LAC
株式会社ラック

ラックセキュリティアカデミー
コースカタログ 2026

インシデントを乗り切る“力”を養う

インシデントは起きるものです。重要なのはそれを乗り越える“人”の力。
当アカデミーの研修は、対応力を磨く実践的なプログラムで構成されています。

LAC Security Academy

INDEX 目次

ラックセキュリティアカデミー概要

P. 1 本カタログについて
P. 2 ラックセキュリティアカデミー概要
P. 3 選べる研修&受講スタイル
P. 4 オープン開催 2026年度スケジュール
P. 6 対象者別お勧めコースと受講順序

コース情報

※オープン開催時の条件です

P. 8 情報セキュリティ事故対応1日コース 机上演習編 …… 120,000円（税込 132,000円）/人
P. 9 情報セキュリティ事故対応2日コース 実機演習編 …… 180,000円（税込 198,000円）/人
P.10 攻撃手法解説コース …… 195,000円（税込 214,500円）/人
P.11 プラットフォーム脆弱性診断 ハンズオンコース …… 150,000円（税込 165,000円）/人
P.12 Webアプリケーション脆弱性診断 ハンズオンコース …… 195,000円（税込 214,500円）/人
P.13 ペネトレーションテストハンズオンコース …… 150,000円（税込 165,000円）/人
P.14 Webセキュリティ設計実装講座 …… 140,000円（税込 154,000円）/人
P.14 デジタル・フォレンジックコース …… 300,000円（税込 330,000円）/人
P.16 セキュリティオペレーション実践コース 初級編 …… 150,000円（税込 165,000円）/人
P.17 セキュリティオペレーション実践コース 中級編 …… 2日コース: 250,000円（税込 275,000円）/人
3日コース: 300,000円（税込 330,000円）/人
P.18 マルウェア解析ハンズオン入門コース …… 2日コース: 300,000円（税込 330,000円）/人
3日コース: 350,000円（税込 385,000円）/人
P.19 マルウェア解析ハンズオン専門コース …… 450,000円（税込 495,000円）/人
P.20 OTセキュリティ入門 …… 80,000円（税込 88,000円）/人
P.21 スマホアプリセキュリティ対策講座 …… 195,000円（税込 214,500円）/人
P.22 セキュリティ・バイ・デザイン講座 …… 80,000円（税込 88,000円）/人
P.23 脆弱性管理コース …… 80,000円（税込 88,000円）/人
P.24 情報セキュリティスペシャリストコース …… 200,000円（税込 220,000円）/人
P.25 情報セキュリティマネジメントコース …… 120,000円（税込 132,000円）/人
P.26 ITと情報セキュリティ初級コース …… 80,000円（税込 88,000円）/人
P.27 セキュリティ競技入門コース …… 受講料はお問い合わせください
P.28 エグゼクティブ向け「サイバーセキュリティ研修」 …… 受講料はお問い合わせください
P.28 CISSP CBKトレーニング／認定試験 …… 早割/団体: 400,000円（税込 440,000円）/人
通常: 490,000円（税込 539,000円）/人
P.30 情報セキュリティ内部監査人能力認定（JASA）準拠対策講座 …… 185,000円（税込 203,500円）/人
P.31 情報セキュリティ理解度チェック プレミアム（JNSA） …… 30,000円～（税込 33,000円～）/年

その他のサービス

P.32 標的型攻撃メール訓練T3
P.35 eラーニング / コンテンツレンタルサービス

P.37 お申込み方法

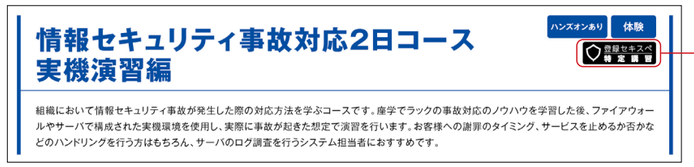
本カタログについて

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“特定講習アイコン”が表記されています。

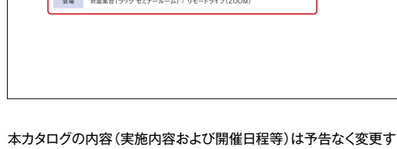


登録セキスペ 特定講習

このアイコンが表示されているコースは
特定講習対象のコースです。

■ お申込み方法

ホームページへアクセスいただき、対象コースの「お申込み」フォームからお申込みください。



備考欄に「IPA登録セキスペ更新」とご入力の上、お申込みください。

※受講当日は、IPA規定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。

コース情報の見方

学習形態の種別

座学 …… 研修内容を講義形式で学んで頂きます。

ハンズオンあり …… 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。

体験 …… 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。

該当コースを受講するにあたり、習得しておいていただきたい知識などを示しています。

該当コースの対象としている参加者のタイプを示してます。

該当コースの開催日時をご確認の上、ご希望の日程をお申込みください。

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、ネットワークセキュリティに関するプロフェッショナルであるアナリストが、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）が収集した攻撃を分析し、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、サイバー空間における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。

＋

サイバー救急センターによる圧倒的な緊急対応経験

ラックが運営するサイバー救急センターは、企業などがサイバー攻撃による被害に遭われた場合に、緊急対応を支援する「サイバー119サービス」を提供しています。
サイバー攻撃の原因調査においては、デジタル・フォレンジック、マルウェア解析などの専門のエンジニアが年間250件を超える対応を行っており、その傾向を踏まえた、セキュリティ教育を提供しています。

＋

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。

JSOC JAPAN SECURITY OPERATION CENTER

JSOC（ジェイソック）は2002年に開設したセキュリティ監視・運用サービス

CYBER EMERGENCY CENTER

サイバー攻撃による被害を受けた企業や団体を支援する専門組織として設立されたのが「サイバー救急センター」

対面集合 / リモートライブ研修

弊社セミナールーム、または指定の会場に集合していただき受講いただく“対面集合形式”、または弊社指定の配信ツールを利用して遠隔地からご参加いただく“リモートライブ形式”の2つの形式で学べます。
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。

eラーニング / コンテンツレンタル

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。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。
eラーニングにて公開中の研修動画や確認テストなどのコンテンツをレンタルすることもできます。レンタルしたコンテンツは社内向けの研修等に利用することが可能です。

選べる研修&受講スタイル

対面集合 / リモートライブ研修は、開催形態と受講形態が選べるコースを多数ご用意しております。
ご自身のご都合に合わせてお申込みください。

開催形態

予定している開催日時にどなたでも受講のお申込みができる「オープン開催」と、企業／団体からのお申込みにより開催する「個社向け開催」を行なっております。

オープン開催（一般募集）

予定している開催日程にお申込みいただく研修形態です。
複数企業・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。

オープン開催のお申込み方法

ご希望コースの開催日をチェック
↓
ホームページ※1またはメールで受講申込み
↓
開催日からご希望日を選んでください

※1 ホームページからのお申込みは、ご希望コースのページからお申込みください。

個社向け開催

企業／団体向けの研修になります。クローズ環境となり、その組織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、オーダーメイド研修（別途見積）を行うことも可能です。

個社向け開催のお申込み方法

ご希望コースをチェック
↓
ホームページ※2またはメールで受講申込み
↓
ご希望の日時を指定してください

※2 ホームページからのお申込みは、お問い合わせフォームからお申込みください。

受講形態

対面集合

弊社会場（永田町）や、お客様指定場所（個社向け開催の場合等）に集合の上、受講していただきます。
同じ空間で受講いただきますので、表情やお手元の操作状況等を実際に確認しながら講義を進める事が可能です。

リモートライブ

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

※ 対面集合とリモートライブを同時に行うコースもございます。受講したいが会場に来られないなど、ご自身のご都合に合わせてどちらかの形態をお選びください。

本カタログの内容（実施内容および開催日程等）は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください。

オープン開催 2026年度スケジュール

月	開催日	コース名	締め切り日	開催形式	特定講習
4・5月	4月21日（火）～23日（木）	情報セキュリティ内部監査人能力認定（JASA）準拠対策講座	4月7日（火）	リモートライブ	-
	5月14日（木）	セキュリティオペレーション実践コース 初級編	4月30日（木）	対面集合	対象
	5月15日（金）	情報セキュリティ事故対応1日コース 机上演習編	5月1日（金）	対面集合	対象
	5月18日（月）～20日（水）※2	マルウェア解析ハンズオン入門コース	5月7日（木）	対面集合	対象
	5月22日（金）	情報セキュリティ事故対応1日コース 机上演習編	5月8日（金）	リモートライブ	対象
	5月25日（月）～29日（金）	CISSP CBK トレーニング	5月1日（金）	リモートライブ	-
6月	6月10日（水）～11日（木）	攻撃手法解説コース	5月27日（水）	対面集合／リモートライブ	-
	6月12日（金）	プラットフォーム脆弱性診断 ハンズオンコース	5月29日（金）	対面集合／リモートライブ	対象
	6月15日（月）～16日（火）	Webアプリケーション脆弱性診断 ハンズオンコース	6月1日（月）	対面集合／リモートライブ	対象
	6月18日（木）～19日（金）	情報セキュリティ事故対応2日コース 実機演習編	6月4日（木）	対面集合	対象
	6月22日（月）～24日（水）※2	セキュリティオペレーション実践コース 中級編	6月8日（月）	対面集合	対象
	6月22日（月）～26日（金）	CISSP CBKトレーニング	5月29日（金）	リモートライブ	-
7月	7月6日（月）～8日（水）	情報セキュリティ内部監査人能力認定（JASA）準拠対策講座	6月22日（月）	リモートライブ	-
	7月8日（水）	情報セキュリティ事故対応1日コース 机上演習編	6月24日（水）	対面集合	対象
	7月9日（木）	セキュリティオペレーション実践コース 初級編	6月25日（木）	対面集合	対象
	7月10日（金）	ペネトレーションテストハンズオンコース	6月26日（金）	対面集合	対象※1
	7月13日（月）～15日（水）	マルウェア解析ハンズオン専門コース	6月29日（月）	対面集合	対象
	7月16日（木）～17日（金）	デジタル・フォレンジックコース	7月2日（木）	対面集合／リモートライブ	対象
	7月21日（火）～22日（水）	スマホアプリセキュリティ対策講座	7月7日（火）	対面集合	-
	7月23日（木）～24日（金）	ITと情報セキュリティ初級コース	7月9日（木）	リモートライブ	-
	7月23日（木）～29日（水）	CISSP CBK トレーニング	早期:6月5日（金）／通常:7月1日（水）	リモートライブ	-
8月	8月3日（月）～5日（水）	情報セキュリティスペシャリストコース	7月21日（火）	リモートライブ	-
	8月6日（木）～7日（金）	情報セキュリティ事故対応2日コース 実機演習編	7月23日（木）	対面集合	対象
	8月17日（月）～18日（火）	攻撃手法解説コース	8月3日（月）	対面集合／リモートライブ	-
	8月19日（水）～21日（金）※2	マルウェア解析ハンズオン入門コース	8月5日（水）	対面集合	対象
	8月24日（月）～25日（火）	情報セキュリティマネジメントコース	8月10日（月）	リモートライブ	-
9月	9月3日（木）	OTセキュリティ入門	8月20日（木）	リモートライブ	-
	9月4日（金）	Webセキュリティ設計実装講座	8月21日（金）	リモートライブ	-
	9月7日（月）～9日（水）※2	セキュリティオペレーション実践コース 中級編	8月24日（月）	対面集合	対象
	9月10日（木）	情報セキュリティ事故対応1日コース 机上演習編	8月27日（木）	対面集合	対象
	9月11日（金）	プラットフォーム脆弱性診断 ハンズオンコース	8月28日（金）	対面集合／リモートライブ	対象
	9月14日（月）～15日（火）	Webアプリケーション脆弱性診断 ハンズオンコース	8月31日（月）	対面集合／リモートライブ	対象
	9月14日（月）～18日（金）	CISSP CBKトレーニング	早期:7月30日（木）／通常:8月21日（金）	リモートライブ	-
	9月16日（水）～18日（金）	マルウェア解析ハンズオン専門コース	9月2日（水）	対面集合	対象
10月	10月5日（月）～7日（水）	情報セキュリティ内部監査人能力認定（JASA）準拠対策講座	9月18日（金）	リモートライブ	-
	10月7日（水）	セキュリティ・バイ・デザイン講座	9月24日（木）	リモートライブ	-
	10月8日（木）	セキュリティオペレーション実践コース 初級編	9月24日（木）	対面集合	対象
	10月9日（金）	ペネトレーションテストハンズオンコース	9月25日（金）	対面集合	対象※1
	10月14日（水）	脆弱性管理コース	9月30日（水）	リモートライブ	-
	10月15日（木）～16日（金）	情報セキュリティ事故対応2日コース 実機演習編	10月1日（木）	対面集合	対象
	10月19日（月）～21日（水）※2	マルウェア解析ハンズオン入門コース	10月5日（月）	対面集合	対象
	10月22日（木）～28日（水）	CISSP CBKトレーニング	早期:9月4日（金）／通常:9月30日（水）	リモートライブ	-
11月	11月6日（金）	プラットフォーム脆弱性診断 ハンズオンコース	10月23日（金）	対面集合／リモートライブ	対象
	11月9日（月）～11日（水）	マルウェア解析ハンズオン専門コース	10月26日（月）	対面集合	対象
	11月12日（木）～13日（金）	攻撃手法解説コース	10月29日（木）	対面集合／リモートライブ	-
	11月16日（月）～18日（水）※2	セキュリティオペレーション実践コース 中級編	11月2日（月）	対面集合	対象
	11月16日（月）～20日（金）	CISSP CBKトレーニング	早期:10月1日（木）／通常:10月23日（金）	リモートライブ	-
	11月19日（木）～20日（金）	デジタル・フォレンジックコース	11月5日（木）	対面集合／リモートライブ	-
	11月24日（火）	情報セキュリティ事故対応1日コース 机上演習編	11月10日（火）	対面集合	対象
12月	12月3日（木）	セキュリティオペレーション実践コース 初級編	11月19日（木）	対面集合	対象
	12月4日（金）	Webセキュリティ設計実装講座	11月20日（金）	リモートライブ	-
	12月7日（月）～9日（水）※2	マルウェア解析ハンズオン入門コース	11月24日（火）	対面集合	対象
	12月10日（木）～11日（金）	情報セキュリティ事故対応2日コース 実機演習編	11月26日（木）	対面集合	対象
	12月14日（月）～15日（火）	Webアプリケーション脆弱性診断 ハンズオンコース	11月30日（月）	対面集合／リモートライブ	対象
	12月14日（月）～18日（金）	CISSP CBKトレーニング	早期:10月29日（木）／通常:11月20日（金）	リモートライブ	-
	12月16日（水）	OTセキュリティ入門	12月2日（水）	リモートライブ	-
	12月18日（金）	ペネトレーションテストハンズオンコース	12月4日（金）	対面集合	対象※1
2027年1月	1月6日（水）～8日（金）	マルウェア解析ハンズオン専門コース	2026年12月23日（水）	対面集合	対象
	1月12日（火）	情報セキュリティ事故対応1日コース 机上演習編	1月4日（月）	リモートライブ	対象
	1月14日（木）～15日（金）	デジタル・フォレンジックコース	1月4日（月）	対面集合／リモートライブ	-
	1月18日（月）～20日（水）	セキュリティオペレーション実践コース 中級編	1月4日（月）	対面集合	対象
	1月19日（火）～21日（木）	情報セキュリティ内部監査人能力認定（JASA）準拠対策講座	1月5日（火）	リモートライブ	-
	1月21日（木）～22日（金）	情報セキュリティ事故対応2日コース 実機演習編	1月7日（木）	対面集合	対象
	1月25日（月）～29日（金）	CISSP CBKトレーニング	早期:2026年12月10日（木）／通常:2027年1月4日（月）	リモートライブ	-
2月	2月2日（火）～3日（水）	スマホアプリセキュリティ対策講座	1月19日（火）	対面集合	-
	2月4日（木）	セキュリティオペレーション実践コース 初級編	1月21日（木）	対面集合	対象
	2月5日（金）	ペネトレーションテストハンズオンコース	1月22日（金）	対面集合	対象※1
	2月8日（月）～9日（火）	攻撃手法解説コース	1月25日（月）	対面集合／リモートライブ	-
	2月10日（水）	セキュリティ・バイ・デザイン講座	1月27日（水）	リモートライブ	-
	2月15日（月）～17日（水）※2	マルウェア解析ハンズオン入門コース	2月1日（月）	対面集合	対象
	2月15日（月）～19日（金）	CISSP CBKトレーニング	早期:1月4日（月）／通常:1月22日（金）	リモートライブ	-
	2月18日（木）	脆弱性管理コース	2月4日（木）	リモートライブ	-
	2月19日（金）	プラットフォーム脆弱性診断 ハンズオンコース	2月5日（金）	対面集合／リモートライブ	対象
3月	3月1日（月）～3日（水）	情報セキュリティスペシャリストコース	2月15日（月）	リモートライブ	-
	3月4日（木）	情報セキュリティ事故対応1日コース 机上演習編	2月18日（木）	リモートライブ	対象
	3月5日（金）	Webセキュリティ設計実装講座	2月19日（金）	リモートライブ	-
	3月8日（月）～10日（水）	マルウェア解析ハンズオン専門コース	2月22日（月）	対面集合	対象
	3月11日（木）～12日（金）	情報セキュリティ事故対応2日コース 実機演習編	2月25日（木）	対面集合	対象
	3月15日（月）～16日（火）	Webアプリケーション脆弱性診断 ハンズオンコース	3月1日（月）	対面集合／リモートライブ	対象
	3月15日（月）～19日（金）	CISSP CBKトレーニング	早期:1月28日（木）／通常:2月19日（金）	リモートライブ	-
	3月18日（木）～19日（金）	デジタル・フォレンジックコース	3月4日（木）	対面集合／リモートライブ	-
	3月23日（火）～25日（木）※2	セキュリティオペレーション実践コース 中級編	3月9日（火）	対面集合	対象

個社向け開催、オーダーメイド研修のご相談を随時承っております。ご希望の方は、ホームページのお問い合わせフォームからご連絡ください。
※1　2025年12月現在、IPA特定講習の取得申請中
※2　2日コースはIPA特定講習の対象ですが、3日コースの3日目は追加課題（オプション）になります。

本カタログの内容（実施内容および開催日程等）は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください。

対象者別お勧めコースと受講順序

■ インシデント対応能力を高めたい方

❶ 攻撃手法解説コース …… P.10 へ
❷ 情報セキュリティ事故対応1日コース 机上演習編 …… P.08 へ
❸ 情報セキュリティ事故対応2日コース 実機演習編 …… P.09 へ
❹ プラットフォーム脆弱性診断ハンズオンコース …… P.11 へ
❺ Webアプリケーション脆弱性診断ハンズオンコース …… P.12 へ
❻ セキュリティオペレーション実践コース 初級編 …… P.16 へ
❼ マルウェア解析ハンズオン入門コース …… P.18 へ
❽ デジタル・フォレンジックコース …… P.14 へ
❾ 情報セキュリティスペシャリストコース …… P.24 へ
❿ SANSトレーニング※

■ ログ分析技術を習得したい方

❶ セキュリティオペレーション実践コース 初級編 …… P.16 へ
❷ セキュリティオペレーション実践コース 中級編 …… P.17 へ
❸ 情報セキュリティ事故対応1日コース 机上演習編 …… P.08 へ
❹ SANSトレーニング※

■ フォレンジック技術を習得したい方

❶ デジタル・フォレンジックコース …… P.14 へ
❷ 情報セキュリティ事故対応1日コース 机上演習編 …… P.08 へ
❸ SANSトレーニング※

■ マルウェア解析技術を習得したい方

❶ マルウェア解析ハンズオン 入門コース …… P.18 へ
❷ マルウェア解析ハンズオン 専門コース …… P.19 へ
❸ SANSトレーニング※

■ 診断技術を習得したい方

❶ プラットフォーム脆弱性診断ハンズオンコース …… P.11 へ
❷ Webアプリケーション脆弱性診断ハンズオンコース …… P.12 へ
❸ 情報セキュリティ事故対応1日コース 机上演習編 …… P.08 へ
❹ SANSトレーニング※

※SANSトレーニングの開催情報はホームページに順次掲載いたします。お申込みについてはお問合せください。

■ 特定領域のセキュリティを学びたい方

❶ OTセキュリティ入門 …… P.20 へ
❷ スマホアプリセキュリティ対策講座 …… P.21 へ
❸ Webセキュリティ設計実装講座 …… P.14 へ
❹ ペネトレーションテストハンズオンコース …… P.13 へ
❺ SANSトレーニング※

■ 現場でエンジニアとして働いている方

❶ 情報セキュリティスペシャリストコース …… P.24 へ
❷ 攻撃手法解説コース …… P.10 へ
❸ 情報セキュリティ事故対応1日コース 机上演習編 …… P.08 へ
❹ 情報セキュリティ事故対応2日コース 実機演習編 …… P.09 へ
❺ プラットフォーム脆弱性診断ハンズオンコース …… P.11 へ
❻ Webアプリケーション脆弱性診断ハンズオンコース …… P.12 へ
❼ セキュリティオペレーション実践コース 初級編 …… P.16 へ
❽ マルウェア解析ハンズオン入門コース …… P.18 へ
❾ デジタル・フォレンジックコース …… P.14 へ
❿ CISSP CBKトレーニング …… P.28 へ

■ IT関連部署からセキュリティ関連部門に配属になる/なった方

❶ 情報セキュリティスペシャリストコース …… P.24 へ
❷ 攻撃手法解説コース …… P.10 へ
❸ 情報セキュリティ事故対応1日コース 机上演習編 …… P.08 へ
❹ 情報セキュリティ事故対応2日コース 実機演習編 …… P.09 へ
❺ プラットフォーム脆弱性診断ハンズオンコース …… P.11 へ
❻ Webアプリケーション脆弱性診断ハンズオンコース …… P.12 へ
❼ セキュリティオペレーション実践コース 初級編 …… P.16 へ
❽ マルウェア解析ハンズオン入門コース …… P.18 へ
❾ デジタル・フォレンジックコース …… P.14 へ

■ 部署異動でIT関連の仕事をする方

❶ ITと情報セキュリティ 初級コース …… P.26 へ
❷ 情報セキュリティマネジメントコース …… P.25 へ

■ 一般職員だがITやセキュリティの基礎知識が必要な方

❶ ITと情報セキュリティ 初級コース …… P.26 へ
❷ 情報セキュリティマネジメントコース …… P.25 へ

本カタログの内容（実施内容および開催日程等）は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください。

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

登録セキスペ 特定講習

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

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。

■ 前提知識

- ○ なし

■ こんな方にお勧め

- ☑ 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 人材（管理系）
- ☑ CSIRT 人材（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. 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

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	2026年 5月15日（金）［締切 2026年 5月 1日（金）］ 対面集合 2026年 5月22日（金）［締切 2026年 5月 8日（金）］ リモートライブ 2026年 7月 8日（水）［締切 2026年 6月24日（水）］ 対面集合 2026年 9月10日（木）［締切 2026年 8月27日（木）］ 対面集合 2026年11月24日（火）［締切 2026年11月10日（火）］ 対面集合 2027年 1月12日（火）［締切 2027年 1月 4日（月）］ リモートライブ 2027年 3月 4日（木）［締切 2027年 2月18日（木）］ リモートライブ
研修期間	1日間　10:00~17:30
受講料	120,000円（税込 132,000円）/人
定員	21名（最少催行人数 5名）
会場	対面集合（ラック セミナールーム） / リモートライブ（ZOOM）

講師　村瀬 毅　他

情報セキュリティ事故対応2日コース 実機演習編

ハンズオンあり　体験

登録セキスペ 特定講習

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

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。

■ 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

- ☑ 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 人材（管理系）
- ☑ CSIRT 人材（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

▶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

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	2026年 6月 18日（木）~ 6月19日（金）［締切 2026年 6月 4日（木）］ 2026年 8月 6日（木）~ 8月 7日（金）［締切 2026年 7月 23日（木）］ 2026年10月 15日（木）~ 10月 16日（金）［締切 2026年10月 1日（木）］ 2026年12月10日（木）~ 12月 11日（金）［締切 2026年11月 26日（木）］ 2027年 1月 21日（木）~ 1月22日（金）［締切 2027年 1月 7日（木）］ 2027年 3月 11日（木）~ 3月12日（金）［締切 2027年 2月 25日（木）］
研修期間	2日間　10:00~17:30
受講料	180,000円（税込 198,000円）/人
定員	21名（最少催行人数 5名）
会場	対面集合（ラック セミナールーム）

講師　永井 夏生　他

本カタログの内容（実施内容および開催日程等）は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください。

攻撃手法解説コース

ハンズオンあり

～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

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。

■ 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

- ☑ IT技術者（インフラ系）
- ☑ SOC（セキュリティ運用）要員
- ☑ 監査担当
- ☑ IT技術者（開発系）
- ☑ CSIRT 人材（技術系）
- ☑ 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

▶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
Webアプリケーションの基本事項 / 脆弱性を利用した攻撃（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）

▶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

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	**2026年 6月10日（水）～ 6月11日（木）［締切 2026年 5月27日（水）］ ハイブリッド *** **2026年 8月17日（月）～ 8月18日（火）［締切 2026年 8月 3日（月）］ ハイブリッド *** **2026年11月12日（木）～ 11月13日（金）［締切 2026年10月29日（木）］ ハイブリッド *** **2027年 2月 8日（月）～ 2月 9日（火）［締切 2027年 1月25日（月）］ ハイブリッド *** *対面集合またはリモートライブのどちらかをご選択ください。
研修期間	2日間　10:00~17:30
受講料	195,000円（税込 214,500円）/人
定員	各21名（最少催行人数 5名）
会場	対面集合（ラック セミナールーム）/ リモートライブ（ZOOM）

講師　佐久間 泰地　他

プラットフォーム脆弱性診断 ハンズオンコース

ハンズオンあり　登録セキスペ 特定講習

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

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。

■ 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

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

■ 実施内容

▶1. プラットフォーム診断概要
PF診断の基礎知識 / 診断の実施計画立案 / 診断における注意点 / 診断方法の検討

▶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
脆弱性スキャナの基礎知識 / 脆弱性スキャナの設定と実行 / 脆弱性スキャナのメリットとデメリット

▶5. 手動による脆弱性診断
PoCの入手と注意点 / コマンドインジェクション / バストラバーサル

▶6. パスワードクラッキング
認証試行によるパスワードクラッキング / パスワードハッシュ値の解析

▶7. 報告書と対策
報告書に記載すべき内容 / CVSSとリスクレベルの定義 / 対策の優先度と実施時期

▶8. 総合演習
疑似環境におけるPF診断演習

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	**2026年 6月12日（金）［締切 2026年 5月29日（金）］ ハイブリッド *** **2026年 9月11日（金）［締切 2026年 8月28日（金）］ ハイブリッド *** **2026年11月 6日（金）［締切 2026年10月23日（金）］ ハイブリッド *** **2027年 2月19日（金）［締切 2027年 2月 5日（金）］ ハイブリッド *** *対面集合またはリモートライブのどちらかをご選択ください。
研修期間	1日間　10:00~17:30
受講料	150,000円（税込 165,000円）/人
定員	各21名（最少催行人数 5名）
会場	対面集合（ラック セミナールーム）/ リモートライブ（ZOOM）

講師　小松 奈央　他

本カタログの内容（実施内容および開催日程等）は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください。

Webアプリケーション脆弱性診断ハンズオンコース

ハンズオンあり　登録セキスペ 特定講習

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

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。

■ 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

- ☑ IT技術者（インフラ系）
- ☑ SOC（セキュリティ運用）要員
- ☑ 監査担当
- ☑ IT技術者（開発系）
- ☑ CSIRT 人材（技術系）
- ☑ 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

▶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

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	2026年 6月 15日（月）～ 6月16日（火）［締切 2026年 6月 1日（月）］ ハイブリッド * 2026年 9月 14日（月）～ 9月15日（火）［締切 2026年 8月 31日（月）］ ハイブリッド * 2026年12月 14日（月）～ 12月 15日（火）［締切 2026年 11月 30日（月）］ ハイブリッド * 2027年 3月 15日（月）～ 3月16日（火）［締切 2027年 3月 1日（月）］ ハイブリッド * *対面集合またはリモートライブのどちらかをご選択ください。
研修期間	2日間　10:00~17:30
受講料	195,000円（税込 214,500円）/人
定員	各21名（最少催行人数 5名）
会場	対面集合（ラック セミナールーム） / リモートライブ（ZOOM）

講師　山本 翔馬 他

ペネトレーションテストハンズオンコース

ハンズオンあり

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

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

■ 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（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）

▶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

▶5. 総合演習

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	2026年 7月10日（金）［締切 2026年 6月26日（金）］ 2026年10月 9日（金）［締切 2026年 9月25日（金）］ 2026年12月 18日（金）［締切 2026年12月 4日（金）］ 2027年 2月 5日（金）［締切 2027年 1月22日（金）］
研修期間	1日間　10:00~17:30
受講料	150,000円（税込 165,000円）/人
定員	21名（最少催行人数 5名）
会場	対面集合（ラック セミナールーム）

講師　戸谷 洋介 他

Webセキュリティ設計実装講座

座学

～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

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

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

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	**2026年　9月4日（金）［締切 2026年　8月 21日（金）］** **2026年12月4日（金）［締切 2026年11月 20日（金）］** **2027年　3月5日（金）［締切 2027年　2月 19日（金）］**		
研修期間	1日間　10:00～17:30	定員	30名（最少催行人数 5名）
受講料	140,000円（税込 154,000円）/人	会場	リモートライブ（ZOOM）

講師　藤本 博史 他

デジタル・フォレンジックコース

ハンズオンあり

～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（P.8）」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（P.9）」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

☑ SOC（セキュリティ運用）要員　☑ CSIRT 人材（技術系）

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場合があり、手動でマルウェアを探す必要があります。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を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。

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	**2026年　7月16日（木）～ 7月17日（金）［締切 2026年　7月2日（木）］ハイブリッド *** **2026年11月19日（木）～11月20日（金）［締切 2026年11月5日（木）］ハイブリッド *** **2027年　1月14日（木）～ 1月15日（金）［締切 2027年　1月4日（月）］ハイブリッド *** **2027年　3月18日（木）～ 3月19日（金）［締切 2027年　3月4日（木）］ハイブリッド *** *対面集合またはリモートライブのどちらかをご選択ください。		
研修期間	2日間　10:00～17:30	会場	対面集合（ラック セミナールーム） リモートライブ（ZOOM）
受講料	300,000円（税込 330,000円）/人		
定員	各21名（最少催行人数 5名）		

講師　伊原 秀明 他

本カタログの内容（実施内容および開催日程等）は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください。

セキュリティオペレーション実践コース 初級編

ハンズオンあり　登録セキスペ 特定講習

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

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。

■ 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

- ☑ IT技術者（インフラ系）
- ☑ CSIRT 人材（技術系）
- ☑ 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
- ☑ 監査担当

■ 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

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	2026年 5月14日（木）［締切 2026年 4月30日（木）］ 2026年 7月 9日（木）［締切 2026年 6月25日（木）］ 2026年10月 8日（木）［締切 2027年 9月24日（木）］ 2026年12月 3日（木）［締切 2026年11月19日（木）］ 2027年 2月 4日（木）［締切 2027年 1月21日（木）］
研修期間	1日間　10:00~17:30
受講料	150,000円（税込 165,000円）/人
定員	21名（最少催行人数 5名）
会場	対面集合（ラック セミナールーム）

講師　山坂 匡弘 他

セキュリティオペレーション実践コース 中級編

ハンズオンあり　オプション付き　登録セキスペ 特定講習

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。

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。

■ 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

- ☑ IT技術者（インフラ系）
- ☑ SOC（セキュリティ運用）要員
- ☑ CSIRT 人材（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

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

▶7. 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】

▶8. 演習
演習 / 演習の解答

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	2026年 6月22日（月）～ 6月23日（火）24日（水）はオプション［締切 2026年 6月 8日（月）］ 2026年 9月 7日（月）～ 9月 8日（火） 9日（水）はオプション［締切 2026年 8月24日（月）］ 2026年11月16日（月）～11月17日（火）18日（水）はオプション［締切 2026年11月 2日（月）］ 2027年 1月18日（月）～ 1月19日（火）20日（水）はオプション［締切 2027年 1月 4日（月）］ 2027年 3月23日（火）～ 3月24日（水）25日（木）はオプション［締切 2027年 3月 9日（木）］
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（税込 275,000円）/人 3日コース 300,000円（税込 330,000円）/人
定員	21名（最少催行人数 5名）
会場	対面集合（ラック セミナールーム）

講師　山坂 匡弘 他

本カタログの内容（実施内容および開催日程等）は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください。

マルウェア解析ハンズオン入門コース

ハンズオンあり　オプション付き　登録セキスペ 特定講習

～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。

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。

■ 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

☑ 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 人材（技術系）

■ 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

▶8. まとめ
解析レポートの作成

2日目

▶9. 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）

▶10. 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）

▶11. 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）

▶12. 総合演習
演習

▶13. 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】

▶14. 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

▶15. 演習
演習

▶16. 新規演習の解答
新規演習の解説

▶17. 演習
演習

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	2026年 5月 18日(月)～ 5月 19日(火) 20日(水)はオプション [締切 2026年 5月 7日(木)] 2026年 8月 19日(水)～ 8月 20日(木) 21日(金)はオプション [締切 2026年 8月 5日(水)] 2026年10月 19日(月)～10月 20日(火) 21日(水)はオプション [締切 2026年10月 5日(月)] 2026年12月 7日(月)～12月 8日(火) 9日(水)はオプション [締切 2026年11月24日(火)] 2027年 2月 15日(月)～ 2月 16日(火) 17日(水)はオプション [締切 2027年 2月 1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（税込 330,000円）/人 3日コース 350,000円（税込 385,000円）/人
定員	21名（最少催行人数 5名）
会場	対面集合（ラック セミナールーム）

講師　金子 博一 他

マルウェア解析ハンズオン専門コース

ハンズオンあり　登録セキスペ 特定講習

～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

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

○ 以下x86アセンブラについて大まかに理解していると講座を理解しやすいですが、講座の中でも説明していますので、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

■ こんな方にお勧め

☑ SOC（セキュリティ運用）要員
☑ CSIRT 人材（技術系）

※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、ImminityDebugger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

■ 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. 静的解析ツール入門
静的解析ツールとその使用方法を理解している

▶10. 静的解析ツール実践
独自IAT修正を行う

▶11. 演習①
静的解析ツールを用いて総合的に判断できる

▶12. 難読化の対応
静的解析ツールを用いて難読化部分を読み解き、適切に対処するための手法の説明

▶13. 演習②
静的解析ツールを用いて難読化部分を読み解き、適切に対処ができる

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

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	2026年 7月13日(月)～ 7月15日(水) [締切 2026年 6月29日(月)] 2026年 9月16日(水)～ 9月18日(金) [締切 2026年 9月 2日(水)] 2026年11月 9日(月)～11月 11日(水) [締切 2026年10月26日(月)] 2027年 1月 6日(水)～ 1月 8日(金) [締切 2026年12月23日(水)] 2027年 3月 8日(月)～ 3月10日(水) [締切 2027年 2月22日(月)]
研修期間	3日間 10:00~17:30
受講料	450,000円（税込 495,000円）/人
定員	21名（最少催行人数 5名）
会場	対面集合（ラック セミナールーム）

講師　金子 博一 他

OTセキュリティ入門

座学

～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

- ☑ 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

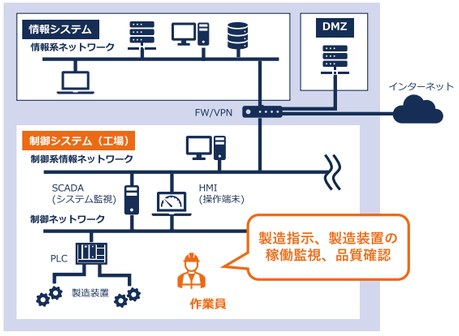
制御システムのセキュリティリスクと重要性 / 制御システムのサイバーインシデント事例紹介 / 制御システムと情報システムのセキュリティ対策の違い

▶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



※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	2026年　9月　3日（木）［締切 2026年　8月20日（木）］ 2026年12月16日（水）［締切 2026年12月　2日（水）］
研修期間	1日間　14:00～17:00
受講料	80,000円（税込 88,000円）/人
定員	30名（最少催行人数 5名）
会場	リモートライブ（ZOOM）

講師　荒井 文昭 他

スマホアプリセキュリティ対策講座

ハンズオンあり

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

- ☑ IT技術者（開発系）

■ 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

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	2026年7月21日（火）～7月22日（水）［締切 2026年7月　7日（火）］ 2027年2月　2日（火）～2月　3日（水）［締切 2027年1月19日（火）］
研修期間	2日間　10:00～17:30
受講料	195,000円（税込 214,500円）/人
定員	21名（最少催行人数 5名）
会場	対面集合（ラック セミナールーム）

講師　荒井 文昭 他

セキュリティ・バイ・デザイン講座

座学

本コースは、セキュリティ・バイ・デザインの知識・経験を身につけるためのプログラムです。セキュリティリスクとその軽減策を学習し、事例や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

- ○ 関係者それぞれの立場から情報セキュリティに関する助言や提案できるようになる
- ○ 典型的な情報セキュリティ上の問題とその対策を検討することができる
- ○ 企画要件定義段階（および他の段階）でどのようにセキュリティ要件を提案すべきかが身につく
- ○ セキュリティに関する取り組みについて、より本質的に理解できる

■ 前提知識

- ○ 弊社、情報セキュリティマネジメントコース受講済み、または情報セキュリティマネジメント合格程度の知識

■ こんな方にお勧め

☑ 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

■ 実施内容

▶1. 事例演習① インシデント対応
インシデント対応を題材に、セキュリティバイデザインの必要性を検討

▶2. セキュリティバイデザインの必要性
脅威や脆弱性等、基本的な概念の確認 / セキュリティバイデザインの全体像と原則

▶3. サービス・業務企画
システムプロファイルの作成 / 脅威分析とリスク評価

▶4. セキュリティ要件定義
要件定義の流れとポイント

▶5. 委託先管理
委託先の選定 / 委託先におけるセキュリティレベル

▶6. セキュリティ設計・実装
開発体制のセキュリティ / セキュリティテスト

▶7. 事例演習② 要件定義・設計
リスクの洗い出し / 制約下での対策優先度の決定

▶8. セキュリティ運用と改善
体制や手順の整備

▶9. 事例演習③ 企画・要件定義
冒頭のインシデントを起こさないための予防を検討

▶10. 振返り・まとめ
全体の振り返り、意見交換

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	**2026年10月　7日（水）［締切 2026年 9月24日（木）］** **2027年　2月10日（水）［締切 2027年 1月27日（水）］**
研修期間	1日間　10:00~17:00
受講料	80,000円（税込 88,000円）/人
定員	30名（最少催行人数 5名）
会場	リモートライブ（ZOOM）

講師　井上 圭 他

脆弱性管理コース

ハンズオンあり

本コースは、「脆弱性管理の重要性は理解しているが、具体的にどう進めればよいか分からない」という方向けに設計された、演習を中心とする実践的な研修です。脆弱性情報の基礎からリスク管理、脆弱性トリアージまで、体系的に学ぶことができます。実務で活用できる考え方や手順を、講師の経験や事例を交えて分かりやすく解説します。

■ 受講の効果

- ○ 脆弱性管理の概念が理解できる
- ○ 脆弱性トリアージの手法が理解できる
- ○ 学んだことを活用し、情報システムのセキュリティレベルの向上に生かせる
- ○ 外部運用ベンダやセキュリティ研究者との円滑なコミュニケーションをするために必要な知識が身につく

■ 前提知識・必要環境

- ○ Excelなどの表計算ソフト:CSVファイルを開き、複数の項目で並べ替え（ソート）ができること
- ○ 会議ツール（弊社で立ち上げたZOOM会議）でCSVファイルを受信できること
- ○ 可能であれば、Webブラウザで NVDなどのウェブサイトを閲覧し、APIの結果を表示できること
  （演習に直接の支障はありませんが、最新の情報を自身で確認することで理解しやすくなります。）
  ※Google ChromeやMicrosoft Edgeなど一般的なブラウザで可。
  ※ネットワーク制限されている環境ではアクセスできない場合があります。
- ○ コマンドの知識は不要です

■ こんな方にお勧め

☑ IT技術者（運用系）　☑ CSIRT 人材（管理系）　☑ 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 人材（技術系）

■ 実施内容

▶1. オープニングとイントロダクション
研修の目的とゴール / 脆弱性管理の重要性

▶2. 脆弱性管理の基礎
脆弱性”管理”とは何か / 組織での役割と、責任分界点

▶3. 脆弱性管理における、リスク管理の基礎
“リスク”とは / リスクへの対応→回避・緩和・移転・受容 / リスクと対応の具体例

▶4. 脆弱性管理の進め方
脆弱性管理のライフサイクル / 脆弱性管理の運用例

▶5. 脆弱性トリアージの詳細と演習
脆弱性トリアージとは何か、なぜ必要か / 基礎的なフレームワークと情報源 / その他のデータやフレームワーク / 演習1.CVSSでのトリアージ / 演習2.KEV Catalogを利用したトリアージ / 演習3.EPSSを利用したトリアージ / 演習4.SSVCを利用したトリアージ / 実務での使い分けと、組合わせ方

▶6. SBOMの活用
SBOMと脆弱性情報の連携 / SBOMの管理・更新と課題

▶7. 振り返りとまとめ、質疑応答

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	**2026年10月14日（水）［締切 2026年9月30日（水）］** **2027年　2月18日（木）［締切 2027年2月　4日（木）］**
研修期間	1日間　10:00~17:00
受講料	80,000円（税込 88,000円）/人
定員	30名（最少催行人数 5名）
会場	リモートライブ（ZOOM）

講師　井上 圭 他

情報セキュリティスペシャリストコース

座学

～『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～

国家資格「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～」（P.26）の受講もご検討ください）

■ こんな方にお勧め

☑ IT技術者（インフラ系）　☑ CSIRT 人材（技術系）　☑ 情報システム・セキュリティ推進部門担当者
☑ IT技術者（開発系）　☑ 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 / ソフトウェア管理、クラウドサービス管理 / インシデント管理 / 情報セキュリティ継続管理

▶3. 情報セキュリティ関連組織、法規、規格等
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 / ハッシュ関数とメッセージ認証 / ハッシュ関数とメッセージ認証 / デジタル署名 / PKIの概要 / PKI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、プロキシサーバ、IDS/IPS、WAF、UTM / サンドボックス、パケットアナライザ、検疫システム / ゼロトラストの概要と関連技術 / エンドポイントセキュリティ

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
メールを使った攻撃 / メールプロトコル関連セキュリティ / 送信ドメイン認証 / OP25B、メールフィルタリング / 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の全体像と具体例 / 人的セキュリティの全体像と具体例

※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.4.1』対応～」（P.25）、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
※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	**2026年8月3日（月）～8月5日（水）［締切 2026年 7月21日（火）］** **2027年3月1日（月）～3月3日（水）［締切 2027年2月15日（月）］**
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（最少催行人数 5名）
会場	リモートライブ（ZOOM）


講師　川島 慧 他

情報セキュリティマネジメントコース

座学

～『情報セキュリティマネジメント試験シラバスVer.4.1』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～」（P.26）の受講もご検討ください）

■ こんな方にお勧め

☑ 管理職　☑ CSIRT 人材（管理系）　☑ 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

▶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 / ソフトウェア管理、クラウドサービス管理 / インシデント管理 / 情報セキュリティ継続管理

▶3. 情報セキュリティ関連組織、法規、規格等
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 / ハッシュ関数とメッセージ認証 / ハッシュ関数とメッセージ認証 / デジタル署名 / PKIの概要 / PKI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 / 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、プロキシサーバ、IDS/IPS、WAF、UTM / サンドボックス、検疫システム / DLP、SIEM、VDI / エンドポイントセキュリティ

▶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 / システムの信頼性設計

▶9. メール、DNSセキュリティ
メールを使った攻撃 / メールプロトコル関連セキュリティ / 送信ドメイン認証 / OP25B、メールフィルタリング / 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の全体像と具体例 / 人的セキュリティの全体像と具体例

※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.24）、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
※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	**2026年8月24日（月）～8月25日（火）［締切 2026年8月10日（月）］**
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（最少催行人数 5名）
会場	リモートライブ（ZOOM）


講師　川島 慧 他

座学

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～

国家資格「ITパスシート」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

☑ 一般社員　☑ 管理職

■ 実施内容

1日目

▶1. 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サービスマネジメント
プロジェクトマネジメント / 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
※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	**2026年7月23日（木）～7月24日（金）［締切 2026年7月9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（最少催行人数 5名）
会場	リモートライブ（ZOOM）

講師　星 代介 他

ハンズオンあり　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

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。

■ 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

☑ 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

■ 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
○ 一部問題の解説

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

本カタログの内容（実施内容および開催日程等）は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください。

エグゼクティブ向け「サイバーセキュリティ研修」

座学

本コースは、経営リスクとなり得るサイバー攻撃に対して、経営層・管理職がどのようなことを意識して組織の資源を割り当てなくてはならないか、もし事故が発生してしまった場合、どのようなことに注意して行動すれば良いのかリスク管理の観点だけではなく危機管理の観点からも学習します。

■ 受講の効果

○ 情報セキュリティを推進する上で経営層・管理職が求められる責任を知る
○ 企業経営の観点で経営層・管理職が必要なセキュリティの知識/考え方を学ぶ

■ こんな企業にお勧め

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。

☑ 管理職

■ 実施内容

▶カリキュラム例

昨今のセキュリティ事情 / 経営とサイバーセキュリティ / 事故発生時の経営層・管理職の役割 / サイバー攻撃に強い組織づくり

※どのような内容の講演を希望されているかヒアリングした後、研修構成をご提案いたします。
※ディスカッション形式の演習も承っております。

■ 実施要項

研修期間	30分～1時間（質疑応答含む）
受講料	受講者数、オーダーメイド度合いによって変動しますので、お問い合わせください。
研修形態	対面集合の場合：貴社指定場所 リモートライブの場合：Zoomなど ※録画はお断りしております。

講師　大竹 章裕 他

CISSP CBKトレーニング/認定試験

座学

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

☑ 管理職　☑ CSIRT 人材（管理系）　☑ 監査担当
☑ SOC（セキュリティ運用）要員　☑ CSIRT 人材（技術系）　☑ 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%

CISSP® Certified Information Systems Security Professional
ISC2 Certification

■ 実施要項

開催日程

開催日程	早期締切	通常締切
2026年 5月25日（月）～ 5月29日（金）	-	2026年 5月 1日（金）
2026年 6月22日（月）～ 6月26日（金）	-	2026年 5月29日（金）
2026年 7月23日（木）～ 7月29日（水）	2026年 6月 5日（金）	2026年 7月 1日（水）
2026年 9月14日（月）～ 9月18日（金）	2026年 7月30日（木）	2026年 8月21日（金）
2026年10月22日（木）～10月28日（水）	2026年 9月 4日（金）	2026年 9月30日（水）
2026年11月16日（月）～11月20日（金）	2026年10月 1日（木）	2026年10月23日（金）
2026年12月14日（月）～12月18日（金）	2026年10月29日（木）	2026年11月20日（金）
2027年 1月25日（月）～ 1月29日（金）	2026年12月10日（木）	2027年 1月 4日（月）
2027年 2月15日（月）～ 2月19日（金）	2027年 1月 4日（月）	2027年 1月22日（金）
2027年 3月15日（月）～ 3月19日（金）	2027年 1月28日（木）	2027年 2月19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:490,000円（税込 539,000円）/人 早期割引条件:セミナー初日の45日前にお申込みが完了すること 団体割引条件:同月のセミナー開催に同企業から3名以上のお申込みがあること
試験費用	130,000円（税込 143,000円）
会場	リモートライブ（ZOOM）
試験について	CAT（Computerized Adaptive Testing） ○ トレーニング開催日の約1週間前に、各受講生のポータルサイトに試験がセットされます。受講期限内に受験ください。 有効期限はポータルサイトに試験がセットされてからおよそ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、NRIセキュアテクノロジーズ株式会社主催のセミナーです。

本カタログの内容（実施内容および開催日程等）は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください。

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

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

- ☑ 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 人材（管理系）
- ☑ CSIRT 人材（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

▶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

※実施内容は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください

■ 実施要項

開催日程	**2026年 4月21日（火）～ 4月23日（木）［締切 2026年4月 7日（火）］** **2026年 7月 6日（月）～ 7月 8日（水）［締切 2026年6月22日（月）］** **2026年10月 5日（月）～10月 7日（水）［締切 2026年9月18日（金）］** **2027年 1月19日（火）～ 1月21日（木）［締切 2027年 1月 5日（火）］**
研修期間	3日間 9:30～17:30
受講料	185,000円（税込 203,500円）/人
定員	20名（最少催行人数 5名）
会場	リモートライブ（ZOOM）

本コースはJASA認定校主催のセミナーです。

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

- ☑ 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～（税込 33,000円～）/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。

本カタログの内容（実施内容および開催日程等）は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください。

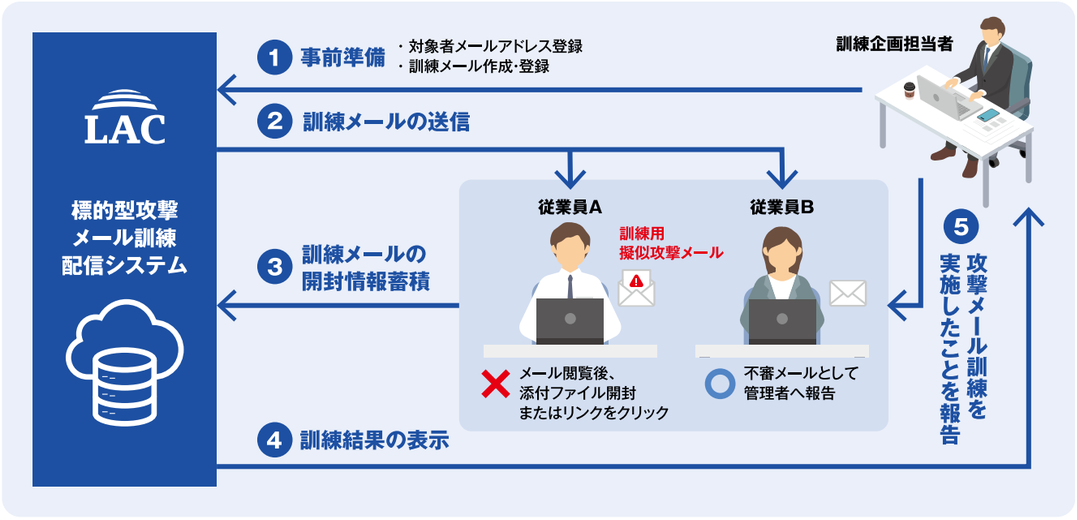
標的型攻撃メール訓練T³

■ 標的型攻撃メール訓練とは

既存のセキュリティ対策では発見が困難な標的型攻撃に対して、疑似的な標的型攻撃メール（訓練メール）を社員へ送付することで、標的型攻撃メールへの対応力を高める体験型学習サービスです。

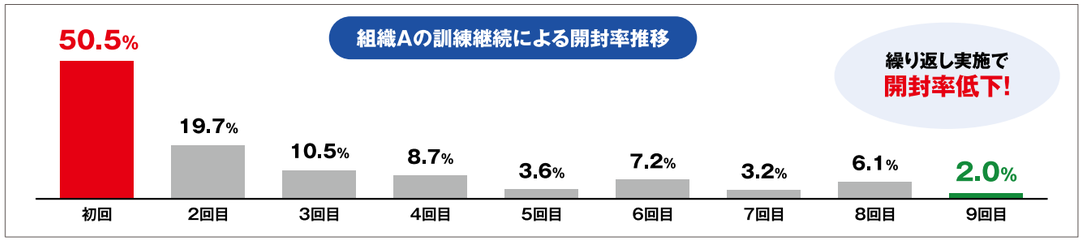
標的型攻撃メール訓練のフロー

1 事前準備 → 2 訓練メールの送信 → 3 訓練メールの開封情報蓄積 → 4 訓練結果の表示 → 5 攻撃メール訓練を実施したことを報告

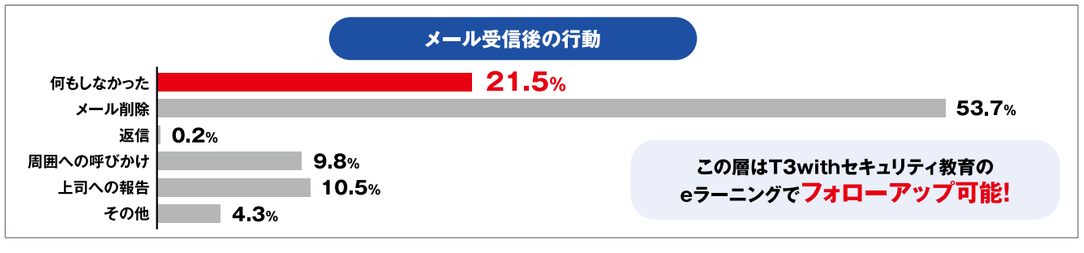


■ サービス効果

標的型攻撃メール訓練は、繰り返し行う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!



■ サービスラインナップ

コストを抑えて効果を試したい 標的型攻撃メール T3		年間複数回&教育までしっかり 標的型攻撃メール T3 with セキュリティ教育		手間をかけずに、丸っとお任せ 標的型攻撃メール T3 PLUS	
安価	価格を抑えて訓練実施	何度でも	好きなタイミングで何度も実施可能	お任せ	お客様の負担を軽減
簡単	初めての方でも操作が簡単	手間いらず	自動更新で手続きは初回のみ	カスタム	ご要望に沿ったカスタムが可能
スピーディ	スピーディーな訓練が可能	教育まで	フォローアップとしてeラーニングが可能	報告まで	報告までを支援

項目	標的型攻撃メール訓練 T3	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 Plus
契約単位	総配信数	対象者数	対象者数 × 配信回数
費用	210,000円（税込 231,000円） / 100通	360,000 円（税込 396,000円） / 100ユーザー	640,800円（税込 704,880円） / 100人×1回
配信作業	お客様		ラック
eラーニング	×	○ ※動画コンテンツラインナップ参照	×
契約期間	スポット	年間	スポット
メールテンプレート	100種類以上		
送信元ドメイン	20種類以上		
実施形式	**添付ファイル形式（zip圧縮可・暗号化可）** ・Office形式（マクロ機能なし）[Word, Excel, PowerPoint] ・PDF（URLリンク） **URLリンク形式** ・メール本文URL挿入型（text） ・HTMLメール（偽装あり / 偽装なし）		
開封結果	システムからダウンロード		ラックから送付
報告書	システムからダウンロード		ラックから送付

訓練サービス

■ T3 with セキュリティ教育 eラーニングコンテンツ一覧

2025年12月現在

No.	ジャンル	コンテンツ名	時間
1	標的型攻撃	標的型攻撃の概要と影響	6:31
2	標的型攻撃	標的型攻撃メールを見分けるテクニック	6:46
3	標的型攻撃	標的型攻撃メールに気づいた時の対処	3:30
4	標的型攻撃	知り合いからのメールでマルウェア感染!?　～感染を広げる最恐のマルウェアEmotetから組織を守る～	7:05
5	リテラシー	仕事をする場所と環境に注意　～外出時の情報の取り扱いを考えよう～	8:25
6	標的型攻撃	疑似攻撃メールテンプレート解説　～【至急】メールボックス容量が上限に近づいています～	4:16
7	リテラシー	クラウドサービス5つの注意点	5:39
8	サイバー脅威	データを「人質」として身代金を要求するランサムウェア攻撃	7:39
9	リテラシー	無線LAN利用時の注意　～安全に利用するために必要なこと～	7:30
10	リテラシー	トラブルに巻き込まれないためのSNSの利用	5:45
11	リテラシー	アカウントの乗っ取りやなりすましに遭わないアカウント管理のセキュリティ	7:36
12	リテラシー	電子メールの利用　～気を付けたいポイントについて～	6:41
13	リテラシー	業務中におけるインターネットの利用	5:26
14	サイバー脅威	身近に潜む不正アクセスの脅威	6:22
15	サイバー脅威	サプライチェーンの弱点を悪用したサイバー攻撃	5:49
16	サイバー脅威	ビジネスメール詐欺　～そのメール、本当に信用していいですか?～	6:25
17	サイバー脅威	サポート詐欺の実態①　～突然の出会い編～	5:33
18	サイバー脅威	サポート詐欺の実態②　～安全への第一歩（ファーストステップ）編～	5:18
19	サイバー脅威	実在の組織やサービスをかたるフィッシング詐欺	5:45
20	リテラシー	情報セキュリティで組織のひとりひとりがこころがけること講座	6:20
21	リテラシー	新入社員向け 情報セキュリティ研修	約40分
22	標的型攻撃	情報セキュリティ研修【標的型攻撃メール対策編】	約35分
23	リテラシー	情報セキュリティ研修【テレワーク編】	約40分
24	リテラシー	ロボタに学ぶ生成AI　4つの約束	5:02
25	リテラシー	情報セキュリティ講座【社員の意識編】	約20分
26	サイバー脅威	情報セキュリティ講座【サイバー攻撃編】	約20分
27	リテラシー	プラス・セキュリティ人材育成講座　セキュリティの基礎	約25分
28	法規制	初めての個人情報保護法	4:33
29	リテラシー	偽・誤情報に騙されないための4つのポイント	5:20
30	リテラシー	管理職向け 情報セキュリティ講座	約25分
31	リテラシー	オフィスの落とし穴を探せ!ロボタと学ぶ物理セキュリティの基本	5:32
32	法規制	知っておきたい!個人情報の第三者提供と開示請求等のルール	7:32
33	リテラシー	「だます技術」手口編 ～増加する金融犯罪・詐欺から身を守る～	8:33
34	リテラシー	「だます技術」対策編 ～増加する金融犯罪・詐欺から身を守る～	4:27

※準備中のコンテンツにつきましては現段階の予定となります。
※今後、テーマの変更や掲載順序の入れ替え等が発生する可能性がございますので予めご了承ください。

■ 無償トライアル実施中

サービスの基本機能を1ヵ月間、無料でお試し頂けます!
使い勝手やeラーニングコンテンツの内容確認など、是非この機会にご活用ください。
トライアルのお申込みは以下のURLからお申込みください。

https://www.lac.co.jp/lp/mailtraining_t3/

eラーニング / コンテンツレンタルサービス

■ eラーニング / コンテンツレンタルの特長

ラックの知見を活かした高品質のセキュリティ研修

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。

ひとりひとりのペースにあわせた学習を

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。

■ eラーニングについて

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。

▶オプションサービス（学習管理）

全社研修など、複数人で受講される場合に、組織の管理者様が受講状況を一括管理できるオプションサービスをご用意しております。

※オプションサービスは無料でご利用いただける機能になります。
※本機能をご利用可能なアカウントは1契約につき2名様となります。

▶ポータルサイトの管理画面でできること

学習状況の管理
コースごとに受講者の学習状況や進捗率を把握できます。

テストの合否および回答内容のチェック
コースに設定されたテストの合否および回答内容を把握できます。

データの抽出
コースごとの学習データをエクセル形式でエクスポートして自由に編集することができます。

※学習環境は、アルー株式会社が提供する「Etudes（エチュード）」のシステムを利用しています。

利用期間		
	開始日	管理対象コースの受講開始日のうち、最初に到来する受講開始日
	終了日	管理対象コースの受講終了日のうち、最後に到来する受講終了日の属する月の末日 （ただし、かかる受講終了日が月の末日からその5日前までの期間に到来する場合は、その翌月の5日まで延長します）

■ コンテンツレンタルについて

研修動画や確認テストなどのコンテンツをレンタルすることができます。レンタルしたコンテンツは社内向けの研修等に利用することが可能です。
レンタル期間は1年間※1、視聴可能人数は無制限※2です。ご希望の研修スケジュールに沿って効率的に視聴いただけます。
標的型攻撃メール訓練用の動画もレンタル可能です。P.34のeラーニングコンテンツ一覧をご確認ください。

※1 継続も可能です。レンタル期間終了前にご連絡ください。
※2 視聴人数は契約時にお決めいただきます。

eラーニング / コンテンツレンタルサービス

■ eラーニングコンテンツ一覧

研修コード	コース名	視聴時間	受講期間	価格（税込）	取り扱う内容の例
GEN0060	新入社員向け 情報セキュリティ研修	40分	30日間	1コース 110,000円/ 50名まで。 50名を超える場合は、 1名追加につき 2,200円	情報セキュリティとは / 情報の取り扱い / アカウント管理 / インターネットの利用 / SNSの利用·電子メールの利用 / もしもの時に備えて
GEN0030	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		標的型攻撃を知る / 騙しの手口を知る / 対策を知る
GEN1020	情報セキュリティ研修 【テレワーク編】	40分	30日間		持ち出す情報の注意 / 持ち出し端末のセキュリティ対策 / 仕事をする場所や環境に注意 / 無線LAN利用時の注意 / クラウドサービス利用の注意 / 偽メールに注意 / もしもの時に備えて
GEN0050	情報セキュリティ講座 【社員の意識編】	20分	30日間		情報セキュリティとは / 情報の価値と性質 / 情報セキュリティにおける人的リスク / ビジネスメール詐欺による金銭被害·不注意による情報漏えい等 / 身近に起こる脅威と対策 / 報告フロー
GEN0051	情報セキュリティ講座 【サイバー攻撃編】	20分	30日間		サイバー攻撃の傾向と対策（サプライチェーン攻撃/ランサムウェア攻撃/フィッシング） / サイバー攻撃に遭遇した場合の対処
GEN0310	プラス·セキュリティ人材育成講座 セキュリティの基礎	25分	30日間		情報セキュリティの基本知識 / 知っておきたいキーワード / セキュリティの脅威と対策
GEN0210	管理職向け 情報セキュリティ講座（1）	25分	30日間		管理職·リーダーが「知っておくべきこと」 / 管理職·リーダーが「やるべきこと」 / 管理職·リーダーが「やってはいけないこと」
GEN0080	サポート詐欺の実態	10分	30日間		サポート詐欺デモ動画 / サポート詐欺とは? / どういう場面で遭遇するのか? / サポート詐欺の特徴 / 電話をかけると何が起こる? / サポート詐欺の被害 / もしも詐欺に遭遇してしまった場合は? / もし電話をかけてしまった場合は?
GEN1010	ロボタと挑戦! セキュリティチャレンジ 【日常編】（1）	60分	30日間		パスワード管理 / 情報管理 / PCの安全管理 / 不審なメールにご用心 / もしもの時の対応 （シーン編→確認編（アンケート編）→解説編の順で各テーマが進みます。）
GEN1011	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		社外での言動·行動に注意 / SNSの利用 / クラウドサービスの利用 / もしもの時の対応 （シーン編→確認編（アンケート編）→解説編の順で各テーマが進みます。）
GEN0300	インシデントレスポンス概論	60分	30日間		準備 / 検知·分析 / 封じ込め·根絶·復旧 / 事故後の対応
OD-IP-001	ITと情報セキュリティ初級コース	4.5時間	180日間	88,000円/人	P.26の講座のeラーニング版となります。
OD-SG-001	情報セキュリティマネジメントコース	6.2時間	180日間	132,000円/人	P.25の講座のeラーニング版となります。
OD-SC-001	情報セキュリティスペシャリストコース	7.7時間	180日間	220,000円/人	P.24の講座のeラーニング版となります。
OD-WB-001	Webセキュリティ設計実装講座	3時間	180日間	154,000円/人	P.14の講座のeラーニング版となります。

※すべての講座で、学習形態は座学形式です。（ハンズオン等はございません。）
※すべての講座で確認テストが付属します。研修コードがGENからはじまる講座では5-10問程度、研修コードがODから始まる講座では50問程度となります。
※コンテンツレンタルの価格は、お問い合わせください。

お申込み方法 （オープン開催、eラーニング / コンテンツレンタル）

■ お申込みから受講までの流れ

お申込み

▶オープン開催（一般募集）
〈ホームページ〉
各コースの参加お申込みフォームに必要事項を入力の上お申込みください。
〈メール〉
ホームページにて申込書をダウンロードし必要事項を記入の上、info-academy@lac.co.jpまでお送りください。

▶eラーニング / コンテンツレンタル
ホームページにて申込書をダウンロードし必要事項を記入の上、ola-info@lac.co.jpまでお送りください。

受付完了

▶オープン開催（一般募集）
受講票をメールでお送りします。

▶eラーニング / コンテンツレンタル
メールまたは弊社営業担当経由でご連絡いたします。

請求書発行

▶オープン開催（一般募集）
〈前払い〉お申込みから10日以内に請求書を郵送いたします。
〈後払い〉研修終了後、請求書を郵送いたします。

▶eラーニング
〈前払い〉お申込みから5営業日目安に請求書を発行いたします。
〈後払い〉受講開始月の翌月第2営業日までに郵送いたします。

▶コンテンツレンタル
コンテンツのご提供、ご請求などにつきましては、個別にご相談させていただきます。

受講

※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。詳しくはラックセキュリティアカデミー運営事務局にお問合せください。
※代理店経由の場合は、お申込み先の代理店にお問い合わせ下さい。
※個社向け開催、オーダーメイド研修のご相談は随時承ります。詳しくはラックセキュリティアカデミー運営事務局にお問合せください。

■ お申込み先

ラックセキュリティアカデミー運営事務局

03-6757-0125
info-academy@lac.co.jp
https://www.lac.co.jp/service/education/

■ 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」駅より 徒歩1分（4番出口）

■ オープン開催のキャンセルポリシー

	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セミナー、 認定試験※1	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日前の17時まで	セミナー初日から起算し 6日前の17時以降	日程変更、受講形態変更、 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 オープンコース	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）※2	-	バウチャーの期限内に限り受験者自身がピアソンVUEにて日程変更可能です。 変更費用は受験者が直接ピアソンVUEにお支払いいただきます。		

·期日を過ぎたキャンセル、日程変更は承れません。
·キャンセル及び日程変更は、期日までに必ずメールまたはFAX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。
※1 セミナー·試験の主催元:（ISC）2 Japan
※2 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）

本カタログの内容（実施内容および開催日程等）は予告なく変更する場合がございますので、最新の情報はホームページをご確認ください。

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/

202512