監査基準報告書315実務ガイダンス第１号

ＩＴの利用の理解並びにＩＴの利用から生じるリスクの識別及び対応に関する監査人の手続に係るＱ＆Ａ（実務ガイダンス）

2021 年 8 月 6 日
改正　2022 年 10 月 13 日
日本公認会計士協会
監査・保証基準委員会
（実務ガイダンス：第5号）

＜目　次＞

《Ⅰ　はじめに》

日本公認会計士協会（以下「本会」という。）は、2021 年６月８日付に改正公表した監査基準報告書 315「重要な虚偽表示リスクの識別と評価」では、適用指針においてＩＴに関する論点や手続についても一定の言及が行われている。

しかしながら、監査実務においては、ＩＴの長足の進歩を踏まえて監査基準報告書 315 を適用してＩＴの利用状況の理解に基づきＩＴの利用から生じるリスクを評価し、さらに監査基準報告書 330「評価したリスクに対応する監査人の手続」を適用して監査手続を立案及び実施する必要があり、監査基準報告書 315 の適用指針のみでは必ずしも十分とは言えない。そのため、本会では、主として、監査基準報告書 315 及び同 330 に定められた要求事項及び適用指針に関連して、ＩＴに関するリスクの評価及び対応の一連の側面に関して会員の実務に資する解説を Q&A 形式で提供することとし、本実務ガイダンスを作成することとした。したがって、本実務ガイダンスは、その利用者が、監査基準報告書 315 及び同 330 の内容を十分に理解していることを前提としており、また、上記の改正公表後の監査基準報告書 315 が適用される監査及び中間監査において参考とすることを想定していることについてご留意いただきたい。

本実務ガイダンスは、一般に公正妥当と認められる監査の基準を構成するものではなく、会員が遵守すべき基準等にも該当しない。また、2021 年８月６日時点の最新情報に基づいている。

《Ⅱ　総論》

Ｑ１　ＩＴの利用から生じるリスクとはどのようなものでしょうか。

（関連する報告書：監基報 315 第 11 項(3)、第 25 項(2)(3)(4)）

Ａ１：

１．ＩＴの利用から生じるリスクの特徴

ＩＴの利用から生じるリスクとは、企業のＩＴプロセスにおける内部統制のデザイン若しくは運用が有効でないことにより、情報処理統制が有効にデザイン若しくは運用されない可能性又は企業の情報システム内の情報のインテグリティ（すなわち、取引及びその他の情報（データ）の網羅性、正確性、正当性）に対し引き起こされるリスクをいいます（監基報 315 第 11 項(3)）。

監査人は、統制活動のうち、アサーション・レベルでの重要な虚偽表示リスクに対応する内部統制に基づいて、ＩＴの利用から生じるリスクの影響を受けるＩＴアプリケーション及び関連するその他のＩＴ環境を識別し、これらについて①ＩＴの利用から生じるリスク、②当該リスクに対応するＩＴ全般統制を識別して、評価しなければならないとされています（監基報 315 第 25 項(2)から(4)参照）。

２．ＩＴの利用から生じるリスクの例

ＩＴアプリケーションでは、あらかじめ定められた方針や規定に従い一貫して処理し、複雑な計算を実行できるという特徴があります。

監査基準報告書 315 付録５では、以下の項目がデータの不正確な処理、不正確なデータの処理又は両方を実行する不適切なＩＴアプリケーションへの依存に関連するＩＴの利用から生じるリスクの例として挙げられています。これらのように、企業のＩＴプロセスにおける内部統制のデザイン又は運用が有効でないことが生じた場合、情報処理統制が有効にデザイン若しくは運用されない可能性又は企業の情報システム内の情報のインテグリティが維持されない可能性が生じます。

(1) データの破壊や不適切なデータの変更につながる可能性のあるデータへの未承認のアクセス（未承認若しくは架空取引の記録又は取引の不正確な記録等）

(2) ＩＴ部門の担当者が担当業務の遂行に必要な権限を超えてアクセス権を取得し、それにより職務の分離を侵害する可能性

(3) マスターファイル内のデータに対する未承認の変更

(4) ＩＴアプリケーション又はその他のＩＴ環境に対する未承認の変更

(5) ＩＴアプリケーション又はその他のＩＴ環境に必要な変更が行われないこと

(6) 手作業による不適切な介入

(7) データの消失又は必要なデータへのアクセスができないこと

上記(3)について補足説明すると、取引データ等を作成する際には、相手先や商品の情報等の繰り返し利用する情報をマスターファイルとして作成し、取引の都度それを参照することで入力誤りのリスクに対応することがありますが、当該マスターファイルに未承認の変更が加えられた場合には計算結果等を誤ってしまうことがあります。

また、上記(6)について補足説明すると、プログラムやデータの作成・修正は手作業で行われることも多く、ヒューマンエラーの可能性があります。それに対して、承認・確認のような複数チェックや処理結果等の査閲などのエラー検出作業が行われます。しかしながら、当該作業が十分に機能しないと、プログラムの修正やデータの入力を誤り、事後的な検出もできないリスクがあります。

このようなＩＴの利用から生じるリスクに適切に対応するためには、ＩＴアプリケーションの性質等に応じた適切なＩＴ全般統制を識別し評価することになります。

Ｑ２　不正リスクや関連手続を検討する場合、自動化された情報処理統制の無効化のリスクと留意点は何でしょうか。

（関連する報告書：監基報 315 第 15 項、第 23 項、A105 項、A107 項、A157 項、付録３第 23 項、付録５第２項、付録６第１項(3)、第２項(1)及び同監査基準報告書 240「財務諸表監査における不正」第 30 項）

（関連する研究文書：財務報告内部統制監査基準報告書第１号研究文書第１号「内部統制報告制度の運用の実効性の確保に係る研究文書」）

Ａ２：

自動化された情報処理統制を変更する場合には、ＩＴアプリケーションのプログラムやパラメータの設定値の変更が必要となります。また、ＩＴアプリケーションで用いられている各種マスター・データや取引データ等は電子データであり、アクセス可能な端末と権限が必要になるため、一般的には自動化された情報処理統制は手作業による情報処理統制よりも無効化は難しくなります。

ただし、自動化された情報処理統制であってもそれらを過信せずに、内部統制の無効化のリスクを完全に防ぐことは困難であるという視点を持つことが重要です。例えば、プログラムやデータへのアクセスを制限していても、アクセスを認められた権限者により不正な操作が行われたケースがあります。また、ＩＤとパスワードの窃用によりアクセスを認められていない第三者により情報流出が行われたケース等、内部統制の構築時には想定されていなかったり、発生可能性が低いと思われた手口により内部統制の無効化が生じることがあります。

さらに、紙の記録に比べて電子記録は変更の痕跡が残り難く、ＩＴアプリケーションのプログラムによる処理内容の検証が難しいことで、内部統制の無効化が生じてもその発見が遅れることもあります。監査上は会社が整備している内部統制の特徴、その内部統制に対する無効化のリスクを考慮した監査手続を立案することになります。

ここでは大きくプログラム、環境設定、アクセス権についてのポイントを解説します。

１．プログラム

内部統制の無効化ではプログラムの改竄だけでなく、使用されているプログラムのロジックに不十分な点があった場合、その脆弱性を利用して内部統制の無効化が行われることがあります。

例えば、過去の取引データを保管する容量の制限があったため、棚卸資産の評価のために「滞留在庫」を抽出するＩＴアプリケーションのプログラムの滞留の判定基準に最終入庫日ではなく最終出庫日を使っていた企業で、担当者は、少数の製品を移動・廃棄することにより最終出庫日を更新し、残りの同種製品を滞留資産の区分から除外するような無効化を行った例があります。

監査人はプログラムの要件定義が会計処理上適切な内容であることを確かめるための手続を必要に応じて実施することになります。また、例示のような制約要因があることが把握されているならば、それを補完するために在庫数と出庫数の比率分析で異常値を検出する手続や毎期末の棚卸資産一覧のデータを用いて経年分析を行う等、情報処理統制を補う手続の要否を検討します。

また、特に自社開発のＩＴアプリケーションの場合には市販のものに比べて、ロジックが企業の仕様で作製されるため、適切でないプログラムが導入されるリスクが高まることがあります。

２．環境設定（パラメータ設定等）

市販のＩＴアプリケーションでは、利用者が自動化された情報処理統制に用いられるパラメータの設定値を変更できる部分があります。例えば、与信管理を行うＩＴアプリケーションで得

意先ごとの与信限度額の設定値を超える受注金額をエディット・チェックで検出し、入力を止めたり、所定のレポートを出力する機能を装備していても、与信限度額のパラメータに過大な値を設定し、あらかじめ定められた与信限度額を超える受注を制限した自動化された情報処理統制を無効化したケースがあります。

また、別の例として、職務分掌のため入力者と承認者を分離した権限設定が可能な会計のＩＴアプリケーションを導入しながら、担当者の全員に両方の権限を与えてしまい職務分掌の内部統制が無効化され自己承認の会計伝票が起票されたケースもあります。

監査人は会社が利用しているＩＴアプリケーションを理解し、それらで使われる環境設定が企業の意向でどのように変更することが可能かを把握し、情報処理統制に影響する場合には当該設定値の登録・変更に関する内部統制の有無及び環境設定の内容の確認などの手続を行うことになります。

３．アクセス権

アプリケーションプログラムやオペレーションプログラム、そしてデータベースにアクセス管理機能を設け、プログラムの操作やデータへのアクセスを制限する手法は幅広く採用されています。

しかしながら、本来の情報処理統制によるデータの処理結果を直接修正する権限等、利用方法によっては内部統制の無効化が可能なアクセス権を保有する者がそれを悪用して通常のデータの処理結果を改竄した事例や、個々のＩＴアプリケーションの権限設定は適切であっても複数の異なるＩＴアプリケーションの操作権限を持っていたために職務分離が成立しなくなった事例があります。

監査人は、通常、各人が保有する権限で実行可能な操作内容を把握し、内部統制の無効化につながるような権限の有無を確かめ、仮にそのような権限がある場合には、アクセス状況や操作内容をモニタリングする適切な内部統制があるかを検討します。

このように自動化された情報処理統制の無効化の可能性を検討する場合には、内部統制の内容を理解し、特に情報処理統制に影響があるものに対して技術的に対応が不十分な場合にはその脆弱性を悪用されないかという観点からの検討が望まれます。

加えて、自動化された情報処理統制の無効化に対する調査方法には、想定される無効化のパターンに応じて必要なデータを取得し、自動化されたツール（コンピュータ利用監査技法（ＣＡＡＴ）等）を適用して再計算結果との差異を分析したり、数年間にわたる分析結果などを比較して異常値を把握する方法も考えられます。

Ｑ３　システム、ソフトウエア、アプリケーション、プログラム、業務処理統制等の用語は他団体の基準等で使われているものと、監査基準報告書で使われるものと同じ意味なのでしょうか。

Ａ３：

１．ＩＴ関連の用語について

企業のコンピュータに関する専門部署には「(情報) システム部門」のような名称が使われることが多くあります。初期のメインフレーム（大型汎用機）のコンピュータの場合、コンピュータを操作するのはシステム部門で、ユーザ部門は紙の入力原票を回付し、印刷された結果を受領するような体制を採用することが多数でした。そのためコンピュータとシステムがほぼ同義語のように用いられることがあります。また、会計システム、会計ソフト（ウェア)、会計プログラムのように特定の業務のために用いられるソフトウエアを実務上、いろいろな呼び方をすることがあります。

監査基準報告書で使われているのはこれらが整理され、内部統制システムや情報システムそして会計システムのような「システム」という用語はコンピュータの処理とそれを利用する手作業の部分の双方を含む広い範囲になっています。そして、メインフレームのような１台のコンピュータを使う環境だけでなく、利用者のクライアントＰＣと複数のサーバのような処理に関係するコンピュータ群とそれを維持する活動もこれに含まれます。

このようにＩＴに関連する用語は、どのような定義や分類を想定して使われているかで異なりますので用語が使われる局面により判断することも必要になります。

(1)	(2)	(3)
ソフトウエア	アプリケーション・ソフトウエア	ＩＴアプリケーション
	システム・ソフトウエア	ミドルウエア
		オペレーティング・システム
ハードウエア	ハードウエア	ハードウエア

(1) コンピュータの構成はハードウエアとソフトウエアに分かれます。ハードウエアは、演算処理装置を中心に入力、出力、保存、通信等の機能を担う機器で構成されます。これらのハードウエアを動作させるために必要なソフトウエアは、一つ又は複数のプログラムから構成されます。そのため、ソフトウエアをプログラムと同義に使う方もいます。

(2) 上記(1)のソフトウエアは、さらにアプリケーション・ソフトウエアとシステム・ソフトウエアに分かれます。アプリケーション・ソフトウエアは特定の作業をするために用いられるソフトウエアであり、監査に関係するものの多くは取引又は情報の開始、処理、記録及び報告において使用されます。監査基準報告書315ではこれをＩＴアプリケーションと定義していますが、一般的にはアプリケーション（・プログラム・ソフトウエア）やソフトウエア（・プログラム）と呼ぶこともあります。

(3) システム・ソフトウエアはハードウエアの管理を中心に担い、異なるアプリケーション・ソフトウエアがハードウエアを操作可能にする共通基盤を構築するソフトウエアであり、基本ソフトウェア（ＯＳ：オペレーティングシステム）が代表的なものです。

また、大勢がコンピュータを利用する場合には、コンピュータの役割を利用者のクライアントと機能や情報を提供するサーバに分け、通信回線で接続するクライアント・サーバ・システム

の構成を採用することが多くあります。この場合、サーバでは複数のクライアントの情報の授受を行うために一部の機能を強化したミドルウエアを搭載したシステム構成にすることがあります。

例えば、財務会計のＩＴアプリケーションを複数で利用する場合、各利用者のクライアントにＩＴアプリケーションのソフトウエアをインストールするのではなく、ＩＴアプリケーションの利用に特化したアプリケーションサーバを準備し、各クライアントＰＣから通信回線を利用して操作するのがクライアント・サーバ・システムの構成になります。

ミドルウエアを搭載したサーバには、アプリケーションサーバの他に、データ参照に特化したデータベースサーバ、外部回線との接続に特化したウェブサーバなどが代表例になります。

２．内部統制関連の用語について

旧監査基準報告書 315 で使われていた業務処理統制（Application controls in information technology）は、監査基準報告書 315 では情報処理統制（Information processing controls）に置き換わっています。そして、手作業の情報処理統制と自動化された情報処理統制（ＩＴアプリケーション）のように、更に詳細に使い分けることもあります。

また、「財務報告に係る内部統制の評価及び監査の基準並びに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」等では監査基準報告書 315 の自動化された情報処理統制に相当するものとして、「ＩＴに係る業務処理統制」という用語で説明しており、これらについて、監査実務上はほぼ同義と考えられます。

なお、旧監査基準報告書 315 で使われていた業務処理統制の定義の中には情報の適時の把握という内部統制目的の有効性・効率性に関連する表現もありましたが、情報処理統制では取引及びその他の情報（データ）の網羅性、正確性、正当性）など財務報告の信頼性の内部統制目的により焦点を当てた定義になっております。内部統制システムは複数の内部統制目的に関係しますが、監査上は主として財務情報の信頼性が中心となるためその差の影響は少ないものと考えられます。

Ｑ４　企業の統制活動における内部統制のうち、情報処理統制とＩＴ全般統制はどのような関係があるのでしょうか。

（関連する報告書：監基報 315 第 11 項(2)、(9)、A5 項、付録３第 20 項、付録６）

Ａ４：

１．企業の統制活動における内部統制における情報処理統制とＩＴ全般統制

企業の統制活動における内部統制には、情報処理統制とＩＴ全般統制が含まれます（監基報 315 付録３第 20 項)。

情報処理統制とは、情報のインテグリティ（すなわち、取引及びその他の情報（データ）の網羅性、正確性、正当性）のリスクに直接対応する、企業の情報システムにおけるＩＴアプリケーションの情報処理又は手作業による情報処理に関連した内部統制です(監基報 315 第 11 項(9))。

また、情報処理統制は、企業の情報に関する方針が有効に適用されるための処理又は手続であり、自動化されている場合（すなわち、ＩＴアプリケーションに組み込まれている。）と手作業の場合（例えば、インプット又はアウトプットに係る内部統制）があり、他の情報処理統制やＩＴ全般統制を含む他の内部統制に依拠することがあるとされています（監基報 315 の A5 項)。

ＩＴ全般統制とは、ＩＴ環境の継続的かつ適切な運用を支援する企業のＩＴプロセスに係る内部統制です（監基報 315 第 11 項(2)参照)。

経営者が財務報告において依拠する内部統制が自動化されている程度が高いほど、自動化された情報処理統制の継続的な運用を支援するＩＴ全般統制の適用は重要となります(監基報 315 付録３第 20 項参照)。

２．情報処理統制

(1) 情報のインテグリティのリスクとの関係

上述のとおり、情報処理統制は、情報のインテグリティ（すなわち、取引及びその他の情報（データ）の網羅性、正確性、正当性）のリスクに直接対応する、企業の情報システムにおけるＩＴアプリケーションの情報処理又は手作業による情報処理に関連した内部統制です。情報のインテグリティの各項目のリスクに直接対処する内部統制（情報処理統制）の例は下表のとおりです。

情報のインテグリティ		情報のインテグリティのリスクに直接対応する内部統制
取引及びその他の情報（データ）	網羅性	システム間インターフェースにおいて、データ出力側で把握されているデータ件数等とデータ入力側で把握されるデータ件数等が整合していることを確認し、整合しない場合には入力されたデータ処理を中止するといったＩＴアプリケーション上の機能
	正確性	取引データの入力時に、事前に登録されているマスターファイル上の項目と入力された項目との突合が行われ、一致しない場合には入力データを受け付けないといったＩＴアプリケーション上の機能
	正当性	処理担当者に許可された業務内容に応じた操作権限をユーザＩＤに事前に付与し、このユーザＩＤ使用者を認証することにより、許可された処理担当者とみなすＩＴアプリケーション上の機能

(2) 自動／手作業による分類

上述のとおり、情報処理統制は、自動化されている場合（すなわち、ＩＴアプリケーションに組み込まれている。）と手作業の場合（例えば、インプット又はアウトプットに係る内部統制）があります。

手作業による情報処理統制は、個々のＩＴアプリケーションによる取引の処理に関連している一方で、ＩＴ作成情報ではない情報を利用して情報システム外で行われており、ＩＴに関連しないものも含まれます。

例えば、システム間インターフェースについて、以下の①のみならず②のような、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も情報処理統制を構成するものと考えられます。インターフェースによるデータ受渡処理が想定どおりに行われなかった場合に、それを是正するように実施される内部統制は、重要な虚偽表示を防止するために重要なものですが、このような内部統制が手作業で行われている場合には手作業による情報処理統制として評価を行います。「情報処理統制＝自動化された内部統制」と短絡的に理解しないように留意することが重要です。

① 自動化された情報処理統制のみ

データ出力側で把握されているデータ件数等とデータ入力側で把握されるデータ件数等が整合していることを確認し、整合しない場合には入力されたデータ処理を中止するといったＩＴアプリケーション上の機能（ＩＴアプリケーションに組み込まれている自動化された情報処理統制）

② 自動化された情報処理統制と手作業による情報処理統制の組合せ

エラーリストのように、ＩＴアプリケーションに組み込まれている自動化された情報処理統制において正常なデータではないと判断され、継続処理が中断となった対象データを出力した情報、又は、継続処理とは別の処理となった対象データを出力した情報を利用して、想定どおりに処理を行うよう、是正するために実施される手作業による情報処理統制

なお、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評価を行う場合、手作業に利用する情報を自動生成するような機能についても、自動化された情報処理統制と同様に必要な評価作業を行うことがあります。このような情報の自動生成の機能は、ＩＴ全般統制により支援されるＩＴにより自動化された機能であるため、当該機能それ自体の評価のみならず、関連するＩＴ全般統制の評価の要否を考慮することになります。

３．ＩＴ全般統制の分類

情報処理統制が主に取引データ等の処理に関する内部統制であるのに対して、ＩＴ全般統制は自動化された情報処理統制の継続した機能の維持に関する内部統制です。

監査基準報告書 315 付録６「ＩＴ全般統制を理解するための考慮事項」には、各ＩＴ環境（ＩＴアプリケーション、データベース、オペレーティング・システム、ネットワーク）に対して通常適用されるＩＴ全般統制の内容、ＩＴプロセス別のＩＴ全般統制の例が記載されています。

Ｑ５　監査人が理解する必要のある、企業のＩＴの利用状況及びＩＴ環境について教えてください。

（関連する報告書：監基報 315 第 11 項(1)、第 18 項(1)、第 19 項、第 25 項、A55 項）

Ａ５：

監査人は、重要な虚偽表示リスクを識別するのに役立つ情報を得るために、企業のＩＴの利用状況及びＩＴ環境を理解する必要があります。

監査基準報告書 315 第 18 項(1)によると、監査人は、企業及び企業環境に関する事項として、例えば、企業の組織構造、所有とガバナンス及びビジネスモデル（ビジネスモデルがＩＴをどの程度活用しているかを含む。）を理解できるように、リスク評価手続を実施しなければならないとされています。

企業のビジネスモデルは、様々な形でＩＴの活用に依拠しています。例えば、ある企業は実店舗において靴を販売しており、先進的な在庫管理システムやＰＯＳシステムを使って靴の販売を記録しているのに対して、別の企業は靴をオンラインで販売しており、ウェブサイト上での受注を含め、全ての販売取引処理がＩＴ環境で実施されている場合、両企業とも靴の販売をしていますが、ビジネスモデルが大きく異なるため、事業上のリスクも大きく異なります。監査基準報告書 315 の A55 項は、こうした例示を記載して、事業上のリスクの多くは財務諸表に影響を与えるため、財務諸表に影響を与える事業上のリスクを理解することは、監査人が重要な虚偽表示リスクを識別するのに役立つことを説明しています。

企業は、ＩＴを業務の支援や事業戦略を達成するために利用します。ＩＴを利用する範囲や程度によって、ビジネスモデルや事業上のリスクは異なり、これらは財務諸表にも影響を及ぼすため、重要な虚偽表示リスクを識別する上で、企業のＩＴの利用状況を理解することが求められています。この場合のＩＴとは、監査基準報告書 315 第 11 項(1)に定義されているＩＴ環境であり、ＩＴアプリケーション及びＩＴインフラストラクチャーをいい、ＩＴプロセスやＩＴプロセスに関わる要員も含まれます。

監査基準報告書 315 第 24 項によると、監査人は、リスク評価手続を通じて、例えば、重要な取引種類、勘定残高及び注記事項に関する企業の情報処理活動として、以下の事項を理解することにより、財務諸表の作成に関する企業の情報システムと伝達を理解しなければならないとされています。

・　企業の情報システムにおける情報の流れ
・　会計記録、特定の勘定及び情報システムにおける情報の流れに関連する他の裏付けとなる記録
・　注記事項を含む、財務諸表を作成するプロセス
・　これらに関連するＩＴ環境を含む企業の経営資源

さらに、監査基準報告書 315 第 25 項によると、監査人は、リスク評価手続を通じて実施する以下の識別及び評価により、統制活動を理解しなければならないとされています。

・　アサーション・レベルの重要な虚偽表示リスクに対応する内部統制について、ＩＴの利用から生じるリスクの影響を受けるＩＴアプリケーション及び関連するその他のＩＴ環境の識別
・　ＩＴアプリケーション及び関連するその他のＩＴ環境について、ＩＴの利用から生じるリスクと当該リスクに対応するＩＴ全般統制の識別
・　上記の個々の内部統制が、アサーション・レベルの重要な虚偽表示リスクに効果的に対応するようにデザインされているか、又は他の内部統制の運用を支援するように効果的にデザインされているかの評価及び業務に適用されているかの判断

すなわち、監査人は、企業の事業上のリスクが財務諸表に与える影響を踏まえて、重要な虚偽表示リスクを識別することに役立てるために、企業のビジネスモデルにおけるＩＴの利用状況を理

解する必要があります。また、財務諸表の作成に関する企業の情報システムと伝達を理解するためや、ＩＴの利用から生じるリスクとアサーション・レベルの重要な虚偽表示リスクとの関連性を考慮しつつ、それぞれに対応する内部統制のデザインの評価と業務に適用されているかの判断を実施するために、ＩＴ環境を理解する必要があります。

Ｑ６　企業のＩＴ環境を理解する際の留意点はどのようなものでしょうか。

（関連する報告書：監基報 315 第 23 項、第 24 項、第 25 項、A119 項、A128 項から A131 項、A159 項、付録５第４項）

Ａ６：

監査人が実施する企業のＩＴ環境の理解の程度は、一律なものではなく、リスク評価手続における監査人の判断に基づいて、必要かつ十分な範囲と深度で実施することになります。

監査基準報告書 315 第 24 項によると、監査人は、リスク評価手続を通じて得た、重要な取引種類、勘定残高及び注記事項に関する企業の情報処理活動の理解等により、財務諸表の作成に関する企業の情報システムと伝達を理解しなければならないとされています。

複雑でない企業の情報システム及び関連する業務プロセスは、大規模企業のそれと比べて精緻ではなく、ＩＴ環境も複雑でないことが多いですが、情報システムの役割は同様に重要です。経営者が直接関与する複雑でない企業では、広範囲にわたる会計手続の記述、詳細な会計記録又は文書による方針を必要としない場合があり、当該企業の監査においては、情報システムに関連する内容の理解に多くの工数をかける必要がなく、理解するために実施する手続は、観察や文書の閲覧よりも質問の割合が多くなる場合があります。しかしながら、関連する情報システムを理解することは、監査基準報告書 330 に従ったリスク対応手続を立案する上で変わらず必要であり、重要な虚偽表示リスクを識別し評価するのに役立つことがある（監基報 315 の A119 項参照）とされています。

情報システムに対する監査人の理解には、企業の情報システムにおける取引の流れや情報処理に関連するＩＴ環境が含まれます。これは、企業がＩＴアプリケーションや関連するその他のＩＴ環境を利用することにより、ＩＴの利用から生じるリスクが高まる場合があるためです（監基報 315 の A128 項参照）。

そして、企業のビジネスモデルや当該ビジネスモデルがＩＴをどの程度活用しているかを理解することにより、情報システムにおいて利用が想定されるＩＴの内容と利用の程度についての有用な情報を得られる場合がある（監基報 315 の A129 項参照）とされています。

監査人は、ＩＴ環境を理解する際に、情報システムにおける取引の流れや情報処理に関連する特定のＩＴアプリケーション及びその他のＩＴ環境を識別し、その内容や数を理解することに重点を置く場合があります。ＩＴアプリケーションのプログラム変更、又は、取引や情報を処理又は保存するデータベース上でのデータの直接修正により、取引の流れ又は情報システム内の情報が変更されることがある（監基報 315 の A130 項参照）とされています。

さらに、監査人は、重要な取引種類、勘定残高及び注記事項に関連する、企業の情報システムにおける情報の流れを理解するのと同時に、関連するＩＴアプリケーション及びそれを支援するＩＴインフラストラクチャーを識別することがある（監基報 315 の A131 項参照）とされています。

企業のＩＴ環境が複雑になるほど、ＩＴアプリケーション及び関連するその他のＩＴ環境の識別、ＩＴの利用から生じるリスクの決定、並びにＩＴ全般統制の識別においてＩＴの専門的なスキルを有するチームメンバーの関与の必要性が高まります。複雑なＩＴ環境については、このような専門家の関与は不可欠であり、広範な関与が必要となる可能性が高い（監基報 315 の A159 項参照）と考えられます。

なお、監査基準報告書 315 付録５第４項において、ＩＴ環境を理解する際に監査人が考慮する事項の例と、企業の情報システムにおいて用いられるＩＴアプリケーションの複雑性に基づくＩＴ環境の一般的な特性の例が示されています。

Ｑ７　監査業務にＩＴの専門的なスキルを有するチームメンバー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。

（関連する報告書：監査基準報告書 220「監査業務における品質管理」第６項(5)、(10)、A9 項、A17 項、監基報 315 第 25 項、A159 項）

Ａ７：

１．監査業務へのＩＴの専門的なスキルを有するチームメンバーの関与の必要性

監査人は、リスク評価を通じて、統制活動のうち、アサーション・レベルの重要な虚偽表示リスクに対応する内部統制を識別しなければならず、ここで識別された内部統制に基づいて、ＩＴの利用から生じるリスクの影響を受ける、ＩＴアプリケーション及び関連するその他のＩＴ環境を識別しなければならないとされています（監基報 315 第 25 項参照）。また、「企業のＩＴ環境が複雑になるほど、ＩＴアプリケーション及び関連するその他のＩＴ環境の識別、ＩＴの利用から生じるリスクの決定、並びにＩＴ全般統制の識別においてＩＴの専門的なスキルを有するチームメンバーの関与の必要性が高まる。複雑なＩＴ環境については、このような専門家の関与は不可欠であり、広範な関与が必要となる可能性が高い」とされています（監基報 315 の A159 項）。

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の専門的なスキルを有するチームメンバー（以下「ＩＴの専門家」という。）を関与させることを積極的に検討します。

２．ＩＴの専門家の位置付け

監査チームは、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から構成されます（監基報 220 第６項(5)）。専門職員には会計又は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（監基報 220 第６項(10)参照）。なお、状況に応じて、外部の専門家を起用する場合もあります。

また、監査チームに期待される適切な適性及び能力を検討する場合に監査責任者が考慮する事項として「ＩＴの知識及び会計又は監査の特定の領域を含む専門的知識」も含まれており（監基報 220 の A9 項）、ＩＴの専門家は監査チームの専門職員（監査以外の分野において専門知識を有する個人）という立場で監査に関与します。

３．ＩＴの専門家の実施業務

ＩＴの専門家が実施する業務は、例えば、ＩＴに関する専門的知識や経験が要求される、ＩＴ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、代替的手続の立案把握、不備に関する監査役等及び経営者とのコミュニケーション等が想定されます。また、情報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。

４．ＩＴの専門家を関与させる際の考慮事項

ＩＴの専門家を関与させる際の考慮事項としては、(1)業務指示の際の合意及び(2)監督及び監査調書の査閲が挙げられます。

ＩＴの専門家への業務指示の際の合意事項としては、例えば、作業の内容、範囲及び目的、並びにＩＴの専門家と監査チームの他のメンバーのそれぞれの役割並びにコミュニケーションの内容、時期及び範囲（監基報 220 の A17 項参照）等が考えられます。作業の内容、範囲及び目的は、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、監査責任者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ことが重要です。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です。

監督及び監査調書の査閲に関する事項としては、ＩＴの専門家の発見事項又は結論の適合性及び合理性、並びに他の監査証拠との整合性を含め、ＩＴの専門家の作業の適切性を評価すること（監基報 220 の A17 項）等が考えられます。すなわち、十分かつ適切な監査証拠となっているか、業務指示の際の合意事項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。

Ｑ８　企業によるＩＴの利用状況の理解及び情報システムに関連するＩＴ環境の理解を行う際の、ＩＴアプリケーション及びＩＴインフラストラクチャーに対する留意点はどのようなものでしょうか。

（関連する報告書：監基報 315 第 24 項、第 25 項、A128 項から 131 項、A160 項、付録５第４項、第 16 項から第 17 項）

Ａ８：

監査人は、リスク評価手続を通じた重要な取引種類、勘定残高又は注記事項に関する企業の情報処理活動の理解の過程で、企業の情報システムにおける情報の流れ（取引の開始から、それに関する情報の記録、処理、必要に応じた修正、総勘定元帳への取り込み、財務諸表での報告に至るまでの流れ）についても理解します（監基報 315 第 24 項参照）。これには企業によるＩＴの利用状況や情報処理に関連するＩＴ環境についても含みます。

企業によるＩＴの利用状況及び情報処理に関連するＩＴ環境を監査人が理解するのは、企業がＩＴアプリケーションや関連するその他のＩＴ環境を利用することによりＩＴの利用から生じるリスクが高まる場合がある（監基報 315 の A128 項参照）ため、及び企業のビジネスモデルや当該ビジネスモデルがＩＴをどの程度活用しているかを理解することにより、情報システムにおいて利用が想定されるＩＴの内容と利用の程度を理解するのに有用な情報を得られる場合がある（監基報 315 の A129 項）ためです。

監査人は、ＩＴ環境を理解する際に、情報システムにおける取引の流れや情報処理に関連する特定のＩＴアプリケーション及びその他のＩＴ環境を識別し、その内容や数を理解することに重点を置く場合があり（監基報 315 の A130 項参照）、重要な取引種類、勘定残高又は注記事項に関連する、企業の情報システムにおける情報の流れを理解するのと同時に、関連するＩＴアプリケーション及びそれを支援するＩＴインフラストラクチャーを識別することがあるとされています（監基報 315 の A131 項参照）。

「その他のＩＴ環境」には、ネットワーク、オペレーティング・システム、データベースが含まれ、状況によってＩＴアプリケーション間のインターフェースが含まれる場合もあります（監基報 315 の A160 項参照）。

情報システムにおける取引や情報処理の流れに関連するＩＴ環境の理解において、監査人は、利用されているＩＴアプリケーションの性質と特性、さらにはそれを支援するＩＴインフラストラクチャーやＩＴに関する情報を収集します（監基報 315 付録５第４項参照）。

１．ＩＴアプリケーションの性質と特性の理解の際の留意点

監基報 315 付録５第４項の表に、ＩＴ環境を理解する際に監査人が考慮する事項の例と、企業の情報システムにおいて用いられるＩＴアプリケーションの複雑性に基づくＩＴ環境の一般的な特性の例が示されています。ただし、これらの特性は傾向を示すものの、企業が利用するＩＴアプリケーションの性質によって異なることがあることに注意してください。

ＩＴアプリケーションの性質と特性を理解する際、例えば以下の事項を実施します。

(1) ＩＴアプリケーション一覧表の作成

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、ＩＴが利用されてい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並びに販売、購買及び物流といった業務アプリケーションの構成を、例えば、以下のような観点から把握して、ＩＴアプリケーション一覧表等を作成します。これらは情報処理統制を把握する際の基礎となるものです。

＜ＩＴアプリケーション一覧表の項目例＞

・　ＩＴ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
・　開発形態（パッケージ／自社開発等）
・　提供形態（オンプレミス／クラウド）
・　パッケージ名
・　アプリケーションオーナー
・　ユーザ部署
・　ユーザ数
・　処理する取引規模（トランザクション量等）
・　ハードウエア
・　オペレーティング・システム（ＯＳ）
・　データベース
・　ネットワーク　ほか

(2)　ＩＴアプリケーションの対象となる業務や取引種類及び注記事項を把握する際、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、相互の接点なども理解します。

(3) 企業の業務プロセスにおけるデータの流れの理解。主な観点は以下のとおりです。

・　ＩＴ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、商品ほか）と取引ファイルの全体イメージ
・　企業の業務プロセスにおける主要な入力原票及び帳票等（これらに関係する、ＩＴアプリケーションへの入力と出力を含む。）
・　監査上使用している帳票やファイル（これらに関係する、企業が利用するデータとＩＴアプリケーションの処理を含む。）

(4)　ＩＴアプリケーション間のデータの整合性を確認するため、ＩＴアプリケーション間で授受されるデータのインターフェースについて、その内容、タイミング・頻度、伝送方式等を把握します。また、企業によるデータ授受の際のチェック方法を内部統制として把握します。

２．ＩＴインフラストラクチャー（関連するその他のＩＴ環境）の理解の際の留意点

ＩＴの利用から生じるリスクの影響を受けるＩＴアプリケーションを監査人が識別していない場合は、通常、その他のＩＴ環境も識別されません。反対に、監査人が、ＩＴの利用から生じるリスクの影響を受けるＩＴアプリケーションを識別した場合は、関連するその他のＩＴ環境（例えば、データベース、オペレーティング・システム、ネットワーク）も識別される可能性が高くなります。その他のＩＴ環境は、ＩＴアプリケーションを支援し、また相互作用があるためです（監基報 315 の A160 項、付録５第 16 項及び第 17 項参照）。

ＩＴインフラストラクチャーを理解する際、例えば以下の事項を実施します。

(1) ハードウエア構成

使用しているハードウエアのメーカー、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、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・ソフトウエア構成

使用しているＯＳ、ミドルウエア、開発言語・ツール、アクセス管理用ソフトウエア、運用管理用ソフトウエア、データベース、ＩＴアプリケーション間のインターフェースのためのミドルウエア、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、ハードウエアと基本ソフトウエ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、取引先との注文・照会に特定のネットワークが使われている場合や、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。

３．外部委託の理解

現在では、外部委託業者によるサービスが充実・普及しています。アプリケーションについては、一から自社仕様で開発するスクラッチ開発よりも標準的な機能を備えたパッケージ・ソフトウェアを利用するケースが増えています。また、インフラストラクチャーについても、施設や設備を自社保有する以外に、データセンターやクラウドのような施設や設備の利用サービスを使うケースも増えています。

企業が外部委託業者を利用している場合には、契約書やサービス・レベル・アグリーメント等により、サービスの内容を理解するとともに、企業で当該サービスを適切に利用する上で構築した内部統制を検討することとなります（Q29 参照）。

Ｑ９　企業が、パッケージ・ソフトウェアを利用している場合、その計算処理の妥当性等を検証する際の留意点はどのようなものでしょうか。

（関連する報告書：監基報 315 付録５第６項）

Ａ９：

企業が利用しているパッケージ・ソフトウェアによる計算処理が、重要な虚偽表示リスクに対応する情報処理統制である場合、監査人は、その計算処理の妥当性等を検証する必要があります。

企業がパッケージ・ソフトウェアを利用する際には、通常、個々の企業組織・制度等に応じて環境設定の変更（例えば、計算処理に関するパラメータの設定や変更）を行い、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・ソフトウェアの計算処理機能と企業の採用する会計方針との整合性を検証する手続に加え、適用されている環境設定と入力される基礎データについて、計算結果の網羅性及び正確性に及ぼす影響を考慮して、これらの妥当性を検証する手続を立案します。

パッケージ・ソフトウェアの計算処理機能の有効性を検証する手続については、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方法又は監査人自らが表計算ソフトウエア等を活用して見積値や推定値を算出して比較分析する方法が考えられます。なお、検証対象の計算処理が、例えば退職給付債務の計算のように複雑であり、監査人自らが再計算することが困難な場合には、専門家の利用を考慮します。

パッケージ・ソフトウェアを利用するために適用されている環境設定と入力される基礎データの妥当性を検証する手続については、監査人が、これらの内容を把握・評価すること、また、その設定・入力・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を評価する方法が考えられます。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、システム上に設定された基準（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・変更手続が適切に行われているか等に留意し、検証手続を実施します。

なお、社会一般で普及している市販のパッケージ・ソフトウェアにカスタマイズやアドオンを行わずに利用する場合には、パッケージ・ソフトウェアの機能の有効性を検証する手続については、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。

Q10　パッケージ・ソフトウェアにカスタマイズやアドオンを行わずに利用しており、かつ、その計算処理の妥当性等を簡易な手続で検証できる場合とは、どのような場合でしょうか。

A10：

パッケージ・ソフトウェアの標準機能では対応できない情報処理に対応できるようにするためには、標準機能に変更を加えて作り変える方法と新たなプログラムを追加する方法があり、本回答では、前者をカスタマイズ、後者をアドオンと整理しています。

画面表示や出力帳票に関する軽微なカスタマイズやアドオンが行われていても、データの登録・変更・削除及び締切・自動計算等の変更を伴う重大なカスタマイズやアドオンが行われていない場合は、パッケージ・ソフトウェアによる計算処理の妥当性等に影響を及ぼさないため、監査上は、パッケージ・ソフトウェアにカスタマイズやアドオンを行わずに利用する場合に該当することがあります。

一方で、データに関連する処理等に影響を及ぼす重大なカスタマイズやアドオンが行われている場合は、通常、パッケージ・ソフトウェアの計算処理の妥当性等に影響を及ぼすことになると考えられるため、当該カスタマイズやアドオンによってパッケージ・ソフトウェアに組み込まれた機能の妥当性等を検証する必要があります。

監査人は、監査に関連するパッケージ・ソフトウェアのデータに関連する処理等に重大な影響を及ぼすカスタマイズやアドオンに該当するかどうかを判断するためには、アプリケーション・システム間のデータ連携等のインターフェースを含めたシステム構成（データベースの基本構造を含む。）を把握し、カスタマイズやアドオンの内容を理解することが重要です。

Q11　グループ監査におけるＩＴの利用の理解及びＩＴ環境の理解に関する内容と程度について教えてください。

（関連する報告書：監基報 600 第 16 項、第 25 項から第 28 項、A21 項、A46 項から A49 項、付録１）

A11：

監査人は企業及び企業環境、適用される財務報告の枠組み並びに企業の内部統制システムの理解を通じて、重要な虚偽表示リスクを識別し評価することが要求されており、グループ監査チームは(1)監査契約の新規の締結及び更新に当たって入手した、グループ全体統制を含む、グループ、その構成単位及びそれらの環境の理解を深めること、(2)連結プロセス（グループ経営者が構成単位に送付する決算指示書を含む。）を理解することを実施しなければならないとされています（監基報 600 第 16 項参照）。また、付録１（グループ監査チームが理解する事項の例示）には、下記のとおりＩＴに関連する事項も挙げられており、グループ全体統制及び連結プロセスの理解の一環として、ＩＴの利用の理解及びＩＴ環境の理解を実施することになります。これらを整理すると以下の表のとおりとなります。

	グループ監査チームが理解する事項の例示（ＩＴ関連抜粋）
グループ全体統制	・　同一のＩＴ全般統制によって管理されている、グループの全体又は一部を対象とする集中ＩＴシステム ・　全ての構成単位又は一部の構成単位に共通するＩＴシステム内の内部統制
連結プロセス	・　連結のためにＩＴがどのように構築されているか（手作業のプロセスと自動化されたプロセス、及び連結プロセスの様々な段階において構築されている手作業による内部統制と自動化された内部統制が含まれる。）。

また、監査基準報告書 330 に基づきリスク対応手続を実施する際に、グループ監査チームは、構成単位の財務情報に関し、グループ監査チーム又はその指示を受けた構成単位の監査人が実施すべき作業の種類を決定しなければならない（監基報 600 第 23 項参照）とされており、これらを十分に実施するために、構成単位におけるＩＴの利用の理解およびＩＴ環境の理解を実施することになります。各構成単位の業務プロセスは精緻でなくＩＴ環境も複雑でない可能性がありますが、このような複雑でない企業であっても、関連する情報システムを理解することは、監査基準報告書 330 に従ったリスク対応手続を立案する上で重要であり、重要な虚偽表示リスクを識別し評価するのに役立つことがある（監基報 315 の A119 項参照）ためです。

より具体的には、重要な構成単位（監基報 600 第 25 項及び第 26 項参照）あるいは重要な構成単位以外の構成単位（監基報 600 第 27 項及び第 28 項参照）について構成単位の財務情報の監査等を実施する場合に、重要な虚偽表示リスクに対してＩＴが関係すると考えられる場合には、各構成単位についてのＩＴの利用の理解及び IT 環境の理解と手続を実施することになり、その程度は、その構成単位が重要な構成単位か重要な構成単位以外の構成単位かによらず、監査を実施するために十分なものとすることになると考えられます。

《Ⅲ　情報処理統制》

Q12　ＩＴを利用した情報システム及び関連する内部統制を理解するための手続と、留意点について教えてください。

（関連する報告書：監基報 315 第 24 項から第 26 項、A44 項、A111 項から A118 項、A131 項、A154 項から A160 項、付録５第３項から第４項、第８項、付録６）

A12：

監査人は、リスク評価手続の一環として、企業の財務情報の取引の開始から記録、処理、報告に至るまでの業務プロセスのフローないし会計処理過程のうち、ＩＴが利用されている部分を識別するために、ＩＴアプリケーション（監基報 315 第 11 項(7)①参照）の構成を理解します。さらに、監査人は、情報のインテグリティのリスクに直接対応するＩＴアプリケーションの情報処理に関連した内部統制を識別し評価します。

ＩＴを利用した情報システムにおける内部統制には、情報処理統制とＩＴ全般統制が含まれます。情報処理統制は、企業の情報に関する方針が有効に適用されるための処理又は手続であり、自動化されている場合（すなわち、ＩＴアプリケーションに組み込まれている。）と手作業の場合（例えば、インプット又はアウトプットに係る内部統制）があり、他の情報処理統制やＩＴ全般統制を含む他の内部統制に依拠することがあるとされています（監基報 315 の A6 項参照）。監査人は、企業の統制活動の理解に際し、企業の情報システム内のインテグリティに対するリスクに企業がどのように対応しているかを理解しなければなりません。

Q13　自動化された情報処理統制のデザインと業務への適用を評価するに当たり、データを含めた処理の流れやシステム帳票の生成過程を理解する方法を教えてください。

（関連する報告書：監基報 315 第 12 項、第 24 項、A13 項、A124 項）

A13：

業務プロセスの理解と業務への適用の評価は、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等について、業務の主管部門、実施部門のみでは確認できない場合には、別途システム部門に確認することに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、例えば、以下のような事項を実施します。

- 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
- 入力画面又は照会画面の閲覧や入力操作の観察
- インターフェース元システムとインターフェース先システムのデータ照合
- アクセスログや操作ログの閲覧（インターネットビジネス等）

上記のほか、業務担当者やシステム部門担当者への質問を組み合わせて、理解を得られるようにします。

監査で利用するシステム帳票の生成過程を理解するには、上記に加え、以下のような事項も実施します。

- マスター・データやトランザクション・データ、変換テーブルと出力帳票との照合
- 再計算
- マニュアルでの加工が必要であった場合の操作の再実施や加工のインプットとなるデータの閲覧

承認プロセスがワークフロー化されていた場合には、以下のような事項も実施します。

- ワークフロー・システムへのログインに係る認証機能の観察
- 承認ルートの確認
- 承認権限者と非承認権限者それぞれにおける画面の観察
- 承認前後における申請データの画面上での閲覧（承認履歴や承認後の修正の可否の確認）

Q14　開発中のシステムについてもＩＴの利用から生じるリスクに対応するＩＴ全般統制を識別し評価するのでしょうか。

A14：

開発中の情報システムについて、ＩＴの利用から生じるリスクに対応するＩＴ全般統制についても、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重要となります。具体的には、主として以下の２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情報処理統制及びＩＴ全般統制の整備・運用状況等）。

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、下記４．の場合を除いてないものと思われます。

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も、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概要を把握し、財務諸表に重要な影響を与えるような課題を認識した場合は、是正を求めたり協議するなどの対応を行うことがあります。そのためには、情報システムの開発、改変に関する内部統制が適時に情報を経営者などの関係者に提供できるものかを評価することになります。

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があります。例えば、経営者に情報システムが適用される財務報告の枠組みに従った財務諸表の作成を適切に支援するという認識が薄く、経営者が

経営上の効率性やコスト削減を、財務諸表を作成する上で必要とされる重要な統制活動の整備やデータの保管よりも優先するようなことも起こり得ます。

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の整備・運用状況を検討します。

情報システムに適切な内部統制を組み込むためには、企業は企画・開発・調達段階で情報システム等に組み込むべき内部統制の内容を検討しますが、当該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が財務報告の信頼性を確保するだけの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、不適切なプログラムが本番環境で実行されることになるため、情報システムの信頼性に影響を及ぼします。

また、業務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整合していない場合には、会計数値に誤りがもたらされ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。

3．旧システムから新システムへのデータコンバージョン（データ移行）に関する統制活動

旧システムから新システムへデータ移行が行われる場合、監査人はデータ移行のための内部統制が、適切に整備・運用されているかについて検討します。

企業がデータ移行プロセスを適切に管理していない場合、必要なデータ移行が行われず新システムに正しくデータが引き継がれなかったり、移行時にデータが改竄されるおそれがあります。

4．開発遅延や中止となった場合の留意点

開発の遅延や中止が生じた場合には、その原因によっては上記の「2．情報システムに関する企画・開発・調達業務の統制活動」に記載されているような内部統制に関連した不備に起因することがあるので、必要に応じて再評価を実施する事になります。

Q15　自動化された情報処理統制の評価手続について説明してください。

（関連する報告書：監基報 315 第 25 項、A136 項、A141 項、監基報 330 第 9 項、A25 項、A26 項）

A15：

プログラムにより自動化された情報処理統制の評価手続では、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、ＩＴ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評価を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あらかじめ設定された出力結果や処理が実施さ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情報処理統制が正しく機能していても、処理結果を記録したデータが簡単に変更される可能性があっては、十分な信頼性が得られません。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、企業の取引が手作業によるチェックが実務的でないほど膨大な量になった場合、取引が定型化され内部統制をプログラム化することが可能になった場合、プログラム化した方が手作業よりも効率化できる場合等が契機となります。

１．自動化された情報処理統制とＩＴから自動生成される情報の例

⑴ 自動計算等

ＩＴ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、処理を自動化することにより、情報の網羅性、正確性、正当性等を確保します。特定の期日の到来や月次処理といったタイミングで、ＩＴアプリケーションでの金額の自動計算、減価償却費の計上、外貨換算の処理等が行われ、その結果が会計システムに連携され、自動的に仕訳が生成されるような処理まで行うものもあります。

⑵ レポート出力

ＩＴアプリケーションにより自動的に帳票を作成する機能をいいます。マスター・データやトランザクション・データなどの明細データを複数表示する明細レポート、数値項目を集計した集計レポート、取引データなどのシステムへの入力内容をそのまま表示するプルーフ・リスト、各種処理でエラーが発見された場合にそのエラーの内容を表示するエラーリストなどがあります。

⑶ 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様式や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。

⑷ マッチング

入力された内容を、あらかじめ定義されたマスター・データ等と照合し、そこ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、ＩＴ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と照合して、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。

(5) 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、入力データの合計額を記録しておき、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します。

(6) アクセス・コントロール

ユーザＩＤとパスワード等により、プログラムやデータを利用できる者を制限する機能をいいます。

例えば、ＩＴアプリケーションにユーザＩＤごとに使用できる機能を設定しておき、アクセスの許可はユーザごとのパスワードをアプリケーション利用時に入力することで管理する方法や、ユーザが排他的に使用する操作端末自体にＩＴアプリケーションの権限を与えておき、操作端末起動時にパスワードを入力するような設定にする方法があります。

２．自動化された情報処理統制とＩＴから自動生成される情報を照合する手続の例

自動化された情報処理統制とＩＴから自動生成される情報を照合するに当たっては、当該内部統制がどのように機能するかを仕様書の閲覧や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) サンプルテストによる照合

当該情報処理統制に依拠しようとする期間にわたって情報処理統制の運用の結果からサンプルを抽出してテストすることにより評価します。自動化された情報処理統制の場合、プログラムの整備状況が適切であれば、処理パターンが同じであれば、サンプルで抽出されたもの以外でも同様の信頼性になることが期待されます。

例えば、外貨換算の正確性を確かめる場合、一つの外貨について為替レートと外貨建ての売上金額により円建ての売上を再計算し、計上された円建ての売上金額とを照合して一致を確認できれば、他の外貨についても同様に正しく計算されると期待されます。

(2) 再実施

ＩＴに組み込まれた内部統制が有効に機能しているかを検証するために、実際に自動化された情報処理統制で行われている内部統制を再現し、同じ結果が得られるかどうかを確かめます。例えば、監査人が会社の業務で使われている端末に権限のないＩＤを入力してもデータやプログラムにアクセスできないことを確かめます。また、実際に本番環境に疑似データを流して仕様どおりの結果が得られることや、仕様と同じ計算環境を作り本番データの処理結果が同一であることを確かめます。

(3) ソース・プログラムのレビュー

ソース・プログラムのレビューとは、当該プログラムにより自動化された情報処理統制に関するコンピュータ・プログラムのソースコードを閲覧し、プログラムが正しく動作するように記述されているかを確認することです。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。

(4) システムクエリーのレビュー

システムクエリーとは、データベース管理システムに対する問合せのことでデータの抽出や更新などの処理要求を文字列で表します。処理対象のテーブルやデータの抽出条件、並べ方などを指定するものです。

通常 SQL というプログラム言語を使用してそれらが指定されます。この内容を閲覧することで、正しいテーブルから正しい条件で正しくデータが抽出又は更新される設定になっているかを確認することができます。そうすることで、プログラムが正しく動作するかどうかの心証を得ることができます。

また、ソフトウエアによっては、SQL での記述を行わずに上記を指定できるようなツールを備えているものがあり、これらの指定内容をそのツール上で閲覧することでも同様の確認をすることができます。

上記(1)から(4)の手続を期中に実施した場合、実施時から期末までの期間プログラムが変更されていないことがプログラムや仕様書の変更履歴等の閲覧により確認可能なＩＴ全般統制が存在するならば、期末に再び上記手続を実施する必要はなくなります。

上記の手続を本番環境以外の環境を用いて実施した場合、本番環境でも同じ動きとなる心証を得るため、手続を実施した環境と本番環境の同一性を、例えば、自動化された情報処理統制に関するコンピュータ・プログラムのバージョンの比較のような手続により確かめます。

自動化された情報処理統制と、ＩＴから自動生成される情報を照合する手続の種類・範囲及び実施の時期を決定する際には、自動化された情報処理統制とＩＴから自動生成される情報のＩＴの利用から生じるリスクを検討することになります。なお、統制活動における内部統制の識別と評価において、監査人は、重要な取引種類、勘定残高及び注記事項に関する取引の流れや企業の情報処理活動のその他の側面を規定する企業の方針に関連する全ての情報処理統制を識別し、評価することは求められていません（監基報 315 の A136 項参照）。

Q16　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。

A16：

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、紙への署名や押印により承認証跡を記録する代わりに、ＩＴアプリケーションにより承認の入力を行い、電子データ上に承認証跡を記録することです。

電子承認であっても、紙の伝票に残される署名・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機能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ります。

また、システム上に、承認又は拒絶を制御する仕組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。）などの仕組がシステム上設定される場合もあります。

承認行為に関する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、次の事項を満たす承認行為でなければ有効な内部統制として機能しないことに留意が必要です。

- 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。

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。

正当な権限者以外が承認できないようになっているかどうかは、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程に従っているか、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、更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、紙に書いて貼ってあるといった状況については、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、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、承認処理が未了のまま放置されることのリスクについても留意します。

Q17　電子署名やタイムスタンプ機能を用いた電子契約における監査上の留意点はどのようなものですか。

A17：

電子契約の普及やスキャナ保存制度の活用により従来書面で保存されていた証憑が電子的イメージで保存される場合もあります。証憑の作成・保存に電子署名やタイムスタンプ機能が活用されている場合には、その機能がどのようなものかを理解するとともに、適切な内部統制の元で実施されているかの理解が有用となる場合があります。タイムスタンプ機能では、記録されている時刻に該当する電子データが存在していたことと、それ以降改竄されていないことを証明することができます。改竄がなされていないかはタイムスタンプに記載されているハッシュ値とオリジナルの電子データから得られるハッシュ値を比較することで、タイムスタンプの付された時刻から電子データが改竄されていないことを確実かつ簡単に確認することができます。

書面の契約書では契約者による押印や署名により、その証拠としての法的効力を持つことになります。一方、電子契約では、電子媒体の契約書に電子証明及び認証業務に関する法律第２条及び第３条に該当し得る電子署名とタイムスタンプを付与することにより、紙の契約書と同等の法的効力を持たせています。

監査人にとっての基本的な留意点は、電子署名を用いた電子承認の場合、例えば次の事項が挙げられます。

- 電子署名は正当な権限者によって行われているか。
- 電子的イメージで保存された証憑は改竄ができないようになっているか。
- 電子署名は電子署名法に基づく要件を満たしているか。

１．電子署名は正当な権限者によって行われているか。

これは基本的に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程に従っているか、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。

電子署名機能により電子承認が行われている場合には、本人性の証明という点が重視され、二要素認証、クライアント証明書によるアクセス端末の制限やIPアドレス制限など様々なセキュリティ対策が同時に行われていることが多く、これらの機能の有効性を検証することでより強い監査証拠を得られる場合もあります。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．電子的イメージで保存された証憑は改竄が出来ないようになっているか。

PDF等の電子的イメージで保存された証憑は編集機能などにより改竄が可能であり、これを防止する為にタイムスタンプ機能が活用されている場合があります。

電子署名に加えてタイムスタンプが押されている場合、いつその契約書が承認されたものであるのか、また、記録された日付以降の改竄がなされていないかなどの検証が可能になります。

ただし、電子署名と同様にタイムスタンプも適切な管理者が実行しているかといった留意点は存在するため、タイムスタンプがある事のみをもって証憑が信頼できるとはならないことに注意が必要です。

３．電子署名は電子署名法に基づく要件を満たしているか。

電子署名を実現する仕組としては様々な方法がありますが、我が国においては、「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針」の第３条において、いずれも公開鍵暗号方式に基づく方式であるRSA、DSA、ECDSAの３方式を指定しています。

公開鍵暗号方式は、暗号化するときに「公開鍵」「秘密鍵」という対になる鍵を使う方式で、公開鍵は広く一般に公開しますが、秘密鍵を受信者だけが保持することで、文書の漏洩対策を行います。ただし、公開鍵暗号方式だけでは、公開鍵が本当に送信者のものかどうかの証明ができません。そこで、公開鍵暗号基盤（Public Key Infrastructure：PKI）を用いて公開鍵が送信者のものであると電子証明書を使って保証することがあります。

電子証明書とは、電子署名を印鑑の代替と考えた時に、印鑑証明書と同じ役割を果たすものです。印鑑証明書は書類に押された印影が真正であることを行政機関が証明しますが、電子証明書も同様に、公開鍵などの情報が真正であることを認証局が証明します。

これらの要件に該当するかの検証は、例えば電子署名に電子証明書が付されているかどうかの確認を行うこと等が考えられます。

Q18　売上を自動的に計上するシステムを採用している場合の自動化された情報処理統制の評価はどのように行うのでしょうか。

A18：

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や適用される収益認識に係る会計基準に従った処理が、システムによって実行可能であること、又は、適切な決算整理仕訳により調整可能であることが財務報告の信頼性を確保するための前提となります。

売上を自動的に計上している場合には、内部統制の評価においては、企業がどのような自動化された情報処理統制としているかを理解することが重要です。

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、以下のような点を考慮します。

(1) システム間のデータのインターフェー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・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。

代理人取引となる場合に、純額で収益を自動計上するシステムの場合には、上記に加えて例えば、以下のような点に留意します。

(5) 本人と代理人の区別がシステムで適切になされ、総額または純額で適切に計上されているか。

(6) 代理人の場合で、自動で売上と仕入の相殺により純額計上している場合、適切な相殺相手で相殺されるような仕組となっているか。

工事アプリケーションのデータを用いて一定の期間にわたり充足される履行義務に応じて工事売上を自動的に計上するシステムの場合には、上記(1)、(2)に加えて例えば、以下のような点を考慮します。

(7) 工事アプリケーションの工事進捗率を基に売上を自動的に計上するシステムの場合、進捗率計算の元となる発生原価が工事ごとに漏れなく集計され、進捗率が適切に計算されているか。

(8) 原価回収基準の場合、発生原価が工事ごとに漏れなく集計されているか。
(9) 取引価格で履行義務に配分されている場合に参照する取引価格が適切なものとなるような仕組となっているか、また、正確に配分計算がなされているか。

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、以下のような点を考慮します。

(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・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。）。実際の出荷日と出荷予定日が異なった場合、実際の出荷日に売上計上日が修正されているか

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の適切性、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。

4．ロボティック・プロセス・オートメーション（ＲＰＡ）を用いて売上を自動計上する場合

ＲＰＡとは、事務処理作業を担う担当者がＰＣなどを用いて行っている一連の作業を自動化できる「ソフトウェアロボット」のことです。あらかじめ入力用データを用意しておいて、ロボットにそれを読み取らせ、データの最後まで情報システムに自動で入力させるといったことがＲＰＡの典型的な例になります。

ＲＰＡを用いて自動的に売上を計上する場合には、例えば、以下のような点を考慮します。

(1) 売上計上のインプットとなるデータは、適切な承認又は信頼できるデータに基づいているか。
(2) 同じインプットデータが二重入力とならないように、適切に設計、運用されているか。
(3) 適切な職務分掌に基づき、入力が制御されているか。
(4) エラーデータは、適切にフォローアップされているか。
(5) 手作業の入力が、ＲＰＡに置き換わることが想定されますが、入力自体がＲＰＡに置き換わるだけで、売上計上に係るシステムの利用は変わらないため、「１．手作業の入力を基に自動計上する場合」の留意点も参照してください。
(6) ＲＰＡは業務担当者等でも容易に設定できる利点がありますが、通常のソフトウエアの導入や運用と同様に、適切なドキュメントの作成・維持の状況も確認することになります。

5．売上計上に関連して人工知能（ＡＩ）を利用する場合

需要予測に基づき商品単価を自動変動させるなど売上計上に関連してＡＩを利用する場合には、例えば、以下のような点に留意します。

(1) ＡＩに学習させるためにＡＩに入力するデータは、適切な承認又は信頼できるデータに基づいているか。

(2) ＡＩが行うデータ処理で使用する学習モデルは適切か。
(3) ＡＩで出力した結果は適切か、また不適切な結果が出た場合の補正はなされているか。
(4) ＡＩが利用する技術的特性や結果の導出方法など、ＡＩが出した結論を人間が理解できるようにするため、利用者への説明責任が果たせるようになっているか。
(5) ＡＩが適切な判断を下せるようにＡＩを適時・適切にチューニングがなされているか。

Q19　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ースの有効性はどのように検証するのでしょうか。

A19：

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、販売取引に関する会計仕訳の情報として会計アプリケーションへのデータの引渡しが想定されます。このようなインターフェースは、企業の利用するアプリケーションにより、販売アプリケーションの出力帳票に基づき会計アプリケーションに手入力するケース、販売アプリケーションで作成された電子ファイルを会計アプリケーションにアップロードするケース、販売アプリケーションから会計アプリケーションに自動的にデータが引き渡されるケースがあります。販売アプリケーションから会計アプリケーションに自動的にデータが引き渡されるような自動化されたインターフェースに適切な情報処理統制やＩＴ全般統制があれば、このインターフェース・データの正確性は高いものと考えられます。

アプリケーション間のデータ・インターフェースは、データを受け取るアプリケーションから見れば、入力方法に違いはありますが当該アプリケーションへのデータの入力に他ならず、このため引き渡されるデータの正確性を確保する必要があります。監査人にとって引き渡されるデータに重要性がある場合、インターフェー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ースの信頼性を検証するには、次のような三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。
- トータル・チェック等のインターフェースの信頼性を担保するシステムに実装されている内部統制が有効に機能していることを確かめる。
- 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ース自体にインターフェー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ー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ースの信頼性を検証する場合、販売アプリケーションの送信データと会計アプリケーション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．トータル・チェック等のインターフェースの信頼性を担保するシステムに実装されている内部統制が有効に機能していることを確かめる。

送信元システム及び送信先システムに実装されるインターフェー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) インターフェースの都度、送信先システムが受け取ったデータと送信元システムで保持しているインターフェースの元データを、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) インターフェースの都度、インターフェー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 仕様書上で送信元システム及び送信先システムに組み込まれているチェックの内容を確かめる。当該チェック内容が内部統制として適切かつ十分なものであるか検討する。

② 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など当該チェックが実際に機能していることを検証する。

３．インターフェースにそ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。

インターフェースの信頼性を担保するコントロールは、取り決めた以外のフォーマットやデータは連携させないよう送信元でチェック機能を設けたり、定められた仕様どおりのファイルフォーマット以外を受け付けない等送信先システムに組み込まれる場合のほか、インターフェースを管理するミドルウエアであるファイル転送ソフトに組み込まれていることがあります。

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、インターフェースの信頼性を担保する多彩な機能を備えています。一般的にインターフェー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ースにおける信頼性は高いといえます。ファイル転送ソフトに実装されているインターフェー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) 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ースにおいて、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ファイル転送ソフトに実装されていれば、データのインターフェースにおける信頼性は高いと言えます。

(2) 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決めのことです。

エラー訂正プロトコルは、通信時に発生したエラーの回復手順を示すプロトコルの一つであり、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。ファイル転

送ソフトが、エラー訂正プロトコルに基づいて、インターフェースが実行されるように制御していれば、データのインターフェースにおける信頼性は高いといえます。

上述(1)から(2)の機能は、インターフェー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、インターフェース元の帳票と関連するインターフェース先の帳票の照合

最近では、システム間インターフェースの手法としてＡＰＩ（Application Programming Interface）連携が多く用いられています。ＡＰＩとは、ソフトウェアコンポーネント同士が互いに情報をやりとりするのに使用するインターフェースの仕様であり、別々の会社に開発されたシステムであってもＡＰＩを活用することで容易にインターフェースが可能になります。ＡＰＩ連携は連携先システムの仕様を知らずとも、インターフェースが可能となり、また、個別にシステム連携プログラムを開発するのに比して導入コストが低いことから広く使われるようになってきました。

ＡＰＩ連携においても、上述の方法によりインターフェースの有効性を検証することが有用となります。

情報処理統制が自動化されている程度が大きいほど、ＩＴ全般統制の重要度が増します。例えば、情報処理統制の継続的で有効な運用は、情報処理統制を実現しているプログラムに対する不正な変更を防止又は発見するＩＴ全般統制（すなわち、関連するＩＴアプリケーションに対するプログラム変更に関する内部統制）の有効性に依存する場合があります。このケースにおいてＩＴ全般統制が有効ではないと予想される場合又は監査人にＩＴ全般統制を評価する計画がない場合は、統制リスクが高く評価されることがあります。

Q20　監査上、企業のＩＴアプリケーションにより企業が作成した情報を利用する場合の留意点にはどのようなものがありますか。

（関連する報告書：監基報 315 第 25 項、A151 項、A154 項、付録５）

A20：

１．企業が作成した情報

企業が作成した情報は、監査人の利用目的に照らして「企業が内部統制において利用する情報」と「監査人が監査証拠として実証手続において利用する情報」に大別することができます。

企業が作成した情報は、元データ・ロジック・パラメータによって生成されており、利用目的の如何を問わず、情報のインテグリティの担保が重要となります。

２．監査手続

・　ＩＴアプリケーションの理解、元データの特定

企業が作成した情報がＩＴアプリケーションによって作成されている場合、監査人はまず、情報がＩＴアプリケーション内のどのデータに基づいて作成されているかという点につき理解します。

・　ＩＴアプリケーションの処理の理解・検証

監査人は仕様書の閲覧などにより、情報の作成に関するＩＴアプリケーションの処理機能を把握し、そのロジックが目的に照らして適切であるか否かを確かめます。

・　元データの信頼性（正確性、網羅性、正当性）

監査人は元データと総勘定元帳や補助元帳などの数値との突合を行い、その正確性、網羅性を確かめます。また、非財務情報についても、外部証憑と突合するなど、その正確性を確かめる点にも留意します。

上記の他、データの作成プロセスを理解することで、そのデータが承認を得た正当なデータであることを確かめることもあります。

・　入力パラメータの正確性

情報の作成に当たって、パラメータを手入力で設定する場合は、入力されたパラメータが目的に照らして適切であるか否かを確かめます。

上記理解を確認するためには、データのインプットから情報作成までのプロセスの再実施を行うことが有効です。

また、企業が作成情報の正確性や網羅性の維持に関連する内部統制を構築している場合は、その内部統制を識別・評価します。

３．監査上の留意点

情報を作成するＩＴアプリケーションは、ＩＴの利用から生じるリスクの影響を受ける可能性が高く、情報の重要性によっては、監査人はＩＴアプリケーションのプログラムやデータの不適切又は未承認の変更に関連するリスクに対するＩＴ全般統制を識別し、ＩＴアプリケーションのＩＴ全般統制の整備・運用状況評価を検討する必要があります。

ＩＴ全般統制が有効に運用されていない場合は、ある一時点において情報が意図したとおりに作成されていても、その情報が継続的に意図したとおりに作成されているという心証は得られないということに留意します。

この留意点は監査人が実証手続において監査証拠として利用する場合に限らず、企業が内部統制において利用する場合でも同様です。

Q21　企業がＩＴアプリケーションから作成し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。

（関連する報告書：監基報 315 第 25 項、A154 項、付録５）

A21：

ＩＴアプリケーション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、その情報のインテグリティについて関連する情報処理統制を評価します。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、全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、延滞期間や滞留期間に応じて、適切に分類・集計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ＩＴ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、その情報のインテグリティに関する情報処理統制を支えるＩＴ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環境設定の理解、すなわち、業務上の延滞債権や滞留在庫の定義と、ＩＴアプリケーション上での延滞、滞留の判定条件が整合しているかを確認します。
- 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、ＩＴアプリケーションからの出力帳票（又はデータ）であるため、インプットされた売上債権や在庫情報のデータが、どのように蓄積、分類、集計されてリストとして出力されているのかを理解することが重要です。
- 商品の入出庫日付や製品数等のデータは、会計システムの財務諸表作成機能とは別の機能であったり、別のシステムで管理され集約した結果が会計システムに連携されることがあります。そのため、滞留在庫リスト等を構成する情報の各項目のうち、非財務情報についても、外部証憑と突合するなど、その信頼性を確かめることに留意します。

・　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、そのデータの合計金額が財務諸表、総勘定元帳及び補助元帳に一致することを確認します。そして、入手した債権データや在庫データを基に、業務上の延滞債権や滞留在庫の定義に従い監査人が再計算を行い、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。

Q22　ＥＵＣの監査上の留意点はどのようなものがあるでしょうか。

（関連する報告書：監基報 315 付録５）

A22：

１．ＥＵＣとは

ＥＵＣ（エンドユーザー・コンピューティング）とは、システムの開発・運用を情報システム部門等で集中的に管理するのではなく、利用部門（エンドユーザー）が実施する管理体制を指します。ＥＵＣでは市販のパッケージ・ソフトウェアが利用される場合もあれば、スプレッドシート等の汎用ソフトウエアをＥＵＣのツールとして用いて独自の処理に使う場合もあります。

企業において使われるスプレッドシートは、単純な集計から、マクロ機能を用いて通常のコンピュータの自動計算と同じような複雑な計算処理まで様々な使い方がありますが、比較的単純なスプレッドシート（マクロ機能を含む。以下同様）については、手作業による検算や、スプレッドシートの整合性チェックツールの利用による補完統制により、信頼性を損なうリスクを低減できる場合もあると考えられます。

一方、自動化機能を多用したスプレッドシートの利用や、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処理が行われている場合には、自動化された情報処理統制と同様の、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、ＥＵＣツールにも、通常のシステムの管理と同等の管理が必要となることがある点に留意します。

２．監査上の留意点

特にスプレッドシートをはじめとしたツールについては、仕様書の作成や変更記録の作成等の全般的な管理体制、アクセス制限に関する内部統制を整備することが困難であることが多く、ＩＴ全般統制と同等の有効性を確保することが難しい場合もあります。

監査人は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リスク評価手続の内容、範囲等を検討します。

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。

・　処理の複雑さ

・　処理する金額の重要性
・　処理する内容・目的
・　変更頻度
・　他システムとの連携の程度等

利用しているＥＵＣのツールが簡易だからといって、統制リスク評価手続が不要となるものではなく、その処理が監査上重要なものと判断される場合は、処理のプロセスを確かめるために設定内容を確認するなどの統制リスク評価手続を実施することに留意します。

Q23　「自動化された情報処理統制」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。

（関連する報告書：監基報 315 第 11 項、A5 項、監基報 330 第 12 項から第 13 項、A34 項から A38 項）

A23：

期中で内部統制の運用状況の有効性に関する監査証拠を入手した場合、運用評価手続を実施した後の当該内部統制の重要な変更についての監査証拠を入手し、また、期末日までの残余期間における追加的な監査証拠の入手を検討します。同様に過年度に入手した監査証拠を利用する際には、当該内部統制の重要な変更が過年度の監査終了後に発生しているかどうかについて監査証拠を入手します。

とりわけ「自動化された情報処理統制」は、「ＩＴアプリケーションに組み込まれている」内部統制であり（監基報 315 の A6 項参照）、プログラムに変更が加えられない限り、ＩＴによる処理に一貫性があります。したがって、監査基準報告書 330 第 12 項及び第 13 項にて記載されている内容や、情報処理統制に関連した障害の発生状況等を考慮した上で、特に(1)関連するＩＴ全般統制が有効であり、(2)「自動化された情報処理統制」に関係するプログラムに変更が加えられていないことを確かめられた場合に、当該「自動化された情報処理統制」については、過年度の監査証拠を利用することが可能となります。

「自動化された情報処理統制」に関係するプログラムに変更が加えられていないことを確かめるために、監査人はまず、前年度からの変更の有無を質問により確かめます。変更がないとの回答が得られた場合は、次にその裏付けを得るため、以下のような手続を実施します。

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

パッケージ・ソフトウェアであれば、バージョン情報を確かめることにより、当該ソフトウエアの更新の有無を確かめることが一般的に可能です。

またバージョンアップ時には、ベンダーからのリリースノートと称される書面に、変更又は追加された機能等についての説明が記載されていますので、その内容を確かめることで、「自動化された情報処理統制」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。

一方、バージョンアップがなくても、環境設定の変更により「自動化された情報処理統制」に影響が生じている可能性がありますので、そのような環境設定変更の有無についても留意します。

２．自社開発ソフトウエアやアドオン開発されているＥＲＰ（Enterprise Resource Planning）を利用している場合

「自動化された情報処理統制」に関係する個々のプログラムを特定し、当該プログラムの最終更新日付をシステム上で確かめることにより、運用評価手続の実施以降にプログラムが変更されていないことを直接的に確かめます。この手続により、自動化された情報処理統制に影響のあるプログラムに変更が無いと判断した場合、過年度の検証結果を利用することが可能です。この場合は、「自動化された情報処理統制」を実現するプログラムを正確かつ網羅的に特定することが重要となることから、手続の実施に当たってはＩＴの専門家の関与の必要性が高くなると考えられます。また変更がない場合であっても、ＯＳの保守期限が到来していたり、適用すべきパッチファイルが適用されていないなど、「変更がない」こと自体が適切であるか否かを検討することにも留意します。

Q24　ＩＴの利用から生じるリスクとアサーションの関連性について、説明してください。

（関連する報告書：監基報 315 第 11 項(4)）

A24：

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、監査人が重要な虚偽表示リスクの識別、評価及び対応において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（監基報 315 第 12 項(1)）。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もあります。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、Ｑ１で示したようなＩＴの利用から生じるリスクを考慮した上で、経営者はＩＴに対する内部統制を構築することになります。

ＩＴの利用から生じるリスクは通常、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ＩＴの利用から生じるリスクがどの程度影響を及ぼすかについて監査人が判断を下すという点で関連性を有するといえます。

《Ⅳ　ＩＴ全般統制》

Q25　財務諸表監査上、ＩＴ全般統制を評価する意味はどのようなものでしょうか。

（関連する報告書：監基報 315 第 12 項(1)、第 25 項から第 26 項、A150 項、監基報 330 第 9 項、A23 項及び監基報 500 の A31 項）

A25：

１．ＩＴ全般統制の定義

監査基準報告書 315 第 12 項(4)では、ＩＴ全般統制を「ＩＴ環境の継続的かつ適切な運用を支援する企業のＩＴプロセスに係る内部統制のことをいう。ＩＴ環境の継続的かつ適切な運用には、継続して有効に機能する情報処理統制及び企業の情報システム内の情報のインテグリティ（すなわち、情報（データ）の網羅性、正確性、正当性）の確保が含まれる。」と定義しています。

具体的には、アクセス権管理のプロセス、プログラムや他のＩＴ環境への変更を管理するためのプロセス、ＩＴ業務を管理するプロセスといったＩＴプロセスに係る、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。

２．ＩＴ全般統制を評価する意味

監査基準報告書 315 第 26 項において、ＩＴの利用から生じるリスクの影響を受ける、ＩＴアプリケーション及び関連するその他のＩＴ環境について、監査人は当該リスクに対応するＩＴ全般統制を識別し評価することが要求されています。ＩＴ全般統制を評価する意味を(1)情報処理統制、(2)情報のインテグリティの確保との関係で説明すると以下のようになります。

(1) 情報処理統制

ＩＴ全般統制が情報処理統制の継続的な運用を支えるという関係性にあるため、情報処理統制が自動化されている程度が大きいほど、ＩＴ全般統制の適用の重要度が増します。例えば、情報処理統制の継続的で有効な運用は、情報処理統制を実現しているプログラムに対する不正な変更を防止又は発見するＩＴ全般統制（すなわち、関連するＩＴアプリケーションに対するプログラム変更に関する内部統制）の有効性に依存する場合があります。

(2) 情報のインテグリティの確保

例えば、ＩＴアプリケーションによって生成されている、企業が作成した情報を監査証拠として利用する場合、監査人は当該情報に対する内部統制を評価する場合があります。ここでいう内部統制の評価には、不適切若しくは未承認のプログラム変更リスク又はレポート上のデータの直接変更に対するＩＴ全般統制の識別や評価を含むことがあります。

３．ＩＴ全般統制を評価する上での留意点

ＩＴ全般統制の評価は、ＩＴの利用から生じるリスクに対応するために実施されるものであるため、監査人は、識別すべきＩＴ全般統制を決定する際には、識別されたＩＴアプリケーション、その他のＩＴ環境及びＩＴの利用から生じるリスクについて得た理解を利用することが有用と考えられます。運用評価手続に当たっては、手作業による内部統制同様に、発生頻度に応じ

たサンプリングが必要である点、残余期間における有効性の評価が必要である点に留意し、十分かつ適切な監査証拠を入手できるよう、監査手続を立案、実施する点に留意します。

また、ＩＴ全般統制は、「ＩＴ環境の継続的かつ適切な運用を支援する」ものですから、ＩＴ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「情報処理統制も有効である」又は「情報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。ＩＴ全般統制の運用評価を実施しない場合、関連する情報処理統制が継続して有効に機能している心証を得るため、評価手続を立案することにも留意します。

《Ⅴ　パッケージ・ソフトウェア》

Q26　ＥＲＰが利用されている場合の留意点はどのようなものがあるでしょうか。

（関連する報告書：監基報 315 付録５第４項、付録６第２項）

A26：

ＥＲＰ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ＩＴ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．情報処理統制の観点

(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ＩＴ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、重要な設定について質問を行う、そして、監査人が実際にユーザの使用する画面を操作し、機能を確認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ＩＴアプリケーションに入力することで、実際の物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ＩＴ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となっていることがあります。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上書され、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ため、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情報のインテグリティの確保のための企業の検証手続が重要となります。その際、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のモジュールを全ては利用せず、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ＩＴ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ＩＴ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内部統制をデザインしているかを理解します。

２．ＩＴ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)。パラメータ値の例としては以下のようなものが挙げられます。

・ 棚卸資産の評価方法（移動平均法、先入先出法等）
・ 上位者の電子承認を要する金額の閾値（例：百万円以上の取引については、担当取締役の承認が定められている等)

重要な自動化された情報処理統制について、パラメータ設定が可能な場合、ＩＴ全般統制の観点では企業の業務に適合したパラメータ値となるよう、承認、事後検証等の管理手続が取られているか、パラメータ値を変更できる権限が、職務上必要なユーザに限定して付与さ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（いわゆるアドオン・カスタマイズ)。このような追加機能に関しては、自社開発のＩＴアプリケーションに関するＩＴ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。

Q27　会計帳簿の作成などに、市販の簡易なパッケージ・ソフトウェアを利用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。

（関連する報告書：監基報 315 第 21 項、第 25 項、A96 項、A158 項、付録５第４項、第６項、付録６第２項、監基報 402）

A27：

市販の簡易なパッケージ・ソフトウェアとは、店頭販売されるようなカスタマイズできないパッケージソフトであり、多くの企業に使用され、その実績が認められている会計システムなどが該当します。また、中堅企業向け等のパッケージ・ソフトウェアでカスタマイズ可能なものであっても、カスタマイズせずに利用する場合は、個別事情を勘案して同様に取り扱うことができる場合があります。これらは、「ＩＴの利用から生じるリスクの影響が高くない場合」の一つの要素に該当し、Q42 で述べているような柔軟な適用を検討することが可能です。

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。各ソフトウエア会社が開示している機能一覧表などを参考に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、主として中小規模の企業を対象ユーザとしている事も多いため、導入コストを抑えるために機能を限定したり、経理業務の経験が乏しい担当者にとって「融通を利かせる」、「使い勝手をよくする」ために、統制機能を省いたり、動作を停止させることもあります。

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、十分な統制機能を有しているか否かだけでなく、さらに、企業がそれらの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・ソフトウェアの利用に当たり、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。

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．基本仕様と初期設定項目（パラメータ）の導入設定・維持等

(1) 仕訳認証：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

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) 変更履歴が残る仕組：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

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になっているため、改竄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竄された場合には、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) アクセス管理：仕訳データへのアクセス管理

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、改竄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が利用されているかを把握します。特に、一つのユーザアカウント（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) 締め処理の実施、期首財務諸表数値の確認

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。

(5) 自動採番、消費税処理、その他配賦の自動計算処理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、伝票自動採番、消費税処理、その他配賦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。このような場合、以下の事項を確かめます。

- 伝票採番等の会計ソフト等の統制機能に係るパラメータ初期設定が適切に行われているか。
- 自動仕訳の基礎となる消費税処理、その他配賦計算処理等に係る初期設定が適切に行われているか。

この税率等に税法改正等に伴う更新が必要な場合、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ことがあります。そこで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、被監査会社によって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。

(6) データの保管、バックアップ

市販の簡易なパッケージ・ソフトウェアを利用し、クライアントＰＣ等にデータを保管している場合には、データの改竄・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。

２．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、データを改竄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竄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。

３．バージョンアップ

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。

４．クラウド会計システムを利用している場合

会計システムのソフトウエアを購入するのではなく、ベンダーがクラウド環境下に設置したソフトウエアをネットワーク経由で利用するようなサービスを使うことがあります。このようなクラウド会計システムを利用する際、自社保有とパブリッククラウドの違いとそれによるリスクを考慮せずに、市販の簡易なパッケージ・ソフトウェアとして評価を行うことがないよう、パブリッククラウド利用のリスクについて検討することは重要です。例えば、会計システムの管理者権限を社外のベンダーが保有する場合には、不適切なアクセスのリスクに対する内部統制について、いかに把握するかが課題になります。また、データのバックアップ体制等についてもベンダーと契約した内容で十分にリスク対応されているかの検討が重要になります。

上記のような事項についてもクラウド業者に往査して十分な情報を得ることは、パブリッククラウドの他の利用者への守秘義務の関係で、制限が加わることも多くあります。そのためクラウドに係るリスクへの対応としては、クラウド会計システムに係る、監査・保証実務委員会実務指針 3402「受託業務に係る内部統制の保証報告書に関する実務指針」に基づき発行された保証報告書等を取得して利用することが考えられます。

《Ⅵ　外部委託》

Q28　ＩＴに関する委託業務にはどのようなものがありますか。

A28：

ＩＴに関する業務の全てを内製化するだけの要員を保有し維持できる企業は限られており、一部の業務を外部委託する状況が増えています。

外部委託する業務としては、開発や保守のように需要に応じた都度委託するものもあれば、運用のように反復継続して委託するものもあります。また、運用については、サーバの死活監視や、バックアップの実施、利用者のＩＤの管理などＩＴ全般統制に関係する業務や、データの入力や更新業務のようなＩＴ情報処理統制に関する業務があります。業務を委託する委託先の対応としては、企業内に常駐して支援する場合や、必要な都度の訪問、ネットワークを利用したリモートによるサポートなどが考えられます。そのため、委託先の管理として社内の従業員に準じた管理もあれば、レポートや定例会などにより管理する場合もあります。

Q29　一般的な委託業務の形態を教えてください。

A29：

委託業務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

ハウジングとは、顧客の通信機器やコンピュータ（サーバ）を、自社の回線設備の整った施設（データセンター）に設置することをいいます。アウトソース先は基本的に機器の設置場所である施設を提供するだけですが、運用・保守の一部のサービスを合わせて提供する場合もあります。

２．ホスティング

ホスティングとは、通信事業者やインターネットサービスプロバイダが保有するサーバを、ネットワーク経由で顧客に貸し出すサービスのことをいいます。

３．共同センター

共同センターとは、複数の企業のため、共通の業務処理システムを稼動させ、受託した様々なデータ処理を行うコンピュータ・センターをいいます。共同センターには、一定地域の同業種の企業数社が共同出資でコンピュータを設置して計算処理を行うもの又は商工会議所などの公共機関が運営し、主として小規模企業を対象として受託計算を行うものがあります。また、金融機関では、信用金庫等が事務処理の共同システムセンターを設置し、稼動させている例があります。

４．ＡＳＰ（Application Service Provider）

ＡＳＰとは、インターネットを通じて事業用のアプリケーション・ソフトウエアを顧客にレンタルする事業者をいいます。ユーザはウェブブラウザを使って、ＡＳＰのサーバにインストールされたアプリケーション・ソフトウエアを利用するため、個々の使用するＰＣにアプリケーション・ソフトウエアをインストールする必要がなくなります。

５．クラウドサービス

インターネットに接続する環境で、ネットワーク上にある不特定のサーバの提供するサービスを必要に応じて利用できるようにする概念です。

クラウドサービスには提供されるサービスの範囲により以下三つの形態があります。

・ IaaS（Infrastructure as a Service）

クラウド事業者がプロセッサー、ストレージ、ネットワーク等のハードウエアを提供するサービス

・ PaaS（Platform as a Service）

クラウド事業者が IaaS で提供するハードウエアに加えて、ＯＳ、ミドルウエア等のシステム・ソフトウエアをも提供するサービス

・ SaaS（Software as a Service）

クラウド事業者が PaaS で提供するハードウエア、ＯＳ、ミドルウエアに加えて、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サービスで、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、アプリケーションの一部貸し出しの仕組です。

顧客はソフトウエアを所有せずに、必要な機能を必要なときに機能単位で利用することができ、利用した機能に応じた料金のみを支払います。

Q30　委託業務に関する内部統制を評価する場合の留意点はどのようなものでしょうか。

A30：

委託業務に関する内部統制を検証する場合、委託会社監査人は、監査基準報告書 402「業務を委託している企業の監査上の考慮事項」に従って内部統制の評価を実施することが必要です。

クラウド会計システム等のクラウドサービスも委託業務に該当します。クラウドサービスを利用する際、自社保有との違いとそれによるリスクを考慮せずに、市販の簡易なパッケージ・ソフトウェアとして評価を行うことがないよう、クラウドサービス利用のリスクについて検討することは重要です。例えば、システムの管理者権限をクラウド業者が保有する場合には、不適切なアクセスのリスクに対する内部統制を含むＩＴ全般統制について、いかに理解及び評価するかが課題になります。また、データのバックアップ体制等についてもクラウド業者と契約した内容で十分にリスク対応されているかの検討が重要になります。

クラウド業者に往査して十分な情報を得ることは、クラウドサービスの他の利用者への守秘義務の関係で、制限が加わることも多くあります。そのためクラウドサービスに係るリスクへの対応としては、「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)」を入手することが考えられます。

《Ⅶ　自動化されたツール及び技法とＣＡＡＴ》

Q31　自動化されたツールと技法及びコンピュータ利用監査技法（ＣＡＡＴ）とは、どのようなものですか。

（関連する報告書：監基報 315 第 13 項、A21 項、A33 項、監基報 330 の A16 項）

A31：

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、コンピュータを利用して監査手続を実施する技法であり、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。企業のＩＴの利用度が高まると、監査で用いる取引記録や関係資料も紙ではなく電子データで保管されることが多くなります。そのため、監査手続の実施に際しても当該電子データをコンピュータに取り込み解読することになります。

そして電子データであれば、単に目視するだけでなく当該データを市販の表計算ソフト等で再計算や分析などを行い、効率的な監査手続の実施が可能となります。さらに、データ容量が大きい場合や複雑な加工が必要な場合には、データ分析の専用ソフトウエアを用いて監査人が設定した条件に該当する項目を抽出することもあれば、母集団の統計的分析や可視化なども行うことがあります。このようにコンピュータ利用監査技法（ＣＡＡＴ）とは利用するツールの話ではなくツールを利用して監査手続を実施する技法のことをいいます。ＣＡＡＴを利用することによって電子的な取引ファイルと勘定ファイルに対する広範な手続が可能となり、重要な電子データからのサンプルの抽出、特性に基づいた取引のソート、母集団全体の検討ができるとされています（監基報 330 の A16 項参照)。

これに対して、監査基準報告書 315 の A21 項では、自動化されたツールと技法という用語が用いられています。自動化されたツールと技法では、ＡＩ、ＲＰＡやドローン等や今後新たに開発されるテクノロジーの利用も想定されており、ＣＡＡＴやデータ分析を含む、より幅広い概念の用語として用いられています。

なお、Q32 については監査基準報告書 315 に合わせて自動化されたツールと技法という用語を用いており、Q33 からQ35 については、監査基準報告書 330 に合わせてＣＡＡＴという用語を用いています。

Q32　リスク評価手続における自動化されたツールと技法の利用法について教えてください。

（関連する報告書：監基報 315 第 13 項、第 24 項、A21 項、A31 項、A52 項、A125 項）

A32：

監査人は、自動化されたツールと技法を使用して、分析、再計算、再実施又は調整のための（総勘定元帳、補助元帳又はその他の業務上のデータの）大量のデータに関するリスク評価手続を実施することがあります。

分析的手続は、自動化が可能な多くのツール又は技法を利用して実施することもあります。近年では、データ分析のための新たなツールの開発が進み、従来のツールに比べて、より大きなサイズのデータをより高速に処理し、様々な観点からの分析を柔軟に実施して、視覚的に分かりやすいフォームで出力することができるようになっています。データ分析には、様々な方法がありますが、監査人が、母集団を構成する項目の特徴が十分に把握されていない段階において、母集団データに対して様々な分析を行う方法もあります。例えば売上高の金額を基準とした階層ごとの項目数や、月別や地域別の売上高等の様々な分析軸を組み合わせて監査人の理解を深めることで、重要な虚偽表示リスクや不正の兆候を識別することが期待できます。

監査人は、情報システムを理解するための監査手続の一部として、取引及びプロセスのフローを理解するために、自動化されたツール及び技法を利用することがあり、その手続の結果として、監査人が企業の組織構造又は企業の取引相手（例えば、仕入先、顧客、関連当事者）に関する情報を入手することがあります。

また、監査人は、取引の会計記録を保存する企業の情報システムのデータベースに直接アクセスする、又は電子的にダウンロードするために、自動化された技法を使用することがあります。監査人は、当該情報に自動化されたツール又は技法を用いて、会計記録の開始から総勘定元帳への記録に至るまで、特定の取引に関する仕訳入力若しくは他の電子的な記録又は取引の母集団全体に関する記録を追跡することにより、情報システム内の取引の流れについて監査人の理解を確認することができます。また、網羅的な又は大規模な一連の取引を分析することにより、通常の又は想定される処理手続からの当該取引の差異が識別され、その結果、重要な虚偽表示リスクが識別される可能性があります。

また、自動化されたツール又は技法が、観察又は文書の閲覧のために利用されることもあります。例えば、特定の資産について、ドローンといった遠隔監視ツールが利用されることがあります。

なお、自動化されたツールと技法については IAASB から「Non-Authoritative Support Material: Using Automated Tools and Techniques When Identifying Risks of Material Misstatement in Accordance with ISA 315 (Revised)」が公表されていますのでご参考にしてください。

Q33　仕訳テスト及び連携して実施すべき取引テストを実施する際にコンピュータ利用監査技法（ＣＡＡＴ）を利用した方がよいのは、どのような場合でしょうか。

（関連する報告書：監査基準報告書 240「財務諸表監査における不正」第 31 項、監基報 330 第 19 項）

A33：

１．仕訳テスト及び連携して実施する取引テストの留意点

(1) 仕訳テストの意義

本実務ガイダンスにおいて、仕訳テストとは、監査基準報告書 240 第 31 項(1)にある財務諸表作成プロセスにおける特定の仕訳入力及び修正について検証するために仕訳データを対象として実施する手続を指します。

また、経営者による内部統制を無効化するリスク等に対応するための手続として、仕訳データだけでなく取引データを対象とした取引テストを実施することが考えられます。

(2) 仕訳テストを実施する際の留意点

- 仕訳テストの対象となる仕訳の母集団の網羅性を検証する際、入手した仕訳データの合計と合計残高試算表の貸借取引発生額の合計が整合しており、不完全な仕訳データの母集団となっていないことを確認します。例えば、起票された全仕訳のデータを期首残高に加算し、期末日現在の試算表の残高と照合して検証することが考えられます。
- 合計仕訳等の仕訳データによる仕訳テストでは不十分な場合、合計仕訳の元の取引データを対象とする取引テストの実施を検討します。
- 例えば、売上を月次合計仕訳で計上するような会社においては、会計システムから仕訳データを入手して、仕訳テストを実施するだけでは十分ではない場合があり、業務システム（販売管理システム等）から、合計仕訳の元となった取引データを網羅的に入手して、仕訳テストの観点を継承して取引テストを実施することが考えられます。
- 非経常的な取引や通例でない取引の仕訳又は修正仕訳といった非定型的な仕訳を含む、仕訳入力に関する内部統制の識別及び評価した上で、経営者による内部統制を無効化するリスクとリスクシナリオ（仮説）を設定することになります。当該リスク及びシナリオ（仮説）と仕訳データの抽出基準の関連性が検討されていることに留意します。
- 仕訳テスト及び取引テストのリスクシナリオ（仮説）に基づき抽出した結果について、ヒアリングだけでなく証憑突合等の詳細テスト手続が十分に実施されていることに留意します。また、仕訳テスト及び取引テストのリスクシナリオ（仮説）に基づき抽出した結果について、通常はサンプリングによる詳細テストが適しないことに留意します。

２．仕訳テストにおけるＣＡＡＴの利用：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を抽出し、それらの抽出した項目についてより深度のある手続を実施したり、大量のデータを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) 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、多く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) 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、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、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言えます。

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。

Q34　リスク対応手続（運用評価手続・実証手続）におけるＣＡＡＴの利用法について教えてください。

（関連する報告書：監基報 330 第９項、A26 項、監査基準報告書 500「監査証拠」第５項、A19 項）

A34：

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。

例えば、権限と責任の付与のような統制環境の一部の要素又はコンピュータによって実施されるような統制活動の一部については、運用に関する証跡は文書で存在しないこともあり、このような場合、運用状況の有効性に関する監査証拠は、質問と観察又はＣＡＡＴを用いる等のその他の監査手続を組み合わせて実施することにより入手されることがあります。

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。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、双方を兼ねているケースもあります。

１．サンプリング

サンプル抽出については、監査基準報告書 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。

２．母集団の階層化

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。

３．特定項目抽出による試査

ＣＡＡＴの利用のメリットとして、大容量のデータを処理することで、異常値を検出することが挙げられます。すなわち、母集団全体のデータを確認し、異常な偏向を示すデータを特定することも可能となります。ただし、サンプル母集団が少数の場合はＣＡＡＴ以外の手続を行った方が効率的な場合もある点を考慮します。

４．具体的な活用例

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、監査基準報告書 500 の 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を利用することがあります。また、分析的手続や計算突合といった局面においてもＣＡＡＴは効果を発揮します。一方、ＣＡＡＴを用いるときに、監査人が利用を予定する情報が含まれていないデータであった場合や、抽出された日付の範囲が異なっている場合等には、有効な手続を行うことができないため、ＣＡＡＴで利用するデータが、監査人の手続の目的に合致していることを確かめることが必要となります。

(1) 運用評価手続での活用例

再実施におけるＣＡＡＴの利用法として、例えば、「売上は、販売管理システムから自動でインターフェースされ、会計システムに仕訳が計上される。」という内部統制がある場合に、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運用評価手続を実施することができます。すなわち、販売管理システムから取得した特定の期間の販売データをＣＡＡＴで集計した結果と会計システム上の計上額を突合することにより、内部統制の運用の有効性を確かめることが可能となります。

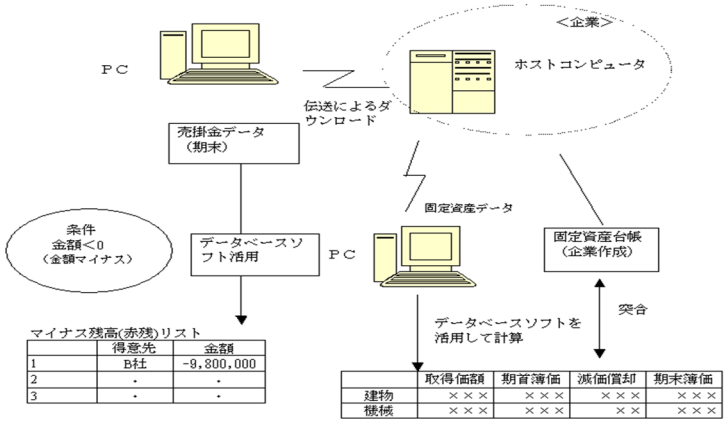
(2) 実証手続での活用例

・　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し、抽出された売掛金残高について貸倒引当金が適切に計上されているか評価する（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。)。



そのほか、監査基準報告書 240 付録２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。

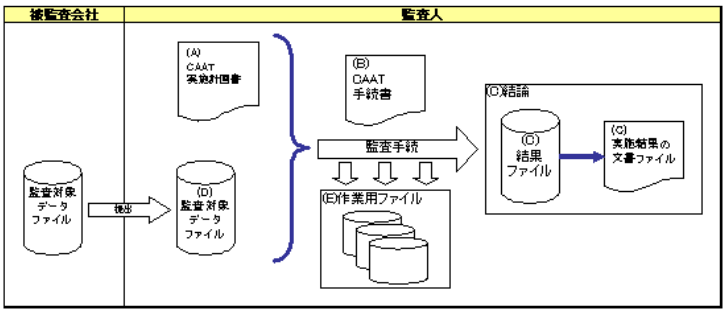
Q35　ＣＡＡＴを利用した監査手続を実施する場合、どのような監査調書を作成すればよいか例示してください。

（関連する報告書：監査基準報告書 230「監査調書」第７項）

A35：

ＣＡＡＴを利用した監査手続を実施する場合には、当該監査手続の目的、検証する内容を明らかにし、それに応じたＣＡＡＴの機能を選択することになります。また、検証に際して企業が入手、利用、生成す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、プロセス単位又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」の控えを含む。）
(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」の控えを含む。）
(9) 実施する監査手続の内容

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について、ＣＡＡＴ実施計画書の随時更新を行うことが重要です。

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。

例えば、ＣＡＡＴにより内部統制として規程に定められた承認の検証を行うのであれば、データの中から未承認の案件を抽出するような手続が行われますし、会社の作成している滞留在庫一覧表の金額を検証するのであれば、在庫情報から再計算した結果を作成し、会社の作成情報との比較のための資料を作成することが考えられます。

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。この際に、会社から入手したデータは適切なプロセスを経て作成されたものであり、過不足なく入手されていること、すなわち情報のインテグリティに留意します。そのため、依頼するデータが社内で作成・加工されている場合にはそれに係るシステムの内部統制についても検証します。

５．作業用ファイル

会社から入手したデータに上記２．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りません(監基報 230 第７項)。この観点から考えると、上記１．から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、後になって改竄されるリスク、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、監査人による保存を検討する場合もあります。

※　ＣＡＡＴツールには、ＣＡＡＴ専用ソフトウエアと汎用的なデータ処理ソフトウエア、表計算ソフトウエアがあります。ＣＡＡＴに使用するソフトウエアによって、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。

《Ⅷ　不備対応》

Q36　ＩＴ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。

（関連する報告書：監基報 315 第 25 項から第 26 項、A154 項、A170 項、A171 項、監基報 330 の A41 項から A57 項）

A36：

監査基準報告書 315 には、内部統制システムにおける内部統制の不備について「監査人は、企業の内部統制システムの各構成要素の評価を実施する際に、ある構成要素における企業の特定の方針が企業の性質及び状況にとって適切ではないと判断することがある。このような判断は、監査人が内部統制の不備を識別するのに役立つ兆候となり得る。監査人は、内部統制の不備を識別した場合、その不備が監査基準報告書 330 に従ったリスク対応手続の立案に与える影響を検討する（監基報 315 の A170 項参照)。」とあります。

ＩＴ全般統制は、「ＩＴ環境の継続的かつ適切な運用を支援する企業のＩＴプロセスに係る内部統制」（監基報 315 第 12 項(4)参照）をいうものです。ここにいうＩＴ環境の継続的かつ適切な運用には、「継続して有効に機能する情報処理統制及び企業の情報システム内の情報のインテグリティ（すなわち、情報（データ）の網羅性、正確性、正当性）の確保が含まれ」）」（監基報 315 第 12 項（4））、たとえ情報処理統制及び企業の情報システム内の情報のインテグリティ（以下、情報処理統制等、という）がある一時点で有効に機能していたとしても、ＩＴ全般統制に不備があれば、当該情報処理統制等が継続的に有効に機能していることの心証は得られず情報システムの内部統制に依拠できない可能性があります。

ただし、ＩＴ全般統制の不備の存在が、直ち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つながるものではなく、当該不備が情報処理統制等の有効性に影響を与えているか否かを検討することが必要です。具体的には以下のような対応を取ることになります。また、リスク評価時点でのＩＴ全般統制の不備が生じた場合、以下の対応（内部統制システムにおける内部統制の不備」（監基報 315 第 26 項、A170 項及び A171 項参照））をとることになります。

１．不備の発見されたＩＴ全般統制を代替又は補完する他のＩＴ全般統制を識別し、評価する。

監査基準報告書 315 の A171 項には「監査人が内部統制の不備を識別した場合、監査基準報告書 265 は、内部統制の不備が、単独で又は複数組み合わさって重要な不備となるかどうかの判断を要求している。不備が内部統制の重要な不備となるかどうかの判断は、職業的専門家としての判断事項である。」とあります。

不備が発見されたＩＴ全般統制が軽減するとしていたＩＴの利用から生じるリスクを軽減する、他のＩＴ全般統制がないか検討し、識別された場合はその有効性を評価します。例えば、防止的なＩＴ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ＩＴ全般統制が有効に機能しているときは、当該リスクが低減されていると判断できることがあります。

２．発見された不備によりＩＴの利用から生じるリスクが発現していないことを確かめる。

ＩＴ全般統制の不備によるＩＴの利用から生じるリスクが発現していないことを監査人が確かめることで、情報システムの内部統制に依拠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。

３．関連する情報処理統制等の評価手続の実施範囲を拡大する。

ＩＴ全般統制の不備の影響を受ける情報処理統制等の範囲を特定し、情報処理統制等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。

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。

これらのＩＴ全般統制の不備の影響を受ける情報処理統制等への対応については、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。

４．実証手続を拡大する。

上述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、注記事項等に対する詳細テストと分析的実証手続）（監基報 330 の A41 項から A57 項参照）を拡大して実施します。

なお、上述の手続を実施する過程で、個別のＩＴ全般統制の不備は重要な不備ではないと評価された場合であっても、それらの不備を組み合わせて評価すると、異なる評価になる場合があることに留意します。

Q37　システムに組み込まれた情報処理統制等の整備状況が、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。

（関連する報告書：監基報 315 第 36 項、A221 項）

A37：

監査人は、仕様書等を査閲することにより、自動化された情報処理統制の整備状況を評価しますが、仕様書等が存在しない、又は最新の状況に更新されていない場合には、次のような対応をとることが考えられます。

１．仕様書等以外の書類等による検討

ユーザマニュアル等のユーザ向け操作手順書により情報処理統制等を読み取ることができる場合があります。この場合のユーザマニュアル等は、ユーザ部門で作成されたものよりも、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と言えます。

また、情報処理統制等に関係するコンピュータ・プログラムのソースコードを閲覧し、その内容を確かめる場合もあります。ソース上に記述されているコメント（保守等の利便性のためにソース上に記述された注釈）が十分でなく機能を読み解けない場合は、他の手続と組み合わせて実施することになります。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ります。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多いと考えられます。

２．上記の対応が取れない場合

１．の対応が取れない場合でも、運用状況の評価手続を実施することで、整備状況の評価を同時に実施できることがあります。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や処理パターンしか確かめられないこと、及び想定していない処理結果が確認された場合に、それが適切な処理か否かを判断することを考慮します。

(1) 業務の実際の操作や制御画面を観察し、組み込まれている情報処理統制等を理解する。

(2) アクセス権限の種類やパラメータ設定等の実際のシステムの設定情報を確かめる。

(3) 原始証憑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、組み込まれている情報処理統制等を確かめる。

なお、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。したがって、仕様書等が確認できない状況は、システム開発、保守のプロセスにおける不備の存在を示唆することに留意します。

Q38　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。

（関連する報告書：監基報 315 付録５から付録６）

A38：

１．ユーザ受入れテストの意義及び関連するリスク

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、関連する情報処理統制等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又はテストの実施記録が残されていない場合、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。また、実施したテストの適切性・充足性を担保するため、その実施項目・結果を記録として残します。

３．ＩＴ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かったり、記録が残されていない場合には、１．で挙げたリスクが想定されます。このような場合には、次のような監査上の対応が考えられます。

(1) システム部門のテスト結果の確認

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) 本番移行後の修正記録の確認

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、情報処理統制等が機能しているかを確かめ、要求する情報処理統制等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。

Q39　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。

（関連する報告書：監基報 315 第 25 項、A154 項から A161 項、付録５から付録６）

A39：

データへの直接アクセスの一例としての「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ＩＴ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へ直接アクセスし、又は情報を直接操作するツールを用いて、データを変更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ＩＴ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、それ自体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、運用します。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が一般的には求められます。また、修正後の会計データに対する承認の手続も一般的には求められます。

(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、ユーザ部門の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．ＩＴ全般統制に不備が存在した場合の対応例

(1) データベースの直接修正に関する承認手続に不備が発見された場合

データベースの直接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、承認なく直接修正されたデータベース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、データベース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全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付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を実施することで、ＩＴ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することになります。

(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、補完統制となる情報処理統制又は実証手続による対応を検討します。

Q40　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。

（関連する報告書：監基報 315 第 25 項、A154 項から A160 項、付録３第 20 項、付録４第 18 項、付録５から付録６）

A40：

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。

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重要です。

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。

例えば、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エ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。

また、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。

このような管理体制では、相互牽制がなく、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竄につながるリスク、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

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、十分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。

仮に、システムの担当者が１名である場合であっても、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．ＩＴ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ＩＴ全般統制を補完する他のＩＴ全般統制によりＩＴの利用から生じるリスクが低減されていると判断できる場合があります。

システム部門において、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、ＩＴの利用から生じる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、更にＩＴの利用から生じるリスクが低減されていると判断できる場合があります。

また、システム部門が存在せず、担当者１名がシステム管理を行っているような場合であっても、システム管理に係る作業記録が残されている場合には、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ＩＴ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、関連する情報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。

Q41　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。

（関連する報告書：監基報 315 第 25 項、A154 項から A160 項、付録５から付録６）

A41：

１．システムの特権ＩＤの意義とその管理に関連するリスク

ＩＴの利用から生じるリスクとして未承認で行われる特権レベルのアクセスがありますが、その一例としてのシステムの特権ＩＤとは、全てのマスター情報、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、必要な内部統制を無効化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
・　上級管理職になりすまし、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．ＩＴ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) 代替的又は補完的な統制によりリスクが低減される程度の評価

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。ただし、この場合「他の帳票」の正確性についても検討することになります。

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の直接的な検証

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顕在化していないことを確かめることができる場合があります。

Q42　監査基準報告書 315 付録５「ＩＴを理解するための考慮事項」の「適用の柔軟性」における、ＩＴの利用から生じるリスクの影響を受ける可能性が十分に低い場合の柔軟な適用について教えてください。

（関連する報告書：監基報 315 第 18 項(1)、第 25 項(2)から(3)、A133 項、A144 項から A145 項、付録５）

A42：

１．監査基準報告書 315 付録５「適用の柔軟性」とは

監査基準報告書315付録５「ＩＴを理解するための考慮事項」には、ＩＴの利用から生じるリスクの影響が高くない場合を以下(1)から(2)のとおり例示して、高くない会社には柔軟な適用することがあると記述されています。監査人は当該例示を参照して、リスクへの影響の度合いが高くないことを判定して、柔軟な適用をするかを判断することになります。

(1) 監査基準報告書315付録５第６項「市販のソフトウエアを使用している複雑でない企業で、プログラムの変更を行うためのソースコードにアクセスができない場合は、企業のＩＴ環境の理解はより容易となる。このような企業は、ＩＴの専任者を有さず、従業員へのアクセス権

の付与又はＩＴアプリケーションに対してベンダーが提供するアップデートのインストールを管理する役割を特定の担当者に割り当てる場合がある。」

さらに、「監査人が市販の会計パッケージ・ソフトウェア（複雑でない企業が情報システムにおいて利用する唯一のＩＴアプリケーションである場合もある。）の性質を理解する際に考慮することがある具体的な事項」が、例示列挙されています。

これらの「ＩＴの利用から生じるリスクの影響が高くない」場合に該当するかは、以下のソフトウエアの特性（程度）を概括的に理解することによって判断することができます。すなわち、監査人は、柔軟な適用をするかを判断するために、ＩＴ環境を概括的に理解します（監基報 315 付録５第６項参照）。

- ソフトウエアの安定性及び信頼性についての評判
- ソフトウエアに実施した修正の内容と程度（カスタマイズの有無・程度）
- データに直接変更を加えることができる程度
- 企業がソフトウエアの設定値をどの程度変更できるか（パッケージ・ソフトウェアにおけるパラメータ等の環境設定の変更ができる程度）。
- 財務諸表の作成に関連するデータに直接アクセスできる程度（すなわち、ＩＴアプリケーションを介さずにデータベースに直接アクセスできる程度）

(2) 第 15 項「状況によっては、取引の量が少なく、複雑性が低い場合、経営者がデータの正確性と網羅性を検証するのに十分な情報処理統制を有している可能性がある（例えば、処理及び請求された個々の受注が、当初ＩＴアプリケーションに入力された紙資料と照合される。）。」また「ＩＴの利用から生じるリスクの影響を受ける可能性が高くないＩＴアプリケーションの特徴例（下記の３(1)②を参照）」

(3) 監査人は、監査基準報告書 315 付録５第６項及び第 15 項の高くない場合の例示を参照して、企業ごとのＩＴ環境を概括的に理解した上で、個別事情に応じて「ＩＴの利用から生じるリスクの影響を受ける可能性」の度合い（高くないか、高いか。）を判定し、調書化します。すなわち、監査人は、当該概括的な理解により入手した情報を総合的に判断し、「ＩＴの利用から生じるリスクの影響を受ける可能性」の度合い（低いか、高いか。）を判定し、その度合いに応じて適用の柔軟性を高めたり下げたりします。例えば、概括的に理解した結果、全ての例示の程度が「高くない。」に該当するＩＴ環境の会社に対して「ＩＴの利用から生じるリスクの影響を受ける可能性」が十分に低いと判定した場合、より柔軟性を高めことができます。

２．ＩＴ利用から生じるリスクの影響を受ける可能性が十分に低い場合の柔軟な適用

ＩＴ環境の理解を行うに当たっては、ＩＴの利用状況が企業によってかなり異なることから、まず、「ＩＴ利用から生じるリスクの影響を受ける可能性が十分に低い場合」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、更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あります。

ただし、リスク評価手続を実施した結果によっては、十分に低いとした判定を見直し、ＩＴに関する詳細な理解を実施することがあります。

なお、グループ監査の監査人は、「ＩＴの利用から生じるリスクの影響を受ける可能性」の度合いを判定するための概括的な理解は、監査対象となった構成単位に対して行うことが重要です。グループ監査の監査人は、「ＩＴの利用から生じるリスクの影響を受ける可能性が十分に低い」と判定された会社に対して、同上の柔軟性の高い適用をすることがあります。

３．ＩＴの利用から生じるリスクの影響を受ける可能性の度合いの判定

(1) ＩＴの利用から生じるリスクの影響を受ける可能性の度合いを判定は、以下の監査基準報告書 315 の例示を参照して、監査人が総合的に判断し、その度合いを決定します。

① 監査基準報告書 315 付録５第６項及び第 15 項のＩＴの利用から生じるリスクの影響が高くない場合の例示

・ 市販のソフトウエアを使用している複雑でない企業
・ プログラムの変更を行うためのソースコードにアクセスができない場合
・ ＩＴの専任者を有さず、従業員へのアクセス権の付与又はＩＴアプリケーションに対してベンダーが提供するアップデートのインストールを管理する役割を特定の担当者に割り当てる場合
・ 取引の量が少なく、複雑性が低い場合
・ 経営者がデータの正確性と網羅性を検証するのに十分な情報処理統制を有している可能性がある（例えば、処理及び請求された個々の受注が、当初ＩＴアプリケーションに入力された紙資料と照合される。）。

② 監査基準報告書 315 付録５第 15 項のＩＴの利用から生じるリスクの影響を受ける可能性が高くないＩＴアプリケーションの特徴例

・ 外部と接続のないスタンドアローンのアプリケーション、データ（取引）の量が大きくない。
・ アプリケーションの機能が複雑ではない。
・ 各取引は紙媒体の原始文書によって裏付けられる。
・ ＩＴアプリケーションは、以下の理由により、ＩＴの利用から生じるリスクの影響を受ける可能性が高くない。

ア．データの量が大きくないため、経営者はデータを処理又は維持するためのＩＴ全般統制に依拠していない。

イ．経営者は、自動化された内部統制や他の自動化された機能に依拠していない。監査人は、アサーション・レベルの重要な虚偽表示リスクに対応する内部統制の識別において、自動化された内部統制を識別していない。

ウ．経営者は、システムにより生成されたレポートを使用するが、当該レポートから原始文書に遡及して照合し、レポートの計算を検証している。

③ 監査基準報告書 315 第 18 項(1) 企業及び企業環境に関する事項に含まれる「ビジネスモデルがＩＴをどの程度活用しているか」

④ 会社のソフトウエア・ＩＴアプリケーションが、以下の区分で「高くない」「複雑でない市販」に該当することを明確にする。

・　監査基準報告書 315 付録５第 15 項の表の「高くない／高い」の区分
・　監査基準報告書 315 付録５第４項の表の「複雑でない市販／中規模中程度に複雑な市販／大規模又は複雑（ＥＲＰシステム等)」の区分

(2) 具体的な判定方法と判定表のサンプル

ＩＴの利用から生じるリスクの影響を受ける可能性の度合い判定の仕方について、一つのサンプルを記載します。

判定方法のサンプルとして、判定項目を質的要素と量的要素に分けて（質的）高／中／低及び（量的）大／中／小の判定した上で、監査人がＩＴの利用から生じるリスクの影響を受ける可能性を総合的に判断する方法が考えられます。例えば、質的「低」かつ量的「小」の場合を「ＩＴ利用から生じるリスクの影響を受ける可能性が十分に低い場合」として判定するのも一つの方法です。

判定項目		判定区分
質的 要素 高 ／ 中 ／ 低	(1) 会社の事業におけるＩＴの利用度（は以下の要素を総合的に判断） ① ビジネスモデルがＩＴをどの程度活用しているか（監基報 315 第 18 項(1)）。 ・ 会社が属する業種（金融機関か否かを含む。） ・ 電子商取引の有無、売上等の計上の自動処理の程度 ② 利用するシステム構成、処理の複雑性 ・ ソフトウエアの特性と監査基準報告書 315 付録５第６項の列挙項目の程度 ・ ＩＴアプリケーションの特徴例と監査基準報告書 315 付録５第 15 項の表：高くない／高いの判別 ・ 監査基準報告書 315 付録５第４項表の「複雑でない市販／中規模中程度に複雑な市販／大規模又は複雑（ERP システム等）のソフトウエア・ＩＴアプリケーションの区分の判別 ③ 内部統制におけるＩＴ活用程度、（監査利用する）重要な企業作成情報のＩＴ活用程度 ・ 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（例えば、内部統制が ERP に依拠している場合は「高」）。 ④ その他のシステム使用状況 (2) ＩＴの安定度、過去１年以内に重要な障害発生の有無 (3) 情報システムの重要な変更、過去１年以内に重要なシステム変更の有無 (4) 過年度の監査におけるＩＴに関連する内部統制上の不備の有無	
量的 要素 大	(1) 企業規模（例えば販売高、取引件数、従業員数等で総合的に判断） ① 取引量が少なく、会社及びグループの規模が小さい。 ・ 年間売上規模（数千億／数百億／数十億)、従業員数（＊＊＊名程度規模）	

／ 中 ／ 小	・　関係会社数（重要な構成単位数） ②　情報システム要員等のリソース規模が小さい。 ・　専門部署、専任者、重要な外部委託先の有無 ・　情報システム維持コスト (2) ＩＴ基盤、評価対象システム、自動化されている程度が高い内部統制等の数 ・　ＩＴ基盤数 ・　評価対象システム数 ・　自動化されている程度が高い情報処理統制（企業作成情報含む。）の数	
総合判定	（記載例）質的要素の全ての項目が「高くない」に該当するため「低」、かつ、量的要素からもＩＴの利用から生じるリスクの影響を受ける可能性を高める事象はなく「小」であるため、ＩＴの利用から生じるリスクの影響を受ける可能性は十分に低いと判断した。 判定の根拠とした、ＩＴ環境の概括的に理解した参照調書 ref：　＊＊＊＊ （ソフトウエアの特性（監基報 315 付録５第６項参照）、ＩＴアプリケーションの特徴例（監基報 315 付録５第 15 項）、ビジネスモデルに含まれるビジネスモデルがＩＴをどの程度活用しているか（監基報 315 第 18 項参照）等を概括的に理解した情報を記載して、判定の根拠とする。）。	（記載例）ＩＴの利用から生じるリスクの影響を受ける可能性は十分に低い

～判定時の留意事項～

質的要素(1)ＩＴの利用度の判定：

一般的には以下のような状況はＩＴの利用が低いと判断される場合がある。

ア　金融機関・社会インフラを担う事業会社等、一般に高いと想定される業種に該当しない。

イ　複雑なシステム処理がない。

ウ　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。

- 内部統制が ERP に依拠していない。
- 機能の限定された市販パッケージソフトのみを利用している。導入に当たってカスタマイズ（改造）を行っていない。
- アプリケーション間のインターフェースが限定的で、かつ、アプリケーションの構成が複雑でない。

エ　その他、システムの使用状況が僅少

- 会計帳簿や取引証憑が電子的に保存されていない。
- 電子商取引を利用した会計取引がない（重要でない。）。
- 自動受発注のような財務報告に関連する処理に自動処理がない（重要でない。）。
- 主要システムに電子承認、ワークフローの機能がない（重要でない。）

以　上

・　本実務ガイダンス（2022 年 10 月 13 日改正）は、次の公表物の公表に伴う修正を反映している。

ー　監査基準報告書（序）「監査基準報告書及び関連する公表物の体系及び用語」（2022 年 7 月 21 日改正）