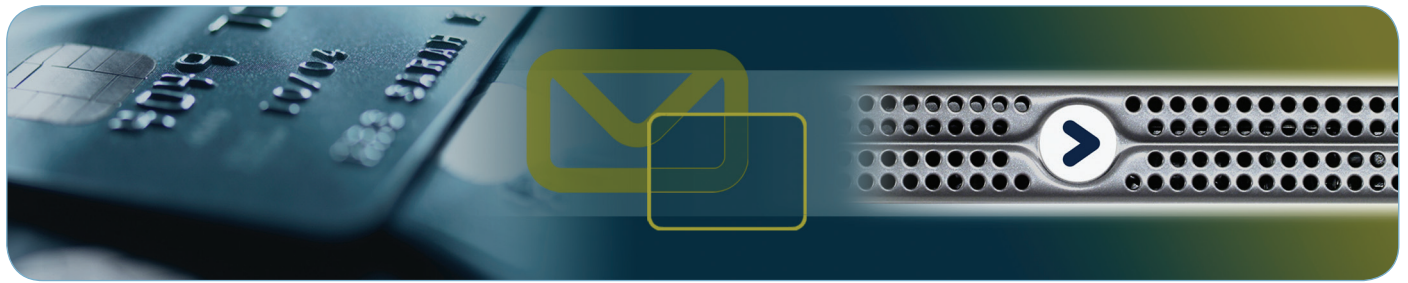


# Proofpoint のソリューションを使った PCI DSS への適合



## 電子メールセキュリティ、情報漏洩防止、暗号化ソリューション



PCI DSS (Payment Card Industry Data Security Standard = PCIデータセキュリティ基準) は、クレジットカードの国際ブランドなどが中心となり、コンピュータシステム間でやりとりされるクレジットカード番号 (PAN: Primary Account Numbers) やセキュリティ対策用のCVV番号 (カード裏面の 3桁の番号)、暗証番号などのカード会員データの漏洩や不正利用を防ぐために、2005年1月に発表したセキュリティ基準です。2006年に v1.1、2008年に v1.2 が発表されました。この基準は、カード会員データを取り扱う企業すべて (オンラインショップ、小売店、決済銀行、サービス業者など) が守るべき 12 の要件から成っています。

PCI DSS はクレジットカード業界が取りまとめているセキュリティ基準ですが、最新のセキュリティ技術の実装基準を幅広く網羅しており、一般企業の情報セキュリティにも十分適用可能な包括的な基準となっています。このため最近では、ISMS などを補完する基準として注目を集めています。

### PCI DSS 準拠への課題

PCI DSS と電子メールセキュリティの両方に対応しなければならないことは、企業のコンプライアンス責任者、監査担当者、システム管理者にとって大きな問題です。カード会員データは、クレジットカード取扱企業のシステムから、電子メールシステムのようなアプリケーションを経由してネットワーク上を移動します。こういった移動は、情報漏洩のリスクを高め、移動の過程で外部の犯罪者に情報が渡る危険があります。情報の漏洩は PCI DSS への準拠違反を意味し、顧客との訴訟、カード会社への高額の罰金、ブランドの毀損などを引き起こすことがあります。情報漏洩を起こすと、システムの修正や度重なる監査への対応で、システム管理部門のパフォーマンスにも重大な影響を及ぼします。さらに、企業は PCI DSS への準拠という観点からだけでなく、電子メールセキュリティの問題に取り組まなければなりません。インバウンドの電子メールに係るウイルスやスパムなどは、企業の生産性やセキュリティに悪影響を及ぼすからです。

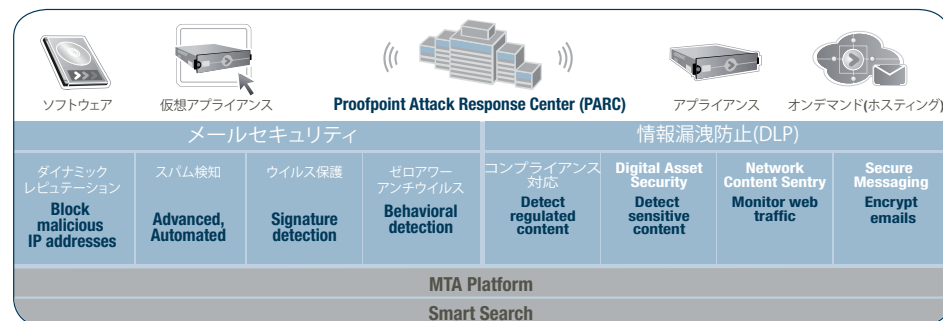
### Proofpoint のソリューション

Proofpoint では、PCI DSS への準拠のために、全世界で豊富な導入実績を持つソリューションを用意しています。これらのソリューションは単一のプラットフォーム上で動作します。

- 情報漏洩防止 (DLP): 電子メール (SMTP)、Web アクセス (HTML)、ファイル転送 (FTP) などの様々な通信経路を通じたアウトバウンド通信の内容を監視
- 電子メールセキュリティ: インバウンドの電子メールとともに入り込むスパム、ウイルスを検知して防御

これらのソリューションは4種類のアプライアンスのどれにでも搭載可能で、Proofpoint Attack Response Center (PARC) の研究と組み合わせて使えば、タイムリーで正確なアンチスパム、ゼロアワーアンチウイルスなどを実現できます。

### Proofpoint Solution Platform



### PCI DSS に準拠する必要がある企業

- クレジットカードを取り扱う小売店、企業
- 決済代行会社
- アクワイアラ、イシュア
- カード所持者団体
- クレジットユニオン

### ビジネス上の課題

- PCI DSS に準拠せずに情報漏洩事件を起こした場合の罰金 (最大 50 万ドル)、企業の社会的評価の毀損
- ネットワーク上を移動中のカード会員データを正確に検出:
  - ・ PCI DSS 要件 4.2 「カード会員データを暗号化せずに電子メールなどで送信してはならない」への適合
  - ・ カード会員データに関連するビジネス上の重要情報の保護
- スパムやウイルスを正確に検知し、効率的に防御:
  - ・ PCI DSS 要件 5 「アンチウイルスソフトウェアまたはプログラムを使用し、定期的に更新すること」への適合
  - ・ 安全で生産的な電子メールの利用

### PCI DSS 要件 4.2 に対応するための機能

- 重要な情報を含む電子メールを自動的に暗号化
- ワークフローを構築し、電子メールを検査・制御
- PCI DSS への準拠についてエンドユーザを教育

### Proofpoint のソリューション

- SMTP、HTTP および FTP 上を流れるカード会員データを正確に検出
- 自動的、あるいはユーザの操作によりポリシーベースで電子メールを暗号化
- スパム、ウイルス、マルウェアを高精度に検知
- 内蔵された MTA により自動的に電子メールを阻止
- エンドユーザ (情報漏洩を引き起こすリスクが最も高い) への教育が不要

# Proofpoint のソリューションを使った PCI DSS への適合

## 情報漏洩防止のプロセス

- SMTP、HTTP および FTP を監視
- 様々な手法によりカード会員データを検出
- ポリシーに則って暗号化や検疫などの処理を自動的に適用
- IT 管理者、ユーザにポリシー違反を通知
- 違反者、傾向などについてのレポートを作成

## Proofpoint の情報漏洩防止モジュール

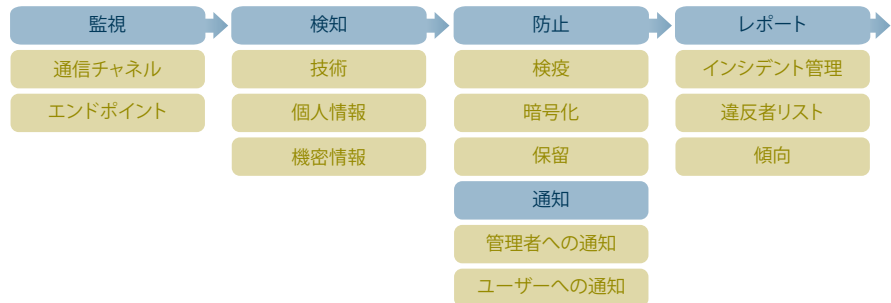
- Regulatory Compliance: 非公開情報を検出
- Secure Messaging: 電子メールの自動暗号化
- Network Content Sentry: HTTP 通信の監視
- Digital Asset Security: ビジネス上の重要情報の保護

## ポリシー設定

- あらかじめ設定されたポリシーの利用
- 特定の送信者/受信者、送信元 IP アドレス/受信 IP アドレスなどの組み合わせを制限
- 多階層での監視と検出
- ワンクリックで簡単に暗号化
- 数々の検疫オプション
- エンドユーザへの通知/警告をカスタマイズ可能

## Proofpoint の情報漏洩防止機能

PCI DSS の要件 4.2 では、カード会員データを、暗号化していない電子メールで送信することを禁じています。Proofpoint のソリューションは、ネットワーク上の通信を監視し、カード会員データなどを検出すると、そのメールを強制的に暗号化したり、送信を停止したり、処理を保留して管理者の指示を待つなどの対応を行います。同時にこれらのポリシー違反について管理者およびエンドユーザに通知し、インシデント、違反者リスト、違反の傾向などについてのレポートを作成します。すべてのプロセスは、Proofpoint の統合されたポリシー管理画面を使って、シンプルかつ容易に管理することができます。



### 監視: どこで違反が起きているか

PCI DSS では、電子メールを情報漏洩リスクの高い通信経路と位置づけており、カード会員データの漏洩を防ぐために、常に監視することを求めています。Proofpoint では、この要件に適合し、さらに高いセキュリティを実現するため、SMTP だけではなく、HTTP (Webメールやブログへの書き込みなど)、FTP (大容量のファイル送信) も監視します。Proofpoint のソリューションはまた、差出人、宛先、添付ファイルや国コードなど、電子メールのあらゆるフィールドを検査することができます。Network Content Sentry™ モジュールは、Yahoo! や Gmail、Hotmail などの主要な Web メールシステムをサポートしています。ポリシー設定により、これらの通信経路を使ったエンドトゥエンドの通信は差出人/宛先、ソース/配信先や Webメールサイトなどの知識をベースにして、さらに解析されます。

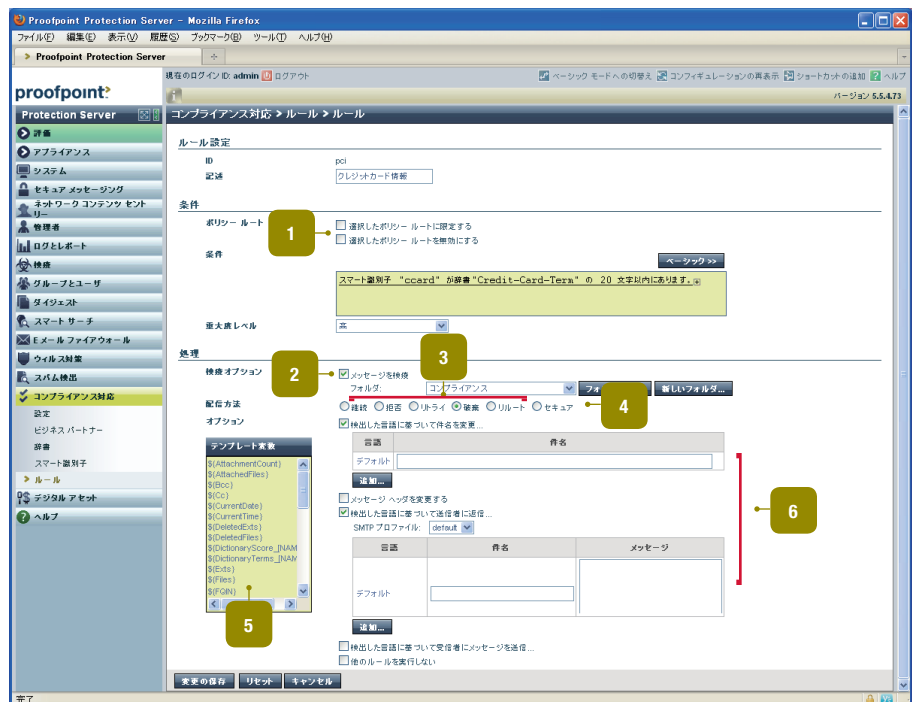
### PCI DSS 準拠のためのシンプルなポリシー設定

Proofpoint Regulatory Compliance™ モジュールは、カード会員データの保護に関するポリシーセットをあらかじめ組み込んでおり、導入と同時に、簡単に運用を開始できます。もちろん、ポリシーのカスタマイズも可能です。

### Proofpoint Regulatory Compliance Module:

- スマート識別子および定義済み辞書を使った簡便なポリシー設定
- カード会員データを含むメールの検疫
- 破棄や継続を含む様々な検疫オプション
- ワンクリックで簡単に暗号化
- エンドユーザへの通知/警告をカスタマイズ可能
- 様々なメッセージ処理
  - 件名の変更
  - メッセージヘッダの変更
  - 差出人への返信
  - そのまま送信
  - コンプライアンス責任者へ通知

### Proofpoint Regulatory Compliance Module



## カード会員データの検出

Proofpoint Regulatory Compliance™ モジュールは、クレジットカード番号や日本の運転免許証番号などの様々なタイプの非公開情報 (NPI) を、様々な手法で検出して情報保護に役立てます。主要な NPI 識別子に対する設定は最初から組み込まれており、後からカスタマイズすることも可能です。PCI DSS においては、クレジットカード番号や顧客情報などを含むカード会員データを検出する設定が登録されています。

- スマート識別子: 有効なカード番号などを検出
- 定義済み辞書: キーワードや正規表現による検索ができる様々な辞書があらかじめ登録されています(カスタマイズも可能)
- 近接一致: 電子メールの中でカード関連用語の近くにあるカード番号を検出

Digital Asset Security™ モジュールは、高度な MLX テクノロジーを使ってファイル間の類似性を解析します。機密情報を含むファイルと類似するファイルもまた、機密情報を含むと考えられるからです。

- デジタル指紋: PCI DSS に関連する機密情報を含むテキストやイメージのハッシュを作成
- コンテンツマッチ: デジタル指紋の全部または一部を含むデータを検出
- ファイルタイプ: xls、doc、ppt などのファイルタイプを検知。(拡張子の変更されていても検出可能)

## ポリシーベースの自動暗号化

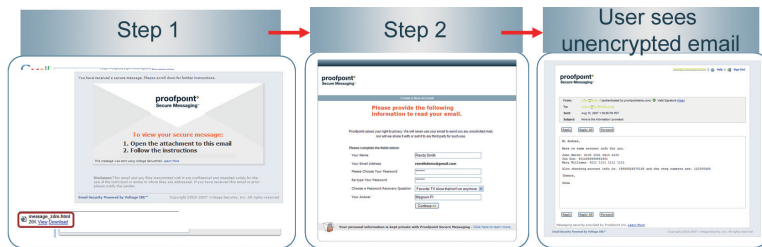
Proofpoint Secure Messaging™ モジュールは、ゲートウェイまたはデスクトップ PC 上で、ポリシーに基づいた電子メールの暗号化を行います。ユーザーが自分で暗号化する場合に比べて、暗号化のし忘れや誤送信などを防ぐことができます。

- ユーザーがそのメールを暗号化すべきかどうか、どのような暗号化技術を使うべきか、迷う必要はありません
- 様々な (Blackberry など) デバイスからのメールも暗号化可能
- ゲートウェイからエンドユーザーへの通信では、Identity Based Encryption™ (IBE) をサポート
- ゲートウェイ間の通信では TLS を利用可能

## 暗号化は PCI DSS 準拠の第一歩

Secure Messaging を使うと、暗号化ソフトを持っていない受信者でも暗号化メールを受け取ることができます。

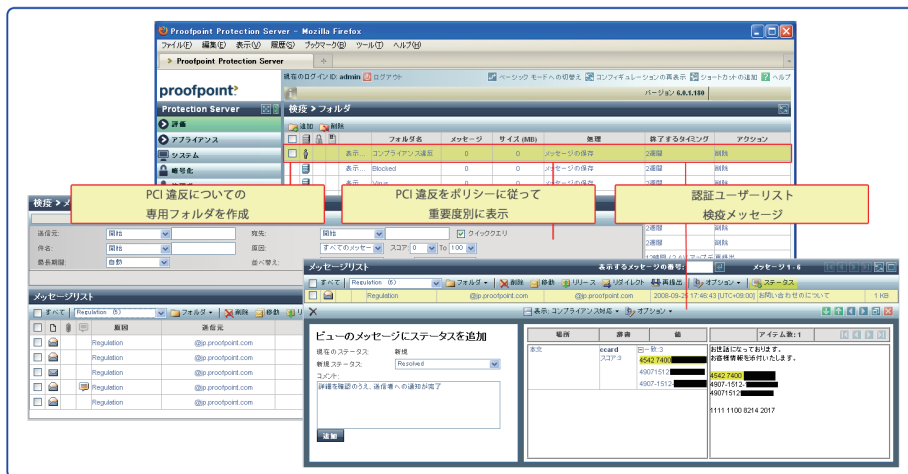
- ステップ 1: 暗号化メールの受信者は、メッセージ本文の場所を示すリンクを受け取ります。
- ステップ 2: 受信者はサイトにアクセスしてパスワードを登録し、暗号化メールを復号化します。



## 重要情報を含む電子メールを検知し、上司の承認まで送信を留保

非常に重要な情報を含む電子メールは、送信前に上司の承認を受けたほうが良いものもあります。Proofpoint の内蔵 MTA は、重要なデータを検知し、送信せずに保留し、上司の承認を待ちます。(検疫機能)

## Proofpoint の検疫・承認機能



## Proofpoint の暗号化

- 誰にでも暗号化メッセージを送ることが可能
- 送信者にも受信者にも暗号化ソフトは不要
- Javascript も ActiveX も不要
- 暗号化された添付ファイルにも対応
- 暗号鍵やメッセージストアが不要
- 受信者はメール中のリンクをクリックするだけで認証され、復号化されたメッセージを取得可能
- Voltage Security 社の IBE による公開鍵暗号を利用可能
- 様々な標準ベースの暗号ゲートウェイと通信可能

## 柔軟なユーザー認証

- ユーザー名/パスワード
- 質問/答え
- 電子メールによる返信
- LDAP, Active Directory
- PKI ベースのスマートカード
- RSA SecurID

## Effective DLP policies

「Proofpoint の電子メール検疫機能は、柔軟なグループ設定と詳細なレポート・状況確認機能が充実しており、電子メールからの情報漏洩を防止するポリシー設定のためには不可欠な機能だ」

Barry Johnson  
VP of Risk Mitigation  
lgxglobal

## ポリシー違反を通知

- IT 管理者へ: 電子メール、syslog、ログビューア、サポートなどによる通知
- エンドユーザーへ: ポリシー違反があった場合に自動的に電子メールで通知することにより教育効果を見込む

## 組み込まれたレポート機能

Proofpoint の「ログ&レポート」機能は、ポリシー違反者リストや違反の傾向などのイベントや傾向について、あらかじめ用意されたひな形に沿ったレポートを作成します。

これらのレポートにより、重点的なトレーニングが必要な従業員/グループを特定でき、トレーニングの内容の検討にも役立ちます。Proofpoint Smart Search™ モジュールには、より詳細な解析/レポート機能が用意されています。

# Proofpoint のソリューションを使った PCI DSS への適合

## メールセキュリティ

PCI DSS は要件 5 でアンチウイルスおよびアンチマルウェアプログラムの利用も必須としています。Proofpoint の最高度の精度をもつアンチスパムとアンチウイルスの組み合わせは、お客様に安全で効率的な電子メールサービスを提供します。

## Proofpoint のプラットフォームも PCI DSS の監査対象です

電子メールのセキュリティソリューション自身もまた、カード会員データを保存し、転送することから、PCI DSS の監査の対象となるでしょう。以下のテーブルには、Proofpoint のソリューションを導入するにあたって関連する、これまで述べた以外の PCI DSS の要件をまとめました。

### メールセキュリティソリューション: まとめ

- アンチスパム: 自動アップデート、マシンラーニングテクノロジー、PARC の研究成果
- シグネチャベースのアンチウイルス: 業界を主導するベンダーからの技術供与
- 行動検知: ゼロアワーアンチウイルス
- スパム検知精度は 99% 以上

PCI Requirement	Proofpoint Solution Modules						
	Secure Messaging	Regulatory Compliance	Digital Asset Security	Network Content Sentry	Anti-Virus	Anti-Spam	Proofpoint Solution
<b>!要件 4.2</b> 暗号化されていないカード番号 (PAN) をエンドユーザメッセージングテクノロジー (電子メール、インスタントメッセージング、チャットなど) で送信しない。	➤	➤	➤	➤			
<b>審査範囲:</b> カード会員データ環境のネットワークセグメンテーション、またはカード会員データ環境の残りの企業ネットワークからの隔離 (セグメント化) は、PCI DSS 要件ではない。ただし、ネットワークセグメンテーションは PCI DSS 評価の対象範囲を狭くする方法として推奨されている。							➤
<b>要件 A.1:</b> A.1.1 ~ A.1.4 に従い、各事業体 (加盟店、サービスプロバイダ、またはその他の事業体) のホストされている環境およびデータを保護する。ホスティングプロバイダは、これらの要件および PCI DSS のその他すべての関連セクションを満たす必要がある。							➤
<b>要件 1:</b> カード会員データを保護するために、ファイアウォールをインストールして構成を維持すること。							➤
<b>要件 2.1:</b> システムをネットワーク上に導入する前に、ベンダ提供のデフォルト値を必ず変更する (パスワード、簡易ネットワーク管理プロトコル(SNMP) コミュニティ文字列の変更、不必要なアカウントの削除など)。							➤
<b>要件 2.2.2:</b> 安全性の低い不必要なサービスおよびプロトコルはすべて無効にする (デバイスの特定機能を実行するのに直接必要でないサービスおよびプロトコル)。							➤
<b>要件 2.2.3:</b> システムの誤用を防止するためにシステムセキュリティパラメータを構成する。							
<b>要件 2.2.4:</b> スクリプト、ドライバ、機能、サブシステム、ファイルシステム、不要な Web サーバなど、不要な機能をすべて削除する。							
<b>要件 2.3:</b> すべてのコンソール以外の管理アクセスを暗号化する。Web ベースの管理やその他のコンソール以外の管理アクセスについては、SSH、VPN、または SSL/TLS などのテクノロジーを使用する。							➤
<b>要件 4.1:</b> オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、強力な暗号化と SSL/TLS またはIPSEC などのセキュリティプロトコルを使用する。							➤
<b>要件 5:</b> アンチウイルスソフトウェアまたはプログラムを使用し、定期的に更新すること。					➤	➤	
<b>要件 6.1:</b> すべてのシステムコンポーネントとソフトウェアに、ベンダ提供の最新セキュリティパッチを適用する。重要なセキュリティパッチは、リリース後 1 か月以内にインストールする。							➤
<b>要件 6.2:</b> 新たに発見された脆弱性を特定するためのプロセスを確立する(インターネット上で無料で入手可能な警告サービスに加入するなど)。							➤
<b>要件 7:</b> カード会員データへのアクセスを、業務上必要な範囲内に制限すること。							➤
<b>要件 8.4:</b> 強力な暗号化を使用して、すべてのシステムコンポーネントでの伝送および保存中にすべてのパスワードを読み取り不能にする。							➤
<b>要件 8.5:</b> すべてのシステムコンポーネントで、以下のように、消費者以外のユーザおよび管理者に対して適切なユーザ認証とパスワード管理を確実に実行する。							➤
<b>要件 10:</b> ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する。							➤

### Proofpoint のお客様の声を聞いてください

Proofpoint が、如何にしてお客様たちの問題を解決したか、リソースセンターで導入事例をご確認ください。 (英語)

<http://www.proofpoint.com/resource-center/>

### お客様自身で体験してください

オンラインでより詳しいデモンストレーションをオンラインでご覧いただけます。 (英語)

<http://www.proofpoint.com/demo>

©2009 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。09/09