テレワークに対応したセキュリティ対策

人材育成上の課題・目標

・テレワークにおいてどのようなセキュリティリスクがあるかを知りたい
・テレワーク時の情報漏えい対策を知りたい
・テレワークにおける秘密事項の取扱い方法を知りたい
・インシデント発生時の初期対応を知りたい

課題解決・目標達成を目指して

・テレワーク特有のセキュリティリスクを理解する
・テレワークに対応した社内ネットワークのセキュリティ対策を理解する
・インシデント発生時の対応を理解する

コースのねらい

テレワーク特有の情報漏えいが発生する原因と発生した場合の対応、防止するために必要となる対策を理解し、テレワークにおいても情報漏えい発生ゼロを目指す組織体制確立のためのポイントを習得する。

カリキュラム（例）

	基本項目	主な内容（例）
基本要素	■ テレワーク下のセキュリティ概論	・就業場所の違いを認識する ・テレワークの方法による違いを認識する （シンクライアント方式等）
基本要素	■ 社外秘事項の取扱い	・規程整備 （アクセス権者の制限、暗号化等）
基本要素	■ 情報漏えいのリスクと対策	・情報漏えい事例とその対策 ・技術的リスクと人為的リスク ・各種リスクへの対策
基本要素	■ インシデント発生時の初期対応	・平常時の備えと有事における対応
基本要素	演習（例）	・情報セキュリティ理解度チェック ・インシデント発生時の対応実践 ・自社にあったリスク管理表作成
応用・実践要素（例）		・巧妙化するハッキングの手口 ・VPN導入事例 ・利用者認証の導入（多要素認証方式・電子証明書）

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
・テレワークを活用した業務効率化
・テレワーク活用
B　組織マネジメント
・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
D　倫理・セキュリティ
・脅威情報とセキュリティ対策
・情報漏えいの原因と対応・対策

※　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。