



Proofpoint Solution Brief

ウイルス・スパム対策の次は **「誤送信対策」**

Proofpoint が提唱する “実用的な” メール誤送信対策

ああっ！ やってしまった・・・
あの思いを、二度としないために



気づいたときにはもう遅い！
送信後でも取り消し可能な
誤送信対策とは？

社内に先
一定時間後
誤送信に社
気づいて

機密情報を含んだメールを
ゲートウェイで検知して保留。
インテリジェントに誤送信を防止！

Proofpoint Protection Server (PPS) は、インバウンドとアウトバウンドの電子メールセキュリティを統合した、包括的なソリューションです。プラットフォームとして、オンプレミスのアプライアンス、仮想アプライアンス、SaaS形式などがあり、最適な導入形態を選ぶことができます。

Proofpoint Secure File Transfer (PSFT) モジュールは、環境にセキュアな大容量送信機能を追加します。

Proofpoint Protection Server

Secure File Transfer

PPS
標準機能 *1
(Email ファイアウォール)

暗号化
モジュール

PSFT
標準機能

一時保留・ワンクリック削除 / 即時配信

送信後のメール取り消し・未読の証明

送信後の添付ファイル取り消し

運用負担を軽減するマネージャ承認

Bcc 化による To/Cc アドレスの秘匿

*1「標準機能」とは、何れかの有償モジュールに含まれる基本機能です。

Proofpoint の誤送信対策は、Proofpoint がこれまで培ってきた技術と、Proofpoint Protection Server の機能を組み合わせて実現する 5 つの対策から構成されています。お客様は、これらの対策を自由に組み合わせて、自社に最適な誤送信対策ソリューションを段階的に構築できます。また、監査モードにより、導入前の効果検証を行うことも可能です。

一時保留・ワンクリック削除 / 即時配信



特定の条件を満たすメールがフィルタリングエンジンにより検疫フォルダに一時保留され、送信者に自動応答メッセージを送信します。送信者はメールを削除するか、そのまま送信するかをワンクリックで選ぶことができます。

送信後のメール取り消し・未読の証明



Proofpoint Encryption でメッセージを自動的に暗号化し、鍵をメッセージごとに生成します。受信者はその鍵を使って暗号化されたメッセージを読みます。誤送信が判明した場合、送信者が解読用の暗号鍵をクラウド上のサーバーから削除することにより、削除後はメールの復号化はできなくなり、誤送信による情報の漏洩・拡散を防ぐことができます。また、暗号化メッセージが開封されたかどうかを送信者側で確実に把握できますから、情報が拡散してしまったかどうかを確認でき、開封されていない「拡散していない（漏洩していない）」ことの証明にもなります。

送信後の添付ファイル取り消し



ユーザが Secure File Transfer にファイルをアップロードすると、ファイルのありかを示す URL を受信者に送信し、受信者はその URL にアクセスして、添付ファイル入手します。万一誤送信が判明した場合、SFT 上から該当するファイルを削除してしまえば、それ以上情報が拡散するのを防ぐことができます。

運用負担を軽減するマネージャ承認

Email Firewall には、条件を満たすメールをそのまま送信せずに、検疫フォルダに保存し、マネージャの承認を得られるまで保留する「検査」機能があります。担当者のメールをそのまま送信するのではなく、いったんマネージャが内容を確認することにより、誤送信を防ぐことができます。

Bcc 化による To/Cc アドレスの秘匿

電子メールの To: や Cc: フィールドに入力されたメールアドレスは、受信者すべてに見えてしまいます。Email Firewall のポリシーで、To: または Cc: に一定数以上のアドレスが含まれる場合や、特定のアドレスが含まれる場合などを設定し、アクションとして、Cc: を削除、To: を送信者アドレスに書き換えて送信します。これで受信者には、送信者以外のアドレスは表示されません。

先行配信、
後に社外へ。
社内誰かが
くれる！

File Transfer™
PPS 導入環
量ファイル転

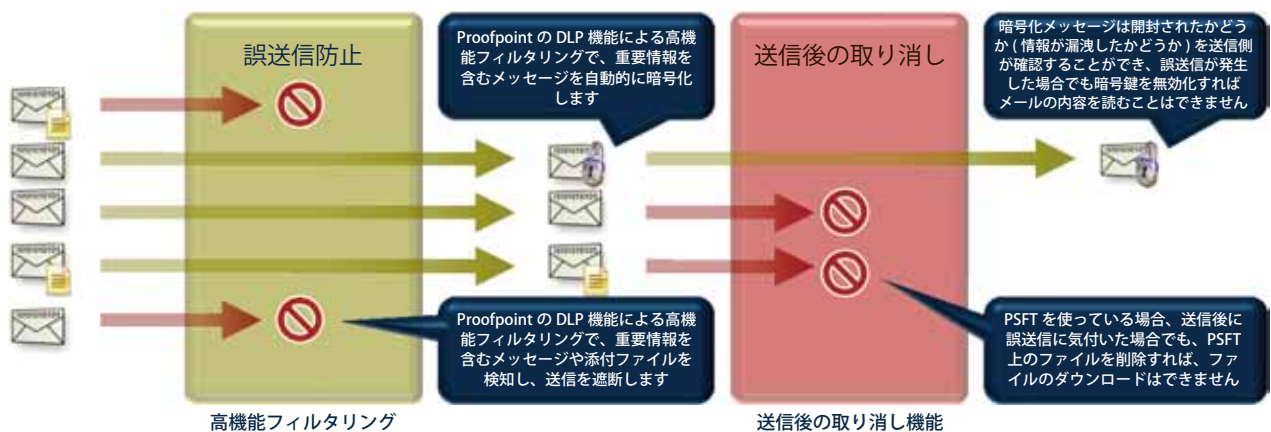
e
sfer

能 *1

電子メールはいまや企業活動にとって必要不可欠なものとなっています。しかし、電子メールの利用頻度が上がるに従い、電子メールに関連した情報の漏洩のリスクがかつてなく高まっています。Proofpointは統合型メッセージングセキュリティのリーディングカンパニーとして、アウトバウンドの電子メールを保護する技術を次々に開発してまいりました。

企業における電子メールのリスクとして、従来から問題となっているウイルス・アンチスパムに加え、誤送信による情報漏えいが問題視されています。これまでは、送信する前に誤送信を防ぐために、DLPテクノロジーをベースとした誤送信防止が提案されてきました。しかし、これらの提案では、送ってしまった後にそのメールを「撤回」することはできませんでした。

Proofpointの誤送信対策は、Proofpointがこれまで培ってきたDLPテクノロジーと、Proofpoint Protection Serverでサポートされた最新の機能を組み合わせて実現する複数の誤送信対策から構成されており、送信後の取り消しも可能になっています。お客様は、これらの対策を自由に組み合わせて、自社に最適な誤送信対策ソリューションを段階的に構築できます。また、監査モードにより、導入前の効果検証を行うことも可能です。



Proofpointは電子メールトラフィックを監視し、特定の条件を満たすメッセージを検出します。条件を満たすメッセージに対して、各種の処理を行うことができ、これらを組み合わせることで、個々の企業に最適な誤送信対策ソリューションを提供することができます。

Proofpoint について

Proofpoint Inc. は 2002 年、Netscape Communications の元 CTO エリック・ハーン (Eric Hahn) によって設立されました。現在では世界 50 カ国以上の企業、ISP、大学および政府機関など 4,000 以上の実績 (11/1 現在) があり、業界で最も急成長している統合型メッセージングセキュリティのリーディングカンパニーです。

Proofpoint の統合型メッセージングセキュリティインフラ

スパム・ウイルスなどインバウンドメッセージの脅威、アウトバウンドメッセージによる情報漏えいやコンプライアンス対応など、エンタープライズゲートウェイにおけるあらゆる種類のメッセージングリスクから組織を守ります。Proofpoint は、クラウド、仮想アプライアンス、アプライアンスなどの顧客ニーズに応じた導入形態に加え、電子メール (SMTP) および Web (HTTP) トラフィックも統合管理できる完全なセキュリティインフラを提供します。

©2010-2011 Proofpoint, Inc. Proofpoint Protection Server, Proofpoint Messaging Security Gateway, Proofpoint Spam Detection, Proofpoint Virus Protection, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint MLX, Proofpoint Dynamic Reputation, および Proofpoint on Demand は、米国およびその他の国々における Proofpoint, Inc. の商標または登録商標です。このカタログ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。

proofpoint

日本プルーフポイント株式会社

〒102-0083 東京都千代田区麹町 3-5-2 ビュレックス麹町
TEL : 03-5210-3611, FAX : 03-5210-3615
Email : sales-japan@proofpoint.com
URL : <http://www.proofpoint.co.jp/>

本カタログの内容は 2011 年 8 月現在のものです。仕様、諸元は予告なく変更することがありますのでご了承ください。ご購入にあたり、最新のサポート状況を弊社もしくは正規販売代理店にお問い合わせください。

お問い合わせ