日本企業はグローバルスタンダードをいかに取り込み発展するか　ISO、J-SOX法

How Japanese Companies Can Introduce Global Standards to Achieve Further Growth: ISO, J-SOX

松田 理恵
Rie Matsuda

三菱UFJリサーチ＆コンサルティング
コンサルティング事業本部
経営戦略部
コンサルタント
Consultant
Corporate Strategy Consulting Dept.
Corporate Strategy Consulting Division

グローバル社会に突入した今日だからこそ、日本企業は激しい環境変化に対応するために戦略リスクを見極めなければならない。そのための一つの手段として、本稿ではマネジメント・ツールを事業の継続のための経営にうまく取り込むことを提案する。

ISOやJ-SOX法などに代表されるように欧米諸国が中心となって決定したマネジメントシステム・ツールが複数存在している。しかしながら、グローバルスタンダードへの動きは多くの企業にとってコストアップ要因や面倒で付加的な作業と捉えられがちである。あれもこれもと取り組んでしまったために本来の目的を忘れてしまう企業さえある。

では、このような失敗を避け日本企業がグローバルスタンダードを取り込み発展するにはどのようにするべきなのだろうか。それは画一的なシステムを導入するのではなく、個々の企業の規模や成長段階、余裕資源にあわせた対応が重要となる。具体的には①統制環境の整備、②戦略リスクを含むリスクの抽出・評価と対応、③適切な経営指標の設定、④経営指標をPDCAサイクルでモニタリングする、の4点である。これら4点について企業規模などにあわせたあるべき姿、既存のマネジメント・ツールの活用や実際の活用事例を紹介している。

従来のように個別のマネジメントシステムをばらばらに実行しているだけでは経営目標を達成することができない。日本企業は全社的な統制環境を整備し足腰を固め、戦略リスクを洗い出し、その上でマイナス面とプラス面を織り込んだ目標項目についてPDCAを回していくことが今後ますます求められるだろう。

In today's age of the "global society", it is more important than ever for Japanese companies to carefully assess their strategic risks in order to deal with the drastic changes in the business environment. This paper will propose how and what management tools can be successfully introduced for the management of business continuity, as a means to address this issue.

A number of management systems tools currently exist which have been developed by the initiative of the U.S. and other western countries, such as the ISO (International Organization for Standardization) standards and the J-SOX Act (the Japanese equivalent of the Sarbanes-Oxley Act). However, the shift to the global standard is considered by many companies merely as a cost pressure factor or another tedious task. Some companies have even forgotten what their initial purpose was, after taking on much more than they can handle.

Then, how can Japanese companies prevent such issues and thrive from introducing global standards? The key to this is opting against the introduction of a standardized system, and making adjustments accordingly based on each company's size, stage of growth, and the capacity of excess funds. There are four points to this in particular: 1) organizing the control environment, 2) extracting, evaluating, and responding to the various risks including strategic risk 3) establishing appropriate management benchmarks and 4) monitoring those benchmarks through a PDCA cycle. The paper introduces the desirable state according to the company size, the application of existing management tools, and the case examples for actual applications related to these four points.

Management targets can no longer be achieved merely through piecemeal implementation of individual management systems, as it has been done in the past.

In the future, expectations for Japanese companies will only increase to strengthen their grounding by improving the control environment at the company-wide level, clarifying their strategic risks, and to then roll out the PDCA cycle, based on targets which allow the measurements of both positive and negative aspects of the process.

1 マネジメント・ツールからみた国際的な潮流

国際標準化機構により規格化されたISOマネジメントシステムには多くの規格があり、品質、環境、情報、リスクマネジメントなどのほか、食品、医療機器向けなど業界別のセクター規格もある。また、国際的なマネジメントのツールとして、ISOのマネジメントシステム以外にもいくつかのシステムが生み出されている。ここでは、その中で主要な7つのマネジメント・ツールを紹介したい。

(1) ISO9001

ISO9001は品質マネジメントシステムに関する国際規格で要求事項が明確に示されている。1987年に初版が制定され、現在は2000年に改訂された規格が最新版となっている。ISO9001の2000年版は、品質レベル及び顧客満足の向上を目指す組織の活動を規定する仕組みである。また、第三者の認証を伴う規格である。

1990年代まではTQM（TQM：Total Quality Management）の流れを汲んで主に輸出を営む製造業が取引先の要請からISO9001を取得することが多かった。しかし、2000年以降は顧客満足の向上や改善活動という視点からサービス業など幅広い業種で取得されている。日本では一頃と比較すると新たに取得する企業の数は鈍化している。

ISO9001の要求事項は、①文書化、②品質方針や品質目標など経営者の責任、③ヒト・モノ・カネなど資源の運用管理、④業務や設計・開発のプロセスを含む製品実現、⑤内部監査、改善や是正などのチェック機能の5つの仕組みに分解されている。

こうした仕組みの構築後、文書や記録の作業に追われてしまう企業もあるが、他方で成果の出ている企業もある。両者の違いはどこから来るか。それは改善を促す組織かどうかである。つまり、組織としてPDCAが機能しているかどうかによる。平たく言えば、⑤内部監査、改善や是正などのチェックがしっかりとしている企業は、残りの①～④の全ての要求事項も自ずと機能していると言えよう。

(2) ISO14001

ISO14001は環境マネジメントシステムに関する国際規格で要求事項が明確に示されている。1996年に初版が制定され、現在は2004年に改訂された規格が最新版となっている。ISO14001の要求事項は、①環境方針や環境目標、環境側面、環境法などの計画、②環境に影響のある項目の運用管理や教育訓練の実行、③内部監査、改善や是正などのチェック機能、④マネジメントの見直しのPDCAの4つに分解されている。

ISO9001と同様にISO14001も第三者の認証を伴う規格である。日本では一頃と比較すると新たに取得する企業の数は鈍化している。

(3) ISO27001

情報セキュリティーに関するマネジメントシステムである。情報セキュリティーに関するマネジメントシステムにはISO27001の前身としてISMSが普及していたがISO27001としてISOで規格化され、さらに2006年に日本でJIS規格化された。第三者認証を伴うマネジメントシステムである。

情報セキュリティー管理のポイントは、①情報に意図しない漏れはないかを管理する機密性、②情報が正しいかどうかを判断する完全性、③必要な時に利用できるかという可用性の3つのバランスである。経営陣の責任、内部監査、マネジメントレビュー、改善といったPDCAのサイクルが要求事項に規定されている。品質マネジメントシステムの代表格であるISO9001との違いは、情報マネジメントシステムのISO27001ではリスクアセスメントのリスクの評価基準を設けることが必要になっていることである。

情報セキュリティーのため、IT業界において認証取得する企業が多い。類義の情報セキュリティーマネジメントシステムとして個人情報の保護に特化したプライバシーマークもある。プライバシーマークはISO27001よりも審査が厳しいという意見も少なくない。

（4）JISQ2001

JISQ2001は、2001年にJIS規格化されたリスクマネジメント構築のための指針であり、認証制度はないもののリスクマネジメントのシステムを構築する際に日本企業が参考にしている。JISQ2001では、リスクマネジメントを組織のリスクに関する戦略的な計画策定、意思決定及び他の過程を含むマネジメントシステムの諸要素と定義している。具体的には、システム構築及び維持のための体制、リスクマネジメント方針、計画策定、実施、パフォーマンス評価及びシステムの有効性評価、是正・改善の実施、組織の最高経営者によるレビューの主に7つの項目から成り立っている。オペレーションリスクに対して、自然災害や緊急時の事故などに対応するための枠組みを示している。

（5）CSR

企業の社会的責任としてCSR（CSR：Corporate Social Responsibility）という言葉を耳にすることも多いだろう。企業の果たすべき責任は、経済、環境、そして社会活動へとシフトしている。第三者評価制度はないもののアメリカ、ナイキ社の児童労働問題が社会問題となるなど企業のCSRへの関心は高い。1990年代後半頃から2000年初めにかけてオーストラリア、アメリカ、イギリスなどの国やGRI（GRI：Global Reporting Initiative）などの組織によりさまざまな規格がつくられた。当初計画よりもかなり進行が遅れているが、ISO26000の規格化に向けてISOの作業部会であるSR総会（SR：Social Responsibility）が動きだし、労働、産業、消費者、政府、NGOという5セグメントのステークホルダー（利害関係者）との意見交換がなされガイダンスの発行を急いでいる。

この国際会議では、CSRの対象は企業のみではないと解釈され、SRとして規格化が予定されている。ステークホルダーとは、企業に対し何らかの要求を主張する個人または集団であり、ステークホルダーの課題を把握することが重要になる。SR総会では、ステークホルダーの主要課題として、環境、人権、労働慣行、組織のガバナンス、公正な商習慣、コミュニティー参画、消費者課題（経済的側面、健康及び安全、サプライチェーン）の7つをあげている。

（6）J-SOX法

J-SOX法とは日本版SOX法ともよばれ、内部統制の強化を目的とした米国SOX法を参考にした経緯からこう呼ばれる。金融商品取引法が存在しているものの、具体的な基準は法律の中では触れられていない。企業は金融庁が発表する実施基準に基づき内部統制の対応を図っている。ここでは内部統制に係わる法律の略称としてJ-SOX法と呼ぶ。

会社法における内部統制の目的は財務報告の信頼性、資産の保全、業務の有効性・効率性、法令順守の4つである。このうち、J-SOX法では上場企業における財務報告の信頼性を対象としている。2009年3月からの決算報告資料には内部監査の報告書を添付しなければならない。エンロンの不正経理事件がきっかけとなり、アメリカで上場企業を対象にしてSOX法が制定された。J-SOXは上場企業に業務フロー、業務記述書、リスクコントロールマトリックスの文書三点セットを作成することを求めている。さらに、作成された文書に基づいて毎年、内部監査人が運用評価をして記録を残し内部監査報告書として公表していくことを求めている。

（7）ERM

ERM（ERM：Enterprise Risk Management）は、全社的リスクマネジメントと訳される。2004年にCOSO（COSO：the Committee of Sponsoring Organization of the Treadway Commission））米国トレッドウェイ委員会組織委員会が発表したCOSO-ERMが現在のERMの主流となっている。米国トレッドウェイ委員会組織委員会ではCOSO-ERMを、ERMを事業体の取締役会、経営、その他によって遂行され、事業体の戦略策定に適用され、事業全体にわたって適用され、事業目的の達成に関する合理的な保証を与えるために、事業体に影響を及ぼす発生可能な事業を識別し、事業体のリスク許容限度に応じてリスク管理が実施できるよう

に設計された一つのプロセス、と定義している。

目的は業務の有効性と効率性、財務報告の信頼性、関連法規制への準拠性、ミッション・戦略への貢献の4つである。構成要素は、内部環境、目的の設定、事象の識別、リスクの評価、リスクへの対応、統制活動、情報と伝達、モニタリングの8つである。

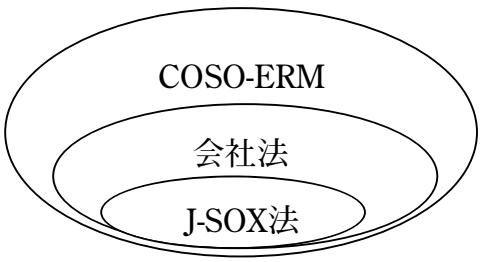
COSO-ERMによれば、「不確実性は、事業体の価値を喪失させたり、付加したりする可能性を持つのでリスクでもあり、事業機会でもある。ERM によって経営者は、不確実性とそれに付随するリスクや事業機会に有効に対応でき、そしてそれによって事業体の価値を創造する事業体の能力を向上させることができる。」とされている。リスクについては、4項（2）で詳しく述べる。

会社法がJ-SOX法を包含し、ERMは会社法を包括していると考えられ、図表1のとおりCOSO-ERMがもっとも大きな概念である。

以上により7つのマネジメントシステム・ツールを紹介した。品質マネジメントシステムがISO化された80年代は、日本企業に対する貿易障壁ではないかと懐疑的に受け止められたこともあった。しかし、グローバル化が進む近年ではあまりそうした声は聞かなくなったのではなかろうか。例えば、CSR（SR）のISO規格化に向けて世界12カ国の主要メンバーによる会議が行われ、日本もそのメンバーの一員として積極的に参加している。マネジメント・ツールの開発においてもグローバル化の波に乗り遅れることないよう規格化の段階から発言していこうという姿勢の表れといえよう。

個別企業の経営面においても人口減少時代に突入した日本企業が生き残るには、グローバルスタンダードをもとにした舵取りが求められるだろう。

図表 1　概念図



出所：各種資料よりMURC（三菱UFJリサーチ＆コンサルティング）が作成

2 日本企業のマネジメントシステムを考える

次に日本企業のマネジメントシステムを考える。図表3のとおり、日本のISO9001、ISO14001ともに認証取得の件数は多い。しかし残念ながら、日本企業は欧米諸国などの海外で規格化された個別のマネジメント・ツールに都度、対応してきた傾向が強い。そのため、複数のマネジメントシステムが並列して走っている企業も多いのではなかろうか。大企業はもちろんのこと、中小企業でも大企業との取引があれば複数のマネジメントシステムを維持していることも少なくない。

ところで、上場企業についてはJ-SOX法により2008年4月以降が財務報告に関わる内部統制の評価対象年度となった。アメリカのエンロンの不適切な会計報告が契

図表 2　主なマネジメントシステムの概要

	名称	分野	第三者による認証制度の有無など	規格化された年など
1	ISO9001	品質	認証制度あり	1987年規格化
2	ISO14001	環境	認証制度あり	1996年規格化
3	ISO27001	情報	認証制度あり	2006年規格化
4	JISQ2001	リスクマネジメント	JIS規格化されているが認証制度はない	2001年JIS規格化
5	CSR	社会的な責任	認証制度の予定はない	2009年にISO26000規格化予定
6	J-SOX法	財務報告	金融商品取引法による上場企業が対象	2008年 4 月より評価対象
7	ERM	ERM（全社的リスクマネジメント）	認証制度はない。COSO-ERMが主流	2004年米国トレッドウェイ委員会組織委員会がCOSO-ERMを発表

出所：各種資料よりMURC（三菱UFJリサーチ＆コンサルティング）が作成

機となり、内部統制システムの構築がグローバルスタンダードになったのである。これにより、いってみれば日本の上場企業も、投資家に対して財務諸表に嘘・偽りがないことを証明する作業が増えてしまったことになる。J-SOX法に関わる内部統制の運用評価の開始に伴い、証明作業のため、上場企業は膨大なコストと時間を投入し、利益に直結しない管理を強化しなければならなくなった、とも言える。今後、IPOを控えている企業にとっては、いかにコストと時間を省いて効果的なシステムを構築するかに関心が集まるだろう。

J-SOX法を簡単に説明すると、以下のように言える。財務報告に関わる一連の業務を文書化し、どこにリスクが潜んでいるのか把握する。リスクに対するコントロールを整備し、必要に応じて業務の流れを見直し文書化する。また、不正が起きないように職務分掌などの規程類を整備・実行しているか、こうした一連の取り組みを内部でチェックし記録を残していく。これらが実行されていなければ是正し、再発防止の措置をとるということになる。全体のスキームはISOに通じるものがあり、ISOの財務版とも言えるだろう。内部統制の場合は、連結ベースであり対象範囲がさらに大きくなる。

内部統制は、法律で定められた義務とはいえISOの取得ブームと似ていると揶揄され、一過性のブームで終わると考える人もいる。米国SOX法と同じようにある程度、緩和されることはあるかもしれない。しかしながら、グローバルスタンダードの波からくる大企業の動きが日本におけるメインストリームとなり、それが中小企業に波及することも十分考えられる。

現実に中小企業が上場企業に買収され子会社となったものの、教育や標準化が不十分なために、担当者が判断に迷いながら決算・財務報告資料を作成しているケースもあるだろう。業務の流れが担当者個人の頭の中にあるだけでは、内部牽制が十分に機能していないばかりか投資家に対する説明責任を十分に果たしているとは言いがたい。その経理担当者が転職してしまった場合は業務がストップしてしまう。

図表 3　ISOの認証取得件数2006年12月現在

		世界の取得件数	日本の取得件数
1	ISO9001	897,866件	80,518件
2	ISO14001	129,199件	22,593件

出所：ISO Survey

中小企業では、人員の不足や人件費の削減などの理由から一人の経理担当者が決算・財務報告作業をしている場合が多い。経営者が経理担当者に費用と収益の期間を意図的にずらすよう指示を出し、経理担当者は指示通り処理してしまっているかもしれない。調達担当者が仕入れた商品を横流して勝手に販売している可能性もある。営業担当が支店ぐるみで架空の売上を毎月システムに計上し続けているかもしれない。どこまでやるか、どういったあるべき姿を描くかについては議論の余地があるが、大企業でも中小企業でもグローバルスタンダードを取り込み発展していくには、内部の牽制をしっかりと効かせる仕組みづくりが必要になるだろう。

3 日本企業のマネジメントシステム活用度

では、日本企業のマネジメントシステムはどのくらい活用されているのであろうか。

例えば、大企業を中心に数年前から社長直轄の企画部門にCSR推進室を設置し、個別のマネジメントシステムを統括する部門をつくる企業が増加した。環境省が2008年に発表した「環境にやさしい企業行動調査」の中で、環境への取組と企業活動のあり方については、「企業の社会的責任の一つである」と回答した企業等の割合が最も高く81.9%である。ステークホルダーに対してCSR報告書を年に一度、冊子として発行するかウェブサイトを通じて活動結果を公表している企業もある。また、ステークホルダーミーティングを開催し、ステークホルダーの生の声を聞いた上で次のアクションにつなげる企業も出てきている。

しかしながら実際には全てがうまくいっているわけではない。というのも、こうしたマネジメントシステムに付随する活動を現場では企画部門からの一方的な目標の

押し付けと受け止めてしまい、部門長から現場担当者への周知が行き届かないこともあるからだ。方針を立て目標を設定し会社として結果を公表しているが、現場の一人ひとりの行動に結びついていない場合もある。また、毎年同じ目標を掲げてPDCAを回している素振りをしているケースや、他の企業のマネやビジネス本から拾い出だした目標をさもわが社独自の目標であるかのうように振舞っているケースも見受けられる。

中小企業のマネジメントシステムの活用度はどうだろうか。たとえば、事業承継にあたってISOを導入し次期経営者のマネジメント力を計画的に育成する企業がある。中小企業は機動性が高いこともあり、ISOというマネジメントシステムの力により経営者をスムーズに代替わりさせることもできる。また、法令順守に留まらず基準を上回るレベルを目指した思考と行動に努めているような環境先進企業の場合は、ISO14001の活動をきっかけとしてレベルアップを図っている。環境マネジメントシステムの導入を序章とし将来的には品質マネジメントシステムを取得することで、より磐石な組織を目指す大企業と比較すると中小企業は、より実益のある形でマネジメントシステムを構築し、活用していることが多い。

一方で、取引先からの要請により場当たり的にISOの取得に向けて動きだした企業では、システムの目的が現場で理解されていないケースもある。また、活動のマンネリ化も散見され、認証取得までの熱はどこにいってしまったのか、今ではネタが切れてしまった、何を目的目標にすれば良いのか正直わからない、ISOのマークを維持するのが目的になっている、いわゆる「ネタ切れ」に対する事務局の悩みも多く聞かれる。これに対する改善点については、4項（3）で詳しく述べる。さらに、全体を統括する人材が不足し、審査前に事務局が記録を残す作業に追われるといったこともある。

これまでの経緯を振り返ると、企業は社会や取引先からの取得要請に応えるべく、時限付きのシステムプロジェクトチームをつくり、各部門に推進員を配置するなどして鋭意システムの構築を行った。ところが、いったん構築されたシステムの運用に入ると、システムそのものがたいへん重く感じられ、システムの運用のため想像以上に作業に追われてしまうことに気がつく。結果として、是正や改善活動よりもむしろ文書の整理や記録の保管方法に悩むという企業もあった。また、たとえ個別のシステムの運用に慣れたとしても、全体としてみるとシステムに重複感がある、他のシステムとの融合ができないものか、誰がどうやって統括していくべきかという声をきくこともある。総じて、部分的には効果のある場合もあるが全体として考えると十分には活用されず効果が十分に出ているとは言い難い状態にあるといえる。

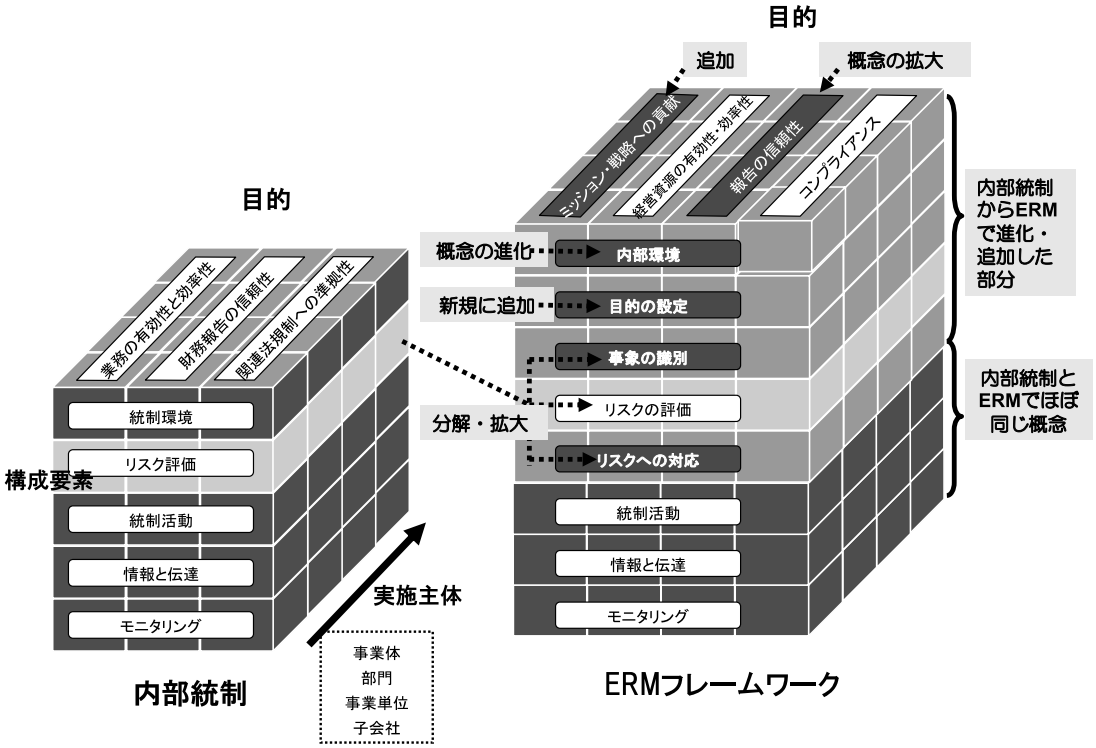
4 日本企業がグローバルスタンダードを取り込み発展するポイント

次に日本企業がグローバルスタンダードを取り込み発展するポイントについて述べる。ポイントは①統制環境の整備、②戦略リスクを含むリスクの抽出・評価と対応、③適切な経営指標の設定、④経営指標をPDCAサイクルでモニタリングする、の4つである。すでにお気づきの読者もいる通り、これら4つのポイントは、COSO-ERMにおける8つの構成要素に密接に関係している（図表4参照）。また、内部統制とCOSO-ERMの関係は、図表のとおりでCOSO-ERMは内部統制のリスク評価の部分を分散・拡大させるなどして進化させたものとされる。

（1）統制環境の整備

統制環境はいわば経営の骨格であり、経営者の理念や社員の倫理感に関わる。統制環境がしっかりしなければどのような活動で肉付けをしても企業は崩れてしまう。ガバナンスの体制をどのように整備するのが企業にとって最も効果的かという議論も関連するだろう。日本企業では従来の監査役による統制が十分には機能していなかったこともあり、欧米諸国のガバナンスに習って、新会社法が施行された。この新会社法では取締役会の中に指名委員会、監査委員会及び報酬委員会を置く委員会設置会社を選択することもできるようになった（会社法2条12号）。委員会には、社外取締役を過半数以上取り入れるなど業務監視機能を高めるために採用する企業も出て

図表 4　内部統制とCOSO-ERMの関係



出所：八田進二監訳『全社的リスクマネジメント〔フレームワーク篇〕』東洋経済新報社を参考にMURC（三菱UFJリサーチ＆コンサルティング）編集

きている。しかしながら、そうした新しい体制を整備するだけでは、企業全体として統制を図ることができるものではなく委員会設置会社における不正経理事件が発覚している。

グローバル社会において、欧米諸国と同様なガバナンスの体制を設置することも重要であるが、そうした体制に加えて日本企業が統制環境を整備するにあたり配慮すべきことがある。それは、①不正や間違いが起きてしまう環境を排除すること、②不正をしなければならないプレッシャーを排除することである。この2点は人間のする行為を統制するにあたってたいへん重要な要因であることから、どのような体制を構築するにあたっても必ず考慮する必要がある。

なお、会社法による内部統制では統制環境とされているが、COSO-ERMでは内部環境としてリスクマネジメントを取り入れている。ここでは会社法による内部統制で必要とされる要素別に具体的な取り組みの例をあげる。これらの事例から、上場企業ではなくともJ-SOX法の全社的統制の指針を参考にして体制を整備していくことができる、ということを理解できよう。

①誠実性及び倫理観

誠実性及び倫理観においては、倫理規程や行動指針を作成し教育することによって社員に求められる倫理感の風土を作り出すことが目的となる。倫理観は一日で成し得るものではない。当たり前のことであっても継続的に情報発信し続けることで社員を教育し、風土を生み出していくことが重要である。

②経営者の意向及び姿勢

経営者の意向及び姿勢には、経営者による社訓・社是について長期的なビジョンとともに社員への周知を図ることが必要となる。カリスマ社長やオーナー企業で一般的にはISOなどの型を必要としない組織であっても、成長段階にあわせてISOを認証取得し、一定の成果を生み出している企業もある。例えば、筆者はトップダウンによってISO14001に取組むオーナー企業の社長に出会ったことがある。社長は自ら環境方針とともにCSR方針を

作成し社員に切々とその必要性を説いていた。経済、環境、社会問題において調和をとりつつ、ステークホルダーとの良好な関係を保つことに配慮するといった経営者の姿勢は社員の行動を変化させた。社長が「今までは私が全てであった。しかし、ISOを取り組んだ後は、組織として改善点を話し合い、自分達でものごとを判断しようとする風土が芽生えた。」と話していたのが印象に残っている。実際に、今まで絶対に表に出そうとしなかった部門の悪い点が内部監査を通じて見えるようになり、そこにPDCAが組み込まれることによって改善活動が活性化したのである。こうした企業の成功事例を取り入れ学ぶことで他の企業もグローバルスタンダードを取り込み発展する機会を得ることができるだろう。

③経営方針及び経営戦略

経営方針や経営戦略は企業が持続的に発展していく上で最も重要な道しるべといえる。経営者の意向に整合した中長期的な経営方針及び経営戦略を実施主体別に落とし込むことが鍵となる。経営方針及び経営戦略については、後述の4項（2）リスクの抽出・評価と対応で後述する。

一方で、前述したとおり不正をしなければならないプレッシャーを排除することも考慮すべきだ。支店に課された過度な売上目標を達成するために、支店長が不適切に数字を操作しているかもしれない。こうした不正がおきないようにするには不正を犯さなければならない環境そのものをつくらないことにも配慮すべきだろう。

④取締役会及び監査役または監査委員会の有する機能

現状の取締役会や監査役または監査委員会の構成員や機能について整理し、ガバナンス体制が十分か、検討する。会社法が施行され委員会設置会社などの新しい制度設計を選択することも可能になった。特に大会社については、独立した社外取締役をおくなどガバナンスを強化させる必要があれば、そうした制度設計に変更し統制環境を整備する。

⑤組織構造及び慣行

成長段階にある企業や顧客のニーズが激しく変化するような企業においては、組織構造が妥当かどうか再度、検討する必要がある。

⑥権限及び職責

内部の牽制が十分に利く職務分掌となっているか判断する。前述したとおり、ここでは特に不正や間違いが起きてしまう環境を排除することがポイントとなる。不正や間違いが発生する可能性の高い業務については、一人で完遂しない仕事の流れにすることが求められる。担当者に加え承認者を配置したり、マスター変更作業を他の部門に任せるなどの工夫を要する。

J-SOX法の実施基準では業務処理統制において、業務のリスクとコントロールの洗い出しが要求されている。この洗い出しを行うと不正経理に対する内部の牽制が十分か否か見え、権限及び職責に欠けている部分が見えてくる。このようにリスクとコントロールを洗い出し、権限及び職責をもう一度検討することにも活用できる。

⑦人的資源に関する方針と管理

人的資源を社内人材の育成にしぼって考えた場合、社内での教育体制の整備をし、社内リーダーを育成する長期的な計画を立案し実行していくことが求められる。計画を実行していくためには、品質マネジメントシステムISO9001の「6.2.2力量、認識及び教育・訓練」を活用することもできる。

3項で述べたように、例えば品質マネジメントシステムを取得している中小企業であれば、内部監査員をリーダー人材として育成し内部監査を通じて業務改善の風土づくりや企業の全体的なレベルアップが期待できる。また、ISO9001ならば品質のみ、ISO14001ならば環境のみという個別のマネジメントシステムにとらわれることなく、PDCAのマネジメントシステムとして活用することが重要である。ISO14001のコミュニケーションでは、全社員から環境だけではなく、業務効率の改善やロスの削減なども含めた意見を拾う機会としてとらえ、良い意見を表彰する制度として利用することができる。また、文書化した手順や改善提案の意見を全社に水平展開し、新入社員や中途採用社員の教育資料としても大いに

活用することができる。このように全社的な観点から人的資源に関する方針を築くことを忘れてはならない。

（2）戦略リスクを含むリスクの抽出・評価と対応

従来型のマネジメントシステムに最も欠けていた部分は戦略的なリスクではなかろうか。戦略リスクに注目しているCOSO-ERMをもとに、ここでは戦略リスクを含むリスクの抽出・評価と対応についてふれる。

ビジネスの環境変化が激しいグローバル社会では、戦略リスクへの対応が特に重要な要素となる。企業が持続的に発展するには、「攻め」と「守り」の両側面を取り入れなければならないだろう。COSO-ERMでは事業体の価値が最大化するには、経営者が「成長とリターンの目標」と「それに関連するリスク」との間を最適なバランスを取るように戦略や目的を設定し、かつ事業体の目的追求のために資源を効率的かつ有効に配分することに着目している。バランス・スコアカードBSC（BSC：Balance　Score Card）にある「攻め」の経営指標に重要業績評価指標KPI（KPI：Key　Performance Indicator）が知られている。可視化された目標が現場の個人レベルの取り組みを促し、こうした活動がいわば企業のドライビングフォースとなる。戦略リスクは、KPIなどの戦略遂行を阻害する要因で、重要リスク指標KRI（KRI：Key　Risk　Indicator）とも言える。戸村氏の著「SOX法・対策・内部統制対策の決定打」によれば、このKRIについて第4世代バランス・スコアカードと表現されている。すなわち、従来の業績評価指標KPIに加え、事業の撤退基準などの意志決定について重要リスク戦略指標KRIを経営戦略に盛り込むことが必要である。

1項（4）で述べたとおりリスクマネジメントシステムJISQ2001には、リスクの抽出・評価の項目があるが、オペレーショナルなレベルでのリスク抽出が中心であった。また、環境マネジメントシステムでも環境上のリスク等を抽出する4.3.1環境側面があるが、個別の活動ごとに環境に対する影響に対して個別に評価するものであった。戦略リスクが今までのリスクの捉え方と大きく異なるのは、投資計画など戦略的な意思決定を伴うリスクの抽出を含む点である。COSO-ERMにおいても抽出されたリスクを発生頻度と影響度の乗数で評価することは同じである。リスクに優先順位をつけリスクの回避、低減、移転、受容といった対応をとることについては従来と大きく異なるものではない。こうしたリスク評価の算定手法は極めて難解であり、定量的な分析が必ずしも正解を導くわけでもない。具体的な評価手法については専門書に譲ることとする。

それでは、どのような考えに基づいて戦略リスクを抽出するのであろうか。ここでは、初心者にもわかりやすいようにCSRの視点を入れた簡易的なステークホルダー分析によるリスク抽出方法を紹介する。

ステークホルダー課題を調査するには、ISO14001の環境側面調査の手法を応用することができる。ステークホルダーの課題は、環境から社会にまで対象範囲を広げた環境側面と考えられるからである。ISO14001と環境側面をステークホルダーの課題に読み替え、ステークホルダーの課題について調査し、把握・分析する（図表5参照）。

抽出の流れは、以下のとおりである。

まず、企業にとってステークホルダーを特定する。前述のとおりISO化にむけたSR会議では労働、産業、消費者、政府、NGOをステークホルダーとし、環境、人権、労働慣行、組織のガバナンス、公正な商習慣、コミュニティー参画、消費者課題（経済的側面、健康及び安全、サプライチェーン）をステークホルダーの主要課題としている。しかしながら、セグメントは全ての企業に共通ではないためそれぞれの企業に応じて柔軟に解釈しステークホルダー分析を行っても構わない。ただし、経年変化をみるためには一企業のステークホルダーは固定化することが望ましい。

次に、ステークホルダー課題を設定し、ステークホルダーごとに目的達成を阻害する戦略リスクKRIを洗い出す。事業の実施主体毎に定期的にステークホルダー分析のシートを用いてアイデア出しからとりかかる。このような大掛かりな調査・分析を行わないにしても、企業に

図表５　ステークホルダー課題の分析

課題の洗い出し		関心度プラス影響	リスク抽出	リスク評価	主なステークホルダー	CSR重点課題⇒改善計画へ	運用管理／緊急時管理	関連法令
視点	ステークホルダー課題の例	大／中／小	ステークホルダー課題におけるリスク	大／中／小	顧客、従業員、供給者、株主、政府、地域社会等	影響度を勘案し重点課題を特定●	規程・マニュアルの名称	法令等の名称
環境	環境に優しい経営を進めるにあたって、ステークホルダーの主要な関心事は何ですか。		左記を行わなかった場合のリスクは何ですか。		左記のCSR課題に関わるステークホルダーは誰ですか。			
	環境配慮商品の販売促進。	中	商品が時代のニーズに合わなくなり、商品が売れなくなる。	大	株主、顧客			
	化学物質の安全な管理。	中	化学物質漏洩し爆発する。	大	地域社会			
お客様	顧客満足を高めるためにあたってステークホルダーの主要な関心事は何ですか。		左記を行わなかった場合のリスクは何ですか。		左記のCSR課題に関わるステークホルダーは誰ですか。			
	担当者が不在な場合の対応が適切であること。	中	担当者不在による対応の遅れ。	中	顧客			
情報管理	機密情報・個人情報の保護を強化にあたってステークホルダーの主要な関心事は何ですか。		左記を行わなかった場合のリスクは何ですか。		左記のCSR課題に関わるステークホルダーは誰ですか。			
	全社取組として機密情報の管理強化の推進。	大	顧客の個人情報が漏洩し信用が落ちる。	大	顧客、個人、従業員	●		
従業員満足	従業員満足（働きがい）を高めるにあたってステークホルダーの主要な関心事は何ですか。		左記を行わなかった場合のリスクは何ですか。		左記のCSR課題に関わるステークホルダーは誰ですか。			
	社内の改善提案制度、表彰制度の仕組みづくり。	大	評価における公平性の確保。	大	従業員	●		
	教育研修やスキルアップのチャンス。		リスクは特にない。	ー	従業員			
調達・供給者	調達を適正に実行するにあたってステークホルダーの主要な関心事は何ですか。		左記を行わなかった場合のリスクは何ですか。		左記のCSR課題に関わるステークホルダーは誰ですか。			
	調達基準を明確にし、不正が起きないようにする。	中	仕入業者と仕入担当者の癒着。	大	サプライヤー、従業員			
人権・労働安全衛生	人権・労働安全衛生に関して適切に実行するにあたってステークホルダーの主要な関心事は何ですか。		左記を行わなかった場合のリスクは何ですか。		左記のCSR課題に関わるステークホルダーは誰ですか。			
	社員の健康管理の徹底すること。定期健康診断の受診、メンタルヘルスの充実など。	大	長期入院などによる人件費コスト増。	小	従業員			
社会貢献活動	社会貢献活動を適切に実行するにあたってステークホルダーの主要な関心事は何ですか。		左記を行わなかった場合のリスクは何ですか。		左記のCSR課題に関わるステークホルダーは誰ですか。			
	ステークホルダーミーティングの実施。	小	特にない。	ー	NPO、地域社会、国際社会			
	植林やごみ拾いなど社会貢献活動を行う。		特にない。	ー	地域社会			
コンプライアンス（法令順守）	コンプライアンスを適切に実行するにあたってステークホルダーの主要な関心事は何ですか。		左記を行わなかった場合のリスクは何ですか。		左記のCSR課題に関わるステークホルダーは誰ですか。			
	内部通報制度の構築。	大	社内において、いやがらせの増加。	小	政府・監督官庁（業界団体）		ガイドライン	
財務報告	財務報告を適切に実行するにあたってステークホルダーの主要な関心事は何ですか。		左記を行わなかった場合のリスクは何ですか。		左記のCSR課題に関わるステークホルダーは誰ですか。			
	財務報告にかかる内部統制の整備。	大	上場廃止リスク。	大	株主・投資家、顧客	●		
事業継続管理（天災など）	事業継続管理・危機管理を適切に実行するにあたってステークホルダーの主要な関心事は何ですか。		左記を行わなかった場合のリスクは何ですか。		左記のCSR課題に関わるステークホルダーは誰ですか。			
	BCP®の策定。 ※BCP（Business Continuity Plan）とは、何らかの事件や事故が発生した場合にその企業の特定された重要な業務が中断しないこと	中	天災や原油資源高など有事の際に事業を行うことができなくなる。	大	従業員			

出所：各種資料を参考にMURC（三菱UFJリサーチ＆コンサルティング）が作成

とってステークホルダーは誰なのか、それぞれのステークホルダーの課題は何だろうか、その内容についてステークホルダーとの対話の機会を持つことも重要だ。ステークホルダーとの対話と表現すると、やや大げさになるが営業担当が顧客の声を積極的に聞き出したことや調達担当者が仕入先の動向をまめにメモしたことを担当部門での共通認識とするというものである。

以上のように、戦略リスクの抽出方法にあたってはコレといった決め手は存在しない。また企業の規模によっては、もともと大掛かりな調査などは必要としないこともある。しかし、どのような企業であっても、戦略リスクに相当する考えを取り入れていくことは必要不可欠となるだろう。

（３）適切な経営指標の設定

抽出・評価されたリスクをもとにリスクに対応するためには適切な指標設定をし、組織全体として行動につなげることが重要になる。たとえば、製造業ならば製品の貢献利益率と貢献利益についてA、B、C、Dなどのランクを設定し、Cランクを下回った場合は臨時にコスト改善委員会を開催する。調達部門は仕入先の見直しによって仕入原価の再検討を図る、また、製造部門は社内工数や外注加工費などの削減の可否について各部門に落とし込んで具体的なアクションにつなげる。また、Dランクを下回った場合は取締役会にかけて原則的に撤退するというような基準である。この他にも、製造業であれば実際原価と予定原価の差額、不良率、二酸化炭素の排出量などについて全社レベルの戦略リスクを設定し、これらを個人の活動レベルまでにブレークダウンすることでより明確で誰にでもわかりやすい指標となる。

ところで、品質マネジメントシステムのISO9001の「5.4.1」に品質目標、環境マネジメントシステムISO14001の「4.3.3」に目的、目標、及び実施計画と

して要求事項に目標管理が組み込まれている。両者ともに品質面、環境面からみた個別の経営指標となるが、方針展開を行い、目標として見える化し、現場レベルでPDCAを回す点については全く同じである。品質マネジメントシステムや環境マネジメントシステムに全社的な戦略リスクの概念を付け加えることで既存のシステムを活用することもできよう。目標は目標値が高ければ良いというわけでもなく、数が多ければ良いというわけでもない。重要なのは戦略にあった目標項目の設定と部門目標、個人目標の設定と日々の行動に結び付きやすい目標内容にすること、及び戦略リスク指標KRIとしてこうした戦略遂行を阻害する要因を盛り込むことが必要である。

また、従来のISOの目標管理など個別のマネジメントシステムの指標を活用させるのであれば、中期経営計画や業務計画といった経営の本来の計画と整合を図ることで組織全体のパフォーマンスの向上が期待できる。業務計画とISOで一致させた目標については、担当者、進捗管理の方法、達成時期などの具体的な方策も一致させた方がより効果的となる。実際に多くの組織で、業務計画とは別にISOのための実施計画を新たに作成していることがあり、ISOの進捗管理だけのために「ISO会議」などと称して会議を開くことも少なくない。しかし、経営と直結したISOにすればそうした負担は軽減され、担当者の意識も変わる。例えばISOの目標値を業務計画の目標値にリンクさせるとそれらの目標値に係わる集団に一本の串が刺さり、円滑なマネジメントが実現できる。担当者にISOは本来の業務そのものであるという当事者意識が芽生えるからだ。必要に応じて、ISO事務局を管理部門ではなく企画部門にすることも検討されるとよい。

一方で、ISOの目標と業務計画を切り離したいという企業があるかもしれない。経営者にしてみれば、業務計画についてまで審査や第三者に審査されたくないという思いがあるからだ。その場合は、全てをISO目標に取り込まずに一部の経営指標のみをISOの目標値とすれば良い。

（4）経営指標をPDCAサイクルでモニタリングする

PDCAが回らないといかなるシステムも崩壊してしまう。システムが適切に機能するには、モニタリングが必要になる。しかしながらモニタリングの方法に定石はない。参考とすべき要求事項にISO9001の「8.2」における監視及び測定やISO14001の「4.5.1」における監視及び測定がある。その考えでは、企業が自ら適切な管理の基準を設定しそれを定期的に測定していく仕組みがあればよいとされている。例えば、経営指標に設定された新規取引先の受注額を取締役会に提出する。こうした結果をもとに担当の取締役は支店長に対して指示を出し、毎月の営業会議で担当者が対応と次の策をねる、というモニタリングの仕組みでも十分に機能する。

適切な管理基準を設定しなくとも、内部監査員を育成し内部監査でシステム全体を補うこともできる。前述の4項（1）のとおり、特に中小企業においては内部監査によるチェックが組織全体のレベルアップにつながることを申し添えたい。今まで表に出そうとしなかった部門の悪い点に対しても内部監査を通じてチェック機能が働き、そこにPDCAが組み込まれることによって改善活動が活性化する例は多くある。

J-SOX法の運用評価の方法を活用すれば、最も厳しいモニタリングとなる。というのも、J-SOX法では内部監査人が各部門のキーとなる統制業務について、その証跡のサンプリングを要求しているからである。日時処理の業務の有効性を判断するには、1年間で25件の証跡、例えば売上日報を25枚もサンプリングしなければならない。さらにサンプリングされた全ての売上日報について、適切な職務分担に基づいた承認行為がなされていること、売上日報と伝票に金額、取引先名、品目、勘定科目、売上計上日などに間違いがないことを再度、照合し記録を残すことが必要なのである。このモニタリング方法は法律で決められているため、上場企業は2009年3月の決算から財務諸表などとともに内部統制監査の結果も報告しなければならない。

大企業の場合は、CSRのステークホルダーミーティン

グを開催し、外部のステークホルダーから監視する体制をとることもできる。3〜4年前までは企業が一方的にCSR報告書を発行していることも多かった。ところがこの数年、B to Cの大企業がステークホルダーミーティングを開催することが多くなっている。双方向のコミュニケーションによって、ステークホルダーの意見を取り入れること、こうした定期的なミーティングを開催すること自体がステークホルダーからのモニタリングとなり、ひいては社会的な責任を果たしていることにつながると考えられる。

この他にもISOのスキームによるマネジメントレビューを応用する、または監査結果を取締役会の報告事項とすることも考えられる。こうした活動もモニタリングの一つになる。いずれにせよ企業が組織として持続的に発展するには計画を作っただけに終わらせることのないよう、PDCAが機能し次のアクションに結びつくモニタリングが必要不可欠である。

5 むすび

日本の人口は減少に転じ日本経済が右肩上がりで安定的に成長した時代は終わりを遂げた。また、地球規模の温暖化による気候変動もあり、穀物相場は予測不可能となり、資源・原油価格が高騰している。世界人口は急増して65億人を超え、新興勢力の台頭により長く続いたドル支配の時代も終わりつつある。結果として食料や資源争奪戦による政情の不安要素は増加している。

こうしたグローバル社会に突入した環境変化の激しい今日だからこそ、企業は戦略リスクを適切に見極める準備をする必要があるのではなかろうか。しかし、ISOやJ-SOX法にみられるグローバルスタンダードへの動きは、多くの企業にとってはコストアップ要因や面倒で付加的な作業と捉えられがちである。では企業はどのように対処すればよいのだろうか。それは、むしろこうしたマネジメント・ツールを事業の継続のための経営にうまく取り込むことである。あれもこれもと取り組むのではなく個々の企業の規模や成長段階、余裕資源にあわせた対応が重要となる。従来のように個別のマネジメントシステムをばらばらに実行するのではなく、日本企業は全社的な統制環境を整備し足腰を固め、戦略リスクを洗い出し、その上でマイナス面とプラス面を織り込んだ目標項目についてPDCAを回していくことが今後ますます求められるだろう。

【参考文献】
・環境にやさしい企業行動調査　環境省　平成20年
・財務報告に係る内部統制の評価及び監査に関する実施基準　金融庁
・わかるCSR　三菱UFJリサーチ＆コンサルティング　CSR研究プロジェクト
・Enterprise Risk Management ― Integrated Framework　COSO
・http://www.coso.org/default.htm
・SOX法・内部統制対策の真髄　第４世代バランス・スコアカード　戸村智憲