McAfee Integrity Control

POSシステムを未承認のアプリケーションと変更から保護

McAfee® Integrity Control™は、業界をリードするホワイトリストおよび変更管理テクノロジーを組み合わせて、POSシステム、ATM、キオスクなどの専用システム上で信頼できるアプリケーションのみに実行を許可するソフトウェアです。McAfee Integrity Controlソフトウェアは、継続的な変更検出機能とともに、未承認の変更の試みをプロアクティブに防止する機能を提供します。McAfee Integrity Controlソフトウェアは、信頼ソースモデルを活用するため、システムがロックダウンされている場合でも、承認されているソースからのソフトウェア更新は許可されます。

主な利点

変更を包括的に把握して制御

専用システム全体の重要なファイルとディレクトリーに対する変更を継続的に追跡

ダイナミックなホワイトリストによって所有コストを削減

専門システム上のデータベース、ルール、更新の手動管理を排除

変更ポリシーの施行

承認済みのポリシーとプロセスに従って変更を実施

透過的な運用

専用デバイスへの追加のオーバーヘッドはなし

未承認のアプリケーションと変更の試みを防止

McAfee Integrity Controlソフトウェアを使用することで、IT組織は運用のためのオーバーヘッドを余計に増やすことなく、POSインフラストラクチャー上で承認済みのソフトウェアのみを稼働させることができます。McAfee Integrity Controlソフトウェアは、重要なシステムの整合性を低下させる可能性がある不正で脆弱な、かつ悪質なアプリケーションを簡単に防止できます。このソリューションは、動的なホワイトリスト信頼モデルを利用してシステムを保護しますが、管理者によって事前に定義された信頼ソースによる承認済みの更新や変更は許可します。このモデルでは、データベースやルール、更新作業が不要なため、他のホワイトリストテクノロジーで要求される、費用のかかる手作業によるサポートは必要ありません。

McAfee Integrity Controlソフトウェアは、ポリシーに従っていない未承認の変更を事前に防止できる変更管理テクノロジーも活用します。この高度な保護機能はポリシーと直接リンクされており、変更を変更元、時間枠、承認済み変更チケットと照合することができます。この機能が有効なシステム上では、ポリシーに従っていない変更の試みは防止され、ログに記録され、管理者にアラートが送信されます。結果として、変更に起因するシステムの停止とコンプライアンス違反を大幅に削減できます。

ファイルの整合性と変更の監視

McAfee Integrity Controlソフトウェアは、ファイル整合性監視（FIM）を利用してファイルとディレクトリーのコンテンツと権限の変更を監視します。McAfee Integrity Controlは、環境のセキュリティテストと検証や、PCIDSS（クレジットカード業界データセキュリティ基準）で規定されている重要なコンプライアンス要件への対応に欠かせない継続的なFIM機能を提供します。McAfee Integrity Controlソフトウェアは、ユーザー、変更に使用されたプログラムを含め、すべての変更に関する包括的な情報を提供します。

ePOを通じた一元的な導入と管理

McAfee ePolicy Orchestrator®（McAfee ePO™）プラットフォームとのシームレスな統合により、McAfee Integrity Controlエージェントの導入、管理、レポート作成を簡単に行うことができます。単一のMcAfee ePOコンソールで専用デバイスのセキュリティとコンプライアンスを一元管理できるため、所有コストも削減できます。そのため、IT組織のハードウェア、トレーニング、および運用コストを節約しながら、この機能が有効化されたATM、キオスク、POSシステムのポリシーと保護を統一的に管理することができます。また、McAfee ePOプラットフォームとの統合を通じて、2つの異なるシステムでデータを管理する必要がなくなります。

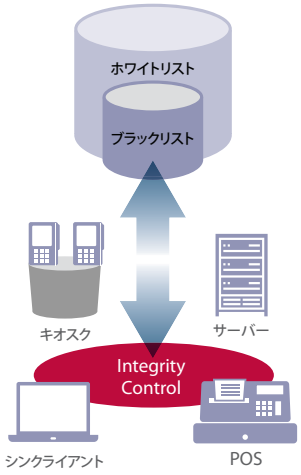


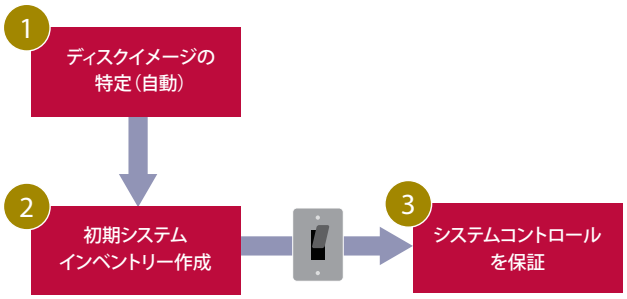
図1. McAfee Integrity Controlは、キオスクやPOS端末などの専用デバイス、レガシープラットフォームに保護レイヤーを拡張し、お客様のリスクを大幅に低減します。

導入効果

専用システムの制御性の向上 — 小売、金融サービス、医療などの規制が厳しい産業では、POS端末、ATM、医療画像システムなどのデバイスによって重要な機能が遂行され、機密性が高いデータが保管されています。McAfee Integrity Controlソフトウェアは、専用のCPUやメモリーリソースを使用して専用の機能を実行するシステムの保護レイヤーの拡張に最適な製品です。このソリューションは、オーバーヘッドが低くフットプリントが小さいため、システムのパフォーマンスに影響を与えません。また、起動時と動作時のオーバーヘッドも最小限に抑えられます。ネットワークアクセスを必要としないスタンドアロンモードでも、同様の効果を発揮します。

PCI DSSコンプライアンスの達成と維持 — ATM、POS端末、キオスクといった多くのPOSシステムは、PCI DSSコンプライアンスを順守する必要があります。McAfee Integrity Controlソフトウェアは、変更されたサーバー、変更が発生した時間、変更を実施したユーザー、変更方法、変更対象（ファイル内のコンテンツ）、変更の承認の有無など、POSインフラストラクチャー全体にわたる変更に関する情報を継続的に提供します。POS環境に対するこの詳細な可視性を提供するのは、McAfee ePOプラットフォームです。この高度な可視性により、IT組織は監査担当者に対してPCI DSSコンプライアンスを実証しながら、POSシステムのセキュリティを継続的に検証することができます。

サービス可用性の改善 — 専用デバイスのダウンタイムの多くは、未承認または未検証の変更によって発生しています。こうしたデバイスの復元までに必要な時間の大半は、変更内容の特定に費やされています。その原因は、実際の変更活動と変更管理プロセスとの間に差異が生じていることです。IT組織は、変更管理におけるこの差異が原因で、手作業で変更をコントロールし、変更のコストと変更に関係するシステム停止を最小限に抑えなければなりません。McAfee Integrity Controlソフトウェアを使用することで、IT組織はこの変更コントロールの差異を解消し、専用デバイスのサービスの可用性を高めることができます。McAfee Integrity Controlソフトウェアでは、McAfee ePOプラットフォームを通じて継続的に変更を追跡できます。また変更ポリシーを選択的に施行し、不明な変更によって問題が発生する前にこのような変更を防止できます。McAfee Integrity Controlソフトウェアを使用することで、可用性低下を引き起こすインシデント（平均故障間隔によって測定）数の削減と、インシデント当たりの回復時間（平均復旧時間によって測定）の短縮が可能になります。



動的なホワイトリストの動作

1. システム上で実行されているすべてのソフトウェアを自動的に完全に検出
2. 非常に軽量な実行時システムによる事前計算
3. システム保守中に、完全に自動的にコード許可をコントロール

McAfee マカフィー株式会社
www.mcafee.com/jp

●製品、サービスに関するお問い合わせは下記へ

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

名古屋営業所　〒460-0002 愛知県名古屋市中区丸の内3-20-17 中外東京海上ビルディング3F
TEL:052-954-9551(代) FAX:052-954-9552

福岡営業所　〒810-0801 福岡県福岡市博多区中洲5-3-8 アクア博多5F
TEL:092-287-9674(代) FAX:092-287-9675

MCABRF-SCIC-1008-MC