Deloitte.
デロイト トーマツ

Global Future of Cyber Survey 第4版

サイバーの展望

サイバーセキュリティのレジリエンス強化による変革価値の向上

サイバーの価値が高まる中で

サイバーセキュリティに対する要求は常に変化しています。新たな脅威やテクノロジー、また変化するビジネスニーズに応じて、組織は業界を問わず、優先事項と可能性をとらえ直し続ける必要があります。

サイバーの未来に対する見通しをより明確にすること。それは、私たちが新たなリスクの先を行くためだけでなく、新たなビジネス価値を見出すためにも絶えず続けていく取り組みです。

今回のGlobal Future of Cyber Survey第4版では、さらなる明確な展望についてご紹介します。サイバーセキュリティとビジネス価値の結びつきはますます強くなっており、テクノロジーを活用したプログラムを可能にし、ビジネスの成果を引き出すうえでますます不可欠な存在になっていることが分かります。また、組織がサイバーについて検討する機会が増大するにつれて、最高情報セキュリティ責任者（CISO）を含む経営幹部の役割がどのように変遷しているかという点も示します。

調査から得られた重要な発見をご紹介できることを光栄に思っています。この後のページでは、データに基づくインサイト、デロイトのサイバー領域におけるグローバルでの豊富な経験に基づく見解に加え、インタビューの回答者から直接得た意見を組み合わせてご説明します。ぜひご一読いただき、さらなる詳細についてのご要望がございましたらお問い合わせください。

Emily Mossburg
Deloitte Global Cyber Leader

目次

変革をもたらすサイバー戦略の新時代

成果とレジリエンスを重視する

サイバーの将来像は、絶え間なく発生するビジネス上の複雑さや変化、無数の新しい脅威とリスクに世界中の組織が対処する中においても、常に進化しています。その一方で、不変なものが一つあります。サイバーとビジネスの価値は強く結びついていることから、サイバーセキュリティは業界を問わずあらゆる組織が求める結果を一貫して実現していく方法の中心にあり続けることです。

サイバーセキュリティとビジネスインパクトの強い結びつきについて、今回のGlobal Future of Cyber Survey第4版では明確に示すことを目的としています。今回の調査では、世界の様々な業界のリーダー約1,200人に、サイバー脅威、企業活動、そして将来に関する見解を伺いました。また、企業の経営幹部のほか、IT、セキュリティ、リスク管理、事業に責任を持つその他の幹部の方々も調査の対象としています。

成果重視の傾向はますます顕著に

前回レポートである第3版においては、サイバーがビジネスの明確な機能領域としてどれほど進化しているかを認識していただけかと思います。サイバーは従来のITという枠を超えて、ビジネス成果を出すための重要なフレームワークの一部となっているということです。

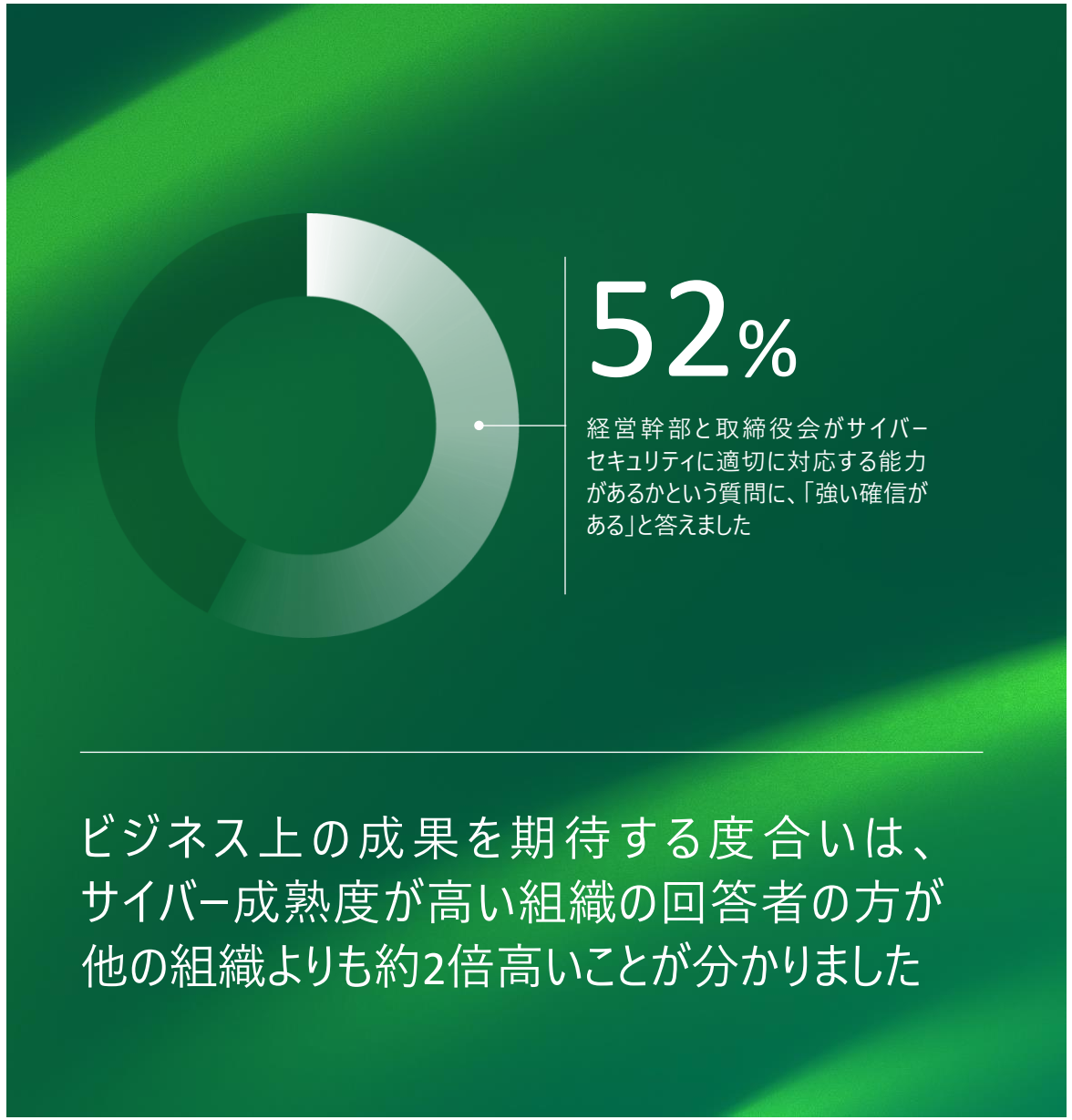
第4版となる今回の調査では、サイバー戦略がビジネス価値を最大化させるために不可欠であることに加え、実際、サイバーセキュリティが技術的変革に向けた活動により一層組み込まれるようになってきていることが明らかになりました。さらに、サイバーに精通した新しい経営幹部の登場とともに、サイバー領域のリーダー（特にCISO）の発言力が重要性を増していることも分かりました。

サイバーセキュリティへの関心が高まっているにもかかわらず、経営幹部や取締役会はサイバーセキュリティに適切に対応する能力があるかという質問に対して「強い確信がある」という回答は約半数（52%）にとどまりました。さらに、サイバーセキュリティを主に担当する経営幹部の回答に限定すると、「強い確信がある」という回答は34%程にとどまり、他の回答者よりも自らの能力に自信がないことがうかがえます。

しかし、サイバー成熟度が高いと分類された組織のみを見てみると、2つの重要な点が確認できます。上級管理職がサイバーセキュリティについて認識しているということと、組織のサイバー成熟度とサイバーセキュリティに適切に対応できるという確信の間には強い相関関係があることです。実際、サイバー成熟度の高い組織では、経営幹部や取締役会に対して確信があるという回答の割合は82%でした。これに対して、サイバー成熟度が中程度の組織では52%、サイバー成熟度が低い組織では39%でした。

今回の調査では、回答者のうち平均86%が、サイバー戦略とその対策を強化するために適度な範囲または最大限の取り組みを実施しており、サイバーを企業の不可欠な要素として受け入れていることが分かりました。また、平均で85%の回答者は、望まれるビジネス上の成果は適度あるいは大幅に達成されると予想しています。これは、戦略を実行して成功させるうえでサイバーが重要な役割を担っていることを示していますが、全ての組織が同じようにこのメリットを実感できるわけではありません。

また、組織のサイバー成熟度が高いほど、潜在的な影響は大きくなります。今回の調査では、ビジネス上の成果を期待する度合いは、サイバー成熟度が高い組織の回答者のほうが他の組織よりも約2倍高いことが確認できました。そのようなサイバー成熟度の高い組織がサイバーセキュリティをどのように理解して対策を講じているかは、サイバー成熟度の向上を目指す他の組織にとって参考となるインサイトと将来の方針となります。



サイバーの成熟度が高ければ脅威から逃れられるということではなく、問題が発生したときのレジリエンスを高め、重要なビジネスの継続性を実現できるということなのです

サイバー成熟度の高い組織は、備えが十分でレジリエンスも高くなります

今回の調査では、複数の要素に基づいてサイバー成熟度の高い組織を特定しました。前回の調査と同様、戦略的なサイバーセキュリティ計画と具体的なサイバーセキュリティ活動のレベル、また取締役会レベルでのサイバーセキュリティへの関与を評価しています。これらの要素に基づくと、サイバー成熟度が最も高い組織では、テクノロジーを活用したプロジェクトをサポートして作り上げるサイバーセキュリティの影響力が3ポイント増加していることが明らかになりました。

しかし、人工知能（AI）技術の急速な進歩により、グローバルな組織はさらに高度な攻撃を受けるようになってきています。同時に、AIを活用したツールやサイバーセキュリティのソリューションに投資する機会も生まれています。そこで今回、サイバー成熟度指数を更新し、回答者がサイバーセキュリティプログラムにおいてAI機能をどの程度活用しているかという観点も含めることにしました（25ページの「サイバー成熟度指数」を参照）。

こうしたサイバー成熟度の高い組織の間では、CISOをはじめとするサイバーセキュリティ責任者が、クラウドを活用したビジネス施策や、AIを取り入れた活動、エンタープライズリソースプランニング（ERP）のモダナイゼーション、その他のデジタルトランスフォーメーション（DX）における優先事項に対する投資をサポートする専門家として求められています。つまり、サイバーセキュリティはテクノロジーの機能に対する資金を確保するうえで大きな役割を果たしているということです。サイバーセキュリティへの関心の高まりは、CISOがDXに関する戦略的な議論により深く関与するようになってきているということでもあります。

そのようなサイバー成熟度の高い組織は、戦略計画・業務計画の策定やサイバーリスクの監視など、基本的なサイバー対策を実施していますが、最も注目すべき点は、サイバー攻撃を受けても迅速に回復できる能力です。サイバー成熟度が高ければ脅威から逃れられるということではありません。そうではなく、問題が発生したときのレジリエンスを高め、重要なビジネスの継続性を実現できるということなのです。

調査の回答者全体と比較すると、サイバー成熟度の高い組織は、世界全体の回答者よりも平均で27ポイント高くビジネス成果の達成を期待しています。また、過去1年間に11件以上のサイバー侵害が報告されているにもかかわらず（全体と比べて8ポイント高い）、悪影響を受けているにもかかわらず（全体と比べて平均7ポイント高い）、こうした期待を持ち続けています。しかしこれはサイバー成熟度の高い組織であるがゆえに、より多くのサイバー侵害を特定して報告しているという可能性もあり、必ずしも侵害発生数が多いというわけではないのかもしれません。

サイバー成熟度が高い組織のリーダーは、避けられない攻撃に対応して回復できるように備えておき、ビジネスを迅速に復旧して稼働させ、顧客にサービスを提供することが最も重要であるということを理解しています。

組織内のレジリエンスが高まる中、何に備えたい（または回避したい）と考えているか、また状況はどう変化したかという点について前回の調査と比較すると、サイバーセキュリティインシデントや侵害による悪影響として、技術的信頼性（システムとデータの信頼性、正確性、可用性）の喪失が第1位となりました。この点は、企業がDXの取り組みを加速させる中で、その重要性がますます高まっているといえます。

サプライチェーンやパートナーのエコシステムを含むオペレーションの混乱は、依然として第2位という上位にあり、パートナーやインフラストラクチャ全体のビジネスを継続させることの重要性が示されています。しかし前回は最上位であったことを考えれば、注目に値する変化ともいえます。評判の失墜は1ランク上昇し、第3位となりました（図1参照）。

今日、組織が取るべきステップは、サイバー投資がどのようにして組織の最適化、保護、価値創造を実現できるかに焦点を当てるべきです。それには、デジタル製品やインフラ全体でデータのセキュリティと整合性を可能にするサイバープラクティスを通じて、将来の成長のための強固な基盤を築くことが含まれます。この基盤には、将来の成長とビジネスの回復力を可能にするための、応答性の高いインフラとデジタルエコシステムの基本も組み込まれるべきです。本調査の最新版では、特に最もサイバー成熟度の高い組織において、より統合された技術変革戦略を通じて、サイバープログラムやCISO（最高情報セキュリティ責任者）がこれらのバリューストリーム全体でより大きな戦略的影響力を持つようになる顕著な傾向が示されています。

効果的なサイバーセキュリティ対策は、従来のインシデント対応のみに焦点を当てるだけでは不十分です。企業がサイバーリスク、セキュリティ、信頼を全体的な戦略に統合する方法を慎重に検討するべきです。全体的でビジネス志向の視点を採用することで、広範なビジネス目標と運用ニーズを結びつけることができます。このアプローチにより、サイバーセキュリティが単なる受動的な対策ではなく、組織の戦略的ビジネス、技術、運用の枠組みの一部として積極的に取り入れられることが保証されます。さらに、デロイトの研究によれば、市場で最もサイバー成熟度の高い組織は、同様のビジネス志向のアプローチを通じて大きな価値を得ています。

組織への悪影響（図1）

サイバーセキュリティのインシデントや侵害による悪影響についての回答は以下の順位となった

サイバーインシデントや侵害がもたらすネガティブな影響	第3版（順位）	第3版（割合）	第4版（順位）	第4版（割合）
技術的信頼性の喪失	6	55%	1	66%
オペレーションの混乱（サプライチェーンやパートナーのエコシステムを含む）	1	58%	2	66%
評判の失墜	4	55%	3	65%
人材確保・維持へのネガティブな影響	7	54%	4	64%
収益の損失	2	56%	5	64%
顧客の信頼の喪失・ブランドへのネガティブな影響	3	56%	6	63%
知的財産の盗難	8	54%	7	63%
規制当局による罰金	10	52%	8	63%
株価下落	9	52%	9	63%
戦略的な施策への資金不足	5	55%	10	63%

> “脅威のアタックサーフェスは急速に増えています。工場を新技術でつなぐと、新たなリスクが生まれます。メンテナンスのために製造元に電話をかけ直したり、組み立てラインのコンポーネントにソフトウェアパッケージをプッシュしたりするサプライヤーのロボットを組み込むと、事態はさらに複雑になります“
>
> **– General Motors 最高サイバーセキュリティ責任者 Kevin Tierney**

インサイトを導き出す方法

調査の背景

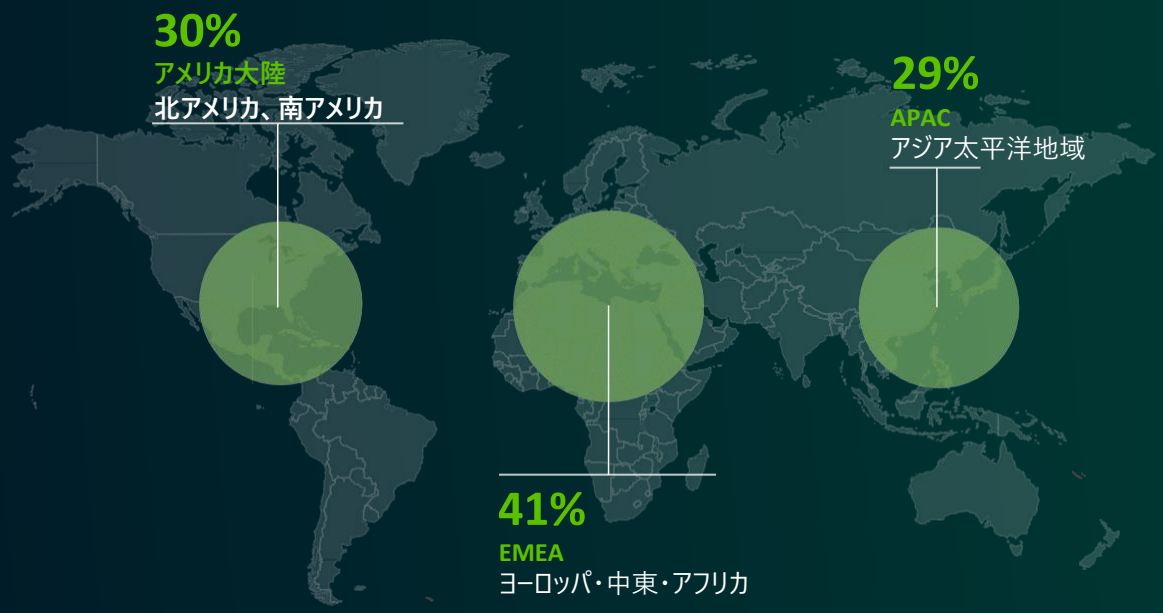
このGlobal Future of Cyber Survey第4版は、今日のビジネスとテクノロジーの状況の複雑さをふまえて作成されました。サイバーセキュリティの重要性を認識しながらもその価値の活用に苦慮している企業リーダーのニーズに焦点を当てています。

今回の結果は、サイバーに関する意思決定者であるディレクターレベル以上の約1,200人を対象とした調査に基づいています。様々なビジネス部門およびIT部門を交えた経営幹部レベルのエグゼクティブに加え、その直属の部下も対象としました。データは43カ国、6つの業界から収集され、対象組織は従業員数1,000人以上で年間売上高5億ドル以上の組織に限定されています。

また、さらに詳細なインサイトを収集し、私たちの見解の妥当性を確認するために、多彩な業界・地域のサイバー関連の上級意思決定者に詳細なインタビューを実施しました。戦略から戦術まで、また文化から技術実装まで、サイバーの未来に関連するあらゆる側面を網羅したインタビューです。

この調査では、サイバーの未来をより明確にするために、未来志向の視点を取り入れながら、前回のレポートからサイバーセキュリティがどのように変化したかを探る取り組みに焦点を当てました。また、経営幹部がどの程度サイバーに精通しているかを明確に把握することを考えました。この調査を通じて、組織が現在経験しているサイバー関連のビジネス価値と影響、また主要な組織が価値向上のために講じている注目すべき対策について理解を深めるためのインサイトが明らかになるように努めました。

調査対象組織の本社所在地



サイバーは戦略的価値にまで影響を及ぼす

より大きなビジネスインパクト実現に向けて

サイバー成熟度向上のための道筋は、サイバーの未来への意識が高まっている現在、より明確になっています。この道筋を行く組織は、サイバーセキュリティリスク戦略、セキュリティ施策、信頼構築アプローチをビジネスとテクノロジーの変革に組み込むことになります。これは、サイバーに精通した経営幹部と影響力の高いCISOがいれば実現可能なことです。デジタルをめぐる状況が急速に進化する中で、より効果的に変革に着手できるように自組織を位置づけることで、成功の度合いに大きく影響を与えられることが期待できます。

組織がサイバー成熟度の向上に継続的な取り組みを行う中で、ビジネスおよび技術運営、リーダーシップ全体にわたってサイバーセキュリティの連携を優先し構築することによって、同業他社との差別化を図ることができます。これにより、前回の調査で優先事項として挙げられていた戦略的成果をより成功裏に達成することができるでしょう。

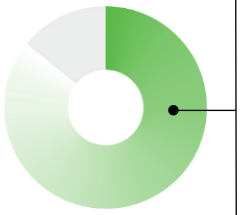
このレポートでは、調査データ、サイバー成熟度指数、世界中のリーダーのインサイトに基づく高度なインサイトを導き出します。これにより、パフォーマンスの高い組織がどの領域でどのように際立っているかを示し、世界のサイバーセキュリティ専門家がサイバー施策の実践において成熟できるようにするためのガイドを提供します。

今回のテーマ

1. サイバーセキュリティは依然として戦略的なビジネス価値の重要な要素であり、さらに関心は高まっている
2. サイバーに精通している経営幹部が増え、 CISOの影響力は拡大している
3. テクノロジーを活用したプログラムやビジネスのDXにサイバーセキュリティは深く組み込まれている
4. サイバー成熟度が高い組織ほど、対応に自信を持ち、サイバー活動と投資を通して大きなメリットを実現できる

サイバーセキュリティは戦略的ビジネス価値のための重要な要素であり続けており、その重要性は増しています

高度な相互接続が進む今日のデジタル環境において、サイバーセキュリティの基本的な重要性は否定しようもありません。また、組織がサイバー対応能力を強化してビジネス価値を高めるための活動や対策、戦略的手段には事欠きません。



86%

サイバーセキュリティ向上のために中程度または大規模な範囲でなんらかの活動・対策を実施していると回答しています。

行動を起こすことは最初の一歩であるが、それで終わりではありません

回答者の多くは、サイバーセキュリティ対策の必要性を深刻に受け止めており、86%がサイバーセキュリティ向上のために中程度または大規模な範囲でなんらかの活動・対策を実施しています。この行動レベルは、組織がこれらの活動および実行するために効果的なサイバーセキュリティプログラムの必要性を極めてよく理解していることを示しています。また、必要な活動のリストが増え続ける中で、それに対応するペースを維持していることも示されています。

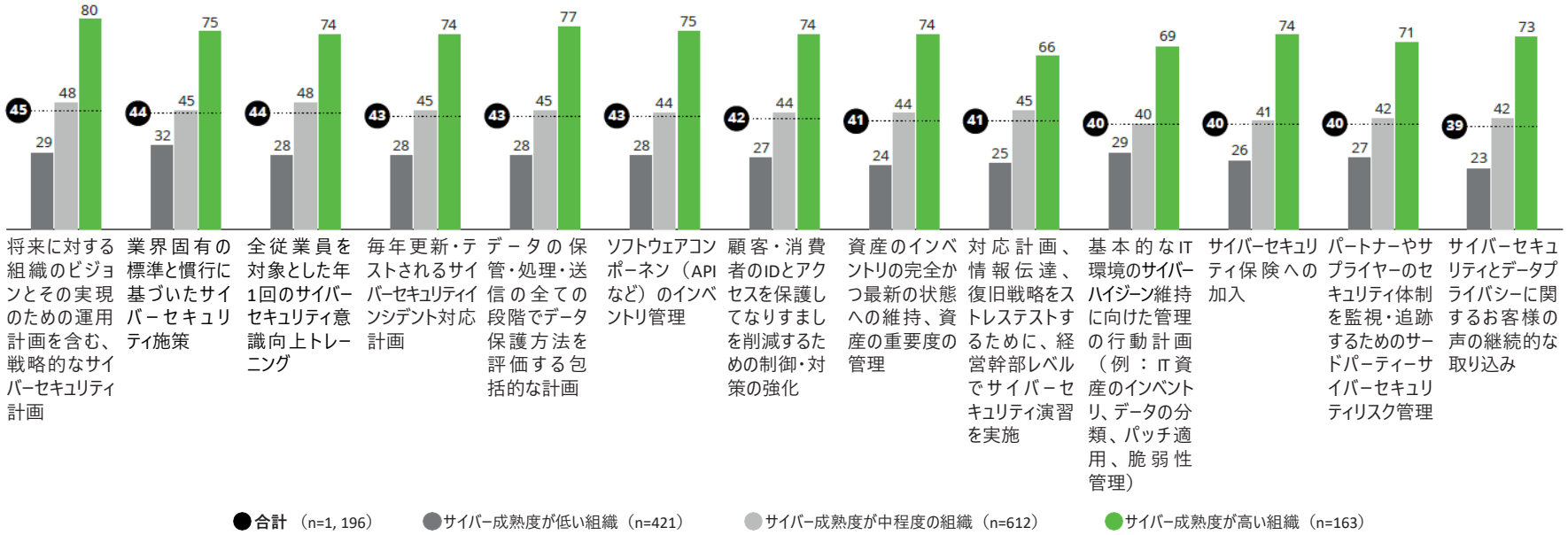
これらの回答者は、リスク軽減、サイバーセキュリティコントロールの強化、インシデント対応の改善、従業員の意識向上、戦略的なサイバーセキュリティ計画の採用など、サイバーセキュリティを管理するための様々な活動の実施に注力しています。

これらの活動をサイバー成熟度の観点からこれらの活動を集計してみると、サイバー成熟度の高い組織はサイバー成熟度の低い組織よりも積極的に取り組んでいることが分かります（図2参照、25ページの「サイバー成熟度指数」も参照）。

> **“重要なのは、基本を正しく理解し、発展させ、習熟度を上げることです。毎日、続けるのです。基本的な制御、資産管理、脆弱性管理などに無心に取り組み、習熟すること。それをやらなければならないのです”**
>
> **– ライフサイエンス・ヘルスケア組織 CISO**

サイバーセキュリティ活動とサイバー成熟度の関係（図2）

サイバー成熟度の高い組織は、サイバー成熟度の低い組織よりも積極的に重要なサイバーセキュリティ活動に取り組んでいる（単位：%）



サイバーセキュリティ戦略の実施状況（図3）

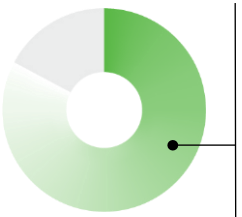
サイバーセキュリティの強化・向上のために実施している具体的な戦略

注記：四捨五入の関係で、それぞれの割合の合計が100%にならない場合があります。

戦略に基づいて、ビジネス全体へのサイバーセキュリティ対策の組み込みは進んでいく

圧倒的多数の組織においては、ベンチマーキングと測定、信頼できるプロバイダにーとの協力、情報共有のためのコンソーシアムへの参加、そしてサイバーセキュリティ能力と投資を管理する上級ビジネスリーダーとITリーダーで構成される管理組織の設立などです。

全体として、調査回答者の83%がこのような対策が全体的なサイバーセキュリティ戦略の不可欠な部分であることに同意、または強く同意しています。この同意のレベルは、サイバーセキュリティ戦略がビジネスに組み込む動きが継続していることを示しています。



83%

そのような対策が全体的なサイバーセキュリティ戦略の不可欠な部分であることに、同意しています。

脅威が高まる中、サイバーセキュリティ投資への注目も高まっている

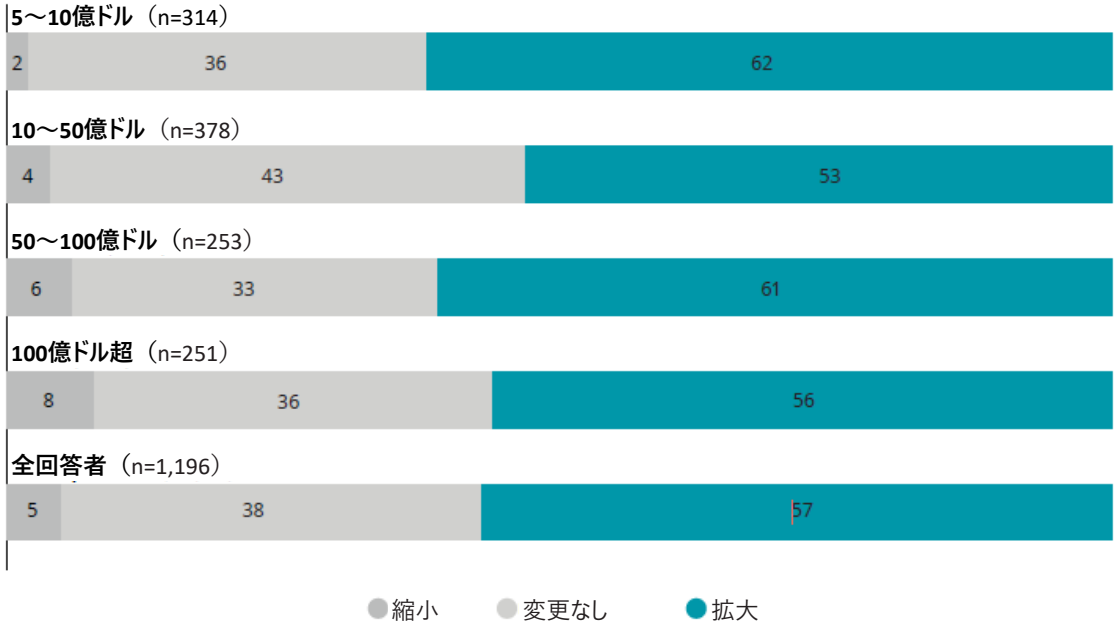
調査対象となった世界中の回答者の過半数（57%）が、今後12～24カ月の間にサイバーセキュリティ予算を増加させることを見込んでいます。また、回答者の58%は、サイバーセキュリティ支出をデジタルトランスフォーメーションイニシアチブ、ITプログラム、クラウド投資などの他のプログラムの予算と統合し始めることを期待していると述べています。このレベルで投資と予算の統合が行われるのは、サイバーセキュリティ活動がビジネス全体にますます密接となっていることが示唆されています。また、サイバーセキュリティ資金の調達はゼロサムゲームである現実を強調せしています。ゼロサム環境では、変革プロジェクトにおいてコストを削減するためにサイバーセキュリティが見過ごされることが多いからです。

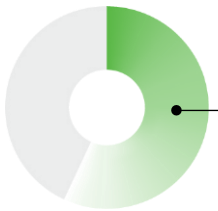
ビジネスおよび技術運用、さらにはリーダーシップ全体にわたってサイバーセキュリティの連携を継続的に優先し構築することは、組織が他と差別化し、戦略的な成果を成功裏に達成するために重要です。サイバーマチュリティの高い組織は、サイバーセキュリティが単なるITの問題ではなく、組織の全ての機能と階層にわたって統合が必要なビジネスクリティカルな要素であることを理解しています。このような強力なサイバーセキュリティの連携を促進することで、組織はサイバーセキュリティに関連する協力体制、情報共有、意思決定を強化できます。

このアプローチにより、リーダーはビジネス目標に合致し、効果的にサイバーリスクを軽減するための情報に基づいた戦略的意思決定を行うことができます。最終的には、サイバーセキュリティを優先し、企業の各機能やリーダーシップの役割を統合するために強力な連携体制を構築する組織は、ますますデジタル化が進む世界で資産、評判、そして全体的な回復力をより良く改善することができます。

予算は拡大の傾向（図4）

回答者の57%は、今後12～24カ月の間にサイバーセキュリティ予算拡大を見込んでいる（単位：米ドル、%）





57%

今後12～24カ月の間にサイバーセキュリティ予算拡大を見込んでいます。

“企業は、規模、保有するデータの種類、オンラインでのプレゼンス、サプライチェーンの慣行などの諸要因が様々であるため、脅威のプロファイルも独自のものになります。全ての企業が、脅威対応の担当者、またその理由、実際の対応策を理解したうえで強力な脅威インテリジェンス戦略を持つことが不可欠です。潜在的な攻撃者の動機や戦術を理解することは、効果的なセキュリティ対策のために重要です”

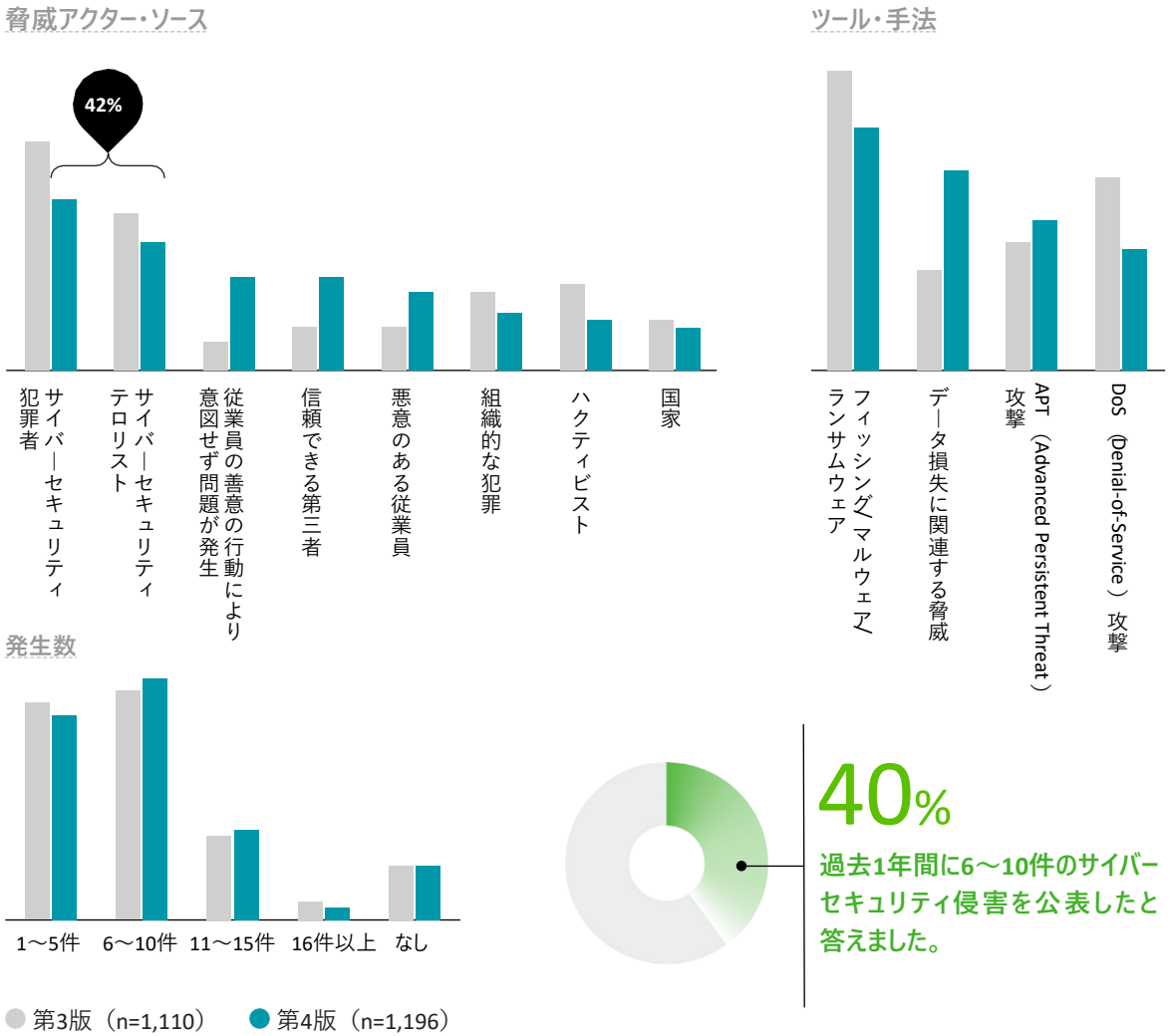
– Johnson & Johnson 最高情報セキュリティ責任者　Gary Harbison

回答者の全体平均で、年間1億4700万ドルから2億6600万ドルがITに費やされていることが分かりました。その19%にあたる3900万ドルはサイバーセキュリティ関連の活動に割り当てられており、回答者は今後12～24カ月でこの額が3%拡大することを見込んでいます。

脅威はどこからどのように発生するか（図5）

サイバーセキュリティ侵害の発生源・手法別に、脅威が発生した組織数を集計

（第3版と第4版の比較　単位：%）



40%

過去1年間に6〜10件のサイバーセキュリティ侵害を公表したと答えました。

新たな脅威や生成AI（GenAI）関連のサイバーリスクを含め、攻撃は現在も拡大しています

投資の増加が見込まれる背景は、サイバー脅威の複合化と件数増加に企業が直面しているためです。前回の調査と同様に、サイバー犯罪者やテロリストが所要な脅威アクターの上位を占め、回答者の42%がハクティビスト（政治的・社会的理念に関する声明発信を目的とする脅威アクター）、サイバー犯罪者（金銭的利益のために悪意のある活動を行う者）、および内部関係者（個人的な不満や利益獲得を狙った者）を含む多様な脅威アクターの中で最も懸念される存在として報告されました。

サイバー攻撃者が使用しているツールや手法については、フィッシング、マルウェア、ランサムウェアの組み合わせが最大の脅威ベクトルです。これを挙げた回答者は34%ですが、前回の調査からは8ポイント低下しています。同時に、データ損失に関連する脅威の報告数が大幅に増加しており、前回の14%から28%に増加しています。

また、回答者の40%が、過去1年間に6〜10件のサイバーセキュリティ侵害を公表したと述べました。これは前回の調査から2ポイントの増加となっており、攻撃の増加が継続しているのは驚くべきことではありません。脅威アクターが利用できる攻撃サーフェスは広く、今も拡大し続けているからです。

この調査では、GenAIの登場によって生じた新たなサイバーリスクに回答者がどのように対応しているかも追跡、分析しています。そのようなリスクに対する認識は、サイバー成熟度の高い組織の方が成熟度の低い組織よりも顕著です。最もサイバー成熟度の高い組織の回答者が挙げた、サイバーセキュリティ戦略に影響を与えるGenAI関連リスクのトップ4は以下の通りです。

- GenAIによる生成物の説明可能性（82%）
- 情報の信頼性にリスクをもたらすGenAIアルゴリズム（81%）
- GenAIと人間の協働を管理する手法の効果的な開発（81%）
- データポイズニング（GenAIの生成物に影響を与えるためにトレーニングデータセットを破壊する行為）（80%）

プロセスを自動化し、サプライヤーやその他のサードパーティーとデータを共有する組織が増えるにつれて、新しい脆弱性が出現する可能性があります。ますます複雑化するデジタルインフラとエコシステムは、新たな攻撃の機会を生み出しているのです。

“あらゆるものが、そして誰もが相互につながっているため、リスクは増大します。よって、サプライチェーン全体を考えなければいけません。様々な企業全体にわたる、あらゆるレベルのセキュリティ機能について考えます。キャンパスと従業員の現状にはかなり満足していますが、ネットワークに接続して利用する人すべてが同レベルの能力を備え、セキュリティと管理に対処できるようにするには、どうすればよいかの検討を続けています”

– Ford Motor Company 最高情報セキュリティ責任者
Patrick Milligan

サイバープログラムのメリットに期待が高まる中、技術的信頼性が最大の懸念事項

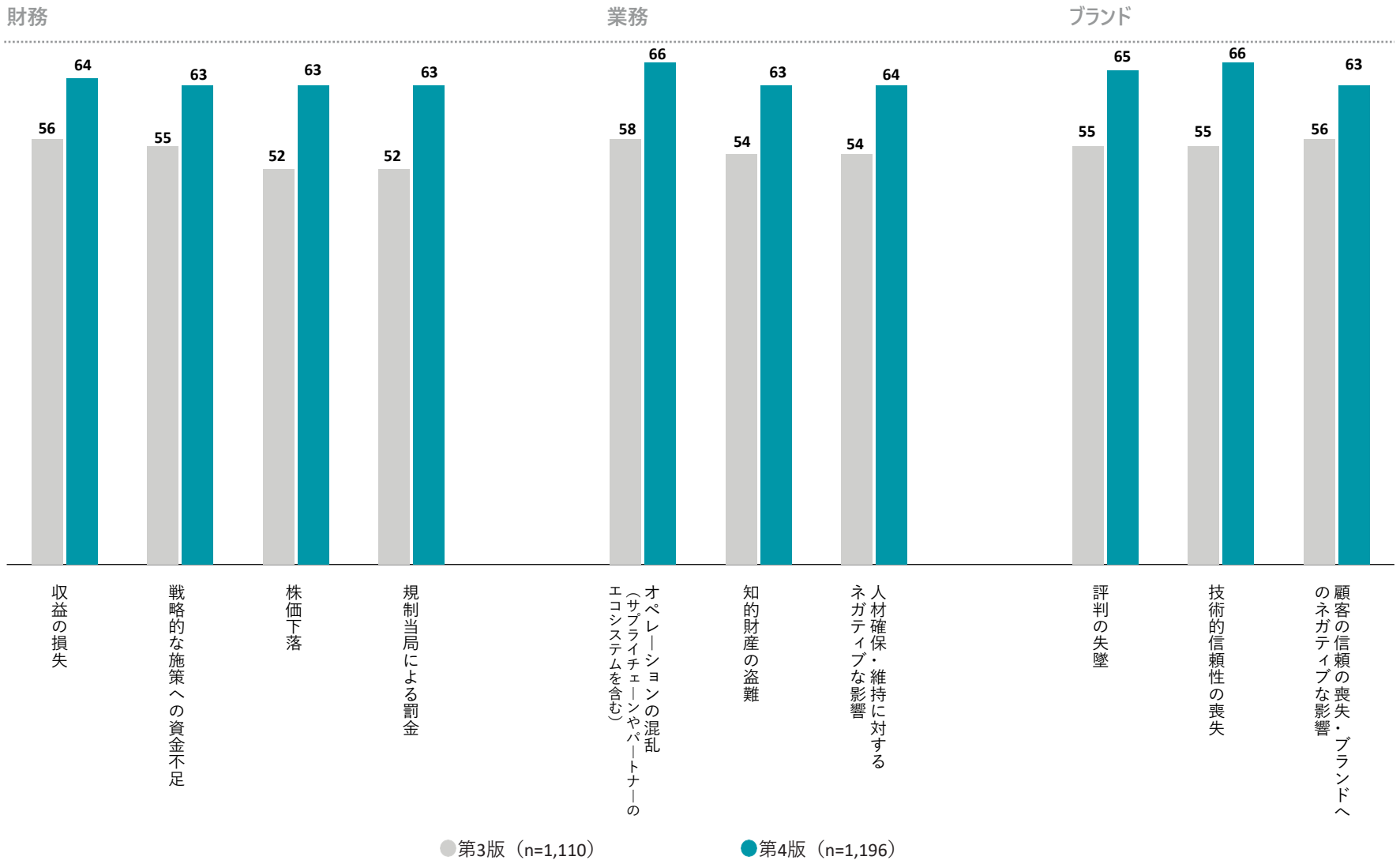
脅威が切れ間なく張り巡らされる中で、組織は、財務、業務、ブランドの3領域にわたる影響を含め、様々な悪影響を受けています（図6）。この3領域を合わせて見ると、上位2つは技術的信頼性失墜とオペレーションの混乱（7ページの図1）です。この点が前回から変わらず挙げられていることは、重要なテクノロジーや業務を維持し、ビジネスのレジリエンスを高めることができる効果的なサイバーセキュリティプログラムの重要性を示しています。

悪影響を実際に経験した割合は、全ての事項について前回よりも高くなりました。第3版では平均56%、第4版では平均64%が全ての事項を中程度または大部分の領域で経験しています。

この悪影響の増加は、2つの現実を示唆しています。第一に、組織がサイバー攻撃の影響をより包括的に報告している可能性があり、これは意識の向上を示しています。第二に、GenAIやその他の先進技術によって攻撃面と頻度が増加していることが考えられます。これにより、将来的にサイバーセキュリティの重要性がますます高まっており、強固なサイバーセキュリティ計画を策定するための明確なきざしとなっているといえます。

悪影響の詳細を3領域で整理（図6）

サイバーセキュリティインシデントが最も大きな影響を与えると回答された事項を、財務、業務、ブランドの3領域で整理（単位：%）



インシデントや侵害によるこのような悪影響は、組織がサイバーセキュリティ施策実施によって達成できると期待するメリット、つまりビジネス成果とは著しく対照的です。今回の調査では、サイバーセキュリティ施策に期待される成果の上位3つは、（1）知的財産の保護、（2）脅威の検出と対応の向上、（3）効率性と機敏性の向上でした（図7）。

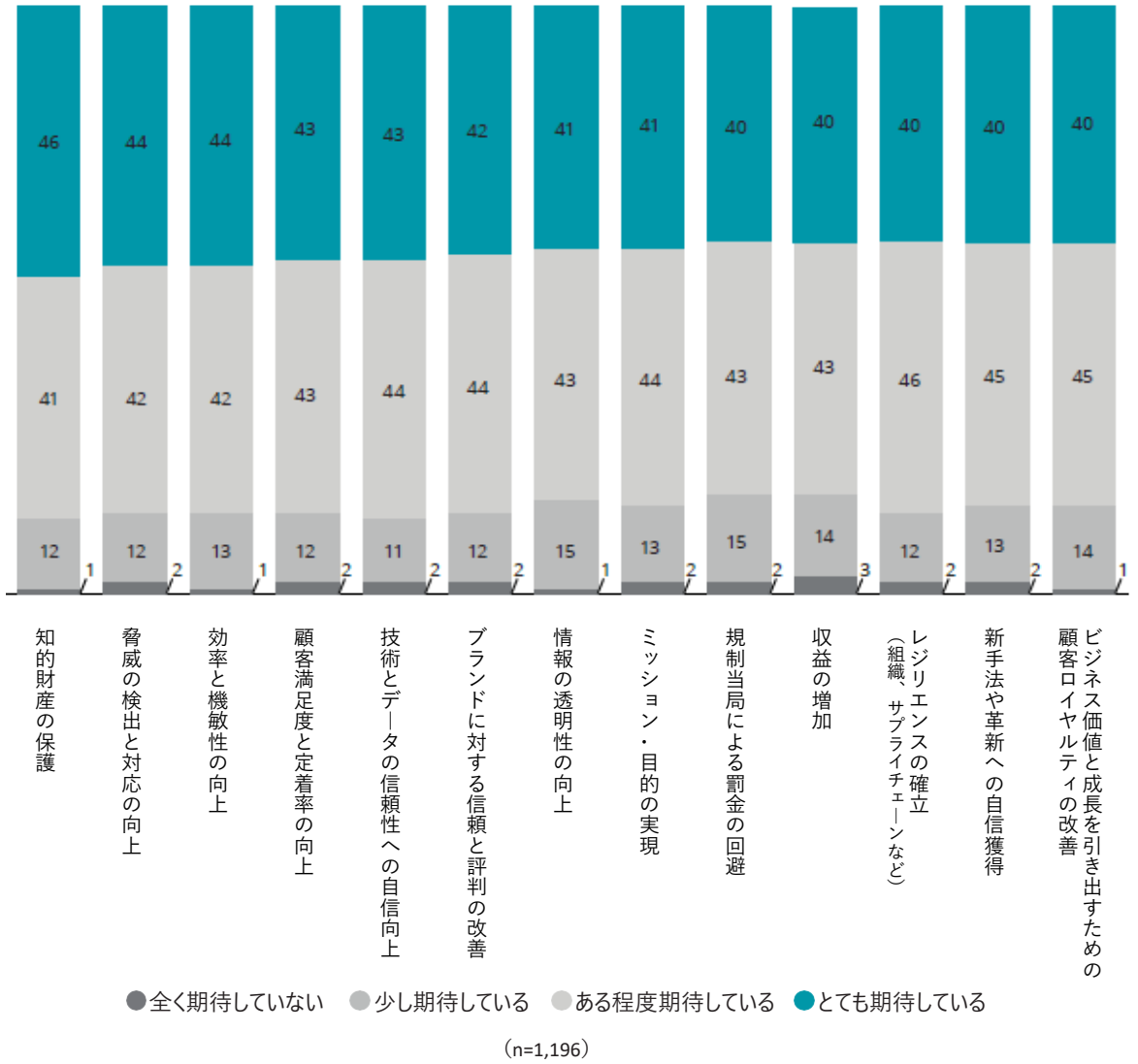
サイバーセキュリティに投資して運用上のレジリエンスが強化されることから期待できるメリットを多くの回答者が挙げていますが、その内容は業界によって多少のばらつきがあります。

消費財	資源・エネルギー・生産財（ER&I）	金融サービス（FSI）	政府・公共サービス（GPS）	ライフサイエンス&ヘルスケア（LSHC）	テクノロジー・メディア・通信（TMT）
技術とデータの信頼性への自信向上	効率と俊敏性の向上	知的財産の保護につながる脅威の検出と対応の向上	知的財産の保護	顧客満足度と定着率の向上	効率と俊敏性の向上

サイバーセキュリティへの期待は明らかに高まっており、組織のサイバー機能に関する主な責任者として、その期待はCISO（最高情報セキュリティ責任者）に向けられています。CISOは、ビジネスの期待を管理し達成するという大きな仕事に直面しています。どの組織にとっても、侵害やインシデントは避けられないですが、サイバーセキュリティの約束はリスクと悪影響を最小限に抑え、可能な限り多くの利益を最大化することです。最終的には、信頼できるデータを使用して成長を促進する、より安全で回復力のある組織の運営を可能にすることです。

サイバーセキュリティに期待する成果（図7）

サイバーセキュリティ施策を実施することで期待されるメリットと、それぞれへの期待度（単位：%）



（n=1,196）

サイバーに精通している経営幹部が増える中で、 CISOの影響力は拡大している

今回の調査でサイバーセキュリティ活動について質問した結果、組織においてCISO（最高情報セキュリティ責任者）は、調査で尋ねたサイバーセキュリティ活動の大部分に対する主要な責任を負う傾向があり、CIO（最高情報責任者）も重要な役割を果たしています。多くの場合、これらのCISOはCIOまたはCTO（最高技術責任者）に報告しています。しかし、調査によれば、約5分の1のCISOは直接CEO（最高経営責任者）に報告しています。これは、C-suite（経営幹部）およびエグゼクティブリーダーシップ全体にわたる影響力を持つビジネスの整合性の重要なシグナルです。

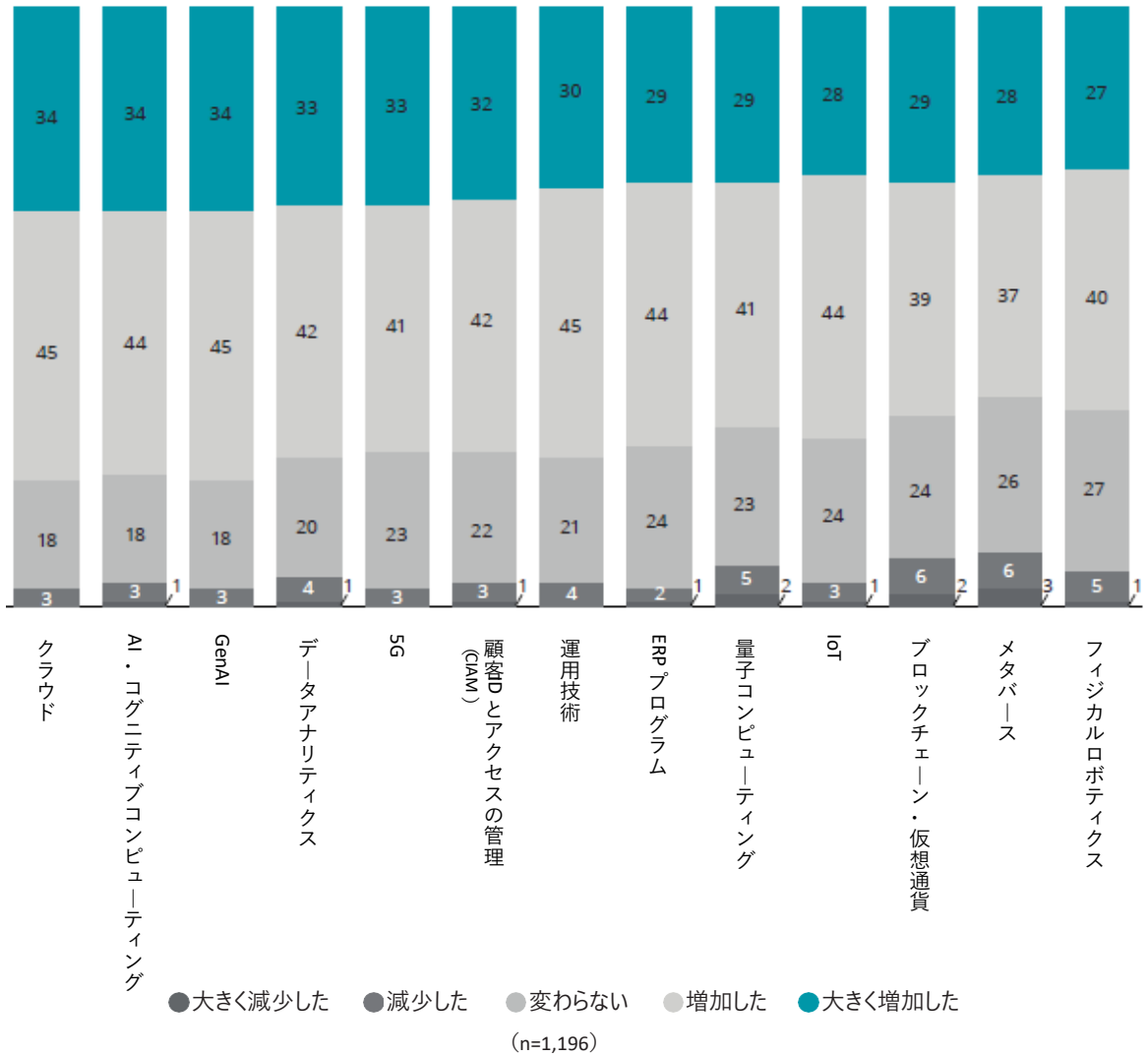
CISOの影響力は他の面でも拡大しているようです。CISOまたはそれに相当するリーダーは、ビジネス価値の推進におけるテクノロジーの機能の重要性が高まってきていることを受け、テクノロジーに関するビジネス上の戦略的な議論に参加するようになってきています。

CISOの関与は、もはや任意ではない

回答者の約1/3は、過去1年でテクノロジーの機能に関する戦略的な議論にCISOが参加することが大幅に増加したと述べています。例えば、クラウド、AI・コグニティブコンピューティング、GenAI、データアナリティクス、5G、顧客IDとアクセスの管理（図8）といった分野に関する議論です。

戦略的な議論へのCISOの参加（図8）

ビジネス上重要なテクノロジーの機能に関する議論にCISOが参加している分野と、その度合い（単位：%）



（n=1,196）

CISOの影響力がリーダーシップ全体で増大し、組織がよりサイバーに精通することを目指す中で、CISOは取締役会および経営幹部に対してセキュリティの脆弱性、リスクシナリオ、レジリエンスを高めるために必要な行動について助言や教育を行うための不可欠なパートナーになると予想されます。将来的には、CISOには組織全体のサイバーセキュリティ戦略を主導するだけでなく、戦略的な指針を示し、他の経営幹部と緊密に協力してセキュリティ施策とビジネス目標とを逸しさせるために指針を示すことが求められます。

サイバーセキュリティに焦点を当てる経営幹部のうち、経営幹部と取締役会がサイバーセキュリティに適切に対応できると確信している割合は34%にすぎません。これは、回答者全体に比べて18ポイント低い値です（図9）。

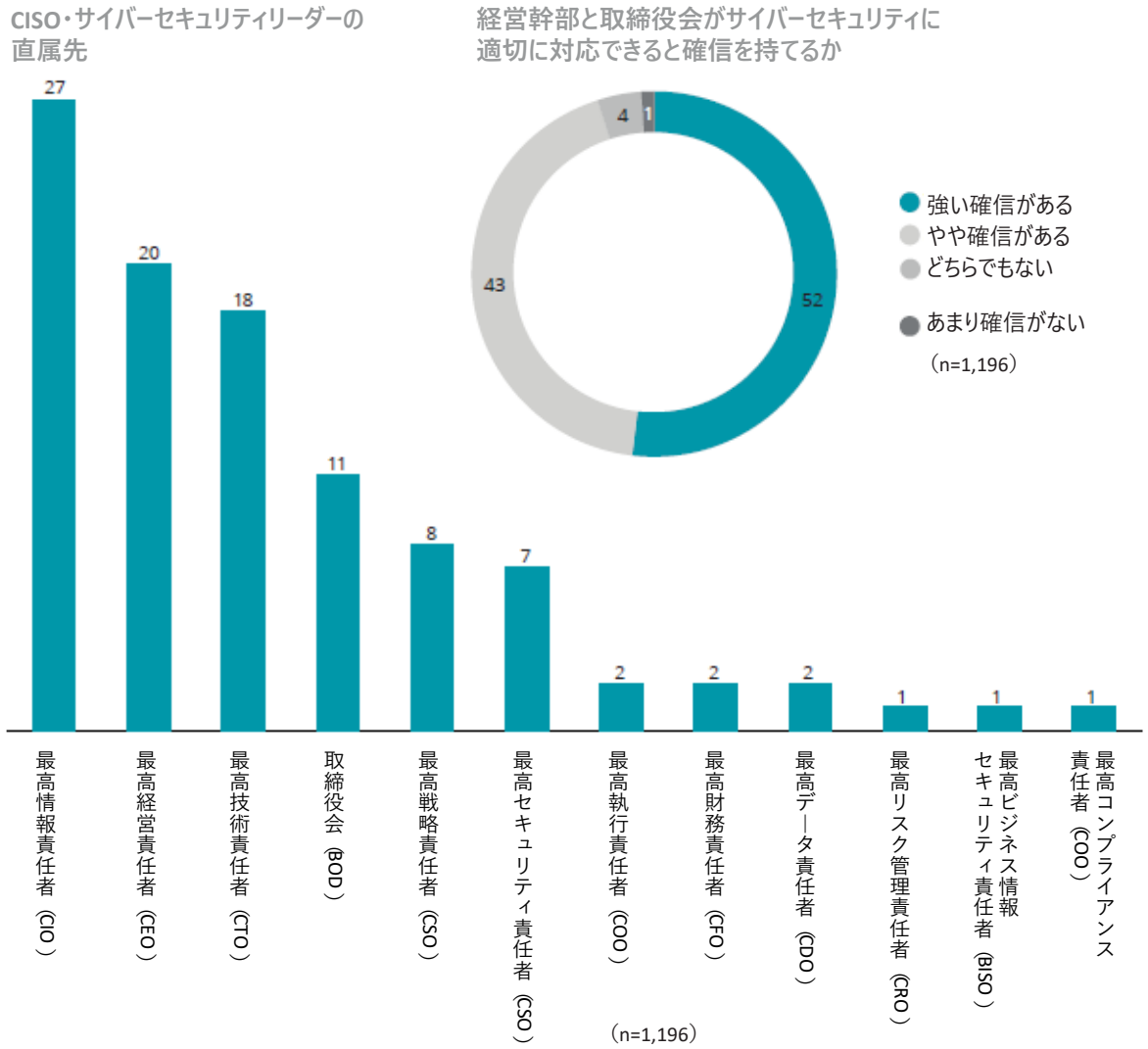
分析によると、サイバー成熟度の高い組織は、CISO（最高情報セキュリティ責任者）の役割が経営幹部および取締役会と連携する上で重要であり、サイバーセキュリティリスクに効果的に対処するための鍵であることを理解しています。これらの組織は、CISOがより影響力のある役割を担うことで、価値あるインサイトと指針が示され、サイバーセキュリティが戦略的なビジネス問題として適切な注意が払われ、リソースも投入されるようにできると認識しています。Deloitteは、このようなCISOの役割拡大という動向を鑑みて、進化し続けるサイバー脅威、技術能力の向上、サイバーセキュリティとビジネスの統合を検討し、CISOの役割を引き上げる対策を加速することを推奨します。

CISOの役割は進化しており、経営幹部の一員としての地位を持っていると言う一方で、経営幹部が今日の複雑なサイバー環境を自信を持ってナビゲートできるという確信はまだ不足しています。この低い信頼レベルは、CISOが効果的にリスクや脅威について教育し、組織の対処能力を伝えることで、経営幹部が今日のサイバー情勢の複雑さを認識するようになったことを示唆している可能性があります。また、回答者全体の中には、組織のサイバー成熟度と回復力に対する過信があることも示しているかもしれません。

“私たちの大きな方向転換は、ソリューション構築後ではなくその前にセキュリティに関する議論を持ち込むことです。従来のように評価段階でセキュリティを考えるのとは反対に、設計段階からセキュリティを組み込む方式に移行し、セキュリティを全体的なビジネスの戦略的な要素にしていきたいと考えています”

– 政府・公共サービス機関 サイバー・ITセキュリティ担当 事務局長

経営幹部のサイバーセキュリティに関する知識とCISOの直属先との関連（図9）
経営幹部に対するリーダーの確信の有無と、CISOの直属先の全体像（単位：%）



サイバーセキュリティは多くの組織の取締役会の主要な議題となっており、回答者の88%が取締役会が少なくとも四半期ごとにサイバー関連の問題に取り組んでいると述べていますが、さらなる教育の余地があり、CISOが戦略的リスクと対応策について助言することが求められています。この点について、デロイトのTech-Forward Boardroomレポートでは、取締役会での議論の質を深めるために、技術リーダーは技術用語をビジネスニーズに置き換え、CFOとより密接に連携してビジネス上の影響を明確にし、報告とベンチマーキングの構造を一貫して整え、取締役会に共同でプレゼンテーションを行い、技術面を掘り下げるワークショップを開催し、フィードバックのループを作成し、これらの活動を小規模な取締役会でのセッションや会議に展開することを推奨しています。

88%

取締役会は少なくとも四半期ごとにサイバー関連の課題に取り組んでいると答えています。

CISOの役割は進化しており、議論に参加する存在になっていると多くの回答者が述べていますが、経営幹部が今日の複雑なサイバー環境に自信を持って対応できるという**確信はまだ不足しています。**

“取締役会とは四半期ごとの情報共有を標準として実施していますが、これは数年前には見られなかったことです。今は開催頻度だけでなく、議論の深さも増していると思います。取締役会が関心を持つ重要なトピックについて、さらに掘り下げるために、より多くの時間を割くようになっています”

– 金融サービス企業 最高情報セキュリティ責任者

テクノロジーを活用したプログラムやビジネスのDX施策にサイバーセキュリティは深く組み込まれている

DXの境界線が曖昧になっているように、サイバーセキュリティの境界線も曖昧になっています。組織がパートナーやその他のサードパーティーとデータやシステムへのアクセスを共有する場合、セキュリティとプライバシーに関する懸念が最も重要になります。結局のところ、ビジネスの成長と、顧客、データ、デジタルの信頼性はサイバーにかかっています。そのため、多くの組織では、ビジネス機能とテクノロジー機能に対して横断的にサイバーセキュリティを統合しています（図10）。

“私はいつもサイバーはイネーブラーであると考えています。高速道路を速く走りたいなら、バンパーとブレーキがあることを確認し、車内で多くの機構が正常に機能していることが分かっていなければいけません。そうでないと、道路を走り続けることはできないのです。サイバーは車を支えるバンパーやブレーキのような役割を果たします。サイバーのおかげで、インターネットのスピードで進んでいくことができるのです”

– Loblaw サイバーセキュリティ・ネットワーク・テクノロジーリスク担当シニアバイスプレジデント　Vivek Khindria

ビジネス横断でサイバーを組み込む

今や、テクノロジーの機能が強化・確立されているだけでなく、新製品を作る方法までもが変化しているのです。例えば、回答者の80%以上が製品開発の初期段階でプライバシー面の配慮を組み入れており、これによって顧客データの保護やデジタルの信頼性の向上につながっていると答えました。このような配慮は、DevSecOpsプロセスの成熟度が新たな段階に達しており、サイバーセキュリティのリーダーが製品設計・開発チームにうまく組み込まれていることを示しています（図10）。

プライバシー、信頼性、倫理の優先状況（図10）
ほとんどの回答者は、製品開発や顧客データ保護などの主要領域でのニーズにサイバーセキュリティを組み込むための対策を講じている（単位：%）

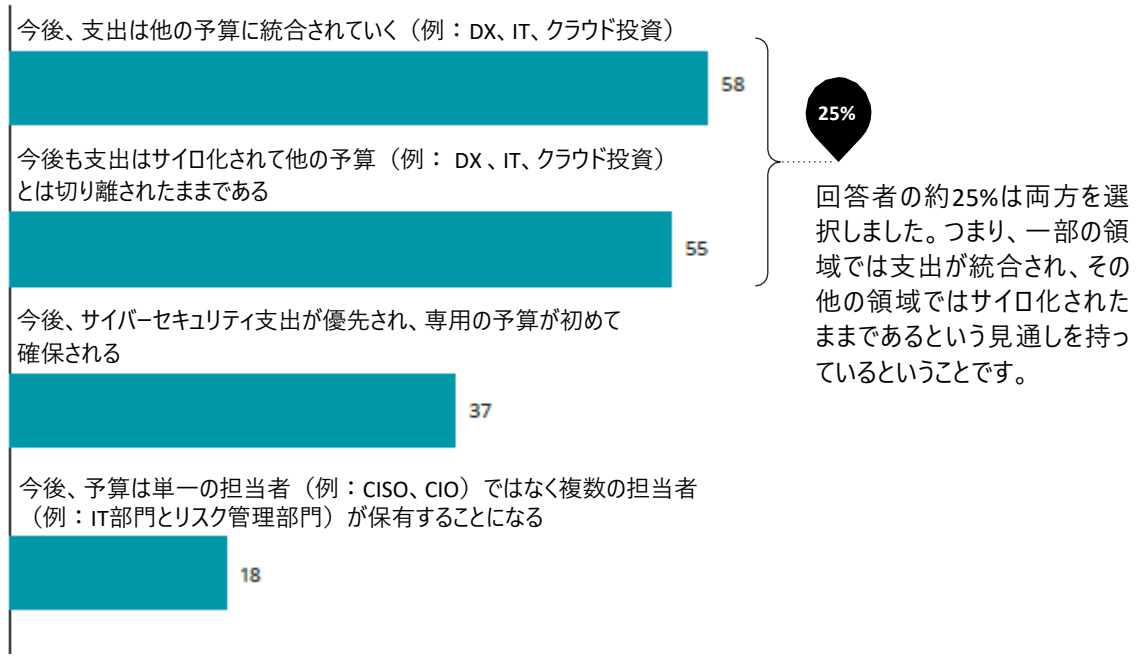
（n=1,196）

サイバーセキュリティの統合はビジネスの多くの側面に広がり、支出にも及んでいます。前述のように、回答者の過半数（58%）は、サイバーセキュリティの支出がDX施策、ITプログラム、クラウドへの投資などの他の予算と統合されると見込まれています。同時に、過半数（55%）は支出が依然としてサイロ化されたままであると見ています（図11）。

このような過半数の意見が2つ出たからといって矛盾しているわけではありません。今後のサイバーセキュリティ関連の支出に関する質問で、回答者の25%が統合された支出とサイロ化された支出の両方を選択しました。この両立状態は複数の組織で見て取れるものであり、Deloitteが組織全体で見ている現象を反映しています。サイバーセキュリティの支出は、専用のサイバーセキュリティ予算だけでなく、IT、DX施策、ビジネス分野、製品の予算からも賄われることがよくあります。つまり、サイバーセキュリティ関連の支出は多くの優先事項にまたがる規模であり、その資金調達のためにリーダーは様々なモデルを、時には並行して検討する必要があります。

サイバーセキュリティ関連の支出とDXの関係性（図11）

デジタル環境が進化することで自組織のサイバーセキュリティ関連の支出にどのような影響が出ると思うか（複数選択）（単位：%）



（n=1,196）

注記：四捨五入の関係で、それぞれの割合の合計が100%にならない場合があります。

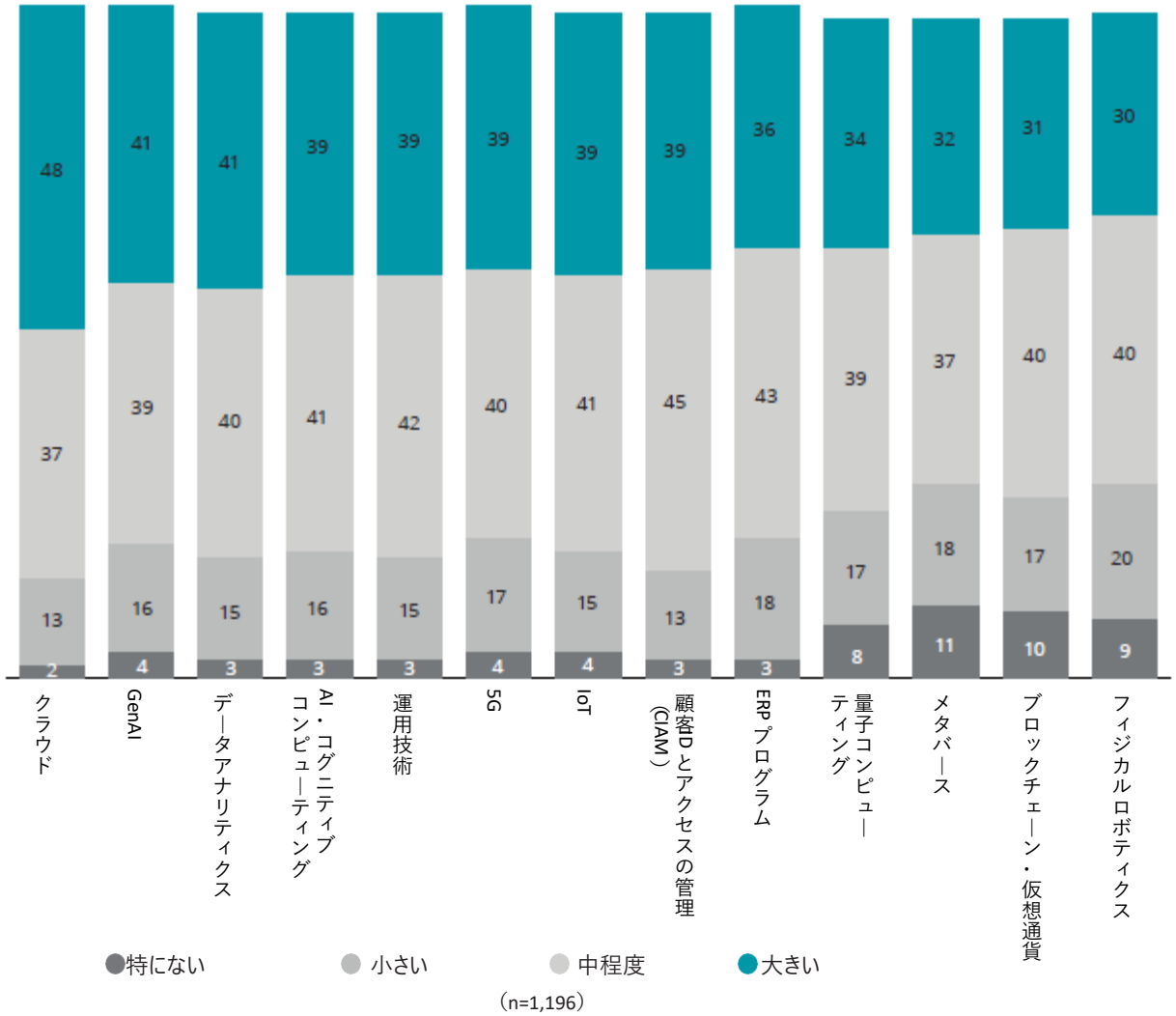
58%

サイバーセキュリティ関連の支出は他の予算と統合されていくと見込んでいます。

サイバーセキュリティ関連予算の統合に向けたこの動きは、新たに浮上してきたもう一つの現実と密接に関連しています。それは、サイバーセキュリティがビジネスの目標達成の推進力であるということです。調査結果によれば、サイバーセキュリティは組織の技術能力への投資を確保する上で大きな役割を果たしており、特にクラウド（48%）、生成AI（41%）、データ分析（41%）といった優先分野において顕著です（図12）。

セキュリティテクノロジー関連の投資確保におけるサイバーセキュリティの役割（図12）

テクノロジー機能に対する予算決定におけるサイバーセキュリティの影響度（単位：%）

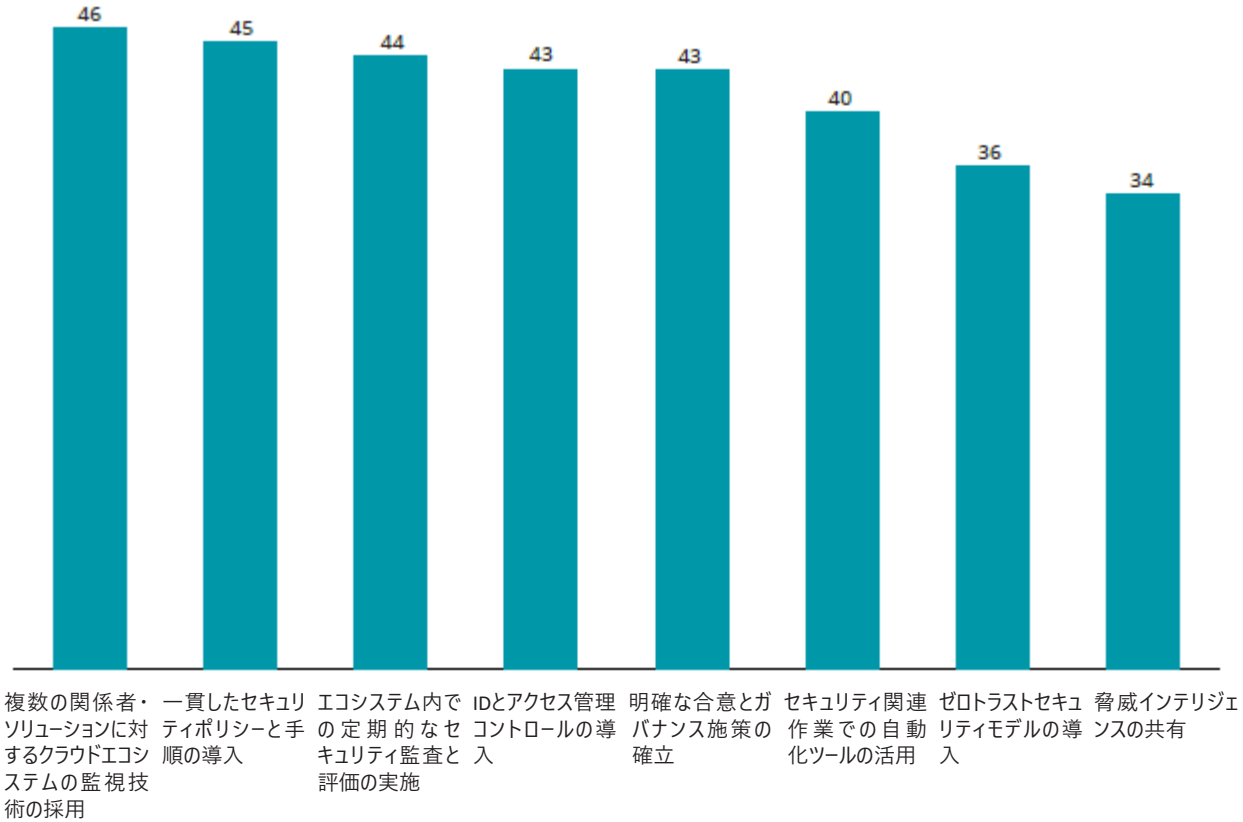


注記：四捨五入の関係で、それぞれの割合の合計が100%にならない場合があります。

> “グローバルに事業を展開する当社グループにとって、セキュリティ強化はDX施策を推進するうえで欠かせない重要な活動です。当社ではJFEセキュリティ統合対応チームという内部組織を設置し、予算や人員などのリソースを割り当て、人的・技術的・物理的な面から必要な施策を実施しています。製品・システム・サービスの開発・設計・製造・提供など、様々な事業活動におけるサイバーセキュリティ対策の強化を目指しています。その結果、サプライチェーン全体のサイバーセキュリティを強化し、最終的には社会全体のサイバーセキュリティ強化にグローバル規模での貢献しています”

– JFEスチール 最高情報セキュリティ責任者　新田哲

クラウドエコシステムの複雑さを軽減するためのサイバーセキュリティ対策（図13）
クラウドエコシステムの複雑さの軽減に向けて、どのようなサイバーセキュリティ対策を実施しているか
（単位：%）



（n=1,196）

クラウド技術に関していえば、サイバーセキュリティはイネーブラー（推進力）として重要な役割を果たし、組織全体のクラウド環境を簡素化しながらセキュリティを強化することに役立ちます。クラウドエコシステムの複雑さを軽減するために回答者が実施しているサイバーセキュリティ対策には、定期的なセキュリティ監査と評価の実施（44%）、一貫したセキュリティポリシーと手順の実装（45%）、複数の関係者・ソリューションに対するクラウドエコシステムの監視技術の導入（46%）が挙げられています（図13）。

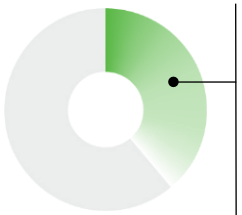
46%

クラウドエコシステムの監視技術を複数の関係者・ソリューションに対して利用していると回答しました。

AIを活用したサイバーソリューションへ注目が高まる

今回の調査第4版では、今日のAIの重要性に鑑み、サイバー成熟度の指標にAIを含めました。組織がサイバーセキュリティ能力を強化するためにAIを活用する主な方法には、デジタルインフラの監視や、高度なシミュレーション、セキュリティ対応の自動化などが挙げられます。

AIにコンテンツを生成させることで、攻撃者ははるかに少ない時間でコンテンツをカスタマイズして作成することができます。現在、AI生成コンテンツという波が企業を標的にして、信頼できる情報源を装って脆弱性を悪用しています。この問題は急速に加速しています。しかし、これが企業が人工的に生成されたコンテンツの津波に対して無力であることを意味するわけではありません。大手企業は、被害を未然に防ぐために積極的な対策を講じています（出所：デロイトのTech Trends 2024「現実を守る：合成メディアの時代における真実」）。



39%

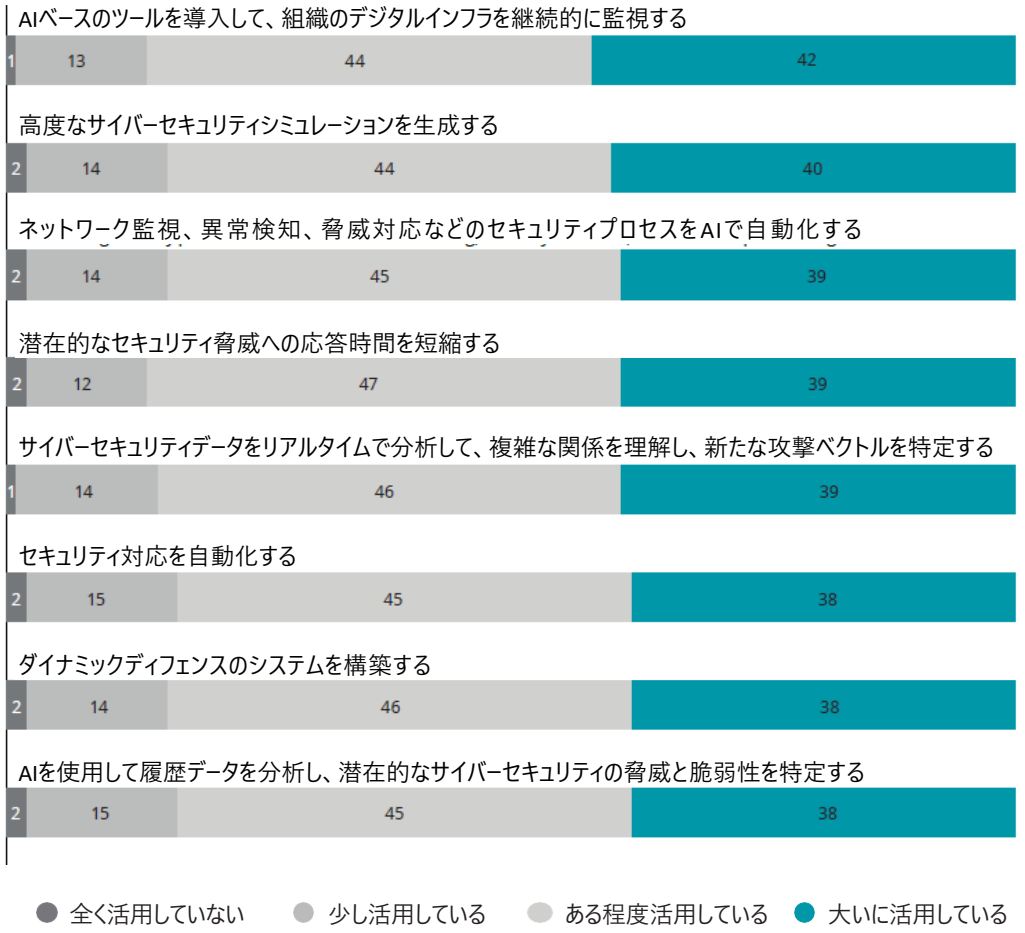
サイバーセキュリティプログラムにおいてAI機能を大いに活用していると回答しました。

このようにAIの未来が進化する一方で、サイバーセキュリティの未来も同様に進化しています。組織が新しいAIソリューションを活用してサイバーセキュリティの負担を軽減するにつれ、両者は共に進化しています。調査回答者の平均39%が、自社のサイバーセキュリティプログラムにおいてAIの機能を大いに活用しています。同時に、回答者はAIに関連する懸念も表明しており、継続的な技術革新に対応するためにサイバーセキュリティ戦略を更新する必要性を感じています（図14）。

> “もちろん、焦点は悪意のある攻撃を排除することです。しかし、AIのような新しいテクノロジーの影響と、それが私たちの状況にどう影響するのかをも考慮しなければなりません。AIを安全かつセキュアに適用し、利用できるようになるのか、どのようにAIを利用すれば自組織のサイバーフレームワーク内でセキュリティを改善できるのかを検討しなければいけません”
>
> **– 政府・公共サービス機関 サイバー・ITセキュリティ担当 事務局長**

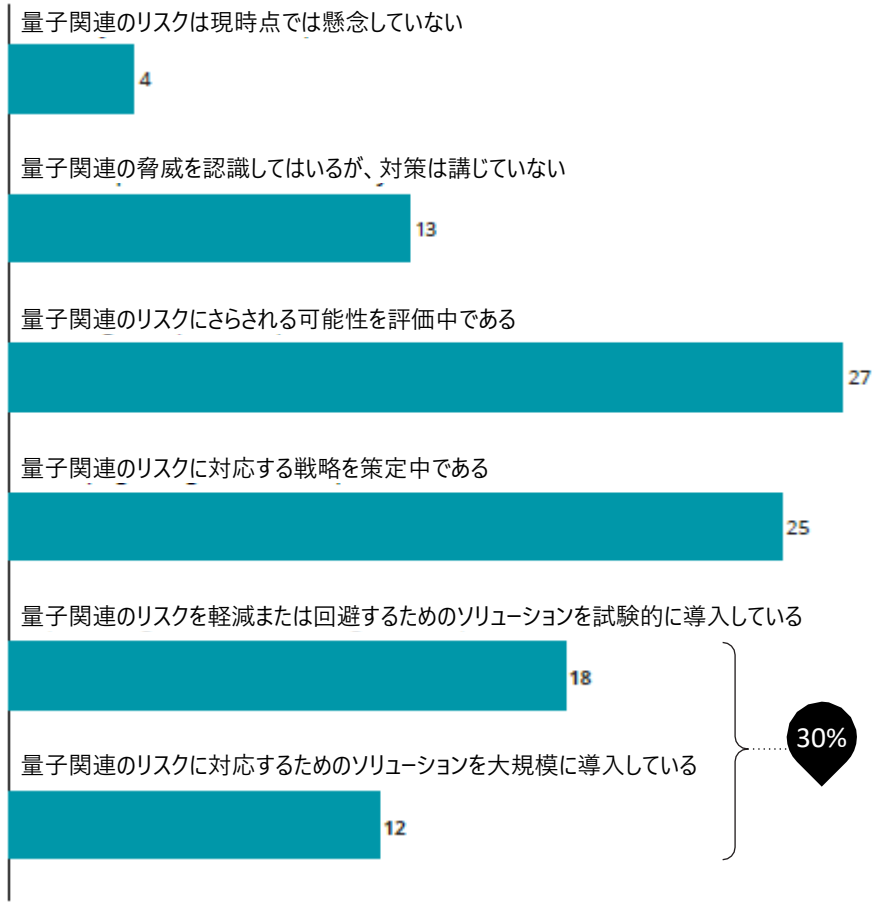
注目されているAI機能（図14）

AIはサイバーセキュリティプログラムのどの領域でどのようにツールとして活用できると見なされているか（単位：%）



（n=1,196）

量子との関連（図15）
迫りくる量子の時代について、また量子関連のサイバーセキュリティに備える必要性について（単位：%）



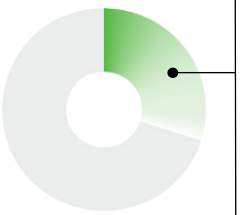
（n=1,196）

新興テクノロジーによる次の波に向けた対応

組織がAI関連するリスクと機会に対応をし続ける一方で、他のディスラプティブ・テクノロジーも進化し、普及に向けて着実に前進しています。量子コンピューティングの活用が現実に近づくにつれ、量子サイバーセキュリティの準備が多くの組織にとってますます重要となっています。量子コンピューティングは今後数年で主流になると予測されており、暗号を解くためにサイバー攻撃者が使用する強力な新しいツールを提供することになります。

今回の調査では、回答者の83%近くが量子関連のリスクを評価するか、何らかの対策を講じていると回答しました。具体的には、戦略の策定、パイロットソリューションの実施、または大規模ソリューションの実装を行っています。回答者の過半数（52%）が自社がリスクに晒される可能性を評価し、量子関連のリスク戦略を開発している段階ですが、その他の回答者（30%）は、ソリューションの早期導入を始めています。

これらの数字は、この問題に対する明確な機運の高まりを示しています。リーダーはリスクの可能性を理解し、データとシステムのガバナンスを見直し、業務関連の脆弱性に優先順位を付け、暗号アルゴリズムの更新に対応するロードマップを策定することで、この課題に先行する対応が可能になります。これにより、複数年にわたる取り組みを先取りし、より広範な企業変革にわたって新しいアルゴリズムを適切な手順で、契約構造の更新を通じて、導入できるようになります。



30%
ソリューションの早期導入を始めています。

サイバー成熟度が高い組織ほど、自信もあり、サイバー活動と投資を通して大きなメリットを実現できる

サイバー成熟度指数

世界中にある数多くの組織と協力してきた経験をもとに、回答者をサイバー成熟度が高い組織、中程度の組織、低い組織に区分しました。

サイバーにおける先駆者である組織を明確に識別し、サイバーセキュリティがビジネスの成功と価値をどの程度支えているかをより深く理解するため、次の4つの先進的手法に基づく組織評価を指数化しました。

- **効果的なサイバーセキュリティ計画：**サイバー脅威に対する防衛・対応のための戦略的、運用的、戦術的な計画がある（計画戦略の全リストは11ページの図3を参照）。
- **重要なサイバーセキュリティ活動：**定性的・定量的なリスク評価、業界ベンチマーキング、インシデント対応シナリオの策定などの活動を実施している（10ページの図2を参照）。
- **取締役会の効果的な関与：**取締役会が定期的にサイバー関連の問題に対処しているなどの取り組みをしている。
- **サイバーセキュリティプログラムへのAI機能の導入：**サイバーセキュリティとAIに関する8つの対策のうち少なくとも5つを大規模に実施している（対策の全リストは23ページの図14を参照）。

AI機能に関するこの最後の基準は、技術とビジネスの進化、そしてサイバー成熟度の意義を反映するために、今回の調査では新たに追加されました。他の3つの基準（前回使用したのと同じ指標）のみを使用すると、サイバー成熟度が高い組織の割合は21%から24%へと3ポイント増加します。これは有望な成長です。

しかし、今回のサイバー成熟度指標にAIという要素を含めることで、サイバーの未来を形作る最前線にいるエリート組織の集団を定義することができます。

今回の調査では、サイバー成熟度の高い組織は調査対象全体の14%でした。これらの組織とサイバー成熟度が中・低程度の組織ではサイバーセキュリティへのアプローチが異なる点は、組織のリーダーが自社のサイバーレベルやビジネスの価値を向上させるために役立つ重要な教訓となります。

サイバーセキュリティの機能への期待は高まり続けている

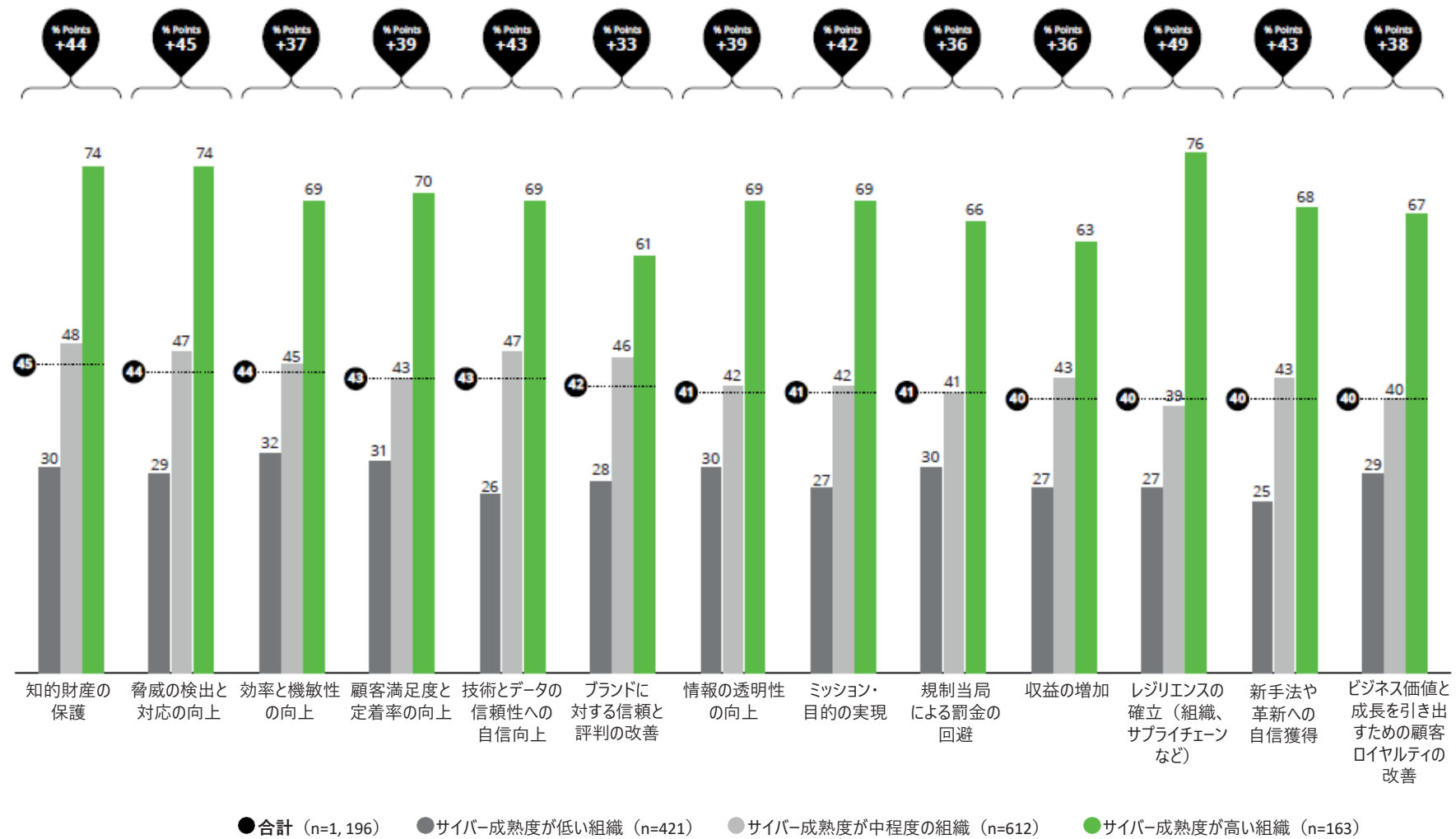
サイバー成熟度の高い組織の回答者は、サイバーセキュリティ対策から得られる潜在的なメリットに非常に敏感です。平均して、サイバーマチュリティの高い組織の回答者は、サイバーマチュリティの低い組織の回答者に比べて2.4倍（中程度のサイバー成熟度の組織の回答者に比べて1.6倍）、サイバーセキュリティ対策からの肯定的な結果を期待しています（図16）。

サイバーセキュリティ対策のメリットには、レジリエンスの確立（76%）、脅威の検出と対応の向上（74%）、知的財産の保護（74%）などがあります。この3つの領域ではサイバー成熟度が高い組織の回答者が期待することは、サイバー成熟度が低い組織の回答者と比較して大きく異なっています。

この状況は、サイバーの課題と可能性の両方を示しています。最もサイバー成熟度の高い組織は、全ての対策に対してかなり高い期待を有しています。サイバーセキュリティが果たすべき重要な役割を認識していますが、その認識が正しい対策をとるためのプレッシャーを一層強めています。

サイバーセキュリティがもたらす成果（図16）

組織がサイバーセキュリティの取り組みに対して期待しているメリット（単位：サイバー成熟度に応じた3つのグループそれぞれの中での割合）



脅威の検知と対応へのアプローチは進化を続けている

サイバー侵害やインシデントの悪影響から免れる組織はありません。サイバー成熟度の高い組織であっても同様です。平均して、サイバー成熟度の高い組織はサイバー脅威を検出する能力が高く、それに対応した報告要件の順守度も高いことが今回の分析で明らかになりました。例えば、サイバー成熟度が高い組織の回答者の25%は、過去1年間で11件以上のサイバーセキュリティインシデントを報告しており、これは回答者全体よりも8ポイント高い値です。一見するとこれはネガティブのように思えますが、これらの組織はより強力な脅威検出能力を持っており、脅威をより効果的に特定して対応することができるのかもしれません。

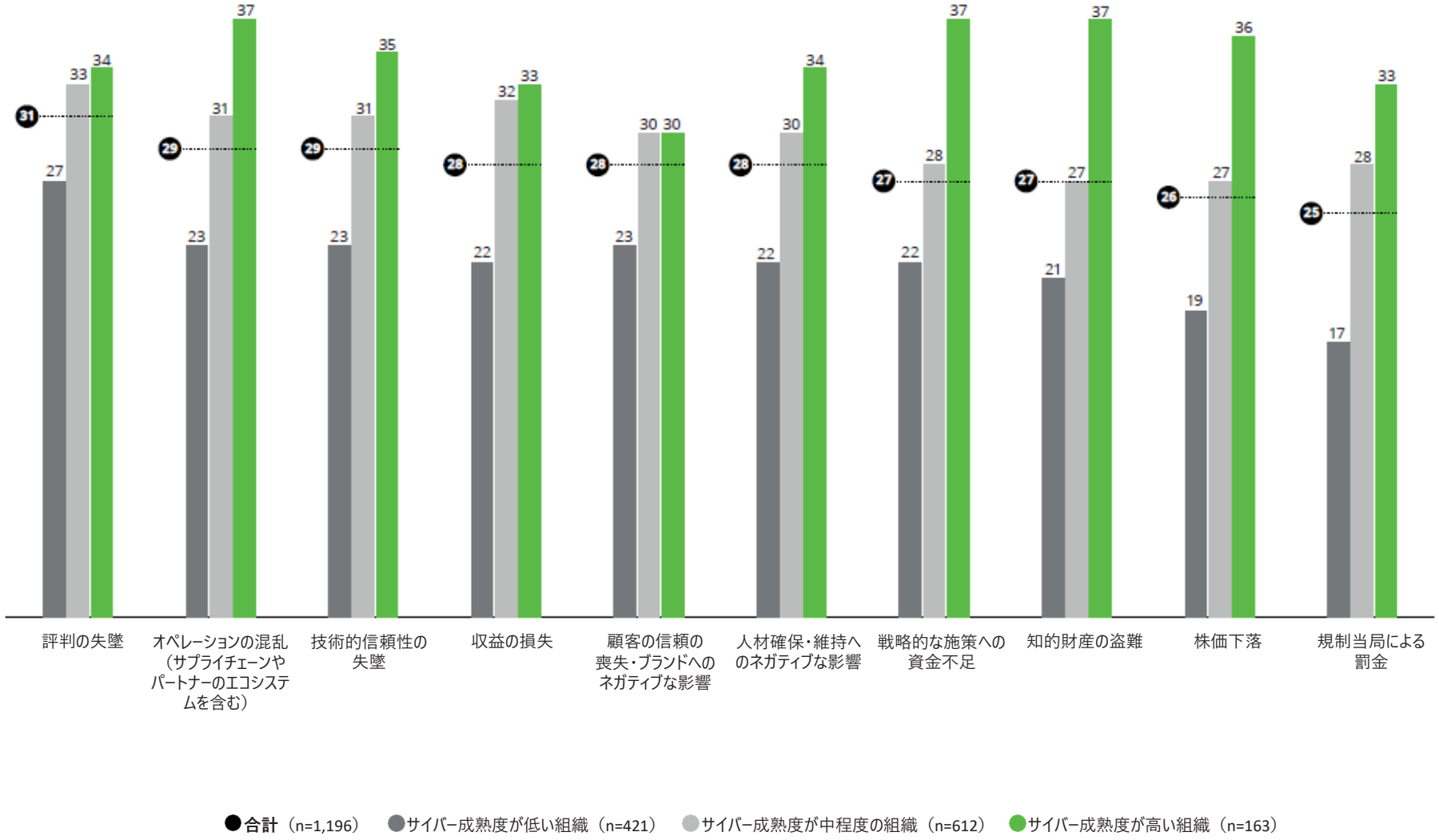
サイバー成熟度が高い組織は、侵害やインシデントに対する意識が高いだけでなく、それに伴う真のコストについても理解しています。また、サイバー成熟度の高いグループは、その他のグループよりも、財務、業務、ブランドでの影響の程度を認識している傾向が平均13ポイント高くなっています。

この理解度の高さは、ビジネスとその技術環境全体にわたるサイバーセキュリティの統合を成長させる取り組みが促進されるという好循環にあることを反映しています。また、CISOの役割を高め、将来的な価値の維持と保護、運用効率とレジリエンスを向上させ、イノベーションと収益増加に関する目標をサポートすることにも寄与します。

成熟度グループ別 予想される悪影響（図17）

サイバー成熟度が高い組織ではサイバーセキュリティインシデント発生数が多いが、これは脅威検出能力が高いことが一因である可能性がある

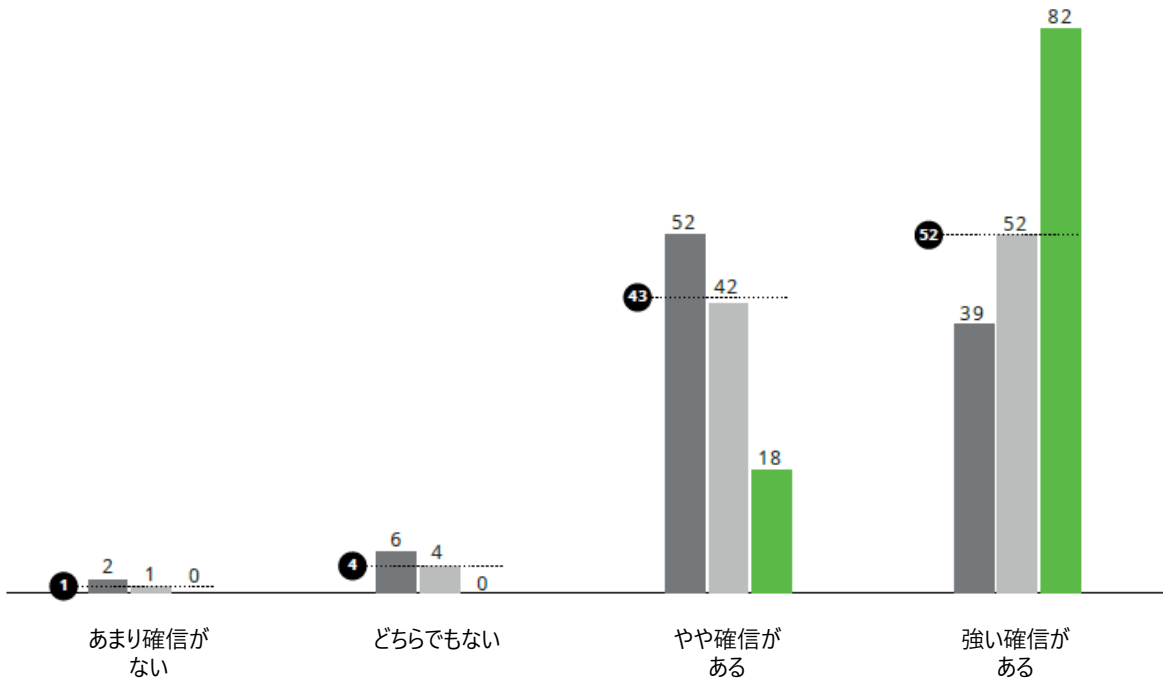
（単位：%）



経営幹部のサイバー対応能力に対する信頼の醸成

サイバー成熟度が高い組織の回答者は、経営幹部に対する高い信頼を示しています。経営幹部や取締役会がサイバーセキュリティのニーズに効果的に対応できる能力を有しているかという質問に強い確信があると答えた割合は、サイバー成熟度の低い組織の回答者の2倍です（図18）。

経営幹部への信頼度（図18）
経営幹部や取締役会のサイバーセキュリティ対応力についての信頼度
（単位：サイバー成熟度に応じた3つのグループそれぞれの中での割合）



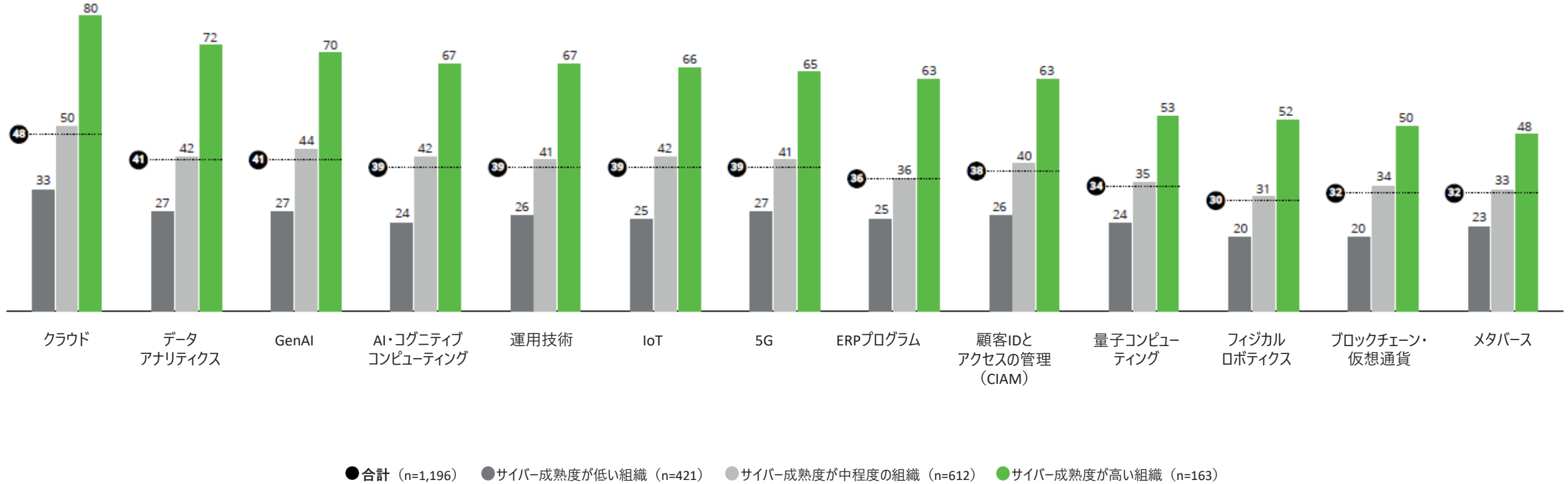
●**合計**（n=1,196）●サイバー成熟度が低い組織（n=421）●サイバー成熟度が中程度の組織（n=612）●サイバー成熟度が高い組織（n=163）

サイバー成熟度の高い組織は、サイバーセキュリティを活用してテクノロジーの機能に対する投資を確保し、DX施策に関する戦略的な議論にCISOを関与させることに長けているようです。

テクノロジーの機能に対する投資を確保するうえでサイバーセキュリティが大きな役割を果たしていると回答した割合は、サイバー成熟度が高い組織の回答者のほうが成熟度が低い組織の回答者よりも平均で2.5倍高くなっています。投資を確保している主な分野には、クラウド、データアナリティクス、GenAI、運用技術（例えば産業用制御システム）、AI・コグニティブコンピューティングがあります（図19）。

成熟度が高い組織ほど、テクノロジーを活用した機能においてサイバーセキュリティが果たす役割が大きい（図19）

サイバー成熟度が高いグループは他のグループよりも、テクノロジーの機能に対する投資を確保する際にサイバーセキュリティが大きな役割を果たしていると考えている（単位：サイバー成熟度に応じた3つのグループそれぞれの中での割合）



テクノロジーの機能に関する戦略的な議論にCISOやサイバーセキュリティ担当リーダーが関与することが大幅に増加したと回答した割合は、サイバー成熟度が高い組織はサイバー成熟度が低い組織より2.3倍高くなりました。サイバー成熟度の高い組織では、CISOの関与度が高い分野は、クラウド、AI・コグニティブコンピューティング、IoT、GenAI、データアナリティクスです（図20）。

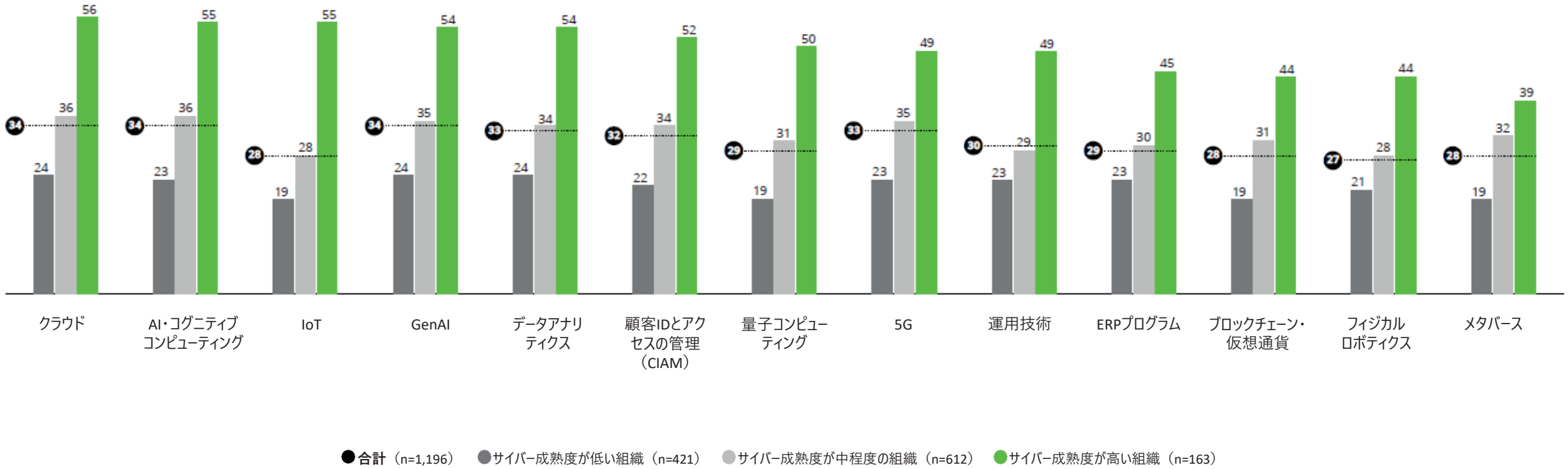
“CISOの役割は進化しています。データに基づいた意思決定を積極的に促進するために適切な戦略を導入する必要があります。それには経営幹部との連携の強化が必要となるため、CISOは技術に習熟しているだけでなく、経営幹部レベルの考え方とビジネスに対する洞察力を持って業務に携わり、サイバー戦略がビジネスにどんな影響を与えるかを示していく必要があります”

– Johnson & Johnson 最高情報セキュリティ責任者 Gary Harbison

サイバー成熟度の高い組織では、戦略的な議論にCISOを関与させる割合が高い（図20）

サイバー成熟度が高い組織では、CISOがあらゆる分野で頻繁に議論に参加するようになってきている

（単位：%）



サイバーの未来を切り開くためのインサイト

組織全体でサイバーセキュリティを向上

サイバーの未来において組織が成功するには、新たなトレンドを理解してそれに対応すること、そして最も重要なのは、実際にアクションを起こして目に見える影響をビジネスにもたらすことです。以下に挙げるいくつかのポイントや考えられる道筋に焦点を当てることで、サイバー成熟度向上を促進し、他社に先んじた対応が可能になります。

サイバーを必須課題として認識し、つながりと連携を促進し、レジリエンスを高める

戦略的なビジネス価値の一要素としてサイバーセキュリティが注目される中、これは単なるITの問題ではないことをリーダーは認識する必要があります。サイバーセキュリティは、組織の全ての機能と階層にわたって組み込む必要があるビジネスクリティカルな問題です。そのためには、ビジネスと技術的運用の中で優先順位を付け、サイバーのつながりを構築することを継続していく能力が必要になります。

組織がリーダーシップを強化して確立し、サイバーのつながりを強化すると、ビジネスニーズとサイバーセキュリティとの関わりが生じる局面で連携、情報共有、意思決定を強化することができます。このように対応することで、リーダーはビジネスの現状に関する情報を十分把握してビジネス目標との整合を保ちつつ、サイバーリスクについても効果的な軽減を考慮したうえで戦略的意思決定ができるようになります。最終的には、サイバーセキュリティを優先事項とし、組織全体でサイバーセキュリティのつながりを強化することで、重要な資産と評判をより適切に保護し、デジタル化が進む世界で全体的なレジリエンスを向上させることができます。

CISOの役割は、かつては企業のITにおけるセキュリティ管理のリード役と見なされていました。しかし現在では、イノベーションとビジネスの将来をサポートしながら、コアとなる業務運用からブランドの評判まで、企業全体を保護する役割へと**進化しています。**

CISOからその他の経営幹部や取締役会に至るまで、リーダーの関与と知識を高める

サイバーの未来に向けた明確な命題は、CISOがテクノロジーの機能とビジネスについての戦略的な議論に積極的に関与できるようにすることが必要なことは明白です。CISOの役割は、かつては企業のITにおけるセキュリティ管理のリード役と見なされていました。しかし現在では、イノベーションとビジネスの将来をサポートしながら、コアとなる業務運用からブランドの評判まで、企業全体を保護する役割へと進化しています。

また、CISOだけでなく、サイバーに精通した経営幹部からの協力も得るべきです。ビジネス目標を考慮しつつサイバーセキュリティのリスクに効果的に対処するには、経営幹部と取締役会が定期的にサイバーセキュリティに関する議論に参加する必要があります。サイバーセキュリティは組織にとって最大のリスクであるため、経営幹部はその管理と監視に深く関与し続ける必要があります。CISOと経営陣が協力してサイバーセキュリティに取り組むことで、サイバーセキュリティは単なる技術的な問題ではなく、戦略的なビジネス課題として適切に認識され、関心と必要なリソースが得られるようになります。これにより、企業はサイバーリスクに対してより強固な防御を築き、ビジネスの持続的な成長と成功を実現できます。

戦略とガバナンスに立脚して予算の統合に意図的に取り組む

サイバーセキュリティ予算が他のDX投資と統合される傾向であることは重要なことです。これはサイバーセキュリティが適切に評価をされるようになっていることを示し、今後はより多くの部門が資金計画にサイバーセキュリティを含める可能性を示唆しています。

こうした統合の動きは、より包括的な戦略の策定と全体的なセキュリティの向上につながる可能性があります。より広範なアジェンダに対応してサイバーセキュリティの目標を定める明確なガバナンスフレームワークを確立することで、ビジネス目標達成に向けた重要な一歩を踏み出すことができます。このようなアプローチは、組織内の全員がサイバーセキュリティの重要性を理解し、適切な投資が約束され、共通の目標に向けた取り組みが行われているということでもあります。

効果的なガバナンスを組織内に確立することで、サイバーセキュリティ施策と他の重要なビジネス上の優先事項の間で整合をとることができます。しかし、このように変革に向けた投資を統合することが問題になる可能性があります。サイバーセキュリティが予算の一項目として明確に記載されていない場合、「価値を高めるための投資」ではなく、「コストの一部」として扱われるため、削減されてしまうかもしれないということです。

> “戦略に関して私たちが成熟させていることの一つは、結果から始めるということです。つまり、数年後にどうなっていたいかを常に考えることです。さらに、2年以上先のセキュリティ戦略を立案する必要があると思っています。脅威もテクノロジーも様々な変化が起こり、大きな変革が必要になるからです。そのため、調査結果を念頭に置いて戦略を構築することをお勧めしております。これは非常に重要なこととなっております“
>
> **– ライフサイエンス・ヘルスケア組織 最高情報セキュリティ責任者**

価値ある未来に向けて

サイバーの未来はまさしく今、刻々と描かれている最中です。新たなリスク、新たなテクノロジー、ビジネス上の新たな選択肢が姿を現しつつあります。それらに対してどのように備え行動するかによって、サイバー成熟度およびビジネスの将来が決まるのです。

サイバーセキュリティの役割に対する企業の認識が高まり、経営幹部がサイバーセキュリティに関する戦略的な議論に積極的に関与するようになり、サイバーセキュリティが変革の目標達成にとっていっそう不可欠なものになってきている現在、新しい局面が開かれつつあります。次に現れる変化をどのように活用するか、あるいは、それをどのようにビジネスに役立てるかを常に検討している必要があります。

さあ、始めましょう

このGlobal Future of Cyber Survey第4版から得られるインサイトのさらなる詳細や、サイバー成熟度が最も高い組織がビジネス価値を高めて他社との差別化を図るために実施している他の取り組みにご興味がございましたら、お問い合わせください。

作成協力者

Saurabh Bansode、Criss Bradbury、Deborah Elder、John Gelinne、Tanneasha Gordon、Matt Holt、Pratik Joshi、Diana Kearns-Manolatos、Isaac Kohn、Daphne Lucas、Mike Morris、Kelly Nelson、Iram Parveen、Sean Peasley、Abdul Rahman、Colin Soutar、Jan Vanhaecht、Marius von Spreti

連絡先

Emily Mossburg
Deloitte Global Cyber Leader
Principal, Deloitte & Touche LLP
emossburg@deloitte.com
+1 571 766 7048

Adnan Amjad
US Cyber Leader
Partner, Deloitte & Touche LLP
aamjad@deloitte.com
+1 713 982 4825

Amir Belkhelladi
Canada Cyber Leader
Partner, Deloitte Canada
abelkhelladi@deloitte.ca
+1 514 393 7035

Ian Blatchford
Asia Pacific Cyber Leader
Partner, Deloitte Australia
iblatchford@deloitte.com
+61 474 288 278

Xavier Gracia
Spain Cyber Leader
Partner, Deloitte Spain
xgracia@deloitte.es
+34 931697257

Andre Gargaro
Brazil Cyber Leader
Partner, Deloitte Brazil
agargaro@deloitte.com
+55 11 5186 6213

Yuichiro Kirihara
Japan Cyber Leader
Partner, Deloitte Japan
ykirihara@tohmatsu.co.jp
+81 803 3672805

Pedro Parra
S-LATAM Cyber Leader
Partner, Deloitte Mexico
peparra@deloittemx.com
+52 55 89785689

Niels van de Vorle
North and South Europe Cyber Leader
Partner, Deloitte Netherlands
nvandevorle@deloitte.nl
+31 88 2882186

Peter Wirnsperger
Central Europe Cyber Leader
Partner, Deloitte Germany
pwinsperger@deloitte.de
+49 40 320804675

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーであるデロイト トーマツ合同会社ならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ リスクアドバイザリー合同会社、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人、DT弁護士法人およびデロイト トーマツ グループ合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザリー、コンサルティング、ファイナンシャルアドバイザリー、税務、法務等を提供しています。また、国内約30都市に約2万人の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト、www.deloitte.com/jpをご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザリー、リスクアドバイザリー、税務・法務などに関連する最先端のサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促し、より豊かな経済、公正な社会、持続可能な世界の実現に向けて自ら率先して取り組むことを通じて、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来175年余りの歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの45万人超の人材の活動の詳細については、www.deloitte.comをご覧ください。

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
http://www.bsigroup.com/clientDirectory

Member of
Deloitte Touche Tohmatsu Limited