カリキュラム

(D)倫理・セキュリティ	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）
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 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	1.5
	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 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。	1.5
	3	情報漏えいの対策	(1)従業員個人の対策 ①標的型攻撃（危険なメール）への対応 ②フィッシングサイトに対する注意 ③電子メール送信時の対策 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 ①人的対策 社員、協力会社への対応 ②組織的対策 セキュリティポリシーの作成、教育、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 (4)情報セキュリティリスクアセスメントの進め方 ①情報資産の洗い出し ②セキュリティリスクの特定・評価 ③対応計画の策定 【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。	3.0
			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、身近な情報漏洩事例を踏まえ、職員個人レベルで実施できるセキュリティ対策の知識とスキルを習得する内容を重視しています。実際に発生した多くの情報漏えい事例を画像や映像で視覚的に捉え、具体的なセキュリティ対策手法を習得します。

訓練に使用する機器等

●機器・ソフトウェア（受講者用）	●機器・ソフトウェア（講師用・その他）
特になし	講師用ノートパソコンを持参します。
●テキスト	**●その他**
自作テキスト・演習シート等	特になし

利用事業主に用意を求める機器等	備考
プロジェクター スクリーン（壁） ホワイトボード 受講者が見やすい時計	特になし