

内部統制導入とISO規格の視点

内部統制構築上の問題と改善のために

名古屋リスク研究会 内部統制グループ

岡田良一、尾崎健造、山本治男、森島龍児

[1] はじめに

平成20年4月1日以降に開始する事業年度から適用される『金融商品取引法等の一部を改正する法律』（以下、『日本版SOX法』という）により、企業の規模にかかわらず全ての上場企業およびその連結子会社では、財務報告に係る内部統制の評価と報告および公認会計士による監査が義務付けられる。

従って、日本の上場企業集団は、内部統制の名のもとに急激な企業改革を求められている。しかし、上場企業といってもその規模は様々であり、個々の業務分担が細分化され、人的にも資金的にも恵まれた大企業集団と、その対極にある中小企業集団とは、内部統制導入過程に立ちはだかる障壁は異なっており、特に中小企業集団においてはクリアすべき課題が多いのが実情である。

本稿では、上場する中小企業集団の内部統制構築過程における様々な問題を検証し、その解決策と構築後の運用について、ISO規格（9000s、14000s、27000s）に照らし合わせ提言するものである。

[2] A社における内部統制導入過程の検証

1. A社について

A県に本社を有するA社は、従業員数約800名、資本金約20億円、売上高約400億円のサービス業を営む上場企業である。近年、最大顧客である製造業の好調な業績に連動し、安定した業績を残している。A社は、中小企業に見られる年功序列型の家族意識の強い社風であり、社員に有利な対応ができるよう就業規則以外の諸規程については、内部統制が求める基準にまで整備しておらず、業務に対応する基準書や標準書といった業務プロセス文書も整備していない状況である。

ただ、一部の業務では平成10年に国際規格であるISO9001を、平成15年には出先の事業所においてISO14001を認証取得しており、業務の文書化やプロセス管理の重要性について一部の役職員は認知している。ただ、多くの役職員は、これらの整備とマニュアルに即した業務対応には非常に抵抗感を示す傾向がある。

2. A社の内部統制導入の経緯

A社では、平成19年1月に日本版SOX法に対応するためのプロジェクト事務局として社長直轄部門の内部統制室を開設した。同室には、総務部門、経理部門、情報システム部門および営業部門からそれぞれ1名ずつが人選され、4名が兼務というかたちで配属となった。人選されたメンバーは、それぞれの部門における

中心的な人材であったが、過去に他のプロジェクトの中心となった経験はなく、内部統制導入プロジェクトに必要となる技術と経験も十分なものではなかった。

それ故、コンサルタントによる指導が必要との判断から、それをA社の会計監査を実施する監査法人の公認会計士に委ねることとなった。内部統制室員は、監査法人や情報システム企業が実施する内部統制セミナー等に積極的に参加し、内部統制の理解に努める一方、公認会計士からは文書化の手法等を学ぶこととなった。同時に、社内に潜在するリスクの抽出やその解決策についての研究も始めることとなった。メンバーの役割分担として、総務部門出身者が全社統制を、経理部門出身者が財務統制を、情報システム部門出身者がIT統制を、営業部門出身者が業務プロセス統制を担うこととなった。

しかし、平成19年4月の定期人事異動により、総務部門から選出されたメンバーが内部統制室の兼務を解かれ、営業部門から選出されたメンバーが総務部門へ異動となり、全社統制と業務プロセス統制を担うことになった。また、この時期から社内の業務プロセスの文書化が開始されることとなった。各部署より文書化メンバーとして2名が選出され、内部統制室員から文書化の指導を受けながら、各部署の業務プロセスを分析し、文書化を進めることとなった。しかし、文書化メンバーの力量の差や他部門との関わりのあるプロセスについて未調整のまま文書化を進める等、混乱をきたす結果となった。

3. A社の内部統制導入の問題点

A社における内部統制導入には、以下の問題点が浮き彫りとなった。

① 社長直轄部門であることの弊害

プロジェクト事務局である内部統制室は社長直轄として開設され、当初選任されたメンバーは、部長代理1名、課長1名、課長代理2名（のちに1名は兼務を解かれる）となっていた。しかし、階層的にも、これまでの職歴からも社長との距離感にはあまりにも大きく、内部統制導入に際する社内の様々な問題についての報告、相談、連絡といったビジネス上の基本動作が滞り、意思疎通が図れないという致命的な問題が浮き彫りになった。

② プロジェクト事務局による組織化の不備と力量不足

プロジェクト事務局メンバーは、先述のとおり内部統制プロジェクトに必要となる技術と経験が不足していたこともあり、役員および各部門の管理職を包含する委員会形式のプロジェクト・チームを構成しなかった。その結果、他部門との連携を図る機会のない文書化メンバーの作成文書は、セク

シヨナリズムに基づく組織横断性のない縦割りのものとなり、水平展開を図ることが不可能なものになった。また、文書化メンバーへの文書化教育に関しても、不慣れな事務局員が行ったため、同一行為や同一目的の書類であるにも関わらず、部門毎に違って使用してきた用語の全社統一化を図らなかったため、事務局員に多大な校正作業が課せられ、本来すべき事務局員の役割分担を果たせなくなった。

③外部コンサルタントの誤選定

A社は、内部統制への取り組みが遅れたこともあり、準備期間が約1年程度と短く、事務局員の力量も不足していたため、外部コンサルタントの活用を取り決めた。しかし、内部統制導入に必要な社内整備の要件や外部コンサルタントに求める課題等について社内討議を十分に行うことなく同社の会計監査を行う監査法人をコンサルタントとして選定した。結果として、監査の独立性を尊重するが故に、選定した監査法人からはA社が期待していた十分なコンサルティングを受けることができない状況となってしまった。後日、同法人の見解としては、コンサルタントではなく、あくまでもアドバイザーである旨の回答を得ることとなった。

④経営層の内部統制に対する抵抗感

A社は、設立以来一貫して右肩上がりの成長を遂げ、財務体質も極め優れており、これまで企業不祥事に遭遇したこともないことから、役職員ともコーポレートガバナンスは十分であると自負している。また、企業体質として独自性を重んじることから、内部統制導入は監査法人による経営への介入につながるものと経営層は懐疑的である。こうしたことから、内部統制導入プロジェクトに関する経営資源の投入は、必要最低限のものとし、法に照らし合わせた最低限の対応でよいとの方針であった。

⑤社内活力の不活用と社内の抵抗

A社は、既に国際規格であるISO9001およびISO14001を導入する企業であり、ISO規格に沿った業務管理を実践し、業務プロセス管理や各種規程類の文書化など内部統制と共通のテーマに精通する人材がいるにも関わらず、こうした社内活力を内部統制制度導入プロジェクトに連携することができなかった。

また、プロジェクト事務局は、文書化の経験がない文書化メンバーに対して、業務の視認性を高める意義や、業務のフローチャート化およびフローチャートから派生する業務プロセスの文書化など、体系的なトレーニングを施さないまま、業務プロセスの文書化を要求するほか、一貫した見解や方針を与えることができず、場当たりの対応となってしまう、現場とのコミュニケーションに隔たりが生じることとなってしまった。このため、社内は混乱し、文書化メンバーから抵抗にあった。

4. A社における内部統制導入に向けた改善

A社では、内部統制導入にあたり準備期間の短さや事務局メンバーの経験不足から様々な問題点が浮き彫りとなった。プロジェクトの初期段階においては、事務局メンバーの選任と外部コンサルタントの選定は、大変重要なファクターとなっている。

そこでA社では、閉塞感のあるプロジェクト問題を改善するため以下の改善策を平成19年10月に実施することとなった。

①社長直轄部門であることの改善

プロジェクト事務局である内部統制室を、社長秘書である常務取締役が管掌する一部門とし、社長とプロジェクト事務局との間における調整役を設けた。以後、プロジェクト事務局からの報告も順次社長に伝達されることになり、社長からの方針も同時に通達されることとなり、意思疎通がうまく図れるようになった。

②プロジェクト事務局による組織化の不備と力量不足の改善

常務取締役が管掌する一部門となったことから、週1回の管理職会議、月1回の取締役会、年4回の取締役・執行役員合同会議の席上、内部統制の進捗状況の報告がなされるようになり、部門間における情報交換や情報共有の機会を得られるようになった。

また、4人体制から3人体制になりマンパワーの不足していたプロジェクト事務局に営業部門から1名の兼務補充がなされ、事務局内の役割分担が機能するようになった。

③外部コンサルタント誤選定への改善

A社が選定した監査法人では、自らが整備した内部統制を、自ら監査するといった自己監査になるため、A社が作成した文書や評価手続きについてコメントを行う程度のサービスしか提供できないことがわかった。A社は、外部コンサルタントに寄せる期待を明確にするために、内部統制プロジェクトに必要なプロセスの確認と文書整備の有無などの洗い出しを再度実施した。その結果、内部統制導入に必要な文書化作業やリスク評価、改善活動、モニタリング、内部監査活動のほとんどを自助努力により行えることが判明した。

④経営層の内部統制に対する抵抗感の改善

社長-常務取締役-プロジェクト事務局というラインが確立して以来、あらゆる機会に内部統制問題が報告されるようになり、A社の経営層も管理職層も内部統制への理解が深まり、内部統制を利用して企業改革を進める機運が高まった。

⑤社内活力不活用と社内抵抗の改善

先述したプロジェクト事務局への兼務補充要員は、国際規格であるISO9001の文書化経験者を充てた。内部統制で必要とされる考え方や手法の多くは、ISO9001やISO14001の規格の要求事項と共通する部分が多いからである。こうした専門的な知識を有する人材をプロジェクト事務局のメンバーにすることにより、

- ・内部統制方針およびプロジェクト計画の策定
- ・全社統制および業務プロセス統制の評価対象の決定
- ・文書化メンバー決定と推進体制および期限の設定
- ・全社統制方針と業務プロセス文書化および評価基準の決定
- ・フォーマット等文書化ツールの策定
- ・文書化メンバーへの説明会実施および教育
- ・作成文書および評価の管理
- ・進捗状況の管理

といった、本来事務局がすべき役割を短期間に担うことができた。

そして、閉塞間のあったプロジェクト事務局と文書化メンバーとの関係も定期的なすり合わせの場を提供したことにより、関連ある部署間の協議も順調に行われ、他部門の文書化の状況と意見交換ができる風土作りもできるようになった。

[3]**A社の事例から考察する内部統制とISOとの関係**

これまでA社を事例に、内部統制導入プロセスにおける様々な問題点と改善策について紹介してきたが、ここで注目したいのは国際規格であるISO規格の要求事項と内部統制との関連性についてである。

内部統制には、以下のとおり4つの目的とそれを具現化する6つの基本的要素から構成されている。(図表1 日本版SOX法COSOフレーム)

1. 目的**①業務の有効性および効率性**

「事業活動の目的の達成のために、業務の有効性及びと効率性を高めること。」と定義されている。

②財務報告の信頼性

「財務諸表及び財務諸表に重要な影響を及ぼす可能性のある情報の信頼性を確保すること。」と定義されている。

③事業活動に関わる法令等の遵守

「事業活動に関わる法令その他の規範の遵守を促進すること。」と定義されている。

④資産の保全

「資産の取得、使用及び処分が正当な手続及び承認のもとに行われるよう、資産の保全を図ること。」と定義されている。

2. 構成要素**①統制環境**

「統制環境とは、組織の気風を決定し、組織内のすべての者の統制に対する意識に影響を与えると同時に、他の基本的要素の基礎となるものをいう。」と定義され、リスクの評価と対応、統制活動、情報と伝達、モニタリングおよびITの利用に影響を及ぼすものであり、具体的には以下のとおりである。

- ・ 誠実性及び倫理観
- ・ 経営者の意向及び姿勢
- ・ 経営方針及び経営戦略
- ・ 取締役会並びに監査役又は監査委員会の有する機能
- ・ 組織構造及び慣行
- ・ 権限及び職責
- ・ 人的資源

②リスクの評価と対応

「リスクの評価と対応とは、組織の目標の達成に影響を与えるすべてのリスクを識別、分析及び評価することによって、当該リスクへの対応を行う一連のプロセスをいう。」と定義されており、具体的には以下のとおりである。

- ・ リスクの評価
組織の内外で発生するリスクを、組織全体の目標に関わる全社的なリスクと組織の職能や活動単位の目標に関わる業務別のリスクに分類し、その性質に応じて、識別されたリスクの大きさ、発生可能性、頻度等を分析し、目標への影響を評価する。
- ・ リスクへの対応
評価されたリスクについて、回避、受容、低減または移転

等、適切な対応をする。

③統制活動

「統制活動とは、経営者の命令及び指示が適切に実行されることを確保するために定める方針及び手続をいう。」と定義され、権限および職責の付与、職務の分掌、手続き、承認行為等が業務プロセスに組み込まれ、遂行されることにより機能していることが求められている。

④情報と伝達

「情報と伝達とは、必要な情報が組織や関係者相互に、適切に伝えられることを確保することをいう。」と定義され、組織内の全ての者が、各自の業務遂行に必要な情報を適宜、適切に識別、把握、処理、伝達しなくてはならないとされ、具体的には以下のとおりである。

・ 情報

組織内のすべての者は、組織目標を達成するため及び内部統制の目的を達成するために、適時かつ適切に各々の職務の遂行に必要な情報を識別し、情報の内容及び信頼性を十分に把握し、利用可能な形式に整えて処理することが求められている。

・ 伝達

組織目標を達成するため及び内部統制の目的を達成するため、必要な情報が適時に組織内の適切な者に伝達される必要がある。経営者は、組織内における情報システムを通して、経営方針等を組織内のすべての者に伝達するとともに、重要な情報が、特に、組織の上層部に適時かつ適切に伝達される手段を確保する必要がある。

・ 外部伝達

法令による財務情報の開示等を含め、情報は組織の内部だけでなく、組織の外部に対しても適時かつ適切に伝達される必要がある。また、顧客など、組織の外部から重要な情報が提供されることがあるため、組織は外部からの情報を適時かつ適切に識別、把握及び処理するプロセスを整備する必要がある。

⑤モニタリング(監視活動)

「モニタリング(監視活動)とは、内部統制の有効性を継続的に監視及び評価するプロセスをいう。」と定義され、モニタリングにより、内部統制は常に監視、評価及び是正されることになる。具体的には以下のとおりである。

・ 日常的モニタリング

内部統制の有効性を監視するために、経営管理や業務改善等の通常の業務に組み込まれて行われる活動。

・ 独立的評価

日常的モニタリングとは別個に、通常の業務から独立した視点で、定期的又は随時に行われる内部統制の評価であり、経営者、取締役会、監査役又は監査委員会、内部監査等を通じて実施されるものである。

・ 評価プロセス

内部統制を評価することは、それ自体一つのプロセスである。内部統制を評価する者は、組織の活動及び評価の対象となる内部統制の各基本的要素を予め十分に理解する必要がある。

・ 内部統制上の問題についての報告

日常的にモニタリング及び独立的評価により明らかになっ

た内部統制上の問題に適切に対処するため、当該問題の程度に応じて組織内の適切な者に情報を報告する仕組みを整備することが必要である。この仕組みには、経営者、取締役会、監査役等に対する報告の手続きが含まれる。

⑥ I T (情報技術) の利用

「I T (情報技術) の利用とは、内部統制の他の基本的要素が有効かつ効率的に機能するために、業務に組み込まれている一連の I T を活用することをいう。」と定義され、組織目標を達成するため組織の管理が及ぶ範囲において、I T 環境に対応した情報システムに関連する内部統制を整備及び運用することが求められている。具体的には以下のとおりである。

・全般統制

I T を利用した業務処理統制が有効に機能する環境を保証する間接的な統制をいう。通常は、ハードウェアやネットワークの運用管理、ソフトウェアの開発、変更、運用並びに保守、アクセス・セキュリティ及びアプリケーション・システムの取得、開発並びに保守に対する統制を含むものである。

・業務処理統制

個々のアプリケーション・システムにおいて、承認された取引がすべて正確に処理され、記録されることを確保するコンピュータ・プログラムに組み込まれた統制をいう。

では、これまで紹介してきた内部統制を構成する6つの基本的要素と国際規格である ISO9001 (品質マネジメントの国際規格) と ISO14001 (環境マネジメントの国際規格) の規格要求事項には、多くの共通点があることに着目したい。(図表2 内部統制と ISO との共通性1)

1. 統制環境における要求事項は、以下に該当する。

ISO9001:「5.1経営者のコミットメント」「5.3.3品質方針」「5.4.1品質目標」「5.5.1責任及び権限」「5.6マネジメントレビュー」「6.2人的資源」

ISO14001:「4.2環境方針」「4.3.3目的、目標及び実施計画」「4.4.1資源、役割、責任及び権限」「4.6マネジメントレビュー」

ISO/IEC27001:「5.1経営陣のコミットメント」

2. リスクの評価と対応における要求事項は、以下に該当する。

ISO9001:「8.5.3予防処置」

ISO14001:「4.3.1環境側面」「4.4.7緊急事態への準備及び対応」「4.5.3不適合並びに是正処置及び予防処置」

ISO/IEC27001:「8.3予防処置」

3. 統制活動における要求事項は、以下に該当する。

ISO9001:「4.1一般要求事項」

ISO14001:「4.1一般要求事項」

ISO/IEC27001:「4.1一般要求事項」

4. 情報と伝達における要求事項は、以下に該当する。

ISO9001:「5.5.3内部コミュニケーション」

ISO14001:「4.4.3コミュニケーション」

5. モニタリング (監視活動) における要求事項は、以下に該

当する。

ISO9001:「5.6マネジメントレビュー」「7.5.3識別及びトレーサビリティ」「8.1一般」「8.2.1顧客満足」「8.2.2内部監査」「8.2.3プロセスの監視及び測定」「8.2.4製品の監視及び測定」「8.3不適合製品の管理」「8.4データの分析」「8.5.1継続的改善」「8.5.2是正処置」「8.5.3予防処置」

ISO14001:「4.5.1監視及び測定」「4.5.3不適合並びに是正処置及び予防処置」「4.5.5内部監査」「4.6マネジメントレビュー」

ISO/IEC27001:「4.2.3ISMS の監査及びレビュー」「6 ISMS 内部監査」「7.1一般」「7.2レビューへのインプット」「7.3レビューへのアウトプット」「8.1継続的改善」「8.2是正処置」

最後に、I T (情報技術) の利用に関しては、日本版 S O X 法特有のものではあるが、ISO9001規格の要求事項にある「6.3インフラストラクチャー」と ISO/IEC27001規格の要求事項「4.2.1ISMS の確立」「4.2.2ISMS の導入及び運用」に共通点を見出すことができるのである。

[4] 中小企業における今後の内部統制と ISO

上場する大企業の多くは、ISO9001や ISO14001などの手法を取り入れたマネジメントを行っている。そして、それぞれの維持活動に別々の委員会や事務局を設置していることが一般的である。例えば、ISO9001は品質管理部門で、ISO14001は環境推進部門で、また、ISO/IEC27001は情報セキュリティ部門でといった例である。更に、内部監査についても、ISO9001の内部監査員と ISO14001の内部監査員が別個に存在していることも多い。

大企業の場合、一般的には非常に組織化が進み、従業員の業務は細分化されるとともに高度に専門化されていることが多い。従って、ISO 維持活動においても、先述のとおり、ひとつの企業で各々の部門が個別に国際規格の維持管理と運営をしている事例が多く見られる。

一方、中小企業の場合、資金は勿論のこと、人的パワーが不足しがちであるため、ひとり一人に課せられる課題は多く、煩雑で、いくつもの業務を兼務しているケースが見られる。また、スペシャリストよりもジェネラリストをを求める傾向が強いのも特徴である。このような環境下で、ISO 維持管理を複数の部署でそれぞれ管理することは非効率であり、今後は、管理の一元化が必要になると思われる。これらは内部監査に対しても同様で、ISO9001、ISO14001、ISO/IEC27001の複合監査を実施できる人員が必要となってくる。

これまで、内部統制は、ISO9001、ISO14001、ISO/IEC27001で求められているマネジメント手法そのものであることを述べてきた。ただ、ISO9001、ISO14001や ISO/IEC27001規格には、経理・財務上のマネジメントの要求事項は含まれておらず、内部統制にはその処理が含まれることに大きな違いがある。一般的に、内部統制を単なる経理上の統制活動と捉えるむきもあるが、実際に内部統制が求めているものは、PDCA サイクルを柱とした経営者方針の明確化とその伝達方法、手段の整備、継続的改善を実施するための社内システムの構築とチェック機能の整備、業務の見える化とそのプロセス管理、コンプライアンスを中心とするリスクマネジメントの構築、そして社内規程の整備など、これまで企業内でブラックボックス化してきた部分の統制、つまり全社的 (総務系) な統制が主であり、決算上の統制とそれに繋がる業務プロ

セスを統制することは、内部統制の一部でしかないのである。

従って、業務プロセスにあたる主要業務工程と業務プロセスを円滑にする実現するための規程、基準、標準など支援工程から構成される ISO9001、ISO14001と ISO/IEC27001のマネジメント手法を理解することは、内部統制の真髄を理解し、円滑に実施するために非常に有効な手段であると思われる。(図表3 内部統制と ISO との共通性2)

さて、A社では、平成20年4月の人事異動では、ISOの認証維持活動と内部統制維持活動を同一セクションに集約するほか、内部監査セクションを新設し、ISO上の内部監査と内部統制上の内部監査を統合し、ムリ・ムラ・ムダのないシステムに移行する計画である。

【5】 おわりに

内部統制導入後の中小企業におけるリスクマネジメントの重要課題は、コンプライアンスを中心とする社員教育であると思われる。同時に、未だ ISO9001や ISO14001の認証を受けていない上場企業および連結子会社、関連企業の場合は、認証取得に向けて取り組むべきである。

内部企業に求められる内部統制の枠組みは、「財務報告」、「業務プロセス」そして「法令遵守」に他ならない。そのうち「業務プロセス」と「法令遵守」は、法により規制されているわけではなく、企業として独自の取り組みに委ねられている。特に、経理部門や総務部門といった法規関連部署は、長らく企業のブラックボックスとなっており、企業不祥事の温床となっている事例が多く存在する。これらにメスを入れる内部統制制度に対し、法規制に最低限のレベルで対応するのか、これを機会として組織運営力を積極的に高めていくのかは、まさに企業の力量であり、企業が社会的存在であることを経営層が真に理解しているかをはかるものさしとなるといえる。

また、ISO 認証取得企業における今後の維持活動は、内部統制活動との融合をはかり、同一の価値観と視点で行ってゆく必要がある。複数の ISO 維持活動に対し、複数の部門が関与し、

また、内部統制活動に別の部門を設立するといったことは、株主利益の保護と顧客満足度の向上、そして公共の利潤を追求する企業にとっては高コスト体質を築いてしまう原因になると思われる。

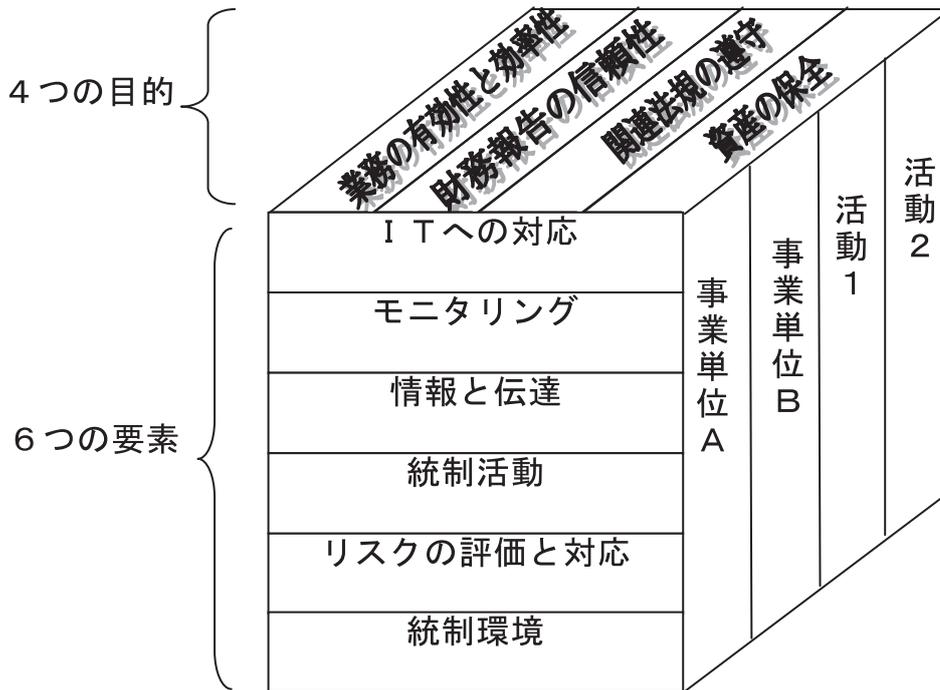
なお、ISOの認証取得に至っていない中小の上場企業は、ISOのいずれかの認証取得に向け取り組むことにより、潜在するリスクの評価とその改善策に自ら取り組まなくてはならず、日本企業の風土に馴染みの薄かったリスクへの予防策を事前に講じることができるようになるため、果敢に取り組むことを切望するものである。

最後に、上場する中小企業の今後のあり方は、コンプライアンス教育を柱に、内部統制と ISO 維持活動を統合したエンタープライズマネジメントを実践することにより、ステークホルダーを意識した透明性の高い経営を行い、社会的存在者として企業統治を強化することであると当グループは提言するものである。

【参考文献・データ出典】

- ・『対訳 ISO9001:2001 品質マネジメントの国際規格』日本規格協会 (2001)
- ・『対訳 ISO14001:2004 環境マネジメントシステム』日本規格協会 (2005)
- ・『対訳 ISO/IEC27001:2005 情報セキュリティマネジメントシステム』日本規格協会 (2006)
- ・監査法人トーマツエンタープライズリスクサービス 監修：久保恵一 著：野坂晃史、仁木一彦、三好直樹『図解一番はじめに読む内部監査の本』東洋経済新聞社 (2007)
- ・平松 徹『これでわかる会社の「見える化」と攻めの内部統制』週刊住宅新聞社 (2007)
- ・京セラコミュニケーションシステム株式会社「イソロジー2006年9月28日発行」〈http://www.kccs.co.jp/sp_issue/060928.html〉(2007/6/3アクセス)
- ・株式会社システム規格社「アイソス2007年11月号」
- ・株式会社マネジメントセンター「マネジメントニュース2007年4月号」〈<http://www.isommc.com/05news/05pdf/200704.pdf>〉(2007/11/2アクセス)
- ・日本ヒューレット・パカード株式会社「財務報告に係る内部統制の評価」〈<http://h50146.www5.hp.com/solutions/infrastructure/compliance/sox/eval.html>〉(2007/11/2アクセス)
- ・株式会社メディア総合研究所「SOX法と内部統制」〈<http://www.j-sox.net/>〉(2007/11/2アクセス)
- ・平林公認会計士事務所「内部統制とは」〈<http://www.naibutousei.info/>〉(2007/11/2アクセス)

【図表1】日本版SOX法COSOフレーム



参照：<http://www.j-sox.net/ARCHIVE/200606/index.html>

【図表2】 内部統制とISOとの共通性 1

6つの基本要素	ISO 9001	ISO 14001	ISO 27001
統制環境 組織の気風決定、統制に対する意識に影響を与える、他の基本要素の基礎	5.1 経営者のコミットメント 5.3 品質方針 5.4.1 品質目標 5.5.1 責任及び権限 5.6 マネジメントレビュー 6.2 人的資源	4.2 環境方針 4.3.3 目的、目標及び実施計画 4.4.1 資源 役割 責任と権限 4.6 マネジメントレビュー	5.1 経営陣のコミットメント
リスクの評価と対応 組織目標の達成を阻害する要因をリスクとして識別、分析、評価	8.5.3 予防措置	4.3.1 環境側面 4.4.7 緊急事態への準備対応 4.5.3 不適合並びに是正処置、 予防処置	8.3 予防処置
統制活動 経営者の命令、指示が適切に実行されることを確保するために定める方針、手続	4.1 一般要求事項	4.1 一般要求事項	4.1 一般要求事項
情報と伝達 必要な情報が識別、把握、処理され、組織内関係者相互に正しく伝えられる	5.5.3 内部コミュニケーション	4.4.3 コミュニケーション	
モニタリング 内部統制が有効に機能していることを継続的に評価	5.6 マネジメントレビュー 7.5.3 識別、トレーサビリティ 8.1 一般 8.2.1 顧客満足 8.2.2 内部監査 8.2.3 プロセス監視、測定 8.2.4 製品監視、測定 8.3 不適合製品管理 8.4 データ分析	4.5.1 監視、測定 4.5.3 不適合並びに是正処置 予防処置 4.5.5 内部監査 4.6 マネジメントレビュー	4.2.3 ISMSの監査及びレビュー 6 ISMS内部監査 7.1 一般 7.2 レビューへのインプット 7.2 レビューへのアウトプット 8.1 継続的改善 8.2 是正処置
ITへの対応 組織内外のITに対して適切に対応するIT環境への対応とIT利用、統制からなる	6.3 インフラストラクチャー		4.2.1 ISMSの確立 4.2.2 ISMSの導入及び運用

【図表3】内部統制とISOとの共通性2

