情報セキュリティ人材育成プログラム

～情報セキュリティインシデント対応を学ぶ～

デジタル社会の進展に伴い、サイバー攻撃によるリスクが増大し、サイバー攻撃が多様化・高度化している現在、サイバーセキュリティ対策はあらゆる組織にとって最重要課題となっています。

兵庫県立大学大学院　情報科学研究科では、これまで、暗号、情報セキュリティ、ネットワークセキュリティ、サイバーセキュリティなどの幅広い分野で理論と実践の両面から教育・研究に取り組むことにより、高度なサイバーセキュリティ人材の育成を行なってきました。

セミナー概要

本セミナーでは、これまでの研究成果を活用し、企業や組織において実務を行う担当者が、最新のサイバー攻撃の動向と対策を学び、セキュリティインシデントに迅速・適切に対応できるスキルを身につけることを目的としたプログラムを実施します。

開催日時

令和7年9月17日(水) ～ 9月19日(金)

各日 10:00～17:00

➢1日目：インシデント対応の基本的な流れを理解する

➢2日目：攻撃者の立場で標的型攻撃を体験する

➢3日目：実践形式でインシデント対応を体験する

※3日間をかけてのセミナーとなります

参加対象

下記の両条件を満たす方

- ❑ 組織で情報システムに関する実務を担う方
- ❑ 3日間を通じてセミナーに参加できる方

※本セミナーは、ログ解析やフォレンジクスの内容が含まれますので、コンピュータとネットワークに関する基礎知識をお持ちの方のご参加を想定しています。

申込み

❑ **申込みフォーム**

https://forms.gle/TyvuAv2rzjH34aycA

❑ **参加費**

民間組織の所属　　100,000円/人 (税込)

地方自治体等の所属 70,000円/人 (税込)

❑ **持ち物**

無線LANに接続可能なパソコン

本研修で習得できる主なスキル

迅速なインシデント検知と初動対応

インシデント発生時に迅速に異常を検知し、適切な初動対応を行うスキルを習得します。

効果的な被害拡大防止

被害を最小限に抑えるための迅速かつ効果的な対応策を実行するスキルを身に付けます。

復旧と事後対応の計画立案

インシデント後の復旧プロセスをスムーズに進めるための計画立案と、再発防止策の策定を行います。

会場

兵庫県立大学
新長田ブランチ
セミナー室（512）

JR新長田駅
下車 徒歩約5分

〒653-0036
神戸市長田区腕塚町 5-2-1
新長田キャンパスプラザ5階

連絡先

兵庫県公立大学法人
情報セキュリティ人材育成基金 事務局
TEL：078-303-1901
E-mail：p-office@gsis.u-hyogo.ac.jp

演習シナリオのイメージ

組織の従業員が標的型メールを受信しました。従業員は取引先からのメールと認識し、添付されていたファイルをクリックしました。その結果、攻撃者に端末を操作され、機密ファイルが外部に持ち出されました。

インシデントレスポンスの流れ		
検知・連絡受付	インシデント発生 	❑ マルウェアが添付されたメールが標的の組織に送信される。 ❑ 社員がメール内に含まれる添付ファイルを実行し、C&Cサーバより RATがダウンロード・実行される
トリアージ	インシデント発生の連絡 	❑ セキュリティイベントが発生した旨の連絡を受け速やかに関係者に情報を連携する。 ❑ 受領した連絡の情報の真偽を確認するとともに、追加で必要な情報を速やかに収集する。
初動対応	状況把握、対応方針の決定 	❑ イベントがインシデントか否かを判断し、対処中のインシデントがあれば優先順位付けを行う。
復旧措置・回復	インシデント対応の実行 	❑ あらかじめ定められた被害拡大の防止のための暫定的措置（抜線など）を行う。 ❑ インシデントに至った直接的な原因（脆弱性など）を是正する。
事後対応	恒久対策・再発防止策の策定 	❑ インシデント発生前の状態に戻す（データ復旧、システムの再構築、サービスの再開など）。 ❑ インシデントが再発させないため、ソフトウェアのバージョンアップや権限の見直しなどの技術的対策を講じる。
	振り返り 	❑ 関係者でインシデント対応について振り返りを実施する。 ❑ 同様のセキュリティインシデントが発生しないように、セキュリティ耐性の総点検をするとともに、定期的な訓練の実施を決定する。

日程	2025年9月17日(水)	2025年9月18日(木)	2025年9月19日(金)
内容	インシデント対応の基本的な流れを理解する	攻撃者の立場で標的型攻撃を体験する	実践形式でインシデント対応を体験する
受講形態	個人	個人	グループ
時間	10:00 開始～17:00 終了 （昼休みの休憩を含む） ※時間はおおよその目安です。終了時間は、当日の進行によって多少前後することがございます。		
演習シナリオ	SOCからの通報によりマルウェアに感染したことが発覚する。 組織内で感染拡大し、ファイルサーバの機密ファイルが外部に持ち出された。	標的型メールで組織内に侵入した後、ADに横展開する。 永続化やアカウント情報を収集した後、ファイルサーバの機密ファイルを外部に持ち出す。	標的型メールでC&CとDNSで通信するマルウェアに感染する。 横展開によりドメイン管理者権限が奪取され、機密ファイルが外部に持ち出された。

実践で活かせるスキルを身に着ける

サイバー演習では、机上での演習と比較した場合に、端末を実際に操作してハンズオンを取り入れることで、高い学習効果が実現できます。セキュリティインシデント対応の理解や技術的なスキルの向上に関しても、実機を用いたサイバー演習は不可欠です。本セミナーでは組織のネットワーク環境を模した演習環境を利用します。仮想環境で模擬的に発生させたサイバー攻撃を体験することで、実践で活かせるインシデント対応の知識やスキルが身につきます。

1日目

講義内容

- ❑ セキュリティの概念
- ❑ CSIRTの役割
- ❑ インシデントレスポンスの流れ
- ❑ マルウェアの侵入経路

演習内容

- ❑ 検知・連絡受付時の対応
- ❑ プロキシログの調査
- ❑ ヒアリング項目の検討
- ❑ 初動対応策の検討
- ❑ ディスクイメージの調査
- ❑ 表層解析と動的解析
- ❑ インシデント報告書の作成
- ❑ 再発防止策の検討

2日目

講義内容

- ❑ 代表的なサイバー攻撃
- ❑ サイバー・キルチェーン
- ❑ MITRE ATT&CK
- ❑ なぜADを標的にするのか

演習内容

- ❑ ネットワークスキャン
- ❑ エクスプロイトの選定
- ❑ ADへの水平展開
- ❑ 永続化
- ❑ 認証情報の収集
- ❑ SIEMによるプロキシログ調査
- ❑ Windwosイベントログ調査
- ❑ フレームワークを用いた分析

3日目

講義内容

- ❑ タイムラインの重要性
- ❑ インシデント対応に求められるノンテクニカルスキル
- ❑ インシデント対応における経営層の役割

演習内容

- ❑ メールヘッダ解析
- ❑ SPFレコード調査
- ❑ DNSログの調査
- ❑ YARAルールの作成
- ❑ 復旧計画の検討
- ❑ インシデント報告書の作成
- ❑ インシデント対応の振り返り

3つの特徴

01 組織のネットワーク環境を模した演習環境を利用

攻撃者の立場で疑似マルウェアや攻撃ツールを操作する体験や、業者の立場でログから侵害の痕跡を分析する体験を通じて、実践で活かせるインシデント対応の知識やスキルが身につきます。

02 経験豊富な講師・チュータのサポート

セミナーでは複数のチュータが皆様の演習をサポートします。
質問や分からないことは適宜確認しながら進めることもできます。

03 短期集中型の集合演習

3日間の短期間で代表的なサイバー攻撃の全体像を学び、セキュリティインシデントに迅速・適切に対応できるスキルを身につけます。テクニカルなスキルだけでなく、円滑なインシデント対応を実現するためのノンテクニカルスキルについても学びます。