McAfee ePolicy Orchestrator

セキュリティを一元管理して情報を共有、環境を可視化して的確に対応

セキュリティ管理では様々なツールやデータを扱います。作業は自ずと煩雑になり、管理プロセスも複雑化しています。この状況は、攻撃側に時間的な余裕を与えることになり、被害の拡大にもつながります。一方、サイバーセキュリティを担当する人材は不足しています。複雑なセキュリティの管理に必要な要員を確保するのも容易ではありません。McAfee® ePolicy Orchestrator® (McAfee ePO™) 管理プラットフォームを使用すると、ミスを誘発しやすい煩雑な作業をなくし、セキュリティをより迅速に、効率的に管理することができます。

セキュリティの基礎

セキュリティの基礎となるものは何でしょう。セキュリティアーキテクチャの中核部分は、エンドポイントとシステムの状態を監視し、管理する能力です。Center for Internet Security **(CIS)** ControlsやNational Institute of Standards Technology **(NIST) SP 800-53**などの標準規格でも、この機能は不可欠な要素とされています。McAfee ePOコンソールを使用すると、環境全体を可視化し、ポリシーの設定と適用を自動的に行い、正常なセキュリティ状態を維持することができます。1つのコンソールで企業全体のセキュリティ製品のポリシーを管理できるので、複数の製品が存在する場合でも管理作業が複雑になることはありません。このセキュリティ機能はITセキュリティ コンプライアンスの基礎となります。

実証済みの高度なセキュリティ管理

McAfee ePOコンソールは30,000を超える企業や組織で採用されています。これらの組織では、McAfee ePOコンソールでセキュリティを管理することで、コンプライアンス プロセスの省力化と自動化を実現し、エンドポイント、ネットワーク、セキュリティ オペレーションの可視化に成功しています。大規模な組織では、拡張性に優れたMcAfee ePOコンソールのアーキテクチャにより、数百あるいは数千のノードを管理しています。McAfee ePOコンソールでは、ポリシーのメンテナンスを簡単に行うことができます。Data Exchange Layer (DXL) 経由でサードパーティの脅威情報を取得し、様々な製品と双方向でポリシーを共有することができます。プロセスやデータ共有が効率化に行われるので、より迅速かつ正確な対応が可能になります。

McAfeeとつながる

効率と統合

ESGの調査によると、大量に発生する脅威やデバイスを管理するため、40%の組織が10～25のツールを使用し、30%の組織が26～50のツールを使用しています。このように様々なツールを使用しているため、管理作業は複雑になり、インストールからレポートまでが統合された管理環境に比べると運用コストは倍になります。この問題を解決するため、McAfeeは「Together is power」というアプローチでセキュリティ管理を提供しています。このアプローチでは、既存の製品を活かしながら、脅威インテリジェンスやオープンソース データを利用し、サードパーティ製品を統合することが可能です。McAfeeは様々なセキュリティ製品のコンプライアンスと管理を一元的に行います。複数の製品から重要なデータを迅速に取得し、必要なポリシー アクションをすぐに実行できます。また、McAfee ePOを使用すると、既存の資産と次世代の技術を1つのフレームワークに統合することができます。

McAfee ePOで管理される製品の一例

McAfee製品	サードパーティ製品
McAfee Endpoint Protection（脅威対策、ファイアウォール、Web管理）	Guidance Software: enCase Enterprise
McAfee Drive Encryption	Avecto: Privilege Guard
McAfee File and Removable Media Protection	AccessData: AccesData Enterprise
McAfee Active Response	Autonomic Software: Power Manager, Patch Manager
McAfee Management for Optimized Virtual Environments（McAfee MOVE）	Xerox MFP
McAfee Data Loss Prevention（McAfee DLP）	DXL
McAfee Policy Auditor	
McAfee Enterprise Security Manager	
McAfee Threat Intelligence Exchange	
McAfee Application Control	
McAfee Cloud Workload Security	
McAfee Advanced Threat Defense	
McAfee Content Security Reporter	
McAfee Database Activity Monitoring	

使用例: McAfee ePOコンソールによるセキュリティ製品の一元管理

製品と技術	一元管理の例	利点
McAfee ePO McAfee Endpoint Security	McAfee Endpoint Securityにより、エンドポイントで既知の不正なファイルが検出されます。McAfee ePOコンソールで、より厳格なポリシーをエンドポイントに設定し、脅威を隔離します。これらの処理は共通の管理インターフェースで行うことができます。	不正なエンドポイントの迅速な封じ込め
McAfee ePO McAfee DLP McAfee Enterprise Security Manager	McAfee Enterprise Security Managerでエンドポイントからの重要データの流出が検出されます。McAfee ePOコンソールでこのエンドポイントにタグを付けます。McAfee ePOコンソールでデータ損失防止ポリシーを適用してデータをブロックし、ユーザーにコンプライアンス違反を通知します。	データ損失ポリシーの自動適用

統合の例

製品と技術	統合の例	利点
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	McAfee Endpoint Securityで不審なホストにフラグが設定されます。McAfee ePOコンソールで追加のスキャンを実行できます。PxGrid経由でCisco ISEに接続し、DXLで情報を交換します (McAfee ePOコンソール)。ホストが許容可能と判断されるまで、Cisco ISEがホストを隔離します。	プロアクティブな保護の強化
Avecto Defendpoint McAfee ePO DXL McAfee Threat Intelligence Exchange	業界最先端の特権管理ソリューションであるAvecto Defendpointを McAfee ePOから配備し、管理します。Avecto Defendpointの設定変更がMcAfee Threat Intelligence Exchangeアプリケーション レピュテーション データによって通知されます。	複雑さの解消 インフラを追加する必要はありません。TCOを低減できます。 脅威インテリジェンスに基づく特権アクセスの変更
Rapid7 Nexpose McAfee ePO DXL	McAfee ePOがNexposeと資産リストを共有します。McAfee ePOコンソールからリスク状況を把握し、的確なポリシーを設定できます。DXLベンダー コミュニティと脆弱性データを共有します。	複雑さの解消 1つのダッシュボードで全体のセキュリティ状況を正確に把握し、優先順位に従ってアクションを実行できるので、リスクを最小限に抑えることが可能です。
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	この統合により、ネットワークやエンドポイント間でリアルタイムの脅威情報を双方向で共有できます。 DXLコミュニティとイベントを共有できます。	検出までの時間を短縮 攻撃をブロックして修復

統合プラットフォームを使用している組織のほうが、保護能力が高く、迅速な対応を行っています。

	統合管理を使用している組織	統合管理を使用していない組織
昨年経験したセキュリティ侵害が5件未満	78%	55%
8時間以内に脅威を検出	80%	54%

2016 Penn Schoen Berland

拡張性に優れたワークフローでプロセスを簡素化

McAfee ePOデータベースは柔軟な自動管理機能を提供します。1つのコンソールで脆弱性、セキュリティ状態の変化、既知の脅威を迅速に識別・管理し、対応することができます。McAfee ePOコンソールでは、環境内のセキュリティ イベントの種類や重大性、ポリシー、ツールに基づいてアラートや対応を定義できます。開発業務とセキュリティ オペレーションに対応するため、McAfee ePOプラットフォームではセキュリティとITオペレーション システム間のワークフローを自動化し、問題の修復を迅速に行うことができます。McAfee ePOコンソールで、厳格なポリシーの割り当てなど、ITオペレーション システムによる修復アクションを開始できます。Webアプリケーション プログラミング インターフェース（API）を利用することで、手動操作を減らすことができます。

一般的な使用例

- セキュリティ コンプライアンス レポートを定期的に作成して問題に対応することで、時間を節約し、労働集約型の作業を減らすことができます。
- 強力なAPIセットを利用することで、McAfee ePOコンソールを既存のビジネス プロセスに簡単に統合し、より多くの情報を収集したり、ワークフローを強化できます（たとえば、チケッティング システム、Webアプリケーション、セルフサービス ポータルなどに統合できます）。
- McAfee ePOコンソールとActive Directoryを同期することで、組織のネットワークに新しいマシンが追加されたときにエージェントとセキュリティ ソリューションを配備し、セキュリティ状態を維持できます。

「現在、市場で最も強力なエンドポイント管理プラットフォームはMcAfee ePolicy Orchestratorでしょう。この製品で社内のすべてのセキュリティ製品を管理することが可能で、大規模な組織が求める能力と柔軟性を兼ね備えています。共通のポリシー エンジンと脅威インテリジェンスの共有により、様々なセキュリティ製品の統合が可能です。」

— Forrester Wave: Endpoint Security Suites 2016（2016年エンドポイント セキュリティ スイート）

迅速な回避と修復

McAfee ePOプラットフォームには高度な機能が組み込まれています。セキュリティ オペレーションの担当者は、これらの機能を使用して脅威の回避や対策を効率的に行うことができます。McAfee ePOの自動応答機能を使用すると、発生したイベントに応じてアクションを自動的に実行できます。アクションは単なる通知の場合もあれば、修復の承認の場合もあります。

自動応答の一般的な使用例

- 事前に設定したしきい値に基づき、新しい脅威、更新の失敗、優先度の高いエラーをメールまたはSMSで管理者に通知します。
- クライアントまたは脅威イベントに基づいてポリシーを適用し、ホストが侵害されている可能性がある場合に外部との通信を遮断したり（コマンドや制御操作を拒否します）、管理者がポリシーをリセットするまで外部へのデータ送信をブロックします。
- 脅威検出時にシステムにタグを付け、オンデマンド メモリー スキャンなどの修復作業を実行します。
- 登録済みの実行ファイルを開始して外部スクリプトやサーバー コマンドを実行します。たとえば、サービス デスクでチケットを生成したり、他のビジネス プロセスに統合したりします。
- より厳格なポリシーを適用して、エンドポイントを自動的に隔離します。

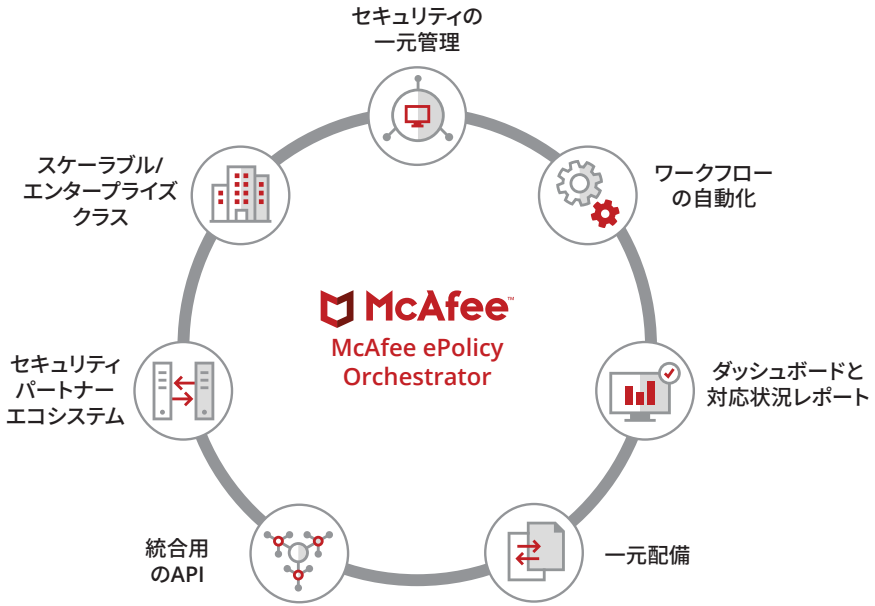

図 1. McAfee ePOコンソールでセキュリティの一元管理

McAfee ePOコンソールで組織全体を管理

セキュリティを一元管理

- 1つのコンソールで数百または数千のノードを一元管理し、企業全体の状態を把握できます。
- オープン フレームワークにより、McAfeeとサードパーティのセキュリティ システムを管理できます。
- 拡張性の高いプラットフォームで既存のITインフラと統合できます。

対応時間を短縮

- 包括的なビューとセキュリティ情報により、内部と外部のセキュリティ問題に事前に対応できます。
- セキュリティ更新と定義を迅速かつ一元的に配布し、最新の脅威からエンドポイントを保護できます。
- 実用的なダッシュボードと高度なクエリー、レポート機能により、対応時間を短縮できます。

複雑さを解消してプロセスを簡素化

- ガイド付きの設定、ポリシーの自動管理、事前定義のダッシュボードなど、すぐに使える便利な機能が用意されています。
- タグに基づくポリシー割り当てにより、ビジネスの役割またはリスク状況に基づいて、事前定義のセキュリティ プロファイルを個々のシステムまたはシステム グループに的確に割り当てることができます。
- タスク カタログと管理作業の自動化により、管理プロセスを簡素化。オーバーヘッドを抑えることができます。
- 複数のエンドポイント製品を1つのエージェントで管理し、エンドポイント間での不一致を減らすことができます。

企業の配備状況に合わせた拡張性

- エンタープライズ クラスのアーキテクチャにより、1台のサーバーで数十万のデバイスを管理できます。
- 異種のシステムで構成された複雑なIT環境も管理できます。
- エンタープライズ レポート機能により、環境全体のセキュリティ状態とコンプライアンスを1つのビューで確認できます。

「McAfee ePOは傑出しています。この製品があれば、社内のすべてのエンドポイントのセキュリティを管理できます。社内に導入しているすべてのMcAfee製品を1つの画面でチェックできます。ダッシュボードは使いやすく、可視化、レポート、配備、更新、メンテナンス、意思決定など、必要な機能がすべて揃っています。」

— Christopher Sacharok
情報セキュリティ エンジニア
Computer Sciences Corporation

McAfee
Together is power.

〒150-0043
東京都渋谷区道玄坂1-12-1
渋谷マークシティ ウエスト20F
Tel. 03-5428-1100（代表）
www.mcafee.com/jp