



McAfee Endpoint Threat Protection

ビジネスの成長に合わせて拡張可能なセキュリティ対策

脅威は進化を続けています。今後もこの状況は変わらないでしょう。エンドポイントはすでに強力な保護対策で保護されています。しかし、新しい技術を常に追加していかなければ、必要な保護レベルを維持することはできません。その結果、セキュリティ対策はさらに複雑になり、サイロ化が進んでいます。McAfee® Endpoint Threat Protectionは、いま必要とされている保護機能だけでなく、新たに発生する高度な脅威にも対応できるセキュリティ対策を提供します。このソリューションには、脅威対策、ファイアウォール、Webやメールの保護、デバイスコントロールなどが統合されています。これらの機能が相互に連携し、脅威をリアルタイムで分析してシステムやユーザーへの被害を未然に防ぎます。

主な特長

- マルチレイヤーの協調型の保護技術でセキュリティを強化します。
- 必要に応じて、保護機能を簡単に拡張できます。
- 一元管理により、生産性が向上します。消費されるシステムリソースは最小限で、スキャンがユーザーの操作に影響を及ぼすこともありません。

協調型のエンドポイント フレームワーク

統合を念頭に置いて開発されたMcAfee Endpoint Threat Protectionは、複数の保護機能が連動し、リアルタイムで情報を共有します。これにより、不審なファイル、Webサイト、不審なプログラムを迅速に識別し、ブロックします。

事例

Web から不正なファイルをダウンロード

ファイルハッシュが Web 管理から脅威対策に送信され、ODS が開始する。

不正なファイルが検出され、フルアクセスが許可される前にブロックされる。

フォレンジック データが収集される (送信元 URL、ファイルハッシュなどの情報)。

イベント データが他のモジュールや McAfee® ePolicy Orchestrator® (McAfee ePO™) と共有され、クライアントのユーザー インターフェースに表示される。

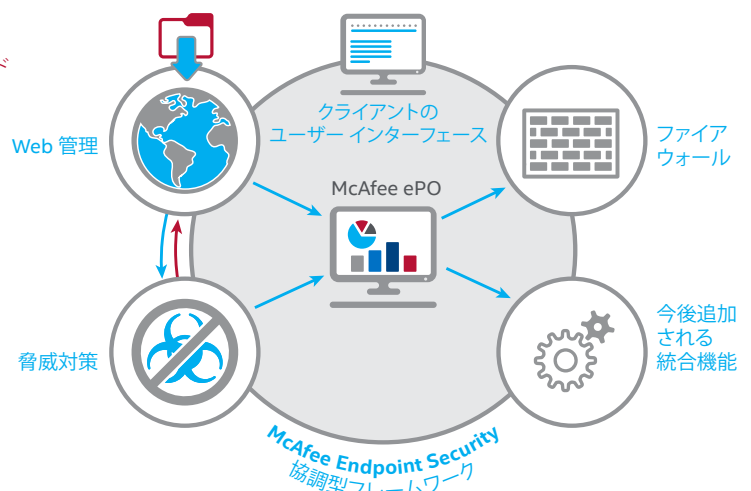


図1. McAfee Endpoint Threat Protectionによる防御体制

現在だけでなく将来にも対応した統合ソリューション

連動性のない単体製品を配備する必要はありません。McAfee Endpoint Threat Protectionでは、協調型のフレームワークが採用され、複数の保護技術がリアルタイムで連携します。これにより、脅威分析を強化するだけでなく、収集されたフォレンジックデータを他の保護機能と共有できるので、別のエンドポイントで発生した脅威や別の入口から侵入した脅威も迅速に識別し、ブロックできます。

このアプローチでは、配備も柔軟に行うことができます。購入時にすべての機能をインストールし、後で設定する機能を決めることもできます。また、ポリシーを変更することで、機能を簡単に有効にすることができます。

弊社のフレームワークは、新しい技術を簡単に追加できるアーキテクチャを採用しているので、必要に応じて保護機能の拡張が可能です。より巧妙な脅威が出現したときに、別の高度な保護機能をいつでも追加することができます。

手頃な価格で、パフォーマンスに対する影響も少ない

McAfee Endpoint Threat Protectionは、拡張可能なフレームワークを採用し、コアとなる保護技術を搭載しています。拡張は簡単で、パフォーマンスへの影響も少ないので、生産性が向上します。たとえば、McAfee ePolicy Orchestratorで集中管理を行うので、業務をより効率的に実施できます。このソフトウェアでは、セキュリティポリシーの配布、モニタリング、管理を1つの画面で行うことができます。環境内で複数のオペレーティングシステムが実行されている場合でも、Microsoft Windows、Apple Macintosh、Linuxシステムに適用できるクロスプラットフォームポリシーを使用できます。McAfee Endpoint Threat Protectionの各コンポーネントでは、共通の言語 (McAfee Data Exchange Layer) を使用しているため、技術や応答速度を考慮してプロセスを最適化できます。また、露出範囲を狭くしてリスクの軽減を図ることもできます。

スキャンは操作に影響を及ぼしません。メモリーやCPUの利用率を最適化し、システムへの影響を最小限に抑えることもできます。分かりやすいユーザーインターフェースが標準装備されているので、実行されたアクションとその理由を簡単に確認できます。

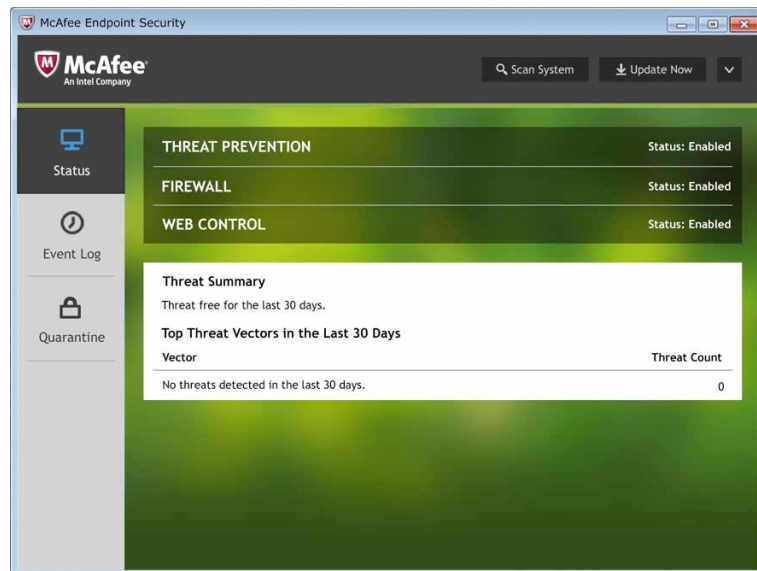


図2. 管理者にもユーザーにも分かりやすいユーザーインターフェース

対応プラットフォーム

- Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary
- Mac OS X 10.5以降
- Linux 32/64ビット プラットフォーム: RHEL, SUSE, CentOS, OEL, Amazon Linux, Ubuntuの最新バージョン

サーバー:

- Windows Server (2003 SP2以降、2008 SP2以降、2012)、Windows Server 2016
- Windows Embedded (Standard 2009、Point of Service 1.1 SP3以降)
- Citrix Xen Guest
- Citrix XenApp 5.0以降

コンポーネント	利点	顧客のメリット	差別化
脅威対策	多層型の保護対策でマルウェアの検出、封じ込め、修復を迅速に行う包括的なセキュリティです。	<ul style="list-style-type: none"> ヒューリスティックやオンアクセス スキャンにより、既知または未知のマルウェアも検出します。 ポリシーと配備を単純化し、Windows、Mac、Linuxプラットフォームを保護します。 信頼されたプロセスにはスキャンを実行せず、不審な対象に優先度を設定します。これにより、パフォーマンスが最適化されます。 	Webの保護やファイアウォールと連携して分析能力を強化し、潜在的な脅威のブロックルールを自動的に適用する多層型のマルウェア対策です。
統合ファイアウォール	ポットネット、分散型サービス拒否 (DDoS) 攻撃、信頼されていない実行ファイル、高度な持続型脅威、危険なWeb接続からエンドポイントを保護します。	<ul style="list-style-type: none"> ポリシーを施行してユーザーを保護し、生産性を維持します。 不要な受信接続をブロックし、送信要求を制御することで帯域幅を保護します。 信頼されたネットワークや実行ファイル、危険なファイルや接続をユーザーに通知します。 	社内ネットワークに接続していないノートPCやデスクトップも、アプリケーション ポリシーと位置情報ポリシーで保護します。
Web管理	Web保護とフィルタリングにより、エンドポイントでのWeb閲覧を保護します。	<ul style="list-style-type: none"> 不正なサイトに移動する前に警告を表示するので、リスクを軽減し、コンプライアンスを遵守できます。 危険なサイトや不適切なサイトを許可またはブロックすることで、脅威を阻止し、生産性を維持できます。 危険なダウンロードは、ダウンロードが開始する前にブロックします。 	McAfee Global Threat Intelligenceと連携して、Windows、Mac、Linux、複数のブラウザーを保護します。
McAfee Data Exchange Layer	セキュリティを統合し、Intel Security製品や他社製品間の通信を簡素化します。	<ul style="list-style-type: none"> 統合により、リスクを軽減し、対応時間を短縮できます。 オーバーヘッドが減少し、運用スタッフのコストを削減できます。 プロセスを最適化し、実用的な推奨事項を利用できます。 	<ul style="list-style-type: none"> セキュリティ製品間で最も重要な脅威情報を共有できます。 他のすべてのエンドポイントと脅威情報を迅速に共有し、脅威を未然に防ぐだけでなく、保護機能も更新できます。
McAfee ePOIによる管理	拡張性と柔軟性に優れた管理機能で、セキュリティ ポリシーを1つのコンソールで管理し、セキュリティ問題の識別と対応を行うことができます。	<ul style="list-style-type: none"> セキュリティ ワークフローを統合して簡素化しています。 可視化と柔軟性を強化し、安心してアクションを実行できるようにします。 カスタマイズ可能なポリシー施行で1つのエージェントを迅速に配備し、管理できます。 動的で自動的なクエリー、ダッシュボード、対応により、情報の取得から対応までの時間を短縮できます。 	<ul style="list-style-type: none"> 1つのコンソールできめ細かい制御を行い、セキュリティ管理作業を迅速に実行できます。また、コストの削減も可能です。 業界で広く知られた優れたインターフェースを利用できます。 ドラッグアンドドロップに対応したダッシュボードでセキュリティ エコシステムを管理できます。 オープン プラットフォームを利用しているので、新しいセキュリティ技術をすぐに導入できます。

McAfee Endpoint Threat Protectionの詳細については、www.mcafee.com/jp/products/endpoint-threat-protection.aspxをご覧ください。



McAfee. Part of Intel Security.

マカフィー株式会社

東京本社 〒150-0043 東京都渋谷区道玄坂 1-12-1
 渋谷マークシティ西20F
 TEL 03-5428-1100 (代) FAX 03-5428-1480
 〒530-0003 大阪府大阪市北区堂島 2-2-2
 近鉄堂島ビル18F
 TEL 06-6344-1511 (代) FAX 06-6344-1517
 名古屋営業所 〒450-0002 愛知県名古屋市中村区名駅 4-6-17
 名古屋ビルディング 13F
 TEL 052-551-6233 (代) FAX 052-551-6236
 〒810-0801 福岡県福岡市博多区中洲 5-3-8
 アーク博多 5F
 TEL 092-287-9674 (代)
www.intelsecurity.com

Intel、Intelのロゴ、McAfeeのロゴ、ePolicy Orchestrator、McAfee ePOIは、米国法人Intel CorporationまたはMcAfee, Inc.もしくは米国またはその他の国の関係会社における商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。Copyright © 2016 Intel Corporation. 1770_1016
 2016年10月