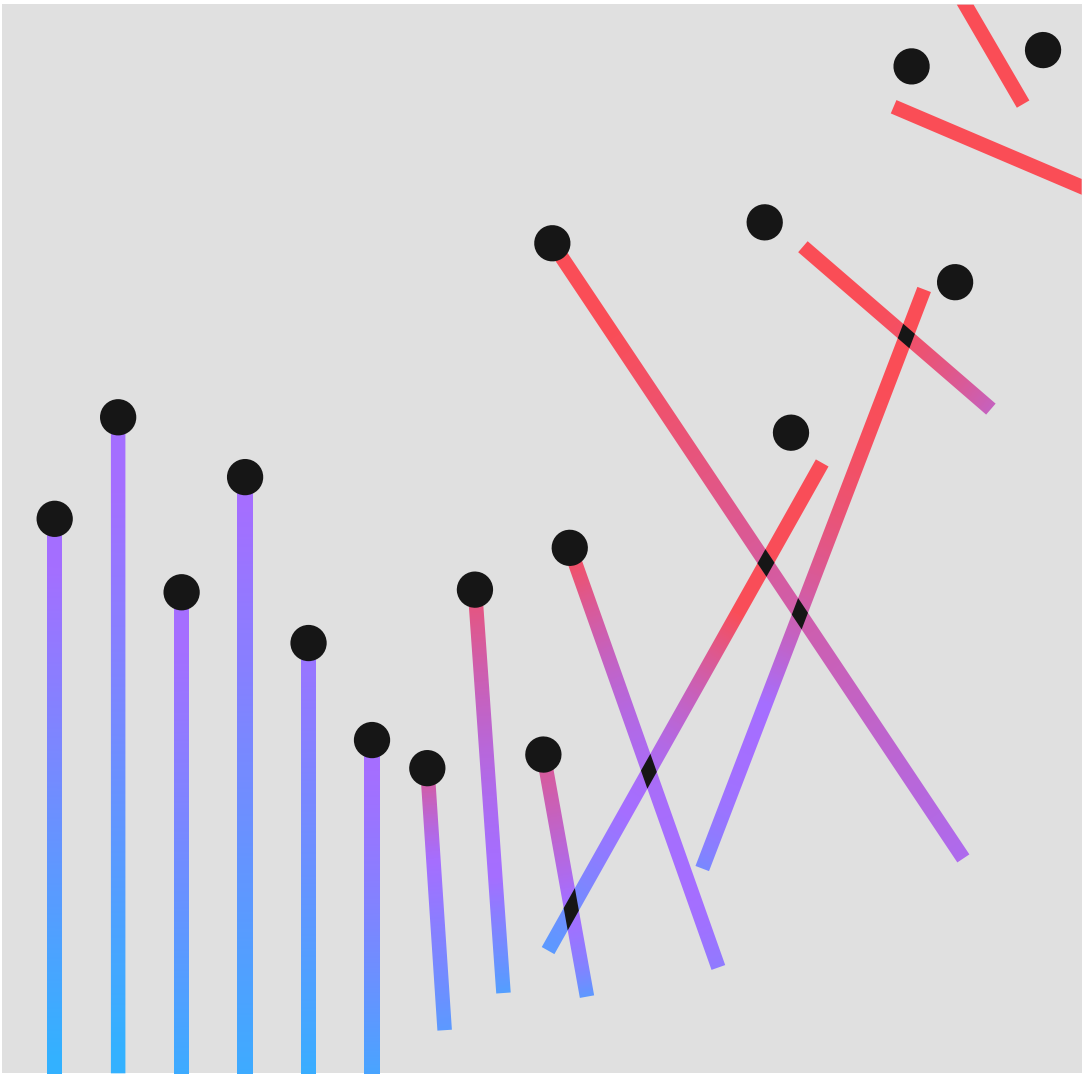
IBM **Security**

2022年
「データ侵害のコストに関する調査」
エグゼクティブ・サマリー



IBM

目次

エグゼクティブ・サマリー

「データ侵害のコストに関する調査」では、IT、リスク管理、セキュリティーのリーダーに、データ侵害によるコストの増加または軽減につながる要因の見方を説明します。

17年目を迎えた本調査は、米調査組織ポネモン・インスティテュート（PonemonInstitute）が実施し、IBMSecurity®がスポンサーとなり、分析し、発行しています。本調査では、2021年3月から2022年3月までに発生したデータ侵害の影響を受けた550社を調査しました。データ侵害は、17の国と地域の17の異なる業界で発生しています。

データ侵害の影響を受けた組織の3,600人超に一人一人インタビューを実施しました。本インタビューでの質問は、データ侵害に対する即時の対応と長期の対応のどちらにも直接関係する異なるアクティビティーについての組織のコストを把握するためのものです。

前年のレポートと同様に、今年のデータにより、何十もの要因が、データ侵害の発生後に増加し続けるコストにどのような影響を与えるのかについて把握できます。さらに、本レポートでは、データ侵害の根本原因、短期的・長期的な影響と、組織の損失削減につながる緩和要因とテクノロジーについて考察します。

調査結果のポイント

こちらの調査結果のポイントは、Ponemon Instituteが収集した調査データに対するIBM Securityの分析に基づいたものです。[1]

435万ドル

データ侵害の平均総コスト

2022年のデータ侵害の平均コストは435万ドルで、過去最高額に達しました。この数値は、データ侵害の平均コストが424万ドルであった前年から2.6%の増加を示しています。2022年の平均コストは、2020年のレポートの386万ドルから12.7%上昇しています。

83%

データ侵害の件数が2件以上の組織の割合

調査対象組織の83%で2件以上のデータ侵害が発生し、これが初めてのデータ侵害だったのは17%のみでした。調査対象組織の60%が、データ侵害が原因でサービスや製品の値上げを実施しました。

482万ドル

重要インフラ組織のデータ侵害の平均コスト

調査した重要インフラ組織のデータ侵害の平均コストは、その他の業界組織の平均コストよりも100万ドル多く、482万ドルでした。重要インフラ組織とは、金融サービス、製造、テクノロジー、エネルギー、運輸、通信、医療、教育、公共事業セクターの業界に属する組織です。17%がビジネス・パートナーのセキュリティーが破られたことによりデータ侵害を経験したのに対して、28%は破壊的な攻撃またはランサムウェア攻撃によるデータ侵害を経験しました。

305万ドル

全面的にセキュリティーにAIと自動化が導入されていることに関連する平均コストの節減額

セキュリティーにAIと自動化を全面的に導入している組織のデータ侵害のコストは、セキュリティーにAIと自動化をまったく導入していない組織よりも、305万ドル少ない金額になっています。導入済み組織（平均コスト315万ドル）と未導入の組織（平均コスト620万ドル）間の平均コストの差は65.2%で、本調査で最大のコストの節減を示しています。セキュリティーにAIと自動化が全面的に導入されている組織において、データ侵害を特定してから被害拡大を阻止するまでの期間であるデータ侵害ライフサイクルは249日で、セキュリティーにAIと自動化が導入されていない組織の323日よりも74日短くなっています。セキュリティーにAIと自動化の利用率は、2020年の59%から2022年の70%まで、2年間で5分の1近く増加しました。

1. 本レポートでは、ドル（USD）でコストを算出しています。

454万ドル

身代金そのもののコストを除いたランサムウェア攻撃の平均コスト

本調査ではデータ侵害の11%がランサムウェア攻撃によるものだったことが明らかになり、2021年の7.8%よりも増加しました。増加率は41%です。2022年のランサムウェア攻撃の平均コストは454万ドルで、2021年の462万ドルからわずかに減少しました。このコストは、データ侵害の全般的な平均総コストの435万ドルよりも若干高くなっています。

19%

盗難または侵害された認証情報が原因のデータ侵害の発生率

盗難または侵害された認証情報の使用は、データ侵害の最も一般的な原因であったことに変わりありません。2022年の調査によると、認証情報の盗難や侵害は主要な攻撃経路で、19%のデータ侵害の原因になっています。2021年の調査でも、これは最大の攻撃経路で、20%のデータ侵害の原因となっていました。認証情報の盗難や侵害が原因のデータ侵害の平均コストは、450万ドルでした。このようなデータ侵害のライフサイクルは最も長く、データ侵害の特定に243日、侵害の拡大防止のためにさらに84日費やすことになります。次に一般的なデータ侵害の原因はフィッシングの16%です。また、データ侵害コストの平均は491万ドルで、最も高額です。

59%

ゼロトラストを導入していない組織の割合

本調査で、ゼロトラスト・セキュリティー・アーキテクチャーを導入していると回答した組織は41%のみでした。ゼロトラストを導入していない、その他の59%の組織では、ゼロトラストを導入している組織と比べて、データ侵害に対して費やすコストが平均で100万ドル多くなっています。重要インフラ組織では、ゼロトラストの非導入率がさらに高く、79%がゼロトラストを導入していません。これらの組織のデータ侵害コストの平均は540万ドルで、世界平均よりもデータ侵害コストが100万ドル強も多くなっています。

100万ドル

リモートワークがデータ侵害を引き起こす要因だった場合とそうではない場合の平均コストの差

リモートワークがデータ侵害を引き起こす要因だった場合のコストは499万ドルで、リモートワークがその要因ではなかった場合の402万ドルよりも平均で100万ドル近く多くなっています。リモートワーク関連のデータ侵害コストの平均は、世界平均と比べて60万ドル多くなっています。

45%

クラウドで発生したデータ侵害の割合

本調査において、データ侵害の45%はクラウド内で発生したものでした。しかし、ハイブリッドクラウド環境で起こったデータ侵害の平均コストは、380万ドルでした。比較対象として、プライベートクラウド内のデータ侵害では424万ドル、パブリッククラウド内のデータ侵害では502万ドルのコストが発生しました。ハイブリッドクラウドとパブリッククラウドのデータ侵害のコストの差は27.6%です。ハイブリッドクラウド・モデルを活用している組織のデータ侵害ライフサイクルは、パブリッククラウドまたはプライベートクラウド・モデルしか採用していない組織よりも短くなっています。

266万ドル

インシデント対応（IR）チームと定期的にテストされているIR計画に関する平均コストの節減

本調査で、4分の3近くの組織がIR計画を備えていると回答した一方、定期的にその計画をテストしていたのは、その中の63%でした。IRチームを備え、IR計画を定期的にテストしていたことが、大きなコストの節減につながっていました。IRチームがありIR計画をテストしていた組織は、IRチームがなく、IR計画のテストをしていない組織よりも、データ侵害のコストが266万ドル抑えられています。この差（326万ドル対592万米ドル）は、コストの58%節減を示しています。

29日

XDR（extended detection and response）テクノロジーを備えた組織による応答時間の節減

44%の組織がXDRテクノロジーを実装していました。これらのXDRテクノロジーを備えた組織は、応答時間において大きな優位性を得ています。これらのXDRテクノロジーを備えた組織のデータ侵害ライフサイクルは、XDRを実装していない組織と比べて、平均で約1カ月短縮されました。具体的には、XDRを導入した組織がデータ侵害の特定と拡大阻止に275日費やしたのに対して、XDRを導入しなかった組織は304日費やしました。この数値は、応答時間の10%の差を示しています。

12年

医療業界が平均データ侵害コストの最高額を記録し続けている年数

医療業界は、データ侵害コストの新たな最高額を記録しました。医療業界の平均データ侵害コストは100万ドル近く増加し、1010万ドルに達しました。医療は12年連続で最もデータ侵害コストが高額な業界であり、そのコストは、2020年のレポートから41.6%増加しています。金融組織の平均コストは597万ドルで医療の次に高額で、これに製薬の501万ドル、テクノロジーの497万ドル、エネルギーの472万ドルが続きます。

944万ドル

世界で最も高額な米国の平均データ侵害コスト

データ侵害の平均コストが高額な上位5つの国と地域は、米国（944万ドル）、中東（746万ドル）、カナダ（564万ドル）、英国（505万ドル）、ドイツ（485万ドル）でした。米国はこれで12年連続1位です。一方、過去1年でコストの上昇率が最も高かったのはブラジルで、108万ドルから138万ドルまで27.8%増加しました。

データ侵害の財務的影響を最小化するための推奨事項

IBM Securityは、本セクションでデータ侵害の財政コストとブランドへの影響を削減するために組織が取り組むことができる手順の概要を説明します。これらの推奨事項には、調査対象組織による実績のあるセキュリティー・アプローチが含まれています。

重要データへの無許可アクセスを防止するためにゼロトラスト・セキュリティー・モデルを採用しましょう。
本調査結果によると、ゼロトラスト・セキュリティー・アプローチを実装している組織は41%のみである一方、これらの組織はこのアプローチの成熟したデプロイメントにより、150万ドルの潜在的なデータ侵害コストの節減を実現しました。リモートワークとハイブリッド・マルチクラウド環境を取り入れている会社は、ゼロトラスト戦略により、アクセシビリティーを制限し、コンテキストを要求することで、データとリソースを保護できます。

異なるシステム間でのデータの共有と集中型のデータ・セキュリティー運用が可能なセキュリティー・ツールにより、セキュリティー・チームが複雑なハイブリット・マルチクラウド環境全体でインシデントを検出できるようにします。ゼロトラスト戦略を推進させることが可能なオープン・セキュリティー・プラットフォームを活用して、さらに深い洞察が得られ、リスクを緩和し、応答を加速させられます。同時に、データを移動させることなく、既存の投資を使用しながら、チームの効率とコラボレーションを向上させられます。

クラウド環境で重要データを保護するために、ポリシーと暗号化を使用しましょう。
クラウド環境でホストされるデータの量と価値の増大に伴い、組織はクラウド・ホスティング・データベースを保護するための対策を講じる必要があります。成熟したクラウド・セキュリティー・プラクティスは、クラウド・セキュリティー・プラクティスがない場合と比較して、データ侵害コストの72万ドル節減に寄与していました。データ分類スキーマと保存プログラムを使用して、データ侵害に対して脆弱な機密情報の可視性を高め、量を削減します。データ暗号化と完全な準同型暗号を使用して、機密情報を保護します。監査向けの内部フレームワークを使用し、組織全体でリスクを評価し、ガバナンス要件でコンプライアンスを追跡することで、データ侵害の検出の能力を向上させ、拡大抑止の取り組みを強化するのです。

SOAR（セキュリティー・オーケストレーション、自動化、対応）とXDRに投資し、検出時間と応答時間を改善しましょう。
セキュリティーにAIと自動化とともに、XDR機能で平均データ侵害コストとデータ侵害ライフサイクルを大幅に削減できます。本調査によると、XDRテクノロジーを備えた組織は、XDRを実装していなかった組織と比べて、データ侵害ライフサイクルを平均で29日短縮するとともに、コストを40万ドル節減しました。SOAR、セキュリティー情報およびイベント管理（SIEM）ソフトウェア、マネージド検出および応答サービスとXDRにより、組織は、既存のセキュリティー・ツールを使用した自動化、プロセスの標準化および統合でインシデント対応を加速できます。

エンドポイントとリモート従業員の保護と監視を支援するツールを使用しましょう。
本調査では、リモートワークがデータ侵害を引き起こす要因だった場合のコストは、リモートワークがその要因ではなかった場合よりも、平均で100万ドル近く多いことが明らかになりました。統合エンドポイント管理（UEM）、エンドポイント検知およびレスポンス（EDR）、ID管理とアクセス管理（IAM）の製品とサービスにより、セキュリティー・チームは不審なアクティビティーへのさらに深い洞察を得られます。この監視には、個人所有デバイスの業務使用（BYOD）と組織のラップトップ、デスクトップ、タブレット、モバイル・デバイス、IoTが関わり、組織にとって物理的なアクセスのないエンドポイントも含まれます。UEM、EDR、IAMにより、調査および応答時間を速め、リモートワークが要因のデータ侵害による被害を分離し、拡大を防止します。

インシデント対応の方針を作成し、テストして、サイバー・レジリエンスを高めましょう。
データ侵害のコスト削減に対して極めて有効な2つの方法は、インシデント対応（IR）チームを組むこととIR計画を徹底的にテストすることです。IRチームを備え、定期的にIR計画をテストしている組織におけるデータ侵害では、IRチームがないまたはIR計画のテストをしていない組織のデータ侵害と比べて、266万ドルのコスト節減が明らかになりました。組織は、詳細なサイバーインシデントの方針を確立させることで、データ侵害による悪影響の拡大防止に向けて迅速に対応できます。机上訓練または、サイバー防御トレーニングセンターのような模擬環境でのデータ侵害シナリオの実行を通じて、定期的に計画をテストします。

レッドチーム演習としても知られる攻撃的シミュレーション訓練では、見落としているかもしれない攻撃の経路と技術を発見し、検出と応答の能力のギャップを特定することにより、IRチームの有効性を強化できます。攻撃対象領域管理ソリューションで、本格的な攻撃体験のシミュレーションを通じて、これまでは不明だった機密漏れポイントを突き止めることにより、組織はセキュリティー動態を向上させられます。

セキュリティー・プラクティスの推奨事項は、教育を目的としており、結果を保証するものではありません。

Ponemon InstituteとIBM Securityについて

Ponemon Institute

Ponemon Instituteは、独自の調査と教育を通して、企業と政府機関における信頼性に優れた情報管理と個人情報管理の実践を推進しています。当社のミッションは、ユーザーと企業に関する機密情報の管理とセキュリティーに影響を及ぼす重要課題について、豊富な経験を活かした高品質な調査を実施することです。

Ponemon Instituteは、データの機密保持、個人情報保護、倫理に関する厳格な基準を順守して調査活動を遂行しています。当社は、企業調査において、個人または企業が特定できるようないかなる情報も収集しません。また、調査対象者に無関係な質問や不適切な質問をしないための厳格な品質基準を順守しています。

IBM Security

IBM Securityは、企業のセキュリティー関連の製品とサービスの極めて先進的で高度なポートフォリオを提供しています。世界的に有名なIBM Security X-Force®の研究により裏付けされるこのポートフォリオは、不確実性の増す世界においても企業が成功を収められるように、ビジネスの構造にセキュリティーを組み込むためのソリューションを提供します。

IBMは、セキュリティーの調査、開発、提供を目的とした、最大級かつ最高レベルの組織を運営しています。IBMは、1万件超のセキュリティー特許を有し、130カ国を超える国で、毎月4兆7000億件以上のイベントを監視しています。詳細については、ibm.com/jp-ja/securityをご確認ください。IBM Security Communityでの会話に参加しましょう。

本調査レポートについてのご質問やご意見（本レポートの引用や再利用の許諾申請を含む）については、手紙、電話、または電子メールでお寄せください。

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City
Michigan 49686 USA

1.800.887.3118
research@ponemon.org

次の一歩を踏み出す

ゼロトラスト・セキュリティー・ソリューション
あらゆるユーザー、デバイス、接続に関するセキュリティーに対応します。
詳しくはこちら

IDおよびアクセス管理
あらゆるアプリに、あらゆるユーザー、API、デバイスを安全に接続します。
詳しくはこちら

データ・セキュリティー
重要なエンタープライズ・データを検知、分類、保護します。
詳しくはこちら

セキュリティー・オーケストレーション、自動化、および対応
オーケストレーションと自動化によりインシデント対応を加速します。
詳しくはこちら

セキュリティー情報およびイベント管理
脅威の検出、調査、対応についての可視性を獲得します。
詳しくはこちら

クラウド・セキュリティー
ハイブリット・マルチクラウドへの移行にセキュリティーを統合します。
詳しくはこちら

エンドポイント・セキュリティー
高度な攻撃からデバイス、ユーザー、組織を保護します。
詳しくはこちら

サイバーセキュリティー・サービス
コンサルティング、クラウドおよびマネージド・セキュリティー・サービスでリスクを削減します。
詳しくはこちら

インシデント対応と脅威インテリジェンス
セキュリティーの脅威に対し、先を見越して管理、対応します。
詳しくはこちら

IBM Security X-Forceの専門家との個別コンサルティングをご予約ください。
今すぐスケジュール

日本アイ・ビー・エム株式組織
〒103-8510
東京都中央区日本橋箱崎町19-21

米国で制作
2022年7月

本書は最初の発行日時点における最新情報を記載しており、IBMにより予告なしに変更される場合があります。IBMが事業を展開しているすべての国で、すべての製品が利用できるわけではありません。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。本書の情報は“現状のまま”で提供されるものとし、明示または黙示を問わず、商品性、特定目的への適合性、および非侵害の保証または条件を含むいかなる保証もしないものとします。IBM製品は、IBM所定の契約書の条項に基づき保証されます。

良好なセキュリティー・プラクティスに関するステートメント：ITシステム・セキュリティでは、組織内および組織外からの不適切なアクセスを予防、検出、応答することにより、システムと情報を保護します。不適切なアクセスにより、情報の改変、破壊、誤用、濫用や、システムの損傷または他のシステムへの攻撃に使用することを含むシステムの濫用につながるおそれがあります。どのITシステムまたは製品も、完全に安全ということはありません。また、どの製品、サービス、セキュリティ対策も、不適切な使用やアクセスを完全に予防することはできません。IBMのシステム、製品、サービスは、合法的で包括的なセキュリティ・アプローチの一部として設計されているため、必然的に運用手順が追加されることになります。また、最も効果的に使用するために他のシステム、製品、サービスが必要になる場合があります。IBMは、いかなる当事者の不正行為または違法行為によるものであっても、いずれのシステム、製品、サービス、またはお客様の組織に対しても、影響が及ばないことを保証するものではありません。

お客様は自己の責任で関連法規を順守しなければならないものとします。IBMは、法律上の助言を提供することはなく、また、IBMのサービスまたは製品が、お客様がなんらかの法律または規則を順守していることの裏付けとなることを表明または保証するものでもありません。IBMの将来の方向性および指針に関する声明は、予告なく変更または撤回される場合があります。これらは目標および目的を提示するものにすぎません。