【責任者向けプログラム】

第1回サイバー危機対応机上演習（CyberCREST）
サイバークレスト

ご案内資料

2019年10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

開催概要

第1回サイバー危機対応机上演習
（CyberCREST: Cyber Crisis RESponse Table top exercise）

制御システムを有する企業における戦略的サイバーセキュリティ対策

本演習※1では、サイバーセキュリティ対策の統括部門の責任者を対象に、制御システムを有する企業において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。高度化するサイバー脅威の全体像、制御システムを有する企業を守る適切な方法、自社組織に適用可能かつサイバーセキュリティ投資の根拠となるリスク分析、インシデント管理の実行フレームワークについてご説明します。

目的

- 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※2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します。
- サイバーセキュリティ対策への投資の根拠となるリスク分析を理解します。
- 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)本演習は米国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。
※2)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

開催概要

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を想定しております 。

日程/開催場所

- 日程:2019年11月15日(金)～11月16日(土) 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 13階

定員

- 30名程度

受講料

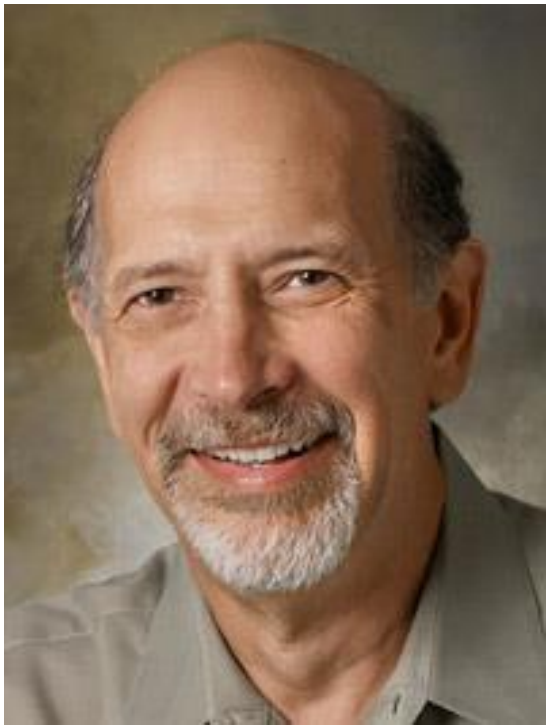
- 受講料:30万円(税込)
- 受講料に含まれるもの:テキスト代

※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

- 本演習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。

特別講演 講師



ポール・モールトン氏
コストコ社副社長兼CIO

世界中のコストコ社のテクノロジーと情報システムを指揮。ワールドワイドでのセキュリティ、インシデント管理やコンプライアンスの責任者。30年以上コストコに在籍しており、25年にわたってコストコの執行役員を務める。

現職への就任前は、倉庫管理者、予算および戦略計画担当取締役、財務担当副社長、企業財務担当者、国際事業担当上級副社長、コストコ・ヨーロッパ担当常務取締役、コストコ・アジア担当取締役社長、エグゼクティブマーケティング担当副社長および不動産開発担当副社長を経験。

コストコ以外では、ヘリテージ大学の前会長、アグロインターナショナルの前会長であり、現在はワシントン州立技術サービス委員会とワシントン大学にて役員を務める。

講師陣

スティーブ・ザルースキー氏（Steve Zalewski）

Levi Strauss & Co社、チーフセキュリティアーキテクト兼サイバーセキュリティインテリジェンス及びインシデントレスポンスディレクター。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。Pacific Gas & Electric Company社の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。

デビッド・ローズ氏（David Rose）

8年以上の経験を持つテクニカルプロジェクトマネージャーとして従事。国際周りやPOV（価値実証）を担当。IronNet入社前は、ブーズ・アレン・ハミルトン（Booz Allen Hamilton）で働きつつ、国家安全保障省（Department of Homeland Security）サイバーセキュリティ担当副次官補（DU / S）特別補佐を務める。

フェルナンド・マイミ氏（Fernando Maymí, Ph.D.）

技術ソリューションの調査・開発・普及に長年従事し、Army Cyber Instituteの元課長補佐として、重要な官民提携活動に従事。現在はSoar Technology社のサイバー関連製品の研究と製品化の取り組みをリード。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。

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。サイバーフォースの第一人者。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。

スケジュール

1日目（11月15日(金) 10:00～18:30、懇親会 19:00-21:00）

10:00～10:10 オープニング

10:10～17:30 トレーニングセッション
（重要インフラ企業における戦略的セキュリティ）

- エンタープライズサイバーセキュリティプログラム
- IRプランの概要と作成方法・ケーススタディ
- サイバーセキュリティにおける環境理解と体制構築・インシデントの優先順位と分類
- 即応的レスポンスガイド・計画のテスト、報告、改善
- まとめと2日目演習への準備

17:30-18:30 特別講演
「セキュリティなき世界におけるセキュリティ」

19:00-21:00 ネットワーキング懇親会

2日目（11月16日(土) 10:00～18:00）

10:00～17:55 ウォーゲーム・セッション
（シナリオに基づいた実践的演習）

- オリエンテーション
- ウォーゲーム（ハッキング対応）
- ウォーゲーム（物理的脅威）
- 振り返りとまとめ

17:55～18:00 クロージング

※ 1日目のセッションの順番については、講師の都合により変更する場合があります。
※ 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。

本演習3つの特徴

NEW!

特徴①

**「昨年参加の皆様から
ご要望の多かった実践的な
インシデント対応計画の作成」**

- 世界トップクラスのセキュリティ専門家から、参加企業に合わせたインシデント対応（IR: Incident Response）計画の作成方法を学びます。演習を通してIR計画の作成について理解を深めます。
- 2日間を通して、自社に適した現実的かつ効率的なIR計画を学べます。

特徴②

**「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。

特徴③

**「米国のサイバーセキュリティ
有識者による特別講演」**

- 米国のサイバーセキュリティ有識者 ポール・モールトン氏（コストコ社副社長兼CIO）が、「セキュリティなき世界におけるセキュリティ」と題して講演します。

過去の受講者の感想

- OTとITの関わりが判りやすく整理されていた点及び基本的な理解へのアプローチの仕方が有益でした。
- インシデントのフレームワークの考え方は実戦的で大変参考になった。BCPと類似しており理解しやすかった。
- 異業種他社の方々と共通のテーマで議論する事で参考となる情報や取組みを共有出来た。
- 私は会社のIT領域の統括責任者であり、先日のWannaCry後に製造、サプライチェーン部門とのOT領域のサイバーセキュリティ対策について話し始めたところでした。そのため今後ディスカッションを進める中でポイントを体系立てて話すことができそうです。
- 2日目の演習が有益であった。組織の中で役割を決め、そのRoleの中で進めていくプロセスを体験でき、いくつか気付きがあった。特にCybersecurityのリスクは企業のリスクマネジメントの一部であると実感した。
- 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。

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:2019年11月8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、本演習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