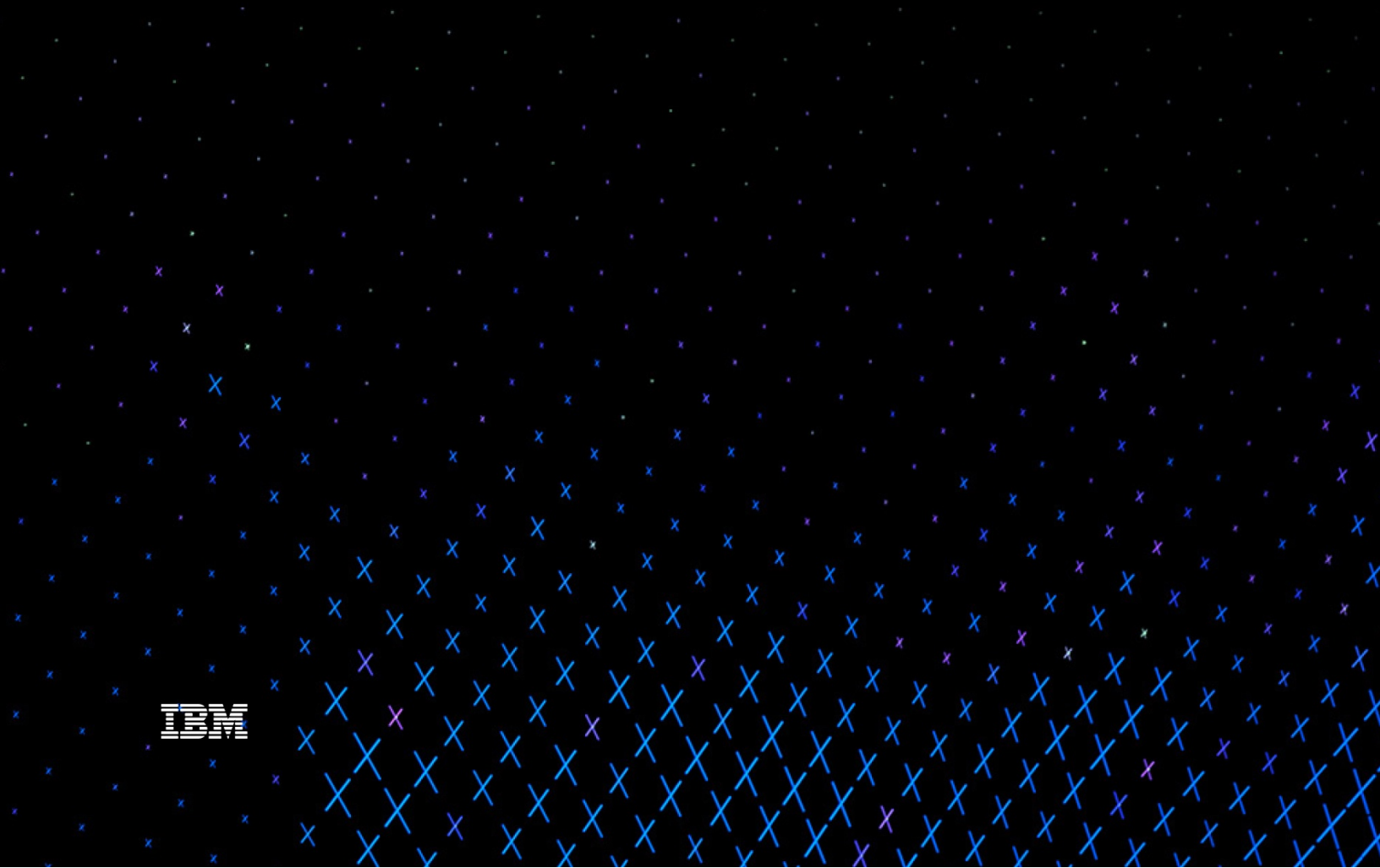
IBM Security

サイバー・レジリエンス・レポート (2020 年版)



IBM

目次

エグゼクティブ・サマリー

サイバー・レジリエンスを備えた組織に関する第 5 回目の年次レポートは、2020 年 4 月に米調査会社 Ponemon Institute が実施した調査に基づいています。この調査は、サイバーセキュリティー・インシデントの検知、防御、封じ込め、対応における組織の能力を明らかにすることを目的に、世界各国の 3,400 名を超える IT とセキュリティーの専門家を対象に行われました。

サイバーセキュリティー・インシデントの発生件数は増加しており、IT プロセスとビジネス・プロセスに大きな混乱をもたらしています。と同時に、高水準のサイバー・レジリエンスを実現したと述べた組織の割合は、2015 年の 35% から 2020 年の 53% へと 51% 増えています。サイバー・レジリエンスを備えた企業とは、データ、アプリケーション、IT インフラストラクチャーへの重大な多くの脅威に対して、防御、検知、封じ込め、対応を効果的に実施できる企業のことです。

現在、回答者の 4 分の 1 超がサイバーセキュリティー・インシデント対策（CSIRP : Cyber Security Incident Response Plan）を企業全体に一貫して採用し、サイバー・レジリエンスの実現を図っています。組織の多くは、自動化、機械学習、AI、クラウド、オーケストレーションを使用してセキュリティー環境を強化しています。

しかし、リソースと予算上の制約、脅威の継続的高度化、IT 環境の複雑性から、セキュリティー・チームのサイバー攻撃封じ込め能力低下に至るまで、課題は依然として山積みです。

このレポートでは、全体的なサイバー・レジリエンスを改善するために組織が取るべきアプローチとベスト・プラクティスについて考察します。強固なセキュリティー体制の一環として、サイバー攻撃にさらされてもビジネスの中断を最小限に抑えるサイバー・レジリエンスの重要性について詳しく説明します。最後に、組織がサイバー・レジリエンスを強化するのに役立つ推奨事項を提案します。

サイバー・レジリエンス・レポートが示す事実

51%

サイバーセキュリティー・インシデントが原因で過去 2 年間に**深刻なビジネスの中断**が生じたと報告した組織の割合

26%

CSIRP を企業全体に適用している組織の割合

55%

自動化ツール使用によりサイバー・レジリエンスが改善したと報告したパフォーマンスの高い組織の割合

52%

クラウド・サービスによりサイバー・レジリエンスが改善したと述べた回答者の割合

45

採用している**セキュリティーのソリューションとテクノロジー**の平均数

2020 年版で追加された調査項目

セキュリティー対応を取り巻く環境の変化を踏まえて、今年のレポートでは、クラウド・サービスの使用によりどのようにサイバー・レジリエンスが改善されたか、また、その主な利点は何かについて初めて調査しました。さらに、マルウェアやフィッシングをはじめとする、一般的なセキュリティー攻撃に対処するために行った、個別の対策についての質問も追加されました。

この質問事項は、昨年取り入れたセキュリティー・ソリューションの数に関する質問を発展させたもので、セキュリティー・インシデントの調査と対応に使用されたツールの数について理解を深めることを目的とします。

昨年に倣って、サイバー・レジリエンスが最も高い組織（ハイ・パフォーマー）を特定し、その差別化要因を明らかにすることにより、サイバー・レジリエンスを測定するベンチマークを作成しました。このレポートでは、自動化ツールの活用、クラウド・サービスの使用、相互運用性の重視など、パフォーマンスの高い組織がサイバー・レジリエンスのレベル向上に役立てている戦術に着目します。

主な調査結果

CSIRP を採用している組織では**ビジネスの中断が減少**しました。

サイバーセキュリティー・インシデント対策 (CSIRP) はビジネスの中断を最小限に抑制

CSIRP の企業全体での適用は徐々に改善しており、2015 年から 44% 増加しています。利点が明らかで使用範囲も拡大しているにもかかわらず、回答者の 51% は CSIRP が企業全体に一貫して適用されていない、あるいは、非公式または一時的な適用にとどまっていると述べました。

CSIRP を公式に採用している組織のうち、DDoS やマルウェアなどの一般的な攻撃に備えて攻撃別の対応マニュアルを準備している組織は 3 分の 1 に過ぎません。ランサムウェアなどの新たな脅威に対する対策を採用していた回答者はさらに少なくなっています。

加えて、CSIRP の見直しを 3 カ月ごとに実施していた組織は 7 %に過ぎず、この数値は過去 5 年間でほぼ横ばい状態です。実際、対策の見直しや更新の期間を設けていない組織は 40% にのぼり、2015 年から 8% 増加しています。 最新の CSIRP を企業全体に適用していない場合、IT プロセスと ビジネス・プロセスで大きな混乱を経験した組織は 23% 多くなっています。

すべての攻撃を阻止することは不可能ですが、適切な準備とプロセスがあれば被害を大幅に減らすことができます。本調査で明らかにされた CSIRP に関わるデュー・ディリジェンス（注意義務）が欠如しているために、攻撃性が増している脅威環境での CSIRP の有効性が限定的となるおそれがあります。

-8%

50 以上のツールを使用している組織は、サイバー攻撃検知能力で**8% 低く**ランク付けされました。

使用ツールが多すぎるとサイバー・レジリエンスは弱まるが、自動化、可視性、相互運用性によりインシデント対応は改善

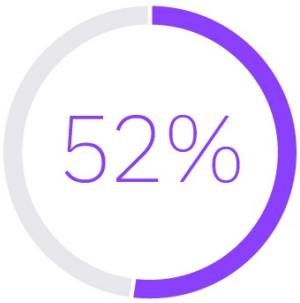
組織は、セキュリティー環境の管理とサイバーセキュリティー・インシデントへの対応で大量のツールを使用していました。組織のほぼ 30% は 50 を超える個別のセキュリティーのソリューションとテクノロジーを使用し、45% は 20 を超えるツールを使用してサイバーセキュリティー・インシデントの調査と対応に取り組んでいました。

しかし、ばらばらのツールの過剰使用により環境は複雑になり、効率の低下を招くことがあります。今回の調査により、組織が使用していたセキュリティーのソリューションとテクノロジーの数が、サイバーセキュリティー・インシデントの検知、防御、封じ込め、対応の能力に悪影響を及ぼしていたことが判明しました。

実際、使用ツールが 50 を超える企業は、50 以下のツールを使用していた企業と比べて、サイバー攻撃検知能力では 8% 低くランク付けされており、攻撃対応能力では 7% 低くランク付けされていました。

アプリケーションとデータの可視性は、過去 3 年間にわたって組織がサイバー・レジリエンスを改善する主要な方法の 1 つでした。今年は、自動化がもう 1 つの説得力のある方法として浮上しており、ハイ・パフォーマーでは特に顕著です。相互運用ツールの使用がサイバー・レジリエンスの向上に役立ったと報告したのは、ハイ・パフォーマーでは 63% なのに対し、他の組織では 46% でした。

相互運用性を重視することは、複数ベンダーのソリューション間で特に求められる可視性の実現に役立つと同時に、複雑性も軽減します。



クラウド・サービスによりサイバー・レジリエンスが改善したと述べた回答者の割合

クラウド・サービスがもたらすサイバー・レジリエンスの向上

回答者の 52% は、クラウド・サービス使用によりサイバー・レジリエンスが改善したと述べています。ハイ・パフォーマーにおいてはサイバー・レジリエンス改善の理由として 63% がクラウド・サービス使用を挙げていますが、他の組織では 49% でした。

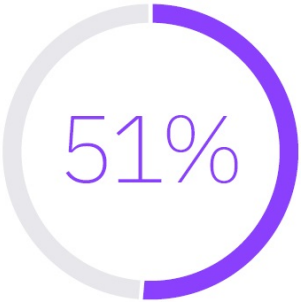
予想に違わず、クラウド早期導入者の金融サービス機関では 60% が、クラウド・サービス使用で自社のサイバー・レジリエンスが改善したと述べています。医療と小売の組織や公共部門も、クラウド・サービスのおかげで平均を上回る改善が実現したと報告しています。医療と小売りの組織や公共部門も、クラウド・サービスのおかげで平均を上回る改善が実現したことを報告しています。

英国、ドイツ、フランス、米国、カナダの企業は、率先してクラウド・サービスを高く評価し、サイバー・レジリエンスの実現に欠かせないとしています。具体的には、これら国々の 3 分の 2 を超える組織がクラウド・サービス使用を重視しています。

クラウド・サービスが改善をもたらした主な理由としてハイ・パフォーマーが挙げたのは、分散環境の活用、規模の経済、可用性に関するサービス・レベル・アグリーメントがもたらすメリットでした。他方、組織の 30% は、クラウド・サービスが適切に構成されていないためにサイバー・レジリエンスの進展が妨げられたことを伝えていました。

クラウド・サービスに投資するだけでは不十分であり、有効な環境を実現するには最適化が絶対に必要です。

その他の洞察

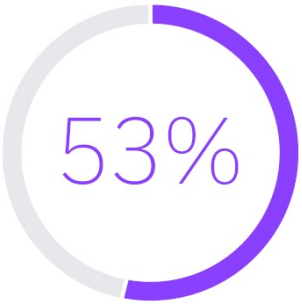


過去 2 年間に**サイバー攻撃によって大きな混乱**が生じた組織の割合

サイバー攻撃の量と重大度が増加

回答した組織の過半数（53%）は、過去 2 年間に、顧客またはビジネスの機密情報を含む 1,000 件を超えるレコードの損失や盗難を伴うデータ漏えいを経験しました。ほぼ同数の組織（51%）は、過去 2 年間にサイバーセキュリティー・インシデントが自社の IT プロセスとビジネス・プロセスに大きな混乱をもたらしたことを報告しました。

67% が過去 1 年間にサイバー攻撃の量が大幅に増加し、64% が重大度が大幅に増加したと報告しました。重大度の測定基準の上位項目では、価値の高い情報資産の漏えい（57%）がトップ、次いで従業員の生産性低下（50%）となっています。



サイバー・レジリエンスが改善した組織の割合

サイバー・レジリエンスは全体的に改善し、攻撃防御能力は過去 5 年間に最も向上

組織のサイバー・レジリエンスは段階的に強化され、過去 5 年間に 51% の改善が報告されています。この改善は、組織のサイバー攻撃防御能力が 2015 年の 38% から 2020 年の 53% へと大幅に向上したことと一致します。

実際、過半数（56%）の組織は、未然に防いだサイバー攻撃件数をサイバー・レジリエンス改善の測定基準のトップにランク付けしています。サイバー・レジリエンス改善で使用されたその他の主な測定基準としては、インシデントの封じ込めに要した時間と従業員の生産性向上があります。

攻撃検知能力は 2015 年からわずかに伸び（11%）、組織によるサイバー・レジリエンスのベンチマーク基準として 2 番目に一般的（51%）になっています。対応の能力は横ばいの状態ですが、封じ込めは困難の度合いを増しているように思われます。回答者は、この分野での 13% の低下を報告しています。

組織の 77% がサイバーセキュリティー・インシデント対策（CSIRP）を採用しているにもかかわらず、CSIRP を企業全体に適用している組織は 26% に過ぎないことを考えれば、このような低下は驚くには当たりません。さらに 77 % の組織のうち、4 分の 1 は対策が非公式または一時的なものであると伝えていました。

50%未満

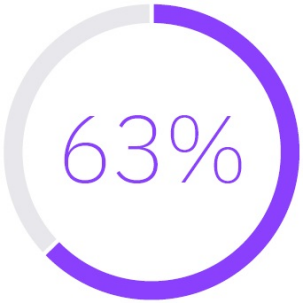
サイバー・レジリエンスについて経営幹部や役員に報告している組織

予算とスキルの不足が引き続きサイバー・レジリエンスの強化を妨げる障壁

改善しなかった主な理由として組織が挙げたのは、予想どおり、熟練した担当者の減少（41%）と予算不足（40%）でした。セキュリティー体制を強化する鍵としてテクノロジーを挙げている回答者が多い反面、最新ツールの確保や保有ツールの最大活用に苦戦している組織もあります。

組織が抱える課題には、サイロ化や縄張り意識の問題（31%）、自動化などの先進テクノロジーの不足（25%）、IT/セキュリティー・インフラストラクチャーのフラグメント化（22%）などがあります。

驚いたことに、サイバー・レジリエンスの状態に関する正式な報告書を経営幹部や役員に提出していると述べた回答者は 45% に過ぎませんでした。しかし、サイバーセキュリティー機能に関する経営レベルの賛同とサポート、役員レベルでの報告は、サイバー・レジリエンスが改善しなかった理由の中で重要性が最も低いと位置づけられていました。



自動化、機械学習、AI、オーケストレーションがサイバー・レジリエンスを高めていると述べた組織の割合

アナリティクス、自動化、AI、機械学習がセキュリティー体制を強化

アナリティクス（46%）、自動化（42%）、AI と機械学習（41%）などのテクノロジーを実装することでサイバー・レジリエンスが改善したと回答者は述べました。

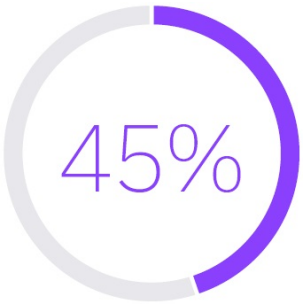
全体として、63% の組織はこれらツールがサイバー・レジリエンスの強固なセキュリティー体制をもたらすとし、次いで、60% が強固なプライバシー体制をもたらすとしています。このレポートで後述するように、サイバー・レジリエンスのハイ・パフォーマー組織であるかどうかはテクノロジーで決まることもあります。

脅威インテリジェンスの共有でサイバー・レジリエンスが改善したと述べた組織の割合

コラボレーションの促進は、脅威インテリジェンスの共有がもたらす最大の利点

回答者の 59% は、脅威インテリジェンスの共有によりサイバー・レジリエンスが改善するという考えを抱いていました。コラボレーションを促進するために、組織の 57% は、サイバー脅威と脆弱性に関する情報を政府機関や同業他社と共有するイニシアチブやプログラムに参加しています。

サイバー脅威に関する情報を共有しない理由を問われた回答者の多くは、自社にとってのメリットが感じられない（70%）、リソースの不足（58%）、コスト（54%）を理由に挙げました。



ランサムウェア攻撃に備えた対策がない組織の割合

DDoS は攻撃別対策での最も一般的タイプ

今回の調査では、特定の攻撃タイプに対処する対策の採用について初めて尋ねました。最も広く採用されていた対策は、分散サービス妨害（DDoS）、マルウェア（スパイウェア、ウイルス、トロイの木馬、ワームなど）、インサイダー・インシデント、フィッシングに対するものでした。

当然ですが、攻撃対策の採用状況は業種によって異なりました。マルウェアの対策は公共部門、小売、製造、消費財などの業種で最も採用されていたのに対し、インサイダー・インシデントの対策は工業において最も広く採用されていました。その他の業界では、DDoS が最も広く採用されていました。

攻撃別の対応マニュアルを採用している場合でも、ランサムウェア攻撃に備えた対策を実施している組織は半数未満（45%）でした。*IBM X-Force 脅威インテリジェンス・インデックス 2020 年度版*によると、ランサムウェアはここ数年で 70% 近く急増している攻撃手段です。 組織の大半が CSIRP を頻繁に更新していなかったため、この重要なリスク領域への対策が欠如していたことから、より頻繁に対策の見直しと更新を行って最新の攻撃方法を取り込むことがいかに重要かを再認識しなくてはなりません。

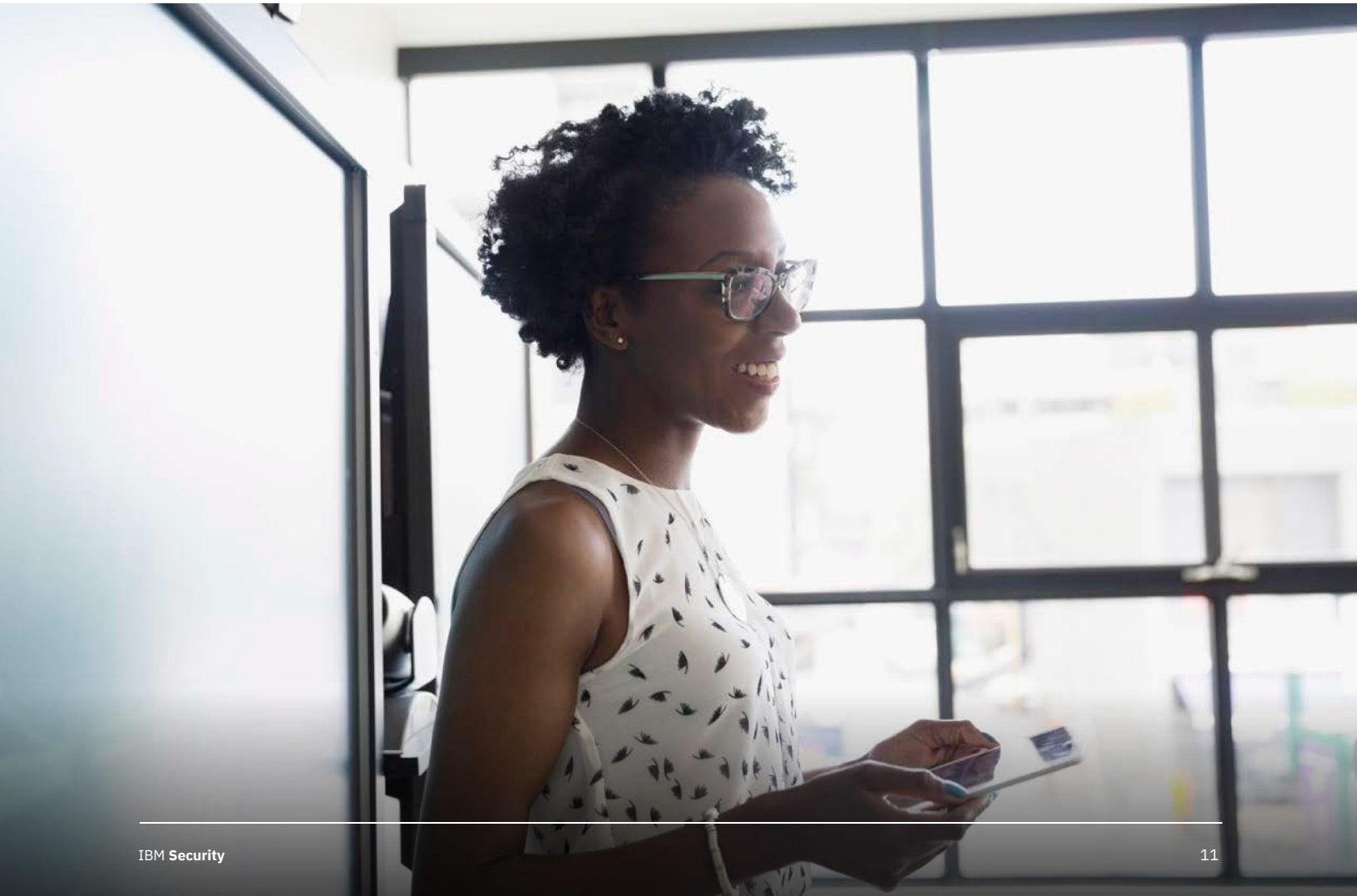
サイバー・レジリエンスの実現には**強固なプライバシー体制が重要**と述べた回答者の割合

プライバシーはサイバー・レジリエンスの実現に不可欠

過去 2 年間に 53% の組織が機密情報を含む 1,000 件以上のレコードに関わるデータ漏えいによる混乱を経験しているので、回答者の 95% がプライバシーの役割の重要性を認識していても驚くには当たりません。この役割を担うのは、顧客や従業員のデータを保護する組織内の担当者です。

しかし、3 分の 1 を超える組織がプライバシーの役割はきわめて重要であると考える一方、サイバー・レジリエンス実現の取り組みを指揮する最高プライバシー責任者を擁する組織は 1% に過ぎません。事業部の責任者または最高情報責任者（CIO）が最終的な責任を負うと述べた組織はそれぞれ 22% でした。

2019 年と同様に、回答者の 60% はサイバー・レジリエンスの実現には「強固なプライバシー体制」が重要と述べました。57% の組織は、EU の一般データ保護規制（GDPR）やカリフォルニア州消費者プライバシー法（CCPA）など、サイバー・レジリエンスの実現に欠かせないデータ保護規制への準拠を挙げました。

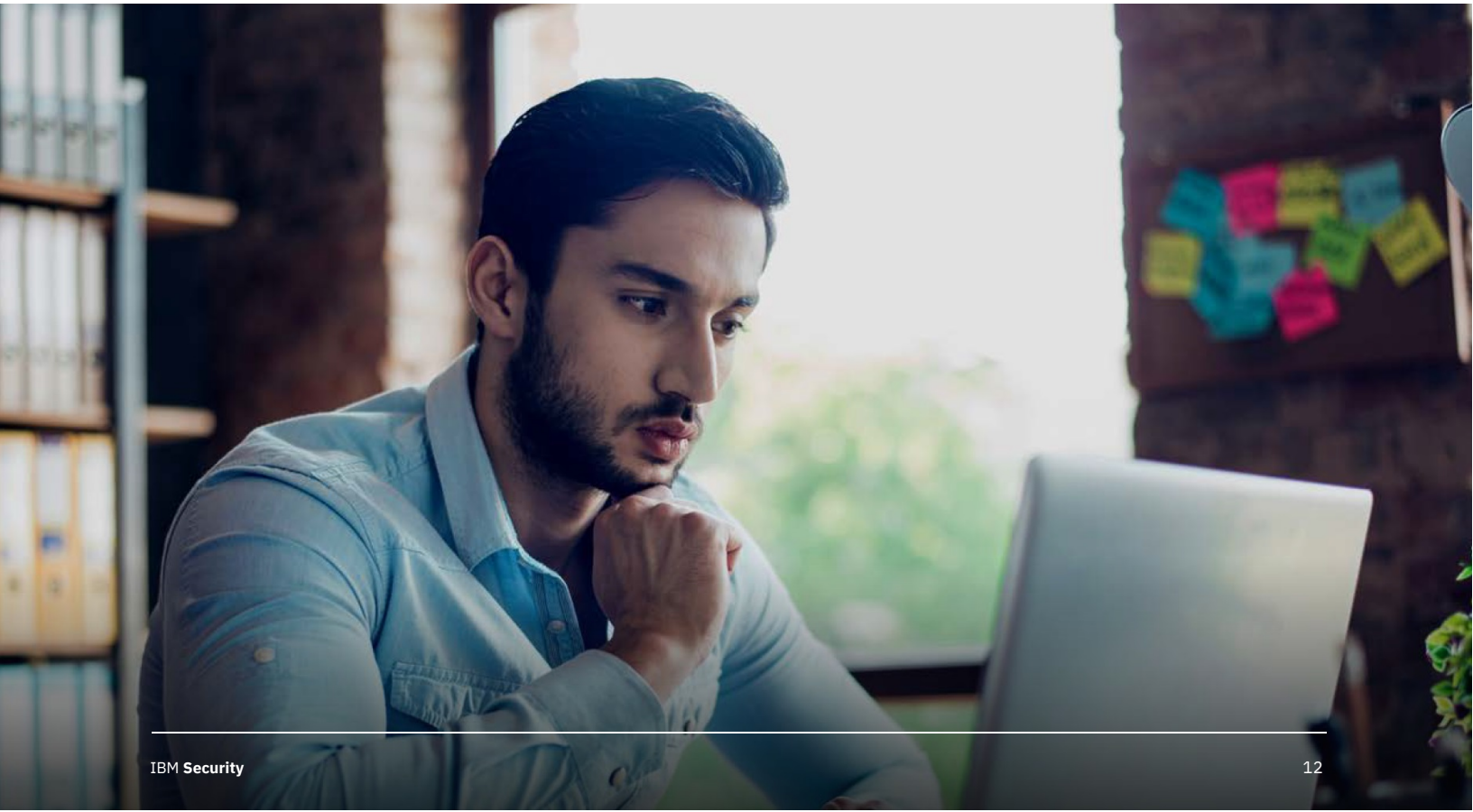


パフォーマンスの高い組織は何が違うのか

自社のサイバー・レジリエンスを 10 点満点で評価するように求めたところ、4 分の 1 近い回答者は 9 を超える評価を付けました。このグループの 59% は、過去 1 年間で自社は大きく改善したと述べました。ここでは、これらの組織をハイ・パフォーマーと呼びます。

昨年と同様に、サイバー攻撃の検知、防御、封じ込め、対応の能力でハイ・パフォーマーは他の組織に勝っています。しかも、今年はその格差がさらに広がっています。差異が一番大きかったのは攻撃の封じ込めと対応でした。

昨年、ハイ・パフォーマーは攻撃の封じ込めで他の組織を 14% 上回っていましたが、この差異が 35% に拡大しました。同様に昨年、サイバー攻撃への対応におけるハイ・パフォーマーと他の組織との差異は 15% でした。2020 年にはこの差が 31% に広がっています。



他の組織が学ぶべきベスト・プラクティスをハイ・パフォーマーが活用していることは明らかです。ハイ・パフォーマーの特徴とアプローチを以下にいくつか示します。

CSIRP の企業全体への実装:

パフォーマンスの高い組織の 43% が CSIRP を企業全体に一貫して適用しているのに対し、他の組織では 20% です。年に 2 回または四半期ごとにこの対策の見直しとテストを実施しているハイ・パフォーマーの割合は 2 倍を超えています。

攻撃別対策の採用:

ハイ・パフォーマーの 50% が攻撃別対策を採用しているのに対し、他の組織では 37% です。

テクノロジーへの投資:

自動化、機械学習、AI、オーケストレーションが強固なサイバー・レジリエンスのセキュリティー体制を実現する鍵と見なしていたハイ・パフォーマーが 73% であるのに対し、他の組織では 60% でした。

自動化の頻繁な使用:

70% が自動化の頻繁な使用または中程度の使用を報告しました。このグループのうち

- 70% は自動化を使用して運用効率を改善
- 64% は自動化を使用して IT セキュリティー・チームを支援

脅威インテリジェンスの共有:

サイバー脅威の検知、封じ込め、対応の能力を改善する脅威インテリジェンスを共有していたハイ・パフォーマーが 69% であるのに対し、他の組織では 50% でした。

経営幹部の可視性:

ハイ・パフォーマーの半数以上は、経営幹部や役員に正式な報告書を提出しています。

他の組織とハイ・パフォーマーの比較

39%

自動化ツールで改善を実現している傾向が高い

25%

クラウド・サービス導入により改善している傾向が高い

20%

AI と機械学習を使用して改善を経験している傾向が高い

31%

相互運用可能なサイバーセキュリティー・ツールで改善を実現している傾向が高い

サイバー・レジリエンス改善に向けたステップ*

CSIRP を企業全体に適用してビジネスの中断を最小化

CSIRP は単に採用するだけでは不十分で、企業全体に適用して定期的に見直す必要があります。攻撃の量と重大度が年々増していくなか、CSIRP の更新を怠ると、IT プロセスとビジネス・プロセスに大きな混乱をもたらすリスクが高まります。

各業界の特定の攻撃に合わせて対策を調整

サイバーセキュリティー攻撃はさまざまな形態をとります。それぞれの業界で最優先すべき脅威を認識し、詳細な対策を作成して、特定の攻撃の調査、修復に必要な措置をチーム・メンバーが把握できるようにすれば、組織はセキュリティー体制を強化できます。

相互運用性を取り入れ、可視性を高めて複雑性を軽減

組織が複雑なセキュリティー環境に対処するとき、相互運用性を活用してツールとデータの可視性を強化し、攻撃の検知と防御を促進すれば、チームは最大の効果を上げることができます。ワークフローを合理化するアプローチは、セキュリティー運用センターの生産性向上に役立ちます。

テクノロジーに投資してインシデント対応を加速

組織がサイバー・レジリエンスを改善した主要な理由として、自動化、アナリティクス、AI、機械学習などのテクノロジーとクラウド・サービスの導入が挙げられました。特に自動化は、調査と対応に必要な価値の高い作業に取り組む時間を生み出すため、企業が運用効率を高めてチームの離反を減らすのに役立ちます。

*セキュリティー・プラクティスの推奨事項は情報の提供を目的とするものであり、結果を保証するものではありません。

セキュリティー・チームとプライバシー・チームの連携

強固なサイバー・レジリエンスを備えた組織は、セキュリティーとプライバシーが不可分であることを認識しています。データ漏えいに対してより効果的に対応できるように、サイロを解消してコラボレーションの文化を促進します。この 2 つのチームを早期に連携させれば、多くの場合、大規模なセキュリティー・インシデントの発生中に初めて連携させるよりも早くセキュリティー体制が改善されます。

経営幹部や役員に正式な報告書を提出し、組織のサイバー・レジリエンスの可視性を強化

ビジネス・リーダーはサイバー・レジリエンスが収益や組織の評判に影響することを認識しているため、必須レベルの投資とリソースを確保するには、サイバー・レジリエンスのパフォーマンスを中心に据えることが不可欠です。

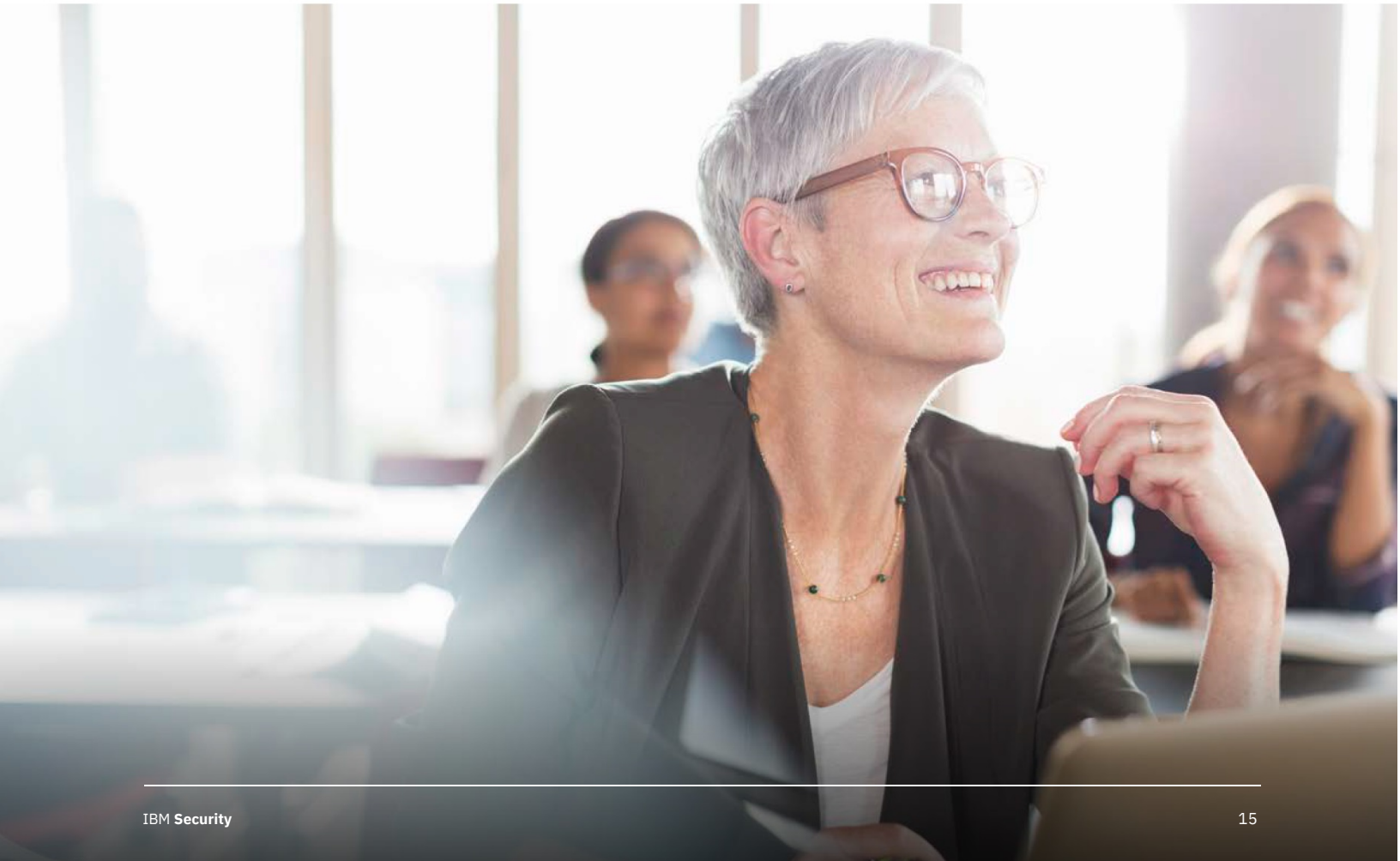


図 1

サイバーセキュリティー・インシデントを経験した組織の割合

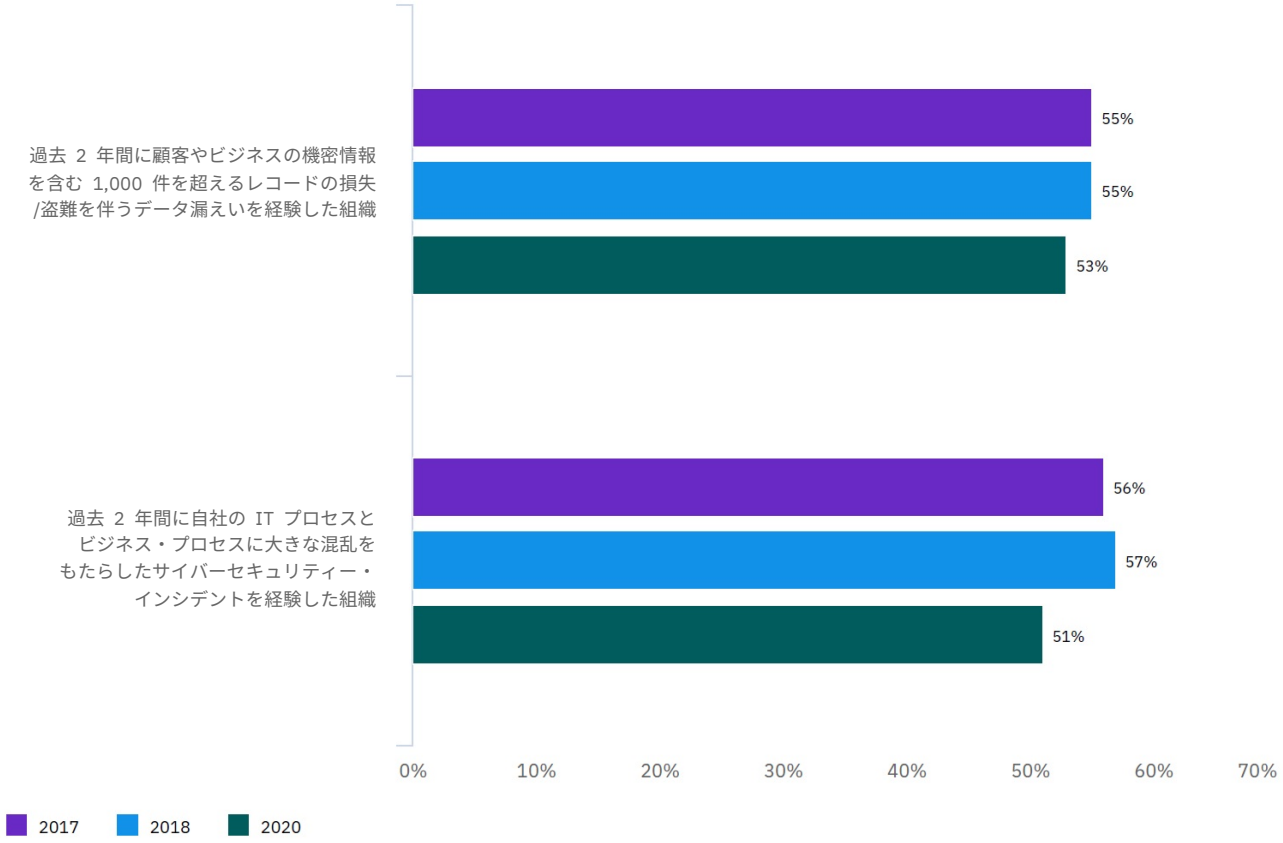


図 1 は、過去 2 年間にデータ漏えいやサイバーセキュリティー・インシデントを経験した組織の割合を示しています。

図 2

改善の測定基準の上位項目

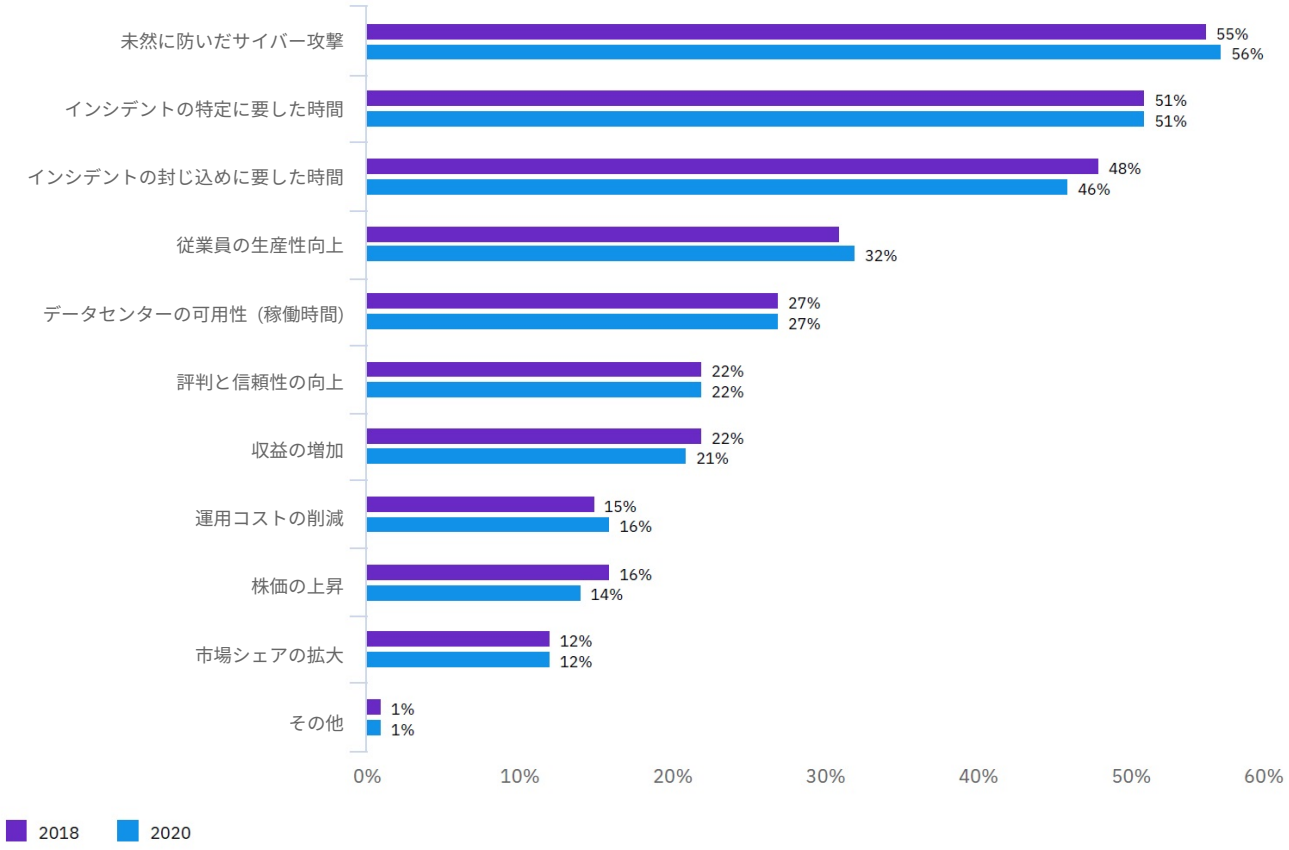


図 2 は、組織におけるサイバー・レジリエンス改善の測定基準の上位項目についての洞察を示します。上位 3 項目は、未然に防いだサイバー攻撃の件数、インシデントの特定に要した時間、インシデントの封じ込めに要した時間でした。

図 3

サイバー・レジリエンスが改善した理由

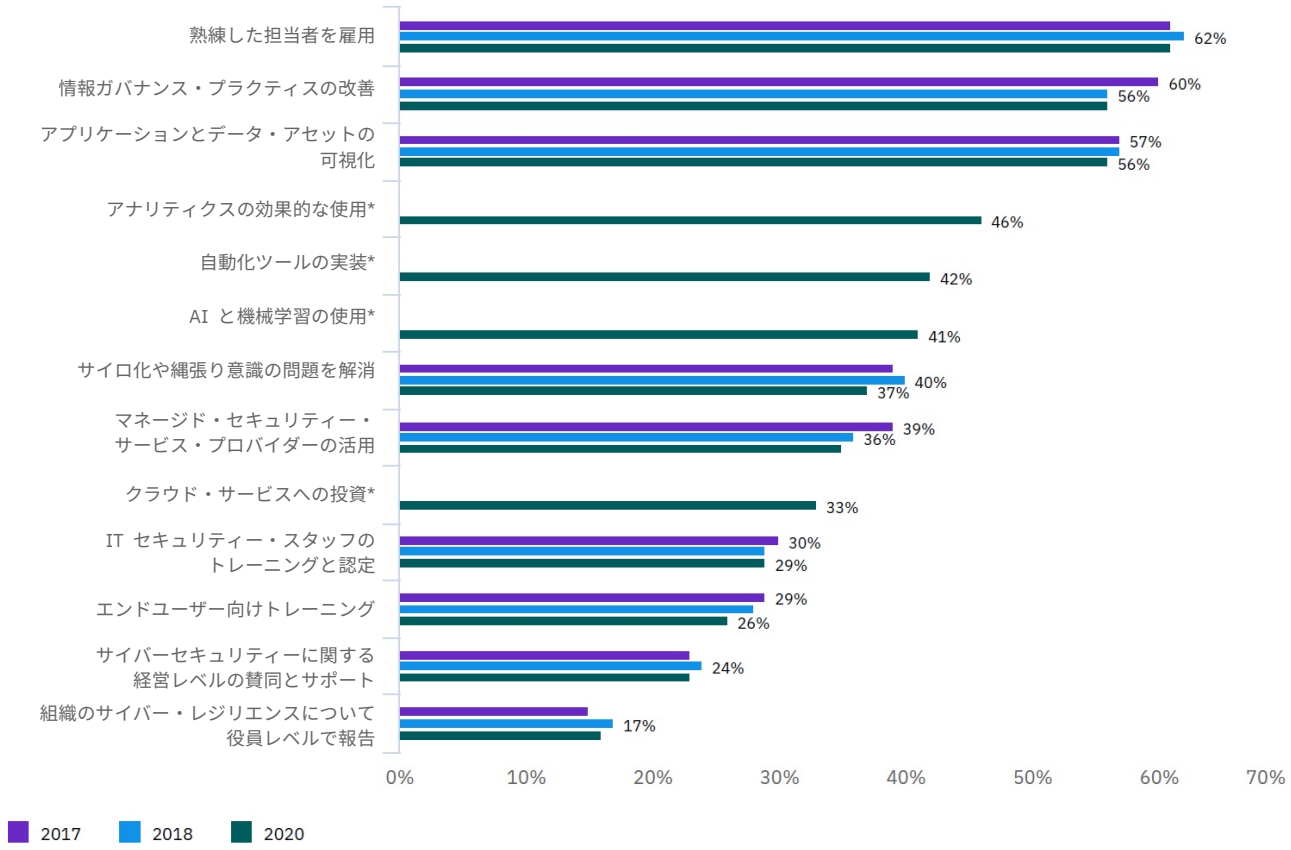


図 3 は、組織がサイバー・レジリエンスを改善できた理由を示しています。上位 3 項目は前年比で大きな変化はありませんが、今年はアナリティクス、自動化、AI と機械学習が重要な役割を果たしました。

図 4

サイバー・レジリエンスが改善しなかった理由

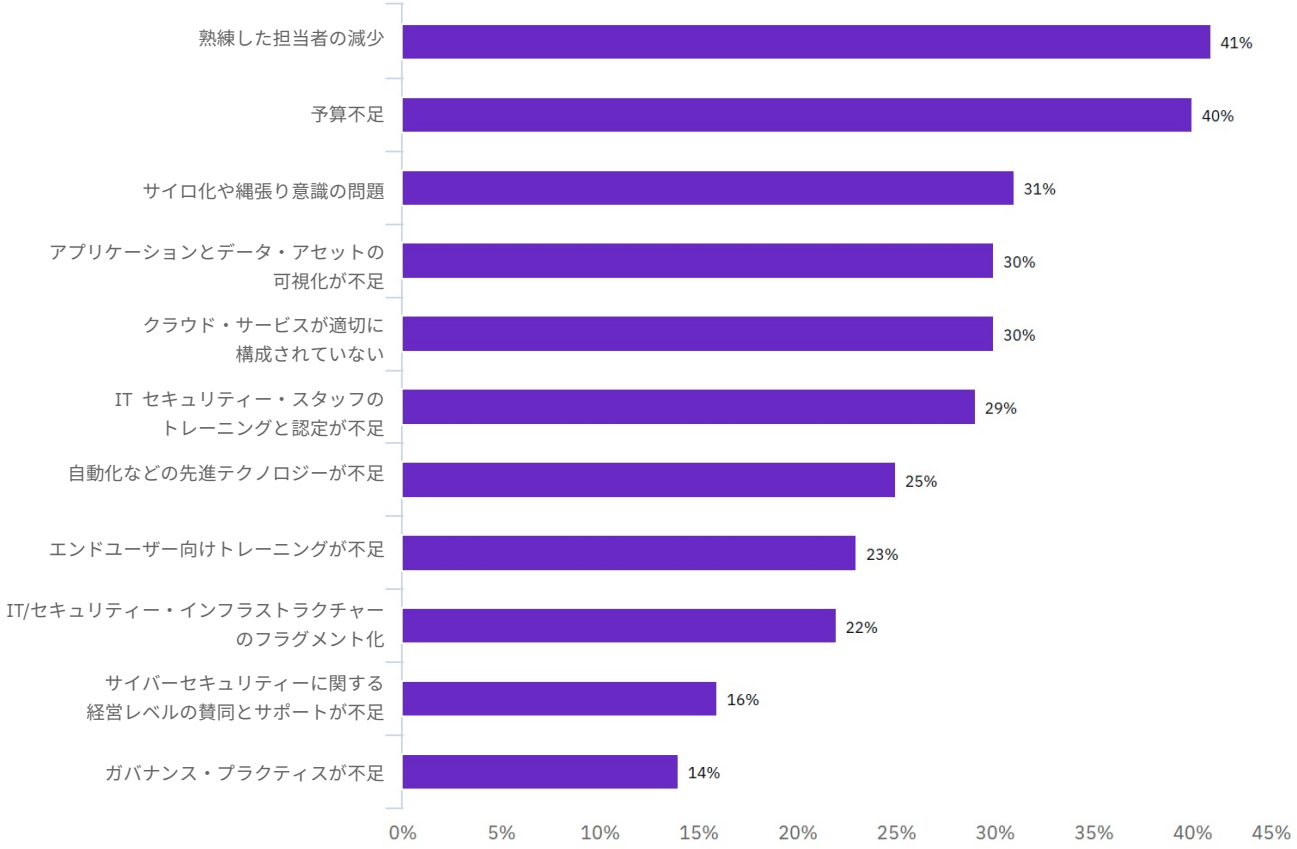


図 4 は、組織が考えるサイバー・レジリエンスが改善しなかった理由を示しています。課題の原因には担当者や人員、プロセス、テクノロジーが混在していました。

図 5

クラウド・サービス使用によるサイバー・レジリエンスの改善

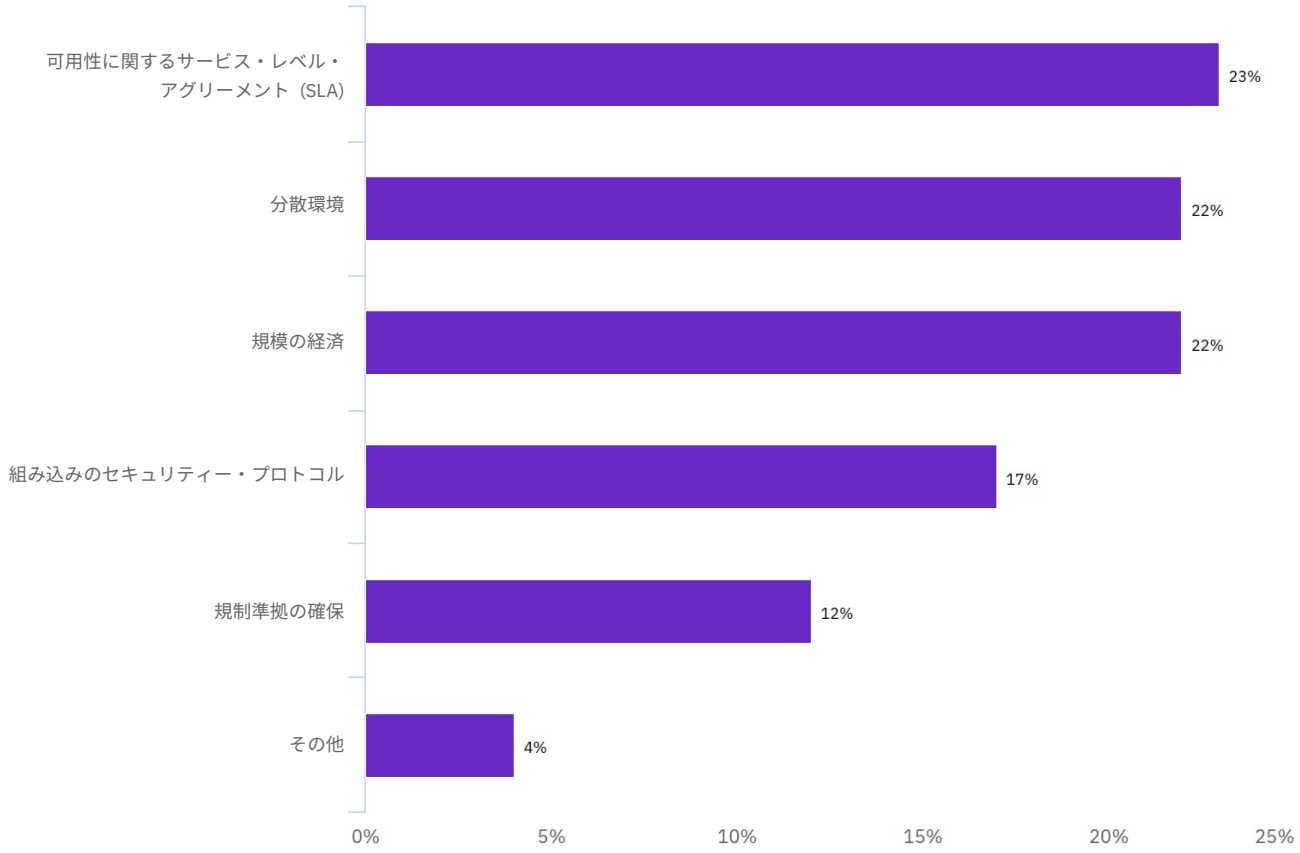


図 5 は、クラウド・サービス使用がどのような形で組織のサイバー・レジリエンス改善に貢献したかを分類したものです。理由の上位 3 項目は、可用性に関するサービス・レベル・アグリーメント、分散環境、規模の経済でした。

図 6

特定の脅威タイプに対する対策

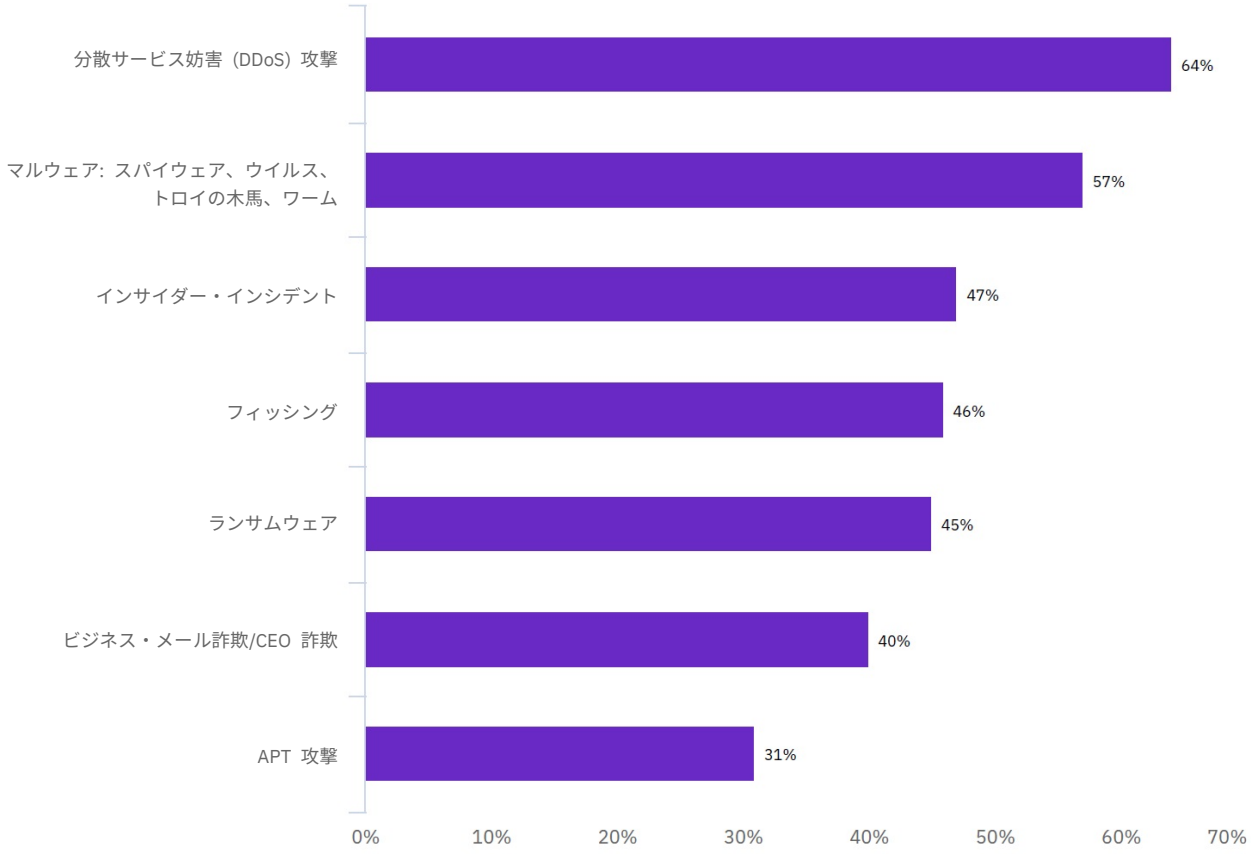


図 6 は、対策の対象となった、特定の脅威タイプの詳細を示しています。DDoS 攻撃、マルウェア、インサイダー・インシデントが上位 3 項目です。

図 7

重大度の測定基準の上位項目

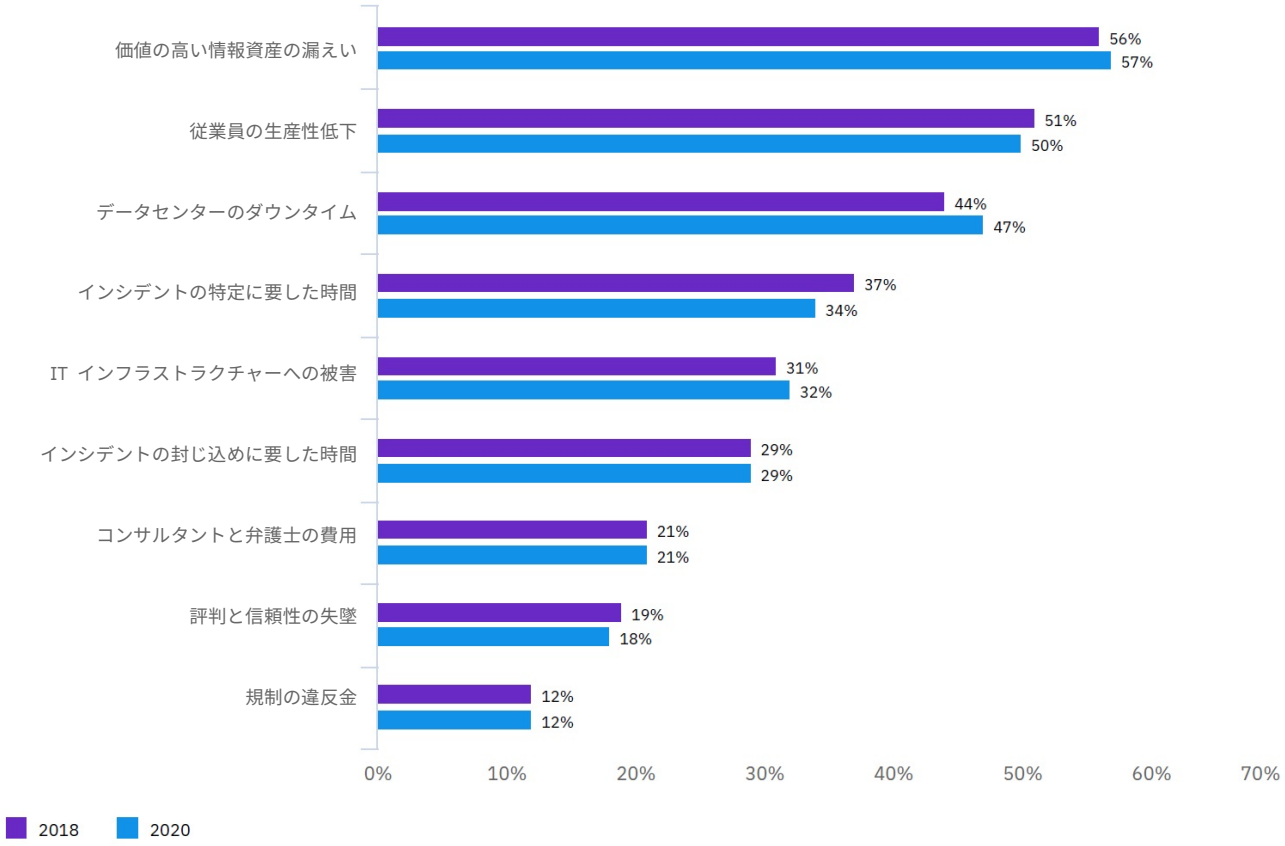


図 7 は組織における攻撃の重大度の測定基準の上位項目を示しており、価値の高い情報資産の漏えいが過去 2 年間にわたってトップとなっています。

図 8

脅威インテリジェンスによるサイバー・レジリエンスの改善

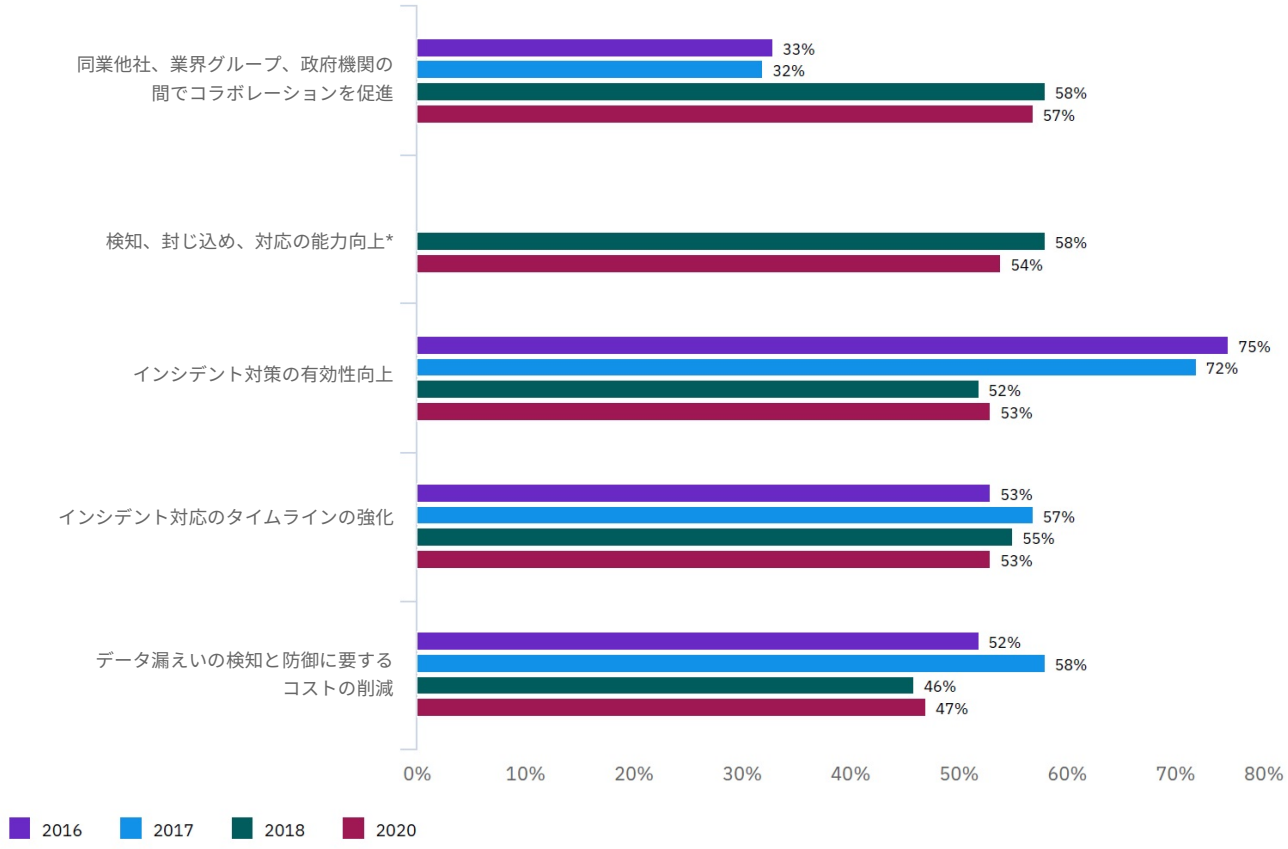


図 8 は、脅威インテリジェンスの共有によりもたらされると認識された価値を示します。インシデント対応策の有効性を改善すると考える回答者は、この 4 年間で 29% 減少しました。

図 9

ハイ・パフォーマーにおける改善の原因

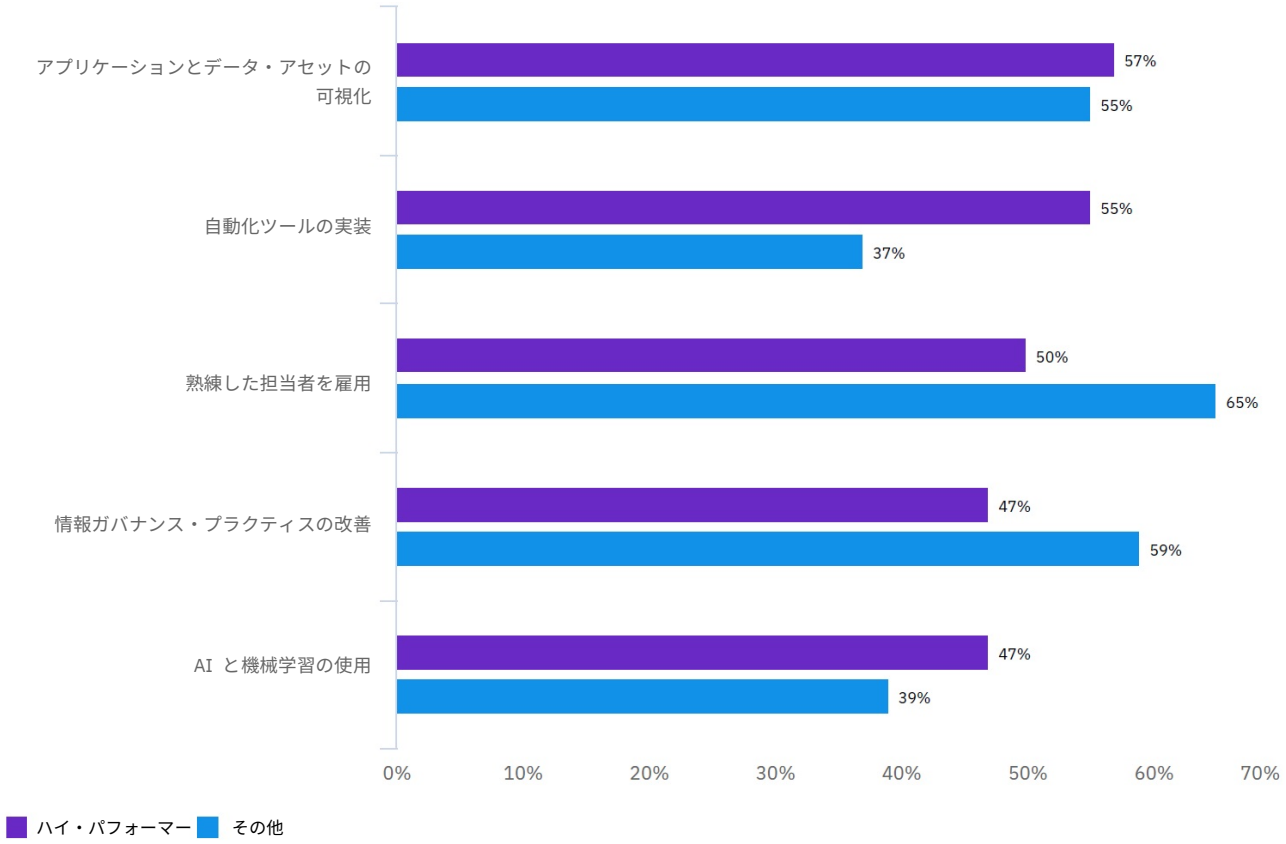


図 9 は、ハイ・パフォーマーのサイバー・レジリエンスが他の組織よりも改善された理由を示しています。

図 10

ハイ・パフォーマーがサイバー・レジリエンスに優れている理由

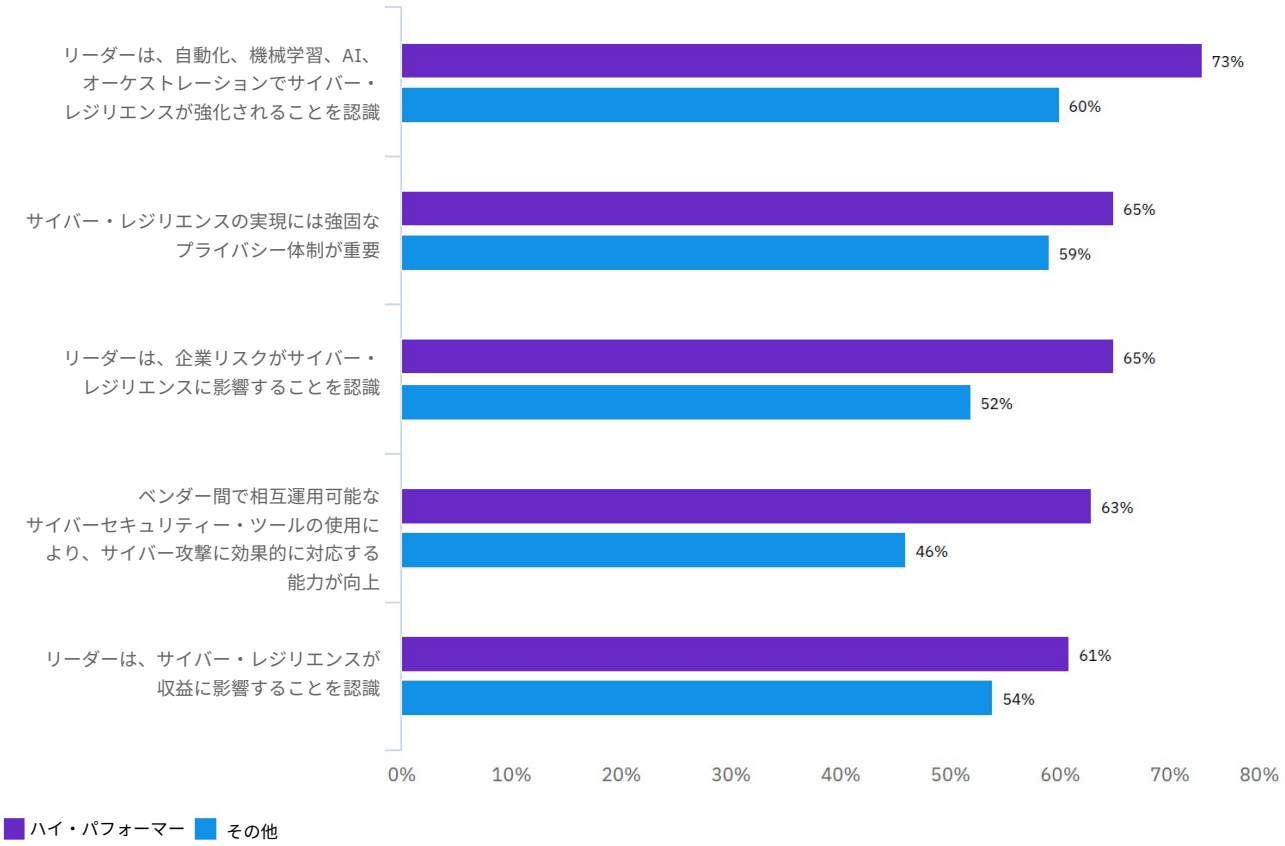


図 10 は、ハイ・パフォーマーがサイバー・レジリエンスに優れている理由を示しています。

図 11

ハイ・パフォーマーにおけるサイバー・レジリエンスについての自信レベル

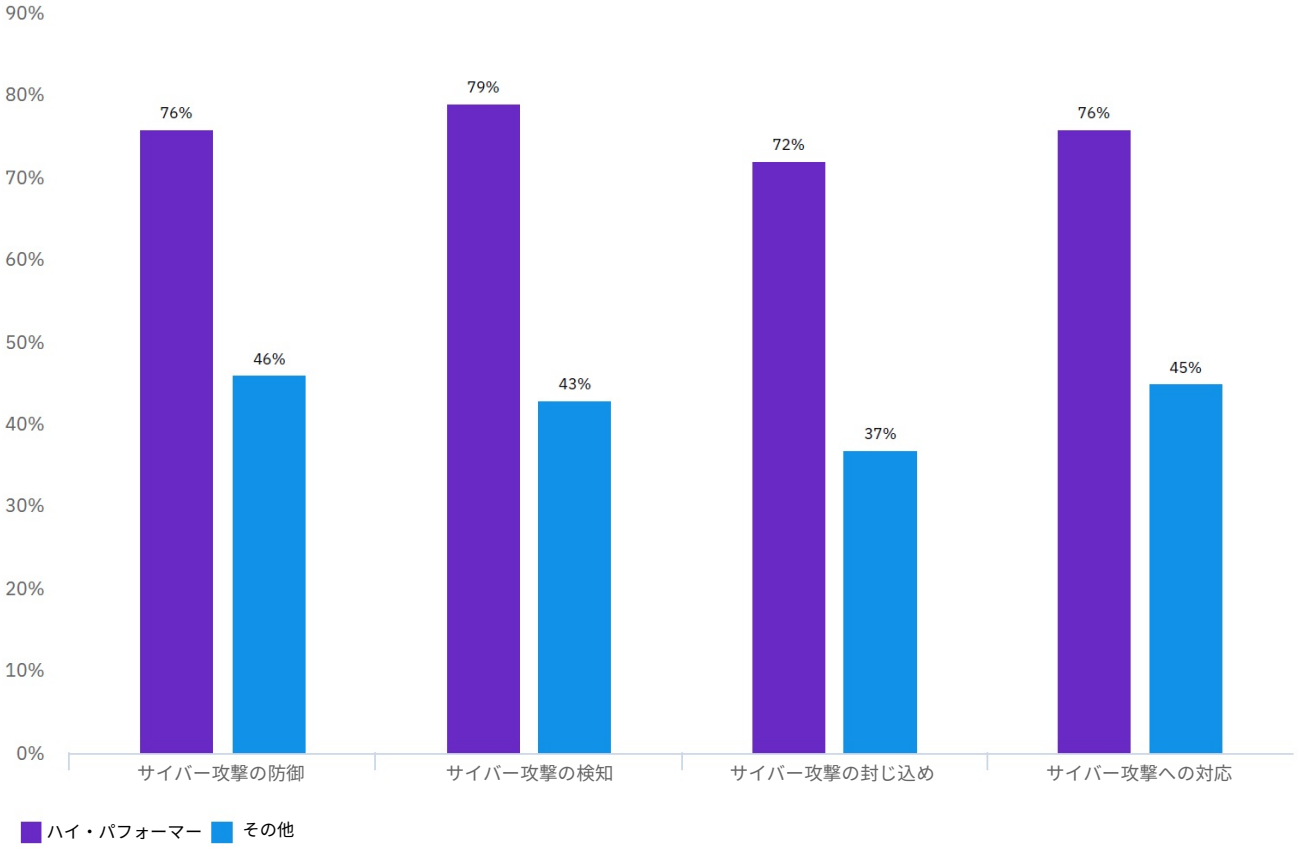


図 11 は、サイバー攻撃に関するハイ・パフォーマーの自信を示しています。ハイ・パフォーマーと他の組織とで自信の差が最も大きいのはサイバー攻撃の検知です。

図 12

セキュリティー・ソリューションの採用数がインシデント対応に与える影響

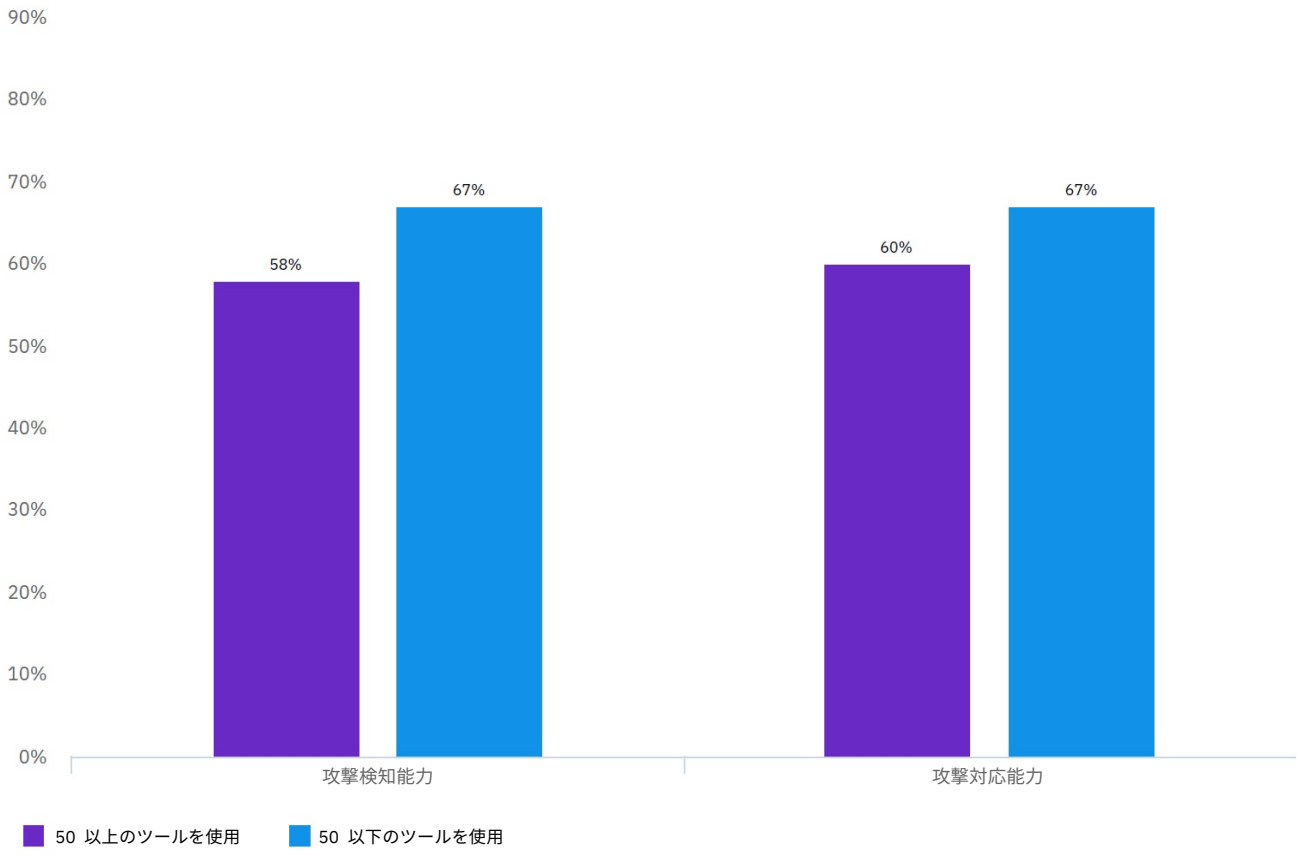


図 12 は、50 以上のセキュリティー・ソリューションの使用がインシデントへの対応に及ぼす影響を示しています。50 以下のツールを使用していた組織は、サイバー攻撃対処能力が向上したと報告しました。

図 13

攻撃別対策の採用状況（地域別）

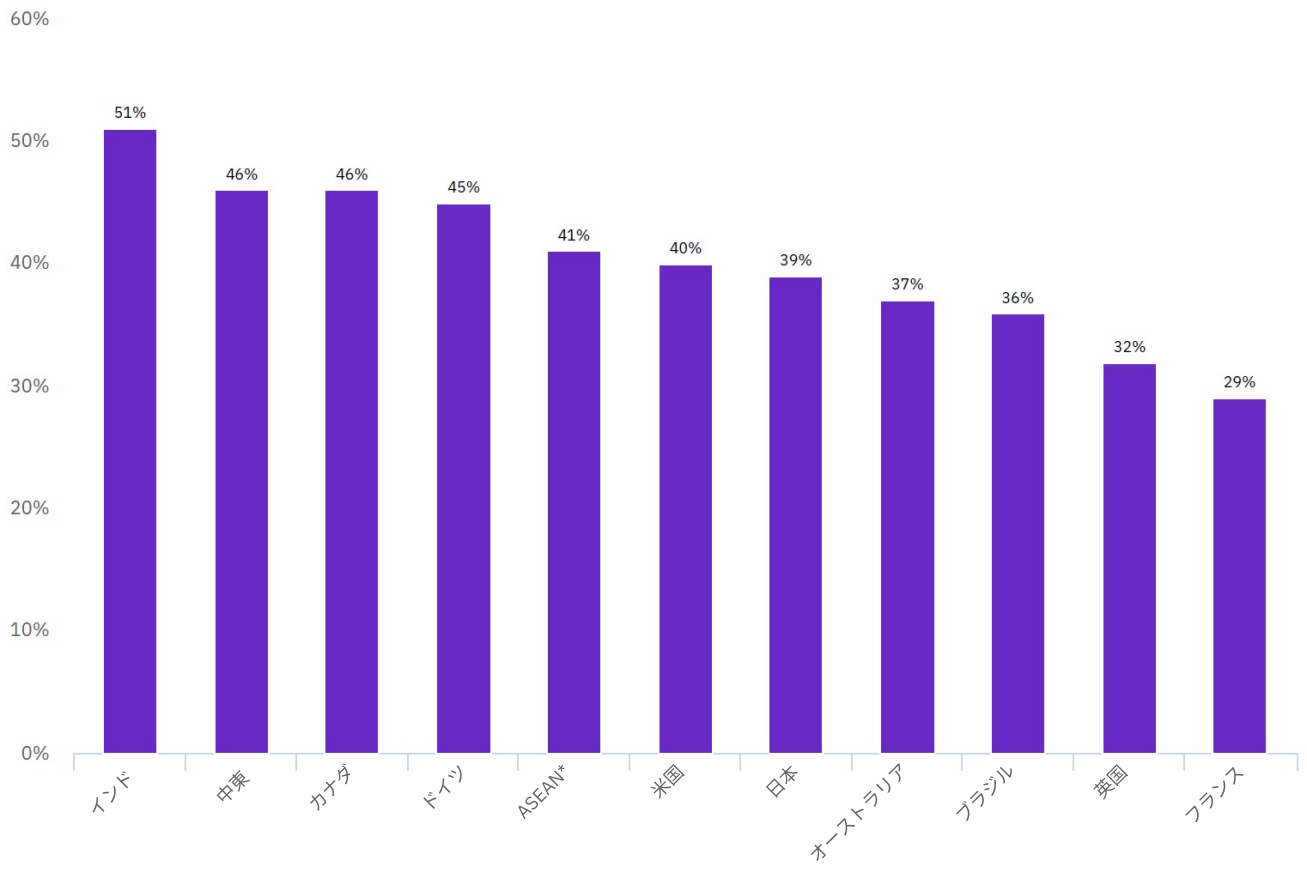


図 13 は、調査対象の各国間での相違を示しています。インドの組織は、サイバー攻撃別対策を採用する傾向が高くなっています。攻撃別対策を採用する傾向が最も低いのは英国とフランスでした。

*ASEAN は、シンガポール、フィリピン、ベトナム、タイ、マレーシア、インドネシアに住む回答者のサンプルです。

**中東は、アラブ首長国連邦とサウジアラビアに住む回答者のサンプルです。

図 14

高水準のサイバー・レジリエンス実現にあたってのクラウド・サービスの価値 (地域別)

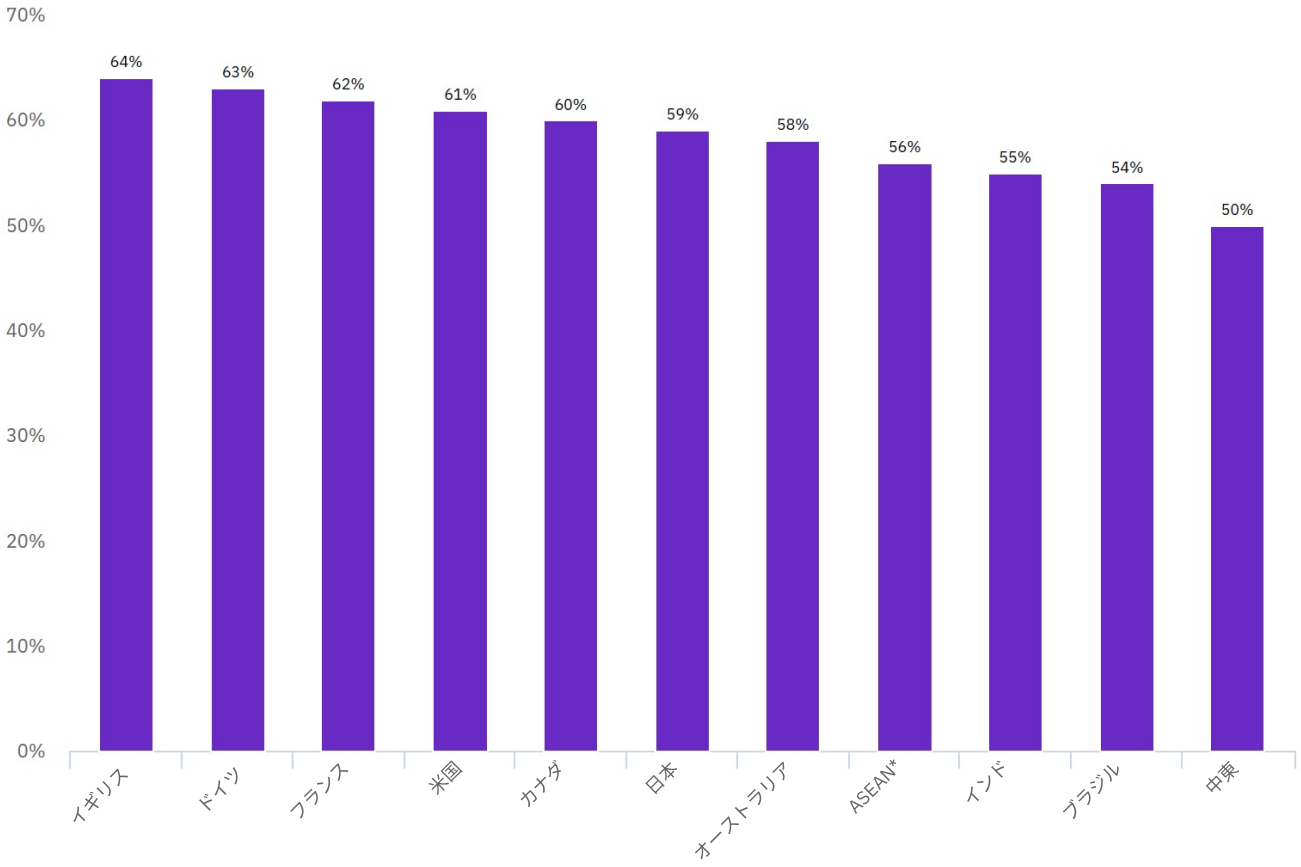


図 14 は、クラウド・サービスがサイバー・レジリエンスにどう影響を及ぼすかについての各国間の違いを示しています。英国、ドイツ、フランス、米国は近接して並んでいます。

*ASEAN は、シンガポール、フィリピン、ベトナム、タイ、マレーシア、インドネシアに住む回答者のサンプルです。

**中東は、アラブ首長国連邦とサウジアラビアに住む回答者のサンプルです。

図 15

クラウド・サービス使用によるサイバー・レジリエンスの改善度合い (業種別)*

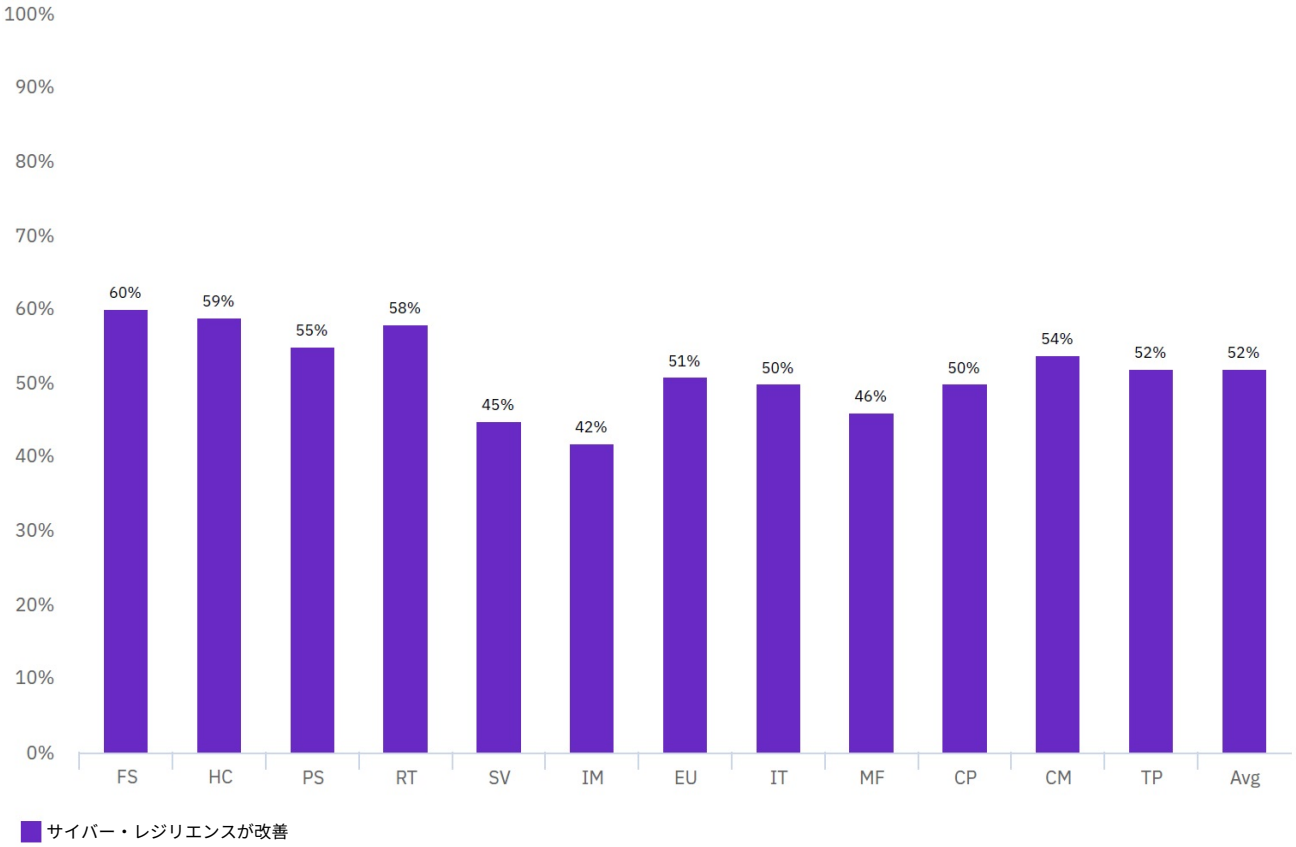


図 15 は、クラウド・サービス使用によってサイバー・レジリエンスがどの程度改善したかを業種別に示しています。

*業種の略語: 金融サービス (FS)、医療/製薬 (HC)、公共部門 (PS)、小売業 (RT)、サービス (SV)、工業 (IM)、エネルギー/公益事業 (EU)、IT/テクノロジー (IT)、製造 (MF)、消費財 (CP)、通信 (CM)、運輸 (TP)、エンターテイメント/メディア (EM)、教育/研究 (ED)、ホスピタリティー (HP)、防衛/航空宇宙 (DF)、農業/食品サービス (AG)、ロジスティクス/流通 (LD)。業種の定義は 34 ページをご確認ください。

図 16

CSIRP の採用状況 (業種別)*

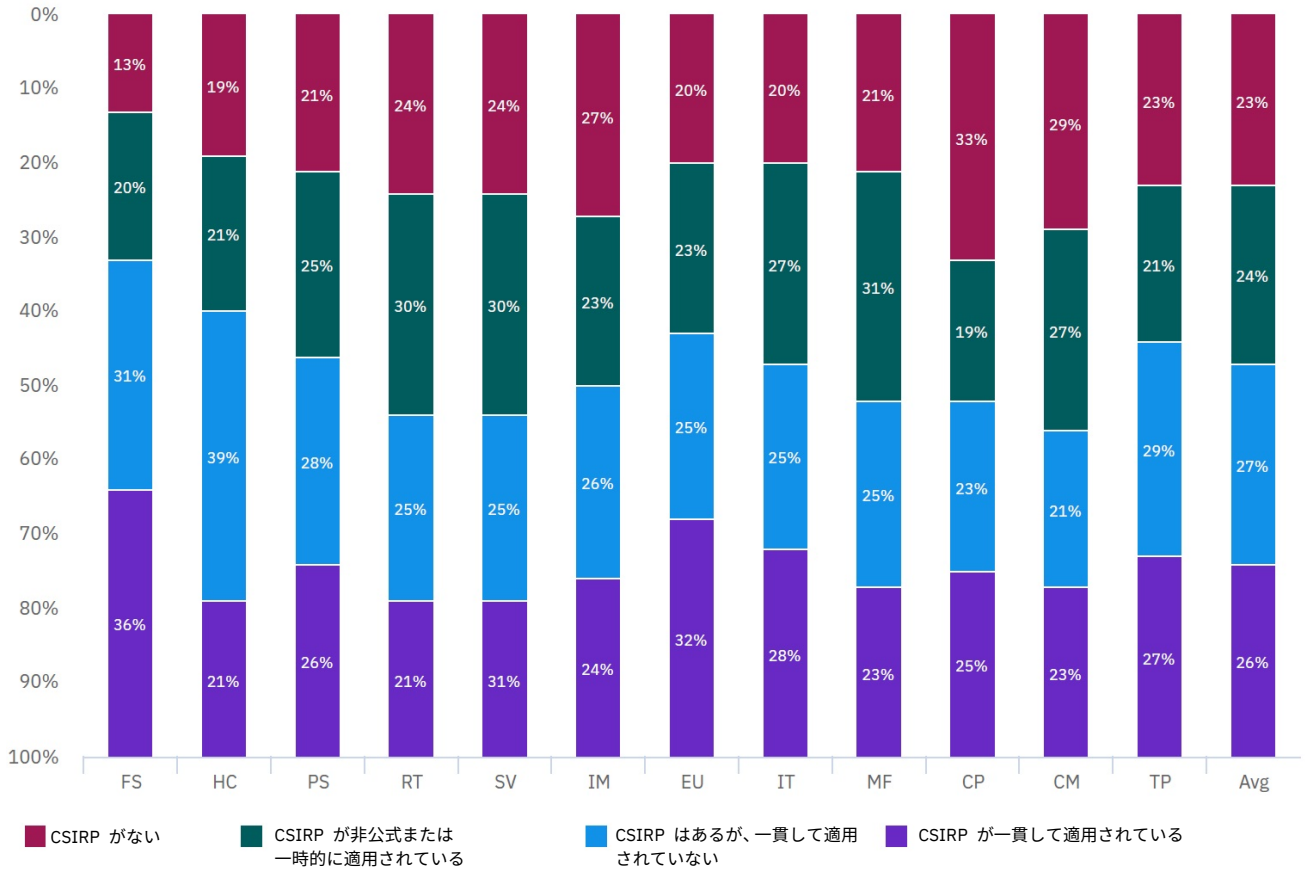


図 16 は、CSIRP の採用状況を業種別に示しています。

*業種の略語: 金融サービス (FS)、医療/製薬 (HC)、公共部門 (PS)、小売業 (RT)、サービス (SV)、工業 (IM)、エネルギー/公益事業 (EU)、IT/テクノロジー (IT)、製造 (MF)、消費財 (CP)、通信 (CM)、運輸 (TP)、エンターテイメント/メディア (EM)、教育/研究 (ED)、ホスピタリティー (HP)、防衛/航空宇宙 (DF)、農業/食品サービス (AG)、ロジスティクス/流通 (LD)。業種の定義は 34 ページをご確認ください。

図 17

サイバーセキュリティーへの投資を正当化する要素

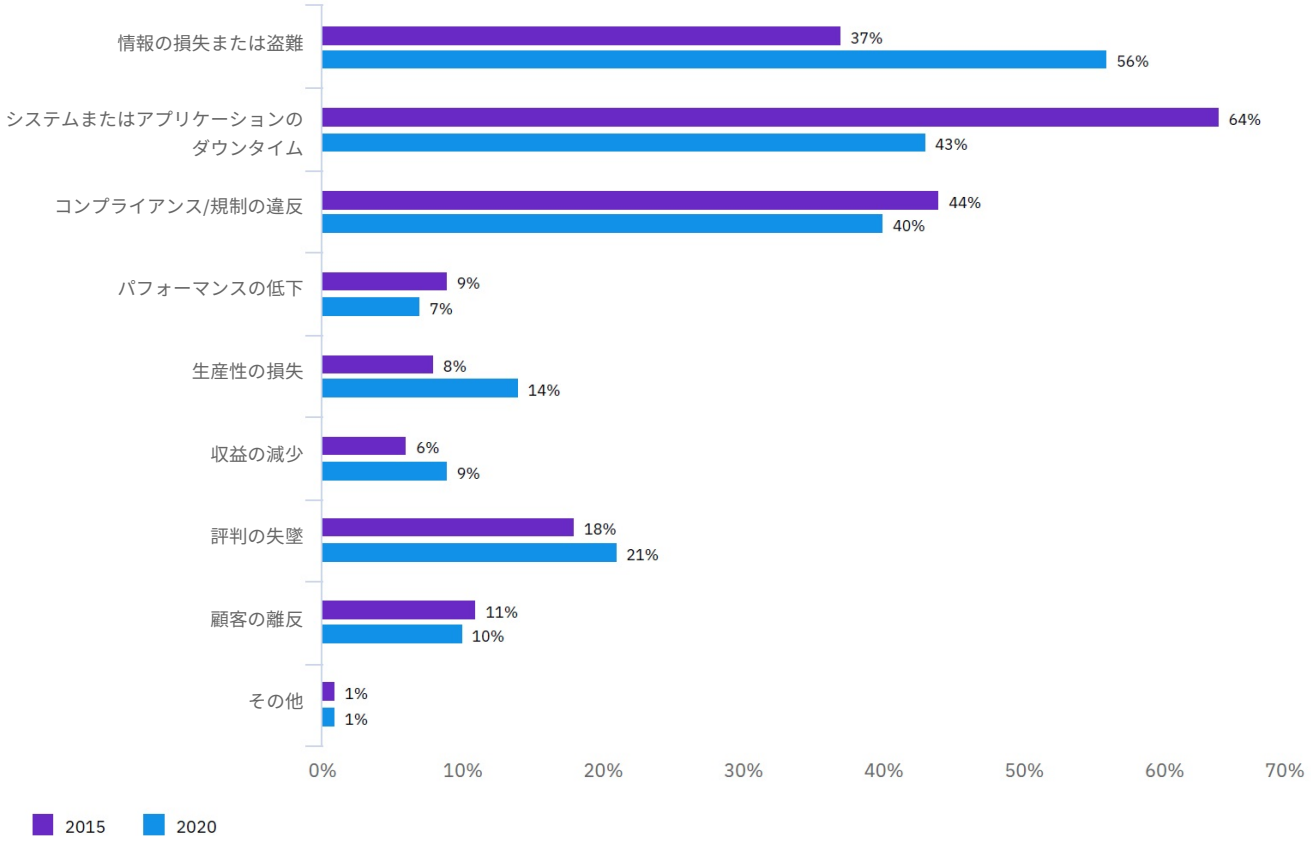


図 17 は、サイバーセキュリティーへの投資を正当化する要素を示しています。2015 年以降に、予算の理由付けは「システムまたはアプリケーションのダウンタイム」から「情報の損失または盗難」へと変わっています。

図 18

サイバー・レジリエンスに割り振られたサイバーセキュリティーの予算

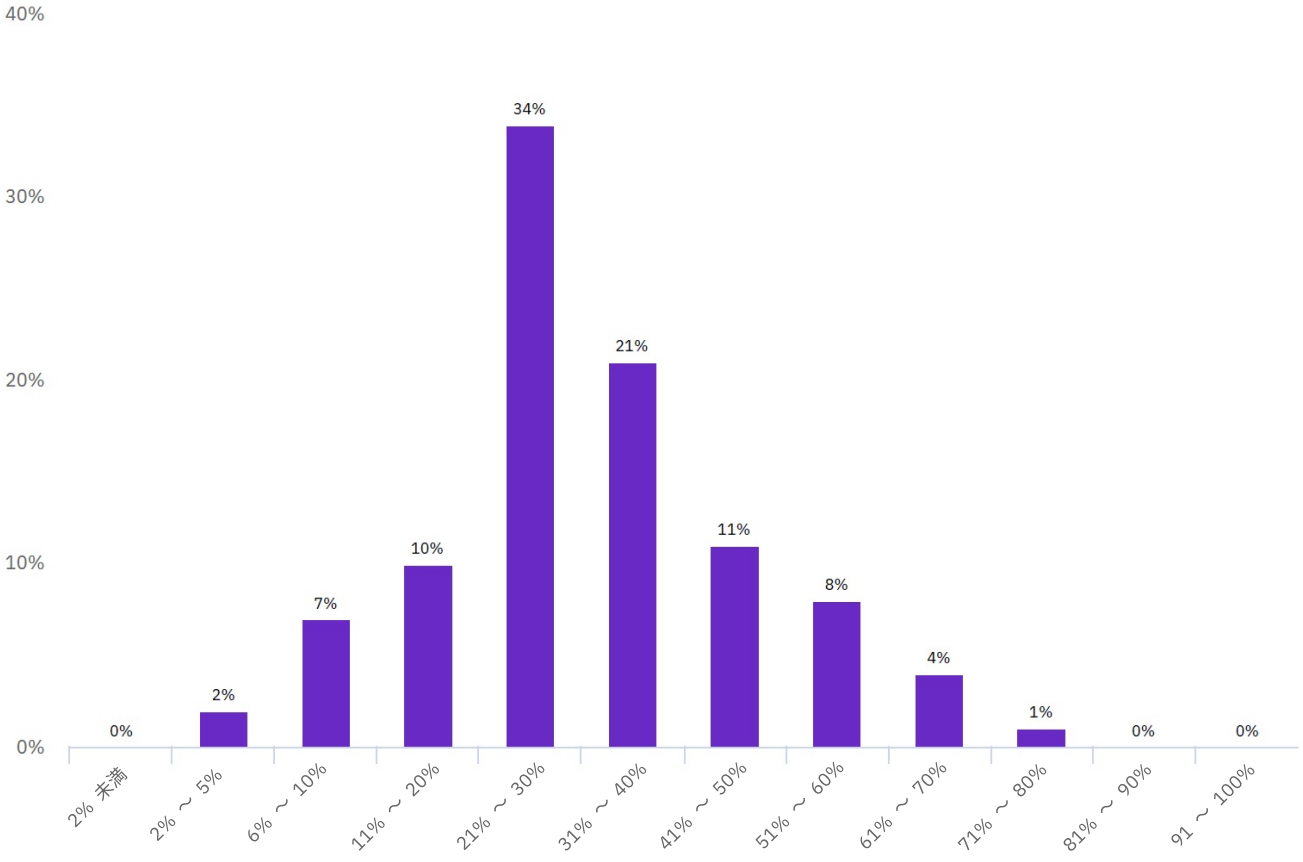


図 18 は、サイバー・レジリエンス関連の活動に割り振られた予算の割合を示しています。

調査組織の特性

サイバー・レジリエンス・レポート (2020 年版) は、米国、インド、ドイツ、英国、ブラジル、日本、オーストラリア、フランス、カナダ、ASEAN*、中東** における IT とセキュリティーの担当者 3,439 名から得た回答で構成されています。

参加している業種

サンプルは 18 の業種セグメントで構成されました。

金融サービス
銀行、保険会社、投資会社

医療/製薬
病院、診療所、生物医学/生命科学

小売業
実店舗と e-コマース

製造
商品または部品の大規模な製造業者

ホスピタリティー
ホテル、飲食店チェーン、船旅会社

公共部門
連邦政府機関、州政府機関、地方政府機関、NGO

運輸
航空会社、鉄道

エネルギー/公益事業
石油会社、ガス会社、公益事業、代替エネルギーの生産者と供給者

消費財
消費財のメーカーと流通業者

ロジスティクス/流通
トラック運送会社、配送会社、サプライ・チェーン・マネジメント

工業
化学プロセス会社、エンジニアリング会社、製造会社

通信
新聞社、書籍出版社、広告会社、広告代理店

IT/テクノロジー
ソフトウェア会社、ハードウェア会社

サービス
法律事務所、会計事務所、コンサルティング会社などの専門的サービス

エンターテイメント/メディア
映画制作、スポーツ、ゲーム、カジノ

農業/食品サービス
農業経営、食品メーカー (作物および家畜)

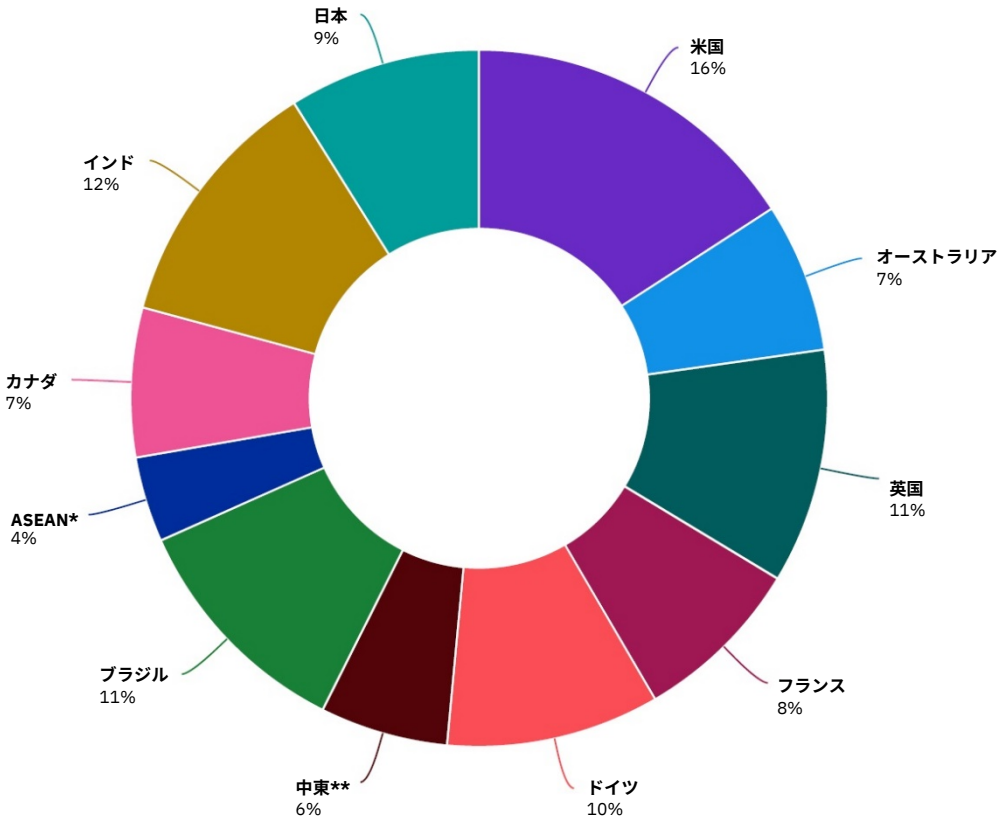
防衛/航空宇宙
民間航空機または防衛関連の航空機とシステムの製造業者や設計者

教育/研究
市場調査、シンクタンク、研究開発、公立大学、私立大学、単科大学、教育研修会社

*ASEAN は、シンガポール、フィリピン、ベトナム、タイ、マレーシア、インドネシアに住む回答者のサンプルです。
**中東は、アラブ首長国連邦とサウジアラビアに住む回答者のサンプルです。

図 19

国または地域別のサンプルの分布



*ASEAN は、シンガポール、フィリピン、ベトナム、タイ、マレーシア、インドネシアに住む回答者のサンプルです。

**中東は、アラブ首長国連邦とサウジアラビアに住む回答者のサンプルです。

図 20

業種別のサンプルの分布

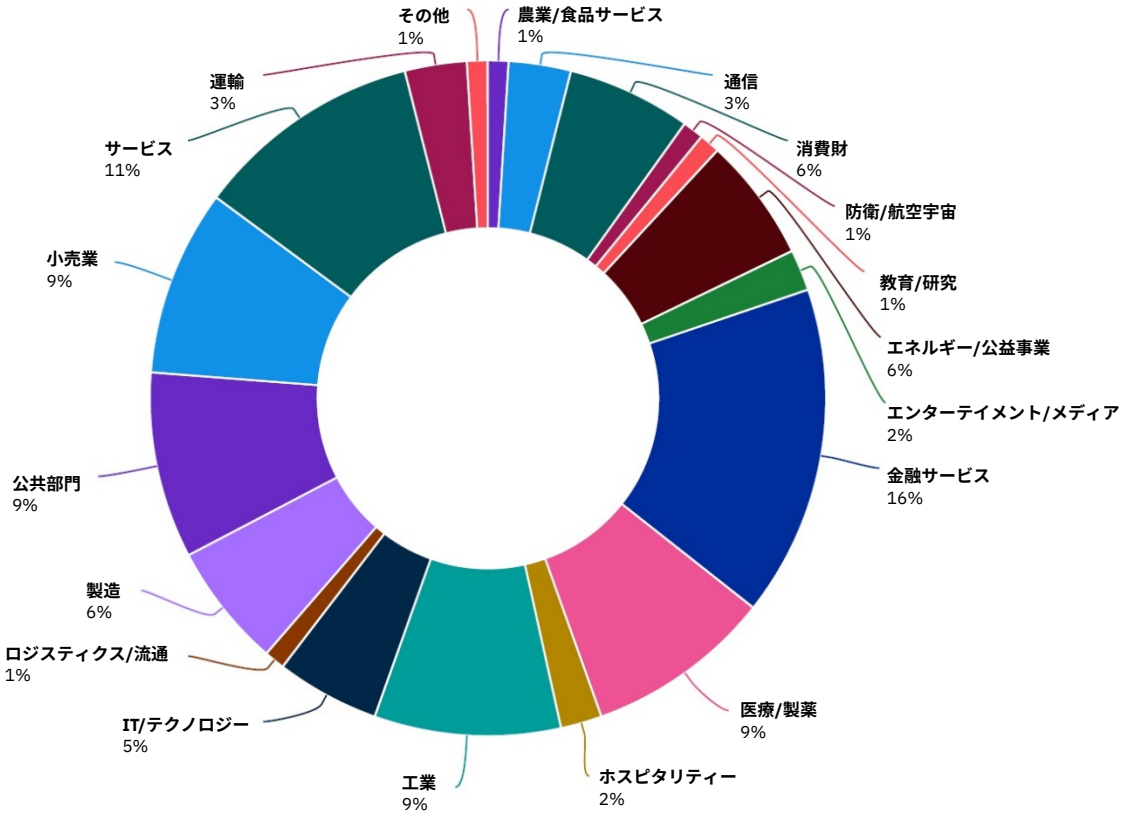


図 21

職務上の役割による分布

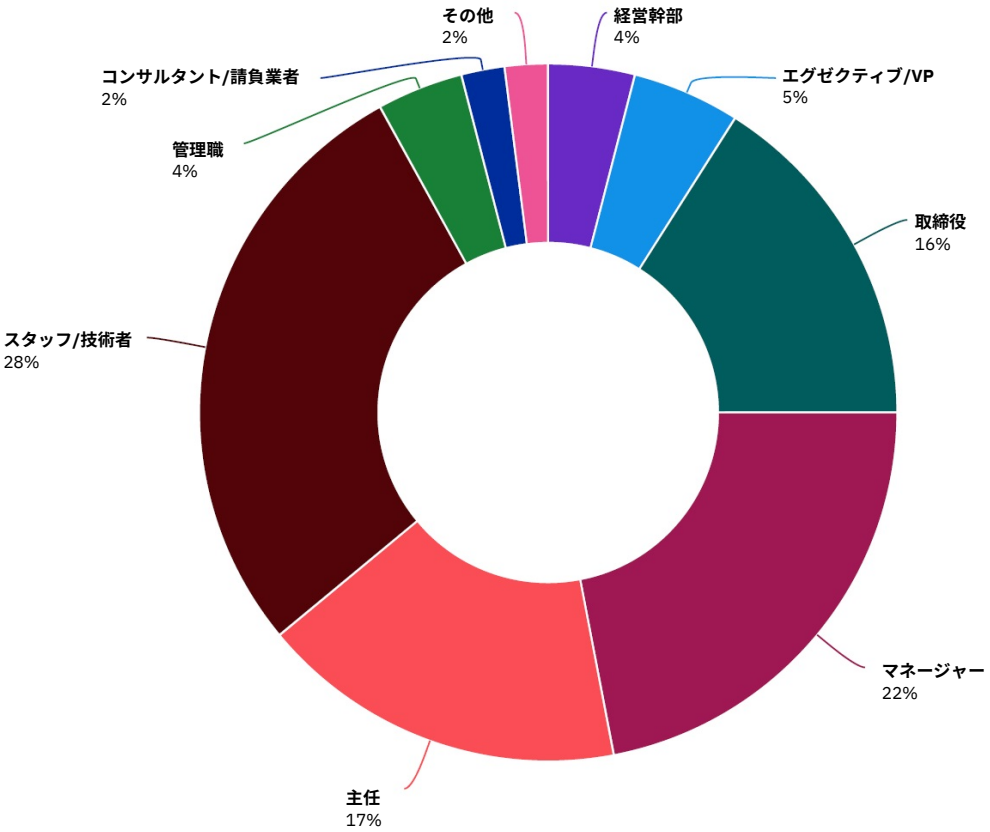
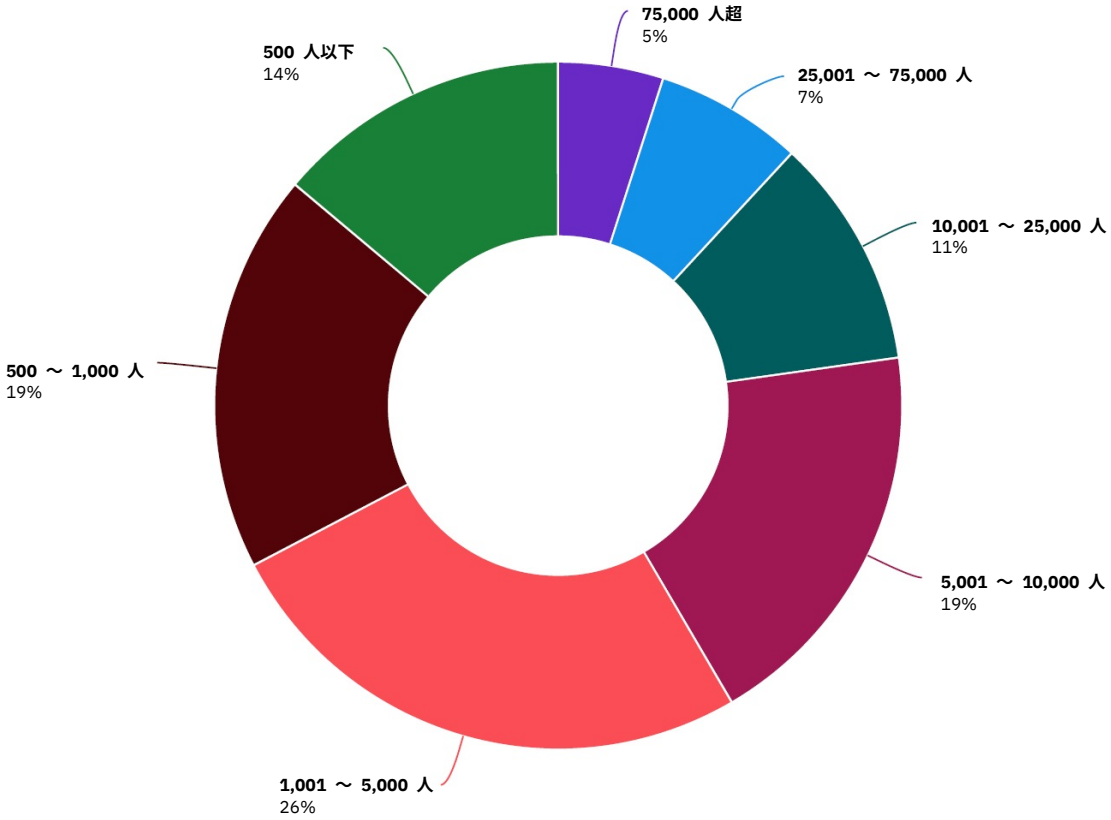


図 22

企業の規模による分布



調査の方法

米国、インド、ドイツ、英国、ブラジル、日本、オーストラリア、フランス、カナダ、ASEAN、中東に住む IT とセキュリティーの担当者にオンライン調査の項目を記入するように依頼しました。

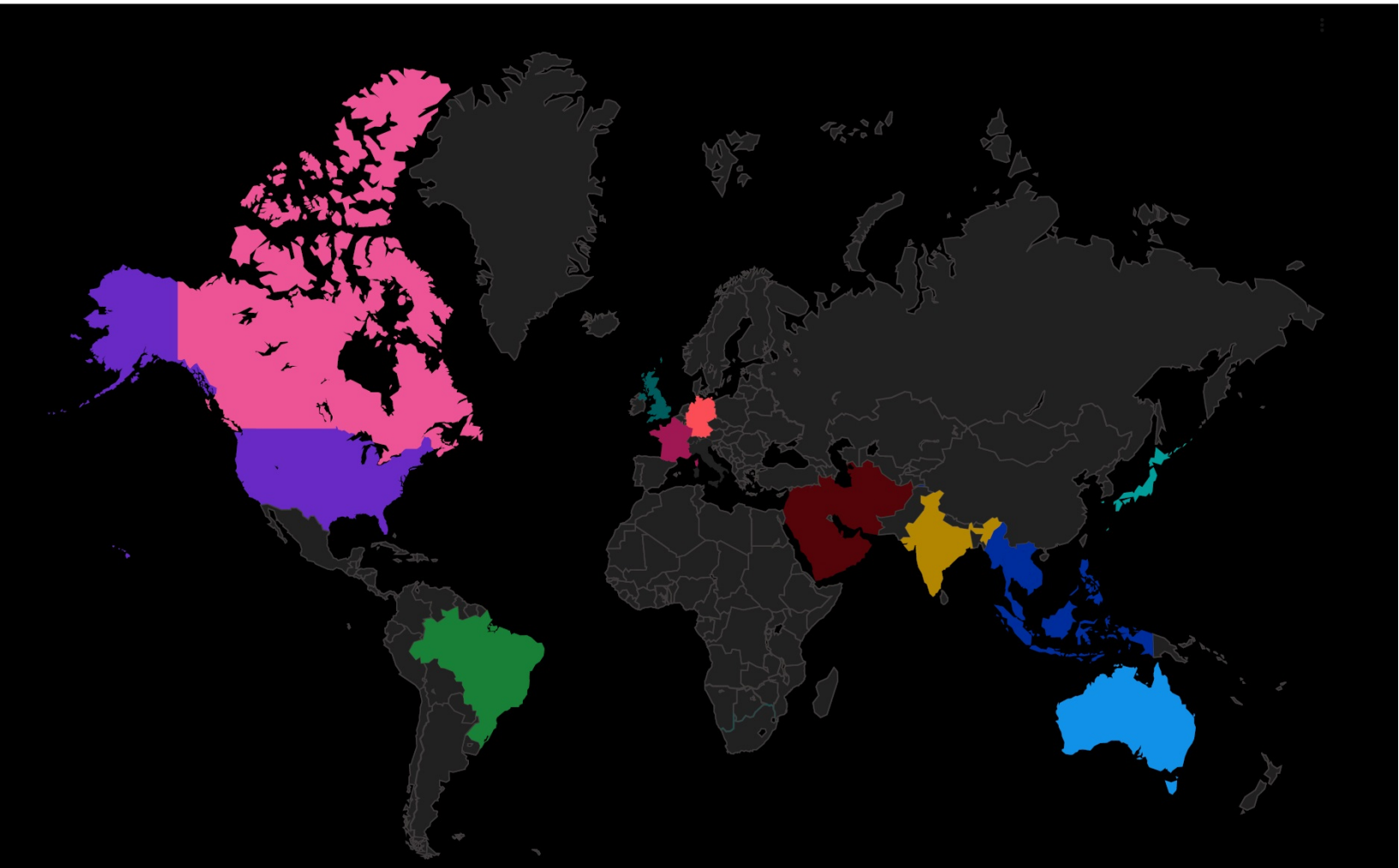
最終的な回答者のサンプルは 3,439 名で構成され、全体の回答率は 3.3% でした。

11

国と地域

3,439

回答者



*ASEAN は、シンガポール、フィリピン、ベトナム、タイ、マレーシア、インドネシアに住む回答者のサンプルです。

**中東は、アラブ首長国連邦とサウジアラビアに住む回答者のサンプルです。

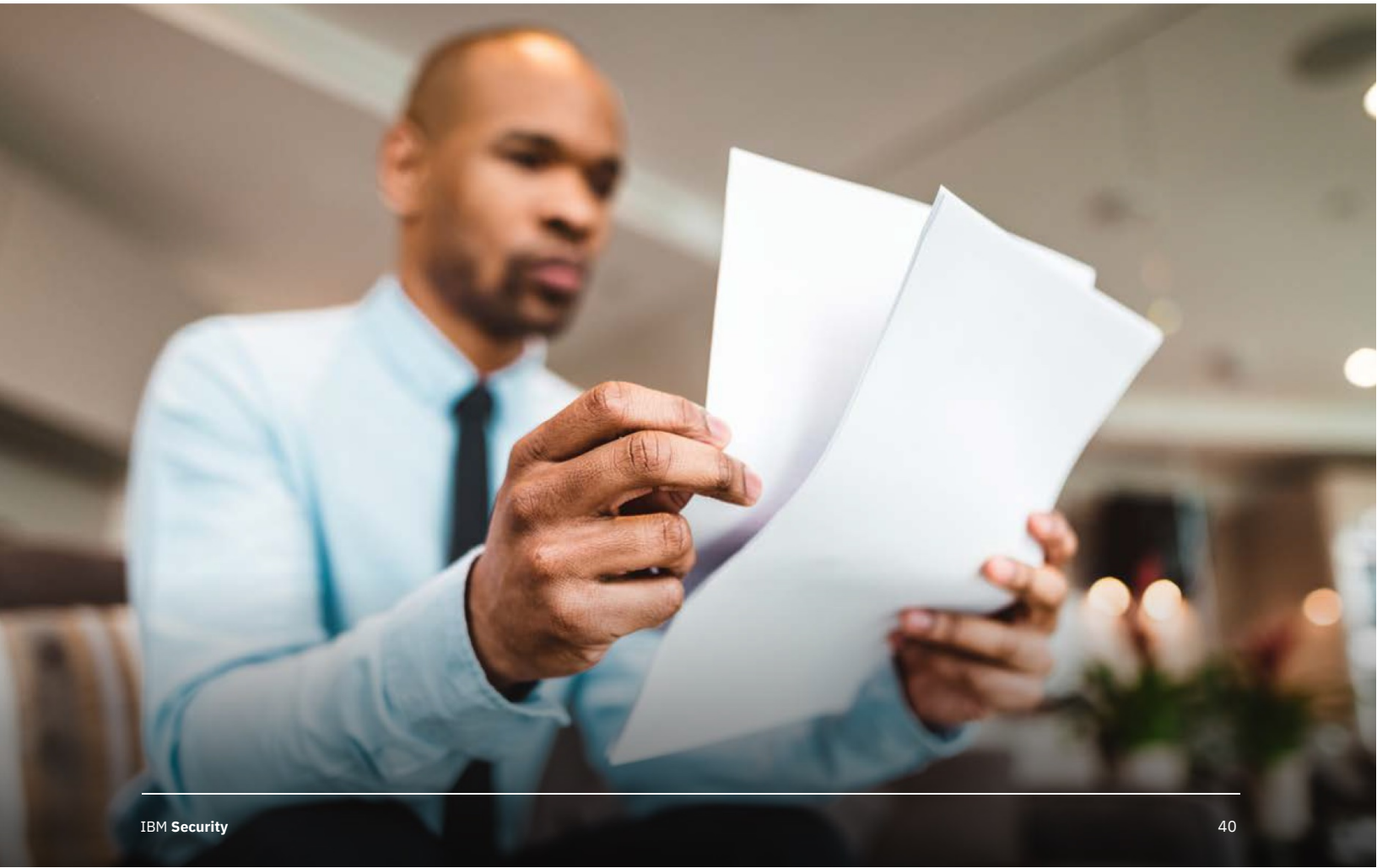
定義

サイバー・レジリエンス

サイバー・レジリエンスとは、サイバー攻撃の対処、軽減、復旧のために防御、検知、対応の機能を配置することと定義されます。これは、サイバー攻撃に直面しても企業がその事業目的と完全性を維持できる能力を指します。サイバー・レジリエンスを備えた企業とは、データ、アプリケーション、IT インフラストラクチャーへの重大な多くの脅威に対して、防御、検知、封じ込め、復旧を実施できる企業です。

ハイ・パフォーマー

この調査の一環として、高水準のサイバー・レジリエンスを実現したことを自己報告し、リスク、脆弱性、攻撃の軽減に成果を上げていた回答者を特定しました。ここでは、これらの組織をハイ・パフォーマーと呼びます。



調査の制約

調査研究には、調査結果から推論を引き出す前に慎重な検討を必要とする固有の制約があります。以下の項目は、Web ベースのほとんどの調査に関連する固有の制約です。

非回答バイアス

今回の調査結果は、調査の回答サンプルに基づいています。私たちは個人の代表サンプルに調査を送付し、結果的に多数の有効な回答が返送されました。非回答の検査でも、参加しなかった人々の意見が回答者の考えと大きく異なる可能性は常に存在します。

サンプリング・フレームのバイアス

調査の正確度は、連絡先情報および、当該リストが IT または IT セキュリティーの担当者である個人を代表している度合いに基づきます。また、マスコミ報道などの外部イベントによって結果にバイアスがかかることも認識しています。最後に、この調査では Web ベースの収集方法を使用したため、Web 以外の郵送調査や電話調査による回答では結果のパターンが異なっていた可能性があります。

自己報告の結果

調査研究の品質は、対象者から得られた内密の回答の完全性に基づきます。調査のプロセスに特定のチェックとバランスを取り入れることはできますが、対象者が正確な回答を提供しなかった可能性は常に存在します。

Ponemon Institute と IBM Security について

*サイバー・レジリエンス・レポート*は、Ponemon Institute と IBM Security が共同で作成したものです。調査は Ponemon Institute が単独で実施し、調査結果の後援、分析、報告、公開は IBM Security が行いました。

Ponemon Institute は、企業や政府機関内で責任を伴う情報とプライバシーの管理手法を促進する、独立した調査と教育に尽力しています。Ponemon のミッションは、人と組織に関する機密情報の管理とセキュリティーに影響する重大な問題について、高品質な実証的研究を行うことです。

Ponemon Institute は厳格なデータの機密保持、プライバシー、調査の倫理規範を擁護し、個人から本人を特定できる情報（または、ビジネス調査では企業を特定できる情報）を収集することはありません。さらに、無関係な質問や的外れの質問、不適切な質問を対象者に行わないように厳格な品質基準を設けています。

IBM Security は、エンタープライズ・セキュリティーの製品とサービスを統合した、最先端のポートフォリオを展開しています。世界的に有名な IBM X-Force® の調査に裏付けられたセキュリティー・ソリューションにより、お客様はビジネスの構造にセキュリティーを組み込んで、不確実性が増す世界においてビジネス成果を上げることができます。

IBM は、セキュリティーの調査、開発、デリバリーを行う世界最大級の組織を運営しています。130 以上の国で毎月 2 兆件を超えるイベントを監視し、3,000 件を超えるセキュリティー関連の特許を保有しています。詳細については、ibm.com/security をご確認ください。

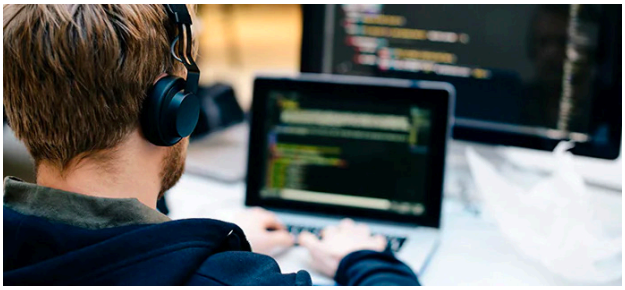
この調査レポートについて質問またはコメントがある場合は（レポートの引用や転載の許可を含む）、以下の連絡先に手紙、電話、メールでお問い合わせください。

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



マルチクラウド環境での利用に最適な統合ツール

詳細を表示 →

脅威の検知

詳細を表示 →

インシデント対応のオーケストレーション

詳細を表示 →

攻撃からの修復と復旧

詳細を表示 →

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2020

IBM Security