McAfee Embedded Control

重要なデバイスのシンプルな防護

現在サイバー攻撃が集中しつつあるのは非従来型のエンドポイントで、これらは装着型のフィットネス トラッカーから、データの生成や分配をつかさどる重要なコネクテッド センサーまで多岐にわたります。コネクテッド デバイスの数が増えるにしたがってマルウェアやサイバー攻撃のリスクも増えていきます。McAfee® Embedded Control は、承認済みのアクセスだけを許可し、未承認の実行ファイルをブロックしてシステムの完全性を確保します。

組み込みシステムに市販のオペレーティング システムが採用され、セキュリティ リスクが増加しています。McAfee Embedded Controlは組み込みシステムのセキュリティに特化したソリューションです。McAfee Embedded Controlはオーバーヘッドが少なく、場所をとらないソリューションです。アプリケーションに依存することもなく、配備後も手間はかかりません。McAfee Embedded Controlは、商用のオペレーティング システム上にシステムを構築し、ブラックボックスにしているので、クローズされた専用のオペレーティング システムのように見えます。ディスク上の未承認プログラムやメモリーに挿入された未承認コードの実行をブロックし、未承認の変更を阻止します。このソリューションを使用すると、製造メーカーはリスクを増大させずに市販のオペレーティング システムを安心して利用できます。また、現場でのシステムの使用方法を管理できます。

整合性の保証

実行プログラムの制御

McAfee Embedded Controlは、マカフィーの動的ホワイトリストに登録されたプログラムにのみ実行を許可します。他のプログラム（exe、dll、スクリプト）は未承認と見なされ、実行がブロックされます。この実行失敗はデフォルトでログに記録されます。これにより、ワーム、ウイルス、スパイウェアなどのマルウェアの実行を阻止できます。

メモリー制御

メモリー制御では、実行中のプロセスを乗っ取りなどの攻撃から保護します。実行中のプロセスに侵入を試みる不正なコードはブロックされ、ログに記録されます。バッファー オーバーフロー、ヒープ オーバーフロー、スタック オーバーフロー、類似したエクスプロイトによるシステムの乗っ取りを防ぎ、ログに記録します[1]。

主な特長

- 組み込みデバイスで実行される処理を制御し、これらのデバイスのメモリーを保護することでセキュリティ リスクを軽減します。
- アクセスを管理し、制御を維持し、サポートコストを削減できます。
- 選択的な実装が可能です。
- 配備後の手間がかかりません。
- デバイスのコンプライアンスと監査をすぐに実施できます。
- リアルタイムな可視性を提供します。
- 包括的な監査を実施します。
- 変更記録を検索できます。
- 閉じた環境で調整できます。

McAfee GTIとの統合: エアギャップ環境でグローバルな脅威に対応するスマートな方法

McAfee® Global Threat Intelligence (McAfee GTI) はマカフィー独自の技術です。世界中に存在する数百万台のセンサーを利用して、ファイル、メッセージ、送信者のレピュテーションをリアルタイムで追跡します。クラウド ベースの情報を使用してコンピューター上のすべてのファイルのレピュテーションを確認し、ファイルを正常、不正、未知のいずれかに分類します。McAfee　GTIとの統合で、ホワイトリストに誤って登録されたマルウェアを確認できます。GTIのレピュテーションはインターネット経由だけでなく、McAfee® ePolicy Orchestrator® (McAfee ePO™)環境でも確認できます。

変更管理

McAfee Embedded Controlは変更をリアルタイムで検出します。変更元を確認し、変更が正しい対象に実施されているかどうか検証します。また、変更の監査証跡を利用して、承認された方法以外の変更を禁止します。

McAfee　Embedded　Controlを使用すると、承認された変更方法を指定して変更管理プロセスを実施できます。変更の適用者、変更の許可に必要な認証情報、変更対象を制御できます。たとえば、特定のファイルまたはディレクトリにのみ変更を許可します。また、変更を適用するタイミングも制御できます。たとえば、週の特定の時間にのみMicrosoft Windowsの更新を許可します。

対象のシステムに変更を適用する前に、変更内容を検証します。このモジュールを有効にすると、ソフトウェアに対する更新を制御できます。

リアルタイムの変更追跡モジュールは、システムの状態に対する変更をログに記録します。コード、設定、レジストリの情報も記録します。変更が発生すると、変更イベントがリアルタイムに記録され、集計とアーカイブを行うためシステム　コントローラーに送信されます。

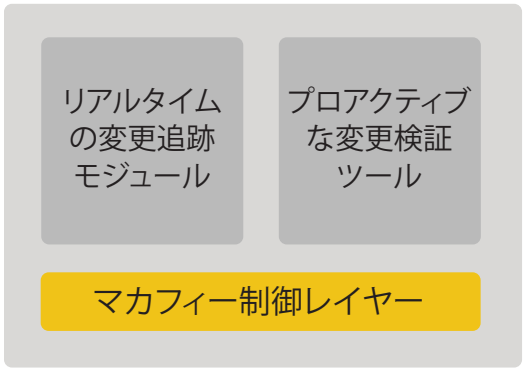

図1. McAfee制御レイヤー。

システム コントローラー モジュールはシステム コントローラーとエージェント間の通信を管理し、エージェントから収集した変更イベントの情報を集計・保存します。

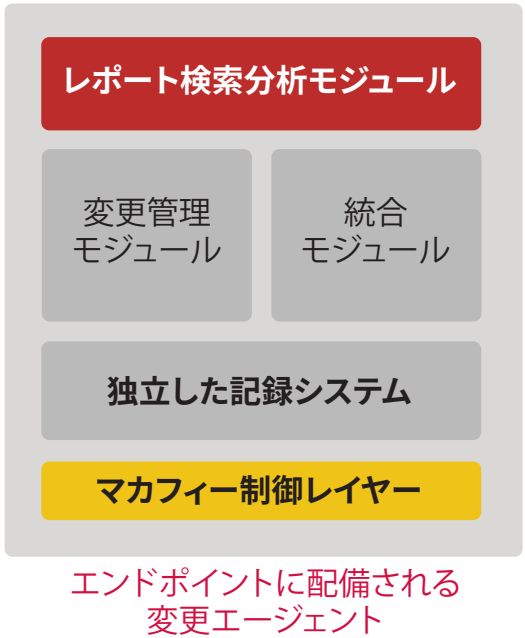

図2. レポート、検索、分析モジュール。

監査とポリシー対応

McAfee® Integrity Controlのダッシュボードとレポートを使用すると、コンプライアンス対応を簡単に行うことができます。ユーザーと管理者はWebベースのMcAfee ePOコンソールを使用してダッシュボードとレポートを確認できます。

McAfee Embedded Controlでは、承認済みと未承認のアクティビティを記録し、統合環境でコンプライアンス対応と監査をリアルタイムで行うことができます。

マカフィーの組み込みセキュリティについて

マカフィーの組み込みセキュリティ ソリューションにより、組み込みシステムの製造メーカーはサイバー脅威や攻撃から自社の製品とデバイスを保護することができます。マカフィーのソリューションは、アプリケーション ホワイトリスト、ウイルス対策、マルウェア対策、デバイス管理、暗号化、リスクとコンプライアンスなど、様々な技術を使用しています。これらの技術のすべてで業界最高のMcAfee Global Threat Intelligenceを利用しています。マカフィーのソリューションは、デバイスとそのアーキテクチャの設計要件に合わせて調整できます。

機能	説明	利点
システム整合性の保証		
外部の脅威に対する保護	承認されたコードにのみ実行を許可します。未承認のコードはメモリーに展開されません。承認済みのコードの改ざんを防止します。	▪ 緊急パッチの適用がなくなります。パッチの数が少なくなり、頻度も少なくなります。パッチの適用前に十分なテストを実行できるので、パッチの適用が難しいシステムのセキュリティ リスクを軽減できます。 ▪ ゼロデイ攻撃、ポリフォーミック型攻撃（ワーム、ウイルス、トロイの木馬などのマルウェアによる）、コード インジェクション（バッファー オーバーフロー、ヒープ オーバーフロー、スタック オーバフローなど）のセキュリティ リスクを軽減します。 ▪ 承認されたファイルの整合性が維持されるので、本稼動環境のシステムの状況を「既知の確認済み」に維持できます。 ▪ 計画外のパッチを制限し、緊急のリカバリでも運用コストを押さえ、システムの可用性を維持できます。
内部の脅威に対する保護	ローカル管理者のロック機能を使用すると、認証キーの入力がない限り、管理者であっても保護対象システムでの実行対象を変更できなくなります。	▪ 内部の脅威を阻止します。 ▪ 本稼働環境の組み込みシステムで実行されている処理をロックします。管理者による変更もブロックします。
高度な変更管理		
製造元による更新のみを許可	現場の組み込みシステムに未承認の更新が実施されないようにします。	▪ 未承認の変更は現場のシステムに適用されません。未承認のシステム変更を阻止し、システムの停止やサポート コールの発生を防ぎます。 ▪ 製造元は、すべての変更管理を自身で行うか、信頼できるエージェントに変更管理を依頼するかを選択できます。
承認プロセスで発生した変更の確認	承認変更プロセス以外で発生した変更は実施されません。	▪ 運用の混乱やコンプライアンス違反を回避するため、財政的に厳しい時期や業務のピーク時に未承認の変更が実行されないようにします。
承認済み更新プログラム	承認済みの更新プログラム（ユーザーまたはプロセス）以外は本稼動システムに変更を行うことができません。	▪ 未承認の変更は本稼動システムに適用されません。
リアルタイムの監査とコンプライアンス		
リアルタイムの変更追跡	組織内で変更が発生するとすぐに変更を追跡します。	▪ 未承認の変更は本稼動システムに適用されません。
包括的な監査	システム変更に対してすべての変更情報（変更者、対象、場所、時間、方法）を収集します。	▪ すべてのシステム変更に対して正確で詳細な情報が記録されます。
変更元の識別	変更者、変更後に発生したイベント、影響を受けたプロセス/プログラムなど、変更に関するすべての情報が関連付けられます。	▪ 承認済みの変更かどうかを検証します。未承認の変更を迅速に識別できるので、変更の成功率が向上します。

機能	説明	利点
ランニング コストの削減		
配備後の手間がかからない	ソフトウェアのインストールは数分で終わります。初期設定やセットアップも不要です。設定作業を定期的に行う必要はありません。	▪ すぐに利用できます。インストール後すぐに機能します。保守に手間がかかりません。セキュリティ ソリューションの構成費用を抑えたい企業には最適な選択肢です。
ルール/シグネチャ/アプリケーションに依存しない	ルールやシグネチャ データベースに依存しません。学習期間も不要です。すべてのアプリケーションですぐに利用できます。	▪ サーバー ライフサイクルで管理者の作業が少なくなります。 ▪ OPEXを抑えながらサーバーを保護できます。 ▪ ルールやポリシーの品質にかかわらず、効率的な処理を行います。
最小限のフットプリントとランタイム オーバーヘッド	使用するディスク容量は20 MB未満です。アプリケーションの実行を妨げることはありません。	▪ パフォーマンスやストレージ要件に影響を及ぼすことなく、ミッションクリティカルな本稼動システムに配備できます。
誤検知と非検知の回避	未承認のアクティビティだけが記録されます。	▪ 正確な結果が記録されるので、毎日または毎週行うログ解析の時間が劇的に短縮されます。他のホスト侵入検知ソリューションと比べてOPEXが減少します。 ▪ 管理作業を効率的に行えるので、OPEXが減少します。

次のステップ

詳細については、**www.mcafee.com/jp/solutions/embedded-security/embedded-security.aspx** をご覧ください。また、お近くの弊社営業窓口までお問い合わせください。

1. Microsoft Windowsプラットフォームでのみ使用可能

〒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