【責任者向けプログラム】

令和3年度第2回（10月開催）
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」ビル、ガス 「プラント系」金属、石油、化学 】

ご案内資料

今回はオンラインにて実施します

令和3年9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3年度 第2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

業界特性を意識した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、ビル、ガス、金属、石油、化学業界に係る制御システムのユーザー企業、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・形態

- 日程：令和3年10月7日（木）　～　10月8日（金）
- 形態：オンライン開催

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、**業界特性に応じたシナリオ**を通じて
  サイバーセキュリティに関する対応力・回復力を
  強化した人材の育成を狙います。

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。

対象業界における過去の授業シナリオ例（抜粋）

- USB給電によるマルウェア感染
- セキュリティ成熟とC2M2
- サプライチェーンリスク
- Industrial IoTにむけた検討
- マルウェア感染の残存リスク
- 化学業界向けガイドライン
- 高所観察とドローンと工場
- 海外法令と日本の影響

等

- 海外子会社、系列企業、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

- **自社では想定していない**、かつ対応が難しい、とてもよく練られたシナリオで、演習を通して気づきを得られた。
- サイバー攻撃等のリスクが高まる中、自身の認識を向上させるだけでなく、**技術を導入し維持する費用がかかる**ことについて、経営層など**舵取りする方々にも理解を深めてもらう必要**を強く感じた。
- 参加者との議論やメンターからのコメントや指摘等で、**思考範囲が広がり**検討が進められた。
- サイバーセキュリティの**世界の動きなど幅広い情報**を教えて頂き、担当する設備が対応できているか見直す良い機会となった。
- 一見、自社に**関係ないと感じる事象でも、サイバーセキュリティの観点から考える**と自社へのサイバーテロの布石と思われるものがあり、そういった事象を認知するセンスが必要であると感じた。

スケジュール（予定）

【1日目】 10:00～18:00	
10:00～ 11:00	**導入講義** － 本演習のねらい － サイバーセキュリティとは － インシデント発生動向
11:00～ 14:30	**グループワーク1** － 課題シナリオ選択 － ディスカッション － 発表資料作成 ※昼食時間(1時間程度)をはさみます
14:30～ 15:30	**グループ発表（1回目）**
15:30～ 18:00	**グループワーク2** － ディスカッション － 発表資料作成

【2日目】 9:30～17:30	
9:30～ 14:00	**グループワーク3** － ディスカッション － 発表資料作成 ※昼食時間(1時間程度)をはさみます
14:00～ 15:30	**グループ発表（2回目）**
15:30～ 16:30	**集中講義** － 規制・ガイドライン解説 － 国際標準解説
16:30～ 17:30	**総合討論・全体講評** － 本演習のまとめ － 講師陣による講評

※「開催報告書」を受講者の皆さまに後日送付（通常1か月以内）

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。）

オンライン開催の案内事項

- 「Zoom」及び「Microsoft Teams」を利用します。
  パソコン等の端末及び通信速度3.0Mbps以上のインターネット接続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を発行します。
  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）をご用意ください。
- 「Microsoft Teams」への接続には、「**Microsoftアカウント**」が必要となります。本トレーニング用のメールアドレスを登録した「Microsoftアカウント」をご準備ください。
  ※会社用Microsoftアカウントの場合、社内ルール等により「Microsoft Teams」に接続できない場合がございますので、事前にご確認ください。
- 「Zoom」および「Microsoft Teams」の接続確認は、**実際に受講する環境とアカウント**で必ずお試しください。

- 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、主催者側が参加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申込者ご自身の責任で確認してください。

お申し込み先・お問い合わせ先

募集期間

令和3年度第2回業界別サイバーレジリエンス強化演習（令和3年10月7日～8日開催）の募集期間は、令和3年9月10日（金）までとします。（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。

受講申込書：　https://www.ipa.go.jp/files/000092666.docx
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：　九嶋/佐藤（陽）
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　九嶋宛

※原則として、納入後の受講料は返金致しかねますので、予めご了承ください。

【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