

# セキュリティ・プログラム診断サービス

情報セキュリティ・プログラムを診断し、  
セキュリティ体制の強化とリスクの軽減を実現



## メリット

- セキュリティ侵害と情報漏えいのリスク軽減
- セキュリティ・インシデントによる被害の軽減
- 要改善項目について合意形成
- 予算とリソースの優先度設定

Mandiantは、2004年の創業以来、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。セキュリティ・プログラム診断サービスは、Mandiantの豊富な専門知識を集め、セキュリティ体制の改善、リスクの緩和、インシデント発生時の被害とコストの軽減に役立つ、個別的で具体的な改善策を提案するサービスです。

## 概要

専門知識と脅威情報を業界標準規格と組み合わせ、10の重要セキュリティ領域でプログラムを評価します。診断の過程では、Mandiantコンサルタントによる文書のレビューや聞き取り調査を実施します。また、お客様の現状を理解し、共同作業を通じて今後の改善を促進するための対話形式のワークショップを開催します。具体的な改善策と実装ロードマップを提示し、お客様の短期的および長期的な目標の達成を支援します。

図1: 10の重要セキュリティ領域





#### サービスの内容と特長

- **エグゼクティブ・サマリー:** 診断結果と改善策の概要、および重要なベンチマークとなる知見です。
- **診断結果とのギャップ分析:** 業界フレームワークをベンチマークとするギャップ分析を実施し、強化や改善が必要な領域を特定します。その上で、セキュリティ体制を強化しリスクを軽減するための、成熟した体制の開発計画を示します。
- **セキュリティ・プログラムのロードマップと改善策:** 戦略的・戦術的な改善策を通じて、各領域の実効性を高めるための手順および優先度を提案します。
- **業界のベンチマークとなる知見:** 類似した規模の同業他社のセキュリティ体制とリスク特性に関する知見をお客様に提供します。

#### Mandiantのアプローチ

組織の情報セキュリティ・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のセキュリティ領域にわたり、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カテゴリにマップされています。最後に、短期、中期、長期の改善策に優先順位を付けた診断結果を提供します。診断時におけるリスク管理体制およびセキュリティ成熟度に基づいて、組織のセキュリティ体制を改善できるようデザインされています。

改善策には、既存のソリューションを最大限に有効活用する方法や、セキュリティ体制の強化とリスクの軽減に役立つ新しいツールおよびプロセスの提案が含まれています。

#### 診断プロセス

**ステップ1:** 文書の収集と解析

**ステップ2:** 対話形式のワークショップ、および経営幹部を対象にしたミーティング

**ステップ3:** 改善策とロードマップ

FireEyeの詳細については、[www.FireEye.jp](http://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

© 2018 FireEye, Inc. All rights reserved. FireEyeはFireEye, Inc.の登録商標です。本資料のその他のブランド名、製品またはサービス名はそれぞれその所有者の商標またはサービスマークとして登録されている場合があります。DS.SPA.JA-032018

#### 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の革新的なセキュリティ技術、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。

