ネットワーク・セキュリティ

セキュリティ侵害から効果的に防御、
規模を問わずあらゆる組織のニーズに対応

今日の組織が直面するセキュリティ上の課題

高度な標的型攻撃など、検知困難なサイバー攻撃が増加している今日、セキュリティ侵害を防ぐことは、かつてないほどの難題となっています。これには、次のような理由があります。

- 高度な手口を用いるサイバー攻撃者は、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、長期にわたってネットワークに潜伏する（2015年の調査によると、外部からセキュリティ侵害の指摘を受けたケースでは1、平均320日）[1]
- マルウェアの68%以上は、特定の組織に対する攻撃への使用に限定され、そのうち80%は一度しか使われない[2]。このため、シグネチャベースのセキュリティ対策では、標的型攻撃に太刀打ちできない
- シグネチャ/ポリシーベースのセキュリティ・ソリューションが発するアラートの80%以上は信頼できない[3]。組織では、このようなアラートの処理にリソースを取られ、重要なアラートへの対応がおろそかになる

今日広がるビジネス主導のIT変革も、結果として、組織に対する攻撃経路を増やす役割を果たしています。

- パブリック・クラウド上のアプリケーションに対する投資は、2020年までに、企業におけるIT投資の2/3を占めるようになると予測される[4]。クラウドの業務利用は、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]。このすべてのトラフィックを検査する必要がある
- 96%の組織では、Windows以外のデバイスも使用されている[6]。これらのデバイスに対するセキュリティ対策は、以前から不十分
- 支社・支店環境の40%は、直接インターネットに接続されている[5]。支社・支店環境の多くは、本社環境のように強固なセキュリティで保護されていないため、攻撃による被害を受けやすい

セキュリティ侵害対策の4条件

甚大な被害をもたらすセキュリティ侵害は、規模を問わずあらゆる組織で発生する可能性があります。このリスクを最小限に抑えるには、次の条件を満たす効果的なセキュリティ・ソリューションを導入する必要があります。

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. 変化し続ける脅威トレンドに継続的に適応可能
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 Network Security

FireEye Network Securityは、規模の大小を問わず、あらゆる組織を保護するサイバー・セキュリティ・ソリューションです。高度な標的型攻撃など、インターネット・トラフィックに潜む発見困難なサイバー攻撃を正確かつ速やかに検知・防御して、甚大な被害をもたらすセキュリティ侵害の発生リスクを最小限に抑えます。FireEye Network Securityの核となるのは、Multi-Vector Virtual Execution™（MVX）およびIntelligence-Driven Analysis（IDA）と呼ばれる2つのテクノロジーです。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、標的型の脅威や検知困難な脅威、未知の脅威を発見します。一方のIDAエンジンは、マシン、攻撃者、被害者に関する情報に基づいて、不正なオブジェクトを検知・ブロックします。

FireEye Network Security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、FireEye Network Security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、インターネット・トラフィックのパス上に置かれた従来型セキュリティ・アプライアンスの背後に配置します。

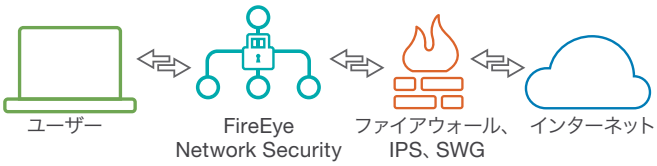

図1： Network Securityソリューションの一般的な構成

FireEye Network Securityは、あらゆる規模の組織をセキュリティ侵害から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、誤検知を最小限に抑えながら、サイバー攻撃を正確に検知します。また、異なるフローや攻撃経路で発生した複数のイベントを相関分析して、多くのソリューションでは検知・防御できない段階的な攻撃に対処します。

FireEye

- **攻撃を即座にブロック。可用性の高い冗長構成にも対応:** インバウンドのエクスプロイトやマルウェア、また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、攻撃を即座に防御します。可用性の高い冗長構成にも対応しているため、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、通信やセキュリティ機能を維持できます。
- **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に基づくインテリジェンス（脅威情報）が含まれています。このため、優先度の高いセキュリティ脅威に素早く対応し、被害の拡大を阻止できます。
- **セキュリティ侵害の証拠や痕跡に関する情報（侵害インジケーター）の取り込み:** Structured Threat Intelligence eXpression（STIX）フォーマットを利用して、独自の脅威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:** 独自のソフトウェアおよびシステム設計を採用しており、複数の脅威対策テクノロジーをソフトウェア・モジュールとして実行できます。

- **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 Network Security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～大規模企業のニーズや予算に対応します。

- **統合型Network Security:** 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Network Security:** Network Smart Nodesと共有MVXサービスの組み合わせにより、組織の複数の拠点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、セキュリティ担当者の作業を効率化します。

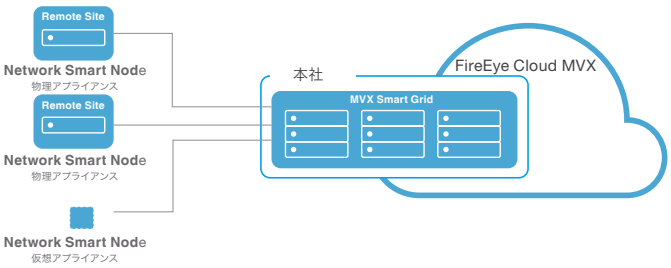

図2: 分散導入モデル

FireEye Network Security Essentialsは、コスト・パフォーマンスに優れた中堅・中小企業向けのモデルです。統合型と分散型のどちらの形態でも導入可能で、パフォーマンスは10 Mbpsから2 Gbpsまで対応します。

	導入モデル			
	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 Network Security（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 Network Security（中堅・中小企業向け）	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

表1: FireEye Network Securityの導入モデル

短期間で投資を回収

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するFireEye Network Securityでは、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 Network Securityの3年間のROIは、コスト削減効果による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。短期および長期のコスト削減の具体例は次のとおりです。

- セキュリティ担当者がリスクの高いサイバー脅威への対応に専念できるため、運用コストが削減される
- MVX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 Network Securityを選ぶ理由

MVXエンジンは、高度な脅威対策技術の中で最も優れた実績を残している、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、FireEyeを市場シェア56%の確固たるマーケット・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 Network Security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 Network Security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。

FireEye Network Securityのメリット

機能	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）	複数のフローや段階にわたる攻撃、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）	障害からの迅速な復旧を可能にするレジリエントな防御
アラート・ノイズの自動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
リスクウェアの個別検知	マルウェアを深刻度に応じて個別に検知し、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、高度なセキュリティ脅威を迅速に封じ込め

機能	メリット
変化し続ける脅威トレンドに継続的に適応	
リアルタイムの脅威情報の共有	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
独自作成およびサードパーティ提供の脅威インテリジェンス（STIX） NEW	FireEyeおよびサードパーティ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サイト（分散型の場合）
フォーム・ファクタ NEW	物理、仮想、クラウド
導入モデル NEW	統合型Network Security、分散型Network SecurityとNetwork Smart Node、MVXサービス・アーキテクチャ

セキュリティ侵害から組織を保護する、正確性、適応性、拡張性に優れたFireEyeのソリューションの詳細については、こちらをご覧ください。

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.
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.”

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
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com