

2007年度 セキュリティガイドラインWGの活動報告

平成20年2月5日

(株)富士通大分ソフトウェアラボラトリ(OSL)

セキュリティセンター 三河尻



背景

ガイドラインの公開後、1年が経過し、さまざまな意見や要望が出てきている。

世の中では、個人情報保護法や新会社法、金融商品取引法など、コンプライアンスへの対応が求められている。

このような中で、データベースセキュリティの重要性や位置づけも変化している。

今回、ガイドライン実装WGの成果も踏まえ、より実践的なガイドラインを目指し、改定を実施する。



目的

- データベースセキュリティガイドラインの内容の充実
 - ・社会動向の反映
 - ・最新技術動向の反映
 - ・実装WG成果反映 など

- データベースセキュリティガイドラインの国内への一層の普及
 - ・他団体(JNSAなど)と連携
 - ・公的機関のガイドラインとの連携 など



検討内容

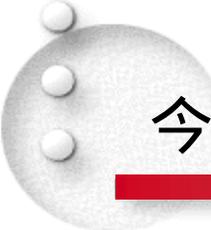
- データベースセキュリティガイドラインWG進め方
 - ・役割分担を行いガイドラインを修正
 - ・メールによる意見交換
 - ・月一回程度の集合レビュー



検討内容

- データベースセキュリティガイドラインの改定指針
 - ・実装WG成果のフィードバック
 - ・情報資産の重要度による重み付けの実施及び、対策レベル（必須、推奨）の見直し
 - ・ガイドラインの内容とフレームワーク(*)との対応付け
 - ・事業継続やJ S O X等の対応

(*)フレームワーク：ISO27001、政府統一基準など

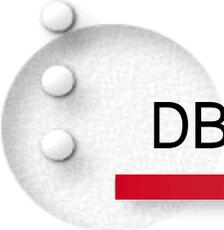


今後のスケジュール(想定)

- ・ 1月 進め方検討・決定 (実施済)
- ・ 2月～3月 改定方針の決定・ガイドライン修正
- ・ 4月～5月 最終調整
- ・ 6月～7月 DBSCサイト上で公開

この時点で本WGは一旦、終了

公開後、反応に応じて再開を検討



DBセキュリティガイドライン(目次)

第1章 はじめに

1.1 目的

1.2 本ガイドラインの前提

第2章 全体のセキュリティ対策における DBセキュリティの位置づけ

2.1 想定システムモデル

2.2 全体のセキュリティ対策の概要

2.3 DBセキュリティの位置付け、対象範囲

2.4 DBに関する脅威の定義

2.4.1 脅威の定義

2.4.2 登場人物の定義

2.4.3 DBに関する情報資産の定義

2.4.4 手口の定義

2.4.5 不正アクションの定義

2.4.6 脅威の一覧

第3章 DBセキュリティ対策

3.1 防御系のセキュリティ対策

3.1.1 初期設定

3.1.2 認証

3.1.3 アクセスコントロール

3.1.4 暗号化

3.1.5 外部媒体の利用制御

3.1.6 その他

3.2 検知、追跡系のDBセキュリティ対策

3.2.1 ログ管理

3.2.2 不正アクセス検知

3.2.3 監査

3.3 対策指針

3.3.1 DBセキュリティポリシーの策定

3.3.2 人的対策