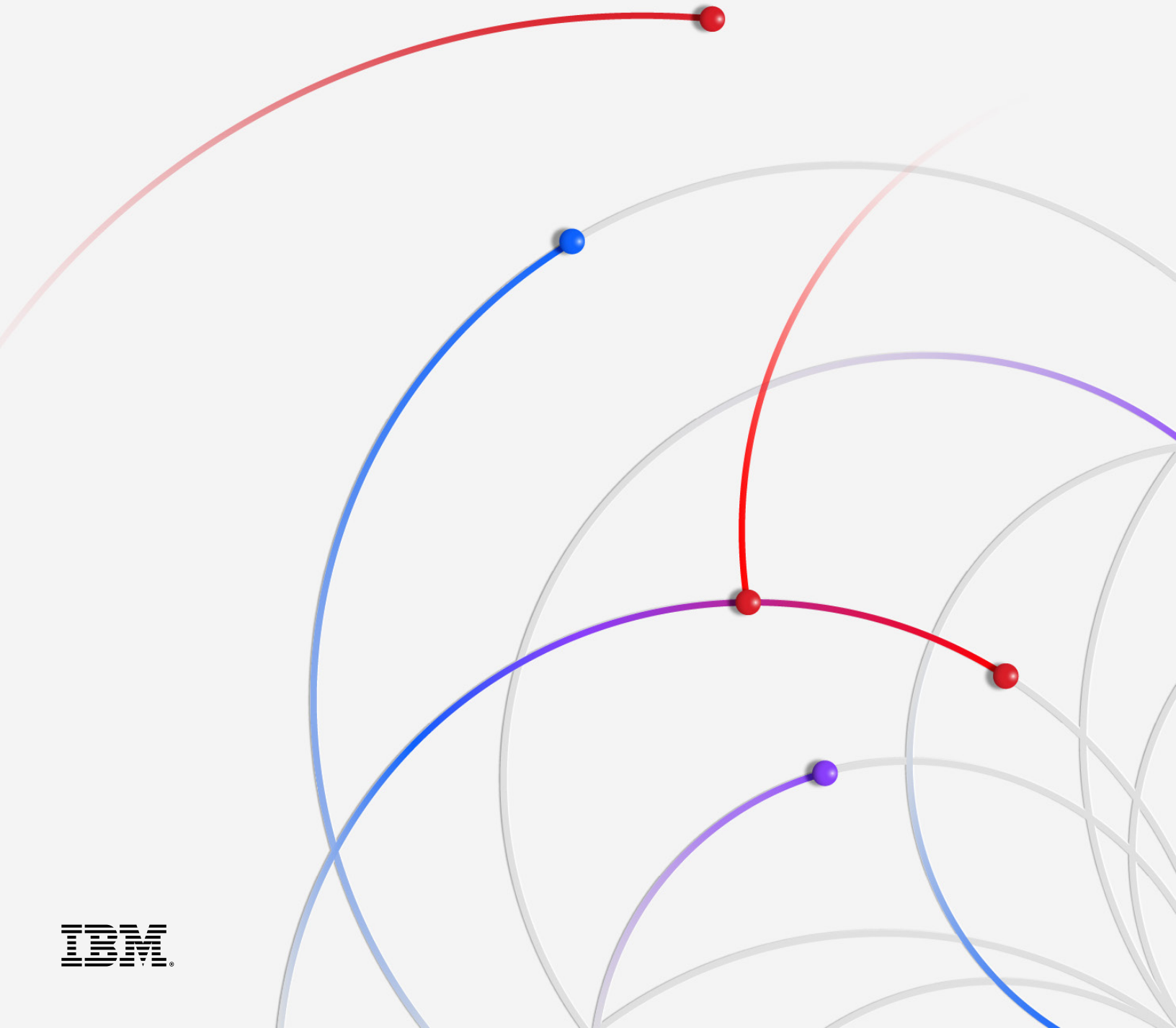
データ侵害のコストに関する調査

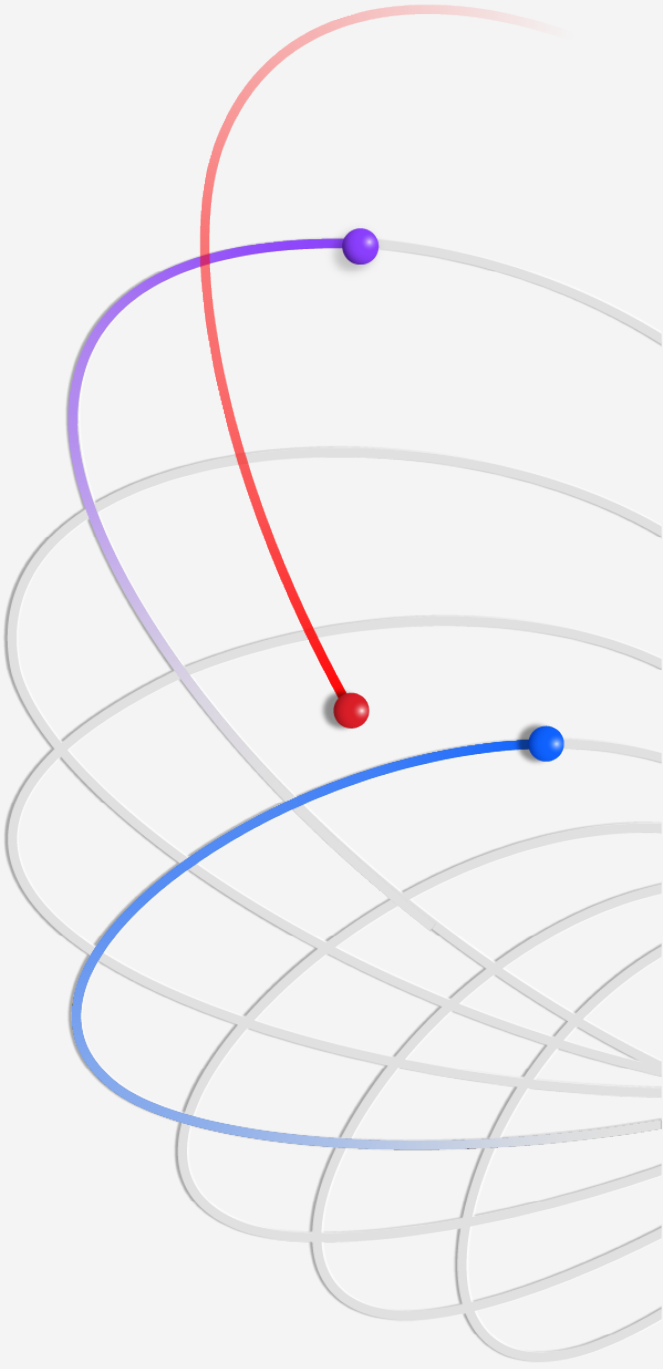
2024



IBM

目次

エグゼクティブ・サマリー



IBMが毎年発表するデータ侵害のコストに関する調査は、IT部門、リスク管理部門、セキュリティー部門の各リーダーに、戦略的意思決定の指針となる定量化可能な証拠をタイムリーに提供します。また、リスク・プロファイルやセキュリティーへの投資をより適切に管理するのに役立ちます。シリーズ19回目となる今年のレポートでは、シャドー・データ（管理されていないデータ・ソースに存在するデータ）の増加や、データ侵害がもたらすビジネスの中断の範囲とコストなど、技術的変動による変化が反映されています。

Ponemon Instituteが独自に実施し、IBMが資金提供、分析、発行したレポートの調査は、2023年3月から2024年2月の間にデータ侵害の影響を受けた604社を対象に行われたものです。研究者たちは、16の国と地域の17の業種にわたる組織と、2,100件～11万3,000件に及ぶ侵害の記録を調査しました。Ponemon Instituteの研究者は、現場での洞察を得るために、各組織でデータ侵害インシデントを直接体験して知識を得た3,556人のセキュリティーおよび経営幹部のビジネス・リーダーにインタビューを実施しました。

その成果として、ビジネス・リーダーやセキュリティー・リーダーがセキュリティー防御を強化し、イノベーションを推進するために利用できるベンチマーク・レポートが完成しました。その内容は特に、セキュリティーにおけるAIの導入や、生成AIの取り組みにおけるセキュリティーに関連しています。

今年のレポートでは、2つの大きな進展を取り上げています。まず、データ侵害の世界平均コストは前年比10%増の488万米ドルに達し、パンデミック以降で最大の増加となりました。このコスト急増の原因となったのは、ビジネスの中断と、侵害後のカスタマー・サポートの修復です。これらのコストにどのように対処しているかという質問に対しては、半数以上の組織が顧客に転嫁していると回答しました。既にインフレによる価格圧力に直面している競争市場では、こうしたコストを顧客に負担させることは問題となる可能性があります。

第二に、防御面では、セキュリティー向けのAIと自動化の適用が功を奏し、侵害コストを平均220万米ドル削減した例もあることが判明しました。AIと自動化のソリューションにより、侵害とその結果生じる損害を特定し、封じ込めるために必要な期間が短縮されています。言い換えれば、AIと自動化を導入していない防御側では、これらのソリューションを導入している防御側と比べて、侵害の検知と封じ込めに時間がかかり、コストが上昇することが予想されます。

業界全体で見られるように、サイバーセキュリティー・チームは常に人員不足です。今年の調査では、侵害を受けた組織の半数以上が深刻なセキュリティー・スタッフ不足に直面しており、スキル格差は前年から2桁増加していることが判明しました。訓練を受けたセキュリティー・スタッフの不足は、脅威が拡大するにつれて深刻化しています。組織のほぼすべての機能で生成AIを導入しようとする競争が続くと、前例のないリスクが発生し、サイバーセキュリティー・チームへのプレッシャーがさらに大きくなることが予想されます。

このレポートは、データ侵害による金銭的および風評的な損害の可能性を軽減するのに役立つ、調査から得られた洞察と推奨事項を提供します。

2024年版レポートの最新情報

毎年、データ侵害のコストに関する調査は、新しいテクノロジーと戦略、および直近のインシデントを反映して進化し続けています。今年のレポートでは、初めて、以下の項目が調査されました。

- 組織が長期的な業務の中断を経験したかどうか（例えば、販売注文の処理不能、生産設備の完全な停止、カスタマー・サービスの非効率性など）
- 管理されていないデータ・ソースに保存されたデータ（シャドー・データとして知られる）が侵害に含まれているかどうか
- セキュリティー運用の4つの領域（予防、検知、調査、対応）のそれぞれにおいて、組織がAIと自動化をどの程度活用しているか
- 恐喝攻撃の性質（例えば、恐喝とランサムウェア攻撃、あるいは恐喝とデータ窃盗のみなど）
- データ、システム、サービスを侵害前の状態に復元するのに要する時間
- 侵害の報告が義務付けられていた場合、報告までに要した期間
- ランサムウェア攻撃後に法執行機関を関与させた組織が身代金を支払ったかどうか

主な調査結果

ここに記載する主な調査結果は、米調査会社Ponemon Institute が収集した調査データをIBMが分析した内容に基づいています。

488万米ドル

データ侵害による平均総コスト
データ侵害の平均コストは、2023年の445万米ドルから488万米ドルに跳ね上がり、10%の急増となり、パンデミック以降で最も高い増加率となりました。この増加の要因として、業務のダウンタイムや顧客の喪失を含むビジネス損失に伴うコストの増加、およびカスタマー・サービスのヘルプデスクへの人員配置や高額な罰金の支払いなど、侵害後の対応コストの増加が挙げられます。これらのコストは合計で280万米ドルとなり、過去6年間におけるビジネス損失と侵害後の活動の合計額としては最高額となりました。

220万米ドル

予防におけるAIの広範な利用によるコスト削減
調査対象の3社のうち2社が、セキュリティー・オペレーション・センター全体でセキュリティー向けのAIと自動化を導入していると回答しました。これは前年比で10%の増加です。攻撃対象領域管理（ASM）、レッドチーミング、ポスチャー管理といった予防ワークフローにAIを幅広く導入した組織は、予防ワークフローにAIを使用していない組織と比べて、侵害コストが平均220万米ドル減少しました。この調査結果は、2024年のレポートで明らかになった中で、最大のコスト削減でした。

26.2%

サイバー・スキル不足の深刻化
セキュリティー侵害を受けた組織の半数以上が、深刻なセキュリティー人材不足に直面しています。この問題は前年比で26.2%増加し、侵害コストが平均176万米ドル増加したことに相当します。5社に1社が何らかの形の生成AIセキュリティー・ツールを使用していると回答しています。これらのツールは、生産性と効率を高めることでギャップの解消に役立つと期待されていますが、このスキル・ギャップは依然として課題となっています。

3分の1

シャドー・データが関与する侵害の割合
侵害の35%にシャドー・データが関与しており、データの急増が追跡と保護を困難にしていることを示しています。シャドー・データの盗難は、侵害のコストが16%増加することと相関していました。研究チームは、環境間でデータを保存することが一般的なストレージ戦略であることを明らかにし、侵害の40%を占めていることを突き止めました。また、これらの侵害の特定と封じ込めには長い日数を要しました。一方、パブリッククラウド（25%）、オンプレミス（20%）、プライベートクラウド（15%）のいずれであっても、単一の環境に保管されたデータが侵害されるケースは少なくなっていました。

499万米ドル

悪意のあるインサイダー攻撃の平均コスト
他のベクトルと比較して、悪意のあるインサイダー攻撃によるコストは最も高く、平均499万米ドルでした。その他の高額な攻撃ベクトルとしては、ビジネス・メールの漏洩、フィッシング、ソーシャル・エンジニアリング、認証情報の盗難や漏洩がありました。生成AIは、こうしたフィッシング攻撃の一部に悪用されている可能性があります。例えば、生成AIを使用すると、英語を話さない人でも、文法的に正しく、もっともらしいフィッシング・メッセージを作成することがこれまで以上に簡単になります。

46%

顧客の個人データに関連する侵害の割合
侵害の半数近くは、顧客の個人情報（PII）が関与するもので、納税者番号（ID）、電子メール、電話番号、自宅住所などが含まれます。知的財産（IP）記録は僅差で2位でした（侵害の43%）。IP記録のコストは昨年から大幅に跳ね上がり、昨年の調査レポートでは1記録あたり156米ドルでしたが、今年の調査では173米ドルという結果でした。

100万米ドル

ランサムウェア攻撃に法執行機関が関与した場合のコスト削減
法執行機関を関与させたランサムウェアの被害者は、身代金支払いのコストを除き、最終的に侵害コストを平均100万米ドル近く下げることに成功しました。また、法執行機関を関与させることで、侵害の特定と封じ込めに必要な時間が297日から281日に短縮されました。

292日

盗まれた認証情報を含む侵害を特定し、封じ込めるまでの日数
盗まれた、または漏洩した認証情報に関連する侵害は、あらゆる攻撃ベクトルの中で、特定と封じ込めに最も長い日数（292日）を要しました。従業員や従業員のアクセスを利用した同様の攻撃も、解決に長い時間を要しました。例えば、フィッシング攻撃は平均261日、ソーシャル・エンジニアリング攻撃は平均257日でした。

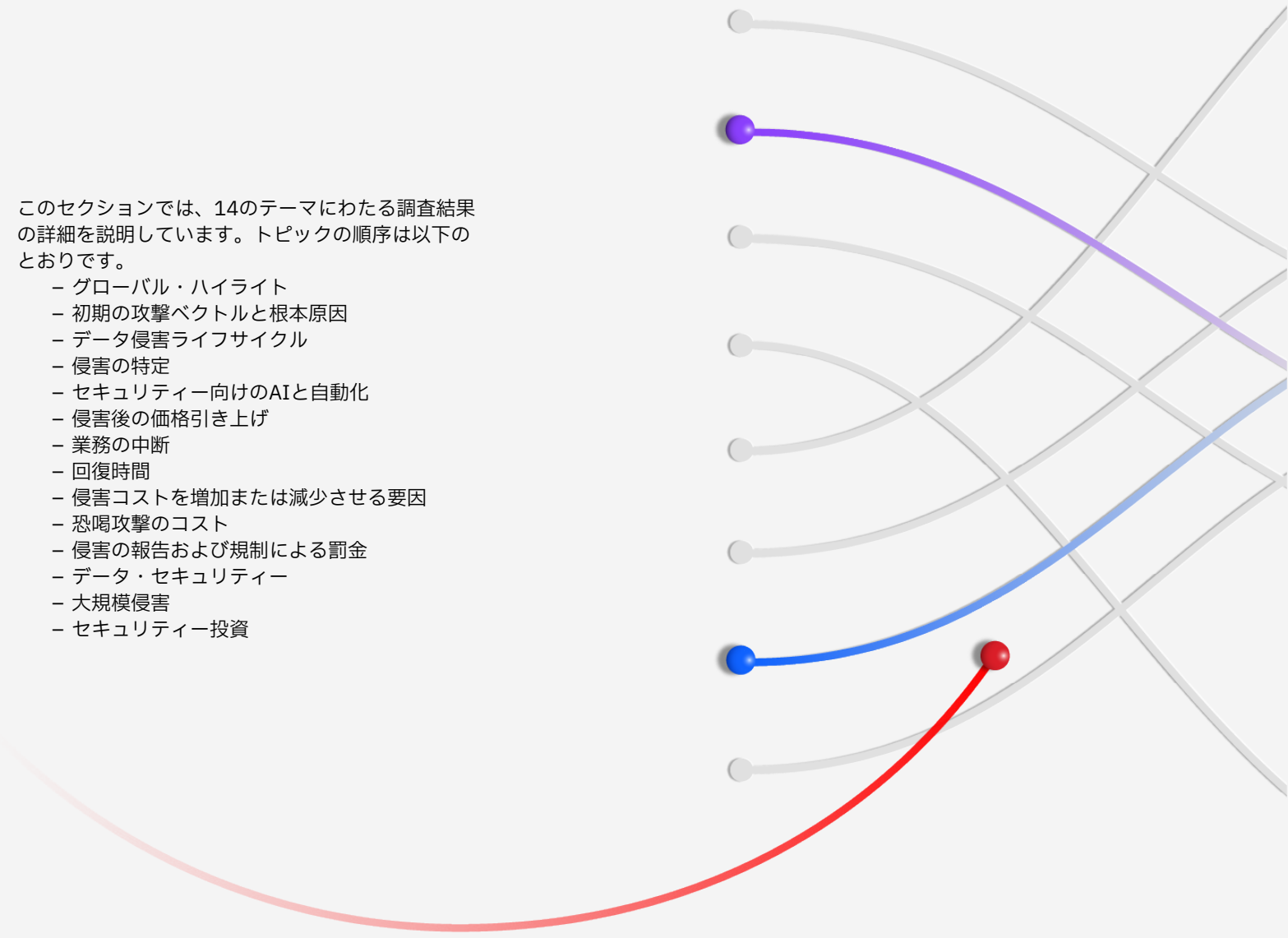
83万米ドル

全業界で最大の平均コスト上昇
工業セクターは、全産業の中でコストが最も増加し、昨年と比べて侵害1件当たり平均83万米ドル上昇しました。このようなコストの急上昇は、産業組織がより迅速に対応できるよう備える必要があることを反映している可能性があります。このセクターの組織は、業務のダウンタイムに非常に敏感だからです。それでも、産業組織におけるデータ侵害の特定と封じ込めに要した日数は、特定に199日、封じ込めに73日で、業界の中央値を上回りました。

調査結果の詳細

このセクションでは、14のテーマにわたる調査結果の詳細を説明しています。トピックの順序は以下のとおりです。

- グローバル・ハイライト
- 初期の攻撃ベクトルと根本原因
- データ侵害ライフサイクル
- 侵害の特定
- セキュリティー向けのAIと自動化
- 侵害後の価格引き上げ
- 業務の中断
- 回復時間
- 侵害コストを増加または減少させる要因
- 恐喝攻撃のコスト
- 侵害の報告および規制による罰金
- データ・セキュリティー
- 大規模侵害
- セキュリティー投資



488万米ドル

データ侵害の世界平均コストの急増

グローバル・ハイライト

世界的に見ると、セキュリティー・チームは、深刻なスキル不足にもかかわらず、侵害の検知と封じ込めにおいてはるかに優れた仕事をしています。侵害を受けた組織の半数以上がセキュリティー要員の不足に直面しており、セキュリティー・リーダーはスキル・ギャップを埋めるためにAIや自動化・ソリューションを活用しています。その努力にもかかわらず、侵害コストは上昇しており、そのほとんどを業務の中断と侵害後の対応に関連する費用が占めています。続くセクションでは、業種や国・地域を問わず、これらの問題やその他の問題に目を向け、セキュリティー・リーダーがリスクを把握しているため、読者がそこから学びを得られるようにしています。

データ侵害の世界平均コストの急増
データ侵害の世界平均コストは前年比10%増の488万米ドルに達し、パンデミック以降で最大の増加となりました。業務の中断と侵害後の対応活動が、この年間コスト増加の大部分を占めています。図1を参照してください。

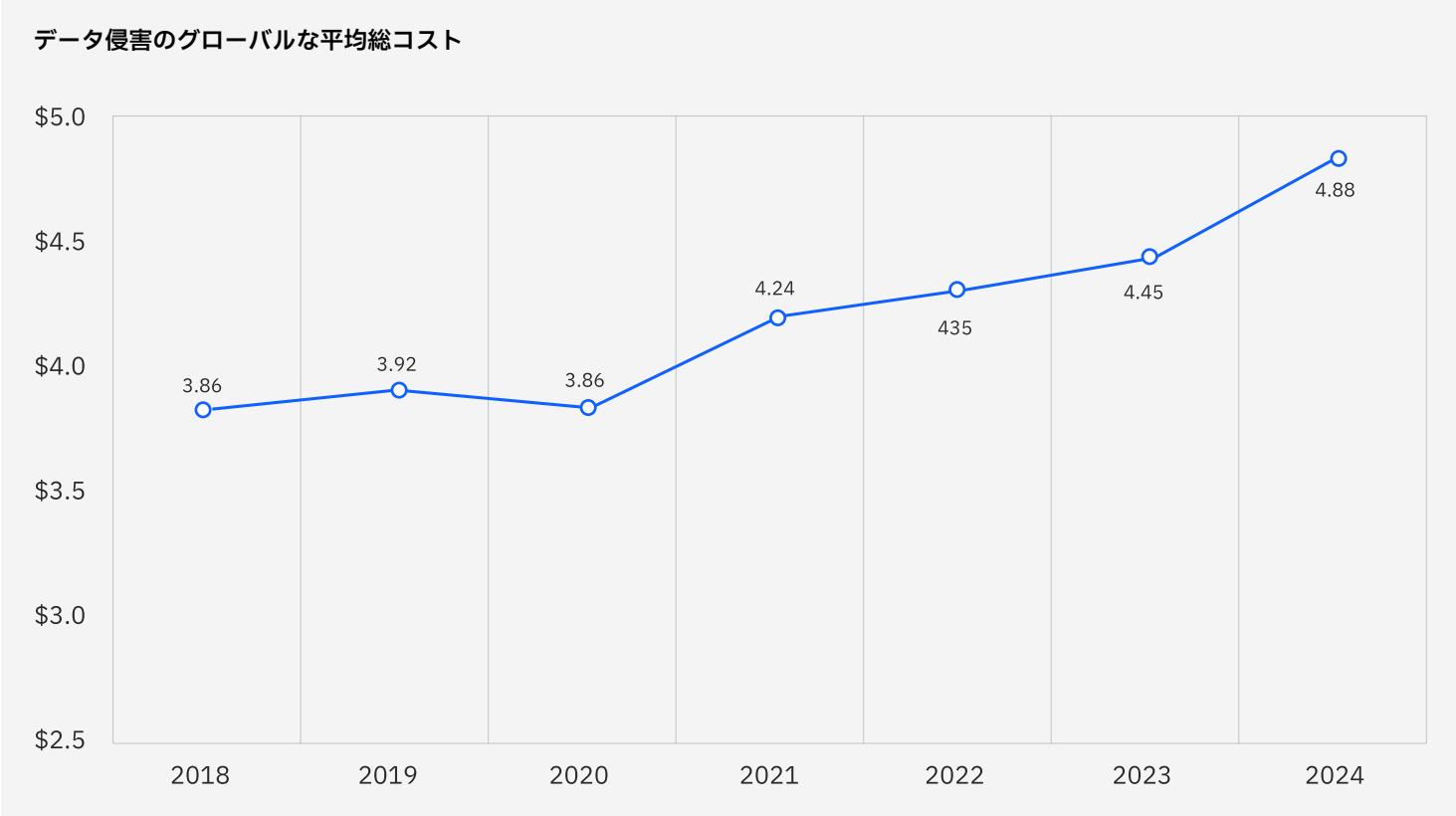


図1：単位は百万米ドル

米国が平均侵害コストで世界一
14年目では、調査対象となった16の国または地域の中で、米国の平均データ侵害コストが最も高く、936万米ドルでした。上位5カ国には、中東、ドイツ、イタリア、ベネルクスが入りました。ベネルクスとはベルギー、オランダ、ルクセンブルクの経済連合で、今年新たに加わりました。注目すべき点は、カナダと日本では平均コストが下がったのに対して、イタリアと中東では大幅に上昇したことです。図2Aおよび2Bを参照してください。

国または地域別のデータ侵害コスト

#	国	2024	2023
1	アメリカ合衆国	$9.36	$9.48
2	中東	$8.75	$8.07
3	ベネルクス	$5.90	—
4	ドイツ	$5.31	$4.67
5	イタリア	$4.73	$3.86
6	カナダ	$4.66	$5.13
7	イギリス	$4.53	$4.21
8	日本	$4.19	$4.52
9	フランス	$4.17	$4.08
10	ラテンアメリカ	$4.16	$3.69
11	韓国	$3.62	$3.48
12	ASEAN	$3.23	$3.05
13	オーストラリア	$2.78	$2.70
14	南アフリカ共和国	$2.78	$2.79
15	インド	$2.35	$2.18
16	ブラジル	$1.36	$1.22

図2A：単位は百万米ドル

上位5か国または地域の2024年と2023年の比較

#	コストの推移	2024	2023
1	↓	**米国** $9.36	**米国** $9.48
2	↑	**中東** $8.75	**中東** $8.07
3	↑	**ベネルクス** $5.90	**カナダ** $5.13
4	↑	**ドイツ** $5.31	**ドイツ** $4.67
5	↑	**イタリア** $4.73	**日本** $4.52

図2B：単位は百万米ドル

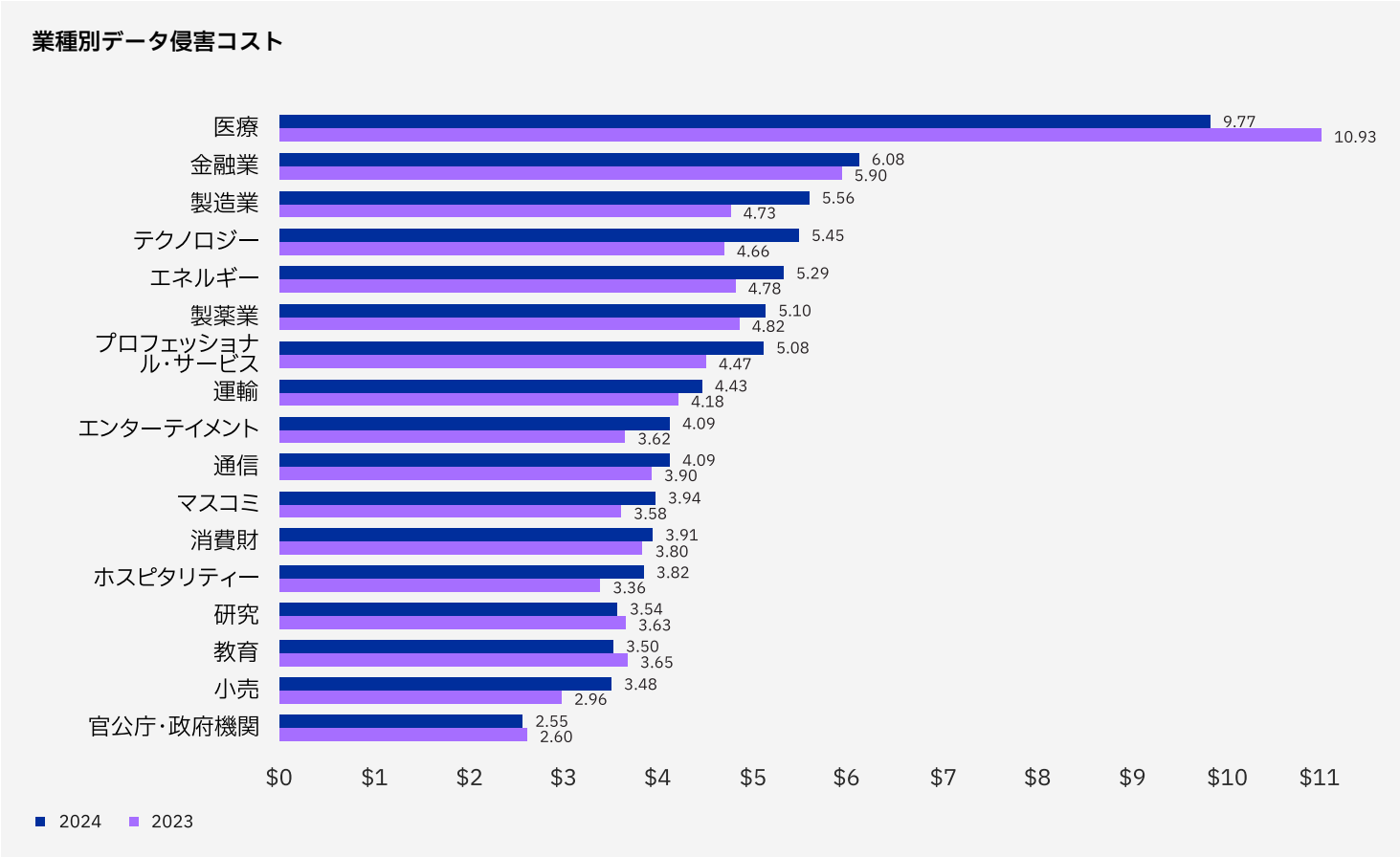


図3：単位は百万米ドル

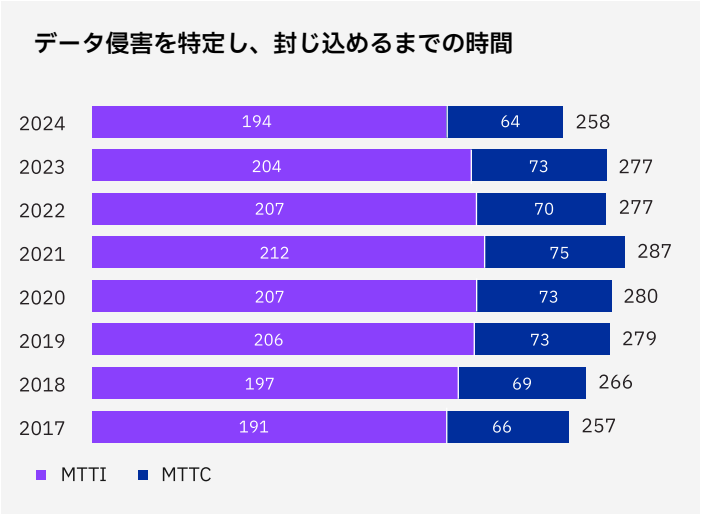


図4：単位は日数

医療業界が依然として侵害コストのトップ
医療業界の平均侵害コストは10.6%減の977万米ドルでした。しかし、この要因だけでは、侵害コストが最も大きい業界として2011年以来続いているトップの座から外れるには十分ではありませんでした。医療業界は既存のテクノロジーに悩まされることが多く、中断に対して非常に脆弱であるため、依然として攻撃者の標的となっています。これは患者の安全を脅かす事態になりかねません。図3を参照してください。

侵害を特定し、封じ込めるまでの平均時間が短縮
防御側が侵害を特定し、封じ込めるのに要した平均時間は、前年の277日から258日に減少し、7年ぶりの低水準となりました。注：この平均特定時間（MTTI）と平均封じ込め時間（MTTC）の世界平均にはベネルクス（ベルギー、オランダ、ルクセンブルク）は含まれていません。これは、ベネルクスが新たな調査対象地域であるため、影響力が大きく、結果が平均よりも大きく偏っていたためです。図4を参照してください。

事業損失コストと侵害後の対応コストが急増
事業損失と侵害後の対応によるコストは前年比で約11%増加し、侵害コスト全体の大幅な上昇につながりました。事業損失コストには、システムのダウンタイムによる収益損失や、顧客損失、評判低下によるコストが含まれます。侵害後のコストには、影響を受けた顧客への対応のためにコールセンターや信用監視サービスを設置する費用、規制による罰金の支払いなどが含まれる場合があります。図5を参照してください。

4つの要素におけるデータ侵害の平均コスト

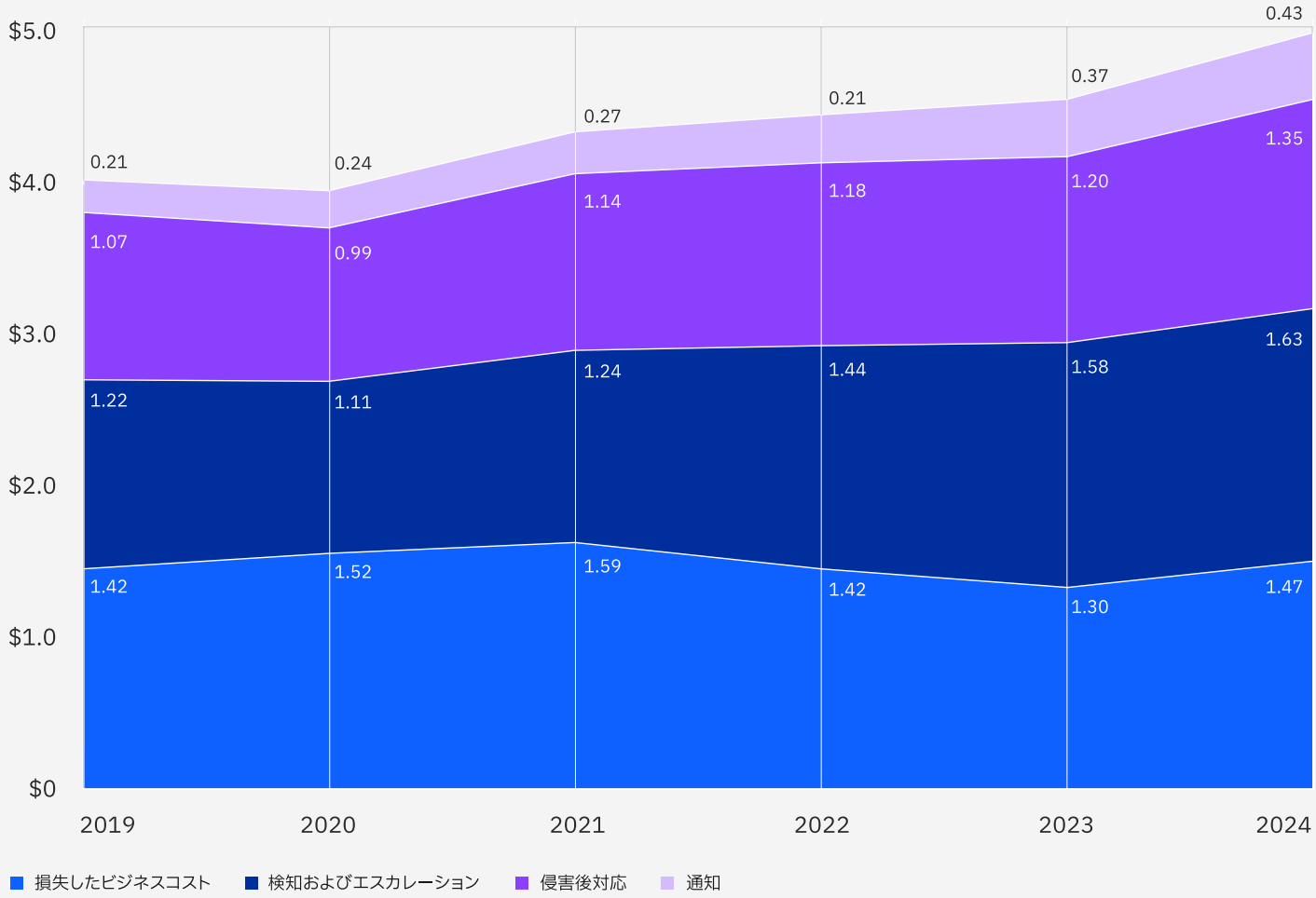


図5：単位は百万米ドル

ほとんどの侵害に顧客PIIが関与
盗難または侵害に遭ったデータの種類で最も多かったのは、顧客PIIで、46%でした。PIIには納税者番号やEメール、自宅の住所などが含まれており、なりすましやクレジットカード詐欺に利用されることがあります。盗難された全レコード・タイプの世界平均は169米ドルにのぼり、従業員PIIが最も高額でした。図6Aおよび6Bを参照してください。

侵害を受けたデータの種類（割合別）

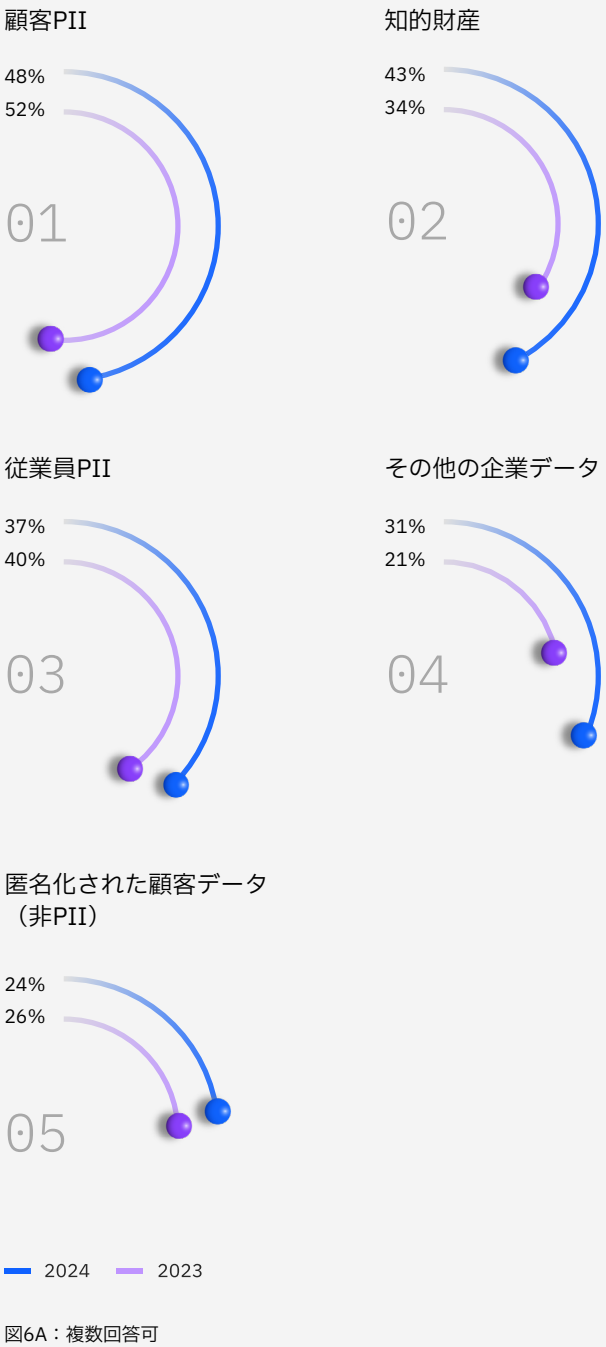


図6A：複数回答可

侵害されたレコード・タイプ別に見たデータ侵害のレコード1件あたりのコスト

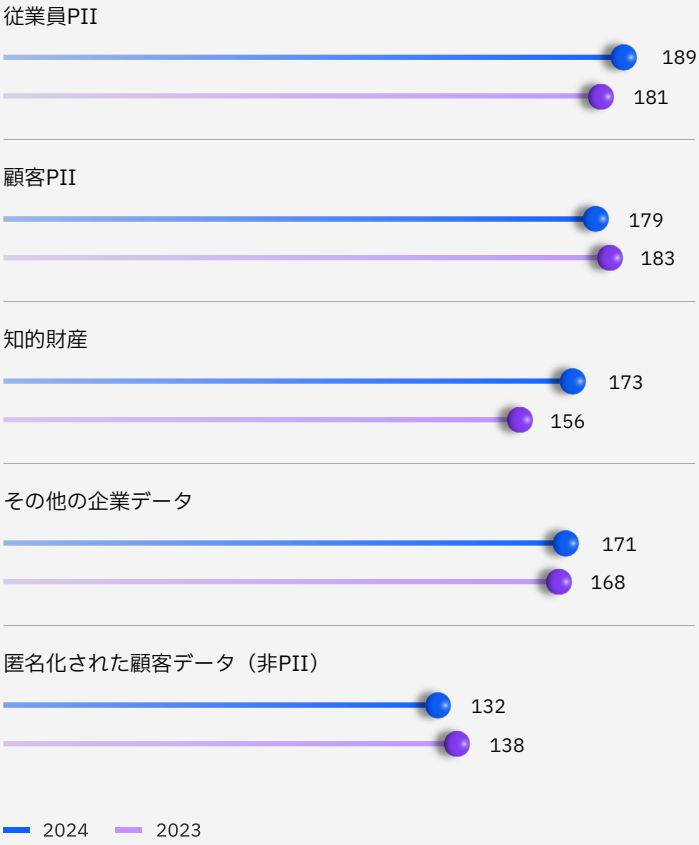


図6B：単位は百万米ドル

481万米ドル

攻撃者が侵害された認証情報を使用した場合の侵害の平均コスト（調査対象の侵害事例の16%で発生）。

初期の攻撃ベクトルと根本原因

フィッシングと認証情報の盗難または漏洩の2つが2年連続で最も一般的な攻撃ベクトルでした。どちらも、最もコストのかかるインシデント・タイプのトップ4にランクインしています。この調査では、侵害の最も一般的な根本原因を特定することに加え、各カテゴリーの平均コストと、侵害を特定して封じ込めるまでの平均時間の比較が行われました。

初期の攻撃ベクトルのトップは、認証情報の漏洩
認証情報の漏洩は、侵害の16%で攻撃者に利益をもたらしました。認証情報の漏洩攻撃は、組織にとっても大きな損害となる可能性があり、侵害1件あたり平均481万米ドルに及びます。フィッシングは、攻撃ベクトルの15%を占め、僅差で2位でしたが、最終的な被害額はさらに大きくなり、488万米ドルでした。悪意のあるインサイダー攻撃による被害額は、499万米ドルと最も大きかったものの、侵害経路全体のわずか7%でした。
図7を参照してください。

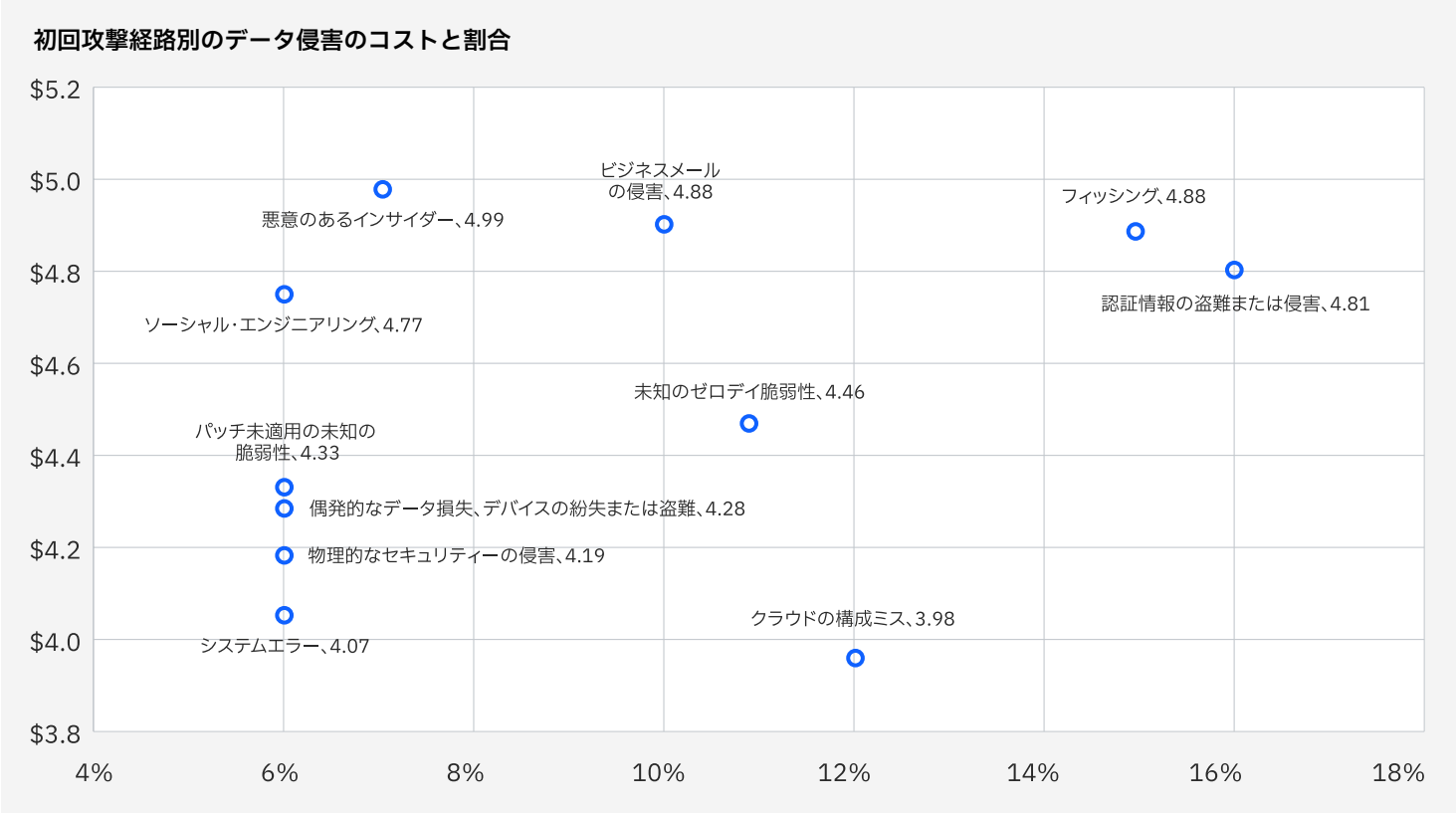


図7：単位は百万米ドル、全侵害に占める割合

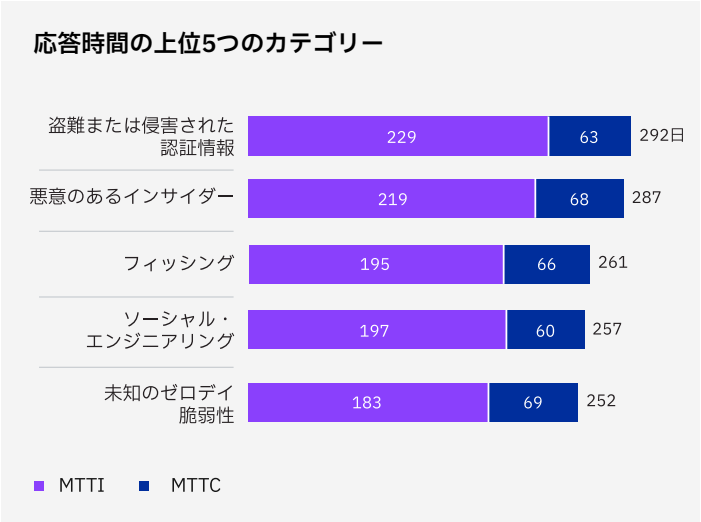


図8：単位は日数

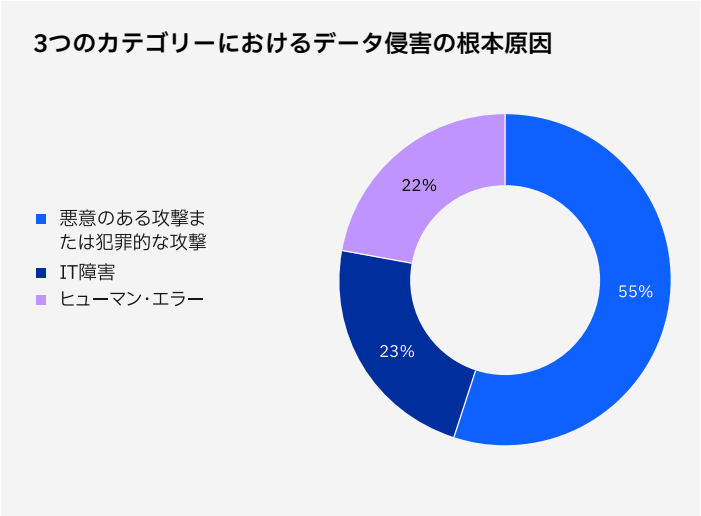


図9：

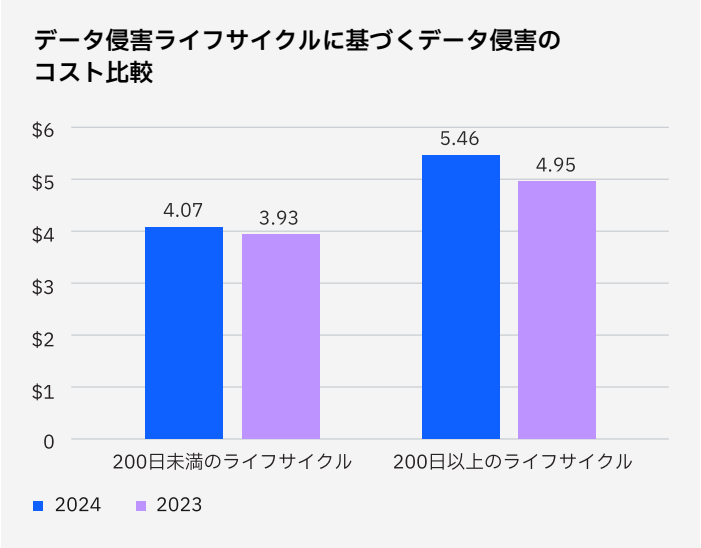


図10：単位は百万米ドル

認証情報を利用した攻撃は、特定と封じ込めに時間がかかった
認証情報が盗まれたか、悪意のあるインサイダーによって使用されたかを問わず、攻撃の特定と封じ込めにかかる時間が増加し、平均合計時間はそれぞれ292日と287日となりました。防御側は、ネットワーク上の正当なユーザー活動と悪意のあるユーザー活動を区別する必要があるため、脅威の特定が余計に困難でした。一方、ゼロデイ脆弱性を利用した攻撃は、封じ込めに最も時間がかかりました。図8を参照してください。

IT障害や人為的ミスが原因による侵害が約半数
外部からの攻撃者や犯罪に関与するインサイダーによる悪意のある攻撃は、全侵害の55%を占めています。このような侵害が懸念されるのと同様に、残りの23%はIT障害によるもので、22%は人為的ミスによるものであることにも留意する必要があります。図9を参照してください。

データ侵害ライフサイクル

データ侵害において時間はお金に比例し、ライフサイクルが長い侵害はよりコストがかかることが、2023年と2024年の調査で明らかになりました。侵害ライフサイクル全体とは、侵害を特定するまでの平均日数と封じ込めるまでの平均日数を組み合わせたものです。両レポートでは、データ侵害のライフサイクル全体が200日未満であった場合の平均コストと、ライフサイクル全体が200日を超えた場合の平均コストを比較しています。

侵害ライフサイクルが長ければ、コストが高くなる
今年度のレポートでは、ライフサイクルが200日を超えるデータ侵害の平均コストが、ライフサイクルが200日未満の侵害の場合と比べて最も高く、546万米ドルであることが判明しました。これらの調査結果は、前年度のものと一致しています。注目すべきなのは、データ侵害のライフサイクルが長い場合のコストが昨年より10.3%増加したのに対し、ライフサイクルが短い場合のコストは3.6%と増加率が小さいことです。図10を参照してください。

侵害の特定

データ侵害を封じ込めるには、まずそれを特定する必要があります。誰がどれだけ早く特定するかによって、データ侵害のコストに違いが現れます。今年は、独自のツールを使用しているセキュリティー・チームは、この分野でのパフォーマンスが向上していることが判明しました。また、侵害が、セキュリティー研究者、法執行機関、コンサルタントなどの無害な第三者や攻撃者自身によって特定されたケースもあります。

セキュリティー・チームがほとんどの侵害を特定
セキュリティー・チームとそのツールが侵害を検知する頻度は42%で、善意の第三者の34%や攻撃者自身の場合の24%を上回っています。この数字は、セキュリティー・チームが侵害を発見した割合がわずか3分の1だった2023年度レポートのときよりも改善されています。この変化は、セキュリティー・チームが検知の迅速化に成功したことを示しています。図11を参照してください。

データ侵害の特定方法

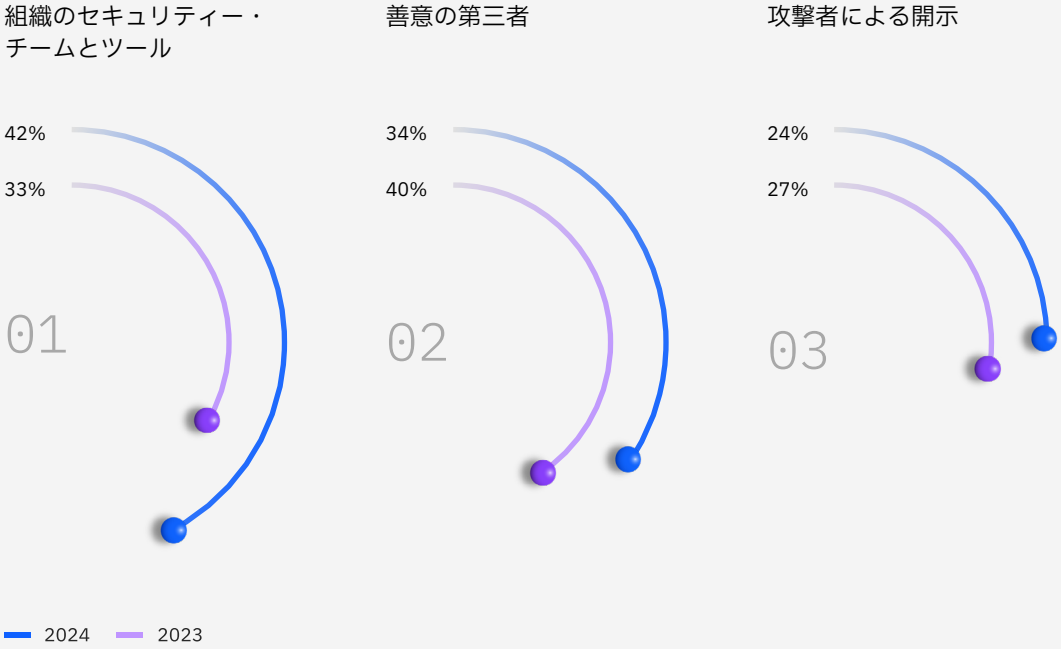


図11：単一回答のみ

553万米ドル

侵害が攻撃者によって開示された場合の平均侵害コスト。

攻撃者によって開示された侵害はコストがより高い
攻撃者が侵害を開示する頃には、既に目的を達成し、かなりの損害を与えている可能性が高く、侵害の全体的なコストは増加しています。攻撃者によって侵害が開示されたときの平均コストは553万米ドルでした。一方、セキュリティー・チームが侵害を特定したときの平均コストは455万米ドルでした。図12を参照してください。

侵害の特定と封じ込めの迅速化
レポートによると、侵害がどのように明らかになったかを問わず、2024年にはその特定と封じ込めが前年よりも平均してより迅速になったことが明らかになりました。本レポートの次のセクションで示すように、AIと自動化の活用がこの迅速化に寄与した可能性があります。図13を参照してください。

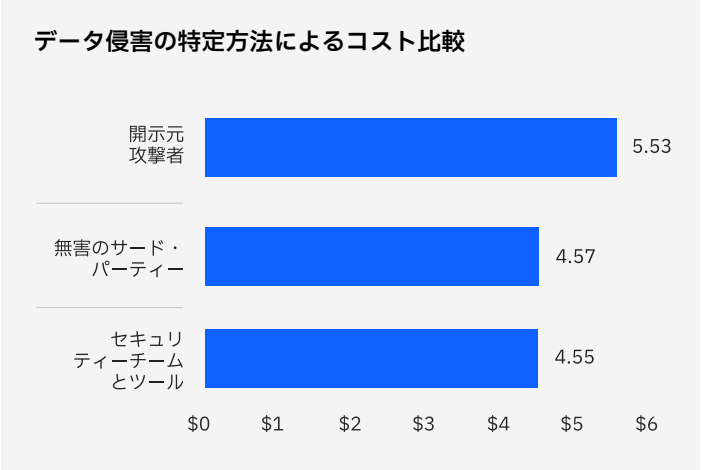


図12：単位は百万米ドル

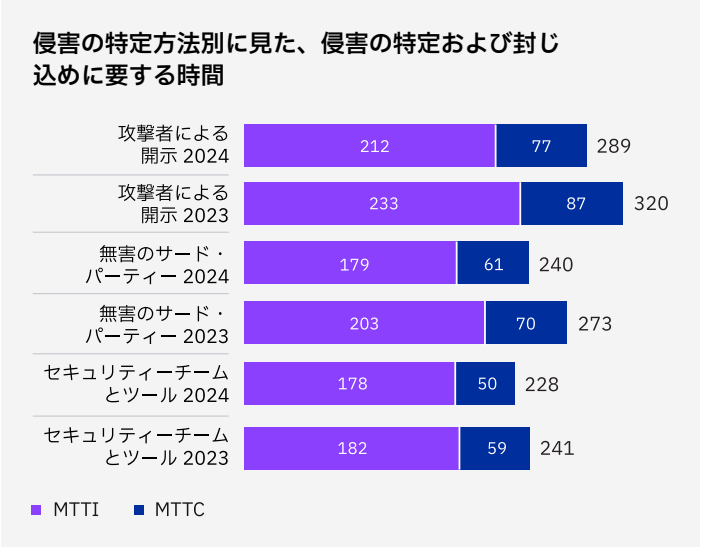


図13：単位は日数

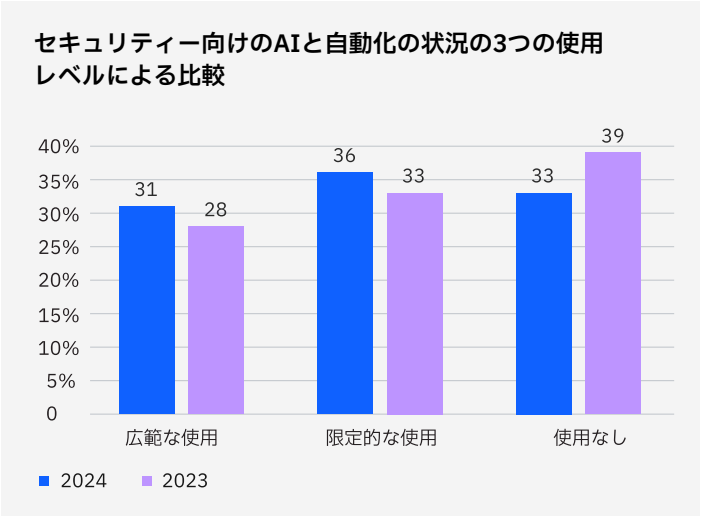


図14：使用レベル別の組織の割合

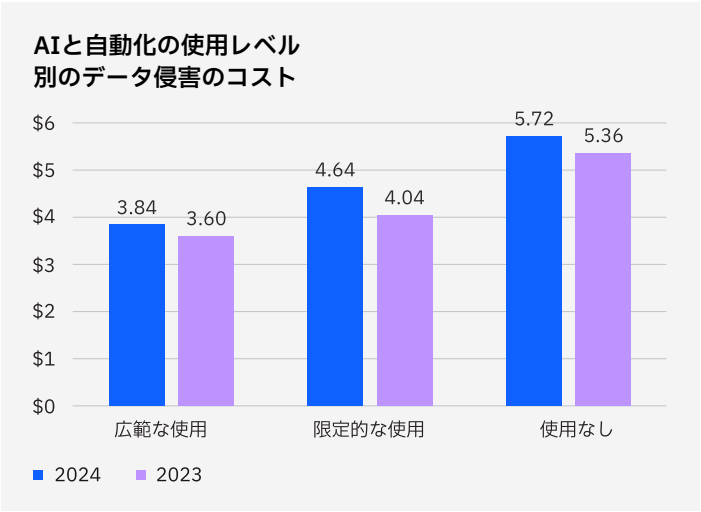


図15：単位は百万米ドル

セキュリティー向けのAIと自動化

AIと自動化が、サイバーセキュリティーの世界を変革しています。これにより、悪意のある攻撃者は攻撃を作成して大規模に開始することがこれまで以上に容易になります。一方、防御側には脅威を迅速に特定し、脅威への対応を自動化するための新たなツールが提供されます。今年度のレポートでは、これらのテクノロジーが侵害の特定と封じ込めを加速させ、コストを削減することが明らかになりました。

AIと自動化の利用が拡大
セキュリティー向けのAIと自動化を広範に利用している組織の数が、昨年の28%から、今年の調査では31%に増加しました。わずか3ポイントの差ですが、10.7%の利用増を意味します。AIと自動化を限定的に使用している組織の割合も、33%から36%に増え、9.1%の利用増となりました。図14を参照してください。

AIと自動化利用の増加は、侵害コスト低下を意味する
AIと自動化を利用している組織ほど、平均侵害コストが低くなります。この相関関係は顕著であり、今年度のレポートの重要な調査結果の1つです。AIと自動化を利用していない組織の平均コストは572万米ドルでしたが、AIと自動化を広範に利用している組織の平均コストは384万米ドルであり、188万米ドル節約したことになります。図15を参照してください。

27%

4つのセキュリティー・カテゴリーでAIと
自動化を利用した組織の割合。

AIの利用により、特定と封じ込めが迅速化
セキュリティー向けのAIと自動化を広範に利用している組織は、これらのテクノロジーをまったく利用していない組織よりもデータ侵害の特定と封じ込めが平均で約100日迅速化されました。図16を参照してください。

セキュリティー・チームはAIと自動化を機能全体に均等に適用
AIと自動化を広範に利用していると回答した組織のうち約27%が予防・検知・調査・対応の各カテゴリーでAIを広範囲に利用していました。また、およそ40%がAIテクノロジーを少なくとも多少は利用していました。図17を参照してください。

AIと自動化の使用レベル別に見た、データ侵害の特定・封じ込めに要する時間

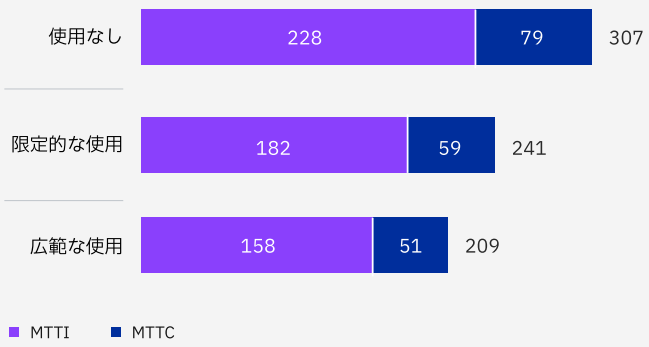


図16：単位は日数

4つのセキュリティー・カテゴリーでAIと自動化を使用した割合

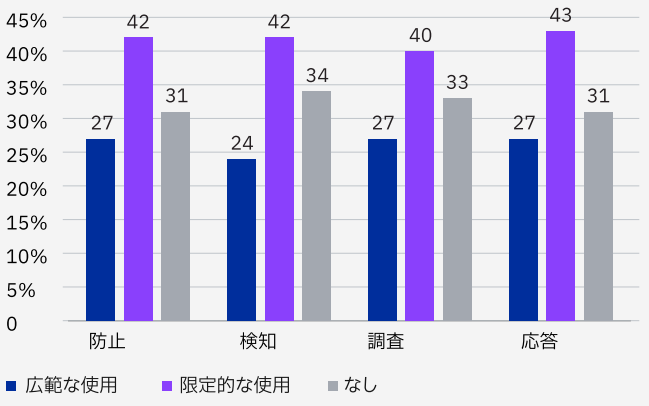


図17：AIと自動化を幅広く利用していると報告した回答者の場合：参考図14

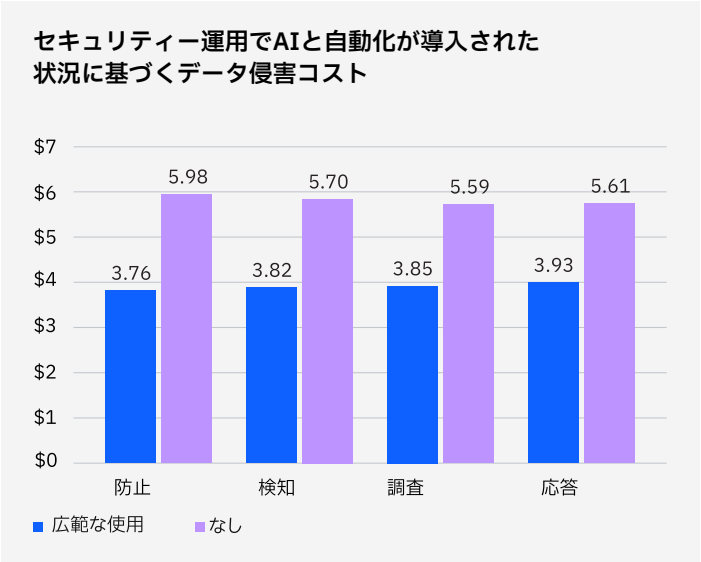


図18：AIと自動化を幅広く利用していると報告した組織の場合（単位：百万米ドル）：図14参照

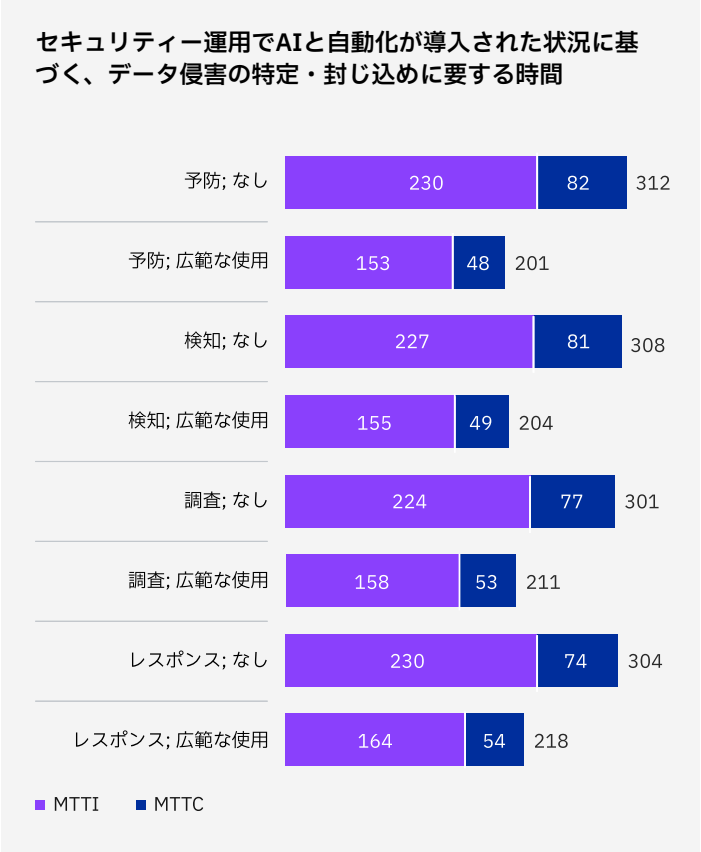


図19：AIと自動化を幅広く利用していると報告した組織の場合（単位：日数）：図14参照

AIと自動化の広範な利用でコスト削減

AIと自動化をセキュリティーの4つの分野でそれぞれ広範に利用した場合、同分野でこれらのテクノロジーを使用しなかった組織と比較して、平均侵害コストが大幅に低下しました。例えば、組織が予防のためにAIと自動化を広範に使用した場合、その平均侵害コストは376万米ドルでした。一方、これらのツールを予防のために使用しなかった組織では、コストが598万米ドルとなり、その差は45.6%でした。図18を参照してください。

AIと自動化により、侵害の特定と封じ込めに要する時間短縮

AIと自動化が適用された分野では、侵害の特定と封じ込めの作業が迅速化されました。予防・検知・調査・対応など、あらゆるセキュリティー機能でAIと自動化を広範に利用することで、データ侵害に対するMTTIとMTTCの平均値が、対応で33%、予防で43%低下しました。図19を参照してください。

70%

侵害の結果、業務に重大な中断または非常に重大な中断が生じた組織の割合。

侵害後の価格引き上げ

データ侵害はその性質上高くつきます。何百万ドルものコストを背負い込むことになった組織は、そのコストを別の場所で回収しようと考えるかもしれません。1つの選択肢は、価格の引き上げという形で自社の顧客に転嫁することで、これは増加傾向にあります。既に価格圧力に直面している市場では、価格の引き上げはリスクを伴うおそれがあります。

組織は侵害コストを顧客に転嫁
ほとんどの組織は、データ侵害後に商品やサービスの価格を引き上げ、コストを顧客に転嫁する予定だと答えました。そのような計画を立てている組織の割合は、昨年の57%から今年は63%に増加し、10.5%の増加となりました。図20を参照してください。

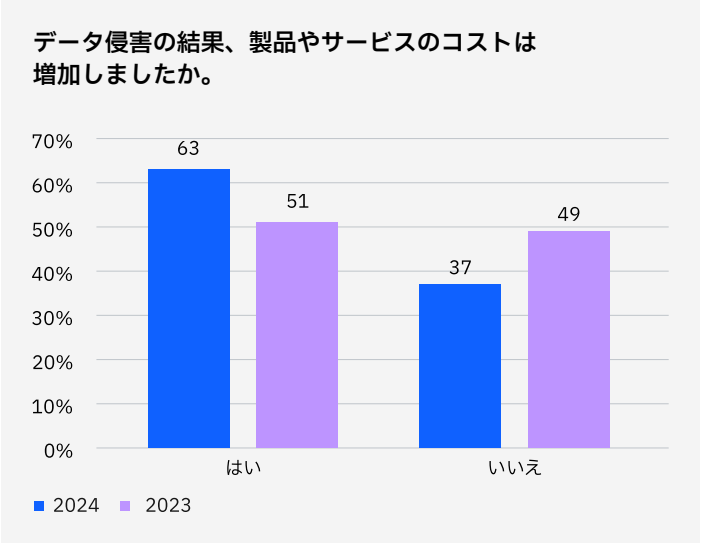


図20：全組織に占める割合

業務の中断

業務はデータで成り立っています。データが侵害されれば、業務が中断されます。こうした中断は、少数のシステムに影響する小規模な侵害から、長期に及ぶ組織全体の業務停止までさまざまです。そこで、これらの中断がどの程度軽微または重大であったか、また中断の深刻度とデータ侵害のコストとの相関関係に関する調査を行いました。

業務中断は相当なレベル
今年の調査対象となった組織の70%で、侵害によって業務に重大なまたは非常に重大な中断が生じました。中断の程度が低いと答えたのはわずか1%でした。図21を参照してください。

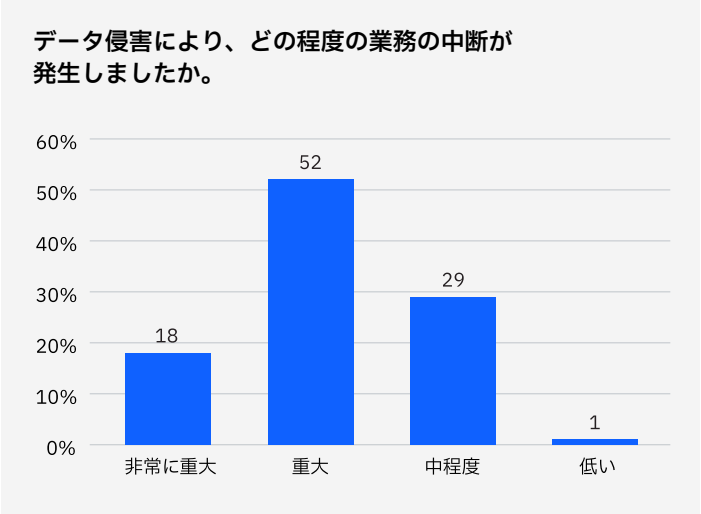


図21：単一回答のみ

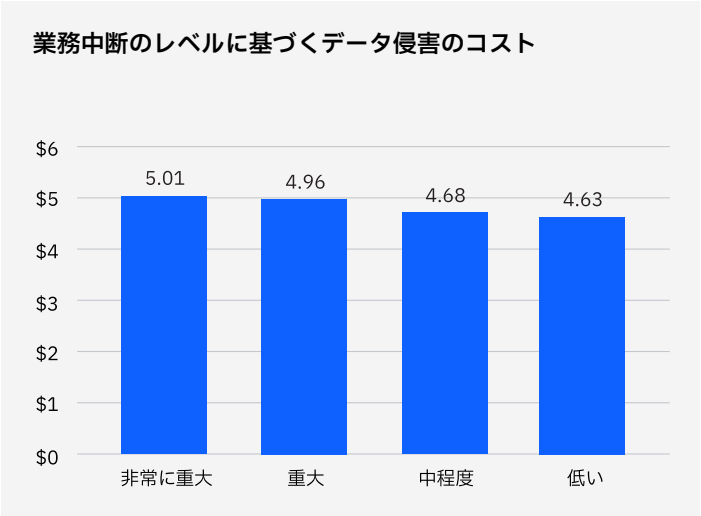


図22：単位は百万米ドル

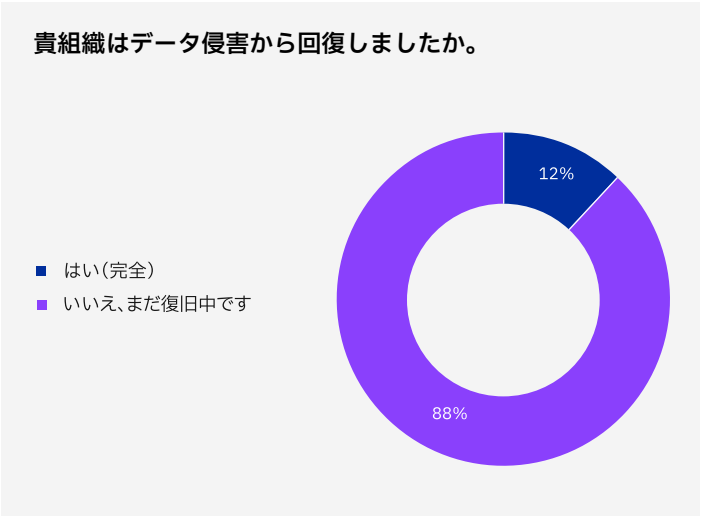


図23：侵害された全組織に占める割合

侵害の平均コストは中断とともに増加
平均侵害コストは、業務の中断が大きいほど高くなりました。中断の程度が低いと報告した組織でさえ、平均463万米ドルのデータ侵害コストが発生しました。非常に大きな中断を報告した組織の平均コストは7.9%高く、501万米ドルでした。図22を参照してください。

回復時間

侵害を封じ込めた後も、回復作業が続きます。この調査では、回復とは以下のことを意味します。

– 侵害の影響を受けた分野で、業務が通常状態に戻る。
– 組織は、罰金の支払いなどのコンプライアンス義務を果たしている。
– 顧客の信頼と従業員の信用が回復している。
– 組織は、将来のデータ侵害を回避するために、管理やテクノロジー、専門知識を導入している。

顧客の信頼を再構築するなど、この作業の多くには、テクノロジー以外の要素が関わっています。ほとんどの組織にとって、回復のための作業は困難で、数カ月かかる場合があります。

侵害の回復率は低い
今年度のレポートでは、データ侵害から完全に回復したと回答した組織はわずか12%でした。ほとんどの組織は、まだ取り組んでいる段階であると答えました。図23を参照してください。

完全回復に100日以上
完全に回復した組織のうち、4分の3以上が100日以上かかったと回答しました。回復には長い時間がかかります。完全に回復した組織のおよそ3分の1が、回復に150日以上を要したと回答しました。完全に回復した組織のうち、50日未満で回復できたのはわずか3%でした。図24を参照してください。

データ侵害からの回復に要する平均時間

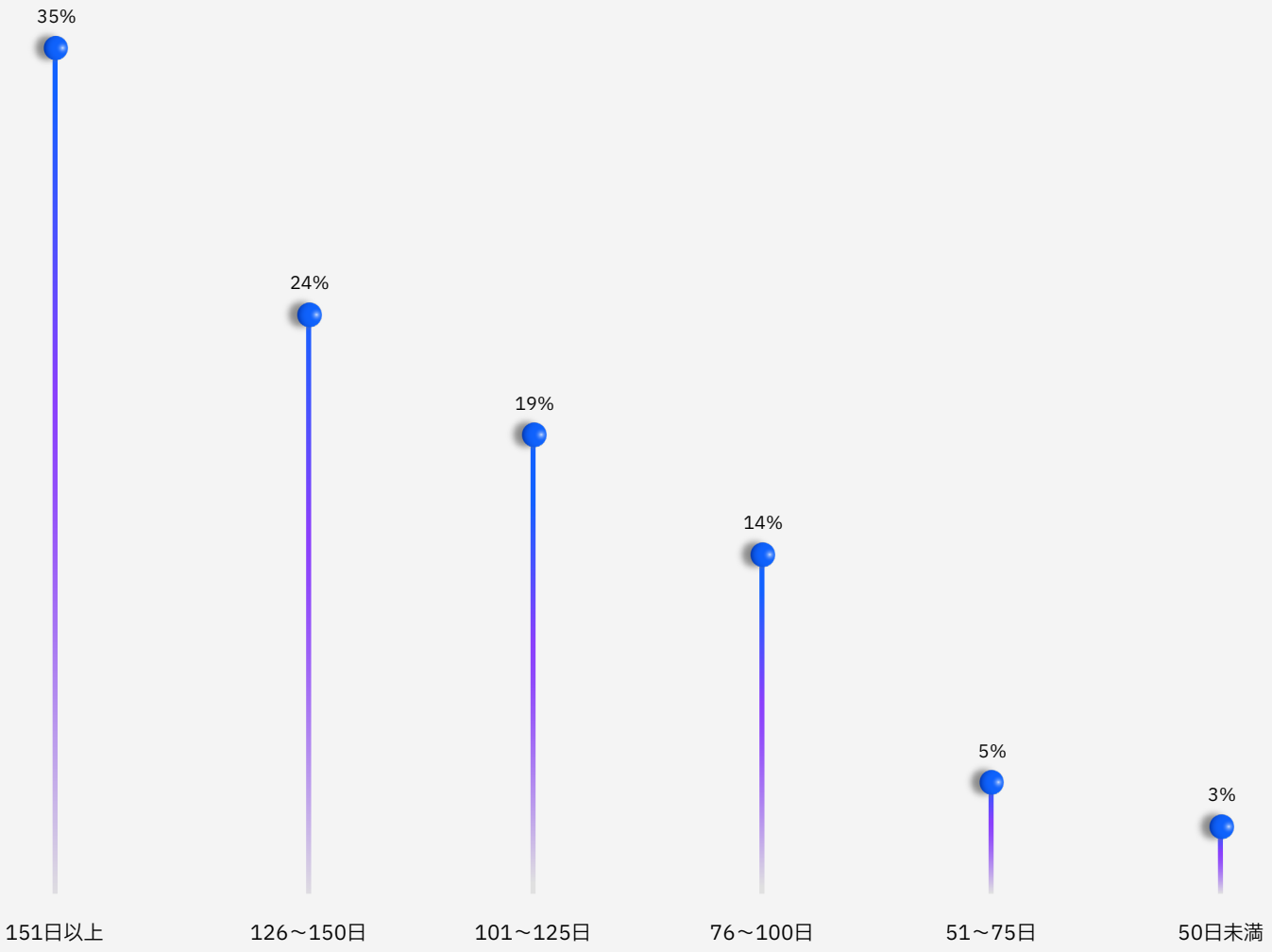


図24：インシデントから回復したと報告した組織の場合（単位：日数）（図23参照）

図25：侵害の平均である488万米ドルとのコストの差（単位：米ドル）

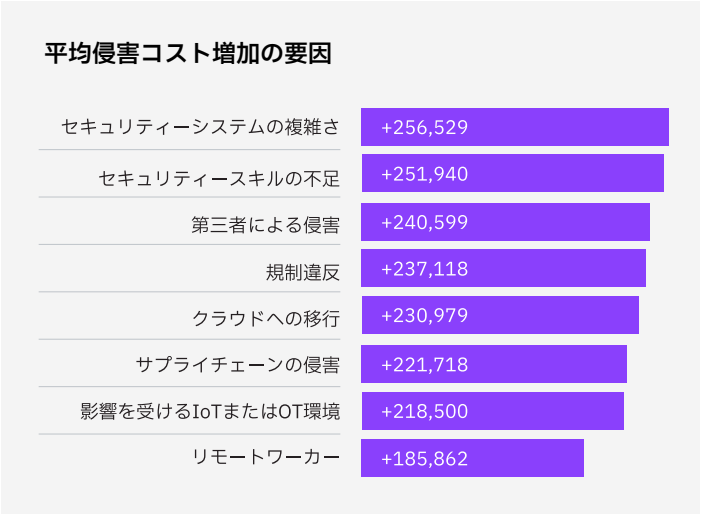


図26：侵害の平均である488万米ドルとのコストの差（単位：米ドル）

平均侵害コストを左右する要因

コストを分析する際には、どのテクノロジーやイベントがコストの増加傾向または減少傾向にあるかを知ることが有益です。判明した一定条件は、AIと自動化はコストを下げる一方で、深刻なサイバー・スキル不足はコストを上げるという点です。この分析では、28の要因を調べました。それぞれの影響を1つずつ、世界平均と比べて検討しました。次に、平均的なデータ侵害コストを増減させる上位3つの要因を調べました。

コスト減少の主な要因
この分析では、従業員トレーニングやAIと機械学習による洞察の活用が、平均的なデータ侵害コストを軽減する要因の上位を占めました。従業員トレーニングは、特にフィッシング攻撃を検知および阻止するためのサイバー防衛戦略において引き続き不可欠な要素となっています。2位には僅差でAIと機械学習による洞察が続きました。図25を参照してください。

コスト増加の主な要因
この分析で、侵害コストを増大させた要因のトップ3は、セキュリティー・システムの複雑さ、セキュリティー・スキルの不足、サードパーティーによる侵害（サプライチェーン侵害を含む）でした。図26を参照してください。

574万ドル

セキュリティー・スキルが非常に不足している
組織の平均侵害コスト

高・低レベルの主要なコスト増大要因の比較
セキュリティー・スキル不足の程度が高い組織の平均侵害コストは574万米ドルであるのに対し、スキル不足の程度が低い組織では398万米ドルでした。同様の差は、他の2つの主要なコスト要因分野でも見られました。図27を参照してください。

高・低レベルの主要なコスト軽減要因の比較
従業員トレーニングのレベルが低い組織では、侵害コストの平均は510万ドルであったのに対し、従業員トレーニングのレベルが高い組織では415万ドルでした。同様の差は、他の2つの主要なコスト要因分野でも見られました。図28を参照してください。

3つのコスト増加要因が高いレベルにある組織と低いレベルにある組織のデータ侵害のコスト

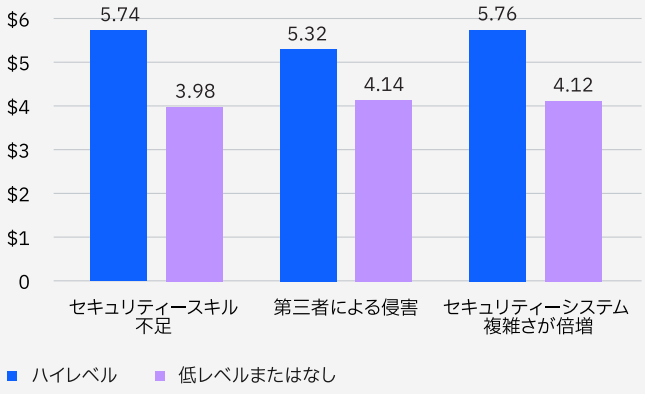


図27：単位は百万米ドル

3つのコスト削減要因が高いレベルにある組織と低いレベルにある組織のデータ侵害のコスト

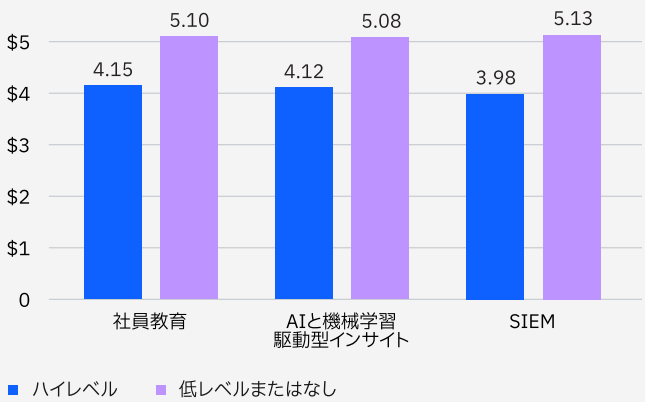


図28：単位は百万米ドル

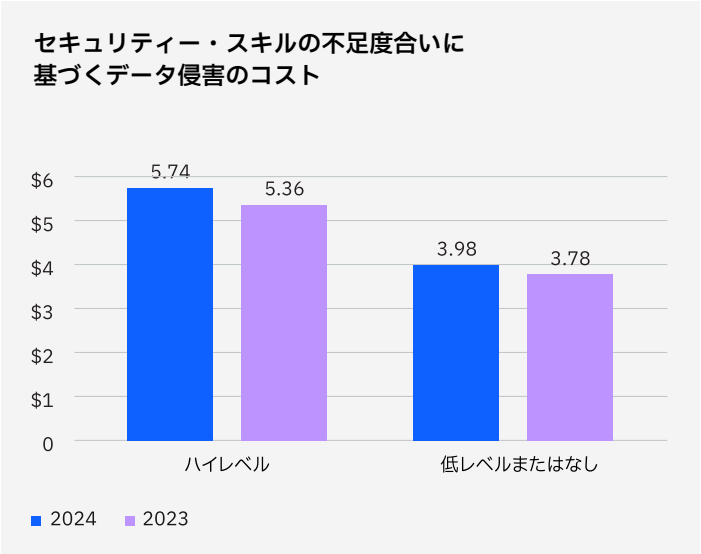


図29：単位は百万米ドル

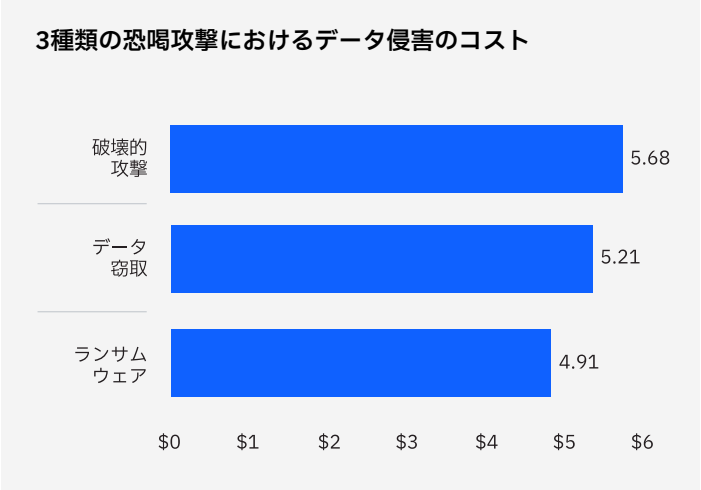


図30：単位は百万米ドル

セキュリティー・スキルの不足

熟練したセキュリティー要員の不足が深刻化している組織の数は、昨年の42%から、2024年には53%に激増しました。今年の調査では、スキル不足の深刻化とデータ侵害コストの上昇との間に強い相関関係があることが判明しました。

スキル不足は侵害コストの増加に等しい
2024年に、高程度のスキル不足に関連する侵害平均コストは、昨年の536万米ドルから574万米ドルに急増し、7.1%上昇しました。この増加は、世界平均の侵害コストを86万米ドル上回ります。図29を参照してください。

恐喝攻撃のコスト

組織が恐喝攻撃に費やすコストは、攻撃の種類（ランサムウェア攻撃、データ窃盗攻撃、破壊的攻撃など）や、組織の対応方法によって異なります。この要因は、今年の調査が示すように、法執行機関に通報された場合に特に当てはまります。法執行機関の捜査官が関与した場合、コストは劇的に減少しました。調査では、データが暗号化され、身代金が要求されるランサムウェア攻撃やデータが盗まれ、組織が恐喝されることもあるデータ窃盗攻撃、攻撃者が自らの目的のためにデータを削除し、システムを破壊する破壊的攻撃という、3種類の攻撃がすべて検証されました。

破壊的攻撃のコストは他の恐喝を上回る
破壊的な攻撃、つまり高額で永続的な損害を意図した攻撃は平均568万米ドルに達し、ランサムウェア攻撃やデータ窃盗攻撃よりもコストが高いことが判明しました。図30を参照してください。

63%

法執行機関を関与させ、身代金の支払いを回避したランサムウェア被害者の割合。

3種類の恐喝攻撃の特定と封じ込めに要する時間
この3種類の攻撃はすべて、特定と封じ込めに284日から294日を要しました。図31を参照してください。

身代金の支払い
組織がランサムウェアの被害に遭った場合、52%が法執行機関に通報しました。そのような組織の大多数（63%）は、身代金を支払いませんでした。図32を参照してください。

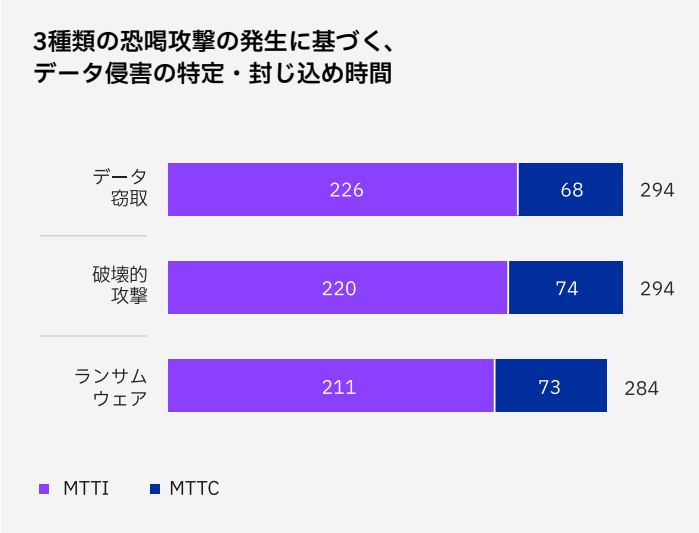


図31：単位は日数

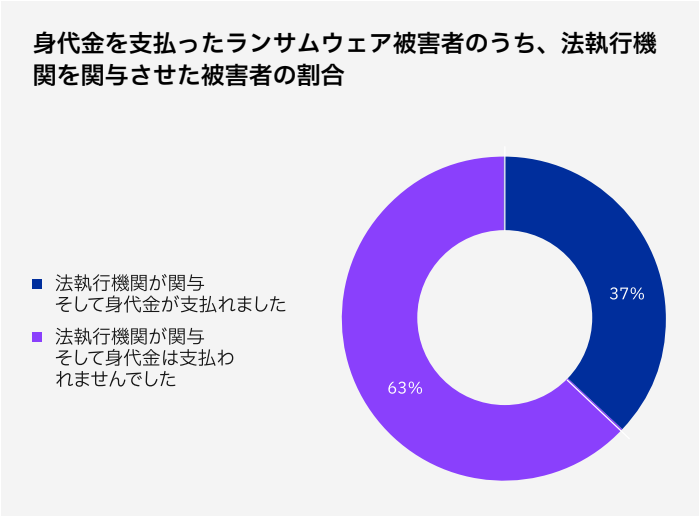


図32：

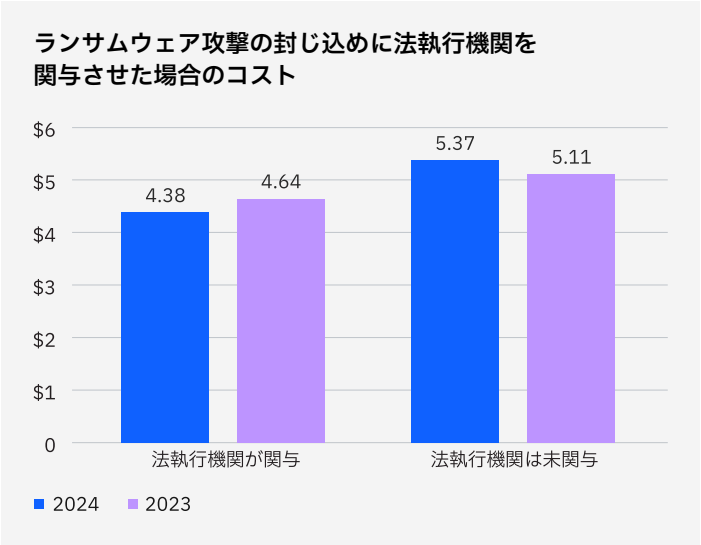


図33：単位は百万米ドル

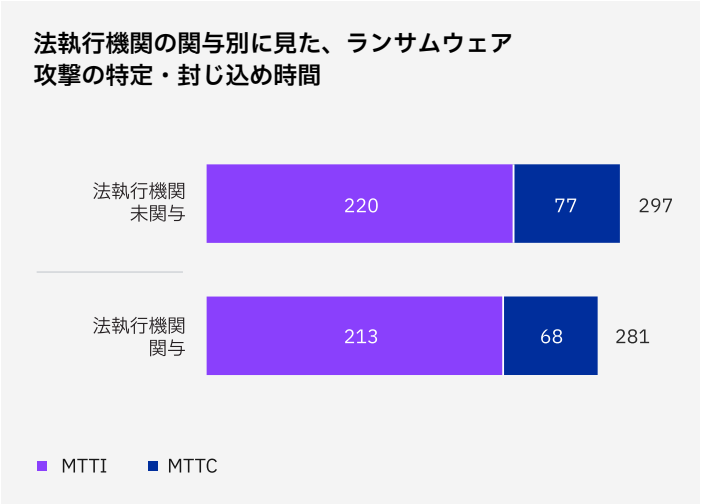


図34：単位は日数

法執行機関の関与が侵害コストを低減
平均侵害コストは、法執行機関を関与させた場合の438万米ドルから、法執行機関を関与させなかった場合の537万米ドルまで幅があり、コストの差は20%以上、つまりほぼ100万米ドルでした。注：これらのコストには身代金の支払いは含まれていません。図33を参照してください。法執行機関を関与させることも、侵害の特定と封じ込めにかかる時間を短縮する要因になりました。図34を参照してください。

↑ 22.7%

5万米ドル以上の罰金を支払う組織の割合の増加。

侵害の報告および規制による罰金

今年のレポートでは、ほとんどの組織が規制当局やその他の政府機関に侵害を報告していることが判明しました。また、約3分の1が罰金を支払っていました。その結果、報告や罰金の支払いが侵害後の対応として一般的なものとなりました。この調査では、罰金の規模と、組織が規制当局に侵害を開示するまでに要した期間を調べました。ほとんどの組織が数日以内に侵害を報告していました。

平均の侵害報告時間
半数以上の組織が72時間以内にデータ侵害を報告しましたが、34%は報告までに72時間以上かかりました。侵害を報告する必要がなかった組織はわずか11%でした。図35を参照してください。

規制当局の罰金額増加
規制当局の高額な罰金を支払う組織が増加しており、5万米ドル以上を支払った組織は前年比22.7%増、10万米ドル以上を支払った組織は19.5%増となりました。図36を参照してください。

規制上の義務により、侵害を報告する必要がありましたか。また、報告する必要があった場合、侵害が検知されてから報告までにどれくらいの時間がかかりましたか。

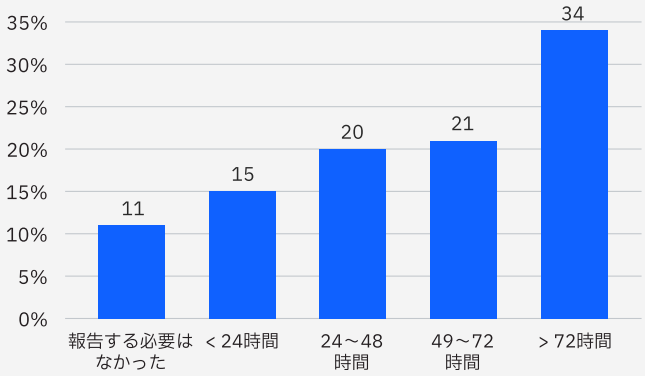


図35：全侵害に占める割合。単一回答のみ

データ侵害を受けたことにより科された罰金の分布

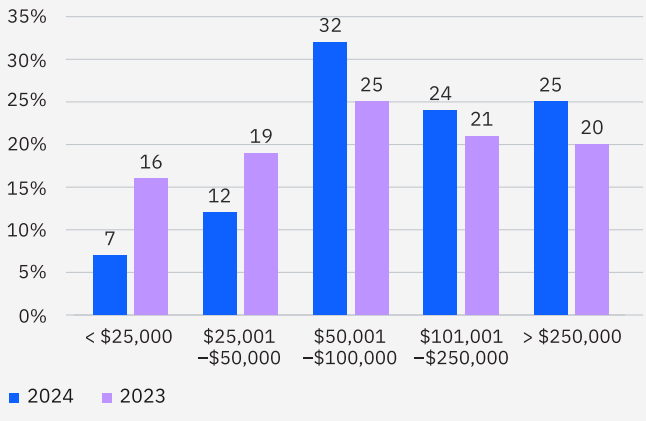


図36：罰金を科された組織（単位は百万米ドル）

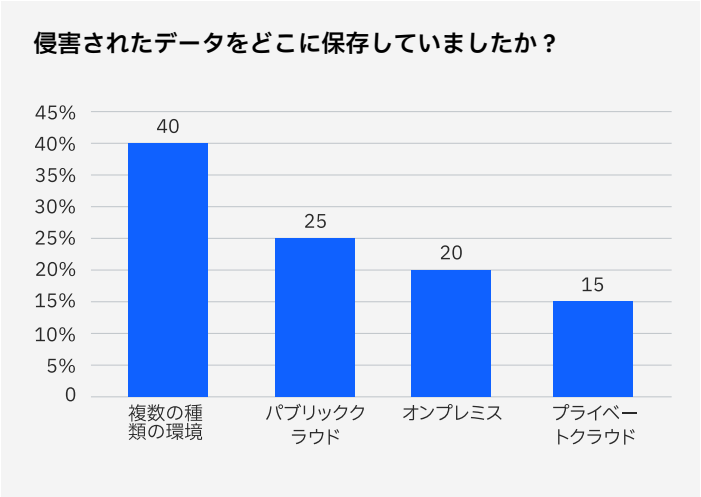


図37：全組織に占める割合。単一回答のみ

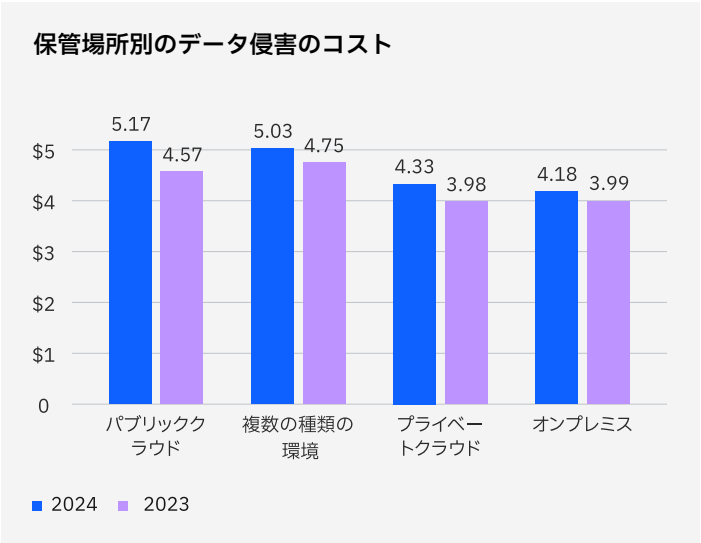


図38：単位は百万米ドル

データ・セキュリティー

データの保管場所に関係なく、データは侵害に対して脆弱になる可能性があります。今年の調査では、場所によってはより脆弱になり、侵害1件あたりのコストが高くなることが示されています。ほとんどの侵害は、複数の環境またはパブリッククラウドに分散されたデータに関係していました。どちらのストレージ・オプションも、侵害ライフサイクルの長期化と侵害コストの上昇を伴っていました。

組織がデータ管理戦略を拡大し、洗練させても、シャドー・データ（管理されておらず、IT部門からは見えない可能性が高いデータ）を見過ごすことはよくあります。これは、従業員が不正なアプリケーションを通じてデータを共有したり、非公式なクラウド・バケットにデータをアップロードしたりした結果である可能性があります。レポートによると、シャドー・データが関与する侵害は、より長期に及び、より大きなコストにつながることがわかりました。

クラウド侵害

データの場所別の侵害
全侵害の約40%は、パブリッククラウドやプライベートクラウド、オンプレミスなど、複数の環境に分散されたデータが関与していました。この調査では、パブリッククラウドやプライベートクラウド、オンプレミスのいずれかのみに保管されたデータが関与する侵害はほとんどありませんでした。データが環境間でより動的になり、アクティブになるにつれて、発見・分類・追跡およびセキュリティーの確保が難しくなっています。図37を参照してください。

場所別およびコスト別の侵害
パブリッククラウドのみが関与するデータ侵害が最もコストが高く、平均517万米ドルかかり、昨年から13.1%増加しました。複数の環境が関与する侵害は、パブリッククラウドが関与する侵害より一般的であるものの、コストはわずかに低くなっています。コストが最も低かったのは、オンプレミスの侵害でした。
図38を参照してください。

527万米ドル

シャドー・データが関与するデータ侵害の平均コスト。

迅速な修復に関連する一元管理
組織がデータをより一元的に管理すればするほど、侵害を平均してより迅速に特定し、封じ込めることができます。オンプレミスにのみ保管されているデータが関連する侵害の特定と封じ込めに要した日数は平均224日で、複数の環境に分散して保管されているデータの場合の283日より23.3%短くなりました。プライベートクラウド・アーキテクチャーとパブリッククラウド・アーキテクチャーを比較しても、ローカル管理と侵害ライフサイクルの短縮という同じパターンが見られました。図39を参照してください。

シャドー・データ

シャドー・データの侵害コスト
シャドー・データが関与するデータ侵害の平均コストは527万米ドルで、シャドー・データが関与しない場合の平均コストより16.2%高くなりました。図40を参照してください。

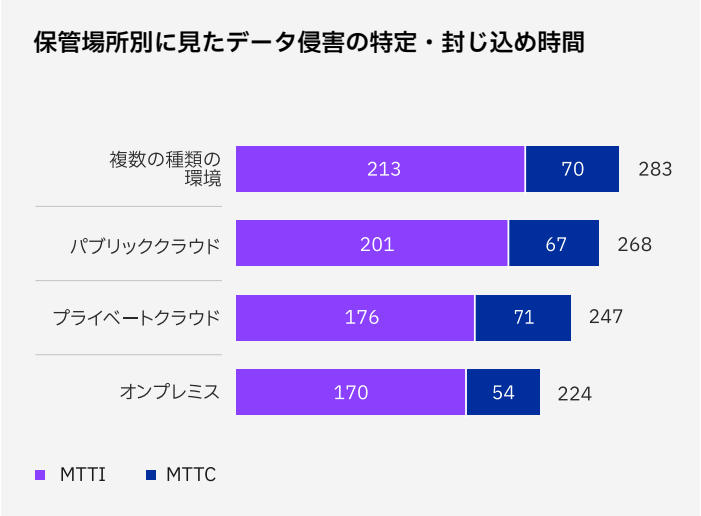


図39：単位は日数

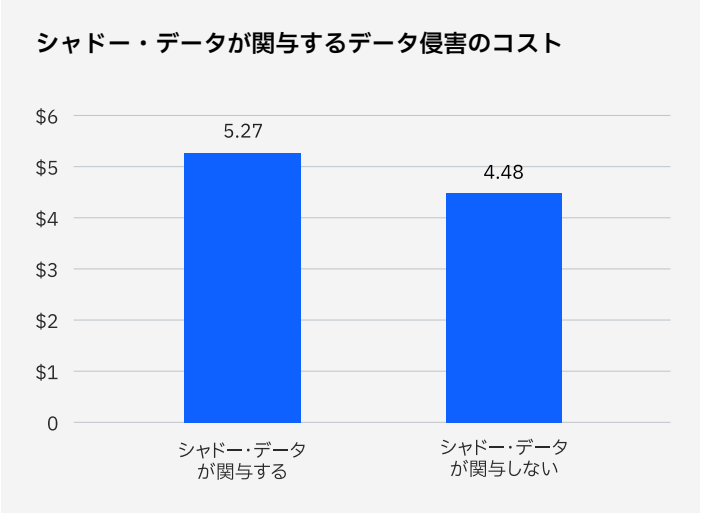


図40：単位は百万米ドル

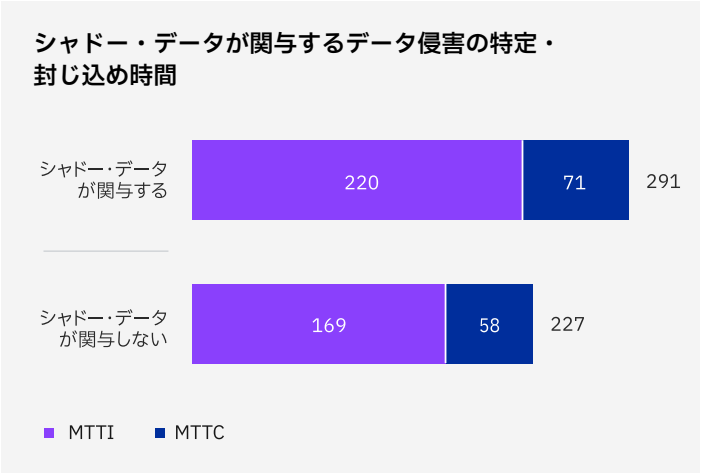


図41：単位は日数

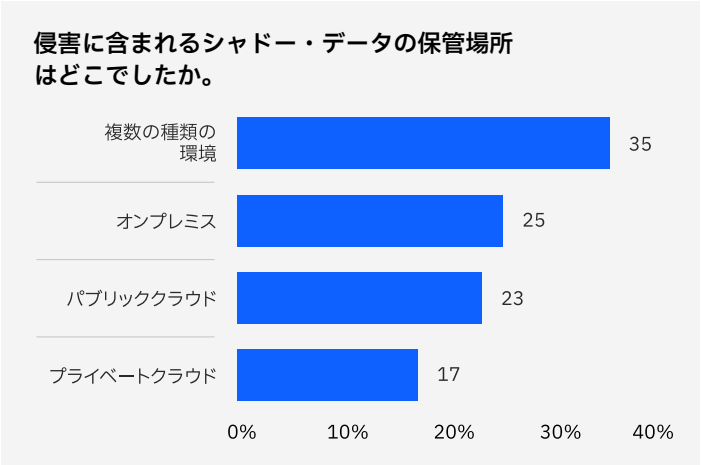
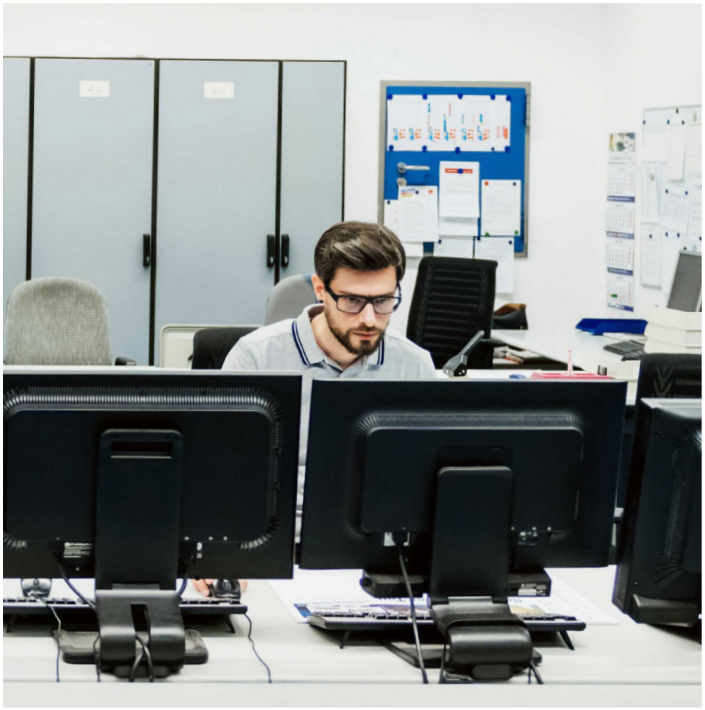


図42：シャドー・データが関与する侵害の割合。単一回答のみ

シャドー・データの侵害ライフサイクル
シャドー・データが関与する侵害は、そうでないものに比べ、特定に平均26.2%、封じ込めに平均20.2%長くかかりました。その結果、データ侵害の平均ライフサイクルは291日となり、シャドー・データが関与しないデータ侵害よりも24.7%長くなりました。図41を参照してください。

あらゆる環境に存在するシャドー・データ
シャドー・データは、パブリッククラウドやプライベートクラウド、オンプレミス、複数環境など、あらゆるタイプの環境で見られましたが、シャドー・データが関与する侵害の25%はオンプレミスでのみ発生していました。この結果は、シャドー・データが厳密にはクラウド・ストレージに関連する問題ではないことを意味します。図42を参照してください。



大規模侵害

侵害されるレコードが100万件を超えるような大規模な侵害は比較的まれです。従って、この調査ではそれらを他のほとんどのデータ侵害とは区別して扱っています。それは、1つには典型的なデータ侵害の分析に歪みを与えないようにするためです。

大規模侵害のコストが増加
あらゆる大規模侵害カテゴリーの平均コストは、昨年より高くなりました。この急増は、5,000万～6,000万件のレコードに影響を与えた最大規模の侵害で最も顕著に現れました。平均コストは13%増加し、これらの侵害は一般的な侵害よりも何倍も高額でした。100万件～1,000万件のレコードという最小クラスの大規模侵害であっても、平均コストは世界平均の9倍近い488万米ドルに上りました。図43を参照してください。

喪失したレコード件数別大規模のデータ侵害によるコスト

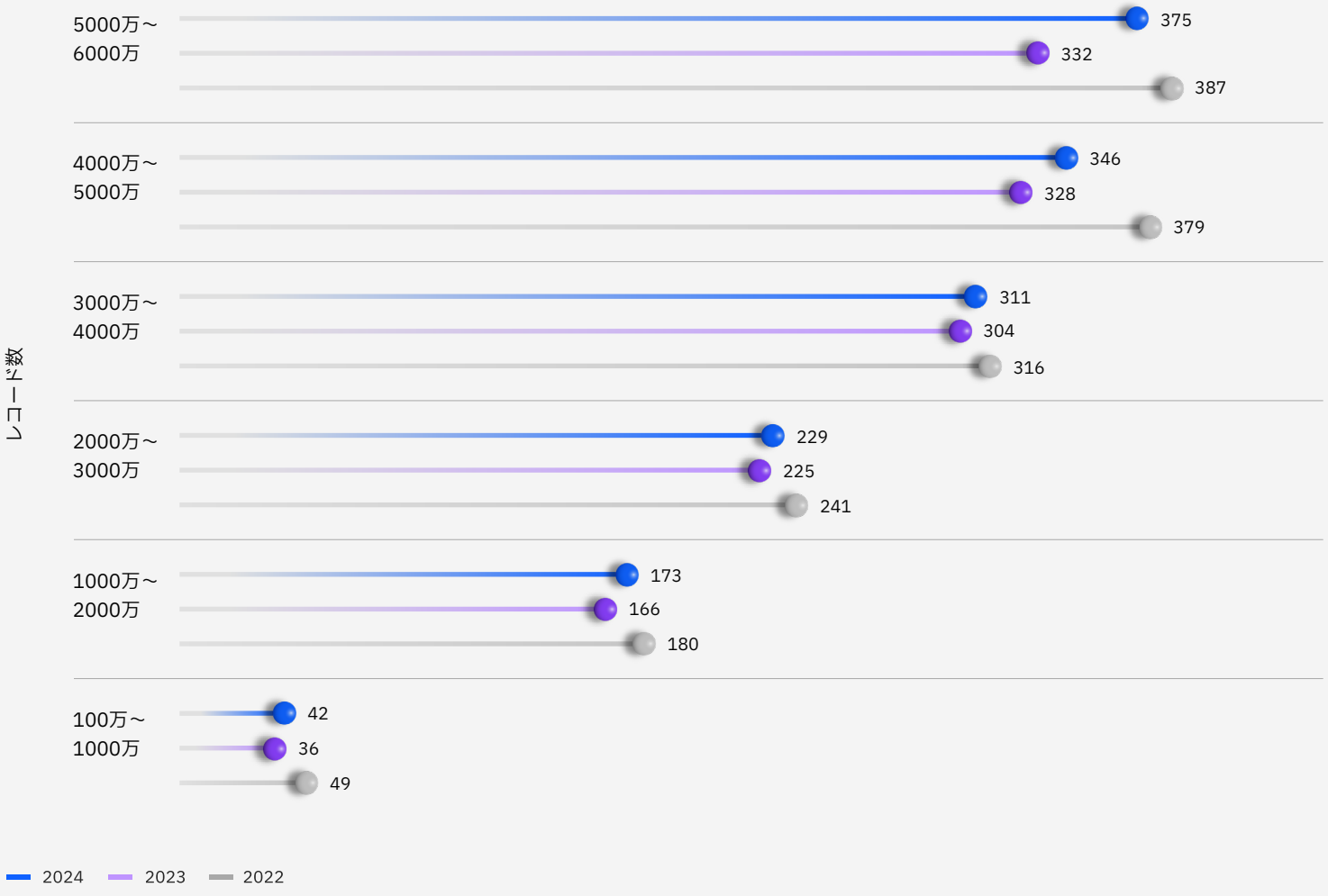


図43：単位は百万米ドル

↑ 23.5%

侵害の発生後、セキュリティー投資の増加を計画している組織の割合の増加。

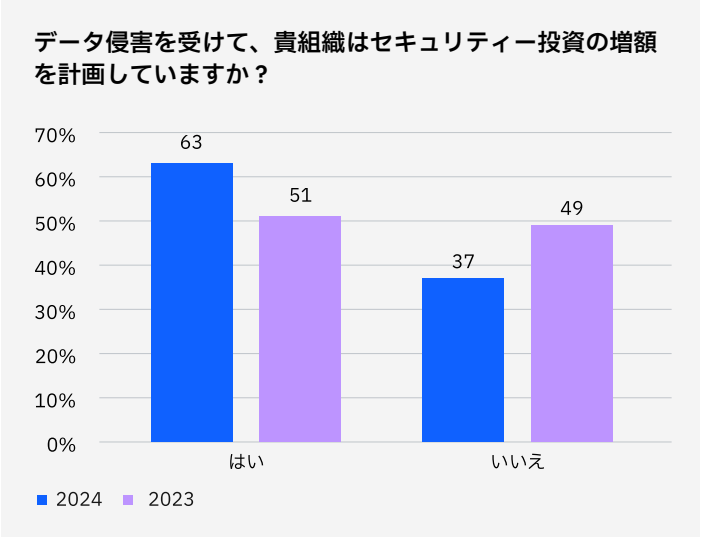


図44：全組織に占める割合

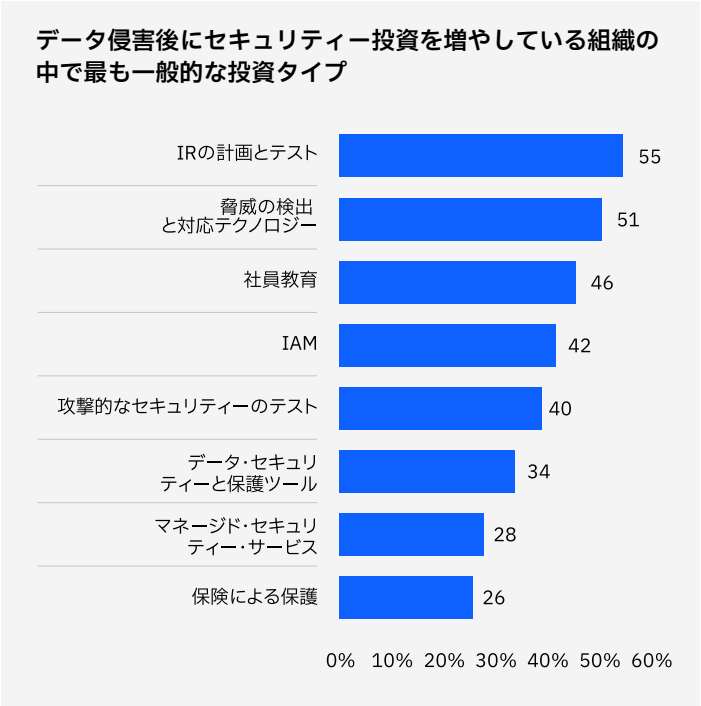


図45：セキュリティー投資を増やしている組織に占める割合。複数回答可

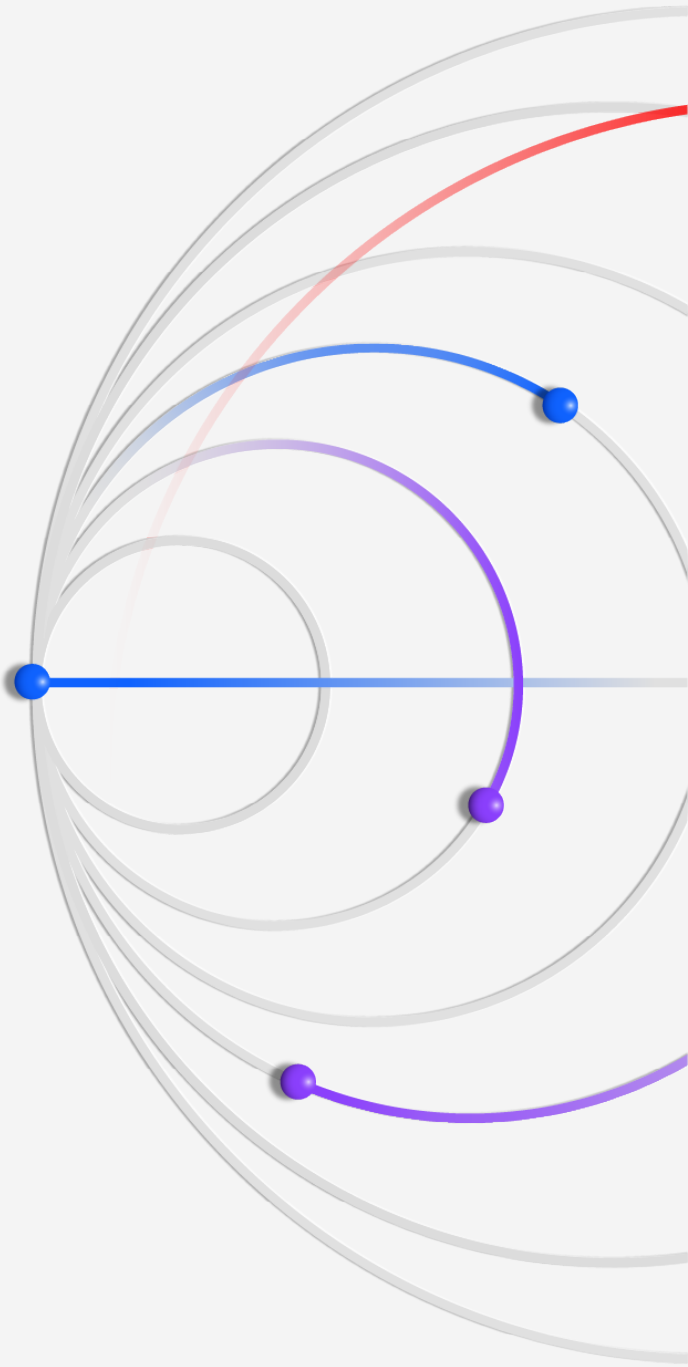
セキュリティー投資

組織が侵害を受けると、そのビジネス・リーダーやITリーダーがセキュリティー投資を増やすことがよくあります。今年の調査では、各組織に今後のセキュリティー支出計画について尋ねました。投資分野を複数特定することが可能でした。

セキュリティー投資を行う組織の割合が上昇
約3分の2の組織が、侵害後にセキュリティー投資を増やすことを計画しており、これは昨年より23.5%増加しました。この増加は、事業損失や規制上の罰金に関連する違反コストが、風評被害の可能性と併せて増加し続けるという認識を反映していると考えられます。図44を参照してください。

セキュリティー投資の人気分野
今年報告されたセキュリティー投資で最も人気の高かった2つの分野は、IR計画とテストで55%、脅威の検知と対応テクノロジーで51%でした。上位2つの投資分野は、不審なインシデントや脅威を検知し、より迅速に対応することに焦点を当てています。また、データ・セキュリティーと保護ツールへの投資を計画している組織は34%、IAMへの投資を計画している組織は42%でした。図45を参照してください。

データ侵害のコストを削減するのに役立つ推奨事項



推奨事項には、コストを削減し、侵害ライフサイクルの短縮に役立つ、実績あるセキュリティー・アプローチが含まれます。

情報の状況を把握する

ほとんどの組織は、オンプレミスのデータ・リポジトリー、プライベートクラウド、パブリッククラウドなど、複数の環境にデータを分散させています。しかし、多くの組織では、データ・インベントリーが不完全であったり、古かったりするため、侵害されたデータとその機密性や秘密度を発見する取り組みが遅れています。このような遅れは、対応を複雑にし、侵害のコストを引き上げる可能性があります。

セキュリティー・チームは、これらすべての環境を包括的に可視化し、データの保管場所に関係なく、継続的にデータを監視および保護できるようにする必要があります。組織は、一貫性のある包括的な保護を実現するために、データ・セキュリティー・ポスチャー管理（DSPM）や、アイデンティティー・アクセス管理、ASMなどのその他のソリューションを、これらすべての環境に適用することができます。

セキュリティー・チームは、ハイブリッド環境とパブリッククラウドに特に注意を払う必要があります。データ侵害の40%は複数の環境にまたがって保存されたデータに関連しており、侵害されたデータがパブリッククラウドに保存されていた場合、平均侵害コストは517万米ドルと最も高くなりました。セキュリティー・チームは、採用するクラウド・サービスごとの具体的なリスクと管理をより深く理解することが不可欠です。

複数の環境にまたがってデータを管理することは、管理されていないデータの影響によってさらに複雑になります。データ侵害の3分の1以上にはシャドー・データが関係しています。現在、セキュリティー・チームは、組織が管理されていないデータ・ソースを持っていることを想定しておく必要があります。AIワークロードのデータを含めて、暗号化されていないデータにより、リスクはさらに増えます。データ暗号化戦略は、侵害発生時のリスクを低減するために、データの種類、使用方法、およびデータの保管場所を考慮する必要があります。

AIと自動化で予防戦略を強化

組織全体での生成AIモデルやサードパーティー・アプリケーションの導入、およびモノのインターネット（IoT）デバイスやSaaSアプリケーションの継続的な利用により、攻撃対象領域が拡大し、セキュリティー・チームにプレッシャーを与えています。

ASM、レッド・チーミング、ポスチャー管理の分野を含め、セキュリティー予防戦略をサポートするAIと自動化の適用は、多くの場合、マネージド・セキュリティー・サービスで対応できます。今年の調査では、AIと自動化をセキュリティー予防に適用した組織が、他の3つのセキュリティー領域（検知、調査、対応）と比較して、AIへの投資による効果が最も大きかったことがわかりました。予防テクノロジーにAIを導入しなかった組織に比べ、平均222万米ドルのコスト削減になりました。

セキュリティー・ファーストのアプローチで生成AIを導入

組織は生成AIを急速に進めていますが、生成AIイニシアチブは24%しか保護されていません。セキュリティーが不十分だと、データやデータ・モデルが侵害される恐れがあり、生成AIプロジェクトが意図するメリットが損なわれる可能性があります。

生成AIの導入が拡大し続ける中で、組織は生成AIのデータ、モデル、使用を保護するためのフレームワークを必要としており、併せてAIガバナンス統制を確立する必要があります。トレーニング・データを盗難や不正操作から保護することで、安全性を確保する必要があります。組織は、データ検出と分類を使用して、トレーニングやファイン・チューニングに使用された機密データを検知できます。また、暗号化、アクセス管理、コンプライアンス監視を通して、データ・セキュリティー・コントロールを実装することもできます。

生成AIにより、組織はシャドー・データのリスクや増加だけでなく、シャドー・モデルにも対応しています。組織は、機密性の高いAIトレーニング・データを保護し、未承認またはシャドーAIモデルの使用を可視化し、AIの誤用やデータ漏えいを防止するために、AIモデル自体にもポスチャー管理を拡張する必要があります。

生成AIモデル開発の安全性を確保するには、パイプラインの脆弱性をスキャンし、統合を強化し、ポリシーとアクセスを適用する必要があります。生成AIモデルを安全に使用するためには、セキュリティー・チームがプロンプト・インジェクションのような悪意のある入力や、機密データを含む出力を監視する必要があります。また、データ汚染、モデル回避、モデル窃取などのAI固有の攻撃を検知して対応できるAIセキュリティー・ソリューションを導入する必要があります。アクセスを拒否し、侵害されたモデルを隔離して切断するための対応プレイブックを作成することも不可欠です。

生成AIやその他のITイニシアチブのために脅威ランドスケープが拡大する中で、AIチームで働くデータサイエンティストやデータ・エンジニアなど、セキュリティー専門家以外の実務者にセキュリティー・トレーニングを提供する必要があります。

サイバー対応トレーニングのレベル・アップ

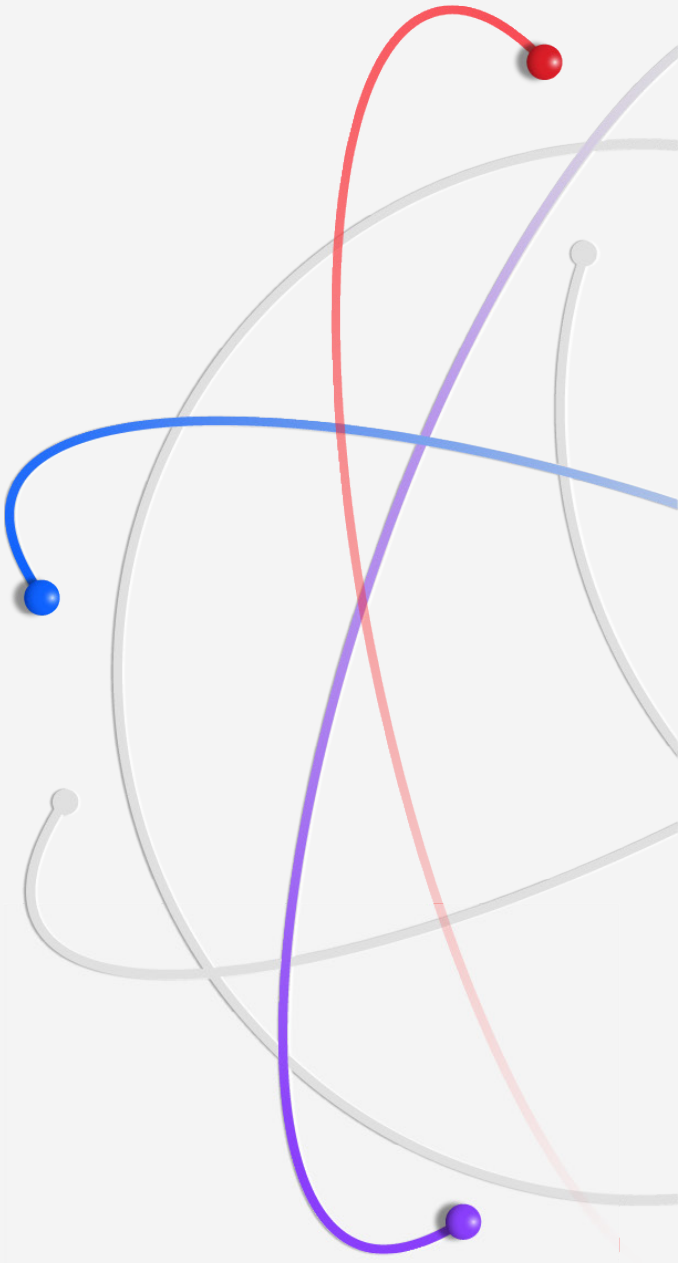
侵害の発生時および発生後に、ビジネス・リーダーや規制当局および顧客に対して組織がどのように対応し、どのようにコミュニケーションを取るかがこれまで以上に重要となっています。影響の大きい攻撃への対処能力を強化するために、組織はサイバーレンジ危機シミュレーション演習に参加することで、侵害対応のマッスル・メモリーを強化することができます。

このような演習には、セキュリティー・チームだけでなくビジネス・リーダーも参加できるため、組織全体の侵害の検知・封じ込め・対応能力が向上します。セキュリティー・リーダーは、事前に組織全体のビジネス部門やコミュニケーション・チームと協力して、対応計画を立案し、それをテスト必要があります。生成AIやその他のITイニシアチブのために脅威ランドスケープが拡大する中で、セキュリティー専門家以外の実務者にセキュリティー・トレーニングを提供する必要があります。このような実務者には、機械学習やAIのチームで働くデータ・サイエンティストやデータ・エンジニア、オンプレミスやクラウド資産にまたがるAIワークロードの継続的な実行を担当する人々が含まれます。

対応準備に投資することで、組織はデータ侵害によるコストのかかる破壊的影響を軽減し、事業の継続をサポートし、顧客やパートナー、その他の重要な利害関係者との関係を維持することができます。さらに、対応をリハーサルしておくことは、従業員の安心につながります。それだけでなく、用意周到なリーダーシップ・チームによって攻撃の急性期が処理、制御、伝達されるため、社内のストレス、苦痛、摩擦が軽減されます。

組織の人口統計

今年は、16の国または地域で、17業種にわたるさまざまな規模の604組織を対象に調査を実施しました。このセクションでは、調査対象の組織を国・地域別、業種別に分析し、業種の分類の定義を明確にします。



地域別人口統計

2024年の調査は、16の国または地域で実施されました。今年、調査に追加された新しい地域の1つは、ベルギー、オランダ、ルクセンブルクの経済連合であるベネルクスです。スカンジナビアは調査から除外されました。

ASEANは、シンガポール、インドネシア、フィリピン、マレーシア、タイ、ベトナムにある組織のクラスター・サンプルです。ラテン・アメリカは、メキシコ、アルゼンチン、チリ、コロンビアにある組織のクラスター・サンプルです。中東は、サウジアラビアおよびアラブ首長国連邦にある組織のクラスター・サンプルです。

グローバル調査の概要

国および地域	2024年のサンプル	全サンプルに占める割合（%）	調査期間（年）	通貨
ASEAN	25	4%	8	シンガポール・ドル（SGD）
オーストラリア	27	4%	15	オーストラリア・ドル（AUD）
ベネルクス	32	5%	1	ユーロ（EUR）
ブラジル	45	7%	12	ブラジル・レアル (BRL)
カナダ	28	5%	10	カナダ・ドル（CAD）
フランス	36	6%	15	ユーロ（EUR）
ドイツ	47	8%	16	ユーロ（EUR）
インド	53	9%	13	インド・ルピー（INR）
イタリア	29	5%	13	ユーロ（EUR）
日本	42	7%	13	円（JPY）
ラテンアメリカ	28	5%	5	メキシコ・ペソ（MXN）
中東	39	6%	11	サウジアラビア・リヤル（SAR）
南アフリカ共和国	24	4%	9	南アフリカ・ランド（ZAR）
韓国	28	5%	7	ウォン（KRW）
イギリス	50	8%	17	英ポンド（GBP）
アメリカ合衆国	71	12%	19	米ドル（USD）
合計	604	100%		

図46：調査対象の全組織に占める割合

業種別人口統計

選別された17種類の業種は、複数年にわたり、本調査の対象となっていた業種です。今年は、金融、製造業、専門サービス、テクノロジーの上位4業種が、調査対象となった604の組織の47%を占めました。

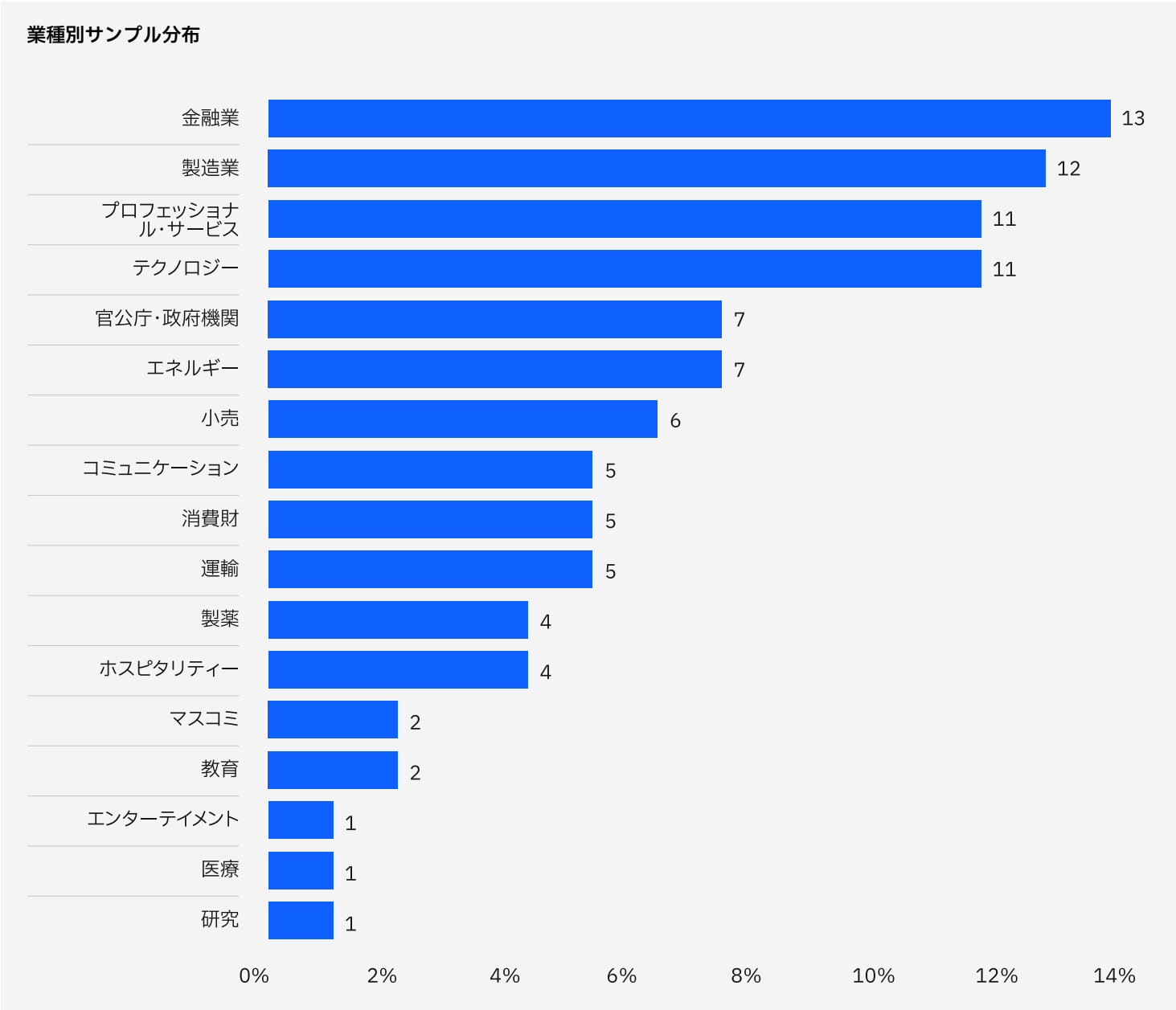


図47：調査対象の全組織に占める割合

業種の定義

医療
病院および診療所

金融業
銀行、保険、投資会社

エネルギー
石油・ガス会社、公益産業、代替エネルギー生産者
および供給業者

製薬業
製薬（バイオメディカル・ライフサイエンスを含む）

製造業
化学品処理、エンジニアリング、製造

テクノロジー
ソフトウェアおよびハードウェア

教育
公立および私立の大学、研修・人材育成

プロフェッショナル・サービス
法律、会計、コンサルティングなど、各種専門サービス

エンターテイメント
映画制作、スポーツ、ゲーム、カジノ

運輸
航空、鉄道、トラック輸送、運送

通信
新聞、出版、広報、広告業

消費財
消費者商品のメーカーおよび流通業者

マスコミ
テレビ、衛星、ソーシャルメディア、インターネット

ホスピタリティー
ホテル、レストラン・チェーン、クルーズ客船

小売
従来型ストアおよびeコマース

研究
市場調査、シンクタンク、研究開発

官公庁・政府機関
国、都道府県、地方自治体の政府機関および非政府組織

調査方法

秘密保持のため、このベンチマーク手法では組織固有の情報を一切収集していません。データを収集する際には、具体的な会計情報は含めず、回答者が数直線上の数値範囲に印をつけることにより概算された直接コストを使用しました。参加者は、各コスト・カテゴリーで、数直線の下限から上限の間の1箇所に印をつけるように指示されました。

秘密を保持し、高い回答率を確保するため、各コスト・カテゴリーでは、具体的な概算値を使用する代わりに、数直線上の数値を選択していただく方法を採用しました。また、このベンチマーク手法では、間接費と機会費用に対する推定値も別途提出するよう回答者に求めました。

ベンチマーク用に管理しやすいデータ・セットを維持するため、本レポートではデータ侵害コストに重大な影響を与える主要なコスト・アクティビティーのみを対象としています。その選別に際しては、専門家に相談し、一定のコスト・アクティビティーが選ばれました。ベンチマーク情報を収集した後、一貫性と完全性を保つため、各測定方法は慎重に再検討されました。

データ侵害コスト要因の範囲は、個人情報に関わる広範な業務に適用される既知のカテゴリーに限定されました。プロセス調査の方がより質の高い結果が得られると考えた上で、データ保護やプライバシー遵守の取り組みではなく、ビジネス・プロセスに焦点が当てられています。

データ侵害コストの計算方法

データ侵害の平均コストを計算する際は、非常に小さい侵害と非常に大きい侵害を除外しました。2024年版レポートの調査対象となったデータ侵害の規模は、侵害を受けたレコードの件数が2,100件～11万3,000件に及びました。大規模データ侵害のコストについては、別の分析方法を用いました。その方法論については、本レポートの「データ侵害FAQ」セクションをご覧ください。

アクティビティーを特定し、実際の使用に応じてコストを分類する活動基準原価計算法が採用されました。組織のデータ侵害にかかる各種コストに影響するプロセス関連アクティビティーは、検知およびエスカレーション、通知、侵害後の対応、機会損失の4つです。

検知およびエスカレーション
組織によるデータ侵害の検知を可能にするアクティビティーには、以下のようなものがあります。

– 犯罪調査およびその他の調査活動
– 評価および監査サービス
– 危機管理
– 役員や幹部職員への報告

通知
組織がデータ対象者やデータ保護規制当局、その他の第三者への通知を行えるようにするアクティビティーには、以下のようなものがあります。

– データ主体へのメール、手紙、外部への電話、または一般的な通知手段
– 規制要件の特定
– 規制者との連絡
– 外部専門家への相談

侵害後対応
データ侵害の被害者が組織と連絡を取り合い、被害者や規制当局に対して救済活動を行うためのアクティビティーには、以下のようなものがあります。

– ヘルプデスクおよび外部からの連絡
– クレジット・モニタリングサービスおよびID保護サービス
– 新規アカウントまたはクレジットカードの発行
– 法的費用
– 製品値引き
– 規制当局により科される罰金

機会損失
顧客の喪失や業務の中断、利益損失の最小化を試みるアクティビティーには、以下のようなものがあります。

– システムのダウンタイムによる事業の中断と収益の損失
– 顧客の喪失および新規顧客獲得のコスト
– 風評被害および信用低下

データ侵害FAQ

データ侵害とは何ですか？
データ侵害は、PIIを含むレコードが漏洩するイベントとして定義されます。金融口座または医療口座の詳細、その他の機密データ、または専有データが攻撃対象となる可能性があります。これらのレコードは電子形式の場合も、紙の場合もあります。本調査の対象となった侵害で、侵害を受けたレコードの件数は2,100～113,000件に及びました。

侵害されたレコードとは？
レコードとは、企業や官公庁・政府機関、または金融関連の機密または専有データを暴露する情報、またはデータ侵害で情報が紛失または盗難された個人を特定する情報のことです。たとえば、個人の名前、クレジットカード情報、その他のPIIが含まれるデータベース、または保険契約者の名前と支払い情報が含まれる健康記録などが含まれます。

データはどのように収集しましたか？
2023年3月から2024年2月の間にデータ侵害を受けた604の組織の3,556人の個人との個別インタビューにより、当社の調査員が詳細な定性的データを収集しました。インタビュー対象者は、組織のデータ侵害や侵害の解決に関連するコストに精通している方々です。その中には、CEO（最高経営責任者）や経営幹部、業務部長、経理担当管理者または財務部長、IT担当者、事業部門リーダーやゼネラル・マネージャー、リスク管理およびサイバーセキュリティー担当者が含まれます。プライバシー保護のため、組織固有の情報は収集していません。

データ侵害のコストには含まれる内容
組織にかかった直接費および間接費の両方の情報を収集しました。直接費には、犯罪調査の専門家の雇用やホットライン・サポートのアウトソーシング、クレジット・モニタリング・サブスクリプションの無料提供、将来の製品およびサービスの値下げが含まれます。間接費には、社内調査とコミュニケーション、ターンオーバーや顧客獲得率の低下による顧客喪失の推定価値が含まれます。

本調査は、データ侵害に直接関連するイベントだけを対象としています。一般データ保護規則（GDPR）やCalifornia Consumer Privacy Act（CCPA、カリフォルニア州消費者プライバシー法）などの規制により、組織がサイバーセキュリティー管理技術への投資を増加させることが推奨されている場合がありますが、本調査では、そのような活動とデータ侵害コストの間の直接的な関係は明確化されませんでした。前年との一貫性を維持するため、会計コストを調整するのではなく、同じ通貨換算法を使用しました。

ベンチマーク調査はアンケート調査とどう違いますか？
データ侵害のコストに関する調査における分析単位は組織です。アンケート調査では、分析単位は個人です。当社は、この研究に参加する604の組織を募集しました。

レコード1件あたりの平均コストは、数百万件のレコードが喪失または盗難にあった侵害のコスト計算に使用できますか？
合計数百万件のレコードが影響を受けた単一または複数のデータ侵害インシデントのコストを計算するために、レコード1件あたりの総コストを使用することは、本レポートの調査方法に合致していません。レコード1件あたりのコストは、各イベントで影響を受けたレコードが11万3,000件以下であった、数百件のデータ侵害インシデントの調査から導き出されています。100万件以上のレコードが影響を受けた大規模なデータ侵害の影響を測定するために、本調査では代わりに、当該規模の17件のイベントのサンプリングに基づくシミュレーション・フレームワークを使用しています。

大規模なデータ侵害のコスト推定にシミュレーション方式を使用した理由は？
大規模なデータ侵害を受けた17組織のサンプル・サイズは、調査のアクティビティー・ベースのコスト手法を使用して統計的に有意な分析を行うのに十分な大きさではありませんでした。この問題を改善するためにモンテカルロ・シミュレーションを採用し、繰り返し実行することにより、不確実な事象の起こり得る結果の範囲を推定しました。合計で26万9000回以上試行しました。全サンプル平均の総平均は、100万～5300万件の影響を受けたレコードまで、データ侵害の規模ごとに最も可能性の高い結果を示しました。

毎年同じ組織を追跡しているのですか？
毎年行われる調査には、毎回異なるサンプル組織が関わっています。前年のレポートと一貫性を保つために、毎年、組織の業界や人数、地理的分布、データ侵害の規模など同じような特性を持つ組織を募集し調整しています。2005年にこの調査を開始してから、6,184の組織のデータ侵害の経験を調査してきました。

調査の限界

本調査でも、これまでの調査で優れた成果をもたらしてきた部外秘の独自ベンチマーク手法を使用しました。しかし、調査結果から結論を導き出す前に、このベンチマーク調査固有の限界について慎重に検討する必要があります。

非統計的な結果
本調査は、世界的な事業体の代表的かつ非統計的なサンプルを使用しています。サンプリング方法が科学的ではないため、統計的推論、誤差、信頼区間はそれらのデータには適用できません。

無対応
非回答バイアスについてはテストしていません。そのため、参加しなかった組織が、潜在的なデータ侵害コストの点で大きく異なる可能性があります。

サンプリング・フレーム・バイアス
当社のサンプリング・フレームは判断に基づくものであるため、結果の質は、そのフレームが調査対象の組織の母集団をどの程度表しているかに影響されます。現在のサンプリング・フレームは、より成熟したプライバシーまたは情報セキュリティー・プログラムを持つ組織に偏っていたと考えています。

組織固有の情報
このベンチマークでは組織を特定する情報は収集していません。個人はカテゴリー応答変数を使用して、組織や業種カテゴリーの人口統計情報の開示が可能でした。

未測定の要因
主要なトレンドや組織の特性などの変数は分析から除外しました。除外した変数がベンチマークの結果にどの程度影響を及ぼしうるかは特定できません。

コストの推定結果
確認作業や調整作業をベンチマーク・プロセスにある程度組み込むことはできますが、回答者が正確で正直な回答をしない可能性は常にあります。また、実際のコスト・データの代わりにコスト推定方法を使用したことにより、意図せず偏りや不正確さが加味される可能性があります。

通貨換算
地域通貨から米ドルに換算したことにより、他国での平均総コスト推定額が過小評価されることがあるため、前年との一貫性を保つ目的で、コストを調整するのではなく、同じ計算方法を使用することにしました。すべての国レベルでの結果は現地通貨で表示されるため、この問題はグローバル分析にのみ影響する可能性があることに注意してください。この調査レポートで使用されている実質為替レートは、2024年3月4日に連邦準備制度理事会が公表したものです。

IBMおよびPonemon Instituteについて

IBM

IBMは、ハイブリッドクラウド、AI、およびビジネス・サービスの世界的なリーディング・プロバイダーであり、175カ国以上のお客様がデータからの洞察を活用し、ビジネス・プロセスを合理化し、コストを削減し、各業界で競争力を獲得できるよう支援しています。これらすべては、信頼性、透明性、責任、包括性、サービスに対するIBMのコミットメントによって裏付けられています。詳細については、www.ibm.com/jp-jaをご覧ください。

セキュリティー体制の強化に関する詳細はこちら：

ibm.com/jp-ja/security

IBM Security Communityで対話に参加することもできます

ポネモン・インスティテュート

2002年設立の米調査会社Ponemon Instituteは、独立した調査と、組織および政府で責任のある情報およびプライバシー管理手法を促進する教育に取り組んでいます。同社のミッションは、人と組織の機密情報の管理とセキュリティーに影響する重要な課題についての、質の高い実証研究を行うことです。

Ponemon Instituteは厳格なデータ機密保持、プライバシーおよび倫理的調査基準を支持し、事業調査の中で個人または企業の特定可能な情報から個人情報（PII）を収集しません。また、厳格な品質基準により、調査対象者が本質的でない無関係のまたは不適切な質問をされることはありません。

レポートの引用や複製許可依頼を含む、この調査レポートについてのご質問やコメントは、手紙、電話、 または電子メールでお問い合わせください。

Ponemon Institute LLC
Research Department
1-800-887-3118
research@ponemon.org

日本アイ・ビー・エム株式会社
〒105-5531
東京都港区虎ノ門二丁目6番1号
虎ノ門ヒルズ ステーションタワー
IBM Corporation
New Orchard Road
Armonk, NY 10504
2024年7月