平成 19 年 12 月 14 日

日本公認会計士協会　御中

全 国 銀 行 協 会

「ＩＴに係る内部統制の枠組み～自動化された業務処理統制等と全般統制～」（公開草案）に対する意見書について

今般、標記公開草案に対する意見を下記のとおりとりまとめましたので、何卒ご高配を賜りますようお願い申しあげます。

記

１.「Ⅰ　本研究報告の目的」

経営者による財務報告に係る内部統制の評価において当研究報告をどのように活用すべきかが明示されていないため、「目的」の中に記載していただきたい。

２.「Ⅱ　財務諸表監査におけるＩＴと内部統制」

(1) 入力したデータの「自動仕訳」について

「自動仕訳」自体は、「ＩＴの利用」に該当するのか、それとも「ＩＴ業務処理統制」に該当するのか確認したい。このような例示にあたっては、業務、ＩＴの利用、重要な統制（ＩＴ業務処理統制およびＩＴ全般統制）の視点から記載していただきたい。

(2) 「企業外から接続されるデータの信頼性の確保」について

・　「企業外から接続されるデータ」に関しては、他社が作成するデータそのものについてはその信頼性につき内部統制下に置くことが不可能であることから、ここでいう「信頼性の確保」とは、自社の環境に他社データを取得した以降のプロセスに限定して言及されているものと理解してよいか。また、そうであれば、「データの信頼性」につき、自社で作成されたデータと他社データを区別する必要はないもの、と考えられることから、例示として「企業外から接続されるデータ」を採り上げることは、必ずしも適切ではないと考える。

・　「企業外から接続されるデータの信頼性を確保することが内部統制上重要となる」との記載に対する対応策が明示されていないため、明確に記載すべきである。

(3) 電子申請および電子承認について

電子申請、電子承認等を利用する場合でも、帳票への押印等が正式な承認手続とされていることはあり得るため、自動仕訳の例示と同様、「帳票への押印等、手作業による承認手続が存在しない場合」等の但書きを付記することが望ましいと考える。

(4) 「ＩＴを高度に利用した情報システム」について

情報システムにおけるＩＴ利用度の高度化と、「企業内にとどまらないグローバルな運用」及び「手作業や人の判断を伴わない処理の自動化」との因果関係を明示する事実が存在するのか疑問。仮に明示された事実を伴うものではないとすると、「企業内にとどまらないグローバルな運用」や「手作業や人の判断を伴わない処理の自動化」は、ＩＴの利用度合いの如何によらず、個々の企業の特性や経営方針・様式等に応じその程度が異なるものと考えられることから、当該記載は削除されるべきと考える。

３．「Ⅲ　自動化された業務処理統制等」

(1) 「１．自動化された業務処理統制等の意義」について

・　「財務報告に係る内部統制」という観点から評価対象とすべき業務処理統制は、あくまで財務報告に関連するものであり、その意味において、「業務処理統制」と「会計処理手続」の区分けは必ずしも明確ではない。金融機関等、通常の業務処理が会計処理に直結している業種も存在することを勘案し、「自動化された業務処理統制」と「自動化された会計処理手続」を区分する（「自動化された会計処理手続」が「業務処理統制ではない」とする）ことの意義につき、改めてご検討いただきたい。

この点、「手作業の統制に利用されるシステムから自動生成された情報」については、監査法人によっては、関連する「手作業の統制」と一体で捉えて「ＩＴ依存統制」という業務処理統制の一形態とする手法も存在するほか、当該情報の自動生成プロセスそのものについても、「自動化された業務処理統制」「自動化された会計処理手続」との差異を見出すことは困難である。

(2) 「２．自動化された業務処理統制等と全般統制」

①「(1) 自動化された業務処理統制の意義」

例示された「エディットチェック機能」が、財務報告の有効性に係る重要な

統制と認識される場合は必ずしも多くないと考えられることから、「自動化された業務処理統制」の例示につき、再考されることが望ましいと考える。

②「(5) 自動化された業務処理統制等の例」について

・　例示された「画面入力時のプルダウンメニュー」が、財務報告の有効性に係る重要な統制と認識される場合は必ずしも多くないと考えられることから、「自動化された業務処理統制等」の例示につき、再考されることが望ましいと考える。

・　アプリケーションレベルのアクセス制限（「端末メニューの制限」）については、監査法人によっては、ＩＴに係る全般統制の一環として評価する手法が存在することを踏まえ、監査実務における混乱を回避する観点から、「自動化された業務処理統制等」の例示を行う際には、両論併記とする等の配慮につき、改めてご検討いただきたい。

４．「Ⅳ　全般統制」

(1)「１．意義」について

・　全般統制は、「会計期間を通して有効であることが必要」とあるが、期中、システムに変更があった場合、当該評価対象年度におけるＩＴ全般統制の有効性評価は、変更前と変更後の両方のシステムが対象となるのか確認したい。

　会計期間のＩＴ統制は、業務プロセスと同様にすべての期末日の財務諸表に当然、反映するものであると認識するが、財務報告に係る内部統制の評価時点は、あくまでも期末日であることと、会計期間中に不備を修正した場合の関連性について明確にしていただきたい。

(2)「２．全般統制の適用範囲」について

①　「(2)」柱書きについて

　本項は企業が単一のシステム基盤を利用していることを前提とした記載とみられるが、複数のシステム基盤（ホスト系／分散系、等）が混在する企業が相当数存在することを勘案し、例えば「全般統制はシステム構成により主となる統制活動が異なってくるため」と変更する等、再考されることが望ましいと考える。

②　ホスト系システムを利用している場合の全般統制の例示について（「(2)

①」）

ホスト系システムに関しても、ホスト機ないしデータセンターへの物理的アクセスや、（アプリケーションレベルのアクセス制限を「全般統制」として捉える場合）職務権限に応じたユーザＩＤの付与・管理状況等、「プログラムとデータの情報セキュリティ管理」は評価対象として重要なものであると考える。

③　「ネットワーク全体の運用・管理」について（「(2)③」）

・　「ネットワーク全体の運用・管理」に関し、どのような統制活動を想定しているのか、具体的に例示していただきたい（アプリケーション、ＯＳ・データベース、及び物理的セキュリティに係る統制とは求められる内容・水準が大きく異なるものと考えられる）。

・　ここでは、イントラネット（企業内ネットワーク）ではなく、インターネットのことを言っていると思われるが、インターネットは世界共通のネットワークであり、企業集団の統制外の部分である。企業集団が主体的にコントロールできない事項におけるリスク軽減・回避のためには、例えばインターネット上を流れるプログラムやデータは通信をＳＳＬで暗号化するなどの対策を施すといった、「５.具体的例示 (4)プログラムとデータの情報セキュリティ管理」の対応をするのであって、「ネットワーク全体の運用・管理」では無いと考える。

例えば、「ネットワーク全体の運用・管理まで一体とした」を、「企業集団の統制外のネットワークを流れるプログラムとデータの情報セキュリティ管理を含めた」とすることが考えられる。

・　本項については、「(2)②」と併せて次のとおり記載することも考えられる。「ＷＥＢアプリケーション、クライアントサーバ型アプリケーションでは、所謂、従来型ホスト系システムとは異なるＩＴ統制（の観点）が必要である。

例えば、個々のアプリケーションシステムに対する全般統制だけでなく、これらを包括するシステムまで一体とした統制活動として全般統制の対象となるケースや、ＩＴ専門部署以外のユーザー部署が全般統制の対象となり、当該部署が全般統制対象システムを所管するケースがある。」

④　「企業外に開かれた接続環境が実現されている場合」について（「(2)④」）

・　「企業の支配力が直接及ばない範囲も管理の対象として考慮する」ことは、内部統制の評価とは相容れないものと考える。「企業外における全般統制の適用状況が全般統制の範囲となる可能性がある」とあるが、どのような範囲のどのような統制活動の適用状況を想定されているか、具体例を示していただ

きたい。

契約に基づくシステム開発・運用や情報処理等に係る外部委託については、当該契約の範囲内で、当該企業の支配力が及ぶ範囲にあるもの、と理解されることから、当該企業のＩＴに係る内部統制として当然、評価対象とすべきであるし、また評価可能であるものと考えられるが、顧客からの発注情報データ伝送で受け付ける場合等は、当該企業の内部統制によりデータの誤発信等を防止することは不可能である（情報の正誤によらず、当該発信情報をあるがままに受信することを担保するのが、当該企業の内部統制である、と考えるべきである。）外部委託に関する記載が別途存在することも勘案し、本項については削除すべきと考える。

・ 「企業外に開かれた接続環境」とは通信事業者の通信ネットワークであり、当社企業集団の統制外の部分である。企業集団が主体的にコントロールできない事項におけるリスク軽減・回避のためには、例えば入力されたデータは削除できなくし、タイムスタンプを取り、入力者による事後の否認を防止するなどの対策を施す、あるいは、出力されたデータはコピーを取り、出力先を記録し、タイムスタンプを取り、出力者による改ざんに対抗するなどの対策を施すといった、「５.具体的例示 (4)プログラムとデータの情報セキュリティ管理」に例示を追加するべきことであって、「企業外における全般統制の適用状況」では無いものと考える。

例えば、「企業外における」を「プログラムとデータの情報セキュリティ管理を含めた」とすることが考えられる。

・ 「ＥＤＩ」は、一般的な用語ではないと考えられるため、用語の解説が必要と考えられる。

(3)「３．全般統制のリスク評価」について

企業会計審議会「財務報告に係る内部統制の評価及び監査の基準」では、「内部統制とは、基本的に、業務の有効性及び効率性、財務報告の信頼性、事業活動に関わる法令等の遵守並びに資産の保全の 4 つの目的が達成されているとの合理的な保証を得るため～」とあり、また「IT への対応は、内部統制の他の基本的要素と必ずしも独立に存在するものではない」とされていることから、「全般統制のリスク評価においては、財務情報に直接関わるリスクではなく」という記述には違和感がある。

「財務情報に直接関わるリスクではなく」を「財務情報に直接関わるリスクに止まらず」という表現に修正することを検討していただきたい。

(4) 「４．統制目標」について

２段落目の「リスクの軽減、リスク対応すべく検討すれば、全般統制の統制目標は次のようなものである」は修正する必要があると思われる。

(5) 「５．具体的例示」について

① 「(3) コンピュータの運用管理」について

・ 「コントロールトータル」は、一般的な用語ではないと考えるため、用語の解説が必要であると考える。

・ エラー処理、リカバリー処理は、プログラムに組み込まれるべきものであれば、「コンピュータの運用管理」よりも、「プログラムの開発」または「プログラムの変更管理」に該当すると考える。

② 「(4) プログラムとデータの情報セキュリティ管理」について

監査法人によっては、アプリケーションレベルのアクセス制限についても、ＩＴに係る全般統制の一環として評価する手法が存在することを踏まえ、監査実務における混乱を回避する観点から、「プログラムとデータの情報セキュリティ管理」の例示を行う際には、両論併記とする等の配慮につき、改めてご検討いただきたい。

(6)「７．全般統制に不備が存在する場合」について

「不備がある場合」という概念の説明が「有効に整備されていない場合」や「有効に運用されていない場合」であるため、表現を、「全般統制に不備がある場合、即ち、有効に整備されていない場合、あるいは有効に運用されていない場合には、」と改める方が適切であると考える。

(7) 「８．全般統制に変更があった場合の有効性検証の意味」について

・ ロールフォワードテストの実施が必要となる「全般統制の重要な変更」及びロールフォワードテストにおける評価方法につき、そのレベル感を具体的に例示していただきたい。

・ 「そのため、全般統制の有効性の評価は毎期実施する必要な場合が多い」は、表現を修正する必要があると思われる。

(8) 「９．エンドユーザーコンピューティング（ＥＵＣ）とスプレッドシート」

について

① 「管理が十分に行き届かないようなＥＵＣ及びスプレッドシート」について

上記記載は、具体的な事実に基づくものであるのか確認したい。仮に、具体的な事実に基づくものではないとすると、上記記載は削除されるべき（または見直されるべき）と考える。

② 「ＥＣＵにおいて自動化された業務処理統制等が高度に利用されている場合」について

業務処理統制等が「高度に利用されている」ことの具体的な基準（例示）を明示していただきたい。

（9） 「10. 外部委託業務にかかる全般統制の有効性の評価」について

本項の「内部統制評価に関する報告書」は、ＳＡＳ70 や 18 号報告を指しているのか確認したい。

また、委託者が「内部統制評価に関する報告書」が入手できない場合は、委託者はどのように全般統制及び自動化された業務処理統制等の内部統制の有効性を評価すればよいのか明示していただきたい。

以　上