【短期プログラム】
金属・石油精製・素材産業（PA）業界様向け
第三回サイバーセキュリティ業界別トレーニングご案内資料

2017年12月

IPA産業サイバーセキュリティセンター

金属・石油精製・素材産業（PA）業界様向け業界別トレーニング ー テーマと特徴

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

トレーニングの特徴

- サイバーセキュリティ対策を統括されているCISO/CIO補佐（課長クラス以上を想定）に該当する方、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に該当する役割の方を対象としたトレーニングです。
- 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
- CISO/CIOとの人脈だけでなく、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。

【参考】
CISO/CIOが直面するサイバーセキュリティ課題

規制

- **海外サイバー規制動向、サイバー法、訴訟動向**
  - ✓ 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

体制

- **CSIRT、BCP（事業継続計画）、サイバーリスク管理**

人材

- **CSIRT人材、IT(情報技術)/OT(制御技術)セキュリティ人材**
  - ✓ 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

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**
  - ✓ 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

技術

- **安全性評価、セキュア調達、サプライチェーン**
  - ✓ 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

文化

- **リスク受容と免責、リーダー像の形成**

金属・石油精製・素材産業（PA）業界様向け業界別トレーニング
ー　開催概要

対象者

- 第3回目の対象業界は、**金属・石油精製・素材産業（PA）業界**の方を対象としております。
- 上記業界において、サイバーセキュリティ対策を統括されている**CISO/CIO補佐（課長クラス以上を想定）**に該当する役割を担っている方
- 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**に該当する役割を担っている方

日程/開催場所

- 日程：2018年2月16日（金）～2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

- 20名程度を想定

その他

- 本トレーニングでは、パソコンは必須でありませんので、持参は不要です。

金属・石油精製・素材産業（PA）業界様向け業界別トレーニング ー 全体像（予定）

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 (※18:30-21:00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）
  - ・架空の企業「サイバー金属」、「サイバー化学」、「サイバー石油」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
- 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）
  - ・架空の企業「サイバー金属」、「サイバー化学」、「サイバー石油」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）
  - ・架空の企業「サイバー金属」、「サイバー化学」、「サイバー石油」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

本トレーニング受講によって得られるアウトカム

- ✓ CISO、CIO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
- ✓ CIO/CISO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

業界別トレーニング　プログラム詳細（シナリオ案）

概要

- 参加者には、架空の企業「サイバー金属」、「サイバー化学」、「サイバー石油」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って頂き、ケーススタディを実施します。
- 架空の企業である、「サイバー金属」、「サイバー化学」、「サイバー石油」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、ケーススタディを通して学ぶことが可能なプログラムとなっております。

プログラム内容

シナリオ①：海外規制対応


国際競争力獲得のため海外子会社の設立を検討するサイバー化学。CISOのあなたは海外におけるサイバーセキュリティ規制・法律動向についてどのような手順で、どれくらいのコストをかけて検討・対応をすすめていきますか？

規制 体制 人材 人脈 **技術** 文化

企業金融情報開示ガイダンス（米）や NIS 指令（欧）などの法律について、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、リスク監査と手順を学びます。

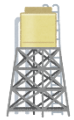
シナリオ②：マルウェアへの対応


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。サイバー石油工場でも驚くほど簡単に感染事件が起こりました。制御システムをサイバー脅威から防ぐCISOのあなたの行動は？

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：周辺への攻撃

工業地帯に位置するサイバー金属工場は電力や水などの資源を地域社会と協力しながら調達しています。サイバー攻撃のリスクを下げ、重要資源を安全に調達するために必要な検討事項とは？

規制 体制 **人材** **人脈** 技術 文化

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、データの改ざんによるサイバーテロ対策を学びます。

業界別トレーニング　プログラム詳細（シナリオ案）

プログラム内容

シナリオ④：リスク監査


サイバー金属工場の生産効率を低減させるためだけのサイバー攻撃。例えば工場内の重要かつ危険な作業工程において場内で使用する警告音を、意図しない場面で再生される問題をどう事前にリスク監査すればよいでしょう？

規制 **体制** 人材 人脈 **技術** **文化**

サイバー空間の拡張により意表を突く攻撃が生まれています。特に人間が認知し難いものは、平時における検討からも外されがちです。本シナリオでは事前検討の範囲を広げる方策を学びます。

シナリオ⑤：地域との共生


サイバー石油の工場周辺では、地方自治体が独自に環境計測装置を導入しています。この機器類の脆弱性が悪用された場合、工場にはどのような影響があるでしょうか？また、事前に何に備える必要があるでしょうか？

規制 **体制** 人材 **人脈** 技術 文化

地域との共生を図る上で、関係者とのサイバー攻撃対策に必要な連携を考えます。また、状況に応じて過不足なく証拠を保全し、信頼できる形で共有していくための議論を行います。

シナリオ⑥：想定外のリスク


サイバー化学の工場内への人・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。空中からの場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？

規制 **体制** 人材 **人脈** **技術** 文化

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
講師陣のご紹介

IPA

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。

業界別トレーニング
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。

金属・石油精製・素材産業（PA）業界向け業界別トレーニング
ー　受講料

受講料

- 価格　8万円（税込）※2日間

受講料お支払い方法

- お申込み後、受入決定後、順次、申込企業様の連絡担当者様宛に「受講決定通知（兼振込依頼書）」などを送付いたします。受講料は記載された指定期日までにお振り込みください。

※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。

金属・石油精製・素材産業（PA）業界向け業界別トレーニング ー お申込み方法・募集期間

お申込み方法

- 受講意思を有する企業様におきましては、本資料の最後に記載のIPA「産業サイバーセキュリティセンター」担当者に、受講プログラム名および受講予定人数をお知らせ下さい。
- 受講者の人選が確定していない場合でも、予約として席を確保させて頂きます。
- 受講意思を有する企業様に対しては別途「受講申込書」をお送りいたします。必要事項をご記入の上、IPA「産業サイバーセキュリティセンター」担当者宛に提出ください。
- 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。

※セミナーに関する説明をお聞きしたい場合、本資料の最後に記載されております、IPA「産業サイバーセキュリティセンター」担当者にお問い合わせ下さい。対面での説明をご希望される場合、訪問対応も可能です。

【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

募集期間

- 第3回（2018年2月16日-17日開催）の募集期間は、2018年1月31日までと致します。

金属・石油精製・素材産業（PA）業界向け業界別トレーニング
ー　機密保持について

- 本プログラムでは、グループディスカッション等において、自社の状況を共有する場合がございます。
  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。

- 今回のプログラムに参加する受講者、講師、他関係者より機密保持誓約書にサインを戴きます。

（ご参考）第一回および第二回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。

金属・石油精製・素材産業（PA）業界向け業界別トレーニング ー　お問合せ先

〒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ビル

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　短期プログラム担当者

TEL：　03-5978-7554（直通）
E-mail：coe-hrd-info@ipa.go.jp

（受付時間）　平日9:30-18:00