『DBセキュリティ 製品別機能対応表』の活用法

Ver.080205

株式会社ラック　サイバーリスク総合研究所
データベースセキュリティ研究所
所長　大野 祐一, CISSP

アジェンダ

1. **背景と経緯**
2. **対応表の内容と活用方法**
3. **今後の活動**

データベースセキュリティガイドライン

- DBセキュリティガイドライン作成WGにて作成
  - 富士通大分ソフトウェアラボラトリ 三河尻リーダ
  - 2006年11月公開 (http://www.db-security.org/report.html)
  - 2008年1月～改訂を予定
  - ポイント
    - Webシステムモデル
    - DBサーバ内におけるセキュリティ対策にフォーカス
    - 対策の分類：「防御」、「検知・追跡」の2つに分類
    - 対策の重要度：「必須」、「推奨」の2つに分類

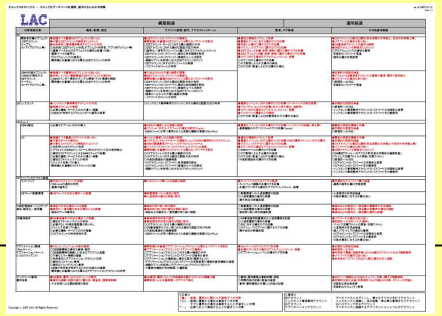
ガイドラインの位置付け

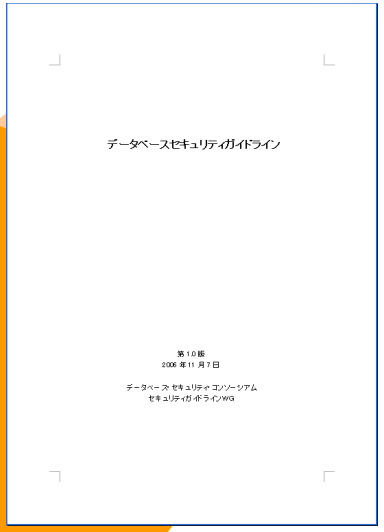
技術対策

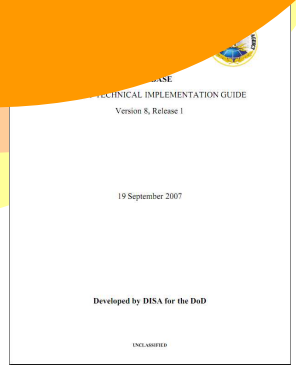
非DBサーバ

DB

データベース
セキュリティ
ガイドライン
(DBSC)







セキュアDBマトリクス

運用対策

背景

- ガイドラインで「あるべき姿」は提示できたが、具体的にDBMSや関連製品の「どの機能」を「どのように」利用して実装するかはSierに委ねられている
- 特に、ログの分野は注目されてきてはいるものの、DBMSでどこまでは標準装備されていて、サードパーティ製品ではどういうことが補われているのかがイマイチわかりくい。
- せっかく作ったガイドラインを有効活用してほしい。
- 上記課題を解決するよう成果物を作ろう！

大まかな流れ

- 誕生
  - 2006.5月 総会後の限定セミナーにて活動計画発表
  - 2006.6月 会員企業に対して募集開始 ⇒ 10社19名でスタート→18社、28名
- 立ち上げ期
  - 当初はガイドラインの内容の手順書を作成する予定だった。
  - WGメンバーでテーマを検討した結果、
    - 分野：関心の高い3分野に分割
    - 成果物：手順書の前にDBMS別、ツール別の機能対応表を作成することに
- 対応表 作成期（～2007.9月）
  - ガイドの記載内容をどこまで詳細化するか（粒度）
  - ○×△の定義（判定基準）
- 内容レビュー（2007.12月）
  - 各社が記載した内容の確認
  - ベンダーによる最終確認
- 公開（2008.2月）
  - セミナー翌日である2008年2月公開予定

テーマを決めるに当たって

- ガイドラインに記載されている内容を**一歩進めた何か**を作り、公開したい。

- WGリーダの想いとしては、
  - 小さくても良いから頻繁に公開したい
  - **技術者が重宝するもの**を作りたい

メンバーから出されたテーマ案

- メンバーからテーマ募集
  - 1) テーマタイトル
  - 2) アウトプットの構成イメージ
  - 3) 必要な環境
  - 4) その他ご意見がございましたら。。。

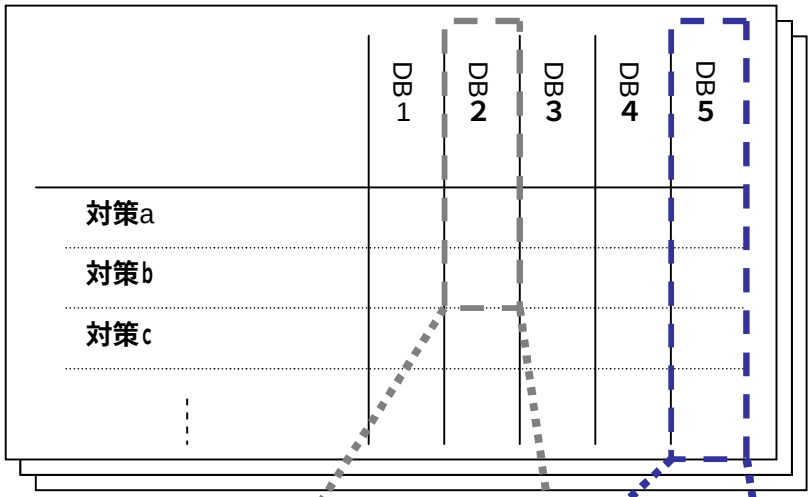
議論した結果。。。

第4章　DBセキュリティ対策
- 4.1　防御系のセキュリティ対策
  - 4.1.1 初期設定
  - 4.1.2　認証
  - 4.1.3　アクセスコントロール
  - 4.1.4　暗号化
  - 4.1.5　外部媒体の利用制御
  - 4.1.6　その他
- 4.2　検知、追跡系のDBセキュリティ対策
  - 4.2.1 ログ管理
  - 4.2.2　不正アクセス検知
  - 4.2.3　監査
- 4.3　対策指針
  - 4.3.1　DBセキュリティポリシーの策定
  - 4.3.2　人的対策

①
②
③

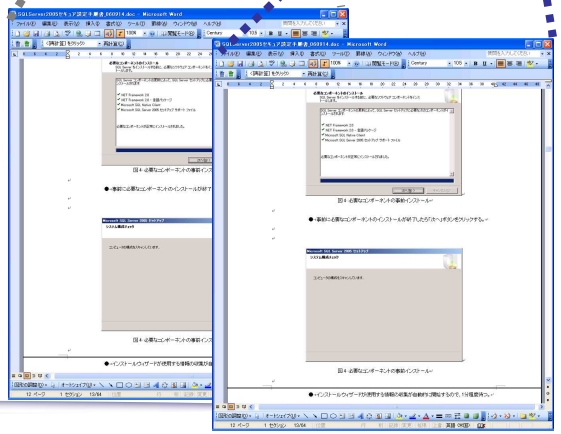
①～③の
3種類に分類

1 DBセキュリティ 製品別機能対応表



2 実装手順書

対応表の内容を
深堀し、手順、
注意事項を記述



実装手順書

- 目的
  - DBMSとOS、その他製品等環境と目的（セキュリティ対策）が決まった場合に、対応表の中身を実装する場合の設計や実装時のポイントや実装／未実装時のリスクを把握でき、さらに具体的な手順がわかるようにする。
- 対象範囲
  - 範囲：対応表の1列分ずつ作成予定
- 対象者：データベース技術者、セキュリティ技術者
- 利用時期：システム設計、製品導入時
- 備考
  - メンバーのパワーを対応表に集中させるため、手順書作成に向けた活動は対応表完成後に再始動予定

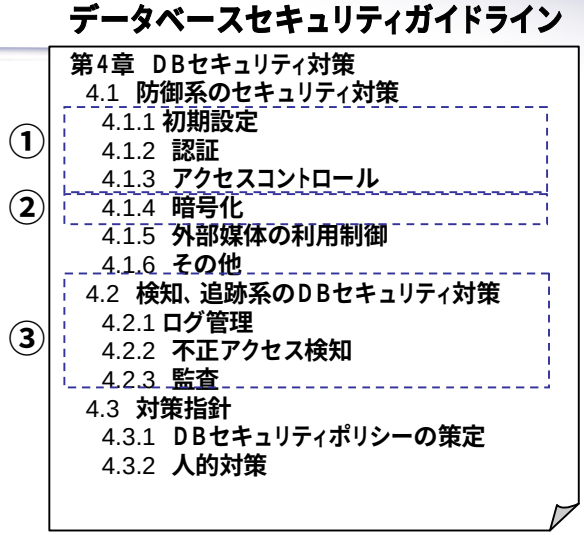
比較表改め対応表

- 目的
  - ガイドに記載されている対策を実装する上で、製品別の対応可否、具体的な機能名を比較でき、製品選定や対策設計時に役立てたい。
- 対象範囲
  - 対策範囲：製品の機能比較がメイン
    - 運用的な対策ではなく、技術的対策分野を抽出
    - 「初期設定」、「ログ」、「暗号化」に絞込み
  - 対象製品：公開前にベンダーチェックが可能な製品
    - DBMS：Oracle、SQL Server
    - DB監査製品：Audit Master、Chakra、IP-Locks、PISO、SSDB監査、SecureSphere
- 対象者：アーキテクト、システム設計者
- 利用時期：システム設計、製品選定

対応表

4.1.2 認証					
	4.1.2.1 アカウントの管理				
		(1)必要なアカウントの作成			
			●必要なアカウントを洗い出し、作成する	必須		
			必要なアカウントの洗い出し		×(必要なアカウントの洗い出しは、ポリシーやルールなどに従い実施する)	
			アカウント作成		◎ ・[GUI] Oracle Enterprise Manager(アカウント管理機能) ・[SQL] Create User	◎ ・[GUI] Management Studio(アカウント管理機能) ・[SQL] Create User
			●利用者の権限を規定する	必須	×(権限の規定は、あらかじめポリシーやルール等に規定しておく)	
			●管理者アカウントと一般アカウントは、それぞれの権限に応じて別々に作成する	必須	◎ ・[GUI] Oracle Enterprise Manager(アカウント管理機能) ・[SQL] Create User	◎ ・[GUI] Management Studio(アカウント管理機能) ・[SQL] Create User
		(2)不要なアカウントの削除				
			●未使用となったアカウントは削除する	必須		
			未使用アカウントの抽出		×(未使用アカウントの抽出は、ポリシーやルールなどに従い実施する)	
			アカウント削除		◎ ・[GUI] Oracle Enterprise Manager(アカウント管理機能) ・[SQL] Drop User	◎ ・[GUI] Management Studio(アカウント管理機能) ・[SQL] Drop User
			●DBMSインストール時にデフォルトで作成される業務に必要がないアカウントは削除する	必須	◎ ・[GUI] Oracle Enterprise Manager(アカウント管理機能) ・[SQL] Drop User	◎ ・[GUI] Management Studio(アカウント管理機能) ・[SQL] Drop User

対応表



- 分野
  - 以下の3分野毎に作成
    - 初期設定 (4.1.1～4.1.3)
    - 暗号化 (4.1.4)
    - ログ (4.2.1～4.2.3)
- 横軸
  - 基本はDBMS製品、ログ編のみサードパーティ製品も
- 環境
  - バージョン：検討時点で最新版
  - エディション：各製品の最高エディションで比較
  - オプション：DBMSのオプションを必要とする場合は、マス中に※印で記述

対応表

- 縦軸
  - ガイドの●のレベルを必要に応じて細分化
    - 例)

4.1.2.1　**アカウントの管理**
(1)必要なアカウントの作成
なりすましなどのアカウントの不正利用を防ぐ為、以下の対策を実施すること。
●必要なアカウントを洗い出し、作成する。(必須)

4.1.2　認証			
	4.1.2.1　アカウントの管理		
		(1)必要なアカウントの作成	
		●必要なアカウントを洗い出し、作成する。	必須
		必要なアカウントの洗い出し	
		アカウント作成	

対応表

- マス内の表現
  - 構成
    - 1段目：対応可否・・ ◎○△×
    - 2段目：機能名・・対策するために利用する製品の機能名
      ただし、あまりにもわかりきった機能名は省略する
    - 3段目：UI・・該当機能を実装する際のインタフェース
    - 4段目：オプションの必要有無 必要な場合のみ「※ｘｘｘオプションが必要」と記述する
  - 対応可否
    - ◎：対象製品の標準機能で**対策可能、さらにGUIなど簡単設定が可能**
    - ○：対象製品の標準機能で**対策可能**
      - 標準機能を利用して作りこみが発生する場合も○
        ただし、作りこみが発生する旨を記述
    - △：対象製品の標準機能で**一部は対策可能**
    - ×：対象製品の標準機能では**対策不可能**
      - 多くの場合は、調査、設計や、運用等で対策するもので、DBMS製品の機能で対策すべきでないもの

対応表の活用方法

- 新規システム構築時の要件や自社のセキュリティ対策基準に反映
  - 対応表で○◎となっている部分に関しては、検証の必要はないので、要件として採用しやすい
- 要件を満たす製品の選定
  - ガイド⇒対応表を確認し、実装すべき機能の有無を確認
    - 製品の機能で実現できない場合には代替の運用を検討
- 自社の設定、運用状況のセルフチェック
  - ガイド、対応表に記載されている内容の実施有無を確認

今後の方向性

- 暗号化
  - 彦田さんの新WGで再スタートを切る予定
- 各列の手順書作成

- 対象DBMSの拡大
  - DB2、MySQL、PostgreSQL...etc
- 利用者の対象を非DB技術者へと拡大
  - 各対策の難易度や手間（工数）などの定量化、ランク化
  - 発注者側の用途拡大につながる改善（具体的には今後協議）

もし、当WGにご興味がございましたら、事務局までご連絡願います。

ご静聴ありがとうございました