



# リスク監視と取締役会： 複雑で進化し続ける領域の考察

2020年12月

取締役会が強固かつ主体的に会社のリスクを監視することは、これまで以上に重要性が増している。

取締役会によるリスク監視の役割は重要である。これにより、非常時と平常時のいずれにおいても、企業と株主に真の価値をもたらすことができる。そのためにはまず、会社の戦略的方向性を理解し、より幅広いステークホルダーの視点を検討し、取締役会に実効的な監視機能を持たせることが求められる。では、あなたの会社の取締役会はどのようにリスク監視アプローチを理解し、実行に移しているのだろうか。

私たちは予測不能なリスクに直面しながら、今という時代を生きている。経済的・社会的に広く影響を及ぼす、世界的なパンデミックのような「ブラックスワン」事象(前例のない未曾有の出来事であり、誰も全く予想しなかったもの)の発生はその象徴ともいえる。会社は、今すぐにでも顕在化しそうなリスクをいつでも予測できるわけではないが、取締役会が強固なリスク監視機能を担うことで、会社がより組織的に、機動性をもってリスクに対処することができる。取締役会が監視するリスクは増加する一方であると同時に、リスクの性質も変化し、相互に関連し合うようになっている。リスクが発生する可能性とその影響度も変化し続けており、リスクの種類によっては、事業の特定の分野にだけ影響を与えるものもあれば、ブランド全体に深刻な影響を与えるものもある。

私たちは絶対に起こらないと高を括っていたような事象を実際に目の当たりにすることで、リスクに対する考え方を広げる必要があることを学んできた。そのためには、より懐疑心を持って将来に備えることが必要である。一般的に、そのための経験値は取締役会の方が経営陣より豊富である。取締役会が戦略計画に沿って、より長期的な目線でリスクを捉えることで、経営陣は日々のリスク管理に専念することができる。

## 戦略とリスクとの関係

大規模な機関投資家は、企業のパーパス(目的)が長期的な戦略と成功にどのように関連付けられているかについて多くの情報を求めている。このように第三者が企業の目的に注目するようになっている中で、会社の目的についての声明文を通じてリスク領域を理解することが取締役会にとって重要となってくる。リスク領域は、企業側の視点だけでなく、株主やその他のステークホルダー(従業員、顧客、サプライヤー、コミュニティ、規制当局など)の視点も踏まえて捉えられるべきである。環境・社会・ガバナンス(ESG)リスクを用いて、このことを説明してみよう。多くの企業において、これらのリスクはすでに認識されている。しかし、大規模な機関投資家が近年ESGリスクに注目し、それに伴って情報開示を求める声が増したことで、これらのリスクがさらに高まってきている。大規模な機関投資家は、ESGリスクが企業の長期的持続可能価値に重大な影響を与えかねないと指摘している。たとえば、ある会社にとっては水が重要な資源であるかもしれない。気候変動により将来水の調達に問題が生じるかもしれないのであれば、最終的には水が企業の長期的持続可能価値に影響を与えるだろう。現代の企業は今や、この種の重要なESGリスクを識別し、それらのリスクをモニタリングおよび監視し、これらの取り組みを株主やその他のステークホルダーに伝えることに一層力を入れている。

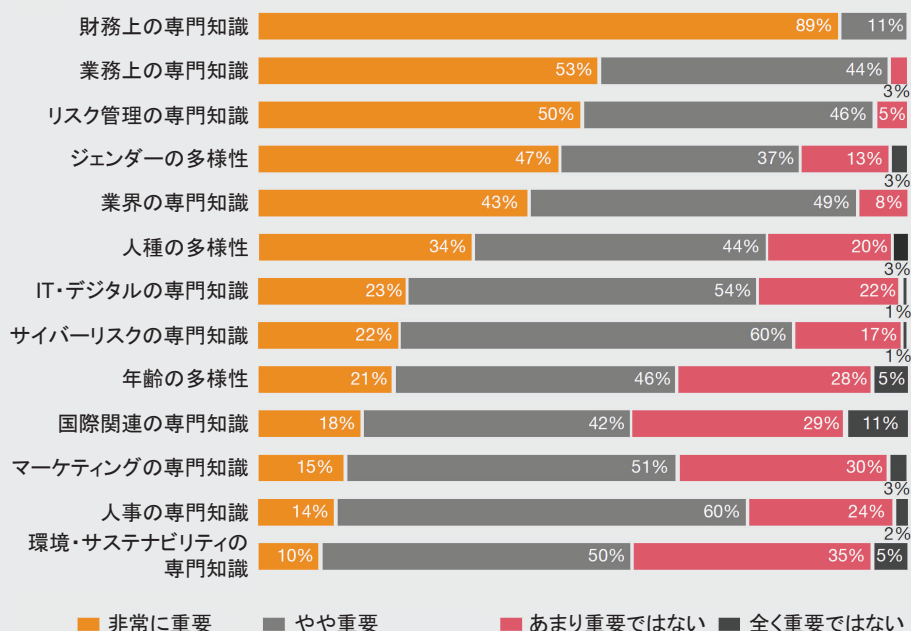
取締役会は、事業上のどの重要リスクが取締役会を含む、いずれの会議体にて積極的に追跡・モニタリングされているかに着目する必要がある。これらの重要リスクをどの会議体で、どのようなタイミングで議論すべきか、という質問に答えることは比較的簡単であるが、取締役会でこれらの重要リスクを実効的に監督する方法を特定することは、困難である。本書では、リスク監視という課題に取締役会がどのように取り組むべきかについて考察する。

# I. 取締役会の構成の多様性

リスク監視の最終的な責任を担うのは、取締役会である。企業が直面しうる幅広いリスクを理解するためには、取締役会に多様なスキル、経歴、経験は不可欠である。例えば、リスク管理の専門知識を有する取締役がいれば、真の価値をもたらすことができるだろう。

## 取締役会の構成・多様性

取締役会にとって、以下のスキル、能力、属性はどの程度重要ですか。



出所: PwC, 2020 Annual Corporate Directors Survey (2020年9月)

取締役会が求める重要なスキルとして、財務上、業務上に次いでリスク管理の専門知識が挙げられている。一方で、環境、社会からガバナンスまで幅広い範囲のリスクをカバーするESGスキルに対する関心は低い。



リスク監視という観点からも、取締役メンバーの経験の多様性は有用である。

業界に関して深い専門知識を持ち、今後の展望について予測することができる取締役の存在は重要である。一方で、リスクを異なった目線でみるための斬新な視点を持つことも重要である。そのためには新任であるかにかかわらず、他の業界の経験または異なったスキルセットを有する取締役の存在が役に立つ。

また、ジェンダーの多様性もリスク監視に良い影響を与えられる可能性がある。実際に、PwC米国による2020年度企業取締役調査に対する回答者の71%が、取締役会におけるジェンダーの多様性が戦略・リスクの監視を改善すると回答している。もしあなたの会社の取締役会における経験や見解の多様性が十分でないとしたら、取締役会のメンバーを刷新したいことだろう。

取締役会のメンバー構成と、取締役会が実効的にリスクを監視するにあたって適切なスキルを有しているかを評価した後に注力すべきことは、会社がどのようにこれらのリスクを識別し、管理しているかを理解することである。

取締役会の多様性が取締役会の監視に影響するか。

71%

の取締役が、取締役会の多様性が戦略とリスクの監視を改善すると述べている。

出所：PwC, 2020 Annual Corporate Directors Survey (2020年9月)





## II. 出発点としてのERM






全社リスクマネジメント(ERM)の位置づけは、人によってさまざまである。会社によっては、自社の価値を保護するため、リスクを識別し、優先順位付けし、報告を行うためにのみERMを利用している。一方、優れた企業は、より良い、そしてより多くの情報に基づく意思決定を行うためにERMを利用し、戦略面、財務面、業務面のパフォーマンスの改善に活用しており、結果として企業価値を高めている。しかし、これを実現するためには、多大な労力と、あらゆる職階の社員からの賛同が必要だ。

### ERMとは？

ERMとは、能力、カルチャー、プロセス、プラクティスの集合体であり、企業が不確実性に直面した際に、より良い意思決定を行うために役に立つ。ERMは従業員がリスクを理解し、識別し、評価し、モニタリングし、管理するのに役立つ枠組みと方針を示し、これにより会社は目的を達成できる。また、ERMは戦略的プランニングと統合されることで最も価値を発揮する。

リスクを評価する、つまり重要なリスクを識別し、優先順位つけることだけが、ERMではない。この時点で会社が作業を中断してしまうと、会社はリスクを把握することができても、それを管理するための積極的な対応を講じることができない。

### 経営者がERMに対する取り組みを改善できるケース

ケース	想定される原因
 戦略に関する議論が好機についてのみで、リスクには触れられていない	<ul style="list-style-type: none"><li>• リスクが戦略策定にあたって不可欠な要素となっていない</li><li>• 経営陣が取締役会にリスクの全体像を示していない</li></ul>
 リスクのリストを提供されただけで、分析が行われておらず、会社の戦略的目的と関連付けられていない	<ul style="list-style-type: none"><li>• 経営陣はERMをコンプライアンスの一環としか捉えていない</li><li>• ERMを単なる年次のリスク自己評価調査としか捉えていない</li></ul>
 財務報告、コンプライアンス、オペレーショナルリスクなど、理解しやすい個別のリスクにだけ焦点が置かれている	<ul style="list-style-type: none"><li>• 経営陣はボトムアップでしかリスクを識別しておらず、戦略と関連付けていない</li><li>• リスク管理にあたって誤ったエリアに着眼しており、また取締役会に正しい情報を報告していない</li></ul>
 ERMは取締役会や上級管理職にとつて、可視性や信頼性に乏しい	<ul style="list-style-type: none"><li>• ERM責任者が、経営幹部から有意義な情報を得たり、賛同を得たりするだけの影響力を有していない</li><li>• CEOがERMを重視していない</li></ul>
 ERMの議論が陳腐化しており、毎年同じリスクを取り扱っている	<ul style="list-style-type: none"><li>• ERMが経営陣に対して、何が変わったのか、そして何が今後の課題となるかを報告していない</li></ul>



認識しているリスクと、精通している事象を検討することは容易である。だが、このためだけにERMを実施するのであれば、会社は好機を逃す可能性が高い。適切な戦略を練り、正しい方向に進むためには、取締役会と上級幹部は、当四半期または当年度以降といった先を見据える必要がある。そうでなければ、ERMと上級管理職が次の「ブラックスワン」事象を予測できる可能性は低い。しかし、ERMが強固であれば、問題を生じさせる技術や、新たな競争相手、環境問題、社会問題、規制、経済、政治情勢の変化などを明らかにすることができる。例えば、年に一度実施されるリスク評価において、戦略的な影響を有する将来のリスクに会社が焦点を当てるのに役立つよう、エマージングリスクも検討の対象とすべきである。

適切に実施されれば、ERMは会社の障害となり得る重要なリスクを識別したうえで、それを必要なステークホルダーに伝達し、適切に管理することができる。しかし、ERMの位置づけや内容は会社によって異なる。では、取締役たちはERMが自社で機能しているかをどのように把握することができるだろうか。

そのためには取締役会の知識に基づいて、ERMプロセスを新たな視点で見直すことが重要である。ERMにより識別されたリスクは、事業固有の戦略的リスクと想定されるものと整合しているだろうか？ERMプロセスは、エマージングリスクを検討しているだろうか？ERMの責任者（多くの場合、最高リスク責任者または最高財務責任者）は、会社を十分に理解し、リスク対応を適切に主導できるだろうか？リスクに対して適切な管理責任者が割り当てられ、軽減計画が策定されているだろうか？

## 経営幹部以外にもERMの浸透を

もしERMが役員主体で運用され、その他の職階がERMを認識していない場合、ERMはすべての社員やスタッフの行動に影響を与えることはできない。実際に、リスクを評価し、対処すべき優先順位を決めるにあたって、さまざまな職階の社員を関与させたいと考えている会社もある。もし会社にとって重要なリスクのいくつかについて、異なるグループの人々に優先順位をつけてもらったとしたら、異なる結果を得ることになるであろう。

取締役会とエグゼクティブチームはリスクの優先順位について同じ見解を持っているかもしれないが、ミドルマネジメント層の優先順位はまったく異なっているかもしれない。リスクの優先順位をどのように付けるかを、経営幹部以外の者から確認することは有用である。そしてこれは同時に2つの効果をもたらす可能性がある。1点目に、ERMプロセスにおいて検出できない、顧客、サプライヤー、その他の従業員のリスクに対する考察を、ミドルマネジメント層を通じて獲得できる。2点目として、エグゼクティブチームがミドルマネジメント層に対して重要なリスクと、それらの軽減に注力する必要性を効果的に教育できていないケースを明らかにできる。いずれの場合であっても、会社がリスク管理に向けてどのように連携しているかを理解するうえで大いに役立つ。

## リスクアペタイト

詳細を十分に理解せずに大きなリスクをとってしまった会社や、倫理的な一線を越えてしまった会社に関する記事を読んだことがある方は多いであろう。一方で、リスクを取ることを躊躇するあまり、業績の向上や成長の機会を逸してしまうケースもある。これらの状況をみて、取締役がこのように悩んでしまうのはもっともである。「成功するために、わが社はどの程度のリスクを取ればよいのだろうか」。

多くの企業では、直観に基づき、リスクテイクを行っている。ほとんどの人は、自分がどのように行動すべきか、どのようなリスクであれば許容できるかについての感覚を持っている。しかし、どのようにすれば上級管理職と取締役会は、リスクを取ることにに関して全社的に同じ考えだ、ということを確認できるのだろうか。そのためには、リスクアペタイトの枠組みを活用することが有用である。経営陣がリスク・アペタイト・ステートメントを明確にすることで、皆が目標を達成する際にどれだけのリスクが許容可能かを把握できるようになる。最高リスク責任者の中には、リスク・アペタイト・ステートメントは策定しても活用できない机上の空論であると考え、その策定を目指す経営陣を手助けすることに消極的な者もいる。しかし、リスク・アペタイト・ステートメントを整備することによって、会社が取るべきリスクの種類と量に関する真の洞察を得ることができるのである。

会社がリスク・アペタイト・ステートメントを整備している場合、それは戦略に適合し、ビジネス上の意思決定に情報を与えるものでなければならない。また、リスク・アペタイト・ステートメントには、定量的情報と定性的情報の両方が含まれていなければならない。取締役会は、リスク・アペタイト・ステートメントを、ERMに基づく監視業務と合わせて毎年検証すべきである。リスク・アペタイト・ステートメントが整備されていない場合、取締役会は少なくとも、会社のリスク許容度と、それが会社のカルチャーにどのように組み込まれているかを理解すべきである。

### リスクの議論において、カルチャーはどのような役割を果たすのだろうか。

カルチャーが非常に優れていれば、カルチャーは会社にとって資産となる。効果的なカルチャーは、明確で一貫性のある倫理観をトップからすべての従業員までもたせ、適切なリスクテイクを促し、透明性を高める。企業の戦略と密接に関連付けられていれば、カルチャーは成功を強力に後押しすることができる。一方、カルチャーが劣悪であると、カルチャーは成功の阻害要因となってしまう。カルチャーが業績の足かせとなり、経営陣が主要な目標を達成することが難しくなり、会社にとって評判や財務面でのリスクとなりがねない。

カルチャーの監視における取締役会の役割については、*Why do boards need to know their company's culture? Hint: to make sure its an asset, not a liability*を参照。

### 優れたリスク・アペタイト・ステートメントとは？

優れたリスク・アペタイト・ステートメントは健全なカルチャーを推進し、意思決定に役立つであろう。それは会社にとって、どれだけの不確実性が許容されるかを把握するための指針となる。また、それは戦略上、業務上の目的を達成するためにどれだけのリスクをとるべきか、その境界を設定する（境界はリスクの種類によっても異なる）。実際に、目標を達成するためにどれだけのリスクが必要か（下限）と、どれだけリスクなら許容できるか（上限）を伝えるために、いくつかの文章にして示す必要があるかもしれない。これによって、リスクテイクの透明性が高められる。

例えば、COSO が 2017 年に公表した *Enterprise Risk Management – Aligning Risk with Strategy and Performance* の *Defining Risk Appetite* のセクションを参照。



## 効果的なリスク機能を支える主要な要素

- **共通のリスク言語**: 共通のリスク定義および標準的なカテゴリが設定されていれば、事業間のリスク情報を適切に関連付けやすくなり、不整合や相互依存性を特定しやすくなる。
- **共通のリスク評価アプローチ**: 単一の評価基準に基づくリスク評価アプローチは、企業が直面するさまざまなリスクについて、異なるチームの視点を共有、比較、組み合わせることを容易にする。
- **統制に対する合理化されたアプローチ**: 多くの企業はさまざまなリスクに長年対処してきたため、統制が非効率的で、重複する結果となっている。
- **内部統制を見直し、簡素化し、これらのプロセスを合理化することで、有効性を損なうことなく、パフォーマンスを向上させることができる。**
- **機能横断的な連携**: リスク管理に貢献する全ての機能に対して、より優れた方法で、より適切に情報が共有されることによって、プロセスを改善することができる。
- **リスク・オフィサーによる一元的管理**: 最高リスク責任者または同等の役員が全社的なリスク管理の取り組みを支えると同時に、経営幹部と取締役会の双方に対するリスク報告を仕切ることができる。





## リスク報告

多くの企業において、リスク管理はサイロ化され、マニュアルに依存している場合が多い。そのため、取締役会へのリスク報告は会社の異なる部門が異なる頻度、異なる形式で、異なるエリアにフォーカスして行ってしまうがちだ。また、企業の各部署が、異なるシステムと異なるリスクと統制の定義を用いて、異なる種類のデータを報告している場合があり、このようなばらばらのアプローチが効率性を一層悪化させている。

会社によっては、さまざまなリスク管理グループから提供された情報に基づき、包括的なリスク報告書を作成している。しかし、そのようなアプローチは別の課題を生じさせ、またそのプロセス自体が非効率となりうる。そこで、リスク報告プロセスを統合するために、GRC(ガバナンス、リスク、コンプライアンス)テクノロジープラットフォームを活用する会社が増えてきている。

取締役会は、リスク監督責任を効果的に果たすため、報告のあり方を決める必要がある。

少なくとも取締役会は、重要なリスクを識別し、追跡した結果の報告を受け、その重大なリスクを削減する計画にふさわしい責任者を任命すべきである。重要なリスクの動向を追跡するためには、取締役会が追跡・監視できる重要リスク指標(KRI)をリスクごとに明示すべきである。

KRIは早期警告の兆候として機能し、取締役にとって特に有用である。リスクが危険な状況になるかどうかを経営陣がどのように確認しているか、取締役会はこれらの指標からうかがい知ることができる。ただ、KRIは将来を予測するものではない。不測の事態を最小限に抑えるために、経営陣は、重要なリスクの影響または発生可能性の変化をKRIによってモニタリングし、対応を講じる。たとえば、国内総生産の減少や失業率の上昇は、小売業者にとっては、ホリデーシーズンの売上が予測ほど堅調ではなく、棚卸資産や人員を削減する時期になるかもしれないというシグナルとなる。最終的には実効的なリスク管理によって狙い通りのパフォーマンスが推進されるため、KRIは重要な業績指標(KPI)と密接に関連付けられているべきである。

企業に高度なERMプロセスが整備されていなくても、取締役会が経営陣とリスク環境がどうなっているのか、何が起きているのか、どのような動きがみられるのか、何が新たに生じているのかについて定期的に話し合うことは、重要なリスクを監督する上で役に立つだろう。

リスクを管理するために必要なデータを会社は入手できているか。

PwCの2020年度グローバルリスク調査の参加者のうち、

# 50%

が、会社は現在既存のリスクおよび新たなリスクを予測し、管理するための適切なデータを保有していると回答している。

# 33%

が、会社にはそれを実現するための適切なテクノロジーおよびツールがあると回答している。

出所: PwC "Three actions to bolster your organization's risk insights" (2020年2月)

### III. 取締役会による透明性の確保

**取締役会はどのようにすれば、投資家やその他のステークホルダーに対し、リスクを実効的に監視していることを納得させることができるのだろうか。**

2010年以降、一般の事業会社は、リスク監視における取締役会の役割をプロキシースタートメントにおいて開示することが義務づけられている。しかし、これまで、企業の多くは詳細をほとんど開示していない。取締役会はしばしば単に「取締役会はリスクを監督する全般的な責任を負う」「監査委員会は財務関連リスクを監督する」「ガバナンス委員会はガバナンス関連リスクを監督する」「報酬委員会は報酬関連リスクを監督する」と示しているだけである。このような基本的事項の開示だけでは、問題となるリスクを取締役会が積極的に監視している、と株主を納得させることはできない。

最近、株主たちは取締役会のリスク監視活動とその実績に関して、より有意義で透明性の高い情報の開示を求めるようになってきている。特に、主要な投資家は、長期的持続可能価値を提供できるかどうかに影響を及ぼしうる気候変動リスクや社会リスクに対し、企業がどのように取り組んでいるかを理解したがっている。行動を促すため、取締役の投票方針の変更を公表した投資家もある。企業がこれらのリスクに対して適切に向き合わず、関連する指標を公表しない場合には、影響力のある株主が取締役に対して反対票を投じる可能性もある。

規制当局もまた、より多くのリスク監視情報の開示を求めるようになってきている。2018年、SECは、サイバーセキュリティリスクとインシデントに関する開示について重点的に取り扱った解釈指針を公表した。当指針では、提出書類の中でサイバーセキュリティに関する事項の開示について適切なセクションを特定している。また、サイバーリスクの管理を監督する上での取締役会の役割を含め、それが事業にとって重要である場合に開示を検討すべき内容を例示している。

このように投資家や規制当局によるリスク監視への注目が高まっていることを受け、今や多くの企業がより具体的な内容となるよう開示を充実させている。



## 適切なリスク監視の開示内容

十分に策定されたプロキシステートメントには、以下に掲げるリスク監視に関する情報が含まれている。

- 取締役会が関与しているかどうか
- 取締役会が会社のリスク管理機能をどのように確認しているかに関する記述
- 取締役会が重要かつ新たなリスクのトピックに焦点を当てていることを示す内容
- 各委員会が重点的に取り組む重要なリスク分野の詳細なリストを含め、委員会によるリスク監視機能の分担に対する取締役会のアプローチ
- 取締役会または委員会への報告の内容・頻度
- リスク監視に関する上級管理職の役割と、リスク管理委員会のメンバーおよび責任についての記述
- サイバーセキュリティ監視に関する具体的な内容。具体的には、サイバーセキュリティが取締役会の議題として提議された回数、取締役会に更新内容を報告した取締役の記述（例：CIO、CISO、CRO）、外部の専門家からの見解を聞いたかどうか、CIOまたはCISOとのプライベートセッションを開催したかどうかなどの記述
- 目的、目標を含む、ESGリスク監視に関する具体的な内容



## 総括

複雑化し、相互の関連性が強まっているビジネスリスク環境において、リスクを監視し、株主に継続的に情報を提供していく上で取締役会は重要な役割を果たしている。まず、取締役会は役員の構成を確認することから開始すべきだ。例えば、リスクについて異なる視点をもたらすような、経験、思考、性別、人種の多様性の存在を検討する。また、自社のERM体制を理解し、ERM体制がリスク監視にどのように貢献できるかを理解することが取締役会にとって重要である。取締役会は、会社固有の監視体制に対して時間を費やさなければならない。別のリスク委員会の設置を検討することも考えられる。さらに、会社にはさまざまなステークホルダーが存在することも忘れてはならない。会社のリスク管理態勢および業務についてどのような情報がステークホルダーに提供されているか把握すべきである。リスク監視に対するアプローチを見直し、精緻化することによって、取締役会は会社と株主に対してより高い価値を提供することができるのである。



# 問い合わせ先

PwCあらた有限責任監査法人

パートナー

**辻田 弘志**

hiroshi.tsujita@pwc.com

パートナー

**小林 昭夫**

akio.kobayashi@pwc.com

パートナー

**出口 真也**

shinya.deguchi@pwc.com

パートナー

**高木 和人**

kazuto.takagi@pwc.com

パートナー

**久禮 由敬**

yoshiyuki.kure@pwc.com

ディレクター

**手塚 大輔**

daisuke.tezuka@pwc.com

マネージャー

**坂上 竜太**

ryuta.sakaue@pwc.com



© 2021 PwC. All rights reserved.

PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.