ＤＢセキュリティ安全度セルフチェックＷＧ 活動報告

Little eArth Corporation

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

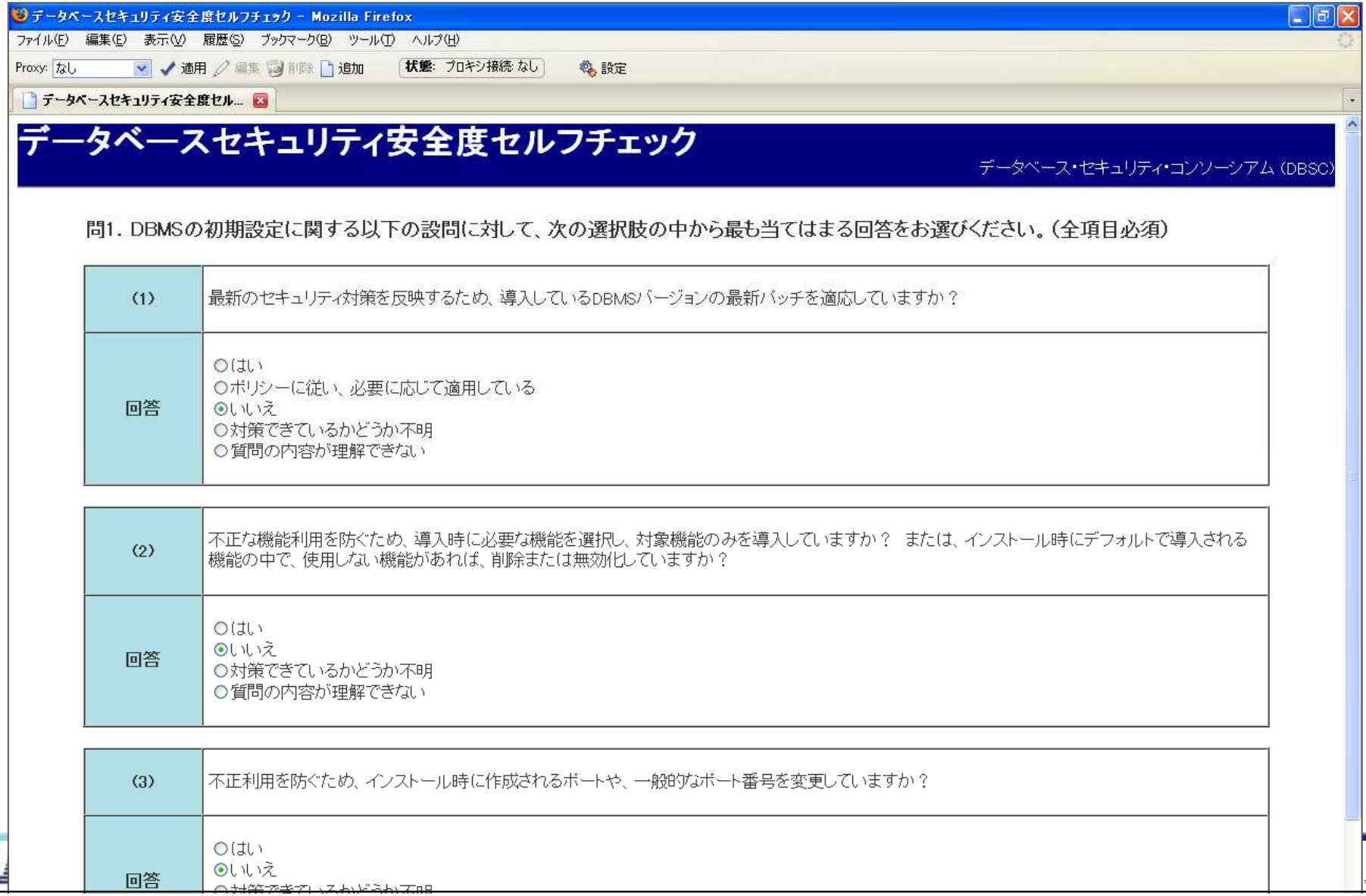
- 5月　　WGスタート
- 6月～1月　ミーティング（1回／月）
- 2月　　DBセキュリティ安全度セルフチェック公開

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

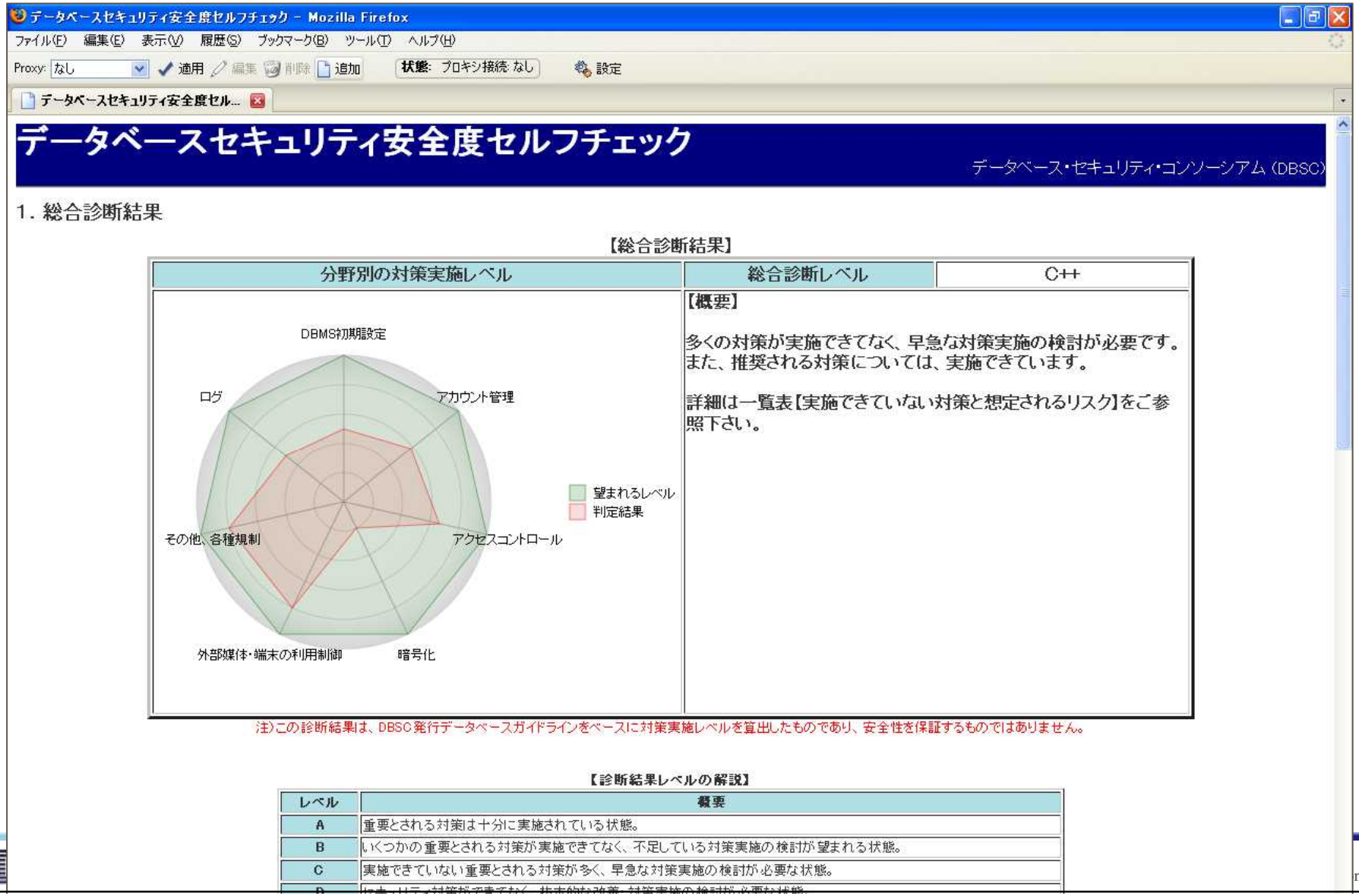
DBセキュリティ安全度セルフチェック

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



DBセキュリティ安全度セルフチェック

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



統計レポート

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

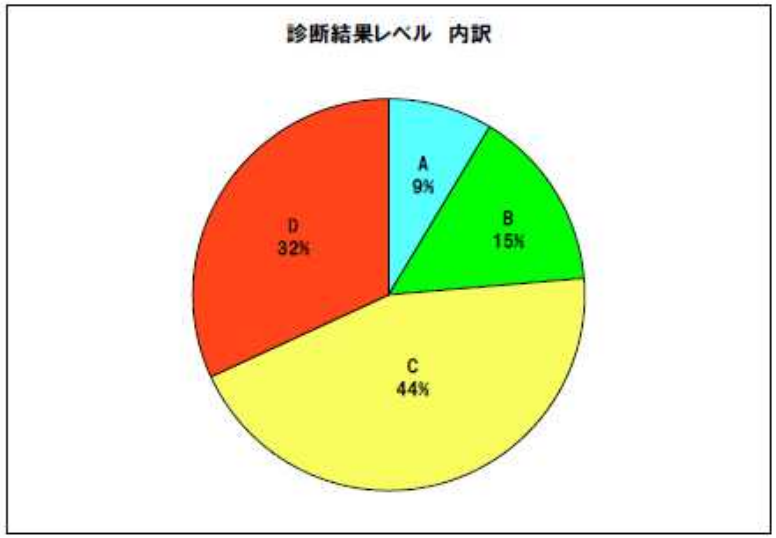
dbsc_selfck_ver2.1.pdf - Adobe Reader

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。

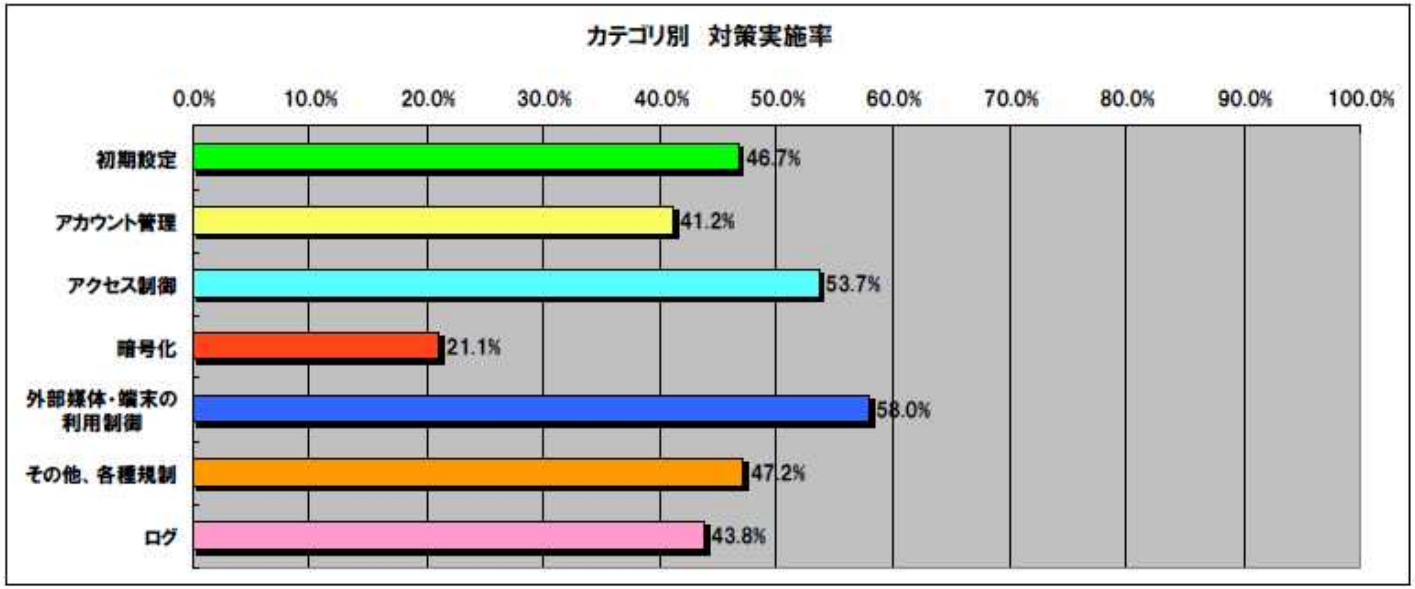
統計レポート

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)

4.1. カテゴリ別 対策実施率



カテゴリ別の対策実施率が一番低いのは「暗号化」であるが、「初期設定」や「アカウント管理」、「アクセス制御」の実施レベルまでもが、非常に実施率が低いということが問題である。

先ず、「初期設定」でできる対策を実施しないことには、該当のデータベースを堅牢にすることはできない。

更に、アカウントを適切に管理していなければ詳細なアクセス制御を実施することはできず、ログを取得しても操作した人物を特定することはできない。また、ア

- 15 -

当WG活動や統計レポートに
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