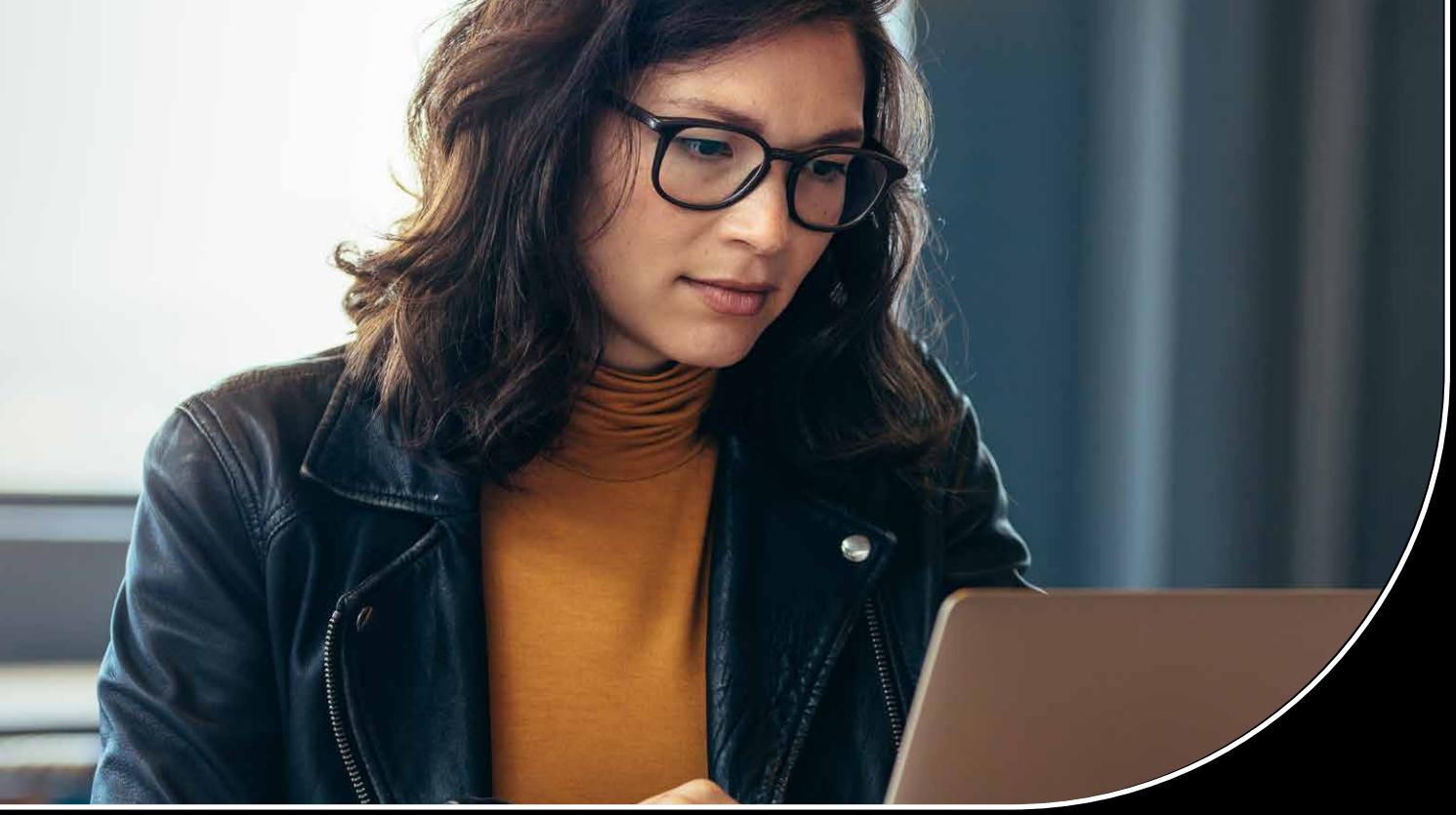
pwc

CxOプレイブック：セキュリティをイノベーションの中核に

「Global Digital Trust Insights 2024」
調査結果より



イノベーションの中核にあるセキュリティ：この非現実的な世界が現実のものになったとしたら?

最先端のセキュリティプログラムへの期待はますます高まっており、配分される予算額も増加しています。しかし、実際のところセキュリティの強化は遅々として進んでおらず、むしろ停滞していると言ってもよいかもしれません。

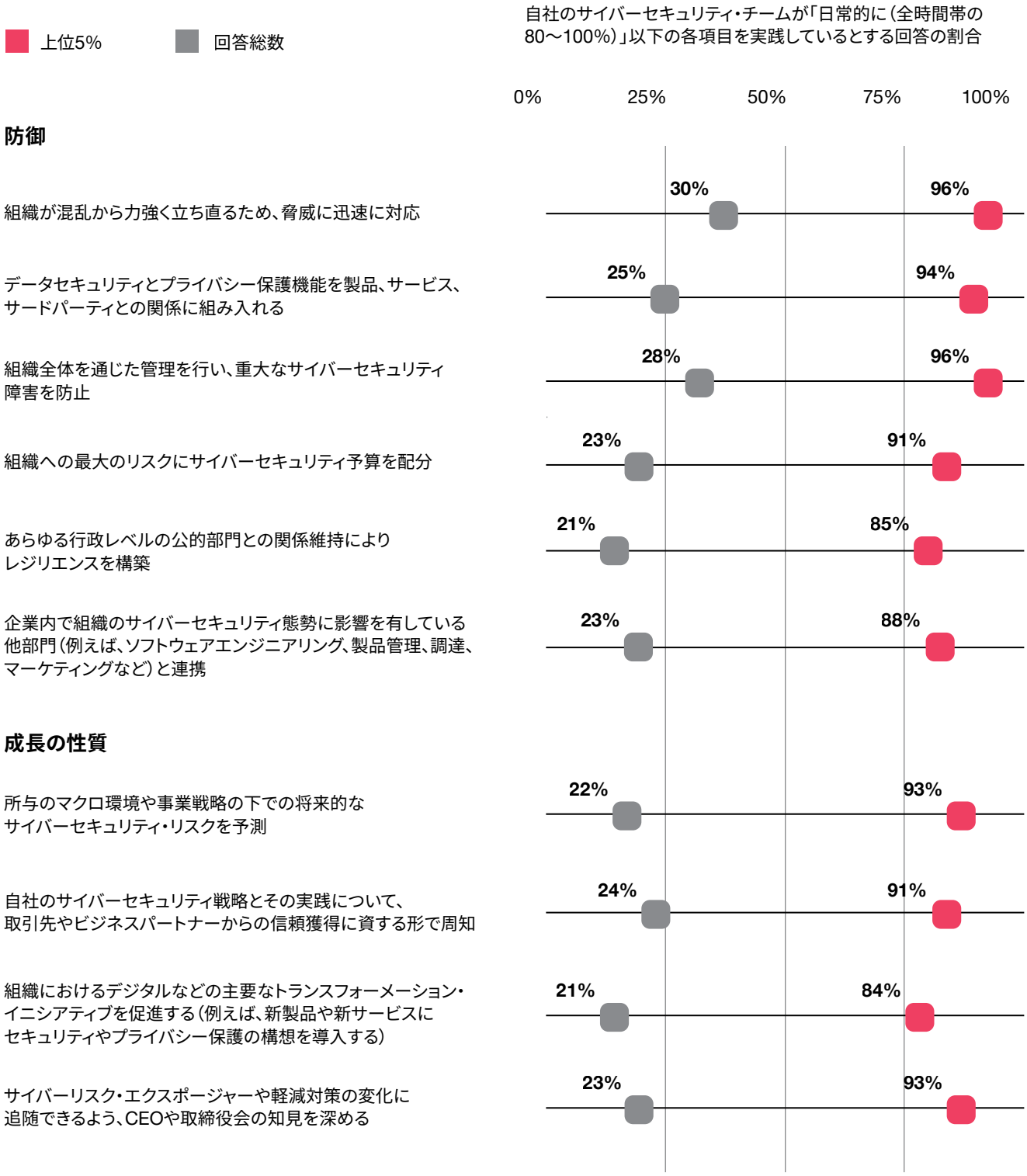
PwCが世界的な大企業のビジネスエグゼクティブとテクノロジー分野のエグゼクティブ（回答者の3割は売上高100億米ドル以上の企業）計3,876名を対象に実施した「Global Digital Trust Insights 2024」調査によると、サイバーセキュリティの分野には改善の余地が大いにあることが明らかになっています。

ここでの結論についてもう少し検討してみましょう。サイバーセキュリティ・インシデントに対処するコストと損害額が高額に上る攻撃の件数は増加を続けています。サイバーセキュリティ上での懸念事項のトップを占めるのはクラウド経由の攻撃ですが、クラウドサービスプロバイダーに関する課題への対処を目的とするリスクマネジメント計画が存在しないとする組織は全体のおよそ3分の1を占めています。最も重要なサイバーセキュリティ分野で「極めて満足」できる技術的能力を有すると評価したのは、回答者全体の半数に過ぎません。3割を超える企業が、サイバーディフェンスにおいて標準的とされる手順に従わないことがあると回答しています。

イノベーションの中核にセキュリティが確保されている状況を想像してみてください。それこそが、すばらしい発想と大胆な野心が興隆する場所なのです。そして、そこにいるCISOが、組織の目標と貴重な資産を守るために活躍している状況を想像してみてください。

一方で、所定の手順が的確に実行されているとする回答が179ありました。回答者の上位5%に相当するこうした「デジタルトラストの番人」である企業は、それ以外の企業が取りこぼしているメリットを享受しています。すなわち、インシデントの低減に加え、たとえ攻撃を受けた場合でも、被害額の抑制が可能になっています。効率化の進んだセキュリティソリューションは、リスク管理の負担軽減に寄与します。加えて、競合他社よりも高い生産性と急速な成長を実現できるポジションに立っています。なぜなら十分に保護されているという確信の下で、躊躇なく新しいテクノロジーを導入できるからです。

「デジタルトラストの番人」の環境を確認してみましょう



質問26：あなたの組織のサイバーセキュリティ・チームが以下のそれぞれをどの程度着実に実行しているか評価してください。
調査ベース：全ての回答者（3,876）
出所：PwC「Global Digital Trust Insights 2024」

テクノロジーが事業の中核に据えられる現在において、テクノロジーの防護は企業自体の防衛と変わらぬ重要性があります。このような事情を受け、PwCは2023年に、経営幹部レベルのエグゼクティブのためのプレイブックを作成しました。その目的は、経営幹部レベルの各エグゼクティブがCISOから提起された問題に的確に回答できるようにすることにあります。

今般、これを改訂して2024年版プレイブックを作成しました。2024年は重要な局面を迎えそうです。サイバーセキュリティは4つの意味で大きな転換点に直面しています。そして、その各々が破壊的な影響力を有している可能性があります。

- コスト削減が求められ、またマクロ経済に不透明感が増す状況下で、CxOがテクノロジーインフラストラクチャーと投資の近代化および強化を主張すること。
- ハイブリッド・サイバーセキュリティの脅威の増大に加え、サイバースパイとサイバー犯罪との境界が曖昧になっている現状を受けて、サイバーディフェンスが、国家レベルのセキュリティの領域に、かつてないほど全面的に組み込まれるようになったこと。
- 革新的な新技術である生成AIがディフェンスへの新たな脅威となると同時に、ディフェンスに未曽有の将来性をもたらしていること。
- サイバーセキュリティ・インシデントとリスク管理の開示強化を求める規制によって、透明性の向上と協力の強化が新たな段階に突入する可能性があること。

ビジネスは常に生まれ変わろうとしています。また、政策立案者は、新たな規制手続きについて検討しています。あなたの会社のシニアエグゼクティブも、自社組織をセキュアに保護する上で、同様に革新的であろうとしているでしょうか。あなた自身はどの程度果敢に取り組んでいますか。また、新たな取り組みとして何が考えられるでしょうか。

水準を分ける9つの指標：上位企業とその他の企業

上位5%の企業の特質

斬新なサイバーセキュリティ・イニシアティブを既に実行しており、それによるメリットを享受している企業の割合が**他の6倍多い**。

現在のサイバーセキュリティ技術能力にとても満足している企業の割合が**他の5倍多い**。

リスクマネジメント計画を継続的に見直し、クラウドリスクを軽減している企業の割合が**他の4倍多い**。

サイバーセキュリティ・レジリエンスのために日常的に行う活動を完成させている企業の割合が**他の9倍多い**。

出所：PwC「Global Digital Trust Insights 2024」

上位5%の企業に認められる傾向

上位企業は、より多くの予算をサイバーセキュリティ目的に投資している。例えば、**2024年のサイバーセキュリティ予算を増額した企業は85%に上り**（回答全体では79%）、そのうち15%以上の予算増を予定している企業は19%（回答全体では10%）に及ぶ。

過去3年間に経験した**サイバー攻撃のうちで最もダメージの大きかった**ものでも、被害額は10万米ドルを下回った（28%、回答全体では19%）。

生成AI（GenAI）を活用した新たなビジネス路線の開拓について、その可能性があると強く考える（49%、回答全体では33%）。

サイバーディフェンスの目的で**生成AIツールを導入する計画がある**（44%、回答全体では27%）。

「生成AIが壊滅的なサイバーセキュリティ攻撃を招く」という考え方には**同意しない**（33%、回答全体では22%）。

サイバーセキュリティ・リスク管理の再構築が急務に

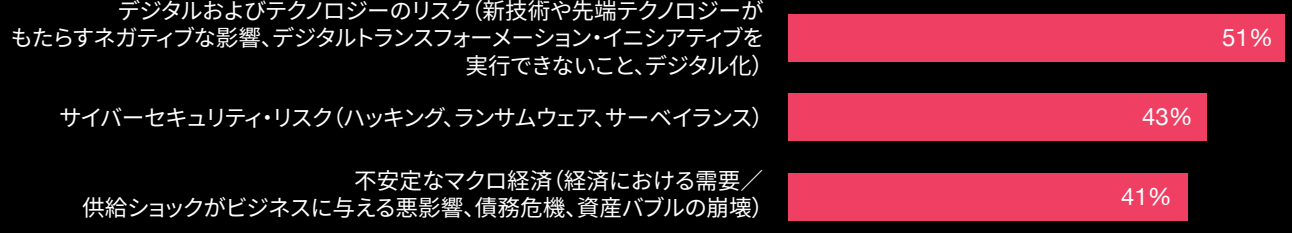
イノベーションには大胆な行動が伴います。そして、安全と安心を維持するために可能な限りの手段を実行したのだという認識、換言すれば、最も重大なサイバーセキュリティ・リスクを判断して対処できたという認識ほど、自分自身を力づけるものはありません。

PwCが実施した「Global Digital Trust Insights 2024」調査によれば、サイバーセキュリティ・リスクの軽減が2024年の最優先課題となっています。「サイバーセキュリティ・リスクの軽減」は、PwCが2023年に実施した第27回「世界CEO意識調査」では、最優先すべきリスクの第4位に後退しましたが、今回調査の回答では、「デジタルおよびテクノロジーのリスク」に次いで第2位となっています。しかも、今回調査の回答者の意識においては、「デジタルおよびテクノロジーのリスク」とサイバーセキュリティ・リスクとは不可分の関係にあります。

今日のビジネス環境にあっては、サイバーセキュリティに言及すること無しにデジタルトランスフォーメーションやデジタル再構築について語ることはできません。今回の調査の回答者がサイバーセキュリティへの脅威として最も強く懸念しているのは、今日のビジネストランスフォーメーションの根幹をなす2大テクノロジーであるクラウドおよびコネクテッドデバイスに対する攻撃です。

デジタルは2側面でリスク要因の最上位

今後12カ月間において優先的に取り組むリスク軽減対策（上位3項目）



質問1：以下のリスクのうち、あなたの組織が今後12カ月で優先して軽減対策に取り組むものを挙げてください（上位3項目）。
調査ベース：全ての回答者（3,876）
出所：PwC「Global Digital Trust Insights 2024」

サイバーセキュリティに対するこのような脅威の間には相互関係が存在しており、ひとたびシステムやネットワークへの悪意のあるアクターの侵入を許すと、破壊の限りを尽くされることが少なくありません。

クラウド攻撃に端を発した攻撃であっても、悪意のあるアクターは、システム内に潜伏してデータを集め、別の手段で被害を与える機会をうかがっているので、やがては進化して執拗な攻撃を加えられる可能性がかなり高まります。システム内のデータをこっそり抽出した上、ランサムウェア攻撃を仕掛け、たとえ身代金の支払いに応じたとしても、データを漏出させます（ハック・アンド・リーク）。

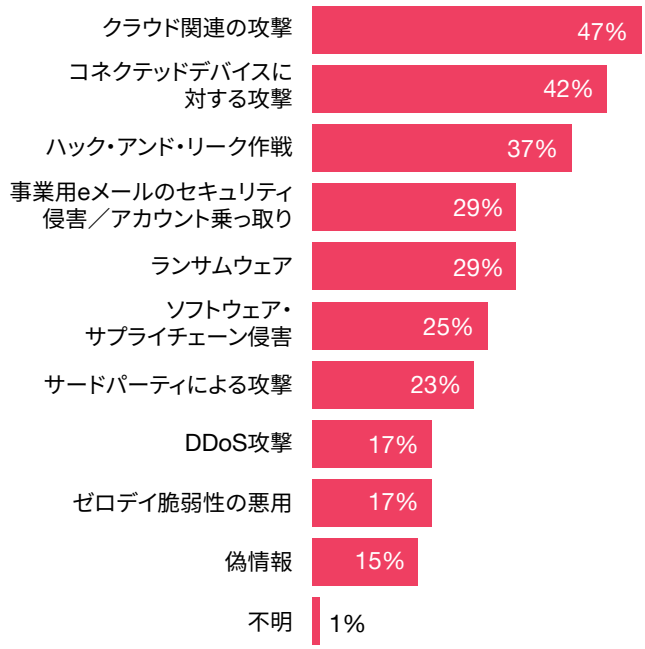
このような攻撃は、例外なく、それ自体の解決が難しいものです。全体として見れば、事業運営に激甚な損害を与え、企業の評判が大きく傷付けられることになります。大規模な攻撃の発生件数は増加傾向にあり、その規模も拡大しています。そして、対処に要するコストも増大しています。過去3年間に経験した最も重大な攻撃への対処費用が100万米ドルを超えたとする回答は、昨年調査の27%から36%に増加しました。

テクノロジーを活用して事業を再構築し変革しようとする動きに衰えの気配はありません。CEOの4割が、現状に安住していては、10年先にはもはや自分の会社が経済的に立ち行かなくなりかねないと懸念しています。このような状況下にあっても、再構築や変革の動きが止まることはありません。

CxOの課題：あなたの組織のサイバーセキュリティ・リスク管理は、世の中の動きに追随できていますか。

サイバー攻撃も含めたあらゆるものがコネクトされる

今後12カ月間で想定される最も重大なサイバー脅威

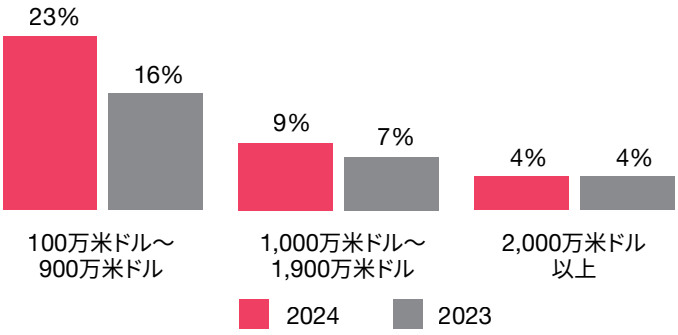


質問3：今後12カ月間において、あなたの組織が最も懸念するサイバーセキュリティ攻撃を以下から挙げてください（上位3項目）。
調査ベース：全ての回答者（3,876）
出所：PwC「Global Digital Trust Insights 2024」

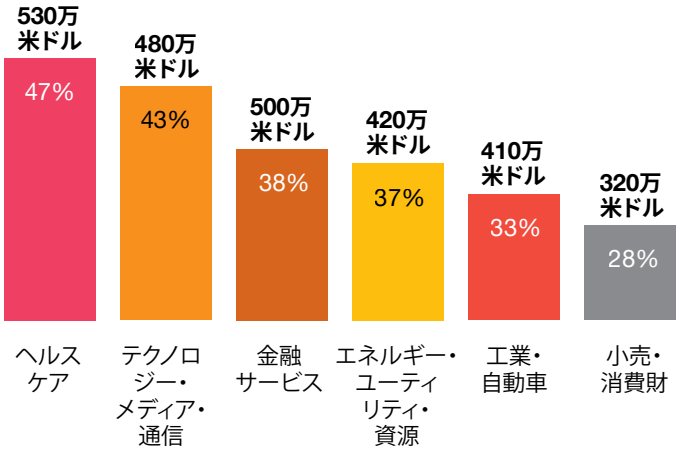
攻撃への対応コストは一層増大

過去3年間で、組織に最大のダメージを与えたデータ攻撃による推定被害額

被害額100万米ドル超の攻撃を受けたことがあるとする回答の割合
2024年全体＝36%、2023年全体＝27%



攻撃による被害額平均（100万米ドル）および100万米ドル以上のダメージを受けた攻撃の割合（%）（部門別）



質問5：過去3年間において最もダメージの大きかったデータ攻撃について考えた場合に、あなたの組織が被った損害はどの程度か推定してください。
調査ベース：セキュリティ、IT分野およびCFO回答者（1,651）
出所：PwC「Global Digital Trust Insights 2024」

サイバーセキュリティ・ツールの簡素化：悪意のあるアクターを破滅に追いやる方策

近代化と最適化は、2024年のサイバーセキュリティ投資における最優先課題です。ビジネスリーダーの約半数（49%）が、サイバーセキュリティ・インフラストラクチャーを含むテクノロジーの近代化を、また、45%が既存テクノロジーの最適化と投資を課題として選択しています。

PwCが2022年に行った調査では、特にCEOの間で、自らの組織が過度に複雑化しており、安全を維持するのが難しいという懸念が強いことが明らかになりました。この調査の時点では、32%の回答者が、簡素化に加え、マネージドサービスと内製化したサービスの役割分担の再編に取り組むために、テクノロジーベンダーを統合したと回答しています。

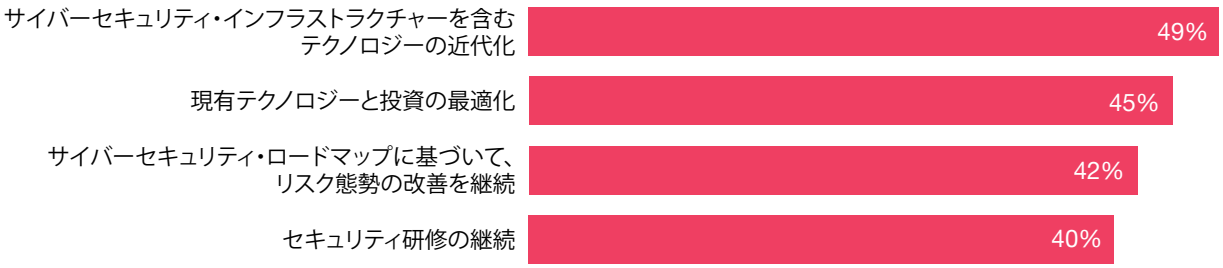
2024年調査では、サイバーセキュリティ技術ソリューションのための統合パッケージソフトを利用しているとの回答が44%、また、今後2年以内にこれに移行する計画があるとの回答が39%を占めました。回答者の5分の1近く（19%）が、サイバーセキュリティ・ソリューションが多すぎるので、統合が必要であるとしています。

主要8分野の全てにおいて、サイバーセキュリティ・ソリューションの技術能力に「とても満足している」と回答したIT担当者およびテクノロジー担当者が5%に過ぎなかったことは、過剰なポイントソリューションの存在が一因かもしれません。ソフトウェア間に連携がなければ、パフォーマンスが低下し、管理のために余分な時間が必要となり、サイバーセキュリティのリスク管理に不可欠とされる全体像の把握が困難になることがあります。

過去3年以内に100万米ドル以上の損害を伴うデータ攻撃を経験している回答者には、自社で利用している過多なサイバーセキュリティ・ソリューションの統合が必要であると認識している傾向が他よりも強く見られます。このことは、攻撃の被害経験者であれば身をもって実感できるでしょう。他方、まとまりのあるサイバーセキュリティ・ソリューション・パッケージソフトを利用している組織は、多額の損害を伴う重大な攻撃をより多く回避できています。

2024年のサイバーセキュリティ予算では、既存ツールの最大限の活用を目指す

ビジネスリーダー：今後12カ月間で優先するサイバーセキュリティ投資（上位3項目）



質問14b：今後12カ月間におけるサイバーセキュリティ予算配分に際して、あなたの組織では、次のどの投資を優先させますか（上位3項目）。
調査ベース：ビジネスの回答者（1,925）
出所：PwC「Global Digital Trust Insights 2024」

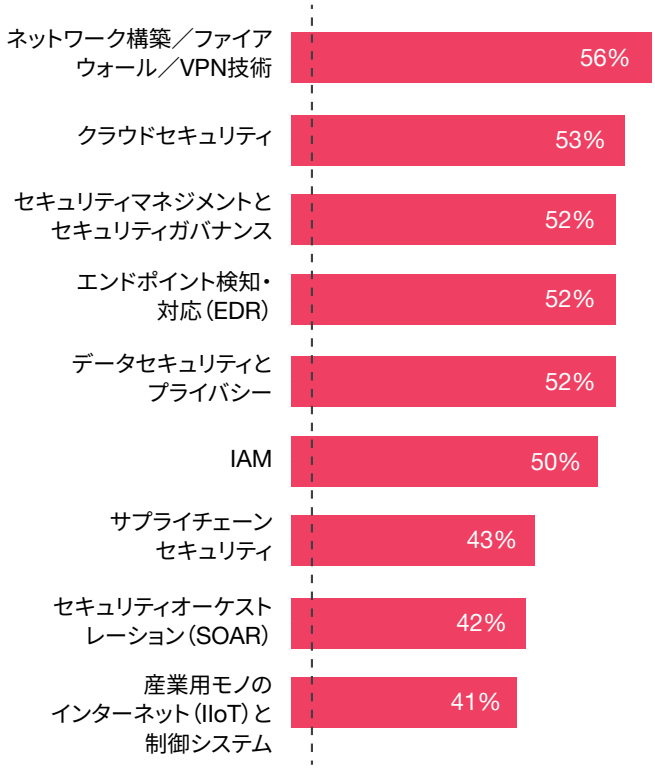
しかし、回答者は支出の手綱を緩めようとはしていません。サイバーセキュリティ支出を増加させるという回答が2023年調査の64%から上昇し、2024年調査では79%と全体の4分の3を超えており、特に年間売上高50億米ドル以上の大企業ではこのような回答が多くなっています。さらに、前年比15%を超えるサイバーセキュリティ予算の増額を計画しているとの回答は、売上高500億米ドル以上の企業、テクノロジー・メディア・通信分野の企業、または来年度に大幅な増収を予想している企業に多く見られます。

サイバーセキュリティ投資がIT、OT、オートメーション予算全体に占める割合も一層拡大しています。平均増加率を全体的に見ると、2023年における予算の11%に対し、2024年における予算では14%となっています。

CxOの課題は、ツールの不足でも投資の欠如でもありません。むしろ、どのようにすれば最適な投資ができるかを考えることです。あなたの会社のITアーキテクチャーは、適切に保護できないほどに複雑化していないでしょうか。防御体制の間隙を脅威アクターに容易に見破られることはないでしょうか。

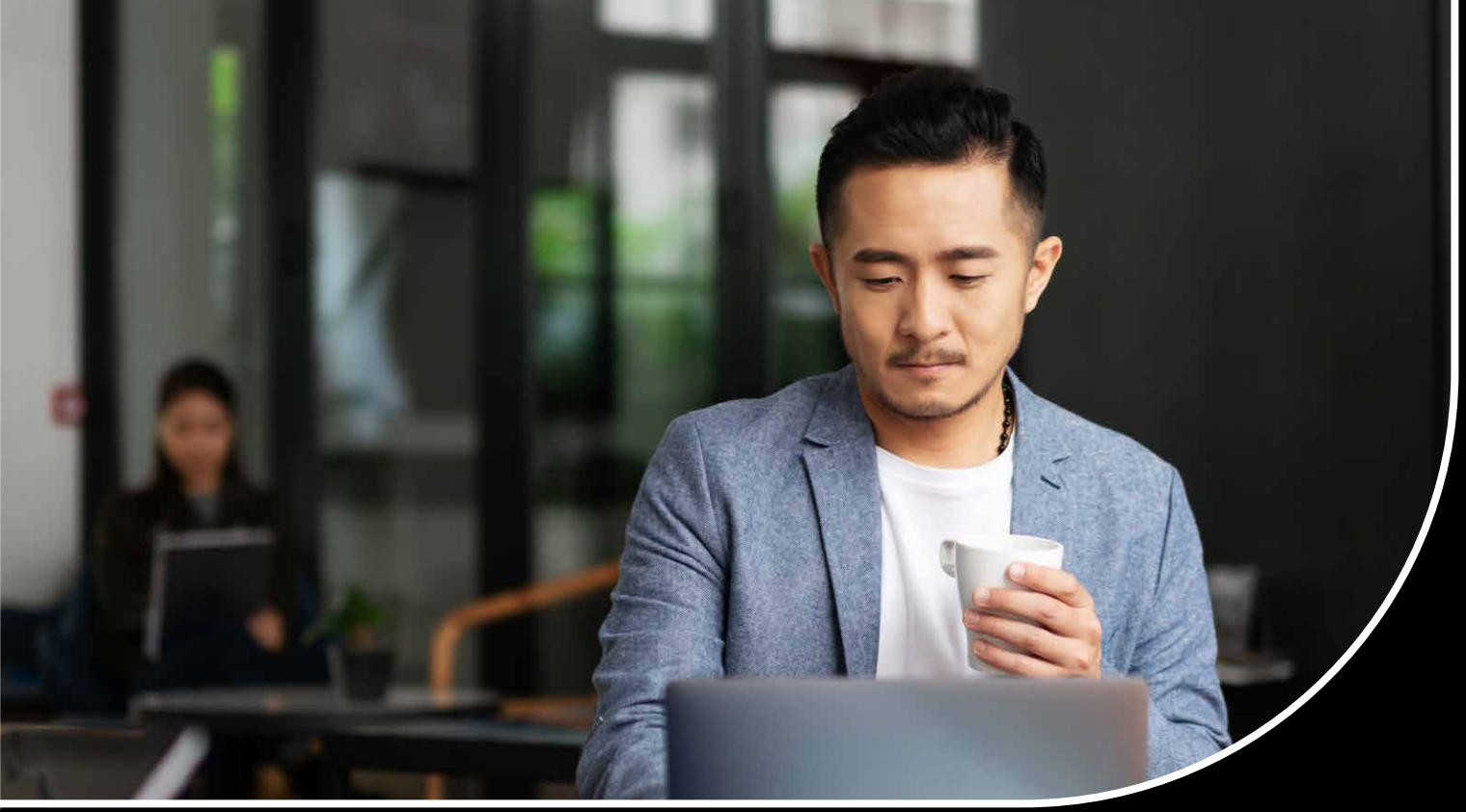
サイバーセキュリティ技術能力に満足しているのは半数のみ

主要なサイバーセキュリティ分野における組織的な技術能力



セキュリティ担当者とIT担当者のうち、全ての分野でとても満足していると回答したのはわずか5%

質問23：以下の各分野について、あなたの組織の技術能力にどの程度満足していますか。
調査ベース：セキュリティおよびIT回答者（1,517）
出所：PwC「Global Digital Trust Insights2024」

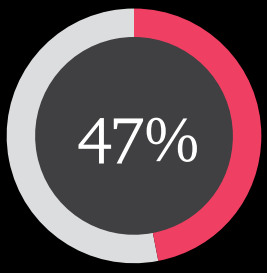


クラウドセキュリティ：不十分な管理体制

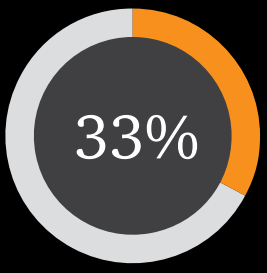
クラウドを活用する目的は、常に事業のイノベーションにあります。例えば、クラウドを活用すれば、世界中どこにいても共同開発が可能になり、よりフレキシブルな新しい働き方が実現します。さらに新たなビジネスモデルの考案、事業運営の改善に資するテクノロジーの結合、取引先や顧客へのサービス改善につなげることができます。

回答者の約半数（47%）が、サイバーセキュリティ・リスク上の懸念事項のトップにクラウドセキュリティを挙げています。悪意のあるアクターが入り込む方法には事実上際限がありません。組織として、あらゆる場面を制御できるようにすべきです。すなわち、アイデンティティとアクセス、ラテラルムーブメント、eメールアカウント、ポータルサイト、アプリケーション、機密情報、顧客インタラクション、オペレーティングシステム、コネクテッドデバイスなど、挙げればきりがありません。

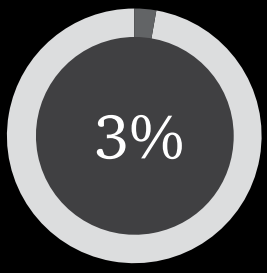
クラウドセキュリティ：最大の脅威であり、最大の投資対象でありながら、管理体制は不十分



最大の脅威



サイバーセキュリティ目的では最大の投資



リスクマネジメント計画を実行し継続的にアップデート

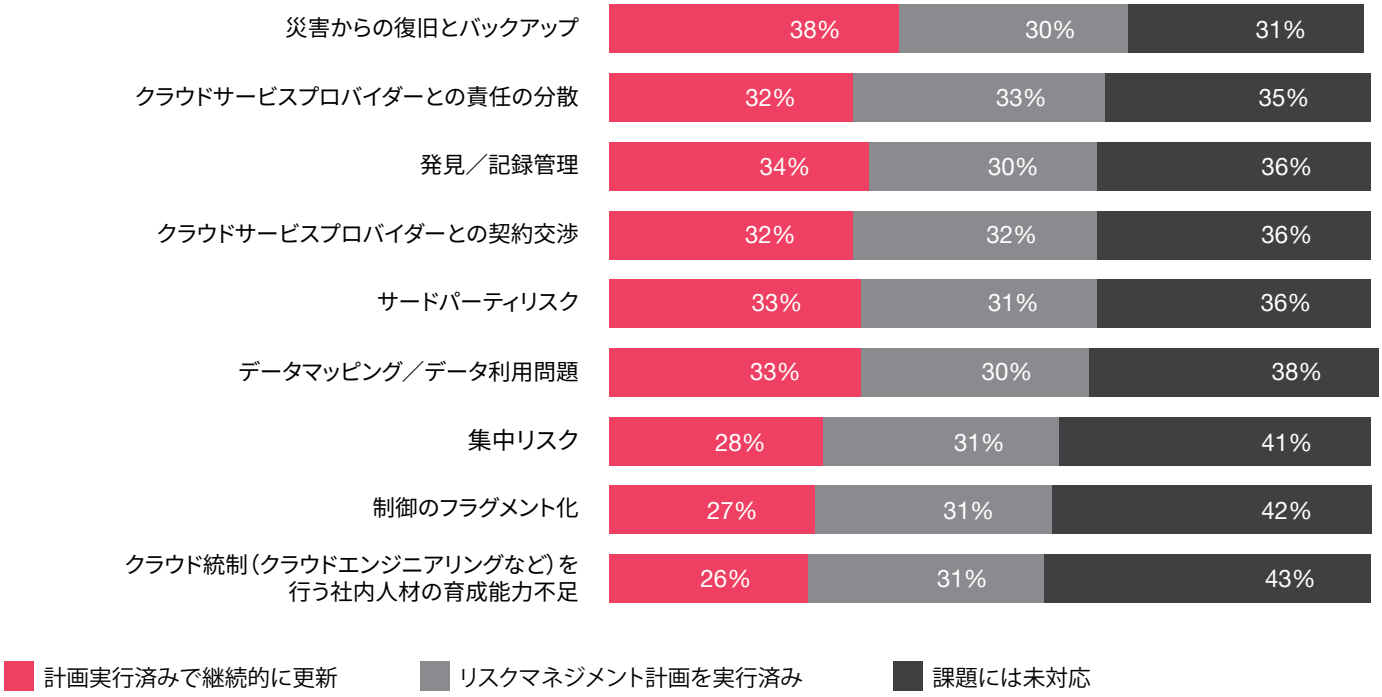
質問3：今後12カ月間で、以下のサイバーセキュリティ脅威のうち、あなたの組織が最も懸念するものを挙げてください（上位3項目）。
調査ベース：全ての回答者（3,876）
質問14a：あなたの組織で今後12カ月間のサイバーセキュリティ予算の配分を行う際に、優先される投資目的を以下から挙げてください（上位3項目）。
調査ベース：IT回答者（1,919）
質問19：あなたの組織は、クラウドサービスプロバイダーに関連する以下の課題にどの程度取り組んでいますか。
調査ベース：クラウドプロバイダーのユーザー回答者（3,648）
出所：PwC「Global Digital Trust Insights 2024」

今回の回答者の多く（42%）は複数のクラウドを利用しています。しかし、複数の（ハイブリッド）クラウドを利用すると、クラウドセキュリティ上の懸念が増大します。このような回答者の54%が、最も急を要するサイバーセキュリティ・リスクはクラウドであると指摘しています。また、ハイブリッドクラウドのユーザーは、翌年に行うセキュリティ投資における3つの優先項目の中にクラウドを含める傾向が他のいずれよりも強く認められます（全回答者が33%である一方、ハイブリッドクラウドユーザーは36%）。

しかし、ほぼ全て（97%）の組織は、クラウドのリスクマネジメント計画において隙間が生じています。クラウドセキュリティ分野の9項目全てをカバーする最新の計画を維持しているとする回答は、全体の3%しかありません。例えば、断片化した制御がもたらすリスクに対処できていないとする回答が42%、集中リスクへの対応計画がないとする回答が41%、サードパーティクラウドのリスクに対応できていないとする回答が36%ありました。

あまりに多いクラウドセキュリティ・リスクに対し不足するリスク管理計画

クラウドサービスプロバイダーの問題に対する組織のポジション



質問19：あなたの組織は、クラウドサービスプロバイダーに関連する以下の課題にどの程度取り組んでいますか。
調査ベース：クラウドプロバイダーのユーザー回答者（3,648）
出所：PwC「Global Digital Trust Insights 2024」

「デジタルトラストの番人」である上位5%の組織では、リスクマネジメント計画を継続的に見直すことによってクラウドリスクの軽減が図られている可能性が、他の4倍高くなっています。しかしながら、それ以外の組織においては、未だにこのような不可欠な対応がほとんど行われていません。

CxOの課題：CxOが連携して、またクラウドセキュリティ・プロバイダーと協力して、どのようにすれば、組織のシステムにおいて最重要のエントリーポイントや資産の防御を、クラウドを介して進めることができるでしょうか。

サイバーディフェンスのための生成AIが増加の一途

回答者の7割近くが、サイバーディフェンスに生成AI（GenAI）を使うようになると予想しています。人間が主導するサイバーセキュリティ攻撃は、その膨大な件数が継続的に増加し、複雑性も強まる一方です。現時点ではサイバーセキュリティ・チームはこれに圧倒されていますが、生成AIツールの活用により、苦境を打開できるかもしれません。

サイバーディフェンスのための生成AI

69%

3分の2超（69%）が、サイバーディフェンスを目的として生成AIを今後12カ月以内に利用するかもしれないと回答。

47%

半分近く（47%）が、サイバーセキュリティ・リスクの検出とその軽減のために生成AIを既に利用していると回答。

21%

5分の1（21%）が、公表後わずか数カ月に過ぎない生成AIがサイバーセキュリティ計画に役立っていると回答。

質問7：生成AIに関する以下の記述はどの程度当てはまりますか。
調査ベース：全ての回答者（3,876）
出所：PwC「Global Digital Trust Insights 2024」

プラットフォーム運営者は、自社のサイバーセキュリティ技術ソリューションと並行して大規模言語モデル（LLM）のライセンスを与えています。Microsoft Security Copilotが目指すのは、セキュリティ動態管理、インシデント対応、セキュリティ報告を行うための生成AI機能を提供することです。Googleからは、これと同様の使用事例を想定したSecurityAI Workbenchが発表されています。

多くのベンダーが、生成AIの限界を押し広げるべく、その潜在性を試行しているところです。defenceGPTが広範囲に利用されるまでには、もうしばらく時間を要しそうです。その一方で、サイバーディフェンスでの生成AIの利用に関しては、脅威の検知と分析、サイバーセキュリティ・リスクとインシデントの報告、適応制御の3つの有望な分野が開けています。

- **脅威の検知と分析** 生成AIは、脆弱性の悪用をプロアクティブに検知し、その程度（リスクにさらされているのは何か、何が既に侵害されたか、どのようなダメージを受けたか）を速やかに評価し、さらにディフェンスと修復のために講じ得る実証済みの方策を提示することにおいて真価を発揮しそうです。生成AIを利用すれば、従前のシグネチャベースの検知システムをすり抜けてきたパターンと異常の検知およびIoCの察知が容易になります。
- **サイバーセキュリティ・リスクとインシデントの報告** 生成AIの利用によって、サイバーセキュリティ・リスク報告とインシデント報告も大幅に簡素化されるかもしれません。自然言語処理（NLP）を活用すれば、技術的なデータを専門外の人々にも理解できる簡潔な内容に生成AIを利用して変換することが可能になります。インシデント対応報告、脅威インテリジェンス、リスクアセスメント、監査や規制の遵守に生成AIを活用できるかもしれません。生成AIを活用して、誰にでも理解できる用語による提案や、さらには不可解なグラフの簡潔なテキストへの変換も行うことができます。
- **適応制御** クラウドやソフトウェアのサプライチェーンの安全を維持するには、セキュリティポリシーやセキュリティ制御を常に最新の状態に保たなければなりません。今日これを行うのは非常に厄介なことです。機械学習アルゴリズムと生成AIツールによって、ある組織が直面している脅威の特徴、その組織のテクノロジーや事業目的に適合するセキュリティポリシーや自動化制御を提案・検証し、起案できるようになる日が遠からずやってくるかもしれません。

CxOの課題：新しいツールをどのように駆使すれば、あなたの組織や社会がこれまでになかったような急激なリスクに見舞われるのを防ぐことができるでしょうか。生成AIの利用に際しての倫理や責任を果たすためには何をすべきでしょうか。

規制：安全な活動と成長の場を確保

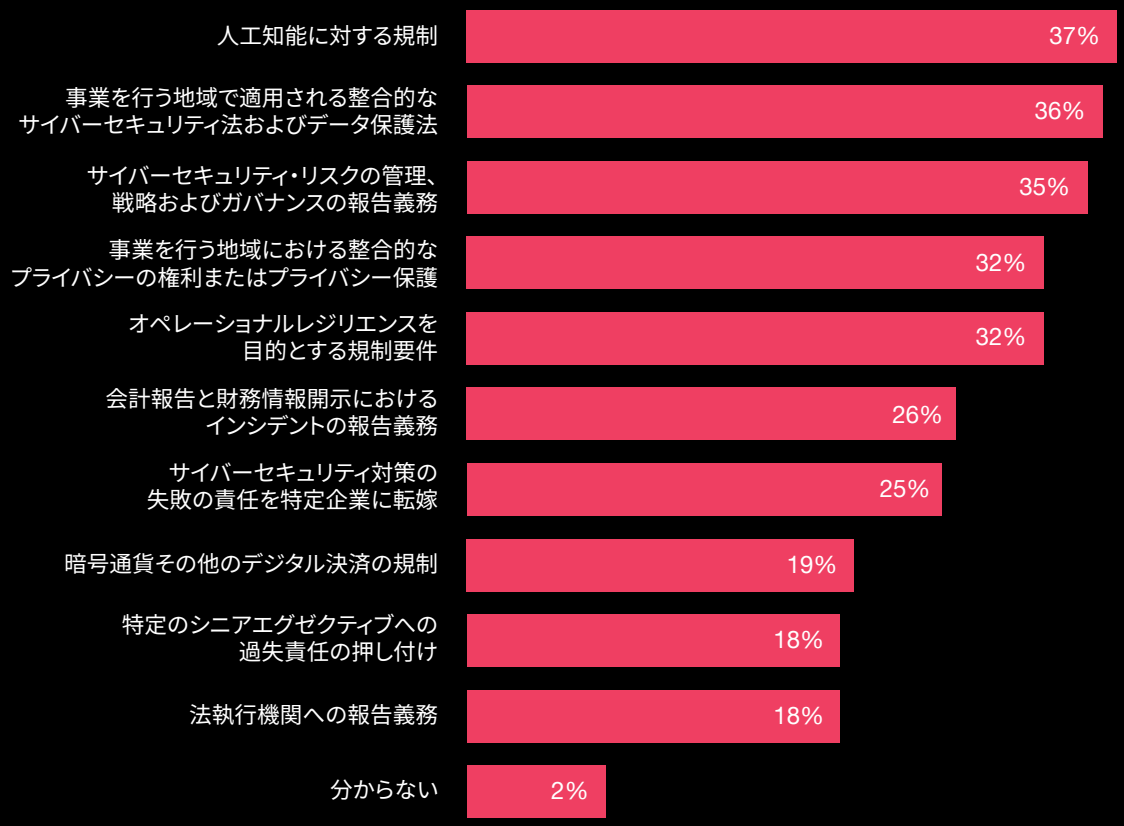
新たな規則や規制は収益の障害となるという見解が主流ですが、少なくとも回答者の3分の1は以下のような見解も述べています。すなわち、監督当局が提案する安全措置を受けて、企業はより思い切った探求、試験、発明や競争が可能になり、リーディングカンパニーは規制の要件を乗り越えて進むことで競争上優位に立てる可能性があるということです。

今年実施した調査では、回答者のおよそ3分の1が、自らの組織が将来的に成長を維持していくために、4つのタイプの規制が非常に重要であると考えています。すなわち、①AIに対する規制（37%）、②サイバーセキュリティとデータプロテクション関連法規の整合化（36%）、③サイバーセキュリティ・リスクの管理、戦略とガバナンスに関する報告義務（35%）、④オペレーショナルレジリエンス要件（32%）の4つです。

透明性向上に関する規制は、世界各国でますます強化されつつあります。米国証券取引委員会（SEC）が新たに設けた規則では、投資家に重大な影響が及ぶ恐れがあると見られるサイバーセキュリティ攻撃についての開示が求められています。デジタル市場法とデジタルサービス法では、データプラクティスおよびアルゴリズムによる意思決定における透明性が求められています。そして、EUで審議中のAI規制法案や生成AIの規制など、AIについて定める規制が間もなく施行される見込みです。

サイバーセキュリティに変化をもたらす可能性がある規制

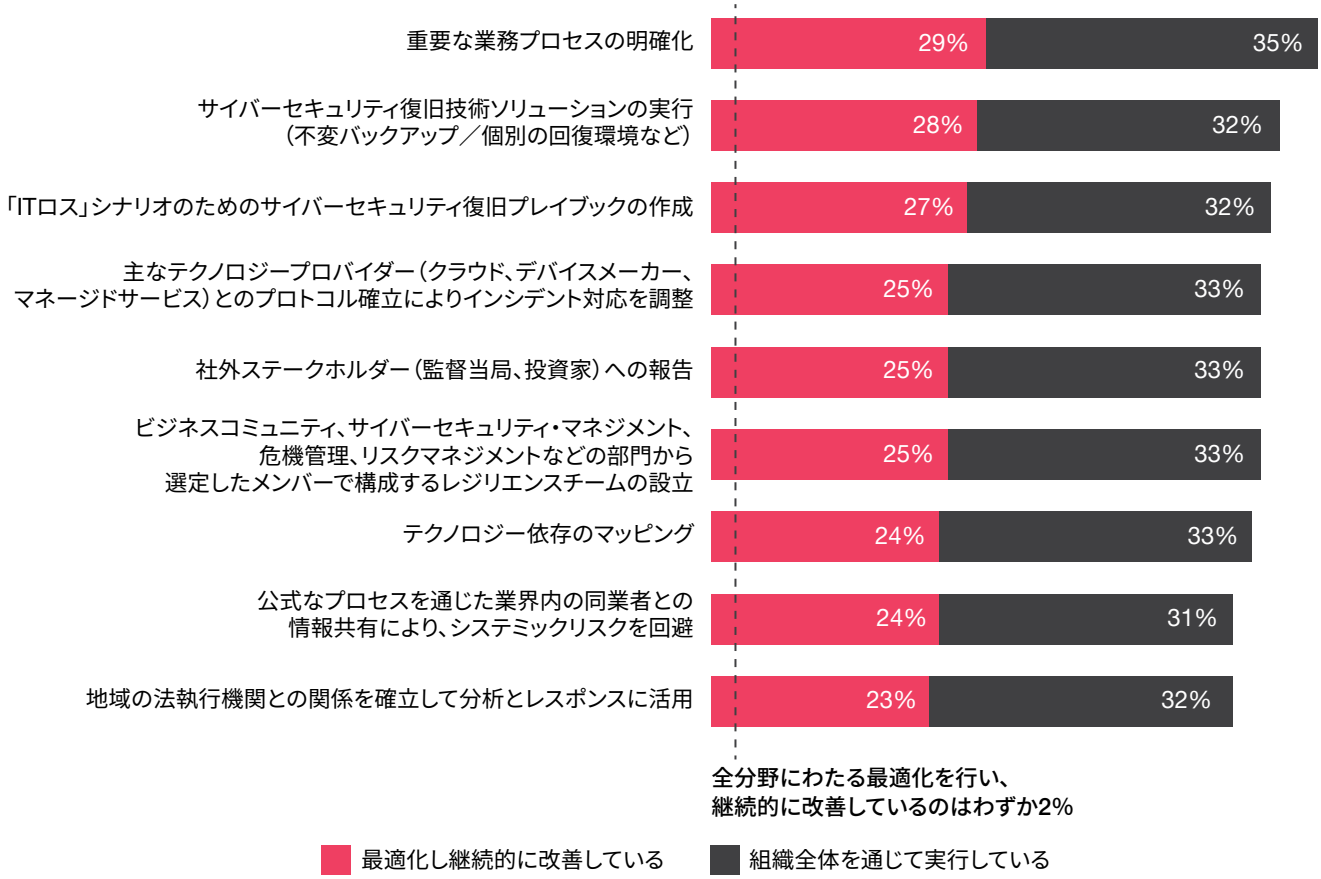
組織の将来的な収益の増加に最も強く影響する規制目標と原則（上位3項目）



質問24：以下に記す提案されている規制目標と原則のうち、あなたの組織における将来的な収益成長力の確保に最も強く影響しそうなものを挙げてください（上位3項目）。
調査ベース：全ての回答者（3,876）
出所：PwC「Global Digital Trust Insights 2024」

遅々として進まないサイバーセキュリティ・レジリエンス

主要なサイバーセキュリティ・レジリエンス対策の実施状況



質問8：あなたの組織では、以下に記すサイバーセキュリティ・レジリエンス対策をどの程度実施するか、または実施を計画していますか。
調査ベース：全ての回答者（3,876）
出所：PwC「Global Digital Trust Insights 2024」

オペレーショナルレジリエンスは、もう一つの重要なテーマです。監督当局者は、相互に関係性がある複雑なリスクという課題に取り組む場合に、CxOチームの多くが現在でも習慣的に行っているようなアプローチ（すなわち、各々の事業部門が抱えるリスク特性を別個のものとして扱うような縦割り型の仕事の進め方）には大きなリスクを伴うものと認識しています。さらに、デジタル・オペレーショナル・レジリエンス法などの規定においては、組織が壊滅的なインシデントを経験するごとに、組織の適応性を向上し、フレキシブルでより強力なものとする中核的な要素との統合レジリエンスが新たに要求される傾向が強まっています。

4分の3もの多くの回答者が、このような規制を遵守するためには、かなりの費用と時間を要するだろうと予想しています。しかし、規制が施行される初期段階から、企業が規制プロセスに頻繁に参画しているならば、高額な費用と収益への悪影響を回避できるかもしれません。すなわち、法執行機関との会合を設けることであり、例えば、パブリックコメントに参画し、さらには監督当局との協議に臨んで、提案されようとしている通達の作成を支援し、影響を与えることです。

CxOの課題：不確実な規制の下、セキュリティとプライバシーを計画的に維持しつつ、変革していく余地をあなたの組織につくり出すことができますか。どのようにしたら、このような新しい規制環境を、競争上の優位性を確保するための根源に転化することができるでしょうか。

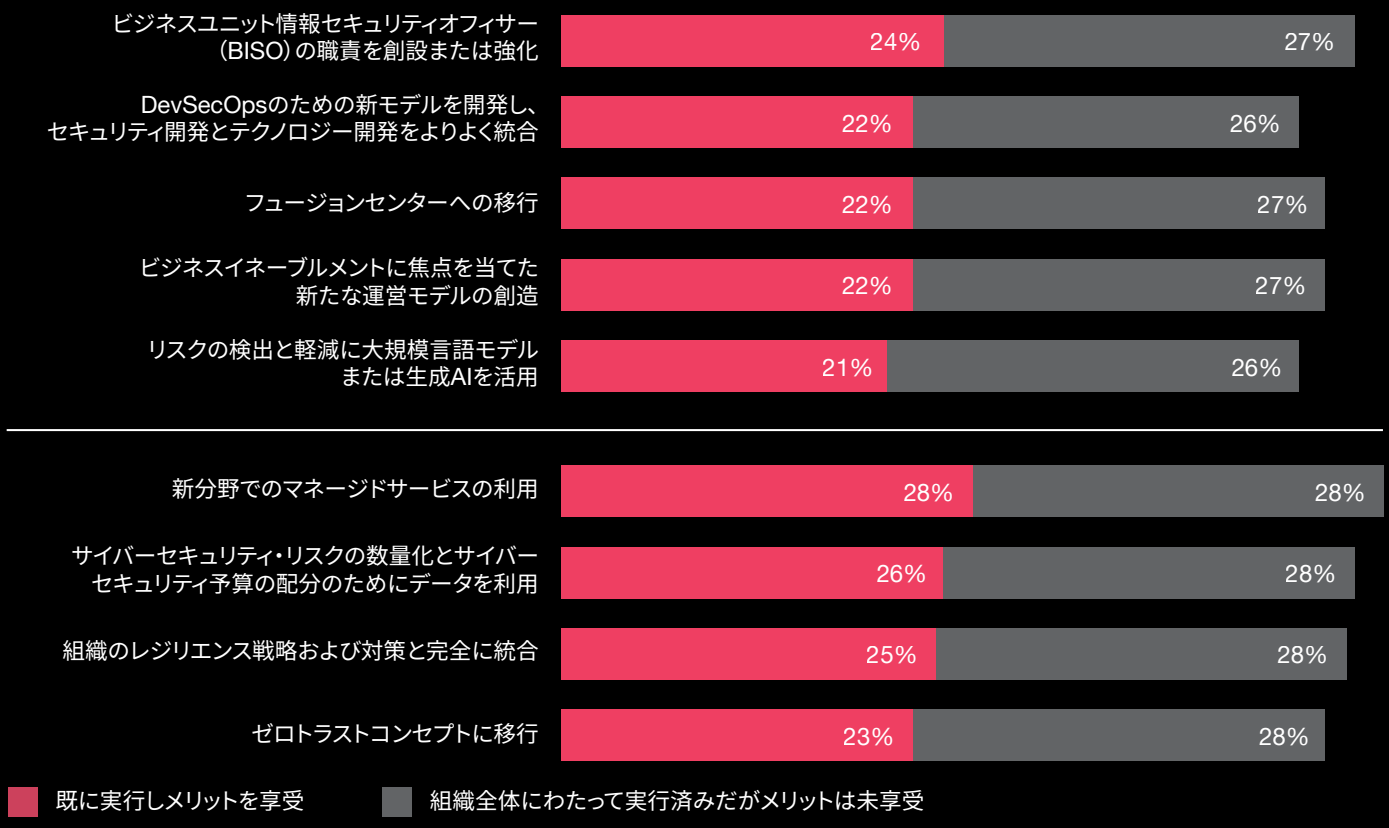
旧態依然のサイバーセキュリティを敢えて打破する：CxOプレイブック2024

あなたの組織で、これまでと変わらぬ業務を続けることはもはやできません。それでも、2024年の「Global Digital Trust Insights」調査で明らかになったように、ほとんどの企業が旧態依然としたサイバーセキュリティに安住しています。断片化したイニシアティブ、複雑化を強める一方のテクノロジー、隙間のあるリスクマネジメント計画それ自体が、リスク要因となっています。真に信頼できるサイバーセキュリティの確立に至る道筋には、期待通りの成果が得られない変化やプロジェクトなど、さまざまな困難が横たわっています。

PwCは2023年のプレイブックで、CxOエグゼクティブがパートナーとして連携して対処すべき重要課題を明らかにしました。このような状況は今日でも変わっていません。

あなたの組織のサイバーセキュリティ・プログラムは、サイバーセキュリティとビジネスのどちらをより重視していますか？

次のグラフの上半分のイニシアティブはサイバーセキュリティにフォーカスしたもの、下半分はビジネスにフォーカスしたものです



質問10：あなたの組織では、以下に記すサイバーセキュリティ・イニシアティブをどの程度実行するか、または実行する計画がありますか。
調査ベース：全ての回答者（3,876）。分析手法は因子分析による。
出所：PwC「Global Digital Trust Insights 2024」

2024年には、次のような課題が待ち受けています：

CxOリーダーとして、思い切って組織の閉塞感を打破し、組織にとって最も重要な決断を大胆に下す覚悟はできていますか?

また、あなたの会社の目標達成を妨げているハードルを最終的に解消できるような大胆な想像の転換ができるでしょうか?

最善の選択のために、既に歩み出した企業もあります。そこには多くの選択肢が幅広く存在しています。

あなたの組織にとって、何が正しい選択でしょうか。

従来と異なる言葉での働きかけ

CISO　CFO　法務

あなた自身をイノベーションの中核に置くということは、社内のリーダーシップ層の居場所において、あなたの行動に対して怖気づかないよう諭すことを意味します。「サイバーランドスケープ」「アタックサーフェス」はもちろん、「ゼロトラスト」といった関係者にしか通用しない言葉は、専門外の人々を必要以上に当惑させるだけです。

ビジネスの会話、技術的な会話、金融の会話や日常的な会話でも、サイバーセキュリティについて語るようにしましょう。また、年次有価証券報告書などの文書でも、あなたの会社の取引先、投資家、ビジネスパートナーに対して、情報を提供し、参加を促すように語りかけましょう。現在のような変革の真っただ中にあっては二律背反や緊張、混迷が発生するのは致し方ないことですが、普通の言葉で語れば、エグゼクティブたちがこのような問題をもっと巧みに処理できるようになるかもしれません。

大胆かつ新しい方法で、サイバーリスクを管理

CISO　CRO　内部監査　CCO　COO

サイバーセキュリティ・リスク・モデリングの手法を高度化しましょう。例えば、脅威のスキャニングにおいて、あなたの会社の各部門や会社のビジョン、戦略に特化した手法を活用することなどです。賞与支給対象の全従業員に対して、リスクに関連する成果にインセンティブを与える仕組みを導入して、リスクカルチャーを醸成しましょう。会社の弱点を見つけ出して補強するための新しい方法を考案しましょう。

おそらく、個別のセキュリティリスク調査に対してインセンティブを与える現代版のバグ報奨金プログラムを創設するとよいでしょう。そして、クラウドファーストの一元管理IDソリューションを調達して活用し、会社の目標である事業拡大をセキュアに進めましょう。

安全策の構築

CISO　CIO　法務　リスク監査

規制の遵守だけを語るのではなく、信頼を勝ち取る言葉で語りましょう。新しい規則の導入が予定されているときは、その規則に影響を与える機会を求めて、早期から積極的に参画しましょう。そして、このような規則が事業の成功の妨げになるのではなく、成功に資するようにしましょう。あなたの会社の経験とインサイトは、AI、メタバース、暗号通貨、プライバシーなどの規制を巡るホットな課題に大きく貢献できるかもしれません。一般の人々と同様に、監督当局者もまた、サイバーセキュリティやテクノロジーの仕組みに困惑している可能性があることを忘れてはなりません。

創造的な思考に向け、退屈な作業からチームを解放（オートメーション、生成AI、マネージドサービス）

CISO CIO CTO CRO COO

オートメーション化や生成AI、マネージドサービスのメリットの一つは、常に目配せできるようになることです。もう一つのメリットは、チームが日常的に行う雑事をこれらのシステムで代行できることです。チームのメンバーを退屈な作業の過酷さから解放することにより、新たなサイバーセキュリティの脅威について熟考し、進化を続ける脅威を阻むための新たな手段を創出する時間と余裕が得られるかもしれません。

サイバーセキュリティを取締役会の主要議題に

CISO 取締役 CEO

多くの企業において、また多くのエグゼクティブ調査において、サイバーセキュリティはリスクレジスターの最上位に位置付けられています。しかし、あなたの会社の取締役会では、サイバーセキュリティが主要議題として検討されているでしょうか？　サイバーセキュリティ・リスクとその制御に関する情報だけでなく、主要なイニシアティブを戦略的にとっていくことが事業の成長と収益の増加にどのように寄与しているかについても良質な情報が得られているでしょうか。セキュリティは、組織が行うあらゆるもの（エグゼクティブたちの議論では必ず取り上げられそうな金融、成長、人事、技術などのビジネス分野）の基礎となります。

サイバーセキュリティ・プログラムを直視することは大胆な行動であるかもしれません。

事業オーナーの視点から思考

CISO CEO

ビジネストランスフォーメーションとサイバーセキュリティ・トランスフォーメーションとは別物ではありません。これらに相違点はないのです。いまやCISOとCEOとが力を合わせ、事業オーナーの立場に身を置いて、事業全体的な取り組みとしてサイバーセキュリティを進んで活用する必要があります。

財務記録、個別受託調査（プロプライエタリー調査）、アプリケーション開発、取引先データなど、全ての局面において、不正閲覧や不正使用からの保護は喫緊の課題です。同時に自社ブランドの保護も不可欠です。サイバーセキュリティを通じてイノベーションを促進し、費用の節減と事業の成長を実現することができます。ここにサイバーセキュリティの存在意義があるのです。

本調査について

「Global Digital Trust Insights 2024」は、2023年5月から7月にかけて、ビジネス、テクノロジー、セキュリティ分野のエグゼクティブ（CEO、企業役員、CFO、CISO、CIO、CxO役員）3,876名を対象に実施した調査です。

回答者の40%は売上高50億米ドル以上の大企業の経営層、そして重要なことに、その30%は売上高100億米ドル以上の企業の経営層です。

回答企業の業種は、製造業（20%）、金融サービス（20%）、テクノロジー・メディア・通信（19%）、小売・消費財（17%）、エネルギー・ユーティリティ・資源（11%）、ヘルスケア（9%）、政府・公共サービス（3%）と多岐にわたっています。

回答者は71カ国に拠点を置いており、その地域別分布は、西欧（32%）、北米（28%）、アジア太平洋（18%）、中南米（10%）、東欧（5%）、アフリカ（4%）、中東（3%）となっています。

「Global Digital Trust Insights」調査は、以前は「グローバル情報セキュリティ調査（GSISS）」として知られていたものです。今年で26年目を迎える本調査は、サイバーセキュリティの動向に関する年次調査として最も長い歴史を有しています。また、サイバーセキュリティ業界で最大規模の調査でもあり、セキュリティおよびテクノロジー分野のエグゼクティブだけでなく、ビジネス部門のシニアエグゼクティブの参画を得ている調査としても他に類を見ないものです。

本調査は、PwCで世界の市場調査とインサイト提供を担当するCentre of ExcellenceであるPwCリサーチが実施しました。

日本のお問い合わせ先

PwC Japanグループ

www.pwc.com/jp/ja/contact.html

綾部 泰二（Taiji Ayabe）
PwC Japanグループ
サイバーセキュリティ&プライバシー リーダー
PwC Japan有限責任監査法人
上席執行役員 パートナー

丸山 満彦（Mitsuhiko Maruyama）
PwCコンサルティング合同会社
パートナー

上杉 謙二（Kenji Uesugi）
PwCコンサルティング合同会社
ディレクター

エレドン ビリゲ（Bilig Eredon）
PwCコンサルティング合同会社
マネージャー

牧 言美（Kotomi Maki）
PwCコンサルティング合同会社
アソシエイト

岡村 彰太（Shota Okamura）
PwCコンサルティング合同会社
アソシエイト

pwc

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびアシュアランス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約11,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、社会における信頼を構築し、重要な課題を解決することをPurpose（存在意義）としています。私たちは、世界151カ国に及ぶグローバルネットワークに約364,000人のスタッフを擁し、高品質な監査、税務、アドバイザリーサービスを提供しています。詳細は www.pwc.com をご覧ください。

本報告書は、PwCメンバーファームが2023年9月に発行した『Global Digital Trust Insights 2024』を翻訳したものです。
翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
オリジナル（英語版）はこちらからダウンロードできます。 https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

日本語版発刊年月：2024年3月　　管理番号：I202401-02