データシート

MANDIANT®
A FireEye® Company

Mandiantコンサルティング・サービス

重大なセキュリティ侵害に対応、資産の保護を支援

Mandiantコンサルティングの概要

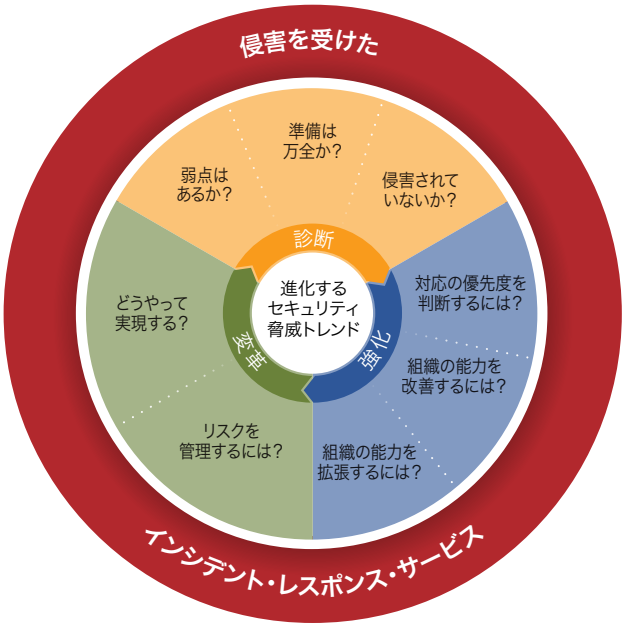
FireEyeのコンサルティング部門であるMandiantは、サイバー・セキュリティとサイバー脅威インテリジェンスの最前線で14年以上にわたり活動を続けてきました。FireEyeのインシデント対応担当者は、世界各地で発生した数々の複雑なセキュリティ侵害事件を現場で経験しています。このため、新旧の攻撃グループや、絶え間なく変化する攻撃者のツール、戦術、手順を深く理解しています。

FireEyeは、セキュリティ侵害からの復旧の支援、攻撃者が悪用を試みる脆弱性の特定、セキュリティ・ギャップを解消するためのガイダンスの提供を通じて、あらゆる規模の組織が将来のサイバー・インシデントのリスクを軽減できるようサポートします。

「Mandiantは、セキュリティ侵害対策のコンサルティングで最先端を行く企業です」

Michael Chertoff（マイケル・チャートフ）氏、
米国土安全保障省の元長官

セキュリティ・ニーズのフレームワーク



Mandiantの特長

Mandiantは、攻撃者の行動に関する深い知識に、絶え間なく変化する脅威トレンドを見通すインテリジェンスや包括的なテクノロジー・プラットフォームの組み合わせにより、広範囲にわたる迅速かつ効率的なサービス提供を実現しています。

専門知識：Mandiantは、現在まで14年以上にわたり、重大なセキュリティ侵害の最前線でインシデント対応を実施してきました。攻撃者が何をどのように行ったか、攻撃にどのようなツールや技術を使用したか、そして攻撃後はどうなったかという点に重点を置き、攻撃の全体像を描きながら、競合製品では実現できない形で、変化し続ける攻撃者の行動や動機について理解することを可能としています。

脅威インテリジェンス：Mandiantのサービスにはインテリジェンス主導型アプローチが採用されており、250名以上のFireEye iSightインテリジェンスのエキスパート、Mandiantによる数千件もの調査、FireEye製品、Managed Defenseサービスから得られる業界最高レベルのサイバー脅威インテリジェンスを活用して、日々変化し続ける世界中のセキュリティ脅威トレンドの把握に努めています。

テクノロジー：Mandiantは、FireEyeエンドポイント・テクノロジー、ネットワーク・センサー、解析プラットフォームを活用します。クライアントのニーズに応じてクラウドまたはオンプレミスで運用可能で、Windows、Linux、macOSのいずれのOSにも対応します。FireEyeのテクノロジーは、コストを最小限に抑えながら、より広範囲にわたって迅速なインシデント対応を実現します。

Mandiantサービスの概要（一部）

セキュリティ機能	セキュリティ・ニーズ	サービス	概要	メリット
インシデント対応	侵害を受けた。	インシデント・レスポンス・サービス	重大なセキュリティ・インシデントを迅速、全面的、効率的に調査して脅威を封じ込め、被害を復旧します。	重大なセキュリティ・インシデントを解決し、構造的な原因に対する長期的解決策を策定。
診断	侵害されていないか？	侵害調査サービス	お客様環境の過去または現在のセキュリティ侵害を特定し、現行のセキュリティ体制に基づいた将来の侵害リスクを評価してインシデント対応能力の向上を実現します。	現在セキュリティ侵害を受けているか、過去に受けていたかを確認。
	弱点はあるか？	レッドチーム・サービスとペネトレーション・テスト	日々のインシデント対応活動でMandiantが遭遇している高度な攻撃グループと同じTTP（ツール、戦術、手順）を駆使して、セキュリティ体制の実効性をテストします。	未知のセキュリティ上の弱点を特定して、攻撃者による悪用を未然に防止。
		産業制御システム・ヘルスチェック・サービス	産業施設の全体的なサイバー・セキュリティ体制について、環境への影響を最小限に抑えながら評価を実施し、ITおよびOT（運用技術）間のセキュリティ・ギャップを解消します。	悪用される可能性のあるICSの脆弱性について把握、システムのサイバー・セキュリティ・リスクを軽減するための計画を策定。
	準備は万全か？	インシデント・レスポンス体制診断サービス	インシデント対応の最前線における豊富な経験に基づき、組織のセキュリティ監視体制とインシデント対応体制の成熟度を客観的に診断します。	お客様組織のセキュリティ体制を改善し、サイバー攻撃を迅速に検知・防御する方法を把握。
		セキュリティ・プログラム診断サービス	組織のセキュリティ・プログラムを細部にわたって診断します。診断の対象は10に及ぶ主要領域にわたり、各領域はコンプライアンス、セキュリティ、業界フレームワークという3つのカテゴリーに分類されています。	セキュリティ・プログラムの実効性を診断し、セキュリティ体制の強化とビジネス・リスクの軽減を実現。
		インシデント・レスポンス・リテイナー・サービス	セキュリティ・インシデントの発生が疑われる場合に、インシデント・レスポンス・サービスを受けるための条件を事前に交渉・合意するためのサービスです。	インシデントへの対応に要する時間を大幅に短縮し、セキュリティ侵害の全体的な影響を軽減。
強化	組織の能力を改善するには？	製品、インテリジェンス、専門知識のトレーニング	セキュリティ・チームに脅威に関する最新の知識を提供し、絶え間なく進化を遂げるセキュリティ脅威に効果的に対処するために必要な運用スキルを向上させます。	理論的なシナリオではなく、現実に即した調査に基づいて教育やトレーニング演習をチームに提供。
	対応の優先度を判断するには？	サイバー脅威インテリジェンス・サービス	お客様が脅威インテリジェンスを取り込み、解析、適用してビジネスを保護できるように、サイバー脅威インテリジェンス（CTI）プロセスおよびソリューションをセキュリティ体制内で構築するサービスです。	インテリジェンス主導型のセキュリティ・プロセスを設計してセキュリティ・チームをサポートし、組織全体にわたる経営幹部の意思決定を支援。
変革	どうやって実現する？	セキュリティ組織構築支援サービス	コンプライアンスを主目的にしたお客様組織の「守り」のインシデント対応体制から、ビジネス要件に即したミッション主体の「攻め」のプログラムへの転換を支援します。	セキュリティ・チームやインシデント対応チームの能力を開発・強化。

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 | TEL: 03-4577-4401 | japan@fireeye.com | www.FireEye.co.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | www.FireEye.com