IPA産業サイバーセキュリティセンターが目指す先

2018年２月７日

独立行政法人情報処理推進機構（IPA）
産業サイバーセキュリティセンター（ICSCoE）
田辺　雄史

本日の内容

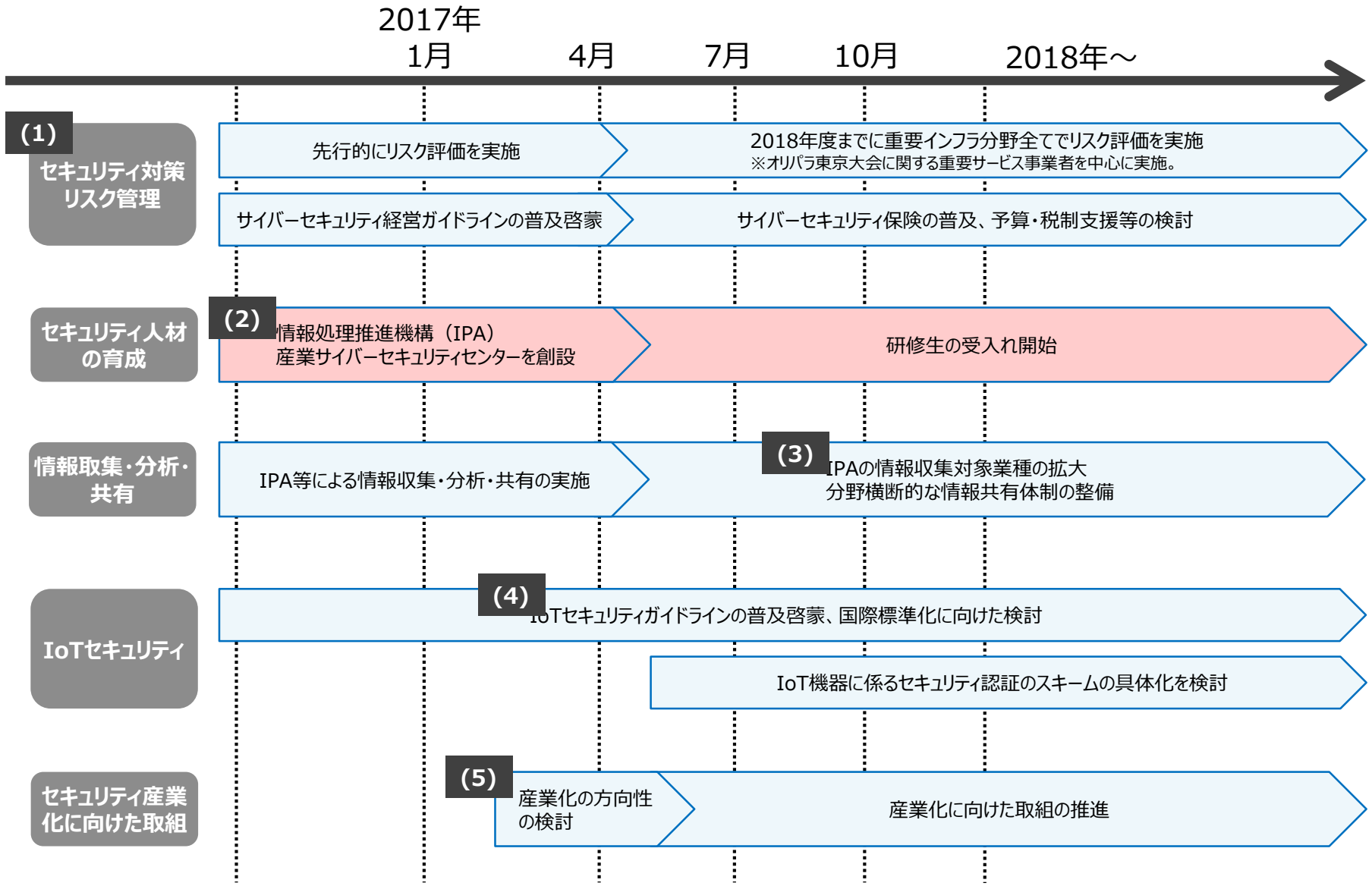
1. 背景～サイバーセキュリティ政策全体課題

2. 産業サイバーセキュリティセンターの設立経緯

3. 産業サイバーセキュリティセンターが実施する人材育成事業
   - ① 長期プログラム： 中核人材育成プログラム
   - ② 短期プログラム： 業界別トレーニング
   - ③ 短期プログラム： 業界共通トレーニング

4. 今後の動き

サイバーセキュリティ政策の全体課題



（経済産業省・平成29年5月12日情報経済小委員会資料「今後の情報政策の方向性」より）

サイバーセキュリティ政策の全体課題

ゴールイメージ

重要インフラ・産業インフラ等のサイバーセキュリティ対策を強化するとともに、IoT製品・サービスのサイバーセキュリティ対策を強化。
加えて、サイバーセキュリティの産業化を図り、日本のサイバーセキュリティ産業の競争力確保を目指す。

課題と対応の方向性

- 依然としてサイバー攻撃による情報漏洩等の事件が頻発。組織のリーダーが率先してサイバーセキュリティ対策に取り組む必要がある。
  →重要インフラにおけるリスク評価の推進、サイバーセキュリティ経営ガイドラインの普及啓蒙等。
  企業による投資を促進するため、サイバーセキュリティ保険の普及、予算などについても検討。

- 企業におけるサイバーセキュリティ対策の重要性は高まっているが、現場で対応する高度な人材が不足。
  →産学官連携による中核人材の育成

- 企業等に対するサイバー攻撃情報・予兆情報が迅速に収集・分析・共有されていないケースがある。
  →情報収集・分析・共有体制の整備

- IoTの進展により、ネットワークに接続する機器の数が莫大に増える中で、個々のIoT機器に対するサイバー攻撃も増加。IoTの実現に向けた新たなセキュリティ対策を講じる必要
  →IoTセキュリティガイドラインの普及啓蒙や国際規格への提案等

- 日本ではサイバーセキュリティが大きな産業として確立していない。また、サイバーセキュリティ分野で活躍している日本企業が少ない。
  →サイバーセキュリティの産業化、産業競争力強化に向けた政策を立案

（経済産業省・平成29年5月12日情報経済小委員会資料「今後の情報政策の方向性」より）

「産業サイバーセキュリティセンター」発足背景

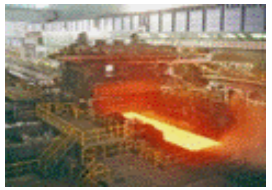
- 近年は社会インフラ・産業基盤に物理的なダメージを与えるサイバー攻撃のリスクが増大。海外においては、既に、他国家等からなされるサイバー攻撃により、社会インフラ・産業基盤の安全が脅かされる事案が発生。
- 社会インフラ・産業基盤における、サイバー攻撃に対する防護力を強化することは、国家全体の喫緊の課題。

原発の制御システム停止（米国、2003年）

発電所の制御システムがウィルスに感染。制御システムが約５時間にわたって停止。

製鉄所の溶鉱炉損傷（ドイツ、2014年）

何者かが製鉄所の制御システムに侵入し、不正操作をしたため、生産設備が損傷。



大規模停電の発生（ウクライナ、2015年）

マルウェアの感染により、変電所が遠隔制御された結果、数万世帯で3～6時間にわたる大停電が発生。

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」を2017年4月に発足

産業用システムとITシステムの違い

- 産業用システムは社会基盤・産業基盤を支えており、稼働が停止すると社会的な影響・事業継続上の影響が大きいため、継続して稼働できることが重視されている。
- 情報システムは大量のデータ処理を目的として導入されることが多いため、可用性よりも処理能力が求められ、顧客情報等の機密情報の漏えいは影響が大きく機密性が重視される傾向がある。

産業用システムと情報システムにおけるセキュリティの考え方の違い

	産業用システム	情報システム
セキュリティの優先順位	システムが継続して安全に稼働できることを重視	情報が適切に管理され、情報漏えいを防ぐことを重視
セキュリティの対象	モノ（設備、製品） サービス（連続稼働）	情報
技術のサポート期間	10年～20年	3～5年
求められる可用性	24時間365日の安定稼働 （再起動は許容されないケースが多い）	再起動は許容範囲のケースが多い
運用管理	現場技術部門	情報システム部門

出典：IPA「制御システム利用者のための脆弱性対応ガイド」

「産業サイバーセキュリティセンター」中核事業

- **人材・組織強化、技術、ノウハウ**を結集し、社会インフラ、及び産業基盤のサイバーセキュリティ対策抜本的強化を図るために、**３つの事業**を柱に推進していく

人材育成事業

- 自社システムのリスクを認識し、必要なセキュリティ対策を判断できる人材の育成
- 模擬プラントを用いた実践演習による、現場で活きるスキルの醸成
- 国内外の有識者、専門家との連携を促進
- 企業等の経営層へ、サイバーセキュリティ対策の必要性、人材活用についての啓発

中核となる3事業

制御システムの安全性・信頼性検証事業

- 実際の制御システムの安全性・信頼性に関するリスク評価・対策立案を行う

※IPAセキュリティセンターと連携して実施する事業

脅威情報の調査・分析事業

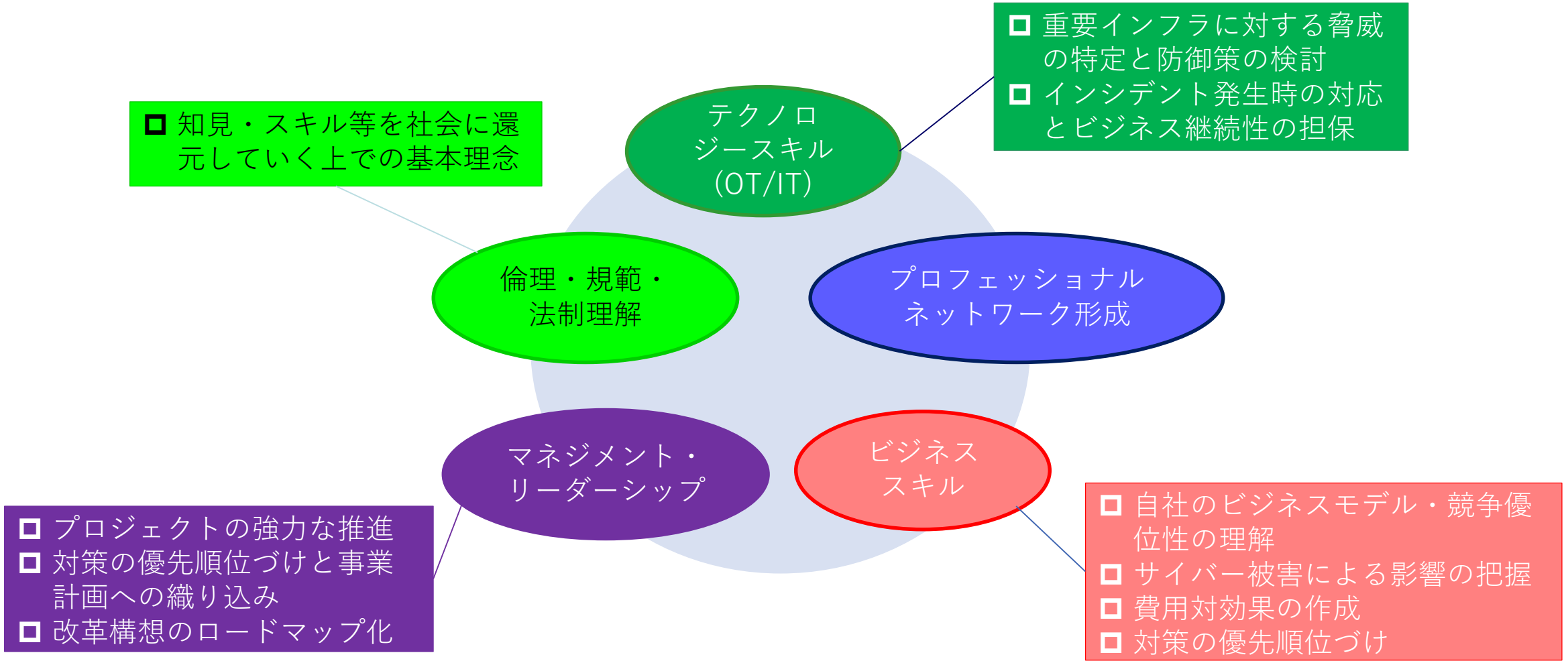
- 脅威情報を収集、新たな攻撃手法など調査・分析

※IPAセキュリティセンターと連携して実施する事業

【注意事項】本資料は、人材育成事業にフォーカスして掲載致します。他の事業については詳細情報が確定次第、随時情報発信して参ります。

目指すべき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）がバランスよく必要となる。



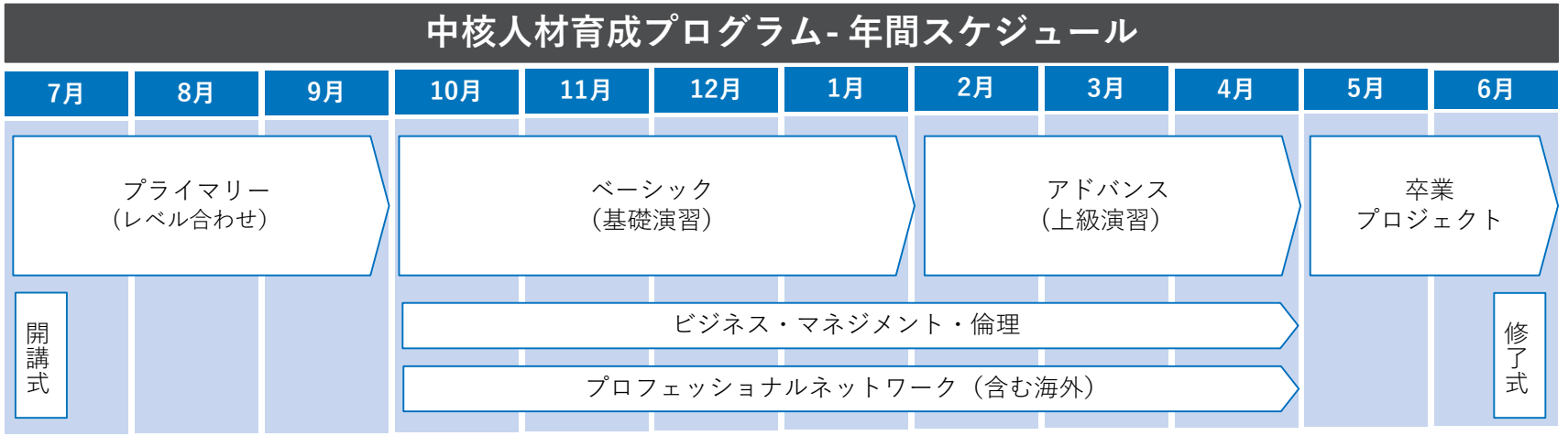
第１回アドバイザリーボード（2017年10月4日）

- 最新のサイバーセキュリティの動向をセンター運営に反映するため、キース・アレキサンダー将軍（元米国NSA長官兼サイバー軍司令官）、バッド・ロス氏（デニス・ブレア提督（元米国国家情報長官）の代理として出席）、名和利男氏（サイバーディフェンス研究所専務理事・上級分析官）にアドバイザーとして出席してもらい、意見交換を実施。

提供プログラム全体像

長期プログラム「中核人材育成プログラム」

- 将来、企業などの経営層と現場担当者を繋ぐ、**“中核人材”**を担う方を対象としたプログラム
- 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を実施
- 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
- 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
- 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



短期プログラム

- CEO、CIO・CISO、部門長等、責任者クラスの方向けに2日間のトレーニングを年6回実施（うち、業界共通トレーニングを3回、業界別トレーニングを3回）
- 業界共通トレーニングは、海外の最先端企業の専門家を講師陣に招へいし、制御システムを守るためのリスク分析やインシデント管理についてウォーゲームセッションを通じて理解
- 業界別トレーニングは、業界別に仮想企業を想定し、シナリオ形式による実践的演習を実施

短期プログラム- 年間スケジュール

7/14-15 業界共通(1回目)	10/13-14 業界共通(2回目)	3/2-3 業界共通(3回目)
8/25-26 業界別(1回目)（電力、不動産･ビル管理）	11/17-18 業界別(2回目)（製造業、自動車）	2/16-17 業界別(3回目)（金属･石油精製･素材）

産業サイバーセキュリティセンターが実施する人材育成事業

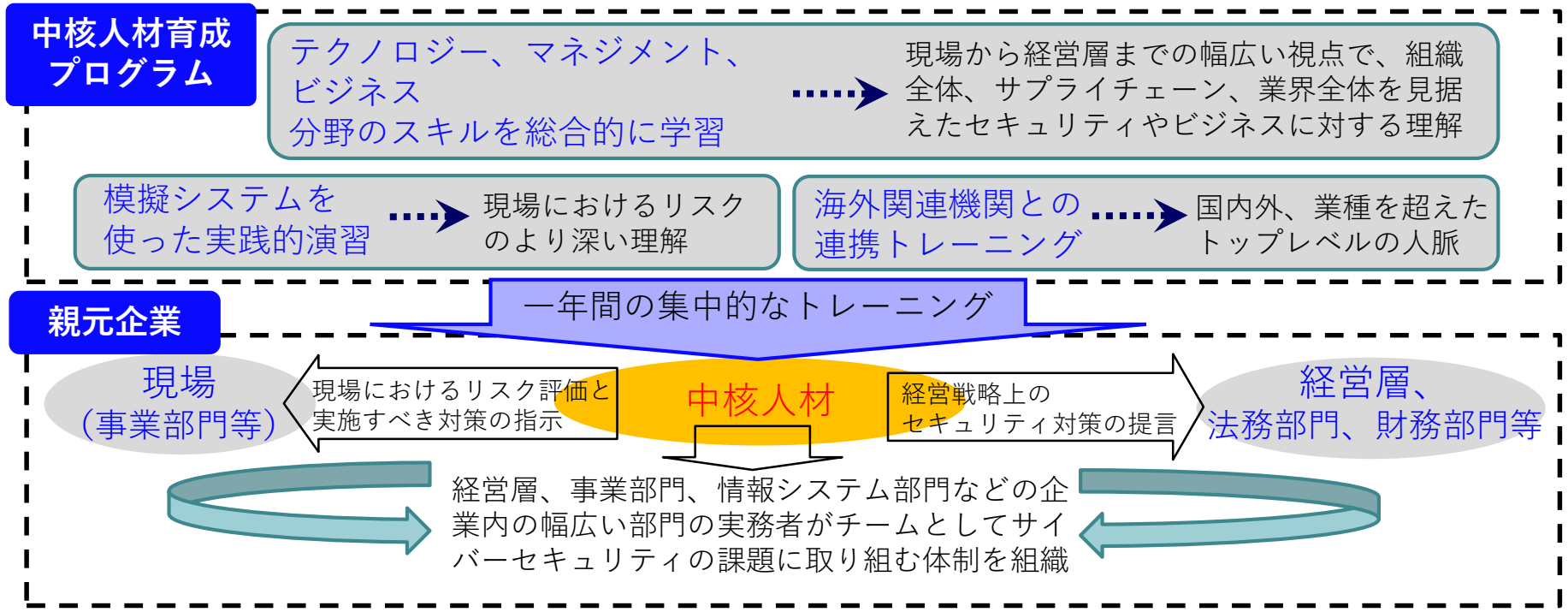
長期プログラム： 中核人材育成プログラム

短期プログラム： 業界別トレーニング

短期プログラム： 業界共通トレーニング

中核人材育成プログラム
プログラムの概要

- 将来、企業などの経営層と現場担当者を繋ぐ**中核人材**を担う方を対象としたプログラム
- 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を実施
- 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（1年）
- 開講オリエンテーション

- 中核人材育成プログラム（1年）は、2017年7月3日よりスタート。受講者は76名。
- 同日のオリエンテーションでは、産業サイバーセキュリティセンター長の中西宏明氏が、自身の経験や本センター設立への思いを込めてメッセージを発信した。

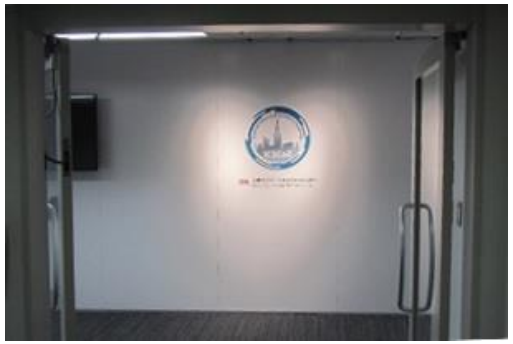
演習で使用する模擬システム（平成２９年度事業の例）

- 受講者が自社に近い環境でのセキュリティ対策を演習できるよう、各業界のシステムを想定した、様々な機能・特性を具備した模擬システムを使用。

模擬システム	特性	システムの概要
鉄鋼圧延システム	● プロセス制御（バッチ）	プロセス制御で個別単発に生産するシステムのうち、特に高速かつ複雑な制御で発生する大量のログから攻撃検知を行うことが困難な「鉄鋼圧延」を模擬
鉄道運行管理システム	● 広域運用 ● 安全停止	人命を重視し安全停止機能を有するシステムである「鉄道運行管理」を模擬
機械製造システム	● シーケンス制御	手順に沿った処理を行うシステムのうち、様々な製品が対象となり、汎用性が高い「機械製造」を模擬。
発電システム	● プロセス制御（フロー）	プロセス制御で入力と出力が連続する生産システムのうち、OT・IT連携が行われるエネルギーマネジメントシステムの1つである「発電」を模擬
スマートグリッド（CEMS）	● 広域運用 ● 稼働継続	広域で高可用性が必要なシステムのうち、OT・IT連携が行われるエネルギーマネジメントシステムと接続する「スマートグリッド」、特にCEMS（地域エネルギーマネジメントシステム）を模擬
施設管理システム	● 拠点集中運用	拠点内の対象を制御・運用するシステムのうち、ほぼ全ての産業が保有し、空調・照明等のビル制御を行う「施設管理」を模擬
化学プラント 施設管理（BA）、 機械製造（FA）	● BCP・インシデント対応	大型の全体演習用模擬システムでは「原子力発電」を模擬。5～6名のグループワークで利用する小型のチーム演習用模擬システムでは「施設管理（エレベータ、信号機）」「機械製造（ロボット）」等を模擬

平成29年度中核人材育成プログラムの実績

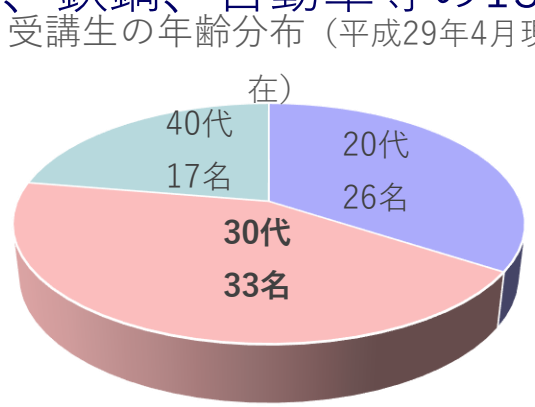
- 平成29年7月3日に「平成29年度中核人材育成プログラム（第1期生）」を開講。

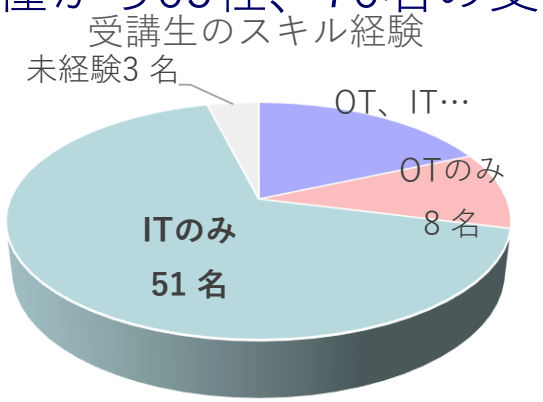


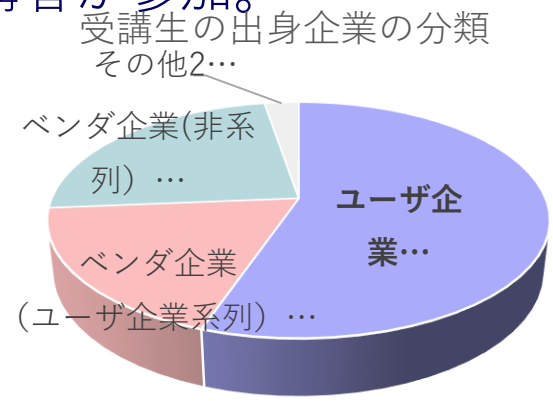
産業サイバーセキュリティセンター入口

開講式

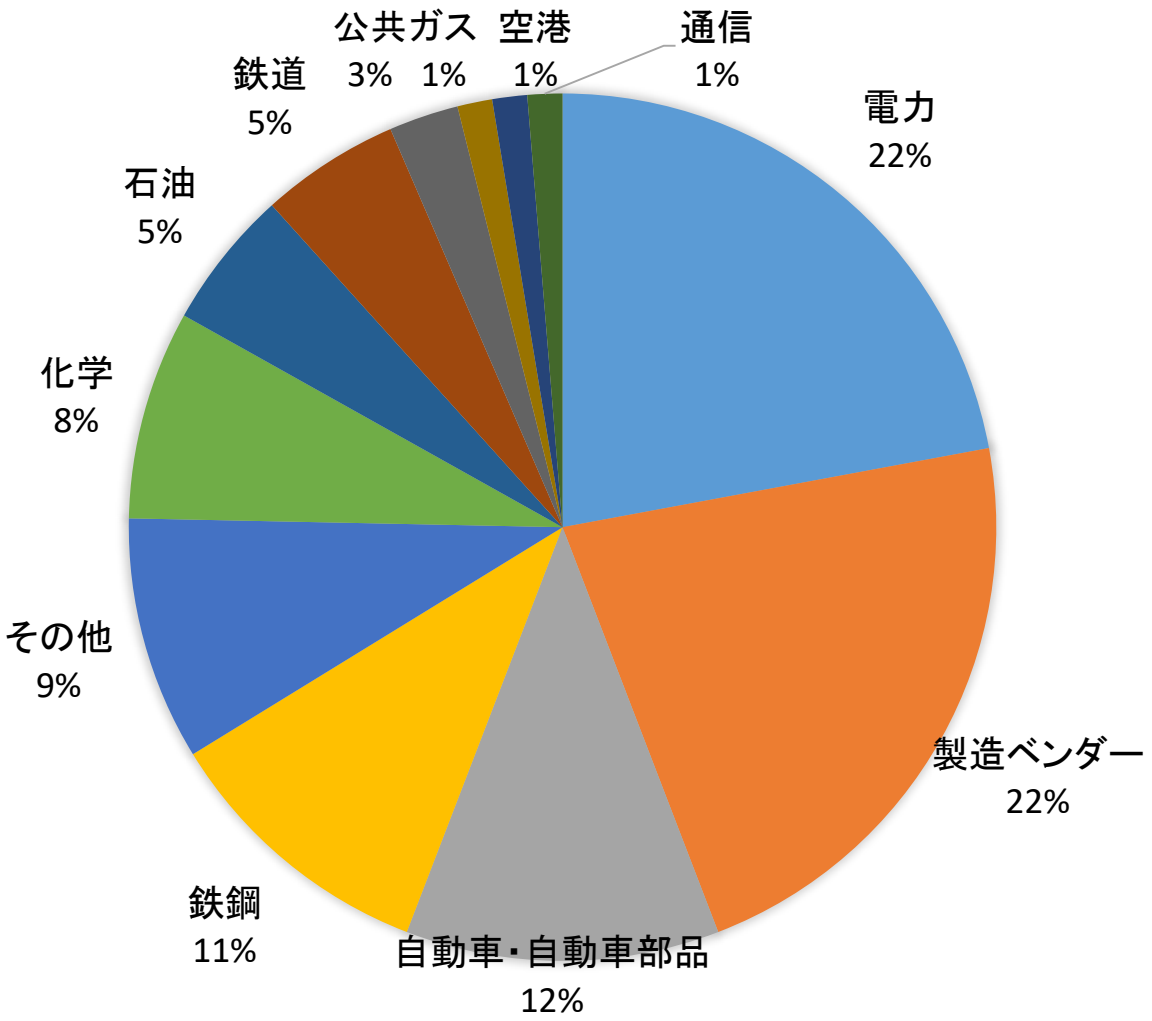
- 電力、鉄鋼、自動車等の13業種から65社、76名の受講者が参加。



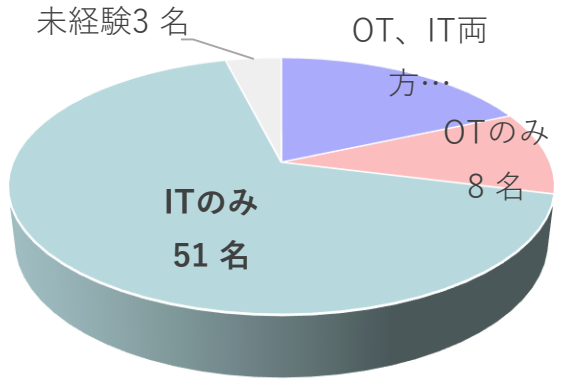




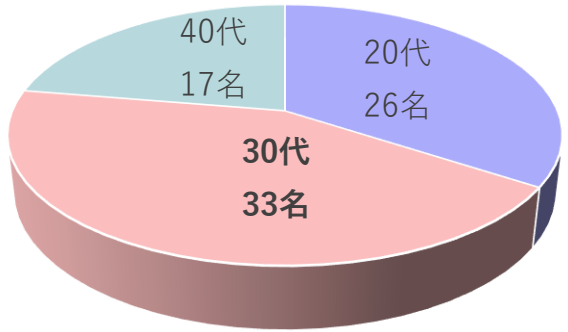
中核人材育成プログラム（1年）
- 受講者の内訳



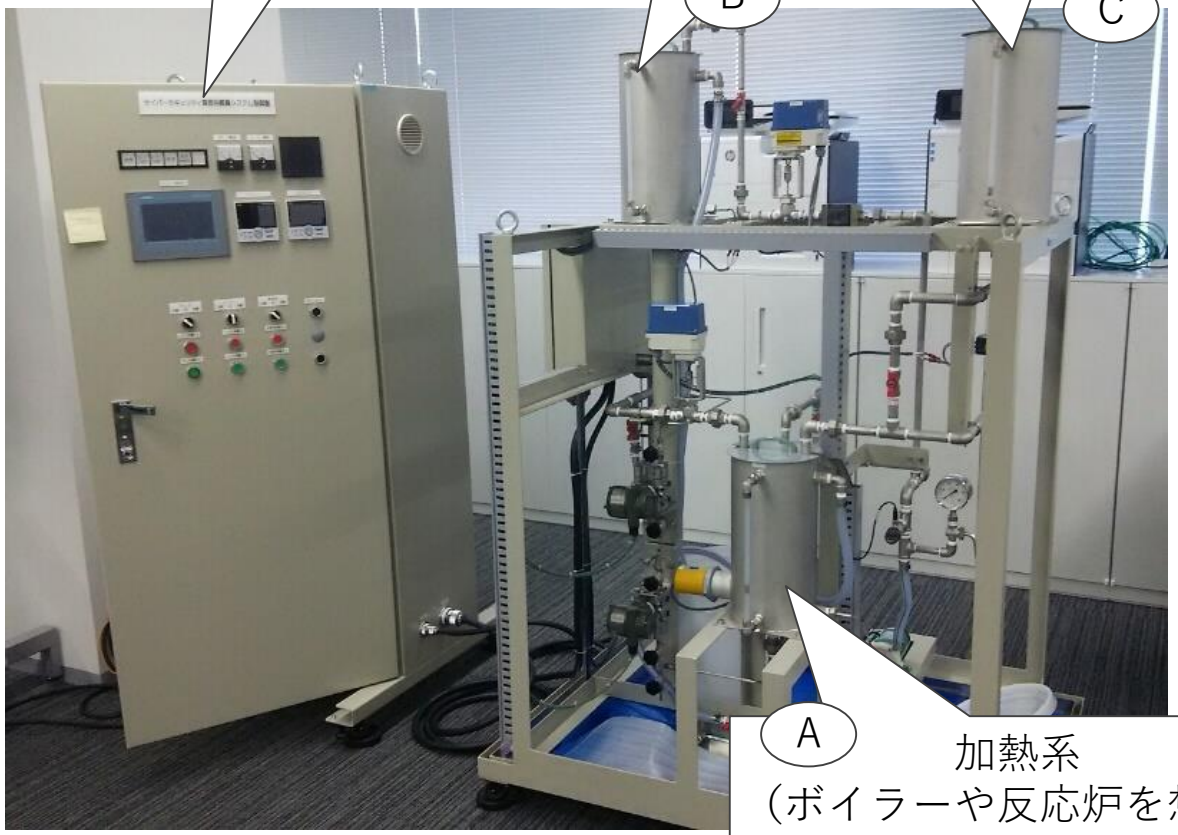
受講生のスキル経験



受講生の年齢分布（平成29年4月現在）



演習で使用する模擬プラント（平成２９年度事業の連続系プラントの例）



文京グリーンコート8階での演習に利用中。

- ローカル制御盤では、A/B/Cの各システムのON/OFFによる安全システム操作を行う。かつては、リレー回路（機械的なリレースイッチで構成）が一般的だったのに対し、最近ではPLC上のプログラムによって実現する傾向。
- このため、PLCがハッキングされると、制御盤でCの供給装置のスイッチをONにしても作動せず、Aの加熱系の異常状態が進行する可能性あり。
- こうした制御システムの特徴を踏まえ、あり得るサイバー攻撃パターンに対して、インシデントレスポンス（例えば、異常対応として中央制御室でCをリモート操作するだけでは不十分で、現場で実際にCの動作を確認等）について演習。
- 更に、プラントから離れた中央制御室等も模擬システムに組み込み、多様なパターンに対応した事業継続演習を提供。

平成29年度中核人材育成プログラムの実績

- 受講者からの声

✓ ここのように制御系システム（OT）のセキュリティについて本格的に学べる場所は他にないと思う。貴重な学びの機会なので、精一杯知識を得て、社に戻りたい。

✓ ここではプライマリーから段階を踏みつつ、セキュリティを総合的に学べるので、今までセキュリティを本格的に学んだことのない初心者でも、やる気さえあれば、高度な知識を身に着けられるように思う。

✓ 授業の内容が実戦向きで、身に着けた知識を自社の現場での活かし方がイメージし易い。

✓ 講師の方々が非常に熱心で宿題も多く、また講師手ずから驚くような高度なエクスプロイトの手法を実演いただき、授業内容は量、質ともに高いと実感する。

✓ 海外で高い評価を得ている良書をテキストに、英語の原文で読んでいくので、骨は折れるが、国際的に高水準で最先端の知識に触れることができる。

✓ 他業種の仲間と切磋琢磨することで、自分の知らない業界での課題や実態について情報交換することができ、視野が広がる。

✓ 学べば学ぶほど、自社のセキュリティ対策の未熟な点が見えてくる。社に戻ったら、様々な対策を提案していきたい。

授業の風景

工場見学の風景

海外機関連携トレーニング（平成２９年度事業の例）

- 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

- 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

フランスにおける産業サイバーセキュリティを直に学ぶための海外派遣演習

- フランス（パリ）において、13大学から構成される学術機関IMTのキャンパスを拠点とし、パリ市内のTelecom Paris Tech大学、パリ郊外のサクレー大学にて講義・施設見学
- フランスの産業界・大学の共同機関訪問、行政担当者の講演を通じて、欧州の最先端知見を学び、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、現地トップレベル機関の人材との人脈を構築

（フランス産業界との交流（例）：　CEA（原子力・代替エネルギー庁）、EDF（フランス電力）、ORANGE社（通信企業）、Thales社（電機企業）、SAFRAN/MORPHO社（セキュリティ企業）、Systematic社（IT企業））

米国国家安全保障局（NSA）元長官による特別講義

- 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。約１時間半にわたり、質疑応答を中心とした白熱教室を展開
- キース・B・アレクサンダー将軍は、現在、重要インフラ分野を強みとするサイバーセキュリティ製品やサービスを提供するIronNet Cybersecurity社のCEOを務めるとともに、当産業サイバーセキュリティセンターのアドバイザーも務めている

産業サイバーセキュリティセンターが実施する人材育成事業

長期プログラム： 中核人材育成プログラム

短期プログラム： 業界別トレーニング

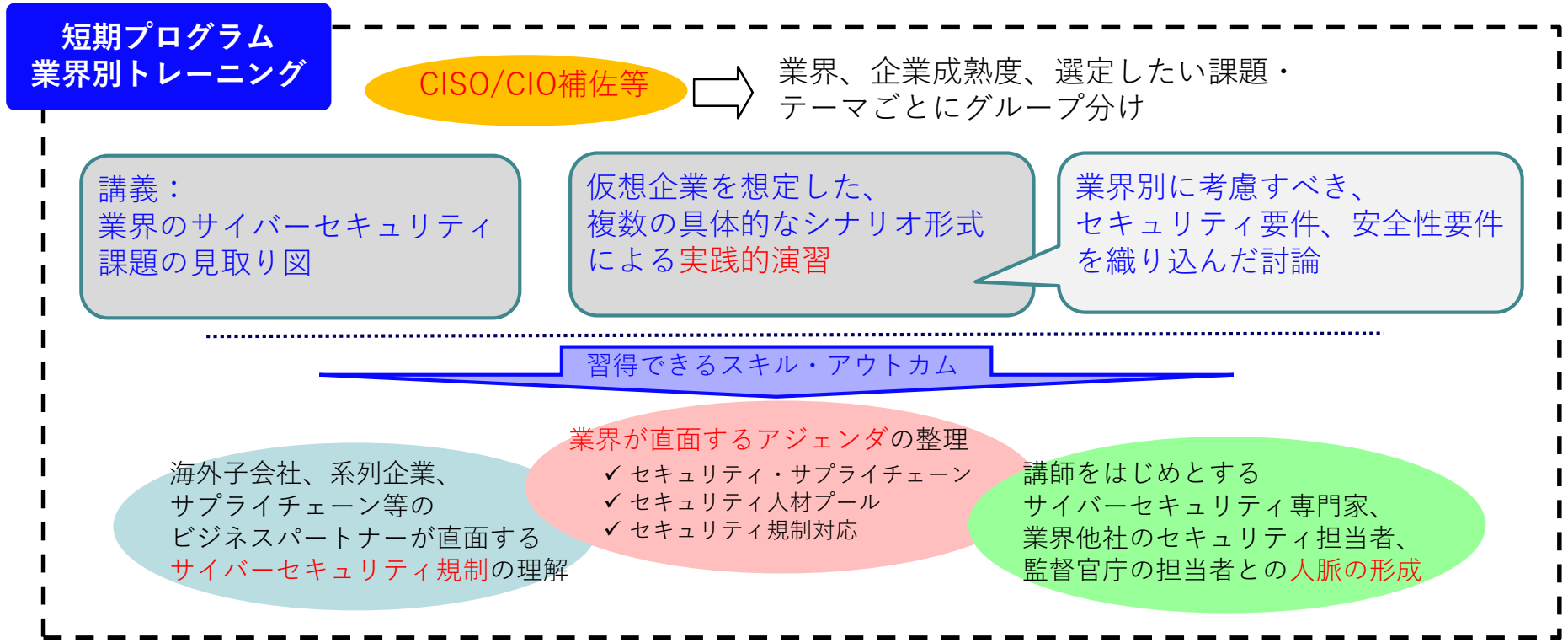
短期プログラム： 業界共通トレーニング

- **業界別トレーニング（第三回）（金属・石油精製・素材（PA））**

  （平成30年2月16日（金）～2月17日（土））

プログラムの概要

- CISO/CIO補佐（課長クラス以上を想定）、または、系列企業やサプライチェーンのビジネスパートナーにおけるCISO/CIO相当の方を対象とするプログラム
- 電力、不動産、自動車・製造業（FA）、金属・石油精製・素材（PA）を対象に、企業が有する制御システム（OT）を襲う様々なサイバーリスクに対して、規制・体制・人材・技術等の総合的な観点を踏まえた、リスク対応スキルを学ぶ２日間のトレーニング
- 仮想企業を想定した、シナリオ形式による実践的演習を中心としたトレーニング



業界別トレーニングカリキュラム

1日目　10:00～18:00 (※18:30-21:00懇談会)

講義・実践的演習セッション

導入講義（10:00-11:00）

・業界別サイバーセキュリティ課題の見取り図の提示

グループワーク（11:00-15:00）

・特定の業界を想定した仮想企業を想定し、5つの課題をシナリオ形式で抽出

・発表のためのポスター作成

※昼食時間(1時間程度)をはさみます

プレゼンテーション&ブレインストーミング（15:00-17:00）

・課題発表と解決策の全体討論

グループ学習＆個人学習（17:00-18:00）

・関連海外動向やケーススタディ資料に基づき、2日目に備えてのテーマを深掘り

・ブレスト後に配布された独習資料（規制解説など）を用いて独習

2日目　9:00～16:00

実践的演習セッション

グループワーク（9:00-12:00）

・特定の業界を想定した仮想企業における課題解決をシナリオ形式で作成

・発表のためのポスター作成

昼食

グループ発表（13:00-14:00）

・特定の業界を想定した仮想企業におけるサイバーセキュリティ成熟度向上

総合討論・全体講評（14:00-16:00）

・講師陣および経済産業省様による講評

開催報告の送付（後日）

・ノートテイカーによる講演と報告の記録文書を、受講者の方に後日送付

演習用シナリオ例（製造業（FA））

- 参加者は、架空の企業「サイバー工場」のCISO/CIO、もしくは、サイバーセキュリティ統括責任者といったステークホルダーのロールを担う
- 次の①から③のシナリオにそって、架空の企業「サイバー工場」に関連する海外の規制・法律についての対応、これらの企業が直面するインシデントに対して、どのような行動をとるべきか、ケーススタディを実施（チームによるディスカッションを中心に進める）

シナリオ①：想定内のリスク

諸外国の重要インフラ向け制御システムをたびたび窮地に陥れたマルウェア。サイバー工場でも驚くほど簡単に感染事件が起こりました。制御システムサイバー脅威から防ぐCISOのあなたの行動は？

サイバー防御の原理・原則を、組織にとって受容な可能な形で落とし込むということが課題です。ここでは、そのための方法を演習を通じて実践的に学びます。

シナリオ②：監視カメラ

サイバー工場に設置された監視カメラは工場外からアクセスできない専用のネットワークに接続されているはずでした。サイバー攻撃による監視カメラの画像の改ざん、情報の漏洩といったリスクにどのように対応しますか？

ICSセキュリティにおける可用性・一貫性・機密性といった基本的な概念を「モニタリングしているデータ」に至るまで当てはめることにより、エアギャップを越えてくるサイバーテロ対策を学びます。

シナリオ③：想定外のリスク

サイバー工場の保有する工場への人・車・船の出入りは厳重に管理されていますが、それでは上空を違法に飛ぶドローンはどうでしょう。空中からの社内システムへのクラッキングに果たしてどのような検討が必要でしょうか？

想定外のサイバーセキュリティ・リスクについて、社内の体制や技術、社外の人脈や業界を守るための規制について、起こり得るサイバーテロシナリオの対策事例から検討します。

業界別トレーニングの実績

- 第1回8月25日、26日に電力業界、ビル・不動産管理業界向けに16社19名、第2回自動車・FA向けに10社12名の参加者で実施。
- 受講者からの声：
  - ✓ 同業他社で情報セキュリティを担当する方々と、同じチームとして課題に取り組んだことは、業界全体としてのリスク認識や現場の悩みを共有するとともに、それらを解決するヒントを得ることもでき、大変有意義だった。
  - ✓ 今回のシナリオは、ドローンによる電波ジャミングや、3Dプリンタによる偽造鍵による侵入といった、従来のセキュリティインシデントの概念から大きく外に広がるテーマも扱っており、セキュリティ対策に対する価値観の変化を伴う驚きがあった。
  - ✓ サイバーセキュリティの概念が、マルウェアやボットのようなITシステムだけに発生するリスクから、ドローンや3Dプリンタのような人間とITとの関わりにおいて発生するリスクまでに広がりつつあることを理解した。CISOとしての役割や視野がより広がってきており、CISOの仕事に新たな興味ややりがいを感じた。
  - ✓ 経済産業省や総務省で政策や規制を担当された方々も交えてのグループ討議は、民間と役所との垣根を超えた議論やケーススタディができ、セキュリティインシデントに対する官庁側の視点からの考え方を聞くこともでき、貴重な機会だった。
  - ✓ 懇親会で他社の情報セキュリティ担当者の皆様との情報交換や人脈作りができたことは、今後の仕事の中でも活かせるものだと思うので、非常に良い機会を得られた。

グループディスカッションの風景

産業サイバーセキュリティセンターが実施する人材育成事業

長期プログラム： 中核人材育成プログラム

短期プログラム： 業界別トレーニング

短期プログラム： 業界共通トレーニング

短期プログラム業界共通トレーニング（第三回）
（平成30年3月2日（金）～3月3日（土））

プログラムの概要

- サイバーセキュリティ対策の統括部門の責任者（CISO、CIO等)を対象とするプログラム
- 制御システム（OT）を有する企業に軸を置き、企業を守る為に必要なスキルとメソッドを学ぶ2日間のトレーニング

① 米国の政府や産業界における サイバーセキュリティ分野の 権威者による基調講演

- 米国の政府や産業界におけるセキュリティ権威者が、最近のサイバー攻撃動向と、サイバー攻撃に対処するための官民連携を含めた最先端のアプローチについて、CISOとして保持すべき戦略的視点についてご紹介
- 第一回は元国家テロ対策センター（NCTC）ディレクターのマット・オルセン氏、第二回はリーバイス社チーフセキュリティアーキテクトのスティーブ・ザルースキー氏が講演

M･オルセン氏

S･ザールスキー氏

② ケース・スタディーを通じた OTサイバー攻撃の対応に 関するベストプラクティスの紹介

- 米国を中心として実際に過去に発生したOTに対するサイバー攻撃のケース・スタディーを実施
- 各事例毎に、企業によって実際に行われたインシデント準備（Preparation）とインシデント対応（Response）について、長所・短所を振り返りながら、最新のベストプラクティスについて学ぶ

③ 2020年東京オリンピック を想定したOTサイバー インシデント対応の実戦演習

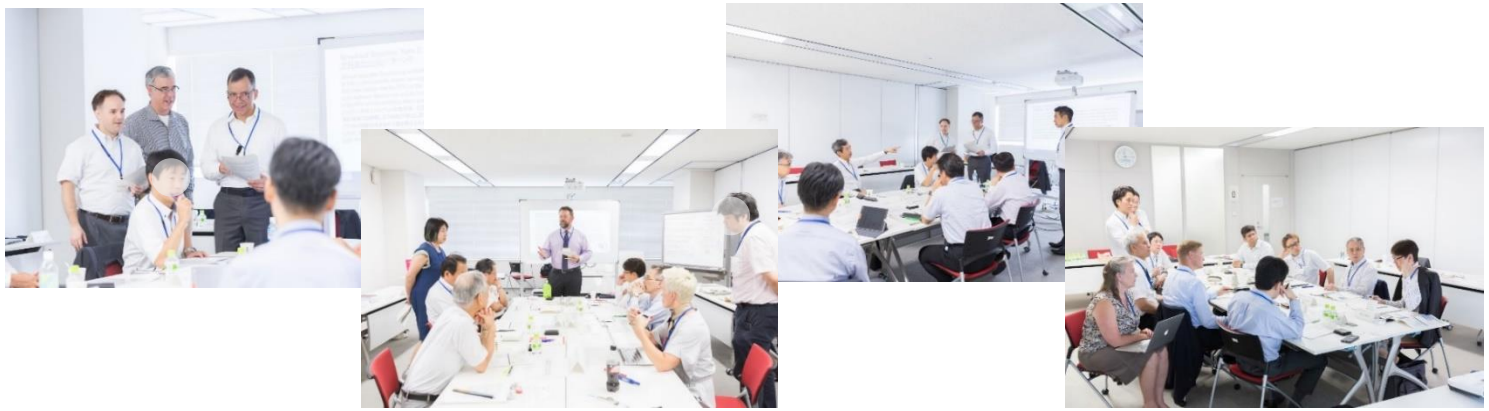
- 2020年東京オリンピックを想定した、重要インフラのOTに対する疑似的なサイバー攻撃シナリオに基づき、インシデント対応を実践形式で演習
- 複数グループに分かれ、各参加者に特定の役割をアサインした上で、攻撃シナリオに基づいて講師から与えられる様々な情報をInputに、インシデント対応における意思決定・判断を演習

※ウオーゲームセッションイメージ

本プログラムは米国アイアンネットサイバーセキュリティ社のナレッジ・ノウハウをベースに、産業サイバーセキュリティセンター提供プログラムとして、日本における社会インフラ、産業基盤をもつ企業向けに**オーダーメイド**でプログラム開発をしております。

業界共通トレーニングの実績

- 第1回7月13日、14日に18名（17社）、第2回10月13日、14日に13名（13社）の参加者で実施。
- 受講者からの声：
  - ✓ 電力の演習シナリオは現実に起こり得る内容で、背筋が冷たくなった。今後、どう事前に手を打っておくべきか、また起こった場合の対処のリハーサルとして、大変有意義であった。
  - ✓ CISOの仕事が非常に幅広く、会社としてどう実現していくべきかを考えさせられるきっかけとなった。社内外の関係部門との調整や、重要インフラの分野間連携の重要さに気づいた。経営層の巻き込みに努力したい。
  - ✓ テロ組織、国家のようなスキルとリソースを十分に持つ組織に狙われたときにどれくらい大きな被害を想定すべきかを再確認した。自社が最終ターゲットでなくとも、攻撃全体のストーリーの中に使われることは今まであまり想定できておらず、勉強になった。
  - ✓ 自社では権限移譲が進んでおり、一部門長でも経営視点を求められている。その視点で考えるべきことを再認識した。



ウォーゲームセッションの風景

今後の方向性

1. 第二期に向けて
    - ① カリキュラムの充実
    - ② 個別ニーズへの対応検討
    - ③ 秋葉原ＵＤＸの活用
2. 業種横断コミュニティの形成
    - ① 卒業生コミュニティ（中核人材、短期）
    - ② 情報共有メカニズム
3. 海外連携
    - ① 共同演習の実施
    - ② 新たなリスク情報の共有など
4. 新たな分野への対応
    - ① サプライチェーンにおけるリスクマネジメント
    - ② 自動車分野　等

ご清聴ありがとうございました。