生産性向上支援訓練カリキュラム（案）概要

機構施設名：千葉職業能力開発促進センター
実施機関名：合同会社瓦林総合研究室

D. 倫理・セキュリティ	脅威情報とセキュリティ対策
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。

講義内容	「基本項目」		「主な内容」	訓練時間（H）
	1	脅威情報	（1）情報セキュリティとは 情報セキュリティの基礎的用語説明、サイバーセキュリティとの違い、情報セキュリティで担保すべき機密性・完全性・可用性など基本的事項について解説する。 【演習】情報セキュリティ意識診断に回答いただき、講師より解説を行う。 （2）脅威の種類と手口 ウイルス、標的型攻撃、フィッシングサイトなどの脅威の種類、Emotetやランサムウェアなどの手口を解説し、代表的な脅威について実際の事例も交えて解説する。またDX推進時のリスク（クラウド、IoT、テレワーク）についても解説する。 （3）セキュリティインシデントによる損害 実際に発生したインシデント事例を損害の内容とともに紹介し、費用・信用失墜・倒産リスクについて解説する。 【演習】自社が守るべき情報資産の列挙とグループ共有。	0.8
	2	セキュリティポリシー	（1）セキュリティポリシーの必要性 企業の情報セキュリティ方針や従業員が守るべき規定類の整備の意義、DXとの両輪推進の必要性について解説する。 （2）セキュリティ対策の考え方 技術的対策、組織的対策、人的対策は継続的に実施する必要があること、侵入後を想定した対策も必要であることを解説する。 （3）セキュリティ体制 一般的なセキュリティ体制とインシデント報告フローを解説する。 【演習】自社規程・体制の整理と強化すべき点の確認。 （4）セキュリティ対策規定集の作成 組織的・人的・情報資産管理・アクセス制御・物理的対策等の各種規定について、具体的サンプルを提示しながら解説する。	0.7
	3	セキュリティ対策手法	（1）リスク分析 リスク分析シートを用いた情報資産のリスク特定と対策検討の流れを解説する。IPAのリスク分析ツールの活用方法もサンプルを示しながら解説する。 （2）技術的対策 ウイルス対策ソフト・セキュリティパッチ・IDS/IPS/UTMなど従来の技術的対策に加え、CASB等DX環境に対応した対策を解説する。 （3）組織的対策 規定整備・運用、セキュリティ監査、予算確保、情報収集方法について解説する。 （4）人的対策 集合研修・eラーニング・トラップメール等の従業員教育を解説する。 【演習】不審メールの判定演習。 （5）物理的対策 サーバー室・執務スペースの施錠・入室制限等の対策について解説する。 （6）DXツール・ケース別対策 IoT・クラウド・テレワーク時のセキュリティ対策と留意点を解説する。	1.5
	演　習		①情報セキュリティ意識診断に回答いただき、講師より解説を行う。 ②自社が守るべき情報資産の列挙とグループ共有を頂く。 ③自社規程・体制の整理と強化すべき点の確認。 ④不審メールの判定演習。	3.0
				計 6.0