

第 部

経営環境とリスクマネジメントシステム

1. 経営環境とリスク

バブル経済崩壊後、組織をめぐる経営環境の変化はその激しさを増してきている。変化のパターンは量的・質的に大きく変化しただけでなく、そのスピードが加速化してきた。保護行政下にあった金融の世界では、公的資金の導入後も不確定要因により回復の道が不透明であっただけでなく、金融への信頼が揺らぎ、株安の影響がさらに拡大し、2002年に入っても、さらなる公的資金の導入が取りざたされている。しかも狂牛病関連では、肉骨粉の混入の実態解明が十分進まない中、肉表示の偽装工作事件が判明し、当該業界における企業倫理の問題が浮き彫りになってきた。

グローバル化した現在の経営環境では一国の市場だけが取引対象ではない。追い討ちを駆けたのが2001年9月のアメリカ貿易センタービルへのテロ攻撃であった。これにより、世界経済に影響が生じ、さらにエンロンの経営破綻により監査法人の信頼性にも陰りが出てきた。

むしろ今日問題なのは、情報が瞬時に世界をめぐり、影響が特定部署にとどまらないという現状を関係者がどのように認識しているかである。とりわけ、組織運営の基底にはコンピュータがネットワークで結合された環境があり、いやがうえにも情報価値を認識・判断し、情報に関わるプロテクションを組織のひとり一人が考えねばならない現状がある。

こうした経営環境の変化の中で、リスクという視点から分析を行う時、情報の世界はこれまでになく脆弱性への対応というガードが重視されざるを得ない。情報システムに関わる脆弱性の認識を誤ると、組織の屋台骨を根底から揺さぶられ、組織の安定性、ひいては存続を不可能にさせることになる。したがって、組織の経営をリスクマネジメントシステムという点から捉え、リスクの影響を明らかにすることが急務となってきたのである。こうした状況から(財)日本規格協会(JSA)より2001年に公表されたのが、次に言及する「リスクマネジメントシステム構築のための指針 - JIS Q 2001 - 」である。

1.1 JIS Q 2001 の概要

JIS Q 2001 のリスクマネジメントシステムについてはすでに紹介があるが²⁾、1995年1月7日に発生した阪神・淡路大震災を契機として、通商産業省工業技術院の委託事業として設置されたリスクマネジメントシステム規格委員会での検討結果である。この委員会の前身として危機管理委員会が設置され、当該委員会では国際標準化機構(ISO)に対して日本発の国際規格提案を行うことが目的の一つにもなっていた。同委員会は再編成され、名称をリスクマネジメントシステム規格委員会(以下、RMS委員会)として再編成された。RMS委員会は2000年3月にリスクマネジメントシステムのJIS規格の開発活動を完了し、「リスクマネジメントシステムの構築に関する指針」のJIS原案のドラフトを完成させ、2001年に『リスクマネジメントシステム構築のための指針 - JIS Q 2001 - 』(日本工業標準調査会審議によるJIS Q 2001として平成13年3月20日制定)がJSAから公表されたの

²⁾ 森宮康・井ノ口和好「リスクマネジメントシステムの標準化について」『予防時報』202号、日本損害保険協会、PP.26～33。

であった。

JIPDEC リスクマネジメントシステム委員会（J RMS 委員会）では、「JIS Q 2001」は情報関連のリスクを焦点にあてているわけではないが、情報システムに関わるリスクに対応する理論的な枠組みとして JIS Q 2001 が利用可能という認識に立ち、「J RMS」を構成することにした。そこで、以下に JIS Q 2001 の枠組みを簡潔に示し、第 部において J RMS の構造について論じることにした。

1.1.1 JIS Q 2001 の特徴

リスクマネジメントシステムでは、問題解決の手法である意思決定論的なプロセスに従い、組織のリスクに関する脆弱性を発見し、対応手段の妥当性を検証する監査をも視野に入れている。

JIS Q 2001 は、大企業、中小規模の企業、病院、研究機関、自治体等々のあらゆる組織を対象としている。しかも、組織を襲うのは日常業務に関わるリスクだけではないことから、緊急事態と称される危機をも想定されていた。ターゲットは組織を襲うあらゆるリスクにしていることから、対策への切り方がかなり包括的であり、その反面、リスクとは何か、緊急事態とは具体的に何を指すのか等々の側面に関しては、経営環境をめぐる可変性を考慮して、リスクをかなり弾力的に捉えている。これは、実際の運営の場において組織の構成員がリスクをどう考えるかについて、あまり厳密であれば、用語の共通理解だけでも困難になるためである。しかしながら、実際の場においてリスクとは何か、緊急事態とは何を指すのか、リスク対策におけるリスク保有とは何かといった用語の理解について関係者の間である程度理解できていることが不可欠である。

1.2 JIS Q 2001 の構成

JIS Q 2001 のリスクマネジメントシステムでは、これまでの ISO9000 シリーズ、14000 シリーズ等々における規格で展開されてきたように P D C A（Plan、Do、Check、Act）というマネジメントサイクルに従っている。これによりリスクマネジメントにおける意思決定のプロセスがフィードバックするように構成されている。

ところで、リスクマネジメントを実際の場で行うためには、その行動指針と基本目的が明確であることが重要である。この点が確定していなければシステムとしての実効性が確保できないからである。リスクの作用が組織にいかなる影響を及ぼすのか、その点からリスク対応の行動指針を明確にし、往々にして抽象的になりがちなりリスク対応の基本目的をできるだけ具体的に設定することが不可欠である。これがリスクマネジメント方針として明示され、それに従いリスクマネジメントの計画が策定されることになる。そうした目的達成のため、計画を策定し、対応組織においてリスクマネジメントを実施し、そのパフォーマンスを評価し、環境変化に応じた是正・改善を行う必要がある。これらの点を要約すれば以下のとおりである。

1.2.1 リスクマネジメント方針

組織としてリスクマネジメントを展開する場合、行動方針・基本目的を明示することが肝要である。JIS Q 2001 では、最高経営者がリスクマネジメント方針を定め、構成員・関係者に文書で明確に表明し、行動指針を定め、それに基づきリスクマネジメントシステムの運用により組織としての到達点等を基本目的として設定することが望ましいとしている。

1.2.2 リスクマネジメントに関する計画 (Plan)

リスクマネジメントに関する計画策定は、マネジメントサイクルの最初のプロセスである。ここではリスク分析、リスク評価、リスクマネジメントの目標設定、リスク対策の選択、それにリスクマネジメントプログラムの策定から構成されている。最初のステップであるリスク分析では、特に組織にマイナスの作用（損失）をもたらすリスクを発見することが出発点となる。とりわけ、日常の業務活動におけるリスクを発見し、特に組織に重大な結果をもたらすリスクを特定化することが望ましい。リスク環境は絶えず変化しているため、リスクを発見するための取組みは継続的に行う必要がある。なお、組織にとり問題状況は平常時だけではないことから、緊急事態も当然考慮される。

(1) リスク分析

リスクマネジメントシステムにおける基本的なプロセスは、以下のとおりである。

- a) リスク発見
- b) リスク特定
- c) リスク算定

以下、これらのステップにおける重要事項について概説しておくことにする。

a) リスク発見

まず出発点はリスクの発見であるが、JIS Q 2001 では「組織に損害を及ぼす可能性のあるリスクを発見することが望ましい」としているが、望ましいこととして「リスクをもれなく明らかにする」と書かれている。だが、学術的な場においても困難なように、こうした表現から実際の経営の場において組織の構成員すべてが同じ理解度をもって発見することができるのかが問われることになる。そこで、JIS Q 2001 では定義を設け、リスクを「事態の確からしさとその結果の組み合わせ、又は事態の発生確率とその結果の組み合わせ」とし、備考の一つに「ある状況では、リスクは予想とのかい離のことである」という記載がある。こうした理解は、あらかじめ予想（予定）していることが実際の結果と食い違うことに視点をあてたものであり、JRAMでの解釈に近似している。

b) リスクの特定

リスクに関する情報を分析し、「組織に重大な結果をもたらすと懸念されるリスク及び/又は結果の重大性の判断が困難なリスクを特定することが望ましい」としている。なお、その上で、脆弱性および危険性の検討を示唆している。またそのための方法としては、ブレーンストーミング、インタビュー、アンケート調査、専門家への相談などにも触れている。

c) リスク算定

特定化したリスクについては、リスク評価の手がかりとして、発生確率・影響の大きさを

定量的・定性的に把握することが望ましいとしている。

(2) リスク評価

特定化したリスクについて、必要に応じ、その重要性の度合いを評価する条件ともいうべきリスク基準を作成し、またリスク対応の優先項目を決めることになる。

(3) リスクマネジメントの目標設定

目標の設定にあたっては、守るべき対象の明確化・法的要求事項（コンプライアンス）などの実行可能な達成目標を組織内外の関係者が容易に理解できるよう明示しておくことが不可欠である。特定の者だけがわかっているのでは、システム全体として十分に機能できるとは考えられないからである。

(4) リスク対策の選択

組織を襲うリスクに対処するための対策は、時間軸に基づいて「事前対策」と「事後対策」から構成されている。特に事後対策としては、組織への影響を考え、被害の最小化・被害の拡大防止を想定した「緊急時対策」と「復旧対策」があげられる。なお、JIS原案では方法としてのリスク対策には「リスク回避」、「リスク移転」、「リスク低減」、「リスク保有」があげられているが、J RMSでは、具体的な方法が示されている。

(5) リスクマネジメントプログラムの策定

リスクマネジメントの目標達成のためにプログラムを策定するわけであるが、その際、望ましいとする設定項目は次のとおりである。リスク対策の具体的な内容、関連部署におけるリスク対策の日程、利用する経営資源、責任の範囲・所在である。

なお、リスクマネジメントプログラムには、上記の事前対策、緊急時対策、復旧対策が含まれる。

さらに、プログラムの策定にあたり考慮すべき事項として次のことが挙げられている。上記の具体的な内容であっても継続的に実施できなければ意味がないことから継続的に実施できる内容、適切な手順、参画すべき責任のある関係者、定期的なレビューに必要な仕組み、経営資源・責任・時期・とるべき対策の優先項目の適切さ、リスクマネジメント方針・一般的計画活動への対応の適切さ、監視・レビューの手順等である。これらは、組織の経営計画に組み込まれるのが望ましい。

1.2.3 リスクマネジメントの実施 (Do)

リスクマネジメントプログラムの実施・緊急時の追加事項・復旧時の追加事項・運用管理が取り上げられている。

(1) リスクマネジメントプログラムの実施

プログラムの実施にあたっては、組織の関連諸部門・部署において策定されたプログラムにしたがって具体的な施策を実施し、その実施状況を責任者に定期的に報告することが望ましい。とりわけ、関連諸部門・部署の関係者間での相互理解を深めておくことが重要と思われる。

(2) 緊急時に特徴的な追加事項

緊急時の対応にはそれなりの実行組織、手順なり準備が必要であるため、追加事項が加味されている。対应手順の策定では、いつ緊急時対応を発動するのか、どのような事態をもって

終了とするのか、組織の内外の機関との協力・連絡関係をどうするのかといった側面が考慮されるべきである。また、実行組織を整備するにあたっての必要事項、すなわち実行組織の責任者はどういう者が望ましいか、情報機能の管理の仕方、分析・評価機能として何をするのか、対応機能の中身は何か、広報機能のあり方といった内容が含まれている。

(3) 復旧に特徴的な追加事項

復旧に対しても必要な追加事項として、外部機関との協力関係の構築、限られた経営資源の有効活用の手順整備が示されている。

(4) 運用管理

これまでのプログラムの実施にあたっては、事前対策の実施手順、緊急時対策の手順、復旧対策の手順、報告様式などの付属資料の文書化など、適切に管理することが望ましいとされている。

1.2.4 リスクマネジメントパフォーマンス評価・リスクマネジメントシステムの有効性評価 (Check)

(1) リスクマネジメントパフォーマンス評価

組織としては、リスクマネジメントプログラムの実施により設定された目標達成に鑑みてそのパフォーマンス(測定可能な結果)がどうなのか、評価を行う必要がある。そのためには手順を確定し、リスクマネジメントの実施状況を監視・測定し、その有効性を評価することが求められる。

リスクマネジメントのパフォーマンス評価に際しては客観性・再現性・検証可能性・実行可能性が重視される。指標と考えられるのは、プログラムやリスク対策実施の進捗度、組織における内部基準、関連する法規制ならびに規格、リスクコミュニケーションの実行度等である。

パフォーマンスの評価は、平常時のみならず緊急時対策ならびに復旧対策についても適宜行うことが重要といえる。

(2) リスクマネジメントシステムの有効性の評価

リスクマネジメントシステムの有効性については、リスクマネジメントの基本目的・リスクマネジメントの目標達成に関する有効性を評価するための手順を確立・維持することが望まれる。

システムの有効性を高めるためには、リスクマネジメント計画、リスク対策、リスクマネジメントシステムの体制・仕組みを見直し、是正・改善がどの程度必要なのか、必要であればどの領域なのかといったことを確定することも重要となる。また、有効性の検証が必要となれば、関係部署の協力を得て、評価を行うことも考えられる。

1.2.5 リスクマネジメントシステムに関する是正・改善 (Check)

(1) 是正・改善の継続的实施

組織をめぐるリスク環境は絶えず変化している。これまで実施してきた対策等のパフォーマンスがリスクマネジメントの目標に照らしてどうなのか、常にチェックする必要がある。それゆえ、リスクマネジメントの実施状況の監視、パフォーマンスの評価、システムの有効性

評価に基づいて、必要に応じてリスクマネジメントシステムを継続的に是正・改善することが求められる。とりわけ是正・改善の実施時期としては、

- a) 継続的是正・改善
 - b) リスクマネジメントシステム監査時
 - c) 緊急事態経験後
 - d) リスクに関する情報の監視結果に基づく要請時
- といった4つが考えられている。

(2) 実施の確認

是正・改善が実際に行われたのか、実施状況の点検・確認について言及されている。ただ、JIS Q 2001 では点検・確認を「望ましい」としているが、現実問題としてこの作業は不可欠といえる。

1.2.6 組織の最高経営者によるレビュー (Act)

最高経営者は、リスクマネジメントシステムを維持し、適切性・有効性を改善するため、リスクマネジメント方針以下、JIS Q 2001 に示された事項について、自ら定めた間隔で当該システムをレビューすることが望ましいとしている。

1.3 JIS Q 2001 におけるシステム維持のための仕組み

情報に関わるリスクの場合、特にリスクマネジメントシステムを実際の場において実施し維持していくための仕組みが不可欠である。そのための仕組みについては、以下の項目からなっている。その概要について示すことにする。

1.3.1 能力・教育・訓練

システムを運用する要員について、その役割ごとに必要な能力が必要である。また、対策実施のため、必要な能力を身に付けさせ、維持させるため、リスクマネジメントに関わる知識等について教育・訓練を実施することが望まれるとしている。

1.3.2 シミュレーション

リスク対応の実施手順の有効性を検証する目的をもってシミュレーションを行うことが必要である。たとえば、それぞれの関係者に役割を与え、活用できる経営資源を設定して、特定のリスクが顕在化していく過程、緊急時になる過程、緊急時を脱して復旧時となる過程などを想定して実施するのがよいといえる。

1.3.3 リスクコミュニケーション

この目的として、リスクの発見・特定のための情報収集、誤解なり理解不足に基づくリスク顕在化の防止等があげられている。また、リスクコミュニケーション実施のための手順の確立・維持について言及されているほか、リスクへの対応に関して組織としていかに対処しているかを明らかにするために広報活動計画を策定すること、さらに関係機関・関係者にリス

ク情報を開示することが指摘されている。

1.3.4 リスクマネジメントシステム文書の作成

組織としていかにリスクに対応しているかを関係者に紙面または電子形式で周知徹底させるとして、その場合、リスクマネジメントシステムの構成および機能、さらに重要な文書類がどこで入手・利用可能かが把握できるようにしておくこととしている。

1.3.5 文書管理

ここでは、他の規格と同様に、種々の文書を作成・改訂し、管理する手順を確立・維持することが重要である。

1.3.6 発見したリスクの監視

組織に作用するリスクの変化を継続的に監視するため、変化を与える要因を特定し、情報を収集することが指摘されている。

1.3.7 リスクマネジメント関係記録の維持管理

記録を維持し管理するのは、リスクマネジメントに関連する様々な活動を追跡可能にするためであり、この点はリスクマネジメントにおいて非常に重要である。

1.3.8 リスクマネジメントシステム監査

リスクマネジメントシステム監査のプログラム・手順を確立し、維持することが望まれている。

1.3.9 組織の最高経営者によるレビュー

最高経営者は、リスクマネジメントシステムを維持し、適切性・有効性を改善するため、リスクマネジメント方針以下、JIS Q 2001 に示された事項について、自ら定めた間隔で当該システムをレビューすることが望ましいとしている。

ところで、JIS Q 2001 では「リスクマネジメントシステム構築のための指針」というタイトルからも理解できるように、組織の経営にとり各項目を実践することが「望ましい」という表現で書かれている。実際にリスクマネジメントを実行するのはそれぞれの組織であるため、組織の判断に委ねるというスタンスに基づくものである。