

第5回 データベース・セキュリティ・コンソーシアム セミナー

DBセキュリティ安全度セルフチェックWG 活動報告



株式会社ラック
サイバーリスク総合研究所
コンピュータセキュリティ研究所
研究員 須田 堅一, CISSP



アジェンダ

1. **WG設立の背景**
2. **活動内容**
3. **DBセキュリティ安全度セルフチェック**
4. **統計レポート**

WG設立の背景

- DBSCから発行されたガイドラインによって、「データベースのあるべき姿」が分かった

ガイドラインと自身のDBを比較

- 自社が管理／運用しているDBは安全か？
- 他社と比較して、遅れていないか？

問題、疑問を解決するため

- DBのセキュリティレベル(安全度)を簡単にチェックできる
- 現状を客観的に把握でき、更には弱点を把握することで適切にセキュリティ対策の実施要件を作成できる
- データベースセキュリティ対策状況の統計値を分析し、DBSCの今後の様々な活動・啓発・情報発信などに役立てる

活動内容

1. 活動内容

- DBセキュリティ安全度セルフチェック公開
- 統計レポート公開

2. 活動実績

2008年度

- 5月 WGスタート
- 6月～1月 ミーティング（1回／月）
- 2月 DBセキュリティ安全度セルフチェック公開

2009年度

- 6月 統計レポートVer. 1 公開
- 12月～2月 ミーティング（1回／月）
- 2月 統計レポートVer. 2 公開

DBセキュリティ安全度セルフチェック

<http://www.db-security.org/selfck/>

データベースセキュリティ安全度セルフチェック - Mozilla Firefox

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

Proxy: なし 適用 編集 削除 追加 状態: プロキシ接続 なし 設定

データベースセキュリティ安全度セルフ...

データベースセキュリティ安全度セルフチェック

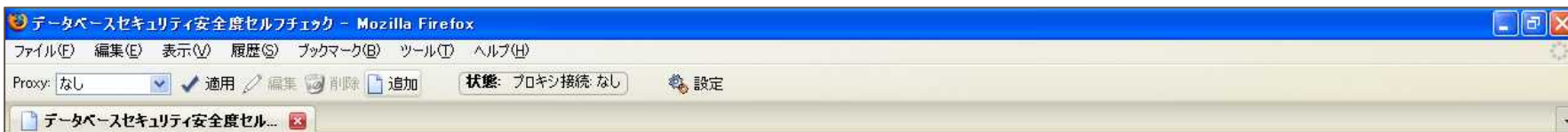
データベース・セキュリティ・コンソーシアム (DBSC)

問1. DBMSの初期設定に関する以下の設問に対して、次の選択肢の中から最も当てはまる回答をお選びください。(全項目必須)

| | |
|-----|---|
| (1) | 最新のセキュリティ対策を反映するため、導入しているDBMSバージョンの最新パッチを適用していますか？ |
| 回答 | <ul style="list-style-type: none"><input type="radio"/> はい<input type="radio"/> ポリシーに従い、必要に応じて適用している<input checked="" type="radio"/> いいえ<input type="radio"/> 対策できているかどうか不明<input type="radio"/> 質問の内容が理解できない |
| (2) | 不正な機能利用を防ぐため、導入時に必要な機能を選択し、対象機能のみを導入していますか？ または、インストール時にデフォルトで導入される機能の中で、使用しない機能があれば、削除または無効化していますか？ |
| 回答 | <ul style="list-style-type: none"><input type="radio"/> はい<input checked="" type="radio"/> いいえ<input type="radio"/> 対策できているかどうか不明<input type="radio"/> 質問の内容が理解できない |
| (3) | 不正利用を防ぐため、インストール時に作成されるポートや、一般的なポート番号を変更していますか？ |
| 回答 | <ul style="list-style-type: none"><input type="radio"/> はい<input checked="" type="radio"/> いいえ<input type="radio"/> 対策できているかどうか不明 |

DBセキュリティ安全度セルフチェック

<http://www.db-security.org/selfck/>

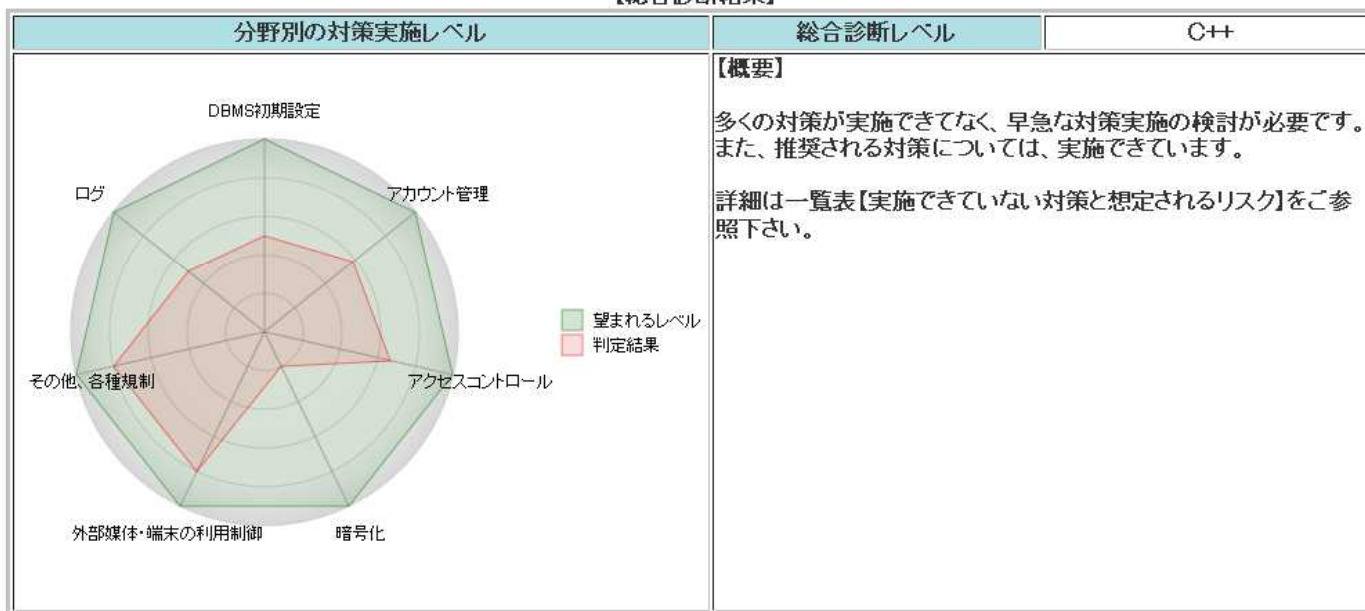


データベースセキュリティ安全度セルフチェック

データベース・セキュリティ・コンソーシアム (DBSC)

1. 総合診断結果

【総合診断結果】



注)この診断結果は、DBSC発行データベースガイドラインをベースに対策実施レベルを算出したものであり、安全性を保証するものではありません。

【診断結果レベルの解説】

| レベル | 概要 |
|-----|---|
| A | 重要とされる対策は十分に実施されている状態。 |
| B | いくつかの重要とされる対策が実施できてなく、不足している対策実施の検討が望まれる状態。 |
| C | 実施できていない重要とされる対策が多く、早急な対策実施の検討が必要な状態。 |
| D | ほとんど全ての対策ができてなく、推奨される対策、対策実施の検討が必要な状態。 |

統計レポート

http://www.db-security.org/report/dbsc_selfck_ver2.1.pdf

dbsc_selfck_ver2.1.pdf - Adobe Reader

ファイル(F) 編集(E) 表示(V) 文書(D) ツール(T) ウィンドウ(W) ヘルプ(H)

3. 診断結果レベル別 利用比率

診断結果のレベルを様々な切り口で分析することで、データベースセキュリティの対策実施度の傾向や、実施レベルの高低の理由などを知ることができる。

3.1. 診断結果レベル 内訳

| 診断結果レベル | 内訳 (割合) |
|---------|---------|
| A | 9% |
| B | 15% |
| C | 44% |
| D | 32% |

診断結果レベルはCとDで80%程度を占めており、特にレベルDは「必須」とされている対策の半分以上ができていないレベルである。ガイドラインで「必須」と定義されている対策は、「該当システムにおいて対応しなければ、セキュリティ上問題があると判断される対策」とされている。その必須対策のほとんどが実施できていないレベルDと判定されたシステムは、非常に危険な状態であると言える。

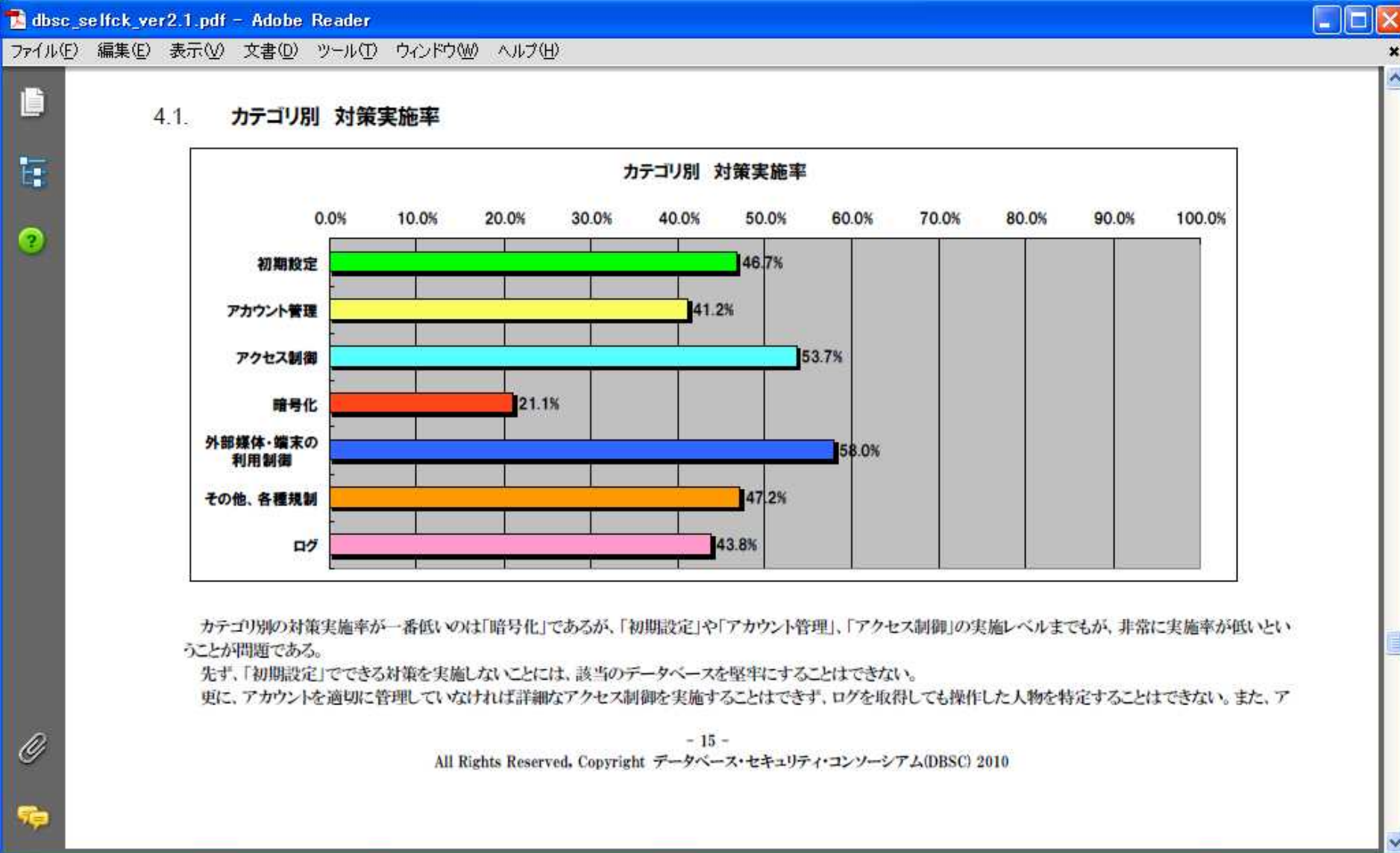
また、レベルCにおいても、実施できていない「必須」対策が多い状態であることから、至急、見直しを検討すべきである。


- 8 -

All Rights Reserved, Copyright データベース・セキュリティ・コンソーシアム(DBSC) 2010

統計レポート

http://www.db-security.org/report/dbsc_selfck_ver2.1.pdf





**当WG活動や統計レポートに
ご興味がありましたら、
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