

リアルタイムなデータ連携が自動で行われる DX時代の内部統制とは



アシュアランスイノベーション本部 AIラボ 公認会計士 本山禎晃

▶ Sadaaki Motoyama

一般事業会社勤務を経て当法人に入社後は主に製造業、テクノロジー産業の会計監査に従事。2022年よりEYリアルタイムコネクト（継続的監査手法）の開発プロジェクトに従事し、現在はその導入推進に取り組んでいる。

I はじめに

EYでは監査法人と被監査会社のファイナンス部門が共創しながらデジタルトランスフォーメーション（DX）を進めることで、双方にとって新たな価値が生まれると考えています。これまでの連載で、監査のDXがどのように被監査会社への価値提供（リスクの適時把握やインサイト提供など）につながるかをお伝えしています。

本稿では、ITシステムにおける内部統制について確認するとともに、DXにより複数のITシステム間で高度にデータの自動連携が進んでいく過程における留意事項について考察します。

II ITの利用から生じるリスク

ITシステムはあらかじめ定められた規則に従い、大量の情報や複雑な計算を正確に処理できるという特徴があることから、多くの企業が業務プロセスの自動化や効率性を高めるために使用しています。しかし、ITシステムの正しい使い方や管理がなされていなければ、＜表1＞のようなリスクに起因して、業務プロセスの誤りや不正行為の発生などの問題が生じる可能性があります。そのため、企業はITシステムの内部統制を適切に整備・運用することが必要不可欠となります。

▶表1 ITの利用から生じるリスクの例^{*1}

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（未承認もしくは架空取引の記録また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越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アプリケーションまたはその他のIT環境に対する未承認の変更
5.	ITアプリケーションまたはその他の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.	データの消失または必要なデータへのアクセスができないこと

III 情報処理統制とIT全般統制

企業の内部統制には、情報処理統制とIT全般統制の2つが含まれます（＜表2＞＜表3＞参照）。

情報処理統制は、企業の情報システムにおける情報処理に関連した内部統制であり、情報の網羅性、正確性、正当性のリスクに直接対応します。情報処理統制は、自動化されている場合と手作業の場合およびその組み合わせの場合があります。

IT全般統制とは、企業のITプロセスに係る内部統制であり、IT環境の継続的で適切な運用を支援します。

^{*1} 日本公認会計士協会 監査・保証基準委員会 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）」

企業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ほどIT全般統制が重要となります。

▶表2 自動化された情報処理統制の例^{*1}

自動計算	定められた期日や処理のタイミングに応じて自動的に金額の計算や減価償却費の計上、外貨換算など
レポート出力	明細レポートや数値項目を集計した集計レポート、入力内容を表示するプルーフ・リスト、エラーリストなどを自動で出力
エディット・バリデーション・チェック	フォーマットチェックやリミットチェックなど、入力内容が予定通りの形式や内容であることをチェックする機能
マッチング	得意先コードが登録されていない場合にエラーとするなど、入力された内容をマスターデータと照合し、登録されているかどうかを確認する機能
コントロール・トータル・チェック	情報の処理過程での入力情報の合計を出力情報と照合する機能。入力データの合計額と出力データの合計額が一致しない場合にエラーリストを出力
アクセス・コントロール	ユーザーIDとパスワードによってプログラムやデータの利用を制限する機能

▶表3 IT全般統制の例^{*1}

アクセス権管理	IT環境へのアクセス権限の適切な管理や監視を行うプロセス。ユーザーの権限の付与や削除、アクセスログの監視などが含まれる
変更管理	IT環境におけるプログラムや他の要素の変更を管理するプロセス。変更の承認、テスト、導入などが適切に行われることで、システムの安定性と信頼性を確保する
IT業務管理	IT関連の業務やプロジェクトの管理を行うプロセス。予算管理、リスク管理、品質管理などが含まれ、ITプロジェクトの成功や目標の達成に寄与する

情報処理統制は情報の処理に焦点を当て、情報そのものの信頼性を直接確保するための内部統制であり、IT全般統制は、ITプロセス全体をサポートし、自動化された情報処理統制の適切な運用を確保するための内部統制と言えます。

IV DXによりもたらされる変化

DXの進展により、リアルタイムにデータが自動連携される社会への移行が進んでいます。<表4>はデータの自動連携の具体例です。このような社会では、複数のITアプリケーションが高度に連携されることにな

るため、情報の信頼性の確保の観点で新たに留意すべき事項が生じています。

▶表4 さまざまなデータ自動連携の例

1. 異なるITアプリケーション間のインターフェース	(例) 上流システムと下流システムの自動連携
2. ITアプリケーション外で行われる自動処理	(例) EUC (スプレッドシートやマクロ機能等) やRPA
3. ITに関する業務委託	(例) ASPやクラウドサービス
4. その他の企業外部とのデータ自動連携手法	(例) EDIやAPI連携

1. ITアプリケーション間のインターフェース

1つのアプリケーションで処理された結果は、帳票等としてアウトプットされるだけでなく、もう1つのITアプリケーションのインプット情報としてデータの引き渡しが行われることがあります(例: 販売管理システムで処理された売上情報が、売上に関する会計仕訳の情報として会計システムに引き渡される)。このような上流アプリケーションから下流アプリケーションへのインターフェースは、帳票等を基に手作業でアップロードするケースや自動でデータが連携するケースなどがあります。自動化されたインターフェースに対して適切な情報処理統制やIT全般統制があれば、データ連携の信頼性は高まります。

2. ITアプリケーション外で行われる自動処理

EUC (エンドユーザー・コンピューティング) という概念があります。これは、システムの開発や運用を情報システム部門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。以前から市販のパッケージ・ソフトウェアやスプレッドシートなど一般的なソフトウェアをEUCのツールとして用いることがありました。

近年では、定型業務の自動化を実現するために「RPA (Robotics Process Automation)」と呼ばれる技術を導入する企業が増えています。RPAは、複数の作業を一連の手続きとして自動化することができます。例えば、全国の店舗にあるPOSシステムや支店からメールで届く売上情報を日次で集計し一覧表を作成するとともに、その情報に基づき会計伝票を作成し売上仕訳を計上するといった一連の作業を、1回の指示で実行することも可能です。RPAを利用することにより、スプレッドシートやマクロを利用した従来の

EUCよりも複雑な作業の自動化が可能となっています。

RPAでは、ソフトウェア等を用いることで、ワークフロー図の作成やパラメーターの設定などの簡単な作業だけで、あらかじめ定めた手続きを自動化することができます。そのため、従来のスプレッドシートやマクロを利用したEUCよりも複雑な作業について、プログラミングなどのITの専門知識がなくても現場部門が自動化を実現することが可能になりました。

RPAの登場により、現場部門が主導的にシステム化できるため迅速かつ柔軟な対応ができるようになった一方で、データ連携のプロセスに情報システム部門が関与しない仕組みが組み込まれることになりデータの信頼性が損なわれるリスクが生じています。例えば、実験的に使用していたRPAを現場主導で本番環境に使用する場合、上流もしくは下流のITシステムへの影響といったシステム全体の俯瞰的な観点の検討が欠けてしまったといったケースがあります。また、テストが不十分であり、RPAが誤って出力またはデータ加工したレポートを基に、誤った判断がなされるリスクがあります。

いわゆる「野良ロボット」問題も存在します。これは、作成されたRPAの管理者が不在・不明になった状態を指しており、RPAが誤動作を起こすことや、適切なメンテナンスができないといったリスクを生じさせます。

このような事態を防ぐためにも、情報システム部門が主導でRPAのルール整備や台帳管理、定期的モニタリング等の管理体制を整備することは有効な手段となります。

3. ITに関する業務委託

従来、企業は自社でサーバーを所有して、その管理を自社で実施、もしくは外部委託することが一般的でしたが、近年ではASP（Application Service Provider）やクラウドサービスといった新しい形態も登場しています。

ASPとは、特定および不特定ユーザーが必要とするシステム機能を、ネットワークを通じて提供するサービスを言います^{※2}。ASPのユーザーはインターネットやVPN（仮想私設通信網）を経由して、ASPのサーバーにインストールされたアプリケーションソフトをサービスとして利用します。クラウドサービスは、インター

ネットに接続された環境で、さまざまなサービスを必要に応じて利用できるようにする仕組みです。ユーザーは自社でサーバーを所有することなく必要な機能だけを必要なときに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。

ASPやクラウドサービスを利用する場合、サービス提供者における情報処理統制やIT全般統制についても注意が必要です。サービスを外部に委託した場合、日常的に行う重要なオペレーションの実態把握が不可能となってしまう状況は避けなければなりません。また、ASPやクラウドサービスは、サービス提供者が所有する環境をユーザーが利用する形態であり、サービスを利用する企業は多くの利用者の一部にすぎません。そのため、サービスを利用する企業の意向は反映されにくい傾向にあります。

そのため、適切なサービス提供者の選定を行い、サービス提供者の信頼性が自社の要求水準を満たしているかを定期的に評価することが重要になります。

サービス提供者の内部統制の実態把握の有効な手段の1つに、サービス提供者から保証報告書（SOCレポート）を入手することが考えられます。これは、サービス提供者が複数の委託元企業の要求に対応するため、監査法人から取得した内部統制の評価結果をまとめたレポートです。ただし、これは有効な情報取得手段の1つではありますが、評価対象が委託元企業の要求と必ずしも一致しない場合もあるため、監査報告書の閲覧に当たって委託元企業は自社の要求との適合状況を確認することに留意する必要があります。

4. その他の外部企業とのデータ自動連携手法

いわゆる電子データ交換（EDI）による企業間のデータ連携は従来見られましたが、最近ではAPI（Application Programming Interface）連携も多く見られます。APIとは、あるプログラムが異なるプログラムやデータを呼び出して利用するインターフェースです。APIを利用することで、別々の会社のシステムであっても容易にデータ連携を行うことが可能になります。例えば、クラウド経費精算ソフトとクラウド会計ソフトをAPIで連携し、自動で会計仕訳を起票するサービスを提供している事例などがあります。

このようなサービスのユーザーがサービス提供者の内部統制を理解するに当たっては、個々のサービス

※2 一般社団法人 日本クラウド産業協会（aspicjapan.org/cloud/index.html）



提供者における情報処理統制やIT全般統制を理解するとともに、サービス提供者間のAPI連携におけるルール（例：責任分界点の明確化や双方の管理状況の定期的な評価等）を理解することも有用です。

V おわりに

DXの進展に伴い、企業をまたいだリアルタイムなデータ自動連携はますます進んでいくことでしょう。これに伴い生じると想定される新たなリスクに対処するためにも、そのリスクについての理解とそれを予防もしくは適時に発見するための内部統制がますます重要となります。

お問い合わせ先

EY新日本有限責任監査法人
アシュアランスイノベーション本部 AIラボ
E-mail : sadaaki.motoyama@jp.ey.com