SHEET

MANDIANT®
A FireEye® Company

教育サービス

企業環境の保護・防御を担当する セキュリティ担当者にトレーニングを実施

ハイライト

- 講師主導型のオンラインおよびeラーニング・コース
- 幅広い業界・政府機関におけるセキュリティの最前線で活躍し、高度なスキルを有する講師陣
- 講義と演習は、仮定のシナリオではなく、実際の攻撃事例がベース
- シミュレート済みの環境、攻撃者の最新のツール、戦術、手順（TTP）が盛り込まれた現実的なシナリオを使用
- コースは世界中どこでも受講可能。各地域に所在するコンサルタントがサポート
- 一貫した教育および演習手法

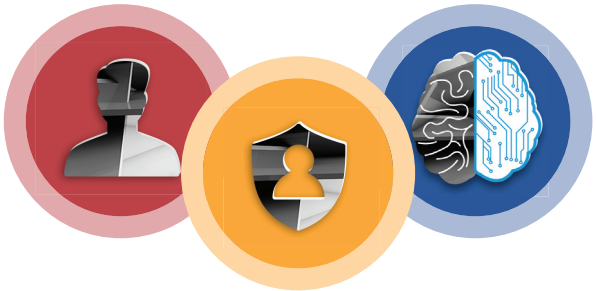
「以上の傾向を踏まえた結果、今後はセキュリティ対策を構成するすべての要素、つまり、人、プロセス、テクノロジーのすべてに、より一層着目すべきとの結論に達しました」

- Mandiant M-Trendsレポート

継続的な教育を通じて、進化する脅威に日々対処するために必要な最新のスキルと知識をセキュリティ・チームに提供します。

FireEyeの教育サービスは、セキュリティ・チームの運用面のスキルを強化するとともに、サイバー攻撃を予防、検知、対応する能力を向上させます。FireEyeのコンサルティング部門であるMandiantが有するFireEye製品の知識、高度なサイバー脅威インテリジェンス、インシデント対応の最前線で得られた専門知識など、FireEyeのあらゆる情報リソースに基づくさまざまなコースを用意しています。

この教育サービスでは、自然な流れで組織が運用体制を開発、改善する支援をします。特定のFireEye製品の基本テクノロジーに関するトレーニングから開始し、Mandiantのカリキュラムのサイバー・セキュリティに関する幅広いトレーニングへと移行します。さらに、実践的なライブファイヤー・エクササイズで、チームがシミュレーション環境でサイバー・イベントに対処します。



FireEye

FireEye製品およびテクノロジーについて学ぶ

FireEye製品トレーニング・コースでは、FireEyeテクノロジーを使用したFireEye製品の実装と管理、アラートへの対応と調査、最新のサイバー・セキュリティ脅威からの防御について学ぶ各種コースを用意しています。各コースは、実環境に被害が及ばないサンドボックス環境でのラボ演習と講義とを組み合わせています。演習では、現実のリスクがない環境で本物のマルウェアに対処します。講師は全員、現場経験の豊富なサイバー・セキュリティ専門家です。

製品の導入と管理に関する包括的なクラスのほか、分析担当者向けのコースでは、FireEye製品によるアラート分析やフォレンジック調査、ハンティングや調査についても扱います。また、システム・マネージャを対象としたトラブルシューティング・コースでは、FireEyeのアプライアンスを使用、管理する方法を学習します。

表1: FireEye製品およびテクノロジーについて学ぶコースの内容

講師主導型のトレーニング（ILT）	自分のペースで進めるオンライン・コース
コア・セキュリティ・プラットフォーム・コース • ネットワーク・セキュリティ（NXシリーズ）導入 • Eメール・セキュリティ（EXシリーズ）導入 • コンテンツ・セキュリティ（FXシリーズ）導入 • 集中管理（CMシリーズ）導入 • フォレンジック分析（AXシリーズ）導入 • アラート分析 • フォレンジックの基礎知識 • FireEyeのトラブルシューティング	コア・セキュリティ・プラットフォーム・コース • FireEyeプラットフォームの概要 • ネットワーク・セキュリティ（NXシリーズ）導入 • Eメール・セキュリティ（EXシリーズ）導入 • コンテンツ・セキュリティ（FXシリーズ）導入 • 集中管理（CMシリーズ）導入 • フォレンジック分析（AXシリーズ）導入 • Eメール脅威対策（ETP）クラウド
エンドポイント・セキュリティ・コース • エンドポイント・セキュリティ（HXシリーズ）導入 • エンドポイント・セキュリティ（HXシリーズ）による包括的な調査 • FireEye HXのトラブルシューティング	エンドポイント・セキュリティ・コース • エンドポイント・セキュリティ（HXシリーズ）導入
ネットワーク・フォレンジック・コース • ネットワーク・フォレンジック（PXシリーズ）の利用と管理 • ネットワーク・フォレンジック（PXシリーズ）の利用と調査解析（IAシリーズ）	ネットワーク・フォレンジック・コース • ネットワーク・フォレンジック（PXシリーズ）導入
FireEye Helixおよび脅威解析コース • 脅威解析プラットフォーム（TAP）導入 • FireEye Helix	マルウェア・フォレンジックおよび解析 • マルウェア・フォレンジック入門 • マルウェア・バイナリ解析入門
Mandiant Intelligent Response（MIR）コース • Enterprise Incident Response（エンタープライズ・インシデント対応）とMIR • 高度なMIR	

Mandiantによるサイバー・セキュリティ教育

サイバー・セキュリティ教育の各コースでは、Mandiantの幅広い現場経験に基づいたトレーニングを実施します。14年以上にわたり、サイバー・セキュリティとサイバー脅威インテリジェンスの最前線で世界中の複雑なセキュリティ侵害に対応してきたMandiantは、新旧の攻撃グループや、絶え間なく変化する攻撃者のツール、戦術、手順を深く理解しています。

この専門知識を活かし、実践的で現実的なセキュリティ・フレームワークに基づく教育コースを構築しています。受講生は、攻撃グループのTTP、攻撃に使用されるツールやマルウェア、攻撃を検知して対応するための実績ある方法論について、理解を深めることができます。

講師を務めるのは、攻撃への対応や新しいマルウェアのサンプル分析、企業ネットワークに対するレッド・チーム・サービスなどでインシデントに日々対応しているセキュリティ専門家です。講師主導型の講義とディスカッション、ラボ演習を組み合わせたコースで最適な学習体験が得られるうえ、サイバー脅威に関する最新情報も把握できます。

表2：サイバー・セキュリティ教育コースの内容

インシデント対応とフォレンジック	マルウェア解析	サイバー・セキュリティと脅威情報
• Enterprise Incident Response（エンタープライズ・インシデント対応） • Network Traffic Analysis（ネットワーク・トラフィック解析） • UNIX/Linux Investigations（UNIX/Linuxの調査） • Windows Investigations（Windowsの調査） • Router Backdoor Analysis（ルーター・バックドア解析） • PLCに関するデジタル・フォレンジックとインシデント対応	• マルウェア解析の必須要素 • Malware Analysis Crash Course（マルウェア解析短期集中コース） • Malware Analysis Master Course（マルウェア解析マスター・コース） • MacOS Malware Analysis for Reverse Engineers（リバース・エンジニア向けMacOSマルウェア解析） • Customized Malware Analysis（マルウェア解析カスタム・コース）	• Introduction to Cyber Crime for Executives（経営幹部向けサイバー犯罪入門） • Introduction to Attribution（攻撃者の特定入門） • Wireless Network Security（無線ネットワーク・セキュリティ） • Creative Red Teaming（独自のレッド・チーム） • Introduction to Linux for Security Professionals（セキュリティ技術者向けLinux入門）

ThreatSpace

ThreatSpaceは、セキュリティ・チームが現実の脅威に対処する技術的な能力、プロセス、手順を評価し、開発することを目的とするテクノロジーベースのサービスです。ご利用の際に実環境に被害が及ぶことはありません。ThreatSpaceによる診断では、ネットワーク・セグメント、ワークステーション、サーバー、アプリケーションなどの一般的なITインフラストラクチャをシミュレートした仮想環境で、シミュレート済みの攻撃シナリオをチームが調査します。

このプロセスの中で、Mandiantのインシデント対応の専門家が、チームの技術的な能力、プロセス、手順の評価を行います。また、フィードバックとコーチングをリアルタイムで提供し、サイバー攻撃に対するセキュリティ・チームの対応能力を強化します。

FireEyeの詳細については、**www.FireEye.jp**をご覧ください。

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03−4577−4401 |
Japan@fireeye.com

会社概要

FireEyeは、インテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデント対応といった、組織がサイバー攻撃対策をするうえでの課題となっていた複雑性や負担を解消します。FireEyeは「Forbes Global 2000」企業の45%以上を含む、世界67か国以上の6,600を超える組織で利用されています。

FireEye