IT 統制の評価が必要となる場合

キーコントロールを識別する過程の中で、IT に係る統制（IT 業務処理統制）がキーコントロールとして識別されれば、その IT 基盤の全般統制を評価対象とするかどうかを検討する。ここで重要なことは、IT 基盤が会社にあるからそれを評価・監査するということではなく、あくまでも一連の財務報告プロセスにおける IT の位置づけを見極めた上で、重要なものを選別して評価・監査するという点である。

■ IT 基盤の識別

評価・監査対象とすべき IT 基盤の識別は一般に次のように行なわれる。すなわちそれぞれの段階での判断が加わるので、すべからく IT を評価・監査しなければならないわけではない。

評価対象とされた業務プロセスを識別

基本的には企業の主たる業務に関わるプロセスすなわちバリューチェーンと呼ばれる部分を識別すべきですが、日本の制度では、いわゆる「三勘定」（売上・売掛金・棚卸資産）とされているので、これに係る部分を識別する。なお、たとえばデリバティブなどを大規模に行なっている場合には、特定された固有のリスクがあるはずなので、三勘定以外にも例えば資金運用なども対象となる。

支える自動化された統制活動

業務プロセスのフローチャートなどによって、財務報告に係るキーコントロールを識別する。ここが最も重要なところで、単にシステムを使っているからということではなく、財務報告に重要な影響を与える数値が生成加工される手続のうち IT により自動化されている部分があるか否かをきちんと識別するべきである。自動化の中にも、単なる転記、集計といった自動化から、複雑な演算（ブラックショールズモデルによるオプション価値の計算など）まで色々とあるので、その依存度、誤りのリスクなどを考慮する。一般には、IT により自動化された部分のうち、最も大事なのは、人と一体となって機能する統制（いわゆるキーレポートの生成）のところである。キーレポートとは、IT から出力される各種帳票（画面を含む）のうち、人がそれを見て何らかの判断をして何らかのアクションを起こすことが期待されているものである。そのアクションには、システム上の会計データに対して必要なフィードバックをするためのものもあれば、会計には直接関わらないが影響すると想定されるものなどが含まれる。たとえば、

- 一日の処理件数を出力して、手元にある入力原票の枚数と照合して、齟齬があればその原因を追究して対策をとる。
- 滞留売掛金のリストを出力して、必要な回収措置をとる。
- 異常なアクセスが検出された場合に、警告を発してアクセスの正当性の確認や、不正アクセスへの防止策をとる。

それを実現するアプリケーションシステム

自動化された処理のうち、キーコントロールに相当するものがあった場合には、それを実現しているアプリケーションシステムを識別する。

そのアプリケーションシステムを機能させる各種基盤

俗にプラットフォームと言われるアプリケーションが稼動する「システムの単位」を識別する。Operating System、データベース管理システム、ハードウェア構成、ネットワーク構成などから共通性を判断する。

それらの機能を保証する IT 全般統制を評価する

識別された IT 基盤に係る、開発管理、変更管理、運用管理、アクセス制御について評価する。

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

ITGC でキーコントロールといえば GAIT

IT 全般統制の評価範囲を決定するに当たっては、The GAIT Principles http://www.theiia.org/guidance/technology/gait/ が発行されているものの中で最も簡潔明瞭な指針となるだろう。

GAIT では４つの原則が示されている。以下意訳すると、

原則１

IT 全般統制プロセスにおけるリスクの認識とそれに関係する統制を識別するには、重要な勘定やそれに関係するリスクやキーコントロールを識別したトップダウン＆リスクベースアプローチの延長として行なわなければならない。

チェックリスト方式などは非効果的で非効率である。

原則２

識別すべき IT 全般統制リスクとは、財務会計上重要なアプリケーションとデータにおける重要な IT 機能に対して影響を与えるものであるべき。

トップダウン＆リスクベースアプローチとは、業務プロセスにおいて虚偽記載をもたらすリスクのあるポイントとそれに関係するキーコントロールを識別する。その上で、それが IT 機能（すなわち、自動化されたキーコントロールや、キーレポート、重要な財務データ）に拠っている場合に、そのアプリケーションは財務会計上重要となるから、IT 全般統制プロセスの欠陥からもたらされる IT 機能のリスクを識別しなければならない。

原則３

識別すべき IT 全般統制プロセスのリスクは、業務プロセス中にあり、かつ、各 IT レイヤ（アプリケーション、データベース、オペレーションシステム、ネットワーク）上に存在している。

原則４

IT 全般統制プロセスにおけるリスクは、IT 統制目標の達成によって軽減されるものであり、個々別々のコントロール手続ではない。

各 IT 全般統制プロセスには、IT 統制目標を支援する手続が埋め込まれている。IT 統制目標とは、

・システムが実装される前に、適切にテストされ評価される
・データは未承認の変更から保護されている
・運用における支障や事故は、適切に対応され、記録され、調査され、解決される

先ず第一に、財務報告に関連する IT 統制目標を識別することが肝要であり、その後にその統制目標を満たす IT 全般統制のキーコントロールを識別すべきである。識別された IT 統制目標に関係

ない IT 全般統制手続は、たとえ重要であっても、ICFR の評価対象に含める必要はない。

IT 統制における留意

IT を用いた統制は「予防的」側面が強い

すなわち IT で生成される情報を活用･分析する手続がないところで、IT の統制を議論しても、それは「財務報告の適正性」という目的からは外れた IT 統制の確立を自己目的化した議論になる可能性がある

全体感が必要

IT 部門とユーザ部門との「統制の擦り合わせ」「統制のバランス」を見ている人がいないとそれぞれに閉じた議論が全体の不効率に繋がる。特に IT を専門にする人と会計を専門にする人との協議は効率的効果的にキーコントロールを選び評価する上で重要である。IT 専門家の統制に対する目標は、コントロールによってあくまでも統制による完全なデータ処理をもたらすことを目指しつつも予算や優先順位などの経営者による制約があることを前提にその中でベストなソリューションを提供することを使命としている。他方、監査に求められる保証はあくまでも合理的保証であることから､常に重要性の判断が加わる。したがって IT 部門だけにキーコントロールの選定を任せるのではなく、経営目標と照らし合わせるというフィルターをかけて、最終的には経営者の意思としてのキーコントロールの選定としなければならない。

蛸壺に陥る原因と考えられるもの

- 知識言語の違い「IT 知識の壁」vs.「会計知識の壁」
- 業務思想の違い「自動処理」vs.「手処理」
- 経営者が意思と目的を明確にしないと蛸壺にこもりがちになる可能性が高い。

教訓

- 内部監査部門は全体としてリスクが軽減されているかどうかを言う観点（＝経営者の視点）をもち、経営者に提言することが期待されているのではないか。
- 財務報告の適正性を検証するに当たっては、IT 統制に依拠する形で検証するのか、IT 統制よりも人間統制を重視した形で検証するのかは、評価者、監査人双方にとっては重要な戦略といえる。

■参考

IT 部門と経理部門との業務に対する思考視点視野の違いを整理してみたい。

観点	IT 担当	経理担当	発生する問題点
サービス対象	財市場、経営、組織	金融市場、経営、組織	
業務目標	情報資産保全と情報付加価値創出	付加価値測定の報告	
経営者の視点	内外サービス提供の手段	サービス測定の手段、法的義務の履行	

関心業務	いわゆる現場業務	経理業務	
扱う情報	活動情報	会計情報	

※ちょっと一言

- 経営者によっては、ＩＴから非ＩＴ化へという流れもあるでしょう。10 年ぐらいまでＩＴ不要論がありましたが、それを思い起こします。 - shibayan (2008 年 03 月 13 日 20 時 49 分 52 秒)
- IT 投資は一旦はじめたら中々やめられませんからね。投資効果は見極めるべきですね。 - なわ (2008 年 03 月 16 日 07 時 35 分 28 秒)
- ＩＴ投資をすることは、悪いことではないですが、それが、財務諸表の作成にどう係ってくるの検討を、投資段階から慎重に判断することがポイントとなりそうですね。 - shibayan (2008 年 03 月 16 日 12 時 21 分 18 秒)
- ごもっとも。おそらく今後は開発段階から財務報告への影響を評価するというプロセスが必要になるだろうという話を他所でしました。 - なわ (2008 年 03 月 16 日 15 時 09 分 41 秒)
- ITCLCって判りにくいけど、この制度での一番のポイントは、きっとそこですね。 - shibayan (2008 年 03 月 16 日 18 時 00 分 23 秒)