
ORACLE®

#odddtky

Oracle DBA & Developer Days 2014

オラクル・コンサルが語る！ データベース・セキュリティ 攻めと守りの極意

日本オラクル株式会社
テクノロジーコンサルティング統括本部
スタッフコンサルタント 小野真樹子、土門大貴

for your **Skill**

使える実践的なノウハウがここにある

Oracle
DBA & Developer Days
2014

ORACLE

- 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。

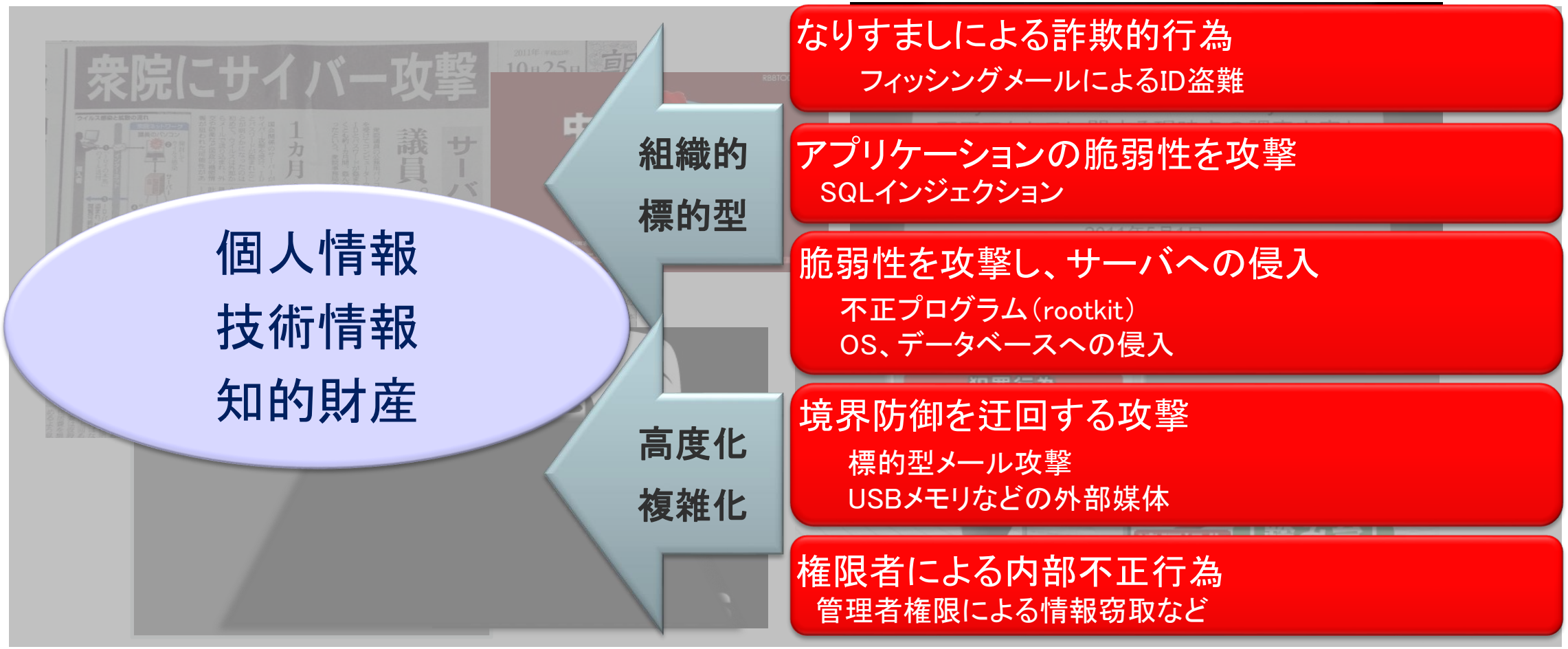
アジェンダ

1. 情報セキュリティとは
2. DBセキュリティ製品のご紹介 – Oracle Database Vault
3. DBセキュリティ製品のご紹介 – Oracle Audit Vault and Database Firewall
4. セキュリティ製品導入プロジェクトのご紹介について

情報セキュリティとは

昨今の情報セキュリティ問題

発見と予防の重要性が高まっている



セキュリティインシデントによる影響

罰金
または
罰則

行政指導

各種対応の増加

ブランド
イメージ低下

インシデント
対応

顧客離れ

会社業績、さらには
企業存続も左右する

不必要経費の増加

情報セキュリティをどう考えるか？

多層防御の考え方

•物理層、境界層での対策を行いつつも、侵入されることを前提に、アクセス層、エンドポイント層と、複数階層でセキュリティ対策を行う

階層 0:物理セキュリティ

データセンター、サーバ、ネットワークへの物理アクセス制限、媒体管理等の物理的な防御

階層 1:境界セキュリティ

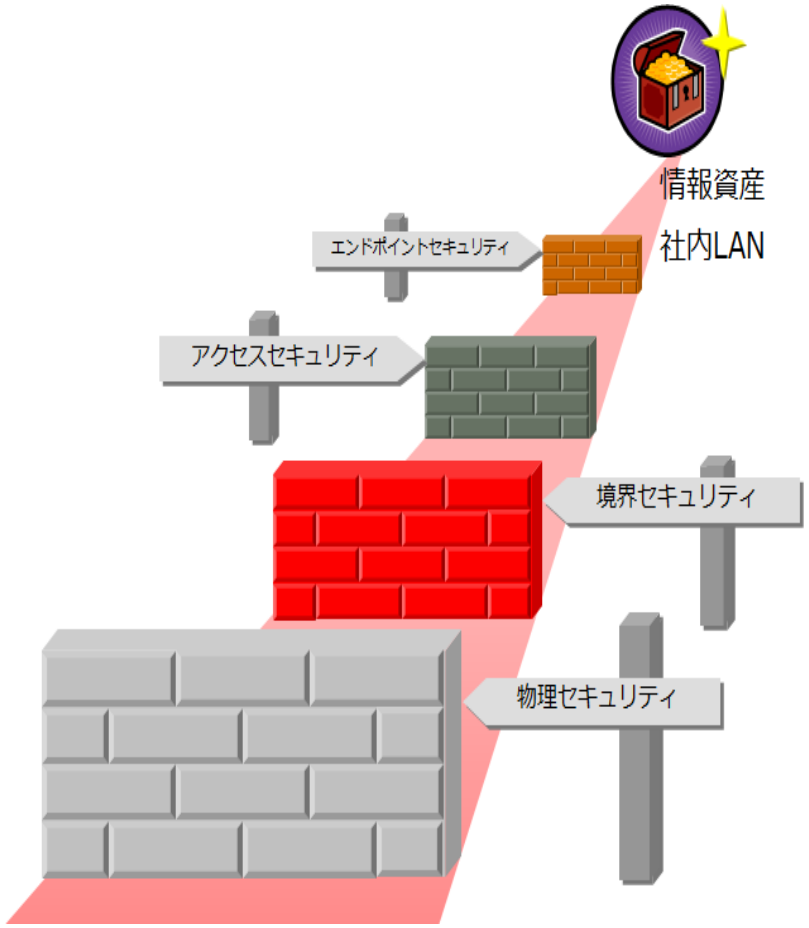
ファイアウォール、ゲートウェイ、侵入検知／防止や等のネットワーク境界での防御

階層 2:アクセス・セキュリティ

認証・アクセス制御、通信路の暗号化など、ネットワーク内部でのアクセス制御、情報漏えい防止

階層 3:エンドポイント・セキュリティ

情報の暗号化や情報への特権ユーザのアクセス制限等による、最後の砦である情報資産や監査証跡の保護

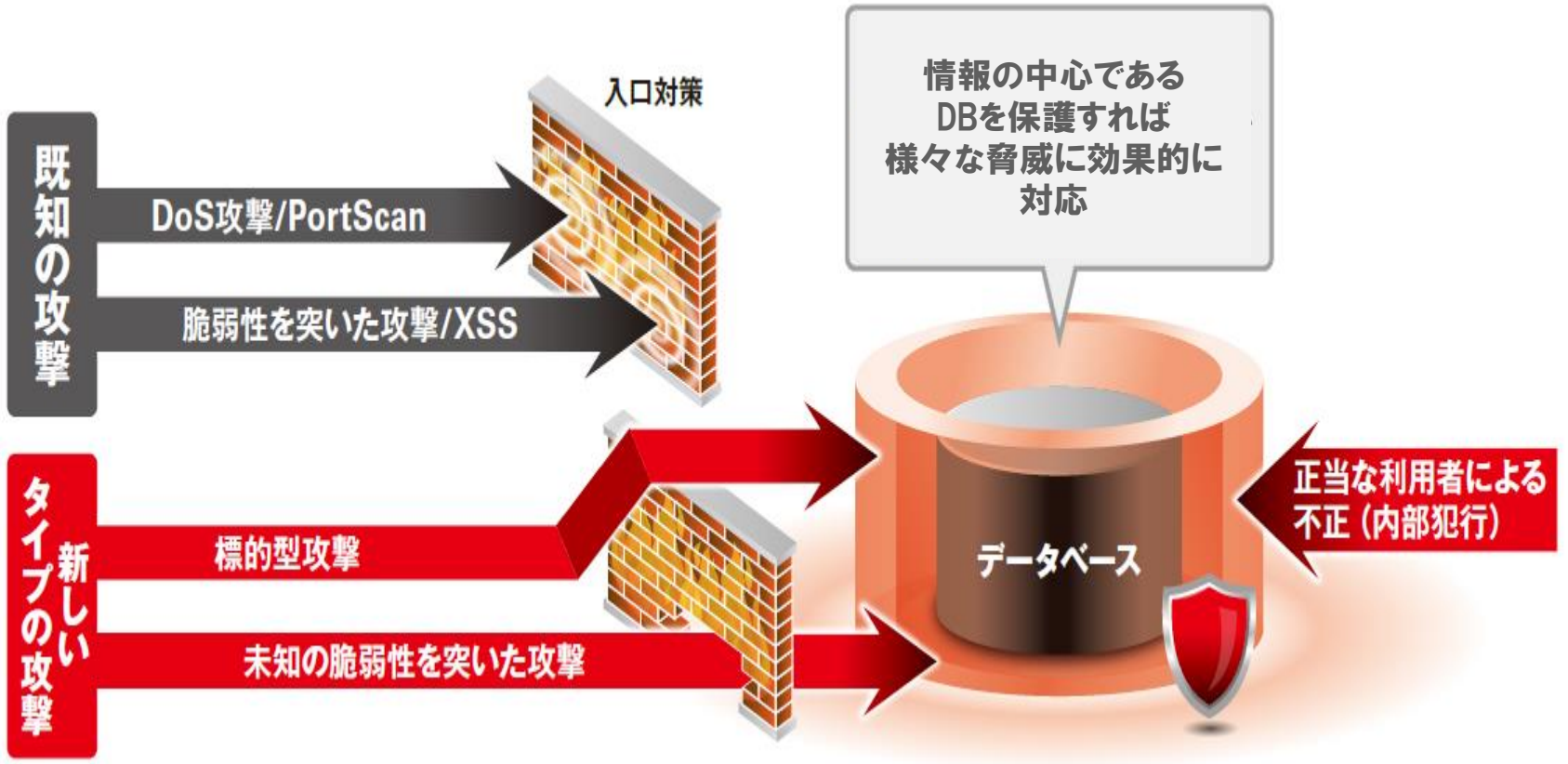


情報保護におけるDBセキュリティの重要性

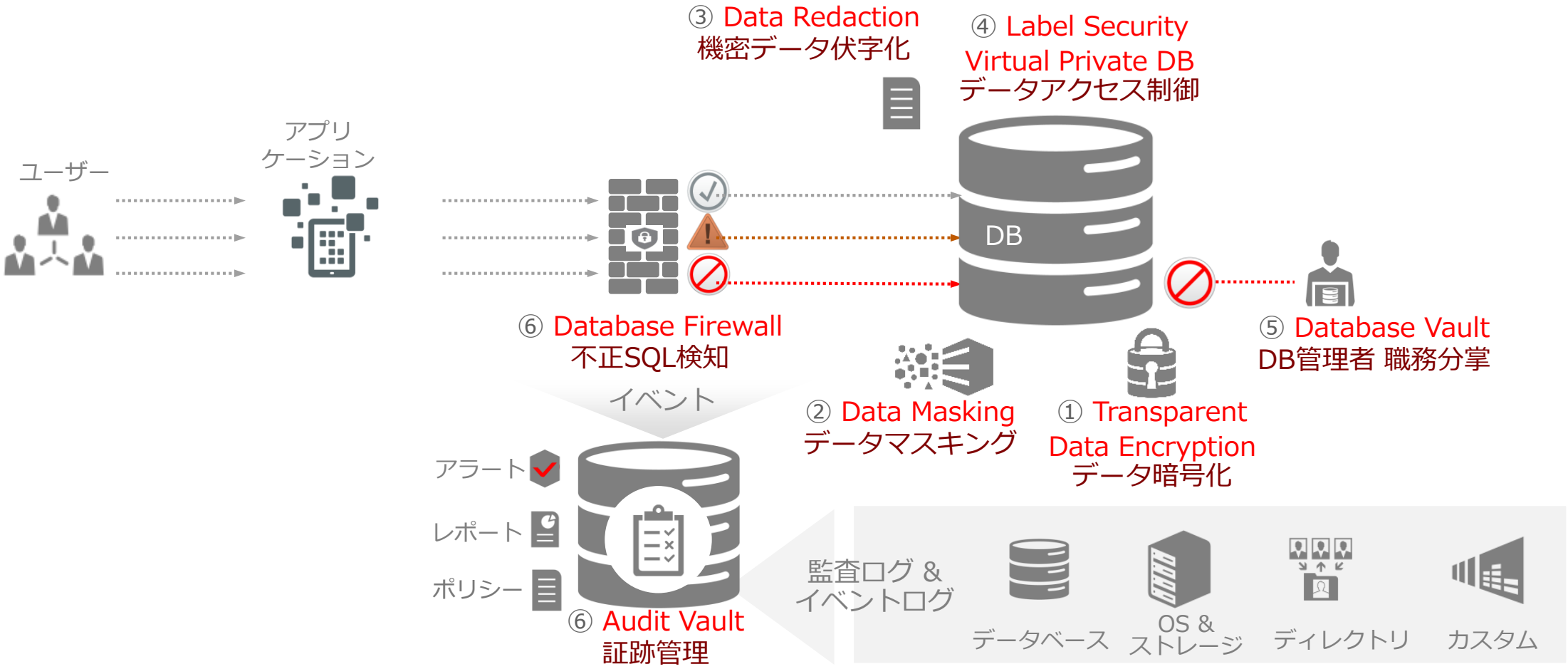
対策がされている場所を迂回する攻撃の増加

98%の情報はデータベースから盗まれている
84%の情報は盗まれたID・権限で侵害されている
71% は数分で陥落
92% は第3者からの指摘で発覚

出展： Verizon DBIR 2012



Oracleが提供するDBセキュリティ・ソリューション



Oracleが提供するDBセキュリティ・ソリューション

機能名	① Transparent Data Encryption	② Data Masking Pack	③ Data Redaction	④ Label Security/ Virtual Private Database	⑤ Database Vault	⑥ Audit Vault and Database Firewall
脅威	データファイル、バックアップデータの奪取	開発・テスト環境データの奪取	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	DB管理者によるデータ奪取	内部不正の追跡、影響範囲の調査不可能
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	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	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	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	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
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	テスト、開発環境の情報を保護	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	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	DB、OSなど、網羅的な監査証跡の取得、管理

DBセキュリティ製品のご紹介

Oracle Database Vault

Oracle Database Vaultについて

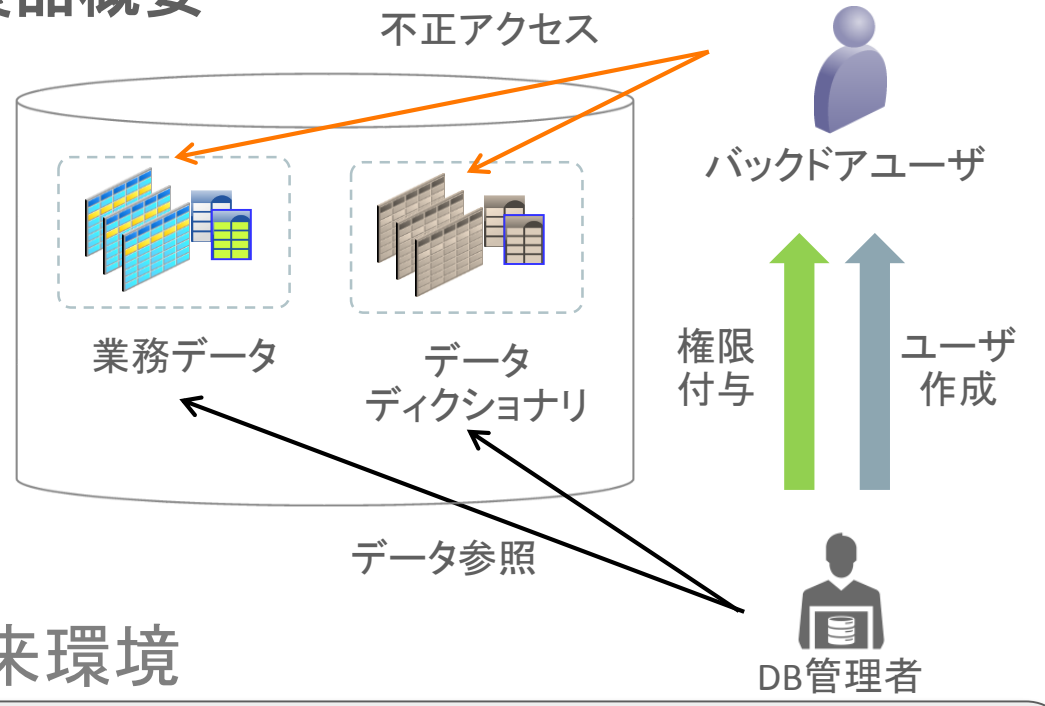
製品概要

- DBのアクセス制御
  - DB接続やデータアクセスを設定し、DB管理者であっても操作を制限することが出来る
- DB管理者の権限を職務分掌
  - 一つのユーザに多くの権限を持たせず、必要な権限のみを持たせる

「**職務分掌**」とは、組織においてそれぞれの職務が果たすべき責任（職責）や職責を果たす上で必要な権限（職権）を明確にするために、職務ごとの役割を整理・配分すること。

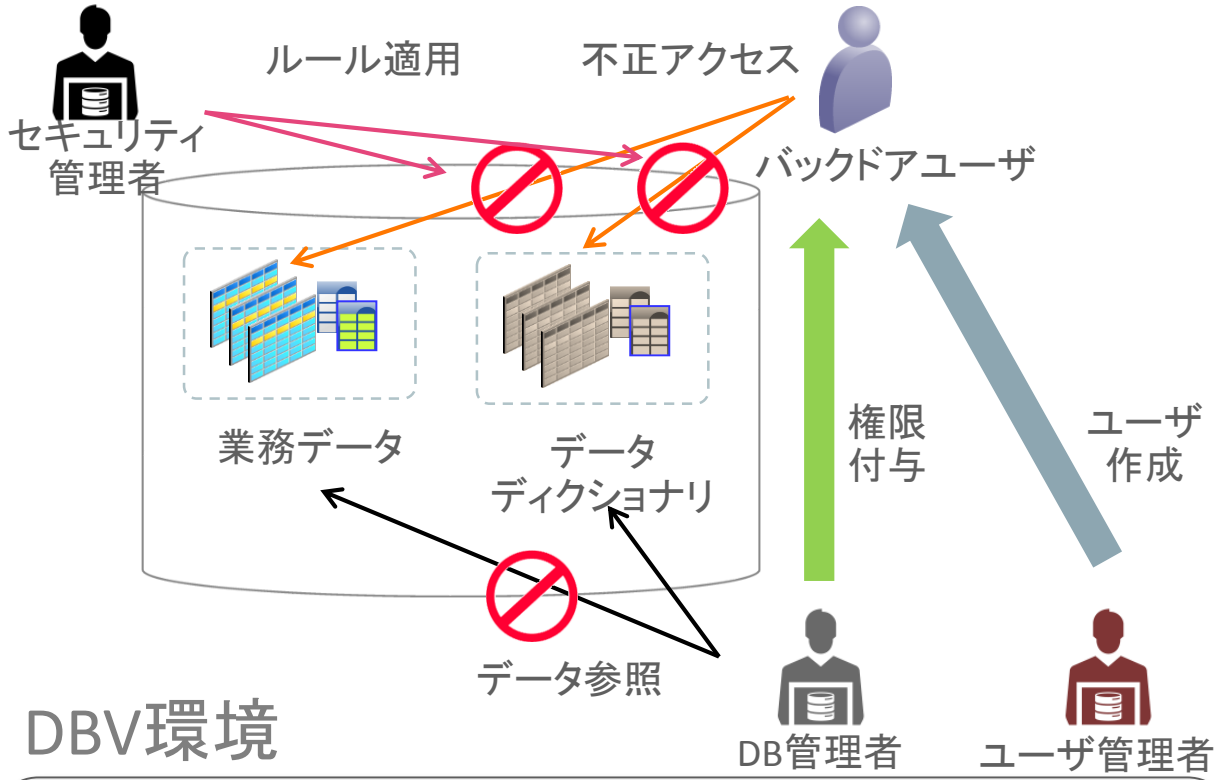
Oracle Database Vaultについて

製品概要



従来環境

・DB管理者はシステム権限により業務データにアクセス可能
・DB管理者はユーザ作成/権限付与の両方が可能であり、バックドアの作成が容易



DBV環境

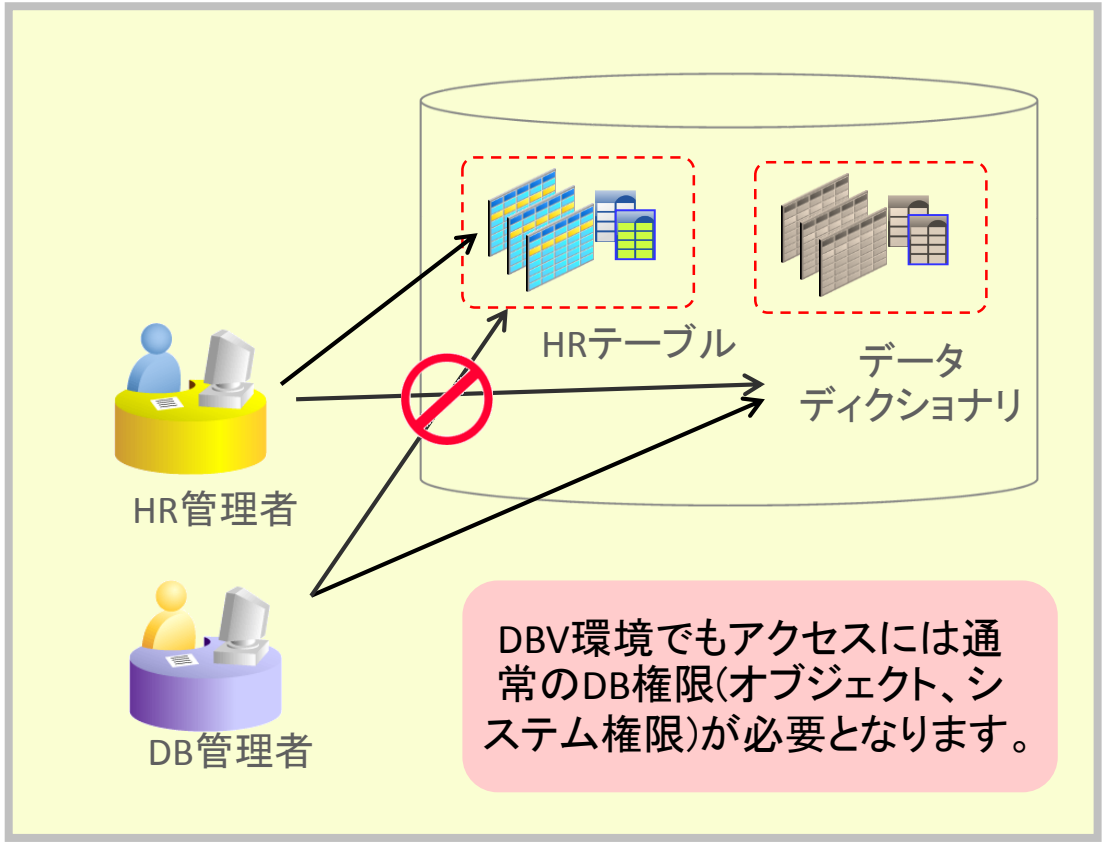
・DB管理者は業務データにアクセス出来なくなる
・”**ユーザ管理者**”と”**セキュリティ管理者**”を作成される
・悪意のあるユーザが**2人以上**いないとセキュリティインシデントにならない

Oracle Database Vaultについて

主な機能— レルム—

- 任意のスキーマ・オブジェクトのセットを保護・管理するための論理的な領域
- 不認可アクセスや DDL は、レルム違反エラーとなり、監査ログとして保存される

ポイント:
HR管理者の持っているオブジェクトをすべてレルムで保護すれば、DB管理者であったとしてもHRオブジェクトへのアクセスは許可されない。

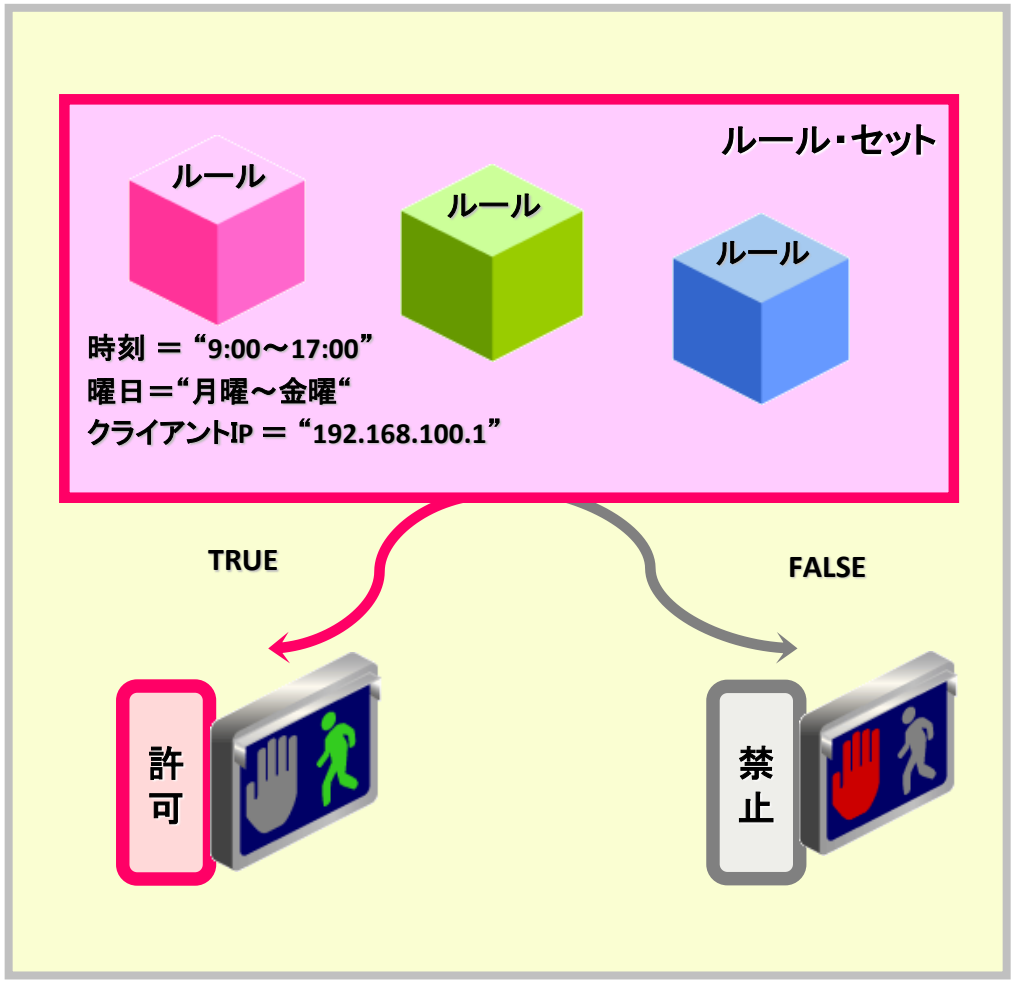


Oracle Database Vaultについて

主な機能― ルール/ルール・セット―

- ルールはDBVで使用される式
- ルールはデータベースで取得できる情報で作成
- ルール・セットにルールを増やし条件を厳しくすることで、アクセス制御の条件を強化

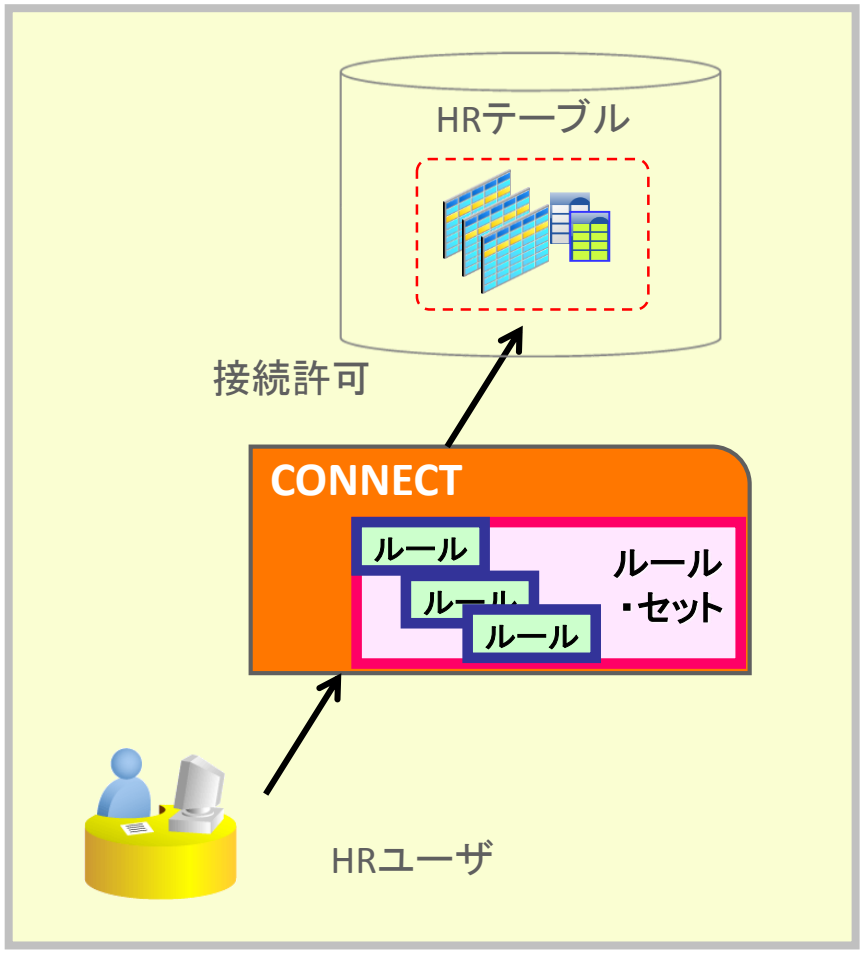
ポイント:
時刻を9:00~17:00/曜日を月~金/IPアドレスを192.168.100.1のルールをそれぞれ作成し、ルール・セットに組み込む。



Oracle Database Vaultについて

主な機能― コマンドルール―

- SQLコマンドの発行を、ルール・セットに基いて制限するためのもの
- SQLコマンドに特定のルール・セットを紐付けておくと、ルール・セットがtrue となった場合のみ、そのSQLコマンドを発行する許可が与えられる。



ポイント:
HRユーザを許可するルール・セットに
”CONNECT”コマンド”を紐付ける。

DBセキュリティ製品導入 Tips

Oracle Database Vault

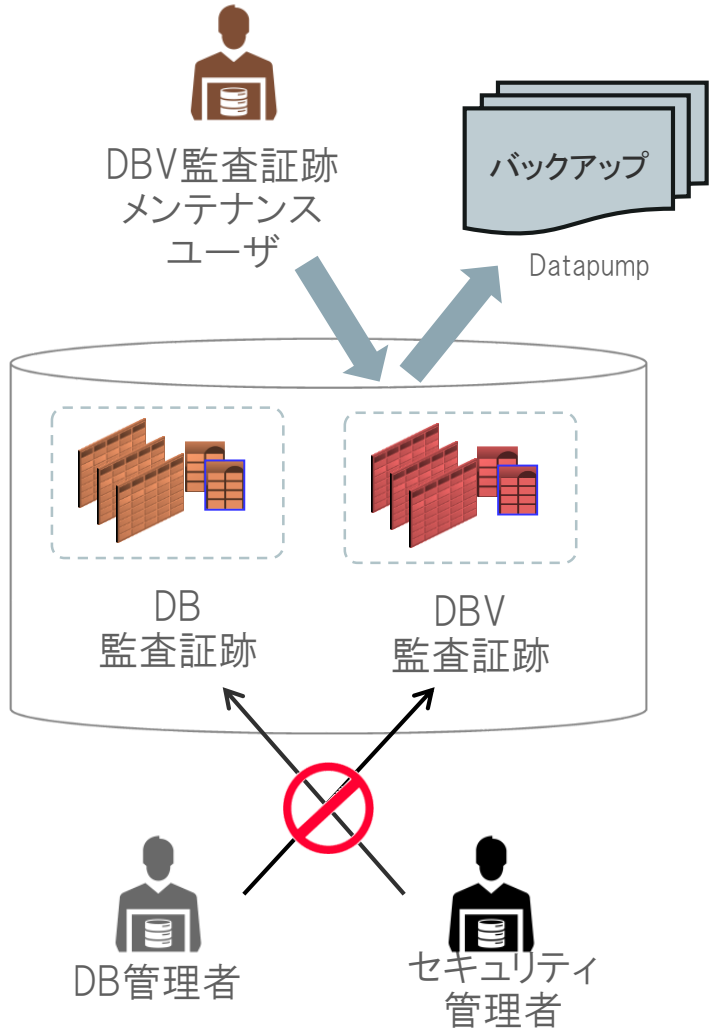
推奨されるコマンドルール

- GRANT/REVOKE文
  - 権限付与のコマンドは**特定ユーザのみ**に制限する
  - 不要な権限付与を制限し、不正な操作を抑止する

- NOAUDIT文
  - NOAUDIT文を**全ユーザで実行させない**
    ※AVDF導入環境ではAVDF管理者のみ付与する
  - DBで監査(AUDIT文)を使用していない環境下でも有効にすることを推奨

DBVの監査証跡の管理とメンテナンス

- DBとDBVの監査証跡と別管理
  - DBとDBVの監査証跡の管理は**別ユーザ**で行う
  - DBVの監査証跡は**表領域**に作成する必要がある
- DBVの監査証跡メンテユーザの作成
  - DBV監査証跡を**バックアップ**するためのユーザ
  - Datapumpに**必要な権限のみ**付与する
    ※メンテユーザの監査証跡の改竄は不可
  - バックアップファイルの管理は別で行う必要がある



DBV環境下での緊急対応時の運用案

1. DB管理者＋DBV管理者相当のユーザ作成
   - DBのすべての業務が出来るユーザの作成し、緊急時の対応に備える
   - 通常運用では使用しない
   - 権限の強さはSYSDBAやroot(OS)ユーザ相当のため**厳重に管理する**

2. 緊急時の無効化スクリプトの準備
   - DBVのコマンドルール/レルムを無効化ジョブするジョブを用意
   - DBV機能のためにデプロイしたコンポーネントを**削除するわけではない**
     ※但し、通常DBA権限の一部が付与されていない点に注意が必要

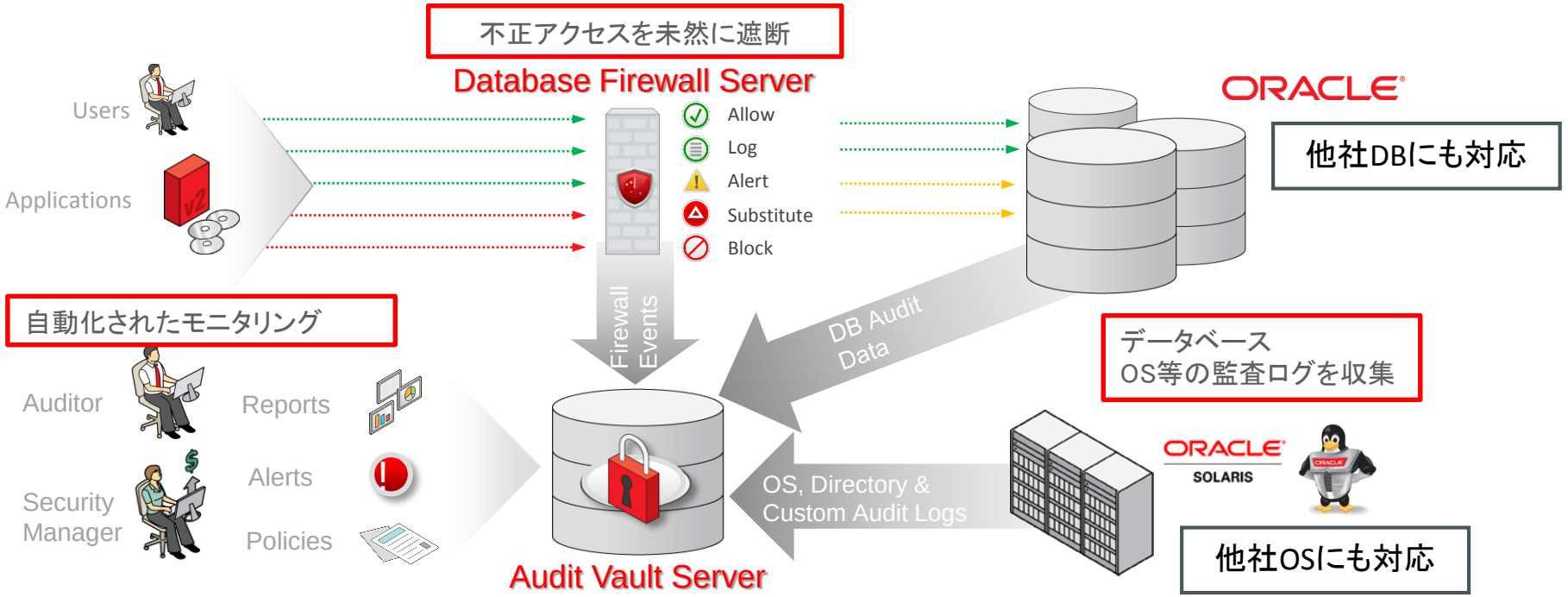
DBセキュリティ製品のご紹介

Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall(AVDF)について

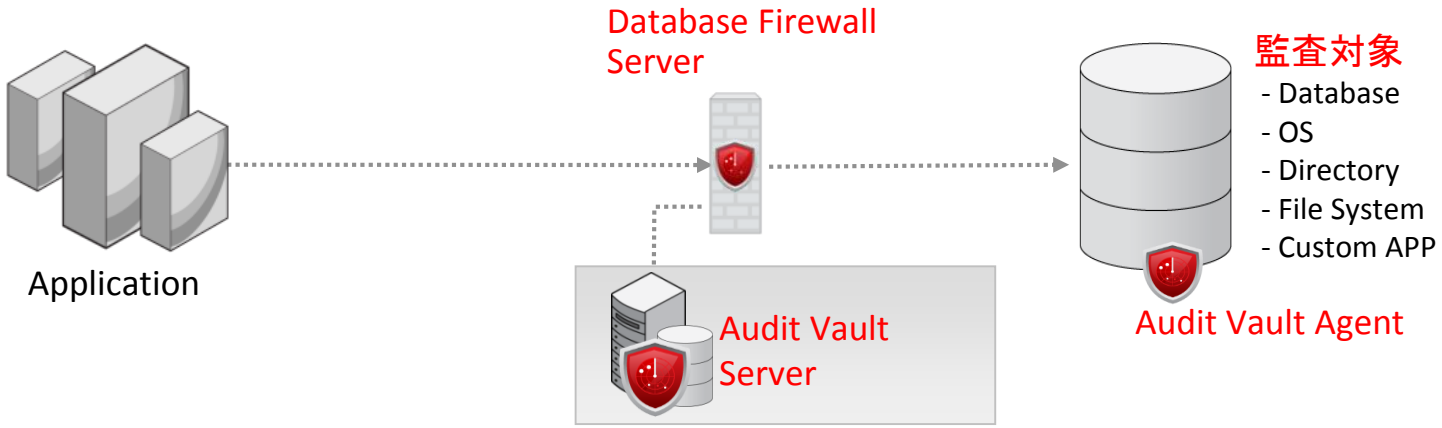
製品概要

文法解析による正確なブロッキング、DatabaseやOSの監査ログをモニタリング
迅速なセキュリティ対策を可能にするソフトウェア・アプライアンス



Oracle Audit Vault and Database Firewall(AVDF)について

AVDFの各コンポネント

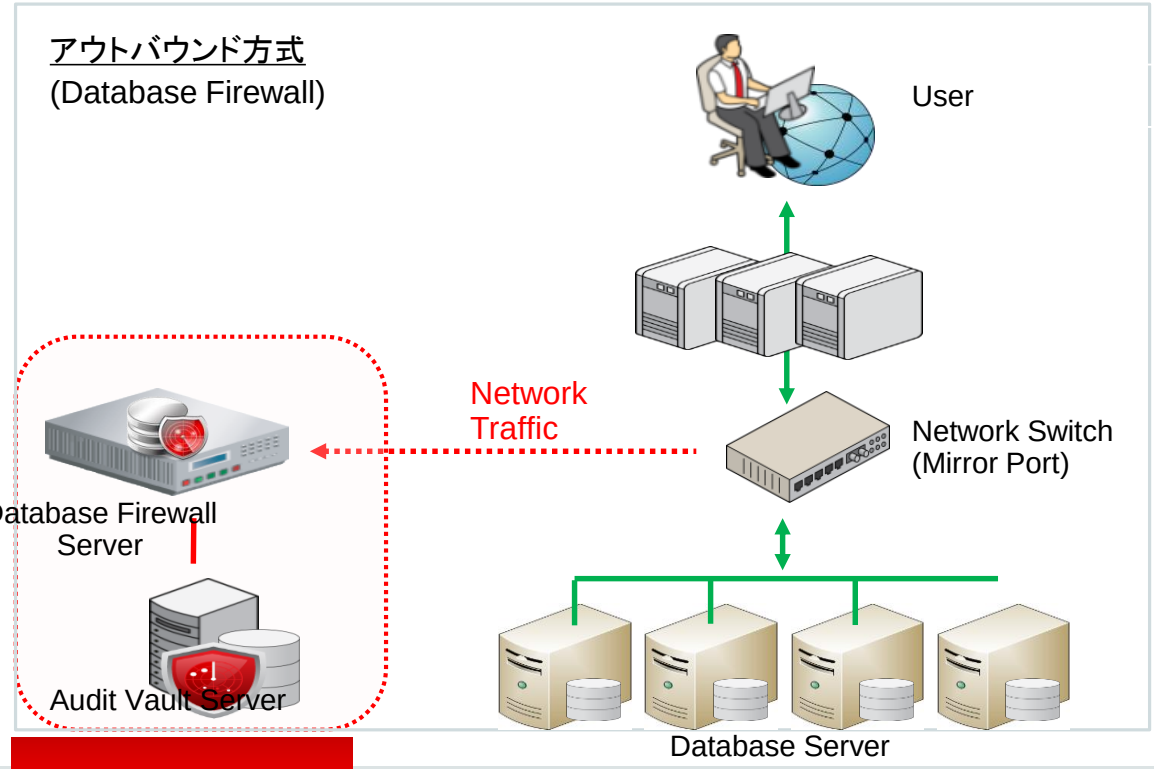


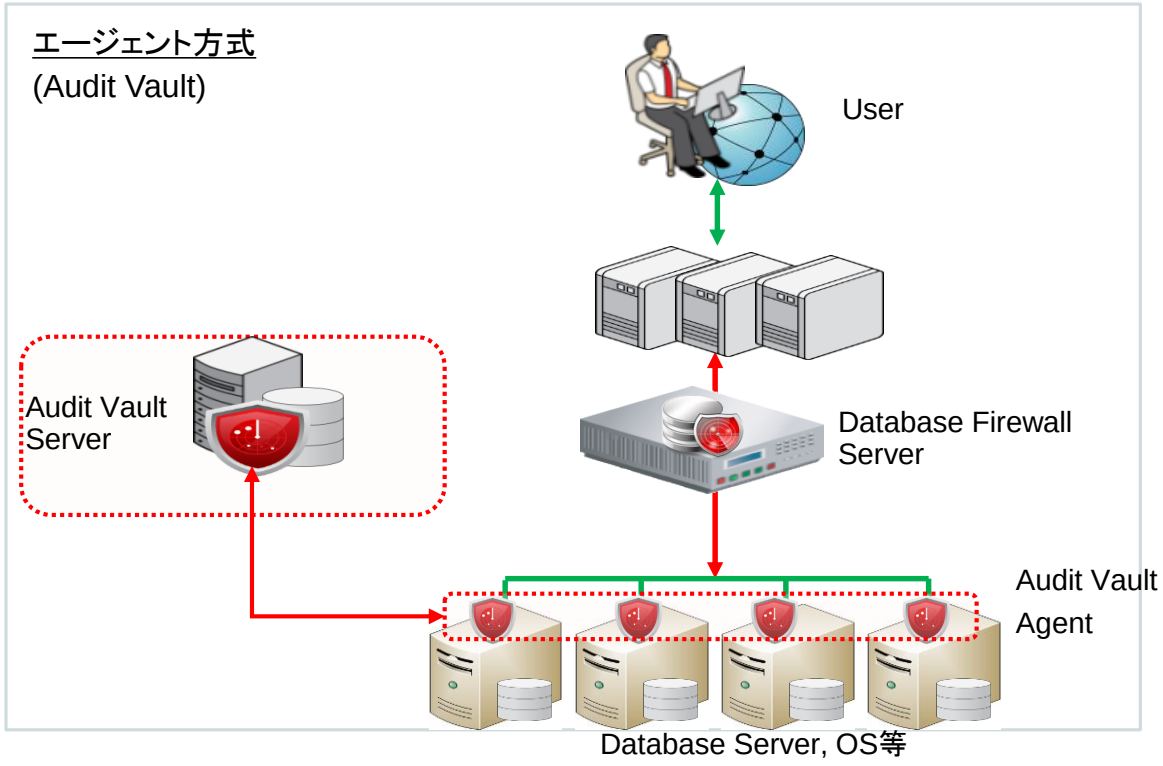
- Oracle Database Firewall Server
  - ネットワークトラフィックを受信し、ポリシーに応じたブロッキング・モニタリングを行うネットワーク・サーバ
  - 配置方式は、AP～DB間に配置するインライン方式、ミラーポートを利用したアウトオブバンド方式、プロキシ方式の3種類
- Oracle Audit Vault Server
  - Database Firewall、Audit Vault Agentから転送されるログを集約するリポジトリ・サーバ
  - すべてのDBFW Server、 Audit Vault Agentの管理・監視を一元的に管理し、ログの分析やアラート、レポーティングを行う
- Audit Vault Agent
  - 監査対象上で動作するJAVAアプリケーション。監査対象が出力した監査ログを収集し、定期的にAudit Vault Serveへ送信する

Oracle Audit Vault and Database Firewall(AVDF)について

AVDFの機能概要　– モニタリング

- スイッチのミラーポートからSQLパケットをDBFW Serverが受信するオーバヘッドのないアウトオブバンド方式
- Databaseだけでなく、OSやユーザ独自のアプリなど幅広い監査ログの取得を実現するエージェント方式
- お客様のシステムや監査対象に応じて最適な方式を選択、また、組み合わせたハイブリッド方式も可能

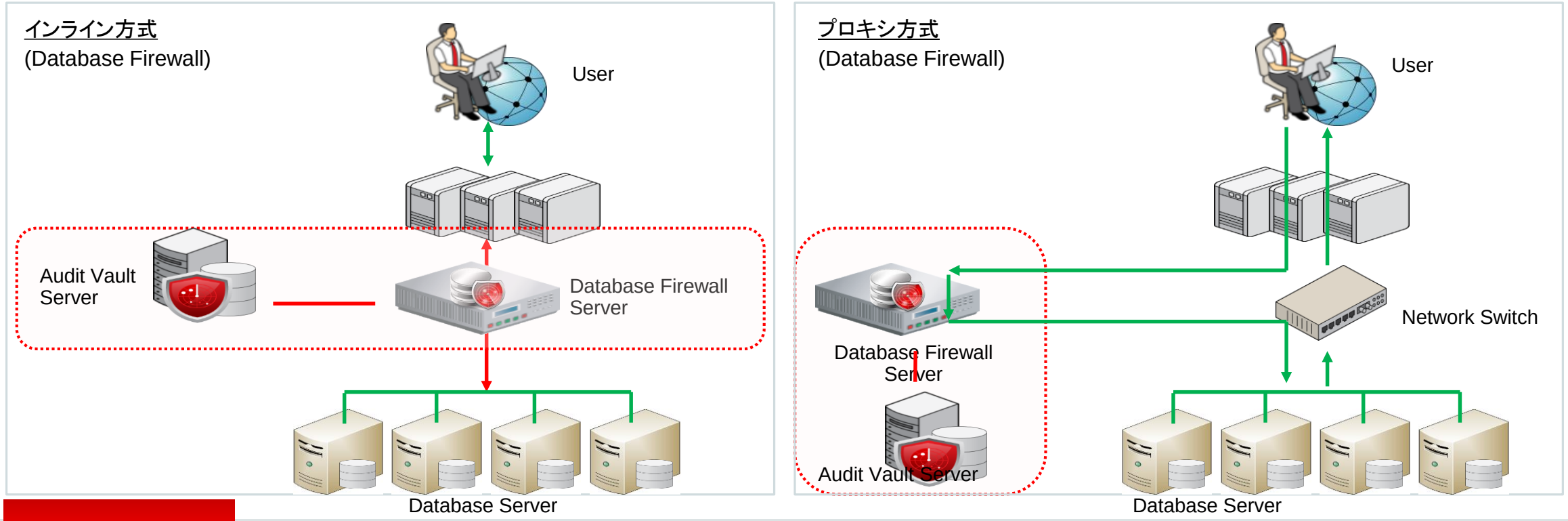




Oracle Audit Vault and Database Firewall(AVDF)について

AVDFの機能概要　- ブロッキング

- 搭載されたSQL文法解析エンジンが語検出のない正確なブロッキングを実現
- アプリケーション、データベースの変更が必要のない透過的な構成（インライン方式）
- 数万を超えるトランザクションでもオーバヘッドを感じさせない高速なマッチング処理を実現



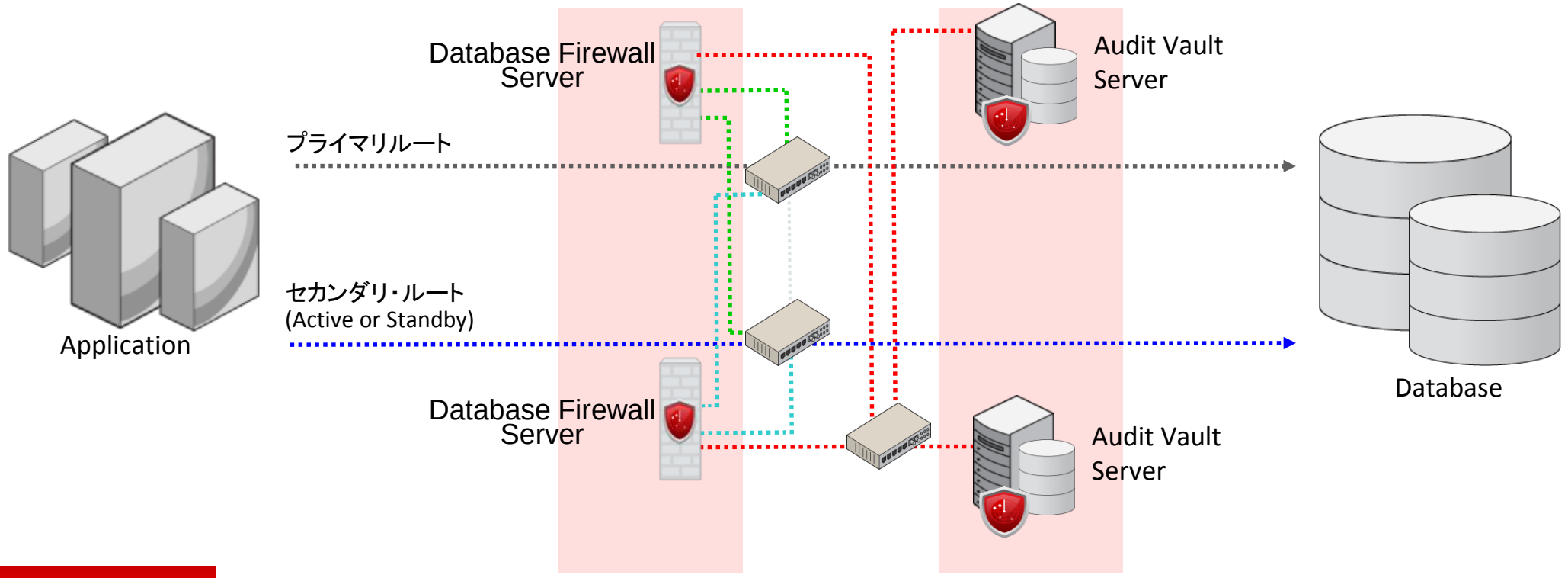
DBセキュリティ製品導入 Tips

Oracle Audit Vault and Database Firewall

ORACLE

AVDFの冗長化構成

- AVDFではDBFWのペア、AVSのペア、あるいは両方を構成することで、高可用性システム・アーキテクチャーを提供することができます。
- DBFW/AVSの障害時に、DBFW/AVSの処理がフェイルオーバーし、継続してモニタリングを行うことで障害時にもセキュリティレベルを落とすことなく処理を継続することができます。



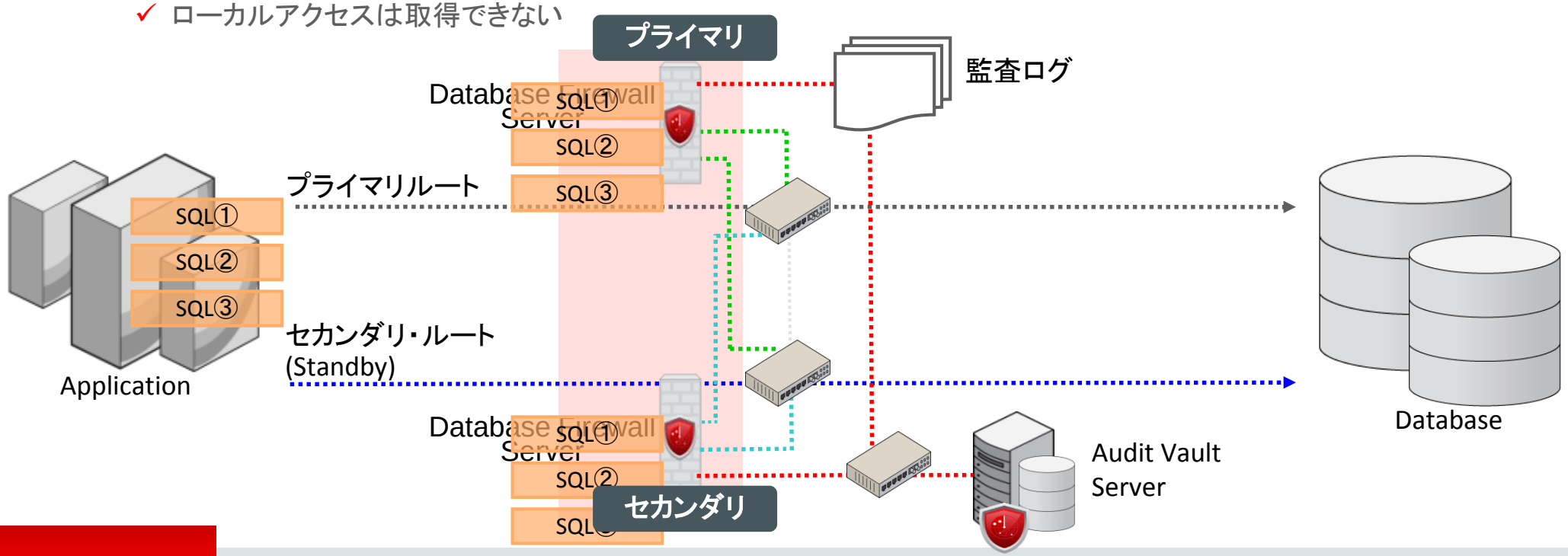
AVDFの冗長化構成

DBFWの冗長化構成について

ログの取得漏れを防ぐため
SW-DBFW間のたすき掛けが必須

AVDFを導入頂いている多くのお客様に、DBFW障害による監査ログの取り漏れを防ぐためDBFWの冗長化構成の採用頂いています。

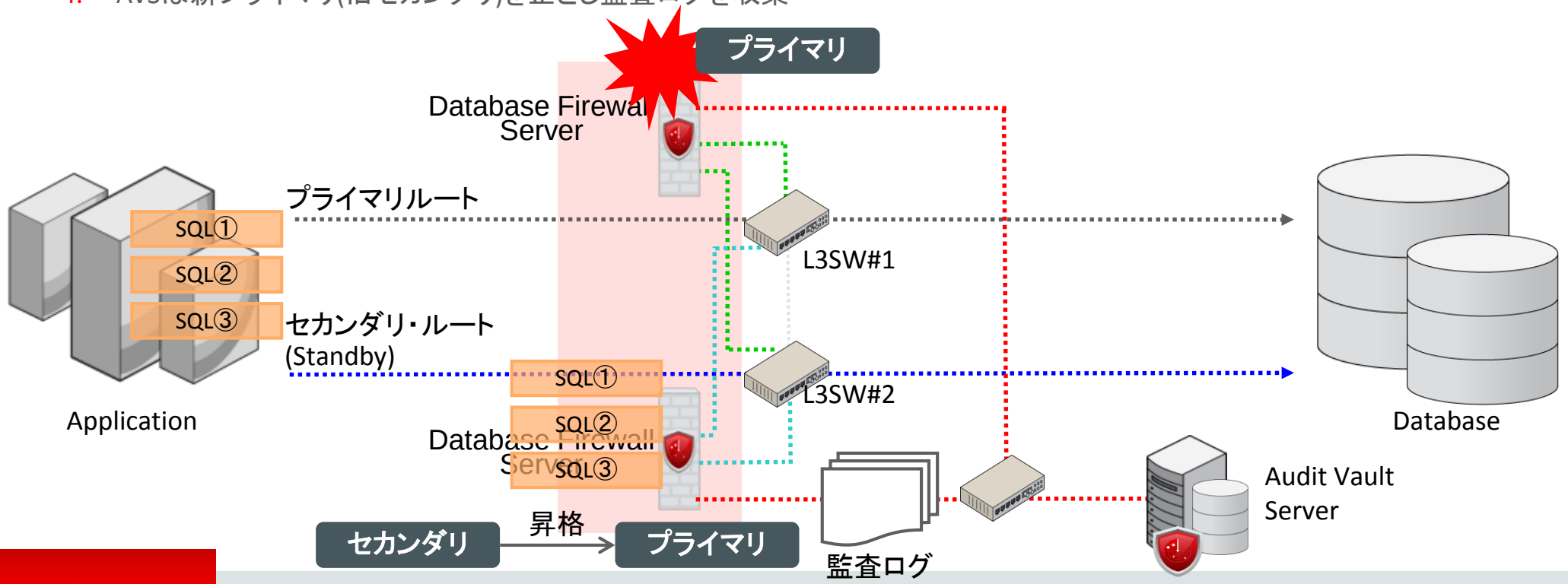
- ✓ スイッチのミラーポートからデータベースの送受信アクセスを取得し、Audit Vault へ送信
- ✓ 冗長化されたスイッチに対して2台のDatabase Firewallで接続し、ログの重複はペアリング機能で制御
- ✓ DBFWの障害時でも、片側のDatabase Firewallでログを収集する
- ✓ ローカルアクセスは取得できない



AVDFの冗長化構成

DBFWの冗長化構成について – プライマリDBFW障害

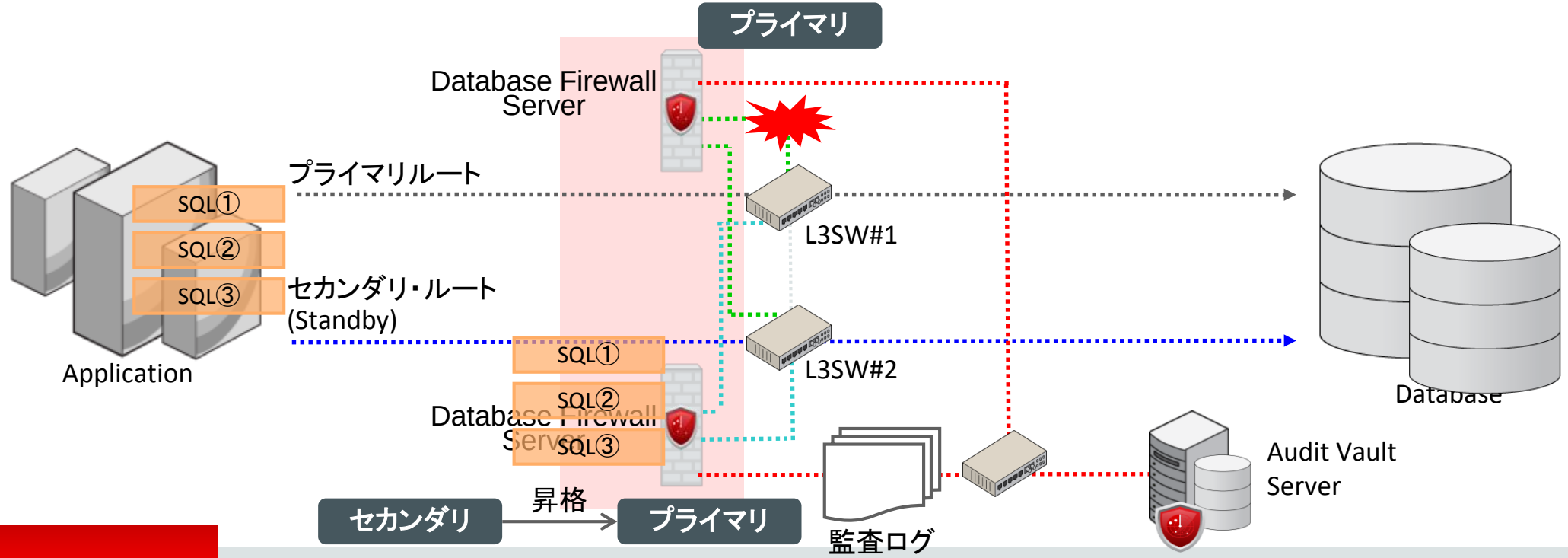
1. プライマリDBFWに障害が発生
2. AVSが障害を検知
3. セカンダリDBFWがプライマリに昇格
4. AVSは新プライマリ(旧セカンダリ)を正とし監査ログを収集



AVDFの冗長化構成

DBFWの冗長化構成について – SW-プライマリDBFW間ネットワーク障害

1. プライマリのSW-DBFW間のネットワーク障害が発生
2. ネットワーク監視による検知
3. 手動でセカンダリDBFWをプライマリに昇格
4. AVSは新プライマリ(旧セカンダリ)を正とし監査ログを収集



AVDFの導入メリット

監査証跡の運用時におけるメリット

- 冗長化構成によるセキュリティレベルの保持
- 監査証跡の完全性担保
  - Audit VaultサーバにはDBVが標準インストール済み。(監査証跡データへの不正アクセスや改ざんを防ぐ仕組み)
- 監査証跡の定期的な分析
  - 取得した監査証跡はレポーティング機能を使い定期な分析を実施することで、不正アクセスや異常な行動を検知。
  - アラート機能を利用することで、緊急性の高いイベントに対してアラート通知が可能。
- 監査証跡の保存ポリシー
  - 監査証跡のオンライン、アーカイブ、バックアップ管理機能を標準機能として提供。
- 複数DBの監査証跡を一元管理
  - 複数DBの監査証跡をAudit Vaultサーバで一元的に管理できる

補足：PCI DSS(Payment Card Industry Data Security Standard)

- クレジットカードを扱う業者の業界スタンダード基準
  - 加盟店・決済代行事業者が取り扱うカード会員様のクレジットカード情報・取引情報を安全に守るために、JCB、アメリカンエキスプレス、Discover、マスターカード、VISAの国際ペイメントブランド5社が共同で策定した、クレジット業界におけるグローバルセキュリティ基準。
- **12の「要件」として規定**
  - ファイアウォールを導入し、最適な設定を維持すること。

    ネットワーク資源およびカード会員データに対するすべてのアクセスを追跡し、監視すること。…などが12の要件に分かれています。
  - 12の要件をさらに詳細な約200項目にブレイクダウンされています。

補足：セキュリティ施策の分類/PCIDSS要件とOracleソリューション

- DBVとAVDFはPCDISSの要件にマッピングすることができます。

- 安全なネットワークの構築と維持
  - 要件1：カード会員データを保護するために、ファイアウォールをインストールして構成を維持する
  - 要件2：システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない
- カード会員データの保護
  - **要件3：保存されるカード会員データを保護する**
  - 要件4：オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する

〈中略〉

- 強力なアクセス制御手法の導入
  - **要件7：カード会員データへのアクセスを、業務上必要な範囲内に制限する**
  - 要件8：システムコンポーネントへのアクセスを確認・許可する
  - 要件9：カード会員データへの物理アクセスを制限する
- ネットワークの定期的な監視およびテスト
  - **要件10：ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する**
  - 要件11：セキュリティシステムおよびプロセスを定期的にテストする
- 情報セキュリティポリシーの維持
  - 要件12：すべての担当者の情報セキュリティに対応するポリシーを維持する

Database Vault

AVDF

PCI DSS 3.0 詳細：https://ja.pcisecuritystandards.org/_onelink_/pcisecurity/en2ja/minisite/en/docs/PCI_DSS_v3.pdf
“クレジットカード業界のデータ・セキュリティ標準への持続可能なコンプライアンス”：
http://www.oracle.com/jp/products/database/security/1006242-security-pci-dss-wp-078843-171764-ja.pdf

セキュリティ製品導入プロジェクトのご紹介

セキュリティ製品導入プロジェクトのご紹介

用語の解説

【予防的統制】
・「悪いことを**させない**」仕組みのこと。
・ブロッキング、アクセスコントロールなどの強制力を伴うもの。

【発見的統制】
・「悪いことが起きたことを**見つける**」仕組みのこと。
・監査証跡、ログ分析などの誰が何をやったかが追跡できる状態（責任追跡性）

Oracleコンサルが考えるDBセキュリティ

- 攻め　⇒　プロアクティブに抑止する　…【**予防的統制**】
- 守り　⇒　最終防衛としての監査証跡　…【**発見的統制**】

(参考)Oracleが提供するDBセキュリティ・ソリューション

【予防的統制】　【発見的統制】

機能名	① Transparent Data Encryption	② Data Masking Pack	③ Data Redaction	④ Label Security/ Virtual Private Database	⑤ Database Vault	⑥ Audit Vault and Database Firewall
脅威	データファイル、バックアップデータの奪取	開発・テスト環境データの奪取	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	DB管理者によるデータ奪取	内部不正の追跡、影響範囲の調査不可能
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	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	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	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	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
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	テスト、開発環境の情報を保護	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	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	DB、OSなど、網羅的な監査証跡の取得、管理

セキュリティ製品導入プロジェクトのご紹介

セキュリティ実装までの流れ

要件
- セキュリティ要件:「何」を「誰」から守るかの整理・定義・ユースケース

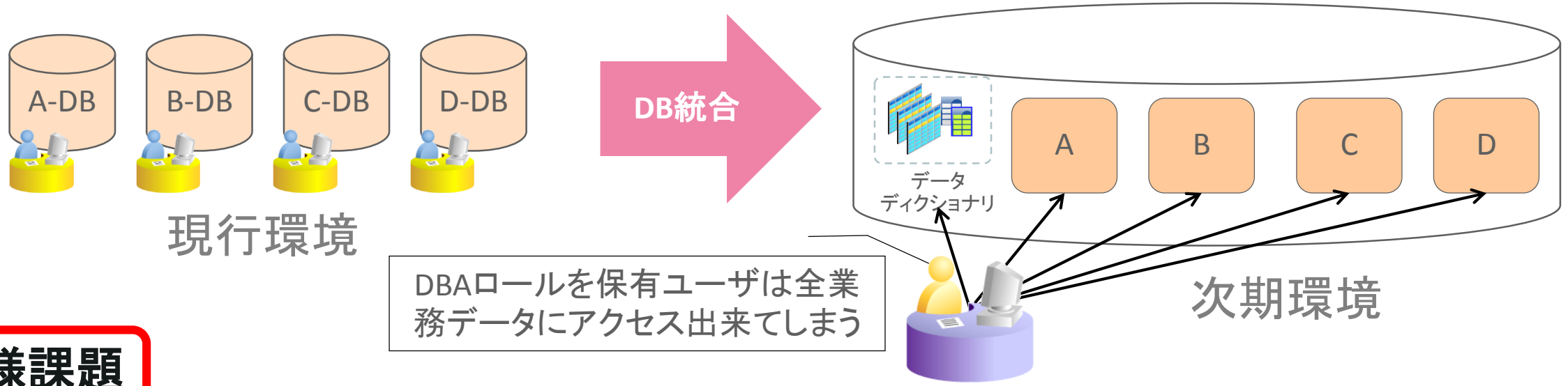
設計
- セキュリティ設計:「何」を「誰」から「どのように」守るかの設計

実装
- セキュリティ実装:「何」を「誰」から「どのように」守るかの施行

運用
- セキュリティ運用:「何」を「誰」から「どのように」守り続けるかの確立

セキュリティ製品導入プロジェクトのご紹介

本プロジェクトの目的

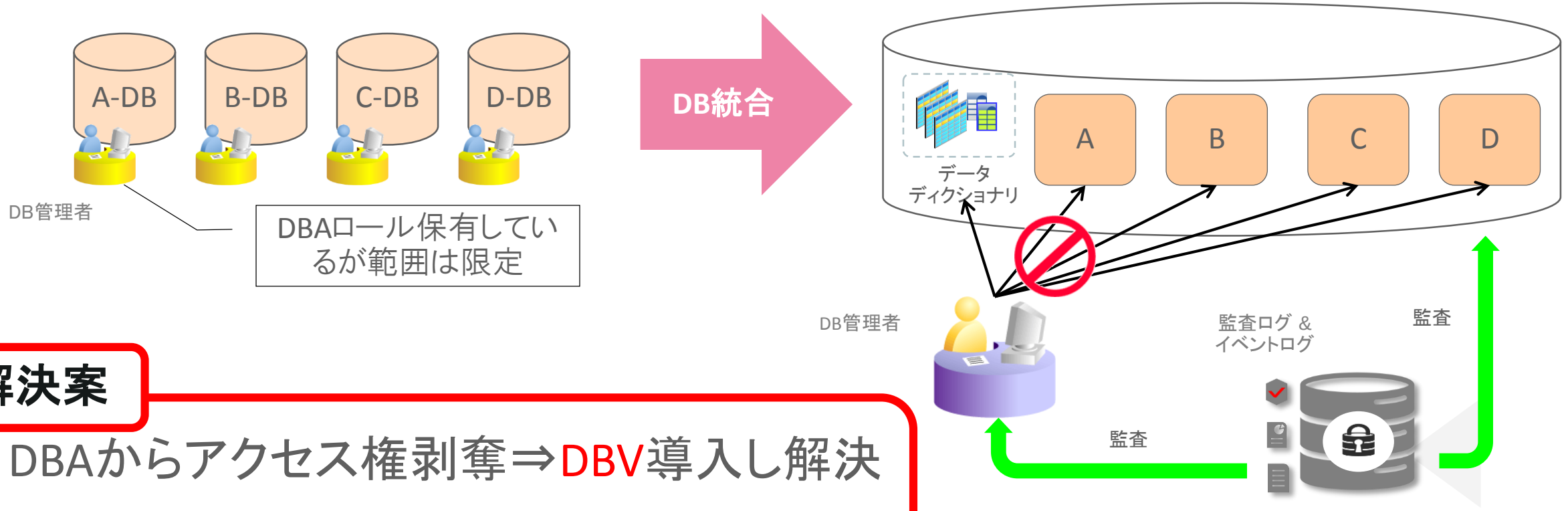


お客様課題

- 現行DBではDBAロールを使用するアプリが存在。
- セキュリティ強化に伴い、監査も強化したい。

セキュリティ製品導入プロジェクトのご紹介

本プロジェクトの目的

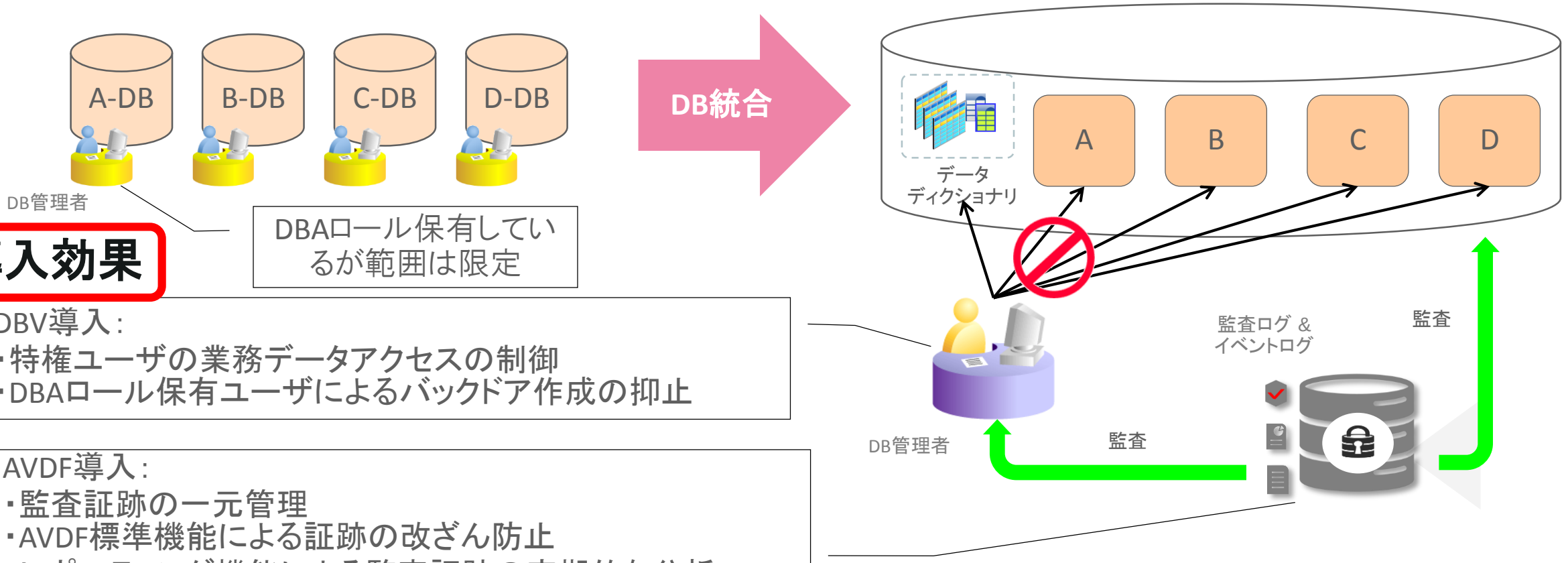


解決案

- DBAからアクセス権剥奪⇒DBV導入し解決
- 監査強化⇒AVDF導入し解決

セキュリティ製品導入プロジェクトのご紹介

本プロジェクトの目的



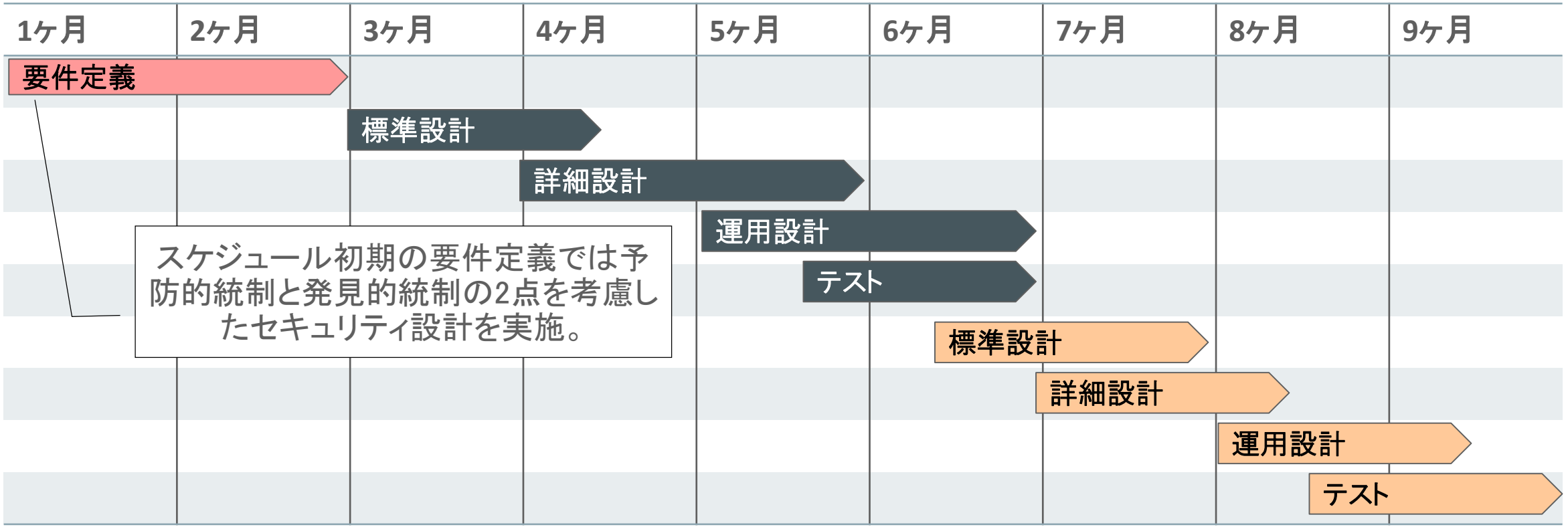
導入効果

DBV導入：
- 特権ユーザの業務データアクセスの制御
- DBAロール保有ユーザによるバックドア作成の抑止

AVDF導入：
- 監査証跡の一元管理
- AVDF標準機能による証跡の改ざん防止
- レポーティング機能による監査証跡の定期的な分析

セキュリティ製品導入プロジェクトのご紹介

スケジュール



セキュリティ製品導入プロジェクトのご紹介

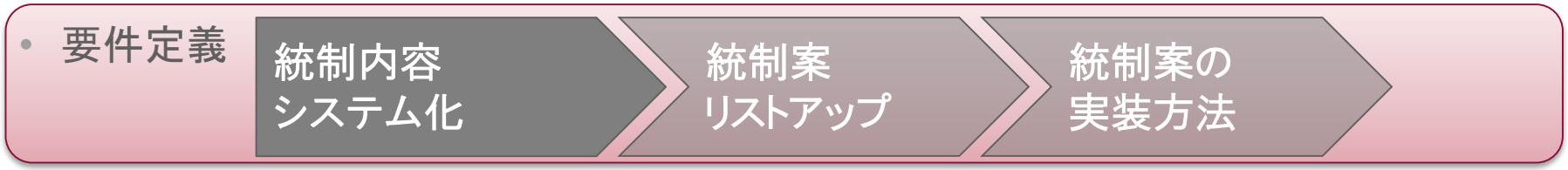
プロジェクトの作業フロー

- 要件定義
  - 監査部からの統制内容は抽象的であったため、システムとしての統制を導くため **「何」、「誰から」** 守るか整理する。
  - 整理した要件を基に**統制を内容の案出し**を実施する。
  - 運用コストなどを考慮して**システムとしての統制内容**を決定する。

- 設計 / 実装
  - 実装は基本的にDBVとAVで「実現できること」「実現できないこと」を検討する。
  - 必須でない統制は運用コストを考慮してAVDFによる発見的統制に振り分ける。

セキュリティ製品導入プロジェクトのご紹介

要件定義 （統制内容システム化）



- 統制内容システム化（ユースケースづくり）
  - お客様にはセキュリティ要件を決定する監査部門から提示された監査要件が存在した。
  - ただし、セキュリティ要件はシステム観点ではざっくりとした内容であるため、下記を整理する。
    - ✓ 守りたいデータは何か
    - ✓ 守りたいデータに対するアクセス(誰を許容して、誰を許容しないのか)
    - ✓ その他管理オペレーションの権限分掌

  例) **DBAユーザの顧客情報アクセスは制限したい。権限付与のオペレーションは管理したい。**
- 統制案リストアップ
- 統制案の実装方法

セキュリティ製品導入プロジェクトのご紹介

要件定義 （統制内容システム化）-管理オペレーションの権限分掌

- ユーザ定義
  - 職責とそれに対するユーザのマッピングを行う。
  - それぞれの職責で担当する作業を簡潔に洗い出す。

例）ユーザ定義

No.	職責	ユーザ	主な担当業務
1	インフラ運用	インフラ運用担当者	・DB起動／停止や性能情報取得など基盤としての運用作業を行う ・業務DB内のオブジェクトなどについての権限は付与されない
2	アプリケーション	アプリケーション利用ユーザ	・アプリケーションにて使用される ・アプリケーションからは、最低限必要な権限が必要となる （データの参照、更新、テーブル作成）
3	セキュリティ運用	セキュリティ担当者	・アカウント発行や、セキュリティ・ポリシー（ルール）、レルムの管理を行う ・DVO(Database Vault Owner)やDVA(Database Vault Account Manager)の権限が付与される ・業務DB内のオブジェクトなどについての権限は付与されない

セキュリティ製品導入プロジェクトのご紹介

要件定義 （統制内容システム化）- 管理オペレーションの権限分掌

- 権限セット
  - 各利用者を想定した権限セットを定義する。
  - 各権限セットでは利用者に必要とされる最低限の権限を付与する。

例）権限セット

No	ユーザ	説明	権限セット	設定方法
1	アプリケーション利用ユーザ	・アプリケーションにて使用される権限 ・アプリケーション以外からアクセスできないように IPアドレスなどで接続を制限される	ALTER SESSION CREATE SESSION CREATE SYNONYM	セキュリティ担当者によって、 作業者アカウントが作成され、 この権限が付与される
2	インフラ運用担当者	・インフラ運用にて使用する権限 ・Database Vaultのインストールにより、 レルムで保護された制限つきのDBA権限となる	DBAロール	アカウント利用要件を確認し、 セキュリティ担当者によって、 作業者アカウントに、 この権限（ロール）が与えられる
3	セキュリティ担当者	・アカウントとアクセス権限のメンテナンスに使用する権限 ・セキュリティ運用部門が使用する ・アカウント発行や、セキュリティ・ポリシー（ルール） レルムの管理を行う	DV_OWNERロール DV_ACCTMGRロール	セキュリティ運用部門の担当者 に紐づく作業者アカウントに、 この権限（ロール）が与えられる

セキュリティ製品導入プロジェクトのご紹介

要件定義 （統制内容システム化）- 管理オペレーションの権限分掌

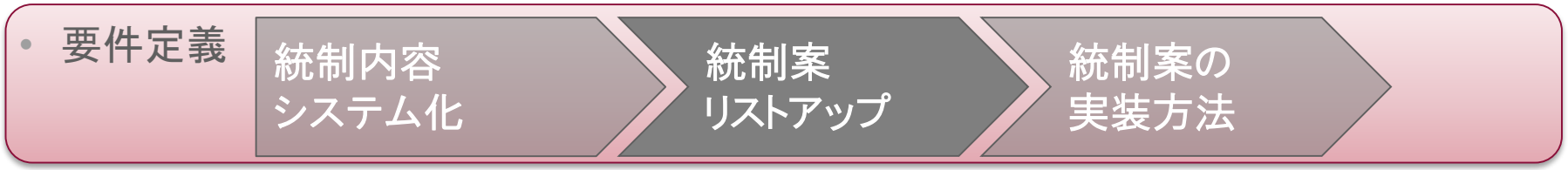
- ユースケース
  - システムライフサイクルの中の各局面で想定されるユースケースと実行するユーザ、業務内容と利用する権限セットをマッピングする。

例）ユースケース

No	ユースケース	ユーザ	業務内容
1	アカウント管理	セキュリティ担当者	アカウント作成
			アカウント削除
			ロール作成・変更・削除
			アクセス権(SYSTEM権限)付与
2	アクセス権限の変更	インフラ運用担当者	アクセス権(SYSTEM権限)付与
			アクセス権剥奪
			ロール(システム/オブジェクト関連)作成
3	DBバックアップ	インフラ運用担当者	DBのバックアップとリストア
4	オブジェクト管理	アプリケーション利用ユーザ	テーブルの作成
			テーブルの削除

セキュリティ製品導入プロジェクトのご紹介

要件定義 （統制案リストアップ）



- 統制内容システム化（ユースケースづくり）
  - お客様にはセキュリティ要件を決定する監査部門から提示された監査要件が存在した。
  - ただし、セキュリティ要件はシステム観点ではざっくりとした内容であるため、下記を整理する。
    - ✓ 守りたいデータ、守りたいデータに対するアクセス、その他管理オペレーションの権限分掌

  例) DBAユーザの顧客情報アクセスは制限したい。権限付与のオペレーションは管理したい。

- **統制案リストアップ**
  - **システム化する統制項目を製品に落とし込み、具体的な統制に対する実装をリストアップする。**

  例) DBV機能で顧客情報表を保護する。権限管理の操作はすべて監査対象とする。

- 統制案の実装方法
  - 「統制案のリストアップ」フェーズで洗い出した案のうち、設計コスト/運用コストを考慮して実装する内容を決定する。

  例) DBVのレルムで保護を行う。AVDFでGRANT文を発行した証跡は取得する。

セキュリティ製品導入プロジェクトのご紹介

要件定義 （統制案の実装方法）

- 要件定義

  - 統制内容システム化（ユースケースづくり）
    - お客様にはセキュリティ要件を決定する監査部門から提示された監査要件が存在した。
    - ただし、セキュリティ要件はシステム観点ではざっくりとした内容であるため、下記を整理する。
      - ✓ 守りたいデータ、守りたいデータに対するアクセス、その他管理オペレーションの権限分掌

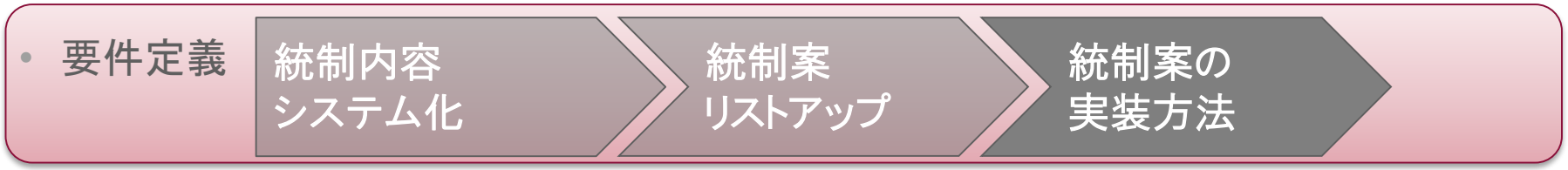
    例) DBAユーザの顧客情報アクセスは制限したい。権限付与のオペレーションは管理したい。
  - 統制案リストアップ
    - システム化する統制項目を製品に落とし込み、具体的な統制に対する実装をリストアップする。

    例) DBV機能で顧客情報表を保護する。権限管理の操作はすべて監査対象とする。
  - **統制案の実装方法**
    - **「統制案のリストアップ」フェーズで洗い出した案のうち、設計コスト/運用コストを考慮して実装する内容を決定する。**

    例) DBVのレルムで保護を行う。AVDFでGRANT文を発行した証跡は取得する。

セキュリティ製品導入プロジェクトのご紹介

要件定義 （統制案の実装方法）



- 統制案の実装方法
  - ✓ 1人(ユーザ)に権限が集中しないように(1人で悪事ができない)権限分掌する。
  - ✓ 基本的には各ユーザは必要最低限の権限を保持する。
  - ✓ DBAの業務データへの不要な参照は監査したい。
  - ✓ ユーザ作成、権限付与はバックドア作成の危険性があるコマンドの監視する。

シンプルに構成

（検討結果の例）

- **不正なユーザ作成の防止** ⇒ **権限分掌で実現**
- **不正な権限付与の防止** ⇒ **権限分掌またはレルムで実現**
- **不要な業務データへのアクセスの抑制** ⇒ **レルムで実現**
- **不正管理作業の監査** ⇒ **AVDFの機能で実現**

  – 各統制内容の実装案については「**統制の強さ**」、「**統制実装**」を鑑みてコストのバランスを考慮する。

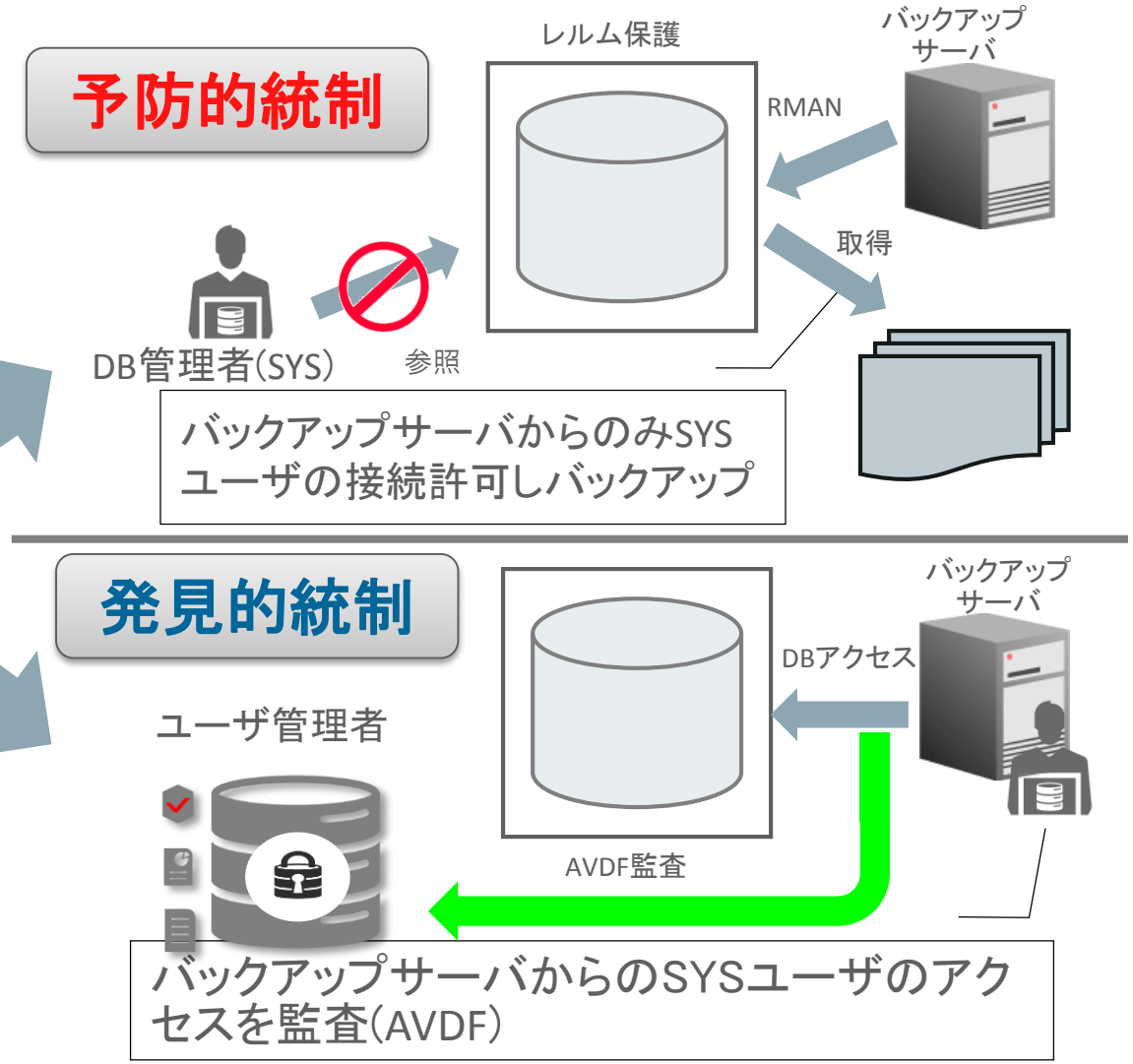
セキュリティ製品導入プロジェクトのご紹介

要件定義 （統制案の実装方法例）

- セキュリティ要件-XXXXXXXXXXXXXXX
- セキュリティ要件-XXXXXXXXXXXXXXX
- セキュリティ要件-特定のサーバからのみDBバックアップが行えること
- セキュリティ要件-XXXXXXXXXXXXXXX
- セキュリティ要件-XXXXXXXXXXXXXXX

考慮事項

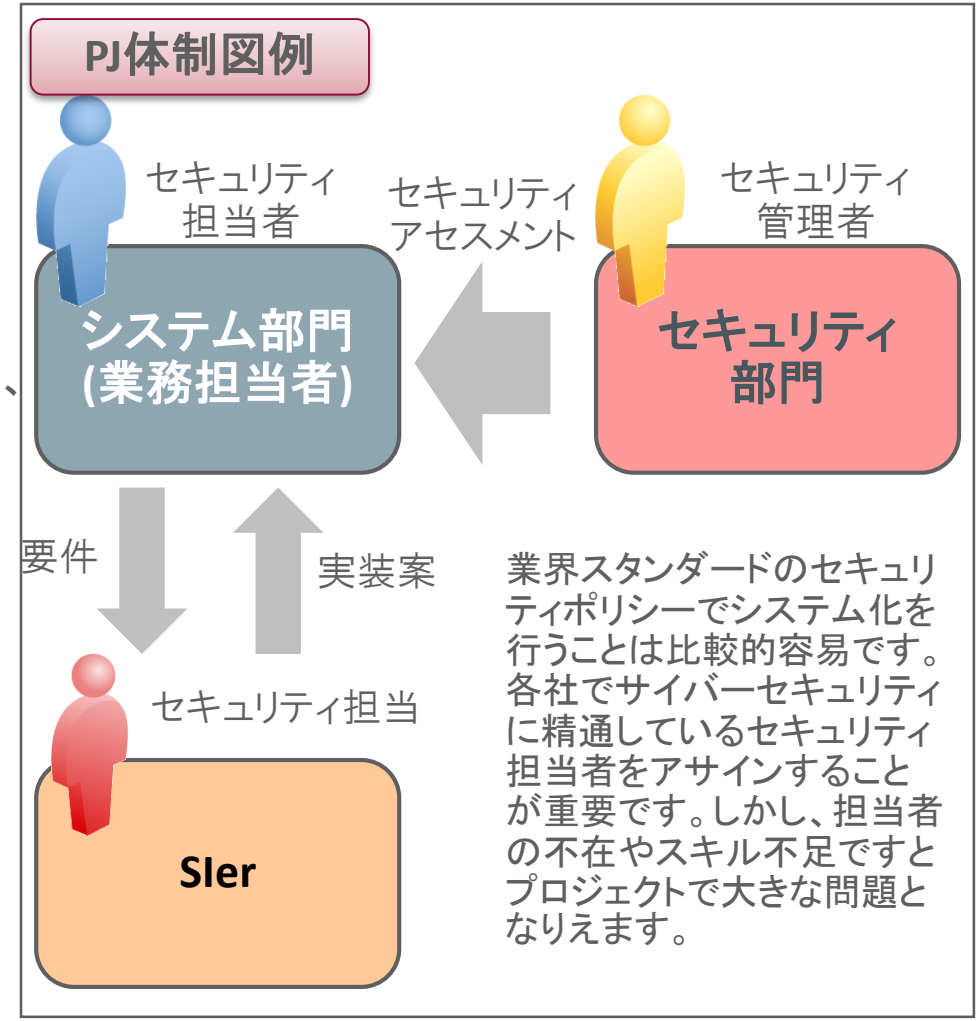
- RMANを使用するにはSYSDBA権限が必要
- 通常SYSDBAユーザでDBA業務を行わない



セキュリティ製品導入プロジェクトのご紹介

勘所

- **セキュリティはトップダウン**
  - セキュリティ方針はお客様の役員層からトップダウンで決まる。その方針をもとに要件定義行う必要があるため、PJでは必ずお客様の中でセキュリティ担当者を立てセキュリティ要件の洗い出しを行う。
- **関係者・部署または各担当との連携が重要**
  - ユースケースなどシステム部門(業務担当者)にしか出せない情報があり、関係者を巻き込んで進めることが重要である。またはその連携体制を作成・維持できることも重要である。
- **セキュリティ要件は都度見直す必要がある**
  - セキュリティの脅威は急速に進化する。常に一定のセキュリティレベルを保つため、定期的にセキュリティポリシーを見直すことが必要である。
- **統制内容に関する落とし所**
  - **最低ライン**を明確にしておく必要がある(「誰が何を実施したか」を特定できる発見的統制など)
  - 要件定義は作成するが、**スモールスタート**を目指す



まとめ

Oracleコンサルの考えるDBセキュリティの攻めと守りとPJの勘所

セキュリティ脅威に対するOracle製品

- 攻めとは ・・・ 【**予防的統制**】 ⇒ アクセス制御、権限分掌
- 守りとは ・・・ 【**発見的統制**】 ⇒ 監査証跡取得、証跡のモニタリング

DBセキュリティ製品導入プロジェクトの勘所

- セキュリティはトップダウン
- 関係者・部署または各担当との連携が重要
- セキュリティ要件は都度見直す
- 最低ラインを定めてスモールスタート

Oracle Database 12c おすすめ研修コース

ORACLE UNIVERSITY

Oracle Database 12*c*: Database Vault

概要	このコースでは、Oracle Database Vaultを有効化し、レルム、ルール·セット、コマンド·ルール、セキュア・アプリケーション・ロールを用いてデータベース・インスタンスのセキュリティを管理する方法を説明します。また、レポートや監視を使用してセキュリティ違反行為をチェックする方法について説明します。講義と演習と通じてOracle Database Vault が提供する強力なセキュリティ統制のための機能の活用方法を習得できます。
学習項目	■ Database Vaultの概要 ■ Database Vaultの構成 ■ 権限の分析 (12c 新機能) ■ レルムの構成 ■ ルール・セットの定義 ■ コマンド・ルールの構成 ■ ルール・セットの拡張 ■ セキュア・アプリケーション・ロールの構成 ■ Database Vaultレポートによる監査 ■ ベスト・プラクティスの実装
コース日数	**2 日間 【トレーニングキャンパス赤坂】2014/12/18-19**

Oracle Database 12*c*: セキュリティ

概要	このコースでは、認証、権限とロールの管理に加えて、Oracle Label Security、データベース暗号化、およびOracle Data Reductionなどを使用した機密データの保護する方法を説明します。また統合監査やファイングレイン監査を構成する方法について説明します。講義と演習を通じてデータベースへのアクセスを保護し機密性を高める方法を習得できます。
学習項目	■ セキュリティ要件について ■ セキュリティ・ソリューションの選択 ■ 基本的なデータベース・セキュリティ ■ ネットワーク・サービスの保護 ■ ユーザーのBasic認証と厳密認証の使用 ■ グローバル・ユーザー認証の使用 ■ プロキシ認証の使用 ■ 権限とロールの使用 ■ 権限分析の使用 (12c新機能) ■ アプリケーション・コンテキストの使用 ■ 仮想プライベート・データベースの実装 ■ Oracle Label Security の使用 ■ データ・リダクション (12c新機能) ■ データ・マスキングの使用 ■ 透過的機密データ保護の使用 (12c新機能) ■ 暗号化の概念とソリューション ■ DBMS_CRYPTO パッケージを使用した暗号化 ■ 透過的データ暗号化の使用 ■ データベース・ストレージのセキュリティ ■ 統合監査の使用 (12c新機能) ■ ファイングレイン監査の使用
コース日数	**5 日間 【トレーニングキャンパス赤坂】2015/1/19-23**

詳細は Oracle University Webサイト にてご確認ください。

ORACLE

Hardware and Software
Engineered to Work Together

VISION 2020

#1 CLOUD

ORACLE JAPAN


ORACLE®