生産性向上支援訓練カリキュラム

D. 倫理・セキュリティ	社内の情報セキュリティを維持するために、今こそ知識を深めよう！
セキュリティ対策	**脅威情報とセキュリティ対策**

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。
対　象	（全層向け） ・ITにおけるセキュリティ対策に取り組む方 ・インシデント事例から情報漏えい防止の対策について学びたい方

講義内容		「基本項目」	「主な内容」	訓練時間（H）
	1	脅威情報	（1）情報セキュリティの必要性 ・インシデント事例を紹介し、インシデントが組織の事業継続に与えた影響とその対応事例により、情報セキュリティ対策の必要性を理解する。 ・インシデントの定義と種類について解説する。 （2）日常における脅威とリスク 日常における情報セキュリティ上の脅威とリスクを理解する。 ・サイバー攻撃やマルウエアなどのネットワークの不正利用 マルウェア、標的型攻撃、ランサムウェア　等 ・日常における情報資産の紛失、盗難、管理ミス、誤操作 パソコンや電子記憶媒体などの電子媒体の紛失・盗難、 メール、FAX、郵便物の誤送信・誤送付、 書類などの紛失・盗難　　等 （3）情報漏えいの原因 ・事故、紛失、故意、技術的要因について解説し、情報漏えいの事象を整理して、それぞれの根本原因を考える。	1.5
	2	セキュリティポリシー	（1）情報セキュリティポリシーの必要性 ・情報セキュリティ事故による組織に与える影響を理解し、情報セキュリティ事故を未然に防止するためには、組織として情報セキュリティルールなどのセキュリティポリシーの制定とそれに基づく情報セキュリティ活動の必要性を解説する。 （2）守るべき情報資産の洗い出しと重要度の評価 ・守るべき情報資産の洗い出し方法を学ぶ。 ・情報資産のリスク評価 ・情報資産管理台帳作成 （3）セキュリティ対策規程集の作成 ・情報セキュリティポリシー（社内規程、ルール等）の作成のポイント。 管理体制、組織的対策、人的対策、物理的環境的対策、　技術的対策、セキュリティ事故対応 等 （4）情報セキュリティ活動 ・組織としての情報セキュリティポリシーに基づくPDCA活動による情報セキュリティの維持管理の運用について解説する。	1.5
	3	セキュリティ対策手法	（1）ITセキュリティ対策 ・IT技術の基本的なキーワードを理解し、サイバー攻撃などを防御するための社内ネットワーク対策の基礎的事項を学ぶ。 ID、パスワード管理、　バケットフィルタリング、 アプリケーション・ゲートウェイ、　不正侵入検知 マルウエア対策（標的型攻撃メール対策など）　等	1.5
	演　習		演習1）情報セキュリティの守るべき資産とその重要度評価について学ぶ 演習2）情報漏えい事例より、原因を掘り下げる演習により、発生を防止する方策を学ぶ	1.5
			合計時間	6.0

カリキュラム作成のポイント

情報セキュリティは組織全体での対応が必要で、脆弱個所を作らないためのセキュリティポリシーとその順守が重要であるということを理解する。あわせて、社内ネットワークにも脆弱性を作らないよう技術的対策の基本を理解する。

備考

受講者：筆記用具