LAC Security Academy

ラックセキュリティアカデミー

全コースガイド 2024 年度版 下半期

インシデントは起こるものです

全ての研修は、脅威・サイバー攻撃への実践的な対応力強化を焦点にプログラム化

LAC
株式会社ラック

ラックセキュリティアカデミー概要

ラックセキュリティアカデミーでは、幅広いセキュリティ分野においてそれぞれ専門性の高い講師陣による実践的な情報セキュリティ教育を行っています。

ラックセキュリティアカデミー 3 つの特長

国内最大規模の監視センター JSOC の豊富な実績

ラックが誇るセキュリティ監視センター JSOC では、アナリストとエンジニアが、24 時間 365 日の体制で、お客様のログをリアルタイムに分析すると同時に、独自に設置しているハニーポット（おとりサーバ）が収集した攻撃の分析を行い、最新のサイバー攻撃の傾向を把握しています。
さらにグローバルでのセキュリティ情報のチェックやセキュリティ問題に発展しやすい政治的なニュースや事件を把握し、インターネット上の有事にいち早く対応できるよう備えています。
ラックセキュリティアカデミーでは、これらの情報により、常に最新のデータを基にした研修を行っております。

＋

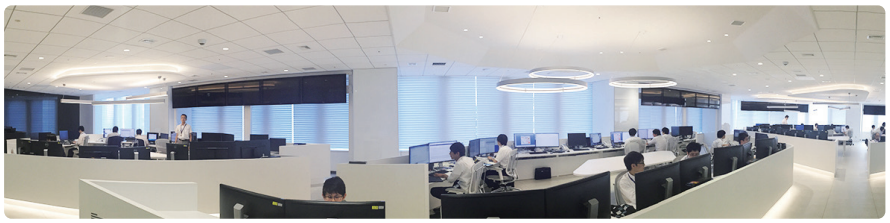
独自の研究所運営による圧倒的な情報量

情報セキュリティ最先端の研究を行うため、フォレンジックやマルウェア解析などの専門研究員が、最新の情報セキュリティ課題を持ち、活動をグローバルに広げ研究に取り組んでいます。

＋

専門性の高い講師陣

現役のアナリスト、研究員、コンサルタントなど、各分野における専門講師がコースを担当します。積み上げてきた実績や最先端の研究により集まった圧倒的な情報量を基に、テキストだけでは伝えられない研修を行います。



ラックのセキュリティ監視センター JSOC（ジェイソック）

集合研修の概要

「集合研修」は、指定の場所、もしくは Web 会議システム上にお集まりいただき、リアルタイムで講義を行う研修です。

各分野における専門講師が、積み上げてきた実績や最先端の情報を元に、講義を行います。
講義内容の質問やサポートもその場で受けられ、また受講者の進み具合や理解度に合わせて講義を進めるため、初学者でも安心してご受講いただけます。

研修形態や受講形態も様々な形態を用意しておりますので、ご希望にあわせて受講いただくことが可能です。詳細は、次ページを参照ください。

オンライン研修の概要

インターネットを利用して、いつでも、どこでも、何度でも受講できるオンデマンド配信型のオンライン学習サービスです。講師のレクチャーで進む e-ラーニングタイプのコースや、パソコンやサーバを使用して実際に操作しながら学習する実践タイプのコースもあります。スマートフォンやタブレットからも受講可能です。実務が忙しくまとまって時間を確保できない方、多岐にわたるセキュリティ領域全般をまずは知識習得として広く学習されたい方などにおすすめいたします。

選べる 研修&受講スタイル

集合研修では、研修形態と、受講形態が選べるコースもご用意しております。

研修形態

オープン開催

・予め、**決められた開催日程**にお申し込みいただく研修形態です。
・**複数の企業・団体から参加**されますので、他業種の方との交流も図れます。

個別開催

・**単一企業向け**の研修になりますので、クローズ環境となり、その企業に特化した受講成果が得られます。
・**ご希望の日程、受講形態**をご指定いただく研修形態です。
・また、オーダーメイドトレーニング（別途見積）を行うことも可能です。

受講形態

対面型

・弊社会場（永田町）や、お客様指定場所（個別開催の場合）に集合の上、受講していただきます。
・他の受講者と同じ空間で受講いただきます。講師は受講者の進み具合や理解度に合わせて講義を進めます。

リモート Live 型

・Web 会議システムを利用して、リモート Live で受講していただきます。
・場所を選ばず受講いただけますので、全国に拠点をお持ちの企業様にもお勧めです。

ハイブリッド

・対面型、リモート Live 型、同時に開催いたします。受講者はどちらかお好きな形態をご選択ください。

集合研修　対象別コース一覧

カテゴリー	コース	掲載ページ	一般社員・職員	管理職	IT技術者（インフラ系）	IT技術者（開発系）	情報システム部門	セキュリティ推進部門	SOC（セキュリティ運用）	CSIRT（管理系）	CSIRT（技術系）	監査担当
スペシャリスト育成コース	IT と情報セキュリティ初級コース	10	◎	◎	○	○	○	○		●	○	○
	情報セキュリティマネジメントコース	11	○	◎				◎		◎		●
	情報セキュリティスペシャリストコース	12			◎	◎	◎		●	○	◎	◎
	Web セキュリティ設計実装講座	13			●	◎	●	●	●	○	●	●
	事故対応 1 日 登録セキスペ特定講習	14	●	◎	●	●	◎	◎	●	◎	◎	●
	事故対応 2 日 登録セキスペ特定講習	15	●	●	◎	●	◎	◎	●	◎	◎	●
	攻撃手法解説コース	16			◎	◎	◎	◎	◎	○	◎	●
	攻撃手法原理詳解コース	17			◎	◎	◎	◎	◎	○	◎	●
	セキュリティオペレーション初級 登録セキスペ特定講習	18			●	○	●	●	◎	○	◎	●
	セキュリティオペレーション中級 登録セキスペ特定講習	19			●	○	●	●	◎	○	◎	●
	プラットフォーム脆弱性診断 登録セキスペ特定講習	20			◎	●	◎	◎	◎	○	◎	◎
	Web アプリ脆弱性診断 登録セキスペ特定講習	21			●	◎	◎	◎	◎	○	◎	◎
	デジタル・フォレンジック 登録セキスペ特定講習	22			○	○	○	○	●	○	◎	○
	ペネトレーションテストハンズオンコース	24			○	○	◎	◎	◎	○	◎	●
	マルウェア解析ハンズオン入門 登録セキスペ特定講習	25			○	○	○	○	●	○	◎	○
	マルウェア解析ハンズオン専門 登録セキスペ特定講習	26			○	○	○	○	●	○	◎	○
	マルウェア解析ハンズオン専門演習 登録セキスペ特定講習	28			○	○	○	○	●	○	◎	○
	スマホアプリセキュリティ対策講座	29			●	◎	●	●	●	○	●	●
	OT セキュリティ入門	30	●	●	○	○	○	●	○	○	○	
	セキュリティ競技入門コース	31			◎	◎	●	●	◎	●	◎	
一般社員	理解度チェック	32	◎									
資格取得	CISSP トレーニング	33		●	○	○	◎	◎	◎	◎	◎	◎
	内部監査人能力認定	34		○	●	●	◎	◎	●	●	●	◎

大変おすすめ ◎ おすすめ ● ややおすすめ ○

オンライン研修　対象別コース一覧

カテゴリー	コース	掲載ページ	一般社員・職員	管理職	IT技術者（インフラ系）	IT技術者（開発系）	情報システム部門	セキュリティ推進部門	SOC（セキュリティ運用）	CSIRT（管理系）	CSIRT（技術系）	監査担当
スペシャリスト育成コース	攻撃手法を知る【入門編】	47			◎	◎	◎	◎	◎	○	◎	●
	攻撃手法を知る【詳解編】～ポートスキャン～	47			◎	◎	◎	◎	◎	○	◎	●
	攻撃手法を知る【詳解編】～パスワードクラッキング～	47			◎	◎	◎	◎	◎	○	◎	●
	脆弱性ハンドリング	47			●	●	◎	◎	◎	◎	◎	●
	ソーシャルエンジニアリング概論	47	●	◎	○	○	◎	◎	○	◎	○	●
	Web サイト開発で知っておきたいセキュリティ設計と実装の考慮	47			●	◎	●	●	●	◎	●	●
	セキュリティオペレーションコース	48			●	○	●	●	◎	○	◎	●
	Web アプリケーション診断コース	48			●	◎	◎	◎	◎	○	◎	◎
	プラットフォーム診断コース	48				●	◎	◎	◎	○	◎	◎
	マルウェア解析 Basic1	48			○	○	○		●	○	◎	○
	実践！インシデントレスポンス侵害調査演習	48				◎	◎	●	●	◎	○	◎
	IR DF（インシデント・レスポンスデジタル・フォレンジック）演習ドリル	48			○	○	○	○	●	○	◎	○
	マルウェア解析のためのアセンブラ入門	48			○	○	○	○	●	○	◎	○
	マルウェア解析入門ドリル	48			○	○	○	○	●	○	◎	○
プラス・セキュリティ人材育成コース	プラス・セキュリティ人材育成講座 セキュリティの基礎	43	◎	◎	●	●	●	●	●	●	●	●
	管理職向け 情報セキュリティ講座（1）	45	●	◎								
	情報セキュリティマネジメントパックコース（前編）	45	●	◎	●	●	◎	◎	●	◎	◎	●
	情報セキュリティマネジメントパックコース（後編）	45	●	◎	●	●	◎	◎	●	◎	◎	●
	ゼロから学ぶ情報セキュリティ基礎	45			●	●	●	◎	◎	●	●	●
	インシデントレスポンス概論	47	●	◎	●	●	◎	◎	●	◎	◎	●
	攻撃手法を知る【入門編】	47			◎	◎	◎	◎	◎		◎	●
	Web サイト開発で知っておきたいセキュリティ設計と実装の考慮	47			●	◎	●	●	●	◎	●	●
	改正個人情報保護法において求められるサイバーセキュリティ態勢	46	○	◎	○	○	●	◎	●	◎	●	◎
一般社員向けコース	ロボタと挑戦！セキュリティチャレンジ【日常編】（1）	42	◎	◎								
	ロボタと挑戦！セキュリティチャレンジ【日常編】（2）	44	◎	◎								
	新入社員向け 情報セキュリティ研修	44	◎	◎								
	情報セキュリティ講座【社員の意識編】	41	◎	◎								
	情報セキュリティ研修【標的型攻撃メール対策編】	42	◎	◎	●	●	●	●	●	●	●	●
	情報セキュリティ研修【テレワーク編】	44	◎	◎								
	情報セキュリティ講座【サイバー攻撃編】	41	◎	◎								
	サポート詐欺の実態	43	◎	◎	●	●	●	●	●	●	●	●

大変おすすめ ◎ おすすめ ● ややおすすめ ○

対象者別お勧めコース

オンライン研修（オンデマンド配信）　集合研修／リモート Live 配信　体験型研修

一般社員向け

基礎 ▶▶▶ 応用

新社会人
- P44 新入社員向け 情報セキュリティ研修
- P45 ゼロから学ぶ 情報セキュリティ基礎
- P49 情報セキュリティ リテラシー向上パック

管理職
- P45 管理職向け 情報セキュリティ講座（1）
- P43 プラス・セキュリティ人材育成講座 セキュリティの基礎
- P45 情報セキュリティ マネジメントパック コース（前編）
- P14 情報セキュリティ事故対応1日コース 机上演習編

一般社員・職員
- P49 情報セキュリティ リテラシー向上パック
- P44 情報セキュリティ研修【テレワーク編】
- P44 情報セキュリティ研修【標的型攻撃メール対策編】
- P44 ロボタと挑戦！セキュリティ チャレンジ【日常編】
- P41 情報セキュリティ講座【社員の意識編】

スペシャリスト育成

基礎 ▶▶▶ 応用 ▶▶▶ 専門

インシデント対応
- P42 情報セキュリティ技術入門パック
- P45 情報セキュリティ マネジメント パックコース
- P49 インシデント初動対応 基本教育パック
- P14 情報セキュリティ事故対応1日コース 机上演習編
- P15 情報セキュリティ事故対応2日コース 実機演習編

開発／SI
- P16, 17 攻撃解説／攻撃原理
- P13 Webセキュリティ設計
- P29 スマホアプリ セキュリティ対策講座
- P20, 21 プラットフォーム脆弱性診断／Web脆弱性診断

デジタル フォレンジック
- P14, 15 情報セキュリティ事故対応1日コース／事故対応2日コース
- P16, 17 攻撃解説／攻撃原理
- P22 デジタル・フォレンジック
- P48 インシデント・レスポンス デジタル・フォレンジック 演習ドリル

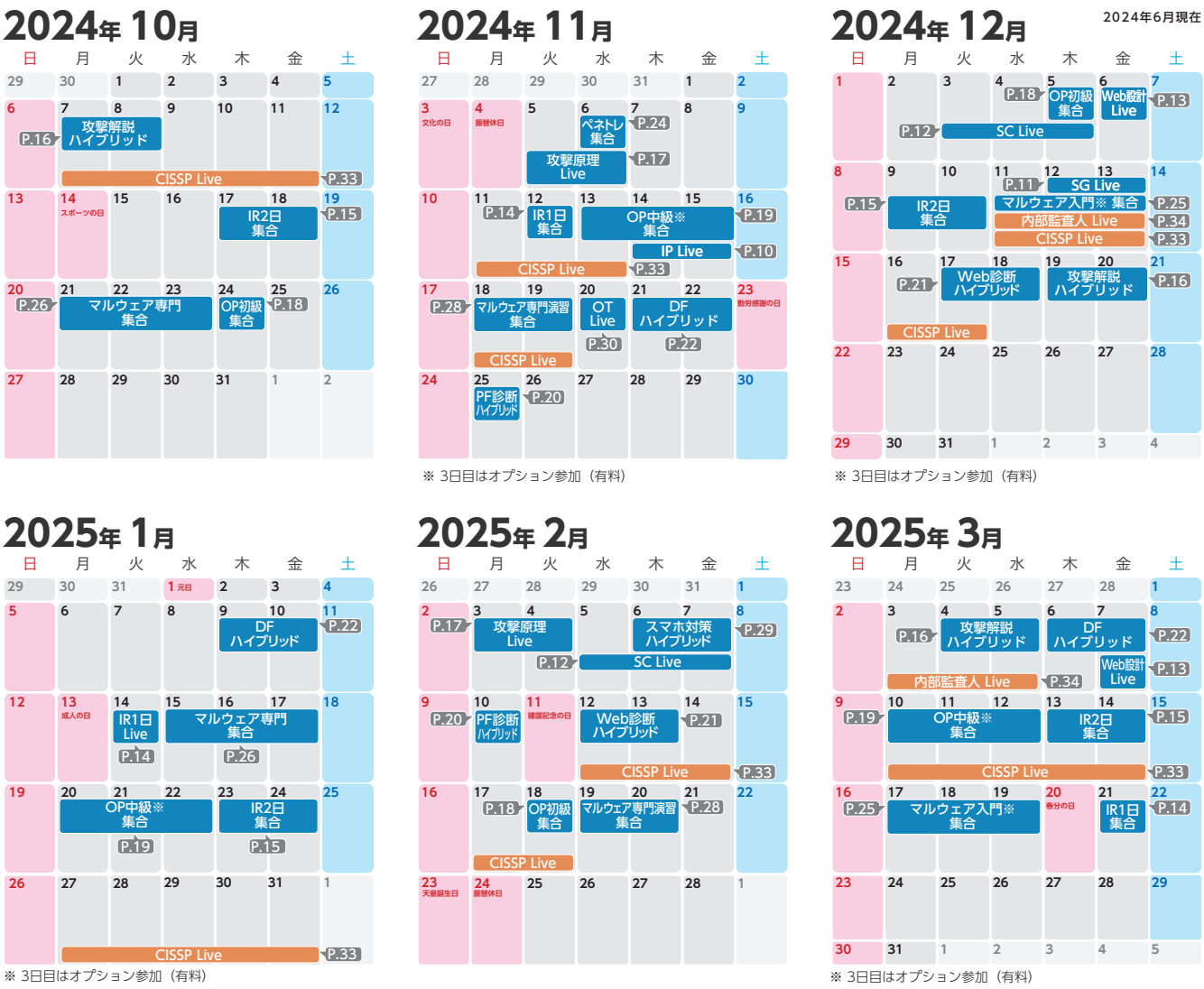
ログ分析（アナリスト）／SOCエンジニア
- P16, 17 攻撃解説／攻撃原理
- P18 セキュリティ オペレーション 実践コース 初級編
- P48 セキュリティ オペレーション
- P19 セキュリティ オペレーション 実践コース 中級編
- P48 インシデント レスポンス 侵害調査演習

マルウェア解析
- P16, 17 攻撃解説／攻撃原理
- P48 マルウェアBasic
- P25 マルウェア入門
- P48 アセンブラ入門
- P26, 28 マルウェア専門／専門演習

※こちらに記載がないコースも多数ご用意しております。

オープン開催 2024 年度下半期スケジュール

2024年6月現在



※開催日は予告なく変更する場合がございます。最新日程はWebにてご確認ください。

分　類	スペシャリスト育成コース　資格取得支援
コース名（略）	IP ..... IT と情報セキュリティ初級コース SG ..... 情報セキュリティマネジメントコース SC ..... 情報セキュリティスペシャリストコース IR 1 日 ..... 情報セキュリティ事故対応 1 日コース 机上演習編 IR 2 日 ..... 情報セキュリティ事故対応 2 日コース 実機演習編 攻撃解説 ..... 攻撃手法解説コース 攻撃原理 ..... 攻撃手法原理詳解コース OP 初級 ..... セキュリティオペレーション実践コース 初級編 OP 中級 ..... セキュリティオペレーション実践コース 中級編 PF 診断 ..... プラットフォーム脆弱性診断ハンズオンコース Web 診断 ..... Web アプリケーション脆弱性診断ハンズオンコース ペネトレ ..... ペネトレーションテストハンズオンコース マルウェア入門 ..... マルウェア解析ハンズオン入門コース マルウェア専門 ..... マルウェア解析ハンズオン専門コース マルウェア専門演習 ... マルウェア解析ハンズオン専門演習コース DF ..... デジタル・フォレンジックコース Web 設計 ..... Web セキュリティ設計実装講座 スマホ対策 ..... スマホアプリセキュリティ対策講座 OT ..... OT セキュリティ入門 内部監査人 ..... 情報セキュリティ内部監査人能力認定（JASA）準拠対策講座 CISSP ..... CISSP CBK トレーニング

情報処理安全確保支援士（登録セキスペ）特定講習

サイバーセキュリティの専門人材の国家資格である情報処理安全確保支援士（登録セキスペ）の資格更新に必要な実践講習のなかで、経済産業大臣が定める民間事業者が提供する「特定講習」として、弊社の研修が採用されました。

特定講習対象コース

各詳細ページのタイトル上に
上記アイコンが表記されています。

お申し込み方法

ホームページ選択
対象コースのホームページを選択してください。

https://www.lac.co.jp/service/education/

お申し込み
「お申し込み」ボタンをクリックしてください。

※外部リンク（トライコーン株式会社が提供する「クライゼル」）に遷移します。

申 告
備考欄に「IPA 登録セキスペ更新」とご記入ください。

※受講当日は、IPA 規程によりご本人確認をさせていただきますので、**写真付きの身分証明書・登録証カード**をご持参ください。

目次

■開催形態の種別について

● オープン： 弊社会場での常設研修です

● 個　　別： 単一企業様向け研修です

オープン・個別どちらでも開催します

個別研修で開催します（オープン開催無し）

■研修形態の種別について

研修内容を講義形式で学んでいただきます

グループでディスカッションしながら行う、ワークショップ形式の体験型講座です

パソコンやサーバを使用して、実際に操作しながら学習する実践タイプの研修です

オンデマンドで学んでいただけるコースもございます。

オープン＋個別＋ | ハンズオン | 座学 | 体験

IT と情報セキュリティ初級コース NEW

～『IT パスポート試験シラバス Ver.6.3』対応～

国家試験「IT パスポート」試験のシラバスに基づき、情報セキュリティはもちろん、IT 全般の知識・技術の基礎が身につくコースです。

受講の効果

・業界や職種関係なく、情報セキュリティをはじめとした IT 全般の知識や技術を体系的に学べる
・IT パスポート試験の合格に向けた知識を学ぶことができる
・他の上級コース受講に必須の知識・技術を得られる

前提知識

・なし

こんな方にお勧めです

■ 一般社員
■ IT 技術者（開発系）
■ CSIRT 要員（管理系）
■ 管理職
■ 情報システム・セキュリティ推進部門担当者
■ CSIRT 要員（技術系）
■ IT 技術者（インフラ系）
■ SOC（セキュリティ運用）要員
■ 監査担当

実施内容

1 日目

1. IT、セキュリティに関連する法規、権利
・知的財産権
・セキュリティ関連法規
・セキュリティ関連ガイドライン
・標準化関連
・組織規範
・契約類型

2. プロジェクトマネジメントと IT サービスマネジメント
・プロジェクトマネジメント
・IT サービスマネジメント
・システム監査

3. システム開発のプロセス
・システム開発のプロセス
・システム開発手法
・システム開発モデル
・開発プロセスに関連する考え方

2 日目

4. ハードウェア、ソフトウェア、システム構成要素
・ハードウェアの概要
・ソフトウェアの概要
・システム構成要素

5. データベース
・データベースモデル
・データベース設計
・データ操作
・トランザクション処理

6. ネットワーク
・ネットワーク方式
・ネットワークの構成要素
・IoT ネットワークの構成要素
・通信プロトコル
・ネットワーク応用

7. セキュリティ
・情報セキュリティとは
・情報セキュリティ管理
・攻撃手法
・情報セキュリティ対策
・暗号技術と PKI
・利用者認証
・開発ライフサイクルとセキュリティ

IT パスポート試験の全範囲を取り上げているわけではありませんのでご注意ください

実施要項

開催日程	**2024** 年 **11** 月 **14** 日 (木) ～ **15** 日 (金)　締切 **10** 月 **31** 日 (木)
研修期間	2 日間　13:00 ～ 17:30
受講料	80,000 円（税込 88,000 円）/ 人
定員	30 名（最小催行人数 5 名）
会場	リモート Live　ツール：Zoom

講師　星 代介　他

オープン＋個別＋ | ハンズオン | 座学 | 体験

情報セキュリティマネジメントコース NEW

～『情報セキュリティマネジメント試験シラバス Ver.4.0』対応～

国家試験「情報セキュリティマネジメント」のシラバスに基づいた、情報セキュリティ全般の知識や技術を身につけられるコースです。

受講の効果

- 特定業界や職種に偏ることなく、情報セキュリティに関連した知識、技術を体系的に学ぶことができる
- 実務や教育経験豊富な講師から、情報セキュリティの実践的な考え方を身につけられる
- 情報セキュリティマネジメント試験の合格に向けた知識を学ぶことができる

前提知識

- IT パスポート試験合格程度の知識（不安な方は「IT と情報セキュリティ初級コース～『IT パスポート試験シラバス Ver.6.3』対応～」（P10）の受講もご検討ください）

こんな方にお勧めです

■ 一般社員
■ IT 技術者（開発系）
■ CSIRT 要員（管理系）
■ 管理職
■ 情報システム・セキュリティ推進部門担当者
■ CSIRT 要員（技術系）
■ IT 技術者（インフラ系）
■ SOC（セキュリティ運用）要員
■ 監査担当

実施内容

1 日目

1. 情報セキュリティマネジメント（概要）
- 情報セキュリティの定義、要素
- 情報資産
- 脅威、脆弱性、リスクの概要
- ISMS の定義、関連規格、評価とレビュー
- 情報セキュリティポリシー
- 情報セキュリティマネジメント体制

2. 情報セキュリティマネジメント（実践）
- リスクマネジメントの流れ
- リスクアセスメント
- リスク対応
- 脆弱性管理
- クラウドサービス管理
- インシデント管理
- 事業継続管理

3. 情報セキュリティ関連組織、法規、ガイドラインなど
- 情報セキュリティ関連組織
- 情報セキュリティ関連法規
- 情報セキュリティ関連規格、ガイドライン
- 情報セキュリティ関連制度、基準

4. 情報セキュリティにおける様々な脅威
- 脅威の分類
- 攻撃者の種類と動機
- 攻撃のプロセス
- 攻撃の準備
- 脅威例：マルウェア、標的型攻撃、DoS、AI を狙った攻撃など

5. 暗号技術と PKI
- CRYPTREC（クリプトレック）
- 共通鍵暗号、公開鍵暗号、ハイブリッド暗号方式
- デジタル署名
- ハッシュ関数とメッセージ認証
- PKI の概要、関連技術
- セキュアプロトコルと VPN

2 日目

6. アクセス管理と認証技術
- アクセス管理とは
- 認証方式

7. ネットワークセキュリティ
- 通信制御の例
- ファイアウォール、プロキシサーバ、IDS/IPS、WAF、UTM
- 検疫システム
- DLP、SIEM

8.Web セキュリティ
- HTTP 要求と HTTP 応答
- Web システムを狙った攻撃と対策例
- 開発ライフサイクルとセキュリティ

9. メール、DNS セキュリティ
- メールを狙った攻撃と対策例
- メールプロトコル関連セキュリティ
- DNS を狙った攻撃と対策例

10. 物理的、人的セキュリティ
- 物理的セキュリティ（防犯環境設計、障害や災害対策など）
- 人的セキュリティ（責務の明確化、クライアント PC のセキュリティなど）

- 情報セキュリティマネジメント試験の全範囲を取り上げているわけではありませんのでご注意ください
- 「情報セキュリティスペシャリストコース～『情報処理安全確保支援士試験シラバス追補版（午前 II）Ver.4.0』対応～」(P.12)、と内容が重複している部分が多々ありますので、同時受講検討の際はご注意ください

実施要項

開催日程	**2024** 年 **12** 月 **12** 日 (木) ～ **13** 日 (金)　締切 **11** 月 **28** 日 (木)
研修期間	2 日間　10:00 ～ 17:00
受講料	120,000 円（税込 132,000 円）/ 人
定員	30 名（最小催行人数 5 名）
会場	リモート Live　ツール：Zoom

講師　川島 慧　他

情報セキュリティスペシャリストコース NEW

～『情報処理安全確保支援士試験シラバス追補版（午前 II）Ver.4.0』対応～

国家試験「情報処理安全確保支援士」のシラバスに基づいた、情報セキュリティの専門知識や技術を深められるコースです。

受講の効果

- 特定業界や職種に偏ることなく、情報セキュリティの専門知識、技術を体系的に学ぶことができる
- 実務や教育経験豊富な講師から、情報セキュリティの実践的な考え方を身につけられる
- 情報処理安全確保支援士試験の合格に向けた知識を学ぶことができる

前提知識

- IT パスポート試験合格程度の知識（不安な方は「IT と情報セキュリティ初級コース～『IT パスポート試験シラバス Ver.6.3』対応～」（P10）の受講もご検討ください）

こんな方にお勧めです

■ 一般社員
■ IT 技術者（開発系）
■ CSIRT 要員（管理系）
■ 管理職
■ 情報システム・セキュリティ推進部門担当者
■ CSIRT 要員（技術系）
■ IT 技術者（インフラ系）
■ SOC（セキュリティ運用）要員
■ 監査担当

実施内容

1 日目

1. 情報セキュリティマネジメント（概要）
- 情報セキュリティの定義、要素
- 情報資産
- 脅威、脆弱性、リスクの概要
- ISMS の定義、関連規格、評価とレビュー
- 情報セキュリティポリシー
- 情報セキュリティマネジメント体制

2. 情報セキュリティマネジメント（実践）
- リスクマネジメントの流れ
- リスクアセスメント
- リスク対応
- 脆弱性管理
- クラウドサービス管理
- インシデント管理
- 事業継続管理

3. 情報セキュリティ関連組織、法規、ガイドラインなど
- 情報セキュリティ関連組織
- 情報セキュリティ関連法規
- 情報セキュリティ関連規格、ガイドライン
- 情報セキュリティ関連制度、基準

2 日目

4. 情報セキュリティにおける様々な脅威
- 脅威の分類
- 攻撃者の種類と動機
- 攻撃のプロセス
- 攻撃の準備
- 脅威例：マルウェア、標的型攻撃、DoS、AI を狙った攻撃など

5. 暗号技術と PKI
- CRYPTREC（クリプトレック）
- 共通鍵暗号、公開鍵暗号、ハイブリッド暗号方式
- デジタル署名
- ハッシュ関数とメッセージ認証
- PKI の概要、関連技術
- セキュアプロトコルと VPN

6. アクセス管理と認証技術
- アクセス管理とは
- 認証方式
- 認証、認可を実現する技術

7. ネットワークセキュリティ
- 通信制御の例
- ファイアウォール、NAPT
- プロキシサーバ、IDS/IPS、WAF、UTM
- パケットアナライザ
- サンドボックス、検疫システム、VDI
- ゼロトラスト

3 日目

8.Web セキュリティ
- HTTP 要求と HTTP 応答
- Web システムを狙った攻撃と対策例
- OWASP Top 10
- 開発ライフサイクルとセキュリティ
- システムの信頼性設計

9. メール、DNS セキュリティ
- メールを狙った攻撃
- メールプロトコル関連セキュリティ
- DNS を狙った攻撃
- DNS 関連セキュリティ

10. 物理的、人的セキュリティ
- 物理的セキュリティ（防犯環境設計、障害や災害対策など）
- 人的セキュリティ（責務の明確化、クライアント PC のセキュリティなど）

・情報処理安全確保支援士試験の全範囲を取り上げているわけではありませんのでご注意ください
・「情報セキュリティマネジメントコース～『情報セキュリティマネジメント試験シラバス Ver.4.0』対応～」（P.11）、と内容が重複している部分が多々ありますので、同時受講検討の際はご注意ください

実施要項

開催日程	**2024** 年 **12** 月 **3** 日（火）～ **5** 日（木） 締切 **11** 月 **19** 日（火） **2025** 年 **2** 月 **5** 日（水）～ **7** 日（金） 締切 **1** 月 **22** 日（水）
研修期間	3 日間　10:00 ～ 16:00
受講料	200,000 円（税込 220,000 円）/ 人
定員	30 名（最小催行人数 5 名）
会場	リモート Live　ツール：Zoom

講師　川島 慧　他

オープン＋個別＋ | ハンズオン | 座学 | 体験

Web セキュリティ設計実装講座

～ Web サイト開発で知っておきたいセキュリティ設計と実装の考慮～

巧妙化・複雑化するインターネットからの攻撃に備え、Web アプリケーションをより安全に設計、構築する必要があります。本コースでは、実際の Web サイト作成に役立つ、より実践的な設計、開発にまつわる内容と、最新の攻撃動向を踏まえて、脆弱性の自己点検の手法を習得することができます。

受講の効果

・Web サイト作成にあたって、必要なセキュリティの要件や、考え方を習得する
※コーディング方法などを学ぶ講座ではありません。

前提知識

・Web 開発・設計における基本知識

こんな方にお勧めです

■ 一般社員
■ 管理職
■ IT 技術者（インフラ系）
■ IT 技術者（開発系）
■ 情報システム・セキュリティ推進部門担当者
■ SOC（セキュリティ運用）要員
■ CSIRT 要員（管理系）
■ CSIRT 要員（技術系）
■ 監査担当

お客様の声

設計や実装の内容がメインだと思っていたが、要件定義で気を付けるべき点も含まれていたので、とてもためになりました。

実施内容

1. 要件定義フェーズでの考慮事項
・HTTPS による Web サイトの保護
・アーキテクチャの選択
・アクセス制御
・サイトデザインに関わる対策

2. 設計フェーズでの考慮事項
・全ての入力パラメータのチェック
・セッション対策
・暴露対策
・ログ管理方針
・エラーハンドリング
・コンテンツの不正利用
・リダイレクト処理

3. 実装フェーズでの考慮事項
・出力対策
 - SQL インジェクション
 - クロスサイトスクリプティング
 - OS コマンドインジェクション
 - ディレクトリトラバーサル
 - HTTP ヘッダインジェクション
 - メールヘッダインジェクション
・Web Storage/JSONP/JSON ハイジャック /XHR
・テキストデータの利用
 （JSON ファイル・XML ファイル）
・Cookie 利用
・データの暗号化

実施要項

開催日程	**2024** 年 **12** 月 **6** 日 (金) 締切 **11** 月 **22** 日 (金) **2025** 年 **3** 月 **7** 日 (金) 締切 **2** 月 **21** 日 (金)
研修期間	1 日間　10:00 ～ 17:30
受講料	140,000 円（154,000 円 税込）/ 人
定員	30 名（最少催行人数 5 名）
会場	リモート Live　ツール：Zoom

講師　藤本 博史　他

オープン ＋個別＋ | ハンズオン | 座学 | 体験

登録セキスペ 特定講習

情報セキュリティ事故対応 1 日コース 机上演習編

組織において情報セキュリティ事故が発生した際の対応方法を学ぶコースです。座学で事故対応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行い、事故対応を体験します。
お客様への謝罪のタイミング、サービスを止めるか否かなどのハンドリングを行う責任者の方、部門長の方におすすめです。

受講の効果

・インシデント対応を机上環境で体験できる
・インシデント対応体制の構築にあたり、必要な準備事項などを洗い出すきっかけを得られる
・被害者、顧客、警察など対外対応や、社員に対する対社内対応を経験し、具体策を検討できる
・インシデント対応演習を通して、事故防止を含めたリスクコントロールの方針を検討できる

前提知識

・なし

こんな方にお勧めです

■ 一般社員
■ 管理職
■ IT 技術者（インフラ系）
■ IT 技術者（開発系）
■ 情報システム・セキュリティ推進部門担当者
■ SOC（セキュリティ運用）要員
■ CSIRT 要員（管理系）
■ CSIRT 要員（技術系）
■ 監査担当

お客様の声

実際のインシデントを元に作成されたというシナリオがとてもリアルで、実践的な内容だと思いました。

実施内容

1. インシデントレスポンス座学
・インシデントレスポンスコース（知識編）
- セキュリティ対策のアプローチ
- 検知と対応
- 万が一に備えて
- インシデントレスポンスのフェーズとその目的
- 各フェーズの対応例
- インシデントレスポンス手順書
- ＣＳＩＲＴ
- 外部との連携のポイント
- イベントの検知
- 事実確認、事故の通知、ＣＳＩＲＴの招集
- 被害拡大の防止
- 原因と被害状況の調査
- 原因の排除と復旧
- 再発防止策の検討と振り返り
- インシデントレスポンス 対応のポイント

2. インシデントレスポンス机上訓練－訓練説明
・インシデント事故発生を想定した机上演習
- 訓練の進め方説明
- 仮想組織の概要説明

3. インシデントレスポンス机上訓練
・訓練実施
・振り返りディスカッション
・発表、まとめ

実施要項

開催日程	2024年11月12日(火)　締切 10月29日(火)	集合研修
	2025年 1月14日(火)　締切 2024年12月27日(金)	リモート Live
	2025年 3月21日(金)　締切 3月 7日(金)	集合研修
研修期間	1 日間　10:00 ～ 17:30	
受講料	120,000 円（132,000 円 税込）/ 人	
定員	21 名（最少催行人数 5 名）	
会場	（集合研修）ラック セミナールーム　（リモート Live）ツール：Zoom	

講師　大塚 英恵　他

登録セキスペ 特定講習

情報セキュリティ事故対応 2 日コース 実機演習編

組織において情報セキュリティ事故が発生した際の対応方法を学ぶコースです。
座学でラックの事故対応のノウハウを学習した後、ファイアウォールやサーバで構成された実機環境を使用し、実際に事故が起きた想定で演習を行います。お客様への謝罪のタイミング、サービスを止めるか否かなどのハンドリングを行う方はもちろん、サーバのログ調査を行うシステム担当者におすすめです。

受講の効果

・インシデント対応を実機環境で体験できる
・インシデント対応体制の構築にあたり、必要な準備事項などを洗い出すきっかけを得られる
・被害者、顧客、警察など対外対応や、社員に対する対社内対応を経験し、具体策を検討できる
・インシデント対応演習を通して、事故防止を含めたリスクコントロールの方針を検討できる

前提知識

・TCP/IP の基本的な知識
・Windows の基本的な操作
・Linux の基本的な知識とコマンド操作（※必須ではありません）
・F/W の基本的な操作（※必須ではありません）

こんな方にお勧めです

■ 一般社員
■ 管理職
■ IT 技術者（インフラ系）
■ IT 技術者（開発系）
■ 情報システム・セキュリティ推進部門担当者
■ SOC（セキュリティ運用）要員
■ CSIRT 要員（管理系）
■ CSIRT 要員（技術系）
■ 監査担当

お客様の声

実機を使用した、現場に近い内容でした。セキュリティに携わる者として技術だけではない心得も学べました。

実施内容

1 日目

1. インシデントレスポンス座学
・インシデントレスポンスコース（知識編）
- セキュリティ対策のアプローチ
- 検知と対応
- 万が一に備えて
- インシデントレスポンスのフェーズとその目的
- 各フェーズの対応例
- インシデントレスポンス手順書
- ＣＳＩＲＴ
- 外部との連携のポイント
- イベントの検知
- 事実確認、事故の通知、ＣＳＩＲＴの招集
- 被害拡大の防止
- 原因と被害状況の調査
- 原因の排除と復旧
- 再発防止策の検討と振り返り
- インシデントレスポンス対応のポイント

2. インシデントレスポンス実機訓練ー訓練説明
・インシデント事故発生を想定した机上演習
- 訓練の進め方説明
- 仮想組織の概要説明

3. インシデントレスポンス実機訓練（1 回目）
・訓練実施（1 回目）
・振り返りディスカッション
・発表、まとめ

2 日目

4. 情報セキュリティ最新動向
・情報セキュリティ最新動向
・情報セキュリティ事件簿
- 最近起きた事件・事故
・インターネットからの攻撃
- 設定の不備
- バッファオーバーフロー攻撃
- パスワードクラッキング
- SQL インジェクション
・イントラネットからの攻撃
- ウイルス感染の主な経路
- 標的型攻撃
- ウイルス感染対策

5. インシデントレスポンス実機訓練（2 回目）
・訓練実施（2 回目）
・振り返りディスカッション
・発表、まとめ

実施要項

開催日程	2024 年 10 月 17 日 (木) ～ 18 日 (金)　締切 10 月 3 日 (木)
	2024 年 12 月 9 日 (月) ～ 10 日 (火)　締切 11 月 25 日 (月)
	2025 年 1 月 23 日 (木) ～ 24 日 (金)　締切 1 月 9 日 (木)
	2025 年 3 月 13 日 (木) ～ 14 日 (金)　締切 2 月 27 日 (木)
研修期間	2 日間　10:00 ～ 17:30
受講料	180,000 円（198,000 円 税込）/ 人
定員	21 名（最少催行人数 5 名）
会場	集合研修 ラック セミナールーム

講師　富田 一成　他

攻撃手法解説コース

～脆弱性を狙う攻撃を実践し、防御のための知識と技術を身につける～

情報システムへの攻撃手法や攻撃による影響を理解し、組織におけるリスクや対策を検討することができます。
セキュリティ専門コースの基礎となるコースですので、専門コース受講前の土台としての受講をおすすめします。

受講の効果

・最近の攻撃傾向や基本的なセキュリティへの考え方を理解できる
・攻撃プロセスを把握できる（攻撃対象への情報収集、脆弱性情報の収集、対象システムへの攻撃）
・リスク評価、脆弱性への対策ができるようになる

前提知識

・ネットワークの基礎知識（TCP/IP など）
・Web サイトの通信の仕組み
・Windows の基本的な知識とコマンドを利用した操作
・Linux の基本的な知識とコマンドを利用した操作

こんな方にお勧めです

■ 一般社員
■ 管理職
■ IT 技術者（インフラ系）
■ IT 技術者（開発系）
■ SOC（セキュリティ運用）要員
■ CSIRT 要員（管理系）
■ CSIRT 要員（技術系）
■ 監査担当
■ 情報システム・セキュリティ推進部門担当者

お客様の声

防御だけでなく、実務経験に基づいた攻撃側の手法についても学べたので、とても勉強になりました。

実施内容

1 日目

1. サイバー攻撃のアプローチ
・サイバー攻撃のフローを MITRE ATT&CK ベースで解説

2. 情報収集
・OSINT
  - Google Hacking
  - Shodan の活用
・ポートスキャン
・ソーシャルエンジニアリング
  - フィッシング

3. プラットフォームを狙った攻撃
・DoS 攻撃
・パスワードクラッキング
・脆弱性の悪用
  - 任意コード実行
  - 権限昇格
・C2 による遠隔操作

2 日目

4.Web アプリケーションを狙った攻撃
・攻撃ツールの紹介
・脆弱性を利用した攻撃
  - SQL インジェクション
・脆弱性を利用した攻撃
  - クロスサイトスクリプティング
  - クロスサイトリクエストフォージェリ

5. マルウェアの脅威
・マルウェアの分類
・感染経路
・マルウェアの疑似感染ハンズオン

6. 攻撃に対する対策のアプローチ
・対策のプロセス

実施要項

開催日程	**2024**年**10**月 **7**日(月)～ **8**日(火) 締切 **9**月**24**日(火) ハイブリッド＊ **2024**年**12**月**19**日(木)～**20**日(金) 締切 **12**月 **5**日(木) ハイブリッド＊ **2025**年 **3**月 **4**日(火)～ **5**日(水) 締切 **2**月**18**日(火) ハイブリッド＊ ＊ハイブリッド（対面 or リモート Live）どちらかご選択ください。
研修期間	2 日間　10:00 ～ 17:30
受講料	195,000 円（214,500 円 税込）/ 人
定員	各 21 名（最少催行人数 5 名）
会場	（集合研修）ラック セミナールーム　（リモート Live）ツール：Zoom

講師　佐久間 泰地　他

攻撃手法原理詳解コース

～攻撃手法原理を知り、効果的な対策を考える～

情報システムへの代表的な攻撃手法の原理・仕組みを解説します。
各攻撃手法がどのような原理で成立するのかを知ることで、その影響度や対策方法を論理的に理解するコースです。

受講の効果

・代表的な攻撃手法の原理を理解できる
・各攻撃手法の影響度合いを把握することができる
・各攻撃手法の効率的な対策方法を論理的に考えられるようになる

前提知識

・Linux の基本的な知識とコマンドラインを利用した操作
・ネットワークの基本的な知識
・プログラミング経験があると望ましい

こんな方にお勧めです

■ 一般社員
■ 管理職
■ IT 技術者（インフラ系）
■ IT 技術者（開発系）
■ 情報システム・セキュリティ推進部門担当者
■ SOC（セキュリティ運用）要員
■ CSIRT 要員（管理系）
■ CSIRT 要員（技術系）
■ 監査担当

お客様の声

基礎知識の解説後、攻撃側の代表的な手法を、デモを交えて説明されたため、理解が深まりました。

実施内容

1 日目

1. ポートスキャン
・ポートスキャンとは
・ポートスキャンの種類とその違い
・ポートスキャンの対策
・攻撃デモ

2. パスワードクラッキング
・パスワードクラッキングとは
・パスワードクラッキングの種類
・UNIX/Linux のパスワードクラッキング
・Windows のパスワードクラッキング
・パスワードクラッキング対策
・攻撃デモ

3.DoS 攻撃
・DoS 攻撃とは
・DDoS 攻撃とは
・DoS 攻撃の種類
・DoS 攻撃の例と対策

4. 盗聴
・パケット盗聴とは
・スイッチング環境における盗聴
・盗聴の対策

5. マルウェア
・マルウェアとは
・マルウェアの種類
・標的型攻撃
・マルウェア対策
・攻撃デモ

2 日目

6. バッファオーバーフロー攻撃
・プロセス / メモリ / レジスタの知識
・バッファオーバーフロー攻撃とは
・バッファオーバーフロー攻撃の原理
・バッファオーバーフロー攻撃の対策
・攻撃デモ

7. フォーマットストリングバグ攻撃
・フォーマットストリングバグ攻撃とは
・フォーマットストリングバグ攻撃の原理
・フォーマットストリングバグ攻撃対策
・攻撃デモ

8.Web アプリの脆弱性
・Web アプリとは
・Web アプリの脆弱性の種類
・セッション管理
・セッションハイジャック

9. クロスサイトスクリプティング
・クロスサイトスクリプティングとは
・クロスサイトスクリプティングの原理
・クロスサイトスクリプティングの対策
・攻撃デモ

10.SQL インジェクション
・SQL インジェクションとは
・SQL インジェクションの原理
・SQL インジェクションの対策
・攻撃デモ

実施要項

開催日程	**2024** 年 **11** 月 **5** 日 (火) ～ **6** 日 (水) 締切 **10** 月 **22** 日 (火) **2025** 年 **2** 月 **3** 日 (月) ～ **4** 日 (火) 締切 **1** 月 **20** 日 (月)
研修期間	2 日間　10:00 ～ 17:30
会場	180,000 円（198,000 円 税込）/ 人
受講料	30 名（最少催行人数 5 名）
定員	リモート Live　ツール：Zoom

講師　白井 雄一郎　他

登録セキスペ 特定講習

セキュリティオペレーション実践コース 初級編

実際に JSOC のセキュリティアナリスト養成に使用されているカリキュラムから、ログや通信内容を確認する機会が多い HTTP 通信を題材に、攻撃の痕跡を発見・分析できるようなポイントをお伝えします。最終的には、Web サーバが攻撃通信によって受けた影響を自ら発見、判断できるよう、実践的な技術の習得を目指します。

受講の効果

- Web サーバのアクセスログの見方や通信ログ（パケットキャプチャ）の解析ツール「Wireshark」の基本的な使用方法を会得できる
- アクセスログや通信ログ（パケットキャプチャ）の解析を通じて、公開 Web サーバへの攻撃を発見したり、攻撃によるシステムへの影響の有無を判断するための技術を会得できる

前提知識

- 以下のような Web アプリに対する攻撃の基礎的な知識がある
  - SQL インジェクション
  - クロスサイトスクリプティング
  - /etc/Passwd 参照
- 検索エンジンを利用した情報収集経験があると望ましい

こんな方にお勧めです

- ■ 一般社員
- ■ 管理職
- ■ IT 技術者（インフラ系）
- ■ IT 技術者（開発系）
- ■ SOC（セキュリティ運用）要員
- ■ CSIRT 要員（管理系）
- ■ CSIRT 要員（技術系）
- ■ 監査担当
- ■ 情報システム・セキュリティ推進部門担当者

お客様の声

基本的なログの見方や Wireshark の実用的な部分などが、とても参考になりました。

実施内容

1. HTTP の基礎知識
・HTTP の通信がどのようにやり取りされているかを学習

2. Web サーバのアクセスログ
・ログに保存される内容、分析に必要な観点

3. Wireshark
・実際にツールを使用し、所望の通信内容を確認できる手法を学習

4. 攻撃通信解析
・Web アプリケーションに対する基本的な攻撃通信をアクセスログとパケットキャプチャから解析

5. 総合演習
・攻撃を発見、解析する手法を学ぶ演習

実施要項

開催日程	**2024** 年 **10** 月 **24** 日 (木)　締切 **10** 月 **10** 日 (木) **2024** 年 **12** 月 **5** 日 (木)　締切 **11** 月 **21** 日 (木) **2025** 年 **2** 月 **18** 日 (火)　締切 **2** 月 **4** 日 (火)
研修期間	1 日間　10:00 ～ 17:30
受講料	150,000 円（165,000 円 税込）/ 人
定員	21 名（最少催行人数 5 名）
会場	集合研修 ラック セミナールーム

講師　許斐 由佳梨　他

登録セキスペ 特定講習

セキュリティオペレーション実践コース 中級編

実際に JSOC のセキュリティアナリスト養成に使用されているカリキュラムを凝縮し、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習得していただきます。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することで、PSOC や CSIRT などで技術を担当する方が実環境に応用可能で実践的な技術の習得を目指します。

受講の効果

- アクセスログなどの通信ログの解析を通じて、不正な通信の発見やシステムへの影響の有無を判断するためのスキルを習得できる。
- 実際の重大インシデントを想定したシナリオを通じて、インシデント発生時の検出から防御までのサイクルを実践するためのスキルを習得できる。
  ※ 題材は日本最大級のセキュリティオペレーションセンター「JSOC」で検知した実際のインシデントから選定。

前提知識

- Linux の基本的な知識とコマンドラインを利用した操作
- ネットワークの基本的な知識と、Wireshark の基本的な操作
- TeraTerm、putty などの Windows 用 SSH クライアントを利用した SSH 接続
- 基本的な HTTP 通信の仕組みを理解していること
- 検索エンジンを利用した情報収集経験があると望ましい

こんな方にお勧めです

- ■ 一般社員
- ■ 管理職
- ■ IT 技術者（インフラ系）
- ■ IT 技術者（開発系）
- ■ SOC（セキュリティ運用）要員
- ■ CSIRT 要員（管理系）
- ■ CSIRT 要員（技術系）
- ■ 監査担当
- ■ 情報システム・セキュリティ推進部門担当者

お客様の声

実際に攻撃をしたのは貴重な経験でした。また攻撃の痕跡を検出し、判断するポイントを学べた事はためになりました。

実施内容

1 日目

1. Web サーバログ解析
・Web サーバのログから不審性の観点を学習

2. IDS/IPS による通信の解析
・シグネチャ作成の手法を習得

3. IDS/IPS の特性
・IDS/IPS による対応範囲の学習

4. インバウンド通信解析
・外部から内部への通信に関する解析技術を習得

2 日目

5. アウトバウンド通信解析
・内部から外部への通信に関する解析技術の習得

6. Proxy サーバログ解析
・Proxy サーバのログから不審性の観点を学習

7. 脆弱性検証
・Metasploit Framework を用いた脆弱性検証手法を習得

8. 総合演習
・検証、分析、検出の一連の流れを確認

3 日目

＜追加課題オプション＞

9. 演習
・演習
・演習の解答

実施要項

開催日程	2024年11月13日(水)～14日(木)　15日(金) はオプション　締切 10月30日(水) 2025年 1月20日(月)～21日(火)　22日(水) はオプション　締切 1月 6日(月) 2025年 3月10日(月)～11日(火)　12日(水) はオプション　締切 2月25日(火)
研修期間	2 日間（追加課題オプション付きの場合は 3 日間）　10:00 ～ 17:30
受講料	2 日コース 250,000 円（275,000 円 税込）/ 人 3 日コース 300,000 円（330,000 円 税込）/ 人
定員	21 名（最少催行人数 5 名）
会場	集合研修 ラック セミナールーム

講師　村松 慶太郎　他

登録セキスペ 特定講習

プラットフォーム脆弱性診断ハンズオンコース

本コースでは、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、実機演習を通して各脆弱性の診断手法を体験できます。診断業務について理解したい方、診断の内製化を検討している方にお勧めです。

受講の効果

- 各種脆弱性の原理・対策・診断手法を習得することができる
- 診断を内製化する上でのポイントを知ることができる
- 外部の診断ベンダーを選定する力が身につく
- 外部の診断ベンダーの報告書の内容が理解できるようになる

前提知識

- ネットワークの基礎知識（TCP/IP、OSI 参照モデルなど）
- Web アプリケーションの基礎知識 (Web サーバ、Web アプリケーションなど)
- Linux の基本的な知識とコマンドを利用した操作
- Windows の基本的な知識とコマンドを利用した操作

こんな方にお勧めです

- ■ 一般社員
- ■ 管理職
- ■ IT 技術者（インフラ系）
- ■ IT 技術者（開発系）
- ■ SOC（セキュリティ運用）要員
- ■ CSIRT 要員（管理系）
- ■ CSIRT 要員（技術系）
- ■ 監査担当
- ■ 情報システム・セキュリティ推進部門担当者

お客様の声

知識だけでなく、実機を通して具体的な脆弱性の検出方法やツールの使用方法について学べたので、とても勉強になりました。

実施内容

1. プラットフォーム診断概要
- 脆弱性診断とは
- プラットフォーム診断とは
- 脆弱性診断の実施計画立案

2. ログの取得
- ログの取得方法
- パケットキャプチャ

3. 情報収集
- OSINT
- ポートスキャンとサービスの列挙
- Web コンテンツの列挙

4. 脆弱性スキャン
- ツールを用いた脆弱性スキャン
- 脆弱性スキャンツールの機能

5. 代表的な脆弱性の診断
- コマンドインジェクション
- 危殆化した暗号アルゴリズム

6. パスワードクラッキング

7. 報告書と対策
- 報告書の作成
- 対策の実施

8. 総合演習

実施要項

開催日程	**2024** 年 **11** 月 **25** 日 (月) 締切 **11** 月 **11** 日 (月)　ハイブリッド *
	2025 年　**2** 月 **10** 日 (月) 締切　**1** 月 **27** 日 (月)　ハイブリッド *
	* ハイブリッド（対面 or リモート Live）どちらかご選択ください。
研修期間	1 日間　10:00 ～ 17:30
受講料	150,000 円（165,000 円 税込）/ 人
定員	各 21 名（最少催行人数 5 名）
会場	（集合研修）ラック セミナールーム　（リモート Live）ツール：Zoom

講師　小松 奈央　他

登録セキスペ 特定講習

Web アプリケーション脆弱性診断ハンズオンコース

本コースでは、プラットフォーム診断および 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体験できます。診断業務について理解したい方、診断の内製化に向けて、まず診断手法を学びたい方にお勧めです。

受講の効果

- 各種脆弱性の原理・対策・診断手法を習得することができる
- 診断を内製化する上でのポイントを知ることができる
- 外部の診断ベンダーを選定する力が身につく
- 外部の診断ベンダーの報告書の内容が理解できるようになる

前提知識

- ネットワークの基礎知識（TCP/IP、OSI 参照モデルなど）
- Web アプリケーションの基礎知識（Web サーバ、Web アプリケーションなど）
- Linux の基本的な知識とコマンドを利用した操作
- Windows の基本的な知識とコマンドを利用した操作

こんな方にお勧めです

- ■ 一般社員
- ■ 管理職
- ■ IT 技術者（インフラ系）
- ■ IT 技術者（開発系）
- ■ 情報システム・セキュリティ推進部門担当者
- ■ SOC（セキュリティ運用）要員
- ■ CSIRT 要員（管理系）
- ■ CSIRT 要員（技術系）
- ■ 監査担当

お客様の声

テキストにない、実体験を例題に、解説してくれたので、より理解が深まりました。

実施内容

1 日目

1. Web アプリケーション診断概要
- Web アプリケーション診断とは
- 診断ツール (Burp Suite) の紹介
- HTTP リクエストとレスポンス
- セッション管理
- データベースと SQL

2. Web アプリケーション診断のフロー
- 基本的な診断のフロー
- ヒアリングシートの項目例と解説
- 診断対象画面の選定方法
- 工数見積もりの手法
- その他、よくある注意事項

3. 手動診断の手法
- SQL インジェクション
- クロスサイトスクリプティング
- クロスサイトリクエストフォージェリ

2 日目

3. 手動診断の手法
- パラメータ改ざん・権限昇格
- 強制ブラウジング
- HTTPS の cookie に secure 属性の指定なし
- その他の脆弱性

4. 自動診断の手法
- 診断ツール (OWASP ZAP) の紹介
- 自動診断と誤報精査の手法
- 手動診断と自動診断の違い

5. 対策の検討
- 診断結果レポートの活用方法
- リスクレベルの検討
- 対策の考え方

6. 総合演習
- やられ役サイトに対する脆弱性診断
- 脆弱性の解説

実施要項

開催日程	**2024** 年 **12** 月 **17** 日 (火) ～ **18** 日 (水)　締切 **12** 月 **3** 日 (火)　ハイブリッド *
	2025 年 **2** 月 **12** 日 (水) ～ **13** 日 (木)　締切 **1** 月 **29** 日 (水)　ハイブリッド *
	* ハイブリッド（対面 or リモート Live）どちらかご選択ください。
研修期間	2 日間　10:00 ～ 17:30
受講料	195,000 円（214,500 円 税込）/ 人
定員	各 21 名（最少催行人数 5 名）
会場	（集合研修）ラック セミナールーム　（リモート Live）ツール：Zoom

講師　山本 翔馬　他

登録セキスペ 特定講習

デジタル・フォレンジックコース

～侵害調査の基礎訓練～

標的型攻撃 (※ 1) などにおける攻撃者の侵害手口は、近年ますます高度化しています。
この為、従来の " ウイルス対策ソフトによるフルスキャン " といった対応手順では、攻撃者が設置した遠隔操作マルウェア（リモートコントロールツール※ 2) などを発見できない事案が増加傾向にあります。
また、攻撃者の侵害スピードが速いことから、侵害が疑われる事象を検知した際には、迅速に事象の把握、被害範囲の特定、封じ込めの実施といった初動対応が重要になります。
本コースでは、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で必要となる基礎的な調査手法を演習形式で体験できます。通信ログや侵害された環境のシステムファイル（レジストリ、イベントログなど）を対象に、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学びます。
（対象は Windows 環境となります）

※ 1 APT：Advanced Persistent Threat
※ 2 RAT：Remote Access Trojan/Remote Administration Tool

受講の効果

- プロキシログから、マルウェアによる不正通信を発見し、影響範囲の確認などができるようになる
- Windows のシステム内に設置されているマルウェアを発見し、被害状況、影響範囲の確認ができるようになる
- 代表的な攻撃手口であるリモートプログラム実行の仕組みを理解し、横展開の痕跡の確認ができるようになる
- 削除ファイルの復元方法を学び、インシデント対応の幅を広げられるようになる

前提知識

- マルウェアの基本的な動作に関する知識
- 標的型攻撃で利用される一般的な侵害手口に関する知識（永続化、横展開、データの持ち出し）

※ 事前に「情報セキュリティ事故対応 1 日コース 机上演習編 (P14)」または「情報セキュリティ事故対応 2 日コース 実機演習編 (P15)」を受講されていると、より本コースの内容について理解が深まります。

こんな方にお勧めです

- ■ 一般社員
- ■ 管理職
- ■ IT 技術者（インフラ系）
- ■ IT 技術者（開発系）
- ■ 情報システム・セキュリティ推進部門担当者
- ■ SOC（セキュリティ運用）要員
- ■ CSIRT 要員（管理系）
- ■ CSIRT 要員（技術系）
- ■ 監査担当

お客様の声

- 専門的な内容のコースでしたが、実例を交えて解説して下さったので、とても分かりやすかったです。
- テキストが手順書のようになっていたので、復習にも活用できました。
- 訓練用データを使った演習形式になっていて、分からない所は補助講師の方が、丁寧に説明してくださったので、取り残されることなく学習できました。

実施要項

開催日程	2024年11月21日(木)～22日(金) 締切 11月7日(木)	ハイブリッド *
	2025年 1月 9日(木)～10日(金) 締切 2024年12月26日(木)	ハイブリッド *
	2025年 3月 6日(木)～ 7日(金) 締切 2月20日(木)	ハイブリッド *
研修期間	2 日間　10:00 ～ 17:30	
受講料	300,000 円（330,000 円 税込）/ 人	
定員	各 21 名（最少催行人数 5 名）	
会場	（集合研修）ラック セミナールーム　（リモート Live）ツール：Zoom	

* ハイブリッド（対面 or リモート Live）どちらかご選択ください。

講師　高松 啓　他

実施内容

1 日目

1. プロキシログ解析

・遠隔操作マルウェアと C2 サーバとの通信
・マルウェアによる通信の特徴
・プロキシログから C2 通信を発見する演習

【 目 的 】

侵害範囲を確認する為、プロキシログを調査します。
初動対応で必要な、影響範囲を特定するために、プロキシログ内から、遠隔操作マルウェアと C2 サーバ間の通信を発見し、侵害されている機器を特定します。
訓練用にカスタマイズされたプロキシログを利用し、演習形式で学びます。

2. マルウェアの手動探索

・マルウェアの特徴と自動起動の手口 (TTPs)
・マルウェアを発見する 3 つの観点
・自動起動に登録されたマルウェアを発見する演習

【 目 的 】

標的型攻撃では、侵害された機器に設置されている、ウイルス対策ソフトでは検知できない遠隔操作マルウェアが用いられているケースが散見されることから、手動でマルウェアを探し出す必要があります。
複数の訓練用データを利用し、ASEP（自動開始拡張ポイント）に登録されているマルウェアを手動で探す方法について、演習形式で学びます。

3. 認証情報窃取・横移動手口の把握

・認証情報窃取演習
・横移動手口の把握
・イベントログを利用した調査演習

【 目 的 】

標的型攻撃において、よく利用される攻撃手口である認証情報窃取・横移動について学びます。
研修環境を用いて認証情報窃取・横移動手口について把握、その後にイベントログを用いた実行痕跡の調査方法について、演習形式で学びます。

2 日目

4. プログラム実行痕跡調査

・プリフェッチファイルを利用した侵害確認
・プリフェッチファイルの可視化と調査
・侵害範囲調査演習

【 目 的 】

攻撃者によるプログラムの実行痕跡を調査し、横展開や情報漏洩などの影響について確認し、被害拡大防止に必要となる IOC 情報を収集します。
攻撃者が利用する代表的なプログラムの実行痕跡について、訓練用データを利用し、演習形式で学びます。

5. ファイルシステムのログ調査

・NTFS USN ジャーナルの可視化
・NTFS USN ジャーナルの調査方法

【 目 的 】

攻撃者が作成・変更、削除したファイルやフォルダの痕跡を、ファイルシステムのログから追跡する手法について、演習形式で学びます。

6. 削除データの調査

・NTFS ファイルシステムの基礎
・削除ファイルの状態遷移
・削除ファイルの復元手法「カービング」

【 目 的 】

NTFS ファイルシステムがファイルやフォルダを管理する仕組みを参照し、ファイルやフォルダが削除された場合の処理、削除ファイル（データ）の代表的な復元方法について演習形式で学びます。

オープン＋個別＋ | ハンズオン | 座学 | 体験

ペネトレーションテストハンズオンコース NEW

ペネトレーションテストを実施するにあたり必要となる知識およびスキルを学ぶコースです。実際にハンズオンを行うことで、様々な攻撃手法に関する理解を深められます。実施にあたって必要となる前提知識や周辺知識についても解説するため、ペネトレーションテストを企画・実施する方におすすめです。

受講の効果

- 標的型攻撃やランサムウェアが利用するサイバー攻撃手法について理解を深められる
- 学んだことを活用して情報システムのセキュリティレベルの向上に活かせる
- ペネトレーションテストを外注する際のベンダ選定や、技術者との円滑なコミュニケーション、テスト結果の報告書の理解に必要な知識が身につく

前提知識

- Windows の OS に関する基本的な知識（ローカルユーザ、レジストリなど）
- Windows のコマンド（PowerShell を含む）を利用した操作
- Linux のコマンドを利用した操作
- ネットワークの基礎知識（TCP/IP、OSI 参照モデルなど）
- Active Directory に関する基本的な知識（ドメインユーザ、ドメイン管理者など）

こんな方にお勧めです

■ 一般社員
■ 管理職
■ IT 技術者（インフラ系）
■ IT 技術者（開発系）
■ 情報システム・セキュリティ推進部門担当者
■ SOC（セキュリティ運用）要員
■ CSIRT 要員（管理系）
■ CSIRT 要員（技術系）
■ 監査担当

実施内容

1. ペネトレーションテスト概要
・ペネトレーションテストとは
・組織を狙う脅威
・攻撃シナリオの構築

2. ペネトレーションテスト実践演習
・ハンズオン環境の概要
・ハンズオンシナリオの概要
・ハンズオン
攻撃パターン①
- C2 通信の確立
- 端末およびドメイン情報の収集
- ローカル管理者権限昇格
- レジストリから認証情報の取得
- 他端末への横展開
- メモリから認証情報の取得

攻撃パターン②
- パスワードスプレー
- 重要ファイルの探索

攻撃パターン③
- Kerberos 認証を悪用した認証情報の取得
- オフラインパスワードクラッキング

・攻撃実施内容のまとめ

3. 報告書
・報告書の構成
・テストの実施概要
・テスト結果の概要
・脆弱性の詳細

4. 対策
・対策の考え方
・組織としてのセキュリティ対策

実施要項

開催日程	**2024** 年 **11** 月 **6** 日 (水) 締切 **10** 月 **23** 日 (水)
研修期間	1 日間 10:00 ～ 17:30
受講料	150,000 円（165,000 税込）/ 人
定員	21 名（最小催行人数 5 名）
会場	集合研修 ラック セミナールーム

講師　戸谷 洋介　他

登録セキスペ 特定講習

マルウェア解析ハンズオン入門コース

～表層解析・簡易動的解析～

本コースでは、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びます。基礎的な実行形式のマルウェアの解析手法について一から習得した後、解析担当者が実務としてよくある例を基に演習を行います。

受講の効果

・耐解析機能を含まない、簡単なマルウェアの解析ができるようになる
・exe ファイル以外のマルウェアの対応ができるようになる
※ 耐解析機能についても、本コースで紹介します。

前提知識

・情報処理推進機構 基本情報処理技術者試験合格程度の知識
・情報系大学、専門学校卒業程度の知識

こんな方にお勧めです

■ 一般社員
■ 管理職
■ IT 技術者（インフラ系）
■ IT 技術者（開発系）
■ 情報システム・セキュリティ推進部門担当者
■ SOC（セキュリティ運用）要員
■ CSIRT 要員（管理系）
■ CSIRT 要員（技術系）
■ 監査担当

お客様の声

マルウェアの様々なタイプのものの解析・環境構築手法など、広く浅く知ることができました。専門コースにも興味が出てきました。

実施内容

1 日目

1. マルウェアとは
・マルウェアとその解析に必要な知識
・昨今の標的型攻撃

2. マルウェア解析とポイント
・マルウェア解析の目標やポイント

3. マルウェア解析の流れ
・マルウェア解析の流れと収集すべき情報
・収集した情報の使用方法と使用目的

4. 解析環境の構築
・マルウェア解析するに当たって必要な環境を自ら準備するための手法

5. 表層解析
・ハッシュ値算出
・ファイルタイプ判定
・文字列情報抽出
・得られた情報からインターネットで検索し既知のマルウェアか否か確認

6. 簡易動的解析 .I
・マルウェアの挙動確認
　- プロセス、ファイル、レジストリ更新についての調査

7. 簡易動的解析 .II
・ネットワークに対するマルウェアの挙動確認
・通信目的を調査するための再解析

2 日目

8. ファイルレスマルウェアへの対応
・ファイルレスマルウェア概要
・ファイルレスマルウェアの解析例
　- リンクファイル解析
　- 演習

9. 文書型マルウェアへの対応
・文書ファイルのマルウェアの解析
　- 一般的な文書型マルウェアの動作
　- Office 製品を悪用したマルウェアと解析
　- その他の文書型マルウェアと解析例

10. その他のマルウェアへの対応方法やツールの紹介
・Web を介して感染するマルウェアに対する対応
　- 悪意のある JavaScript の解析とツール

11. 総合演習
・演習

12. 解析困難なマルウェアとその理由
・耐解析機能概要
・耐解析機能を見分けられる例

3 日目

＜追加課題オプション＞

13. 既存演習と新規演習の概要説明
・既知演習のファイルの場所などのまとめ
・新規演習の説明

14. 演習
・演習

15. 新規演習の解答
・新規演習の解説

16. 演習
・演習

実施要項

開催日程	**2024** 年 **12** 月 **11** 日 (水) ～ **12** 日 (木)　13 日 (金) はオプション　締切 **11** 月 **27** 日 (水) **2025** 年 **3** 月 **17** 日 (月) ～ **18** 日 (火)　19 日 (水) はオプション　締切 **3** 月 **3** 日 (月)
研修期間	2 日間（追加課題オプション付きの場合は 3 日間）10:00 ～ 17:30
受講料	2 日コース 300,000 円（330,000 円 税込）/ 人 3 日コース 350,000 円（385,000 円 税込）/ 人
定員	21 名（最少催行人数 5 名）
会場	集合研修 ラック セミナールーム

講師　金子 博一　他

登録セキスペ 特定講習

マルウェア解析ハンズオン専門コース

～動的解析・静的解析～

本コースでは、マルウェア解析ハンズオン入門コースの上位コースとして、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。マルウェアの持つ機械語命令を人が読み取れるものへと変換し、それらを用いて解析するホワイトボックス手法を取り扱い演習を行います。最終日には、入門・専門を通じて習得した各種技術を用いて、マルウェア解析の総合演習を行います。

受講の効果

- 耐解析機能を持つマルウェアの解析ができるようになる
- マルウェアの機能を論理的に理解できるようになる
- 膨大なアセンブラ命令から必要な情報を抽出し、見るべきポイントを抑える

こんな方にお勧めです

- ■ 一般社員
- ■ 管理職
- ■ IT 技術者（インフラ系）
- ■ IT 技術者（開発系）
- ■ 情報システム・セキュリティ推進部門担当者
- ■ SOC（セキュリティ運用）要員
- ■ CSIRT 要員（管理系）
- ■ CSIRT 要員（技術系）
- ■ 監査担当

お客様の声

アセンブラやアンパック、IDA は日本語で詳しく説明しているサイトが少ないため、この知識を得られたことは有意義でした。

前提知識

- 入門編の受講経験がある（以下経験があれば、必須ではありません）
  - マルウェアの表層解析を理解しており、実践可能
  - ProcessMonitor などの、デバッガ以外のツールを使った動的解析が可能
- 弊社オンラインコースの「マルウェア解析のためのアセンブラ入門」の受講経験がある（以下 x86 アセンブラについて大まかに理解していれば、必須ではありません。）
  - mov,lea,add,sub,and,xor,rep,jmp,call,retn などの代表的な命令を大よそ理解している
  - レジスタ及びフラグレジスタの大よその役割を理解している
  - サブルーチンの呼び出しと、その際のスタックの動作について理解している
  - 数行程度の簡単なコードであれば、まとめてどのような機能か理解し、説明することができる

※ 本コースではデバッガを駆使したマルウェア解析を行いますので、Immunity Debugger とその操作要項を理解しておくとよりスムーズに理解できるようになります。

※ 使い方については各ツールを公開するサイトのドキュメントや、以下のような書籍を参考にしてください。

- デバッガによる x86 プログラム解析入門 著者：Digital Travesia 管理人うさぴょん

※ アセンブラに全く触れたことがない方は、オンラインコースにて「マルウェア解析のためのアセンブラ入門」(P.48) を提供しております。

実施要項

開催日程	**2024** 年 **10** 月 **21** 日 (月) ～ **23** 日 (水)　締切 **10** 月 **7** 日 (月) **2025** 年 **1** 月 **15** 日 (水) ～ **17** 日 (金)　締切 **2024** 年 **12** 月 **27** 日 (金)
研修期間	3 日間　10:00 ～ 17:30
受講料	450,000 円（495,000 円 税込）/ 人
定員	21 名（最少催行人数 5 名）
会場	集合研修 ラック セミナールーム

講師　金子 博一　他

実施内容

1 日目

1. 耐解析機能と概要
- 対応すべき耐解析機能
- アセンブラとデバッガの知識の必要性

2. アセンブラ
- マルウェアの特徴を抑えるためのアセンブラの学習
  - 基本命令、データの取り扱い、スタック、フラグレジスタ、元のソースコードなど

3. デバッガとその使い方
- デバッガとその使い方
- 攻撃者の意図を特定

4. 耐解析機能の回避
- 耐解析機能の回避
- 耐解析機能として動作する関数やコードの発見、対応
- 耐解析機能書き換え手法

5. マニュアルアンパックと必要な知識
- マニュアルアンパック手法
  - PE ファイルフォーマット
  - メモリダンプ手法
  - 実践可能なツール

6. マニュアルアンパック実践
- マニュアルアンパックの実践

2 日目

7. 静的解析
- 静的解析とは
  - IDA Pro

8. 簡易静的解析
- デコンパイル可能なマルウェアの簡易動的解析
- 実在したマルウェアの解析
- 静的解析の考え方

9. IDA 入門
- IDA と使い方

10. IDA 実践
- IDA を使ったアセンブラの読み方
- よくある問題についての対応

11. 演習と時間短縮テクニック
- IDA を用いた特定マルウェアの特徴把握

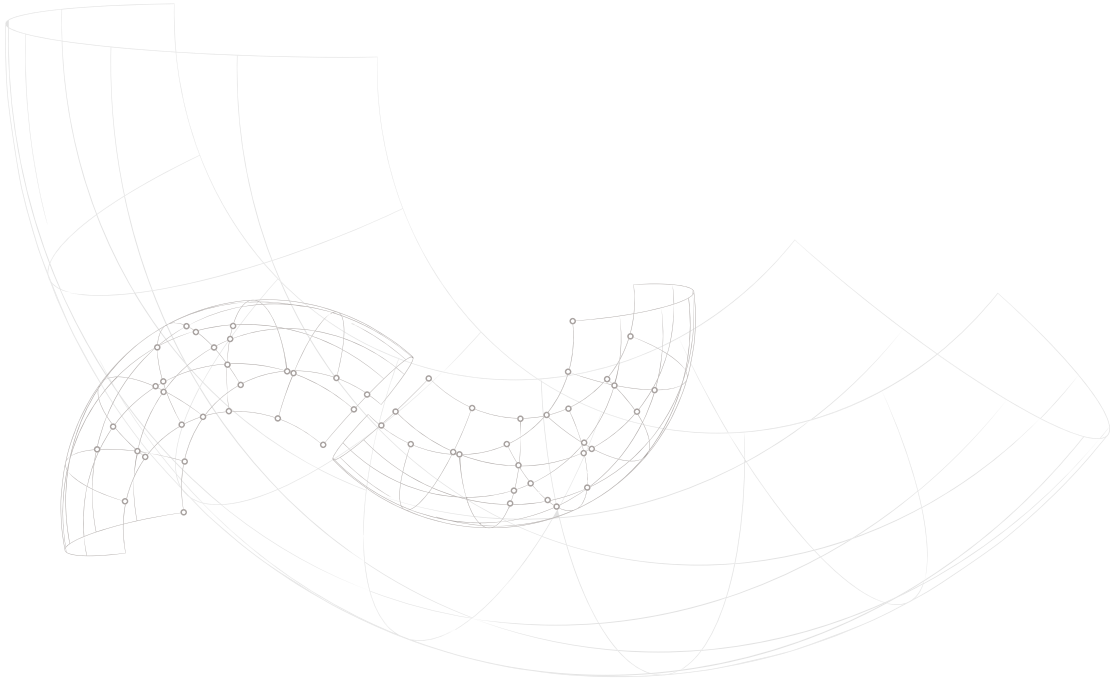
12. 演習 ①
- IDA を用いてアセンブラを読むべき場所の特定、推定

13. 演習 ②
- 難読化された箇所の特定と難読化解除ルーチンの推定、実践演習

3 日目

14. 総合演習 I
- 比較的簡単なマルウェアについての表層解析、動的解析、必要に応じて静的解析

15. 総合演習 II
- マルウェア解析



オープン ＋個別＋ | ハンズオン | 座学 | 体験

登録セキスペ 特定講習

マルウェア解析ハンズオン専門演習コース

～解析環境検知機能無効化と難読化解除実践～

本コースでは、マルウェア解析ハンズオン専門コースの上位コースです。
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演習主体のコースです。

受講の効果

- マルウェアの耐解析機能に対して、より具体的な対応手法を自ら考え対応できるようになる
- 最適なデバッガを取捨選択していく技能
- アセンブラを読み解く能力の向上
- マルウェアが使用するが入手できない関連ファイルに対して、コードから役割や内容を推定できる

前提知識

マルウェア解析専門コースを受講済みか、以下のような能力を有する方

- マルウェアの耐解析機能（パッキング、解析環境検知、難読化）の大まかな効果と対応の方針を理解している

※本講演ではデバッガを駆使したマルウェア解析を行いますので、Imminity Debugger、x32dbg とその操作要項を理解しておくとよりスムーズに理解できるようになります。

こんな方にお勧めです

- ■ 一般社員
- ■ 管理職
- ■ IT 技術者（インフラ系）
- ■ IT 技術者（開発系）
- ■ 情報システム・セキュリティ推進部門担当者
- ■ SOC（セキュリティ運用）要員
- ■ CSIRT 要員（管理系）
- ■ CSIRT 要員（技術系）
- ■ 監査担当

お客様の声

- 演習を基本としているので、技術が身についたと感じる。
- 本物のマルウェアを使用した演習なので、リアルで実践的に感じられた。
- 耐解析機能についてよく学ぶことができた。

実施内容

1 日目

1. 懐かしの銀行系マルウェア _1
- マニュアルアンパックの実践と解析環境検知機能を無効化、通信先を特定

2. ランサムウェアのイメージを掴む
- GUI ベースのランサムウェアを用いて、ランサムウェアの基本的な挙動について学びます。
- プロセスなどの確認、暗号化する拡張子を調査
  - マニュアルアンパック実践
  - IDA を用いた静的解析
  - 耐解析機能の確認
  - デバッガーを用いた解析環境検知機能の無効化
  - 調査するためのあたりの付け方
  - Wireshark などを用いた通信先の特定

3. 懐かしの銀行系マルウェア _2

4. 最近のランサムウエアを解析してみよう
- 前半の問題と比較し、耐解析機能の数が多く、応用の問題となります。
  - ツールを用いた挿入されたコードの確認
  - インジェクションされたプロセスへのアタッチ方法

2 日目

5. 難読化コードの理解と解除方法の考案、実践
- 難読化コードとその特徴
- 難読化の解除方法の立案
- 難読化の解除実践

6. 演習
- 前半の問題と比較し、耐解析の数が多く、応用の問題となります。
- 前半の内容に加えて以下のような内容が取り扱われます。
  - メモリを意識したデータの上書きとその結果の予測
  - マルウェアが外部ファイルを取り扱う場面において、その後の挙動からファイルの内容や役割を推測

実施要項

開催日程	**2024** 年 **11** 月 **18** 日 (月) ～ **19** 日 (火) 締切 **11** 月 **5** 日 (火) **2025** 年 **2** 月 **19** 日 (水) ～ **20** 日 (木) 締切 **2** 月 **5** 日 (水)
研修期間	2 日間　10:00 ～ 17:30
受講料	350,000 円（385,000 円 税込）/ 人
定員	21 名（最少催行人数 5 名）
会場	集合研修 ラック セミナールーム

講師　武田 貴寛　他

オープン＋個別＋ | ハンズオン | 座学 | 体験

スマホアプリセキュリティ対策講座

本コースは、スマートフォンアプリケーションのセキュリティ対策の知識を身につけるためのプログラムです。OWASP MASVS に沿ってセキュリティリスクとその軽減策を学習し、ハンズオン演習を通じて上流から対策することの重要性について学びます。

受講の効果

- セキュア開発のガイドラインを理解することができる
- 典型的な脆弱性の原理・対策方法を習得することができる
- 外部の診断ベンダーを選定する力が身につく
- 外部の診断ベンダーの報告書の内容が理解できるようになる

前提知識

- Android/iOS アプリケーションの基礎知識
- Web アプリケーションの基礎知識（HTTP 通信）
- Linux の基本的な知識とコマンドを利用した操作
- Windows の基本的な知識とコマンドを利用した操作

こんな方にお勧めです

- ■ 一般社員
- ■ 管理職
- ■ IT 技術者（インフラ系）
- ■ IT 技術者（開発系）
- ■ 情報システム・セキュリティ推進部門担当者
- ■ SOC（セキュリティ運用）要員
- ■ CSIRT 要員（管理系）
- ■ CSIRT 要員（技術系）
- ■ 監査担当

実施内容

1 日目

1. スマートフォンアプリケーションセキュリティの概要
- セキュリティリスクと脆弱性
- セキュリティ検証標準

2. ソフトウェア開発ライフサイクル
- 開発工程とセキュリティ活動
- MASVS 概説

3. アーキテクチャ、設計、脅威モデリング
- Android, iOS のセキュリティ特性
- 主要コンポーネント
- 個人情報保護と法規制

4. 技術要件解説
- データストレージとプライバシー
- 暗号化
- 認証とセッション管理

2 日目

5. 技術要件解説
- ネットワーク通信
- プラットフォーム連携

6. コード品質とビルド設定
- セキュアコーディングの原則
- よくあるセキュリティミス

7. 脆弱性診断サービスの実際
- テストプロセス
- 静的解析と動的解析

8. 脆弱性を作りこまないために
- 脆弱性の発生ポイント
- 設計ガイドライン
- 脆弱性診断のサイクルとベンダー選定

実施要項

開催日程	**2025** 年 **2** 月 **6** 日 (木) ～ **7** 日 (金)　締切 **1** 月 **23** 日 (木)　ハイブリッド * * ハイブリッド（対面 or リモート Live）どちらかご選択ください。
研修期間	2 日間　10:00 ～ 17:30
受講料	195,000 円（214,500 円 税込）/ 人
定員	各 21 名（最少催行人数 5 名）
会場	（集合研修）ラック セミナールーム　（リモート Live）ツール：Zoom

講師　荒井 文昭　他

オープン ＋個別＋ | ハンズオン | 座学 | 体験

OT セキュリティ入門 NEW

～製造現場における制御系システムのセキュリティ対策とインシデント対応を学ぶ～

本コースは、OT セキュリティ対策とインシデント発生時の対応方法を学ぶコースです。
産業用制御システムにまつわるセキュリティリスクと対策について事例を交えて学習した後、机上演習を通じてインシデント発生時の初動対応を体験します。

受講の効果

・制御システムに関する最新の脅威情報が分かる
・制御システムにおけるセキュリティの重要性を理解できる
・制御システムと情報システムとセキュリティ対策の違いを理解できる
・セキュリティインシデント発生時の初動対応力が向上する

前提知識

・なし

こんな方にお勧めです

■ 制御システムの運用に携わる現場担当者
■ システムエンジニアやネットワーク管理者
■ 制御システムのセキュリティ知識を向上させたい組織の従業員

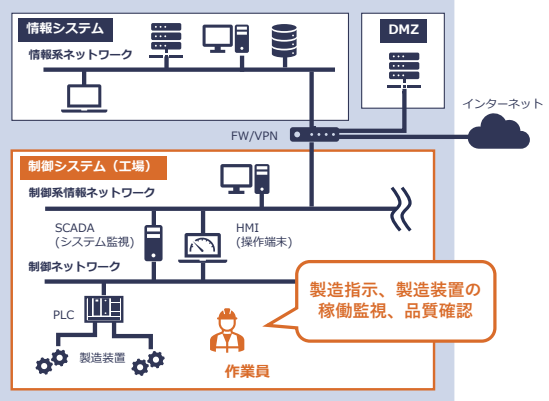
実施内容

1. セキュリティの基本概念
・サイバーセキュリティの基本的な定義や目的、セキュリティの重要性
・セキュリティの三要素、脅威と攻撃手法、基本原則

2. 制御システムのリスクと対策
・制御システムのセキュリティリスクと重要性
・制御システムのサイバーインシデント事例紹介
・制御システムと情報システムのセキュリティ対策の違い

3. インシデントレスポンス概論
・インシデントハンドリングの基本的な概念・定義
・インシデント対応の基本プロセス

4. セキュリティインシデント机上演習
・製造業の工場を題材とした初動対応（個人ワーク）
・演習の解説



実施要項

開催日程	**2024** 年 **11** 月 **20** 日（水） 締切 **11** 月 **6** 日（水）
研修期間	1 日間　14:00 ～ 17:00
会場	80,000 円（88,000 税込）/ 人
受講料	30 名（最小催行人数 5 名）
定員	リモート Live　ツール：Zoom

講師　荒井 文昭　他

個別 ハンズオン 座学 体験

セキュリティ競技入門コース

～ CTF（Capture The Flag）～

CTF（Capture The Flag）と呼ばれるセキュリティ技術を競う競技が世界各地で開催されています。CTF ではサーバやファイルに対して様々なアプローチを試して FLAG と呼ばれる答えを探します。クイズ形式で問題を解いて得点を重ねていく Jeopardy 形式を取っており、「FLAG を見つける」というゲーム感覚に近い演習形式で、セキュリティを学習することができます。単なる学習目的以外への利用にも十分な効果を上げています。

受講の効果

- ゲーム感覚で楽しみながら学ぶことで、自己学習のキッカケやノウハウ獲得が期待できる
- 実際に手を動かすことで、頭で理解していたことを整理し更なる技術力向上が期待できる
- 今まで視えなかったセキュリティ人材の発掘が期待できる
- 毎年 CTF を開催することで一つの目標に対してスキルアップを目指すことができるため、長期的な人材育成や技術者のコミュニティ活性化も期待できます

前提知識

- Web アプリケーションの基礎知識（Web サーバ、Web アプリケーションなど）
- Linux の基本的な知識とコマンドを利用した操作
- ネットワーク、OS などのコンピュータ基礎知識

※セキュリティの基礎知識あれば尚可

こんな企業にお勧めです

■自組織のエンジニアに、セキュリティの技術に興味を持ってもらいたい、理解を促進したい企業
■セキュリティ技術を有する潜在的な人材を可視化したい企業
■自組織で CTF を開催していたが、問題作成などの準備が大変なのでアウトソースしたい企業

お客様の声

問題はとっつきやすく、興味のわく問題が多かったため、初心者からするとゲーム感覚で楽しかったです。

提供形態・詳細

提供形態は大きくわけて 2 つあります。ご要望や用途をヒアリングし、最適な提供形態をご提案します。

1．講師派遣型の個別開催

ご指定の会場に講師を派遣し、CTF をオンサイトで実施します。
CTF の開催が初めての企業様にお勧めです。

【実施内容例】
- CTF 概要説明
- サンプル問題の紹介
- CTF 開催
- 一部問題の解決

受講料	お問い合わせください
研修期間	1 日間
定員	20 名 （10 名以上を推奨します。20 名以上の場合は、ご相談ください）
会場	貴社指定場所

2．CTF 環境の提供

CTF 開催に必要なスコアサーバと問題を一定期間ご提供します。
環境のみのご提供のため、よりリーズナブルに CTF を開催できます。
毎年 CTF を開催している企業様など、CTF 開催にかかる準備を軽減したい企業様にお勧めです。

ご提供価格	お問い合わせください
ご提供期間	5 週間程度

講師　藤原 真也　他

ハンズオン　座学　体験　オンライン

情報セキュリティ理解度チェック プレミアム（JNSA）

組織の社員・職員がそれぞれパソコンを１台使用し、メールを使っての連絡やインターネットを利用して情報を受発信することが業務の重要な手段となってきています。
そのような状況の中では、社員・職員１人ひとりが適切な情報セキュリティの知識を身につけて安全な利用を図ることは大変重要ですが、それとともに、組織の管理者が自組織の職員の情報セキュリティの理解度がどの程度であるかを把握することが大事です。理解度レベルに合わせて適切な教育を行い、組織全体の情報セキュリティを確保することは、管理者の重要な職責なのです。
この「情報セキュリティ理解度チェック」サイトでは、組織の管理者の方が自組織の社員・職員をユーザ登録し、受講させることで、１人ひとりの受講結果を知ることができます。また、自組織の全体としての情報セキュリティ知識レベルを確認できるだけでなく、さらに同業種の中でのランキングを知ることもでき、自組織の情報セキュリティ知識レベルの客観的な把握が可能になります。

受講の効果

・管理者がユーザーの受講結果を把握でき、同業種企業との比較などが行えます。

こんな企業にお勧めです

■ セキュリティ研修がマンネリ化している企業
■ 社員のセキュリティ知識レベルを客観的に把握したい企業
■ 継続教育を効果的・効率的に実施したい企業

実施内容

以下の分野問題にユーザーがオンラインで答えます。管理者はその受講結果を見て、セキュリティ管理に役立てることができます。

問題分野

1. 電子メールの知識と利用方法
2. ウイルスの知識と対処方法
3. インターネットの利用法と注意点
4. パスワードの知識と管理
5. PC の利用上の注意点
6. オフィスにおける情報セキュリティ
7. ルールや規則の遵守
8. 社外における情報セキュリティ

問題は左の 8 つのカテゴリーに分けられており、一回の受講で 10 ～ 25 問の問題が出題されます。
2 回目以降は、出題パターンも変わるため、繰り返しの受講で知識の底上げを行う事も可能になっています。
プレミアム機能で自社問題を追加することも可能です。

「情報セキュリティ理解度チェック」は、無償で利用できる機能と、「プレミアム版」と呼ばれる有償で利用できる機能を持っており、ラックを通じて購入可能です。
無償版であっても管理者はユーザーの受講結果を把握でき、同業種企業との比較などが行えますが、有償提供の「プレミアム版」では、さらに独自問題の追加や、管理者による出題問題の選択、受講者の回答内容などの確認ができるため、その後のセキュリティ教育をより具体的に実施できるようになります。

実施要項

受　講　料	30,000 円～（33,000 円 税込～）/ 年　＊登録ユーザ数によって変動します。

本コースは、JNSA 提供のサービスです。

ハンズオン　座学　体験

CISSP CBK トレーニング / 認定試験

セキュリティプロフェッショナル認定資格制度（CISSP）は、国際的に認定されている資格であり、この資格の保有者がセキュリティ共通知識分野（CBK）の 8 分野について、深い知識を有していることを証明するものです。戦略的かつ公平な判断のできるベンダーフリーの認定資格 CISSP により、セキュリティ専門家としてのスキルの裏付けを提供します。

受講の効果

・高度な専門知識と豊富な経験を実証できる
・セキュリティ専門家として信頼性が得られる

こんな方にお勧めです

■ 一般社員
■ 管理職
■ IT 技術者（インフラ系）
■ IT 技術者（開発系）
■ SOC（セキュリティ運用）要員
■ CSIRT 要員（管理系）
■ CSIRT 要員（技術系）
■ 監査担当
■ 情報システム・セキュリティ推進部門担当者

実施内容

1 日目
・情報セキュリティ環境
・情報資産のセキュリティ

2 日目
・アイデンティティとアクセスの管理
・セキュリティアーキテクチャとエンジニアリング

3 日目
・通信とネットワークセキュリティ
・ソフトウェア開発セキュリティ

4 日目
・セキュリティの評価とテスト
・セキュリティの運用

5 日目
・全チャプターのまとめ
・CISSP 資格に関する情報
Applied Scenario(応用シナリオ) の解説
まとめ・確認問題及び全体に関する質疑応答

CISSP 試験出題範囲

ドメイン	出題比率	ドメイン	出題比率
1. セキュリティとリスクマネジメント	16%	5. アイデンティティとアクセスの管理	13%
2. 資産のセキュリティ	10%	6. セキュリティの評価とテスト	12%
3. セキュリティアーキテクチャとエンジニアリング	13%	7. セキュリティの運用	13%
4. 通信とネットワークセキュリティ	13%	8. ソフトウェア開発セキュリティ	10%

実施要項

開催日程	早期締切	通常締切
2024 年 10 月 7 日 (月) ～ 11 日 (金)	8 月 22 日 (木)	9 月 13 日 (金)
2024 年 11 月 11 日 (月) ～ 13 日 (水) + 11 月 18 日 (月) ～ 19 日 (火)	9 月 26 日 (木)	10 月 18 日 (金)
2024 年 12 月 11 日 (水) ～ 13 日 (金) + 12 月 16 日 (月) ～ 17 日 (火)	10 月 25 日 (金)	11 月 19 日 (火)
2025 年 1 月 27 日 (月) ～ 31 日 (金)	12 月 12 日 (木)	1 月 3 日 (金)
2025 年 2 月 12 日 (水) ～ 14 日 (金) + 2 月 17 日 (月) ～ 18 日 (火)	1 月 3 日 (金)	1 月 21 日 (火)
2025 年 3 月 10 日 (月) ～ 14 日 (金)	1 月 23 日 (木)	2 月 14 日 (金)

研修期間	5 日間　9:30 ～ 18:30
受講料	早割 / 団体：400,000 円（税込　440,000 円）/ 人 通常：450,000 円（税込　495,000 円）/ 人 早期割引条件：セミナー初日の 45 日前にお申込が完了すること 団体割引条件：同月のセミナー開催に同企業から 3 名以上のお申込があること
試験費用	130,000 円（税込 143,000 円）
会場	リモート Live　ツール：Zoom
試験について	CAT（Computerized Adaptive Testing） ・お申し込み後バウチャー（受験チケット）をお渡ししますので、有効期限内に受験下さい。有効期限は納品時にお知らせしますが最大 1 年間です。 ・試験のみ受験の方は、(ISC)² もしくはピアソン VUE に直接お申し込みください。 ・試験会場は複数からお選びいただけます。詳しくはピアソン VUE の Web サイトにて確認ください。

本コースは (ISC)² 主催のセミナーです。

ハンズオン　座学　体験

情報セキュリティ内部監査人能力認定（JASA）準拠対策講座

本コースでは、情報セキュリティのための内部監査に必要な知識とプロセスを、情報セキュリティ監査制度に則った内容で、基礎から体系的に学習します。システムログ、権限・設定を見るのも内部監査人の大切な役割です。

受講の効果

・情報セキュリティ内部監査の体系的知識が身につく
・JASA「情報セキュリティ内部監査人能力認定」の資格取得を目指せる

こんな方にお勧めです

■ 一般社員
■ 管理職
■ IT 技術者（インフラ系）
■ IT 技術者（開発系）
■ 情報システム・セキュリティ推進部門担当者
■ SOC（セキュリティ運用）要員
■ CSIRT 要員（管理系）
■ CSIRT 要員（技術系）
■ 監査担当

実施内容

情報セキュリティ監査の基礎
・情報セキュリティマネジメントの確立・実装・運用及びマネジメントシステムにおける監査の役割

情報セキュリティ監査の実務
・各種監査基準を利用した監査手続きの習得

情報セキュリティ内部監査の実務手順
・監査計画、予備調査、監査の実務、意見形成、監査報告のプロセスを習得し、調書や報告書の作成
・監査の演習：テンプレートを用いた、ロールプレイによる監査体験

情報セキュリティ技術監査
・情報セキュリティ監査に関連する技術要素と技術監査方法など

情報セキュリティ演習
・情報セキュリティ監査に関連する技術要素と技術監査方法など

実施要項

開催日程	**2024**年**12**月**11**日（水）～**13**日（金）　締切 **11**月**27**日（水） **2025**年　**3**月　**3**日（月）～　**5**日（水）　締切　**2**月**17**日（水）
研修期間	3 日間　9:30 ～ 17:30
受講料	185,000 円（203,500 円 税込）/ 人
定員	20 名（最少催行人数 5 名）
会場	リモート Live　ツール：Zoom

本コースは JASA 認定校主催のセミナーです。

CompTIA

CompTIA 認定資格は、ベンダーニュートラルの認定資格としてワールドワイドで認知されている資格です。 IT 業務の設計・構築、保守・運用などの職務につかれている方々に広く活用されており、キャリアパスをスタートさせる上で欠かせないスキルを身に着けることができます。

試験名		教材		試験概要	対象者例
CASP+	①	ラボ	おすすめ	セキュリティ要件、リスク管理、インシデント対応、エンタープライズセキュリティでのスキルを網羅します。IT 管理者として 10 年、うちセキュリティ管理者として 5 年以上の実務スキルを評価します。	・サイバーセキュリティプロフェッショナル ・IS プロフェッショナル ・情報セキュリティアナリスト ・セキュリティアーキテクト
	②	試験バウチャー			
CySA+	③	ラボ		企業 / 組織のセキュリティに必要な脅威検出 / 分析のツールを使用、分析、監視するスキルを証明します。セキュリティ実務者としての 3 ～ 4 年の実務スキルを評価します。	・セキュリティアナリスト ・脆弱性アナリスト ・サイバーセキュリティスペシャリスト ・セキュリティエンジニア
	④	試験バウチャー			
PenTest+	⑤	ラボ		ネットワーク上の脆弱性を特定、報告、管理するための侵入テストに関わる実務家向けの資格です。侵入テストの手法、脆弱性評価、また攻撃から回復するために必要なスキルを評価します。	・ペネトレーションテスター ・ペネトレーションテストアナリスト ・ネットワークセキュリティ管理者 ・脆弱性評価アナリスト ・脆弱性評価マネージャ ・脆弱性管理エンジニア
	⑥	試験バウチャー			
Security+	⑦	ラボ		脅威や脆弱性の分析、ネットワーク設計、リスクマネジメントやアイデンティティ管理など、セキュリティ全般を網羅します。セキュリティ関連業務の 2 年程度の実務スキルを評価します。	・セキュリティスペシャリスト ・セキュリティコンサルタント ・セキュリティエンジニア ・セキュリティ管理者
	⑧	試験バウチャー			
Network+	⑨	ラボ		ネットワーク技術者が実務上共通して必須な、構成、運用、問題解決、セキュリティ、分析ツール、仮想化などのスキルを網羅します。ネットワーク関連業務の 9 ヶ月程度の実務スキルを評価します。	・ネットワークエンジニア ・ネットワーク管理者 ・フィールドエンジニア ・IS コンサルタント
	⑩	試験バウチャー			
Linux+	⑪	ラボ		ベンダーニュートラルの Linux 認定資格として、複数のディストリビューションを網羅します。Linux システムの設計・構築とセキュアな運用・保守に必要とされるスキルを評価します。	・Linux システム管理者 ・ネットワーク管理者 ・Web 管理者 ・テクニカルサポート
	⑫	試験バウチャー			
Server+	⑬	ラボ		サーバの構築、管理・運用において、サーバの役割や仕様、環境問題の特定、災害復旧や物理セキュリティ、ソフトウェアセキュリティの理解と実装、問題解決などのスキルを評価します。	・サーバ管理者 ・ストレージ管理者 ・サーバエンジニア
	⑭	試験バウチャー			
A+ core1	⑮	core1 試験バウチャー		IT 運用管理業務の 12 ヶ月程度の実務スキルを評価します。ハードウェア（PC やタブレット、モバイルなど）、OS（Windows、iOS や Android など）やソフトウェア、プリンターなどの周辺機器を取り上げます。CompTIA A+ を取得するためには、2 つの試験に合格する必要があります。	・テクニカルサポートエンジニア ・フィールドサポートエンジニア ・IT サポートエンジニア ・IT 管理者
A+ core2	⑯	core2 ラボ			
	⑰	core2 試験バウチャー			
Project+	⑱	試験バウチャー		小規模から中規模プロジェクトを遂行する上でのリーダーシップ、マネジメント、コミュニケーションなどについて、12 ヶ月のプロジェクトマネジメント経験に相当するスキルを評価します。	・プロジェクトマネージャ ・プロジェクトメンバー ・ビジネス企画 ・エンジニア
Cloud+	⑲	試験バウチャー		クラウドの運用や提供などに関わる IT エンジニアに必要な、セキュアなクラウド環境の実装と運用・管理、仮想化などの技術のスキルを評価する認定資格です。	・クラウドエンジニア ・クラウド管理者 ・システム管理者 ・ネットワークエンジニア ・ネットワーク管理者 ・データセンターエンジニア

上記表にない教材なども取り扱いがございます。
価格はお問い合わせください。

本コースは CompTIA 主催のコンテンツです。

CompTIA

お申込方法

お申し込みから受講までの流れ

お申し込み
Web・E-mail にてお申し込みください。

受付完了
受講票をメールでお送りします。

手続き開始
お申し込みいただいた内容に沿って、手続きを開始します。

請求書発行（前払い）
お申し込みから10日以内に請求書を郵送いたします。

ご受講

請求書発行（後払い）
研修終了後、請求書を郵送いたします。

※見積書、請求書、領収書、受講修了証など各種書類の発行も承っております。詳しくは事務局にお問合せください。
※代理店経由の場合は、お申込先の代理店にお問い合わせ下さい。

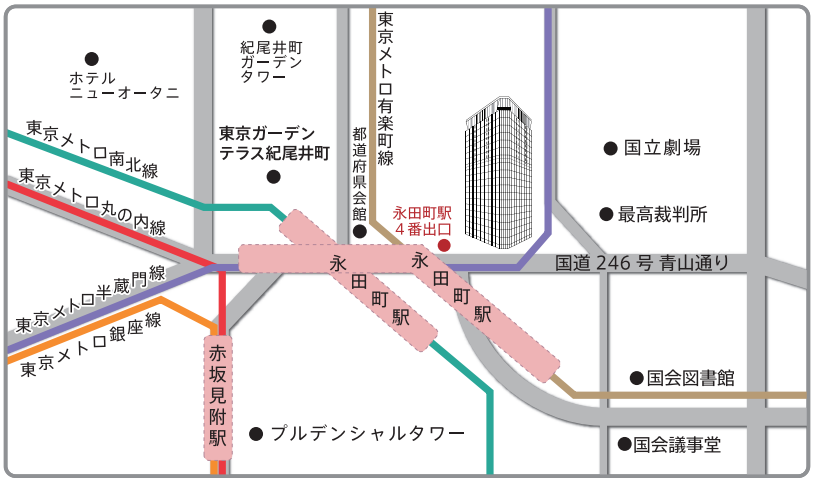
お申込先

https://www.lac.co.jp/service/education/

ラックセキュリティアカデミーまたは代理店各社
TEL　03-6757-0125　Email　info-academy@lac.co.jp

研修会場

株式会社ラック　セミナールーム 2F
〒 102-0093　東京都千代田区平河町 2-16-1 平河町森タワー



アクセス
東京メトロ 有楽町線・半蔵門線・南北線「永田町」駅 徒歩 1 分より 徒歩 1 分（4 番出口）

プログラム一覧（集合研修）

集 合 研 修

カテゴリ	ページ	コース名	研修形態	研修期間	価格 / 人（注 1）	開催有無決定期限（注 1）
スペシャリスト育成コース	10	IT と情報セキュリティ初級コース	座 学	2 日間	80,000 円 (88,000 円 税込)	開催日の 14 日前
	11	情報セキュリティマネジメントコース	座 学	2 日間	120,000 円 (132,000 円 税込)	開催日の 14 日前
	12	情報セキュリティスペシャリストコース	座 学	3 日間	200,000 円 (220,000 円 税込)	開催日の 14 日前
	13	Web セキュリティ設計実装講座	座 学	1 日間	140,000 円 (154,000 円 税込)	開催日の 14 日前
	14	情報セキュリティ事故対応 1 日コース 机上演習編	座 学 体 験	1 日間	120,000 円 (132,000 円 税込)	開催日の 14 日前
	15	情報セキュリティ事故対応 2 日コース 実機演習編	ハンズオン 体 験	2 日間	180,000 円 (198,000 円 税込)	開催日の 14 日前
	16	攻撃手法解説コース	ハンズオン	2 日間	195,000 円 (214,500 円 税込)	開催日の 14 日前
	17	攻撃手法原理詳解コース	座 学	2 日間	180,000 円 (198,000 円 税込)	開催日の 14 日前
	18	セキュリティオペレーション実践コース 初級編	ハンズオン	1 日間	150,000 円 (165,000 円 税込)	開催日の 14 日前
	19	セキュリティオペレーション実践コース 中級編	ハンズオン	2-3 日間	2 日コース 250,000 円 (275,000 円 税込) 3 日コース 300,000 円 (330,000 円 税込)	開催日の 14 日前
	20	プラットフォーム脆弱性診断ハンズオンコース	ハンズオン	1 日間	150,000 円 (165,000 円 税込)	開催日の 14 日前
	21	Web アプリケーション脆弱性診断ハンズオンコース	ハンズオン	2 日間	195,000 円 (214,500 円 税込)	開催日の 14 日前
	22	デジタル・フォレンジックコース	ハンズオン	2 日間	300,000 円 (330,000 円 税込)	開催日の 14 日前
	24	ペネトレーションテストハンズオンコース	ハンズオン	1 日間	150,000 円 (165,000 円 税込)	開催日の 14 日前
	25	マルウェア解析ハンズオン入門コース	ハンズオン	2-3 日間	2 日コース 300,000 円 (330,000 円 税込) 3 日コース 350,000 円 (385,000 円 税込)	開催日の 14 日前
	26	マルウェア解析ハンズオン専門コース	ハンズオン	3 日間	450,000 円 (495,000 円 税込)	開催日の 14 日前
	28	マルウェア解析ハンズオン専門演習コース	ハンズオン	2 日間	350,000 円 (385,000 円 税込)	開催日の 14 日前
	29	スマホアプリセキュリティ対策講座	ハンズオン	2 日間	195,000 円 (214,500 円 税込)	開催日の 14 日前
	30	OT セキュリティ入門	座 学	1 日間	80,000 円 (88,000 円 税込)	開催日の 14 日前
	31	セキュリティ競技入門コース	ハンズオン 体 験	1 日間	お問い合わせください	-
一般社員	32	情報セキュリティ理解度チェック　プレミアム（JNSA）	e ラーニング	—	30,000 円～ (33,000 円 税込～) / 年	-
資格取得支援	33	CISSP CBK トレーニング / 認定試験	座 学	5 日間	早割 / 団体 : 400,000 円 (440,000 円 税込) 通常 : 450,000 円 (495,000 円 税込) (注 2)	開催日の 7 日前
	34	情報セキュリティ内部監査人能力認定（JASA）準拠対策講座	座 学	3 日間	185,000 円 (203,500 円 税込)	開催日の 14 日前

(注 1) オープン開催時の条件です。
(注 2) 早期割引条件：セミナー初日の 45 日前にお申込が完了すること　　団体割引条件：同月のセミナー開催に同企業から 3 名以上のお申込があること

【集合研修 キャンセルポリシー】コースごとにキャンセルポリシーを設定しております。

コース・試験	日程変更可・キャンセル可	日程変更可・キャンセル不可	日程変更不可・キャンセル不可	備　考
CISSP CBK トレーニング (注 3)	セミナー初日から起算し 22 日前の 17 時まで	セミナー初日から起算し 21 日前～ 5 日前の 17 時まで	セミナー初日から起算し 5 日前の 17 時以降	日程変更、キャンセルには 1 回につき 14,300 円 (税込) の手数料がかかります。
上記以外のコース	コース初日から起算し 14 日前の 17 時まで	-	コース初日から起算し 14 日前の 17 時以降	コース初日から起算し 13 日～前日は受講者の変更のみ可能です。
認定試験（バウチャー）(注 4)	-	バウチャーの期限内に限り受講者自身がピアソン VUE にて日程変更可能です。変更費用は受講者が直接ピアソン VUE にお支払いいただきます。		

(注 3)　セミナー・試験の主催元：(ISC)2 Japan
(注 4)　試験運営元：ピアソン VUE（会社名：ナショナル・コンピュータ・システムズ・ジャパン）
・キャンセル及び日程変更は、期日までに必ずメールにてご連絡ください。
・期日を過ぎたキャンセル、日程変更は承れません。
・当日欠席された場合につきましても、受講料・受験料の全額を申し受けます旨ご了承ください。
・開催中止または日程・内容変更はセミナー初日の 14 日前までにメールにて通知します。

ラックセキュリティアカデミーオンライン

https://www.lac.co.jp/service/education/online.html

さぁ、セキュリティの知識を身に着けよう!

ラックセキュリティアカデミー オンラインは、インターネットを利用して、
いつでも、どこでも、何度でも受講できるオンデマンド配信型の学習サービスです。

オンラインコースの特長

**ラックの知見を活かした
セキュリティ研修を全方位でカバー**

各コースは集合研修でおなじみのラックの講師が講義・監修を担当。
「一般社員教育」から「スペシャリスト育成」まで幅広い層をオンラインでトレーニングできます。

**集合研修と同じように
実機演習で実践力アップ**

講義での学びに加え、クラウド上に用意された演習環境で実際に手を動かしながら学習できるコースや手元の PC で演習課題を解き進めるドリル形式のコースなど、実践的コースもご用意しています。

**あなたのペースに
あわせた学習を**

受講期間は全コースたっぷり 30 日間、スマートフォンやタブレットからも受講可能です。移動中やすきま時間も使いながら、あなたのペースでじっくり学習に取り組めます。

※ 30 日間以上のコースもあります。詳細はP.49 ～ 50 のオンライン研修一覧をご参照ください。

組織のセキュリティ教育に最適

全社研修など、複数人で受講される場合は、組織の管理者が受講状況を一括管理できるサービスがご利用いただけます。詳細はオプションサービス紹介ページ（https://www.lac.co.jp/service/education/online_option.html）をご確認ください。

幅広い受講者レベルに対応

6 段階の受講レベルで、一般社員から上級の情報セキュリティ関連技術者まで、幅広い受講者に対応するコースをご用意しています。

0	・一般社員・職員	
1	・IT 技術者（情報セキュリティ以外）	・部門のセキュリティ担当者
2	・まだ経験の浅い情報セキュリティ技術者 ・セキュリティ要素が必要になる IT 技術者	・部門のセキュリティ担当者 ・CSIRT などのインシデント対応チームへの参画者
3	・情報セキュリティ関連技術者＜中級者＞	・CSIRT などのインシデント対応チームの責任者
4	・情報セキュリティ関連技術者＜中～上級者＞	・CSIRT などのインシデント対応チームの責任者
5	・情報セキュリティ関連技術者＜上級者＞	・CSIRT などのインシデント対応チームの責任者

コースタイプは 4 種類

GEN

General e-Learning（GEN）
社会人向けの一般的なセキュリティ教育です。全社セキュリティ教育や新人教育などにご利用ください。

OLL

On Line Learning（OLL）
講師のレクチャーで進む e-ラーニングタイプです。講師による実機デモを交えたコースも多く、ウイルス感染やサイバー攻撃時の動きなど、レクチャーだけでは得られない疑似体験的な学習効果もあります。

OLT

On Line Training（OLT）
クラウド上に用意された演習環境内を手元の PC から実際に操作し、調査や解析などの演習に取り組みながら実践力を磨けるコースです。

DRL

DRL（Drill）
ドリル形式で、たくさんの演習問題にチャレンジしながら実践力を磨けるコースです。

ピックアップコース

Pick Up!

情報セキュリティリテラシー向上パック

基本の情報セキュリティ研修のほか、テーマ別の標的型攻撃メール対策編、テレワーク編、ウイルス感染デモ体験と、楽しく学べるアニメ形式のコースをまとめました。 すべての社員の情報セキュリティリテラシー向上におすすめのパックです。

■コースコード：PAC0001　■受講期間：90 日間
■受講料：18,000 円（19,800 円税込）

https://www.lac.co.jp/service/education/ola_literacy_packs.html

Pick Up!

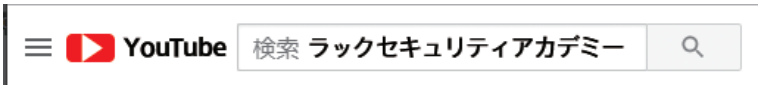
情報セキュリティマネジメントパックコース（前編＋後編）

国家試験である情報セキュリティマネジメント試験の午前シラバス（v3.1）を参考にし、日本における情報セキュリティの基礎を、網羅的に、効率よく得られるよう構成した、情報セキュリティの責任者、担当者、関係者になられた方におすすめのパックです。

■コースコード：PAC0040　■受講期間：90 日間
■受講料：39,000 円（42,900 円税込）

https://www.lac.co.jp/service/education/ola_management_packs.html

YouTube にて紹介動画を配信中です！



お申し込みから受講までの流れ

ラックセキュリティアカデミートップページにアクセス
https://www.lac.co.jp/service/education/

1. コース選択

ラックセキュリティアカデミートップページ（https://www.lac.co.jp/service/education/）から、受講したいコースを選択してください。

2. お申し込み

選択したコースの内容をご確認の上「お申し込み」ボタンをクリックしてください。ラックセキュリティアカデミーオンラインポータルサイト（以下、受講専用サイトという）のコース購入画面へ遷移します。

※外部リンク（アルー株式会社が提供する「etudes（エチュード）」）に遷移します。

・複数人・複数コース同時申込や後払い（法人のみ）をご希望の方は、選択したコースの「お申し込み」ボタンの下にある「複数受講または後払いを希望の方はこちら」から申込書類をダウンロードして必要事項を記入・捺印の上、ola-info@lac.co.jp までお送りください。
・後払いの場合は、申込書受領後、3 営業日を目安に受講案内メールをお送りします。受講案内メールをお送りした翌日からご受講できます。御請求書は、受講開始後、開始月の翌月第 2 営業日までに郵送します。

3. 購入手続き

購入方法は、クレジットカードによるお支払いか、銀行振込（前入金）のいずれかをお選びいただけます。
クレジットカードによるお支払いは【購入（クレジット）】、銀行振込（前入金）によるお支払いは【購入（クレジット以外）】をクリックしてください。

4. ログイン

「ユーザ ID」「パスワード」を入力してログインしてください。
＜初めてご利用の方＞
お申し込みには、新規会員登録をしていただく必要があります。
「新規会員登録がまだお済みでない場合はこちら」から、新規会員登録を行ってください。

5. お支払い（※ 2）

● クレジットカードによるお支払いは、受講専用サイトからクレジット決済画面に進み、お手続きください。
■ 前入金による銀行振込でのお支払いは、お申し込みから 5 営業日以内に請求書を発行します。請求書に記載の口座へ、入金締切日までにご入金ください。入金締切日は請求書発行日を起算として約 10 日後に設定します。

6. 受講開始

● クレジットカードによるお支払いは、カード決済完了後すぐにご受講できます。
■ 前入金によるお支払いは、入金締切日の翌日に弊社にて入金確認後、3 営業日を目安に受講案内メールをお送りします。受講案内メールをお送りした翌日からご受講できます。

新規会員登録の手順

1. 会員情報入力

「新規会員登録がまだお済みでない場合はこちら」から新規会員登録画面に進み、必要事項を記入してください。
記入が完了したら、「確認に進む」→「登録」をクリックしてください。

2. 新規ユーザ ID 登録

info@etudes.jp から「【ラックセキュリティアカデミーオンライン】新規ユーザ ID 登録のご案内」というメールをお送りします。メール本文の指示に従って会員登録手続きをしてください。

3. 初期パスワードの変更

会員登録が完了すると、info@etudes.jp から「【ラックセキュリティアカデミーオンライン】新規ユーザ ID 登録完了のご案内」というメールをお送りします。メール本文の指示に従い、受講専用サイトへアクセスして初期パスワードを任意のパスワードに変更してください。

4. 登録完了

受講専用サイトへログインできたことを確認したら、再度、コース購入画面へ進み、【購入（クレジット）】もしくは【購入（クレジット以外）】をクリックします。その後は、「5. お支払い（※ 2）」に戻り、申込手続きを進めてください。

ご質問・お問い合わせ

Email　ola-info@lac.co.jp
ラックセキュリティアカデミー オンラインコース専用窓口

General e-Learning（GEN）おすすめコース

一般社員向けコース｜情報セキュリティ基礎

コースコード GEN0050

おすすめ 情報セキュリティ講座【社員の意識編】

この講座では、最新のセキュリティ情報を交えながら、組織内個人として身につけるべき情報セキュリティについて学習します。さまざまなリスク・脅威から企業や組織、そして自分自身を守るために、組織における情報セキュリティルールをなぜ守らなければならないのかを理解することと、情報セキュリティルールに則り、業務を行えるようになることを目的とした講座です。
※ 2024 年 4 月 19 日にコース改訂を行いました。

受講の効果

- 情報セキュリティの正しい考え方を身につけることができる
- 業務を行う上で起こりがちな事故事例に対してどう対応すべきかを学ぶことができる

受講の前提知識

- 特になし

こんな方にお勧めです

- 全ての社員、職員
- 社員教育、セキュリティ教育を任されている担当者
- 組織のセキュリティ委員会や危機管理委員会、リスクマネジメント委員会などのメンバー

実施要項

受講料	110,000 円（税込）/50 名迄
お支払方法	銀行振込（前入金 or 後払い［後払いは法人のみ］のいずれか）
受講期間	30 日間
視聴時間	20 分

一般社員向けコース｜情報セキュリティ基礎

コースコード GEN0051

おすすめ 情報セキュリティ講座【サイバー攻撃編】

この講座では、最新のセキュリティ情報を交えながら、組織内個人として身につけるべき情報セキュリティについて学習します。さまざまなリスク・脅威から企業や組織、自分自身を守るために、組織を狙うサイバー攻撃の傾向や手口がどのようなものかを理解すること、情報セキュリティルールをなぜ守らなければならないのかを理解することを目的とした講座です。
※ 2024 年 4 月 19 日にコース改訂を行いました。

受講の効果

- 情報セキュリティ上の脅威とその対策についての知識が身に付く
- 情報セキュリティに関わる意識が向上する

受講の前提知識

- 特になし

こんな方にお勧めです

- 全ての社員、職員
- 社員教育、セキュリティ教育を任されている担当者
- 組織のセキュリティ委員会や危機管理委員会、リスクマネジメント委員会などのメンバー

実施要項

受講料	110,000 円（税込）/50 名迄
お支払方法	銀行振込（前入金 or 後払い［後払いは法人のみ］のいずれか）
受講期間	30 日間
視聴時間	20 分

一般社員向けコース｜情報セキュリティ基礎

コースコード GEN0030

おすすめ

情報セキュリティ研修【標的型攻撃メール対策編】

標的型攻撃とは何か、攻撃者はどのような手口を使って攻撃を仕掛けてくるのか、どのような対策をするべきかについて学習します。標的型攻撃では、組織内の個人も攻撃の対象となります。標的型攻撃から身を守るための知識を身につけ、社員・職員ひとりひとりの IT リテラシーを高めましょう。

受講の効果

・ 標的型攻撃の特徴や手口、対策についての知識を得られる

受講の前提知識

・ 特になし

こんな方にお勧めです

・ 一般社員、職員
・ セキュリティについてまずは学習を始めたい技術者
・ セキュリティ対策を任されている担当者
・ 組織のセキュリティ委員会や危機管理委員会、リスクマネジメント委員会などのメンバー

実施要項

受講料	110,000 円（税込）/50 名迄
お支払方法	銀行振込（前入金 or 後払い［後払いは法人のみ］のいずれか）
受講期間	30 日間
視聴時間	35 分

一般社員向けコース｜情報セキュリティ基礎

コースコード GEN1010

おすすめ

ロボタと挑戦!セキュリティチャレンジ【日常編】(1)

アニメ形式で日常に潜む脅威と対策をまなぶ。組織の情報をまもるために身に着けておきたいセキュリティ対策を 5 つのテーマから学習し、最後に理解度チェック（10 問）で理解度を確認します。 1 テーマ 10 分程度。テーマ毎に少しずつ取り組むこともできます。

受講の効果

・ システムだけではカバーしきれない、ひとりひとりが日常で意識して取り組む基本的なセキュリティ対策を学習できる
・ 日常起こり得るシーンを見ながらセキュリティ上の問題点を自ら考え、答えることで、対策の重要性を自分事として捉えることができる

受講の前提知識

・ 特になし

こんな方にお勧めです

・ 一般社員、職員

実施要項

受講料	110,000 円（税込）/50 名迄
お支払方法	銀行振込（前入金 or 後払い［後払いは法人のみ］のいずれか）
受講期間	30 日間
視聴時間	1 時間

一般社員向けコース ¦ 情報セキュリティ基礎

コースコード GEN0310

おすすめ

プラス・セキュリティ人材育成講座 セキュリティの基礎

DX とは、IT を活用して新しいビジネスやサービスを創出し、企業として成長していくための変革です。IT は日々進歩し、あらたなサービスが生まれています。それらを取り込んで、いち早く自組織のビジネスに活用することが、他社との優位性を図りながら DX を推進するアクセルになります。
一方で、IT にはまだ顕在化していないリスクや、機能を組み合わせることにより生まれるリスクが考えられます。そのため、危険を感じ取るセンサーや、しっかりと減速、一時停止できるブレーキとしてのセキュリティの考え方や、対策を実装しておく必要があります。
本講座では、DX 推進というアクセルに対して、安心して止まれるブレーキを実装する際に、セキュリティの専門家に要望を伝えるために必要な知識について学びます。

受講の効果

- セキュリティの必要性を知る
- セキュリティの基本的な用語を知る

こんな方にお勧めです

- 顧客向けの新規サービスを企画されている方
- IT を活用した事業を推進している担当者

受講の前提知識

- 特になし

実施要項

受講料	6,600 円（税込）/ 人
お支払方法	クレジットカードによるお支払いか、銀行振込（前入金 or 後払い [後払いは法人のみ]）のいずれかをご選択ください。
受講期間	90 日間
視聴時間	25 分

一般社員向けコース ¦ 情報セキュリティ基礎

コースコード GEN0080

NEW

サポート詐欺の実態

サポート詐欺は金銭だけでなく「情報」も標的となる可能性があり、企業における脅威の一つと言えます。 どのような詐欺であるかを知ることで自分自身が被害に遭う確率を下げられ、さらには情報共有することで同僚や家族などを守ることにもつながります。
この講座では、サポート詐欺を専門とするアナリスト監修のもと、サポート詐欺の基本を解説していきます。 実際のサポート詐欺のデモ動画を交えながら、組織内個人として身につけるべき対応策について学習しましょう。

受講の効果

- サポート詐欺の基本知識と対応策を知ることができる
- 実際のサポート詐欺の様子をデモ動画で知ることができる

こんな方にお勧めです

- 全ての社員、職員

受講の前提知識

- 特になし

実施要項

受講料	110,000 円（税込）/50 名迄
お支払方法	銀行振込（前入金 or 後払い [後払いは法人のみ] のいずれか）
受講期間	30 日間
視聴時間	10 分

オンライン研修　一般社員向けコース

GEN

General e-Learning（GEN）

社会人向けの一般的なセキュリティ教育です。
全社セキュリティ教育や新人教育などにご利用ください。

ロボタと挑戦！セキュリティチャレンジ【日常編】（1）

アニメ形式で日常に潜む脅威と対策をまなぶ。組織の情報をまもるために身に着けておきたいセキュリティ対策を 5 つのテーマから学習し、最後に理解度チェック（10 問）で理解度を確認します。 1 テーマ 10 分程度。テーマ毎に少しずつ取り組むこともできます。

■コースコード：GEN1010　■ Level 0　■受講期間：30 日間　■受講料：100,000 円（110,000 円 税込）

ロボタと挑戦！セキュリティチャレンジ【日常編】（2）

アニメ形式で、SNS やクラウドサービスなど、仕事とプライベートの境界が曖昧になりがちなセキュリティ対策を学習します。4 つのテーマから学習し、最後に理解度チェック（10 問）で理解度を確認します。 1 テーマ 10 分程度。テーマ毎に少しずつ取り組むこともできます。

■コースコード：GEN1011　■ Level 0　■受講期間：30 日間　■受講料：100,000 円（110,000 円 税込）

新入社員向け 情報セキュリティ研修

学生時代には気にしなくてよかったことも、社会人になると大きな事故につながる場合があります。本コースは、新入社員がついしてしまいがちな情報セキュリティ事故事例をもとに、脅威と対策を説明します。社会で活躍するためにまず必要な情報セキュリティ基礎知識を身に着けるためのコースです。

■コースコード：GEN0060　■ Level 0　■受講期間：30 日間　■受講料：100,000 円（110,000 円 税込）

情報セキュリティ講座【社員の意識編】NEW

ここの講座では、最新のセキュリティ情報を交えながら、組織内個人として身につけるべき情報セキュリティについて学習します。さまざまなリスク・脅威から企業や組織、そして自分自身を守るために、組織における情報セキュリティルールをなぜ守らなければならないのかを理解することと、情報セキュリティルールに則り、業務を行えるようになることを目的とした講座です。※ 2024 年 4 月 19 日にコース改訂を行いました。。

■コースコード：GEN0050　■ Level 0　■受講期間：30 日間　■受講料：100,000 円（110,000 円 税込）

情報セキュリティ講座【サイバー攻撃編】NEW

この講座では、最新のセキュリティ情報を交えながら、組織内個人として身につけるべき情報セキュリティについて学習します。さまざまなリスク・脅威から企業や組織、自分自身を守るために、組織を狙うサイバー攻撃の傾向や手口がどのようなものかを理解すること、情報セキュリティルールをなぜ守らなければならないのかを理解することを目的とした講座です。※ 2024 年 4 月 19 日にコース改訂を行いました。

■コースコード：GEN0051　■ Level 0　■受講期間：30 日間　■受講料：100,000 円（110,000 円 税込）

情報セキュリティ研修【標的型攻撃メール対策編】

標的型攻撃とは何か、攻撃者はどのような手口を使って攻撃を仕掛けてくるのか、どのような対策をするべきかについて学習します。標的型攻撃では、組織内の個人も攻撃の対象となります。標的型攻撃から身を守るための知識を身につけ、社員・職員ひとりひとりの IT リテラシーを高めましょう。

■コースコード：GEN0030　■ Level 0　■受講期間：30 日間　■受講料：100,000 円（110,000 円 税込）

サポート詐欺の実態 NEW

サポート詐欺は金銭だけでなく「情報」も標的となる可能性があり、企業における脅威の一つと言えます。 どのような詐欺であるかを知ることで自分自身が被害に遭う確率を下げられ、さらには情報共有することで同僚や家族などを守ることにもつながります。この講座では、サポート詐欺を専門とするアナリスト監修のもと、サポート詐欺の基本を解説していきます。 実際のサポート詐欺のデモ動画を交えながら、組織内個人として身につけるべき対応策について学習しましょう。

■コースコード：GEN0080　■ Level 0　■受講期間：30 日間　■受講料：100,000 円（110,000 円 税込）

情報セキュリティ研修【テレワーク編】

テレワーク環境におけるセキュリティリスクの認識を深め、そのリスク対策について分かりやすく解説しています。テレワークを導入しているが、利用者への教育が不十分という組織の方に最適なコースです。アニメ形式の動画と理解度テストで構成されています。1 テーマ 5 分程度のため、少しづつ取り組むことができます。

■コースコード：GEN1020　■ Level 0　■受講期間：30 日間　■受講料：100,000 円（110,000 円 税込）

オンライン研修　プラス・セキュリティ人材育講座

GEN
General e-Learning（GEN）
社会人向けの一般的なセキュリティ教育です。全社セキュリティ教育や新人教育などにご利用ください。

OLL
On Line Learning（OLL）
講師のレクチャーで進む e-ラーニングタイプです。講師による実機デモを交えたコースも多く、ウイルス感染やサイバー攻撃時の動きなど、レクチャーだけでは得られない疑似体験的な学習効果もあります。

プラス・セキュリティ人材育成講座 セキュリティの基礎
DX は IT を活用した企業変革で、進化する IT サービスを素早く導入し、新しいビジネスやサービスを生み出して企業成長を促進します。しかし、未知の IT リスクが潜むため、センサーやセキュリティ対策を導入し、DX 推進の際の安全なブレーキを確保します。この講座では、DX を進めつつ、セキュリティ知識を専門家に伝える手段を学びます。

■コースコード：GEN0310　■ Level 1　■受講期間：90 日間　■受講料：6,000 円（6,600 円 税込）

管理職向け 情報セキュリティ講座（1）
本コースは、組織運営のキーマンとなる管理職に対して、情報セキュリティを推進する上で管理職としてどのような役割が求められているのか、そして、その役割を担うために管理職として「知っておくべきこと」「やるべきこと」「やってはいけないこと」について情報セキュリティの観点から学習します。管理職に対して「情報セキュリティ推進の心構え」を醸成したいといった場合におすすめです。

■コースコード：GEN0210　■ Level 0　■受講期間：30 日間　■受講料：4,000 円（4,400 円 税込）

情報セキュリティマネジメントパックコース（前編）
国家試験である情報セキュリティマネジメント試験の午前シラバス（v3.1）を参考にし、日本における情報セキュリティの基礎を、網羅的に、効率よく得られるよう構成しています。前編では、情報セキュリティの基本概念から、リスクマネジメント、組織、関連法規などを取り扱います。

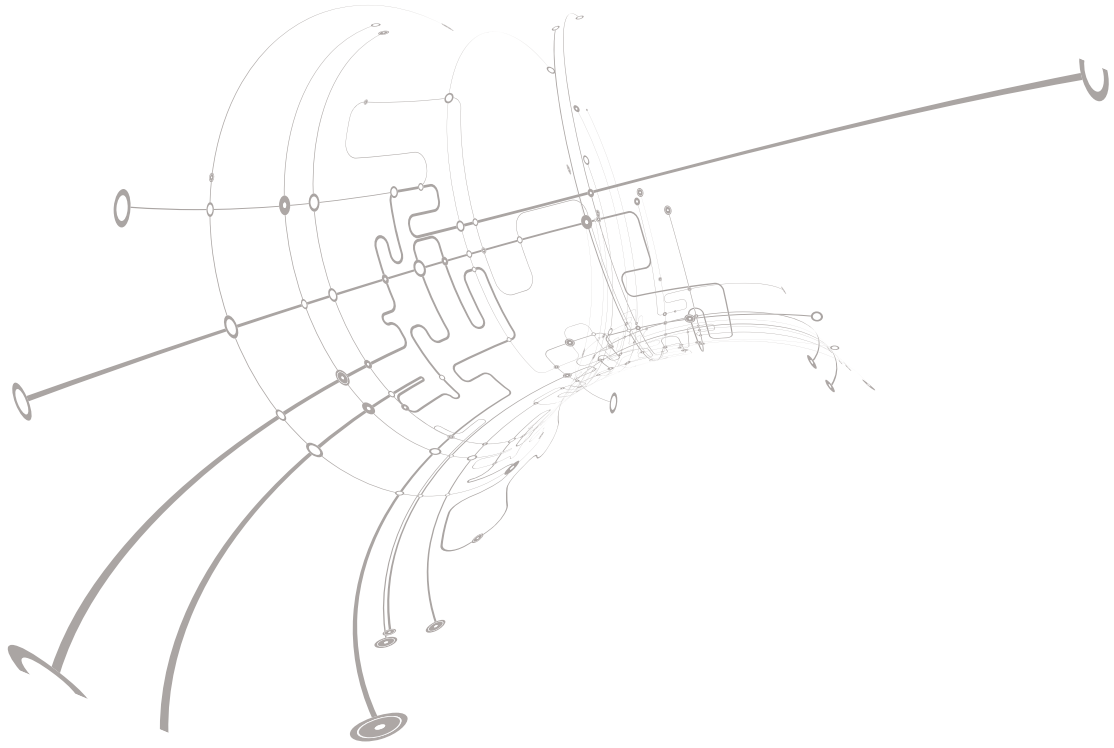
■コースコード：OLL0040　■ Level 2　■受講期間：30 日間　■受講料：19,000 円（20,900 円 税込）

情報セキュリティマネジメントパックコース（後編）
試験である情報セキュリティマネジメント試験の午前シラバス（v3.1）を参考にし、日本における情報セキュリティの基礎を、網羅的に、効率よく得られるよう構成しています。後編では、システム構成・運用から、暗号や認証、ネットワークと多層防御、攻撃手法などを取り扱います。

■コースコード：OLL0041　■ Level 2　■受講期間：30 日間　■ 29,000 円（31,900 円 税込）

ゼロから学ぶ情報セキュリティ基礎
情報セキュリティを学習する上で、何から始めてよいか分らない方、まずは全体像を掴みたい方におすすめです。基礎知識だけでなく、サイバー攻撃や内部犯行の手口とその対策、事故発生時の対応も学習できます。 また、サイバー攻撃をデモで“疑似体験”でき、理解を深められる構成となっています。

■コースコード：OLL0010　■ Level 1　■受講期間：30 日間　■受講料：9,500 円（10,450 円 税込）



OLL

On Line Learning（OLL）

講師のレクチャーで進む e-ラーニングタイプです。講師による実機デモを交えたコースも多く、ウイルス感染やサイバー攻撃時の動きなど、レクチャーだけでは得られない疑似体験的な学習効果もあります。

インシデントレスポンス概論

集合研修『情報セキュリティ事故対応 1 日コース 机上演習編』の座学部分をオンライン用にカスタマイズしたコースです。 組織で情報セキュリティ事故が発生した時に、組織の内外へのアプローチや原因の調査過程において、どのように行動をすべきかを体系的に学習します。

■コースコード：OLL0030　■ Level 2　■受講期間：30 日間　■受講料：4,000 円（4,400 円 税込）

攻撃手法を知る【入門編】

集合研修『攻撃手法解説コース』の内容をオンライン用にカスタマイズしたコースです。 デモを交えて攻撃手法を解説するので、実機操作に不慣れな方やマネジメント層でも攻撃手法とそのリスクに対して理解を深められる構成となっています。 セキュリティ専門分野に進む前の学習としてもおすすめです。

■コースコード：OLL0020　■ Level 2　■受講期間：30 日間　■受講料：19,000 円（20,900 円 税込）

Web サイト開発で知っておきたいセキュリティ設計と実装の考慮

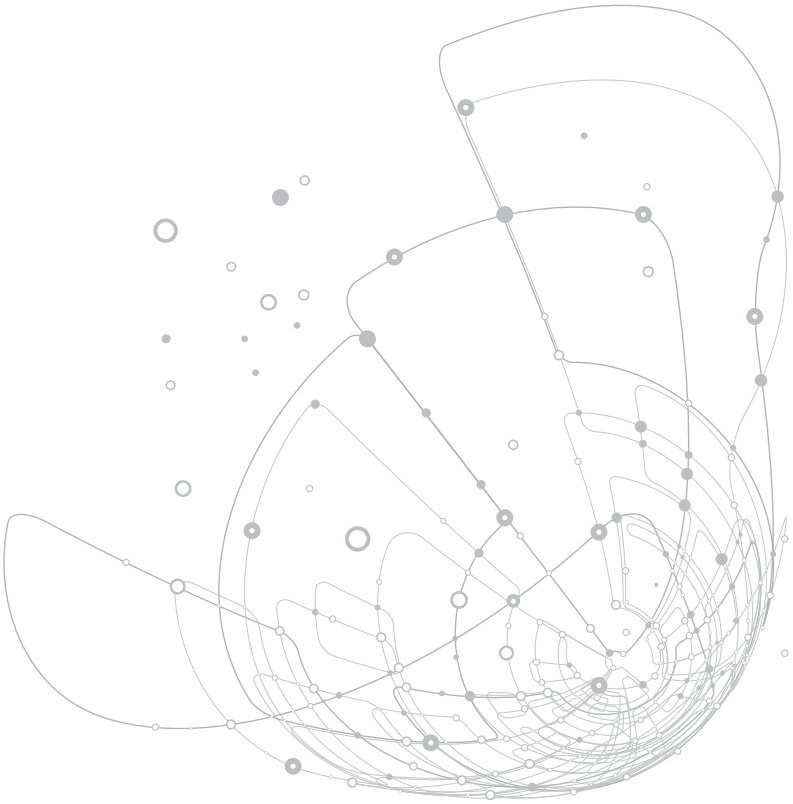
集合研修『Web セキュリティ設計実装講座』の内容をオンライン用にカスタマイズしたコースです。巧妙化・複雑化するインターネットからの攻撃に備え、Web アプリケーションをより安全に設計、構築する必要があります。実際の Web サイト作成に役立つ、より実践的な設計と実装の考慮点と、最新の攻撃動向を踏まえた脆弱性の自己点検の手法を知ることで、適切に脆弱性の対策を行い、Web アプリケーションを安全に保つことを目指します。

■コースコード：OLL0071　■ Level 3　■受講期間：90 日間　■受講料：100,000 円（110,000 円 税込）

改正個人情報保護法において求められるサイバーセキュリティ態勢

個人情報保護法は 3 年毎に見直しが行われることとなっており、令和 2 年、3 年に大きく改正されました。本コースはこれを解説するとともに、ビジネス・サービスを展開する上で知っておくべき、個人データの取扱い・管理・利用に関する基本的な知識や考慮すべきポイントについて理解することを目指します。

■コースコード：OLL0080　■ Level 2　■受講期間：90 日間　■受講料：20,000 円（22,000 円 税込）



オンライン研修　スペシャリスト育成コース

OLL

On Line Learning（OLL）

講師のレクチャーで進む e- ラーニングタイプです。講師による実機デモを交えたコースも多く、ウイルス感染やサイバー攻撃時の動きなど、レクチャーだけでは得られない疑似体験的な学習効果もあります。

インシデントレスポンス概論

集合研修『情報セキュリティ事故対応 1 日コース 机上演習編』の座学部分をオンライン用にカスタマイズしたコースです。 組織で情報セキュリティ事故が発生した時に、組織の内外へのアプローチや原因の調査過程において、どのように行動をすべきかを体系的に学習します。

■コースコード：OLL0030　■ Level 2　■受講期間：30 日間　■受講料：4,000 円（4,400 円 税込）

攻撃手法を知る【入門編】

集合研修『攻撃手法解説コース』の内容をオンライン用にカスタマイズしたコースです。 デモを交えて攻撃手法を解説するので、実機操作に不慣れな方やマネジメント層でも攻撃手法とそのリスクに対して理解を深められる構成となっています。 セキュリティ専門分野に進む前の学習としてもおすすめです。

■コースコード：OLL0020　■ Level 2　■受講期間：30 日間　■受講料：19,000 円（20,900 円 税込）

攻撃手法を知る【詳解編】～ポートスキャン～

本コースでは、攻撃の前段階として実行される「ポートスキャン」のメカニズムを学習します。 攻撃手法のメカニズムを理解することで、その攻撃手法の影響や対策方法を論理的に理解できるようになることを目指します。

■コースコード：OLL0101　■ Level 2　■受講期間：30 日間　■受講料：19,000 円（20,900 円 税込）

攻攻撃手法を知る【詳解編】～パスワードクラッキング～

本コースでは、他人のパスワードを見破る手法「パスワードクラッキング」のメカニズムを学習します。 攻撃手法のメカニズムを理解することで、その攻撃手法の影響や対策方法を論理的に理解できるようになることを目指します。

■コースコード：OLL0102　■ Level 2　■受講期間：30 日間　■受講料：19,000 円（20,900 円 税込）

脆弱性ハンドリング

自組織の環境で検出した脆弱性への対策を、円滑に推進するための脆弱性管理の考え方について、学習します。脆弱性管理とは何か、なぜ脆弱性管理が必要なのか、そして、脆弱性管理とはどのようなプロセスで行うのかを知ることで、適切に脆弱性を管理し、脆弱性を悪用したサイバー攻撃から組織やビジネスを保護できるようになることを目指します。

■コースコード：OLL0050　■ Level 2　■受講期間：30 日間　■受講料：29,000 円（31,900 円 税込）

ソーシャルエンジニアリング概論

ソーシャルエンジニアリングとは、人の心理・行動の隙を狙う「人の脆弱性」を狙った攻撃の総称です。国内外事例や手口などを紹介し、組織や個人でどのような対策をするべきかについて説明します。情報を扱う「人」がどのように狙われるのかを知ることで、セキュリティ意識を底上げすることを目指します。

■コースコード：OLL0060　■ Level 1　■受講期間：30 日間　■受講料：4,000 円（4,400 円 税込）

Web サイト開発で知っておきたいセキュリティ設計と実装の考慮

集合研修『Web セキュリティ設計実装講座』の内容をオンライン用にカスタマイズしたコースです。巧妙化・複雑化するインターネットからの攻撃に備え、Web アプリケーションをより安全に設計、構築する必要があります。実際の Web サイト作成に役立つ、より実践的な設計と実装の考慮点と、最新の攻撃動向を踏まえた脆弱性の自己点検の手法を知ることで、適切に脆弱性の対策を行い、Web アプリケーションを安全に保つことを目指します。

■コースコード：OLL0071　■ Level 3　■受講期間：90 日間　■受講料：100,000 円（110,000 円 税込）

OLT

On Line Training（OLT）

クラウド上に用意された演習環境内を手元の PC から実際に操作し、調査や解析などの演習に取り組みながら実践力を磨けるコースです。

DRL

DRL（Drill）

ドリル形式で、たくさんの演習問題にチャレンジしながら実践力を磨けるコースです。

セキュリティオペレーションコース

クラウド上に用意した演習環境を用いて学習するハンズオンコースです。 集合研修『セキュリティオペレーション実践コース中級編』の内容の一部をカスタマイズしました。 様々なログや通信から攻撃の痕跡を検出・判断するプロセスを、講師のデモを交えて学習し、演習にて自ら試行します。

■コースコード：OLT0010 ■ Level 4 ■受講期間：30 日間 ■受講料：100,000 円（110,000 円 税込）

Web アプリケーション診断コース

クラウド上に用意した演習環境を用いて学習するハンズオンコースです。 Web アプリケーション診断の実施に必要な知識やスキルを学びます。単なる知識の習得だけでなく、演習を通して各脆弱性の診断手法を体験できます。 診断業務について理解したい方、診断の内製化を検討している方にお勧めです。

■コースコード：OLT0020 ■ Level 3 ■受講期間：30 日間 ■受講料：68,000 円（74,800 円 税込）

プラットフォーム診断コース

クラウド上に用意した演習環境を用いて学習するハンズオンコースです。 プラットフォーム診断における知識の習得に加え、演習を通してプラットフォーム診断の手法を体験できます。 診断業務について理解したい方、診断の内製化を検討している方にお勧めです。

■コースコード：OLT0025 ■ Level 3 ■受講期間：30 日間 ■受講料：68,000 円（74,800 円 税込）

マルウェア解析 Basic1

クラウド上に用意した演習環境を用いて学習するハンズオンコースです。 集合研修『マルウェア解析ハンズオン入門コース基礎編』で学習する「表層解析」と「動的解析」の内容をベースとしたコースで、実行形式のマルウェアを使い、基礎的な解析手法を習得できます。

■コースコード：OLT0030 ■ Level 3 ■受講期間：30 日間 ■受講料：68,000 円（74,800 円 税込）

実践！インシデントレスポンス侵害調査演習 ～ Web サイト初動調査編～

クラウド上に用意した演習環境を用いて学習するハンズオンコースです。 集合研修『IR（インシデントレスポンス）ファースト』のオンライン版コースです。 ※報告書作成は含まれません。この演習は、攻撃を受けた Web サイトから攻撃の痕跡や悪用された脆弱性を調査し、侵害された原因や影響範囲を特定する実技を行います。 実技を通じてログから攻撃の痕跡を追跡する感覚を養い経験の蓄積を狙いとしています。

■コースコード：OLT0040 ■ Level 4 ■受講期間：30 日間 ■受講料：100,000 円（110,000 円 税込）

IR DF（インシデント・レスポンスデジタル・フォレンジック）演習ドリル

ご自分の PC 上で任意のツールを利用して解析を試すことができるハンズオンコースです。 Windows 環境で発生したマルウェアによるセキュリティ・インシデントにおいて、初動対応で必要となる基本的なデジタル・フォレンジック（DF）技術について演習形式で学習していきます。

■コースコード：DRL0010 ■ Level 3 ■受講期間：1 年間 ■受講料：95,000 円（104,500 円 税込）

マルウェア解析のためのアセンブラ入門

集合研修『マルウェア解析ハンズオン専門コース』を受講する際に必要な、マルウェアの特徴を押さえるためのアセンブラを学びます。ご自分の PC 上で指定のツールを利用して例題や演習を行うハンズオンコースです。例題と演習には詳細解説が付いています。また、コース前半部分ではアセンブラの概要も説明しています。集合研修の予習・復習としてだけではなく、アセンブラの入門学習としてもおすすめです。

■コースコード：DRL0030 ■ Level 3 ■受講期間：30 日間 ■受講料：50,000 円（55,000 円 税込）

マルウェア解析入門ドリル

4 つの演習を通して、マルウェア解析の『表層解析』と『動的解析』のスキルアップを目指した講座です。よく見られる解析パターンを知ることで、効率的に解析を行えるようになることを目指します。オンラインコース『マルウェア解析 Basic1』受講後の更なるスキルアップにもおすすめです。演習は事前に取得された表層解析と動的解析のログを、自身の PC 上でツールを用いて解析を行う形式で進めます。

■コースコード：DRL0040 ■ Level 3 ■受講期間：30 日間 ■受講料：68,000 円（74,800 円 税込）

プログラム一覧（オンライン研修）

オンライン研修

[目的別おまとめパック] おすすめの研修コースをひとつのパックにしました。専門別に効果的に学習できます。

コースタイプ	コースコード	レベル	コース名	価格 (税込)/ 人	視聴時間	受講期間	テストの有無
目的別おまとめパック							
GEN	PAC0001	1	**情報セキュリティリテラシー向上パック** **パックに含まれるコース** 情報セキュリティ研修【テレワーク編】 ロボタと挑戦！セキュリティチャレンジ【日常編】（1） ウイルス感染デモ体験 情報セキュリティ研修【標的型攻撃メール対策編】 情報セキュリティ講座【社員の意識編】 情報セキュリティ講座【サイバー攻撃編】 サポート詐欺の実態 インシデントレスポンス超初動の心得（1）	¥19,800	5 時間	90 日間	一部有
OLL	PAC0010	2	**インシデント初動対応 教育基本パック** **パックに含まれるコース** インシデントレスポンス概論 インシデントレスポンス超初動の心得（1） インシデントレスポンス超初動の心得（2） インシデントレスポンス超初動の心得（3） インシデントレスポンス超初動の心得（4） インシデントレスポンス超初動の心得（5）	¥17,600	9 時間	90 日間	無
OLL	PAC0020	2	**情報セキュリティ技術　入門パック** **パックに含まれるコース** ゼロから学ぶ情報セキュリティ基礎 攻撃手法を知る【入門編】 インシデントレスポンス概論 脆弱性ハンドリング ソーシャルエンジニアリング概論	¥55,000	11 時間	90 日間	一部有
OLL	PAC0040	2	**情報セキュリティマネジメントパックコース（前編＋後編）** **パックに含まれるコース** 情報セキュリティマネジメントパックコース（前編） 情報セキュリティマネジメントパックコース（後編）	¥42,900	7.5 時間	90 日間	有

プログラム一覧（オンライン研修）

オンライン研修

コースタイプ	コースコード	レベル	ページ	コース名	価格（税込）/ 人	視聴時間	受講期間	テストの有無
一般社員向けコース								
GEN	GEN1010	0	42	ロボタと挑戦！セキュリティチャレンジ【日常編】（1）	Web ページからご確認いただけます。 https://www.lac.co.jp/service/education/online.html	1 時間	30 日間	有
GEN	GEN1011	0	44	ロボタと挑戦！セキュリティチャレンジ【日常編】（2）		45 分	30 日間	有
GEN	GEN0060	0	44	新入社員向け 情報セキュリティ研修		40 分	30 日間	有
GEN	GEN0050	0	41	情報セキュリティ講座【社員の意識編】		20 分	30 日間	有
GEN	GEN0030	0	42	情報セキュリティ研修【標的型攻撃メール対策編】		35 分	30 日間	有
GEN	GEN1020	0	44	情報セキュリティ研修【テレワーク編】		40 分	30 日間	有
GEN	GEN0051	0	41	情報セキュリティ講座【サイバー攻撃編】		20 分	30 日間	有
GEN	GEN0080	0	43	サポート詐欺の実態		10 分	30 日間	有
プラス・セキュリティ人材育成コース								
GEN	GEN0310	1	43	プラス・セキュリティ人材育成講座 セキュリティの基礎	¥6,600	25 分	90 日間	有
GEN	GEN0210	0	45	管理職向け 情報セキュリティ講座（1）	¥4,400	25 分	30 日間	有
OLL	OLL0040	2	45	情報セキュリティマネジメントパックコース（前編）	¥20,900	3 時間	30 日間	有
OLL	OLL0041	2	45	情報セキュリティマネジメントパックコース（後編）	¥31,900	4.5 時間	30 日間	有
OLL	OLL0010	1	45	ゼロから学ぶ情報セキュリティ基礎	¥10,450	3 時間	30 日間	有
OLL	OLL0030	2	47	インシデントレスポンス概論	¥4,400	2 時間	30 日間	無
OLL	OLL0020	2	47	攻撃手法を知る【入門編】	¥20,900	4 時間	30 日間	有
OLL	OLL0071	3	47	Web サイト開発で知っておきたいセキュリティ設計と実装の考慮	¥110,000	3 時間	90 日間	有
OLL	OLL0080	2	46	改正個人情報保護法において求められるサイバーセキュリティ態勢	¥22,000	1 時間	90 日間	有
スペシャリスト育成コース								
OLL	OLL0030	2	47	インシデントレスポンス概論	¥4,400	2 時間	30 日間	無
OLL	OLL0020	2	47	攻撃手法を知る【入門編】	¥20,900	4 時間	30 日間	有
OLL	OLL0101	2	47	攻撃手法を知る【詳解編】～ポートスキャン～	¥20,900	2 時間	30 日間	有
OLL	OLL0102	2	47	攻撃手法を知る【詳解編】～パスワードクラッキング～	¥20,900	2.5 時間	30 日間	有
OLL	OLL0050	2	47	脆弱性ハンドリング	¥31,900	45 分	30 日間	有
OLL	OLL0060	1	47	ソーシャルエンジニアリング概論	¥4,400	1 時間	30 日間	無
OLL	OLL0071	3	47	Web サイト開発で知っておきたいセキュリティ設計と実装の考慮	¥110,000	3 時間	90 日間	有
OLT	OLT0010	4	48	セキュリティオペレーションコース	¥110,000	5 時間	30 日間	無
OLT	OLT0020	3	48	Web アプリケーション診断コース	¥74,800	5 時間	30 日間	無
OLT	OLT0025	3	48	プラットフォーム診断コース	¥74,800	3.5 時間	30 日間	無
OLT	OLT0030	3	48	マルウェア解析 Basic1	¥74,800	5.5 時間	30 日間	無
OLT	OLT0040	3	48	実践！インシデントレスポンス侵害調査演習～ Web サイト初動調査編～	¥110,000	2.5 時間	30 日間	無
DRL	DRL0010	3	48	IR DF（インシデント・レスポンス デジタル・フォレンジック）演習ドリル	¥104,500	4 時間	1 年間	無
DRL	DRL0030	3	48	マルウェア解析のためのアセンブラ入門	¥55,000	3.5 時間	30 日間	無
DRL	DRL0040	3	48	マルウェア解析入門ドリル	¥74,800	1 時間	30 日間	無

コースタイプ GEN General e-Learning　OLL On Line Learning　OLT On Line Training　DRL Drill

【オンライン研修 キャンセルポリシー】

コースの全部または一部を配信することが可能になった以後は解約することはできませんのでご注意ください。
詳しくは弊社 Web ページ (https://www.lac.co.jp/service/education/online_flow.html) に記載している利用規約、特定商取引法による表示をご覧ください。

標的型攻撃メールによる脅威をゼロに近づける

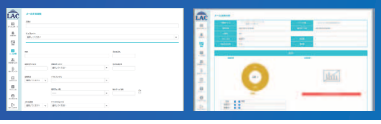
標的型攻撃メール訓練 T3 with セキュリティ教育

標的型攻撃メール訓練 T3 with セキュリティ教育とは

本サービスは、従業員に向けて疑似攻撃メールを配信する実践型訓練と、訓練学習前後のフォローアップとなるｅラーニング研修を組み合わせた情報セキュリティ意識向上プラットフォームです。
契約期間中は「訓練」と「教育」を、**いつでも何度でも利用可能です。**

標的型攻撃メール訓練 T3

配信システムにて、疑似攻撃メール配信・開封結果の確認、開封率の他社比較やより詳細な結果が分かる簡易報告書のダウンロードが可能です。



数多くの訓練メール配信テンプレート
一般的～最新の傾向・トレンドまで網羅。
５人に１人が開くリアリティに富んだモノも！

初めてでも安心・かんたん！
作業マニュアルに沿って設定を進めるだけ。
契約前に無償トライアルでも確認可能！

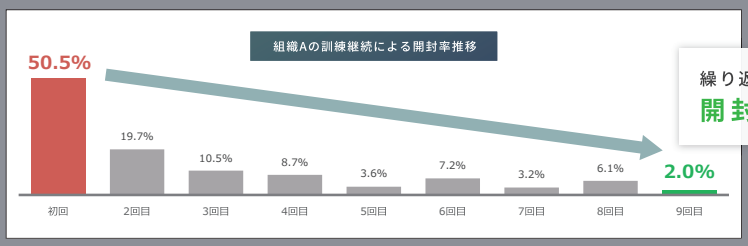
セキュリティ教育（eラーニング）

標的型攻撃メール訓練の前後にフォローアップとして、ｅラーニングを受講いただけます。

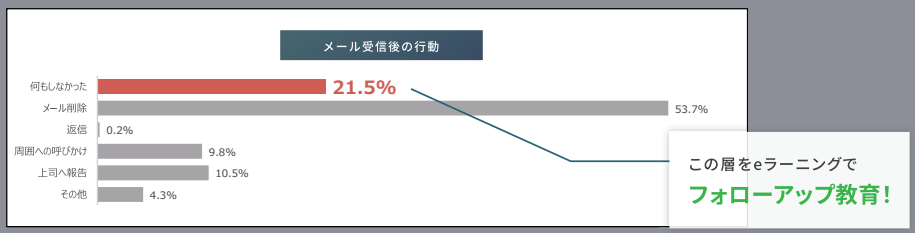
基礎知識から、最新の傾向まで学べる
基礎知識は勿論、最新のサイバー攻撃についても学べます。定期的に新作講座も追加予定。

短時間の動画と確認テストでスピード学習！
要点を絞った短時間の動画コンテンツに加え、確認テストによる理解度の確認も可能。

標的型攻撃メール訓練は、繰り返し実践することで効果があります



訓練のあと、何もしなかった層がリスク！



好きな時に、何度でも

追加料金なしで
何回でも訓練可能！
全教育講座も見放題

始めやすい価格

１人あたり
月額50円～300円

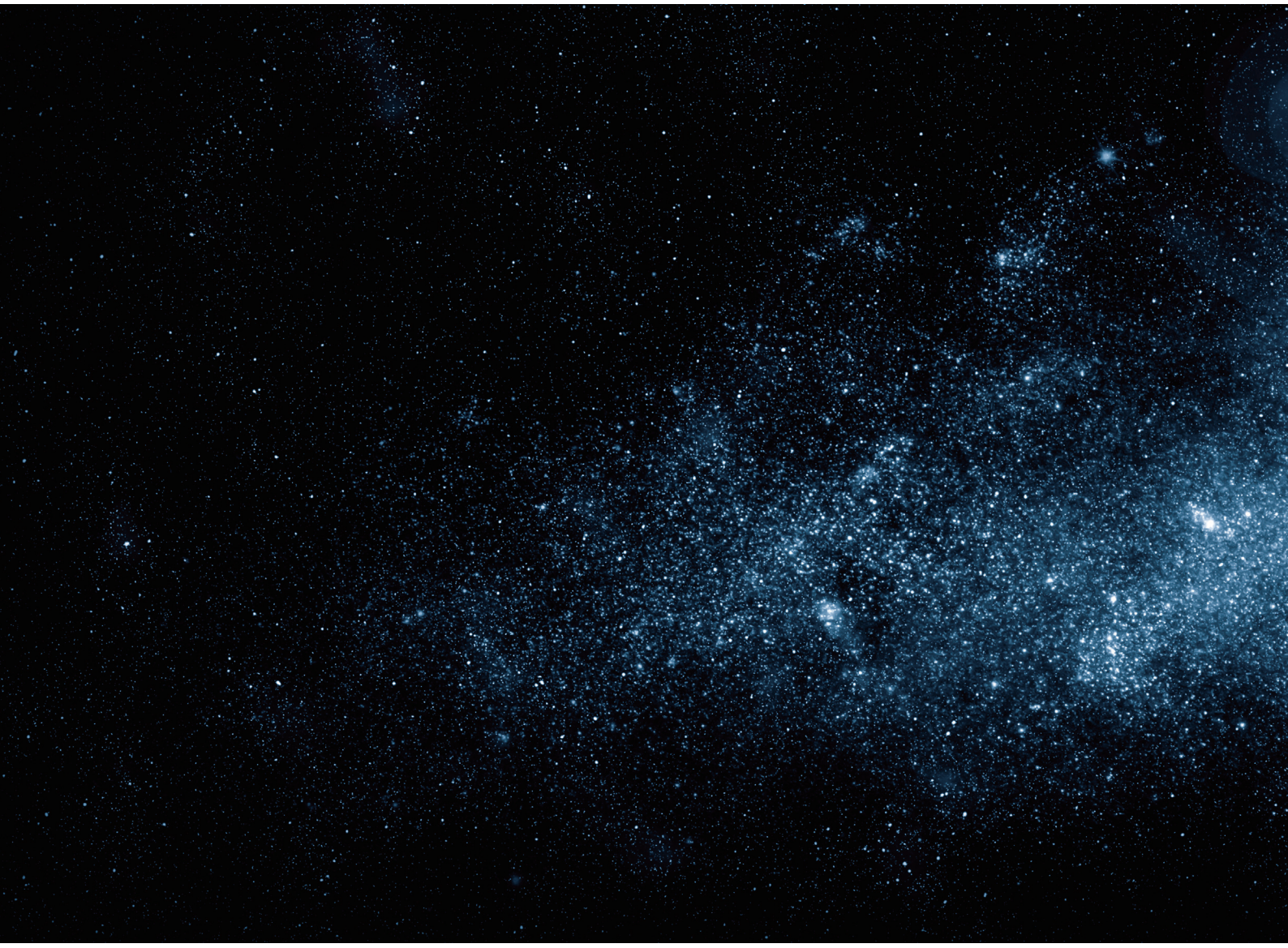
国内最大級の診断実績

累計配信団体数
約1,800団体

※2024年4月時点

無償トライアル実施中！

サービス詳細や料金はこちらから
https://www.lac.co.jp/lp/mailtraining_t3/



LAC Security Academy

株式会社ラック セキュリティアカデミー
〒102-0093
東京都千代田区平河町 2-16-1 平河町森タワー
TEL 03-6757-0125 FAX 03-6757-0112

Email info-academy@lac.co.jp
https://www.lac.co.jp/service/education/