリティ・サービスについて～

DB内部不正対策WGメンバー
伊藤忠テクノソリューションズ株式会社
製品・保守事業推進本部
北條　将也

会社紹介（伊藤忠テクノソリューションズ株式会社）

会社名	（**略称** CTC） 伊藤忠テクノソリューションズ株式会社
英文社名	ITOCHU Techno-Solutions Corporation
創立	1972年4月1日
本社所在地	〒100-6080　東京都千代田区霞が関3-2-5　霞が関ビル TEL 03-6203-5000（代） URL http://www.ctc-g.co.jp/
代表者	代表取締役社長　　菊地　哲
資本金	21,763百万円
社員数	8,088名
事業内容	コンピュータ・ネットワークシステムの販売・保守、ソフトウェア受託開発、情報処理サービス、科学・工学系情報サービス、サポート、その他

2015年4月1日現在

DBセキュリティ・サービスのご紹介 ～ 対応機能/製品 ～

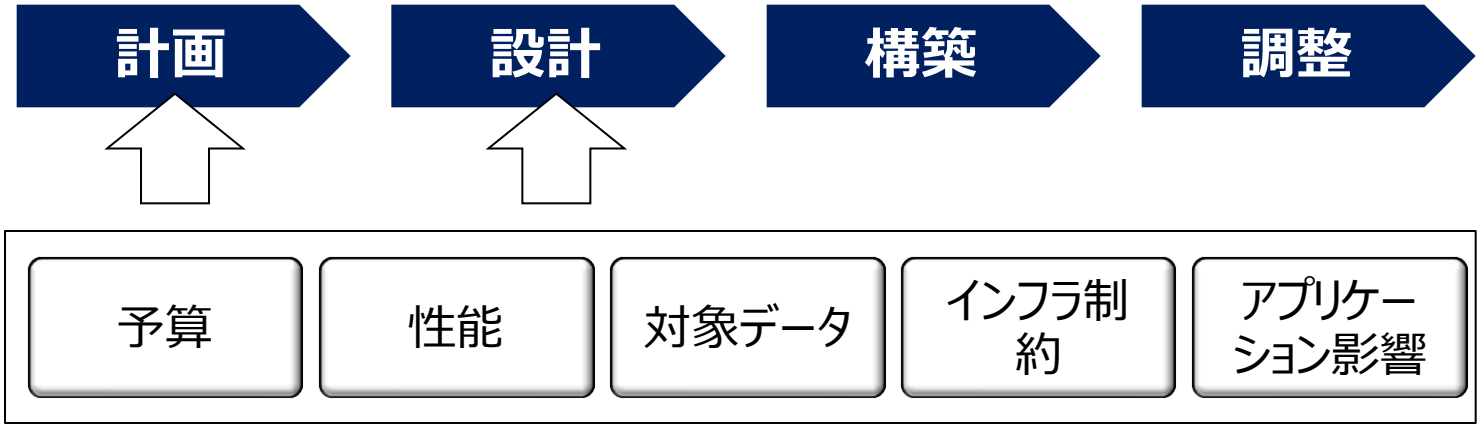
DBセキュリティ対策において一番重要なのは計画・設計・調整（チューニング）です

計画　お客様毎に異なるデータベース環境に最適な方式の選定

設計　保護対象データの選定と性能、予算のバランスを取った設計

調整　実環境テスト結果をうけた性能・セキュリティの設定チューニング

弊社は計画・設計フェーズからお客様のDBセキュリティ対策のご支援を実施いたします



DBセキュリティ・サービスのご紹介 ～ サービス全体像 ～

計画 → **設計** → **構築** → **運用**

アセスメント（セキュリティ）

- DB セキュリティ方針どこまでやるか？
- 現状運用課題・設定分析
- 予算感
- 機能/ツールの選定
- アプリケーション影響
- パフォーマンス影響

コンサルティングサービス DBセキュリティ

- 権限分掌設計・構築
- 暗号化設計・構築
- 監査設計・構築
- マスキング設計・構築
- セキュリティ実装に伴うデータベースチューニング
- セキュリティ実装に伴う運用設計・構築

DB運用サービス

- DB定期診断
- チューニング
- 技術問合せ窓口
- 障害復旧支援
- セキュリティ報告
- 監査報告

アセスメント（ﾎﾜｲﾄﾎﾞｰﾄﾞｾｯｼｮﾝ）

※アセスメントサービス簡易版
- セキュリティ対策をコンサルタントとディスカッション

セキュリティ機能・S/W導入

監査 （Oracle標準機能）	基本作業 ・ 監査対象ヒアリング～実装～ログ管理 オプション作業 ・ ログ出力量試算、チューニング、監査報告等
監査 （Audit Master）	
監査 （AVDF）	
権限分掌 （DB Vault）	基本実装のみ　詳細レルム・権限設計は人月方式で提供可
暗号化 DB構築オプション	DB作成サービスのオプション

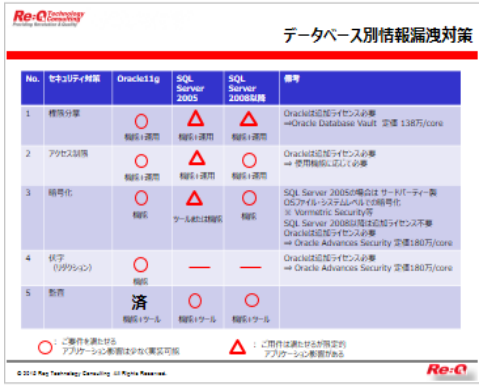
DBセキュリティ・アセスメント・サービスのご紹介　サービス対象

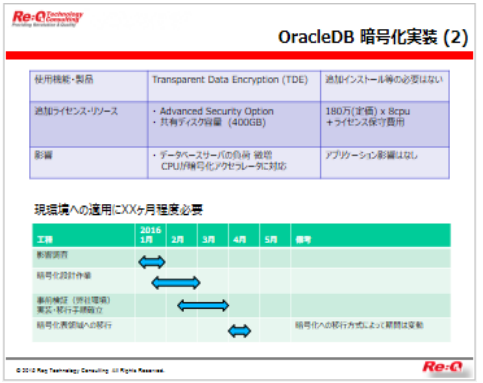
本サービスは、DBセキュリティ強化を検討中のお客様を対象としています

- 既にデータベースを運用中のお客様
  - 現在のセキュリティ・レベルや脆弱性を把握したいお客様
  - 内部統制や監査対応として、セキュリティを強化したいお客様
  - 今後のシステム更改に向けて、セキュリティ強化対策を検討しておきたいお客様
- 新たにデータベース・システムを構築されるお客様
  - サービス稼働の前にセキュリティを見直したいお客様
  - どのようなセキュリティ対策が必要かを確認したいお客様

お客様のシステムに最適化したDBセキュリティ設計・構築をご支援いたします

[レポート例]





DBセキュリティ・アセスメント・サービスのご紹介　サービス内容

お客様のデータベースセキュリティに関する方針、課題をヒアリングさせて頂き、
情報漏えいリスクやその強化対策案をレポーティング、検討させて頂きます

[参考]導入期間・価格
期間：4～6週間
価格：150万円～

No	アセスメント項目	項目詳細
1	お客様セキュリティ方針確認	・どのようなセキュリティ強化を検討しているのか ・情報漏えい対策の目標 （いつまで、予算、強化レベル感）
2	現状セキュリティ課題確認	・具体的な課題の確認 （何かのセキュリティ基準に適応させる等） ・事故等の事象の確認
3	現状の設定・運用に関する診断 ※基本はヒアリングベース ※オプションとして実環境を弊社側で調査	・DBアクセス構成（人、アプリケーション、端末・サーバ） ・DB診断（アカウント管理、権限設定、パッチ適用状況、OS設定） ・運用状況（パスワード、管理内容） ・（必要に応じて）アプリケーション内SQL実行
4	強化案（概要）の提示	・方針、予算、スケジュールにあった案の提示 推奨構成（機能、ソフトウェア）、導入方式（概要） ・パフォーマンス影響、アプリケーション影響　（想定概算レベル）

※レポート内容、形式は要相談

DBセキュリティ・サービス体制

DBセキュリティ・サービス推進体制

CTC Challenging Tomorrow's Changes × Re:Q Technology Consulting Providing Revolution & Quality

戦略的パートナ

セキュリティ部門での認定・表彰

国内で唯一「Oracle Database 11g **Security**」Oracle Specialization認定

Oracle Excellence Awards Oracle Excellence Award Specialized Partner of the Year 2013

Oracle Award「**Security** & Data Integration」（日本）受賞

Oracle Authorized Solution Center(OASC) の活用

CTCの総合検証センターがアジア太平洋地域で**初認定**

最新機材を活用し、セキュリティ製品の動作確認可

経験豊富なエンジニアがご支援

ORACLE AUTHORIZED SOLUTION CENTER

「答えは、CTC。」

Challenging Tomorrow's Changes

コーポレートロゴマークには、「世の中の変化を素早く読み取り、市場の変化に即応するだけでなく、
CTC自らがその変化を誘発する側に立とう」という熱い志を凝縮しました。
マークの下にある「**Challenging Tomorrow's Changes**」は、この志を一文で表したものです。

全方位型データベースセキュリティソフト

Chakra Maxのご紹介

DB内部不正対策WGメンバー
日本ウェアバレー株式会社　代表取締役
武田　治

目次

ウェアバレーのご紹介

先進のデータベースセキュリティ

WareValley
EXCELLENCE IN IT SOLUTIONS

データベースセキュリティソフトの専業メーカー

オラクルの技術者が起業したベンチャーとしてスタートしました

会社情報	
会社名	WareValley Co., Ltd.
設立	2001年2月
本社	韓国ソウル
社員数	75名
日本法人	2012年8月設立

プロダクト	
Chakra Max	全方位型DBセキュリティソフト
Galea	透過的データ暗号化ソフト
Cyclone	DB脆弱性診断ソフト
Orange	DBクライアントツール
PetaSQL	カラム型DBMS

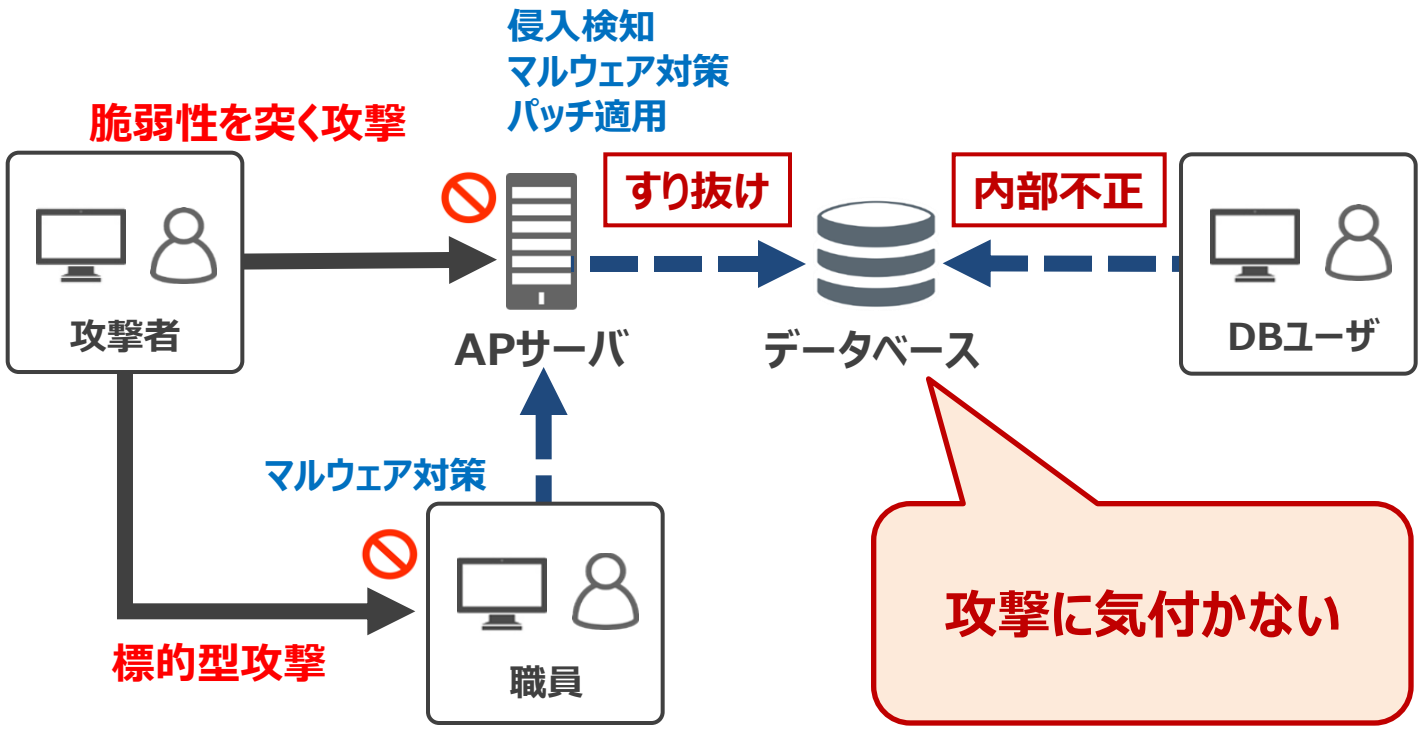
全方位型データベースセキュリティとは

全方位型データベースセキュリティとは

既存セキュリティ対策の盲点

外部からの指摘で情報漏えいが発覚

①既存対策を**すり抜ける**攻撃が拡大　　②**内部不正**に無防備



全方位型データベースセキュリティとは

求められる対策

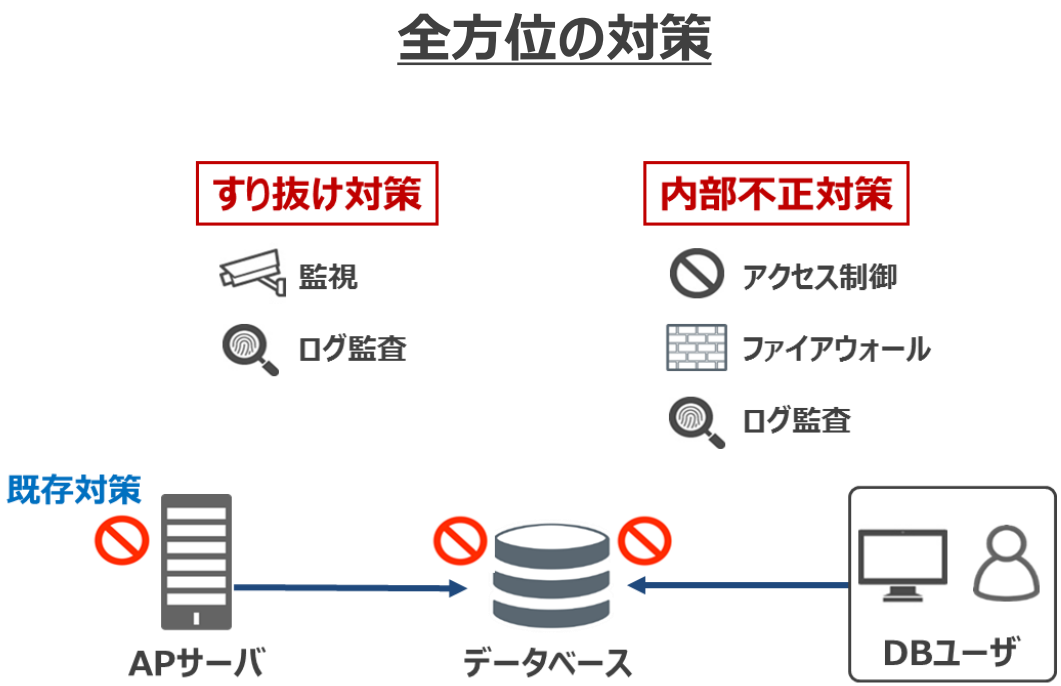
4つの対策で全方位に盲点をなくします

予防 アクセス制御
ユーザID管理・認証
アクセス権限を限定

検知 監視
リアルタイム表示
不正検知・アラート通知

防御 ファイアウォール
監視 ＋ 遮断

検証 ログ監査
ログの記録
ログの検索・レポート



全方位型データベースセキュリティとは

Chakra Maxで出来ること｜#1

4つの対策を１つのプラットホームで実現します

Chakra Maxはオールインワン

一般的な製品カテゴリー

	アクセス制御	監視	ファイアウォール	ログ監査
DB監査ツール				✔
DB監視ツール		✔		✔
DBファイアウォール		✔	✔	
DBMSの追加機能	✔			
Chakra Max	✔	✔	✔	✔

全方位型データベースセキュリティとは

Chakra Maxで出来ること｜#2

内部不正対策を強化しました

覗き見・不正コピー対策

データマスキング

機密データをマスク表示

権限悪用を防止

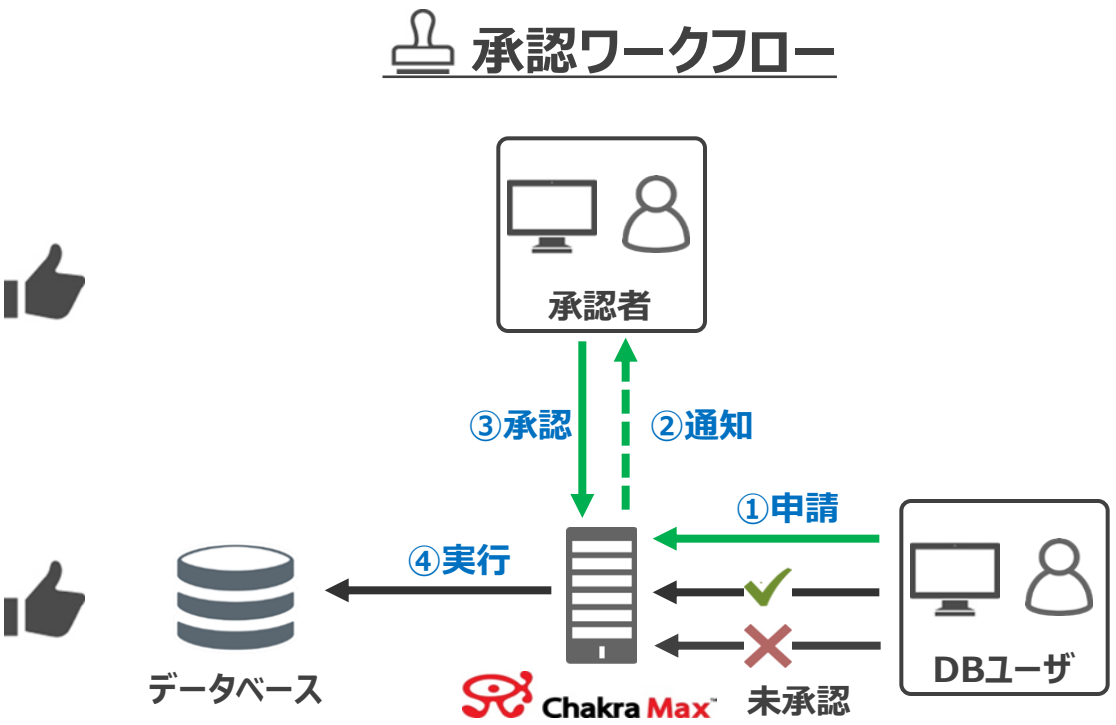
承認ワークフロー

未承認の操作を遮断

小分けにした持出しを監視

不正の兆候検知

アクセス頻度の上昇をリアルタイム検知



全方位型データベースセキュリティとは

Chakra Maxのライセンス

対策別に必要な機能をパッケージしました

Chakra Max Basic

- 監視
- ログ監査
- セッション切断
- 不正の兆候検知

すり抜け対策

Chakra Max User Control

- アクセス制御
- ファイアウォール
- ログ監査
- データマスキング
- 承認ワークフロー
- 不正の兆候検知

内部不正対策

Chakra Maxの構成

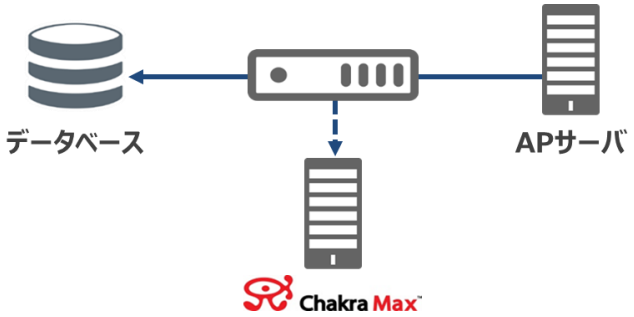
Chakra Maxの構成

基本構成

ネットワーク上で通信パケットを解析して動作します

スニフィング構成（監視）

Chakra Max Basic

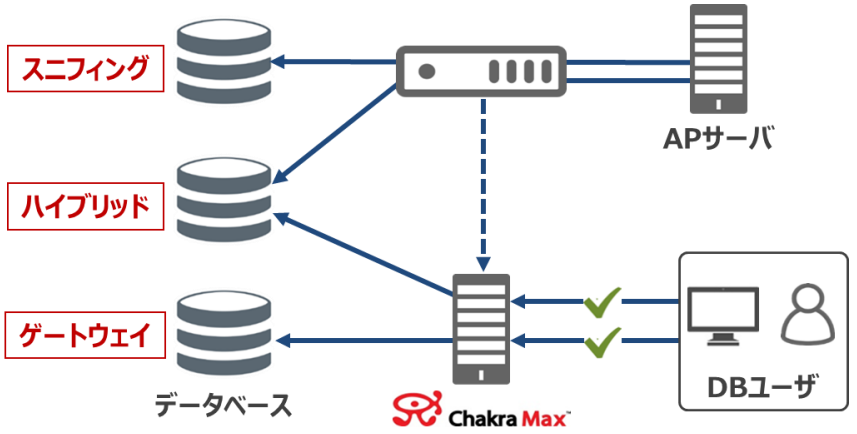


ゲートウェイ構成（ファイアウォール）

Chakra Max User Control

ハイブリッド構成

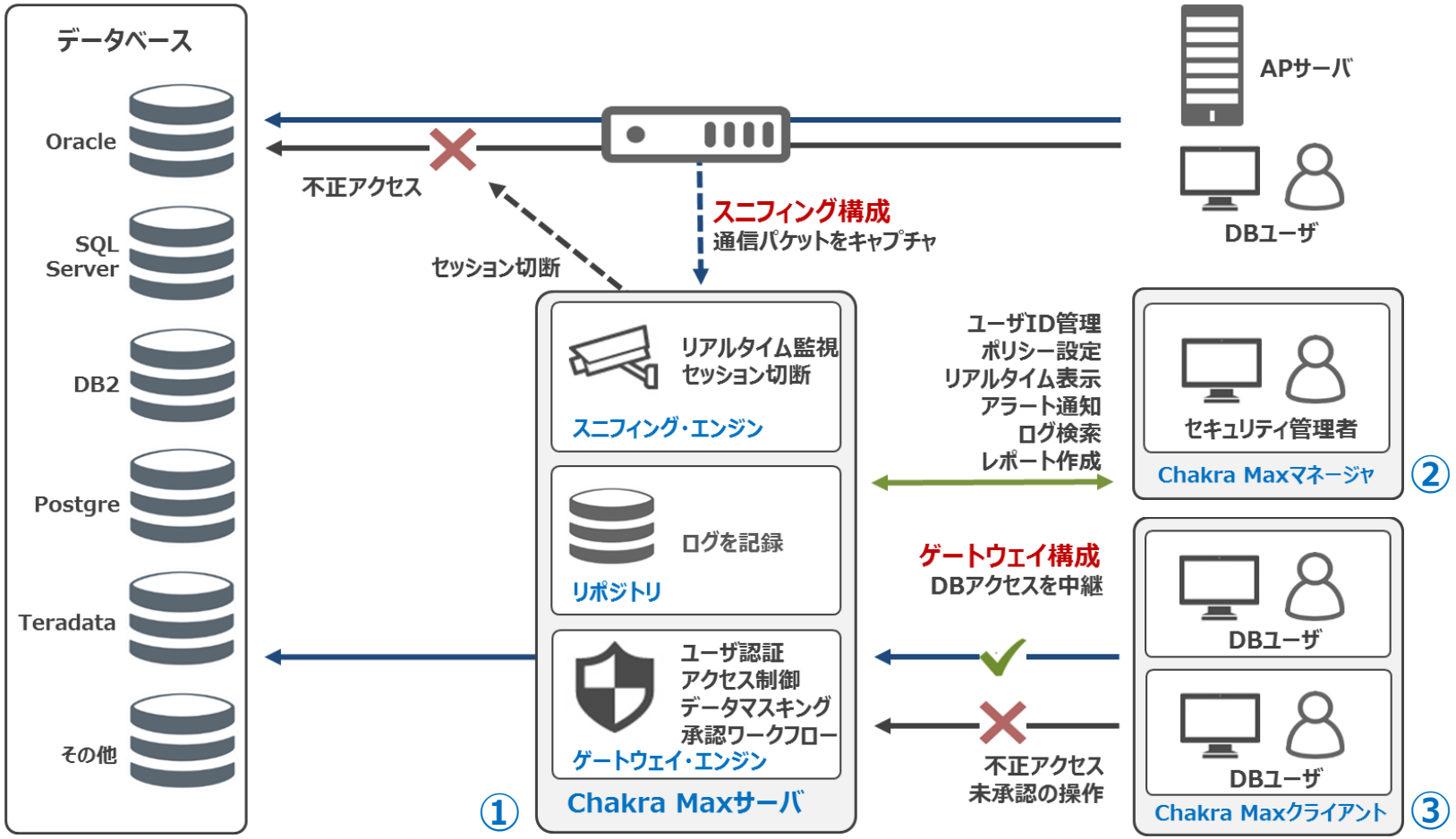
- ２つの構成が同時に動作
- 構成の組み合わせが自在



Chakra Maxの構成

構成モジュール｜動作

３つのモジュールで構成します



Chakra Maxを選択する理由

Chakra Maxを選択する理由

進化したセキュリティ技術

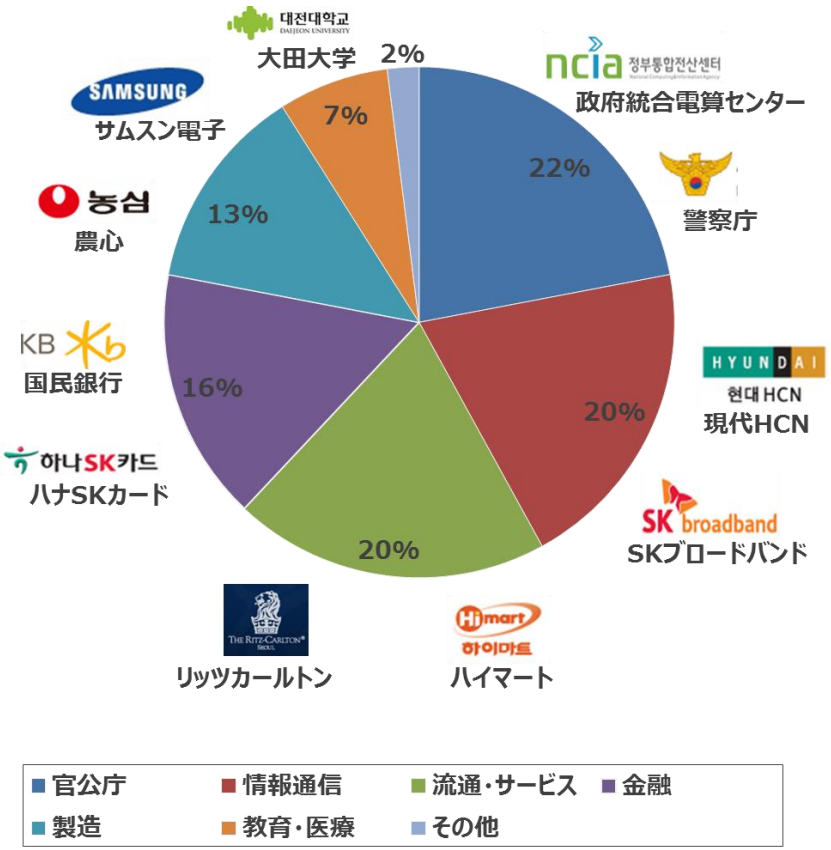
韓国版マイナンバーの経験が活きています

■ 環境からの要請
- ➢隣国からのサイバー攻撃
- ➢マイナンバー流出事件が多発
- ➢開発・普及を国が後押し

■ 実戦で鍛えたノウハウ
- ➢大手銀行と10年間の共同開発
- ➢世界最大の電子政府システムに採用

■ 豊富な導入実績
- ➢1600ユーザ／3500システム

Chakra Maxのお客様



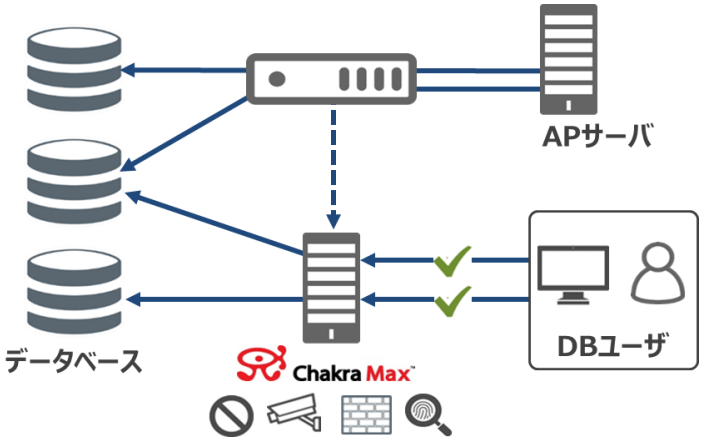
Chakra Maxを選択する理由

コストパフォーマンス

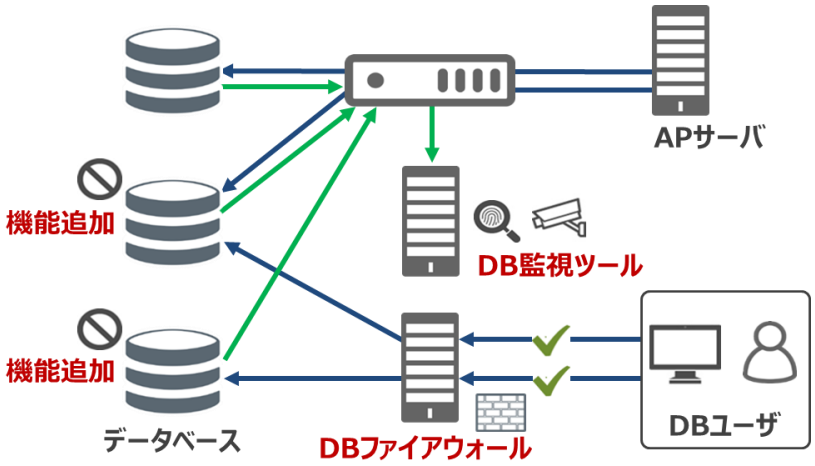
投資と管理コストの無駄をなくします

■ シンプルな構成
- ➢無駄のない投資
- ➢一元的な運用管理

■ データーベースを一括管理
- ➢最大500台
- ➢主要なデータベース全てに対応



異なる機器を組み合わせた例



よくある質問｜FAQ

#1｜よくある質問｜FAQ

マイナンバー法に対応しますか？

はい、マイナンバー法で義務付けられている以下の技術的安全管理措置に対応します。

a アクセス制御
- アクセス権を付与すべき者の最小化
- 付与する権限の最小化
- 特定個人情報ファイルの内容に対するアクセス制御

b アクセス者の識別と認証
- ユーザーID｜パスワード｜磁気･ICカード｜生体情報等

c 不正アクセス等による被害の防止等
- 不正アクセスの検知（ログの分析）
- 被害を最小化する仕組み（遮断）
- 不正な構成変更（許可されていない機器の接続、ソフトウェアのインストール等）の防止

#2｜よくある質問｜FAQ

個人情報保護法に対応しますか？

はい、個人情報保護法で義務付けられている以下の技術的安全管理措置に対応します。（マイナンバー法の記載に追加して必要な措置の例示）

①個人データへのアクセスにおける識別と認証
- ■ 端末・アドレス等の識別と認証

②個人データへのアクセス制御
- ■ 情報システムの利用時間の制限
- ■ データベースへのアクセス制御を別に実施
- ■ 特権ユーザーに対するアクセス制御

③個人データへのアクセス権限の管理
- ■ 管理者権限の分割

④個人データへのアクセスの記録
- ■ 専用サーバにログを移動｜特権ユーザのログ改ざん・不正消去対策

⑧個人データを取り扱う情報システムの監視
- ■ 個人データへのアクセス状況・操作内容の監視

#3｜よくある質問｜FAQ

対応するデータベースは？

主要なデータベース全てに対応します。

Oracle｜SQL Server｜DB2｜Symfoware｜Sybase ASE
PostgreSQL｜MySQL｜MariaDB
Teradata｜Sybase IQ｜IBM PureData System(Netezza)

動作するOSは？

Chakra Maxサーバ

- Microsoft Windows Server
- Red Hat Enterprise Linux
- Linux Cent OS

Chakra Maxマネージャ｜Chakra Maxクライアント

- Microsoft Windows
- Microsoft Windows Server

#4｜よくある質問｜FAQ

仮想化やクラウドに対応しますか？

はい、仮想化やクラウドなど、環境に応じて柔軟に構成できるソフトウェア提供です。

クラウドでは通常、ポートミラーやネットワークTAPなどパケットを収集する物理的な機器を設置することができません。このためスニフィング構成で監視する場合は、データベースサーバにエージェント（ソフトウェアTAP）を設置してパケットを収集します。

リモートアクセスを監視できますか？

はい、以下のリモートアクセスを監視できます。

セッション情報や使用されたコマンドを監視し、アラート通知やセッションの遮断・切断を行うことができます。

- TELNET｜FTP｜R-cmd｜R-login
- SSH｜RDP（ゲートウェイ構成のみ対応）

#5｜よくある質問｜FAQ

日本語対応していますか？

はい、UI・マニュアルともに完全日本語対応しています。

GUI対応していますか？

はい、コマンド入力が不要で直感的に操作できるGUIを提供します。

データベースの登録、DBユーザの登録、ポリシーの作成、レポートの作成など、ほとんど全ての設定がウィザード形式で進行します。画面に従って簡単にミスなく設定することができます。

お問い合わせはこちらまで

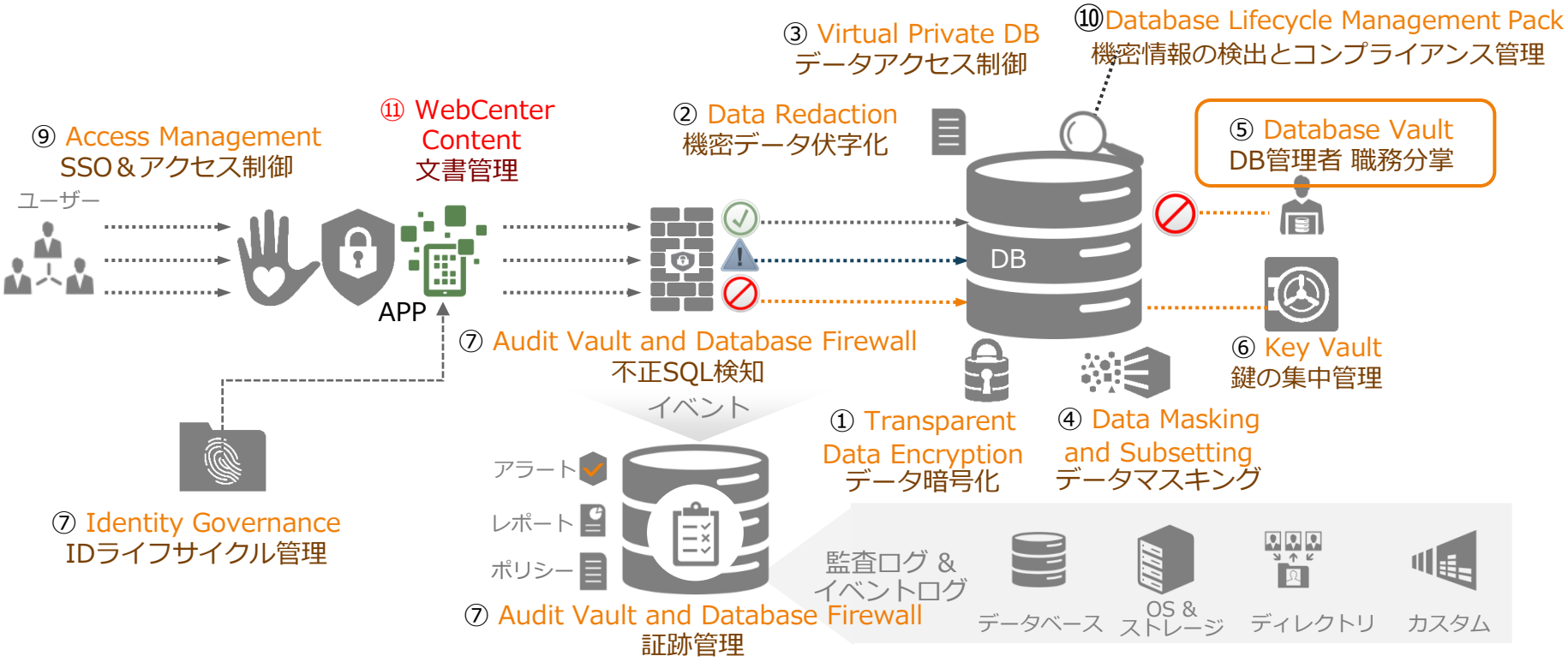
http://www.warevalley.co.jp

ORACLE DATABASE VAULT ご紹介

2016年3月9日
日本オラクル株式会社

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

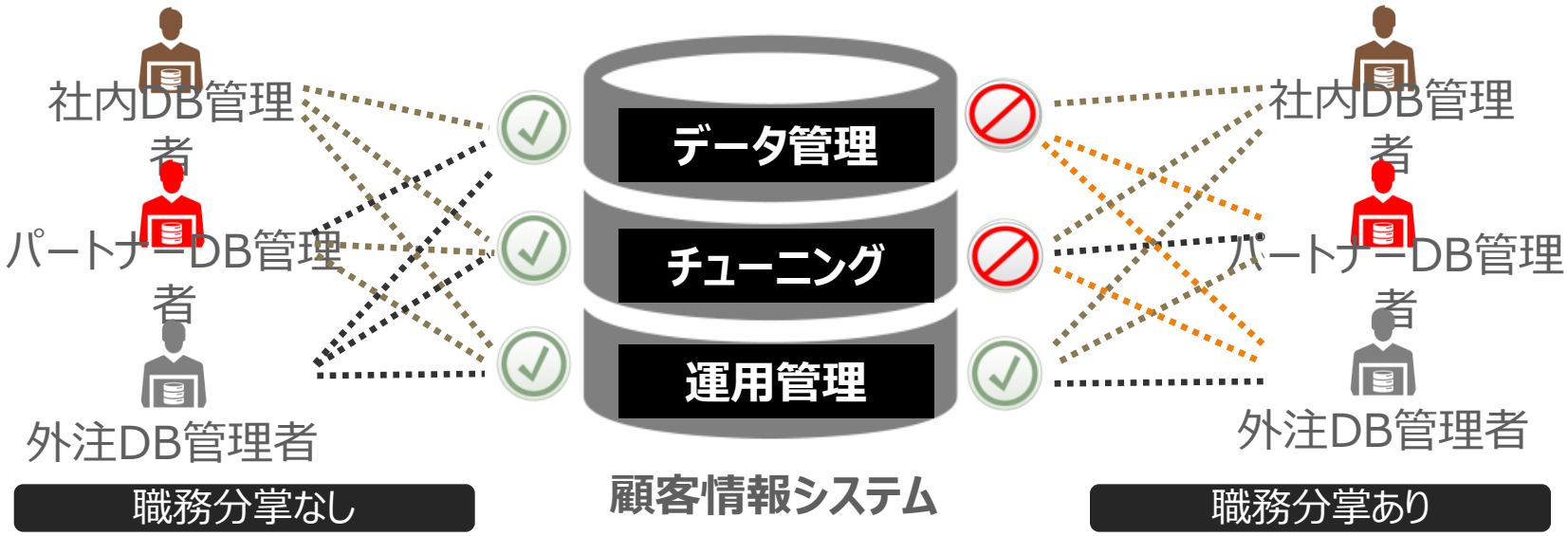
オラクルが提供するセキュリティソリューション



ご参考：オラクルが提供するセキュリティ・ソリューション機能概要

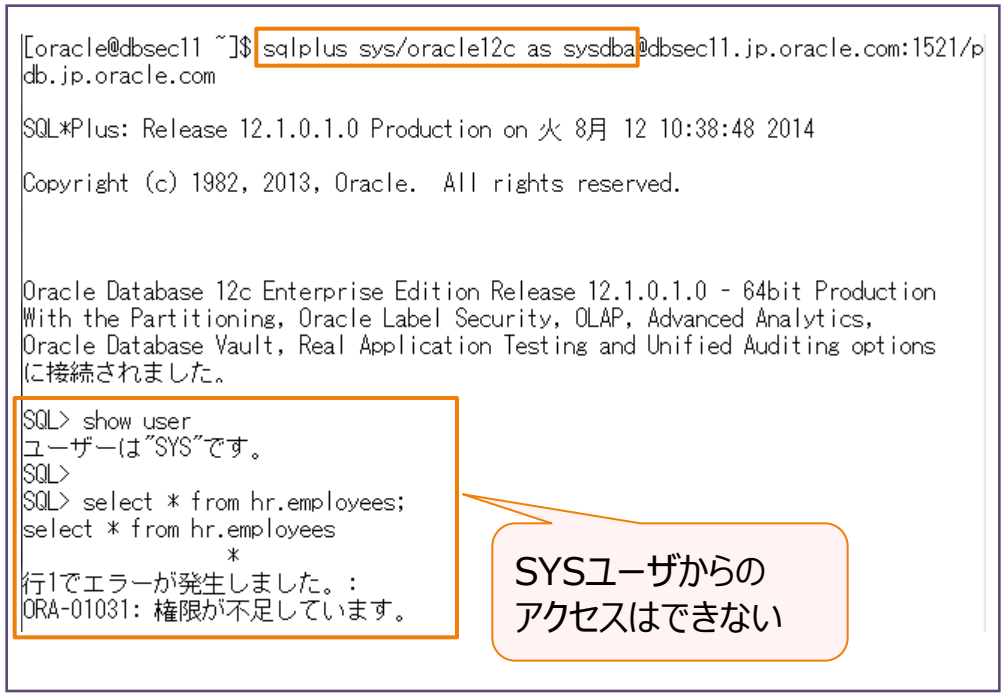
機能名	① Transparent Data Encryption	② Data Redaction	③ Virtual Private Database	④ Data Masking and Subsetting	⑤ Database Vault	⑥ Key Vault	⑦ Audit Vault and Database Firewall	⑧ Identity Governance	⑨ Access Management	⑩ Database Lifecycle Management Pack	⑪ WebCenter Content
脅威	データファイル、バックアップデータの奪取	正規利用者の業務を逸脱した不適切アクセス	正規利用者の業務を逸脱した不適切アクセス	開発・テスト環境データの奪取	DB管理者によるデータ奪取	暗号鍵の紛失	内部不正の追跡、影響範囲の調査不可能	共有特権ユーザIDを使用した不正アクセス	Webシステムに対する不正アクセス	セキュリティ設定漏れを突いた不正アクセス	営業秘密文書の不正取得と外部漏洩
機能概要	既存のアプリケーションに変更なく、透過的に本番、バックアップデータを暗号化	特定の表への参照範囲を列レベルで制限。 この機能は、データベース内で実施されるため、アプリケーション側からは透過的に利用可能。	特定の表への行・列レベルでのより厳密なアクセス制御を実現	開発・テスト環境の実データのマスキング（伏字化） ステージ環境を用意することなくExport時にマスキングデータを生成	DB管理者の業務データアクセスを制御。 特定のDB設定やパスワード変更、業務データの閲覧等を制限する	公開鍵、秘密鍵、Oracle Wallets、Javaキーストア他の集中管理 Oracle製品(データベース、ミドルウェア、OS)の鍵を一元管理	DB、OSなどのログをもれなく取得。 定常的なレポートと不正なアクセスを検知。 証跡を改ざん・削除されないようログを保全	人事情報と連動したID/権限の作成・変更・削除の自動実施 DBやOS等の特権IDに対して申請ベースでワンタイムパスワードの発行し、利用者を限定し、コマンド操作を取得	Webアプリケーションの認証一元化と部署・役職に応じたアクセス制御の実現 多段要素認証によるなりすましを防止	企業の全管理対象データベースに対してセキュリテイ未対策の機密情報、個人情報を検出 企業、業界標準のコンプライアンスフレームワークやベストプラクティスルールを利用し違反を検出し問題解決	文書を一元管理し、企業のセキュリティポリシーに対応したアクセス権限を強制適用 文書のダウンロードや更新などの各種操作をログとして蓄積。
使途	本番データ、バックアップファイルに含まれる情報を保護	参照時における列レベルでの伏字化	参照、更新時における行・列レベルでのアクセス制御	テスト、開発環境の情報を保護	データベース管理者の職務分掌 業務データにアクセスさせない	暗号化した本番、バックアップデータの暗号鍵を管理、保全	DB、OSなど、網羅的な監査証跡の取得、管理	個人ID管理の厳格化 OS, DBなどの共有特権ID管理、監査の厳格化	Webアプリケーションの認証とより厳密なアクセス制御	セキュリティ対策が不十分な機密情報を検出し可視化 コンプライアンス基準への対策証明	営業機密となる文書の一元管理と保護

データベース管理者からの機密情報の閲覧を遮断



- 職務分掌　| 特権ユーザー（SYS、DBA権限）であっても情報にはアクセスさせない。管理権限も分割
- 透過的　| 既存アプリケーションの変更不要、12c Multitenant Architecture対応
- 厳密　| ユーザー、クライアント情報（IPアドレス、言語、他）、時間を組み合わせポリシー設定

データベース管理者のアクセス制御例



たとえ、すべての表へのアクセス権限(SELECT ANY TABLE)をもつデータベース管理者であっても、Database Vaultで保護された表にはアクセス不可能

アクセスするためにはデータベース管理者とは別のセキュリティ(Database Vault)管理者からの認可が追加で必要

アクセスの失敗は監査ログとして残るため、管理者による不正アクセスをいち早く発見可能

詳細なルール設定によるアクセス制御

- 表へのアクセスやコマンドの実行ごとに詳細な実行条件を設定可能
- コマンド実行のためのオブジェクト権限・システム権限は別途必要

マイナンバー対応事例

- 「特定個人情報の適正な取り扱いに関するガイドライン」で定められている安全管理措置要件を実現するためにOracle Databaseのオプション製品群を利用
  - Oracle Advanced Security (暗号化)
  - Oracle Database Vault (特権管理)
  - Oracle Audit Vault and Database Firewall (ログ取得・分析)

SBIトレードウィンテックとODKソリューションズが提供する金融機関向けクラウド型マイナンバー管理システムに、オラクルのセキュリティ製品群を導入

特定個人情報データに関する安全管理措置の基準を満たす高セキュリティ環境をクラウドで提供

Tokyo, Japan—2016/03/01

SBIトレードウィンテック株式会社(本社:東京都新宿区、代表取締役執行役員社長:中尾哲也、以下SBIトレードウィンテック)と株式会社ODKソリューションズ(本社:大阪府大阪市、代表取締役社長:西井生和、以下ODKソリューションズ)、日本オラクル株式会社(本社:東京都港区、代表執行役社長兼 CEO:杉原博茂、以下日本オラクル)は本日、SBIトレードウィンテックとODKソリューションズが共同開発した金融機関向け「マイナンバー管理システム」のセキュリティ対策のため、オラクルのデータベース・セキュリティ製品群を導入したことを発表します。

社会保障・税番号制度(以下マイナンバー制度)が施行され、「社会保障」と「税」、「災害対策」の3分野を皮切りに制度の運用が始まったことに伴い、金融機関においても顧客のマイナンバー情報を含む特定個人情報のデータを「特定個人情報の適正な取扱いに関するガイドライン」に沿って安全かつ厳格に管理することが求められています。また、ガイドラインが定める安全管理措置の基準を満たすためには、マイナンバー情報の管理体制整備や、システムのセキュリティ面の強化など、金融機関にとって大きな負担を要していました。

金融機関向けのパッケージソフトウェアおよびコンサルティング、アウトソーシングサービスを提供するSBIトレードウィンテックと、証券会社向けの各種システムによるバックオフィス業務サポートやアウトソーシングサービスを提供するODKソリューションズは、マイナンバー制度対応支援サービスの一環として共同開発し、クラウド・サービスとして提供する「マイナンバー管理システム」を、2016年1月に提供開始しました。両社は、安全管理措置に沿って金融機関が収集したマイナンバーを安全に管理できる高セキュリティ環境を構築できるソリューションを検討した結果、オラクルのデータベース・セキュリティ製品群の信頼性と実績を評価し、2015年5月に導入を決定しました。本サービスは、証券会社、生命保険会社、損害保険会社、海外送金サービス会社等、金融業界に幅広く利用されており、今後は一般事業会社、学校法人への展開も予定しています。

「マイナンバー管理システム」のシステム基盤に導入されたオラクルのデータベース・セキュリティ製品は、「データの暗号化を行う「Oracle Advanced Security」、特定個人情報に対するアクセス制御／権限管理を行う「Oracle Database Vault」、アクセスログの取得・監視を行う「Oracle Audit Vault and Database Firewall」等によりマイナンバーを格納するデータベースに求められる安全管理措置(特定個人情報保護委員会発行の「特定個人情報の適正な取扱いに関するガイドライン」にて定められる要件)を実現しました。

https://www.oracle.com/jp/corporate/pressrelease/jp20160301.html

オムニチャネル統合基盤保護のための施策事例

- オムニチャネル統合IT基盤を保護するためにOracle Databaseのオプション製品群を利用
  - Oracle Advanced Security (暗号化)
  - Oracle Database Vault (特権管理)
  - Oracle Audit Vault and Database Firewall (ログ取得・分析)

セブン&アイ・ホールディングス、オムニチャネル戦略の本格展開を支えるIT基盤をオラクル製品で構築

グループ横断型の新通販サイト「omni7」をはじめネットビジネスとグループ傘下の実店舗を連携させ、個々の顧客に最適なサービスを提供

Tokyo, Japan—2015/10/29

日本オラクル株式会社(本社:東京都港区北青山、代表執行役社長 兼 CEO:杉原 博茂、以下 日本オラクル)は本日、株式会社セブン&アイ・ホールディングス(本社:東京都千代田区二番町、代表取締役会長 最高経営責任者(CEO):鈴木 敏文、以下 セブン&アイHLDGS.)が、同社のオムニチャネル戦略を支えるIT基盤として、クラウドやハードウェアとソフトウェアを一体化することにより、あらかじめ最適に動作するよう設計されたオラクルのエンジニアド・システムをはじめとする製品群を包括的に導入し、このたび稼働開始したことを発表します。

セブン&アイHLDGS.では、「いつでも、どこでも、スムーズに、お客様が求める商品を購入でき、人に紹介したくなるサービス」をコンセプトに、セブン-イレブンをはじめとする国内1万9,000以上の店舗とインターネット販売を融合させるオムニチャネルの構築を、経営戦略の柱として推進しています。2015年11月1日には、グループ横断型の新通販サイト「omni7(オムニセブン)」を開設し、セブン-イレブンやイトーヨーカ堂、そごう・西武などグループ企業の商品約180万品目を販売する予定です。また、セブン-イレブンの店頭に専用の注文端末を設置し、店舗での受け取りも可能とすることで、ネットと実店舗を融合させた、いつでもどこでも買い物を楽しめる環境を提供します。

セブン&アイHLDGS.は、このようなネットとリアルの融合と複数事業体のシームレスな連携を可能にするオムニチャネルを実現するため、IT基盤を新たに構築しました。このたび稼働開始した新オムニチャネル統合基盤においては、ネットや実店舗から発生する膨大なデータをセキュアに蓄積、管理、分析するとともに、高速なアプリケーション基盤と高機能なWebサイトを構築するために、オラクルのエンジニアド・システムやクラウドなど最先端の技術を駆使したオラクル製品の包括的な導入しています。オラクル製品によって構築される統合IT環境の優位性、それによってもたらされる運用管理のサービスレベル向上と効率化、高い性能に加え、オラクルのグローバルでの実績を高く評価した結果、幅広い製品群の採用を決定しています。

このたび導入されたオラクル製品は以下の通りです。

(中略)

- **セキュリティ:**不正アクセスなどの外部攻撃や内部不正からデータベースを保護する「Oracle Audit Vault and Database Firewall」、データベースを暗号化し保護する「Oracle Advanced Security」、データベースへのアクセス制御によりデータの整合性とプライバシーを保護する「Oracle Database Vault」

https://www.oracle.com/jp/corporate/pressrelease/jp20151029.html

Integrated Cloud

Applications & Platform Services


ORACLE®

NECの内部不正対策ソリューションご紹介

日本電気株式会社
プラットフォームサービス事業部 エキスパート
山内　悟

内部不正対策のポイント

不正をさせない仕組み作りが重要

不正行為の発生 ＝ 《動機》 × 《機会》 × 《正当化》

- 《動機》：行動や意思を決定する際の心理的な直接のきっかけ、原因、目的
- 《機会》：管理や制限がない等で不正が可能な状況や環境がある状態
- 《正当化》：責任転嫁や都合の良い解釈により、理にかなっているようにみせること

マネージメントによる対策

- ルールの策定　：複数管理者、二重チェック
- ルールの周知　：教育等による意識付け
- 作業の記録　：ログ、監視カメラ(抑止効果)
- 記録の監査　：不正チェック
- ：

＋

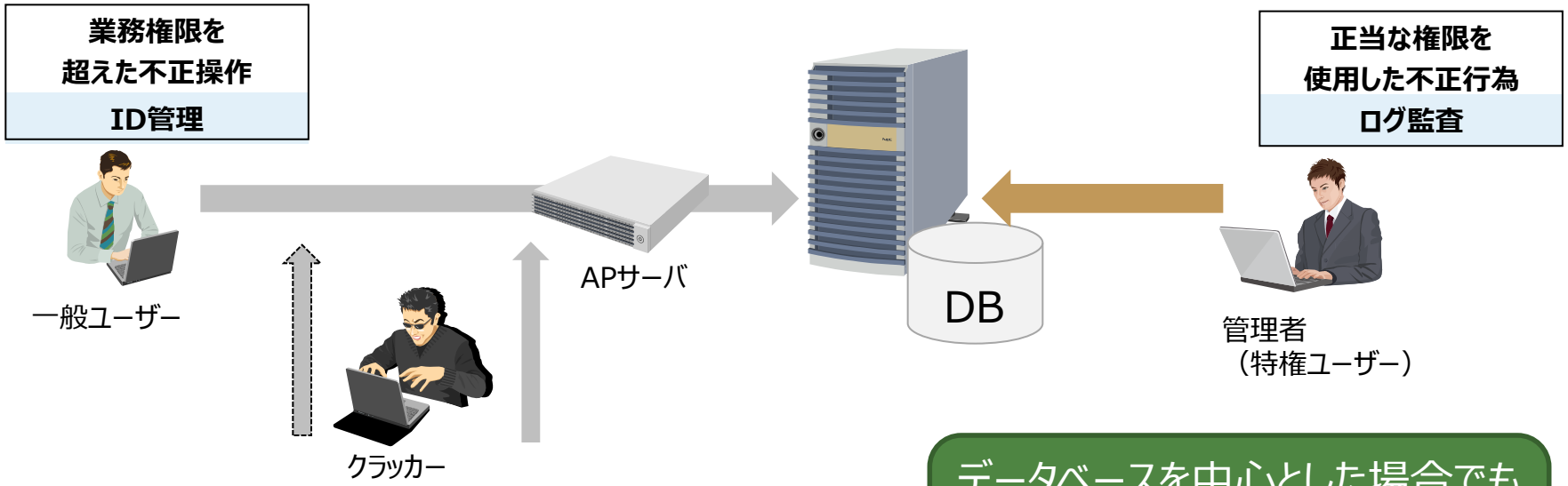
ITによる対策

- データの暗号化
- 管理者権限の分離
- アクセス制御、監視
- 持ち出し制御
- ：

⇒ 不正行為3条件を断ち切る

IT対策における悩み

１つの製品で全てを対策するのは困難



データベースを中心とした場合でも
複数のセキュリティ対策の検討が
必要

各製品機能をうまく組み合わせ、漏れがない・運用負担が少ない
効率的なセキュリティ強化が望まれる

NECが提供するソリューションの特長

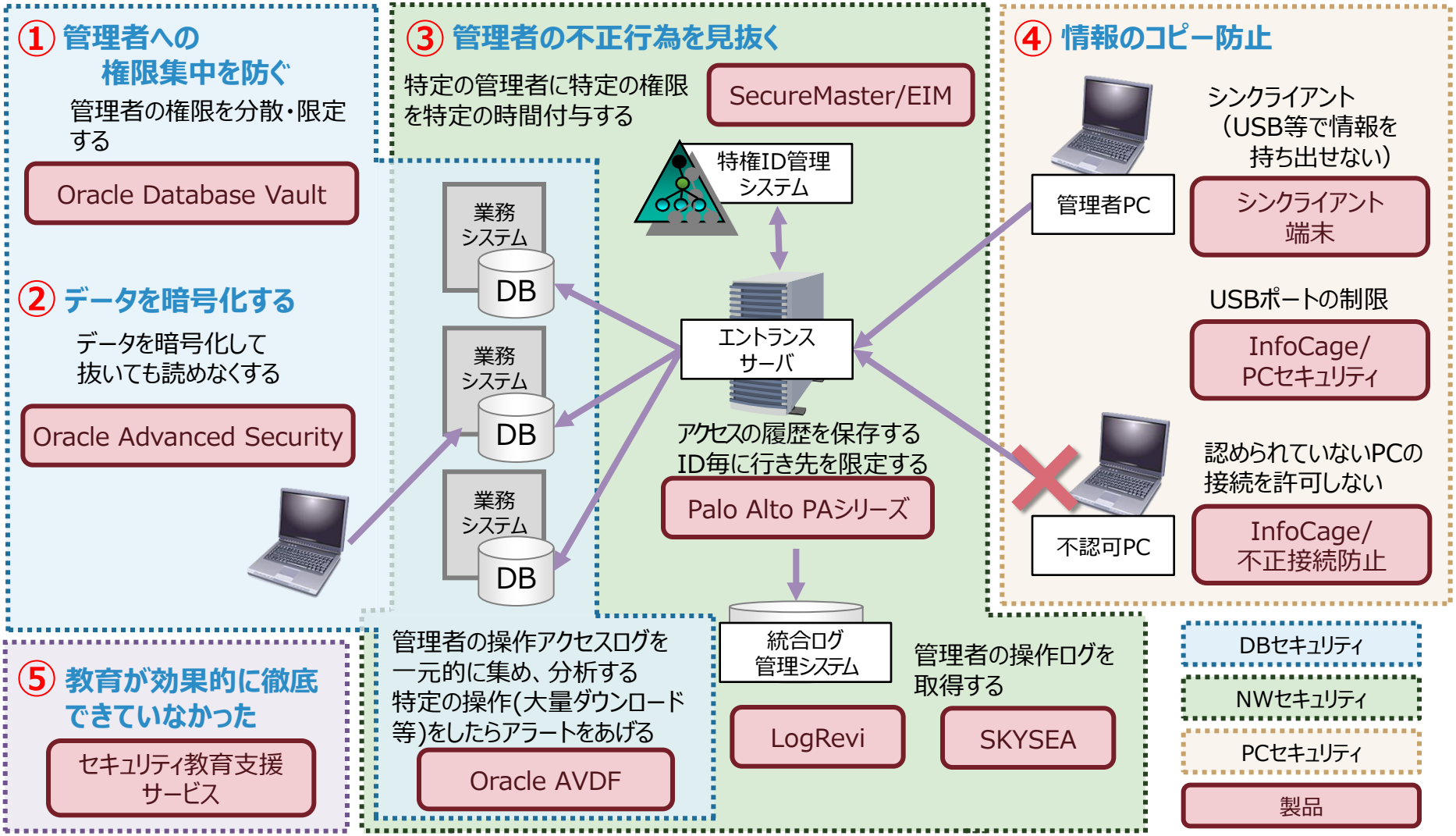
複数の製品・機能の組み合わせを検証済み

- ソリューションを適用するターゲット像を想定
- 実運用を想定したシナリオを検討
- シナリオに合った製品・機能の組み合わせを選定
- 実機にて対策の効果を検証
- 検証により有効なパラメータ設定・ポリシーを確認

各製品機能をうまく組み合わせ、漏れがない・運用負担が少ない
効率的なセキュリティ強化が実現可能

内部不正対策ソリューション全体イメージ

《管理者の内部不正による情報の持ち出しを多層で防御》

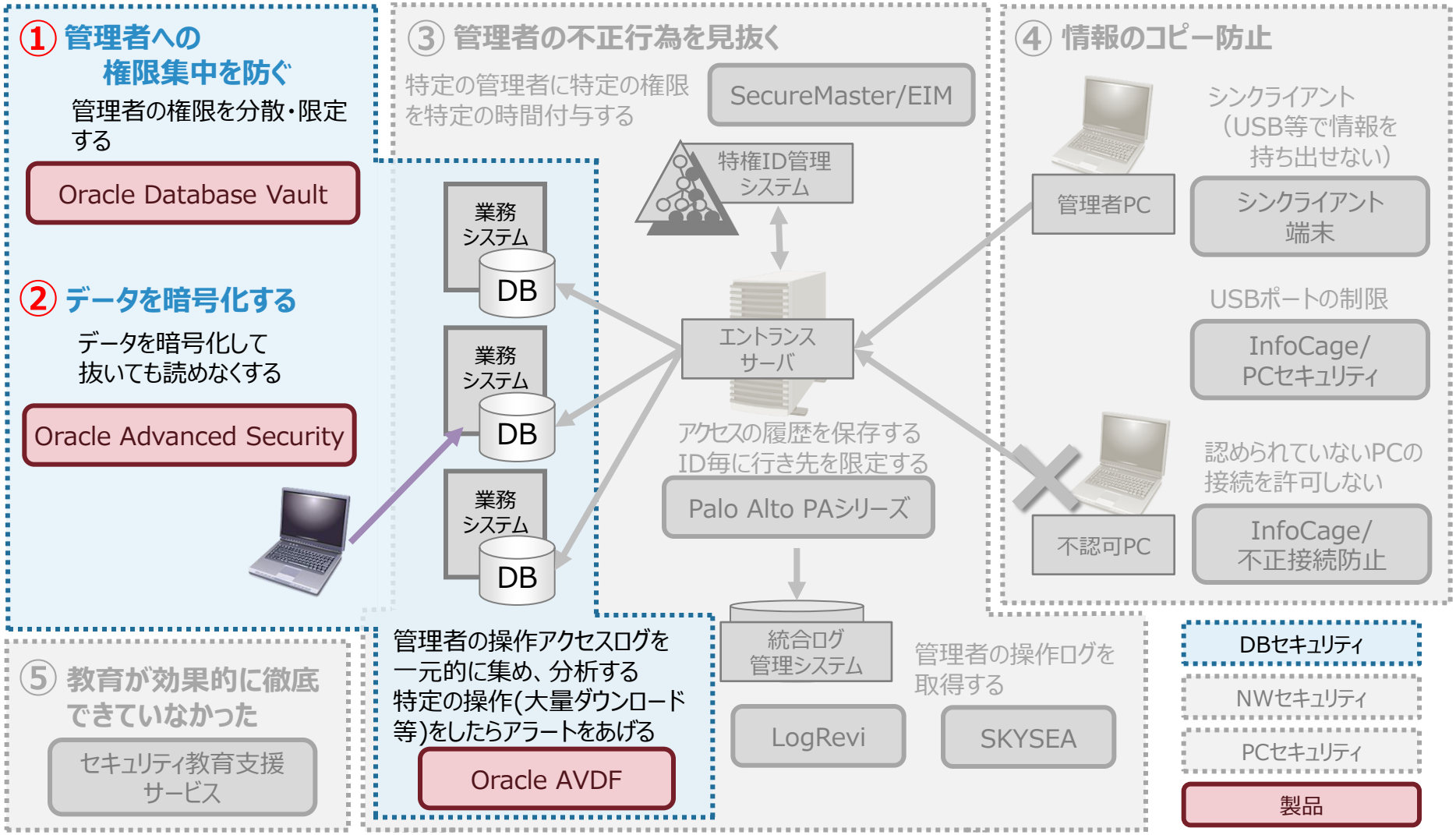


本ソリューションの想定ターゲット像

DBを扱うシステムを自社で管理する事業者

- 顧客層
  - マイナンバー等の個人情報、秘匿性の高い情報を取り扱う事業者（業種横断）
  - Oracle Database Enterprise Editionが導入済み
- 運用イメージ
  - 管理者：5～10人
  - ログは、基本的に24時間365日保管する
  - 管理者がアクセスする時間帯は日中9:00～17:00
- その他
  - 管理者は、急に増やせない
  - 管理者以外のエンドユーザ（AP利用者）の不正行為は、AP側で対策する

内部不正対策ソリューション《DBセキュリティ対策》



DBセキュリティ 対策方針

システム管理者が不正にデータアクセスしないよう適切な権限を付与

- 特権アカウントの権限を不正使用できないよう、DBの特権アカウントを廃止し、システム管理者の業務に必要な権限のみを付与（権限分掌）

システム管理者がアクセス可能なデータを不正取得しないようデータマスキングやアクセス監視による抑止で対応

- データメンテナンス等の管理者業務で参照する必要のない重要データはマスキングすることで不正取得を防止
- 管理者業務で重要データを参照する必要がある場合は、管理者の操作を監視し、不正な操作(兆候)を検知

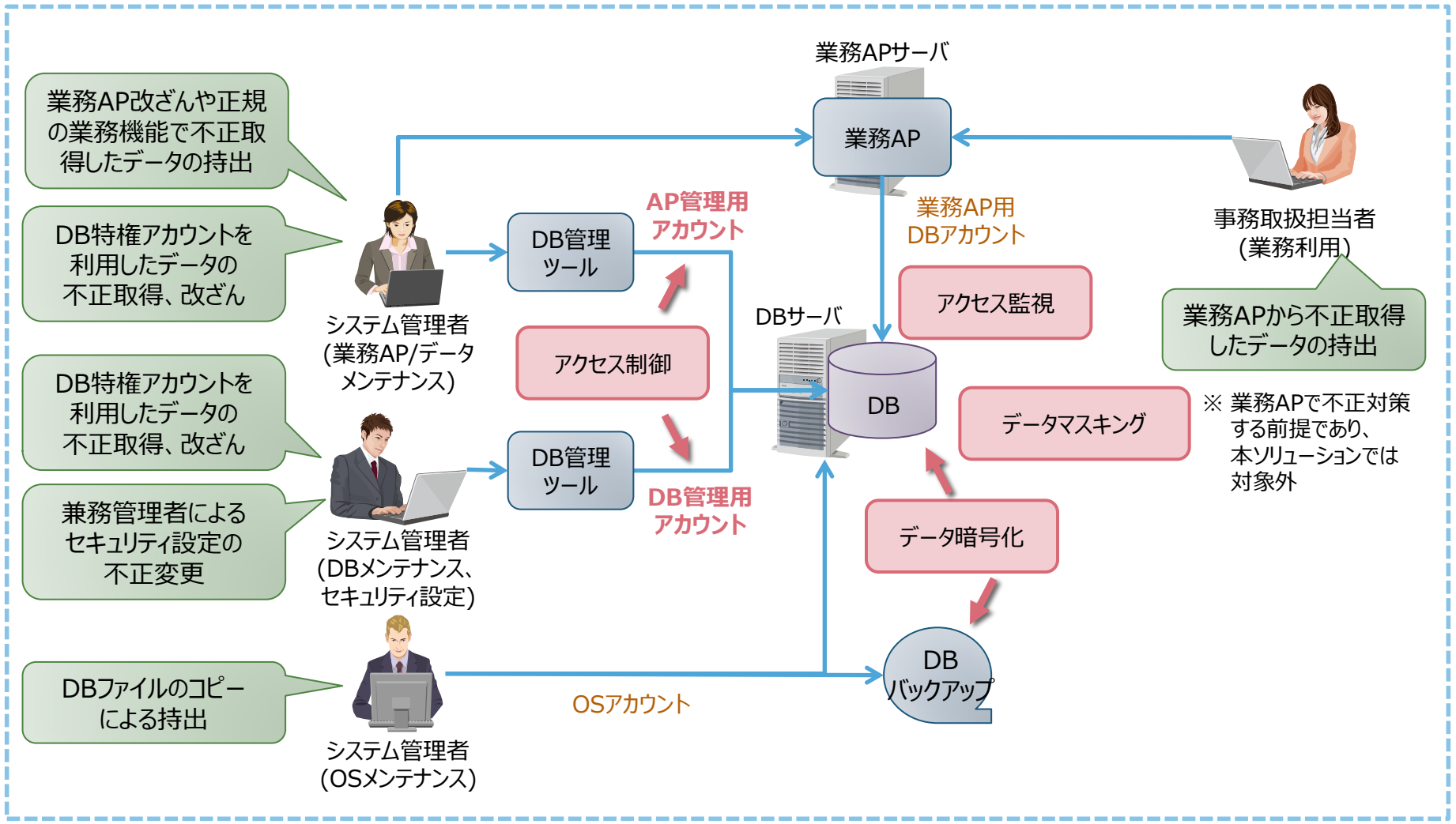
システム管理者がDBファイルを持ち出してもデータ参照不可

- DBファイルのコピーやバックアップしたファイルを持ち出しても、データを　暗号化することで、データの参照を防止

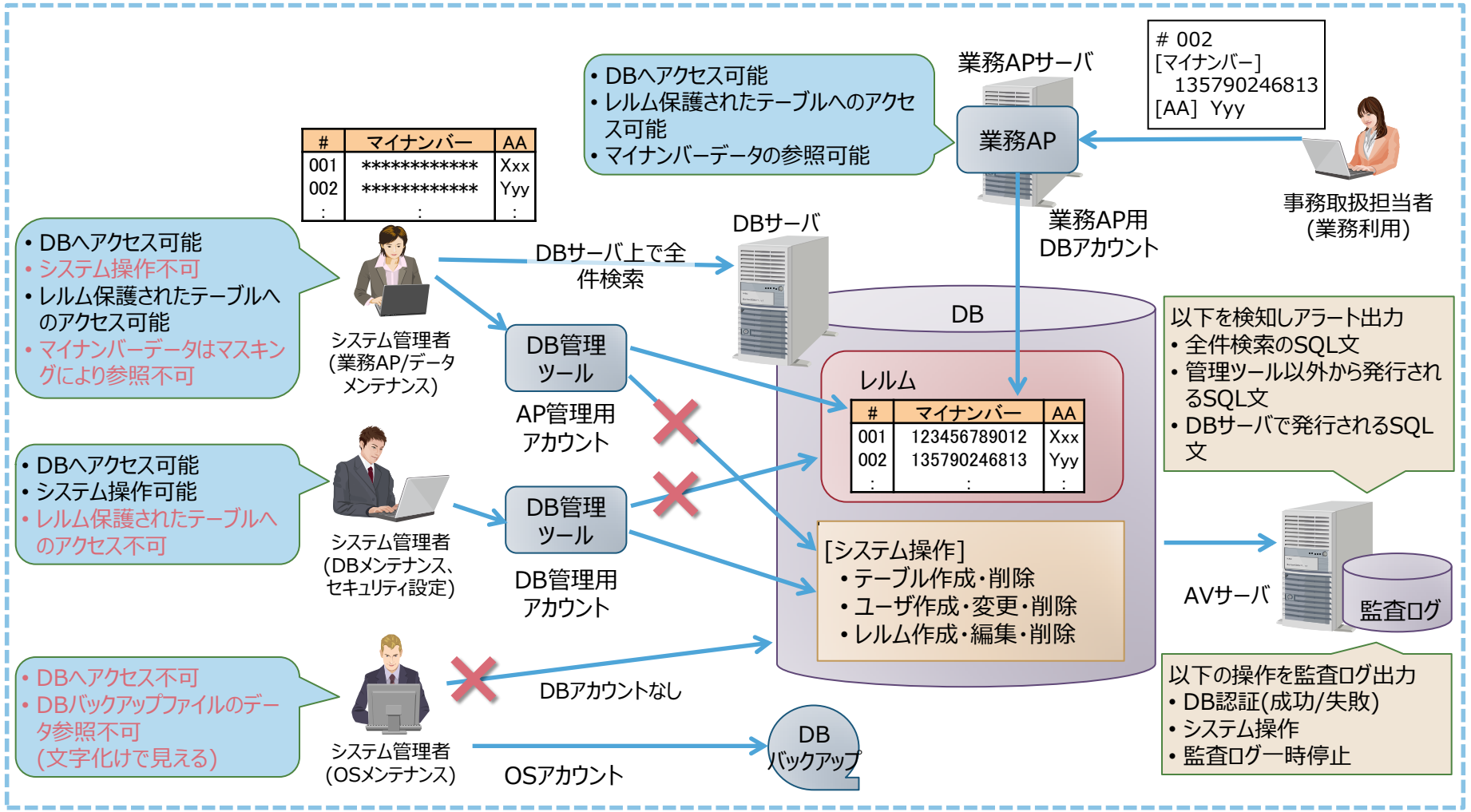
兼務管理者がDBセキュリティ設定を不正に変更しないよう抑止

- 兼務管理者の操作の監査ログを収集し、不正操作を抑止

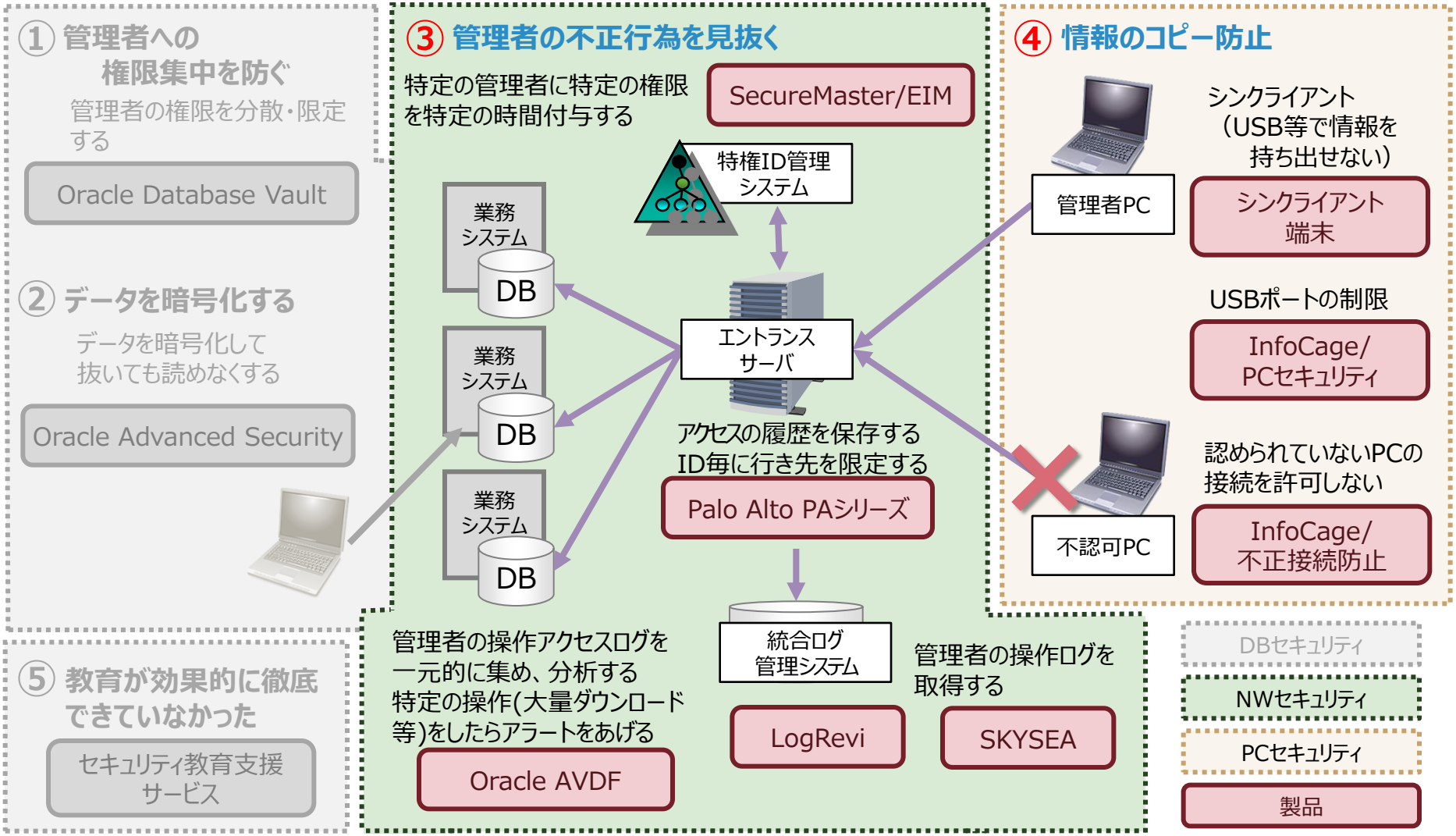
DBアクセス者毎の脅威とセキュリティ対策



セキュリティ対策適用後の効果（例）



内部不正対策ソリューション《PC&NWセキュリティ対策》



PC&NWセキュリティ 対策方針

DBから抜き出したデータを外部に持ち出さないよう、PC側で対策

- シンクライアントを導入し、仮想PCから物理PCへのデータの取得（ダウンロード）を禁止
  管理業務は仮想PCから業務サーバへアクセスする
- PCのUSBポートを制限し、私物のUSBメモリ等、許可されていない機器の接続を禁止
- ネットワークへ接続するPCを管理し、私物のPC等、認可されていないPCによるアクセスを遮断
- 管理者の操作をログ（画像とテキスト）として取得することで、不正操作を抑止

管理者による業務に必要のない管理サーバへのアクセスを制限

- 管理サーバへアクセスできる特権IDを一元管理
- 管理者の業務は全て電子申請制とし、管理者の作業（「いつ」「だれが」「どこで」「なにを」するか）を管理
  作業申請に基づき、管理者は、申請した時間、サーバ以外ではアクセスできないよう制限
- 運用上、アクセス制限できない場合は、管理サーバへのアクセスログを収集し、電子申請と突き合わせることで、不正なアクセスを検知し、アラートを通知
- 不正アクセスのあった管理者の操作内容を、監査ログや操作ログで確認

作業申請による管理者のアクセス制御・監視の仕組み

管理者の作業を管理することにより、不正な操作を抑止

① 作業申請

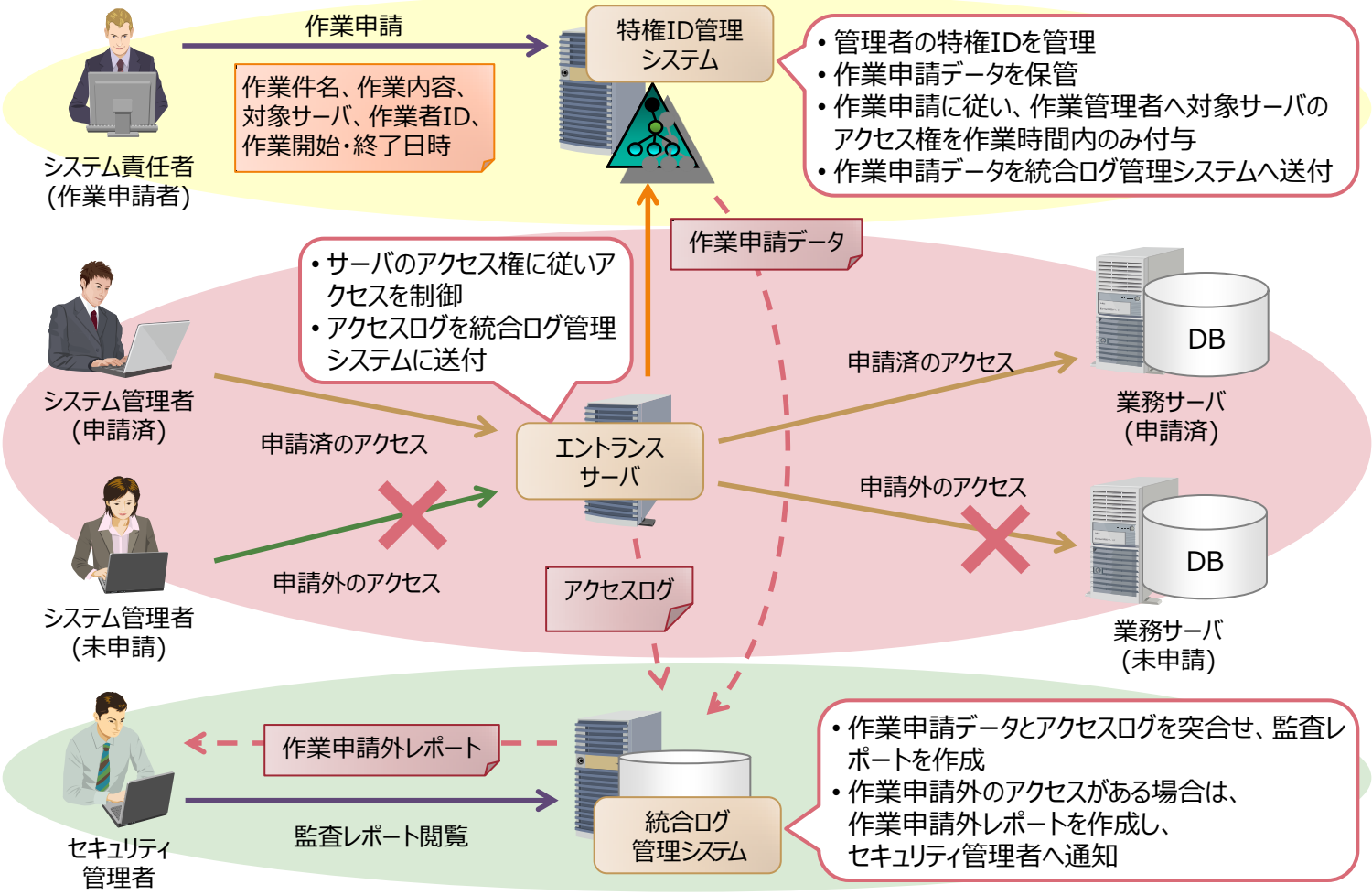
- システム責任者が、事前に作業申請を実施します

② アクセス制御

- システム管理者が、申請された作業を 実施します
- 申請したサーバ以外へのアクセス、申請した管理者以外によるアクセス、申請した時間外のアクセスは制御されます

③ アクセス監視

- 申請外のアクセスは自動的にセキュリティ管理者へ通知されます
- 管理者の作業状況を監査レポートで確認できます



まとめ

- 内部不正へのセキュリティ対策はNECにおまかせください
- 機密データが格納されるデータベースを中心としたセキュリティ対策に限らず、トータルセキュリティをNECではご提供可能です
- 各セキュリティ製品の特徴や組み合わせを把握し、これまでの対応実績からお客様業務に適したセキュリティ・ポリシー作成をご支援致します

NECの内部不正対策ソリューションの
ご利用をぜひご検討ください

詳細・お問い合わせはこちら

http://jpn.nec.com/cybersecurity/solutions/insider.html

ご清聴ありがとうございました。