特集：SOX法対応

ITサービスを提供する事業者における内部統制監査について

公認会計士
深 見 浩 一 郎 氏

1．はじめに

2005年12月8日、金融庁から企業会計審議会内部統制部会の「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」（以下「基準案」）、いわゆる日本版SOX法における内部統制監査制度に関する基準案が公表された。昨年7月の公開草案発表から約4ヵ月を要しての公表である。「基準案」には、詳細な実務上の指針として「実施基準」の検討が明記されているが、平成18年4月の時点で、公表の予定は定かとなっていない。

その一方、2006年3月13日、「基準案」の根拠法規である「金融商品取引法」が国会に提出された。今国会での法案成立を想定すると、最短で平成20年4月開始事業年度（2009年3月期）からの内部統制監査の適用が予想される。しかし、具体的な実施時期については、今後公表される施行令等に継続して注意する必要がある。

本稿は、以上の状況を踏まえ、ITサービスを提供する事業者に対して日本版SOX法、とりわけ内部統制監査制度がどのような影響を与えるのかを考察したものである。

2．内部統制監査制度

日本における内部統制監査制度は、①経営者（企業）自らによる内部統制の有効性評価、②経営者による内部統制報告書の作成、③内部統制報告書の外部監査の適用、④外部監査人の内部統制監査報告書の作成を骨子とする制度である。この制度により初めて企業の内部統制の状況が開示され、内部統制の有効性が外部保証されることになる*1。内部統制監査制度は、財務報告の信頼性確保を目的としている*2。この制度は、2002年米国で成立した企業改革法*3（通称SOX法）404条における規制と同様の趣旨のものである。

3．内部統制と監査

監査は、財務報告の信頼性を外部保証する制度である。現在実施される財務諸表監査は、試査、すなわちサンプリングに基づいて実施される。試査による監査が成立するためには、被監査会社の内部統制が有効に機能していることが前提となる。

一定規模以上のいわゆる大手企業に対して試査によらない監査*4を適用することは、決算期末から3ヵ月以内とい

＊1）内部統制の有効性評価は、従来から監査手続きとして実施されてきた。内部統制の評価結果を監査意見として公表しない現在の財務諸表監査は、内部統制の有効性を保証するものではない。同様に、監査意見を公表しないシステム監査もシステムの信頼性を外部保証するものではない。

＊2）内部統制監査で対象とする内部統制は、財務報告に関連する内部統制である。したがって、内部統制監査制度の目的は、コンプライアンス（法令順守）ではなく、財務報告の信頼性確保である。

＊3）企業改革法の正式名称は、「証券諸法に準拠し、かつその他の目的のために行われる企業のディスクロージャの正確性と信頼性の向上により、投資家を保護するための法」である。法の目的は開示の規制と市場の信頼性回復にある。

＊4）試査によらない監査手続きは、精査である。精査では、財務報告を構成するすべての会計取引を検証対象とする。

う法定された報告期限や監査コスト面からも、現実的に不可能である。結果として、監査意見が得られなければ、企業は、株主や投資家への説明責任を果たせず、証券市場からの撤退を余儀なくされる。誤解を恐れず単純化すれば、内部統制が有効に機能していることが公開企業としての存続条件の1つとなっている。

4．内部統制とIT

内部統制は、企業活動が経営目的に沿って、合理的に実施されることを促進する。経営者は、財務報告の信頼性確保のため、内部統制を整備する。財務報告の信頼性は、内部統制により担保されなければならない。したがって、財務報告の信頼性を検証するには、内部統制が企業内で有効に機能していることを検証しなければならない。

しかし、高度に情報化が進展した今日、企業活動はおおむねITに依存し実施されている。このため、内部統制の有効性を検証するには、ITに基づく内部統制の有効性を確認することが必要不可欠となっている。

「基準案」では、この点を「ITへの対応」として取り上げ、その内容を「IT環境への対応」と「ITの利用および統制」とに区分している。

以上から、現代企業は、財務報告の信頼性に関して説明責任を果たすためには、ITに基づく内部統制の有効性を確保し、これに関して外部監査による検証を受けなければならない。

5．IT統制とIT統制目標

ITに基づく内部統制の有効性を検証するためには、ITに関連する内部統制機能を検証する必要がある。ITに関連する内部統制機能は、IT統制と呼ばれる。IT統制は、COSOフレームワーク（参考文献1参照）によれば、IT全般統制と業務処理統制[*5]とに区分される。

IT統制の機能に関する評価は、一定の評価基準をもって行われる。ITを評価する基準ないし尺度が、IT統制目標である[*6]。

欧米で広く普及しているIT統制目標としては、ITガバナンス協会（参考文献4参照）の「COBIT」がある[*7]。国内では経済産業省の「システム管理基準」などがある。わが国の内部統制監査制度において、経営者が実施するIT統制の評価基準として何をどのようにして採用すべきかという点に関しては、今後公表される「実施基準」等で示されることになろう。

経営者がどのような内部統制フレームワークを採用するかに関しては、米国における先例では、公開草案等の公開のプロセスを踏んで確立されたフレームワークであればよいとされている。この点に関しては、国内においても同様の取り扱いではないかと思われる。なお、表1は、COBIT第3版で示されているIT統制目標である。

表1　COBITのIT統制目標

有効性（effectiveness）	該当する業務プロセスと関係のある有用な情報を取り扱うこと。また、タイムリーに、正確に、首尾一貫して、使いやすいように提供されていること
効率性（efficiency）	情報提供が、資源を効率的（最も生産的かつ経済的）に利用し行われること
機密性（confidentiality）	無許可の開示から情報を保護すること
完全性（integrity）	情報が正確で漏れがなく、ビジネス価値と期待に照らし情報が妥当であること
可用性（availability）	業務プロセスで必要とされる情報が必要とされる時に利用可能なこと
準拠性（compliance）	業務プロセスが従わねばならない法律、規則、契約条項を遵守すること
信頼性（reliability）	経営者が組織運営し、受託義務とガバナンスの責任を果たす上で、適切な情報を提供すること

6．内部統制とITサービス

「基準案」の中において、内部統制監査制度におけるITサービスを提供する事業者の位置づけを確認することが出来る箇所がある。経営者による内部統制評価の評価範囲に関する定義の終わりにある次の注書きがそれである。

「外部に委託した業務の内部統制については評価範囲に

＊5）IT全般統制には、通常、情報処理センター業務、システムソフトウェアの取得と保守、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開発と保守に関する統制が含まれる。
業務処理統制は、業務処理の完全性、正確性、承認および有効性を保証する統制である。
業務処理統制が有効に機能する前提をなすのがIT全般統制であり、有効性を維持するには、相互に有機的な関連性を維持することが必要である。

＊6）内部統制の評価は、次の順に行われる。
① IT統制目標の達成評価
② IT統制の有効性評価
③ 内部統制の有効性評価

＊7）COBIT（Control Objectives for Information and related Technology）は、直訳すればIT統制目標である。その他のIT統制目標としては、ISO/IEC17799、eSAC、ITILなどがある（参考文献4、6参照）。

含める*8」

この注書きにより、ITサービスの提供を受け、そのサービスを利用して事業を運営する場合でも、外部委託した業務に関する内部統制の構築維持の責任は、業務を受託する事業者にではなく、業務を委託した企業の側にあることが明確となった*9。

したがって、委託する業務が委託企業の財務諸表に対して重要な影響を与えていると判断された場合*10、その業務は委託企業の経営者による内部統制の評価対象となる。委託企業は、現実には、業務を外部委託し代わりにITサービスを受け取っているだけで、IT統制はすべて受託事業者に依存している。このため、委託企業による内部統制評価は受託事業者に依存して実施することになろう。結果として、この注書きは委託企業のITサービスを提供する事業者へのビジネス上の要請として働くことになる。例えば、業務委託契約に、「内部統制評価に耐えられるIT統制を設置すること」という新たなサービスレベル条件が追加されることになる。

7．委託業務に関する内部統制監査

7.1　経営者による委託業務の評価

ITサービスを提供する事業者は、内部統制監査に関する規制内容を十分理解した上で、受託する業務に関して顧客ごとに適切な水準にIT統制を設置し、業務受託を開始しなければならない。受託業務のIT統制評価は、ITサービスを提供する事業者のIT統制目標の達成状況を評価するもので、定期的に、委託企業の経営者によって実施されなければならない。

このため、委託企業と受託事業者との間で、事前に次の点などで合意する必要があるだろう。

① 委託企業の経営者による内部統制評価の実施時期
② 評価手続の内容
③ 受託事業者の施設への立ち入りの権限
④ 受託事業者の協力体制

この委託企業による評価手続きは、内部統制の整備運用状況のテスト結果として文書化され、委託企業の経営者の作成する内部統制報告書の一部を構成することになる。

この内部統制報告書は、委託企業の財務諸表監査を担当する監査人によって内部統制監査が実施され、内部統制監査報告書が作成される。監査人は、必要に応じ受託業務に関する内部統制の評価状況を確認するため、受託事業者の業務実施状況を実際に検証することになる。

7.2　監査人による委託業務の評価

以上のようなプロセスを経てITサービスの保証が遂行されるのであるが、このプロセスにはやや非現実的な点がある。ITの外部委託を請け負う事業者には、複数の企業から同時に並行して、業務を受託するケースが多く存在するからである。そのようなケースでは、3月決算など多くの企業の決算が集中する時期に、委託業務の内部統制監査を一斉に実施する必要が生じ、各委託企業の外部監査人が一時期に受託事業者に往査に訪れる事態を招いてしまう恐れがある。これを解決するための監査手順としては、委託会社の監査人が別の監査人の監査結果を利用することで内部統制監査手続きの単純化を図ることが必要となる。

このようなケースを想定して、米国においてはSAS70、国内においては監査基準委員会報告第18号「委託業務に係る統制リスク評価」（以下委員会報告18号）では、システムの運用受託を行う共同データセンター業務への内部統制評価の手続きを規定している。

内部統制評価とSAS70ないし委員会報告18号とは、次のような関係となる。

① 業務を受託する事業者が外部監査人に対し自己のデータセンターでのIT統制に関するSAS70ないし委員会報告18号に基づく監査の実施を依頼する。
② 監査結果は、SAS70または委員会報告18号の監査報告書として受託企業の経営者に報告され、受託企業の経営者からさらに各委託企業に提出される。
③ 委託企業の経営者はその監査報告書の内容を検証し、妥当と判断すれば、委託業務に関する経営者による内部統制の有効性評価結果をこの監査報告書に代えることが出来る。
④ この監査報告書に対して委託企業の財務諸表監査を担当する監査人が内部統制監査を実施する。

以上の手順で留意すべき点としては、次のようなものが挙げられる。

上記②の監査報告書に関してSAS70では、タイプⅡと呼ばれる監査報告書が必要とされている。国内で委員会報告18号の適用に際してもその取り扱いを確認する必要がある*11。また、監査報告書を利用する場合には、監査報告書の監査対象期間と委託企業の会計年度が一致していることが原則

＊8）「基準案」P18

＊9）外部委託に関する取り扱いは、米国SOX法でも同様（PCAOB監査基準2号「Appendix B, para B18」参照）。

＊10）委託企業の財務諸表に重要な影響を与えるとは、委託業務の取引処理に伴う財務諸表項目が、委託企業の財務諸表の重要な勘定科目に金額的ないし質的重要性を与えることを言う。

＊11）委員会報告18号でSAS70のタイプⅡに相当する報告書は、「内部統制の整備及び運用状況報告」である。

である。一致しない場合には、必要に応じ委託企業の経営者は追加の手続きを実施する必要がある。

SAS70及び委員会報告18号は、委託企業の経営者の内部統制評価に関する責任を免ずるものではない点にも注意する必要がある。そのため、前記③の経営者による報告書の報告内容の検証手続きは必須である。この検証手続きで何らかの不足が発見された場合には、経営者は必要に応じて追加の手続きを実施しなければならない。

8．終わりに

以上本稿では、ITサービスを提供する事業者と内部統制監査との関連を、共同データセンターにおける委託業務の内部統制評価手続などを通して紹介した。2006年4月より、銀行、保険などの金融機関から業務を受託する事業者に対して金融庁の立ち入り検査が法的に可能となった。このことは、ITサービスを提供する事業者が日本経済の中核である金融機関等の事業基盤を支えているだけでなく、金融ビジネスの根幹である内部統制に重大な影響を与える極めて重要な存在であることが認識された結果といえよう。今後、ITサービスの提供とIT統制の有効性維持とは密接不可分なものとして外部評価の対象とされることに十分留意しなければならない。

［著者紹介］

深見　浩一郎（ふかみ こういちろう）
深見公認会計士事務所／コンサルティング・ネットワーク
ITAS代表
大手都市銀行を経て、国内大手監査法人マネジメントコンサルティング室長、外資系コンサルティング会社ERP担当マネージング・ダィレクター等を経て、現職。
一昨年から公認会計士、システム監査技術者、システム・コンサルタントによるネットワークITASを創設。内部統制構築､IT統制整備に関するコンサルティング・サービス、メソドロジーの教育研修を展開。

〈参考文献〉

1. COSO［1992］, *Internal Control : Integrated Framework*（鳥羽至英・八田進二・高田敏文共訳［1996］『内部統制の統合的枠組み―理論篇―』、『内部統制の統合的枠組み―ツール篇―』白桃書房）
2. *Enterprise Risk Management Framework*［2004］（八田進二監訳［2006］『全社的リスク・マネジメント フレームワーク篇』、東洋経済新報社）
3. *Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting Public Comment*［2005］, http://www.coso.org/
4. *IT Governance Institute*［2004］, *IT Control Objectives for Sarbanes-Oxley*（ISACA東京支部訳［2006］『SOX法遵守のIT統制目標』、http://www.itgi.org/）
5. 鳥羽至英［2005］、『内部統制の理論と実務』、国元書房
6. 堀江正之［2006］、『IT保証の概念フレームワーク』、森山書店