pwc

サイバー有事に備えた CxO結束の必要性

『Global Digital Trust Insights 2023年版』調査結果より

www.pwc.com/jp

サイバーセキュリティ対策は、進展を遂げています

誰にも予想できなかった急速な環境の変化を目の当たりにして、ビジネスリーダーたちは近年、居心地のよい環境から脱して、自分の会社を、また自分自身を、新たな世界へと追い立ててきました。例えば、オフィスからリモートワークへの移行、クラウドの推進、サプライチェーンのデジタル化などです。このような新たな試みに伴って、サイバーリスクがこれまでになく高まっています。

情報セキュリティ最高責任者（CISO）とサイバーセキュリティチームは、こうした課題に立ち向かっています。CxOは、自らの果敢な経営判断に伴って、組織が直面するサイバーリスクの脅威が増大していることを認識しており、CISOやサイバーセキュリティチームとの連携を強めています。

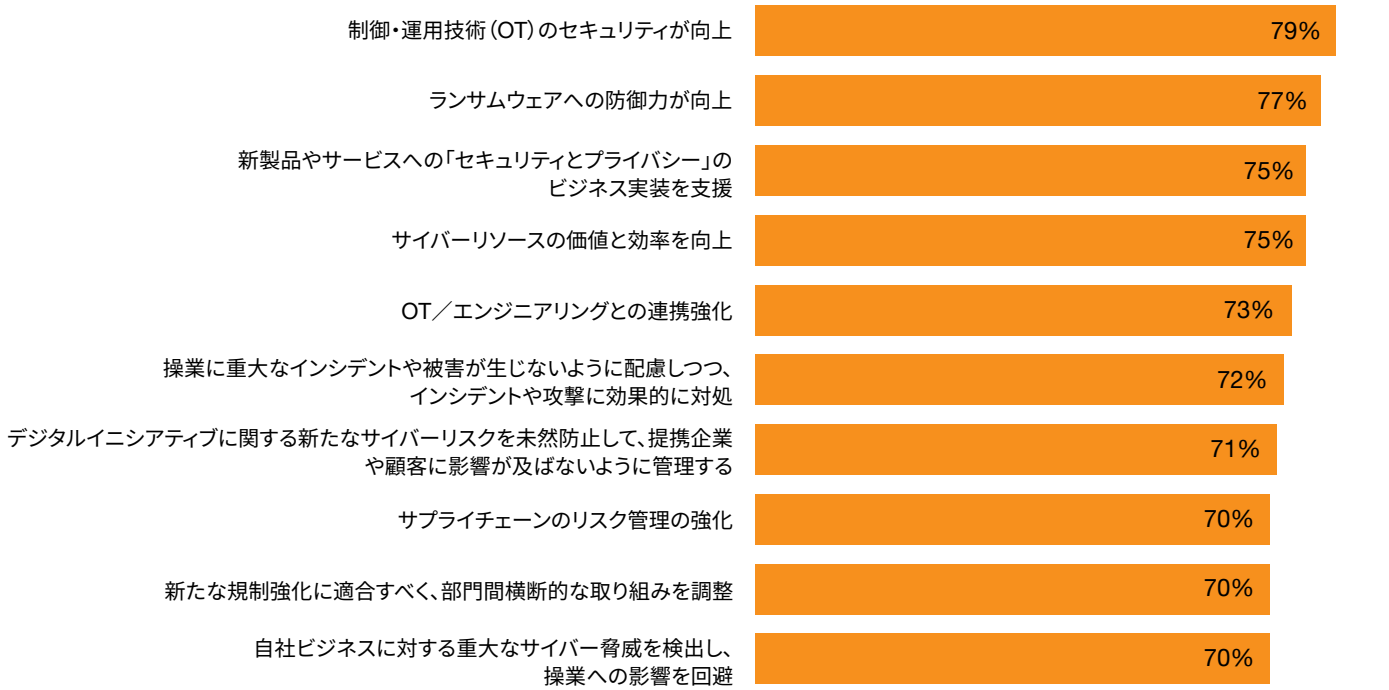
2020年以降サイバーセキュリティが進展

調査対象の経営幹部と技術担当エグゼクティブ（回答総数3,522件）の70%以上が、今年になって、社内のサイバーセキュリティが強化されたと回答しています。これは、投資を継続したことに加え、CxOからの協力が寄与しています。回答者の4分の1以上（26%）が、当社の考えるサイバーセキュリティ成熟（cyber maturity）の重大要素10分野の全てで、進展が見られたとしています。

多くの分野でサイバーセキュリティが進展（CxOレポート）

26%が全10項目を達成したと回答

過去12カ月以内にサイバーセキュリティチームが以下のそれぞれの項目で成果を上げたとする回答（全体に対する構成比：%）



質問：あなたの組織のサイバーセキュリティチームが過去12カ月間で、以下に掲げる各項目を達成したか否かを記してください。調査対象：3,522件
出所：PwC『Global Digital Trust Insights調査 2023年』

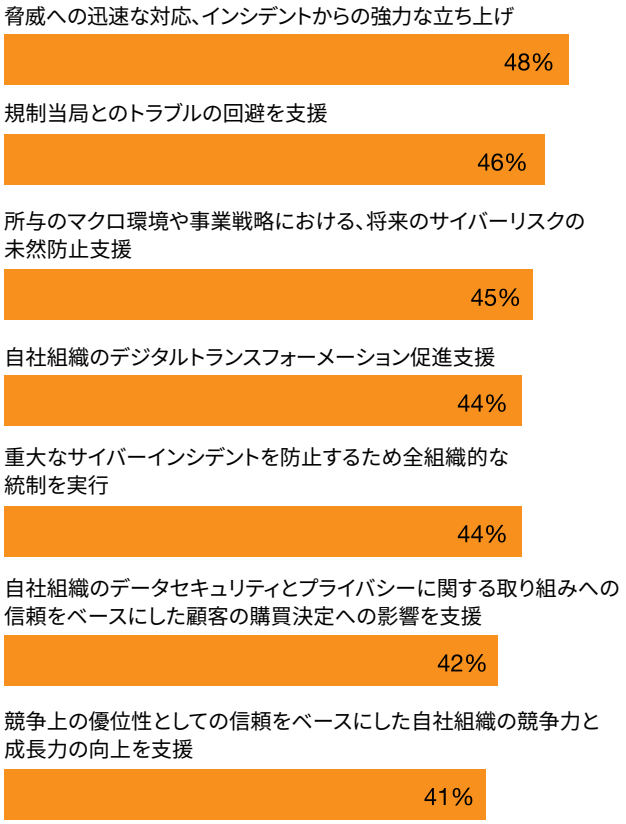
上記の10分野で改善が見られたとする回答の内訳は以下の通りです。

- 今後のサイバーリスクの脅威への迅速な対応やその未然防止対応等の結果において、CISOが非常に優れた成果を出していると評価したのは、CEOが他より3倍多くなっています。回答の8%近くは、CISOが全ての分野で成果を出しているとしています。
- サイバーセキュリティ・プログラムやプライバシー・プログラムを高く評価したのは、CRO／COOが他より2倍多く、その5%以上が、自社のプログラムは全ての分野で成果を出していると回答しています。
- 自社のサイバーセキュリティ・プログラムやプライバシー・プログラムが組織にとって価値があると認めているとの回答では、CMO／CDO／CPOが他の回答者の2.5倍となっており、その最大のメリットは、顧客からの信頼向上に結び付いているという自覚が得られることであるとしています。

他の役員から見たCISOとそのチームへの高評価（CEOの見解）

CEOの8%が全分野でCISOが優れた成果を挙げていると評価

CISOが予想に反して優れた成果を出しているとする回答の割合（%）



質問：2022-23年における貴社のサイバーセキュリティに関して、以下のような成果や期待に情報セキュリティ最高責任者（CISO）がどの程度応えていますか。
調査対象：CEOおよび役員　計919名
出所：PwC『Global Digital Trust Insights調査 2023年』

CISOとそのチームに対する他の役員（CRO／COO）からの高評価

5%が「自社プログラムが全てで成果を挙げている」と回答

サイバー／セキュリティ・プログラムが優れた成果を出しているとした回答の割合（%）

質問：2021-22年における貴社のサイバーセキュリティに関して、以下に示す結果と期待に、サイバーセキュリティ／プライバシー・プログラムがどの程度応えていると評価しますか。

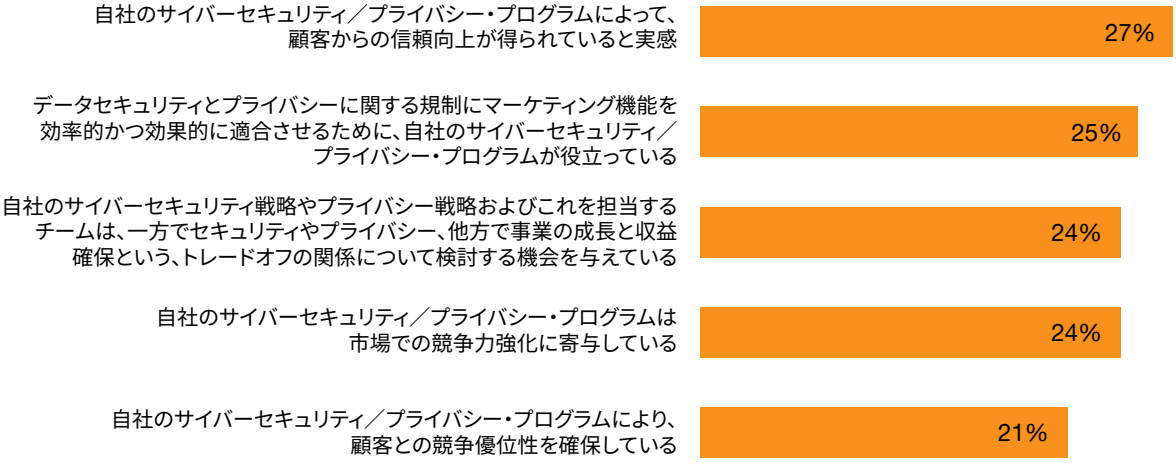
調査対象：CRO、COOならびにリスク、コンプライアンス、運用担当上級管理者　計711名

出所：PwC『Global Digital Trust Insights調査 2023年』

CISOとそのチームに対する他の役員（CDO、CPO、CMO）からの高評価

6%が自社プログラムに高評価

サイバーセキュリティ／プライバシー・プログラムとその担当チームに関して、以下の状況が該当するとした回答の割合（%）



質問：貴社のサイバーセキュリティ／プライバシー・プログラムやその担当チームが生み出す価値について、以下のそれぞれがどの程度当てはまると思いますか。

調査対象：CDO、CPO、CMOおよび顧客対応部門の上級管理職　計412名

出所：PwC『Global Digital Trust Insights調査 2023年』

必須となるダイナミックなサイバーセキュリティ対策

デジタイゼーション（訳注：アナログ形式で表現されているものをデジタル形式に変換すること）によって、誰もがセキュリティに携わることになります。システムのつながりはますます進展し、データ量は飛躍的に増大するでしょう。それとともに、敵対者の組織化もさらに進化すると見られます。サイバーリスクが高まり続けるなか、景気の低迷に直面しつつも、ビジネスリーダーがなすべきことはさらに増えています。

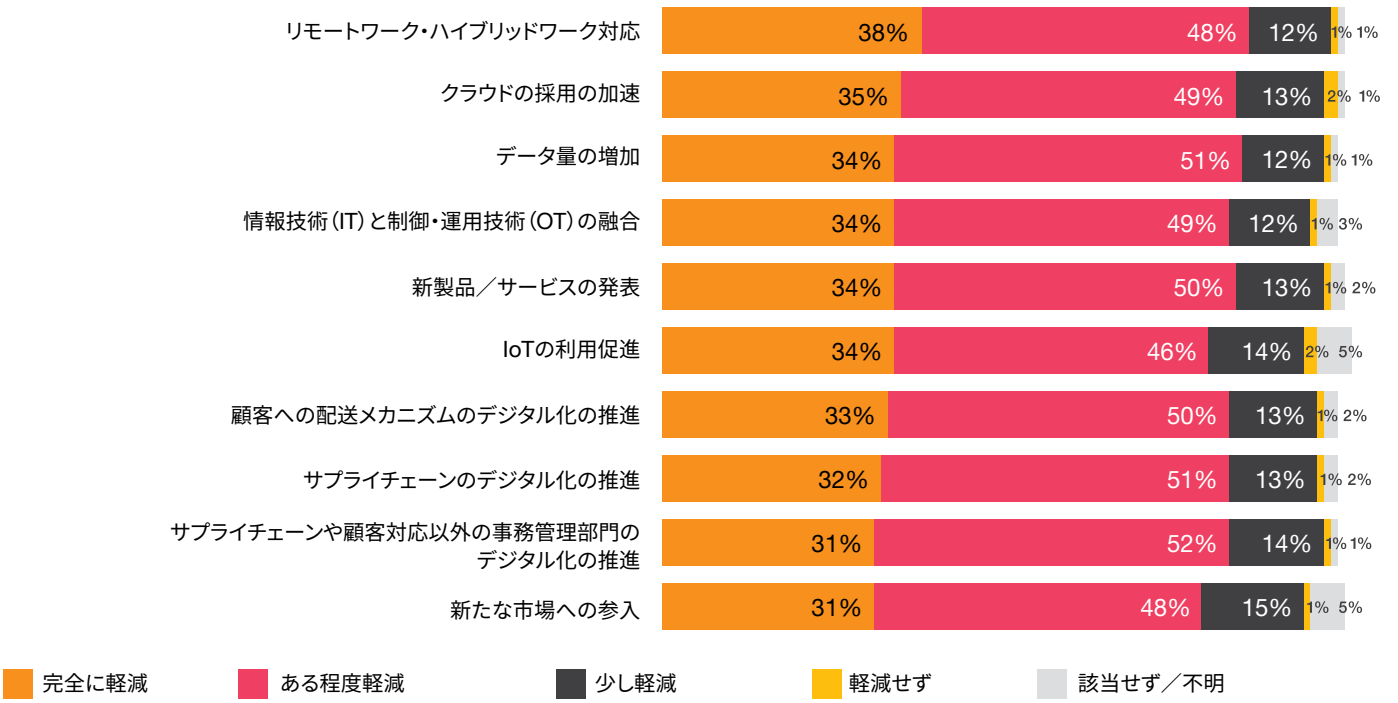
回答者の4割弱が、2020年以降の思い切った方向転換に伴うリスクを軽減する方策を十分に講じたとしています。

最も注目されるのは、リモートワーク（38%）とクラウドへの移行（35%）です。こうしたリスクの軽減策が進んだとするのは、北米を中心として、比較的大規模な企業（売上高10億米ドル超）に多いようです。10のリスク全てに完全に対応しているとの回答は、全体の3%にも届きません。

サイバーリスクの脅威を完全に軽減したのは全体の4割弱

以下のそれぞれに伴うサイバーリスクを軽減したとする回答の割合（%）

あらゆるイニシアティブに伴うリスクを完全に軽減したのは全回答の3%未満



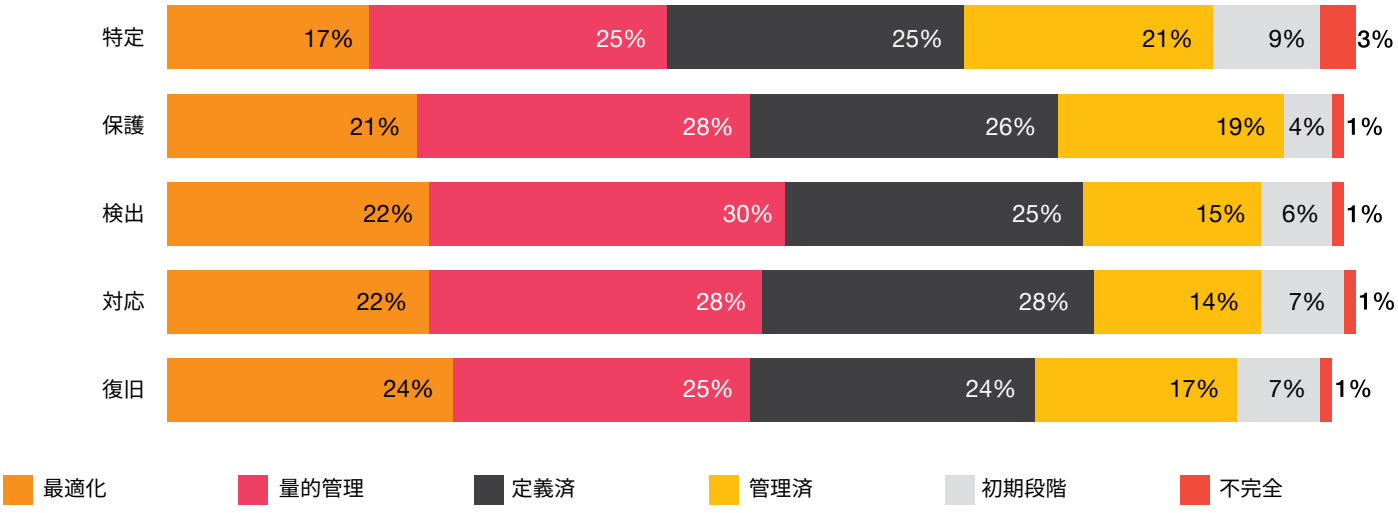
質問：貴社において、過去12カ月間で、以下のそれぞれに伴うサイバーリスクがどの程度軽減されていますか。1から10で評価してください。
対象総数：3,522件
出所：PwC『Global Digital Trust Insights調査 2023年』

各社のCISOたちは、米国国立標準技術研究所（NIST）のサイバーセキュリティ・フレームワークに記載されている5つの基本的なサイバーセキュリティ能力をさらに進める必要があるものと自己評価しています。この5つのサイバーセキュリティ能力の全てを「最適化している」と回答したのは、全体の3%に過ぎません。

売上高10億米ドル超の大規模な組織は、特定（Identity）の項目で、最適化しているとする回答が多く見られます（21%）。売上が増加をたどっており、将来的にも増加が続くと予想している企業からは、全ての項目で最適化しているとの回答が多くなっています。

CISOは5つのサイバーセキュリティ能力の強化を進めることが必要と認識

5項目の全てを最適化したのは全回答の3%のみ



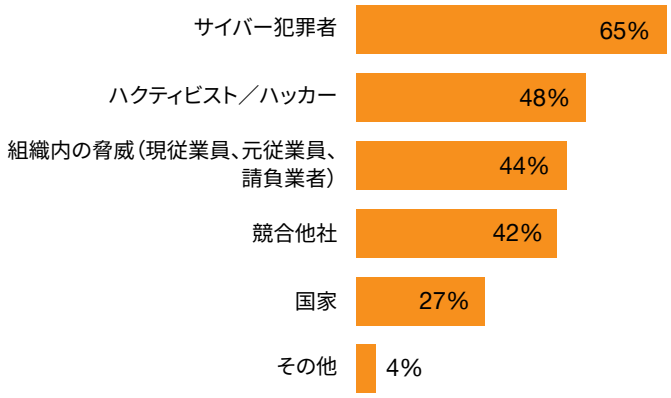
質問：貴社のサイバーセキュリティ能力を全体的に見た場合、以下の5分野のそれぞれにおける貴社の組織的成熟度を評価してください。
調査対象：CISO　計465名
出所：PwC『Global Digital Trust Insights調査 2023年』

各社の上級管理者は、脅威の高まりに対して、自社の態勢が十分ではないと懸念しています。2023年調査において、高まりつつある組織的脅威として上位を占めたのは、サイバー犯罪行為（65％）、モバイルデバイス（41％）、電子メール（40％）、クラウドベースのデータ漏えい（38％）、ビジネスメールの侵害／アカウントの乗っ取り（33％）、ランサムウェア（32％）の順となっています。

多くの組織が2023年における脅威とサイバーインシデントの増加を懸念

脅威アクター

2023年において、前年と比べ、以下の脅威アクターが自社の組織に重大な影響を与えるとする回答者の割合（%）

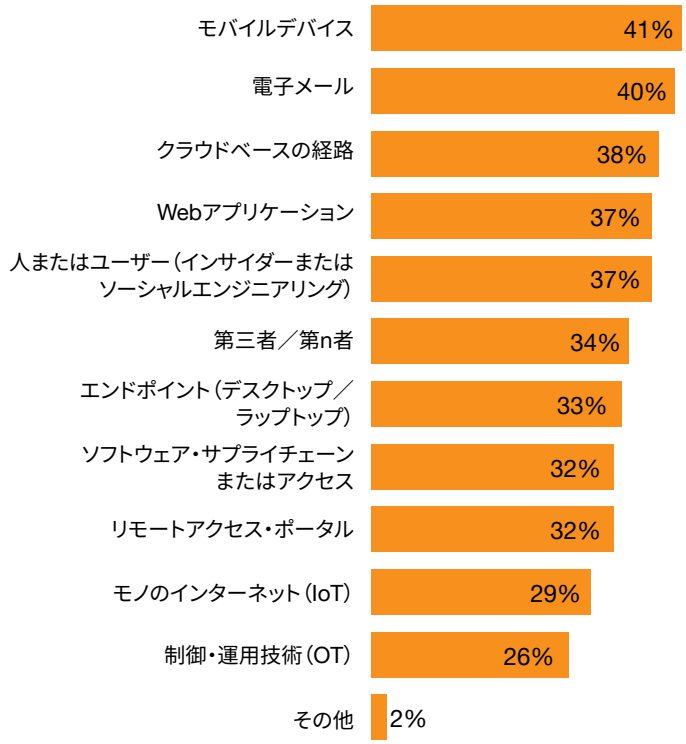


質問：以下の各脅威アクターについて、2023年において、前年と比べ、貴社の組織に重大な影響をもたらしそうなものを挙げてください。
調査対象：3,522件
出所：PwC『Global Digital Trust Insights調査 2023年』

多くの組織が2023年における脅威とサイバーインシデントの増加を懸念

攻撃経路

2023年において、前年と比べ、重大な影響をもたらしうる攻撃経路として、以下の項目に関する回答の割合（%）

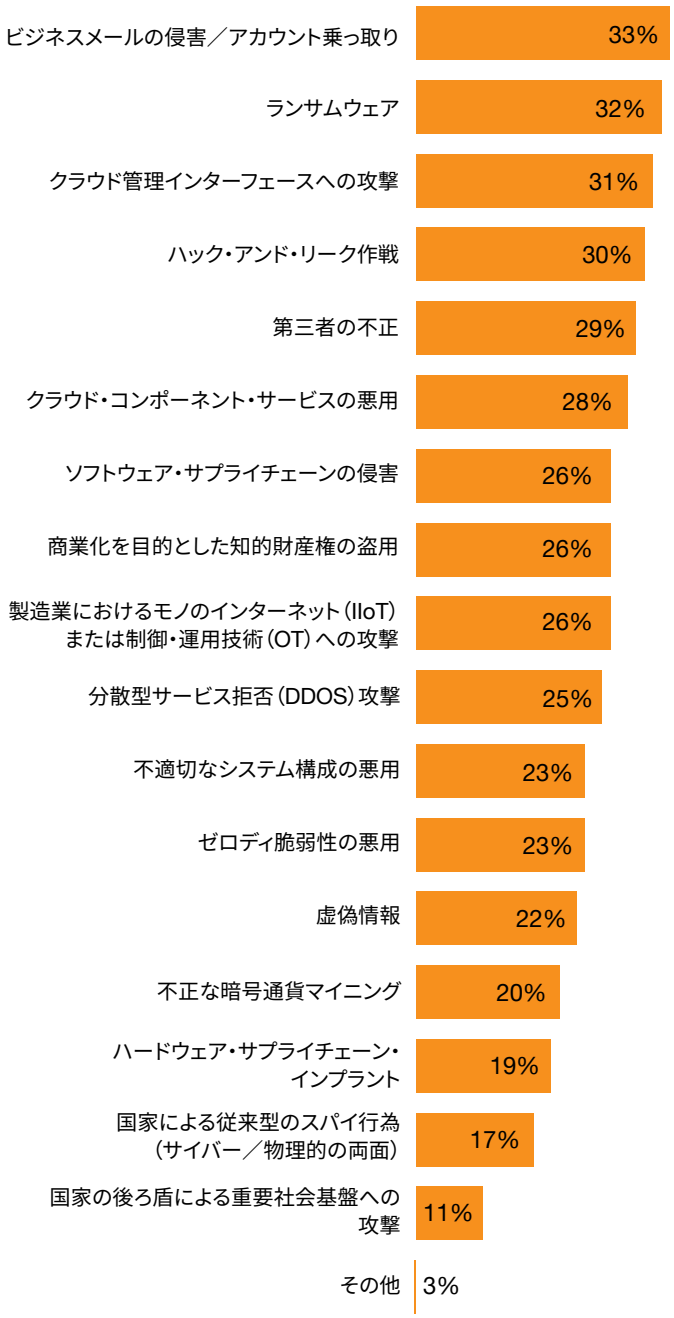


質問：貴社のシステムへの攻撃者の侵入経路として、2023年において、前年と比べ、貴社に重大な影響を与えそうなものを選択してください。
調査対象：3,522件
出所：PwC『Global Digital Trust Insights調査 2023年』

多くの組織が、2023年における脅威とサイバーインシデントの増加を懸念

サイバーインシデント

2022年から23年にかけて、以下の攻撃の増加を予想すると回答した割合（%）



質問：2023年において、前年と比べ、貴社の組織への攻撃として大きく増加しそうなものを挙げてください。
調査対象：3,522件
出所：PwC『Global Digital Trust Insights調査 2023年』

2023年の新たな課題

- サイバーインシデントの報告を求める規制的な圧力は強まっていますが、回答者のうちで、開示要件を効率的にほとんど問題なく満たすことができるとしているのは、全体の9%に過ぎません。

  例えば欧州では、欧州ネットワーク・情報セキュリティ機関（ENISA）により、重大なサイバーインシデントが発生した場合、重要なサービスプロバイダーから各国の当局に報告することが求められています。

  米国証券取引委員会は、上場企業に対して、サイバーリスクの管理、戦略、ガバナンスに関する情報開示に加え、「重大な」サイバーインシデントの報告を求める規則を設けることを検討しています。

  今年3月に大統領の署名を得て成立した2022年重要社会基盤に対するサイバーインシデント報告法（CIRCIA、仮訳）を受けて米国サイバーセキュリティ庁（CISA）が提案している規則では、16の重要インフラ事業者に関連する組織に対して、重大なサイバー攻撃とインシデントについては72時間以内に、また、ランサムウェアへの身代金支払いを行ってから24時間以内に報告することが求められる見込みです。

- 上級管理者は、重大な被害をもたらすサイバー攻撃だけでなく、世界的な景気後退、健康に対する新たな危機、インフレの長期化、サプライチェーンにおけるボトルネックといった課題に対しても、警戒を強めている。しかし、統一的な態勢で回復できているのは全体の7%に過ぎません。

- 消費者、消費者寄りの規制当局、プライバシー擁護派やESG活動家が勢いづいています。多くの組織は、データセキュリティとプライバシーに脆弱性を抱えています。10の基準を常時実行し、顧客情報の保護と管理の実践を指導していると回答している上級管理者は、全体の5%にも達しません。

上級管理者は、重大な被害をもたらすサイバー攻撃だけでなく、世界的な景気後退、健康に対する新たな危機、高インフレ、サプライチェーンにおけるボトルネックといった課題に対しても、警戒を強めています。しかし、統一的な態勢で回復できているのは全体の 8%に過ぎません。

CxOのための
サイバーセキュリティ
プレイブック

CxOのためのサイバーセキュリティプレイブック

サイバーセキュリティの分野は、ビジネスにおける進歩と歩調を合わせて変化を遂げており、動きが急加速しています。

課題解決に必要なのは、ダイナミックな対応ができることです。変化を続けていくにはどうしたらよいか。CISOとサイバーセキュリティチームが影響力を発揮することで最大限の成果を挙げられるのはどんな分野でしょうか。

CxOのためのサイバーセキュリティプレイブックは、PwCの『Global Digital Trust Insights』最新版を活用しており、関係者がこれまで実践してきたこと、現在行っていること、そして、2023年の課題に立ち向かうために行うべきことに焦点を当て、同じ分野に携わる上級管理者が連携しつつ、**将来的なサイバーセキュリティ対応力**の構築を目指しています。

“スイートスポット”のサイバーセキュリティ

CISOが主導権を握り真にリードするために、独立したサイバーセキュリティ専門家の役割から踏み出し、少数の上級管理者だけでなく、CxO全体を巻き込んでいく必要があります。こうした協力体制は、これまで以上に重要になっています。

上級管理者の42%が、会社のシステムへのサイバー攻撃が2020年以降増加したと回答しています。企業の管理者や取締役は、「サイバー攻撃の影響を受けていないか」、そして問題がない場合でも、「脆弱性はないか」を常に自問自答すべきでしょう。

CISOやCFOの報告によれば、過去3年間に、4分の1を超える企業において、間接的なデータ漏えいが発生し、100万米ドルを超える支出を余儀なくされており、さらに、およそ10%の企業では、支出額が1,000万米ドル以上にのぼっています。

CFOにとって、インシデント発生時（データ漏えい以外のもの）に最も深刻だったのは以下の通りでした。

- 操業中断または停止
- サービスや製品品質へのダメージ
- 契約やビジネス機会の損失

一般の人々と接するプライバシー担当およびデータ担当の管理者にとって、インシデント発生時の最も深刻な影響として、以下のようなものがあります。

- 顧客の喪失
- データの復旧に要するコスト（身代金支払い以外）
- 顧客情報の喪失（復旧できない場合）

このように大きな苦痛を伴う経験は、協力体制構築への契機となるでしょう。ひとたびインシデントが発生すれば、その影響は生産現場から役員室まで波及することが鮮明に認識され、CxOが「一致団結して」行動することが求められます。

結果として、CxOは、サイバーセキュリティの強化やプライバシー保護に関する認識を改め、経営層は一致団結して行動することが必要であると理解しはじめることになります。

CxOの一致団結の中心にいるのがCISOです。CISOは、サイバーセキュリティのより良き未来を提唱し、そのための協力を行い、全体を指揮する権限をCEOから与えられています。CEOの46%（そしてかつてインシデントが発生した組織の49%）が、来年には、セキュリティ向上に関する協力を推進するため、CISOにもっと多くの権限を委ねることを望んでいます。

注記

管理チームの構成は国ごとに異なります。それゆえに、本資料で用いているCxOの役職名が、皆さんの組織では存在しない可能性もあります。

ここでの役職名は、組織内でサイバーセキュリティに責任を有する最高責任者（CISO）、事業全体を統括する責任者（CEO）、経営監督および企業ガバナンス取締役（Board）、最高情報責任者・最高技術責任者（CIO／CTO）、最高財務責任者（CFO）、最高執行責任者（COO）、最高リスク管理責任者（CRO）、最高データ責任者（CDO／CPO）、最高人事責任者（CHRO）の各役員と連携しつつ業務を遂行する役員のことを簡潔に表記したものと考えていただいて結構です。

CEOによる今年のサイバーセキュリティに対する姿勢はより積極的に

CEOの半数以上が、事業や運営の大幅な見直しを行うごとに、サイバーリスクマネジメント計画の策定を求めると言っています。また、サプライチェーンの合理化や、会社のサイバーセキュリティ体制を脆弱にする製品の削減などの重要な取り組みの先頭に立つとするCEOも半数を超えています。

かつてインシデントを経験したことがある会社のCEOは、サイバーセキュリティへの対応方法を変えることに、一層確固たる決意を持っています。

CEOたちは、自らの組織のサイバーセキュリティ・プログラムをよりよく監督するために、もっと多くの情報を求めています。

回答したCEOの35%が、以下の3つの分野での報告の強化を優先するとしています。

- サイバーリスクの評価と実践
- サイバーインシデント発生時における事業継続計画、危機管理計画、復旧計画
- 主なサイバーリスクに関するダッシュボード

各社のCISOは、サイバーセキュリティ・プログラムや自らの組織が直面しているリスクに関して、どのようにしたらCEOに正しい情報だけを上げることができるか、学習しています。

CEOへのメッセージ

サイバーセキュリティにおいて、最も違いを見せられるのはどんな分野でしょうか。サイバーセキュリティ体制の強化を進めるために、最も効果的なのは、大きな変化を起こすことかもしれません。その意思決定は、CEOだけができることです。

自社の事業や技術が不必要なくらいに複雑化していて、その改善ができると分かっているのに、看過していることはないでしょうか。こうした状況を変えていかねばなりません。

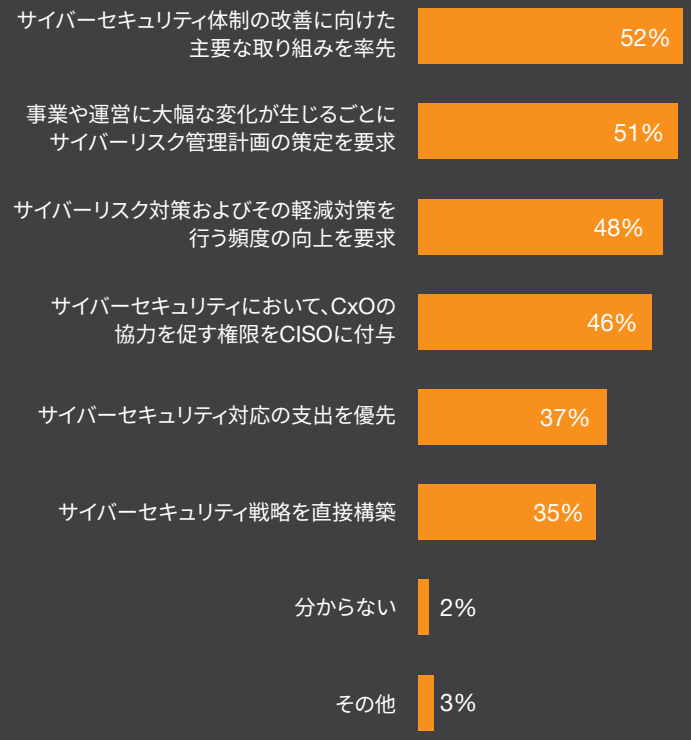
しかし、重大なサイバーインシデントの発生後の調査において、技術というよりもシステムに弱点があると判明することが極めて多いのです。それは、こうした弱点の存在にチームが気づいていても、企業のリーダーがそれに注目して必要な手立てを講じなかったことによるものです。CEOの皆さんは劇的な転換をサポートする準備ができているでしょうか。それこそが、最も効果的な解決策なのです。

会社の経営幹部の間で、または会社とサイバーセキュリティ部門の間で発生する認識のズレによって、成長分野における取り組みが鈍化しています。例えば、消費者用のアプリ、人工知能（AI）を利用した新たな事業分野、新市場への参入、生産現場でのモノのインターネット（IIoT）の利用などです。これらの全てを確保するために、今こそ、力を結集すべきではないでしょうか。

サイバーセキュリティの不安に立ち向かうCEOたち、およびその成功事例

回答者の4%が6つの方法全てに関与する予定

サイバーセキュリティ問題に個人的に関与したいとするCEOの割合（%）



質問：貴社におけるサイバーセキュリティ問題に関与する場合、今後12カ月間でどのようなアクションを行おうとしていますか。
調査対象：CEO　計795名
出所：PwC『Global Digital Trust Insights調査 2023年』

取るべき行動：貴社におけるサイバーセキュリティへの取り組みを共有しましょう。ご自身の影響力により大変革を起こし、サイバー攻撃に対抗する共同戦線を構築しましょう。安全の確保こそが事業を成功に導く近道であるという考え方を、CxO の間に浸透させましょう。

取締役会による監督強化に向けたサイバー報告促進の推奨

自社を取り巻くリスクの増大を受けて、各社の取締役がサイバーセキュリティへの関与を強めています。回答者の54%が、デジタル化を進めるにつれて、サイバーリスクが増しているとしており、44%は、自社システムへのサイバーインシデントが2020年以降増加したと報告しています。

サイバーセキュリティの最新動向を常に把握するのが重要であることは分かっています。しかし、現時点では、次の6つの分野において、サイバーセキュリティの管理を「非常に効果的に」行っているとしたのは、取締役の半数にも届きません。例えば、サイバーリスクの原因とその影響について「とてもよく」理解しているのは37%、サイバーリスクの管理と業務上のニーズとのすり合わせを監督しているのは43%と、ともに半数を下回っています。全ての分野にわたって、サイバーセキュリティの管理が「非常に効率的に」行われているとするのは、9%に過ぎません。

しかし、サイバーセキュリティの管理は、将来的には違ったものになるかもしれません。企業の役員は、以下に示すように、サイバーセキュリティについて、時間をかけてもっと学びたいと望んでいます。それによって、2023年には、サイバーセキュリティの管理をより適切にできるようになると考えています。

- 管理者による、取締役向けの研修（47%）
- サイバーセキュリティを対象とした会合をより多く開催（47%）
- サイバーインシデント、運用、改善に関する報告の強化（44%）
- サイバーセキュリティの専門知識を有する人材を取締役として登用（43%）

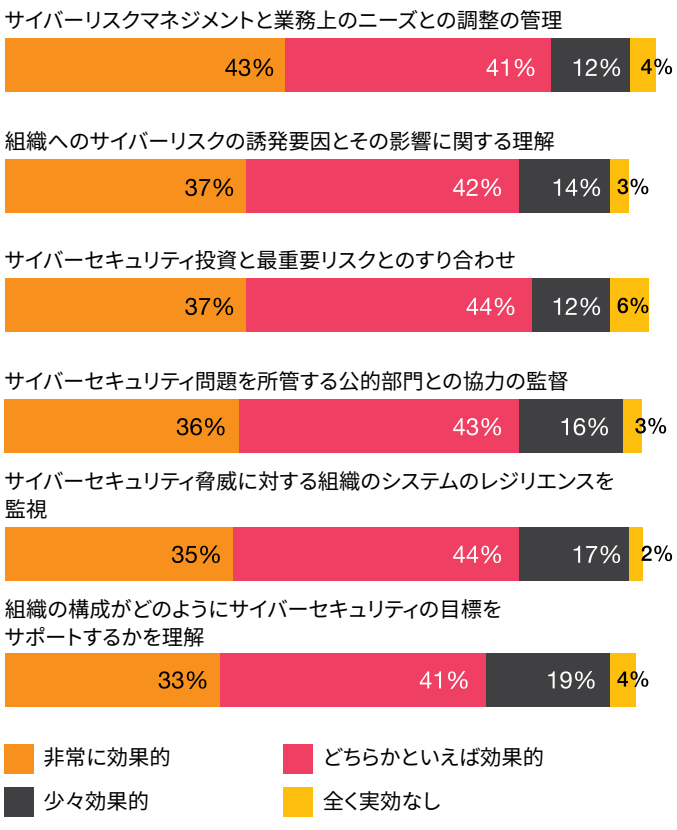
CISOやCxOは、サイバーセキュリティに関する報告において取締役が特に改善を期待している以下の事項について、サイバーセキュリティに関する知見が深まるよう、支援を行うことができます。

- 関連する尺度を用いることにより、組織が抱える主なサイバーリスクを取締役会メンバーが理解しやすくするスコアカード／ダッシュボード
- 組織的なサイバーセキュリティ戦略ならびに、これと全社的戦略とを調和させる方策
- サイバーインシデント発生時における事業継続計画、危機管理計画、復旧計画

会社を取り巻くリスクの増大を受けて、取締役会はサイバーセキュリティへの関与を深めている。

取締役はサイバーセキュリティ課題にもっと貢献する必要性を認識

全6項目で、取締役が極めて効率的に管理しているのは全体の9%



質問：取締役会メンバーとしての責務において、現在の貴社におけるサイバーセキュリティに関する以下の各項目に対する監督を、どの程度適切に実行できていると評価しますか。

調査対象：各社役員　計124名

出所：PwC『Global Digital Trust Insights調査 2023年』

各社役員へのメッセージ

取るべき行動：第一に、ご自身の検討課題として、CISOとサイバーセキュリティの問題に、より多くの時間を割いてください。第二に、取締役会への報告から、自社の戦略的な動きに関連するサイバーリスクを管理できていることに確証が持てない場合や、管理状況について明確な理解が得られない場合は、こうした報告に満足しないでください。サイバーセキュリティは進化し続けるべきものであるため、会社のサイバーセキュリティ体制がどのように改善されているか、また、新たな脅威への防御力は十分かどうか、監視し続けなければなりません。会社のサイバーレジリエンスに関する理解を容易にする演習に参加してください。

新時代を迎えたサイバーセキュリティ・トランスペアレンシーの動き

会社が直面するサイバーリスクの管理状況について、より多くの情報提供を求める利害関係者からの声が強まっています。

プライバシーの不正や侵害から市民を守り、出資者がより的確な判断を下せるようにし、産業全体やシステム全体を巻き込んだインシデントを回避するため、規制当局は、サイバーセキュリティの実践を可視化しようとしています。インドでは、情報技術法（Information Technology Act）で要求されるサイバーインシデントの通知に係るガイダンスを発行しています。英国財務報告評議会（Financial Reporting Council）は、FTSE350を構成する一部の会社が開示する内容について、現状では投資家のニーズを十分に満たしておらず、しばしば「ボイラープレート（訳注：ほとんど変化しないこと）」で、極めて変化に乏しいと判明したことを受けて、デジタル・セキュリティ・リスクの開示に係るガイダンスを発行しました。米国証券取引委員会（法案）および米国サイバーセキュリティ庁（Cybersecurity & Infrastructure Security Agency）（法）に係属中の規則に加え、ニューヨーク州金融サービス局（New York State Department of Financial Services）では、対象事業者について、先進的な取り組みを規制要件化する提案に関する検討が進められています。

投資家が求めているのは、ニーズに適った投資先を選定するために、一貫性があり比較可能性がある情報開示です。サイバーインシデントが発生すれば、一時的に、または永続的に株主価値に影響が及ぶ可能性があります。

個々人は、サイバーインシデントに対して、自らのデータやプライバシーがどれほど脆弱であるか知っています。**ビジネスパートナー**は、自らのデータやその他の資産の安全性が保たれるよう望んでいます。サイバーセキュリティの脅威が増大するなかで、その会社やシステム全体の対抗力にどの程度の信頼を置いてよいのか、利害関係者たちは知りたがっています。

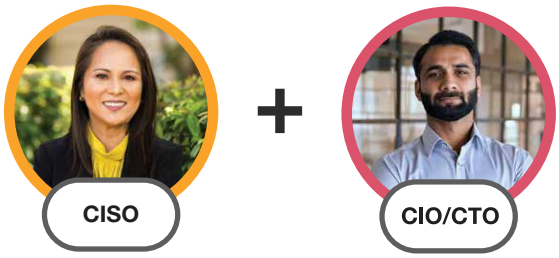
各社のCxOは、このように全般的な透明化を進めるのがよいことだと理解しています。今回の調査において、上級管理者の5分の4が、利害関係者の信頼と信用を獲得するために、比較可能で一貫性のある様式を用いたサイバーインシデントの報告を義務化することが必要であるとの認識で一致しています。

しかし、確実にこれに適合できると考えている企業は10%を下回っています。半数を超える企業は、以下の点で不安を感じています。

- 重大インシデントや重要なインシデントの発生後、所定の時間内に、必要な情報を報告できるかどうか（不安とする回答が58%）
- 報告するために、サイバーインシデントの重大性の評価ができるかどうか（同58%）
- 報告するために、サイバーセキュリティに関する取締役の専門知識を記述することができるかどうか（同59%）
- サイバーインシデントに関して、開示できる情報とそれ以外の情報を規定する方針があるか否か（同60%）
- サードパーティーのリスクマネジメントに関する情報を提供できるかどうか（同63%）

取るべき行動：CISOは、CFO、相談役その他の上級管理者と協力できるように自らのチームを配置して、会社のサイバーリスクの管理についての戦略や実践などを、正確にまとまった、説得力のあるストーリーに言い換えて伝えていかなければなりません。サイバーセキュリティの透明化という新時代においては、CISOは、取締役、上級管理者、投資家の全てが理解できて、それに基づいて行動するようなやり方で、情報を伝える術に長じるようになることが求められます。それには、サイバーセキュリティの世界でしか通用しない専門用語とは違ったコミュニケーション戦略が必要とされます。

クラウドセキュリティにおける CIO、CTO、CISOの連携



「当社のクラウドセキュリティ計画は、当社の事業継続計画と同程度のレジリエンスレベルですか」――CIOやCISOは今こそこのように自問自答すべきでしょう。

クラウドベースの脅威は、40%近い組織で増加をたどっています。一方で、クラウドの適用に伴うリスクが完全には緩和できていないとする上級管理者は、全体の3分の2近くにのぼります。

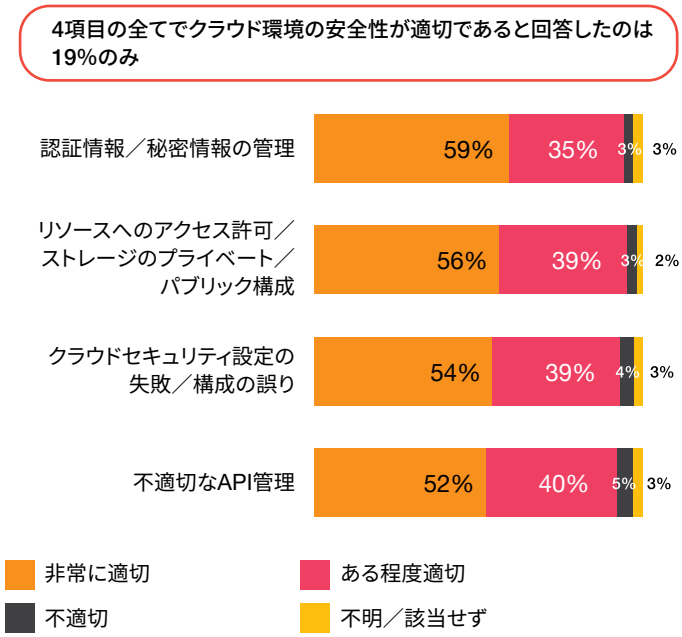
しかし、ネガティブなことばかりではありません。CISO、CIO、CTOの半数は、認証情報の管理、リソースへのアクセス許可、クラウドセキュリティの構成やAPI管理を、より適切に行えるようになったとしています。

しかし、こうしたクラウドインシデントの一般的経路の全てを、組織として適切に安全化できたと自認できているのは、全体の19%に過ぎません。

CIOまたはCTOとそのDevOpsチームは、クラウドが可能とする俊敏さ、スピードと共同作業性を活用したいと望み、また活用を迫られる状況に置かれているかもしれません。

クラウドセキュリティのイニシアティブは結実しつつあるが、さらなる課題が残る

4項目の全てでクラウド環境の安全性が適切であると回答したのは19%のみ



質問：貴社のクラウド環境に関して、クラウドセキュリティ・インシデントが発生する以下の理由に対処して、どの程度適切な安全策が講じられていると認識していますか。
調査対象：CIO、CISO、CTO、その他ITおよびセキュリティ担当上級管理者 計1,253名
出所：PwC『Global Digital Trust Insights調査 2023年』

彼らは、セキュリティ対策が講じられる前に、開発者がクラウド環境でプロジェクトを立ち上げることを許可するかもしれません。または、リフト・アンド・シフト で既存のシステムをクラウドに移行させ、安全対策はその後に講じればよいと考えるかもしれません。

CISOから体系的で安全第一のアプローチに従うよう指示されることはほとんど明らかなので、彼らはCISOを回避しようとする可能性があります。目まぐるしいスピードで進化するデジタルの世界で、事業者側としては、企業がその目標を達成するためにはスピードが必要であると認識しています。敏捷性とスピードこそが目標とされる状況下で、ブレーキを踏まれることを望む者があるでしょうか。

しかし、カギを握るのはまとまりのあるガバナンスであり、特に、セキュリティ能力とセキュリティ要件がクラウド・サービス・プロバイダーごとに異なるマルチクラウド環境においてはそれが該当します。新たなフィーチャーやアップデートが頻繁にリリースされる状況下では、まさに空に浮かぶ雲のように、会社を取り巻くクラウド環境が絶え間なく変化しています。

2023年におけるセキュリティアーキテクチャは、皆さんの会社で利用している全てのクラウドプラットフォームを含む、包括的な設計であるべきです。

会社のセキュリティ管理を全て統合すれば、1カ所から、しかも可能な限り自動化して安全を確保することが可能となります。

インフラストラクチャ・アズ・コード（IaC）やDevSecOpsツールを構築し、全てのクラウドプラットフォームのセキュリティチェックを自動で正しく設定します。

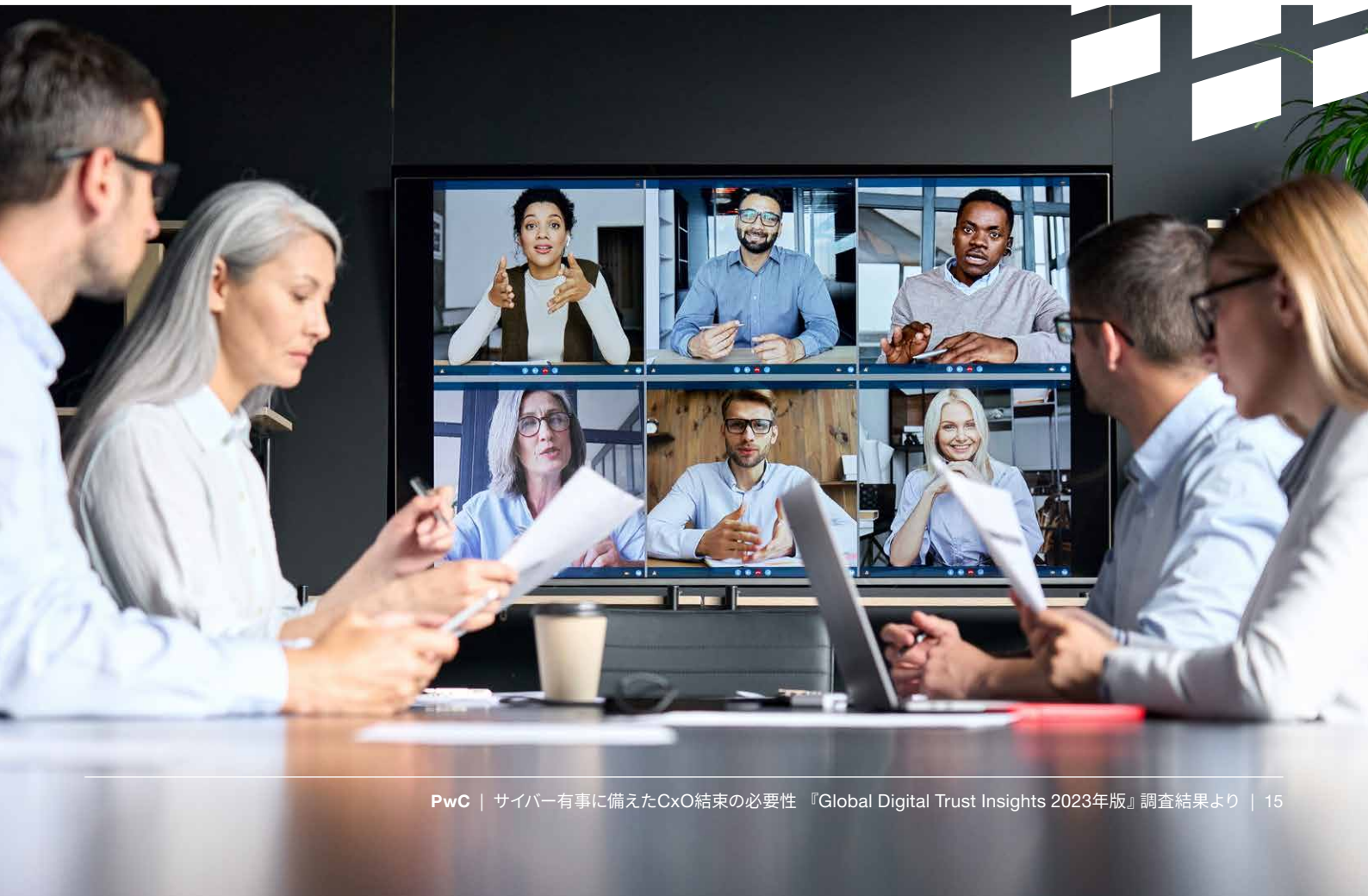
CISOからは、開発者に対して、利用が容易で組織のセキュリティ方針に適合するクラウド・セキュリティ・サービスを提供します。例えば、開発業者用の暗号化APIを構築することによって、アプリケーションの市場化を迅速化するとともに、会社に承認されたプロトコルを利用する暗号化を確実にすることが可能となるでしょう。

CIOとCTOへのメッセージ

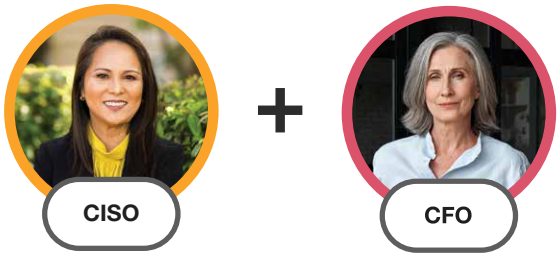
貴社のCISOとDevSecOpsチームと連携してください。「シフトレフト」パラダイムを採用し、クラウドを利用開始する前にクラウド・セキュリティ・メカニズムを導入します。既にクラウドを利用している場合でも、可能な限り早く導入するようにします。

迅速な開発と強力な管理を同時並行的に進めることができます。リーディングカンパニーにおいては、監督という言葉からしばしば連想される緩慢としたペースではなく、DevOpsの素早く俊敏なペースで、制御を設計し、管理しています。このような組織では、誰もが勝者となります。

取るべき行動：バックエンド、フロントエンド、IoT、制御・運用技術（OT）を安全にするためには、CISO と連携して、クラウド環境を封鎖します。



CFOとCISOによるサイバーセキュリティ投資コストとリターンの熟慮

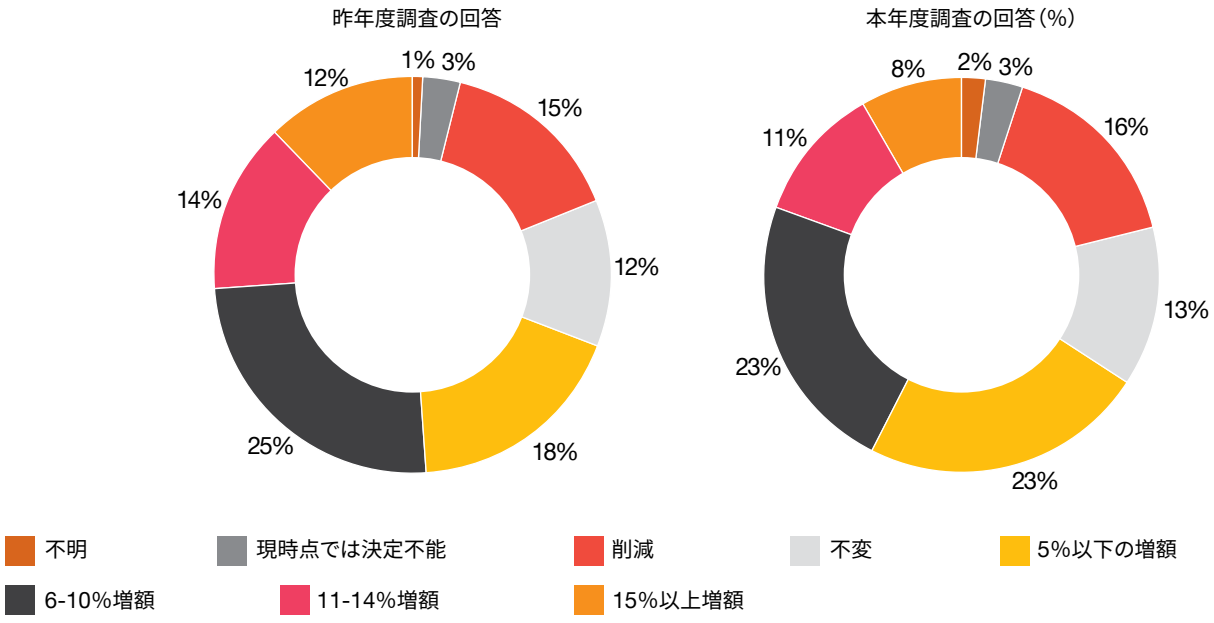


サイバーセキュリティに係る各社の支出は継続的に増大しています。上級管理者の65%が、2023年における支出増を見込んでいます（2022年に増加したのは69%）。

しかし、サイバーセキュリティ関連の予算を前年比で見ると、2022年よりも増加幅が縮小しています。2022年には、サイバーセキュリティ予算が10%以上アップすると予想した企業が全体の4分の1を超えましたが、23年にもこれと同程度の増額を予測するのは全体の5分の1を下回っています。

2023年のサイバーセキュリティ関連支出を強化するとしているのは、これまでにインシデントを経験した企業が圧倒的に多いのは驚くにあたりません（インシデント経験のある企業の68%に対し、経験のない企業は55%）。年間売上高10億米ドル超の大企業の10%が、サイバーセキュリティ関連支出の15%以上の増加を予定しています。

各企業はサイバーセキュリティ関連支出の増加を抑制

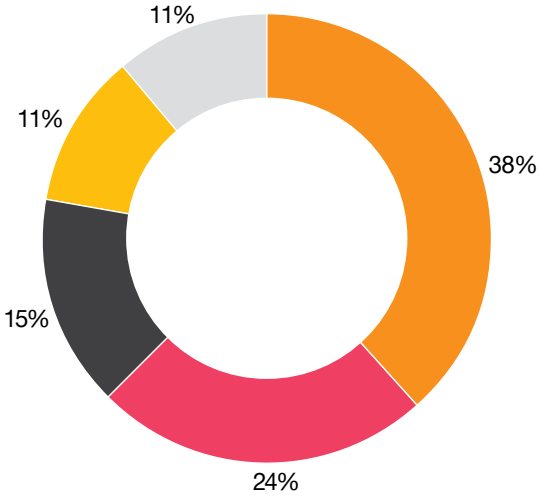


質問：2023年におけるサイバーセキュリティ関連予算は対前年比でどうなりますか。
調査対象：事業・テクノロジー担当役員　計3,522名（本年調査）、セキュリティ・テクノロジー担当役員　計1,638名（昨年調査）
出所：PwC『Global Digital Trust Insights調査 2023年』

関連予算の変化

サイバーセキュリティ関連予算に対する企業のスタンスはもっと包括的です。CEO、CFO、CISOのおよそ4割が、制御・運用技術（OT）や自動化を含め、技術支出全体の何パーセントという形でサイバーセキュリティ関連の支出を行っているとしています。また別の15%は、売上高の何パーセントという形で予算を組んでいるとしています。

サイバーセキュリティ関連予算の組み方



- IT支出額および自動化／制御・運用技術（OT）支出の額合計に対する一定割合
- IT支出総額に占める一定割合
- 売上高増加の一定割合
- 前年のサイバーセキュリティ関連予算に伸び率を乗じたもの
- 予算請求額／承認された事業およびリスク軽減計画に向けられるリソース／事業活動から総合的に判断

質問：貴社のサイバーセキュリティ関連予算はどのように決定されていますか。
調査対象：CEO、CFO、CISO、CIO、CTOその他財務、セキュリティ、IT担当役員 計2,498名
出所：PwC『Global Digital Trust Insights調査 2023年』

多くの企業において、サイバーセキュリティ投資戦略にも変化が見られるようになりました。半数以上が、以下を含む7つの主要パラメーターにかなりの程度従いながら、サイバーセキュリティ関連支出額を決定しているとしています。

- 全体的な事業戦略と一致している（55%）
- サイバーセキュリティ優先度を反映している（55%）
- 企業に付加価値をもたらす（52%）
- 喫緊の必要性と長期的な必要性のバランスをとる（51%）
- リスクの数値化から情報を得る（51%）
- 組織のリスク選好を考慮する（51%）
- 組織が抱えるリスクに応じて適切に配分する（51%）

このような変化は2021年調査から認められるようになりました。同調査では、上級管理者の50%が予算編成において事業戦略をより良く反映したいと言っており、44%が予算編成プロセスの改善を、また44%がリスクの数値化を望んでいます。

しかし、全ての分野でこうした変化が生じているとしたのは全体の8%を下回っています。投資決定方法を変えたとする傾向は、最も規模が大きな企業群でとりわけ顕著に見られ、例えばその60%が、会社の事業戦略をサポートする支出を行っていると言っています。

技術の近代化

サイバーセキュリティ技術ソリューションは、自社のサイバーセキュリティ体制を改善するために不可欠であると各社のCFOが認識する分野の最上位を占めています。

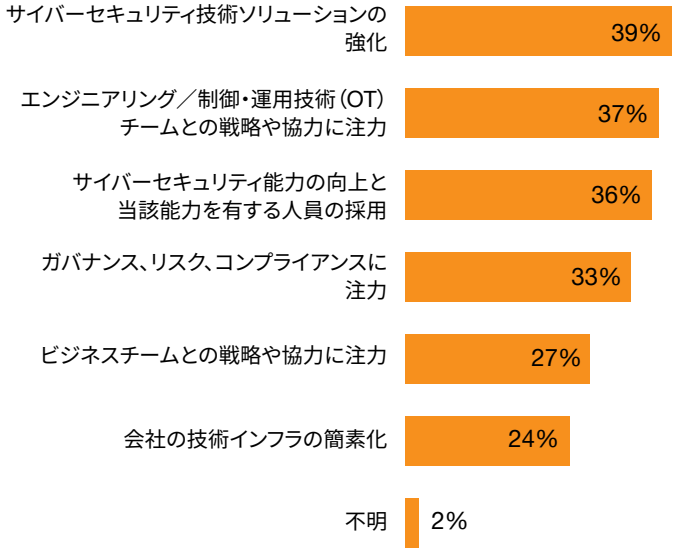
実際のところ、現在でも多くの組織で、特に制御・運用技術（OT）の遅れが課題となっています。旧式化した技術やその脆弱性の管理は、制御・運用技術（OT）におけるセキュリティの強化にとって最大の障害であると、CISO、CIO、CTOたちは指摘しています。

複雑さも、相変わらず大きな懸念事項となっています。ソフトウェアポートフォリオの簡素化と集約化は、過去3年間でインシデントが発生した企業において、2023年の最優先課題です。2022年版の『Global Digital Trust Insights』はこの傾向を予見しています。それによれば、回答者の75%から、自社のデータ、技術、その他の運用があまりに複雑で、サイバーリスクの懸念を惹起していると報告されています。

インシデントを経験したことがある企業では、これ以外に注力していることとして、技術的負債（スピード最優先の開発の過程で端折られてしまった、文字通りのコストや寓意的なコスト）の解消を挙げていることは示唆に富んでいます。未経験の企業においては、これは、サイバーセキュリティ・トランスフォーメーション目標の最下位近くに位置しています。

CFOは、サイバーセキュリティ体制を強化するためのリソースの配分を増加

今後12カ月間においてリソース配分の増加を検討する分野（%）



質問：今後12カ月間において、貴社のサイバーセキュリティ体制を強化するために、リソース配分を最も増加するのはどの分野ですか。
調査対象：CFO　計326名
出所：PwC『Global Digital Trust Insights調査 2023年』

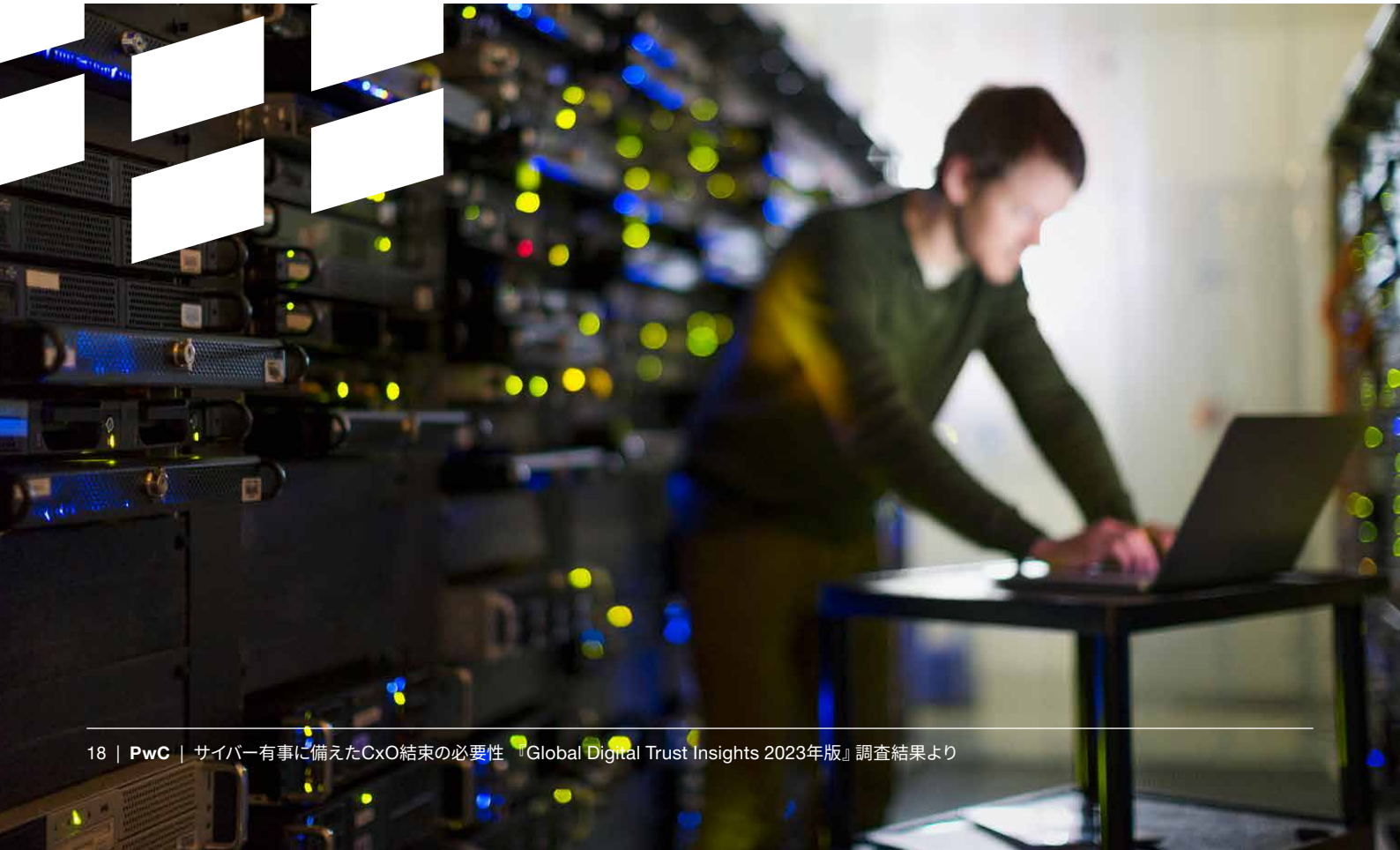
CFOへのメッセージ

「正しい分野に十分な支出が行われているか。投資額に見合う適正なサイバーリスクの軽減効果が得られているか」と問うのは当然のことです。

技術ソリューションが普及するにつれて、さまざまなレベルで組織の安全を確保する大局的な計画を策定するために、そして、会社のソフトウェアを簡素化して整理するために、CISOと協力する必要が生じるでしょう。初期のクラウド展開を思い起こしてみてください。それは、既存のシステムを「リフト・アンド・シフト」でクラウドに移行することでした。これもまた、技術的負債の増加をもたらしました。

クラウドのオープンな性質は、各組織に、信頼パラメーターをゼロに設定し直すことも強いています。ゼロトラスト・アーキテクチャに移行するためには、大局的な計画を策定する必要があります。CISOの36%は、ゼロトラストのコンポーネントの実行を開始したと言っており、これ以外の25%も、今後2年内に開始する予定としています。

取るべき行動：IT の最新化と簡素化を進めるに際して、支出をそれぞれ増加することによって、どのようにサイバーリスクを最大限に低下できるか考えてください。リスクのもたらす資金的コストを認識する企業は、計画的に安全を確保し、結果的に資金を節約することができます。



COOとCISOによるサプライチェーンと制御・運用技術（OT）を標的とした攻撃への対処

サプライチェーンは、サイバーセキュリティその他の脅威、競争やマクロ経済上の圧力、ESG懸念の焦点となっています。

CROやCOOの過半数（56%）が、サプライチェーンが攻撃を受けたら持ちこたえられるか、**非常に強く懸念**、またはとても懸念していると回答しています。

サイバー攻撃を受けてもサプライチェーンに支障を来さないように、自社の制御・運用担当チームが所要のデジタル能力を有している、または十分な投資を行ってきたことに確信を持っていると回答したのは全体のおよそ4分の1にとどまっています。

そして、こうした脅威を制御する能力の一部はサードパーティーに委ねなければならないが、彼らのセキュリティレベルも不十分だと懸念しています。サイバー攻撃からサプライチェーンを守るために、サードパーティーの提携者やサプライヤーが投資を行って十分な対応ができていると確信しているのは、回答者の5分の1だけでした（13%はこれに同意せず）。

CRO や COO の過半数（56%）が、サプライチェーンが攻撃を受けたら持ちこたえられるか、非常に強く懸念、またはとても懸念していると回答。

制御・運用技術（OT）：ソリューションのさらなる改善が必要

制御・運用技術（OT）や情報技術の収束に関連するリスクやIoTの利用拡大に伴うリスクを完全に緩和できているとしたのは、全回答のおよそ3分の1にとどまっています。

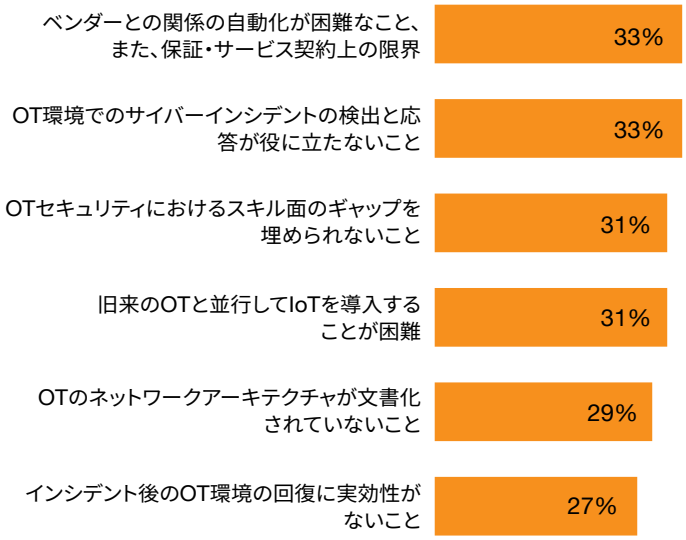
これ以外でCOOやCROが懸念している分野としては、制御・運用技術（OT）の安全性があります。人工知能や機械学習の利用を通じた生産現場の自動化促進など、制御・運用技術（OT）やソリューションがさらなる高度化を遂げるなかで、会社組織は、自社の運営を安心・安全に保つという困難な課題に取り組んでいます。

このような課題に注目しているのはCROやCOOだけではありません。CISOやCIOもまた、こうした課題を認識しています。しかし、最新で安全性が完全に確保された運用に対する最大の阻害要因に関しては、両者は見解を異にしています。

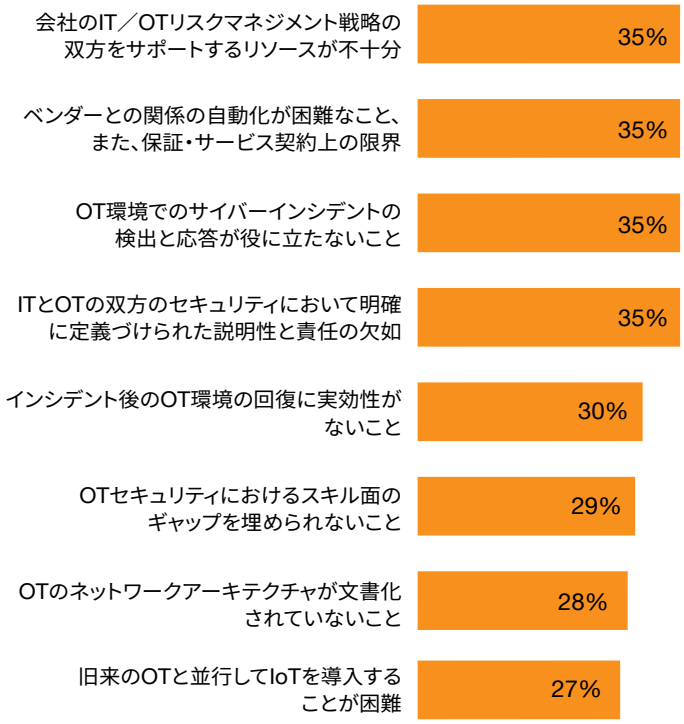
- 両者とも、不適切な技術ソリューションが、OTの改善における最大の阻害要因であることでは一致しています。また、OTのセキュリティに特に対応するソリューションを望んでいます。
- しかし、CISOやCIOは、最大の阻害要因は旧式化したソフトウェアや脆弱性管理ツールの利用であると認識しており、CROも含め、27%の回答者がこの問題を指摘しています。
- 同時に、CROやCOOは、制御・運用技術（OT）のサイバーリスクに対する、より包括的なアプローチ（事業リスクや財務リスクだけでなく、健康、安全、環境へのリスクにも配慮するもの）が適切であると認識しています。こうした懸念事項に対する考え方に相違があることが、OTの改善を阻害する最大の要因となっていると指摘しています。

このような不備を認識しつつ、CISOやCIOは、運用環境の回復のために不可欠な、OTのデータ、人員、システム、設備に関する完全かつ正確な資産インベントリが社内で整備されていないことを指摘しています。

CISO、CIO、CTOの見解



CRO、COOの見解



質問：貴社において制御・運用技術（OT）を改善するに当たって最も重大な課題は何ですか。上位5件を挙げてください。
調査対象：CIO、CISO、CTO、その他IT、セキュリティ担当上級管理者　計1,253名；CRO、COO、その他リスク・運用担当上級管理者　計711名
出所：PwC『Global Digital Trust Insights調査 2023年』

COOへのメッセージ

企業運営のデジタル化が進展するにつれて、全てを安全に保つために、そしてサードパーティーの提携者やサプライヤーの不備を補うための方策を講じるために、サイバーセキュリティチームと協力することの重要性が認識されています。

貴社において、リスク対応チーム、内部監査チーム、コンプライアンスチームは、数多くのサイバーセキュリティ案件で、既にサイバーセキュリティチームと連携しているかもしれません。CROやCOOの半数が、このようなチームが連携して、リスクの監視や優先順位付けを常時行っていると回答しています。その他の3分の1の回答者も、たまにこうしたことが行われているとしています。

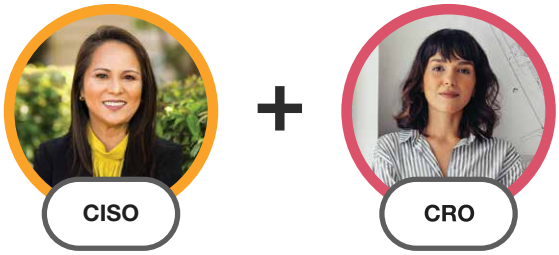
こうしたチームワークは成果を挙げつつあります。5分の4近い回答者（79%）が、過去1年間で、サイバーセキュリティチームによって、OTの安全化が進展したと指摘しています。また、回答者のおよそ4分の3が、サイバーセキュリティチームとOTチームとの協力関係が改善したと認めています。これが偶然の一致ではないことは確かです。

しかし、サプライチェーンやOTに対する攻撃は、想定される脅威のリストの上位には入っていません。これは防御レベルを下げても大丈夫という意識を招く可能性があります。常に警戒を怠ってはなりません。今年に入ってからでも、ソフトウェア・サプライチェーンに対する防御レベルを下げた会社に何が起こりうるかを知る機会がありました。また、OTへの攻撃は増加をたどっています。貴社のシステムに侵入しようとするサイバー脅威のアクターは、しばしばシステムで最も抵抗力の弱いポイントに狙いを定めて攻撃を仕掛けます。それゆえ、貴社のドメインが攻撃ポイントとされないようにしてください。

取るべき行動：

CISO に積極的に協力して、モニタリングなどの日常的なタスクから、ガバナンスのような大局的な案件に至るまで、OT やサプライチェーンのセキュリティにおいて貴社の各担当チーム間の連携を確保してください。サプライチェーンに発生したインシデントや遅延、さらには OT システムへの攻撃から復旧する体制をどのようにしたら構築できるか、連携しつつ検討してください。そして、事業運営を大幅に変革する場合には、常に CIO や CISO と連携して、サイバーセキュリティ・リスク・マネジメント計画を策定するプロセスを構築してください。

CROとCISOによるサイバーレジリエンスあるリスク対応策の検討



今日のサイバーセキュリティにおいて、「リスク」という文言が頻繁に登場します。サイバーセキュリティチームは、リスク、内部監査、コンプライアンスを担当する各チームと、ますます連携を強めています。これは、企業におけるリスク管理の優先課題に占めるサイバーセキュリティの地位が高まっていることを示すものです。

CRO、CAE、そして最高コンプライアンス責任者の間に、サイバーセキュリティがビジネスを意味するという認識が広まっています。回答者の半数が、「サイバーセキュリティチームは他の機能と並行しつつ、絶えずリスクの監視と優先順位付けを行っている」と言っています。また、これ以外のおよそ3分の1の回答者も、時々こうしたことが行われているとしています。

50%	リスクを常時監視
50%	リスクを優先順位付け
49%	企業のリスク管理にサイバーリスクがどのように該当するかに関する共通認識を形成
49%	取締役に報告する
48%	サイバー攻撃とインシデントに同時に対応
45%	共通のデータ管理モデルを適用
44%	エコシステム全体を通じたリスクや脅威に関する統一見解を形成
44%	リスクを数値化
43%	事業ユニットのリーダー（リスクオーナー）に、事業の最前線や運用に絡むリスクをより的確に管理するためのツールを与える
41%	共通のデジタル管理モデルを適用
40%	リスク担当部門やサイバーセキュリティ担当部門間で責任を分担するための単一の運用モデルに従う

かつてインシデントを経験したことがある企業の50%が侵入に常時対処していると回答しており、そうでない企業が38%にとどまっているのと比べると、はるかに多くなっています。

しかし、サイバーリスク対応において、「1人は皆のため、皆は1人のため」というアプローチがとられることは、想像されるより多くありません。リスクに関連するあらゆる活動で他のリスク部門といつも連携しているサイバーセキュリティチームは7%に過ぎません。CROやCOOがこの分野でなすべきことは少なくありません。

CROやCOOは、自社のサイバーセキュリティチームやプライバシーチームのパフォーマンスを非常に高く評価する傾向があります。例えば、彼らの半数近くが、自社のこうしたチームが、事業を復旧するために欠かせない、重大なインシデントを回避するための制御の実行を含め、重要な目標の達成において並外れた成果を挙げていると評価しています。しかし、サイバーセキュリティチームやプライバシーチームがあらゆる期待に「並外れた」成果を挙げていると考えているCROやCOOは、全体の5%に過ぎません。

2023年におけるレジリエンステスト

「あれこれと考えているうちにいろんなことが起こるのが人生だ」と格言に言われていますが、これはビジネスの世界にも当てはまることです。

レジリエンスとは、予期せぬ問題が発生したときでも、平常にとどまれることを意味します。こうした問題としては、例えば、破滅的なサイバー攻撃、世界的な景気後退、新たな健康被害やコロナ感染症の再流行、インフレの高進などがあるでしょう。

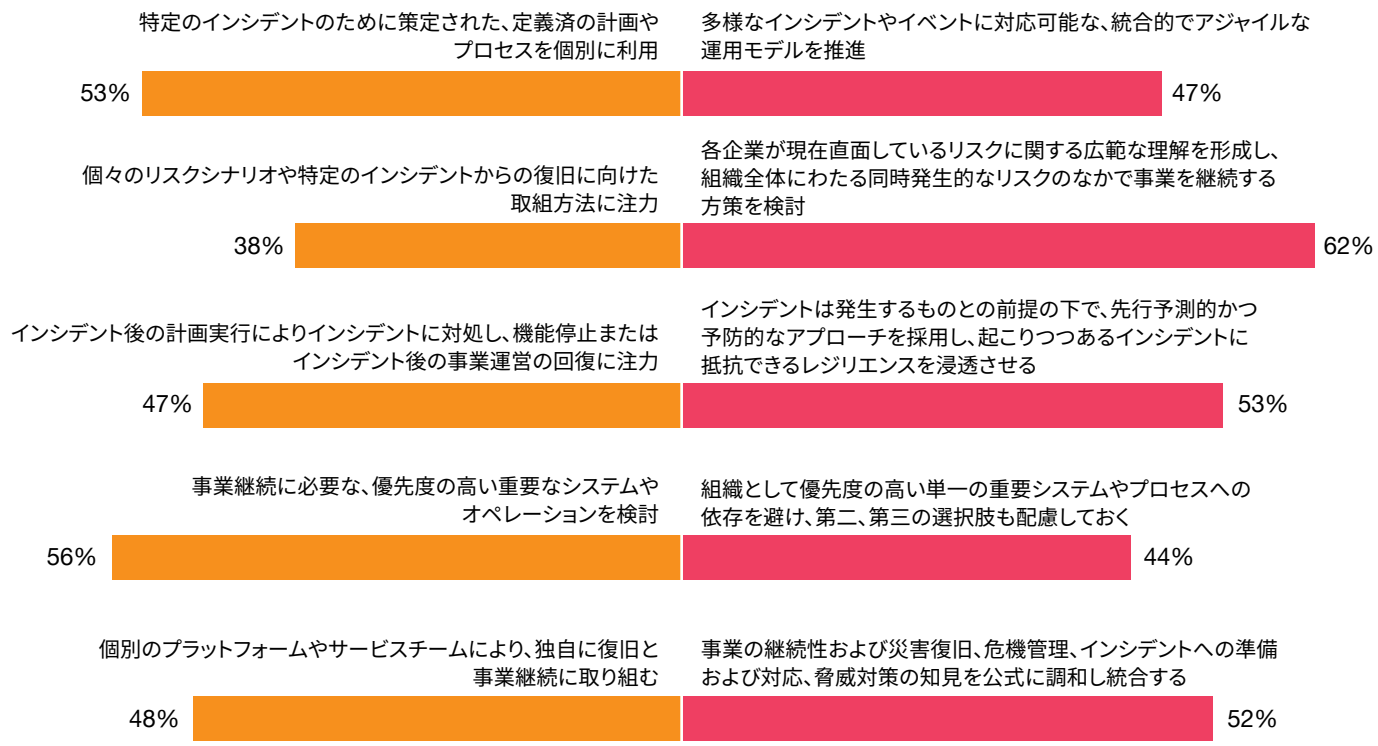
これらは、今後12カ月から24カ月の間で懸念される事項として回答の上位を占めたものです。しかし、これらに平然と対処する準備ができている組織はほとんどありません。

現在私たちを取り巻くリスク環境に照らしてみれば、支障をもたらす要因を特定する「オールハザード」アプローチをとることが、あらゆる組織に求められています。しかし、レジリエンスを定義する5つの主要能力に対して、本当の意味での統一的かつ総合的なアプローチをとっているとする上級管理者は、全体の7%に過ぎません。

CROやCOOにとってポジティブなことといえば、全体の62%がリスクに総合的に対処していることです。しかし、インシデント対応、事業の継続性、災害復旧等、その他の全ての分野については、組織の約半数が、それぞれのインシデントを、レジリエンスの中核をなすさまざまな能力から得られた教訓と統合するのではなく、一度限りの経験として扱っているように思われます。

CROやCOOたちは、このようなアプローチの仕方は、ダクトテープを貼って水漏れを防ぐようなもので、もっと実効性のある抜本的な修理とは別物であると自覚しています。

断片化か包括化か：組織のレジリエンスのためにとるべきアプローチ



質問：以下の各一対の記述のうち、あなたの組織のサイバーセキュリティ回復アプローチやレジリエンスに該当するのはどちらですか。
調査対象：3,522件
出所：PwC『Global Digital Trust Insights調査 2023年

CROへのメッセージ

2023年に予想されるシナリオでは、CxOの連携が欠かせません。

インシデントは避けがたいものと見られています。余裕を持って対処できるかどうかは、強力かつレジリエンスのあるサイバーセキュリティの土台を構築するためにこれまで行ってきた基礎固めに概ね左右されます。余裕があれば、悪意のあるアクターから受けるダメージを大幅に抑え込むことができます。

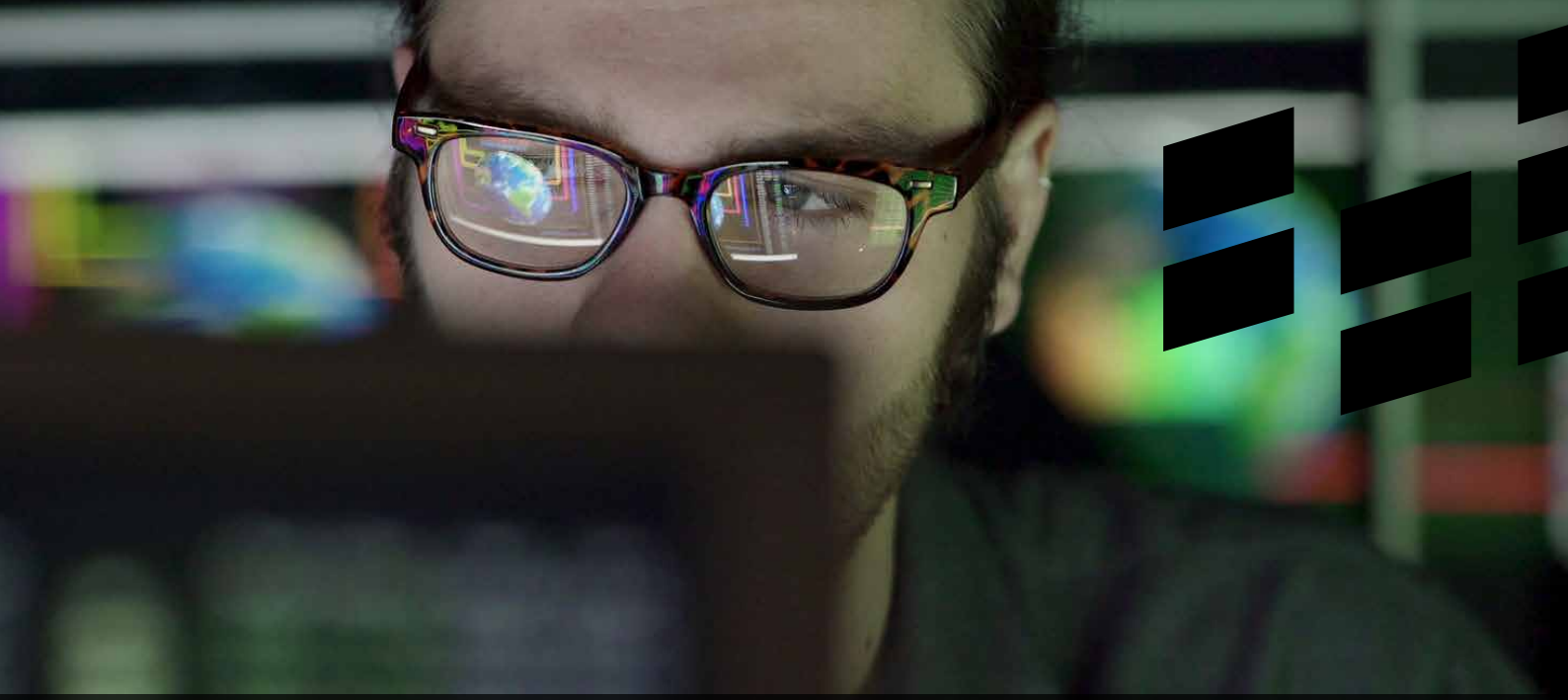
世界各国で、ますます多くの財務当局が、協調して金融機関のストレステストを行っています。規制ガイダンスや当局による執行に向けた動きは、金融サービスの枠を越えて広まりつつあります。

CROとして、「真にレジリエンスを兼ね備えた組織を作るには、CxOが一丸となって、先導していく必要がある」ということを、CISOと連携しつつ、CEOや取締役に対して、論理的に説明していかねばなりません。

CEOたちは、居心地のよい場所を避けるために、たまには外から突き動かされることも必要としているかもしれません。

とりわけCEOが惰性に陥っているような場合には、その必要性があります。会社には既に危機管理計画、事業継続計画、災害復旧計画が備わっているので、行動を起こす必要はないとCEOは考えるかもしれません。しかし、このような計画間の調整はどの程度とれているのでしょうか。組織的にテストしたことはあるのでしょうか。そして、計画に示されている時間軸で、本当に復旧が可能なのでしょうか。

取るべき行動：会社のレジリエンスの限界を知るために、リスク選好を再検討してください。個別のレジリエンスが意味するところは、その組織のリスク許容度とリスク選好によって一部影響されます。危機管理計画、事業継続計画、災害復旧計画を改定して、まとまりのある企業回復計画に仕立て直してください。経営幹部と協調して、問題発生時でも会社を支障なく運営できるよう、調和のとれたアプローチを確立してください。



データセキュリティとプライバシーの保護に向けた協調は喫緊の課題です

各社は顧客の望むものと顧客から得られるものをより良く認識するため、ますます巧みにデータを利用するようになりました。いまやデータは顧客中心のデジタルトランスフォーメーションの一部であり、そのパッケージを構成するものとなっています。

CMO、CDO、CPOの3分の1が、顧客からのフィードバックをモニタリングして、その顧客だけの顧客体験を提供するために、データを常時利用していると言っています。また4分の1を超える回答者が、未開拓のセグメントを見つけ出し、事業の成長を図るために、絶えずデータを利用しています。

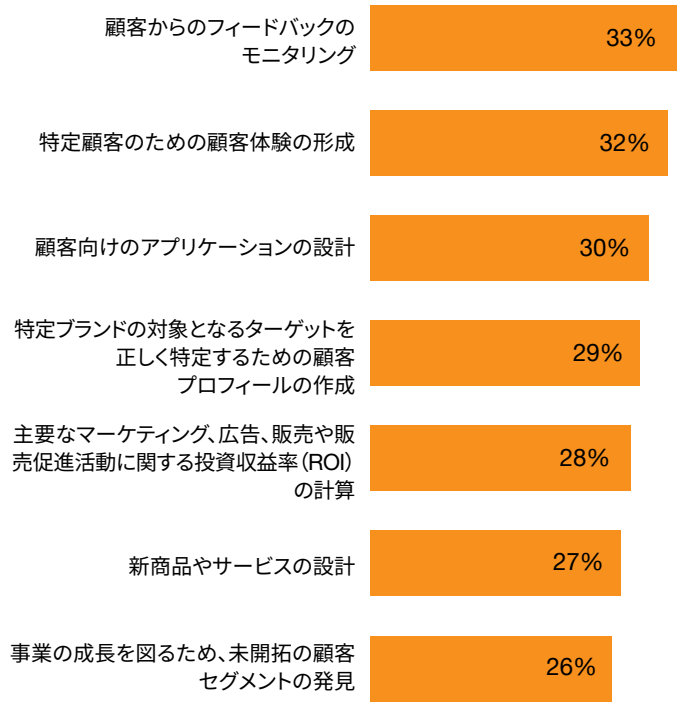
こうした情報の変換から得られる持続的な価値を捕捉するため、各社においてはデータとアルゴリズムを知的に、また効率的に処理して管理する必要があります。それと同時に、公共の倫理やプライバシー上の懸念に取り組み、規制の基準にも適合しなければなりません。

しかし、顧客の同意とプライバシーを本当に真剣にとらえている企業がどれくらいあるのでしょうか。各社の上級幹部が報告するデータ管理とガバナンスへのアプローチには驚くべきものがあります。それと同時に、やっぱりそうかという印象もあります。

CMO、CDO、CPO の 3 分の 1 が、顧客からのフィードバックをモニタリングし、顧客独自の顧客体験を提供するため、データを常時利用している。また 4 分の 1 を超える回答者が、未開拓のセグメントを見つけ出し、事業の成長を図るために、絶えずデータを利用している。

データは顧客サービスのマストアイテムとなっている

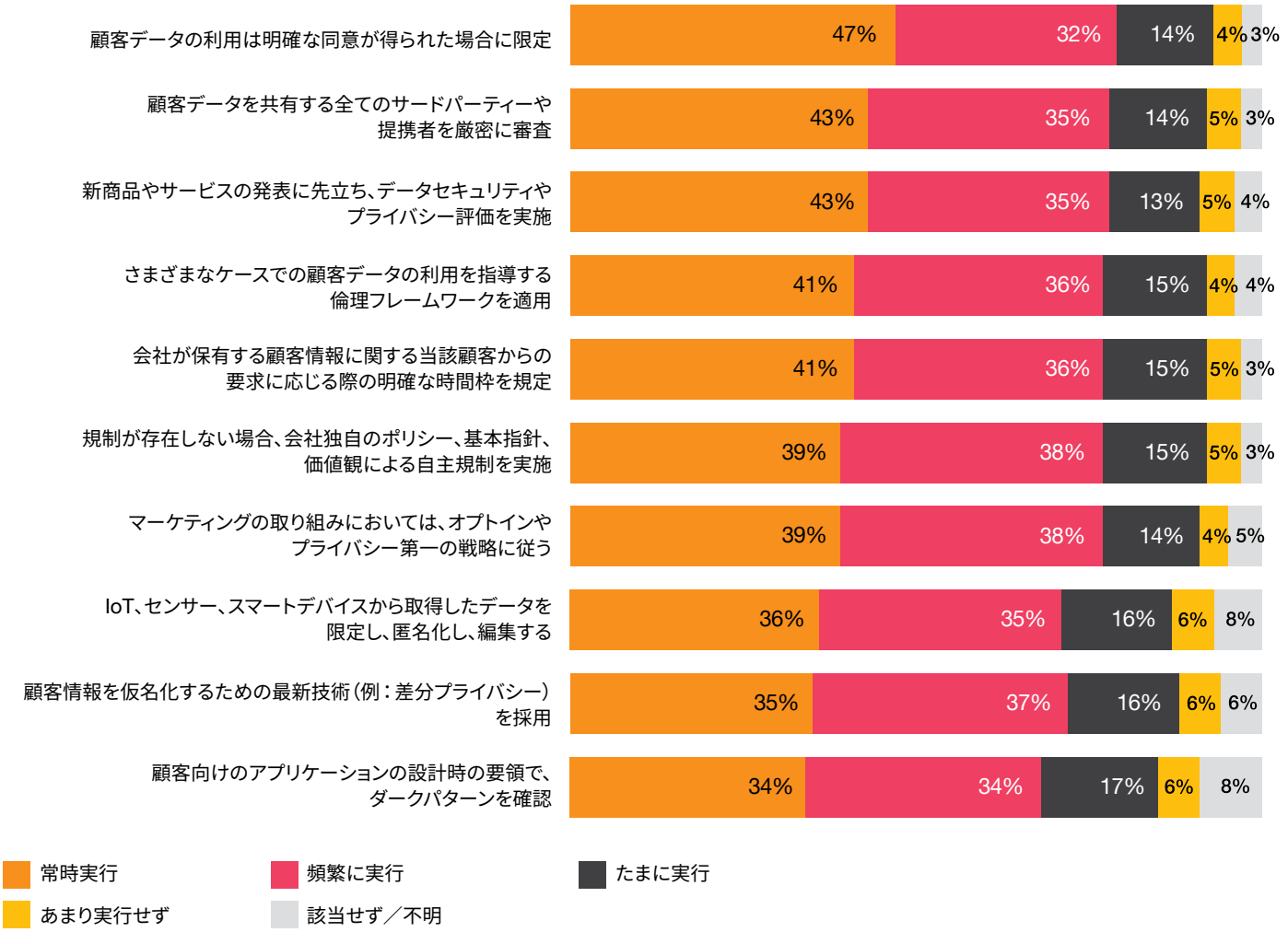
以下の目的で顧客のデータを常時収集・利用している組織の割合（%）



質問：以下の目的のために、顧客データの収集・加工・利用をどの程度行っていますか。
調査対象：CDO、CPO、CMOその他顧客に接する部門の上級幹部　計412名
出所：PwC『Global Digital Trust Insights調査 2023年』

データセキュリティとプライバシーは多くの組織にとってのアキレス腱

以下のプラクティスとポリシーの全てを常時実行しているのは5%だけ



質問：過去12カ月間において、以下のそれぞれに関連するサイバーリスクを軽減するための方策をどの程度講じていますか。1から10で評価してください。
調査対象：3,522件
出所：PwC『Global Digital Trust Insights調査 2023年』

回答者の半数が、顧客からの明確な同意がなくても、顧客情報を使うことが時々ありうると回答

顧客データを共有する全てのサードパーティーや提携者に対する厳密な審査を必ずしも行っているわけではないという回答が、全体の54%を占めています。

そしてこれと同じ割合が、時には、データセキュリティやプライバシーに係る評価を行うことなく、新商品やサービスを発表することがあると回答しています。

ほぼ60%が、顧客が利用するアプリケーションを設計するときの要領で、ダークパターンをいつも確認しているわけではないと言っています。

実際、企業エグゼクティブの50%が、意思決定においてデータの利用が大きく広まらない最大の要因は、セキュリティとガバナンスの欠如だと指摘しています。データが利用しにくいこと（47%）、不正確なこと（42%）、有用性の欠如（42%）が僅差でこれに続いています。

自社のサイバーセキュリティやプライバシーに関するプログラムやこれを担当するチームが、以下の全てを満たしていると自信を持って言えると回答したのは、CMO、CDO、CPO、CISOの5分の1から3分の1にとどまります。

- 信頼を醸成する能力がチームに備わっている（27%）
- 効率的かつ効果的に規制に適合できるよう、マーケティング部門を支援している（25%）
- 一方にセキュリティやプライバシー、他方に事業の成長と収益確保が存在するというトレードオフの関係を役員が検討する機会を与えている（24%）
- 市場での競争力の強化に寄与している（24%）
- 顧客との競争優位性を確保している（21%）

CDO、CPOへのメッセージ

皆さんは、データの管理とプライバシーの保護を改善する必要性を認識しています。PwCのマーケット・ウイナーズ調査2022受賞企業において、信頼の向上に寄与する顧客データの取り扱い、顧客に分かりやすい言葉で記されたデータプライバシー規約の共有が、今後2年間のサイバーセキュリティ投資計画の最上位を占めました。

こうした計画の実行に必要なチームが既に雇用されています。調査対象となったCMO、CDO、CPOは、以下のそれぞれとの間で、とても実効的な協力関係を仕事上で構築していると言っています。

- 最高データ責任者（41%）
- 顧客データ分析チーム（41%）
- トラスト・アンド・セーフティチーム（41%）
- 最高データサイエンティスト（40%）
- 最高デジタル責任者（40%）
- プライバシーチーム（39%）
- 商品開発チーム（37%）
- 市場リスク責任者（37%）
- DevOpsチーム（34%）
- CISO（31%）

顧客ロイヤルティの向上、データ利用の承諾の改善、顧客満足度の向上のために、プライバシーを最優先する事業戦略の潜在的メリットは非常に大きなものがあります。

しかし、取り組みがちぐはぐになる可能性もまた極めて大きいのです。データの管理とプライバシー保護に係る責任を統制できるCISO、CDO、CPOなどの上級幹部の間で、責任の重複がみられます。

しかし、ほとんどの組織にはCDOのポジションがありません。世界の大企業2,500社のうち、上級幹部レベルとしてCDOの職位を設けているのは21%に過ぎません。またCDOを置いている場合でも、保険、銀行、メディア、エンターテインメントなど、限られたセクターと地域（米州）に集中しています（PwC『最高データ責任者調査2021』より）。また、CDOの42%はCxOではありませんでした。

顧客データを非公開のまま企業が安全に利用するには、その管理と保護をどのように行ったらよいのでしょうか。雇用主から始めましょう。目標を明確に伝え、さまざまな責任や伝達を理解しましょう。

取るべき行動：CDO、CPO、CISO は、データセキュリティとプライバシーの管理、利用しやすさ、正確さを含め、重要な全ての観点を 1 冊に網羅したプレイブックを作成し印刷するのがよいでしょう。

CISOとCHROによる人材への認識改善

＋

人員の減少がますます大きな問題となっていると認識するCISO、CIO、CTOは39%にのぼります。また、他の15%はサイバーセキュリティの目標に向けた前進の妨げになっていると考えています。

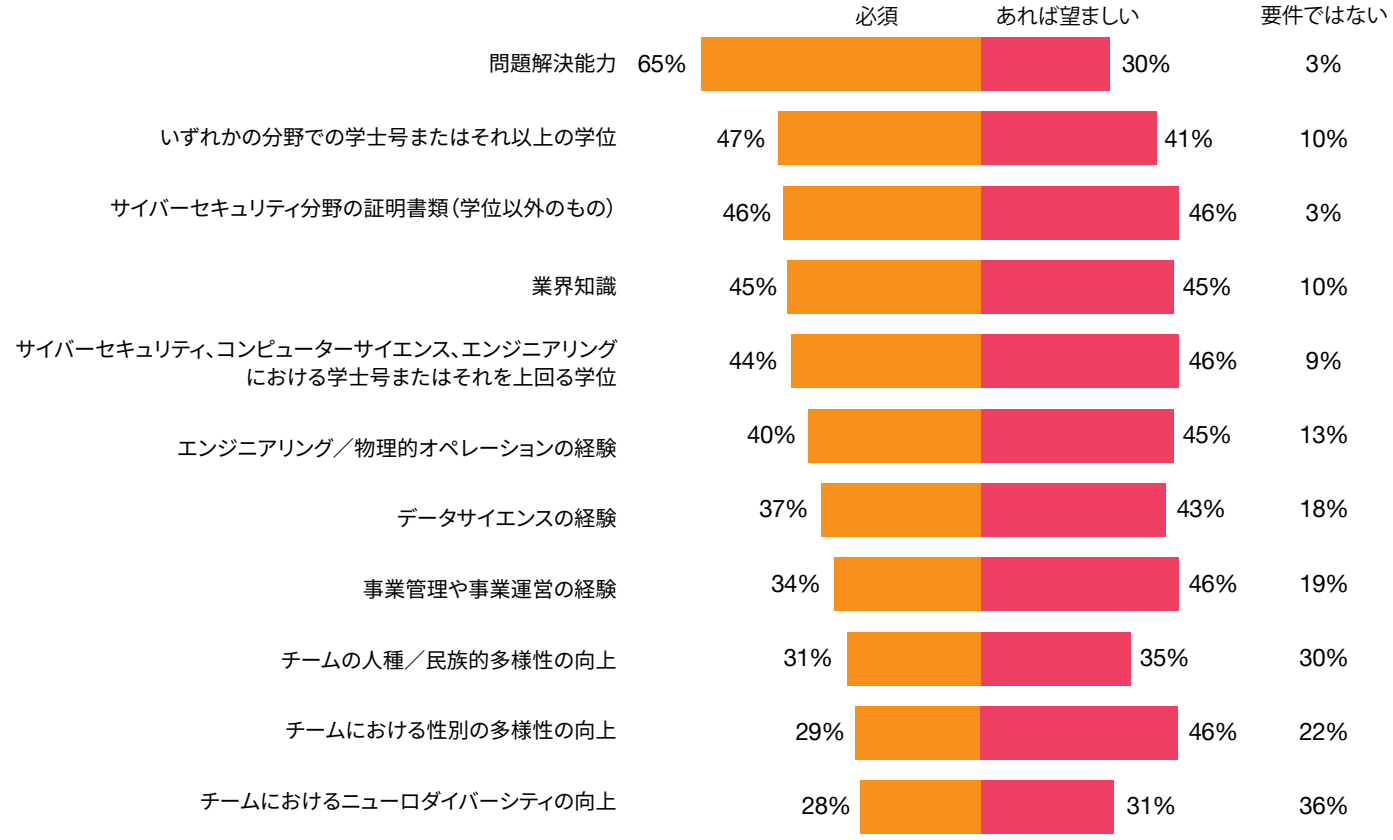
これに対応すべく、CISOやCHROは、旧弊を打破することにより、サイバーセキュリティのポジションをより早く充足し、自社の専門知識を維持しようとしています。

そして、証明書類や技術関連の学位だけでなく、問題解決能力など一部の資質も、少なくともこれらに劣らず重要であるという認識の下で、採用活動において人材を発見するために用いるパラメーターを拡張しています。

こうした発想の転換によって、候補となる人材の層を厚くすることができます。いずれかの分野での学士号またはそれ以上の学位の取得を要件とするとの回答が、サイバーセキュリティ、コンピューターサイエンス、エンジニアリング分野の学士号の取得を要件とするものに迫っています。どちらの学位も要求しないものが約10%あります。

全ての要件において候補者の能力が拮抗している場合には、性別の多様性が選好されることが多くなっています。

要件の拡張により、能力のある候補者を見つけ出すことが容易



質問：サイバーセキュリティチームの人員採用を行うに当たり、最終選考において以下の資質がどの程度考慮されますか。
調査対象：CISO計465名
出所：PwC『Global Digital Trust Insights調査 2023年』

能力のギャップを解消するための方策として、CISOは以下の3つのアプローチが特に有効であると認識しています。

- スキルアップ（45%）
- 採用のためのインセンティブ（入社時一時金等）（41%）
- サイバーセキュリティのためのマネージド・サービス（36%）

マネージド・サービスのセキュリティ確保

2023年において優先的に行うサイバーセキュリティ投資案件中、マネージド・セキュリティ・サービスは、ネットワークセキュリティに次いで第2位でした。

マネージド・セキュリティ・サービス・プロバイダー（MSP）への支出と依存が勢いづくのと同時に、MSPをターゲットにした悪意のあるサイバーセキュリティ活動も増加しています。

2022年5月には、英国、オーストラリア、カナダ、米国のサイバーセキュリティ当局から、このようなトレンドの加速に対して各企業が自己防衛策を講じるように促す共同勧告が発出されています。

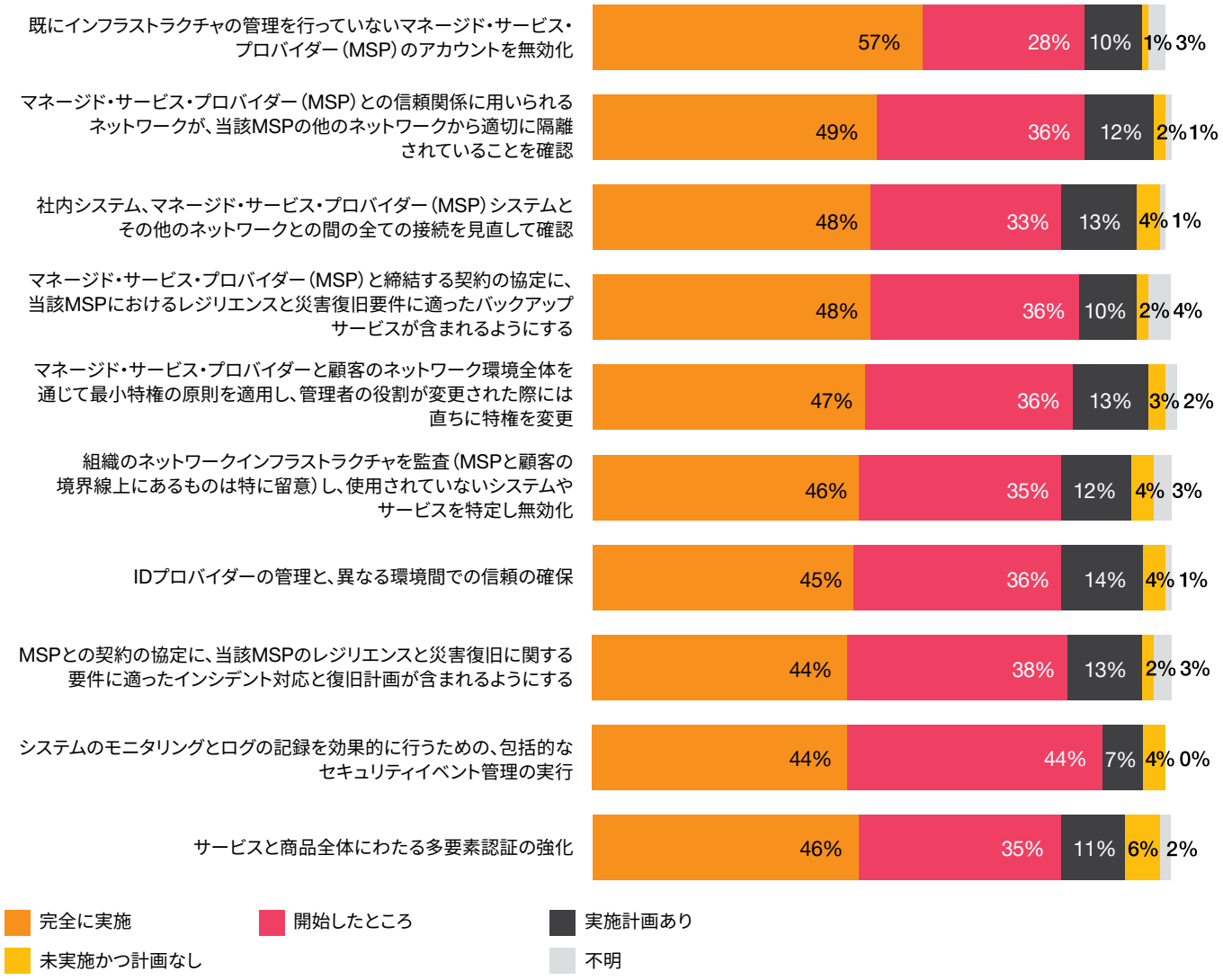
今回調査を行ったCISOのおよそ半数が、サードパーティーのリスクを管理するために、いくつもの対策を十分に講じたとしています。

CISOの57%が、既にインフラストラクチャの管理をしていないMSPのアカウントを無効にしたと報告しています。45%は、全てのサービスや商品にわたって、多要素認証の実施を強化しています。

しかし、まだなすべきことは残されています。全取締役を対象として、こうしたセキュリティプラクティスを全て実行しているのは2.2%に過ぎません。

各企業はマネージド・サービス・セキュリティの利用法を模索

10のプラクティス全てを完全実施しているのは2.2%だけ



質問：マネージド・サイバーセキュリティ・サービスを利用するとの想定において、サイバーセキュリティ人材と能力のギャップに対処するために外部リソースを利用する際に、これに関連するリスクを管理するため、あなたの会社では以下の方策をどの程度実施していますか。
調査対象：サイバーセキュリティ人材のギャップを埋めるための有効な方策として、マネージド・サービスを上位に挙げた回答者計278名
出所：PwC『Global Digital Trust Insights調査 2023年』

CHROへのメッセージ

さまざまなマーケットで従業員の離職率が上昇しています。一方で、景気後退の脅威に直面している企業の側は、雇用計画に不安を抱いています。不透明さが増すなかで、企業は、全ての意思決定を先送りしようとするかもしれません。とりわけ、「大再考時代」「大辞職時代」「静かな退職者」などと、さまざまに表現される現象の下で、危険を避けるために何か新しいことを試みる必要があると認識している場合は、これが該当します。

CISOとリスク担当エグゼクティブは、従業員の減少がもたらす累積的な影響と連鎖的な運営リスクについてCHROが究明できるよう支援する必要があります。才能ある人材を採用して維持するために事業者がどのようにクリエイティブな対応を行うとしても、経営幹部は、会社の評判に対するリスク管理もできるようにしておく必要があります。

取るべき行動：サイバーセキュリティ計画を実施するために、どのようなスキルが本当に必要とされるのかをよく考え、サイバーセキュリティ人材を採用する戦略を見直し、彼らが会社にとどまる動機付けとなるようなインセンティブと成長の道筋を提供してください。マネージド・サービスなどの外部リソースへの依存は今後も高まる一方です。契約にはサイバーセキュリティのための方策も織り込むようにしてください。

サイバーインシデントシナリオとCxO連携の必要性

上級管理者が最も懸念すべきサイバーインシデントのタイプを3つ選定しました。

こうしたシナリオに用いられる戦術と手法を理解するには、技術的な専門知識を必要としますが、その影響が企業経営、財務、データ、リスク管理のそれぞれを担当する役員が対処することを迫られる分野にまで波及するということです。

各CxOが取るべき行動は、規範的なものを意図したわけではありません。むしろ、サイバー攻撃に対して、全面的かつ持続的な対処を行っていくために必要とみられるさまざまな観点から説明しています。サイバーセキュリティの世界では、孤立したエグゼクティブは、インシデント発生の震源地となるのです。

さまざまなシナリオに備えましょう

2023年には、各組織がさまざまな危機のシナリオに直面するなかで、その上級管理者が連携して、事業に支障を来さないように対応できるかどうかが試されることになるでしょう。

破滅的なサイバー攻撃が最大の懸念事項であることは、ほぼ全回答で一致しています。これを2位にしたのはCFOだけです。CFOがトップに挙げたのは、世界的な景気後退と、同時並行的に進行する健康被害への懸念（新型コロナウイルス感染症＜COVID-19＞の再流行）でした。

このようなシナリオ下では、CxOの連携した行動が求められます。しかし、解決のために総力を挙げた取り組みを求められるのは、サイバーセキュリティが唯一であるかもしれません。そして、ほぼ確実に、組織として、ある程度の制御が可能であるともいうことができます。

エグゼクティブの3分の2が、来年において、自らの組織への最も重大な脅威アクターとなるのは、サイバー犯罪だと考えています。サイバー攻撃はビジネスとして隆盛を極めており、サイバー犯罪者にとっては、実入りのよいキャリア形成の機会となっています。

サービスとしてのサイバー犯罪と既成のツールを用いて、犯罪者はさまざまな攻撃を実行あるいは画策して、金を手にすることができるようになりました。例えば、ランサムウェアの実行は、いまやビジネスとして確立しており、主要な犯罪組織は、関係者からランサムウェアをリースしているほどです。サイバー犯罪者は、このようにリースしたランサムウェアを大規模に展開し、複数のターゲットに攻撃を仕掛けることができるようになっています。

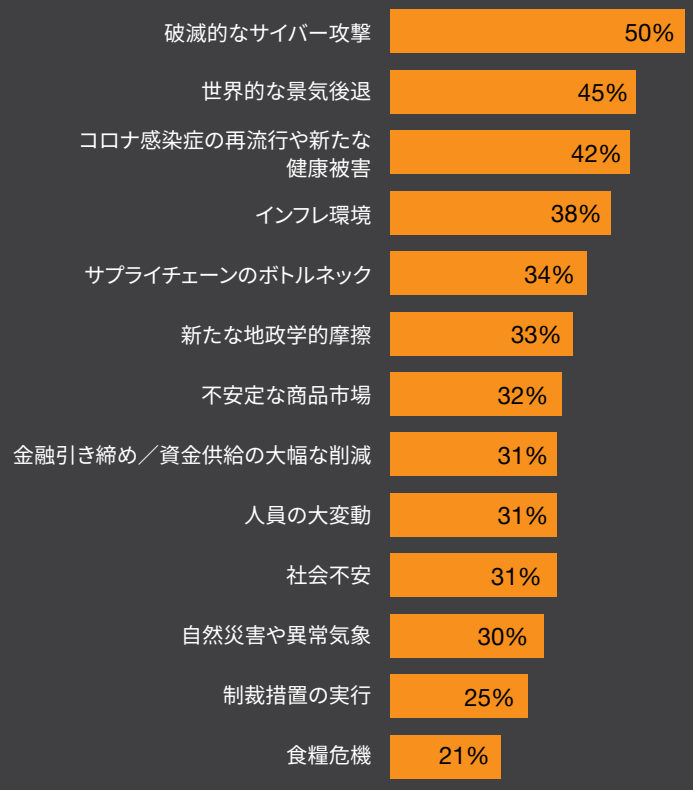
PwCの脅威インテリジェンスグループは、2021年以降、サイバー犯罪ツールを供給する商業的なクォーターマスター、すなわち、スパイウェア、ゼロデイエクスプロイト、その他の種類のマルウェアを、より多くの国の顧客に販売する会社の増加を指摘してきました。

このような世界展開によってサイバー犯罪に手を染めるのが容易になっています。脅威アクターたちは、もはや、自らの手でマルウェアを開発しなくてもよいのです。 同時に、マルウェアが分散されることで、犯人の特定が一層困難になっています。

商業的に手に入れられるこのようなツールは、おそらく政府の役人や民間部門の上級管理者を含む、幅広いターゲットに対して有効です。こうしたタイプの脅威が自らの組織の領域外にあるとみなしているなら、考えを改める必要があります。

認識されている広範な脅威のトップはサイバーセキュリティ

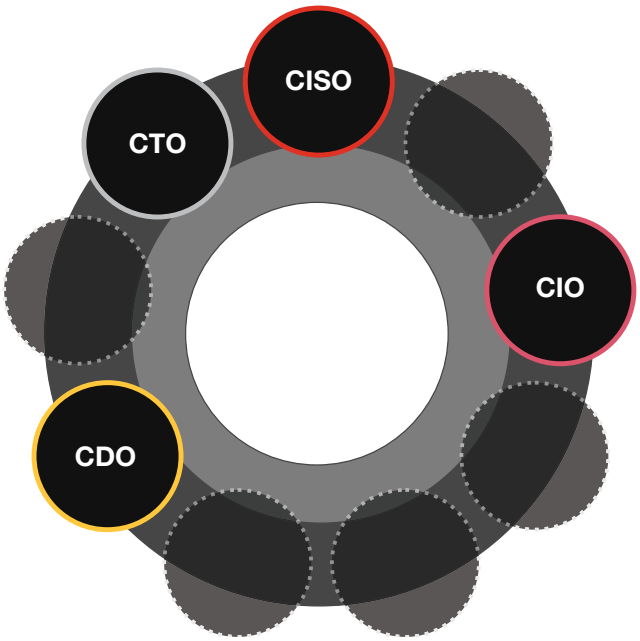
以下のシナリオをトップ5に位置付けた回答の割合（%）



質問：今後12－24カ月間における全般的リスクについて検討し、貴社の組織的な復旧計画に正式に組み込むと思われるシナリオを、上位5番目まで挙げてください。
調査対象：3,522件
出所：PwC『Global Digital Trust Insights調査 2023年』

第1のシナリオ：クラウドベースの攻撃

回答者の38%が、2023年にはクラウド経由の重大な攻撃が増えると予想



侵害の概要

攻撃者がインターネットに接続するクラウドホストのアプリケーションの構成の誤りなどを利用して、ユーザーデータを盗み出した後、ダークウェブ上で販売するなど侵害が生じます。

攻撃がもたらす影響

データ所有者への通知に多額なコストがかかります。また、会社に対する集団訴訟が提起される可能性もあります。さらに、会社への信頼喪失につながることになります。

何が問題？

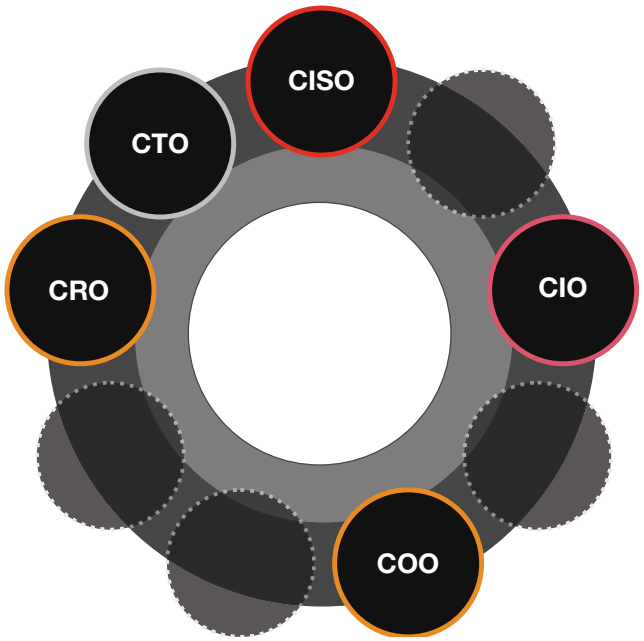
不十分なセキュリティ対策、綿密な防御策の欠如、コードエラー、記述されたコードやライブラリコードテストの不徹底、不適切なデータ暗号化などが挙げられます。

防御を強化するための連携のあり方

- CIO：アプリケーションの開発において（アプリの事前起動テスト期間中を含め）、DevSecOpsを可能にします。ユーザーおよび自動化された展開の二つの方法で構成の誤りを修正します。
- CISO：アプリとデータの保護、脆弱性テストと侵入テスト、修正プログラムの定期的な適用、継続的なコンプライアンスモニタリング、セキュリティイベントやインシデントの監視（SIEM）に係る方針と手順を確立し徹底します。
- CTO：クラウド・サービス・プロバイダーやサードパーティーから、これらの環境全般にわたる構成の誤りを検出するためのダッシュボードやツールの提供を求めます。
- CDO：アプリがプライバシー要件に適合していること、また、顧客データの区分化と暗号化によりその保護が強化されていることを確認します。データの保存中、送信中および使用中に暗号化するための対策を講じます。

第2のシナリオ：制御・運用技術（OT）への攻撃

大企業の29%が、制御・運用技術（OT）への攻撃が増加すると予想



侵害の概要

旧来の制御・運用技術（OT）が抱えている生産システムの攻撃可能な脆弱性がランサムウェアの攻撃を受けるなど侵害が生じます。

攻撃がもたらす影響

被害の拡大を防ぐために攻撃されたシステムをシャットダウンするため、生産・操業停止を余儀なくされ、サプライチェーン全体に影響が波及します。

何が問題？

攻撃者は、パッチが適用されていない脆弱性に対してランサムウェア攻撃を行います。この悪用される脆弱性は、会社のシステムに対するパッチの適用は行われていますが、レガシーシステムに対するパッチの管理、監視、検出能力が不足することによって検出されないまま残存していたために発生しています。

防御を強化するための連携のあり方

- CIO：CISOやCTOと協力して、ITシステムとOTシステムの収束や両者の重要な依存関係をマッピングします。
- CISO：CIOやCTOと協力して、ITとOTとを分離させ、OTに直接アクセスできないように安全なランディングゾーンを開発し、また、従業員に対して適切なアクセス方法やインシデント対応時の役割に関する研修を実施するよう要求します。
- CTO：CISOやCIOと協力して、エンドポイントのパッチ適用とモニタリングに係る計画を策定します。
- CRO：OT環境に存在するサイバーリスクを評価する手法を開発します。ITとOTの対応プロセスをつなぎ合わせるシナリオをインクルードし、かかるシナリオの下でのインシデント対応手順を習熟させます。
- COO：産業用制御システムの調達プロセスにおいて、クラウドプロバイダーとの契約に際して、また、外部のサービスプロバイダーとのサービス契約を定義するに際して、サイバーセキュリティを入念に検討します。

第3のシナリオ：ランサムウェア

セキュリティおよびIT担当役員の45%が、ランサムウェア攻撃のさらなる増加を予想

侵害の概要

医療従業員がフィッシング詐欺メールに添付されたファイルを開けることで、マルウェアがアクティブ化されました。

攻撃がもたらす影響

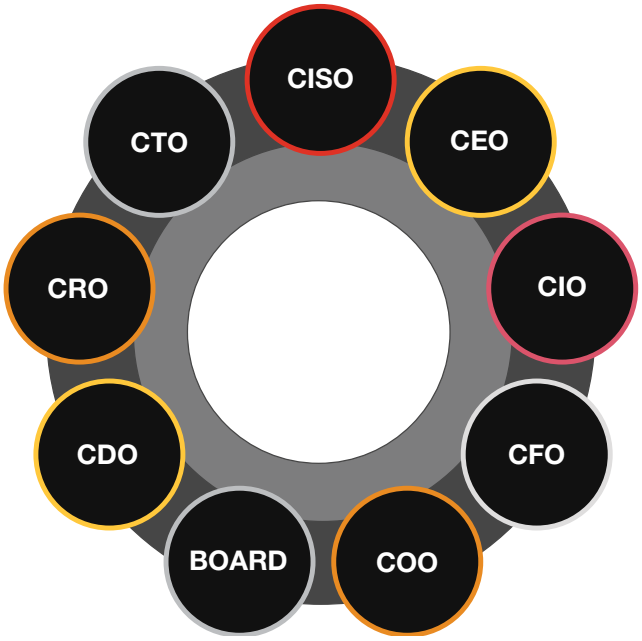
サービスにインシデントが発生し、病院のネットワークがほぼ完全にシャットダウンしました。

何が問題？

アンチウイルスソフトウェアの有効期限が切れていたため、悪意のある添付ファイルに仕込まれたマルウェアを検出できなかったために被害が発生します。多要素認証がなかったことが、攻撃者に最初のアクセスを許すことになりました。その後数週間にわたり社内ネットワークで検知されなかったことから、このサイバー犯罪者は、ネットワーク内を偵察し、最終的にドメイン管理アカウントを取得します。そして、昇格された特権を獲得し、重要なITインフラストラクチャの大部分をシャットダウンしてバックアップを侵害するマルウェアの起動に成功しました。

防御を強化するための連携のあり方

- CEO：全組織的なセキュリティ認識研修を支援します。
- CIO：ITシステムと組織の環境とのつながりを再検討します。
- CTO：医療デバイスを狙う攻撃シナリオにおいて、当該デバイスの脆弱性を評価します。
- COO：類似の状況下において患者の安全確保のためにとるべき対応の強化をはかるため、CIOとCISOを支援します。
- CISO：ITと制御・運用の間に存在するセキュリティギャを埋めます。
- CDO：COO、CISO、CPOと協力して、顧客データの盗難や破損に伴うダメージの評価を行います。



- CRO：危機管理チームおよびBC／DRチームとともに、レジリエンステストを実施します。
- CFO：CISOやCIOと協力して、規制当局や一般向けの情報開示を行う。発見された脆弱性の観点から、CISOやCIOと協力して、サイバーセキュリティ関連の支出（サイバーセキュリティ保険を含む）の再検討を行います。ランサムウェアの身代金支払いに関する会社の方針を決定します。
- 取締役：ランサムウェア攻撃に備えた管理職による机上訓練についての理解を深めます。サイバーインシデントやランサムウェア攻撃を受けた場合、取締役に情報を上げるべきタイミングを確認します。

ランサムウェアイベントのインシデントの事後レビューの事例については、アイルランド保健サービス委員会（HSE）に対するランサムウェア「Conti」によるサイバー攻撃を参照してください。

本調査について

『Global Digital Trust Insights 2023』は、ビジネス、技術、セキュリティの各分野を担当するエグゼクティブ（CEO、企業役員、CFO、CISO、CIO、CxO）3,522名を対象として、2022年7月から8月にかけて実施した調査です。また、女性エグゼクティブが占める割合は全体の31%です。

回答者の52%は大企業（売上高10億米ドル以上）のエグゼクティブ、16%は売上高100億米ドル以上の企業のエグゼクティブです。

回答企業の事業分野は、製造業（24%）、技術・メディア・通信（21%）、金融サービス（20%）、小売・消費者市場（18%）、エネルギー・電力・資源（9%）、保健衛生（5%）、政府・公共サービス（3%）と多岐にわたっています。

回答者の活動拠点は以下の通りです。西欧（31%）、北米（28%）、アジア太平洋（18%）、南米（12%）、東欧（5%）、アフリカ（4%）、中東（3%）。

Global Digital Trust Insights調査は、かつて情報セキュリティに関する世界情勢調査（Global State of Information Security Survey、GSISS）と呼ばれていたものです。

本調査は、PwCで市場調査とインサイト提供を担当するグローバルな研究拠点であるPwCリサーチが実施しました。

pwc

本調査に関するお問い合わせ先

Sean Joyce

Global Cybersecurity & Privacy
Leader, US Cyber, Risk & Regulatory
Leader
PwC US
sean.joyce@pwc.com

日本のお問い合わせ先

PwC Japanグループ

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

丸山 満彦

PwCコンサルティング合同会社
パートナー

綾部 泰二

PwCあらた有限責任監査法人
パートナー

www.pwc.com/jp

本報告書は、PwCメンバーファームが2022年3月に発行した『2023 Global Digital Trust Insights』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：2023年1月　　管理番号：I202210-03