FUJITSU 人材育成・研修サービス
講習会
サイバー攻撃手法と攻撃検知手法

本コースでは、APT攻撃（Advanced Persistent Threat：持続的標的型攻撃）のような高度なサイバー攻撃を検知する着眼点を学びます。受講者自らがAPT攻撃を行いそれを検知する実習を通して、ファイアウォール・ミドルウェアなどのログからサイバー攻撃を検知します。

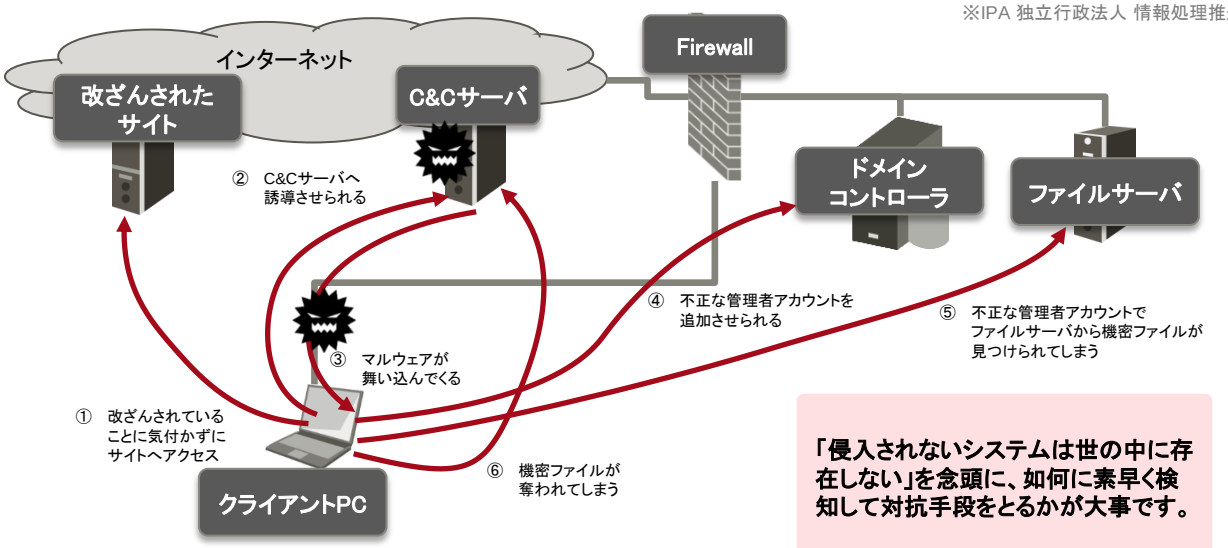
こんな課題をお持ちの方にお勧めします

- **高度なサイバー攻撃を検知するための着眼点を知りたい方**
- **高度なサイバー攻撃対策の考え方を知りたい方**
- **APT攻撃がどのようなプロセスで行われるのかを知りたい方**
- **APT攻撃を受けると最終的にどのような被害が出るのかを知りたい方**

参考：本コースで体験するサイバー攻撃のイメージ

APT攻撃をIPA※では、新しいタイプの攻撃と命名し、「ソフトウェアの脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャルエンジニアリングにより特定企業や個人を狙い、対応が難しく執拗な攻撃の総称」と定義しています。
以下に本コースで体験するサイバー攻撃のイメージを図示します。

※IPA 独立行政法人 情報処理推進機構



「侵入されないシステムは世の中に存在しない」を念頭に、如何に素早く検知して対抗手段をとるかが大事です。

本コースおすすめのポイント！

本コースでは実際のATP攻撃を受講者自らが行い、その攻撃をどのように検知できるか、という観点で実習を行います。
これにより、高度なサイバー攻撃を検知する着眼点が身に付きます。

コースの概要

サイバー攻撃手法と攻撃検知手法

期間：2日間

項目	内容
型番	USA61L
受講対象	SOC（セキュリティオペレーションセンター）のような業務を今後担当される方
コース概要	近年の攻撃者は標的およびそのシステムを綿密に調査し長期間にわたって機会をうかがって攻撃を行います。そのため、「侵入されることを前提」として、素早く検知し、対抗手段をとるかが重要です。未知の攻撃が増えている現在においては、現存の攻撃手法を知り、それを検知する実体験の積み重ねが重要です。本コースの演習ではAPT攻撃を模した攻撃演習シナリオを用いて攻撃手法および検知手法を体験し知見を得ることを目的としています。攻撃演習シナリオに沿って、攻撃者の立場で実際に企業ネットワークに模した環境に攻撃を実施し、防御側の立場で実際に攻撃の痕跡を検知します。この体験を通し、さらなるセキュリティマインド、検知/防御技術の向上に役立ててください。
前提知識	Windows OSの基本的な機能を知っており、MCSC程度の知識を有すること。LPICレベル2程度の知識を有すること。
コース価格	300,000円（税別）

日程・スケジュール

時間	1日目	2日目
午前	第1章　サイバー攻撃手法と攻撃検知手法 1.1　サイバー攻撃を取り巻く背景 1.2　Cyber Kill Chain 第2章　侵入とその検知手法 2.1　侵入の手口とその検知手法 2.2　マルウェアの潜伏手法	第4章　Active Directoryの奪取とその検知手法 4.1　権限昇格と検知手法 4.2　AD管理者アカウントの奪取手法
午後	第2章　侵入とその検知手法（続き） 2.2　マルウェアの潜伏手法 第3章　情報奪取とその検知手法 3.1　情報奪取とその検知方法	第4章　Active Directoryの奪取とその検知手法（続き） 4.3　AD奪取と検知手法 第5章　侵入拡散とその検知手法 5.1　他PCへの侵入拡散と検知手法

関連コースのご案内：2018年度上期 新設コース

コースコード	USA60L
コース名	サイバーレンジによる実践的インシデント訓練
受講対象	一般的なシステム開発、運用を担当するSE
コース概要	システム運用の現場において、セキュリティインシデントが発生した場合、多様なOSやミドルウェア、プロダクト、ネットワーク機器やセキュリティ機器から発生する情報を収集し、セキュリティインシデントかどうかの判断が求められる。本教育は、セキュリティインシデント発生時における初動対応を実現するために、簡易的な調査や分析が行えることを確認する（実践的な内容のため講義は最小限です）。
期間	2日間
価格	250,000円

お問い合わせ先

お客様総合センター

0120-55-9019

受付時間 9:00～17:30（土・日・祝祭日を除く）

株式会社富士通ラーニングメディア　〒108-0075 東京都港区港南2-13-34 NSS-IIビル　http://www.knowledgewing.com/

Q1801008
有効期限2018年9月