情報処理安全確保支援士特定講習　講習情報

ＮＥＣマネジメントパートナー株式会社

【フリーシナリオ形式】実践！サイバーセキュリティ演習

実施機関名	ＮＥＣマネジメントパートナー株式会社		
講習名	【フリーシナリオ形式】実践！サイバーセキュリティ演習		
特定講習番号	22-004-027		
講習形態	リモート形式	定員（１回あたり）	20 名
受講日数	2 日間	受講時間	12 時間
受講料	220,000（円/税込み）		

対象分野 <ITSS+（セキュリティ領域）>	主な分野	セキュリティ調査分析・研究開発	関連分野

講習内容	仮想組織で発生したインシデントへの対応ストーリーを通じて、インシデントハンドリングを経験し、インシデント発生時の対応力強化を目指します。【フリーシナリオ形式】はセキュリティ実務経験者を対象にしており、検知・連絡受付後のすべての判断と対応は、CSIRT（受講者グループ）に任されています。ステークホルダー役である講師・チューターと、随時コミュニケーションを取りながらインシデントハンドリングを進めます。 ※シナリオが発散するのを防ぐため、講師・チューターによる誘導があります。 ※特定講習番号22-004-028【ステップバイステップ形式】実践！サイバーセキュリティ演習 と同一シナリオです。
具体的な到達目標	・インシデントハンドリングの手法を学び、自組織がサイバー攻撃を受けた際に、適切に行動できる。 ・CSIRTの必要性や業務概要、要求されるスキル等を説明できる。 ・最新のサイバー攻撃の動向や事例について説明できる。
修得できるスキル	・インシデント発生時の対応（インシデントハンドリング）スキル ・インシデントの内容の整理、原因分析をおこない、再発防止を提案するスキル
講習の理解・習得のために推奨される実務経験	・Windows、Linuxのシステム管理経験があることが望ましい。 ・Windows操作、Linuxのコマンドライン操作ができることが望ましい。 ・セキュリティに関する実務経験があることが望ましい。
講習の理解・習得のために推奨される知識・技術	セキュリティに関する基礎知識を有することが望ましい。 ・代表的な攻撃手法　（事前調査、権限取得、不正実行、事後処理） ・セキュリティ対策技術の機能、特徴　（FW、IDS/IPS、マルウェア対策など） ・暗号技術の基礎知識　（暗号方式、ハッシュ、ディジタル署名、PKIなど）
技術・知識の到達度の把握・測定方法	・実習操作状況把握のため、画面のモニタリングやヒアリングをおこなう。 ・グループワークの際は各グループを巡回（ヒアリングを含む）して状況を把握する。 ・グループワーク後の発表内容、質疑応答内容の妥当性を確認する
修了認定の判断基準	・出席率３／４以上、かつ以下を総合的に審査し決定する。 ①グループ作業およびディスカッションへの参加度合い ②実習課題においておこなったセキュリティインシデントへの対応が合理的な内容となっているか ③実習中の講師による進捗、取組み状況、課題、方針などの確認に対する回答が妥当性を有しているか
修了認定基準に満たない受講者への措置	修了と認められない場合には、受講者へ通知の上、修了の認定をおこなわない。
受講者に対するサポート体制	・常時チャット、音声による質問を受付ける。 ・講師が各グループを巡回して状況を把握し、必要に応じて追加説明・アドバイスをおこなう。 ・発表内容や質疑応答内容において理解度に不安のある場合には、詳細な解説や個別に補足説明をおこなう。
講習実施施設所在地	東京都港区芝浦
ホームページ	https://www.neclearning.jp/courseoutline/courseId/SN475/