2024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

2024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）

DX化促進を背景に高まる新たなサイバー攻撃の脅威に備え、レジリエンス強化を目指すグローバル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プログラム

DXの進展に伴い、OT環境における業務効率の向上が期待される一方、新たなサイバー脅威への対応が喫緊の課題となっています。特に海外拠点におけるOTシステムは、各国の異なる法規制やインフラ環境に影響を受けやすく、セキュリティリスクが高まっています。これを背景に、DX化によるOT領域のリスクと海外拠点のセキュリティ強化に焦点を当て、具体的な軽減策を検討し、リーダー層が国際的なOTセキュリティ戦略を強化するための実践的な知識やスキルの習得するプログラムを提供します。

グローバルにビジネスを展開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・経験をオンデマンド講習および机上演習を通じて供与します。

プログラム概要（２）

本プログラムで得られること

- 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
- 海外拠点を有するグローバルに展開する企業の経営陣の視点から、地政学的なサイバー脅威の現実と対策の在り方の理解
- 机上演習を通じて、最新の攻撃手法を踏まえたインシデント対応を実践的に体験し、新たな脅威動向を理解するとともに、既存のセキュリティ戦略における改善すべき点を発見し、実務に活かせる洞察を深める
- 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 ※本プログラムは、日本の社会インフラ・産業基盤を守ることを目的に設計されたプログラムです。 日本国籍を有することを条件とし、これらを満たさない場合、受講をお断りさせて頂く場合がございます。 予めご了承ください。
実施日程	【オンデマンド学習コンテンツ配信期間】 2024年12月26日(木) ～ 2025年1月24日(金) ※机上演習のご参加は、上記期間にオンデマンド学習上で提供するミニクイズの回答が必須です。 (動画視聴は任意) 【机上演習-集合研修】 2025年2月12日(水)、13日(木) 10:00 – 17:00 (終日 2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

シラバス　①オンデマンドコンテンツ

オンデマンド学習コンテンツ　<配信期間　12/26(木)~1/24(金)>

	プログラム内容 ※ ()内は動画再生時間の目安	到達目標
第1部	1-1. 産業制御システムセキュリティの動向(60分) 1-2. ICS アーキテクチャ、HMI の役割(60分) 1-3. ICS のセキュリティポリシーと標準(60分) 1-4. サイバー攻撃デモ(90分) 1-5. IT とICS のセキュリティの相違点(30分) 1-6. ICS 環境での攻撃経路(60分)	• 産業制御システムの特性とサイバー攻撃の実態を知り、産業制御システムへのサイバー攻撃の脅威を理解する。 • リーダーシップを発揮できるよう、攻撃のデモやケーススタディを通して、サイバー攻撃者の戦術(Tactics)・技術(Techniques)・手順(Procedures)を理解する。
第２部	2-1. 産業制御系分野のサイバー攻撃事例(60分) 2-2. OT システムへの攻撃デモ(60分) 2-3. 利用可能な保護ツール(60分) 2-4. ICS ネットワークの保護(30分) 2-5. 物理セキュリティ(45分) 2-6. インシデント対応計画(45分)	• 産業制御システムへのサイバー攻撃の実態を知り、インシデントへの対処を習得する。 • 実際にサイバー攻撃を受けた場合に、攻撃に対し意思決定者としてプロアクティブに対応できるマインドを醸成する。

- オンデマンド学習の1コンテンツは、再生時間15分程度。トータルの再生時間は11時間程度です。
- コンテンツ毎(終了後)に、内容確認のミニクイズが設定されています。
- オンデマンド学習コンテンツの動画視聴は任意です。
  ただし、ミニクイズの回答は、集合研修の机上演習参加前に必須となります。<ミニクイズ回答期限　1月24日(金)>

シラバス　②机上演習・基調講演

机上演習および基調講演　＜集合研修2日間：2025年2月12日(水)、13日(木)＞

	プログラム内容	目的	到達目標
1日目	1. 基調講演 2. ケーススタディ	・企業におけるDX化と海外拠点のセキュリティ強化を、経営者視点で学ぶ ・国家脅威アクターの概要、及び彼らのサイバー空間での活動とケーススタディを学ぶ	• DX化の推進とリスクを知り、リスク低減のためのセキュリティ強化を理解する • 海外拠点のセキュリティ強化の際に必要な知識を身につける
	【机上演習　-1日目】 1.イントロダクション 2.インシデントレスポンス・プレイブックの概観 3.インシデント検出と分析 4.対応と緩和策 5.復旧と事後分析 6.セキュリティ戦略の見直しと強化	・最新のインシデントレスポンス・プレイブックを基に、DX化によるOT環境での新たなサイバー脅威への対応方法を習得する ・2024年のサイバー攻撃手口を基にしたシナリオを通じて、OT環境に適した実践的な対応策を学ぶ	• DX化に伴うOT環境のインシデントレスポンス手法の理解と評価 • OTシステムへのサイバー攻撃手口の分析と、それに基づく対応力の向上 • 各国の法規制やインフラ環境に基づいたセキュリティ対策の見直し • 様々なシナリオを通じて、OT環境での冷静かつ効果的な対応力を身につける
2日目	【机上演習　-2日目】 1.イントロダクション 2.インシデントレスポンス・プレイブックの応用 3.インシデント検出と分析 4.対応と緩和策 5.復旧と事後分析 6.セキュリティ戦略の見直しと強化 7.プログラム全体の振り返りワーク	・1日目の学習を基に、OT環境での実践的なシナリオを通じて、具体的なセキュリティ対策を強化する ・海外拠点におけるセキュリティ戦略を見直し、法規制や環境に対応したOTセキュリティ強化策を検討する	• 実際のシナリオを通じてインシデントレスポンス手法を応用し、OT環境での対応力を強化 • 海外拠点ごとのリスクと法規制を考慮したセキュリティ戦略の再構築 • インシデント発生時の復旧と事後対応を強化し、OT環境における継続的なセキュリティ改善を提案 • チーム全体での対応力向上を図り、各国拠点における実効的なチームワークを実現する

講師陣（机上演習・基調講演）

名和 利男　机上演習　<2025年2月12日(水)、13日(木)実施>

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。

金沢 貴人　基調講演　<2025年2月12日(水)実施>

大日本印刷株式会社(DNP)
常務取締役、ABセンター長、情報システム本部担当、情報セキュリティ委員会委員長、技術・研究開発本部ICT統括室担当

研究開発部門に長らく携わり、印刷原版を作成するCADシステムの設計開発などに従事した後、製造の技術部門、企画部門を経験。現在はABセンターなどの新規事業創出部門と情報システム本部、技術・研究開発本部ICT統括室を担当、情報セキュリティ委員会 委員長（DNPグループのCIO、CISO）。BIPROGY取締役（非常勤）も兼務する。

講師陣（オンデマンド配信講座）

松山哲也

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

株式会社DNP情報システム　サイバーフュージョンセンター　サイバーナレッジアカデミー室
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

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。

お申し込み先

募集期間

2025年 1月15日（水）17：00 まで

（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。

- 受講申込書　ダウンロードページ
https://www.ipa.go.jp/jinzai/ics/short-pgm/cybercrest/2024.html

- 受講申込書　送付先
coe-promo-ap@ipa.go.jp

申込みから受講までの流れ

申込

- 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。**
  受講申込書送付先　coe-promo-ap@ipa.go.jp

受付

- 受講お申込書を受理次第、受講料お振込み依頼のご連絡を差し上げます。

振込

- 受講料のお振込みを確認次第、オンデマンド視聴のご案内(配信システムアクセス方法およびユーザーID）を送付します。

オンデマンド講習

- オンデマンドコンテンツの視聴およびミニクイズ回答　**2025年1月24日(金)まで**
  ※動画の視聴は任意、**ミニクイズ回答は集合研修参加に必須**となります。

集合研修

- 机上演習および基調講演への参加
  2025年2月12日(水)、13日(木) (終日　2日間)

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/奥山

演習内容に関すること・・・豊田/北條

※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

【更新日】2024年11月26日
2024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/2024.html

【発行元】独立行政法人情報処理推進機構
©Information-technology Promotion Agency, Japan（IPA）
https://www.ipa.go.jp/