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）ご案内資料

サイバークレスト

2020年12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/開催場所

- 2021年1月27日(水)～1月29日(金) 3日間
- 独立行政法人　情報処理推進機構
  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 13階会議室

※新型コロナウイルス感染症の状況により、延期もしくはオンラインでの開催となる場合がございます。

定員

- 25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。

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.
プロフェッショナルサービス部門ディレクター

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)

1日目（1月27日 (水) 10:00～18:00）

10:00～10:30　オープニングセッション

10:30～12:45　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

※途中休憩あり

12:45～13:45　お昼休み

13:45～15:45　攻撃デモ　- OTペネトレーション -

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

16:00～17:00　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

17:00～18:00　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)

2日目（1月28日 (木) 10:00～18:00）

10:00～11:00　特別講演

北米電力信頼度協議会の元副社長兼
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

※米国よりZoomを使用しての講演となります

11:00～12:45　コレクティブ・ディフェンス

・**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

※途中休憩あり

12:45～13:45　お昼休み

13:45～16:15　コレクティブ・ディフェンス

・**コレクティブ・ディフェンスの相互運用性**
- より効率的に運用するための人々の役割、組織、プロセス等を理解する

・**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

16:15～18:00　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

スケジュール　3日目(予定)

3日目（1月29日 (金) 10:00～18:00）

10:00～10:30　グループ演習イントロダクション

10:30～11:30　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

11:45～12:45　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

12:45～13:45　お昼休み

13:45～14:15　セッション

・悪意ある行動の分析

14:15～15:15　グループ演習3

・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

15:30～16:30　グループ演習4

・任務保証のために架空の組織を準備する
ロールプレイング演習を経験いただきます

16:30～17:30　グループ演習5

・コレクティブ・ディフェンス、任務保証を統合した
インシデント対応をシナリオに基づいて学習します

17:30～18:00　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

お申し込み先・お問合せ先

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、下記担当者よりご連絡差し上げます。

お申し込み先・お問合せ先: 03-5978-7554
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
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 中山宛

締切日:2020年12月18日（金）
（募集定員に到達し次第、募集を締め切らせて頂きますので、お早めにお申し込みください。）

※原則として、ご入金後に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。

【個人情報の取り扱いについて】
弊機構は、本演習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、本演習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