情報処理安全確保支援士特定講習　講習情報

株式会社ワイ・イー・シー

Ｗｉｎｄｏｗｓ　Ｆｏｒｅｎｓｉｃｓ

実施機関名	株式会社ワイ・イー・シー		
講習名	Ｗｉｎｄｏｗｓ　Ｆｏｒｅｎｓｉｃｓ		
特定講習番号	21-002-004		
講習形態	集合形式	定員（１回あたり）	15 名
受講日数	3 日間	受講時間	18 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	Windowsは現在のIT環境に対応するための様々な機能追加が行われており、Windows端末のデータ保全・解析するには今までとは異なるアプローチが必要となります。本講習では、Windowsに対する以下の点を中心に実演・演習を交えて解説します。①Windows端末を対象とした初動対応として、Windowsの機能や特徴をはじめとしたFast Forensics（一般的なアーティファクト解析）の解説　②Windows端末の解析手法について各種アーティファクトの解析プロセスを中心にWindowsに実装されたフォレンジックに関わる機能・特徴等の解説を行います。
具体的な到達目標	以下の能力を身に着け、インシデントに関係したWindows端末の適切な証拠保全から一般的なフォレンジック調査手法をできるようになる。 ①Windowsが調査対象となるインシデントにおいて初動調査を実施できるようになる ②Windowsが対象となるインシデントの原因や影響範囲の実態把握が出来るようになる
修得できるスキル	・Windows端末の初動調査 （基礎的な解析をするスキル（Webアクセス履歴、ファイル操作、プログラム実行履歴等）） ・Windows端末の詳細調査 （各種証跡の構造を理解し解析するスキル（Webアクセス履歴の構造解析、レジストリ解析、ジャンプリストやクイックアクセス等のユーザー挙動の解析等））
講習の理解・習得のために推奨される実務経験	インシデントレスポンスの実務経験とコマンドラインを利用した操作ができることが望ましい CSIRT要員（技術系）、SOC要員（運用、監視）
講習の理解・習得のために推奨される知識・技術	デジタルフォレンジックにおける基本的な保全と解析の知識を有することが望ましい
技術・知識の到達度の把握・測定方法	・出席率 ・演習課題の解答内容 ・実機による実習状況
修了認定の判断基準	・出席率：全体の3/4以上 ・演習課題への解答の正誤、解答を導き出したプロセスの習得状況を総合的に判断して決定する。
修了認定基準に満たない受講者への措置	受講生の習得状況が修了認定基準に著しく満たないと講師が判断した場合は、講師又は補助講師が個別に補講や助言（計1時間以内）を実施する。 出席率が満たない場合：補講の実施で対応する。 補講実施後も修了と認められない場合には、受講者へ通知の上、修了認定を行わない。
受講者に対するサポート体制	各演習課題の解答や解答プロセスなどの状況から修了認定を与えることが難しいと懸念さえる受講生には、講師または講師補助が個別に不明点などヒアリングの上、補足説明を加えたレクチャーやアドバイスを実施する。
講習実施施設所在地	〒100-0006東京都千代田区有楽町 〒530-0017大阪府大阪市北区角田町
ホームページ	https://www.kk-yec.co.jp/products/forensic/training.html