115

脅威情報とセキュリティ対策

人材育成上の課題・目標

・脅威となる対象・種類を知りたい
・セキュリティ対策の進め方を知りたい
・情報セキュリティの管理体制を確立したい
・不正アクセス、ウイルス感染やサイバー攻撃の脅威から情報資産を守りたい
・社内ネットワークにセキュリティ対策を施したい

課題解決・目標達成を目指して

・セキュリティリスクの対象と確認方法を理解する
・インシデントの種類を理解する
・セキュリティポリシーの策定方法を習得する
・社内ネットワークのセキュリティ対策を構築できる

コースのねらい

社内の情報セキュリティを維持するために、セキュリティポリシーの必要性を理解し、セキュリティ対策に必要な知識と技能を習得する。

カリキュラム（例）

	基本項目	主な内容（例）
基本要素	■ 脅威情報	・ウイルス・マルウェア ・標的型攻撃 ・フィッシングサイト ・情報漏えいによる損害 ・インシデント事例と対応
基本要素	■ セキュリティポリシー	・セキュリティポリシーの必要性 ・セキュリティ対策の考え方 ・管理体制 ・セキュリティ対策規定集の作成
基本要素	■ セキュリティ対策手法	・ウィルス対策及びセキュリティパッチの適用 ・パケットフィルタリング ・アプリケーションレベル・ゲートウェイ ・不正侵入検知
基本要素	演習（例）	・ＩＴ業務のインシデントの洗い出し（情報資産、脅威、脆弱性などの洗い出し） ・セキュリティ対策規定集の作成演習
応用・実践要素（例）		・インシデント発生事例に基づくケーススタディ ・利用者サイドのセキュリティ対策 ・プライバシーマーク制度

※　基本項目は必須としますが、主な内容や演習、応用・実践要素は、ご要望に応じてカスタマイズすることが可能です。
なお、訓練時間によっては、上記の全ての内容を実施できるものではありません。

日程設定と受講料（例）

（１）１日（６時間）コース
２，２００円（税込）
（２）２日間（１２時間）コース
３，３００円（税込）

※　金額は、１名あたりの受講料です。
※　４～３０時間の間で設定可能です。
※　推奨訓練時間は、６～１２時間です。

推奨対象者

ＩＴにおけるセキュリティ対策に取り組む方

関連コース

A　バックオフィス
・ＩｏＴ導入に係る情報セキュリティ　・テレワーク活用
・テレワークを活用した業務効率化
B　組織マネジメント
・個人情報保護と情報管理
・リスクマネジメントによる損失防止対策
・ｅビジネスにおけるリーガルリスク
・ネット炎上時のトラブル対応
・知的財産権トラブルへの対応（1）
D　ネットワーク
・ワイヤレス環境に必要となる無線ＬＡＮとセキュリティ
・社内ネットワークに役立つ管理手法
D　情報発信
・ＳＮＳを活用した情報発信
D　倫理・セキュリティ
・情報漏えいの原因と対応・対策　ほか