研究会報告

ＣＩＡフォーラム研究会報告

内部統制におけるＩＴ統制評価の研究

＜1＞

関西研究会No.14

ＣＩＡフォーラムは、ＣＩＡ資格保持者の研鑽及び相互交流を目的に活動する、社団法人日本内部監査協会（ＩＩＡ－ＪＡＰＡＮ）の特別研究会である。各研究会は、担当の座長が責任をもって自主的に運営し、研究期間、目標成果を設定し、研究成果を発信している。

当研究報告書は、ＣＩＡフォーラム関西研究会No.14が、その活動成果としてとりまとめたものである。報告書に記載された意見やコメントは、研究会の「見解」であり協会の見解を代表するものではなく、協会がこれを保証・賛成・推奨等するものでもない。

【目次】

第１章　テーマ設定の背景

ＩＴ統制に関しては、金融庁の「実施基準」において、対象となるプロセス等は記載され、基本的な考え方は示されてはいるものの、その具体的なアプローチ方法に関しては、記述されておらず、各事業法人は、ＣＯＢＩＴ等にその解決の道を探るなど、多くの労力をこれまでに費やしてきた。

「実施基準」が公表された後においても、

経済産業省によるＩＴ統制ガイダンスが発表され、また、日本公認会計士協会からも取組指針が公表されたが、必ずしも方法論が同一のものと理解しにくく、事業法人の実務家は、この１年、取組みの早かった企業ではここ数年にわたり、「航海図のない旅」を余儀なくされてきたように思える。

私達は、こうした状況下にあって、実務家の立場で現場目線からの有意義なアプローチを見出すことはできないだろうかとの強い思いから、ＩＴ統制とりわけＩＴ全般統制のスコーピングと評価を含めたアプローチ方法を研究することとした。

１.「ＩＴ統制」の「ＩＴガバナンス」と「内部統制」における位置付け及び問題認識

ＩＴ統制に関しては、「ＩＴガバナンス面から語られるケース」と「ＵＳ－ＳＯＸや日本の金融商品取引法の観点から述べられるケース」が、また、内部統制全般との関連においても、「会社法対象としての４つ（業務の有効性・効率性、財務信頼性、法令遵守、資産保全）を目的とするケース」と、「金融商品取引法上の財務信頼性確保を目的とするケース」から述べられることがある。

経営上のリスクは、環境と目的によって決まり、それに対するリスクアプローチやスコーピングも異なってくる。リスクをスタート段階で区分（例えば、ＩＴガバナンスとしてのリスクか、財務信頼性以外のリスクか、あるいは財務信頼性確保上のリスクか）しない場合、スコーピングも的確なものにはならないように思われる。

よく引き合いに出される例として、「Ａ証券会社による単価、数量の誤発注」事件がある。この事件を、内部統制における「会社法の求め」と「金融商品取引法の求め」から捉えると、会社法上でのリスクとしての「注文ミスによる損失の発生リスク」の一方、金融商品取引法上では「損失が適切に処理されておれば、リスクは特になし」と、それぞれ区分して把握の上対応することは、通常、理解されていることであると思う。この例においては、会社にとって、「注文による損失の発生リスク」は、日常業務の中で繰り返される危険性の高いリスクであり、これに対する統制活動は、最も厳しい内容とすべきであると考える。

更に例をあげてみると、ソシエテ・ジェネラルにおける不正業務事件がある。

この事件の原因は、ＩＤの改廃手続の杜撰な管理にあるが、「業務の適正な運営」からの観点では、リスクアプローチする「深さ」に、差をつけて取り組むべきではないだろうか、という問題認識がある。

通常のアプローチでは、ＩＤ管理がルールにそって適切に運用されておれば、「適正」の評価となるが、上述の「業務の適正」という観点からは、「重要業務につくメンバーのＩＤ管理ルールとチェック」方法は、通常のＩＤ管理より厳しく、設定されるべきだとも考えられる。

これは、私達の反省も含めてではあるが、この区別が最初に明確にされない状況下で、また、評価も金融商品取引法対応としての「財務信頼性確保」の観点からの方法が論じられてはいるものの、会社法対応としての観点からの評価方法が未着手段階のため、統制範囲のスコーピングや評価方法が「一般論」として、形式的に、また、最大公約数的に語られてきたのが、実態ではなかっただろうか。

つまり、ＩＴ全般統制段階では、「リスク」を「一般化」しているのが、これまでのアプローチであったように思う。また、評価方法も「一般化」、「最大公約数」的に実施されてきているとも推測している。スコーピングの曖昧さと評価方法の曖昧さは、内部統制が、法的対応事項であるだけに、少し注意深く考えるべき事項のように思っている。

もう少し突っ込んだ言い方をすると、「財務信頼性のスコーピング」を厳密に意識して取り組まないことが一般的なアプローチへと流れ、ひいては会社法の期待するアプローチにも「深さ」が不足するような、焦点の定まらないものとなり、その評価手法とも相俟って会社法上での善管注意義務違反が問われる事態に陥らないかという懸念である。これは、「統制行動の評価」が、金融商品取引法の「実施基準」では明示されてはいるものの、会社法上では、具体的には明示されているわけではなく、一般的には「実施基準ベースでの評価の応用編」として認識しているレベルにあることも影響している。

内部統制違反事件が発生したとき、裁判に臨んで「金融商品取引法の『実施基準』にそって、一般的な管理の運用を決め、文書化３点セットも整備し、評価も定期的に行っていたが、十分機能していなかったことが問題であった」という説明で会社はエクスキューズできると考えられるのだろうか。

例えば、「適切なＩＤ管理の実施」が問われた時に、一般的な「ＩＤ管理ルールの設定」を形式的に説明するだけでは、事件発生時には、十分な抗弁とはなり得ないのではないか、というのが私達の研究テーマの１つの問題認識としてある。つまり、スコーピングと評価は、リスクごとにポイントを絞り、明確かつ厳密に行うことが、本来の統制行動につながると考えている。

以下は、そうした問題意識を持つに至った経緯と主要な課題についての私達の提言である。

２．研究のステップ

今回私達は、メンバーの所属する企業の中で、ＩＴ統制に関する取組みがどのように進められたのかを、まず共有化することから始めている。

この共有化の過程で、国内企業の取組みがどのように変遷していったかを、まずレビューする（第２章：要所で意見も加えている）とともに、その中で浮かび上がった問題を抽出しながら、一部の項目において１つの方向性の提言を試みた。この段階では、スコーピングなど体系だったアプローチに基づくものではなく、端的にいえば、メンバー全員の「勘」、「落とし所」といったそれぞれのビジネスマン経験に裏打ちされたものである（第３章：なお、各社の取組状況の詳細については、別添の「金融商品取引法上の内部統制取組におけるＩＴ統制評価の実状」を参照。次号掲載予定）。そうした「落とし所」に根拠を与える手法として、体系だったアプローチについて探求することとした。

１つは、私達研究会メンバーとしての手法（メンバーが依拠した日本の監査法人のアプローチを含む）として、もう１つは、ＧＡＩＴアプローチの検討を通じてである（第４章）。

最後に、私達の取組みのメインテーマであるＩＴ統制評価に関しての提言である。ここでは、「評価体制」や「評価方法」」について、監査部門の「客観性」、「独立性」とも関連させて提言する（第５章）。

３．本論における用語の定義

本論における「ＩＴ統制」関連の用語の定義について冒頭にふれる。用語については、基本的には金融庁「実施基準」にそって使用している。「ＩＴ全般統制」は実施基準の「ＩＴに係る全般統制」を指し、一般的にＩＴＧＣと略称されている。本論の第２章から第６章までは、「ＩＴ全般統制」に関する記述である。「ＩＴ全社統制」、「ＩＴ業務処理統制」については、当研究会参加企業にて実態調査を行う対象としたことから、添付資料３（次号掲載予定）において使用している。これらの定義については、「ＩＴ統制」も含めて用語集（今号・次号とも掲載）において説明している。

第２章　ＩＴ全般統制の国内取組状況レビュー

１．ＩＴシステムとスコーピング

Ｊ－ＳＯＸへの対応は、初めての取組みでもあり、多くはアメリカの構築事例の影響下で、明確な方法論が不在のまま、ともかく全方位で進められた面があった。当初から「財務報告の信頼性」に軸足を置き、それに対するＩＴシステムのリスク・コントロールの整備・運用に絞っていれば、経験の深いシステム責任者のアプローチは、恐らく相当違ったものになっていたであろう。アメリカにおいても、ＧＡＩＴメソドロジーというトップダウンアプローチによるＩＴリスクへの対応手法が示されたのは、2002年ＳＯＸ法制定から６年後のことであった。

当初、情報システム部門は、「ＩＴへの対応」の取組みについて、どのようなスタンスをとっていたであろうか。

情報システムは数年で変革できるようなものではない。仮にＩＴ全般統制上、不備事項があったとしても、それだけの理由で、すぐに手を加えられるほど情報システムは簡単なものではない。システム停止の影響は社内にとどまらず社外にも多大の損害を与える。情報システム部門のこうした認識から、「ＩＴへの対応」は当初から本腰の入らないものにならざるを得なかったのではないかと考える。過去に多額の投資と時間と労力を注ぎ込んで構築されてきた情報システムは、組織体の財産であるだけでなく、組織風土の一部ともなっている。長年培われた既存システムは、人的な慣れもあり、簡単にリプレース、又は統合できる対象ではないのも現実である。情報システム部門の長であっても自社システムの全体を必ずしも把握し切れているわけでもない。初年度のＩＴへの対応について、大半の組織体で十分な対応がとれなかったことは、以上の背景と無縁ではなかった。

ＩＴシステムは、これからも使い続けられ、内部統制も終わったわけではなく、これから毎年見直しながら理想の姿を目指して改善を繰り返していかねばならない。初年度に不十分な整備状況であったとしても、組織体は今後の長期課題として「ＩＴへの対応」を改善していかねばならない。

例えばログ情報の取得が容易なシステム環境があれば、経営者は新しい戦略目的を立案し、そのリスク認識に基づいて、コントロールとそのテスト方法を自由に設計することができる。こうした逆進テストが実施できる環境が実装されて、初めてＩＴ全般統制についてのテスト範囲、スコーピングを無理なく行うことが可能となる。アプリケーションの変更管理も、システムの機能として実装されていれば、ＩＴ全般統制のスコーピングは、該当アプリケーションの変更ログを見るだけで、その信頼性を保証できる。情報セキュリティ管理についても、どのような取引が行われたか、すべてのログが取得されていれば、監査人が独立した立場で取引ログデータを抽出してチェックできる。ＩＤ・パスワードが個別に与えられ、その変更管理がシステムの機能として実装されていれば、監査人は、その実装を確認するだけで信頼性を保証でき、スコーピング範囲も自在に設定してサンプルテストを実施できる。だが、このような情報システム環境が一朝一夕に実現できないことは明らかである。

こうした状況を踏まえると、当分の間「ＩＴへの対応」、ＩＴ全般統制のスコーピングは、自社システムの現状と、理想のシステムとの乖離度合いを認識した上で、本来の目的である「財務報告の信頼性確保」にフォーカスし、目的を絞ったトップダウン型のリスクアプローチを続けることが妥当であろう。そして、いずれかのタイミングで、一気に内部統制を考慮したシステムにレベルアップすることになると考える。

以下では、試行錯誤を繰り返し取り組んできた初年度までの「ＩＴへの対応」状況を振り返り、⑴「実施基準」公表まで、⑵公表後、⑶「11の誤解」公表の３フェーズで、それぞれ、金融庁、監査法人のコンサルティングサービス、企業の対応について三者三様の動きを整理し、その反省から、ＩＴ全般統制のスコーピングのあり方について考察していく。

２．スコーピングの変遷――迷走したＪ－ＳＯＸへの取組み

⑴　金融庁「実施基準」公表前夜――ＵＳ－ＳＯＸ中心のアプローチ

①　社会現象：内部統制ＩＴ狂騒曲――ＩＴ統制はＩＴ産業のチャンス？

Ｊ－ＳＯＸに、内部統制の基本的要素として「ＩＴへの対応」が盛り込まれ、「内部統制」、「ＩＴへの対応」が、にわかにクローズアップされ、話題が先行することになった。

財務報告の信頼性を担保する要素としてＩＴが極めて重要らしいといった漠然とした合意が企業人の中で共有され、それに伴い、これをビジネスチャンスと捉えたＩＴ産業は、一斉に内部統制入門セミナーを開催し始めた。

しかし「ＩＴへの対応」をひとくくりで議論していた当時を振り返り、改めて整理してみれば、次の３つの区分を念頭に置き、その対応を明確にしてスタートを切るべきであった。

１．ＩＴを活用している業務処理に対する統制
２．ＩＴそれ自体の全般的統制
３．内部統制の構築・強化におけるＩＴの利用（吉田 洋教授「ＩＴ環境における内部統制・ガバナンスの動向」『月刊監査研究』2009年６月号参照）

いうまでもなく、各種セミナー主催者の狙いは３項にあって、その導入部として１項、２項の説明がセットされたものであった。

前提となっていたのはＵＳ－ＳＯＸ法が要求していた膨大な文書化作業、そして評価に際して求められる証憑準備が日本でも不可欠になるとする見通しであり、それらに対応するためには、既に米国で開発されたＩＴ整備ツールが必要になるであろうとするものであった。

各種セミナーでは、ＵＳ－ＳＯＸの構築事例紹介から、本番年度までの時間が少ないことを認識させ、日本でも、早期にＩＴツールを導入し、文書化作業に着手することを推奨していた。そのためＵＳ－ＳＯＸで活用された文書化ツール、文書保管ＤＢ、運用評価のための検索ツールなどの紹介合戦が繰り広げられていた。

②　監査法人のコンサルティングサービス：COBIT for SOXに準拠

監査法人は、コンサルティングサービスを受ける企業に対して、金融庁の「実施基準」が公表されるまでは、ＵＳ－ＳＯＸ法をベースに、全方位で取り組むことを推奨せざるを得なかった。すなわちCOBIT for SOXに準拠したチェックリスト又はリスクコントロールマトリックス（ＲＣＭ）の活用が専ら推奨された。

既に公表されていた金融庁の「実務指針」はＣＯＳＯフレームワークに準拠した内容であり、全勘定科目の業務プロセスを対象にＩＴ統制を考慮しておけば、どのような「実施基準」が公表されても対応できると当時は考えられていたのである。

本番開始年への時間的制約があり、最も時間を要する業務フローの分析と、文書化作業から着手するスケジュールが、最初に提示されていた。しかし「ＩＴへの対応」部分は、具体的に示されないままであった。

後日、監査法人側の体制を振り返ってみると、財務報告の信頼性を主たる業務とする担当チームには「ＩＴへの対応」ノウハウが少なく、ＩＴ統制に関するコンサルティングサ

ービスは、別の専門チームに頼りがちで、業務担当チームはＩＴには踏み込まない傾向があったようである。

③　企業の対応：ＵＳ－ＳＯＸの「不備」、「重要な不備」、「重要な欠陥」に学ぶ

企業内で立ち上げられた内部統制推進チームの多くは、経理部門又は内部監査部門中心の体制で、それとは別建てチームでＩＴへの対応を計画するところが多かった。また監査法人もＩＴコンサルティングサービスの要員不足があり、当初からＩＴへの対応に関する検討と出番は先送りされてしまった。

業務プロセスフローがほぼ出来上がった頃、「ＩＴへの対応」チームメンバーがシステム開発部門から選定された。この別建てチームで開始された「ＩＴへの対応」は、システムの信頼性保証が中心で業務プロセスフローとのリンクは、当初考慮されていなかった。

システム開発の現場部門が認識するリスク対応は、必然的に、過去に経験した不備事例からのボトムアップアプローチが主流となる。情報システム部門のメンバーは、独自にＩＴ企業が主催するセミナーに足を運び、ＩＴ上のキーコントロールの不備が発見され、是正されなければ、内部統制の信頼性全体が否定されるといった誤解も生じていた。

既存システムの問題点ばかりが注目され、現場で長く利用されてきた便利なＩＴシステムであっても、「アプリケーションの変更管理」、「情報セキュリティ管理」、「ＩＤパスワード管理」に内部統制のコントロール不備があれば、無条件で使用できなくなるとさえ思われた。

これらは、確かに業務の有効性を高めるために重要なコントロールだが、直ちに財務報告の信頼性に影響するとまでは言い切れない。しかし「財務リスク：財務の信頼性確保に影響するリスク」と「業務リスク：業務の有効性・効率性に影響するリスク」の区別がつかない現場では、ＩＴ全般統制の問題指摘項目だけが一人歩きした。

過敏な対応ではあるが、「ＩＴの不備指摘を避けるのが先決であり、本番年度まで新規システム開発は凍結すべきだ」といったことさえ主張されていた。

④　会社法施行（2006年５月）

2006年５月会社法施行に伴い、５月の取締役会で「内部統制体制の整備に関する基本方針」を決議した企業は多かった。

経営トップが関与し、取締役会決議がなされたが、実際は形式的な手続にとどまり、具体的な取組みは内部統制推進チームに丸投げしていた企業も少なからず存在したようである。内部統制整備はトップの役割だとの認識が経営トップに浸透していたとはいいがたかった。

会社法により求められる内部統制の構築は、その目的において、金融庁の「実施基準」より広範囲であり、業務の有効性やコンプライアンスについて取締役会の善管注意義務を求めている。

会社法　第362条（取締役会の権限等）取締役会は、すべての取締役で組織する。
４項　取締役会は、次に掲げる事項その他の重要な業務執行の決定を取締役に委任することができない。
一～五　省略
六　「取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備」
会社法施行規則　第100条（業務の適正を確保するための体制）法第362条第４項第６項に規定する法務省令で定める体制は、次に掲げる体制とする。（１項）
一　取締役の職務の執行に係る情報の保存及び管理に関する体制
二　損失の危険の管理に関する規程その

他の体制
三　取締役の職務の執行が効率的に行われることを確保するための体制
四　使用人の職務の執行が法令及び定款に適合することを確保するための体制
五　当該株式会社並びにその親会社及び子会社から成る企業集団における業務の適正を確保するための体制

これらの中身をよく読めば、会社法施行規則第100条第１項を遵守するには、ＩＴの活用及びＩＴによる統制が不可欠であることは論を俟たない。だが会社法に基づき「内部統制体制の整備に関する基本方針」を決議した企業において、業務に関わるＩＴ統制の不備に関して議論されることは少なかった。

第１章でふれた「Ａ証券会社による単価、数量の誤発注」事件や、「ソシエテ・ジェネラルにおける不正業務事件」は会社法が求める「業務の有効性・効率性に影響するリスクへの対応」に関してＩＴ面で対策がなされていなかった結果生じたものであり、「内部統制の整備」において、今後検討を深めなければならない重要課題と考えている。

⑤　システム管理基準（2004年10月）

また我が国には1985年１月に制定され2004年10月８日に再改訂された「システム監査基準」があり、同時に策定された「システム管理基準」がある。

その前文には、以下のようにＩＴ統制の目的が定義されている。

「組織体が情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的は、以下のとおりである」

・情報システムが、組織体の経営方針及び戦略目標の実現に貢献するため
・情報システムが、組織体の目的を実現するように安全、有効かつ効率的に機能するため
・情報システムが、内部又は外部に報告する情報の信頼性を保つように機能するため
・情報システムが、関連法令、契約又は内部規程等に準拠するようにするため

上記３項に「内部又は外部に報告する情報の信頼性を保つように機能するため」という整備目的が記述されている。金融庁の「実施基準」が求める「財務報告の信頼性」を保証するためには、組織体の情報システムが原則として「システム管理基準」を監査上の判断尺度として用い、企画・開発・運用・保守していくことが求められていると考えられる。しかし、「財務報告の信頼性」に絞り込んで、システム管理基準（278項目）を、どのように、どこまで点検すれば、効果的に信頼性が保証されるかについての議論は、なされなかった。

ＩＴ統制監査とシステム監査との相違については、３章で改めて取り上げることにする。

⑵　金融庁「実施基準」（2006年11月21日公開草案）以後

①　社会現象：日本版はＵＳ－ＳＯＸの反省に立つ軽装備仕様

内部統制の構築は、金融商品取引法における「財務報告の信頼性確保」に法的拘束力があり、これを前面に押し出して初年度の構築対象とすべきであった。

しかし会社法対応上の「内部統制の４つの目的」も、推進すべき課題であり、現場では、「業務の有効性・効率性」も目的に加え、全方位で業務プロセスの文書化が進められ、これを機会にプロセスの見直しで業務改善につながり、ＢＰＲ（Business Process Reengineering）にも役立つと考える経営者も少なからず存在した。

②　監査法人のコンサルティングサービス：財務報告の信頼性に特化することを推奨

金融庁「実施基準」公表時点では、「４つ

の目的」に基づく大半の業務プロセス文書化は完了し、後戻りするには時間がなかった。この段階では、金融庁「実施基準」を受けた監査法人による「評価」の対象は「財務報告の信頼性」に関わる「財務リスク」に絞られてきた。

③　企業の対応：金融庁「実施基準」に絞った対応に割り切り

金融庁の「実施基準」に対応した内部統制は、「財務報告の信頼性確保」にポイントがあると判断した企業は、従来の全方位アプローチから「財務報告の信頼性確保」のみへと大きく舵を切るに至る。

具体的には既に文書化されたフローチャートを「財務報告の信頼性確保」と「業務の有効性・効率性確保」の２区分で仕分けする作業に入り、業務の有効性に関わるリスクは業務リスク（ビジネスリスク）であり、今回の金融商品取引法上の整備状況評価や運用状況評価の対象にはならないことを、改めて現場に徹底した。

(3)　金融庁「内部統制報告制度に関する11の誤解」(2008年３月11日)

①　社会現象：過度な対応からの軌道修正

金融庁は、2008年３月、「内部統制報告制度に関する11の誤解（以下11の誤解)」を提示した。企業のコスト負担をミニマイズし、内部統制の構築ができるよう指導してきたが、実務現場では、一部に過度な対応が見られたので、この状況を踏まえ、「11の誤解」を例示し、改めて制度の意図を説明した。

注目すべき点は、トップダウン型のリスクアプローチこそが日本版ＳＯＸ法の重要な改善であることが冒頭にふれられていたことである。

金融庁が示した、実際にあるべき姿の主要点を再度振り返ってみたい。

１．米国ＳＯＸ法と同じか。
　日本版は、トップダウン型のリスク・アプローチ。不備と重要な欠陥の２区分。

２．特別な文書化が必要か。
　企業の作成・使用している記録等を適宜、利用して良い。
　文書化３点セット（フローチャート、業務記述書、ＲＣＭ）は必須ではない。

３．すべての業務に内部統制が必要か。
　売上、売掛金、棚卸資産の３科目について売上等の３分の２の重要拠点対象。
　売上５％以下の重要性の低い業務は除外可。

４．中小企業でも大がかりな対応が必要か。
　上場企業のみ対象。社内部門の相互モニタリング、社外専門家の利用も可。

５．問題があると罰則等の対象になるのか。
　重要な欠陥があっても、直ちに上場廃止や、罰則の対象にはならない。
　直接の罰則対象は虚偽記載のみ。

６．監査人等の指摘には必ず従うべきか。
　自社のリスクを最も把握している経営者が、主体的に判断。

７．監査コストは倍増するのか。
　財務諸表監査と一体的に作成でき、監査証拠も相互利用可なので効率的。

８．非上場の取引先も内部統制の整備が必要か。
　上場企業と取引があることだけで、内部統制の整備は求められない。

９．プロジェクトチーム等がないと問題か。
　既設の部署の活用で可。専門のチーム、担当者の設置も不要。

10．適用日までに準備を完了する必要があるのか。
　内部統制はプロセスであり、問題点があればその都度、是正することが重要。

11．期末のシステム変更等は延期が必要か。
　予定を変更せず、そのまま実施しても、内部統制は有効。評価範囲から除外可。

「やむを得ない事情」→「無限定適正

意見」表明可能。

② 監査法人のコンサルティングサービス：整備状況評価、運用状況評価手法の視点

監査法人の対応においても、上記の金融庁の「11の誤解」公表もあり、内部統制の構築最終局面では、かなり思い切った絞り込みが行われた。文書化３点セットに関しても、とりわけＲＣＭの活用に集中するケースが目立ち、業務のリスクから、財務リスクだけを残し、極端な場合は、１つ又は２つのキーコントロールに絞り込んで、残るリスクとコントロールはフローチャート上から消去することまで踏み込むケースも少なからず生じた。

また、ＩＴ全般統制については監査法人内での別動の専門部隊意見と業務担当チームの意見が必ずしも一致しない状況も散見された。

③ 企業の対応：業務部門と情報システム部門とのプロセス結合作業

「４つの目的」か「財務報告の信頼性確保」優先かといった対立概念ではなく、素直に全方位で業務プロセスの文書化を進めてきた、業務チームのリーダーは、この段階で非常に困惑したのが実状と思われる。

監査法人コンサルティングチームの指導で文書化を進めてきたリーダー達は、金融庁「実施基準」対応で「財務報告の信頼性」に関わるリスクのみに絞るよう要望され、「11の誤解」公表で、内部統制推進の真の意図を確認した次第である。

ともあれ、別々のチームで進めてきた業務プロセス全体を結合し、業務プロセス統制、ＩＴシステム統制に分散したリスクを限定していかねばならない。この作業は、企業によっては「プロセス結合」と称した。

ＩＴ全般統制は情報システム部門主体での対応であったが、業務プロセスにおけるＩＴ業務処理統制から導かれるＩＴ全般統制評価は考慮せずに計画しており、再整備を必要とした。

順序は全く逆なのだが、業務、ＩＴの両チームが、別々に構築してきたプロセスを、ここで始めて突き合わせ、お互いにキーコントロールを再確認することになった。その中で、キーコントロールとされたものが運用テストの対象となり、それを支えるシステムであれば、自動的にＩＴ全般統制の対象システムに浮上することになった。

こうした取組みで、土壇場になって突如古い現行システムがＩＴ全般統制の対象となり、そこに不備が存在するといった事態が発生したが、この対応には困難を伴った。

現行システムを開発した時代は、財務報告に関わる内部統制の不備指摘事項を意識するシステム要件が設計に組み込まれておらず、情報システム部門は、ＩＴ業務処理統制そのものを業務チームが記述したフロー上から削除するよう変更、見直しを求めた。

その結果ＩＴシステムによるキーコントロールが実際に機能していても、業務フロー上からは除去し、改めて手作業統制としてキーコントロールを記述変更するケースも生じていた。

以上、国内におけるＩＴ全般統制に係る取組みをレビューしてきたが、その変遷をいくつかのキーワードとしてまとめると次のとおりである。

1．ＩＴ現場部門の過去の不備事例をベースとしたボトムアップアプローチからトップダウンアプローチへの流れ。
2．ＵＳ－ＳＯＸ法を最大公約数として、COBIT for SOX準拠の全方位ＲＣＭ活用から財務諸表に関する虚偽記載リスク対応への絞込みへの流れ。
3．会社法対応としての「内部統制４つの目的」から金融商品取引法対応としての「財務報告の信頼性確保」への流れ。すなわち、「業務リスク対応」から「財務リスク対応」への流れ。

第３章　各社実態調査で浮上したＩＴ全般統制に関する課題

各社におけるＩＴ統制への取組事例をまとめる中で浮上した課題は次のとおりである。このうち、私達が第４章及び第５章で提言しようと考えている課題は次のうち、１．２．６．である。３．～５．に関する考え方は、この章で提言しており、また「ＩＴ統制監査とシステム監査の相違」に関しては次項７．にてとりまとめている。

１．ＩＴ統制の評価体制と要員確保
２．内部統制における主要目的（会社法と金融商品取引法との相違）
３．システムのロジック評価
４．ログの活用について
５．スプレッドシートの取扱いについて
６．監査体制と評価方法
７．ＩＴ統制監査とシステム監査との相違について

１．ＩＴ統制の評価体制と要員確保

ＩＴ統制の評価体制構築は、未だ着手したばかりであり、体制面では外部監査への依存や情報システム部門から内部監査部門への転属、また、方法面では、情報システム部門で自己点検の上、内部監査部門でその手続を監査するといった方法など、様々な対応が図られている。

２．内部統制における主要目的（会社法と金融商品取引法との相違）

金融商品取引法に基づく「財務信頼性確保」に目的を絞った取組みと、会社法における「４つの目的」まで対象を拡大した取組みとが、スタート段階で混在したケースがほとんどであった。リスクは、環境と目的によって決まり（異なり）、一言でリスクアプローチといっても、スコーピングも評価も異なってくる。この点での理解は、今回の内部統制への取組みを正確に進めていく上では、重要なポイントであったように思う。

３．システムのロジック評価

ＩＴ統制の対象とした、システム自体の正当性、完全性及び正確性についてはそもそもどのように検証すれば良いのであろうか。監査法人によってはプログラムのソースコードまで要求したという話もあるが、開発会社自体がソフトウェアの信頼性を確保するのに苦慮している中で、第三者がプログラムを見て評価できるとも思えない。私達の研究会の中では、重要プロセスに係るシステムの機能のみロジック評価を実施したという例があったが、

①　システムの仕様上で確認する。
②　システムの仕様書が責任者によって承認されていることを確認する。
③　入力原票と出力帳票の整合性をチェックする。
④　レポート間の整合性をチェックする。

という方法による評価方法も採用できると考えた。

ちなみに、開発から相当年数が経過したシステムについては、仕様書やマニュアルがあればロジックは信頼できると考えて良いし、また、ドキュメントが不整備であっても、「再実施」結果で合理性が証明できれば（補完的整備）、信頼できるとして良いと考える。なお、パッケージソフトをカスタマイズせずそのまま利用している企業については、“市販されているパッケージの導入”をもってシステムは信頼できると考えることも可能と判断している。

４．ログの活用について

ＩＴ全般統制又はＩＴ業務処理統制のコントロール、評価項目としてログを活用したのは当研究会メンバー10社中４社であり、ログを活用した事例は少なかった。“ログ”と一

概にいっても、ＯＳのログもあれば、データベース、アプリケーションのログがあり、また、ＯＳのログだけ見てもWindowsの場合とLinuxの場合ではログが異なるし、セキュリティログとアラートログのように、１つのＯＳの中に複数種類のログがあるなど、ログの種類は多く、項目や形式、内容について統一されていない。加えて、それらのログについて、利用者のＩＤが統一されていないことも多い。

ＥＲＰなど統一されたＩＴ基盤上のログであれば管理は容易であるし、発見的コントロールとして有効であるかもしれないが、異なるＩＴ基盤上におけるログに関しては、収集や分析が困難であり、ログ管理システムなどの投資が必要となる場合が多い。金融商品取引法上でのＩＴ統制項目という観点でログを考えたとき、ログ以外の方法による補完的コントロールが考えられるのであれば、当面は、これらの対応で目的は達成しうるものと考えている。

なお、当課題は、今後の重要な検討課題ではある。

５．スプレッドシートの取扱いについて

スプレッドシートの取扱いに関しては、当研究会メンバーで１社だけ、決算財務報告プロセスでの引当金等の見積りに関するシートをＩＴ統制の対象として選択した企業があったが、残りの９社については、いずれもマニュアルコントロール、すなわち「電卓」と同じ扱いとして、ＩＴ統制の対象に含めていない。スプレッドシートは元々ＥＵＣ（エンドユーザ・コンピューティング）が可能な計算手段として広く浸透したアプリケーションであり、ＩＤ管理やアクセス制御などの内部統制機能を基盤として持っていないため、自動化された統制ではあるがＩＴ統制の対象システムとして見るには、スプレッドシート自体に対する内部統制を有効に整備及び運用することが難しいということであろう。

ただし、ＩＴ統制の対象としないまでも、決算処理などではスプレッドシートを利用している場合が多いため、今後、監査法人より、スプレッドシートの取扱いが厳格化された場合の対応については検討しておく必要がある(今年度は文書による指示はなかったが、アクセス権の制限について今後検討する旨、監査法人から口頭で説明された企業もあったようである)。システムとして自動化された内部統制を保証することは難しいが、「電卓」としてその機能が有効であることを確認するコントロール（ＩＴ業務処理統制）は必要と考える。

６．監査体制と評価方法

上述の１．と関連する課題ではあるが、いくつかの課題を列挙しておく。

① ＩＴ統制評価は、専門家である情報システム部門経験者が実施しないと実質的意味を成さない。会社によっては、リソース面から対応に問題がある。

② 監査の独立性・客観性の観点から、情報システム部門経験者を監査部門に配置することが不可欠なのかどうかという点等について、どのように整合性を保持するのかが課題である。

③ 情報システム部門、経理財務部門、内部監査部門の監査に関する関係性を整理することが必要である。

７．ＩＴ統制監査とシステム監査との相違について

各社での取組みをレビューする中で、「財務の信頼性確保」を担保する「ＩＴ統制監査」の検討がいつの間にか「システム監査」の内容に切り替わってしまい、焦点の定まらない取組みとなったことが、節々で報告されている。この点は、区分して考えることが大切で

ある。私達は、理解しやすいように「ＩＴガバナンス…システム監査」、「Ｊ－ＳＯＸ…ＩＴ統制監査」と区分して考えた。

「ＩＴ統制監査」と「システム監査」との相違について、「金融商品取引法（実施基準）」対「システム監査基準・管理基準」、「システム管理基準 追補版」をベースに以下の主要ポイント［項目］について記載する。

金融商品取引法（実施基準）にそったＩＴ統制監査を「A」、システム監査基準・管理基準、システム管理基準 追補版における対応項目を「B」と略記する。なお、研究会としての提言も含まれている。

①　定義

A：経営者による財務報告に係る内部統制の有効性評価結果に対して公認会計士等が実施する監査のうち、ＩＴ統制に係る部分。

B：組織体の情報システムに関連したリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行い、もってＩＴガバナンスの実現に寄与することにある。（出典：経済産業省「システム監査基準」の「Ⅱ．システム監査の目的」より）

［注１］「システム管理基準 追補版」ＩＴ統制の概念

①ＩＴ環境への対応	社内外のＩＴの活用状況の考慮
②ＩＴの利用	財務情報の信頼性に係る内部統制の実現におけるＩＴの利用（例：アクセス制御機能による財務情報へのアクセス制限）
③ＩＴ（の）統制	ＩＴを利用した情報システムに対する内部統制（例：アクセス制御機能による財務情報へのアクセス制限を有効に機能させるためのＩＤ、パスワードの管理）

②　実施主体者

A：公認会計士、又は監査法人。

B：システム監査人［監査対象から独立かつ客観的立場であること］。

（出典：経済産業省「システム監査基準」の「Ⅲ．一般基準－３．専門能力」より）

［注２］システム監査人は、適切な教育と実務経験を通じて、専門職としての知識及び技能を保持しなければならない。

システム監査人と認定される者：情報処理技術者試験／システム監査技術者、ＮＰＯ日本システム監査人協会認定／公認システム監査人、ＮＰＯ日本セキュリティ監査協会認定／公認情報セキュリティ監査人、㈶日本規格処理開発協会／ＩＳＭＳ審査人（EDP Auditors Association 現・ＩＳＡＣＡ）／公認情報システム監査人（ＣＩＳＡ）・公認情報セキュリティマネージャー（ＣＩＳＭ）等。

［注３］公認会計士監査や監査役監査においては、監査対象が情報システムそのものでなく、本来の監査対象がそれぞれ別に存在する。しかし、それらが情報システムの影響を受けているので、公認会計士や監査役が自ら情報システムの統制状況を評価するために、システム監査を行うものがある。

公認会計士監査によるシステム監査は、一般には会計システムを中心とした情報システムの信頼性の評価に重点が置かれている。監査役監査におけるシステム監査は、経営計画と情報戦略であるシステム化計画との適合性、情報システム部門管理の適法性等に重点が置かれる。

③　位置付け

A：ＩＴ統制監査人は、会計監査人を支援（補助）する立場で、内部統制報告制度に寄与する。

B：システム監査人は、直接依頼者（経営者、情報システム部門、システムに関する委託元等）に監査結果報告書を提出する。

④　監査対象

A：財務会計の信頼性に焦点を置く。第一義

的には経営者の作成した内部統制報告書。
監査対象システム：財務報告に係る内部統制に関連するシステムを対象範囲。
監査対象プロセス：ＩＴの企画・開発・運用・保守すべて。

Ｂ：内部統制の目的のそれぞれにおいて、被監査対象の実態（プロセス）をその評価対象とする。
（出典：経済産業省「システム監査基準」の「Ⅰ．前文」よりの一般的解釈）

［注４］システム監査が対象とする情報システムは、コンピュータシステムそのものに限らず、これを利用するユーザ部門まで含めた、コンピュータを中核とする広義の情報システムの傘下にある部門まで対象とする。対象とする業務はシステム化企画業務、システム開発業務から運用業務・保守業務にまでわたる全業務である。
監査対象システム：依頼者が選定したシステムを対象範囲。
監査対象プロセス：ＩＴの企画・開発・運用・保守のうち対象とするプロセス。

⑤　法定化

Ａ：実質的に法定化された。

Ｂ：経営者の意思に基づく任意の監査としてその多くが実施されてきた。

［注５］信頼性、安全性が強く求められる公共性の高い情報システムについては、内部監査が十分実施されるとともに、独立した第三者による監査を必要とすることは考えられる。

国際業務を行う銀行の場合、３年に１回は外部監査として客観的に実施することが取り決められている（銀行監督国際機関であるバーゼル委員会が決定）。

［注６］三様監査・システム監査の位置付け

①	法定監査	外部監査	公認会計士監査、監査法人監査
			Ｊ－ＳＯＸ対応、内部統制監査の一部としてのＩＴ統制監査
②	法定監査	内部監査	監査役監査
③	任意監査	内部監査	経営監査、業務監査、会計監査
			システム監査（含むセキュリテイ監査）
			コンプライアンス監査
			環境監査、品質監査、業法監査、安全監査　等

⑥　保証

Ａ：会計監査人に積極的保証意見を求めており、ＩＴ統制監査もその積極的意見を支えるもの。

しかし、いたずらに「範囲」や「深さ」を拡大して、責任範囲を拡げることに意図があるのではなくて、監査対象が「経営者の作成した内部統制報告書」であること、またテスト手法も「ＩＴ的に監査を実施することではない」ことには十分配慮することが大切である。

Ｂ：問題点の検出や消極的保証意見にとどまる。

［注７］（出典：経済産業省「システム監査基準」の「Ⅴ．報告基準」より）。

１．監査報告書の提出と開示：システム監査人は、実施した監査の目的に応じた適切な形式の監査報告書を作成し、遅滞なく監査の依頼者に提出しなければならない。

２．監査報告の根拠：システム監査人が作成した監査報告書は、監査証拠に裏付けられた合理的な根拠に基づくものでなければならない。

３．監査報告書の記載事項：監査報告書には、実施した監査の対象、実施した監査の概要、保証意見又は助言意見、制約又は除外事項、指摘事項、改善勧告、その他特記すべき事項について、証拠との関係を示し、システム監査人が監査の目的に応じて必要と判断した事項を明瞭に記

載しなければならない。

⑦　時期

A：監査対象期間全体にわたる有効性の検証のためには、テスティングのサンプル抽出は期間全体を母集団とする必要がある。

B：任意の期間又は任意の時点を対象として監査可能。

⑧　件数

A：サンプル件数は、監査理論上の所定の件数に基づく。

B：助言型監査の場合にはサンプル件数によらない。保証型監査の場合は理論上の所定の件数とすることができる。

⑨　テスト手続

A：（再実施、再計算）「自動化された統制活動」のテストを、すべて「ＩＴ的」にテストデータを流すなどの方法で実施する必要はなく、画面や出力帳票等を閲覧して、統制が実装されていることを確認できれば十分である。統制活動がＩＴ的に行われていることと、そのテストをＩＴ的に行うこととは、全く別次元のことである。

B：システムの開発、運用・保守の信頼性、品質管理として使用されるテストデータ法、プログラムレビュー等種々の手法がある。また脆弱性監査・ペネトレーションテストにおいては、当監査・テスト固有の手法、ツールが採用される。

⑩　サンプルテスト

A：（ジャッジメントサンプル）　サンプルテストも、アドバイスとして「統計的サンプル」の考え方が紹介されることがあるが、これまで監査法人でさえ行ってきていないことを、急に企業が実施できる環境にはなく、現実としてはジャッジメントサンプルで十分である。

B：統計的サンプル、非統計的サンプル（判断的サンプル、評価者の経験等に基づくサンプリング）に大別され、統計的サンプルは準拠性をテストする属性サンプリング、実証性をテストする変数サンプリングがある。

目的に応じたテスト法の採用とあわせて適切なサンプリングが採用される。

［注８］準拠性テスト：コントロールが管理方針、手続に準拠する方法で適用されているかを判定する。

実証性テスト：実際の処理のインテグリティ、結果とし合っているかを実証する。

［注９］（出典：ＮＰＯ日本システム監査人協会編「Ｊ－ＳＯＸ対応　ＩＴ統制監査実践マニュアル」）

準拠性調査、実証性調査の他に試査を区分している。

試査：監査テーマごとに監査対象の一部に対してのみ監査手続を適用し、その結果に基づいて監査対象全体の状況を推定する監査方法、サンプリング監査。

［注10］（出典：経済産業省「システム管理基準 追補版」の「付録５　サンプリング」より）

○サンプリングの種類

①　統計的サンプリング

②　非統計的サンプリング（評価者の経験等に基づくサンプリング等）がある。

母集団全体の状況を推定する際には、一般に統計的サンプリングによる評価が向いている。したがって、運用状況の評価においても統計的サンプリングを利用することが多くなるものと思われる。しかし、四半期の処理、月次処理、週次処理等では、母集団が小さいため、統計的サンプリングによらなくても良い。

○サンプル件数

①　手作業による場合

サンプル件数がどの程度が適切であるかを一概にいうことはできないが、全社的な内部統制が適切である場合には、業務プロセスに係る内部統制の運用状況の評価を行うためのサンプル件数及びその

ときの許容逸脱件数として、例えば、付録図表５－１の表をあらかじめ定めておいて判定することが考えられる。実施の頻度は、内部統制の評価を行う対象の数であり、例えば、「取引件数」等が挙げられる。

ＩＴ全般統制は、財務報告の虚偽記載に直接影響を及ぼすものではないが、ＩＴ業務処理統制が有効に機能していることを保証するので、ＩＴ業務処理統制ごとにアプリケーション・システムを検証することを軽減できる。この場合のサンプル件数は、例えば、付録図表５－１を参考にして選ぶことができる。

②　自動化された内部統制の場合

ＩＴ統制は、一度内部統制が設定されると、変更やエラーが発生しない限り一貫して機能するという性質がある。したがって、付録図表５－２のような方針に基づき運用テストを実施することができる。

⑪　運用管理におけるログの記録、保存

Ａ：“ログ”と一概にいっても、ログの種類は多く、項目や形式、内容について統一されていない。それらのログについて、利用者のＩＤが統一されていないことも多い。異なるＩＴ基盤上におけるログに関しては、収集や分析が困難であり、ログ管理システムなどの投資が必要となる場合が多い。

金融商品取引法上でのＩＴ統制項目という観点でログを考えたとき、ログ以外の方法による補完的コントロールが考えられるのであれば、当面は、これらの対応で目的は達成しうるものと考えている。

Ｂ：（整備状況の評価）：企業にログ採取に関する方針があることを確かめる。

（運用状況の評価）：必要なログ（不正操作等のモニタリングに必要な項目）が記録され、保管されていること、また保管されたログを利用できることを確かめる。

⑫　監査体制

Ａ：財務報告に係わる内部統制の有効性について、①これに関する経営者の評価（内部統制評価）と、②第三者である監査人（公認会計士又は監査法人）による監査（内部統制監査）を義務づけている。更に、以上の前提として、財務報告に係わる内部統制の整備・運用が必要である。

監査室監査を軸とするが、内部統制プロジェクトを含めて、「監査の一元化」を図ることが大切である。状況によっては、監査室、経理部門、情報システム部門の合同チームといった構成により、実質的な効果を狙う方法も考えられる。

Ｂ：システム監査基準において、以下記述されている。

（出典：経済産業省「システム監査基準」の「３．監査の実施」より）

○監査業務の体制：システム監査人は、システム監査の目的が有効かつ効率的に達成されるように、適切な監査体制を整え、監査計画の立案から監査報告書の提出及び改善指導（フォローアップ）までの監査業務の全体を管理しなければならない。

○他の専門職の利用：システム監査人は、システム監査の目的達成上、必要かつ適切と判断される場合には、他の専門職による支援を考慮しなければならない。

他の専門職による支援を仰ぐ場合であっても、利用の範囲、方法、及び結果の判断等は、システム監査人の責任において行われなければならない。

⑬　モニタリングの実施証跡の確認

Ａ：内部統制全体を俯瞰する位置からは、以下のように区分されるが、日常的モニタリングの確認は、毎月で十分としたい。

	日常的モニタリング	独立的モニタリング
実施方法	通常の業務に組み込んで実施 自己点検、自己評価	業務から独立した視点で実施

	も含む	
実施者	経営層、管理層、現業各層	内部監査部門、監査役による監視等第三者
実施時期	恒常的、定期的（週、月、年）に実施	定期的、随時に実施

B：一定期間を区切り、本番登録のログから対象となったプログラム及び登録目的を確認して、その登録行為が関係部門の承認を得ているかどうかを確認する。

「システム管理基準 追補版」において、以下のとおりに記述されている。

（出典：経済産業省「システム管理基準 追補版」の「Ⅳ章－５．モニタリング」より抜粋）

○日常的モニタリング

① 経常的なモニタリング：経常的に実施され、一定の目標値と実績との差をチェックする。

② 定期的なモニタリング：定期的（週次、月次、年次等）にマスターファイル等の棚卸（マスターファイルの内容について誤りがないか点検）する、アクセスログ等をチェック（アクセス権の違反や許可されていないアクセスが起きていないかを確認）する。

③ 異常値モニタリング：異常値や、非定形的な事象の有無をチェックする。

○独立的モニタリング（内部監査部門等による監視体制）

① ＩＴ全社統制のモニタリング

② ＩＴ全般統制のモニタリング

③ ＩＴ業務処理統制のモニタリング

独立的モニタリングは、内部監査部門、監査役による監視等第三者による監視活動である。

独立的モニタリングとしてＩＴ統制に関する内部監査の実施は、情報システム部門以外の部門によって実施される。独立的モニタリングの１つである内部監査においてＩＴを利用するのは、ＣＡＡＴ（Computer-Assisted Audit Techniques）と呼ばれるコンピュータ支援監査技法の利用も考えられる。

独立的なモニタリングは日常的なモニタリングと独立して実施される場合と補完的に実施される場合とがある。一般的に、日常的モニタリングが適切に実施されている場合には、独立的モニタリングの実施頻度を減らすことができる。

［注11］（出典：ＮＰＯ日本システム監査人協会編「Ｊ－ＳＯＸ対応 ＩＴ統制監査実践マニュアル」）

モニタリングを日常的モニタリングと独立的モニタリングとに区分し、前者を更に①恒常的なモニタリング、②定期的なモニタリング、③異常値モニタリングに区分している。

［注12］（出典：経済産業省「システム管理基準 追補版」の「Ⅳ章－５．モニタリング」より）

付録図表５－１　サンプル件数の例

実施の頻度	サンプル件数	許容逸脱件数
１日につき多数	25	0
日次	25	0
週次	5	0
月次	2	0
四半期次	2	0
年次	1	1

付録図表５－２　自動化された内部統制の運用テスト

条件	運用テスト
・関連する全般統制の整備及び運用状況を確認及び評価した結果、全般統制が有効に機能していると判断できる場合	ＩＴに係る業務処理統制ごとに１つのアプリケーションを検証する。
上記に加え、以下の３つの条件に適合する場合	４つの条件に適合していることを記録し、前年度に実施した内部統

・前年度に内部統制の不備が発見されていない ・評価された時点から内部統制が変更されていない ・障害・エラー等の不具合が発生していない	制の評価結果を継続して利用する。

第４章　ＩＴ全般統制のスコーピングに関する提言

既述のとおり、第２章末尾において、キーワードを「まとめ」として、以下のように整理している。

１．ＩＴ現場部門の過去の不備事例をベースとしたボトムアップアプローチからトップダウンアプローチへの流れ。
２．ＵＳ－ＳＯＸ法を最大公約数として、COBIT for SOX準拠の全方位ＲＣＭ活用から財務諸表に関する虚偽記載リスク対応への絞込みへの流れ。
３．会社法対応としての「内部統制４つの目的」から金融商品取引法対応としての「財務報告の信頼性確保」への流れ。すなわち、「業務リスク対応」から「財務リスク対応」への流れ。

また、第３章で提起した課題、とりわけ「２．内部統制における主要目的（会社法と金融商品取引法との相違）」による取組みの相違を踏まえた、スコーピングにおける、１つのアプローチ上の仮説は、①リスク及びキーコントロールの絞込み（第４章）、②評価から見た逆からのアプローチ（第５章）である。

１．ＩＴ全般統制は既に存在している

ＩＴガバナンス協会「企業改革法遵守のためのＩＴ統制目標～財務報告に係る内部統制の設計と導入におけるＩＴの役割について（第二版）～」（2006年９月）では、ＩＴ全般統制を以下のように定義している。

「ＩＴ全般統制：信頼できる運用環境を提供し、アプリケーション統制の有効な運用をサポートする、ＩＴプロセスに組み込まれた統制。ＩＴ全般統制には、以下が含まれる。

・プログラム開発
・プログラム変更
・プログラムとデータへのアクセス
・コンピュータ・オペレーション

そしてＩＴ統制特有の課題として、ＩＴの専門家の多くが、内部統制の複雑さに十分に精通していないことを挙げ、これはＩＴがリスクを管理していないことを意味するのではなく、企業の経営者や監査人が求めている方法ではリスクが形式化、あるいは構造化されていないことを意味していると解説している。

その解決策として企業は、企業改革法のチームにＩＴ専門家を参加させる必要があり、

・組織の内部統制のプログラムと財務諸表作成プロセスの理解。
・内部統制及び財務諸表作成プロセスをサポートするＩＴ環境（ＩＴサービスとプロセス）と財務諸表との関連付け。
・これらのＩＴシステムに関するリスクの把握」（以下省略）

などについて重要な責任分野とすることを勧めている。

このレポートで重要なのは、これに続く以下の提言にある。次年度以降ＩＴ統制を整備される企業にあっても、大変示唆に富んでいるので引用する。

企業改革法に影響を与えるＳＥＣの規則が複雑であることは間違いなく、導入には時間とともに多くの費用がかかっている。ＩＴ統制の評価作業を進めるにあたり、考慮に入れなければならない二つの重要な事項がある。
①　わざわざ一からやり直す必要はない。

実質的には、ほとんどの公開企業には何らかのＩＴ統制がある。統制が非公式で、文書化が十分でなく、統制機能に関する十分な証拠に欠けていているかもしれないが、一般的に、情報セキュリティと変更の管理の分野においてＩＴ統制は存在している。

② 多くの企業は、既存のＩＴ統制プロセスを企業改革法の条項を遵守するように作り上げることが可能である。多くの場合、企業に欠けているものは統制の文書化の一貫性と品質ならびに証拠である。しかし一般的なプロセスはしばしば機能しており、多少の修正を必要としているに過ぎない。

この点は金融商品取引法対応においても、変わりはない。ＩＴ統制は特別なものではなく、従来から存在し機能してきた統制であることを再確認し、その表現の仕方については、ＩＴ専門家を参加させ、財務報告プロセスとＩＴの関係付けや、内部統制への理解を基に簡潔で適切なＩＴ統制評価を行えば目的は達成されると理解できる。

2．ＧＡＩＴアプローチについて

図表１はＧＡＩＴメソドロジーを適用する場合のトップダウン型のリスクアプローチ流れ図である。

ここで試みとして、金融庁「実施基準」をベースに、ＧＡＩＴメソドロジーを適用したトップダウン型のリスクアプローチでは、どのように各フェーズでの検証を行い、またＩＴ全般統制のキーコントロールを絞り込んでいくことになるのかを検討してみる。

ＧＡＩＴを含むトップダウン・プロセスをみると、最初にＰＣＡＯＢ（米国公開会社会計監視委員会）のＡＳ（監査基準書）／５を用いるようになっている。

（「ＧＡＩＴ Methodologyの概要」『月刊監査研究』2009年１月号、53頁図表１参照）

１．全社的統制の有効性を識別し、理解し、評価する。
２．重要な勘定科目、拠点及び適切なアサーションを識別する。
３．重要な業務プロセス及び主要なクラスの取引を識別する。
４．プロセスにおいて誤謬又は不正が起こり得るポイントを識別する。
５．検証すべき統制として、誤謬又は不正を適時に予防又は発見する統制を識別する。

日本における内部統制システムは、以下の３項目について、整備状況評価、運用状況評価が行われてきた。

１．全社的統制
２．決算・財務報告プロセス
３．「売上」、「売掛金」、「棚卸資産」に関わる売上高３分の２拠点の業務プロセス統制

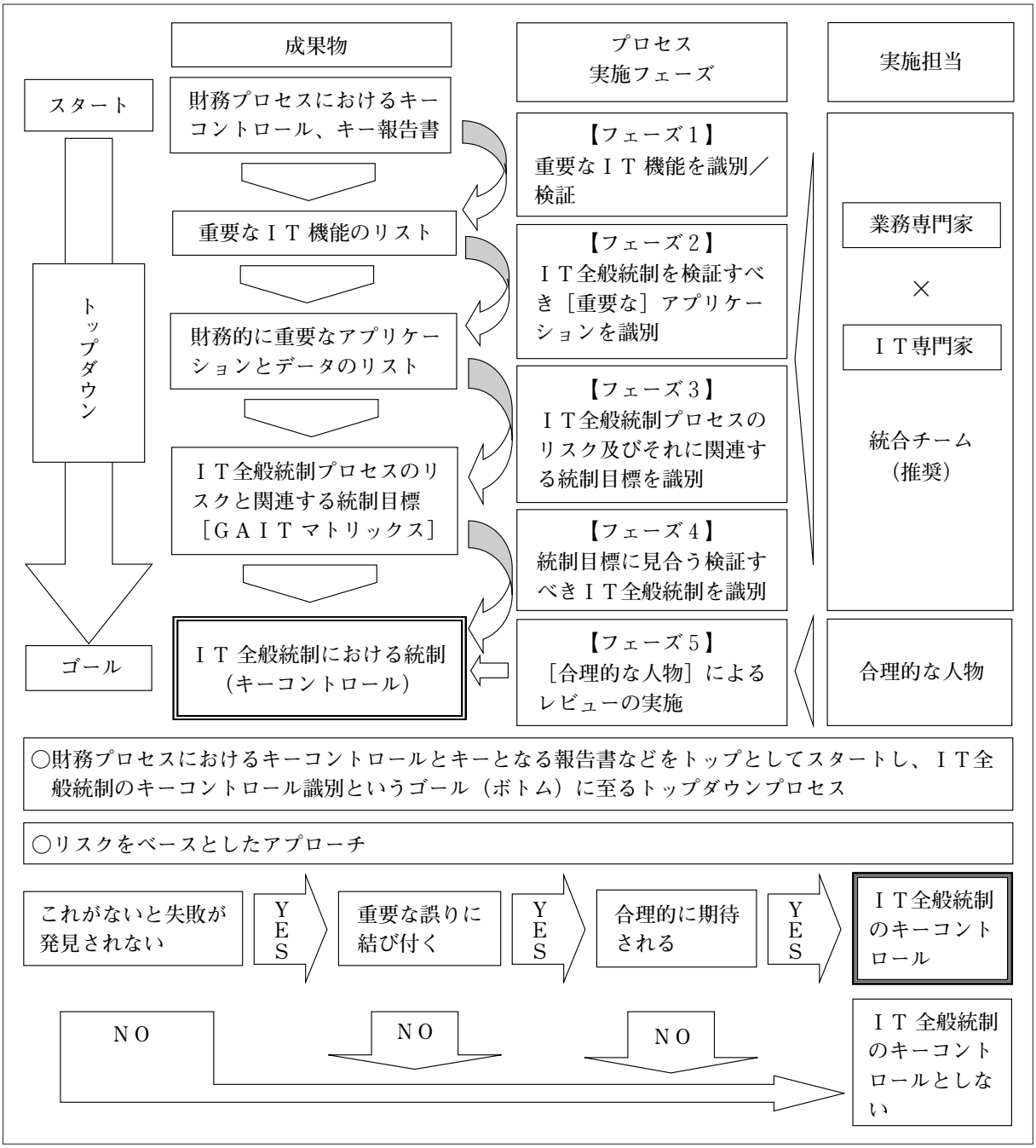
１項の全社統制の有効性識別、評価は、ＧＡＩＴプロセスの前段階にあり、ＧＡＩＴの適用は、決算・財務報告プロセス以降となる。

3．研究会参加企業が採用したスコーピング方法とＧＡＩＴメソドロジーの比較

今回研究会に参画した企業の１社が、A監査法人（以降A法人）のアプローチ方法を採用しており、この方法とＧＡＩＴメソドロジーとのアプローチの差異を確認するため、それぞれの考え方を図表３のように整理してみた。

この比較表から判断できることは、いずれもリスクベースのトップダウンアプローチを採用しており、アプローチ順序においても、ＧＡＩＴでは、ＡＳ／５を前提として「重要な科目」、「重要な業務プロセス」、「プロセス上のリスク」識別が存在し、一方A法人では、

＜図表１＞ＧＡＩＴメソドロジー　トップダウン型のリスクアプローチ



「重要勘定」、「業務プロセス」、「リスク手続識別後の自動化された統制活動」とのアプローチ順序となっている。ただ、A法人では、この後すぐに「それを提供するアプリケーション」となっているため、ややスコーピングとしては広めになる感じは残る。

この部分について、ＧＡＩＴメソドロジーの「４つの原則」では、「業務プロセスにおける重要な科目」、「関連するリスク及びキー項目」を、また、「５つのフェーズ」では、「重要なＩＴ機能の識別」、「重要なアプリケーションの識別」を経て、「ＩＴ全般統制プロセスのリスク及び関連する統制目標を識別」、更にその上で、「キーとなるＩＴ全般統制を識別」となっており、「かなりの絞込みの実現」が図られることになると考える。

研究会参画企業は、自企業にてA法人アプローチ方法を採用した結果と、ＧＡＩＴメソ

＜図表２＞ＧＡＩＴメソドロジー　トップダウン型のリスクアプローチ（金融庁「実施基準」にそって）

【フェーズ１】
重要なＩＴ機能を識別／検証する。

１．決算・財務報告プロセス
２．「売上」、「売掛金」、「棚卸資産」に関わる売上高３分の２拠点の業務プロセス統制
　上記に関わるＩＴシステムを識別／検証する。
（例　経理、販売管理、在庫管理システムなど）

【フェーズ２】
ＩＴ全般統制を検証すべき【重要な】アプリケーションを識別する。

１．決算・財務報告プロセスに使用されるシステムのアプリケーションを識別
２．売上計上、在庫管理のアプリケーションを識別

【フェーズ３】
ＩＴ全般統制プロセスのリスク及びそれに関連する統制目標を識別する。

１．決算・財務報告プロセスをレビューし、データ生成、権限、承認、最終突合といった各ステップでリスク及びそれに関連する統制目標を識別する。
２．売上計上、在庫管理プロセスをレビューし、データ入力、権限、承認、最終確認といった各ステップでリスク及びそれに関連する統制目標を識別する。
３．識別された統制目標は４つのＩＴレイヤー（アプリケーション・プログラムのコード、データベース、オペレーティングシステム、ネットワーク）のリスクにより、その重要度を識別する。

【フェーズ４】
統制目標に見合う検証すべき、ＩＴ全般統制を識別する。

１．統制目標である「財務報告の信頼性」に対して、識別されたリスクは、発生可能性、影響度の面で、重要なリスクであり、虚偽記載に結び付くか？
２．個別システムに虚偽記載リスクがあっても、「財務報告の信頼性」を保証する仕組みが全体として構築されていれば、統制目標は達成される。
３．上記を踏まえ、テストすべきＩＴ全般統制のキーコントロールを識別する。

【フェーズ５】
合理的な人物によるレビューを実施する。

合理的な人物（専門性と独立性を具備した人物）、すなわち内部監査部長、システム統括部長、経理部長の三者から成る協議体で、ＩＴ全般統制のキーコントロールが、財務諸表に対するリスクとして合理的な見方をしていることを確認する。

ドロジーアプローチを採用した場合の結果とを比較してみたところ、フォーカスされた結果に大きな差異が発生していないことを確認している。その理由は、当該会社が、「常に絞込み」を意識した取組みに心がけたため、「重要な業務プロセス」、「重要なリスク」、「キーとなりうるリスクと統制活動」の各アプローチが、ＧＡＩＴメソドロジーの「４つの原則」、「５つのフェーズ」を前段のアプローチにて取り込む形で進められたためである。ただ、「５つのフェーズ」における「フェーズ１」及び「フェーズ２」については、優劣順位はなく「ＩＴ機能識別」、「重要なアプリケーション識別」は同時一体として理解している。

そうした観点からみると、Ａ法人のアプローチは、取組姿勢によっては、ＧＡＩＴメソドロジーよりも、広めのアプローチとなりうる部分を残している。

翻っていえば、ＧＡＩＴメソドロジーは、「財務信頼性の確保」という目的に焦点を当てた明確なアプローチといえる。また、他の内部統制上の目的（業務の有効性・効率性やコンプライアンス）に関しても、アプローチ方法の共通的な考え方として、特に、スコーピングについてリスクごとにポイントを絞り、明確かつ厳密に行うという点において、今後広く応用されていくものと思われる。

＜図表３＞ＧＡＩＴアプローチ方法に関して――Ａ法人によるスコーピング方法との相違

ＧＡＩＴメソドロジー	Ａ法人のスコーピング
ＡＳ／５ ①全社的統制の有効性の識別、理解、評価 ②重要な科目、拠点、アサーション ③重要な業務プロセス、主要クラスの取引識別 ④プロセスにおける不正が起こりうるポイントの識別 ⑤不正を適時に予防又は発見する統制の識別	全般統制のアプローチ順序 ①重要勘定 ②取引フロー（業務プロセス） ③自動化された統制活動 ④それを提供するアプリケーション ⑤基盤 ⑥全般統制プロセス
（４つの原則） 原則　１ トップダウン・リスクアプローチ 重要な科目 勘定科目に関連するリスク及び業務プロセスにおけるキーコントロール 原則　２ 財務的に重要なアプリケーションにおける重要なＩＴ機能 財務的に重要なアプリケーションに関連するデータ 原則　３ ＩＴレイヤー上のリスクの存在 アプリケーション プログラムコード データベース オペレーティングシステム及びネットワークシステム 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り軽減される。…個別の統制により軽減されない。	スコーピング　１ 全般統制プロセス「種類」への落とし込み 例：処理ロジック管理、アクセス権管理、ジョブ実行管理、バックアップ管理、等 スコーピング　２ 上記全般統制プロセス種類ごとに「システム」への落とし込み 例：プログラム管理でも「経理システム」、「ＥＲＰ」、「自製Ｃ／Ｓシステム環境」、「工場別の生産管理システム環境」、等 スコーピング　３ 上記「システム」ごとに、「ＩＴリソース」種類への落とし込み 例：「ＥＲＰ環境」の「プログラム管理」でも、「コアプログラム」、「アドオン」、「ＤＢＭＳ」、「インタフェースソフト」、等 スコーピング　４ 以上のように細分されたプロセスで、「内部統制が同じ」であるがゆえに「同じ母集団」からサンプル抽出をしても良いとみなせる「束ね」の単位の判別 例：「ＥＲＰ環境」と「自製Ｃ／Ｓ環境」ではアクセス権管理以外（プログラム管理もバックアップ管理も）はすべて共通（人も場所も手順は同じ）、等 ＊スコーピング２～４の順番には意味はない。
（５つのフェーズ） フェーズ　１　重要なＩＴ機能を識別する フェーズ　２　重要なアプリケーションを識別する フェーズ　３　ＩＴ全般統制プロセスのリスク及び関連する統制目標を識別する フェーズ　４　キーとなるＩＴ全般統制を識別する フェーズ　５　「合理的な人物」によるレビューの実施	

４．ＧＡＩＴアプローチのメリット

ＧＡＩＴメソドロジーはリスクの発生可能性、影響度により、識別されたＩＴ全般統制のキーコントロールを評価することを提言している。

ＧＡＩＴ手法を用いることにより想定される評価上の効果については、第５章４．で詳述するが、ここでは、その手法から来る方法論的メリットと、ＩＴを利用する企業にもたらされる付随的メリットを整理しておく。

まず方法論的メリットだが、ＧＡＩＴメソドロジーは、リスクベースアプローチであることから「これがないと失敗が発見されないか」、「重要な誤りに結び付くか」、「合理的に

期待されるか」というフィルターを通過したコントロールのみが、ＩＴ全般統制のキーコントロールと認定される。ＧＡＩＴが推奨する統合チームは、監査、システム、財務の専門家が合同で検討することで、多面的なリスク識別が可能となり、プロジェクト開始初期に、キーコントロールを適切に選定することができる。

更に合理的人物（内部監査部長、システム統括部長、経理部長）によるレビューにより、仮にＩＴ全般統制に不備があっても、人的な補完的統制が存在し不備をカバーしていることを説明できる。

次に付随的メリットとしては、監査法人の窓口となる経理部長が、合同作業を通じてＩＴシステムの内容を十分理解し、ＩＴ全般統制のキーコントロール識別理由と補完的統制を自ら説明できるようになる。ＧＡＩＴメソドロジーは、そのための「説明シート」を用意している。ＩＴ全般統制キーコントロール選定理由をきっちり説明できれば、恣意的にＩＴをキーコントロールから除外することや、せっかくのＩＴ機能を手作業とみなしてサンプルテストを実施するなどといった対症療法に陥る懸念はなくなるものと考える。

① 方法論的メリット
1．合同作業を通じて、プロジェクトの初期ＩＴ全般統制キーコントロールを識別できる。
2．合理的人物がレビューし、補完的統制を含めた説明ができる。
② 付随的メリット
1．経理部長が「説明シート」を使って、監査法人にキーコントロール識別理由を説明できる。

システムは生き物であり、利用シーンも時代とともに常に変遷している。

システム開発・運用の外部委託の時代、そしてウェブアプリケーションの一時利用から、クラウドコンピューティングへとＩＴ技術も進化しつつある中、アプリケーションの変更管理などに関する統制行動もその評価を含めて、大きく変化していくことが予想される。

そうした意味においても、トップダウンアプローチによって、業務の基本部分を明確に認識した上で、ＩＴ利用シーンにおけるキーコントロールを合理的に識別し、財務報告の信頼性に影響しないことを「説明シート」によって正確に押さえておくことが、第三者にもわかりやすい内部統制報告書へと結び付くものと考える。

第５章　ＩＴ全般統制の評価方法に関する提言

第４章で述べたように、ＧＡＩＴメソドロジーは財務報告の信頼性を確保するためにＩＴ全般統制プロセスのリスクを低減するための統制目標を識別し、その統制目標を達成するためのＩＴ全般統制プロセスのキーコントロールを識別するといった、トップダウン型のリスクベースアプローチである。

このアプローチは、財務報告の信頼性に関する内部統制においてＩＴ全般統制の評価の範囲を絞り込み、財務報告の信頼性とＩＴ全般統制の関係を整理する有用な方法であると理解している。

それでは、ＧＡＩＴメソドロジーによって識別されたＩＴ全般統制のキーコントロールの不備はすべて財務報告の信頼性に対して重大な影響を与えるものとなるのか、また識別されたすべての不備に対して是正措置を実施しなければならないのかが検討課題となる。

ここでは、ＧＡＩＴメソドロジーによって識別されたＩＴ全般統制のキーコントロールの不備の評価に対するＧＡＩＴ－２の有用性について検討を行い、更にＧＡＩＴメソドロジーとＧＡＩＴ－２（以下、「ＧＡＩＴ手法」

という）を導入することにより想定される効果と課題について整理してみることとする。

1．初年度に実施された評価についての振り返り

第３章の内容に基づいて、この研究で取り上げた初年度のＩＴ全般統制の評価事例を振り返ってみると、概して識別されたＩＴ全般統制の不備と財務報告の信頼性の関係を整理することなく、その不備の是正措置を実施している傾向が認められる。

具体的にどのような傾向が認められたのか、以下に考察する。

⑴ 評価対象分野と評価項目の選定

各企業は、金融庁の「実施基準」に記載された以下の４つの分野を対象にＩＴ全般統制の評価を実施している。

① システムの開発・保守
② システムの運用・管理
③ システムの安全性の確保
④ 外部委託に関する契約の管理

これら４つの分野を基本として、監査人との協議の下、ジョブ実行管理、バックアップ管理、アクセス管理、障害管理等に細分化して評価を行っている企業がほとんどである。

また、評価方法として各企業ともに上記４つの分野についてチェックシート方式、ＲＣＭ方式により評価を実施している。これらの方式で評価すべき事項として選定した項目は、ＣＯＢＩＴをベースとしたものや監査人と協議して選定したものがほとんどであるが、評価項目数が30～100項目と企業によってかなりバラツキがある。

更に、各評価項目を見てみると明確にアサーションと関連付けて評価している企業はほとんどなく、財務報告の信頼性の視点で評価するのか、ＩＴガバナンスの視点で評価するのか明確ではない。

⑵ 不備の評価

上記⑴で述べたように、ＩＴ全般統制の評価対象分野及び評価項目と、財務報告の信頼性との因果関係を明確に整理して取り組んでいるところはほとんどなかった。

こうした状況下、実際には財務報告に係る信頼性への影響を十分に評価することなく、また統制目標を達成するという視点ではなく、識別された個々のＩＴ全般統制の不備を個別に是正するという、ややもすれば対症療法的ともいえる対応になっているように見受けられる。

これら⑴⑵にみられる各企業のＩＴ全般統制に関する初年度の評価の取組傾向から、

> ① 財務報告の信頼性との関連を明確にしながらＩＴ全般統制の評価範囲、キーコントロールを選定する方法を確立すること。
> ② 識別したＩＴ全般統制のキーコントロールに関する例外事項が財務報告の信頼性に対して不備、重要な欠陥であることを識別するための合理的な評価方法を確立すること。

が課題であると考えられる。

上記①の課題の解決については、第４章でＧＡＩＴメソドロジーが有用な方法の１つであると我々は提言した。したがってこの第５章では上記②の課題を解決する方法について考察する。

2．ＧＡＩＴ－２の適用について

⑴ ＩＴ全般統制の不備の扱い

金融庁の「実施基準」によれば財務報告の信頼性とは「財務諸表及び財務諸表に重要な影響を及ぼす可能性のある情報の信頼性を確保すること」と定義されている。我々は、ＩＴ全般統制のキーコントロールが“財務諸表及び財務諸表に重要な影響を及ぼす”といった視点で識別されているか、また影響を及ぼすものであるかどうかを認識する必要がある。

この“財務諸表及び財務諸表に重要な影響

を及ぼす”といった視点で識別されているかどうかについてはＧＡＩＴメソドロジーを用いて重要な役割を担うＩＴ全般統制のキーコントロールを効果的に識別できることを理解した。

それでは、このように識別されたＩＴ全般統制のキーコントロールに不備が発見された場合、それは即、財務報告の信頼性に重要な影響を与えるものと判断して良いのであろうか。敢えて誇張した言い方をすれば、先の振り返りで確認したように多くの企業が初年度の取組みの中で識別したＩＴ全般統制に係る不備については、「すべての不備は発見、即是正対応」的なことを行っており、対応する担当者が財務報告の信頼性に与える影響を理解しながら、かつ納得しながら対応しているとはいいがたいのではと考えている。

例えば、重要なアプリケーションの操作に係るアクセス権の登録手続といった統制を考えた場合、その統制目標を考えると、

① 財務報告の改ざんのリスクを低減するといった財務報告の信頼性に係る統制目標
② 企業の財務に係る情報漏洩のリスクを低減するといった情報セキュリティに係る統制目標

というようにいくつかの目標が考えられ、必ずしも財務報告の信頼性に係る統制目標を達成するだけではない。したがって、重要なアプリケーションの操作に係るアクセス権の登録手続の不備が発見されたとしても、業務上のどのポイントで不備が発見されたかによって関連する統制目標が異なることが考えられる。

この点を明示的に整理せずに「すべての不備は発見、即是正対応」的なことを行ってしまっていることが、多くの企業担当者が「対応する担当者が財務報告の信頼性に与える影響を理解しながら、かつ納得しながら対応しているとはいいがたい」、「評価が難しいと感じている」ことの大きな原因ではないかと考える。

したがって、財務報告の信頼性との関係を整理しながら絞り込むことによって識別したＩＴ全般統制のキーコントロールについて、

① その不備が財務報告の信頼性に重要な影響を与えるものであるのかどうか。
② その不備に対する是正措置の統制目標は財務報告の信頼性を確保するものであるかどうか。

を十分に検証した上で是正措置を実施する必要がある。

⑵ ＩＴ全般統制の不備の評価

それでは、ＩＴ全般統制のキーコントロールの不備は具体的にどのように検証すれば良いのであろうか。我々はその具体的な方法として、ＧＡＩＴシリーズのＧＡＩＴ－２に着目し考察した。

ＧＡＩＴ－２が有用でないかと我々が着目した点は、ＧＡＩＴ－２が示す“依拠の連鎖(Reliance Chain)”と“ＩＴ全般統制の統制目標の評価”の２つの考え方である。

まず１番目の“依拠の連鎖（Reliance Chain)”は、個々のＩＴ全般統制のキーコントロールの不備と財務諸表の信頼性との関係を整理する一連の流れを示すもので、先のＧＡＩＴメソドロジーの流れを逆の方向に辿るものである。このことにより、個々のＩＴ全般統制のキーコントロールの不備と統制目標の達成の関係、統制目標の達成の状況と財務諸表の信頼性が損なわれるリスクの関係を整理、評価する。

この関係を理解することで、識別したＩＴ全般統制の不備が財務報告の信頼性に対して間接的で捉えにくく、不備又は重要な欠陥であるかどうか（どのような影響を与えるのか）といった評価が難しいと感じている企業が評価方法についての考え方を整理することができるのではないかと考える。

次に、２番目の“ＩＴ全般統制の統制目標の評価”についてＧＡＩＴ－２は、ＩＴ全般

統制の統制目標の達成は、個々のコントロールの不備でなく、統制目標を同じくするコントロールグループの不備としてその影響を評価するという考えを持つ。

これは、財務報告の信頼性に関する不備について、ＩＴ全般統制上の個々の不備が存在する理由（不備の存在そのもの）を説明することではなく、その不備が重大な欠陥でないか否かを評価することを重視する、という考え方である。言い換えれば、不備の存在をなくすことに注力する前に、その不備の影響を評価し、統制目標の未達成が重要な欠陥につながるものであるかを評価することに注力することである。

このことは、初年度のＩＴ全般統制の評価において識別された個々のキーコントロールの不備について「すべての不備は発見、即是正対応」的対応を実施した企業にとって、１つの指針を与えるものである。

以上のことから、

> ＧＡＩＴ－２は、識別した個々のＩＴ全般統制のキーコントロールの不備が財務報告の信頼性に対して不備、重要な欠陥であるといえるための合理的な評価方法を導く、有用かつ基本的な考え方の１つである。

と考える。

３．評価体制について

評価体制に関して、「専門性対独立性の観点」、「組織特性（規模特性）の観点」、「業種特性の観点」、「システム基盤の観点」から、ＧＡＩＴ手法を導入する前後の変化について考察した。

⑴ 専門性 対 独立性

ＧＡＩＴ手法では、ＩＴ全般統制のキーコントロールの識別に対して“合理的な人物”によるレビューを実施することを求めている。この“合理的な人物”とは専門性と独立性を兼ね備えた“人物”と解釈できるが、必ずしも実在する特定の人物を指すわけではなく、専門性と独立性を兼ね備えた組織でも良いと考える。しかし、実際問題として、専門性と独立性を両方具備している人物（組織）は非常に限定されているので、内部監査部長、システム統括部長、経理部長の三者の協議体がこの“合理的な人物”の役割を果たすことになる。

自社内部監査部門にＩＴの専門性がない場合、一般的に各企業は次の４つの中から選択しているのが実情である。

① ＩＴ全般統制の評価を外部委託するケース
② 情報システム部門から内部監査部門に移籍してもらって評価するケース
③ 情報システム部門の協力の下で、評価するケース
④ 情報システム部門が自己点検した結果を、内部監査部門がその合理性を評価するケース

ＧＡＩＴ手法は未だ一般的になっていないので、各企業が自立的に学習していくケースが多くならざるを得ないと考える。すなわち、財務報告に係る内部統制の整備、評価について、各企業自身で対応する必要があり、上記①の外部委託するケース以外を選択することが合理的な対応であると考える。

⑵ 組織特性

組織特性としては、やはり企業規模の影響が一番大きい。大規模企業では一般的に次の６つの組織が役割分担しながら内部統制の整備、評価を実施しているケースが多い。なお、以下の①～④は執行側の部門である。

① ユーザー部門
② プロセスオーナー
③ 情報システム部門
④ 内部統制推進チーム
⑤ 内部監査部門
⑥ 内部統制推進委員会

ＧＡＩＴ手法では、アプリケーション層、

データベース層、オペレーティングシステム層、ネットワーク基盤における変更管理、運用、情報セキュリティにフォーカスしているので、評価体制としては、情報システム部門の協力が不可欠なものであり、情報システム部門と内部監査部門が連携して実施せざるを得ない。

また、中堅企業では内部監査室の陣容が小さいことから、情報システム部門が行った自己点検結果を内部監査部門が評価することは業務上の負荷が大きくなる。そのため、中堅企業では、前項⑴で検討した専門性と独立性を確保し、リソース不足を補うために、専門性のあるコンサルティング会社に委託して評価してもらうか、外部監査人に直接評価してもらうことになるケースが多くなるであろう。

⑶ 業種特性

業種によるリスクの違いはあるが、ＩＴ全般統制の評価体制という観点では、業種による差異はないと思われる。

⑷ システム基盤

各企業においては、業種業態に応じて様々なシステム基盤を導入しており、それに伴って財務報告に影響を与えるリスクも異なることが容易に想定される。よってシステム基盤ごとに、評価に必要なスキルが異なることから、基本的にはシステム基盤ごとに評価体制を考える必要がある。

特に、大規模なシステム基盤を対象とする場合は、各システム基盤ごとに評価体制を構築することになる。

ただし例えば、ユーザーからの開発要求に対する承認手続、テスト手順、開発側から運用側への移管手続といったシステム基盤にかかわらず評価すべき項目の共通化を図ることで、その効率化を実現できる。

また、前項⑵でも検討したように中堅企業では、小規模なシステム基盤が複数あることが想定されるため、１つのチームですべてのシステム基盤を評価する体制にせざるを得ないであろう。

結論として、初年度に多くの企業が採用した体制と上記検討内容を比較すると、ＧＡＩＴ手法を導入することによる評価体制上の著しい差異はないように思われる。

すなわち、情報システム部門の協力の下に内部監査部門が評価する体制に変化はないと考える。

４．ＧＡＩＴ手法の採用により想定される効果

⑴ 財務報告の信頼性との関係がより明確になる

Ｊ－ＳＯＸの本来の目的である「財務報告の信頼性の確保」と「ＩＴ全般統制」の関連性については、かねてより大きな課題となっている。ＧＡＩＴ－２では評価原則として「一定の評価が終了した時点での不備が財務報告に与える影響」についてフォーカスしているため、現状明確な指針がないまま不備についての対症療法的な是正を行っている各社にとっては、現実的な対応を行いうる妥当な方法だと考えている。

またＧＡＩＴ－２では、トップダウンアプローチで導き出されたＩＴ全般統制のキーコントロールにおける不備が識別された場合、その不備を起点に逆から遡って勘定科目に到達させるプロセスであるため、当初の考え方でのボタンのかけ違い（財務報告に関連性のない統制）を再検証することで財務報告との関係がより明確になるものと思われる。

⑵ 評価対象分野と評価項目が適切に識別される

各社の初年度のＩＴ全般統制の評価においては、財務報告の信頼性とＩＴ全般統制の評価対象範囲や評価項目の因果関係を明確にして評価を実施したとはいいがたい状況にある。

これに対して、ＧＡＩＴメソドロジー及びＧＡＩＴ－２は個々のコントロール機能の評

価ではなく、財務報告の信頼性を確保するための統制目標が達成されているかどうかを評価する。したがって、網羅的に個々のコントロールをリストアップして評価するのではなく、あくまで財務報告に大きな影響を与えるリスクに対する統制目標を達成するためのコントロール（キーコントロール）を識別し、評価することを目指している。

⑶ リスクの変化（外部環境の変化）に適応しやすい

当然のことながら、各社のＩＴに関する環境、方針、統制は、法規制、各種基準、市場動向等の外部環境の変化によって修正を余儀なくされるものであり、そのたびに念頭に置いておく必要があるのは⑴の「財務報告の信頼性」との関係である。ここが不明確なまま外部環境の変化に対応しようとした場合、社内の様々な立場（経営層、情報システム部門、ユーザー部門、管理部門、内部監査部門等）の共通理解がないままに重要なシステム変更の意思決定がなされ、更なる悪循環に陥ることが予想される。

⑷ 統制目標（グループ）の達成による標準化と効率向上を推進できる

ＧＡＩＴ－２の特徴である前項目⑵“財務報告の信頼性に対する統制目標の達成は、個々のコントロールの不備でなく、統制目標を同じくするコントロールグループの不備としてその影響を評価する”ことにより、適切な標準化と業務効率の向上が見込まれる。これは、単体としての個別のシステム対応でのコントロール不備に対する局所的な是正をやみくもに実施するのではなく、システム全体としての統合化された原則的な統制を改めて構築することでの利点である。

例えば、「不正アクセスによるデータ改竄されないためのアクセス管理」という統制目標については、Ａシステムのテストによりたまたま１件の権限者以外の特別アクセスが発見されたような場合、このＡシステムでの１件に対する要因に基づく是正を実行することよりも、全社共通規制による標準的なアクセス管理手法を再確立する方が長期的な視点での効率性において有効であると思われる。

（ＧＡＩＴ－２評価プロセスシミュレーション（仮想事例）参照）

⑸ コストの削減（内部工数、是正対応）が可能となる

ＩＴに係るコストの透明化・明確化は、Ｊ－ＳＯＸに限らずすべての企業にとっての重要な経営課題である。今回のＩＴ全般統制についても、構築、評価、是正の各段階で従来想定していなかった様々なコストが発生しているはずであり、企業、特に経営者にとっては、目に見えない（見えにくい）改善に対してのコスト発生は、できる限り避けたいところであると思われる。

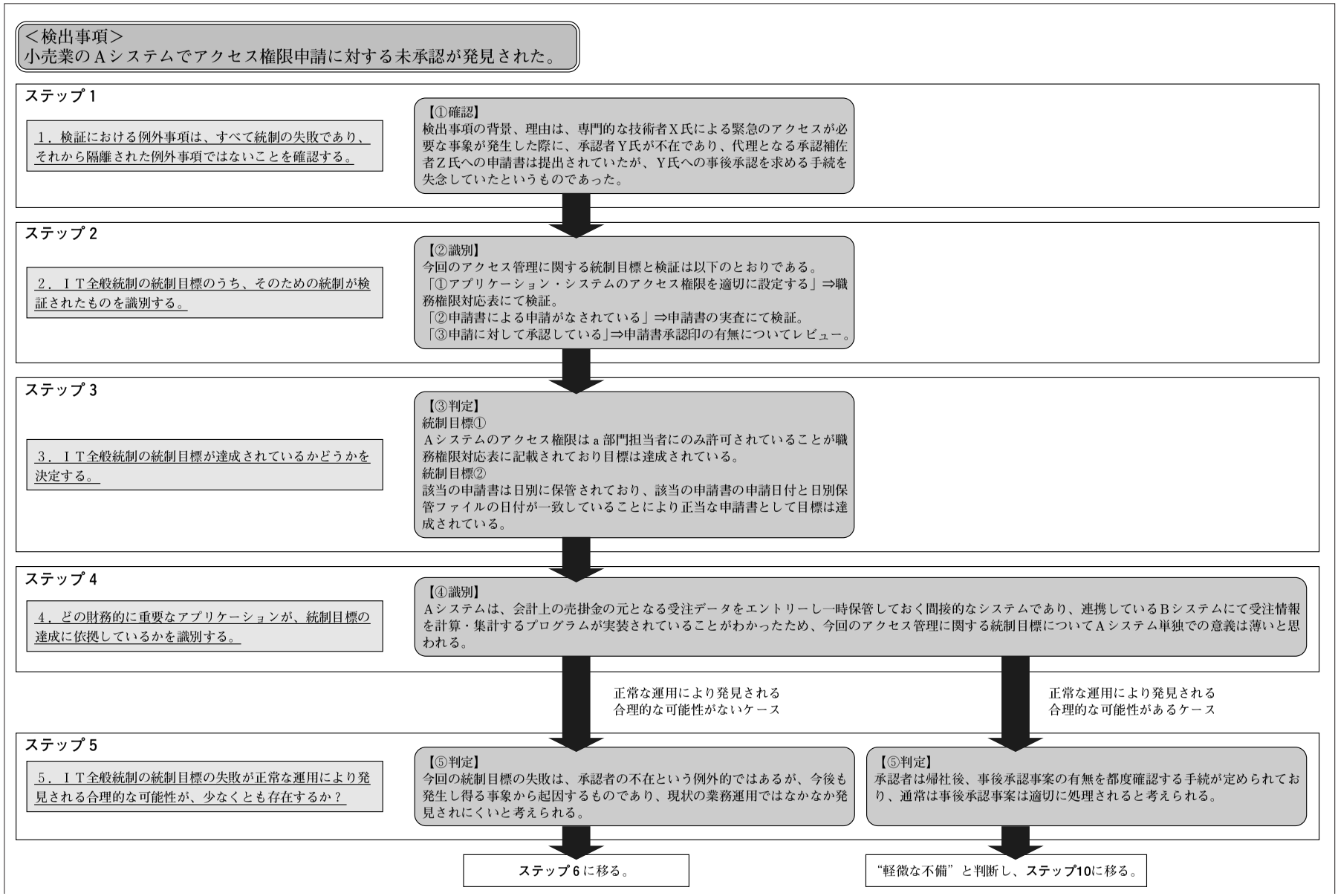
ＧＡＩＴ－２での統制目標（グループ）の達成が定着することにより、目的の明確化と標準的統制が図られ、是正活動のための人的及びシステム的な全体コストは削減されるはずである。

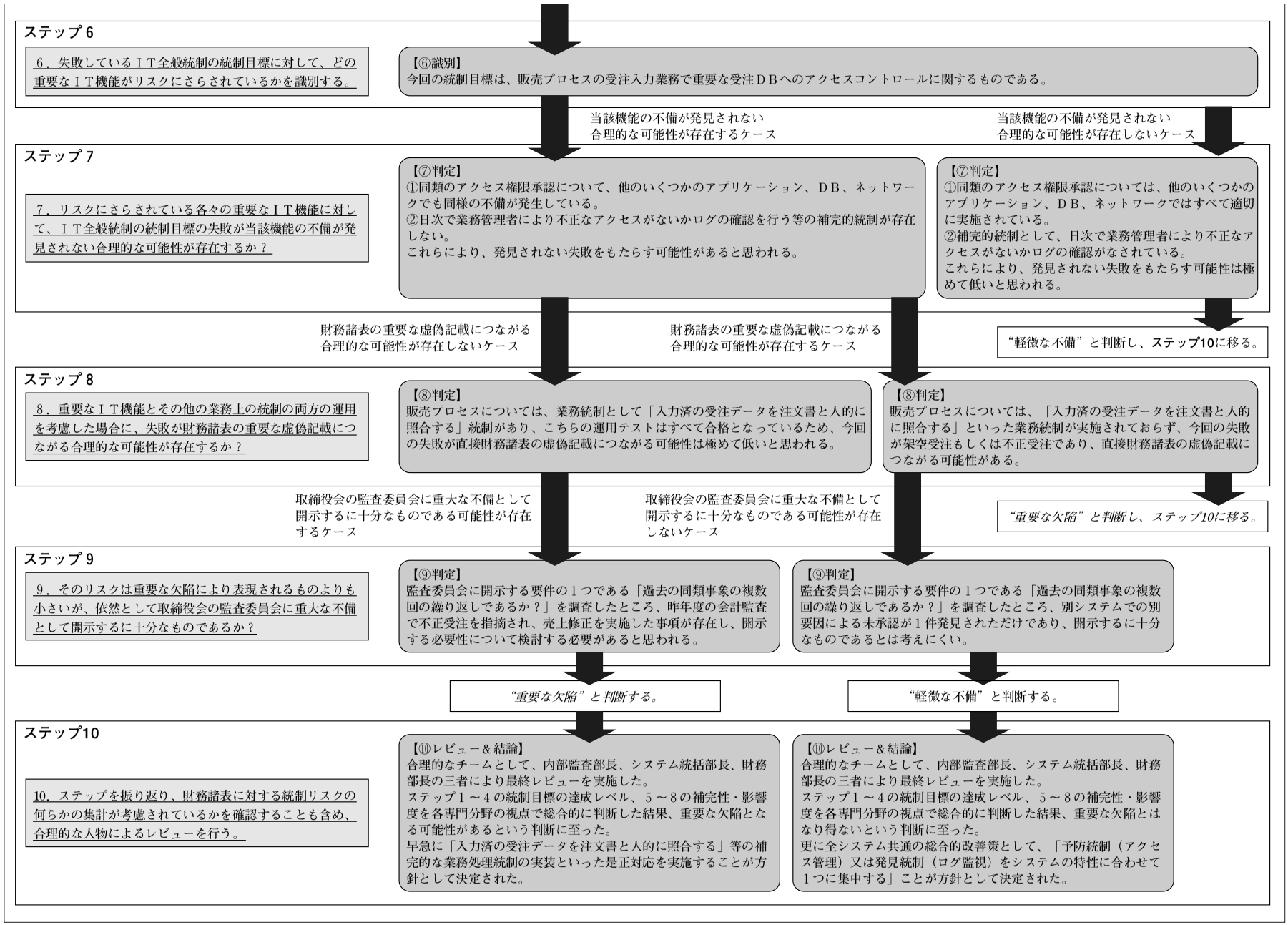
⑹ リスクベースによる根本原因の識別が容易になる

ＧＡＩＴ－２での評価原則「重要な欠陥が存在するためには、ａ）発生可能性、ｂ）影響度の２つの検証が充足されなければならない」すなわち重要な欠陥となりうるか判断するためにはリスク評価手法を適用することになり、改めて「この場合のリスクは何なのか？」という意識を全社共通理解することで、不備の根本的な原因を早く、適格に識別できることになると考える。

実態として、評価後の是正段階では、関係者の疲弊、期末評価時点までの時間不足等により、リスクに対する視点が失われたまま、対症療法的に是正を実行しなければならないケースも多かったのではないかと思われる。

＜図表４＞ＧＡＩＴ－２評価プロセスシミュレーション（仮想事例）




ステップ6
6．失敗しているＩＴ全般統制の統制目標に対して、どの重要なＩＴ機能がリスクにさらされているかを識別する。
【⑥識別】
今回の統制目標は、販売プロセスの受注入力業務で重要な受注ＤＢへのアクセスコントロールに関するものである。
当該機能の不備が発見されない
合理的な可能性が存在するケース
当該機能の不備が発見されない
合理的な可能性が存在しないケース
ステップ7
7．リスクにさらされている各々の重要なＩＴ機能に対して、ＩＴ全般統制の統制目標の失敗が当該機能の不備が発見されない合理的な可能性が存在するか？
【⑦判定】
①同類のアクセス権限承認について、他のいくつかのアプリケーション、ＤＢ、ネットワークでも同様の不備が発生している。
②日次で業務管理者により不正なアクセスがないかログの確認を行う等の補完的統制が存在しない。
これらにより、発見されない失敗をもたらす可能性があると思われる。
【⑦判定】
①同類のアクセス権限承認については、他のいくつかのアプリケーション、ＤＢ、ネットワークではすべて適切に実施されている。
②補完的統制として、日次で業務管理者により不正なアクセスがないかログの確認がなされている。
これらにより、発見されない失敗をもたらす可能性は極めて低いと思われる。
財務諸表の重要な虚偽記載につながる
合理的な可能性が存在しないケース
財務諸表の重要な虚偽記載につながる
合理的な可能性が存在するケース
“軽微な不備”と判断し、ステップ10に移る。
ステップ8
8．重要なＩＴ機能とその他の業務上の統制の両方の運用を考慮した場合に、失敗が財務諸表の重要な虚偽記載につながる合理的な可能性が存在するか？
【⑧判定】
販売プロセスについては、業務統制として「入力済の受注データを注文書と人的に照合する」統制があり、こちらの運用テストはすべて合格となっているため、今回の失敗が直接財務諸表の虚偽記載につながる可能性は極めて低いと思われる。
【⑧判定】
販売プロセスについては、「入力済の受注データを注文書と人的に照合する」といった業務統制が実施されておらず、今回の失敗が架空受注もしくは不正受注であり、直接財務諸表の虚偽記載につながる可能性がある。
取締役会の監査委員会に重大な不備として
開示するに十分なものである可能性が存在
するケース
取締役会の監査委員会に重大な不備として
開示するに十分なものである可能性が存在
しないケース
“重要な欠陥”と判断し、ステップ10に移る。
ステップ9
9．そのリスクは重要な欠陥により表現されるものよりも小さいが、依然として取締役会の監査委員会に重大な不備として開示するに十分なものであるか？
【⑨判定】
監査委員会に開示する要件の１つである「過去の同類事象の複数回の繰り返しであるか？」を調査したところ、昨年度の会計監査で不正受注を指摘され、売上修正を実施した事項が存在し、開示する必要性について検討する必要があると思われる。
【⑨判定】
監査委員会に開示する要件の１つである「過去の同類事象の複数回の繰り返しであるか？」を調査したところ、別システムでの別要因による未承認が１件発見されただけであり、開示するに十分なものであるとは考えにくい。
“重要な欠陥”と判断する。
“軽微な不備”と判断する。
ステップ10
10．ステップを振り返り、財務諸表に対する統制リスクの何らかの集計が考慮されているかを確認することも含め、合理的な人物によるレビューを行う。
【⑩レビュー＆結論】
合理的なチームとして、内部監査部長、システム統括部長、財務部長の三者により最終レビューを実施した。
ステップ１～４の統制目標の達成レベル、５～８の補完性・影響度を各専門分野の視点で総合的に判断した結果、重要な欠陥となる可能性があるという判断に至った。
早急に「入力済の受注データを注文書と人的に照合する」等の補完的な業務処理統制の実装といった是正対応を実施することが方針として決定された。
【⑩レビュー＆結論】
合理的なチームとして、内部監査部長、システム統括部長、財務部長の三者により最終レビューを実施した。
ステップ１～４の統制目標の達成レベル、５～８の補完性・影響度を各専門分野の視点で総合的に判断した結果、重要な欠陥とはなり得ないという判断に至った。
更に全システム共通の総合的改善策として、「予防統制（アクセス管理）又は発見統制（ログ監視）をシステムの特性に合わせて１つに集中する」ことが方針として決定された。

5．ＧＡＩＴ手法の採用により想定される課題

⑴　ＧＡＩＴによるＩＴ全般統制の評価に対して監査人の理解

一般的に監査法人に所属している公認会計士、システム監査人については、所属法人による独自の指針があると思われる。一方、ＧＡＩＴに関しては、ＩＩＡが公表している指針であり、これに対する外部監査人の視点としてどのような見解があるかは現状では認識できていない。

財務報告の信頼性に焦点を絞っている部分は、合意を得られるはずであるが、問題となるのは「過年度においていったん結論を出している指摘事項」を、ＧＡＩＴを用いた指針で外部監査人に説得しえるかという点だと思われる。

⑵　評価における作業見積り時間の事前準備

ＧＡＩＴ手法を全面的に活用していくに際しては、スコーピングに関するＧＡＩＴメソドロジー、評価に関するＧＡＩＴ－２においての準備段階での作業に時間を費やす必要があると思われる。

そのため最初の計画立案の時点で必要な作業時間を的確に見込んでおく必要がある。重点としては、評価範囲を設定するスコーピングと評価後の不備の検討に時間を割くべきであり、純粋な作業としての自己点検、運用テスト等については、一度経験した作業をマニュアル化しできる限り時間短縮して全体配分を適切に考えていくことが重要であると思われる。

⑶　内部統制推進チーム内での認識、理解のための教育

上記⑴、⑵とも関連してくるが、社内での関連部門（ＣＦＯ（Chief Financial Officer）、ＣＩＯ（Chief Information Officer）、経理、情報システム、関連業務部門等）の理解を得ておくことは必須であり、そのための教育の場が必要であると考える。

共通となる基盤の理解は果たせているので、自社のＩＴ環境の中でどのように認識を深めていくことができるかを試行錯誤しながら進めていくことにより実践的な教育としての要件が満たせるのではないかと考える。

その際に想定されうる内部統制推進チーム内での課題としては「財務報告に影響がある業務とシステムは何か」が考えられる。「業務側からシステムがどこまで見えるか」、「システム側から業務がどこまで見えるか」、「この２つと財務報告との関係は」といった全体俯瞰的な視点が必要となるはずであり、それについては、内部監査部門等の評価部門が今後も橋渡し的な役割を果たしていく必要がある。

この章では初年度に各企業が実施した内部統制評価を振り返りながら、ＩＴ全般統制の評価方法についてレビューを行い、いくつかの提言を行った。

1．識別された不備について、重要な欠陥に当たるかどうかの合理的な評価方法としてＧＡＩＴ－２が有効であると考えられること。
2．ＧＡＩＴ－２を導入することにより、財務報告の信頼性とＩＴ全般統制の関係を明確にすることができると考えられること。
3．ＧＡＩＴ－２を導入した場合、評価体制への影響はほとんどないと考えられること。
4．今後の課題として監査人や組織内の理解を得る必要があること。

【用語集】

用語	用語の説明
ＵＳ－ＳＯＸ	アメリカ「企業改革法」。404条：内部統制に関する法令。
Ｊ－ＳＯＸ	「いわゆるＪ－ＳＯＸは、金融商品取引法の第24条４の４及び４の６を指す」
ＣＯＢＩＴ	Control Objectives for Information and related Technology 企業・自治体の組織のＩＴガバナンスの指針として、アメリカの情報システムコントロール協会（ＩＳＡＣＡ）などが推奨しているＩＴガバナンスの実践規範のこと。
COBIT for SOX	IT Control Objectives for Sarbanes-Oxley（COBIT for SOX） COBIT for SOXは、ＩＴガバナンスのフレームワーク「COBIT 4.0」を「財務報告にかかる内部統制」の視点で抽出・整理し、ＵＳ－ＳＯＸで必要とされるＩＴ統制の目標を明確にしたものとされている。
実施基準	金融庁企業会計審議会の「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」のこと。
実務指針	2005年12月８日に企業会計審議会内部統制部会が公表した「財務報告に係る内部統制の評価及び監査の基準のあり方について」を通称「実務指針」と呼んだ経緯から、当論文でも「実務指針」として使用している。なお、上述の「実施基準（公開草案）」は、約１年後の2006年11月21日に公表されている。
ＩＴ統制	「実施基準」の中で規定されている「ＩＴの統制」のこと。 ＩＴを取り入れた情報システムに関する統制を指す。
ＩＴ全社統制	「実施基準」の中で、「（参考１）財務報告に係る全社的な内部統制に関する評価項目の例」として、ＩＴへの対応に関して５つの評価項目が記載されている。 「実施基準」の中ではＩＴ全社統制という言葉は使用されていないが、ＩＴに関する全社的な内部統制の評価項目ということで、この５つの評価項目を「ＩＴ全社統制」と定義する。
ＩＴ全般統制	「実施基準」の中で規定されている「ＩＴに係る全般統制」のこと。 業務処理統制が有効に機能する環境を保証するための統制活動を意味する。
ＩＴ業務処理統制	「実施基準」の中で規定されている「ＩＴに係る業務処理統制」のこと。 業務を管理するシステムにおいて、承認された業務がすべて正確に処理、記録されることを確保するために業務プロセスに組み込まれたＩＴに係る内部統制のこと。
アサーション	財務報告の信頼性を保証するための、経営者による適切性主張項目。 １．実在性　２．金額評価　３．期間配分　４．網羅性　５．権利／義務　６．表示／開示
キーコントロール	６つのアサーションを最も効果的にカバーする重要な統制
ＧＡＩＴメソドロジー	ＩＩＡの「GAIT Methodology」のこと。 ＩＴ全般統制のキーコントロールの絞込み手法として、トップダウン型のリスクアプローチ手法が規定されている。
ＧＡＩＴ―２	ＩＩＡの「GAIT for IT General Control Deficiency Assessment」のこと。 発見されたＩＴ全般統制のキーコントロールの不備が、重大なリスクであるかを評価する手法が規定されている。

＜ＣＩＡフォーラム関西研究会No.14メンバー＞　（順不同・敬称略）

（座　　長）八槇　博和

（メンバー）飯田　豊志／岡谷　亨／影山　裕／工藤　秀隆／鈴木　章彦／関口　善昭／
寺本　勲／中西　豊和／村上　不二男／和田　光平