【第2回半導体産業サブワーキンググループ】

中核人材育成プログラムについて

2025年3月31日

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

センターの発足背景

- **社会インフラ・産業基盤に物理的なダメージを与えるサイバー攻撃のリスクが増大。海外においては、既に、他国家等からなされるサイバー攻撃により、社会インフラ・産業基盤の安全が脅かされる事案が発生。**

例）製鉄所の溶鉱炉損傷（ドイツ、2014年）、変電所へのサイバー攻撃による停電（ウクライナ、2015年、2016年）など

社会インフラ・産業基盤における、サイバー攻撃に対する防護力を強化することは、国家全体の喫緊の課題

OT(制御技術）とIT（情報技術）の知見を結集させた
世界レベルのサイバーセキュリティ対策の中核拠点
「産業サイバーセキュリティセンター」（ICSCoE）を2017年4月に発足

＜センター長＞

2024年7月1日～
澤田 純

日本電信電話株式会社 取締役会長
経団連副会長

中核人材育成プログラムの概要

日本の社会インフラ・産業基盤の強靭化へ向けて産業サイバーセキュリティ人材を育成

- 将来、企業などの経営層と現場担当者を繋ぐ**中核人材としての役割を担う方**が対象
- 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**
- 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**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・ビジネスを総合的に学習	➡	現場から経営層までの幅広い視点から組織・サプライチェーン・業界全体を俯瞰しセキュリティやビジネスについての知見を深める
模擬システムを使った実践的演習	➡	現場でのリスクをより深く理解
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を形成

派遣元企業

一年間の集中トレーニング

現場（事業・営業部門等） ← 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提言 → **経営層 法務・財務 その他管理部門**

経営層・事業部門・情報システム部門など、企業内の実務者がチームとして横断的にサイバーセキュリティの課題に取り組む体制づくり

中核人材育成プログラム

年間スケジュール

➢ 初歩的なレベル合わせから、ハイレベルで実践的な演習・卒業プロジェクトまでを1年間で実施。

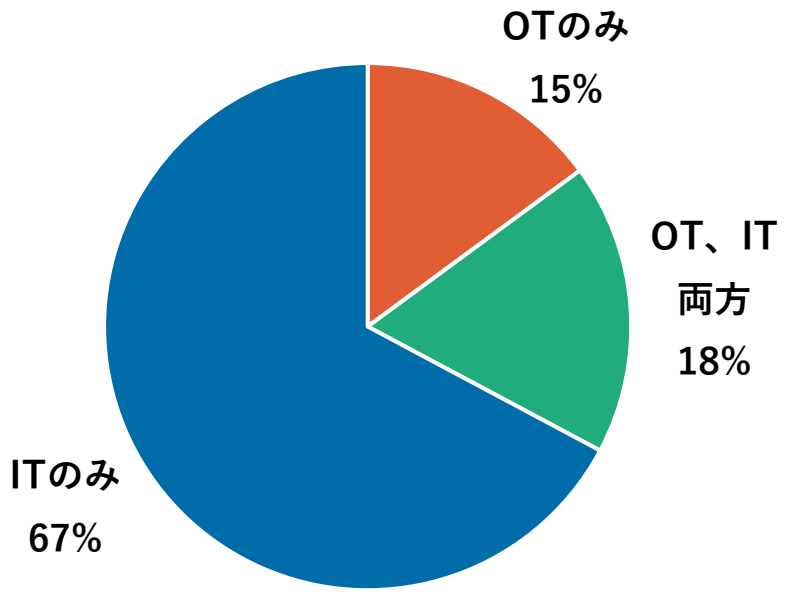
※修了後は、「産業サイバーセキュリティエキスパート」（商標登録番号6158314号）の称号付与。
また、情報処理安全確保支援士試験の全部免除を受けられる。

中核人材育成プログラム

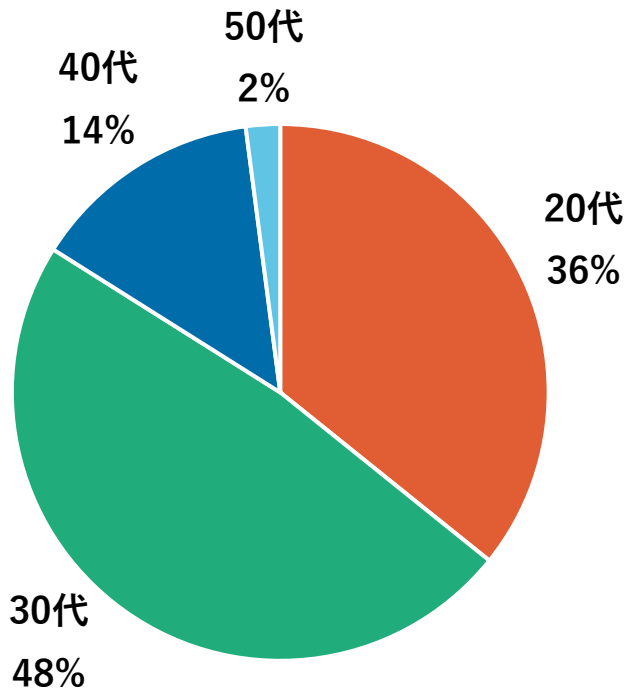
受講者の構成①

- 第1期は76名、第2期は83名、第3期は69名、第4期は46名、第5期は48名、第6期は48名、第7期は65名が修了。
- 2024年7月1日に「第8期中核人材育成プログラム」を開講。57名の受講者が参加。

第1～7期 受講者スキル経験



第1～7期 受講者 年齢

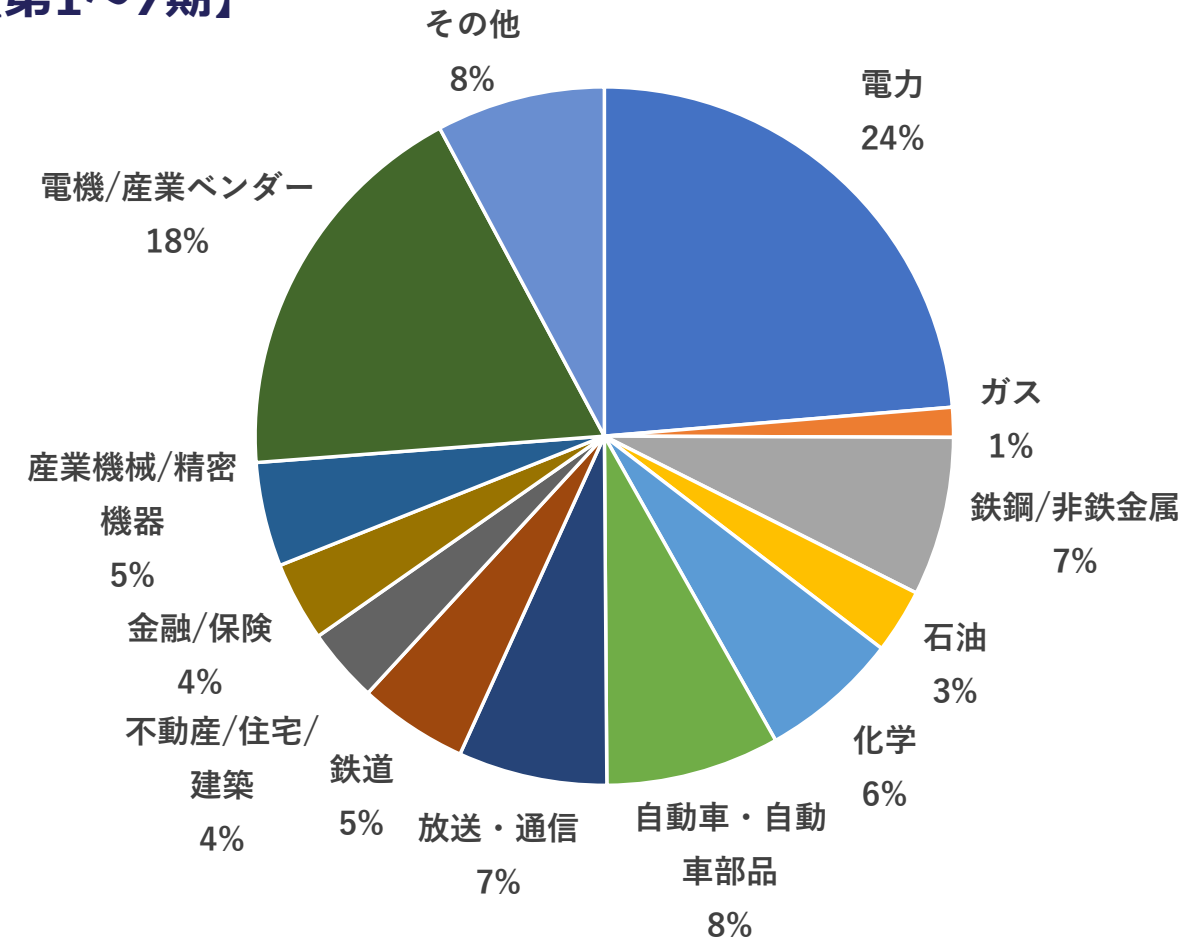


中核人材育成プログラム

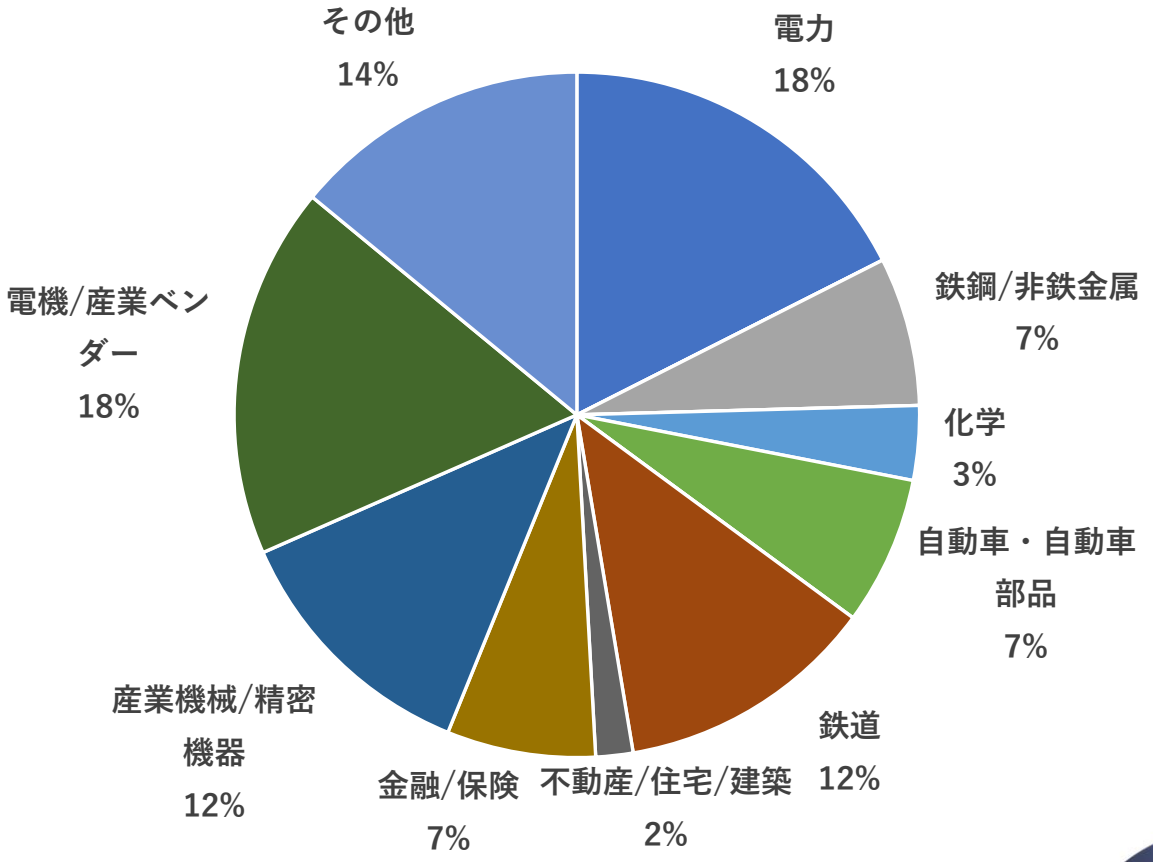
受講者の構成②

➢ 電力、石油、ガス、化学、自動車、鉄道分野等の企業から参画。

【第1～7期】



【第８期】



中核人材育成プログラム

修了者コミュニティ「叶会（かなえかい）」

- 修了者コミュニティとして「叶会（かなえかい）」が設置。
- 1年間のプログラムを通じて築かれる”横”のつながり、年1回の総会や部会活動等を通じた”縦”のつながりにより、業界を横断した連携体制を構築。セミナーやシンポジウムを通じて知見を社会に還元。

【ロゴ】

Will Come True 叶会

【目的】

- 卒業後も知見をアップデート
- 卒業年次を超えた人脈
- 修了者の知見の社会還元

→ **業界を横断した制御システムのセキュリティに係る連携体制の構築**

Interop Tokyo 2024での発表の様子

【主な活動】

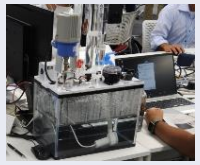
- 年１回の総会で最新動向と演習・発表
- サイバーセキュリティ情報提供活動
- ノウハウシェア部会、地域部会などの部会活動をコロナ禍においてもリモートを活用し積極的に実施
- 外部カンファレンスや展示会などでエキスパートとして取り組みや有益な情報を発信

（参考）

責任者・実務者向け 短期プログラム

IPA

➢ **CISOから部門長など向けに「責任者向けプログラム」を、制御システムのサイバーセキュリティを担当または今後担当を予定されている方向けに「実務者向けプログラム」を実施。**

	短期プログラム一覧			
責任者向け	**業界別サイバーレジリエンス強化演習** *CyberREX* *Cyber Resilience Enhancement eXercise by industry*	 業界に分かれてグループディスカッション	• **業界別**に**仮想企業を想定したシナリオ**を用いた演習 • 業界特性に応じた対策・対応について**グループで議論**	2日間
責任者向け	**サイバー危機対応机上演習** *CyberCREST* *Cyber Crisis RESponse Tabletop exercise*	 攻撃を想定した机上演習	• **国家脅威アクター**にサプライチェーンを狙われる等のシナリオに基づいた**机上演習** • **国際動向・攻撃事例**や、サイバーセキュリティ対策に有効な**標準・フレームワーク**についての**講義**	オンライン（事前学習） ＋ 2日間
責任者向け	**サイバーセキュリティ企画演習** *CyberSPEX* *Cyber Security Planning Exercise*	 立案・提言をシミュレーション	• 事業継続を目的としたサイバーセキュリティの**企画立案**や、**役員会での提言**を想定した**シミュレーション演習** • **企画立案**（体制、予算、ポリシーなど）**スキル**を習得	4日間
実務者向け	**制御システム向けサイバーセキュリティ演習** *CyberSTIX* *Cyber SecuriTy practIcal eXercise for industrial control system*	 演習で使用するプロセス制御の模擬システム	• 産業用制御システムの**模擬システム**を用いたサイバー攻撃と対応を体験する**ハンズオン演習** • **ITセキュリティとのギャップ**を認識しながら**OTセキュリティを習得**	2日間

※「業界別サイバーレジリエンス強化演習」「制御システム向けサイバーセキュリティ演習」は**情報処理安全確保支援士の実践講習として受講可能**