SOX法対応を超えた実効性ある内部統制の構築

「オペレーショナライジングERM」の実現に向けて

能勢幸嗣 
宗　裕二 
エリック・ファンドリッチ 

CONTENTS

要約

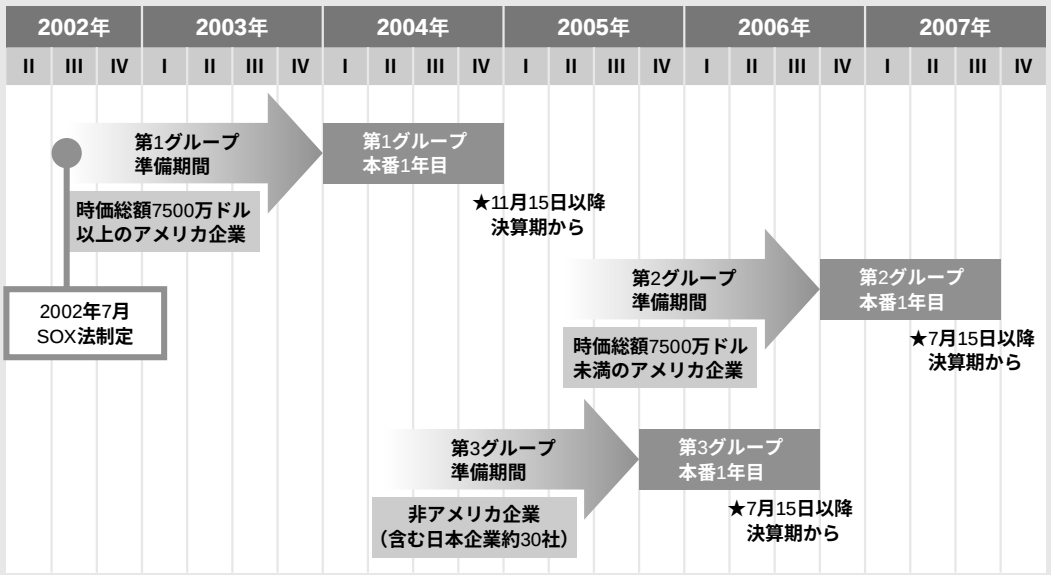
1　アメリカでは、企業のSOX法（企業改革法）対応に時間とコストがかかっているが、資本市場からの信頼を回復するまでには至っていない。その原因は、「経営者の不十分な関与」と「運用（継続的な内部監査と業務改善）についての意識欠如」にあると考えられる。

2　日本でも、SOX法に相当する法律が、今年度に金融商品取引法の一部として法制化される予定であり、多くの企業が取り組みを始めている。しかし、SOX法対応の「手順」だけを追っている企業が多く、アメリカ企業と同じ課題に直面するものと思われる。

3　先進企業の取り組みなどを参考にすると、SOX法対応を単なる法対応に終わらせないためには、①経営システムへの組み込み、②IR（投資家向け広報）を活用した経営トップの目標管理、③IT（情報技術）を活用した内部監査支援および継続的な業務改革の発展――などが必要と考えられる。特に、外部および内部監査の人材が不足する日本では、ITの活用は不可欠ともいえる。

4　競争環境の不確実性が高まるにつれ、経営戦略までを踏まえたERM（エンタープライズ・リスクマネジメント）が重要になる。SOX法対応にとどまらず、法律・規制に係るホリスティックコンプライアンス（全体総括的管理）、ERMへと、「内部統制・リスク管理」を発展させていく必要がある。そのように考えるなら、「内部統制・リスク管理」は経営モデルの変革そのものである。

図1　アメリカのSOX法（企業改革法）適用スケジュール



Ⅰ　SOX法制定後も信頼を得られないアメリカ企業

アメリカでは2002年７月、企業改革法（サーベンス・オクスリー法、略称SOX法）が、エンロン事件、ワールドコム事件に代表されるような不祥事を防ぎ、企業の資本市場、投資家からの信頼を回復すべく、制定された。

SOX法では、SEC（証券取引委員会）に登録している約１万5000社が規制の対象となっている。その施行タイミングの関係から、2004年11月15日以降に決算期を迎えた大企業約3000社が、内部統制に関する１回目の報告を終えた段階である（本号が刊行される３月下旬には、２回目の報告が終わっていると考えられる）。図１に示すように、ニューヨーク証券取引所などに上場する日本企業は、第３グループとして、2006年度決算から報告が必要であり、現在最後のリハーサル（文書化、統制評価）に追われている。

「SOX法対応」と一言でいっているが、今巷をにぎわしているのは、全体で11章69条あるSOX法のうち、第404条の部分である（図２）。第302条対応で、経営者が財務報告

図2　SOX法の構成

第1章　PCAOB（公開会社会計監督委員会）	
第2章　監査人の独立性	
第3章　企業の責任	〈宣誓〉 第302条 CEOおよびCFOには、四半期報告、年次報告のたびに報告内容に間違いがないことを保証し、宣誓することが義務付けられる
第4章　財務情報開示の強化	
第5章　証券アナリストの利益相反	〈証明〉 第404条 内部統制の整備状況と運用状況に関する報告書を、年次財務報告書と一緒に提出することが義務付けられる
第6章　証券取引委員会の財源と権限	
第7章　調査および報告	
第8章　企業と犯罪的不正行為に対する説明責任	
第9章　ホワイトカラー犯罪に対する罰則強化	〈罰則〉第906条 意図的な違反があった場合、CEOおよびCFOに対して20年以下の禁固刑または500万ドルまでの罰則、ないしはその両方が科される
第10章　法人税申告書	
第11章　企業不正に対する説明責任	

注）CEO：最高経営責任者、CFO：最高財務責任者

について内容に間違いないことを「宣誓」することとなっているが、第404条はその「証明」に相当する部分である。SOX法には詳細な方法は記載されておらず、SECの作成したルールや、PCAOB（公開会社会計監督委員会）の出している「財務報告に関する内部統制監査基準２号」が、実務指針として詳細を定めている。

SEC登録企業は、それらの実務指針を解読しながら第404条対応の準備を行っているが、統制の文書化や内部監査の社内人員増強、コンサルティング会社への委託、監査法人への支払いに多額の費用がかかっており、ある調査によれば、売上高の約0.1%のコストを要しているといわれる。筆者らはこの数字をもとに、複数のアメリカ企業と議論したが、どの企業からも一様に経済的費用以上の疲弊感、徒労感が伝わってきた。

それなりの人員を投入し、コストをかけて対応しているにもかかわらず、多くの企業が財務諸表に関する内部統制に重大な欠陥があると報告している。大手監査法人のデロイト・トウシュの調査によると、2005年８月11日時点で年次報告を提出した3197社のうち、13%に当たる416社の財務諸表に関する内部統制に、重大な欠陥の記述があった。

さらには、重大な欠陥が存在するだけでなく、大きな不祥事が発生した。アメリカの商品取引会社レフコにおいて、関係会社への不正融資、それに伴う不良債権隠蔽という大掛かりな粉飾事件が発覚したのである。この不正が発表され、経営トップが起訴されて、株価が暴落し、経営が破綻した。

この事件で何よりも衝撃を受けたのは、レフコは2005年８月にニューヨーク証券取引所に上場したばかりで、上場から２カ月しか経過していないことである。上場に当たって、2005年２月決算を踏まえた目論見書には、内部統制に重大な欠陥があることが明記されている。にもかかわらず、外部監査人によって不正が発見されず、取締役会でも内部統制の重大な欠陥が修正されていない。そして上場審査を通過している。

このようにSOX法が制定され、多くの企業がその対応に時間とコストを割いているにもかかわらず、資本市場から信頼を得るまでには結びついていないのが現状である。

II　アメリカにおけるSOX法対応の問題点

SECやPCAOBの各種資料の分析や、SEC登録企業へのヒアリングによれば、「経営者の不十分な関与」と「運用（継続的な内部監査と業務改善）についての意識欠如」が、SOX法対応を不完全なものにしている。

1　経営者の不十分な関与

2005年４月13日、SECラウンドテーブルが、民間企業、監査法人、機関投資家、PCAOBメンバーなどの参加のもとに開催され、SOX法第404条対応についての反省や、今後の対応についての議論がなされた。そこにおいて、トップダウンでのリスクアプローチを採用しなかったこと、監査法人と十分なコミュニケーションがとれていなかったこと、IT（情報技術）への理解が不十分であることなど、「経営者」の関与が浅いことが指摘されている。

筆者らが訪問したSEC登録企業の中でも、

SOX法第404条への対応がスムーズに終わった企業は、トップダウンでのコーポレートガバナンス（企業統治）や内部統制に対する考え方が徹底しており、執行役員レベルでも担当部門のリスクなどについて優先順位付けがしっかりと行われていた。逆に、スムーズに終わっていない企業は、大抵、ボトムアップ的にひたすら文書化対応を進めており、経営トップの関与が不十分であると感じられた。

そもそも、SOX法制定以前に内部統制について評価が行われていなかったわけではない。監査法人は、財務諸表上のどの点について精査すべきか濃淡をつけるために、内部統制の評価を行ってきた。ただし、そのような評価では、エンロンやワールドコムのような大きな不正・不祥事を未然に防ぐことができなかった。そのため、監査法人が評価を行う前に、「経営者自ら」が内部統制について評価・報告を行うことを法制化したと理解することができる。

アメリカでも、SOX法だけでなく、愛国者法や、情報セキュリティの国際認証規格「ISO27001」、事業継続管理のための指針「PAS56」など内部統制に関する法律や規則・付則が存在する。内部統制の主体が経営者自身であり、そのことがしっかりと理解されていれば、内部統制に関する同様の法律について、その相違点、共通点などを議論し、全体総括的な取り組みが検討されるはずである。

イギリスのCSFI（金融イノベーション研究所）が2005年に行った調査によれば、リスクが高いと認識される課題の１位に「多すぎる規制」がランキングされている。2003年の調査で６位だった項目がトップになったわけだが、実際は2000年から2005年にかけて金融機関のコンプライアンス（法令遵守）対応コストは50%程度増加している。

経営者は、内部統制やコンプライアンスについて問題意識は持っているが、いまだに主体的な取り組みが不足しており、結果として内部統制に関する同様の法律・規制に対してサイロ型、つまり法律ごとに個別対応しているのである。

2　内部統制の運用面についての意識欠如

２つ目の大きな問題点は、内部統制体系の評価・報告・更新といった運用面を意識している企業が少ないことである。

この１年ほど、複数のSEC登録日本企業と継続的に議論を行っている。それらの企業で、SOX法第404条対応の準備が終了し、本番年に近づけば近づくほど、運用に関する問題意識が高まってきている。特に顕著な問題意識としては、以下の２点があげられる。

（1）重要なリスクを論理的に説明できない

「大量の業務フローやリスクコントロール・マトリックスは作成したが、それらを経営トップの視点でながめて、何が重要なリスクなのかを論理的に説明することができずに困っている」

この企業の場合、最初にSOX法第404条対応プロジェクトの手順を決めると、適宜経営を巻き込んで報告・議論することなく、文書化にとにかく邁進してしまっている。そのため、何百枚という業務フローと数千というリスク項目、およびそれに対応する統制項目が抽出されたが、最後の「報告」という手順に

ついての意識が不足している。

（2）運用を想定した仕組み、経営資源が不足している

「文書化は終了したので、来年度以降、内部監査を中心に運用していく。しかし、内部監査で評価した結果、統制に問題点があった場合、誰が主体的に改善に取り組むのか、またその改善状況を把握する部署が不明確なままで困っている」

多くの企業の場合、SOX法対応を委員会またはタスクフォースといった時限的組織で行っているが、その時限的な特性から、準備が終了すると解散してしまう。その後、内部監査部門が統制の不備を発見した場合、内部監査部門は助言・アドバイスを行うことはできるが、主体的に改善を主導することができない。そのため、改善を主体的に主導する部署が必要なわけだが、多くの企業の場合、内部統制についての改善を主導する役割を明確に決めていないようである。

図3　アメリカのSOX法と日本版SOX法との差異

SECラウンドテーブル（2005年4月13日）	金融庁企業会計審議会（2005年12月8日）
トップダウンおよびリスクアプローチの不採用	トップダウン型リスクアプローチの採用
評価対象範囲の絞り込み不足	内部統制の不備の区分
財務監査と内部統制監査の統合が不十分	ダイレクトレポーティングの不採用
経営者のITに対する理解が不十分	内部統制監査と財務諸表監査の一体的実施
経営者と監査法人とのコミュニケーションが不足	内部統制監査報告書と財務諸表監査報告書の一体的作成
	監査人と監査役、内部監査人との連携

注）IT：情報技術、SEC：証券取引委員会

このことはさらなる問題へと発展する可能性がある。なかには、SOX法対応と業務改革を同時に進めることが難しいので、SOX対応の準備期間中は業務改革を一時中断する企業もあった。そのような企業が業務改革やシステム見直しに着手するとき、SOX法対応の業務フローやリスク、統制を文書化したものを、誰が更新・管理していくのかが問題である。更新を主管する組織の不在という問題に加え、業務フローやリスク・統制を文書化する段階で、「更新」ということを前提とした作成方法、ツールが選定されていないことにも問題がある。

III　日本版SOX法

1　法制化の動向

日本でも、SOX法に相当する法律が、金融商品取引法の一部として2006年の通常国会で議論される。その法律は、アメリカのSOX法への企業や監査法人の対応状況の反省を踏まえ、作業面の軽減がなされているといわれる。しかし、内容を見る限り、外部監査法人の対応負荷が軽減するだけで、企業の対応負荷にはほとんど変わりがないように感じられる。

金融庁企業会計審議会が2005年12月８日に発表した、日本版SOX法の基準案ともいえるものは、SECラウンドテーブルなどで議論されたSOX法第404条対応の反省点などを活かしたものとなっている（図３）。リスクアプローチの採用、内部監査と財務諸表監査の一体化、ダイレクトレポーティングの不採用などである。

確かにリスクアプローチについては、総花

的にリスクに対応するのではなく、企業ごとのリスクの重要性に基づいて絞り込まれたリスクを評価し、対応策を検討するようになっており、これは企業の作業負担を減らすものと期待できる。しかし、それ以外の項目については、外部監査法人の負荷は軽減すれど、企業内部の負荷まで軽減するような策であると読むのは難しい。

2　懸念される問題

昨今、SOX法第404条対応に関する書籍が刊行され、セミナーなども多く開催されている。そのなかで、前述のような法制化の動きや、実際の第404条対応の「手順」が説明されているのをよく見かける。野村総合研究所でも、上場企業約2400社を対象に、SOX法、日本版SOX法および内部統制について調査した（詳細は本号の「SOX法に関する日本企業の課題と対応方策」を参照）。

そこでも、「文書化の負荷」についての企業側の認識は高く、書籍やセミナーなどで十分な刷り込み活動が行われた成果であると感じた。確かに文書化の負荷は大きく、かつ重要な作業ではあるが、それは本質的なものではない。日本版SOX法対応でも、アメリカのSOX法対応と同様に、経営者の姿勢と統制の運用（継続的な内部監査）が重要な課題であると考えられる。

日本でも、経営者こそが内部統制の重要な要素であることは、過去に発生した不祥事の分析からも明らかである。2005年７月13日、金融庁企業会計審議会から日本版SOX法の公開草案とも呼ばれるものが提示された。実は同日、経済産業省から、「コーポレートガバナンス及びリスク管理・内部統制に関する開示・評価の枠組について――構築及び開示のための指針（案）」が提示されている。

この中で、過去の大きな不祥事24件について、「コーポレートガバナンス」「内部環境」「リスクの認識・評価」「リスクへの対応」「情報と伝達」「統制活動」「監視活動」の７つの角度から、原因の分析が行われている（表１）。それを見ると原因はさまざまだが、「コーポレートガバナンスにおける問題及び内部環境に関する問題（その中でも特に行動規範に関する問題）において企業に何らかの問題があったことが、多くの不祥事発生及び発生後の重大な損害の拡大の重要な原因となったのではないかと考えられた」と報告書は

表1　企業不祥事の原因

視点	具体的な原因
コーポレートガバナンス	●良好な企業風土の崩壊 ●企業経営者のリスクの認識の欠如に対する取締役会の監督不備 ●企業経営者の専門性の不足に対する取締役会の監督不備 ●監査役、外部監査人の独立性の欠如などに起因する監視・検証の不備
内部環境	●行動規範に関する問題 法令遵守などに係る社風形成、行動規範の未確立 目標達成圧力に起因する違法行為 ●職務権限に関する問題 職務権限の範囲が不明確 スタープレーヤーへの過度の依存
リスクの認識・評価	●複雑な取引に対する理解の欠如 ●社会に与える影響の認識、考慮が不足 ●他事例の教訓に対する考慮が不足
リスクへの対応	●不適切な子会社管理 ●安全・倫理的行動を優先しない姿勢
情報と伝達	●通報者保護の不徹底といったヘルプラインの不適切な運用 ●危機発生時の情報伝達経路の不備などによる被害の拡大
統制活動	●マニュアル運用の形骸化 ●管理階層による担当者層への統制の不備 ●ITに関する統制の不備
監視活動	●内部監査の対象外 ●専門性を有し、かつ業務執行ラインから独立した内部監査機能の不在

出所）経済産業省企業行動の開示・評価に関する研究会「コーポレートガバナンス及びリスク管理・内部統制に関する開示・評価の枠組について――構築及び開示のための指針（案）」2005年7月より作成

まとめている。

カネボウ、西武鉄道、ライブドアなど、どの案件を見ても「経営者の不正」が直接的な原因である。また、大和銀行、カシオ計算機にしても、経営者が専門性の高い現場の業務とそのリスクを理解できないことに問題があった。やはり、経営者が鍵を握っている。

また、日本版SOX法だけでなく、新会社法、金融庁確認書など、財務諸表に関する内部統制強化についての法律・規制も制定されている（表２）。そのどれにも共通するのは、経営者を主体者として定めていることである。互いにきわめて類似している法律・規制であり、日本においてこそ経営者の全体総括的な取り組みが必要とされていることの現れと考えられる。

経営者が主体的に内部統制に取り組むべきだと指定しているにもかかわらず、経営者が中心となって十分に取り組めてはいないのではないか。日本版SOX法への取り組み状況をヒアリングすると、経営者がプロジェクトオーナーである企業は多い。しかし、プロジェクトのなかで、経営者が中心となって議論を進めている企業は少なく、実質的には「現場を中心とした文書化作業プロジェクト」となってしまっている企業が多かった。

さらに、SEC登録企業の場合、運用面で「報告」や「統制の変更」への対応などに課題を抱えていたが、日本企業は、それらの課題だけでなく、より大きな「内部監査人材の不足」という問題に直面すると思われる。

日本における会計監査人の数は約１万6000人（日本公認会計士協会登録数）、アメリカのそれは約33万人（アメリカ公認会計士協会登録数）である。人口や経済規模が異なるので一概に比較するのは難しいが、アメリカの10分の１程度しか会計監査人がいない。

このため、外部監査よりも内部監査が重要な役割を担う、つまり企業における内部監査人の役割が重要になってくる。しかし、この内部監査人の数も、会計監査人と同様に少ないといわれる。労働人口が減少していくことなどを考えると、これまで以上に内部監査に社内の経営資源（人材）を割り当てることは難しく、人手に代わる仕組みによる支援が必要と考えられる。

このように、経営者が主体であるにもかかわらず、その取り組みが真剣になされない

表2　内部統制関連の法律・規制

テーマ	法律・規制		主体	対象範囲	開示方法	適用時期
内部統制全般	新会社法（法務省令）	内部統制システムの基本方針	取締役会	内部統制全般	営業報告書	2006年5月から
開示内容に係る宣誓書など	SOX法（アメリカ）	宣誓書（第302条）	CEO、CFO	年次報告書など（日本企業は年次のみ）	年次報告書などに添付	2002年8月以降
	金融庁	確認書（任意）	経営者	有価証券報告書など	有価証券報告書などに添付	2004年3月期から
	東証など	確認書（強制）	代表者			2005年3月期から
		適時開示姿勢の宣誓（強制）		情報開示全般	取引所に提出後、公衆縦覧	2005年2月から
財務報告に係る内部統制の経営者による評価と外部監査	SOX法（アメリカ）	第404条	経営者	年次報告書、有価証券報告書の財務報告に関連する部分	年次報告書などに添付	2007年3月期から
	金融庁	基準案（2005年12月8日）	経営者（執行の代表者）		未定	未定

点、および内部監査があたかもコンピュータの2000年問題のように一過性の対応プロジェクトとして捉えられ、運用まで考慮に入れた対応が行われない点が、日本でも危惧される課題である。

これらの課題について真摯に議論することなく、手順、作業を追う限り、日本版SOX法対応を企業価値向上へと結びつけることは難しく、単なるコンプライアンスの１つで終わってしまう可能性が高い。では、企業は一体どのように取り組むべきなのだろうか。

Ⅳ　SOX法対応を企業価値向上へ

1　他社との差別化要因となる高レベルの内部統制

そのヒントを求めて、アメリカの先進企業を何社か訪問し、ヒアリングを行った。何より驚かされたのは、SOX法対応以前の問題として、日常の経営サイクルに法対応、内部統制が組み込まれていたことである。

内部統制に優れ、高業績を維持しているある企業を訪問し、SOX法対応について丸一日かけて話を聞いたのだが、半日はコーポレートガバナンスの話であった。どれだけ、経営が内部統制について真摯に考えているか、それを社員だけでなく協力会社にまで伝え、守らせる工夫をしているか、コンプライアンス担当執行役員から説明された。

特に印象的だったのは、難しい規程などを平易な記述、事例、写真などを交えてハンドブックにまとめ、それを社員だけでなく取引業者にまで交付していた点である。内部統制をあたかも商品・サービスのように理解することができた。

通常、コンプライアンスおよび内部統制という言葉だけを聞くと、内向きの活動であり、法律・規制で求められること以外は特段社外にアピールするものではないと感じる。しかし、無形のサービスの提供を中心に事業を展開している企業にとっては、非常に重要なサービスの一部と理解することができる。

特に金融機関のように、法人向けに無形のサービスを提供している企業にとっては、商品・サービスの差別性を証明するものが乏しく、しかもそれが適正に運用されているかを示すものはほとんどないのが実情である。そうした企業にとっては、内部統制こそが商品・サービスが適正に運用されていることを証明する手段であり、他社に先駆けて確立し、積極的に外部に発信していくことが重要な差別化要素となってくる。

このような視点で考えると、単に高い業績を上げるだけでなく、高い内部統制レベルを伴い、それを外部にアピールしていくことは、永続性、継続性が求められる企業にとってきわめて重要である。

2　ハコではなく実質的な議論

アメリカの先進企業の事例は、実は長年継続した結果であり、日本企業にとってはまず内部統制の経営サイクルへの取り込みが求められる。ここで提案したいのは、ハコとしての組織論ではなく、実質的な議論を行う必要性である。

経営サイクルへの取り込みを提案すると、多くの企業はまず会議体を設定し、その会議体を中心としたPDCA（計画、実行、評価、改善）の業務サイクルを設計する。しかし、実際の企業にはすでに多くの会議体があり、

しかも内部統制の専門家（経営資源）は乏しいため、多くの場合、新しい組織をつくっても適切には機能しない。

新しい組織や業務サイクルの設計よりも、むしろ、現実に経営が最も重要視している経営サイクルで、内部統制について、どのタイミングで何をテーマとして取り上げ、継続的に議論するのかを決定する方が重要である。

たとえば、あるユーティリティ企業では、競争環境の変化に対応するため、統合的なリスク管理の枠組みであるERM（エンタープライズ・リスクマネジメント）を全社に導入した。その際に、できるだけ既存の組織・システムを活用することが方針の１つとして掲げられた。その方針を実行に移すに当たっては、監査部だけでなく総合企画部を巻き込むことが重要であったという。総合企画部と一緒に取り組むことで、経営や現場を最初のステップから巻き込むことができた結果、現在では、ERMは経営サイクルに落とし込まれて定常的に運用されている。陣容も、リスク推進室としてはたった２人である。

このように、大きな組織を設けなくても、既存の組織を巻き込むことで、内部統制を経営サイクルに定着させることができる。

複数企業の日本版SOX法第404条対応プロセスに関する計画書を見たところ、組織体制上には経営トップがプロセスオーナーと記してあるが、それ以外のページに、プロジェクトオーナーや経営がプロジェクトの中でどのように議論に参画したり、報告を受けたりするかを明記しているものはまずなかった。

いきなり日本版SOX法を飛び越え、上記のユーティリティ企業のようにERMに向けて経営が何をするかを検討することは難しい。しかし、少なくとも日本版SOX法対応というプロジェクトの中で、経営がどのように参画し、議論するのかを決めることが、最初のステップであると考える。

3　経営トップの不正を防ぐために

リスクを抽出し、統制を検討する文書化作業に経営を巻き込むことは、最初のステップである。しかし、それだけではCEO（最高経営責任者）やCFO（最高財務責任者）といった本当のトップレベルの不正を発見、防止することは難しい。本当の意味での経営トップであるCEO、CFOの不正を防止するためには、他の仕掛けも必要である。

経営トップに対して物を言うのはなかなか難しい。このため、内部監査機能を補強する意味で、外部コンサルタントを雇用することや、執行と経営を完全に分離するようなことも１つの手段となる。また、上場企業の場合、IR（投資家向け広報）という活動を経営トップ自身の目標管理と位置づけるような開示のあり方が必要であろう。

社員レベルについては、多くの企業が目標管理制度などを導入しており、期初に数値目標や行動目標などが立案されている。一方で経営トップは、実はIRにおいて戦略や数字目標を提示するだけにとどまっている。

内部統制については、やっと日本版SOX法対応で証明、宣誓を行うことになるが、それらは「結果」でしかなく、内部統制についての「目標提示」はなされない。開示については、結果を報告するという位置づけにとどまらず、目標を提示する、資本市場に約束する場として位置づけることが、経営トップの不正を防止する一助になると思われる

（図４）。なお、情報開示については本号の「内部統制と情報開示」を参照されたい。

4　運用支援のためのIT活用

経営の主体性と同程度以上に問題の「運用に対する意識欠如」「内部監査の経営資源不足、仕組み不足」については、ITにより改善できる領域が大きく２つある。１つは重要な統制をシステム化、自動化することで、もう１つは内部監査業務を支援する証憑一元管理システムを構築することである。

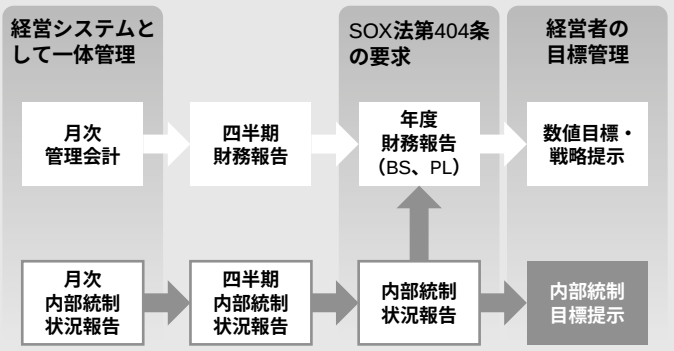
SOX法第404条対応を終えつつある企業と話をすると、統制項目は1000から１万までと、業種業態や企業規模により千差万別である。共通するのは、毎年その統制項目について運用評価、つまり証憑を確認するサンプルテストが必要なことである。サンプルの数は、その統制の頻度、および自動か手作業によるものかによって変わってくる（図５）。

マニュアルに統制作業が記されていても、手作業で毎日行っているものは、マニュアルと一致しない例外処理や、手作業によるミスが発生する可能性がある。そのため、テストのサンプル数も多くする必要がある。

そのような統制作業を自動化、つまりシステム化することで、（そのシステムについてのIT全般統制がしっかりとしている前提では）サンプルテストはほとんど不必要になり、現場および内部監査のテスト負荷を削減することが可能となる。日本版SOX法制定を機に、統制の自動化、標準化に貢献するERP（統合基幹業務システム）やアイデンティティマネジメント（システム利用者の属性や権限に基づく統合的なアクセス管理）などのシステムソリューションが普及することが考えられる。

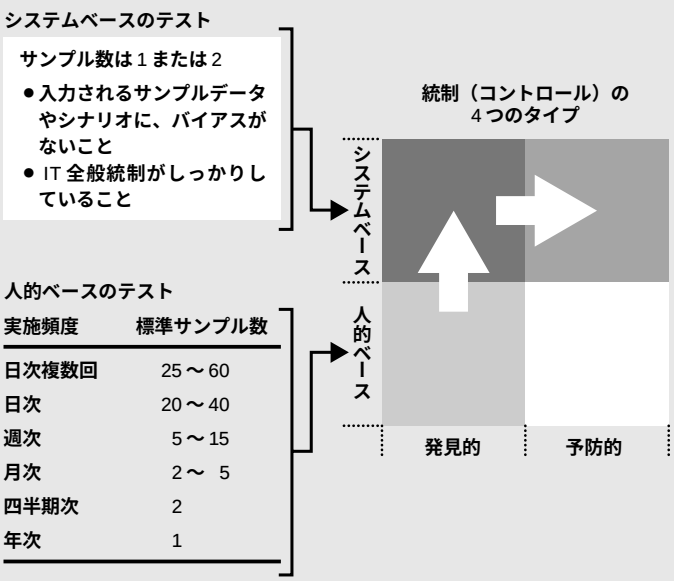
証憑、ログなどの一元管理の仕組みも重要である。SOX法対応の運用業務、つまり内部監査業務は、本来きわめて複雑であるが、あえて簡素化すれば「証憑を準備し、それを確認・評価する」作業である。その際に、評価作業と同等以上に、証憑の準備、収納などに時間がかかっているという。評価作業自体は社員自身が行わねばならないが、準備はシステムで支援することができる。

図4　内部統制についての「目標」開示



注）BS：貸借対照表、PL：損益計算書

図5　統制タイプによるテスト負荷



アメリカで複数の金融機関にヒアリングしたところ、皆一様に証憑管理の難しさについて語ってくれた。数百という統制作業について、それぞれの証憑を管理し、現場での自己評価、内部監査、外部監査のたびにサンプルを選んで準備しなければならない。統制の証憑には、書類もあれば、デジタルデータもあり、それを一元管理しなければならない。

ある先進的なグローバル企業では、「文書」管理規程を「情報」管理規程へと改定・変更することで、デジタルと書類（アナログ）を一元的に管理するようになっていた。また所管部署も、デジタルはIT部門、書類は総務部門という分別管理ではなく、一括してIT部門つまりCIO（最高情報責任者）が管理していた。

そのほかにも、個人のデスクトップ関連のデータ、電子メールや電話による顧客とのやりとりの管理についてのシステム化など、コンテンツマネジメントに関する取り組みが強化されているようである。アメリカの調査会社、フォレスター・リサーチやIDCによる調査でも、この傾向は顕著に現れている。

5 ERMシステムでSOX法を超える

筆者らは、このような内部監査を支援する仕組みを、「ERMシステム」と呼んでいる。ERMシステムは、直前に迫る日本版SOX法への対応に際して重要な機能を果たすだけでなく、他の法律・規制ともかかわるホリスティックコンプライアンス（全体総括的管理）を実現し、経営ダッシュボード（経営者向け情報システム）、継続的な業務改革へとつながる拡張要素を有しているため、期待を込めてERMシステムと呼んでいる。

ERMシステムには、まず、来るべき日本版SOX法対応に向け、内部統制の文書（業務フロー、リスクコントロール・マトリックス）および評価結果の管理や、統制活動で発生した運用評価に必要な証憑類の管理・保全など、重要な機能を果たすことが求められる。そのために、次のような具体的機能を備えることになる。

①データの一元管理

各システム内に分散して保存されているデータを一元管理し、データの検索、取り出しを容易にすることで、内部監査業務を効率化する。また、そのデータを監査業務の省力化に応用する。

②データの再現

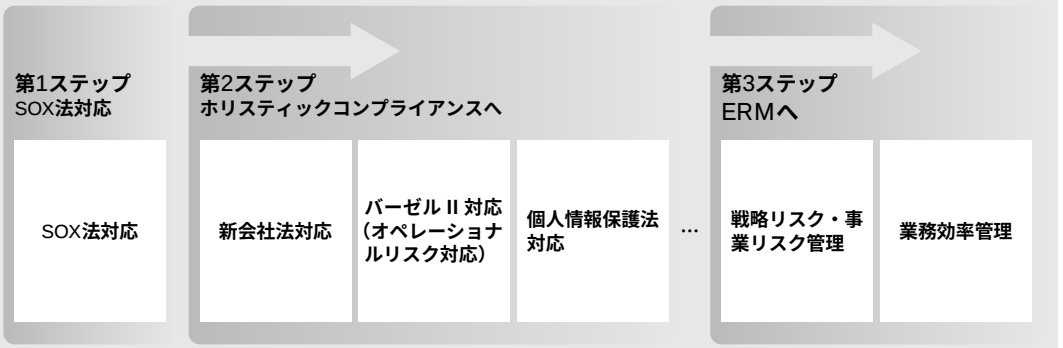
過去の評価結果および証憑を、再現性ある形で再現する。業務プロセスは、改善活動を通じて変化していくので、バージョンを正しく管理することが併せて求められる。

③データのセキュリティ

内部統制上の重要データである統制評価結果や証憑を、隠滅されたり改ざんされたりしないように管理・保全する。また、人的ミスや自然災害から、データを安全に守ることも必要となる。

実は、この３つの要件は、他の法律・規制にも関連する共通の必須機能である。多くの法律・規制が、現状の業務を記述した業務フローや、リスクと統制の関係を管理する類似のマトリックス、さらには証憑を管理することを求めている。当初は日本版SOX法対応の文書・証憑管理システムであっても、いずれは同様の内部統制関連の法律の対象となる文書の統合管理システム（ホリスティックコ

図6　ERMシステムのカバー範囲



注）ERM：エンタープライズ・リスクマネジメント

ンプライアンス・システム）へと発展することが可能である（図6）。

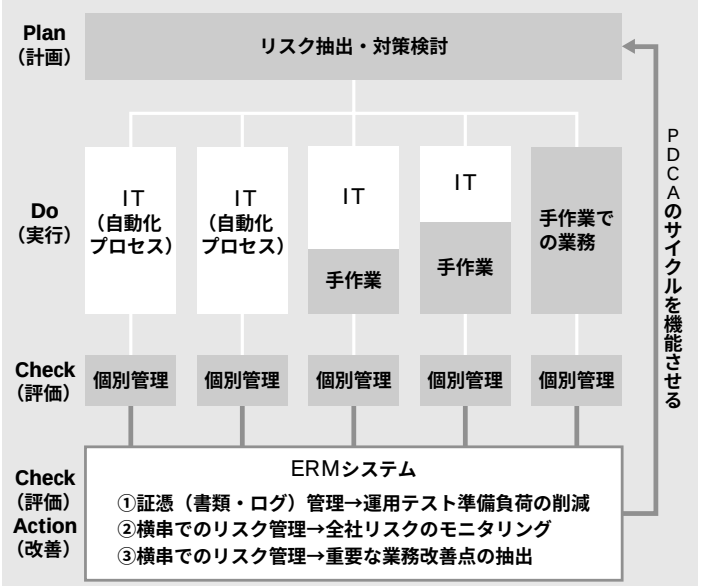
各法律・規制に対応する個々の企業活動とそれに関連する情報（証憑）をデータとして収集し分析する基盤が整備できれば、①内部統制に関する業務（内部監査業務）を効率的に行うのを支援することから、②企業活動に関するリスクを一定の論理で算出することで、全社リスクをモニタリングすることへ、そして③業務プロセスごとの業務量、リスク量を定量的に測定し、業務プロセス再構築の元データの提供および分析を支援することへと、発展が可能となる（図7）。

昨今、多くの企業では、システムのオープン化、分散化が進んでおり、各業務アプリケーションが個別のシステム基盤の上に構築されている。このようなシステム基盤の多様化に伴い、業務やシステムのパフォーマンスが企業内で一元的に把握されていない。そのため、どの業務アプリケーションの更改に着手すべきかという優先順位付けも難しい。仮に、業務アプリケーションの更改に着手し、部分的に効率化が実現したとしても、企業全体としては業務負荷を増やし、効率性を損ねる場合も考えられる。

しかし、たとえシステム基盤のオープン化が進んでいようが、ERMシステムの構築により、企業内の全業務プロセスに関する業務量、リスク量が定量的に測定できていれば、継続的な業務改革にもつながる。

前述のように、システムソリューションを導入して、内部監査業務や統制活動を支援することは可能である。ただし、システムソリューションはあくまでツールでしかない。どのような内部統制を実現したいのか、経営管

図7　ERMシステムの可能性



理、内部監査の仕組みをどのように構築したいのか、という経営の意思があって初めて機能するものである。その意味では、システムソリューションの導入についても経営が主体となるべきであり、内部統制を経営モデルとしてどのように取り込むか、真摯に議論することが非常に重要である。

V　求められる「オペレーショナライジングERM」

日本版SOX法を単なる文書化プロジェクトに終わらせないための解決策として、①経営システムへの組み込み、②IRを活用した経営トップの目標管理、③ITを活用した内部監査支援および継続的な業務改革への発展――について述べてきた（図８）。

内部統制というと、現場にとってはどちらかというと業務を妨げる邪魔モノで、本社機能の一部でひっそりと実行されるものという印象を持つ人が多い。しかし、資本市場から受けた資金を事業に投資して運用する、また顧客企業の非コア機能を受注するという視点で考えると、本稿で提案した３つの施策は、実は経営モデルそのものとして理解することができる。また、この考え方は、ERMの考え方が普及するに伴い、ますます広がっていくと考えられる。

企業価値に占める将来の比率は高い一方、将来の不確実性は高まっている。一度立案した戦略が、長年有効であるとは限らない。財務諸表に関する内部統制やオペレーショナルリスク（システム障害や事務処理上のミス、不成行為などにより損失を被るリスク）を管理することは重要だが、それだけでは経営者としてリスクを十分管理しているといえなくなってきた。COSO（トレッドウェイ委員会組織委員会）の枠組みも、1992年の内部統制フレームワークから、2004年にはERMフレームワークへと発展している（図９）。

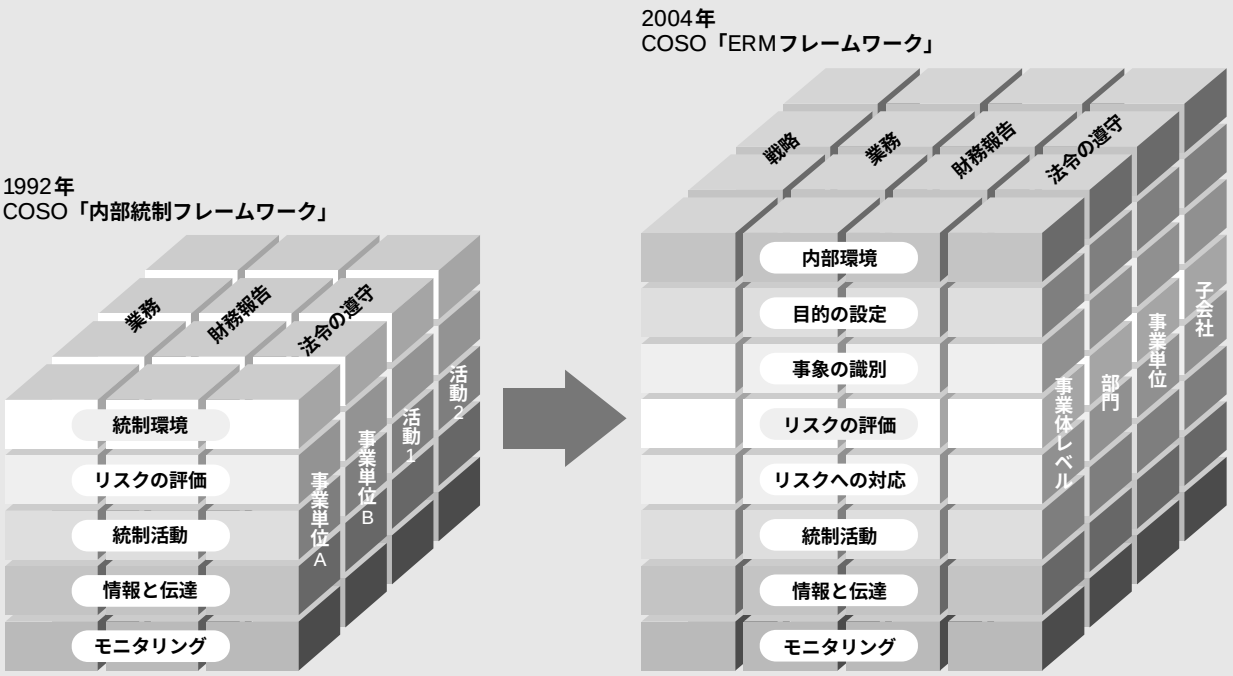
そうした視点で考えると、経営者のリスク管理に対する責任はますます重くなり、「内部統制・リスク管理＝経営モデル」として、戦略管理、業績管理と一体で管理することが求められる。一体管理とは、単に一緒に進捗管理することだけではない。ビジョンや戦略があいまいであれば、企業としてのリスク選好もできない、つまりリスクアプローチも十分にできないことを意味している。

つまり、経営者は、戦略・ビジョンを明確に提示することをも求められている。これはCOSOのERMフレームワークで、「目標の設定」を構成要素として取り上げていることからも明らかである。

図8　企業価値向上に向けて

注）IR：投資家向け広報

図9　内部統制フレームワークからERMフレームワークへ



注）COSO：トレッドウェイ委員会組織委員会

筆者らは常々、「オペレーショナライジング（Operationalizing）ERM」という考え方を提唱している。筆者らの造語になるこの言葉は、以下のことを意味する。

「単なるSOX法対応にとどまらず、ホリスティックコンプライアンス、さらには全社的な内部統制、企業全体のリスク管理（ERM）へと管理範囲を広げ、しかもそれを実効性のあるものにすること（つまり、オペレーションとして徹底すること）が企業価値につながる」

ERM、内部統制を経営モデルとして定着させることは、相当の苦労を伴う大規模な企業風土改革プロジェクトであり、変革意識を創り出すチェンジマネジメント・プロジェクトである。この「オペレーショナライジングERM」が、単なる概念ではなく、内部統制を中心とする新しい経営モデルとして世の中に認知されたとき、企業は、資本市場から信頼を勝ち取ることができるに違いない。

著者

能勢幸嗣（のせこうじ）
事業推進二部上級コンサルタント
専門はチェンジマネジメント（経営戦略・事業戦略立案、経営管理システム設計、実行支援）、企業再生、リスクマネジメント

宗　裕二（むねゆうじ）
事業推進二部上級システムアナリスト
専門は金融情報システム、リスクマネジメント

エリック・ファンドリッチ（Eric Fandrich）
事業推進二部上級コンサルタント
専門はリスクマネジメント、BC・DR（事業継続・災害復旧）、企業価値評価、M&A