東京海上日動リスクコンサルティング（株）
情報グループ
主任研究員　　吉賀　豪

内部統制とIT統制

１．はじめに

内部統制の要素の一つに「IT への対応」がある。しかし、「内部統制を整備するために、IT 統制をしなければならない」と漠然と認識することは危険である。「IT 統制をしなければならない」という意識が先行すると、「COBIT※1 に準拠しよう」、「システム管理基準※2 に準拠しよう」、「ISO27001※3 に準拠しよう」など、デファクトスタンダードとされている規格への対応に目がいってしまう。しかし、そのような対応だと、「なぜ IT 統制をやるのか」という本質が見えずに、規格に準拠することが目的になってしまう。規格に準拠することは IT 統制の本来の目的ではない。また、IT 統制そのものも内部統制の目的ではなく、あくまで内部統制を実現するための手段の一つである。そこで本稿では、本来 IT 統制とはどのように考えるべきなのかを考察したい。

２．IT 統制の目的

上に述べたとおり、IT 統制は内部統制の手段である。逆に言えば、IT 統制の目的は内部統制の実現にある。では内部統制の目的とは何であろうか。金融庁が発行した実施基準※4 における内部統制の定義を復習したい。

内部統制は、基本的に、企業等の４つの目的（①業務の有効性及び効率性、②財務報告の信頼性、③事業活動に関わる法令等の遵守、④資産の保全）の達成のために企業内のすべての者によって遂行されるプロセスであり、６つの基本的要素（①統制環境、②リスクの評価と対応、③統制活動、④情報と伝達、⑤モニタリング、⑥IT への対応）から構成される。

このように、実施基準では「業務の効率性及び有効性」「財務報告の信頼性」「法令等の遵守」「資産の保全」が内部統制の４つの目的として書かれている。しかし、ここで誤解してはならないのは、これらは「内部統制そのものの目的」ではないということである。ここでは「４つの目的を達成するプロセスが内部統制」と定義しているだけであり、なぜ内部統制をおこなうのか、つまり内部統制を整備すること自体の目的は何なのか、ということは触れられていない。もう一度定義を読み返して欲しい。これら４つの目的は「企業等の目的」と書かれている。内部統制の目的とは書かれていない。

ここで少し考察したい。「企業等の目的」とはこれが全てだろうか。例えば、読書の皆様がご自身で会社を立ち上げることを想像して欲しい。「私は財務報告の信頼性を確保するために会社を立ち上げる」という方はいるだろうか。または「私は法令遵守をするために会社を立ち上げる」という方はいるだろうか。おそらく多くの方は「〇〇といった製品（サービス）を世に提供する」という目的で会社を立ち上げるのだろう（お金儲けを第一目的にする方もいるであろうが）。そして、そのための自明の目的として会社の維持・発展というものが出てくるだろう（これはお金儲けを第一目的にする方でも異論のないところだろう）。さらに、会社を維持・発展させるためには、内部統制が求めるところの「業務の効率性及び有効性」「財務報告の信頼性」「法令等の遵守」「資産の保全」を必然的におこなうこ

とになるであろう（我が社は上場しないから財務報告の信頼性は関係ない、と思われる方もいるかもしれない。しかし、例えば、税金の計算などのためにも、やはり財務報告は正しくなければならない）。そのように考えると、内部統制を整備することの目的は、会社の維持・発展であると言える。

だいぶ遠回りになってしまったが、これで内部統制そのものの目的がはっきりした。また、内部統制実現の手段の一つである、IT 統制の最終的な目的もはっきりしたことになる。IT 統制の直接の目的は内部統制の実現にある。しかし、最終的な IT 統制の目的は、会社の維持・発展（および製品（サービス）の提供）である。このことを忘れてはならない。（図１参照）

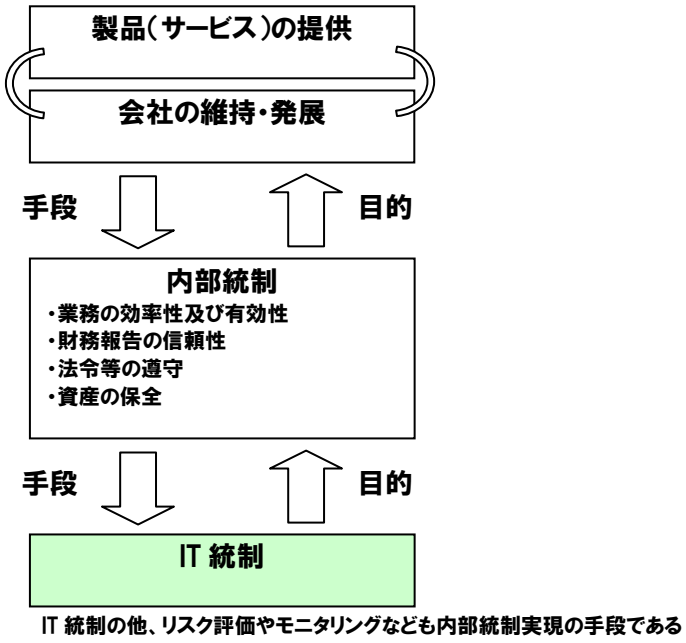

図1．IT 統制を取り巻く目的と手段

３．IT 統制実現の手段

さて、ここまで IT 統制の目的について述べてきたが、やはり現実問題として頭をよぎるのは「どうすればいいのか」ということだろう。現在多くの企業の担当者の悩みは、IT 統制をおこなうと対策が膨大で費用が相当にかかる、という漠然とした恐れである。そこで以下では、どのように IT 統制を実現させていくのかを考察したい。

本稿の初めにも述べたが、「IT 統制」という言葉だけに注目すると、「COBIT への準拠」、「システム管理基準への準拠」、「ISO27001 への準拠」などが思いつく。しかし前章で、IT 統制の目的は内部統制の実現であることを示した。特に日本版 SOX 法[※5]への対応に注目した場合は、内部統制の一部である「財務報告の信頼性」の確保が強く要求される。つまり、「我が社は COBIT に準拠しなければ、財務報告の信頼性が確保できない」という判断であれば、日本版 SOX 法に対応するために COBIT に準拠する、ということが IT 統制実現の解になるだろう。

では「財務報告の信頼性が確保できない」とはどういうことであろうか。ここを明確にしないままでいると、「よく分からないが、とりあえず COBIT に準拠しよう」ということになってしまう。「財務報告の信頼性が確保できない」とは、言い換えれば「財務報告の信頼性を脅かすリスクに対応できていない」ということである。リスクの例としては、「経理シ

ステムの売上データが誰でも変更できてしまう」などがある。つまり、財務報告の信頼性を確保するためには、まず、リスクとしてどのようなものがあるのかを明確にする必要がある。そして、リスクを明確にしてから「さあ、どう対応しようか」と考えるのである。これは一般的にリスクアプローチと言われる考え方で、実施基準においてもリスクアプローチを用いて内部統制を整備するよう求められている。そしてこの考え方は IT 統制についても例外なく当てはまる。

リスクアプローチを用いて IT 統制をどのように整備するのかを具体的に考えてみよう。リスクを明確にする段階で「経理システムの売上データが誰でも変更できてしまう」というリスクが発見されたとする。そのようなリスクへの対応としては、「限られた人だけが売上データを変更できるようにアクセス制御をする」というものがあるだろう。しかし検討するべき対応方法はそれだけではない。確かに、アクセス制御を実施すれば「経理システムの売上データが誰でも変更できてしまう」というリスクには対応したことになる。しかし、例えば「なぜアクセス制御のない経理システムがあったのか」ということまで考えを広げるとどうであろうか。そもそも、経理システムを導入する段階でしっかりとアクセス制御を設定していれば、「経理システムの売上データが誰でも変更できてしまう」という状況にはならなかったであろう。このように考えると「システム導入をしっかり管理する」といった対策が見えてくるだろう。このように、リスクを入口として、表面的な対策だけでなく、隠れている根本的な対策まで掘り下げて考えていくことが、リスクアプローチによる IT 統制の実現である。

また、もしここで「どのようにシステム導入を管理して良いのか分からない」ということであれば、COBIT やシステム管理基準などの規格を参考にすることが有効である。これらの規格は、どのように IT を管理するのかという指針を示してくれている。また、リスクへの対応方法の検討に慣れていない場合は、「データが誰でも変更できてしまう」というリスクから「システム導入を管理する」という対策が発想できないかもしれない。そのような場合にも規格は参考となる。なぜならこれらの規格は、IT 統制に必要な要素を一通り網羅しているからである。そこから必要と思われる対策を選び、実行していけば良いということになる。つまり、規格に書かれているすべての対策をおこなう必要はないということである。ただし、「規格に書かれているすべての対策をおこなう必要はない」と聞いて油断してしまわぬよう一言釘を刺しておくと、これはあくまでリスクに応じてメリハリをつけて対策を選択することを認めているのであり、「経費がないからやらなくて良い」と言っているわけではない。

４．まとめ

これまでに述べた IT 統制のポイントは以下のとおりである。

・IT 統制の最終目的は会社の維持・発展である
・IT 統制はリスクアプローチで考える
・COBIT などの規格はあくまで参考資料であり 100%準拠する必要はない

これら IT 統制の本質的な考え方を忘れなければ、会社は適切な IT 統制を整備することが出来るだろう。また、IT 統制を実現する担当者がしっかりとその本質を理解し、IT 統制という言葉に対する漠然とした悩みや不安が少しでも解消されることを期待したい。

※1：米国 IT ガバナンス協会発行。IT 統制の指針。Control Objectives for Information and related Technology の略
※2：経済産業省発行。IT 統制の指針
※3：情報セキュリティマネジメントシステム（ISMS）に関する国際規格
※4：本稿においては、金融庁発行の「財務報告に係る内部統制の評価及び監査の基準」および「財務報告に係る内部統制の評価及び監査に関する実施基準」の総称を指す
※5：本稿においては、金融商品取引法における内部統制に関する部分（第 24 条など）を指す

http://www.tokiorisk.co.jp/

参考文献：
・最新 リスクマネジメントがよ～くわかる本（東京海上日動リスクコンサルティング㈱）
・RISK RADAR 2007-1：「内部統制とリスクマネジメント」
・TRC EYE Vol.124：「内部統制は健康の維持・増進システム」
・TRC-EYE Vol.133：「内部統制とコンプライアンス」
・TRC-EYE Vol.137：「内部統制と会社法」
・内部統制ハンドブック（東京海上日動火災保険㈱）

以上