



## リスクマネジメントとコーポレートガバナンス・内部統制

【『標準化と品質管理』2007年8月号に掲載されたものを財団法人日本規格協会の許可を得て転載しています】

### 1. はじめに

2001年にJIS Q 2001「リスクマネジメントシステム構築のための指針」が登場した背景には、自然災害・人為的災害等が発生した場合、それらの組織や社会に及ぼす影響に対応するための仕組みなりガイドラインの存在が不可欠であるといった認識があった。さらに、状況の変化の中で、組織の経営にとり大事なのは部分最適ではなく、組織の全体最適であり、そのためのリスクマネジメントの実践、ガバナンス、内部統制の強化が重視されてきている。そこで、現在、着目されている動きに焦点をあて、以下、考察を進めたい。

### 2. 注目される企業全体のリスクマネジメント

リスクマネジメントはその発展において複数のルーツがあるが、最近では企業全体を対象としてリスクマネジメントを捉える考え方が注目されてきている。リスクマネジメントのルーツの例としては

- ①製品の安全設計や事故をいかに防ぐかという安全防災の考え方
- ②防火対策と火災保険の関係から開発されてきた、合理的な防災費用と保険費用の配分の考え方
- ③株式投資や為替投資の合理的な投資方法として発展した金融工学的考え方
- ④新規事業や大規模プロジェクトの完成に向け、工期を守りプロジェクトの失敗を防ぐプロジェクトマネジメントの考え方
- ⑤ゴーイングコンサーンとしての企業の発展を阻害する要素をリスクとし、そのリスクを合理的に排除する全社的リスクマネジメントの考え方
- ⑥企業が予期せぬ事態に遭遇した場合に損失を軽減し素早く復旧する、事業継続や危機管理の考え方などがある。このほかにも分類によっては幾つもの理論が存在する。ここでこれらのどれが正しいという議論をするつもりはないが、少なくとも同じ「リスクマネジメント」という言葉であっても、異なる概念や背景や理念をもっている人々がいるということを認識することが大切である。

近ごろ盛んに議論されているのは、企業全体をリスクマネジメントの対象として捉える「全社的リスクマネジメント」の考え方である。このように企業全体のリスクマネジメントが注目されるようになったのは、2006年に施行された会社法や、同じく2006年に可決成立した金融商品取引法で「内部統制」が注目されたことによる。

会社法はその362条等を基本に施行規則98条、100条などにおいて、すべての会社に対して損失の危険の管理を行う規定や体制をもつことを定めた点で、リスクマネジメントの観点から見ると画期的な法律である。また金融商品取引法においては、2005年に発表された金融庁企業会計審議会内部統制部会の説明資料の中で、米国で1992年に発表されたCOSO (The Committee of Sponsoring Organizations of the Treadway Commission) の考え方を全面的に取り入れたことが明らかであり、全社的リスクマネジメントの議論のきっかけとなったのは間違いない。これらの全社的リスクマネジメントの考え方は2001年に制定されたJISである、組織を対象としたJIS Q 2001にその思想が明示されており、この規格にある「組織」を「企業全体」に当てはめたものと考えて差し支えない。

### 3. リスクマネジメントプロセスの考え方

リスクマネジメントの発展には幾つかの道筋がある。しかし、その考え方には共通する思想があり、それを抽出したものがリスクマネジメントプロセスである。現在ISOではリスクマネジメントプロセスの標準規格の議論が進められている。その議論の中で日本が主張しているものは、リスクマネジメントプロセスは本来無色透明であり、何を対象としてリスクマネジメントを行うかによって、安全の促進に関するリスクマネジメントや、保険の適応に関するリスクマネジメント、いかに企業が発展するかという全社的リスクマネジメント等のそれぞれが派生するという考え方である（図1参照）。この図1はオーストラリア・ニュージーランド合同規格AS/NZS 4360を修正し示したものである。以下にそのプロセスを説明する。

- ① リスクマネジメントを適用させる対象としての課題を設定する。
- ② 課題には必ずその課題を解決したいという課題の保有者（オーナー）が存在するのでそれを明確にする。
- ③ 課題の解決を行う責任者を明確にする。保有者と解決する責任者は個人の場合には同一となる場合もあるが、保有者が責任者にその解決を委ねることもある。この場合、保有者と解決の責任者の間にガバナンスが存在する。
- ④ 課題の解決のための組織を取り巻く外部環境、組織内の内部環境を明確にする。利用できる経営資源や制約条件を明確にする。
- ⑤ リスク分析を行う。リスクを発見し、特定し、頻度と影響度などを算定する。
- ⑥ 算定した結果を評価基準と照らし合わせて優先順位付けなどの評価を行う。
- ⑦ リスク対策〔回避、最適化（低減）、移転、保有〕などの計画の策定を行う。
- ⑧ 対策を実施する。対策の実施のための統制活動を行う。
- ⑨ 対応状況の自己点検や監視活動などモニタリングを行う。
- ⑩ 結果について責任者がレビューを行う。

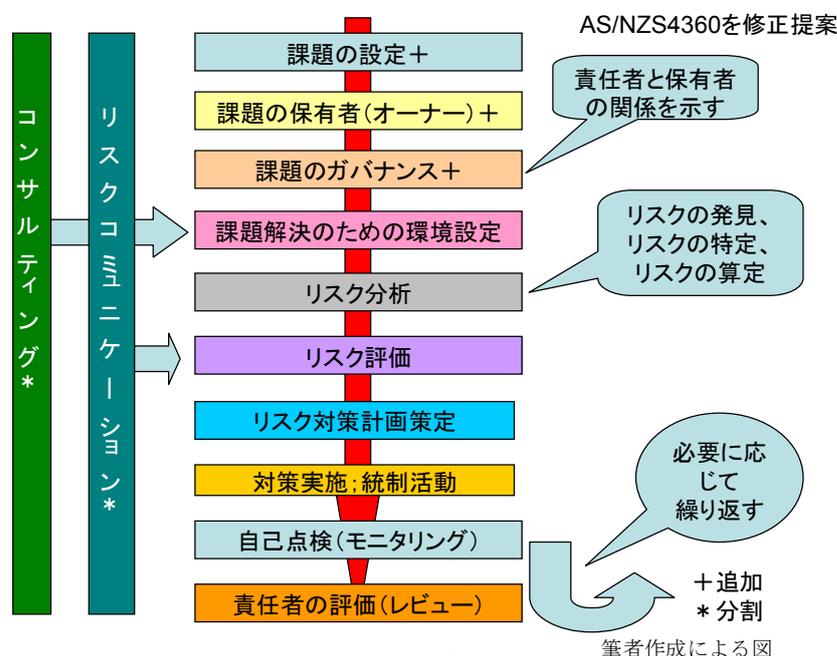


図1 リスクマネジメントプロセス図

これらの活動を必要に応じて繰り返すことになるが、これらの各ステップを実施するために、情報を関係者で共有する「リスクコミュニケーション」と外部・内部の専門家から意見をもらう「コンサルティング」も重要なサブプロセスとして位置付けられる。

これらのプロセスはどのような課題に対しても適応することができる。企業全体のこともあれば、製品の改良、限られた予算を保険と防災にどのように振り分けるか、事業継続の検討、事件事故が発生した危機管理の最中に発生する各課題の解決など、様々なものをリスクマネジメントの対象にすることが

できる。

このプロセスを企業全体の日常の取組みに適応させると、企業の健全な発展を課題とし、この課題の保有者が株主、課題の対応の責任者が経営者という整理となり、企業全体のリスクマネジメントであるERM(Enterprise-wide Risk Management)の概念となる。

#### 4. リスクマネジメントとコーポレートガバナンス

先に、リスクマネジメントプロセスで、課題の保有者と課題の対応者が異なる場合があることに言及したが、ここで組織論における「課題のガバナンス」の考えを明確にする。

本来ガバナンスとは組織の最高経営者の独断を阻止する仕組みであるといえる。会社をはじめ組織で仕事を行うために、各組織はそれぞれ一定程度の枠組みをもっている。一般に組織には階層構造がある。組織は上位階層から下位階層に業務の執行権限を委譲し業務を実施する。このため、上位階層は下位階層に対して①職務範囲を限定し、②下位組織の進むべき方向性を示し、③下位組織が実施している目的の遂行状況について中間報告や結果報告など一定の報告を要求し、④実施するための手段の選択に対して稟議を行い指示や承認を行う。通常の企業では、企業の一番上の階層に企業の実質上の保有者である株主という組織があり、その株主の下に企業が存在する。

この企業には内部に階層構造をもつ組織があり、一番上位の階層が経営会議や取締役会などを含む経営者組織である。経営者の意図を実現するための執行部門として、部、課、係などの社内組織をもつ。この経営者、部、課、係もまたそれぞれが一つの組織である。この組織は職務権限規定などで定められた任務の執行にあたるが、任務の執行条件が設定され、目的遂行のための経営資源と権限が与えられる。組織はその任務の執行にあたって、組織の上下関係のほか、営業や製造などの現場部門と人事や経理などの管理部門などの組織間の横方向の関係や、組織の業務を行うために不可欠な取引先などの外部組織あるいは自らの業務執行により影響を受ける顧客（企業や個人など）、市民などのステークホルダーとの関係を必ずもつこととなる。この意味で「ガバナンスとは組織間の関係性」と認識するとよい（図2参照）。

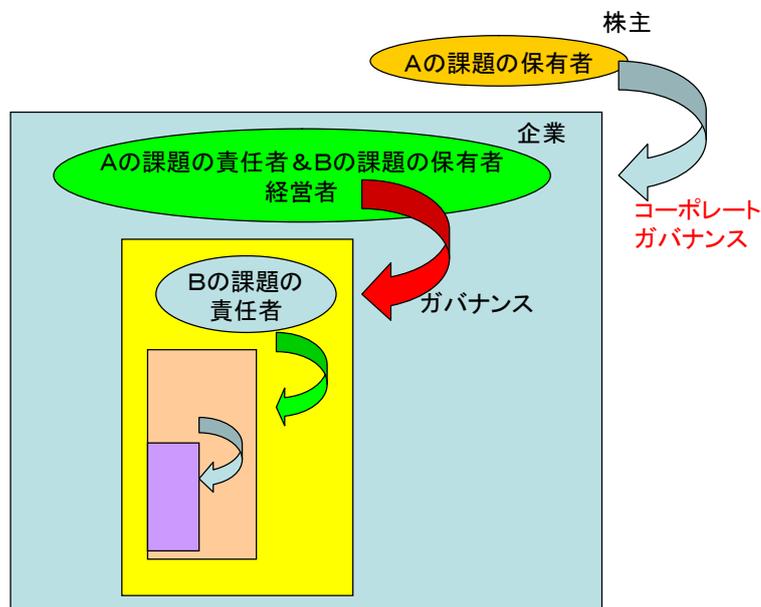


図2 ガバナンスの関係

筆者作成による図

このように、企業の中の各組織は各々上位組織から権限を委譲され、経営資源を割り当てられて職務の執行にあたる。この一つひとつの組織の関係がガバナンスであるが、このように整理すると、企業の組織で最上位階層である経営者と法律上の所有者である株主との関係が特に「コーポレートガバナンス」と言われる関係性となる。また、企業と株主以外の取引先や消費者などとの関係性もコーポレートガバナンスの議論に含まれる。

最近「ガバナンスが効いていない」という言葉をよく耳にするが、これは上位組織が下部組織に委ね

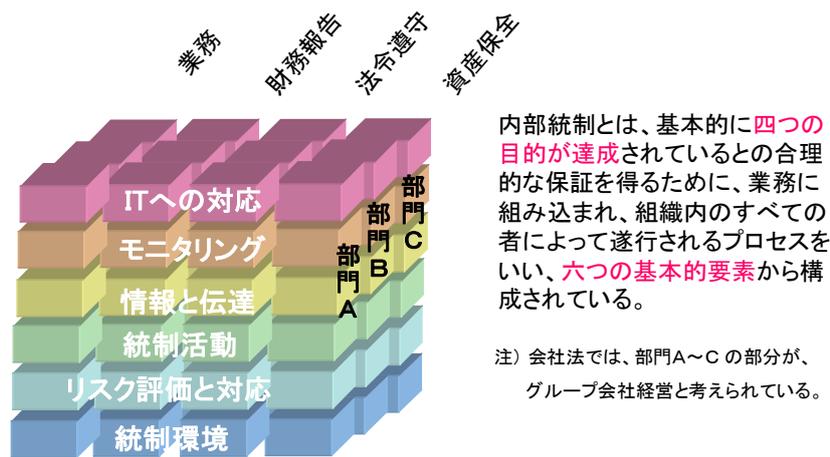
て実施する業務の執行状況が思わしくない場合、あるいは上位組織やその他の関係者が承認していない行為が行われている場合である。企業の中の各組織では、該当の組織の長である部長や課長が暴走しないように、上位者の強い権限や管理部門の牽制により、組織長の行動に歯止めをかけることが期待出来るが、上場企業で株主が分散している場合には経営者の暴走を株主が抑制しにくい状況が容易に発生し得る。この上位組織の権力が分散している点が、一般のガバナンスと区別してコーポレートガバナンスが特別視されるゆえんである。

現在、経営者の暴走を防ぐためのコーポレートガバナンスをめぐる様々な取組みが試行錯誤されている。2004年から有価証券報告書などにコーポレートガバナンスの項目が新設され、会社機関の内容、内部統制システムの整備状況、リスク管理体制の整備状況、役員報酬、監査報酬を開示し、株主からの意見を反映しやすくすることが求められたのもその表れである。この中で組織内に相互牽制を行う仕組みをもつ「内部統制」が一つの解決策として提示されている。

## 5. リスクマネジメントと内部統制

会社法や金融証券取引法でにわかに脚光をあびた内部統制は、もともとは“Internal Control”の訳で、組織運営を適切にコントロールするための自立的な仕組みのことであり、法律や倫理、定款などに違反せずにいかに適切に顧客や取引先の支持を取り付け、企業を発展させるかという積極的な概念であった。2007年現在の日本では、内部統制というと粉飾決算の防止のための財務諸表の適切化のみに焦点があてられているが、金融庁の示す枠組みでも内部統制の目的には、「業務効率」、「財務報告」、「法令遵守」、「資産保全」の四つがあり、企業の業務効率の発展という積極的な目的が含まれていることを忘れてはならない。

ここでは、四つの目的の達成を阻害するものをリスクと定義し、それを排除するために、「統制環境の整備」、「リスク評価と対応」、「統制活動」、「情報と伝達」、「モニタリング」、「ITへの対応」という六つの基本的要素を実施することが明示されている。ここで、リスクマネジメントプロセスとの関係を整理すると、課題として四つの目的のどれを当てはめても、ここでいう六つの基本的要素はいずれもリスクマネジメントプロセスの一部となる（図3参照）。金融商品取引法では財務諸表の正確性の確保を目的にこれら六つのプロセスの実施を求めており、中でもモニタリングを重視し、自己点検や内部監査の充実が要求されている。



「財務報告に係る内部統制の評価及び監督の基準案」  
(金融庁企業会計審議会内部統制部会 2005年12月18日公表)から

図3 日本における内部統制の定義

ここで、内部統制とリスクマネジメントの関係を整理する。リスクマネジメントプロセスは無色透明なモジュールであるため、何にでも適応が可能である。したがって、内部統制の四つの目的はどれもリスクマネジメントプロセスの課題として設定することが可能である。そして四つの目的すべてを対象に

リスクマネジメントを実施する場合はERMであるといえることができる。つまり内部統制とリスクマネジメントとは相矛盾するものではない。

一方、リスクマネジメントシステムと内部統制の枠組みであるCOSOフレームワークとの違いもある。JIS Q 2001はリスクマネジメントシステムというPDCA(Plan-Do-Check-Act)を繰り返す時間の経過の概念があるダイナミックな動的モデルであるが、COSOフレームワークは、ある時点で組織の活動をチェックしたときに、ここに記載されている六つの基本的要素の活動が何らかの手段で実施されていることを求めており、それがPDCAを踏まえて行われているかどうかは問わない静的なモデルである。したがってこれらのどちらが良いかを議論しても無意味であり、企業風土にあった対応がなされ、企業のリスクが日常活動の中で予防され抑止されているかという本質を見極めることが大切である。

## 6. おわりに

変化の著しい現代の経営環境にかんがみて、これまで指摘してきたように、リスクマネジメント、ガバナンス、内部統制の重要性を社会が敏感に受け止めてきており、これらの概念を十分理解してリスクに強い企業になることが望まれる。

以上