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

インシデントレスポンス基礎　－マルウェア解析編－

実施機関名	ＮＥＣマネジメントパートナー株式会社		
講習名	インシデントレスポンス基礎　－マルウェア解析編－		
特定講習番号	22-004-026		
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	13 時間
受講料	176,000（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	マルウェア感染が原因でインシデントが発生した際のマルウェアの解析方法、影響範囲の分析や対応の検討方法を修得します。主にマルウェアの表層解析や動的解析について、講義と実習を通して修得します。
具体的な到達目標	以下の能力を身に付け、マルウェア感染が原因でインシデントが発生した際のマルウェアの解析方法、影響範囲の分析や対応を検討できるようになる。 ・マルウェア解析の「考え方」と「手法」を説明できる ・インシデント対応の現場において、マルウェアを解析し、解析結果を第三者に説明することができる
修得できるスキル	・マルウェアの表層解析、動的解析スキル
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。
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。 ・実習の際は各受講者へのヒアリング等により状況を把握する。 ・実習後の質疑応答内容により理解度を確認する。
修了認定の判断基準	以下を総合的に審査し決定する。 ・出席率３／４以上 ・内容理解（質疑応答状況、および講師からのヒアリングへの応答が妥当性を有しているか等） ・実習状況（所定項目に関する進捗・到達度、および講師による取組み状況の確認などに対する回答の妥当性）
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。 ・実習時にはヒアリング等により状況を把握し、必要に応じて追加説明・アドバイスをおこなう。 ・質疑応答内容において理解度に不安のある場合には、詳細な解説や個別の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/SN412