EXECTIVE PERSPECTIVES ON TOP RISKS

トップリスクに関する
エグゼクティブの視点

2024 & 2034

CAEが予測する厳しいリスク環境：サイバー攻撃の脅威、人材不足、テクノロジーの混乱が大きく立ちはだかる

アンドリュー・ストルザース-ケネディ著
グローバルプラクティスリード、内部監査・経理財務アドバイザリー

世界のエグゼクティブから寄せられた2024年および10年後におけるリスクの洞察を統合して分析した結果、関連性のある課題がいくつか明らかになりました。これらは組織のビジネスの俊敏性や回復力を試す重大な出来事になる可能性があります。

トップリスクの注目度が前年度からどのように変化したかを見ると、地政学的動向の激化に起因する事象を含め、市場を混乱させる可能性のある状況の変化が多いことに気が付きます。こうした事象の多くは、ビジネスモデルや微妙に変化するグローバル市場での競争バランスに、長期的な影響を及ぼすと予想されます。このような現実の変化を認識し、事業戦略に沿った全社的なリスク分析を通じてその変化に対応する取締役やCレベルの経営幹部は、組織が避けることのできない破壊的な変革に直面した際の準備と適応能力を、競合他社と同等またはそれ以上に高めて差別化するスキルを有しています。

ノースカロライナ州立大学とプロティビティのERMイニシアチブは、第12回の年次調査で、世界中の取締役および経営幹部が現在関心を寄せているトップリスクについて報告しました。このグローバル調査の結果は、来年（2024年）および10年後（2034年）に広範なリスクがどの程度組織に影響を及ぼす可能性があるかについての彼らの見解を反映したものです。本調査の回答者には、世界各国から1,143名の役員およびCレベルの経営幹部（うちCAEは193名）が含まれ、今後12ヶ月間および今後10年間に、以下の3つの領域から36のリスク課題が及ぼす潜在的な影響について、それぞれの見解を示しました[1]。

- 組織の成長機会に影響を与え得る**マクロ経済リスク**
- 成長を追求する戦略の妥当性に影響を与え得る**戦略リスク**
- 戦略を実行する上で組織の主要な業務に影響を与え得る**オペレーショナルリスク**

1　各回答者は、36の個々のリスク問題を10点満点で評価。【評価が1の場合】回答者の組織には「まったく影響なし」。【評価が10の場合】回答者の組織には「多大な影響」。36のリスク課題それぞれについて、全回答者の平均点を算出。

解説 - 最高監査責任者(CAE)

最高監査責任者(CAE)は最新の「トップリスク調査」に回答したほとんどの経営幹部よりも、近い将来および長期にわたる環境をよりリスクが高いと見ています。最新のトップリスク調査への全Cレベルの回答者の中で、CAEは今後12ヶ月間に組織の業績目標達成能力が問われると予想されるリスクに対して最も高いリスク評価を与えています。またCAEは10年後の2034年に組織が直面すると予想される問題についても、全Cレベルの経営幹部の中で高いリスク評価を与えています。

この2つのタイミングでCAEが最も高く評価している懸念事項はほぼ同じです。CAEは、サイバー脅威を他のリスクを大きく引き離す最大のリスク課題であると考えています。組織がデータ主導型となりテクノロジーベンダーへの依存度が高まるにつれて、サードパーティ・リスクが、サイバーセキュリティ・リスクの急拡大も含めて重要な懸念事項です。人材および技術に関連する問題は、人材管理と技術の活用が内部監査の変革と関連性の鍵を担う役割として、CAEが考える最も重要なリスクです。

2024年のトップリスクの概要

サイバー脅威は、今年のCAEのリスク懸念事項のトップとして際立っており(世界全体の回答では3位)、内部監査リーダーは、このリスクを10点満点で評価し、Cレベルの回答者よりもはるかに高いスコアを付けました。プロティビティとIIAが実施した同種の調査では、CAEとテクノロジー監査リーダーの75%以上が、サイバーセキュリティを高リスク分野と考えていると回答しています[2]。これらの調査結果は、CAEのリスクに対する考え方やサイバーリスクとその影響の流動的な性質を考えれば理解できることであり、サイバー情勢は間違いなくより複雑になっています。ランサムウェアやフィッシングからSIMスワッピングに至る高度なテクニックを駆使する国家や洗練された集団を含む悪意のある行為者の増加は、規制上の影響や評判の管理など、多方面にわたって組織のリスクと危険度を高め続けています。顧客や取引先のデータの損失は重大な結果をもたらしており、米国証券取引委員会(SEC)は最近、重要なサイバーインシデントを経験した公開企業に対する開示要件を最終決定することとなりました。

2023年7月、SECは上場企業によるサイバーセキュリティのリスク管理、戦略、ガバナンス、およびインシデント報告に関する規則の改正を採択しました[3]。4営業日以内に事故を報告しない場合は、ほぼ例外なく規制当局からの罰金と調査が発生し、組織が公表されることとなります[4]。SECのサイバー開示規則は、内部監査機能と年次監査計画に大きな影響を及ぼし、包括的なサイバーセキュリティ・リスク評価と、脅威と侵害をタイムリーに特定し伝達する計画を要求しています。また、組織がクラウドベースのシステムやその他のインターネットに接続しているデバイスの利用を拡大し、さまざまな事業運営や優先事項をサポートするためにデータの収集を増やすにつれて、セキュリティとプライバシーが切っても切れない関係になっていることも明らかです。

CAEと内部監査部門が経営陣と協力して潜在的なサイバーリスクに対応し軽減するためには、これらの分野について一緒に考えることが不可欠です。特に、組織のリスク管理、ガバナンス、内部統制のプロセスが効果的に機能していることを独立した立場から保証する使命の一環として、内部監査のリーダーは、指導的立場にある同僚が、情報公開および財務報告プロセス全体におけるサイバーセキュリティ関連の責任を理解していることを確認する必要があります。

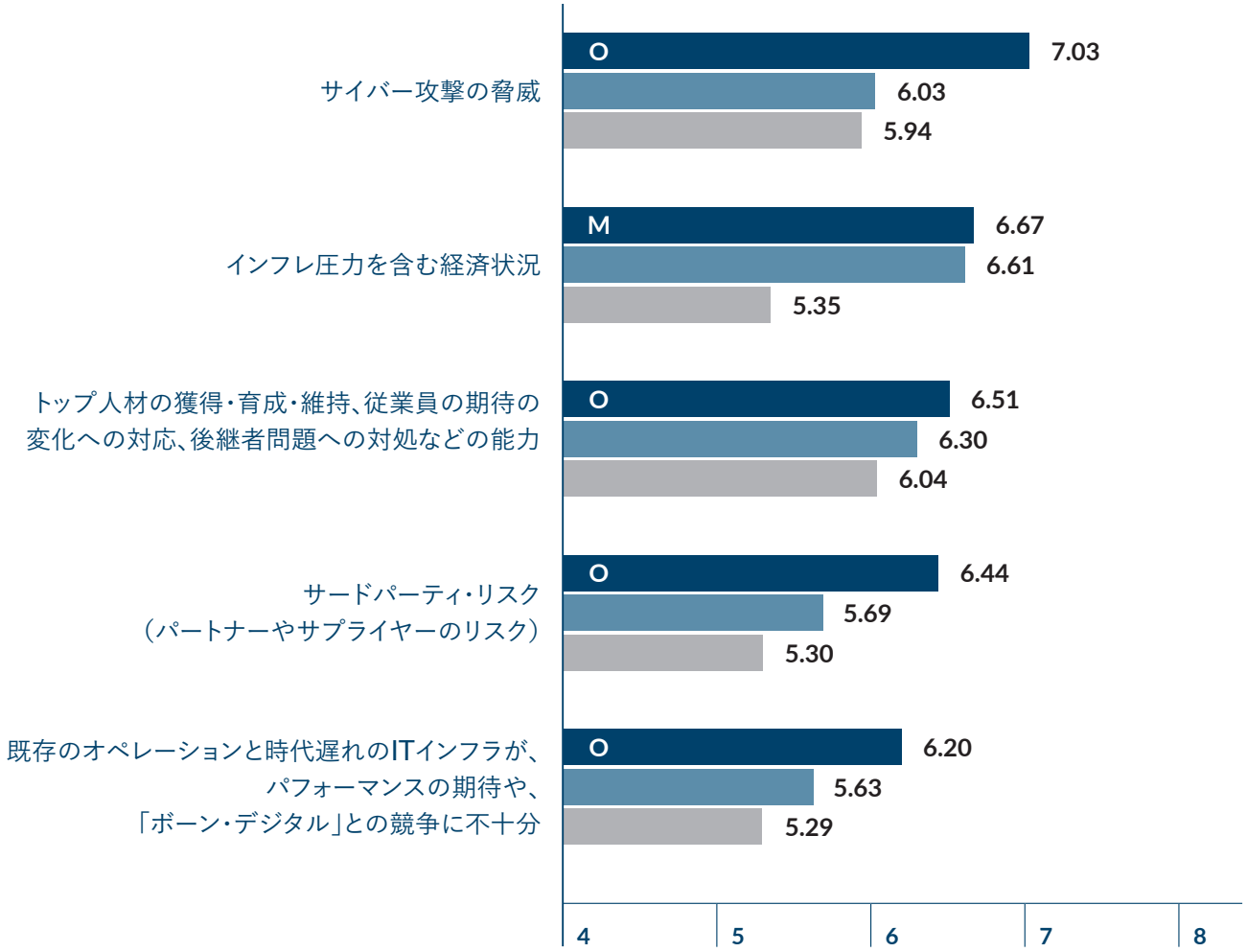
CAEの2024年のその他リスク懸念として、インフレ圧力を含む経済情勢、人材管理と後継者問題、第三者リスク、技術インフラの老朽化または不十分さに関連するリスクなどが高く位置づけられています。

2 Navigating a Technology Risk-Filled Horizon: Assessing the Results of the Global Technology Audit Risks Survey, Protiviti and The Institute of Internal Auditors, October 2023: www.protiviti.com/gl-en/survey/it-audit-survey.

3 "SEC Cybersecurity Disclosure Enhancements: Efforts to Boost Investor Confidence," Protiviti Flash Report, 2 August 2023: www.protiviti.com/us-en/flash-report/sec-cybersecurity-disclosure-enhancements-efforts-boost-investor-confidence.

4 具体的には、組織は、違反が重大であると判断されてから4営業日以内に報告しなければならない。

CAEs – 2024



M マクロ経済リスクの問題　S 戦略的リスクの問題　O オペレーショナルリスクの問題　2024　2023　2022

CAEが2024年に想定しているサードパーティ・リスクの大きさと深刻度は、昨年の調査におけるこれらの分野に対する見解と比較して大幅に高くなっています。このような重要性の高まりは、少なくとも部分的には、サードパーティおよびフォースパーティのリスク管理がサイバーセキュリティ全体にとって、ますます重要な要素であるという理解を反映しています。組織はサードパーティやベンダーやその他のビジネス・パートナーといったエコシステム内の他のメンバーとも、より多くのデータを共有し続けています。この共有データの重要性は、企業が情報からより多くのビジネス価値を生み出すにつれて高まっており、世界的な規制当局の監視の強化や、信頼性と透明性に関する利害関係者の期待によってさらに高まっています。これらの要因により、第三者プロバイダーに対する厳格なリスク評価が不可欠となっています。幸いなことに、CAEとその内部監査グループは全社的な責任を負っているため、組織がテクノロジーとデータ関連の活動だけでなく、より広範なニーズをサポートするために依存しているベンダー像を明確に把握しています。

経済情勢に関しては、過去24ヶ月間の世界経済の不安定さを考えれば、CAEの見解は驚くべきものではありません。2024年初頭には、インフレ傾向が緩和され明るい経済指標がいくつか出てきたとはいえ、CAEは依然として警戒し

ています。不安定な地政学的情勢、予期せぬ経済イベント、さらには常に起こり得る自然災害の脅威も、景気を下向きに転じさせる誘因のひとつです。景気の明るいニュースも増えている（そして不況に向かうと「自ら語ること」の罠は避けなければならない）が、CAEをはじめとするビジネスリーダーは、事態が急速に変化する可能性があることを理解しています。特に、地政学的緊張の高まりとサプライチェーンにかかる試練、そして今年世界中で行われる多くの重要な国政選挙を考慮すると、経済の見通しに関する不確実性は2024年を通して続く可能性が高いです。

優秀な人材を獲得し、育成および維持する能力、従業員の期待の変化に対応する能力、後継者計画に取り組む能力は、依然としてCAEの重大な関心事です。人材やスキルに関連するリスクは、内部監査機能だけでなく企業全体に関わるものです。組織全体として、人材の採用と確保はかつてないほど大きな課題となっており、競争は激しく、熟練した専門家の数は減少しています。今後数年間は、ベビーブーム世代の従業員が引退に向かう一方で、その不足を埋めるために相応の人材が入社してこないため、課題はさらに大きくなるでしょう。

優秀な人材を獲得し、育成および維持する能力、従業員の期待の変化に対応する能力、後継者計画に取り組む能力は、依然としてCAEの重要な課題です。

CAEにとって、こうした人材やスキルに関する懸念は内部監査機能にも及んでいます。多くの経験上、内部監査計画にしばしば盛り込まれる広範なリスク領域に対応するために必要な人材を獲得することが困難であり、ましてやイノベーションと変革活動に十分に注力することも困難です。内部監査のリーダーたちは、有能な候補者を採用し人材を確保およびスキルアップする能力が、業務遂行を抑制する手ごわい要因になっていると指摘します[5]。

内部監査のリーダーは、2024年のリスク懸念事項として、テクノロジーに関連する他の2つの問題を挙げています。1つは、既存業務とレガシーITインフラによって組織のパフォーマンスが期待を達成する能力を阻害されていると、2つ目は「ボーン・デジタル」組織（創業時からデジタルを前提としたビジネスモデルで発展してきた企業）との競争です。多くのCAEは、先進的なクラウドベースのテクノロジーやその他のデジタルプロセスおよび機能を企業に組み込んでいる他のより機敏な競争相手と対峙しながら、「レガシー」な組織が遅れを取り戻そうとしていることをよく認識しています。組織がテクノロジー近代化のイニシアチブを進める中で、内部監査部門がビジネス担当者と連携し、これらの分野におけるリスク評価、保証の提供、アドバイザリーサービスの提供を支援するだけでなく、組織の広範な変革の取り組みにより深く関与する機会が数多く存在します。

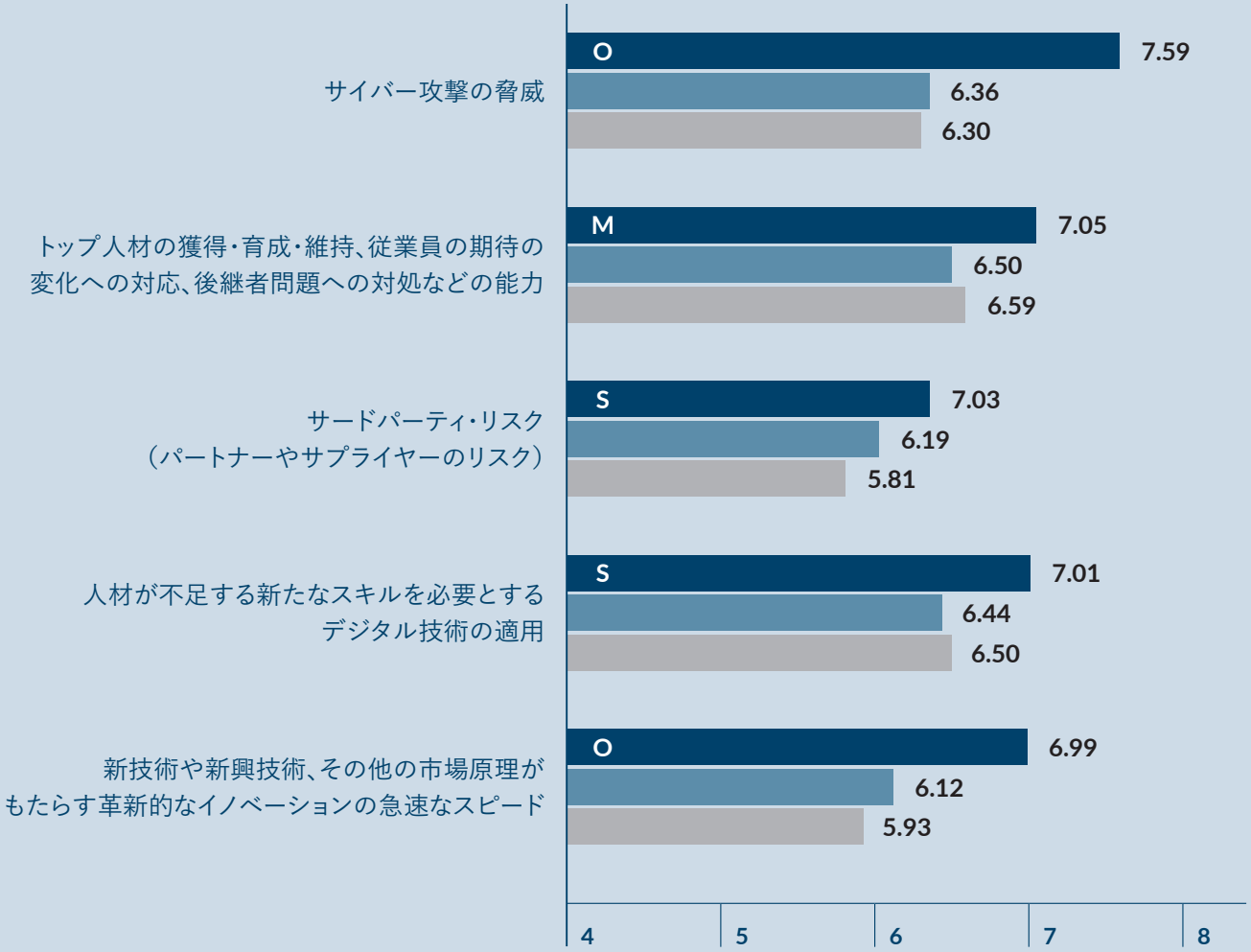
内部監査のリーダーもまた、このリスクが自分たちの領域にも及んでいることを認識しており、特に対峙しているテクノロジーの進歩に伴い、どのような変革や近代化の機会が可能であるかを判断するため、自らの機能内に目を向けるようになってきています。人工知能や機械学習、高度な分析、プロセスマイニング、最先端の自動化への投資などは、内部監査変革の基盤となる推進力です。これらの先進ツールは、優秀な内部監査の専門家たちがスキルセットの拡大、特に先進テクノロジーへの習熟を望んでいることから、採用・定着活動の強化にもつながります。レガシーの技術インフラとその結果生じる対処すべき技術的負債は、これらの次世代内部監査ツールの採用を遅らせ、内部監査機能をボーン・デジタルな競合他社に対して不利な立場に追いやる可能性があります。

2034年のトップリスクの概要

サイバー攻撃の脅威が技術的に高度化および継続的に進化する中、経験豊富なCAEは、今後10年間で自社や第三者のサイバー防御がさまざまな方法で破られる可能性を理解しています。CAEの2034年のリスク懸念はこの厳しい現実を反映して、サイバー攻撃の脅威が2024年のリスク評価と比較してさらに大きな差をつけて再びトップの座を占めており、それはグローバルの他回答者よりもはるかに高いレベルの評価です。サイバーセキュリティの脅威を含むサードパーティ・リスクも、2034年のCAEの懸念事項の上位に入っています。

5 Achieving Audit Relevance, Protiviti, March 2023: www.protiviti.com/gl-en/survey/next-gen-ia-2023.

CAEs – 2024



2024年の評価と比較すると、CAEは2034年の懸念事項のトップリスク全てに著しく高い評価スコアを与えています。この懸念事項には、サイバー攻撃の脅威やサードパーティ・リスクに加え、人材管理と後継者育成計画、スキルの可用性、新興技術による革新的イノベーションの急速なスピードなどが含まれます。

内部監査のリーダーたちは、人材の採用と維持に関する全体的な懸念に加え、デジタル技術の導入に関連するスキルへのアクセスを重大なリスク問題として挙げています。この問題は、内部監査グループを含む組織全体に影響し、内部監査グループの継続的な変革と機能の中核的価値は、高度な監査技術を導入する能力に大きく依存しています。そのためには、CAEをはじめとする内部監査のリーダーが、これらのツールを使用し最適化するために必要な人材やスキルにアクセスする必要があります。技術の飛躍的進歩により、革新的なイノベーションが現在よりもさらに速いペースで生み出されるため、このニーズは今後10年間でさらに強まることが予測されます。

内部監査のリーダーたちは、デジタル技術の導入に関連するスキルへのアクセスを重要なリスク問題として挙げています。

時間が経てば2034年の見通しが持続するかどうかはわかりますが、2024年のトップリスクのいくつかは10年後も間違いなく存在し続けます。10年という時間軸を考慮することは、リスクに関する議論を支配しがちな短期的な思考に異議を唱え、2034年以降に重要となるリスクに対して、より視野を広げ、既成概念にとらわれないアプローチを推進するのに役立つでしょう。

CAE（最高監査責任者）および内部監査のリーダーが検討すべき行動

CAEは、内部監査の変革を進めその価値と関連性を最適化することを追求する一方で、リスク懸念に対処するため、新たな労働市場の現実を反映するよう人材管理の考え方と活動を更新すべきです。また、内部監査機能と企業がサイバーセキュリティ、サードパーティ・リスク、全体的な経済状況に適切なレベルで着目し注意を払う必要があります。この章では、CAEと内部監査リーダーがこれらの分野に取り組むために検討すべき行動を以下に提示します。

サイバー攻撃の脅威：組織は、フィッシングの試みを認識するための従業員トレーニング、高度なマルウェア検知およびセキュリティ監視システムの導入、強固なインシデント対応計画の策定など、多層的なセキュリティ管理策の実施に重点を置くべきです。定期的なセキュリティ監査とコンプライアンス・チェックを実施し、最新のSECガイドラインに合わせるとともに、インシデント対応と復旧能力の有効性のテストに重点を置くべきです。

サードパーティ・リスク：CAE は、包括的なサードパーティ・リスク管理プログラムの実施を提唱します。これにはデューディリジェンス・プロセス、サードパーティのセキュリティ対策の継続的なモニタリング、サードパーティ・リスクの組織全体のリスク管理枠組みへの統合が含まれます。組織は、サードパーティに対するサイバーセキュリティ上の期待と要求を概説する明確な契約を締結します。

人材：組織は、競争力のある報酬体系を提供するだけでなく、戦略的なタレントマネジメント計画を策定します。これにはキャリア開発の機会、従業員の経験、スキルアップや新しいスキル習得プログラム、多様性、インクルージョン、専門性と自己啓発を重視する強固な組織文化が含まれます。

経済情勢：グローバル市場で続く不確実性を乗り切るため、CAEは経営陣と協働し、経済情勢の変化に迅速に適応できる柔軟な財務戦略および経営戦略を策定します。これによりCAEは、監査計画（および個別監査またはアドバイザリープロジェクト）において、業務効率化の推進に適切な焦点を当てるとともに、コスト抑制や関連する施策への好機および潜在的な影響に焦点を当てることができます。

「トップリスクに関するエグゼクティブの視点」調査について

私たちは、世界中のさまざまな業種の役員および経営幹部1,143人を対象として、今後12カ月および今後10年間における36の固有のリスクが組織に及ぼす影響をどう評価するか調査しました。この調査は2023年9月と10日に実施されました。回答者は、各リスクが組織に与える影響を10段階で評価し、評価1は「まったく影響なし」、評価10は「広範囲に影響する」と位置づけました。36のリスクそれぞれについて、全回答者の平均スコアを算出し、スコアの大きいものから小さいものへとランク付けを行いました。

「トップリスクに関するエグゼクティブの視点調査」に関する要約（エグゼクティブサマリー）および全レポートは、プロティビティまたはNC State University ERM Initiativeのウェブサイトをご覧ください。。