

McAfee Data Protection

マカフィー データ プロテクション

情報漏えいに対する包括的な防御と社内コンプライアンスの強化



McAfee®

守るべきは、システムですか？
情報ですか？

リスクへの意識も高く、対策もとられているのに、なぜ情報は漏えいするのでしょうか。

それは現状の対策そのものに問題があるから。現在の多くの情報漏えい対策は、アクセス制御や不正侵入対策が主流。システムやネットワークにおける対策が中心で、実は本当に守るべき「情報」そのものは無防備に近い状態といえるのです。

マカフィーは、データ・セントリックプロテクション。情報そのものを守ります。

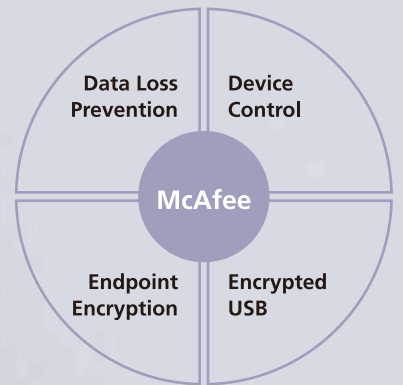
ノートPCに移され自宅で作業する。電子メールで送られ取引先で使用される…ビジネスにおいて、情報は「動く」もので、社内システム内のみにあるとは限りません。だから、漏えい対策はシステムではなく、「データ中心(データ・セントリック)」に行われる必要があります。それがマカフィーの情報漏えい対策。情報を、「静止中のデータ」「移動中のデータ」「使用中のデータ」に分類し、利用・保存・アクセスの方法・保管場所に関係なく守ります。

静止中のデータ	移動中のデータ	使用中のデータ
デスクトップ	電子メール	USBメモリ
ノートブック	Webメール	CD / DVD
データベース	IM / チャット	iPod
メールアーカイブ	ブログ	外付けハードドライブ
ファイル共有	ファイル共有	プリントアウト
文書管理システム		

Icons: Server, Desktop, Laptop, Internet, Envelope, Printer, USB

社内外のデータを守るテクノロジーをリンク。情報漏えい事前・事後対策を提案します。

McAfee Data Protectionは、PC上に格納されている重要情報の洗い出しやポリシー作成・適用、データへの制限／監視から、モバイル環境下でのデバイス制限、暗号化までを網羅。製品間の高度な連携を実現し、包括的な視点で「動く」データに対応します。



McAfee Data Protection

真の情報漏えい対策は、データ保護の観点に立った事前・事後対策にあります。

McAfee Data Protectionは、データの扱い方を考慮した制限や監視などによる事前対策と、暗号化することでデータを保護し、持ち出された後のリスクを軽減する事後対策を提供。信頼性の高い情報漏えい対策を実現します。

McAfee Host Data Loss Prevention

「タグ」をつけることで、社内のあらゆるデータを監視・制御。不正利用を防ぎます。

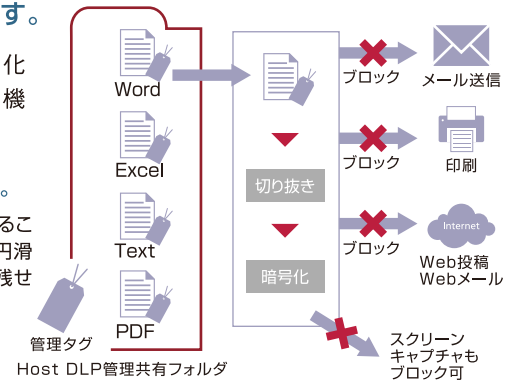
情報そのものに「タグ」と呼ばれる認識コードをつけることで、通常情報はもちろん、圧縮・暗号化された情報、加工された情報など、ビジネスで使われるあらゆるデータを保護。詳細なログ解析機能と相まって、情報の不正利用を防止します。

PC内の未知のデータも検出、ルールを適用。

PC内の「どこに」「どんな」データがあるかを自動で検出し、最適な保護ルールを適用することが可能。導入時の負荷軽減はもちろん、データの把握というコンプライアンス強化にも貢献します。

データのブロックを解除することも可能。

データ使用時に、使用者が理由の正当性を入力することで、ブロックを解除することが可能。ビジネスの円滑性を妨げることはありません。もちろんログとして残せるので監視・管理体制も万全です。



McAfee Device Control

エンドポイントへの接続を監視し、許可されたデバイスだけに接続を許可。無断コピーによる流出を防ぎます。

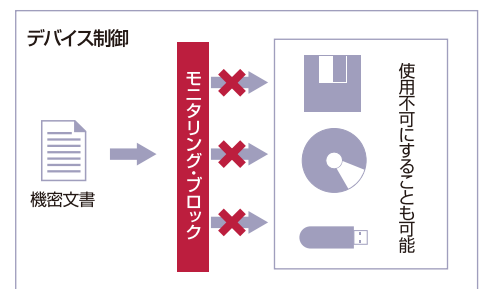
社内のホストに配備されたエージェントがデバイスの使用を自動的に監視することで、設定されたポリシーに違反するデバイスの使用やデータ転送をブロックします。ポリシーの設定や操作ログは集中管理されるため、運用管理も容易です。 ※本製品の機能は、McAfee Host Data Loss Preventionにも含まれています。

デバイスへの不正転送をブロック。

リムーバブルストレージの全面使用不可、指定デバイスのみ使用可といった指定が可能。さらに転送できるデータ、利用できるユーザについても各種制御を実施することもできます。

詳細なログで監査ニーズにも対応。

リムーバブルストレージへの転送に関わる行為は、ユーザおよびデバイスレベルで詳細にログ収集が可能。監査とコンプライアンスのニーズにも的確に応じることができます。



McAfee Endpoint Encryption

強力な暗号化とアクセス制御ですべてのデータを保護。持ち出し後のデータの不正利用を防ぎます。

デスクトップPCからノートPCにいたるまで、ディスク丸ごとまたはファイル・フォルダ単位での暗号化を実現。盗難・紛失時もデータの機密性が保たれ、情報の流出が防げます。また暗号化することでセーフハーバーにも対応できます。 ※モバイルデバイスでのご使用は、個別対応となります。

高度な暗号化と強固なユーザ認識。

FIPS 140-2やEAL 4などの高度な暗号化技術に対応。データの持ち出し後や紛失・盗難時の情報の拡散を防止し、ハイレベルな信頼性を提供します。

有効なコンプライアンス体制を確立。

「高度な暗号化等の秘匿化」が施せるため、個人情報保護法などのセーフハーバーに対応。漏えいに伴う信用やブランドの失墜を回避することが可能です。

ディスク暗号

- ハードディスク上のすべてのデータを暗号化。
- ユーザは暗号化されていることを意識する必要がないため、ユーザの意識や操作にセキュリティ強度が左右されない。

ファイル・フォルダ暗号

- 任意のフォルダやファイルを選択して暗号化できるため導入が容易。
- 電子メールによる取引先へのデータ送付など、社外へ持ち出す必要のある情報が第三者に漏えいするのを防止。

McAfee Encrypted USB

暗号化とアクセス制御でストレージメディアの安全を確保。メディアを介して転送されるデータを保護します。

外部ストレージメディア使用時、メディアにデータをコピーした時点で自動的に暗号化。メディアを介して転送される機密データを保護し、アクセス権のある利用者にも読み取りを許可します。

移動中のデータの機密性を確保。

AES 256、FIPS 140-2など、業界をリードする暗号アルゴリズムおよび認証に対応。また、パスワードと指紋による認証で、第三者による不正使用を防御。

USBポートに差し込むだけで利用可能。

オペレーティングシステムから独立したセキュリティを提供。ソフトウェアのインストールや管理者権限は必要ないため、柔軟な導入が可能です。



McAfee Endpoint Encryptionの認証デバイスとしても利用可能

製品名	情報漏えい対策				暗号化			統合管理
	メール/ Web投稿	コピー& ペースト	印刷制御	デバイス制御	フルディスク 暗号	ファイル・ フォルダ暗号	暗号化USB	
McAfee Total Protection for Data	McAfee Host Data Loss Prevention	●	●	●	●			●
	McAfee Device Control ^{*1}				●			●
	McAfee Endpoint Encryption for Devices					●		●
	McAfee Endpoint Encryption for Files and Folders						●	●
McAfee Encrypted USB							●	● ^{*2}

※1 本製品の機能は、McAfee Host Data Loss Prevention にも包含されています。 ※2 個別対応となります。

防御とコンプライアンスの管理を一元化。ユーザのリスクを軽減します。

マカフィーは、ITインフラの効果的なリスク管理プロセスを構築します。McAfee ePolicy Orchestrator によって資産の把握からリスクの選別、対策実施、そして事後評価に至るまで、すべてのマカフィー製品を一元的に管理。複数のセキュリティシステムのログやレポートを統合管理することができ、企業としてのセキュリティポリシーの更なる徹底を実現します。



最新情報はこちらをご覧ください http://www.mcafee.com/japan/products/total_protection_for_data.asp

●製品、サービスに関するお問い合わせは下記へ



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 中東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 〒810-0801 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

McAfeeの英文/和文社名、各商品名、ロゴはMcAfee, Inc. またはその関連会社の商標または登録商標です。本書中のその他の登録商標及び商標はそれぞれの所有者に帰属します。©2009 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合せください。●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。

McAfee Data Protection

システム要件

情報漏えい防止ソリューション

McAfee Host Data Loss Prevention

※ McAfee Host Data Loss Prevention v3.0

■ McAfee ePolicy Orchestratorサーバ	
CPU	Intel Pentium 4 2.8GHz
メモリ	最低1GB(2GB推奨)
HDD(空きディスク容量)	最低80GB
OS	Windows Server 2003 Standard(SE)SP1以降 Windows Server 2003 Enterprise(EE)SP1以降
データベース	Microsoft SQL Server 2005、Microsoft SQL Server 2005 Express Edition

■ エンドポイントのデスクトップ、ノートPC	
CPU	Intel Pentium III 1GHz以上
メモリ	最低512MB(1GB推奨)
HDD(空きディスク容量)	最低200MB
OS	Windows 2000 Professional SP4以降 Windows XP Professional(32ビット)SP1以降 Windows Vista Enterprise(32ビット) Windows Vista Business(32ビット)
ネットワーク接続	TCP/IPによるリモートアクセス

リムーバブルメディア利用制限ソリューション

McAfee Device Control

※ McAfee Device Control v3.0

■ McAfee ePolicy Orchestratorサーバ	
CPU	Intel Pentium 4 2.8GHz
メモリ	最低1GB(2GB推奨)
HDD(空きディスク容量)	最低80GB
OS	Windows Server 2003 Standard(SE)SP1以降 Windows Server 2003 Enterprise(EE)SP1以降
データベース	Microsoft SQL Server 2005、Microsoft SQL Server 2005 Express Edition

■ エンドポイントのデスクトップ、ノートPC	
CPU	Intel Pentium III 1GHz以上
メモリ	最低512MB(1GB推奨)
HDD(空きディスク容量)	最低200MB
OS	Windows 2000 Professional SP4以降 Windows XP Professional(32ビット)SP1以降 Windows Vista Enterprise(32ビット) Windows Vista Business(32ビット)
ネットワーク接続	TCP/IPによるリモートアクセス

ディスク、ファイル、フォルダ暗号化ソリューション

McAfee Endpoint Encryption

※ McAfee Endpoint Encryption for Devices v5.1.8

■ 集中管理サーバ	
CPU	Intel Pentium 互換(Intel Pentium III 以上相当)
メモリ	最低512MB
HDD(空きディスク容量)	最低1GB
OS	Windows 2000、Windows Server 2003

※McAfee ePolicy Orchestratorを使用する場合、ePOのシステム要件に従います。

■ エンドポイントのデスクトップ、ノートPC	
CPU	Intel Pentium互換
メモリ	最低256MB
HDD(空きディスク容量)	最低30MB
OS	Windows Vista(32ビット/64ビット全バージョン) Windows XP Windows 2000
ネットワーク接続	TCP/IPによるリモートアクセス

※必要なHDDの空きディスク容量は、ローカライゼーションとデバイス数によって変動します。

※Windows Mobileエンドポイントのご使用は個別対応となります。

暗号化USB

McAfee Encrypted USB

■ McAfee ePolicy Orchestratorサーバ	
McAfee ePolicy Orchestrator version 4.0(patch 2)以降 McAfee Agent 3.6(patch 3)以降	

※システム要件は選択したデバイスによって異なります。

※McAfee ePolicy Orchestratorによる管理は個別対応となります。

■ Standard Driverless	
OS	Windows Vista Windows XP Windows 2000

■ Zero-Footprint及びハードディスク	
OS	Windows Vista Windows XP Windows 2000 Mac OSX