McAfee ePO Deep Command

オペレーティング システムを超えたセキュリティ管理で運用コストを削減

セキュリティ インシデント、ウイルスの大量発生、暗号化パスワードの紛失などによるオンサイト サポートやヘルプデスクへの問い合わせを減らしましょう。電源がオフになっているエンドポイントや無効化または暗号化されているエンドポイントにもセキュリティを配備し、管理する必要があります。McAfee® ePO™ Deep Command[1]はIntel® vPro™ Active Management Technology（AMT）によりオペレーティング システムを超えた管理を自動的に行います。これにより、運用コストを削減しながらセキュリティとコンプライアンスを強化できます。また、リモートにあるPCや専用端末の修復を迅速に行うことができます。

主な特長

- **Intel AMTの迅速な検出とプロビジョニング:** Intel vPro搭載PCを簡単に識別し、Intel AMTを有効にします。
- **安全なロック解除**: McAfee Complete Data Protectionスイートと一緒に使用すると、McAfee ePO Deep Commandで安全にロックを解除し、暗号化されたエンドポイントのプリブート環境にアクセスできます。
- **修復時間の短縮:** 場所に関係なく、リモートからハードウェア レベルでPCまたはエンドポイントに接続し、修復作業を行うことができます。
- **ユーザーの生産性の向上:** リソースを集中的に使用するタスクを時間外に実行し、ユーザーへの影響を抑えることができます。
- **ITコストの削減:** オンサイト サポートの回数やサービス コールの時間が少なくなります。
- **エンドポイントの省電力化:** 省電力プログラムを実行しながら、セキュリティの管理やパッチの適用を実行できます。

セキュリティ管理者は、増大するコストと脅威、厳しさを増すビジネス要件への対応に苦労しています。マルウェア感染などの脅威でオンサイト サポートを行うと250ドルもコストがかかることがあります。この他にも移動費がかかります。リモート オフィスや自宅、モバイル環境で仕事を行う従業員はすぐに仕事ができるようにサービスの提供を求めてきます。このような多忙なユーザーの多くは問題を無視し、マルウェアによって悲劇的な状況に陥るまで脆弱な状態のシステムを使い続けます。

エンドポイントに対する脅威は日々増大しています。サイバー犯罪者は新しい脆弱性をすぐに悪用し、ボットネットやWebサイトを介してステルス型の脅威やゼロデイ マルウェアを拡散しています。ユーザーのPCや専用端末を使用不能にし、オペレーティング システム レベルの対策を無効にするマルウェアも存在します。

このような複雑な環境でさらに省電力化が求められているため、CIOはアイドル状態のデスクトップにも対策を講じなければなりません。未使用のシステムの電源をオフにしながら、セキュリティとコンプライアンスを維持し、ITプロセス（スキャン、更新、パッチの適用など）を実施できる方法が求められています。これらの活動は、ユーザーに影響を及ぼさずに行わなければなりません。

Intel vProプラットフォームの検出と有効化

McAfee ePO Deep Commandを使用すると、Intel AMTアラーム クロック、リモート ウェークアップ機能、KVM（キーボード、ビデオ、マウス）、IDEリダイレクトなど、Intel vPro技術をフルに活用することができます。まず、McAfee ePO Deep Commandの検出/レポート モジュールが環境内でAMT対応のPCを検出します。詳細なレポートが出力されるので、McAfee ePO Deep Commandエージェントが必要なPCとエンドポイントをピンポイントで特定できます。McAfee ePO Deep CommandはIntel AMTのプロビジョニングを簡素化し、Intel AMTの有効化を簡単に行うことができます。プロビジョニングされたAMT PCやエンドポイントにMcAfee ePO Deep Commandをインストールすると、オペレーティング システムを超えたハードウェア レベルでリモートから管理作業を行うことができます。

システム要件

- McAfee ePO 4.6（検出/レポート モジュール）、McAfee ePO 4.6（McAfee ePO Deep Command）、McAfee ePO 5.0以降
- McAfee Agent 4.5以降
- McAfee Drive Encryption 7.0以降（暗号化のリモート管理機能）
- Windows XP、Windows Vista、Windows 7、Windows 8、Windows Server 2003、Windows Embedded XP、Windows Embedded 7
- Intel vPro AMT 2.2以降
- インテル セットアップ・コンフィグレーション・ソフトウェア（SCS）8.2以降

リモートからの復旧作業

セキュリティ管理者は、電源や暗号化の状態に関係なくエンドポイントに接続し、ハードウェア レベルで制御することができます。セキュリティ ポリシーやコンプライアンス ポリシーをリモートから施行できるので、セキュリティの運用コストを削減できます。電源管理プログラムを導入すると、セキュリティ状況の改善だけでなく、エンドポイントへのアクセスを維持しながら消費電力を抑えることができます。McAfee ePO Deep CommandはIntel vPro AMT技術を利用してエンドポイントにアクセスします。オペレーティング システムには依存しません。ハードウェア レベルでアクセスするので、エンドポイントの電源をオンにしてセキュリティ タスクの実行後、電源状態を元に戻すことができます。McAfee ePO Deep Commandは、McAfee Complete Data Protection（エンドポイント暗号化）により、エンドポイントのブート プロセスを安全に開始できます。リモートからセキュリティ タスクを行うためにユーザーの認証情報を入力する必要はありません。これらの操作はアラーム クロックの電源オンまたはオンデマンドの電源オンによりすべて自動的に実行されます。

McAfee ePO Deep Commandを使用すると、オペレーティング システムを超えたレベルでエンドポイントと通信を行うことができます。これにより、管理の難しいエンドポイントの設定や修復を中央のMcAfee ePOから実行できます。

起動と実行

セキュリティ メンテナンスや時間のかかる作業を時間外やユーザーの邪魔にならない時間に実行できます。AMTアラーム クロックを使用すると、暗号化されているエンドポイントでも電源を入れて起動し、次のようなセキュリティ タスクを実行できます。

- セキュリティと設定の更新（.DATなど）
- オンデマンド スキャン
- 別のセキュリティ製品のインストール
- イベントのレポート
- アプリケーションまたはオペレーティング システムへのパッチの適用

機能しないエンドポイントをリモートから復旧

オペレーティング システムが機能しなくなったり、ハードディスクに障害が発生した場合、McAfee ePO Deep Commandの統合管理機能により、システムを復旧することができます。エンドポイントやPCがリモートにある場合でも、管理者は機能しなくなったPCやエンドポイントのKVM（キーボード、ビデオ、マウス）にAMT経由で接続し、ネットワーク上の別のISOイメージからPCを起動できます。大半の場合、エンドポイントを有線でネットワークに接続する必要はありません。McAfee ePO Deep CommandはセキュアなWi-Fiに対応しているエンドポイントを管理できます。

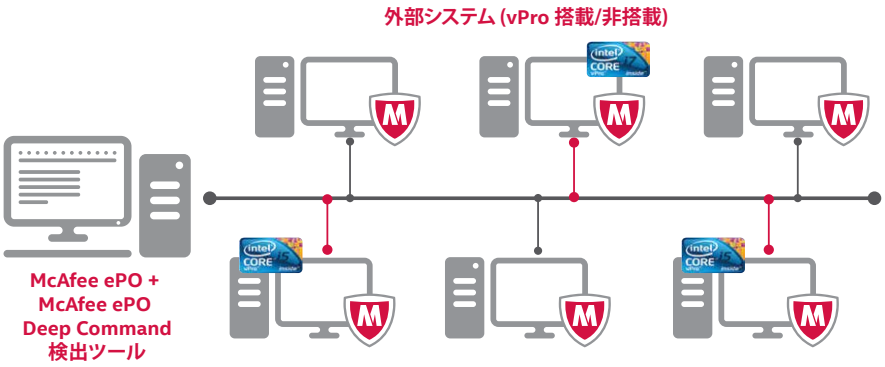

図 1. McAfee ePO Deep CommandがvProシステムを検出してソフトウェアを配備し、Intel AMTを有効にします。

Intel AMTのFCFH（Fast Call for Help）機能を使用すると、McAfee ePOの管理者に簡単に連絡して、ヘルプを依頼できます。McAfee ePOの管理者は次の作業を簡単に実行できます。

- ネットワーク上の別の場所にあるイメージからエンドポイントを起動する。
- ローカルのKVMを完全に制御する。
- ユーザーの暗号化パスワードをリセットする。
- 感染、無効化または隔離されたシステムを自動的にクリーンアップし、修復する。

脅威を未然に防ぐセキュリティ

包括的なセキュリティ統制により、新たに発生する脅威を未然に防ぎ、エンドポイントを保護します。脅威が侵入する前にシステムを更新し、リモートから対策を講じることができます。ユーザーの作業に影響を及ぼすことなく、データの安全性を維持できます。

エンドポイントの省電力化

McAfee ePO Deep Commandは、エンドポイントを起動してポリシーの更新を行い、元の電源状態に戻します。セキュリティを侵害することなく、消費電力を抑えることができるので、省電力プログラムを安心して利用できます。省電力の詳細については、マカフィーにお問い合わせください。

エンタープライズ クラスの拡張性とレポート機能

McAfee ePO Deep Commandは、ePolicy Orchestrator®（McAfee ePO™）の管理フレームワークを強化します。数十万のエンドポイントも管理できます。分散環境のセキュリティ管理にも対応しているMcAfee ePOは、マカフィーのセキュリティ インフラ全体のポリシー管理とレポーティングを統合環境で一元的に行います。また、オペレーティング システムを超えてポリシーを施行し、コンプライアンス管理を行うことができます。McAfee ePOのダッシュボードとレポートに表示される情報量を増やすと、エンドポイントの対応状況と組織全体のセキュリティ状況をより正確に把握できます。相互に関連付けられたデータを使用するので、監査を簡単に行うことができます。

詳細については、**http://www.mcafee.com/jp/products/epo-deep-command.aspx** をご覧ください。

McAfee ePO Deep Commandは、スタンドアロン製品として利用することも、McAfee Complete Data Protectionスイートと一緒に利用することもできます。詳細については、**www.mcafee.com/jp/products/data-protection/index.aspx** をご覧ください。

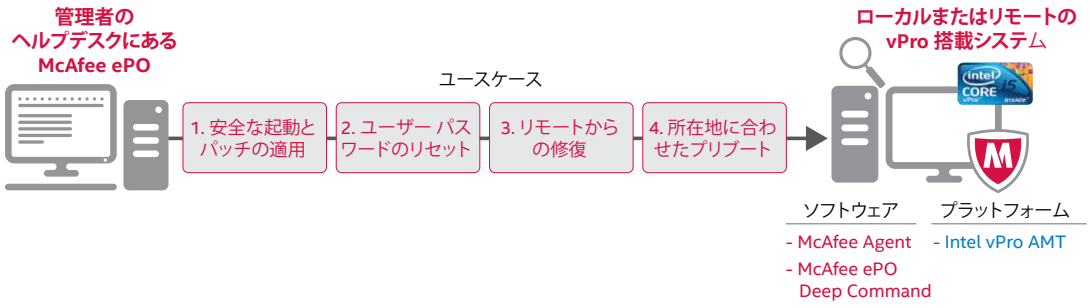

図2. McAfee ePO Deep Commandを利用すると、ローカルまたはリモートでヘルプ デスクが作業を行うことができます。

McAfee. Part of Intel Security.
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）
www.intelsecurity.com

1. McAfee ePO Deep Commandは、スタンドアロン製品として利用することも、McAfee Complete Data Protectionスイートと一緒に利用することもできます。詳細については、**www.mcafee.com/jp/products/data-protection/index.aspx** をご覧ください。

61371ds_epo-deep-command_1014