ＩＴ委員会研究報告第 46 号

重要な虚偽表示リスクと全般統制の評価

平成 26 年 9 月 30 日
日本公認会計士協会

目　次

Ⅰ　本研究報告の目的

本研究報告は、全般統制の具体例と全般統制が機能しなかったことがＩＴに起因する重要な虚偽表示の要因となった事例を併せて示し、全般統制と重要な虚偽表示リスクの関連を明らかにするとともに、全般統制を評価する際の留意事項についてまとめている。

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「監基報 315」という。）及び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。）を中心にＩＴが内部統制にもたらす利点やリスク、統制活動としての全般統制についての記載はあるが、実務的な対応について詳細には触れられてはいない。そのため、本研究報告では、全般統制が対応するＩＴに起因するリスクの具体的な事例を取りまとめている。

ＩＴの形態とその利用は企業ごとに異なり、また、日々急速に変化している。監査人がこのような状況を踏まえたリスク評価手続及びリスク対応手続を実施するため、本研究報告においては、監査基準委員会報告書で定義されている全般統制に関する事項の整理ではなく、実務的な分かりやすさを考慮してまとめている。

Ⅱ　全般統制

１．意義

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。全般統制には、通常、次の事項に対する内部統制が含まれる。（監基報 315 A92 項及びＩＴ実６号第 34 項参照）

- データ・センターとネットワークの運用
- 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

これらの事項についての具体的な例は、ＩＴ実６号第 35 項から第 39 項までに示されている。

実務的には、企業が採用しているＩＴの管理のフレームワークに合わせて全般統制の評価を行うことがある。本研究報告では、例として次のように分類している。

- 開発・変更に係る全般統制
- システムの運用に係る全般統制
- 情報セキュリティに係る全般統制
- 外部委託業務に係る全般統制

２．全般統制の適用範囲・評価単位

全般統制はシステムの開発、運用等に関わる統制活動であるため、大型汎用機やクライアント・サーバからＥＵＣやスプレッドシート等に至るまで、利用する全てのタイプの情報システムにおいて存在している。

監査人が監査計画を策定するに当たっては、ＩＴの利用に関する概括的理解を行う（ＩＴ実６号第４項及び第５項参照）。企業の利用するＩＴの全てが重要な虚偽表示リスクにつながるものとはならないため、内部統制の評価の対象となる業務処理統制について、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て全般統制の評価範囲を決定する。

グループ監査においては、グループ全体、重要な構成単位及びこれらのＩＴに関する環境と、連結プロセス（連結のためにＩＴがどのように利用されているか）を理解することが求められている（ＩＴ実６号第８項参照）。

ＩＴに関連する業務が外部委託されていたり、クラウドコンピューティングの利用といったように、必ずしも企業の内部で完結しない場合があるため、実態を踏まえて全般統制を評価する必要があることに留意する。

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又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。

３．全般統制が対応するリスク

全般統制は企業のＩＴに関わる業務が適切に実施されることを担保するための内部統制である。ＩＴに関わる業務が適切に実施されない場合には、業務処理統制が適切に組み込まれない、適切に機能しない、又は無効化されるといった事態をもたらし、結果として、財務報告に係る取引が適切に処理されない可能性につながる。全般統制が対応するリスクの評価においては、ＩＴ特有のリスクとして、例えば次のような業務処理統制の有効性を脅かすリスクについて考慮する。

- 開発･変更管理に係る内部統制が十分に整備、運用されず、経営者の意図した業務処理統制が適切に組み込まれない。
- 運用管理に係る内部統制が十分に整備、運用されず、経営者の意図した業務処理統制が適切に機能しない。
- 情報セキュリティ管理に係る内部統制が十分に整備、運用されず、業務処理統制が無視されたり、バイパスされるような方法で、内部統制が無効化される。
- 外部委託業務管理に係る内部統制が十分に整備、運用されず、求めるサービスレベルが達成されずに、経営者の意図した業務処理統制が適切に機能しない。

４．開発･変更に係る全般統制

(1) 開発･変更に係る全般統制

システムの開発・変更では、システム開発・変更担当とシステム運用担当の分離、プログラムの十分なテストの実施、開発・変更手続に基づく各段階での承認等が内部統制として識別・評価される。

パッケージ・ソフトウェアを導入する場合であっても、同様の内部統制が導入されることが考えられる。

(2) 具体的例示

システムの開発・変更管理の目的は、業務処理統制が適切に組み込まれるようにすることにある。システムの開発・変更管理に係る全般統制の具体例を示せば次のようになる。

① システム開発・変更と運用が組織的に分離している。又は、必要な職務の分離が行われている。

② システムの開発計画（購入計画を含む。）が作成され、適切な者により承認される。

③ システム変更について適切な者により承認される。

④ システムの開発・変更時の成果物は、適切な者により承認される。

⑤ システムの開発・変更時のテストは、適切な者により承認される。

⑥ 本番環境に影響を与えないようにするために、テスト環境は本番環境から分離されている。

⑦ 本番環境へのリリースについて、適切な者により承認される。

⑧ データ移行の移行計画及び移行結果について、適切な者により承認される。

⑨ ＯＳ、ＤＢＭＳ、ハードウェア等の追加・更新（システム設定変更及びバージョンアップを含む。）を行う場合に、追加・更新内容について、適切な者により承認される。

(3) 全般統制が機能しなかった事例

① 要件定義

新会計基準の適用に対応するためのシステム変更に関する設計書を確認した結果、新会計基準に準拠しない要件が定義されていた。原因について調査したところ、経理担当者が、新会計基準の適用に対応するためのシステムの要件定義の確認を行っていなかったことが原因であることが判明した。

② テスト環境と本番環境の分離

実証手続の中で残高が一致しないデータが発見された。その原因を調査したところ、本番環境で直接テストデータを作成してテストを実施していたが、そのテストデータを削除する際に誤って本番データの一部を削除していたことが判明した。これはテスト環境が本番環境から分離されていないことと、プログラム変更における手続の事前確認及び結果確認が不十分であったことに起

因している。

③　ユーザ受入テスト

連結パッケージソフトを導入したが、期末決算の連結作業時に不完全な連結精算表が自動作成される事象が発生した。原因を調査したところ、ユーザ受入テストが不十分で、導入した子会社から決算データがインターフェースできないことを認識していなかったことが原因であると判明した。

④　データ移行

グループ共通システムの導入に伴い、勘定科目体系を合わせるべく総勘定元帳のデータを移行したが、移行前後で残高の不一致が発生した。原因は各社で統一後の勘定科目へのひも付けが正確に行われていないことを発見できなかったためである。これは移行計画及び結果確認が不十分であったことに起因している。

(4) 用語の解説

・　システム開発とシステム変更

システム開発とは、新規のシステムの作成・導入、既存のシステムに新機能を追加することなどをいう。

システム変更とは、既存のシステムに対して機能変更、不具合の修正を行うことなどをいう。

なお、企業の方針により、一定の金額、工数（規模）により開発と変更とを分けることもある。

・　適切な者

開発・変更の規模や組織形態により異なることがあるが、４(2) 具体的例示における適切な者とは例えば次のようになると考えられる。

統制の具体的例示	４(2)における該当箇所	経営者	システム部門	ユーザ部門
開発計画の承認	②	○	○	○
システム変更の承認	③		○	○
成果物の承認	④		○	○
テストの承認	⑤		○	○
本番環境へのリリースの承認	⑦	△	○	○
データ移行の承認	⑧		○	○
ＯＳ、ＤＢＭＳ、ハードウェア等の追加・更新の承認	⑨		○	

※　○は承認を行う者、△は開発・変更の規模等により承認を行う者を意味する。

・　ユーザ受入テスト

ユーザ受入テストとは、実際にシステムを利用するユーザが参加して業務に必要な機能が正常に作動するかについてのテストを行うことであり、機能単位のリリースとシステム全体のリリースの際に実施されることがある。

・　リリース

リリースとは、テスト等が完了したプログラムやシステムを実際の業務処理で使用開始できるようにすることをいう。

・　成果物

成果物とは、システムの開発・変更の各段階で作成される文書であり、例えば次のようなものがある。

ア．要件定義書：実装すべき機能や満たすべき性能などを明確にした文書

イ．基本設計書：構成や仕様、機能などの概要をまとめた文書

ウ．詳細設計書：基本設計で定義された要素の仕様や作動の詳細を定義した文書

エ．テスト計画書：プログラムが設計どおりに作成され、実際の業務に即した利用の仕方を試し、問題なく作動するかのテストを計画した文書

オ．テスト報告書：テスト結果を報告した文書

カ．移行計画書：プログラムやデータの移行・変換作業を計画した文書

キ．移行報告書：プログラムやデータの移行・変換作業の結果を報告した文書

なお、変更の場合は、上記が簡易的にまとめて作成されることがある。

・　インターフェース

インターフェースとは、あるシステムからデータを受け渡して、別のシステムへそのデータを反映させることをいう。データの受渡し方法はシステムによって異なるが、送り側のシステムのデータを受け側のシステムで処理できる形式に変換し、受け側のシステムのデータとして更新・取り込みを行う。例えば、販売管理システムの月次売上金額を月次の売上計上の仕訳データに変換して、会計システムへ仕訳として反映させることをいう。

５．システムの運用に係る全般統制

(1) システムの運用に係る全般統制

システムの運用に係る全般統制では、例えば、ジョブスケジュールの管理、臨時処理、情報システムの稼働確認、バックアップデータの保管、障害が発生した場合の復旧等に係る内部統制が識別・評価される。

(2) 具体的例示

システムの運用管理の目的は、システムの運用管理を適切に行うことにより業務処理が滞ることのないようにすることにある。システムの運用管理に係る全般

統制の具体例を示せば次のようになる。

① ジョブスケジュールの登録・変更は、適切な者に承認される。

② システム運用について稼働監視される。

③ 運用上の障害は適時に把握・記録され、遅滞なく問題解決される。障害発生状況は定期的にモニタリングされ、分析されるとともに、問題解決のため適切な者に報告される。

④ 臨時処理（スケジュールに基づかないジョブ）の実行について、手順が整備されており、適切な対応がとられる。

⑤ 必要なバックアップが取得され保管される。また、バックアップからのデータ復元が可能となっている。

(3) 全般統制が機能しなかった事例

① ジョブスケジュール

ある企業では、倉庫担当者が棚卸資産管理システムに出荷入力をする。日次のバッチで棚卸資産管理システムのマスタが出荷済に更新され、その後、売上管理システムにデータをインターフェースして売上を計上している。システム部門担当者のジョブスケジュールの登録作業ミスにより、倉庫部門で出荷業務が行われていたにもかかわらず、ジョブが起動しなかった。結果として、出荷済に変更するマスタ更新が行われず、翌日に未出荷として取り扱われて二重の出荷業務を行ってしまった。

② 障害への対応

ある企業の月次締め作業の中で、経理担当者が会計システム上の売上勘定残高と売上管理システム上の金額に不整合があることを発見した。この企業では、日次で売上管理システムから売上データを会計システムにインターフェースしている。調査の結果、ある日のジョブがシステム障害によりエラーで終了していたにもかかわらず、それを把握、対応していなかったことが判明した。過去に同様の障害が発生していたが、障害対応として金額の不整合を修正するのみで、原因分析と恒久的対策が講じられていなかったことも原因となっている。

③ バックアップ

ある企業では、会計システムのバックアップ作業を経理部員が担当していた。担当者は定期的にバックアップを行っていたが、システムに関する知識が十分ではなかった。ある日、データベースのメンテナンスを行った際に、誤ってデータを削除したため、バックアップを利用してデータを復元しようとしたところ、既にディスク容量がいっぱいになるまで書き込みされており、最新のバックアップが取得できず、データの復元ができない状況であったことが判明した。

(4) 用語の解説

・ バッチとは、処理の方式として一定量のデータを一連の処理としてまとめて実行する方式をいう。

・　ジョブとは、システム内における処理の単位をいう。
・　ジョブスケジュールとは、ジョブを自動的に実行するツール(スケジューラ)に登録される実行順序、時間、条件等のことをいう。
・　障害対応とは、システムのエラーにより処理が中断する等の障害が発生した場合に、問題を解決するための一連の対応をいう。処理を完了するために中断・停止されたジョブを復旧･継続させる暫定対応と、障害の原因を分析して再発防止を実施する恒久的な対策がある。

６．情報セキュリティに係る全般統制

(1) 情報セキュリティに係る全般統制

情報セキュリティでは、ユーザＩＤ管理やログ管理といった、プログラム、データ等の情報資源へのアクセスを制限するための論理的セキュリティのツールの導入・運用やアクセス権限付与に係る承認、入退出管理や情報機器への物理的なアクセス制限等が、内部統制として識別・評価される。

(2) 具体的例示

情報セキュリティ管理の目的は、プログラムとデータの情報セキュリティ管理を適切に行うことにより、業務処理統制が無視されたり、バイパスされるような方法で、内部統制が無効化されないようにすることにある。情報セキュリティ管理に係る全般統制の具体例を示せば次のようになる。

①　システムへのアクセスは、認証メカニズムにより、制限されている。
②　ユーザＩＤ作成が可能等の特別な権限のあるＩＤは、承認された特定の管理者のみに付与されている。
③　本番稼働しているプログラム、データ(マスタデータを含む。)、システムユーティリティへのアクセスが制限されている。
④　ユーザＩＤの申請は適切な者により承認される。
⑤　ユーザＩＤとアクセス権限に関して、人事異動・退職に伴う見直しを含め、定期的に確かめている。
⑥　ユーザ・アクセス及びセキュリティ上の問題とする監視対象が規定されており、その規定に従い監視が実施されている。また、問題事象は重要度に応じて適時に経営者等に報告される。
⑦　情報処理施設のある領域へのアクセスは、権限のある者に制限され、適切な認証を必要とされている。

(3) 全般統制が機能しなかった事例

①　過大な権限付与によるシステムの不正な操作

社内規程上は経理部の担当者にのみ付与されることとなっている仕入先マスタの登録権限が、仕入部の入力担当者に付与されていた。仕入部担当者は仕入先の担当者と結託して仕入先マスタに架空の支払口座を登録し、仕入代金を

横領した。これにより、本来の支払先への仕入債務が過少計上されることとなった。これらの不正は、社内規程上は、四半期に一度以上行うこととされているユーザＩＤの棚卸しが行われていなかったことにより、長期間発見することができなかった。

② セキュリティの監視が行われないことによる不正アクセスへの対応の遅れ

商品の出荷承認権限を有する退職者のユーザＩＤが適時に削除されずに有効なまま残っており、そのＩＤを使って売上高の架空計上が行われる事件が発生した。社内規程上、アクセス及びセキュリティ上の問題とする監視対象が規定されておらず、またパスワードの試行回数の制限も設定されていなかったため、不正アクセスを適時に発見することができなかった。

(4) 用語の解説

・ 認証メカニズムとは、システム等を利用しようとする者が、正当な権限を持った者であるかを確認する仕組みである。ユーザＩＤとパスワードによる本人確認やＵＳＢキーによる認証等を行うことにより、正当な権限を持つ者以外の利用を制限する。

・ ユーザＩＤの申請とは、システムで設定されるユーザＩＤの新規発行、アクセス権限の変更、使用の一時停止や削除の依頼を行うことである。

・ セキュリティの監視とは、故意又は不注意により正当な権限を持たない者によるシステムへのアクセス、意図しないデータ等の改竄･流出、システムのダウン等を意図した攻撃を受けていないかを監視することである。多くの場合は、システムやデータベースへのアクセスや更新等の記録（ログ）を取得し、それらの中から問題となる事象が発生していないかを抽出して監視する。監視対象となる事象として、違反又は違反試行、特権的ユーザのアクセス、セキュリティ違反、セキュリティ事故、不正アクセス等が想定される。

７．外部委託業務に係る全般統制

(1) 外部委託業務に係る全般統制

外部委託では、外部委託先の管理手続、業務要件の担保やモニタリングが内部統制として識別・評価される。

(2) 具体的例示

外部委託業務の管理の目的は、求めるサービスレベルが達成されずに、業務処理統制が適切に機能しないことのないようにすることにある。外部委託業務管理に係る全般統制の具体例を示せば次のようになる。

① 外部委託先の選定基準や外部委託先の管理手続が定められている。

② 委託業務の適切な実行を担保するための事項（セキュリティ要件、定期的な報告、委託先の監査権の行使等）が業務委託契約書に反映されている。

③ 外部委託先が契約を順守しているか否かについて、定期的にモニタリングす

る。

④　クラウドコンピューティングの利用に際しては、サービス品質やセキュリティ管理、サービス提供の継続性などクラウドコンピューティングに起因するリスクを評価する。

なお、システム開発業務を外部委託する場合や、自社内にハードウェアを設置し、システム運用業務を外部委託する場合は、内部で業務を実施する場合と全般統制が大きく異なることはないのが一般的であるが、外部のデータ・センターにハードウェアを設置し、システム運用業務を外部委託する場合は、業務内容合意書（サービス・レベル・アグリーメント）を締結し、外部委託先から定期的な報告を求めるケースが多い。また、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「監保実 86 号」という。）に基づく受託業務に係る内部統制の保証報告書を入手して評価を行うことが考えられる。

(3) 全般統制が機能しなかった事例

①　外部委託先の選定

会計システムの入替プロジェクトを経理部門主体で推進した結果、外部委託先の選定を適切に行うことができず、委託会社の要求水準を満たしていない委託先が選定されてしまった。委託先が実施したテスト結果の詳細の提出を委託会社が求めなかったこともあり、会計システムの入替えが完了し実際に利用する段階になってから、一部の機能に不具合があることが判明した。

②　業務委託契約

システム運用業務を外部委託するに当たり、外部委託先の業務の実施状況に関する報告義務などサービス水準に関する合意文書が交わされておらず、委託会社の外部委託先に対する監査権も業務委託契約書の中に織り込まれていなかった。結果として、外部委託先の運用担当者がシステム障害を発見した際に、適時かつ適切に委託会社に状況が報告されず、システム障害に起因する不適切な処理結果への対処が遅れてしまった。

また、委託会社が外部委託先での業務の品質水準に関する監査を実施することができず、委託業務の品質改善等に関して、委託会社による主導的な対応を行うことができなかった。

③　モニタリング

システム開発業務を外部委託するに当たり、外部委託先が使用するユーザＩＤは外部委託先側で管理を行い、ＩＤや権限は定期的に棚卸しするとともに、その結果を委託会社へ報告するよう業務委託契約書上取り決めていた。しかし、実際には外部委託先からの定期的な報告は行われず、委託会社からも報告を求めていなかった。外部委託先の開発担当者全員に、本番環境の更新権限が付与されていたことから、開発担当者が誤って本番環境でプログラム変更のテストを実施してしまい、既存のシステムやデータに不具合が生じてしまった。

④　リスク評価

ユーザ部門が、クラウドコンピューティングをＩＴに関わる業務の外部委託と認識しておらず、リスクの評価やシステム部門との協議を行うことなく、クラウドの仕様の理解が不十分なまま利用を開始してしまった。結果として、管理が不十分な環境に自社のデータを置くこととなり、データを消失してしまった。

(4) 用語の解説

・　受託業務に係る内部統制の保証報告書

業務を受託している企業が受託している業務に係る内部統制について監保実 86 号に基づき発行される保証報告書をいう。この保証報告書には、「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）とがある。外部委託しているＩＴに関わる業務とこれらに対する内部統制が、委託会社の財務報告に関連する情報システム（関連する業務プロセスを含む。）の重要な一部を構成している場合には、当該委託業務は財務諸表監査に関連することになるため、委託業務の種類と重要性、委託会社の内部統制に与える影響について理解するとともに、適切な監査手続を立案し、実施する。外部委託の手続として、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」（以下「ＩＴ研 42 号」という。）のQ32 からQ34 までが参考となる。

・　クラウドコンピューティング

サーバやストレージ、ソフトウェアなどのコンピュータ資源を、ネットワーク（特にインターネット）を介して利用することをいい、単にクラウドと略すことも多い。ネットワーク構成図などにおいてネットワークを雲（Cloud）の絵で表現することが多いため、このように呼ばれている。クラウドコンピューティングの形態は様々であるが、他者のコンピュータ資源の利用という点においては共通であり、外部委託の一種と理解することが適切であることが多い。一方、利用形態によりＩＴに起因するリスクは異なるため、リスク評価を行うに当たっては、クラウドコンピューティングがどのように利用されているかを理解することが重要である。例えば、ネットワークを介してアプリケーション・ソフトを利用させる、ＡＳＰ（アプリケーション・サービス・プロバイダー）と呼ばれるサービスはこれまでも存在しているが、最近ではこれらのサービスもクラウドコンピューティングと呼ぶことが増えている。

８．全般統制のリスク評価手続の留意事項

監査人は、リスク評価手続及びリスク対応手続の立案に当たって、監査対象期間における業務処理統制の継続的な運用の有効性を確かめるため、関連する全般統制の整備及び運用状況の有効性に関して、十分かつ適切な監査証拠を入手する評価手続を立案し、実施する。さらに、業務処理統制のリスク評価を勘案して、それを支えている全般統制の評価手続を実施する。

全般統制はそれ自体が統制活動の一種であり、手作業により実施されるものと、プログラムに組み込まれて自動化されているものがある。手作業により実施されるものについては、売上等の業務プロセスで実施されている手作業の内部統制と同様の評価手続となる。自動化されているものについては、自動化された業務処理統制と同じように、その有効性について評価を行うことを検討する。

全般統制に係る内部統制のデザインと業務への適用についての監査証拠を入手するための手続としては、他の統制活動と基本的には同じであるため、次の事項を含むことがある（監基報 315 A63 項参照）。

- 企業の担当者への質問
- 特定の内部統制の運用状況の観察
- 文書や報告書の閲覧
- ウォークスルー

「質問」は、全般統制に限らず、全ての対象に対して有効な手続であり、内部統制が意図したように運用されていることを担当者に確かめる手続となる。ただし、証明力が比較的弱い手続であり、「質問」のみでは、内部統制のデザインと業務への適用についてのリスク評価手続の目的には十分ではないことに留意する。

「観察」は、内部統制の実施状況について観察を行う手続であり、例えば、システムの運用、管理現場の視察を、システム運用、変更に関する統制についての評価手続として実施する。また、ＩＤとパスワードによるアクセス･コントロールや特定の事象に対するエラー表示など、プログラムに組み込まれて自動化されているものについて、想定されている状況において全般統制が機能していることを確かめる手続としても有効である。

全般統制はその多くが手作業により実施されているものであり、監査人は、担当者が統制活動を実施していることを示す文書や報告書を閲覧して、意図したように運用されていることを確かめる。例えば、変更依頼やテスト、移行に係る記録を閲覧し、適切なプログラム変更の手続に従って実施されていることを確かめる。担当者による記録の正確性や網羅性には一定の限界があり、それだけでは不十分な場合があることに留意する。例えば、作業ミスによりアクセス権限を管理する台帳と、システムに実際に設定されている状況とが不一致であるケースが考えられる。必要に応じて、システムから実際に設定されている情報を出力して適切に設定されているかを検討する。また、システム設定上の問題点を診断できるツールが用意されて

いることがあるので、ＩＴの技術的な検証が必要となる場合にはそれらの活用を検討する。

全般統制は、主にＩＴの管理に関連する業務を対象としており、財務報告に関連する取引を処理するものではないため、取引の開始から財務諸表に反映されるまでを追跡する取引のウォークスルーの概念にはなじまない。しかしながら、全般統制が対象とする業務のフローの開始から完了までを追跡することでウォークスルーを行うことがある。

９．全般統制の運用評価手続の留意事項

全般統制に係る内部統制の運用評価手続としては、他の統制活動と基本的には同じであり、内部統制の運用状況の有効性に関する監査証拠を入手するために、質問とその他の監査手続を組み合わせて実施する（監査基準委員会報告書 330「評価したリスクに対応する監査人の手続」（以下「監基報 330」という。）第９項参照）。例えば、次の事項を含む。

① 監査対象期間において内部統制がどのように運用されていたか。
② その運用は一貫していたか。
③ 誰が又はどのような方法で運用していたか。

全般統制に係る内部統制の運用評価手続の範囲を決定するに当たっては、内部統制への依拠の程度と次の事項を考慮することがある（監基報 330 A27 項参照）。

- 依拠する期間における内部統制の実施頻度
- 監査対象期間のうち監査人が有効に運用されている内部統制に依拠する期間
- 内部統制の予想逸脱率
- 内部統制の運用状況の有効性について入手された監査証拠の適合性及び証明力
- 関連した別の内部統制について実施した運用評価手続から入手した監査証拠の程度

サンプリングを利用する場合は手続の目的と母集団の特性を考慮して実施する。全般統制のうち、手作業により実施されるものについては、売上等の業務プロセスの内部統制と同様にサンプル件数を決定する。自動化されたものについては、ＩＴにより一貫して処理されることを考慮して運用評価手続を拡大する必要がない場合もある。

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する場合には、運用評価手続実施後の当該内部統制の重要な変更についての監査証拠の入手と、期末日までの残余期間に対してどのような追加的な監査証拠を入手すべきかを決定する（ＩＴ実６号第 50 項参照）。

全般統制は、業務処理統制が継続して有効に機能することを合理的に保証するための統制である。監査人は、運用評価手続の立案と実施に当たって、有効に運用さ

れている内部統制への依拠の程度が高いほど、より確かな心証が得られる監査証拠を入手しなければならないことを考慮して（監基報 330 第８項参照)、全般統制の運用状況に関して過年度の監査証拠を利用するかを慎重に判断し、当該内部統制に過年度監査終了後に発生した重要な変更の有無と、過年度から引き継ぐ監査証拠の適合性を確かめる（ＩＴ実６号第 52 項参照)。

10．全般統制に不備が存在する場合

全般統制はアサーション・レベルの重要な虚偽表示リスクに広範に関係していることから、全般統制に重要な不備があった場合には、監査人は重要な虚偽表示リスクの評価を変更する必要性について検討する。不備の対応の手続を立案するに際しては、ＩＴ研 42 号のQ23 からQ29 までを参考にすることができる。

以　　上