生産性向上支援訓練カリキュラム

D. 倫理・セキュリティ	企業の信頼性を維持するために情報セキュリティの知識を深めよう！
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） ・セキュリティ対策に取り組む方 ・インシデント事例や情報漏えい防止策を学びたい方

講義内容	「基本項目」		「主な内容」	訓練時間（H）
	1	脅威情報	（1）社内における情報セキュリティの必要性 ・インシデントが組織の事業継続に与える影響により、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）日常業務に潜む脅威とリスク ・日常業務に潜む脅威とリスクおよび行動基準を学ぶ 情報資産の紛失・盗難、管理ミスや誤操作による情報漏えい、電子化情報の紛失・盗難、メール・FAXの誤送信、郵便物の誤送付 （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）社内における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、およびそれを社内に定着化させるための組織的活動の必要性を解説する。 （2）社内の重要情報資産の洗出し ・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）の作成のポイントを理解する。 管理体制、組織的対策、人的対策、物理的対策、技術的対策 等 （4）情報セキュリティの向上と維持活動 ・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向上・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、サイバー攻撃などの脅威から社内の情報資産を守るための基礎的なツールやしくみを学ぶ。 認証管理、ファイアーウォール、不正侵入検知、Webフィルター、マルウエア対策、EDR、フィッシングメール　等 ・不審メールの扱い方。 （2）最近の情報セキュリティに関する脅威と対策 ・最近のサイバーセキュリティ・インシデントの傾向、主な原因と対策を学ぶ。 （ランサムウェア、サプライチェーン攻撃、内部不正 等）	1.5
	演　習		演習1）社内の守るべき情報資産の洗い出しとその重要度づけについて学ぶ 演習2）情報漏えい事例から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