



Information-technology
Promotion
Agency, Japan

【第一回 国際トレーニングご案内資料】

2018年9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

2018/9/20 : 更新

サイバーセキュリティ国際トレーニング 概要

テーマ

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

- サイバーセキュリティ対策の統括部門の責任者（部門長、CISO、CIO等）を対象とする本セミナーは、制御システム（OT：Operational Technology）を有する企業に軸を置き、企業を守る為に必要なスキルとメソッドを紹介します。
- 高度なサイバー脅威が増加していること、制御システムを有する企業を守るベストな方法とは何か、そして自社組織に適用可能な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理解することが出来ます。

本セミナーの目的

- CISO(もしくはCIO)と海外セキュリティ専門家間のコミュニティやリレーションの構築をします。
- 制御システムを有する企業を防御するためのコンティンジェンシー・プランニング、組織組成、手順に関するベストプラクティスをもとにした討議を実施します。
- 重要インフラ、制御システム、脅威を与える組織・人（ハッカー、犯罪組織、ハクティビト等）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。
- 自社組織に導入可能な、制御システム防御の実行可能なソリューションを参加者に提供します。
- 実際のインシデント発生前に、政府関係者や各機関とのやり取りを含む、インシデントレスポンスの演習を実施します。

サイバーセキュリティ国際トレーニング 本プログラム3つの特徴

本プログラムは米国アイアンネットサイバーセキュリティ社のナレッジ・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、日本における社会インフラ、産業基盤をもつ企業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。

特徴①

「米国エジソン電気協会
スコット・アーロンソン氏
による基調講演」

- 米国エジソン電気協会 (EEI) 副会長のスコット・アーロンソン氏 (経歴後述) による基調講演となります
- 最近のサイバー攻撃動向と、そうしたサイバー攻撃に対処するための官民連携を含めた最先端のアプローチおよび、グローバルな視点からCISOの役割、セキュリティ人材育成について学ぶことができます

特徴②

「ケース・スタディーを通じた
OTサイバー攻撃の対応に
関するベストプラクティスの紹介」

- 米国を中心として実際に過去に発生したOT (Operational Technology) に対するサイバー攻撃のケース・スタディーを実施します
- 各事例毎に、企業によって実際に行われたインシデント準備 (Preparation) とインシデント対応 (Response) について、長所・短所を振り返りながら、最新のベストプラクティスについて学ぶことができます

特徴③

「2020年東京オリンピック
を想定したOTサイバー
インシデント対応の実戦演習」

- 2020年東京オリンピックを想定した、重要インフラのOTに対する疑似的なサイバー攻撃シナリオに基づき、インシデント発生時の不確実且つストレスの大きい状況下で、インシデント対応を実践形式で演習します
- 複数グループに分かれ、各参加者に特定の役割をアサインした上で、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Inputに、インシデント対応における意思決定・判断を演習します

【ご参考】

CISOの役割と知識・スキル

主要な 役割	セキュリティプログラム に係るリーダーシップ	CIOやその他Cレベルの経営層に対して、IT・OTセキュリティ、プライバシーに関するアドバイス提供、および組織大でのセキュリティガバナンスの実行
	ポリシー・コンプライアンス・ 監査対応	IT・OTセキュリティ、プライバシーに関する効果的かつ合理的なポリシー、プロセスの開発・実装の指揮、および監査に関するガイダンスの提供
	リスク管理とインシデント対応	セキュリティリスク管理、コンプライアンス対応、技術的セキュリティ基準の開発・実装・管理、新しい技術のセキュリティへの適用に関するリーダーシップの発揮
主要な 知識・ スキル	セキュリティ機能に 関する深い知識	企業・組織が保有する重要・資産データの保護における全ての側面に関連するIT・OTセキュリティ機能に関する知識
	セキュリティ・プライバシー関連の 法律・基準に関する深い知識	IT・OTセキュリティ、プライバシーに関する法律（連邦法および州法）、業界標準・基準、ポリシーフレームワークに関する知識
	セキュリティ関連の意思決定に おける高いマネジメント能力	組織における部門・個人がIT・OTセキュリティおよびプライバシーに対するリスク管理責務を全うする上で必要となる意思決定とガイダンス
	ID・アクセス管理に関する 深い理解	ID・アクセス管理、および関連する技術やソリューションに関する知識
	企業戦略とセキュリティ要求の バランスを見極め・維持する力	企業における戦略、計画、価値等とセキュリティ要求のバランスを図り、効果的なセキュリティ対応策・解決策を策定する能力
	卓越した対内外 コミュニケーション能力	技術的・非技術的な要員を含む、セキュリティに係る全てのステークホルダー、経営層、外部組織と円滑かつ正しくコミュニケーションする能力
	ハイレベルな対人スキル	セキュリティに関するあらゆるレベルにおいて、技術的・非技術的な要員と円滑に協業するために必要となる対人能力

サイバーセキュリティ国際トレーニング トレーニング受講者の感想

- 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。

サイバーセキュリティ国際トレーニング プログラム全体像（予定）

本プログラムはアイアンネット社のナレッジ・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、日本における社会インフラ、産業基盤をもつ企業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。

1日目 10:00～19:00（※19:00-21:00懇談会）
CIO/CISO向けトレーニング・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）

基調講演：
米国エジソン電気協会 副会長スコット・アーロンソン

IPA産業サイバーセキュリティセンタ関係者 スピーチ：

トレーニング・セッション

CIOの役割と責任

企業のリスク管理・OTとサイバースペースの脅威

サイバーセキュリティとOTに関する企業の防御可能性

サイバーセキュリティインシデントに対する計画と準備・
OT企業のインシデント対応プロセス・ケーススタディ

まとめと2日目演習への準備

ネットワーキング懇親会（スコット・アーロンソン氏他も参加）

2日目 10:00～18:00
CIO/CISO向けウォーゲーム・セッション
（シナリオに基づいた実践的演習セッション）

ウォーゲーム・セッション

オリエンテーション

ウォーゲームセッション（企業レベル）

ウォーゲームセッション（危機対応）

振り返りとまとめ

クロージングスピーチ
テーマ：TBD 登壇者：TBD（予定）

- 1日目のセッションの順番については、スピーカーの都合により、前後する可能性があります。
- 両日共に以下の日本語サポートを予定しております。
 - 1日目（講義）：講義資料の日本語版の配布と日本語サポート要員の配置
 - 2日目（演習）：日本語サポート要員の配置（ご発言の逐次英訳も対応いたします）
- ネットワーキング懇親会には、スコット・アーロンソン氏を始め、IPA産業サイバーセキュリティセンター関係者も参加予定。

サイバーセキュリティ国際トレーニング

講演者プロフィール（1日目基調講演）



スコット・アーロンソン氏
(Mr. Scott Aaronson)

スコット・アーロンソン氏、2009年以来、電力網の近代化、サイバーセキュリティ政策、電気通信の優先事項など、セキュリティといくつかの新技术の問題を政府関係機関で担当してきました。

現在は、EEI（米国エジソン電気協会）の副会長として、セキュリティ・準備チームを率い、電力部門のセキュリティを強化するために、政府と電力会社間などの協力パートナーシップの確立に尽力しています。

また、アーロンソン氏は、電力サブセクター調整協議会（ESCC）の会長も務め、電力セクターが政府とどのように協力して国家の安全を改善するかも検討しています。

スコット・アーロンソン氏、基調講演の実施、及びネットワーキングに参加予定です。

サイバーセキュリティ国際トレーニング プログラム詳細案（1日目トレーニングセッション）

概要

- セキュリティインシデントを特定、管理、解決する上で必須の検討事項について、特にOTセキュリティに焦点をあてて取り上げ、参加者間での経験の共有を通じて、企業・業界・国レベルでのインシデント管理の在り方や改善方法について学びます。

研修 目的

- 自社で適用可能なインシデント管理フレームワークの学習および自社組織における実践能力の獲得
- 過去の主要インシデント（良い事例と悪い事例双方）の理解
- 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
- 通信が利用できない場合や不正アクセスされている場合等の、コミュニケーション方法の学習
- インシデント発生後に組織内で対応を管理改善する手法を取得

予防

- インシデントの発生前に必要となる、組織、ポリシー、プロセスを確立する方法を学ぶ

検知・インシ デント報告

- インシデントマネジメントのための、OT/ITモニター技術、脅威インテリジェンス、報告プロセス、アクティブ脅威ハンティングの応用を学ぶ。「いつ」「誰が」「どのように」インシデント発生を宣言し、対応プロセスの開始を判断するかについて学ぶ。

インシデント 対応原則

- 脅威を把握し、排除し、回復することにおける意思決定戦略とそれに基づいた施策を学ぶ。インシデントマネジメントにおいて、関係者間で共通の状況認識を形成し、法的・倫理的要件を満たすためのコミュニケーション・情報管理の手法を学ぶ。

インシデント 発生後対応

- 最善の対策を打っていたとしても、インシデントは必ず発生する。インシデントのエビデンス情報の収集とその分析方法など、インシデントからの学び、プロセスを改善する方法を学ぶ。

サイバーセキュリティ国際トレーニング プログラム詳細案（2日目：ウォーゲームセッション）

概要

- 2日目は、インシデント対応方法について、疑似的なサイバー攻撃のシナリオと、それに基づいて発生しうる想定イベントに沿って、グループ演習を実施します。
- 【進め方のイメージ（想定）】
- ✓ 5～7名程度/1グループの複数グループに分かれて演習を実施
 - ✓ 各グループを疑似的な重要インフラ事業者として見立て、各参加者にサイバーセキュリティ・インシデント対応におけるステークホルダーの役割を割当て（CISO、リスクマネジメント室長など）
 - ✓ シナリオ・イベントに沿って講師から与えられる様々な課題に対して、グループ内で討議の上、インシデント対応を実践する

研修 目的

- 1日目で学んだインシデント管理フレームワークを活用し、インシデント発生時の、不確実且つストレスの大きい状況下で、対内外コミュニケーション・連携を通じて、いかに効率的、効果的にインシデント対応・管理をすべきかを実践的に学ぶ



※セッションイメージ

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人员たちが、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



想定 シナリオ イベント

シナリオ①：企業に大きな影響を与えるインシデント（例）

- 各業界別のスパ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スパフィッシング攻撃
- 小規模のOTシステム障害（続き…）

シナリオ②：2020年東京オリンピックに関する国際的な危機（例）

- 複数の変電所のPLC内のマルウェアによって停電発生
- オリンピック開催場所近くで爆発が発生、しかし街灯や信号が機能せず人々の避難が困難な状態に（続き…）

サイバーセキュリティ国際トレーニング 講師陣紹介



**スティーブ・ザルースキー氏
(Steve Zalewski)**

Levi Strauss & Co社における、サイバーセキュリティインテリジェンスおよびインシデント対応担当チーフセキュリティアーキテクト兼ディレクター。グローバルサイバーセキュリティ戦略とサイバーセキュリティインシデント対応組織の管理を担当。それ以外にも、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を経験。



デビッド・ローズ氏(David Rose)

8年以上の経験を持つ技術プロジェクトマネージャーであり、製品やサービスの契約を成功裏に完了するための取り組みを推進している。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）を特別補佐として支援。



**フェルナンド・マイミ氏
(Fernando Maymí,
Ph.D.)**

革新的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。サイバーフォース準備の第一人者。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を支援。27年に渡るサイバー運用とあらゆる通信における功績。脅威情報共有フレームワークの一部として、スキルの高いチームの構築。米輸送軍の準備および作戦部門補佐官の軍歴を通して、通信ネットワークの構築に従事。

サイバーセキュリティ国際トレーニング 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。（部門長、CISO、CIO）

日程/開催場所

- ・ 日程：2018年11月2日（金）～11月3日（土）
- ・ 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二丁目28番8号
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

- ・ 受講料に含まれるもの：事前資料、テキスト代
- ※1日目終了後の懇談会、宿泊費・交通費は含まれておりません。
- ・ 受講料 2日間30万円（税込）

※原則として、納入後の受講料は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。

サイバーセキュリティ国際トレーニング お申し込み先・お問合せ先

募集期間

第一回（2018年11月2日～3日開催）の募集期間は、2018年9月28日までと致します。（募集定員に到達し次第、募集を締め切りとさせていただきますので、お早めにお申し込みください。）

お申し込み方法

WEB上の受講申込書に必要事項を記入していただき、郵送でお申し込みください。

※お申込みいただきましたら、担当者よりご連絡差し上げます。

お問い合わせ先： 03-5978-7554（直通）（受付時間）平日9:30-18:00
coe-hrd-info@ipa.go.jp

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

URL：<http://www.ipa.go.jp/icscoe/index.html>

【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）で利用させていただきます。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。

<http://www.ipa.go.jp/about/privacypolicy/index.html>