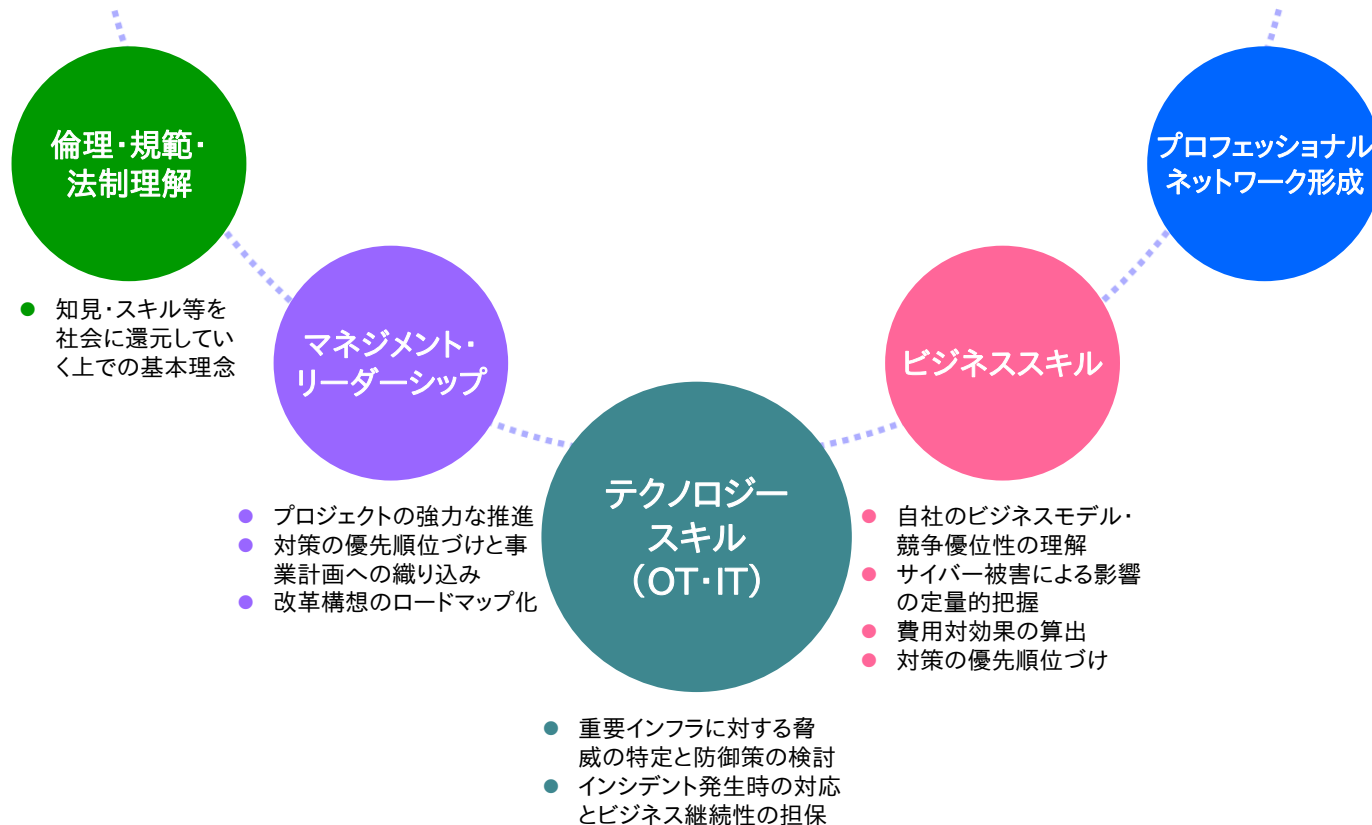


第5期中核人材育成プログラム(令和3年7月開講) カリキュラムご案内資料

独立行政法人情報処理推進機構 (IPA)

- 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核として有し、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する、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



- 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年程度のトレーニング
- 開始当初3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

派遣元企業

一年間の集中的なトレーニング

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

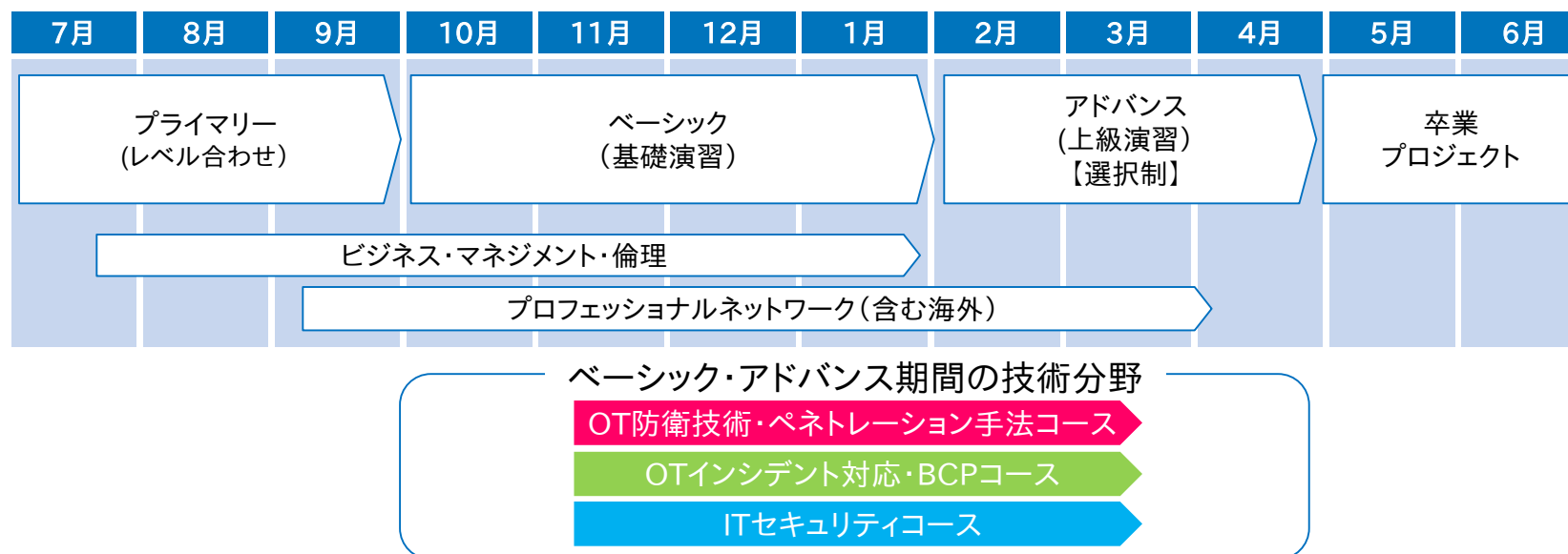
中核人材

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(第4期事業の例。予定を含む)



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
- 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3コースに、「DXセキュリティ・国際標準コース」を加えた4コースから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

カリキュラム(第4期事業の例(予定を含む)。第5期はこれをベースに調整中。以下同じ)



	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) OT防衛技術・ペネトレーション手法コース 制御システム固有のセキュリティリスクの理解 制御システムへの攻撃に対する防衛技術理解 - 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 - ログイング、モニタリング 等 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 制御システムBCP対応演習(机上) - 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 - 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	アドバンス 制御システム固有のセキュリティ関連技術の取得 攻撃への防衛技術習得 - 防衛技術の習得 等 模倣プラントを用いた対策企画立案 - 攻撃防衛体験演習 - リスクシナリオ検討 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)	卒業プロジェクト 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。	
		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 OT側の可用性を踏まえたITインシデント対応 制御システムへの攻撃検知手法の理解・体験 ガバナンス・コンプライアンス 制御システムセキュリティ - 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
		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 - バジエティング 等

- 海外トップレベルのセキュリティ対策のノウハウの獲得、海外有識者との人脈形成等を目的として、海外の産業セキュリティ関連機関との連携トレーニングを実施。
※コロナ禍のため、第4期はオンライン主体にて実施

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

- イギリス派遣演習@オンライン(12月8、9日)
 - 英国政府のサイバーセキュリティにおける取り組みと民間との協力の理解、および現地トップレベル機関やその人材とのネットワーク構築を目的として実施。受講者生26名が参加。
 - イギリスの政府機関(NCSC、英国大使館など)による政策や5G等のセキュリティに関する講義を受講。
- フランス派遣演習@オンライン(1月19日)
 - サイバーセキュリティ専門家から、産業サイバーセキュリティへの取り組みについての講義を受講。具体的には、船舶(港湾)のセキュリティに関する講演など。
- イスラエル企業による特別講演(1月21日)
 - イスラエル大使館の協力を得て、同国政府のサイバーセキュリティ政策、イスラエル電力公社によるインフラ企業における対策に関する講義を受講。
 - イスラエル企業によるセキュリティ技術の解説を受け、技術動向などを学習。





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

- 新しいインターネットアーキテクチャの創出及び体系化や、パケットのトレースバック技術の研究等に従事。
- MITRE社やcisco社等の有名海外企業、EU等との共同研究経験を持つなど国際感覚に優れている。平成29年より「サイバーレジリエンス構成学研究室」を設立し、研究開発、標準化、実証実験、国際協調などを国内外の産官学組織との連携を進める予定。
- 学生向けのセキュリティ人材育成プロジェクトであるenPiT-SecCapの講師を務めるなど、人材育成の取組の経験も豊富。

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り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
- ログイング、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

講師略歴



橋本 芳宏

名古屋工業大学 社会工学科
教授

- プロセス制御、運転支援が主な研究分野であるが、平成23年に経済産業省制御システムセキュリティ検討タスクフォースに参画以来、制御系の安全確保を中心にしたサイバーセキュリティ研究に従事。
- 守り切れないし、いざという時にとれるのは通信の遮断と自動システムを頼りにしない操業という観点で、安全確保だけでなく事業継続のためのサイバーセキュリティを検討。
- 計測自動制御学会プロセス塾講師、SIP重要インフラのセキュリティ人材育成委員、つるまいプロジェクト世話人などを歴任。

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務めており、脅威情報の収集、分析、情報発信に従事。
- 2015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。

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



ICSCoE

Industrial Cyber Security Center of Excellence