

情報セキュリティ教本と2007 マネジメントコースとの対応

情報セキュリティセミナー2007 マネジメントコース

【マネジメントコース概要】

具体的な事例を用いて、情報資産を組織的かつ継続的にどう管理すればよいかについて、情報セキュリティ対策ベンチマーク、情報管理等に触れながら説明する。

【マネジメントコースの対象者】

企業における管理面からの情報セキュリティ対策に関して理解を深めたい方
(セキュリティ教育担当者、経営者、セキュリティ責任者、マネジメントの観点からの対策を担当するセキュリティ担当者、システム管理者)

マネジメントコース 講演資料 目次 (教本の各章との対応)

1. 背景と基礎知識

- 1.1 情報セキュリティに関わる脅威の傾向
- 1.2 情報セキュリティ対策の目的、方針
- 1.3 情報セキュリティマネジメントと PDCA サイクル **【教本 1 章 4. p.25-28】**
- 1.4 情報セキュリティ対策実施上の問題点と施策ツール

2. 情報セキュリティ対策ベンチマーク

【教本 10 章 2.2 p.276-283】

- 2.1 情報セキュリティガバナンスと自己診断テストの活用
- 2.2 情報セキュリティベンチマークの概要
- 2.3 情報セキュリティベンチマークの利用方法
- 2.4 情報セキュリティベンチマークの診断結果
- 2.5 情報セキュリティベンチマークの利用状況

3. ケーススタディ：パソコンの紛失

【教本 8 章 4.3 p.222-227】

- 3.1 事故発生の経緯
- 3.2 事故対応の流れ
- 3.3 情報の特定
- 3.4 事故対応：緊急対策会議での決定
- 3.5 A 社の事故対応体制
- 3.6 对外発表のポイント
- 3.7 再発防止策の例

4. そこにある情報資産

- 情報資産の洗い出し **【教本 4 章 1. p.70 - 75】**

- 4.1 守るべき情報資産とは
- 4.2 情報資産の例
- 4.3 情報資産の価値
- 4.4 情報資産はどこにある？
- 4.5 情報資産の洗い出し
- 4.6 情報の管理責任者、管理担当者、利用者
- 4.7 機密情報、個人情報、その他の情報
- 4.8 情報システム、電子文書、紙文書

5. 情報の分類と格付け **【教本 4 章 2. p.76 - 94】**

- 5.1 情報の分類と格付けはなぜ必要か？
- 5.2 政府機関統一基準の分類と格付け
- 5.3 機密性、完全性、可用性に応じた情報の分類
- 5.4 情報の分類と格付けの基準 (例)
- 5.5 情報漏えい防止に留意した情報の分類例

6. 情報のライフサイクルと

情報の取扱い **【教本 4 章 3. p.82 - 94】**

- 6.1 情報のライフサイクル
- 6.2 情報の作成と入手
- 6.3 情報の利用・加工
- 6.4 情報の保存
- 6.5 情報の移送 (送信と運搬)
- 6.6 情報の提供
- 6.7 情報の消去

7. 情報セキュリティポリシーと

情報の管理 **【教本 3 章 p.40 - 68】**

- 7.1 情報セキュリティポリシーの構成
- 7.2 情報セキュリティ基本方針
- 7.3 情報セキュリティ対策基準
- 7.4 情報セキュリティ実施手順
- 7.5 対策基準とガイドライン・実施手順の関係
- 7.6 情報セキュリティポリシー運用上の留意点
- 7.7 情報の管理に関する複数の諸規程

8. 情報の管理と対策のヒント

- 8.1 情報の管理と対策の基本原則
- 8.2 リスク対応とは **【教本 5 章 4. p.117-121】**
- 8.3 リスク対応 - 相互の関係

9. 情報の管理と法令遵守 **【教本 12 章 p.316-326】**

- 9.1 IT 社会の変化と法的対応の変遷
- 9.2 個人情報保護法
- 9.3 不正競争防止法