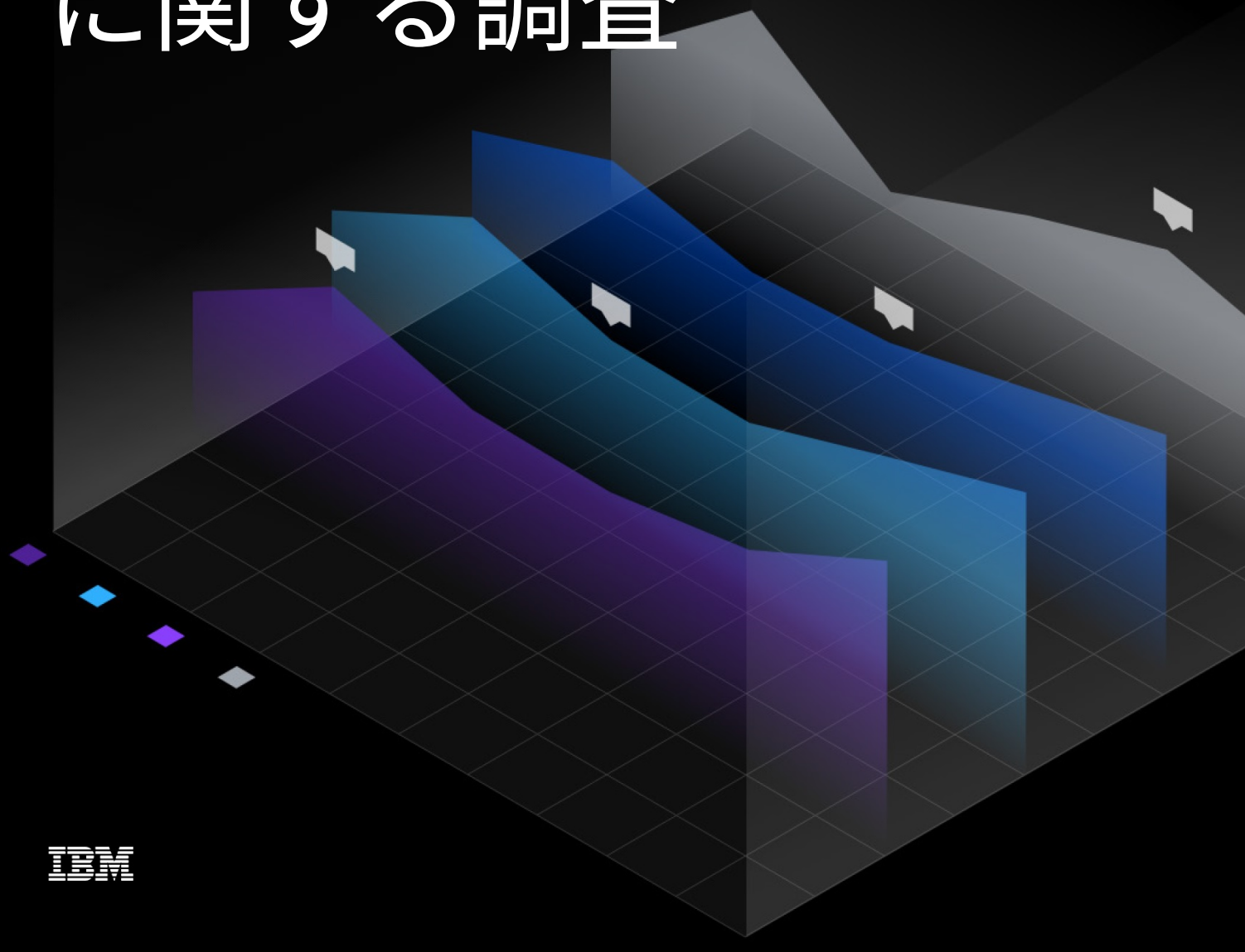
IBM Security

2020 年

情報漏えい時に発生するコストに関する調査



IBM

目次

エグゼクティブ・サマリー

Ponemon Institute が「情報漏えい時に発生するコストに関する調査」を開始してから今回で 15 年目になります。そのうちの 5 年間は、IBM Security がスポンサーとして調査結果を発行しています。情報漏えいやサイバーセキュリティー・インシデントは、あらゆる種類や規模の企業にとってリスクとなっています。そうした時代にあって、企業がイノベーションを推進し、顧客の信頼を維持するためにこの調査が役立つことを願っています。

本レポートは、サイバーセキュリティー業界の主要なベンチマーク・ツールの 1 つになっています。IT、リスク管理、およびセキュリティーのリーダーはこの調査を活用して、情報漏えいのコストの軽減や、増大要因の把握に役立てています。本レポートではまた、数年間に及ぶ分析から得られたコストの一貫性と変動の両方を示しながら、情報漏えいの傾向を紹介します。

「2020 年 情報漏えい時に発生するコストに関する調査」は、2019 年 8 月から 2020 年 4 月までに情報漏えいの被害に遭った 524 社からの聞き取り調査に基づいています。調査が多種多様な企業を網羅するように、17 の国と地域と 17 の業種に及ぶさまざまな規模の企業を対象としています。調査担当者は、企業内の情報漏えいインシデントについて知識のある 3,200 人以上の個人に聞き取り調査を行いました。

情報漏えい時に発生するコストに関する調査で判明した事実

524
漏えいの被害に遭った企業

3,200
聞き取り調査を行った人数

17
調査対象の国や地域

17
調査対象の業種

*本レポートに記載する年は、発表時の年を示しており、漏えいが発生した年とは限りません。2020 年の調査で分析された情報漏えいは、2019 年 8 月から 2020 年 4 月までに発生したものです。

聞き取りでは、企業が情報漏えいを発見し即座に対応するために何を実施したかを明らかにするために、数多くの質問を行いました。コストに影響を与えた可能性がある問題として、情報漏えいの根本原因、企業がインシデントの検知と拡大防止にかかった時間、および漏えいの結果として生じたビジネスの中断と顧客の喪失にかかる推定コストについても調査しました。漏えいが発生する前に実装されたセキュリティー対策や、企業とその IT 環境の特徴など、他の多くのコスト要因を調査しました。

その結果、膨大なデータ、広範な分析、および傾向の洞察を扱ったレポートが完成しました。このエグゼクティブ・サマリーの後では、情報漏えいのコストの計算方法と、この調査の主な結果について、簡単に説明しています。データの詳細については、「調査結果完全版」に分析および属性情報を 49 のグラフで説明しています。

IT リーダー、サイバーセキュリティー戦略家、およびリスク管理担当者向けに、情報漏えいがもたらす財務およびブランドへの潜在的な損害を軽減するための、最も効果的なセキュリティー対策を、調査結果に基づいて推奨しています。そして、レポートの最後では調査方法について詳しく説明します。

2020 年の最新情報

レポートを毎年更新する目的は、過去のレポートに基づく分析を提供し、テクノロジーと傾向の変化に後れを取らずに新しい分野を開拓することです。これにより、リスクとデータ保護の基準をより明確にすることができます。

2020 年は非常に重大な年になりました。テクノロジーと脅威の周期的な変化に加えて、世界的なパンデミックは世界中の企業と消費者の生活に大混乱をもたらしました。

この調査が開始されたのは、新型コロナウイルス感染症の拡大が広範な影響を与える数カ月前で、調査対象のほとんどの漏えいインシデントが既に発生した後のことでした。しかし、調査では、パンデミックによるリモートワークへの影響についても補足的な調査を行いました。大多数の企業（76%）が、リモートワークにより、潜在的な情報漏えいへの対応がはるかに困難な課題になると予測していました。

今年のレポートで導入された新しい調査では、情報漏えいのレコード 1 件当たりのコストや情報漏えいの根本的な原因など、長年調査してきたデータのタイプをより深く掘り下げています。この調査では、被害レコード 1 件当たりのコストを初めてセグメント化して、顧客の個人情報（PII）、従業員 PII、知的財産（IP）といった流出レコードのタイプに基づくコストを調べました。情報漏えいの根本原因の分析では、資格情報の盗難から内部関係者の脅威に至るまで、悪意のある漏えいをより具体的な種類に掘り下げて調査しました。

今回の調査では、国家主体の攻撃者や金銭目的の攻撃者など、漏えいの原因と推定される脅威アクターのタイプについて、初めて参加企業に質問しました。コスト分析の結果、最もコストが高いのは、悪意のある漏えいの中で最も一般的なタイプのもの（金銭目的のサイバー犯罪者によるもの）ではないことが分かりました。

また、ランサムウェアや破壊的なマルウェア攻撃がますます一般化しているため、今年のレポートでは新しいコスト分析が追加されました。その結果、これらの悪質な攻撃の平均コストは、総合的な情報漏えい時に発生する平均コストより多額になることが判明しました。

情報漏えいの統計

386 万ドル

平均総コスト

アメリカ

平均コストが最も高い国

医療

平均コストが最も高い業種

280 日

漏えいの検知と被害拡大防止にかかる平均時間

今年の調査では、いくつかの新しいコスト要因が追加されました。これには、脆弱性検査の影響、侵入テストに敵対的アプローチを使用するレッドチーム演習の影響、それにセキュリティー・スキルの不足やリモートワーカーがコストに及ぼす影響が含まれます。分析された 25 の要因のうち、スキル不足は情報漏えいの平均コストを増加させる要因のトップ 3 に入るのは当然と考えられます。一方、レッドチーム演習は、漏えいの平均コストを軽減するコスト要因のトップ 5 にエントリーしました。

他には、最高情報セキュリティー責任者（CISO）が果たす役割と、サイバーセキュリティー保険がカバーする費用のタイプについて、新たに掘り下げた質問を行いました。

今年のレポートで、情報漏えい時に発生する平均総コストが、昨年の 392 万ドルから今年の 380 万ドルへとわずかに減少したことは注目に値します。これにより、情報漏えいコストは頭打ちになったと考える人もいるでしょう。

一方、調査によると、自動化や正式なインシデント対応チームといった先進的なセキュリティー・プロセスを採用している企業と、これらの分野でのセキュリティー体制がそれほど整えられていない企業との間では、情報漏えいのコストの差が拡大しています。

これはグローバル・レポートであり、膨大な調査データが収集されたため、調査対象となったすべての国や業種における情報漏えいコストの微妙な相違までここで取り上げることはできません。そのような理由から、IBM では ibm.com/databreach にオンライン計算とデータ・エクスプローラー・ツールを公開し、各企業が独自にカスタマイズして調査できるようにしました。

これらは、有意義な洞察を取得し、ビジネスの成功に必要なデータをより適切に保護するための結論を導き出すために活用していただけます。

情報漏えい時に発生するコストの計算方法

情報漏えいの平均コストを計算するために、この調査では、非常に小さな漏えいと非常に大きな漏えいを除外しています。2020 年は、被害レコードが 3,400 ～ 99,730 件の情報漏えいについて調査しました。非常に大きな「大規模漏えい」のコストについては、別個の分析を使用して、調査しています。 これについては、本レポートの「調査結果完全版」のセクションで詳しく説明します。

情報漏えい時に発生するコストの計算には、活動基準原価計算と呼ばれる会計手法を使用しました。この手法では、情報漏えいに伴う活動を特定し、実際に使用されたコストを割り当てます。4 つのプロセス関連活動により、情報漏えいにかかわる費用が発生します。その 4 つとは、検知とエスカレーション、通知、漏えい後の対応、および機会損失です。

本レポートで使用されている手法の詳細な説明については、調査方法のセクションを参照してください。

4 つのコスト・センターは以下のとおりです。

検知とエスカレーション

企業が漏えいを合理的に検知できるようにするための活動。

- フォレンジック活動および調査活動
- 評価サービスおよび監査サービス
- 危機管理
- 経営陣や取締役会への連絡

機会損失

顧客喪失、ビジネスの中断、減収を最小限に抑えることを目的とした活動。

- システムのダウンタイムによるビジネスの中断や減収
- 顧客喪失と新規顧客獲得のコスト
- 企業評価の低下と業務上の信用の失墜

通知

漏えい対象者、データ保護規制当局、およびその他の第三者に企業が通知できるようにするための活動。

- E メール、手紙、電話、不特定多数への情報開示
- 規制要件の決定
- 規制当局との連絡
- 外部専門家の関与

情報漏えい後の対応

漏えいの被害者が企業と連絡を取るのを支援する活動、被害者への救済活動、規制当局に対する是正活動。

- ヘルプ・デスク/問い合わせ対応
- 信用の監視と 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
- 法務の費用
- 製品の割引
- 規制要件への対応（罰金）

主な調査結果

ここで説明する主な調査結果は、Ponemon Institute が集めた調査データを IBM Security が分析した結果に基づいています。

-1.5%

2019～2020 年調査での
平均総コストの純変化

情報漏えい時に発生する平均総コストは前年比でわずかに減少したものの、多くの企業ではコストが増加。

2019 年の調査では 392 万ドルでしたが、2020 年の調査では 386 万ドルに若干減少しました。一部の最も成熟した企業や業種ではコストは非常に低いものの、セキュリティー自動化やインシデント対応プロセスなどの分野で後れを取っている企業では非常に高くなりました。同様に、紛失や盗難に遭ったレコード 1 件の平均コスト（レコード 1 件当たりのコスト）を詳細に分析すると、紛失や盗難に遭った漏えいデータのタイプに応じて、コストはさまざまに異なりました。

150 ドル

顧客 PII のレコード 1 件当たりの
平均コスト

調査対象の情報漏えいで、漏えいの頻度が最も高く、コストが最も高かったレコードのタイプは、顧客の個人情報（PII）。

漏えいの被害に遭った企業の 80% は、顧客 PII が漏えいで流出したと述べており、その他のタイプのレコードよりもはるかに多い数字になっています。紛失や盗難に遭ったレコード 1 件当たりの平均コストは、情報漏えい全体の平均は 146 ドルでしたが、顧客 PII が含まれる場合、被害レコード 1 件当たりのコストは 150 ドルでした。

悪意のある攻撃による漏えいでは、顧客 PII のレコード 1 件当たりのコストは 175 ドルに上昇しました。調査対象の漏えいの 24% で匿名化された顧客データが被害に遭っており、その平均コストはレコード 1 件当たり 143 ドルでした。これが、悪意のある攻撃による漏えいでは、レコード 1 件当たり 171 ドルに増加していました。

13 万 7,000 ドル以上

リモートワークが平均総コストに与える影響

新型コロナウイルス感染症拡大時のリモートワークにより、情報漏えいコストとインシデント対応時間の増大が予測される。

新型コロナウイルス感染症拡大の結果としてリモートワークが必要となった企業のうち、リモートワークによって情報漏えいコストが増加すると回答した企業は 70%、潜在的な情報漏えいの検知と被害拡大防止の時間が増加すると回答した企業は 76% に上りました。リモートワーカーがいる場合、情報漏えい時に発生する平均総コストの 386 万ドルが 13 万 7,000 ドル近く増加して、調整後の平均総コストは 400 万ドルに達すると分かりました。

悪意のある情報漏えいの原因のうち最も被害額が大きいのは、資格情報の盗難や流出。

悪意のある情報漏えいの被害を受けた 5 社に 1 社 (19%) は、資格情報（クレデンシャル）の盗難や流出によって外部から侵入され、漏えいの平均総コストが 477 万ドルへと 100 万ドル近くも上昇していました。全体的に見ると、悪意のある攻撃が最も頻度の高い根本原因と見なされ (調査では漏えいの 52%)、その平均総コストは 427 万ドルでした。それに対し、人的ミスは 23%、システムの欠陥は 25% でした。

+14%

クラウドの構成ミスが平均総コストに与える影響

クラウドの構成ミスは、漏えいの主な原因。

資格情報の盗難や流出に加えて、クラウド・サーバーの構成ミスは、悪意のある攻撃によって引き起こされた漏えいにおける最も頻度の高い初期脅威要因として、19% を占めています。クラウドの構成ミスによる漏えいにより、平均コストは 50 万 ドル以上増加し、441 万ドルになりました。

152 万ドル

機会損失の平均総コスト

ビジネス機会の損失は引き続き情報漏えいコストの最大要因。

機会損失コストは、情報漏えい時に発生する平均総コストの 40% 近くを占め、2019 年の調査時には 142 万ドルでしたが、2020 年の調査時には 152 万ドルに増加しました。機会損失コストには、顧客離れの増加、システムのダウンタイムによる減収、企業の評判の低下による新規ビジネス獲得コストの増加が含まれます。

358 万ドル

セキュリティー自動化なしの場合と比較した、セキュリティー自動化が全面的に導入されている場合のコスト節減額の平均

情報漏えいコストに対するセキュリティー自動化の影響は、過去 3 年間で増加。

セキュリティーの分野での自動化技術の全面的な導入とは、人工知能プラットフォームと自動化された漏えい対応オーケストレーションを使用することを指します。セキュリティー自動化が導入されている企業の割合は、2018 年には 15% でしたが、2020 年の調査では 21% に増加しました。

その間、情報漏えいの平均コストを削減する上でのセキュリティー自動化の効果は高まり続けています。セキュリティー自動化を導入していない企業の平均総コストは 603 万ドルです。セキュリティー自動化を全面的に導入している企業の情報漏えいの平均コストは 245 万ドルであるため、2 倍以上に相当します。セキュリティー自動化を全面的に導入している企業は、セキュリティー自動化を導入していない企業と比べて、漏えいの平均コストを 358 万ドル節減しています。2018 年の調査では 155 万 ドルの節減額だったのと比べると大きく増加しています。

100 倍

平均的な漏えいのコストと比較した、大規模漏えい (5,000 万レコード超) のコストの乗数

大規模漏えいのコストは数百万ドルも増大。

100 万件を超えるレコードの漏えい被害に遭った企業では、非常に大規模な情報漏えいのサンプルで、引き続きコストが全体平均の何倍にも上っています。100 万～ 1,000 万件のレコードの漏えいには、平均 5,000 万ドルのコストがかかります。10 万件未満の漏えいの平均コストは 386 万ドルであるため、25 倍以上に相当しています。5,000 万件を超えるレコードの漏えいでは、平均コストは 3 億 9,200 万ドルで、平均の 100 倍以上でした。

国家主体のアクターによる漏えいの被害は最も高額。

悪意のある漏えいの大部分は金銭目的のサイバー攻撃者によって引き起こされましたが、国家主体のアクターによって引き起こされたもののコストが最も高額でした。2020 年の調査によると、悪意のある漏えいの 53% は金銭目的のサイバー犯罪者が実行したと考えられています。これに対し、国家主体の脅威アクターによるものは 13%、ハクティビストによるものは 13%、不明が 21% となっています。しかし、金銭目的の漏えいのコストは 423 万ドルであるのと比較して、国家主体の漏えいのコストは平均 443 万ドルと推定されます。

+29 万 2,000 ドル

セキュリティー・システムの複雑さが平均総コストに与える影響

セキュリティーの複雑さとクラウドへの移行は、企業にとって最大の負担。

セキュリティー・システムの複雑さは、25 のコスト要因の中で最も高く、これによって漏えいの平均総コストは 29 万 2,000 ドル増加し、調整後の平均総コストは 415 万ドルになりました。漏えい時に大規模なクラウドへの移行を行った場合、漏えいの平均コストは 26 万 7,000 ドル以上増加して、調整後の平均コストは 413 万ドルに達しました。

+ 96 日

医療業界と金融業界の漏えいライフサイクルの比較

漏えいの検知と被害拡大防止にかかる平均時間は、業種、地域、およびセキュリティーの成熟度によって大きく異なる。

平均すると、2020 年の調査対象企業は、2019 年に漏えいの検知に 207 日、被害拡大防止に 73 日を要し、「ライフサイクル」は合計 280 日になりました。

医療セクターでは、漏えいのライフサイクルは平均 329 日でしたが、金融セクターでは、平均ライフサイクルが 96 日短い結果になりました (233 日)。セキュリティー自動化が全面的に導入されている企業では、そうでない企業と比較して、漏えいのライフサイクルが 74 日短縮され、308 日から 234 日になりました。

200 万ドル

インシデント対応チームとテストを導入しない場合と比較した、導入した場合のコスト節減額の平均

インシデント対応（IR）準備は企業がコストを最も削減できる要因。

IR チームを備え、机上訓練やシミュレーションによって IR 計画をテストした企業では、情報漏えい時に発生する平均総コストが 329 万ドルでした。一方、IR チームがなく IR 計画のテストも実施しない企業のコストは 529 万ドルと、その差は 200 万ドルにも上りました。2019 年の調査では、これらのグループ間のコストの差は 123 万ドルでした。

16 カ国中 12 カ国

2019 年の調査以降に平均総コストが増加した国

地域や業種の違いによって、2019 年からいくつかの大きな変化が見られる。

情報漏えいコストが世界で最も高かったのは、引き続き米国で、平均 864 万ドルです。続いて、中東が 652 万 ドルです。2019 年と 2020 年の両方で調査対象となった 16 の国や地域のうち 12 の国や地域で平均総コストの増加が見られました。最も増加が大きかったのはスカンジナビアで、12.8% でした。

医療業界は、10 年連続で平均漏えいコストが最も高く、713 万ドルを記録しました。これは、2019 年の調査と比べて 10.5% の増加です。同様に、エネルギー・セクターでは 2019 年から 14.1% 増加し、2020 年の調査では平均 639 万ドルに達しました。全体として、17 業種中 13 業種では、平均総コストが前年比で減少し、最も急激な減少が見られたのは、メディア、教育、公共セクター、接客業でした。

調査結果完全版

このセクションでは、今回の調査結果を詳しく説明します。トピックの順序は次のとおりです。

1. グローバルな調査での結果とハイライト
2. 情報漏えいの根本原因
3. 情報漏えい時に発生するコストに影響を及ぼす要因
4. セキュリティー自動化のトレンドと効果
5. 情報漏えいの検知と被害拡大防止にかかる時間
6. 情報漏えい時に発生するロングテール・コスト
7. 新型コロナウイルス感染症の潜在的な影響
8. 大規模な情報漏えいのコスト

グローバルな調査での結果とハイライト

「情報漏えい時に発生するコストに関する調査」は、17 の国/地域および 17 の業種に及ぶ 524 の企業から得た結果を組み合わせたグローバル・レポートであり、世界的な平均を知ることができます。ただし、一部のケースでは、比較のために国/地域または業種別に結果を示しています。国/地域および業種によっては、調査対象企業の規模が非常に小さいことがありますが、対象の企業は代表として選ばれています。

主な調査結果

713 万ドル

医療業界での情報漏えいの平均コスト。2019 年の調査と比較して 10% 増加していました。

80%

顧客 PII を含むレコードを含む漏えいの割合。レコード 1 件当たりの平均コストは 150 ドル。

552 万ドル

従業員数が 25,000 人を超える企業における漏えいの平均総コスト。それに対し、従業員数が 500 人未満の企業では 264 万ドル。

図 1

グローバル調査の概要

国または地域	2020 年調査対象	調査対象の割合	通貨	調査年数
アメリカ	63	12%	USD	15
インド	47	9%	INR	9
英国	44	8%	GBP	13
ドイツ	37	7%	Euro	12
フランス	36	7%	Euro	7
ブラジル	35	7%	BRL	9
日本	33	6%	Yen	11
中東*	29	6%	Riyal	7
カナダ	26	5%	CA Dollar	6
韓国	24	5%	Won (KRW)	3
ASEAN#	23	4%	Singapore Dollar	2
オーストラリア	23	4%	AU Dollar	11
スカンジナビア諸国	23	4%	Krone	2
イタリア	21	4%	Euro	9
ラテンアメリカ**	21	4%	Peso	1
トルコ	20	4%	Turkish Lira	3
南アフリカ	19	4%	SA Dollar	5
合計	524			

今年の調査では、17 の国/地域の調査対象企業で漏えいを調査。

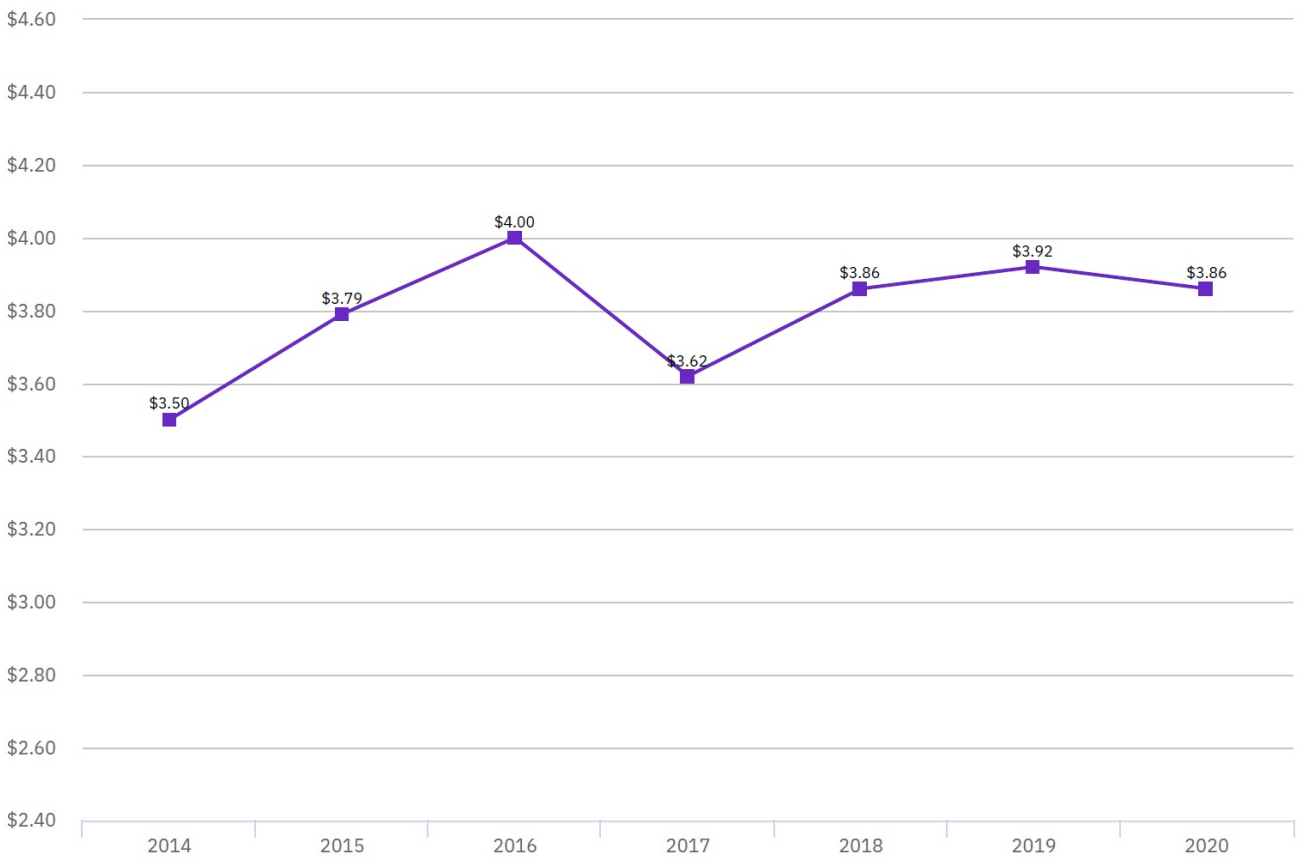
国/地域には、米国、インド、英国、ドイツ、ブラジル、日本、フランス、中東、カナダ、イタリア、韓国、オーストラリア、トルコ、ASEAN、南アフリカ、スカンジナビアに加え、初めてラテンアメリカが含まれています。これはメキシコ、アルゼンチン、チリ、コロンビアを含む地域です。図 1 は、本グローバル調査で調査対象とした各国/地域の企業の数、通貨、および各国/地域が調査対象となった年数を示したものです。

* 中東とは、サウジアラビアとアラブ首長国連邦にある対象企業群を指します。
# ASEAN とは、シンガポール、インドネシア、フィリピン、マレーシア、タイ、ベトナムにある対象企業群を指します。
スカンジナビア諸国とは、デンマーク、スウェーデン、ノルウェー、フィンランドにある対象企業群を指します。
** ラテンアメリカとは、メキシコ、アルゼンチン、チリ、コロンビアにある対象企業群を指します。

図 2

情報漏えい時に発生する平均総コスト

単位: 100 万米ドル



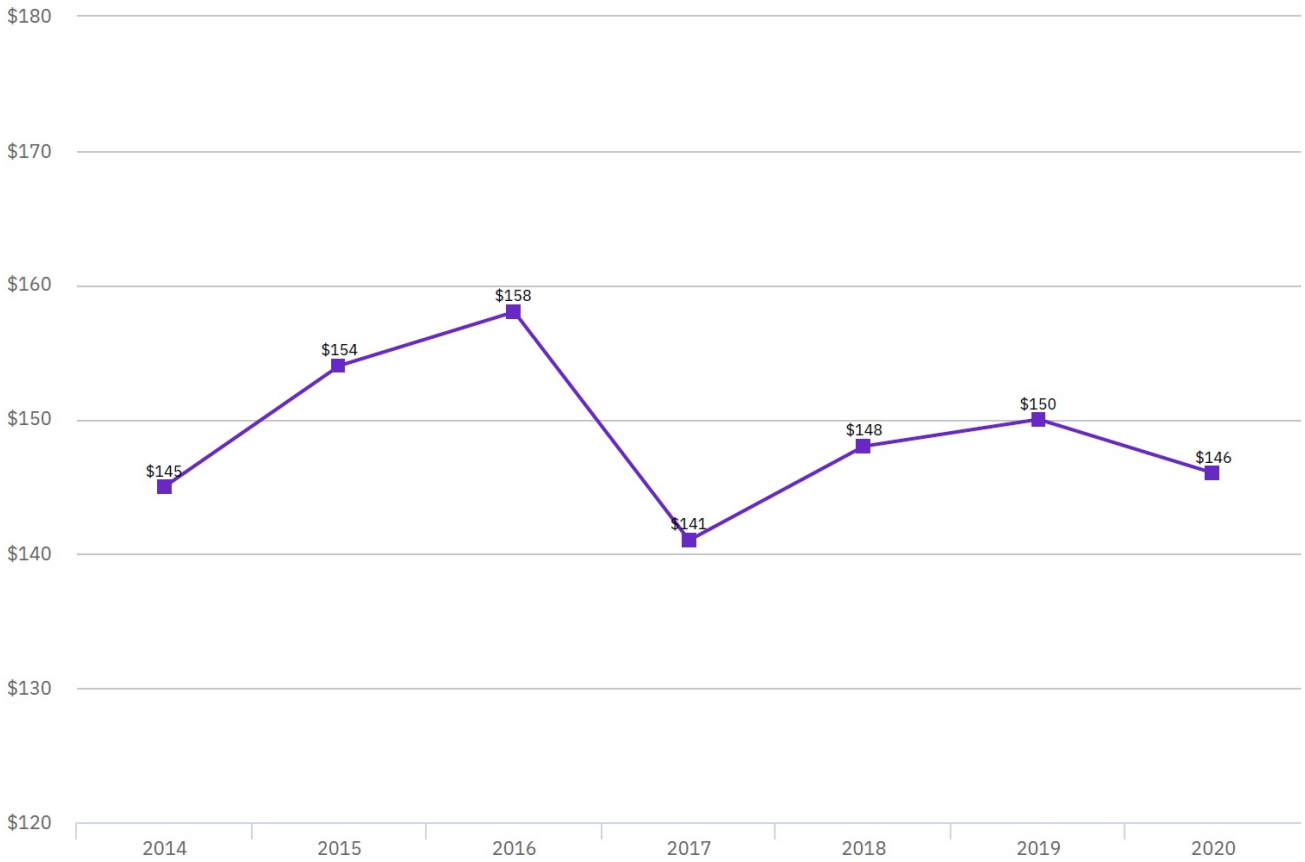
情報漏えい時に発生する平均総コストは、2014 年以降 10% 増加。

図 2 は、情報漏えい時に発生する総コストの世界平均を過去 7 年間にわたって示したものです。2020 年の調査における平均総コストをまとめると、386 万ドルで、2019 年の 392 万ドルからわずかに減少しています。7 年間の加重平均コストは 379 万ドルになります。

図 3

レコード 1 件当たりの平均情報漏えいコスト

単位: 米ドル



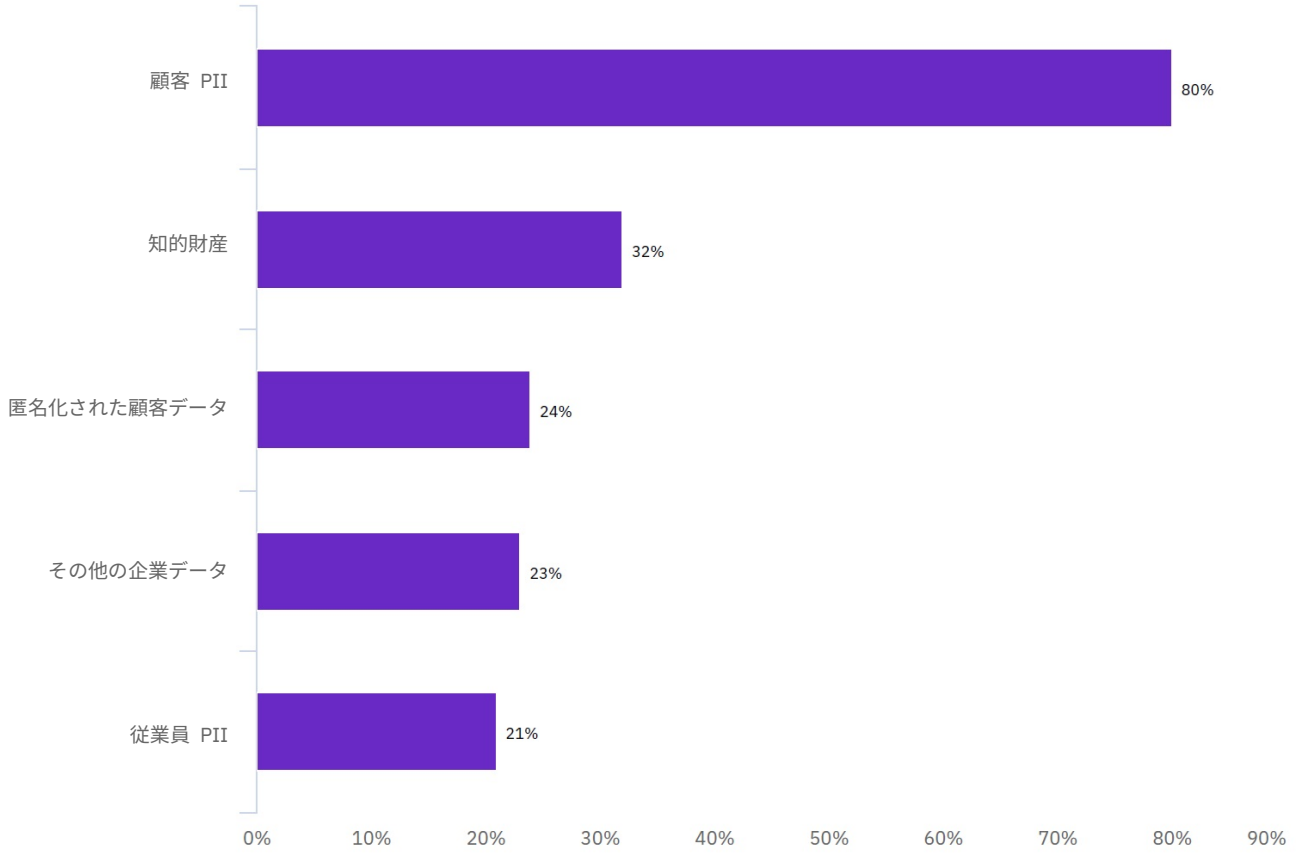
レコード 1 件当たりの情報漏えいコストはわずかに減少して、146 ドル。

図 3 は、被害レコード 1 件当たりの平均情報漏えいコストを過去 7 年間にわたって示したものです。7 年間の加重平均コストは、レコード 1 件当たり 149 ドルになります。

図 4

被害レコードのタイプ

各カテゴリーのデータが関連する漏えいの割合



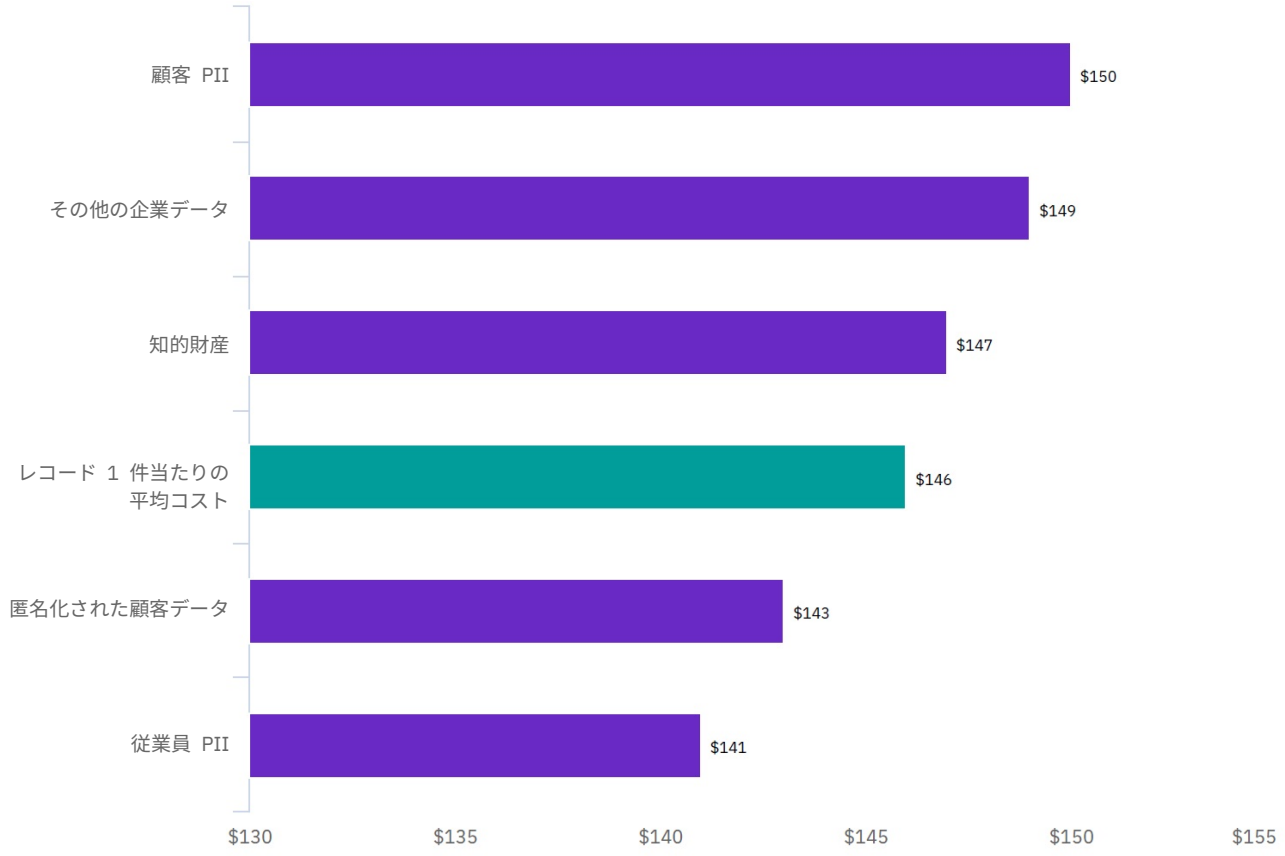
顧客 PII は、漏えいで紛失や盗難が最多だったデータのタイプ。

図 4 で示されているように、情報漏えいの 80% が顧客 PII に関連しています。知的財産は情報漏えいインシデントの 32% で、匿名化された顧客データは 24% で流出しています。

図 5

被害に遭ったデータ・タイプ別のレコード 1 件当たりの平均コスト

単位: 米ドル



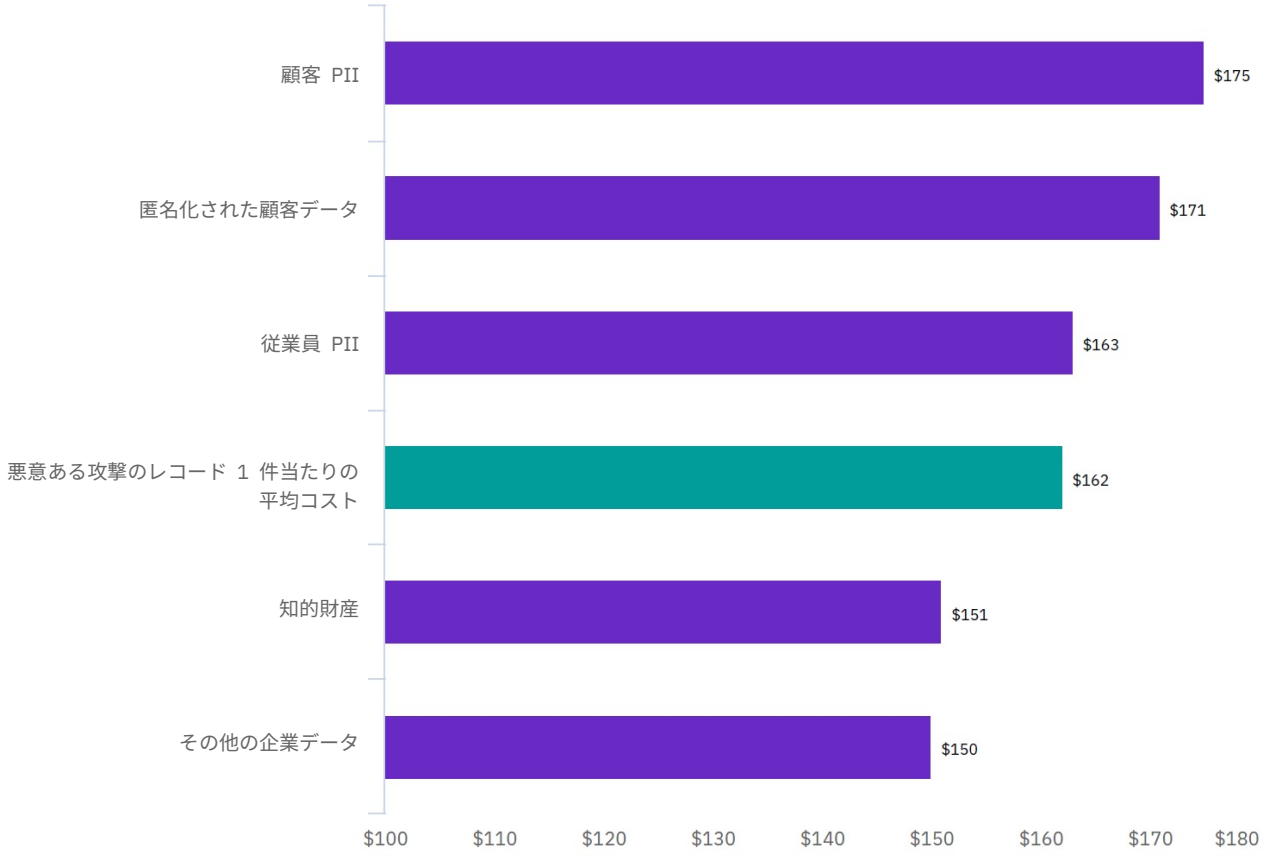
顧客 PII は、漏えいで被害に遭ったデータ・タイプのうち、コストが最大。

図 5 に示すように、紛失や盗難に遭ったレコード 1 件当たりの平均コストは、顧客 PII の場合は 150 ドルとなっています。知的財産の場合は 147 ドル、匿名化された顧客データ (非 PII) の場合は 143 ドル、従業員 PII の場合は 141 ドルがレコード 1 件当たりのコストとなっています。

図 6

悪意のある攻撃で被害に遭ったデータ・タイプ別のレコード 1 件当たりの平均コスト

単位: 米ドル



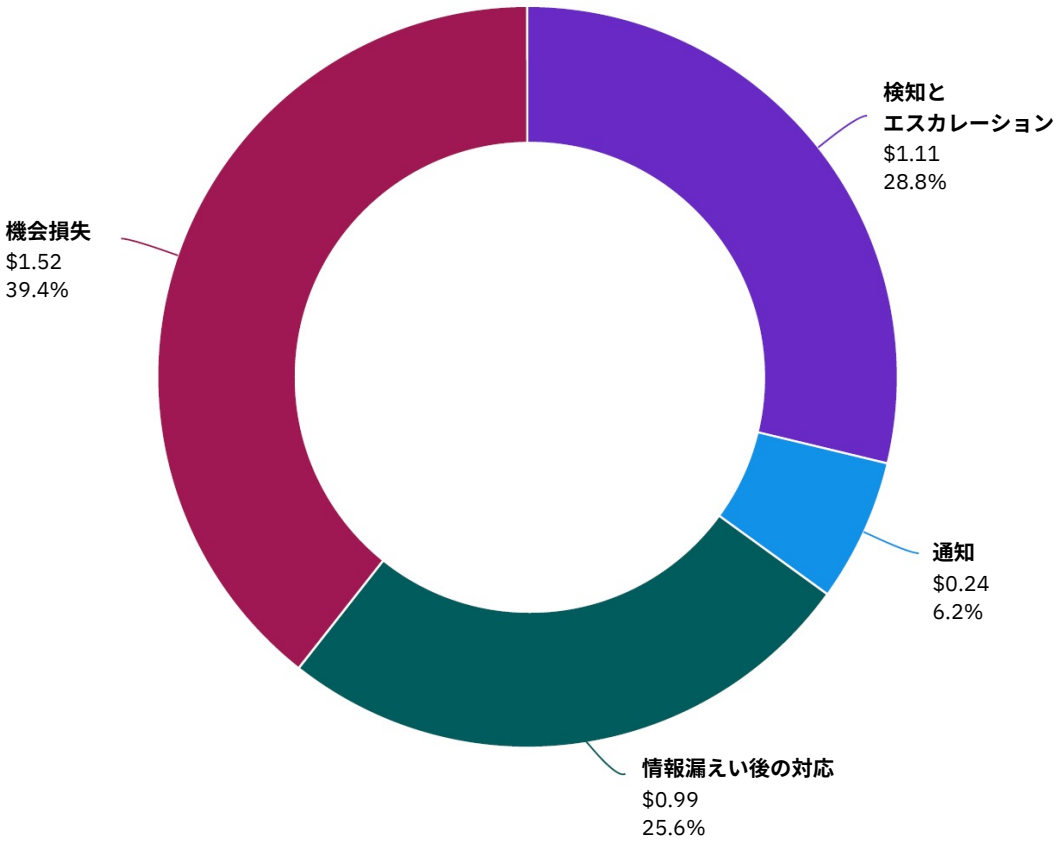
レコード 1 件当たりのコストは、悪意のある攻撃に起因する漏えいの方が高い。

図 6 に示すように、悪意のある攻撃での顧客 PII のレコード 1 件当たりのコストは 175 ドルです。これは、あらゆるタイプの漏えいで被害に遭った顧客 PII のレコード 1 件当たりの全体的な平均コスト（レコード 1 件当たり 150 ドル）よりも 17% 近く高い結果になりました。

図 7

4 つのカテゴリーで分類した情報漏えいの平均総コスト

単位: 100 万米ドル



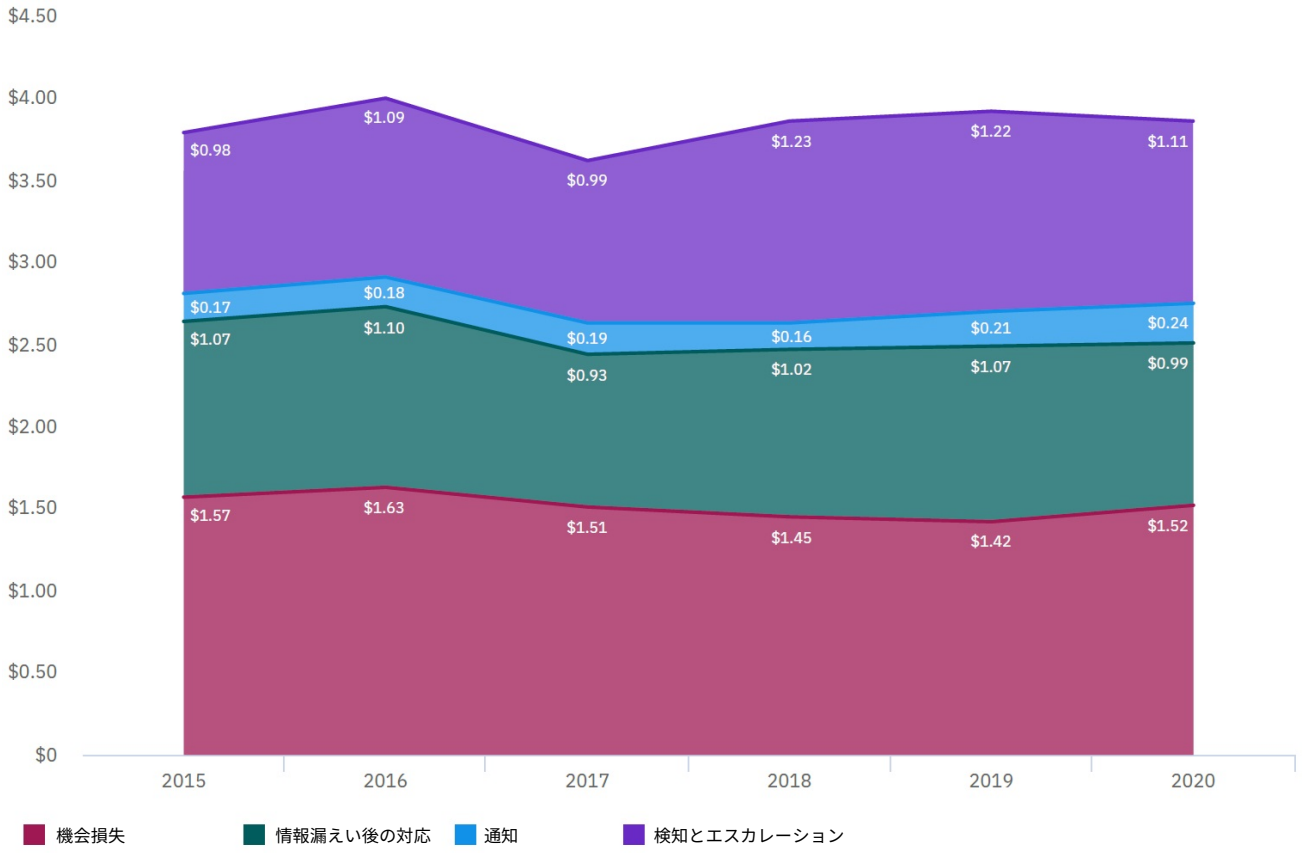
機会損失コストは、情報漏えいの平均コストの最大割合を占める。

図 7 は、4 つのコスト・セグメントを米ドルで示し、情報漏えいの総コストに占める割合を示しています。機会損失コストは平均 152 万ドルで、総コストの 39% を占めました。コストが最も低かったのは、情報漏えいの通知に関するもので、24 万ドルでした。これは総コストの 6% を占めています。

図 8

4 つのカテゴリーの平均情報漏えいコストの傾向

単位: 100 万米ドル



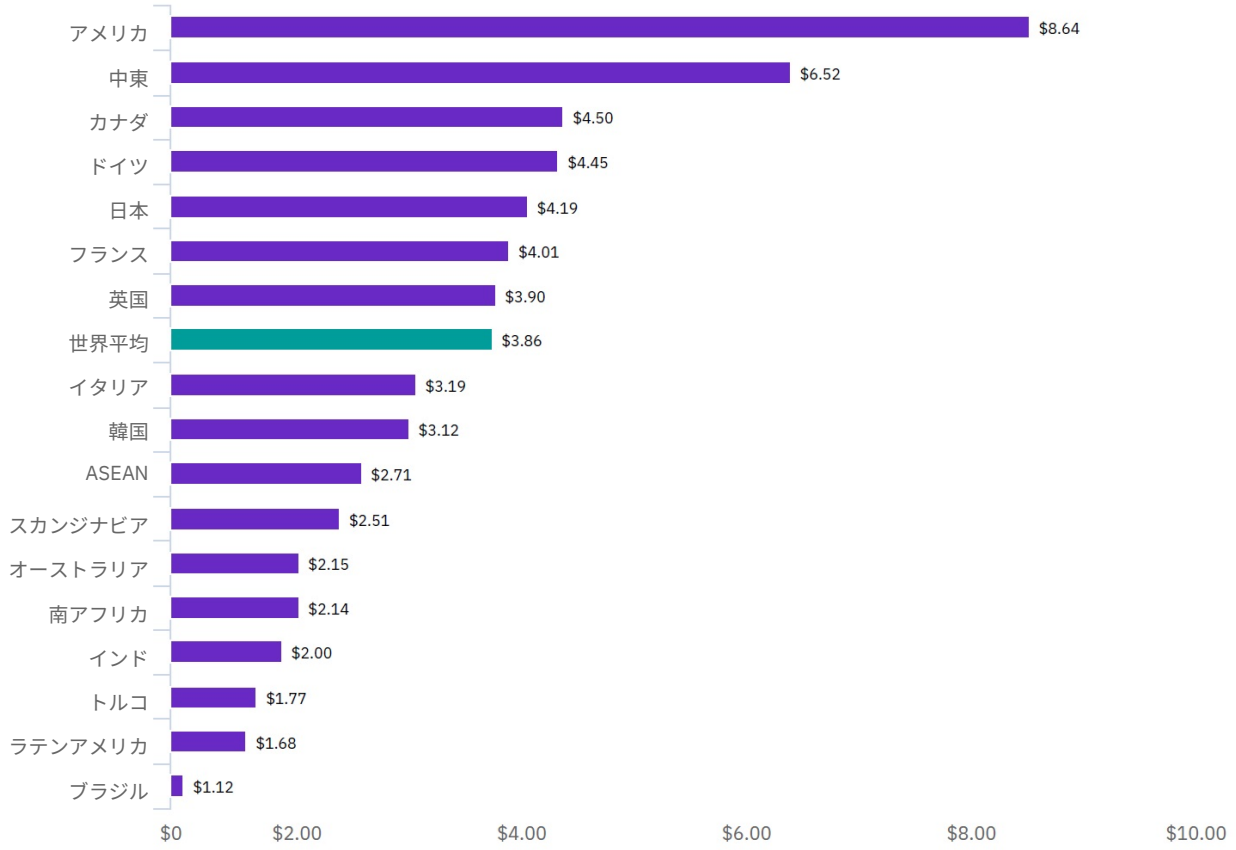
機会損失コストは、前年比で微増。

図 8 は、過去 6 年間の機会損失、漏えい後の対応、通知、検知とエスカレーションのコストの傾向を示しています。パターンはこれらのコストに見られる一貫性を示しています。通知は引き続き最も低く、機会損失コストは最も高くなっています。

図 9

情報漏えいの平均総コスト (国/地域別)

単位: 100 万米ドル



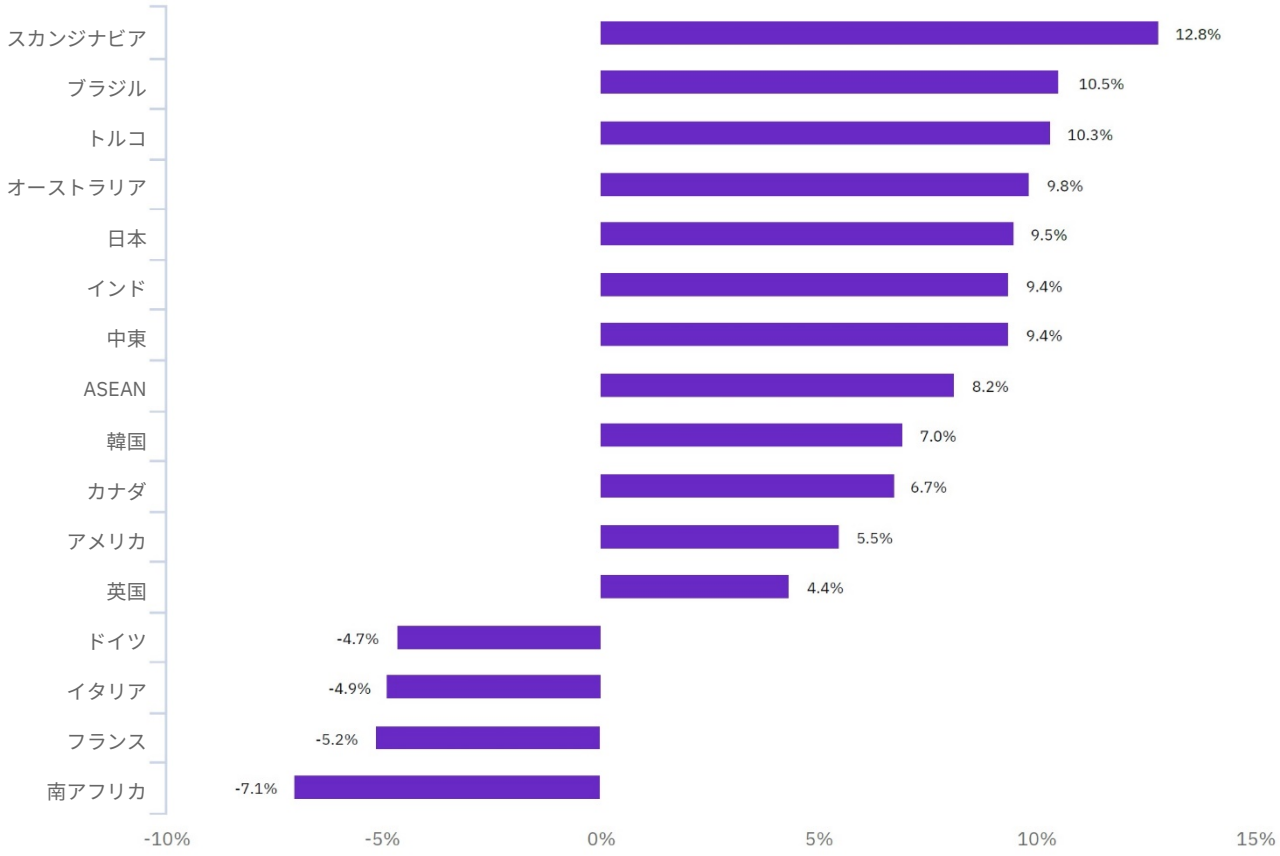
情報漏えいの平均総コストは国によって異なる。

図 9 は、情報漏えいの平均総コストを国別に示したものです。平均総コストが最も高かったのはアメリカの企業で 864 万ドル、次いで中東の 652 万ドルです。一方、平均総コストが最も低かったのはラテンアメリカとブラジルの企業で、それぞれ 168 万ドルと 112 万ドルでした。

図 10

2019～2020 年の平均総コストの変化の状況（国/地域別）

現地通貨で計算



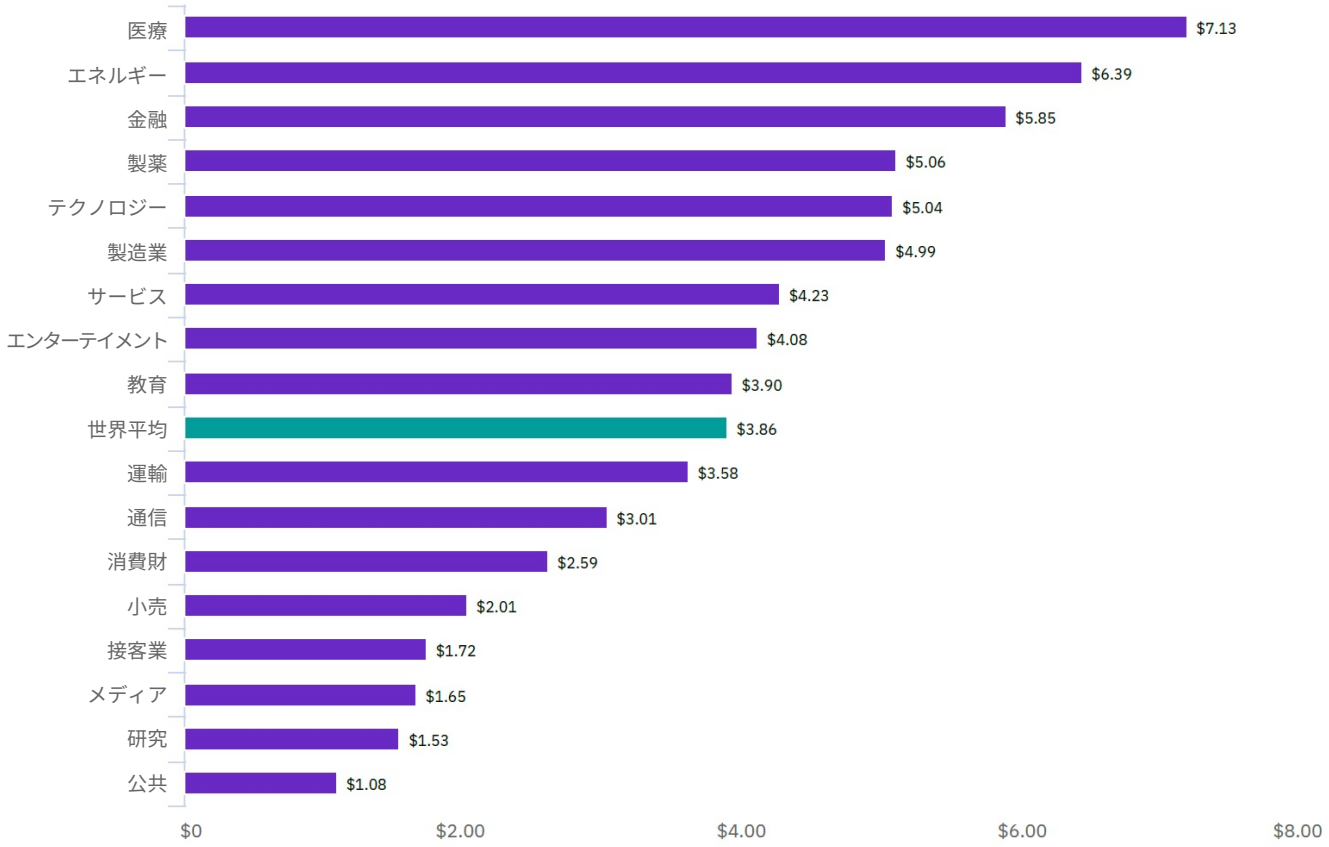
情報漏えいの平均総コストは、 16 カ国中 12 カ国で増加。

図 10 に示すように、2019 年と 2020 年の調査の間に、情報漏えいの総コストの増加率が最大だったのはスカンジナビアで、減少率が最大だったのは、フランスと南アフリカです。

図 11

情報漏えいの平均総コスト (業種別)

単位: 100 万米ドル

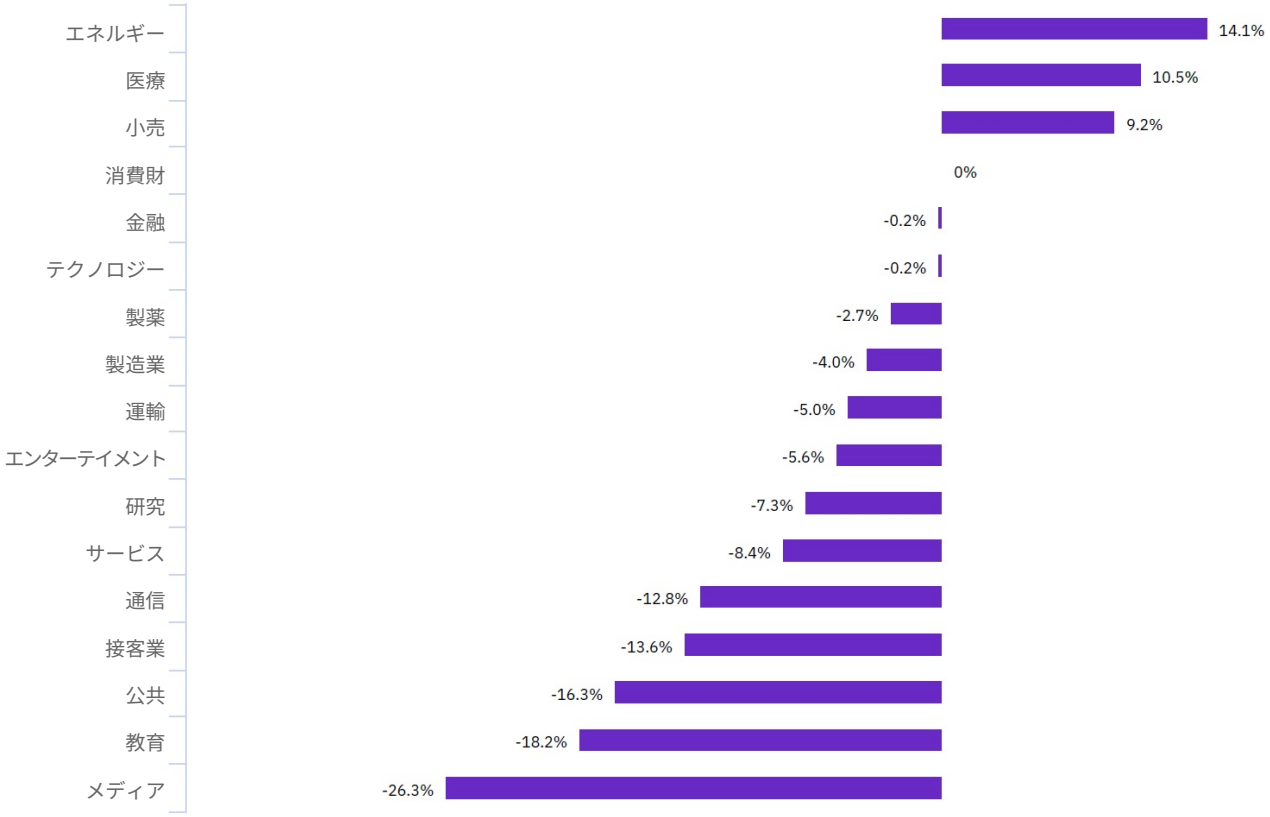


規制要件が厳しい業界の企業ほど、情報漏えいの平均コストが高くなる。

図 11 から、医療、エネルギー、金融サービス、製薬の各業種の企業は、規制の緩やかな業種（接客業、メディア、研究など）の企業に比べて、情報漏えいの平均総コストが非常に高いことが分かります。公共セクターの企業は、情報漏えいの結果として大規模な顧客喪失を被る可能性が低いので、この調査では情報漏えいのコストが従来どおり最も低くなっています。

図 12

2019～2020 年の平均総コストの変化の状況（業種別）



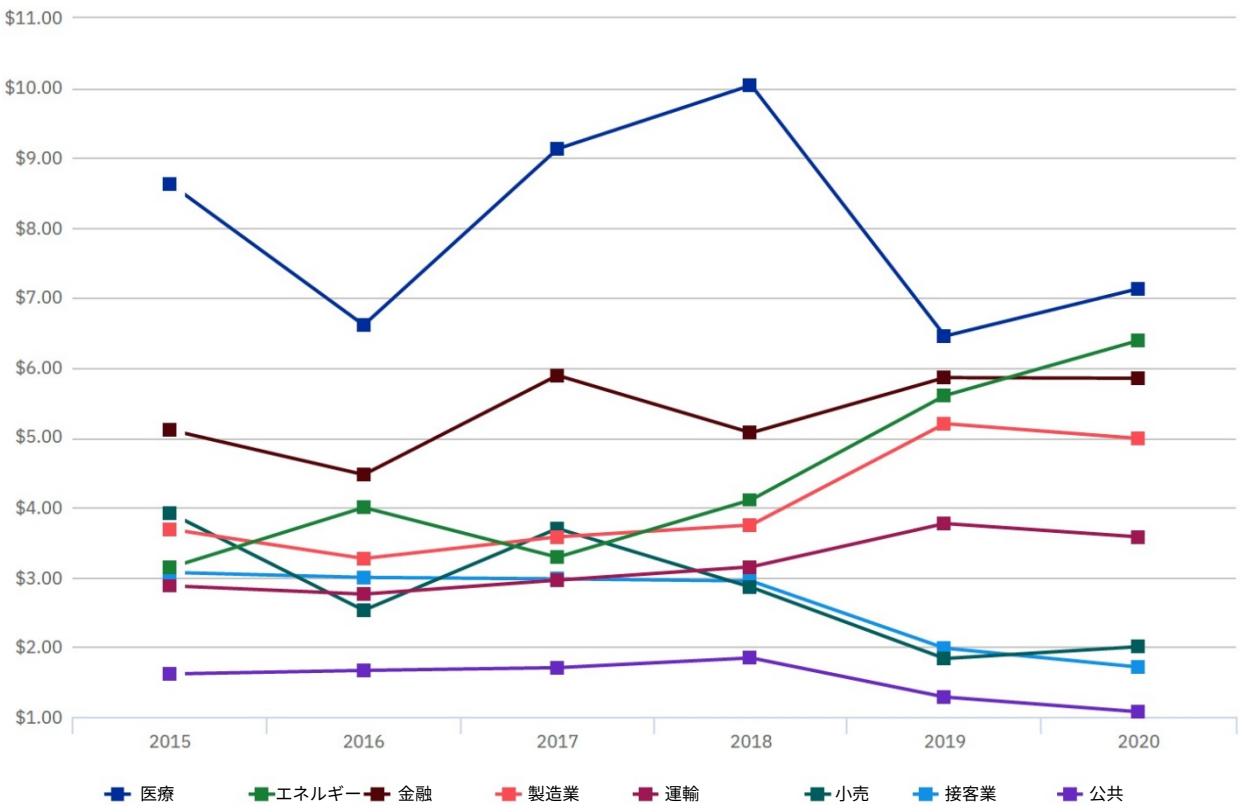
エネルギー、医療、小売の各業種の企業は、情報漏えいコストが最も大きく増加。

図 12 は、2019 年と 2020 年の調査の間に、情報漏えいコストの増加が 17 業種中 3 業種でのみ発生したことを示していますエネルギー、医療、小売では平均総コストが最も増加し、公共セクター、教育、メディアでは最も減少しました。

図 13

8 つの業種における情報漏えいの平均総コストの傾向

単位: 100 万米ドル



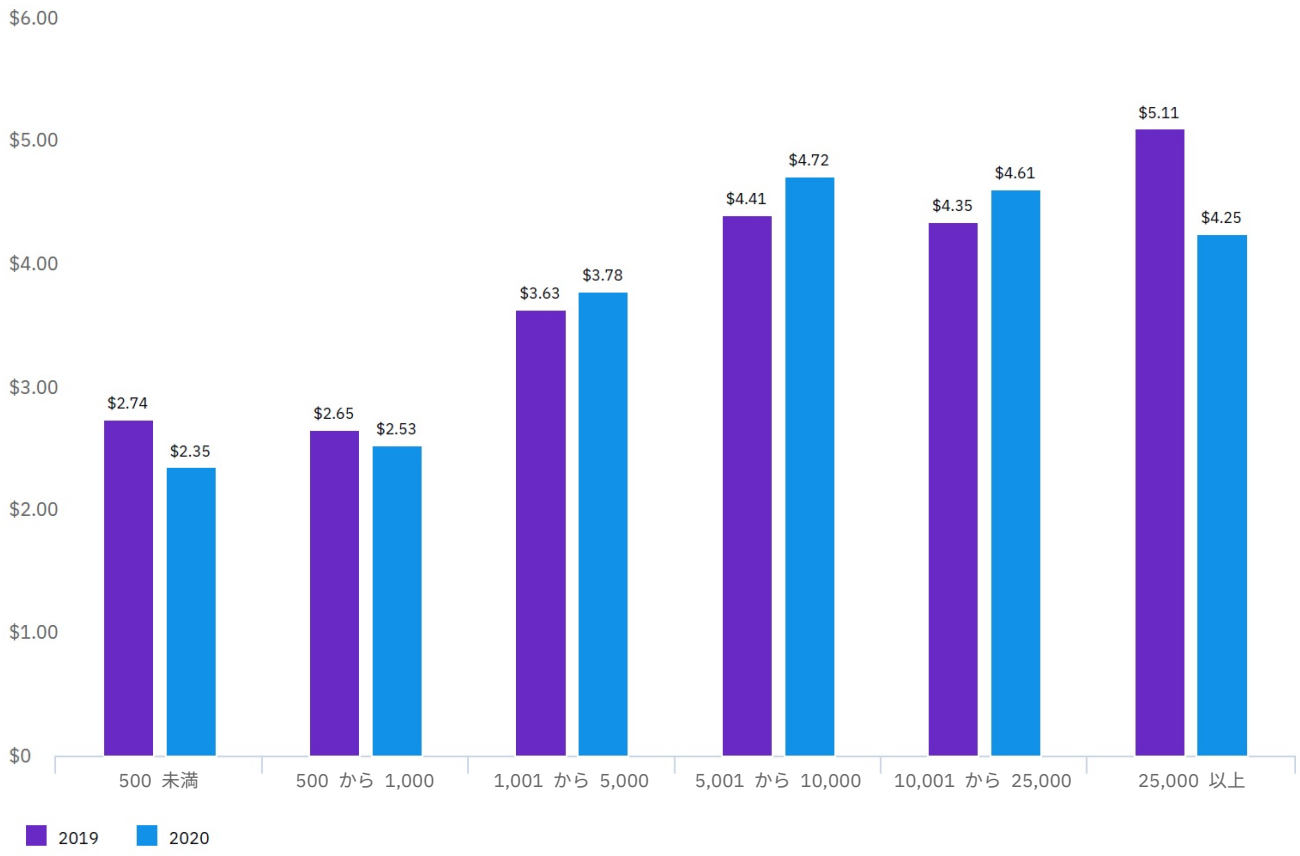
医療および金融の業種では、情報漏えいコストが常に最も高い。

図 13 は、8 つの業種のそれぞれについて過去 6 年間のコストを折れ線グラフで示したものです。 医療は常にコストが最も高く、公共セクターは常に最も低くなっています。

図 14

情報漏えいの平均総コスト (企業規模別)

単位: 100 万米ドル



情報漏えいの平均コストは中規模企業で増加している。

図 14 は、情報漏えい時に発生する平均総コストが、2019 年と 2020 年の調査の間に、最小規模の企業 (従業員数 1,000 人以下) と最大規模の企業 (従業員数 25,000 人超) では減少したことを示しています。 従業員数 25,000 人超の企業は、平均総コストが 511 万ドル (2019 年) から 425 万ドル (2020 年) に減少しました。これは、16.8% の減少を意味します。ただし、中規模企業では、漏えいの総コストは平均して増加しました。従業員数が 5,001 ～ 10,000 人の場合、漏えい時に発生するコストは 平均 441 万ドル (2019 年) から 472 万ドル (2020 年) へと 7% 増加しました。企業の規模が小さくなるのに比例して、従業員 1 人当たりの平均コストは高くなりました。

情報漏えいの根本原因

数年前から、この調査では参加企業に情報漏えいの原因を尋ねてきました。過去数年間、根本原因は 3 つのカテゴリーに分類されていました。それは、IT とビジネス・プロセスの両方の障害を含むシステムの欠陥、人的ミス (従業員や請負業者の不注意による情報漏えいを含む)、およびハッカーや内部の犯罪者によって引き起こされる可能性のある悪意のある攻撃です。

今年の調査では、これら 3 つのカテゴリーの漏えいについて引き続き報告します。ただし、詳細な分析では、初期の脅威ベクトルや攻撃者のタイプなど、悪意のある攻撃の原因について、より詳細な情報を入手しました。このセクションでは、これらの両方の分析の結果を報告します。

主な調査結果

52%

悪意のある攻撃によって発生した漏えいの割合。平均コストは 427 万ドル

19%

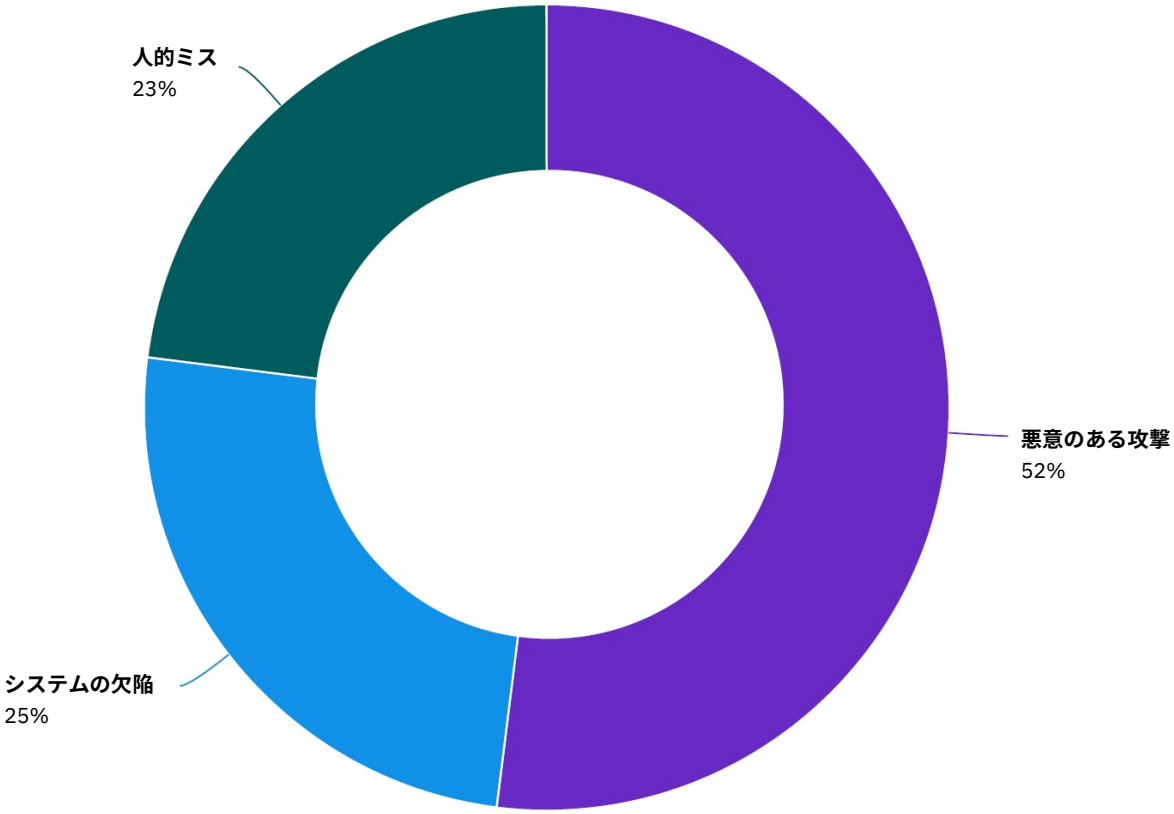
資格情報の流出（19%）とクラウドの構成ミス（19%）によって発生した悪意のある漏えいの割合

443 万ドル

国家主体の攻撃者が引き起こした漏えいの平均コスト。悪意のある漏えいの 13% を占める

図 15

情報漏えいの根本原因の 3 つの内訳



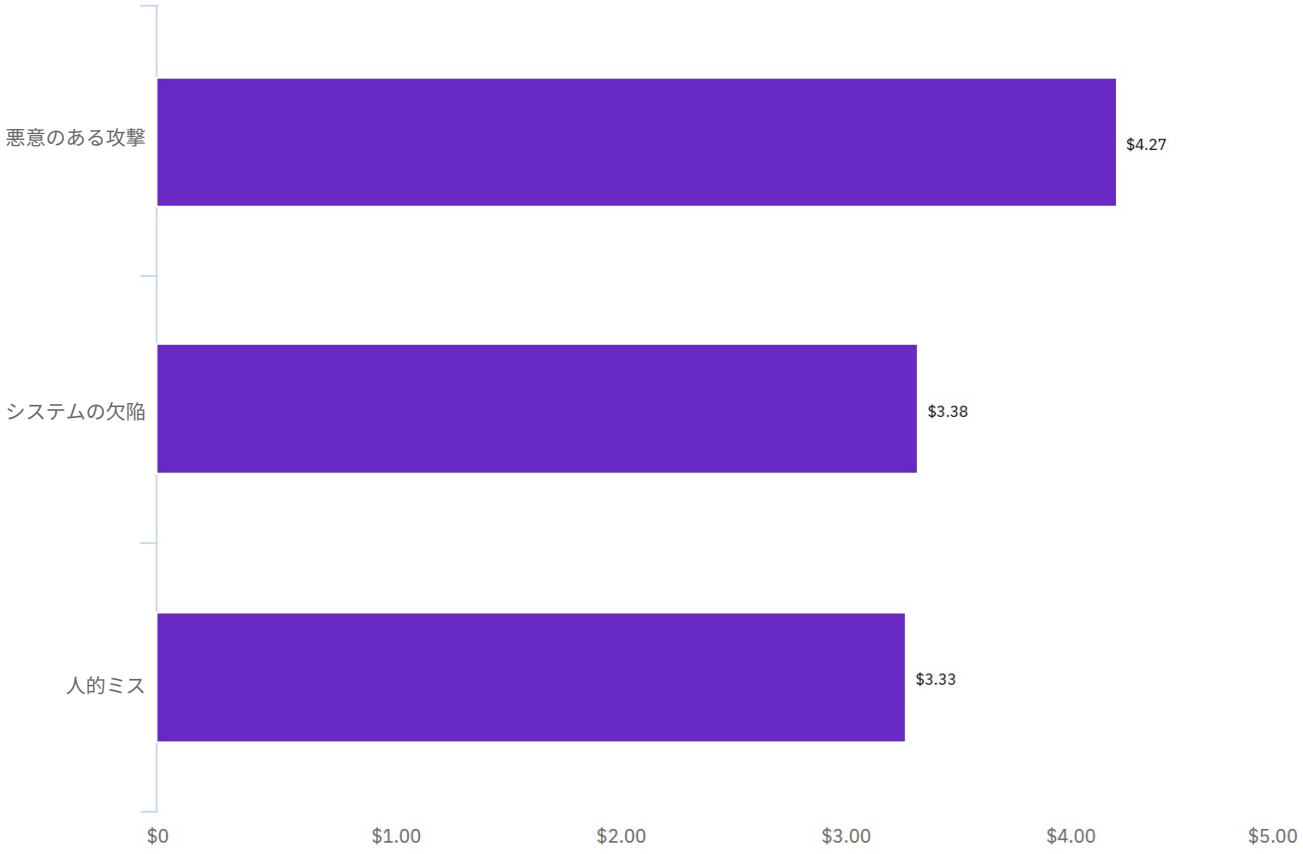
悪意のある攻撃が情報漏えいの過半数の原因。

図 15 は、情報漏えいの根本原因の 3 つの主要なカテゴリーを示しています。インシデントの 52% は悪意のある攻撃に関係しています。一方、25% はシステムの欠陥によるもので、23% は人的ミスによるものです。

図 16

情報漏えいの 3 つの根本原因別の平均総コスト

単位: 100 万米ドル



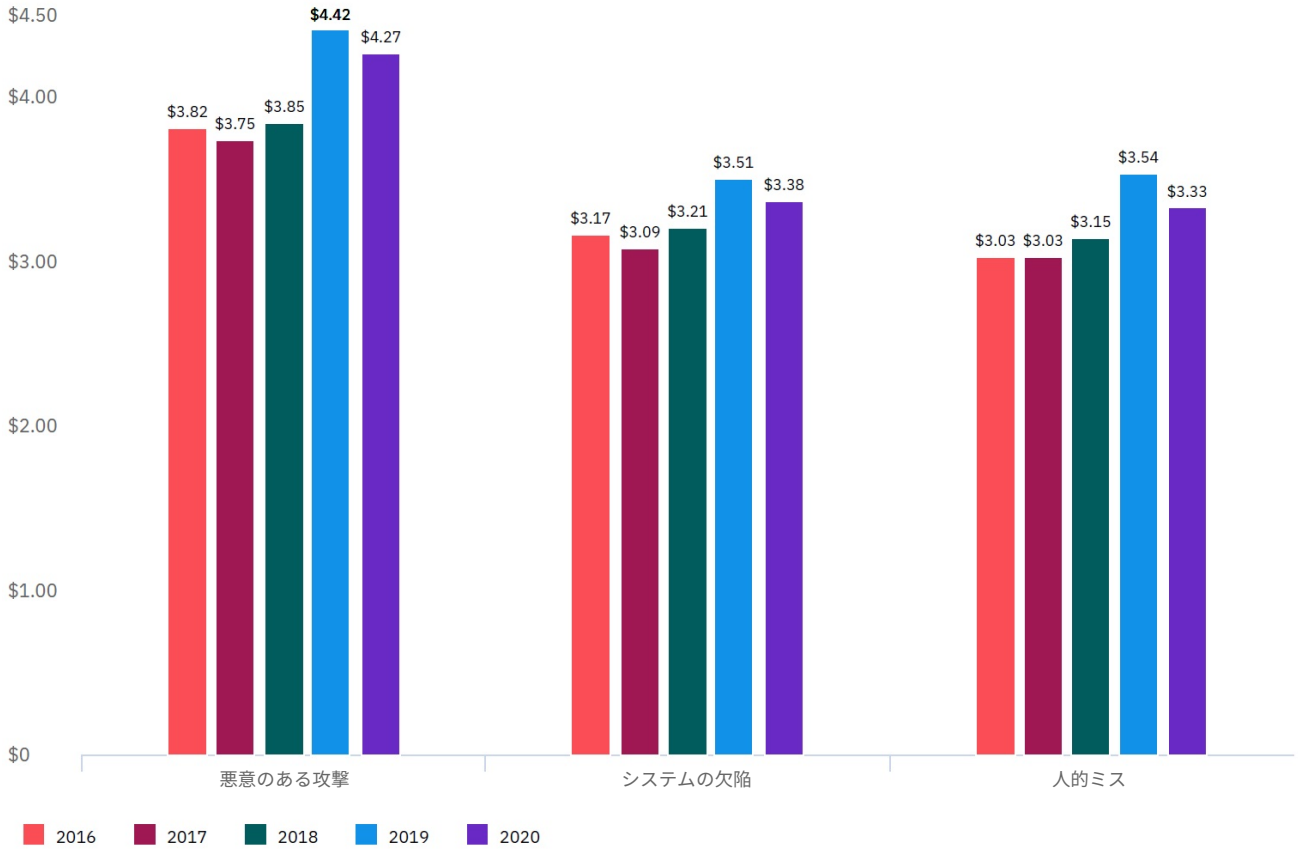
悪意のある攻撃は、最もコストの高い根本原因。

図 16 に示すように、2020 年の調査では、悪意のある攻撃による漏えいの平均コストは 427 万ドルです。これは、システムの欠陥や人的ミスによって発生した漏えいよりも 100 万 ドル近く多い数字です。

図 17

情報漏えいの根本原因別の平均総コストの傾向

単位: 100 万米ドル

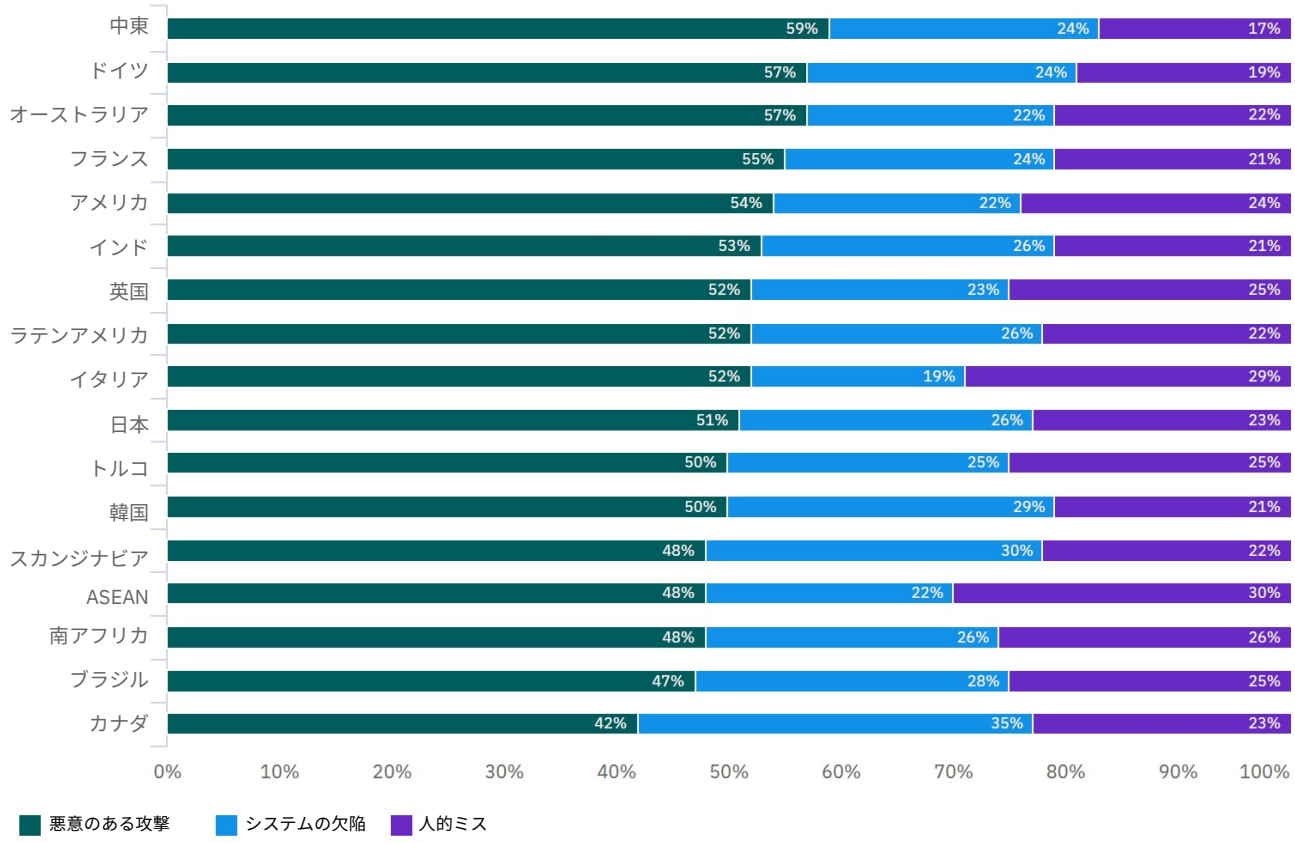


悪意のある漏えいは、過去 5 年にわたり最もコストが高い。

図 17 は、情報漏えいの 3 つの根本原因ごとに過去 5 年間の平均総コストを示したものです。2016 年の調査以降、根本原因のパターンはかなり一定しています。2020 年の調査では、2019 年と比較してコストがわずかに減少しています。悪意のある漏えいの平均総コストは、2016 年の調査以降、12% 近く増加しています。

図 18

情報漏えいの根本原因の内訳 (国/地域別)

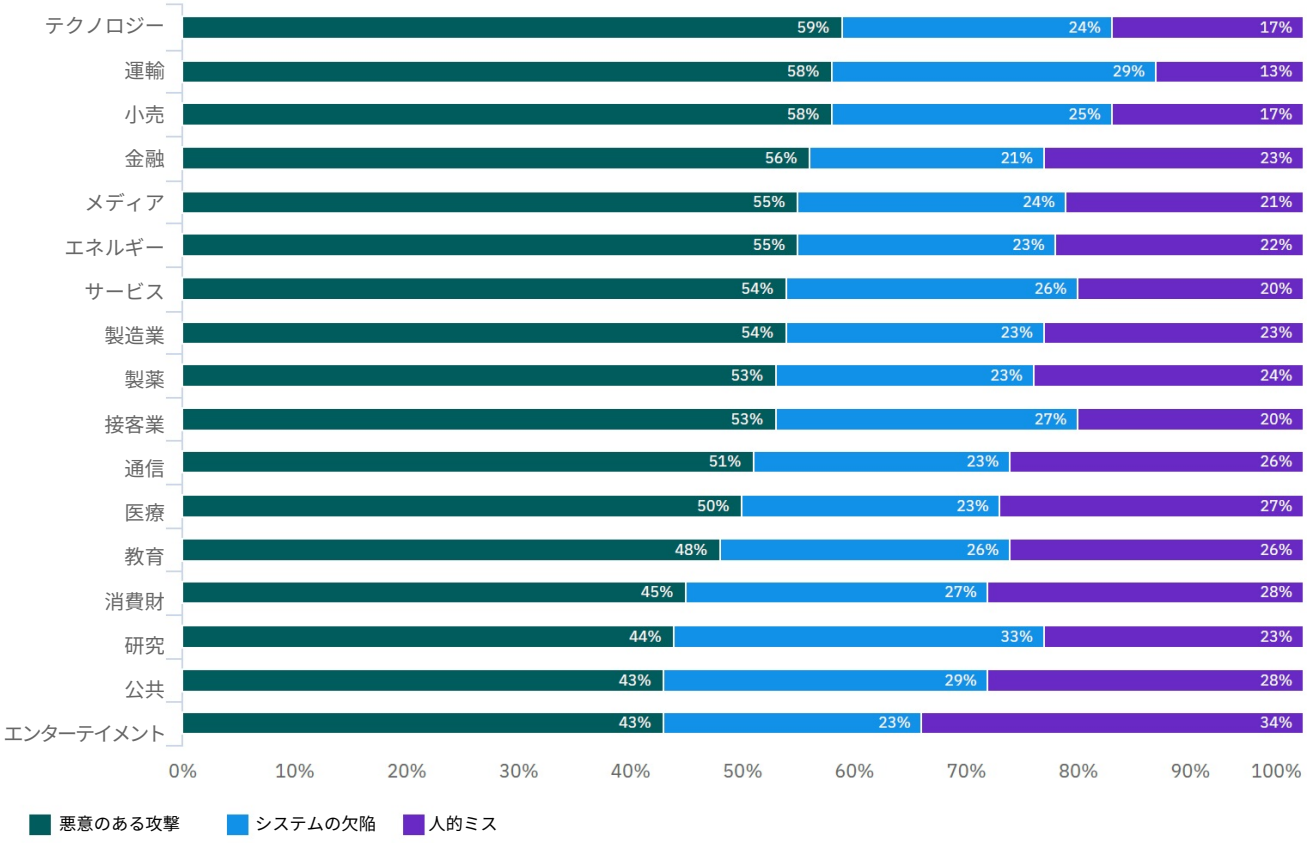


漏えいの根本原因は地域によって異なる。

図 18 によると、悪意のある攻撃による漏えいの割合が最も高いのは中東、ドイツ、オーストラリアで、最も低いのは南アフリカ、ブラジル、カナダでした。システムの欠陥によって発生する情報漏えいは、カナダが最も高くなっています。ASEAN とイタリアは、人的ミスによる情報漏えいの割合が最も高くなっています。

図 19

情報漏えいの根本原因の内訳 (業種別)



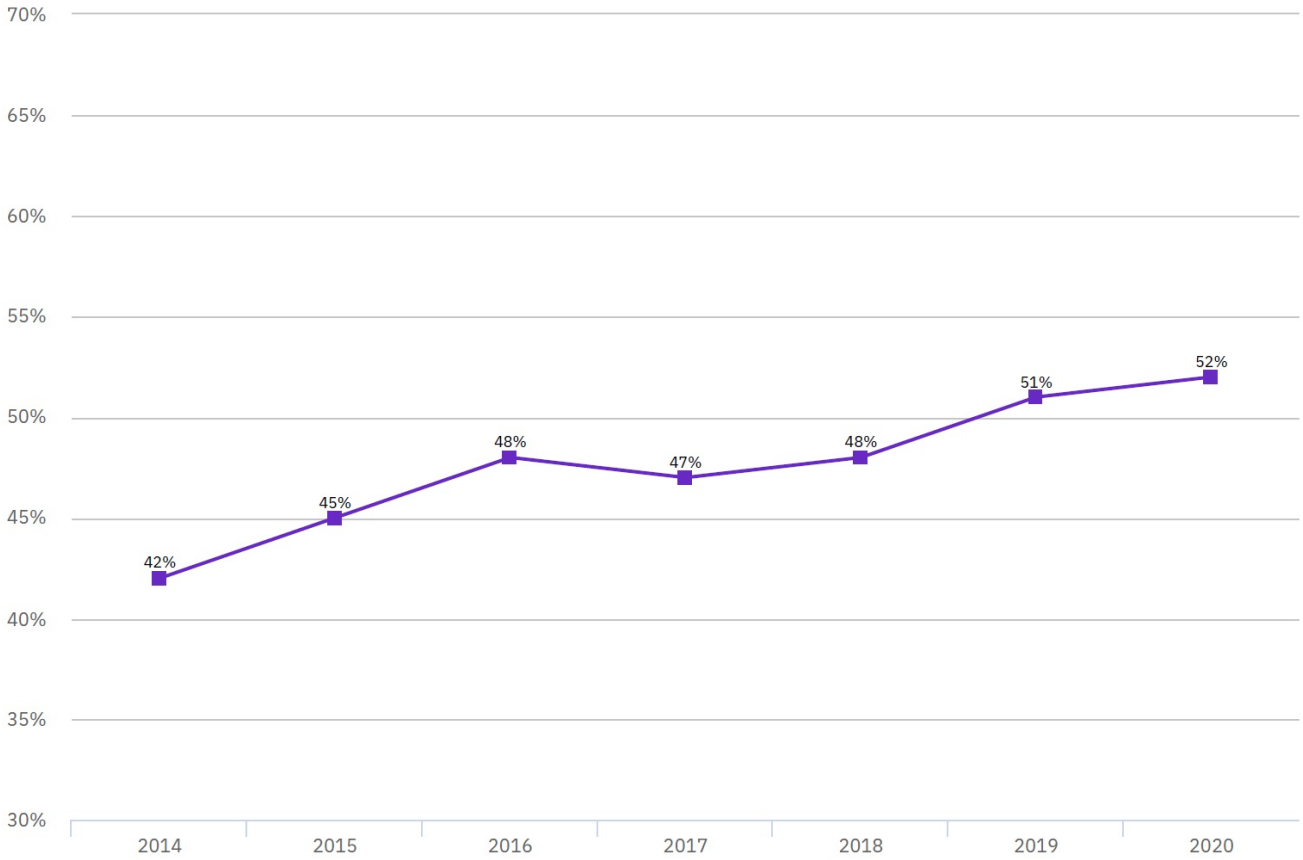
情報漏えいの根本原因の内訳は業種によって異なる。

図 19 に示すように、悪意のある攻撃の割合が最も高かったのは、テクノロジー、輸送、小売、金融の業種です。エンターテインメント、公共セクター、消費財の業種では、人的ミスによる情報漏えいの割合が最も高くなっています。研究、公共セクター、輸送の業種では、漏えいの根本的原因としてシステムの欠陥が比較的多く見られます。

図 20

悪意のある攻撃によって発生する情報漏えいの傾向

すべての漏えいにおける割合



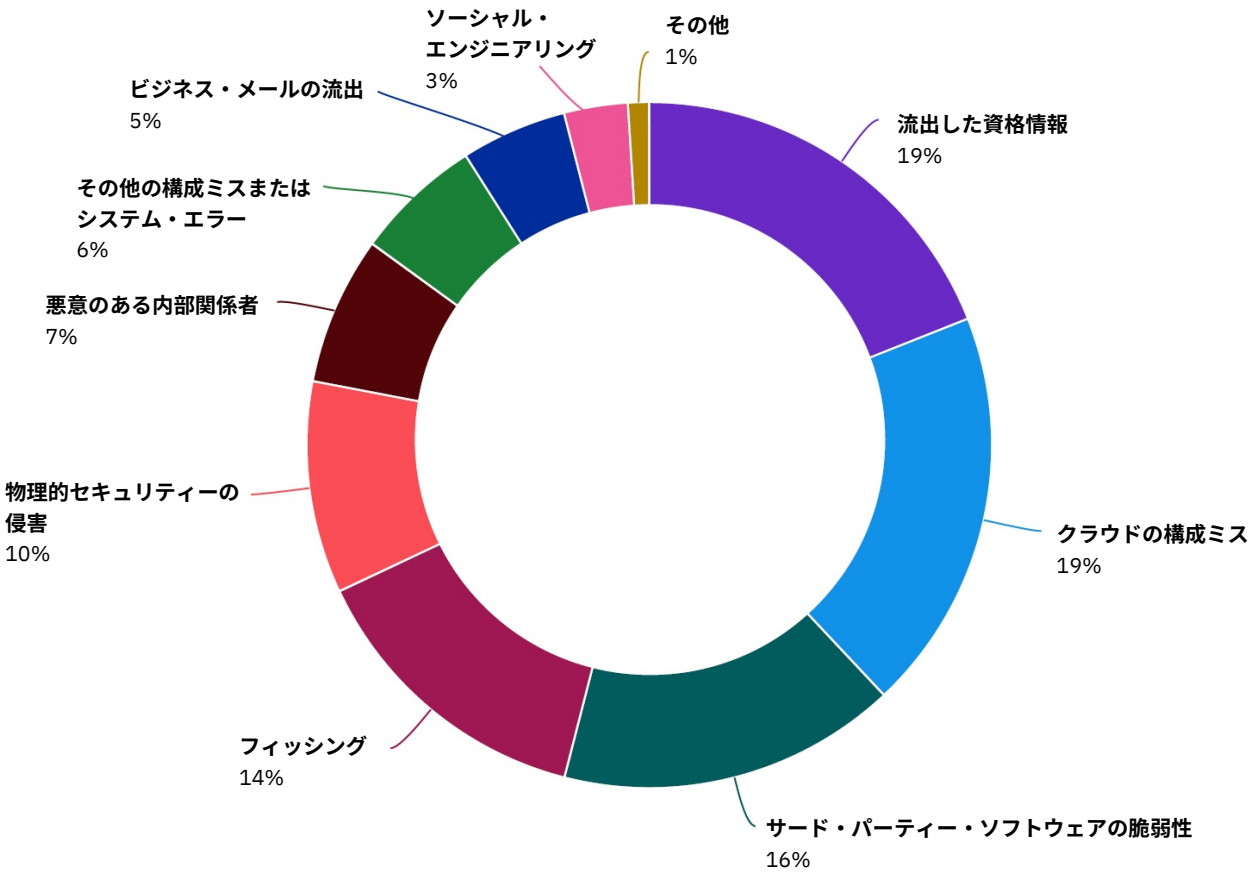
悪意のある攻撃によって発生した漏えいの割合は、時間とともに着実に増加傾向にある。

図 20 は、悪意のある攻撃によって発生した漏えいの割合が、42% (2014 年のレポート) から 52% (2020 年のレポート) に増加したことを示しています。この 10 % の増加は、悪意のある攻撃によって発生した漏えいの割合では約 24% の増加 (成長率) に相当します。

図 21

悪意のある情報漏えいの根本原因の内訳 (脅威ベクトル別)

悪意のある攻撃によって発生した情報漏えいの割合



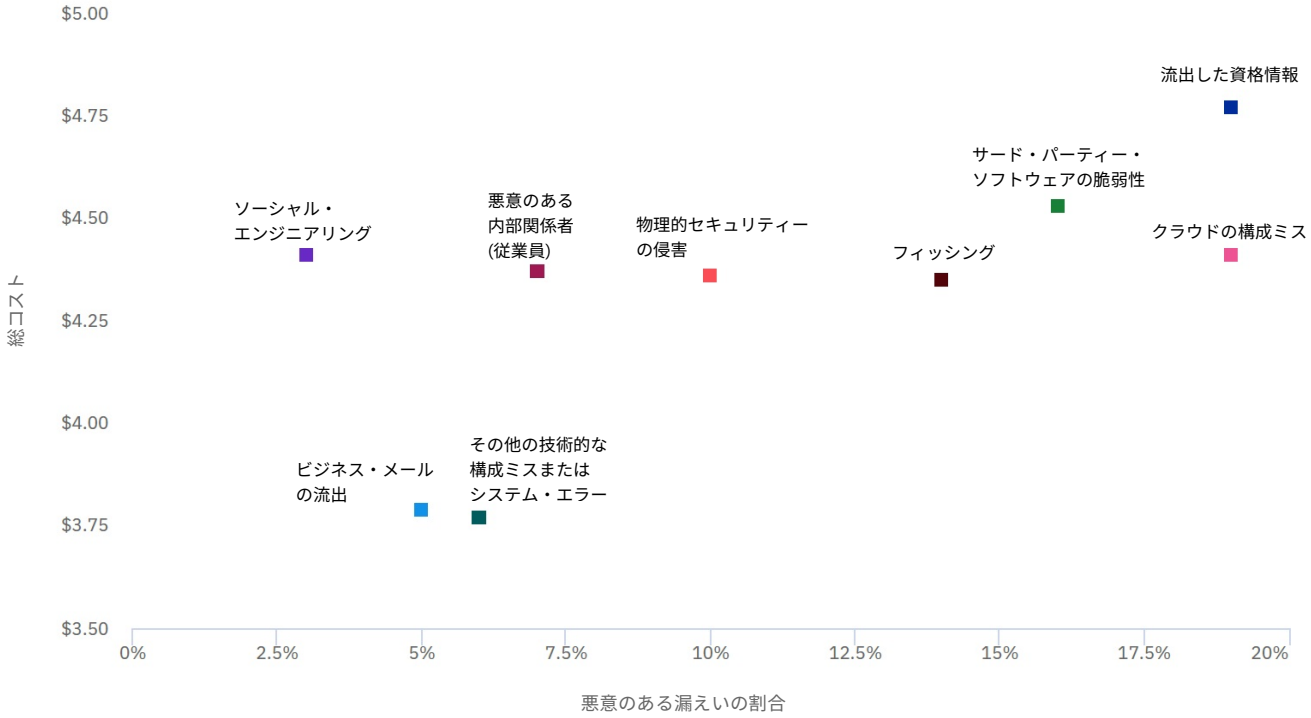
悪意のある情報漏えいの大部分は、資格情報の流出、クラウドの構成ミス、またはサード・パーティー・ソフトウェアの脆弱性が原因となっています。

盗難や流出に遭った資格情報とクラウドの構成ミスが主要な初期脅威ベクトルであり、それぞれ悪意ある漏えいの 19% に関与していました。**図 21** によると、悪意ある漏えいの 16% で、サード・パーティー・ソフトウェアの脆弱性が初期の脅威ベクトルになっています。

図 22

悪意ある情報漏えいの平均コストと頻度（根本原因ベクトル別）

単位: 100 万米ドル

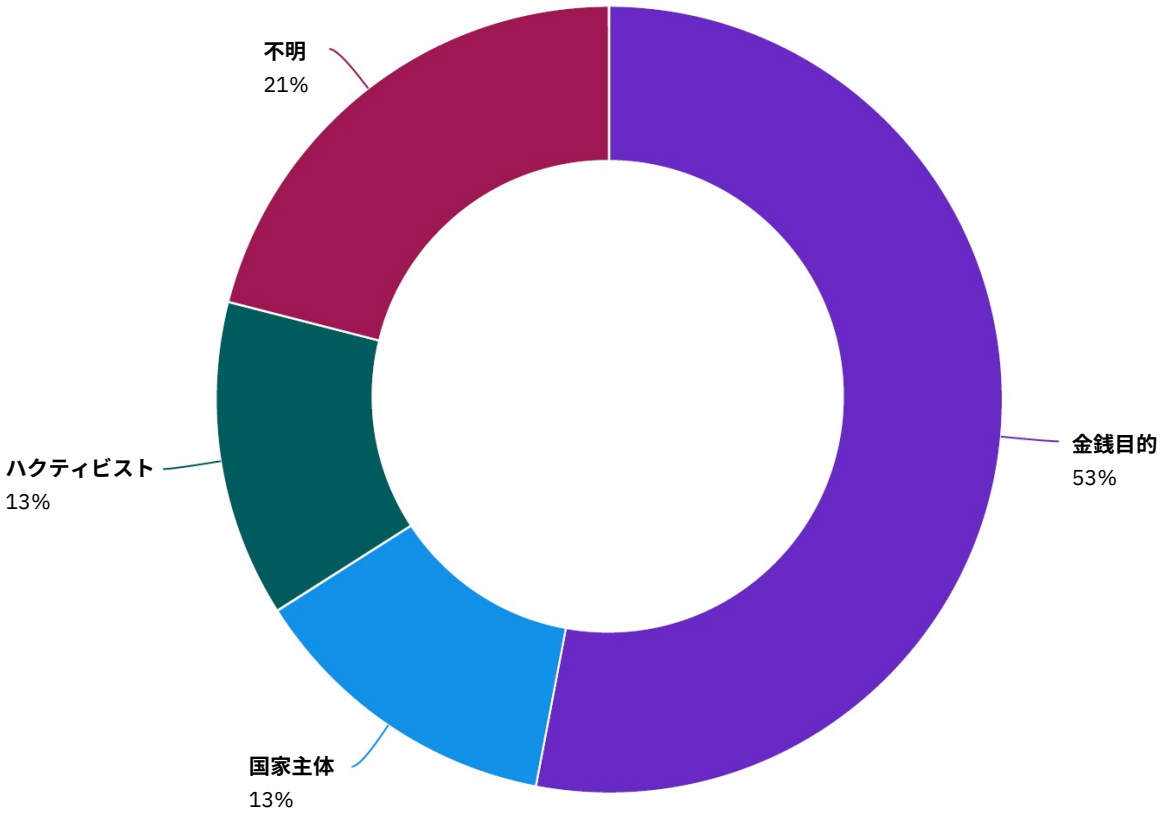


資格情報の流出は、コストと頻度が最も高い脅威ベクトル。

図 22 は、悪意のある漏えいにおける 9 つの初期脅威ベクトルを散布図に示しています。X 軸は漏えいの割合、Y 軸は平均総コストです。資格情報の流出は、グラフの最も右上にある脅威ベクトルです。これは、悪意のある情報漏えいにおける頻度とコストの両方が最高であることをを示しています。

図 23:

脅威アクターの種類別に整理した悪意のある情報漏えい



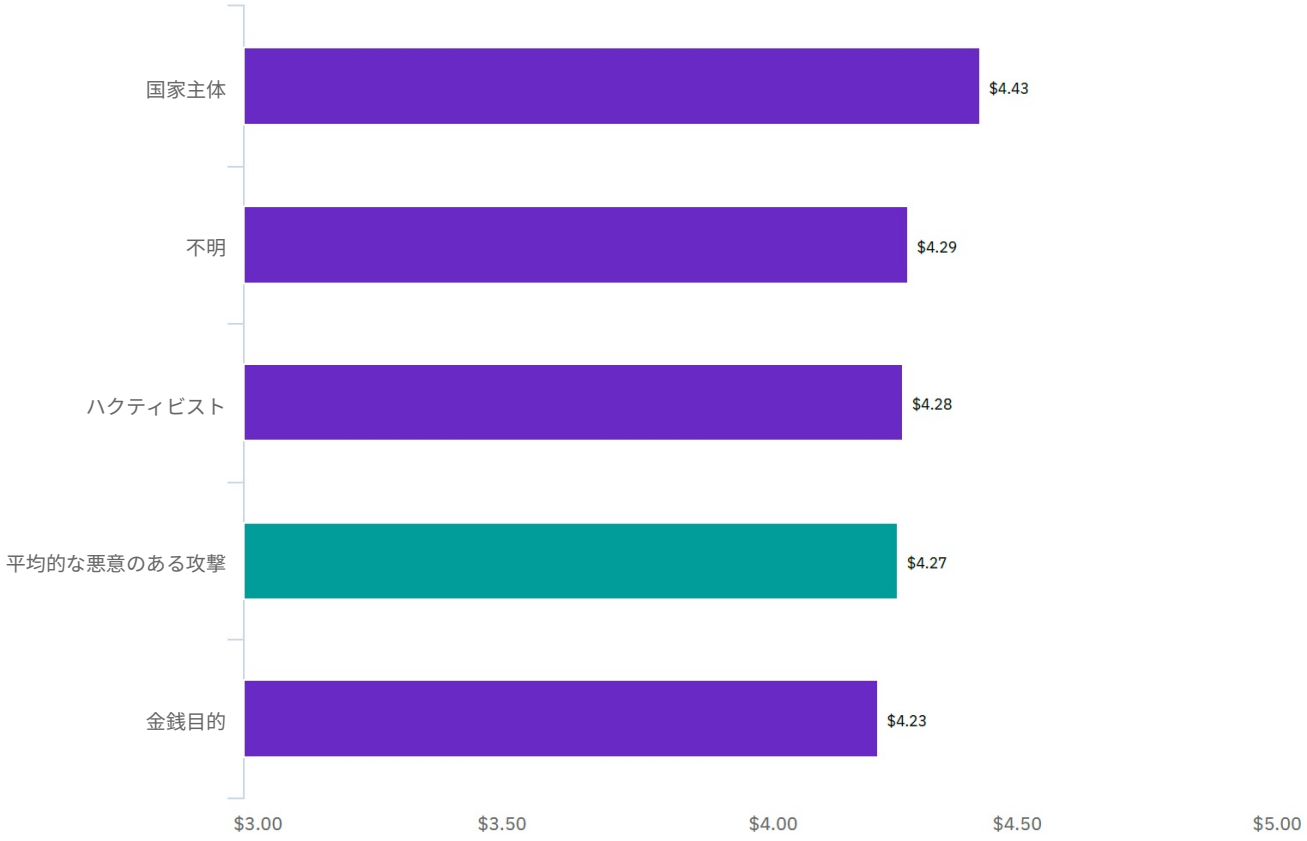
悪意のある情報漏えいの大部分を引き起こしているのは、金銭目的の攻撃者。

図 23 によると、悪意のある漏えいの大部分（53%）は、金銭目的の攻撃者によるものです。国家主体の脅威アクターは悪意ある漏えいの 13%、ハクティビストは 13% に関与しています。また、悪意ある情報漏えいの 21% は、動機不明の攻撃者によって引き起こされました。

図 24:

悪意ある情報漏えいの平均コスト (脅威アクター・タイプ別)

単位: 100 万米ドル



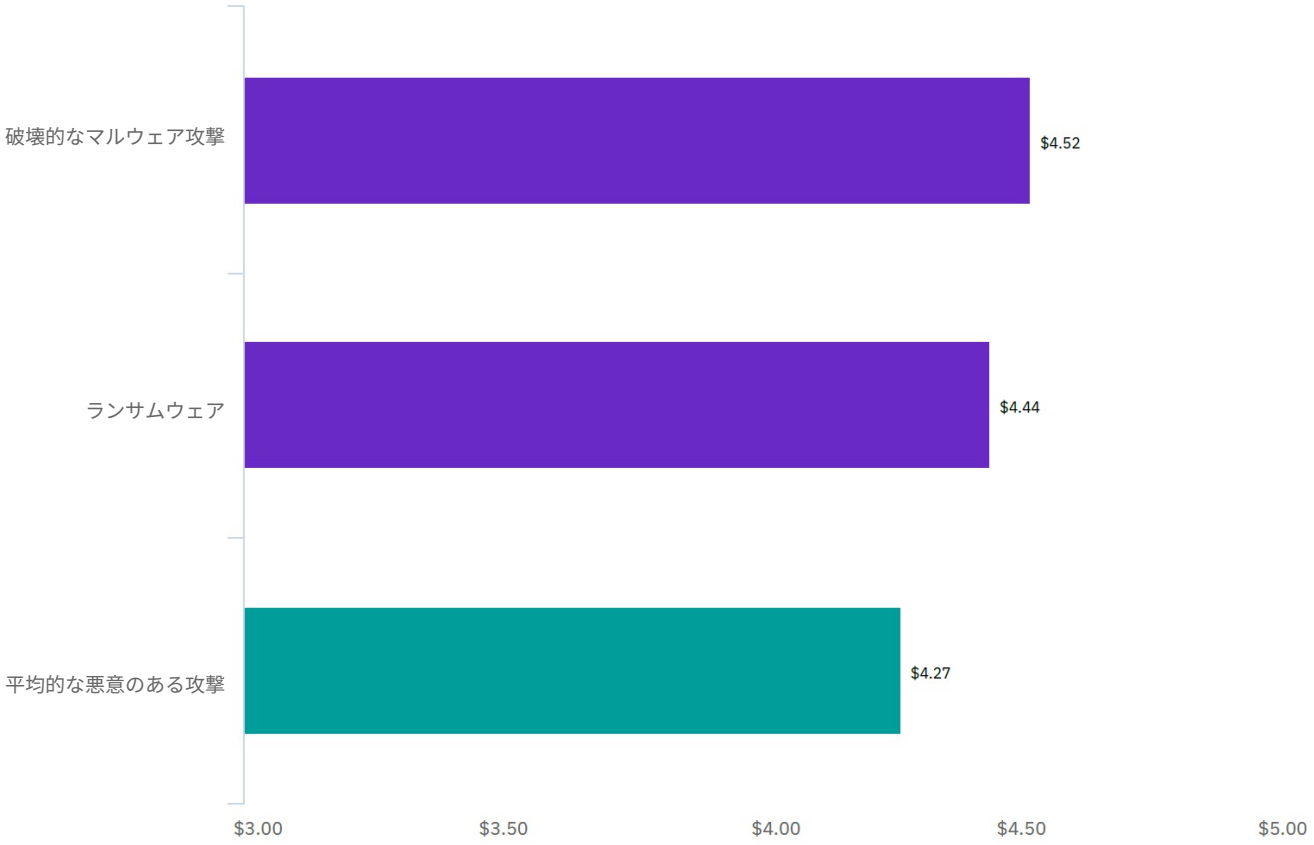
コストが最高なのは、国家主体の攻撃者が引き起こした悪意ある情報漏えい。

図 24 は、攻撃者タイプ別の情報漏えいのコストを示しています。悪意ある漏えいの中で最もコストが高かったのは、国家主体のアクターによって引き起こされたもので、平均 443 万ドルでした。ハクティビストが関与する悪意ある漏えいのコストは平均 428 万 ドルでしたが、金銭目的のサイバー犯罪者による漏えいのコストは、平均 423 万ドルでした。

図 25:

ランサムウェアや破壊的なマルウェアによる漏えいの平均コスト

単位: 100 万米ドル



ランサムウェアや破壊的なマルウェアによる漏えいは、平均的な悪意ある攻撃よりもコストが高い。

図 25 によると、破壊的/ワイパー型の攻撃でデータを破壊する悪意ある攻撃（平均コストは 452 万ドル）とランサムウェア攻撃（444 万ドル）は、平均的な悪意ある漏えい（427 万ドル）や平均的な情報漏えい（386 万ドル）よりもコストが高くなっています。

情報漏えい時に発生するコストに影響を及ぼす要因

このセクションでは、さまざまなセキュリティー・テクノロジーと実践、IT 環境、サード・パーティーの関与など、情報漏えい時に発生するコストに影響を及ぼす多数の要因について詳しく説明します。今年の調査では、軽減（漏えい平均総コストの抑制） または増大（漏えい平均総コストの上昇）のいずれかの影響を与える 25 の固有のコスト要因について分析を行っています。

今年の調査では、コスト抑制要因としてレッドチーム演習、脆弱性検査、マネージド・セキュリティー・サービスが、コスト上昇要因としてセキュリティー・スキルの不足とリモートワーカーが新たに追加されました。

また、情報漏えい時に発生するコストを軽減する効果が示された 3 つの領域、つまり CISO、サイバー保険、インシデント対応チームの役割についても詳しく調べます。

主な調査結果

29 万 1,870 ドル

複雑なセキュリティー・システムによる情報漏えいの平均総コストの増加額

51%

サイバー保険でコンサルティングと法的サービスの費用をカバーするために保険金請求を使用した企業の割合

46%

情報漏えいの責任が最も重いのは CISO であると答えた回答者の割合

図 26:

情報漏えいの平均総コストに対する 25 の主要要因の影響

平均総コスト 386 万ドルからの変化（米ドル）

セキュリティー・システムの複雑さとインシデント対応計画のテストは、情報漏えいの総コストに最も大きな影響を与えた。

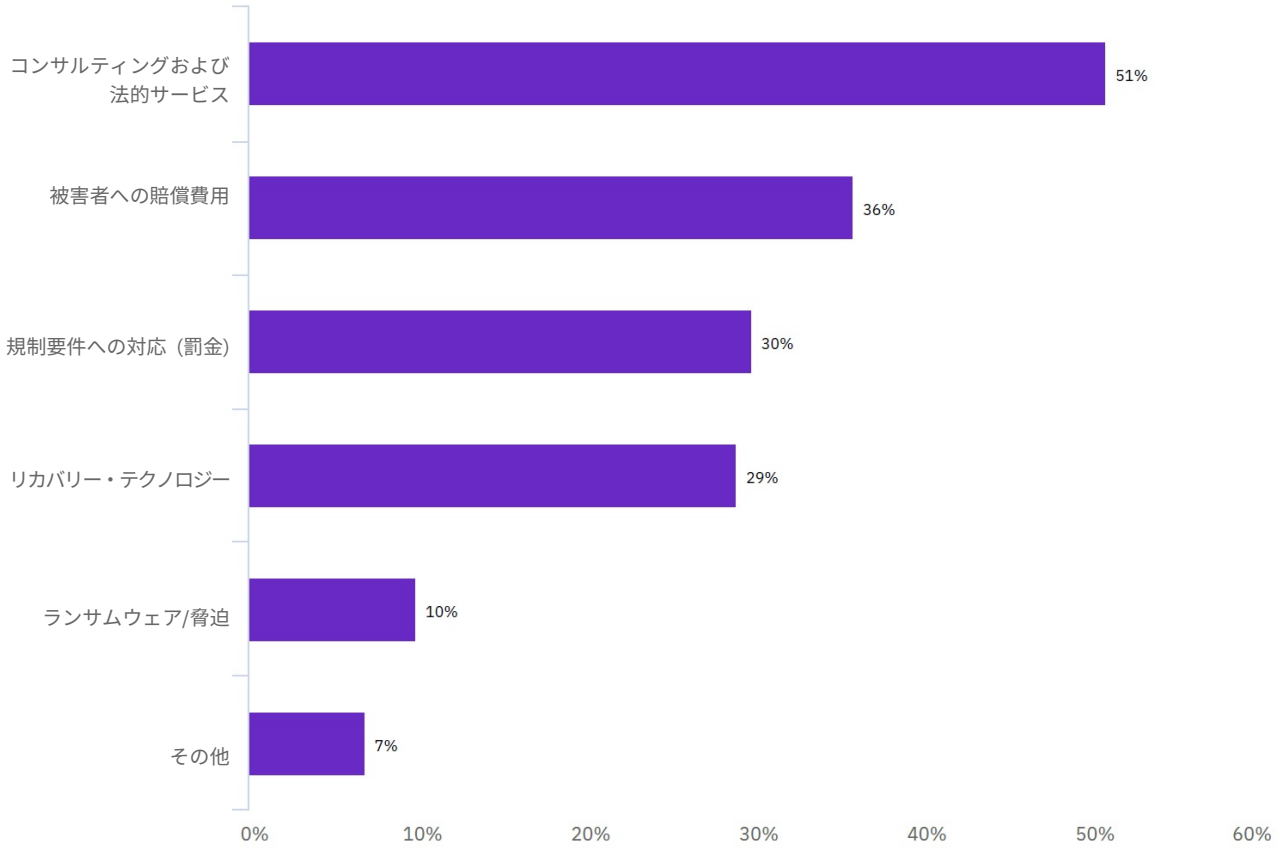
図 26 は、25 の要因の平均コストをリストし、それが情報漏えい時に発生する平均総コスト 386 万ドルにどのように影響するかを示したものです。利用するテクノロジーの数と社内の専門知識の欠如によって生じたセキュリティー・システムの複雑さにより、情報漏えいの平均総コストは平均 29 万 1,870 ドル増加しています。クラウドへの移行を行うと、情報漏えい時に発生するコストが平均よりも高くなり、平均コストは平均 26 万 7,469 ドル増加しました。

情報漏えいの平均総コストを抑制した要因として、インシデント対応計画と事業継続性を管理する広範なテストの実施があります。インシデント対応計画は平均コストを平均 29 万 5,267 ドル、事業継続管理は 27 万 8,697 ドル削減しました。

図 27:

サイバーセキュリティー保険金の請求をして回収されたコストのタイプ

回答の割合、複数回答可



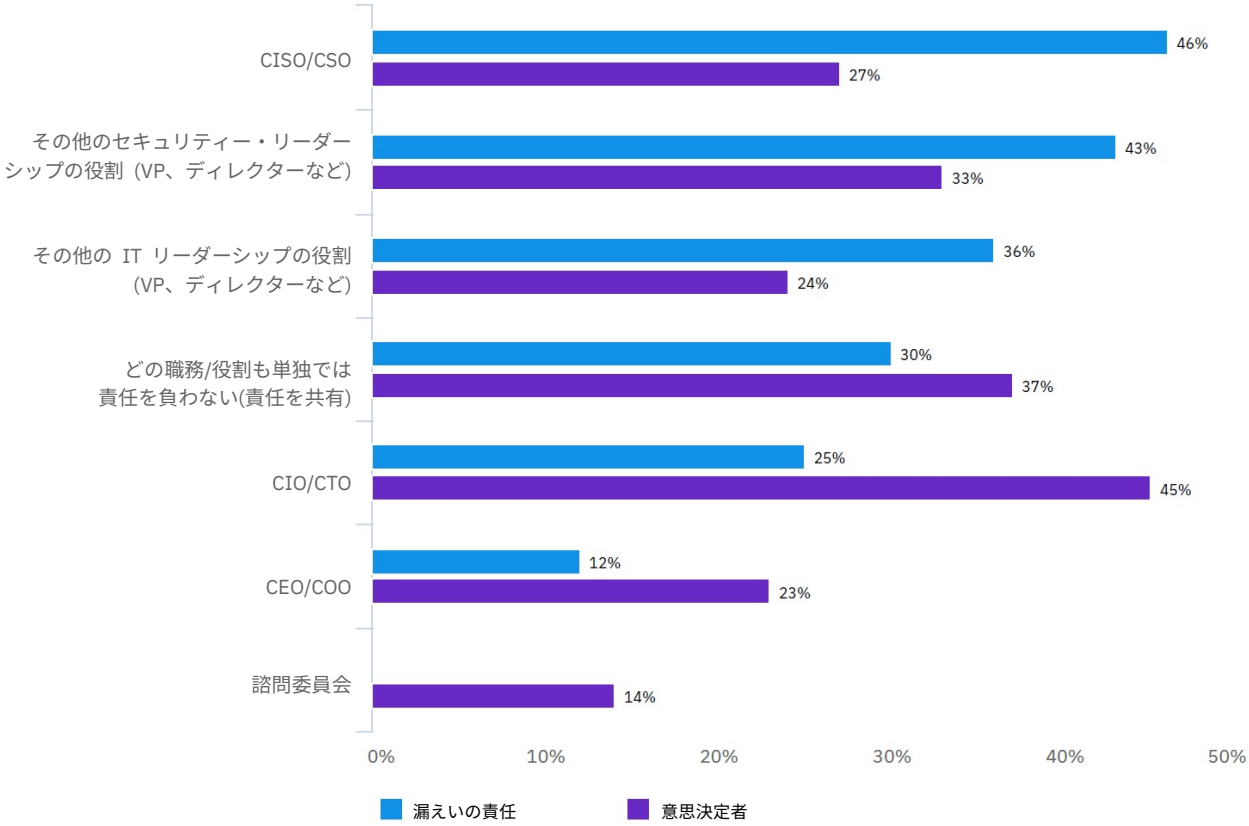
サイバー保険は、ほとんどの場合、サード・パーティー・サービスと被害者の賠償の費用をカバーする。

図 27 によると、サイバー保険に加入している企業の 51% が、保険金請求を使用してサード・パーティーのコンサルティングと法的サービスの費用をカバーしています。企業の 36% は、被害者への賠償費用をサイバー保険でカバーしました。ランサムウェアや脅迫の費用をカバーするために保険金請求を使用したのは、サイバー保険に加入している企業の 10% だけでした。

図 28:

漏えいおよびサイバーセキュリティー・ポリシーとテクノロジーの決定の責任者

回答の割合、複数回答可



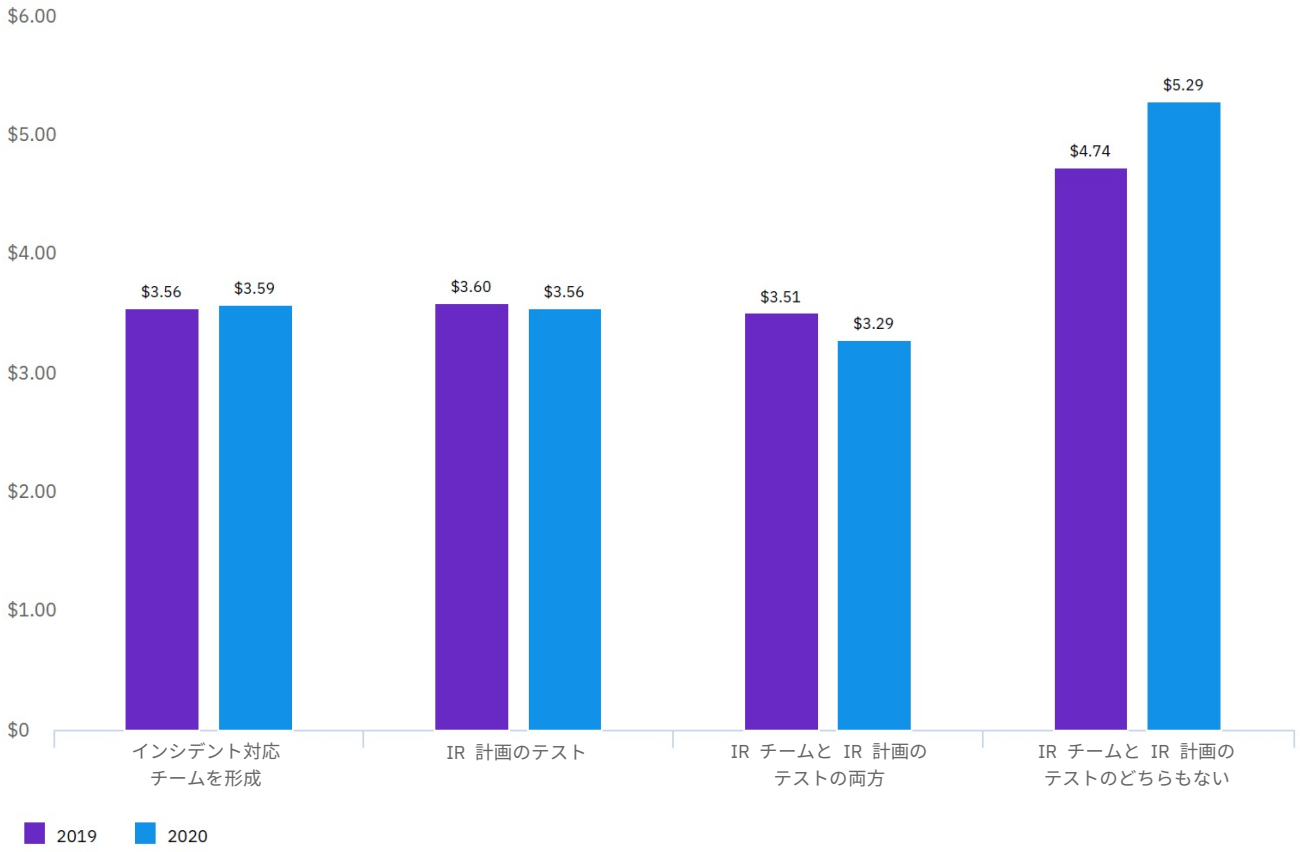
最終的に、情報漏えいの責任があると考えられるのは CISO。

図 28 に示すように、回答者の 46% は、CISO/CSO に情報漏えいの責任があると答えました。しかし、CISO/CSO にサイバーセキュリティー・ポリシーとテクノロジーの決定責任があると答えた回答者は 27% に過ぎませんでした。情報漏えいの責任が CEO と COO にあると考えた回答者は最も少ない結果になりました。また多くの場合、CIO/CTO の役割はサイバーセキュリティーのポリシーとテクノロジーの最終的な決定と考えられています。

図 29:

インシデント対応チームと IR 計画のテストを使用した場合の情報漏えいの平均総コスト

単位: 100 万米ドル



インシデント対応チームとインシデント対応計画のテストを組み合わせることで、情報漏えいのコストが大幅に削減。

図 29 に示すように、インシデント対応チームを組織し、インシデント対応計画のテストを広範に実施した企業は、情報漏えいの平均コストが 329 万ドルでした。対照的に、これらの手順のいずれも行わなかった企業では、平均総コストは 529 万ドルで、その差は 200 万ドルもあります。

セキュリティー自動化のトレンドと効果

今回は、情報漏えいコストとセキュリティー自動化の関係を調査し始めてから 3 年目になります。ここで取り上げるセキュリティー自動化とは、サイバー攻撃や情報漏えいを検知して被害を防止する際に、人的な介入を拡充する、またはそれに置き換わるセキュリティー・テクノロジーという意味です。このようなテクノロジーは、人工知能、機械学習、分析、および自動化オーケストレーションを利用しています。

主な調査結果

21%

2020 年におけるセキュリティー自動化が全面的に導入された企業の割合（2018 年の 15% から増加）

358 万ドル

セキュリティー自動化が導入されていない企業と全面的に導入されている企業の情報漏えい時に発生する平均総コストの差

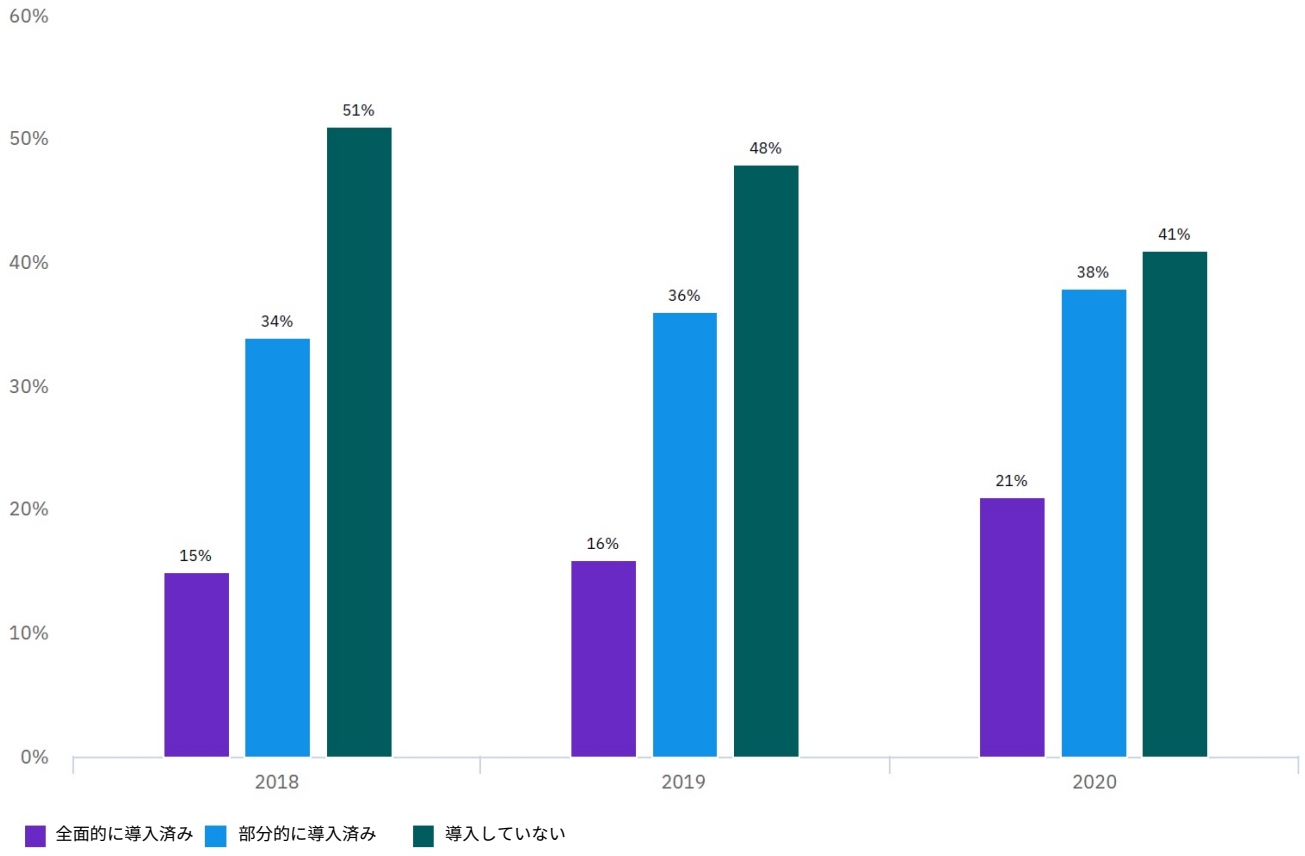
30%

ドイツにおいてセキュリティー自動化が全面的に導入されている企業の割合、すべての国の中で最高

図 30:

3 つの導入レベル別に見たセキュリティー自動化の状況

自動化レベルごとの企業の割合



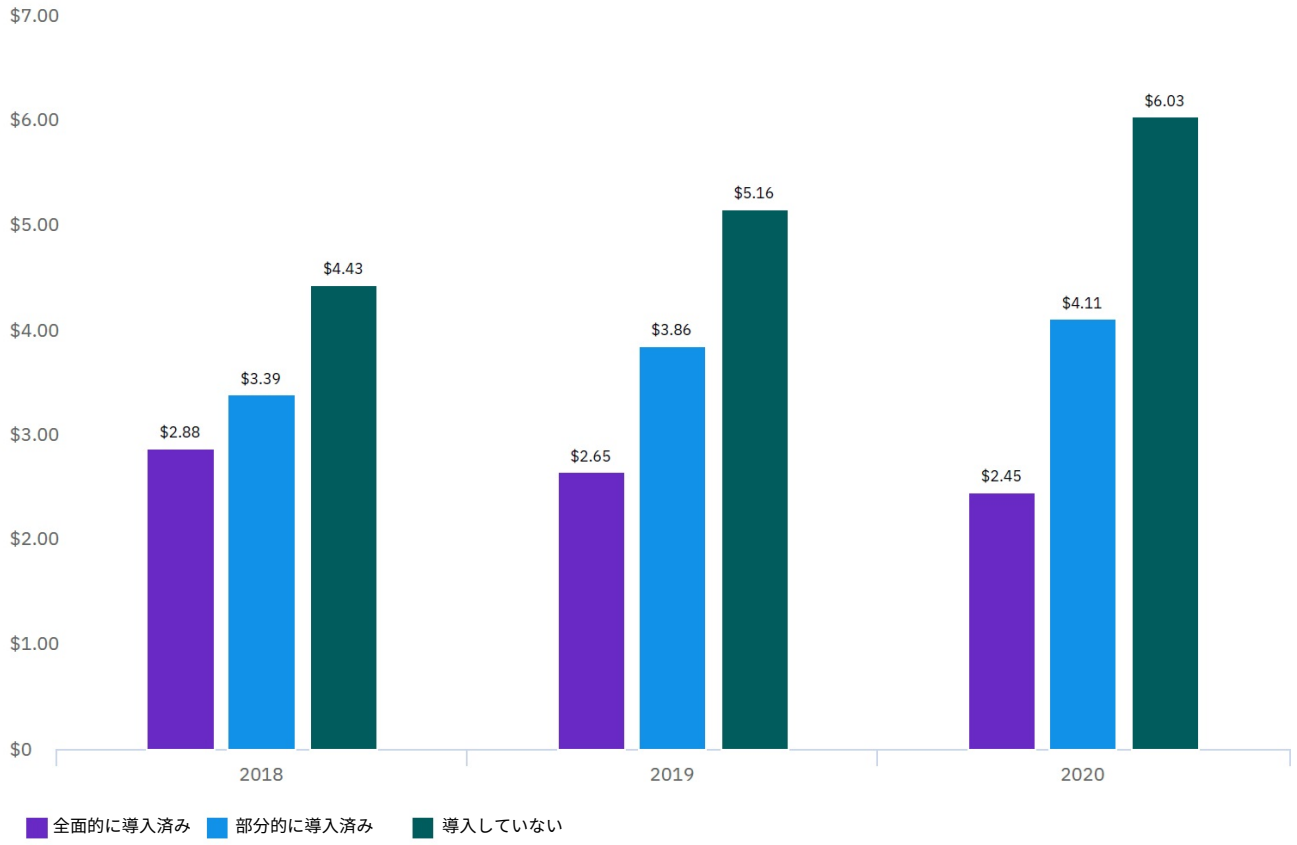
自動化の全面的な導入は、過去 3 年間で増加。

図 30 に示すように、2020 年の調査でセキュリティー自動化の全面的な導入を報告した企業は 21% に過ぎませんが、2018 年の 15% および 2019 年の 16% と比較すると増加しています。2020 年の調査では、他の 38% は自動化を部分的に導入し、41% は自動化を導入していないと報告しています。

図 31:

セキュリティー自動化導入レベル別の情報漏えいの平均総コスト

単位: 100 万米ドル



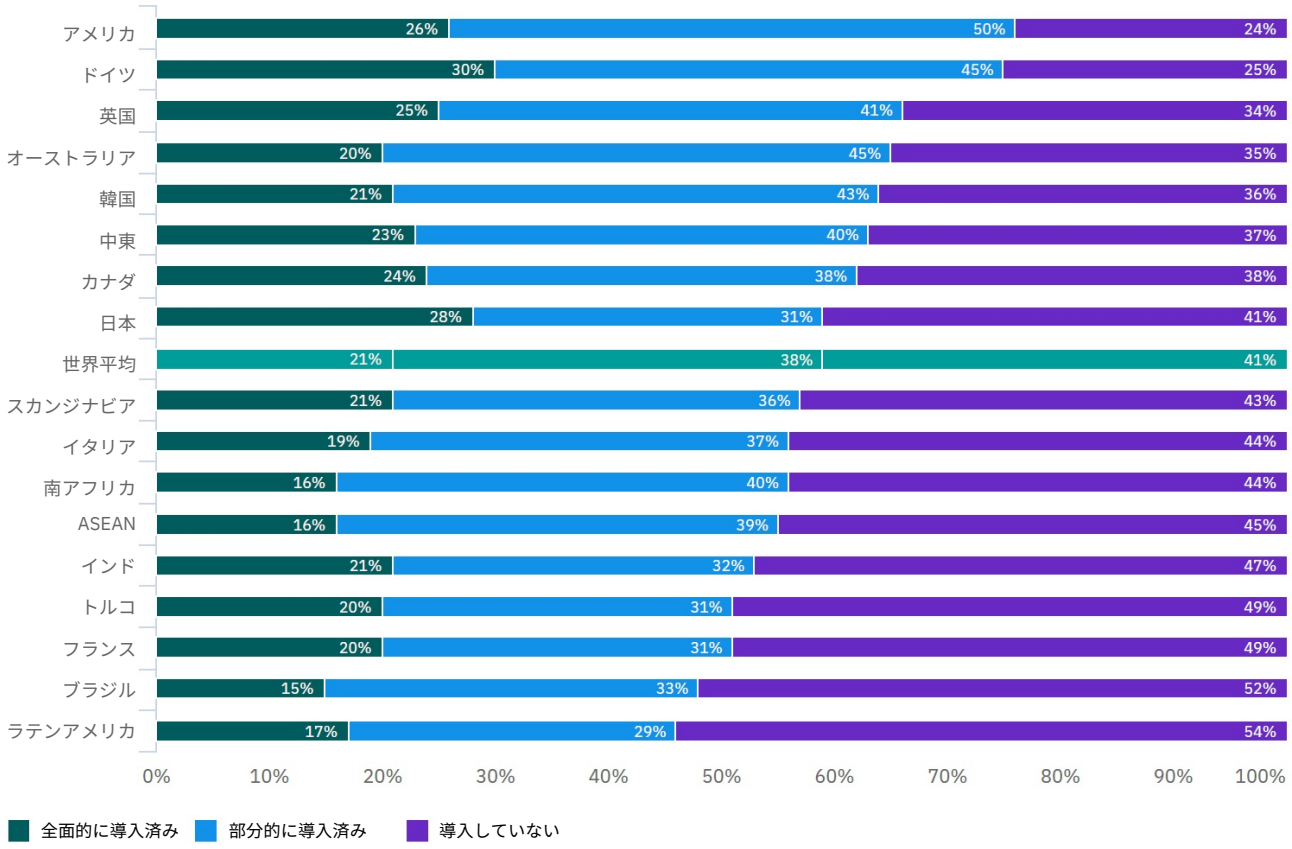
セキュリティー自動化による情報漏えいコストへの影響は、過去 3 年間で増加。

図 31 に示すように、2020 年の調査では、セキュリティー自動化を全面的に導入した企業の情報漏えいの平均総コストは 245 万ドルでした。これは、セキュリティー自動化が導入されていない企業の平均コストより、358 万ドルも少ない数字です。2018 年の調査では、自動化が全面的に導入されている企業と導入されていない企業の漏えい発生時の平均コストの差は 155 万ドルで、2019 年ではその差は 251 万ドルでした。

図 32:

セキュリティー自動化の導入の平均 (国別)

3 つの自動化レベルで表した企業の割合



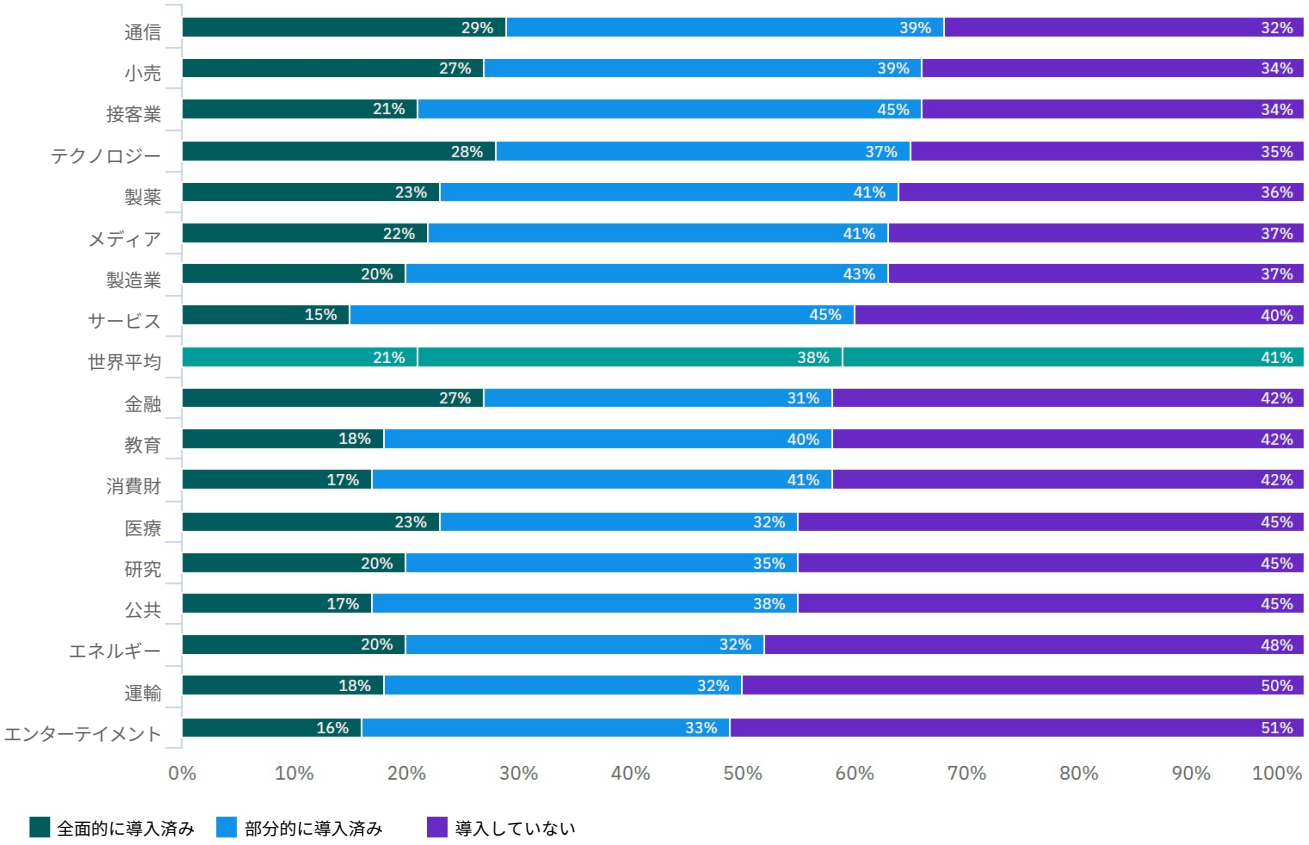
セキュリティー自動化の導入レベルは、国/地域によって異なる。

図 32 によると、自動化が全面的または部分的に導入された企業の割合が高かったのは米国とドイツです (米国では 76%、ドイツでは 75%)。セキュリティー自動化が全面的に導入されている割合は、米国で 26%、ドイツで 30% でした。自動化が導入されていない企業の割合が最も高かったのは、ラテンアメリカとブラジルです (それぞれ 54% と 52%)。

図 33:

セキュリティー自動化の導入状況 (業種別)

3 つの自動化レベルで表した企業の割合



セキュリティー自動化の導入レベルは業種によって異なる。

図 33 に示されているように、通信、テクノロジー、小売の業種では、自動化が全面的または部分的に導入されている企業の割合が最も高くなっています。金融機関では、セキュリティー自動化が全面的に導入されている企業の割合が平均より高くなっています (27%)。しかし、自動化が部分的に導入されている企業の割合は比較的低くなっています (31%)。つまり、自動化が全面的および部分的に導入されている金融機関の割合を合わせると、世界平均を下回ります (世界平均が 59% であるのに対し、金融機関は 58%)。エンターテイメントと輸送では、自動化を導入していない企業の割合が最も高くなっています。

情報漏えいの検知と被害拡大防止にかかる時間

過去数年間、この調査では情報漏えいの検知と被害拡大防止に早く取りかかれば、それだけコストを抑制できることを示してきました。検知の平均時間とは、インシデントの発生を検出するのに要する時間を表します。被害拡大防止にかかる時間とは、インシデントが検出されてから状況を解決し、最終的にサービスを復元するのに要する時間を指します。

漏えいが最初に検出されてから被害拡大防止が実施されるまでの経過時間を、情報漏えいのライフサイクルと呼びます。企業のインシデントへの対応プロセスと被害拡大防止プロセスの効果を測定するために、これらの測定基準を使用できます。今年の調査で初めて、情報漏えいのライフサイクルに対するセキュリティー自動化の影響について、調査を実施しました。

主な調査結果

280 日

情報漏えいの検出と被害拡大防止にかかる平均時間

315 日

悪意のある攻撃によって引き起こされた情報漏えいの検出と被害拡大防止にかかる平均時間

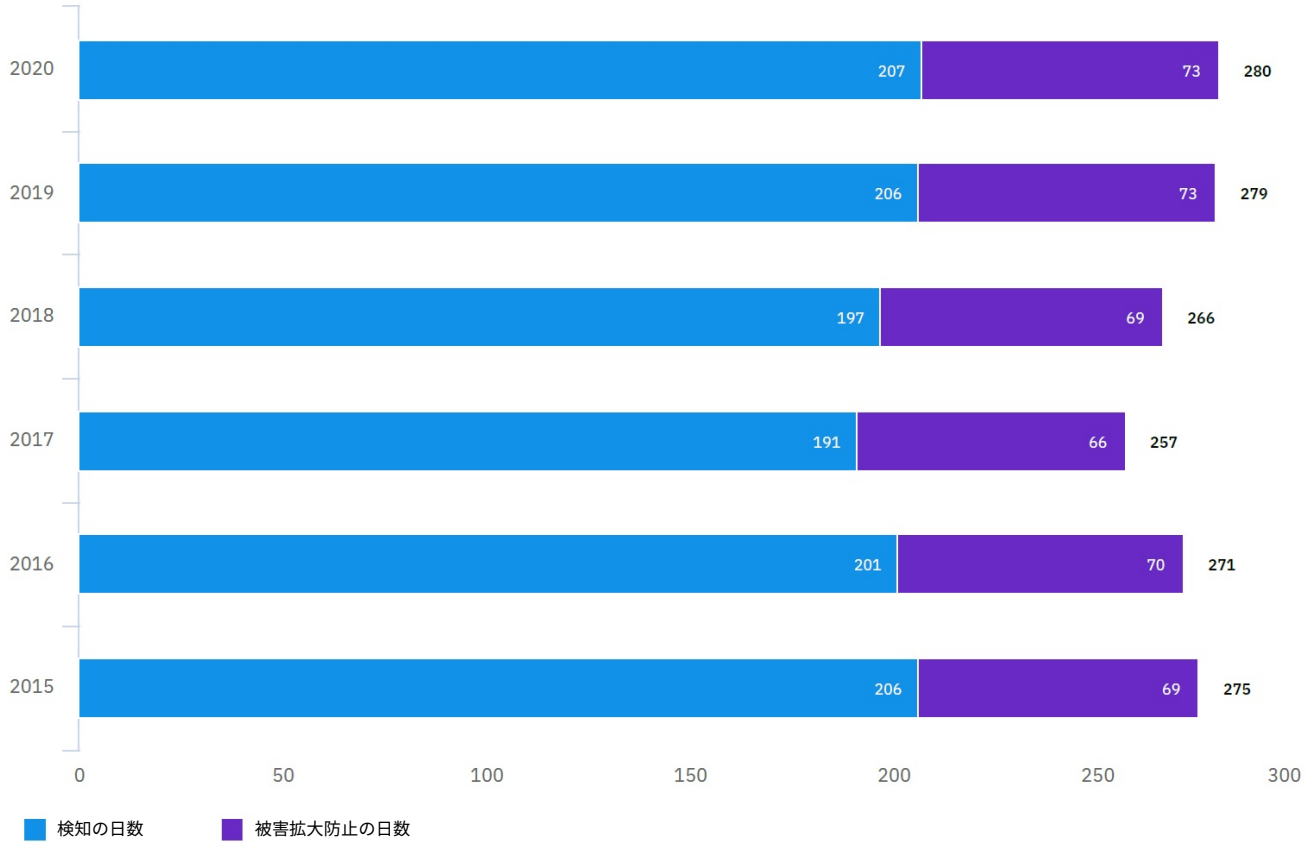
112 万ドル

被害拡大防止にかかる時間が 200 日未満の場合に、200 日超の場合と比較した平均コスト節減額

図 34:

情報漏えいの検知と被害拡大防止にかかる平均時間

単位: 日数



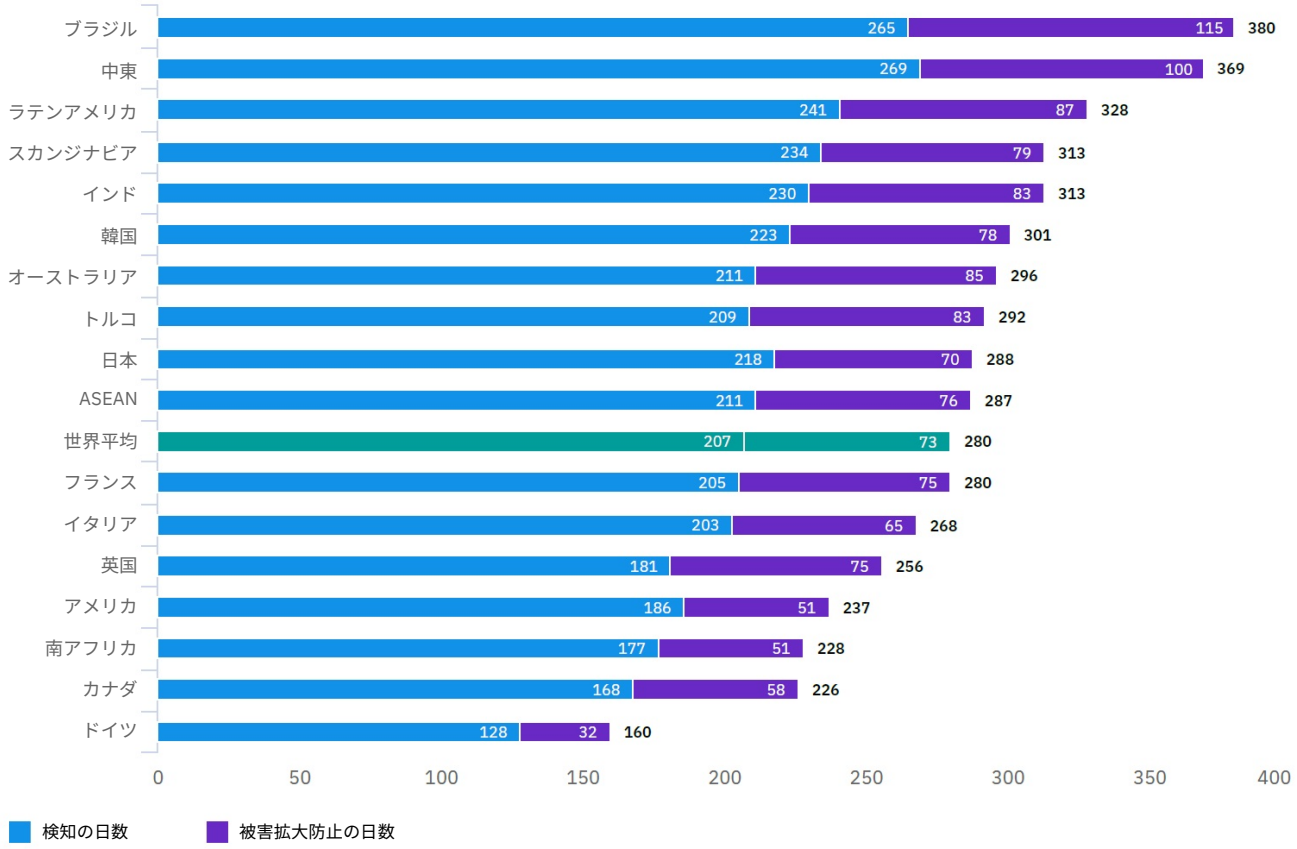
漏えいの検知と被害拡大防止にかかる平均時間は一貫している。

図 34 に示すように、過去のいくつかのレポートでは、情報漏えいの検知までの時間と被害拡大防止の時間に大きな変化はありません。2020 年の調査では、検知までの平均時間は 207 日、被害拡大防止までの平均時間は 73 日で、合計 280 日間でした。2019 年の情報漏えいライフサイクルの合計は 279 日でした。

図 35:

情報漏えいの検知と被害拡大防止にかかる平均時間（国/地域別）

単位: 日数



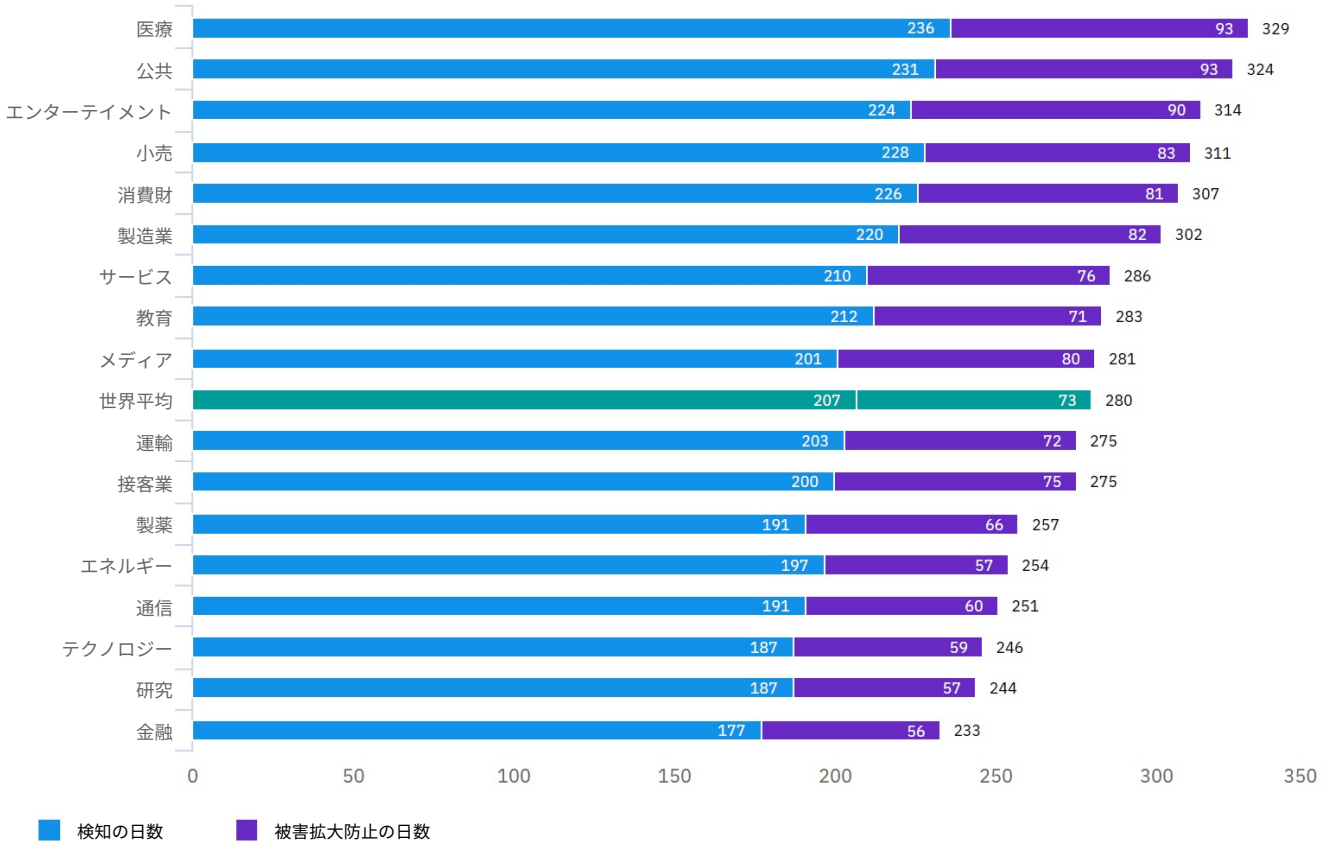
漏えいの平均ライフサイクルは国/地域間で大きく異なる。

図 35 によると、ブラジルと中東では、情報漏えいの検知と被害拡大防止にかかる時間が平均よりはるかに長く、それぞれ平均 380 日と 369 日でした。一方、南アフリカ、カナダ、ドイツでは情報漏えいのライフサイクルが非常に短く、ドイツの企業では被害拡大防止までにかかった平均時間はたったの 160 日でした。

図 36:

情報漏えいの検知と被害拡大防止にかかる平均時間（業種別）

単位: 日数



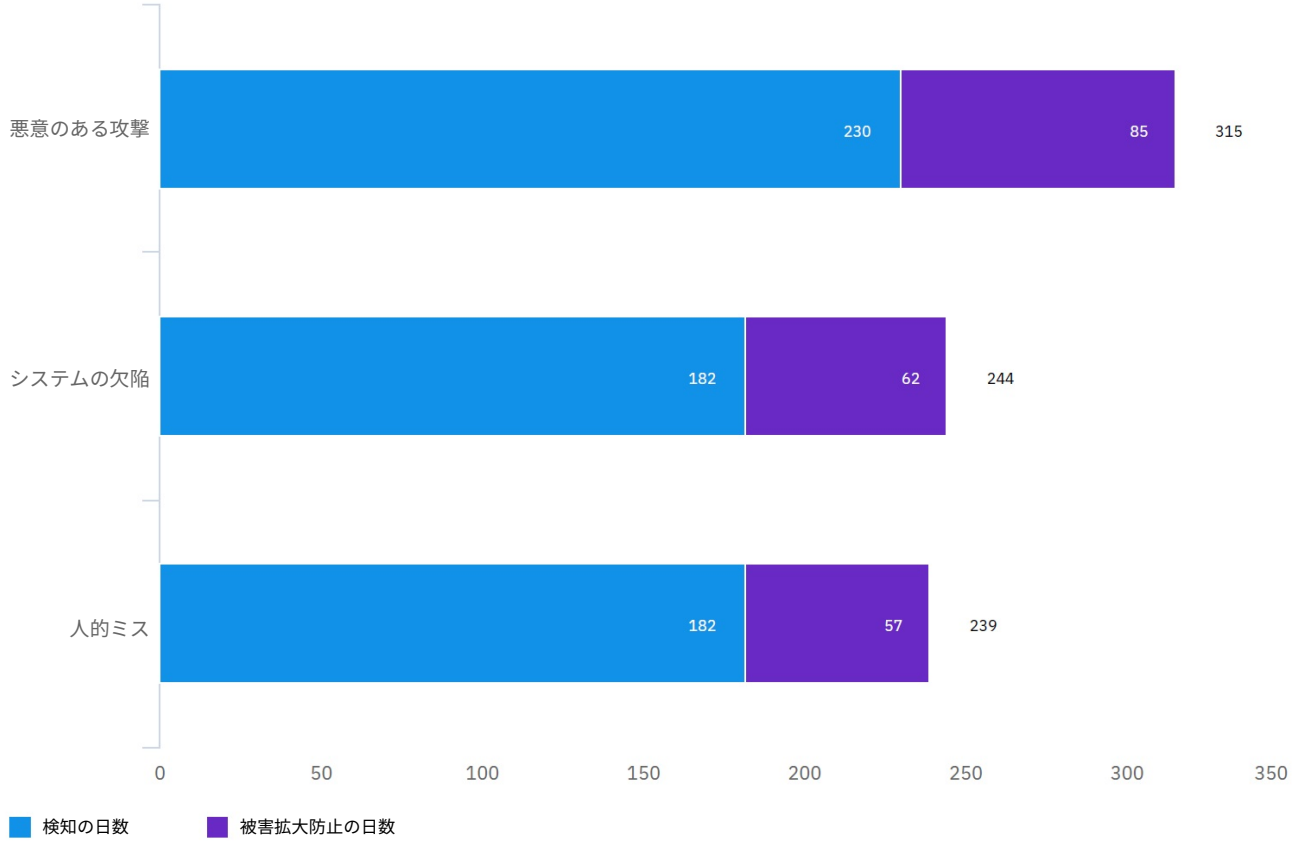
金融業界と医療業界では、漏えいの検知と被害拡大防止にかかる時間に非常に大きな開きがある。

図 36 に示されているように、医療業界では漏えいの検知と被害拡大防止にかかる平均時間が最も長く、329 日でした。金融業界では、漏えいの検知と被害拡大防止にかかる平均時間が最も短く、233 日でした。9 つの業種が平均を上回り、8 つの業種は世界の漏えいライフサイクルの平均時間である 280 日を下回りました。

図 37:

情報漏えいの検知と被害拡大防止にかかる平均時間（根本原因別）

単位: 日数



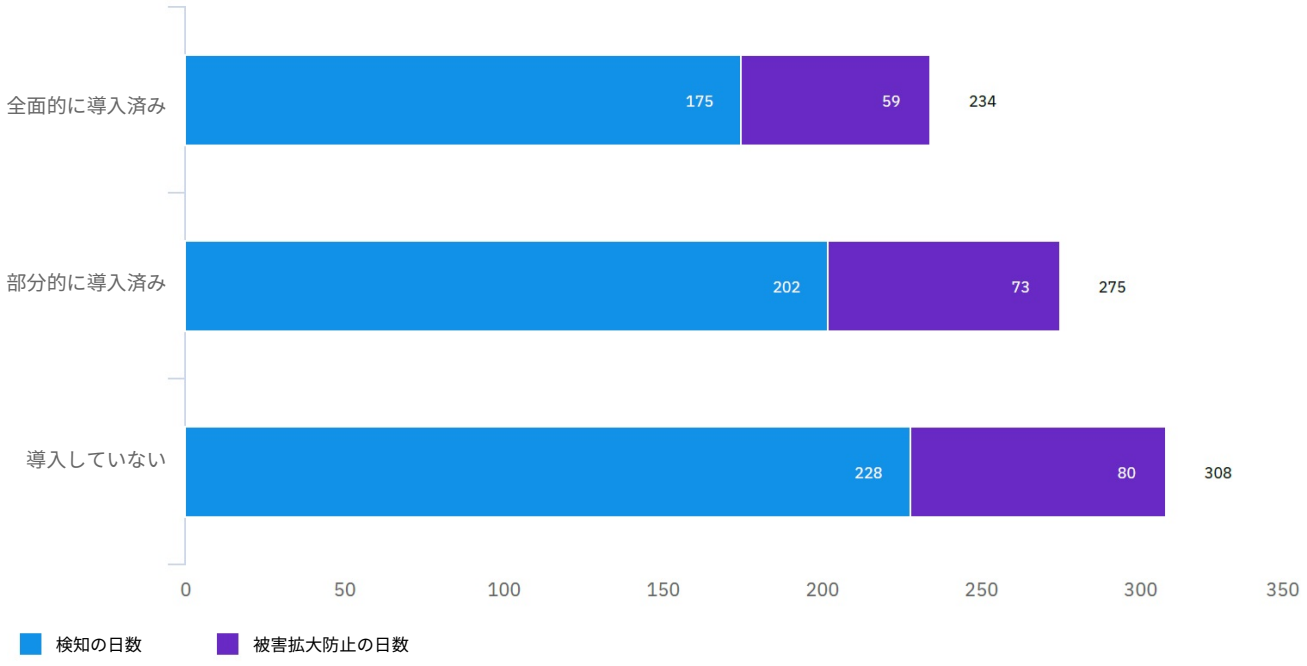
悪意のある攻撃によって引き起こされた漏えいの検知と被害拡大防止には、最も長い時間がかかった。

図 37 に示すように、2020 年の調査では、悪意のある情報漏えいの検知と被害拡大防止には、平均 315 日かかっています。他の根本原因による漏えいを比較してみましょう。システムの欠陥による漏えいの検知と被害拡大防止には平均 244 日、人的ミスによって生じた漏えいの検知と被害拡大防止には 239 日かかりました。悪意ある情報漏えいの検知に要する日数は、情報漏えいの平均より 23 日長くなっています。悪意のある情報漏えいの検知には平均 230 日かかり、全体平均は 207 日です。

図 38:

情報漏えいの検知と被害拡大防止にかかる平均時間（セキュリティー自動化レベル別）

単位: 日数



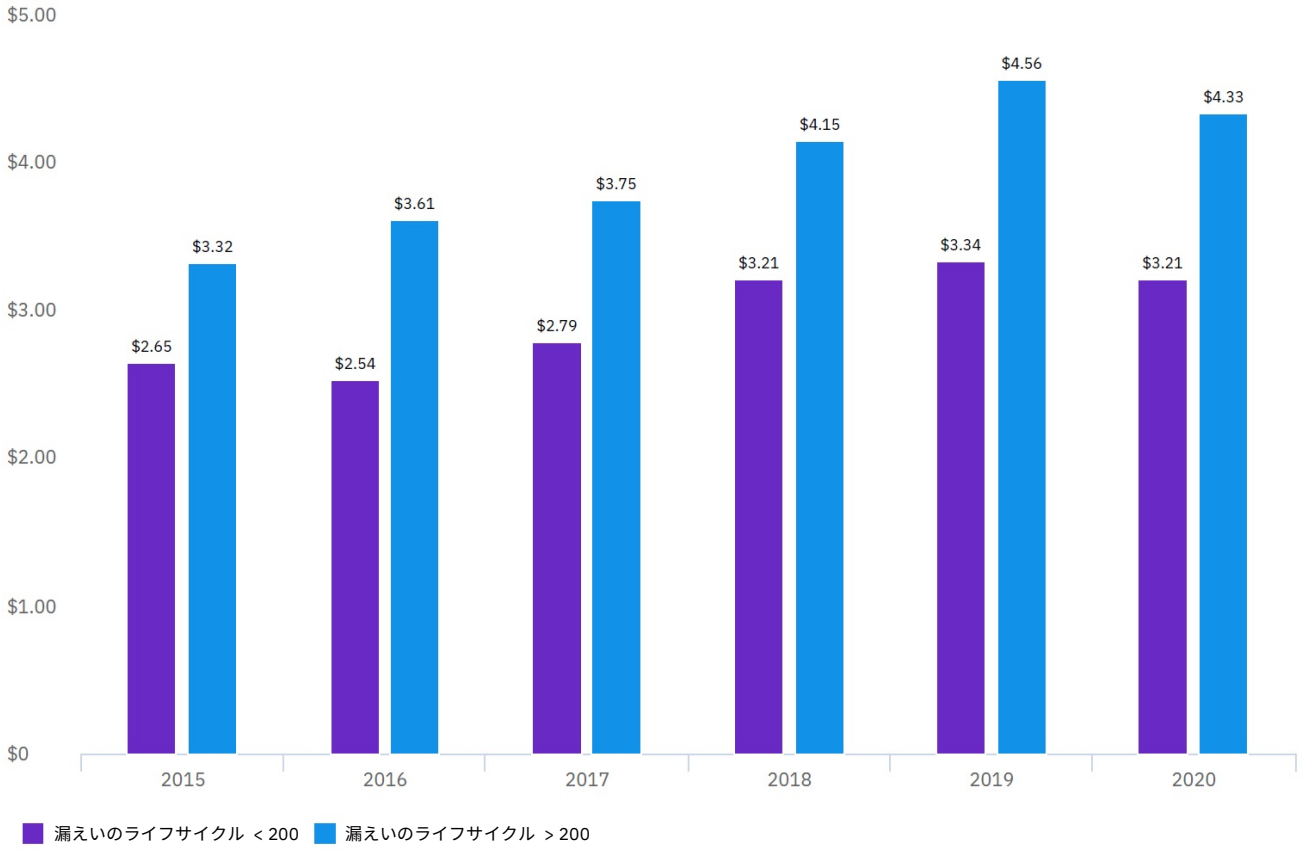
セキュリティー自動化により、情報漏えいの検知と被害拡大防止に必要な時間が短縮。

この調査では、情報漏えいライフサイクルに対する自動化の影響についての調査を初めて実施しました。**図 38** によると、自動化が全面的に導入されている場合、検知までの時間は平均 175 日、被害拡大防止にかかる時間は平均 59 日です。自動化を導入しなかった場合、この数値は大幅に増加し、漏えいの検知に平均 228 日、被害拡大防止に 80 日、合計で 308 日かかっています。

図 39:

平均的な情報漏えいライフサイクルに基づく、情報漏えい時に発生する平均総コスト

単位: 100 万米ドル



情報漏えいライフサイクルは、平均漏えいコストに影響を与える。

過去 6 年間の調査では、ライフサイクル (漏えいの検知と被害拡大防止にかかる時間) が 200 日を超える漏えいは、ライフサイクルが 200 日未満の漏えいよりも、はるかにコストが高いことが常に示されています。**図 39** に示すように、2020 年の調査に注目すると、ライフサイクルが 200 日を超える漏えいの平均コストは、ライフサイクルが 200 日未満の漏えいの平均コストより 112 万ドル上回っています (200 日超では 433 万ドルに対し、200 日未満では 321 万ドル)。

情報漏えい時に発生するロングテール・コスト

情報漏えいのコストへの影響は、漏えい発生後も数年間続く可能性があります。昨年の調査では、2 年以上の期間に情報漏えいのコストが組織にもたらす影響を初めて調査しました。分析によると、漏えい後の最初の 1 年間で最大コストを記録しますが、2 年後に再び増加する傾向がありました。

そこで、規制の厳しい業界の企業における漏えいと、データ保護規制が緩やかな業界の企業における漏えいの「ロングテール・コスト」の差を調べました。規制が厳しい業種には、エネルギー、医療、消費財、金融、テクノロジー、製薬、通信、公共セクター、教育が含まれる、と定義しました。一方、小売、製造、エンターテイメント、メディア、研究、接客業界の企業は、規制が緩やかな環境にあると見なしました。規制の厳しいカテゴリーと緩やかなカテゴリーの業種を分析した結果、漏えい後の数年間に、規制コストと法的コストがコスト増加の要因になった可能性があるという結論に達しました。

2020 年の調査では、2 年以上の情報漏えいコストが発生した 101 社を調査しました。

主な調査結果

61%

初年度に発生した情報漏えいコストの割合の平均

44%

規制の厳しい業種で初年度に発生した情報漏えいコストの割合の平均

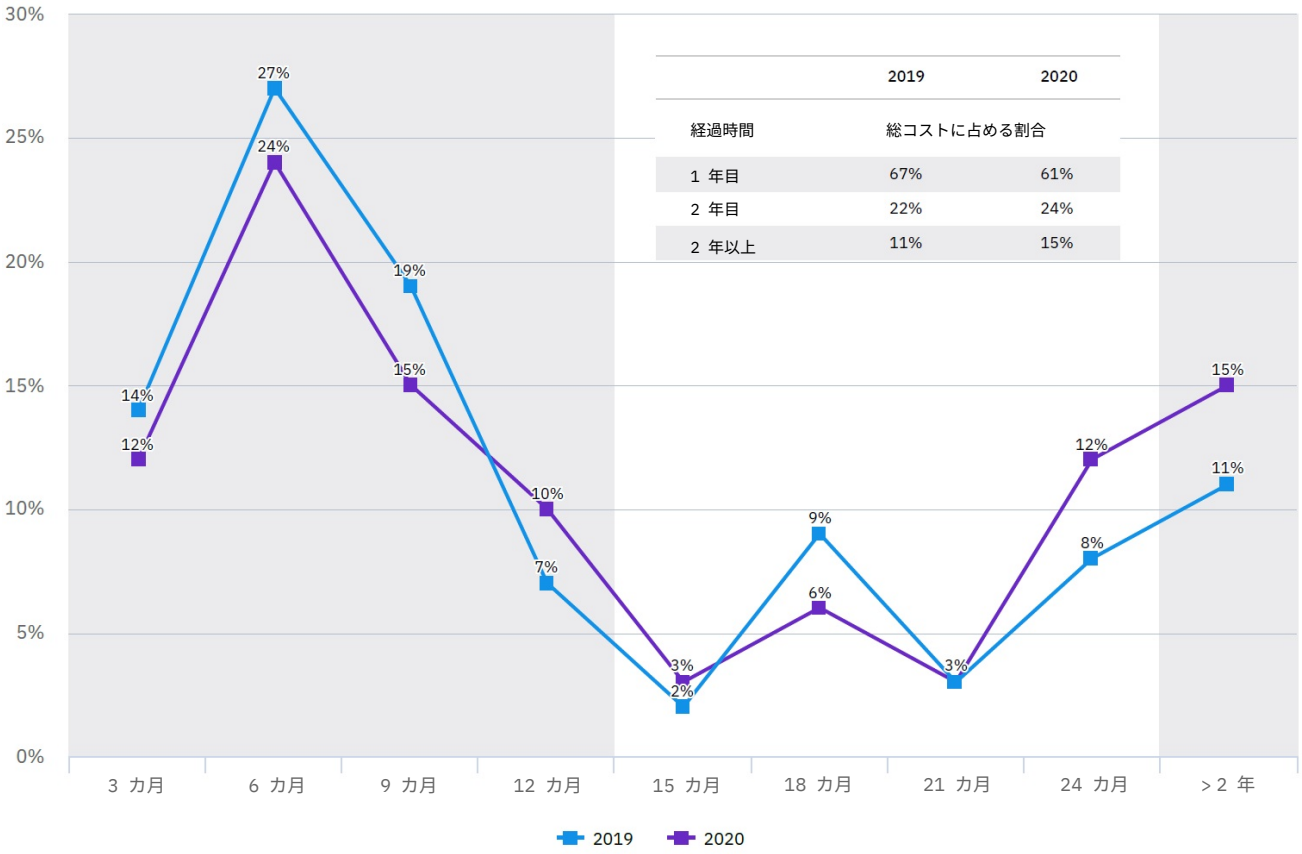
92%

規制が緩やかな業種で最初の 2 年間に発生した情報漏えいコストの割合の平均

図 40:

2 年以上の期間における情報漏えいコストの平均分布

3 カ月間隔で発生したコストの割合



経過時間	総コストに占める割合 2019	2020
1 年目	67%	61%
2 年目	22%	24%
2 年以上	11%	15%

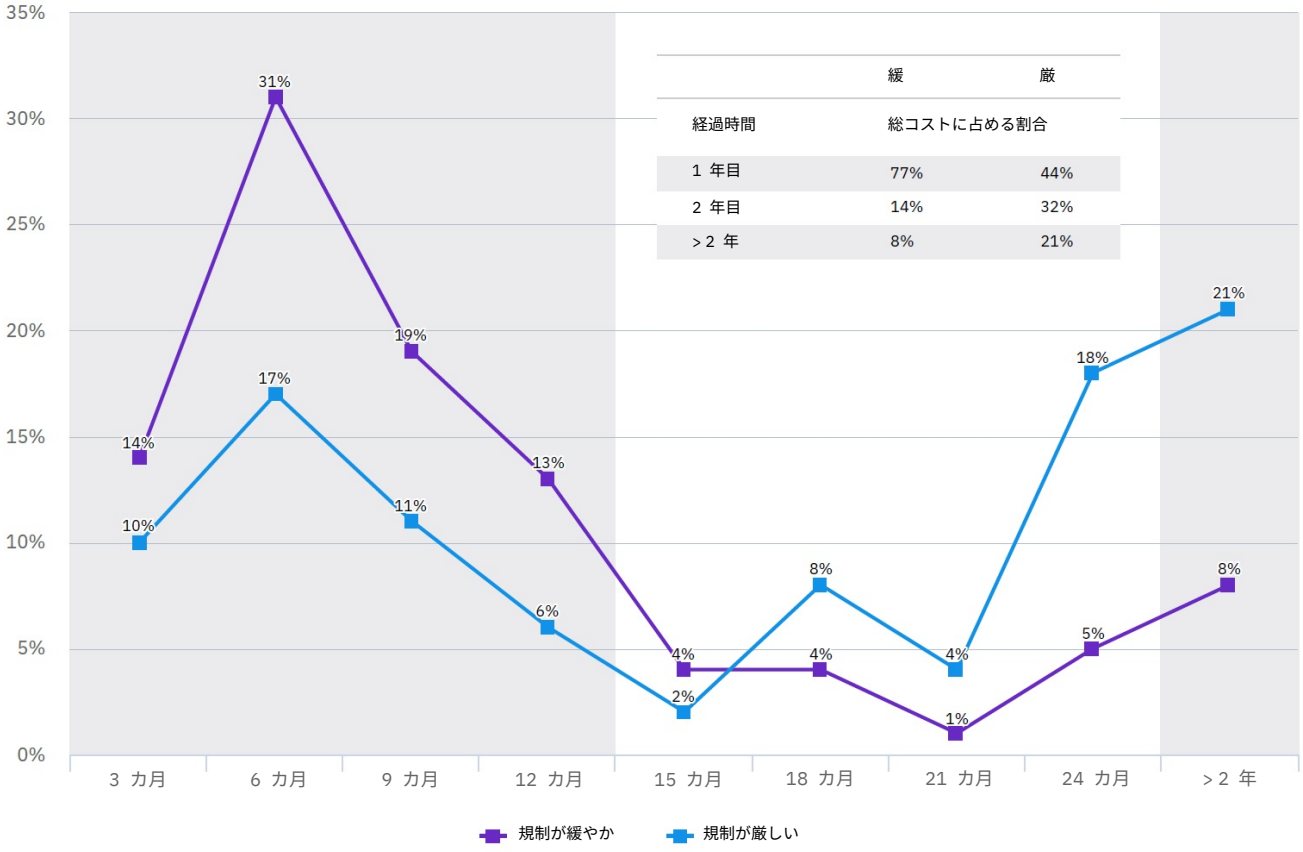
2020 年の調査では、2 年経過後に発生した漏えいコストの割合が増加。

図 40 によると、ロングテール・コスト分析では、情報漏えいコストの平均 61% が 1 年目に発生し、2 年目に 24%、3 年目以降に 15% 発生しています。2019 年の分析では、漏えいから 3 年目のコストは 11% の増加だったことと比べると、微増であると言えます。

図 41:

規制が緩やかな環境と規制が厳しい環境における情報漏えいコストの経年分布

3 カ月間隔で発生した総コストの割合



	緩	厳
経過時間	総コストに占める割合	
1 年目	77%	44%
2 年目	14%	32%
> 2 年	8%	21%

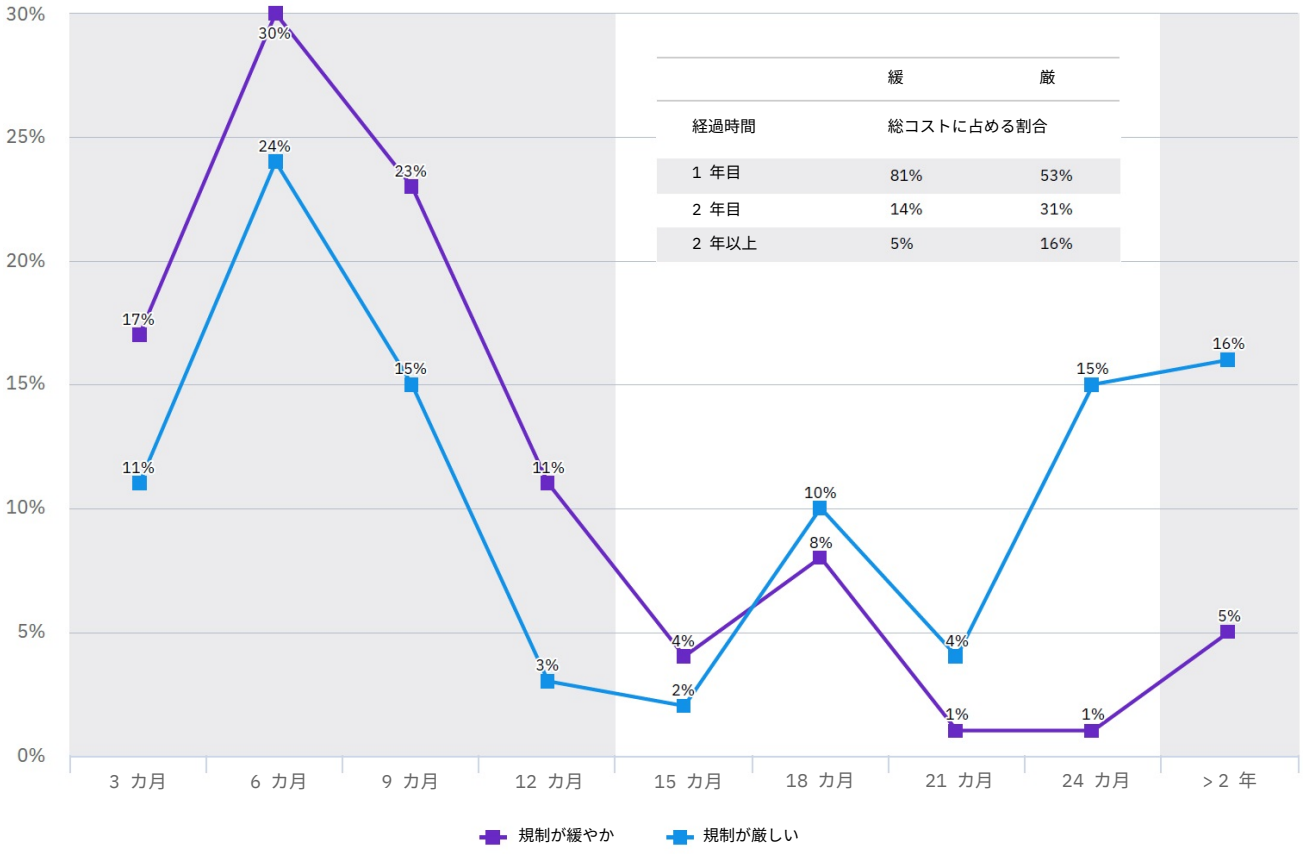
規制が厳しい業種における漏えいでは、コストの大部分が 2 年目以降に発生。

図 41 によると、規制が緩やかな環境にある企業では、最初の 1 年間で情報漏えいコストがすべて発生する可能性が非常に高くなります。規制が厳しい企業で漏えい後 1 年以内に発生するコストの平均は 44% ですが、規制が緩やかな業種では 1 年目に平均 77% のコストが発生しています。

図 42:

2019 調査年度における、規制が緩やかな環境と規制が厳しい環境での情報漏えいコストの経年分布

3 カ月間隔で発生した総コストの割合



	緩	厳
経過時間	総コストに占める割合	
1 年目	81%	53%
2 年目	14%	31%
2 年以上	5%	16%

規制が緩やかな環境と規制が厳しい環境の 2019 年の分析によると、漏えいから 3 年目に発生するコストの割合が低くなっている。

図 42 は、2019 年の調査でのデータ保護規制環境が緩やかな場合と厳しい場合のロングテール漏えいコストを示しています。2019 年の調査によると、規制が厳しい業種では平均 16% のコストが 3 年目に発生しました。これは、2020 年の調査における規制が厳しい業種の 3 年目のコスト (21 %) に対応します (図 41 を参照)。

新型コロナウイルス感染症の潜在的な影響

新型コロナウイルス感染症の拡大は、多くの企業の働き方を変革しました。多くの従業員が在宅勤務をするようになり、ビデオ会議、クラウド・アプリケーション、ネットワーク・リソースの需要が高まっています。この新しい現実を理解するために、補足的な調査を行い、新型コロナウイルス感染症が情報漏えいコストに及ぼす潜在的な影響について調査参加企業の意見を集めました。

主な調査結果

54%

新型コロナウイルス感染症への対応としてリモートワークが必要になった企業の割合

76%

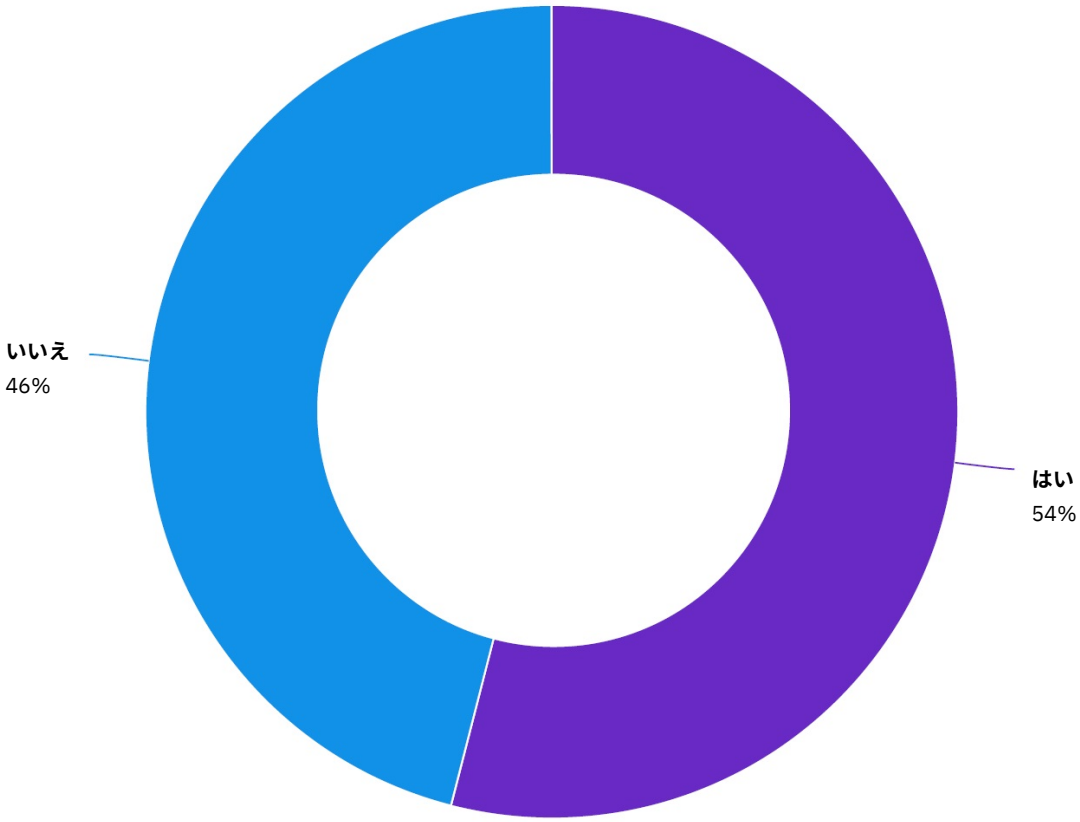
リモートワークにより、情報漏えいの検知と被害拡大防止のための時間が増えると回答した参加企業の割合

70%

リモートワークにより、情報漏えいコストが増えると回答した参加企業の割合

図 43:

企業が 新型コロナウイルス感染症への対応として従業員にリモートワークを要求した割合

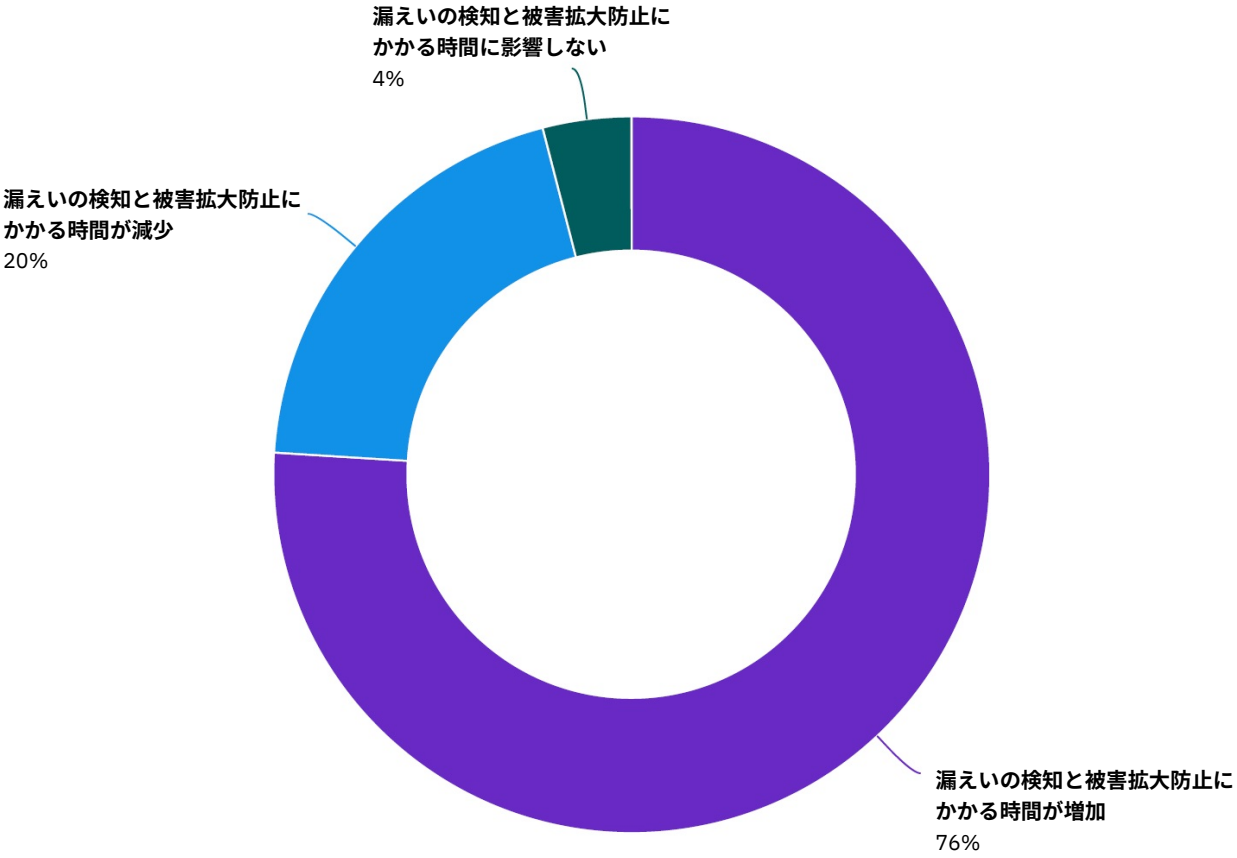


大部分の企業では、新型コロナウイルス感染症への対応としてリモートワークが必要になった。

図 43 に示すように、調査対象の企業の大多数（54%）は、新型コロナウイルス感染症の拡大への対応としてリモートワークが必要になりました。

図 44:

リモートワークが情報漏えいへの対応能力に与える影響

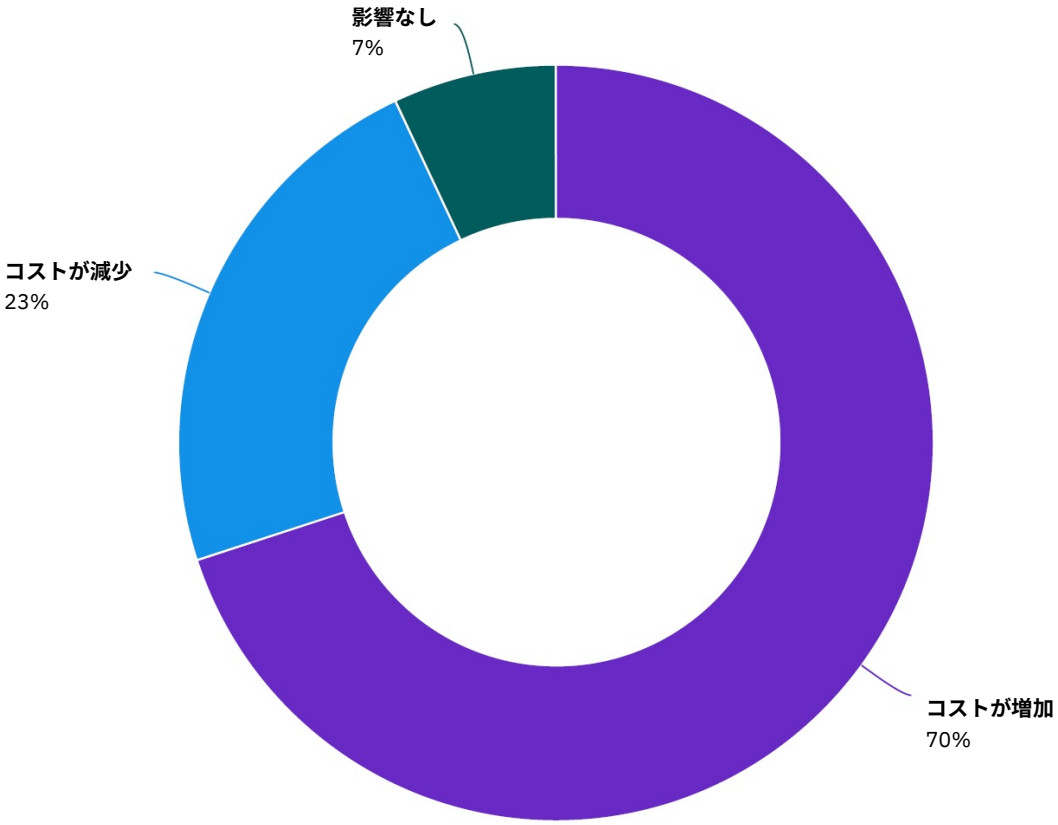


参加企業の 4 分の 3 は、情報漏えいの検知から被害拡大防止までの時間がさらに長くなると予測。

図 44 によると、新型コロナウイルス感染症への対応としてリモートワークが必要と回答した参加企業のうち 4 分の 3 以上（76%）が、情報漏えいの検知と被害拡大防止にかかる時間が増加すると回答しました。また、20% が漏えいの検知と被害拡大防止にかかる時間が減少すると回答し、4% は影響はないと回答しました。

図 45:

リモートワークが情報漏えいコストに与える影響



リモートワークにより、今後の情報漏えいコストが増加する見込み。

図 45 によると、新型コロナウイルス感染症への対応としてリモートワークが必要と回答した参加企業の 70% が、今後情報漏えいが発生したときはそのコストが増加するだろう、と述べています。さらに 23% は、リモートワークにより情報漏えいコストが削減されると回答し、7% は影響はないと回答しました。

大規模な情報漏えいのコスト

被害レコードが 100 万件を超える大規模な漏えいのコストを調査し始めてから、今回で 3 年目になります。多くの企業にとって、大規模な漏えいは日常的に起こるものではありませんが、これは消費者と業界に非常に大きな影響を与えます。2018 年の調査でこの分析を導入して以来、大規模漏えいの平均コストは増加の一途をたどっています。

今年の調査は、100 万 件以上のレコードの紛失や盗難を伴う情報漏えいの被害に遭った 17 社の分析に基づいています。分析方法の完全な説明については、このレポートの最後にある「情報漏えい時に発生するコストに関する FAQ」を参照してください。

主な調査結果

3 億 9,200 万ドル

5,000 万件を超えるレコードの漏えいの平均コスト

100 倍

5,000 万件を超えるレコードの漏えいと平均的な情報漏えいの平均コストの差

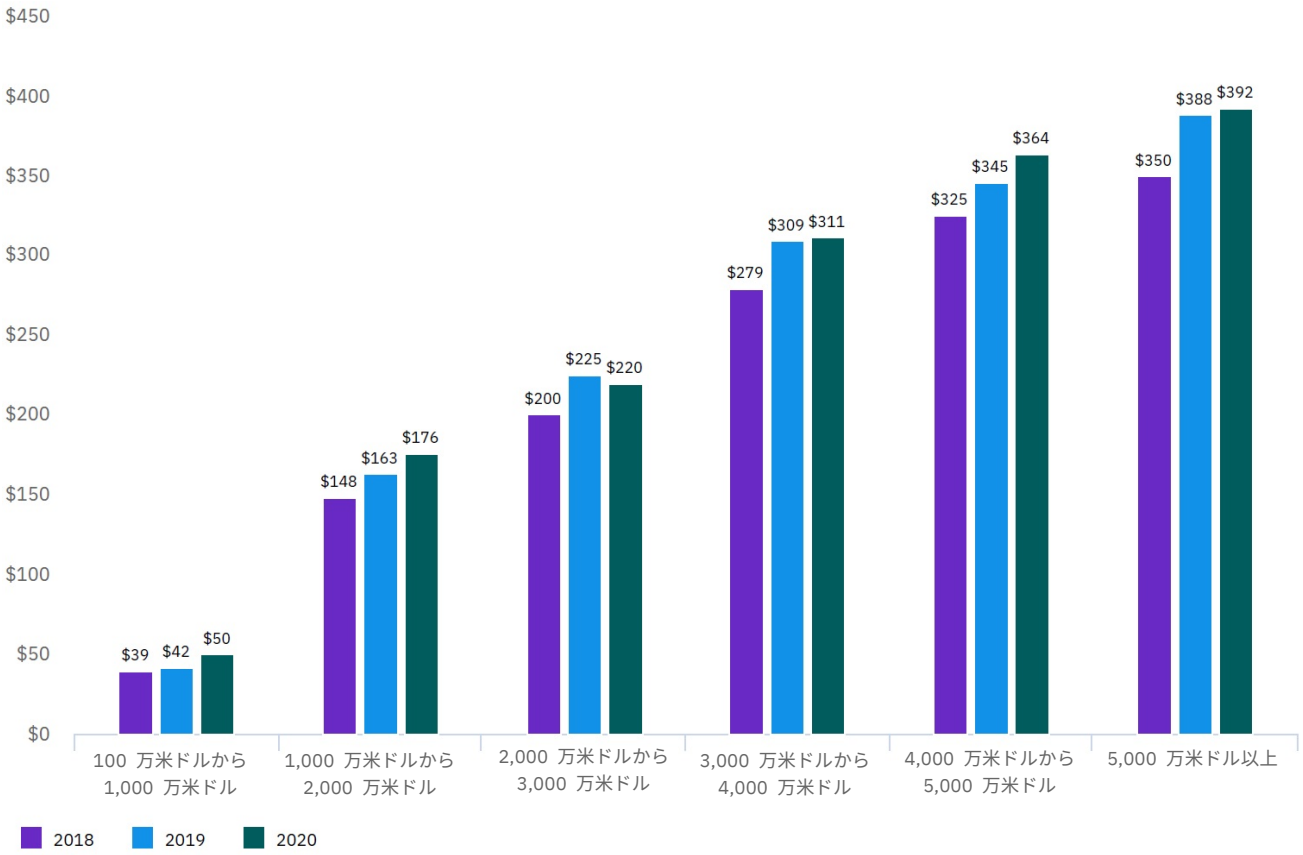
1,900 万ドル

2019 年と 2020 年の調査における、4,000 万〜 5,000 万件のレコードの漏えいの平均コストの増加

図 46:

大規模な情報漏えいの平均総コスト（漏えいしたレコード件数別）

単位: 100 万米ドル



大規模漏えいのコストはさらに急上昇。

図 46 によると、100 万～ 1,000 万件のレコードの漏えいには、平均 5,000 万ドルのコストがかかります。これは、10 万件未満の漏えいの平均コスト（386 万ドル）の 25 倍以上に相当します。100 万から 1,000 万件のレコードの漏えいコストが最大の増大率で上昇し、2018 年の平均 3,900 万ドルから 2020 年の 5,000 万ドルへと 22% も増大しました。

5,000 万件を超えるレコードの漏えいでは、平均コストは 3 億 9,200 万ドルで、情報漏えいの平均コストの 100 倍以上でした。コストの増加が明らかに最大だったのは、5,000 万件を超えるレコードの漏えいでした。これは、2018 年には平均 3 億 5,000 万ドルだったのに対し 2020 年には 3 億 9,200 万ドルに増加しました。

情報漏えいが財務および企業ブランドに与える影響を最小限に抑えるための手順

*このセクションでは、調査対象の企業が情報漏えいの財務的なコストとブランドへの影響を削減するために実施した対策について IBM セキュリティーが概説します。**

Security Orchestration, Automation and Response (SOAR) を活用して、検出と対応時間を改善する。

情報漏えいコストの調査では、セキュリティー自動化の導入により、漏えいを検知して対応するための平均時間と平均コストが大幅に削減されることが分かりました。SOAR ソフトウェアおよびサービスは、自動化、プロセスの標準化、および既存のセキュリティー・ツールとの統合により、企業がインシデント対応を加速できるよう支援します。人工知能、アナリティクス、自動オーケストレーションなどの自動化テクノロジーはすべて、情報漏えいコストを平均以下にする効果がありました。

ゼロトラスト・セキュリティー・モデルを採用して、機密データへの不正アクセスを防止する。

調査結果によると、情報漏えいの最も一般的な根本原因は、資格情報の紛失や盗難、およびクラウドの構成ミスです。企業はリモートワークや分離されたハイブリッド・マルチクラウド環境を組み込むように移行しています。そこで、ゼロトラスト戦略を採用して、適切なコンテキストでのみ限定的にアクセスを許可することで、データとリソースを保護することができます。

インシデント対応計画のストレス・テストを実施して、サイバー・レジリエンスを高める。

インシデント対応 (IR) チームを組織し、インシデント対応計画をテストしている調査対象企業は、IR チームを組織せず、IR 計画もテストしていない企業と比較して、情報漏えいの平均総コストを 200 万ドルも節減しています。「訓練は実践のごとく、実践は訓練のごとく」という名言は、攻撃に対して迅速かつ効果的に対応するビジネスの能力を最適化するために、インシデント対応戦略を開発およびテストすることを意味します。

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

エンドポイントとリモートワーカーを保護および監視するのに役立つツールを使用する。

この調査では、新型コロナウイルス感染症の拡大への対応としてリモートワークを導入した企業の 70% が、情報漏えい時に発生するコストが増加すると考えていました。統合エンドポイント管理 (UEM) およびアイデンティティー/アクセス管理 (IAM) 製品とサービスを使用すると、セキュリティー・チームは社内の不審なアクティビティーや、企業が物理的にアクセスできないエンドポイントを含む持ち込みの (BYO) 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、および IoT をより深く把握できます。これにより、被害を分離して封じ込めるための調査および対応時間を短縮できます。

ガバナンス、リスク管理、コンプライアンスに投資する。

検知とエスカレーションのコストは、機会損失コストに続き、本調査の情報漏えいコストの中で 2 番目に大きなカテゴリーでした。監査、全社的なリスク評価、ガバナンス要件を用いたコンプライアンスの追跡のための内部フレームワークは、情報漏えいの検知と被害拡大防止の取り組みのエスカレーションに向けた企業の能力向上に役立ちます。

IT およびセキュリティー環境の複雑さを最小限に抑える。

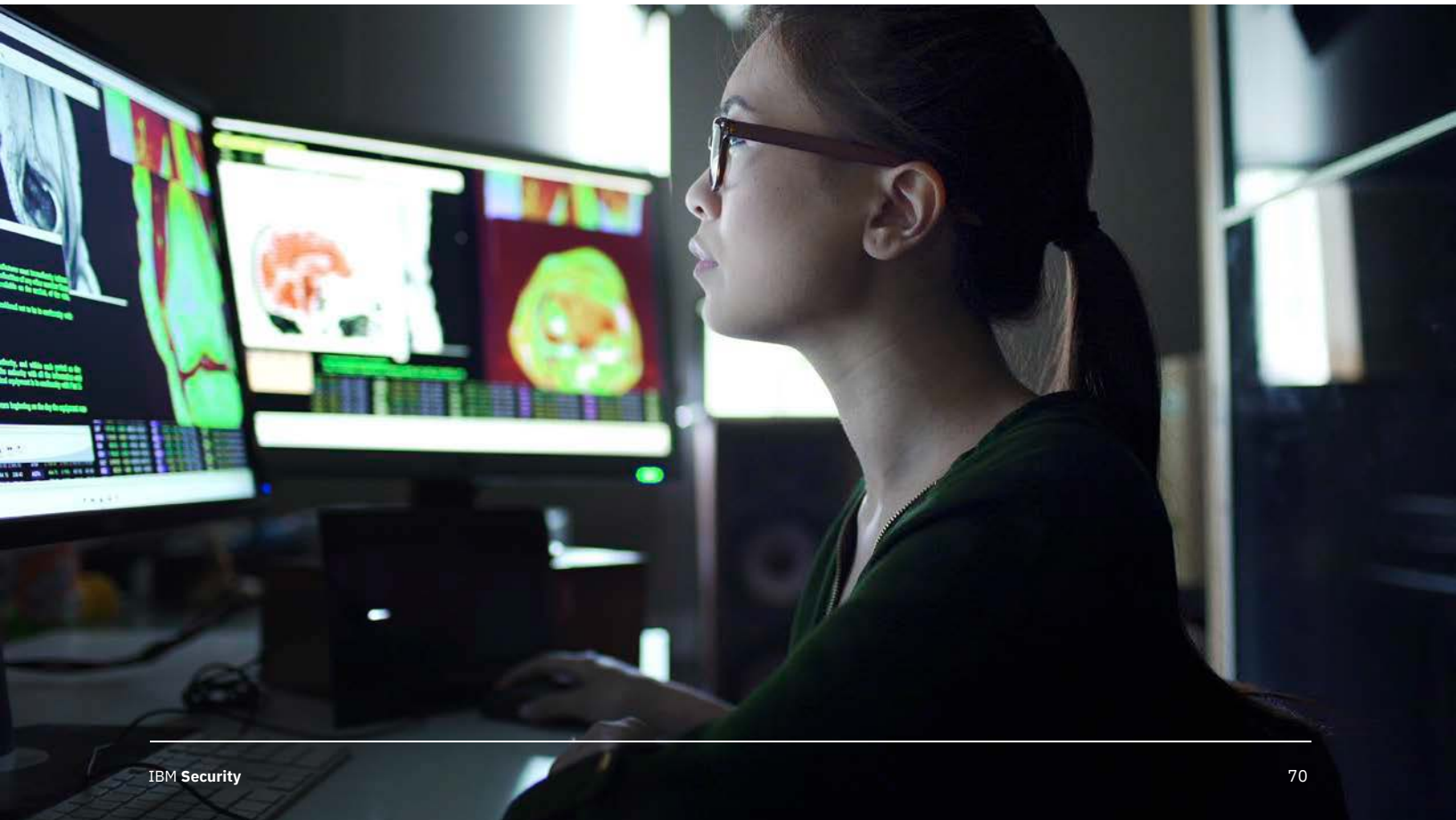
今年の調査では、25 のコスト要因の中で、セキュリティー・システムの複雑さが、平均的な情報漏えいコストの増加をもたらす最大の要因でした。サード・パーティー、クラウドへの大規模移行、および IoT/OT 環境が原因で発生する情報漏えいも、情報漏えいコストの増加に関連していました。異種システム間でデータを共有できるセキュリティー・ツールは、セキュリティー・チームが複雑なハイブリッド・マルチクラウド環境全体でインシデントを検出するのに役立ちます。

ポリシーとテクノロジーを使用して、クラウド環境で機密データを保護する。

クラウド環境でホストされるデータの量と価値が高まっているため、企業はクラウドでホストされる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。データ分類スキーマおよび保存プログラムを使用して、情報漏えいに対して脆弱な機密情報の可視性を高め、その量を減らし、暗号化を使用して保護します。脆弱性スキャン、侵入テスト、およびレッドチームを使用して、クラウドでホストされているデータベースの脆弱性の暴露や構成ミスを特定します。この調査では、これらのソリューションはすべて、平均的な情報漏えいコストの削減に結び付いています。

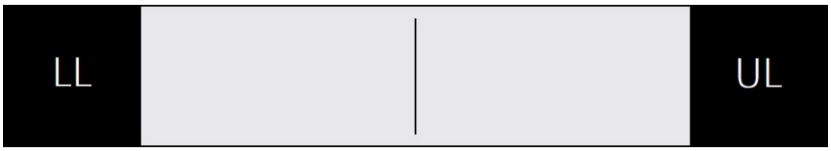
マネージド・セキュリティー・サービスを使用して、セキュリティー・スキルのギャップを埋める。

調査対象の企業は、セキュリティー・スキルの不足を情報漏えいコストの増加をもたらす主要な要因の 1 つとして特定していますが、マネージド・セキュリティー・サービスは平均的な情報漏えいコストの削減に結び付きます。マネージド・セキュリティー・サービス・プロバイダーは、継続的な監視と統合されたソリューションおよびサービスにより、セキュリティーとリスクを簡素化できます。



調査方法

情報機密を保持するために、ベンチマーク文書では企業が特定できるような情報を一切収集していません。機密保持のために、企業は情報漏えいに関する実際の会計情報は提供していません。それに代わる手法として、参加企業は数直線形式で定義された可変の範囲にマークを付ける方法で直接コストの概算を記入しました。参加企業には、コスト・カテゴリーごとに、数直線の上限と下限の間に点を 1 つ付けるよう依頼しました。



カテゴリーごとに具体的な推定額を 1 つ記入してもらう代わりに、数直線に基づいて数値を取得することで、情報の機密性が保たれ、回答率も高くなります。ベンチマーク文書の次の段階では、間接コストと機会損失コストの推定値を入力するよう調査回答者に依頼しました。

ベンチマークでは、プロセスが煩雑にならないよう、情報漏えい時に発生するコスト評価に欠かせないと判断した業務のコスト・センターだけを慎重に選び、対象項目に設定しました。専門家との協議を通して、必要なコスト関連業務を含む一連の項目が最終決定されました。ベンチマーク情報の収集では、一貫性と包括性を保つため、各文書が繰り返し検証されました。

個人情報の取り扱いを伴う幅広い業務運用に対応するよう、ベンチマーク文書に記載された情報漏えい時に発生するコスト項目の範囲は、一般的に知られているコスト・カテゴリーだけに限定されています。今回の調査では、データ保護業務や個人情報のコンプライアンス業務を対象とせず、ビジネス・プロセス関連業務だけに注目したことで、高品質な結果が得られたと確信しています。

情報漏えい時に発生するコストに関する FAQ

情報漏えいとはどのようなことですか。
情報漏えいとは、個人の名前、医療情報や金融資産情報あるいはデビット・カードが、電子形式/紙形式を問わず、危険にさらされる事象のことと定義されています。調査に含まれる情報漏えいでは、被害レコードが 3,400 ～99,730 件の範囲に及んでいます。

被害レコードとはどのようなものですか。
レコードとは、情報漏えいにおいて情報が紛失や盗難に遭った人（個人）を特定する情報です。例として、個人の名前、クレジット・カード情報、およびその他の個人情報（PII）を含むデータベースがあります。別の例として、医療保険会社における契約者の名前や支払情報を含む医療記録があります。

データの収集方法を教えてください。
調査員は、2019 年 8 月から 2020 年 4 月までの間に情報漏えいの被害に遭った 524 社の企業で、3,200 件以上の個別の聞き取り調査を個人に行い、詳細な定性データを収集しました。調査対象企業の募集は 2019 年 10 月に開始し、聞き取り調査は 2020 年 4 月 21 日に完了しました。調査では、IT、コンプライアンス、情報セキュリティーの担当者と面談しました。いずれも、各社の情報漏えいとその対応に要したコストについて詳しい方々です。プライバシー上の理由により、企業固有の情報は収集していません。

コストの計算方法を教えてください。
情報漏えいの平均コストを計算するために、企業が負担した直接経費と間接経費の両方の情報を収集しました。直接経費にはフォレンジックの専門家への依頼、ホットライン・サポートの外注、信用度監視の無料申し込みの提供、製品やサービスの将来的な割引などが含まれます。間接経費には内部調査や情報伝達のほか、顧客流出の発生や顧客獲得率の低下などに起因する顧客流出から生じると推定される金額が含まれます。

本調査では、情報漏えい経験に直接関係する事象のみが対象となっています。例えば、新しい規則（一般データ保護規則（GDPR: General Data Protection Regulation）やカリフォルニア州消費者プライバシー法（CCPA: California Consumer Privacy Act）など）は、サーバーセキュリティー実装技術への投資増加を促すものですが、この調査で示される情報漏えいコストには直接影響しません。

過去の年との整合性を維持するために、会計コストを調整するのではなく、同じ通貨換算方法を使用します。

ベンチマーク調査とサーベイ調査の違いを教えてください。
「情報漏えい時に発生するコストに関する調査」では、企業を分析の単位としています。サーベイ調査では、分析の単位は個人です。今回の調査では 524 社の企業を募集しました。

レコード 1 件当たりの平均コストから、何百万件というレコードの紛失や盗難が発生する漏えいの財務的影響を計算することはできますか。
本調査における情報漏えいの平均コストは、Equifax、Capital One、Facebook のような壊滅的な大規模情報漏えいには適用されません。これらは、ほとんどの企業が経験するような典型的な情報漏えいではないためです。

それゆえ、情報漏えいコストの振る舞いを理解する上で役立つ結論を導くために、被害レコード数が 100,000 件を超えない情報漏えいインシデントを対象としています。レコード 1 件当たりのコストから、合計何百万件というレコードが関係する 1 件または複数の漏えいの財務的影響を計算することは、この調査の趣旨と一致していません。ただし、この調査では、シミュレーション・フレームワークを使用して、100 万件以上のレコードを含む非常に大規模な漏えい 17 件のサンプルに基づいて、同様の「大規模な漏えい」の財務的影響を測定しています。

大規模な情報漏えいのコストを推定するために、シミュレーション方式を使用している理由を教えてください。
大規模な情報漏えいを経験した企業が 17 社というサンプル・サイズでは小さ過ぎて、活動ベースのコスト方式を使用して統計的に意味のある分析を実行することはできません。この問題を修正するために、モンテカルロ・シミュレーションを実行しました。これにより、反復的な試行を通して、可能性のある（ランダムな）さまざまな結果を推定することができます。

総計で 15 万回を超える試行を実行しました。すべての調査対象平均の総平均は、情報漏えいの各規模（被害レコードが 100 万件から 5,000 万件の範囲）において、最も可能性の高い結果を示します。

毎年、同じ企業を追跡調査していますか？
調査対象企業は毎年異なります。以前の調査との整合性を保つため、業種、社員数、地理的な営業範囲、情報漏えいの規模などの特性が類似した企業を毎年募集しています。調査を開始した 2005 年から、3,940 社の企業について情報漏えいを調査してきました。

調査対象企業の特性

2020 年の調査はさまざまな規模の 524 の企業を対象とし、さまざまな地域や業種でサンプリングされました。そして、17 の国や地域と 17 の業種で実施されました。

今回の調査で初めて、メキシコ、アルゼンチン、チリ、コロンビアを含むラテンアメリカの対象企業群の調査が実施されました。

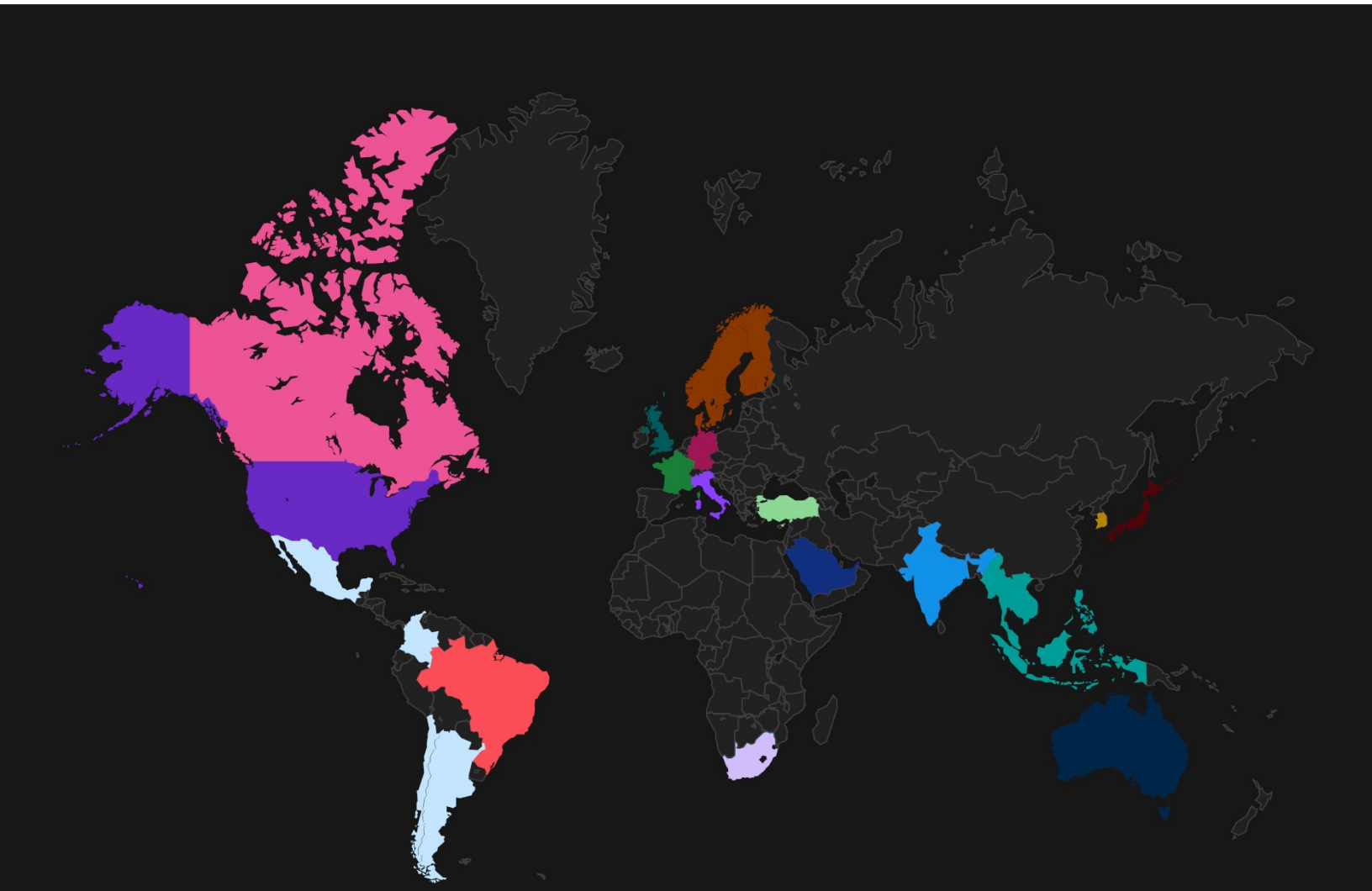
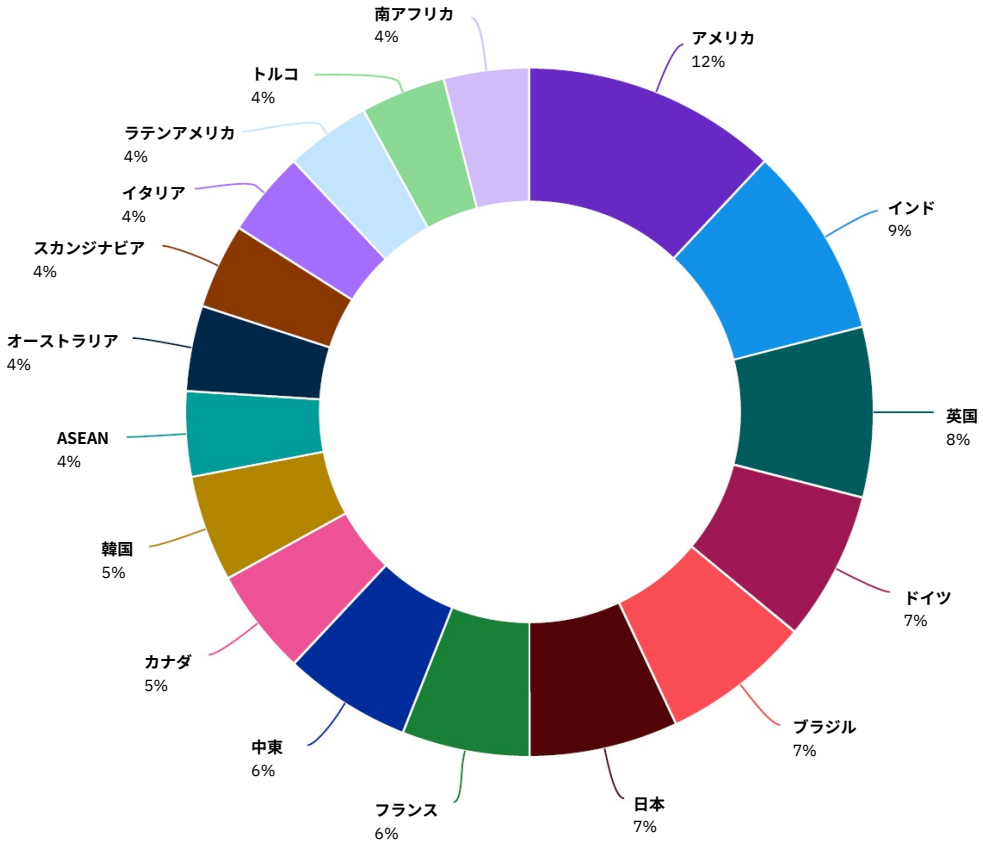


図 47:

調査対象の内訳（国または地域別）



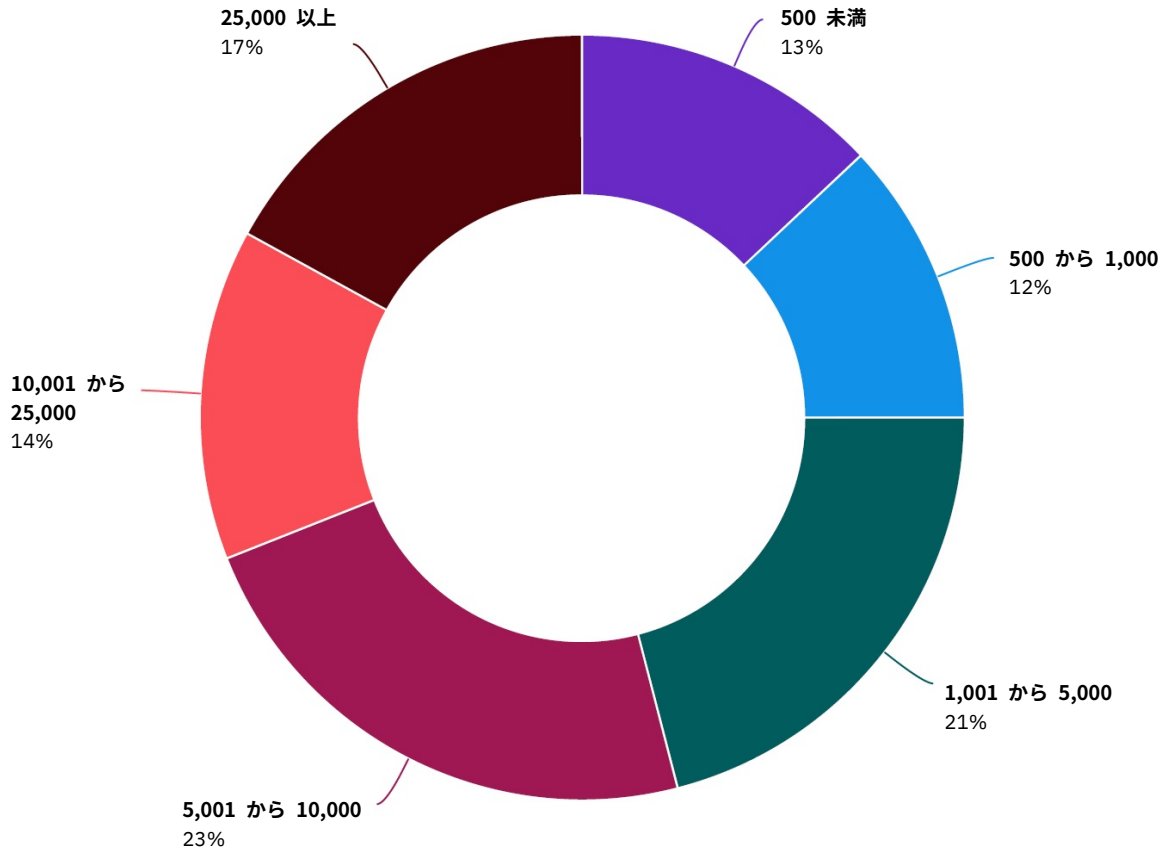
この調査では、6 つの大陸の国/地域が代表として選ばれている。

図 47 はベンチマーク対象の企業の内訳を国や地域別に示したものです。米国が最も多く（12%）、次いでインド（9%）、英国（8%）と続きます。最も少ない国/地域は、ASEAN、オーストラリア、スカンジナビア、イタリア、ラテンアメリカ、トルコ、南アフリカです。

図 48:

調査対象企業の分布 (企業規模別)

単位: 従業員数

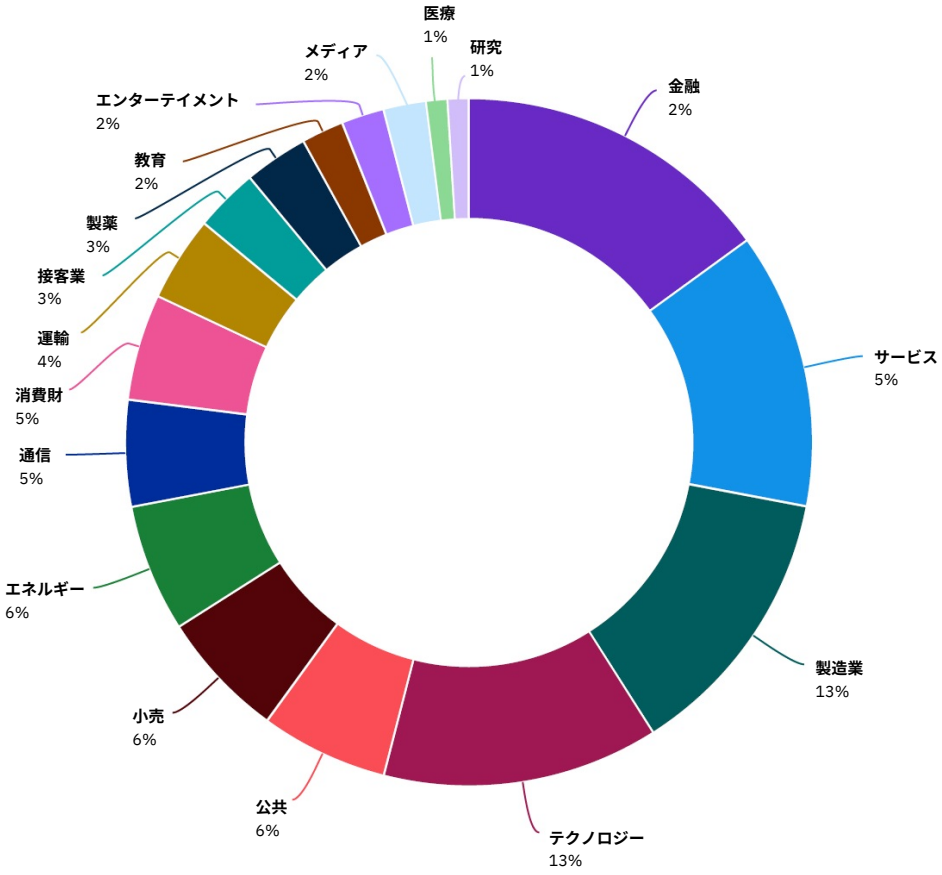


小規模、中規模、および大規模な企業が代表として選ばれている。

図 48 は、調査対象の 524 の企業の分布を、企業規模の代わりに従業員数別に示しています。調査対象は中規模の企業の比重が少し高く、従業員数が 1,001 ～ 25,000 人の企業が 58%、1,000 人未満が 25%、25,000 人超が 17% でした。

図 49:

調査対象企業の分布（業種別）



代表として選ばれている業種はいくつかの大規模なセクターに偏っている。

図 49 は、ベンチマーク対象の企業の内訳を業種別に示したものです。本年の調査では 17 業種が対象となりました。最も多いのは、金融、サービス、製造、テクノロジーです。 各業種の定義を別途説明します。

業種の定義

医療
病院、診療所

金融
銀行、保険、投資会社

エネルギー
石油会社、ガス会社、公益事業、代替エネルギーの製造会社と供給会社

製薬
生命医学ライフサイエンスを含む製薬会社

製造業
化学プロセス、エンジニアリング、製造の会社

テクノロジー
ソフトウェア会社、ハードウェア会社

教育
公立大学、私立大学、教育研修会社

サービス
法務、会計、コンサルティングなどの専門的サービスを提供する会社

エンターテイメント
映画製作、スポーツ、ゲーム、カジノ

運輸
航空会社、鉄道会社、トラック輸送会社、配送会社

通信
新聞、出版、広報、広告などの会社

消費財
消費財の製造会社と流通会社

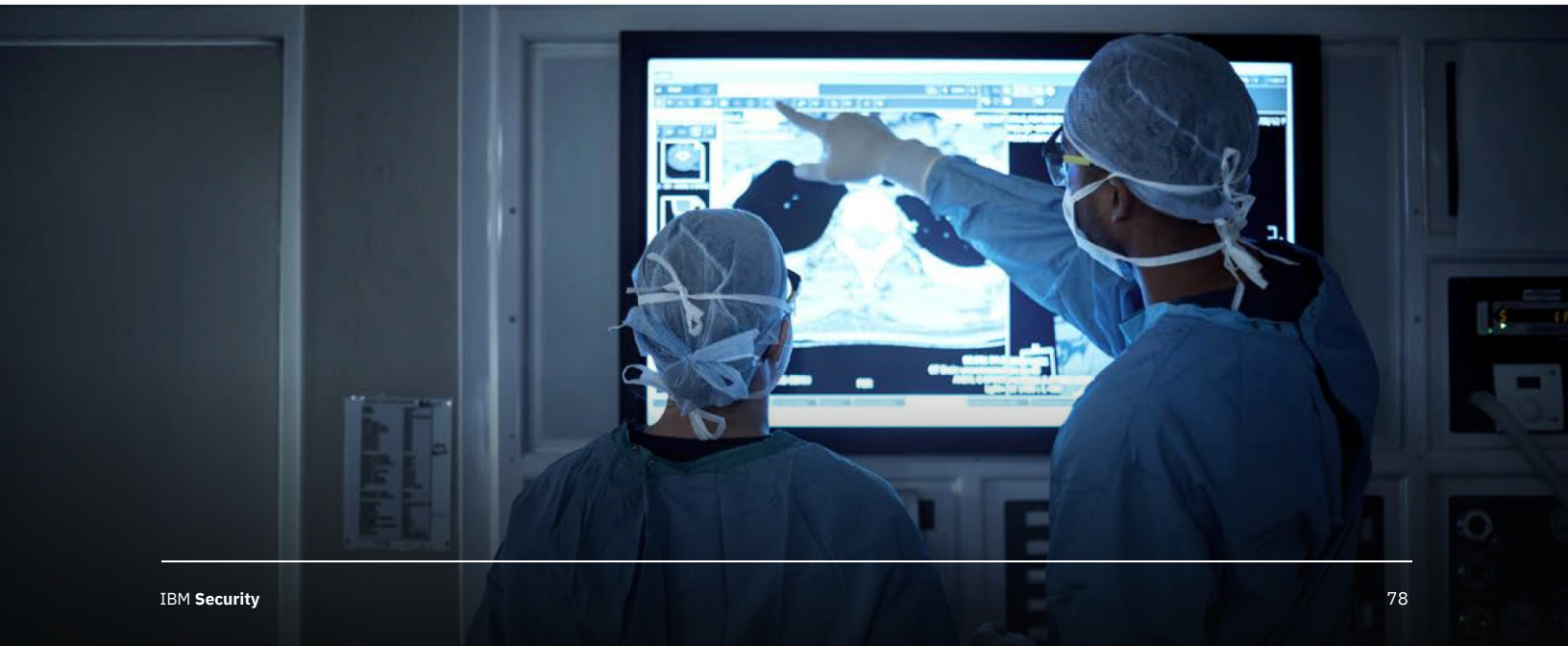
メディア
テレビ、衛星、ソーシャル・メディア、インターネット

接客業
ホテル、レストラン・チェーン、船旅会社

小売
実店舗、e-コマース

研究
市場調査、シンク・タンク、R&D

公共
連邦、州、地方の政府機関、NGO



調査の制限事項

この調査では、前回の調査で問題なく実施できることが確認された、機密かつ独自のベンチマーク手法が使用されています。同時に、このベンチマーク調査には回避できない制限事項があります。本調査結果から結論を導き出す際は、次に示す制限事項について慎重に検討してください。

結果が非統計的
今回の調査の基になったのは、世界中の企業の非統計的な代表サンプルです。科学的ではないサンプリング手法のため、統計的推論、許容誤差、信頼区間をこれらのデータに適用することはできません。

無回答の存在
無回答のバイアスはテストされていません。このため、情報漏えい時に発生するコストの傾向が、非回答企業ではまったく異なる可能性が存在します。

サンプリング・フレームのバイアス
サンプリング・フレームは独自の判断で決定されているため、今回のサンプリング・フレームが調査対象企業の母集団をどの程度反映しているかによって、結果の品質は変化します。今回のサンプリング・フレームは、個人情報保護や情報セキュリティーの取り組みが一定以上進んでいる企業に偏っていると判断しています。

企業固有の情報
ベンチマークでは、企業を特定できるような情報は収集されていません。企業と業種に関するカテゴリーで属性情報を提供する際は、カテゴリー別の応答変数の使用を許可しています。

調査対象外の要因
主なトレンドや企業の特徴といった可変要素は分析から除外されています除外された可変要素がベンチマーク結果に与え得る影響は特定できません。

推定に基づくコスト結果
ベンチマーク・プロセスに一定のチェック・アンド・バランスを適用することも可能ですが、回答者が不正確または不誠実に回答している可能性は常に存在します。また、実際のコスト・データではなくコスト推定の手法が採用されているため、何らかの事情で偏った結果や不正確な結果が推定されている可能性もあります。

推定に基づくコスト結果
本年は、米ドル高がグローバルなコスト分析に大きく影響しました。現地通貨から米ドルへの換算により、レコード 1 件当たりのコストと平均総コストの概算が低くなっています。過去の年との整合性を維持するために、コストを調整するのではなく、同じ会計処理方法を引き続き使用することにしました。

Ponemon Institute と IBM Security について

「情報漏えい時に発生するコストに関する調査」は、Ponemon Institute と IBM Security が共同で作成しました。調査は Ponemon Institute が独立して実施し、結果は IBM Security がスポンサーとなって、分析、報告、公開しています。

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遵守して調査活動を遂行しています。当社は、個人が特定できるようないかなる情報も収集しません（企業調査の場合は、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遵守しています。

IBM Security は、企業向けのセキュリティー関連の製品とサービスで構成される高度に統合されたポートフォリオを提供しています。世界的に有名な IBM X-Force® の研究活動によって裏づけされるこのポートフォリオは、企業が不確実性の増す世界においても成功を収められるように、ビジネスの根幹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、3,000 を超えるセキュリティー特許を有し、毎月 130 カ国以上で 2 兆ものイベントをモニタリングしています。詳細については、ibm.com/security をご参照ください。

本調査レポートに関するご質問やご意見をお寄せいただく場合（本レポートの引用や再利用の許諾申請を含む）は、手紙、電話、電子メールのいずれかでお問い合わせください。

Ponemon Institute LLC

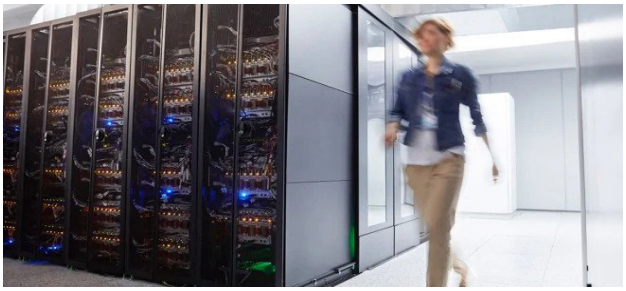
Attn: Research Department
2308 US 31 North
Traverse City, Michigan
49686 USA

1.800.887.3118
research@ponemon.org

次のステップ

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、マネージド・セキュリティー・サービスでリスクを軽減
詳細情報 →

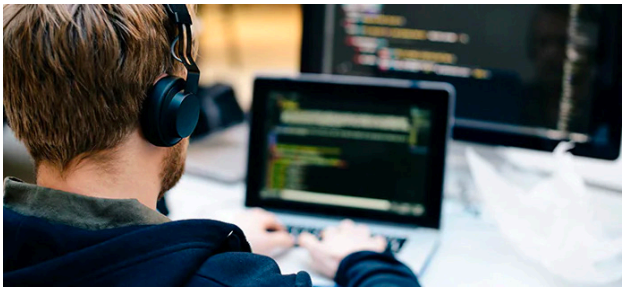
アイデンティティー/アクセス管理
すべてのユーザー、API、デバイスをすべてのアプリに安全に接続
詳細情報 →



データ・セキュリティー
機密性の高い企業データを特定、分類、保護
詳細情報 →

セキュリティー情報およびイベント管理
脅威を検出、調査、対応するための可視性を獲得
詳細情報 →

Security Orchestration, Automation and Response (SOAR)
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迅速化
詳細情報 →



クラウド・セキュリティー
ハイブリッド・マルチクラウドへの移行にセキュリティーを統合
詳細情報 →

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2020

IBM Security