データシート

MANDIANT
A FireEye® Company

セキュリティ組織構築支援サービス

攻撃耐性に優れた独自のセキュリティ・オペレーション・プログラムの策定

メリット

- **現在のセキュリティ体制を強化：**セキュリティ監視体制やインシデント対応能力のうち、高度な攻撃を防御するために改善が必要な領域を特定し、問題を解決します。
- **要改善項目について合意形成：**知識の共有と要改善点の優先度設定により、組織内部での共同作業とコミュニケーションを促進します。
- **セキュリティ・インシデントの影響を軽減：**検知および対応能力を強化し、サイバー・リスクを最小化します。
- **予算とリソースの優先度設定：**セキュリティ予算とリソースを適切に配分し、防御体制とインシデント対応体制全般を強化します。

Mandiantの特長

FireEye Mandiantは、2004年以来、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活動を続けてきました。Mandiantのインシデント対応担当者は、世界各地で発生した数々の複雑なセキュリティ侵害事件を現場で経験しています。このため、新旧の攻撃グループや、絶え間なく変化する攻撃者の戦術、手法、手順を深く理解しています。

概要

セキュリティ組織構築支援サービスでは、組織のリスクを最小限に抑え、セキュリティ侵害の影響を軽減する効果的なセキュリティ・オペレーション・プログラムの策定を支援します。お客様の戦略上の目標に直接適用可能なセキュリティ・モデルをベースに、Mandiantの豊富な現場経験に基づく現状の改善策を提案します。お客様との緊密な協力関係の下、お客様組織のセキュリティ・プログラムに必要な改善を加え、Adaptive Defense（適応型防御）の実現を支援します。

Mandiantのアプローチ

Mandiantの専門家は、高度な攻撃者の戦術、技術、手順を熟知しています。セキュリティ組織構築支援サービスでは、お客様と協力しながら、基盤となる機能とプロセスをお客様組織のプログラムに実装していきます。

サイバー攻撃を確実に検知して対応策を実施するために、インシデント対応プログラムには、適切な人材とテクノロジーを用いた効果的なプロセスおよび作業手順と、プログラムの実効性を継続的に評価する指標を組み込む必要があります。そこでMandiantでは、数々の深刻なセキュリティ・インシデントへの対応を重ねた経験に基づき、攻撃耐性の高いセキュリティ・プログラムに不可欠な6つの主要能力で構成されるフレームワークを策定しています。フレームワークを構成する6つの能力は次のとおりです。

- **ガバナンス：**組織編成は、組織全体のビジネス目標やミッションと整合しているか。
- **コミュニケーション：**組織内外での効果的な情報共有を促進するためのプロセスが確立されているか。
- **可視性：**システムおよびネットワークにおけるアクティビティを把握するためのテクノロジーとプロセスが導入されているか。
- **インテリジェンス：**脅威インテリジェンスを利用して現状を把握し、セキュリティ計画、脆弱性管理、インシデント対応体制を強化できるか。

FireEye

- **指標：**使用しているインシデント対応指標は、組織全体のビジネス目標と整合しているか、セキュリティ・チームの継続的な改善に役立っているか。
- **インシデント対応：**セキュリティ・イベントを確認、分類、調査し、被害を復旧するための確固たるテクノロジーとプロセスが導入されているか。

このサービスでは、お客様と協力しながらセキュリティ・プログラムを策定し、基盤となるプロセスとテクノロジーを実装していきます。また、お客様のスタッフが新しいテクノロジーやプロセスに慣れるまでの一定期間、セキュリティ・インシデントの監視をお手伝いすることも可能です。

表1：セキュリティ組織構築支援サービスのプロセス

段階	目的	作業
基盤構築	インシデント対応を効果的に実施し、リソースを有効活用するための基盤を構築する	• エスカレーション・マトリックスとインシデント対応ワークフローの概要設計 • 戦略計画とプログラム管理計画を策定 • パフォーマンス指標とレポーティング計画を策定
統合	新しいプロセス、作業手順、テクノロジーを現在の運用環境に組み込む	• トレーニングを策定、実施 • 運用のサービス・レベルを設定 • テクノロジーを導入、設定
運用	運用プロセス、解析プロセスを実行に移し、監視機能を提供する	• 初期監視機能を提供 • 運用プロセス、解析プロセスを継続的に改善 • お客様のセキュリティ・チームに運用を引き継ぎ、またはスタッフを派遣

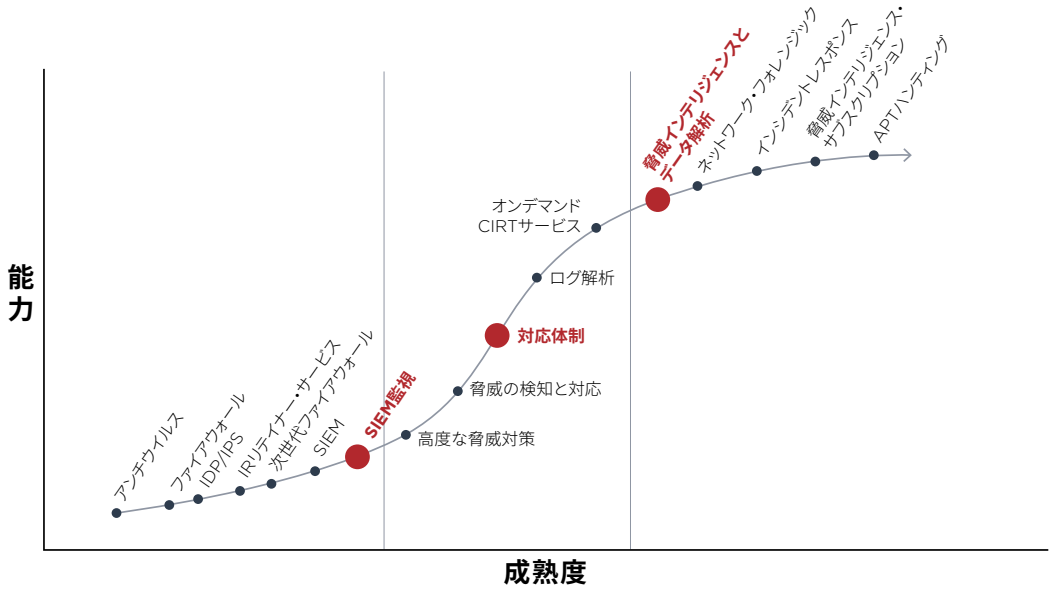

図1：サイバー・セキュリティ・プログラムの構築モデル

セキュリティ組織構築支援サービスでは、Mandiantの6つの主要能力モデルに基づき、「守り」のインシデント対応体制を、組織のミッションやビジネス目標に即した「攻め」の体制へと転換できるようお客様を支援します。

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 | www.fireeye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com

FireEyeについて

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・レスポンスといった、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