IPA Better Life with IT

【責任者向けプログラム】
第1回業界別サイバーレジリエンス強化演習（CyberREX）

サイバーレックス

【対象業界：電力、鉄道、ビル、自動車（製造系）、ファクトリーオートメーション】
ご案内資料

2019年7月

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

開催概要

■ 第1回業界別サイバーレジリエンス強化演習(CyberREX)

サイバーレックス

Cyber Resilience Enhancement eXercise by industry

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

～高まる「サイバーインシデント」の脅威、あなたの部門の備えは万全ですか～

対象業界・対象者

- **対象業界**は、電力、鉄道、ビル、自動車（製造系）、ファクトリーオートメーション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、下記の方を対象としております。
  - ✓CISOに相当する役割を担っている方
  - ✓IT部門、生産部門などの責任者・マネージャークラスの方

開催日程・場所

日程：2019年8月23日（金）～ 8月24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

受講料・定員

- 受講料8万円（税込）（※受講料には、交通費・食事代は含みません。）
- 最大30名（※定員になり次第、募集を締め切らせて頂きます。）

本演習の目的・特徴

- 「**サイバーレジリエンス**」とは、
  サイバーセキュリティに関する**対応力・回復力**を
  強化し、企業組織全体の**強靭化**を図ることです。

トレーニング実施風景

目的

- 本演習では、**部署・部門**のサイバーセキュリティに
  関する対応力・回復力を強化し、**業界特性**を意識
  した企業組織全体の強靭化を目的としています。

※昨年度の「業界別トレーニング」から「業界別サイバーレジリエンス強化演習」に
名称を変更し、目的を明確にしました。

特徴

- そのため、**業界別**に仮想企業を想定した、
  シナリオによる**実践的演習**の形式を中心とした
  トレーニングとなっています。

一週間前にマルウェア感染が疑われ、交換したばかりの保守用機器が、再びマルウェアに感染する事案が発生した。～～～～～～系統制御に影響は出ていないものの、問題が再発したということで、何かしらの脅威の残存が疑われている。

この問題に対して、セキュリティ責任者であるあなたは、即時の対応、短・中期的な対応、中・長期的な対応について方針を検討することになった。

講義シナリオ（抜粋）

- また、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やガイドライン等の解説に関する**集中講義**を行います。

2019年度の変更点

- 一度参加された企業、あるいは一度参加された方でも再度参加して頂けるよう、最新の情報を取り込み、新たな**シナリオを追加**しています。

- ご要望の多かったサイバーセキュリティ規制やガイドライン等の解説に関する「**集中講義**」を新たに追加しています。

- 今回、2017-2018年度に実施した演習の中から反響の大きかった業界（電力、鉄道、ビル、自動車（製造系）、ファクトリーオートメーション）をピックアップし開催します。

※ なお、以前よりご要望の多かった**大阪での開催**(9月)を設定することで、西日本の方々にも参加しやすい機会をご用意しました。

受講による効果・受講生の声

受講による効果

- 受講後は、責任者クラスが認識すべき「サイバーセキュリティ課題」や「自社の体制や規程等とのギャップ分析」への**理解度及び対応力の向上**、さらに「起こりうるリスクシナリオ」、「国内外の規制動向、海外事例」に対する**知見の蓄積**といった効果を得られます。
- 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。

受講生の声

- CSIRT等組織としての**体制整備**の重要性と**サイバーセキュリティに対する感度**の向上の必要性を再認識した。
- OT責任者として、**制御サイバーセキュリティ対策の体制、規程化**に向けて非常に参考になった。
- **通常考えないようなケース**があり刺激的であった。また業界特性が想像していたより多くあり、**業界別**の意義が感じられた。
- 従来の経験、知識では想定できない攻撃手法、リスクを学ぶ事ができた。関係者とも情報共有して、**特異なケースのリスク**と思われる内容が将来の大きく広範囲な脅威となり得る事を注意喚起していきたい。
- 海外の取り組み動向や事例は普段業務の中で調査する機会がほとんどない為、非常に有益であると感じた。また**人材交流**の面でも同業者の他部門の方と交流できた事は非常に有益であった。

スケジュール

IPA

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）

・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

※懇親会（18:30～20:00、任意参加）

・受講生・講師・関係者等との人脈形成、ネットワーク構築

2日目 10:00～19:00

講義・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

グループ発表（14:00～16:00）

・仮想企業におけるサイバーセキュリティ成熟度向上

集中講義（16:00-17:00）

・海外の規制、ガイドライン、セキュリティ標準の解説に関する集中講義

総合討論・全体講評（17:00-19:00）

・講師陣による講評

※開催報告書の送付（通常1か月以内）

・開催報告書を受講者の方に、後日送付

講師陣紹介

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、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。
- 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。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。
- 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。

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。
- 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。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。

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頂きます。）

- 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。）

お申し込み先・お問い合わせ先

募集期間

第1回業界別サイバーレジリエンス強化演習（2019年8月23日～24日開催）の募集期間は、2019年7月1日～31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。）

お申し込み方法

WEB上の受講申込書に必要事項を記入していただき、**メールにてPDFで送付頂くと共に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。

お問合せ先：　03-5978-7554（直通）（受付時間）平日9:30-18:00
coe-promotion-info@ipa.go.jp

担当者：　中山、小林（太美子）

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
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：　https://www.ipa.go.jp/icscoe/program/short/specific_industries/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