# McAfee Data Loss Prevention Monitor

## 重要なデータを保護する

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 メッセンジャー、FacebookなどのWebアプリケーションで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（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。

### 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、以降の動作を防止します。

**すべてのネットワーク トラフィックの収集とインデックスの作成**

- 機密情報のフィルタリングと制御により、隠れたリスクや新たなリスクを特定します。
- すべてのコンテンツにインデックスを作成します。クエリーで機密情報とその送信先を検索できます。
- ファイル共有に対する内部アクセスを監視します。

**高度なルールの作成と調整**

- 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。

### 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、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。McAfee DLP Monitorは、ユーザーが操作を変更できるように、情報保護ルールに対する違反をエンドユーザーに通知します。

### リアルタイムでのスキャンと情報分析

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、情報の窃盗を識別できます。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。

### 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。

## 仕様

### システム スループット

- 最大200 Mbpsでコンテンツを分類（サンプリングなし）

### 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）

### 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

- 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

### 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
- HTTP、HTTPS、SMTP、IMAP、POP3、FTP、Telnet、Rlogin、SSH、Webメール、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

### 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可能

## 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から包括的なレポートを参照し、情報の送信者、送信先、送信方法などを確認して、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。

## 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。

## 仕様: McAfee DLP 5500 アプライアンス

| コンポーネント | 要件 |
|---|---|
| **プロセッサー** | Intel E5-2620 6コア x 2、15 MBのキャッシュ、2.0 GHz、7.20 GT/s Intel QPI |
| **メモリー** | 32 GB DDR3-1333 MHz |
| **電源** | 760Wホットスワップ電源モジュール x2 |
| **ハードドライブ** | 2 TB SATA 7.2K rpmドライブ x 8 |
| **NICカード** | Intel Dual Copper 1 Gbps Ethernet I/Oモジュール |
| **IPMI** | Intel Remote Management Modules 4（AXXRMM4） |
| **製品サイズ** | 2ラック ユニット（2U） |

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。

**McAfee. Part of Intel Security.**

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

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

名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F
TEL 052-551-6233（代） FAX 052-551-6236

福岡営業所　〒810- 0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F
TEL 092-287-9674（代）

www.intelsecurity.com

Intel、Intelのロゴ、McAfeeのロゴは、米国法人Intel Corporation、McAfee, Inc.もしくは米国またはその他の国の関係会社における商標です。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 © 2016 Intel Corporation.568_0716