

# Proofpoint Encryption



Proofpoint Encryptionは、暗号化を意識せずに使える簡便で安全な通信手段を提供します。Proofpointの強力なポリシーベースの暗号化機能は、通常の業務に影響を与えることなく、法規制違反や情報漏洩、社内ポリシー違反によるリスクを低減します。Proofpoint Encryptionは重要な情報を守る必要のあるあらゆる組織に適用でき、パートナーやエンドユーザーにもすぐに使ってもらうことができます。

## 概要

電子メールは今や、ビジネスにとって無くてはならないものになりました。一方で、企業は個々のメッセージのセキュリティについてますます心配しなければならなくなっています。電子メールは、重要な、もしくは機密の情報を送ることに普通に使われています。企業内外のビジネスの運用上の情報、営業秘密、法律文書、財務情報、個人の健康情報や個人情報などです。これらの情報を保護し、増え続ける法規制を遵守するためには、ポリシーベースの暗号化が必須です。Proofpoint Encryptionはこれらの要求に応える、業界でも最も強力な柔軟なポリシーベースの電子メール暗号化ソリューションです。

## 特徴

### ポリシーベースの電子メール暗号化

一般的に、電子メール暗号化ソリューションの正しい使い方をエンドユーザーに教え、徹底することは非常に難しく、導入の障害になっています。Proofpoint Encryptionは、ソリューションを使うのも、管理するのも非常に簡単です。Proofpointのメッセージ保護ソリューションは、企業のセキュリティポリシーに基づき、ゲートウェイレベルで自動的かつダイナミックに暗号化および復号化を行います。この結果、エンドユーザーは暗号化によるメッセージ保護を行うための特別な作業を何らすることなく、セキュリティポリシーは適切かつ正確に適用されるのです。

### 容易な管理

他の暗号化手法と異なり、Proofpointの電子メール暗号化ソリューションは、管理者の負荷やインフラにかかるコストを増やすことなく、重要な情報を効果的に保護できます。

- 簡便なポリシー管理：法規制や社内的なセキュリティへの要望など、全ての暗号化ポリシーは中央で集中管理され、ゲートウェイレベルで適用されます。Proofpoint Regulatory Compliance、Proofpoint Content Compliance または Proofpoint Digital Asset Security などによってメッセージを監視し、暗号化ポリシーを適用します。Proofpoint のメッセージングセキュリティコンソールは、これらの暗号化ポリシーを設定するためのグラフィカルなインターフェースを提供します。
- 簡素化された鍵と証明書の管理：Proofpoint Encryption は従来の暗号化システムにつきものだった管理上のオーバーヘッドを解消します。Proofpoint Encryption を使えば、オンプレミスでの導入でも Proofpoint on Demand のデータセンターの利用でも、個々のインスタンスごとに鍵が作成されます。
- データの保存とアーカイブは最小限：Proofpoint Encryption は、従来のメッセージ暗号方式で必要とされていた保存とバックアップを簡素化します。Proofpoint Hosted Key Service は Proofpoint on Demand の SaaS インフラを使って全ての鍵を管理します。



### Proofpoint の次世代 SaaS アーキテクチャによる暗号化

Proofpoint Encryption は PHKS により、鍵管理のオーバーヘッドを解消します。Proofpoint Encryption によって作成される鍵は、Proofpoint のクラウドインフラに保存され、バックアップされます。PHKS は鍵や証明書の管理を不要にします。

### PHKSの動作

- 個々のメッセージを暗号化するために鍵が作成され、暗号化されたメッセージは送信されます。
- 同時に、鍵そのものは PHKS に送られます。
- 受信者がメッセージを受信して開封すると、セキュアな https リクエストが発行されます。
- 受信者が認証されると、PHKS は適切な鍵を提供し、受信者はメッセージを復号化できます。
- この仕組みは、エンドユーザーが自分で暗号化 / 復号化のための鍵を管理する必要がなく、包括的で簡便な方法です。

# Proofpoint Encryption

## 特徴

### 容易な操作

Proofpoint Encryption はエンドユーザーに対して透過的に動作し、個々のクライアントにソフトウェアをダウンロードしたり、インストールしたり管理したりする必要はありません。Proofpoint の暗号化ソリューションは、エンドユーザーが複雑な電子証明書や暗号鍵を使ったり管理しなくても、ポリシーに従って重要なデータを含むコンテンツを自動的に暗号化します。

### 低いTCO

Proofpoint Encryption は Proofpoint Regulatory Compliance や Proofpoint Digital Asset Security などの、他の Proofpoint の DLP 機能とシームレスに統合されています。簡単な導入と最小の管理はセキュアなメッセージングソリューションを維持していくためのコストを劇的に引き下げます。また、Proofpoint の比類無い簡便さはサポートやトレーニング、ヘルプデスクのコストを最小化します。

## 強力でセキュアなポリシー適用

### 暗号化ポリシーの詳細な設定

Proofpoint のアンチスパム、アンチウイルスおよびコンテンツセキュリティ機能と同様、セキュアメッセージングセキュリティコンソールを使うことにより、全社的なセキュリティポリシーを、一カ所から管理することができます。いったんポリシーを定義してしまえば、暗号化ポリシーはゲートウェイの段階で適用されますから、エンドユーザーの操作ミスを心配せずに済みます。

Proofpoint Encryption と Proofpoint Hosted Key Service を併用することにより、非常に詳細な、メッセージごとの制御が可能になります。たとえば、特定の宛先へのメッセージだけを、他のメッセージには何ら影響を与えることなく、無効化したりすることができます。メッセージの暗号化ポリシーも、同様に非常に詳細に設定できます。

暗号化は、以下のどの組み合わせでも適用できます。

- 非公開情報 (NPI) の検出: Proofpoint Regulatory Compliance は、メッセージや添付ファイル中の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を「スマート識別子」として検知します。
- コンテンツマッチ: Proofpoint Digital Asset Security モジュールは、MLX 技術を使ってファイル間の類似性を解析し、非構造的な機密情報を検知します。
- Proofpoint Email Firewall と同様に、定義済み辞書を使って、キーワードおよび正規表現による検索が可能です。
- メッセージの送信元や宛先: 特定の宛先や送信者からのメッセージを暗号化します。添付ファイルの形式など、他の属性による暗号化も可能です。

### 暗号化されたメッセージへのインバウンドポリシーの適用

暗号化されたスパムやマルウェア、違法なメッセージを配信前に検出するために、ゲートウェイの段階で復号化してポリシーを適用することができます。

### 電子メール暗号化: 簡素化

Proofpoint Encryption は、エンドユーザーの負荷を軽減しつつ、重要なデータを保護するための仕組みを提供します。たとえば、医師が患者に対し、秘密の医療データを含むメッセージを送る場合を考えてみましょう。

プロセスは以下のように進みます。

- 医師が患者宛に、通常使っている電子メールクライアントを使ってメールを書き、送信します。Proofpoint の DLP 機能がメッセージの内容を検査し、機密情報を検出すると、暗号化ポリシーを適用します。
- Proofpoint Encryption が送信前に AES-256 を使ってメッセージを暗号化し、DSA 署名を使ってデジタル署名します。
- 患者は暗号化されたメッセージを受け取ると、Proofpoint Secure Reader を使って認証し、メッセージを復号化するためのアタッチメントをクリックします。Proofpoint Secure Reader は、Proofpoint on Demand またはローカルの Proofpoint アプライアンスで運用されている、暗号化メールを読むための Web ベースのアプリケーションです。
- 患者が正しく認証されると、Proofpoint Encryption は PHKS から正しい暗号化 / 復号化鍵を取得します。
- 患者は、Proofpoint Secure Reader を使って医師に安全に返信することができます。

©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。09/11