MANDIANT®
A FireEye® Company

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

事例：
MANDIANTによるIRの実績

世界各国の事業所に数万台のコンピュータを所有する国際的な専門サービス企業が、重要な顧客データへのセキュリティ侵害が発生した可能性があるとして、Mandiantにインシデント対応を依頼してきました。

1日目 - Mandiantは、依頼から4時間以内に、クラウドベースのエンドポイント・テクノロジーを1万8,000台のシステムに展開開始

- 同日中に調査を開始
- 調査開始から4時間でセキュリティ侵害の確たる証拠を発見

6日目 - 大半の調査活動が終了。1万8,000台以上のシステムを解析し、80台のシステムで詳細なライブ・レスポンス解析を実施

7日目 - 封じ込め作業を実施。業務への影響はゼロ。攻撃者の再侵入を防止するため、ネットワークの監視を継続

11日目 - お客様が通常業務を再開。すべてのインシデント対応作業はリモートから実施された

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。

数千件のインシデント対応経験に基づく調査および復旧に関する専門知識と、FireEyeが有する業界有数のインテリジェンス（脅威情報）、最先端のネットワークおよびエンドポイント・テクノロジーを組み合わせ、高度なインシデント・レスポンス・サービスを提供しています。

Mandiantは、大々的に報道された史上最大規模のセキュリティ・インシデントに対応してきた貴重な経験を有しています。このため、技術的な対応作業から危機管理に至る、インシデント対応のあらゆる側面でお客様を支援することが可能です。

迅速かつ効率的な調査および復旧により、お客様にとっての最優先事項、つまり通常業務の速やかな再開を支援します。

概要

Mandiantのインシデント・レスポンス・チームは、お客様データのプライバシーに配慮しながら、クラウド型とオンプレミス型の両ツールを駆使して、即座に調査を開始します。そして初動から数時間以内に、ネットワーク・トラフィックと大量のエンドポイントの情報を対象にした解析作業を開始。サイバー攻撃の調査現場とその他の情報ソースから得た豊富な脅威情報を武器に、攻撃者が用いる最新の戦術、技術、手順に対抗します

Mandiantのインシデント・レスポンス・サービスは、技術的な調査やセキュリティ脅威の封じ込め、被害の復旧にとどまらない包括的な内容となっています。経営幹部とのコミュニケーションや危機管理など、法律および規制への対応や広報対応を含む、より高次の問題にも対処します。社会的信用の失墜や法的責任の範囲を最小限にとどめるためには、適切な危機管理が必要不可欠です。

表1： Mandiantが主に対応しているインシデントの種類

知的財産の窃取	企業秘密など機密性の高い情報の窃取
金銭目的の犯罪	クレジット・カード情報の窃取、ACH/EFTを利用した違法送金、恐喝、ランサムウェア
個人を特定可能な情報（PII）	個人の特定に利用できる情報の漏えい
保護すべき医療情報（PHI）	保護すべき医療情報の漏えい
内部の脅威	社員や取引先などの関係者による不適切または違法な行為
破壊活動	情報やシステムを回復不能にするなど、標的組織の活動妨害を唯一の目的とする攻撃

FireEye®

MANDIANTの特長

- **豊富な調査実績：** Mandiantの調査担当者は、大規模で複雑なインシデントにおける調査および復旧作業で磨き上げられた高度なスキルを有しています。
- **脅威情報：** Mandiantでは、インシデント対応の最前線、FireEye Dynamic Threat Intelligence（DTI）、そしてiSIGHTの情報ソースから得られた業界有数の脅威情報をインシデント対応に活用しています。
- **テクノロジー：** Mandiantは、FireEyeが開発したクラウド型およびオンプレミス型の最新テクノロジーを駆使して、即座に調査を開始します。迅速かつ大規模なインシデント対応を実現するこれらのテクノロジーにより、ネットワーク・トラフィックと、各種OS（Microsoft Windows、Linux、Mac OS X）が動作するエンドポイントの可視化が実現します。また、FireEyeのMVXテクノロジーを利用したサンドボックスでのマルウェアの自動実行によって、シグネチャベースのテクノロジーでは対処できない未知のマルウェアの検知を可能にしています。
- **危機管理：** Mandiantのインシデント対応担当者は、経営幹部とのコミュニケーションや広報対応、情報開示など、インシデント発生時のコミュニケーションについて、お客様に助言してきた豊富な経験を有しています。
- **マルウェア解析：** 業界屈指の技術力を誇るリバース・エンジニアや研究者が、調査中に発見されたマルウェアを解析し、その機能を特定します。

Mandiantのアプローチ

Mandiantの調査では、ホストおよびネットワークベースの解析を実施して、環境全体を総合的に診断します。対応作業の内容は状況に応じて異なり、関連する規制や社会的信用への影響を考慮しながら、速やかにインシデントを解決して被害を復旧できる、最善の方法が選択されます。多くの場合、調査によって次の事項が明らかとなります。

- 影響を受けたアプリケーション、ネットワーク、システム、ユーザー・アカウント
- 使用された不正なソフトウェアや脆弱性
- アクセスまたは窃取された情報

インシデントの解析

1. **テクノロジーの導入と初期の手がかりの調査：** 迅速かつ包括的なインシデント対応に最も適したテクノロジーを導入します。同時に、お客様から提供していただいた初期の手がかりをもとに、IOC（侵害インジケーター）の作成に着手します。セキュリティ侵害の証拠や痕跡をまとめたIOCは、環境全体で不正な活動の痕跡を調査し、攻撃者の行動を特定するために使用されます。

2. **危機管理計画の策定：** お客様組織の経営幹部や法務担当者、ビジネス担当責任者、上級セキュリティ担当者と協力して、危機管理計画を策定します。

3. **インシデントの影響範囲の特定：** 現在の攻撃活動を監視するとともに、過去の活動の証拠を検索し、インシデントの影響範囲を特定します。

4. **詳細解析：** 攻撃者の行動を解析して、初期の攻撃経路、攻撃活動の流れ、侵害の範囲を特定します。ここでは、次の作業を実施します。
   - ライブ・レスポンス解析
   - フォレンジック分析
   - ネットワーク・トラフィック解析
   - ログ解析
   - マルウェア解析

5. **被害の把握：** 影響を受けたシステム、設備、アプリケーションとアクセスされた情報を特定します。

6. **復旧：** 攻撃者の行動とビジネス・ニーズに基づいて、脅威の封じ込めおよび被害の復旧のための独自の戦略を策定します。この戦略では、将来の攻撃による被害を防止または軽減するために、攻撃者を撃退してセキュリティ状況を改善することを目指します。

文書の提供

第三者による精査にも耐えうる内容の概要レポート、調査レポート、復旧レポートを提出します。

- **エグゼクティブ・サマリー：** タイミングと調査プロセス、主な調査結果、実施した脅威の封じ込め/駆除作業について解説した概要レポートです。
- **調査レポート：** 攻撃の流れと主な攻撃活動（攻撃者がネットワーク内でどのように活動を展開したか）を詳細に説明したレポートです。影響を受けたコンピュータ、場所、ユーザー・アカウントの一覧と、窃取された情報、危険にさらされた情報などが記載されています。
- **復旧レポート：** 実施した脅威の封じ込め/駆除作業を詳細に説明したレポートです。組織のセキュリティ体制を強化するための戦略的な推奨事項も記載されています。

インシデントの発生が疑われる場合は、**investigations@mandiant.com** までEメールでお問い合わせいただくか、次のサイトをご覧ください。**https://www.fireeye.jp/company/incident-response.html**

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