McAfee Data Loss Prevention Monitor

重要なデータを保護

社会保障番号、クレジットカード番号など、顧客と社員の個人情報を保護することは当然のことです。情報漏えいの原因として、社員の誤操作、ノートPCの紛失、USBデバイスの置き忘れなどがありますが、これはどの組織でも起こりうる問題です。Google Gmail、Yahoo! Mail、インスタントメッセージ、FacebookなどのWebアプリケーションでデータを転送したり、共有したりしていると、情報が流出し、犯罪者の手に渡る可能性もあります。McAfee® Data Loss Prevention Monitor（McAfee DLP Monitor）は高性能なデータ損失防止ソリューションです。すべてのインターネット通信を分析し、不正または不適切な情報送信を自動的に識別します。これにより、セキュリティ担当者の負荷を軽減し、コンプライアンス要件を満たしながら、知的財産などの重要資産を保護できます。

送受信されるデータの監視、追跡、レポート

どの業種でも、アプリケーション、プロトコル、ポートなどを介して送受信される機密情報を高い精度で識別するには可視化が不可欠です。

McAfee DLP Monitorを使用すると、ネットワーク全体で移動中のデータをリアルタイムで収集・追跡し、レポートを作成できます。これにより、社内のユーザーと外部との間で送受信されている情報を確認できます。McAfee DLP Monitorでは、ポートやプロトコルで送受信されている300種類以上のコンテンツを高性能な専用アプライアンスで検出します。これにより、データに対する脅威を特定し、情報漏えいを防ぐアクションを実行できます。さらに、ユーザーが操作を変更できるように、データ保護違反をエンドユーザーに通知します。

主な特長

- **McAfee® ePolicy Orchestrator®（McAfee ePO™）と完全に統合:** 共通のポリシーを共有し、McAfee DLP Endpointのインシデント/ケース管理機能を実行。
- **高いパフォーマンスと拡張性:** 最大8台までのアプライアンスをクラスタリング。スキャン処理に6 Gbpsの帯域幅を使用。
- **包括的な分析:** 任意のポートやアプリケーションで300種類以上のコンテンツを検出。
- **使いやすい組み込みポリシー:** コンプライアンスから知的財産の適切な使用まで、様々なポリシーとルールを用意。

McAfeeとつながる

情報をリアルタイムでスキャンし、分析

McAfee DLP MonitorをSPANまたはタップ ポートでネットワークに統合すると、ネットワーク トラフィックをリアルタイムでスキャンし、分析できます。McAfee DLP Monitorには、コンプライアンスから知的財産の適切な使用まで、150以上のルールが事前に定義されています。これらのルールと文書全体または一部を比較して、情報の窃盗を識別します。また、ネットワークの規模に関係なく、異常なネットワーク トラフィックも検出します。

以前に特定できなかったリスクも検出

McAfee DLP Monitorでは、リアルタイム ルールに一致する情報だけでなく、すべてのネットワーク トラフィックが分類され、インデックスが作成されます。これらの履歴情報を利用することで、機密情報かどうかをすばやく識別し、情報の使用方法、利用者、送信先を特定します。きめ細かい調査を行うことで、これまで認識されていなかったリスク イベントやデータの露出を検出できます。McAfee DLP Discoverと一緒に配備すると、ネットワーク上でデータが保存されている場所と所有者も識別できます。

インシデント レポートとアクションの通知

McAfee DLP Monitorの分類エンジンがトラフィックをスキャンし、分析と分類が完了すると、すべての関連情報が専用のデータベースに格納されます。分かりやすいインターフェースを利用して、情報を検索したり、包括的なレポートを作成できます。これにより、情報の送信者、送信先、送信方法などを確認し、漏えいしている情報、場所、方法を特定できます。これらの情報を元に、コンプライアンスを強化し、機密情報を保護するために必要な対策を講じることができます。

仕様

- **システム スループット:** サンプリングを行わず、最大800 Mbpsでコンテンツを分類。
- **ネットワーク統合:** SPANポートまたは物理的なインライン ネットワーク タップのいずれかでネットワークをパッシブに統合（オプション）。
- **クラスタリング機能:** 最大8台のアプライアンスをクラスタ化、6 Gbpsのパフォーマンスを実現。
- **300種類以上のコンテンツを分類:**
  - Office文書
  - マルチメディア ファイル
  - P2P
  - ソースコード
  - デザイン ファイル
  - アーカイブ
  - 暗号化されたファイル
- **次のプロトコル ハンドラーに対応:**
  - FTP
  - HTTP
  - IMAP
  - IRC
  - LDAP
  - POP3
  - SMB
  - SMTP
  - Telnet

あらゆるデータを分類

McAfee DLP Monitorは様々な機密情報をスキャンします。一般的な定型データだけでなく、複雑な知的財産もスキャンできます。McAfee DLP Monitorはオブジェクト分類メカニズムを利用する高度な分類エンジンを搭載しています。これにより、機密情報のフィルタリングと検索を行い、隠れたリスクや新たなリスクを特定することができます。

オブジェクト分類メカニズムの特徴は次のとおりです。

- **多層的な分類:** コンテキスト情報と階層形式のコンテンツの両方に対応しています。
- **文書の登録:** 変更時に情報の署名を追加します。
- **文法分析:** テキスト文書からスプレッドシート、ソースコードまで、すべてのコンテンツで文法または構文を検出します。
- **統計分析:** 特定の文書またはファイルで署名、文法、バイオメトリクスが一致した回数を記録します。
- **ファイル分類:** ファイルまたは圧縮ファイルの拡張子に関係なく、コンテンツ タイプを識別します。

フォレンジックとルール調整機能

固有の収集機能により、独自の履歴データを利用して、より迅速で効率的な実装が可能になります。推測に基づく試行錯誤を何か月も行う必要はありません。また、ビジネスの中断も防ぐことができます。常に変化するビジネス要件に合わせてDLPルールを簡単に調整できます（分類の調整も可能）。この収集技術はフォレンジック調査にも役立ちます。デジタルレコーダーとして機能し、発生したDLPインシデントを再現して詳しい調査を実施できます。この収集技術は仮想環境だけでなく、SASケーブルでNDLP 6600アプライアンスに接続した2U 16TBのストレージ アレイでも利用できます。

フォームファクタとアプライアンス オプション

McAfee DLP Monitorは、仮想アプライアンス オプション付きのハードウェア アプライアンスとして利用できます。詳細については、**McAfee DLP 6600ハードウェア アプライアンス データシート**をご覧ください。

McAfee Together is power.

〒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（代表）
www.mcafee.com/jp