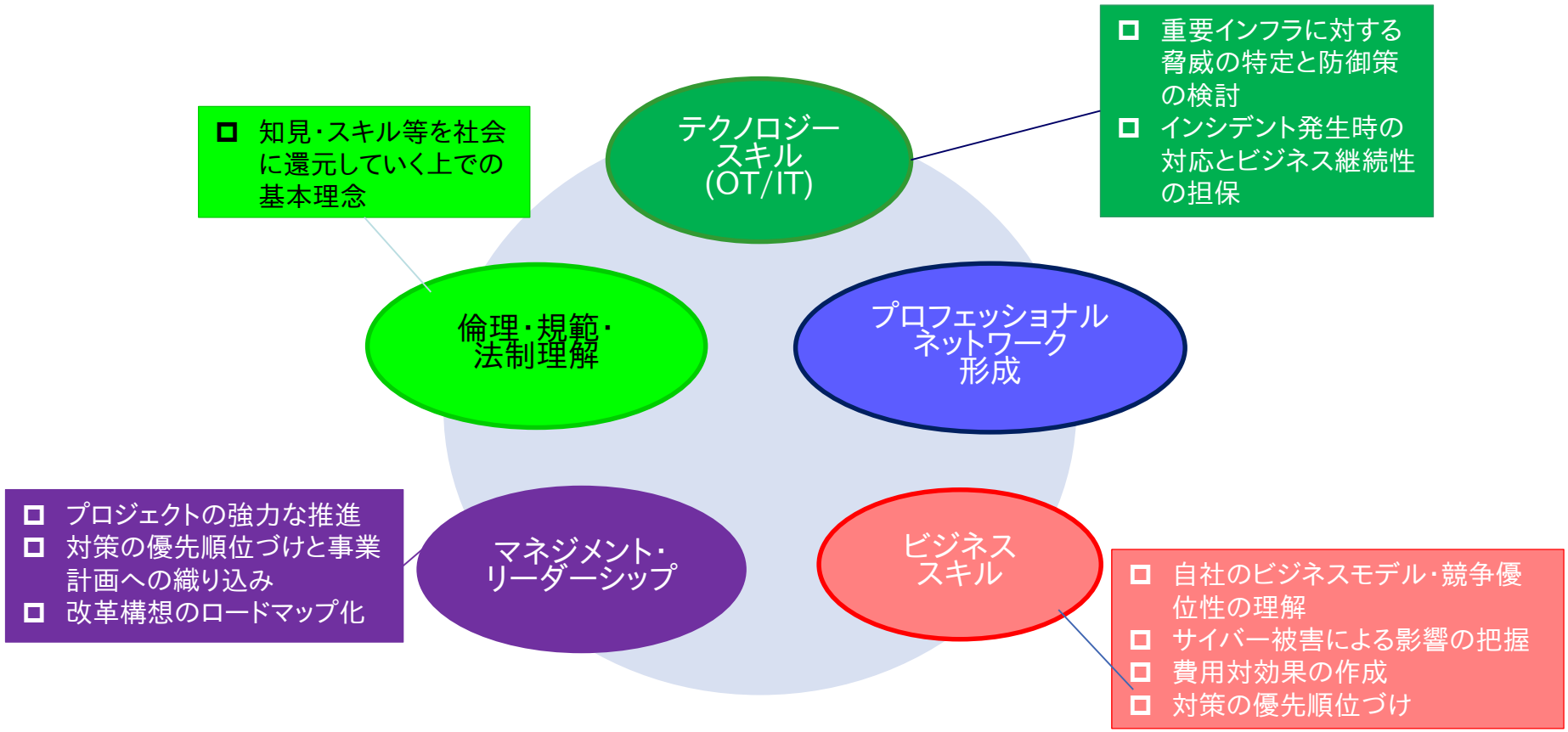
第二期中核人材育成プログラム（平成30年7月開講）カリキュラムご案内資料

独立行政法人情報処理推進機構（IPA）

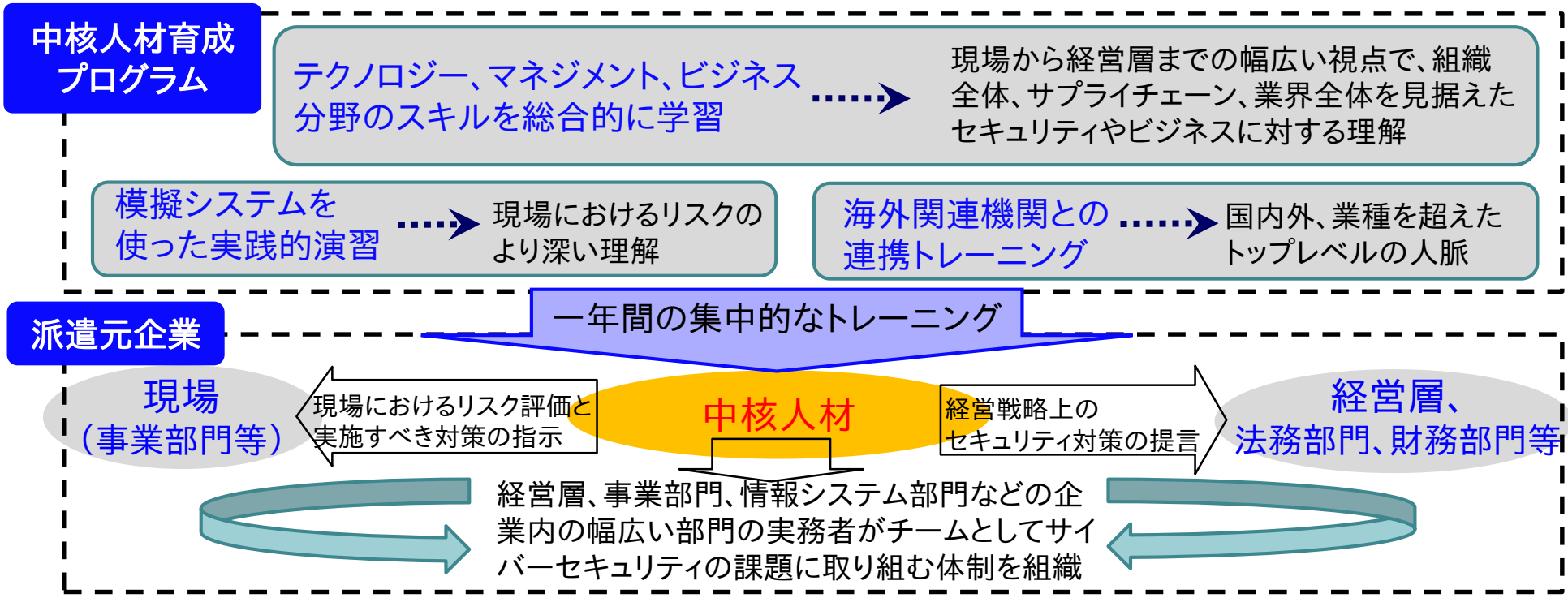
目指す産業サイバーセキュリティ人材像

- 情報システム（IT）と制御システム（OT） 双方のスキルを核とした上で、サイバーセキュリティ対策の必要性を把握し（ビジネススキル）、プロジェクトを強力に推進していく力（マネジメントスキル・リーダーシップ）をバランスよく兼ね備える。



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



カリキュラム（第1期事業の例。第2期はこれをベースに調整中。以下同じ）

IPA

	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）	防衛技術・ペネトレーション手法	**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	**総合演習** - ベーシック、アドバンスで学習した内容をもとにしてグループで受講生自らサイバー演習を企画し、実施 - 最終的には、ステークホルダー（各企業のマネジメント層）も招待して演習を実演　等 **個人プロジェクト** - 受講生一人ひとりが各自で自社のサイバーセキュリティ課題を特定。自社の経営層に対して、産業サイバーセキュリティ関連の課題解決に向けた提言をするための報告書を作成。等
			インシデント対応・BCP	**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（物理セキュリティあど）、機器・システムに関わる課題を中心に、受講生と専門家の間で、質疑応答を実施。		数ヶ月単位ではなく、単発~数日で実施予定
		IT	ITセキュリティ	**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	

ビジネス・マネジメント・倫理	**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	**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	**倫理・規範** - ビジネス倫理 - セキュリティ倫理・価値等

数ヶ月単位ではなく、単発~数日で実施予定

海外先進事例・国際標準

海外先進事例紹介

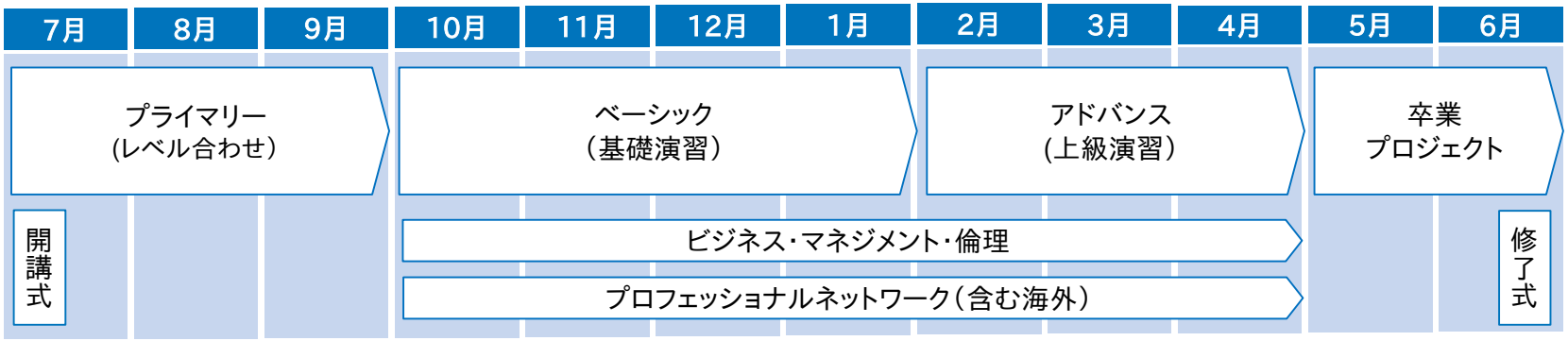
【米国】
- DHS　ICS-CERT
- Iron Net
- PAI research training

【欧州・イスラエル等】
- IRT System X
- 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

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

年間カレンダー①（第1期事業の例）



プライマリー

- 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

- 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

アドバンス

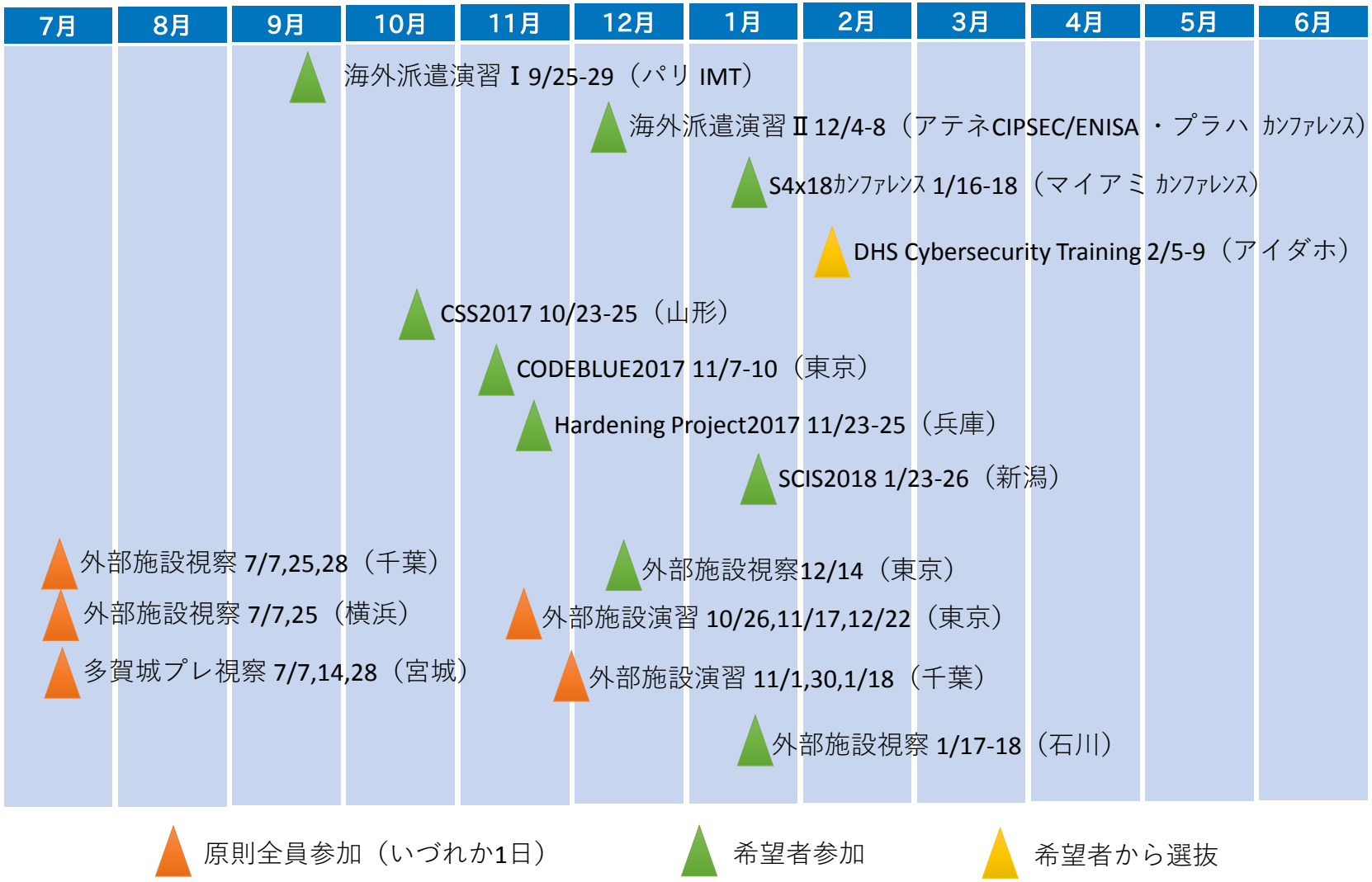
- 実践的なトレーニング及び演習を実施し、更なる知見の向上

卒業プロジェクト

- 習得した知識や経験を活かし、個人及びグループで演習を企画立案

年間カレンダー②（第1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、海外を含め、関連施設やカンファレンス等でのフィールドワークも積極的に実施（※以下は第1期事業における実施例の一部）。



海外関連機関との連携トレーニング（第1期事業の例）

- 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や、海外有識者との人脈形成を目的に、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。

米国国土安全保障省（DHS）が提供するサイバー演習「ICS Cybersecurity」の実施（9月上旬）

- DHSの制御システムセキュリティの担当部門であるICS-CERTが提供するプログラムを、米国から招へいした講師の指導のもと、本場のトレーニングを体験
- プロセス制御システムに対する攻撃が実際にどのように開始され、どのように行われるかを理解させるとともに、制御システムネットワークのサイバーセキュリティ対策を向上する戦略を紹介

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（パリ）の学術機関IMT、Telecom Paris Tech大学、サクレー大学等を訪問し、現地の産業界・大学の研究者や行政担当者による講演や、彼らとの意見交換を通じて、欧州の最先端知見を習得し、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（9月下旬）。
- ギリシアに本部を置くEUのセキュリティ・エージェンシーであるENISAを訪問し、EUのセキュリティ行政の担当者との意見交換を行い、欧州全体におけるサイバーセキュリティ戦略を理解するとともに、現地キーパーソンとの人脈を構築（12月上旬）。

European Union Agency for Network and Information Security

米国やイスラエルの政府や産業界の権威者による特別講義

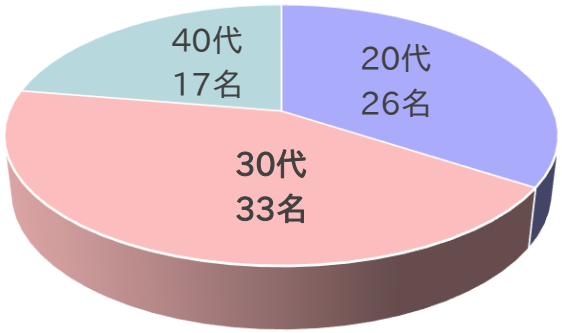
- 米国国家安全保障局（NSA; National Security Agency）の元長官で、米国サイバー軍の初代司令官も務めたキース・B・アレキサンダー将軍による特別講義を実施（10月上旬）。
- 米国元国家情報長官のデニス・ブレア提督による特別講義を実施（10月下旬）。
- イスラエル国家サイバー局の新サイバー技術ユニット代表責任者であるYigal Unna氏他によるイスラエルにおける重要インフラ向けサイバーセキュリティ戦略に関する特別講義や、イスラエル電力公社のCEOがモデレーターを務める机上演習を実施（11月下旬）。

キース・アレクサンダー将軍

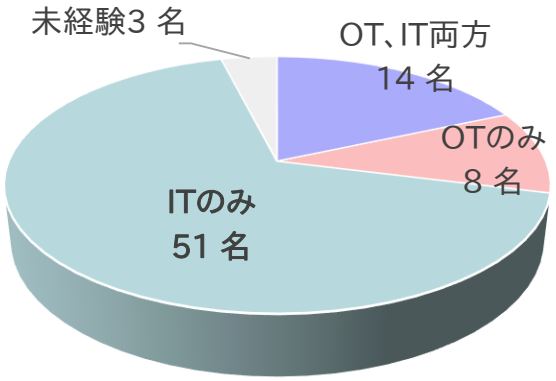
第1期中核人材育成プログラム（平成29年7月開講）の受講者属性

- 電力、鉄鋼、自動車等の13業種から65社、76名の受講者が参加。

受講生の年齢分布（平成29年4月現在）



受講生のスキル経験



受講生の出身企業の分類