McAfee Endpoint Security

プロアクティブな脅威管理と、実績あるセキュリティ コントロール

エンドポイント セキュリティ: 何を優先するか

セキュリティを1つのチームで管理している企業もあれば、複数のチームで管理している企業もあります。多くの場合、セキュリティ対策は IT 管理チームやセキュリティ オペレーション チームなどといった複数のチームで分担されています。エンドポイント保護ソリューションに関していえば、組織の中でどのような役割であっても、最も関心の高いことはその機能と結果でしょう。

どのようなソリューションでも、最も優先度の高い問題が解決されなければ意味がありません。McAfee® Endpoint Securityは、どのような役割の方でもあっても、そのニーズを満たす機能を提供します。単に脅威を阻止するだけでなく、脅威ハンティングからセキュリティ コントロールの調整まで対応しています。McAfee® MVISION Insights では攻撃を受ける前に対応できるよう、脅威の優先順位付けをします。またシステムの常時稼働、自動化の対象の選別、複雑なワークフローの簡易化などが実現できます。

稼働時間と可視化の強化

McAfee Endpoint Securityを使用すると、プロアクティブな保護機能と修復ツールにより、脅威対策のライフサイクルを管理できます。自動ロールバック修復により、システムを正常な状態に戻すことができます。ユーザーや管理者の作業が中断することはありません。また、膨大な時間のかかる修復作業も短時間で完了できます。感染したマシンのリカバリや再イメージングも迅速に行うことが可能です。エンドポイントと McAfee® MVISION EDR は、グローバル脅威インテリジェンス及びリアルタイムのローカル イベント インテリジェンスを共有して脅威イベント情報を収集し、検出を回避しようとする脅威も検出して阻止し、これらをさらに調査できるよう MITRE ATT&CK フレームワークにマッピングします。管理作業は1つのコンソールで行うので、無駄な作業がなくなります。このコンソールはローカルに配備することも、SaaS や仮想環境に展開することも可能です。MVISION Insights は、組織のセキュリティ体制が十分な防御能力を有するか判断するとともに、攻撃が懸念される優先度の高い脅威を独自に可視化して脅威を制御します。これにより重大な脅威を防止し、攻撃を未然に防ぎます。

MVISION Insights は業界や地域などの特性に基づき、攻撃の可能性の高い、優先度の高い潜在的脅威についてアラートや通知を出します。さらに、セキュリティ体制を評価して、その脅威への対策ができているかを判断します。また脆弱性のあるエンドポイントを識別して、何をアップデートすべきなのかを推奨します。こういったプロアクティブな対策により、攻撃を事前に回避できるようになります。

主な特徴

- **高度な脅威に対する高度な防御:** 機械学習、認証情報窃盗防止、そしてロールバック修正で、Windows デスクトップとサーバーシステムの基本セキュリティ機能を補完
- **複雑化を回避:** McAfee のテクノロジー、Windows Defender Antivirus ポリシー、Defender Exploit Guard、Windows Firewall の設定は、すべて単一のポリシーとコンソールで管理
- **MVISION Insights:** 最新の実用的なセキュリティ インテリジェンス ソリューションで、標的となるセクターや地域に基づき優先度が高いと判断される潜在的な脅威キャンペーンに即時に対応。保護が不十分なエンドポイントを予測して、脅威の検出を向上させる対処法を提供します。優先順位付け、予測、対処を同時並行的に行う唯一のエンドポイント セキュリティ ソリューションです。

McAfeeとつながる

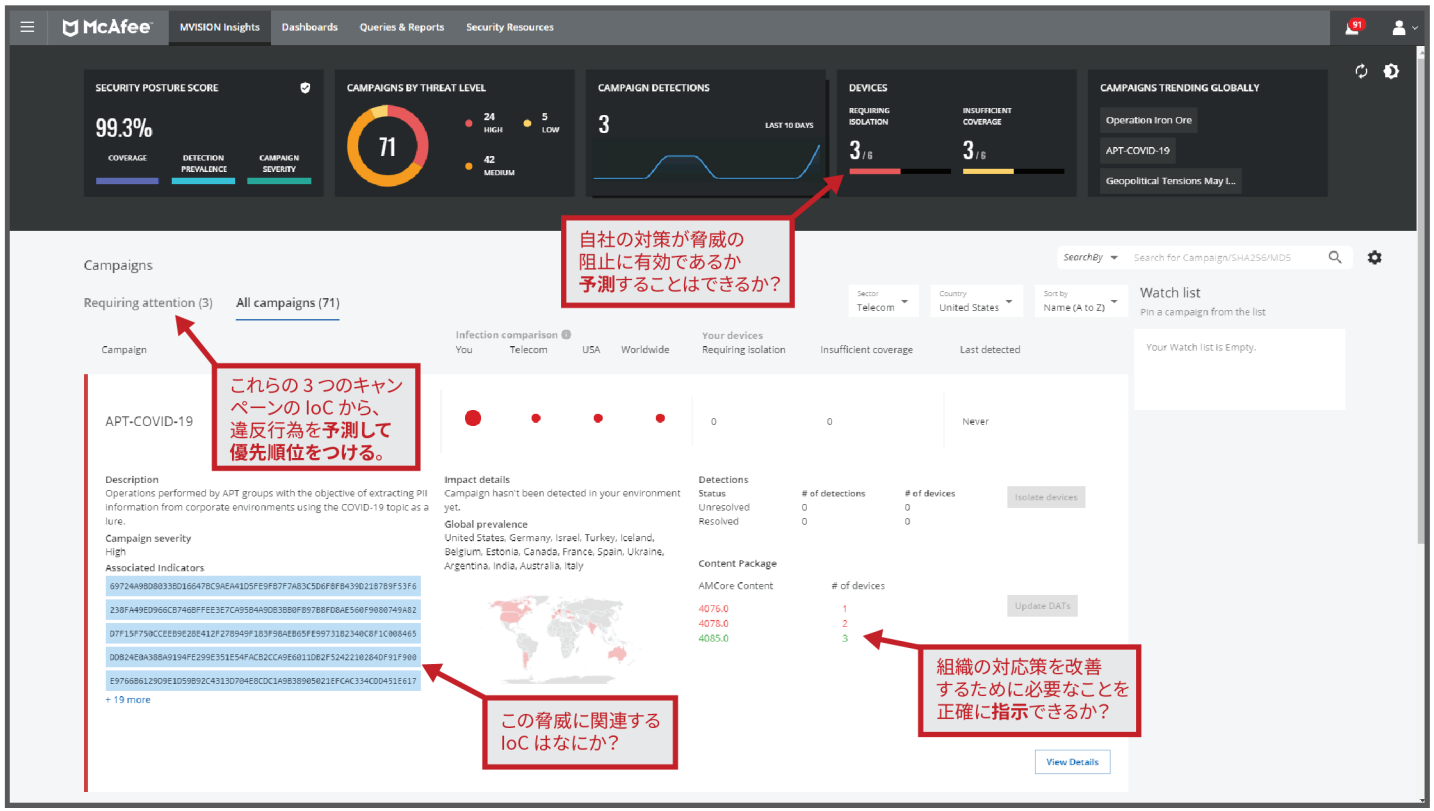

図 1. MVISION Insights ダッシュボード (MVISION Insights が適切に機能するためには、McAfee Endpoint Security の利用統計情報への同意 (オプトイン) が必要です)

McAfee Endpoint Securityは、1つのソフトウェアエージェントを使用して複数の階層の情報源から脅威情報を収集します。単体製品を併用した場合と異なり、重複を排除することができます。この統合セキュリティ アプローチにより、マニュアルでの脅威相関分析が不要になります。さらに調査が必要な脅威については、インシデント対応チームに自動的にエスカレーションされます。Story Graph はシンプルかつ一目でわかるようなフォーマットで脅威について説明し、管理者はこれをもとに脅威を簡単に調査できるようになります。

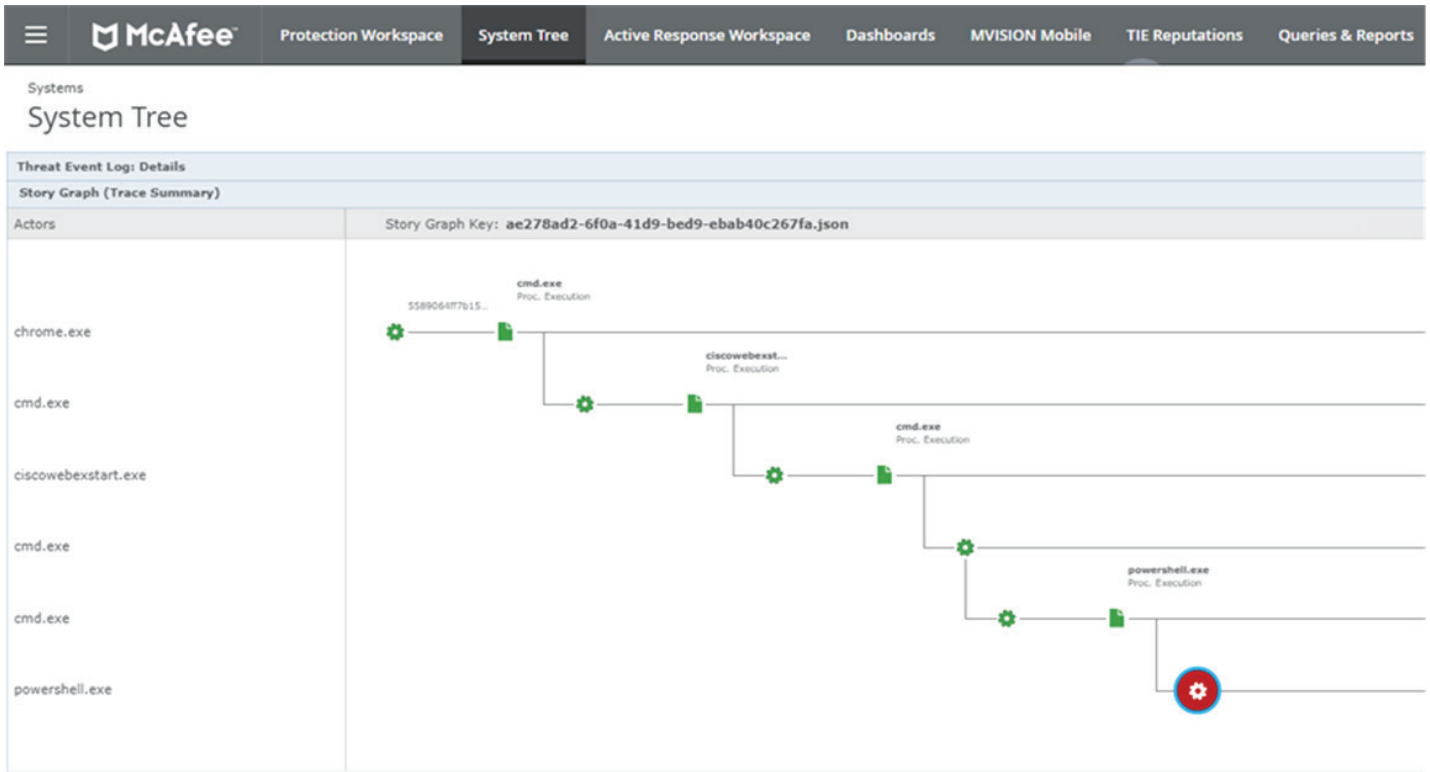

図 2. Story Graph

統合された高度脅威対策による自動化で対応時間を短縮

McAfee Endpoint Security の統合フレームワークっでは、アプリケーションの動的隔離（DAC）などの高度脅威対策も利用できます。これにより、お客様は最新の高度脅威を阻止できます。[1] たとえば、DAC はグレーウェイや未知のマルウェアを分析してアクションを実行し、これらの脅威を封じ込め、感染の拡大を防ぎます。

高度脅威対策の別の技術としてReal Protectが搭載されています。この技術では、機械学習により動作分析を行い、ゼロディ　マルウェアを検出し、検知能力を改善させています。シグネチャを使用しない分類作業をクラウド上で行うためクライアントのリソースは最小限で済み、さらにほぼリアルタイムで検出します。実用的な分析結果は、攻撃指標 (IoA) や不正指標 (IoC) の作成にも活用できます。これは、環境での感染拡大、最初の感染場所の特定、脅威主体の特定、フォレンジ

ック調査、修復作業に役立ちます。Real Protectは、動作分類の精度を自動的に向上させていきます。識別した動作に基づいてルールを追加していくので、分析の速度が向上していきます。類似した攻撃が発生した場合、静的な機能とランタイム機能により、こうした攻撃を特定します。

最後に、感染を即座に食い止めて IT セキュリティ管理者の作業負荷を減らすため、感染の確認後クライアントがエンドポイントを既知の正常な状態にまで修復します。

インテリジェントなエンドポイント保護で現在の攻撃の状況を把握

優れたインテリジェンスが良い結果をもたらします。McAfee Endpoint Securityは、収集した情報をフレームワークに接続している複数のエンドポイント保護技術とリアルタイムに共有します。これにより、不審な動作を迅速に識別し、保護対策の連携を強化できます。また、標的型攻撃やゼロディ脅威に対する保護を強化できます。ハッシュ、ソースURL、AMSI、PowerShellイベントなどの分析情報を追跡し、他の保護対策だけでなく、クライアントや管理インターフェースと共有します。これにより、ユーザーが攻撃を認識し、すぐに役立つ脅威フォレンジックを管理者に提供できます。

また、McAfee® Threat Intelligence Exchange技術は、ゲートウェイ、サンドボックス、セキュリティ情報とイベント管理（SIEM）ソリューションなど、McAfeeの他のソリューションと連携し、適応型の脅威対策を強化します。ローカル、コミュニティ、グローバルのセキュリティ情報を収集し、配布することで、攻撃の発生から検出、封じ込めまでの時間を数週間または数か月からミリ秒に短縮できます。

McAfee Endpoint Security フレームワークは McAfee® Global Threat Intelligence (McAfee® GTI) を使って、ファイル、Web、メール、ネットワークなどへの新しい脅威をクラウド上でリアルタイムに監視し、これに対処します。既存のエンドポイント フットプリントと管理システムをローカルとグローバルの脅威インテリジェンスで強化し、未知の標的型マルウェアを迅速に阻止できます。不審なアプリケーションとプロセスに対して自動的にアクションが実行されるので、新たに発生した攻撃を他の保護対策やグローバル コミュニティに通知し、迅速に対応することができます。

DACとReal Protectを利用することで、巧妙な脅威とその動作を詳しく分析できます。たとえば、DACは、隔離されたアプリケーションとそのアプリケーションが試みたアクセスの種類（レジストリやメモリーなど）に関する情報を提供します。

エンドポイントのプロセスに対する脅威情報の収集、マルウェアのハンティング、インシデント対応を行う組織は、Real Protectで不審な挙動を分析し、脅威を分類します。こういった情報は、正規のアプリケーションの圧縮、暗号化、または改ざんなどといったテクニックで検出を回避しようとするファイルベースのマルウェアの検出に特に役立ちます。

優れたパフォーマンスにより短時間で対応

インテリジェントな保護対策でも、スキャンでユーザーの操作を妨げられたり、インストールに時間がかかったり、管理作業が複雑であれば意味がありません。McAfee Endpoint Securityは、共通のセキュリティ レイヤーでユーザーの生産性を保護します。また、新しいマルウェア対策のコア エンジンはユーザーのシステムで消費するリソースや処理能力が少なくなっています。エンドポイントのスキャンはデバイスがアイドル状態のときにのみ実行されます。また、再起動やシャットダウン後にシームレスに再開するので、ユーザーの操作を妨げることはありません。

適応型のスキャン プロセスは信頼されたプロセスとソースを学習し、不審なものや不明なソースから送信されたものだけをスキャンします。これにより、必要なCPU量が少なくなります。McAfee Endpoint Securityは、McAfee GTIを使用する統合ファイアウォールを使用し、ボットネット、分散型サービス拒否（DDoS）攻撃、高度な持続型攻撃、危険なWeb接続からエンドポイントを保護します。

複雑さを解消し、持続可能性を高めることでストレスを軽減

類似した機能を提供するセキュリティ製品が急速に増えています。これらの製品を利用するには別々の管理コンソールが必要です。潜在的な脅威の全体像を把握するのは難しくなっています。オープンで拡張可能なフレームワークを採用する McAfee Endpoint Security は、強固で長期的な保護を提供し、現在および将来のエンドポイント ソリューションを集約する基盤としても機能します。このフレームワークは、Data Exchange Layer により、既存のセキュリティ ソリューションとの連携を可能にしています。この統合アーキテクチャは、McAfeeの他の製品をリームレスに連携し、セキュリティ ギャップ、テクノロジのサイロ化、冗長性を解消します。管理の煩雑さがなくなるので、生産性が向上し、運用コストを削減できます。

McAfee® ePolicy Orchestrator®（McAfee ePO™）でエンドポイントの監視、展開、管理を行うことで、さらに管理作業の省力化を進めることができます。カスタマイズ可能なビューと実用的なワークフローにより、セキュリティ状態をすぐに把握し、感染場所を特定できます。システムの隔離、不審なプロセスの停止、データ送信のブロックにより、脅威の影響を防ぐことができます。さらに、1か所ですべてのエンドポイント、McAfee製品の機能を管理できます。130を超えるMcAfee以外のセキュリティ ソリューションも管理できます。

機能	利点
プロアクティブな脅威検出 / 対応 (MVISION Insights)	▪ 業界や地域などの特性に基づいて潜在的な脅威を予測して事前に検出します。 ▪ 潜在的脅威への対策ができているかセキュリティ体制を評価し、改善のためのアドバイスを提供します。 ▪ プロアクティブな対策で攻撃を事前に回避します。
Real Protect	▪ 機械学習により動作の分類を行います。これにより、ゼロデイ脅威をほぼリアルタイムで検出し、有効な脅威インテリジェンスを提供します。 ▪ 行動分類の精度を自動的に向上させて行動を識別し、さらに将来の攻撃の識別に向けてルールを追加します。
標的型攻撃からのエンドポイントの保護	▪ エンドポイント保護は標的型攻撃の検出から封じ込めまでをミリ秒レベルで実行します。 ▪ McAfee Threat Intelligence Exchangeが複数の情報源からインテリジェンス情報を収集します。これにより、複数のセキュリティ コンポーネントが相互に通信を行い、新たに発生する脅威や複雑な攻撃に関する情報を交換できます。 ▪ AMSI と PowerShell のイベント ロギングにより、ファイルレスの攻撃やスクリプトベースの攻撃を検出し、阻止することができます。
インテリジェントで適応型のスキャン	▪ 信頼されたプロセスはスキャンせず、不審なプロセスやアプリケーションを優先することで、パフォーマンスと生産性を向上します。 ▪ 適応型の動作スキャンにより、不審なアクティビティをモニタリングし、エスカレーションします。
ロールバック修復	▪ マルウェアが行った変更を自動的にロールバックして、既知の正常な状態に復元します。
プロアクティブなWebセキュリティ	▪ Web 保護とフィルタリングでエンドポイントを保護し、安全に Web を閲覧できるようにします。
アプリケーションの動的隔離	▪ アプリケーションの動的隔離 (DAC) でランサムウェアやグレイウェアを阻止して被害を未然に防ぎます。[2]
高度なネットワーク攻撃を阻止	▪ 統合ファイアウォールでは McAfee GTI のレピュテーション スコアを使用してボットネット、DDoS 攻撃、高度な持続型脅威、不審な Web 接続からエンドポイントを保護します。 ▪ ファイアウォールにより、システムの起動時に送信トラフィックのみが許可されます。エンドポイントが社外のネットワークに接続しているときもエンドポイントを保護します。
Story Graph	▪ 感染場所、発生理由、脅威の持続期間をすぐに確認できます。脅威を正確に把握し、迅速な対応が可能になります。
複数の選択肢がある集中管理機能 (McAfee ePOプラットフォーム)	▪ 優れた集中管理機能により、可視化が強化されます。セキュリティ機能を一元管理できるので、管理作業を効率的に行い、コストを削減できます。
オープンで拡張可能なエンドポイント セキュリティ フレームワーク	▪ 統合アーキテクチャにエンドポイント保護機能を加えることで、保護能力を強化できます。 ▪ これにより無駄な作業をなくしプロセスを最適化して運用コストを削減します。 ▪ 他の McAfee 製品やサードパーティ製品とシームレスに統合して、隙のないセキュリティを提供します。

表 1. 主な機能と利点

サイバー脅威を未然に防ぐ

McAfee Endpoint Securityは、インテリジェンス、連携した防御機能、複雑な環境を簡単に管理できるフレームワークを提供します。攻撃者よりも優位に立つために必要な機能がすべて揃っています。第三者が検証した強固で効率的なパフォーマンスと効果的な検出能力を備えれば、ユーザーを保護して、生産性を高め、なによりも安心を得ることができます。

McAfee は、エンドポイント セキュリティのマーケット リーダーとして、強力な保護策と効果的な管理手法を組み合わせることで、多大なリソースを投じることなく迅速に問題を解決する、先を見据えた対策を提供します。

簡単な移行

McAfee ePO ソフトウェア、McAfee VirusScan® Enterprise、McAfee® Agent の最新バージョンを使用している環境では自動移行ツールが利用でき、既存のポリシーを 20 分弱で McAfee Endpoint Security に移行できます。[3]

McAfee Endpoint Security には、次のようなメリットもあります。

- ゼロインパクトのユーザー スキャンでユーザーの生産性を維持
- Story Graph でフォレンジック データを表示し、調査を容易にしてポリシーを強化
- マルウェアによる変更を自動的にロールバックし、システムを正常な状態に維持
- MVISION Insights で優先度の高い脅威に関するプロアクティブな情報と脅威対策ガイダンスを提供
- 管理対象のエージェントとスキャンを削減して作業負荷を軽減
- 相互連携するセキュリティで高度な脅威を阻止
- その他の高度脅威及びエンドポイント検出/対応 (Endpoint Detection and Response: EDR) ソリューションに対応可能な次世代フレームワーク

詳細情報

McAfee Endpoint Security の詳細については、こちらをご覧ください。

McAfee Endpoint Security が連携する McAfee 製品ポートフォリオについては、次をご覧ください。

- MVISION Endpoint
- MVISION 製品ファミリ
- McAfee Threat Intelligence Exchange
- MVISION EDR
- McAfee ePolicy Orchestrator
- MVISION Insights

1. ほとんどの McAfee エンドポイント スイートで利用できます。詳細については、営業担当者にお問い合わせください。
2. 同上
3. 移行の所要時間は、既存のポリシーと環境の状況によって異なります。

マカフィー株式会社　www.mcafee.com/jp
東京本社　〒 150-0043　東京都渋谷区道玄坂 1-12-1　渋谷マークシティウエスト 20F　TEL：03-5428-1100 (代)　FAX：03-5428-1480
西日本支店　〒 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