

McAfee Embedded Control

(旧名称:McAfee Embedded Security)

組み込みデバイスへの不正な変更を防止

組み込み業界のビジネス上の課題


組み込みデバイスおよびアプライアンスは、現在重要なインフラに幅広く導入されています。たとえば、POS端末、セルフチェックアウト、キオスク、小売店の携帯端末、Point-of-Careの医療モダリティ(病院のX線、超音波、CTスキャン、MRTデバイスなど)、銀行のATM、企業内のシンクライアント、プロセス管理システムやSCADAデバイスなどの重要なインフラストラクチャ、産業用コントローラー、ストレージアプライアンスなどがあります。

組み込みデバイスは、長い間、専用ハードウェアとプロプライエタリー・ソフトウェアで構成されていました。しかし最近では、小売業界のUPOSなどの標準化機構の推進によって、標準化の方向に移行しています。この標準化によって、デバイスの相互接続が進み、商用オペレーティングシステムやオープンなオペレーティングシステムを実行するコモディティハードウェア上で既成のソフトウェアを使用できるようになりました。

この移行によって、デバイスメーカー、チャネル、および顧客は、それぞれのコアビジネスに集中できるようになり、恩恵を享受しています。また、ソフトウェアを柔軟に選択することや、開発期間の短縮、ライフサイクルの途中で新しいテクノロジーを採用することも可能になりました。

「私たちは、コントロールされていない変更がPOSデバイスの可用性低下やメンテナンスコスト増加の主な原因であることを割り出しました。POSシステムにMcAfee Embedded Controlを導入した結果、各デバイスへの変更を完全にコントロールできるようになりました。コントロールの強化によって、ポリシーに従わないすべての変更を防止するとともに、緊急なパッチ適用が不要になり、サポートコストを大幅に削減することができました」

—NECインフロンティア
i-Appliance部門
ゼネラルマネージャー
Hiroshi Komura氏

過去	現在
プロプライエタリーOS	Windows OS 
独立したネットワーク	インターネットによる相互接続
高額なデバイスコスト	安いデバイスコスト
低いサポートコスト	高いサポートコスト
パッチ適用はほとんどなし	パッチ適用は一般的
独自のセキュリティリスク	高まるセキュリティリスク

変化する組み込みシステム

「CADstreamは、胸部MRI研究のために医師の方々に毎日活用されています。私たちは、不正な変更によってシステムの整合性と可用性が脅かされることが当社のお客様に許容されないことを十分承知しています。McAfee Embedded ControlをCADstreamに統合することで、CADstreamのセキュリティ、可用性、サポートとも改善されるでしょう」

— Confirma社 研究開発担当副社長 Paul Budak氏

しかし、このメリットをもたらしている標準化と柔軟性は、マイナス要素もあります。組み込みデバイスは、標準的なPCと同様に、セキュリティリスク、頻繁なパッチの適用、ウイルス対策ソリューションの頻繁な更新の影響を受けるようになりました。また、故障の原因にもなる、増加している未承認の変更にも無防備になっています。このようなデバイスは現場で点検されるため、コンプライアンスに非準拠になってしまう可能性もあります。多くのデバイスメーカーとサービスチャネルは、このようなデバイスを製造、配備した後、どのようなソフトウェアが誰にいつインストールされるか、現在どのようなソフトウェアが稼働しているかをコントロールできません。そのため、デバイスのライフサイクルにおける総所有コストが上昇します。その結果、「組み込みデバイスが出荷時と同様のまま現場で継続的に機能する」という主張がますます難しくなっています。

デバイスのコントロールを強化

McAfee Embedded Controlは、未承認の変更を防止するため、デバイスメーカーやサービスチャネルは、デバイスを構築、配備したあと、コントロールすることが可能になります。

「(マカフィーは)既知の適切なアプリケーション構成に基づいてシステムのロックダウン(システムのハードニング)を行うので、他のアプリケーションを実行できなくなります。一部のプロバイダーも、ハードニングプロセスにベースOSを含めています。この手法は、組み込みシステム、専用サーバー、キオスクに適しています」

— Gartner Group 情報セキュリティプライバシー担当グループ VP兼研究ディレクター
Neil MacDonald氏

このソリューションでは、チャネルに有益なソフトウェア変更ポリシーを現場の組み込みデバイスに施行できるので、ポリシーに従っていない不正なソフトウェア変更を防止し、現場での故障を低減するとともに、デバイスのポリシー遵守を徹底できます。McAfee Embedded Controlは、セキュリティを強化し、パッチ適用の頻度を低減し、ゼロデイ攻撃からデバイスを保護します。

McAfee Embedded Controlはフットプリントが小さく、デバイス上に迅速にセットアップすることができ、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。また、デバイスメーカー、サービスチャネル、エンドユーザーの製造、供給、監視、変更管理、現場メンテナンスの各プロセスと統合し、現場で誰がサービスを提供する場合でも、組み込みデバイスに対するコントロールを強化します。

McAfee Embedded Control

McAfee Embedded Controlには、2つの重要な機能があります。

変更管理

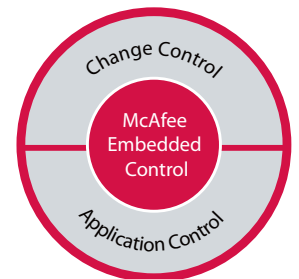
McAfee Embedded Controlでは、2つの異なるワークフローで、デバイス所有者のソフトウェア変更ポリシーを柔軟に施行できます。最初の多段階の製造過程では、複数のチャネルベンダーが各自のソフトウェアと付加価値サービスをデバイスにインストールします。次の稼働中の保守およびサポート段階では、デバイス所有者や複数のチャネルベンダーが各自のソフトウェア/ハードウェアのソフトウェア更新を行います。

変更管理機能は、デバイスライフサイクル中の運用に柔軟性を提供します。たとえばMcAfee Embedded Controlは、製造期間中および稼働中にデバイスにインストールできるソフトウェアを、デバイス所有者に許可されたソフトウェアのみに限定できます。また、選定されたチャネルパートナーのみにデバイスへの更新を許可し、コンプライアンスやフォレンジックのために、実施された更新を記録することができます。

さらにMcAfee Embedded Controlは、PCI、FDA、HIPAAや他の法規制のコントロール要件を満たすためにも活用できます。これにより、法規制で求められている改ざんが防止された監査ログをデバイスに保持し、法規制に対応する制御を実施していることを実証できます。

アプリケーション管理

McAfee Embedded Controlは、マルウェア(ワーム、ウイルス、トロイの木馬、バッファオーバーフロー攻撃など)を通じた既知および未知の多様なゼロデイ攻撃から本番環境のデバイスのセキュリティを確保し、保護します。また、緊急なパッチの適用が不要になり、またパッチ適用の頻度が低減するため、事前に時間をかけてパッチをテストできるようになります。さらに、ローカルサポート体制が整っていない遠隔地や分散して配備されている地域など、パッチ適用が難しいデバイスのセキュリティリスクも低減します。アプリケーション管理機能によって、計画的なパッチ適用の頻度と予期しない復元に必要な時間がともに低減されるため、運用コストの削減が可能になり、デバイスの可用性も向上します。必要なタッチポイント数を減らしてサポート費用を削減するこのソリューションは、ローエンドデバイスに最適です。



McAfee Embedded Controlは、ITインフラストラクチャをコントロールするための包括的なソリューションをお客様に提供します。

デバイスメーカーに提供するメリット

以下の表は、デバイスメーカーが直面している一般的な問題と、McAfee Embedded Controlのお客様が享受しているメリットをまとめたものです。

「マカフィーの革新的なソフトウェアとIT保護機能は、私たちの包括的なセルフサービスチャネル保護アプローチであるNCR Secureにとって重要な要素です。NCRでは、顧客からATMチャネルへの信頼を維持するため、業界が最高の戦略を予測、計画、実行できるように真剣に支援に取り組んでいます」

—NCR—財務ソリューション部門
セルフサービス担当副社長
Bob Tramontano 氏

組み込みライフサイクルの課題

大規模な攻撃の発生によるセキュリティの脆弱性の増大

複数のベンダーが関与するライフサイクルで、いつどのソフトウェアがインストール、実行されるかをコントロールできない

高いサポートコスト

- サポート/メンテナンス中に行われた未承認の変更が原因で現場のデバイスが故障する
- すべてのパッチをテスト、検証する必要がある
- 一元的なソフトウェア配布モデルなどのオンサイトスタッフサポートが適さない

現場での変更が原因でFDA、HIPAA、PCI、その他の規制を遵守できない

サードパーティ製ソフトウェアの高額なコスト: サードパーティ製ソフトウェアはピーク時のパフォーマンスの影響が高く、頻繁な更新や管理者の集中的な操作が必要

マカフィーの利点

既知の攻撃およびゼロデイ攻撃に対するセキュリティを強化

チャネルに有益な管理機能: メーカーおよびサービスチャネルのソフトウェア管理ポリシーを柔軟に施行
所有コストを低減

- 現場での故障とサポートコールを低減するとともに、タッチポイント数を削減
- 個別および一括のパッチ適用の必要性を排除
- 制御された複数のソフトウェア更新モデルの活用が可能

ソフトウェア変更管理と実行時管理により、導入後すぐにコンプライアンスに対応

影響の少ないソリューション: パフォーマンスへの影響を最小限に抑え、継続的な更新を排除し、管理者の負担を軽減

まとめ

McAfee Embedded Controlは、組み込みデバイスを保護し、組み込みデバイスへのソフトウェア変更ポリシーの施行を自動化する業界初の唯一のソリューションです。McAfee Embedded Controlは、組み込みデバイスメーカーとそのサービスチャネルの総所有コストを削減します。ATM、POS端末、医療デバイス、シンクライアント、ストレージブライアンスなどのデバイスの主要メーカーに導入されており、これらのお客様は、現場へのサポートの派遣や未承認の変更に起因する故障を大幅に削減し、短期間でこのソリューションへの投資から大きな利益を得ています。

仕様

プラットフォームのサポート

- Windows 7
- Windows 7 Embedded
- Windows Vista
- Windows XPE
- Windows XP
- Windows 64ビット/x86-64 XP
- Windows 2008
- Windows 2008 R2
- Windows 2003
- Windows 2003 R2
- Windows 2000
- Windows NT
- WEPOS, POSReady 2009
- WES 2009
- Linux RHEL 3 (32ビット)
- RHEL 4/5 (32ビット/64ビット)
- CentOS (32ビット/64ビット)
- SuSE EL 9/10 (32ビット/64ビット)
- SuSE (32ビット)
- SuSE Pro 9.3 (32ビット)
- Open SuSE 10/11 (32ビット)

システム要件

- Windows/UNIX
- 単一/複数のIntel Pentium
- 512MBのRAM
- 200MBの空きディスク容量
- システムの管理者権限

McAfee, Inc.について

McAfee, Inc.は米国カリフォルニア州サンタクララに本社を置く、世界最大のセキュリティ専門ベンダーです。マカフィーは、世界中のセキュリティに関する手強い難題に絶えず取り組んでいます。そのプロアクティブで実績あるソリューションとサービスは世界中のシステムとネットワークを保護し、ユーザーのインターネットへの安全なアクセス、Webの閲覧および取引の安全を確実に支えています。受賞歴を誇るすばらしい研究チームとともに、マカフィーは革新的な製品を送り出しています。個人ユーザーをはじめ、企業、官公庁・自治体、ISPなど様々なユーザーは、コンプライアンスの確保、データの保全、破壊活動の阻止、脆弱性の把握を実現し、またセキュリティレベルを絶えず管理し、改善することができます。詳細については、<http://www.mcafee.com>を参照してください。



An Intel Company

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	〒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

●製品、サービスに関するお問い合わせは下記へ