カリキュラム

(D)倫理・セキュリティ 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。

講義内容		「基本項目」	「主な内容」	訓練時間（H）
	1	脅威情報	(1)ウイルス・マルウェア ①ウイルス・マルウェアの種類と特徴 ②近年発生しているウイルス・マルウェアの事例 ⅰ)ランサムウェア ⅱ)Emotet　他 (2)標的型攻撃 ①標的型攻撃の特徴と被害事例 ②標的型攻撃のプロセス ③進化する標的型攻撃の手法 (3)フィッシングサイト ①フィッシングサイトによる情報搾取の手口 ②フィッシングサイトの直近での被害事例 (4)その他情報漏えいにつながる脅威 ①SNSに関するインシデント ②営業秘密の漏えい ③内部犯行 (5)情報漏えいによる損害 ①情報漏えいによる信用リスクと経済的損失 ②身近な中小企業で発生した不正アクセスによる情報漏えい事案 ③情報漏えい時の対応手順 (6)インシデント事例と対応 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	2.5
	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 ①企業における情報セキュリティの重要性 ②セキュリティポリシーによる社内情報セキュリティの管理 (2)セキュリティ対策の考え方 ①情報セキュリティの基本的な管理策を把握する。 組織的／人的／物理的／技術的対策 ②情報セキュリティリスクアセスメントの進め方を理解する。 【演習】グループワーク ⅰ)ある職場のケース事例を基に、情報セキュリティ リスクアセスメントを実施する。 ⅱ)上記の結果に基づき、情報セキュリティ管理策を 検討する。 (3)管理体制 情報セキュリティ社内組織体制（役割、責任、権限）について (4)セキュリティ対策規定集の作成 ①セキュリティ対策規定の体系について ②セキュリティ対策規定の作り方 【演習】個人ワーク＆ディスカッション 一般社員向けの情報セキュリティ対策規定（サンプル）をもとに、自社の規定の一部の策定を体験する。	2.5
	3	セキュリティ対策手法	(1)セキュリティパッチの適用 ①セキュリティパッチ適用の必要性について ②個人で使用するパソコンのセキュリティパッチ適用の確認方法、設定方法 ⅰ)WINDOWSのUPDATE ⅱ)ウィルス対策ソフトのUPDATE (2)メール受信時の確認 ①開いてはならないメールの見破り方 ②不審なメールへの対応方法 ③受信メールのセキュリティ対策ツール (3)認証管理 ①推測・割り出されにくいID・パスワードの設定方法 ②ID・パスワードの安全な保管方法 ③多要素認証 (4)情報漏えいに関する管理策 ①パケットフィルタリング ②アプリケーションレベル・ゲートウェイ ③不正侵入検知 ④EDR (5)脆弱性のチェック ①個人で使用するパソコンの脆弱性のチェックの方法 ②社内のデバイスの脆弱性管理	1.0
			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、セキュリティ対策に取り組まれる幅広い業種の方であることを想定し、どの業種でも共通して脅威となり得る身近な情報漏えい事例を踏まえ、企業として、またセキュリティ対策担当者として実施すべき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作成しています。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て習得します。

講師から一言

情報を制する者はビジネスを制する！　社内の情報管理についてすべきことを具体的に把握し、顧客の信頼向上と事業の成長を図りましょう！