カリキュラム

機構施設名： 山口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

(D)倫理・セキュリティ セキュリティ対策	情報漏えいの原因と対応・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（事故、紛失、故意、技術的他） ランサムウェア攻撃などの情報漏えいに関する直近の調査報告より、情報漏えい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、社内における責任を理解する。 ④情報漏えいインシデントの与える社内業務への影響を事例から理解する。	2.0
	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誤送信・誤送付による情報漏えい発生時の対応 ②紛失・盗難による情報漏えい発生時の対応 ③マルウェア感染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 もしも自社がサイバー攻撃を受けたら、どう対応するかについて、ケース事例に対し初動対応をシミュレーションする。	2.0
	3	情報漏えいの対策	(1)従業員個人の対策 ①整理・整頓　②情報の持ち運び ③情報の受け渡し　④安全な廃棄 ⑤盗聴・漏れ聞こえ防止　⑥機器・装置の保護 ⑦電磁記憶媒体の保護　⑧複写・配布制限 ⑨電子メール等を経由したサイバー攻撃への対策 ⑩フィッシングサイトに対する対策　⑪セキュリティパッチの適用 ⑫ID・パスワードの設定・管理 ⑬リモートワーク（社外作業）における対策 (2)組織としての対策 ①物理的対策 エリアの管理・鍵管理・入退室管理 ②技術的対策 ⅰ攻撃対象の最小化　ⅱアクセス制御と認証 ⅲ脆弱性対策　ⅳ拠点間ネットワーク対策 ⅴ攻撃メール対策　ⅵ内部対策 (3)技術的対策 ①セキュリティポリシーの必要性 ②管理体制 ③リスクアセスメントの考え方 【演習】グループワーク ケース職場のレイアウト図、ネットワーク図等に対し、情報セキュリティリスクアセスメントを体験する。 ④セキュリティ対策規程の策定方法 ⑤情報セキュリティ内部監査の方法 ⑥協力業者の管理	2.0
			合計時間	6.0

カリキュラム作成のポイント

サイバー攻撃に関する脅威情報を中心に、紛失・盗難、SNSへの掲載、取扱いミス、内部犯行など多くの発生事例を用いてお伝えします。
特に、近年増加している標的型ランサムウェア攻撃などの攻撃パターンを題材に、対処すべき事項を具体的にお伝えします。
オープンコースの訓練であるため、情報システム担当者、管理者、一般社員等のそれぞれの担当業務で役立つスキルをバランスよく配分します。

講師から一言 （リーフレット掲載用 50～70字程度）

情報漏えいのメカニズムを理解し、リスクに備えるための知識を習得します。