



McAfee Device Control

ネットワークでのリムーバブルメディアの不正使用を防止

USB ドライブ、MP3 プレーヤー、CD、DVD などのリムーバブルメディアは、便利な反面、実は、企業にとって危険因子となっています。このような小型・大容量のストレージデバイスによって、極秘の顧客データや知的財産が社外に流出、悪意の第三者の手に渡って紛失・盗難に遭う、ということが起こりやすくなります。

McAfee® による調査では、回答者の半数以上(55%)が毎週ポータブルデバイスを用いて機密文書を会社から持ち出していると答えています¹。誰が、何を、どのデバイスに保存しているか、把握していますか？ また、たとえデータを使う権限を持つ人であっても、きちんと機密を保っていることを確認するすべはありますか？

主な利点

強力な保護機能

- リムーバブルストレージデバイスの不正使用による情報漏えいを防止。

総合的なデバイス管理

- ハードウェアおよびコンテンツをもとに、リムーバブルストレージデバイスにおいて機密データを細かくフィルタリング、モニタリング、ブロック。
- リムーバブルメディアデバイスの安全な使用を保証。「すべてブロック」してしまって業務生産性を損なうことはありません。

ePO による集中管理

- McAfee のセキュリティリスクマネジメントプラットフォームを強化、リムーバブルストレージデバイスからの情報漏えいを防止。
- セキュリティポリシーの配置・管理を一元化、リムーバブルメディアからの機密情報漏えいを防止。

完全な可視化

- 監査、取締役会その他利害関係者に対して法令遵守措置が正しく実施されていることを証明。

情報漏えいによるコストアップを抑制

情報漏えいは、今日、企業が直面するセキュリティ問題の中でも、最も広範かつ深刻で、損失の大きな問題のひとつです。事実、Fortune 1000 企業の 75%以上が偶発的または悪意の情報漏えいの被害を受けています。損失も甚大で、2007 年には、企業が情報漏えいによって受けた損害の平均額は 630 万ドルでした²。

ポータブルデバイス・リムーバブルメディアにコピーされたデータを監視・管理

McAfee Device Control は、USB ドライブ、iPod、Bluetooth デバイス、書込可能な CD や DVD などのリムーバブルメディアから最重要データが企業外部に持ち出されるのを防ぎます。ユーザや機密データがどこにあるか、またコンピュータが企業のネットワークに接続しているか否かを問わず、デスクトップ、ノートパソコンなど全てのコンピュータからのデータ移転を監視・管理できます。

Device Control は漏えいの危機にさらされやすいデータをきめ細かく管理することが可能です。使用できるデバイスとできないデバイスを指定したり、使用できるデバイスにコピーできるデータとできないデータを設定したり、さらにユーザのデータコピーについて、機密情報を格納しているファイルサーバなどの特定のロケーションや、機密報告書を作成するのに使われるアカウントプログラムなど、特定のアプリケーションからのコピーを制限したりすることができます。

デバイスとデータに対する詳細なポリシーを自動的に適用

情報資産を集中管理する仕組みを簡単に構築できます。McAfee ePolicy Orchestrator® (ePO™) で、管理下のデスクトップコンピュータやノートパソコンに McAfee Device Control エージェントを配布します。次にどのデータがどのリムーバブルメディアにコピーできる(またはできない)か、ポリシーを詳細に指定します。残りの作業は Device Control で行います。自動的に使用を監視し、設定されたポリシーに違反するデバイスの使用やデータ転送を、データの修正、コピー、貼り付け、暗号化に関わらず、ブロックします。また、Device Control はコンプライアンスに対応した業務を中断させることはありません。

コンプライアンスを常に証明

McAfee Device Control の導入により、リムーバブルストレージデバイスやメディアへの機密情報の転送を完全に可視化し、管理できるようになります。ePO で統合することにより、デバイス、タイムスタンプ、データ証明などの使用に関する重要データを簡単に収集できます。クリックするだけでリアルタイムのイベント監視や詳細な捜査レポート作成などを行い、監査、取締役会その他利害関係者に対して法令遵守措置が正しく実施されていることを証明できます。

¹ McAfee, The Threats Within Volume II: Data Loss Disaster(2007年2月)

² Ponemon Institute, 2007 Cost of Data Breach Study

システム要件

ePO サーバ

オペレーティングシステム

- Microsoft Windows Server 2003 SP1, 2003 R2

ハードウェア要件

- ディスク空き容量：250MB
- メモリ：512MB(1GB 推奨)
- CPU：Intel Pentium II クラス以上 (450MHz 以上推奨)

Device Control エンドポイント

オペレーティングシステム

- Microsoft Windows XP Professional SP1 以上
- Microsoft Windows 2000 SP4 以上

ハードウェア要件

- CPU：Intel Pentium III 1GHz 以上
- メモリ：512MB 以上推奨
- ディスク空き容量：最小 200MB
- ネットワーク接続：TCP/IP によるリモートアクセス

主な機能

強力なデータ保護機能

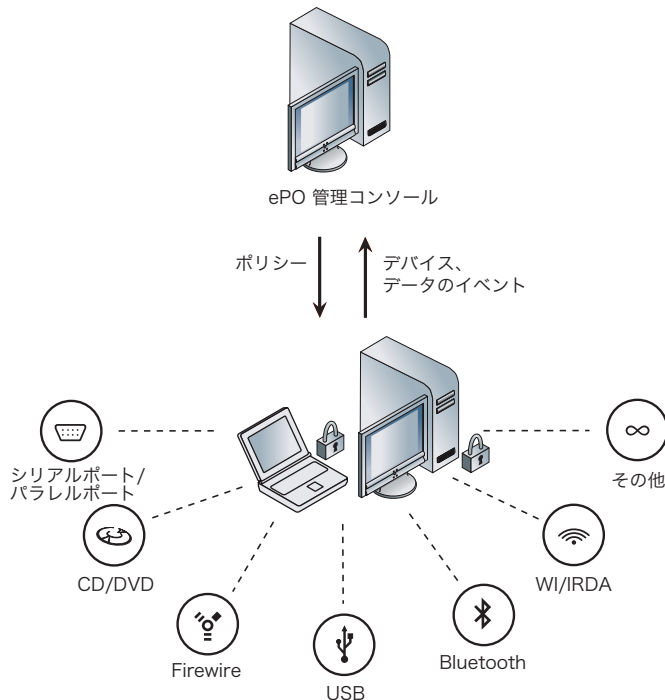
- ユーザによるデータコピーを制限します。対象デバイスは、USB ドライブ、iPod、書込可能な CD および DVD、フロッピーディスク、Bluetooth デバイス、IrDA デバイス、映像機器、COM ポート、LPT ポートなど。
- データに修正・コピー・貼り付け・圧縮・暗号化の処理が行われた場合でも、全データ、フォーマットおよびその派生物を保護します。
- 通常業務を中断させることなく、ユーザのロケーションに関係なく、情報漏えいを防止します。

McAfee ePO による集中管理

- 中央管理コンソールから、ポリシーおよび環境内のエージェントを迅速・簡単に設定、配置、更新できます。
- ユーザ、グループ、部門ごとにデバイスとデータのポリシーを設定できます。
- 製品 ID、ベンダー ID、シリアル番号、デバイスクラス、デバイス名などの Windows デバイスパラメータをもとに、使用可能なデバイス・使用不可のデバイスを指定できます。
- アクセス可能なデバイスに対して、どのデータをコピーできるか（またはできないか）を指定できます。

簡単かつ完全な可視化と管理

- ユーザ毎、およびデバイス毎の詳細なログにより、監査・コンプライアンスの要件に対応します。
- デバイス、タイムスタンプ、データ証明などのイベントの詳細を集め、即座に適切な回答・調査・監査ができるようにします。



McAfee Device Control では、どのデバイスに何のデータがコピーできるか指定できます。

McAfee®

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

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

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

福岡営業所 〒812-0011 福岡県福岡市博多区博多駅前3-2-1 日本生命博多駅前ビル 11F
TEL:092-452-3511 (代) FAX:092-452-3515

McAfee、マカフィー、ePolicy Orchestrator、ePOは、米国法人McAfee, Inc またはその関係会社の登録商標または商標です。本書中のその他の登録商標および商標はそれぞれその所有者に帰属します。©2008 McAfee, Inc. All Rights Reserved.

●製品、サービス、サポート内容の詳細は、最寄りの代理店または弊社事業部までお問い合わせください。●製品の仕様、機能は予告なく変更する場合がありますので、ご了承ください。MCADS-MDC-0804A-RD

●製品、サービスに関するお問い合わせは下記へ