

Proofpoint Digital Asset Security Module



電子メールが今日の企業で最も重要な通信手段となったことで、電子メールシステムは機密情報やミッションクリティカルな情報がいちばん多く置かれている場所になっています。また、企業は電子メールで会社から出て行く情報について大きな懸念を抱くようになりました。最近 Proofpoint と Forrester Consulting が行った調査¹によると、回答した大企業の 70 パーセント以上が貴重な知的財産や企業秘密の電子メールによる漏洩に懸念がある、もしくは非常に懸念があると答えています。個人のプライバシーや金融情報の秘密保護を心配している企業は 76 パーセントを超えていました。

概要

Proofpoint Digital Asset Security™ は、組織の機密情報、専有情報、要注意情報の事故や故意による漏洩に対する保護を容易にします。

貴重な知的財産や機密情報を保護

Proofpoint Messaging Security Gateway™ と Proofpoint Protection Server® のオプションコンポーネントである Proofpoint Digital Asset Security モジュールは、貴重な法人資産や機密情報が電子メールによって社外に漏洩することを防止します。強力な MLX マシンラーニングテクノロジーが機密文書を分析して秘密扱いに分類し、継続的にアウトバウンドのメッセージストリームにその情報がないか監視します。Proofpoint Digital Asset Security は秘密扱いの内容を単に監視する以上の機能を持っています——内容のセキュリティ違反が起きる前に止められるのです。

特徴

簡単なトレーニングと安全なドキュメントリポジトリ

Digital Asset Security モジュールは、特許出願中の Proofpoint MLX™ マシンラーニングテクノロジーを使って、機密にしておきたいドキュメントを解析します。ドキュメントをシステムに与えると、Digital Asset Security モジュールが「トレーニング」して、ドキュメントやその内容が認識されるようになります。

解析するドキュメントは、Proofpoint のグラフィカルユーザインターフェイスによって、ファイルシステムもしくはドキュメントリポジトリから (Proofpoint Enterprise Data Connector を経由して) ローディングすることができますし、特別なメールボックスに宛てて電子メールに添付して送ることもできます。送られた情報は MLX テクノロジーで解析され、安全な形で Proofpoint のドキュメントリポジトリに保存されます。問題のないものをローディングして、会社の報道情報など、一般的な非機密扱いの内容を無視するよう、システムをトレーニングすることも可能です。

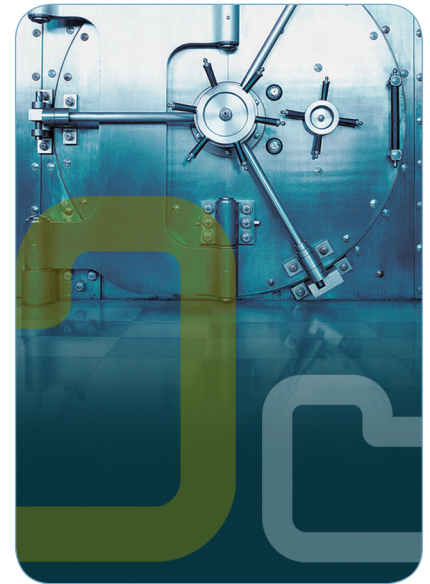
アクセスコントロールによって、トレーニングモジュールへのアクセスを一定のビジネスユーザのみに許可し、システムをトレーニングするドキュメントを追加できるユーザを制限することができます。

複数のカテゴリによるドキュメント保護

グラフィカルユーザインターフェイスによって、保護するドキュメントのタイプごとに異なるカテゴリを定義し、それぞれに別のアクセスコントロールやプロパティを与えることができます。たとえば、内部メモ、プレスリリースの下書き、組織図、価格表などといったカテゴリを別々に作成することが可能です。それぞれのカテゴリは、ドキュメントの有効期間のデフォルト値、ドキュメントの類似の一致しきい値など、独自のプロパティを持つことができます。

柔軟なポリシーの定義と管理

社外へ発信されるメッセージに機密情報が検知された場合にどう扱うかというポリシーは、グラフィカルユーザインターフェイスから簡単に定義することができます。特定の場合ごとに、ポリシーはいくつでも作成でき、高度に調節が可能です。それぞれのポリシーは指定したドキュメントタイプとカスタマイズ可能なドキュメント類似スコアに基づいて起動することができます。ルートベースの定義によって、デジタル資産の保護ポリシーを、インバウンドのメッセージストリームに発見された場合と、アウトバウンドで発見された場合で別々に作成することが可能です。



企業のコンテンツセキュリティ

スパム、ウィルス、フィッシングなどインバウンドのメッセージによる脅威にも増して、企業や大学や政府機関は、アウトバウンドの電子メールにポリシーを適用して、カスタマや従業員のプライバシー情報を守り、機密情報の漏洩を防止し、電子メール関連の法令遵守を助けるメッセージングセキュリティソリューションを求めています。Proofpoint は設定の簡単なモジュールの充実したスイートを提供して、これらの問題を解決します。

Proofpoint Messaging Security Gateway と Proofpoint Protection Server の Proofpoint's Content Compliance™、Digital Asset Security™、Regulatory Compliance™ の各モジュールは今日の企業にとって完璧なコンテンツセキュリティソリューションの代表格です。

コンテンツセキュリティモジュール

- Proofpoint Content Compliance を使うと、メッセージのコンテンツや添付ファイルに対して、企業が (キーワード、正規表現、および辞書に基づいて) 容認可能な使用のポリシーを定義して適用することができます。
- Proofpoint Digital Asset Security は、貴重な資産や機密情報が電子メールやその他のネットワークプロトコルによって組織から漏洩することを防ぎます。
- Proofpoint Regulatory Compliance は、HIPAA や GLBA などのプライバシー保護規制に伴う負担から組織を守ります。

¹Outbound Email Security and Content Compliance in Today's Enterprise, 2007年6月

Proofpoint Digital Asset Security Module

特徴

柔軟なポリシーの定義と管理(続き)

機密情報が含まれていると思われるメッセージは、Proofpoint の標準的なメッセージ処理を使って対応することができます。処理方法には、検疫、拒否、注釈付加、転送、差出人への返信、破棄、その他多数があります。たとえば、秘密のメモの一部を含んでいるアウトバウンドのメッセージは、検疫し、適切な管理職による調査用にフラグ付けをすることが可能です。

デジタル資産検疫の機能拡張

Web ベースの管理者 GUI では、適切な許可を受けた管理者が、検疫された疑わしいメッセージと元のトレーニングドキュメントを並べて比較することができます。このメッセージが検疫される原因となった部分が「オリジナル」ドキュメントの対応部分と共にハイライトされ、Proofpoint がどの部分を違反と識別したかが明白にわかります。自動インシデント・ステータス・トラッキングなどのワークフロー機能により、管理者が各メッセージにコメントを追加、検疫内に保存されたコンプライアンス違反メールのトラック・検索および該当したメッセージのエクスポートを可能にし、ワークフローに欠かせない人的リソースの負担を最小限に抑えます。

レポート

The Digital Asset Security モジュールにはビルトインのグラフィックなレポート機能があり、どのポリシーが一定期間の間に起動されたかを示すトレンドラインの表示などが行えるため、どのタイプの資産が最もリスクにさらされているか一目でわかります。

サポートするドキュメントタイプ

Proofpoint Digital Asset Security は、300 種以上のドキュメントタイプの安全確保に使えます。次はその一部です。

- プレーンテキストや電子メール。たとえば、内密な電子メールのメモなど。
- Microsoft Wordをはじめとするワープロのフォーマット。
- Microsoft Excelをはじめとするスプレッドシートのフォーマット。
- Microsoft PowerPointをはじめとするプレゼンテーションのフォーマット。
- Adobe PDF のドキュメント
- DWG、DWF、DXF その他のフォーマットによる CAD の図面
- ZIP、GZIP、TAR、および TNEF (Windows 電子メールアーカイブ)をはじめとするフォーマットのアーカイブ内のドキュメント

カスタムおよび独自のドキュメントタイプのサポート

Proofpoint のアウトバウンド電子メールセキュリティモジュールが元々認識する数百種類に加え、管理者は Proofpoint の File Type Profiler を使うことによって、新規または独自のファイルタイプ(たとえば独自の CAD/CAM フォーマット)にも容易にサポートを拡張することができます。

抜群の拡張性

Proofpoint Enterprise Data Connector™ テクノロジーによって、Proofpoint Digital Asset Security モジュールはファイルシステム、データベース、コンテンツ管理(EMC Documentumを含む)、バージョン管理システム、その他の外部アプリケーションと容易に統合し、新規または変更された機密情報の自動的なインデックス付けが行えます。アクセスコントロールやポリシーの情報は自動的にシステムにインポートが可能で、初期設定の時間と継続的な保守を大幅に減少させます。

電子メールを超えた保護

Proofpoint Network Content Sentry™ アプライアンスを追加すると、Proofpoint Digital Asset Security は HTTP と FTP の各プロトコルによる知的財産の漏洩を防ぐことができます。これによって機密資料がブログやその他の掲示板に投稿されたり、Web ベースの電子メールシステムや FTP サイトに送信されるのを確実に防げます。

Proofpoint Digital Asset Security は、EMC Documentum コンテンツ管理ソリューションとシームレスに統合できることが認証されています。



Proofpoint MLX テクノロジー

デジタル資産を安全に

Proofpoint Digital Asset Security モジュールは、特許出願中の Proofpoint MLX マシンラーニングテクノロジーを使って機密ドキュメントを解析し、それが電子メールによって組織から出ていくことを防止します。Digital Asset Security は、業界トップのスパム対策エンジン——現在流通している中で最も正確だと広く認識されています——に使用されているのと同じ最先端の統計技法を活用しています。

Proofpoint の研究者やエンジニアがスパムと正当な電子メールの両方を使って Proofpoint の MLX スパム対策エンジンを「トレーニング」するのと同じように、Proofpoint Digital Asset Security はシステムに与えられた特定のドキュメントを解析することによって機能します。「陽性」のケース(安全にしておきたいドキュメント)と「陰性」のケース(会社の報道情報など、一般的な非機密扱いの内容)の両方をシステムにローディングすることができます。

Proofpoint MLX テクノロジーはトレーニング用ドキュメントの統計表現を作成し、これとすべてのメッセージを比較して一致を探します。この技法は Proofpoint Protection Server や Proofpoint Messaging Security Gateway が非常に高速でしかも正確にスキャンすることを可能にします。機密情報の漏洩に対するスキャンは、ウィルススキャンなど他の処理と並行して効率的に実行されます。

これを利用したコンテンツセキュリティソリューションは、非常に正確でパフォーマンスが高く、トレーニングも保守も容易です。

Proofpoint はこうした最先端の統計技法をインバウンドのスパム検知とアウトバウンドのコンテンツフィルタリングの両方に応用している唯一のベンダです。Proofpoint Attack Response Center の研究者は、新しい先進的な統計技法の基礎的な研究と、MLX に基づく新たな防御の開発を続けています。この継続的な研究開発によって、Proofpoint のソリューションが常にメッセージングインフラに対するセキュリティの脅威よりも一歩前を行くことが保証されています。

©2008 Proofpoint, Inc. Proofpoint Protection Server は米国およびその他の国々における Proofpoint, Inc. の登録商標です。Proofpoint、Proofpoint Messaging Security Gateway、Proofpoint Content Compliance、Proofpoint Digital Asset Security、Proofpoint Regulatory Compliance、Proofpoint Enterprise Data Connector、Proofpoint MLX は米国およびその他の国々における Proofpoint, Inc. の商標です。この文書に含まれるその他すべての商標はそれぞれの所有者の所有物です。09/08