

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：パナソニックエレクトリックワークス創研株式会社

24-22-12-115-034

D. 倫理・セキュリティ	115 脅威情報とセキュリティ対策
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。
---------	--

		「基本項目」	「主な内容」	訓練時間 (H)	日 程		
					月 日	時刻	
講義内容	1	■ 脅威情報	<p>(1) 情報セキュリティの必要性</p> <ul style="list-style-type: none"> ◎情報セキュリティは何故必要なのか ・インシデント事例 ・インシデントが企業の事業継承に与える影響 <p>(2) 日常における脅威とリスク</p> <ul style="list-style-type: none"> ◎日常における情報セキュリティ上の脅威とリスク ・サイバー攻撃、マルウェア、ランサムウェア 等々 ・情報資産の紛失、盗難、管理ミス、誤操作 ・パソコンや電子媒体の紛失、盗難、メールの誤送信 <p>(3) 情報漏えいの原因【演習あり】</p> <ul style="list-style-type: none"> ◎情報漏えいの根本原因 ・事故、紛失、故意、技術的要因 ・情報漏えいの事象の整理 	1.5	令和6年 8月1日(木) ポリテクセンター 静岡	9:30～16:30 昼休憩 12:00～13:00	
	2	■ セキュリティポリシー	<p>(1) セキュリティポリシーの必要性</p> <ul style="list-style-type: none"> ・情報セキュリティ事故が組織に与える影響 ・事故を未然に防ぐための ①セキュリティルール②セキュリティポリシー <p>(2) 守るべき情報資産の洗い出しと重要度の評価【演習あり】</p> <ul style="list-style-type: none"> ・情報資産の洗い出し方法 ・情報資産のリスク評価 ・情報資産管理台帳作成 <p>(3) セキュリティ対策規定集の作成</p> <ul style="list-style-type: none"> ・セキュリティポリシー作成ポイント ～管理体制、組織的対策、人的対策、物理的環境的対策、技術的対策、事故対応 等 <p>(4) 情報セキュリティ活動</p> <ul style="list-style-type: none"> ・情報セキュリティ維持管理のPDCA 	3.0			
	3	■ セキュリティ対策手法	<p>(1) ITセキュリティ対策</p> <ul style="list-style-type: none"> ◎IT技術の基本的キーワードの理解と社内ネットワーク対策の基礎的事項 ・ID ・パスワード管理 ・バケットフィルタリング ・アプリケーション ・ゲートウェイ ・不正侵入検知 ・マルウェア対策 等 	1.5			
				合計時間	6時間		

カリキュラム作成のポイント
現場の業務に即した実践的な内容でカリキュラムを構成しております。 学習定着率の観点から、講義のみでなく、演習～グループディスカッションをカリキュラムに組み込んでおります。