Proofpoint Information Protectionのアクセスとプライバシーの制御

従業員の権利を保護し、バイアスを排除しながらコンプライアンス要件に対応する

主なメリット

- 従業員の信頼を維持
- 重要なビジネス情報を保護
- プライバシー規制への準拠
- 調査におけるバイアスを防止

このソリューションは、人に起因するリスクの4つの主要エリアを低減する、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。

データプライバシーの保護はますます重要かつ困難になってきています。さらにデジタルトランスフォーメーションの急速なペース、ハイブリッドワーク、クラウドアプリケーションの普及により、機密データを保護する作業はかつてないほど複雑になっています。また、組織がこれまで以上に大量のデータを収集し続けているため、データに対する価値が認識されるようになっています。残念なことにこのような価値の増大は、内部関係者からの情報漏えいや情報窃取のリスクももたらします。

しかし課題が山積みになっているからといって、企業にミスは許されません。世界中の企業は、強力なデータセキュリティとプライバシー対策を義務付ける厳格なプライバシー法の遵守に迫られています。コンプライアンス違反は大きな代償となり、多額の罰金や市場機会の喪失などを引き起こします。実際に、セキュリティ担当者の3分の1以上が、情報漏えいが発生すると、規制上の違反とみなされ、罰金が科せられると述べています[1]。

プルーフポイントは、データセキュリティを強化し、内部脅威を管理し、データプライバシー規制への準拠を確保する、包括的な製品スイートを提供します。Proofpoint Information Protectionソリューション ファミリーは、堅牢なアクセスとプライバシーの制御を実装します。本当に知る必要がある人のみに可視性を制限し、個人を特定できる情報を機密扱いにすることで、ユーザーの匿名性を維持します。これにより、プルーフポイントは、データセキュリティを強化するだけでなく、調査におけるバイアスを排除することもできます。また情報セキュリティにバランスの取れたアプローチを採用することが可能となります。

プライバシー ファーストのアプローチ

Proofpoint Information Protectionは、プライバシー バイ デザインの原則の下にゼロから構築されています。この手法は、データ保護に対するプロアクティブなアプローチを採用しています。システム設計の最前線にプライバシーを置くことで、ITシステム、インフラストラクチャ、業務プロセスにおいて、プライバシーが最初から考慮すべき重要な事項となります。このアプローチは、可視性、透明性、ユーザー中心をその設計に統合するものです。

1 「Proofpoint 2024 Data Loss Landscape - 情報漏えいの全容」レポート

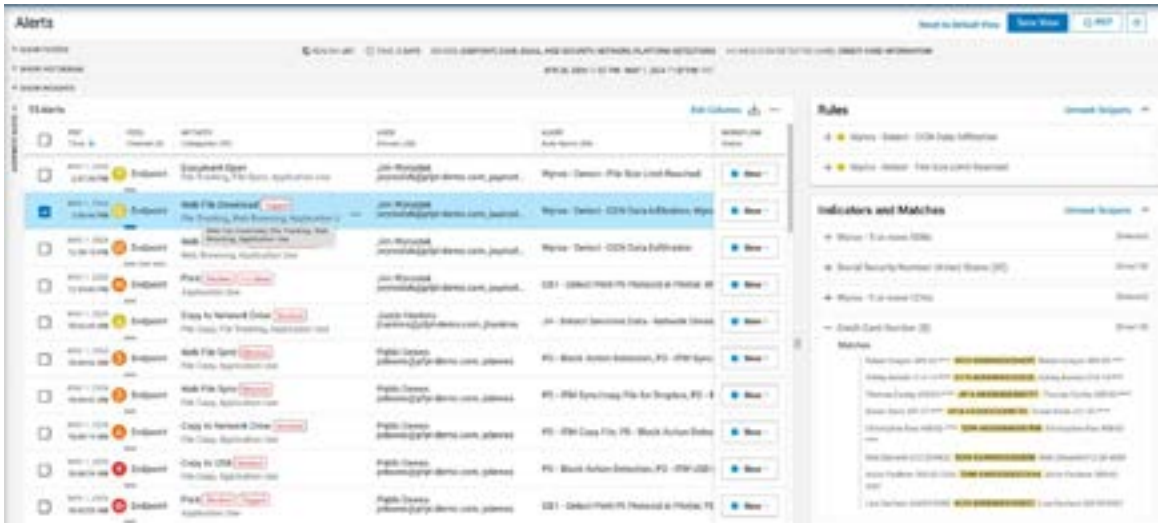

図1:Proofpoint Information Protectionでのクレジットカード番号のマスキング

データの保存先や保管の管理

プルーフポイントは、米国、カナダ、欧州、オーストラリア、日本の地域別データセンターを戦略的に配置し、データプライバシーとデータ保存先の要件に対応しています。これらのすべてのデータセンターで、データの保存場所を完全に管理することができます。

エンドポイントのデータストレージを管理するために、プルーフポイントでは、「レルム」(Realm)と呼ばれるエンドポイントのグループ化を行うことができます。各レルムは、特定のデータセンターに割り当てることができるため、簡単にデータを地理的に分離することができます。例えば、米国のレルムは、米国のデータセンターに送信されるエンドポイントデータを管理するように設定できます。

属性ベースのアクセス制御でプライバシーに対応する

Proofpoint Information Protectionの属性ベースのアクセス制御は、データアクセスを管理するための柔軟かつ効率的な方法を提供します。これにより、セキュリティ アナリストは、知る必要がある範囲でのみデータを可視化できます。

例えば、米国を拠点とするセキュリティ アナリストは、欧州またはアジア太平洋地域のデータを見ずに、米国のデータだけを表示できるようにきめ細かいポリシーを作成し、アクセスをを割り当てることができます。特定のアクセス制御をこのようなレベルで適用できるため、不必要にデータがさらされるリスクを大幅に低減することができます。

また、アナリストが調査のために特定のユーザーデータにアクセスする必要があれば、システム管理者は、このアクセスに時間制限をかけることもできるため、アナリストがこのデータをどのぐらいの間表示できるかを指定することができます。

スニペット マスキングでデータを非公開に

Proofpoint Information Protectionは、データマスキング機能により、データのプライバシーを保護します。データマスキングは、コンソールに保存されている保護されるべき医療情報(PHI)や個人を特定できる情報(PII)といった機密のフォレンジックデータを把握しづらくし、こうした情報を特定できないようにします。このアプローチにより、データにアクセスする必要がある人だけが、マスクされていない状態でデータを完全に確認することができます。

システム管理者は、隠したいデータ識別子を設定することができます。例えば、クレジットカードの下4桁のみを表示し、残りはすべて隠すといったことが可能です。また、ユーザーの役割に応じて、そのユーザーがどのようなデータをどのぐらい表示できるかを設定することも可能です。例えば、承認されたアナリストのみが機密データのスニペットを表示するように設定することができます。

ユーザーデータを匿名化で保護する

Proofpoint Information Protectionはまた、匿名化によってユーザーデータを保護し、ユーザーのアイデンティティ(身元)を隠すことができます。ユーザー名、ホスト名、IPアドレス、位置情報、ファイル名を匿名化できます。

匿名化により、承認されたセキュリティ アナリストのみが監視対象のユーザーを特定できる情報を表示することができます。このプロセスは、調査におけるバイアスを排除するのに役立ちます。例えば、企業ポリシーに違反したユーザーが経営幹部であったとします。違反したのが経営幹部だと知ってしまっては、違反の処理に手心が加わるかもしれません。あるいはセキュリティ アナリストが見て見ぬふりをするかもしれません。

図2:Proofpoint Information Protectionでのユーザーデータの匿名化ビュー

調査を進めていくうちにユーザーのアイデンティティを明らかにする必要があれば、セキュリティ アナリストは、権限をもつ管理者に匿名化の解除を要求することができます。

データプライバシーとセキュリティのバランスを取る

データプライバシーとセキュリティのバランスを取ることは、どの組織にとっても重要です。これを効果的に行うには、以下の原則を覚えておく必要があります。

- **重要な情報漏えいチャネルを監視:** 従業員の働き方に合わせたデータセキュリティの取り組みを考えます。ほとんどの情報漏えいは、メール、クラウド アプリケーション、USBドライブ経由で発生します。
- **明確性と透明性を維持:** 従業員に、データセキュリティやプライバシーに関する企業ポリシーを周知徹底します。また、組織が監視している情報を正確に伝えます。こうすることで信頼が築けます。
- **自動通知でユーザーを教育:** 企業ポリシーに違反したユーザーに、自動的に通知が送信されるようにします。自動通知を使用することにより、人事部や上司とこのことについて話す上で恥ずかしさを味わったり、感情的になったりすることなく、リスクのある行動についてユーザーを教育することができます。
- **選び分ける:** すべての人、すべてのことについてデータを収集する必要はありません。どのデータが重要であり、従業員の行動について本当にどのぐらい知る必要があるかを判断します。
- **データアクセスを制御:** セキュリティ管理者、アナリスト、法務部門、人事部門は、従業員に関するデータへのフルアクセスが可能である場合があり、これはプライバシーの観点から見ると、必ずしも良いものとは限りません。そこで、情報漏えい対策(DLP)ツールやITMツールに付属するアクセス制御を使用します。

プルーフポイントでデータプライバシーを確保する

Proofpoint DLP (Data Loss Prevention) やProofpoint ITM (Insider Threat Management) など、Proofpoint Information Protection ソリューションを使用することで、データプライバシー規制に準拠しながら、最も強力なデータ保護を維持することができます。これはまた、調査におけるバイアスを排除する上でも役立ちます。Proofpoint Information Protection は、コンテンツや振る舞いを認識できるため、機密データや規制対象データを特定できるだけでなく、リスクのあるユーザーアクティビティや悪意のある意図にフラグを付けることができます。これらすべてを行える一元的なコンソールが、エンドポイント、メール、クラウド、Webなど、さまざまなチャネルを可視化します。

Proofpoint Managed Information Protection は、正しい人、プロセス、技術を統合するものです。これにより、組織のプログラムの設計、実装、進化が可能となり、データ保護を最適化し、データプライバシーを確保することができます。

詳細はこちら

詳細は、**proofpoint.com/jp**でご確認ください。