寄稿

IT統制の重要性と企業に求められる対応

内山　悟志（うちやま　さとし）
株式会社アイ・ティ・アール
代表取締役　シニア・アナリスト

1．ITと内部統制の関わり

日本版SOX法の法案化を受けて、多くの企業で内部統制推進室の設置や専任担当者の任命などの準備を進めつつある。日本版SOX法そのものの解説は、実施基準や各種書籍などで多く紹介されているので、ここでは省略することとする。

さて、日本版SOX法は、米SOX法でも参照されたCOSO（トレッドウェイ委員会組織委員会）の内部統制フレームワークがベースとなっている。ただし、COSOの内部統制フレームワークで定義された「統制環境」「リスクの評価」「統制活動」「情報と伝達」および「モニタリング」という5つの基本的要素に、日本版SOX法では「ITへの対応」が追加されたことが特徴的である、という点はよく知られている。

これは、多くの企業においてITが多面的に活用されており、IT抜きには業務を遂行できないほど、ITが浸透しているという現状を強く反映したものである

ここで、企業の内部統制におけるITの役割および内部統制とITの関わりを整理すると、以下の3点が重要な接点として浮かび上がる。

① ITを活用している業務処理に対する統制：ITを活用して作成される財務報告の信頼性や、ITによって遂行される業務処理の適正性を確保すること

② ITそのものの全般的な統制：さまざまな業務で活用している情報システムそのものが、適正に開発、運用、保守および管理されていること

③ 内部統制の構築・強化におけるITの利用：統制環境を整備

したり、統制活動を効率的に実行していくために手作業ではなく情報システムによって対応すること

日本版SOX法のITへの対応の中の「ITの利用および統制」に当てはめて考えると、①および②がIT統制にあたる部分で、それぞれ業務処理統制と全般統制と呼ばれる領域である。一方、③は「ITの利用」にあたる部分である。

2．IT統制の重要性

企業のIT部門が投入する技術とプロジェクト管理手法が進化し、IT部門自身が最善を尽くしても、ITプロジェクトが予定どおり履行できない、あるいはサービスが安定的に提供できないといったリスクはつきまとう。米ITPI（Information Technology Process Institute）の調査によると、平均でITオペレーション予算の35%もの額が予期しないダウンタイムに費やされている。

こうした事象の原因として、ITプロセスに対する内部統制が不十分であることが考えられる。統制の対象が計画策定、プロジェクト管理、オペレーションであろうが、データアクセスやデータの完全性であろうが、適切な統制が機能していなければその被害は甚大となる。

システム上のトラブルや問題における欧米の事例は、もはや対岸の火事ではなく、国内においても同様の事態は頻発している。証券取引所や金融機関におけるシステム障害、大規模な個人情報漏えいといった情報システムに関連するトラブルが、一企業の問題ではなく、経済や社会に大きな影響を及ぼすことは、昨今の報道を見ても明らかである。また、多くの重要なビジネスプロセスでITが中心的な役割を担っていることから、適正な業務処理を実行するためには、健全なIT環境とIT運営管理の適正性の確保が求められるようになってきている。IT統制は、日本版SOX法などの法制度化を機に注目を集めるようになったが、企業が本来果たすべき社会責任と、ITを活用するうえで備えるべき体制という観点からは、従前から必要とされていた根源的な重要テーマと言えるだろう。

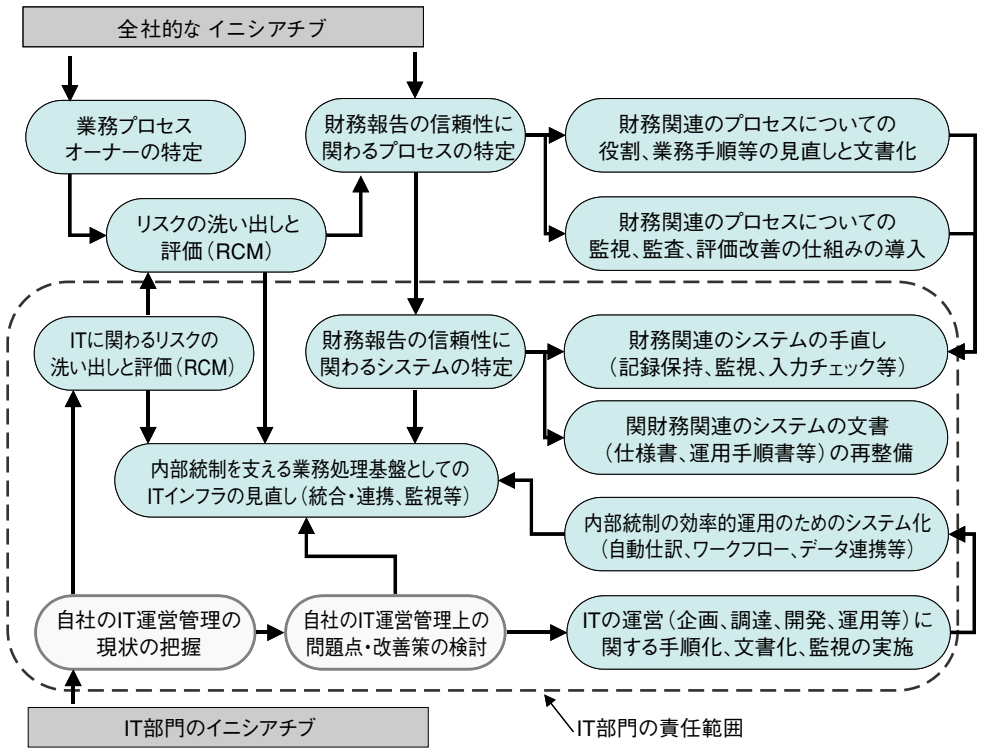
CIOおよびIT部門は、これまでのように、ITを活用して業務の効率化やサービスの向上などに間接的に貢献するという任務に加えて、企業活動の適正性の確保やその保証のための仕組みの提供という、IT内部統制の担い手として役割を果たしていくことが求められる。特に、CIOの役割として重要となるのは、IT内部統制環境の整備とITの適正運営および利用に関する企業風土改革の断行である。

3．日本版SOX法に向けた準備の全体像

企業の内部統制強化は本年度から急に必要となったわけではなく、以前から存在した重要課題ではあるが、法制度化をきっかけに必須の対応が認識され、準備に時間制限が設けられ、取り組みが本格化したと考えられる。これまでも、企業ではコンプライアンス委員会の設置、企業リスクや情報セキュリティへの対策、業務の標準化などに取り組んできたが、これから数年間のイニシアチブの多くは、企業の内部統制報告および内部統制監査を意識して優先順位をつけた取り組みが主流となろう。

企業の取り組みを観察すると、日本版SOX法では財務報告の信頼性が最も重要かつ根源的な目的となることから、全社的なイニシアチブは財務部門または経営企画部門が主導しているケ

図1　日本版SOX法対応に向けた準備のアプローチ



（注）RCM：Risk Control Matrix

ースが多い。

この領域では、まず監査法人やコンサルティング会社から情報を得て、業務の対象範囲や今後の進め方について検討される。具体的には、対象となる業務に対して業務オーナーまたはプロセスオーナーを明確にし、彼らに対してリスクの洗い出しや評価を依頼し、それをリスク・コントロール・マトリックス（RCM）として取りまとめることが最初の作業となる（図1）。また、特に財務報告の信頼性に影響を及ぼすプロセスを特定し、RCMによって洗い出されたリスクを照らし合わせて、特に優先度の高いプロセス、体制、制度、システムなどについて対応策が検討されることとなる。また、役割分担、承認手続き、指示系統、監査・報告の実施などについては、社内規定や運営手順書などに文書として記載されているかどうかが問われることが多いため、文書化の作業も企業にとって大きな負荷となろう。

4．IT部門に求められる初期の取り組み

IT部門に求められる取り組みとしては、全社的なイニシアチブからの要請に対応するために、IT部門が業務オーナーとなる業務に関するリスクの評価と、財務報告の信頼性に影響を及ぼすシステムの特定が最優先の作業となる。リスクの評価については、全社的なイニシアチブからリスクの定義、抽出の条件、RCMの記載内容および書式が指示されるのが一般的であるため、それに従って実施することとなる。財務報告の信頼性に影響を及ぼすシステムの特定についても、監査人などのアドバイスに基づい

て範囲および抽出の条件が指示されるであろうが、抽出するシステムの粒度（サブシステム単位化など）やシステムの種類（ツール類やデータベース管理システムは対象となるかなど）については詳細な定義が示されない場合が多いため、確認を取りながら進める必要がある。

一方、全社的なイニシアチブからの指示を待つことなく、IT部門が独立して進められる初期の作業としては、自社のIT運営管理の現状把握と問題点、改善策の検討がある。事前にこれを行っておくことで、IT部門が業務オーナーとなる業務に関するリスクの評価に対するインプットとなるだけでなく、財務関連のシステム文書（仕様書、運用手順書など）の再整備およびIT運営（調達、開発、運用など）の手順の明確化および文書化といった作業で必要となる工数を推定でき、後の作業をスムーズに進めることができる。

5．計画化が求められる施策

財務関連のプロセスの変更に伴うシステムの手直しや、内部統制が効率的に運営されるためのシステム化といった情報システムの開発や修正が必要となる作業については、要員や予算の確保が必要となる場合が多いため、優先順位に基づいて計画を立てて実行していくことになる。また、文書（仕様書、運用手順書など）の再整備、IT運営（調達、開発、運用など）の手順の明確化および文書化、IT運営の適正な実行を確保する監視・監査の実施についても、日本版SOX法に向けた内部統制監査で指摘される領域と、IT内部統制に間接的に寄与する領域を分けて優先順位を検討しなければならない。これらの中でも、財務関連のシステムの文書（仕様書、運用手順書など）の再整備と財務関連のプロセスの変更に伴うシステムの手直しは優先度が高いと考えられる。

情報システムの開発や修正が必要となる作業の中には、個別のアプリケーションごとに機能（入力チェック、記録保持、アクセス制御など）を追加・修正するよりも、内部統制基盤としてのITインフラ再整備の一環として、ミドルウェア層で対応する方が長期的に考えると有効な場合が多いと考えられる。しかし、ITインフラの再整備を待たず緊急に対応しなければならない事項も少なからずあるため、機能の重複や二度手間を最小限に抑えられるよう全体的な将来像を見据えて計画化することが求められる。

内部統制を強化するために業務プロセスを変更することで、承認、記録保持、二重チェックなどの作業が増加し、業務の生産性が低下する可能性がある。このため、内部統制が効率的に運営されるためのシステム化（ワークフロー、システム間連携など）が必要となることが想定されるが、一般的にはこのようなシステム化は後回しになりがちなため、あらかじめ計画に組み込んでおくことが推奨される。

IT部門に求められる対応は多岐にわたり、作業負荷も想像を超えるものとなる可能性があるため、定常業務を兼務する数名のスタッフで切り抜けるのは困難であることを覚悟しておかなければならない。また、内部統制報告の作成および監査が終了したらそれで終わりというわけではなく、その後も指摘改善事項への対応、さらなるレベルアップの取り組み、および内部統制の効率的運営のための環境整備など、さまざまな作業が継続して発生する可能性があることを想定しておかなければならない。