DBセキュリティ監視運用ガイドラインWG
活動報告

Little eArth Corporation

株式会社ラック
サイバーセキュリティサービス事業部
サイバーリスク対策部
吉岡道明, CISSP

アジェンダ

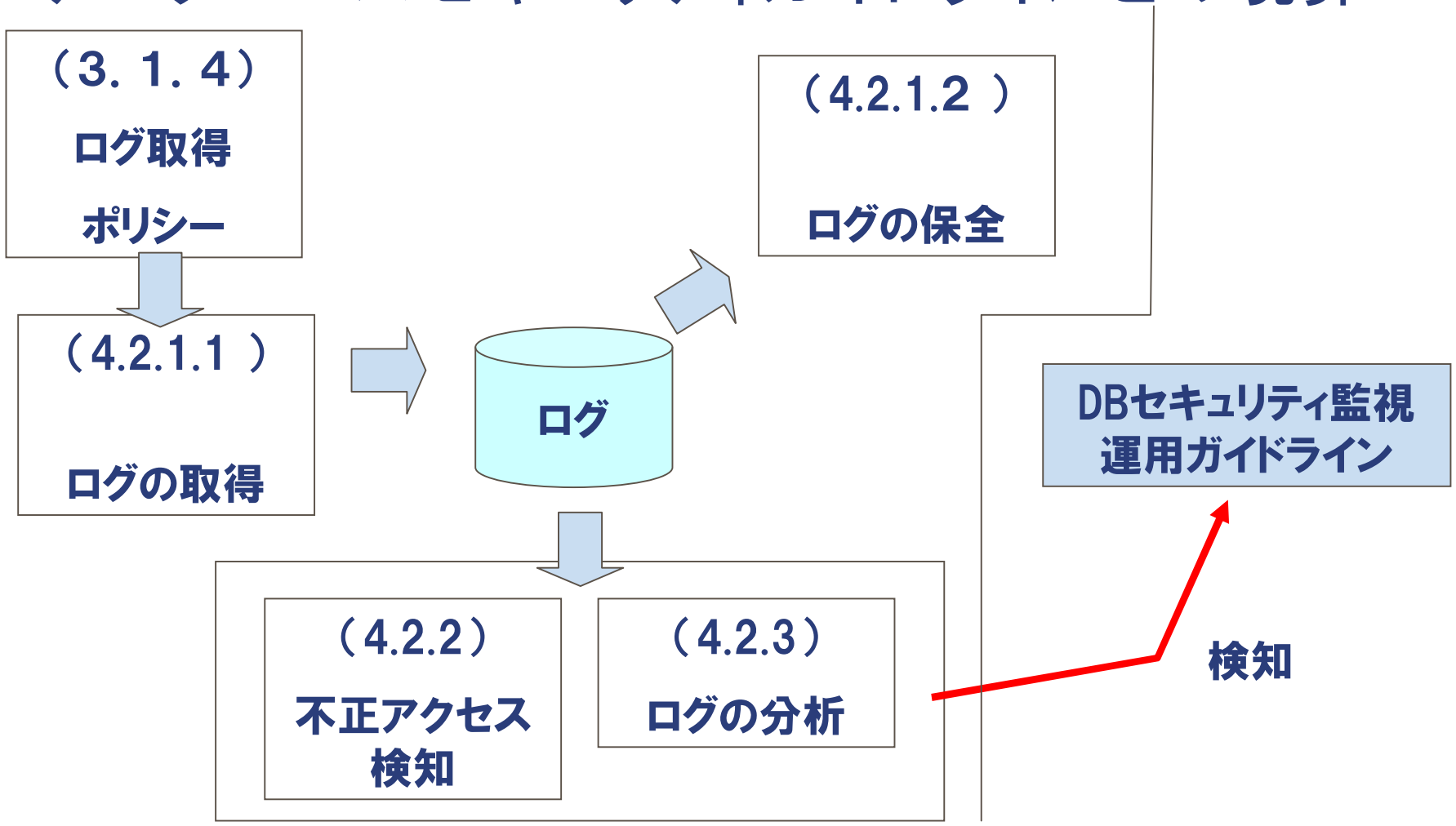
- 背景
- 検討内容
- 活動報告
- 今後の活動

背景

- データベースセキュリティガイドライン
  - セキュリティポリシーの作成
  - 技術的なデータベースセキュリティ対策
  - 「実施すること」をまとめている
- データベースセキュリティ監視運用ガイドライン
  - ログの取得、検知する仕組みを実装後の運用
  - 検知された不審なアクセスに対する対応（レスポンス）をまとめる
- ガイドラインの対象者
  - DBセキュリティ監視運用を推進しようとしているITセキュリティ担当者

背景

- データベースセキュリティガイドラインとの境界



前提条件

想定するデータベース運用

- 申請承認ベースのデータベース運用
  - 検知されたアクセスを精査するために必要

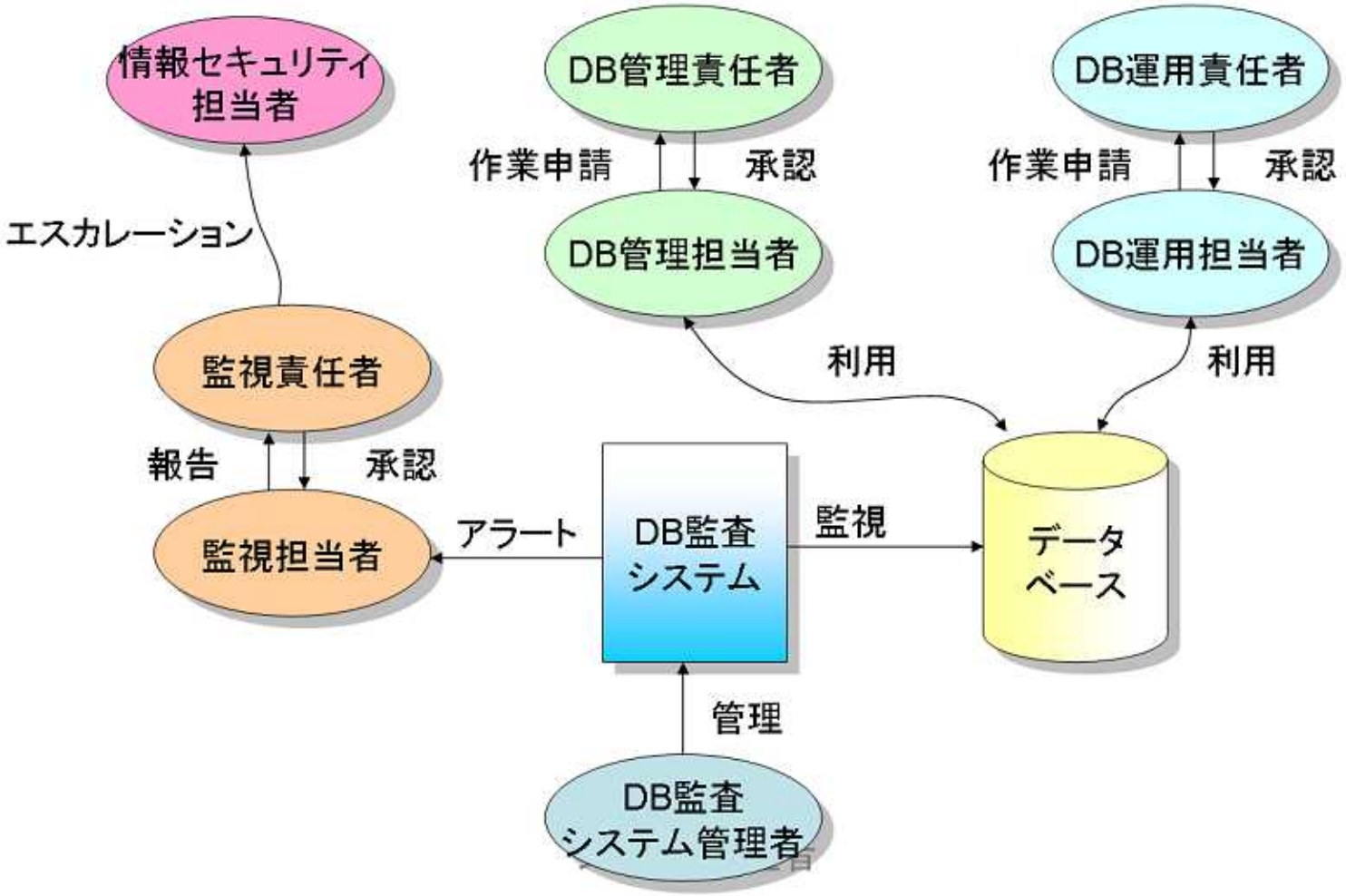
申請承認されていないアクセスはさせない
基本的な運用

前提条件

想定する登場人物

登場人物	定義、役割
DB管理者	・DBMS導入設定および運用を行う者。 ・データベースセキュリティガイドラインのDB管理者と同義。
DB管理責任者	・DB管理者の作業責任を持つ者。**作業承認者**。
DB運用者	・業務運用（テーブル、データ含む）を行う者。 ・データベースセキュリティガイドラインのDB運用者と同義。
DB運用責任者	・DB運用者の作業責任を持つ者。**作業承認者**。
監視担当者	・マニュアルに従い、監視業務を遂行する者。必要に応じて改善提案を実施する。
監視責任者	・監視担当者を統括する者。監視担当者からの報告の受付、および作業承認者。必要に応じて改善を実施する。
DB監査システム管理者	・不正アクセスの兆候を検知するシステムの管理業務（運用、検知条件設定等）を遂行する者。
情報セキュリティ担当者	・データベースに対するインシデントの内、不正アクセスと判断され緊急に組織として対応をしなければならない場合のエスカレーション先。

前提条件



目次(案)

目次(案)

目次(案)

- 3.2.3　問題レコードの定義
- 3.2.4　問題レコードの記録条件
- 3.3　報告業務

- 第4章　監視業務のアウトソーシング
- 別紙

利用してもらうために

- 本格的なデータベース監視運用を想定
- 小規模の監視体制でも利用できるように
- 各ガイドライン項目の意図を明確にする

活動報告

WGメンバー

- 参加表明者数　　12名
- 活動メンバー数　　7名

ミーティング開催

- 第1回　2008年6月26日
- 第2回　2008年7月29日
- 第3回　2008年8月29日
- 第4回　2009年12月9日
- 第5回　開催日調整中

今後の活動

- ガイドラインの執筆
- ベータ版の公開
  - DBSC内でのレビュー
- 正式版の公開

当WG活動にご興味がございましたら、
事務局までご連絡願います。

info@db-security.org

ご静聴ありがとうございました