

日本版SOX法対応への考察

1. 日本版SOX法の実施基準の進展状況

財務報告の適正性を確保するため、上場企業に対して内部統制の構築を義務付ける内容を含む金融商品取引法(日本版 SOX 法)が 6 月 7 日、参院本会議で可決、成立した。2005 年 12 月に「財務報告に係る内部統制の評価及び監査の基準案」を発表。現在は内部統制の構築、評価、監査のガイドラインとなる実施基準を策定している。最終確定は 10 月以降になると見られる。

日本版 SOX 法が適用されるのは 2008 年 4 月 1 日からの事業年度。

2. 内部統制の基本的枠組み(4つの目的、6つの基本要素)

内部統制は、①業務の有効性・効率性、②財務諸表の信頼性、③事業活動に関わる法規の遵守、④資産の保全への目的を達成する為に、合理的な保証を提供することを意図した、取締役会、経営者及びその他の職員によって遂行される1つのプロセスである。更にその中の6種の構成要素について、経営者が内部統制を適正に運用されているか評価し、外部に対して「内部統制報告書」として示す。会計士は更に内部統制の適正性を外部からチェックする「内部統制監査報告書」を作成する。

目的	①業務の有効・効率性 ②財務報告の信頼性 ③事業関連法令遵守 ④資産の保全	事業活動の目的の達成の為、業務の有効性及び効率性を高めること 財務諸表とその重要な影響を及ぼす可能性のある情報の信頼性を確保 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 資産の取得・使用・処分が正当な手続及び承認下に行われるようにする
基本要素	①統制環境 ②リスク評価 ③統制活動 ④情報と伝達 ⑤監視活動 ⑥IT 統制	企業内全ての統制活動のベース(倫理観・経営姿勢・構造・慣行。機能・方針) 目標達成に影響する全てのリスクを識別、分析、評価し、リスクに対応する 経営者の命令、指示が適切に実行される事を確保する為の方針、手続き 必要な情報が組織や関係者に適切に伝えられることを確保する 内部統制の有効性を継続的に監視、評価するプロセスであるモニタリング 内部統制が有効、効率的な機能するために情報システムの適正性等を保つ

3. IT統制

組織目標を達成するための管理が及ぶ範囲において、IT 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 IT 統制は、「全般統制」と「業務処理統制」の 2 つに分けられる。

(1) 全般統制

IT を使った業務処理統制が健全かつ有効に機能する基盤・環境を保証する統制である。IT 戦略、企画、開発、運用、保守、およびそれを支える組織、制度、基盤システムに対する統制を含み、各レベルの IT プロセスおよび個別要素である「ユーザー認証」「ログ監視」「暗号通信」「バックアップ」等が含まれる。上場会社会計監視審議会(PCAOB)では、①プログラム開発 ②「プログラム変更 ③コンピュータ運用 ④「プログラムやデータへのアクセスの 4 つを例示している。ハードウェアやソフトウェア、ネットワーク、アプリケーション等の企画から開発、運用迄の品質が一定レベルになる様、チェックリストが確立され、運用されているかが問われる。

(2) 業務処理統制

個々の業務処理システムにおいてデータの網羅性、正確性、正当性、維持継続性を確保するための統制をいう。業務システムにおけるデータの入力、処理、出力が正しく行われることが確か

あることを保証するためのもので、「二重入力チェック」「コントロール・トータルチェック」「限度チェック」などが含まれる。各アプリケーションで承認された取引が全て正確に処理され、記録されることを確保する為の統制。ベリングポイントでは「其々のアプリケーション、システムが企画、設計通りに開発され、運用されているかを確保すること」としている。草案では「各業務領域において利用されるコンピュータなどのデータが適切に収集、処理され、財務報告に反映されるプロセスになっていることを確保すること」と例を挙げている。

日本版SOX法は、適切に対応しないと処罰を科せられるだけでなく、対応のために多額のコストが予想される。米国の事例で最もコストがかかるのは、内部統制の基本と位置付けられる文書化のフェイズ。**文書化とは、企業がある決定をしたり、財務諸表のある数値を決定する際に、その決定を行うまでの社内外の手順を文書化、また実際のプロセス処理結果を文書として残すことを意味する。**この文書を基に経営者、会計士が内部統制の評価と監査を実行する。

業務処理プロセスを流す中でのリスクの洗い出しも必要だ。例えば受注から入金までの貸し倒れ、売上げの架空計上などプロセスに内在するリスクがある。そのリスクアセスメントと対応が必要となる。更に業務処理プロセスの変更などをその都度、反映させないといけない。

4. 日本版SOX法とIT部門の心得

IT統制では、「業務処理統制」「モニタリング機能」「セキュリティ機能」「システム可用性」の4つのポイントを再点検する必要がある

業務処理統制	アプリケーションへの入力ミスを軽減する桁数や値の妥当性のチェック機能
モニタリング機能	業務の設計通りの実施確認、経営者への必要な情報を提供、アラート表示
セキュリティ機能	アクセス権限の設定やコンピュータ・ウイルス、不正アクセスの防止策、
システム可用性	システムダウンやパフォーマンスの低下が起きないように監視する機能

日本版SOX法への対応では、まだ法整備がされていないため、本格的な活動は難しいとしながらも、「内部統制に関するクイックスキャン」やその結果に基づく「方針決定」や「文書化」などは現時点でも行える。このあとに続く、運用テストなどを法律が決まった来年以降に行えばよい。

日本版SOX法で求められる情報システムの対応は、ユーザー企業がすでに持つアクセス管理や文書管理などのツールでほとんどできる。重要なのは職務権限の明確化など、ユーザー部門のビジネスを変えることだ。内部統制は企業全体のビジネスプロセスに関係するテーマで、IT部門だけの問題ではない。日本企業には上司は常に正しいという暗黙の前提がある。上司から指示があれば違法な行為でも行う、明文化された倫理規定がないなど統制環境の軽視がある。更に次の様な内部統制の前提が欠けていることを指摘される。

(1) 終身雇用・年功序列制度の終焉

日本企業はかつて終身雇用制度と年功序列制度によって社員の企業への忠誠心が高く、内部統制のレベルが高かったとされている。いわば「非常な少費用で高い統制のレベルが得られた。だが、経済環境や企業体質の変化で終身雇用制度や年功序列制度は実質的に崩壊。高いレベルを誇ってきた統制環境の前提がなくなってしまった。日本企業が内部統制を再構築するためには経営者が意識を持って取り組む必要がある。経営の仕組みを変えないといけないが、それができるのは経営者だけだともいえる。

(2) 優先順位に基づくリスクマネジメント

内部統制強化のためのプロジェクトは経営者の指示の下、財務部門、内部監査部門、法務部門、IT部門などで構成するケースが多いという。このプロジェクトが大枠の方針を決定し、IT部門がITシ

システムの対応を検討、実行する。IT部門が最初に行うことは「プロセスとそれらの内部統制を文書化すること」。情報システムにおける不正アクセスの可能性などプロセス毎のリスクを洗い出し、そのリスクを軽減するためにどのような対処を行うかを明記する。しかし、プロセスに関するすべてのリスクを洗い出すと文書化の作業は膨大になる。「多額のお金が処理される場所や、すでにトラブルが発生しているところに集中すべき」である。

5. 日本版SOX法の内部統制は特別のものではない

企業はまず何をやるべきかを明確にすべきである。企業は内部統制構築の計画を立案して順番にやっていけばよく、過剰反応することはない。内部統制の強化というと2008年3月期にも導入されると見られる日本版企業改革法(日本版SOX法)ばかりが目立つ。しかし、新会社法が今年5月に施行されている。新会社法では内部統制システムの構築を企業に対して求めている。日本版SOX法が財務報告に関する内部統制の構築を要求するのに対して、新会社法は企業業務の適正性確保を求めるといえる。企業は日本版SOX法だけでなく、新会社法も意識して内部統制を構築する必要がある。内部統制システムを一発で構築できることはあり得ない。あまり過剰に反応せずに何段階かに分けて対応すべきである。

(1) ISOのISMS或いはQMSの財務プロセスの管理で対応可能

内部統制はCOSOフレームワークがベースであり、①「業務効率化」②「法令遵守」③「財務信頼性」④「資産の保全」が4本柱になる。この4本柱と、外部に公開する「内部統制ポリシー」「セキュリティポリシー」「プライバシーポリシー」等が完全に一致するかが問われる。つまり「内部統制」と、ディスクロージャー制度などによる「外部統制」を同期させることが企業の信頼性を高めるという考えとなっている。ISOのマネジメントシステムにおけるプロセスアプローチで要求されている事と同様な内容となっている。

(2) プロセスアプローチによる継続的改善の趣旨と同じ(プロセス監査による対応)

企業が内部統制システムを構築する場合、ポイントになるのは「業務改善と業務の透明化」である。企業のビジネスプロセスには担当者の経験や勘に頼ったブラックボックスのフローがある場合が多い。内部統制の観点ではこのブラックボックスがリスクになる。担当者以外はフローの内容を点検できず、不正があっても分かりづらい。内部統制システムとはこの経験と勘に頼ったビジネスプロセスを図式化し、文書化して、その推移が見えるようにすることだともいえる。フローを透明化することで監視や代替が可能になり、効率性も上るといえる。個人情報保護法施行後も情報漏えいが絶えないのは業務改善をしていないから。内部統制でもIT化の前に業務の可視化、効率化を図るべきである。

6. 経営者が主導するリスクマネジメントの重要性

日本版SOX法について「目玉はITへの対応」と指摘。たとえITシステムをそれほど活用していない企業であっても、「取り巻く環境は進んでいる。それとの整合性の理解が重要となる。また、昨年来発生している証券取引所のシステム障害や銀行ATMのパスワード盗撮事件などに関係した企業はITの利便性に胡坐(あぐら)をかいて、リスクへの理解が不足していた。ITの脆弱性や危険性も理解する必要はある。

企業の実際の対応について「ある程度の指針は示されるが一律的に適用できるものではなく、「まず経営トップがどのような状況であれば自分が財務諸表の信頼性にサインをすることができるのか、洗い出すことが必要。そのときに会計システムがバラバラだったりするとリスクを生む可能性がある。ITを使った標準化や集約化は当然、必要になってくるかもしれないといえる。しかし、そうでなくてはいけない、ということではなく、経営者が主導する内部統制構築・運用の重要性が顕著になっている。