日立グループが提供する教育メニュー （1/3）

HITACHI
Inspire the Next

【セキュリティ人材育成】

参考リンクから詳細と申し込み方法を確認できます。
学習期間のめやすが個別相談となっているサービスは、各サイト内にあるお問合せから個別に相談ください。

No.	サービス名	概要	教育形態	学習期間のめやす	参考リンク
1	セキュリティ統括 CSIRT	・CSIRTの役割や分類など、CSIRTに関する基礎的な知識を習得 ・不正アクセスやマルウェア感染の脅威を映像で疑似体験することで、CSIRT運用の重要性を理解	eラーニング/オンライン	半日	CSIRT基礎
2	PSIRT	・PSIRTの役割や分類など、PSIRTに関する基礎的な知識を習得 ・製品・サービスの脆弱性を利用した不正アクセスやマルウェア感染によるDDoS攻撃への加担など、脅威を映像で疑似体験することで、PSIRT運用の重要性を理解	eラーニング/オンライン	半日	PSIRT基礎
3	FSIRT	・制御システムを取り巻く脅威、FSIRTの基礎について学習 ・FSIRT技術者として対応するための、インシデント発生前・発生中・発生後の役割習得	eラーニング/オンライン	半日	FSIRT基礎
4	サイバー攻撃対策	・サイバー攻撃の一般的な種類とその対策方法を習得 ・攻撃者がマルウェア感染したパソコンを遠隔操作しネットワーク内の機密情報を搾取する様子など、攻撃者の手口を映像で確認しながらサイバーキルチェーンの攻撃行動を学習 ・サイバー攻撃の対策として必要になる「技術」「人」「組織」それぞれの対策について紹介	eラーニング/オンライン	半日	サイバー攻撃対策（基礎）
5	セキュリティマネジメント	・情報セキュリティ維持、個人情報保護のための管理システムと情報セキュリティに関連する規格、法律制度など管理的対策に関する概要を学ぶ	eラーニング/オンライン	6時間～1日	セキュリティマネジメント
6	サイバーレジリエンス	・サイバーレジリエンスとはなにかといった基礎的な内容を習得 ・脆弱性、不正アクセスといったサイバーレジリエンスの脅威を疑似体験 ・サイバーレジリエンスを実現するために企業が備えるべき「予測力」「抵抗力」「回復力」「適応力」について、具体的な対策技術とあわせて学習	eラーニング/オンライン	半日	サイバーレジリエンス基礎
7	脆弱性ハンドリング	・効果的な脆弱性管理/対策を学ぶ ・実際にセキュリティ診断を実施することを映像で疑似体験しながら、サイバーセキュリティ診断の手法を学ぶ ・ホワイトハットハッカーとのライブ中継で実際に脆弱性を分析し、リスク評価を実践	eラーニング/オンライン	半日	脆弱性ハンドリング
8	ネットワークセキュリティ	・ネットワークセキュリティにおける攻撃手法および防御手法を学ぶ	eラーニング/オンライン/マシン実習	6時間～3日	ネットワークセキュリティ

日立グループが提供する教育メニュー （2/3）

HITACHI
Inspire the Next

【セキュリティ人材育成】

No.	サービス名	概要	教育形態	学習期間のめやす	参考リンク
9	クラウドセキュリティ	・クラウドやクラウドサービスの基礎、セキュリティの脅威について学習 ・安全にクラウドサービスを利用・提供するための、さまざまな技術的・人的・組織的対策を習得	eラーニング/オンライン	半日	クラウドセキュリティ基礎
10	アーティファクトハンドリング	・サイバー攻撃が残す代表的な痕跡（アーティファクト）と対応までの一連の流れを習得 ・サイバー攻撃やマルウェアの静的解析／動的解析を映像で疑似体験 ・ホワイトハットハッカーとのライブ中継でアーティファクト解析を実施し、影響範囲の特定などハンドリングを理解する	eラーニング/オンライン	半日	アーティファクトハンドリング
11	インシデントハンドリング	・インシデントハンドリングの流れを学ぶ ・不正アクセスの痕跡調査を疑似体験し、早期検知、対応を学ぶ ・ホワイトハットハッカーとのライブ中継でログ分析を実践し、ログ管理の重要性を理解する	eラーニング/オンライン	半日	インシデントハンドリング
12	マルウェア解析技術者育成	・専門的な知識および解析ツールを用いた解析技術の習得が可能 ・セキュリティアナリストによる講義、および実機を使用した実践形式での研修	集合研修	2日～5日	マルウェア解析技術者養成コース

【組織の対応力向上】

No.	サービス名	概要	教育形態	学習期間のめやす	参考リンク
13	組織連携型サイバー訓練（定型）	・仮想組織で発生するセキュリティインシデントを演習環境で実体験しながら、インシデントレスポンスのハンドリングを学んでいきます。 ・状況付与型の机上演習により、インシデントレスポンスにおける実組織での対応や、部門間連携を検証、評価	集合演習/オンライン	個別相談	サイバーセキュリティ演習（初級） インシデント対応訓練
14	組織連携型サイバー訓練（カスタム）	・大みか事業所内に、サイバー攻撃を想定した防衛訓練施設「NxSeTA」を設置 ・社会インフラ事業や製造業向けにリモート環境での実践的なインシデント対応訓練を提供	集合演習/オンライン	個別相談	サイバー防衛訓練サービス
15	課題抽出型サイバー訓練	・インシデント発生時に、組織内で策定されているインシデント対応マニュアル通りに対応できるかを、机上演習を通じて検証、評価	集合演習/オンライン	個別相談	インシデント対応マニュアル検証

日立グループが提供する教育メニュー （3/3）

【一般社員の意識向上】

No.	サービス名	概要	教育形態	学習期間のめやす	参考リンク
16	情報セキュリティ対策	・情報セキュリティの基本的な概念を習得 ・ビジネスメール詐欺の添付ファイルを開封するとどのような事態になるのかなど、身近な脅威を映像で体験しながら理解し、防御方法を学習 ・脅威を見分けるための着眼点や、脅威が発生した際の初動対応について紹介	eラーニング/オンライン	半日	情報セキュリティ対策（基礎）
17	標的型メール訓練（座学）	・近年のサイバー攻撃のトレンドを紹介、流行するサイバー攻撃の手口を理解 ・不審メールの添付ファイル開封やURLリンククリックで発生する被害の疑似体験、影響の学習 ・不審メールを見分けるポイントの解説、添付ファイルの開封、URLリンクをクリックしてしまった場合の対処として社員・職員一人ひとりが実施する内容を紹介	eラーニング	動画配信は半日	標的型攻撃メール対策（一般向け）（座学）
18	標的型メール訓練（訓練メール配信）	・標的型攻撃メールを模擬した訓練メールを対象者に送信します ・従業員へ標的型攻撃メールへの意識向上や受信時の初動対応について事前教育をすることで、標的型メールを受信した際の対策を従業員個人で可能にします	訓練メール配信	個別相談	標的型攻撃メール訓練サービス（日立システムズ） 標的型攻撃メール訓練サービス（日立ソリューションズ） 標的型攻撃メール訓練サービス（日立ソリューションズクリエイト）

【特定業界向け】

No.	サービス名	概要	教育形態	学習期間のめやす	参考リンク
19	金融機関向け人材育成プログラム	・金融庁と日本銀行より求められている「地域金融機関におけるサイバーセキュリティセルフアセスメント」に準じたサイバーセキュリティ人材の育成、ならびに金融機関のセキュリティレベルの底上げが可能 ・日立グループで実践している対策方法や、現場での経験・体験談を提供することで「マニュアルの知識」にとどまらないノウハウやスキルを習得でき、セキュリティリスクの管理やセキュリティ対策の企画・立案などができる人材・組織を育成	集合研修/オンライン	約6か月	金融機関向けセキュリティ人材育成プログラム

本資料に記載の内容は、サービスの改良などにより予告なく変更することがあります。

2024/12版