情報処理安全確保支援士特定講習一覧

令和5年4月1日

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	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１日版	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	22-001-024
5	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２日版	本物のサイバー攻撃を受けて調査分析・封じ込め・再発防止までの対応を、実機を用いた環境で体験することで、インシデント対応対処に必要な基礎スキルをフェースごとに実践的に学ぶコースです。	セキュリティ監視・運用	23-001-036
6	株式会社ワイ・イー・シー	Ｗｉｎｄｏｗｓ　Ｆｏｒｅｎｓｉｃｓ	Windows端末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
7	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
8	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
9	トレンドマイクロ株式会社	標的型攻撃対応・防御トレーニング５日版	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・解析を学習するトレーニングです。	セキュリティ監視・運用	21-003-007
10	トレンドマイクロ株式会社	標的型攻撃対応・防御トレーニング３日版	ネットワークセキュリティの脅威や標的型攻撃の攻撃手法、侵害されたネットワークの調査・解析手法など、SOCやCSIRT対応で必要とされる技術を集中的に学習するトレーニングです。	セキュリティ監視・運用	22-003-025
11	トレンドマイクロ株式会社	インシデント調査トレーニング　クライアント端末版	Windowsの機能や各種ツール、EDRを活用した、インシデント発生源および影響範囲等の調査とその対処方法を学習するハンズオントレーニングです。	セキュリティ監視・運用	23-003-037
12	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
13	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
14	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
15	ＮＥＣマネジメントパートナー株式会社	インシデントレスポンス基礎　－マルウェア解析編－	マルウェア感染が原因でインシデントが発生した際のマルウェアの解析方法、影響範囲の分析や対応の検討方法を修得します。主にマルウェアの表層解析や動的解析について、講義と実習を通して修得します。	セキュリティ調査分析・研究開発	22-004-026
16	ＮＥＣマネジメントパートナー株式会社	【フリーシナリオ形式】 実践！サイバーセキュリティ演習	仮想組織で発生したインシデントへの対応を通じて、インシデント発生時の対応力強化を目指します。一連のインシデントハンドリングを受講者グループの判断で進めた後、最後に全貌の解説をおこないます。	セキュリティ調査分析・研究開発	22-004-027
17	ＮＥＣマネジメントパートナー株式会社	【ステップバイステップ形式】 実践！サイバーセキュリティ演習	仮想組織で発生したインシデントへの対応ストーリーを通じて、インシデントハンドリングを経験し、インシデント発生時の対応力強化を目指します。ステップごとにグループ発表と解説をおこないます。	セキュリティ調査分析・研究開発	22-004-028
18	ＮＥＣマネジメントパートナー株式会社	サイバー攻撃トレーニング －Ｒｅｄ　Ｔｅａｍ　Ｔｒａｉｎｉｎｇ－	レッドチーム（攻撃を行う側）として演習用システムにサイバー攻撃をおこなうことで、ペネトレーションテストに必要な技術を養います。また、攻撃者の着目点や攻撃手法を修得し、防御策の策定に活かします。	脆弱性診断・ペネトレーションテスト	22-004-029
19	ＮＥＣマネジメントパートナー株式会社	インシデントレスポンス基礎 －フォレンジック解析編－	セキュリティインシデントが発生した際、デジタル機器の証拠保全や証拠の解析をおこなうために必要となる、フォレンジック解析スキル（主にWindowsを対象とした調査手法・技術）を修得します。	セキュリティ調査分析・研究開発	23-004-038
20	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
21	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
22	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
23	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
24	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
25	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

No.	実施機関名	講習名	講習内容	主な分野※	特定講習番号
26	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
27	株式会社ラック	情報セキュリティ事故対応１日コース 机上演習編	情報セキュリティ事故が発生した際の対応方法、インシデントレスポンスを学びます。インシデントレスポンスの一連の流れを学習した後、ストーリー仕立てのシナリオに沿って机上演習を体験していただきます。	セキュリティ調査分析・研究開発	22-005-030
28	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	組織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、情報資産の調査、リスクアセスメントの概要、部門ルールの策定について、ケーススタディを通じて1日で学習します。	セキュリティ統括	21-006-021
29	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
30	株式会社インターネットイニシアティブ	攻撃技術理解・防御 APT対策基礎コース	高度標的型攻撃の一連の流れ（侵入、権限昇格、ファイル設置、横展開、ファイル転送、ログ削除）を体験し、どのような対策や検知方法が有効であるかをグループで討議し、その結果を発表します。	セキュリティ監視・運用	23-007-039
31	株式会社インターネットイニシアティブ	セキュリティ対策基礎 実践コース	サーバに備わっている機能等を活用し、パスワード制限やセキュアなサーバ設定、及びインシデント発生時の情報収集方法等の実習を行い、セキュリティ対策への課題を検討し、検討した内容を発表します。	セキュリティ監視・運用	23-007-040
32	国立研究開発法人情報通信研究機構（NICT）	実践サイバー演習 RPCI（リプシィ）	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
33	株式会社バルクホールディングス	Ｃｙｂｅｒ－Ｔｈｒｅａｔｓ ａｎｄ Ｄｅｆｅｎｓｅ Ｅｓｓｅｎｔｉａｌｓ	実際にAPT攻撃を受けて検知する業務を実体験するハンズオンを中心とした実践的なトレーニング。仮想化技術によって安全に分離された環境下でリアルタイムに実際のAPT攻撃を受け、対応を行います。	セキュリティ監視・運用	22-009-031
34	株式会社バルクホールディングス	Ｆｏｒｅｎｓｉｃｓ Ｔｒａｉｎｉｎｇ	コンピュータやネットワークのフォレンジックスキルを実機を使って習得し、デジタルエビデンスについて学習します。	セキュリティ調査分析・研究開発	22-009-032
35	NRIセキュアテクノロジーズ株式会社	セキュアＥｇｇｓ応用編（インシデント対応）	インシデントとその対応をステップに分けて学んだ後、実機を使った演習とグループワークを実施し、インシデント発生への準備と対応プロセスを学びます。	セキュリティ監視・運用	22-010-033
36	NRIセキュアテクノロジーズ株式会社	セキュアＥｇｇｓ応用編（フォレンジック）	情報セキュリティインシデント対応時の調査(フォレンジック)をハンズオンで体験し、フォレンジックの基礎と簡単な調査手法を学びます。	セキュリティ監視・運用	22-010-034
37	NRIセキュアテクノロジーズ株式会社	セキュアＥｇｇｓ応用編（Ｗｅｂアプリケーションセキュリティ）	Webアプリケーションに対する攻撃手法をハンズオンで体験し、セキュア開発やセキュリティテストの手法を学びます 。	脆弱性診断・ペネトレーションテスト	23-010-041
38	グローバルセキュリティエキスパート株式会社	Ｍｉｃｒｏ Ｈａｒｄｅｎｉｎｇ：Ｅｎｔｅｒｐｒｉｓｅ Ｅｄｉｔｉｏｎ（マイクロハードニング：エンタープライズエディション）	受講者は4人～6人のチームに分かれ、ECサイトをさまざまな攻撃から守る、サイバー攻撃対応演習です。確認検証を行うことにより、サイバー攻撃の対応能力向上を目指します。	セキュリティ監視・運用	22-011-035
39	株式会社アクト	Ｃｙｂｅｒ Ｔｈｒｅａｔｓ ａｎｄ Ｄｅｆｅｎｓｅ Ｅｓｓｅｎｔｉａｌｓ	実際のサイバー攻撃を受け、複数の検出・監視ツールを駆使してサイバー攻撃を検出し、その分析を行うためのスキルを習得します。	セキュリティ監視・運用	23-012-042
40	株式会社日立アカデミー	ケーススタディから学ぶ情報セキュリティリスク対策	本コースでは、脆弱性への対策、脅威への対策、残存リスクの評価などを行います。また併せて、対策立案時の実務におけるポイントやノウハウ（再利用可能な整理の仕方など）も解説します。	セキュリティ統括	23-013-043

※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/skill-standard/plus-it-ui/index.html）を参照下さい