Case Study | 導入事例

コロラド州、マカフィーの新しいセキュリティコントロールの採用によりサイバーセキュリティを強化

コロラド州

顧客プロファイル:
コロラド州知事の情報技術室

産業:
州および地域の政府

IT環境:
27,000台のノード、16の部署

課　題

- Council on CyberSecurityのセキュリティコントロールを限られた予算とリソースで適用し、HIPAAとPCIのコンプライアンスを証明する。

導入製品

- **McAfee® ePolicy Orchestrator® (McAfee ePO™)**
- **McAfee Enterprise Security Manager**
- **McAfee Enterprise Log Manager**
- **McAfee Advanced Correlation Engine**
- **McAfee Event Receiver**
- **McAfee Network Security Platform**
- **McAfee Vulnerability Manager**

効　果

- 積極的な取り組みにより、最初の5つのセキュリティコントロールの導入という目標を達成
- McAfee ePOによるウイルススキャンとソフトウェアインベントリの作成
- McAfee Enterprise Security Managerの脆弱性評価による修正の迅速化と効果の向上

Jonathan Trull氏は、コロラド州知事の情報技術室(OIT)の情報セキュリティ担当責任者(CISO)に採用されたときに、資金不足や複雑なセキュリティ制御などの課題を引き継ぎました。「当時、州全体のITセキュリティ予算は6,000ドルでした。」と語るTrull氏はコロラド州の副監査人を務めた後、2012年に現職に就きました。

しかし、予算不足は知事のITセキュリティ部門の改革において、課題のひとつにすぎませんでした。もうひとつの問題は、既存のセキュリティコントロールのフレームワークです。NIST 800-53はガイドラインを含む長い文書なので、OITのスタッフと予算では完全に準拠するのは困難でした。そのため、Trull氏はリソースの割り当てを覆すことにしました。「時間とリソースの80%をPCIやHIPAAなどの規制のコンプライアンスに、20%を実際のセキュリティリスクの改善に割り当てることになっていましたが、それを逆転することにしたのです。規制を遵守する一方で、時間の80%を情報漏洩の防止に最も効果的な技術リソースを活用することに費やしました。資金とツールがあれば、リスクを大幅に削減できると確信していました。」

顧客のニーズへの対応:状況認識

行政および立法部門を説得して、セキュリティ強化のための資金を得た後、Trull氏はその目標を達成するために必要なツールセットを検討しました。「業務上、何よりも重要なのはリアルタイムの状況認識です。システムの現在の状態、システムの攻撃者、現在のセキュリティ構成でのコンプライアンスの状態とレベルを知ることです。そのためには、収集した情報を1つのダッシュボードにまとめる必要がありました。「すべての基準を満たし、データをシームレスに1つのダッシュボードに統合できる唯一の製品がマカフィーでした。」と、Trull氏は言います。

同氏がマカフィーの製品と人材を採用すると決断したことによって、サイバー攻撃の保護を強化する効率的な制御(コントロール)と優れた手順(プロセス)のスムーズな導入が約束されました。

セキュリティコントロールの重視

OITでは州のITセキュリティの90%を担う新しい仕組みとして、Council on CyberSecurityの上位20の重要なセキュリティコントロールを採用し、最初の5つに着手しました。マカフィーのチームは州がすでに所有するテクノロジーのインベントリを作成し、プロジェクトの目標達成に必要な要素とギャップを示すグリッドを作成しました。契約はすぐに成立しました。製品と3年間のオンサイトでの専門コンサルティングを50対50で組み合わせた契約には、マカフィーの柔軟な製品ライセンスも含まれます。コロラド州では15の製品で構成される技術を選択して、上位20の重要なセキュリティコントロールと、そのセキュリティプロジェクトの目標に取り組みました。OITは1日ですべてのツールを導入したり使用することはできませんでしたが、マカフィーとの契約によって意思決定が簡略化され、OITはプロジェクトの進行に合わせて必要になるすべてのツールを確認することができました。

「マカフィーとともに最初の5つのコントロールの本格導入に取り掛かったのですが、それは大変な作業でした。そのため、集中的に取り組むことにしました。着手からハードウェアとネットワークの設置、ツールへの人的プロセスの組み込みまで、決められたスケジュールで5つのコントロールを導入することを目標にしました。かなり無理をしましたが、厳しいスケジュールにもかかわらず、なんとかやり遂げることができました。」と、Trull氏は述べています。

intel Security

マカフィーのその他のソリューション

- McAfee Application Control
- McAfee Policy Auditor
- McAfee Change Control
- McAfee Database Activity Monitoring
- McAfee Enterprise Mobility Management
- McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus
- McAfee ePO Deep Command
- McAfee Deep Defender
- McAfee Complete Endpoint Protection—Enterprise suite
- McAfee Data Center suite

すべての基準を満たし、データをシームレスに 1 つのダッシュボードに統合できる唯一の製品がマカフィーでした。
どのような脅威であれ、どのようなウイルスであれ、攻撃を受けたら McAfee Network Security Platform、ファイアウォール、McAfee Vulnerability Manager を通して ESM（McAfee Enterprise Security Manager）にフィードされます。SIEM によってそれらすべてを分析できるため、より的確な意思決定が可能になりました。

コロラド州 情報セキュリティ担当責任者　Jonathan Trull 氏

マカフィーのテクノロジにより、OIT は最初の 5 つを実現

1 **すべてのネットワークデバイスのインベントリ**
正規および不正の両方を作成、不正なデバイスを検出後 48 時間以内に排除
McAfee Vulnerability Manager、McAfee Asset Manager、McAfee Rogue System Detection、McAfee ePO によるネットワークデバイスの検出とインベントリ

2 **正規 / 不正のすべてのソフトウェアのインベントリ**
後者はメディアプレーヤーを含めたピアツーピアの不正なソフトウェア
McAfee Application Control によるコンピュータ上での実行を許可されたソフトウェアインベントリの制御
McAfee ePO によるリスクと McAfee Global Threat Intelligence のアプリケーションのレピュテーションの制御

3 **デバイスの安全な標準構成の確立**
McAfee Application Control と McAfee Policy Auditor for Center for Internet Standards benchmarks

4 **脆弱性修正の評価**
McAfee Vulnerability Manager によるインターネットの境界および内部のサーバーのスキャン
McAfee Policy Auditor によるエンドポイントへの対応

5 **マルウェアからの防御**
McAfee VirusScan® をエンドポイントへに導入
McAfee Web Gateway による不正ペイロードを送信する既知のサイトをブロック

適切な情報による的確な意思決定

McAfee ePO ソフトウェアを使用すると、ウイルススキャンからソフトウェアなどのインベントリを作成するエージェントまで、すべてを管理できます。導入環境の中枢としてすべての機能を維持し、垂直方向のあらゆるソースから重要なデータを収集します。「Enterprise Security Manager はこれらすべてのデータを統合し、関連付ける役割を担っています。どのような脅威であれ、どのようなウイルスであれ、攻撃を受けたら［McAfee ］Network Security Platform、ファイアウォール、［McAfee］Vulnerability Manager を通して ESM［McAfee Enterprise Security Manager］にフィードされます。SIEM によってそれらすべてを分析できるため、より的確な意思決定が可能になりました。」と、Tull 氏は言います。

脅威が特定されたら、即座に修正する必要があります。以前の OIT では脅威を高、中、低に分類し、そのすべてにパッチを適用していました。現在では、SIEM によって高度な脆弱性が特定されると、OIT がアクティブな脅威の存在を確認し、その脅威を最優先して修正しています。「マカフィーのツールによって状況認識、重要な意思決定、リソースの割り当て、そして何よりも重要な、時間配分が的確にできるようになりました。これには非常に満足しています。」と、Trull 氏は総括しています。

最新導入事例はこちらをご覧ください　http://www.mcafee.com/jp/case-studies.aspx

intel Security

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

名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅4-6-17 名古屋ビルディング13F
TEL：052-551-6233（代）FAX：052-551-6236

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）

● 製品、サービスに関するお問い合わせは下記へ

MCACS-COLO-1504-GRP