



ONRISK

リスクを理解し、認識を合わせ、最適化するためのガイド

2021



目次

はじめに.....	3
OnRiskの調査方法.....	4
2021年のトップリスク.....	5
重要な所見.....	6
重要な所見の説明.....	7
パンデミック対応は、組織体とリスクとの関連性評価を高める.....	8
組織体改善のための優先課題.....	9
組織体とリスクとの関連性については、経営幹部の認識が異なる.....	11
能力については、全体的に認識が一致している.....	12
組織体のガバナンス・リスクについては、認識が分かれる.....	13
新型コロナウイルス感染症のリスク・マネジメントへの影響.....	15
リスクのアシュアランスと3ラインモデル.....	16
リスク.....	19
サイバーセキュリティ.....	20
第三者.....	22
取締役会への情報提供.....	23
サステナビリティ.....	24
破壊的イノベーション.....	26
経済・政治情勢の変動.....	27
組織体のガバナンス.....	28
データ・ガバナンス.....	29
人材管理.....	31
文化.....	32
事業継続性と危機管理.....	33
調査方法.....	35
本レポートの利用方法.....	36
調査方法の活用.....	37
リスク段階.....	38
図表について.....	39

はじめに

リスク

目標の達成に影響を与える事象発生の可能性。

— 内部監査人協会 (IIA) 『専門職の実施の国際フレームワーク』(IPPF)

リスクは現代の経済理論の一部である。確かに、組織化された社会が始まった頃から、リスクを認識し、活用し、管理することで、人類は卓越するようになった。社会、ビジネス、および政府機関が、より複雑化しグローバル化して絡み合うにつれて、リスク・マネジメントの理論と実務を習得することがこれまで以上に不可欠になり、また、捉えどころがなくなってきた。

昨年、IIAは「OnRisk 2020: リスクを理解し、認識を合わせ、最適化するためのガイド」を発表したが、これは、リスク・マネジメントの主なプレーヤーである取締役会、経営幹部、および内部監査部門長 (CAE) の三者の基本的な認識を初めてまとめたものであった。OnRisk 2020は、CAEへの調査とともに、3つの全グループの人々への一連のインタビューを通じて、リスク・マネジメントに最も直接的に影響を与える人々の交流と認識について、独特で洞察に満ちた調査結果を示した。2020年のガイドは、個人の知識とリスクを管理する組織体の能力に基づいて、トップリスクに関する彼らの認識を測定することにより、リスク・マネジメントのプレーヤーである三者間の認識をより一致させることを意図して設計された。OnRisk 2021は、認識の一致を測定する際の要素として、リスクと組織体との関連性に関する主なプレーヤーの認識を追加している。

今年の所見では、重要リスクに関する知識と能力に関する認識がより一致していることが示されているが、一部のリスクの組織体との関連性の認識については、ばらつきがある可能性が示されている。また、本レポートでは、組織体がリスク・マネジメントのアシュアランスをどこに求めるかについても検討している。

新型コロナウイルス感染症の影響を取り上げなければ、2020年のリスクの調査は完結しない。このパンデミックへの対応は、世界経済を長期間閉鎖することによる明らかな影響を超えて、事業継続性、リスク・マネジメント、およびコミュニケーションに関してリスク・マネジメント・プレーヤー間の全般的な認識をより一致させることにも寄与した。パンデミックはまた、組織体が混乱を管理する方法の強みと弱みを明らかにした。しかし、新型コロナウイルス感染症の最も重大な長期的影響は、サイバーセキュリティ、人材管理、経済・政治情勢の変動、および破壊的イノベーションに対するテクノロジーのプラスとマイナスの影響が顕著に加速したこともかもしれない。

OnRiskの調査方法

OnRiskの調査では、組織体のリスク・マネジメントへの主な貢献者の認識を独自に集めるという革新的な手法を用いている。リスクに関する知識、能力、および組織体との関連性についてリスク・プレーヤーの認識を合わせることは、効果的なガバナンスを支える強力なリスク・マネジメントを達成するための重要な一歩である。

調査では、様々な90の組織体の取締役30人、経営幹部30人、およびCAE30人へ定性インタビューを行った。さらに、CAEの協力による定量調査で、348件の回答を得た。

定性調査と定量調査を組み合わせることで、組織体が直面するトップリスクを調べるための強固なデータセットが得られ、リスク・マネジメント・リーダーからの回答に基づく客観的なデータ分析と主観的な洞察の両方が可能になる。OnRiskの調査方法、本レポートの利活用方法、およびOnRiskと併せて開発したリスク段階モデルの詳細は、本レポートの付録に記載している。

2021年のトップリスク

11のリスクは、2021年に組織体に影響を与える可能性が高い幅広い種類から選ばれ、取締役、経営幹部、およびCAEへの詳細なインタビューを通じて精査された。一部のリスクは初回のOnRiskレポートから変更されておらず、説明の一部が更新されているが、その他のリスクはトップリスクのリストに新たに追加されている。これらのリスクは、組織体の規模、業界、複雑さ、または種類に関係なく、普遍的に当てはまるはずである。しかし、このリストは、すべての組織体のあらゆる重大リスクを網羅しているわけではない。この分析から除外されたリスクでも特定の状況次第では、組織体にとって特別な関連性、さらには重要な関連性を持つ可能性がある。

サイバーセキュリティ: サイバー攻撃は高度化し多様化して、組織体のブランドや評判に大きな打撃を与え続けており、多くの場合、悲惨な経済的影響をもたらしている。このリスクでは、混乱や風評被害を引き起こす可能性のあるサイバー脅威を管理するための準備が、組織体に十分に整っているかを検討している。

第三者: 組織体が成功するためには、外部のビジネスパートナーやベンダーとの健全で実りある関係を維持しなければならない。このリスクでは、組織体が第三者との関係を選択してモニターする能力を検討している。

取締役会への情報提供: 規制当局、投資家、および一般市民が取締役会による監督の強化を要求するにつれて、取締役会は意思決定のために提供される情報により大きく依存している。このリスクでは、取締役会が完全で、適時で、透明性が高く、正確で、関連性の高い情報を受け取っていると確信しているかを検討している。

サステナビリティ: 環境、社会、ガバナンス(ESG)に対する意識の高まりは、組織体の意思決定にますます影響を及ぼしている。このリスクでは、長期的なサステナビリティの問題に対処するための戦略を策定する組織体の能力を検討している。

破壊的イノベーション: 私たちは、破壊的なテクノロジーに支えられた革新的なビジネスモデルの時代にいる。このリスクでは、組織体が混乱に適応したり、混乱を利用したりする準備ができているかを検討している。

経済・政治情勢の変動: 国政選挙、多国籍貿易協定、保護関税の新設または延長、およびマクロ経済循環のタイミングに関する不確実性はすべて、組織体が活動する市場に変動をもたらす。このリスクでは、動的で潜在的に不安定な経済・政治環境下で組織体が直面する課題と不確実性を検討している。

組織体のガバナンス: ガバナンスとは、組織体がどのように指揮・管理されるかについてのあらゆる側面、すなわち、組織体を運営するための規則、慣行、プロセス、およびコントロールのシステムを包含する。このリスクでは、組織体のガバナンスが目標の達成を支援しているか妨げているかを検討している。

データ・ガバナンス: 組織体のデータへの依存度は飛躍的に拡大しており、テクノロジーの進歩と規制の変更によって複雑化している。このリスクでは、データの収集、使用、保存、セキュリティ、および廃棄など、組織体の全般的な戦略的データ管理を検討している。

人材管理: 成長するギグ・エコノミー、動的な労働条件、およびデジタル化の継続的な影響により、仕事のやり方が再定義されている。このリスクでは、組織体が目標を達成するために適切な人材を見極め、獲得し、スキルを磨き、定着させる上で直面する課題を検討している。

文化: 「ここでの仕事のやり方」は、多くの企業不祥事の核心になってきた。このリスクでは、望ましい行動を促す姿勢、インセンティブ、および措置を、組織体が理解し、モニターし、管理しているかを検証している。

事業継続性と危機管理: 組織体は、サイバー侵害やパンデミックから風評スキャンダルや後継者計画に至るまで、存続という重大な課題に直面している。このリスクでは、組織体が準備、反応、対応、および回復する能力を検証している。

重要な所見

OnRisk 2021の調査は、リスク・マネジメントの主な推進者たちがどのように交流し、どのようなリスクが組織体に最大の課題をもたらすかについて、スナップショットを示している。データを分析した結果、リスクがどのように理解され、組織体のリスク・マネジメント能力がどのように認識されているかを明らかにする5つの重要な所見が得られた。これらの所見の詳細な検討内容は、本レポートの後半に記載している。

- 「事業継続性と危機管理」と「サイバーセキュリティ」は、2021年のトップクラスのリスクである。新型コロナウイルス感染症のパンデミックによって前例のない課題がもたらされたことと、テクノロジーとデータへの依存が拡大しつつあることが、この2つのリスクをトップリスクのリストの最上位に押し上げた。従業員が安全性の低い在宅勤務環境へ突然移ったことや、パンデミック対応のために電子商取引へ集中的に移行したことでサイバー脅威が高まったことにより、この2つのリスクは一緒に挙げられることが多い。
- 2つのリスクは、組織体改善のための優先事項を示している。回答者全員が、「破壊的イノベーション」と「人材管理」を組織体との関連性の高いリスクと評価した。しかし、経営幹部は、個人の知識とこれらのリスクに関する組織体の能力を、最も低く評価した。
- 組織体とリスクとの関連性に関する経営幹部の認識は、一般的に取締役会やCAEとは異なる。OnRisk 2021に含まれているリスクと組織体との関連性について、取締役とCAEの認識は概ね一致していた。しかし、関連性に関する経営幹部の評価は全体的に低く、「組織体のガバナンス」と「経済・政治情勢の変動」に対する認識に特に大きなギャップがあった。実際、経営幹部は、「人材管理」、「文化」、「事業継続性と危機管理」などのオペレーショナル・リスクとの関連性は高いと評価した。
- リスクを管理する能力についての認識は、より一致している。今年は、リスクを管理する組織体の能力の評価において、回答がより一層集約されていた。昨年のレポートで指摘された取締役会の過信は、減ったようである。新たなリスク評価と、リスク・マネジメント・プレーヤー間のより頻繁なコミュニケーションと協力を重点を置いた新型コロナウイルス感染症への対応は、組織体の強みと弱みに対する認識をより一致させた可能性が高い。
- 経営幹部は取締役会や内部監査よりも、「組織体のガバナンス」を自らの組織体とは関連性が低いリスクと見なしている。リスクとしての「組織体のガバナンス」の関連性評価の相違は、大きな影響があり意味がある。このリスクに関する経営幹部の関連性評価の低さは、個人の知識と組織体の能力に関する評価の高さと合わせると、この分野に対する経営幹部の過信と、取締役会やCAEとの認識の違いを示している。

重要な 所見の説明

次ページからは、5つの重要な所見について詳しく検討している。前述の通り、OnRisk 2021の定性調査と定量調査は、3つの主な推進者たちの目を通して、リスク・マネジメントの内容と理解に関する率直な認識を引き出すことを意図していた。データの分析により、回答者間の交流と連携に関する重要な洞察が明らかになり、そうした交流と連携がリスク・マネジメントにどのように影響するかについての啓発的な結論が導き出された。



パンデミック対応は、組織体とリスクとの関連性評価を高める

定性調査と定量調査の両方に基づくと、「事業継続性と危機管理」と「サイバーセキュリティ」の2つのリスクは、OnRisk回答者間で組織体との関連性が最も高いと評価されており、これは2020年の独特の状況を反映している。事業継続に関連する明確な現在のリスクは、サイバー脅威に関連して拡大し続けるリスクと並んで評価された(図表1)。

10人中9人(87%)近くの取締役が、「事業継続性と危機管理」を「非常にまたは極めて関連性がある」と評価し、さらに10人中9人(93%)超のCAEが、「非常にまたは極めて関連性がある」と評価した。しかし、経営幹部の中でそのように評価した人ははるかに少なく、10人中6人(63%)が「非常にまたは極めて関連性がある」と評価した。一般的に経営幹部は、調査した全リスクについて、組織体との関連性をより低く評価した。

CAEの評価は、「サイバーセキュリティ」の全体的な評価を高めに歪めており、90%が「非常にまたは極めて関連性がある」と評価した。しかし、取締役は「サイバーセキュリティ」よりも他のリスクを優先しており、「文化」、「人材管理」、「取締役会への情報提供」、および「組織体のガバナンス」を、より組織体との関連性があると評価している。経営幹部は、「サイバーセキュリティ」を全体で2番目に高く評価したが、「非常にまたは極めて関連性がある」と評価した割合は低かった(73%)。

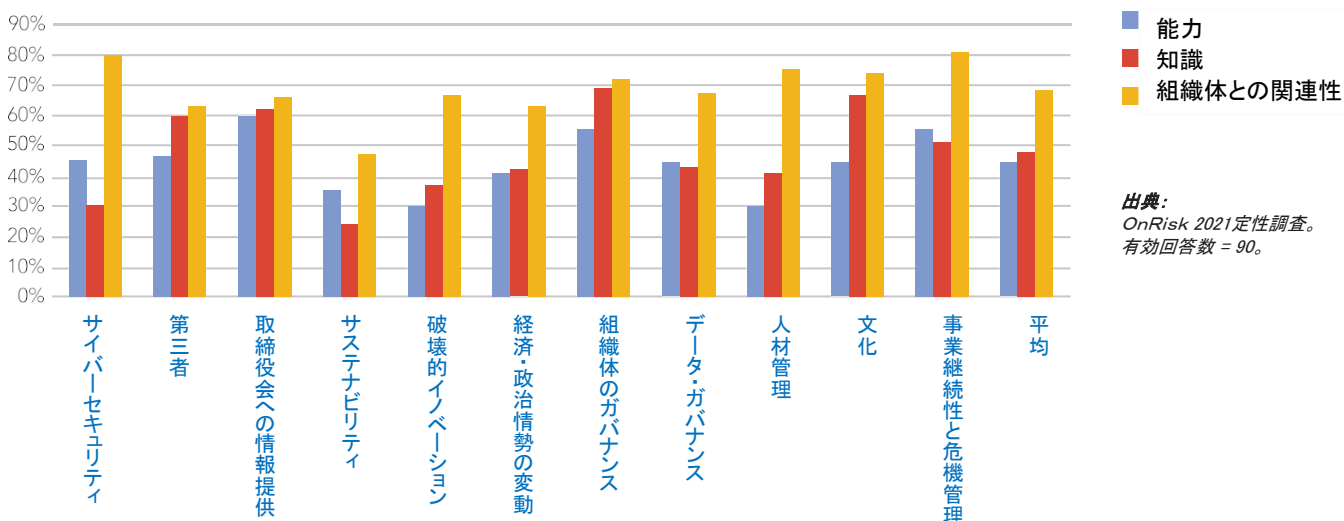
取締役会と経営幹部の回答者は、「サイバーセキュリティ」に関して、個人の知識のレベルを最も低く評価している。これは、テクノロジーの進歩とそれに関連する破壊的イノベーションによって絶えず進化しているリスクについて、不確実性が続いていることを反映している可能性がある。CAEは、このリスクについての知識の評価において、依然として他の2グループとは乖離している。サイバーリスクを管理する組織体の能力については、3つの回答者グループは足並みが揃っており、特に自信がなかった。平均で回答者の半数未満(46%)が、組織体を「非常にまたは極めて能力がある」と評価した。

これら2つのリスクの組織体との関連性に対する新型コロナウイルス感染症の影響は、驚くに当たらない。組織体の存続に対するパンデミックの脅威は、致命的なウイルスに対処するために取られた極端な対策も加わって、新たなサイバー脆弱性を生み出した。例えば、新しいユビキタスな在宅勤務環境では、オフィス外にいる全従業員にサイバーセーフティ・プロトコルを実行させるという途方もない作業が発生した。業務の変更、一般向けの通信ソフトウェアの脆弱性の軽減、顧客やベンダーとの関係の厳格なオンライン管理、および内部監査による往査ができないことによって、サイバー関連リスクの関連性と緊急性の認識は、さらに高まった。

「新型コロナウイルス感染症は確かにリスクを高めている...Zoom会議で財務書類を見せている。」

-製造業/公益事業の取締役

図表1: OnRisk 2021 リスク評価-全回答者

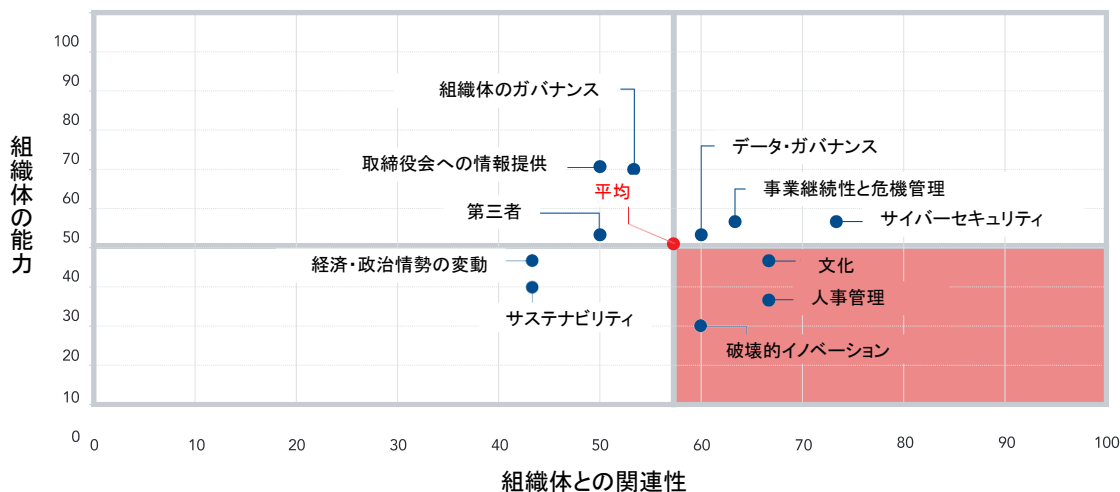


組織体改善のための優先課題

「人材管理」と「破壊的イノベーション」は、改善すべき明確な分野として浮上。

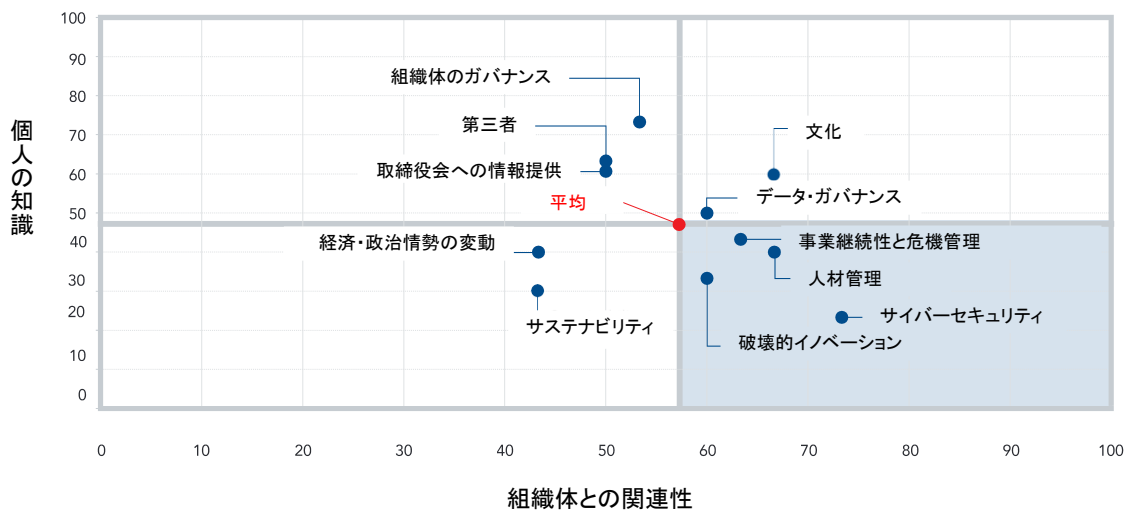
全回答者の中で、「人材管理」と「破壊的イノベーション」は、組織体との関連性の高いリスクとして浮上した。しかし、経営幹部回答者は、これらのリスクに関する個人の知識と組織体の能力について、最も低い評価を与えた。この食い違いは、2つの分野が組織体改善に直結することを明らかにしている。次の比較は、リスク・マネジメントの弱点となり得る分野について、単純だが強力な洞察を示している。下のグラフのX軸(図表2と図表3)は、特定された11の重要リスクそれぞれについて経営幹部回答者が評価した組織体との関連性を示している。対応するY軸は、個人の知識、または各リスクを管理する組織体の能力に関する経営幹部の評価を示している。各グラフの右下の象限は、重要度は高いが知識や能力が低い分野を表している。両方のグラフの右下の象限(強調表示)に「人材管理」と「破壊的イノベーション」が見られることは、これらのリスク分野に最大の改善機会があることを視覚的に示している。

図表2:
改善分野: 経営幹部



出典:
OnRisk 2021定性調査。
有効回答数 = 30。

図表3:
学習機会: 経営幹部



出典:
OnRisk 2021定性調査。
効回答数 = 30。

組織体改善のための優先課題

続き

OnRisk 2021レポートの調査のタイミングは、「人材管理」と「破壊的イノベーション」両方の、組織体との関連性評価に影響を与えた可能性が高い。新型コロナウイルス感染症は、経営幹部に人材管理に関する厳しい決断を迫った。同様に、多くの組織体の競争力が特に弱く、復旧を支援するために新たなテクノロジーを迅速に採用するというプレッシャーを感じていた時期に、経営幹部は継続的な破壊的イノベーションの潜在的な影響を認識して対応した。しかし、両分野に関連する個人の知識や組織体の能力に対する経営幹部の自信のなさ、看過できない。

人材管理

優秀な人材を見極め、採用し、定着させることは、永遠の、そしてグローバルな課題である。新型コロナウイルス感染症への対応として組織体は、ロックダウン、関連するサプライチェーンとキャッシュフローの混乱、および従来の職場からの従業員の集団移動に慌てて対応したため、この種のリスクは著しく複雑になった。パンデミックの影響が数日から数週間、さらに数か月間に及ぶにつれて、賃金の引き下げ、自宅待機、および人員整理が続いた。

人材管理に対するこの重大な混乱は、士気、生産性、および職場文化への影響と同様に、組織体に短期・長期的な影響を及ぼしている。次の3分野は、人材管理が混乱する可能性の証拠を示している。

1. パンデミックに適応するために組織体が新たなテクノロジーを素早く採用したため、新たなスキルや変更されたスキルを持つ人材を見つけることが非常に重要になってきた。この課題に最も機敏かつ効果的に対応した組織体は、パンデミックから強力な立場で浮上する可能性が高い。
2. 在宅勤務という現象は、組織体が高齢人材を採用し管理する方法を根本的に変えてきた。このような雇用契約の加速的な進化には、プラスとマイナスの意味合いがある。従業員の大多数が自宅で業務を行っているため、テクノロジー、サイバーセキュリティ、およびロジスティクスに重大で差し迫った課題があったが、適切な人材を見極めて採用する際の地理的な制約はほとんどなくなった。さらに、組織体が将来的に最高の人材を求めて競争したいと望むならば、在宅勤務という手厚い選択肢は標準となる可能性がある。
3. 雇用の「ニューノーマル」は、ワーク・ライフ・バランスの問題を複雑にし、有給休暇、生産性、士気、および職場文化に関連する人材管理へ多様な影響をもたらした。

破壊的イノベーション

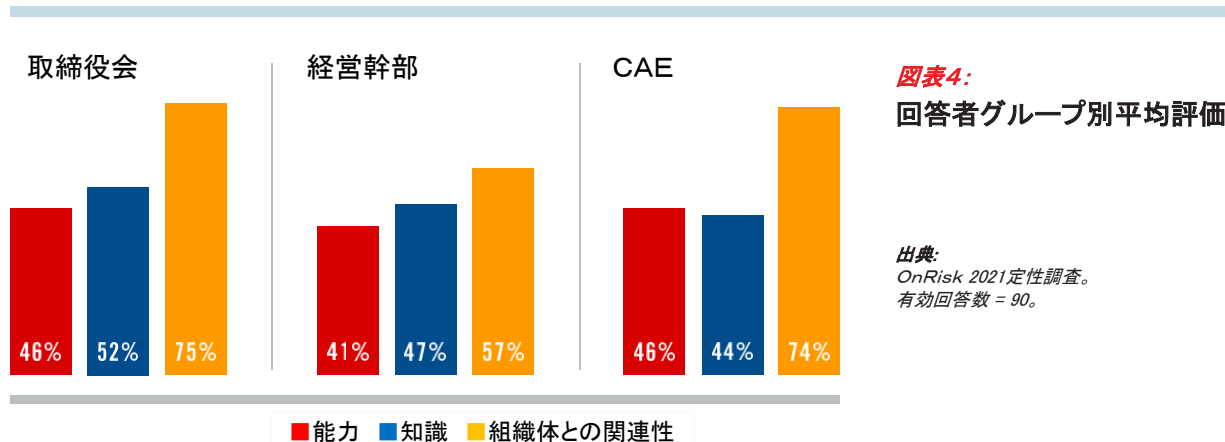
組織体は、パンデミック関連の制約下で効果的に業務を行うための新しい方法を見出すことへのプレッシャーを感じたため、少なくとも短期的には、新たなテクノロジーの採用を加速し、イノベーションに対する慎重な「様子見」のアプローチを放棄した。この対応は、飛躍を遂げることができる組織体にとっては良い兆候である。しかし、このパンデミックへの対応は、重大な弱点となる可能性を露呈した。すなわち、実際には技術革新とそれに関連する混乱の速度を遅らせるものは何もないのに、組織体はこのリスクを活用したり管理したりする準備が整っていないようである。

テクノロジー主導の取り組みは、時代遅れのビジネスモデルを解体し、21世紀で最も有名なブランドのいくつか(Uber、Amazon、Apple、Netflix)を確立した。さらに、破壊の最大の加速は、一連の軌道上の通信衛星を通じて低コストのインターネット・サービスを世界の遠隔地にもたらすことを約束しているスペースX社のスターリンク・プロジェクトのような、強力な技術的進歩を組み合わせることによってもたらされる可能性がある。新たなテクノロジーを受け入れ、最先端の開拓者となる組織体は、成功するのに最適な立場に立てる。そのためには、破壊的イノベーションを理解して活用するだけでなく、それを育む21世紀型の経営が必要になる。

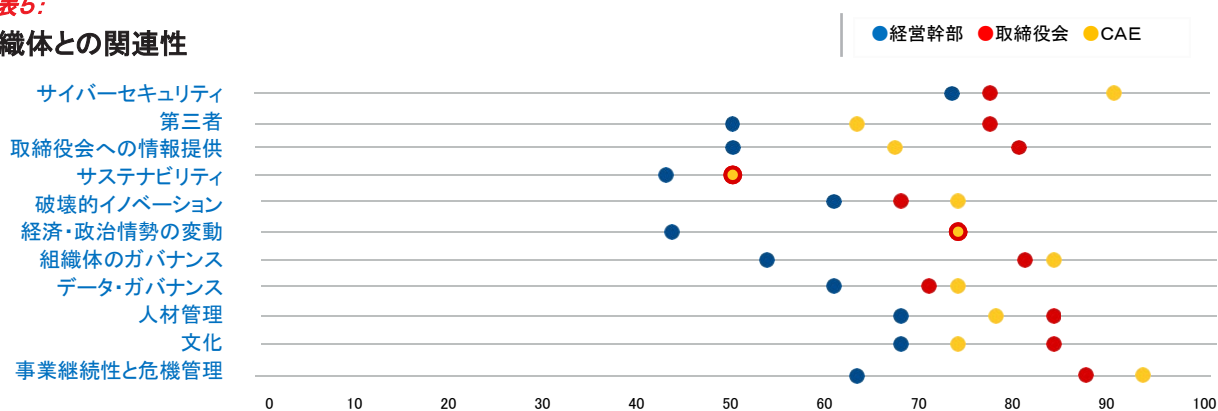
組織体とリスクとの関連性については、経営幹部の認識が異なる

全体的なリスク・マネジメントの尺度としてOnRisk 2021に組織体との関連性を導入することで、ガバナンスに対する重要な洞察がもたらされている。全体的に本レポートで調査した11の重要リスクに関して、個人の知識と組織体の能力については、リスク・マネジメント・プレーヤーである三者間にかなり一致した認識がある。ただし、リスクが組織体にどの程度関連しているかについての平均評価は、経営幹部の評価(57%)よりも取締役会とCAEの間でより一致していた(それぞれ75%と74%) (図表4)。

組織体との関連性評価の詳細な内訳によると、取締役会は経営幹部よりも、組織体と各リスクとの関連性をより高く評価していることをさらに証明している。さらに細かく見ると、どのリスクが各グループにとって最も組織体と関連していたかが明らかになる(図表5)。例えば、「人材管理」と「文化」は、経営幹部と取締役会の両者にとって非常に組織体との関連性が高いようだが、取締役会の関連性評価は、経営幹部の評価をそれぞれ約20%上回った。また、両グループとも「事業継続性と危機管理」の関連性を高く評価したが、取締役会はこのリスクを経営幹部よりも約25%高く評価した。この2つのグループは、「サイバーセキュリティ」リスクの関連性評価で、最も足並みが揃っていた。ただし、「サイバーセキュリティ」リスクの組織体との関連性は、経営幹部回答者にとっては1番目であったものの、取締役にとっては6番目であった。



図表5: 組織体との関連性

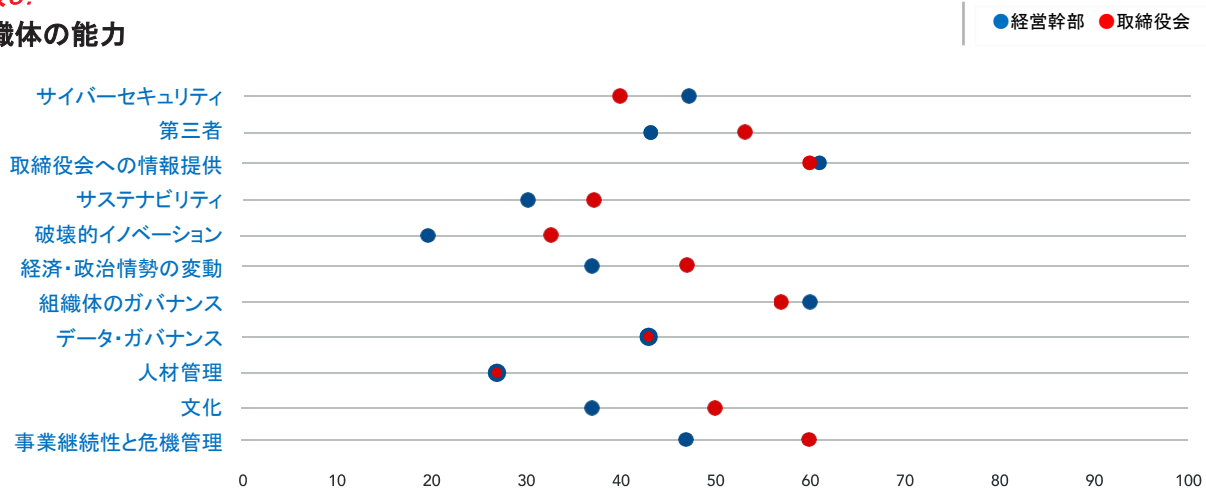


能力については、全体的に認識が一致している

取締役会のリスク・マネジメント能力は、もはや他と乖離していない。

リスクを管理する組織体の能力に関する認識は、2019年と比べてより一致している。これは主に、「人材管理」、「取締役会への情報提供」、および「データ・ガバナンス」(以前は、データ倫理、データ保護、およびデータと新たなテクノロジー)を含むいくつかのリスク分野(図表6)において、取締役会による今年の評価が下がったことによるものである。これは、必ずしも自信の喪失を示すものではないが、これらのリスク分野についてより現実的に理解している可能性が高い。パンデミックは、リスクと能力について、より優れたコミュニケーションと新たな評価を促した可能性がある。これは、2019年と比較して今年は、取締役がリスクに関する個人の知識を平均的に高めに評価したことで裏付けられている。

図表6:
組織体の能力



出典: OnRisk 2021 定性調査。有効回答数 = 60。

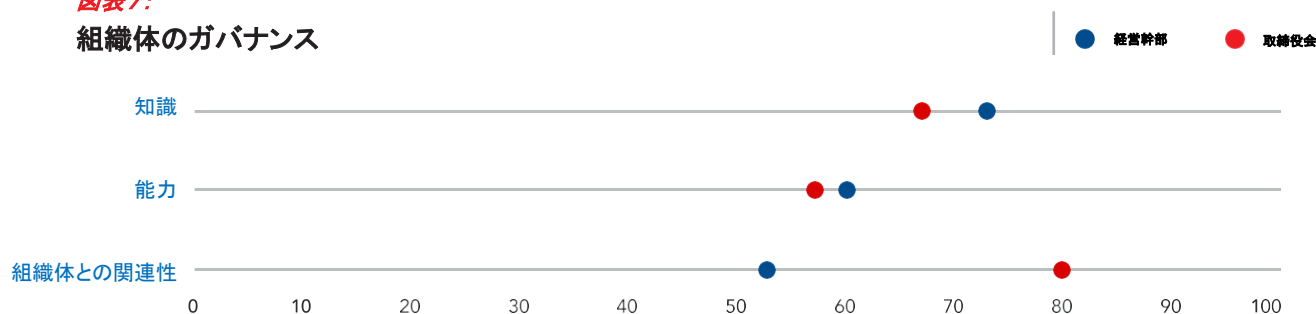
組織体のガバナンス・リスクについては、 認識が分かれる

経営幹部は取締役会よりも、知識と能力を高く、組織体との関連性を低く評価している。

経営幹部は、「組織体のガバナンス」リスクについて、取締役会とはかなり異なる認識を示している。リスクに関する個人の知識とリスクを管理する組織体の能力について、経営幹部回答者は取締役会よりも若干高く評価しているが、組織体とリスクとの関連性については、かなり低く評価している(図表7)。この評価パターンは新たな発見である。

ガバナンスとは、組織体がどのように指揮・管理されるかについてのあらゆる側面を包含するものであり、一般に、経営実績の有用なバロメーターと見なされている。実際、組織体の全般的なガバナンスの強さは、組織体目標を達成する能力を高める。

図表7:
組織体のガバナンス



出典: OnRisk 2021定性調査。有効回答数 = 60。

経営幹部回答者は、「組織体のガバナンス」リスクを管理するための個人の知識と組織体の能力を、取締役会や内部監査よりも高く評価した。また、組織体との関連性については、両リスク・マネジメント・パートナーよりも低く評価した。

経営幹部と取締役会との間の組織体との関連性に関する評価のギャップは、簡単に片付けるべきではない。経営幹部回答者の5割強が、「組織体のガバナンス」リスクの組織体との関連性は、「非常にまたは極めて高い」と評価した。対照的に、取締役会回答者の約8割が、「非常にまたは極めて高い」と評価した。このギャップ(約25%)は、食い違いを示している。このギャップは、個人の知識や組織体の能力に関する経営幹部の高評価と合わせると、経営幹部が「組織体のガバナンス」リスクに関して自信過剰であるか、この分野に関する取締役の懸念レベルを単に認識していないか、のいずれかを反映している。

COVID



新型コロナウイルス感染症の リスク・マネジメントへの影響

新型コロナウイルス感染症は、予期せぬ、歓迎されない、かつ阻止できない、リスク・マネジメントの試練であった。最近の記憶にある他の事象とは異なり、パンデミックは、組織体が卓越したり、競争力を維持したり、あるいは単にチャンスを得るために悪戦苦闘する中で、リスク・マネジメントの実務や実績を検証するよう強いている。

さらにいえば、どんな組織体も逃れることはできず、2つの組織体が同じように影響を受けることもない。新型コロナウイルス感染症は、組織体の規模や官民や新旧を問わず、リスク・マネジメント上の独自の課題と機会をもたらす。それは、各組織体のリスク・マネジメントとガバナンスの強みと弱み、および危機を乗り越えて管理するための機敏性と柔軟性を明らかにする。そしてリーダーたちに、激変が約束されている新型コロナウイルス感染症以降の事業環境において、どのような成功と競争が見えてくるかを想像させることになる。

確かにパンデミックの影響は、仕事と家庭の境界線をいかに曖昧にしているから、社会的交流をいかに再定義し続けているかまで、私たちの生活のあらゆる側面で明らかになっている。ビデオチャット・プラットフォームは、新たな役員会議室であり、ハッピーアワーの居酒屋でもある。フェイスマスクは口紅の売り上げに大打撃を与えているが、ファッションアクセサリーとして急成長している。Amazon、UPS、およびFedExのトラックは、2020年版の移動販売車として近隣地域に侵入している。

OnRisk 2021の調査データは、組織体が短期的なオペレーショナル・リスクをより重視するなど、予想されるパンデミックの影響の一部を確認している。また、リスク意識の向上とリスク・マネジメント・プレーヤー間の認識の一致についても説明している。しかし、最も影響力のある新事実、新たなテクノロジーの採用を加速させる兆候が現れつつあることかもしれない、これは、仕事のやり方を根本的に変えることを期待させる動きである。ある経営幹部回答者は、この加速を「わずか数か月で、テクノロジーの規模を数年分進化させている」と表現した。

破壊的イノベーションを受け入れるためのこの競争の短期・長期的影響は多様であり、最善の状況下であってもテクノロジーの導入は流動的で思うように進まない場合があるため、予測は困難である。新型コロナウイルス感染症以降の世の中の要求を満たすために、異常なスピードで業務プロセス、文化、および顧客体験を変革すれば、嬉しいハプニングと同じくらい多くの致命的なミスに必ずつながる。それはほぼ確実に、組織体が管理する準備をしなければならない、まだ予期せぬ新たなリスクにつながるだろう。

OnRisk 2021のデータとIIAによる追加の調査は、パンデミックからの別の教訓を裏付けている。新型コロナウイルス感染症以前に、組織体内部の強力な関係構築とテクノロジーに投資した組織体は、パンデミックの課題と不確実性に最もうまく耐えることができた。この教訓は、新型コロナウイルス感染症の大きな影響から組織体が浮上する際に重要である。明確に定義されたデジタル化の課題を進めながら、連携を強化し促進できる企業は、パンデミックの余波の中で生き残るための最善の位置が確保できるだろう。

「このウイルスによって『破壊的イノベーション』が引き起こされているのは驚きである。わずか数か月で、テクノロジーの規模を数年分進化させている。破壊的イノベーションの加速は、事実上すべてのビジネスに影響を与える。」

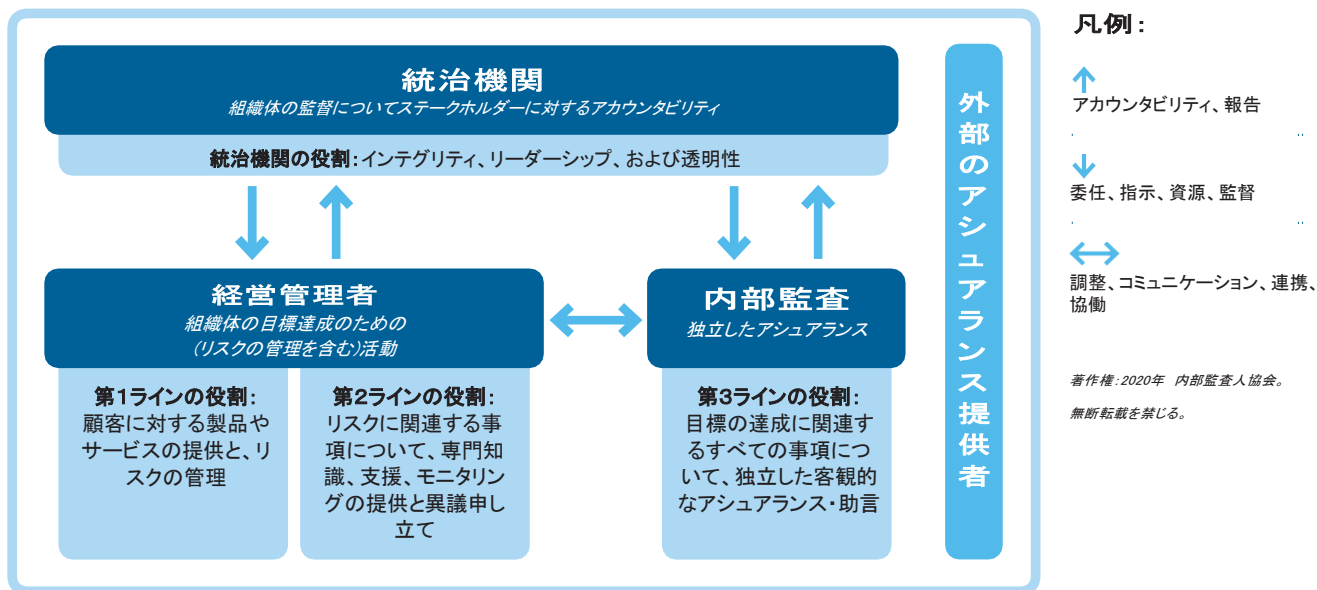
- 保険業、経営幹部

リスクのアシュアランスと3ラインモデル

3ラインモデル(図表8)は、組織体が強力なガバナンスとリスク・マネジメントを促進する構造とプロセスを特定するのに役立つように設計されている。新モデルは、IIAが「3つのディフェンスライン」を改訂して2020年7月に公表したもので、アシュアランスの問題が特に明確になっている。原則ベースのモデルは、統治機関からのアカウントビリティ、組織体の目標を達成するための経営管理者からの(リスクの管理を含む)活動、および独立した客観的な内部監査機能からのアシュアランスを可能にする、適切な構造、プロセス、および役割を明らかにしている。

図表8:

IIAの3ラインモデル



アカウントビリティ、活動、およびアシュアランスを達成するための役割を明確に定義するにあたり、このモデルはアシュアランスに関する重要な指針と、独立した内部監査機能が提供する「厳密な調査と洞察に基づくコミュニケーションを通じた改善」という価値を示している。

しかし、OnRisk 2021の定性・定量調査から得たデータは、真に独立したアシュアランスが不足していることが多く、アシュアランスの提供者は概して一貫していないことを示唆している。リーダーたちは一般的に、誰が提供したかに関係なく、彼らが得ているアシュアランスのレベルに満足している。ただし、この自由放任主義のアプローチでは、独立したアシュアランス評価の価値を検討できない。

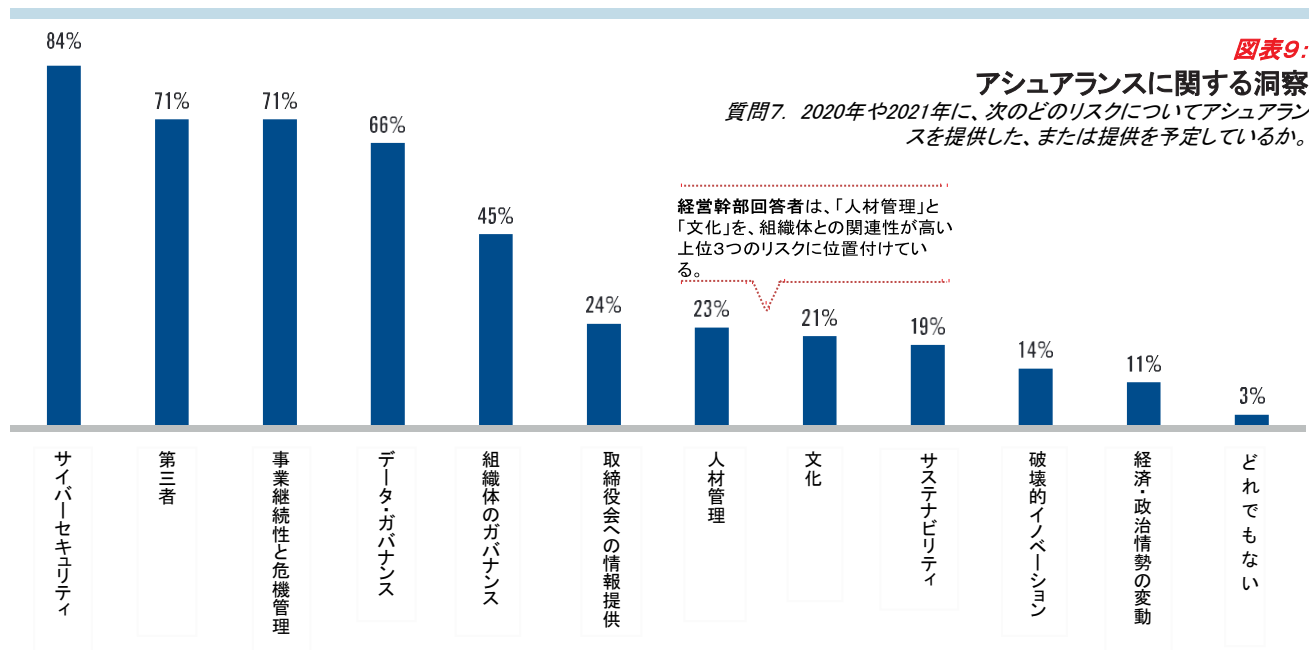
内部監査が対象とする重要リスクの範囲はかなり広いが、完全とはほど遠い。CAEは、OnRisk 2021で調査した各重要リスクに対するアシュアランスを提供していると回答しているが、その割合は、「サイバーセキュリティ」、「第三者」、「事業継続性と危機管理」、および「データ・ガバナンス」以降は劇的に低下している(図表9)。CAEはまた、「経済・政治情勢の変動」と「破壊的イノベーション」の分野ではアシュアランス業務の提供割合を最も低いと回答しているが、CAEグループはこれら両方を組織体との関連性が高いと評価している。

さらに、経営幹部のリスク関連性評価と比較すると、内部監査は、経営幹部が組織体との関連性が高いと評価した上位3つのリスクのうち2つ(11ページの図表5参照)に対するアシュアランスの提供割合が最も低い。アシュアランスの対象範囲が不完全なのは、資源、スキル、または業務範囲の制約による可能性がある。

「一般的にいて、それで十分だと思う。

大きな問題は発生していない…これまでのところ、とても良い。」

- 金融業、経営幹部



出典: OnRisk 2021 定量調査。有効回答数 = 348。OnRisk 2021 定性調査。有効回答数 = 30。

だが、アシュアランスに影響を与えるもう1つの要因は、内部監査をコンサルティング業務として利用することである。組織体は、助言業務を行うための、リスクに関する内部監査の全社的な知識や視点への依存を高めている。十分なリソースがない限り、この慣行は内部監査という資産を従来のアシュアランス業務から遠ざける可能性がある。OnRisk 2021の回答者は、内部監査の組織体内での役割について、様々な認識を示した。取締役会や経営幹部の回答者の中には、内部監査人に対して、「チェック係」に過ぎない会計士、あるいは、真のビジネスパートナーとして信頼できない「警官」、という古い認識を持つ者もいる。また、組織文化と内部監査のリーダーシップの弱さを要因として指摘する者もいる。

図表10:

アシュアランスのヒント

OnRisk 2021の回答者は、アシュアランス業務とプロセスを改善するために、数多くの提言をした。

- 内部監査の業務範囲が組織体のアシュアランス・ニーズを反映するようにする。内部監査人は、単なるチェック係以上のことをしなければならない。
- 内部監査は取締役会に直属するようにして、透明性を高め、情報共有を改善する。
- 監査チームには、知識が豊富で、自信があり、積極的な実務家をバランスよく配置するようにする。
- 内部監査が、コンサルティング業務だけでなく高品質のアシュアランス業務を行うことに重点を置く。
- 内部監査人と外部監査人の役割を明確にする。

「内部監査の役割については、企業によって大きな違いがある。警官のようだと、実は好かれていない場合もある。だが、コントロールを改善するための真のビジネスパートナーであり、また、十分に訓練された従業員のためのリソースと見なされている場合もある。」

- 小売・食料品業、取締役

出典: OnRisk 2021 定性調査。有効回答数 = 90。





リスク

リスクの管理とは、活動するかしないか、予測するかしないか、計画するかしないかによって、何が得られたり失われたりするかを理解して価値を構築する技術である。知らないということを自覚している人は、質問することができる。知らないということを自覚していない人は、無力である。本節では、個々のリスクに関連した重要な所見を検討し、リスク・マネジメントの取り組みを強化するために取締役会、経営幹部、およびCAEが取るべき措置を提言し、さらに、各リスクの進展段階を明らかにする。これらの所見を裏付ける方法と、リスク段階を決定するための定義に関する詳細な情報は、付録に記載している。

リスク

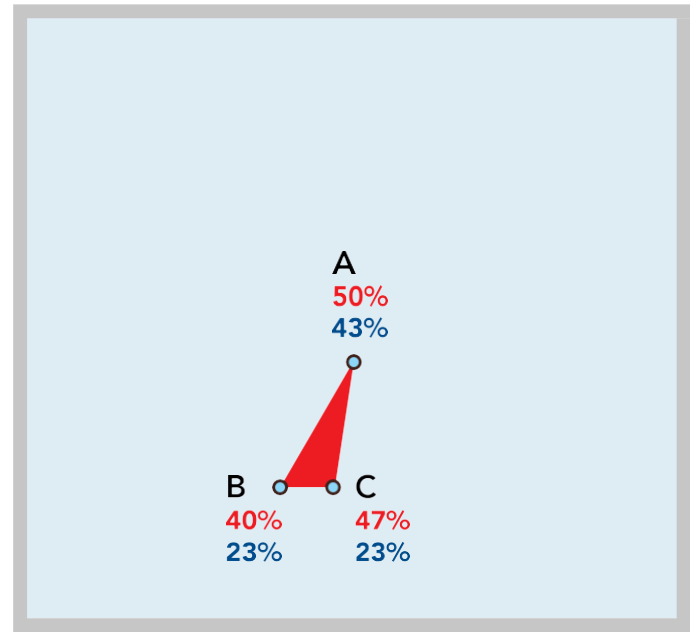
サイバーセキュリティ

分析:

経営幹部は、サイバーセキュリティが他の重要リスクよりも、組織体との関連性が高いと考えている。しかし、この影響度の高いリスクについての知識は、取締役会と経営幹部の双方とも特に低いままである。このような知識レベルの低さは、サイバー脅威の内容が絶え間なく進化していることから生じている可能性が高い。全関係者とも、特にリスクの関連性と比較した場合、組織体の能力が非常に低いという認識で一致している。

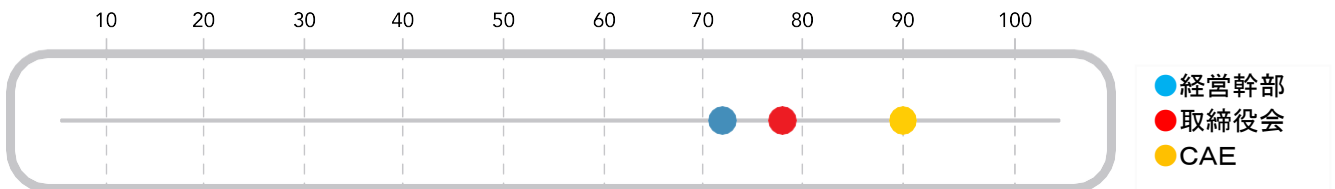
知識

A: CAE B: 取締役会 C: 経営幹部



能力

組織体との関連性



取るべき措置:

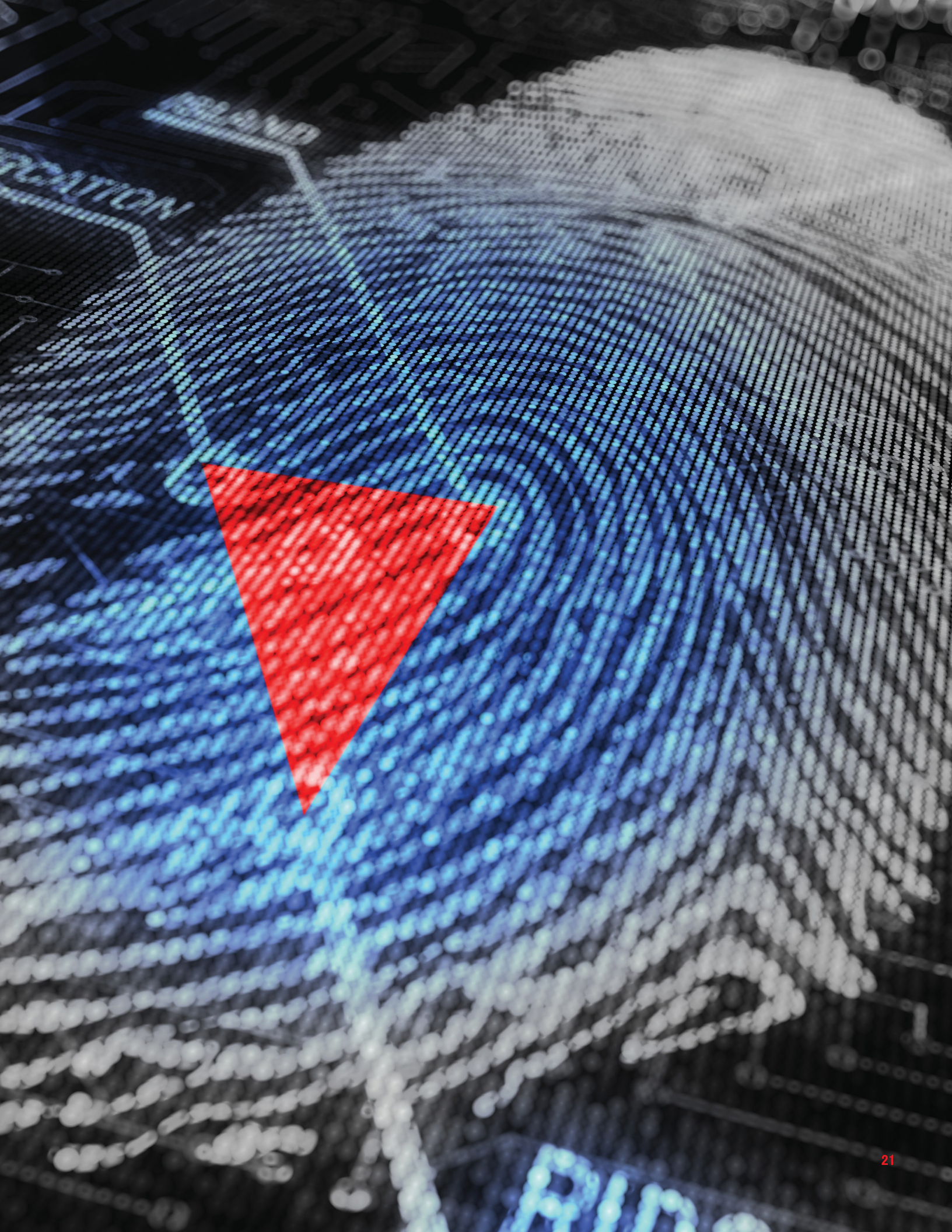
経営幹部: 新たなサイバー脅威を常に評価し、現状を完全に把握し、透明性が高く徹底した最新情報を取締役会に提供するために、組織体内外の必要なリソースを割り当てる。

取締役会: 取締役会議の議題の中で、経営幹部、内部監査、そして場合によっては外部の対象分野の専門家のために適切な時間を割り当てて、新たなサイバー脅威、組織体の取り組み、および既存の脆弱性について現実的な視点から取締役を啓発するようにする。

CAE: 新たなサイバーリスクについて経営幹部と取締役会を啓発する機会を見出し、また、サイバーセキュリティに関連するすべてのリスク・マネジメント機能を定期的に評価する。

リスク段階



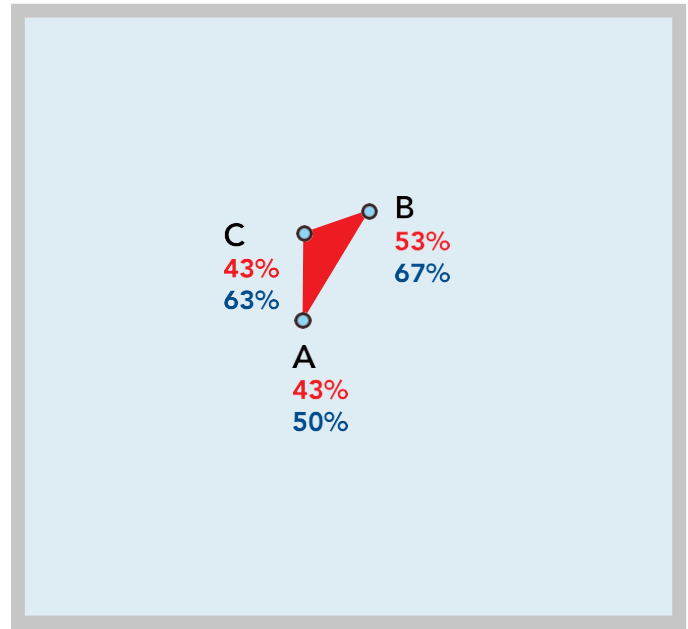


リスク

第三者

A: CAE B: 取締役会 C: 経営幹部

知識

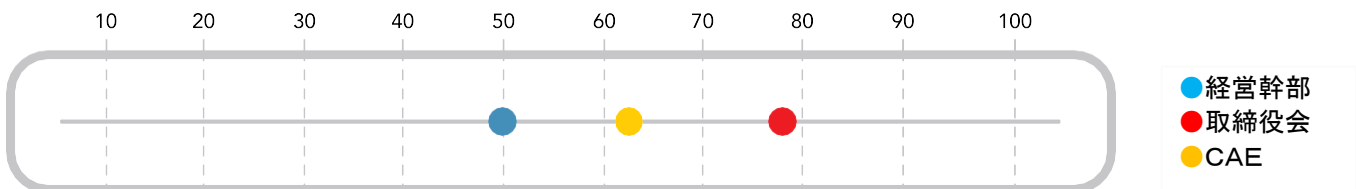


能力

分析:

CAEと経営幹部は、第三者のリスクを管理する組織体の能力について認識が一致している。しかし、取締役はより自信を持っている。驚くべきことに、組織体と第三者のリスクとの関連性が高いと考えている割合は、取締役やCAEよりも経営幹部回答者の方が少ない。

組織体との関連性



取るべき措置:

経営幹部: 経営幹部は、第三者との取り決めの包括的なリストを維持し、第三者との関係を確保しモニターするためのリスク・ベースのアプローチを開発し、それに従うようにすべきである。

取締役会: 内部監査計画を評価して、適切なリソースが第三者リスクに配分されるようにすべきである。経営幹部が定期的に重要な第三者との関係の状況を伝えるよう期待を示す。

CAE: 第三者との関係を築いてモニタリングするための管理プロセスを定期的に評価する。組織体にとって業務上または戦略上重要な第三者との関係をレビューするための監査業務を含めることを検討する。

リスク段階

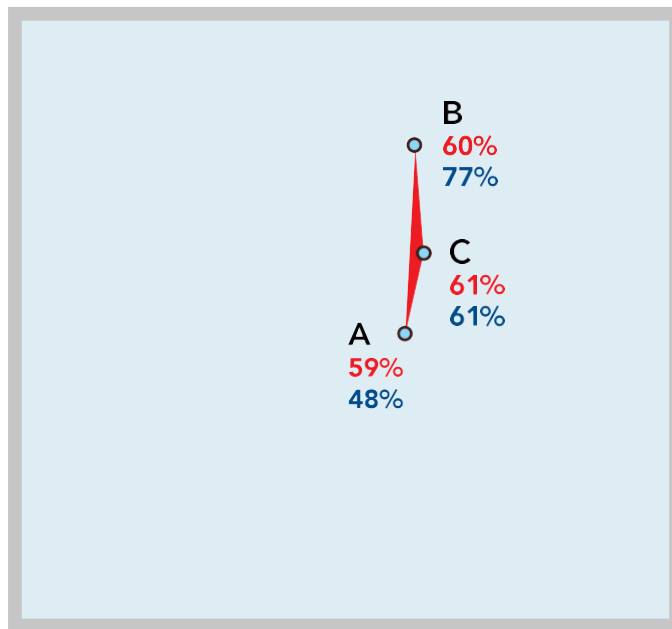


「検討」のままであった

取締役会への情報提供

A: CAE B: 取締役会 C: 経営幹部

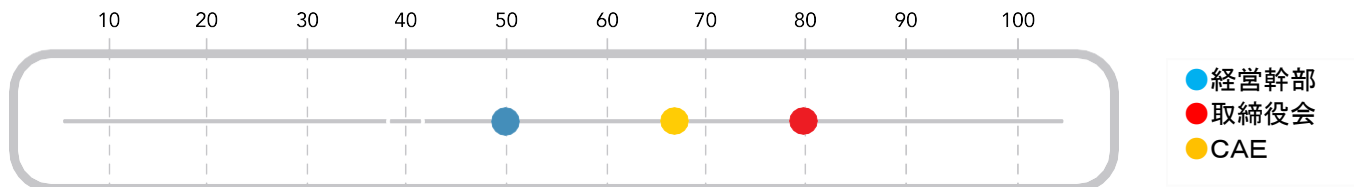
知識



分析:

全関係者は、取締役会に提供する情報の質に関連するリスクを管理する組織体の能力について、一致した認識を示している。当然のことながら取締役は、このリスクカテゴリーについての知識が豊富であると自らを評価している。

組織体との関連性



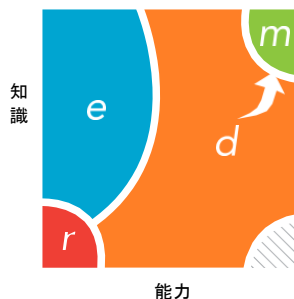
取るべき措置:

経営幹部: コミュニケーションを強化して、特に重要なリスクに関して、透明性があり、完全で、適時な情報を取締役会に確実に提供する。

取締役会: 提供される情報のレベルについて、経営幹部とCAEに期待を示す。情報量が過剰なためにメッセージが明確に伝わらない場合は、進んでそう知らせる。提供される情報の質に関する独立したアシュアランスを求める。

CAE: 取締役会に提供された情報を評価して、矛盾や脱落を指摘する。提供されている情報の質について取締役に問い合わせ、客観的な評価に積極的に貢献する。

リスク段階



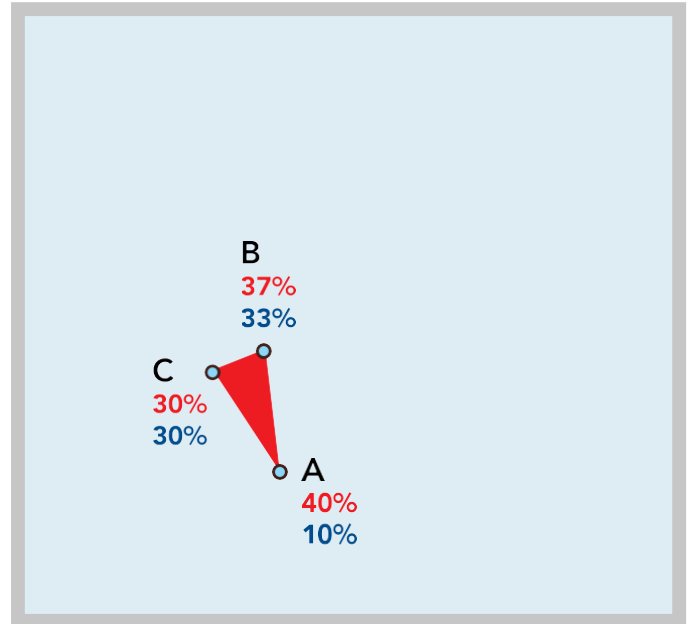
「展開」から「維持」へ進展した

リスク

サステナビリティ

A: CAE B: 取締役会 C: 経営幹部

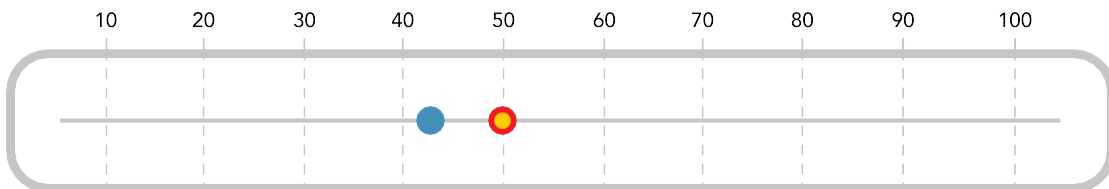
知識



分析:

全関係者は、サステナビリティを総合的に構成する環境、社会、およびガバナンスのリスクを管理する組織体の能力に関して、ある程度一致した認識を示している。しかし、自信はかなり低い。CAEは、組織体との関連性がますます高まっているこのリスクカテゴリーに関する個人の知識を、非常に低いと評価している。

組織体との関連性



能力

● 経営幹部
● 取締役会
● CAE

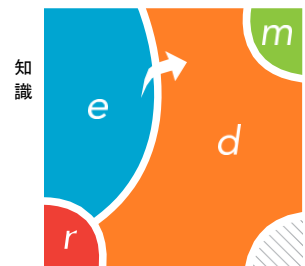
取るべき措置:

経営幹部: 顧客、従業員、投資家などの組織体のステークホルダーにとってサステナビリティの重要性が増していることを認識する。戦略的機会としてサステナビリティのリーダーシップを活用することにより、長期的な株主価値を高める機会を特定する。

取締役会: サステナビリティを戦略計画に組み込むよう、経営幹部にプレッシャーをかける。自主的な、または義務付けられているサステナビリティ報告に関連するアシュアランスを提供するように、内部監査人へ期待を示す。

CAE: サステナビリティに関連する新たなリスクや、サステナビリティが組織体の業務上および戦略上の優先事項にどのように当てはまるかについて、内部監査チームを教育する。

リスク段階





41

リスク

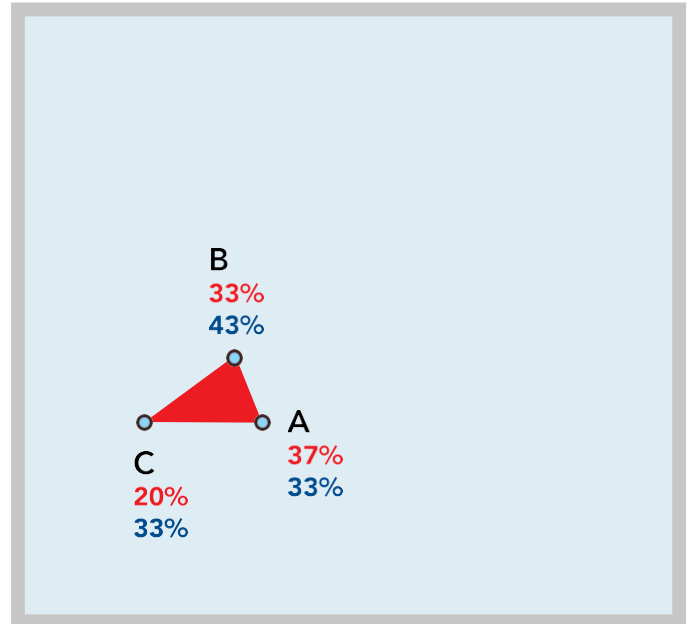
破壊的イノベーション

分析:

リスク・マネジメントの役割を担う全員は、破壊的イノベーションが組織体との関連性の最も高いリスクの1つであると**考えている**。これはおそらく、世界的なパンデミックによって悪化した世界経済の変化によるものである。しかし、個人の知識と組織体の能力に関しては、かなり認識の相違がある。取締役会とCAEは、組織体が破壊的イノベーションに対して適切に先を見越して対応したり反応したりする能力について、経営幹部よりも自信を持っている。また取締役は、破壊的イノベーションに関連するリスクについて、経営幹部やCAEよりもかなり知識があると自認している。

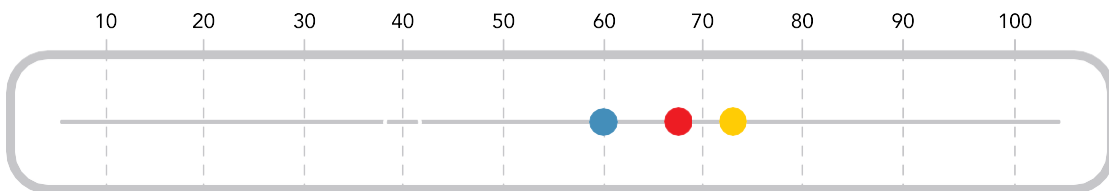
知識

A: CAE B: 取締役会 C: 経営幹部



能力

組織体との関連性



● 経営幹部
● 取締役会
● CAE

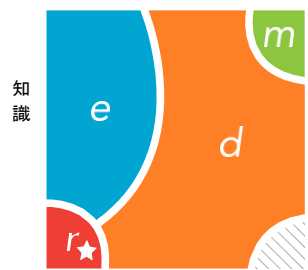
取るべき措置:

経営幹部: 取締役の知見を活用してイノベーションの方法を見つけ、また、今まで通りのやり方を破壊するような競合他社の試みを特定する。

取締役会: 外部の多様な経験を通じて蓄積されたガイダンスや知恵を組織体と共有する。経営幹部に対して、競争上の優位性のためにイノベーションを活用し、混乱に適時に反応する準備をするような、先を見越した戦略を用意するよう期待を示す。

CAE: 破壊的イノベーションを活用するための戦略上のリスクと機会を十分に理解し、破壊的イノベーションのための組織体の戦略を妨げ得る潜在的なリスクを特定する。

リスク段階



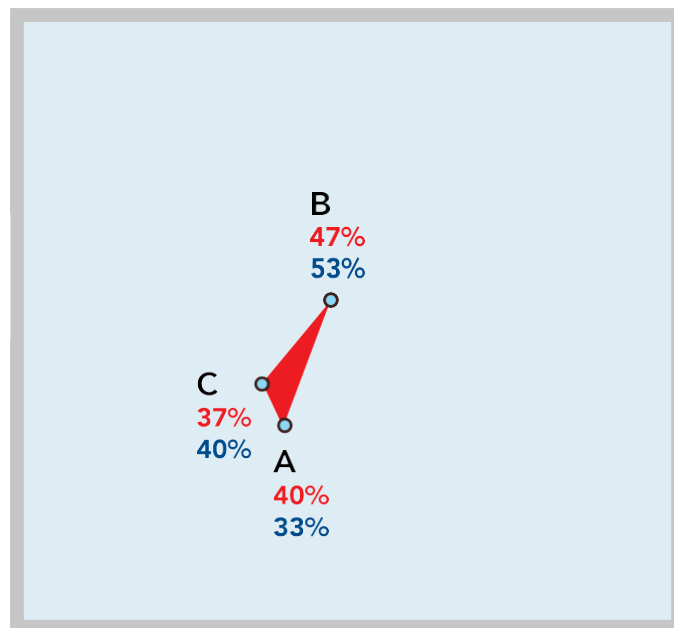
OnRiskに初登場

リスク

経済・政治情勢の変動

A: CAE B: 取締役会 C: 経営幹部

知識

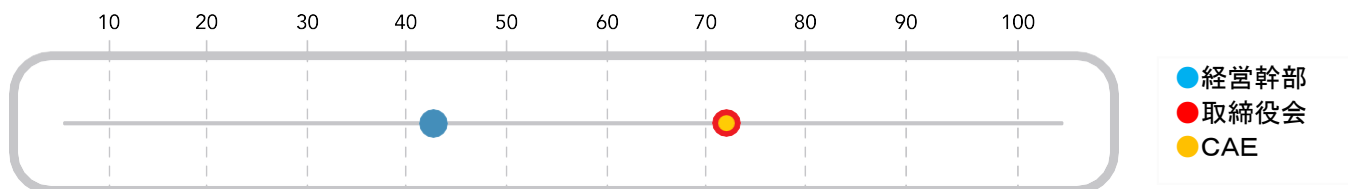


分析:

全関係者は、経済・政治情勢の変動を管理する組織体の能力について認識が一致しているが、外部の変動を管理するための個人の知識レベルについては認識にばらつきがある。さらに、取締役とCAEは、このリスクが組織体にとってどの程度関連性があるかについて認識が一致しているが、これを極めて関連性の高いリスクと見なす経営幹部は、はるかに少ない。

能力

組織体との関連性



取るべき措置:

経営幹部: 潜在的な結果に対処するための緊急時対応策とシナリオ計画を作成する。政治的変化や経済的変動の潜在的なプラス面とマイナス面について取締役会とコミュニケーションを取る。

取締役会: 潜在的な経済的および政治的影響に関する議論に経営幹部と内部監査人を関与させ、組織体が柔軟に対応する準備ができているかどうかを尋ねる。

CAE: このリスクを管理するための組織体の能力を適切に評価するために、内部監査人は、経済的および政治的不確実性が組織体の目標を達成する可能性にどう影響するかについて、よりよく学ばなければならない。

リスク段階

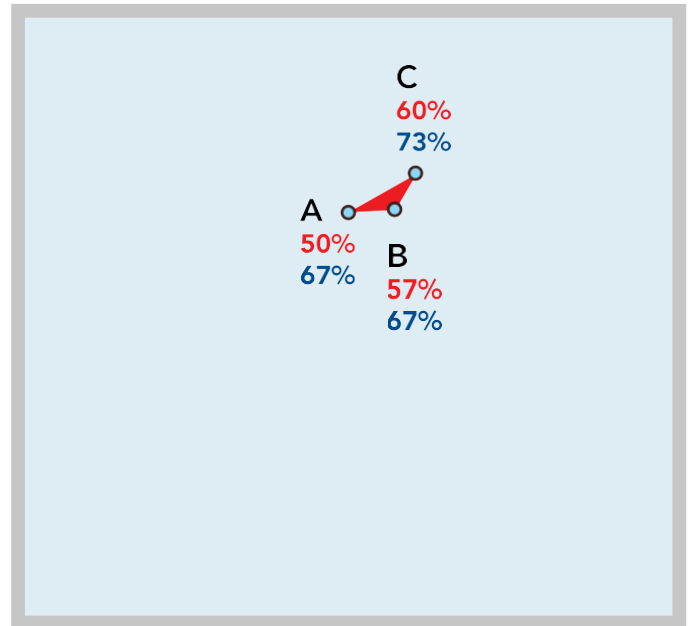


リスク

組織体のガバナンス

A: CAE B: 取締役会 C: 経営幹部

知識

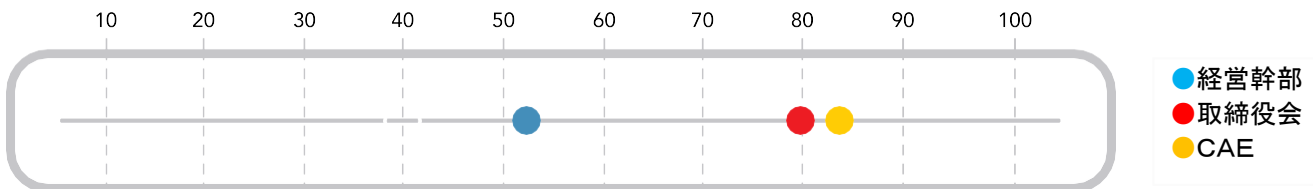


能力

分析:

この成熟したリスクについては、全ステークホルダー間で、個人の知識と組織体の能力について非常に強い認識の一致が見られる。しかし、このリスクの組織体との関連性について、取締役とCAEの認識はよく合っているが、目標を達成する組織体の能力との関連性が高いと考える経営幹部は、より少ない。

組織体との関連性



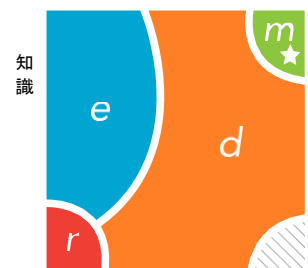
取るべき措置:

経営幹部: 組織体のガバナンスの組織体との関連性について取締役会との調整を図り、リスク・マネジメントおよび3つの重要なガバナンスの役割すべてについて、健全な対話を継続する。

取締役会: 組織体の目標を達成するための優先事項として、経営幹部が組織体のガバナンスを理解して合意するようにする。

CAE: 取締役との一貫したコミュニケーションを維持し、彼らのニーズが満たされるようにする。

リスク段階



能力
OnRiskに初登場

リスク

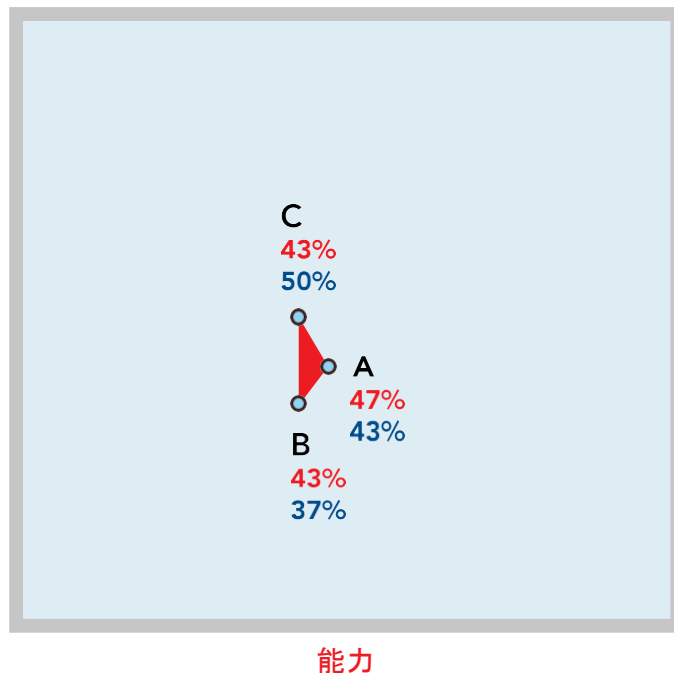
データ・ガバナンス

分析:

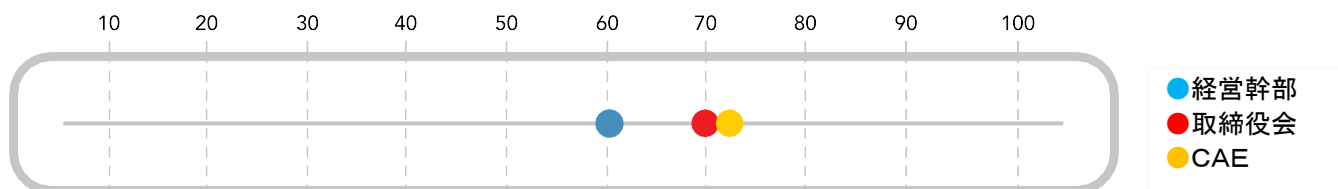
組織体の能力に関しては、全ステークホルダー間で非常に強く認識が一致しているが、組織体の目標達成に対するこのリスクの関連性に関しては、ある程度認識が一致している。ただし、取締役はデータ・ガバナンスに関する個人の知識を、経営幹部やCAEよりも大幅に低く見ているが、これはおそらく、データ・ガバナンスがデータの技術面に関連していると認識しているためである。

知識

A: CAE B: 取締役会 C: 経営幹部



組織体との関連性



取るべき措置:

経営幹部: 戦略目標の達成に向けて前進するだけでなく法規制の遵守も確実にする、データ・ガバナンスにおける先進的な実務を推進する。

取締役会: データ・ガバナンスの重要な側面に関する教育を期待して、組織体がデータを戦略的に管理する方法に関して経営幹部と内部監査に説明を求める。

CAE: データ・ガバナンスの重要な側面について取締役に研修を行い、経営管理者の実務が最先端のものであるというアシュアランスを提供する。

リスク段階

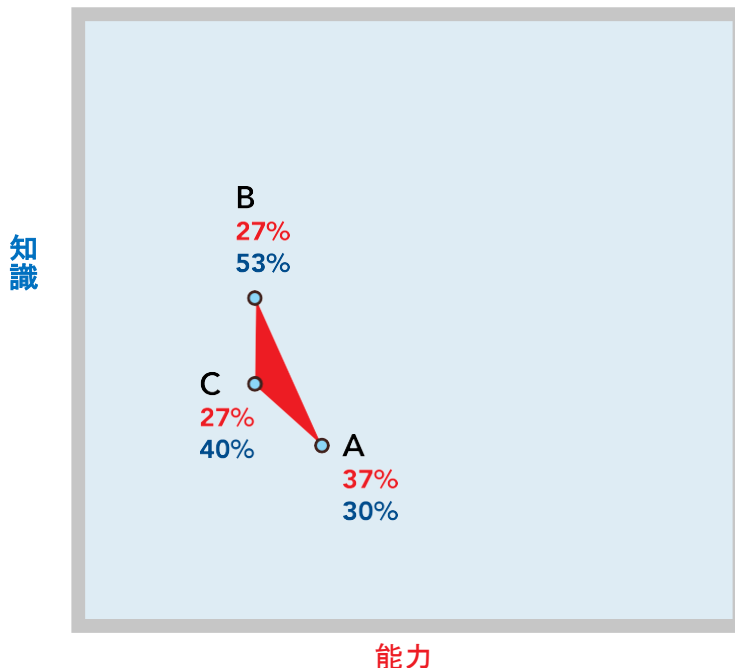




リスク

人材管理

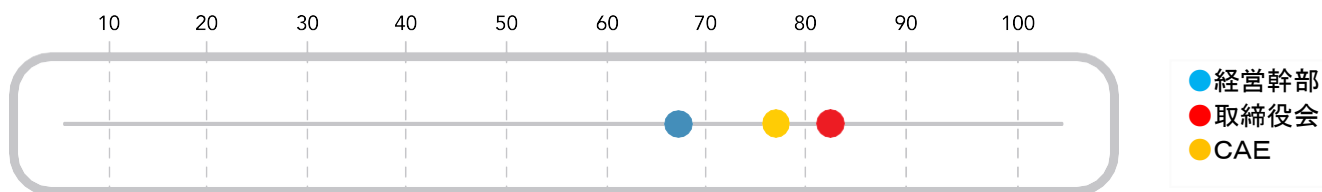
A: CAE B: 取締役会 C: 経営幹部



分析:

経営幹部と取締役会は、人材管理に関連するリスクに対処する組織体の能力について認識が一致している。ただし、取締役はこのリスクについての知識が豊富であると自認しており、経営幹部よりもこのリスクの組織体との関連性が高いと考えている。

組織体との関連性



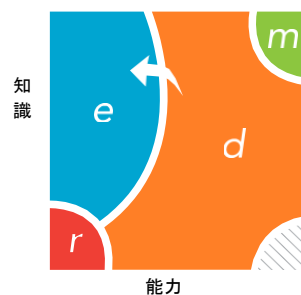
取るべき措置:

経営幹部: 最も需要の高まりつつある能力に焦点を当てて、効果的な後継者育成計画、スキルアップ戦略、および採用を通じて、組織体がそれらの能力を満たす人材を確保して定着させるための戦略を策定する。

取締役会: 経営幹部が組織体の全階層の人材管理に取り組み続け、人材関連のプロセスと施策に関する一貫した説明をすることを期待する。

CAE: 人材管理プロセスに関してステークホルダーへアシュアランスを提供することに焦点を当てた監査業務を検討し、人材に焦点を当てた重要分野の展望について、取締役会とのオープンなコミュニケーションを維持する。

リスク段階



リスク

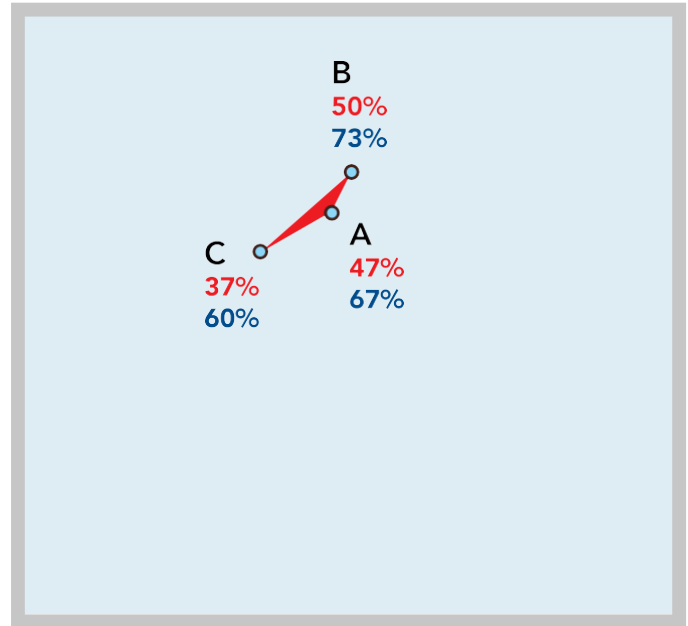
文化

分析:

リスク・マネジメントの重要なプレーヤーの大部分は、文化が組織体の成功に非常に関連していると考えており、文化に関する個人の知識に比較的自信を持っている。しかし、この重要リスクを管理する組織体の能力が高いと感じる人数については、大きなギャップがある。組織体の職場環境からもともと離れている取締役は、経営幹部やCAEよりも全体的に高い自信を持っている。

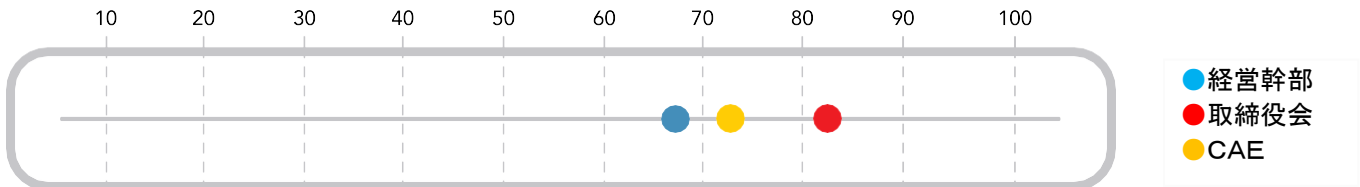
知識

A: CAE B: 取締役会 C: 経営幹部



能力

組織体との関連性



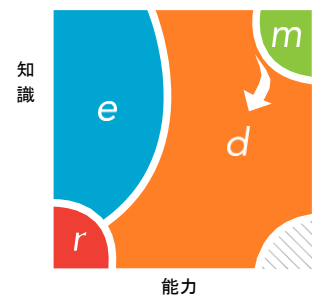
取るべき措置:

経営幹部: 効果的な文化を促進するように行動する。文化を評価し、その認識を取締役に適時に伝えるための一貫したプロセスを確立する。

取締役会: 組織体の文化の評価を、内部監査機能と経営幹部とともに確認する。経営幹部の目標とインセンティブが効果的な組織文化の促進と整合するようにする。

CAE: 組織体の文化を客観的に評価する監査業務の実施を検討する。経営幹部の行動が、組織体の文化に関連する先進的な実務に沿っているというアシュアランスを提供する。

リスク段階



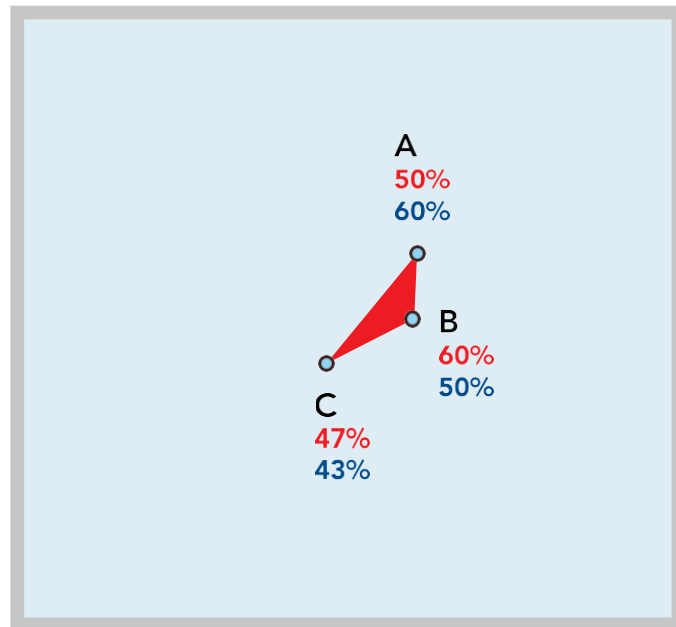
「維持」から「展開」へ後退した

リスク

事業継続性と危機管理

A: CAE B: 取締役会 C: 経営幹部

知識

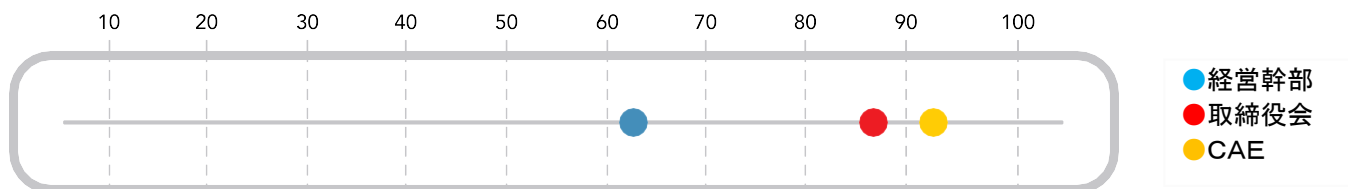


能力

分析:

2020年の出来事を考えれば当然のことながら、ほぼすべての取締役とCAEは、このリスクが組織体に非常に関連していると考えている。皮肉なことに、経営幹部回答者のうち、このリスクを非常に関連していると考えている割合は低く、また、この重要リスクを管理する組織体の能力に自信を持っている割合は著しく低い。

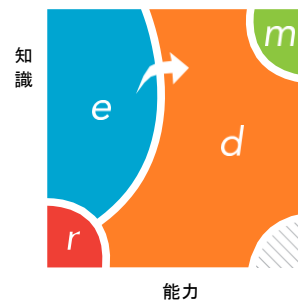
組織体との関連性



取るべき措置:

すべて: 世界的パンデミックの経験を活用して、組織体の強みと改善の機会を特定し、必要に応じて協力して改善策を実施する。

リスク段階



付録



調査方法

定性・定量調査

On Risk 2021のレポートは、優れたガバナンスを支え組織体の成功を達成するためにリスクとリスク・マネジメントに関するステークホルダーの認識をまとめる、というIIAの画期的なアプローチを踏襲している。定量調査と定性調査を組み合わせることで、2021年に組織体が直面するトップリスクをしっかりと把握している。これにより、リスク・マネジメント・リーダーからの回答に基づいた、客観的なデータ分析と主観的な洞察の両方が可能になる。

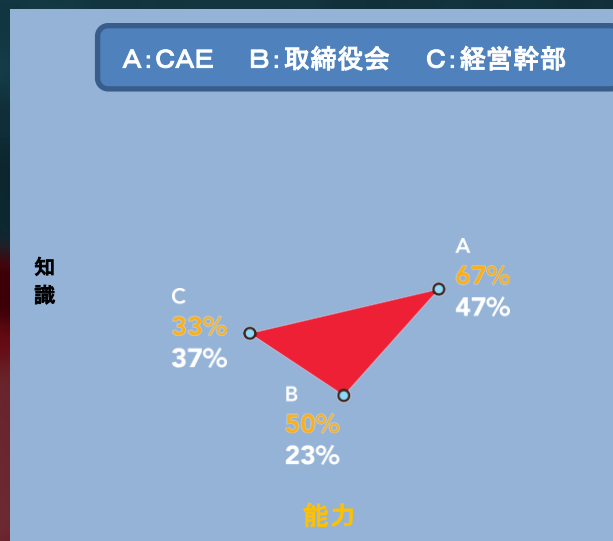
11の重要リスクのそれぞれについて組織体との関連性評価を加えたことで、リスクがどのように活用され管理されるかについての追加の比較情報もたらされている。定性調査と定量調査は、北米を拠点とする組織体に対象が限られていたが、その多くはグローバルな拠点を有している。

定量調査は、CAEを中心とする348人の北米内部監査リーダーから見たトップリスクを対象としている。包括的な調査では、内部監査がアシュアランスを提供する分野や焦点を当てる取り組みを含め、リスク・マネジメントに対する組織的なアプローチについても取り上げた。

定性調査は、北米の取締役会、経営幹部、および内部監査部門の専門職を対象とした、合計90人への詳細なインタビューに基づいている。回答者は90の異なる組織体から選ばれた。インタビューの一環として、回答者は11の重要リスクを3つの尺度で評価するよう求められた。それらは、各リスクに対する個人の知識についての認識、各リスクに対処する組織体の能力についての認識、および各リスクと組織体との関連性についての認識である。評価は7段階のリッカート尺度に基づいており、「まったく知識がない」、「極めて能力がない」、「まったく関連性がない」が最低評価の1で、「極めて知識がある」、「極めて能力がある」、「極めて関連性がある」が最高評価の7である。

次に、知識と能力の評価を組み合わせた回答を用いて、各リスクに対する各回答者グループの位置を表示した。X軸は認識された組織体の能力を示し、Y軸はリスクについての個人の知識を示している(図表11)。表示する位置は、7段階評価で6または7と回答した回答者の割合で決まり、対象としているリスクに関する個人の知識や組織体の能力についての高い確信度を表している。各表示位置をつなげて作成した三角形は、各リスクに対する3つの回答者グループ間の認識の相違を視覚的に示している。

今年新たに加えたのは、各回答者グループによる組織体との関連性評価であり、リスクごとに1つの横軸で示している。



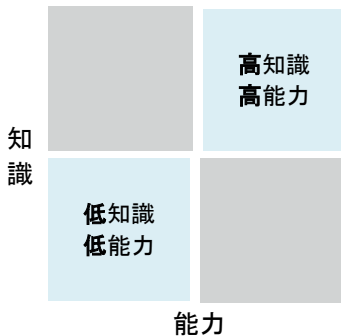
図表11: 個人の知識と組織体の能力の図

本レポートの利用方法

図表の説明

90人の専門職への詳細なインタビューに基づいて、3つの回答者グループそれぞれの知識と能力を測定し、リスクごとに位置を表示した。シンブルな象限マッピングは、回答者グループの認識を反映するための効果的で一貫性のあるツールである(図表12)。

図の4つの象限は、2つの尺度のそれぞれの大きさに対応している。例えば、知識と能力の平均が高い回答は、右上の象限に表示される。逆に、知識と能力の低い回答は、左下の象限に表示される。前節で述べたように、平均は、知識や能力の特性について上位2つの評価をした回答者の割合に基づいて決まる。



図表12:
象限図

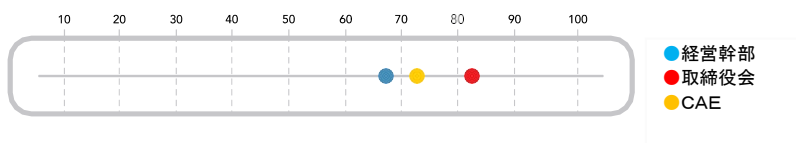
表示位置

3つの回答者グループのそれぞれの位置は、各リスクに関する相対的な知識と能力を明らかにするためだけでなく、グループ間に認識の相違がある可能性を示すために、象限図に表示される。こうしてできた三角形(本レポートでは単に認識三角形と呼ぶ)は、リスクがどの程度よく理解され、総合的に管理されているかを示す強力な指標となる。各三角形の大きさ、形状、および位置は、認識の相違の原因を知る手掛かりにもなる(関連する補足説明を参照)。

新たな関連性図

各回答者グループによる組織体との関連性に関する評価は、単一の軸に示されており、取締役、経営幹部、およびCAEの関連性評価のばらつきを明確に描くことができる(図表13)。

図表13: 関連性図



認識三角形: 何を意味するのか。

各リスクに対する各回答者グループの認識を示して作成した認識三角形は、リスクが現在どのように管理されているかを知る手掛かりになる。各三角形の形状もまた、価値ある情報が示せる。

低くて狭い

この基本的な形の三角形は、各グループのリスクの知識の程度はかなり一致しているが、リスクに対処する組織体の能力については、1つの回答者グループに重大な認識の相違があることを示唆している。

高くて狭い

反対に、この基本的な形の三角形は、リスクの知識に関して回答者グループ間でかなり幅があるが、組織体の能力に関する認識には強い認識の一致があることを示唆している。

低くて広い

この基本的な形は、複数の回答者グループの認識の相違を示唆しており、リスクに対処する組織体の能力に関して最も重大な認識の相違がある。

高くて広い

この基本的な形は、複数の回答者グループの認識の相違を示唆しており、知識と能力の両方について重大な認識の相違がある。

小さくて対称

この形は、知識と能力に関して3つの回答者グループすべての認識がかなり一致していることを示唆している。三角形の位置にもよるが、これは、十分に理解され管理されているリスク(右上の象限)や、十分に理解されておらず管理されていないリスク(左下の象限)を表している可能性がある。

調査方法の活用

OnRisk 2021の読者は、本レポートで取り上げた11の重要リスクのそれぞれについてデータを確認し分析すべきであり、また、組織体の取締役会、経営幹部、および内部監査部門の間で同様の分析をすることを推奨する。

定性インタビュー参加者からの意見は、OnRisk 2021全体に散在しており、各リスクについての意見だけでなく、リスクの捉え方も垣間見ることができる。これらの意見はいくつかの洞察をもたらしているが、目標を設定して達成するための組織体の取り組みに対するリスク、組織体のリスク管理能力、および個々のリスクと組織体との関連性を、リスク・マネジメント・プロセスの各プレーヤーがどのように理解しているかについて、すべての組織体が同様の議論をすることが極めて重要である。

このような分析における重要なステップは、リスク・マネジメントの責任者が自分の役割をどのように理解して実行するかについて、明敏な調査を行うことである。IIAが最近発表した3ラインモデルは、ガバナンスの本質とその本質を支える役割を理解するための追加的な指針を示している。

- アカウンタビリティ — 組織体を監督するために、統治機関(取締役会)がステークホルダーに対して果たす。
- (リスクの管理を含む)活動 — 組織体の目標を達成するために、経営管理者が行う。
- アシュアランスと助言 — 継続的改善のために洞察、信頼、および奨励を、独立した内部監査機能が提供する。

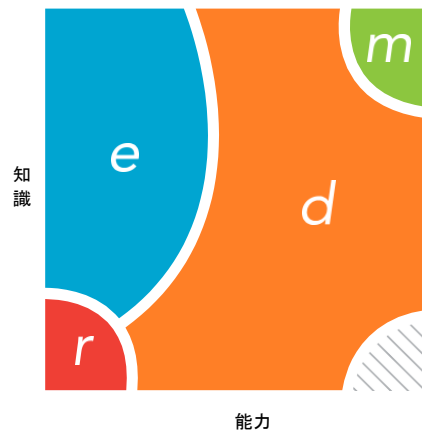
本レポートの前半で述べたように、新型コロナウイルス感染症のパンデミックは、組織体がコミュニケーションを改善し、継続的にリスクを評価し、重要リスクについて綿密に連携するようにと、駆り立てた。この新たな協力とコミュニケーションは、役割に対する深い理解と組み合わせられると、リスク・マネジメントとガバナンスを成功させるための理想的な条件を生み出す。

リスク段階

本レポートで説明しているリスクは、組織体への潜在的な影響と、それらに対処するために組織体が講じているはずの措置について、4段階(認識、検討、展開、および維持)のいずれかに分類されている。リスク段階モデル(図表14)は、リスク評価の2つの尺度である知識と能力において、リスク・マネジメントがどう進展しているかを示している。

さらに、各リスクの組織体との関連性は、各組織体に独特のものとして理解すべきである。各リスクの組織体との関連性評価は、組織体の規模、業種、種類はもちろん、競争、成熟度、サプライチェーン、流動性などの様々な要因によって異なる。前述のように、本レポートの分析には含まれていないが、特定の状況によっては一部の組織体に特に関連するリスクが存在する可能性がある。この独特な側面があるため、組織体との関連性はリスク段階モデルには示していない。

図表14:
リスク段階モデル



リスク段階は、認識(r)、検討(e)、展開(d)、維持(m)である。

リスク段階の説明

認識

リスクは、新たに発生していると認識されているが、ステークホルダー間のリスクに関する知識は低い。

基本的なリスクについての理解が低いため、リスク対応戦略は、実施されていない、または効果的に設計されているとは考えられていない。

モニタリング・プロセスは、検討されていない。

固有リスクのレベルは、十分に理解されていない。

知識-低

能力-低

r

検討

リスクに関する知識は、全員ではないが、一部のステークホルダー間で高まっている。

リスクは、新たに発生しているもの、または動的なものとして認識されている可能性がある。

リスク対応戦略は、検討されているが、完全には実施されていない。

モニタリング・プロセスは、検討されていないか、実施されていない。

固有リスクのレベルは、一般的に理解されている。

知識-中から高

能力-低

e

展開

少なくとも経営幹部のリスクの知識は高い。

リスク対応戦略は、策定されているか、実施されている可能性がある。

モニタリング・プロセスは検討中かもしれないが、完全に実施されたとは限らない。

残余リスクは、一般的に理解されている。

知識-低から高

能力-中から高

d

維持

リスクは、関連するすべてのステークホルダーに十分に理解されており、大きく変化しているとは認識されていない。

リスク対応戦略は、策定され実施されており、組織体とリスクとの関連性についての認識が一致している。

モニタリング・プロセスが活用されており、リスク対応戦略が設計通りに効果的に運用されるようにしている。

残余リスクのレベルは、組織体にとって許容できるレベルにあると理解され信じられている。

知識-高

能力-高

m

図表について

図表1—OnRisk 2021リスク評価—全回答者

出典: OnRisk 2021定性調査。質問: 次の各リスクについてどの程度の知識がありますか。次の各リスクへの対応について、組織体はどの程度の能力を持っていますか。次の各リスクは、組織体にとってどの程度関連していますか。スコアは7が最高であり、スコア6と7を合わせた割合をグラフに表示した。有効回答数は90。

図表2—改善分野: 経営幹部

出典: OnRisk 2021定性調査。質問: 次の各リスクへの対応について、組織体はどの程度の能力を持っていますか。次の各リスクは、組織体にとってどの程度関連していますか。スコアは7が最高であり、スコア6と7を合わせた割合をグラフに表示した。有効回答数は30。

図表3—学習機会: 経営幹部

出典: OnRisk 2021定性調査。質問: 次の各リスクについてどの程度の知識がありますか。次の各リスクは、組織体にとってどの程度関連していますか。スコアは7が最高であり、スコア6と7を合わせた割合をグラフに表示した。有効回答数は30。

図表4—回答者グループ別平均評価

出典: OnRisk 2021定性調査。質問: 次の各リスクについてどの程度の知識がありますか。次の各リスクへの対応について、組織体はどの程度の能力を持っていますか。次の各リスクは、組織体にとってどの程度関連していますか。スコアは7が最高であり、スコア6と7を合わせた割合をグラフに表示した。有効回答数は90。

図表5—組織体との関連性

出典: OnRisk 2021定性調査。質問: 次の各リスクは、組織体にとってどの程度関連していますか。スコアは7が最高であり、スコア6と7を合わせた割合をグラフに表示した。有効回答数は90。

図表6—組織体の能力

出典: OnRisk 2021定性調査。質問: 次の各リスクへの対応について、組織体はどの程度の能力を持っていますか。スコアは7が最高であり、スコア6と7を合わせた割合をグラフに表示した。有効回答数は60。

図表7—組織体のガバナンス

出典: OnRisk 2021定性調査。質問: 次の各リスクについてどの程度の知識がありますか。次の各リスクへの対応について、組織体はどの程度の能力を持っていますか。次の各リスクは、組織体にとってどの程度関連していますか。スコアは7が最高であり、スコア6と7を合わせた割合をグラフに表示した。有効回答数は60。

図表8—IIAの3ラインモデル

出典: 内部監査人協会

図表9—アシュアランスに関する洞察

出典: OnRisk 2021定量調査。質問7: 2020年や2021年に、次のどのリスクについてアシュアランスを提供した、または提供を予定していますか。有効回答数は348。OnRisk 2021定性調査、経営幹部回答者。質問: 次の各リスクは、組織体にとってどの程度関連していますか。スコアは7が最高であり、スコア6と7を合わせた割合をグラフに表示した。有効回答数は30。

図表10—アシュアランスのヒント

出典: OnRisk 2021定性調査。質問11: リスク・マネジメントの有効性についてのアシュアランスをどこから得ていますか。有効回答数は90。

図表11—個人の知識と組織体の能力の図

出典: 内部監査人協会

図表12—象限図

出典: 内部監査人協会

図表13—関連性図

出典: 内部監査人協会

図表14—リスク段階モデル

出典: 内部監査人協会



内部監査人協会(IIA)について

内部監査人協会(IIA)は、内部監査専門職に関する提唱者、教育者として、ならびに基準、ガイダンスおよび各種認定資格の提供者として、世界で最も広く認識されている。1941年に設立され、現在、世界170以上の国と地域に20万人以上の会員がいる。同協会の国際本部は、アメリカ合衆国フロリダ州レイク・マリーにある。詳しくは、www.globaliia.orgを参照。

免責事項

IIAは、情報提供と教育を目的として本レポートを発行する。本レポートは、個別具体的な状況に対する確答を提供することを目的とするものではなく、あくまでも指針としてご使用いただくものである。IIAは、特定の状況に直接関係する独立した専門家の助言を求めることを推奨する。IIAは、本レポートのみに依拠する者に対して一切の責任を負わない。

著作権

Copyright © 2020内部監査人協会。無断転載を禁じる。転載の許諾については、copyright@theiia.orgにお問い合わせください。

Global Headquarters

The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 149
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org



The Institute of
Internal Auditors