2025年4月1日

No.	実施機関名	講習名	講習内容	主な分野※	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
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 基礎演習２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	23-001-036
3	大日本印刷株式会社	サイバー攻撃対処コース_講義＆実機演習_基礎_3日	実際に起きている最新のサイバー攻撃手法に基づいたシナリオによる、サイバーレンジ上での実践的な演習。	セキュリティ監視・運用	25-001-054
4	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。	セキュリティ調査分析・研究開発	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。	セキュリティ調査分析・研究開発	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	株式会社ワイ・イー・シー	マルウェア解析基礎	マルウェア解析に必要となる一般的な基礎知識、基礎的な静的解析（表層解析）手法、動的解析手法等を中心に講習を行う。	セキュリティ調査分析・研究開発	24-002-044
8	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
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
10	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
11	トレンドマイクロ株式会社	ランサムウェア 対応・防御トレーニング	ランサムウェアで使われる最新の攻撃・侵入手法を座学を中心に技術演習やグループワークを交えながら学習し、ランサムウェア対応に必要な知識や技術を基礎から学ぶトレーニングです。	セキュリティ監視・運用	24-003-045
12	ＮＥＣビジネスインテリジェンス株式会社	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ビジネスインテリジェンス株式会社	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ビジネスインテリジェンス株式会社	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ビジネスインテリジェンス株式会社	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ビジネスインテリジェンス株式会社	【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ビジネスインテリジェンス株式会社	【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ビジネスインテリジェンス株式会社	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ビジネスインテリジェンス株式会社	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	ＮＥＣビジネスインテリジェンス株式会社	インシデントレスポンス基礎　－ログ解析編－	サイバー攻撃の予兆分析や、発生したセキュリティインシデントの全体像の把握・原因特定に必要となる、ログ解析スキルを修得します。また、マシン実習を通して実践的なログ解析手法を修得します。	セキュリティ調査分析・研究開発	24-004-046
21	ＮＥＣビジネスインテリジェンス株式会社	【短期集中】実践！サイバーセキュリティ演習	サイバー攻撃（標的型攻撃）に係るインシデントハンドリングの内容を、ひととおり体験します。インシデントハンドリングのポイントを短期間で習得できます。	セキュリティ調査分析・研究開発	25-004-055
22	ＮＥＣビジネスインテリジェンス株式会社	情報セキュリティマネジメント（リスクアセスメント実践編）	本研修ではケーススタディを通じ、ISO/IEC 27000 ファミリー規格をベースとしたリスクアセスメント、リスク対応、リスク受容の一連の流れを経験することで、実践的な能力を身に着けます。	セキュリティ統括	25-004-056
23	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
24	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
25	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
26	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
27	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

No.	実施機関名	講習名	講習内容	主な分野※	講習番号
28	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
29	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。	セキュリティ監視・運用	21-005-019
30	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
31	株式会社ラック	マルウェア解析ハンズオン専門演習コース	マルウェア解析を難しくしている耐解析機能（パッキング、解析環境検知、難読化）に対し、本物のマルウェアを通じ、解析能力のレベルアップを目的とした実践的な対応方法を学ぶコースです。	セキュリティ調査分析・研究開発	24-005-047
32	株式会社ラック	情報セキュリティ事故対応2日コース 実機演習編	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ぶコースです。座学でインシデントレスポンスのノウハウを学習した後、実機環境を使用し、演習を行います。	セキュリティ監視・運用	24-005-048
33	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
34	株式会社アイ・ラーニング	プロが教えるインシデント対応実践ワークショップ	インシデント対応の流れと重要性を理解し、注意すべきバイアスやプレッシャー等を紹介します。実際の事例を基に作成したシナリオによる疑似体験により、実践的なスキルを1日で習得できます。	セキュリティ調査分析・研究開発	24-006-049
35	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評価	情報セキュリティマネジメントは自動的に最適化されるものではありません。本研修では組織の意思決定を支える評価の基礎を学び、評価結果を組織の成果につなげる実践的な監査技法の習得を目指します。	セキュリティ監査	25-006-057
36	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
37	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
38	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
39	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 ASM基礎コース	ASM（Attack Surface Management)について理解をするとともに、攻撃面に対するIT資産/サービスに関するセキュリティ管理方法を習得します。また、ASMをはじめとしたWebサーバの対策や従業員へのセキュリティ対策について学びます。	セキュリティ監視・運用	25-007-058
40	NICT（国立研究開発法人情報通信研究機構 ）	実践サイバー演習RPCI(リプシィ)	実際のインシデントを想起させるリアルな攻撃シナリオによるサイバー攻撃に対し、実機を用いて攻撃の痕跡を調査する実践的インシデントハンドリングです。★25年度より新シナリオとなりました。	セキュリティ監視・運用	21-008-023
41	株式会社サイバージムジャパン	Ｃｙｂｅｒ－Ｔｈｒｅａｔｓ ａｎｄ Ｄｅｆｅｎｓｅ Ｅｓｓｅｎｔｉａｌｓ	APT攻撃への対応を実践的に学ぶことを目的とした、ハンズオン形式の講習です。安全に隔離された仮想環境において、リアルタイムで模擬APT攻撃を受け、その検知および対応をします。	セキュリティ監視・運用	22-009-031
42	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
43	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。	セキュリティ調査分析・研究開発	22-010-034
44	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
45	NRIセキュアテクノロジーズ株式会社	セキュアEggs応用編（DevSecOps）	DevOps・アジャイル開発の速度や文化に適したセキュリティの考え方や開発速度を落とさずセキュリティを強化する技術について講義と演習で学びます。	デジタルプロダクト開発	25-010-059
46	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
47	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
48	株式会社サイバーディフェンス研究所	OTシステムハッキング｜独自プロトコル解析とサイバー攻撃の実践	OTシステムをターゲットとした通信を悪用した攻撃の流れをハンズオンで学習します。攻撃手法や攻撃者の思考を踏まえてセキュリティ施策の検討・実行を進められるようになります。	脆弱性診断・ペネトレーションテスト	24-014-050
49	株式会社サイバーディフェンス研究所	ハッキング｜ハードウェア	ハードウェアハッキングに必要な基礎知識とテクニックを習得します。様々なIoTに関与する技術者が、攻撃手法や攻撃者の思考を踏まえてセキュリティ施策の検討・実行を進められるようになります。	脆弱性診断・ペネトレーションテスト	24-014-051
50	株式会社サイバーディフェンス研究所	マルウェア解析Ⅰ	マルウェアの解析に必要な知識と基礎から学び、ハンズオンでの検体解析をとおして、実戦的なマルウェア解析技術の習得を目指すトレーニングコースです。	セキュリティ調査分析・研究開発	24-014-052
51	株式会社サイバーディフェンス研究所	マルウェア解析Ⅱ	マルウェア解析に必要なリバースエンジニアリングの基礎を学びます。モニタツールによる動的解析では難しい、マルウェアが潜在的に有する機能や通信プロトコルを解析できるようになることを目的とします。	セキュリティ調査分析・研究開発	24-014-053
52	株式会社サイバーディフェンス研究所	デジタルフォレンジック基礎＆実践演習	当社で提供しているファストフォレンジックツールCDIRを活用しながら、Windowsを対象にファストフォレンジックに必要となる知識、技術をハンズオン形式で学びます。 CSIRTの初動対応機能を強化したい組織、外部ベンダーとの連携を前提とした組織、組織犯罪等においてデジタルフォレンジック対応を担当する方に向けた内容となっています。	セキュリティ調査分析・研究開発	25-014-060
53	株式会社Armoris	侵入型サイバー攻撃（標的型攻撃）に関する攻撃・防御学習講座	サイバー攻撃により記録されるエビデンス情報及びログの調査を疑似環境を用いて経験し、攻撃側・防御側それぞれの視点で侵入型サイバー攻撃への対応スキルの習得を図る。	セキュリティ調査分析・研究開発	25-015-061
54	技術研究組合制御システムセキュリティセンター	制御システムセキュリティ教育講習（入門編）	座学に加え、会場に設置の模擬システムを使用した参加型インシデント対応演習を複数実施。グループディスカッション、発表を通じて制御システムの実情と脅威に関する基礎を習得する。	デジタルプロダクト運用	25-016-062

No.	実施機関名	講習名	講習内容	主な分野※	講習番号
55	株式会社網屋	Cyber-Threats and Defense Essentials	サイバーセキュリティの基礎の復習と、実際にサイバー攻撃を受けて検知する業務を実体験する実践的なトレーニングです。セキュリティエンジニア率いるレッドチームと連携し、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攻撃を体験できます。 ※株式会社サイバージムジャパンで提供されている同名の講習がございますが、内容は異なりますので御注意ください。	セキュリティ監視・運用	25-017-063
56	株式会社網屋	インシデント初動対応トレーニング	インシデント発生時の基本的な初動対応を実践的に習得するトレーニングです。インシデントに適切に対応することで、被害範囲の最小化・証拠保全による原因の早期究明に繋がります。	セキュリティ監視・運用	25-017-064

※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。