# 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

## Ｍａｃ　Ｆｏｒｅｎｓｉｃｓ

| | | | |
|---|---|---|---|
| 実施機関名 | 株式会社ワイ・イー・シー | | |
| 講習名 | Ｍａｃ　Ｆｏｒｅｎｓｉｃｓ | | |
| 特定講習番号 | 21-002-005 | | |
| 講習形態 | 集合形式 | 定員（１回あたり） | 12 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<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 | 本講習では、macOS端末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。<br>①macOS端末を対象とした証拠保全時の留意点や各種手法<br>②macOS端末のシステム設定やログ等の解析、固有のアーティファクトやユーザーの操作履歴などの解析 |
| 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Mac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。<br>・Macに搭載されているセキュリティ機能やインタフェース等に応じた適切な証拠保全手法を選択・実践できる<br>・Mac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 | ・Mac端末の証拠保全<br>（データ保全手法、データ保全における注意点、ディスクイメージのマウント方法、ファイルシステムの理解）<br>・macOSの解析<br>（システムログやUnifiedLoggingの解析、システム設定（バージョン情報、ネットワーク設定、マルウェアが利用する自動実行設定など）の解析、Mac固有のアーティファクトやユーザーの操作履歴などの解析） |
| 講習の理解・習得のために推奨される実務経験 | デジタルフォレンジックの実務経験（OS問わず）、WindowsやLinux等でのコマンドラインによる操作が出来ることが望ましい<br><br>CSIRT要員（技術系） |
| 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関する基礎の知識・スキル、ターミナルによる操作に抵抗がないことが望ましい |
| 技術・知識の到達度の把握・測定方法 | ・出席率<br>・演習課題の解答内容<br>・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<br>・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。<br>出席率が満たない場合：補講の実施で対応する。<br>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<br>〒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 |