

Proofpoint Network Content Sentry



企業はアウトバウンド電子メールへのポリシー適用、機密情報の漏洩に対する防御、法令遵守の確保にますます気を遣うようになってきている一方で、HTTP や FTP のトラフィックを初めとする他のアウトバウンドメッセージングストリームが作り出すリスクにも気づきはじめています。最近 Proofpoint と Forrester Consulting が行った調査¹によると、回答した企業の半数以上が Web メールがプライバシー情報の漏洩源になることを懸念する、もしくは非常に懸念すると答えています。また、同数の企業がブログ、掲示板など HTTP のアウトバウンドトラフィックによる情報漏えいのリスクを軽減することが重要であると述べています。Proofpoint Network Content Sentry は Proofpoint のデータ漏洩防止とコンテンツセキュリティ機能を、Web ベース電子メール、ブログや掲示板への投稿、その他 HTTP や FTP に基づくアクティビティなどのアウトバウンドメッセージストリームに拡張します。

概要

Proofpoint Network Content Sentry™ は、すべてのアウトバウンドネットワークトラフィックをリアルタイムで検査し、機密情報、内密な顧客や従業員のデータ（個人的なヘルスケア、金融、身元識別情報など）を初め、その他企業から漏洩する可能性のある機密コンテンツを監視するハードウェアアプライアンスです。そのような違反が検知されると、Proofpoint Network Content Sentry は——Proofpoint Protection Server™ ソフトウェアまたは Proofpoint Messaging Security Gateway™ アプライアンスと連携して動作して——管理者（コンプライアンス担当責任者など）に警告を発して適切なアクションがとれるようにします。

知的財産への保護拡張とコンプライアンスの改善

Proofpoint のソフトウェアまたはアプライアンスの導入された環境に Proofpoint Network Content Sentry を追加すると、SMTP ベースの電子メールに対して定義されたのと同じ、コンテンツセキュリティ、法令遵守、使用容認のポリシーを、HTTP および FTP の各プロトコルベースの通信に適用することができます。

- **知的財産と機密情報の保護**：Proofpoint Digital Asset Security™ モジュールと連動して、Proofpoint Network Content Sentry はアウトバウンドのネットワークトラフィックに、あらゆるタイプの機密資産が含まれていないか監視します。Proofpoint MLX™ のメッセージ分類技術を利用して、Proofpoint Digital Asset Security は機密ドキュメントを解析し、分類して、その後は継続的にその情報の全部または一部について、外部に出ていくネットワークトラフィックを監視します。Proofpoint Digital Asset Security を使うと、電子メールメッセージ、テキストファイル、ワープロファイル、ソースコード、CAD 図面、スプレッドシート、プレゼンテーションフォーマットを初めとする数百種類のドキュメントタイプを保護することが可能です。
- **プライバシーの保護と法令遵守**：Proofpoint Regulatory Compliance™ モジュールと連動して、Proofpoint Network Content Sentry はアウトバウンドのネットワークトラフィックに非公開情報が含まれていないか監視します。対象となる情報には、PHI(HIPAA によって定められた薬剤名、傷病名、患者識別コード、治療コードをはじめとする保護対象健康情報)、個人識別情報（日本の運転免許証番号や住民票コード、アメリカ社会保障番号、イギリス国民保険番号など）、個人の金融情報（JCB をはじめとするクレジットカード番号やアメリカの銀行協会銀行支店コードなど）といったものがあります。Proofpoint の“スマート識別子”が、低い擬陽性で正確な非公開情報の検知を保証します。



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攻撃の脅威にも増して、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 Network Content Sentry に加えて、Proofpoint の 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組織から漏洩することを防ぎます。Proofpoint MLX テクノロジーが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。
- Proofpoint Regulatory Compliance は、アウトバウンドのメッセージに含まれる個人の金融情報、ヘルスケア情報、身元識別情報を正確に検知して、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 Data Loss Prevention in Today's Enterprise, 2008.

Proofpoint Network Content Sentry

概要

高性能のHTTPおよびFTPプロトコル監視

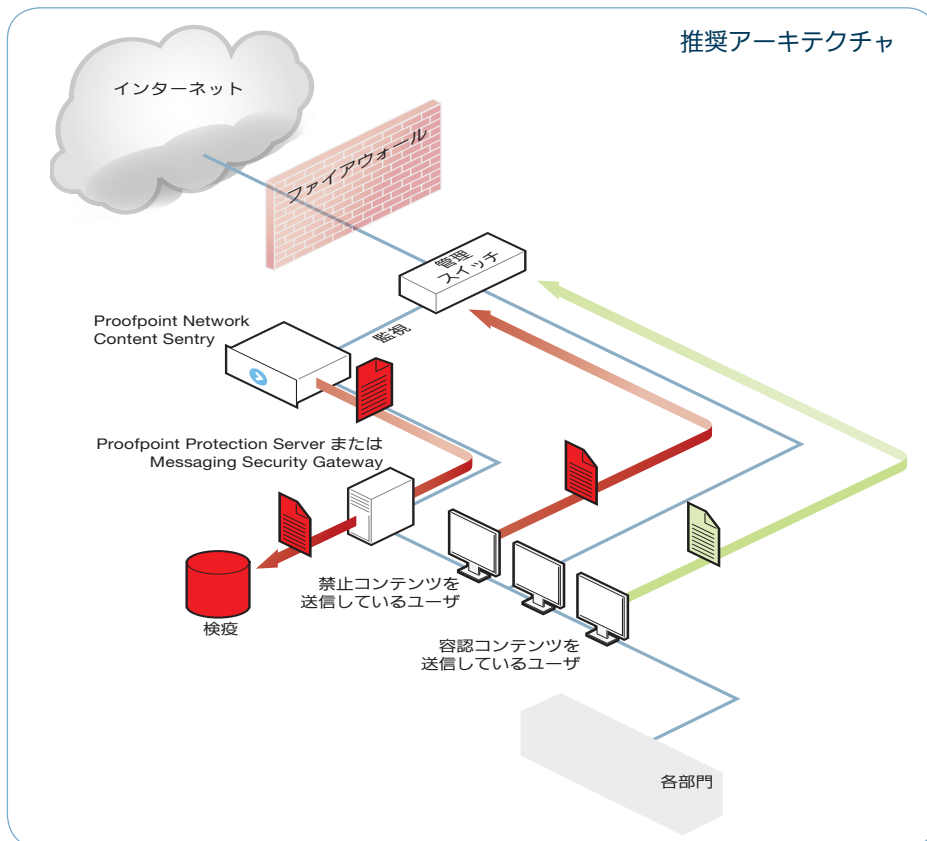
Proofpoint Network Content Sentry は、すべてのアウトバウンド HTTP および FTP プロトコルトラフィックを高いデータレートで知的に捕捉して再構築します。あらゆる HTTP ポスティング—— Web ベースの電子メール発信 (MSN Hotmail, Yahoo! Mail, AOL Mail, Google GMail など)、ブログへの書き込み、掲示板への投稿、Web ベースファイル保管システム (GMail FS など) の使用、その他一般的なポスティング——が傍受され、情報の漏洩やポリシーへの違反がないかスキャンされます。

このシステムは、アクティブモードとパッシブモード両方の FTP 通信について、リモートサーバへ送信されるバイナリファイルとテキストファイルを監視します。HTTP ポスティングと同様、多種多様なポリシーを FTP アクティビティに適用することが可能です。これには、特定のファイルに対する監視、ファイルサイズの限定、不適切な宛先への FTP 送信の検知などが含まれます。

柔軟なポリシー定義とインシデント管理

Proofpoint Network Content Sentry ポリシーの定義には、アウトバウンド SMTP 電子メール用のポリシー定義に使うのと同じインタフェースが使われます。それぞれのポリシーは、特定のドキュメントタイプやカスタマイズ可能なドキュメントの類似スコアに基づいて起動させることができます。ポリシーを起動させた HTTP または FTP のメッセージは、詳しい調査のために検疫することが可能です。

Proofpoint の Compliance Incident Manager™ インタフェースを使うと——コンプライアンス、セキュリティ、リスク管理、人事、その他事業部門などの管理者といった——ビジネスユーザが、容易に電子メールやネットワークコンテンツセキュリティのポリシーを管理して、違反の調査、例外の承認、インシデントの監視を、使い勝手のよい電子メールベースの通知システムによって行うことができます。Compliance Incident Manager は、ポリシー違反とその重大度をアクティブに通知します。管理者は容易にしかも効果的に問題となったメッセージのレビューや追跡、Proofpoint のグラフィカルユーザインタフェースを使ってリリース、リルート、承認、またはその他のインシデント管理を行えます。



サポート対象プロトコル

Proofpoint Network Content Sentry は、アウトバウンドの HTTP と FTP トラフィックをすべて捕捉して解析します。検知機能には次のものが含まれます。

HTTP Web メール送信:

- MSN Hotmail
- Yahoo! Mail
- AOL Mail
- Google GMail (Gmail FS File System 転送含む)
- Lycos webmail
- Network Solutions webmail
- Comcast webmail
- カスタムの Web メールアプリケーション

一般的 HTTP ポスティング:

- Web ブログへの書き込み
- 掲示板への投稿
- 一般的 HTTP ポスティング、添付ファイルや Web フォームの送信

FTP トラフィック:

- テキストファイルやバイナリファイルの送信
- FTP のアクティブモードとパッシブモードをサポート

導入オプション

すべての Proofpoint アプライアンスは、企業ネットワークの出口にインストールした Proofpoint Network Content Sentry として構成することができます。

- アプライアンスはファイアウォールの内側で、できる限り近くに接続してください。ファイアウォールの前に接続すると、クライアントの IP 情報が捕捉できません。
- HTTP と FTP のトラフィックを捕捉するには 2 通りの配備オプションがあります。
 1. 管理スイッチまたはルータのスパンポートに取り付ける。
 2. ネットワークタップ経由でネットワークストリームの出口に接続する。
- アプライアンスには 2 つのネットワークポートがあります。1 つは LAN に接続する管理ポートです。もう 1 つは捕捉用ポート (左図の「監視」) ですが、これはプロミスクラスで、IP アドレスを必要としません。

©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 Network Content Sentry, 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のすべての商標はそれぞれの所有者の所有物です。09/08