IPA Better Life with IT

【責任者向けプログラム】
令和2年度第3回

業界別サイバーレジリエンス強化演習（CyberREX）

【対象業界：「インフラ系」電力、鉄道、ビル・物流
「産業系」自動車（製造）、ファクトリーオートメーション】

ご案内資料

令和2年8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

■ 令和2年度第3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 **E**nhancement e**X**ercise 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・物流、自動車（製造）、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

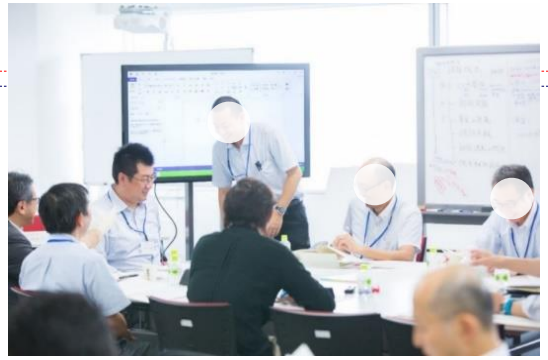
- 日程：令和2年11月27日（金）　～　11月28日（土）
- 場所：ナレッジキャピタルカンファレンスルームタワーB RoomB01+02
  大阪府大阪市北区大深町3-1 グランフロント大阪 北館タワーB 10階
  ※会場までのアクセス案内：https://www.kc-space.jp/conference/items/towerB.pdf

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。）※最少催行人数を10名とします

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。

> 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）

特徴

- **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。
- 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。

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。

受講者の声

- 技術的なスキルで解決できることと経営層視点で考えるべきことをチームで協議でき、有意義であった。確かに**経験できるインシデントは実際は少ない**ので本演習は有効だと感じた。
- 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。
- 期待を上回り有意義であった。自分の同業種、そして立場に近い方々と交流することができ、**悩みや課題を共有**し、今後にもつながるプログラムであった。
- 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（予定）

1日目 10:00～18:00

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1（11:00～13:30）

・他業種交流も兼ねて、各業界に共通的な課題シナリオを抽出して、仮想企業を想定した討議
・発表のための資料作成
※昼食時間(1時間程度)をはさみます

グループ発表（13:30～14:30）

・仮想企業におけるサイバーセキュリティ成熟度向上

グループワーク2（14:30～17:00）

・業界別に、関心の高い課題シナリオを抽出し、仮想企業を想定した討議
・発表のための資料作成

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

2日目 10:00～19:00

グループワーク3（10:00～14:00）

・同じグループで別の課題シナリオを抽出し、仮想企業を想定した討議
・発表のための資料作成
※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
東京大学 情報理工学系研究科
准教授
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、奈良先端科学技術大学院大学を経て現職。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。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。

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、予めグループ編成を行います。
- 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、自社の状況をお話し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、他関係者より秘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（オンライン実施時を除く）。ご持参頂いた場合は、グループ発表の資料作成などに活用いただくことができます。（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。）

- 新型コロナウイルス感染防止対策のため、マスクの着用をお願いします。対策の詳細については「新型コロナウイルス感染症防止対策のご案内」をご確認ください。
- 11月19日（木）時点で、実施場所に「緊急事態宣言」が発令されている場合は、集合形式での実施は中止とし、「オンライン実施」とします。案内事項につきましては次ページをご確認ください。

オンライン実施の案内事項

- オンライン実施の場合、インターネットを通じて「Zoom」および「Microsoft Teams」を利用して行います。通信速度3.0Mbps以上のインターネット環境をご用意ください。
- 「Zoom」および「Microsoft Teams」は主催者側で準備し、招待URLを発行いたしますので、参加者の皆様は本トレーニング用のメールアドレス（私用・会社用どちらでも差し支えありません）をご準備ください。
- 事前に、Zoomの接続テストサイト（https://zoom.us/test)において、接続テストを行ってください。
- なおグループワークの発表資料作成は、「Microsoft PowerPoint」等のOFFICE製品が用いられますので、ご自身が使用するPCにインストールすることをお薦めします。

- オンライン実施の場合であっても、「秘密保持誓約書」をご提出いただきます。
- できるだけ自宅や所属会社の会議室等で参加し、第三者が立ち入らない環境を確保してください。第三者による不正参加防止の観点から、参加に使う場所をビデオで確認いたしますので、必ずビデオをオンにしてご参加ください。

  ※貸し会議室、ホテル等の商業施設を利用する場合、施設の営業状況や利用可能状況に関してはご自身の責任で確認してください。

詳細は、オンライン実施となることが確定した場合、別途ご連絡させて頂きます。

お申込み先・お問い合わせ先

募集期間

令和2年度第3回業界別サイバーレジリエンス強化演習（令和2年11月27日～28日開催）の募集期間は、令和2年10月23日（金）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頂き、メールにてPDFを送付ください。
※お申込み頂きましたら、担当者よりご連絡差し上げます。

お問合せ先：　03-5978-7554（直通）
coe-promotion-info@ipa.go.jp
担当者：　中山、笹崎
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/2020.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。https://www.ipa.go.jp/about/privacypolicy/index.html