アシスト

SEP/OCT 2008

特別寄稿

『リスク過敏の内部統制はこう変える！』

■内部統制の大事なポイント

内部統制と言うと、これまで、教育機関において財務会計分野の監査論の一部としてしか扱われてこなかったため、専門家の中にも「内部統制は監査論の一部の特殊分野だ」と勘違いされている方も残念ながら多くいます。しかし、内部統制は単なる財務会計の話ではなく、経営活動そのものを反映する広い概念です。皆様がご存知の日本版COSOモデルを見ても、内部統制には4つの目的があります。①「業務活動の有効性／効率性を高める目的」ではこれまでの改善活動や製造工程における不良品発生率の低減等が該当、②「財務報告の信頼性を高める目的」では、特にJ-SOX対策で求められる粉飾決算がないようにする会計面での対応が該当、③「法令を遵守する目的」では、身近なところで言えば個人情報保護法のマネジメント・システムを確立するPマークも、職場の安全配慮義務の観点からOSHASも該当、④「資産の保全という目的」においては、ヒト／モノ／カネ／情報を保全する様々な活動（例えば、BCM：事業継続性マネジメント）が該当します。つまり、これまでの固定概念よりはるかに幅広い、組織横断的な全社的プロジェクトとして対応すべき問題です。具体的に言えば、ISOをはじめとする規格マネジメント・システムは、日本版COSOモデルのそれぞれの目的や要素を埋めてきたというように見ることができます。

業務活動の有効性／効率性を高めるためのISO9000や、製造工程における極限まで不良品発生率を低減する6シグマは、まさしく内部統制の業務活動に関する目的を達成するためのものです。また職場の労働環境安全配慮義務の観点からは、OSHAS（労働安全に関する規格マネジメント・システム）や、個人情報保護法（Pマーク）としてJISQ15000等が、法令遵守の目的に合致しています。また資産の保全では、会社の資産や環境における資源という観点からISO14000（環境）、事業継続性マネジメントとして会社の資産（ヒト／モノ／カネ／情報）を保全して継続的に事業を行うためにはBS25999（BCM規格マネジメント）等があります。またＩＴにフォーカスすると、おなじみのＩＳＭＳ／ISO27000や、ITIL／ISO20000やCOBIT等が、ITへの対応という構成要素を担ってきました。

広範な対象を含む内部統制における重要なポイントを一言で述べるなら、「当たり前のことを当たり前にやる」ということに尽きます。しかし、この一見ごく単純な一言も、現実の社会で実行することは難しいようです。不祥事が起きている背景として、「業界の当たり前」は、内部統制の目的の1つである法令遵守の観点からは、もはや「社会の非常識」になっている点です。ミートホープ社や飛騨牛をはじめとする食肉偽装問題も、「業界ではこれくらい当たり前だよ、他社でもやっているよ」という言い訳がむなしく響きわたる記者会見に辟易された方も多くいらっしゃるかと思います。環境偽装として再生紙の含有率とその表示を巡る問題では、大手製紙会社十数社が一斉にマスコミに取り上げられ、もはや業界の常識は法的観点から通用しないものとして業界全体を揺るがす問題として露

日本マネジメント総合研究所　理事長
岡山大学大学院非常勤講師
公認不正検査士（CFE）
戸村　智憲　氏

呈しました。耐震偽装問題も、あるマンションで鉄筋が何本足りないとか、計算書の偽造など、これまで見過ごされてきた業界の常識が、改めて問われる状況になっています。

こういった問題を起こした企業の中には、社是に「我が社はお客様に最高の品質／サービスを提供します」というような文言を掲げている企業もあり、社是が現場や現場の判断に徹底されない状況は、もはや経営偽装と呼ばざるを得ないでしょう。内部統制は、経営理念／社是から導かれる戦略／業務活動の裏側にある障害／阻害要因（リスク）をいかに管理するかというところに行き着きます。つまり、内部統制の出発点は、自社は何を志向し何を是とし非とするのかという経営理念／社是であり、戦略／業務活動と共にリスク管理をいかに一体のものとして経営理念／社是に基づいてブレなく効果的かつ効率的に貫徹するかに尽きる「ミッション経営」なのです。

■内部統制における「当たり前」：七文字式内部統制

さて、内部統制における「当たり前」についてですが、詳細を事細かに提示しても、現場で混乱するばかりか、形式的な文言が参照／適用されない紙爆弾として存在するだけになる可能性があります。そこで私は7文字の原則だけを守っていただければ内部統制の問題が起きない、逆に、7文字の中で1文字でも欠けると内部統制上の問題になるという「七文字式内部統制」を提唱しています。その7文字とは3つの「正」の文字と「適時適切」の4文字です。具体的には、「正直に」「正確に」「正式に」対応することを「適時適切」に行えば良いということです。「正直に」：嘘をついたり隠蔽したりしないで、「正確に」：どの工程、どの活動にどのくらいリスクがあり、そのリスクが発生した場合にどのような重要性のある問題がどのくらい発生するのかについて正確に把握／情報開示すると共に、「正式に」：一般法規や社内規程や官公庁のガイドラインに沿って正式な対応を、「適時適切」に行う、ということです。1つ目と2つ目の「正」が欠けた不祥事の例として、賞味期限偽装や産地偽装という「正直」かつ「正確」な対応を怠った食肉偽装問題が挙げられます。3つ目の「正」が欠けた例として、原子力発電所で、官公庁や社内のガイドラインやマニュアル等に「正式に」従わず、「これくらいはいいか」と安易に作業の手抜きを行って、バケツで核物質を容器に入れ替えたところ、臨界事故を起こしてしまった例が挙げられます。この例では、まさしく、内部統制に沿って仕事をしていれば健全かつ安全に働き続けることができたものを、内部統制をないがしろにした結果、社員も近隣住民も被爆や原子力の不安に直面することとなった例と見ることができます。つまり、内部統制は、社員や地域住民を守るための重要な問題であるということが明確になった例と言えそうです。では、事故や問題が起きた際に、「正直に」「正確に」「正式に」対応していたものの、その報告が官公庁や業界団体への報告期間を大幅に過ぎた2年後だとすれば、果たして、内部統制がきちんとできていると言えるかといえば、答えはNOです。つまり、定められた期間内に適時な

特別寄稿

『リスク過敏の内部統制はこう変える！』

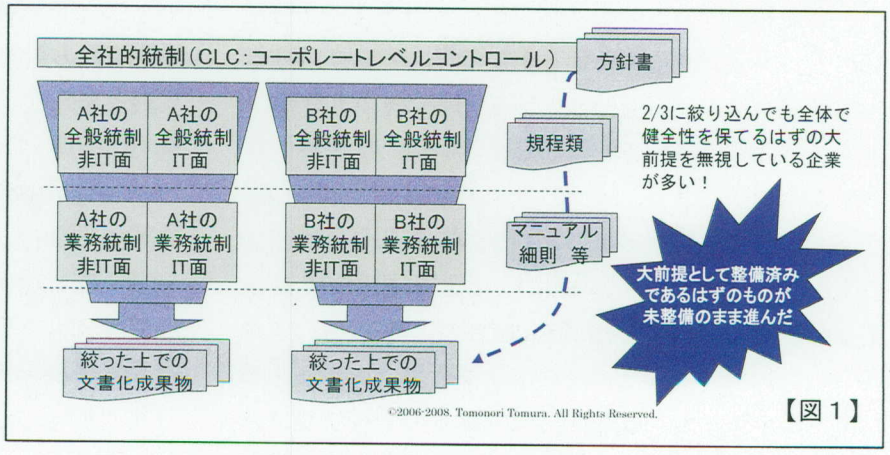
対応を、適切な内容やフォーマットをもって行うことが必須なのです。内部統制を現場まで浸透させるのには、やたら難しい用語を詳細に並べ立てるのではなく、内部統制の思考軸となる七文字式内部統制を徹底することが、内部統制の形骸化を防ぐ上で必要なのです。

■内部統制のリスク過敏症に陥るのはなぜ？

全国各地でコンサルティング／相談会／講演等を行う中で、多くの企業がリスク過敏症に陥っているように見受けられます。文書化やアセスメントを経て、たくさんのリスクを前にして途方に暮れていらっしゃる企業も多い中で、コンサルタントや監査法人のアドバイザリー・サービスは一体何をしているのかと不思議に思う場面に出くわすことも多々あります。何をどこまでやればいいのか、全く見当もつかず、コンサルタントやアドバイザリー・サービスの公認会計士に尋ねても確たる答えやヒントすら見つからないというような企業も残念ながら散見されます。

さて、ここで、私からの質問です。「いきなり文書化から始めませんでしたか？」「日本版COSOモデルは知っていても、その論理的な手順に従って内部統制の構築／運用を行っていますか？」

内部統制は日本版COSOモデルに従えば、実は非常に単純です。構成要素の上から順に構築／運用すれば良いだけです。そして、キーポイントが、第2番目の構成要素である「リスクの評価と対応」です。具体的には、構成要素の上から順に、①統制環境の整備として内部統制教育／規程類の整備などで、何をして良くて何をしてはならないかという判断軸を明確にする。②文書化やアセスメントであぶり出されたリスクについて、重要度と発生可能性からリスクの重み付けを行い、それぞれ重み付けされたリスクへの対応策を決めていく、つまり、このリスクはそもそも発生しても非常に軽微なリスクなので切り捨てる（受容する）とか、このリスクは逆に非常に重要なので、重点的に統制をとる、というように割り振り、なぜそう考え、そう主張できるのかという思考プロセスを示す。③実際に統制活動を行う。④情報と伝達において内部統制の報／連／相をきちんと行う。⑤それらがきちんとできているかをモニタリング（チェック）して問題があれば改善する。⑥最後に日本版COSOモデルで付け加わったITへの対応として、IT自体が健全であることと、そのITを用いて内部統制を強化するという観点から全体を見直す。ここで、②のリスクの評価と対応は、何もお金をかけなくても、A3用紙縦1枚でできます。A3用紙の上半分にリスクマッピング（リスクの影響度と発生可能性からリスクの重み付け／優先順位付け）をして、下半分にプロットされた各リスクの対応策をそ



【図1】

戸村 智憲 氏　略歴

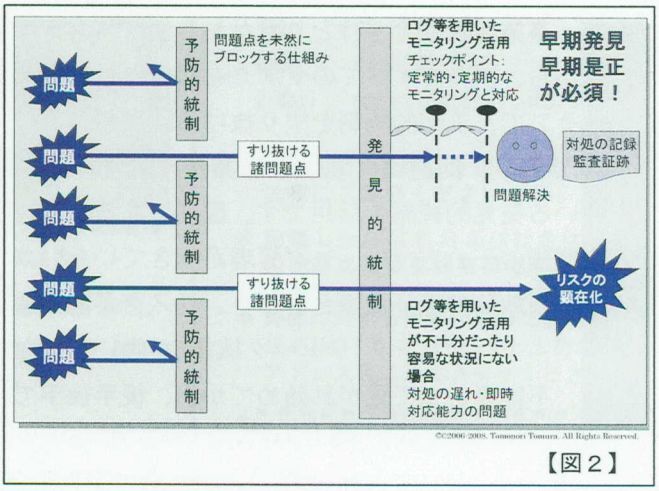
早稲田大学卒。米国ＭＢＡ 修了。国連にて内部監査業務ミッション・エキスパート、国連戦略立案ミッション・エキスパート・リーダー等を経て、民間企業では企業役員として内部監査を担当。内部統制・ＳＯＸ 法対策のエキスパート資格である公認不正検査士（CFE）を取得。J-SOX 対応促進協議会顧問に招聘される。2006 年７月１日（於：甲南大学）に管理会計学会にてSRB スコアカード（通称：COSO-ERM 志向の内部統制対応型第４世代BSC）を世界初で発表。ERM やAfter J-SOX の実践手法を先駆けて開発・発表。日米の各メディアにて論文・記事等の掲載多数。内部統制の最先端の研究で注目されている。岡山大学大学院非常勤講師として内部統制／ＥＲＭ を担当し、産学両面で活躍中。

の根拠／判断の思考過程とともに箇条書きで示し、何から着手するかを明示するだけでリスク過敏症は防げます。これは今から活用しても遅くはありません。

現在多くのコンサルタントや公認会計士が、米国版SOX 法のテキストを基に、日本版SOX 法対策を十分理解できていない状況で各企業で指導されたりしているため、過剰に網羅性に縛られてリスクを洗い出したり指摘したりするのに躍起になっているようです。日本版SOX 法対策は、あくまでも重点的な内部統制をベースにしているので、米国式の内部統制対策のように、とにかく文書化で現場のリスクを90 ～95% 洗い出せばいい、というようにはいきません。図１のように、本来は全社的統制や全般統制で全体の健全性をある程度確保した上で、絞ったスコーピングで文書化するはずが、実施基準の2/3 基準という数字だけがひとり歩きして、全社的統制／全般統制が後付けという不健全な対応を余儀なくされている、または、不健全であることを意識することすらなく文書化から始めることが当たり前だと思ってしまっている企業も多く見られます。

■内部統制＆善管注意義務における「当たり前」の８文字：「早期発見／早期是正」

ところで、J-SOX 対象企業とその子会社、関連会社においては、文書化３点セットはすでに終了し、ドライラン（仮想監査）の指摘事項を基に改善を進め、内部統制の運用／評価において万全を期している企業が多いかと思われます。しかし、ここでも「当たり前」のことが当たり前にできていない状況が散見されます。具体的には、ログの取りっ放しで管理ができていなかったり、そもそも、十分にログすら取れていない、あるいは、お金



【図２】

がかかるのでログは必要ないと根拠なき自信の下に対応を拒んでいるといったケースです。内部統制においては、トレーサビリティを保つためにレコード・マネジメント、つまり、いつ誰が何をどのように行ったためどのような問題が生じているかについて、US-SOX でもJ-SOX でも「最後の砦」となる発見的統制が欠落している企業が多いのには非常に驚かされます。内部統制においては、図２のように当たり前のこととして、予防的統制（入口：物事が起こる前に水際で予防する統制活動）と発見的統制（出口：物事が起こった際にいかにダメージを最小化し、元のレベルまでいかに早期に復旧するかという統制活動）の２点から、入口と出口をしっかり締める対応が必要不可欠です。

図２にあるように、様々な問題に対して、まずは、水際作戦として予防的統制で問題をはじきます。例えば、アクセス管理（許可されていない人のアクセスを予防）や入退室管理（入室許可されていない人の入室を予防）や職務分掌（購買と支払の担当者を別々にして買った＆支払ったことにして着服するのを防ぐ牽制機能としての予防）などで、入口をしっかり締めます。

特別寄稿

『リスク過敏の内部統制はこう変える！』

しかし、事業を行うことはとりもなおさずリスクテイクですから、入口ですべてのリスクをゼロにはできません。そこで、予防的統制をすり抜ける諸問題が出てくるのですが、問題は、多くの企業が手薄な状況になっている発見的統制の活用です。図2にあるすり抜ける諸問題の下の方では、ログ管理ができていないログの取りっ放しのような場合であり、リスクが顕在化するまで、モニタリング(チェック機能)が働いていないため、不祥事として騒がれ始めてから、後手後手で過去のログをチェックするような対応が強いられます。

一方で、図2のすり抜ける諸問題の上の方では、ログの取りっ放しではないログ管理(ログに関するPDCAサイクルを回している)で、ログを定常的にモニタリングして問題やポリシー違反行為を早期に発見し、問題がある場合には早期に是正することで問題を最小化すると共に、不祥事／不正で足下をすくわれないで健全な経営を継続する体制が取れている状態です。

監査法人によっては「ログは月に1回くらい見ていればいいですよ」と助言をしているところもありますが、ログのポリシー違反で実際に不正が起きた場合、月に1回のチェックでは、月間の膨大なログをチェックしきれず、いい加減な対応や不正の見落としにつながります。ここで、早期発見／早期是正をキーワードに挙げていますが、これは、つまるところ、企業として善良なる管理者としての注意義務を果たすためには、仕組みとして問題を早期発見／早期是正できる、つまり、ログで言えば取りっ放しではなく、常にチェックし、問題があればアクション(改善／是正)できる状況でなければ善管注意義務を果たせているとは言えないためです。これは、ある大手印刷会社で860万件を超える個人情報の漏洩事件があった際、やはり、ログのチェックが月1回だけで不正や不正の兆候を見落として大きな問題になった実例を参考としていただければ、容易にご理解いただけるのではないでしょうか。もちろん、ログの管理にも大変な工数がかかります。その点は、アシストが取り扱う、ログのポリシー違反から対応／是正までの対処記録を監査証跡として書き換え不可の状態(WORM)で残せる「監査れポータル」等を検討されてもよいでしょう。

■まとめ

繰り返しますが、内部統制は財務会計分野の監査論の特殊論ではなく、企業がもっと健全に儲け続けるための仕組み／システムです。リスク過敏症に陥る必要もなく、日本版COSOモデルに沿って構成要素の上から順に論理的に対応するだけで良い、実にシンプルなものです。また当たり前のこととして、予防的統制の整備／運用と、発見的統制として定常的なモニタリングで問題の早期発見／早期是正を果たせる仕組み作りが必要であるということを押さえていただき、日本版SOX法対策における重点的な統制に基づいて、軽微／微小なリスクに怯えることなく、かといって、監査法人からの指摘を無視せず、自社としての内部統制の論理を持って落としどころをつける健全な内部統制の構築／運用にあたっていただければ幸いです。

本稿でお伝えし切れなかった点につきましては、拙著『リスク過敏の内部統制はこう変える！』(出版文化社)をご覧ください。