IPA Better Life with IT

【責任者向けプログラム】

サイバー危機対応机上演習（CyberCREST）
サイバークレスト

ご案内資料

2021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(1)

制御システムを有する企業・団体における
戦略的なサイバーセキュリティ対策を学ぶ3日間

サイバー危機対応机上演習※1,2では、制御システムを有する企業・団体のサイバーセキュリティ責任者を対象に、組織を守る為に必要なスキルとメソッドをご紹介します。

ITやOT(Operational Technology)に関する最新のサイバー脅威を学ぶとともに、米国の先進的なサイバーセキュリティ戦略である「**コレクティブ・ディフェンス**」、近年重要性が説かれている「**任務保証**」を学習いただけます。

本演習では、米国サイバーコマンド出身の専門家やCISO、セキュリティアーキテクトの専門家らが講師を担当します。各講師が自身の経験を共有するとともに、ロールプレイング演習を交えながら、この戦略が企業にどのようなメリットをもたらすのか、どのように企業に適用すればよいのかをご紹介します。

※1 サイバー危機対応机上演習(CyberCREST: Cyber Crisis RESponse Table top exercise)
※2 米国IronNet Cybersecurity社のナレッジ・ノウハウをベースに、産業サイバーセキュリティセンター提供プログラムとして、IronNet Cybersecurity社とIPAが日本における社会インフラ、産業基盤をもつ企業様向けにオーダーメイドで演習開発をしております。

開催概要(2)

対象者

- 制御システムを有する企業・団体のサイバーセキュリティ対策を統括されている責任者
  ※セキュリティ・オペレーション・センター(SOC)の責任者、サイバーセキュリティ対策部門の管理職の方々もご参加いただける内容となっております。

本演習で得られること

- 現実的な攻撃デモを通して、防御側が検知しにくい複雑な手法による攻撃を分析し、攻撃パターンを理解できます。
- コレクティブ・ディフェンスを理解し、自社に導入できるようになります。
- 受講者の方々や海外セキュリティ専門家とのコミュニティやリレーションを構築できます。

開催概要(3)

日程/開催形態

日程:　2021年9月15日(水)～9月17日(金) 3日間

開催形態:　**オンライン**(Webexを使用予定)

※ご自宅またはオフィス等からご参加ください。
※新型コロナウイルス感染症の状況により変更しました。

定員

- 10名

受講料

- 30万円(税込)

言語サポート

- 本演習は英語ベースで行いますが、日本語テキストのご提供、同時通訳(日英)などを予定しております。
- オンライン開催用の同時通訳のご提供を予定しております。

オンライン開催のご案内事項

お願い事項

◆ 用意いただきたいもの

- オンライン開催に伴い、受講用のPCをご用意ください。
- 演習ではWebexを使用予定です。各自でご用意いただいたPCにWebexをあらかじめインストールいただくようお願いいたします。
  ※通信速度5.0Mbps以上のインターネット環境をご用意ください。
- 同時通訳用に受講用PCとは別に端末（スマートフォン等）をご用意ください。
- 有線のヘッドセット（マイク/イヤホン）、カメラをご用意ください。
  ※カメラはPCに付属しているもので構いません。

◆ 実施いただきたいこと

- 演習1週間前を目安に事前のWebex接続テストを行いますのでご参加ください。テストのご案内は別途ご連絡いたします。
- 同時通訳のアプリをスマートフォンへインストールください。アプリの詳細は別途ご連絡いたします。

スペック要件

- 推奨OS　Windows7 SP1/MacOS 10.12以上
  ※通訳をPCで聴く場合は、Google Chromeが動作するWindows 10もしくはMac OSの端末をご用意ください。
- 推奨CPU　Intel Core i5 以上
- 推奨RAM　4.0 GB以上

コレクティブ・ディフェンス

コレクティブ・ディフェンスとは

- サイバー脅威は日々複雑性を増しており、個々の企業だけでは自組織を守ることが難しくなっています。国家や、国家の支援を受けた攻撃者など、潤沢なリソースを持つ脅威主体に対して、企業側が政府や同業他社と情報共有を図り、協働して立ち向かう戦略**「コレクティブ・ディフェンス」**が重要となっています。
- 米国サイバースペースソラリウム委員会（CSC: The Cyberspace Solarium Commission）における報告書※1では、これまでのサイバー脅威に対抗する戦略を再構築し、サイバー抑止力を高めるための方法として、コレクティブ・ディフェンスの必要性を説いています。

※1 The Cyberspace Solarium Commission (2020). “Cyberspace Solarium Commission Report”

任務保証

任務保証とは

- 重要インフラ事業者などの企業が、自らが遂行すべき業務やサービスを「任務」として捉え、それを着実に遂行するために必要となる能力や資産を確保する概念。障害や攻撃が発生しても、サービスの継続的な供給に関する責任を全うする考え方です。
- 内閣サイバーセキュリティセンターが発行するサイバーセキュリティ2020では、任務保証が持続的なサイバー空間の発展に必要であると記載されています。

本演習3つの特徴

特徴①

「米国の先進的なサイバーセキュリティ戦略“コレクティブ・ディフェンス”」

- Red Team(攻撃者側)とBlue Team(防御側)の視点で、攻撃手法や攻撃パターンについて学ぶとともに、これらのリスクを軽減させ、自社をどのように守っていくべきかを学習いただけます。
- 実践的な演習を通じて、コレクティブ・ディフェンスがご自身の企業へどのような利益をもたらすのか、導入方法も含めて学んでいただけます。

特徴②

「CISOとして成長するための個別フィードバック」

- 担当講師より、演習全体を通して受講者お一人ずつへフィードバックを行います。CISOとして成長するための助言をいたします。

特徴③

「米国重要インフラ分野の有識者による特別講演」

- 米国重要インフラ分野の有識者が、自身のコレクティブ・ディフェンスに関連するこれまでの経験談などをお話いただく予定です。

講師陣

ジョージ・ラモント氏（George Lamont）

IronNet Cybersecurity, Inc.
最高情報セキュリティ責任者（CISO）

米サイバーコマンドの大佐として、初の合同サイバートレーニング、認証基準およびサイバーフラッグ演習を始めた第一人者。
これまで、様々な国で通信ネットワークを構築し、世界中でチームを率いた経歴がある。ニューハンプシャー大学で数学と電気工学の理学士号を、オクラホマシティ大学でMBAを取得。CISSP保有。

フェルナンド・マイミ博士（Fernando Maymí, Ph.D.）

IronNet Cybersecurity, Inc.
トレーニング部門　本部長

米陸軍のシンクタンクであるArmy Cyber Instituteの所長代理を歴任し、産官学のパートナーシップ活動に従事。また、サイバー空間の問題に関する議会のリーダーや企業の重役を務めた。
CISSP All-in-one Exam GuideおよびCompTIA CySA+ Cybersecurity Analyst Certification All-in-One Exam Guideの著者。

講師陣

スティーブ・ザルースキー氏（Steve Zalewski）

Levi Strauss & Co.
副最高情報セキュリティ責任者（副CISO）

Levi Strauss & Co.社の副CISO(Chief Information Security Officer)であり、チーフセキュリティアーキテクト、サイバーセキュリティインテリジェンスやインシデント対応ディレクター。
サイバーセキュリティ戦略とインシデント対応組織のマネジメントを担当し、前職ではPacific Gas and Electric Company社でエンタープライズセキュリティアーキテクトなどの役職も経験。

ブライアン・ディクストラ氏（Brian Dykstra）

Atlantic Data Forensics社
最高経営責任者（CEO）

コンピュータフォレンジックや電子的データ探索、フォーチュン500向けのデータ漏えいのインシデント対応を行うAtlantic Data Forensics社の創立者兼CEO。
Mandiant社の共同創立者であり、CIOやプロフェッショナル教育ディレクター、FBIアカデミーでのサイバー犯罪の講師を歴任。CCFP、CISSP、CISSP-ISSAP、CIFI。

スケジュール　1日目(予定)

通訳形態：
同時通訳

9月15日 (水) 9:00～17:00

9:00～9:45　イントロダクション

9:45～12:05　攻撃デモ

ステージ1　攻撃デモ　- ITペネトレーション -
ステージ2　攻撃デモ　- ITからOTへの横展開 -
攻撃者側はフィッシング攻撃などからITシステムへ侵入します。侵入したマルウェアは横展開をし、OTシステムへの侵入を図ります

※途中1時間のお昼休みを挟みます

12:05～13:05　お昼休み

13:05～15:25　攻撃デモ

ステージ3　攻撃デモ　- OTペネトレーション -
ステージ4　攻撃デモ　- OTへの物理的影響 -
OTのゲートウェイを突破したマルウェアは物理的にOTシステムにダメージを与えます

※途中休憩あり

15:25～16:25　ケーススタディ
- CISOへのインタビュー -

実際にコレクティブ･ディフェンスを導入している米国企業の事例紹介

16:25～17:00　コレクティブ･ディフェンス　導入講義

スケジュール　2日目(予定)

9月16日 (木) 9:00～17:00

通訳形態：
同時通訳

9:00～10:00　特別講演

Eclectic Technology 社長
（元・北米電力信頼度協議会副社長兼
最高セキュリティ責任者）である
ティム・ロクシー氏による特別講演

10:00～13:10　コレクティブ・ディフェンス

・企業におけるセキュリティ概要

・実用的脅威インテリジェンス
- 組織の脅威インテリジェンスプログラムを設計、改善できるようにする

・コレクティブ・ディフェンスによる協力

※途中休憩あり

13:10～14:10　お昼休み

14:10～15:20　コレクティブ・ディフェンス

・コレクティブ・ディフェンスの開発
- サプライチェーン、同業他社等の関わり合いを理解し、コレクティブ・ディフェンスを実装できるようにする

※途中休憩あり

15:20～16:35　任務保証

・導入講義
- 主要な機能、資産、依存関係を理解する

・ミッション重視のリスクマネジメント
- ミッションを重視したリスクアセスメントや第三者の評価、リスクを低減するための連携を理解する

16:35～17:00　コレクティブ・ディフェンスと任務保証のオープンディスカッション

スケジュール　3日目(予定)

9月17日 (金) 10:00～18:00

通訳形態：
逐次通訳

9:00～9:30　グループ演習イントロダクション

9:30～10:55　グループ演習1

・コレクティブ・ディフェンス計画を策定するためには
　どうすればいいのかを学習します
※途中休憩あり

10:55～12:10　グループ演習2

・政府や同業他社と協働した、迅速なアラートのトリアージ
　について学習します

12:10～13:10　お昼休み

13:10～14:35　グループ演習3

・悪意ある行動の分析
※途中休憩あり

14:35～16:00　グループ演習4

・コレクティブ・ディフェンスを必要とするインシデント対応を
　シナリオに基づいて学習します
※途中休憩あり

16:00～17:00　全体振り返り・フィードバック

・講師より、演習全体を通して受講者お一人お一人へ
　フィードバックを行います
　CISOとして成長するためにはどうすればよいのか等を
　お教えいたします

お申込み先・お問い合わせ先

募集期間

令和3年度サイバー危機対応机上演習（CyberCREST）（令和3年9月15日～17日開催）の募集期間は、令和3年9月10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をご送付ください。**
※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：　九嶋、佐藤

※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/all_industries/2021.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