エンドポイント・セキュリティ

オンサイト/リモートのエンドポイントを既知・未知の
セキュリティ脅威およびエクスプロイトから保護

高度化した今日のサイバー攻撃は、従来型のEPP（Endpoint Protection Platforms）を容易にすり抜けます。それぞれが単一の脅威に焦点を当てた対策で、全体で連携して機能していないためです。一方、FireEyeエンドポイント・セキュリティでは、はるかに堅牢なEPPを実現しています。アンチウイルス/アンチマルウェア、脅威インテリジェンス、振る舞い解析、EDR（エンドポイントの検知と対応： Endpoint Detection and Response）の各種機能が統合されており、さまざまな脅威の特性に基づいて検知、防御します。より高度なセキュリティ・プロセスの自動化を実現しながら、アクティブな検査および解析を実施し、疑わしい活動を特定して排除することが可能です。主な機能は次のとおりです。

- Triage ViewerおよびAudit Viewer：セキュリティ脅威の存在を示す証拠や痕跡（インジケーター）を検査、解析
- エンタープライズ・セキュリティ・サーチ：疑わしい活動やセキュリティ脅威を迅速に検索、特定、判別
- Data Acquisition：エンドポイントを詳細に検査、解析
- Exploit Guard：エンドポイントやアプリケーションに対するエクスプロイト攻撃を検知、報告、防御

FireEyeエンドポイント・セキュリティは、エンドポイントを攻撃する既知および未知のセキュリティ脅威を予防的に検知、防御、検査、解析して封じ込め、被害を最小限に抑えます。

水面下で展開されるエクスプロイト攻撃を検知、防御

単純なシグネチャやパターンに基づく従来型の技術であるEPPでは、エクスプロイトの検知は困難です。一方、FireEyeエンドポイント・セキュリティは、Exploit Guardの行動分析機能により、エクスプロイトの活動に関する柔軟性に優れたデータ主導のインテリジェンスを提供します。EDR機能も提供するExploit Guardは、従来型のエンドポイント・ソリューションでは発見できない領域の詳細情報を収集。FireEye独自の詳細なインテリジェンスに基づいて、一見無関係な複数の活動を相関分析してエクスプロイトを検知します。

エンドポイントの保護に脅威インテリジェンスを活用

脅威インテリジェンスは、攻撃発生の時点で利用できなければ、あまり意味がありません。FireEyeエンドポイント・セキュリティで提供されるEDR機能は、他のFireEye製品が備える脅威インテリジェンス機能をエンドポイントまでシームレスに拡張する技術です。あるFireEye製品がネットワーク上で攻撃を検知した場合、その情報はエンドポイントに自動配信されます。アナリストは、Triage ViewerとAudit Viewerを使用して、セキュリティ侵害の証拠や痕跡である侵害インジケーター（IOC）の有無をすべてのエンドポイントで素早く詳細に検査し、発見されたIOCについての情報を収集できます。

エンドポイントを詳細に可視化

アラート発生の根本原因を特定し、セキュリティ脅威の詳細解析を実施して侵害状況についての判断を下すためには、エンドポイントの包括的な可視化が欠かせません。FireEyeエンドポイント・セキュリティの履歴キャッシュ機能を使用すると、エンドポイントで発生した過去および現在のアラートを検査、解析して綿密なフォレンジック調査と最適な対応を実施できます。

ハイライト

- オンプレミス型のアプライアンスとエンドポイント・エージェント・ソフトウェアのどちらの形態でも導入可能で、リモート/オンサイトのエンドポイント上での活動を監視してエクスプロイトを検知、防御し、既知および未知の脅威への迅速な対応を実現
- 単一のエンドポイント・エージェントに新しいアンチウイルス（Q3までは検知のみ）と、Advanced Threat Intelligenceおよび振る舞い解析機能を統合
- 各ワークフロー内の活動の包括的なタイムラインを使用してエンドポイントを詳細に調査、IOCを特定してセキュリティ脅威を封じ込められるように支援
- 数万台規模のエンドポイントがオンサイトやリモートに存在する場合でも、わずか数分でセキュリティ脅威を検索、検知、特定、封じ込め
- Triage ViewerとAudit Viewerを使用してあらゆるエンドポイント活動を単一のインタフェースで効率よく検証。検知、阻止したインシデントはワンクリックで解析、封じ込めが実施できるため、従来を上回る迅速な対応が可能

FireEye

自社ネットワーク内外のエンドポイントを包括的に保護

オンサイトまたはリモートのいずれのエンドポイントでも、サイバー攻撃を受ける可能性が高まっています。FireEyeエンドポイント・セキュリティは、これらすべてのエンドポイントの保護に対応しており、インターネット接続の種類を問わずインテリジェンスをプッシュ配信できます。このため、セキュリティ脅威を検知、防御できるほか、VPN接続を別途利用することなく、世界中に分散するエンドポイントを調査し、侵害を受けたエンドポイントを隔離することも可能です。

侵害を受けたエンドポイントを隔離、ネットワーク内での被害の拡大を阻止

エンドポイントから始まった攻撃は、瞬く間にネットワーク全体に広がる可能性があります。FireEyeエンドポイント・セキュリティでは、攻撃を検知した後、セキュリティ侵害を受けたエンドポイントをワンクリックで即座に隔離して攻撃を遮断し、被害の拡大や深刻化を阻止できます。その後、感染拡大のリスクを懸念せずに、落ち着いて詳細なフォレンジック調査を実施できます。

FireEyeエンドポイント・セキュリティの動作の仕組み

FireEyeエンドポイント・セキュリティは、数万台規模のエンドポイントが対象となる場合でも、わずか数分で既知および未知の脅威を検索、調査できます。FireEyeのエンドポイント・セキュリティ製品やネットワーク・セキュリティ製品、ログ管理製品が発したアラートを、FireEye Dynamic Threat Intelligence経由で相関分析します。その結果、セキュリティ脅威の検証により次の点を明らかにできます。

- エンドポイントへの侵入に使用された攻撃経路
- 攻撃が発生、持続したのは、特定のエンドポイントに限定されているかどうか
- 他のエンドポイントにも被害が拡大した場合、そのエンドポイントの特定
- エンドポイントがセキュリティ侵害を受けていた期間
- 外部に送信されていた知的財産の有無
- 被害拡大を防止するために隔離する必要のあるエンドポイントおよびシステム

FireEyeエンドポイント・セキュリティのシステム要件

FireEyeエンドポイント・セキュリティには、クロック周波数1 Ghz以上のPentium互換プロセッサ、300MB以上の空きディスク容量が必要です。サポートするオペレーティング・システムは下記のとおりです。

オペレーティング・システム	最小システム・メモリ（RAM）
Windows XP SP3	512 MB
Windows 2003 SP2	512 MB
Windows Vista SP1以降	1 GB（32ビット）、2 GB（64ビット）
Windows Server 2008（R2を含む）	2 GB（64ビット）
Windows 7	1 GB（32ビット）、2 GB（64ビット）
Windows Server 2012（R2を含む）	2 GB（64ビット）
Windows 8	1 GB（32ビット）、2 GB（64ビット）
Windows 8.1	1 GB（32ビット）、2 GB（64ビット）
Windows 10	1 GB（32ビット）、2 GB（64ビット）
Windows Server 2016	2 GB
Mac OS 10.9以降	1 GB

ハードウェア・アプライアンスの仕様

FireEyeエンドポイント・セキュリティのハードウェア導入オプションでは、通信および脅威インテリジェンスを利用するためにアプライアンスを1台使用します。1台のアプライアンスは、最大10万台のエンドポイントをサポートします。

仕様	HX 4402/HX 4400D
ストレージ容量	1.8 TB HDD 4台、RAID 10、2.5インチ、フィールド交換対応
エンクロージャ	1RU、19インチ・ラックに適合
シャーシの寸法（幅×奥行×高さ）	437×706×43.2 mm
AC電源	冗長電源（1+1）750W、100～240 VAC
消費電力（最大）（ワット）	313W
平均故障間隔（時）	3万5,200時間
重量（アプライアンスのみ）	15 kg

詳細については、FireEyeのWebサイトをご覧ください。
www.FireEye.jp

FireEyeについて

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4割以上を含む、世界67か国以上の5,600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
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 |
877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com

FireEye