

財務報告に係るIT統制とその評価

櫻井 憲二

あずさ監査法人
代表社員 IT監査部長
公認会計士 システム監査技術者

財務報告に係る内部統制の必要性

証券・資本市場が十分に機能していくためには、信頼できる企業情報が適時に開示されることが必要不可欠である。しかしながら、エロン事件を発端に、米国では相次いで財務報告に係る不正事件が発生し、わが国でも有価証券報告書の開示内容に不適正な事例が続発してきた。

これら事例の発生原因は、ディスクロージャーの信頼性を確保すべき企業の内部統制の不備、機能不全に根ざすことが明らかになり、米国においては、企業改革法「サイベインズ・オクスリー法」(SOX法)が成立し、急速に内部統制の整備・充実が求められている。わが国においても同様に内部統制の重要性が認識されはじめ、いわゆる日本版SOX法による制度作りが走り出した。

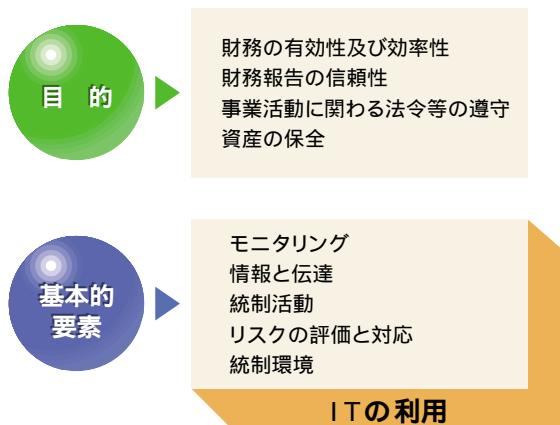
内部統制の枠組みにおけるIT統制の位置付け

わが国の内部統制の概念は、広く認識されてくるCOSO(Committee of Sponsoring Organizations of the Treadway Commission)の枠組みをベースに、目的に資産保全を加え、サイバー(Information Technology)の利用を独立した要素として、企業会計審議会「財務報告に係る内部統制の評価及び監査の基準」平成17年7月13日公開草案(草案)。

この草案によると、内部統制とは、業務の有効性及び効率性等の4つの目的を達成するために、業務に組み込まれ、組織内のすべての者によって遂行されるプロセスと定義され、6つの基本

的要素すなわち「統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング」そして「ITの利用から構成されている。この中でITの利用とは、さらに「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ITを活用することを」と定義されている。さらにとりわけ、組織の情報システムがITを高度に取り入れている場合には、内部統制の他の基本的要素の実施上の重要な一部として重要な影響を及ぼすことになる」と位置付けている。

内部統制の目的と基本的要素



ITを活用した内部統制

ITを利用した内部統制には、全般統制と業務処理統制の二つの概念がある。草案ではこの二つを次のように定義している。

(一)全般統制

ITを利用した全般統制とは、IT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。全般統制は、通常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・セキュリティおよ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。

(二)業務処理統制

ITを利用した業務処理統制とは、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。

業務処理統制にいう業務処理とは、販売、購買、在庫管理、固定資産管理等の企業活動の業務に係る処理であり、業務処理統制は、業務処理で承認を受けたデータが漏れなく入力され(正当性、網羅性)、入力されたデータはコンピュータ内で正確に処理され(正確性)、適正に記録・保存がされる(維持継続性)ことを確保するための統制であるといつことができる。

IT統制の評価

ITを利用した統制は、以上のように全般統制と業務処理統制に大別されるが、両者は完全かつ正確な情報を確保するために一体として機能することになる。そのため、IT統制の信頼性の評価においても、両者を複眼的に、あるいは並行的に評価する必要がある。

(一)全般統制の評価

日本公認会計士協会のIT委員会報告第一号「財務諸表監査における情報技術(IT)を利用した情報システムに関する統制リスクの評価」(「委員会報告一号」)において、全般統制の評価について、全般統制に関する統制活動の例示として、次の六つに分けて評価することとしている。

- 情報システムに関する計画と組織の統制活動
- 情報システムに関する企画・開発・調達業務の統制活動
- 情報システムに関する運用業務の統制活動
- セキュリティに関する統制活動
- 外部委託とそのサービスレベルの統制活動
- 監視活動

ITの全般統制においては、以上の諸活動について、採用している統制方針、マニュアル、職務権限、ルール策定、報告制度、契約管理、アクセス管理、教育訓練等の整備・運用状況が、当該企業のシステムに係る適正な統制目標を果たせるのか、さらに実際機能しているのかを評価することになる。

(二)業務処理統制の評価

委員会報告一号では、業務処理統制の評価においては、その業務処理を行うアプリケーション・システムを分析し、評価するための指針として、ITのコントロール目標について次のような例示を挙げている。

- 会計データの網羅性、正確性、正当性
- 会計データが漏れなく、重複なく記録され、残高更新され、未決済及びエラーとなった会計データは、期間内に全て適切に処理されていること
- 会計データは、正確に適時に適切な勘定に記録されていること
- 会計データは、実際に生じた経済事象を表し、かつ、当該企業に関連するものであり、承認されたものだけが入力され、処理されていること
- ファイルの維持継続性
- マスタ・ファイルは、常に最新の状態に保たれ、正しく維持及び継続されていること
- 異なるIT間で利用される分散マスタ・ファイル間の整合性が保たれていること
- アプリケーション・システムは企業規模、業態によって、また、同種・同規模の企業間でも異質なシステムになることが少なくない。そのため、実務ではビジネスプロセスの内容の深い理解と、各企業の実態に応じたシステムの分析の上に立つた評価が求められることになる。

終わりに

IT統制というと、内部統制の中の特殊な領域と思いがちである。確かにITそのものに対するスキルは一部の専門家の領域であるが、ITを利用した内部統制は、構築されたシステムと業務処理で接点を持つ人々に対する統制活動が重要な部分を占めると考えられる。すなわち、明確な運用方針策定の下での適切な権限および職責の付与、効果的な職務の分掌の他、ドキュメンテーション、継続的な教育訓練、作業エラーリング等の重要ポイントは、他の内部統制との共通的な側面を持つと位置付けられる。