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

マルウェア解析ハンズオン専門コース

実施機関名	株式会社ラック		
講習名	マルウェア解析ハンズオン専門コース		
特定講習番号	21-005-016		
講習形態	集合形式	定員（１回あたり）	20 名
受講日数	3 日間	受講時間	19.5 時間
受講料	495,000（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 セキュリティ監視・運用 脆弱性診断・ペネトレーションテスト

講習内容	マルウェアに施された耐解析機能への対応手法や隠された機能を特定する手法などを習得します。 最終日には、入門・専門を通じて習得した各種技術を用いて、マルウェア解析の総合演習を行います。 （カリキュラム概要）耐解析機能と概要、アセンブラ、デバッガとその使い方、耐解析機能の回避、マニュアルアンパックと必要な知識、マニュアルアンパック実践、静的解析、簡易静的解析、IDA入門、IDA実践、演習と時間短縮テクニック、総合演習
具体的な到達目標	耐解析機能を持つマルウェアの解析ができるようになる マルウェアの機能を論理的に理解できるようになる 膨大なアセンブラ命令から必要な情報を抽出し、見るべきポイントを抑える
修得できるスキル	マルウェアに施された耐解析機能への対応手法スキル 隠された機能を特定する手法スキル 各種技術を用いたマルウェア解析の総合手法スキル
講習の理解・習得のために推奨される実務経験	IT技術者（インフラ系・開発系）、SOC（セキュリティ運用）要員、CSIRT要員（技術系）、インシデント調査技術、マルウェア解析業務等々、セキュリティ調査関連の専門業務経験全般
講習の理解・習得のために推奨される知識・技術	・マルウェアの簡易解析を経験済み（ 表層解析が可能、デバッガ以外のツールを使った動的解析が可能） ・マルウェア解析のためのアセンブラの知識をお持ちの方 （x86アセンブラについて大まかに理解していれば、必須ではありません）
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、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/malware_assembly.html