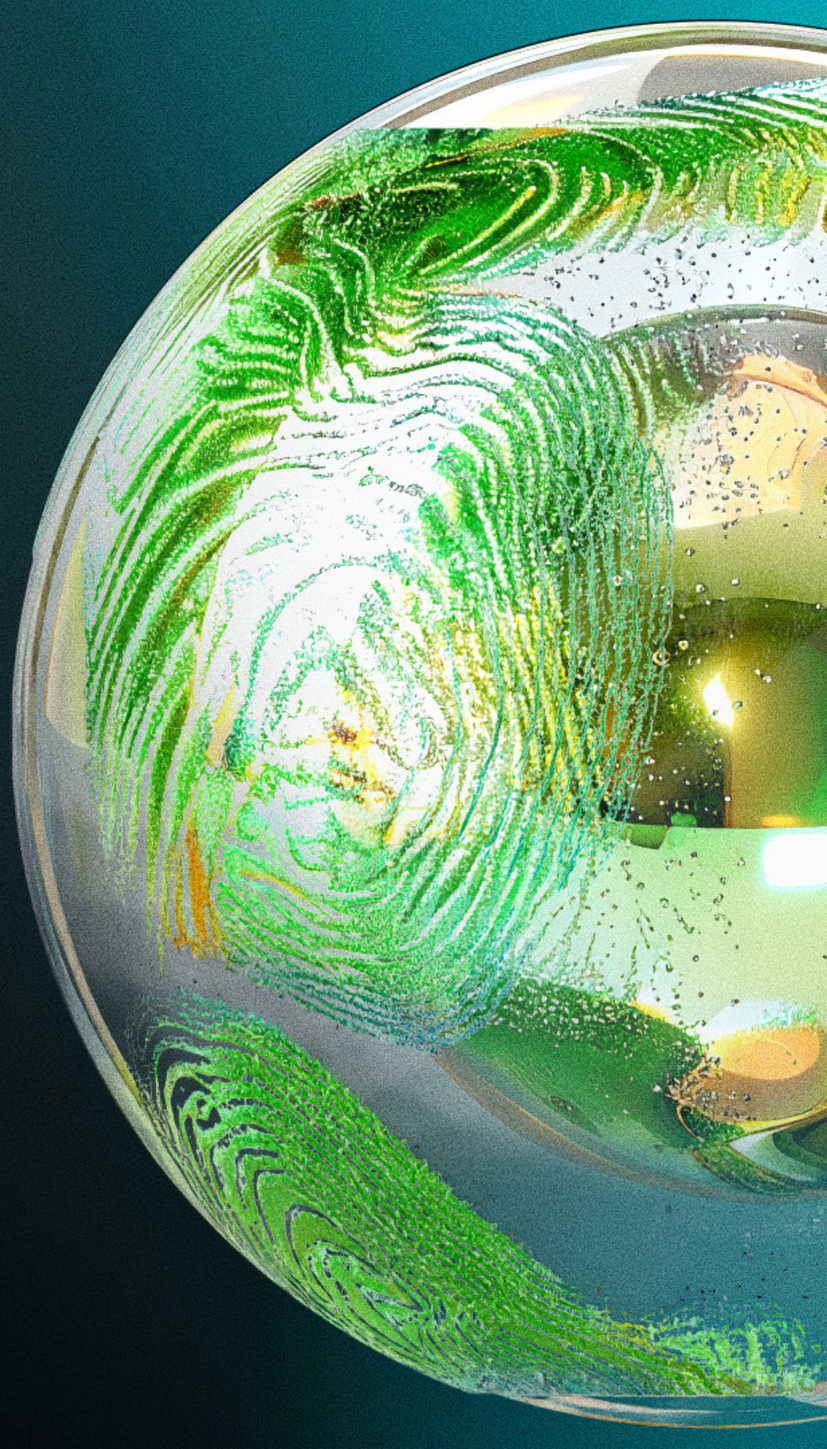
Deloitte.
デロイト トーマツ
Together makes progress

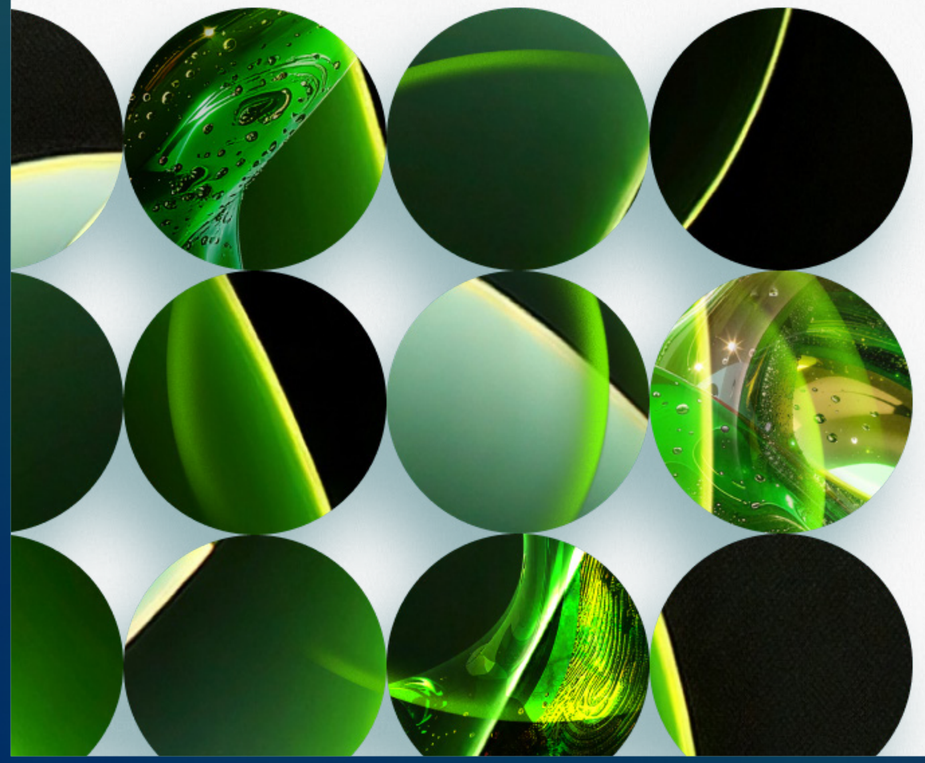
THE GLOBAL FUTURE OF CYBER SURVEY, 5TH EDITION

サイバーの未来を形作る 5つのパラドックス

サイバー戦略に潜む矛盾をどう解いていくのか
先進企業のリーダーが実践するアプローチ



進化と
パラドックス



Deloitteでは本調査を長年にわたり実施し、事業環境が一段と厳しさを増す中で、サイバー対処能力が着実に進化していることを確認してきました。脅威に関する状況もこの数年で大きく変化してきました。しかし、調査回答者はこれまでのところ、経営層の支援および予算措置を背景に冷静な対応を維持し、増大するサイバーリスクに対する防御に成功しています。

今年の調査では、世界のサイバー分野およびビジネス分野のリーダー1,000人超の見解を分析し、現在の事業環境と今後の展望をどのように捉えているかを分析しました。今回確認されたのは、複数の重要なパラドックスの存在が明らかになりました。一見すると相反して見えるデータであっても、詳細な分析を通じて、サイバー分野の意思決定者が直面する課題や、複雑かつ変化の激しい市場環境への対応状況について、より深く有用な示唆を得ることができます。

2025年後半に実施したサイバーセキュリティの分野の調査において、一見するとパラドックスのような要素や矛盾しているように見える傾向が確認されたとしても、それ自体はは必ずしも意外なことではありません。ここ数年は変化（脅威の状況だけでなく、サイバー戦の攻撃と防御の双方で使用されるツールやテクノロジーなど）が非常に大きかったため、戦略レベルと実行レベルの間に乖離が生じることは、ある程度避けられなかったと考えられます。

こうしたパラドックスにはその発生要因の如何を問わず、組織のサイバー戦略に一定の責務を担っている担当者が慎重に検討すべき重要な示唆が含まれています。そこには早急に是正すべき弱点や対応上のギャップが表れている可能性があるためです。

次ページ以降の内容では、調査にご協力いただいた調査回答者のデータに基づく洞察と、Deloitteが実施した詳細な市場インタビューおよびDeloitteのグローバルなサイバーセキュリティ領域に関する豊富な知見を踏まえた、将来志向の考察についてご紹介します。

本レポートの洞察が、皆さんのサイバー施策に役立つことを願っています。ぜひご一読ください。

Emily Mossburg
Deloitte Global Cyber Leader

サイバーセキュリティにおける フロントランナー企業の差別化要因

サイバー市場がどのように変化しているのか、また組織が将来に向けてどのような計画を進めているかを調査していく際に、Deloitteは特に、優れたリーダーに見られる特徴に注目してきました。過去の本レポートにおいては、調査データに基づき、所定のサイバー関連施策を効果的に実行している組織を特定・可視化するDeloitte独自のサイバー成熟度指数が主要な特徴の一つとなってきました。こうした先進的な組織の知見や行動、実践は、他の組織がサイバー対応力を迅速かつ効果的に高めるうえで有益な示唆となり、既に顕在化した課題や停滞要因を回避するうえでも重要な示標となります。

これまで本レポートでは、組織のリスク低減を目的として主要なサイバープログラム要素を最も多く取り入れ、あわせてAIへの継続的な注力を維持している組織を、リーダー企業と定義してきました。今や、これらの要素はサイバーセキュリティを重視するあらゆる組織にとって、備えていて当然の要件となっています。このように市場における基準水準が変化した現在、リーダーに必要な条件を捉え直す観点から、得られた発見を踏まえてデータを分析し、新たな評価フレームを策定しました。

今回の最新調査では、調査回答者が自社のサイバー対応能力に対する自信と、今後想定されるサイバー上の課題に関する備える実際の準備度との間に乖離があることが明らかになりました。こうした状況を踏まえ、先進的な取り組みの導入度合いに基づき調査回答者のサイバー成熟度を評価・類型化する当社独自の指標を見直し、発展させました。更新した指標により、サイバーに対する自信と将来への備え併せ持つ調査回答者に着目し、その隔たりを着実に解消するために実行されている施策を検証・理解することが可能となりました。

本レポートは、自信と備えの水準に基づき、調査回答者を3つのグループに整理しています。フロントランナー企業のグループは、サイバーに対する自信と将来への備えの双方に関する設問において、総じて最高水準の評価を示しています。これに対し、評価が相対的に低い調査回答者は、その水準に応じて「フォロワー」企業のグループ、次に「基盤ビルダー」の企業グループとしました[1]。

フロントランナー企業	フォロワー企業	基盤ビルダー企業
17%	60%	24%

調査回答者の分類方法の詳細については、本レポート末尾の「調査方法」のセクションを参照してください。

5つのパラドックス

フロントランナー企業は、重要な関係者との連携強化が進むとともに、サイバー戦略を経営上層部による意思決定への定着も大きく進展しています。一方で、ここで特定した5つのパラドックスは、相反する要因がサイバー対応の準備態勢、実行力、プラットフォーム戦略、成果創出、安定性を阻害し得ることを示唆しています。その影響は、現在にとどまらず将来にも及ぶ可能性があります。

[1] 四捨五入しているため合計が100%にならない場合がありますが、エラーではありません。

パラドックス ＃1

サイバーセキュリティへの自信はある。
しかし、組織の準備は本当に万全か？

サイバー領域のリーダー企業は大きく前進し、自信を付けている

Deloitteの前回のレポートでは、サイバー対処能力とサイバー成熟度が向上していることが明らかになりました。調査回答者は総じて、最高情報セキュリティ責任者（CISO）の役割が組織内で十分に定着して成熟段階に進みつつあり、サイバー戦略が組織の幅広い領域に統合され、経営幹部の間でもサイバー戦略が実際の事業価値の創出に果たす役割への理解が深まり、さらに前向きな事業成果の実現に向けた意識も高まっていると回答しました。

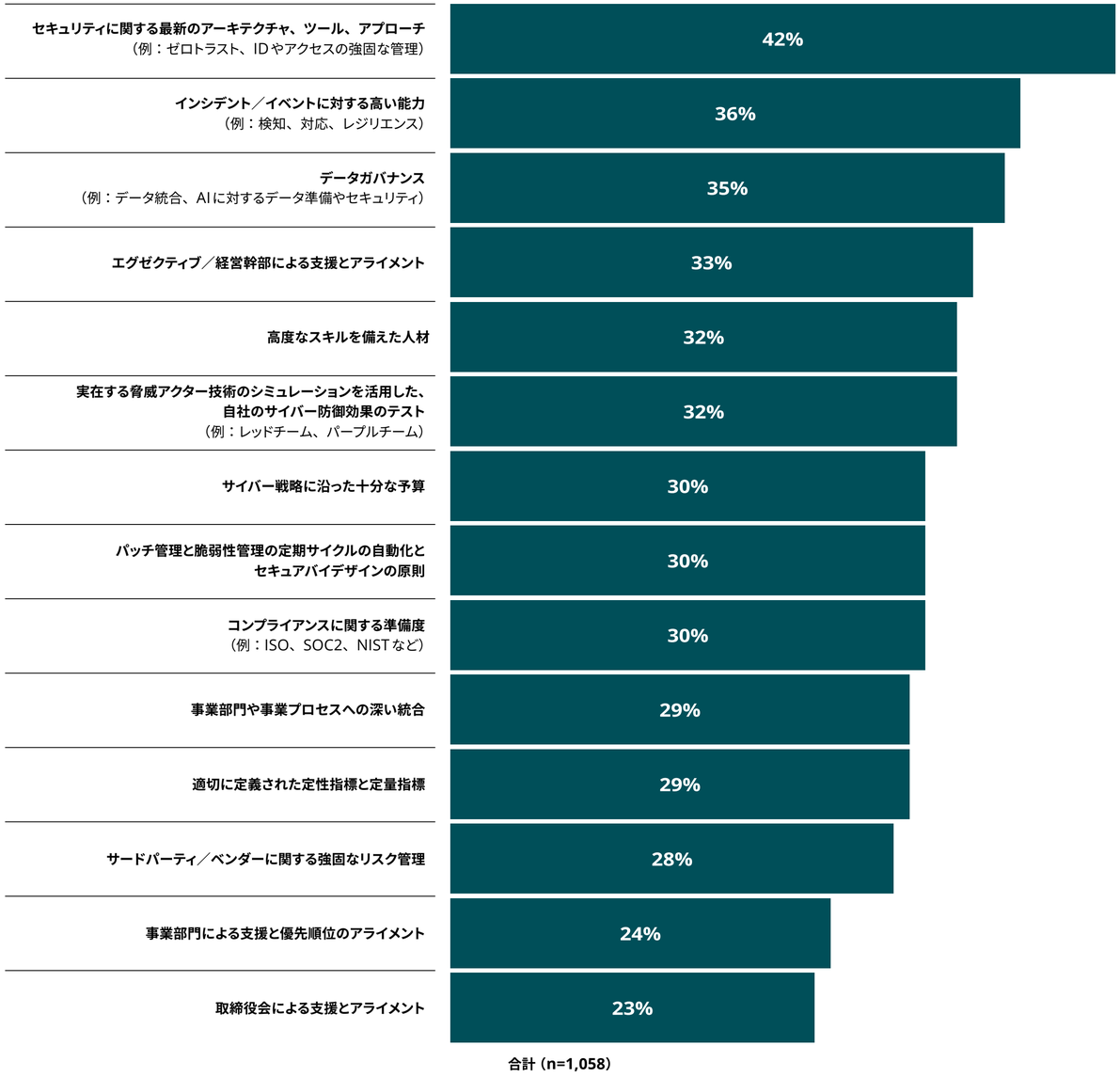
今回の調査では、調査回答者の85%が自社のサイバーセキュリティ戦略に一定以上の自信を示しておりと述べました。その理由として、「最新のセキュリティアーキテクチャ」、「高いインシデント対応能力」、「データガバナンス」などが挙げられています（右図参照）。

また、調査回答者は経営幹部から強い支援を受けており、先行対応に必要な予算を確保しやすいと回答しています。このような支援は、サイバーが事業運営のサイクルに統合されつつあることからも確認できます。調査回答者の54%が、サイバーを自社の事業・テクノロジー戦略計画に組み込んでいる、あるいは将来を見据えた戦略にサイバー要件として反映させる取り組みを進めているとしています。

調査回答者が自信を持つ理由は少なくはありません。一方で、その自信が実態以上に高い可能性も否定できません。

組織のサイバー戦略への自信を高めた主な要因

Q：現在、貴組織のサイバー戦略に最も大きく寄与している要因は、以下のうちどれですか。



組織が将来の脅威に十分備えられていない可能性については、依然として懸念が残っている

調査回答者のサイバーセキュリティに対する準備度を把握するため、サイバーセキュリティ関連の施策一覧を提示して、それぞれの施策が各組織でどの程度導入・実施されているかを確認しました。

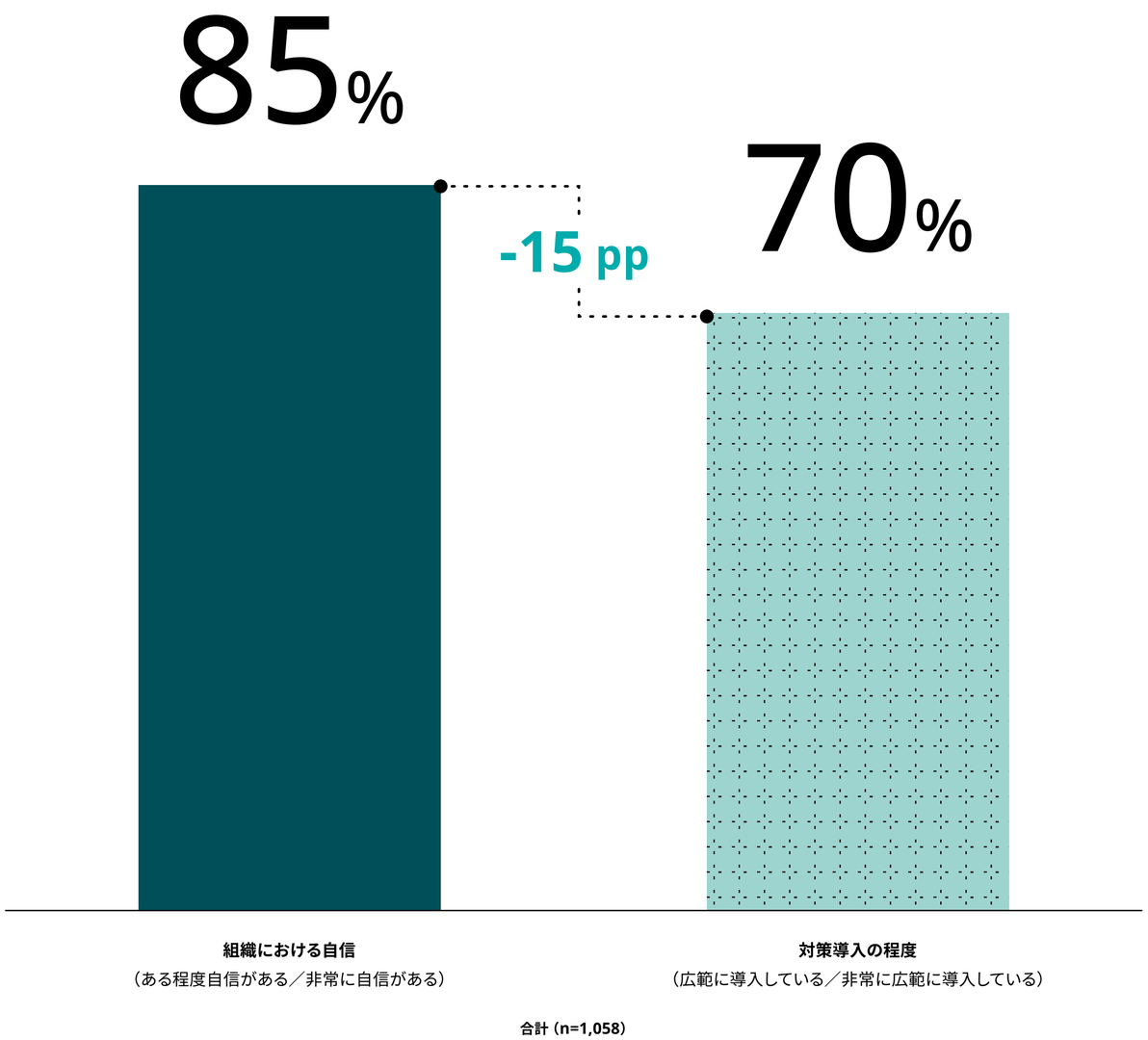
平均して調査回答者の70%が、リストにある全ての対策を「広範に導入／非常に広範に導入」しており、準備度が高いことが伺えます。しかしこの結果と、サイバーセキュリティ戦略の導入に関する自信の程度を測定した調査データとの間には、顕著なギャップがあることが明らかになりました。セキュリティ対策導入よりも組織のサイバー戦略に関する自信のほうが平均で15ポイント高い結果になりました。

「自社では、十分な投資が行われており、必要なリーダーシップも発揮されています。また、適切なツールとプロセスもあります」と、あるヘルスケア企業のCISOは述べます。「しかし、どの大企業でもいえることですが、内在するリスクと脅威環境に対する理解力に自信を持つことと、万全を期しているから深刻なインシデントは発生しようがないと断言できることは別物です」。

自信と準備度のギャップ

サイバーセキュリティ対策導入の程度

Qa：貴組織が導入している以下のサイバーセキュリティ戦略について、どの程度自信がありますか（全回答平均）。
Qb：貴組織は、以下のサイバーセキュリティ対策をどの程度導入していますか（全回答平均）。



調査回答者の組織では、取締役会レベルからの支援と必要な資金を確保しており、これまで自組織が積み重ねてきた取り組みに対して自信を示しています。将来の脅威や課題への備えを進めているにもかかわらず、なぜサイバー準備度がさらに高く評価されていないのでしょうか。その要因を考える上で、以下の４つの調査結果が特に理由を読み解くヒントとなります。

ビジネス連携が不十分である

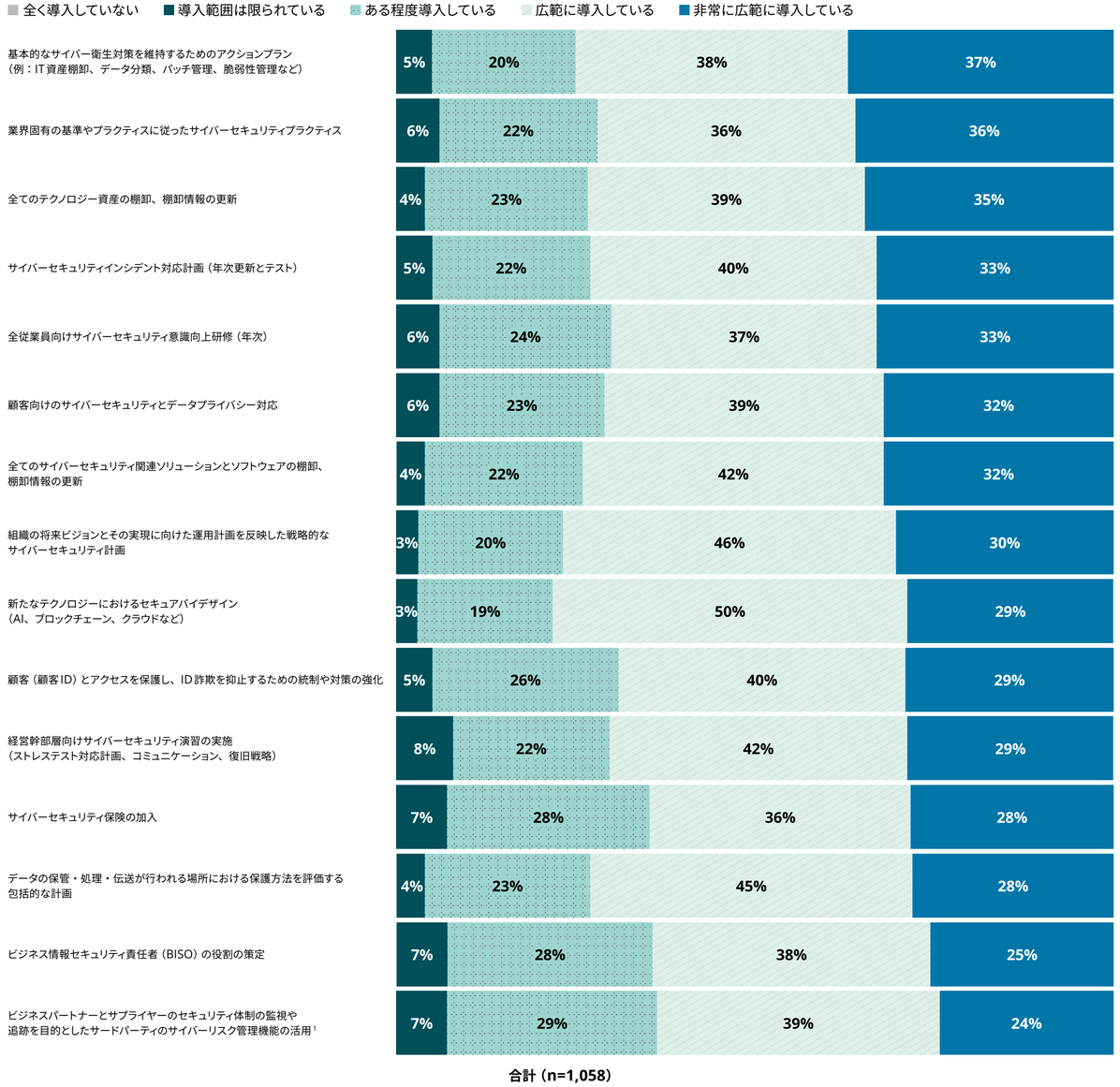
多くの調査回答者は、ビジネス情報セキュリティ責任者（BISO）の役割がまだ確立されていないとしています。その一方で、BISOは成熟度の高いサイバー戦略に欠かせない機能として認識が広がっています。BISOの導入が大きく進んでいると答えた調査回答者は63%にとどまりました。これは、多くの組織で事業領域とセキュリティ・リスク・レジリエンス機能を連携させるメカニズムが十分ではない可能性を示しています。

サードパーティに関するサイバーリスク管理の能力は依然として十分に活用されていない

本調査では、テクノロジーベンダーへの依存度がますます高まっていることがわかりました。その一方で、組織のセキュリティ態勢を監視や追跡を目的とするサードパーティのサイバーリスク管理機能を導入するかどうかについては、各種サイバーセキュリティ対策の中で最も導入が進んでいないという結果になりました。これらの機能を「広範に導入／非常に広範に導入」していると回答した割合は65%にとどまっており、看過できない未対応リスクが残っている可能性が示されています。

サイバーセキュリティ対策導入の程度

Q1：貴組織では、以下のサイバーセキュリティ対策をどの程度導入していますか。



合計（n=1,058）

[1] 四捨五入しているため合計が100%にならない場合がありますが、エラーではありません。

人材面の懸念を深めるスキルギャップ

調査回答者に、俊敏な対応やサイバー課題への対処を阻む主な要因を尋ねたところ、「高度なスキルを備えた人材の不足」が上位に挙がり、最大の制約要因と位置付ける調査回答者の割合が最も高くなりました。1位に挙げた調査回答者の割合は10%で、最も高くなりました。サイバー準備度を高めるうえで人材スキルの重要性が強調された結果となりました。

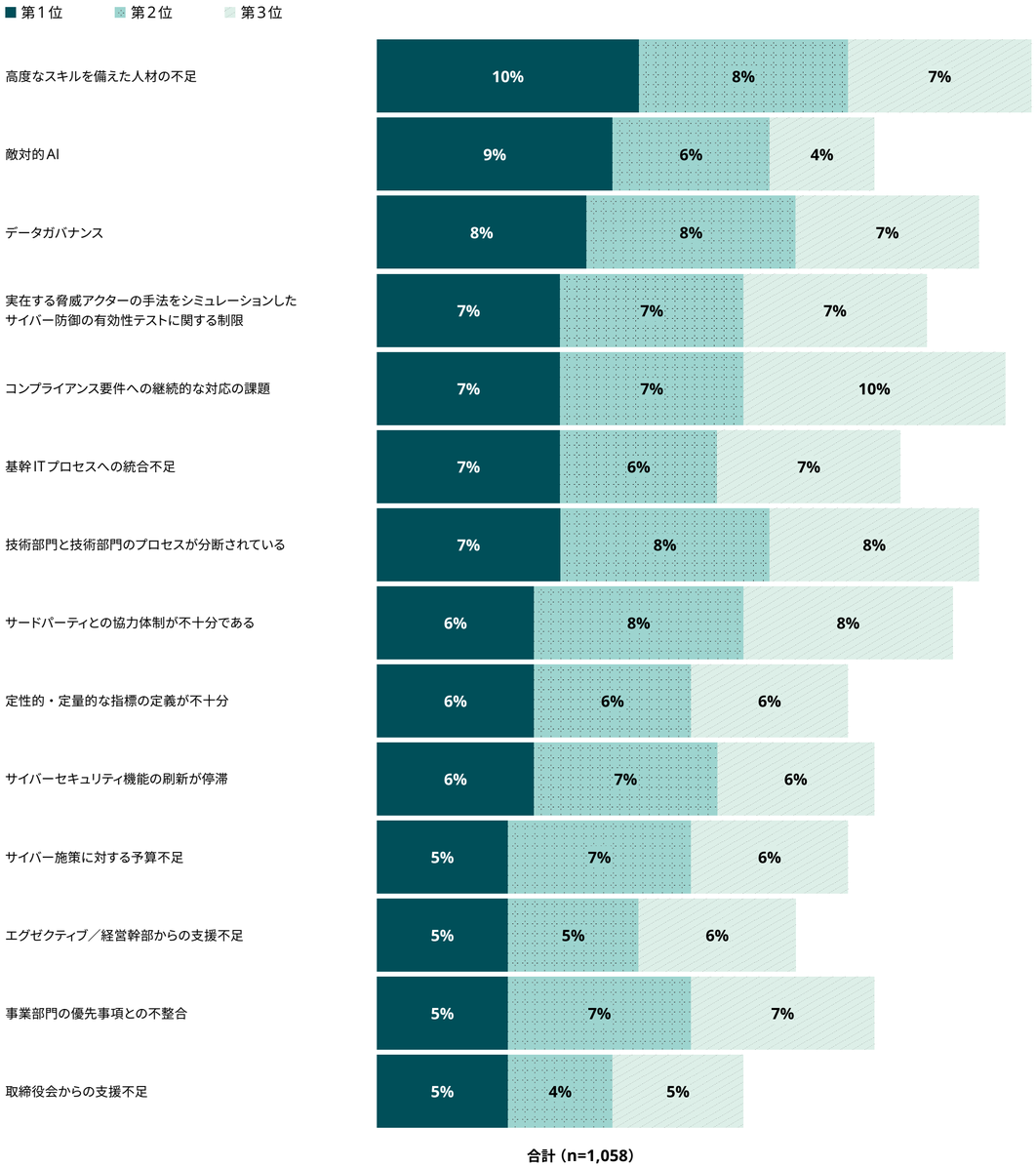
進化する脅威環境

敵対的AIとは、攻撃者がAIシステムの脆弱性を標的にしたり、高度なAI技術を使って攻撃を実行したりする場合に発生します。ソーシャルエンジニアリング、ディープフェイク、合成ID、偽情報、データポイズニングはいずれも敵対的AIの例であり、調査回答者はこれを、サイバー課題への機敏な対応を妨げる第2の要因と認識していました。この結果は、調査回答者が急速に変化する技術環境への適応や、AIがもたらす予測困難な脅威への対応に不安を抱いており、自社の対応準備に影響を及ぼすと見ていることを示唆しています。

ある医療テクノロジー企業のグローバルセキュリティ担当副社長は、「脅威の中には、検知された後に自ら振る舞いを変え、マルウェアのように防御側の対処に応じて対抗してくるAIシステムも存在する」と述べています。さらに、「異なるタイプのマルウェアに変化し、攻撃が大規模に展開されるおそれがあるといえるでしょう。このような攻撃を防ぐには、自動化された対応が不可欠です。仮に攻撃側が大量のエージェント型AIによる攻撃を実行する場合は、防御側も同等に高度なAI防御を用いて攻撃パターンを学習しながら対抗する必要がある」とも述べています。

サイバー課題への対応を阻害する主な要因

Q：サイバー課題への貴組織のアジャイルな対応を阻害している主な要因トップ3を、以下から選択してください。



合計（n=1,058）

パラドックスの解明

サイバーセキュリティへの自信と準備度の間にあるギャップは、戦略やビジョンを実行へと落とし込んでいく過程の中で捉えると、最も理解しやすいといえます。サイバー施策に対する経営層の支援や予算の確保、さらには事業部門の関係者と連携した戦略レベルのサイバー計画の策定・実行に長年取り組みは進んでいる一方で、サイバーの原則や運用プロセス、技術基盤を組織全体に本格的に定着させることが依然として課題になっていることが明らかになりました。組織がサイバー課題に取り組むうえで支援できると確信している一方で、準備態勢を確実なものにするための仕組みはまだ十分には整っていません。

戦略レベルで得た成果を現場での確実な実行へと結びつけるには、リーダーに必要な次の一手として、どのような対応が求められるでしょうか。Deloitteの調査結果と調査回答者への詳細なインタビュー、特に自信と準備態勢の両面で高い水準にある調査回答者の見解からは、次のような重要なマイルストーンが明らかになっています。

BISOを議題に挙げる

BISOは、サイバーセキュリティ部門とビジネス部門間の重要な調整役を担うことができます。優れたサイバー戦略を事業レベルで実現しようとしている組織にとって、これほど重要な役割はないかもしれません。実際には、多くの組織が製品開発部門、DevOps部門、アーキテクチャ部門と緊密な連携を維持するために、セキュリティアーキテクトやBISOの役割を取り入れていると報告しています。従来は戦略に重点が置かれていたことを踏まえると、これまでBISOに対する関心が比較的限定的であったとしても、さほど不思議ではありません。

BISOという役割は、すべての組織に適しているとは限りません。しかし、事業部門と技術部門の間でプロセスおよび機能を緊密に統合することは、どの組織にも重要となっています。小規模な組織（または中央集権的な組織）では、新しい役職としてBISOを設けるよりも、セキュリティ担当者を含むアジャイル型の小規模チームを活用するほうが適している場合もあります。

外部パートナーの戦略的能力を活用する

煩雑で時間のかかる作業に対応が組織内のリソースだけで対応できない場合、外部パートナーが当該の業務を担うか、あるいは業務の自動化の目的で活用されることがよくあります。組織の能力が向上し、組織間の相互関係が成熟するにつれて、より価値の高い戦略的な連携に発展する可能性があります。外部パートナーは、強力なサイバー態勢に不可欠な要素です。

新たな脅威について、懸念と実際のリスクのバランスを見極める

本調査では、調査回答者の敵対的AIに対する懸念は高く見える一方で、Deloitteの顧客支援で得た知見に照らすと、現時点で実際に存在するリスクに比べて過度となっている可能性があります。選定した調査回答者へのインタビューでは、敵対的AIの性質が十分に解明されていないことへの懸念が示されました。調査回答者は、「分からない点が何であるかは把握できている課題」への対応経験はあるものの、「何が分からないのか自体が分からない未知の課題」に向き合うことは、当然ながらより強い不安を覚えているということです。

敵対的AIは、サイバー領域のリーダー企業が注意深く対処すべきですが、現時点では、生成AI環境における想定外のデータ漏洩や機密データの不正利用など、既知で対処可能な課題に優先して取り組む方が、より大きな成果につながる可能性があります。敵対的AIに取り組む際には、不安に振り回されるのではなく、実態をさらに調べる必要があります。また、どの程度の投資が妥当かを見極めるべきであり、その一方で、他のより差し迫った課題への着実な対応も続けるべきです。

> 「**自社では、必要に見合った適切な投資を確保し、求められる経営層の関与も得られた上で、適切なツールと運用プロセスも整っています。**しかし、大規模な組織に共通することとして、もともと内在するリスクや脅威の状況を把握できていると自信を持つことと、実際に有効な対応が可能であることとは別の問題となります」
>
> **ー ヘルスケア企業 CISO**

パラドックス ＃2

経営陣はサイバーセキュリティを優先。
しかし、現場への影響は限定的に

経営層による高い関与

サイバーセキュリティはビジネスにおける最優先事項です。このことは、前回の調査で得られた重要な知見であり、Deloitteの最新データからも、サイバーセキュリティの優先事項に対する経営層の支援が引き続き堅調であることがうかがえます。

フロントランナー企業では、CISOが90%以上のC-suite（経営幹部）、CEO、取締役会と強固な関係性を築いていることが確認されました。次に、フォロワー企業では、CISOが取締役会やCIOのそれぞれ80%と強固な関係性を築いており、基盤ビルダー企業のCISOはCIOの72%との関係性が強いという結果でした。

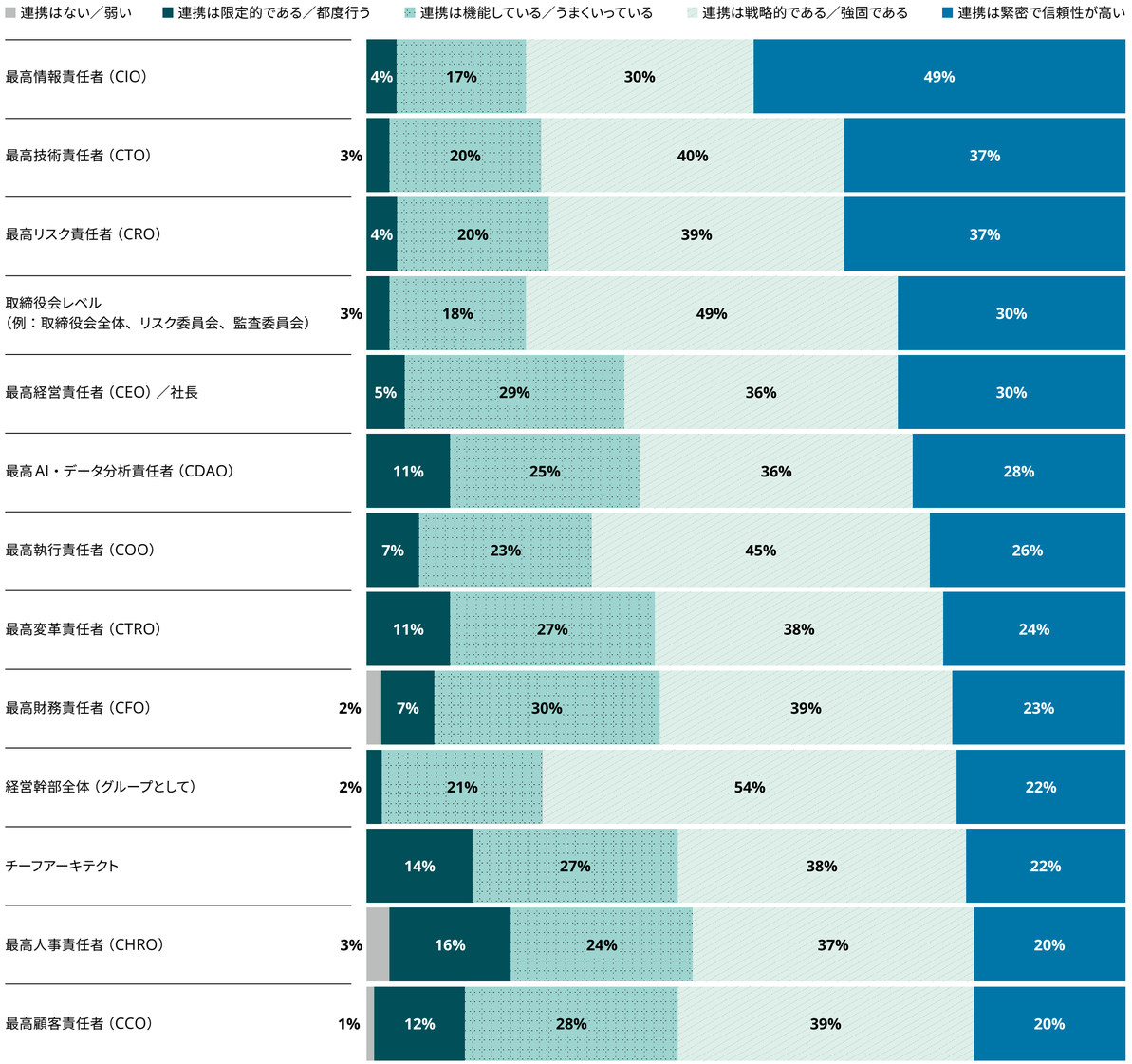
調査回答者の66%が自社のCISOがCEOと強固な関係を築いていると答え、さらに76%の調査回答者がCISOとC-suite全体との関係が強固であると評価しています。こうした関係性は、将来のサイバー課題に備える組織の態勢を整えるうえで重要です。

CISOの多くは、CEO（28%）またはCIO（33%）に報告する体制にあり、その結果として経営層と直接連携ができる立場にあります。調査回答者で最も多かったのは、サイバーを事業戦略および技術戦略全体にすでに統合している、あるいは将来を見据えた戦略の中にサイバー要件を積極的に組み込んでいると答えた層で、54%を占めました。フロントランナー企業では、サイバーセキュリティが戦略策定あるいは予算の面で重要となっていると回答しています。また、61%が基幹のIT基盤に対して、57%が事業戦略に対する予算を組んでいます。これは、フォロワー企業がそれぞれに43%と29%の予算を組んでいたり、基盤ビルダー企業がそれぞれに31%と15%の予算を組んでいるという結果に比較してはるかに高い割合です。

サイバー関連の取り組みは経営陣に広く支持されている一方、日常業務レベルでの実務プロセスや意思決定にまで浸透させることに苦労していると回答されています。

CISOとその他のビジネスリーダー間の関係の強さ

Q：貴組織のCISO（または同等のセキュリティリーダー）は、以下のビジネスリーダーとどの程度の連携関係がありますか。



合計（n=1,039）*

*「不明」は除外

サイバーの影響力は、構想段階から実行段階へは十分に移行していない

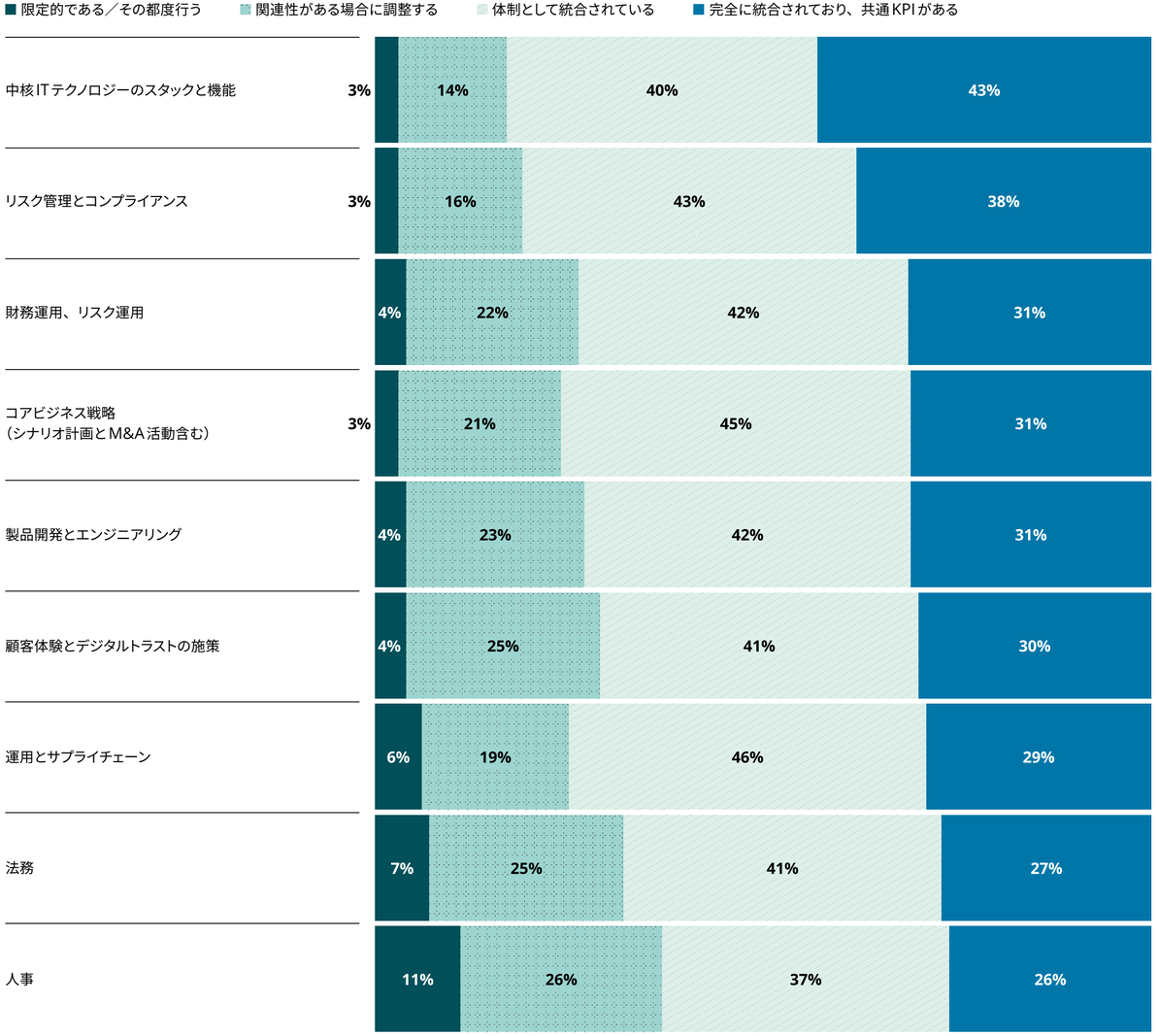
C-suite（経営幹部）ではサイバーに関する認識が概ね一致しているので、多くの組織では次の段階として、主要な事業部門や技術機能の中にサイバーを体系的に組み込む必要があります。

サイバー戦略の効果的な展開を実現するには、事業部門による着実な実行は重要な要素の一つです。調査回答者は、９つの領域の中で、サイバー分野が中核的なITおよびリスク管理に関する戦略やプロセスに最も大きな影響を与えていると回答しました。この２つの領域において、調査回答者の80%以上が、事業とサイバー施策との強固な整合性を示す主要な指標が整備されていると述べています。それ以外の領域では、サイバー分野は中核的な事業戦略やその他の機能に対する影響が限定的であることが示されています。一方で、フロントランナー企業の大多数は、自社がサイバーをより広範な全社戦略に完全に統合していると回答しました。さらに、事業戦略とサイバーを結び付けるためのあらゆる仕組みを整備している可能性が高く、特に組織のリスクマネジメント戦略では96%にもおよび、その傾向が顕著になりました。

「CISOの目標とは新たな方法論を通じて、サイバーセキュリティを戦術的・技術的な側面に偏重した状態からよりビジネスに資するものへと移行させることです。その新しい方法論により、事業収益を生み出すバリューチェーンに対して脅威モデリングやリスク評価の実施が可能になるはずです。ビジネスリーダーはこのようなバリューチェーンを最も重視しているのです」と、ある金融サービス企業のグループCISOは述べています。

組織内でサイバー戦略を他の領域に統合している程度

Q：貴組織では、計画策定や日々の意思決定において、サイバーセキュリティを以下の領域にどの程度統合していますか。



合計（n=1,058）

さらに、サイバーセキュリティはまだ、技術製品開発に大きな影響を与えるには至っていません。DevSecOpsの成熟期に達しており、調査回答者の78%が自社のサイバー領域のリーダー企業がDevSecOps運用に正式に組み込まれていると述べる一方で、主要な指標を共有した上での適切な共同責任体制が確立されていると考えている調査回答者はわずか40%にとどまりました。DevSecOps全体にわたるより緊密な共同責任体制の構築について、フロントランナー企業はフォロワー企業を22ポイント上回っています（61%と39%）。また、ソリューション設計と脅威モデリング（52%と26%）や、技術スタックに関するガイドライン（51%と28%）においても、フロントランナー企業がフォロワー企業を大幅に上回っていることが確認されました。

現時点で、組織のコントロールメカニズムを「統括する」CTOやチーフアーキテクトのようなリーダーがサイバーセキュリティを十分に影響力を行使できていないために、上記のような結果となった可能性があります。CTOやチーフアーキテクトの戦略的な関与は重要であり、製品エンジニアリング、アプリケーション設計、セキュリティの各担当部門にコントロールメカニズムをより深く統合していくための鍵となります。

現在、CISOが影響力を発揮するための報告経路や関係性は整っていません。例えば、こうした報告系統の在り方から、組織内におけるその関係性の状況をうかがい知ることができます。CTOは技術開発と実行に不可欠なパートナーであるにもかかわらず、CTOと深く信頼できる関係を築いているCISOは、わずか37%に過ぎません。同様に、組織の将来の技術的基盤を形成する責任を担うチーフアーキテクトと深い信頼関係にあるCISOはわずか22%でした。これらの調査結果からも、前述の「自信と準備度」に関するパラドックスで明らかになったように、ビジョンと実行の間にはギャップが存在することの裏付けられています。

> 「CISOの目標とは新たな方法論を通じて、サイバーセキュリティを**戦術的・技術的な側面に偏重した状態からよりビジネスに資するものへ**と移行させることです。その新しい方法論により、事業収益を生み出すバリューチェーンに対して脅威モデリングやリスク評価の実施が可能になるはずです。ビジネスリーダーはこのようなバリューチェーンを最も重視しているのです。」
>
> **ー 金融サービス企業 グループCISO**

パラドックスの解明

サイバーイニシアチブについて経営層から幅広い支持が得られています。その一方で、サイバーは日常の実務レベルのプロセスや意思決定にまで関わる主要事業部門にはまだ十分に統合されていません。このセクションでは、このような流れを変えていくために最も重要なステップのいくつかを以下に示します。

サイバーを常に議題に挙げる

ほとんどの組織にはサイバーセキュリティの基盤があります。例えば、DevSecOpsの原則とプロセスは広く採用されています。しかし、サイバーセキュリティをテクノロジーアーキテクチャに正確に組み込むには、エンジニアリングリーダーとセキュリティリーダーがパフォーマンス指標に関する共通認識を持ち、相互に責任を担えるシステムを構築する必要があります。それこそが、システムの初期段階からセキュリティ原則を組み込む「セキュアバイデザイン」というアプローチで目指す姿です。しかし、このアプローチを実践するには、サイバーに対する強固な態勢や形式的な対応だけでは、実装にまでは至りません。セキュリティの原則が組み込まれたエンタープライズアーキテクチャを構築するためには、「プロセスに従う」という考え方から脱却し、アジリティとレジリエンスを実現するためのエンジニアリングなど共通の成果を達成する姿勢を持てるよう、組織を変えていく必要があります。これらの取り組み全てを達成するためには、組織全体で、可能な限り早い段階からサイバーセキュリティをプロセスの一部として組み込む必要があります。

CISOとチーフアーキテクトの関係構築に真剣に取り組む

今日、CISOはチーフアーキテクトとの強固な戦略レベルの関係が築けていません。製品エンジニアリングやアプリケーション設計、テクノロジーの機能性に対して、サイバーセキュリティの原則やプラクティスを組み込むためにもこの関係が必要になります。どのような関係においても言えることですが、関係が自然に強化されることはありません。今後開発されるソリューションにサイバーセキュリティ対策が開発時に組み込まれることを確実にするため、CISOは、これらの重要なステークホルダーとより強固な関係を築くための計画を策定する必要があります。

「以前は、テクノロジー部門の責任者は中央集権型のエンタープライズアーキテクチャチームを管理していましたが、前任のCTO（最高技術責任者）の下で、その機能は各部門がそれぞれ担う形になりました。（中略）そのため、推進力がやや低下（中略）そのため、私のチームはアーキテクチャセキュリティレビュー委員会を立ち上げ（中略）、「ここは、アドバイスを求めに来れる場所ですよ」と呼びかけることから始めましたと、あるヘルスケア企業のCISOは語ります。

CISOとチーフアーキテクトの関係性が強化されれば、組織に重要なメリットをもたらす可能性があります。例えば、調査回答者の約半数は、エンタープライズアーキテクチャとサイバーセキュリティの統合が短期的にも長期的にもITや運用の復旧時間に大きなメリットをもたらすと考えています。また、脅威インテリジェンスやアプリケーションセキュリティの強化を主要なメリットとして挙げています。これらは全て、チーフアーキテクトからの賛同と積極的なサポートが必要とされる分野です。

組織の優先事項をその責任者とすり合わせる

今日、組織においてミッションクリティカルな優先事項はどこにあるでしょうか。また、そのような優先事項を管理する責任はどのリーダーが負っているのでしょうか。これらの問いに対する答えは、CISOやサイバーセキュリティの責任を負うその他の人々にとって、次に築くべき最も重要な関係性への実践的な道しるべとして役立つかもしれません。組織が顧客に焦点を当てた新たな戦略を推進しているのであれば、顧客データに関する課題、顧客体験、プライバシーなど、あらゆる面でサイバーセキュリティについて検討する必要があります。これらのビジネス上の重要な関係は、サイバーセキュリティを戦略構想のみにとどめず、主要事業の運用に組み込むためには議論が不可欠であり、またその影響も大きいと考えられます。フロントランナー企業では、CISOの61%がサイバーセキュリティの責任者と共にIT運用標準を策定や管理を行っていると回答しました。また、フロントランナー企業はソリューション設計と脅威モデリングに関する助言サポートの提供においても、他の企業グループに先んじており、フロントランナー企業ではCISOの52%がこのようなイニシアチブに取り組んでいると回答しています。

ソフトスキルを向上させる

CISOをはじめとするサイバーリーダーは、通常、その高い技術力と戦略的能力の高さに基づき、その役割を担います。しかし、組織の他部門と良い関係を築く能力（サイバー関連の職務の重要な特徴でもある）は、これまでの職責ではあまり重視されていない、いわゆる「ソフトスキル」の有無に少なからず依存しています。サイバーセキュリティのリーダーは、聞き上手であり、コミュニケーション能力が高いでしょうか。CISOやその他のサイバーリーダーは、同僚や他のリーダーと合意点を見いだせるでしょうか。このようなソフトスキルを備えることで、サイバーセキュリティはビジネスを妨げるものではなく、むしろビジネスを促進させるものであると他者を直接説得できるようになります。

「以前は、テクノロジー部門の責任者は中央集権型のエンタープライズアーキテクチャチームを管理していましたが、前任のCTO（最高技術責任者）の下で、その機能は各部門がそれぞれ担う形になりました。（中略）そのため、推進力がやや低下（中略）そのため、私のチームはアーキテクチャセキュリティレビュー委員会を立ち上げ（中略）、「ここは、アドバイスを求めに来れる場所ですよ」と呼びかけることから始めました」

ー ヘルスケア企業 CISO

パラドックス ＃3

「ベンダーを減らしたい」と
「もっと必要だ」というジレンマ

ベンダー過多

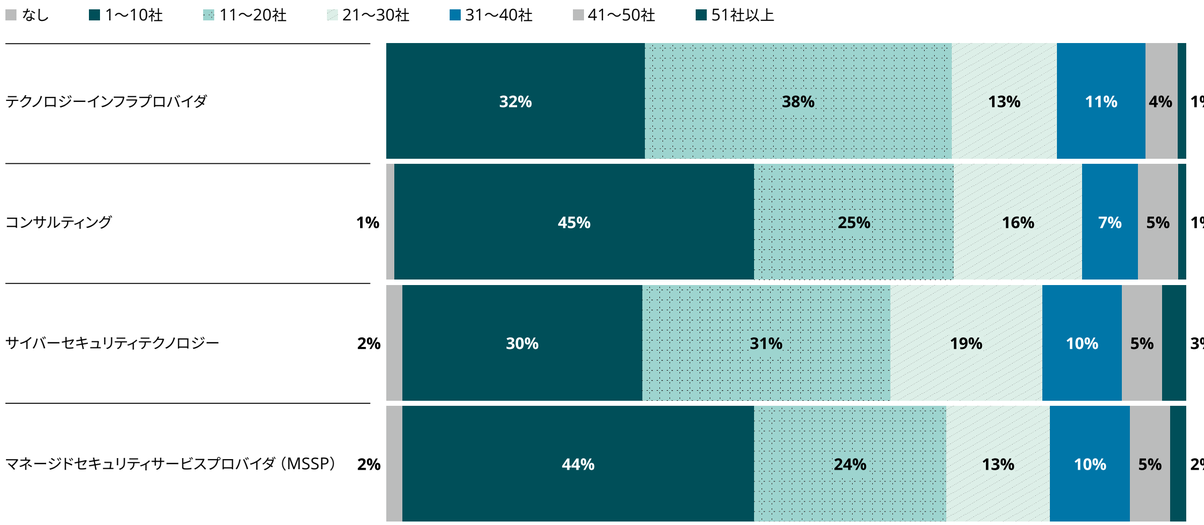
サイバーセキュリティの専門家は、変化し続ける脅威環境と、絶えず進化する一連のソリューションや技術力に相まって、増え続ける多数のベンダーと連携するようになっており、その流れには終わりが見えない状況です。

既に管理するには多すぎるとみられる数のベンダーと取引しており、今後3〜5年間でさらにその数が増加するだろうという回答が散見されます。例えば、技術インフラについては、プロバイダ数が11〜20社と回答した割合が38%と最も多くなっていますが、21社以上と回答した割合も29%となっています。

また、当社のインタビュー結果によれば、プラットフォームへの移行に関する関心が高まってはいるものの、多くの企業は必ずしも契約ベンダーを増やすことを望んでいないことが明らかになりました。一方、既存テクノロジーが現在または将来のニーズを満たせない場合、ベンダー数を増やさざるを得ない可能性もあります。一部の組織では、複数のベンダー（多くの場合は20社以上）を維持することを、ベンダー集中リスクを回避するための意図的な戦略と位置付けています。統合の簡素化や運用の複雑性の低減を目的として、より少数のベンダーと提携したいと考えるリーダーであっても、統合によってベンダー集中リスクが高まるとの見方が多数を占めています。すなわち、ベンダー数が少ないと、一部に依存が偏り、障害発生時の影響が大きくなるおそれがあります。このジレンマに対して、あらゆる組織に当てはまる万能な解決策はありません。

カテゴリーごとのサイバーベンダー数

Q：以下カテゴリーにおける、貴組織のサイバーベンダー数を教えてください。



合計（n=1,058）

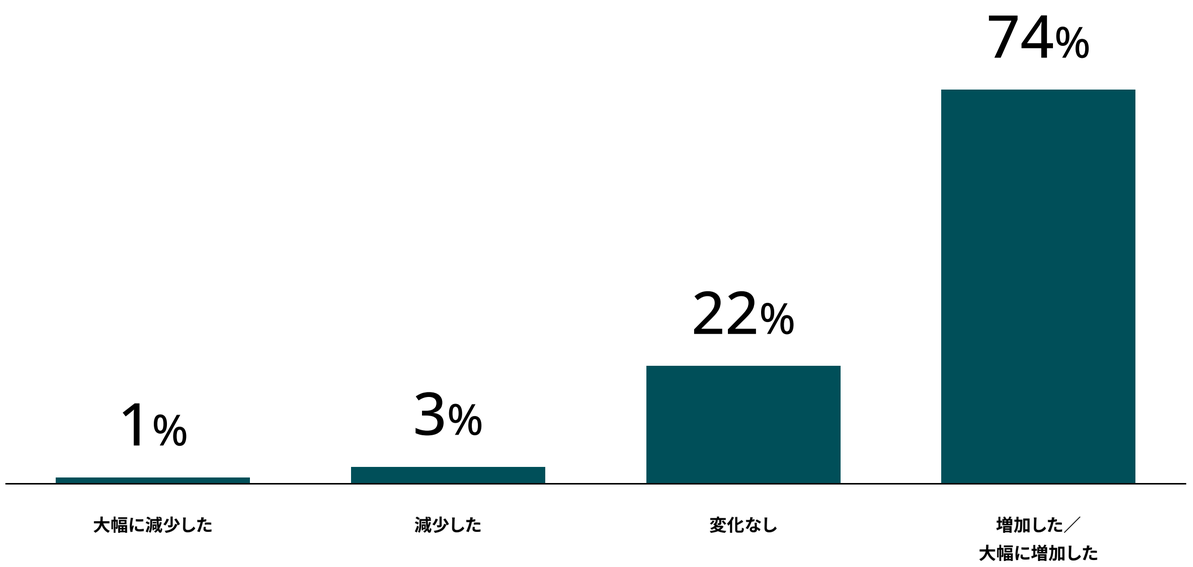
ベンダーポートフォリオ：大規模化と拡大傾向

調査回答者は、既に多数のベンダーと提携しているにもかかわらず、過去１年間でベンダーの総数が「増加した」または「大幅に増加した」と述べています。また、１年後、３年後、５年後においてはさらに多くのベンダーとの提携が見込まれていると回答しています。調査回答者の74%は自社が提携するサイバーセキュリティ関連の企業数について過去１年の間に「増加した」または「大幅に増加した」と述べています。

ある金融サービス企業のCISOは、「サイバーセキュリティソリューションを提供するベンダーを新たに加えただけでなく、IT部門によりインフラストラクチャサービスの一部を管理するベンダーもさらに数社追加した」と述べています。同社のCIOも同様で、アプリケーション担当のチーム向けに、ソリューションやベンダーを増やしています」と述べています。サイバーベンダー数について、来年も変わらないと予想しているのはわずか38%にとどまり、調査回答者の大半は今後増加すると予想しています。今後３年間でベンダー数が「増加する」または「大幅に増加する」と回答した割合は79%でした。今後５年間で「増加する」または「大幅に増加する」と回答した割合はさらに高く、85%に上りました。

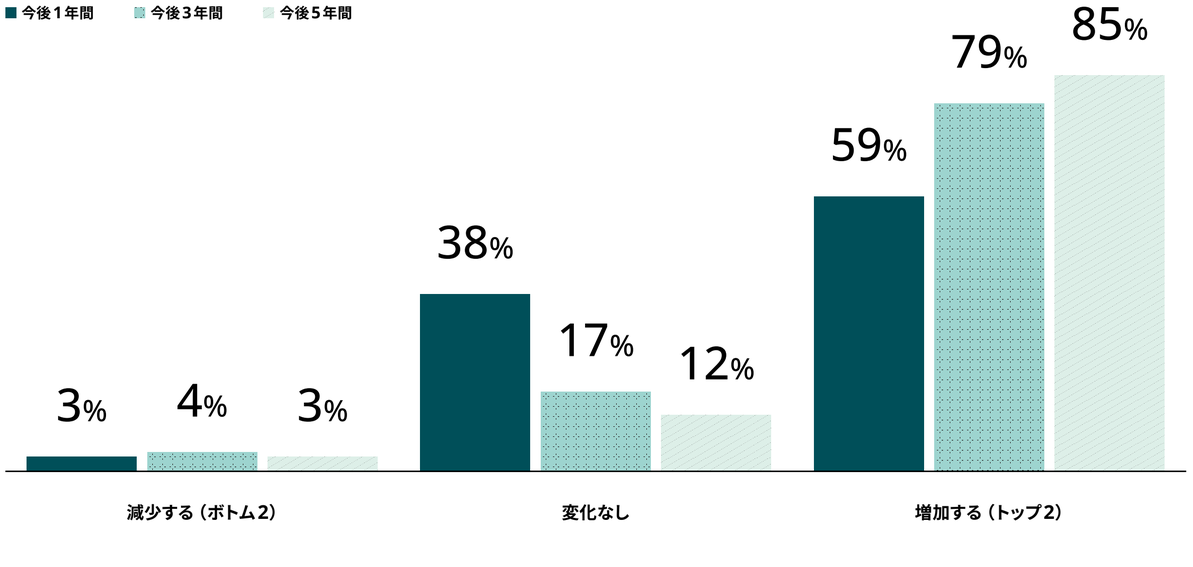
サイバーベンダー数の過去１年間の変化

Q：貴組織では過去１年間に、サイバーベンダー数はどのように変化しましたか。



サイバーベンダー数の変化予測

Q：今後１年間、３年間、５年間で、貴組織のサイバーベンダー数はどのように変化すると予測していますか。



合計（n=1,058）

ベンダー数増加の要因

AIの出現により新規ベンダー開拓が進展

企業はすでに多くのベンダーと取引していますが、新たな戦略的関係を構築する理由の一つは、新しい技術的能力の活用や新たなリスクに対応するためです。過去1年間においては、AIによりサイバー対応力が大幅に高度化されており、調査回答者の約75%はリアルタイムでの脅威分析やデジタルインフラストラクチャ監視のための高度な推論機能を組み込むことで既存のセキュリティプログラムを更新したと述べています。調査回答者の76%は、サービスにAIを組み込んでいるサイバーセキュリティベンダーを活用していると回答しました。

サイバー対策が技術スタックにうまく統合されていない

現時点では、サイバー対策が技術スタックに十分に統合されていると考えている調査回答者が約30%にとどまっていました。このデータは、冗長なアーキテクチャパターンが存在している可能性を示しており、より簡素化されたエンタープライズアーキテクチャを活用することを通して、ベンダー数の整理や集約を進める余地があることを示唆しています。調査回答者は、自社においては今後12～24か月の間に整理や集約に進む可能性があると述べており、その場合にはサイバー対策が統合される割合は8ポイント増加すると予想しています。当社では、ベンダーエコシステムの効率化（可能であれば集約）を進める手段として、より統合型のサイバープラットフォームへの移行が進展していると見ています。

「**サイバーセキュリティソリューションを提供するベンダーを新たに加えただけでなく、**IT部門によりインフラストラクチャサービスの一部を管理するベンダーもさらに数社追加し、同社のCIOも同様で、アプリケーション担当のチーム向けに、ソリューションやベンダーを増やしています」

— 金融サービス企業 グループCISO

パラドックス ＃3

統合型サイバープラットフォームへの移行、2024年から2026年にかけて5倍に拡大

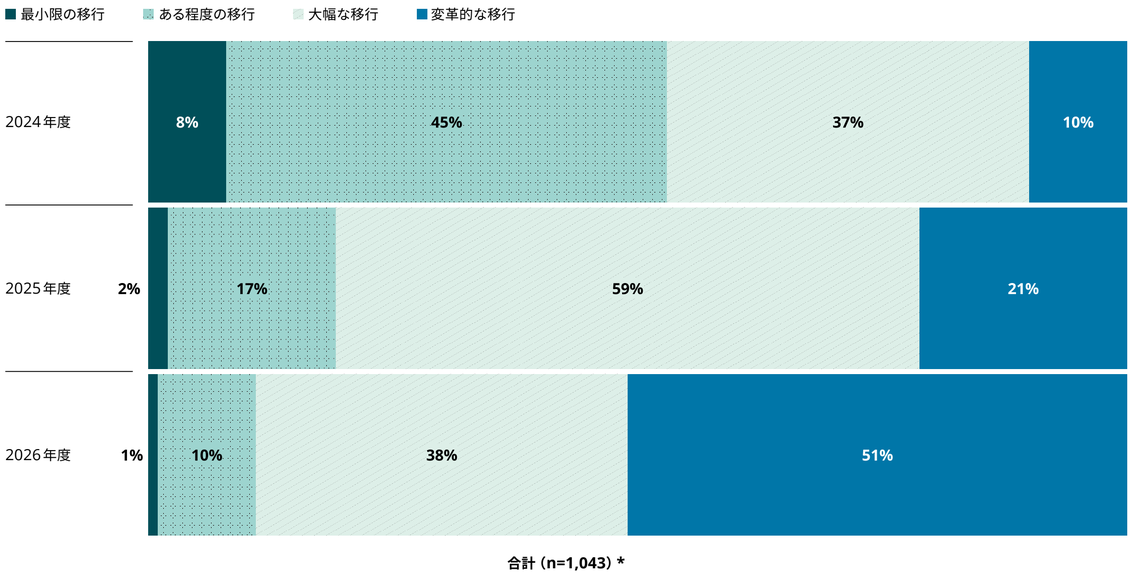
前回実施した2024年の調査では、統合型サイバープラットフォームへの移行を変革として推進していると回答した割合はわずか10%でした。2025年には、その割合が2倍以上の21%になりました。さらに、2026年には、調査回答者の51%が統合型プラットフォームにより変革がもたらされることを期待していることから、統合型プラットフォームへの移行の勢いが大きく高まっていることがうかがえます。フロントランナー企業の間では、この移行はさらに顕著です。2024年時点に「大幅な移行」または「変革的な移行」を進めていると回答した割合は64%でしたが、2026年にはこの回答割合が94%にまで増加しました。

統合サイバープラットフォームへの移行が進んだ要因は何でしょうか。このような移行の背景には、複雑性の提言やプラットフォームの総保有コストの削減といった従来からの要因があると考えられます。一部の企業では、特定の分野に特化した複数の業界最高のサービスを提供する最先端ベンダーを管理するよりも、「必要十分な」単一プラットフォームに移行したいと考えるものです。

AIをはじめとする他の要因も作用している可能性があります。サイバー領域およびテクノロジー領域のリーダーはいずれも、AIを有効に活用するには一貫性のある正規化されたデータが必要であり、そのために統合プラットフォームが非常に適していると認識しています。エージェント型AI戦略を推進する企業にとって、統合プラットフォームはエージェント型ワークフローの構築に必要となる標準化されたデータモデルが提供できます。

サイバー活動における統合プラットフォームへの移行の程度

Q：前年度、今年度、来年度について、貴組織のサイバー活動が統合プラットフォームへどの程度移行していますか。



*「不明」は除外

パラドックスの解明

ベンダーの増加は避けられないのでしょうか。現在は、脅威を取り巻く環境が依然として流動的です。このような脅威に迅速に対応するための新たなツールや機能が求められていることから、現状はベンダーが増加しているように見えるかもしれません。十分な予算と経営層の支援があれば、多くの企業は採用するベンダーやセキュリティツールを次々と増やしていくと調査回答者は述べています。

このような状況を踏まえると、プラットフォームへの関心が高まっていることは十分に理解できます。特に、運用の負担が小さく、専門特化型の製品群に近い機能を幅広く備え、異なる技術を比較的低コストでまとめて扱えるプラットフォームへの評価が高まりやすい状況です。

AIや統合不足のアーキテクチャによって生じたベンダー乱立の抑制を行うために、組織がいま取るべき施策を検討する必要があります。

ベンダーアセスメントを行い、ベンダーの真の価値と潜在的な可能性を見極める

現在、ベンダーは組織のサイバー戦略を支えるうえで欠かせない存在となっています。現在、各ベンダーからどのようなサービス提供を受けているのか、各ベンダーのサービスに重複があるのか、さらにベンダーがどの領域で付加価値となるサービスを提供できるのかについて、最新の状況を明確に把握できているでしょうか。戦略性、計画性、リスクベースの視点、手順に沿った体系的なベンダー評価の仕組みがなければ、こうした状況を正確に把握することは大変困難となります。

エンタープライズアーキテクチャの視点で事業継続に不可欠なベンダーと重複領域を見極める

組織では、事業部門や地域ごとに異なる差し迫ったリスクへ対応するため、これまで新たなベンダーを追加してきた経緯がある一方で、その結果としてベンダーの重複や冗長性につながった可能性もあります。AIに関しては、妥当な目的のもとで進められたベンダー拡張の近年における代表例の一つです。組織は、エンタープライズアーキテクチャ部門と緊密に連携し、重複する機能を特定するとともに、合理化・統合・集約の機会を検討することで、事業継続に不可欠なベンダーを特定し、集約の余地があるかを把握できます。

プラットフォームはコストや効率性の先にある利点にも目を向けて価値を評価する

プラットフォームの拡大は、コスト削減や業務効率化に加え、AI活用の推進、データ変換、エージェント型ワークフローの再設計など、さまざまな要因を背景に進められています。エージェント型AIへの関心が高まる中、プラットフォームの標準化や統制、統合のための基盤を提供するだけでなく、ベンダーの集約や最適化戦略の推進にも役立てることができます。

パラドックス ＃4

侵害は頻発するも、
ビジネスへの影響は抑制できている

サイバー侵害は今後も継続的に発生

調査回答者は引き続き、インシデントの件数が多いと報告しています。2025年に少なくとも1件の侵害を公表した組織の割合は78%で、2024年の91%から低下しています。2025年に6〜10件の侵害を報告した組織は約3分の1にのぼりましたが、その割合は2024年の40%より低くなっています。報告された侵害件数は前年比で減少したものの、依然として高い水準にあります。

また、サイバー侵害の一部には未報告のままとなっているインシデントがあることも考えられます。特に、そうした事案を検知し報告するための体制や能力が十分でない組織では、その傾向が強いと考えられます。

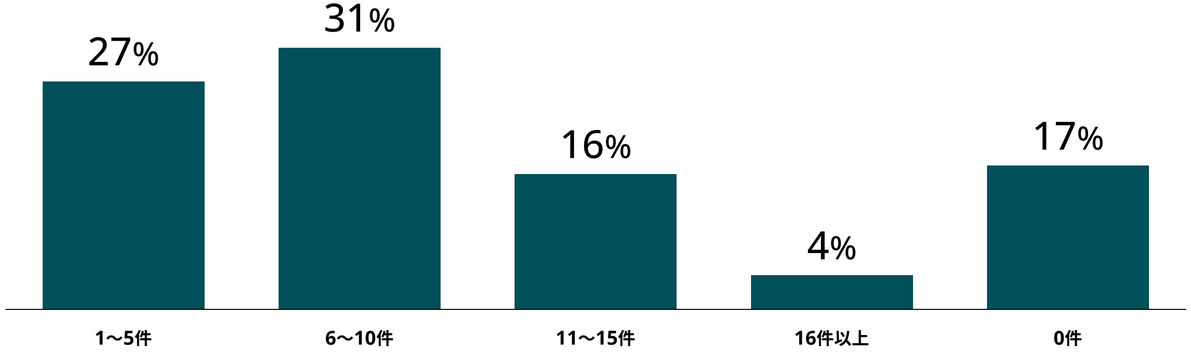
調査回答者が懸念している脅威主体は、主にサイバー犯罪者（30%）、サイバーテロリスト（15%）、ハクティビスト（10%）などのよく知られた脅威アクターに向けられています。こうした脅威アクターが使用する手法や技術も同様によく知られているものであり、ランサムウェア（20%）、マルウェア（15%）、データ漏洩（14%）が再び上位の懸念事項となっています。一方で、今年の調査では新たに注目すべき傾向も確認されました。AIの悪用が新たな懸念事項として浮上し、懸念項目の中で同率で4位となっています。

「**システムやアプリケーション、各種環境への侵害は、今後も起こり得るものとして考える必要があります。**あらゆる侵害を未然に防ごうとすると、組織における業務遂行が著しく難しくなる可能性があります。重要なのは、システム侵害が発生した際にできるだけ早く検知し、それをできるだけ迅速に検知し、影響が大きくなる前に封じ込めと根絶を行って、被害拡大を防ぐ体制を構築することです」

ー ヘルスケア企業 グローバルCIO

公表しセキュリティ侵害の件数*

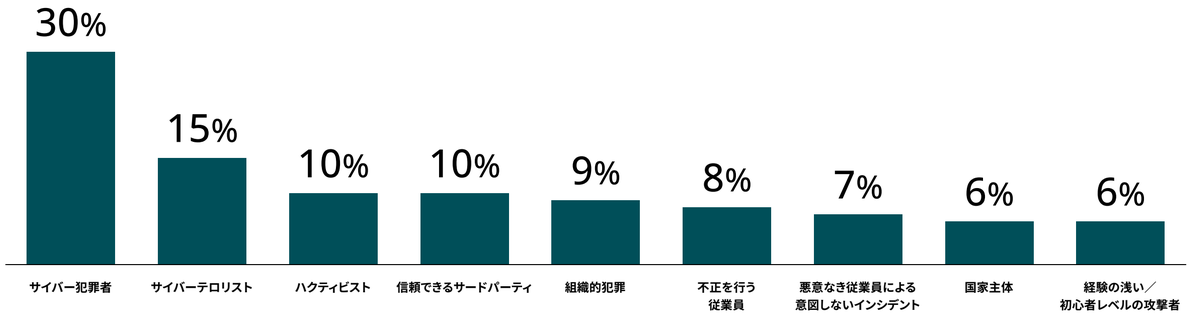
Q：前年度、貴組織が公表したサイバーセキュリティ侵害は何件ですか。



* 調査回答者の5%が公開報告義務のない非上場会社であるため、合計は100%にはなりません。

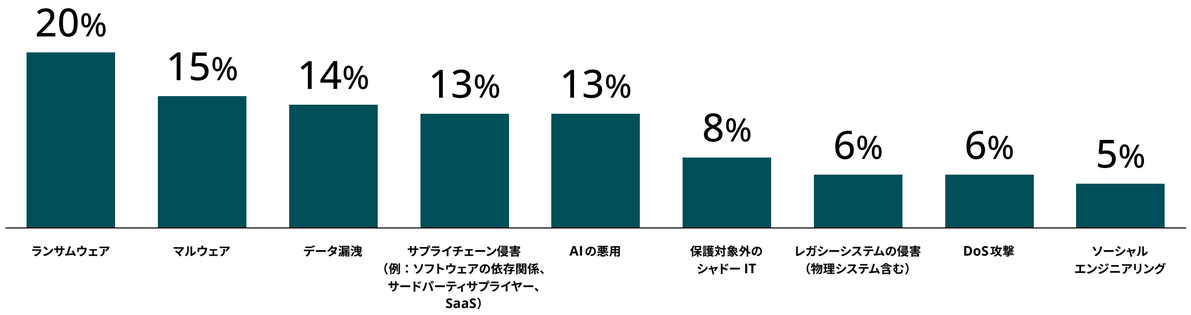
サイバーセキュリティに関して最も懸念される脅威要因（アクター／要因）

Q：貴組織がサイバーセキュリティに関して最も懸念している最大の脅威要因を1つ挙げてください。



サイバーセキュリティに関して最も懸念される脅威要因（ツール／技術）

Q：貴組織がサイバーセキュリティに関して最も懸念している最大の脅威要因を1つ挙げてください。



合計（n=1,058）

組織はこれまでのところ、侵害による影響の最小化に成功

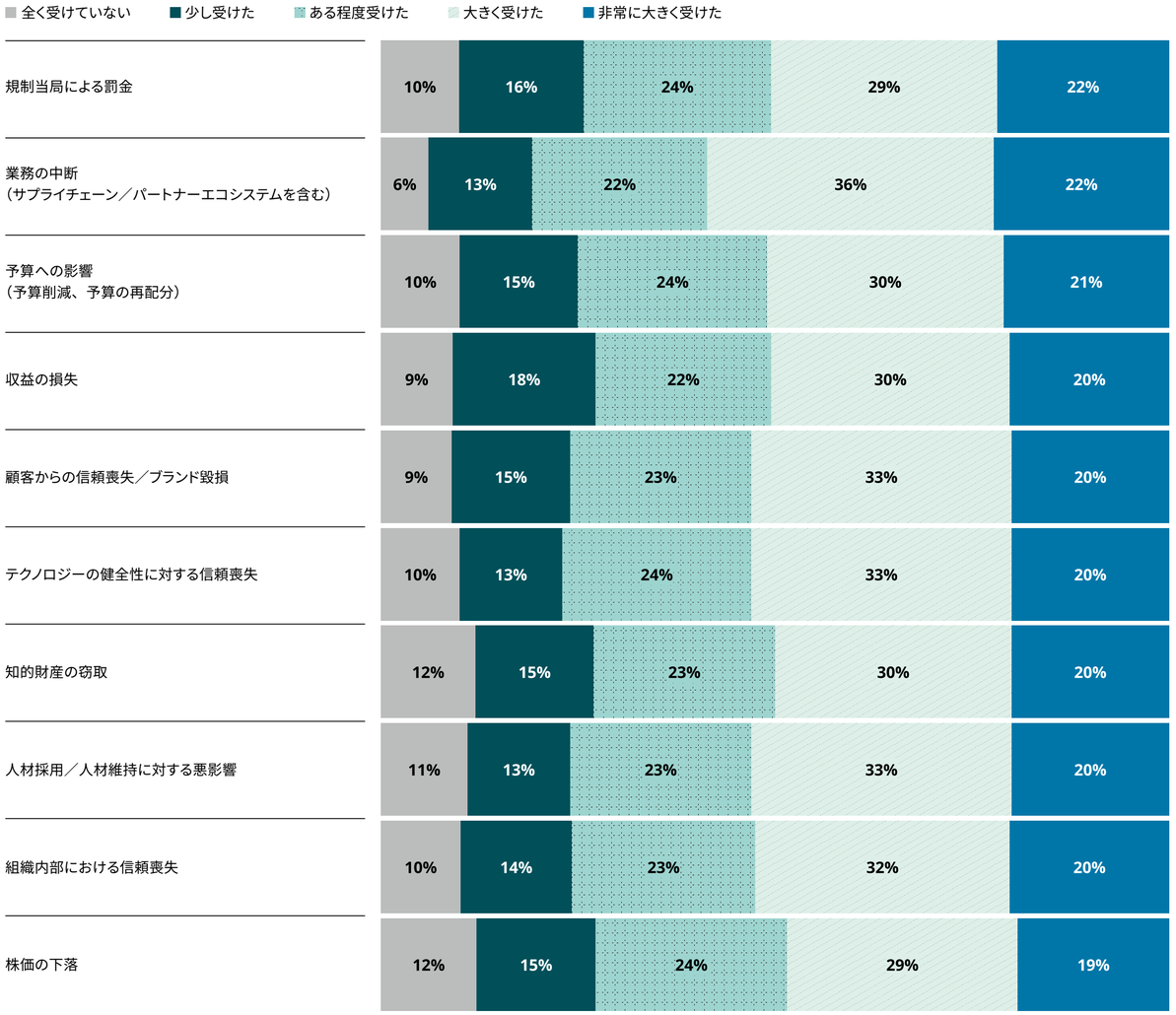
サイバー侵害の件数は依然として多いものの、さまざまな影響項目において、サイバーセキュリティインシデントにより組織が深刻な悪影響を受けたと回答した人の割合は平均52%となり、前年の64%から低下しています。

ただし、これは影響を過小評価しているわけではありません。サイバーセキュリティインシデントによる最も大きな影響は業務中断であり、58%が組織大規模またはそれ以上の業務上の支障を経験し、サプライチェーンや取引先のエコシステムにも影響が出たと回答しています。一方で、1年前の調査では同様の回答が66%であったことから、組織は悪影響への対処や管理が以前より向上していることが示唆されています。あるヘルスケア企業のグローバルCIOは、「システムやアプリケーション、各種環境への侵害は起こり得ます。あらゆる侵害の防止を徹底しようとしすぎると、組織内で業務を円滑に進めることが非常に難しくなります。重要なのは、システムが侵害された際にできるだけ早くその侵害を把握し、ただちに封じ込めと排除を行って、影響が広がる前に対処できる体制を構築することです」と語っています。

フロントランナー企業は特にこの傾向を顕著に示しています。高度な脅威インテリジェンスをを持つ組織では、同業他社よりも多くの侵害事例を報告する傾向があります。前年度に11件以上のサイバー侵害を報告した組織の割合は、フロントランナー企業が26%で最も高く、フォロワー企業は19%、基盤ビルダー企業では20%でした。フロントランナー企業のほうがより多くのインシデントを報告しているにもかかわらず、サイバーインシデントによって被害を受けたとする割合はフォロワー企業と同程度でした。

サイバーインシデントが組織に与えた影響の程度

Q：貴組織は、サイバーセキュリティのインシデントや侵害により、以下の分野においてどの程度の悪影響を受けましたか。



合計（n=823）*

*「不明」は除外

パラドックスの解明

「何か」がうまく機能している―このポジティブなパラドックスから導き出される最も明確な結論です。脅威が拡大する環境下にあっても、調査回答者の組織はサイバーインシデントに伴う悪影響を効果的に抑え込めていることがうかがえます。

一定の成果は見られるものの、組織が警戒を緩めることはできません。こうした前向きな傾向をさらに促進するうえで有効となる実践的な方法をいくつか紹介します。

侵害の報告件数が増加していても、過度な対策強化を実施しない

侵害の報告件数の増加は、実際には強力なサイバー対策が機能していることを反映している可能性が高く、脅威に対する効果的な検知や対応の体制が整備され、適切に運用されていることの表れであることもあります。いずれの場合であっても、より詳細な分析を行う必要があります。侵害の件数だけでは有用な判断指標にはならず、何を検知しているのか、どの程度の速さで検知しているのか、さらにその侵害が事業に及ぼし得る影響についての洞察があって初めて適切に評価できます。

侵害件数そのものよりも、発生パターンや結果に重点を置いて検討することが重要です。侵害件数の増加は、影響の小さい多数のインシデントを迅速に多く検知できるようになった結果でしょうか。その結果を組織のセキュリティ成熟度の向上を示す前向きな兆候ととらえることができます。侵害件数の増加は、繰り返し悪用される攻撃経路、長期化する侵入後の潜伏期間、あるいは業務への支障と関連しているのでしょうか。このような背景情報がなければ、経営層は不必要な統制措置を講じて過剰に対応する一方、喫緊のリスクへの曝露を過小評価するおそれがあります。

侵害の報告件数が少ない場合は精査する

組織で侵害が報告されていないことは好ましい兆候とも考えられる一方で、侵害の検知能力が不十分であることを示している可能性もあります。その結果、このような組織には悪意ある活動や侵害を特定するための監視および分析機能が十分に備わっていない可能性があり、潜伏型の攻撃に対して依然として脆弱である可能性があります。

徹底的にレジリエンスの強化を追求する

調査回答者の67%は、サイバーセキュリティと事業戦略を結びつけるため、レジリエンス構築を支える数ある重要施策の1つとしてシナリオプランニング演習を積極的に推進しています。こうした演習は、組織にとってのサイバーの価値を明確にするうえでも役立ちます。例えば、サイバーセキュリティの実装は、主に収益向上のためなのか、収益保護のためなのか、それとも事業中断やその対応コストを回避することを重視しているのかを明確にするためです。シナリオプランニングは、組織が直面する脅威の急速に変化している実態に即した速度で展開していく必要があります。

パラドックス ＃5

予算は安定。
しかし、事業環境は極めて不安定

サイバーセキュリティ支出は組織に支えられた安定投資

投資の必要性を事業の観点から明確に説明できる組織ほど、必要な予算を確保しやすいと考えられます。

あるヘルスケア企業のグローバルCIOは、「妥当性の高い説明と説得力ある事業上の根拠があれば、資金承認を得られる可能性は高いです」と述べています。サイバーセキュリティの予算は今後1年で緩やかな増加が見込まれる一方、事業の優先事項ごとの予算配分に大きな変化はあまり見られません。その背景には、数年にわたる投資計画や、事業部門・IT部門・リスク管理部門が共同でサイバーセキュリティを担う体制によるものと考えられます。サイバーセキュリティ施策に積極的に投資しているフロントランナー企業は、同業他社に比べて具体的な事業成果を期待する傾向がはるかに強く、特に以下のような分野においてその傾向が顕著です。

- 効率性、迅速性、戦略性
- 信頼性、確実性、レジリエンス
- 顧客価値

フロントランナー企業の90%以上は、各分野での成果向上を見込んでいます。

85%の調査回答者は、サイバー予算を前年比で増額したと回答しており、さらに多い88%の調査回答者が今後12か月での予算拡大を見込んでいます。一部の組織では、サイバー関連支出の増加幅がかなり大きくなる見込みです。調査回答者の8%は今後12か月で支出が25%超増えると見込んでおり、3分の1以上の調査回答者はIT、事業部門、全社リスク管理やその他を含む組織全体のサイバーセキュリティ関連予算が10～25%増額すると予想しています。

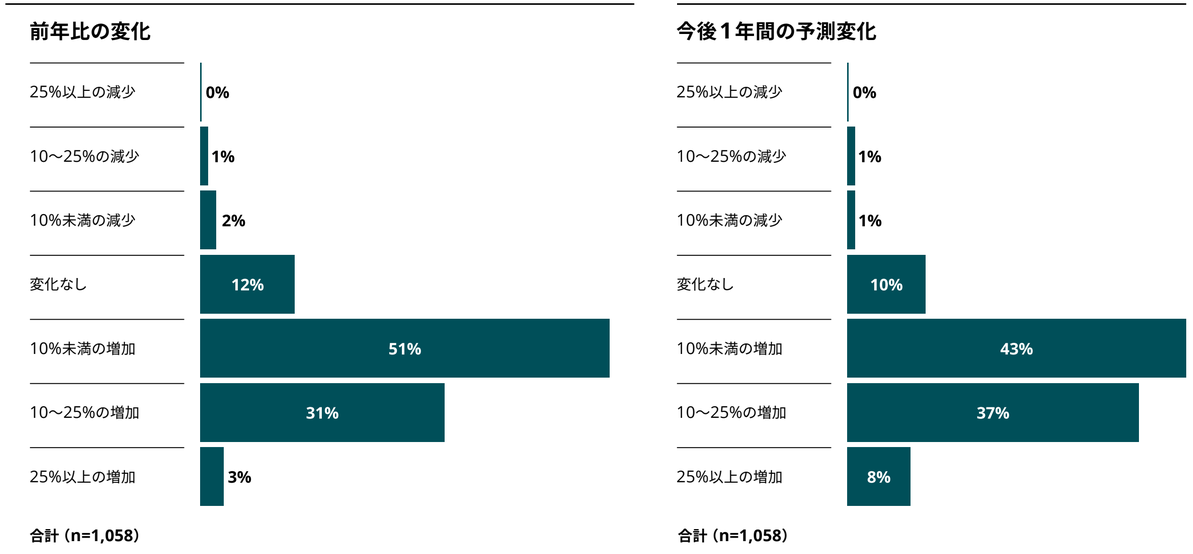
特筆すべきことに、調査回答者は今後12～24か月においても予算の財源構成[1]は比較的安定すると見ており、主な注力先として以下を挙げられています。

IT部門	事業部門	全社リスク管理
43%	30%	26%

[1] 注：数値の四捨五入により合計が100%にならない場合があります。また、残りの割合は「その他」に該当します。

組織のサイバーセキュリティ予算

Qa：前年度と比較して、貴組織のサイバー関連予算（ITやその他の財源全てを含む）の総計はどの程度変化しましたか。
Qb：今後1年間で貴組織のサイバー関連予算（ITやその他の財源全てを含む）の総計はどの程度予測していますか。



調査対象者のほぼすべての組織は複数年にわたるサイバー投資を予算化しており、単年度の予算サイクルのみに依存していると回答したのはわずか7%にとどまりました。あるヘルスケア企業のグローバルCIOは、「当社では、施策を通常2〜3年単位で策定していますが、予算については単年度で組んでいます。長期的な目標や中長期の施策はあるものの、予算編成は依然として毎年見直しされ、設定される形です」と述べています。

以下のように、複数年計画の内訳を見ると、サイバー予算の最も大きな割合は1〜2年の計画期間に属しており、全体の61%を占めています。

サイバー予算サイクル：

35% は単年度

サイバー予算サイクル：

26% は2年ごと

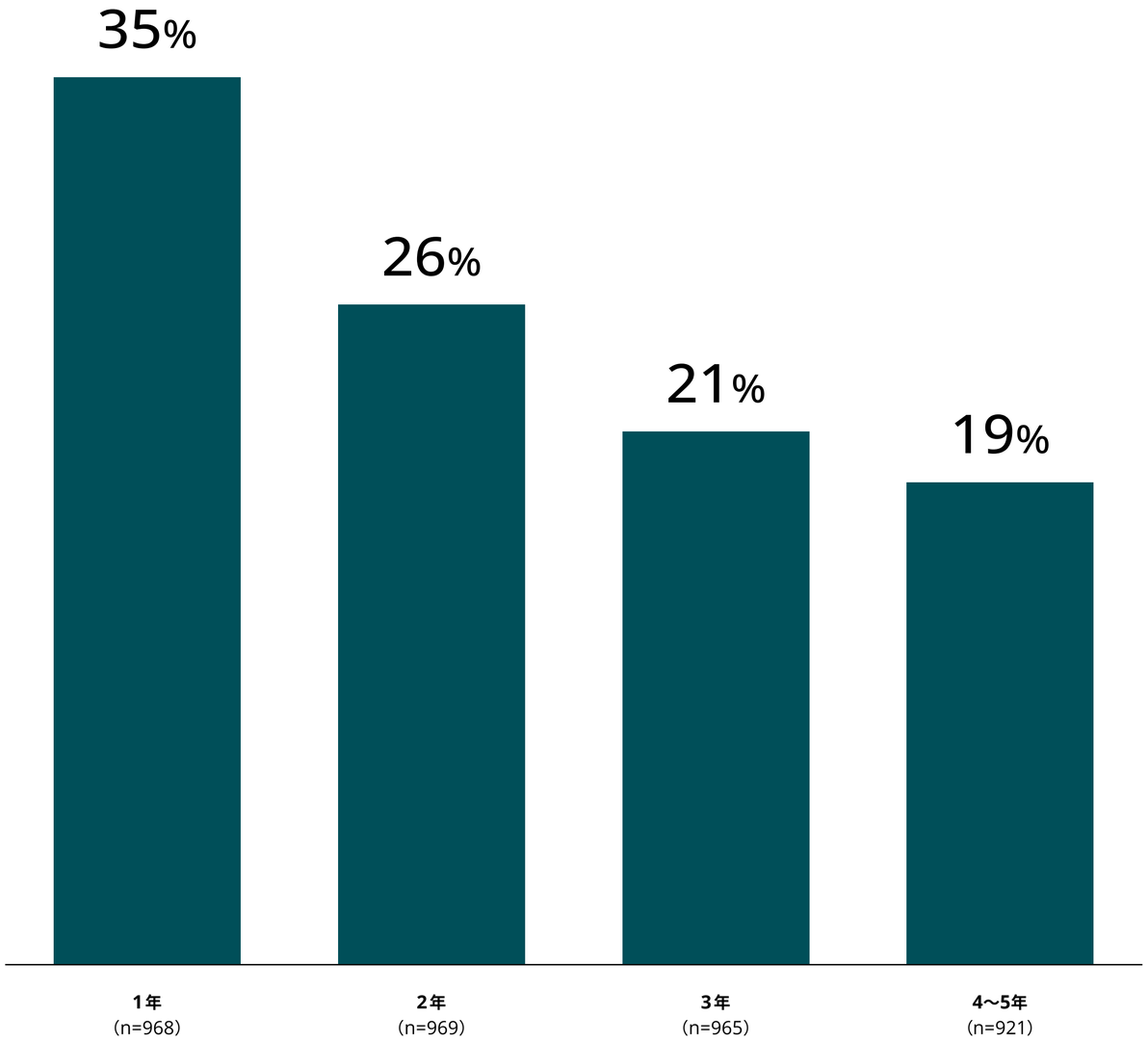
なお、サイバー予算サイクルが4〜5年先を見据えた複数年で確保されている組織は19%を占めました。

サイバー施策の優先事項に大きな変化は見られず、支出項目にも大きな変化は見られません。実際、調査回答者によると、来年度の予算配分は今年度とほぼ同水準で推移する見込みであり、最も大きな予算配分は脅威の検知・対応に対する20%で最上位となっています。これに続く主要な支出分野は、インフラセキュリティ、データ／ID／アプリセキュリティ、そして戦略・ガバナンス・コンプライアンスの順に配分されています。

> 「妥当性の高い説明と説得力ある事業上の根拠があれば、**資金承認を得られる可能性は高いです**」
>
> **ー ヘルスケア企業 グローバルCIO**

複数年投資へのサイバー関連予算の配分＊

Q：今年度のサイバー関連予算において複数年にわたる投資を行っている場合、その投資期間はどのくらいですか。



＊ 複数年にわたる投資を行っていない組織は、集計から除外されています。(n=71)

サイバー環境は安定的でも予測可能でもない

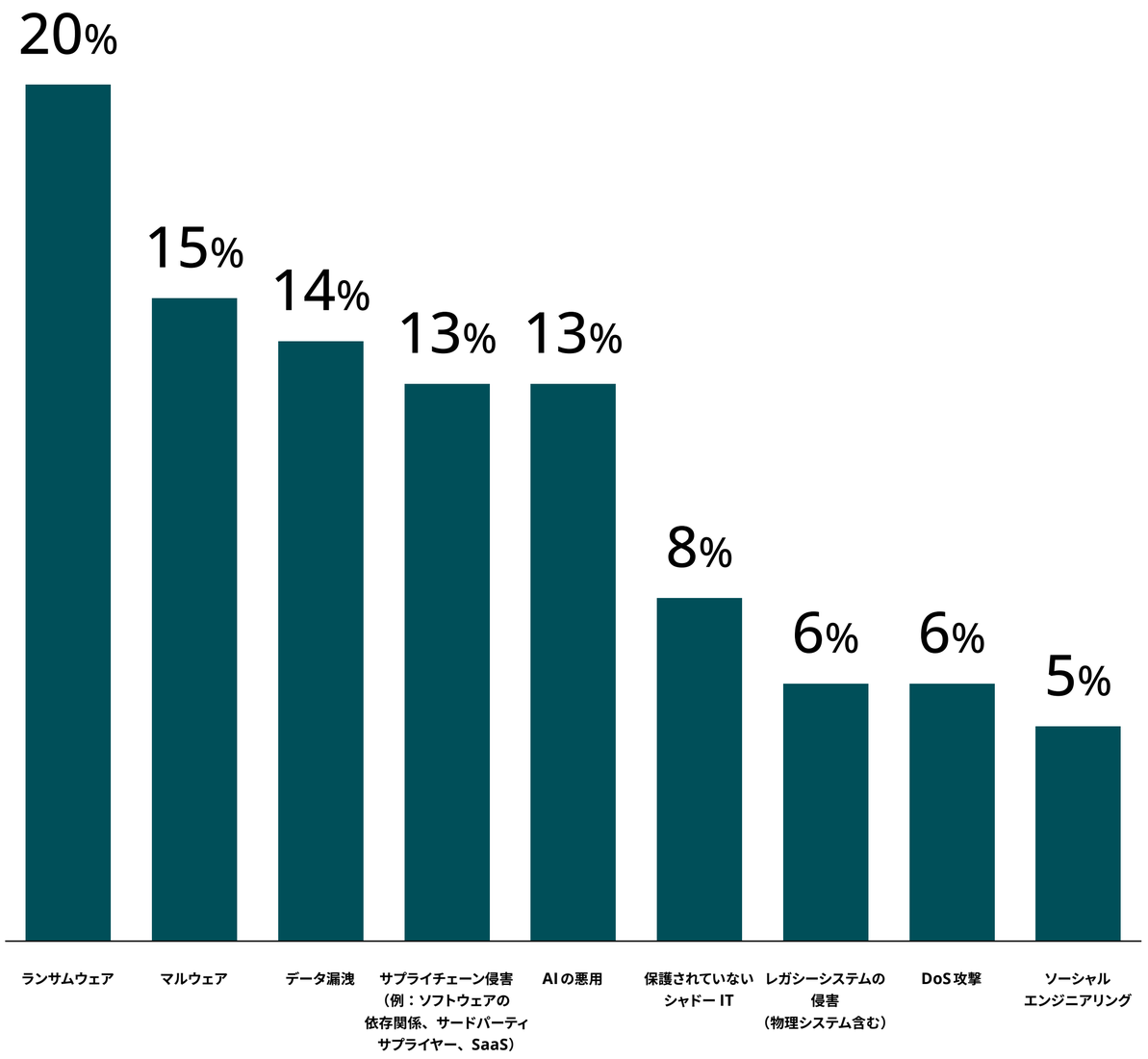
生成AIの急速な進展という1つの要因を考えてみても、サイバー環境がいかに急激に変化しているかが明白です。わずか2、3年前までは、生成AIへの迅速な投資の必要性が広く真剣に論じられていたわけではなく、実際に投資へ踏み切る動きはさらに限られていました。現在では、調査回答者の約4分の3（72%）が、10数件のサイバー施策において、ベースの推論アプローチを既存のAI活用基盤に組み込んでいると回答しています。これは予期せぬことであり、十分に計画されていたとも言いがたい変化であり、固定予算の枠組みではほとんど対応しきれない性質のものでした。

脅威の様相も変化しています。例えば、3年前には「AIの悪用」が調査回答者の特定する脅威リストには含まれていませんでした。現在では、ランサムウェア、マルウェア、データ漏洩と並ぶトップ5の懸念事項に位置づけられており、従来とは異なる新たな対応策が必要です。AIへの対応においては、従来型の統制をそのまま適用するだけでは十分とは言えません。例えば、非決定論的AIシステムは、プロンプトハッキングのような脅威に対抗するために、きわめて具体的なガードレールの整備が必要です。このことは、組織が現在取り組むべき課題が、新たなレベルの複雑さを伴っていることを示しています。

> 「**当社では、施策を通常2〜3年単位で策定していますが、予算については単年度で組んでいます。**長期的な目標や中長期の施策はあるものの、予算編成は依然として毎年見直しされ、設定される形です」
>
> **ー ヘルスケア企業 グローバルCIO**

サイバーセキュリティに関して最も懸念される脅威要因（ツール／技術）

Q：貴組織がサイバーセキュリティに関して最も懸念している最大の脅威要因を1つ挙げてください。



合計（n=1,058）

パラドックスの解明

どの組織にとっても、見通しの立てやすさや安定性を重視するのは自然なことであり、特に予算面ではその重要性が一層高まります。

技術革新のスピードが加速する中、テクノロジー予算全体についても大幅な見直しが必要になるという認識が広がっています。しかし、そのような状況にあっても、サイバーリスクは事業に深刻な影響を及ぼす可能性があるため、サイバー防御への投資は他の投資とは別の視点で考える必要があります。例えば、AIの導入は多くの部門で効率化やコスト削減につながると考えられていますが、サイバー領域では事情が異なります。攻撃者がAIを新たな手段として活用することで、むしろ対応コストや負荷が増す可能性があります。脅威アクターが新たな手法でAIを悪用するためです。サイバー領域の責任者は、AIの導入によりセキュリティ予算の最適化を進められる可能性がある一方で、進化を続けるさまざまな脅威に対応するため、AIの活用を大幅に拡大する必要に迫られる可能性もあります。

ある意味では恵まれた状況にあるとしても、予算枠が安定した水準で推移し、資金配分が固定されている中で、どうすればそれを実現できるのでしょうか。

変化に対応できるサイバー予算を設計する

これは不測の事態に備えるための予算確保と捉えることができます。例えば、年間サイバー予算の10〜20%を確保しておくことで、新たに必要となる機能への機動的な投資や、予測困難な脅威への迅速な対応できるようになります。

複数年にわたる予算運用の在り方を再考する

複数年予算は、変化への対応という点で制約が大きすぎるのではないでしょうか。従来の複数年予算に代わる選択肢として、ローリング予測や継続的予算編成といった柔軟性の高いアプローチの採用を検討することが重要です。

予算編成の発想を転換する

組織の財務責任者や予算の決定者は、サイバーセキュリティ特有の課題が予算計画に与える影響を十分に織り込めていない場合があります。その認識が十分でない場合には、組織全体で発想を転換する時期に来ているかもしれません。財務責任者や予算決定者にサイバー環境の実情を適切に説明し、予算編成に関する新たなアプローチを共同で検討する好機と捉えるべきです。サイバー領域の責任者が、組織が直面しているサイバーリスクを財務的な影響として定量化できれば、予算や対応方針に関する議論はより緊急性と具体性が明確なものになります。例えば、組織の特定の部門が他部門よりも高いリスクを抱えており、それに伴う潜在的な財務影響も大きい場合には、その部門に対してより重点的な投資を行うことが必要になる場合があります。

パラドックスの利点

本調査で明らかになったパラドックスは、新たな取り組みの機会を示しています。これらの課題を解消できる組織は、構想と実行のギャップを埋めるうえで有利な立場に立つことができます。

サイバー戦略と実行の変革を促すために必要な条件の多くは、今日すでにかなり整っています。全社戦略を担う責任者は、組織の最重要目標の実現におけるサイバーの重要性を理解しており、十分な予算を通じてサイバー戦略を支援する姿勢を示しています。一方、CISOをはじめとするサイバーセキュリティ責任者は、増大するサイバー脅威から組織を守るために必要な戦略やプロセス、体制を着実に整えてきました。

今こそ、これらの重要な要素を有機的に統合し、将来の課題にも対応できる、より強靭で全社的に行き渡ったサイバー文化の仕組みを形成することです。この変革を前進させるには、変革の担い手が必要です。本レポートの読者である皆様こそが、その中核的な役割を果たす立場にあると考えられます。まずは、本レポートで明らかになったパラドックスの観点から自組織を捉え直し、特に関連性の高い論点を特定したうえで、関係部門と連携しながらその解消に取り組むことから始めるべきです。

本調査の詳細についてさらにご興味がある場合、レポートの洞察について意見交換されたい場合、組織やその目標に対する潜在的な影響をさらに検討されたい場合や、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。

執筆者

Diana Kearns-Manolatos
Emily Mossburg
Kelly Nelson
Iram Parveen

作成協力者

Volker Burgers
Evan Carvouni
Jonathan Chan
Tim Corder
Felix De Andres
Miguel Olias De Lima
Jason Frame
Javier Francisco
John Gelinne
Tanneasha Gordon
Rob Jacoby
Jimmy Joseph
Daphne Lucas
Tara Mahoutchian Mortazie
David Mapgaonkar
Jeffrey Minick
Stephanie Montalvo
Will Nelson
Jose Pela Neto
Sean Peasley
Anand Raghawa Prasad
Frank Santucci
Jennifer A. Sullivan

問い合せ先

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

Daphne Lucas
Canada Cyber Leader
Partner, Deloitte Canada
dlucas@deloitte.ca
+1 403 267 1737

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

Jose Pela Neto
Brazil Cyber Leader
Partner, Deloitte Brazil
jpela@deloitte.com
+55 11 5186 6396

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

Paula Alvarez
S-LATAM Cyber Leader
Partner, Deloitte Mexico
palvarez@deloittemx.com
+52 55 5080 6558 ext: 6558

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

Marius von Spreti
Central Europe Cyber Leader
Partner, Deloitte Germany
mvonspreti@deloitte.de
+49 89 290365999

調査方法

DeloitteのGlobal Future of Cyber Survey（第5版）は世界43カ国、5つの業界、23のセクターに属する1,058名のビジネスおよびテクノロジーリーダーから収集したデータが活用されています。

本調査の分析においては、サイバーセキュリティのトレンドに精通している9名の経営幹部に行ったインタビュー内容も踏まえて作成しています。

今年度の調査レポートでは、自信の程度と準備度に基づき、調査回答者を3つのカテゴリーに分類しています。

フロントランナー企業は、サイバーセキュリティに対する自信と準備度に関して、以下の項目で「ある程度自信がある」または「非常に自信がある」と回答した割合が最も高い結果となりました。

- サイバーセキュリティ投資の効果を測定するための、リスク定量化ツールの使用
- 自社のデジタルサプライチェーン全体でサードパーティリスクに対処している程度
- サイバーセキュリティインシデント対応計画の策定と、その計画の年次更新とテスト
- サイバーセキュリティプラクティスと業界固有の基準・プラクティスとのアライメント
- その他

フォロワー企業は、同様の質問において、自信と準備度に関する評価が全体として中程度でした。

基盤ビルダー企業は、自信と準備度に関する評価が最も低い結果となりました。

サイバーセキュリティに関する自信と準備度の指標は、14の対策のうち「非常に広範に導入している」とされた対策数と、8つの戦略のうち「非常に自信がある」と回答された戦略数を基に作成されました。

ビジネス戦略との連携不足

Q1：導入の準備度

対策の導入範囲が「非常に広範／組織全体」と回答した数に従い、調査回答者に設定した比重は以下の通りです。

10〜15 件の対策数の場合は比重を3に設定

4〜9 件の対策数の場合は比重を2に設定

0〜3 件の対策数の場合は比重を1に設定

Q2：自信

戦略について「非常に自信がある」と回答した数に従い、調査回答者に設定した比重は以下の通りです。

5〜8 件の戦略数の場合は比重を3に設定

3〜4 件の戦略数の場合は比重を2に設定

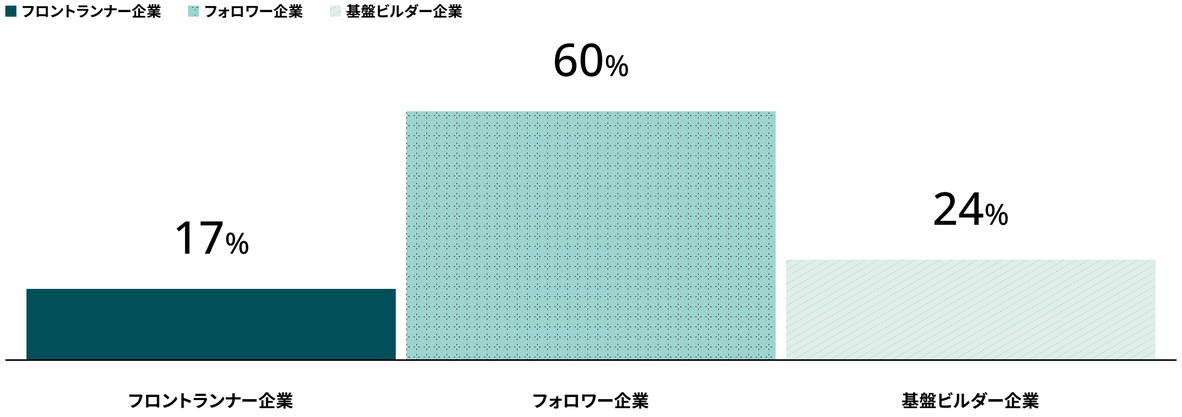
0〜2 件の戦略数の場合は比重を1に設定

サイバーセキュリティ戦略および施策に対する自信と準備度の比重を総合的に評価するため、両者の重みを合算して全体スコアを算出しました。

- 合計が5〜6の調査回答者はフロントランナー企業
- 合計が3〜4の調査回答者はフォロワー企業
- 合計が2の調査回答者は基盤ビルダー企業

フロントランナー企業は、本レポートの第一のパラドックスを克服した調査回答者となります。本レポートに示したその他のパラドックスにうまく対処するための取り組みについて、フロントランナー企業の経験から貴重な洞察を得ることができます。

自信と準備度の指標（総回答数に対する割合 *）



* 四捨五入しているため合計が100%にならない場合がありますが、エラーではありません。

N=1,058	フロントランナー企業	フォロワー企業	基盤ビルダー企業
戦略と対策に関する自信と準備度の比重合計（最小2、最大6）	5-6	3-4	2
回答数	176社	631社	251社
総回答数に対する割合	17%	60%	24%

Deloitte.
デロイト トーマツ

Together makes progress

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合同会社デロイト トーマツ グループならびにそのグループ法人（有限責任監査法人トーマツ、合同会社デロイト トーマツ、デロイト トーマツ税理士法人およびDT弁護士法人を含む）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プロフェッショナルサービスを提供しています。また、国内30都市以上に2万人超の専門家を擁し、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、Deloitte Touche Tohmatsu Limited（“Deloitte Global”）、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。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。Deloitte Globalおよびそ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。Deloitte Global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 リミテッドは保証有限責任会社であり、Deloitte Globalのメンバーファームです。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、最先端のプロフェッショナルサービスを、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進することで、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180年の歴史を有し、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約46万人の人材の活動の詳細については、www.deloitte.comをご覧ください。

Member of
Deloitte Touche Tohmatsu Limited

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