

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、この問題はどの組織でも発生する可能性があります。Google Gmail、Yahoo! Mail、インスタントメッセージおよびFacebookのようなWebアプリケーションを介して転送や共有を行うと、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タイプ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McAfee DLP Monitorは、

ユーザーが動作を変更できるように、データ漏えい違反をエンドユーザーに通知します。

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、情報の窃盗を識別することができます。また、ネットワークの規模に関係なく、ネットワークトラフィックの異常も検出できます。

主な特長

- 重要な情報の識別と保護：
 - 使いやすい検索エンジンで機密情報をすばやく特定できます。
 - フォレンジック分析により、現在と過去のリスクイベントを関連付け、リスクの傾向と脅威を識別できます。
 - ルールを迅速に作成し、以降の動作を未然に防ぎます。
- 完全に統合したMcAfee® ePolicy Orchestrator® (McAfee ePO™) ソフトウェア。
- McAfee ePO ソフトウェアによって完全に管理することができるので、McAfee DLP Endpointで共通ポリシー、インシデントおよびケース管理を共有し、高度なルールの作成および調整ができます。
 - 任意のポートやアプリケーションで使用される300種類以上のコンテンツタイプを識別します。
 - ネットワークトラフィックとポートの依存関係を分類します。
 - 数十万の同時接続に対応できます。

データシート

以前に特定できなかったリスクの検出

McAfee DLP Monitorを使用すると、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、送信先を特定できます。また、きめ細かい調査を行うことで、これまでは認識されていなかったリスクイベントと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、ネットワーク上でのデータの保存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

分類エンジンがトラフィックをスキャンし、分析と分類を行うと、McAfee DLP Monitorはすべての関連情報を専用のデータベースに格納します。分かりやすい検索インターフェースを使用して、包括的なレポートを参照できます。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維持し、機密情報を保護するために様々なアクションを実行できます。

仕様

システム スループット: サンプルングを行わず、最大200 Mbpsでコンテンツを分類します。

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します (オプション)。

ファイル分類で300以上のコンテンツ タイプをサポートしています:

- Microsoft 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

データシート

あらゆるデータを分類

McAfee DLP Monitorを使用すると、様々な機密情報をスキャンできます。決まった形式の一般的なデータだけでなく、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正確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:** 情報にバイオメトリクス署名を使用します。

- **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。

フォームファクタおよび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** をご参照ください。

仕様、続き

対応プロトコル

- トランスポートプロトコルとしてTCPを使用する任意のプロトコルまたはポート経由での送信に対応しています。
- HTTP, HTTPS, SMTP, IMAP, POP3, FTP, Telnet, Rlogin, SSH, webmail, Yahoo! Chat, AOL Chat, MSN Chat, ICY, RTSP, SOCKS, PCAnywhere, RDP, VNC, SMB, Citrix, Skype, IRC, LDAP, DASL, NTLM, Kazaa, BitTorrent, eDonkey, Gnutella, DirectConnect, MP2P, WinMX, Sherlock, eMuleなどのプロトコルハンドラーを搭載しています。

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が用意されています。
- McAfeeの収集データベースを利用して、ビジネス固有の要件に合わせてルールをカスタマイズできます。



〒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

McAfee、McAfeeのロゴ、ePolicy Orchestrator、McAfee ePOは米国法人McAfee, LLC または米国またはその他の国の関係会社における登録商標または商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。Copyright © 2017 McAfee, LLC. 3002_0517
2017年5月