IPA Better Life with IT

【短期プログラム】
電力、ガス、水道、情報通信など（広域インフラ系）業界向け
第二回責任者クラス向け業界別トレーニングご案内資料

2018年9月

IPA産業サイバーセキュリティセンター

2018/9/20：更新

業界別トレーニング　－　トレーニングの特徴

トレーニングの特徴

- サイバーセキュリティ戦略に関係する**責任者クラス向け**のトレーニングです。
  - CISO、CIOに相当する役割を担っている方
  - IT部門、生産部門、事業企画部門などの統括責任者及びマネージャークラスの方
  - セキュリティ、システム、ネットワーク運用管理責任者
- 業界別に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です。
- 業界別に考慮すべきセキュリティ要件、安全性要件を織り込んだ具体的なディスカッションを行っていきます。
- **直観とは相反するサイバーリスク**の特徴を具体的なシナリオに基づいて経験することができます。
- 海外子会社、系列企業、そしてサプライチェーン等の**ビジネスパートナーが直面するサイバーセキュリティ規制**について、具体的なシナリオに基づいて経験することができます。
- グループワークを通じて、**業界が直面するアジェンダ**を整理することが可能です。
  - 業界別のサイバーセキュリティ・サプライチェーン
  - 業界別のサイバーセキュリティ人材プール
  - 業界別のサイバーセキュリティ規制対応等
- 受講者間の人脈だけでなく、講師をはじめとするサイバーセキュリティ専門家、監督省庁や関係者との人脈形成、ネットワークを構築頂けます。

電力、ガス、水道、情報通信など（広域インフラ系）業界向け 業界別トレーニング － プログラム内容（シナリオ案）

- 2日間を通じてシナリオ形式のグループワークが中心となり、参加者には、仮想企業のサイバーセキュリティ戦略に関係するシニアリーダーとして責任者クラスのロールを担って頂き、業界別に企業が直面するサイバーリスクへの対応について熟議をしていただきます。
- 欧米におけるサイバー規制や政策の動向、ベストプラクティスなどを学ぶことが可能なプログラムとなっております。

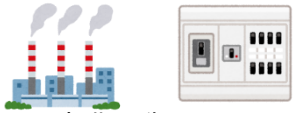
シナリオ①：海外規制対応

海外では重要インフラ向けのサイバーセキュリティガイドラインが整備され、サイバー電力も対応を迫られることになりそうです。果たして何のガイドラインを、どこまで、いつまでにやれば良いのでしょう？

規制 **体制** 人材 人脈 技術 文化

様々な業界別の規制やガイドラインについて、規制動向や法律に則った情報作成・開示などの作業を通じ、サイバーセキュリティ・レジリエンス向上策と手順を学びます。

シナリオ②：残存リスク



諸外国の産業制御システムをたびたび窮地に陥れたマルウェア。サイバーガスでも感染が発生し、機材を交換しましたが、症状は改善されません。制御システムを守るあなたの行動は？

規制 **体制** 人材 人脈 **技術** **文化**

サイバー防御の原理・原則を、組織にとって受容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③：センサーとIoT

サイバー通信のデータセンターでは、空調の適切な制御が課題となっています。一方で、センサー機器へのサイバー攻撃についてはどのような対策が考えられるでしょう？責任分解をどう考えますか？

規制 体制 **人材** 人脈 **技術** 文化

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、データの改ざんによるサイバーテロ対策を学びます。

シナリオ④：重要区画と監視

制御室及び機器が格納されている部屋の入退室管理や監視は行き届いていますか？技術革新によりサイバー攻撃に使う手口もより高度化している昨今、サイバー水道局が取るべき対策は？

規制 体制 **人材** **人脈** **技術** 文化

サイバー防御におけるリスク査定では、これまで想定されていなかったリスクに直面することが少なくありません。リスクに対する対策及び投資対効果だけでなく、リスク感度を高める方法を学びます。

※シナリオ案は一例としてご紹介しています。グループ編成などによってご紹介していないシナリオを実施させて頂く場合もありますのでご了承ください。

（ご参考）責任者クラスが直面するサイバーセキュリティ課題

- グループワークで熟議を深めていく中で、以下の6つの視点による課題整理を目指します。

①規制

- **海外サイバー規制動向、サイバー法、訴訟動向**などからセキュリティリスクに関する課題を整理
  - ✓ (日本）サイバーセキュリティ基本法
  - ✓ (欧州）NIS Directive, EU一般データ保護規則（GDPR）
  - ✓ (米国) Cybersecurity Information Sharing Act
  - ✓ 欧米における訴訟動向

②体制

- **CSIRT、BCP（事業継続計画）、サイバーリスク管理**など体制の課題を整理

③人材

- **CSIRT人材、IT(情報技術)/OT(制御技術)セキュリティ人材**など横展開に向けた課題を整理
  - ✓ 人材像と人材配置、人材の評価手法
  - ✓ 能力開発のロードマップとマイルストーン
  - ✓ “産業セクタ全体での人材プール“vs“自社人材“
  - ✓ 国内外における人材育成プログラムの動向

④人脈

- **政府機関、国内外のサイバーセキュリティ専門家・有識者との人脈形成**して活用するための課題を整理
  - ✓ 監督省庁関係者、国内外のCISO/CIO、ISAC、学術・非営利組織、スタートアップ企業

⑤技術

- **安全性評価、セキュア調達、サプライチェーン**など技術的な要求事項などの課題を整理
  - ✓ 安全性評価の基本的考え方とサイバーリスクの特性
  - ✓ セキュア調達において必要となる国際技術標準
  - ✓ セキュア調達、安全性評価などの海外検討動向
  - ✓ サプライチェーン・セキュリティの実現

⑥文化

- **リスク受容と免責、リーダー像の形成**など組織文化における課題を整理

業界別トレーニング　－　ご留意事項

ご留意事項

- 本トレーニングでは、参加者の役職や担当職務、事前に送付させて頂くアンケート、また受講人数のバランスも踏まえグループ編成を行わさせて頂きますのでご協力をよろしくお願いします。また本トレーニングで実施するシナリオについては、講師の判断により進めさせて頂きます。

- 本トレーニングでは、グループディスカッションによって仮想企業における意思決定とガイダンスを行いますが、業界別に熟議を行いサイバーセキュリティに関する課題を整理して頂くため、自社の状況の共有をお願いさせていただく場合がございます。この場合、受講者のご判断により、開示できる範囲でご対応のほどお願いします。（本トレーニングに参加する受講者、講師、他関係者より機密保持誓約書にサインを戴きます。）

- 本トレーニングでは、パソコンは必須でありません。ご持参頂いた場合は、グループ発表の資料作成などに使用することが出来ます。（その場合トレーニング終了後に一旦作成頂いた資料を集約させて頂きます。）

- 本トレーニングにて作成頂いたグループ発表の資料、またノートテイカーによる講演と報告を記録した開催報告書は、トレ―ニング終了後にお時間を頂きグループごとに送付させて頂きます。（通常1か月以内に送付させて頂きます。）

（ご参考）2017年度業界別トレーニング受講者の感想

- 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。

- 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。

- 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。

- シナリオが非常にリアリティがあり、新規性もあって大変勉強になりました。実際に自動車業界で起こり得る脅威に対する対象について自動車業界の情報セキュリティ担当者の方と語り会えたことは、大変貴重な経験になりました。

- 実際にシナリオをやってみて、理解が深まりましたし新しい気づきがありよかったです。また知識ではなく知恵を学ぶ人脈の重要性を認識できました。

講師陣のご紹介

講師略歴

門林　雄基
奈良先端科学技術大学院大学 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年以上にわたり従事。また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。業界に200人以上の卒業生を輩出している。
- IPA「産業サイバーセキュリティセンター」における人材育成事業に構想段階より参画。この他、内閣サイバーセキュリティセンターが主催する重要インフラ13分野の分野横断的演習においても有識者委員を務める。
- 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する。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させた。
- 欧米との豊富な人脈を生かし、日本と海外のサイバー人材交流を続けている。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。

講師陣のご紹介

講師略歴

宮本　大輔
奈良先端科学技術大学院大学 特任准教授

- 東京大学情報基盤センターを経て現職。フィッシング対策研究およびセキュリティ人材育成に従事。
- 日欧国際共同研究プロジェクトに参画した経験を持つ。ビッグデータと機械学習をセキュリティ用途に応用し、海外からも注目を集める。
- 研究の傍ら、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する。国際電気通信連合　電気通信標準化部門(ITU-T)においてフィッシング対策のための国際標準を成立させた。またインターネット技術の国際標準化団体IETFにも参画した経験をもつ。
- IPA産業サイバーセキュリティセンターにおいて海外の標準化動向や規制動向をふまえたサイバー演習や人材育成を担当する。

2018年度業界別トレーニング　－　対象業界について

業界別トレーニングの対象業界

項目（実施予定日）	対象業界	テーマ
第一回 ⇒8/24(金),25(土)	金属、石油、化学、製薬、スマートファクトリーなど[産業基盤系]業界	・製造業を中心としたP-SIRTの体制構築、また高品質を実現する生産体制についてディスカッションできる。 ・工場自動化関係、自動車製造などスマートファクトリーに関する課題を検討できる。
第二回（今回実施） ⇒11/16(金),17(土)	電力、ガス、水道、情報通信など[広域インフラ系]業界	・送電、ガス、また水道などの広域的なライフラインを安全・安定運用する体制についてディスカッションできる。 ・遠隔での保守点検や遠隔情報収集などスマートメーターに関する課題を検討できる。
第三回 ⇒2/15(金),16(土)	鉄道、航空、船舶、スマートモビリティなど[交通・物流系]業界	・交通系に対する安全運用、また高い品質を持つ製品やサービス（モバイル決済など）についてディスカッションできる。 ・スマートモビリティ（自動運転）に関する課題を検討できる。 ・ビル施設の運用・管理の課題を検討できる。

電力、ガス、水道、情報通信など（広域インフラ系）業界向け 業界別トレーニング － 開催概要

テーマ

業界戦略、経営課題解決のためのセキュリティ戦略

- 「サイバーセキュリティ経営」の時代、備えは進んでいますか

対象者

- 第二回目の対象業界は、**電力、ガス、水道、情報通信など（広域インフラ系）業界**に係る制御システムユーザー企業、系列企業、ハード・ソフトウエアベンダー企業などを対象としております。
- 対象者は、上記企業において下記の責任者クラスの方を対象としております。
  - CISO、CIOに相当する役割を担っている方
  - IT部門、生産部門、事業企画部門などの統括責任者及びマネージャークラスの方
  - セキュリティ、システム、ネットワーク運用管理責任者

日程/開催場所

- 日程：2018年11月16日（金）～ 11月17日（土）
- 場所：独立行政法人情報処理推進機構

東京都文京区本駒込二丁目28番8号　文京グリーンコートセンターオフィス8階

定員

- 最大30名（定員になり次第、募集を締め切らせて頂きます。）

受講料

- 価格　8万円（税込）（受講料には、交通費・食事代は含みません）

電力、ガス、水道、情報通信など（広域インフラ系）業界向け 業界別トレーニング　－　全体像（予定）と受講によって得られるアウトカム

業界、企業成熟度、選定したい課題・テーマごとにグループを分け、サイバーセキュリティ対策能力における自社の成長ステージに応じたトレーニングを受講頂くことが可能。

1日目　10:00～18:00 (※18:30-20:00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（11:00-17:00）

・仮想企業を想定し、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

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　10:00～17:00

実践的演習セッション

グループワーク（10:00-14:00）

・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
※昼食時間(1時間程度)をはさみます

グループ発表（14:00-15:00）

・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（15:00-17:00）

・講師陣による講評

開催報告の送付（後日）

・開催報告書(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

本トレーニング受講によって得られるアウトカム

- ✓ 責任者クラスが理解・認識すべきサイバーセキュリティ課題の把握
- ✓ 自社とのギャップ分析　※自社のサイバー対策の成熟度の把握
- ✓ 受講者人脈、サイバーセキュリティ専門家有識者との人脈形成
- ✓ 国内外規制動向の把握、ベストプラクティスの把握
- ✓ 海外事例の把握
- ✓ リスクシナリオの蓄積

サイバーセキュリティ業界別トレーニング
お申し込み先及びお問合せ先

募集期間

第二回（2018年11月16日～17日開催）の募集期間は、2018年10月15日までと致します。
(募集定員に到達し次第、募集を締め切りとさせて頂きますので、お早めにお申し込みください。)

お申込み方法

WEB上の受講申込書に必要事項を記入していただき、**郵送でお申し込みください。**
※お申込みいただきましたら、担当者よりご連絡差し上げます。

お問い合わせ先：　03-5978-7554（直通）（受付時間）平日9:30-18:00
coe-hrd-info@ipa.go.jp

受講申込書送付先：〒113-6591　東京都文京区本駒込2-28-8
文京グリーンコートセンターオフィス17階
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　中山宛

※原則として、納入後の受講料はキャンセルされる場合でも、返金は致しかねますので予めご了承ください。

URL：　http://www.ipa.go.jp/icscoe/index.html

【個人情報の取り扱いについて】
弊機構は、本プログラムの申込のためにご提出頂いた個人情報の適切な管理に努めております。ご提供頂いた個人情報は、本プログラムを提供するために必要な範囲（事務処理および講師への当日受講者リストの配布等）で利用させて頂きます。個人情報保護についての詳細は下記のページをご参照ください。
http://www.ipa.go.jp/about/privacypolicy/index.html