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

ＣＳＩＲＴ強化トレーニング　テクニカル編（ＣＴＦ形式）

実施機関名	ＮＥＣマネジメントパートナー株式会社		
講習名	ＣＳＩＲＴ強化トレーニング　テクニカル編（ＣＴＦ形式）		
特定講習番号	21-004-010		
講習形態	リモート形式	定員（１回あたり）	20 名
受講日数	1 日間	受講時間	6.5 時間
受講料	88,000（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	必要となる予備知識（文字列、ディスクフォレンジック、ネットワーク、実行ファイル、メモリ等）に関する事前学習を経た上で、オンライン上でCTF（Capture the Flag)形式の実践型セキュリティ技術演習に取り組みます。 複数のステージに設定された技術的な課題をクリアしていくことで、基本的なインシデント解析技術と解析ノウハウを学びます。
具体的な到達目標	・インシデントレスポンス時にアーティファクトの詳細な調査および解析支援をおこなうことができる ①IOC情報の取得　②マルウェアの動作検証　③エビデンスデータの取得 ④原因の推定　⑤発生日時の特定　など ・フォレンジック調査で使用するソフトウェアツールを使用することができる ①ログ解析　②メモリ解析　③ディスク解析　④ネットワークキャプチャ解析　⑤マルウェア動作検証　など
修得できるスキル	・ログ解析スキル ・メモリ解析スキル ・ディスク解析スキル ・ネットワークキャプチャ解析スキル ・マルウェア動作検証スキル
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 ・Windowsアプリケーションの開発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	以下の知識を有することが望ましい。 ・Windowsの知識（ファイルシステム、レジストリ、イベントログ、API） ・TCP/IPの知識　・正規表現記法の知識 ・メモリ解析の知識　・ハッシュ関数の知識
技術・知識の到達度の把握・測定方法	・出席率 ・実機による実習状況 ・実習課題の回答内容 ・講師からの質疑応答への対応状況
修了認定の判断基準	出席率３／４以上　かつ、以下①～③を総合的に審査し決定する。 ①グループ作業への参加度合い（発言状況、関与度） ②解答率50%以上（誤解答についてもそこに至るまでの作業内容が妥当で合理性を有していれば可とする） 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、修了の認定を行わない。
受講者に対するサポート体制	・常時チャットでの質問を受け付ける ・実習の際は、講師、講師補助者が各グループを頻繁に回り進捗確認を行う ・実習課題の各段階において、合格に満たない懸念のある受講者、グループに対しては個別に理解度を確認するヒアリングを実施し、補足説明を行う
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/SN376/