カリキュラム

機構施設名： 静岡職業能力開発促進センター
実施機関名： **株式会社Gサポート**

25-22-12-116-028

D. 倫理・セキュリティ	116 情報漏えいの原因と対応・対策
セキュリティ対策	

コースのねらい	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、情報漏えい発生ゼロを実現する組織体制確立のためのポイントを習得する。

	「基本項目」		「主な内容」	訓練時間（H）	日程 月日	日程 時刻
講義内容	1	情報漏えいの原因と損害	（1）情報漏えいのプロセス 身近な情報紛失・漏えい事例を通じて、情報セキュリティの重要性を認識する。 【演習】グループディスカッション 身近な情報ヒヤリハットについての情報交換 （2）情報漏えいの原因 （事故、紛失、故意、技術的他） 情報漏えいに関する調査報告より、情報漏洩の発生のメカニズムとその原因について認識を深める。 【演習】個人ワーク＆ディスカッション 自社職場の情報漏えいリスクの簡易アセスメント （3）情報漏えいによる損害 ①情報漏えい事例をとおして損害賠償等の直接的な損失を認識する ②情報漏えい事例をとおして信用低下等の間接的な損失を認識する ③刑事上、民事上、社内における責任	1.0 0.5 0.5	令和7年 12月9日（火）	9:30～16:30 昼休憩 12:00～13:00
	2	情報漏えい発生時の対応	（1）情報漏えい発生時の対応ステップ ①情報漏えいの認識と報告 ②応急処置と影響の緩和策の実施 ③利害関係者とのコミュニケーション ④原因分析と恒久対策 （2）情報漏えいのタイプ別対応 ①事故による情報漏えい発生時の対応 ②故意の情報漏えい発生時の対応 ③標的型攻撃等の技術的要因による情報漏えい発生時の対応 （3）対応手順 ①もう一つの側面「事業継続」についての対応手順 ②情報漏えいの発生事例より、詳細な対応手順について理解を深める。 【演習】グループワーク 情報漏えいのケース事例に対し、初動対応をシミュレーションする。	0.5 0.5 1.0		
	3	情報漏えいの対策	（1）従業員個人の対策 ①標的型攻撃への対策 ②フィッシングサイトに対する対策 ③安全性を高める電子メールの設定 ④ID・パスワードの設定・管理 ⑤リモートワーク（社外作業）における対策 ⑥情報システムを利用する上での禁止事項 （2）組織としての対策 ①DX化の推進に伴い必要となる情報漏えい対策とは ②人的対策 社員、協力会社への教育、監視 ③組織的対策 セキュリティポリシーの作成・展開、監査等 （3）技術的対策 ①物理的対策 施錠管理、レイアウト対策、情報セキュリティのための5S ②技術的対策 情報端末の管理、ファイアウォール、マルウェア対策、アクセス制御、ログの監視、暗号化等 ③情報リスクアセスメントの進め方 【演習】グループワーク とある職場のケース事例に対し、情報セキュリティリスクアセスメントを体験する。	1.0 0.5 0.5		
			合計時間	6.0		

カリキュラム作成のポイント

本カリキュラムは、企業がDX化を推進するにあたり拡大する情報漏えいリスクを踏まえ、ITにおけるセキュリティ対策に取り組む方が、自社において取るべき具体的な方策を講じるための知識を習得することを目的としております。セキュリティ対策には、情報セキュリティマネジメントの国際規格であるISO27001：2022をベースに、近年に実際に発生した多くの情報漏えい事例を踏まえ、一般従業員や協力業者に対する具体的な指導事項や、ゼロトラストの概念に基づく情報システム上の技術的対策を含め、理解を深めます。