データシート

FireEye Threat Intelligence™

サイバー攻撃の脅威情報とコンテキスト情報を提供し、
検知および防御、インシデント対応を支援

ハイライト

- FireEyeが検知した脅威の技術的な情報とコンテキスト情報を継続的に提供。FireEyeの脅威対策プラットフォームの能力をさらに強化
- 数百万台のネットワーク/エンドポイント・センサー、数百件に及ぶインシデント対応経験、数十億件のセキュリティ・イベントから得られたFireEye独自の脅威情報を提供
- ゼロデイ攻撃をはじめとする、危険性の高い手法による攻撃の検知と防御を自動化
- セキュリティ解析担当者やインシデント対応担当者によるインシデントの調査と優先度の判定を支援し、作業を効率化
- 目的に応じた3レベルのサブスクリプション・サービスを提供

概要

多くのセキュリティ担当者は、組織にとってどのセキュリティ脅威が最もリスクが高いかを判別するのに日々苦労しています。メディアでは、毎日のように新たな脅威の出現が報じられており、セキュリティ担当者はその都度、対応の必要性や対策の選択を速やかに判断する必要に迫られているのです。

FireEye Threat Intelligenceでは、FireEyeが独自に収集したセキュリティ脅威情報と解析情報を提供します。セキュリティ担当者は、このサービスを利用することで、高度なサイバー攻撃を素早く検知、防御して、インシデント対応を実施するために必要となるコンテキスト情報を入手できます。

機能

FireEye Threat Intelligenceは、サブスクリプション型のサービスです。侵害の兆候を示す「侵害指標」に基づく保護とともに、各種ツールや、高度なサイバー攻撃者の攻撃手法、目的、行動パターンを解析したコンテキスト情報を提供します。次に示す3段階のサブスクリプション・レベルが用意されています。

Dynamic Threat Intelligence (DTI)

Web、電子メール、ファイルを悪用した脅威に関する情報を、FireEyeのグローバル規模のクラウド・ネットワーク全体で匿名情報として共有、配信し、サイバー攻撃を検知、防御します。この情報は1時間毎に更新され、世界中で導入されているFireEye環境で確認された最新の攻撃に関する情報が反映されます。

Advanced Threat Intelligence (ATI)

FireEyeの脅威対策プラットフォームが攻撃を検知した場合に警告を発するとともに、攻撃の実行者やマルウェアについて確認された情報を通知します。関与している攻撃者の素性や推測される目的、使用されているマルウェア、お客様環境が攻撃の標的になっているかどうかの調査に役立つその他の情報を提供します。

Advanced Threat Intelligence Plus (ATI+)

高度なサイバー攻撃の実行者に関する一連の調査情報、傾向、ニュース、解析情報に加え、標的とされている業種のプロファイル情報（狙われやすいデータの種類など）を提供します。また、高度なコミュニティ機能が用意されており、信頼できるパートナーと連携しながら情報を共有し、独自の防御コミュニティを構築することもできます。

FireEye Threat Intelligenceのメリット

FireEye Threat Intelligenceで提供される脅威情報や解析ツールを利用すると、優先的に対処すべき脅威を把握して、重大なサイバー攻撃を確実に検知、防御できます。また、高度な脅威から組織を保護し、セキュリティ侵害の影響を最小限に抑えるために必要なコンテキスト情報も入手できます。主なメリットは次の通りです。

- **未知の攻撃を検知** - グローバル規模の情報エコシステムを基盤とするFireEyeのソリューションにより、ゼロデイ攻撃などの高度なサイバー攻撃の検知と防御を自動化できます。
- **セキュリティ解析作業を効率化** - セキュリティ解析担当者は、情報の確認、調査、解析を単一のインタフェース上で行えるため、多種多様な情報の評価が短時間で済みます。
- **迅速なインシデント対応を実現** - セキュリティ脅威の対応優先度を判別して、重要なセキュリティ・インシデントの調査、解決に要する時間を短縮できます。また、攻撃者の素性やその目的を把握することも可能です。
- **リスクを低減** - 最もリスクの高い脅威に優先的に対応できます。また、特定の業種を標的とする攻撃者の傾向や攻撃手法を詳しく把握して、攻撃の事前予測が可能になります。
- **セキュリティ投資のROIを向上** - セキュリティ対策の現状を評価し、その結果に基づいてリソースの配分を変更することで、新たな脅威に対する防御が強化され、セキュリティ・インシデントの迅速な解決が実現します。
- **状況を正確に把握** - 自社を狙う可能性が高い攻撃グループやその目的、対処方法を把握し、対策に役立てることができます。

FireEye Threat Intelligenceの優位性

FireEyeでは、高度なサイバー攻撃の実行手法や攻撃者の行動パターン、マルウェアに関する情報を10年以上にわたり収集、解析し続けています。業界最高水準の緻密さを誇るFireEyeの脅威情報は、次の情報元から収集されています。

- **ネットワーク/エンドポイント・センサー** - 数百万台に及ぶFireEyeのセンサーが、1日あたり40万種類以上のマルウェアに対し、500億回以上の解析を実施しています。
- **Mandiantのインシデント対応サービス** - Mandiantのコンサルタントは、年間10万時間以上を大規模な侵入インシデントへの対応に費やしており、フォレンジック調査の過程でさまざまな侵入の痕跡や攻撃手法を確認しています。
- **脅威の研究者と情報の解析担当者** - FireEyeの情報解析チームは昨年、非常に多くのゼロデイ脆弱性を発見しました。その数は、FireEye以外のセキュリティ・ベンダーが発見したゼロデイ脆弱性の合計を上回ります。また数十人に及ぶ解析担当者が、200以上の既知の攻撃グループを追跡しています。これらの活動から得られた戦略的な知見や解析情報は、検知時点の情報を補完する役割を果たします。

世界中に配置されたFireEyeの脅威対策プラットフォームは、グローバル規模の情報収集ネットワークから集められた最新の情報で随時更新されます。60分毎に行われるその頻度は、他社平均の1日1回を大幅に上回ります。

FireEye Threat Intelligenceの各サブスクリプション・レベルで提供されるサービス

	Dynamic Threat Intelligence (DTI)	Advanced Threat Intelligence (ATI)	Advanced Threat Intelligence Plus (ATI+)
FireEyeプラットフォームの脅威情報の更新	×	×	×
一方向または双方向での脅威情報の共有	×	×	×
コミュニティによる脅威情報の共有	×	×	×
アラートと既知の攻撃者の関連付け		×	×
マルウェア・ファミリーについての解説		×	×
脆弱性とキル・チェーンの解析		×	×
FireEyeの解析担当者による継続的な監視			×
マルウェア・ファミリーについての詳細情報			×
攻撃者のプロファイル情報			×
攻撃者の傾向についての詳細な解析とレポート			×

ファイア・アイ株式会社 | 〒101-0054 東京都千代田区神田錦町1-1 神田橋安田ビル6階 | TEL: 03-4577-4401 | jp-info@FireEye.com | www.FireEye.co.jp

FireEye