取締役会はリスクと如何に向き合うべきか
―リスクオーバーサイトと、攻めと守りのERMの視点から―

神林　比洋雄

【キーワード】　ERM（全社的リスクマネジメント）、リスクオーバーサイト、コーポレートガバナンス、内部統制、カルチャー

はじめに

長期間、低迷を続ける日本経済を更なる成長軌道に乗せるべく、いっそうのリスクテイクの促進を目的として、2015年6月、我が国のコーポレートガバナンス・コードが公表され、「実効的なコーポレートガバナンスの実現に資する」73原則が提示された。その原則がどのように実践されているか、2017年3月に東京証券取引所より公表された「コーポレートガバナンス白書2017」では、「多くの上場会社や、上場会社と建設的な対話を行う投資家において、ガバナンス改革を形式から実質へと深化させていくための真摯な取り組みがなされている」としている。また、新たに導入され、注目を集める「コンプライ・オア・エクスプレイン」、いわゆる自主的な取り組みの概況も整理されている。そこでは「全73原則をすべて実施している会社は19.9%」で、「64.8%の会社が全原則のうち90%以上を実施」としており、相応にコーポレートガバナンス・コードに対応しようとする企業の姿勢がうかがえる。ただ、まだ期待される実効性が十分には伴っていないのではという声も数多く耳にする。

一方で、日本企業の信頼性を大きく損ないかねない不祥事が後を絶たない。企業価値創造に向けて果敢に攻めるリスクテイクと、企業価値の維持を支えるリスクマネジメント、これらリスクに係る攻めと守り双方のバランスを如何に図るかがあらためて問われている。

長期的な企業価値を生み出すことを目的にする経営執行陣の経営活動が適切かどうか、その方向性を見極め、的確な助言と監視を行うガバナンス機能の実質的な強化をめざし、会社法、金商法などのハードロー、東証のコーポレートガバナンス・コードなどのソフトローの両面からの整備も進んでいる。しかし、企業はそれぞれ、異なる生い立ちや、特色のあるビジネスモデル、多様なステークホルダーの存在など、その在り様は一律ではなく、すべての企業にフィットする経営管理や、リスクマネジメントにおいて一律の仕組みは存在しない。そこで、企業価値向上を目指すうえで、経営執行陣および取締役会がどのようにリスクに対

処し、未来に向けてどう立ち向かっていくべきか、経営執行陣が目指すべきリスクマネジメント、および、取締役会がガバニングボディとして果たすべきリスクオーバーサイト（リスク監視）の在り方について考察を試みる。

ここで、リスクオーバーサイトとは、ガバナンス機能の一環としてリスクマネジメントにおいて果たすべき役割であると定義する。従ってリスクオーバーサイトの中心的な担い手としてのガバニングボディは一般に取締役会とされる。我が国のガバナンス構造では監査役会・監査役も含まれる。リスクオーバーサイトの対象となる経営執行陣が推進する全社的リスクマネジメントについては以下の定義をベースとする。

- 企業は経営理念の実現のために、機会と脅威を慎重に見極めつつ、経営資源の最適な有効活用を基盤とする中長期経営方針を策定し、単年度計画に落とし込む。
- 経営理念を実現するために策定された戦略・事業目標の達成に影響を与える不確実性（リスク）を特定・優先順位付けする。
- 重要なリスクの源泉に焦点を当て、必要な権限委譲、役割分担を明確にし、必要にして十分な内部統制を整備運用する。
- 自主点検と独立第三者による評価（モニタリング）を通して、企業価値向上の観点からリスクマネジメントの有効性の確認と改善提案を行う。
- 事業環境の変化に応じて継続的な改善を適宜実施する。

リスクオーバーサイトとは、これらの全社的リスクマネジメントのPDCAのプロセスがしっかりと実践できているかどうかを判断することである。つまり、経営理念のもと、中長期的観点から企業が取るべきリスクを取っているか、取ってはならないリスクを取っていないか、受け入れたリスク相応のリターンを確保すべく企業の経営力が相応の対応能力を有しているか、継続的なモニタリングを行い、軌道修正が適時・的確になされているかを判断し、企業の成長を支援することである。

本稿では、リスクオーバーサイト並びにリスクマネジメントのプロセスの両面から、我が国企業の課題と対策について検討する。

1　企業を取り巻く不確実性（リスク）とは

AIやロボティックスがもたらすパラダイムシフトなど、世界規模で急速に増大する不確実性の中においても、企業が持続的に成長・発展を遂げるためには、リスクを許容し成長に向けた投資を行う（リスクテイク）とともに、将来発生するであろう損失を阻止、あるいは許容できるレベルまで軽減しなければならい。経営陣が素早く次の一手を打ち出すためには、企業が潜在的に抱えている、あるいは抱えるであろうリスク（不確実性＝機会と脅威）への適時適切な把握・対応を行い、その状況が適時に報告され、ダッシュボードなどで“見える

化”される必要がある。このようなリスクマネジメントの仕組みをしっかりと構築していくことは、激変する環境の中での経営課題としてその重みが今まで以上に増している。

では、そもそもリスクとは何か、リスクにはさまざまな見方や考え方があり、リスクが語られる時、何を意味しているかよく理解したうえでコミュニケーションを進める必要がある。語源としては、ラテン語のRisicareといわれるが、その意味は、勇気をもって試みる、あるいは挑むということで、とかく一般に言われる脅威や負のイメージとは異なる。それはもっと前向きで積極的な意味合いがあったようである。語源として、地中海交易で嵐の中に船を漕ぎ出すという勇気をもって試みるところからきているとのことだが、ちなみに同じ頃、日本においても、紀伊國屋文左衛門が嵐の中、ミカンを和歌山から江戸に船で運んだという話もあり、勇気をもって試みるというリスクテイクは古今東西、共通の概念であろう。

現代では、リスクは、ⅰ）自然災害などのリスクの発現による損害をベースにした結果からみた分類で、いわゆる怖いもの、ⅱ）外部および内部要因からみたリスクの源泉に焦点を当てた分類で、事前の適切な対応を図るもの、ⅲ）「報われるリスク」（投下した経営資源より成果の方が大きくなるリスク）と「報われないリスク」（いかに努力してもコストや損失のみが発生するリスク）で、リスクマネジメントの成果に焦点を当てるもの、などの視点から分類される。

例えば、会社法に規定される「損失の危険」や、金商法に規定される「財務報告に係る虚偽記載リスク」は、本来自律的に取組むべき課題であるが、リスクに対する内部統制の在り方が法制化されたことから、内部統制を他律的なものと捉えることで“やらされ感”が強く、さらにできて当たり前、やって当然という感覚もあり、その意味でも「報われないリスク」に入る。一方、経営戦略策定や企業買収などにおける事業上の意思決定に係るリスクはまさにしっかり対応すれば、コストを上回る成果が期待できる「報われるリスク」となる。ただ、やりようによっては、手痛い失敗を招きかねず、「報われるリスク」とするにしても、相応の覚悟と知恵をもって対処しなければならない。

現代においては、リスクとは怖いもので「報われないリスク」との従来からよくある“思い込み”にとらわれることなく、「報われるリスク」にも焦点をあて、リスクマネジメントが単なるコストドライバーではなく、戦略達成に貢献する強力で頼もしいバリュードライバーであることに注目したいものである。

コーポレートガバナンス・コードでは、リスクに関連する分野として、取締役会の役割として、「*経営陣幹部による適切なリスクテイクを支える環境整備を行うこと、独立した客観的な立場から、経営陣・取締役に対する実効性の高い監督を行うこと*」としている（基本原則4）。さらに「*取締役会は、内部統制やリスク管理体制を適切に整備すべきである。*」とし（原則4－3（3））、また、「*コンプライアンスや財務報告に係る内部統制や先を見越したリスクマネジメント体制の整備は、適切なリスクテイクの裏付けとなり得るものであるが、取締*

役会は、これらの体制の適切な構築や、その運用が有効に行われているか否かの監督に重点を置くべきであり、個別の業務執行に係るコンプライアンスの審査に終始すべきではない」としている（補充原則４－３②）。

つまり、コーポレートガバナンス・コードでは、リスクテイクを支える環境整備、独立した立場からの経営陣・取締役に対する実効性の高い監督、内部統制やリスク管理体制の適切な整備とその運用の有効性の監督を取締役会の役割としている。まさにリスクオーバーサイトの在り方を示しているのである。また、コンプライアンスや財務報告リスクにも言及し「報われないリスク」を対象にしている一方で、「リスクテイクを支える環境整備」、「先を見越したリスク管理体制」で示されるリスクには「報われるリスク」の意味合いが強く感じられるのである。

リスクテイクで示されるリスクとは、一般にはリスクを積極的に受け容れ、相応の成果を目指す意味で使われ、リスクマネジメントで言われるリスクは、どちらかと言えば、災害やセキュリティ、コンプライアンス等に係るリスクで損失を回避または軽減するという意味で使われており、この二つのリスクの意味合いには大きなギャップがある。リスクマネジメントを前者のリスクの意味でも使い、アップサイド、ダウンサイド双方のリスクを対象にした、いわゆる全社的リスクマネジメント（ERM）を導入している企業は日本ではまだまだ２割程度と言われている（「リスクマネジメント動向調査」東京海上日動リスクコンサルティング、2016年）。コーポレートガバナンス・コードでは、リスクは両方の意味で使われていることになるが、リスクの意味するところは、その定義、範囲や管理目的は、企業によって、組織によって、人によってまちまちである。リスクを語るときにはその定義を明確にしていくことが望まれる。定義が異なる環境では、同じ土俵で相撲を取ることができず、組織の内外において適切なコミュニケーションを行うことが極めて困難となりかねない。

ノーリスク、ノーリターンとよく言われる。また、テイクチャンスとテイクリスクは英語では同義であると学んだ。“失敗は成功の母”、“諸刃の剣”（一方では非常に役立つが、他方では大きな損害をもたらす危険もあるというたとえ）、“禍を転じて福と為す”、“先憂後楽”など、多くの故事が物事の両面を鋭く突いている。リスクという見えないものも、怖いものだけではなく、楽しく幸せなものでもあるという両面を意識した取り組みをすべきである。その意味で、事業とはリスクそのものであり、企業価値を創造し、維持していくには、リスクの定義は、幅広く捉え、「報われるリスク」と「報われないリスク」双方を意識した取り組みが不可欠となる。そのような取り組みを支援する全社的リスクマネジメント（*Enterprise Risk Management：ERM*）が今、あらためて注目を集めている。

積極的なM&Aを通して、今や、売上の７～８割を海外で稼ぎ出す日本企業が、遠心力を効かせた経営管理だけではなく、本社の求心力を高め、真のグローバル企業として競争優位を確保しながら持続的成長を図るには、遠心力と求心力のリバランシングが必要である。異

なる文化を効果的に融合するには、グローバルな価値形成を展開する必要がある。そのためには、激変する事業環境において、リスクという機会と脅威に関して、衆知を集めて、グローバル企業が組織全体を通じて共通言語を再構築するか、強化するか、高度化することが鍵となる。事業の成功を目指して、企業理念とその実現に係る機会と脅威について、如何に共通言語を共有するかであり、ここにあらためて全社的リスクマネジメントを検討する価値があるのである。

2　不確実性（リスク）の高まりに関する調査

では、近時において、いかに不確実性（リスク）が高まりを見せているか、さらにそのような環境でリスクをどのように定義しているか、いくつかのリスクの調査報告・リスクの開示情報を見てみよう。

2.1　ダボス会議のリスクレポート

世界経済フォーラム年次総会（ダボス会議、2017年1月）で報告されたグローバルリスクには、5つの分野（経済、環境、地政学、社会、テクノロジ）から構成され、ここではリスクは、今後10年間で発生し、多くの国・産業に重大な悪影響を及ぼす可能性のある不確実な事象とされている。上位リスクとしては、異常気象、自然災害、大規模難民、テロ、サイバー攻撃、水資源危機などであり、直近の10年の傾向では、環境、社会やテクノロジのリスクが、より重要となると評価が変わってきており、ESGやロボティックスやAIへの関心の高まりを示している。ここでは、リスクが悪影響を及ぼすものと定義されていることもあり、これらは企業の視点からは「報われないリスク」が多い印象であるが、一方で、AI、バイオ、ブロックチェーンなどの新たなテクノロジにより、旧来のバリューチェーンを創造的に破壊しかねず、この変化に対応できない企業は現在の競争優位性を瞬時に失うことになると警告している。企業にとっては、変化を「報われるリスク」として、いかに全社的に組織として取り組むかが試されることになるものと思われる。

2.2　源泉系のリスク調査

次に、ノースキャロライナ州立大学（ERMイニシアティブ）とプロティビティが、企業が直面するマクロ経済、戦略および業務リスクに関して、700名を超える上級経営者と取締役（55%が米国、45%がEUおよびアジア）を対象とした年次調査（2016年秋）を見てみよう。経営陣が最も気に掛けるリスクは次の通りである。これはリスクの源泉に焦点を当てた源泉系のリスクモデルをベースにしている。源泉系リスクのポイントは、何を源泉として、何が原因で、リスクが発生するのかに焦点を当て、リスクの発現を根本から断ち切るなり、発生の影響を経営陣が示す許容範囲に収めることを目的とするものである。なお、かっこ内

は前年順位、下線はリスクの源泉（外部・内部：戦略、ガバナンス、業務）、さらに、報われる・報われないリスクの区分を示している。

① 市場の動向が、成長の機会を著しく妨げる（2位、外部、報われる）
② 法規制の変更ならびに規制当局の監視が、事業モデルへの影響を高める（1位、外部、報われない）
③ サイバー攻撃の脅威を管理する準備が十分にできていない（3位、外部、報われない）
④ ビジネスモデルを大幅に変更しなければ、破壊的な技術革新や新規テクノロジの急激な進展が競争力やリスクマネジメント能力を上回る（6位、内部・戦略、報われる）
⑤ 情報セキュリティの保護に、かなりの資源投入を必要とする（5位、内部・業務、報われる）
⑥ 後継者や有能な人材の確保が事業目的の達成を制限する（4位、内部・戦略、報われる）
⑦ グローバルな金融市場で想定されるボラティリティが、重大な課題となる（8位、外部、報われない）
⑧ 組織の文化が、戦略達成に著しく影響を与えかねないリスクについて、適時の識別や報告を促進するものではない可能性がある（9位、内部・ガバナンス、報われる）
⑨ 変化に対する抵抗が、必要な調整の妨げとなる（7位、内部・ガバナンス、報われる）
⑩ 顧客のロイヤルティの保持が、嗜好変化や地理的移動により難しくなりつつある（10位、内部・業務、報われる）

このトップ10リスクでは、リスクの源泉からみると、4つの外部リスクに対し、6つの内部リスク（戦略リスク2、ガバナンスリスク2、業務リスク2）であり、また、7つの「報われるリスク」に対して、「報われないリスク」が3つとなっている。外部よりは内部に起因するリスク、さらに、「報われないリスク」より「報われるリスク」への関心が高い結果となっている。これは“外”の変化に“内”がどのように対処するか、戦略、ガバナンス、業務に係る「報われるリスク」への経営者の意識が世界的に高いことを物語っている。

2.3　我が国有価証券報告書における事業等リスク

最後に、日本の上場企業において、2004年3月より義務化された事業等リスクであるが、これは、「投資者の判断に重要な影響を及ぼす可能性のあるリスク」を、具体的に分かりやすく、かつ簡潔に開示することとされている。日本の主要産業の一角を占める電気機器業種、製薬業、商社について、東証一部上場企業77社を対象として、2016年3月期における有価証券報告書を分析したところ、外部リスクは47%、内部リスクは53%（業務プロセスリスク45%、戦略リスク7%、ガバナンスリスク1%）という結果であり、2.2の源泉系のリスク調査結果と拮抗している。また、環境や自然災害、法令対応、情報セキュリティなどの「報

われないリスク」を中心とする記載が大半を占める一方で、製品開発、品質、投資効率などの「報われるリスク」の記載も注目されるところである。

ただ、事業環境の変化に係る戦略の改訂やビジネスモデルの見直しなどの戦略リスクや、取締役会の実効性など、ガバナンスリスクなどの記載は極めて限定的であり、コーポレートガバナンス・コードが期待する「リスクテイクを支える環境整備」に係る組織内部におけるリスクの開示はほとんど皆無であった。多くのステークホルダーが高い関心を寄せている機会と脅威につながる不確実性（リスク）と戦略との関連を理解することはほとんど不可能であった。これらの限定的な開示に留まるリスクはすべて「報われるリスク」である。

以上から読み取れることは、我が国企業では、リスクの定義が、「報われないリスク」に偏っているのではないか、戦略・事業目標の達成にプラスにもマイナスにも影響を与える不確実な事象がリスクであるという認識が普及していないのではないか、さらにガバナンスがリスクマネジメントにどのように好影響を及ぼすのかというリスクオーバーサイトへの期待についても、まだ共通認識が醸成されていないのではないか、ということになろう。実際には、プラス・マイナスのリスクを検討しながら経営は行われているのは当然ではあり、開示の良し悪しを問うのではなく、リスクの定義が企業それぞれにおいて限定的であるがゆえにその範囲での開示になっていると解するべきであろう。ただ、現時点での開示状況に対するステークホルダーにとっての満足感は低いとみるべきであろう。

2.4　期待されるリスクの定義の見直し

グローバルに展開するいくつかの我が国の大手製造業においては、最近、「報われないリスク」に加えて、「報われるリスク」も全面的にリスクと認識し始めている。さらに従来は、各事業、機能毎にリスクマネジメントの仕組みを持ち、相互に連携はなかったものの、横ぐしで、リスクの定義の共通化を図り、全社的なリスクマネジメントを推進している企業がわずかであるが徐々に増えつつある。例えば、最近、大規模で戦略的なM&Aを行い、買収した相手にお手並み拝見という遠心力を効かせる日本的な対応の限界が露呈してきている企業において、求心力を高めるため、市場ガバナンスへの対応のみならず、組織ガバナンス、いわゆるグループ組織内の統制力を強化しようとする動きが顕著になってきている。リスクの共通言語化をグローバルに展開し始めているのである。これは、大変注目に値する動きである。機会と脅威に関する共通言語を、グローバル組織全体で共有することができれば、どれだけ経営効率を上げることができるであろうか。導入企業では、期待以上の成果を上げているとの声をよく聞く。

従来、我が国企業では、全体としては一つの組織であるものの、事業部制を中心としてさまざまな機能が、事業部ごと、あるいは国や地域ごと、あるいは職能ごとに、間接機能を持つやり方が多く、この間接機能のサイロ的な活動はリスクマネジメントにおいても例外では

ない。古来、日本の文化は縦の文化と言われる。自然豊かな環境で、雨は天から縦に降り、水は山から里へ縦に流れる。横に降るとそれは台風であり、横に流れるとそれは氾濫であり津波ともなる。横縞より縦縞模様が好まれ、槍は縦に突くもので、第三者が介入する横槍は嫌われてきた。ただ一方で、横糸のない縦糸だけでは衣が完成しないように、ムラの掟は全員が同意するまで、さまざまな根回しが行われ、納得感のある結論にムラの住人はついてきた。組織の合意形成は、本来は日本のお家芸であって、稟議制度にその名残がみられる。この合意形成は、守るべきのムラの掟に対する共通理解があったからこそ可能となったのである。

いい製品、売れる製品を扱う事業部が力を持つのは当然の流れであるが、異なる製品やサービスを取り入れる事業多角化の時代においても、共通の間接機能を、全体の間接機能をとりまとめる部門に任せず、事業部で間接機能を持ち続けた結果、専門性の欠如や、組織全体としての整合性や方針が明確にならず、経営効率を妨げてきた背景がある。最近の不祥事の特徴は、事業部が強すぎ、間接機能が対応すべき決算においても悪影響を与えたとする第三者委員会報告が目立つ。いわゆる縦の論理で、横槍を入れられることを嫌う日本人の特質が裏目に出たものではないだろうか。

リスクマネジメントにおいても、強い事業部と遠心力は横の連帯を妨げ、ユニットそれぞれのリスクの定義を持ち、一般的に「報われないリスク」に焦点を当て、個別リスク管理を進めてきた経緯がある。個別最適は、必ずしも全体最適にはつながらず、競争優位の観点からも、経営の効率の観点からも、投資家への説明責任の観点からも許容されるものではなくなってきている。全社的なリスクの認識が強く要請される背景がここにある。

では、次にそのようなリスクがいかに洗い出され、優先順位を付け、どのような体制で管理し、評価され、見直しがされるべきかを検討する。

3　リスクマネジメントの現状と対策

日本企業によくあるリスクマネジメントにおける課題は、リスクの定義が限定的であり、リスクマネジメントの成果が経営者の重要な意思決定に反映されず、また、全社横断的な視点が欠如していることから、海外拠点を含むグループ全体としてのリスクマネジメント状況が不明瞭である。これらに不安や不満を抱き始めた経営者が増えてきている。これらの懸念に対処するには以下の進め方が有効である。

3.1　企業のミッション、ビジョン、コアバリューを再認識する

経営において最も大事なことは企業理念であり、存在意義である。ミッション、ビジョン、コアバリューで示される企業の価値観であり、社風であり、企業文化、倫理感である。

戦略および事業目標は、企業理念から通常導き出される。理念を実現するものが戦略である。企業理念を表す、ミッション、ビジョン、コアバリューを再認識する中で、戦略を持った瞬間に、戦略を達成できるかどうかという不確実性＝リスクが発現する。戦略策定においてもリスクはしっかりと見据えているが、いったん戦略が確定するとあらためてその戦略が持つリスクをしっかりと見極める必要がある。このリスクの発現を、経営陣の許容度の範囲に収まるように設計するのが内部統制である。内部統制は、ここではもはや、JSOXだけでもなく、会社法の内部統制システムだけでもなく、理念の実現を支える極めて重要で幅広い仕組みなのである。

このように経営を、理念、戦略、リスク、内部統制の枠組みで考えると、不変の理念に、戦略は内外の動きに合わせて変える。変化する戦略にリスクも変化するし、内部統制も変化する。問題は何を変えればいいか、どこまで変えればいいか、いつ変えればいいか、さらにこれらは何をもって判断するかである。そもそも戦略が理念を支えるかどうかも、常に見直しが必要であり、これらの問いに答える情報をどう生成し、収集し、いつ経営陣に提供するかが問題となる。テクノロジを駆使し、質の高い情報収集が今後一層期待されるところであるが、最後は、いかなる場合も経営陣の覚悟と決断を仰ぐことになることは不変である。

3.2　リスクプロファイルを把握する

リスクプロファイルとは、企業が推進する事業環境におけるリスクの特性、特徴のことである。外部環境としては、安定的な事業なのか、常に技術革新が要求される業界なのか、競合関係が厳しい状況なのか、規制が厳しい業界なのか、あるいは、内部的には、グローバリゼーションが進んでいる企業なのか、新興企業なのか、人材は十分に育ってきているのかなどにより、リスクプロファイル、つまり、その事業の中長期経営計画に達成に与える影響の大きさ、複雑さ等が変わってくる。時系列的にも、過去の業績がどうであり、その延長線上での成功への確実性がどの程度、見極められるのか、あるいは最近のロボティックスやAIを駆使するなど全く新たな環境で攻めていかなければならない状況なのかも検討が必要であろう。さらに、地政学的な問題、カントリーリスクなども視野に入れて、さまざまな手法を駆使して、リスクプロファイルを明らかにする必要がある。

3.3　リスクの定義を見直す

望ましい姿としては、リスクの定義を、現時点のリスクプロファイルの中で、短期・中長期的視点から、戦略と事業目標に影響を与える不確実性または可能性とし、自然災害等の「報われないリスク」のみならず、戦略に係る分野をリスクの範囲として取り込むことにより、「報われるリスク」を対象に加え、従来の定義を見直し、拡大することが重要である。

戦略は選択の問題である。選択には情報が必要である。しかも品質が高く、タイムリーな

情報が経営陣に提供されてはじめて的確な意思決定が可能となる。どのようなリスクを取るかは、経営陣の強い思いと情報が決め手になる。戦略における種々の可能性や不確実性の検討において、決め手となるべき情報をいち早く把握した企業が勝ち残れるとすれば、戦略における不確実性をリスクマネジメントの枠組みで捉え直すということは新たな視点を経営陣に提供することになる。企業価値を創造し、維持していく過程で、経営陣の的確な意思決定を支える上で、最も相応しいリスクの定義は、「戦略および事業目標の達成に影響を与える可能性」とすることであろう。

3.4　リスクの識別および優先順位づけはトップ率先で関連情報を有する人が実施する

リスクを洗い出し、重要度を判断する人はそのリスクに関連する情報を最も多く持っている人が行うべきである。となれば、もっとも相応しい人は経営陣であり、続いて現場に精通した事業ユニットの責任者、さらに組織横断的に情報を有しているコーポレート機能のメンバーであろう。それぞれの立場で識別するリスクが異なることがよくあるが、それは良し悪しの問題ではなく、持っている情報が異なるからであり、この情報ギャップをいかに埋めるかが良質なリスクマネジメントの鍵となる。

そこで、組織内の合意形成というプロセスが大変重要となり、リスクマネジメントとは合意形成プロセスといっても過言ではない。それは異なる情報を共有することで、お互いの状況や背景をより理解する中で、それぞれのリスクの重要性に関する理解が深まり、組織全体として最適な判断が可能になるからである。

この調整役として近年、ファシリテーターという役割が注目を集めているが、適切なプロセスを経て合意された内容は、当初はコンフリクトがある社員同士（典型例としては、販売と製造の間での“作るのが下手だから優秀な営業マンでも売れない”、“いいモノを作っても売り方が下手だから売れない”）であってもいったん何が最も重要であるかについて合意がなされるとお互いにしっかりとフォローしあうという環境が生み出され、社内通達を発信するより、組織目標の達成に向けてはるかに強いコミットメントが得られることが多い。グローバル企業数社で、東京、ニューヨーク、シンガポール、ロンドン等、地域拠点でリスクのファシリテーションを何度も実施しているが、通達やメールなどよりもはるかに中身の濃いコミュニケーションが可能となり、参加者の満足感も極めて高い。これは、その場で活発に議論ができ、双方の情報を共有しながら合意形成を進めるというプロセスを経て、組織としての意思決定への参画意識を実感できるということがポイントになるのである。

3.5　リスク対応には、戦略への反映と内部統制の強化という大きく二つの選択肢がある

リスクの優先順位づけがなされると、次にいかに対処するかであるが、通常、リスク対応戦略には５つの対応、つまり、活用、受容、回避、共有、軽減があるとされる。最初の４つ

はすべて戦略課題であり、例えば、①市場のニーズを先読みし新規事業への進出、投資などリスクテイクを思い切って進める活用、②既存技術を活かした既存事業の周辺にある機会確保を目指す滲み出し戦略を取るなどという受容、③リスクは受け入れず当該事業から撤退するという回避、④パートナーとのJV組成や保険を活用する共有・転嫁などは、リスクの重要性を加味して、経営戦略策定時に経営陣が事業戦略に盛り込むか、期中において戦略の前提事項の変更により見直しをするか、という戦略上の課題ということになる。これら4つの対応は内部統制の範疇ではないとされる所以である。

一方、リスクを一定の許容度の範囲内に軽減するには内部統制が最も有効とされ、リスクの軽減こそが内部統制の本源的価値であるとされる。例えば、「報われるリスク」においては、売上目標やコスト削減目標に対して経営陣が期待する範囲（業務目標やリスク許容度）でこれらの戦略を実現する確からしさを高めるのは内部統制である。成果が不確実だとしても売上の一定規模の資金を研究開発に継続的に投入するのは研究開発型の事業モデル企業における戦略上の課題であるが、研究開発の進捗状況をモニタリングし、経営陣に、次フェーズに進むのか、断念するか否かに係る、必要で高品質の判断根拠を提供するのは内部統制である。逆に言えば、内部統制を強化することにより、企業は更なる新たなリスクテイクが可能となるのである。形骸化とか、やらされ感満載とか、巷に言われる“内部統制悪者論”はここに至ってはその根拠を全く失うことになる。

「報われないリスク」への対応は倫理観を含む内部統制にもっぱら依存することになる。つまり災害やコンプライアンス対応では、リスクを軽減すべき範囲（例えば、防災基準や、JSOXでの開示すべき重要な課題がないことなど）が明示されている場合には、リスクの発現をその範囲（リスク許容度）に収める機能を果たすのが内部統制なのである。

2013年に改訂された、米国COSOの内部統制フレームワークに基づいて、内部統制が有効であると経営陣が表明するには、統制環境などの5つの構成要素ならびに関連する17原則すべてが存在し共に機能していると判断され、重大な欠陥がないことが必須となる。なお、17原則には不正対応も入っており、不正リスクに対するリスクマネジメントは米国企業にとっては導入しなければならないものとなっており、我が国でも具体的な検討・導入が望まれるところである。

3.6　リスクマネジメントの対応実践能力と成熟度

リスク対応方針が決まれば、如何に効果的、効率的に実行するかである。その実行状況を判断する上で有効と思われるリスクマネジメント能力の成熟度を見てみよう。成熟度は、初期段階、連続反復、定義制度化、管理自律化、最適化という5つのレベルがある。

3.6.1　初期段階では、英雄的な要素に依存し、制度・プロセスは存在せず、対応は場当たり的な状況である。どの組織にもあの人に任せれば大丈夫という主のような人がいる。大変

ありがたい存在であるが、ただ見方を変えれば組織的な対応が不十分で、Post“英雄”が常に問題となる。

3.6.2　次に連続反復では、“英雄”が実践していたベストプラクティスが部分的に認知継承され、社内で反復可能なプロセスが形成されていく状態である。共通言語がある程度醸成され、初期のインフラ要素ができ上がってきている状態だが、まだ決して安心できる状態ではない。

3.6.3　定義制度化になると、制度対応に必要な方針・プロセスが定義されており、さらに単に整備されていればいいということではなく、整備された方針通りに運用されているかどうかが、適切なモニタリングを通して確かめられている状態である。この段階では、リスク管理に関する共通言語が確立されており、次のステージへの準備が整っていると言える。

例えば、グローバル化の推進において、国内グループにおける共通言語が、海外グループ、特に新規に買収した組織等に日本企業固有の共通言語をいかに普及するかである。生産技術や販売方針、決算方針、資金管理、IT戦略のみならず、人材戦略を含むまさに経営理念のレベルでの共通言語の浸透をいかに図るかが、熾烈な競争を勝ち抜く上で、不可欠な要素と言っても過言ではない。

3.6.4　管理自律化になると、リスクとリターンのトレードオフについての徹底的な討論がなされ、その動きが適切なKPIや厳密な測定方法/分析等でモニタリングされている状況である。伊藤レポートが示したROE8%は日本企業に一定の刺激を提供し、ROICや売上利益率、マーケットシェアなどそれぞれの企業が大切にする指標の議論をあらためて惹起したことに意義がある。この段階の特徴は、戦略実行の組織的支援とモニタリングが自律的に行われる段階である。

3.6.5　最後の最適化とは、経営理念がグローバルに浸透し、適切なグローバル・グループの組織ガバナンスによって、あるいはアップサイド・ダウンサイド両面に焦点を当てたグローバルリスク戦略により、競争優位性が常に産み出される状況である。スピード感を持って変化に対応しながら戦略の実現をさらに確かなものとしていくことに貢献できる状態である。あらゆる変化の兆候を見逃さず、組織内の課題には自浄機能が働き、持続的成長がより確かなものとできる状況である。

この成熟度モデルを活かすには、自らの組織がどのような成熟度にあるかを認識することから始めることが必要である。同時に、それぞれの企業の特性を最大限反映した成熟度5段階の定義を個々に決定することにある。次に、どのレベルまでに、いつまでに向上させていくかを決定し、現状とのギャップを特定し、その上で、ギャップ解消のためのアクションプランを策定し実行することになる。目指すべき望ましいレベルは4ないし5であることは言うまでもない。成熟度に関する開示、コミュニケーションが今後望まれるところである。

4　取締役会等がリスクオーバーサイトを効果的に推進するには

今まで示して来たような全社的リスクマネジメントがどのように整備運用されているかを判断し、価値創造に向けて、より的確な方向性を協議していくのがリスクオーバーサイトである。そこでリスクオーバーサイトにおける要点の整理を試みた。

4.1　取締役会は、リスクオーバーサイトのための体制構築を検討しているか

リスクマネジメントとは、リスクテイクの方針の下で設定された業務目標やリスク許容度に沿って経営陣が必要なプロセスを遂行することであることから、リスクオーバーサイトはリスクマネジメントプロセスがどのように整備、運用、評価されているかを判断することになる。従って、リスクオーバーサイトの体制、運営の在り方は、企業規模、構造、複雑性、社風、重要リスク等の状況を考慮してそれぞれの企業で最もふさわしいリスクオーバーサイトの在り方を決めることになるであろう。このリスクオーバーサイトの責任は監査役を含む取締役会のすべてのメンバーが負うべきであり、従って取締役会が企業戦略の全体像を把握するには、戦略に伴う重要リスクを把握する必要がある。

4.2　識別されたリスクは直面している重要なリスクを反映しているか

経営陣が取締役会に提示するリスク情報では、留意すべき新たなリスク、既存リスクのアップデートなどを明らかにすべきである。「影響大・発生可能性小」のリスクについても、レピュテーションへの影響、影響の速度、影響の持続性、企業の対応準備度の観点から優先的に考慮することもありうる。また新規リスクを適時に識別するには、例えば、戦略の主要な前提が崩れていないか検討したり、グローバルトレンドに留意したり、全く新しい事業を買収するなどのコアビジネス以外の事業展開による影響を評価したり、サイバーテロ脅威その他企業の事業戦略を根底から覆しかねないリスクを検討する、などがある。

4.3　変容するビジネス環境の中でリスクを効果的に管理できるよう、リスクマネジメント能力を継続的に改善しているか

重要なリスクが特定された後、担当部署が適切に設定され、さらに十分なリスクマネジメント能力を有しているか、必要な継続的改善がなされているかを、取締役会は確かめる必要がある。例えば、主要な全社的リスクを管理・監視する強固なプロセスが確立されているか、ビジネスの変化速度の上昇や複雑化に合わせてリスクマネジメント能力が改善されているか、リスクに関する報告が適時にかつ信頼性をもってなされているか等について確認すべきであろう。

4.4　取締役会と経営者はリスク選好について同意しているか

取締役会は、企業がとるべきリスク、回避すべきリスク、その状況を示す指標について経営者と定期的な協議をもつ必要がある。リスクテイクに係る協議では、例えば、「自社のビジネスモデルがリスク選好指標の範囲内で実施されていることを、どうやって知ることができるか」といった議論がなされるべきである。これを明確にわかるようにするには、リスク選好を個別のリスク許容度にさらに分解し、事業目的達成に関する業務の変動幅の管理に利用するのが最も効果的な方法であろう。例えば、リスク許容度は売上変動幅、利率の変動、人材の雇用・育成・維持等に関する指標等で示され、さらに兆候を示す先行指標が意思決定に重要な影響を与えるものとして示すことが重要である。

4.5　自社のリスク文化は正しい行動を奨励できているか

いかにリスクマネジメントがしっかりできていても、社会秩序を乱す組織的行動が存在し、許容されていては意味がない。トップがリスクマネジメント部門からの危険信号を無視したり、取締役会が戦略の前提やリスクについて厳しい追及をしなかったり、悪い知らせが疎まれる空気があると、重要な変化を見誤る可能性が大きい。その結果、不適切なリスクテイクや、誤った戦略から適時に撤退することができなくなる。望ましい文化のもとでは、多様な価値観、目的、ベストプラクティスが共有され、リスクが企業の意思決定に織り込まれ、風通しのよさや、倫理的行動が徹底されることが大切である。

4.6　リスクマネジメントは適切な経営プロセスと統合しているか

リスクマネジメントが経営プロセスと統合することで、企業の目的を達成し戦略を遂行できるという確信を持つことが可能となる。統合の質と程度は業種や企業ごとに異なり、また経営者の経営スタイルによっても異なる。通常、統合の範囲は、中長期戦略策定、年次計画策定、業績管理、予算策定、競争優位性、設備投資予算、M&Aのターゲット設定、デューデリジェンス、買収後の統合、内部統制全般等である。統合を効果的に進めることにより、リスクマネジメントが企業の持続的な競争優位性の確立や業績改善のために大いに貢献をすることになる。

最後に

リスクオーバーサイトの体制・運用は、業種や経営スタイルによってさまざまであるが、価値創造を目的とする戦略と事業目的の達成に向けて、「報われるリスク」と「報われないリスク」を対象として、戦略上の対応を適宜検討し、必要で十分な内部統制をいかに構築運用するか、独立的立場からの意見をいかに経営に反映する仕組みを構築するかは経営陣の専

決事項である。リスクとは勇気をもって試みることであると再度申し上げたい。

（かんばやし　ひよお・プロティビティ LLC 会長兼シニアマネージングディレクタ）