平成 15 年 12 月 10 日

I T 委員会研究報告第 24 号

「 I T 委員会報告第 1 号関係用語集」

日 本 公 認 会 計 士 協 会
I T 委 員 会

はじめに

本研究報告は、平成 15 年 1 月に公表した I T 委員会報告第 1 号「財務諸表監査における情報技術（I T）を利用した情報システムに関する統制リスクの評価（中間報告）」（以下「I T 委員会報告第 1 号」という。）の中で使用されている I T 関係の用語について、その意味を解説したものである。

なお、本用語集で採り上げている用語は、同報告書で使用している I T 関係の用語のすべてではなく、同報告書を理解し監査業務を実施する上で必要と思われるキーワードのみに限定している。記載を省略している I T 関係の一般的な用語については、市販されているコンピュータ関係の各種用語辞典や各種ホームページが参考となる。

用語

あ行

アクセス管理（第 3 章、第 1 項、(2)-(2) 4 行目）

コンピュータ、ネットワーク、データ等に、正当な権限を持った者だけが、決められた正規の手順に従って正当な承認を受けたうえでアクセスでき、それ以外の不正なアクセスが行われないようにすること。

この管理は、不正アクセスを発見し、それによる被害の有無を確認し、是正することを含む。

アプリケーション・システム（第 1 章、注 1、1 行目）

アプリケーション・システムとは、企業のビジネスプロセスに関連するデータと情報を、入力、格納、処理、保有、伝送又は検索するために必要なコンピュータプログラム、仕様、手続及び技術をいう。

I T は、アプリケーション・システムと I T 基盤（インフラ）から成り立っている。

アプリケーション・システムの運用監視体制（第 2 章、第 6 項、(3)-(2) 1 行目）

アプリケーション・システムが適時に実行され、正常に終了し、必要な結果が得られるよう監視する体制をいう。

具体的には、プログラムの実行中のエラーを検知したり、データの処理件数や金額から処理漏れや、異常がないか等をチェックし、システムを意図した目的に従って機能させるような組織上、権限上の仕組又は構造を指す。

維持継続性（第 2 章、第 6 項、(2)-(6)）

Maintainability。必要な情報が継続的に保持・更新されて利用可能であることをいう。

例えば、新しい得意先が得意先リストに追加されない状態は、維持継続性が害されていることになる。

運用管理（第 2 章、第 6 項、注 4、1 行目）

ハードウェア、ソフトウェア、ネットワーク構成、性能、セキュリティ、障害

対応、テストなどを包括的に管理し、システムを意図した目的に従って機能させること。

オンラインリアルタイムのデータ転送（付録、表 2、改善点-1. 出荷データの入力 9 行目）

データの入力装置とホストコンピュータなどが、相互に接続されたオンライン環境で、データを発生時点で即時に転送・処理し、結果を表示する情報交換方式のこと。

夜間などに、データを一括して処理するバッチ処理方式と対比して用いられる。

か行

開発管理（第 3 章、第 1 項、(2)-③ 4 行目）

コンピュータシステムの開発管理局面において、適切なスケジュール管理や完成物のチェックを行うこと。

こうした管理体制が十分に構築されていないと、開発の遅延や開発費用の増大を招いたり、システムが十分に機能できないなどの不具合が生じる。また、文書化が十分でないとシステムの維持管理が困難になる。

外部委託のサービスレベル（第 3 章、第 2 項、(7)）

システムの運用管理などを外部委託する際に、委託先が委託元に提供するサービスの程度。

委託元が、自社に必要とされるサービスの程度（例えば、ヘルプデスクの対応時間帯やシステムの利用不能時間の上限など）を明確にしておかないと、業務の目的を達成しているかを判断できない。別途、サービスレベルアグリーメント（SLA）を締結する場合がある。

可用性（第 2 章、第 6 項、(2)-③）

Availability。情報が必要とされるときに利用可能であること。

例えば、システム障害によりシステムが利用できない状態は、可用性が害されていることになる。

監視活動（モニタリング）（第 2 章、第 7 項、(1)-⑤）

モニタリングは監視活動と訳されているが、一般的に理解される監視という言葉の意味よりは広い。すなわち、問題点の検出だけではなく、その問題点の是正改善活動までが含まれた概念である。

経営者は、状況の変化に対応できるように、常時、統制活動の実施状況と例外事項について把握し、必要な是正・改善活動を行い、内部統制を一定のレベルに保つ必要がある（監査基準委員会報告第 20 号第 16 項から第 19 項参照）。

関連するマスタの自動照合機能（付録、表 2、改善点-4. マスタ管理 1 行目）

分散マスタ・ファイル間の整合性をチェックすること（後段の「分散マスタ・ファイル間の整合性」を参照）。

基幹システム（第3章、第1項、(2)-①-7.)

監査上の観点からは、企業におけるビジネスの基幹業務に関する情報を処理しているシステムのこと。

一般的な製造業の場合、購買・販売・物流・生産管理などが基幹業務に含まれる。これに対して、人事、総務、会計などは支援業務といわれる。

基本ソフトウェア構成（第3章、第1項、(1)-① 4行目）

アプリケーション・システムを実行するために必要な環境としてのオペレーティングシステム（OS）、データベース管理システム（DBMS）などの構成をいう。

機密性（第2章、第6項、(2)-④）

Confidentiality。情報が正当な権限者以外に利用されないように保護されていること。

例えば、企業内部及び外部からの不正アクセスによるシステム侵入が可能な状態は、機密性が害されていることになる。

境界のない接続環境（第1章、第1項、6行目）

インターネットなどを介して企業外部とネットワークが接続されている状態をいう。

業務処理統制（第2章、第6項、(3)-①）

個々のアプリケーション・システムにおいて、開始された取引が承認され、漏れなく正確に記録され、処理されることを確保する統制活動をいう。

業務処理統制には、プログラムに組み込まれた統制活動と、人とITが一体となって機能する統制活動がある。

クライアント・サーバシステム（第3章、第1項、(2)-③）

パソコン（PC）などのクライアントが、情報処理の中核を担うサーバに、ネットワークで処理を要請する構成の分散型システムをいう。

情報処理の一部をクライアント側で行うので入力に対する返答は速くなる。

さ行

サービスレベル（第3章、第2項、(7)）

システムの運用管理等を委託された者（受託者）が、委託者に提供するサービスの品質の程度（レベル）のこと。

例えば、委託者と受託者の間で、システムの運用時間や停止時の対応を保証するなど、サービスの品質について、サービスレベルアグリーメント（SLA）の形で契約する場合がある。

実行スケジュール管理（第3章、第4項、(6)-③ 6行目）

プログラム等が動作する時期、順序や条件を管理すること。

正しいプログラムであっても、正しい時期・正しい順序で実行しなければ、正

しい出力結果とならない。

自動実行ツール（第3章、第4項、(6)-③ 4行目）

プログラムの実行順序及び時間、条件等を登録して自動的に実行するツール(プログラム) のこと。スケジューラとも呼ばれている。

情報資産（第2章、第9項、6行目）

情報は利用者にとって有用なデータや意味あるデータをいい、企業にとって価値ある情報は資産として認識し、管理する。

情報資産という場合には、電子データのみならず、そのインプットの原票、アウトプット帳票類も含む。

情報システム（第1章、第1項、5行目）

情報を識別、収集、処理及び報告するためのシステムをいう。

情報システムの信頼性（第2章、第6項、(1) 3行目）

情報システムの品質。例えば、障害の発生頻度・影響の範囲・回復の度合いをいう。

情報セキュリティ（第2章、第6項、図2-*）

セキュリティとは、重要な資産を喪失、漏洩、損傷から保護することを意味する。

したがって、情報セキュリティとは、情報も重要な資産であるとの認識のもと、情報及びその情報を伝える情報システムを、未承認の物理的、論理的アクセス・コントロール等の不備（準拠性、網羅性、可用性、機密性、正確性、維持継続性、正当性の欠如）から生じる危害から保護することを意味する。

情報の信頼性（第2章、第5項）

ITにおける情報の信頼性とは、人、物、金の動きとデータが一致することをいう。

例えば、売上計上基準が出荷基準とすると、販売プロセスの出荷のファンクションで売上データが作成されること、つまり、売上データが出荷の事実に基づいて作成されることである。

セキュリティ管理（第3章、第1項、(2)-② 5行目）

セキュリティが確保されているかどうかを管理すること（情報セキュリティ参照）。

セキュリティ・ポリシー（第3章、第4項、(6)-①-7. 14行目）

企業が情報資産や情報システムに対してどのように取組み、組織がどのように行動すべきか、という全社的なセキュリティの方針を、経営のトップが明文化した規範をいい、企業倫理や業務内容を反映したものをいう。

全般統制（第2章、第6項、(3)-②）

業務処理統制が有効に機能する環境を保証する間接的な統制のこと。

一般に、ネットワークの運用管理、システム・ソフトウェアの取得及び保守、アクセス・コントロールやアプリケーション・システムの取得、開発及び保守に関する統制活動が含まれる。

存在チェック（付録、表1、会計データの正当性-統制活動の例 5行目）

入力データの発生時点などにおいて、その中で使用される情報が、予め定めたマスタファイルなどに登録されているかどうかをチェックすること。

た行

データオーナー（データの所有者・管理者）（第3章、第4項、(6)-1-イ. 16行目）

データを本来の目的のために利用する権利を有する者（データの所有者）及びそのデータが本来の目的外で利用されないように管理する義務をもつ者（データの管理者）のこと。

デットスタンプ（付録、表2、改善点-1.出荷データの入力 7行目）

業務処理の日付を日付印としてデータに記録すること。

システム内部に設定されている日付を利用することもある。

電子商取引（第2章、第3項、7行目）

インターネットや専用回線等のネットワーク上で行われる商取引の総称。

電子商取引には、企業間の取引（Business to Business、「B to B」）と企業対消費者の取引（Business to Customer、「B to C」）等がある。

統合型のアプリケーション・システム（第3章、第1項、(2)-⑤ 1行目）

業務プロセスごとに独立しているアプリケーション・システムを相互に参照して、業務横断的に機能するのが統合型のアプリケーション・システムである。

いわゆるERPソフトも、統合型のアプリケーション・システムの一つである。

統合型のアプリケーション・システムは、企業戦略の実現のために、経営者が判断に必要な情報を適時に提供するために活用される。

これらのアプリケーション・システムのいくつかには、企業のビジネスプロセスの管理メニューも用意されている。

な行

入力環境（第3章、第1項、(2)-② 3行目）

データを入力する環境のこと。

以前は、セキュリティが確保された専用端末（入退室管理の行われる専用ルームに端末が設置されて、専門のオペレータのみが操作可能な場合など）が想定されていたが、現在では各自のPC、POSレジ、携帯電話等にまでその範囲が拡大している。

認証（第3章、第4項、(6)-③ 16行目）

システムやネットワークへのアクセス時に求められる本人確認のこと。

ネットワークの運用管理（第2章、第6項、注4、1行目）

ネットワークが目的どおりに正常に動作しているかどうかを確認すること。

ハッカー対策やコンピュータウイルス対策等を含めたセキュリティ対策も含まれる。

は行

パスワードの管理（第2章、第9項、3行目）

他者から推測可能なパスワードの使用禁止や、パスワードの定期的な変更、更新時のルール等を実践すること。

ハッカー対策（第3章、第4項、(6)-④ 9行目）

本来、ハッカーとは、高度なコンピュータ技術の保有者を指したが、一般的には、コンピュータシステムに不正な侵入、データ窃盗・改竄等を行うクラッカーと混在して用いられている。

ハッカー対策とは、コンピュータシステムへの不正な侵入・データ窃盗を予防・検知するために講じる手段等を指し、そのためのハードウェア・ソフトウェアも開発されている。

バックアップ体制（付録、表3、対策-運用管理 1行目）

不慮の事故が生じた際に、速やかに復旧を終え、業務への障害を最小限にするための一連の管理体制をいう。

プログラムやデータなどのファイルを、別の記録メディアに複製・保存すること、停電に備えて無停電電源装置や、災害時に起動する外部の予備施設・予備通信回線等を設置することなどをいう。

バッチ（付録、表1、会計データの網羅性-統制活動の例 9行目）

ユーザにより入力されたデータに対して、予め登録された一連の処理をまとめて実行する方式をいう。

処理の間隔により、日次バッチ・週次バッチ・月次バッチ等と表現されることがある。

これに対して、ユーザによる入力の都度、データ処理を実行する方式をリアルタイム処理という。

ビジネスプロセス（第1章、注1、2行目）

企業のビジネスプロセスとは、事業目的を達成するために、企業の経営者及び構成員が行う一連の活動（例えば、売上プロセス、入金プロセス、仕入プロセス、出金プロセスなど）をいう。

ビジネスモデル（第1章、第1項、1行目）

企業が事業で利益を獲得するために、どの分野で、何をどのように行うかとい

う「利益を獲得するための具体的なビジネスのやり方の雛型」のこと。

ファンクション（働き）（第3章、第4項、(1) 5行目）

ビジネスプロセスを構成する個々の機能をいう。

販売活動を例にすると、売上計上プロセスと債権回収プロセスに大別され、売上計上プロセスは、さらに受注・与信確認・出荷といったファンクションから構成される。

プログラム等の移行・変更管理（第3章、第4項、(6)-② 9行目）

システムの正常な運用を保証するため、プログラムを別のプログラムに移行・変更する場合に、環境、手順、変更内容の履歴の文書化などを管理すること。

分散マスタ・ファイル間の整合性（第3章、第4項、(3)-④ 3行目）

異なるシステム間で同一内容のマスタ・ファイルを使用する場合（分散マスタ・ファイル）において、当該マスタ・ファイル間の内容が同一であることを確保すること。

ホスト系システム（第3章、第1項、(2)-③ 2行目）

中央のコンピュータ（ホスト）で集中して演算処理を行い、各端末装置では入出力のみを行うシステムの構成をいう。

本人の認証（第3章、第4項、(6)-③ 16行目）

ネットワークなどでアクセス権を要求しているユーザが本人であるかどうかを検証する作業をいう。

認証の方法として、ユーザ名とパスワードを入力させるのが一般的である。

ま行

マスタの定期的な棚卸（付録、表2、改善点-4. マスタ管理 7行目）

IT委員会報告第1号の付録【表2】「4. マスタ管理」の改善点を参照のこと。

マスタ・ファイル（第2章、第6項、(3)-① 3行目）

顧客マスタや単価マスタなどの業務の基幹となるような固定的な情報を記録したファイルをいう。

モジュール（第3章、第4項、図4）

論理的に分離可能なソフトウェアやハードウェアの構成部品又は構成単位をいう。

ら行

ライブラリ管理（第3章、第4項、(6)-③ 8行目）

ライブラリとは、ソースプログラム、実行ファイルを保管する領域を意味する。

したがって、ライブラリ管理とは、ソースプログラム等の受払いを管理するこ

とをいう。

I T

I T間の不整合（第3章、第1項、(2)-①-イ 5行目）

異なるシステム間でのデータ様式の不統一や処理タイミングのずれにより、データ更新の失敗や、システム自体が停止するなどの不具合が生じること。

I T基盤（インフラ）（第1章、注1、1行目）

I T基盤とは、アプリケーション・システムを支援するために必要なハードウェア、ソフトウェア、並びにネットワークの構成要素（コンポーネント）及びそれらの連携したものをいう。

I Tは、アプリケーション・システムとI T基盤（インフラ）から成り立っている。

I Tのコントロール目標（第2章、第6項）

I Tのコントロール目標の例として、準拠性、網羅性、可用性、機密性、正確性、維持継続性、正当性が挙げられる。（I T委員会報告第1号のⅡ-6(3)図2参照）。

監査業務においては、I Tのコントロール目標と監査要点との関係を理解することが重要である。

I Tの専門家（第2章、第2項、4行目）

I Tに係る統制リスクの評価を行う上で必要なI Tに関する知識、経験を有している専門家をいう。

I Tの専門家としては、情報処理技術者、システム監査専門家などを想定している。

I Tの専門家の業務の客観性の評価（第2章、第2項、5行目）

I T委員会報告第1号に記載されているI Tの専門家の業務の客観性の評価については、監査基準委員会報告書第14号「専門家の業務の利用」の第6項から第8項に記載されている内容が参考となる。

I Tの標準化（第3章、第4項、(6)-イ 6行目）

I Tに関する管理の有効性、効率性を高めるために標準（ルールなど）を設け、それに従ってI Tの構築、運用を行うこと。

I Tの品質水準（第3章、第4項、(6)-イ 5行目）

I Tが提供するサービスの質的水準をいう。

一般的には、I Tのサービスの品質が高いと業務結果の信頼性も高いと判断される。したがって、監査業務においてI Tの品質水準のレベルを推定することは重要である。

以 上