【責任者向けプログラム】

第2回サイバー危機対応机上演習（CyberCREST）ご案内資料

サイバークレスト

2020年1月

独立行政法人情報処理推進機構
産業サイバーセキュリティセンター

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

開催概要(1)

制御システムを有する企業・団体における
戦略的なサイバーセキュリティ対策を学ぶ2日間

サイバー危機対応机上演習※1,2では、制御システムを有する企業・団体のサイバーセキュリティ責任者を対象に、組織を守る為に必要なスキルとメソッドをご紹介します。

ITやOT(Operational Technology)に関する最新のサイバー脅威を学ぶとともに、実践的なインシデント対応(Incident Response, IR)を体験いただきます。机上演習のツールキットを用いて、自組織向けに演習を設計する方法や演習の進め方も学べます。

本プログラムでは、米国サイバー軍経験者、CISO(Chief Information Security Officer)、重要インフラのセキュリティアーキテクト経験者、サイバーセキュリティの博士号取得者など米国サイバーセキュリティ専門家が講師を務めます。

本プログラムで得られること

- 重要インフラ、制御システム、脅威となる組織・人(ハッカー、犯罪組織、ハクティビスト※3等)に重点を置きながら、現在のサイバー脅威の全体像を理解できます。
- 受講者の方々や海外セキュリティ専門家とのコミュニティやリレーションを構築できます。

※1 サイバー危機対応机上演習(CyberCREST: Cyber Crisis RESponse Table top exercise)
※2 米国IronNet Cybersecurity社のナレッジ・ノウハウをベースに、産業サイバーセキュリティセンター提供プログラムとして、IronNet Cybersecurity社とIPAが日本における社会インフラ、産業基盤をもつ企業様向けにオーダーメイドでプログラム開発をしております。
※3 社会的・政治的な主張を目的としたハッキング活動を行う集団

© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence

開催概要(2)

対象者

- 制御システムを有する企業・団体のサイバーセキュリティ対策を統括されている責任者

日程/開催場所

- 日程:2020年2月19日(水)～2月20日(木) 2日間
- 場所:独立行政法人　情報処理推進機構
  東京都文京区本駒込2-28-8
  文京グリーンコートセンターオフィス 8階

定員

- 30名程度
  ※最少催行人員は6名です。

受講料

- 受講料:30万円(税込)
- 受講料に含まれるもの:テキスト代
  ※懇親会・宿泊費・交通費は含まれておりません。

言語サポート

- 本プログラムは英語ベースで行いますが、日本語テキストのご提供、同時通訳(日英)などを予定しております。

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

講師陣

スティーブ・ザルースキー氏（Steve Zalewski）

Levi Strauss & Co.社の副CISO(Chief Information Security Officer)であり、チーフセキュリティアーキテクト、サイバーセキュリティインテリジェンスやインシデント対応のディレクターを歴任。サイバーセキュリティ戦略とインシデント対応組織のマネジメントを担当。前職ではPacific Gas and Electric Company社でエンタープライズセキュリティアーキテクトなどの役職も経験。

ジョージ・ラモント氏（George Lamont）

IronNet社の最高情報セキュリティ責任者。米サイバー軍の第一人者。民間企業へIronNet社のエンドツーエンドサイバーセキュリティソリューション、脅威情報共有フレームワークの一部としてのチーム構築の支援をする。27年間に渡り、サイバー運用と通信において高い評価を受けている。

フェルナンド・マイミ氏（Fernando Maymí, Ph.D.）

IronNet社のプロフェッショナルサービス部門のディレクター。以前は、米陸軍サイバー研究所の課長補佐として、重要な官民提携活動に従事。米国ミリタリーアカデミーでは、コンピュータサイエンスやサイバーセキュリティの講師を務める。政治家、経営者等に対するサイバー関連アドバイザーとして豊富な経験を有する。CISSP All-in-one Exam Guideの著者。

ブライアン・ディクストラ氏（Brian Dykstra）

コンピュータフォレンジックや電子的データ探索、フォーチュン500向けのデータ漏えいのインシデント対応を行うAtlantic Data Forensics社の創立者兼CEO。Mandiant社の共同創立者であり、CIOやプロフェッショナル教育ディレクター、FBIアカデミーでのサイバー犯罪の講師を歴任。CCFP、CISSP、CISSP-ISSAP、CIFI。

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

スケジュール(予定)

1日目（2月19日(水) 10:00～18:15、懇親会 18:30-20:00）

10:00～10:30 オープニング

10:30～13:30 トレーニングセッション

- サイバー脅威
- 企業におけるサイバーセキュリティプログラム
- インシデント対応計画
- ケース・スタディ（実世界のサイバー攻撃事例）

14:30～17:30 ウォーゲーム・セッション（机上演習）

- ウォーゲーム・セッション 1
- ウォーゲーム・セッション 2
- 振り返り

17:30-18:15 基調講演

18:30-20:00 ネットワーキング懇親会

2日目（2月20日(木) 10:00～18:15）

NEW!

10:00～13:15 トレーニングセッション（ツールキット作成演習）

- イベント計画
- シナリオ構築
- ファシリテーション・評価
- 振り返り

14:15～17:30 ウォーゲーム・セッション（机上演習）

- ウォーゲーム・セッション 3
- ウォーゲーム・セッション 4
- 振り返り

17:30～18:15 演習総括・クロージング

※ セッションの時間は目安であり、当日の進行状況により変更される場合があります。
※ 両日共に同時通訳などの日本語サポートを予定しております。
※ ネットワーキング懇親会は、IronNet Cybersecurity関係者との交流を目的としたものになります。懇親会の参加者が少人数となる場合には中止とさせていただく場合がございます。懇親会では通訳がない点につきご留意ください。

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

本演習3つの特徴

特徴①

「2020年東京オリンピックを想定したサイバーインシデント対応の実践演習」

- 2020年東京オリンピックを想定したIRの実践演習を行います。重要インフラの制御システムに対する実際に起こりうるサイバー攻撃シナリオに基づいて、不確実かつストレスの大きい状況下でIRの演習を行います。
- グループワークでは、各受講者に個別の架空の企業における役割をアサインします。攻撃シナリオに基づいて講師から与えられる様々な情報を利用して、IRにおける意思決定・判断を演習します。

NEW!

特徴②

「机上演習を自組織へ展開できるツールキット」

- 毎回好評いただいているウォーゲーム・セッション（机上演習）を自組織で体験するためのツールキットをご提供します。
- 机上演習のファシリテーションや評価方法を学ぶことが出来ます。

特徴③

「米国のサイバーセキュリティ有識者による基調講演」

- 米国重要インフラ企業のCIO/CISOによる講演を予定しております。

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

1日目プログラム詳細（予定）

概要

- IT分野・OT分野における最新のサイバー脅威や、セキュリティインシデントへの対応方法、実際の企業で発生したサイバー攻撃の事例等を学習します。
- ウォーゲーム・セッション（机上演習）を通じて、実際にインシデントが発生した際にどのように対処すべきかを学びます。

研修目的

- ITとOTにおける運用条件、セキュリティの重要度、サイバー空間の脅威や脅威アクターについて理解する。
- インシデント対応のフレームワークやライフサイクルについて理解し、インシデント対応計画について知る。
- セキュリティインシデントの各機関への報告タイミングや手法、また組織内の誰が関与すべきなのかの理解する。
- 実際に米国で発生したサイバー攻撃の事例を理解する。
- 高いストレス状況の中、インシデント発生時に企業は何を優先すべきかを学習する。

ウォーゲーム・セッションの様子
参加者は仮想の企業において、それぞれ役割を与えられ、重大なインシデント発生時にどのように企業は対処すべきかを議論します。
セッションが進むにつれてインシデントの深刻度が大きくなっていく中で、企業の資産をどう保護すべきか、ストレスフルな状況下で意思決定をしなければなりません。

想定シナリオイベント

疑似的な背景・ストーリー（例）

日本政府を敵視しているある組織の工作員たちが、2020年の東京オリンピックの開会式を、自組織の能力を世界に誇示するまたとないチャンスであると捉え、ハクティビスト団体等と協力をして一連のサイバー攻撃を計画・実行

セッション①: 企業に大きな影響を与えうるインシデント（例）

- 業界別のフィッシングキャンペーンを展開
- 電力会社経営者への高度なフィッシング攻撃
- 小規模のOTシステム障害（続き・・・）

セッション②: 2020年東京オリンピックに関する国際的な危機（例）

- 複数の変電所システムでマルウェアによる停電が発生
- オリンピック開催場所近くで爆発が発生、街灯や信号が機能せず人々の避難が困難な状態に　（続き・・・）

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

2日目プログラム詳細（予定）

概要

- 初日に実施したウォーゲーム・セッション（机上演習）の設計方法や演習の進め方を学びます。参加者はイベント計画、シナリオ構築、ファシリテーションの方法等を学習するだけでなく、実際にウォーゲーム・セッション（机上演習）を進行していただきます。

研修目的

- 講師がどのように1日目のウォーゲーム・セッション（机上演習）を設計・実施したのかを理解する。
- イベント計画における体制構築や、シナリオ構築の際のベストプラクティスを学習する。
- 受講者自身が自組織でウォーゲーム・セッション（机上演習）を実施できる。
- 机上演習の評価・振り返りの手法を習得する。

取り上げるトピック

計画

- イベント計画における体制構築の手法を学ぶ。

シナリオ構築

- 良いシナリオとは何なのか、ベストプラクティスやリスクアセスメントの手法を学ぶ。
- 振り返りや与えられた役割を元にシナリオを学ぶ。

実施

- 演習のファシリテーションや評価の手法を学ぶ。
- 与えられたMSEL(Master Scenario Event List)やIR計画を元に評価フォームを改善する。

© Information-technology Promotion Agency, Japan　Industrial Cyber Security Center of Excellence

過去の受講者の感想

- **ウォーゲームセッションがかなりリアリティある内容だった。**シーンに応じて何を考え、何を決めていくか、IR(インシデント対応)が確実に機能することを確認する必要があることを実感をもって理解できる。

- ウォーゲーム・セッションで、**実際にインシデントが発生した場合の判断の難しさを痛感した。**限られた情報と時間で最善の判断ができるように今後も訓練していきたい。

- **実体験に元づく教訓の多い話**は、記憶に残り、今後の参考になった。

- **IR(インシデント対応)計画の必要性を痛感した。**IR計画を作成しておくことで、インシデント対応をスムーズに進めることが出来ると思った。

- インシデントにおいて**意思決定をする人やCSIRT等セキュリティを担当する人にも受講してほしい**。

- テロ組織、国家のようなスキルとリソースを十分に持つ組織に狙われた時にどれくらい大きな被害を想定すべきかを再確認しました。また、**自社が最終ターゲットでなくても攻撃全体のストーリーの中に使われることがあることは今まであまり想定していなかった**ので勉強になりました。

※過去に開催したプログラムでの感想であり、今回のプログラムとは内容が一部異なります。

© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence

お申し込み先・お問合せ先

WEB上の受講申込書に必要事項を記入していただき、**メールにてPDFで送付頂くと共に郵送でお申し込みください。**お申込みいただきましたら、下記担当者よりご連絡差し上げます。

お申し込み先・お問合せ先: 03-5978-7554
coe-promotion-info@ipa.go.jp

担当者: 中山、笹崎

受講申込書送付先: 〒113-6591 東京都文京区本駒込2-28-8
文京グリーンコートセンターオフィス17階
独立行政法人情報処理推進機構
産業サイバーセキュリティセンター 中山宛

締切日:2020年1月31日(金)
(募集定員に到達し次第、募集を締め切らせて頂きますので、お早めにお申し込みください。)

※原則として、ご入金後にキャンセルされる場合でも、返金は致しかねますので予めご了承ください。

【個人情報の取り扱いについて】
弊機構は、本プログラムの申込のためにご提出頂いた個人情報の適切な管理に努めております。ご提供頂いた個人情報は、本プログラムを提供するために必要な範囲(事務処理および講師への当日受講者リストの配布等)で利用させて頂きます。個人情報保護についての詳細は下記のページをご参照ください。https://www.ipa.go.jp/about/privacypolicy/index.html

© Information-technology Promotion Agency, Japan Industrial Cyber Security Center of Excellence