FIREEYE™

検知できない攻撃をどう検知するか

巧妙化するネットワーク脅威への挑戦

今日のセキュリティ上の課題

高度な標的型攻撃などの検知を回避する攻撃により、セキュリティ侵害を効果的に防ぐことは極めて困難になっています。

- サイバー犯罪者は、高度な攻撃を用いて次世代ファイアウォールやIPS、アンチウイルス・ソリューションをすり抜け、数か月にわたって組織内に潜伏する（外部から指摘の場合、2015年では平均320日）[1]
- マルウェアの68%以上が特定の標的を攻撃するために作成されており、そのうちの80%は一度しか使用されない[2]。したがって、シグネチャベースのセキュリティでは標的型攻撃に対応できない
- シグネチャベースとポリシーベースのセキュリティによって生成されるアラートの80%以上は信頼性が低く[3]、リソースを重要なアラートに集中させることができない

今日のビジネス主導のIT変革によって、組織に対する攻撃経路が広がり、課題が増しています。

- パブリック・クラウド・アプリケーションに対する支出は、2020年までに企業支出の2/3以上を占めると予測される[4]。クラウドの運用は、企業のインバウンド / アウトバウンドのインターネット・トラフィックと、それに付随する潜在的な脅威を40%増加させる[5]。このトラフィックをすべて検査する必要がある
- 現在の組織の96%が、Windows以外のデバイスも使用している[6]。これらのデバイスは、以前からセキュリティ対策が不十分である
- 支社や支店の環境の40%は、インターネットに直接接続されている[5]。強固に保護された本社以外で、攻撃による被害が増えている

セキュリティ侵害対策に求められる4つの条件

大きな損害をもたらすセキュリティ侵害のリスクを最小限に抑えるには、あらゆる規模の組織で攻撃を効果的に防御するソリューションが欠かせません。それには次の条件を満たす必要があります。

1. 従来型のセキュリティ製品では対応できない脅威を検知、防御
2. 発生したインシデントに素早く対応し、被害の拡大を阻止
3. 変化を続ける脅威トレンドに継続的に適応
4. 組織の成長やITサービスの提供方法の変化に柔軟に対応

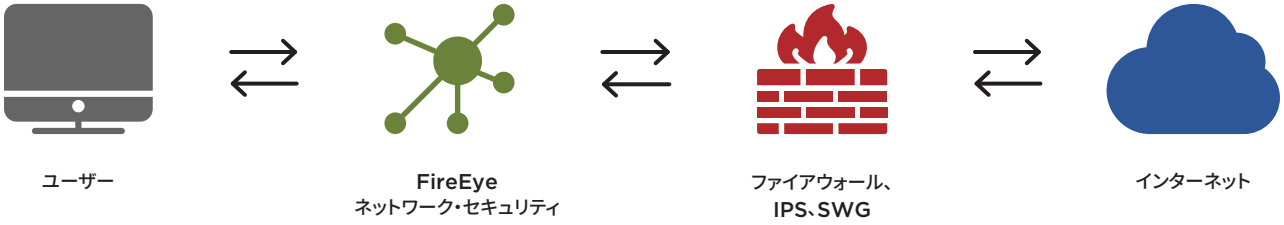
FireEye ネットワーク・セキュリティ

FireEyeネットワーク・セキュリティは、どのような規模の組織でも、高度な標的型攻撃やインターネット・トラフィックに潜むサイバー攻撃を正確かつ速やかに検知、防御し、セキュリティ侵害リスクを最小限に抑えます。FireEyeネットワーク・セキュリティは、Multi-Vector Virtual Execution™（MVX）およびIntelligence-Driven Analysis（IDA）と呼ばれる2つのテクノロジーから構成されます。シグネチャレスのダイナミックな解析エンジンであるMVXは、疑わしいオブジェクトを検査して、標的型攻撃や検知を回避する攻撃、未知の脅威を特定します。IDAエンジンは、マシン、攻撃者、被害者に関するインテリジェンスに基づき、不正なオブジェクトを検知、ブロックします。

FireEyeネットワーク・セキュリティには、幅広い製品のラインアップや導入モデルが用意されています。通常は、次世代ファイアウォールや侵入防御システム（IPS）、セキュアWebゲートウェイ（SWG）などの従来型ネットワーク・セキュリティ機器の背後、インターネット・トラフィックの経路に配置します。

1 FireEye (February 2016). M-Trends 2016.
2 Joshua Goldfarb (September 19, 2016). “Detection Innovations.”
3 Ponemon Institute LLC (January 2015). “The Cost of Malware Containment.”
4 Forrester (September 2016). “The Public Cloud Services Market Will Grow Rapidly to $236 Billion in 2020.”
5 IDC (February 2016). “Communication Service Provider Adoption of SD-WAN Technology and Its Impact to MPLS VPN Services.”
6 JAMF Software (2015). 2015 Survey: Managing Apple Devices in the Enterprise

図1：ネットワーク・セキュリティ・ソリューションの一般的な構成



FireEyeネットワーク・セキュリティは、あらゆる規模の組織をセキュリティ侵害から効果的に保護する次の機能を備えています。

- **正確な検知：**MVXとIDAの両テクノロジーは、少ない誤検知で、サイバー攻撃を正確に検知します。また、複数のフローや攻撃経路で発生したイベントを相関分析して、他のソリューションでは検知や阻止ができない段階的な攻撃に対処します。
- **攻撃を即座にブロック、耐障害性を高める高可用性構成にも対応：**インバウンドのエクスプロイトやマルウェア、複数のプロトコルで行われるアウトバウンドのコールバック通信をインラインでブロックし、攻撃を即座に阻止します。高可用性構成に対応しており、ネットワーク・リンクやデバイスに障害が発生した場合でも、迅速に機能を復旧して保護できます。
- **具体的な情報：**アラートには、サイバー・セキュリティの最前線で得られた具体的な証拠とコンテキスト情報が含まれています。このため、優先度の高い脅威に素早く対応し、被害の拡大を阻止できます。
- **インジケーターの取り込み：**Structured Threat Intelligence eXpression（STIX）フォーマットを利用して、独自のインテリジェンスをIDAエンジンに取り込めます。
- NEW **拡張性に優れたアーキテクチャ：**ソフトウェアとシステム設計により、複数の脅威対策テクノロジーをソフトウェア・モジュールとして運用できます。

- **多様な環境の保護に対応：**最も広く使用されているオペレーティング・システムのMicrosoft WindowsやApple Mac OS X、140種類以上のファイル・タイプに加え、各種オペレーティング・システム、サービス・パック、アプリケーションの組み合わせを数千種類にわたってサポートしているため、さまざまな攻撃に対応できます。
- **対応ワークフローの統合：**アラート検証、リスクウェアの個別検知、詳細な調査を可能にするパケット・キャプチャの各機能により、アラート対応ワークフローを自動化、高速化できます。

あらゆる組織のニーズに対応

FireEyeネットワーク・セキュリティには、最大8 Gbpsのパフォーマンスを提供する、柔軟性と拡張性に優れた幅広い導入モデルが用意されており、中規模から大規模の企業のニーズや予算に対応します。

- **統合型ネットワーク・セキュリティ：**MVXサービスを使用するスタンドアロン型のオールインワン・ハードウェア・アプライアンスで、単一のインターネット・アクセス・ポイントを保護します。
- NEW **分散型ネットワーク・セキュリティ：**Network Smart Nodeおよび共有MVXサービスで、組織全体にセキュリティを適用します。
  - **Network Smart Node：**各インターネット・アクセス・ポイントに設置する物理または仮想のアプライアンスです。疑わしい活動を検知し、対処します。
  - **MVX Smart Grid または FireEye Cloud MVX：**オンプレミス型またはクラウド型のMVXサービスで詳細な解析を実施します。高度なサイバー攻撃を検知し、セキュリティ・チームの作業を効率化します。

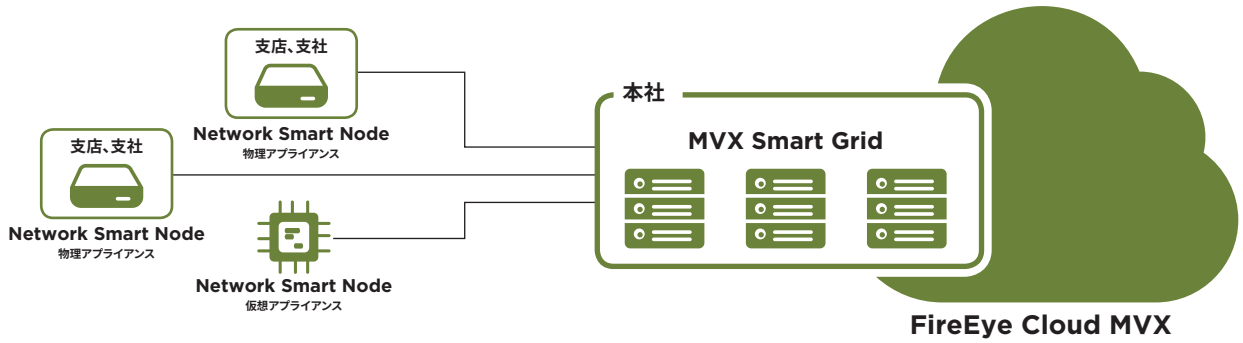


図2：分散型ネットワーク・セキュリティ

FireEyeネットワーク・セキュリティ Essentialsは、コスト・パフォーマンスに優れた中小規模企業向けのモデルです。統合型と分散型での導入が可能で、10 Mbpsから2 Gbpsまで対応します。

表1: FireEyeネットワーク・セキュリティ導入オプション

	統合アプライアンス	Network Smart Node	MVX Smart Grid Network Smart Nodeが必要	FireEye Cloud MVX Network Smart Nodeが必要
FireEyeネットワーク・セキュリティ（中規模～大規模企業向け）	オンプレミス	物理または仮想	オンプレミス型＋分散型	クラウド型＋分散型
FireEyeネットワーク・セキュリティ Essentials（中小規模企業向け）	オンプレミス	物理または仮想	利用不可	クラウド型＋分散型

短期間で投資を回収

FireEyeネットワーク・セキュリティは単一サイトの保護と複数サイトの保護のどちらのニーズにも対応し、セキュリティ侵害のリスクを最小限に抑えながら、短期間で投資を回収できます。

Forrester Consultingの最近の調査によると[7]、FireEyeネットワーク・セキュリティのROIは、コスト削減効果により3年超で152%と見込まれ、初期投資の回収期間はわずか9.7か月とされています。以下の取り組みを実現することで、短期的および長期的なコスト削減につながります。

- セキュリティ担当者が本物のサイバー攻撃への対応に専念できるため、運用コストが削減される
- MVXのキャパシティを共有するオプションや、環境の規模に最適なパフォーマンスを選択できる多様なモデルが用意されているため、設備投資が最適化される
- 拠点数やインターネット・トラフィック量の増加に合わせて性能を段階的に拡張できるため、初期投資が無駄にならない
- 統合型から分散型へとコストなしで移行できるため、既存の投資が無駄にならない
- 拡張性に優れたモジュール型のアーキテクチャを採用しているため、将来の設備投資が少なくて済む

FireEye ネットワーク・セキュリティを選ぶ理由

FireEye MVXエンジンは、高度な脅威対策ソリューションの中で最も優れた実績を上げている、FireEye独自のテクノロジーです[8]。

- 2013年以降、FireEyeは現実に発生したゼロデイ攻撃を多数発見しています。その数は、FireEye以外のソリューションが発見したゼロデイ攻撃の合計を上回ります。
- 2016年、Frost & Sullivanは、市場シェア56%のFireEyeをマーケット・リーダーと認定しました。FireEyeのシェアは、後続10社の合計を上回ります[9]。
- FireEyeネットワーク・セキュリティは、SANS Institute、SC Magazine、CRNなどの組織やメディアから多数のアワードを受賞しています。
- FireEyeネットワーク・セキュリティは、市販のセキュリティ・ソリューションとして初めて、米国土安全保障省の「SAFETY Act」認定を受けています。

7 Forrester (May 2016). “The Total Economic Impact Of FireEye.”
8 IDC (2015). Worldwide Specialized Threat Analysis and Protection Market Shares.
9 Frost & Sullivan (September 2016). “Network Security Sandbox Market Analysis.”

表2: FireEyeネットワーク・セキュリティのメリット

能力	メリット
従来型のセキュリティ製品では対応できない脅威を検知、防御	
シグネチャレスの脅威検知エンジン（MVX）	複数のフローや複数の段階を経る攻撃、ゼロデイ攻撃、ポリモーフィック型の攻撃、ランサムウェアなど、検知困難な攻撃に対応
リアルタイムでの検知と遡及的な検知	既知および未知のセキュリティ脅威をリアルタイムで検知すると同時に、新たな情報に基づいて以前に見逃した脅威を検知
複数の攻撃経路にわたる相関分析	Eメール、エンドポイント、ファイルにまたがる攻撃を自動的に検証、ブロック
多様なOS、ファイル・タイプ、アプリケーションをサポート	用途が異なる各種エンドポイントの混在環境をサポート
セキュリティ強化ハイパーバイザー	検知回避手法に対応
発生したインシデントに素早く対応し、被害の拡大を阻止	
リアルタイムのインライン・ブロック	攻撃を即座に防御
統合されたセキュリティ・ワークフロー	検知から調査、対応へとスムーズに移行
高可用性（HA）	レジリエントな防御
ノイズの低減機能を備えたシグネチャベースのIPS	膨大なアラートのトリアージを自動化、高速化して、手作業の負担を軽減
リスクウェアの検知と分類	深刻度に応じてマルウェアを個別に検知し、対応の優先度を判断
具体的なコンテキスト情報	攻撃と攻撃者に関する詳細情報で、高度な脅威を迅速に封じ込め
変化を続ける脅威トレンドに継続的に適応	
リアルタイムでの脅威インテリジェンスの共有	グローバルに共有されるセキュリティ侵害情報で未知のサイバー攻撃を即座にブロック、迅速な対応を支援
NEW 独自作成およびサードパーティー提供の脅威インテリジェンス（STIX）	FireEyeおよびサードパーティーが提供するインジケーターをSTIX対応のIDAエンジンに取り込み
戦略的な脅威インテリジェンス	セキュリティ脅威トレンドの変化をいち早く把握し、一歩先を行くセキュリティ体制を実現
組織の成長やITサービスの提供方法の変化に柔軟に対応	
帯域幅	10 Mbps～8 Gbps
拡張性	単一サイトから数千のサイト（分散型の場合）
サポートされる製品	物理、仮想、クラウド
導入モデル	Network Smart NodeおよびMVXサービス・アーキテクチャを使用した、統合型ネットワーク・セキュリティと分散型ネットワーク・セキュリティ

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 | 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上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™