McAfee Data Loss Prevention Discover

重要なデータを識別・分類して保護する

ノートPC、共有ファイル サーバー、クラウド ストレージに存在する機密情報が組織を脅かす危険性があります。保護する情報はテラバイト、ペタバイト規模の膨大なものとなります。機密情報にラベルが付いているとは限りません。大半の組織では、アクセス制御を導入していても、機密情報が危険な状態かどうか確認したり、存在場所を把握する手段がありません。通常、機密情報は構造化されていないデータから構成されています。知的財産（IP）などは、クレジットカードや社会保障番号などの構造化データのように簡単に定義できません。McAfee® Data Loss Prevention（DLP）Discoverを使用すると、機密情報を簡単に識別・分類し、使用状況を確認して窃盗や漏えいを未然に防ぐことができます。

主な特長

情報漏えいのリスクを識別

- オンプレミスとクラウドに保存された情報をスキャンします。
- 機密データの保存場所とコンテンツの所有者を特定します。
- 分かりやすいインターフェースからスキャン済みのデータを検索して、表示できます。

ポリシーとカスタム レポート

- クエリーの結果から保護ルールを作成できます。
- コンプライアンス、コーポレート ガバナンス、知的財産に関するポリシーが事前に定義されています。
- 他の情報セキュリティ システムに機密情報を登録できます。

情報漏えいの分類、分析、修復

- 複数の分類基準で機密情報をフィルタリングし、管理します。
- すべてのコンテンツにインデックスを作成します。クエリーで機密データを検索できます。
- 署名を登録して生成し、文書とその情報を窃盗や改ざんから保護します。
- コンテンツが保護ポリシーに違反すると、アラート通知を送信します。

McAfee DLP Discoverの新機能

新しいMcAfee DLP Discoverでは、クラウド ストレージ（Box）にあるデータをスキャンし、保護できるようになりました。集中管理プラットフォームであるMcAfee ePolicy Orchestrator®（McAfee ePO™）でポリシーを簡単に定義し、スケジュールに従って自動的にスキャンを実行できます。インシデントに関する特別なレポートや詳細な分析結果も利用できます。

ハイライト:

- McAfee DLP Discoverはソフトウェアのみで利用できます。ハードウェアやVMベースのアプライアンスを用意する必要はありません。コストをさらに削減できます。
- McAfee ePOから配備し、管理できます。DLP Endpointと同じ管理機能とDLPポリシーを共有します。
- DLP Endpointの分類機能に完全に対応しています。
- Windows Server 2008とWindows Server 2012に対応しています。
- 既存サーバーの空き容量を利用して分散配備が可能です。地理的に離れた場所にも配備できます。
- DLP Discoverアプライアンス バージョン9.3.xまたはDLP Discoverソフトウェア専用バージョン9.4のライセンスを使用できます。

仕様

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。

- Boxクラウド ストレージ
- Microsoft Office文書
- マルチメディア ファイル
- 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
- 組み込みポリシー
- 知的財産

対応リポジトリ

- CIFS（Common Internet File System）/SMB（Server Message Block）[1]
- Network File System（NFS）
- HTTP/HTTPS
- FTP/FTPS
- Microsoft SharePoint[1]
- EMC Documentum
- データベース: Microsoft SQL、Oracle、DB2、MySQL Enterprise

文書登録

任意のリポジトリの文書を登録できます。登録文書の署名をローカルで使用し、機密情報の存在場所を特定したり、他のMcAfee DLPアプライアンスで使用できます。

レポート

インシデントと検索結果を処理する強力な分析エンジンにより、2つのピボット ポイントに基づいてサマリー 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使用できます。カスタマイズ可能な20以上のレポートが事前定義されています。

機密情報の漏えい回避

ソースコード、ビジネスの上の機密、事業計画、知的財産、その他の情報資産は、会社のブランドや評判、競争力に大きな影響を及ぼします。移動中のデータを保護することも重要ですが、機密情報の存在場所を把握し、不正にアクセスされたり、許可なく移動される前に機密情報を保護することが防御の第一歩となります。

McAfee DLP Discoverを使用すると、情報漏えいから組織を保護することができます。これまでのソリューションは、保護すべきコンテンツをユーザー自身が把握しておく必要がありました。McAfee DLP Discoverは様々な形式の情報に対応し、機密情報を識別します。

保護する情報の識別

McAfee DLP Discoverでは、機密情報に対するリスクを識別するため、スキャンするリポジトリを指定して明示的に保護することもできます。McAfee DLP Discoverが収集したデータにはすべてインデックスが作成され、分かりやすいインターフェースからアクセスできます。これにより、機密情報の可能性がある情報をすばやく検索し、コンテンツの存在場所と所有者を特定できます。

保護ポリシーの定義

McAfee DLP Discoverを使用すると、情報を適切に保護することができます。McAfee DLP Discoverでは、ポリシーやレポートを一元管理できるので、より多くの時間を情報保護戦略の検討に充てることができます。McAfee DLP Discoverのポリシー、ルール、分類には次のメリットがあります。

- 数多くのポリシーが事前に定義されているので、導入後すぐに利用できます。
- 強力なルール作成エンジンを搭載しています。簡単なデータ（クレジットカード、社会保障番号など）だけでなく、知的財産などの複雑な情報からでもルールを作成できます。
- 検索の分析結果から保護ルールを作成できます。ルールの作成と検証が簡単です。
- 他の情報セキュリティと統合し、一貫したセキュリティを実現できます。
- 公開文書や一般的なテキストを除外し、インシデントの誤検知を防ぎます。

ネットワーク上の違反をスキャン

McAfee DLP Discoverでは、定義したポリシーを使用してネットワーク リソースを定期的にスキャンし、ポリシー違反を検出できます。柔軟なスケジュール オプションを使用して、スキャンの実行頻度（連続、毎日、毎週、毎月）を設定できます。

McAfee DLP Discoverは、ノートPC、デスクトップ、サーバー、文書リポジトリ、ポータル、ファイル転送など、アクセス可能なすべてのリソースを自動的にスキャンし、ポリシー違反を検出します。IPアドレス、サブネット、アドレス範囲、ネットワーク パスに基づいてスキャン グループを定義できます。また、パラメーターを使用して特定の処理を実行することもできます。たとえば、すべてのユーザーのマイ ドキュメントフォルダーのみをスキャンし、システム フォルダーを除外したり、特定のユーザーが所有するファイルや特定の種類/サイズのファイルを検索できます。

違反の確認と修復

McAfee DLP Discoverでは、インシデント ワークフローとケース管理が統合されています。重要な情報の拡散を最小限に抑えることができます。保護ポリシー違反を検出すると、McAfee DLP Discoverはインシデントを生成し、通知を送信します。McAfee DLP Discoverが生成したインシデントをケース管理フレームワークに追加すると、社内の様々な部門から専門家を集め、違反に対処することができます。また、リスク ダッシュボードにより、セキュリティ担当者はポリシー違反の分布を簡単に確認し、問題のあるデータに基づいてレポートを作成できます。

仕様: ソフトウェア専用

McAfee DLP Discoverはソフトウェアとして利用できます。システムの最小要件は次のとおりです。

ハードウェア要件

- CPU: Intel Core 2 64ビット
- RAM: 4 GB以上
- ディスクの空き容量: 100 GB以上

対応プラットフォーム

- Windows Server 2008 R2 Standard（64ビット）
- Windows Server 2012 Standard（64ビット）
- Windows Server 2012 R2 Standard（64ビット）

対応の仮想化システム

- vSphere ESXi 5.0 Update 2
- vCenter Server 5.0 Update 2

McAfee ePOとエージェント

- McAfee ePO 4.6.8以降または5.1以降
- McAfee Agent 4.8.2以降または5.0以降

保存されたデータの収集と分析

McAfee DLP Discoverは、ネットワーク リソースをスキャンしてポリシー違反を検出するだけでなく、ネットワーク上で検出したすべてのコンテンツにインデックスを作成します。McAfee DLP Discoverを使用すると、機密情報をすばやく識別し、情報の使用方法、所有者、保存場所、送信先を確認できます。

複雑なデータの分類

McAfee DLP Discover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 Discoverは、オブジェクト分類メカニズムにより、オブジェクトを正確に分類します。これにより、機密情報のフィルタリングと制御を行い、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。

仕様: McAfee DLP 5500アプライアンス

McAfee DLP Discoverは物理または仮想アプライアンスとして利用できます。アプライアンスの仕様は次のとおりです。

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）

仕様: 仮想マシン

McAfee DLP Discoverは、VMware環境で動作する仮想アプライアンスとして利用できます。仮想アプライアンスのハードウェア最小要件は次のとおりです。

コンポーネント	要件
プロセッサー	Intel x86 4x vCPU
メモリー	16 GB RAM
ハードドライブ:	ドライブ1: 最小サイズ ― 100 GB（VMソフトウェア用） ドライブ2: 最小サイズ ― 512 GB（DLP 仮想イメージ用）
ネットワーク	4個の仮想NIC
BIOS	VTスレッド対応

1. McAfee DLP Discover 9.4ソフトウェア専用バージョンは現在、CIFS、Microsoft SharePoint 2010、Microsoft SharePoint 2013に対応しています。

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