第8期中核人材育成プログラム（令和6年7月開講）
カリキュラムご案内資料

独立行政法人情報処理推進機構（IPA）

育成する産業サイバーセキュリティ人材

- OT(制御技術)とIT(情報技術)**双方にわたる技術的なスキル**を備え、リーダーシップなどの**業務推進能力**、**セキュリティ専門家などとの人脈**も有し、経営層と現場を繋ぐ橋渡しとして、**組織全体のサイバーセキュリティ対策の中核となる人材**

概要

- 将来、企業などの経営層と現場担当者を繋ぐ**中核人材**を担う方を対象
- テクノロジー（OT・IT）、マネジメント、ビジネス分野を総合的に学ぶ1年間のトレーニング
- 開始当初2ヶ月の初歩的なレベル合わせからハイレベルな卒業プロジェクトまで実施
- 受講者が自社に近い環境での演習を体験できるよう、各業界のシステムを想定した模擬システムを使用
- 海外のトップレベルのセキュリティ対策のノウハウの獲得等を目的に、海外関連機関との連携トレーニングを実施

中核人材育成プログラム

テクノロジー、マネジメント、ビジネス分野のスキルを総合的に学習 ⇢ 現場から経営層までの幅広い視点で、組織全体、サプライチェーン、業界全体を見据えたセキュリティやビジネスに対する理解

模擬システムを使った実践的演習 ⇢ 現場におけるリスクのより深い理解

海外関連機関との連携トレーニング ⇢ 国内外、業種を超えたトップレベルの人脈

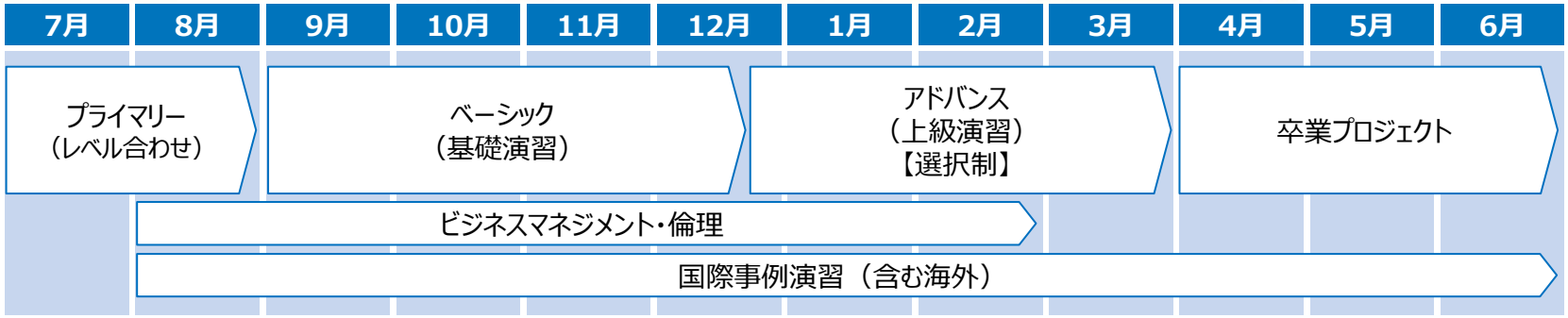
1年間の集中的なトレーニング

派遣元企業

現場（事業部門等） ← 現場におけるリスク評価と実施すべき対策の指示 ― 中核人材 ― 経営戦略上のセキュリティ対策の提言 → 経営層、法務部門、財務部門等

経営層、事業部門、情報システム部門などの企業内の幅広い部門の実務者がチームとしてサイバーセキュリティの課題に取り組む体制を組織

年間カレンダー①（第6期事業の例）



ベーシック期間の技術分野

- IT/OT分野における検知技術・防衛技術・レジリエンス手法等コース
- OTインシデント対応・BCPコース
- ITセキュリティコース

アドバンス期間の技術分野

- IT/OT分野における検知技術・防衛技術・レジリエンス手法等コース
- OTインシデント対応・BCPコース
- ITセキュリティコース
- DXセキュリティ・国際標準コース

プライマリー期間
- ITセキュリティ基礎とOTセキュリティ基礎を学習
- レベル合わせ

ベーシック期間
- 制御システムセキュリティ、ITセキュリティ、BCP等の考え方を網羅的に習得
- 2～3クラスに分かれて、上記技術分野の３コースをローテーションして学習

アドバンス期間
- 特定分野における実践的なトレーニング及び演習の実施による更なる知見の向上
- 上記4分野から２つ選択

卒業プロジェクト期間
- アドバンス期間までで習得した知識や経験を活かし、グループもしくは個人で自らが定めた産業サイバーセキュリティをテーマとした課題に取り組む

年間カレンダー② カリキュラム（第6期事業の例）

	プライマリー	ベーシック			アドバンス		卒業プロジェクト
テクノロジー	情報システム基礎 - コンピュータ構成要素 - システム構成要素 - ソフトウェア - ハードウェア - ネットワーク　等 情報システムセキュリティ基礎 - 情報セキュリティ管理 - セキュリティ技術評価 - 情報セキュリティ対策 - 関連法規 - 標準化関連　等 制御システム基礎 - 制御システムプロセス全体像 - フィールド装置の概要 - プログラミング技法 - 制御システムの種類 - ネットワークアーキテクチャ - 情報システムとの違い　等 制御システムセキュリティ基礎 - 制御システムにおける脅威の現状 - 攻撃のシナリオ - 制御システムとビジネスリスク - セキュアな制御システムの構成 - セキュリティ対策 - 攻撃の検知 - セキュリティ標準規格(CSMS、EDSA等)に基づいたセキュリティマネジメント・アプローチ 安全制御基礎 - 制御システム安全基礎 - プラント運転安全基礎 - 多重防護基礎　等	制御(OT)	IT/OT分野における検知技術・防衛技術・レジリエンス手法等コース	制御システム固有のセキュリティリスクの理解 - 制御システムセキュリティ概論 - 攻撃モニタリング・攻撃体験 - パケットキャプチャ - ペネトレーション - ロギング、モニタリング　等 制御システムへの攻撃に対する防御技術理解 - 防御技術紹介 - 攻撃回避手法体験 - フォレンジック入門　等	制御システム固有のセキュリティ関連技術の取得 - 装置ペネトレーション - ログ改ざん - フォレンジック演習　等 攻撃への防御技術習得 - 防御技術の習得　等 模擬プラントを用いた対策企画立案 - 攻撃防御体験演習 - リスクシナリオ検討　等	グループ／個人プロジェクト（総合演習など） - 受講者がプライマリーからアドバンスに至るまでの知識を活用して、グループもしくは個人にて産業サイバーセキュリティに関する課題解決に向けたテーマを定めて取り組む。 - 最終的には、ステークホルダー（受講者派遣元企業のマネジメント層や上司等）を招待してプロジェクトテーマにて取り組んだ内容の結果を報告。
			OTインシデント対応・BCPコース	安全性と事業継続性を両立するOTインシデント対応 - レジリエンスエンジニアリング - セーフティ＆セキュリティインシデントマネジメント - 制御システムの安全とセキュリティ - 脅威分析・被害想定・対策評価 - 事業リスクと事業継続計画 - リスク・コミュニケーション　等 - 事業継続マネジメント - 制御システム復旧 - リスクアセスメント手法　等 制御システムBCP対応演習（机上） - サイバー攻撃デモ - テストベッド構築 - BCP作成 - サイバー机上演習　等	プラント・制御系の安全/セキュリティ管理 - プラント安全設計・運転 - プラント安全管理(OHSAS18001) - 制御システム安全設計運転 - 制御ネットワーク設計・管理(IEC62443) - 制御システム復旧 - インシデント解析　等 ストレス条件下でのBCMの利活用 - BCP・BCM - インシデントコマンダー - インシデントコマンドシステム等 制御システムBCM対応演習（ドリル） -演習システム構築 -サイバードリル・結果分析　等 (予兆・緊急・復旧フェーズ)	
			個別セッション	IT・OTに跨る課題に関するワークショップ - 実務経験豊富な専門家を招致し、制御セキュリティや、情報セキュリティ及び制御セキュリティに跨るガバナンス（リスク管理、資産管理、内部不正、セキュリティポリシーなど）、組織・体制（物理セキュリティなど）、機器・システムに関わる課題を中心に、受講者と専門家の間で、質疑応答を実施。			
		IT	ITセキュリティコース	制御システムセキュリティ実現のためのIT設計 - 環境構築 - リスクアセスメント - セキュアな設定・環境（資産管理ソフト、アカウント管理ログなど） - ログ分析、情報共有　等 ガバナンス・コンプライアンス - 内部統制 - セキュリティポリシー　等 OT側の可用性を踏まえたITインシデント対応 - インシデント対応演習 - 関連法規・PKI等 - Webセキュリティ　等 企画・体制整備 - CSIRT(インシデント管理対応) - CSIRT（復旧） - IT企画・運用・監査　等	制御システムへの攻撃検知手法の理解・体験 - リスク分析・リスク評価 - NWセキュリティ - 攻撃検知 - 攻撃コード分析 - OS組み込みセキュリティ　等 先進技術 - IoTセキュリティ（概論、企画・設計等）　等 ガバナンス・コンプライアンス - ガバナンス - コンプライアンス - リスク管理（内部統制、外部受託等）　等 制御システムへ攻撃に対するインシデント対応演習 - 事例研究 - インシデント対応演習　等	

海外先進事例・国際標準	海外先進事例紹介 【米国】 - ICS-CERT 【欧州・イスラエル等】 - IRT System X - NCSC - ENCS/Hague Security Delta	海外専門家を招いての最新国際標準 - 国際標準に基づく サイバーセキュリティのモデリング - 国際的な重要インフラのサイバーセキュリティにおける規制体系 - 国際的なサイバーリスク管理体制、など	啓発としての有識者講演 海外イベント・学会参加 - ICSJWG - イスラエルCyber Week　等	DXセキュリティ・国際標準コース	DXセキュリティ・国際標準 - AI,IoT,クラウド,DLT等のセキュリティ課題と対策 - 日米欧の関連法規制、ガイドライン、国際標準、判例
ビジネス・マネジメント・倫理	国内外の法制度 - 国内セキュリティ関連法制度 - 海外セキュリティ関連法制度 - 危機管理　等	現場を動かすマネジメント力 - 組織行動とリーダーシップ - 人材マネジメント　等	マネジメント層に必要なビジネス基礎 - アカウンティング/ファイナンス - プレゼンテーション　等	IT戦略 - セキュリティ投資 - バジェッティング　等	倫理・規範 - ビジネス倫理 - セキュリティ倫理・価値等

年間カレンダー③（第6期事業の例）

- カリキュラムでは、当センターの施設での講義・演習のほか、関連施設やカンファレンス等、海外も含めたフィールドワークも積極的に実施（※以下は第6期事業において実施した視察・演習、及び推奨したイベント等の例）。

海外関連機関との連携トレーニング（過去事業の例）

海外における産業サイバーセキュリティを直に学ぶための派遣演習

- **フランス派遣演習**
  フランス（パリ）の学術機関を訪問し、現地の産業界・大学の研究者らによる講演や、彼らとの意見交換を通じて、サイバーセキュリティの国際的標準を理解するとともに、現地キーパーソンとの人脈を構築。第6期は4/3～6で実施。
  （2017年9月、2018年9月、2019年9月、2021年1月*、2022年5月）

- **イギリス派遣演習**
  在日英国大使館のアレンジにより、英国の政府機関や金融・海運業界におけるサイバーセキュリティの取り組みの事例紹介、ベンチャー企業等を訪問し、彼らとの意見交換等を通じて、英国における官民の取組を理解するとともに、現地キーパーソンとの人脈を構築。
  また、2019年にはNCSCを訪問し、設立背景や組織概要、取組みの紹介を受けた。
  （2018年12月、2019年12月、2020年12月*、2021年12月*）

*はコロナ禍のため、オンラインで交流実施

日本の取組みを発表し、
専門家と意見交換を行う

英国政府による
サイバーセキュリティ戦略の講義

講師陣紹介①（第6期事業の例）

講師略歴

門林 雄基
奈良先端科学技術大学院大学
情報科学研究科 教授

- 産官学連携によるサイバーセキュリティ研究開発に20年以上、サイバーセキュリティ人材育成に10年以上にわたり従事。
- 欧米セキュリティ専門機関とともにサイバーセキュリティ国際標準化を推進。国際電気通信連合電気通信標準化部門（ITU-T）におけるサイバーセキュリティ作業部会の主査を2013年より務め、20件の国際標準を成立。
- 予測困難なサイバーリスクと対峙するために、情報交換とならんで相互理解やプロフェッショナル人脈の重要性を説く。

担当するカリキュラム

- ネットワーク・セキュリティの国際標準
- 国際的なサイバーリスク管理基準
- 国際的なサイバーリスク管理体制
- 国際的に用いられているネットワークセキュリティ手法
- 国際的に用いられているリスク分析・評価手法
- 模擬インシデントの発生前、発生時および事後における規制動向に対応したインシデント対策手法

講師陣紹介②（第6期事業の例）

講師略歴

小林 和真
慶応義塾大学
特任教授

- 通信・放送機構（現NICT）IPv6システム評価検証センター長を務め、JGNの運用を行う、などネットワークに関する研究活動に従事。岡山情報ハイウェイの構築など豊富なネットワークの構築・運用経験を持つ。
- 近年は制御システムセキュリティに関する取組みにも注力しており、平成24年には技術研究組合制御システムセキュリティセンター（CSSC）立ち上げに顧問として参画。制御システムセキュリティの検証や、演習による普及・啓発等に尽力している。

担当するカリキュラム

- 制御システムセキュリティ概論
- パケットキャプチャに関する講義および実習
- ペネトレーションに関する講義および実習
- システムペネトレーションに関する講義および実習
- ロギング、モニタリングに関する講義および実習
- フォレンジックに関する講義および実習
- 攻撃手法および防御技術に関する講義および実習、など

講師陣紹介③（第6期事業の例）

講師略歴

越島 一郎
名古屋工業大学
工学研究科 客員教授

- 昭和54年4月千代田化工建設に入社し、プロセス・エンジニア、アナリスト, エンジニアリング・マネージャとして複数のプロジェクト（水素プラントの設計・建設・運転、イラ–イラ戦時下でのプラント建設からLNG受け入れ基地トレーニングシミュレータや宇宙ステーション「きぼう」搭載の画像取得装置の開発まで）に従事
- 平成10年4月プロジェクトマネジメントを専門に教育する千葉工業大学に移動。
- 平成20年9月より現職、現在重要インフラ防御のための、安全とセキュリティの同時達成を目指した制御システムセキュリティBCP/BCM研究を実施し、その成果を制御システムセキュリティセミナーを通して産業界に提供している。

担当するカリキュラム

- プラント安全設計・安全運転・安全管理
- 制御システム設計
- 脅威分析
- 被害想定・対策評価
- インシデントマネジメント
- 事業リスクと事業継続計画
- リスク・コミュニケーション
- BCP・BCM
- インシデントコマンダー
- インシデントコマンドシステム
- 各種演習（構造分析、結果分析）
- 演習システム構築　など

講師陣紹介④（第6期事業の例）

講師略歴

満永 拓邦
東洋大学 情報連携学部
准教授

- 一般社団法人JPCERTコーディネーションセンターにおいて早期警戒グループマネージャー、技術アドバイザーを歴任し、脅威情報の収集、分析、情報発信に従事。
- 平成27年からは、東京大学情報学環の「セキュア情報化社会研究寄附講座」の中核メンバーとして、サイバー攻撃の実践演習環境（SiSOC TOKYOサイバーレンジ）を東京八重洲に立ち上げ、実地訓練による人材育成とともにハッキング防御技術やセキュリティ耐性の評価を実施している。

担当するカリキュラム

- ITシステム概論
- ネットワークセキュリティ
- セキュリティインシデント緊急対応体制（CSIRT）
- インシデントハンドリング
- セキュリティを意識したITシステムの企画・運用・保守など
- ITガバナンス及び投資戦略
- プロジェクトマネジメント/開発管理
- セキュリティ関連法規
- セキュアプログラミング
- 脅威情報共有スキーム及び国際的な動向および活用
- 攻撃コード分析

講師陣紹介⑤（第6期事業の例）

講師略歴

登 大遊
サイバー技術研究室 室長
筑波大学 客員教授

- 筑波大学入学直後、IPA未踏ソフトウェア創造事業で SoftEther VPN を開発し、スーパークリエータ認定。同ソフトウェアは、経済産業大臣表彰を受賞。
- VPN やコンピュータネットワーク、光ファイバー専用線網のセキュリティなどについて深く研究をし、IPA セキュリティ・キャンプや国のセキュリティ組織等でネットワーク・セキュリティに関する講義などを実施。
- IPAではサイバーセキュリティに関する業務に従事。また、NTT 東日本特殊局、茨城県警察サイバーセキュリティ対策テクニカルアドバイザーなど広く活動。

担当するカリキュラム

- サイバー技術研究奥の院（特別講義）
- 受講者間のコミュニティ形成支援
- サイバー技術研究室室長として、攻撃情報の調査・分析を通して、サイバー技術に関する研究開発や人材育成の支援などを実施。
- センター受講者が実験、卒業演習および修了後も利用できるような、自由で広大なおもしろネットワーク環境の構築と運用。
- 世界にも負けない日本の技術者に最も重要なサイバー技術研究環境やホワイトハッカーのコミュニティ構築形成を支援。