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

2022

目次

はじめに

*「この世の仕組みは、**いかに複雑**で予測不可能なものか。」*

— カート・ヴォネガット

新型コロナウイルス感染症のパンデミックが初めて世界を封鎖して以降の１年半で、組織体は予期せぬ事態を受け入れることを学んだ。リスク・マネジメントの主なプレーヤーである取締役、経営幹部、および内部監査部門長（ＣＡＥ）は、発生可能性は低いが影響度の高いリスクをもっと考慮する必要があるとわかった。この気付きは取締役会に衝撃を与え、リスク・マネジメントの弱点に対する認識を高め、より機敏でレジリエントな組織体を構築するよう経営幹部を鼓舞し、より幅広い価値を提供するように内部監査を位置付けた。

確かにパンデミックは、信頼される機関に対する見方、時間に対する価値と優先順位、ならびに私たちを取り巻く世界の仕事、多様性、および健康に関する長年の社会的契約へのコミットメントに変化をもたらした。これらの変化のどれが一時的か永続的かについて、決定的な答えを出すのは時期尚早である。しかし、確かなことが１つある。社会、事業、政治、および経済について核となる考え方を試す百年に一度のテストは、微妙な変化と大規模な変化の両方を生み出すだろう。

歴史的に重要ではあるが、長引くパンデミックとそれに関連する副産物だけが 2022 年のリスクに影響を与え得る要因ではない。社会的混乱の拡大、国家レベルでの規制当局の姿勢の大幅な変化、継続的な経済・政治情勢の変動、気候変動の継続的な影響、ならびに環境、社会、およびガバナンス関連の問題の著しい加速が組み合わさり、来年は予測不能かつ機会に満ちたものになるだろう。

*「**新型コロナウイルス感染症は、**組織体が予期せぬ事態に備えて計画を立てるための警鐘だった。これらの『ハリウッドタイプ』のリスクシナリオは、組織体内である程度議論する必要がある。」*
– テクノロジー企業、経営幹部

*「**今日のリスクは、**非常に不安定で無秩序になっている。ニュースで見る世界中で起きているこれらのリスクは、原因と結果の相関関係が低いようである。」*
– 小売業、取締役

OnRisk の調査方法

OnRisk のアプローチは、革新的な手法に基づいており、組織体のガバナンスの主なステークホルダーである取締役会、経営幹部、およびＣＡＥの視点を独自にまとめている。個人の知識、組織体の能力、および組織体とリスクとの関連性に関するこれらのステークホルダ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。

本調査では、様々な 90 の組織体の取締役 30 人、経営幹部 30 人、およびＣＡＥ 30 人へ定性的インタビューを行った。本調査は、組織体が直面しているリスクをしっかりと把握しており、リスク・マネジメントのリーダーからの回答に基づいて、客観的なデータ分析と主観的な洞察の両方を得ることを可能にしている。

各グループの総合評価には、各リスクの特定の側面を７段階で６または７と評価した回 答者の割合に基づいた値が割り当てられている。例えば、取締役の 10 人中７人が、データ・プライバシーに関する組織体のリスク・マネジメント能力を６または７と評価した場合、スコアは 70%になる。

OnRisk の調査方法、本レポートの利用方法、および OnRisk アプローチに関連して開発したリスク段階の詳細は、本レポートの後半に記載している。

2022 年のトップリスク

12 以下の 12 のリスクは、2022 年に組織体に影響を与え得る様々なリスクから慎重に選ばれ、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 OnRisk 2021 から変更されていないが、一部は更新され、その他は追加されている。例えば、2021 年のサステナビリティのリスクは、2022 年には環境のサステナビリティ、社会のサステナビリティ、および組織体のガバナンスに分類されている。OnRisk 2022 の全リスクは、組織体の規模、産業、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、この分析に含まれていないリスクでも、特定の状況次第では組織体にとって特別な関連性を持つ可能性がある。OnRisk 2022 の回答者が評価したとおりに、リスクは関連性の高い順に示されている。

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。

人材管理：在宅勤務を含むリモート業務の必要性と受け入れの増加、および動的な労働条件の継続により、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。

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・プライバシー：世界中の法域で増え続ける規制のリストは、データ・プライバシーをますます複雑で動的にしている。このリスクでは、組織体がどのように機密データを保護し、適用されるすべての法規制への遵守を確保するかを検討している。

カルチャー：フルタイムやパートタイムでリモート作業する専門職の従業員の割合が増加しているため、組織体はカルチャーを維持、強化、またはコントロールすることが求められている。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討している。

経済・政治情勢の変動：通常のマクロ経済循環の動きと結び付いたパンデミックの継続的な影響は、組織体が活動する市場に不安定さを生み出す可能性がある。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。

規制環境の変化：規制に対する政府の姿勢の根本的な変化は、規制が厳しくないと思われている組織体を含め、組織体に重大な影響を与える可能性がある。このリスクでは、動的で曖昧な規制環境下で組織体が直面する課題を検討している。

サプライヤーとベンダーの管理：組織体が成功するには、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、第三者との関係を選択してモニター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、破壊的イノベーションへの適応や利用の準備が組織体にできているかを検討している。

社会のサステナビリティ：雇用する人々、バリューチェーンで働く人々、製品やサービスを消費する人々、およびコミュニティに住む人々に組織体は大きな影響を与える、という認識がますます高まっている。このリスクでは、組織体の行動が人々やコミュニティに与える直接的および間接的な影響を理解して管理する組織体の能力を検討している。

サプライチェーンの混乱：世界的なパンデミックを原因とする世界規模での通常業務の混乱は、組織体の戦略目標の達成を支援するサプライチェーンのレジリエンスの必要性を浮き彫りにした。このリスクでは、組織体が現在および将来のサプライチェーンの混乱に適応する柔軟性を組み込んでいるかを検討している。

環境のサステナビリティ：組織体は、組織体が事業を行う環境に与えている影響を評価して開示するよう求める、株主、規制当局、顧客、および従業員などのステークホルダーからの圧力の高まりに直面している。このリスクでは、組織体が環境への影響を確実に測定して評価し、さらに正確に報告する能力を検討している。

重要な所見

OnRisk 2022 の定性的インタビューは、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、さらに、リスク・マネジメントの取り組みの連携が成功にどのように影響するかについて、スナップショットを示している。結果の分析により、リスクがどのように理解されているかだけでなく、リスクを管理する能力がどのように認識されているかも明らかにする６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。

- **特定のリスクについて、リスク・マネジメント・プレーヤー間で顕著な違いがある。**総じて、組織体の能力、組織体とリスクとの関連性、および個人の知識は、概ね整合している。ただし、いくつかの重要なリスク領域には注目に値する違いがある。

- **組織体とリスクとの関連性と組織体の能力の評価の間に大きなギャップが存在するリスクがある。**リスク・マネジメント・プレーヤーが評価した組織体とリスクとの関連性と組織体の能力とのギャップは、人材管理、破壊的イノベーション、データ・プライバシー、サイバーセキュリティ、およびカルチャーについて驚くほど大きい。

- **今後注意を払うべきリスク。**回答者が真っ先に思い浮かべたリスクは、サイバーセキュリティ、人材管理、カルチャー、破壊的イノベーション、および経済・政治情勢の変動の５つであった。注目すべきことに、５つのうち４つは、組織体とリスクとの関連性と組織体の能力の間に最大のギャップがあり、取り組みが必要な場所をリスクプレーヤーが理解していることを示唆している。

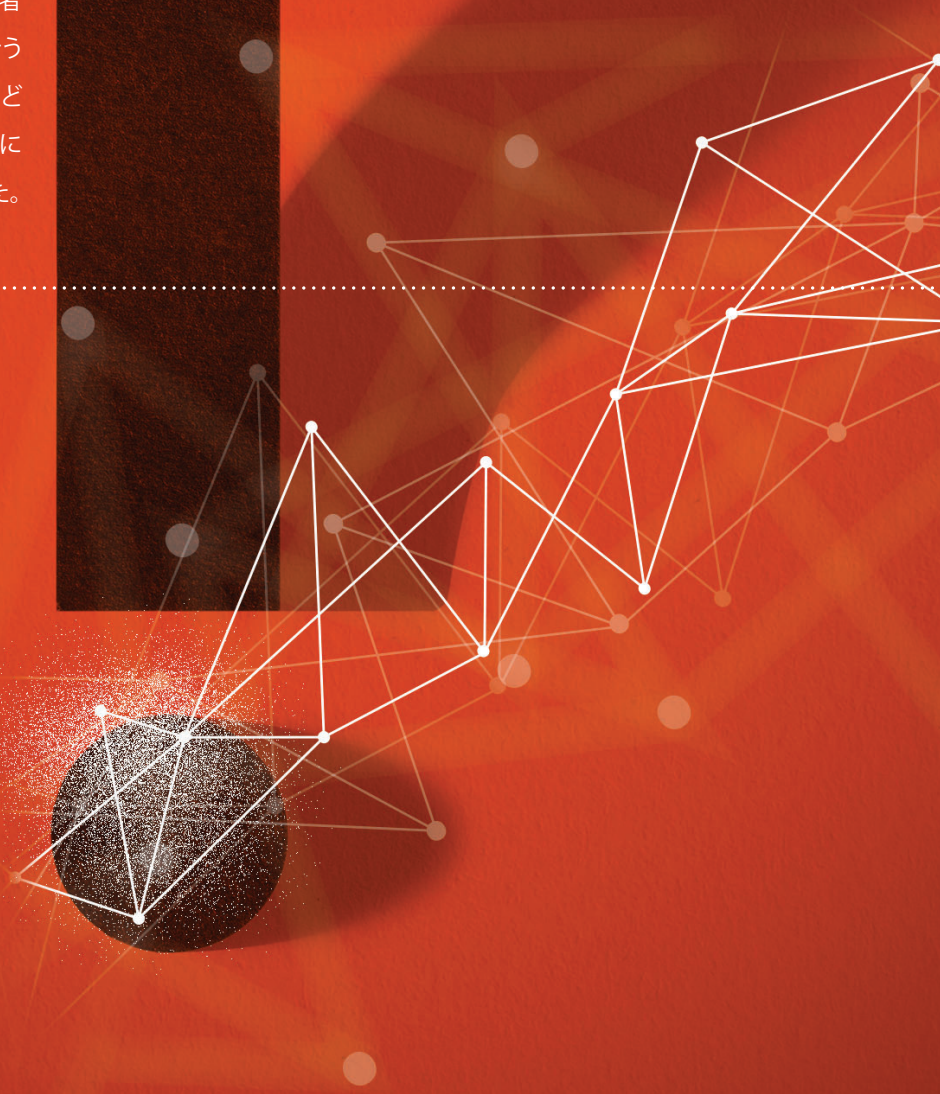
- **組織体とリスクとの関連性の認識は、ＥＳＧの構成要素によって大きく異なる。**３つのグループ間の認識の整合性はこれらのリスクに関して比較的強いが、組織体のガバナンスは、社会のサステナビリティや環境のサステナビリティよりも回答者にとってはるかに大きな関連性がある。

- **パンデミックは、組織体のリスク・マネジメントの改善機会を明らかにした。**新型コロナウイルス感染症は、リスクを予測する能力は改善しなかったかもしれないが、多くの人々がリスクに反応することへの自信を高めた。ある人々にとっては、リスクの管理方法、および分散型や縦割りの状態でのリスク・マネジメントに関連するさらなる課題についての注意喚起となった。

- **経営幹部と取締役会は、より広範な内部監査業務を望んでいる。**回答者は、現在のアシュアランス業務を適切であると感じているが、アシュアランスの報告の改善を提案している。これは、幅広いリスクに対する独立したアシュアランスの価値を実証する機会をもたらしている。

重要な所見の説明

次からは、６つの重要な所見を詳しく説明している。
前述の通り、OnRisk2022 の定性的インタビューは、主な推進者三者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視点を引き出すことを意図していた。これらの所見の分析と調査により、回答者間の交流と認識の整合性に関する重要な洞察と、そうした交流と認識の整合性がリスク・マネジメントにどのように影響するかについての有益な結論が明らかになった。



特定のリスクについて、能力と関連性に顕著な違いがある

３つの回答者グループの全体的な評価は概ね整合しているように見えるが、各グループの組織体の能力と組織体とリスクとの関連性の評価を詳細に分析すると、いくつかのリスク領域、特に破壊的イノベーションに注目に値する違いが見られる。

経営幹部は、破壊的イノベーションを除き、調査した殆どのリスク領域で組織体の能力に自信を持つ傾向があった。破壊的イノベーションでは、回答者の 10 人中２人だけが能力を高いと評価した（図１）。これにより、経営幹部と取締役会の２つの回答者グループ間で、組織体の能力の評価に 23%ポイントという最大の差が生じた。

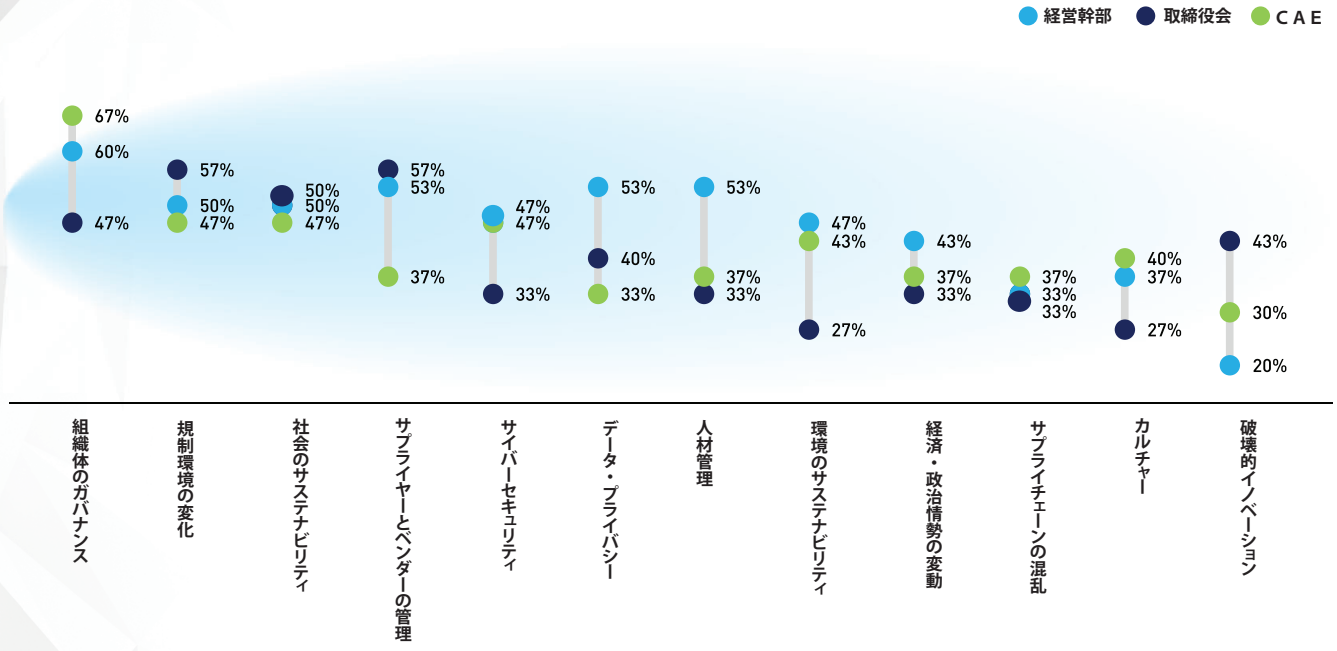
取締役会は、特定のリスクを管理する組織体の能力について、経営幹部ほどは自信がない。人材管理と環境のサステナビリティについては、取締役会の回答者の能力評価は、経営幹部の回答者と比較して 20 ポイント低かった。組織体のガバナンスでは 13 ポイント低かった。

一方、ＣＡＥは、サプライヤーとベンダーの管理のリスクに対処する組織体の能力に自信がなかった。ＣＡＥの評価は、取締役会の回答者より 20 ポイント低く、経営幹部より 16 ポイント低かった。

図１：

リスク領域ごとの役割別の組織体の能力評価

７段階で６または７と評価した割合



注：OnRisk2022 インタビューの質問：総じて、全社的リスクを扱うことに関して、あなたの組織体はどの程度能力がありますか。回答者は、７段階から評価を選択でき、１が最低（「まったく能力がない」）、７が最高（「極めて能力がある」）である。リスク領域は、平均スコアが高いものから低いものへと並べ替えられた。有効回答数＝ 90。

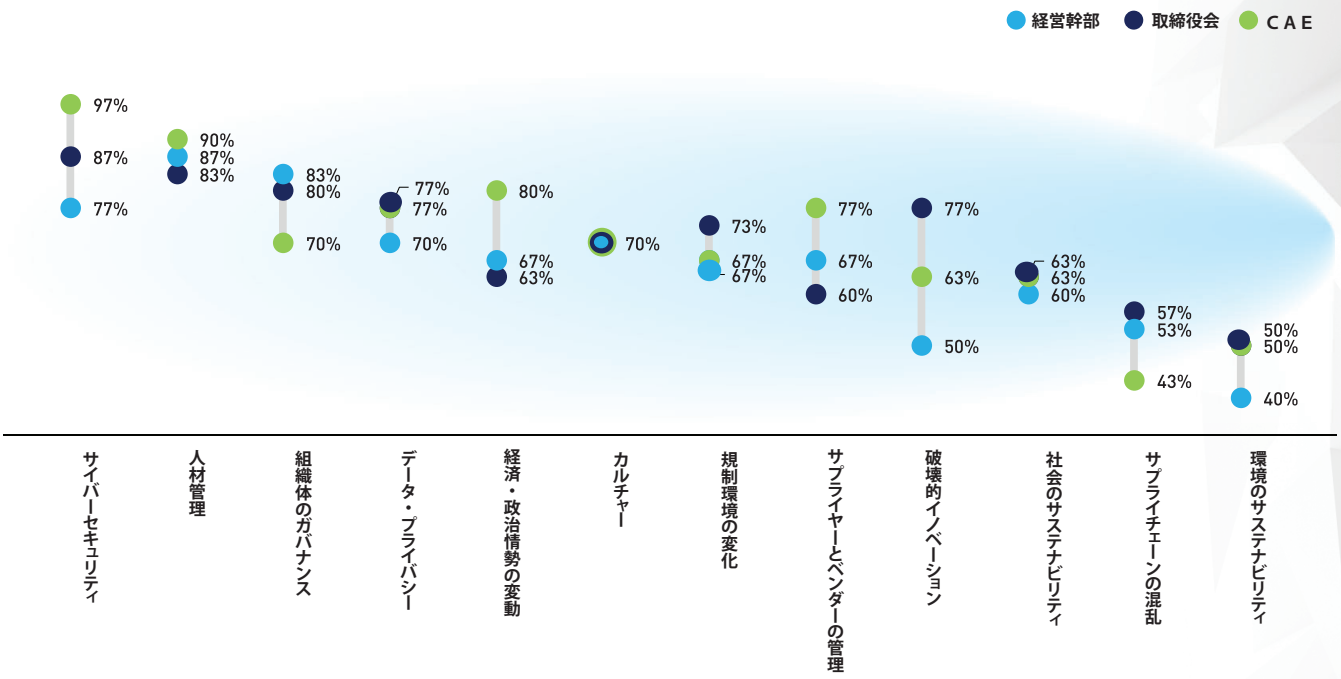
組織体とリスクとの関連性の評価にも同様の違いが見られた（図２）。取締役会（77%）は経営幹部（50%）よりも、破壊的イノベーションを関連性の高いリスクとして評価する傾向が大幅に高かった。この 27 ポイントの差は、組織体とリスクとの関連性評価において、２つの回答者グループ間で最大であった。

ほぼすべてのＣＡＥ（97%）が、サイバーセキュリティを組織体との関連性が非常に高いリスクと評価したが、取締役会の回答者は 10%ポイント低く（87%）、経営幹部は 20%ポイント低かった（77%）。ＣＡＥはまた、サプライヤーとベンダーの管理を組織体との関連性が高いと評価する傾向があり、取締役会より 17 ポイント高く、経営幹部より 10 ポイント高い。同様の 17 ポイントの差は、経済・政治情勢の変動に関するＣＡＥと取締役会の評価に見られる。

図２：

リスク領域ごとの役割別の組織体との関連性評価

７段階で６または７と評価した割合



注：OnRisk2022 インタビューの質問：次の各リスクは、現在の組織体にどの程度関連性がありますか。回答者は、７段階から評価を選択でき、１が最低（「まったく関連性がない」）、７が最高（「極めて関連性がある」）である。リスク領域は、平均スコアが高いものから低いものへと並べ替えられた。有効回答数＝ 90。

組織体とリスクとの関連性と組織体の能力の評価の間に大きなギャップが存在するリスクがある

個々の回答者グループ間でいくつかの評価のばらつきが予想されたが、３つの回答者グループの評価を組み合わせた分析により、さらなる洞察が明らかになった。分析により、いくつかの領域で、組織体とリスクとの関連性は高いが組織体の能力は低いという大きなギャップがあることが特定された。この関連性と能力のギャップは、リスク・マネジメントの著しい脆弱性を反映している可能性がある。

これらの中で最も重要なリスクはサイバーセキュリティであり、組織体の大小、公私、営利・非営利を問わず憤慨させ続けている。このユビキタスで動的なリスクは、人材管理とともに回答者が最も関連性があると評価した（図３）。だが平均して、組織体の能力は大幅に低い。人材管理、破壊的イノベーション、カルチャー、データ・プライバシー、および経済・政治情勢の変動についても大きな差が見られる。

「今年、パイプラインへのハッキングを目の当たりにしたように、これらのサイバーセキュリティ攻撃は大きなトリクルダウン効果をもたらす可能性がある。すべての業界が、ある程度サイバーセキュリティ・リスクの影響を受けやすくなっている。」

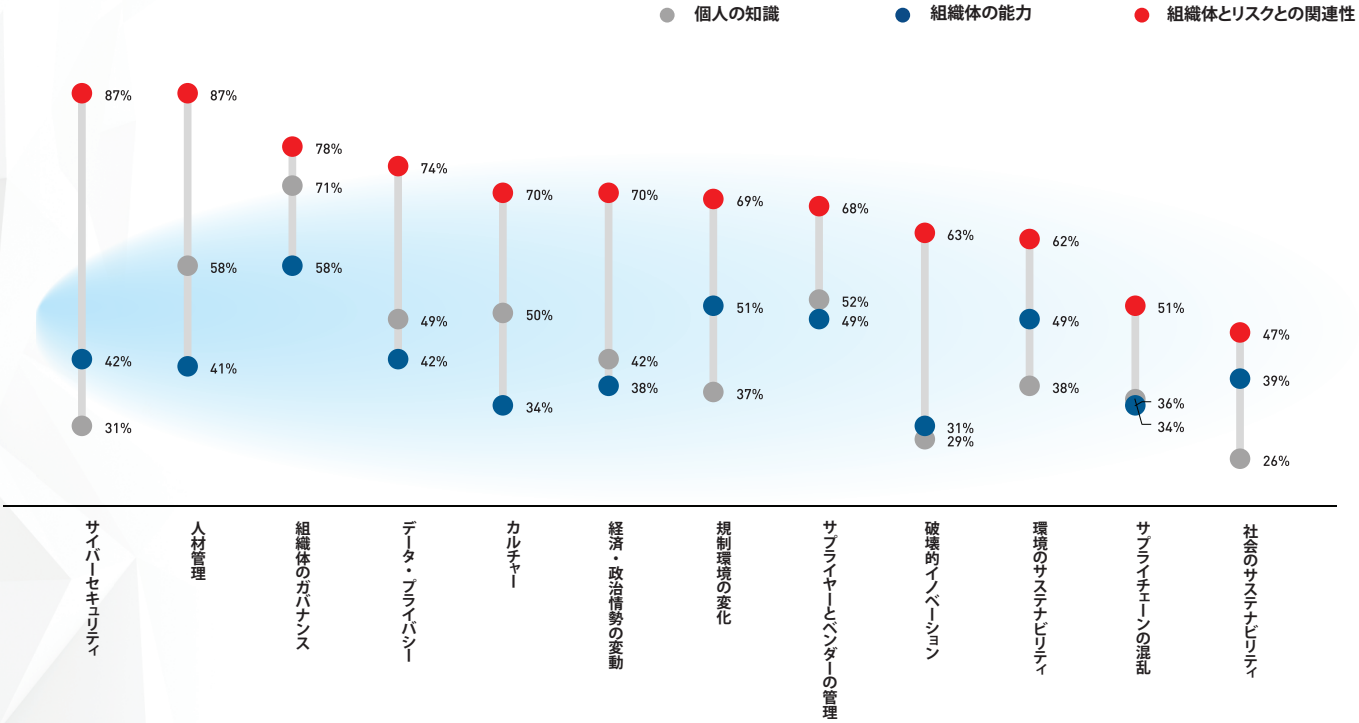
– 製造業、取締役

これらのリスクについて、関連性と能力の関係は様々である。組織体との関連性が高いリスクは、例えばリスクの速度を増大させ得る外部要因のために予測不可能で容易にコントロールできないことから、管理がより困難になる可能性がある。これは、最大の差がある６つのリスクのうちの３つ、すなわちサイバーセキュリティ、破壊的イノベーション、および経済・政治情勢の変動に当てはまるようである。しかし、コントロールとプロセスを通じて組織体内部で管理できるリスクである、人材管理、カルチャー、およびデータ・プライバシーの場合、ギャップはコントロールの欠如ではなく、パンデミックから生じる不確実性を反映している可能性がある。

図３：

リスク領域ごとの平均評価

７段階で６または７と評価した割合



注：OnRisk 2022 インタビューの質問：次の各リスクについて、どの程度知識がありますか。次の各リスクは、現在の組織体にどの程度関連していますか。総じて、全社的リスクを扱うことに関して、あなたの組織体はどの程度能力がありますか。回答者は、７段階から評価を選択でき、１が最低（「まったくない」）、７が最高（「極めてある」）である。リスク領域は、平均スコアが高いものから低いものへと並べ替えられた。有効回答数＝ 90。

例えば、人材管理の関連性と能力のギャップは、パンデミックによって引き起こされた１年半近くの孤立から組織体が脱する最中の不確実性を反映している可能性がある。労働力管理に関するこの不安は、効果的な職場復帰戦略を立案するという課題から、雇用主と従業員の間の社会的契約のより深刻な変化にまで及ぶ。

あるヘルスケア企業の経営幹部は、この領域の中でパンデミックに気付かされたことを認めた。「今、考えている最大のことは、リモートワークに対応しつつ一部の従業員をオフィスに戻すことや、ワクチン接種を受けることなどである。パンデミックは、私がリモートワークのリスクに関して思考プロセスに固執しすぎていることをはっきりと気付かせた」。

回答者は、直接影響を与えることができないリスクを管理するための様々アプローチを示した。例えば、ある金融業の取締役は、規制の変更は関連性があり注意深くモニタリングしているが、大部分は組織体ではコントロールできないと指摘した。「例えば、規制環境の変化は非常に重要である。規制の影響には細心の注意を払っている。しかし、実行は難しく、誰もが実際にコントロールできるものではない」。

一方、別の金融業の取締役は、統治できるものに焦点を当てることにしていると述べた。「自社でコントロールできるリスクに注意を払っている。コントロールしにくい関連リスクを検討する際は、市場と競合他社を理解することが重要である」。

前述のように、回答者グループ間では、個人の知識、組織体の能力、および組織体とリスクとの関連性の評価は、概ね整合している。ただし、関連性と能力の相違は、各回答者グループの評価の平均が明白に示している（図３）。

今後注意を払うべきリスク

回答者は、今後３年から５年で組織体との関連性が高まると予想される５つのリスクを特定した。サイバーセキュリティ、人材管理、破壊的イノベーション、カルチャー、および経済・政治情勢の変動である。これらはそれぞれ、関連性と能力のギャップが大きいと特定されたリスク領域に分類されている。この一致は、組織体が将来のリスクを管理する能力に大きく後れを取っているという厄介な兆候、あるいは、リスクプレーヤーが能力の弱点を直感的に認識していてそれらを修正するために行動しなければならないことを理解しているという明るい兆候、と考えられるかもしれない。

サイバーセキュリティ：サイバーセキュリティは関連性と能力に 45 ポイントのギャップがあり（図３を参照）、サイバーリスクの進化と厄介な性質に追いつくための絶え間ない苦闘を反映している。サイバーハッカーは、悪用するための新たな弱点と、犯罪に利用するための新たな方法を常に探している。2021 年５月に米国の主要な石油流通システムの運用を一時的に停止したサイバー攻撃に反映されるように、ランサムウェアやその他のサービス妨害タイプの攻撃の数と巧妙さが増しており、その結果はより広範な影響を及ぼしている。

人材管理：人材管理は、当面の間、最大のリスクであり続けると予想される。このリスクの関連性と能力のギャップは、サイバーセキュリティを抜く 46 ポイントで、今年調査したすべてのリスクの中で最大であった。パンデミックが労働市場に与える影響と、雇用主と従業員の間の従来の社会的契約に関する懸念は、このリスクをリスク・マネージャーの心の中心に据え続けている。

OnRisk2021 で述べたように、「人材管理に対するこの重大な混乱は、士気、生産性、および職場のカルチャーへの影響と同様に、組織体に短期・長期的な影響を及ぼしている」。潜在的な混乱の証拠として示された２つの領域は、すぐに現実のものとなった。

在宅勤務という現象は、組織体が人材を採用および管理する方法を根本的に変えた。従業員の大部分がリモートワーク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生じたが、適切な人材を特定して採用する際の地理的な問題という制約はほぼなくなった。ある製造業の経営幹部は、次のように述べた。「人材管理は、労働力における世代間ギャップが強調されるようになり、より難しくなる可能性がある。最高の人材をどこで見つけようとしているのだろうか」。

今後注意を払うべきリスク

（続き）

それでも在宅勤務の試みは、労働力の様々な部分のワークライフバランスに関する考え方にも大きな影響を与えたようである。フォーブス誌[1]の 2021 年 6 月の記事によると、多くの人々の期待は、その年の在宅勤務で変わった。例えば、この記事では、法科大学院と医大への応募がそれぞれ 20%と 18%急増していることを引用して、多くの人がキャリアパスを考え直しているという証拠に言及している。

自主退職する社員が増えている。「大量（自主）退職」と呼ばれるこのパンデミックの副産物は、労働力に長期的な影響を与えることは確かである。米国労働統計局のデータによると、米国では 2021 年 4 月だけで 400 万人近くが退職しており、これは単月では過去最大の急増である。さらに 360 万人が 5 月に自主退職した。この現象は米国に限ったことではない[2]。

英国放送協会[3]によると、世界中の 3 万人以上の労働者を対象としたマイクロソフト社の調査では、今年は 41%の労働者が辞職や転職を検討していた。同レポートでは、パンデミックが始まって以降リンクトイン社へのリモート求人依頼が 5 倍に増加し、46%以上の労働者が、リモートワークができるようになったと感じたため転居を計画していると述べている[4]。

組織体は労働者をオフィス環境に戻すことを重視しているため、労働市場の逼迫と、それが給与、福利厚生、およびワークライフバランスにおける労働者の期待とどのように関連しているかを慎重に検討する必要がある。

カルチャー：パンデミックによって分散した労働力は、職場のカルチャーについて大きな懸念を引き起こしている。このリスクの関連性と能力のギャップは 36 ポイントである。

組織体のカルチャーの構築や維持は、事実上重大な課題を提起し、組織体は現在、パンデミック前の就労形態に戻るか、より多くのリモート労働者に適応する方法を見つけるかという問題に直面している。在宅勤務の経験は、信頼の向上、階層の平坦化、およびより迅速で機敏な意思決定を組織体が目の当たりにするなど、前向きな変化をもたらした。それでも、コミュニケーション、労働者の交流、協働、人間関係の構築、および合意形成を支援する上での課題は残っている。従業員と雇用主の間の社会的契約の根本的な変化（人材管理の節を参照）は、この厄介なリスクをさらに複雑にしている。

*「**私たちは皆カルチャーを**『経験している』が、それを管理して変更する方法を理解することは、まったく別の話である。」*
– 金融業、ＣＡＥ

経済・政治情勢の変動：パンデミックによる継続的な政治的・経済的影響がこのリスクを引き起こし、関連性と能力のギャップを 32 ポイントに押し上げている。

2021 年 7 月の米国議会調査局報告書によると、パンデミックの発生は世界的に均一ではなく、特に発展途上国で経済の変動が続くことを意味する。

「パンデミックの経済的影響は、ワクチン接種によってパンデミック前の活動レベルに戻りつつある先進国では減少すると予想される。しかし、発展途上国では、新たなウイルス変異株の流行がパンデミックを長引かせ、回復の見通しを弱める可能性がある」と報告書は述べている。

さらに、新たなウイルスの変異株によって引き起こされた新型コロナウイルス感染症例の復活は、経済の回復を長引かせたり、一時的な後退を引き起こしたりする可能性がある[5]。

*「**2008 年から 2009 年にかけての世界金融危機までは、物事は簡単だった。**現在、2020 年、2021 年から 2022 年にかけて、大きな変動が予想される。経済がどこに向かっているかについて確かな感触はないが、製品の不足、遅延、混乱などの大きな影響については、現在、より多くを計画している。」*
– 金融業、経営幹部

1: Kreznar, Christian, "Employers, Don' t Fear The 'Great Resignation' —It' s Already Here," Forbes, June 3, 2021.
2: Economic News Release, "Table 4. Quits levels and rates by industry and region, seasonally adjusted," U.S. Bureau of Labor Statistics, Washington, D.C., https://www.bls.gov/news.release/jolts.t04.htm
3: Morgan, Kate, "The Great Resignation: How employers drove workers to quit," BBC, July 1, 2021.
4: Microsoft 2021 Work Trend Index, https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work
5: "Global Economic Effects of COVID-19," U.S. Congressional Research Service, July 9, 2021, Washington, D.C.

歴史的に、政治の変動は経済ショックに続いており、最近では 2007 年から 2008 年の世界金融危機を受けて起きた。2021 年 4 月、国際通貨基金のマネージング・ディレクター、クリスタリナ・ゲオルギエバ氏は、パンデミックによって悪化した既存の不平等は、マクロ経済の不安定性だけでなく、二極化の拡大、政府への信頼の低下、および社会不安の増大につながる可能性があると警告した [6]。

破壊的イノベーション：破壊的イノベーションは、組織体にとってリスク・マネジメント上の最大の課題の 1 つであり、組織体との関連性と組織体の能力に関する取締役会と経営幹部の間の著しい認識の相違に反映されている。これは、回答者の評価を組み合わせた場合のリスクとの関連性と組織体の能力の間の総合的な 32 ポイントの差の一因でもある。取締役会レベルの苛立ちは明らかである。一部の回答者は、そのような課題を管理する準備ができていないことを認識している。例えば、あるヘルスケア企業の取締役は、「私たちは革新的ではなく、変化は非常に遅い。目の前のことで手一杯で、適応する準備と能力はない」と述べた。

小売業の取締役は、リスクの範囲がわからないことに苛立っていた。「（破壊的イノベーションが）どんなものかを知っていれば、それに取り組んでいる。しかし、何が来るのかがわからない」。ただし、動きの速いリスクや新たなリスクに対してより機敏で対応力のある組織体を構築するという経営幹部の動きは、このリスク領域の改善に貢献する可能性がある。ネットフリックス社対ブロックバスター社のニュースは、破壊的イノベーションを認識して活用することが、見事な成功と驚くほどの失敗という違いをもたらすことができるという典型的な例である。

ブロックバスター社は、実店舗の広大なネットワークを通じて、ビデオレンタルサービスを開拓して支配した。実際、同社は 2000 年に、ネットフリックス社の通販ビデオサービスとの統合の提案をはねつけた。しかし、わずか 6 年後、ブロックバスター社の加入者 200 万人に対してネットフリックス社は 630 万人の加入者を獲得して、オンラインビデオレンタルを支配した。2008 年、ネットフリックス社の首脳陣は、テクノロジーがビジネスモデルを著しく破壊する可能性があることを認識して対応したことを再び示した。同社はシュターツ社の映画をストリーミングする契約に署名し、2010 年までに、ソニー社、パラマウント社、ライオンズゲート社、およびディズニー社との追加契約に署名した後、北米の視聴量の 20%のシェアを獲得した。その同じ年に、ブロックバスター社は破産を申請した。

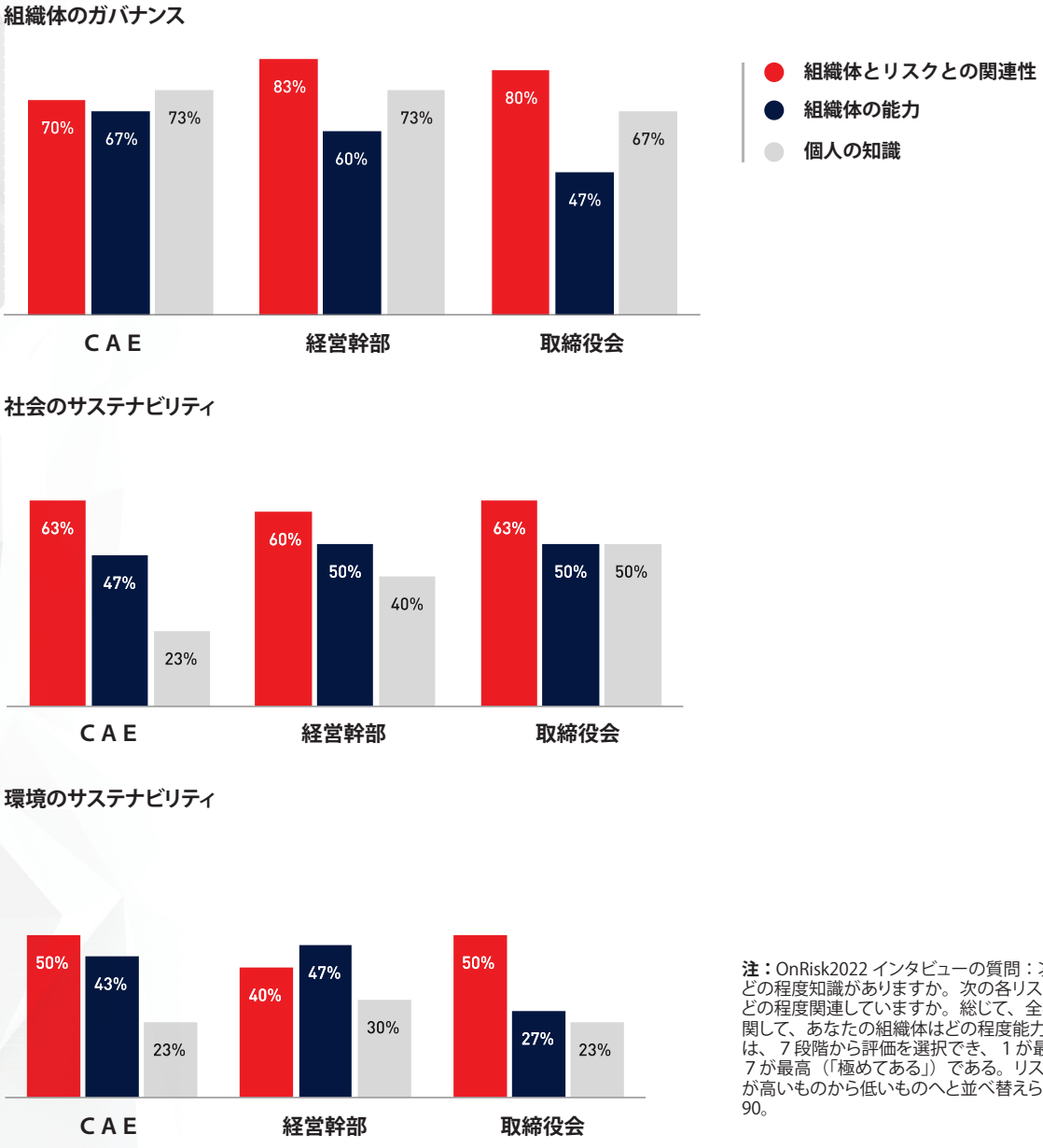
6: Hammond, Andrew, "The world is facing even greater political upheaval in post-pandemic world," Arab News, April 8, 2021.

組織体とリスクとの関連性の認識は、ＥＳＧの構成要素によって大きく異なる

OnRisk 2022 は、ＥＳＧに関連する３つのリスク領域である、環境のサステナビリティ、社会のサステナビリティ、および組織体のガバナンス**を分析している。**回答者の評価と回答は、調査参加者にとって組織体のガバナンスが社会のサステナビリティと環境のサステナビリティよりも重要であることを明確に示している（図４）。個人の知識、組織体の能力、組織体とリスクとの関連性という３つの OnRisk 指標すべてにおいて、回答者は組織体のガバナンスを調査した全リスクの中で最も高く、社会のサステナビリティと環境のサステナビリティのリスクよりもはるかに重要であると評価している。

図４：

ＥＳＧ指標―各役割の関連性、知識、および能力の比較
７段階で６または７と評価した割合



注：OnRisk2022 インタビューの質問：次の各リスクについて、どの程度知識がありますか。次の各リスクは、現在の組織体にどの程度関連していますか。総じて、全社的リスクを扱うことに関して、あなたの組織体はどの程度能力がありますか。回答者は、７段階から評価を選択でき、１が最低（「まったくない」）、７が最高（「極めてある」）である。リスク領域は、平均スコアが高いものから低いものへと並べ替えられた。有効回答数＝90。

このような高い評価は、組織体のガバナンスが幅広い関連性を持つことに影響された可能性がある。実際、大部分の組織体は、目標の達成に影響を与える様々なリスクにわたって強力なコントロールを行うことの必要性と価値を認めている。また、パンデミックが引き起こしたガバナンスの課題に対応するための大胆で協調的な取り組みと、それらの課題を克服するための強力なリーダーシップの必要性を反映している可能性もある。さらに、これは、より強力な組織体のガバナンスを支援する主なリスク・マネジメント・プレーヤー間で、リスクに対する認識を合わせることの利点について意識が高まっていることを示している。

ある製造業の経営幹部は、認識の整合と成功を結びつけた。「私たちは認識が整合しているという結論に達した。それは、大部分のことに対する認識の整合を示しており、成功に役立つと思う」。別の意見は、組織体の強力なガバナンスの価値と脆弱なガバナンスの危険性に対する認識の高まりを反映している。

*「**多くの公開企業については、**能力はもっと高くなる可能性がある。発生する問題のいくつかを見て欲しい。もしも誰もが本当に上手にやっていたならば、上場 企業の構造が崩壊するのをそれほど多くは見なかっただろう。」*

– 金融業、取締役

*「**現在、取締役会内にリスク専門の専門委員会を設置している。**これにより、様々なリスクに対する組織体の対応に関する優れた文書を作成することができた。」*

– 金融業、取締役

*「**他のすべてのリスクをどのように計画するかは、**組織体のガバナンスによって決まる可能性がある。それは非常に重要であり、すべてに及ぶ。」*

– 製造業、経営幹部

(19 ページに記載した、「パンデミックは、組織体のリスク・マネジメントの改善機会を明らかにした」の追加の分析を参照。)

企業のサステナビリティの擁護者は、社会と環境のサステナビリティが組織体のガバナンスの全般的な健全性にとって重要な要素であることをすぐに指摘する。しかし、OnRisk の回答者によるリスク関連性の評価は、そのような明確な関連性を反映していなかった。実際、社会のサステナビリティと環境のサステナビリティは、リスクとの関連性の下位４分の１に位置付けられている。気候変動に関する広範な懸念にもかかわらず、回答者の半数未満しか、環境のサステナビリティを組織体との関連性が非常に高いリスクとして特定していなかった。確かに、一部の回答者の意見は、環境のサステナビリティに関する狭い範囲の状況を反映していた。

*「**職場の人々は、食べたり、飲んだり、トイレを使用したりするが、**どこかに廃棄しなければならない毒を生み出しているわけではないので、環境のサステナビリティが話題に上ることはない。」*

- 金融業、取締役

ＥＳＧ報告書を作成する組織体数の増加と、そのような報告書に対する投資家の圧力の高まりに反映されているように、ＥＳＧリスクに対する認識が高まっているが、変化は、サステナビリティの価値に対する基本的認識ではなく、短期的な懸念によって起こる可能性が高いようである。例えば、世界的な出来事と社会活動の高まりによって、過去１年半で社会のサステナビリティが焦点になったが、環境のサスティナビリティはまだ遅れている。

回答者は、真の変化と上辺だけの変化が混在していると考えているが、大部分は、組織体が真の変化を推進していると考えている。ただし、一部の回答者の意見は、短期的な懸念と偏狭な考え方の混在を反映している。

ある製造業の経営幹部は、ＥＳＧの動きを全般的なサステナビリティよりもマーケティングに関連付けた。「入札手続きを経て落札して仕事を得るためには、サステナビリティに対する十分な意識を持つ必要があるが、これまでのところ、真の市場主導の願望というよりも、顧客向けの戦術のようである」。

しかし、環境への影響を管理することの価値を理解している人もいる。ヘルスケア企業の取締役は、そのような懸念は他のリスクに匹敵しなければならないと嘆いた。「大部分の組織体は、環境のサステナビリティについての優れた方針、手続、およびプログラムを持つことを望んでいるが、すべてのリスクに対処する際に、環境のサステナビリティが常に中心になるとは限らない」。

組織体とリスクとの関連性の認識は、ＥＳＧの構成要素によって大きく異なる
（続き）

別の回答者は、ＥＳＧの構成要素が組織体内でどのように連携して機能するかについて、より広範な見解と理解を表明した。

*「**サステナビリティは、富を保全し、維 持し、増やすために絶対に不可欠である。**これは、事業への他の投資と同じである。創出した価値を保全して維持するためには、サステナビリティへの投資を行う必要がある。」*

– 金融業、取締役

*「**社会のサステナビリティの変化に対して、**オープンマインドで、変化を望み、仕事に積極的に取り組むリーダーが必要である。そうでなければ変化は起きない。」*

– 教育業、ＣＡＥ

組織体の規模と成熟度も、ＥＳＧリスクを管理する上での潜在的な制約として挙げられた。リソースが限られていると、ＥＳＧリスク、特に環境と社会に関連するリスクの優先順位が低くなる。

非営利組織体の経営幹部は、「ＥＳＧでより良くなることを願っているが、それは優先事項ではない。小規模事業なので、サイバーセキュリティや組織体のガバナンスなどが優先され、環境と社会のサステナビリティは後回しになる。幸い、ＥＳＧに専念するチームやＥＳＧ担当者がいる組織体もあるが、現状では手一杯である」と嘆いた。

ＥＳＧを測定して報告するための明確な方向性や基準の欠如も妨げとして挙げられた。ある金融業のＣＡＥによると、「ＥＳＧについて何らかの測定を行うことは、真の変化を推進するのに役立つ。アカウンタビリティを果たし、実際に起こっていることを示してから、起こっていることを文書にして報告する必要がある」。

ただし、報告に重点を置きすぎる企業はＥＳＧリスク・マネジメントの真のメリットを見逃していると、製造業のＣＡＥは考えている。「問題は、報告を重視している企業が上辺だけになりがちなことである。彼らは単にチェックマークを付けて、ステークホルダーが満足するようにリスク・マネジメントを行ったと報告書を出す可能性がある。より多くの施策と実際の活動が起こる必要がある」。

パンデミックは、組織体のリスク・マネジメントの改善機会を明らかにした

新型コロナウイルス感染症は、大部分の組織体に、リスク・マネジメント活動を組織体全体でどのように調整するかを、ある程度重視させた。パンデミックは、リスクを予測する能力は改善しなかったかもしれないが、多くの人々がリスクに反応することへの自信を高めた。一部の人には、レジリエンスを評価または再評価する機会をもたらした。別の人には、分散型や縦割りの状態でリスクと危険性をどのように管理するかについての注意喚起となった。

ある非営利団体の理事は、パンデミックがいかに驚くべきものであるかが証明されたと説明した。「将来発生し得る、管理しなければならないシナリオがあることを認識した。現在、リスクアプローチの不足を非常に認識している」。

他方で、小売業の取締役は、パンデミックがもたらした内省の良い点と悪い点を考えた。「リスクの予測があまり得意ではなかったとわかったが、非常にうまく反応したと思う。将来発生し得るシナリオと、それらをどのように処理するかを考えさせられた」。

パンデミックは、組織体のリスク・マネジメントの改善機会を明らかにした
（続き）

OnRisk の回答者は、第三者のプロバイダーやパートナーとの連携についても懸念を示した。ある教育業のＣＡＥによると、「第三者は、特にサイバーセキュリティなどのリスクに関して、目的や報告が整合していないという懸念がある。組織体は、第三者との合意事項、契約管理、および関係構築をモニタリングする方法を改善すべきである。多くの場合、組織体は単に「片付ける」だけであり、じっくり考えてはいない」。

１年以上閉ざされた経済活動、在宅勤務者、負荷や混乱のあった供給ライン、および世界で 400 万人を超える驚くべき死者数から世の中がゆっくりと抜け出す際、新型コロナウイルス感染症後のリスク・マネジメントに対する初期の焦点は、主に短期的な懸念へ当てられているようである。

「リスクに関しては、間違いなく私たちの見方に影響を与えている。しかし、リスク戦略や長期的なことを変更するための具体的な計画はまだ決まっていないと思う。ハイブリッドシステムを作り、従業員の健康と安全を維持することに重点を置いている」と、ある政府機関のＣＡＥは述べている。

一方、あるテクノロジー企業の経営幹部は、単に可能性を残す努力をしていると説明した。「私たちはまだ生き残りをかけた状態にある。パンデミックの永続的な影響については考えていない。パンデミックが起こるとは思っていなかったので、ただ乗り越えようとしている」。パンデミックは一部の人々に、組織体全体にリスクがどのように現れるかについて貴重な教訓をもたらした。「新型コロナウイルス感染症は、リスク・マネジメントに関して、より集中化した包括的な戦略と指導を実施する必要があることを教えてくれた」と、ある教育業のＣＡＥは述べた。

新型コロナウイルス感染症後の雇用主と従業員の人間関係の複雑さと力関係は、多くの OnRisk 回答者が高いと評価した。パンデミックは、人材とカルチャーを管理することの重要性を浮き彫りにした。ある不動産業の経営幹部によると、「私たちの心配は、新規採用者とカルチャーを共有する機会を失うことである。彼らは採用と同時に在宅勤務となるため、（カルチャーを）実際に体験することがなかった」。

長期計画のための会議は多くの人にとって最重要事項ではなく、回答者は、将来の緊急時対応計画に、より重点を置くと述べている。

「現実には、大部分の企業には緊急時対応計画がまったくない。今や企業は、緊急時対応計画と、予期せぬリスクに対応するためのチームと職位を割り当てることの重要性を理解するために取り組まなければならない」と、ある地方自治体の理事は述べた。

経営幹部と取締役会は、より広範な内部監査業務を望んでいる

多くの組織体にとって、新型コロナウイルス感染症の経験は、主なプレーヤー間のリスク・マネジメントの整合性の価値だけでなく、財務リスクやコンプライアンスリスク以外のリスク・アシュアランスを活用する可能性についての認識を高めた。OnRisk の回答者は、業務リスクと全社的リスクに対するアシュアランスの拡大、およびリスクに積極的に対応する必要性への関心の高まりを示した。これらの進展は、特にサイバーセキュリティ、人材管理、および組織体のガバナンスなどの組織体との関連性の高いリスク領域において、内部監査業務をさらに活用する機会を示している。総じて回答者は、現在のアシュアランス業務を適切であると感じているが、アシュアランス報告の改善を提案している。

*「**監査人が全社的リスクではなく財務リスクに焦点を当てていたために、**私たちの認識が相違していた時期があった。組織体は両方を扱う必要がある。」*

– ヘルスケア企業、経営幹部

全社的リスク・マネジメントに対する理解と認識が高まるにつれて内部監査に対して、内部監査の範囲を拡大し、取り扱っていないリスクを特定し、新たなリスクをモニタリングし、ステークホルダーに明瞭かつ簡潔に報告し、テクノロジーをさらに活用して強固なリスク・マネジメント・アシュアランスを提供するようにという要求が高まる。

ある小売業の取締役は、組織体内での内部監査に対する見方を広げる時が来たと述べた。「一部の人々は、内部監査はあまりにも受動的で、その時点でのニーズに左右されているだけだと考えている。内部監査がプロセスについて考え、前進し、ギャップを特定するのは良いことだと思う」。

テクノロジー企業の経営幹部は内部監査に、業務を拡大して新たなリスク領域を扱うよう求めた。「現在、当社の内部監査は、環境のサステナビリティや規制環境の変化など、一部のリスクには手を付けていない」。

適切なリスク・マネジメントのアシュアランスのために内部監査が不可欠であると、すべての回答者が感じているわけではない。あるＩＴ業界の経営幹部によると、「当社には、内部監査はないが外部監査があり、必要性を満たすには十分だと思う」。一部の組織体は、リスク・マネジメントのアシュアランスを外部監査のみに依拠しているが、この近視眼的なアプローチには固有のリスクがある。

従来から主に財務報告とコンプライアンスに焦点を当ててきた外部監査によるリスク・マネジメントのアシュアランスに依拠することは、それ自体がリスクを伴う。あるテクノロジー企業の経営幹部は、リスク・マネジメントに必要な視点を加えた、より洗練されたアプローチを明確に述べた。

「当社には正式なＥＲＭプロセスがあり、組織体全体の年次レビューを主導する担当者がいる。リスクが評価され、ギャップが特定されてから、発生可能性と重要性、および許容度が決定される。200 のリスクが評価され、様々なカテゴリーに分類される。当社にはこのプロセスがあり、監査機能はリスクを非常に理解しているため、十分なアシュアランスがあると思う」。

OnRisk の回答者は、アシュアランス報告の一貫性を高めることに加えて、より多くのデータと分析や、報告書の読み手に基づいて調整された詳細など、発見事項を伝達するためのより良い方法を望んでいると述べた。ある金融業の取締役は、関連性のある実用的なリスク情報を効果的に提示する必要性を強調した。「一部のリスクレポートは詳細すぎる場合があり、洞察を引き出しにくい。詳細なのは良いが、ステークホルダーや取締役向けに関連情報の要約があるべきだ」。

さらに、内部監査は、危機の際に実行して価値を付加する能力を実証しなければならない。ある製造業の経営幹部によると、「私は火災避難訓練の例えを考えている。火事がないことがわかっている時は、一列縦隊で落ち着いて外に出るのは簡単である。実際の火災の時でもまったく同じように行動するだろうか」。

OnRisk 調査に対するＣＡＥ回答者は、内部監査を向上させるための機会と必要性を次のように認識している。

*「**自分一人で物事は行えない。**パートナーを持つべきであり、それは誰もが成功する方法である。縦割りで報告や管理をするのではなく、組織体全体で一貫性を保つべきである。」*

– 政府機関、ＣＡＥ

*「**重要リスク指標を決定し、**それらを測定し、反映し、対処し直し、再報告する必要がある。それはサイクルである。」*

– テクノロジー企業、ＣＡＥ

*「より多くのデータ・アナリティクスを構築し、事実に基づくより多くのデータを使用してリスクを評価することについては、**常に改善の余地がある。**」*

– 金融業、ＣＡＥ

洞察と取るべき措置 ー取締役会

財務とコンプライアンスの問題以外のリスクに関する個人の知識を広げている取締役の英知は、かつてないほどはっきり認められる。迅速な技術革新、破壊的イノベーション、組織体のガバナンスの動き、パンデミック、およびその結果としての経済・政治情勢の変動は、取締役がリスク・マネジメントにおける自らの役割の捉え方を広げるための十分な刺激となっている。

今後１年間で、取締役会は次のことを行うべきである。

経済・政治情勢の変動に関する知識を向上させる。先に述べたように、このリスク領域は、事業のやり方を変え得る深刻な長期的影響を与える可能性がある（12 ページの「今後注意を払うべきリスクー経済・政治情勢の変動」を参照）。

- *取締役は、経済と政治の両方の変動が組織体の運営にどう影響するかについて理解を深めるべきである。*
- *取締役会は、危機管理計画に変動のシナリオを含めるよう経営幹部に指示し、そのようなシナリオと対応をテストすることを検討すべきである。*

経営幹部と内部監査にＥＳＧリスク・マネジメントを奨励する。組織体は、ＥＳＧ報告に関する規制要件や投資家の期待の高まりに備えるべきである。米国証券取引委員会やその他の規制当局は、この領域の規制強化への関心を明確に示している。取締役会は、ＥＳＧ報告に加えてＥＳＧリスクを管理するための全社的なアプローチを推進すべきである。

- *組織体のＥＳＧリスク評価を要請する。*
- *経営幹部に、組織体のＥＳＧ報告の妥当性を判断するためにどのようなフレームワークを使用しているかを尋ねる。*
- *内部監査に、ＥＳＧコントロールの設計と運用の有効性の評価に関連するアシュアランス業務や助言業務を依頼する*

カルチャーと人材管理に関する詳細情報を求める。

- *組織体のカルチャーの独立した評価を求めることを検討する。*
- *経営幹部に、パンデミックに起因する人材管理関連の意思決定と変更について取締役会に知らせ続けるよう要求する。*

組織体のガバナンスの重要性を強調する。

- *主なリスク・マネジメント・プレーヤー間でリスクに関する認識を合わせることの重要性を継続的かつ一貫して強調する。*
- *縦割りや分散型のリスク・マネジメントのアプローチを認めない。*
- *このリスク領域に対して独立したアシュアランスを提供する際の内部監査の役割を拡充する。*

洞察と
取るべき措置－経営幹部

経営幹部は、新型コロナウイルス感染症との１年半の戦いによって複雑化した**無数のリスク・マネジメントの課題に直面している。**事業継続性や危機管理から、人材管理やカルチャーへの長期的な影響まで、パンデミックの影響は、リスクとリスク・マネジメントに長期にわたる影響を及ぼすだろう。

今後１年間で、経営幹部は次のことを行う べきである。

経済・政治情勢の変動に関する知識を強化する。先に述べたように、このリスク領域は、事業のやり方を変え得る深刻な長期的影響を与える可能性がある（12 ページの「今後注意を払うべきリスクー経済・政治情勢の変動」を参照）。

ＥＳＧ報告に関するプロセスとコントロールを成熟させるための計画を立てる。

- *全社的リスク・マネジメントや定評のあるリスク・フレームワークに関する内部監査の知識を活用して、ＥＳＧに関する有効な内部統制の構築を支援する。*
- *外部監査人がガイダンスを示すのを待ったり、規制当局が規則を制定するのを待ったりしない。*
- *特にＥＳＧ報告に関連するため、既存のＥＳＧコントロールの有効性に関するアシュアランスを提供するよう内部監査に指示する。*

人材管理とカルチャーについて取締役会を積極的に啓発する。

- *就労形態の好み、従業員の士気、生産性、および定着率に関する取り組みなど、人材管理に関連する意思決定を慎重に実施して評価する。*
- *職場復帰計画、およびカルチャーへの影響を含む関連リスクの範囲に関して、内部監査の意見を入手する。*

洞察と
取るべき措置－内部監査部門長（ＣＡＥ）

百年に一度の最も不安定で動的な時期の真最中に、ステークホルダーはリスク・マネジメントのより大きなアシュアランスが必要であると知らせている。内部監査は、対応しなければならない。

今後１年間で、ＣＡＥは次のことを行うべきである。

新たなＥＳＧ報告要件を予測する。

- *組織体内のプロセスとコントロールを理解することにより、新たな要件の先を行く。*
- *定評のあるサステナビリティ・フレームワークの採用を提唱する。*
- *ＣＯＳＯの内部統制の統合的フレームワークを活用して、非財務報告に係るコントロールの評価を始める。*

組織体との関連性と能力のギャップが高いリスク領域に関する知識を向上させる。

- *OnRisk のリストや組織体のリスクのリストの中で、個人の知識の評価が高くないリスクを特定する。*

取締役会と経営幹部の間に認識の相違がある場合は常に、パイプ役となる。

- *OnRisk の調査方法を活用して、組織体のリスク分析を行う。*
- *組織体に最も関連性のあるリスク領域について、認識の相違があるかを判断する。*
- *OnRisk 2022 の中で関連性のある重要ポイントを取締役会および経営幹部と簡潔に共有し、調査されたリスクが組織体にどう関連しているかについて対話を促す。*

カルチャーと人材管理のリスクに、より大きな焦点を当てるように支援する。

- *組織体がパンデミック後の世の中に移行する際に起こり得る認識の相違を知る。*
- *カルチャーや人材管理に関連するアシュアランス業務や助言業務を行う。例えば、従業員調査、退職時面接、またはダイバーシティとインクルージョンの施策から得たデータの分析において取締役会や経営幹部を支援する。*

調査方法

定性的調査は、組織体の認識の整合性を測定している

OnRisk 2022 レポートは、優れたガバナンスと組織体の成功を支援するために、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。**定性的調査は、2022 年に組織体が直面する主なリスクをしっかり把握している。レポートは、リスク・マネジメントのリーダーからの回答に基づいて、客観的なデータ分析と主観的な洞察の両方を示している。

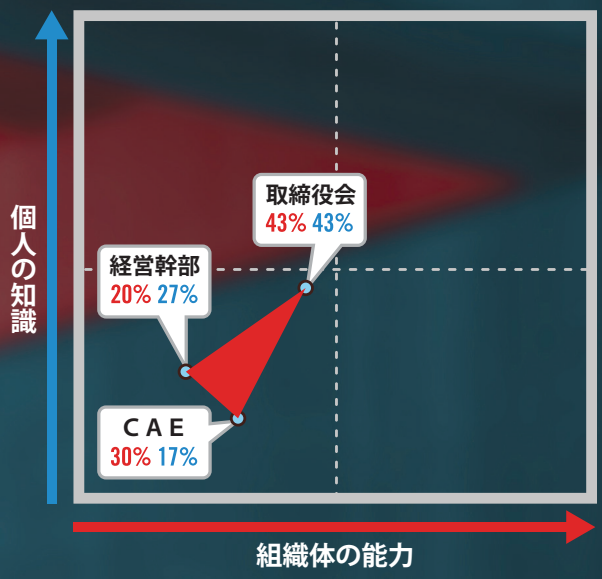
定性調査は、北米（米国およびカナダ）の取締役会、経営幹部、および内部監査部門の専門職を対象とした、合計 90 人への詳細なインタビューに基づいている。回答者は 90 の異なる組織体から選ばれた。インタビューの一環として、回答者は 3 つの尺度で 12 の重要リスクを評価するよう求められた。それらは、各リスクに関する個人の知識についての認識、各リスクに対処する組織体の能力についての認識、および各リスクと組織体との関連性についての認識である。評価は 7 段階で、「まったく知識がない」、「まったく能力がない」、「まったく関連性がない」が最低評価の 1 で、「極めて知識がある」、「極めて能力がある」、「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軸は組織体の能力に対する認識を示し、Ｙ軸はリスクについての個人の知識に対する認識を示している（図 5）。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整合性を視覚的に示している。

図 5:

個人の知識と組織体の能力

7 段階で 6 または 7 と評価した割合



本レポートの利用方法

図の説明

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個人の知識と組織体の能力を測定し、リスクごとに位置を表示した。シンプ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６）。

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、知識と能力の評価の平均が高い回答は、右上の象限に表示される。逆に、知識と能力の評価の平均が低い回答は、左下の象限に表示される。前述のように、平均は、知識と能力について６または７と回答した回答者の割合に基づいて決まる（２ページの「OnRisk の調査方法」を参照）。

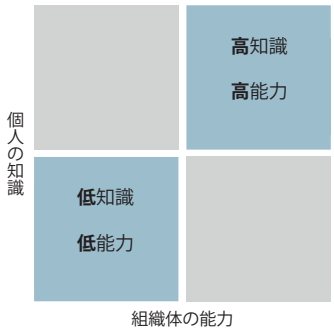


図６: **個人の知識と組織体の能力の象限図**

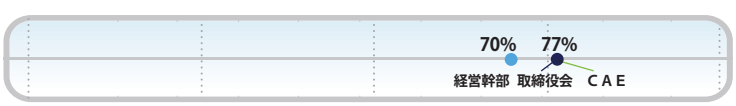
表示位置

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、象限図に表示されている。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、認識の相違を知る手掛かりにもなる（関連する補足説明を参照）。

組織体とリスクとの関連性の図

組織体とリスクとの関連性に関する各回答者グループの評価は、単一の軸に表示されており、取締役会、経営幹部、およびＣＡＥの関連性評価のばらつきを明確に示している（図７）。

図７: **組織体とリスクとの関連性の評価**



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整合しているが、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はかなり整合してい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整合していることを示唆している。三角形の形にもよるが、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。

リスク段階モデル

今日の動的でテクノロジー主導の世界では、猛烈なスピードでリスクが発生して成熟する可能性がある。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８）は、リスク評価と同じ尺度である個人の知識と組織体の能力において、組織体内でリスク・マネジメントがどう進展しているかを示している。

尚、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、競合、成熟度、市場での地位、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、組織体とリスクとの関連性はリスク段階モデルには示していない。

図８:
リスク段階モデル

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

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、概ね理解されている。

知識―中から高
能力―低

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、概ね理解されている。

知識―低から高
能力―中から高

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

リスク

本節では、個々のリスクに関連する**重要な所見を検討する**。各リスクのページには、定性的インタビューに基づいたリスクの定義と簡単な概要を記載している。また、個人の知識、組織体の能力、および組織体とリスクとの関連性に関する主なリスク・マネジメント・プレーヤー間の認識を示している。さらに、インタビュー対象者からのリスクに関する洞察に満ちた意見も引用している。該当する場合は、各リスクの進展段階について前年からの変化を示している。

サイバーセキュリティ

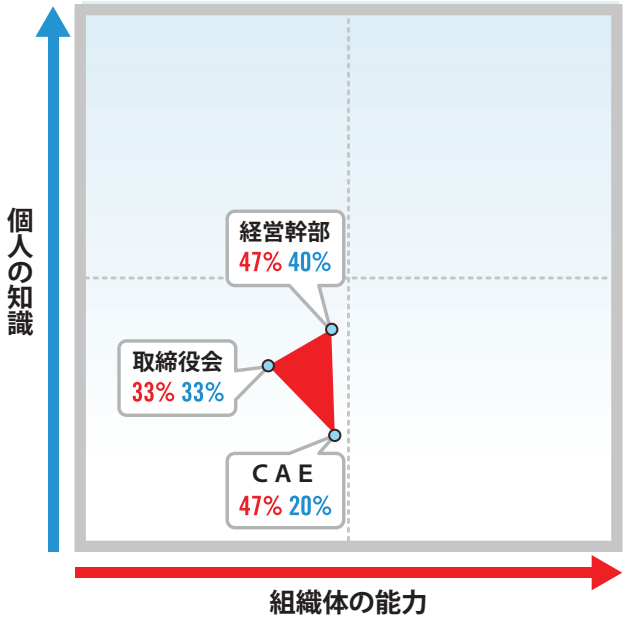
定義：

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。

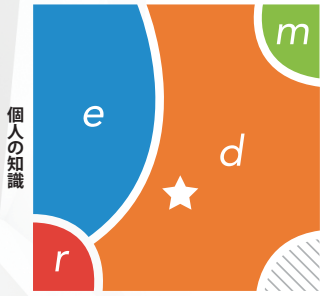
分析：

ほぼすべての回答者が、サイバーセキュリティは組織体との関連性が高いと考えている。ただし、この非常に影響力のあるリスクに関する個人の知識は、全プレーヤー、特にＣＡＥはとりわけ低いままである。この知識レベルの低さは、絶え間なく進化するサイバー脅威の性質に起因する可能性がある。総じて、全グループともサイバーセキュリティを管理する組織体の能力を高いと評価した割合は低かった。特に、組織体がサイバーセキュリティを高度に管理できると認識している取締役は少なかった。

個人の知識と組織体の能力
７段階で６または７と評価した割合



リスク段階



「展開」のままであった

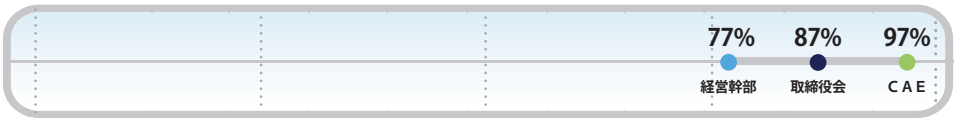
引用：

「サイバーセキュリティ・リスクは常に進化するリスクである。（サイバーセキュリティに）対処するために使用してきたアーキテクチャと計画のプロセスは、テクノロジーが普及するにつれて、より複雑になっている。」－金融業、取締役

「今年、パイプラインへのハッキングを目撃したように、これらのサイバーセキュリティ攻撃は大きなトリクルダウン効果をもたらす可能性がある。すべての業界が、ある程度はサイバーセキュリティ・リスクの影響を受けやすくなっている。」－製造業、取締役

組織体とリスクとの関連性

７段階で６または７と評価した割合
－サイバーセキュリティ



人材管理

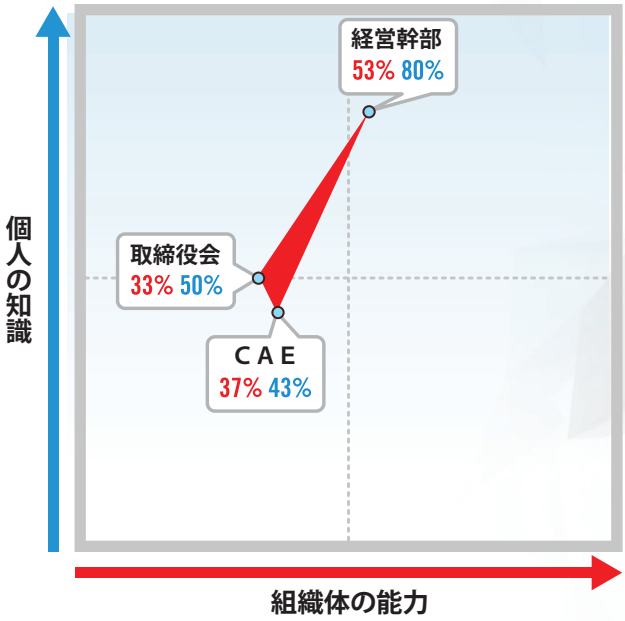
定義：

在宅勤務を含むリモート業務の**必要性**と受け入れの**増加**、および動的な労働条件の継続により、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。

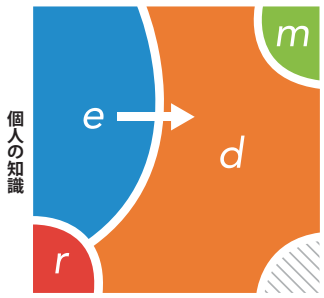
分析：

主な全プレーヤーが人材管理を組織体にとって最も関連性のあるリスクの１つと考えている**にもかかわらず、**取締役とＣＡＥについては、個人の知識と組織体の能力の両方に対する認識が比較的低いままである。この領域における経営幹部の個人の知識と組織体の能力に対する認識は、はるかに高い。

個人の知識と組織体の能力
７段階で６または７と評価した割合



リスク段階



「検討」から「展開」へ進展した

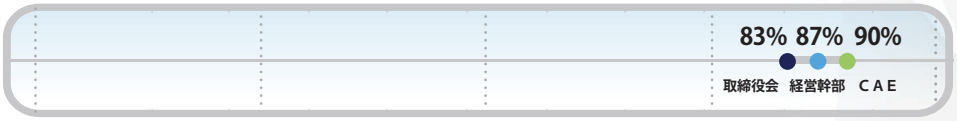
引用：

「企業は生き残るために懸命に取り組んでいるが、すべての戦略は、もはや問題ではない。従業員と直接会えない場合、戦略遂行は困難である。」－政府機関、理事

「このリモート環境での採用によって、地理的な制約なく採用を検討することができた。私たちが今自問しているのは、完全にリモートで働く、より質の高い候補者を雇うのか、それとも、オフィスに来ることができる、より質の低い候補者を雇うのか、である。
－自動車産業、ＣＡＥ

組織体とリスクとの関連性

７段階で６または７と評価した割合
－人材管理



組織体のガバナンス

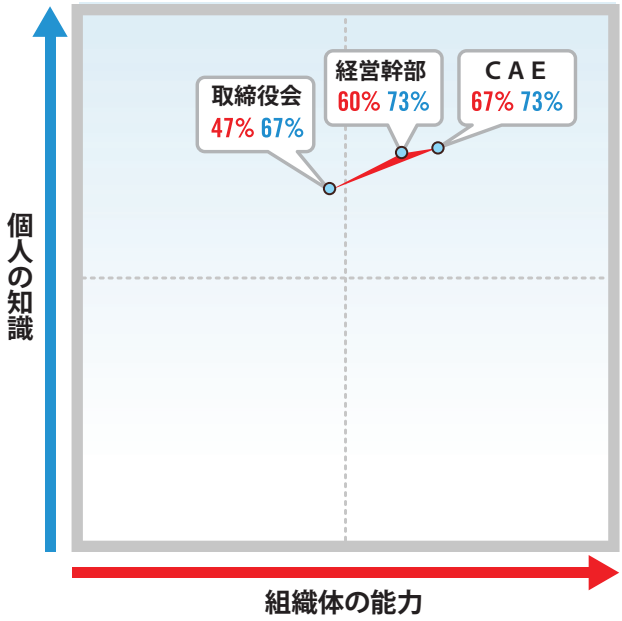
定義：

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。

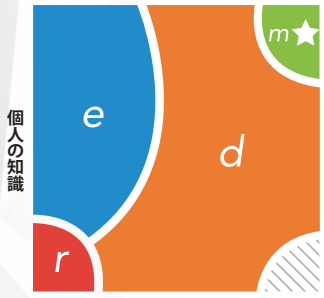
分析：

この比較的成熟したリスクに関する**個人の知識**は、３つの全リスク・マネジメント・プレーヤーで高く、関連性が高いと広く考えられている。しかし、ＥＳＧのこの重要な構成要素を管理する組織体の能力については、著しい認識の相違がある。組織体がこのリスク領域に対して高い能力を持っていると評価したのは、経営幹部よりも取締役の方が少なかった。

個人の知識と組織体の能力
７段階で６または７と評価した割合



リスク段階



「維持」のままであった

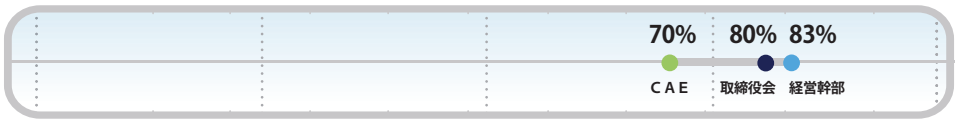
引用：

「他のすべてのリスクをどのように計画するかは、組織体のガバナンスによって決まる可能性がある。それは非常に重要であり、すべてに及ぶ。」－製造業、経営幹部

「多くの公開企業は、能力がより高くなる可能性がある。発生する問題のいくつかを見て欲しい。もしも誰もが本当に上手くやっていたならば、上場企業の構造が崩壊するのをそれほど多くは見なかっただろう。」－金融業、取締役

組織体とリスクとの関連性

７段階で６または７と評価した割合
－組織体のガバナンス



データ・プライバシー

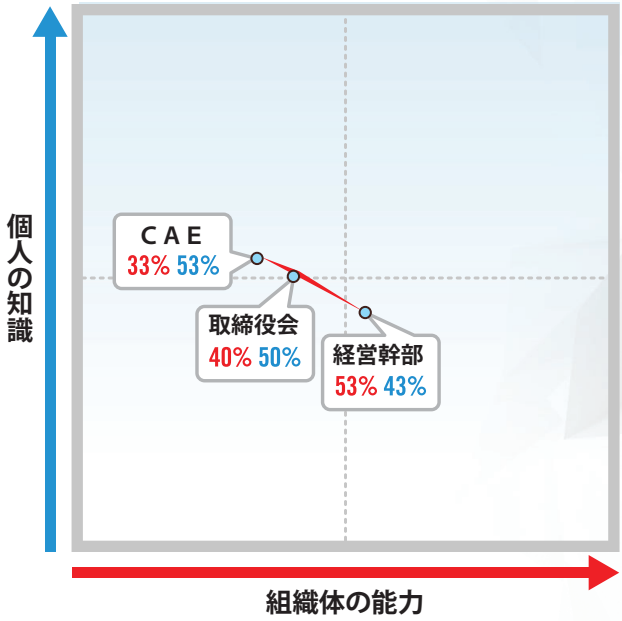
定義：

世界中の法域で**増え続ける**規制の**リスト**は、データ・プライバシーをますます複雑で動的にしている。このリスクでは、組織体がどのように機密データを保護し、適用されるすべての法規制への遵守を確保するかを検討している。

分析：

この規制が強化されつつあるリスクの**個人の知識が低**く、組織体との関連性についての認識が低**いにもかかわらず、**経営幹部は、取締役やＣＡＥよりも組織体の能力についての認識が高い。

個人の知識と組織体の能力
7段階で6または7と評価した割合



リスク段階

「展開」として OnRisk に初登場

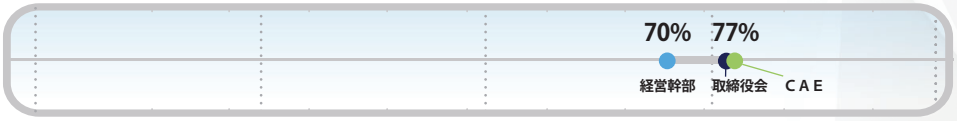
引用：

「組織体全体の共通の実務として、データを分析、収集、および保存するための手続を整備することが重要である。」ー政府機関、ＣＡＥ

「10年前と比べてデータ・プライバシーについて多くのことを聞いているが、その重要性はますます高まっていくと思う。」ーヘルスケア企業、経営幹部

組織体とリスクとの関連性

7段階で6または7と評価した割合
ーデータ・プライバシー



カルチャー

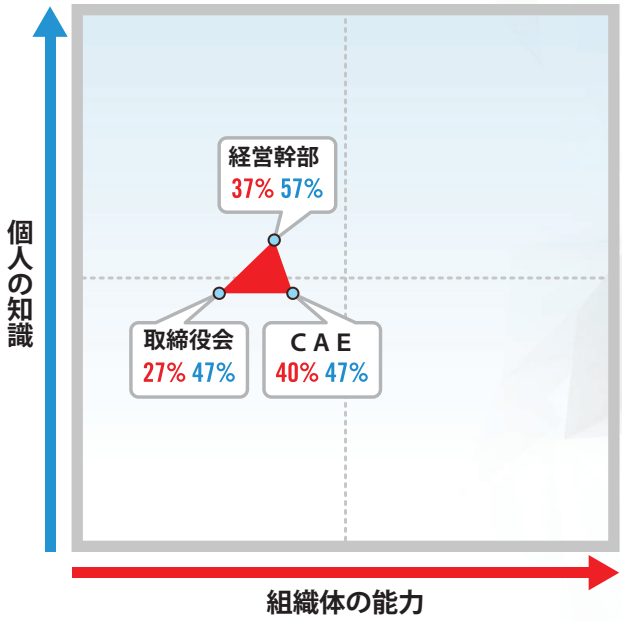
定義：

フルタイムやパートタイムでリモート作業する専門職の従業員の割合が**増加している**ため、組織体はカルチャーを維持、強化、またはコントロールすることが求められている。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討している。

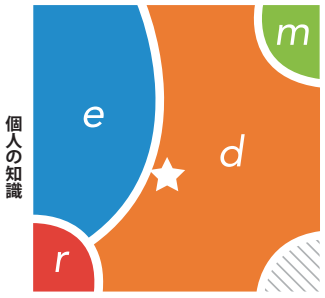
分析：

カルチャーと組織体の成功との関連性に関して、主なリスク・マネジメント・プレーヤーすべての**認識が一致している**。ただし、このリスクについて個人の知識が豊富だと認識している取締役と経営幹部の数にはギャップがある。同様に、組織体がこのリスクを管理する能力は高いと認識している取締役が少ない。これは、組織体が世界的パンデミックから脱却するにつれて、組織体にとってますます重要である。

個人の知識と組織体の能力
7段階で6または7と評価した割合



リスク段階



「展開」のままであった

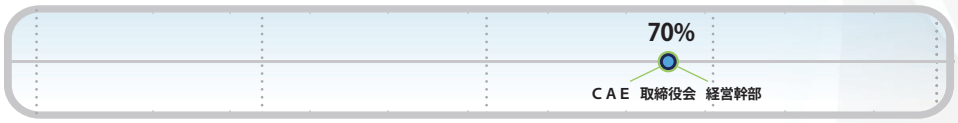
引用：

「私たちは皆カルチャーを『経験している』が、それを管理して変更する方法を理解することは、まったく別の話である。」ー金融業、CAE

「私たちの心配は、新規採用者とのカルチャーを失うことである。彼らは採用と同時に在宅勤務となるため、（カルチャーを）実際に体験することがなかった。」ー不動産業、経営幹部

組織体とリスクとの関連性

7段階で6または7と評価した割合
ーカルチャー



経済・政治情勢の変動

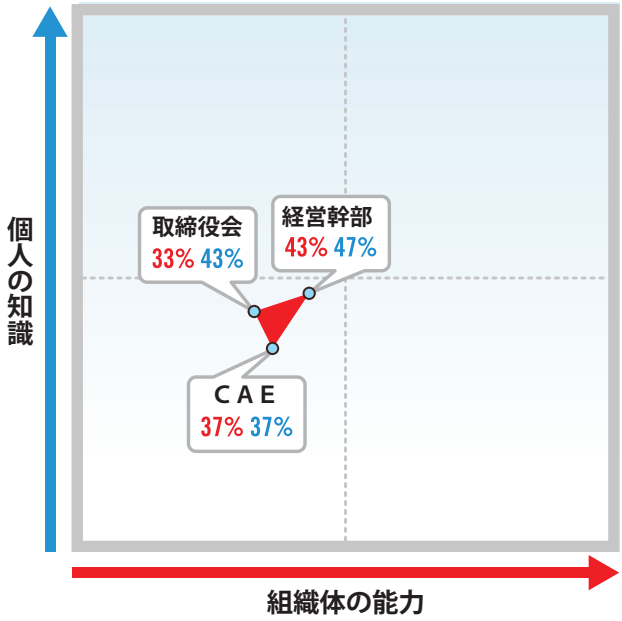
定義：

通常のマクロ経済循環の動きと結び付いた**パンデミックの継続的な影響**は、組織体が活動する市場に不安定さを生み出す可能性がある。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。

分析：

総じて、経営幹部、取締役、およびＣＡＥの間には、組織体とリスクとの関連性、個人の知識、および組織体の能力全体でかなり強い認識の整合性がある。しかし、全回答者の３分の２以上が、経済・政治情勢の変動に起因する潜在的な影響が組織体に大きな影響を与えると考えている一方で、このリスクを巡る個人の知識と組織体の能力に対する認識は比較的低いままである。

個人の知識と組織体の能力
７段階で６または７と評価した割合



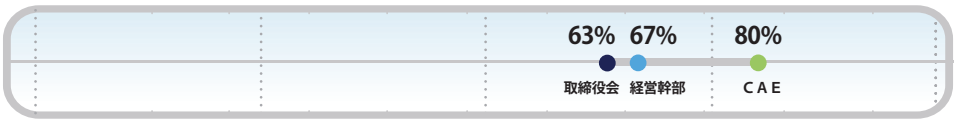
リスク段階

引用：

「2008 年から 2009 年にかけての世界金融危機までは、物事は簡単だった。現在、2020 年、2021 年から 2022 年にかけて、大きな変動が予想される。経済がどこに向かっているかについて強い感触は持っていないが、製品の不足、遅延、混乱などの大きな影響については、現在、より一層の計画をしている。」－金融業、経営幹部

組織体とリスクとの関連性

７段階で６または７と評価した割合
－経済・政治情勢の変動



規制環境の変化

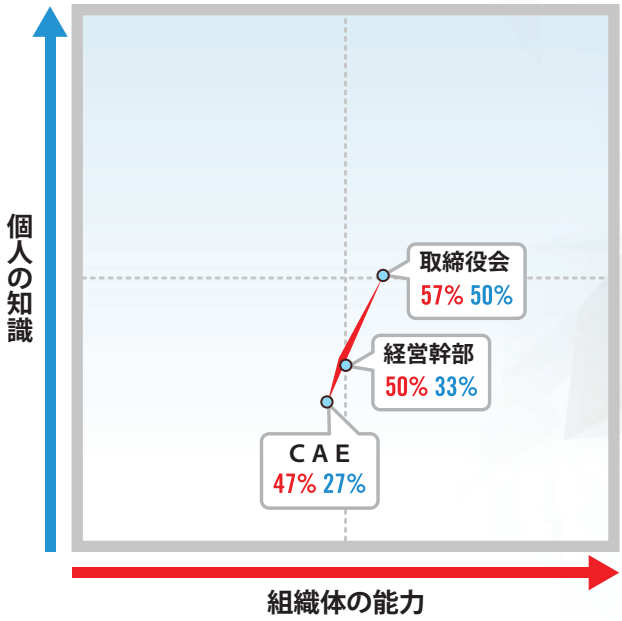
定義：

規制に対する政府の姿勢の**根本的な変化**は、規制が厳しくないと思われている組織体を含め、組織体に重大な影響を与える可能性がある。このリスクでは、動的で曖昧な規制環境下で組織体が直面する課題を検討している。

分析：

規制環境の変化というリスクと組織体との関連性が高まっていることについて、**全者の認識が整合しているにもかかわらず、**特にＣＡＥと経営幹部は、このリスクに関する個人の知識が低い。取締役の間では、このリスクに関する個人の知識は高いが、それでも他のいくつかのリスクよりは低い。取締役は、この重要なリスクを管理する組織体の能力にいくらか自信を持っている。

個人の知識と組織体の能力
７段階で６または７と評価した割合



リスク段階

「展開」として OnRisk に初登場

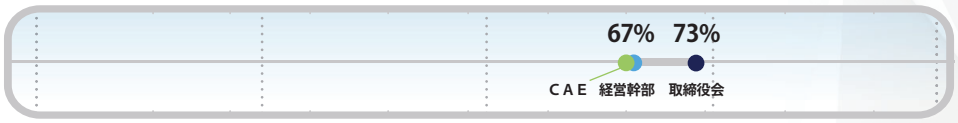
引用：

「これは大きな問題になる可能性があり、ここには本当のリスクがある。規制の変更に目を光らせておくことが重要である。」－金融業、ＣＡＥ

「強制されない限り、多くの企業は一歩踏み出すことを躊躇する。」－ヘルスケア企業、経営

組織体とリスクとの関連性

７段階で６または７と評価した割合
－規制環境の変化



サプライヤーとベンダーの管理

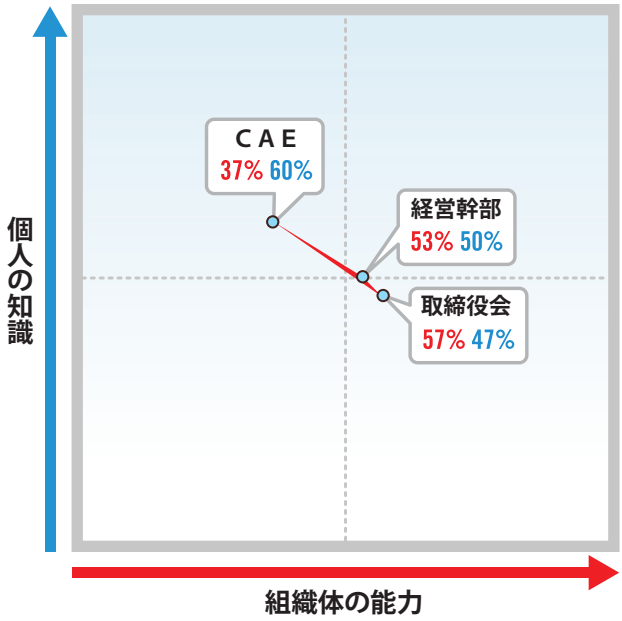
定義：

組織体が成功するには、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、第三者との関係を選択してモニターする組織体の能力を検討している。

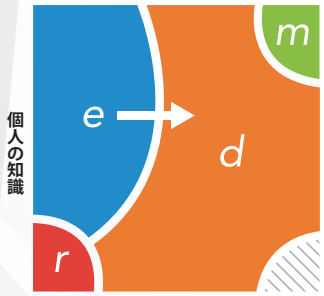
分析：

一層つながりが強まる事業環境において、**より多くのＣＡＥが**この重大なリスクについて高い知識を持っているものの、組織体がこのリスクを管理する高い能力を持っていると認識する人は少ない。ＣＡＥとそのステークホルダーの間の組織体の能力に関する認識のギャップは、このリスクを組織体との関連性が高いと考えるＣＡＥの割合が高いことが原因であり得る。これは、公に報告されたサイバー脅威、コンプライアンス関連の問題、および第三者との関係から生じるその他の破壊的事象に起因している可能性がある。

個人の知識と組織体の能力
７段階で６または７と評価した割合



リスク段階



「検討」から「展開」へ進展した

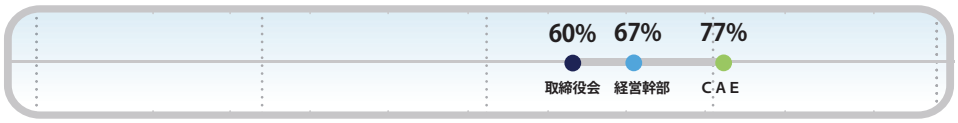
引用：

「課題は、長年のベンダーとのこの関係をどのように維持するか、そして同時に、そのベンダーがサービスを提供できない場合に、どのように他で必要なものを見つけるかである。」ー製造業、経営幹部

「当社は非常に強力な関係を築いているが、データのプライバシー、保護、サイバーセキュリティなど、サプライヤーの管理が難しいため、能力スコアを低く評価した。」ーテクノロジー企業、ＣＡＥ

組織体とリスクとの関連性

７段階で６または７と評価した割合
ーサプライヤーとベンダーの管理



破壊的イノベーション

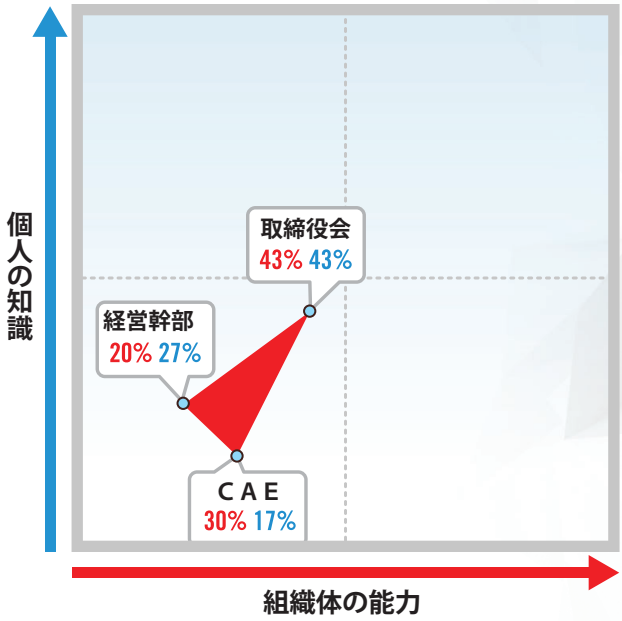
定義：

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、破壊的イノベーションへの適応や利用の準備が組織体にできているかを検討している。

分析：

このリスクを組織体との関連性が高いと考える取締役の割合は、経営幹部と比較して**かなり大きな差がある。**さらに、より多くの取締役が、この非常に重要なリスクについての個人の知識が高いと認識している。しかし、取締役は、経営幹部よりも組織体がこのリスクを管理する能力が高いと考えているため、破壊的イノベーションを管理する組織体の能力に自信過剰な可能性がある。

個人の知識と組織体の能力
7段階で6または7と評価した割合



リスク段階

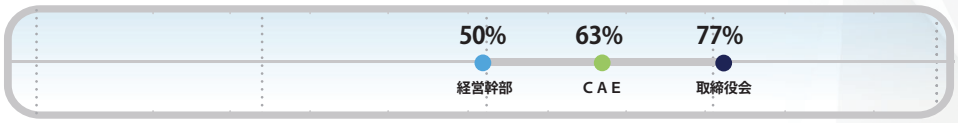
引用：

「それは認識と研究の問題である。現れてはすぐ消えるイノベーションもあるが、暗号通貨のように流行するイノベーションもある。」ー非営利団体、経営幹部

「私たちは革新的ではなく、変化は非常に遅い。すべては目の前のことについてであり、適応する準備と能力はない。」ーヘルスケア企業、取締役

組織体とリスクとの関連性

7段階で6または7と評価した割合
ー破壊的イノベーション



社会のサステナビリティ

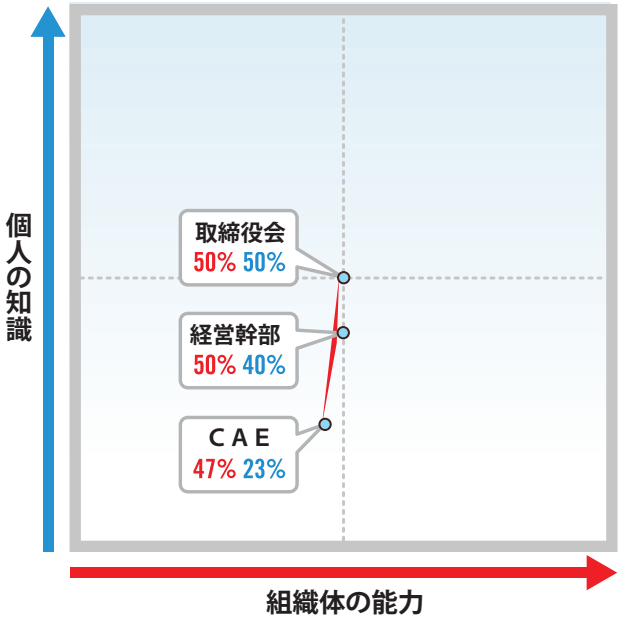
定義：

雇用する人々、バリューチェーンで働く人々、製品やサービスを消費する人々、およびコミュニティに住む人々に組織体は大きな影響を与える、という認識が**ますます**高まっている。このリスクでは、組織体の行動が人々やコミュニティに与える直接的および間接的な影響を理解して管理する組織体の能力を検討している。

分析：

主なリスク・マネジメント・プレーヤーの間では、すべての業界に影響を与えるこの急速に出現するリスクに対する組織体とリスクとの関連性と組織体の能力の認識に非常に強い整合性がある。ただし、ＣＡＥグループは、このリスクに関する個人の知識に関して、ステークホルダー・グループよりも大幅に後れを取っている。

個人の知識と組織体の能力
７段階で６または７と評価した割合



リスク段階

「展開」として OnRisk に初登場

引用：

「サステナビリティは、富を保全し、維持し、増やすために絶対に不可欠である。これは、事業への他の投資と同じである。これらの投資は、創出した価値を保全して維持するために行う必要がある。」－金融業、取締役

組織体とリスクとの関連性

７段階で６または７と評価した割合
－社会のサステナビリティ

サプライチェーンの混乱

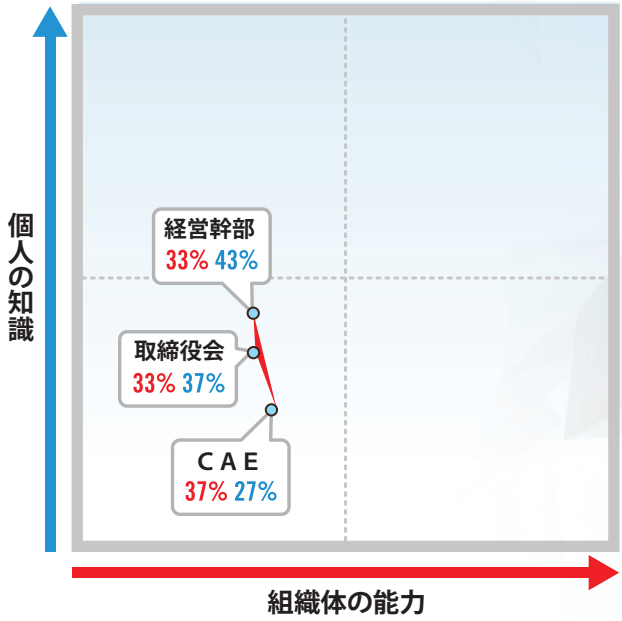
定義：

世界的なパンデミックを原因とする**世界規模での通常業務の混乱**は、組織体の戦略目標の達成を支援するサプライチェーンのレジリエンスの必要性を浮き彫りにした。このリスクでは、組織体が現在および将来のサプライチェーンの混乱に適応する柔軟性を組み込んでいるかを検討している。

分析：

サプライチェーンの混乱のリスク関連性に関しては、取締役と経営幹部の間で**強い認識の整合性があり、**彼らの半数強が組織体にとって非常に関連性の高いリスクであると考えている。ＣＡＥグループは、世界経済においてますます重要になるこのリスクに関する個人の知識で後れを取っている。これは、このリスクを組織体との関連性が高いと考えるＣＡＥが少ない結果かもしれない。

個人の知識と組織体の能力
７段階で６または７と評価した割合



リスク段階

「検討」として OnRisk に初登場

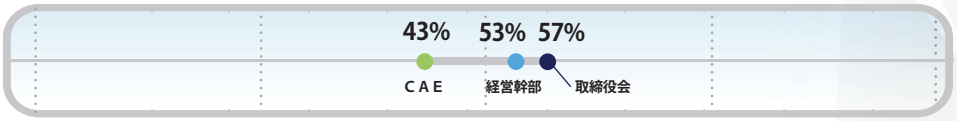
引用：

「国境が閉鎖され、スエズ運河が塞がれるなどのことで、サプライチェーンの問題に対する理解が深めさせられた。」－金融業、ＣＡＥ

「以前はガソリンスタンドに乗り入れた時だけに考えていたものだが、今では多くの業界で重要になっている。」－金融業、取締役

組織体とリスクとの関連性

７段階で６または７と評価した割合
－サプライチェーンの混乱



環境のサステナビリティ

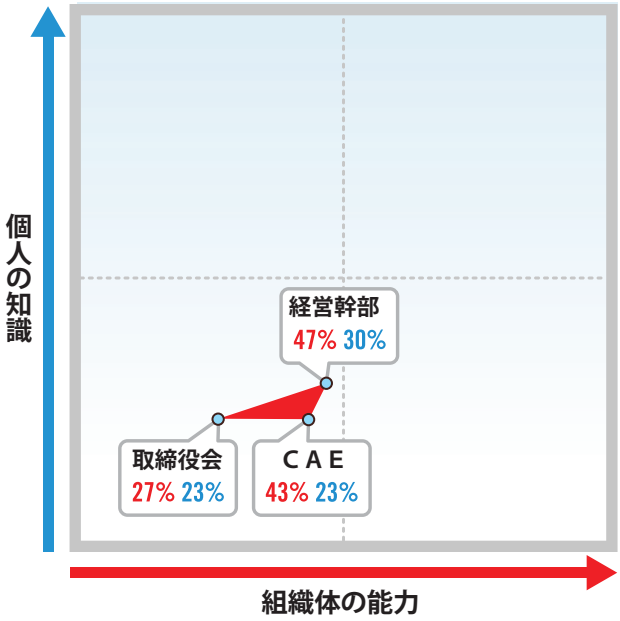
定義：

組織体は、組織体が事業を行う環境に与えている影響を評価して開示するよう求める、株主、規制当局、顧客、および従業員などのステークホルダーからの**圧力の高まりに直面している。**このリスクでは、組織体が環境への影響を確実に測定して評価し、さらに正確に報告する能力を検討している。

分析：

この領域ではかなり強い認識の整合性があるが、この急速に出現するリスクを組織体と非常に関連性があると考えているのは、特に経営幹部では比較的少数である。全グループの個人の知識もかなり低かった。自らの組織体が環境のサステナビリティのリスクを管理する高い能力を持っていると信じている取締役は少ない。

個人の知識と組織体の能力
7段階で6または7と評価した割合



リスク段階

「展開」として OnRisk に初登場

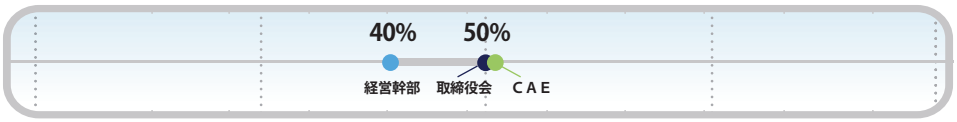
引用：

「すべての組織体にとって測定という問題がある。この領域では測定と報告が標準化されていないため、混乱が生じている。」ーヘルスケア企業、CAE

「大部分の組織体は、環境のサステナビリティについての優れた方針、手続、およびプログラムを持つことを望んでいるが、すべてのリスクに対処する際に、環境のサステナビリティが常に中心になるとは限らない。」ーヘルスケア企業、取締役

組織体とリスクとの関連性

7段階で6または7と評価した割合
ーサプライチェーンの混乱



内部監査人協会（ＩＩＡ）について
内部監査人協会（ＩＩＡ）は、内部監査という専門職の提唱者として、教育者として、さらに基準、ガイダンス、公認資格の提供者として、最も広く認められている。1941 年に創立されたＩＩＡには、現在 170 を超える国と地域に 19 万人を超える会員がいる。ＩＩＡ国際本部の所在地はアメリカ合衆国フロリダ州のレークマリーである。詳細な情報は、www.globaliia.org を参照のこと。

免責事項
ＩＩＡは、この文書を情報提供および教育目的で公表しているのであって、特定の状況に対する決定的な解決策を提供することを意図している訳ではなく、ガイドとして使われることを意図しているだけである。ＩＩＡは、特定の状況に対応する場合は常に、独立した専門家からその状況に直接関係した助言を求めることをお勧めする。ＩＩＡは、このガイダンスのみに依拠した者に対し責任を負うものではない。

著作権

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401 Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org

The Institute of Internal Auditors