

2006年12月20日

「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（公開草案）」に対する意見並びに質問等について

J-SOX 対応促進協議会 事務局

J-SOX 対応促進協議会は、上場企業に対して内部統制に関係するさまざまなノウハウ・情報・技術・サービスなどをフラットな立場で支援する任意団体です。コンサルタント、システムベンダー、アプリケーションベンダー、セキュリティベンダー、公認会計士、不正検査士、ユーザ企業など約 60 社を会員として推進している協議会です。今回の公開草案に対して、J-SOX 対応促進協議会の会員の声を取り纏め、以下の通り 39 項目をレポート致します。

ご査収頂きご検討のうえ公開回答を賜り度くご高配のほど宜しくお願い申し上げます。

## 記

## 1. 「草案」全般に関して

- 1) 公開草案全体を通して考察しますと、網羅性をもって平易に記載されております。が一方で内容的には冗長性が非常に高く、深い見識を持たない一般の上場企業の方が理解するのは難しいようです。専門家ではなく、内部統制に対応しなければならない一般企業の方に理解をしてもらうのが第一義と考えます。このままでは別途解説書を作ることになりかねません。従って指針要点を的確に把握出来るように、例えば基準と解説と例示を明確に別立てに分けて記述して頂きたい。また重複も多いため、3 章構成についても基準編、解説編、事例編と区分するような形式など再考して頂きたいと考えます。完璧なレポートであるがゆえに理解を阻害しているのではないかと危惧しております。内部統制に対応しなければならない一般企業の視点で見直して下さい。
- 2) 金融商品取引法の第二十四条の四の四に規定された内閣府で定める体制、内閣府令で定めるところにより評価した報告書とあるが、内閣府令はいつごろ出されるのでしょうか。省令の後にガイドラインなどが出されるのが

通例だと思います。今回は何故草案が先に公開されたのでしょうか。

- 3) 実施基準に関するノンアクションレター（法令適用事例確認手続き）を活用したいと考えておりますが、対応して頂けますでしょうか。
- 4) 経済産業省は「ITに係る全般統制」について「システム管理基準」補迫としてCOBITを検討しており、来年1月には草案が公開される予定です。この経済産業省の対応と、本草案(金融庁)との連携及び位置づけを、一般企業はどのように解釈して行政の対応を受け取れば宜しいのでしょうか。
- 5) 政府全体で取り組んでいるベンチャー育成・支援の観点からも、新興市場への導入を遅らせる、または手続きを緩和するなど上場コストを低減することを継続して検討して頂きたいのですが、見解をお聞かせ下さい。
- 6) 金融商品取引法においては、内部統制報告書は「会社の属する企業集団及び当該会社に係る財務計算に関する書類その他の情報の適正性を確保するために必要な体制について評価した報告書」とされていますが、当公開草案では財務報告に係る内部統制のみの基準が掲載されています。（「財務計算に関する書類」は内部統制報告書に記載すべき内容の例示に過ぎないとの理解）。「財務報告」以外の内部統制については、別途基準が提示されるのでしょうか。
- 7) 全体的に、Ⅱ財務報告に係る内部統制の評価および報告よりⅢの財務報告に係る内部統制の監査の方が詳しいので、結果監査報酬のアップに繋がるような印象がもたれます。監査基準をもう少し緩和する方策を考慮して下さい。
- 8) 内部統制にITを利用していくことによって生じる新たなリスクを減少させるためには、まずは、情報システムの運用ログを確保しておくことが大前提となります。但し、ログ情報は電子データであるので紙文書等に比較して、「改ざんが容易で痕跡が残りにくい」あるいは「改ざんされていないことを後日証明することが困難になる」といった欠点を持つことに注意が必要です。この電子データ特有の欠点を補完するためには、「タイムスタンプ」の適用が有効です。電子署名法に基づくPKI技術と並行して時刻署名も電子化の社会では重要な技術であります。このタイムスタンプの必要性を改竄・破壊防止及び記録保存する上での適用例として記載して頂きたい。

## 2. 「内部統制の基本的枠組み」に関して

- 1) 内部統制の目的及び基本要素はCOSOをベースとしていますが、「資産の保全」、

「IT への対応」を追加した背景や理由・根拠を示して下さい。

- ① 「IT への対応」を見ると、ITEL (ISO/IEC20000) の要素が多分に盛り込まれていますが、J-SOX のポリシーから鑑み、内部統制の基準とするにはややポイントがずれ、且つ負荷がかかるように思われます。メニューに入れた真意を明示して下さい。
  - ② COSO、COBIT、ITEL、ISMS と「IT 統制」だけでも幾つかの規定が絡み合い基準が不明瞭になっていると思料しますが、IT を組み入れたそもそもの目的と要求を明示して下さい。
- 2) 「リスクの評価・対応との統合」で全社リスクの記載がありませんが記載漏れでしょうか。
  - 3) 財務報告に係る内部統制の評価の意義の中に記載されている「一般に公正妥当と認められる内部統制の評価の基準に準拠して、その有効性を自ら評価しその結果を外部に向けて報告することが求められる。」この準拠すべき基準を明示して下さい。
  - 4) 「アクセス管理」の重要性が 2、3 記載されておりますが、その意味には暗号・制御・認証のセキュリティ 3 要素が含まれております。ここで言う言葉の定義を明示して下さい。
  - 5) IT への対応についての記載ですが、早急に IT 化を推進しなければならないような誤解を招き、財務報告プロセスからは逸脱していくような危惧をします。見解をお聞かせ下さい。
  - 6) IT 統制について内部統制上、「情報セキュリティ」確保は最も重要な IT 基盤と思料しますが、内部統制の範囲に一切記載がありません。安全税・機密性・アクセス管理などの定性的な記載はありますが、「情報セキュリティ」の重要性と位置づけが明記されていません。また、電子政府・行政が推進した ISMS 取得や ISO など国際規格を考慮した基準を提示することが、企業の対応負荷を軽減することに繋がると思料しますが、ご検討下さい。
  - 7) 内部統制の限界は経営判断により、費用と便益との比較衡量を行い、内部統制の整備及び運用を行うものとされていますが、同時に税引前利益の 5%程度を超過した場合は、「重要な欠陥」とみなされ対応が求められています。費用と便益との比較衡量による「リスクの受容」について、具体的・実務的な評価への反映方法を明示して下さい。

### 3. 「財務報告に係る内部統制の評価及び報告」に関して

- 1) 財務報告に係る内部統制の評価の意義の中で「一般に公正妥当と認められる評価の基準に準拠して」とありますが、「評価基準」の具体的な指針を明示下さい。また、「一般に公正妥当と認められるは誰によって、いつ作成されるのかを明示して下さい。
- 3) 財務報告に係る内部統制の評価の意義の有価証券報告書の記載内容について記述されているが、「財務諸表の表示等を用いた記載」が、単に数値的なものを意味しているのか、個々の開示文書の文言や言い回しも含めているのか、不明瞭と思料します。もう少し解り易く明示して下さい。
- 4) 財務報告に係る内部統制の評価の意義の中の在外子会社の適用について、「所在地国に内部統制報告制度がない場合であっても、歴史的、地理的な沿革等から我が国以外の第三国の適切な内部統制報告制度が導入されている」例を示して下さい。
- 5) 財務報告に係る内部統制の評価の意義の中で、税引前利益の5%程度と例示されているが、特別損益が大きく発生した場合は、当年度に限りその分を除外して検討するのが妥当と考えられます。であれば、税引前利益でなく経常利益をベースに考えるほうがシンプルといえますが見解を示して下さい。(国際会計基準への移行を意識した記述なのであれば理解できますが)
- 6) 財務報告に係る内部統制の評価とその範囲の中で、委託会社による評価結果の利用について、委託業務に関連する内部統制の評価結果を記載した報告書を評価の代替とできるとしていますが、要件を満たしうる具体的な報告書が何であるかを示して下さい。監査第18号報告なのか、SAS70にあたるものを整備するのか、ご教示下さい。
- 7) 財務報告に係る内部統制の評価とその範囲の中の、決算・財務報告に係る業務プロセスに関して、「総勘定元帳に取引合計を入力する手続き」と例示していますが、法令対象会社の大半が経理システムで集計している中、具体的にどのような業務をイメージしているかが解りません。月次締めから記述するのか、振替処理から記述するのか、例示をもう一段具体化して下さい。また、①財務報告の範囲では、単体決算も対象となるような表記(38年大蔵省令59号)であるが、決算・財務報告に係る業務プロセスについては連結決算のみと受け取れるため、踏み込んだ記述をして下さい。
- 8) 財務報告に係る内部統制の評価とその範囲のITを利用した内部統制の評価の

中で、ITに係る全般統制の評価に関して、いくつか観点が例示されていますが、概要レベルであり、具体的に何を求められているのか解りません。『Ⅲ. 財務報告に係る内部統制の監査』の章を見ることで理解できますが、その内容を整備すべき役割が企業側にあるのか、監査人側にあるのか、示して下さい。また、役割が企業側にある場合、従来の監査人監査における IT 監査との切り分け・統合を明確化することが望ましいと思料しております。

- 9) 決算・財務報告プロセスのうち、「全社的な観点で評価することが適切なもの」は、たとえば各連結子会社の個別集計を含む連結決算プロセスと考えられますが、評価の範囲から除外された子会社についても、結局、決算プロセスそのものが対象になるのではないかと危惧しておりますが問題はないでしょうか。
- 10) 持分法関連会社は軽減案に対し、逆に強化されているため、米国同様に対象外とすることは可能でしょうか。
- 11) 外部委託業務の評価に記載されている委託業務結果の報告書の記載要件が判りません。明示して下さい。
- 12) 重要性の大きい業務プロセスについては、個別に評価対象に追加と記載されていますが、重要性の基準を明確にして示して下さい。
- 13) 重要な事業拠点の選定の中で、「例えば、本社を含む各事業拠点の売上高等の金額の高い拠点から合算していき、連結ベースの売上高等の一定の割合に達している事業拠点を評価の対象とする」とありますが、子会社が本社に製品を販売し、連結仕訳で相殺される場合どのように考えればよいのかが明確化されていません。例えば次のような例です。  
「工場で生産した製品を 100 億円で本社に販売。本社では 120 億円で外部に販売。連結ベースでは工場の販売と本社の仕入れで相殺されるため、売上高は 120 億円。一定割合を 2/3 とすると 80 億円が基準値となります。単体での売上高は本社が 120 億円、工場が 100 億円となります。この場合、本社と工場を一体とみなして、全てを対象とする考えで宜しいのでしょうか？だとすれば、当該文書の後に「なお、子会社等から商品等を購入している場合、連結仕訳で総裁がなされるが、その場合は、当該子会社等は親会社の一部とみなし、業務プロセス評価の対象とする」との趣旨の文章を挿入すべきだと思います。このようなケースはほとんどの連結グループに見られることから、指針にて明確化しないと監査の現場で混乱を招くことが予測されます。是非明確化して下さい。

- 14) ITに係る全般統制の評価の記載ですが、内部統制の基本的な枠組みと同一記載で、どの様な視点で何処までを監査するのか見えません。具体的に明示下さい。
- 15) ITの全般統制が有効であるための指針として、例えば仕様書は必須とか、テスト仕様書等で可能とか具体例を示して下さい。またその場合の運用テストのサンプル件数はどの程度と想定すれば宜しいのでしょうか。
- 16) ITの業務処理統制の運用テストはテストデータを使った結果で宜しいのでしょうか。
- 17) 財務報告に係る内部統制の評価の方法、記録の保存の中で、後日第三者による検証が可能となっているが、各文書は機密事項であるため、第三者を監査人、規制当局、捜査当局、取引所等に絞ることが望ましいと思料しますが追記記載して頂けますでしょうか。
- 18) ITを利用した内部統制の評価は、財務関連業務を離れ、企業の組織体制や情報システムマネジメントに対する評価としては理解できるが、其々の企業のおかれている環境は同じではないために、例えばIT化が進んでいない上場企業は、先ずIT化を推進しなければならない錯覚に陥り易いのではないのでしょうか。また他方ISMS等の認証取得を有する場合にはそれなりの配慮をして頂けますでしょうか。

#### 4. 「財務報告に係る内部統制の監査」に関して

- 1) 監査人は内部統制監査を行うにあたって、「監査基準の一般基準及び監査に関する品質管理基準を遵守する」としてありますが、この基準は公認会計士協会のどのレポートを参照すれば良いのでしょうか。また、「「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係わ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きについて」の一部改訂」公認会計士協会の公開レポートは本草案で採用されておりますが、実施基準草案と公認会計士協会レポートの位置づけはどのように解釈すれば宜しいのでしょうか。
- 2) 内部統制報告書の雛形及び記載事項を明示して下さい。昨年出された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」には具体的な記載がありました。これは今回の草案とどのような関係になるのでしょうか。

- 3) 内部統制監査の実施、IT を利用した内部統制の評価の検討の IT に係る業務処理統制の評価の検討について、システム設計書等を閲覧し、整備状況を確認するとされているが、既存システムで設計書が存在しない場合については、検証が不可能となってしまいます。運用評価での、本番機（または同等のテスト機）によるテスト結果の確認により、設計の確からしさを類推するほうが現実的である。例示としても、システム設計書の閲覧だけでなく、画面コピーの閲覧も追加して記述することが望ましいと思います。見解をお聞かせ下さい。
- 4) 内部統制監査の実施、IT を利用した内部統制の評価の検討ですが、End-User-Computing 自体に係る IT 統制の有効性評価については、特段有効性を評価すべきとの指摘がない。EUC に関しても設計やセキュリティの統制を求めると、本来の EUC の利点を逸失させることにも繋がるため、対象としないことが望ましいが、改善に時間を要するため監査人によるバラツキが低減されるよう、その旨を記述して頂けますでしょうか。
- 5) 運用状況の評価の実施方法（サンプル件数、サンプルの対象期間、実施時期等）の具体的な決定指針ですが、日常反復継続する取引での信頼度 90%を得るためには 25 件のサンプルが必要とあるが、その他の場合の基準を明示して下さい。
- 6) 専門家の業務の利用の中で、「公正妥当と認められる基準に準拠」とありますが、この基準の具体的な要件・内容を示して下さい。

以上