

## McAfee Change Control ソフトウェア

未承認の変更から継続的に企業活動のコンプライアンスを保護



多くの IT 組織では、承認および文書化された変更と、実際の変更活動との間に差異が生じています。複数のコンプライアンス要件に準拠する必要がある企業は、ファイルと構成の変更を監視する機能、および変更許可ポリシーを一元的に施行して徹底する機能があれば、可用性を高めると同時に、コンプライアンスも向上させることができます。McAfee® Change Control ソフトウェアは、単一の管理プラットフォームである McAfee ePolicy Orchestrator® (ePO™) と緊密に統合されており、ePO コンソールを利用して変更イベント通知やその優先順位の指定を含む変更ポリシープロファイルを設定できるため、効率的に管理することができます。マカフィーは、変更防止機能を通じて、重要システムコンポーネントのファイルや構成設定を未承認の変更から完全に保護します。

今日、多くの IT 組織は、変更管理システムやサービスデスクのようなプロセスの自動化ツールに費用を投じています。しかし、実際の変更活動と、文書化されている変更管理プロセスやポリシーとの間には差異が生じています。IT 組織は、この変更の差異が原因で、監査への対応やインシデントイベントの調整のために、実際のシステムレベル変更と変更作業要求やトラブルチケットを手作業で照合しなければならず、多大な労力を費やしています。さらに、未承認あるいは未検証のまま、変更が場当たり的に行われることも珍しくはありません。その結果、システムセキュリティ構成が低下し、システムが企業ポリシーから逸脱したり、サーバーのパフォーマンスや可用性に影響が及ぶことがあります。McAfee Change Control ソフトウェアは、集中管理型または事前定義された信頼モデル(変更可能な時間枠、変更元、承認済みユーザー)を利用して承認された変更を実施し、変更のコストを最小限に抑えるとともに、継続的にファイルの整合性を監視します。企業は、McAfee ePO 管理コンソールを使用して、保護対象のシステムのタイプや範囲を柔軟に調整することができます。また、変更アラートの対象になるファイル、ディレクトリー、構成、およびアラートの優先順位も決定できます。最も一般的なサーバーオペレーティングシステムとエンタープライズアプリケーション向けに開発されたデフォルトプロファイルが用意されていますので、一からプロファイルを作成せずに重要なコンポーネントを監視することができます。さらに、信頼できるソース以外が開始したファイル、ディレクトリー、構成への変更を防止するポリシーを施行して、単純な

監視よりも保護を強化する新しいプロファイルもいつでも有効化することができます。変更防止ポリシーは、きめ細かい調整が可能です。たとえばネイティブアプリケーションには中断なしで継続的なファイルの更新を許可し、他のすべてのアプリケーションやユーザーに対しては McAfee Change Control ソフトウェアの読み取り/書き込み防止機能を利用して、ファイルの変更だけでなく、読み込みも防止することができます。McAfee Change Control ソフトウェアは、分散されたりリモートのロケーションで行われる変更を継続して検出する機能、および望ましくない変更をブロックして変更を防止する機能を提供します。McAfee Change Control ソフトウェアによって、IT 組織は変更管理を制御することが可能になり、実際の変更活動と、文書化された変更の差異を解消することができます。このソリューションを使用すれば、コンプライアンスのために PCI および SOX 管理を自動化することも、変更に関連したシステム停止を防止してサービスの可用性の向上や、ITIL (Information Technology Infrastructure Library) 導入の加速を図ることも簡単です。McAfee Change Control は、簡易で操作性は高くオーバーヘッドが低い、さらに幅広いサーバーハードウェアプラットフォームに導入できるソリューションです。

## 継続的な変更管理

McAfee Change Controlは、システム状態のスナップショットを作成して比較するスキャンベースのソリューションとは異なり、定義済みの変更管理プロファイルに基づいて、試行されているすべての変更をリアルタイムで追跡して正当性を検証します。

McAfee Change Controlソフトウェアと連携して動作するMcAfee Change Reconciliationは、サーバーに実施された変更と、既存のチケットシステムに文書化されている変更チケットを関連付けます。McAfee Change Reconciliationは、HP Service ManagerやBMC Remedyなどの主要な変更管理システムと統合できます。また、BMC Atrium、HP UniversalCMDBなどの主要な構成管理データベース（CMDB）とも統合します。トラブルチケット、または作業チケット内で実施された変更の詳細は、まとめてチケットシステムに組み込まれるため、企業ではワークフローだけでなく、実施された作業のシステムレベルの詳細も追跡することができます。

またMcAfee Integrity Monitorソフトウェアは、McAfee Change Controlソフトウェアの機能を補完し、PCIDSSを含む多くのコンプライアンス基準で指定されているデータベースとネットワークデバイスの監査証跡の要件にすばやく簡単に対応する手段を提供します。管理者は、McAfee ePO管理コンソールのレポート機能を利用して、サーバー、アドオンデータベース、ネットワークデバイスへのすべての変更を表示し、コンプライアンスポリシー違反の発生箇所を確認することができます。このソリューションは、ファイルが不適切に変更され、また元に戻されるような一時的な違反を特定して警告するほか、変更の正確な時間など、すべての変更の具体的な詳細情報を記録します。

## エンタープライズソリューション

### PCI DSSコンプライアンスの達成と維持

小売業者とサービスプロバイダーがPCI DSS（クレジットカード業界セキュリティ基準）コンプライアンスを達成するには、12のカテゴリーにわたるおよそ180の要件を満たす必要があります。しかし、PCIDSS要件の中でも、ファイル整合性監視と監査証跡の使用を規定しているカテゴリー10および11への対応が最も難しいことが判明しており、最近の調査でも、最も満たされていない要件であるという結果が出ています。この要件への対応が困難なのは、既存のツールには、リソースを消費するシステムスキャンを通じて変更を検出する「定期的な」ファイル整合性監視機能しか装備されていないためです。

ITインフラストラクチャーに対する絶対的なコントロールを提供するMcAfee Change Controlソフトウェアにより、小売業者やクレジットカード取引を処理する企業は、効果的かつコスト効率よく、難しいPCI要件を満たし、PCIコンプライアンスを実証できるようになります。

マカフィーは、あらゆる規模の小売業者がPCI DSSのセクション1、10、および11に規定されているファイル整合性監視と監査証跡の要件を簡単にコスト効率よく満たすことができるように、McAfee Change ControlソフトウェアおよびMcAfee Integrity Monitorソフトウェアを提供しています。世界の主要な認定監査機関（QSA）は、包括的なPCIコンプライアンス戦略に欠かせない要素として、これらのソリューションを認定し、推奨しています。

### SOX法とその他のコンプライアンス要件をサポートするIT管理フレームワーク

米SOX法（米国企業改革法）の制定によって、企業がバナンスに抜本的な変化がもたらされました。現在企業は、平均で4つのコンプライアンス基準に準拠しなければならないと言われています。企業が複数のコンプライアンスの必要性に直面し、取り組んだ結果、コンプライアンスは一時的なプロジェクトではなく、ビジネスプロセスとセキュリティの可視性と説明責任を確保するために持続していかなければならないことが明らかになりました。このような厳格なコンプライアンス要件を満たすために、多くの企業はコンプライアンスポリシーを導入していますが、こうしたポリシーは手作業で管理されるためエラーが発生しやすく、多くのリソースも要求されます。

McAfee Change Controlソフトウェアは、McAfee Change Reconciliationソフトウェアを使用してセルフサービス型の自動IT管理フレームワークを構築することによって、多数のお客様のSOX法コンプライアンスの複雑な課題解決を支援しています。このフレームワークでは、単一のレポートシステムでコンプライアンス状況の検証に必要な情報を取得できます。マカフィーが提供する継続的な変更検出機能と自動化された非常に正確な変更調整機能によって、承認内容に対して変更を自動的に検証できます。プロセスに従っていない変更（緊急の修正など）は自動的に記録、調整されるので、監査が容易になります。SOX法監査のためにMcAfee Change Controlソフトウェアを使用しているお客様は、リスクの低減とコスト削減の2つ面で大きなメリットを享受しています。多くの場合、最初に得られるメリットは、従来の手作業だったコントロールの自動化です。2つ目のメリットは、環境ファブリック内にコントロール機能が組み込まれたことが監査担当者を実証され、コントロールセットが合理化、削減されることです。

### セキュリティとコンプライアンスの最適化

中規模および大規模組織の大半は、セキュリティおよびコンプライアンスを効率化する手段を模索しています。変更がコントロールされている環境でなければ、自動化および効率化ツールは変化するインフラストラクチャー上で稼働しているのも同然であるため、これらのツールへの投資から期待ほどの利益は生まれません。特にプロジェクトは、大規模で複数の段階を踏んで実施していくので、ビジネスにとってのROIの実証がプロジェクトの成功を妨げる大きな文化的要因となっています。お客様は、McAfee Change Controlソフトウェアを使用することで、ビジネスにもたらすROIを実証するまでの期間を飛躍的に短縮するとともに、ITの説明責任能力を大幅に高めることができます。導入されたMcAfee Change Controlソフトウェアは、継続的にコントロールされた環境を維持し、自動化を実現します。お客様は、変更に対する可視性を確保するとともに、一元管理コンソールであるMcAfee ePO管理プラットフォームを利用して、ローカルおよび分散サーバーに即座に効果を発揮する変更ポリシーを選択的に施行することができます。



[www.mcafee.com/jp](http://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