McAfee Data Loss Prevention Endpoint

データ漏えいを防ぎましょう

知らないうちにデータが盗まれていませんか？顧客情報、知的財産、財務データ、個人用のファイルが外部に流出しているかもしれません。侵入者はハッカーだけとは限りません。従業員の不注意で情報が漏えいしている可能性もあります。故意かどうかにかかわらず、データ漏えいはメール、Webへの送信、USBドライブ、クラウドへのアップロードなど、あらゆる経路で発生する可能性があります。また、漏えいによる被害は甚大なものになります。毎日多くの企業で大規模なデータ漏えいが発生しています。データ漏えいを簡単かつ効率的に阻止する方法はないのでしょうか。企業や政府のコンプライアンスを満たすと同時に、知的財産を保護する方法はないのでしょうか？このような課題を解決するのがMcAfee® Data Loss Prevention Endpoint（McAfee DLP Endpoint）です。

デバイスからクラウドまでを網羅するDLP

McAfee DLP Endpoint は、MVISION Cloud DLP と統合されています。オンプレミス向けの DLP ポリシーは、クリック 1 回の簡単操作で 1 分以内に高速でクラウドに拡張できます[1]。オンプレミスのDLP分類タグがクラウドのDLPポリシーと共有されるため、一貫したデータ漏えい検出を実現できます。

高度な保護能力

McAfee DLP Endpointは、リムーバブル ストレージ デバイス、クラウド、メール、インスタント メッセージング、Web、印刷、クリップボード、スクリーン キャプチャ、ファイル共有アプリケーションなど、漏えいの可能性のあるすべてのチャネルを保護する包括的なセキュリティ対策を提供します。

主な特長

- **デバイスからクラウドまでを網羅するDLP:** オンプレミスのDLPをクラウドに簡単に展開し、一貫したデータ漏えい検出を実現。
- **高度な保護能力:** フィンガープリンティング、分類、タグ付けにより、知的財産や企業秘密などの重要な非構造化データを保護します。
- **集中管理:** McAfee® MVISION ePolicy Orchestrator® (MVISION ePO™) ソフトウェアとの統合により、ポリシーおよびインシデント管理が合理的にできます[2]。
- **コンプライアンスの維持:** メールの送受信、クラウドへの送信、リムーバブル メディアへのダウンロードなど、ユーザーの日々の操作を監視し、コンプライアンスを維持します。
- **ユーザー教育：**ポップアップでリアルタイムにフィードバックを表示し、セキュリティ意識を高め、企業の方針を共有できるようにします。

McAfeeとつながる

McAfee DLP Endpointキーの機能は次のとおりです。:

- 送受信中のデータに Microsoft Azure Information Protection (AIP) ラベルを付け、AIP ラベルの付いたファイルを認識する機能を提供します[3]。
- サードパーティのユーザー動作分析（UEBA）との統合で内部の脅威を阻止します。セキュリティ分析により、ユーザーやエンティティによる異常な動作とリスクの高い動作を検出します。
- 手動分類 ― エンドユーザーが手動で文書を分類し、従業員にデータ保護の意識付けを行い、管理作業を軽減できます。
- ユーザーによるスキャンと修復の開始にって、ユーザーがエンドポイントの検出スキャンを実行し、修復作業を行うことができます。
- ディクショナリ、正規表現と検証アルゴリズム、登録文書、サードパーティのユーザー分類ソリューションのサポートなど、柔軟な分類が可能になりました。
- 起源に基づいた文書を識別するための一意のタグ付けの技術により、Web アプリケーション、ネットワーク アプリケーション、ネットワーク共有からの重要な情報の複製、名前の変更、または組織外への送信を阻止できます。
- 高度な可視性により、リモート デスクトップと仮想デスクトップインフラストラクチャ(VDI) ソリューションを保護します。

集中管理

- クラウドネイティブの管理コンソールである MVISION ePO で管理するため、ポリシーおよびインシデント管理を効率化できます[4]。
- McAfee® MVISION Cloud（CASB）、McAfee® Network DLP と同じポリシー、分類エンジン、インシデント ワークフローを共有します。
- 複数のポリシーと再利用可能なルール セットを使用して、組織全体に複数のDLPポリシーを定義したり、事務所、部門、法規制などに応じてポリシーを作成することができます。
- インシデント管理の柔軟性が向上しました。インシデント プロパティ（デバイスのシリアル番号、エビデンス ファイルの名前、グループなど）ごとにクエリー、フィルタリング、表示を行うことができます。
- イベント管理と監査を一元的に行うことができます。
- ポリシー管理やインシデント レビューで、役割ベースのアクセス制御（権限の分担）が改善されました。
- ヘルプ デスクのインターフェースに簡単にアクセスできます。

対応プラットフォーム

- Windows 10（32ビット/64ビット）
- Windows 8、8.1（32ビット/64ビット）
- Windows 7（32ビット/64ビット）
- Windows Server 2019
- Windows 2016（64ビット）
- Windows 2012（64ビット）、Windows 2012 R2（64ビット）
- Windows 2008（32ビット/64ビット）、Windows 2008 R2（32ビット/64ビット）
- macOS Catalina 10.15以降
- macOS Mojave 10.14以降
- macOS High Sierra 10.13以降
- macOS Sierra 10.12以降
- OS X El Capitan 10.11以降
- OS X Yosemite 10.10以降
- OS X Mavericks 10.9.0以降

対応ブラウザー

- Internet Explorer 11以降
- Mozilla Firefox 48以降
- Google Chrome 65以降

コンプライアンス強制の維持とエンドユーザーの教育

組織の境界が曖昧になっている現在、企業にとってコンプライアンスの維持は難しい課題になっています。McAfee DLP Endpointは、日々のユーザーの操作を監視するだけでなく、ユーザーの教育を行い、コンプライアンス対応を支援することもできます。ボタンをクリックすると、McAfee DLP Endpointが監査担当者、上級管理者、コンプライアンス対応の関係者に詳細なレポートを送信します。また、テンプレート化された法規制とユースケースに関するポリシーにより、コンプライアンスを簡単に維持することができます。ユーザーがポリシーに違反する操作を行うと、ポップアップが表示され、フィードバックがリアルタイムで提示されます。これにより、セキュリティに対する意識を向上させ、セキュリティに対する企業文化を高めることができます。

サポートされるMcAfee ePO

- McAfee ePO 5.9.1、5.10（DLP 11.1以降）

McAfee MVISION ePO のサポート (SaaS)

- DLP 11.5 以降については、ソフトウェアまたは DLP 拡張機能のインストールは必要ありません。MVISION ePO にアクセスするには認証用のユーザ名とパスワードが必要です。

サポートされるプラットフォーム、ブラウザー、ソフトウェアの詳細については、McAfeeナレッジベースをご覧ください。

詳細を見る

詳細については、www.mcafee.com/dlp-endpointをご覧ください。

1. **McAfee社内ラボでのテスト結果に基づく**
2.McAfee DLP Endpoint バージョン 11.5 以降
3.同上
4.同上

〒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 © 2020 McAfee, LLC. 4456_0520
2020年5月