proofpoint.

情報漏えい対策ソリューションのバイヤーズガイド

本バイヤーズガイドでは、先進的な情報保護ソリューションにおいて最も重要な機能をご紹介します。本ガイドは、世界中のあらゆる業界、あらゆる規模の組織のために、プルーフポイントが情報漏えい対策（DLP）プログラムを構築してきた経験から培われた知識をまとめています。DLPの取り組みをはじめたばかりの方や、既存のDLPシステムのアップデートを進めている方に、便利な参考ガイドとしてご利用いただけます。

「人」を中心としたセキュリティで始める

一般的な脅威や特別な脅威からデータを保護するには、「人」を中心としたHuman-Centricなセキュリティモデルをサポートするプラットフォームが必要です。では、「人」を中心としたセキュリティモデルとは何でしょうか? このモデルの基本は、ユーザーが機密データをどう扱っているかを完全に可視化し、リスクのある行動があればこれを追跡することです。これにより、データが紛失した、もしくは盗まれた場合、またはユーザーが不審な行動を取った場合に、その意図について重要なコンテキストを得ることができます。

「人」を中心としたアプローチを採用したソリューションにより、メールやエンドポイントに加え、Microsoft 365、Google Workspace、Salesforceなどのクラウドアプリにおける情報漏えいリスクを短時間で確認することができます。このように知見を得ることにより、迅速に行動し、情報漏えいインシデントを防ぐための適切な措置を講じることができます。

先進的なDLPソリューションの主要要素

情報漏えいを抑止し、内部脅威を阻止するには、インシデントの検知、分析、防止、対応を実行できなければなりません。これらのアクションが連携して、はじめてリスクを減らすことができます。

監視

データを保護するためにコンテンツだけにフォーカスしていては不十分です。ユーザーがそのコンテンツで何を行っているかを可視化する必要があります。エンドポイント、メール、クラウド、Webにおいてすべてのユーザーのデータアクティビティを監視することにより、包括的なビューとコンテキスト化された知見が得られます。

85%

2023年に情報漏えいインシデントを1回以上経験した組織の割合

50%

過去2年間で転職し、退職時にデータを持ち出したことを認めた社会人の割合

検知

可能な限りリアルタイムに近い状態で、たとえ本格的な「インシデント」のレベルには達していないような場合でも、ユーザーが危険なアクションを行った場合、またはデータが潜在的にさらされた場合、これを検知できるソリューションが必要です。検知機能は、バランスの取れたアラートを提供できなければなりません。つまり、適時かつ対応可能なものである必要があります。アラートが多すぎて疲れるようなことがあってはなりません。

分析

すぐれた分析により、ユーザー行動の傾向を把握し、脅威を察知できます。これを実現できる唯一の方法は、複数のチャネルにおけるユーザー アクティビティを組み合わせることができるDLPソリューションです。これにより、リスクのあるユーザー行動をとらえることができます。これを自動的に実行しながら、必要に応じて分析者がデータを深く探ることができなければなりません。

対応

インシデントを迅速かつ効率的に調査し、対応することが重要です。内部脅威が長く続けば続くほど、組織の評判や収益に与える被害は大きくなります。先進的なDLPソリューションなら、自動的にポリシーを適用し、脅威を修復できます。自動化により、貴重なデータの安全性を維持し、セキュリティチームの効率を高めることができます。

防止

防止とは、ユーザーが誤ってまたは意図的にセキュリティ ポリシーに違反しないようにすることです。これは、ユーザー教育、リアルタイムのリマインダー、そして必要に応じてユーザーの行動を阻止することで実現できます。

3つの主なユースケース

組織のデータが漏洩する主な経路は3つあります。これらはすべて人が原因です。「人」を中心とした情報保護プラットフォームは以下に対処する必要があります。

- 機密データに注意を払わない不注意なユーザー
- 生成AI(GenAI)アプリの使用時に機密データを流出させている不注意なユーザー
- 意図的に害を加えようとする、悪意のある内部関係者

$35億 2025年までに予想されるDLP支出総額[1]

77日 内部脅威の解決にかかった日数[2]

85% クラウド攻撃で標的となった組織の割合[3]

56% ユーザーの不注意に関連したインシデントの割合[4]

1：不注意なユーザーと一般的なミス

プルーフポイントの「Data Loss Landscape 2024 - 情報漏えいの全容」レポートによると、情報漏えいの主な原因は不注意なユーザーとされています。こうしたユーザーは、データを故意に流出させているのではなく、むしろ、ただできるだけ効率的に仕事をしようとしてミスをおかしてしまいます。しかし、こうしたミスが、事業中断、ブランドの風評被害、競争力低下、規制に対する違反や罰金、訴訟といった、重大な結果につながるおそれがあります。

こうしたユーザーによる、リスクをもたらしうる行動をいくつかご紹介します。

- 添付ファイルの有無を問わずメールの送り間違い
- フィッシングサイトへのアクセス
- 未承認のソフトウェアのインストール
- 機密のファイルやデータの公開
- 個人を特定できる情報（PII）を個人のメールアカウントに送信
- 機密の企業データを個人のデバイスに保存

不注意な行動への対策

リスクのある行動を阻止するには、「人」を中心とした効果的な情報保護システムが必要です。また、どのような行動が正しくなかったかについて指導できる機能があれば、不注意なユーザーは行動を改めることができます。

重要なポイント

- **分類：**メール、データ、およびコンテンツを、手作業とAIの両方で常に監視して、リスクのあるユーザーを特定し、分類する必要があります。ユーザーが「高リスク」に分類された場合、リスクスコアを割り当て、これに応じたデータ保護を提供できることがシステムに求められます。
- **検知：**システムはメール、ドキュメント、データを監視し、コンプライアンスリスクを一貫して評価できる必要があります。コンテンツは、エンドポイント、メール、クラウド、Webなどのチャネル間を移動するため、こうした移動や共有が組織のポリシーに違反していないことを確認するために、検査できる必要があります。メールにおいて違反が検知された場合、セキュリティチームがメールを阻止する、または詳細な調査のために追跡できるようなシステムが求められます。
- **防止：**さまざまなチャネルやデバイスにおいてユーザーによる機密データの持ち出しを阻止する必要があります。添付ファイルの有無を問わずメールの誤送信、USBメモリ、Webアップロード、クラウド同期、印刷が監視対象です。ユーザーがミスをすれば、コンテキスト化された警告メッセージを瞬時にそのユーザーに提供し、管理者による操作不要で、リアルタイムで情報漏えいインシデントを修復し、防止できる必要があります。ユーザーがデータにアクセスすることが正当であれば、その理由を説明できるはずです。セキュリティチームはその説明に基づいてアクセス要求を許可または拒否できます。

1 The Radicati Group、「Data loss prevention (DLP) market value revenue forecast worldwide from 2019 to 2025」（2019年から2025年の世界の情報漏えい対策（DLP）市場収益の予想）、2022年5月
2 Ponemon Institute、「2022 Cost of Insider Threats Global Report」（2022年内部脅威による損失グローバルレポート）、2022年2月
3 Assaf Friedman、Itir Clarke（プルーフポイント）、「How Attackers Use Compromised Accounts to Create and Distribute OAuth Apps」（攻撃者が不正アクセスしたアカウントを使ってOAuthアプリを作成し、配布した方法）、2021年5月
4 Ponemon Institute、「2022 Cost of Insider Threats Global Report」（2022年内部脅威による損失グローバルレポート）、2022年2月

2：不注意なユーザーと生成AIアプリ

ユーザーは、ChatGPTや他の生成AIツールを使用することにより、生産性を大幅に向上させることができます。しかし、機密データは多くの場合、こうしたツールから漏えいします。生産性が抑制されることなく、情報漏えいを回避するには、堅牢なデータ保護対策が必要です。そこで、生成AIに適切な利用規定を適用するには、コンテンツについてや、従業員がどのようにこうしたコンテンツを扱っているかを理解する必要があります。

不注意な生成AI行動への対策

機密データが生成AIツールを通じて漏えいしてしまうのを防ぐために、堅牢なデータ保護対策が重要です。とはいえ、生成AIツールへのアクセスを完全にブロックしてしまうことは良策とはいえません。こうしたツールは生産性を向上させ、イノベーションを促進するため、どのようにユーザーにアクセスを提供するか、その方法を見つけることが重要です。

データセキュリティを危険にさらすことなく、従業員が生成AIツールを使用できるようにするには、情報漏えいに対する「人」を中心としたアプローチを採用する必要があります。こうしたアプローチを使用し、従業員の行動や入力内容に基づいて、従業員による生成AIツールの使用の許可または拒否を行うために介入できるソリューションが求められます。データが操作されている、または複数のチャネルを移動していても対応できる必要があります。

重要なポイント

- **機密コンテンツの特定：**どのコンテンツの保護が重要かをシステムが特定できれば、情報漏えいをより効果的に阻止することができます。光学式文字認識（OCR）、完全なデータ一致（EDM）、インデックス文書一致（IDM）といった、コンテンツの識別や分類の高度な方法が必要です。
- **ユーザーの監視：**組織環境において、誰がどのように生成AIツールを使用しているかを可視化する必要があります。システムは、多くのさまざまなユーザーアクションの検知、ブロック、アラートを提供できる必要があります。ソースコードファイルのアップロードや、企業の知的財産のコピーといったアクションも対象となります。
- **プロアクティブなリスク管理：**カスタム エクスプロレーションを構築し、保存することにより、チームは定期的に、データの持ち出しや、生成AIツールに関連した、その他のリスクある行動がないかを確認することができます。

3：悪意のあるユーザー

悪意のあるユーザーは、機密データを持ち出すのに理想的なポジションを確保しているため危険です。また、退職する従業員は、最もリスクのある内部関係者の種類の一つです。2023年の9か月間において、クラウドテナントでのProofpoint Information Protectionプラットフォームを使用したファイルの異常な持ち出しの87%が、退職する従業員によるものでした。こうしたユーザーは多くの場合、自身が関わったプロジェクトに費やした時間をふまえると、退職時に情報を持ち出してもかまわないと考えています。

悪意のある内部関係者は、腰を据えてチャンスをうかがい、特権アクセスを利用して貴重なデータやセキュリティの弱点を見つけ出すことができるため、これが脅威となります。また、企業は多くの場合、従業員が個人のデバイスからデータにアクセスし、保存することを許可しているため、企業自ら状況を悪化させています。これにより、従業員が機密データを盗むことが、より簡単になります。

絞り込まれた特定のユーザーをより密接に監視する、「人」を中心としたシステムが必要です。そして、最もリスクのあるユーザーに対してはより厳格なセキュリティ制御を適用できる必要があります。

悪意のあるユーザーへの対策

絞り込まれた特定のユーザーをより密接に監視する、「人」を中心としたシステムが必要です。そして、最もリスクのあるユーザーに対してはより厳格なセキュリティ制御を適用できる必要があります。また、従業員の退職時または契約終了時など、リスク要因に基づいて悪意のある行動をプロアクティブに阻止できることが求められます。

重要なポイント

- **可視性：**エンドポイント、メール、クラウド、Webにまたがって包括的なビューを提供し、ユーザーが何を行っているかについてコンテキスト化された知見を提供できるような可視性が求められます。また、機密ファイルの名前を変更したり、承認されていないWebサイトやクラウド同期フォルダにアップロードしたりした場合など、ユーザーによるデータやシステムとのやり取りに関するテレメトリを収集する必要があります。ユーザーが承認されていないアプリケーションをインストールしようとしているか、あるいは実行しているか、といったことも監視する必要があります。また、セキュリティチームは、アラートを発動させたユーザーをリアルタイムで監視できる必要があります。
- **調査：**最も一般的なユースケース（勤怠改ざん、データ持ち出し、セキュリティ制御の回避）をカバーする、アラートの包括的な脅威ライブラリが必要です。これにより、迅速に稼働できます。セキュリティチームに送信されるアラートには、詳細なメタデータやユーザーアクティビティのスクリーンショットが含まれている必要があります。また、コンテキスト化されたイベントのタイムラインにより、調査者はユーザー アクティビティの「誰が、何を、いつ、どこで、どのように」といった情報を知ることができます。
- **最新のアーキテクチャ：**クラウドネイティブ プラットフォームのメリットは、数十万のユーザーへと拡張できることです。プラットフォームが属性ベースのアクセス制御、データのマスキングと匿名化、多地域のデータセンターサポートに対応していれば、データプライバシーと国/地域の要件に適合することができます。また、最新のシステムであれば、組織のセキュリティシステムを拡張でき、以下などのさまざまなツールと簡単に統合できます。
  - SOAR（セキュリティ オーケストレーション、自動化、対応）
  - セキュリティ情報およびイベント管理（SIEM）
  - インシデント レスポンス
  - チケット管理システム

必要な機能

「人」を中心とした先進的なDLPシステムは、どのような保護を提供できるかについてご覧いただきました。では、実際に必要な機能について詳しく見ていきましょう。3つのカテゴリに分類されます。

- 情報漏えいリスクの検知と防止
- 分析と対応
- デプロイと実装

情報漏えいリスクの検知と防止

セキュリティチームがユーザーの行動や機密コンテンツに関する知見を得ることができれば、データリスクに適切な方法で正確に対応することができます。

顧客のニーズ	必要な機能
機密コンテンツの検知	メール、エンドポイント、クラウド、Webにおいて機密データを検知して分析
	事業環境に基づいて機密データを分類できる機能搭載
	大規模言語モデル（LLM）を用いた、AIを活用したデータ分類
	以下などの高度な識別方法 • 光学式文字認識（OCR） • Exact Data Matching（EDM、完全なデータ一致） • Indexed Document Matching（IDM、インデックス文書一致）
	以下などの機密データを検知するための、あらかじめ設定されているポリシー • 個人を特定できる情報（PII） • PCI、SOX、GLBA、SECインサイダー取引規制 • PHI、HIPAA、ICD-9、ICD-11、ナショナル医薬品コード • GDPR、UK-DPA、EU-DEPD、PIPEDA
	Microsoft Information Protection (MIP)の秘密度ラベルを読み取り、適用してビジネスに重要なデータを識別するようポリシーを設定できる機能

顧客のニーズ	必要な機能
ユーザー行動の監視	以下に関する知見を提供することでアナリストが迅速に対応できるようにする、「人」を中心としたアプローチ • ユーザーの意図 • データ アクセス パターン • アプリケーション アクセス パターン
	管理対象/非管理対象のエンドポイントやクラウドにおける、以下などのユーザーによるデータ操作を監視できる機能 • ファイルの名前変更 • ファイル拡張子の変更 • Webでのアップロードとダウンロード • USBメモリへのコピー • クラウド共有同期 • ドキュメント開封 • 異常なファイル アクティビティ
	以下などのWebサイトおよびアプリケーションの使用を監視 • 生成AIサイトへのコンテンツのアップロード、貼り付け、入力 • データバックアップ ツールやハッキングツールのダウンロードやインストール
	Windowsレジストリを操作してコントロールを解除するといった、最もリスクのある内部関係者の行動を監視し、意図を把握してリスクを低減
	プライバシーを確保するため、アラートが発動した場合のみ、スクリーンショットを作成することでリスクのあるユーザーをプロアクティブに監視
	ユーザーを指導し、ブロックして生産性（メール、エンドポイント、クラウド、Web）に影響を与えるよりも、機密データにアクセスするための正当な理由を尋ねる機能
情報漏えいの防止	サイバーセキュリティ リスクを回避する方法、そして機密データを保護する方法の学習により、ユーザー行動の変化を促すセキュリティ意識向上トレーニング
	管理対象エンドポイントから以下などの機密データ持ち出しを防止 • 許可されていないUSBメモリにファイルをコピー • 個人のクラウドフォルダにファイルをアップロード • 機密ドキュメントの印刷 • 機密コンテンツをクリップボードから貼り付け • ネットワーク共有
	クラウド アプリケーションでのファイルの広範な共有を修復し、ファイル共有権限を自動的に削減
	非管理対象デバイスから、IT部門により承認されたクラウド アプリケーション内の機密ファイルへのセキュアなアクセス
	添付ファイルの有無問わずメールの送り間違いを自動的に検知して防止
	送り先は間違っていないが誤ったファイルを添付したメールを自動的に検知して防止
	個人のメールアカウントや他の許可されていないアカウントへの未定義の機密データの共有を防止

分析と対応

セキュリティチームにとって、さまざまなチャネルにおいてインシデントを迅速に解決できることが重要です。また、プライバシーを保護するために、データが過度にさらされないようにする必要があります。

顧客のニーズ	必要な機能
クロスチャネルのインシデント解決	以下をサポートする、メール、エンドポイント、クラウド向けの統合されたクロスチャネルのプラットフォーム • アラートの優先順位付け • 調査 • カスタム エクスプロレーション • 対応
	以下を表示するクロスチャネルの分析 • ユーザー アクティビティの経時変化 • 作成、変更、共有といった、ファイル アクティビティの経時変化
	リスクのあるユーザー行動をリアルタイムで可視化する、プロアクティブなエクスプロレーション
	既存のツールを使用したワークフローの優先順位付けを可能にする、組織のSIEMとの統合
	侵害されたユーザーによる情報漏えいリスクを検知し、以下により自動的に対応できる機能 • セッションの終了 • パスワードのリセット • リスクの修復 • 影響の特定
プライバシー	知る必要がある範囲でのみデータがアナリストに表示される柔軟なアクセス制御
	ユーザーを特定できる情報の匿名化と機密コンテンツのマスキングによりデータを保護し、アナリストのバイアスを排除

導入と実装

組織に最適なDLPソリューションの選定を終えたら、今度はそれを導入する必要があります。円滑な実装プロセスの鍵は、DLPの取り組みをサポートしてくれる適切なパートナーを選ぶことです。

顧客のニーズ	必要な機能
導入	迅速に導入できるクラウドネイティブのソリューション
	1テナントあたり数十万のユーザーに簡単に拡張できる、拡張性に優れたソリューション
	アップデートについては明確に通知され、必要に応じてベンダーのサポートが受けられる、最小限のケアで簡単に維持できるソリューション
	さまざまな国/地域のデータ要件に適合する、一元的なポリシーと管理
	以下のソリューションなど、組織のセキュリティ エコシステムと統合できる柔軟なプラットフォーム • Microsoft • OktaとSailpoint • CrowdStrike • SplunkとService Now • ZscalerとCitrix ShareFile
	以下を実現する、軽い、ユーザーモードのエンドポイント エージェント • 潜在的な内部脅威の可視性を向上させる • ユーザー生産性を強化 • 安定性の問題を排除 • 他のソリューションとのコンフリクトなし
導入	熟練のエキスパート チームによる迅速なデプロイと、ニーズに合わせたシステムの調整をサポートするプロフェッショナル サービス。DLPソリューションの実装には以下のステップが必要。 • 要件の確認 • 設計 • ソリューションのカスタマイズ • テストと調整 • 管理者およびユーザーのトレーニング • ドキュメント化
マネージドDLP	どのような規模の組織でも、マネージドDLPサービスの使用を検討すべきです。マネージドサービスは、プログラムの設計、デプロイ、共同管理を行い、従業員の継続性を確保する熟練のエキスパートによるサポートを提供します。

詳細はこちら

詳細は、proofpoint.com/jpでご確認ください。