情報処理安全確保支援士特定講習　講習情報

株式会社インターネットイニシアティブ

インシデントハンドリング実践コース

実施機関名	株式会社インターネットイニシアティブ		
講習名	インシデントハンドリング実践コース		
特定講習番号	21-007-022		
講習形態	集合形式	定員（１回あたり）	20 名
受講日数	1 日間	受講時間	7 時間
受講料	80,000円		

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	セキュリティ統括 セキュリティ監視・運用 セキュリティ調査分析・研究開発

講習内容	SOCサービスが検知したインシデント報告書をもとに、セキュリティ機器やサーバから必要なログを採取し、発生しているインシデントの被害状況を把握し、初動対応から封じ込め、根絶を実施いたします。また、発生したインシデントに対する再発防止策をグループで検討・発表することでインシデントハンドリングに関する一連の流れを習得していただきます。
具体的な到達目標	以下のスキルを習得することでインシデントの連絡を受けた際にインシデントハンドリング一連の流れを行えるようになる ①必要なログを収集・解析し被害範囲の特定を行うことができる ②発生したインシデントに対し初動対応を行うことができる ③経営的な視点も考慮した再発防止策の検討を行うことができる
修得できるスキル	・ログの収集および解析（ファイアウォールログ、IDS/IPSログ、プロキシログ、Mailログ、イベントログ等） ・初動対応の検討（ファイアウォール、IDS/IPS、プロキシでの通信遮断） ・インシデントによるビジネスへの影響の考え方 ・再発防止策の検討
講習の理解・習得のために推奨される実務経験	・情報システム部（ネットワーク運用、システム管理） ・CSIRT（PoC、インシデント対応）
講習の理解・習得のために推奨される知識・技術	・ネットワークに関する基礎知識 ・RDPによるwindowsへの接続および操作 ・SSHによる接続とLinuxターミナル操作ができることが望ましい
技術・知識の到達度の把握・測定方法	・講習全体の出席率 ・実機による実習の操作状況、および、演習の発表内容 ・終了後のアンケート内容
修了認定の判断基準	以下3点を満たしていること ①出席率80%以上 ②初動から封じ込めまで実習を行い、技術的、人的、組織的観点で再発防止策を検討している ③アンケートを記入し提出している
修了認定基準に満たない受講者への措置	インシデントハンドリングに関する流れ再確認させ、追補資料を提出させる。
受講者に対するサポート体制	講師および、チュータにより受講者の実習進捗状況を適宜確認する。 実習の進捗が遅れている受講者に対して、講師およびチュータからコマンドの説明など支援を行う。
講習実施施設所在地	東京都千代田区富士見2-10-2　飯田橋グラン・ブルーム
ホームページ	https://www.iij.ad.jp/svcsol/security-education/