LAC Security Academy

ラックセキュリティアカデミー

# 全コースガイド 2025 年度版

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。

＋

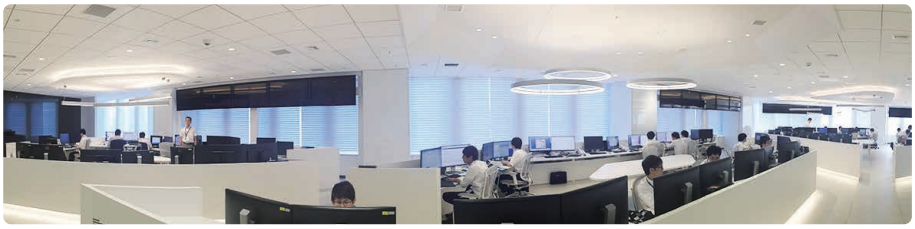
### 独自の研究所運営による圧倒的な情報量

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／リモート研修の概要

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。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／リモート研修では、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

### 集合

- 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

- 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

- 集合型、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／リモート研修　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 | 11 | ◎ | ◎ | ○ | ○ | ○ | ○ | | ● | ○ | ○ |
| | 情報セキュリティマネジメントコース | 12 | ○ | ◎ | | | | ◎ | | ◎ | | ● |
| | 情報セキュリティスペシャリストコース | 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 | ● | ● | ◎ | ● | ◎ | ◎ | ● | ◎ | ◎ | ● |
| | Web セキュリティ設計実装講座 | 16 | | | ● | ◎ | ● | ● | ● | ○ | ● | ● |
| | OT セキュリティ入門 | 17 | ● | ● | ○ | ○ | ○ | ● | ○ | ○ | ○ | |
| | 攻撃手法解説コース | 18 | | | ◎ | ◎ | ◎ | ◎ | ◎ | ○ | ◎ | ● |
| | スマホアプリセキュリティ対策講座 | 19 | | | ● | ◎ | ● | ● | ● | ○ | ● | ● |
| | 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 | 20 | | | ● | ○ | ● | ● | ◎ | ○ | ◎ | ● |
| | 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 | 21 | | | ● | ○ | ● | ● | ◎ | ○ | ◎ | ● |
| | プラットフォーム脆弱性診断　登録セキスペ 特定講習 | 22 | | | ◎ | ● | ◎ | ◎ | ◎ | ○ | ◎ | ◎ |
| | Web アプリ脆弱性診断　登録セキスペ 特定講習 | 23 | | | ● | ◎ | ◎ | ◎ | ◎ | ○ | ◎ | ◎ |
| | デジタル・フォレンジック　登録セキスペ 特定講習 | 24 | | | ○ | ○ | ○ | ○ | ● | ○ | ◎ | ○ |
| | ペネトレーションテストハンズオンコース | 26 | | | ○ | ○ | ◎ | ◎ | ◎ | ○ | ◎ | ● |
| | マルウェア解析ハンズオン入門　登録セキスペ 特定講習 | 27 | | | ○ | ○ | ○ | ○ | ● | ○ | ◎ | ○ |
| | マルウェア解析ハンズオン専門　登録セキスペ 特定講習 | 28 | | | ○ | ○ | ○ | ○ | ● | ○ | ◎ | ○ |
| | 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 | 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 | ◎ | | | | | | | | | |
| | エグゼクティブ向け「サイバーセキュリティ研修」 | 33 | | ◎ | | | | | | | | |
| 資格取得 | CISSP トレーニング | 34 | | ● | ○ | ○ | ◎ | ○ | ◎ | ○ | ◎ | ○ |
| | 内部監査人能力認定 | 36 | | ○ | ● | ● | ◎ | ◎ | ● | ● | ● | ◎ |

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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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） | 47 | ◎ | ◎ | | | | | | | | |
| | ロボタと挑戦！セキュリティチャレンジ【日常編】（2） | 47 | ◎ | ◎ | | | | | | | | |
| | 新入社員向け 情報セキュリティ研修 | 47 | ◎ | ◎ | | | | | | | | |
| | 情報セキュリティ講座【社員の意識編】 | 47 | ◎ | ◎ | | | | | | | | |
| | 情報セキュリティ講座【サイバー攻撃編】 | 47 | ◎ | ◎ | | | | | | | | |
| | 情報セキュリティ研修【標的型攻撃メール対策編】 | 47 | ◎ | ◎ | ● | ● | ● | ● | ● | ● | ● | ● |
| | インシデントレスポンス概論 | 48 | ● | ◎ | ● | ● | ◎ | ◎ | ● | ◎ | ◎ | ● |
| | プラス・セキュリティ人材育成講座 セキュリティの基礎 | 48 | ◎ | ◎ | ● | ● | ● | ● | ● | ● | ● | ● |
| | 管理職向け 情報セキュリティ講座（1） | 48 | ● | ◎ | | | | | | | | |
| | サポート詐欺の実態 | 48 | ◎ | ◎ | ● | ● | ● | ● | ● | ● | ● | ● |
| | 情報セキュリティ研修【テレワーク編】 | 48 | ◎ | ◎ | | | | | | | | |

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 | P47 新入社員向け 情報セキュリティ研修 | | | |
| 管理職 | P48 管理職向け 情報セキュリティ講座（1） | P48 プラス・セキュリティ人材育成講座 セキュリティの基礎 | P48 インシデント レスポンス概論 | 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 | P48 情報セキュリティ研修【テレワーク編】 | P47 情報セキュリティ研修【標的型攻撃メール対策編】 | P48 インシデント レスポンス概論 | |
| | P47 ロボタと挑戦！セキュリティチャレンジ【日常編】 | P47 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 | 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 | P18 攻撃解説 | P16 Webセキュリティ設計 | P19 スマホアプリセキュリティ対策講座 | P22, 23 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 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 | P18 攻撃解説 | P24, 25 デジタル・フォレンジック |
| ログ分析（アナリスト）／SOCエンジニア | P18 攻撃解説 | P20 セキュリティオペレーション実践コース 初級編 | P21 セキュリティオペレーション実践コース 中級編 | |
| マルウェア解析 | P18 攻撃解説 | P27 マルウェア入門 | P28 マルウェア専門 | P30 マルウェア専門演習 |

※こちらに記載がないコースも多数ご用意しております。

# 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


| | |
|---|---|
| 情報セキュリティ事故対応 1 日コース 机上演習編 | P.14 |
| 情報セキュリティ事故対応 2 日コース 実機演習編 | P.15 |
| セキュリティオペレーション実践コース 初級編 | P.20 |
| セキュリティオペレーション実践コース 中級編 | P.21 |
| プラットフォーム脆弱性診断ハンズオンコース | P.22 |
| Web アプリケーション脆弱性診断ハンズオンコース | P.23 |
| デジタル・フォレンジックコース | P.24 |
| マルウェア解析ハンズオン入門コース | P.27 |
| マルウェア解析ハンズオン専門コース | P.28 |
| マルウェア解析ハンズオン専門演習コース | P.30 |


※ 2025 年度の特定講習継続申請中（2024 年 12 月現在）

登録セキスペ
特 定 講 習

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。

# オープン開催 2025 年度スケジュール

2024年12月現在

## 2025年 4月

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| 30 | 31 | 1 | 2 | 3 | 4 | 5 |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 27 | 28 | 29 昭和の日 | 30 | 1 | 2 | 3 |

## 2025年 5月

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| 27 | 28 | 29 | 30 | 1 | 2 | 3 憲法記念日 |
| 4 みどりの日 | 5 こどもの日 | 6 振替休日 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 P.20 | 15 OP初級 集合 | 16 IR1日 集合 | 17 P.14 |
| 18 | 19 P.27 マルウェア入門※ 集合 | 20 | 21 | 22 DF ハイブリッド | 23 | 24 P.24 |
| | CISSP | | | | | P.34 |
| 25 | 26 | 27 | 28 内部監査人 | 29 | 30 | 31 P.36 |

※ 3日目はオプション参加（有料）

## 2025年 6月

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 P.11 IP Live | 10 | 11 | 12 攻撃解説 ハイブリッド P.18 | 13 PF診断 ハイブリッド | 14 P.22 |
| 15 P.23 | 16 Web診断 ハイブリッド | 17 | 18 | 19 | 20 IR2日 集合 | 21 P.15 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| | OP中級※ 集合 | | | P.21 | | |
| | CISSP | | | | | P.34 |
| 29 | 30 | 1 | 2 | 3 | 4 | 5 |

※ 3日目はオプション参加（有料）

## 2025年 7月

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| 29 | 30 | 1 | 2 | 3 | 4 | 5 |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| P.12 | SG Live | | IR1日 Live P.14 | OP初級 集合 P.20 | ペネトレ 集合 | P.26 |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| P.28 | マルウェア専門 集合 | | | DF ハイブリッド | | P.24 |
| | CISSP | | | | | P.34 |
| 20 | 21 海の日 | 22 | 23 | 24 | 25 | 26 |
| | | スマホ対策 集合 | | P.19 | | |
| 27 | 28 | 29 | 30 | 31 | 1 | 2 |

## 2025年 8月

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| 27 | 28 | 29 | 30 | 31 | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| P.13 | SC Live | | | IR2日 集合 | | P.15 |
| | | | 内部監査人 | | | P.36 |
| 10 | 11 山の日 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| P.18 | 攻撃解説 ハイブリッド | | P.30 | マルウェア専門演習 集合 | | |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | | | | | | |

## 2025年 9月

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| 31 | 1 | 2 | 3 | 4 | 5 | 6 |
| | | | P.17 | OT Live | Web設計 Live | P.16 |
| | | | P.14 | IR1日 集合 | | |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| P.21 | OP中級※ 集合 | | | DF ハイブリッド | | P.24 |
| | CISSP | | | | | P.34 |
| 14 | 15 敬老の日 | 16 | 17 | 18 | 19 | 20 |
| | P.23 | Web診断 ハイブリッド | | | PF診断 ハイブリッド | P.22 |
| 21 | 22 | 23 秋分の日 | 24 | 25 | 26 | 27 |
| | | P.27 | マルウェア入門※ 集合 | | | |
| 28 | 29 | 30 | 1 | 2 | 3 | 4 |

※ 3日目はオプション参加（有料）

## 2025年 10月

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| 28 | 29 | 30 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 スポーツの日 | 14 | 15 | 16 | 17 | 18 |
| | P.11 | IP Live | | IR2日 集合 | | P.15 |
| | | | | CISSP | | P.34 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| P.28 | マルウェア専門 集合 | | | | OP初級 集合 | P.20 |
| | CISSP | | | | | |
| 26 | 27 | 28 | 29 | 30 | 31 | 1 |

## 2025年 11月

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| 26 | 27 | 28 | 29 | 30 | 31 | 1 |
| 2 | 3 文化の日 | 4 | 5 | 6 | 7 | 8 |
| | | | | P.14 | IR1日 (福岡) 集合 | |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| P.30 | マルウェア専門演習 集合 | | | OP中級※ 集合 | | P.21 |
| | | | | CISSP | | P.34 |
| 16 | 17 | 18 | 19 P.22 | 20 | 21 | 22 |
| P.18 | 攻撃解説 ハイブリッド | | PF診断 ハイブリッド | DF ハイブリッド | | P.24 |
| | CISSP | | | | | |
| 23 勤労感謝の日 | 24 振替休日 | 25 | 26 | 27 | 28 | 29 |
| | P.14 | IR1日 集合 | | | | |
| 30 | | | | | | |

※ 3日目はオプション参加（有料）

## 2025年 12月

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| 30 | 1 | 2 | 3 | 4 | 5 | 6 |
| P.13 | SC Live | | | OP初級 集合 P.20 | Web設計 Live | P.16 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| P.27 | マルウェア入門※ 集合 | | | IR2日 集合 | | P.15 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| | | ペネトレ 集合 | P.26 | Web診断 ハイブリッド | | P.23 |
| | | | 内部監査人 | | | P.36 |
| | CISSP | | | | | P.34 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | 29 | 30 | 31 | 1 | 2 | 3 |

※ 3日目はオプション参加（有料）

## 2026年 1月

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| 28 | 29 | 30 | 31 | 1 元旦 | 2 | 3 |
| 4 | 5 | 6 P.28 | 7 マルウェア専門 集合 | 8 | 9 | 10 |
| 11 | 12 成人の日 P.14 | 13 IR1日 Live | 14 | 15 | 16 DF ハイブリッド | 17 P.24 |
| 18 P.21 | 19 OP中級※ 集合 | 20 | 21 | 22 | 23 IR2日 集合 | 24 P.15 |
| 25 | 26 CISSP | 27 | 28 | 29 | 30 | 31 P.34 |

※ 3日目はオプション参加（有料）

## 2026年 2月

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 スマホ対策 集合 | 7 P.19 |
| 8 | 9 攻撃解説 ハイブリッド P.18 | 10 | 11 建国記念日 | 12 PF診断 ハイブリッド P.22 | 13 OT Live | 14 P.17 |
| 15 P.30 | 16 マルウェア専門演習 集合 P.12 | 17 SG Live | 18 P.20 | 19 OP初級 集合 | 20 | 21 |
| 22 | 23 天皇誕生日 | 24 | 25 | 26 | 27 | 28 |

CISSP P.34

## 2026年 3月

| 日 | 月 | 火 | 水 | 木 | 金 | 土 |
|---|---|---|---|---|---|---|
| 1 P.13 | 2 SC Live | 3 | 4 | 5 IR1日 集合 P.14 | 6 Web設計 Live | 7 P.16 |
| 8 P.27 | 9 マルウェア入門※ 集合 | 10 | 11 | 12 IR2日 集合 | 13 | 14 P.15 |
| 15 P.23 | 16 Web診断 ハイブリッド | 17 | 18 DF ハイブリッド | 19 | 20 春分の日 P.24 | 21 |
| 22 | 23 OP中級※ 集合 | 24 | 25 | 26 P.21 | 27 | 28 |
| 29 | 30 | 31 | 1 | 2 | 3 | 4 |

内部監査人 P.36
CISSP P.34

※ 3日目はオプション参加（有料）

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

分　類　**スペシャリスト育成コース**

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
- 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

**資格取得支援**

- 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

# 目次


ラックセキュリティアカデミー概要 ..... 2
選べる 研修&受講スタイル ..... 3
集合研修　対象別コース一覧 ..... 4
オンライン研修　対象別コース一覧 ..... 5
対象者別お勧めコース ..... 6
情報処理安全確保支援士（登録セキスペ）特定講習 ..... 7
オープン開催 2025 年度スケジュール ..... 8
目次 ..... 10
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 ..... 11
　情報セキュリティマネジメントコース ..... 12
　情報セキュリティスペシャリストコース ..... 13
　情報セキュリティ事故対応 1 日コース 机上演習編 ..... 14
　情報セキュリティ事故対応 2 日コース 実機演習編 ..... 15
　Web セキュリティ設計実装講座 ..... 16
　OT セキュリティ入門 ..... 17
　攻撃手法解説コース ..... 18
　スマホアプリセキュリティ対策講座 ..... 19
　セキュリティオペレーション実践コース 初級編 ..... 20
　セキュリティオペレーション実践コース 中級編 ..... 21
　プラットフォーム脆弱性診断ハンズオンコース ..... 22
　Web アプリケーション脆弱性診断ハンズオンコース ..... 23
　デジタル・フォレンジックコース ..... 24
　ペネトレーションテストハンズオンコース ..... 26
　マルウェア解析ハンズオン入門コース ..... 27
　マルウェア解析ハンズオン専門コース ..... 28
　マルウェア解析ハンズオン専門演習コース ..... 30
　セキュリティ競技入門コース ..... 31
一般社員向け
　情報セキュリティ理解度チェック プレミアム（JNSA） ..... 32
　エグゼクティブ向け「サイバーセキュリティ研修」 ..... 33
資格取得支援
　CISSP CBK トレーニング / 認定試験 ..... 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 ..... 36
　CompTIA ..... 37
お申込方法 ..... 38
プログラム一覧（集合研修 / リモート研修） ..... 39
ラックセキュリティアカデミーオンライン ..... 40
　General e-Learning（GEN）おすすめコース ..... 44
　オンライン研修　一般社員向けコース ..... 47
標的型攻撃メール訓練 T3 ..... 49


■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＋

オープン・個別どちらでも開催します

個別

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

座学

研修内容を講義形式で学んでいただきます

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

ハンズオン

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

オンライン

オンデマンドで学んでいただけるコースもございます。

# 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

## こんな方にお勧めです

■ 一般社員
■ IT 技術者（開発系）
■ CSIRT 人材（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 人材（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. 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 | 2025 年 6 月 9 日(月) ～ 10 日(火)　締切 5 月 26 日(月)<br>2025 年 10 月 14 日(火) ～ 15 日(水)　締切 9 月 30 日(火) |
| 研修期間 | 2 日間　13:00 ～ 17:30 |
| 受講料 | 80,000 円（88,000 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　星 代介　他

# 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～

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～」（P11）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 人材（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 人材（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
- 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
- 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.13）、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 | **2025** 年 **7** 月 **7** 日（月）～ **8** 日（火） 締切 **6** 月 **23** 日（月）<br>**2026** 年 **2** 月 **17** 日（火）～ **18** 日（水） 締切 **2** 月 **3** 日（火） |
| 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

## ～『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.11) 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 人材（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 人材（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
- 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
- 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.4.0』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 | 2025 年 8 月 4 日(月) ～ 6 日(水)　締切 7 月 22 日(火) |
| | 2025 年 12 月 1 日(月) ～ 3 日(水)　締切 11 月 17 日(月) |
| | 2026 年 3 月 2 日(月) ～ 4 日(水)　締切 2 月 16 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 人材（管理系）
- ■ CSIRT 人材（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 | 2025 年 5 月 16 日（金） | 締切 5 月 2 日（金） | 集合研修 |
| | 2025 年 7 月 9 日（水） | 締切 6 月 25 日（水） | リモート Live |
| | 2025 年 9 月 4 日（木） | 締切 8 月 21 日（木） | 集合研修 |
| | 2025 年 11 月 7 日（金） | 締切 10 月 24 日（金） | 集合研修（福岡） |
| | 2025 年 11 月 25 日（火） | 締切 11 月 11 日（火） | 集合研修 |
| | 2026 年 1 月 13 日（火） | 締切 1 月 5 日（月） | リモート Live |
| | 2026 年 3 月 5 日（木） | 締切 2 月 19 日（木） | 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（福岡）ホームページをご確認ください | | |

講師　大塚 英恵　他

# 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 人材（管理系）
- ■ CSIRT 人材（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 | 2025 年 6 月 19 日（木）～ 20 日（金）　締切 6 月 5 日（木） |
| | 2025 年 8 月 7 日（木）～ 8 日（金）　締切 7 月 24 日（木） |
| | 2025 年 10 月 16 日（木）～ 17 日（金）　締切 10 月 2 日（木） |
| | 2025 年 12 月 11 日（木）～ 12 日（金）　締切 11 月 27 日（木） |
| | 2026 年 1 月 22 日（木）～ 23 日（金）　締切 1 月 8 日（木） |
| | 2026 年 3 月 12 日（木）～ 13 日（金）　締切 2 月 26 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　富田 一成　他

# 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 人材（管理系）
- ■ CSIRT 人材（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 | 2025 年 9 月 5 日（金） 締切 8 月 22 日（金）<br>2025 年 12 月 5 日（金） 締切 11 月 21 日（金）<br>2026 年 3 月 6 日（金） 締切 2 月 20 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

# OT セキュリティ入門

## ～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

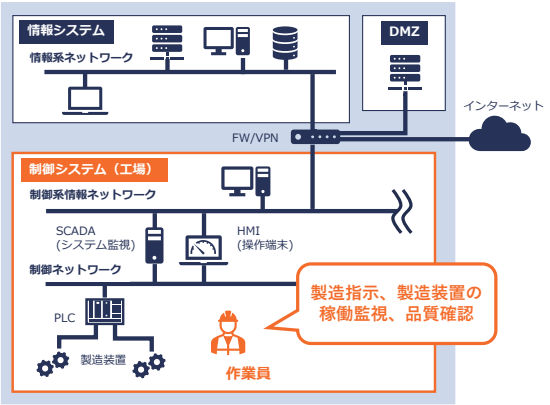
## 実施内容

**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 | **2025** 年 **9** 月 **4** 日（木） 締切 **8** 月 **21** 日（木）<br>**2026** 年 **2** 月 **13** 日（金） 締切 **1** 月 **30** 日（金） |
| 研修期間 | 1 日間　14:00 ～ 17:00 |
| 受講料 | 80,000 円（88,000 税込）/ 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　荒井 文昭　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）
- ■ 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（管理系）
- ■ CSIRT 人材（技術系）
- ■ 監査担当

## 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**
- 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 | 2025 年 6 月 11 日（水）～ 12 日（木） 締切 5 月 28 日（水） ハイブリッド＊<br>2025 年 8 月 18 日（月）～ 19 日（火） 締切 8 月 4 日（月） ハイブリッド＊<br>2025 年 11 月 17 日（月）～ 18 日（火） 締切 11 月 4 日（火） ハイブリッド＊<br>2026 年 2 月 9 日（月）～ 10 日（火） 締切 1 月 26 日（月） ハイブリッド＊<br>＊ハイブリッド（集合 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（214,000 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 佐久間 泰地 他

# 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 人材（管理系）
- ■ CSIRT 人材（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 | **2025** 年 **7** 月 **22** 日（火）～ **23** 日（水） 締切 **7** 月 **8** 日（火）<br>**2026** 年 **2** 月 **5** 日（木）～ **6** 日（金） 締切 **1** 月 **22** 日（木） |
| 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 | 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　荒井 文昭　他

# 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 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

## 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 | 2025年 5月15日(木) 締切 5月 1日(木) |
| | 2025年 7月10日(木) 締切 6月26日(木) |
| | 2025年10月24日(金) 締切 10月10日(金) |
| | 2025年12月 4日(木) 締切 11月20日(木) |
| | 2026年 2月19日(木) 締切 2月 5日(木) |
| 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　山坂 匡弘　他

オープン＋個別＋ | ハンズオン | 座学 | 体験 | オプション付き | 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 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

## 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 | 2025 年 6 月 23 日（月）～ 24 日（火） 25 日（水）はオプション 締切 6 月 9 日（月） |
| | 2025 年 9 月 8 日（月）～ 9 日（火） 10 日（水）はオプション 締切 8 月 25 日（月） |
| | 2025 年 11 月 12 日（水）～ 13 日（木） 14 日（金）はオプション 締切 10 月 29 日（水） |
| | 2026 年 1 月 19 日（月）～ 20 日（火） 21 日（水）はオプション 締切 1 月 5 日（月） |
| | 2026 年 3 月 23 日（月）～ 24 日（火） 25 日（水）はオプション 締切 3 月 9 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 250,000 円（275,000 円 税込）/ 人<br>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　山坂 匡弘　他

# 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）
- ■ 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（管理系）
- ■ CSIRT 人材（技術系）
- ■ 監査担当

## 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 | 2025年 6月13日(金) 締切 5月30日(金) ハイブリッド＊<br>2025年 9月19日(金) 締切 9月 5日(金) ハイブリッド＊<br>2025年11月19日(水) 締切 11月 5日(水) ハイブリッド＊<br>2026年 2月12日(木) 締切 1月29日(木) ハイブリッド＊<br>＊ハイブリッド（集合 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

# 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 人材（管理系）
- ■ CSIRT 人材（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 | 2025 年 6 月 16 日 (月) ～ 17 日 (火)　締切 6 月 2 日 (月) ハイブリッド * |
| | 2025 年 9 月 16 日 (火) ～ 17 日 (水)　締切 9 月 2 日 (火) ハイブリッド * |
| | 2025 年 12 月 18 日 (木) ～ 19 日 (金)　締切 12 月 4 日 (木) ハイブリッド * |
| | 2026 年 3 月 16 日 (月) ～ 17 日 (火)　締切 3 月 2 日 (月) ハイブリッド * |
| | * ハイブリッド（集合 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

# 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 人材（管理系）
- ■ CSIRT 人材（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 | 2025年 5月22日(木) ～ 23日(金) 締切 5月 8日(木) ハイブリッド＊ |
| | 2025年 7月17日(木) ～ 18日(金) 締切 7月 3日(木) ハイブリッド＊ |
| | 2025年 9月11日(木) ～ 12日(金) 締切 8月 28日(木) ハイブリッド＊ |
| | 2025年11月20日(木) ～ 21日(金) 締切 11月 6日(木) ハイブリッド＊ |
| | 2026年 1月15日(木) ～ 16日(金) 締切 1月 5日(月) ハイブリッド＊ |
| | 2026年 3月18日(水) ～ 19日(木) 締切 3月 4日(水) ハイブリッド＊ |
| | ＊ハイブリッド（集合 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 | 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 |

講師 伊原 秀明 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。

・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

# ペネトレーションテストハンズオンコース

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 人材（管理系）
- ■ CSIRT 人材（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
  - 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 | **2025** 年 **7** 月 **11** 日（金） 締切 **6** 月 **27** 日（金）<br>**2025** 年 **12** 月 **16** 日（火） 締切 **12** 月 **2** 日（火） |
| 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

オープン＋個別＋ | ハンズオン | 座学 | 体験 | オプション付き | 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 人材（管理系）
■ CSIRT 人材（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 | 2025 年 5 月 19 日（月）～ 20 日（火） 21 日（水）はオプション 締切 5 月 7 日（水） |
| | 2025 年 9 月 24 日（水）～ 25 日（木） 26 日（金）はオプション 締切 9 月 10 日（水） |
| | 2025 年 12 月 8 日（月）～ 9 日（火） 10 日（水）はオプション 締切 11 月 25 日（火） |
| | 2026 年 3 月 9 日（月）～ 10 日（火） 11 日（水）はオプション 締切 2 月 24 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 300,000 円（330,000 円 税込）/ 人<br>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

# 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 人材（管理系）
- ■ CSIRT 人材（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、Imminity 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 | 2025年 7月14日(月) ～ 16日(水) 締切 6月30日(月)<br>2025年10月20日(月) ～ 22日(水) 締切 10月 6日(月)<br>2026年 1月 7日(水) ～ 9日(金) 締切 12月24日(水) |
| 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

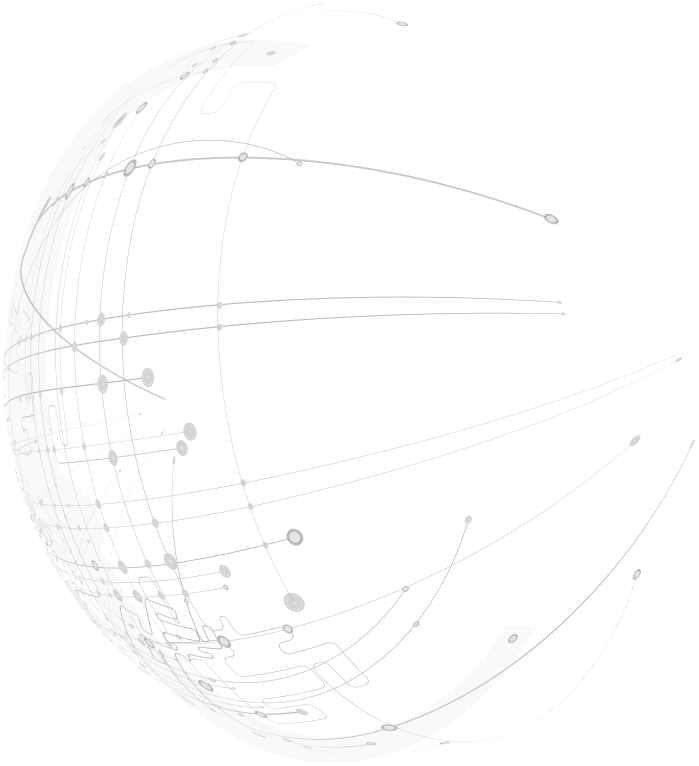
**13. 演習 ②**
- 難読化された箇所の特定と難読化解除ルーチンの推定、実践演習

### 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

・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



# 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（Ghidra を用いて）～

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）に対して、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。また、本コースでは、Ghidra を用いた解析も行います。

## 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 人材（管理系）
- ■ CSIRT 人材（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. 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. Ghidra 操作方法説明と操作演習**

**6. 難読化コードへの対応**
- Ghidra の基本的な操作を説明
- Ghidra を用いた耐解析機能回避
- 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

**7. 難読化対応演習**

**8. 耐解析機能を Ghidra を用いて解析してみよう 1**

**9. 耐解析機能を Ghidra を用いて解析してみよう 2**
- 難読化の解除実践
- Ghidra を用いた耐解析機能回避

・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 | 2025 年 8 月 21 日（木）～ 22 日（金） 締切 8 月 7 日（木）<br>2025 年 11 月 10 日（月）～ 11 日（火） 締切 10 月 27 日（月）<br>2026 年 2 月 16 日（月）～ 17 日（火） 締切 2 月 2 日（月） |
| 研修期間 | 2 日間 10:00 ～ 17:30 |
| 受講料 | 400,000 円（440,000 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

# 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<br>（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

# 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。

# エグゼクティブ向け「サイバーセキュリティ研修」

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。

## こんな企業にお勧めです

・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。

- ■ 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 人材（管理系）
- ■ CSIRT 人材（技術系）
- ■ 監査担当

## 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

## 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、カスタマイズ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 | 集合の場合：貴社指定場所<br>リモート Live 配信の場合：Zoom など<br>＊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

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 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**
・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 |
|---|---|
| 1. セキュリティとリスクマネジメント | 16% |
| 2. 資産のセキュリティ | 10% |
| 3. セキュリティアーキテクチャとエンジニアリング | 13% |
| 4. 通信とネットワークセキュリティ | 13% |
| 5. アイデンティティとアクセスの管理 | 13% |
| 6. セキュリティの評価とテスト | 12% |
| 7. セキュリティの運用 | 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 |
|---|---|---|
| 2025年 5月19日(月)～23日(金) | - | 4月25日(金) |
| 2025年 6月23日(月)～27日(金) | - | 5月30日(金) |
| 2025年 7月14日(月)～18日(金) | 5月29日(木) | 6月20日(金) |
| 2025年 9月 8日(月)～12日(金) | 7月24日(木) | 8月15日(金) |
| 2025年10月16日(木)～17日(金)＋10月20日(月)～22日(水) | 8月29日(金) | 9月24日(水) |
| 2025年11月13日(木)～14日(金)＋11月17日(月)～19日(水) | 9月26日(金) | 10月22日(水) |
| 2025年12月15日(月)～19日(金) | 10月30日(木) | 11月21日(金) |
| 2026年 1月26日(月)～30日(金) | 12月11日(木) | 1月 5日(月) |
| 2026年 2月16日(月)～20日(金) | 1月 5日(月) | 1月23日(金) |
| 2026年 3月11日(水)～13日(金)＋ 3月16日(月)～17日(火) | 1月23日(金) | 2月17日(火) |

| | |
|---|---|
| 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<br>通常：490,000円（税込　539,000円）/ 人<br>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<br>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）<br>・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。<br>・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。<br>・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。

# 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 人材（管理系）
- CSIRT 人材（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 | 2025年 5月28日(水) ～ 30日(金)　締切 5月 14日(水) |
| | 2025年 8月 6日(水) ～ 8日(金)　締切 7月 23日(水) |
| | 2025年12月17日(水) ～ 19日(金)　締切 12月 3日(水) |
| | 2026年 3月11日(水) ～ 13日(金)　締切 2月 25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<br>・IS プロフェッショナル<br>・情報セキュリティアナリスト<br>・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<br>・脆弱性アナリスト<br>・サイバーセキュリティスペシャリスト<br>・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<br>・ペネトレーションテストアナリスト<br>・ネットワークセキュリティ管理者<br>・脆弱性評価アナリスト<br>・脆弱性評価マネージャ<br>・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<br>・セキュリティコンサルタント<br>・セキュリティエンジニア<br>・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<br>・ネットワーク管理者<br>・フィールドエンジニア<br>・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<br>・ネットワーク管理者<br>・Web 管理者<br>・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<br>・ストレージ管理者<br>・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<br>・フィールドサポートエンジニア<br>・IT サポートエンジニア<br>・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<br>・プロジェクトメンバー<br>・ビジネス企画<br>・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<br>・クラウド管理者<br>・システム管理者<br>・ネットワークエンジニア<br>・ネットワーク管理者<br>・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。

# 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。

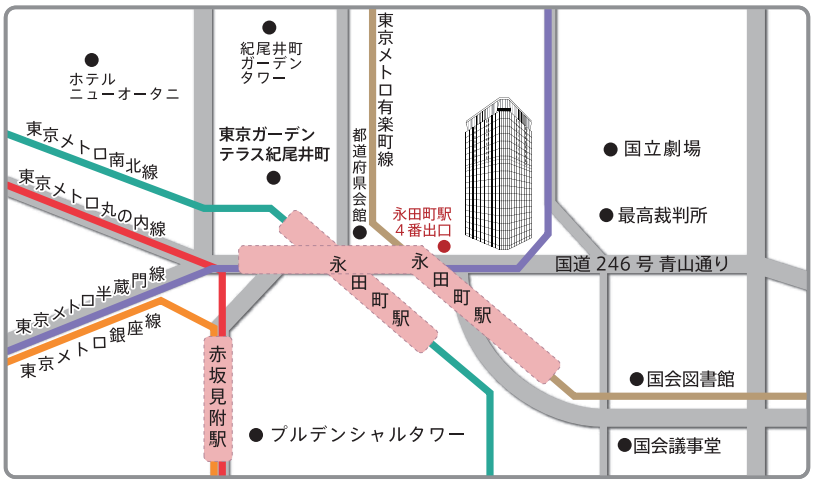
※見積書、請求書、領収書、受講修了証など各種書類の発行も承っております。詳しくは事務局にお問合せください。
※代理店経由の場合は、お申込先の代理店にお問い合わせ下さい。

## 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 / リモート研修）

## 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 | 11 | 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 |
| | 12 | 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 |
| | 13 | 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 |
| | 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<br>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<br>体 験 | 2 日間 | 180,000 円（198,000 円 税込） | 開催日の 14 日前 |
| | 16 | 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 |
| | 17 | 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 |
| | 18 | 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 |
| | 19 | 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 |
| | 20 | 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 |
| | 21 | 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）<br>3 日コース 300,000 円（330,000 円 税込） | 開催日の 14 日前 |
| | 22 | 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 |
| | 23 | 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 |
| | 24 | 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 |
| | 26 | 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 |
| | 27 | 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）<br>3 日コース 350,000 円（385,000 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 |
| | 30 | 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 | 400,000 円（440,000 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<br>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 | - |
| | 33 | エグゼクティブ向け「サイバーセキュリティ研修」 | 座 学 | 30 分～<br>1 時間 | お問い合わせください | - |
| 資格取得支援 | 34 | 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）<br>通常：490,000 円（539,000 円 税込）（注 2） | 開催日の 7 日前 |
| | 36 | 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<br>22 日前の 17 時まで | セミナー初日から起算し<br>21 日前～ 5 日前の 17 時まで | セミナー初日から起算し<br>5 日前の 17 時以降 | 日程変更、キャンセルには 1 回につき<br>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<br>14 日前の 17 時まで | - | コース初日から起算し<br>14 日前の 17 時以降 | コース初日から起算し 13 日～前日は<br>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）　セミナー主催元：NRI セキュアテクノロジーズ株式会社
（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）

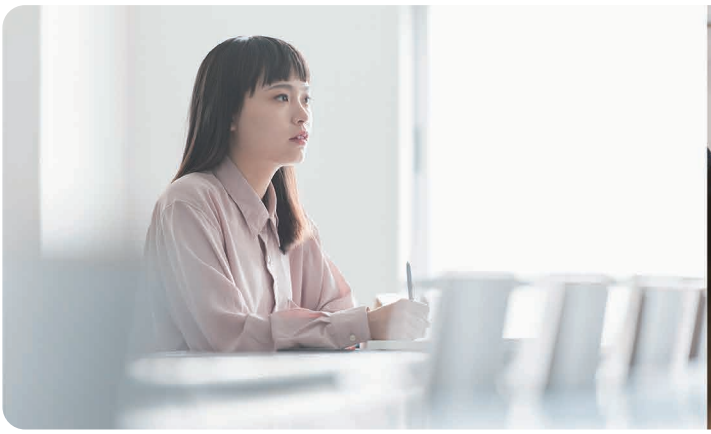
・キャンセル及び日程変更は、期日までに必ずメールにてご連絡ください。
・期日を過ぎたキャンセル、日程変更は承れません。
・当日欠席された場合につきましても、受講料・受験料の全額を申し受けます旨ご了承ください。
・開催中止または日程・内容変更はセミナー初日の 14 日前までにメールにて通知します。

# 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
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。

**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。

## 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。詳細は次のページをご確認ください。

# 受講者の学習状況を一括管理

オンラインコース
## オプションサービス（学習管理）

ラックセキュリティアカデミーオンラインでは、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すべてのオンラインコース（GEN）にて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。

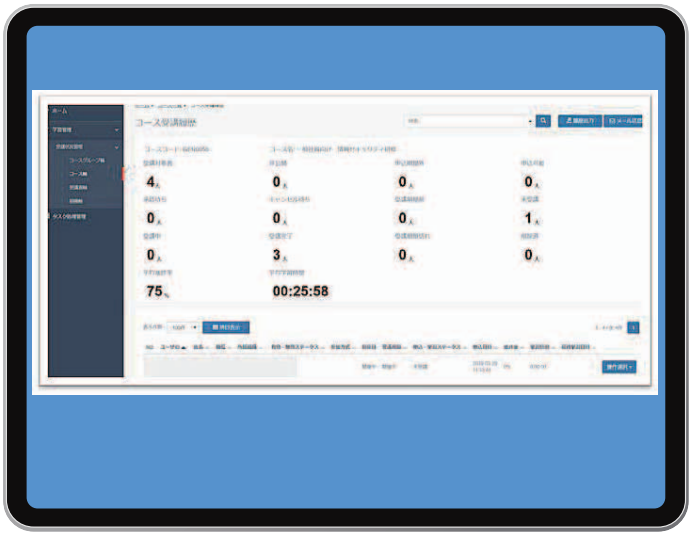
### オプションサービスの内容

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の管理画面で、次のことが行えます。

**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）

## コースタイプ

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。

## ピックアップコース

**Pick Up!**

### 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　■受講期間：30 日間
■受講料：100,000 円（110,000 円税込 50 名まで）

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

※すべてＧＥＮコースの料金体系になります。

**Pick Up!**

### 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」を醸成させたいといった場合におすすめです。

■コースコード：GEN0210　■受講期間：30 日間
■受講料：100,000 円（110,000 円税込 50 名まで）

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

## 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/

### お申し込み
申込書類をダウンロードして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
メールにてご連絡します。

### 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 5 営業日目安に請求書を発行いたします。

### ご受講

### 請求書発行（後払い）
受講開始後、受講開始月の翌月第二営業日までに郵送いたします。

## 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

### 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

### 受講の前提知識

- 特になし

### 実施要項

| | |
|---|---|
| 受講期間 | 30 日間 |
| 受講料 | 100,000 円（税込 110,000 円）/50 名まで<br>※ 50 名を超える場合は、1 名追加につき 2,000 円（税込 2,200 円）がかかります。 |
| 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

### 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

### 受講の前提知識

- 特になし

### 実施要項

| | |
|---|---|
| 受講期間 | 30 日間 |
| 受講料 | 100,000 円（税込 110,000 円）/50 名まで<br>※ 50 名を超える場合は、1 名追加につき 2,000 円（税込 2,200 円）がかかります。 |
| 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

| | |
|---|---|
| 受講期間 | 30 日間 |
| 受講料 | 100,000 円（税込 110,000 円）/50 名まで<br>※ 50 名を超える場合は、1 名追加につき 2,000 円（税込 2,200 円）がかかります。 |
| 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

| | |
|---|---|
| 受講期間 | 30 日間 |
| 受講料 | 100,000 円（税込 110,000 円）/50 名まで<br>※ 50 名を超える場合は、1 名追加につき 2,000 円（税込 2,200 円）がかかります。 |
| 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

| | |
|---|---|
| 受講期間 | 30 日間 |
| 受講料 | 100,000 円（税込 110,000 円）/50 名まで<br>※ 50 名を超える場合は、1 名追加につき 2,000 円（税込 2,200 円）がかかります。 |
| 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 GEN0300

NEW

# 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。

## 受講の効果

- インシデント発生時にどのような行動をすべきかのヒントを得られる
- 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

## こんな方にお勧めです

- 一般社員、職員
- ネットワークやシステム運用に携わっている技術者
- 部門の責任者や情報セキュリティ担当者
- 組織のセキュリティ委員会や CSIRT のメンバー

## 受講の前提知識

- 特になし

## 実施要項

| | |
|---|---|
| 受講期間 | 30 日間 |
| 受講料 | 100,000 円（税込 110,000 円）/50 名まで<br>※ 50 名を超える場合は、1 名追加につき 2,000 円（税込 2,200 円）がかかります。 |
| 視聴時間 | 1 時間 |

# 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　■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　■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　■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】

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　■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】

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　■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　■受講期間：30 日間　■受講料：100,000 円（110,000 円 税込）**

## インシデントレスポンス概論 NEW

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：GEN0300　■受講期間：30 日間　■受講料：100,000 円（110,000 円 税込）**

## 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　■受講期間：30 日間　■受講料：100,000 円（110,000 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　■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

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　■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　■受講期間：30 日間　■受講料：100,000 円（110,000 円 税込）**

# 標的型攻撃メール訓練 T3

*Targeted Threat mail Training*

## 標的型攻撃メール訓練 T3 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。

## サービスラインナップ

### T3

金額コストを抑えたい＆まずはお試し

**エントリー**

安価
簡単
スピーディ

- 価格を抑えて訓練実施！
- 初めての方でも操作が簡単！
- スピーディーな訓練が可能！

### T3 with セキュリティ教育

年間複数回＆教育までしっかり

**プレミアム**

何度でも
手間いらず
教育まで

- 好きなタイミングで何度も実施可能！
- 自動更新で手続きは初回のみ！
- フォローアップとしてeラーニングが可能！

### T3 Plus

手間をかけずに、丸っとお任せ

**エンタープライズ**

お任せ
カスタム
報告まで

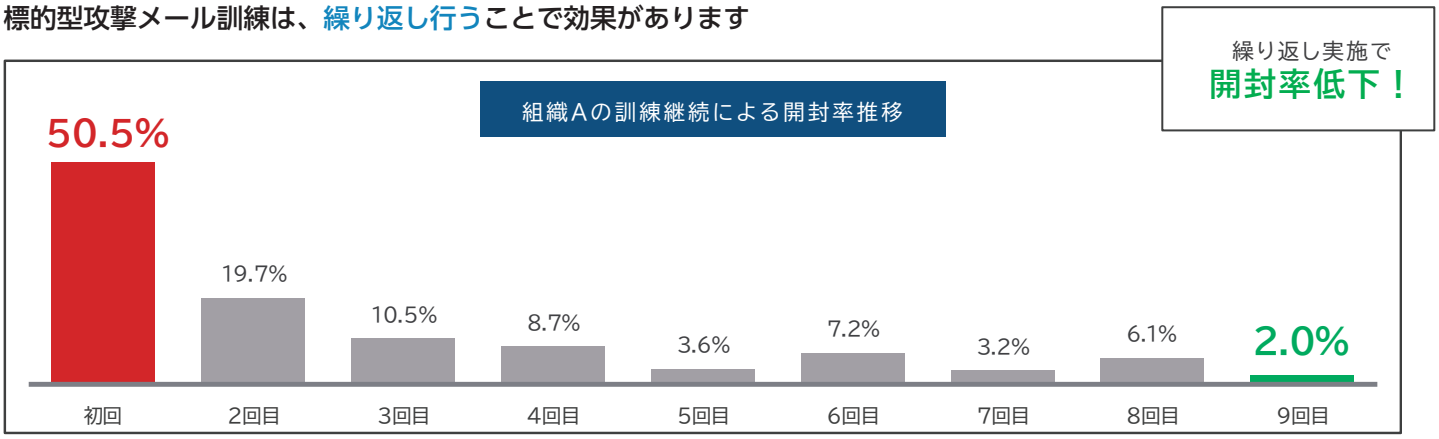
- お客様の負担を軽減！
- ご要望に沿ったカスタムが可能！
- 報告までを支援！

# サービスラインナップ

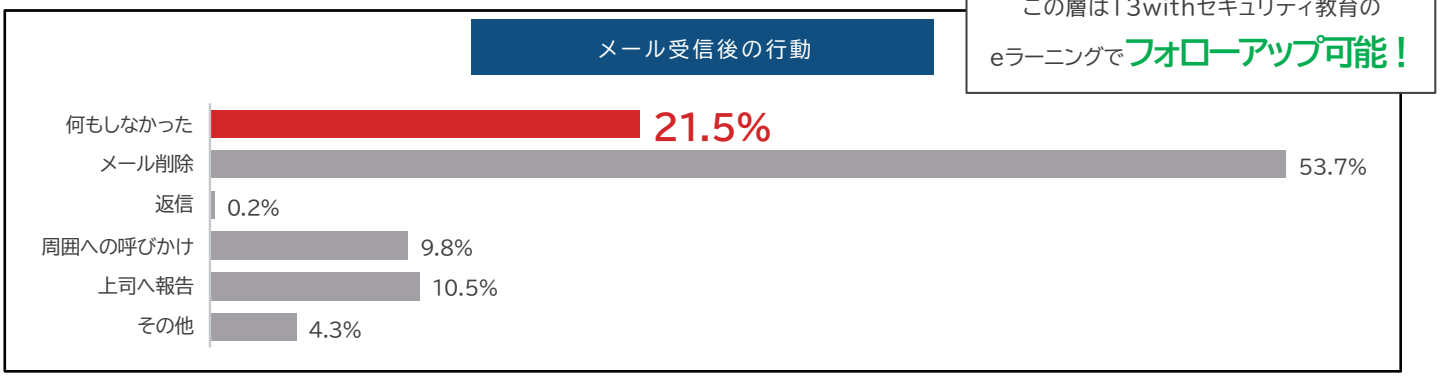
| 項目 | 標的型攻撃メール訓練 T3 | 標的型攻撃メール訓練 T3<br>with セキュリティ教育 | 標的型攻撃メール訓練 T3 Plus |
|---|---|---|---|
| 契約単位 | 総配信数 | 対象者数 | 対象者数 × 配信回数 |
| 費用 | 210,000 円(231,000 円 税込)/ 100通 | 360,000 円(396,000 円 税込)/ 100ユーザー | 640,800 円(704,880 円 税込)/ 100人×1回 |
| 配信作業 | お客様 | | ラック |
| eラーニング | × | ○<br>※動画コンテンツラインナップ参照 | × |
| 契約期間 | スポット | 年間 | スポット |
| メールテンプレート | 95種類 | | |
| 送信元ドメイン | 22種類 | | |
| 実施形式 | 添付ファイル形式(zip圧縮可・暗号化可)<br>・ Office形式(マクロ機能なし)<br>[Word, Excel, PowerPoint]<br>・ PDF(URLリンク)<br><br>URLリンク形式<br>・ メール本文URL挿入型(text)<br>・ HTMLメール(偽装あり／偽装なし) | | 添付ファイル形式(zip・lzh圧縮可・暗号化可)<br>・ Office形式(マクロ機能なし)<br>[Word, Excel, PowerPoint]<br>・ Office形式(マクロ機能あり)<br>[Word, Excel]<br>・ PDF(URLリンク／JavaScript)<br>・ 偽装ショートカット(.lnk)<br>・ 偽装実行ファイル(.exe, .pif, .scr)<br>・ コンパイル済みヘルプファイル(.chm)<br>・ Windowsスクリプトファイル(.wsf)<br>・ JavaScriptファイル(.js)<br>・ RTFファイル(.rtf)<br>・ csvファイル(コマンド実行なし／あり)<br>・ IQYファイル(.iqy)<br>・ HTMLファイル(.html)<br><br>URLリンク形式<br>・ メール本文URL挿入型<br>(text／サブドメイン使用)<br>・ 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 |

# 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！



# 動画コンテンツラインナップ

2024 年 12 月現在

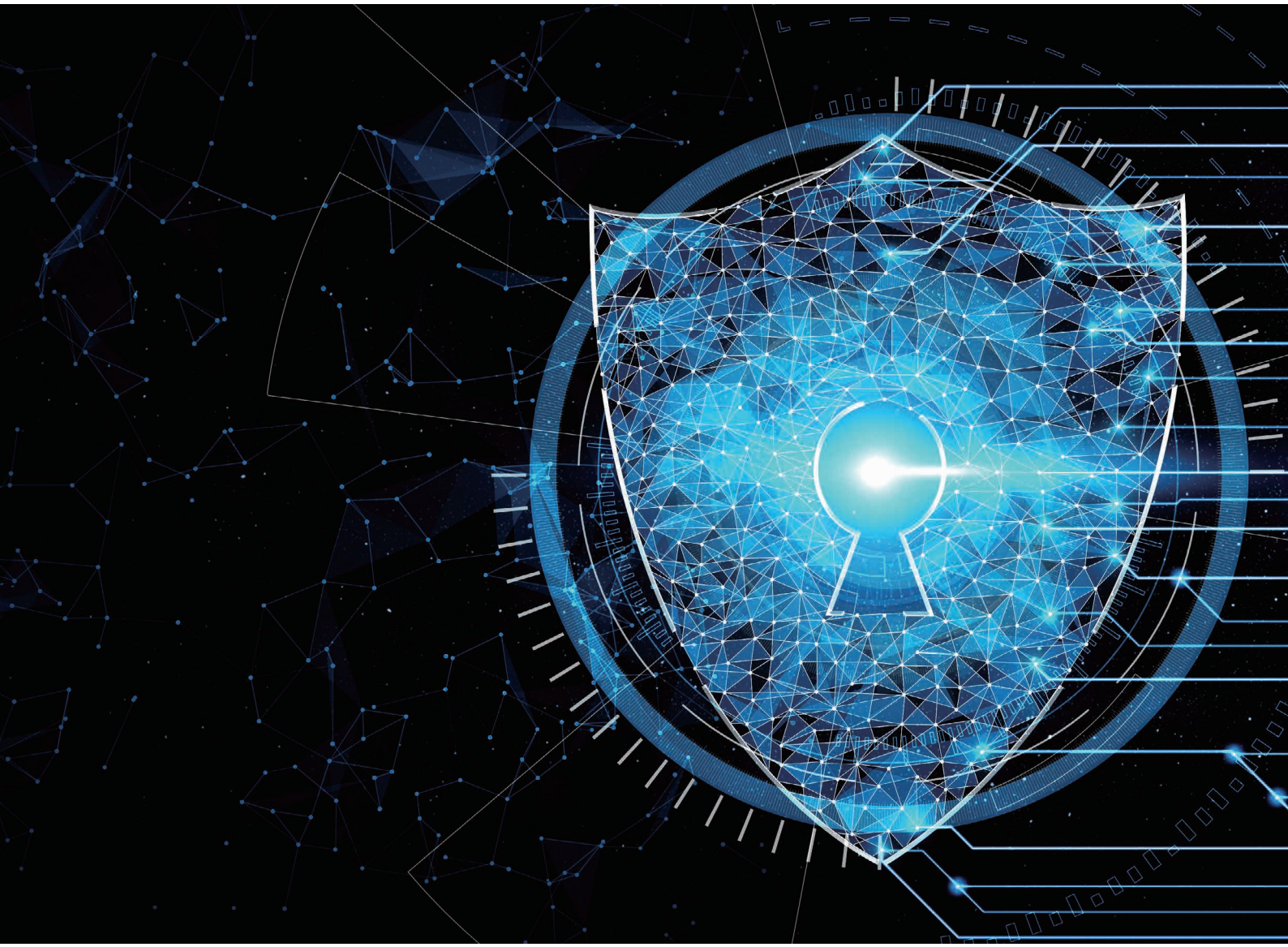
| カテゴリ | 種類 | 動画タイトル | 視聴時間 | 確認テスト |
|---|---|---|---|---|
| 標的型 | 短編 | 標的型攻撃の概要と影響 | 6分 | 3問 |
| | | 標的型攻撃メールを見分けるテクニック | 6分 | 3問 |
| | | 標的型攻撃メールを受信したことに気付いた時の対処 | 3分 | 3問 |
| | | 感染を広げる最恐のマルウェア「Emotet」から組織を守る | 7分 | 3問 |
| | | 疑似攻撃メールテンプレート解説 ～【至急】メールボックス容量が上限に近づいています | 4分 | 3問 |
| | 長編 | 情報セキュリティ研修 ～標的型攻撃メール対策編～ | 35分 | 5問 |
| リテラシー | 短編 | 仕事をする場所と環境に注意 | 8分 | 3問 |
| | | クラウドサービス5つの注意点 | 5分 | 3問 |
| | | 無線LAN利用時の注意 | 7分 | 3問 |
| | | トラブルに巻き込まれないためのSNSの使い方 | 5分 | 3問 |
| | | アカウント管理のセキュリティ | 7分 | 3問 |
| | | 電子メールの利用　－気を付けたいポイントについて－ | 6分 | 3問 |
| | | インターネットの利用について | 5分 | 3問 |
| | | 組織のひとりひとりがこころがけること講座 | 6分 | 3問 |
| | 長編 | 新入社員向け 情報セキュリティ研修 | 40分 | 10問 |
| | | 情報セキュリティ研修 ～テレワーク編～ | 40分 | 10問 |
| サイバー脅威 | 短編 | 悪質化、巧妙化するランサムウェア攻撃の現状と対策 | 7分 | 3問 |
| | | サプライチェーンの弱点を悪用したサイバー攻撃 | 5分 | 3問 |
| | | 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分 | 3問 |
| | | サポート詐欺の実態①　～突然の出会い編～ | 5分 | 3問 |
| | | サポート詐欺の実態②　～安全への第一歩編～ | 5分 | 2問 |
| | | 実在の組織やサービスをかたるフィッシング詐欺 | 5分 | 3問 |
| | | 身近に潜む 不正アクセスの脅威 | 6分 | 3問 |

# T3 with セキュリティ教育　トライアル

## ▼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。
トライアルの申し込みは下の QR コードもしくは以下の URL からお申込みください。

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/

LACAC202505 ©2025 LAC、ラック、ラックセキュリティアカデミーは株式会社ラックの登録商標です。その他記載されている会社名、製品名は一般に各社の商標または登録商標です。