

コースコード：GX-MicroHardening

税込価格：132,000円（税抜価格：120,000円）

日数：1日間

トレーニング内容

Micro Hardening：Enterprise Editionは、サイバー攻撃への対処をゲーム感覚で学べるハンズオントレーニングです。45分間の演習を1セットとし、1日に4セット実践演習を行うことができます。毎回、同じタイミングで同じ攻撃が発生するように設定されているため、チャレンジするたびに少しずつ攻撃の状況を観測し、対処する方法を実際に試すことでどのような事が起こるのか、スリルとクリアする快感を伴って「経験」できます。

- ・参加者は与えられたECサイトのサーバを様々な攻撃から守り、制限時間内に最大の売上を目指してサイトを運用しなければなりません。そのためには、いまサイトに何が起きているのか見極める目、事象を把握するための知識、攻撃に対処するための技術、ECサイトのサービスを止めない運用力が求められます。

- ・参加者は1人で参加でき、サイトの監視と防御に集中することで、攻撃対処の実践経験を効率的にトレーニングする事ができます。

- ・参加者はチームごとにECサイト（サーバ）を与えられ、1日で演習を4セット経験する事ができます。各セットは全て同じ攻撃シナリオで行われるため、セット毎に振り返りができ、何を見落としただか？自分の取った行動や対策が有効だったか？さまざまな角度から確認検証ができ、さらに復習定着まで、極めて短時間に密度の濃いスキルアップを行えます。

培った知識を現実に即した「攻撃への対処」として実践する事で、短時間に大きな経験を積むことができます。企業におけるサイバー攻撃対応の課題解決として、手を動かせるエンジニアを育成する超実践型トレーニングとなっています。

ここに注目!!

トレーニングを通じて、サイバー攻撃の手法・攻撃者の狙い・システムに存在する脆弱性を学びます。サイバー攻撃の検知・対処を繰り返し実践することで、対応方法が定着。企業のセキュリティ人材の育成に必要な「現場の経験」を提供します。

【参考】マンガでわかるMicro Hardening

[サイバー攻撃対応トレーニングMicro Hardening \(株式会社川口設計\)](#)

【情報処理安全確保支援士 特定講習】

このトレーニングは、情報処理安全確保支援士の特定講習（民間講習）に採用されています。特定講習としてお申込みされる場合は、以下ご確認いただき、お申し込みください。

(1) 特定講習受講の事前申告について

特定講習として受講するには、お申込み時に事前申告が必要です。

お申込みページにおいて、

- ・特定講習として申し込むこと
- ・情報処理安全確保支援士の登録番号

をご記入ください。

もし、事前申告がない場合、講習をご受講いただいても特定講習としての受講修了として認められ

ませんので、ご注意ください。

(2) 本人確認について

特定講習は法定講習のため、講習当日に以下の本人確認を行っています。

【講習開始前】

講習開始30分前（9時30分）から受付を行っており、その時にご本人の確認を行います。

以下の2点をご準備し、講習のZoomにログインしてください。（詳細は受講票に記載）

- ・有効な写真付き身分証明書（運転免許証もしくはパスポートなど）
- ・情報処理安全確保支援士登録証（写し）または情報処理安全確保支援士登録カード

【講習中】

ご本人がご受講していることを確認するために、講義中は常にカメラをONにした状態でご受講していただきます。

(3) 修了条件について

特定講習には修了条件があります。本講習の修了条件は、以下の項目の内容を総合的に判断し、修了を判定します。

- ・出席率（75%以上の出席が必要）
- ・演習状況（スコア、積極性、質問内容等々）

情報処理安全確保支援士特定講習については経済産業省のページを参照ください。

[情報処理安全確保支援士特定講習（経済産業省）](#)

ワンポイントアドバイス

Micro Hardening：Enterprise Editionはサイバー攻撃に対応する方法をゲーム形式で学ぶハンズオントレーニングです。トレーニングを通じて、サイバー攻撃の手法・攻撃者の狙い・システムに存在する脆弱性を学びます。サイバー攻撃の検知・対処を繰り返し実践することで、対応方法が定着。企業のセキュリティ人材の育成に必要な「現場の経験」を提供します。

受講対象者

このコースの受講対象者は次の通りです。

- ・情報システム部門のエンジニア
- ・CSIRTメンバーやSOC担当者
- ・セキュリティエンジニアやテクニカルコンサルタント
- ・公開系システムを開発、運用するエンジニア
- ・エンジニア職の新入社員

前提条件

このコースを受講する前に受講者が習得しておく必要がある知識およびスキルは次のとおりです。

- ・インターネットに関する知識
- ・SSHを使いLinuxのリモートホストに接続し、コマンドを実行できること

目的

このコースを修了すると次のことができるようになります。

- ・被害を受けるパターンとその対策について疑似体験を通して学びます。

- ・サイバー攻撃発生時の対応方法をインシデン対応の実経験を通して習得することができます。
- ・インシデント対応に於ける見える化と事前準備の重要性を認識することができます。
- ・インシデント対応の運用とチームコミュニケーションの重要性を経験を通し理解できます。

アウトライン

【1日の流れ】

事前解説：ルールと環境について解説します

インシデント対応演習（1セット45分 x 4セット）：様々なサイバー攻撃からECサイトを
守り、最大の売上を目指すチーム対抗戦

チームディスカッション

解説＆フィードバック

休憩回避および講座終了時間は、講座の進行状況により前後する可能性があります。あ
らかじめご了承ください。