情報処理安全確保支援士特定講習一覧

令和３年４月１日現在

No.	実施機関名	講習名	講習内容	主な分野※	特定講習番号
1	大日本印刷株式会社	サイバー・インシデントレスポンス・マネジメントコース 基礎演習	実務者向けコース全ての基礎となるインシデントレスポンスのスキルを身につけるためのコース。一般企業のWindows系仮想環境にサイバー攻撃を受けてチームで対処するハンズオン演習になります。	セキュリティ監視・運用	21-001-001
2	大日本印刷株式会社	サイバー・インシデントレスポンス・マネジメントコース 実践演習	企業のネットワーク構成を模した環境の中で、実際にあったインシデントに基づく攻撃シナリオに対処し、実践的なスキルを身につけたい方に最適なコースになります。	セキュリティ監視・運用	21-001-002
3	大日本印刷株式会社	サイバー・インシデントレスポンス・マネジメントコース 実践演習Ⅲ	企業のネットワーク構成を模した環境の中で、実際にあったインシデントに基づく攻撃シナリオに対処し、実践的なスキルを身につけたい方に最適なコースになります。	セキュリティ監視・運用	21-001-003
4	株式会社ワイ・イー・シー	Ｗｉｎｄｏｗｓ１０　Ｆｏｒｅｎｓｉｃｓ	Windows 10に対する一般的な初動対応・データ保全及び各種アーティファクト等の構造・解析手法等を中心に講習を行います。	セキュリティ監視・運用	21-002-004
5	株式会社ワイ・イー・シー	Ｍａｃ　Ｆｏｒｅｎｓｉｃｓ	macOS端末を対象とした証拠保全時の留意点や各種手法、macOS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一般的な解析手法を中心に講習を行います。	セキュリティ監視・運用	21-002-005
6	株式会社ワイ・イー・シー	Ｆｉｌｅ　Ｓｙｓｔｅｍ　Ｆｏｒｅｎｓｉｃｓ	一般的なOSに使用されるファイルシステム構造（NTFS, FAT, exFAT,EXT2/3/4のファイルシステム構造について）、File Systemごとの特徴とフォレンジック調査における重要性について講習を行う。	セキュリティ調査分析・研究開発	21-002-006
7	トレンドマイクロ株式会社	Ａｄｖａｎｃｅｄ　Ｔｈｒｅａｔ　Ｄｅｆｅｎｃｅ　Ｔｒａｉｎｉｎｇ　５Ｄａｙｓ	高度化する標的型攻撃に対し、攻撃のステージにおけるその技術と手法から攻撃者の意図を理解し、侵害されたネットワークの調査・解析を学習するSOC/CSIRTの技術者の為のハンズオントレーニングです。	セキュリティ監視・運用	21-003-007
8	トレンドマイクロ株式会社	Ａｄｖａｎｃｅｄ　Ｔｈｒｅａｔ　Ｄｅｆｅｎｃｅ　Ｔｒａｉｎｉｎｇ　４Ｄａｙｓ	高度化する標的型攻撃に対し、攻撃のステージにおけるその技術と手法から攻撃者の意図を理解し、侵害されたネットワークの調査・解析を学習するSOC/CSIRTの技術者の為のハンズオントレーニングです。	セキュリティ監視・運用	21-003-008
9	ＮＥＣマネジメントパートナー株式会社	ＣＳＩＲＴ強化トレーニング　マルウェア感染対応編	仮想組織で発生したマルウェア感染事案への対応ストーリーを通じて、マルウェア解析、インシデント全体像の組み立て、原因追究、対策立案を体験し、セキュリティ対応力の強化を目指します。	セキュリティ監視・運用	21-004-009
10	ＮＥＣマネジメントパートナー株式会社	ＣＳＩＲＴ強化トレーニング　テクニカル編（ＣＴＦ形式）	CTF（Capture the Flag)形式を採用した、実践型セキュリティ技術演習です。複数のステージに設定された技術的な課題をクリアしていくことで、基本的なインシデント解析技術とノウハウを学びます。	セキュリティ調査分析・研究開発	21-004-010
11	ＮＥＣマネジメントパートナー株式会社	サイバー防御トレーニング ―Ｂｌｕｅ　Ｔｅａｍ　Ｔｒａｉｎｉｎｇ―	レッドチーム（攻撃を行う側）である講師が仕掛ける現実に近い様々なサイバー攻撃に対して、ブルーチーム（防御する側）である受講者がセキュリティ対策を講じてシステムを堅牢化します。	セキュリティ監視・運用	21-004-011
12	株式会社ラック	Ｗｅｂアプリケーション脆弱性診断ハンズオンコース	Webアプリケーション診断を実施するにあたり必要となる知識やスキルを学びます。単なる知識の習得だけでなく、実機演習を通して各脆弱性の診断手法を学習します。	脆弱性診断・ペネトレーションテスト	21-005-012
13	株式会社ラック	プラットフォーム脆弱性診断ハンズオンコース	プラットフォーム診断を実施するにあたり必要となる知識やスキルを学びます。単なる知識の習得だけでなく、実機演習を通してプラットフォームにおける各脆弱性の診断手法を学習します。	脆弱性診断・ペネトレーションテスト	21-005-013
14	株式会社ラック	マルウェア解析ハンズオン自動化コース	マルウェア自動解析機能実装のサンドボックスを活用し不審なファイルやマルウェアの解析手法を学習します。	セキュリティ調査分析・研究開発	21-005-014
15	株式会社ラック	マルウェア解析ハンズオン入門コース	ウイルス対策ソフトやフォレンジック分析によって発見されたマルウェアの解析手法を学習します。＊コース名称「入門」とありますが、マルウェア解析技術としては入門で、ITSSでのレベル４に該当します。	セキュリティ調査分析・研究開発	21-005-015
16	株式会社ラック	マルウェア解析ハンズオン専門コース	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。	セキュリティ調査分析・研究開発	21-005-016
17	株式会社ラック	セキュリティオペレーション実践コース 初級編	HTTP通信を題材に攻撃の痕跡の発見と分析ポイント学習。Webサーバが攻撃通信によって受けた影響の発見と判断の実習します。 ＊「初級編」とはSOCアナリストとしての初級。ITSSではレベル４に該当します。	セキュリティ監視・運用	21-005-017
18	株式会社ラック	セキュリティオペレーション実践コース 中級編	ラック社SOCアナリスト養成のカリキュラムを凝縮。様々なログや通信から攻撃の痕跡を検出・判断するポイントを学習し、最終的には攻撃の検証から検出、成否判断までを自ら試行実習する。	セキュリティ監視・運用	21-005-018
19	株式会社ラック	デジタル・フォレンジックコース	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い、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。	セキュリティ調査分析・研究開発	21-005-019
20	株式会社アイ・ラーニング	日本ＩＢＭインシデント・レスポンス研修 ―プロが教えるＣＳＩＲＴ要員育成コース―	インシデント発生時に、セキュリティ専門家によるERSの支援を最大限に活用することを含め、迅速な初動対応、被害の最小化、再発防止策立案ができる人財を養成することを目的としています。	セキュリティ統括	21-006-020
21	株式会社アイ・ラーニング	情報セキュリティマネジメント構築	部門の情報セキュリティマネジメントを構築するための基準や、効果的なリスクアプローチと形骸化を防ぐ構築をケーススタディを通じて学習します。	セキュリティ統括	21-006-021
22	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	SOCサービスから受領したインシデントレポートを元に、初動対応から封じ込め、根絶の実習、および再発防止策の検討までの一連のインシデントハンドリングを実践するコースです。	セキュリティ監視・運用	21-007-022
23	国立研究開発法人情報通信研究機構	実践サイバー演習 ～大規模演習環境を活用してリアリティを高めたインシデントハンドリング演習～(CIRP: Cyber Incident Response Practice for RISS)	仮想組織のネットワークをシミュレートした演習環境を舞台に、実際に起こり得る攻撃シナリオで、実機を用いてインシデントハンドリングのプロシージャーを1から10まで学ぶことができる。	デジタルプロダクト運用	21-008-023

※主な分野は、ＩＴＳＳ＋（セキュリティ領域）のうち、当該講習が対象とする主な分野を掲載しています。ＩＴＳＳ＋（セキュリティ領域）は、企業のセキュリティ対策に必要となるセキュリティ関連業務のまとまりを17 分野に整理したものです。詳細は、独立行政法人情報処理推進機構のＨＰ（https://www.ipa.go.jp/jinzai/itss/itssplus.html）を参照下さい。