ＩＴ委員会研究報告第 42 号

ＩＴ委員会実務指針第６号「ＩＴを利用した情報システムに関する重要な虚偽表示リスクの識別と評価及び評価したリスクに対応する監査人の手続について」に関するＱ＆Ａ

平成 24 年６月５日
日本公認会計士協会

－目　　次－

Ⅰ　はじめに

日本公認会計士協会は、監査基準委員会の新起草方針に基づく最終報告書の公表に合わせて、平成 23 年 12 月 22 日付けでＩＴ委員会実務指針第６号「ＩＴを利用した情報システムに関する重要な虚偽表示リスクの識別と評価及び評価したリスクに対応する監査人の手続について」（以下「ＩＴ実６号」という。）を公表した。

ＩＴ実６号は、監査基準委員会報告書 315「企業及び企業環境の理解を通じた重要な虚偽表示リスクの識別と評価」（以下「監査基準委員会報告書 315」という。）及び同 330「評価したリスクに対応する監査人の手続」（以下「監査基準委員会報告書 330」という。）を適用するに当たり、重要な虚偽表示リスクに関してＩＴに関する手続をどのように実施すべきかについて記載している。本研究報告はそのＱ＆Ａとして作成したものである。

Ⅱ　総論

Ｑ１：システム監査、情報セキュリティ監査等の結果を財務諸表監査の一環として行う重要な虚偽表示リスクの評価に代替すること、または、財務諸表監査の一環として行う情報システムに関する重要な虚偽表示リスクの評価をシステム監査、情報セキュリティ監査等として利用することはできますか。

Ａ１：

システム監査、情報セキュリティ監査等の結果を、財務諸表監査の一環として行う重要な虚偽表示リスクの評価に代替することはできません。財務諸表監査の一環として行う重要な虚偽表示リスクの評価と、例えば、システム監査（「システム監査基準」「システム管理基準」（平成 16 年 10 月 経済産業省公表））、情報セキュリティ監査（「情報セキュリティ管理基準（平成 20 年改正版）」（平成 20 年経済産業省告示第 246 号）及び「情報セキュリティ監査基準」（平成 15 年経済産業省告示第 114 号））等とはその目的も責任範囲も異なるため、監査人は、重要な虚偽表示リスクの評価を行う上では関与先に対して誤解や期待ギャップを与えないよう、十分に配慮する必要があります。

最近、情報セキュリティや個人情報保護に関する社会的関心が高まり、監査人に対し、情報セキュリティ監査やＩＳＭＳ構築・認証、さらに、情報セキュリティ検証業務（ＩＴ委員会研究報告 39 号「情報セキュリティ検証業務」参照）、プライバシーマーク取得に必要な審査など第三者に対し情報セキュリティなどを保証して欲しいというニーズが高まりつつあります。

監査人が財務諸表監査の一環として行う情報システムに関する重要な虚偽表示に関するリスク評価手続及びリスク対応手続を実施するだけではシステム監査や情報セキュリティ監査に相当する意見表明はできないため、誤解や期待ギャップが生じないように留意する必要があります。

監査人が財務諸表監査において重要な虚偽表示リスクの評価を実施したとしても、監査人は、内部統制自体の信頼性・有効性に関して意見を表明しません。同様に、監査人が財務諸表監査の一環として、ＩＴを利用した情報システムに関するリスク評価手続及びリスク対応手続を実施したとしても、監査人は、ＩＴを利用した情報システム自体の信頼性・有効性に関して意見を表明しません。

なお、システム監査、情報セキュリティ監査等を行う場合には、「独立性に関する指針」、独立性に関する法改正対応解釈指針第４号「大会社等監査における非監査証明業務について」等を参照して監査人としての独立性の問題が生じないように留意します。

Ⅲ　監査計画の策定に当たってのＩＴに関する留意事項

Ｑ２：「ＩＴの利用に関する概括的理解」の位置付けについて教えてください。

Ａ２：

１．「ＩＴの利用に関する概括的理解」とは

ＩＴ実６号第４項に記載されているとおり、「監査計画の策定に際して、以下の判定をすることが可能となる程度に重要な構成単位のＩＴの利用に関する環境を理解し、重要な虚偽表示リスクの評価の対象とするＩＴを把握する。」ことが「ＩＴの利用に関する概括的理解」となります。

- ＩＴの利用度
- 情報システムの安定度
- 情報システムの前年度からの重要な変更
- 過年度の監査におけるＩＴに関連する内部統制上の不備

企業におけるＩＴの利用状況と重要な虚偽表示に関する潜在的リスクとの関係は必ずしも一様ではないため、上記の４つの点を総合的に判断した結果、ＩＴの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低いと監査人が判断できる場合があります。この場合、監査人はＩＴに関連する内部統制を評価せずにリスク対応手続を行うこととなり、内部統制の理解におけるＩＴに関する詳細な理解を省略することが可能となります。ただし、ＩＴに依存した内部統制に依拠する場合には、ＩＴに関する詳細な理解を省略することはできない点に留意します。

なお、グループ監査における重要な構成単位に対して実施しなければならない「ＩＴの利用に関する概括的理解」は、ＩＴの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低いか否か、及びＩＴの専門家を参画させるか否かを判断することができる程度の理解です。

２．「ＩＴの利用に関する概括的理解」の位置付け（内部統制の理解との関係）

ＩＴの概括的理解は内部統制の理解の中に含まれるものです。ＩＴの概括的理解を行うに当たっては、ＩＴの利用度は企業によりかなり異なることから、まず、「ＩＴの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低い場合」に該当するか否かを把握することを行います。該当しない場合は、さらに内部統制の理解においてＩＴに関する詳細内容を理解しますが、該当する場合には、ＩＴに関する内部統制の理解におけるＩＴに関する詳細な理解を省略することが可能です。

「ＩＴの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低い場合」における、その後省略可能なリスク評価手続とは、具体的には概括的理解を除いたＩＴに依存した内部統制の理解及び評価に関する手続です。会社がデザインしている内部統制のうちどれを監査上利用するかは、監査人の判断に委ねられています。例えば、ＩＴの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低い場合、ある業務プロセスあるいは勘定について、業務処理統制を利用しないで必要十分な監査手続が行えると監査人が判断した場合、つまり手作業による内部統制のみを評価対象とすれば必要十分であると判断した場合には、概括的理解を除き、ＩＴに依存した内部統制の詳細な理解及び評価に関する手続は行う必要がなくなります。したがって、このような場合には、全般統制及び業務処理統制を詳細に理解する必要はなくなるとともに、統制環境の中のＩＴにかかわる部分も概括的理解以上には理解する必要もなくなります。ただし、その後、手作業による内部統制に関するリスク評価手続を実施した場合に、ＩＴに関する潜在的リスクが十分に低いという評価を見直す必要があることが判明する場合もあることに留意します。

これらをまとめると以下の表のようになります。（ＩＴ実６号第５項より引用）

	リスク評価手続	
	「Ⅳ　１．ＩＴの利用に関する概括的理解」	「Ⅴ　内部統制を含む、企業及び企業環境の理解」以降
ＩＴの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低い場合	リスクの判定のため必須	ＩＴに依存した内部統制の理解と評価に関する手続について省略することが可能
ＩＴの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低くない場合	リスクの判定のため必須 ただし、継続監査において「Ⅴ　内部統制を含む、企業及び企業環境の理解」を実施する際に、ＩＴの利用に関する概	必須（「Ⅳ　１．ＩＴの利用に関する概括的理解」の内容を包含する。）

	括的な理解の内容を包含して実施する場合には、「Ⅴ　内部統制を含む、企業及び企業環境の理解」と一体として実施できる。	

Ｑ３：ＩＴの利用度は、どのように判定すればよいか教えてください。

Ａ３：

ＩＴ実６号第５項に例示されているＩＴの利用度が低いと判断される状況に留意して、個別企業ごとにＩＴの利用度が低いか否かを監査人が判断します。

１．業種及び企業規模

・　金融機関等、一般にＩＴの利用度が高いと想定される業種に該当しない。

・　企業規模が比較的小規模である。

具体的には、例えば、金融機関であれば、一般にＩＴの利用度が低いといえることは稀であると考えられます。多くの上場企業についても、ＩＴの利用度を低いと判断することは難しいと想定されます。また、販売高、取引件数、従業員数等の企業規模に係る指標から、ＩＴ利用度について判定することが可能な場合もあります。

２．会計及び関連する業務システムの概要

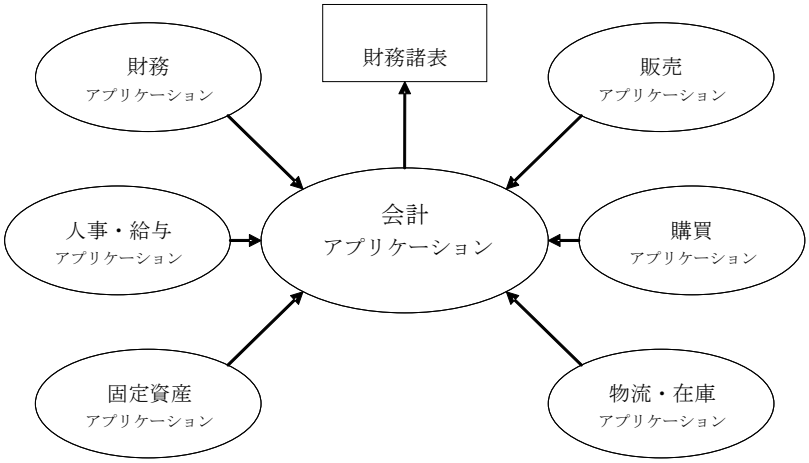
・　複雑なシステム処理がない。

・　内部統制において自動化された内部統制ではなく手作業による内部統制により重点を置いている。

・　情報システムが、市販の簡易なパッケージ・ソフトウェアのみで、パッケージ・ソフトウェアをカスタマイズせずに、ほぼそのまま使用している。

・　アプリケーション間のインターフェイスも限定的であり、アプリケーションの構成が複雑でない。

具体的には、まずは財務諸表作成に関連する会計アプリケーション及び販売アプリケーション等の業務アプリケーションとの連携イメージなどを把握します。



会計アプリケーションについては、市販の簡易なパッケージ・ソフトウェアのみで、パッケージ・ソフトウェアをカスタマイズせずに、ほぼそのまま使用しているか否かなどを判定します。

会計取引に係る主要な業務アプリケーションについては、アプリケーション名、所管部門、外部接続・インターネット接続の有無、会計アプリケーションとの連携などを概要把握してまとめることにより、アプリケーション間のインターフェイスが限定的で、システム構成が複雑でないといった判定をします。

例えば、金融システムやインターネットを利用した取引システムを運用しているような場合は、ＩＴの利用度は低いとはいえない場合がほとんどであると考えられます。また、主要システムを自社開発しているような場合にも、ＩＴの利用度は低いとはいえないことが多いと考えられます。ＩＴ関連及び内部統制に関する責任者から、情報システム組織の規模・要員数、システム関連予算の規模などの情報を入手することも、システム処理の複雑性、自動化された統制の有無といった、ＩＴの利用度を判断する上で効果的な場合があります。

３．その他

・　その他、システムの使用状況が低い（例えば、ペーパーレスの状況、電子帳簿保存法への対応の有無等を考慮する。）。

具体的には、電子商取引の有無、日常業務で発生する取引証ひょうの電子的データ(ペーパーレス)保存の有無、電子帳簿保存法への対応の有無を把握し、有りの場合であってもその内容についてシステム使用状況が低いと判断できるか検討します。

例えば、自動受注や自動発注のような会計的な影響を有する自動処理の有無、販売アプリケーション等のサブシステムから会計アプリケーションにデータを受け渡して自動的に仕訳を生成する機能の有無、主要システムにおける電子承認ないしはワークフロー（業務書類回付の自動化など）の機能の有無、電子商取引を利用した会計取引の有無等に留意します。上記の１．から３．は例示であり、上記の状況に係る事項を把握するだけで「ＩＴの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低い場合」に該当するかどうかを判断できる場合もありますが、もっと幅広く把握しなければ判断できない場合もあることに留意します。例示されている「ＩＴ判定チェックリスト」（付録１）を利用することも判定方法の一つです。

Ⅳ　内部統制を含む、企業及び企業環境の理解

Ｑ４：開発中のシステムについても重要な虚偽表示リスクを評価するのでしょうか。

Ａ４：

開発中の情報システムに関する重要な虚偽表示リスクの評価についても、他の監査対象項目と同様に、財務諸表全体レベル及びアサーション・レベルの二つのレベルでのリスクを識別し評価することが必要となります。具体的には、主として以下の３点が挙げられます。

- 新たな情報システムが、企業の採用する会計方針に合致したものであるか（会計方針に沿った会計処理の機能が当該システムに適切に盛り込まれているか等）。
- 新たな情報システムによって、重要な虚偽表示リスクへどのような影響があるか（適切な職務分掌の設定や、業務処理統制及び全般統制の整備・運用状況等）。
- ソフトウェアの会計処理を適切に行うための内部統制が整備されているか。

一方、監査対象期間中は開発が完了せず、業務プロセスにおいて利用される見込みもない場合は、監査対象期間において財務諸表に影響を及ぼすリスクは３点目に限定されることになると思われます。

しかしながら、翌期以降に利用されることが予定されている情報システムについて、情報システムの開発が終了し実際に稼動してからではなく、企画段階又は開発段階から監査人が評価し、財務諸表に重要な影響を与える可能性のある不備があれば、是正を求めることが重要となります。そのためには、監査人が開発計画を把握できるように、情報システムの開発、改変に関する内部統制を評価しておかなければなりません。

１．経営者のＩＴに関する理解と認識

企業が情報システムの新規開発や大幅な改訂を行う場合には、経営者のＩＴに関する理解と認識が内部統制に重要な影響を与えることになります。例えば、経営上の効率性（又はコスト削減）を経営者が優先するため、財務諸表を作成する上で必

要とされる重要な統制活動が設定されない、あるいは、財務諸表監査上必要なデータが入手できなくなるといったことが起こり得ます。

２．情報システムに関する企画・開発・調達業務の統制活動

情報システムに関する企画・開発・調達業務では、監査人は、情報システムの新規開発や市販のパッケージソフトの導入、及び情報システムの運用・管理のための内部統制が整備・運用されているかについて検討します。

企業が、情報システムに適切な内部統制を組み込むためには、企画・開発・調達段階で組み込むべき内部統制の内容を検討します。企業が情報システムに関する企画・開発・調達の過程を適切に管理していない場合には、完成した情報システムの信頼性が監査上期待される水準に達していないことがあります。具体的には、ユーザ部門の企画段階からの参画による要件定義や開発期間における十分なテストの実施、適切なプログラム等の移行・変更管理が十分に行われていない場合、情報システムの信頼性に影響を及ぼします。

また、ビジネスプロセスにおけるルールや会計処理の方針と、情報システム上での処理とが合致していない場合には、内部統制の不備が生じる可能性があります。例えば、出荷基準で売上を計上する企業で、出荷の事実ではなく出荷予定をもって出荷があったものとみなすようなシステムや、検収基準で売上を計上する企業が出荷をもって売上を計上するようなシステムを構築してしまった場合には、売上計上に重要な影響を及ぼすことがあります。

さらに、企業は、情報システムに関する企画・開発・調達業務を、情報投資の計画に沿って実施する必要があります。企業が統一性を欠く情報システムの導入を行った場合には、監査人は、各基幹システム間のデータの受渡しに支障が生じ、データの不整合を招くなど、会計データの信頼性を損なうことがあり得ることに留意しなければなりません。

３．ソフトウェアの会計処理との関係

社内利用ソフトウェアを自社で開発し、それを資産計上する場合には、資産性の判定と資産計上開始時期、資産計上終了時期を把握します。そのためには、開発に関する内部統制が整備・運用されていることが前提です。会計制度委員会報告第12号「研究開発費及びソフトウェアの会計処理に関する実務指針」第12項及び13項にある例示は、開発に関する内部統制の例示でもあります。

Ｑ５：ＥＲＰが利用されている際のリスク評価手続及びリスク対応手続における留意点はどのようなものでしょうか。

Ａ５：

ＥＲＰ（Enterprise Resource Planning）は、通常、自社開発よりも主に統合型パッケージとして販売されているものをイメージしますが、本来は企業の事業経営資源の活用を最適化する目的で、組織横断的にビジネスプロセスを把握するためのアプリケーションを意味しています。市販されているＥＲＰは統合業務パッケージとして、基本的にその機能に企業の業務を合わせることにより業務自体の効率化を実現しようとするものです。このようなＥＲＰについての主な留意点は以下のとおりです。

１．業務処理統制の観点

(1) 企業が使用しているパッケージの種類と特徴を理解します。ＥＲＰには、高度にシステム化された統制機能が織り込まれているものから、統制機能があまり考慮されていないものまで多種多様なものがあります。このため、監査人は、そのＥＲＰに組み込まれている統制機能を、その特性に留意して把握します。なお、ＥＲＰパッケージを利用している場合であっても、カスタマイズにより独自の仕様のプログラムが付加された部分については、当該ＥＲＰパッケージ固有の機能として織り込まれている統制機能は存在しません。したがって、当該部分についてはＥＲＰパッケージ固有の機能に応じた手続ではなく、自社開発のシステムと同様の評価手続を検討します。

ＥＲＰの場合には、ユーザマニュアルがあってもそのアプリケーションの仕様の説明が明確でない場合があります。こうした場合には、ＥＲＰの開発・販売企業に監査人が直接質問をすることが可能ならば、必要な設定について質問を行う、そして、実際にあるべき内部統制を想定して、ユーザの使用する画面を実際に試行しながら検証するなどの手続を実施することになります。

(2) ＥＲＰには、上述のとおり内部統制に関して、事前にシステム化された統制機能が組み込まれています。しかしながら、企業がＥＲＰに組み込まれたそれらの統制機能を、その設計時に想定されたデザインどおりに利用していない可能性もあります。例えば、在庫データに関して、デザイン上は入出庫の取引の発生と同時にアプリケーションに入力することで、物や金の動きとデータを一致させて企業の経営資源の動きを瞬時に把握して適正な経営資源の配分を実現するという目的で設計されたアプリケーションを、出庫データは出庫時に逐次入力する一方、入庫データは週次でまとめて入力しているような場合は、入庫の入力が完了するまでは在庫がマイナス残高で計上されるといった状況が生じる可能性があります。

(3) ＥＲＰでは、一つの取引に対して１回の入力で販売・購買といった業務プロセス上のデータも会計データも同時に作成される仕組みとなっていることが本来の姿です。このため、例えば、リアルタイムの残高とは別に、ある一定時点の残高を持つことができない設計のＥＲＰパッケージを使用すると、取引が発生する都度リアルタイムで会計データの残高も書き換えられてしまいます。そのため、

棚卸実施時点の会計データを別途保管しておくなど、ある一定時点の残高の管理がどのように行われるかを監査人として理解します。

また、業務の取引データがリアルタイムで会計データに反映されることを原則とするということは、会計アプリケーションと連携する業務システムのデータインプットの正当性、網羅性、正確性などの確保の検証を行います。この際に自動仕訳がどのように生成されているか、貸借の一致の統制機能についても留意します。

(4) ＥＲＰのモジュールをすべては利用せず会計のモジュールだけを利用している等の場合、会計処理以外で利用しているアプリケーションから会計データをＥＲＰに転送するなどの処理が行われていることがあります。この際に、会計処理以外で利用しているアプリケーションの処理データと転送処理後のＥＲＰデータとの間で差異が発生するリスクがあるため、企業が当該リスクに対してどのような統制をデザインしているかを理解します。

２．全般統制の観点

(1) ＥＲＰパッケージの標準機能に対して企業の業務に応じて数値等による設定を行うことがあります（いわゆるパラメータ設定）。この場合、全般統制の観点ではパラメータ設定に関して企業の業務に適合した値となるよう、テスト、承認、事後検証等の管理手続が取られているかを検証することが重要となります。

(2) ＥＲＰパッケージの標準機能では企業の業務に十分に対応できないような場合には、追加機能として独自の仕様のプログラムをＥＲＰに付加することがあります。このような追加機能に関しては、自社開発のアプリケーションに関する全般統制の検証手続と同様の手続が適用されることとなります。

Ｑ６：「内部統制を含む、企業及び企業環境の理解」におけるＩＴインフラの概要、アプリケーションの構成についての留意点はどのようなものでしょうか。

Ａ６：

「内部統制を含む、企業及び企業環境の理解」として監査人はＩＴの統制環境を理解し、アプリケーションの構成だけでなく、それを支えるＩＴインフラの概要を合わせて理解することとされています。

ＩＴ実６号第22項に記載のアプリケーションの構成及び第23項に記載のＩＴインフラの概要の各項目について、留意点を挙げると以下のようになります。

１．アプリケーションの構成についての留意点（ＩＴ実６号第22項）

取引の発生から財務諸表の作成に至るまでの会計処理過程のうち、情報システムが関与する部分を識別するために、監査人は、導入されている会計アプリケーション、及び販売、購買、物流といった業務アプリケーションの構成を、例えば、アプ

リケーション一覧表を作成した上で、以下のような観点から把握します。これらは業務処理統制を把握する際の基礎となるものです。

＜アプリケーション一覧表の項目例＞アプリケーション名、対象とする業務プロセス、関連する勘定科目、形態（パッケージ／ＡＳＰ／自社開発等）及びパッケージ名、アプリケーションオーナー、ユーザ部署、処理する取引規模（トランザクション量等）、ハードウェア・ＯＳ・データベース・ネットワーク　他

(1) アプリケーションの対象となる業務や取引種類を把握する際、自動化されている機能だけではなく、手作業による部分とＩＴシステムの利用により実現している機能の範囲、相互の接点などに留意します。

(2) データの流れを把握するため、以下に留意します。

・　アプリケーションで使用される主要なマスター･ファイル（顧客、商品他）と取引ファイルの全体イメージ

・　主要な入力原票及びデータ、主要な出力帳票等を把握し、アプリケーションに入力されるデータと、どのデータに基づいて帳票が出力されるかに留意します。さらに、監査上使用している帳票やファイルが、どのアプリケーションから、どのようなデータに基づいて出力されたものかを理解することは必須となります。

(3) アプリケーション間のインターフェイスについてアプリケーション間で授受されるデータの内容、タイミング・頻度等に留意します。データ授受の際のチェック方法を業務処理統制として把握することになります。

２．ＩＴインフラの概要についての留意点（ＩＴ実６号第 23 項）

ＩＴ環境を理解する目的は、重要な虚偽表示リスクの評価の過程で、内部統制の整備・運用状況を評価するための基礎情報を得ることです。監査人は、ＩＴインフラの概要の把握を基に、内部統制の整備・運用状況を評価する計画を立案し、評価対象、往査場所、重点項目の選定を行った上で、監査手続を検討します。

(1) ハードウェア構成

使用しているハードウェアのメーカー、モデル、数量、設置場所に関する情報を入手します。これらの情報から情報システムとその関連業務の規模や、セキュリティや運用管理の導入状況等をある程度推測することができますので、監査計画を立案するための基礎資料となります。

(2) システム・ソフトウェア構成

使用しているオペレーティング・システム（ＯＳ）、ミドルウェア、開発言語・ツール、アクセス管理用ソフトウェア、運用管理用ソフトウェア、データベース、各種ユーティリティソフトウェア等の情報を入手します。なお、ハードウェアと

基本ソフトウェアがセットで導入されている場合も多く、両者を合わせて把握します。

(3) ネットワーク構成

ネットワークの形態や使用回線の種類、接続場所に関する資料を入手します。これらは、データの流れや端末の設置場所、利用部門を把握するときにも有効です。社内だけでなく、取引先に注文・照会用の端末が設置されている場合や、インターネットを介して注文・取引等の情報の入力等が行われている場合には、それに対応した内部統制を検討します。

Ｑ７：ＩＴ管理に関連する業務のウォークスルーとは、具体的にどのような手続ですか。

Ａ７：

一般にウォークスルーとは、財務報告目的の情報システムにおいて、取引の開始から財務諸表に反映されるまでを追跡することをいいます。ＩＴ管理に関連する業務が財務報告に関連する取引を処理することは通常なく、全般統制の統制活動が特定のアサーションと直接関係することもありませんが、業務及び全般統制の理解の一環として、業務フローの開始から完了までを追跡することがあり、全般統制のウォークスルーとはこの手続を指します。

例えば、コンピュータ・プログラムの変更であれば、ユーザ部門での変更依頼書の起票に始まり、システム部門での受入れ、プログラムの変更、テストの実施、本番移行に至る一連の業務フローを追跡することがウォークスルーとなります。

ＩＴに関する重要な虚偽表示リスクと、関連する統制活動を適切に理解するには、ＩＴ管理に関連する業務の全体を理解することが重要であり、ウォークスルーはそのための主要な手続の一つです。

一般的な意味でのウォークスルー同様、全般統制のウォークスルーについても、実施事項には以下のような項目が含まれます。

- 規程、業務マニュアル等の閲覧
- 責任者、担当者への質問
- 関連証ひょうの閲覧、照合
- 統制活動実施状況の観察

Ｑ８：業務プロセスがＩＴ化されている場合、ウォークスルーの実施上留意すべき点は何かありますか。

Ａ８：

ＩＴ化された業務プロセスには、ＩＴの利用により自動化された統制活動が存在します。したがって、業務プロセスがＩＴ化されている場合は、手作業による統制活動

と自動化された統制活動を一体で理解することが重要となります。

そのためには、ウォークスルーの実施において、書類や手作業の流れを追跡するだけではなく、データの入力から帳票の出力までのシステム上のデータの流れについても追跡しなければなりません。ウォークスルーの実施時に、ＩＴの専門家を参画させることでより理解が深まることもあると考えられます。

なお、業務プロセスのウォークスルーは、通常は業務の主管部門、実施部門にて実施しますが、システム上のデータの流れについては、業務の主管部門、実施部門では確認できないことが多く、その場合別途システム部門への確認することとなる点に留意します。

システム上のデータの流れを追跡するには、以下のような事項を実施します。

- 業務担当者への質問
- システム部門担当者への質問
- データフロー図やシステム仕様書の閲覧
- ユーザマニュアルの閲覧
- 入力原票と出力帳票の照合

Ｑ９：コンピュータ利用監査技法（ＣＡＡＴ）の留意点はどのようなものですか。

Ａ９：

１．コンピュータ利用監査技法(ＣＡＡＴ)とは

コンピュータ利用監査技法（以下 Computer - Assisted Audit Techniques の略称として「ＣＡＡＴ」という。）とは、監査のツールとして、コンピュータを利用して監査手続を実施するための技法（ＩＴ実６号第３項(5)）であり、監査手続の有効性及び効率性を改善することが可能となります。ただし、ＣＡＡＴを利用することがＩＴを利用した情報システムに関する重要な虚偽表示リスクに対するリスク評価手続及びリスク対応手続を実施したことになるものではないため、その利用に当たってはどのような重要な虚偽表示リスクに対するリスク評価手続及びリスク対応手続として利用するかを、実施前に明確にしておかなければならないことに留意します。また、ＣＡＡＴは、その利用方法によって業務処理統制のテスト手法（Q21 参照）及び実証手続のテスト手法（Q31 参照）いずれにも利用されることが考えられます。

ＣＡＡＴは手続を実施するために必要なコンピュータ・プログラムと被監査会社におけるデータにより構成されます。

ＣＡＡＴの利用については、大きく次の３つの方法があります。

(1) 被監査会社の汎用コンピュータに監査人が作成した汎用監査プログラムをロードし、抽出、計算、比較、統計処理等を実施し出力する方法

(2) 被監査会社の電子記録化された監査対象データを電子記録のまま入手し、監査人の管理下にあるＰＣ等を用いて、監査人が、入手したデータを利用し、必要な監査手続（合計調べ・抽出・分析等）を実施する方法

(3) 被監査会社より貸与されたクライアントＰＣ等からネットワークを介してデータベースへアクセスし、必要な監査手続（合計調べ・抽出・分析等）を実施する方法

過去においては(1)による方法が主でしたが、ユーザ向けデータ活用ツールの普及、高性能・小型ＰＣの出現、表計算ソフトやデータベースソフトの充実により、現在は(2)や(3)の方法が主流となっています。また、通常(1) や(3)の方法はシステムに精通した専門の担当者が実施することが多いため、本研究報告では(2)の留意点を説明していきます。(2)を前提に手作業の場合とＣＡＡＴの場合の違いを比較すると以下のようになります。

内　容	手作業の場合	ＣＡＡＴの場合
データの形態	帳票	電子記録
処理可能データ量	少ない	多い
入手データの加工の容易さ	限界あり	容易
複雑な監査手続の適用	限界あり	容易

また、ＣＡＡＴを利用することにより、手作業によった場合では実施が困難であるような、大量のデータ処理を伴う監査手続の実施が可能となることも、その特徴といえます。

なお、(1)や(3)を採用する場合には、監査人による誤操作等により被監査会社データへ不適切な変更が生じないよう留意する必要があります。読み取り専用権限を利用するといった対応が考えられます。

２．ＣＡＡＴにおける手続

監査人が大型汎用コンピュータやサーバについての専門的な知識を必要としなくても、被監査会社の電子データを利用することが可能となってきています。表計算ソフトやデータベースソフトを通常の監査業務で利用する監査人は増えてきていますが、これらのソフトの理解によってそのままＣＡＡＴの実施につなげることが可能となるといえます。

実際の手続としては、以下の流れになります。

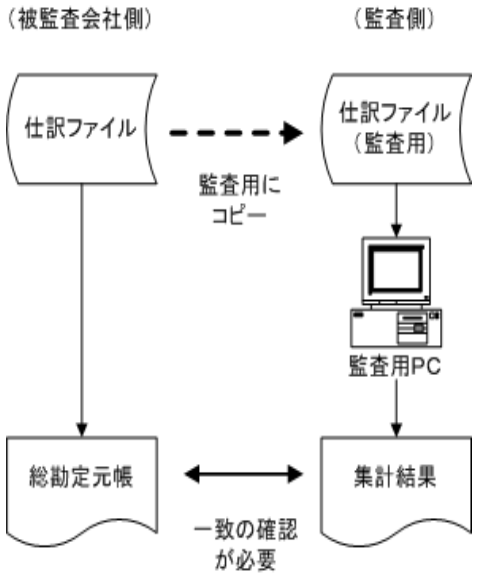
(1) 被監査会社との間でデータ入手又は利用の合意
(2) 被監査会社の情報システムの概要調査
(3) 監査対象ファイルの決定（具体的には必要項目や対象期間も決定する）
(4) データを入手又は被監査会社のＰＣを利用しＣＡＡＴを実施

まず、被監査会社との間でデータの入手又は被監査会社のＰＣ（端末）を利用したデータアクセスを行うのであれば、データ利用等について合意します。被監査会社の対象データファイルに対して直接アクセスすることは、書き換えやファイル破壊の可能性という危険性があり、権限の限定などでそのようなおそれがない場合を除き避けることが望まれます。また、ファイルのコピーにおいてもデータ漏洩の問題があるので、保管責任という点からも留意します。

次に、被監査会社の情報システムの概要調査を行い、どのファイルからどのような帳票が出力されるのか、他のシステムとの関係はどうなっているのか、ファイルレイアウトなどファイルに関する概要などを調査し、監査対象ファイルを決定します。この場合、例えば、販売に関する明細データであると膨大なファイルサイズとなってしまう可能性があるため、監査用のファイルを作成する場合には、必要な項目や対象期間等でファイルの絞り込みを行うことが望まれます。

なお、ＣＡＡＴを実施する際には、被監査会社から入手したデータが正しいか、必要な情報を網羅したものかどうかについて確かめることが必須となります。確かめる方法としては例えば、監査人側で特定の科目の合計金額や件数を集計し、入手したデータと被監査会社の総勘定元帳と突合して確かめる方法（図表１参照）があります。また、データ参照範囲の権限管理により監査上必要な項目にまで制限がかかっている場合がありますので留意する必要があります。

図表１



Q10：仕訳テストを実施する際にＣＡＡＴを利用した方がよいのは、どのような場合でしょうか。

A10：

１．仕訳テストの意義

本研究報告において仕訳テストとは、監査基準委員会報告書 330 第 19 項や監査基準委員会報告書 240 「財務諸表監査における不正」（以下「監査基準委員会報告書 240」という。）第 31 項にある財務諸表作成プロセスにおける重要な仕訳入力及び修正について検証する手続に該当します。

２．ＩＴの利用状況とＣＡＡＴの利用の適否

仕訳テストにおいて、ＣＡＡＴを利用することにより、不正や誤謬による重要な虚偽表示リスクが相対的に高い項目についてより深度のある手続を実施したり、大量のデータ対象により効率的に手続を実施することができる場合があります。仕訳テストにＣＡＡＴを利用することが適切か否かを検討するに当たっては、監査基準委員会報告書 240 に例示されているリスク要因に加えて、以下のような事項が検討ポイントとなります。

- 仕訳データの量
- 仕訳入力権限を持つユーザ数
- 仕訳パターンの種類
- 自動仕訳生成機能の複雑さ

以下では、これらの検討ポイントを踏まえた、利用についての検討の事例を説明します。

(1) 財務アプリケーション及び会計アプリケーションが他の業務アプリケーションと連携していない場合

この場合、すべての仕訳は手入力されていることになります。入力権限を持つユーザ数、入力可能な端末の設置状況等にもよりますが、一般的にこのような環境下では、入力権限者もテスト対象となる仕訳データの量もそれほど多くはないと考えられますので、ＣＡＡＴを利用しなくても、必要かつ十分な仕訳テストを実施できる可能性は高いものと考えられます。

(2) 財務アプリケーション及び会計アプリケーションと他の業務アプリケーションが連携している場合

販売アプリケーションなどの他の業務アプリケーションから、財務アプリケーション及び会計アプリケーションに仕訳データが連携しているような場合、連携データにより自動計上される仕訳と、財務アプリケーション及び会計アプリケーションに直接手入力される仕訳の二種類の仕訳が存在し、仕訳データ量も多くな

ります。例えば、テスト対象となる仕訳データからＣＡＡＴにより、相対的に重要な虚偽表示リスクの高い手入力の仕訳データや発生頻度が低い自動計上された仕訳データを抽出することで、効果的な監査手続を実施することが可能となります。

(3) ＥＲＰ等が利用されている場合

財務会計と販売管理や在庫管理などの機能が高度に統合されているＥＲＰのような場合は、仕訳及び修正の入力が可能なユーザ又は端末が広範に存在することが一般的です。このような環境下では、不適切な仕訳を発見できないリスクが高まると同時に、テスト対象となる仕訳の数も多くなると考えられることから、ＣＡＡＴを利用して仕訳テストを行うことが効果的かつ効率的であることが多いといえます。

なお、ＥＲＰの仕訳等の検索機能や監査機能を利用できる場合があります。

３．仕訳テストに利用可能なＣＡＡＴツールの例

仕訳テストに利用可能なＣＡＡＴツールには、以下のようなものがあります。

(1) 汎用ＰＣソフトウェア

広範に利用されている簡易データベースソフトウェアや表計算ソフトウェアにも、仕訳データの検索や並替えといった機能がありますので、テスト対象となる仕訳データの量に応じて、これらを用いて仕訳テストを実施することも可能であると考えられます。状況によっては、ＳＱＬのようなより高度なツールを利用することがあります。

(2) 汎用監査ソフトウェア

仕訳データの抽出や並替え、集計といった、監査で通常よく使う機能が簡単に扱えるようになっている汎用監査ソフトウェアが市販されています。このような監査ソフトウェアを使えば、テスト対象とすべき仕訳の条件を決め、監査ソフトウェアに条件を設定することで、対象仕訳が抽出されるので、効果的かつ効率的に仕訳テストを行うことができます。

(3) 仕訳テスト専用ツール

テスト対象とすべき仕訳パターン（例えば、期末日及び期末日近くの仕訳、一定以上の金額又はマイナス金額の仕訳、特定の勘定科目が入った仕訳）があらかじめ幾つか用意されており、金額等の情報をパラメータとして設定するだけで、テスト対象仕訳が抽出されるように作られたツールで、汎用監査ソフトウェア上で機能するように作成されたスクリプト（プログラム）として開発されるのが一般的です。パラメータを幾つか登録するだけで仕訳テストを実施できることから、汎用監査ソフトウェアのみの場合よりも、さらに効果的かつ効率的に仕訳テストを実施することが可能です。

Q11：ＰＣ用の市販の簡易なパッケージ・ソフトウェアを利用して会計帳簿を作成している場合の留意点にはどのようなものがあるでしょうか。

A11：

会計用ソフトウェアは、財務諸表に直接的な影響を及ぼすため、不当な仕訳データの改ざんなどが行われた場合には重要な虚偽表示に直結するという点で、監査人にとっては最も重要な評価対象といえます。

ＰＣ用の市販の簡易なパッケージ・ソフトウェアの中には、社会一般で問題なく使われていることから、会計取引の記帳から財務諸表を作成する機能については、その信頼性が比較的高いと考えることができるものがあります。このような機能自体の評価については、詳細な検証は行わず、リスクが低いとして企業の適用状況の確認等の簡易な手続で十分な心証を得ることができる場合もあると考えられます。この際には、各ソフトウェア会社が何らかのＩＴの基準に基づいて開示している機能一覧表などを利用してパッケージ機能の内容を把握し、内部統制の観点からその適用状況を評価できる場合があります。

しかしながら、市販の簡易なパッケージ・ソフトウェアは、主として中小企業を対象ユーザとしているものが多いため、導入コストを抑えるために機能を限定する必要があることや、経理業務の経験が浅い担当者にとって「融通が利く」という意味での使い勝手をよくするために、統制機能が省かれているものもあります。

また、このような市販の簡易なパッケージ・ソフトウェアを利用している企業では、経理担当者が社内に１名しかいないケースや、システム管理責任者が兼務していて実質的に統制機能やモニタリング機能が働かない状況も生じているケースが考えられます。このような場合には、重要な虚偽表示リスクが高いと判断される可能性もあるため、市販の簡易なパッケージ・ソフトウェアそのものとハードウェア、ネットワークなどのインフラ、それを運用する体制の両面について評価の対象とすることが求められる場合もあります。なお、そのような場合においては、通常求められる全般統制そのものではなく、簡易な手続によるか、あるいは、手作業による内部統制と実証手続により確かめることで足りる場合も多いと考えられます。

さらに、市販の簡易なパッケージ・ソフトウェアをそのまま利用するのではなく、自社の業務処理に合わせる形でカスタマイズしている場合も多く見られます。カスタマイズの内容によっては、本来そのパッケージ・ソフトウェアが持っていた統制機能が無効となることもありますので、カスタマイズの有無とその内容を確かめることが必要となります。

監査人は、企業の利用している市販の簡易なパッケージ・ソフトウェアが、必要な統制機能を有しているか否かだけでなく、さらに、企業が必要な統制機能を実際に使用しているか否かに留意します。初期設定項目（パラメータ）の設定・維持等、市販

の簡易なパッケージ・ソフトウェアを利用するに当たり、別途必要となる内部統制を企業が整備し、有効に運用しているか否かにも留意します。また、財務諸表作成に関連する他の業務をＰＣの表計算ソフトやデータベースソフトなどを利用して行っている場合も同様です。

市販の簡易なパッケージ・ソフトウェアに特有の留意点としては、例えば、以下の点が挙げられます。

１．入力された仕訳データについて、管理者による市販のパッケージ・ソフトウェア上での承認手続を経て正式に処理する仕組み

管理者による承認手続の機能がない場合には、紙に仕訳データを打ち出し、管理者がチェックし、承認印を押印するなど、手作業での承認手続が重要な内部統制となる場合があります。

２．仕訳データの変更（修正）を行う際に、正規の承認を受けた変更のみを処理し、かつ、変更履歴が残る仕組み

多くの市販の簡易なパッケージ・ソフトウェアでは、経理業務に不慣れな担当者が修正しやすいように入力した仕訳の修正ができないようにする確定機能を使わないと、仕訳データを随時上書き変更することができる一方で、変更履歴が残らない仕組みになっているため、改ざんを防止又は発見することが難しくなっています。監査人の往査後に仕訳データが改ざんされた場合には、虚偽表示を発見できない可能性が高くなります。

したがって、例えば、運用上、仕訳データを上書き修正するのではなく、修正を要する仕訳を必ずマイナス処理（逆仕訳）し、正しい仕訳を改めて入力するような仕組みを設け、さらに毎月の月次処理が終了、確定した場合に紙で最終データを残しておくなどの対策が考えられます。

３．仕訳データへのアクセス管理

ＰＣにインストールされている市販の簡易なパッケージ・ソフトウェアに誰でもアクセスできる状態になっている場合には、改ざんやデータ破壊などの可能性が高まります。したがって、監査人は、ＩＤ、パスワード等によるアクセス・コントロールの仕組みが利用されているかを把握します。特に、１台のＰＣを複数の担当者で共有しているような場合には、ユーザが特定できない場合があるため、会社の管理方法を確認します。

また、パッケージ・ソフトウェアのシステム開発担当者やシステム開発会社（以下「ベンダー」という。）が保守のためにリモートでアクセスできるような権限を有している場合があります。ベンダーのアクセスがバージョンアップ等のイベント時だけに限定されている場合には、作業終了後に使用されたＩＤが削除（又は無効

化）されていれば、本番データへの不適切なアクセスが防止されていると考えられます。一方、ベンダーのアクセスが常時可能となっている場合には、ベンダーが実施している作業内容と、会社の実施している確認方法を把握します。

４．ハードウェアの保護

例えば、ノートＰＣに市販のパッケージ・ソフトウェアをインストールして使っている場合には、仮に、ノートＰＣが盗まれたり壊されたりした場合には、経理業務そのものが不可能になり、財務諸表の作成すらできなくなります。したがって、ＰＣそのものが十分に現物管理され、外部に持ち出さないなどの対策が取られているかを確認します。

５．ＰＣをＬＡＮなどのネットワーク上で利用している場合

ＰＣをＬＡＮなどのネットワーク上で利用している場合には、他のＰＣからネットワーク経由で侵入し、データを改ざんしたり破壊されたり外部に持ち出されたりする可能性が高まります。したがって、監査人は、ネットワーク経由の侵入を防ぐ仕組みがあるかどうかを確かめます。また、ＰＣがインターネットに接続されている場合には、インターネット経由での侵入やコンピュータウイルス等による改ざんやデータ破壊の可能性が高まりますので、これらへの対応が適切になされているか、会社の対応の状況を確かめます。

６．締め処理の実施、期首財務諸表数値の確認

ＰＣ用の市販の簡易な会計用パッケージ・ソフトウェアについては、締め処理機能を有していないもの、締め処理機能を有していても、簡単なフラグの設定のみで容易に再オープンを行い、財務情報の確定した前期分として仕訳の入力が行えるものが存在します。月次での締め処理も同様です。また、こうしたパッケージ・ソフトウェアを利用して経理業務を行っている会社等の担当者は、締めについての感覚が乏しく、確定決算後に前期の仕訳漏れに気付いた場合等に締め処理を行った年度に対して仕訳の追加又は修正を行う場合があります。したがって、監査人は、パッケージ・ソフトウェアにおける締め処理の機能について理解するとともに、必要に応じて期首財務諸表数値の正確性について確かめます。

７．税法等に係るパラメータの設定等の確認

一部の簡易なパッケージ・ソフトウェアでは、消費税率、固定資産の減価償却等について自動計算が行われ、自動仕訳が作成されるものがあります。このような計算の基礎となる税率等が、パッケージベンダーによるパラメータ、パッチ（プログラム）等の形で、パッケージベンダーとの間の保守契約に基づき提供される場合な

どがありますが、会計パッケージソフトについて保守契約が更新されていない場合などは、システムに対する適切な変更が行われず、誤った情報に基づいた計算、仕訳の投入につながる危険性があります。

また、被監査会社により、直接パラメータ変更等が行われている場合には、その変更が適切な実施時期、方法により行われないリスクも存在することに注意します。

８．データの保管、バックアップ

ＰＣ用の市販の簡易なパッケージ・ソフトウェアを利用し、当該ＰＣにデータを保管している場合には、データの改ざん・破壊、ハードウェア（ＰＣ）の故障によるデータ破壊などのリスクが高く、財務諸表作成そのものが不可能になったり監査が不能になったりする場合もあり得ることから、例えば、アクセス権を制限し、セキュリティ面に十分配慮した対応が取られているサーバ上にデータを置いたり、定期的にバックアップを取っておくなどの対策が講じられているかなども、必要に応じて確かめます。

９．バージョンアップ

ＰＣ用の市販の簡易なパッケージ・ソフトウェアのバージョンアップを実施する場合には、本来予定している内容以外のバージョンアップについて実施されることがないよう留意するとともに、必要なバージョンアップが適切に行われているかを理解することも、会社の利用する統制機能を理解する上で有用な場合があります。

Q12：入力データの承認が、電子承認で実施されている場合の監査上の留意点はどのようなものですか。

A12：

承認は、発生した取引が企業で処理され記録されるべき正当な取引であることを確保するための手続として実施されるものです。ここでいう電子承認とは、承認した結果を紙に署名・押印して記録する代わりに、アプリケーション上で承認の入力・記録を行うことです。

電子承認であっても、紙の伝票上で行われる承認における署名・押印のように、画面上に承認の証跡が表示される場合がある一方、承認がないと次の処理に進めないなどの設計がシステムに組み込まれているのみで、画面上では特に承認の証跡が表示されない場合もあるため留意します。

また、システム上に、承認又は拒絶を制御する仕組みを組み込む場合もあります。例えば、値引きなど、ある一定の幅は担当者が値引き可能で、システム上で自動的に承認されますが、一定額以上の値引きが入力された場合には、権限者による承認がないと先の処理が拒絶される（例えば、出荷ができない。）などの仕組みがシステム上

設定される場合もあります。

監査人にとっての基本的な留意点は、紙の伝票への押印による承認でも電子承認でも同じであり、例えば次の事項が挙げられます。

・　承認は正当な権限者によって行われているか。
・　承認は権限者本人によって行われているか。
・　承認漏れはないか。
・　承認は事前か事後か。

電子承認の場合、上記の具体的な留意点は以下のようになります。

１．承認は正当な権限者によって行われているか。

これはシステムへのアクセス権限の設定によって行われます。アクセス権限テーブルの設定が企業の職務権限規定に従っているか、承認の入力画面は権限のあるＩＤからアクセスした場合にのみ、表示されるように設定されているか、ＩＤはその権限を保有している正当な権限者に付与されているか、などを確かめることになります。

監査手続としては、システム上の設定内容を質問し、その設定内容が職務権限規程に合致しているかを確かめ、さらにその設定どおりに実際に適用されているかを、アプリケーションの画面等を観察することで確かめることになります。

２．承認は権限者本人によって行われているか。

紙の伝票の場合に、印鑑を部下に預けるなどのケースが見られるのと同様に、電子承認の場合にも、設定上は適正な権限者にのみ承認権限があるにもかかわらず、部下が権限者のＩＤとパスワードを知っているなど運用上の問題がある場合や、実務的に運用するために、代行での入力を認める設定をする場合があります。

権限者のＩＤとパスワードをその課の全員が知っているとか、紙に書いて貼ってあるなどの状況については、現場での運用状況の観察等によって実態を把握することになります。

代行入力が行われる場合は、常時代行入力の権限が与えられているのか、代行入力についての記録は残るように設定されているかなどの観点から、適切な管理体制が整えられているか留意します。また、その場合には、権限者が事後的に承認するなど、代行入力等による承認が適切に行われているかを検証する手続が取られているかについても留意します。

３．業務上承認は必須か。

紙の伝票での処理の場合には、押印無しで処理されているものについては、伝票を通査して確かめることができます。電子承認の場合は、まずシステムの設定

が承認無しでは次の処理に進まないようになっているのか、承認無しでも次の処理に進めるかを確かめます。

承認無しでも次の処理に進めるシステム設定の場合には、次の（4）の事後承認の処理がどのように運用されているかなどを確かめます。例えば、与信限度を超えると出荷できない設定を行っている場合には、与信限度を超えると出荷できませんが、与信限度を超えても単にアラームを出す設定の場合には、アラームが出た場合の出荷の許可をどうするかの手順が適切に運用されていないと与信以上の出荷が許可無しに実行されることになり、与信設定の実効性がなくなってしまいます。

一方、承認無しでは次の処理に進めないシステムの場合には、実際にシステム上で承認処理の有無と、その後の処理の可否が制御されているかを、システムの画面を観察するなどにより確かめることが考えられます。また、承認処理がされないことによるリスクについても留意します。例えば、支払承認権限者が承認を怠ったために、債務の認識が遅れ、支払処理の滞留が発生し、データが会計アプリケーションに到達しないため負債が簿外になるようなことが起こらないようにする仕組みも必要です。

４．承認は事前か事後か。

紙の伝票による処理の際に、口頭で了解を得て事後に押印をする場合や、営業所の小口の支払などで出金後に事後承認する場合があります。この場合に、事後承認が小口のみであるなどリスクがある程度限定されるものか、与信限度を大幅に超える売上など多大なリスクが発生するものなのかを評価して、その監査上の対応を決定しなければなりません。

なお、事後承認が必ず実施されているかも確かめることになります。

Q13：業務処理統制の検証手続について説明してください。

A13：

業務処理統制は、通常、業務プロセスにおいて個々のアプリケーションによる取引の処理に適用される手続であり、手作業による場合とプログラムに組み込まれて自動化されている場合とがあります。したがって、プログラムに組み込まれている自動化された業務処理統制と、ＩＴから自動生成される情報について、自動化された部分の検証をすることになります。

プログラムにより自動化された業務処理統制の検証では、内部統制が期待される機能を果たしているかどうかについて、合理的な心証を得ることになります。なお、必ずしも、アプリケーションのプログラムの機能を完全に再現することや、プログラムの手順どおりに実施する必要はありません。当該内部統制の機能を理解した上で、入

力された情報や状況に対して期待された出力結果やアクションがとられることを確かめることで検証できる場合があります。

また、プログラムにより自動化された業務処理統制が正しく機能していても、チェックされたデータについて簡単に変更が加えられる可能性があっては意味がありません。そのため、データが適切なアクセス・コントロールの下に運用されていることを確かめます。

内部統制をプログラム化するのは、企業の取引が膨大な量になり手作業によるチェックが物理的に不可能になったこと、取引を定型化することにより内部統制をプログラム化することが可能になったこと、プログラム化した方が手作業よりも効率化できることなどの理由からです。

１．自動化された業務処理統制とＩＴから自動生成される情報の例

(1) エディット・バリデーション・チェック

入力内容が、入力を予定している内容と一致しているかどうかをチェックする機能をいいます。

具体的には、入力項目として金額を数字で入れるべきところに文字を入れた場合にエラーとするなどのフォーマットチェック、入力必須項目にデータが入力されていないときにエラーとする必須項目チェック、仕訳データの貸借のバランスなどをチェックするバランスチェック、値の上限値や下限値をチェックするリミットチェックなどの方法があります。

(2) マッチング

入力内容が、マスター・データ等のあらかじめ参照するデータに記録されているかどうか確かめる機能をいいます。

例えば、得意先コードを入力するときに、アプリケーションに登録されている得意先マスター・ファイルのコードを参照して、マスター登録されていないコードが入力されようとした場合にはエラーとします。

(3) コントロール・トータル・チェック

情報の処理過程において受入情報の数値項目等の合計を出力情報と照合する機能をいいます。

例えば、データを入力するときに入力データの合計額を計算してその値も登録しておき、処理後の出力データの合計額と比較して一致しなければエラーリストを出す方法がこれに当たります。

(4) アクセス・コントロール

ユーザＩＤとパスワード等により、権限者とそうでない者を区分・承認する機能をいいます。

例えば、操作端末自体に使用できるアプリケーションの権限を与えておき、操作端末にパスワードを設定する、又はアプリケーションレベルでユーザＩＤごとに使用できる機能の権限を設定しておき、アクセスはユーザごとのパスワードで管理する方法があります。

(5) 自動計算等

利息の金額の自動計算、減価償却費の計上、外貨換算の処理等、アプリケーションの機能により人手を介することなく自動処理されるものをいいます。処理を自動化することにより、情報の正確性、網羅性、適時性等を確保します。

２．自動化された業務処理統制とＩＴから自動生成される情報を検証する手続の例

自動化された業務処理統制とＩＴから自動生成される情報を検証するに当たっては、当該内部統制がどのように機能するかを質問等により理解します。その上で、以下のような手続により期待どおりに機能するかどうかについての心証を得ます。

(1) プログラムのレビュー

実現可能であれば効果的な手続が、当該プログラムにより自動化された業務処理統制に関するプログラムをレビューすることです。技術的、時間的制約があるため、必要に応じて実施することになります。

プログラムのレビューを期中に実施した場合、実施時から期末までの期間変更されていないことが合理的に検証できれば、期末に再びレビューを実施する必要はなくなります。

(2) サンプルテストによる検証

一定数のサンプルについて、当該内部統制に依拠しようとする期間にわたって内部統制をテストすることにより検証できます。

例えば、為替レートと円建ての売上金額により外貨建ての売上を再計算して、計上された外貨売上と照合したり、請求書の価格と承認された売上価格一覧表について照合する方法です。

(3) モニタリングレポートのフォローアップ

ＩＴから自動生成される情報のうちモニタリングレポートが正しく生成されていることは、チェック機能が働き例外処理等を抽出した場合の、当該出力内容に関するフォローアップ状況の検証によっても確かめることができます。

例えば、売上値引が商品別にセットされた値引率によって計算されていない場合に、当該取引がモニタリングレポートとして出力され、適切に内容の検討、承認が実施されているかどうかを検証することです。

(4) ＣＡＡＴ

詳細については、Ｑ９、10、21、30、35 を参照してください。

Q14：売上を自動的に計上するシステムを採用している場合、内部統制の検証手続はどのように行うのでしょうか。

A14：

売上計上に係るシステムは、売上高や売掛金などの勘定科目のアサーションと密接に関係します。

売上を自動的に計上するシステムの場合は、企業の採用している会計方針に従った処理をシステムによって、実行可能であることが前提となります。また、発生が予想される定型外の取引や大口取引、与信超過などについて、モニタリングに必要な情報を提供できるかも検討します。

売上を自動的に計上している場合には、例えば、次のリスクがあります。

- 実態と合わない取引を自動的に計上してしまう。
- 自動計算の誤りにより売上計上の金額を誤る。
- 一部の取引が計上漏れになる。
- 処理タイミングにより適切な会計期間に取引が記録されない。
- 不正な手作業により取引が追加・削除・改ざんされる。

システムの把握･検証に当たっては、自動化されている範囲、売上計上のタイミングに特に留意します。売上計上に係る自動化には以下のように、幾つかのパターンがあります。

１．手作業の入力を基に自動計上する場合

出荷情報を入力することにより、あらかじめ登録された商品マスター（単価情報を含む）等に基づき売上金額を自動的に計算し売上を計上する場合には、例えば、以下のような点に留意します。

(1) あらかじめ商品情報がマスター登録されていない商品の売上は計上できない仕組みとなっているか。

(2) あらかじめ登録された単価情報以外の金額で売上計上できない仕組みとなっているか。

(3) 単価訂正が可能な場合には、適切な承認を得て行われているか。その履歴が残っているか。

(4) 商品マスターは適切にメンテナンスされ、最新の情報に保たれているか。

２．他のシステムのデータを基に自動計上する場合

物流アプリケーションの出荷データを基に売上を自動的に計上するシステムの場合には、例えば、以下のような点に留意します。

(1) システム間のデータのインターフェイスは適切に行われているか。

(2) エラーデータは、適切にフォローアップされているか。

(3) 物流システム（受渡側）で行われた取消し・変更が、売上計上時までに売上シ

ステム（受入側）に適切に反映されるか。

(4) 物流システムと売上システムの商品マスターは適切にメンテナンスされ、同期を取って最新の情報に保たれているか。

３．売上計上予定日に自動的に売上を計上するシステム

売上計上予定日に自動的に売上を計上する場合には、例えば、以下のような点に留意します。

(1) 売上予定の登録は、適切な承認又は信頼できるデータに基づいているか。

(2) 売上の数量、金額、予定日等の取消し・変更は適時に入力されているか。

(3) エラーデータは、適切にフォローアップされているか。

(4) 売上計上予定日と実際の売上計上日に不整合はないか（例えば、出荷基準の場合、出荷予定日と実際の出荷日が合っているか)。

特に、何らかの理由により出荷ができなかった場合、取消し入力が適時に行われないと、架空の売上が計上される結果となる点に留意します。

いずれの場合においても、計上金額の自動計算の方法が適切であるか、得意先に対する与信限度額のチェック、未承認の入力・変更を防止するシステムへのアクセス・コントロールは、重要な留意点となります。

Q15：販売アプリケーションと会計アプリケーションのインターフェイスの有効性はどのように検証するのでしょうか。

A15：

販売アプリケーションで処理された結果は、出力帳票等としてアウトプットされるだけでなく、会計アプリケーションにインターフェイス（データの引渡し）される場合があります。この場合にはインターフェイス・データを送り出す販売システムにおいて、適切な業務処理統制や全般統制があれば、このインターフェイス・データの正確性は保証されているはずですが、アプリケーションの開発時期の相違によるアプリケーション間の構造の違い等により、必ずしもデータが正確にインターフェイスされるとは限りません。

インターフェイス・データを受け取る会計システムから見れば、他のシステムからのインターフェイスはデータの入力に他なりません。データの入力時には、データの正確性を確保する必要があります。データの引渡しに重要性のある場合、インターフェイスの信頼性を検証するためのテストを行うことがあります。

一般的にインターフェイスの信頼性を検証するには次のような３つのアプローチが考えられます。

・　送信データと受信データを突合し、送信データが誤りなく受信されていることを確かめる。

・　システムに実装されているコントロール・トータル・チェック等のインターフェイスの信頼性を担保するコントロールが有効に機能していることを確かめる。
・　インターフェイス自体にインターフェイスの信頼性を担保する機能が実装されていることを確かめる。

それぞれのアプローチによる売掛金残高データのインターフェイスをチェックする具体例としては、次のようなものがあります。

1．送信データと受信データを突合し、送信したデータが誤りなく受信されていることを確かめる。

販売システムと会計システムのインターフェイスの信頼性を検証する場合、販売システムの送信データと会計システムの受信データを突合し、送信したデータが誤りなく受信されていることを確かめることになります。

2．システムに実装されているコントロール・トータル・チェック等のインターフェイスの信頼性を担保するコントロールが有効に機能していることを確かめる。

システムに実装されるインターフェイスの信頼性を担保するコントロールとしては、次のものが挙げられます。

(1) インターフェイスの都度、受け取ったデータとシステムで保持しているインターフェイスの元データを、それぞれのシステムから取り出しデータを照合する機能を実行し、不整合があった場合にはエラーリストを出力する。

(2) インターフェイスの都度、インターフェイスされた元データの数値項目などの合計を受け取った情報の数値項目などの合計と照合し、不整合があった場合にはエラーリストを出力する。

このような内部統制が有効に機能しているかどうかの検証を行うために、一般的には次のような手続を行うことになります。

①　仕様書上で組み込まれているチェックの内容を確かめる。
②　当該チェック内容の適切性、十分性を検討する。
③　当該チェックが実際に機能していることを検証する。

3．インターフェイスにインターフェイスの信頼性を担保する機能が実装されていることを確かめる。

インターフェイス自体に実装されているインターフェイスの信頼性を担保する機能としては、次のものが挙げられます。

(1) ファイル転送ソフトの利用

ファイル転送ソフトとは、企業内・企業間の業務システムにおいて、日常のシステム運用で発生するデータ連携を自動化するツールです。ファイル転送ソフトの中には、文字コード変換機能や、転送が異常終了した場合のリカバリー機能な

ど、インターフェイスの信頼性を担保する多彩な機能を備えます。一般的にインターフェイスにファイル転送ソフトが利用されている場合、データのインターフェイスにおける信頼性は高いといえます。

(2) ハッシュ値の比較

何らかの理由によるファイルの破損、オリジナルからの変更をチェックする場合には、ファイルのハッシュ値を比較する方法があります。販売システムと会計システムのインターフェイスにおいて、送信前のファイルのハッシュ値と受信されたファイルのハッシュ値を比較する機能が実装されていれば、データのインターフェイスにおける信頼性は高いといえます。

(3) エラー訂正プロトコルの採用

プロトコルとは、コンピュータ等の電子機器間で通信する際の取り決めのことです。

エラー訂正プロトコルは、プロトコルの一つであり、通信時に発生したエラーの回復手順を示すプロトコルであり、一般的にはエラーを検出してから、自動的にデータの再送が行われます。一般的にエラー訂正プロトコルに基づいて、インターフェイスが設計されていれば、データのインターフェイスにおける信頼性は高いといえます。

上述①～③の機能は、インターフェイス時におけるデータ伝送の信頼性を高めるものですが、送信されたデータに含まれる勘定科目、金額等、送信内容の正確性を担保するものではないことに留意します。

上記２．及び３．を直接検証しようとすれば、エラーとなるはずのデータを含んだテストデータを実際に処理させることになりますが、このテストデータの処理が実際に稼動しているシステムに影響を与えないようにすることは非常に困難です。上記２．及び３．の手続は、例えば、実際に稼動しているシステムと別に、同様のテスト環境が用意できるのであれば、実施可能となります。

したがって、このような直接的な検証ができない場合の代替的方法として、次のような手続が考えられます。

- 当該チェックのソース・プログラムのレビュー
- 新規開発や大きな変更が行われたシステムについて、開発時のテスト計画、本番移行直前のテスト結果のレビュー
- 稼動中のシステムについて、実際に出力されているエラーリスト、プルーフ・リストのレビュー
- 稼動中のシステムについて、インターフェイス元の帳票と関連するインターフェイス先の帳票の照合

Q16：企業が、新規にパッケージ・ソフトウェアを導入した場合、監査人はその計算処理の妥当性等について検証する必要がありますか。

A16：

企業が市販のパッケージ・ソフトウェアを利用している場合であっても、監査人は、当該パッケージ・ソフトウェアによる計算処理の妥当性等について検証することが必要になると考えられます。

企業がパッケージ・ソフトウェアを利用する場合、通常、個々の企業組織・制度等に応じてシステムを設定し、計算処理を行う上で必要となる基礎データ等を入力することで、算出すべき数値の計算を行うものと考えられます。このため、監査人は、パッケージ・ソフトウェアによる計算処理等そのものが企業の採用する会計方針に準拠して処理されているかを検証する手続に加え、パッケージ・ソフトウェアの利用に当たり、適用されているシステム設定・基礎データの入力方法・頻度などが、計算結果の正確性等に及ぼす影響を考慮して、検証すべき手続を策定することが求められます。なお、社会一般で普及している市販のパッケージ・ソフトウェアをカスタマイズせずに利用する場合には、ソフトウェアの機能自体の評価については簡易な手続で十分な心証を得ることができることもあると考えられます。

企業がパッケージ・ソフトウェアを利用している場合に、その計算処理の妥当性等を検証する際には、主として以下の点に留意します。

１．パッケージ・ソフトウェアによる計算処理の検証

検証対象となる計算処理機能には、ソフトウェアに組み込まれている処理機能をそのまま利用する、又は業務に合わせてカスタマイズする、の二つが考えられます。パッケージ・ソフトウェアによる処理結果については、監査人が、企業が導入・変更時に実施した処理の検証結果を利用して計算処理の妥当性を検討する、又は監査人自らが表計算ソフトウェア等を活用して見積値、推定値を算出し、これらの結果を比較分析することで計算処理の妥当性を検討するなどの方法が考えられます。

なお、退職給付債務の計算等が複雑で、監査人自らが見積値、推定値を算出することが困難な場合には、アクチュアリー等の専門家を利用してパッケージ・ソフトウェアの処理結果を分析することで、その処理が妥当であるかを検証することが考えられます。

２．パッケージ・ソフトウェアを利用するために行われるシステム設定の検証

パッケージ・ソフトウェアを利用する際に、企業は当該パッケージ・ソフトウェアによるシステム処理が、企業の組織・制度等の設計に準拠して行われるよう、システム上の設定を行います。したがって、そのシステム上の設定及びその登録・変更手続が正しく行われない場合、システムの処理結果が正しく得られないことになります。

このため、監査人は、企業がパッケージ・ソフトウェアを利用するに当たり、システム設定が適切に行われているか、また、その登録・変更手続が適切な申請、承認等の手続を経て行われているか等について把握・評価することで、パッケージ・ソフトウェアによる処理が妥当であるかを検証します。例えば、連結会計システムにおいて、仕訳、為替、税率等の各種マスターの設定が適切に登録・変更されているか、退職給付債務パッケージ・ソフトウェアにおいて、システム設定上の基準（給与基準、ポイント基準等）が企業の制度に対応しているか、割引率・死亡率等の基礎数値が適切に設定されているか、また、これらの設定値の登録・変更手続が適切に行われているか等に留意し、監査手続を実施することになります。

Q17：システムから出力された延滞債権リストや滞留在庫リストを利用する場合に留意すべき事項について教えてください。

A17：

システムから出力された延滞債権リストや滞留在庫リストを利用して実施される内部統制は、ＩＴから自動生成される情報を利用して実施される手作業による内部統制の代表例です。

延滞債権リストや滞留在庫リストのようなＩＴから自動生成された情報が、企業の重要な手作業による内部統制のために利用されている場合には、監査人は、その情報の正確性や網羅性について評価します。まず、リスト生成の基になる売掛金データや在庫データが漏れなく正確であるということについて評価し、さらに、延滞債権リストや滞留在庫リストが、すべての売掛金データや在庫データを対象として一定の条件に該当するものが漏れなく正しく抽出されているかを評価します。

評価するに当たっては、延滞債権リストや滞留在庫リストを出力する情報システムの全般統制の整備及び運用状況の有効性についても考慮します。自動生成された情報が、ある時点において意図されたとおりに作成されていたとしても、その自動生成された情報を支える全般統制が有効に機能していない場合、その自動生成された情報が意図されたとおりに継続的に生成されているという心証は得られないことに留意します。

具体的な監査手続としては、以下のような手続が考えられます。

- 延滞債権リストや滞留在庫リストを出力する情報システムの処理環境やアプリケーションの十分な理解を行います。この理解には、延滞債権や滞留在庫を記録し表示する仕組みの理解が重要です。債権の延滞や在庫の滞留の定義と条件について、システム上の要件と業務上の要件の理解（例えば、一部入金や一部出荷により延滞債権や滞留在庫として認識されなくなる可能性等）します。
- 延滞債権リストや滞留在庫リストを出力するまでのリスト作成過程のウォークスルーの実施が有効です。これらのリストは、システムからの出力帳票であるため、

売上債権や在庫情報のインプットから出力までにどのようにデータが蓄積され、更新されているのかを理解することが重要です。

・　延滞債権リストや滞留在庫リストについて、企業がこれらのリストの情報の正確性や網羅性に関する内部統制を整備し、運用を行っている場合は、その内容について検討を行います。

また、監査人は企業が作成した情報を監査手続に利用する場合、その情報の正確性及び網羅性を確かめるための手続を実施します。例えば、債権データや在庫データを入手し、そのデータが財務諸表、総勘定元帳及び補助元帳に一致し、漏れなく正確であることを確かめます。そして、延滞債権リストや滞留在庫リストの再計算を行い、企業の作成した延滞債権リストや滞留在庫リストのデータと比較し、データの正確性や網羅性を確かめます。

Q18：全般統制評価の財務諸表監査上の意味はどのようなものでしょうか。

A18：

１．全般統制の財務諸表監査上の意味

ＩＴ実６号第 34 項には、「全般統制は、多くのアプリケーションに関係する方針及び手続であり、情報システムの継続的かつ適切な運用を確保することにより、業務処理統制が有効に機能するよう支援する。」とあります。具体的には、データ・センターとネットワークの運用管理、アプリケーションの取得、開発及び保守、システム・ソフトウェアの取得・変更及び保守、プログラム変更、アクセス・セキュリティに関する統制活動が含まれており、ＩＴを利用した情報システムの運用・管理に関する統制活動のことです。

ＩＴを利用した情報システムにおいては、いったん適切に組み込まれた内部統制（特に統制活動）は、意図的に手を加えない限り継続して有効に機能するという性質を有しています。しかし、開発段階で必要な内部統制が組み込まれなかったり、システムがダウンしたり、プログラムに不正な改ざんが行われたり、不正な侵入が行われたりすると、この“継続して有効に機能する”という性質が保証されなくなります。こうしたシステムの開発、運用、保守にかかわる内部統制が全般統制です。

したがって、業務処理統制の評価を伴わない全般統制のみの評価では、内部統制（特に統制活動）の有効性を確かめることはできません。また、反対に、一定時点で業務処理統制のみ評価を行い、全般統制の有効性を確かめない場合には、監査対象期間を通じての有効性を評価することはできません。全般統制と業務処理統制の評価は、両者ともに行うことにより初めて意味のあるものとなります。

市販の会計パッケージ・ソフトウェアを購入してそのまま利用していても、全般統制の評価を全面的に省略できるものではなく、例えば、アクセス制限を評価する

といった、そのパッケージ・ソフトウェアの特性に応じた評価が必要なこともあります。

２．全般統制の評価単位

全般統制は、業務処理統制の継続的な運用を支えるものですから、「業務処理統制が評価の対象となる場合には、それを支える全般統制に依存している程度と範囲について検討し、全般統制の評価範囲を決定する。したがって、企業のすべての情報システムを対象として、評価を実施するものではない。」（ＩＴ実６号第 40 項）ことに留意します。

また、「全般統制の評価は必ずしも対象となる情報システムごとに実施しなければならないものではなく、情報システムの種類等や設置場所、あるいは、運営組織を考慮し、共通に評価できるものを一つの評価単位とすることも可能である。」（ＩＴ実６号第 40 項）ため、全般統制の評価は、通常ＩＴに関する基盤（インフラや管理体制等）単位で評価することになります。例えば、企業が購買、販売、流通の３つのアプリケーションを有している場合には、監査人としては、それぞれのアプリケーションがどのような基盤（インフラや管理体制等）の上で動いているかを把握します。

購買、販売、流通の３つのアプリケーションが共通センターの一つのホストで集中管理されている場合など、すべて同一インフラの上で動いていて、その管理体制が同一である場合には、全般統制に関する統制リスク評価は、基本的には共通の評価単位一つで済みますが、すべて別のインフラの上で動いている場合や、管理する部門が異なるなど管理体制が異なる場合には、全般統制に関する統制リスク評価は３つの評価単位を対象として行わなければならなくなります。

一方、業務処理統制は、上記どちらの場合であっても、基本的には個々のアプリケーションごとに行わなければなりません。

監査人として、どのようなインフラ・管理体制の下で、どのようなアプリケーションが動いているのかを識別することが、全般統制に関する統制リスク評価の第１歩となります。

３．全般統制評価の意味

また、全般統制評価は、いわばＩＴに関する基盤（インフラや管理体制等）に対する評価ですから、その有効性の評価結果が直ちに統制リスク評価に結び付くものではありません。全般統制は、あくまで「情報の信頼性を確保すること、及び業務処理統制の継続的な運用を確実にすることを間接的に支援するもの」ですから、いくら全般統制が有効に機能していると評価されたとしても、それだけで「業務処理

統制も有効である」あるいは「業務処理統制に係る統制リスクは低い」という結論には至りません。

Q19：スプレッドシートに関する統制リスクの評価手続の留意点にはどのようなものがあるのでしょうか。

A19：

企業において使われるスプレッドシートは、単純な集計のみを行うような手作業に近い使い方から、複雑な割引現在価値計算等の通常のコンピュータの自動計算と同じような処理を行うものまで様々なものがありますが、一般的には、四則演算を行うような比較的単純なものの占める割合が相当程度あるものと想像されます。

比較的単純なスプレッドシートについては、検算等の手作業での統制手続により、十分にリスクを低減できる場合もあると考えられます。

一方、機能を自動化するマクロの利用や処理の内容が複雑でブラックボックス化しているような相当に複雑なスプレッドシートが利用されている場合には、自動化された業務処理統制と同様の処理の一貫性を維持するような内部統制の整備が求められる場合もあります。例えば、データベース機能を活用し、在庫管理などの基幹システムとして高度に利用するような場合には、通常のシステムの管理と同等の管理が必要となることに留意します。

スプレッドシートの利用状況としては、スプレッドシートが単独で利用されている場合（他システムとの接続がない場合）と、他システムと連携している場合（メインシステムからデータを取り込みスプレッドシート上で加工するのみの場合、及びスプレッドシートにデータを取り込んで加工した後、メインシステム等に再びアップロードして処理を続ける場合等）があり、他システムと連携している場合には、その連携に人手が介在するのかどうかにより考え得るリスクが異なってきます。さらに、データのダウンロード・アップロードが自動で行われていたとしても、スプレッドシート上でのデータの加工後に他システムへアップロードする場合には、それがつながっている先のシステムの変更管理やデータのアクセス・コントロールにどのような影響があるかについて考慮することが必要となる場合があります。

したがって、監査人は、スプレッドシートについて、その処理の内容や財務諸表の記載事項に影響を与えるリスクの程度等を勘案し、それに応じて必要と認められる統制手続の内容、範囲等を検討します。

スプレッドシートのリスクの程度を評価する観点としては、例えば、以下のようなものが考えられます。

- スプレッドシートの複雑さ
- スプレッドシートが処理する金額の重要性
- スプレッドシートが処理する内容・目的

・　スプレッドシートの変更頻度
・　スプレッドシートと他システムとの連携の程度等

利用しているスプレッドシートが簡易だからといって、統制手続が不要となるものではなく、特定のスプレッドシートが監査上重要なものと判断される場合は、少なくとも計算処理の結果を確かめるために、検算等の何らかの適当な統制手続が必須となることに留意します。

複雑かつ重要なスプレッドシートについての統制手続の例としては、以下のようなものが考えられます。

・　ロジックの検証
　組み込まれたロジックの正確性は検算等により適切に確認されているか。
・　アクセス・コントロール
　スプレッドシートへのアクセスは適切に制限されているか。
・　変更管理
　仕様の確定、テスト、責任者による承認等の手続が正式に定められているか。
・　バックアップ
　バックアップの頻度、対象、保管場所、保存期間は適切か。
・　バージョン管理
　命名規則等の最新のバージョンのみが使用されるための仕組みはあるか。
・　データの完全性とセキュリティ
　数式やマスター・データ等のデータ処理にとって重要な項目が、不正又は不注意な変更から保護されているか。
・　文書化
　スプレッドシートの仕様等は文書化され、適切に更新されているか。
・　他システムとの連携の程度
　他システムとのデータのダウンロード・アップロードは自動で行われているか、またアップロードの場合、連携先システムのデータアクセスや変更管理手続が適用されているか。

Ⅴ　重要な虚偽表示リスクの識別と評価

Q20：ＩＴのコントロール目標とアサーションの関連性について、説明してください。

A20：

アサーションは、経営者が財務諸表において明示的か否かにかかわらず提示するものであり、監査人が発生する可能性のある虚偽表示の種類を考慮する際に利用するものであるとされています（監査基準員会報告書 315 A107 項）。例えば、発生のアサ

ーションは記録された取引や会計事象が発生し企業に関係していることを提示しますが、監査人は企業に関係しない取引や実在しない取引が会計記録に含まれる可能性はないかの視点から、架空取引等の不正リスクを識別することになります。そして、監査人は、リスク対応手続として、経営者が架空取引等のリスクを低減するための内部統制を構築しているかを評価することになります。

企業の多くは業務にＩＴを利用していますので、経営者はＩＴに対する内部統制も構築することになりますが、具体的にＩＴに内部統制を組み込むための統制目的が「ＩＴのコントロール目標」といわれるものです。ＩＴのコントロール目標もまた経営者が情報システムを有効なものとするために、経営者が設定することとなります。

ＩＴのコントロール目標としては、例えば、下記のものが挙げられます。（ＩＴ実６号参照）

目　標	定　　義
準拠性 (Compliance)	会計原則、会計基準及び関連する法律等に合致していること
網羅性 (Completeness)	情報が漏れなく、重複なく記録されていること（完全性と表現される場合もあります）
可用性 (Availability)	情報が必要とされるときに利用可能であること
機密性 (Confidentiality)	情報が正当な権限者以外に利用されないように保護されていること
正確性 (Accuracy)	情報が正確に記録され提供されていること
維持継続性 (Maintainability)	必要な情報が正確に更新されかつ継続使用が可能なこと
正当性 (Approval)	情報が正規の承認手続を経たものであること

ＩＴのコントロール目標は、通常、アサーションと直接的に関連するものではありませんが、アサーションから導き出される重要な虚偽表示リスクに対応する内部統制を監査人が評価する上で、ＩＴのコントロール目標の達成度合を検討することが役立つ場合があります。

例えば、可用性は、システムが安定稼動していることを意味します。システムの運用が不安定で頻繁に中断されるような場合には、重要なデータが喪失してしまう、また、誤った処理が実行され誤ったデータが登録されるなどのリスクがあります。可用性の欠如が、特定のアサーション・レベルの重要な虚偽表示リスクに直接に結び付くものではありませんが、データ自体が破損することは、会計データの正確性、網羅性

を損なうことにつながり、重要な虚偽表示リスクにつながることがあります。機密性の具体的な実装は、例えば、パスワード等によるアクセス・コントロールですが、機密性の欠如は、プログラムやデータへのアクセスを容易にし、その変更や破壊を容易にします。これも重要な虚偽表示リスクにつながることがあります。

アサーション・レベルの重要な虚偽表示リスクに対する内部統制を考慮することは、具体的な重要な虚偽表示リスクをアサーションから導き出し、内部統制を考慮することになります。例えば、売上、売掛金の虚偽表示は架空売上、架空売掛金ですが、それは、発生、実在性のアサーションを基に具体的な重要な虚偽表示リスクを求めることになります。記録された取引が企業に関連しているか、実際に存在しているかがリスク評価のポイントになります。具体的に売上取引が実際にあったかは、得意先からの注文が本当にあったか、また、その注文に従って出荷され、先方に到着、又は検収されたかによって検証されます。どの時点で売上を認識するかは商取引の実態に沿って判定することになります。ＩＴを利用して売上を計上する場合に、架空取引を排除するために実装されるべきＩＴのコントロール目標は、まずは受注データの正当性、正確性、網羅性です。あらかじめ取引先審査の手続に基づき正規に登録された相手先からの注文のみが受注され、その注文内容が正確で漏れがなく重複もないための内部統制が求められます。そのデータに基づいて、出荷指図、出荷が行われることにより、売上の発生のアサーションが達成されます。正当性の具体的な実証はＩＴを利用した承認システムによる業者登録の承認や受注承認、受注データからのみ出荷データが作成される仕組みにより担保されます。

ＩＴのコントロール目標である「網羅性」は、受注から出荷等のデータが漏れなく、重複なく捕捉され、収集され処理されることを意味します。一方、監査対象期間の取引種類と会計事象に係るアサーションの「網羅性」は、記録すべき取引や会計事象がすべて記録されていることを意味します（監査基準員会報告書 315 A107 項）。つまり、ＩＴのコントロール目標である網羅性は受注データに誤りがあった場合にも、そのデータが修正されるまで、エラー表示がされ、処理される仕組みをＩＴに組み込むことです。例えば、販売システムからデータが網羅性を確保して会計システムに転送された結果として、会計上記録すべき売上の記録がすべて記録されるアサーションに結び付くことになります。ただし、元の売上システムのデータの正確性、正当性の確保がないと処理されたデータが会計上記録すべきデータであるかの最終的な内部統制にはなりません。

なお、ある重要な虚偽表示リスクの発見及び防止のために実装する内部統制は、その他の重要な虚偽表示リスクの発見又は防止することに役立つ場合があります。販売システムの受注入力時に得意先のマスター・ファイルとの存在性チェックは、同時に正確性と正当性を担保し、それによって発生と実在性のアサーションを満たすことになります。もし、マスター・ファイルとの存在性チェックがされずに、架空の出荷先

入力が可能な場合には、実在しない売上取引が計上され、発生と実在性のアサーションは達成されない可能性があります。他に有効な内部統制が存在しない場合には、重要な虚偽表示リスクが高まります。

Ⅵ　評価したリスクに対応する手続

Q21：リスク対応手続（運用評価手続）としてのＣＡＡＴの利用法について教えてください。

A21：

監査人は、アサーション・レベルの重要な虚偽表示を防止又は発見・是正する内部統制について、その運用状況の有効性を評価するために運用評価手続を立案し実施します。監査人が行う運用評価手続においては、監査対象期間全体からサンプルを抽出し、運用状況に係る証跡を確かめることによって、当該内部統制が実際に全期間にわたって有効に継続して運用されていることに関する監査証拠を入手する場合があります。

この場合のサンプル抽出については、監査基準委員会報告書 530「監査サンプリング」において、無作為抽出法や系統的抽出法について乱数ジェネレーターを利用するＣＡＡＴを想定したサンプル抽出が例示されています。

また、監査人は、サンプリングリスクを高めることなくサンプル数を減少させるため、母集団の階層化を行うことがあります。各階層に含まれる項目の持つ特性のバラツキを抑えるための分析にＣＡＡＴを利用することも考えられます。

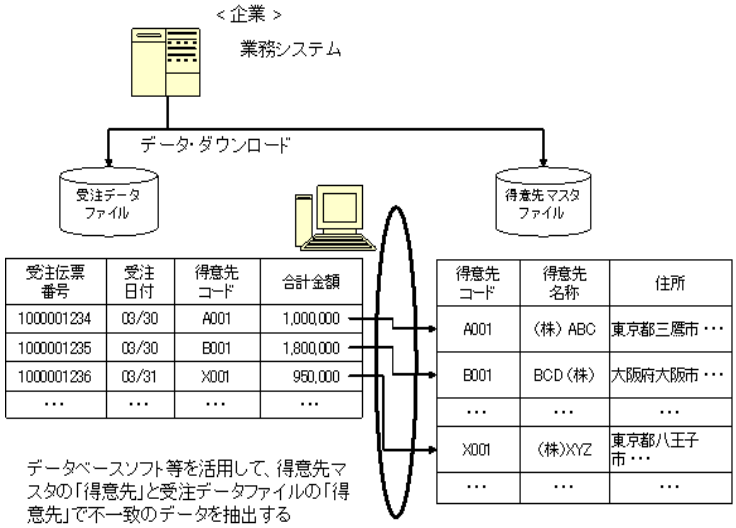
なお、実務ではサンプルによるテストを行う場合、リスク対応手続のうち、運用評価手続のためか実証手続のためかが区分しにくい場合もあり、同時に兼ねているケースもあります。サンプル抽出のみでなく、例えば、販売取引に関する内部統制において、「受注入力は得意先マスター・ファイルに登録されている得意先からの注文についてのみ入力することができる」という内部統制がある場合に、取引の発生というアサーションに対し、監査人はＣＡＡＴを適用することによって効果的かつ効率的な監査を実施することができます。すなわち、得意先マスター・ファイルに登録されていない得意先が入力できないことを確かめますが、ＣＡＡＴを利用することにより、得意先マスター・ファイルに登録されていない得意先が受注データファイルに存在していないことを確かめることが可能となります（図表２参照）。

なお、この方法のみでは当該自動化された業務処理統制自体の有効性を検証し直接的心証を得ているわけではありませんが、得意先マスター・ファイルへ未登録の得意先からの注文入力がなされるリスクが顕在化していないことについては確かめることはできます。

さらに、再実施や再計算の具体的な手法としてＣＡＡＴを用いることも考えられま

す。例えば、監査基準委員会報告書 500「監査証拠」（以下「監査基準委員会報告書 500」という。）A19 項では、再計算は手作業によって又はＩＴを用いて実施する旨の記載があり、これらの監査手続の実施にＣＡＡＴを利用することが想定されています。

図表２



Q22：「自動化された業務処理統制」について、前年度からの変更がないことを確かめる監査手続について教えてください。

A22：

監査人は、「自動化された業務処理統制」について、まず、前年度からの変更の有無を質問により確かめます。変更がない場合の回答の裏付けを得るための手続として、以下のような方法や前年度と同様の検証手続の実施が考えられます。

１．プログラムやシステム設定等、システム自体に全く変更がなく、評価対象の「自動化された業務処理統制」については変更がない場合

(1) 市販されている簡易なパッケージ・ソフトウェアをカスタマイズなく利用している場合

例えば、バージョン情報を確かめることで当該ソフトウェアに更新があったかどうか分かります。前年度とのバージョン番号の比較や最終更新日付を確かめることで、監査対象期間中に変更がなかったかどうかを確かめることが可能です。バージョン情報については、マニュアルの閲覧や被監査会社の担当者への質問等で容易に確かめることが可能です。

なお、システム設定の変更等の有無についても留意します。

(2) 自社開発ソフトウェアやＥＲＰを利用している場合

全般統制の評価手続においてプログラムのバージョン管理台帳や変更管理台帳の正確性及び網羅性の心証を得ている場合は、当該台帳等に変更案件がないことをもって、システム自体に変更がないという心証を得ることができます。

２．プログラムや設定等、システム自体に変更はあるが、評価対象の「自動化された業務処理統制」については変更がない場合

(1) 市販されている簡易なパッケージ・ソフトウェアをカスタマイズなく利用している場合

通常、バージョンアップ時には、機能改善又は追加された箇所がリリースノートに記載されています。当該リリースノートの内容を確かめることで、「自動化された業務処理統制」に変更があったかどうかの心証を得ることができる場合があります。

(2) 自社開発ソフトウェアやＥＲＰを利用している場合

プログラム等に関する変更の有無について、プログラム管理台帳や変更管理台帳の記載を確かめることで、「自動化された業務処理統制」に関連するプログラムやプログラムの変更を伴わない設定等の変更の有無に関する心証を得ることができる場合があります。また、台帳の記載からのみでは十分な心証を得られない場合には、追加手続を実施します。

追加手続の実施に当たっては、ライブラリ管理ソフトウェアを利用してプログラムのバージョン管理をしている場合や、一部のＥＲＰにおいてシステム的な変更履歴が取得可能な場合があります。これらはシステム的な変更履歴であるため、手作業で管理されている各種台帳よりも信頼性が高いので、入手可能であれば当該変更履歴を確かめることで、システム変更の有無に対する高い心証を得ることができます。ただし、開発担当者と運用担当者の職務分離の状況、ＯＳ／ＤＢＭＳ（DataBase Management System）へのアクセス権やライブラリ管理ソフトウェア及びＥＲＰの設定状況等によっては、当該変更履歴の信頼性が低下する場合もあることに留意します。なお、一連の手続の実施に当たってはＩＴの専門家の関与の検討が望まれます。

仕様書や手作業の管理台帳といった文書のみを確かめるか、実際のシステム等の状況までを確かめるか、すなわちどの程度まで心証を得る手続を実施するかについては、システムの規模、複雑性、安定性、過去における障害の発生状況又は全般統制の整備及び運用状況等を勘案して決定します。

Ⅶ　全般統制の不備対応

Q23:全般統制に不備があった場合の取扱いはどのようになるのでしょうか。

A23：

1．全般統制に不備がある場合の取扱い

全般統制に不備がある場合には、関連するすべての業務処理統制及びアサーションに影響が及ぶことに留意します。

つまり、全般統制は、情報システムの継続的かつ適切な運用を確保することにより、業務処理統制が有効に機能するよう支援するものですから、たとえ業務処理統制が有効に機能していたとしても、継続的な運用を保証する全般統制に重要な不備があれば、情報システムの内部統制は有効に機能しないため、統制リスクが高まることになります。

基本的には、以上のような結論になりますが、全般統制が有効に機能していないといっても、無条件に情報システムの内部統制に依拠できないという結論に至るものではありません。全般統制の中でも、ある財務諸表の虚偽表示を防止ないし発見できる業務処理統制との関連性が薄い部分についてのみ信頼性がない場合には、当該虚偽表示の防止又は発見に対応する業務処理統制の有効性に関しては、情報システムの内部統制に依拠できることがあります。

例えば、全般統制のうちシステムの企画業務だけに問題点がある場合には、すでに稼動している業務アプリケーションの業務処理統制と運用とは関連性が薄いため、統制リスクが高いと判断しない場合もあります。

全般統制の不備によるデータの破壊、不正なプログラム変更の可能性などにより情報の信頼性が損なわれるなど、統制リスクが高いと判断される場合に、監査人は、リスク評価手続の追加の必要性及び実施する手続の内容、範囲等を検討する、あるいは実証手続の件数を増加するなど何らかの追加手続を実施することになります。例えば、不正なプログラム変更が容易に可能であるといった不備が全般統制に存在する場合には、関連する業務処理統制に対するリスク評価手続及びリスク対応手続のうちの運用評価手続の範囲を拡大し、また評価の頻度を増やす等の対応を行います。

2．全般統制の不備についての考え方の例示

全般統制の不備を評価する際には、そのシステムの状況や実際に財務諸表の数値にどのような影響があるかを考慮して判断します。

(1) バックアップデータの保管

バックアップデータの保管において求められるのは、財務報告の作成のための基礎データが失われるリスクの低減です。よって、要請される管理レベルは、財務報告目的としては、データの復旧が可能なレベルです。

バックアップデータの外部保管は、必ずしも、外部業者への保管を要請しているものではありません。サーバルームにバックアップデータが保管されている場合に火災等によってサーバと同時にバックアップデータが消失し、財務報告の作成のための基礎データがすべて失われてしまうリスクを低減するために別の場所に保管することにあります。当該リスクを考慮して、サーバのデータが失われても財務報告の作成に必要なデータが復旧可能な状態で確保されているかが重要であり、保管場所が社内か外部倉庫かが本質的な問題ではありません。複数拠点を有する企業では、自社内の各拠点を利用することで、必ずしも外部の業者を利用しなくても外部保管は可能であり、拠点間で相互にサーバがレプリカを持つ場合には、媒体（メディア）による保管がなくても目的は達している場合もあります。

(2) アクセスログの取得

情報システムに関するあらゆるアクセスログを取ることが必須ではありません。アクセスログを取得し保管することが内部統制の目的ではなく、正当な職務権限による財務データへのアクセス以外の不当な入力や改ざんがないかを監視することに意味があります。例えば、アプリケーションへのアクセスについて、そのログをどのレベルで取得しなければならないかは、そのアプリケーションの構成や利用人数、保管場所などの環境を考慮することになります。また、スタンドアロンの経理システムで、施錠により部外者の立入り制限等、業務端末への物理的なアクセス制限があり、経理担当者が業務時間に管理者の監督下でのみ経理データを入力し、入力後に入力者が伝票に押印するなどの内部統制がある場合には、厳密なアクセスログが必要とされないことも考えられます。ただし、金額や科目の訂正等についてのログや伝票等の記録により、訂正を誰がいつ実施したかについての証跡を確保することは必要と考えられます。ログはあくまで事後的な発見的統制であり、正当な権限のある入力者でない人が入力できないような防止的な統制、アクセス権と入力の職務権限が一致している等の内部統制と組み合わせて重要な虚偽表示リスクを低減することが重要です。

(3) 職務の分離と権限の分掌について

職務の分離と権限の分掌は、職務を分離することが内部統制の目的ではなく、兼務すると牽制機能が働かなくなる職務を分けることにより、財務報告の正当性を確保することが目的です。よって少人数で職務の分離が困難な場合については全体として財務諸表に与える影響を考慮して、リスクとその内部統制の有効性を検討し、職務の分離と権限の分掌の不備を補完する内部統制を検討することになります。例えば、開発とプログラム保守は兼務可能ですが、運用については不正なプログラムの改ざんを防ぐために職務を分離して異なる要員が実施することが内部統制として重要です。よって小規模企業等においてシステム要員が少数で

あり、要員を分けることが困難である場合には、そのプログラム保守の正当性、つまり、不正なプログラムの作成をどのように防止又は発見する内部統制があるかを検討することになります。開発、プログラム保守要員が運用の業務を兼務する場合には、プログラム変更には管理者が必ず、事前に承認することや、プログラム保守の記録を取り、管理者が確認するなどの内部統制でリスクを低減できる場合もあります。これらの補完する内部統制を十分とするか否かは、実際のシステムや企業の実情により、リスクを勘案して決定することになります。システムの中には、長期間にわたり、全くプログラム変更がない場合もあり、プログラム保守要員と運用要員を別途に置くことが非現実的である場合もあります。全般統制のリスクは、そうしたシステムの利用状況等を考慮した上で、不正なプログラム改ざんのリスクが低減可能な内部統制があるかを評価し、一律に職務の分離と権限の分掌の有無のみで内部統制が十分かどうかを判定するものではないことに留意します。

３．全般統制の不備に対する一般的な手続

監査人が特定の全般統制の不備を発見した場合は、(1)当該不備を補完する他の全般統制を評価する、(2)関連する業務処理統制の評価手続を拡大する、又は(3)実証手続を拡大する、といった対応があります。

(1) 当該不備を補完する他の全般統制を評価する対応

全般統制のリスクの評価においては、ＩＴのコントロール目標の達成度を考慮に入れるため、監査人が特定の全般統制の不備を発見した場合において、同じ目的を達成する他の全般統制によりリスクを低減できることがあります。

一般に、監査人は、リスク評価手続の実施の際に防止と発見の組合せによって、同じ目的を達成する他の全般統制によりリスクを低減できるかを考えます。例えば、監査人が防止的な全般統制の不備を発見した場合において、事後の承認やログのレビュー等の発見的な全般統制が有効に機能しているときは、リスクが低減されていると判断できることがあります。

なお、監査人が全般統制の不備に基づくリスクが発現していないことを確かめることで、リスクに対応できる場合があります。例えば、プログラムの変更管理に不備があった場合、対象となる業務処理プログラムが期間中変更されていないことを、対象プログラムごとの変更履歴や、当該プログラムの登録日付により確認することで確かめることなどが考えられます。

(2) 関連する業務処理統制の評価手続を拡大する対応

全般統制に不備が存在した場合には、当該全般統制により継続的な運用を支えられている業務処理統制の有効性が崩れてしまうため、そのままでは情報システムの内部統制に依拠できなくなる可能性があります。ただし、全般統制の不備の

影響を受ける業務処理統制の範囲を特定し、業務処理統制の運用評価手続の範囲（件数、期間等）を拡大する等の対応を行います。（ＩＴ実６号第 53 項参照）

また、監査人は、インプットデータとアウトプットデータの突合や、データ間の整合性の検討、計算結果の再計算などにより、結果が正しく処理されているかを検証することもできます。その際には、情報システムに対して実施されるテストをすべて再現するわけではなく、財務報告の作成に影響する部分について必要な手続を実施することに留意します。

(3) 実証手続を拡大する対応

監査人は、(1)又は(2)の対応により、十分な心証を得られない場合には、財務諸表項目レベルの重要な虚偽表示を発見するために実施する実証手続（取引、勘定残高、開示等に対する詳細テストと分析的実証手続）（監査基準委員会報告書 330 A41 項から A57 項参照）を実施します。

Q24：システムに組み込まれた業務処理統制の整備状況が、仕様書等により評価できない場合に想定されるリスクの評価及び対応例について教えてください。

A24：

１．仕様書等の不備が全般統制の評価手続に与える影響

システムの仕様書等は、システムの企画開発の段階から、システムの設計に変更を加える保守の段階まで、設計の内容を明らかにするために作成されます。現状のシステムについての仕様等を記録するプロセスの全般統制の不備としては、(1)仕様書等が作成されておらず、もともと存在しない場合、(2)仕様書等が作成されているが、記録が不完全又はシステムの改修の記録がないなど不十分である場合、とがあります。

上記(1)又は(2)である場合、監査上必要とされる業務処理統制がどのように設計されているかが判明しないままで整備状況を評価することになる点に留意します。

２．仕様書等の機能

システムの仕様書等は、一般的に次のような点に留意して、確立したプロセスにおいて設計の内容を記録として残したものです。

(1) 企画開発段階において記述の標準化を図り、記述を一定のルールの下で作成して判読を容易にする。また、設計途中での変更の管理をし、記述の不整合や漏れを防止する。

(2) 保守段階においてシステムの変更管理の手順を定め、変更の履歴を残し、変更内容の記述を標準化する。

監査人はこれらの点に留意して、業務処理統制の整備状況を評価するために必要な範囲の仕様書等が適切に作成されていることを確かめます。

３．仕様書等の不備が存在した場合の対応例

監査人は、システム開発者やユーザに対してシステムに組み込まれている業務処理統制について質問し、仕様書等により確かめます。しかし、仕様書等が不十分で確かめられない場合には、次のような対応が考えられます。

(1) 仕様書等以外の書類等による検討

① 監査人は、ユーザマニュアル等のユーザ向け操作手順書により業務処理統制を読み取る。この場合、ユーザマニュアル等は、システム開発者が作成したものやパッケージ・ソフトウェアのベンダーから提供されたものであることが望ましい。

② 監査人は、業務処理統制となるプログラムのソースコードを利用し、その内容を確かめる。プログラム上に記述されているコメント（コンピュータ言語で記述されているソースコードではなく、人がプログラムの修正などのメモとして記述した注釈）が十分でない場合は、他の手続と組み合わせて実施することにより、業務処理統制を確かめる。

この方法は、ソースコードが入手可能で、かつ、理解できること及び、ソースコードと本番環境に実装されているプログラムとが一致していることを確認できることが前提となる。また、実施に当たっては、ＩＴの専門家の関与が必要になる場合がある。

(2) 上記の対応が取れない場合の検討

(1)の対応が取れない場合には、監査人は、例外的に運用状況の評価手続を実施することにより確かめることが考えられます。ただし、この場合はシステムの設計内容が明確に把握できないため、質問やユーザマニュアル等により確認できた特定の機能しか確かめられないこと及び特定していない処理結果が確認された場合に不正な処理か否かを判断する必要があることに留意します。

① 業務の実際の操作や制御画面を観察し、組み込まれている業務処理統制を確かめる。

② アクセス権限の制御、承認入力や与信設定等の実際のシステムの設定情報を確かめる。

③ 原始証ひょうや入力データ等を用いた処理の結果について、手作業やＣＡＡＴによる再計算等により、組み込まれている業務処理統制を確かめる。

Q25：データベースの会計データを直接修正する手続に不備が存在した場合に想定されるリスクの評価及び対応例について教えてください。

A25：

「データベースの会計データを直接修正する手続」とは、会計システムなどのアプ

リケーションを通さず、データベースの更新権限を持つＩＤを使って、データベース上の会計データに直接アクセスし、データの追加、変更又は削除を行うことをいいます。

１．データベースの直接修正に関する全般統制に不備が存在したことにより想定されるリスク

アプリケーション上に保持されている会計データは、各業務プロセスにおいて各種の承認手続を経て登録や計上されたものであり、その修正方法についても業務プロセス上で定められ、アプリケーション上で実行されているのが通常です。しかしながら、業務上修正が必要であるにもかかわらず、アプリケーションの機能ではユーザにより会計データの修正を行えない場合や、バグなどの影響により、会計データがユーザの意図しない状態に変わってしまった場合には、例外的にデータベースを直接修正しなければならないことがあります。データベースの直接修正に対する全般統制に不備が存在した場合には、業務上は意図しない内容の会計データの修正が行われるリスクが存在します。

なお、データベースの直接修正が頻繁に発生しているような場合には、監査人は、それ自身が重要な虚偽表示リスクとなる可能性があることに留意します。

２．想定されるリスクに対する内部統制

データベースが直接修正されるリスクに対する内部統制としては、一般に次のようなものが考えられます。

(1) データベースの直接修正に関する承認

プログラムの変更手続と同様に、データベースの直接修正について変更の申請及び承認に関する内部統制を整備し、運用する必要があります。例えば、データベースの直接修正について事前に申請を行い、適切な権限者の承認を得ていることが必要となります。また、修正後の会計データに対する承認の手続も必要です。

(2) 職務の分離

職務の分離を適切に実施することにより、データベースの直接修正に関するリスクを低減することができます。例えば、ユーザ部門が自ら会計データを修正するのではなく、依頼によりシステム部門が修正を実施します。

(3) 更新権限の限定

データベースの更新権限を付与する人員は、システム部門内でも一部の担当者に限定し、それ以外の担当者への更新権限の付与を制限します。

(4) 更新ログの分析によるモニタリング

データベースの直接修正が行われた場合には、その内容を後で確かめることができるよう、修正に関するログを残し、モニタリングします。

３．全般統制に不備が存在した場合の対応例

(1) データベースの修正に関する承認手続に不備が発見された場合

データベースの修正に関する承認手続に不備が発見された場合、監査人は、修正された内容の妥当性を個々に確かめることで、会計数値への影響の有無を評価することが可能と考えられます。また、データの直接修正に関するログと申請・承認書類とを突合することにより検出された不備以外には承認のない変更が存在しないことを確かめ、被監査会社が行ったすべての変更に問題がないことを根拠に不備に対する監査手続を実施し、十分な証拠を入手できたと結論づけることも可能と考えられます。

(2) 職務の分離及び更新権限の限定に不備が発見された場合

職務の分離及び更新権限の限定に関して、例えば、次のような状況があった場合には不備と考えられる可能性があります。

- データベースの更新権限者がプログラム開発や保守業務にも従事している。
- データベースの更新権限者がユーザ部門の業務にも従事している。
- データベースの更新権限者を特定できない（ＩＤやパスワードの共有、データベース管理業務に関係していないユーザへの更新権限の付与など）。

上記のような場合には、更新ログの分析によるモニタリングにより、全般統制の不備を補完することが可能と考えられます。監査人は、モニタリングの実施方法やその結果について評価又は検討が必要となります。

(3) 更新ログの分析によるモニタリングに関する不備が発見された場合

更新ログの分析結果により十分な心証が得られない場合には、監査人は、被監査会社に追加的に分析を依頼し、再度その結果を入手することを検討します。例外的に、分析の結果の検討ではなく、監査人自らがログを分析することで心証を得ることができる場合があります。

更新ログが適切に保管されていない場合には、監査人は、ログを利用したモニタリングの評価を有効に行うことができないため、「２．(4) 更新ログの分析によるモニタリング」に対する内部統制に依拠することができません。このような場合、監査人は、まず、「２．(1)データベースの直接修正に関する承認」、「２．(2)職務の分離」又は「２．(3)更新権限の限定」に対する内部統制の評価で十分に心証を得られるかどうかを確かめます。その際に、アクセスログを利用できる場合があります。

十分な心証が得られない場合には、監査人は、補完統制となる業務処理統制又は実証手続による対応を検討します。

Q26：システム部門が存在せず、担当者１名のみでシステムの管理を行っている場合に、プログラム開発担当者や保守担当者と運用担当者の職務の分離がされていないときに想定されるリスクの評価及び対応例について教えてください。

A26：

１．プログラム開発担当者や保守担当者と運用担当者の職務の分離の全般統制に不備が存在したことにより想定されるリスク

システム部門が存在せず、担当者１名のみでシステムの管理を行っている場合には、実際の業務で使用されているソフトウェアが稼動している本番環境に新規又は変更したプログラムを適用するに当たって、あらかじめ導入手順が明確に定められていたとしても、誤って又は故意に当該手順に従わずに行うことが可能です。これにより、データが不適切に修正されたり、機能の検証等が不十分なプログラムやバージョン違いのプログラムが本番環境に適用される可能性があります。

２．想定されるリスクに対する内部統制

システムの担当者が１名である場合には、プログラム開発担当者や保守担当者と運用担当者の職務の分離を行って内部統制を機能させることができません。

ただし、担当者が１名であっても、上位の権限者の事前承認や利用部門の動作確認を得ることによって、一定の牽制機能が期待できる場合があり、定められた手順に従って業務を実施したことについて作業記録を残す方法が考えられます。作業記録には、自動的に取得されるログだけではなく、紙に記録しているものも含まれます。作業記録には、業務の実施前に権限者が承認した結果、実際の作業内容、利用部門の動作の確認結果や作業の結果報告などが考えられます。

３．全般統制に不備が存在した場合の対応例

作業記録が残されている場合において、監査人は、プログラム等の重要な変更について適切に内容が記載されており、その作業記録に対して権限者による承認等が行われているかを評価し、当該変更について全般統制の不備の影響が小さいと判断できることがあります。

作業記録が残されていない場合には、関連する業務処理統制の評価手続又は実証手続を拡大するといった対応を取ることになります。

Q27：システム部門において、プログラムの開発担当者や保守担当者と運用担当者の職務の分離がされず、業務が運用されている場合に想定されるリスクの評価及び対応例について教えてください。

A27：

１．システム部門において、プログラムの開発担当者や保守担当者と運用担当者の職務の分離に関する全般統制に不備が存在したことにより想定されるリスク

プログラム開発担当者や保守担当者と運用担当者の職務の分離とは、一般的には、プログラム開発担当者や保守担当者と運用担当者の職務を区分し、前者の本番環境へのアクセスを認めない、又は一定の手続を定めてアクセスを制限することを指します。

しかし、障害が発生したときの対応が効率化されることや、ユーザ部門からの変更要求に迅速に応えられる等の業務的な利点を考慮し、プログラムの開発担当者や保守担当者が運用を担当している場合があります。

本番環境で稼動するプログラムは、新規に開発される場合又は変更される場合であっても、当初意図したとおりの動作をすることが十分にテストされ、品質が保証された上で業務に利用されることが必要です。職務の分離が十分でない場合には、開発担当者や保守担当者自身が本番環境に容易にアクセスできるため、自身で開発や変更したプログラムを、ユーザによる受入れテスト、移行承認等の他者のチェックを入れずに、本番環境で稼動させることができる状態にあります。このような管理体制では、相互牽制なく単独で本番用のプログラムを変更してしまうことが可能となることからプログラムの改ざんにつながるリスク、不適切な内容、バージョン違いのプログラムやデータが本番環境で適用されるリスクが存在します。

２．想定されるリスクに対する内部統制

システム部門の存在する被監査会社では、アプリケーションやデータベース等を開発又は変更するときには、ユーザ部門からの依頼として受け付けます。プログラム開発担当者や保守担当者が、開発環境において開発又は変更の作業を行い、運用担当者がプログラムを本番環境へ導入します。導入作業をプログラム開発担当者や保守担当者が行う場合でも、通常は本番環境への無制限のアクセスを認めず、一定の手続を定めてアクセスを許可します。プログラム開発担当者や保守担当者と運用担当者が同一の場合には、必要なチェックを受けることなく、本番環境にプログラムを導入することができるため、両者を分離して一定の牽制を働かせます。プログラム開発担当者や保守担当者の誤り又は故意による不適切な変更を避けるために、書面による承認プロセスの確立や、ワークフロー・システムが導入されます。また、プログラムの管理を行うライブラリ管理システムが導入される場合があります。

３．全般統制に不備が存在した場合の対応例

システム部門において、プログラムの開発担当者や保守担当者と運用担当者の職務の分離がされていない場合には、新規又は変更されたプログラムの品質等が十分に担保されないリスクがあります。ただし、監査人は、次のように不備が存在した

全般統制を補完する他の全般統制によりリスクが低減されていると判断できる場合があります。

システム部門の存在する被監査会社では、アプリケーションやデータベース等を変更するときには、ユーザ部門からの依頼に基づき作業を実施します。ユーザ部門からの依頼事項は、ワークフロー・システムや書面で起票され、ユーザ部門内での承認を受けた上でシステム部門に連絡され、システム部門内で台帳管理されます。

さらに、システム部門では、プログラムの本番環境への移行や、プログラムの修正等の実施した作業内容の記録を残す手続が決められており、これらの記録には、実施したテスト結果、システム部門内の上位者による承認、ユーザ部門などの検証及び本番環境を変更した作業日時などが含まれます。これらの記録を監査人が確かめることにより、リスクが低減されていると判断できる場合があります。

システム部門が、システム的にプログラム変更履歴、本番環境へのアクセス記録や本番環境での操作履歴等の各種ログを記録し、これらのログと作業記録とを検証している場合があります。また、システム部門において、品質管理の一環でプログラムの事後レビュー等を実施している場合もあります。これらにより、監査人は、さらにリスクが低減されていると判断できる場合があります。

Q28：システムの開発過程においてユーザ受入れテストが実施されていない場合に想定されるリスクの評価及び対応例について教えてください。

A28：

1．ユーザ受入れテストに関する全般統制に不備が存在したことにより想定されるリスク

ユーザ受入れテストは、システムを本番環境に移行する前のユーザによる最終確認フェーズであり、本番と同等の環境で、実際にシステムを利用するユーザが参加して、関連する業務処理統制を含む機能が正常に機能するかについて確かめるものです。システムの開発過程においてユーザ受入れテストが行われない場合、業務に必要な機能の確認が適切に行われずにユーザ部門が要求する業務要件を満たしていないシステムが本番環境にリリースされるリスクがあります。

2．想定されるリスクに対する内部統制

システムの開発過程において、ユーザの業務要件に基づきシステムの仕様が決定され、プログラムが作成されます。システムにユーザの業務の要件が適切に反映されているかどうかを確かめるには、システム部門のテストだけでは十分ではない場合があります。そのため、業務要件を理解した適切な能力を有するユーザが、テスト項目や内容を十分に検討し、テストを行います。

３．全般統制に不備が存在した場合の対応例

ユーザ受入れテストが実施されていない場合には、業務処理統制を含む機能が、システムに実装されているかの検証が十分に行われていないというリスクが想定されます。このような場合には、次のような対応が考えられます。

(1) 通常のシステムの開発過程においては、ユーザ受入れテストの前にシステム部門が様々なテストを実施します。システム部門が実施する一連のテストにおいても、システムに必要な機能が充足されているかどうかの検証を行うことになります。システム部門によるテストにおいても、十分に業務を熟知している担当者がユーザ視点も踏まえてテストを実施している場合や、極めて簡易なシステムのためユーザ自身が確認を行う必要性が低い場合などにおいて、システム部門のテストでユーザ受入れテストと同等とみなせることもあります。

(2) ユーザが、あらかじめシステムの本番移行後の試用期間を設定し、適切な数値の集計や業務処理統制が機能しているかを確かめ、要求する業務処理統制を含む機能が実現されていない場合においては、修正を依頼していることがあります。監査人は、これらの修正依頼の記録を確かめることで、リスクが低減されていると判断できる場合があります。

Q29：会計システムの特権ＩＤの管理が不十分で、必要最小限のユーザ以外にも権限が付与されている場合に想定されるリスクの評価及び対応例について教えてください。

A29：

１．会計システムの特権ＩＤの管理に関する全般統制に不備が存在したことにより想定されるリスク

会計システムの特権ＩＤとは、例えば、すべての勘定マスター情報、パラメータ設定値の変更や会計データの作成、変更、削除及びそれらの権限の設定等が可能な、操作に制限を受けない特別なＩＤをいい、通常はシステム管理者が使用するＩＤとして想定されています。

特権ＩＤの管理が不十分で、必要最小限のユーザ以外にも権限が付与されている場合は、例えば、次のような会計データに対する不正や誤謬についてのリスクが高まることになります。

・ 特権ＩＤを用いて本来会計伝票の修正を赤黒処理すべきところを直接修正したり、締め後のデータを直接修正するなど、必要な内部統制を回避して修正するリスク

・ 特権ＩＤの使い方や効力を理解していないユーザが、データやマスターを変更、破壊してしまうリスク

・　経理部門の上級管理職になりすまし、自ら経費の水増し伝票を起票し、かつ承認することも可能になってしまうなど、自ら起票した伝票を自身で承認するリスク
・　特権ＩＤが共有されており、誰が使用して会計データを修正したかを特定することが困難なリスク

２．想定されるリスクに対する内部統制

特権ＩＤは強力な権限を有しているため、必要最小限の者のみに付与されるべきであり、通常の操作に使用するＩＤの管理に加えて、例えば、次のような内部統制が考えられます。

・　特権ＩＤと通常の操作に使用するＩＤとを区別し、特権ＩＤの使用を必要とする者でも会計システムの通常利用においては、通常の操作に使用するＩＤを使用する。
・　特権ＩＤの管理をシステム部門に移管し、ユーザ部門で特権ＩＤの使用を必要とする場合には、その都度に使用できる特権ＩＤの貸出し及び返却を管理する。特権ＩＤを都度貸出しする場合、返却後にパスワードを変更する。
・　個々の会計担当者の職責及び職務権限に応じてシステム上の権限が付与されるように、機能を限定した管理用のＩＤを個人ごとに設定し、発行する。
・　特権ＩＤの操作に関しては、操作内容を文書化し、ユーザ部門管理者の承認を受ける。
・　会計システムのログの取得機能を活用し、事後的にモニタリングする等の発見的な内部統制を組み込む。

３．全般統制に不備が存在した場合の対応例

特権ＩＤの管理の不備の内容や程度によって、会計データが歪められているリスクの程度や可能性は変わるため、監査人は、次のような対応を検討することが考えられます。

(1) 代替的又は補完的統制によりリスクが低減される程度を評価

例えば、会計伝票がシステム出力を含む紙媒体で運用され、起票者及び承認権限者の印が押印されていることや、月次締めで他の帳票との照合を行うことなどの手作業による内部統制が有効であれば、監査人は、会計データが歪められているリスクが手作業による内部統制により低減されていると判断できる場合もあります。

また、特権ＩＤの使用状況についてログの適時かつ適切なモニタリングが整備及び運用されていれば、特権ＩＤの管理の不備による不正や誤謬が実際に発生したとしても、適時にそれが発見される可能性が高まります。したがって、監査人

は、会計データが歪められているリスクは低減されていると判断できる場合もあります。

(2) 特権ＩＤの利用について不正や誤謬がないことを直接的に検証

監査人自らが会計帳簿や伝票を閲覧し、アクセスログを検証する等の手続を実施することにより、本来通常の操作に使用するＩＤを用いてアクセスや操作がされるべきところに特権ＩＤによってアクセスや操作が行われていないこと、又は特権ＩＤによって会計データが不正に操作されているリスクが高くないことを確かめることができる場合があります。

Ⅷ　実証手続

Q30：リスク対応手続（実証手続）としてのＣＡＡＴの利用法について教えてください。

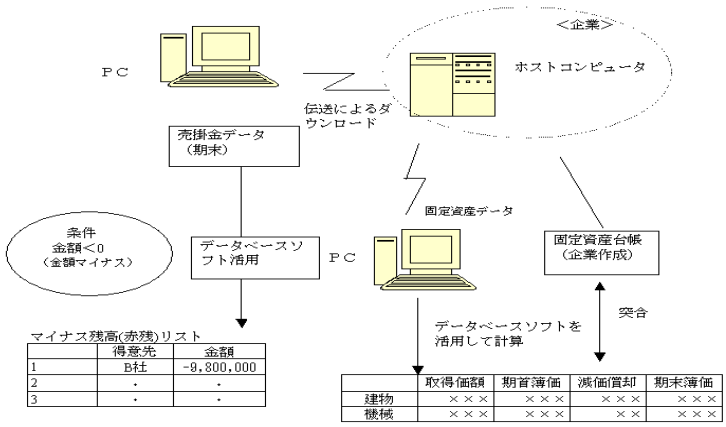
A30：

監査基準委員会報告書 500 A19 項では、「再計算は、手作業によって又はＩＴを用いて実施する」 との記述があります。ＩＴを用いた再計算（ＣＡＡＴによる再計算）は、Ｑ９で述べたリスクについて十分認識する必要はありますが、積極的な活用が望まれます。

監査サンプリングについてQ21 で詳細に述べていますが、実証手続としてのサンプルの抽出においてもＣＡＡＴは有効ですし、分析的手続や計算突合においてＣＡＡＴは効果を発揮します。実証手続としてＣＡＡＴを利用する場合の適用例としては、以下のようなものが考えられます（図表３参照）。

- 期末売掛金残高についてマイナス残高の有無を確かめ、マイナス残高発生についての被監査会社による発生理由調査結果と照らし合わせる（売掛金データベースから期末残高がマイナスのものを抽出する）。
- 売掛金残高に対して滞留月数６か月（180 日）以上の売掛金残高を抽出するとともに、滞留発生についての被監査会社による発生理由調査結果と照らし合わせる（売掛金データベースにおいて、例えば、回収予定日がデータ項目としてあれば、そこから期末日時点で回収予定日を 180 日経過しているものを抽出する）。
- 固定資産における減価償却費の再計算を実施して計算結果を照合する（固定資産データベースから取得価額、取得日、耐用年数などの必要なデータ項目を抽出し、このデータ項目からあるべき減価償却費を計算し、実際の固定資産データベース上の減価償却費との一致を確かめる。）。

図表３



監査基準委員会報告書 240 では、アサーション・レベルの不正による重要な虚偽表示のリスクに対応する監査人の手続が例示されています。

例えば、より証明力が強く適合性の高い監査証拠を入手するために、又は裏付けとなる追加的な情報を入手するために、実施する監査手続の変更が必要となり、重要な勘定や電子的な取引ファイルに含まれるデータについてより多くの証拠を集めるためにＣＡＡＴを利用する場合があります。

また、実施する監査手続の範囲の変更が必要となる場合に、ＣＡＡＴを用いることにより、電子的な取引ファイルと勘定ファイルに対するより広範囲な手続の実施が可能となる場合があると例示されています。

このように、実証手続においてＣＡＡＴを活用することは、監査の効率化につながるとともに、今までできないと考えていた手続を実施することも場合によっては可能となりますので、この点では監査の質という面でも向上につながると考えます。

Ⅸ　専門家の業務の利用

Q31：ＩＴの専門家を関与させる際の留意点にはどのようなものがあるでしょうか。

A31：

「監査人の利用する専門家」は、「監査人が十分かつ適切な監査証拠を入手するに当たって、会計や監査以外の分野について専門知識を有する個人又は組織の業務を利用する場合の当該専門知識を有する個人又は組織をいう」とされています（監査基準委員会報告書 620「専門家の業務の利用」第５項(1)）。専門家には「監査人の雇用する内部の専門家（監査事務所又はネットワーク・ファームの社員等又は専門職員（非常勤者を含む。））」と「監査人が業務を依頼する外部の専門家」が含まれます（同第５項(1)）。

１．監査人の雇用する内部の専門家

監査事務所又はネットワーク・ファームに所属する者で、監査を実施する社員等及び専門職員によって監査チームは構成されます（監査基準委員会報告書 220 第６項(5)）。専門職員には会計や監査以外の分野において専門知識を有する個人も含まれます（監査基準委員会報告書 220 第６項(11)）。

２．監査人が業務を依頼する外部の専門家

外部の専門家を利用する場合には、当該専門家は監査チームを構成しません（監査基準委員会報告書 220 第６項(5)）。例えば、ＩＴに関連する内部統制の評価を実施する際に依頼する専門家が該当します。

関与させる場合には、事実の確認や個別で具体的な手続に関する結果について採用するか否かを判断するよりも、例えば、リスク評価全般を監査人と一緒に実施する場合が多いと考えられます。したがって、監査人がＩＴの専門家を関与させる場合には、その専門家が単にＩＴの知識のみではなく、情報システムに関する重要な虚偽表示リスクの評価について必要な技能、知識及び経験を有していることが求められることに留意します。

ＩＴの専門家を関与させるか判断する際には、監査業務においてＩＴに関連する事項がある場合、必ずＩＴの専門家を関与させなければならないわけではないということに留意します。ＩＴの専門家を関与させるかどうかについて明確な判断基準はありませんが、例えば、企業においてＩＴ化された環境が構築されていることによりＩＴを利用した複雑な情報システムとなっている等、監査人の知識や技術では十分な対応が困難な場合や、監査人が実施するよりも効率的に実施可能と認められる場合には、ＩＴの専門家を関与させることを検討する余地があるといえます。

ＩＴの専門家を関与させる一般的なケースとしては、全般統制の理解と評価に関して関与させるケースが挙げられます。全般統制に関して重要な不備の有無及びその影響度の把握、代替的手続の把握、不備に対する改善提案等を実施する際には、ＩＴに関する専門的知識や経験が要求されるため、ＩＴの専門家の関与が必要となることが想定されます。また、業務処理統制の理解に関しては、アプリケーションによって自動化された内部統制の理解に、ＩＴの専門家を関与させることで効率的に手続を実施することが可能な場合があります。

ＩＴの専門家を利用する際の留意点としては、①依頼時のコミュニケーション及び②継続的なモニタリングが挙げられます。

依頼時のコミュニケーションとしては、第一に作業目的を明確に伝える必要があります。作業目的は、ＩＴの専門家が実施する手続や成果物に重要な影響を与えるため、監査人は対象となる情報システムの範囲及び監査人が想定するリスクをＩＴの専門家と具体的かつ十分に協議し、想定した作業結果が入手できるよう努める必要があり

ます。また、手続や成果物のイメージを確かめる意味で、監査調書等の定型書式を提供することも有用と思われます。

依頼時のコミュニケーションが十分に行われていたとしても、作業の過程における想定外の事象の発生、ＩＴの専門家の能力不足等により、監査人が期待した結果が入手できない可能性があります。このため監査人は、専門家の業務内容について定期的な報告を受け、適時に対応ができるよう、継続的にモニタリングすることが必要となります。特に、「監査人が業務を依頼する外部の専門家」を利用する場合には、継続的なコミュニケーションが困難になる可能性があるため、注意が必要です。

ＩＴの専門家による作業結果を監査証拠として利用するかについては、あくまで監査人が判断する必要があります。すなわち十分かつ適切な監査証拠となっているか、監査人が自ら判断します。具体的には、例えば、監査人が依頼時に設定した基準（手続内容、対象期間、範囲・件数など）を充足しているかについて、ＩＴの専門家の作成した監査調書を査閲します。その結果について、監査人は自らが行うリスク評価手続及びリスク対応手続に適切に結び付けなければなりません。

監査人は、ＩＴの専門家の関与、専門家としての能力、客観性の評価、専門家との協議内容及び業務の結果について、ＩＴの専門家が実施した業務の結果を受けて、監査人が判断した結果を監査調書に適切に記載しなければなりません。

Ｘ　アウトソーシングの位置付け

Q32：システム開発や運用をアウトソーシング（外部委託）している場合の内部統制の検証手続はどのようなものでしょうか。またアウトソーシングについて受託会社が報告書を入手している場合の留意点はどのようなものでしょうか。

A32：

アウトソーシングに関する内部統制の検証において、委託会社監査人は、監査基準委員会報告書 402「業務を委託している企業の監査上の考慮事項」（以下「監査基準委員会報告書 402」という。）に従って実施します。また、受託会社監査人は、監査・保証実務委員会実務指針第 86 号「受託業務に係る内部統制の保証報告書」（以下「監査・保証実務委員会実務指針第 86 号」という。）等に従って実施することになります。

１．システム開発のアウトソーシング管理について

システム開発のアウトソーシング管理は、基本的には内部での開発管理と同様です。ユーザニーズを満たす観点からシステム設計がなされているか、開発手順の標準化がなされているかがポイントです。システム開発が成功するか否かは、ユーザの要望が明確にベンダーに伝わっていることが重要となります。また、開発に関するプロジェクト管理体制があるかを検討することになります。

システム開発のアウトソーシング管理では、いわゆるＲＦＰ（Request for Proposal）といわれるシステム開発の仕様書が、業務の分析を基に作成されているか、ユーザの要望を実現するか、が鍵になります。この検討が企業内で十分に行われて発注されていること、開発の手順が標準化されていること、開発のドキュメントが残されていることが重要です。特にドキュメントの管理が十分でない場合には、後日、システム変更をする際に詳細が不明で変更することができない、又は不十分な変更によりエラーが発生するなど会計データの信頼性を損なうリスクがあります。ベンダーの選定に際して、その提案書がＲＦＰの要望を満たしているかの評価をします。

システム開発の際に、監査人としては、監査上必要な監査証跡が新システム上に保持されているか、必要とされる会計データが捕捉できるように設計されているか、会計データの正当性、正確性、網羅性、維持継続性といったＩＴのコントロール目標を保持するような仕組みがあらかじめ組み込まれているか、情報資産に必要なセキュリティのレベルが設定されているかなどが、留意する点になります。これは、本来ＲＦＰにシステムの要件として組み込まれるべきものです。こうした観点も含んでシステム最適化が検討されているかを確かめることになります。

２．システム運用のアウトソーシング管理について

システム運用のアウトソーシングについては、自社内にコンピュータがあり運用のみをアウトソーシングする場合と、ホスティングやハウジングなど外部のデータ・センターにコンピュータがあり、そのコンピュータ自体が借り物であり運用を委託する場合とがあります。

複数企業で利用する外部のデータ・センターの場合において、監査人にとって重要なポイントは、受託会社との契約上、顧客側からの外部監査が可能な契約か、受託会社が信頼できる第三者のシステムに関する内部統制の監査を受けているかなど、その外部のデータ・センターが一定レベル以上のシステムの信頼性を確保するような内部統制を維持しているという保証を得ることが可能かどうか、またその保証を検証できるかどうかということです。具体的には下記の点につき留意することとなります。

(1) 業務内容合意書（サービス・レベル・アグリーメント）

運用業務のアウトソーシングでも外部のデータ・センターでも重要なことは、運用のサービスレベルの明確な取り決めです。これらのアウトソーシングの管理レベルを規定するものが、サービス・レベル・アグリーメント（ＳＬＡ）といわれるものです。このＳＬＡの前提として、企業としていかなるレベルのサービスをどの業務に求めるかの検討分析をします。この検討分析は、本来はシステムの

開発段階で実施されるべきものであり、特にシステムの可用性の確保が監査上は重要です。

また、業務処理の途中でネットワークやシステム障害が発生すると会計データが消滅するリスクがあります。この場合、どのような時間内で障害に対処して復旧をするか、復旧したデータの信頼性の検証方法などの取り決めが具体的になされているかが監査上の検討項目です。

運用業務のアウトソーシングについては、運用状況の定期的な報告を求め、要求した運用のサービスレベルが維持されているか、運用上セキュリティの問題が発生している傾向がないかを分析するといったモニタリングが必要となります。

企業のビジネスの観点からは、効率性の確保も重要です。レスポンスの時間は、平均してどれくらいかの保証がないと業務に支障が生じる可能性があります。情報漏洩等が発生した場合には委託会社の責任を問われるため、機密保持条項が必須となります。また、損害賠償についての取り決めが明確であることも留意点となります。

(2) セキュリティの維持

データの喪失、改ざん等を防止するため、受託会社にも自社と同様に一定レベルのセキュリティの維持が必要であり、セキュリティに関する運用体制について留意します。

(3) 監査の取り決めについて

外部のデータ・センターを利用する場合などにおいて、委託会社監査人が外部のデータ・センターに対して監査を実施できるか否かは、契約上の取り決めによることになります。監査については、単独で実施する場合と委託している複数の監査人と共同で実施する場合があります。外部のデータ・センターが、独自に監査人を選定して監査を実施する場合は、他の監査人の利用となります。全く監査の実施ができないような契約はリスクを伴いますので、委託会社の会計データを保全するために必要な内部統制が受託会社にあるかの検証が監査人にとって必要となります。

３．アウトソーシングについて受託会社が報告書を入手している場合の留意点

アウトソーシングを行っている企業の監査において、受託会社監査人の報告書を利用できる場合があります。その報告書が、監査・保証実務委員会実務指針第 86 号及びその同等のものに従った受託会社の内部統制の整備状況及び運用状況の有効性に関する報告書の場合は、委託業務に係る重要な虚偽表示リスクの評価に利用することができます。

なお、受託会社が財務諸表監査を受けており適正意見が表明されていたとしても、その監査報告書は、受託会社の財務諸表の信頼性に関するものであり、アウトソー

シングに関する内部統制に対する保証は行われていないため、利用することはできません。

監査・保証実務委員会実務指針第 86 号では、報告書として「受託会社のシステムに関する記述書及び内部統制のデザインに関する報告書（タイプ１の報告書）」と「受託会社のシステムに関する記述書並びに内部統制のデザイン及び運用状況に関する報告書（タイプ２の報告書）」の二つのタイプが定義されています。このうち、タイプ１の報告書は、リスク評価手続の実施には役立ちますが、リスク対応手続を実施するには、タイプ２の報告書を入手し、検討する必要があります。このタイプ２の報告書では、内部統制のデザインが有効である旨の意見の他、除外事項が付されている場合や内部統制の運用状況が有効でないとの意見が表明されることもあります。

報告書を利用する場合には、報告書の対象となる業務が監査上必要なアウトソーシングの範囲に合致しているか、評価手続の内容、範囲、実施時期、その結果について留意します。

報告書の評価範囲が、委託会社のアウトソーシングの範囲に合致していない場合や、評価期間が十分でない場合は、委託会社経由で受託会社を通じて、受託会社監査人又は他の監査人に追加の手続の実施を依頼することが必要になる場合があります。若しくは、監査人が独自に受託会社に往査する等の追加の手続も考えられます。

また、内部統制に係る報告書を検討するだけでなく、受託会社監査人の信頼性の程度を確かめます。

報告書が提供する証拠の十分性と適切性を評価した結果、受託会社監査人の実施した手続に不足があると判断された場合には、必要な手続を自ら実施するか、又は受託会社監査人に依頼して実施する必要があります。

委託会社監査人と受託会社との間には、通常、契約関係はありませんが、業務上知り得た事項については守秘義務を負うことになります。

Q33：アウトソーシングの受託会社監査人の留意点はどのようなものですか。

A33：

アウトソーシングの受託会社からの依頼を受けて監査・保証実務委員会実務指針第 86 号に係る業務（以下「86 号業務」という。）を受嘱する場合や 86 号業務が情報システムに関する他の制度と混同されるのを避けるために以下の点について留意します。

１．86 号業務と認証制度の違い

86 号業務は、委託業務に係る内部統制の認証業務ではありません。プライバシーマークやＩＳＭＳ等の認証制度のような 86 号マークという制度は存在せず、受

託会社監査人は報告書の発行をもって86号マークの認定をできるというものではありません。

監査・保証実務委員会実務指針第86号では「本指針は、公認会計士等が、委託会社の財務報告に関連する業務を提供する受託会社の内部統制に関して、委託会社とその監査人が利用するための報告書を提供する保証業務に関する実務上の指針を提供するものである。」とされています。また、86号業務の報告書は不特定多数の利用者を想定したものではありません。86号業務の報告書には受託会社、委託会社及び委託会社の監査人のみの利用を想定しており、想定利用者以外への配布、想定利用者以外の使用、又は他の目的の使用を明確に制限する表現を含めることが適切とされています(監査・保証実務委員会実務指針第86号第63項(5)、A61項)。

２．データ・センターへの委託会社（顧客）が未定の場合の86号業務について

データ・センター業務の開始に当たって、まだ、顧客が確定していない時点でデータ・センターの内部統制の評価を依頼される場合があります。この場合に86号業務として実施できる状況であるかについては十分に検討します。86号業務は、上述(1)で記載したように、財務報告に関する業務を外部に委託している企業の監査人がその報告書を利用することを目的とする業務です。顧客がいないことにより評価の対象となる内部統制が実在しない段階では、86号業務に向けた指導・助言は実施できるとしても、86号業務の提供はできないと考えられます。

３．ネットワーク運用業務等の提供

86号業務は、財務報告の基礎となる業務の委託を前提としています。したがって、受託している業務が委託会社の財務諸表の基礎となる業務の重要な一部となるかを検討します。

例えば、業務委託の対象がファイヤーウォールの設定・監視や物理的な入退出管理のみの場合は、その統制の対象が必ずしも財務報告の基礎となるシステムを対象としていない、又は対象であっても重要な一部とはみなされないこともあるため、慎重に判断します。同様に、ホスティングやハウジングについても単なる場所貸しに相当するような場合については、86号業務の対象ではないと判断される場合がありますが、その受託内容により、財務諸表の基礎となる業務の業務アプリケーションについての運用業務とみなされる場合、その運用業務に関する全般統制は86号業務の対象となる場合があります。受託しているネットワーク運用業務が財務諸表の基礎となる業務の重要な一部となると判断される場合には、86号業務の対象とされ、ファイヤーウォールの管理が内部統制の評価対象項目として検証される場合もあります。

４．ＡＳＰやＳａａＳのサービスの提供

ＡＳＰやＳａａＳについては、受託会社で取引の処理が行われていることが想定されますが、委託会社が受託会社から提供されたサービスの内容とその形態によって財務報告の基礎となる業務に係る内部統制が委託元にあるか受託先にあるか判断し、財務報告の基礎となる業務の内部統制が受託先にあると認められる場合に86号業務の対象となります。ＡＳＰやＳａａＳといったサービス形態の名称だけではなく、財務報告の基礎となる業務アプリケーションについての業務運用、その業務運用に関する全般統制は86号業務の対象となる場合があります。なお、留意すべきは、財務諸表の基礎となる業務の委託について受託会社に86号業務の報告書を求めるか否かは、委託会社及び委託会社の監査人がその業務の重要性等を勘案して決定することになります。

上記のサービスの形態を整理すると以下のようになります。

(1) ハウジング

顧客の通信機器やサーバ等を設置するための、回線設備等が備わった施設を提供するサービス。

(2) ホスティング

必要なコンピュータ（サーバ及び関連するＩＴインフラ）の容量を共用できるようにして顧客に貸出しするサービス。

(3) ＡＳＰ（Application Service Provider）

アプリケーションを顧客が個々に所有するのではなく、ＡＳＰ業者が提供するソフトウェアにより処理を行うサービスを利用するもの。

(4) ＳａａＳ（Software as a Service）

ネットワークを通じて顧客にアプリケーションソフトの機能を必要に応じて提供する仕組み。ＳａａＳによって、顧客はソフトウェアを所有せずに、機能単位で提供される必要最小限のサービスを利用することができる。実際には、①ハウジング、②ホスティング及び③ＡＳＰとの組み合わせをＳａａＳといっている場合もある。

Q34：システム開発や運用を外部委託している場合、受託会社から独立監査人の報告書が入手できないときの委託会社監査人が実施すべきリスク評価手続はどのようにしたらよいでしょうか。

A34：

監査基準委員会報告書402第10項及び第11項では、委託会社監査人は、重要な虚偽表示リスクの識別と評価に対する基礎を得るために、受託会社が提供する業務の内容と重要性、及びそれらが委託会社の監査に関連する内部統制に与える影響に関して、十分な理解を得る必要があるが、受託会社が提供する業務に関する十分な理解を委託

会社から得られなかった場合は、以下の手続を一つ又は複数組み合わせて実施して理解を得なければならない、とされています。

1.「受託会社のシステムに関する記述書及び内部統制のデザインに関する報告書（タイプ１の報告書）」又は「受託会社のシステムに関する記述書並びに内部統制のデザイン及び運用状況に関する報告書（タイプ２の報告書）」を入手する（利用可能な場合）。

２．委託会社を通じて受託会社に連絡して特定の情報を入手する。

３．受託会社を往査し、受託会社の提供する業務に関連する内部統制について必要な情報を入手するための手続を実施する。

４．受託会社の提供する業務に関連する内部統制について、必要な情報を入手する手続の実施に他の監査人を利用する。

そして、評価した重要な虚偽表示リスクへの対応、運用評価手続の実施に際しても、同様な手続の実施により、受託会社の内部統制に関する十分かつ適切な監査証拠を入手することとされています。

独立監査人の報告書（タイプ１又はタイプ２の報告書）が入手できない場合とは、上記の１．の手続が実施できない場合と考えられます。

上記２．に対応する手続としては、次のような手続があります。

・　受託会社が、委託会社に対して受託業務の結果や状況について定期的な運用報告書等を提出している場合、当該運用報告書等の内容を分析する。

・　受託会社が、委託会社に対してシステム開発・運用の受託業務の内部監査報告書を提出している場合、当該内部監査報告書の内容を分析して、受託業務に関連する内部統制を評価する。

・　委託会社監査人は、委託会社とデータ・センター等の全般統制の評価手続を協議し、委託会社が実施したデータ・センター等の全般統制評価について、その評価結果を入手し利用する。

上記３．及び４．に対応する手続としては、次のような手続があります。なお、上記４．は、遠隔地等の事情により、他の監査人に依頼して実施する方法であるため、必要とされる手続は３．と同様になります。

・　委託会社監査人又は他の監査人が受託会社に往査する場合は、受託会社の同意を得て実施します。したがって、一般的には、業務委託契約書に監査条項が存在するか、別途監査に関する合意書等を取り交わします。監査を実施する際には、監査目的、監査実施時期、受託会社の協力及び機密保持等が協議されます。場合によっては、複数の委託会社監査人が共同して監査を実施することもあります。

なお、上記の２．から４．の手続により入手した監査証拠については、１．の手続により入手した監査証拠とは必ずしも同等ではないため、監査証拠として利用する情報の適合性と信頼性に留意する。

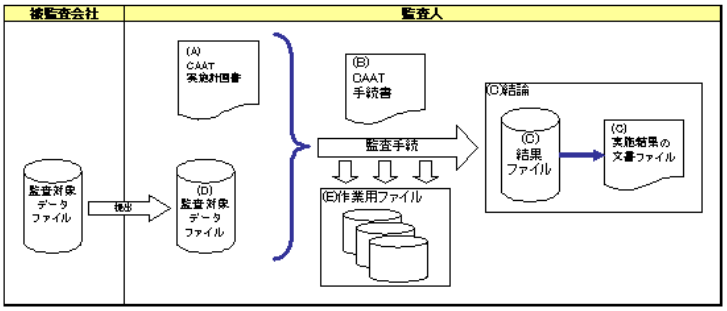
ＸＩ　監査調書

Q35：ＣＡＡＴを利用した監査手続を実施する場合、どのような監査調書を作成すればよいか例示してください。

A35：

まず、ＣＡＡＴを利用した監査手続を実施する場合に入手、利用、生成されるデータファイルの流れを整理しておきます。

以下の図はＣＡＡＴを利用した監査手続を実施する場合のデータファイルの入手、利用、生成される大きな流れの概要を示しています。以下にそれぞれの定義を記述します。



１．ＣＡＡＴ実施計画書

ＣＡＡＴ実施計画書とはＣＡＡＴを利用して実施する監査手続を策定する段階において、手続の目的や概要、手続実施に必要な情報を詳細に記述した文書をいいます。ＣＡＡＴ実施計画書には、通常以下の内容が含まれ、プロセス単位あるいは勘定科目単位で作成されます。

(1) 実施対象のプロセス
(2) 実施目的
(3) 対象となるシステム
(4) データ入手依頼先
(5) 実施予定時期
(6) 想定されるデータ件数
(7) 会社へ依頼したデータの概要（会社へ提出した「データ依頼書」の控を含む。）
(8) 会社より入手したデータの概要（会社へ提出した「データ受領書」の控を含む。）
(9) 実施する監査手続の内容

なお、会社へＣＡＡＴを利用して実施する監査手続を実施するためのデータを依頼する場合、会社へ提出するＣＡＡＴ依頼書例については付録２を参照ください。また、ＣＡＡＴ実施計画書に記述された事項に変更があった場合には、変更内容及び変更した根拠等をＣＡＡＴ実施計画書に随時更新する必要があります。

２．ＣＡＡＴ手続書

ＣＡＡＴ手続書とは、ＣＡＡＴツール（※）のコマンド等を監査手続の実施目的、手続の具体的手順に沿って記述した表であり、手続の詳細を記述するものをいいます。

３．結論

結論には結果ファイルと実施結果の文書ファイルが含まれます。結果ファイルは、ＣＡＡＴツールで作成されたテーブル等を意味し、実施結果の文書ファイルは、結果ファイルを取りまとめたものであり、監査手続の最終的な結論を記録した文書を意味します。

４．会社から入手したデータファイル

上記１．(7) の「データ依頼書」に基づき会社から受領した監査対象となるデータファイルをいいます。

５．作業用ファイル

会社から入手したデータに上記(B)のＣＡＡＴ手続書に記述した手続を適用する過程で一時的に作成される作業用ファイルをいいます。

監査人は、経験豊富な監査人が、以前に当該監査に関与していなくても、実施した監査手続の種類、時期及び範囲、監査手続を実施した結果及び入手した監査証拠、監査の過程で生じた重要な事項とその結論及びその際になされた職業的専門家としての判断等の事項を理解できるように監査調書を作成しなければならない。（監査基準委員会報告書 230「監査調書」参照）この観点から考えると、上記１．～５．のうち、「１．ＣＡＡＴ実施計画書」、「２．ＣＡＡＴ手続書」、「３．結論」を監査調書として保存し、「４．会社から入手したデータファイル」、「５．作業用ファイル」は監査人が保存する必要がないと考えることができます。ただし、「４．会社から入手したデータファイル」については、会社の記録が保存されていないリスク、後になって改ざんされるリスク、会社の状況が変化したため、同じデータファイルを入手できなくなるリスク等を考慮し、リスクが大きいと判断する状況では、監査人が保存することが必要になる場合もあります。

※　ＣＡＡＴツールには、ＣＡＡＴ専用ソフトウェアと汎用的なデータ処理ソフトウェア、表計算ソフトウェアがあります。ＣＡＡＴに使用するソフトウェアによって、コマンドが異なるため、ＣＡＡＴを行うに当たってはあらかじめＣＡＡＴツールを決めておきます。

付録１　ＩＴ判定チェックリスト（Ｑ３参照）

IT判定チェックリスト

会社名:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿　年　度:＿＿＿＿＿＿＿＿＿＿＿＿

監査担当者:＿＿＿＿＿＿＿　査閲者:＿＿＿＿＿＿＿

チェック事項	回答			備考
	Y	N	n/a	
1. 業種・監査の種類 1-1　業種・業態は銀行・証券会社・保険会社等の金融機関か 1-2　上場会社か				
2. 企業規模 2-1 売上高、取引件数、従業員数などの企業規模の指標が大きくない				
3. 会計取引にかかわる主要な業務システム 3-1　主要業務はIT化されているか 3-2　主要システムにインターネット等の外部接続はあるか 3-3　主要システムは自社開発か 3-4 主要システムがパッケージの場合、自社用に変更をしているか				
4. システム関連支出 4-1　以下のシステム関連支出（今後の支出予算）は多額か ・ ハードウェア、ソフトウェアの取得及びリース（研修開発費として処理されたソフトウェア関連費用を含む） ・ システム関連の人件費 ・ システム関連の外部委託費				
チェック事項	回答			備考
	Y	N	n/a	
5. 要員の規模 5-1 情報システムを担当している部署は、専門の部署か 5-2 情報システム部門を担当している専任者は、多数か				

5-3 情報システムに関する重要業務を外部委託していないか				
6. システムトラブル発生状況（システムの安定度の状況） 6-1 過去1年以内にシステムトラブルにより、主要な業務の停止が発生したことがあるか 6-2 システムトラブルによりシステムが停止（システムダウン）した場合に、手作業での業務（ビジネス、会計）継続は困難か				
7. 業務電子化 7-1 自動受注や自動発注のような会計的な影響を有する取引ないし処理が、システムにより自動的に処理されるような機能があるか 7-2 販売システム等のサブシステムから会計システムにデータを受け渡して自動的に会計上の仕訳を生成する機能があるか 7-3 主要システムに、電子承認ないしはワークフロー(業務書類回付の自動化など)の機能を有するものがあるか 7-4 日常業務で発生する取引証ひょうが、電子的データ(ペーパーレス)で保存されているか 7-5 電子帳簿保存法に基づき保存される帳簿、書類があるか				
8. 電子商取引の利用 8-1 電子商取引を利用した会計取引があるか				
9. システム変更 9-1 過去1年間に会計情報に影響を与えるシステム変更が行われているか 9-2 当期に会計情報に影響を与えるシステム変更が行われるか				

判定理由

判定結論（いずれかにチェックを付す。）

〇ITの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低いとはいえない。原則的なリスク評価手続を実施する(以下「原則手続」という。)。

〇ITの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低い。ITに依存した内部統制の理解と評価に関する手続について省略する（以下「省略手続」という。)。

判定の履歴（いずれかを〇で囲む。）

年度	前々期 年度	前期 年度	当期 年度
判定結論	原則手続／省略手続	原則手続／省略手続	原則手続／省略手続

記入上の留意点

《 全般的留意点 》

1） IT判定チェックリストは、ITの利用に関する概括的理解において、リスク判定の基礎として利用する。
2） チェック事項のうち「1．業種･監査の種類」の回答が、一つでも「Y」となった場合には、ITの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低いとはいえない場合がほとんどであろうと考えられる。また、量的基準により判断が必要なものについては、あらかじめ基準を設定し、それとの比較により判定する。他のチェック項目について「Y」となった場合は、それぞれ個別に検討を要するが、多くの場合、ITの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低いとはいえないものと想定される。
3） 各項目の「備考欄」は、回答が「Y」,「N」となった根拠やその原始資料名などを記入することを想定している。
4） 「判定理由」には、チェック項目ごとに「Y」となった回答及びそれをそのまま採用する、あるいは特定の理由を示して採用しない旨を明確に記述し、それらを総合して「判定結論」となったことを明記する。明確な理由を示せない場合は「Y」の回答を採用する。また、判定結論は、チェック項目の個別結果を総合的に勘案して決定されることになるが、チェック項目が一つでも「Y」となった場合には、多くの場合、ITの利用に伴う重要な虚偽表示に関する潜在的リスクが十分に低いとはいえないとの結論になるものと想定される。
5） 一部のチェック事項について回答の記入を省略した場合は、その理由を「判定理由」に明記する。
例えば、業種・業態、規模等のIT依存度の高さ（システムダウン時の影響の高さ）、主要システムの開発、保守、運用、障害の発生頻度等のアプリケーションのリスク（アプリケーションのダウンの可能性）、その他のリスク（ネットワークを含むハードウェアのリスク等）を総合的に判断した過程を明記する。業種・業態、規模等のIT依存度の高さ（システムダウン時の影響の高さ）は、チェック事項のうち「1．業種・監査の種類」、「2．企業規模」、「4．システム関連支出」、「5．要員の規模」、「7．業務電子化」を勘案して判断することが考えられる。主要システムの開発、保守、運用、障害の発生頻度等のアプリケーションのリスク（アプリケーションのダウンの可能性）は、チェック事項のうち「3．会計取引にかかわる主要な業務システム」、「6．システムトラブル発生状況（システムの安定度の状況）」、「9．システム変更」といった要素を勘案して判断することが考えられる。また、ネットワークやハードウェアといったその他のリスクも勘案することに留意する。
6） 過去2年度の「判定結論」の履歴を「判定の履歴」として記載し、当年度判断の基礎として参照する。

以　上

付録２　ＣＡＡＴ依頼書（Q35 参照）

(株)○○○○

経理部長　○○　○○殿

平成○年○月○日

○○公認会計士事務所

公認会計士　○○　○○

201x 年 x 月期財務諸表監査の一環として、コンピュータ利用監査技法（ＣＡＡＴ）を用いた監査手続を実施させて頂きたいと考えております。お手数をお掛け致しますが、下記につきご協力頂きますようお願い申し上げます。

記

１．　依頼内容

下記３．に記載したデータをご提供ください。

２．　実施目的

財務諸表作成プロセスにおける重要な仕訳入力及び修正について検証します。

３．　依頼データ

・対象：財務会計システムに登録されている仕訳データ下記期間中全件

・期間：201○年○月○日～201○年○月○日

なお、以下の項目について監査手続を実施予定です。

No	フィールド名	内容
1	会計年度	仕訳が転記された会計年度
2	仕訳番号	仕訳番号
3	仕訳行番号	仕訳の明細
4	勘定科目ＣＤ	勘定科目コード
5	勘定科目名称	総勘定元帳コードの名称又は説明
6	仕訳種別	仕訳発生元、発生種別
7	入力日	仕訳がシステムへ入力された日付
8	転記日	転記日
9	貸借区分	借方/貸方の識別コード
10	金額	金額
11	入力ユーザＩＤ	仕訳を入力したユーザのＩＤ
12	摘要	仕訳の内容説明

*1　上記「フィールド名」は一般的なシステムフィールド名称として記載しております。データをご準備頂く際には貴社のフィールド名称をご使用ください。

*2　データの提供フォーマット、授受の方法については別途協議を予定しております。

以　上