McAfee DLP Prevent

ポリシーを施行して重要な情報を保護

情報を電子的に共有するユーザーが増えるにつれ、企業の機密情報が流出し、危険に晒されるリスクが高まっています。社内の情報はメール、Web、インスタント メッセージング（IM）、FTPなど、様々な経路で外部に送信されています。メッセージの送信を許可する場合でも、暗号化を行い、データの機密性を保護しなければなりません。それ以外の通信は承認せず、常にブロックする必要があります。データのセキュリティとコンプライアンスを維持し、知的財産を保護するには、適切なポリシーを的確なタイミングで施行することが重要です。

移動中のデータに対するセキュリティ ポリシーの施行

会社の部門間では、データの共有に複数のアプリケーションやプロトコルが使用されています。外部に送信される機密情報をプロアクティブに保護し、適切なビジネス プロセスを実施することで、不注意や故意によるデータ漏えいを防ぐ必要があります。

McAfee® DLP Preventを使用すると、SMTP（Simple Mail Transfer Protocol）またはICAP対応のWebプロキシを使用するメッセージ転送エージェント ゲートウェイを統合し、メール、Webメール、IM、Wiki、ブログ、ポータル、HTTP/HTTPS、FTP転送でネットワークから送信される情報にポリシーを施行できます。McAfee DLP Preventでは、ポリシー違反の検出時に暗号化の適用、ブロック、リダイレクト、隔離など、様々なアクションを実行できます。これにより、機密情報の保護に関する法規制を遵守し、セキュリティ脅威のリスクを軽減できます。

McAfee ePolicy Orchestrator（ePO）との完全な統合

McAfee DLP Preventは、McAfee® ePolicy Orchestrator®（McAfee ePO™）と完全に統合されています。McAfee® Data Loss Prevention Endpoint（McAfee DLP Endpoint）と同じポリシーを使用し、インシデント/ケース管理を行うことができます。McAfee ePOで1つのメール/Web保護ポリシーを作成して、エンドポイントとネットワークに配布できます。また、McAfee DLP EndpointとMcAfee DLP Preventは共通の分類エンジンを使用するので、同じメール/Webポリシー

主な特長

既存のインフラの利用

- メッセージ転送エージェント（MTA）ゲートウェイを統合し、会社のメールを保護します。SMTPでXヘッダーを使用し、ブロック、バウンス、暗号化、隔離、リダイレクトを行います。
- ICAP（Internet Content Adaptation Protocol）対応のWebプロキシと統合してトラフィックを規制することで、HTTP、HTTPS、IM、FTP、Webメールのコンテンツ違反をブロックします。

様々な情報に対してポリシーをプロアクティブに施行

- 300種類以上のコンテンツ タイプを保護できます。
- 重要性が分かっている情報にだけポリシーを施行するのでは十分な対策とは言えません。
- 数十万の同時接続に対応できます。

McAfeeとつながる

を共有できます。同じ辞書と正規表現構文を使用して、共通のWeb/メール保護ルールを作成できます。McAfee DLPソリューションを一元管理できるので、作業効率が向上し、管理コストを軽減できます。

モバイル メールの監視

モバイル メール用のMcAfee® DLP Preventは、モバイル デバイスにActiveSyncプロキシ経由でダウンロードされるメールを傍受し、DLPの機能でモバイル メールのコンテンツを識別して保護します。さらに、オンプレミスのMicrosoft ExchangeとMicrosoft Office 365 Hosted Exchangeの両方でActiveSyncを傍受します。この機能はMcAfee DLP Preventのライセンスに含まれ、McAfee ePOから完全に管理できます。モバイル デバイスにエージェントをインストールする必要はありません。モバイル メール用のMcAfee DLPを使用すると、メールのコンプライアンス状態を確認し、証拠を収集できるので、管理対象だけでなく、管理対象外のモバイル デバイスも保護できます。

Webプロキシ、MTAとの統合で保護を強化

McAfee DLP Preventは、Webプロキシ（ICAP）とMTA（Xヘッダー）を使用して、必要なアクションを実行します。TCPセッションをドロップせずにアプリケーション レイヤーで未承認のトランザクションを終了するので、アプリケーションの動作は変更されません。アプリケーションがポリシー違反で拒否されたトランザクションを開始しようとすると、McAfee DLP Preventがアラートを生成します。McAfee DLP Preventが保護対象を学習し、同じ動作の再発を防ぐため、組織のデータ保護が強化されます。

既知または未知の機密情報を保護

McAfee DLP Preventは、300種類以上のコンテンツ タイプを分類できます。これにより、社会保障番号、クレジットカード情報、財務データなどの重要な情報を保護できます。また、複雑な知的財産など、保護が必要な情報や文書も特定できます。McAfee DLP Preventでは、コンプライアンス対応、知的財産の利用方法などの様々なポリシーで文書全体または一部をルールと比較することで、まだ保護していない重要な情報も保護できます。

カスタマイズ可能なビューとインシデント レポート

McAfee ePOにより、2つのコンテキスト ピボット ポイントに基づいて、セキュリティ インシデントとアクションのサマリー ビューをカスタマイズできます。サマリー ビューで傾向を表示するだけでなく、リストや詳細ビューも簡単に表示できます。McAfee DLP Preventには、非常に多くの事前定義レポートが用意されています。これらのレポートは、保存して後で参照したり、定期的に配布することもできます。

重要なデータを分類、分析し、データ漏えいを防止

- 機密情報のフィルタリングと制御により、未知のリスクも検出できます。
- すべてのコンテンツ タイプにきめ細かいセキュリティ ポリシーを設定し、施行できます。
- 内部のファイル共有アクセスにポリシーを適用し、情報やリポジトリに対する未承認のアクセスを阻止します。

仕様

システム スループット

最大150 Mbpsのスループットで、フルコンテキスト分析、インデックス生成、データ保存を実行します。

ネットワーク統合

MTAやICAPに対応のWebプロキシを使用して、データパス内で有効な外部アプライアンスとしてネットワークに統合できます。

コンテンツ タイプ

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

複雑なデータの分類

McAfee DLP Preventを使用すると、様々な機密情報を保護できます。決まった形式の一般的なデータだけでなく、複雑な知的財産も保護できます。McAfee DLP Prevent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、機密情報の送信をブロックし、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のオプション

McAfee DLP Preventは、ハードウェア アプライアンスまたは仮想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。

- デザイン ファイル
- アーカイブ
- 暗号化されたファイル

対応プロトコル

ICAP対応プロキシに対して、ICAPプロトコル経由でHTTP、HTTPS、FTP、IMプロトコルをサポートしています。プロキシで使用可能なプロトコルについては、プロキシの提供元に確認してください。MTAとの統合により、SMTPをサポートします。

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