

カリキュラム

機構施設名： 大分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	脅威情報とセキュリティ対策
セキュリティ対策	

到達目標	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。
-------------	--

	「基本項目」	「主な内容」	「訓練時間」(H)	
指導内容	1	脅威情報 (1) 情報セキュリティの基本 ① 直近の事故事例から見る情報セキュリティのテーマ ② 身近な中小企業で発生した事故事例の紹介 【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) 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 iii) 圧縮・展開ソフトの脆弱性を悪用したマルウェア ③ 有効な対策手法 (3) 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 ④ 有効な対策手法 (4) フィッシングサイト ① フィッシングサイトによる個人情報等の搾取 ② フィッシングサイトの直近での被害事例 ③ 有効な対策手法 (5) その他情報漏えいにつながる脅威 ① SNSに関するインシデント ② 営業秘密の漏えい ③ 内部犯行 (6) 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 身近な情報セキュリティにおける押さえておきたいことを把握する。 【演習】個人ワーク&ディスカッション これまでの講義内容を振り返り、簡易なチェックリストに基づき自社の情報セキュリティ実施レベルを自己診断し課題を発見する。 (7) インシデント事例と対応 ① インシデント発生時の応急処置 ② 事業継続の観点からの応急処置 【演習】グループワーク とある職場でのサイバー攻撃ケース事例に対し、応急処置実施項目を話し合い、計画する。	2.0	
	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 社内におけるセキュリティポリシーの意義 (2) セキュリティ対策の考え方 情報リスクアセスメントと安全対策の策定 【演習】個人ワーク&ディスカッション ケース事例に対し、簡易な情報リスクアセスメントを体験的に実践し、その結果を情報共有する。 (3) 管理体制 情報セキュリティ社内組織体制について (4) セキュリティ対策規定集の作成 セキュリティ対策規定の体系について 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、自身の対応状況を自己チェックし、ディスカッションすることで身近な注意点についての理解を深める。	2.0
	2	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) ID・パスワードの管理 ① 推測・割り出されにくいID・パスワードの設定方法 ② ID・パスワードの安全な保管方法 (4) データの暗号化 ① データの暗号化の仕組み ② 暗号化ソフトの選び方(信頼性と特徴 比較紹介) (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 自社の情報セキュリティ診断ツール IPAの情報セキュリティ診断ツールの紹介	2.0
		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洩事例を踏まえ、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。

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

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