情報処理安全確保支援士特定講習　講習情報

株式会社ラック

デジタル・フォレンジックコース

実施機関名	株式会社ラック		
講習名	デジタル・フォレンジックコース		
特定講習番号	21-005-019		
講習形態	リモート形式又は集合形式	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	330,000（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	セキュリティ統括 デジタルプロダクト運用 脆弱性診断・ペネトレーションテスト セキュリティ監視・運用

講習内容	侵害が疑われる状況において、デジタル・フォレンジック技術を利用した初動対応を行うことにより、被害拡大の防止、影響範囲の確認、情報漏洩を判断する基礎的な手法について演習形式で学びます。 ＜カリキュラム概要＞ プロキシログ解析、マルウェアの手動探索、プログラム実行痕跡調査、ファイルシステムのログ調査、削除データの調査
具体的な到達目標	・プロキシログから、マルウェアによる不正通信を発見し、影響範囲の確認などができるようになる ・Windowsのシステム内に設置されているマルウェアを発見し、被害状況、影響範囲の確認ができるようになる ・削除ファイルの復元方法を学び、インシデント対応の幅を広げられるようになる
修得できるスキル	デジタルフォレンジックスキル インシデント対応（初動から完了まで）スキル
講習の理解・習得のために推奨される実務経験	IT技術全般（インフラ系・開発系）、情報システム・セキュリティ推進業務、SOC（セキュリティ運用）要員業務、その他インシデント対応に関連した業務
講習の理解・習得のために推奨される知識・技術	マルウェアの基本的な動作に関する知識 標的型攻撃で利用される一般的な侵害手口に関する知識（Persistence, Lateral Movement, Exfiltration）
技術・知識の到達度の把握・測定方法	・実機による実習状況 ・総合演習の実行状況及び結果 ＊上記を総合的に講師が判断
修了認定の判断基準	100%の出席率に加え、講師が総合的に評価を行った上で修了判定を行います。 判断基準については、実機利用の演習等は「一人で完了できている」～「多少のサポートで完了」～「研修時間内にまったく出来ない」が目安。また、実機演習も含め研修全体を通して講師からの質問への対応や、質問の状況など講師と補助講師が随時チェックして最終的に相対評価とします。
修了認定基準に満たない受講者への措置	新規に申込してもらい再度受講してもらう措置とします。費用は自己負担となります。
受講者に対するサポート体制	講義内各段階において懸念のある受講者に対し、講師と補助講師で適時認識合わせを実施します。その上で補助講師が個別にサポートを手厚くしていきます。また、研修終了後の学習方法などもアドバイスしていきます。
講習実施施設所在地	東京都千代田区平河町2-16-1　平河町森タワー　株式会社ラック本社
ホームページ	https://www.lac.co.jp/service/education/digitalforensic.html