# 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　マルウェア感染対応編

| | | | |
|---|---|---|---|
| 実施機関名 | ＮＥＣマネジメントパートナー株式会社 | | |
| 講習名 | ＣＳＩＲＴ強化トレーニング　マルウェア感染対応編 | | |
| 特定講習番号 | 21-004-009 | | |
| 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<br><ITSS+（セキュリティ領域）> | 主な分野 | セキュリティ監視・運用 | 関連分野 | セキュリティ調査分析・ 研究開発 |
| 講習内容 | インシデント対応の考え方および流れ、インシデント検知後の事実確認・状況把握フェーズの考え方、留意点、マルウェア解析、再発防止策の考え方に関する事前学習を経た上で、オンライン上で、グループワークを実施します。<br>グループワークでは、仮想顧客からの依頼により、顧客組織内で発生したマルウェア感染事案への対応おこないます。マルウェア感染ストーリーを通じて、主に表層解析、動的解析等の解析技術を学ぶと同時に、ヒアリングなどサービス対象者とのコミュニケーションを通じて、インシデント全体像の組み立て、原因追究、対策立案を体験し、セキュリティ対応力の強化を目指します。 | | |
| 具体的な到達目標 | ・ インシデント発生時の事実確認、状況把握のために、関係者に対するヒアリング項目を挙げることができ、適切な初動提案、調査シナリオが作成できる<br>・原因究明、フォレンジックのために必要な情報を選定できる<br>・ 解析ツールを駆使し基本的なマルウェア解析ができる<br>・セキュリティインシデントの恒久的対策立案の考え方が説明でき、サービス・製品の導入、運用改善などの対策立案の支援ができる | | |
| 修得できるスキル | ・インシデント対応スキル（主にCSIRTにおけるハンドラー、インベスティゲータ、フォレンジック担当に該当するスキル）<br>・関係者に対するヒアリングスキル<br>・ログ解析スキル、マルウェア解析スキル | | |
| 講習の理解・習得のために推奨される実務経験 | ・組織における情報システム、ネットワーク運用管理経験があることが望ましい<br>・Windowsアプリケーション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 | Windows OSに関する知識、および以下を含む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。<br>・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）<br>・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）<br>・セキュリティマネジメントの概要 | | |
| 技術・知識の到達度の把握・測定方法 | ・出席率<br>・実機による実習状況<br>・実習課題の回答内容<br>・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。<br>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（発言状況、関与度）<br>②各実習課題への回答が正しい解釈で合理的な内容となっているか<br>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<br>・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<br>・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/SN375/ | | |