2023年度 【責任者向けプログラム】
サイバー危機対応机上演習（CyberCREST）
ご案内資料

2023年11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

プログラム概要（１）

**世界情勢の不確実性を背景に高まるサイバー攻撃の脅威に備え、
レジリエンス強化を目指す企業や団体の責任者層に不可欠な
サイバーセキュリティの知識やスキルを学ぶ3日間**

昨今の世界情勢や国際問題を契機に、経済安全保障上のサイバーセキュリティへの懸念は日々高まっています。世界各地にサプライチェーンを展開する日本の企業にとって、海外子会社や現地サプライヤー等のセキュリティ対策は喫緊の経営課題であり、グローバルな視点からのサイバーセキュリティ対策や、近年急速に発展する生成AIによるサイバーセキュリティリスクを理解し、管理するための戦略を含むレジリエンス強化は不可欠です。

本プログラムは、制御システムを有する企業や社会インフラ・産業基盤を担う企業のサイバーセキュリティ責任者が、将来より良いCISOとして活躍するためにさらなるスキル向上を目指し、実践で使える技術・知識・経験を供与します。

プログラム概要（２）

本プログラムで得られること

- グローバル視野の最新サイバー攻撃の動向及び攻撃手口に対する対応力の向上
- 意思決定者として攻撃に対してプロアクティブに対応できるマインドの醸成
- 産業制御システムを狙うサイバー攻撃者の戦術(Tactics)・技術(Techniques)・手順(Procedures)の理解
- 国際的にビジネスを展開する企業におけるセキュリティ専門家の基調講演により、地政学的なサイバー脅威の現実と対策の在り方の理解
- 急速に活用が広まる生成AIによるサイバーセキュリティ上のリスクの理解、および管理するための戦略
- 同じ意思決定層である他の受講者の方々とのコミュニティやセキュリティ専門家とのリレーション構築

プログラム概要（3）

プログラム要項

受講対象	国内外にサプライチェーンを展開する企業や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（CISO)やサイバーセキュリティ対策部門の管理者層 CISO候補者 将来CISOを目指す方
日　時	2024年1月30日(火) ～ 2月1日(木) 10:00 – 17:00 (終日　3日間)　※昼休憩等、適宜休憩がございます
場　所	東京都文京区本駒込２－２８－８　文京グリーンコート　15階 独立行政法人情報処理推進機構　会議室
受講料	30万円(税込)　※受講料に交通費、食事代等は含まれません
募集定員	30名（最大）　※定員に達し次第、締め切ります

プログラム内容(時間割) 1日目

1日目 OT環境へのサイバー攻撃の脅威

	時刻	内容
午前	**10:00 ~ 10:45**	**オリエンテーション、机上演習のチーム編成用アセスメント**
		（休憩）
	10:55 ~ 11:45	**産業制御システムセキュリティの動向と生成AIの動向**
	11:45 ~ 12:00	**ICS アーキテクチャ、HMI の役割**
	12:00 ~ 13:00	（昼休み）
午後	**13:00 ~ 13:50**	**ICS のセキュリティポリシーと標準**
		（休憩）
	14:00 ~ 15:30	**サイバー攻撃デモ**（途中10分休憩挟む）
	15:30 ~ 15:50	**IT とICS のセキュリティの相違点**
		（休憩）
	16:00 ~ 17:00	**ICS 環境での攻撃経路**

※ すべてのプログラム内容ごとに、質疑応答10分の時間を設けます

プログラム内容(時間割) 2日目

2日目 攻撃の実態、インシデントへの対処

	時刻	内容
午前	**10:00 ~ 10:50**	**産業制御系分野のサイバー攻撃事例**
		（休憩）
	11:00 ~ 12:00	**OT システムへの攻撃デモ**
	12:00 ~ 13:00	（昼休み）
午後	**13:00 ~ 13:50**	**利用可能な保護ツール**
		（休憩）
	14:00 ~ 14:30	**ICS ネットワークの保護**
	14:30 ~ 15:00	**物理セキュリティ**
		（休憩）
	15:10 ~ 15:50	**インシデント対応計画**
	15:50 ~ 16:00	（休憩）
	16:00 ~ 17:00	**基調講演：イスラエルELTA社** ※ 基調講演のスピーカーは変更となる可能性がございます。

※ すべてのプログラム内容ごとに、質疑応答10分の時間を設けます

プログラム内容(時間割) 3日目

3日目 机上演習

	時刻	内容
午前	**10:00 ~ 10:30**	**オリエンテーション** 演習の目的と流れの説明/セキュリティインシデントの基本原則の確認
	10:30 ~ 11:20	**シナリオ紹介とブリーフィング** 2023年のサイバー攻撃トレンドのレビュー/国家脅威アクターによるサプライチェーン攻撃のシナリオ説明 （途中10分休憩挟む）
	11:20 ~ 12:00	**役割分担と戦略会議**
	12:00 ~ 13:00	（昼休み）
午後	**13:00 ~ 15:00**	**机上演習・シミュレーション実施** （途中10分休憩挟む）
	15:00 ~ 16:30	**分析とフィードバック** インシデントの分析とレスポンスの評価/セキュリティ対策の強化提案
	16:30 ~ 17:00	**総括と次のステップ** 演習総括/長期的なセキュリティ強化の計画立案

講師陣（講義）

松山哲也　講義（1-2日目）

大日本印刷株式会社（DNP）
ABセンターサイバーセキュリティ事業開発ユニット　セキュリティサービス部　リーダー
入社時よりホログラムの複製プロセス開発、設備開発、品質設計を担当、製品分野は光学用途、偽造防止、ブランド保護、加飾（プリクラ向け等）。その後、生産総合研究所にて溶融型熱転写プリンタの設計・開発、及びプリンタを用いた製造プロセス設計に従事。ジェネラルマーケティングの業務を経験した後、サイバーセキュリティの販促、コース開発や講師業務に従事。

紀伊国 啓　講義（1-2日目）

株式会社DNP情報システム　サイバーナレッジアカデミー事業本部　セキュリティコンサルティング部　主幹企画員
セキュリティ監査、セキュリティポリシー作成、セキュリティ教育に従事。2016年3月よりサイバーナレッジアカデミーにてCyber Rangeのシステム企画・導入・販売支援業務やインシデントレスポンスマネジメントコースの教育等に従事。　GIAC Certified Forensic Examiner, GIAC Web Application Penetration Tester, GIAC Certified Forensic Analyst,　情報処理安全確保支援士 第025949号を保持

半田 富己男　講義（1-2日目）

大日本印刷株式会社（DNP）
ABセンターサイバーセキュリティ事業開発ユニット　セキュリティサービス部　主席研究員
情報システム部門を経て、研究開発部門でICカードOSへの公開鍵暗号アルゴリズム実装の研究開発に従事。「CRYPTREC 暗号運用委員会」委員、ISO/TC68 国内検討委員会委員等を歴任。
CISSPを保持。

講師陣（机上演習・基調講演）

名和 利男　机上演習（3日目）

株式会社サイバーディフェンス研究所
専務理事 上級分析官

航空自衛隊において、信務暗号・通信業務／在日米空軍との連絡調整業務／防空指揮システムなどのセキュリティ担当（プログラム幹部）業務に従事。その後、国内ベンチャー企業のセキュリティ担当兼教育本部マネージャ、JPCERTコーディネーションセンター 早期警戒グループのリーダーを経て、株式会社サイバーディフェンス研究所に参加。防衛産業領域、原子力発電・核物質防護領域、宇宙システム領域などにおいてサイバー演習（机上演習）の実施支援に注力。

Avi Atzur　基調講演（2日目）

ELTA Systems社
サイバーセキュリティチームリーダー

イスラエル空軍（IAF）にて通信・制御技術業務に従事。2013年より、イスラエル電力公社(IEC)にて物理セキュリティ、サイバーセキュリティを担当。ELTA Systemsにてサイバーセキュリティ研究チームをリードし、OT、SCADA、レーダー、航空セキュリティに豊富な経験を持つ。

お申し込み先

募集期間

令和5年度責任者向けプログラムCyberCREST（令和6年1月30日～2月１日開催）
の募集期間は、**令和6年1月23日（火）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頂きますので、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ご記入後、**メールにてPDFをご送付ください。**
※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。

申込みURL：

https://www.ipa.go.jp/jinzai/ics/short-pgm/cybercrest/2023.html

お問合わせ先

電話：　　03-5978-7554（直通）

受付時間：　　平日 9:30-18:00

メールアドレス：　　coe-promo-ap@ipa.go.jp

担当者：　　お申込みに関すること・・・鈴木/北村

演習内容に関すること・・・豊田/高見沢

※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。

【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URLからご確認ください。
https://www.ipa.go.jp/privacy/index.html

ご参考）ICSCoE 短期プログラム 一覧

産業サイバーセキュリティセンター（ICSCoE）では以下のプログラムを提供しています。
課題や学び方（演習形式）に合わせてお選びいただけます。

受講者層	対象企業・団体	課題	学び方	受講プログラム名
責任者/ 責任者になる方	社会インフラ/ 産業基盤に関わる	**企画（体制、予算、ポリシーなど）立案スキル**を学びたい	**提言シミュレーション演習** 企画立案、経営層への提言をシミュレーション	**サイバーセキュリティ企画演習** **CyberSPEX**
	制御システムのユーザー/ベンダー	**業界に特化**した事例で学びたい **サイバーレジリエンス**能力を強化したい	**ディスカッション** インシデントリスクや国内外の規制動向への対応を想定したシナリオを用いた演習	**業界別サイバーレジリエンス強化演習** **CyberREX**
		グローバルな脅威への対策・対応を学びたい	**机上演習** 国家脅威アクターによるサプライチェーンへの攻撃などのシナリオに基づいた演習	**サイバー危機対応机上演習** **CyberCREST**
実務者	制御システムのユーザー/ベンダー	**産業用制御システムの実践的な防御法**を学びたい	**ハンズオン演習** 模擬システムを用いたサイバー攻撃と対応のハンズオン演習	**制御システム向けサイバーセキュリティ演習** **CyberSTIX**
	ERAB事業者（AC, RA）等	**ERAB事業者に求められるサイバーセキュリティ対策**を学びたい	**オンライン講義/演習** ERAB模擬システムへの攻撃実演・リスク分析の実演および演習	**ERABサイバーセキュリティトレーニング**

【更新日】2023年12月8日
2023年度　サイバー危機対応机上演習（CyberCREST）ご案内資料
https://www.ipa.go.jp/jinzai/ics/short-pgm/cybercrest/2023.html

【発行元】独立行政法人情報処理推進機構

https://www.ipa.go.jp/