IT 全般統制とは

IT 環境を適切に保つための統制

IT 全般統制とは何かについては、公認会計士監査の基準となっているＩＴ委員会報告第３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重要な虚偽表示リスクの評価及び評価したリスクに対応する監査人の手続について」（通称 IT3 号）にも明確に記載がありません。あえて定義らしい定義を選ぶと、第 13 項に次のような記載があります。

> 全般統制は、取引、勘定残高及び開示における情報の信頼性を確保すること、及び業務処理統制の継続的な運用を確実にすることを間接的に支援するものである。

これだけ世の中を騒がせながらその概念定義がないというのは、よほど世間に共通認識があるものと考えられているのでしょうか。確かに会計監査の世界では、EDP 監査という用語が使われていた 80 年代頃には既に全般統制という用語は使われていました。

しかしそれではあまりに不親切と考えたのか、IT3 号を解説したＩＴ委員会研究報告第 31 号（31 号とか IT3 号 Q&A と呼ばれる）Q2 の１には次のような解説が補足されています。

> ネットワークの運用管理、システム・ソフトウェアの取得及び保守、アクセス・コントロールやアプリケーション・システムの取得、開発及び保守に関する統制活動が含まれており、ＩＴを利用した情報システムの運用・管理に関する統制活動のこと

すなわち IT 全般統制とは次のような定義ができるでしょう。

> **IT を用いた業務処理の継続的な運用を確実にし、**
> **（財務）情報の信頼性を確保するために行われる、**
> **情報技術を利用した情報システムの運用・管理に関する統制活動**

財務報告にかかる内部統制という観点からは、(1) 財務情報を作成する基礎となるデータを適切な形に生成・維持・加工・廃棄する仕組みが必要であり、また（2）そのようにして作られたデータを悪意ある変更や消去（すなわち改竄）から守ることも必要です。

(1) の目的は通常の場合、IT が設計で意図した通りに作動しまた人間が設計で意図した通りに IT を利用している限りにおいては、設計で意図した結果をもたらすものと考えられます。したがって財務報告の信頼性の前提となる情報の信頼性を確保するためには、設計意図通り（仕様上の問題をカバーすることも含めて)に IT が機能するように環境を整備する必要があります。これが IT 全般統制の一つの側面です。

さらに (2) の目的は、それ自体が IT 全般統制のもう一つの側面であるとともに、(1) の目的を阻害しないようにデータやプログラムのおかれている環境を整備する必要が生じます。

IT 全般統制のレベル感

IT 全般統制の目的を理解すれば自ずと解ることですが、IT 全般統制は IT 業務処理統制と比べると、どの程度の統制を整備していればそれが有効（すなわち財務報告上のリスクを合理的に低減できる）と言えるのか曖昧模糊としています。

例えば経理部員が３人しかいないような小さな会社で、仕訳入力をしたら試算表や元帳などが印

刷されるような PC 用のソフトウェアを使っているようなケースで、例えばパソコンルームへの入室制限や個人別 ID のアクセス権限の変更管理などが必要でしょうか。ソフトウェアを PC に設定する人とその PC を利用する人との分離が必要でしょうか。

換言すれば、IT 全般統制はそれ自体が財務報告上のリスクに対して直接的に作用するものではないため、先ずはどの程度のリスクを想定してどの程度の全般統制を整備する（裏返せば、どの程度の業務処理統制が機能しないで誤ったデータが生成されるリスクや、悪意によってデータ等が改竄されるリスクを許容する）か経営者による判断が必要ということになります。

一言で経営者による判断というのは簡単ですが、経営者が直接判断するというよりも、IT への投資予算方針や業務依存方針などを通じて間接的に判断されていると考えればよいでしょう。

私見ではありますが、結局は、不正をどの程度まで想定（類型、頻度、金額）するかということと、不正や誤謬による財務報告上の許容できない虚偽記載がきちんと発見できるかどうかということと相俟って議論しなければ、IT 全般統制の深度を議論しても建前論に終始してしまうことになるでしょう。不正や誤謬は防止･発見できるに越したことはありませんし、その可能性はゼロということは論理的に不可能ですので、「リスクが心配だ、だから統制が必要だ」という一側面だけで議論していると、「必要な」統制は一方的に膨らんでいく一方です。制度はリスクの「合理的な軽減」を期待しているに過ぎませんが、システムを業として担う人は、何とか完璧に防止発見しようと努めるでしょう。しかし必ずしも予算がつく（つまり経営者が資源を配分してくれる）とは限りません。また、財務報告上の重要な虚偽記載を防止発見するための統制のレベルと、会社の他の業務を適切に行うための諸活動を維持する統制のレベルとは、自ずと資源配分の重点が異なるはずです。そういった諸々の条件をバランスよく理解して落とし処を探ることが、リスクの評価という行為に他なりません。経営判断とは、リスクとリターンとの比較考量ですから、必ずしもリスクの高い領域が機械的に優先措置されるものとも限りません。それらを会社の中できちんと議論して論点を明らかにして経営者に判断を仰ぎ、さらに経営者の判断を取締役会等において様々な知見を通じて批判検討するという状態が、制度が想定している健全な内部統制の姿であり、IT に関して言えば「IT 全社統制」と言われている分野の論点です。

※ちょっと一言

- ITAC で 25 件サンプルテスト頑張る覚悟があるなら、ITGC 評価不要。別に大層なものじゃないと思う - 名無しさん (2010 年 12 月 21 日 10 時 23 分 50 秒)
- そうですね。統制評価に「こうであればよい」とか「こうでなければならない」というのはありませんね。あくまでリスク判断によって変わるものですから。 - 著者より (2014 年 01 月 12 日 17 時 48 分 09 秒)