■ Change Control 導入事例 —

株式会社インターネットイニシアティブ

「PCI DSS対策を施行されるお客様に向けて、IIJ金融システム事業部では、PCI DSS要件11.5のファイル整合性監視ツールとして、McAfee Change Controlを選択しました。採用の決め手は、バッチ型スキャンでの変更検知ではなく、すべての変更をリアルタイムにロギングできること、また、将来的な変更防止まで含めた機能拡張性でした」

McAfee Change Controlの監査ログも監視するIIJのモニタリング&オペレーションサービス

— まず、PCI DSS対策[1]を施行されるお客様に向けて、IIJが展開されているMcAfee Change Controlの標準的な導入構成について、お聞かせください。

McAfee Change Controlは、PCI DSS要件11.5「ファイル整合性の監視」[2]を実現するセキュリティツールです。具体的な実現機能としては、ファイル、ディレクトリー、レジストリーに対する変更をリアルタイムに検知します。また、いつ、誰が、どのプログラムを介して、何を変更したかの監査ログが取得できます。

1 クレジットカード業界で策定された、カード会員データを取り扱う事業者向けのセキュリティ対策・遵守基準。施行対象は、イシュア（カード発行会社）、アクワイアラ（加盟店管理会社）、そして、加盟店（小売店等の対面取引事業者、ECショップ等のネット取引事業者）、および、加盟店等のデータ処理を代行するプロセッサやサービスプロバイダーとなります。

2 ファイル整合性監視ソフトウェアを導入し、重要なシステムファイル、コンテンツファイルに対する不正・未承認の変更を管理者に通知すること。また、重要なファイルの比較を週次で実施すること。（出展：PCI Security Standards Council, LLC.）

株式会社インターネットイニシアティブ

企業プロファイル

株式会社インターネットイニシアティブ（以下、IIJ）は、1992年、日本で初めてインターネットの商用化を目的とした会社として設立されました。以来、卓越した技術力とネットワークで、社会基盤としてのインターネットを支えています。インターネット等のネットワークサービスの提供、ネットワーク・システムの構築および保守・運用、通信機器の開発および販売を行っています。1,000種類以上の豊富なバリエーションから選択可能で、HaaS/IaaSからSaaSメニューまでの幅広いニーズに対応したクラウドサービスとして、IIJ GIO（ジオ）サービスを展開しています。

金融システム事業部について

IIJ金融システム事業部では、外国為替証拠金取引(FX)システムのASP型ソリューション「IIJ Raptorサービス」を提供するほか、ネットワークやデータセンターといったサービス基盤と10年来培ったノウハウを活用した運用基盤をベースに、金融業界のネットビジネス、および基幹システムのITインフラのシステムインテグレーション＆アウトソーシングサービスを提供しています。

IIJでは、サーバーのシステム監視、オペレーション支援をはじめとする包括的なモニタリング＆オペレーションサービスも提供しており、McAfee Change Controlの監査ログも、ログモニタリングサービスに統合しています。

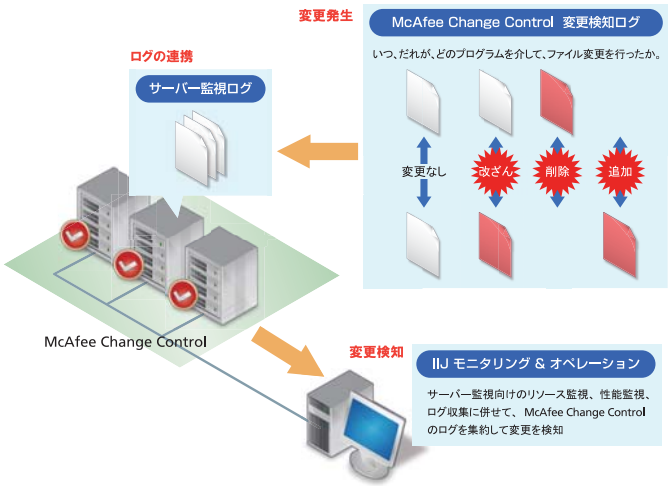

図1：IIJでのMcAfee Change Controlの標準的な提案構成

豊富なシステム運用実績を持つIIJだからできる、実運用重視のPCI DSS対策支援

— ツール選定・構築だけでなく、オペレーション支援を含めた運用面まで関わられている背景をお聞かせください。

金融システム事業部
プロフェッショナルサービス部
プロフェッショナルサービス1課
渡邉勇太 氏

PCI DSS対策では、セキュリティの実装のみならず、ポリシー実装後の運用・モニタリングが極めて重要視されます。PCI DSS認証取得までの流れとして、QSA/ASVの監査事前に、現状分析と改善策の洗い出しを目的としたコンサルテーションが利用されます。この段階で、PCI DSS対策における運用面の重要性に気づかれるお客様が多いようです。

IIJとしては、基盤技術分野で蓄積してきた高度な技術力をもって、データセンターやクラウドサービスを軸としたITインフラのインテグレーションから各種監視・運用サービスまでをワンストップで提供しています。

さらに、IIJは、日本初オンライン専業証券システムの構築運用で培ったノウハウを元に、多くの銀行などの金融機関やFX事業者のシステムインテグレーションの実績があります。

運用までを見据えた製品選定、導入構築、そして、場合によりますが、運用アウトソーシングまでを任せたいというお客様のニーズに対して、豊富なシステム運用実績を持つIIJだからこそ、お応えできていると考えています。実際には、メインフレームで構築されたレガシー・システムからのダウンサイジング、システム刷新に併せて、PCI DSS準拠も完了しておこうというイシュア、アクワイアラの動きも加速しており、IIJにて導入構築支援をしています。

不正アクセス防止までの拡張性を重視する場合、McAfee Change Controlが最適

— さて、PCI DSS要件におけるファイル整合性監視ツールの推奨として、McAfee Change Controlを選択するにあたり、どのような製品比較を行われましたか。

実は、PCI DSS要件11.5のファイル整合性監視に基づく要件だけでは、McAfee Change Controlと他社製品での優劣はつけられませんでした。お客様の導入目的をより踏み込んで検討した結果、ツールへの期待は改ざん検知だけでなく改ざんの未然防止であると考え、単なるファイルの事後的な変更検知のレベルではなく、よりリアルタイムでの変更検知、さらには、変更防止への拡張性が望まれると捉えました。PCI DSS要件を満たすとともに、将来的により厳格なファイルアクセス制御が可能なツールが必要という結論に至りました。

その結果、McAfee Change Controlは、監査ログのリアルタイム性、変更検知から防止までの拡張性の点、さらには価格体系や導入構成の柔軟性についても優れていると判断し、採用しました。

すべての変更ログをリアルタイムに取得

— 監査ログのリアルタイム性について、McAfee Change Controlと他社製品の比較内容、そして、その必要性について、ご説明頂けますか。

まず、他社製品での変更検知機能では、予めスケジュール化されたタイミングにて、ファイル構成のスナップショットを取得し、前回のスキャンとの構成比較により、変更の有無を判断しています。このような機能設計では、仮に、各々のスキャンタイミングの間に、不正なシステム変更が行われ、且つ、不正アクセス後にシステム構成を元通りにされてしまうと、不正アクセスを見抜けない可能性、懸念が残ります。

McAfee Change Controlの場合、変更が発生したタイミングで変更ログを取得しますので、よりリアルタイムでの変更検知が可能となります。発生した変更ログは漏れなく取得でき、監査証跡の精度が高まります。

不正アクセス・リスクを最少化するための変更防止機能

― 同様に、変更防止機能への拡張性について、如何でしょうか。

金融システム事業部
プロフェッショナルサービス部
プロフェッショナルサービス1課
シニアテクニカルマネジャー
前川陽一 氏

確かに、変更検知の為のスキャンタイミングを増やし、ログレビューの回数を増やせば、よりリアルタイムに近い変更検知ができます。しかし、これに比例して、現場の運用負荷も高まります。また、どれだけリアルタイムに変更検知を行っても、それはあくまで、発生した変更を事後的に把握しているに過ぎません。

お客様が、PCI DSS要件を超えて、さらに不正アクセス防止を強化されたい場合、やはり、変更防止機能の実装が必要になってきます。McAfee Change Controlは変更検知と変更防止の両機能が備わっており、変更防止の設定が行われているファイルへの不正アクセスのトライもログとして取得できます（図2）。

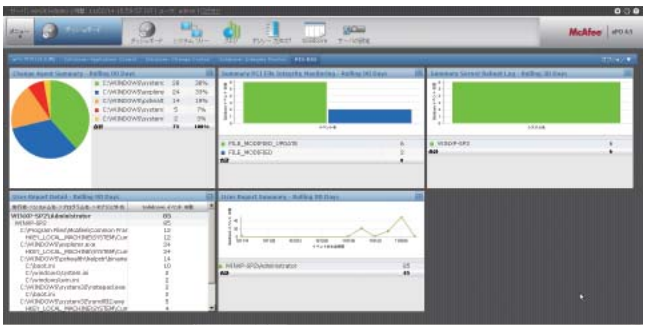

図2：McAfee Change Control ログ画面

変更の検出	適正なシステム運用を実現するため、 リアルタイムに変更を検出します。
監査ログ・データ	いつ、誰が、どのプログラムを介して、 何を変更したかのログ取得を行います。
監査ログ精度	高度化された不正改ざんを検知する為、 一時的な変更も漏らすことなく検出します。
変更防止	プロアクティブなセキュリティ実現のため、 ポリシーに従わない変更をブロックします。

McAfee Change Controlの機能概要

柔軟な導入構成と合理的な製品価格体系

― 価格体系、導入構成についてはいかがでしょうか。

費用対効果を考えた場合、ファイル整合性監視ツールの価格、および、最少構成で必要となる周辺コストも十分に考慮しました。

PCI DSS対策のポイントとして、認証取得が必要なシステム範囲を適切にスコーピングし、対策範囲を限定することによってコストと対策効果のバランスを取ることが大切です。

他社製品の場合は、ファイル整合性監視対象のサーバー数が数台でも有償の管理サーバーとライセンスを購入する必要があるのに対し、McAfee Change Controlは管理サーバーが無い環境でも、監視対象サーバーに導入することが可能です。また、監視対象サーバーの台数が多い場合には、McAfee ePolicy Orchestrator（マカフィー製品の統合管理コンソール）を用いた統合・集中管理が行えますので、導入規模に応じた、構成面での柔軟性が確保できます。また、課金体系として、McAfee Change Controlの場合、監視対象サーバー1台ごとの課金となり、統合管理コンソールによる追加費用は発生しませんので、合理的な価格体系ではないでしょうか。

― そのほかに、考慮された事項があれば、教えてください。

お客様が気にされる導入実績の点でしょうか。確かに、国内において、McAfee Change Controlは後発です。しかし、この点については、セキュリティベンダーとしてのマカフィー社の日本でのプレゼンス、そして、このような製品機能・価格面での比較結果をより重要視しました。その結果として、PCI DSS向けファイル整合性監視ツールとして、当社では、McAfee Change Controlを標準的な推奨製品とすることに決めました。

セキュリティ分野での全体最適・統合運用ソリューションへの期待

— 最後に、McAfee Change Control、および、マカフィーに対する今後の期待について、お聞かせください。

ファイル整合性監視や変更管理ソリューションは、PCI DSSのみならず、SOXといったITインフラの内部統制で要となるツールと捉えています。その為、PCI DSS対策の用途のみならず、McAfee Change Controlがより広く利用されることを望みます。

但し、変更管理ソリューションだけで、サーバーシステム・セキュリティのすべてを解決するわけでもないと感じています。大局的な視点ですが、国内の現状として、システム監視・運用の分野では統合管理という概念、そして、関連ツールが定着していますが、一方のシステム・セキュリティ分野では統合管理が進んでおらず、結果的に、ツールに対する初期投資のみならず、運用コストまでも肥大化する状況に陥っているように見受けます。

このような業界環境において、マカフィーは統合セキュリティベンダーとしてのビジョンとソリューションポートフォリオを強く意識していると感じます。先述の通り、McAfee Change Controlによる変更防止機能への拡張実装もそうですが、お客様の要望に応じて、将来的には、McAfee Application Control[3]による外的脅威によるプログラムの不正改ざん防止といった、基幹系サーバーを保護するための提案も行っていきたいと考えます。その為にも、マカフィーには、今後とも、一層のソリューションポートフォリオの拡充とそれらの日本市場における浸透に努めてほしいと期待します。

取材日時 2011年3月

3 McAfee Application Control は、サーバー上で実行するアプリケーションをホワイトリストとして登録することで、マルウェアを含む未承認のプログラム実行を防止します。

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

MCACS-IIJ-1105-MC