

# インシデント・レスポンス・リテイナー・サービス

将来起こりうるセキュリティ・インシデントに備え、迅速かつ総合的なインシデント対応体制を確立、ビジネスへの影響を最小化

## Mandiantの特長

Mandiantは、インシデント対応専門のコンサルティング企業です。世界中の高度な攻撃グループへの対応を10年以上積み重ねた豊富な経験をベースに、世界各国の組織から厚い信頼を得ています。セキュリティ侵害発覚後の緊急事態における対応支援から、有事に備えた検知・対応・封じ込め体制の強化まで、インシデント対応に関する幅広いサポートを提供しています。

- **調査能力**: 10年以上に及ぶインシデント調査の経験で培われた高度な技術力と調査能力
- **脅威インテリジェンス**: ツール、戦術、手順 (TTP) など、多数の攻撃グループの特徴と、セキュリティ侵害の証拠や痕跡 (IOC: 侵害インジケータ) を把握
- **危機管理能力**: 管理職から経営幹部、取締役まで、組織の主要な利害関係者と協議しながらインシデントに対応した豊富な経験
- **テクノロジー**: 独自のツールにより、調査の各工程を自動化。ネットワーク・トラフィックやホストに残る攻撃の痕跡を解析し、現状をリアルタイムに可視化して迅速な診断を実施。数十万台規模のシステムが接続された大規模ネットワークにも対応
- **専任のマルウェア解析チーム**: 不正なソフトウェアのリバース・エンジニアリングや最新エクスプロイトの研究に特化したチームがお客様を支援

## 概要

インシデント・レスポンス・リテイナー (IRR) サービスは、インシデント・レスポンス・サービスの契約条件を、セキュリティ・インシデントの発生前に交渉・合意するためのサービスです。あらかじめ契約条件を決定しておく、いざというときに速やかにインシデント・レスポンス・サービスを受けられます。このアプローチにより、インシデント対応に要する時間を大幅に短縮し、セキュリティ侵害による影響を最小限に抑えられます。

Mandiantでは、お客様の多様なニーズや予算に合わせ、次の3種類のリテイナー・サービスを提供しています。

### ティア1: 初期費用が不要

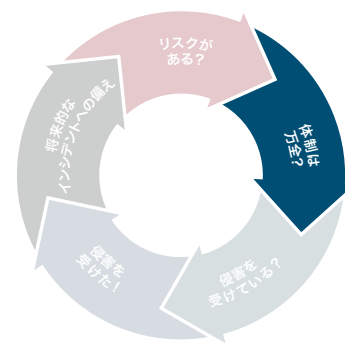
ティア1では、インシデント発生時のインシデント・レスポンス・サービスについて、お客様とMandiantの間で契約条件を交渉・合意します。利用する関連サービスとテクノロジーの時間あたりの料金を決定します。最低料金や年間料金は設定されておらず、インシデント・レスポンス・サービスの実施時のみ費用が発生します。

### ティア2: 一定時間分のサービス料金を事前支払い、サービス・レベルを保証

お客様とMandiantの間で契約条件を事前に交渉・合意するのはティア1と同様ですが、それに加えて事前支払い・割引料金による一定時間分のサービスが付属します。また、サービス・レベルが保証されるほか、インシデント対応能力の強化を目的とした、インシデント対応体制の事前評価サービスを受けられます。

事前支払い分が未消化となった場合は、契約期間中、Mandiantが提供する別のサービスにその分を割り当てるのが可能です。

**MANDIANT**  
A FireEye® Company



攻撃の有無ではなく、攻撃がいつなされるか、という問題です。セキュリティ侵害を想定した備えが必要です。

## メリット

- 契約条件を事前に交渉・合意して、インシデント対応に要する時間を短縮
- セキュリティ侵害が疑われるインシデントが発生した場合の対応時間を保証
- Mandiantのインシデント・レスポンス・サービスを割引料金で利用
- Mandiantの専門家チームが初動対応を担当
- 業界をリードするMandiantの各種テクノロジーにアクセス

### ティア3: サービス料金を事前支払い、サービス・レベルを保証

セキュリティ体制を強化する予防的なサービスが提供されます。インシデント・レスポンス・サービスの料金が最も割安なうえに、サービス・レベルが保証され、Mandiantの予防サービスを受けられます。サービス料金の事前支払いは必要ありません。セキュリティ体制の強化を目的としたMandiantのサービス・ラインナップから必要なサービスを選択し、契約期間中に利用できます。インシデント発生時には、サービス・レベルが保証されたサービスが最も割安な料金で提供されるため、余裕を持って対応することができます。

ティア3は、サイバー保険を契約中、または契約を検討中の組織に最適です。多くの保険が補償する範囲は、直接的なインシデント対応に要した費用に限定されます。

#### インシデント対応能力評価サービス

- 監視、ログ管理、検知のための導入済みテクノロジーを検証
- 現在のネットワークおよびホスト・アーキテクチャを確認
- インシデント対応の初動体制を診断
- 一般的なインシデント対応計画の作成を支援
- 改善策を提案

#### サービス・レベル:

- インシデント対応のリクエストを24時間受付(直通電話)
- リクエストから4時間以内に連絡(Eメールまたは電話)
- 初動対応の担当者を24時間以内に割り当て<sup>2</sup>

#### 初動対応:

- ライブ・レスポンス解析でシステム上の不正な活動を検知
- 最も古いセキュリティ侵害の証拠を確認
- 侵入に使用された攻撃経路を特定
- Mandiantのインテリジェンス調査チームが提供するコンテキスト情報を活用

	サービスの内容	SLA
ティア1	<b>説明</b> <ul style="list-style-type: none"><li>• インシデント・レスポンス・サービスの基本的な契約条件を交渉・合意</li><li>• サービス・リクエストの24時間受付(直通電話またはEメール)</li><li>• Mandiantのインシデント・レスポンス・サポートおよび各種テクノロジーにアクセス</li></ul>	無償 - ベスト・エフォート
ティア2	<b>説明</b> <ul style="list-style-type: none"><li>• インシデント・レスポンス・サービスの基本的な契約条件を交渉・合意</li><li>• サービス・リクエストの24時間受付(直通電話またはEメール)</li><li>• インシデント対応能力評価サービス</li><li>• Mandiantの各種テクノロジーにアクセス</li><li>• 事前支払いによる一定時間分のサポート</li><li>• 割引料金でのインシデント・レスポンス・サポート</li><li>• 割引料金での追加サポート</li></ul>	事前支払いによる一定時間分のサービス + SLAを保証
ティア3	<b>説明</b> <ul style="list-style-type: none"><li>• インシデント・レスポンス・サービスの基本的な契約条件を交渉・合意</li><li>• サービス・リクエストの24時間受付(直通電話またはEメール)</li><li>• インシデント対応能力評価サービス</li><li>• Mandiantの各種テクノロジーにアクセス</li><li>• 事前支払いのMandiantコンサルティング・サービス</li><li>• 割引料金でのインシデント・レスポンス・サポート</li></ul>	事前支払いによるサービス + SLAを保証

<sup>1</sup> 契約期間中の開始が必要

<sup>2</sup> サービス・リクエストの承認後

Mandiantの詳細については、次のWebページをご覧ください。

<https://www.fireeye.jp/services.html>

FireEye®はインテリジェンス主導型のSecurity-as-a-Serviceのリーダー企業です。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4割以上を含む、世界67か国以上の6,000を超える組織で利用されています。

#### 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](http://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](http://www.FireEye.com)