

[初級者向け]

【サイバーセキュリティ防衛の人材育成講座】

e-learning

初級
Lev.3

*プログラム提供・運営

本講座は新しくセキュリティ部門に配属される方にとって役立つ知識を集めた講座です。
セキュリティ体制構築と運営について学んでいただきます。

アプリケーションに潜む脆弱性の危険や保護手法について学んだ後、各種マルウェアやマルウェアに感染してしまった場合の症状について学びます。感染の症状や痕跡は、ネットワークにも残る事があるため、ネットワーク上で感染の痕跡を見つけるための知識について学習して頂きます。

次に、感染した後の対応のうち法律に関わる部分の学習を行って頂きます。個人情報の保護に関連する話や個人情報を悪意あるハッカーが取得するための手法の一つであるフィッシングについての学習を通して攻撃への対処方法を知って頂きます。

日頃使用している検索エンジンに引っかからない情報が検索できるダーク web についての知識、よくあるサイバー攻撃の手法、攻撃がどのように検出され、どうすれば防止出来るのか学習を行う事で、まずは目立つものからであっても、自身で攻撃の検知を行えるようになります。

*受講者特典として組織体制の例、インシデント報告書などのサンプルフォーマットを進呈。

【開催日程】

- ・随時、受講可能（eラーニング形式）
- ・講義時間：約 16 時間（6 か月間、繰り返し視聴可能）

【主な受講対象者】

- ・ プラスセキュリティ人材*を目指される方
- ・ 新しくシステム部門／セキュリティ部門に配属となる方
 - *本来の業務を担いながら IT を利活用する中でセキュリティスキルも必要となる人材のこと
 - *プログラミングの知識やセキュリティに関する資格保有の有無は問いません。

【得られる知識・スキル】

- ・ 情報セキュリティとはなんなのかといった基本的な知識を身に付け、業務を行う上での注意点を気づくことが出来る。

【実施方法】

- ・ eラーニング形式です。インターネットが使用できる環境ならご都合に合わせた時間・場所で受講が可能です。
- ・ お申込み頂いた方には、受講用方法をメールでご案内します。
- ・ 1つのお申込みに対して、1名のみが受講いただけます。

【申込み方法】

別紙の参加申込書に記入の上、事務局あてに、メールでお送り下さい。
お申し込みを受領後、請求書を送付いたします。

【参加費】（税込） 参加費にテキスト（PDF）、修了証を含む。

- ・ 賛助会員 : 30,000 円／名
- ・ 非賛助会員 : 42,000 円／名 *9名以上ご参加の場合は、賛助会員ご入会がお得です。

【全コースのラインナップと本講座の位置づけ】

サイバーセキュリティのコースは、大きく分けて初～上級まで3段階あり、本講座は、**初級 Level.3**です。
*サイバーセキュリティ人材育成講座の全ラインナップの概要は次ページをご参照下さい。

【プログラム】

メニュー	詳細
事前学習テキスト	セキュリティ体制構築と運営
アプリケーションセキュリティ	アプリケーションに潜む脆弱性の危険について
マルウェア	ユーザーが知っておくべきこと
疑わしいアクティビティのブロック	ユーザーは何ができるのか
内部ネットワーク攻撃	一般的な攻撃の種類
サイバーセキュリティと法律	証拠の収集と起訴
フィッシング	フィッシングへの対処
ユーザーのプライバシー	組織ネットワークにおけるユーザーのプライバシー
個人情報漏洩	個人情報漏洩の防止
検索エンジン	ダークウェブ
よくあるサイバー攻撃と動機	攻撃の検出と防止
ホームネットワークの保護	IoT・スマートホーム・デジタルアシスタント
サイバーアウェアネスの向上	サイバーアウェアネスーWhat & Whyー



レベル	到達レベル	実施形態／特徴
上級	Lev.3	○APT 攻撃に関する攻撃ツールと対処概要を理解し、各セキュリティプロダクトのオペレーション能力やフォレンジックやインシデントレスポンス能力を身に付け、幅広い知識とスキルで自社のセキュリティ中核人材を務められる。
	Lev.2	○ペネトレーションテストの計画から報告までの手法が理解でき、脆弱性に関する情報収集手法や、ツールを使用したペネトレーションテストの実施ができる。
	Lev.1	○複数の検出・監視ツールを駆使してサイバーインシデントを検出し、検出したインシデントの初期分析ができる。
中級	Lev.3	○攻撃用のツールを実際に操作することで、防御するための対策を検討できる。
	Lev.2	○調査と証拠保全のツールを使用し、マルウェアの発見駆除を行うことで、未知のマルウェアに対しても対応できる。
	Lev.1	○講義とデモを通じてハッカーの攻撃手順、調査・証拠保全の手法を理解し、初動対応を行える。
本講座	Lev.3	情報セキュリティとは何か。といった基本的な知識を身に付け、業務を行う上での注意点に気づくことができる。
初級	Lev.2	サイバー攻撃を受けた際に実行すべき対応について理解することができ、サイバーセキュリティに対応する業務を行う担当者に協力することができる。
	Lev.1	ハッカーの攻撃手法とその特徴、関連する法律を理解し、サイバーセキュリティに対応する業務を行うことができる。 *SMS や P マークの担当者も該当。
経営者編	Lev.2	○「サイバーセキュリティマネジメント+法務+交渉」の切り口で、実践的な講義・演習を行います。実際に被害にあった場合の対応方法を習得。
経営者編	Lev.1	○経営層として把握しておくべき基礎知識を学習し、善管注意義務を果たすために最低限実施しなくてはならない対応を習得。

***今回募集以外の講座は、ご案内の準備ができ次第、ウェブサイト上にリンクを設定し、参加お申込みいただけるようになります。**

【サイバーセキュリティ防衛の人材育成講座（初級 Level.3）】

参加申込書

E-Mail:innovation@ostec.or.jp

(大阪科学技術センター イノベーション推進室 篠崎宛)

機関名：		
所在地：〒		
TEL：() — FAX：() —		
氏名	所属・役職	メールアドレス

個人情報の取扱いについて

- ・本講座へのお申込みにあたり、個人情報保護のため、(一財)大阪科学技術センターが、適切に取り扱います。
- ・ご記入頂いた個人情報は、本ワークショップの運営・管理等に関するご連絡及び関連する事業等のご案内以外には使用致しません。個人情報の取扱いは、当財団の「個人情報保護規程」に従って対応いたします。