

Proofpoint Regulatory Compliance Module



大企業、大学、政府機関は、ある種の非公開情報 (NPI) の取り扱い方を定めるプライバシー関連法規の規制を受けますが、近年そうした法規が増え、また組織から発信される電子メールの内容にも規制が及んでいます。

包括的なコンプライアンス

アウトバウンド電子メールのコンプライアンス確保

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 Regulatory Compliance™ モジュールは、アウトバウンドの電子メールが、HIPAA、GLBA、PCI コンプライアンスガイドライン、SEC 規則など多種多様な電子メール関連法規を確実に遵守することを容易にします。定義済みの辞書と“スマート識別子”が、自動的なスキャンによって PHI (HIPAA によって規定された保護対象健康情報)、PFI (GLBA によって規定された個人金融情報) に加え、日本の運転免許証番号や住民票コードなど、幅広い非公開情報を探し、違反している通信に適切な対応がとれるようにします。

ルールは point-and-click インタフェースによって容易に作成や変更が行え、上記以外にも州法 (たとえばカリフォルニア州の California AB 1950 や California SB 1386 など)、カナダの PIPEDA、ヨーロッパのさまざまなプライバシー規制など、多様な情報保護やデータセキュリティについての法令遵守を行わせることができます。

特徴

電子メール内のあらゆるタイプのプライバシーデータを検知

Proofpoint Regulatory Compliance には組織が今日の情報保護規則を守ることを助ける幅広い機能がそのまま使える形で用意されています。Proofpoint Regulatory Compliance は、一般的な NPI 識別子だけでなく辞書にも基づき、発信されるすべての電子メールを監視して NPI を検知します。

定義済み辞書とカスタム辞書

さまざまな定義済み辞書とサンプルのポリシーが組み込まれています。これらの辞書には、一般的に保護される健康情報のコード体系——ヘルスケア業界で使われる標準的な疾病、薬剤、治療、診断などのコード (裏面のコラムを参照) ——が定義されており、HIPAA 遵守が簡単に行えます。Proofpoint には金融プライバシーの辞書——金融サービス業界で使われる SEC、インサイダー取引、取引確認などの用語——も組み込まれていて、GLBA、PCI、および SEC とのコンプライアンスを助けます。

新しい辞書を定義することもできます。こうした辞書では完全一致も正規表現もサポートが可能です。組み込まれている HIPAA 辞書は拡張が可能で、特定の医療環境に特有の用語やコードを含めることができますし、NASD や PIPEDA などその他の規制を遵守する新しい辞書を追加することも可能です。辞書の用語には、用語毎に強度を増減し最適なウェイトを設定することや、例外を許すこともできます。インストールされている辞書のコードが常に最新の状態になっていることは Proofpoint Dynamic Update Service™ が保証します。

日本運転免許証など各種 NPI 識別機能

Proofpoint Regulatory Compliance は、日本の運転免許証番号や住民票コード、アメリカの社会保障番号や銀行協会銀行支店コード、JCB をはじめとするクレジットカード番号など、国内外の一般的な NPI 識別子をスキャンすることもできます。これらの“スマート識別子”は単純な正規表現よりも精巧で、正しい桁数の数字だけでなく、チェックサムの計算も行って、NPI に類似した数字列が実際に保護される情報であることを確認します。この技術は擬陽性の確率を大幅に削減します。カスタムスマート識別子も容易に追加することが可能で、アカウント番号、患者番号、医療記録番号、請求番号、ローカルな形式の身分証明書番号など、組織固有のデータタイプを識別させることができます。Proofpoint に組み込まれているスマート識別子同様、カスタムで作成された識別機能は複雑なアルゴリズムの処理を行って、高精度を確実にして擬陽性を最小限に抑えることができます。



柔軟なメッセージ処理

NPI を含んでいると識別されたメッセージは、Proofpoint の標準的なメッセージ処理のいずれかを使って対処することができます。

- 暗号化、または暗号化デバイスにリルート。たとえば、PHI 辞書に入っている用語を 3 つ以上含むメッセージは、Proofpoint Secure Messaging モジュールへ自動的に送ることができます。
- リダイレクト。メッセージを法務またはコンプライアンスの責任者へ送って、さらにレビューしてもらい、またはメッセージを保存と監査証跡のためアーカイブのメールボックスに送ります。
- 検疫。メッセージを特定のフォルダに送り、後で再検査します。
- 送信者に返信。違反を記述した本文に、組織のプライバシーポリシーを説明しているイントラネットのサイトへのリンクを付けた電子メールを送信者に送ります。
- 拒否またはブロック。厳格なポリシーを採用したい場合、これらのオプションを使うと適合しないメッセージが組織から発信されないことを保証できます。
- ヘッドを付加。メッセージヘッドに文字列を追加して、Regulatory Compliance モジュールによってフィルタリングされたすべてのメッセージを追跡します。
- 注釈。メッセージのフッタまたは件名行の注釈として、メッセージに免責条項を追加します。

Proofpoint Regulatory Compliance Module

特徴

柔軟なプライバシールールとポリシー定義

point-and-click インタフェースによって、複雑なプライバシールールの定義や変更も手早く簡単に行えます。ルールはNPIそれぞれの発生に適用させることも、辞書またはNPI識別子が一定数に達したときに適用させることも可能です。たとえば、クレジットカード番号の詐欺や盗難を追跡するルールを、1メッセージ内に3個以上のクレジットカード番号が検知されたときにのみ起動するように設定することができます。

特定のコンプライアンス要件を満たすためのプライバシールールはいくつでも定義できます。複数のルールをポリシーにマッピングすることが可能です。たとえば、HIPAA ポリシー、GLBA ポリシー、AB 1950 ポリシーなどが定義できます。ポリシーは、リストに指定した取引先のみや、インバウンドまたはアウトバウンドのメッセージルートのみに適用するよう、さらにカスタマイズが可能です。

暗号化のサポート

多くの法令では非公開データを、セキュアな暗号化されたフォーマットで送信するよう定めています。Proofpoint Regulatory Compliance は数種類の暗号化をサポートしています。

○ TLS (Transport Layer Security)

Proofpoint Messaging Security Gateway アプライアンスと組み合わせて使う場合、Regulatory Compliance モジュールを使って電子メールを常に暗号化しなければならない一連の取引先を定義することができます。これらの取引先に送信されるメッセージは自動的にTLSゲートウェイ間暗号化プロトコルを使って送られます。

○ Proofpoint Secure Messaging およびその他サードパーティ暗号化ソリューション

Proofpoint Secure Messaging™ によって、メッセージの内容を自動的に認識して暗号化することができます。検知されたNPIの内容、送信者、宛先、その他の条件によってメッセージを暗号化するポリシーが、簡単に構成できます。さらに、Proofpoint Regulatory Compliance は、さまざまなサードパーティのセキュアメッセージングソリューションと容易に統合できます。

レポート

Proofpoint Regulatory Compliance は、コンプライアンスの進行状況の監視や追跡をグラフィックなレポートによって助けます。これらのレポートには指定された期間内の法令違反の合計回数と共に、こうしたポリシーへの主な違反者が示されます。レポートはスケジュールに基づいて電子メール送信させることも、イントラネットのサイトに置くことも可能です。

大部分の企業では、コンテンツのセキュリティポリシーが、コンプライアンスやデータ保護の責任者であるさまざまなビジネスユーザによって管理されています。Proofpoint Compliance Incident Manager™ のレポートは、これらの管理者がコンテンツのセキュリティ違反を追跡・レビューして、適合しないメッセージに適切なアクションを取ることを助けます。管理者にはポリシー違反とその重大度レベルが即座に通知されるので、ビジネスユーザにもメッセージのリリース、リルート、承認、または廃棄が、Proofpoint のグラフィカルユーザインタフェースを使って容易に行えます。

電子メールによる法令違反のリスクがどの程度か理解するための第一段階として、Proofpoint Regulatory Compliance を監査モードで導入することが可能です。これによって、メッセージには何の変更も行わずにすべての法令違反の監視が行えます。その後、レポートを使ってリスクのレベルを測ることができます。

添付ファイルのスキャンと独自のドキュメントタイプのサポート

ビルトインの添付ファイルスキャン機能によって、Regulatory Compliance ポリシーをメッセージの添付ファイルにも適用することが可能です。300種類以上のドキュメントタイプについて、その内容にポリシーを適用することができます。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て、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。

より強固なセキュリティ

プライバシーやデータセキュリティに関する法令の多くは非公開データの扱いに関する規則だけでなく、こうした情報を処理するシステムについてもセキュリティ要件を定めています。Proofpoint はこうした法令が要求するセキュリティやアクセスコントロールを満たす機能を提供します。

厳格なパスワードポリシー

任意に厳格なパスワードを要求して、パスワードの期限を限定するよう、サーバに設定することができます。

アクセスコントロール機能

Regulatory Compliance モジュールに対するアクセスを選ばれた個人やグループに限定することができるので、権限を持つ職員だけがコンプライアンスポリシーの作成や変更を行えます。

辞書と識別子

幅広いプライバシー規制に対応する基本的な構成要素を、そのままですぐに使える形で組み込んでいます。

ヘルスケアのコード体系

モジュールにはHIPAAをはじめとするヘルスケア規制へのコンプライアンスで要求されるPHI検知用のコード体系を組み込んだ多数の辞書が用意されています。

- ICD-9-CM 診断および処置コード
- HCPCS 一般処置コード
- NDC 薬剤コード
- その他多数の医療コード体系

金融およびプライバシーのスマート識別子

日本国内をはじめ各国の個人情報やPFIを検知するスマート識別子が組み込まれています。以下はその一部です。

- 日本運転免許証番号や住民票コード、アメリカ社会保障番号、カナダ社会保険番号、イギリス国民保険番号、その他個人識別情報
- アメリカ銀行協会銀行支店コード
- 各種クレジットカード番号(日本JCB、アメリカおよび国際標準など各種対応)
- CUSIP証券識別コード、SECファイリング、取引確認

カスタムスマート識別子

プラグインのアーキテクチャによってカスタムや地域に独特のデータタイプに応じたカスタムスマート識別子を追加することができます。次はその例です。

- 医療記録番号
- 金融サービスの口座番号
- 地域的な個人識別フォーマット(運転免許証番号、身分証明書番号など)

©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 Dynamic Update Service, Proofpoint Content Compliance, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, 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