［論　説］

IT マネジメントとシステム監査

吉　田　　洋

はじめに

IT システムは、企業の会計の現場はもとより、全ての経営活動の中にまで入り込んでおり、その恩恵は計り知れない。それは、プラスの面であり社会生活の利便さ向上、企業経営の価値の向上などである。

IT マネジメントで検討すべき課題はプロジェクトマネジメント、サービスマネジメントそしてシステム監査である。本稿では、IT マネジメントの主要分野を紹介したのち、システム監査に焦点を当て検討する。

IT 化が進めば進むほど便利になる反面、様々な問題が生じてくるのは技術の進歩に共通する悩みである。それは、マイナスの面であり、犯罪・プライバシー情報の漏洩、システムの停止による社会的混乱などである。

そのような問題の一つに、事故や災害などでコンピュータシステムが止まってしまって仕事が遂行できなくなる事態や、コンピュータ犯罪の発生やプライバシー情報の漏洩という社会的な影響が大きいトラブルがある。システムが停止してしまったら想像以上のダメージを受けることは、大震災での生産活動に与えた影響だけではない。かつて銀行の統合システムがダウンして多くの企業活動が数日にわたって停止してしまった事件でもわかる[1)]。また、ウイルスの

ように一企業内だけの問題ではなくネットワークを通じて関連するすべての企業に被害をもたらすことになる。

このような様々な観点から企業や自治体および各種団体の情報システムについて、その問題点を指摘し改善提案をするのが「システム監査人」といわれる技術者である。これはわが国の情報処理技術者試験においてシステム監査技術者試験を実施しているし、アメリカに本部を置く民間団体、情報システムコントロール協会（ISACA）の公認情報システム監査人（CISA）や一般社団法人日本内部監査協会の情報システム監査専門内部監査士でも同様の資格を付与している[2)]。

監査は前向きな IT マネジメントである。「システム監査」は保証型と助言型があって、助言型監査では「どうすればよいかを提言する」ことが目的である。今後の IT 化の普及につれ、益々多くの企業で重要な役割を担うものであることは言うまでもない。本稿では改めて過去の議論を含めて新たな方向性を模索したい。

1．IT マネジメントの主要分野

システム監査は会計監査の IT への対応に関する部分を研究する分野でもあり、会計学の一分野であることは間違いない。しかし、わが国で実施されている例えば基本情報技術者試験では IT マネジメントとしてプロジェクトマネジメント、サービスマネジメントそしてシステム監査 3 つが主要分野とされている。次にシステム監査以外のものについてその概要を示そう[3)]。

(1) プロジェクトマネジメント

アメリカの PMI（Project Management Institute：プロジェクトマネジメント協会）が策定したプロジェクトマネジメントの知識体系のことである。プロジェクトマネジメントの工程を次の 5 つのプロセス群に分類している。

立上げプロセス群

計画プロセス群
実行プロセス群
監視・コントロール・プロセス群
終結プロセス群

また、管理する対象によってプロジェクトマネジメントを 10 の知識エリアに分類している。

プロジェクト統合マネジメント
プロジェクト・スコープ・マネジメント
プロジェクト・タイム・マネジメント
プロジェクト・コスト・マネジメント
プロジェクト品質マネジメント
プロジェクト人的資源マネジメント
プロジェクト・コミュニケーション・マネジメント
プロジェクト・リスク・マネジメント
プロジェクト調達マネジメント
プロジェクト・ステークホルダー・マネジメント

(2) サービスマネジメント

IT のサービスマネジメントの体系としてはイギリス政府が策定した国際的なガイドライン、ITIL がある。ITIL は ITSMS（IT Service Management System：IT サービスマネジメントシステム）とも言われ、以下を目的として掲げて、ベストプラクティス（成功例）を示して運用管理業務を解説している。

・サービスサポート
サービスデスクを中心としてユーザを支援するプロバイダのベストプラクテスがまとめられている。
・サービスデリバリ
サービスレベルの管理を中心として事業を支えるサービスをいかにして供給し

ていくかという観点で、プロバイダの活動が説明されている。

また、IT サービスマネジメントに関する国際規格に ISO/IEC 20000 があり、IT サービスの提供者が顧客の求めるサービス品質を継続的に供給し、改善するために必要な事項を規定し、この規格を JIS 化したものが JIS Q 20000 である。

2．システム監査基準策定の経緯

システム監査基準の策定の経緯を振り返っておこう。システム監査は、組織体が自発的に実施する内部監査の一環として発展してきたものであり、通商産業省（現在の経済産業省）の監査関連施策を歴史的に見ると、その出発点は 1951 年 7 月の「企業における内部統制の大綱」に端を発している。通商産業省では、1985 年 1 月、システム監査に関するガイドラインとして、「システム監査基準」を策定・公表した。これは通商産業省が 1983 年 12 月に発表した産業構造審議会情報産業部会の中間答申に基づくものである。システム監査基準では「システム監査は、コンピュータシステムの信頼性、安全性、効率性等[4]を確保するため、監査対象から独立した監査人が一定の基準に基づいて、コンピュータシステムを総合的に点検・評価し、関係者に助言、勧告するものである」と定義付けている。それにあわせるかのように、1986 年には第 1 回システム監査技術者試験が実施された。その後、後述する情報環境の変化、国際化、災害対策等への対応するため、1996 年 1 月、システム監査基準を改訂し、2004 年 10 月にさらに改訂が行われ現在に至っている。システム監査基準にかかわる経済産業省の監査関連施策は図表 1 のようである[5]。現在、システム管理基準の大幅な改訂が進んでいる。

図表 1　経済産業省のシステム監査関連施策

1951 年 7 月
企業における内部統制の大綱
1953 年 2 月
内部統制の実施に関する手続き要領
1980 年 3 月
日本情報処理開発協会がシステム監査基準（試案）公表
1983 年 12 月
産業構造審議会情報産業部会中間答申でシステム監査基準の策定を提言
1985 年 1 月
システム監査基準策定
1986 年 10 月
第 1 回システム監査技術者試験実施
1991 年 3 月
システム監査企業台帳に関する規則（通商産業省、現経済産業省告示第 72 号）
1996 年 1 月
システム監査基準第 1 回改訂
2003 年 4 月
情報セキュリティ監査基準、情報セキュリティ管理基準公表
情報セキュリティ監査企業台帳に関する規則（経済産業省告示第 113 号）
2004 年 10 月
システム監査基準第 2 回改訂、システム管理基準公表
2007 年 3 月
システム管理基準追補（財務報告に係る IT 統制ガイダンス）
2017 年
「システム管理基準」改訂委員会（仮称）発足

改訂システム監査基準（1996 年）では、「監査対象から独立かつ客観的立場のシステム監査人が情報システムを総合的に点検及び評価し、組織体の長に助言及び勧告するとともにフォローアップする一連の活動」（システム監査基準、Ⅱ用語の定義）として、改定前のシステム監査基準と比べ、関係者から組織体の長に変更され、監査目標の定義から趣旨に移動され、フォローアップが含ま

れるといった変更が行われた。

改定基準の構成や性格には大きな変化が見られないが、次の点が検討されている。

(1) 情報環境の変化への対応

近年のダウンサイジング化、アウトソーシング化等々の進展により、情報システムは従来のメインフレームによる集中処理システム中心から、クライアント/サーバーなどによる分散処理システムの導入へと大きく転換している点やインターネットの普及に見られるネットワークの利用・応用の多様化といった、ダイナミックな情報環境の変化に対し、対応した。

(2) 国際化への対応

国際協力開発機構（OECD）改定基準が 1992 年に公表した「情報システムの、セキュリティ・ガイドライン」の第一の原則（現在は第二原則）である「責任原則」の精神をシステム監査基準に反映させるため、システム監査人の責任・権限を明確にした。

(3) 災害対策への対応

阪神・淡路大震災を教訓として、災害対策やバックアップ対策のあり方を重視した。

(4) 他の施策との整合

通商産業省が施策している他のセキュリティ関連基準等との整合性をとり、相互関連を明確にし、より効果を高めるようにする必要があるとした。

a. 用語の定義

改定基準では、この基準で使用する主な用語の定義をしている。

b. 一般基準

改定基準では、OECD のセキュリティ・ガイドラインの主旨を受け入れて「システム監査人の責任・権限」という項目とともに、「職業倫理」、「守秘義務」いう項目も定め、システム監査人の位置づけをより強固にしている。したがって、システム監査人の責任が重くなったと言える。

c. 実施基準

実施基準の構成には、大きな変化が見られる。旧基準では、「企画業務」、「開発業務」、「運用業務」の三つに分類していたが、改定基準では、これらに「保守業務」をくわえ、さらに各業務に共通する内容については、「共通業務」として独立させている。「保守業務」では、システムやプログラムの保守についてふれている。「共通業務」として、ドキュメント管理、進捗管理、要員管理、外部委託、災害対策を取り上げている。これらは、情報システムの内部統制でいうところの全般統制（general control）である。

d. 報告基準

報告基準に関しては、内容的な変更はないが整理されている[6)]。

3．現行のシステム監査基準、システム管理基準

(1) システム監査の目的

2004 年の第 2 回改訂では「システム監査の目的は、組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行い、もって IT ガバナンスの実現に寄与することである（システム監査基準、Ⅱ．システム監査の目的）」とされている。従来からの目的であった情報システムの信頼性、安全性、効率性の向上は後述するリスクに対するコントロールに統合され、保証・助言、IT ガバナンスが今回の目的に加わった点であり、その目的は大きく変化した。しかし、構成は引き続き、一般基準、実施基準、報告基準の順になっている。

システム管理基準では「組織体が主体的に経営戦略に沿って効果的な情報システム戦略を立案し、その戦略に基づき情報システムの企画・開発・運用・保守というライフサイクルの中で、効果的な情報システム投資のための、またリ

スクを低減するためのコントロールを適切に整備・運用するための実践規範である。」とされている。

(2) 監査人の行為規範

システム監査基準は、システム監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範である（システム監査基準、前文）今回の改訂での大きな変更点は「監査人の行為規範」と「情報システム管理の基準」との峻別したことである。企業会計であれば、「監査基準」と「企業会計基準」の関係である。

監査主体の行為規範を定めた基準として「システム監査基準」(一般基準、実施基準、報告基準）が公表され、効果的な情報システム戦略を立てるための実績規範を定めた基準つまり、監査の際、監査人が行う判断の尺度として「システム管理基準」(情報戦略、企画業務、開発業務、運用業務、保守業務、共通業務）が公表された。システム監査の実施に当たっては、組織体における情報システムにまつわるリスクに対するコントロールの適否を判断するための尺度である（システム監査基準、前文)。新たに設けられたシステム監査基準は、従来のシステム監査基準の内で、実施基準として監査対象業務ごとに挙げられていた 191 項目を 287 項目に拡張したものである。「システム管理基準」はISACA（情報システムコントロール協会）の関連団体である IT ガバナンス協会が公表している COBIT 3（2000 年)[7] と整合性をとっている。

(3) IT ガバナンス

従来の「システム監査基準」は情報システムのライフサイクル各段階におけるリスクが適切に管理されていたかを監査するための必要な事項を記していたが、今回の改訂では IT ガバナンスの観点を考慮している。経済産業省は IT ガバナンスを次のように定義している。

「企業が競争優位性構築を目的に、IT（情報技術）戦略の策定・実行をコン

トロールし、あるべき方向に導く組織能力」

組織の経営戦略と IT 戦略を整合させ、IT 投資を適切に管理し、IT 要員やその体制、IT に関するリスクのコントロール等のフレームワークを確立する IT ガバナンスがきわめて重要になる。

(4) 技術革新に伴う新たなリスクへの対応

技術革新に伴う新たなリスクへの対応のための管理項目が追加されている。システム監査は、組織体の情報システムにまつわるリスクに対するコントロールが適切に整備・運用されていることを担保するための有効な手段となる。情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的として次のようなものを挙げている（システム監査基準、前文)

情報システムが、組織体の経営方針及び戦略目標の実現に貢献するため

情報システムが、組織体の目的を実現するような安全、有効かつ効率的に機能するため

情報システムが、内部及び外部に報告する情報の信頼性を保つように機能するため

情報システムが、関連法令、契約又は内部規定等に準拠するようにするため

これらの考え方の根底には、アメリカのトレッドウェイ委員会組織委員会による内部統制の定義（COSO 報告書、COSO-ERM のフレームワーク）を念頭においている。COSO-ERM（全社的リスク管理のフレームワーク）によれば、リスク・マネジメントの目的として戦略、業務、報告（財務、非財務を含む)、コンプライアンスへの貢献を挙げている[8)]。

2004 年のシステム監査基準、システム管理基準はこの流れに従って拡充がはかられている。従来の情報システムの信頼性、安全性、効率性の考え方を発展させながら変更していると考えられる。

(5) 保証型目的の監査

従来は内部監査の一環とした助言型のシステム監査を想定していたが、今回の改訂では情報システムに保証を付与することを目的とした監査、いわゆる保証型のシステム監査であっても利用できるようになっている。

(6) 外部への監査結果の開示

監査の説明責任を果たすため、内部だけでなく外部への監査結果の開示も想定した手続きとなっている[9]。

(7) システム監査関連基準

・情報セキュリティ監査

情報セキュリティ監査基準、情報セキュリティ管理基準に基づく検証をする。

・個人情報保護監査

個人情報の扱いが JIS Q 15001 規格に適合するかを検証する。適合すればプライバシーマーク制度によりプライバシーマークの使用が許可される。

・コンプライアンス監査

著作権法、不正競争防止法、労働基準法などの法律を遵守しているかについて検討する。

4．システム監査基準、システム管理基準の今後の課題

システム監査基準、システム管理基準は何らかの見直しが必要であろう。システム監査基準は金融庁の監査基準になぞらえて、再度見直しを図れば良いのであるが、システム管理基準をどうするかである。

わが国のシステム監査基準のような助言型監査は基本的にはコンサルティングであるので、助言型、保証型といった区分が国際的に理解を得られない。情

報システム監査とコントロールを中心に世界的をリードしている ISACA（情報システムコントロール協会）の COBIT 5 と整合性をとることで可能となる。システム管理基準は IFRS と同様で国際的に通用する基準にするべきである。わが国だけ独自の基準を作成しても世界的には通用しない[10]。そのことは IT マネジメントの三分野であるプロジェクトマネジメント、サービスマネジメントにおいて世界で認められた標準を使っており、それが日本でも尊重されていることである。ただし、それらがシステム内部監査人に理解でき、万全なコントロールの助言ができるかどうかは教育にかかっている。

システム監査の実施率と監査テーマ・内容について内部監査の一環としてのシステム監査の実施率を見てみよう。内部監査人がテクノロジーを理解する必要性は IIA Standard 1200 Proficiency and Due Professional Care（専門的能力と専門職の正当な注意）に求めることができる[11]。内部監査人の一般社団法人日本内部監査協会が実施している第 60 回内部監査実施状況調査結果によれば、情報システムに対する内部監査の実施率は全業種で 53.4%であり、前年度から実施率は上昇している。業種別でみると、製造業は 56.7%、非製造業は 52.4%であり、製造業で実施率が上昇した。

監査テーマ・内容は（着眼点・要点）の実施例は次のようなものであった。

情報システム業務規程、情報システム投資計画、PC、情報端末、モバイル通信機器、携帯電話、USB メモリ、大容量記憶媒体、権限者決済、分離統制、基幹システム整備、情報セキュリティマネジメントシステム（ISMS）認証、金融情報システムセンター基準対応、IT インフラの可用性、サービスレベル管理、ISO27001、JISQ15001、データ・バックアップ、保守メンテナンス体制、ファイヤーオール、SNS、クラウド管理、サーバー管理、ホームページ運用、コンテンツ管理、ライセンス管理、アクセス権管理、ユーザアカウント管理、ID・パスワード管理、個人情報、顧客情報管理、機密情報保持、情報漏洩防止、サーバーテロ対策、システム障害対策、情報システム教育、システム投資の予実管理、IT-BCP（事業実施計画）、顧客クレーム対応、J-SOX 対

応、IT 全般体制、IT 業務処理統制（ITAG）などが挙げられている[12)]。これらのテーマは各社においてリスクアセスメントの結果として選択されているものと推察される。今後は、内部システム監査人は AI 革命にも対応することが望まれる。IoT、ビックデータ、ディープラーニング（深層学習）の 3 技術が AI 革命の中核技術である[13)]。

むすび

日本内部監査協会の調査からすると、監査テーマは古色蒼然としてものであって、従来の内部監査人に対する教育・研修ではこれからのフィンテックと AI 革命時代における内部監査専門職に必要とされる知識とスキルが備わっていないことが懸念される。さらに、統計科学や情報技術に関する知識とスキルをも有する次世代型のシステム監査内部監査人が求められる。システム内部監査人が消滅することはないであろうが、定型的な業務の多くは、AI やブロックチェーンに代替されるのである[14)]。

伝統的システム内部監査人は失職し、1982 年のロンウェーバーの文献[15)]ですでに述べられているように、システム内部監査は伝統的監査、情報システム管理、行動科学、そしてコンピュータ科学といった他のディシプリンと結合した理論・実務とならざるをえない。現状の研究や実務を見るとこのような視点が十分でない。

システム監査については IT マネジメントひいては IT ガバナンスの観点から IT マネジメントの他の二つの分野と同様に国際的な団体による権威ある基準を採用し監査人を教育しなければ、世界から取り残されてしまうだろう。

注

1）井上治子、長谷川聡、吉田　洋、林　慶雲「「経営情報論」の研究・教育に関する論考」

『名古屋文理大学紀要』4 号、名古屋文理大学、59-64 頁、2004 年。

2）吉田　洋「第 7 章 IT プロフェッションの育成」堀江正之編著『IT のリスク・統制・監査』同文舘、163-187 頁、2009 年。

3）吉田　洋「IT 監査における統制とガバナンスの動向と課題」『愛知大学経営総合科学研究所』愛知大学、2009 年、53-70 頁。

Project Management Institute, A Guide to the Project Management Body of Knowledge (PMBK Guide), Fifth edition, Project Management Institute, 2013.

菅野厚『ITIL の基礎』マイナビ、2013 年、21 頁。

4）例えば、信頼性、安全性、効率性の例をあげれば次のようなものがある。

「信頼性」(可用性、正確性を含む)

例 1　システムは二重化等の障害対策を講じているか

例 2　入力値が正しいかの検証をチェックしているか

例 3　設計者のレビューを実施しているか

「安全性」

例 1　アクセス制御・管理機能が適切に設計・運用されているか

例 2　メールの添付ファイルはパスワード設定を行っているか

例 3　災害からシステムを保護しているか

例 4　記録媒体に秘密を意味する表示をしているか

「効率性」

例 1　ソフトウェアのライセンス証書などのエビデンスが保管されているか

例 2　企業経営に効果的に活用されているか

例 3　投資効果の向上が図られているか

月江伸弘『これでナットク! 基本情報技術者［午前］マネジメント/ストラテジ 集中対策』リックテレコム、2016 年。

5）日本のシステム監査の年表は以下に詳しい。

鳥居壮行『システム監査の歴史　提唱から 30 年の歩み』駿河台大学、2002 年、年表部分を一部修正。

6）吉田　洋『情報システム監査』税務経理協会、2002 年、122-124 頁。

7）現在は COBIT 5 が公表されている。詳しくは ISACA の HP（http://www.isaca.org/cobit/pages/default.aspx）を参照されたい。

COBIT のスコープは次のように変化している。

1996 年	COBIT 1 監査
1998 年	COBIT 2 コントロール
2000 年	COBIT 3 マネジメント
2005 年 2007 年	COBIT 4 IT ガバナンス
2012 年	COBIT 5 事業体の IT ガバナンス

詳しくは日本 IT ガバナンス協会の HP、http://www.itgi.jp/cobit/を参照されたい。

8）Moeller, Robert R., COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework, Wiley, 2007.

9）日本情報処理開発協会『新版　システム監査基準/システム管理基準解説書（平成 16

年基準改訂版）関連資料編』2004 年、日本情報処理開発協会。

10）例えば、会計基準を国際的に統一する方法では採用、承認、収斂がある。
採用とは国際的な会計基準の設定主体によって国際的な会計基準を設定して、各国の会計基準がそれを受け入れる方法である。システム管理基準の場合、採用ということであればISACA（COBIT 5）や IIA（GTAG）の基準ということになる。

11）Gibbs, Nelson, Divakar Jain, Amitesh Joshi, Surekha Muddamsetti, Sarabjot Singh, A New Auditor's Guide to Planning, Performing, and Presenting IT Audits, The Institute of Internal Auditors Research Foundation, 2010, p.1.
内部監査人協会『専門的実施の国際フレームワーク（2017 年版)』抜粋、一般社団法人日本内部監査協会、2017 年、17-19 頁。

12）丸太起大「解説・所見『第 60 回内部監査実施状況調査結果』」『第 60 回内部監査実施状況調査結果』一般社団法人日本内部監査協会、2017 年、12 頁。

13）岡田幸彦、野間幹晴「FinTech が引き起こす会計情報革命」『企業会計』Vol.16 No.6、中央経済社、2017 年、38 頁。

14）藤田勉「金融に革命が起こる！FinTech の基礎知識」『企業会計』Vol.16 No.6、2017 年、中央経済社、17 頁。

15）Ron Weber, EDP Auditing: Conceptual Foundations and Practice, McGraw-Hill, 1982, p.12.

吉田洋（愛知大学経営総合科学研究所客員研究員、名古屋文理大学健康生活学部教授）