静岡開催

組織とデータをサイバー攻撃から守るプロフェッショナルへ

サイバーセキュリティ対策実践講座

主催　株式会社浜名湖国際頭脳センター／企画協力　株式会社アドウィル

～インシデント対応に必要な「判断・調査・説明」の３つの力を習得します～

サイバー攻撃は防ぐだけでなく、**発生後にどう動くか・どう説明するか**が問われる時代です。本講座では、**最新の攻撃動向**や**ログ解析**に加え、**インシデント発生時の初動対応の進め方、社内・関係者への説明のポイント**まで、現場で活用できる実践的な知識・技術を習得します。**「検知はできるが、その後の対応や説明に不安がある」**そんな課題を解決する、実務直結型の講座です。

［日程・テーマ］ **詳細**は**裏面**をご参照ください／**1回ごとでもご受講いただけます**

第1回	6月4日（木） 10:00～16:00	「サイバー攻撃の動向と企業に求められる技術対策」 ～サイバー攻撃発生時に、初動対応の方向性を判断できる～ （1）最新の攻撃の傾向と攻撃内容・グループの動向 （2）ダークウェブ閲覧と情報流出対応 （3）インシデント初動対応で求められる技術と判断
第2回	6月15日（月） 10:00～16:00	「通信ログの解析手法とOSINT活用」 ～ログや公開情報から異常を把握し、調査につなげられる～ （1）通信の仕組みとサービスについて （2）コマンドやツール（Wiresharkなど）を使った通信状況の確認方法 （3）OSINTの活用による流出確認と対応策
第3回	7月2日（木） 10:00～16:00	「脆弱性とWindows・Linuxログ調査、生成AIでの脅威」 ～調査結果を整理し、社内へ分かりやすく説明できる～ （1）Webアプリの脆弱性解説と技術対策 （2）パソコンのフォレンジック方法と解析、社内への説明 （3）AIエージェント含めた生成AIでの攻撃の脅威

［対　象］ 情報システム担当者・情報セキュリティ担当者
初級インフラエンジニア（サーバエンジニア、ネットワークエンジニア、セキュリティエンジニア）

［会　場］ 静岡県男女共同参画センター「あざれあ」（静岡市駿河区馬渕 1-17-1）

［講　師］ 但野　正行　氏　（ValueUpLab 株式会社　代表取締役社長）
取締役 CTO 技術開発部部長や技術フェローを歴任し、ValueUpLab(株)を設立。これまでサイバーセキュリティ教育で**800名以上を指導**した実績を持つ。**開発と講師のいずれも担える数少ないエンジニア**の一人。21年から静岡県警察「サイバー犯罪対策テクニカルアドバイザー」。本講座5年目で受講者からの評価も高い。

［定　員］ 15名（最少催行人数各回5名）

［受講料］ 全3回セット **89,000**円（税別）/名（税込97,900円）　***10,000円（税別）お得です！***
1回ごと **33,000**円（税別）/名（税込36,300円）

［その他］ パソコンをご持参ください。

［お申込］ メールでお申込いただけます（**裏面**をご参照ください）
【申込〆切】全3回セット：5月25日（月）まで（各回お申込みは開催10日前まで）
＊キャンセルにつきましては、裏面「キャンセル及びキャンセル料について」をご参照ください。

〈浜松開催〉 同じ内容を浜松（クリエート浜松）でも開催します。
日程　第1回　6月10日(水)　第2回　6月24日(水)　第3回　7月6日(月)

［カリキュラム］

回	テーマ・日時	内　容
第1回	サイバー攻撃の動向と企業に求められる技術対策 6月4日(木)10:00～16:00	①IPA「10大脅威2026」を、サイバーセキュリティ専門家の視点で解説します。 ②最新のサイバー攻撃の内容やグループの動向の変化についてお伝えし、企業が実施すべき対策方法について技術面も含め学びます。 ③一般では閲覧が難しい「ダークウェブ」にアクセスして受講者とともに閲覧し、ダークウェブの実態と脅威を認識し、あわせて情報流出時に「何から対応すべきか」の判断ポイントを学びます。
第2回	通信ログの解析手法とOSINTの活用 6月15日(月)10:00～16:00	①OSIやTCP/IPなど通信の仕組みとサービスを理解します。 ②上記を踏まえ、ネットワークプロトコル解析ソフト「Wireshark」を使った通信状況の確認と解析の演習を行います。 ③一般公開情報を収集し分析する「OSINT」の活用方法から、OSINTを通じた情報流出の確認、対応の優先判断の考え方を学びます。
第3回	脆弱性の体験とWindows・Linuxのログ調査、生成AIでの脅威 7月2日(木) 10:00～16:00	①Webアプリの脆弱性についてエンジニアの視点から解説するとともに、脆弱性ごとに必要な対策方法を学びます。 ②Windows/Linuxでの各種ログの内容を知り、ログの調査・解析方法から、現場での判断、技術内容を経営層や非エンジニアに伝える際のポイントを学びます。 ③AIエージェントも含めた生成AIの最新技術と、それに伴って進化するサイバー攻撃の脅威について解説します。

＊内容は変更になる場合があります

受講者の声（実務で役立ったポイント／抜粋）

■ **実務でそのまま使える内容だった**

「無償講座では学べない深い内容で、すぐに業務に活かせると感じました」

■ **現場のリアルな話が聞けた**

「実際のインシデント対応に基づいた話が非常に参考になりました」

■ **実務でそのまま使える内容だった**

「受講後すぐにログ確認の手順を社内で共有し、実務に活かせました」

■ **手を動かす演習が分かりやすい**

「Wireshark などを実際に操作でき、理解が深まりました」

［お申込方法］　申込〆切：全3回セット：5月25日（月）／ 1回ごと：各回10日前

■送信先 jinzai@hamanako.co.jp

■件名 「サイバーセキュリティ講座静岡申込」

メールに以下をご記載の上、お送りください。

(1)貴社名
(2)ご住所（郵便番号）
(3)ご担当者 お名前（ふりがな）／部署・役職／電話番号／メールアドレス
(4)受講者 お名前（ふりがな）／部署・役職／メールアドレス／申込形式：全3回セットまたはご希望回

＊受講者が複数名いらっしゃいましたら、人数分ご記載ください。
＊受講者とご担当者が同じ方でしたら、その旨ご記載ください。
＊お送りいただいた情報は、本講座のご連絡のほか、今後の情報提供で利用する場合がございます。

キャンセル及びキャンセル料について

・キャンセルされる場合には、講座開催日（複数日開催の場合は開始日）10日前の17：00までに、メールまたはお電話でご連絡ください。それ以降のキャンセルにつきましては、原則として受講料の全額をご負担いただきます。
・受講者の変更は、キャンセル料は発生いたしません。

［お問い合わせ先］株式会社浜名湖国際頭脳センター　担当：米良・佐藤
TEL：053-416-4002／Mail：jinzai@hamanako.co.jp