データシート

FireEye Central Management

デバイスと脅威情報を一元的に管理し、攻撃経路のデータを相関分析

ハイライト

- 複数のFireEyeプラットフォームを集中管理
- 複数の攻撃経路を相関分析して複合型の脅威をブロック
- 1時間程度で導入できる専用開発のプラットフォーム
- 高度な標的型攻撃への対策状況が一目で分かるセキュリティ・ダッシュボード
- セキュリティ・イベント情報を集約し、レポート作成や監査対応を効率化
- 複数のFireEyeソリューションの管理を効率化し、構成や脅威アップデート、ソフトウェア・アップグレードの管理に要する時間を短縮

図1: CM 4500およびCM 9500（このほかにCM 7500をラインナップ）

概要

FireEye® Central Management（CMシリーズ）は、FireEye製品の管理、レポート作成、データ共有を統合する、容易に導入可能なネットワークベースの管理ソリューションです。Central Managementでは、自動生成された脅威インテリジェンスをリアルタイムに共有し、組織に対する高度な標的型攻撃を検知、ブロックします。また、各FireEyeソリューションの構成、管理、レポート作成を一元化できます。

ローカル環境で検知された脅威インテリジェンスをリアルタイムに共有

各FireEyeソリューションは、FireEye Multi-Vector Virtual Execution™（MVX）エンジンを使用してリアルタイムの脅威インテリジェンスを生成します。Central Managementは生成された脅威インテリジェンスを、システムに導入された複数のFireEye環境に配信し、各ソリューションはそれを利用して、高度なサイバー攻撃をダイナミックに防御できます。FireEye Dynamic Threat Intelligence™（DTI）クラウドに参加している場合は、匿名化された脅威インテリジェンスの送受信をCentral Managementで集中管理し、世界中の企業やテクノロジー・パートナー、サービス・プロバイダーに導入されたFireEyeソリューションと脅威インテリジェンスを共有できます。

ダッシュボードでセキュリティ状況を素早く把握、詳細な解析にも対応

Central Managementには、さまざまな操作を集中的に行い、セキュリティ状況を正確に把握できる統合セキュリティ・ダッシュボードが用意されています。このダッシュボードにより、感染システム数をリアルタイムで把握し、さらに詳しい調査を行って、次に行うべき対策を判断できます。

高度な標的型攻撃を総合的に解析

複合型の脅威を解析して、不正なURLを含むスピア・フィッシング・メールの正確な検知や、境界のアラートとエンドポイントの相関分析などを実施できます。これにより、セキュリティ・アナリストは複合型攻撃の全体像を把握し、対策の実施に必要となる詳細情報を入手して、高度な標的型攻撃からネットワークを保護することができます。

WebベースのGUIコンソールとアラート機能

Central Managementに用意されているWebベースのコンソールで、イベントを確認、検索、フィルタリングしたり、SMTP、SNMP、syslog、またはHTTP POST経由でリアルタイムのアラートを受け取ることができます。管理者は、種類や日付、IPアドレス範囲を条件にイベントをフィルタリングできますが、表示されるのはその管理者の役割で閲覧可能な情報のみとなります。アラートは、サードパーティのセキュリティ情報/イベント管理（SIEM）ツールに送信することもできます。イベントのリンクをクリックすると、該当するFireEyeソリューションに直接接続し、そのソリューションで保護しているネットワーク・セグメントの状況を確認できます。

プラットフォームの構成とアップグレードを集中管理

各FireEyeプラットフォームをダイナミックに構成するCentral Managementでは、導入作業を効率よく行うことができます。各プラットフォームの設定を一括して行った後、適切なタイミングでネットワーク全体に配信します。管理者は、各FireEyeセキュリティ・ソリューションの構成や設定の確認をリモートから実施できます。また、アップグレードはすべての管理対象ソリューションに対して同時に配信され、各ソリューションのセキュリティ機能が常に最新の状態に維持されます。

セキュリティ・データの集約と詳細なレポートの作成

厳格な規制が適用される大規模組織では、Central Managementを使用して、セキュリティ・データの総合的なレポートを効率よく作成できます。Central Managementでは、長期間のデータ保存を求める規制に対応できるよう、監査に関係するセキュリティ・イベント情報を収集、保存できます。

Central Managementは、特定の脅威を名前や種類別に検索して、レポートを作成できるため、ネットワークの感染ホスト数や検知数の多いマルウェア、コールバック・イベントの件数、地理情報などを集計して確認できます。また、傾向ビューでは、感染システムの減少状況を時系列で把握することが可能です。

表1: アプライアンスの仕様

	CM 4500	CM 7500	CM 9500
ネットワーク・インターフェイス・ポート	1GigE BaseTポート x 2	1GigE BaseTポート x 2	1GigE BaseTポート x 2
管理ポート（背面パネル）	1GigE BaseTポート x 2	1GigE BaseTポート x 2	1GigE BaseTポート x 2
IPMIポート（背面パネル）	搭載	搭載	搭載
前面パネルLCDおよびキーパッド	搭載	搭載	搭載
PS/2キーボードおよびマウス・ポート、DB15 VGAポート（背面パネル）	搭載	搭載	搭載
USBポート（背面パネル）	Type A USBポート x 2	Type A USBポート x 2	Type A USBポート x 2
シリアル・ポート（背面パネル）	115,200 bps、パリティなし、8ビット、1ストップ・ビット	115,200 bps、パリティなし、8ビット、1ストップ・ビット	115,200 bps、パリティなし、8ビット、1ストップ・ビット
ストレージ容量	4 TB HDD x 4、RAID 10使用可、8 TB	4 TB HDD x 4、RAID 10使用可、8 TB	4 TB HDD x 4、RAID 10使用可、8 TB
エンクロージャ	1RU、19インチ・ラックに適合	2RU、19インチ・ラックに適合	2RU、19インチ・ラックに適合
シャーシの寸法（幅×奥行×高さ）	437 x 650 x 43.2 mm	438 x 620 x 88.4 mm	438 x 620 x 88.4 mm
AC電源	冗長電源（1+1）750W AC PSU	冗長電源（1+1）800W AC PSU	冗長電源（1+1）800W AC PSU
消費電力（最大）（ワット）	245W	456W	612W
熱放散（最大）（BTU/時）	836 BTU/時	1,556 BTU/時	2,088 BTU/時
平均故障間隔（時）	3万5,200時間	6万700時間	6万700時間
重量（アプライアンスのみ/梱包時）（kg）	13.6 kg/18.6 kg	20.0 kg/29.6 kg	22.9 kg/32.5 kg

注: パフォーマンス値は、システム構成や処理するトラフィックの特性によって異なります。

表1: アプライアンスの仕様

	CM 4500	CM 7500	CM 9500
安全性に関する適合規格	IEC 60950、EN 60950、CSA 60950-00、CE Marking	IEC 60950、EN 60950、CSA 60950-00、CE Marking	IEC 60950、EN 60950、CSA 60950-00、CE Marking
EMC/EMIの適合規格	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A
規制への対応	RoHS、REACH、WEEE	RoHS、REACH、WEEE	RoHS、REACH、WEEE
温度（動作時）	0℃～35℃	0℃～35℃	0℃～35℃
相対湿度（動作時）	10%～95%@40℃（結露なきこと）	10%～95%@40℃（結露なきこと）	10%～95%@40℃（結露なきこと）
動作高度	1,500 m	1,500 m	1,500 m

注: パフォーマンス値は、システム構成や処理するトラフィックの特性によって異なります。

表2: 仮想アプライアンスの仕様

モデル	CPUのコア数	RAM	仮想NIC数	ハードディスク容量
CM2500V	4	32 GB	4（合計）： 1（管理対象） 1～3（予備）	512 GB
CM7500V	16	128 GB	4（合計）： 1（管理対象） 1～3（予備）	1200 GB

注: 各仮想アプライアンスは、上記の仕様を満たしている必要があります。

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

FireEyeについて

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・レスポンスといった、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。