Digital Communications and Governance / デジタルコミュニケーション & ガバナンス

無秩序なデジタル社会でコミュニケーションをスマートに管理する

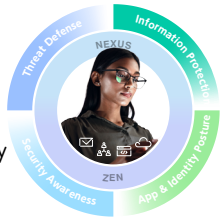
製品

- Proofpoint Capture / コミュニケーションのキャプチャ、管理、保持
- Proofpoint Patrol / ソーシャルメディアの監視と修復
- Proofpoint Track / データ送信の調整とコントロール
- Proofpoint Archive / e-Discovery対応メールアーカイブ
- Proofpoint Discover /高度なe-Discovery分析
- Proofpoint Supervision / コンプライアンス遵守確認作業の支援
- Proofpoint Automate / 高度なケース管理と分析

主なメリット

- 多くの一般的なデジタル コミュニケーション プラットフォームにおいて不正行為を数秒でインテリジェントに検知
- 調査における確認時間を大幅に削減
- プライベートクラウドでもネイティブ パブリッククラウドでもデプロイできる優れた柔軟性
- コンプライアンスを確保できる統一された方法でユーザーデータを管理
- 堅牢かつ高速なデータの取り込みと分析でデータ移行を迅速化し、時間とコストを節約
- あらゆるコンプライアンス要件や企業のポリシーに先手を打つ

このソリューションは、人に起因する4つの主要リスクを低減する、プルーフポイントのHuman-Centric Security統合型プラットフォームの一機能です。



バーチャルファーストの流動的な経済状況において、モバイルツールやインスタント メッセージ ツール、クラウドコラボレーション プラットフォームの使用が急激に増加しています。今日のワーカーは、こうしたツールを使用して外出先で人とやり取りをしたり、作業を行ったりしています。今やかつてないほど、Microsoft Teams、Slack、Zoomなど、確立されたプラットフォームで関係を構築したり、やり取りするようになっており、さらに数百の新しいツールが登場し続けています。

例えば、Microsoft Teamsは3億2000万の月間アクティブユーザーを抱えています[1]。Slackユーザーは、毎週15億のメッセージをサービスに送信していると報告されています[2]。こうしたデジタル コミュニケーションが乱立する時代において、最近調査を行ったデータ責任者の約41%が、1千を超えるデータソースへの対応に追われていることも驚きではありません。こうした責任者の3分の1以上が、データプライバシーとセキュリティの向上や、データの管理とガバナンスの自動化を望んでいます[3]。

企業は今や、デジタル コミュニケーション全体において、最高レベルのリスクと脅威にさらされています。また、コミュニケーションが乱立している問題にも直面しています。IT、コンプライアンス、法務、セキュリティのチームにとって、これは、組織にとって最も重要なアセットである従業員の保護に注力しなければならないことを意味します。

この課題をプルーフポイントが解決します。プルーフポイントは、多様なデジタル コミュニケーションの統合、管理、保存、調査、監視をサポートするAIベースのデジタル コミュニケーション ガバナンス プラットフォームを提供します。Proofpoint Digital Communications Governanceにより、必要十分な企業・規制コンプライアンス保護を構築できます。

1 Microsoft、Microsoft Fiscal Year 2024 First Quarter Earnings Conference Call (Microsoft 2024年第1四半期 電話カンファレンス)、2023年10月
2 David Curry (Business of Apps)、「Slack Revenue and Usage Statistics (2024)」(2024年Slackの収益と使用状況の統計)、2024年1月
3 CDO Magazine Bureau、Why CDOs Need AI-Powered Data Management to Accelerate AI Readiness in 2024 (2024年、CDOがAIレディネスを加速するために、AIを活用したデータ管理を必要とする理由)、2024年3月

バーチャルファーストへの移行において最も問題となるのは「人」

デジタル変革はもはや新しいパラダイムシフトではなくなっており、すでに問題が起きています。影響を受けているのは、従業員、通信方法、使用するツールなどです。従業員が日常的にコミュニケーションを取るために使用する方法は6つ以上にのぼります。リモートワークへの移行により、従業員が使用し、やり取りするためのデジタル プラットフォームの導入がますます増えています。

社内コミュニケーションやプロジェクト コラボレーションはオンラインで行われるようになっています。顧客や見込み客はソーシャルメディアで組織とつながることを求めています。組織は、こうしたコンテンツをキャプチャ、管理、監視、保持できなければなりません。これは、組織が規制対象になっている場合、訴訟リスクが高い場合、高度な可視性が要求される企業ポリシーを導入している場合などに、特に重要です。

さらに規制上および法的な理由から、訴訟や監査に際しては、保持しているコンテンツを検索できる必要があります。組織のリソースが限られていたり、先進的な職場環境についていけない旧式のテクノロジーを使用していれば、従業員は仕事で能力を十分に発揮できない可能性があります。

プルーフポイントは、効果的なセキュリティおよびコンプライアンスの戦略の構築と維持をサポートする、強力なデジタル コミュニケーション ガバナンス ポートフォリオを提供します。プルーフポイントのアプローチは、人と情報の保護を中心に据えています。訴訟リスクの高い、特に厳しい規制の対象になっている組織のための戦略は、以下の手順で構成されます。

1. コミュニケーションのキャプチャ
2. コミュニケーションの戦略的管理
3. コミュニケーションを完全な精度で保持し、記録証明を作成
4. コミュニケーションのインテリジェントな分析、監視、監督

さまざまなチャネルにおける信頼性の高いコミュニケーション

組織において何が起こっているかを理解するために、非持続型ですぐに消えてしまうコミュニケーション コンテンツをリアルタイムでキャプチャし、管理する必要があります。また、こうしたコンテンツを、アーカイブシステムや監視システムなどのダウンストリーム サービスに振り分ける必要があります。

メールについて必要なソリューションを導入している組織でも、その他のコンテンツソースについてはソリューションを導入していないこともあります。Microsoft TeamsやSlackといったコンテンツソースとダウンストリーム サービスとの接続をIT部門が構築している組織もあるでしょう。

しかし、こうした種類のカスタム接続は理想的ではありません。多くの場合、重要な情報をキャプチャできないばかりか、接続を維持するためには常に社内リソースを割かなければなりません。さらに、ソースごとに情報のフォーマットが異なることも多く、同時に起こったすべてのやり取りのコンテキストを理解することが困難になっています。

Proofpoint Capture

Proofpoint Captureは、新しいものも含め、一般的に使われているさまざまなコミュニケーション ソースからのコンテンツを、セキュアな方法で収集します。このコンテンツをダウンストリーム サービスへと送ることもできます。完全な精度とコンテキストでコンテンツをキャプチャします。これを使えば、必要な情報の検索、管理、確認が容易になります。Proofpoint Captureはすべてのコンテンツを1つのプラットフォームで統合します。また、コンテンツソースのアップデートも監視して、常に最新の接続が維持されるようにします。

コミュニケーションの管理とコントロール

金融サービスや、訴訟リスクの高い企業などの業界では、コンプライアンス規制に違反するコミュニケーションはブロックまたは修復する必要があります。これにより、従業員と組織を罰金や法的問題から保護することができます。成長過程にある組織や地理的に分散した組織であれば、インテリジェンスを活用したテクノロジーを使って従業員を保護することもできます。

手作業の分析やランダムなサンプリングだけでは、注力すべき問題を見逃すことも、リスクの低いもののために貴重なリソースを消費することもあります。

コミュニケーションとデータを戦略的に管理すべきです。これにより、真のリスクの解決に注力できます。ソーシャルメディアやその他のパブリックチャネルにおける迅速な対応にもつながります。コンプライアンス違反が起これば迅速に修復することが重要です。このことが拡散し、不本意な注目を集めてしまう前に対処する必要があります。

Proofpoint Patrol

Proofpoint Patrolにより、ソーシャルメディアの監視、コントロール、修復のルールに対応することができます。Proofpoint Patrolは、従業員とブランドのソーシャルメディア上でのプレゼンスをリアルタイムで完全に可視化します。機械学習と自然言語処理を使用して、監視対象のアカウントにあるコンテンツを正確に分類します。従業員または企業のアカウントからコンプライアンス違反を検知すると、問題になる前に通知します。問題のあるコンテンツを削除するよう設定することもできます。

コミュニケーションを完全な精度で保持する

現代のコミュニケーションは、安全で、アクセス可能、かつ検索可能なアーカイブで保持する必要があります。記録の証明も作成できる必要があります。従来からのオンプレミスのソリューションでは、クラウドベースのコミュニケーションに対応できない場合や、検索のスピードが遅くなる場合があり、多くの場合、想定されるサービスレベル アグリーメントもありません。これでは、監査やe-Discoveryにすぐに対応することができません。特に、監査の場合は、組織の記録が完全であって、裏づけが得られることが必須です。

Proofpoint Track

Proofpoint Trackにより、コンテンツを不変のデータストアで転送・維持でき、コンプライアンスに準拠した記録保持や調査のためにアーカイブしておくことができます。コンテンツソースから得られた各メッセージがアーカイブで適切に処理されていることを確認するフィードバック ループ機能が内蔵されています。プロセスが失敗すればデータを再送します。Proofpoint Trackは、コンテンツをフィルタリングして複数のサービスへ振り分ける場合にも使用できます。

Proofpoint Archive

Proofpoint Archiveは、インテリジェントなクラウドネイティブのアーカイブ ソリューションです。長期的な事業上および規制上のデータ保持要件を満たすことができます。メールと他のデジタル コミュニケーション プラットフォーム（インスタント メッセージング、コラボレーション、ソーシャルメディアなど）のコンテンツをサポートしています。Proofpoint Archiveは、高パフォーマンスの検索、訴訟ホールド、エクスポートを提供します。これらの機能により、重要なe-Discovery要件すべてに対応できます。

FedRAMP認定

FedRAMP（Federal Risk and Authorization Management Program）とは、米国政府機関によるクラウドサービスの導入と使用について、セキュリティ要件が規格化されたものです。米国政府機関は、ベンダーのクラウドサービスが政府機関の情報を適切に保護していることを確認するためにFedRAMPを用いています。Proofpoint Archiveは、FedRAMPのセキュリティインパクトレベル「中」の認定を受けています。

PCI DSSコンプライアンス

基本的なレベルで、ペイメント カード インダストリー データ セキュリティ スタンダード（PCI DSS）は、決済カード情報を保護するための基本的な要件を定めたものです。決済カード情報を長期間保存する場合は、PCI-DSSに準拠したアーカイブが必要です。Proofpoint ArchiveはPCI DSSに準拠しています。PCI DSS準拠状況についてさらにご確認いただくには、ご要望に応じて、プルーフポイントのAoC（Attestation of Compliance、コンプライアンス証明）やResponsibility Matrix（責任マトリクス）をお見せできます。

調査時間を数日から数秒に短縮

医療、製薬、小売、その他のBtoC業界において訴訟リスクの高い企業は、e-Discoveryや調査への対応に苦労しています。これは、知見が適時に得られず、効果的な決定が行えないためです。訴訟において関連性の高い証拠を速やかに提出できなければ、企業には高い罰金やその他のネガティブな結果が待っています。

Proofpoint Discover

Proofpoint Discoverは、アーカイブ検索パフォーマンスとアーカイブシステムの可用性の両方に対し、財務的に支援されたサービスレベル アグリーメントを提供する、Proofpoint Archiveを補完するものです。Proofpoint Discoverは、組織のe-Discoveryワークフローを効率化し、関連コストを削減する高度な機能を提供します。

ケース管理機能により、コラボレーションやケースの進捗状況の追跡も可能です。Proofpoint Discoverは、e-Discoveryの要請や社内調査への対応を調整します。高度な視覚化ツールにより、直感的に検索結果から一定の知見を得ることもできます。

非準拠による多額の罰金を回避

特定の業界や部門においては、従業員の監督や監視を求める規制要件が数多く存在します。北米の金融サービス企業の場合、FINRA 3110、SEC 206(7)、IIROC NI 31-103、CFTCといった規則があります。ヨーロッパでは、英国のFCA、EUのESMAとMiF ID IIがこうした規制に該当します。こうした規制に準拠していない場合、多額の罰金などの処罰が下されます。

Proofpoint Supervision

Proofpoint Supervisionもまた、Proofpoint Archiveを補完するサービスです。デジタル コミュニケーションやメールが企業・規制コンプライアンスに沿っているかを監視できます。コンプライアンス リスク ダッシュボードからは、インテリジェントなアプローチを生かして、主なコンプライアンス リスクや違反傾向を特定できます。より深い知見を得るために選択的に掘り下げた分析を行うこともできます。高度なフィルタリング、サンプリング、検知により、結果におけるノイズを減らすことができます。これにより、特定のコンテンツがなぜリスクの可能性ありと判定されたのかがわかりやすくなります。

Proofpoint Automate

Proofpoint Automateは、プルーフポイントの機械学習インフラをベースに構築されています。設定不要の検知モデルにより、市場乱用の行為、従業員の不正行為、誤情報の共有のリスクを検知することができます。モデルは、無数のレビュー担当者の決定と共にトレーニングされているため、価値や関連性の低いコンテンツは排除されています。Proofpoint Automateは、従来のシステムと比較して、誤検知を最大84%減少させることができます。監視プロセスを効率化し、コストを効率化することができます。

詳細は、proofpoint.com/jp/products/digital-communications-governance をご確認ください。

詳細はこちら：proofpoint.com/jp