【大阪科学技術センター・スキルシステムズ(株)*・サイバーコマンド(株)*共催】

[中級者向け]
【サイバーセキュリティ防衛の人材育成講座】

Zoom ｳｪﾋﾞﾅｰ　中級 Lev.1

・セキュリティ担当者をもたない小規模事業者（病院・中小企業）の方
・14 分野の重要インフラ事業はおよびサプライチェーン事業者の方
・サイバー攻撃の手口を知り、インシデント発生時の初動対応を習得したい方
　⇒本講座にぜひご参加ください！

＊プログラム提供･運営

デジタル技術の活用（DX）が世界的に加速し、大規模なサイバー犯罪が急増しています。国内でも大企業のサプライチェーン事業者や医療データのサイバー攻撃が増加しており、サイバーセキュリティ人材の育成が喫緊の課題となっています。

国のサイバーセキュリティ戦略に基づき、**2022 年度より、情報通信や電力など 14 分野の重要インフラ事業者＊に求められるサイバー攻撃への備えとしての行動計画**は、責任の所在、攻撃への対応体制、緊急対応の組織作りなどが必要となり、本講座ではこれに対する基本的な対応を含め解説します。

完全に防ぐことのできない**サイバーセキュリティは、事業損失や信用に直結するビジネスリスク**であり、サイバー攻撃への対応は一刻を争います。そのため、IT ベンダーへの委託に依存すると被害が大きくなる事もあり、まずは自社で一時対応として現状把握と初動対応を行えることが望ましいです。

本講座は、サイバー攻撃の手口を理解し、攻撃の検出方法、攻撃を受けた際の調査と証拠保全方法を学ぶことで、**自社がサイバー攻撃を受けた際の初動対応を実践的に身に着けられます。**

＊14 分野の重要インフラ事業者:「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」及び「石油」

【開催日程】

2022 年 **7 月 13 日**（水）9:30～17:30（Zoom によるウェビナー形式）

【主な受講対象者】

・中小企業のキーパーソン（大企業のサプライチェーン事業者、病院等）
・重要インフラ企業のキーパーソン（複数名の受講を推奨）
・サイバー攻撃の手口を理解し、インシデント発生時に自社の初動対応を身に着けたい方
・事業部門において「プラス・セキュリティ」としてセキュリティの知識を身に着けたい方

＊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】

・サイバー攻撃の手口の理解
・複数の監視ツールを駆使したサイバーインシデントの検出方法
・検出したインシデントの初期分析・証拠保全
・サイバー攻撃を受けた際の初動対応の方法

【講師】

・横濱　悠平（サイバーコマンド(株)取締役 CTO、Certified Ethical Hacker：認定ホワイトハッカー）
・浦中　究（サイバーコマンド(株)代表取締役、(一社)情報処理安全確保支援士会　近畿担当理事）

【実施方法】

・オンライン（Zoom ウェビナー）で実施します。
・Zoom を使用できる PC をご用意下さい。（低速の通信回線、低スペックの PC は避けて下さい）
・お申込み頂いた方には、受講用の URL を後日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。

【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、中級 Level.1 です。

＊初級は、6 月より e-learning で受講可能です。

＊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以下をご参照ください。

【プログラム】

メニュー	詳細
①オープニングセッション	トレーニング概要とスケジュールの説明
②ハッカーの視点とその対策	企業システムへのハッキングの手口と検出方法
③被害の実例(物理的/金銭的)	サイバー攻撃を受けた企業等の被害状況の実例の紹介
④各種ガイドライン	経済産業省と IPA が公開した「サイバーセキュリティ経営ガイドライン」をベースに、経営者が進めるべき重要な対策の実施手順や検討のポイント等を解説
⑤自主調査のためのツール解説、対策の推進ロードマップ案の紹介	自社の脆弱性を自主調査するためのツール解説 サイバー攻撃の対策推進のためのロードマップ案紹介
⑥実際のサイバー攻撃と初動対応のデモンストレーション	講師によるサイバー攻撃および初動対応のデモンストレーションを実施
⑦サマリー	1 日のまとめと質疑応答

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着け、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。	世界最高水準のサイバーセキュリティ教育プログラムを提供する CYBERGYM 大阪アリーナ』で実際のサイバー攻撃と対応演習で実践力を習得できます。
	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。	集合研修
	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。	集合研修
本講座	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。	オンライン (ウェビナー)
初級	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出来る。	e-learning で実施。都合にあわせて WEB で期間内に繰り返し受講して効率的に学べます。
	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出来き、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。*ISMS 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。	集合研修で実施
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。	ウェビナーで実施

＊今回募集「中級（Lev. 1)」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します。

【定　員】先着３０名

＊定員超過の場合は、開催日を別途設ける予定です。

【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。
30 名の定員となりますので、お早めにお申込み下さい。

【参加費】（税込）　**参加費にテキスト（PDF)、修了証を含む。**

・賛助会員　：54,000 円／名
・非賛助会員：76,000 円／名　　＊5 名以上ご参加の場合は、賛助会員ご入会がお得です。

【キャンセルについて】

参加者のご都合が悪い場合は、原則、代理の方がご出席ください。
キャンセル料はお振込みの有無にかかわらず下記のとおりです。

キャンセルご連絡日	キャンセル料
開催７日前～前々日(開催当日含まず)	参加料の 30%
開催前日および当日	参加料の全額

＊既にお振込済みの場合は差額をご返金します。返金口座をご連絡ください。

【募集期間と受講のご連絡】

応募締切り：2022 年 7 月 8 日(金)　＊定員に達し次第、締め切ります。

【講　師】

横濱　悠平
（サイバーコマンド(株)取締役 CTO、Certified Ethical Hacker：認定ホワイトハッカー）

2000 年から Sler 数社にてネットワークエンジニアとしてネットワーク、セキュリティ、開発の経験を積む。2003 年～2005 年 中国における飲食店検索サイトを開発、運営。2006 年から東京に戻り、システム開発会社を設立。主に web サービス系の開発事業、プログラマー育成事業を行う。
キャリア当初はネットワークやセキュリティのテクニカルな部分を担当。社内ネットワーク（オンプレ数百台）の設計、構築、実装を担当。その後、web 系の開発を担当する。主に PM やテックリードを担当。

浦中 究
（サイバーコマンド(株)代表取締役、(一社)情報処理安全確保支援士会 近畿担当理事）

国内大手 Sler、世界的なソフトウェアメーカーにて、プロジェクトマネージャ、サービスマネージャとしての実績と、サーバインフラ、ネットワーク、データベース、クラウド、サイバーセキュリティのエンジニアとして経験を積み、ベンチャー企業にて CISO(情報セキュリティ統括責任者)を務めた後、サイバーコマンド株式会社代表取締役に就任。
自社の「ホワイトハッカー育成事業」ではエンジニア育成を自ら行っているほか、一般社団法人情報処理安全確保支援士会の近畿担当理事を務め、近畿地方における「産・学・官・個」の連携推進、活性化のためのイベントを主催するなど、積極的な活動を行っている。

【サイバーセキュリティ防衛の人材育成講座】
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）

＜申込締切日＞

2022 年 7 月 8 日(金)まで

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。