IBM Security

インサイダー脅威のコスト調査：グローバル・レポート

2020 年版

調査

Ponemon INSTITUTE

協賛

observe it IBM

目次

はじめに

Ponemon Institute は、ここに 2020 年版のインサイダー脅威のコストに関する世界的調査レポートを発表します。ObserveIT および IBM の協賛によって実施されたこの調査は、インサイダー脅威から間接的、直接的に発生するコストを特定するために行われた、3 回目のベンチマーク調査です。最初の調査は 2016 年に米国企業のみを対象として実施されました。この調査には、北米、欧州、中東、アジア太平洋地域にある企業が含まれます。

本調査の文脈では、インサイダー脅威は以下の原因で発生します。

– 正社員または契約社員の過失または不注意

– 内部関係者の犯罪行為または悪意、あるいは

– 認証情報を狙ったハッカーによって

重要な結論として、インサイダー脅威の中でも認証情報の漏えいがインシデント当たり最もコストが大きいことがわかりました。このようなインシデントの発生頻度とコストは大幅に増加しています。事実、企業当たりのインシデント発生頻度は、2016 年の平均 1 回から 3.2 回に増加し、コストは 493,093 米ドルから 2019 年の 871,686 米ドルに増加しています。年間で見ると、組織がインサイダー過失対策に費やす経費は増加していますが、インシデント当たりのコストは大幅に低くなっています。

本調査では、北米 （アメリカおよびカナダ）、欧州、中東およびアフリカ、アジア太平洋地域にある 204 の組織で働く、964 人の IT セキュリティー担当者と面談をしました。面談は 2019 年 9 月に完了しました。

204
の組織

964
の個人

各組織では、内部関係者によって引き起こされた重大な事案が発生していました。これらの組織で過去 12 か月間に発生したインサイダー・インシデントは、総計 4,716 件にのぼりました。調査の対象となった組織は、従業員数 1,000 名以上のグローバル企業です。

内部からの情報漏えいによるコスト

世界平均

認証情報の漏えいから発生する平均コスト

493,093 ドルから
871,686 ドルへ

2019 年

発生頻度

会社当たりのインシデントの発生頻度は 3 倍に増加

1 回から
3.2 回へ

2016 年以後

認証情報の漏えいインシデントの修復に最もコストがかかっています。

インサイダー脅威のコストは、インシデントの種類によって大きく異なりました。

正社員または契約社員の過失から発生したインシデント当たりの平均コスト

307,111 ドル

インシデントにおいて、なりすましまたはハッカーによる認証情報の漏えいが起こった場合は、平均コストが 3 倍近くに増加しました。

871,686 ドル

最もコストの高い認証情報の漏えいは、特権ユーザーの認証情報の漏えいに関連したものです。

本調査の対象となった組織では、内部関係者の犯罪行為または悪意のある行為によるコストは

756,760 ドル インシデント当たり

コストを引き上げる活動として、モニタリングと監視、調査、エスカレーション、インシデント対応、封じ込め、事後分析と修復が挙げられます。

大部分のインシデントの根本原因は、内部関係者の過失です。

本調査中のインシデントの大部分は、内部関係者の過失が原因で発生していました。

具体的には、4,716 件のインシデントの内、

2,962 件は、正社員または契約社員の過失または不注意が原因で発生

1,105 件は、内部関係者の犯罪行為または悪意から発生

649 件が認証情報の漏えい関連

191 件が特権ユーザーの認証情報の漏えい関連

過去 12 か月間の内部関係者が関連するインシデントのコストに関する主な統計を以下に示します。

204
ベンチマーク調査の実施総数

14%
ユーザーの認証情報漏えいに関連するインシデント

4,716
内部関係者インシデントの総件数

458 万ドル
過失インシデントにかかる年間コスト

1145 万ドル
総平均コスト

408 万ドル
内部関係者の犯罪行為にかかる年間コスト

63%
過失に関連するインシデント

279 万ドル
認証情報漏えいにかかる年間コスト

23%
内部関係者の犯罪行為に関連するインシデント

組織の規模と業界によって異なるインシデント当たりのコスト

インシデントのコストは組織の規模によって 異なります。従業員数 500 人以下の小規模企業でインサイダー・インシデントの影響に対応するためにかかっているコストは平均で 768 万ドルでした。金融サービス、サービス業、テクノロジーおよびソフトウェア業界の企業で発生したコストは、それぞれ 1405 万ドル、1231 万ドル、 1230 万ドルでした。

すべての種類のインサイダー・リスク脅威が増加

2016 年以降、 正社員または契約社員の過失によるインシデントの平均発生数は 10.5 件から 14.5 件に増加しています。認証情報漏えいの平均発生数は、過去 2 年間で 1.0 件から 3.2 件と 3 倍に増加しています。60 % 以上の企業で年間 20 件以上のインシデントが発生しています。

年間ベースでは、コストが最も高いのは正社員または契約社員の過失インシデント

年間総額で見ると、 正社員または契約社員の過失が、最もコストのかかる内部関係者プロフィールです。

インシデント当たりでは、認証情報の漏えいが最もコストがかかる

各インシデントの修復にかかる コストは 871,686 ドルです。

平均 2 か月以上かかるインサイダー・インシデントの封じ込め

30 日未満で封じ込められたインシデントはわずか 13 %でした。

1792 万ドル

従業員数 75,000 人を超える大企業では、内部関係者関連のインシデントの解決に、平均 1792 万ドルが費やされています。

60%

企業の 60 % で年間 20 件以上のインシデントが発生しました。

29%

認証情報の漏えいの 29 % は、特権ユーザーの認証情報の漏えいに関係しています。

77 日間

インシデントの封じ込めには平均 77 日間かかりました。

調査について

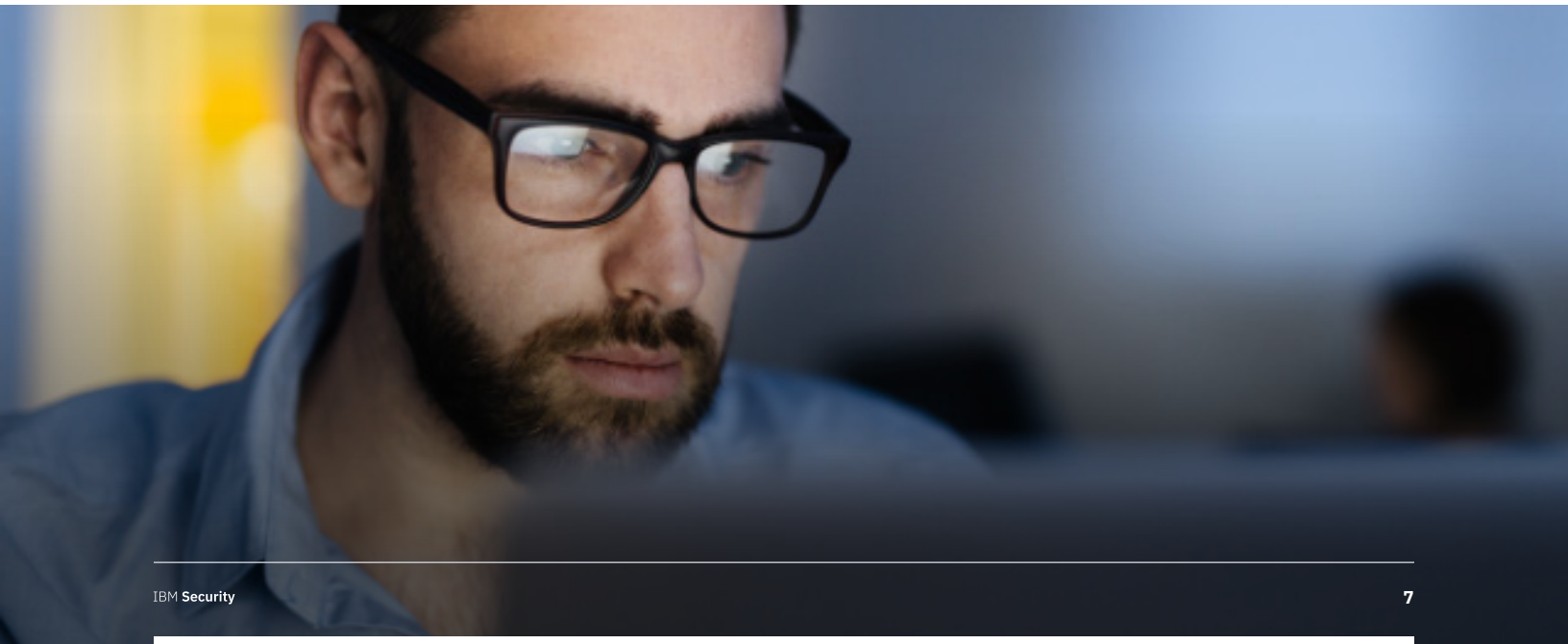
本調査では、過去 12 か月に組織の経費に影響を与えた、実際のインサイダー関連の事象またはインシデントを対象としました。

本調査の方法では、以下のビジネス脅威を含みますが、これらに限定されない、直接および間接的なコストの両方が含まれます。

- ミッション・クリティカルなデータまたは知的財産の漏えいまたは喪失
- ダウンタイムまたは組織の生産性への影響
- 設備や他の資産への損害
- 検知、システムおよび基幹ビジネス・プロセスの修復にかかるコスト
- 弁護士料金を含む法律および規制から受ける影響
- 信頼性と主な利害関係者の信用の喪失
- 市場ブランド力の低下と風評被害

本調査では、活動ベースのコスト (ABC) を使用しています。調査は 2 か月間にわたって実施され、2019 年 9 月に終了しました。最終ベンチマーク・サンプルは、204 の個別の組織から収集されました。これらの組織の役職にある従業員に対し、合計 964 回の対面調査を実施しました。現在の調査の活動コストは、厳格な機密性のもと実施された、すべての回答者との面談、または施設への視察から得られたものです。対象組織は以下の通りです。

- 民間および公共部門の組織
- 総従業員数 500 人以上
- 以下の地域に所在:北米、欧州、中東およびアフリカ、アジア太平洋地域
- オンプレミスおよび/またはクラウド環境ビジネス・プロセスを統括する中央集中 IT 部門を有する
- 内部関係者の不注意、悪意または犯罪行為による重大なインシデントが 1 件以上発生した



調査について

本調査では、内部関係者が原因で発生した事象またはインシデントが経費に与えたコストを完全に測定する客観的なフレームワークが提案されています。

以下は、204 の組織で発生したインサイダー関連のコストを分類し分析するために使用されたケース・プロフィールです。

– 正社員または契約社員の過失または不注意

– 正社員または契約社員の悪意を含む内部関係者の犯罪行為

– 従業員/ユーザーの認証情報漏えい （なりすましリスク）

この調査の第一歩は、世界中の組織への協力依頼でした。調査担当者は、面談による診断と活動単位のコスト分析を行って、コスト・データを収集し、推算しました。Ponemon Institute は、以下の手順を含むこの調査プロジェクトのすべての段階を実行しました。

– ObserveIT および IBM との討議による調査対象分野の設定

– ベンチマーク実施企業の募集

– 活動ベースのコスト分析フレームワークの構築

– 調査プログラムの管理

– 適切な信頼性チェックによる全結果の分析

– すべての主な調査結果をまとめたレポートの作成

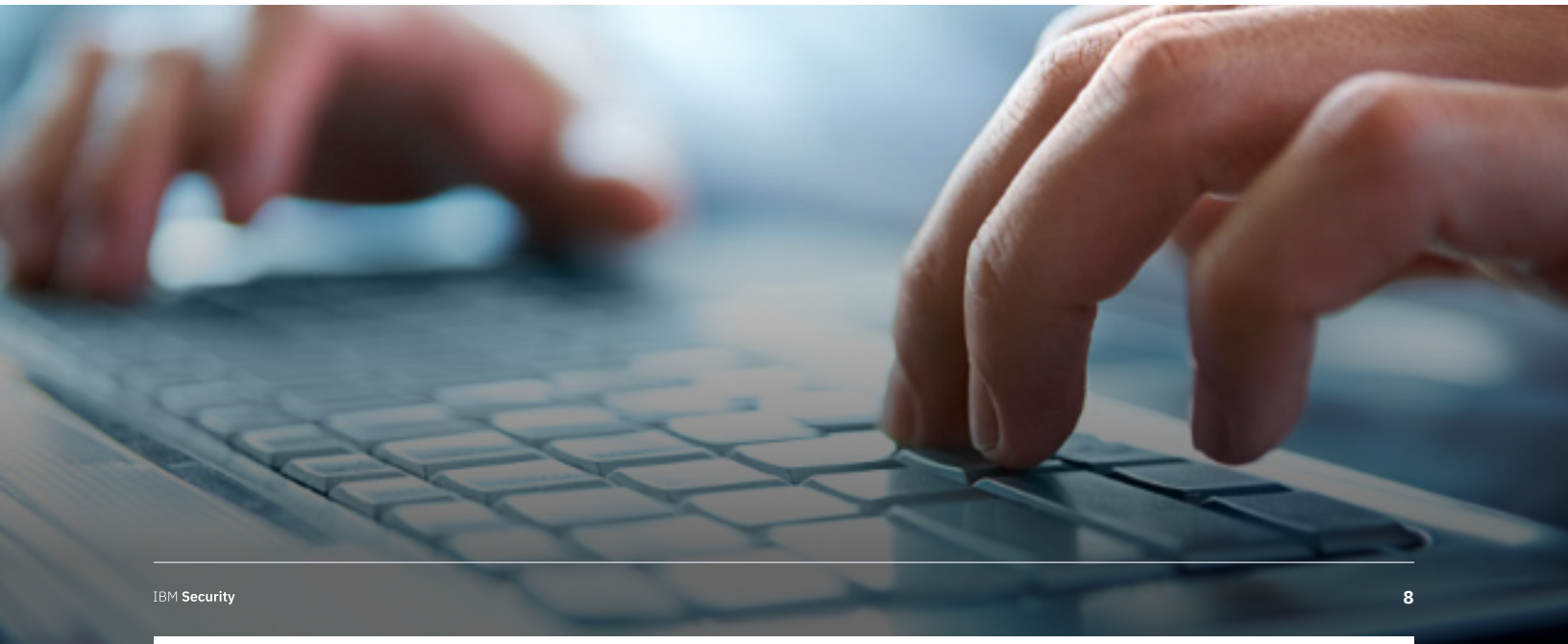


図 1：

参加組織の業界部門

n = 204 社

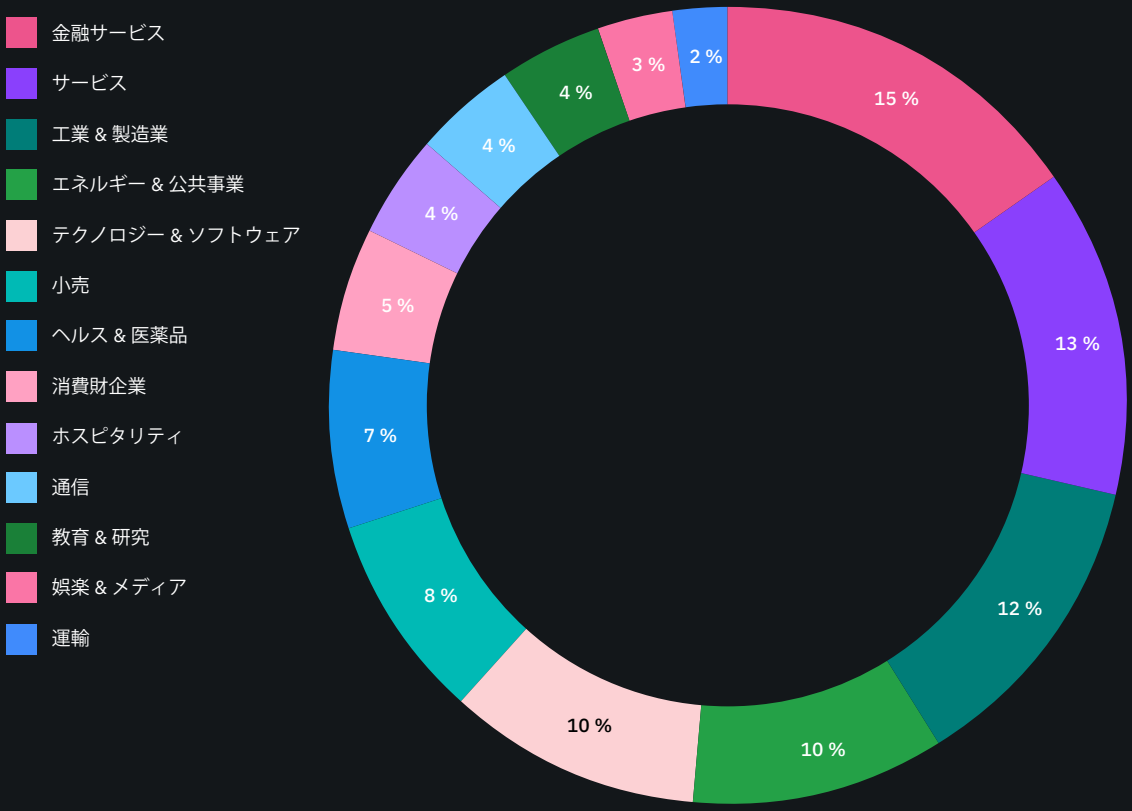


図 1 ベンチマーク調査の分析単位は組織である。上記の円グラフは、13 の業界部門にわたる企業の分布率を示す。最も大きな 3 つの部門は金融サービス、サービス、工業および製造である。金融サービス組織には、銀行、保険、投資管理、証券会社が含まれる。サービス組織とは、専門サービス企業を含むさまざまな種類の企業が含まれる。

図 2：

参加組織の従業員数 （規模）

n = 204 社

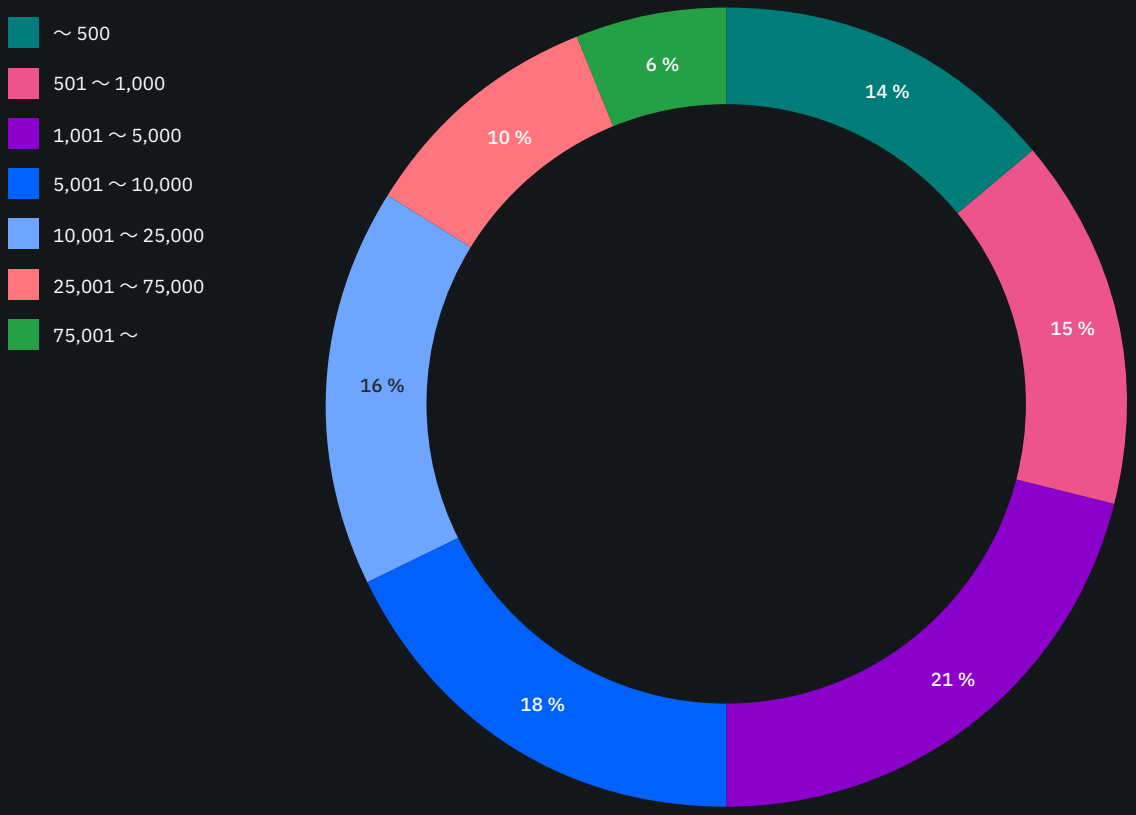


図 2 は、組織規模を示す、世界の従業員数を基準とした企業の分布率を示す。グラフからわかるように、サンプルの 50 % には、正社員数 5,000 人以上の大規模企業が含まれる。

図 3：

役職または部署ごとの回答者

n = 964 人の回答者

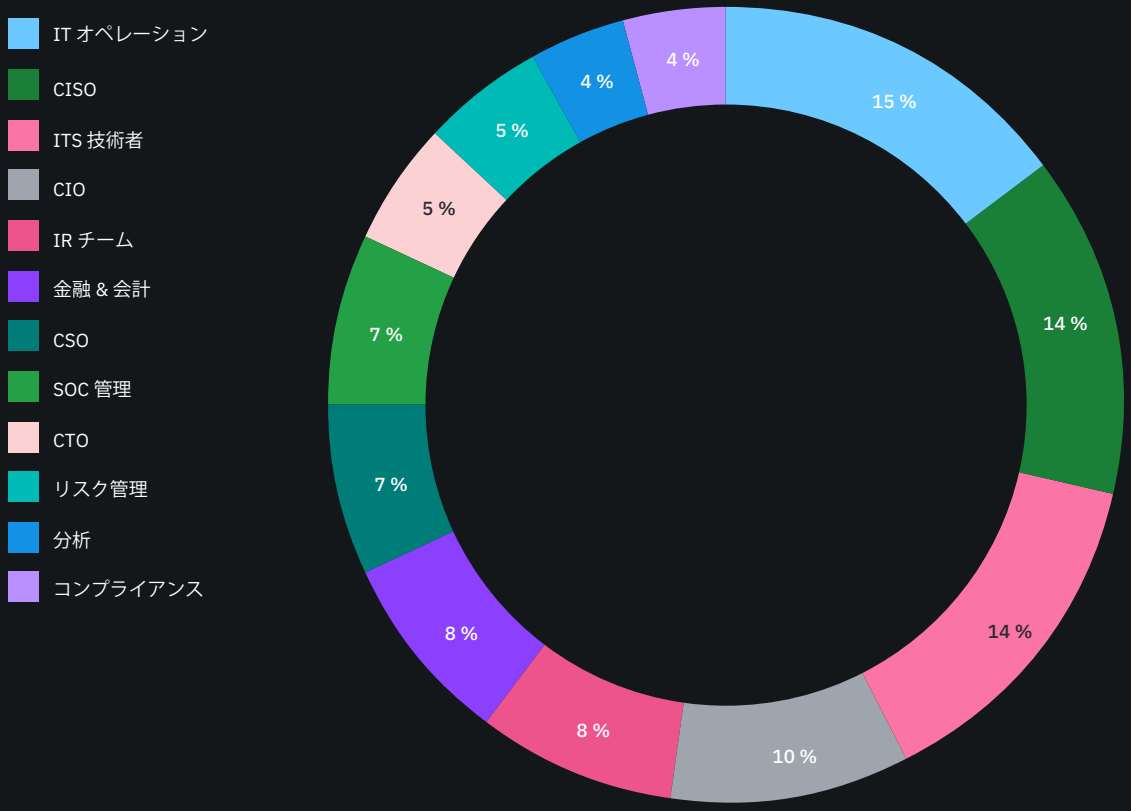


図 3 図 3 が示す通り、3,964 人の個人が現場での対面調査に参加した。各ケース・スタディには平均 4.7 名の個人がかかわった。3 大部門には、IT 運用 （15 %）、CISO （14 %）、IT 技術者 （14 %） が含まれる。

図 4：
世界中の組織の地域分布
n = 204 社

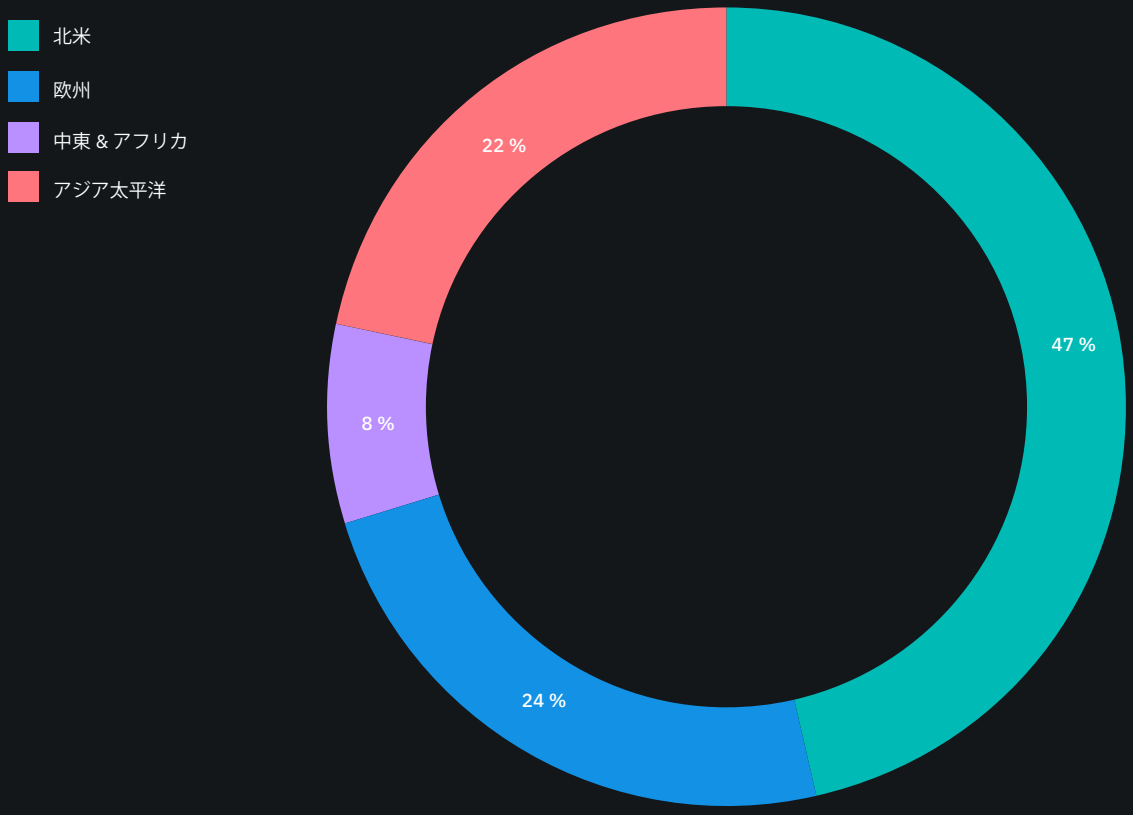


図 4 は、本調査に参加した地域を示す。北米が最大を占め （企業の 47 %）、中東が最小を占める （企業の 8 %）。サンプル・サイズが小さいため、欧州と中東を合わせて EMEA 区分とした。

図 5：

3 つのインサイダー・プロフィールで 4,716 件のインシデント発生頻度

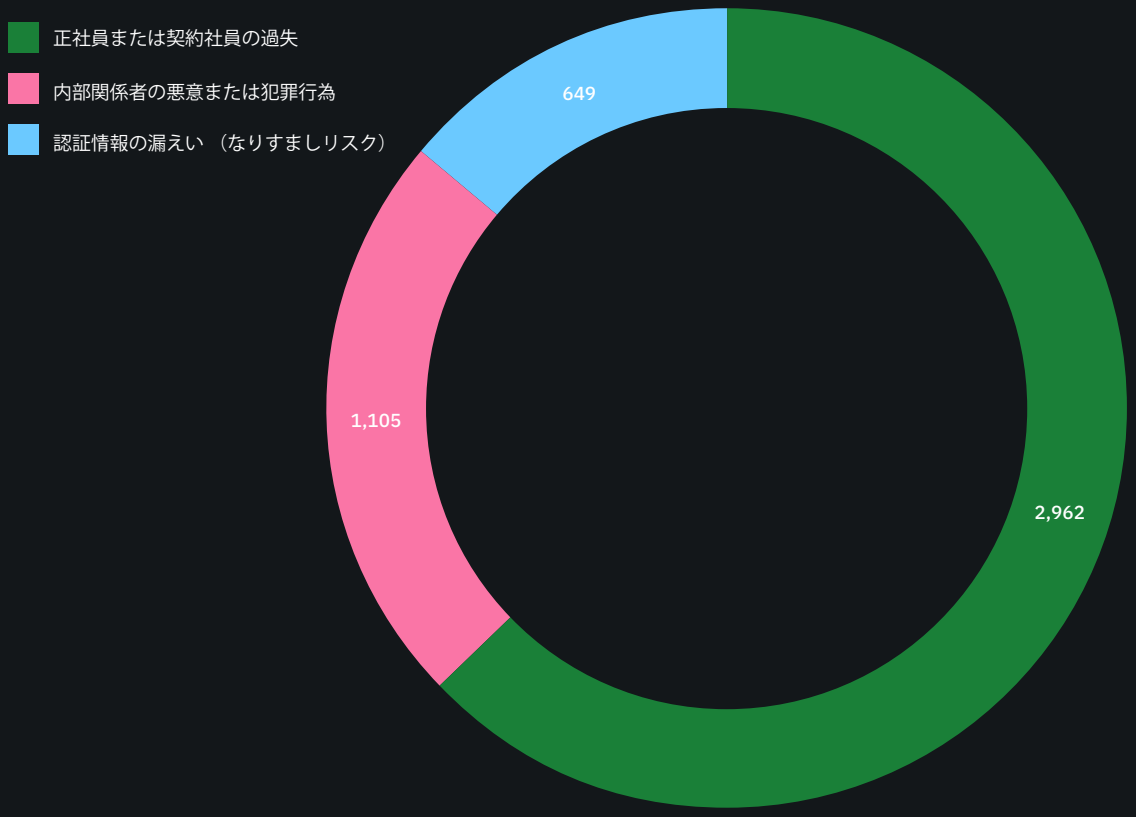


図 5 は、サンプルで分析された 4,716 件の報告済み攻撃の分布を示す。合計 2,962 件の攻撃 （63 %） が、正社員または契約社員の過失に起因していた。内部関係者の犯罪行為または悪意による攻撃は 1,105 件 （23 %） であった。

649 件 （14 %） の攻撃で、認証情報の漏えい （なりすましリスク） が発生した。これらの内、191 件で特権ユーザーの認証情報が漏えいした。回答した特定の企業 1 社につき報告された最大インシデント件数は 45 件で、最小インシデント件数は 1 件であった。

図 6：

企業ごとの、内部関係者が関係したインシデントの発生頻度割合

3 つのプロフィールを統合

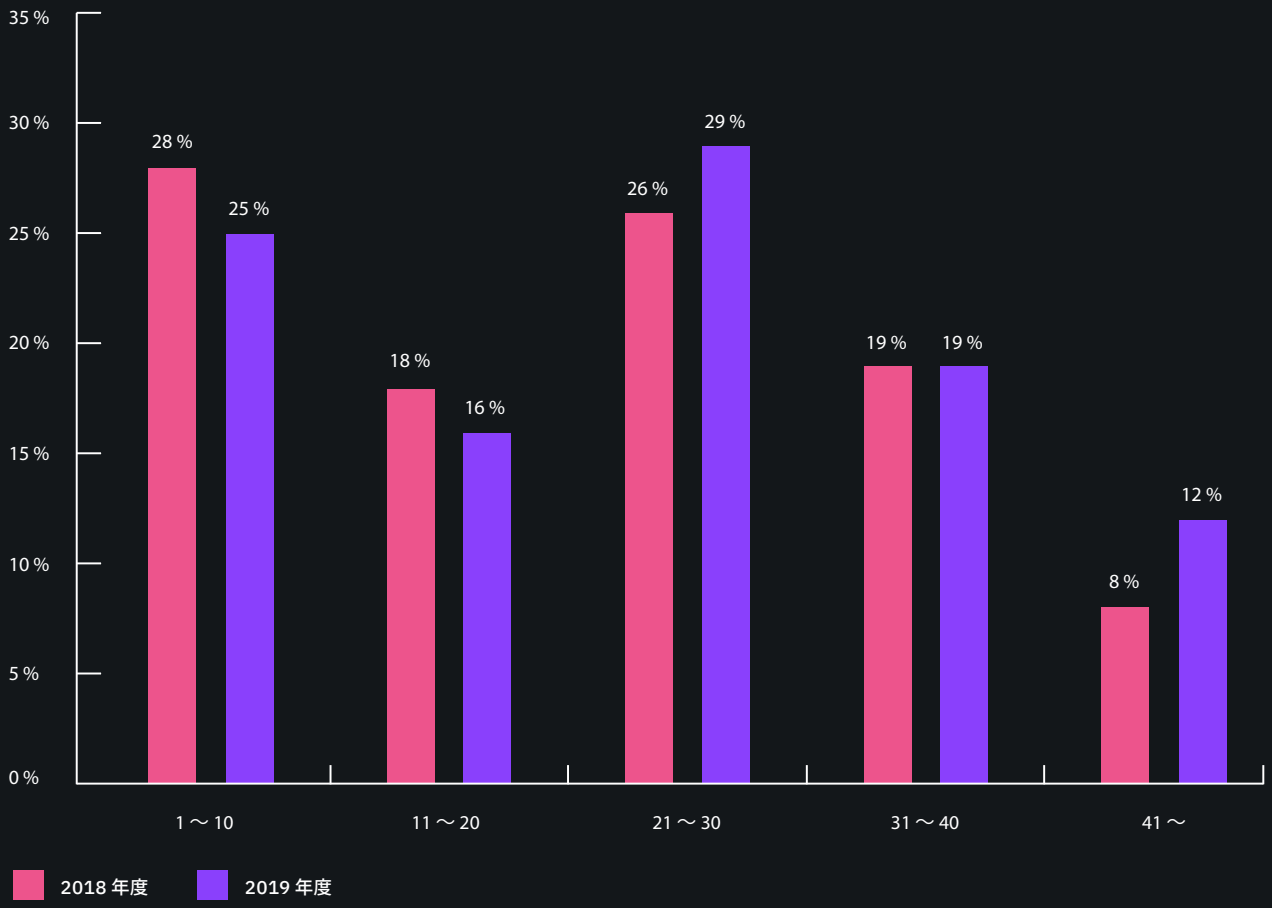


図 6 は、過去 12 か月間に 204 社のサンプル企業で発生したインサイダー・インシデントのヒストグラムである。図からわかるように、60 % の企業で、年 20 件以上のインシデントが発生している。

図 7：
インサイダー・インシデントの 3 つのプロフィールの発生頻度

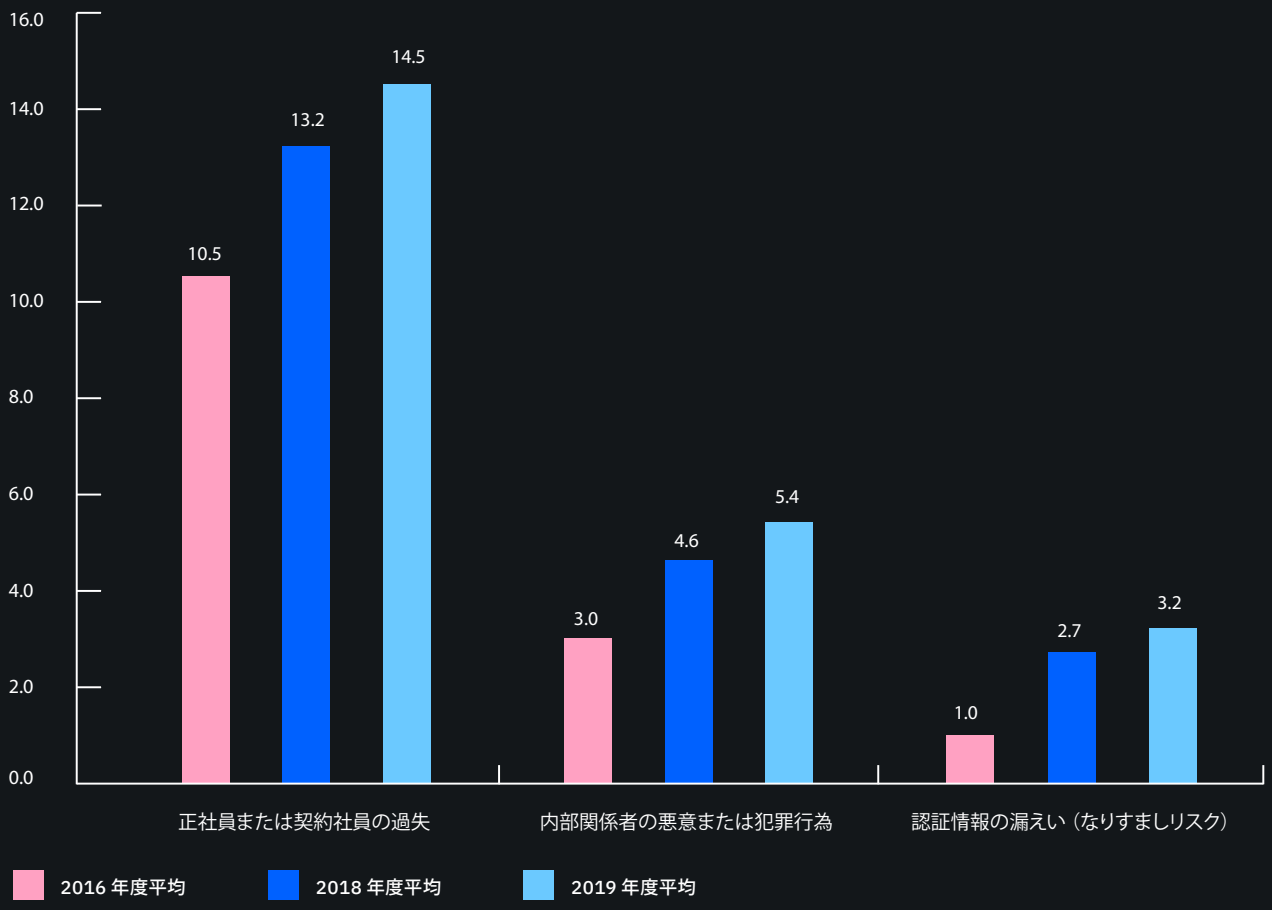


図 7 すべての種類のインサイダー脅威が増加している。図 7 が示す通り、2016 年以降、正社員または契約社員の過失によるインシデントの平均発生数は 10.5 件から 2019 年の 14.5 件に増加している。企業ごとの認証情報漏えいの平均発生数は、過去 3 年間で 1.0 件から 3.2 件と 3 倍に増加している。[1]

2016 年のデータは、米国企業のみから収集された。2019 年のデータには、北米、欧州、中東およびアフリカ、アジア太平洋地域が含まれる。2016 年の米国企業レポートは多国籍企業であるため、データは比較可能であると考えられる。

図 8：

3 つのプロフィールのインシデント平均発生率

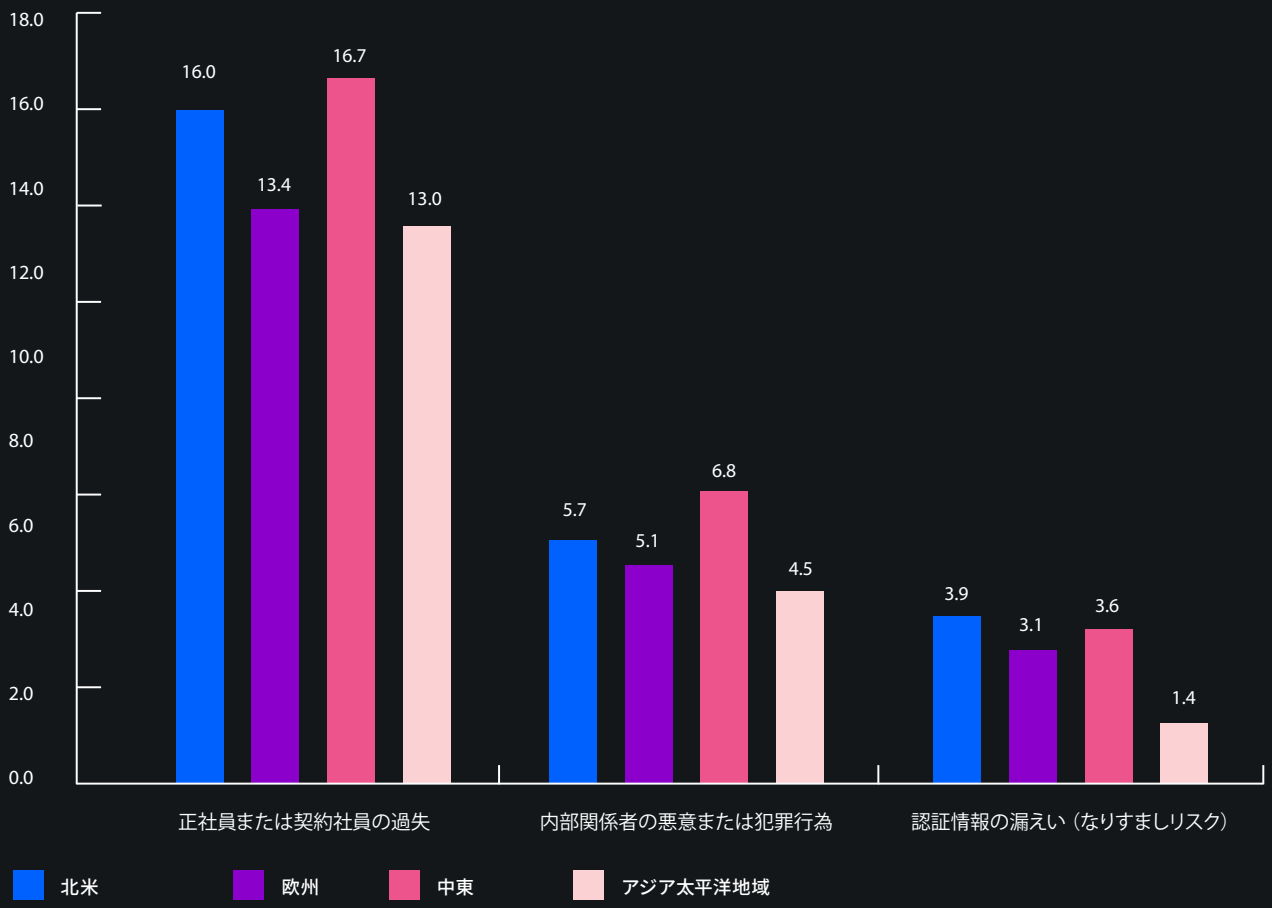


図 8 インサイダー・インシデント数は中東の企業で最も多く、最も少なかったのはアジア太平洋地域の企業であった。図 8 は、調査対象の 4 つの地域のインサイダー・インシデントの発生頻度を示す。すべての地域で最も発生頻度が高かったのは、正社員または契約社員による過失であった。認証情報の漏えいが最も多かったのは北米と中東であった。

図 9：
インサイダー・インシデントの 3 つのプロフィールの地域ごとの発生頻度

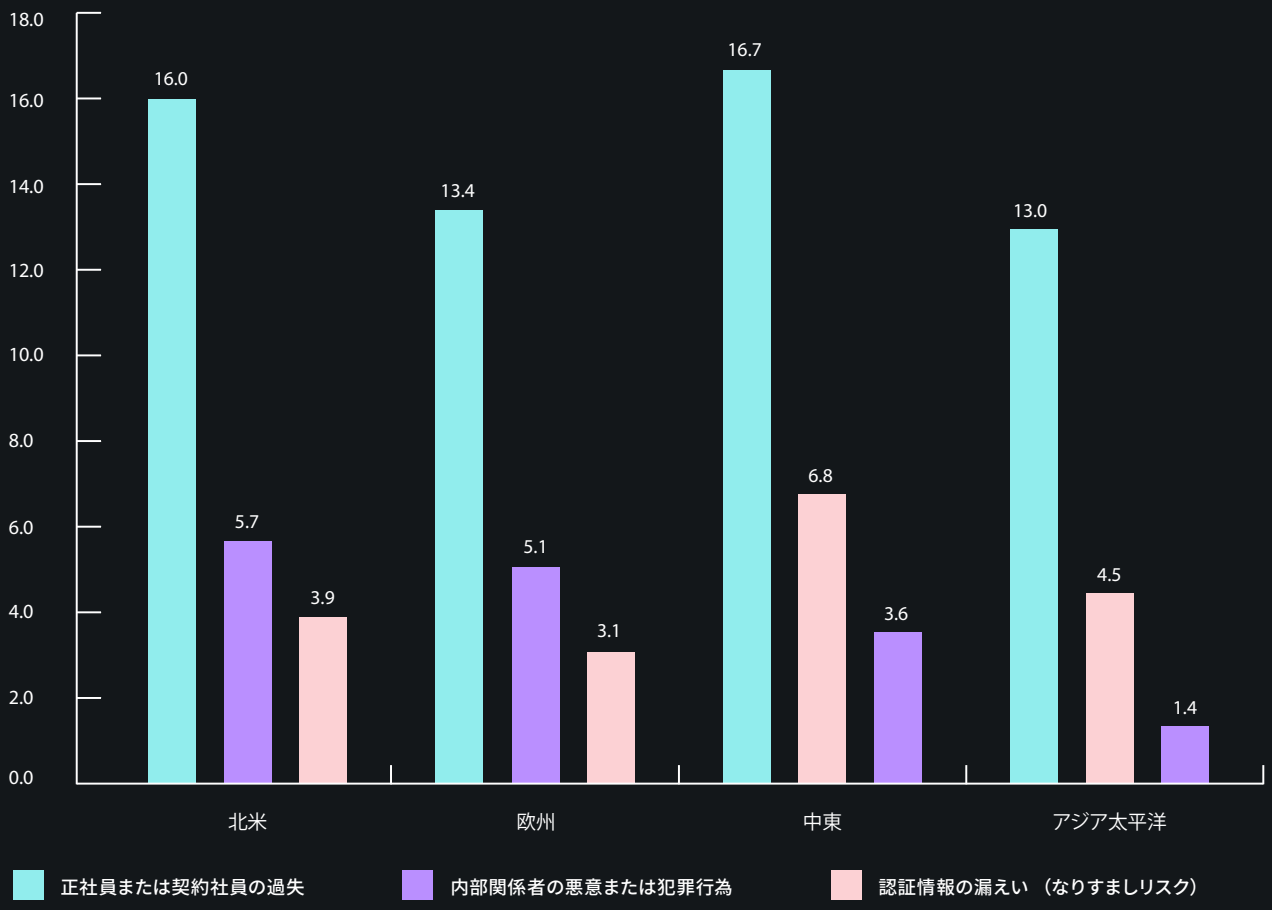


図 9 インサイダー脅威の発生頻度は、地域によって異なる。図 9 に示した通り、北米および中東地域の企業では、過去 12 か月間に発生した内部関係者関連のインシデント数が最も高くなっている。反対に、内部関係者関連のインシデント数が最も低かったのはアジア太平洋地域の企業であった。

図 10：

地域ごとの平均活動コスト

平均 = 1145 万ドル

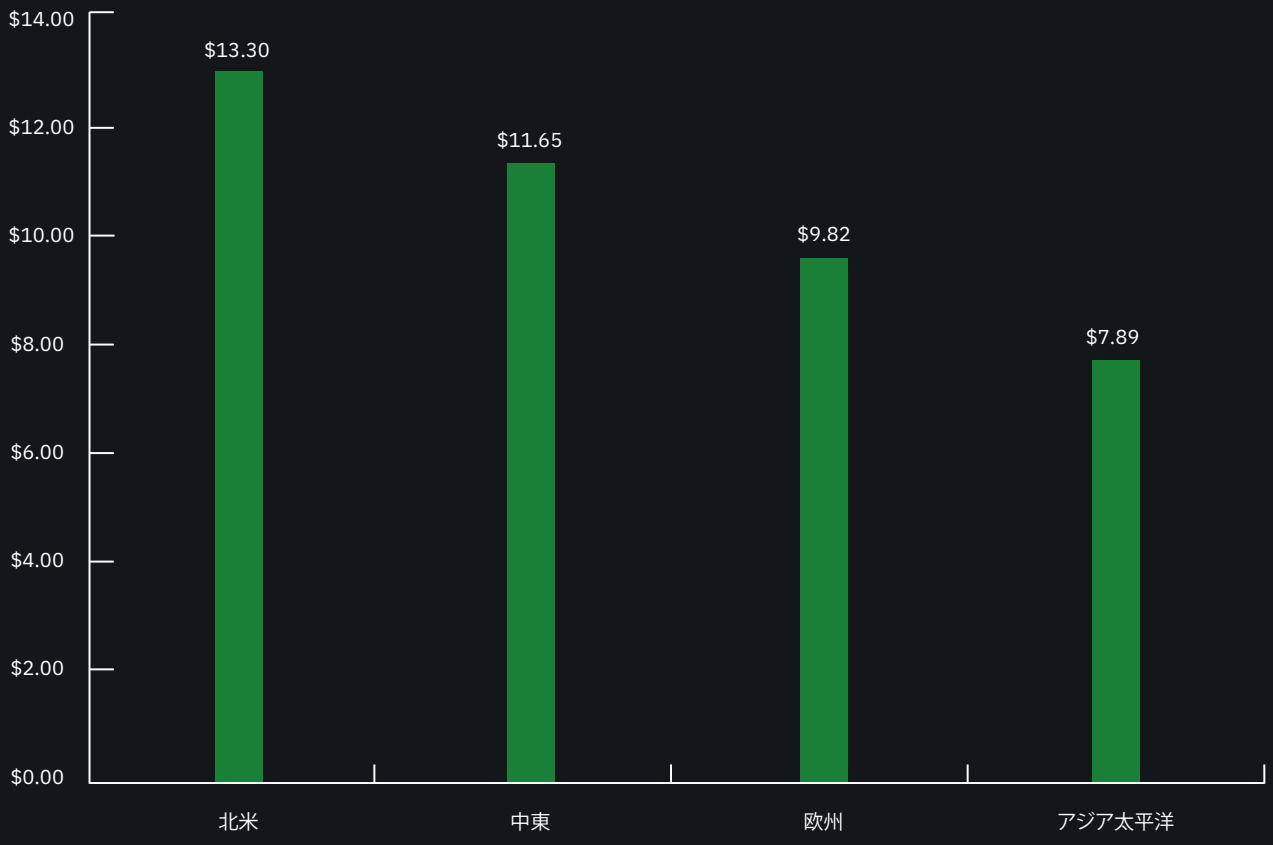


図 10 北米の企業の平均年間コストは平均コストより高かった。3 つの地域の年間コスト総額を図 10 に示した。北米の企業のコストは 133 万ドルと最も高かった。2 番目に高かったのは中東の企業で、1165 万ドルであった。欧州およびアジア太平洋地域の平均コストは、204 社すべての企業で平均コスト総額を下回った。

図 11：

従業員数 （規模） 別の昇順インサイダー・インシデント数

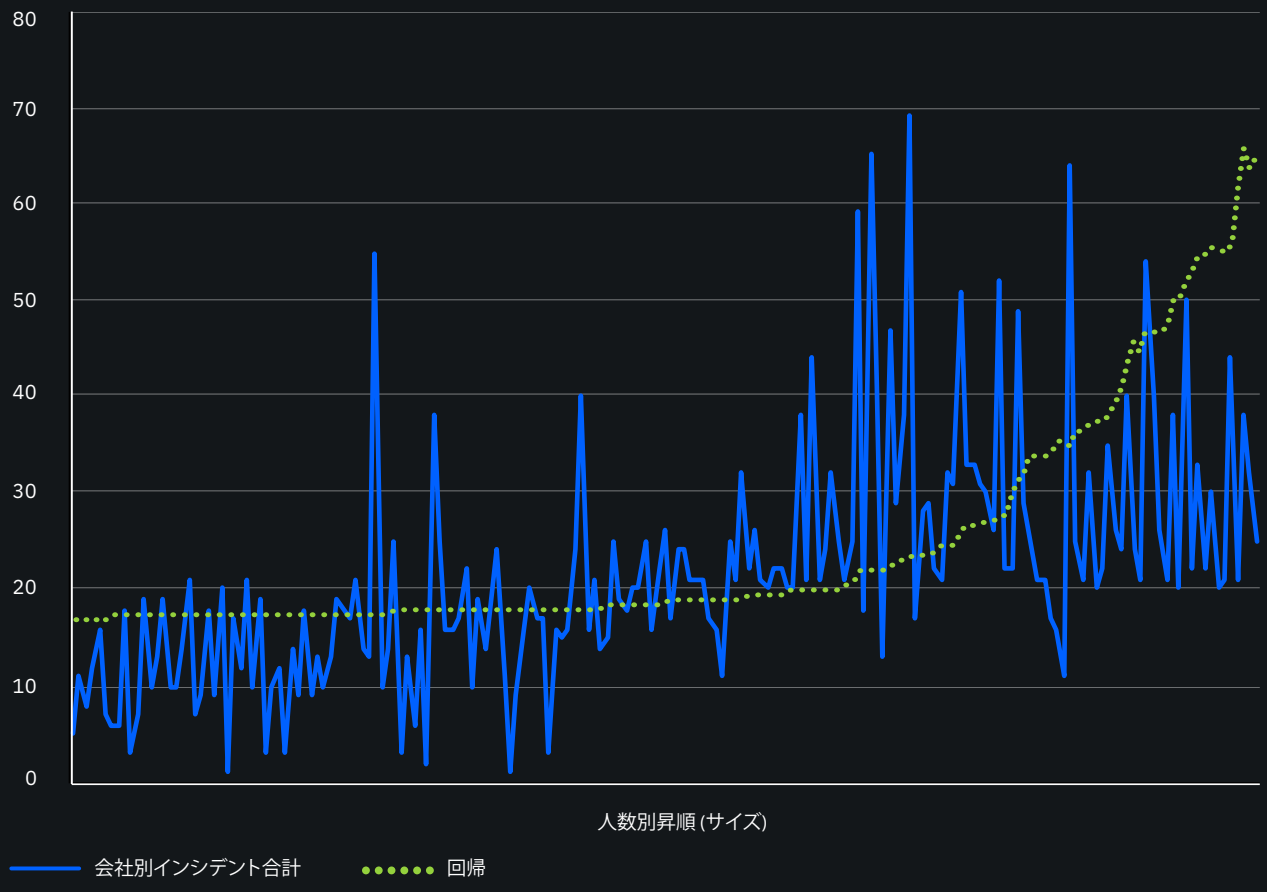


図 11 単純な線形回帰モデルを使用し、データから 0.21 の R2 値が算出された。企業の規模が大きいほど、インサイダー・インシデント数も増加した。図 11 は、インサイダー・インシデントの分布を従業員数別、または回答企業の規模ごとに昇順で示したものである。図から、上方向の傾きから、インサイダー・インシデントの発生頻度が組織規模と正の相関があることがわかる。その相関は、より規模の大きい企業で顕著である。

図 12：
地域ごとの平均活動コスト
平均 = 1145 万ドル

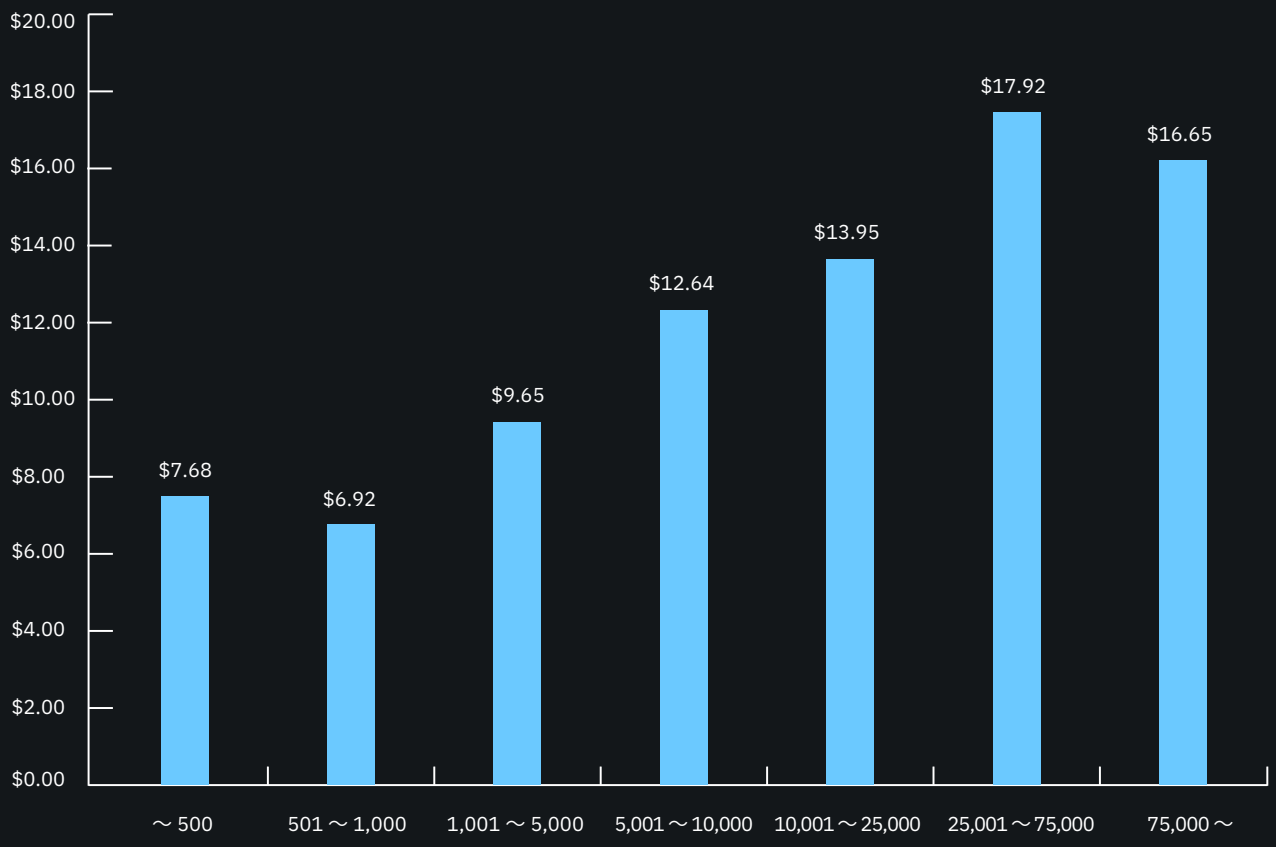


図 12 企業の世界の従業員数に対し調整した年間コスト総額を図 12 に示した。従業員数 25,001 ～ 75,000 人の企業のコスト総額は 1792 万ドルと最も高く、従業員数 500 ～ 1,000 人の企業は 692 万ドルと年間コストが最も低かった。

コスト分析

本調査では、 内部関係者が関連するインシデントに対する会社の対応に関係して、さまざまな経費が発生する中心プロセス関連の活動を対象とします。本調査のフレームワークの中心となる 7 つの内部コスト活動を以下のように規定します。[2]

- **モニタリングと監視：** 企業がインサイダー・インシデントや攻撃を合理的に検知し、防止できる可能性のある活動です。これには、リスク低減や早期発見を促進するための特定のテクノロジーに割り当てられた（諸経費） コストが含まれます。

- **調査：** 1 つ以上のインシデントの発生源、範囲、規模を完全に把握するために必要な活動です。

- **エスカレーション：** 企業内の主な利害関係者間で実際のインシデントについて意識を高めるために行われる活動です。このエスカレーション活動には、初期管理対応を組織するために取られる手順も含まれます。

- **インシデント対応：** 最終管理対応を策定するために取られた手順を含め、インシデント対応チームの編成と関与に関連する活動です。

- **封じ込め：** インサイダー・インシデントまたは攻撃を阻止、またはその重大性を軽減するための活動です。これには、脆弱性のあるアプリケーションやエンドポイントの封鎖が含まれます。

- **事後対応：** 今後、組織が内部関係者が関係するインシデントおよび攻撃が発生する危険性を最小限に食い止めるための活動です。

  これには、被害を最小限に食い止めるための推奨事項の作成など、社内および社外の主な利害関係者への通達手順も含まれます。

- **修復：** 組織のシステムや基幹プロセスの復旧や修復に関連する活動です。これには、被害を受けた情報資産や IT インフラの修復が含まれます。

[2]内部コストは、直接および間接コストを示す工数 （時間） を使用して推算しました。この方法は、テクノロジーに対する複数年にわたる投資などの固定費の諸経費部分を割り当てるためにも使用されています。

表 1:

コスト活動 （インシデント当たり）

（100 万米ドル）

コスト活動 （インシデント当たり）	正社員または契約社員の過失	内部関係者の悪意または犯罪行為*	資格情報の窃盗	平均コスト
モニター & 監視	$21,538	$21,857	$22,977	$22,124
調査	$49,441	$114,524	$147,429	$103,798
エスカレーション	$9,282	$29,513	$26,619	$21,805
インシデント対応	$62,877	$159,398	$132,677	$118,317
データ封じ込め	$75,903	$175,962	$382,794	$211,553
事後分析	$21,035	$19,282	$18,121	$19,480
是正	$67,036	$235,223	$141,069	$147,776
合計	$307,111	$755,760	$871,686	$644,852

表 1 企業でインシデント当たりに費やされる経費は平均 644,852 ドルである。表 1 は、3 つのタイプのインシデントと 7 つの活動項目で内部関係者が関連するインシデントに費やされる平均コストを示している。表が示す通り、封じ込めと修復が最もコストのかかる活動である。最もコストが低い活動は事後分析とエスカレーションである。

表 2:

活動コスト

（100 万米ドル）

コスト活動センター	2016 年度	2018 年度	2019 年度	3 年間の純増
モニター & 監視	$9,610	$12,634	$22,124	79%
調査	$41,461	$78,398	$103,798	86%
エスカレーション	$8,919	$12,542	$21,805	84%
インシデント対応	$66,370	$91,263	$118,317	56%
データ封じ込め	$122,796	$173,060	$211,553	53%
事後分析	$8,498	$11,491	$19,480	78%
是正	$91,397	$138,532	$147,776	47%
合計	$349,052	$517,920	$644,852	60%

表 2 調査とエスカレーションにかかるコストの方が多い。
表 2修復コストは、他の活動のコストほど急増していない。

図 13：

3 つのプロフィールのインシデントごとにかかる平均コスト

（100 万米ドル）

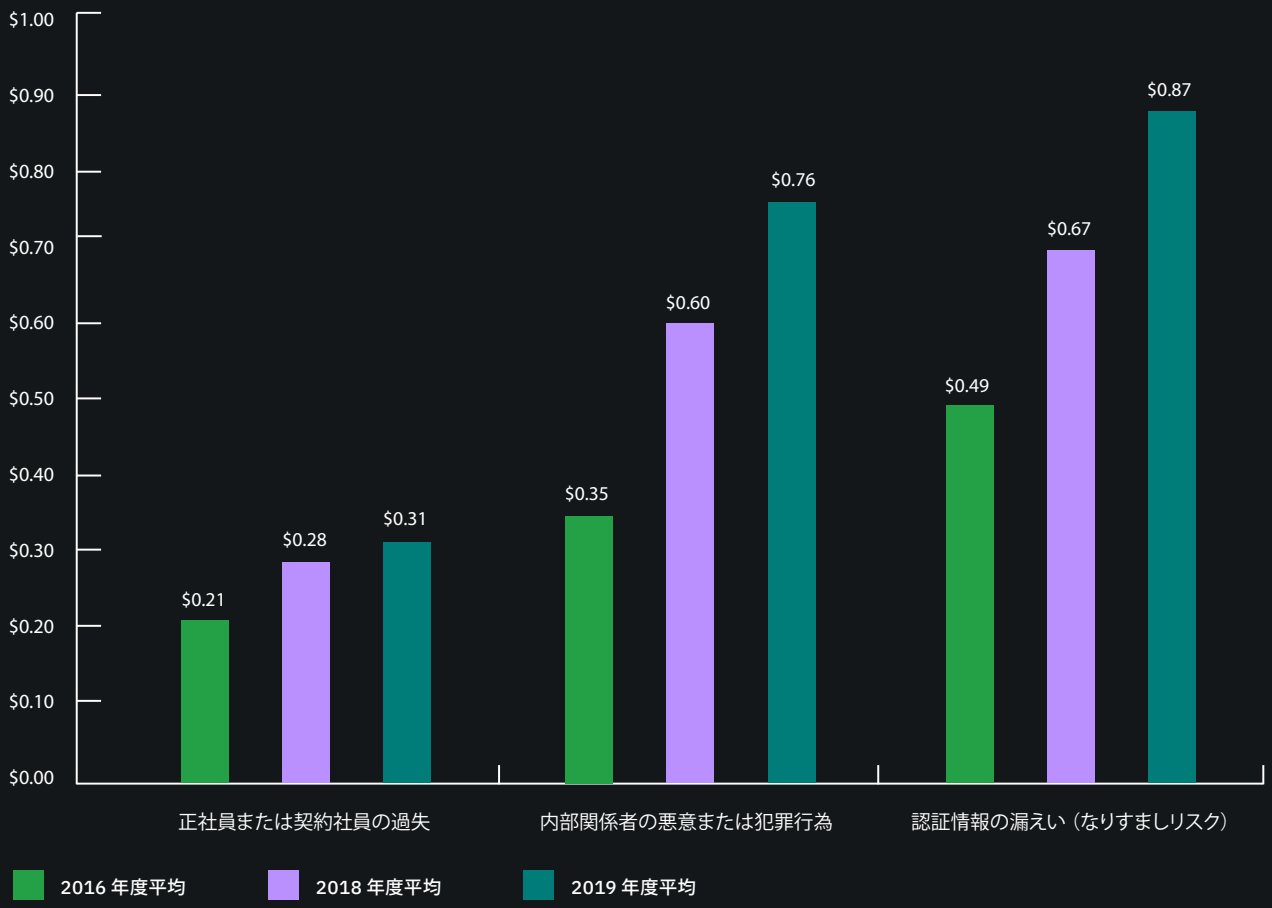


図 13 図 13 に示した通り、最もコストがかかるインサイダー・インシデントは認証情報の漏えいで、正社員や契約社員の過失によって起こるインシデントに比較して、2.5 倍以上のコストがかかる。

図 14：

3 プロフィールの平均年間コスト

（100 万米ドル）

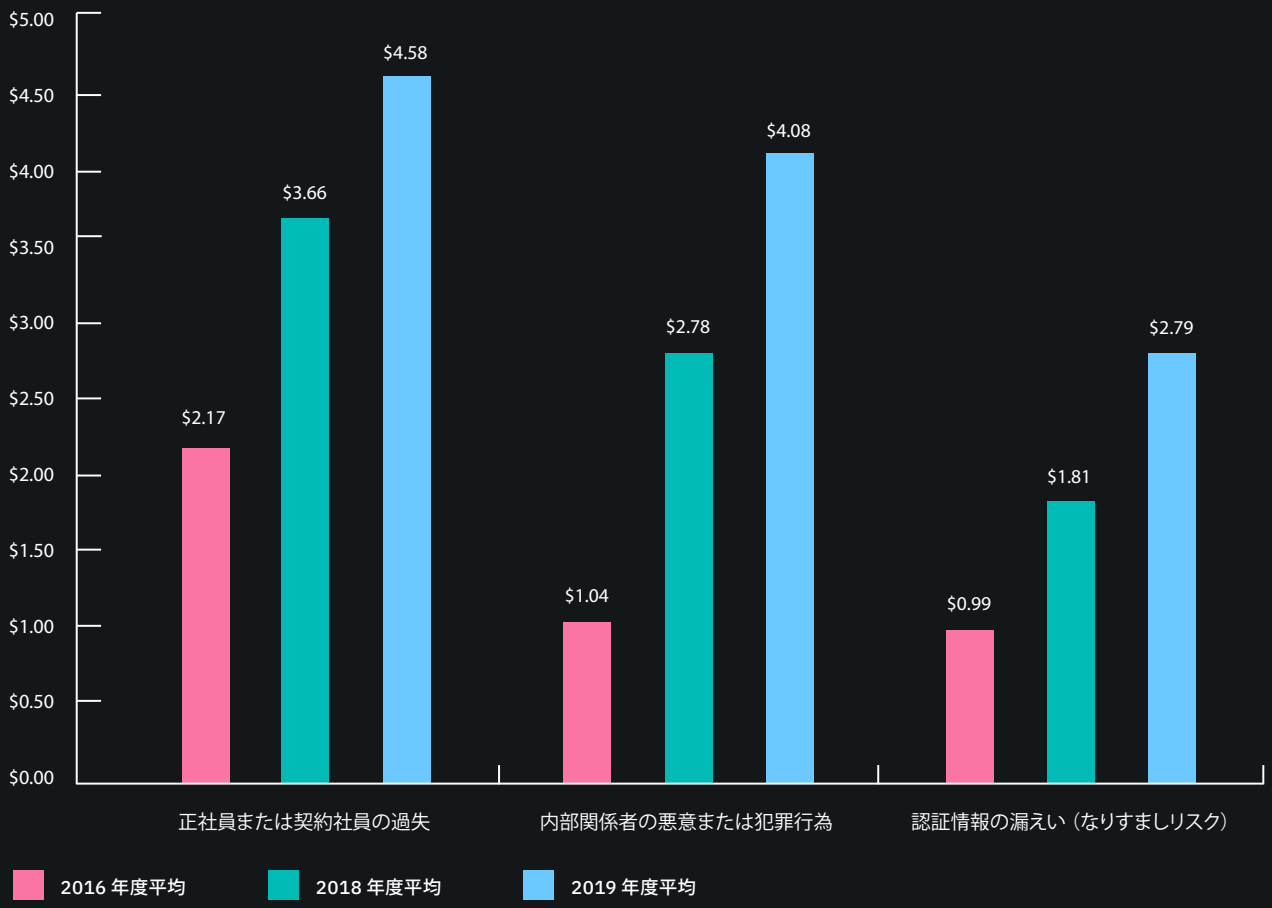


図 14 年間ベースで見ると、正社員または契約社員の過失インシデントにかかるコストが最も高かった図 14 は、3 つのプロフィールごとの内部関係者が関連するインシデントの年間コストを示す。年間コスト総額については、正社員または契約社員の過失が最もコストのかかるインサイダー・プロフィールであることが明らかである。単位コストで見ると認証情報の漏えいが最もコストが高いが、年間で見ると最もコストの低いプロフィールである。

図 15：

過去 12 か月間のインサイダー・インシデントのコストに関するサンプル統計

3 つのプロフィールを統合 （100 万米ドル）

図 15 は、過去 12 か月のインサイダー・コスト （3 つのプロフィール合計） の中央値、平均、最小、最大値を示す。平均と中央値は、それぞれ 1145 万ドル、1080 万ドルである。最小コスト値は 43 万ドルで、最大コストは 2699 万ドルである。

図 16：

活動ごとのインサイダー・インシデントのコスト比率

n = 204 社

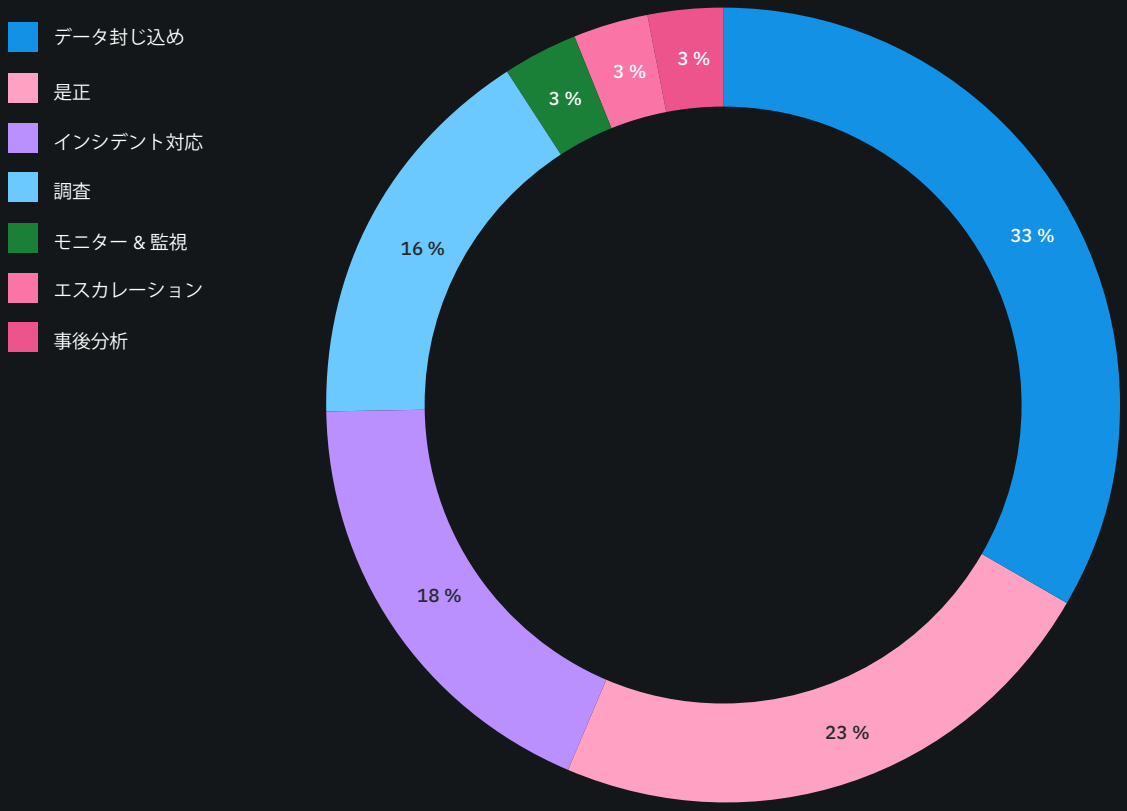


図 16 封じ込めがすべてのコストの 3 分の 1 を占める。上記の円グラフは、7 つの活動のコスト比率を示す。図 16 によると、封じ込めは、内部関係者関連の年間コスト総額の 33% を占める。修復とインシデント対応に関連する活動は、コスト総額に対しそれぞれ 23%、18% を占める。

図 17：
標準カテゴリー別のインサイダー・コスト比率

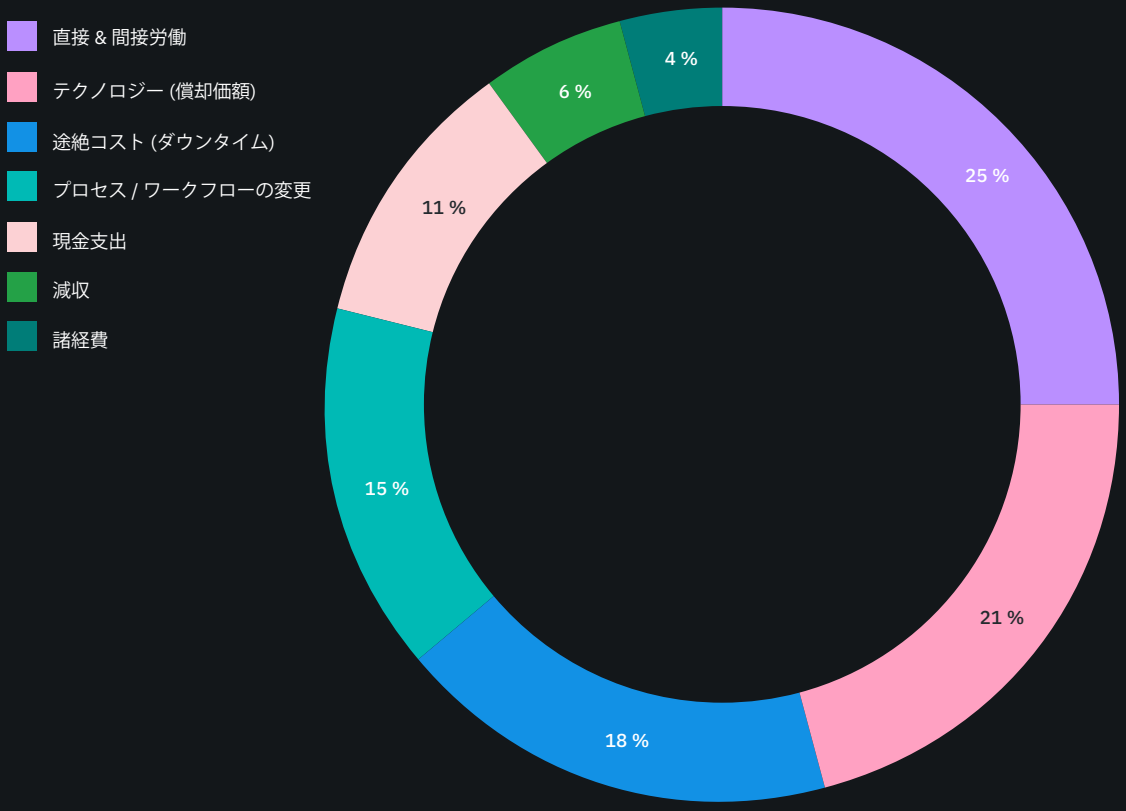


図 17 企業がインサイダー・インシデントを解決するために費やす経費の大部分は、人件費とテクノロジーに使われている。図 17 は、7 つのコスト・カテゴリーに従って、正社員の不注意または過失、内部関係者の犯罪行為、認証情報の漏えいによるインサイダー・コストの比率を示す。2 大コスト・カテゴリー （直接および間接工数） には、社内人員および派遣社員、契約社員に関連する直接および間接経費が含まれる。これに次いでコストが高いのはテクノロジーで、内部関係者が関連するインシデントに対応するために展開されたソフトウェアおよびハードウェアの償却価額およびライセンス料金が含まれる。

プロセス・コストには、脅威や攻撃に対応するための統治および統制システム活動が含まれる。サービス中止のコストには、インサイダー・インシデントの結果低下した正社員/ユーザーの生産性が含まれる。諸経費には、人員や IT セキュリティー・インフラの支援のために発生したさまざまな雑費が含まれる。

図 18：

活動の直接費と間接費の比率比較

3 つのプロフィールを統合

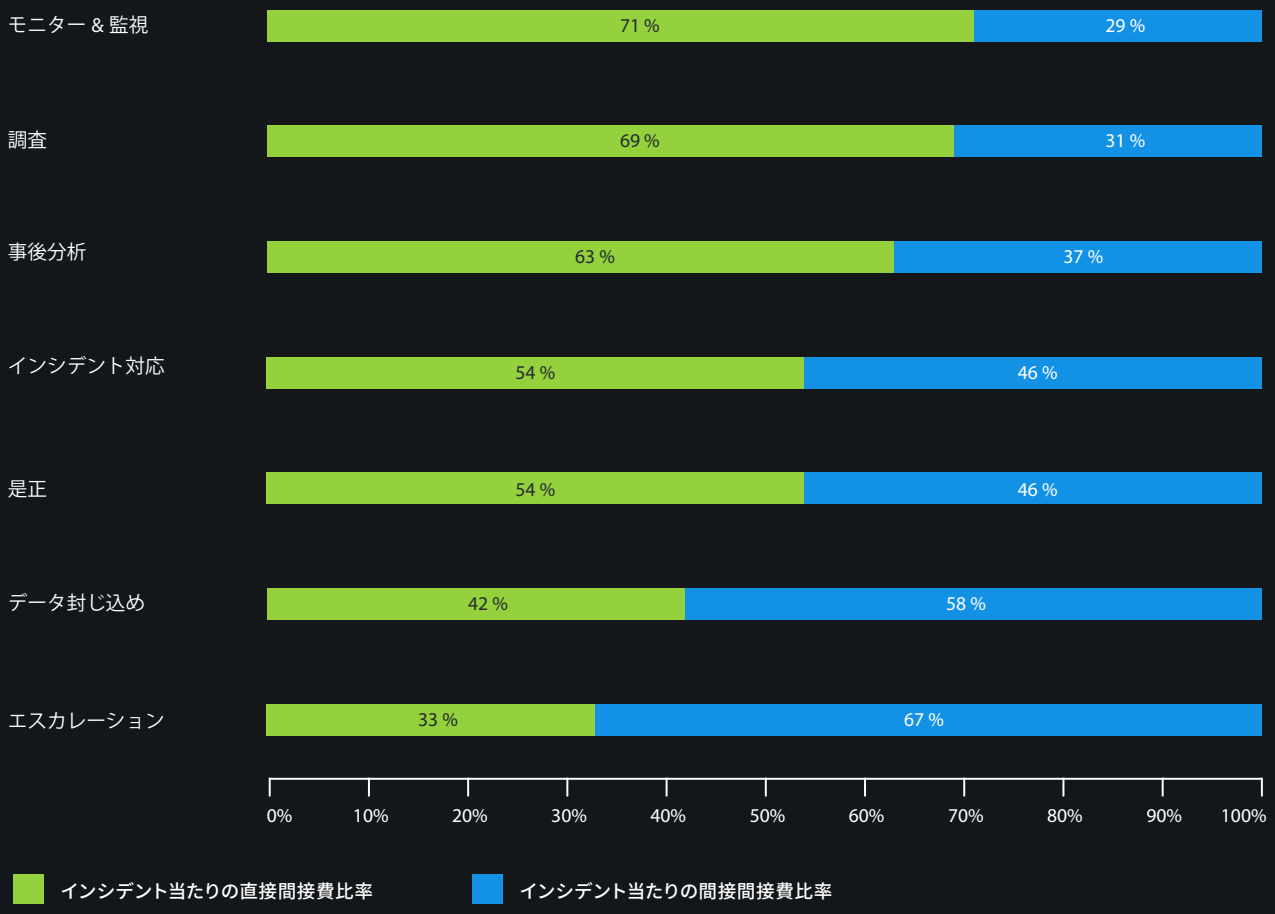


図 18 企業には、直接現金支出としてではなく 、特定の活動を確立するために費やされた直接費や時間、工数や他のリソース （間接費） を見積もるよう依頼した。図 18 は、7 つの内部活動コストについて直接および間接コストの比率を示したものである。図からわかるように、モニタリングおよび監視に関するコストが直接コストに占める割合が最も高かった。反対に、間接費で最も比率が高かったのはエスカレーションであった。

図 19：

内部関係者が関連するインシデントの封じ込め期間の比率分布

平均 77 日間

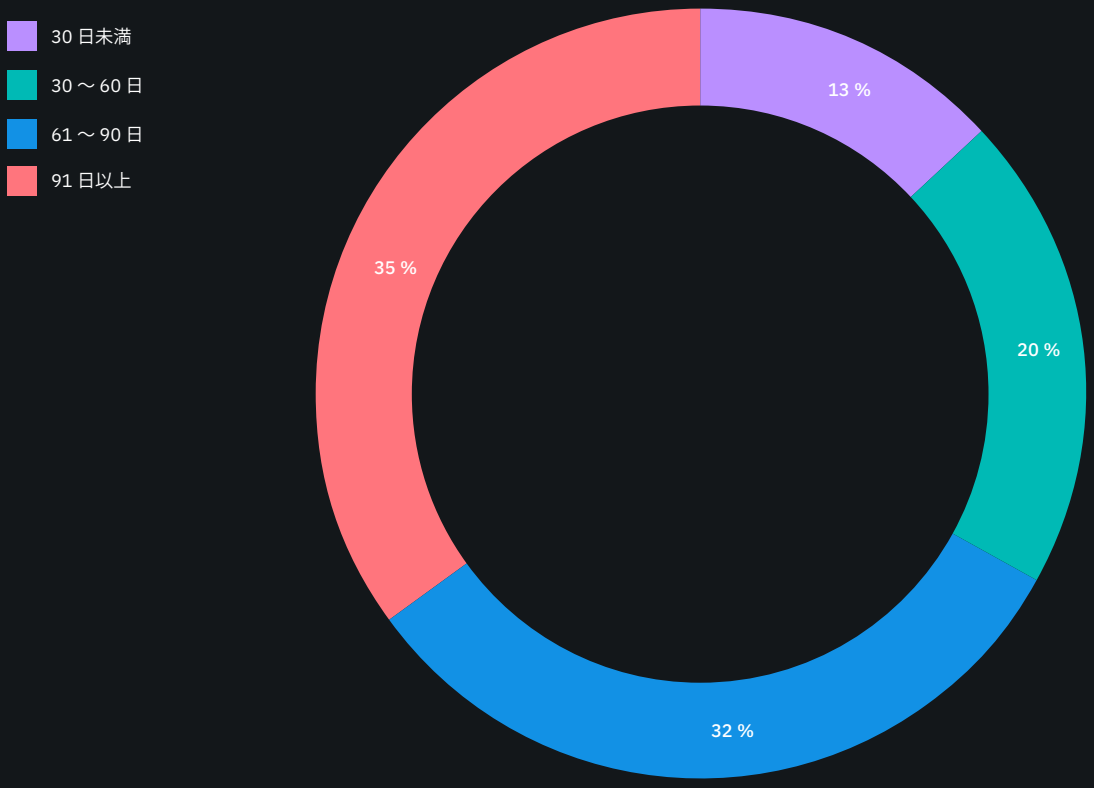


図 19 企業がインシデントの封じ込めにかかる期間は平均 2 か月以上である。図 19 によると、このベンチマーク・サンプル内で内部関係者が関連するインシデントの封じ込めにかかる時間は平均で 77 日だった。30 日未満で封じ込められたインシデントはわずか 13 %であった。

図 20：

インシデントの封じ込めにかかった日数別の平均活動コスト

平均 = 1145 万ドル

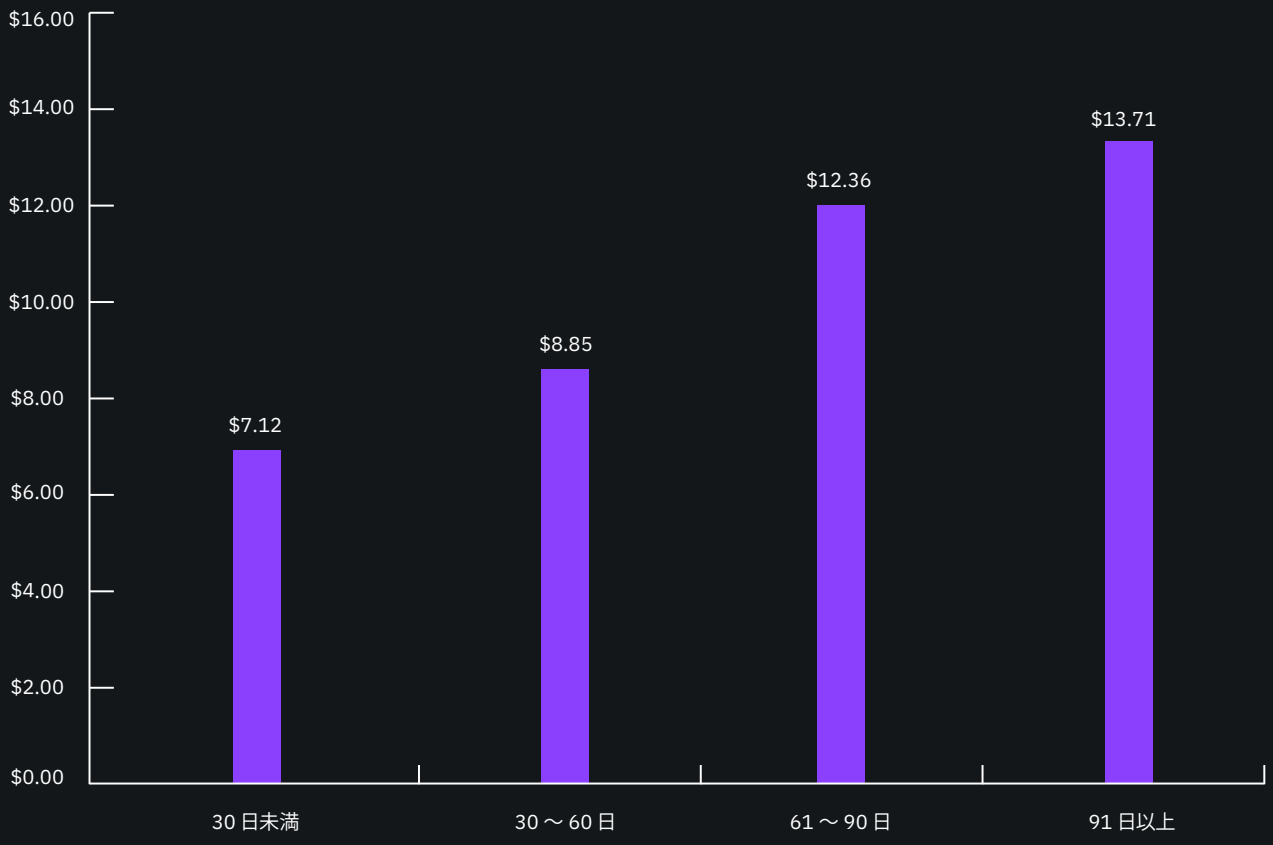


図 20 封じ込めにかかる時間が短いほど、コストは小さくなる。年間コスト総額は、内部関係者が関連するインシデントの封じ込めにかかる時間と正の相関関係があると考えられる。図 20 に示した通り、封じ込めに 90 日以上かかったインシデントは、年間コスト総額が平均で最も高かった（1371 万ドル）。反対に、30 日未満で封じ込められたインシデントは、年間コスト総額が平均で最も低かった（712 万ドル）。平均年間コストは 1145 万ドルである。

図 21：

業界部門別の年間活動コスト

平均 = 1145 万ドル

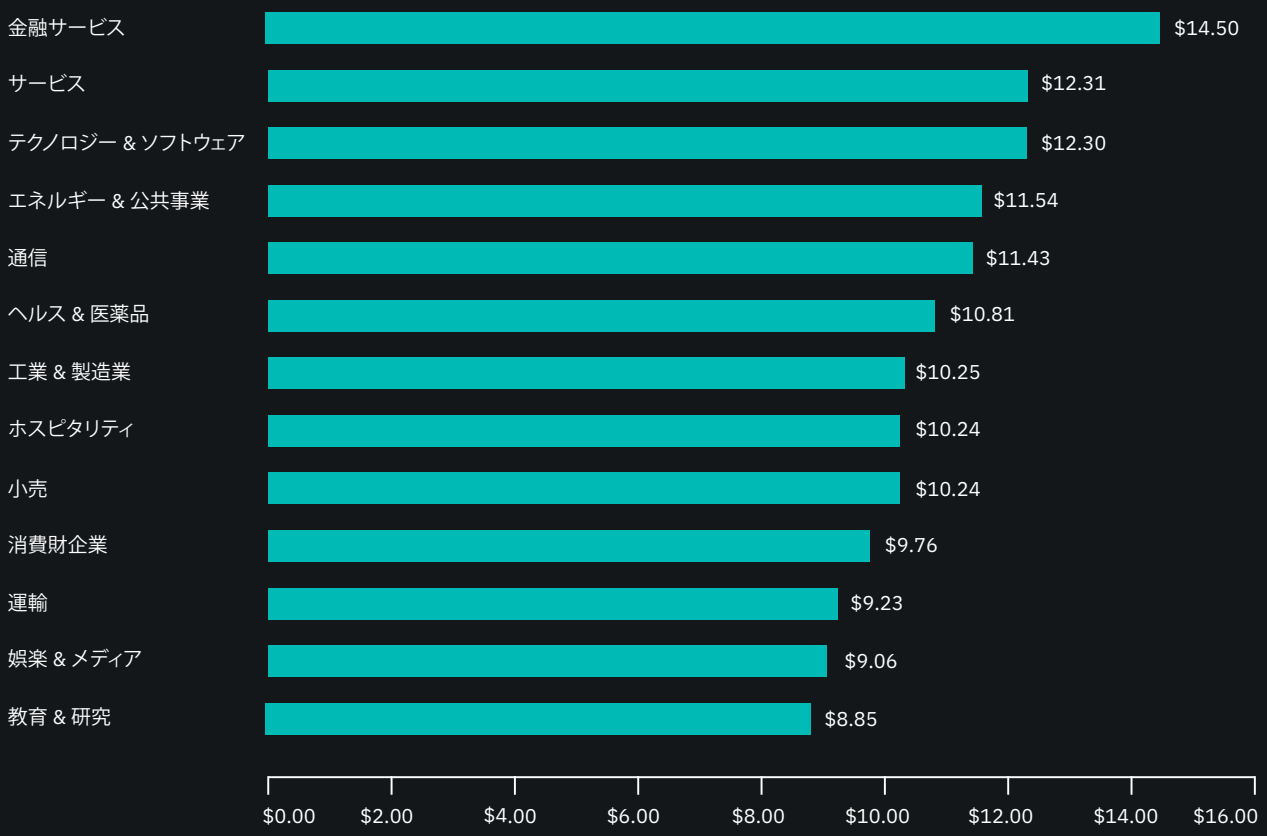


図 21 3 つの産業部門の年間コスト総額を図 21 に示した。[3] 金融サービス業界のコスト総額が最も高く、1450 万ドルであった。次にコストが高かったのはサービス業、テクノロジーおよびソフトウェア業界で、それぞれ 1231 万ドル、1230 万ドルであった。反対に、教育および研究業界の企業の年間コスト総額は最も低く、885 万ドルであった。

[3]業界部門間の差については、サブサンプル・サイズが小さいことを考慮されたい。

図 22：
企業ごとの、内部関係者が関係したインシデントの散布図
n = 204 社

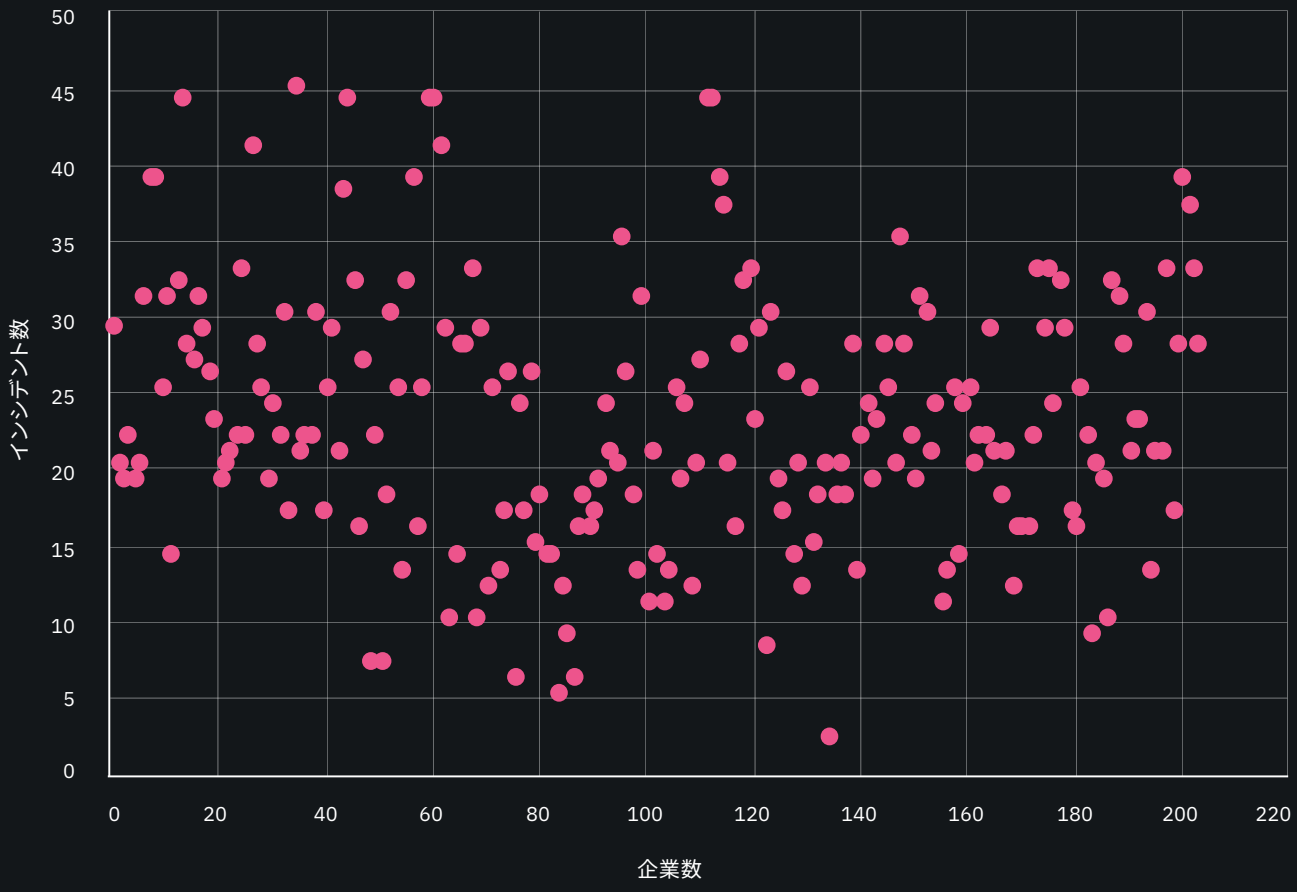


図 22 は、企業別のインサイダー・インシデントの年間コスト総額の散布図である。204 社の回答企業の内、124 社 （61%）の過去 12 か月の平均コスト総額は平均値 1145 万ドル、またはそれ以下であった。残りの 80 社 （39%） は平均の 1145 万ドル以上であった。この結果から、分布は歪んでいることが考えられる。

[3]業界部門間の差については、サブサンプル・サイズが小さいことを考慮されたい。

表 3:

インサイダー脅威の低減につながったツールと活動

セキュリティツール & 活動	企業頻度	企業割合
ユーザートレーニング & 意識	112	55%
データの情報漏洩対策 (DLP)	110	54%
ユーザー行動分析 (UBA)	102	50%
従業員のモニター & 監視	96	47%
セキュリティインシデント & イベント管理 (SIEM)	91	45%
インシデント対応管理 (IRM)	89	44%
厳格なサードパーティ審査手順	87	43%
脅威インテリジェンスの共有	85	42%
特権アクセス管理 (PAM)	80	39%
ネットワークトラフィックインテリジェンス	77	38%

表 3 表 3 のように、企業の大多数で、インサイダー脅威防止のためのユーザー意識向上教育 (55%) 、データ漏えい防止 (54%) 、ユーザー行動分析 (50%) の取り組みが実施されている。

図 23：

サイバー・リスク低減ツールおよび活動の導入によるコスト節減

平均 = 1145 万ドル

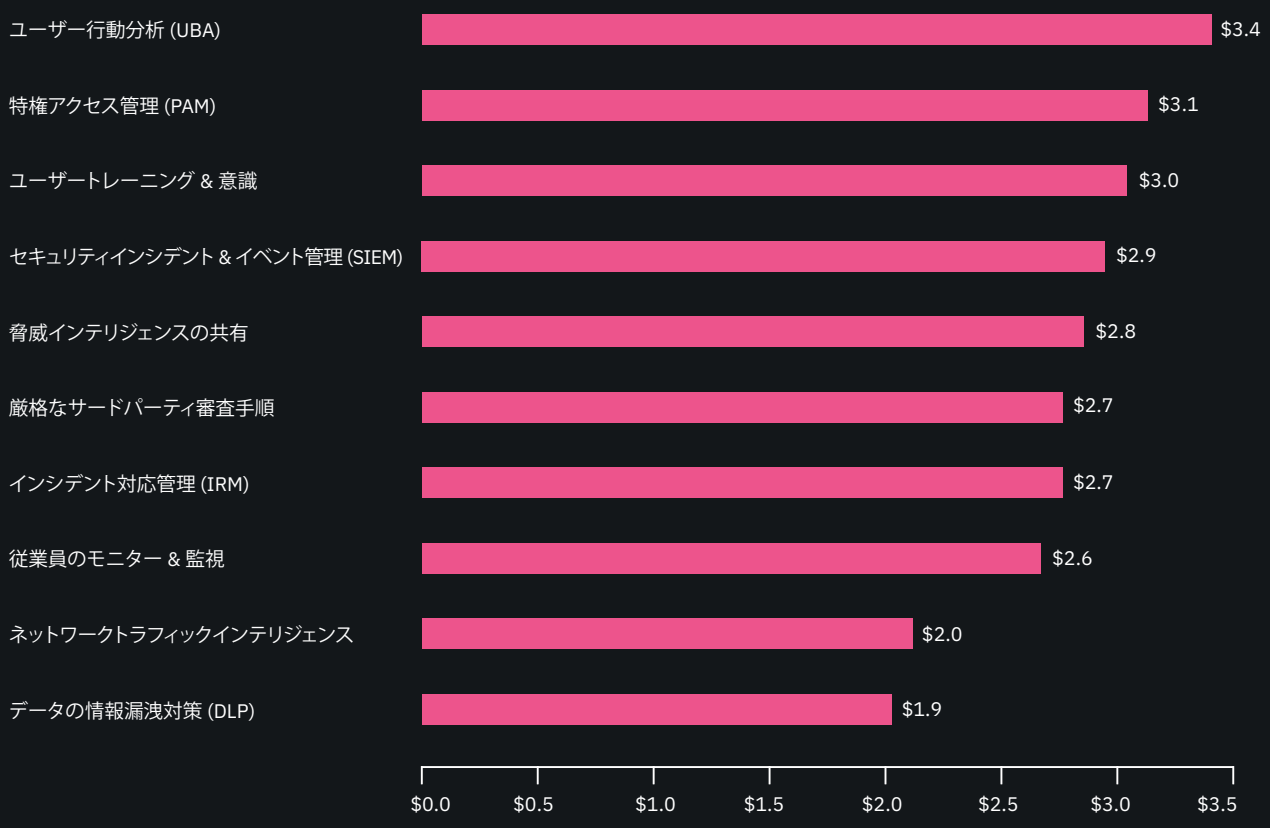


図 23 UBA、PAM およびユーザー意識向上教育は、最も効果的なツールおよび活動である。図 23 からわかるように、UBA および特権アクセス管理 （PAM） ソリューションを導入することで、それぞれ平均 340 万ドル、310 万ドルを節減できる。最も導入頻度の多いツールと活動を表 3 に示した。表によると、112 社の企業で、インサイダー脅威について従業員の意識を向上するためのトレーニング・プログラムが実施されている。データ漏えい防止ツールを使用している企業の数は 110 社で、疑わしいネットワーク活動を検出するユーザー行動分析 （UBA） が導入されているのは 102 社であった。

フレームワーク

本調査の目的は、インサイダー脅威が原因で発生するコストの種類についてガイダンスを提供することです。このコスト調査の特徴は、内部関係者の過失や犯罪行動に対する企業の対応に関連し発生するさまざまな経費の原因となる基幹システムやビジネス・プロセス関連の活動に言及している点にあります。本調査では、企業の基幹データ、ネットワークまたはエンタープライズ・システムの衰退の原因となる内部関係者が関連するインシデントを定義します。これには、正当な従業員/ユーザーの認証情報を不正に取得した部外者による攻撃も含まれます。

このベンチマーク方法では、内部関係者が関連するインシデントの実際の実例と結果を抽出することを目的としました。各組織のさまざまな幹部レベルの個人と面談によって得た回答から、2 つの異なるコスト傾向に従ってコストを分類しました。

インサイダー脅威の最小化に関連するコスト（内部コスト活動中心）

インシデントの結果に関連するコスト（事象または攻撃の外的影響）

社内コスト中心は、インサイダー脅威環境のモニタリングと監視から始まって、修復活動の終了まで、時系列的に分析しました。商機の損失や業務の中止によるコストも含めました。各コスト活動中心について、回答者に直接費、間接費、該当する場合は機会費用を見積もることを依頼しました。これらは以下のように定義されます。

直接費 – 特定の活動を行うために支出される直接経費

間接費 – 直接の現金支出としてではないが、費やされた時間、工数、およびその他の組織資源

機会費用 – インシデントが原因で評判が失墜したことにより失われた商機から発生した経費

情報資産の喪失、業務の中止、設備の損害、減収などの外部経費はシャドウ・コスト法を使って計算した。コスト総額は 7 つの異なるコスト項目に割り当てられた。[4]

このコスト調査では、内部関係者が関連するインシデントに対する企業の対応に関連して発生するさまざまな経費の原因となる基幹システムやビジネス・プロセス関連の活動を対象とする。本調査のフレームワークでの 7 つの内部コスト活動は以下のように規定される。[5]

モニタリングと監視： 企業がインサイダー・インシデントや攻撃を合理的に検知し、防止できる可能性のある活動。これには、リスク低減や早期発見を促進するための特定のテクノロジーに割り当てられた （諸経費） コストが含まれる

調査： 1 つ以上のインシデントの発生源、範囲、規模を完全に把握するために必要な活動

エスカレーション： 企業内の主な利害関係者間で実際のインシデントについて意識を高めるために行われる活動。このエスカレーション活動には、初期管理対応を組織するために取られる手順も含まれる

インシデント対応： 最終管理対応を策定するために取られた手順を含め、インシデント対応チームの編成と関与に関連する活動

封じ込め： インサイダー・インシデントまたは攻撃を阻止、またはその重大性を軽減するための活動。これには、脆弱性のあるアプリケーションやエンドポイントの閉鎖が含まれる

事後対応： 今後、組織が内部関係者が関係するインシデントおよび攻撃が発生する危険性を最小限にくいとめるための活動。これには、被害を最小限に食い止めるための推奨事項の作成など、社内および社外の主な利害関係者に通知するための手順も含まれる

修復： 修復に関連する活動や 組織のシステムや基幹プロセスの復旧や修復に関連する活動。これには、被害を受けた情報資産や IT インフラの修復が含まれる

[4]これら 7 つのコスト・カテゴリーは、相互に独立しておらず、すべてのコスト活動を網羅する包括的なものではないことを認識されたい。

[5]内部コストは、直接および間接コストを示す労働 （時間） を使用して推算した。この方法は、テクノロジーに対する複数年にわたる投資などの固定費の諸経費部分を割り当てるためにも使用される。

上記のプロセス関連の活動に加え、組織では、外的影響やインシデントの余波に関連するコストが発生することが多い。
本調査では、これらの外的影響に関連する 4 つの一般的なコスト活動を示す。

情報の喪失または漏えいのコスト: インサイダー攻撃の結果発生した機密情報の喪失または漏えい。このような情報には、知的財産 （ソース・コードを含む）、顧客情報、従業員レコードなどが含まれる。このコスト・カテゴリーには、個人情報が不正に取得された事象を受けてデータが漏えいしたことを通達するコストも含まれる

業務の中止コスト： 組織がデータ処理要件を満たせなくなる、ダウンタイムや計画外のサービス中止が与える経済的影響

設備への損害コスト： 情報リソースや重要なインフラに対するインサイダー攻撃の結果として発生した設備やその他の IT 資産への損害を修復するコスト。

減収： インサイダー攻撃の結果として発生したシステム遅延やシャットダウンを原因とする顧客 （顧客離れ） や他の利害関係者の喪失。このコストの見積もりには、各回答組織について定義された平均的な顧客の「生涯価値」を基に、シャドウ・コスト法を使用した。これには、被害を受けた情報資産や IT インフラの修復が含まれる

ベンチマーク

このベンチマーク方法は、実際に検知された内部関係者が関連したインシデントまたは攻撃の結果、直接または間接的に発生した実際のコストに関して、IT、情報セキュリティーおよび他の重要な個人から情報を収集することを目的としています。このコスト法では、対象者は実際の会計結果を提供する必要はなく、4 週間にわたる面談データからの見積もりと推算を基に計算します。

コスト見積もりは、各ベンチマーク調査対象組織内の主な回答者との内密の面談による診断を基に計算します。データ収集法では、実際の会計情報は含まれず、各回答者の知識と経験を基にした数値見積もりを基に計算しました。カテゴリーごとにコスト見積もりは 2 段階プロセスで計算されました。まず、このベンチマーク法では、回答者が以下の数字行形式で定義された範囲変数にチェックを付けることで各コスト・カテゴリーの直接費見積もりを評価してもらいます。

数字行の使用方法：各データ漏えいコストのカテゴリーの下にある数字行を用いて、発生した現金支出、工数、諸経費の総額を見積もってください。上記に設定された下限と上限の中から 1 点のみにチェックを付けてください。調査実施中、いつでも数字行の下限と上限を再設定できます。

［対象のコスト・カテゴリー］の直接費の見積額をここに回答してください。

下限
上限

各コスト・カテゴリーの推算値ではなく、数字行から数値を得ることにより機密性が守られ、回答率が向上します。このベンチマーク法では、間接費と機会費用のそれぞれについて二次見積もりを提供してもらいます。

次に、これらのコストの相対規模を基に、特定のカテゴリー内の直接費と比較して、組織ごとにコスト見積もりを計算します。最後に、内部関係者が関連するインシデントまたは攻撃の結果発生する見積もり減収額を含め、追加の要素を収集するための一般的な面談を行いました。

調査項目の規模と範囲は、異なる業界部門にわたる既知のコスト・カテゴリーに限定されています。これまでの経験から、プロセスを対象とした調査の方が回答率が高く、結果の品質も高くなります。また、機密性を保証するために、電子調査ではなく、書類による方法を使用しました。

完全な機密性を維持するため、調査法ではいかなる種類の企業固有の情報は収集していません。調査対象の素材には、追跡コードなどの回答企業と回答を紐付けるいかなる方法も含まれていません。
ベンチマーク方法を管理可能な規模に抑えるため、コストの測定に不可欠と考えられるコスト活動のみに項目を限定しました。経験豊富な専門家との討議を基に、直接費または間接費活動の限定されたグループに最終項目を絞りました。ベンチマーク情報を収集した後、各方法の一貫性と完全性を慎重に調査しました。本調査では、回答が不完全、一貫性がない、または無回答であったため、対象企業から数社を除外しました。

米国以外の通過の為替レートは、本調査のタイムフレームの時点で最新です。実地調査は 2019 年 3 月に開始されました。すべてのベンチマーク企業の一貫性を維持するため、組織の体験についての情報は連続した 4 週間に限定しました。この時間枠は、本調査の他の組織と同じとは限りません。推算された直接費および間接費は、4 週間にわたって収集されたコスト総額を分割することによって年間コストを計算しました (比率 = 4/52 週間)。

限界

本調査では、過去の調査で導入され成果が実証された機密性が高く独自のベンチマーク方法が使用されています。ただし、このベンチマーク調査には、結果から結論を導き出す前に慎重に考慮に入れる必要がある本質的な限界があります。

非統計的な結果：
本調査は、過去 12 か月間に内部関係者が関連したインシデントが 1 件以上発生した組織の代表的な非統計的サンプルを対象としています。このサンプリング方法は科学的でないことから、これらのデータに統計的推論、誤差、信頼区間は適用することができません。

無回答：
現在の結果は、小規模で代表的なベンチマーク・サンプルを基に導かれています。このグローバル調査では、507 社がベンチマーク・プロセスを完了しました。
無回答バイアスは検証されていないため、回答しなかった企業が、根本的なデータ漏えいコストの観点から大きく異なっている可能性があります。

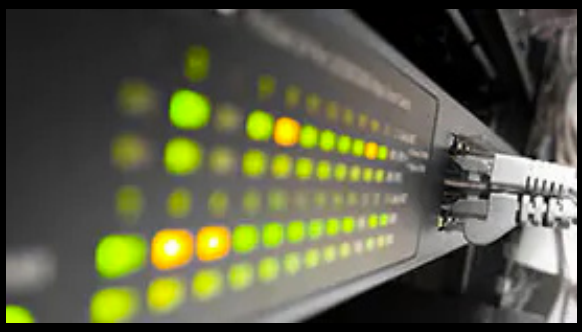
サンプルフレームのバイアス：
このサンプリング・フレームは判断によるため、結果の品質は、調査対象の企業の集団を表わす程度によって影響を受けます。現在のサンプリング・フレームは、より成熟したプライバシーまたは情報セキュリティー・プログラムが策定された企業寄りに偏っていると考えられます。

企業固有の情報：
ベンチマーク情報には機密情報が含まれます。このため、現在の方法では会社が特定できる情報は収集されていません。また、この方法では、個人は、明確な回答変数を使用して企業や業界カテゴリーに関する人口統計学情報を開示することができます。

係数が未測定：
質問の一貫性を守り、的を絞ったものにするため、主な傾向や組織の特性などの他の重要な変数を省略して分析しました。
省略された変数がベンチマーク結果をどの程度説明できたかについては判断できません。

推算されたコスト結果：
ベンチマーク調査の質は、参加した企業の回答者によって提供された信頼性のある回答の整合性を基に決定されます。特定のチェックや相殺がベンチマーク・プロセスに統合されているとはいうものの、回答者が正確で真実の回答を返さなかった可能性は常にあります。また、 コスト推算方法を実際のコスト・データの代わりに使用したことにより、意図しないバイアスや不正確性が発生している可能性があります。

次のステップ

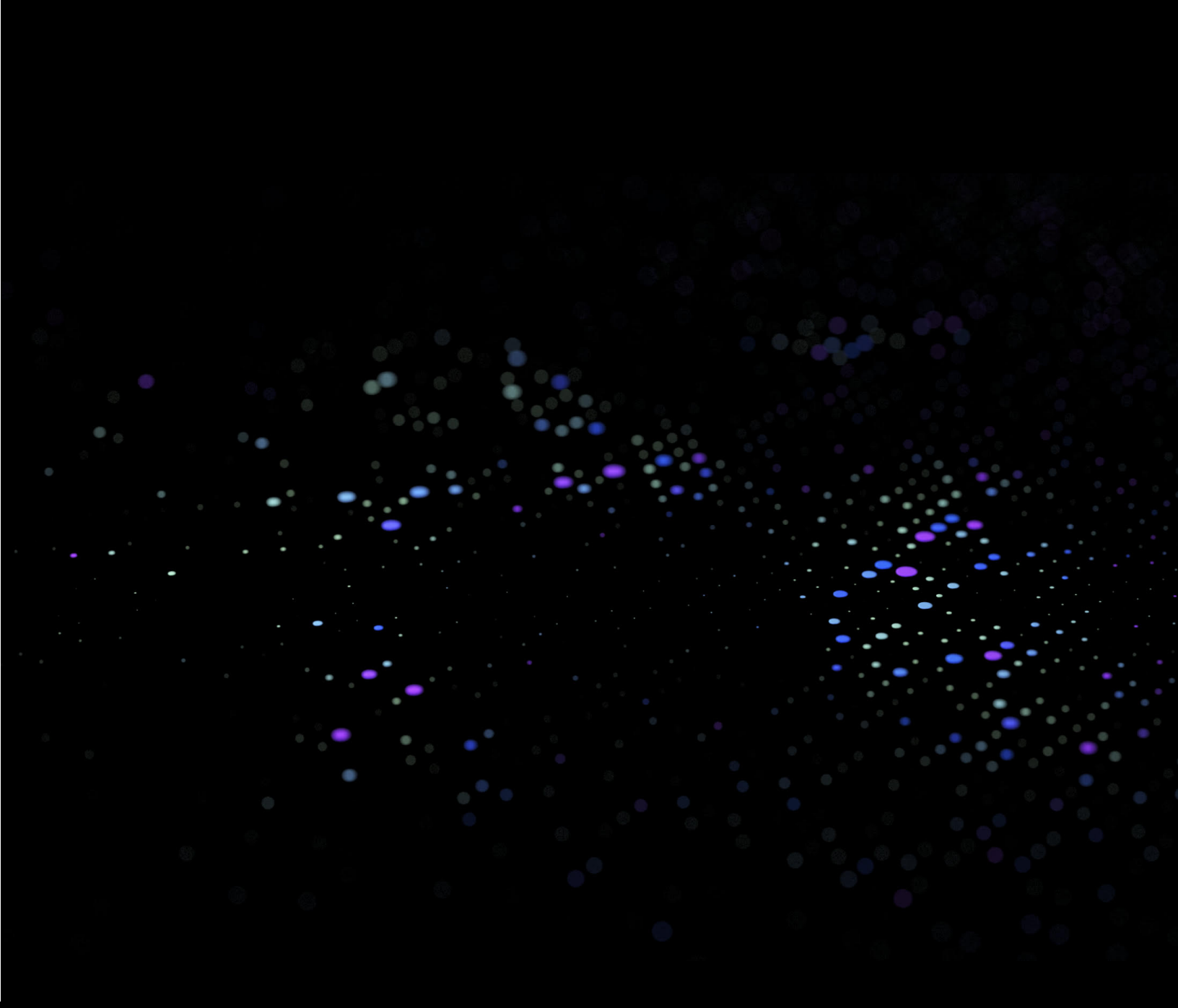


デジタル・トラストの提供
シームレスなユーザー体験でお客様の組織をインサイダー脅威から守り、事業を拡大しましょう。

資産の保護
アプリやエンドポイントを通して安全なデータ・フローを保証しましょう。

IDの脅威
脅威の検知と対応を企業全体で自動化しましょう。

修復と対応
高度で継続的な脅威や最新型の攻撃を分析し対応しましょう。



本調査報告について不明な点やご意見・ご感想がおありの場合、または本書の複写が必要な場合 （本レポートを引用または再利用する許可を含め） は、文書、電話、または電子メールにて以下ま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

インサイダー脅威のコスト・レポートは、IBM Security および Observe IT の協賛により作成されました。
昨年のデータ漏えいのコスト・レポートは、以下から入手できます。**ibm.com/**security/data-breach

Ponemon Institute LLC
Advancing Responsible Information Management

Ponemon Institute は、企業および政府内における責任ある情報およびプライバシー管理方法を促進する、独立した調査および教育機関です。当研究所の使命は、人や組織に関する機密情報の管理とセキュリティーに影響を与える重要な問題について、高品質で経験的な調査を行うことです。

当研究所は、厳格なデータ機密性、プライバシー、倫理的な調査基準を支持しています。当研究所が、個人から個人を特定できる （あるいはビジネス調査の場合、会社を特定できる）情報を収集することはありません。また、調査対象者に無関係で不適切な質問をしないよう、厳格な品質標準を規定しています。

IBM Security について

IBM Security は、企業向けセキュリティー製品およびサービスの最も先進的で統合されたポートフォリオを提供します。世界的に評価されている IBM X-Force の調査に基づいたポートフォリオは、組織による脅威の阻止、コンプライアンスの証明、安全な成長に役立つセキュリティー・ソリューションを提供します。

IBM は、最も多様で専門的なセキュリティー調査を、開発、提供している組織の 1 つです。IBM は、130 か国以上で毎月 2 兆以上の事象を監視し、3,000 以上のセキュリティー特許を取得しています。詳細については、**ibm.com/**jp-ja/securityをご覧ください。

IBM **Security**