FireEye

データシート

Central Management System

ローカルの脅威データをリアルタイムで共有し、企業の配備環境を統合管理

ハイライト

- 専用のアプライアンスを 30 分以内で配備可能
- 5 台以上の FireEye アプライアンスを配備し、FireEye Web MPS、Email MPS、File MPS、MAS を使用している環境に理想的なソリューション
- FireEye 配備規模に合わせて 2 つのモデルを用意
- 複数の FireEye アプライアンスを一元管理。構成管理、脅威情報の更新、ソフトウェアのアップグレードに必要な時間を短縮
- セキュリティダッシュボードで高度な標的型攻撃に対する防御状態を素早く確認
- 統合されたセキュリティイベントストアハウスでレポートと監査を簡素化

ネットワークのセキュリティ状態とアプライアンスの負荷がダッシュボードにリアルタイムで表示される

FireEye Central Management System（CMS）では、配備が容易なネットワークアプライアンスに導入された FireEye Malware Protection Systems（MPS）を一元的に管理し、レポート生成、データ共有を行うことができます。

CMS では、FireEye 配備環境で自動的に生成されたマルウェア情報をリアルタイムに共有し、組織を狙う高度な攻撃を阻止することができます。また、FireEye セキュリティアプライアンスの構成、管理、レポート生成を一元的に行うことができます。

ローカルのマルウェア情報をリアルタイムに共有

FireEye アプライアンスは Virtual Execution（VX）エンジンを使用して高度なマルウェアをリアルタイムに阻止します。CMS は分散ハブとして機能し、FireEye 配備環境全体を高度な標的型攻撃から保護します。Malware Protection Cloud（MPC）のユーザーはマルウェア情報の送受信を CMS で一元管理できます。

ドリルダウン機能を備えたダッシュボードでセキュリティ状況を素早く確認

CMS には、セキュリティ状況を正確に把握し、様々な操作を実行できる統合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、感染システムの数をリアルタイムに確認できます。また、ドリルダウン機能で感染の詳細を確認し、次に行う対策を判断することができます。

高度な標的型攻撃を統合解析

FireEye Web MPS、Email MPS、File MPS、Malware Analysis System（MAS）と FireEye CMS を配備すると、不正な URL を配布するスピアフィッシング詐欺メールなどの複合的な脅威を詳しく分析できます。これにより、セキュリティアナリストは複合的な攻撃の全貌を解明し、高度な標的型攻撃から組織を守ることができます。

「当校ではユーザーのセキュリティ対策に真剣に取り組んでいます。デスクトップにアンチウイルスを導入し、セキュリティパッチを適用しています。ゲートウェイにはファイアウォールと IPS システムを配備していますが、感染したユーザーがリモートからアクセスしたり、スピアフィッシング、ゼロデイ攻撃、標的型攻撃の標的になる可能性もあります。しかし、シグネチャベースのソリューションでは現在の Web エクスプロイトやボットネットを完全に防ぐことはできません。」

— 芸術系大学のシステム / サーバー管理者

エンタープライズクラスのコンソールとアラート機能

CMS の Web GUI コンソールでは、イベントの検索とフィルタリングが可能です。また、SMTP、SNMP、Syslog、HTTP POST を介してリアルタイムでアラート通知を送信できます。イベント、日付、IP 範囲で結果をフィルタリングできますが、管理者に割り当てられた役割で許可されていない情報は表示されません。また、ArcSight、Nitro Security、Splunk、RSA などのサードパーティの SIEM ツールに通知を送信することもできます。

CMS コンソールでイベントをクリックすると、特定の FireEye アプライアンスにシームレスに接続し、ローカル管理システムを表示してネットワークセグメントの保護状態を確認できます。

構成とアプライアンスのアップグレードを一元管理

FireEye CMS では、構成を動的に行い、組織全体で効率よく配備することができます。設定は一元管理され、必要に応じて配布されます。管理者は 1 台のアプライアンスまたはアプライアンスグループの設定をリモートから表示し、管理できます。また、管理対象のすべてのアプライアンスにアップグレードを配備し、すべてのアプライアンスのセキュリティ機能を最新の状態にすることができます。ボタンをクリックするだけで、VX エンジンに対するアップグレード（新しいゲストイメージの最新のサービスパックなど）をプッシュできます。

統合されたストアハウスと詳細レポート

規制の厳しい大企業では、CMS のセキュリティデータストアハウスを利用すると、統合されたレポートを効率よく生成できます。CMS では、監査関連のセキュリティイベントを収集してデータを保存し、法規制を遵守することができます。

FireEye CMS では、特定の脅威レポートを名前や種類で検索できます。感染の多いホストやマルウェア、コールバックイベント、地理的情報などのサマリも確認できます。傾向ビューを表示すると、侵害されたシステム数の変化を確認できます。

技術仕様

	CMS 4310	CMS 7300
筐体サイズ	1U ラックマウント	1U ラックマウント
重量	13.6 Kg	13.6 Kg
寸法（幅 x 奥行 x 幅）	43.7 x 65.0 x 4.3 cm	43.7 x 65.0 x 4.3 cm
格納装置	19 インチラック	19 インチラック
管理用インターフェース	10/100/1000 BASE-T ポート 2 個	10/100/1000 BASE-T ポート 2 個
モニタリングインターフェース	N/A	N/A
AC 入力電圧	100 ~ 240 VAC 自動切換え（全範囲）	100 ~ 240 VAC 自動切換え（全範囲）
AC 入力電流	8.5-6 A	8.5-6 A
電源装置 /RAID	冗長 /3 SAS HDD（HW RAID5）	冗長 /3 SAS HDD（HW RAID5）
周波数	50-60 Hz	50-60 Hz
AC 電源	最大 700 W	最大 700 W
周囲温度	40° C	40° C