opentext™

データリスクの定量化：財務リスクの可視化

opentext™

目次

opentext™

データディスカバリを自動化することも、リスクの定量化や優先度の設定を行ううえで役立ちます。『IBM Cost of Data Breach Report 2023』によると、侵害されたレコードの主なカテゴリとして、顧客の PII (1 レコードあたりの平均コストが 183 米ドル)、従業員の PII (181 米ドル)、企業データ (168 米ドル)、知的財産 (156 米ドル)、PII 以外 (138 米ドル) などが挙げられています[1]。

はじめに

データセキュリティの体制を真の意味で向上させるには、機密データの保存場所、そのデータにアクセスできるユーザー、そのデータの用途を把握することに留意し、その目的を常に意識しておかなければなりません。ビジネスの環境が非常に広大で、しかも無秩序に広がっていることは、多くの人々が直面している課題です。優先度を設定して、どこから手を着けるべきかを判断するまでに相応の時間がかかります。こうした状況の理解を深める際には、データディスカバリ、データサンプリング、リスクモデリングなど、さまざまな戦略を活用すると、データエコシステム全体でデータの価値を評価できるようになります。このような評価とタスクの実行中に、データに関連する財務リスクを視覚化して差し挟むことができるとしたらどうでしょうか。

データディスカバリ

すべてのデータが同じように作成されているわけではなく、すべての機密データが同じリスクにさらされているわけでもありません。データディスカバリによって、データの機密性、冗長性、古さ、些末性が評価されます。機密データを明確にすることで、リスクの高いアプリケーションやデータの保存場所に的を絞った修正と保護が可能になります。データハイジーンプログラムは、価値の低いデータや価値のないデータを保持するリスクを軽減するうえで役立ちます。

データディスカバリを自動化することも、リスクの定量化や優先度の設定を行ううえで役立ちます。『IBM Cost of Data Breach Report 2023』によると、侵害されたレコードの主なカテゴリとして、顧客の PII (1 レコードあたりの平均コストが 183 米ドル)、従業員の PII (181 米ドル)、企業データ (168 米ドル)、知的財産 (156 米ドル)、PII 以外 (138 米ドル) などが挙げられています[1]。このモデルで考えると、22,000 件の顧客レコードが保存された SharePoint サイトの場合、およそ 400 万米ドルの財務リスクがあります。一連のローカルファイルサーバーに 9,000 件の重複した企業レコードが保存されているとすると、その重複データを削除すれば、151 万米ドル相当の財務リスクを軽減することができます。

データサンプリング

あらゆるデータを分析する時間や予算はありません。インテリジェントなサンプリング技術を用いると、機密データがぎっしりと詰まっている領域を特定して、セキュリティチームとコンプライアンスチームが作業を開始すべき箇所を可視化できます。

メタデータのスキャンでは、リスクの特定に至りません。正規表現に基づく分析では、誤検知が多すぎてデータのコンテキストを十分に把握することはできません。インテリジェントなデータサンプリング技術であれば、ごく一部のデータを分析するだけで、潜在的な影響と機密性レベルに基づいて「ホットスポット」としてリスクの優先度を設定できます。この手法を利用することで、組織はリソースの割り当て、効果的な支出、最重要課題への対処を実現できます。

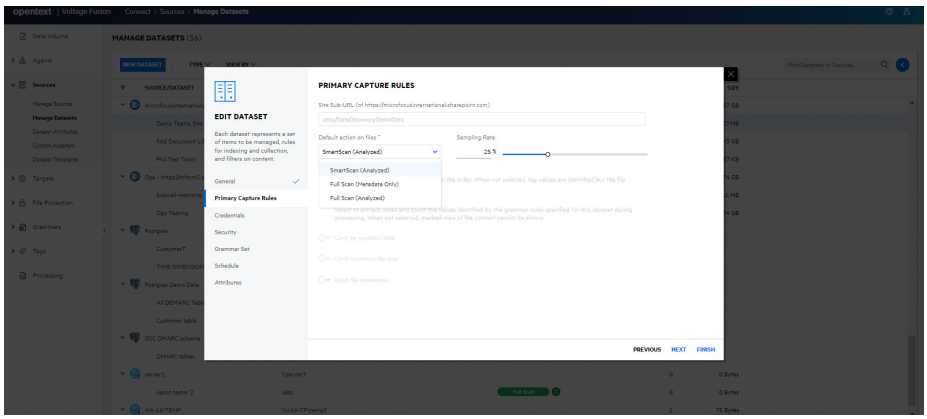

図 1：データサンプリングのスクリーンショット – OpenText Cybersecurity

1 IBM, Cost of a Data Breach Report 2023

リスクモデルの財務的要素について言えば、IBM のレポートでは、2023 年のデータ侵害の平均コストは 445 万米ドルに上ったと言及されています [2]。データ侵害がもたらす課題の幅広さを示しているという点で全般的にはこのモデルは注目に値しますが、財務リスクのモデリングは単なる線形モデルにとどめず、より実用的にリスクを定量化する必要があります。

リスクモデリング

企業データに関するリスクをモデル化する方法はいくつか存在します。リスクスコアリングは、機密データエンティティが 1 つ以上含まれた個々のレコードやファイルのリスクを測定するのに役立ちます。クリーンアップ、リスクアセスメント、データ保護といった各アクティビティに関して、データディスカバリタスクの優先度を設定できます。ただし、リスクスコアは、誤検知や不十分な実装方法によって歪められる可能性があります。

リスクモデルの財務的要素について言えば、IBM のレポートでは、2023 年のデータ侵害の平均コストは 445 万米ドルに上ったと言及されています [2]。データ侵害がもたらす課題の幅広さを示しているという点で全般的にはこのモデルは注目に値しますが、財務リスクのモデリングは単なる線形モデルにとどめず、より実用的にリスクを定量化する必要があります。

財務リスクを定量化するには

データ損失、検知とエスカレーション、侵害後の対応、通知、損失のビジネスコストなど、データ侵害のコストを評価する場合、多くの要素が関わります。

線形スケールに基づくリスク

IBM の『Cost of Data Breach Study 2023』では、データ侵害による損失の平均を線形スケールで分析しています。この場合、データ侵害の平均コストは 445 万米ドルです。2023 年のコストの内訳は次のとおりです [3]。

- 36% は、データ侵害の検知とエスカレーションにかかったコスト (2018 年から 8% 増加)。
- 27% は、データ侵害後の対応にかかったコスト (2018 年から微増)。
- 8% は、データ侵害の通知にかかったコスト (2018 年から 4% 増加)。
- 29% は、ビジネスの損失に関連するコスト (2018 年から 8.5% 減少)。

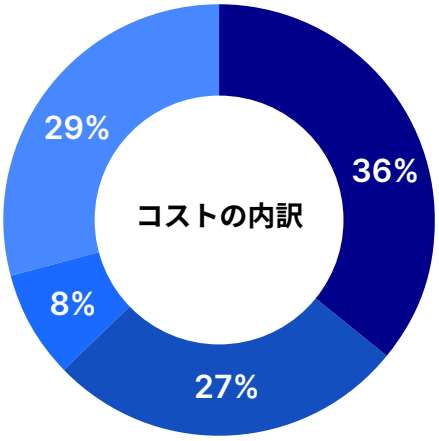

図 2：データ侵害のコストの内訳

2 IBM, Cost of a Data Breach Report 2023

3 同上

失われたレコードの数だけに基づいて潜在的な財務上の損失を表すことは、単純すぎて無意味と考えられます。今日では、線形スケールで損失を表すと、小規模な侵害のコストが過小評価され、結果的に大規模な侵害のコストが過大評価されることが、証拠により示されています。

データ侵害はすべて同じように発生するわけではない：対数スケールに基づくリスク

失われたレコードの数だけに基づいて潜在的な財務上の損失を表すことは、単純すぎて無意味と考えられます。今日では、線形スケールで損失を表すと、小規模な侵害のコストが過小評価され、結果的に大規模な侵害のコストが過大評価されることが、証拠により示されています。Cytenia Institute の『2022 Information Risk Insights Study』では、データ侵害の可視化、傾向分析、財務上の正確な損失の特定を容易にするモデルが使用されています。Cytenia の調査は、データ侵害の規模、頻度、確率に関しても、各業界にわたって評価しています。

Cytenia の調査では、過去の損失に基づいて、データ侵害のコストは 20 万米ドルと推定されています。ただし、侵害の中でも極端な 10% は、2,000 万米ドルを超えています [4]。一方、Fortune 250 企業の財務リスクは 1 億米ドル以上とみなされており [5]、広範囲にわたってデータを比較すると、大きな乖離が見られます。結果として Cyentia は、データ侵害の確率と経済的影響を対数正規化分布で表しています。このモデルの方が、上端の影響を把握できず実際の損失の可能性を適切に表せない線形モデルよりも、視覚的にわかりやすくなっています。

財務リスクの解釈

IBM の調査の良いところは、失われたレコードの価値とデータ侵害に関連するコストセンターの内訳までも評価している点です。2023 年にはさらに一歩進めて、業界や地域をまたぐデータ侵害についても調査を行っているのですが、データ侵害の平均コストは依然として線形スケールで表されています。しかし、最高情報セキュリティ責任者や経営幹部は、処理対象、使用対象、管理対象の各データの財務的な影響を評価するため、さらに詳細な情報を必要とします。

4 Cyentia Institute, IRIS 2022 Information Risk Insights Study

5 同上

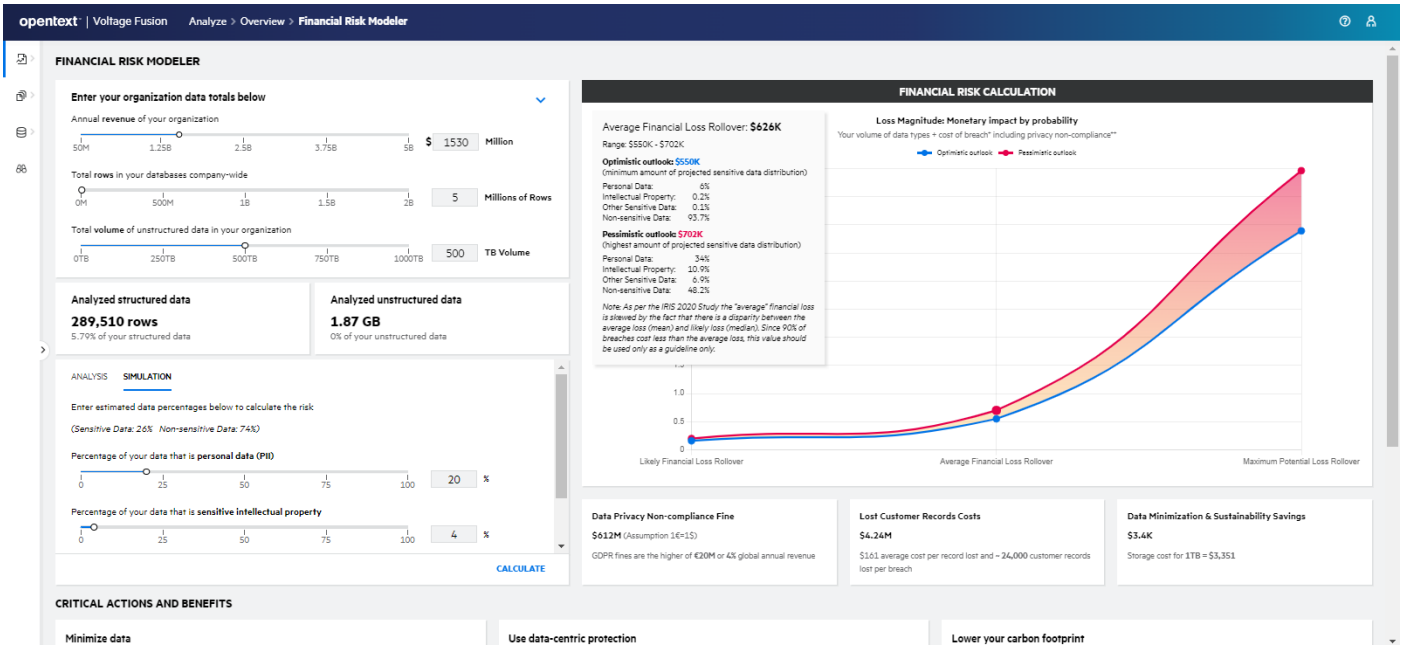

図 3：財務リスクのモデル画面のスクリーンショット – OpenText Cybersecurity

opentext™

2012 年以降、データ侵害のインシデント数は 44.7% 増加しました [6]。一部の業界におけるデータ侵害イベントの数もまた極端に多くなっています。たとえば、Cytenia によると、医療と金融サービスにおけるインシデント数は、鉱業や農業の 76 倍です [7]。

データ侵害の確率と頻度

2012 年以降、データ侵害のインシデント数は 44.7% 増加しました [6]。一部の業界におけるデータ侵害イベントの数もまた極端に多くなっています。たとえば、Cytenia によると、医療と金融サービスにおけるインシデント数は、鉱業や農業の 76 倍です [7]。

さらに、このレポートでは、Fortune 250 (収益 1,000 億米ドル超) 企業の場合、1 年に 1 回を超える件数のデータ侵害イベントが発生する可能性は 29% を超えると推定されています [8]。一方で、小規模企業 (収益 1,000 万～ 1 億米ドル) の場合、1 回のデータ侵害発生の確率は 0.5% 未満です [9]。

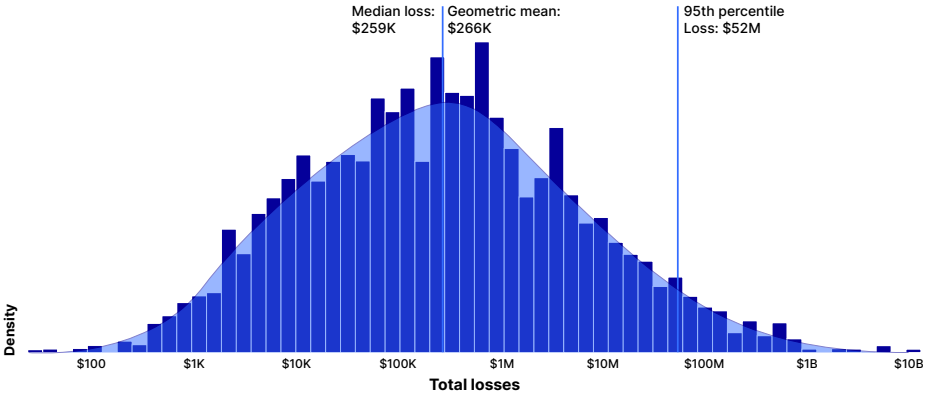

図 4：2012 年から 2021 年にかけて報告されたセキュリティインシデントによる損失の分布 [10]

同じレポートで Cytenia は、業界ごとの損失発生の頻度も示しています。公共部門を基準にして、各業界のデータ侵害イベント数を比較すると、接客業、金融サービス、小売、医療などで、1 年に 1 回を超える件数のデータ侵害イベントが発生する可能性が非常に高くなっています。教育、不動産、製造、建設などの他の業種では、データ侵害イベントの発生確率は 1 年に 1 回未満となっています。

機密データの管理リスクの軽減

データディスカバリを実施するフェーズで、リスクを軽減しリスクのあるデータを修正することは、データ侵害イベントの影響を抑えながら脅威の状況の緩和、運用コストの削減、財務リスクの低減を行ううえで不可欠です。

データのリスクを管理するには

1. データとリスクのあるデータソースを特定して分類する

機密データは、メールシステム、ファイル共有、クラウドリポジトリ、ビジネスアプリケーション、データベースに無秩序に広がっています。今すぐ行動を起こして、機密データがどこにあるかを把握し、リスク許容度に基づいて脅威対策の優先度を決定する必要があります。データの可視性を向上させると、データ侵害イベントへの対処、データ修正の優先度設定、情報に基づいた適切な意思決定を行う能力が向上し、イノベーションと成長を促進できます。

このようなインサイトをディスカバリソリューションとともに活用すると、データ保護の効率化、プライバシーの保護、コンプライアンスの確保を実現するうえで役立ちます。さらに、データディスカバリと分類に関して予防的なアプローチを講じることで、定期的なセキュリティ評価の拡張と効率化のみならず、新たなサイバーセキュリティの脅威にも適用できるようになります。

6 Cyentia Institute, IRIS 2022 Information Risk Insights Study
7 同上
8 同上
9 同上
10 同上

opentext™

データ侵害が発生すると調査が必要になります。ただし、適切なディスカバリと保護の機能があれば、混乱を鎮めて、イベントの関連コストを **64% 以上**削減できます [11]。

2. レガシーデータに対応する

ビジネス上の価値がなくなったデータ、義務付けられた保存期限に達したデータ、または重複したデータが見つかった場合、それに対処する必要があります。責任者とともに情報を確認し、ビジネスにとって価値のないデータを削除し、機密データを長期的なリポジトリにアーカイブします。そうすることで、長期にわたってより効果的にデータを保護、管理できるようになります。こうしたアプローチが、運用コストとランタイムコストの削減につながるとともに、データ侵害イベントの脅威を緩和します。

3. 使用中のデータを保護する

アプリケーションによるデータの処理中またはデータへのアクセス実行中に、そのデータが攻撃に対して脆弱になる可能性があります。ディスカバリ後のプロセスの一貫として、いくつかの有用な手法によってゼロトラストセキュリティをサポートすることができます。フォーマット保持型暗号 (FPE) を使用してデータを暗号化およびトークン化すると、主要なアプリケーションやデータベースのデータを永続的に保護できます。データ処理には、セキュアエンクレーブなど安全で分離された環境を使用することを検討してください。最小権限モデルを適用する厳密なアクセス制御を実装し、分析と AI のパイプラインで使用される機密データは匿名化してリスク許容度と耐障害性を高めます。

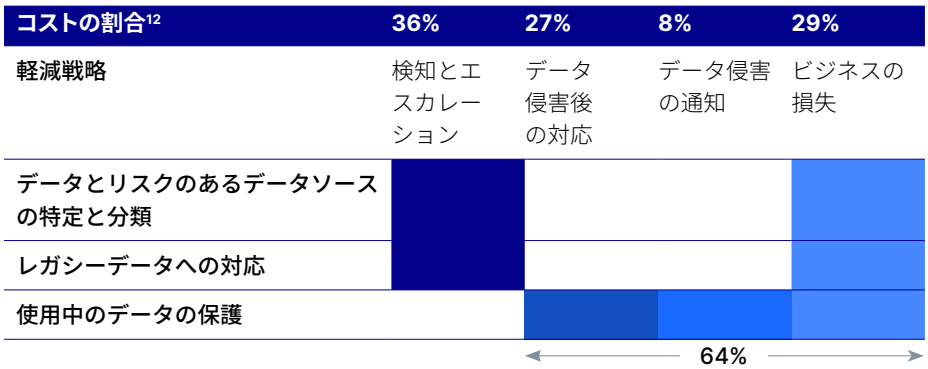

図 5：リスク軽減戦略

リスクおよびセキュリティ管理者にとっての重要なポイント：

- 潜在的な財務上の損失を特定し、真の意味での財務リスクを評価するためには、レコードあたりのコストを均等に評価する以上のことが必要となります。
- ほとんどのデータ侵害は、財務損失モデルの下端に分類されます。ただし、まれに発生する極端なケースによる重大な財務損失の可能性を無視してはなりません。
- 業界や組織の規模に基づいて、業種別にデータ侵害の確率を予測することは困難です。ただし、財務リスクやイベントの発生確率を、セキュリティ体制とリスク許容度を評価するためのガードレールにすることはできます。
- リスクと財務的影響の評価に役立つツールを探し、データセキュリティ対策と侵害からの防御策の優先度の決定に役立ててください。
- データの匿名化、暗号化、トークン化など各種のデータ保護技術を使用すると、イベントへの対応、データ侵害の通知、ビジネスの損失によるダウンストリームへの影響を最小限に抑えて、データ侵害のコストを大幅に削減できます。
- データ侵害が発生すると調査が必要になります。ただし、適切なディスカバリと保護の機能があれば、混乱を鎮めて、イベントの関連コストを **64% 以上**削減できます [11]。

11 Cyentia Institute, IRIS 2022 Information Risk Insights Stud

12 IBM, Cost of a Data Breach Report 2023

opentext™

詳細

https://www.opentext.com/ja-jp/products/voltage-fusion-platform

https://www.microfocus.com/ja-jp/products/voltage-fusion/request-demo

さらに詳しく

財務リスクとデータセキュリティは、共生関係にあります。データ侵害は、重大な金銭的損失、ブランドの評判低下、法的な影響につながる可能性があります。一方、不安定な財務状態は、堅牢なサイバーセキュリティ対策への投資と維持の妨げとなり、サイバー脅威に対する脆弱性につながる可能性があります。したがって、総合的なリスク管理戦略においては、財務リスクとサイバーセキュリティリスクの両方に対処する必要があります。

前述のように、データ侵害への対応とリスクの関連性を追求することは困難です。OpenText Cybersecurity が提供するデータセキュリティソリューションならびに ID およびアクセス管理ソリューションは、業界をリードするデータディスカバリ、保護、アクセスガバナンスの機能を備えており、財務リスクの評価、データ侵害に対する防御の強化、機密データの保護を実施できます。

OpenText について

「The Information Company」を掲げる OpenText は、市場をリードする情報管理ソリューションを通じて、お客様がオンプレミスでもクラウドでもインサイトを獲得できるようにします。OpenText (NASDAQ：OTEX、TSX：OTEX) の詳細については、opentext.com をご確認ください。

SNS 情報：

- OpenText の CEO、Mark Barrenechea のブログ
- X (旧 Twitter) | LinkedIn