Technology Blueprint

McAfee
An Intel Company

リムーバブルメディアの保護

USBメモリーなどのポータブルストレージデバイス使用の効果的な管理

SECURITY CONNECTED REFERENCE ARCHITECTURE

LEVEL 1 2 **3** 4 5

Security Connected

マカフィーのSecurity Connectedフレームワークは、複数の製品、サービス、パートナーの統合を可能にすることで、効率的かつ効果的に一元的なリスク軽減を実現します。20年以上の実績を持つセキュリティプラクティスを基盤に構築されたSecurity Connectedアプローチを通じて、規模やセグメントを問わず、すべての地域の組織がセキュリティ体制を改善し、セキュリティを最適化することでコスト効率を高め、戦略的にセキュリティとビジネスイニシアチブを整合させることが可能になります。Security Connectedリファレンスアーキテクチャーは、構想から実装までの具体的な手法を提供します。このアーキテクチャーを利用することにより、Security Connectedの概念をお客様独自のリスク、インフラストラクチャー、ビジネス目標に適合させることができます。マカフィーは、常にお客様を保護する新しい方法を見出すことに専心しています。

USB メモリーなどのポータブルストレージデバイス使用の効果的な管理

現状

リムーバブルメディアは現在、幅広く利用されていながら、セキュリティが最も脆弱なデバイスのひとつです。これには USB メモリー、スマートフォン、バックアップドライブなどが含まれます。その脆弱性の原因は、社員がリムーバブルメディアに対する制限がないことに慣れてしまい、組織もポリシーを適用してもユーザーが守れないと思い込んでいることにあります。しかし、Ponemon Institute によると、過去 2 年間に発生した企業の機密情報漏えいの原因の 70% はリムーバブルメディアにあります。また、USB デバイスにセキュリティポリシーを適用している組織のうち、データ漏えい防止（DLP）ツールを使用しているのはわずか 21% です [1]。機密データの損失に加え、リムーバブルメディアはマルウェアの標的にもなっています。

OS には、リムーバブルメディアの使用に対する管理や監査の機能はありません。そのため、多くの組織は、社員がどのようにリムーバブルメディアを利用しているか把握していません。また、そのリスクに対する危機感がないため、ビジネスとデータを保護するポリシーや管理には投資していません。

課題

多くの組織が機密情報を持ち、保護する必要がありながら、リムーバブルメディアの使用には何の対策も講じていません。また、リムーバブルメディアには、セキュリティの確保を困難にする特別な事情があります。

- **リムーバブルメディアの使用方法の把握**: リムーバブルメディアを使用している社員とその使用目的を把握し、その使用が正当なビジネス活動であるかを判断するのは困難です。
- **リムーバブルメディアの適切な使用のためのポリシーの決定**: OSではリムーバブルメディアのセキュリティポリシーが管理されないため、第三者のソリューションを使用する必要があります。これらの製品の多くはポイント製品であるため、総合的な管理には複数のメーカーの、複数の製品が必要になります。
- **リムーバブルメディアのデータの暗号化**: ユーザーが組織の機密情報をコピーする場合、暗号化が必要です。ただし、暗号化するデータの量が多いとユーザーの不満の原因となり、時間もCPUも消費します。選択した部分のみを暗号化するには、転送するデータやファイルの内容を理解する必要があります。データを暗号化することを決めたら、会社が所有する資産でのみアクセスを許可するのか、任意のコンピューターでのリムーバブルメディアの使用を許可するのか決める必要があります。
- **ポリシーとツールに対するユーザーの受け入れ**: 複雑なソリューションはユーザーの生産性に影響します。ユーザーには、会社のリムーバブルメディアに対するポリシーに従ってもらう必要があります。そのためには、損失した場合のリスクの重大さに加え、ポリシーに従う方法と理由を理解させなければいけません。

解決策

リムーバブルメディアのセキュリティのベストプラクティスは、リスクの低減、リスクの緩和、コンプライアンスの証明の順に展開します。最初に、会社のシステムに接続するデバイスがある場合は、そのデバイスを制御して、データ漏えいのリスクを低減します。次に、デバイスに転送するデータを制限します。最後に、デバイスに転送したデータを保護します。デバイスが紛失した場合、最大の問題となるのは、「どのようなデータが保存されていたか」と「データは暗号化されていたか」です。確実に暗号化されていれば紛失時にも、個人情報保護法で規定されているような侵害による開示を防止できます。

適切なアプローチは組織によって異なります。ユーザーが正当な理由からリムーバブルメディアを必要とする場合もあれば、規制当局によって、開示に対して厳しいルールが適用される場合もあります。次に具体的な方法を説明します。

- **リムーバブルメディアの使用方法の把握**: データ漏えい防止(DLP)ソリューションの情報を使用して、リムーバブルメディアの使用状況を把握しながら監視します。このような製品では、詳細な監査によってコピーされたデータとその場所を特定して、各イベントを特定のユーザーに関連付けることができます。また、DLP製品のレポート機能を使用すると、現在の使用状況と傾向を把握できます。
- **適切な使用のためのポリシー作成**: 正当な業務上の必要性を理解して、リムーバブルメディアの使用に関する適切なポリシーを作成します。
  - » リムーバブルメディアの使用許可の定義: 最も厳格なポリシーでは、DLPソリューションを使用して、正当な業務上の理由がない限り、ユーザーに対してすべてのリムーバブルメディアの使用をブロックします。リムーバブルメディアを使用する正当な理由のあるユーザーに対しては、ポリシーによってハードウェア暗号化機能を備えたメディアの使用を許可します。
  - » マルウェア対策の使用: StuxnetやConfickerなど、マルウェアがリムーバブルメディアを通して組織に侵入するケースが増加しています。ポリシーではマルウェア対策機能を備えたデバイスのみを許可し、コピーするすべてのデータを自動でスキャンし、感染の原因となるコードを検出することを義務付けます。
  - » リムーバブルメディア上の機密データにアクセスするシステムの決定: 多くの組織は、会社所有のノートPCとデスクトップPCに接続するリムーバブルメディアがアクセス可能な機密データを制限しています。それに対して、会社所有であるかどうかを問わず、すべてのシステムの機密データにアクセスできる組織もあります。

ソリューション選定の要素

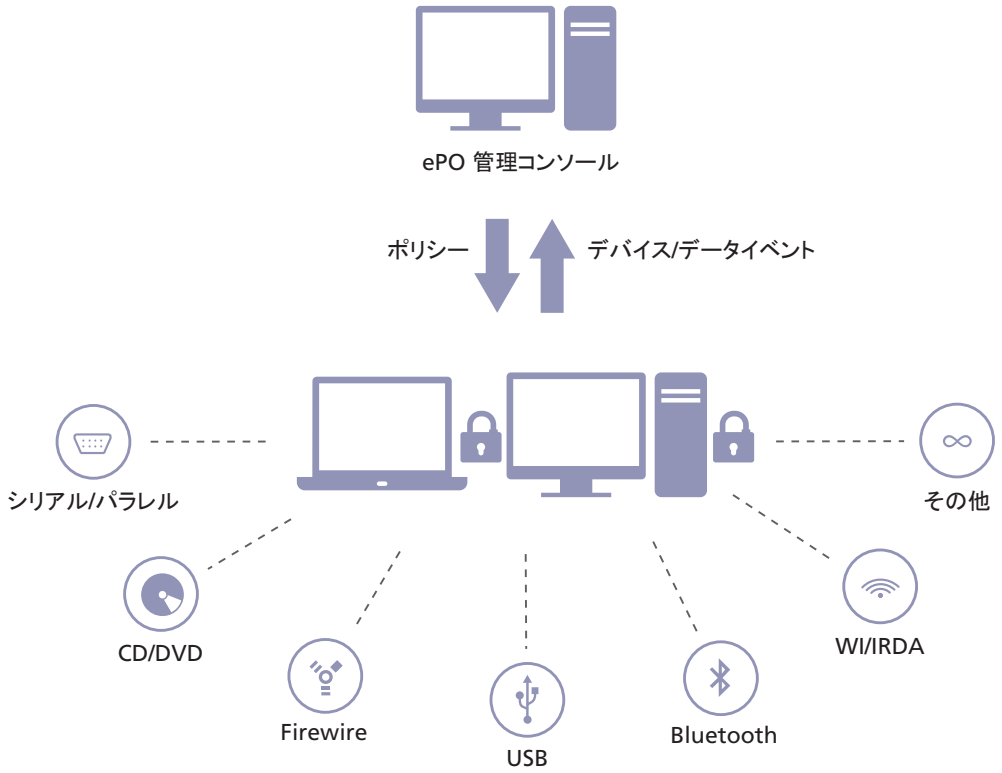
アーキテクチャーには、次のような要素が影響します。

- リムーバブルメディアの利用ポリシーに従って、ブロックまたは暗号化しているか。
- 会社所有のデバイスに対してのみリムーバブルメディアを使用しているか。
- リムーバブルメディアをマルウェアから保護する必要があるか。
- McAfee ePolicy Orchestrator(McAfee ePO)を現在使用しているか。

- **リムーバブルメディアのデータの暗号化**: 軍事レベルの暗号化を使用してデータを保護する必要があります。導入はシステムとデータによって異なります。信頼性の高い保護には、単純で直接的な暗号化が必要不可欠です。暗号化が自動化されるため、エンドユーザーが意思決定する必要がありません。
  - » すべてのデータ: 多くのDLPソリューションでは、ルールを設定してリムーバブルメディアに転送するすべてのデータを自動で暗号化したり、ファイルの内容によって指定したファイルのみを暗号化することができます。さまざまな状況に対応するには、ユーザーがデバイスに接続したら自動的に暗号化されるようルールを設定します。
  - » データの選択: DLPソリューションでは、クレジットカード番号、HIPAA ICD9診断コードまたは「企業秘密」とラベル付けされたドキュメントなど、事前に設定したコンテンツのルールに基づいて暗号化されます。また、DLPソリューションによってタグ付けされたファイルがリムーバブルメディアにコピーされた場合、適切な暗号化ポリシーが適用されます。
  - » 企業所有の資産: 企業所有の資産でのみデータへのアクセスを許可する場合、ファイルレベルで暗号化することが推奨されます。暗号化ツールを使用して、リムーバブルメディアに転送するファイルを暗号化します。企業所有の資産でのみ、そのファイルを開くことを許可します。
  - » すべての資産: コンテナを使用して、リムーバブルメディアのデータを暗号化し、すべてのデバイスからのアクセスを許可します。この方法では、メディアはあらゆるデバイスに接続できますが、暗号のパスワードを持つユーザーだけがデータへのアクセスを許可されます。
- **ポリシーとツールに対するユーザーの受け入れ**: 自動で暗号化することによって、エンドユーザーのコンプライアンスに対する負担は大幅に軽減されます。また、DLPソリューションによってさまざまな情報が提供されます。DLPソリューションを使用すると、エンドユーザーがリムーバブルメディアに接続したとき、警告を発することができます。警告には、ユーザーの行為が監視されていることを示すメッセージ、または会社のリムーバブルメディアのポリシーへのリンクなどを使用できます。

マカフィーのソリューションで使用されているテクノロジー

マカフィーの提案するソリューションには、McAfee® Device Control、McAfee Data Loss Prevention Endpoint、McAfee Endpoint Encryption for Files and Foldersのオプションがあります。McAfee ePolicy Orchestrator®（McAfee ePO™）を単一の管理コンソールとして使用し、クライアントシステム上ではMcAfee Common Management Agentを単一のエージェントとして使用することで、アーキテクチャーが効率化されます。また、単一のエージェントを使用することで、クライアントシステムのリソース消費を最小化できます。



マカフィーが提供する保護では、一元管理によってリムーバブルメディアの使用に対するポリシーの適用が効率化されます。

McAfee ePolicy Orchestrator

これは、ポリシーと管理のためのプラットフォームです。このプラットフォームを使用して、クライアントシステムでMcAfee Data Loss Prevention EndpointとMcAfee Endpoint Encryption for Files and Foldersのソフトウェアを設定し、ポリシーを適用します。単一のコンソールを使用して、クライアントにマカフィーのソフトウェアをインストールして管理できます。この2つのソリューションだけでなく、マカフィーの他のエンドポイントソフトウェアのレポートやアラートを作成する機能も備えています。また、コンプライアンスに関するレポートとアラートの作成を自動化できます。たとえば、McAfee ePOコンソールからユーザーのリムーバブルメディアの内容と暗号化に関するレポートを作成できます。このレポートはデバイス紛失時に役立ちます。

McAfee Data Loss Prevention Endpoint

McAfee Data Loss Prevention Endpoint（DLP Endpoint）では、機密情報の配布を管理します。クライアントマシンにこの製品がインストールされますが、コンポーネントには、McAfee Device Controlが統合されています。McAfee Device Controlを使用すると、会社所有のシステムのリムーバブルメディアにユーザーがアクセスするのを防止できます。たとえば、CD書き込み用アプリケーションへのアクセスを制限できます。また、データの内容によって、システムからの機密データの持ち出しを監視またはブロックするには、McAfee DLP Endpointを使用します。McAfee DLP Endpointでは、データのタイプとその機密性に合わせてルールを設定できます。たとえば、クレジットカード番号のファイルをリムーバブルメディアにコピーするのを防止する場合に使用します。この製品には、リムーバブルメディアの制御以外にも優れた機能があります。制御のルールと内容別のルールは、Webベースやクライアントベースの電子メールアプリケーションでのファイルの配布など、他のメディアにも適用できます。また、すべてのルールはデータのブロックまたは監視に設定できます。アプリケーションはウィザードを使用して、簡単に導入できます。

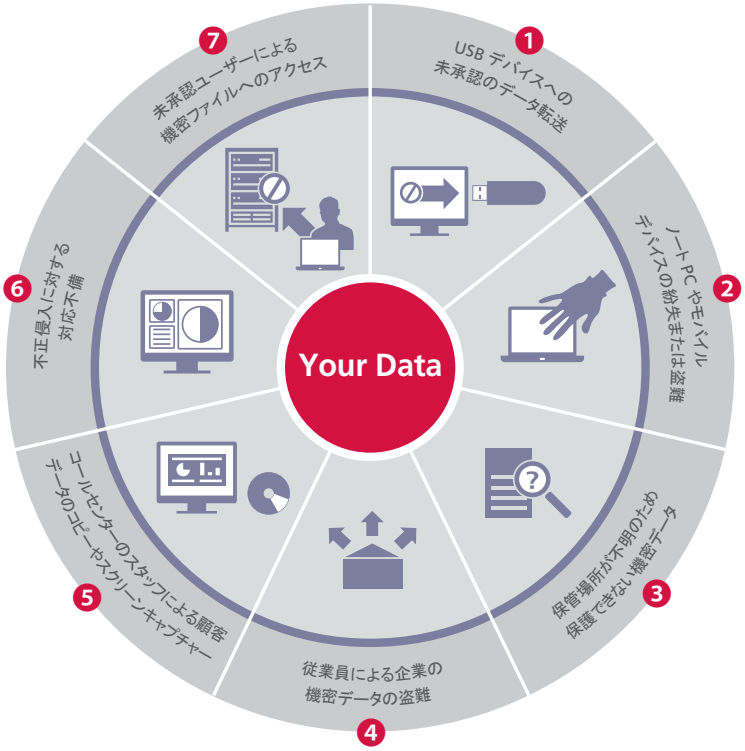
McAfee Endpoint Encryption for Files and Folders

McAfee Endpoint Encryption for Files and Foldersでは、市販のリムーバブルメディアがソフトウェアによって暗号化されます。リムーバブルメディアにコピーするデータの暗号化ポリシーは簡単に設定できます。また、ポリシーによって、会社所有のデバイス（ノートPCなど）のみ、またはすべてのデバイスでデータにアクセスできます。この自動のアプローチの代わりに、ユーザーがリムーバブルメディアを挿入したら、暗号化するかどうかを質問する設定も行えます。「はい」を選択すると、パスワードの入力が求められ、入力したパスワードが検証されます。「いいえ」を選択すると、デバイスが読み取り専用モードになり、機密データはデバイスにコピーされません。

導入効果

マカフィー製品では、リムーバブルメディアの使用に対するユーザーのニーズに対応しながら、データも保護できます。1つのコンソール、1つのエージェントで構成されるソリューションによってユーザーのニーズの正当性を監査および把握してから、ポリシーと自動化された管理によってユーザーコミュニティが受け入れやすく、一貫性のある保護が提供されます。また、柔軟な暗号化オプションによって、データを保護しながら、ユーザーはシステムの種類や場所を幅広く選択できます。

マカフィーは一元管理を通して導入、ポリシー管理、可視化、レポート、アラートのコスト削減に貢献します。マカフィー製品を使用すると、複雑な組織に最適なUSB管理を実践できます。



さまざまな方法で起こるデータ漏えいを防止するため、マカフィーのソリューションではポリシーを使用して適切な管理を可能にします。

追加情報

www.mcafee.com/japan/products/epolicy_orchestrator.asp
www.mcafee.com/japan/products/endpoint_encryption.asp
www.mcafee.com/japan/products/data_loss_prevention.asp

＊本書は 2012 年 10 月時点での情報です。仕様等の変更が生じる場合や、一部、日本未発売の製品も含まれています。詳細はお問い合わせください。

著者について

Bruce A. Boyd はマカフィーの上級セールスシステムエンジニアです。専門分野はデータ漏えい防止、ファイアウォール、フォレンジックおよび暗号化です。企業顧客に向けた情報セキュリティソリューションの提供と導入では 15 年を超える実績があります。北テキサス大学で経営管理の学士号を取得しています。1980 年代後半、scan.exe を手始めに、マカフィー製品に親しみ、EMC、RSA、3Com、Network Intelligence などの業界大手で実務経験を積んでいます。また、セキュリティプロフェッショナル認定資格（CISSP）を取得しています。

1『Information Week』（2011年8月8日）で引用：http://www.informationweek.com/news/storage/security/231300434

McAfee An Intel Company
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　〒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

MCABP-SYRM-1210-MC