情報セキュリティ管理者向け　基礎から学べる情報セキュリティ管理講座 カリキュラム

１．期間

２日間　※AM：9:00～12:00（３時間）、PM：13:00～17:00（４時間）

２．対象者

情報セキュリティ管理者、責任者

（所属部署のセキュリティ管理を推進する人または部署のセキュリティ責任者）

３．講座概要

情報セキュリティの基礎を講義で学び、リスク分析や情報セキュリティ対策の策定・管理、インシデント対応の演習を通じ、実践力を身に付ける。

４．学習項目とスケジュール概要

1日目 AM：情報セキュリティの基礎と管理（講義）

１．情報セキュリティの重要性

- 社会的背景と組織のリスク管理
- 情報セキュリティ（機密情報保護）に関する法律
- 情報セキュリティ事件・事故の事例
- よくある事故事例とその主たる要因

２．情報セキュリティの基礎

- 情報セキュリティとは
- 情報資産と脅威と脆弱性
- 情報セキュリティのリスク

３．情報セキュリティ対策

- 情報セキュリティ対策とは
- 必須の情報セキュリティ対策
- あった方が良い情報セキュリティ対策
- 情報セキュリティ対策のポイント

４．情報セキュリティ管理

- 情報セキュリティ管理とは
- 情報セキュリティポリシーの策定（Plan）
- 情報セキュリティポリシーの導入と運用（Do）
- 情報セキュリティポリシーの確認と評価（Check）
- 情報セキュリティポリシーの改善（Act）

５．最近の脅威の変遷

- 攻撃目的の変遷
- Web システムの脅威と脆弱性
- 標的型攻撃

- 重要インフラへの攻撃
- スマートフォン・SNS 利用上の脅威
- その他の攻撃

1 日目 PM：

６．リスク管理（講義）

- リスク管理とは
- リスクの特定と分析（詳細リスク分析）
- リスク評価
- リスク対応

７．リスク管理（演習）

例題企業における情報資産に対し、リスクを洗い出し、リスク分析をグループで検討する。

- 例題企業の概要説明
- リスク分析の検討
- グループ発表
- まとめ

2 日目 AM：

８．情報セキュリティ管理（演習）

例題企業におけるセキュリティ上の問題点を抽出し、どのような対策を取るべきかグループで検討する。

- 問題点の洗い出し
- 問題点に対する対策の検討
- 対策の優先順位付け
- グループ発表
- まとめ

2 日目 PM：

９．インシデント対応（講義）

- 事前対応と事後対応
- 事故対応の流れ
- インシデント対応チーム（CSIRT）の役割と概要
- インシデント対応と BCP・BCM

10．インシデント対応（演習）

例題企業でインシデント（セキュリティ事故）が発生したとき、どのような対応を取るべきかグループで検討する。

- インシデント対応の検討
- グループ発表
- まとめ