

システム監査の一実現方法†

——統制マトリックス法の提案——

高橋光裕^{††} 坂内広蔵^{††}

本論文では、システム監査実務や内部統制の設計/分析を支援する手法、統制マトリックス法を提案する。システム監査人は、個々の情報システムの機能や処理方法を熟知していなければならない。また、安全性や信頼性のほか、効率性等も監査の範疇に含まれており、監査範囲が非常に広範である。したがって、監査人が情報や知識を整理し、活用するための枠組みが必要である。統制マトリックスは、人間系の作業を含めた広義の情報システムに対して、内部統制を、局面と観点から二次的に分類整理するためのワークシートである。ここで、局面は、業務手続き（フロー）上の個々の単位作業に対応し、データ入力、書面審査、帳票出力等、あらかじめ定められた十数種類の作業項目の一つである。一方、観点は、内部統制を目的別に分類するための枠組みであり、承認、処理記録、網羅性、不当排除、正確性の5種類である。内部統制は、達成の確実度の面から、ハードウェア、システムソフトウェア、アプリケーションソフトウェア、規則、指導の5段階にさらに分類される。統制マトリックスを用いて内部統制を整理すると、各単位作業に対する統制の充足度を複数の観点から検討する、ある観点について業務全体の流れの中での統制の充足度を検討する等が容易になる。また、統制マトリックスは、監査ノウハウや文献等から得た知識を整理したり、内部統制を設計する際にも利用できる。

1. はじめに

今日の社会では企業の日常業務のほとんどすべての分野でコンピュータによる情報処理が行われている。特に最近では、システムのオンライン化や部門別システムの統合化、情報の共有化が進められており、今後はさらに、ネットワークを活用した部門/企業横断的な『開かれた』システムが増えていくと考えられる。

このようなシステムは、その機能や処理内容が複雑なため、利用者はもちろん、開発者にとってもシステムの全体像が把握しにくいという問題がある。また、システム利用者が社内外に広く散在するため、運用管理や不正防止等が難しい。

一方、業務処理のコンピュータへの依存度は非常に高くなっており、システム障害の発生によって、広範囲の業務が停止したり、膨大な損害を被る危険がある。このようなシステムリスクを回避するために、システム監査の必要性が言われて久しいが、その実施には種々の問題が存在し、現時点では、システム監査が十分に普及し、機能しているとは言い難い状況である。中でも最大の問題は、情報システムは個々に異なる機能や処理手順を持っているため、会計監査の場合のような一義的な監査基準が決め難いことである。

本論文では、システム監査の概要を簡単に述べた後、システム運用面の監査に焦点を当て、システム開発・運用部門で内部統制を設計/文書化する作業や、監査人が各システム用のチェックリストを作成する作業を支援する手法『統制マトリックス法』を提案する。

2. システム監査の概要

2.1 監査、内部統制、システム監査の三者の関係

監査には、一般に、①公認会計士による『財務諸表監査（会計監査）』、②監査役による『監査役監査』、③社内の考査・監査部門等による『内部監査』の3種類がある。このうち①と②を外部監査といい、実施が法的に義務付けられている。③の内部監査は、法的な義務付けはなく、企業の経営者の自発的な命令によって、企業内の人間が、自社の業務を査察し、検証する。

一方、内部統制（internal control）とは、「企業における業務を正確かつ迅速に行わしめるためのあらゆる管理活動を総称したもの¹⁾」であるとされている。換言すれば、組織内で日常的に行われている管理業務（個々の統制方策）の総称である。ここで、各方策は、職務分掌、執務マニュアル等で明文化されているものと、管理職による監督、指導等のように管理者の判断によるものがある。統制方策は、対象範囲によって、部門統制、業務統制、全般統制に大別できる（図1）。また、内部監査は、各統制方策が正しく機能し、業務

† Control Matrix Method: An Approach to Information System Auditing by MITSUHIRO TAKAHASHI and KOZO BANNAI (Information System Department, Economic Research Center, Central Research Institute of Electric Power Industry).

†† (財)電力中央研究所経済研究所情報システム部

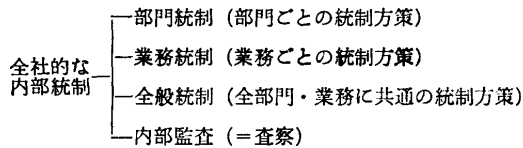


図1 内部統制の分類

Fig. 1 Categories of internal controls.

処理の結果は正しいかを検証する作業であり、これ自体も全社的な内部統制の一部（一つの統制方策）であると言える。

監査と聞くと、一般に、監査人による査察だけを考えがちであるが、日常の管理をきちんと行える体制が整っていないと、査察を行っても十分な効果が期待できない。なぜなら、第三者による査察では、あくまでも過去の業務処理の結果や現在実施中の業務の一部だけしかチェックできないからである。監査を実効性あるものとするためには、監査対象業務に対して、十分な内部統制が設定され、実施されていることが前提となる。しかし、純粋な勘違い等のような意図せぬ過ちや、管理者ぐるみの背任行為等は、内部統制の充実だけでは防止できないので、監査も必要である。

このように、監査と内部統制は、どちらかだけを充実すればよいという代替可能な性質を持つものではなく、両者を有機的に実施することによって、互いの短所を相互に補完しあう必要がある。

したがって、システム監査について論じる場合にも、本来は、査察に関する事項だけでなく、部門統制、業務統制、全般統制等の内部統制方策の設定と実施という、日常の管理もその範疇に含めて議論しなければならない。以下ではこれを『広義のシステム監査』とよび、査察を『狭義のシステム監査』とよぶことにする。

通産省のシステム監査基準⁴⁾が目的として挙げている「システムの信頼性、安全性、効率性の向上」を達成するためには、広義のシステム監査を考える必要がある。しかしその実施基準は、査察だけを扱っており、実態は狭義のシステム監査である。この目的と実施基準の内容の乖離が、システム監査の普及を妨げていると著者らは考えている。

2.2 システム監査のねらいと位置付け

著者らの考える広義のシステム監査は、コンピュータ関連業務に対して、様々な規程や管理指針を設定し、実施するという現場での日常の管理（内部統制）と、それらの内部統制が設定者の意図したとおりに確実に実施され、期待した効果が得られているかを

チェックするための査察（狭義のシステム監査）、という2種類の作業を併せたものである。

システム監査を論じる場合、『牽制』や『内部統制』等といういかめしい言葉が頻繁に使われるため、利用者部門やシステム開発部門等の被監査部門に必要な以上の警戒心を植え付けたり、反発をまねいたりする例がみられる。しかし、広義のシステム監査の真のねらいは、業務や情報システムを取り巻く種々のリスクに対して事前に防止/対応策を講じておくことによって、業務担当者が安心して業務を行えるような環境を整備することであると著者らは考えている。この意味で、広義のシステム監査は、むしろ、開発、運用、利用者、監査の各部門による『コンピュータ関連業務における品質管理 (QC) 活動の一種』と考えるべきである。

情報システムに対する品質やリスクの管理は、どの企業でも従来から様々な形で実施されている。しかし、システムが次第に巨大化し、業務に対するリスクが複雑化してくると、縦割りの組織内で個々の管理をバラバラに行っていたのでは、もれやムダが生じやすい。

著者らは、広義のシステム監査の目的を達成するためには、情報システムの企画、開発から、運用までの全過程に対して、部門や業務の枠にとらわれず、システム全体を一元的に管理できる体制を確立する必要があると考えている。従来は、システム管理方策を、部門ごとや業務ごとに独立に設定していたが、これを改め、部門・業務横断的な見地から、全体的な整合性や有効性が最も高い管理方策を作成し、また、各部門が定められた管理方策を確実に実施しているかどうかをチェックするための専任者を置く必要がある。

著者らは、『システム監査人』がこの管理の総括者に相当すると考えている。したがって、システム監査人は、自らが直接的に現場を管理するのではなく、また、単なる査察者でもなく、現場で働く人々にとっての良き助言者でなければならない。この助言者的役割は、これまで、情報システム部門（開発・運用部門）に求められる場合が多かったが、①コンピュータと業務の両方に関する専門知識が必要であること、②利用者部門と開発・運用部門の仲介者となる必要があること、③開発・運用部門が一般に多忙であること等から、システム監査人には、独立の専任者を当てる必要があると著者らは考える。

3. システム監査の現状と問題点

3.1 システム監査の現状

(1) システム監査の諸定義

システム監査に関しては、様々な団体や省庁等が、その立場や問題意識に沿って定義付けを行っている。

表1に3種類の著名な機関による定義を示す。

このうち、①は、監査という行為に焦点をしばった定義になっている。また、この定義では、『システムの有効活用』という問題が、重要な目的のひとつとされている。②は、定義主体の性格上、会計監査的な視点で定義している。③は、米国内部監査人協会の依頼によってスタンフォード研究所が行った研究の報告書(SAC レポート)⁵⁾における定義であり、内部統制の重要性を強調している点に特徴がある。

(2) システム監査の普及動向

昭和60年に通産省の『システム監査基準』が公表された頃から、わが国ではシステム監査が俄に脚光を浴びた。しかし、実際に実施している企業は未だ少ない。(財)日本情報処理開発協会が昭和63年と平成元年に実施した『システム監査普及状況調査』^{3),6)}を見ても、金融・保険業を除くと、システム監査の実施率は全産業平均で20%弱のまま横ばいである。また、システム監査を実施していると回答した企業においても、専任のシステム監査人を置いている企業はわずか10%程度である。

さらに、両調査でシステム監査が普及しない理由を問うたところ、「担当者の確保が難しい」、「システム監査の方法、制度、手続き等が十分でない」等があげ

られており、約50%の企業が、実施したいけれども実施できないとしている。このほかにも、別の調査によると、「当社にはコンピュータの不正や犯罪はない」等の理由をあげて、システム監査は不要と考えている企業もかなり多い。

3.2 システム監査の普及を阻害する問題点

前出の調査結果からも分かるように、現状で、わが国におけるシステム監査の普及を阻んでいる最大の理由は、監査を実施できる人材が不足していることである。ここでは、いくつかの観点から、人材不足の背景となっている諸問題点をあげる。

(1) 会計監査との本質的な違い

会計の分野では、法令や規則等によって処理の細部までが詳細に規定されており、企業間での差異や特殊性が非常に少ないため、一義的な監査基準が成立可能であり、公認会計士という社外の専門家(第三者)による監査が十分に機能する。

一方、情報システムが扱う一般業務には法令等による規定がほとんどなく、また、会社ごとに全く独自の機能と処理方式を採用しているため、監査対象システムの細部までを熟知している者でなければ、そのシステムを監査できないという問題がある。

この意味で、情報システムの監査人は、できるならば、社内の人間であることが望ましいが、実際には、大企業においても、業務内容と情報システムの細部を両方とも熟知している人材を確保することは、容易なことではない。また、ほとんどの企業が膨大な開発/保守バックログを抱えている現状では、真に優秀な人材を、システム開発・運用部門から監査部門に派遣する余力はほとんどなからう。一方、業務や監査の専門家に、複雑で大規模なシステムを監査できる技術力を求めるのも無理な場合が多い。

(2) 内部統制の不明確さ/不備

監査対象業務における内部統制(日常の管理)に関する文書類の有無、良否は、システム監査の作業効率、監査結果の有効性を左右する重大な要因である。

実際に監査人が査察を行う際には、①その業務に対して設定されている内部統制を調査し、②システムのリスクや期待されている効果を分析し、③既存の内部統制方策が妥当かどうか、それらがきちんと実施され機能しているかを検証するためのチェックリストを作成し、④それに基づいて査察や検証を行い、⑤結果をもとに改善勧告を行う、という5段階の手順を踏む。

ところが、日頃から場当り的な管理しか行っていない

表1 システム監査の諸定義

Table 1 Definitions of information system auditing.

定義した機関	定義
①通産省 (システム監査基準)	監査対象から独立したシステム監査人が情報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り、セキュリティ対策の实效性の担保およびシステムの有効活用を図る上で効果的な手段であると考えられる ¹⁾ 。
②日本公認会計士協会	EDPシステムによって作成された会計記録の信頼性の程度を確かめるために、システムに組み込まれている内部統制の信頼性を検討・評価し、EDPシステムによって作成された取引記録のデータ処理の有効性と妥当性を検討・評価すること ¹⁾ 。
③米国内部監査人協会	内部統制の特化された段階であり、データ処理およびその結果、例えばデータ・ファイルおよび出力レポートを律する統制を点検し、評価し、検証する ¹⁾ 。

かったり、管理内容が文書化されていない場合には、部外者の監査人には、日頃の業務がどのように管理されているかが全く分からず、その妥当性はチェックしようがない。特に、わが国では、企業風土として、あまり事細かに規則を作ることを好まず、また、規則を作る際にもわざと内容的に曖昧なものにしたり、細部を明文化しない場合が多い。このため、情報システムを監査する段になってから、どのような内部統制が決められており、いつ行われているのか、その目的は何か等を、監査人が一々調査しなければならないという場合が多く、監査制度が有効に機能しにくい土壌がある。

(3) 監査ガイドラインの偏り

最近では、様々な省庁等からシステム監査基準やチェックリスト、ガイドライン等が公表されている。しかし、これらの監査対象範囲は、各省庁が自ら直接所轄する範囲に限定されている。例えば、通産省の監査基準では人/コンピュータによるエラー/事故に重点が置かれているのに対して、郵政省の基準では通信回線のエラー/事故に、自治省の基準ではプライバシー保護に重点が置かれている。結局、個々の監査基準は、システム監査の範疇のうち、偏った一部をカバーしているにすぎない。

したがって、ある業務について監査を実施しようとする場合には、複数の基準等を比較検討し、その上で、監査対象に適合するような自社なりのチェックリストやガイドラインを作成する必要がある。

(4) 監査ノウハウの蓄積不足

文献や監査基準の多くは、内部統制を目的別/対象範囲別に分類し、それに基づく一般論としての監査用チェックリストを示したり、概念的な監査手順を述べている。しかし、個々の企業、個々の業務における内部統制の現状を具体的にどう調査するのか、また、理想的な内部統制を設定するためには何に留意し、どのように具体化すればよいのかまでは、ほとんど言及していない。

また、文献や監査基準、チェックリスト等は、その作成過程では、専門家による様々な検討が加えられ、意味付けされていたのであろうが、最終的に成文化されたものは、抽象的な結論(一般論)だけになってしまふ場合が多い。したがって、行間を読み取るのが非常に重要である。例えば、チェックリストに「～を検証する」とあっても、なぜその検証が必要なのか、何をどう調べればよいのかが分からなくては、チェッ

クリスト作成者の意図を実務に活用できない。

現時点では、基準のどこからどのような項目を持ってきて、どのような手法で検証すればいいか、その検証の際の重点項目は何か等の実務的な部分は、すべてを監査人個人の経験やノウハウに頼っており、監査人の人材不足、養成の難しさの大きな原因となっている。

(5) 監査手法やツールの不足

現時点では、システム監査に特有の作業、つまり内部統制の設定や検証、監査人による監査計画立案から立入り検査、報告書作成までの作業全体を一貫して支援できる実用的な手法や方法論が存在しない。

現在、システム監査の手法とよばれているものは、開発管理やテスト支援のための手法やツールを利用しているのが実状である。最近注目されている『汎用監査ツール(ソフトウェア)』も、媒体/形式が異なるファイルやデータベースをひとつのソフトウェアでアクセスできる、統計的サンプリングができる、といったデータ抽出ツール程度のもものがほとんどである。これらのツールや手法は、システム開発の専門家にしか使いこなせない場合が多く、また、監査という目的から見ると、実務上満足できる水準に達していない。

監査手法として、例えば、チェックリストの作成作業をとっても、そこに記載された項目にもれやムダがないか等を検証する手立てが必要である。また、たとえ適切なチェックリストがあったとしても、リストの各項目ごとに、何を、どう調査し、その結果をどう判断すればよいのかが不明確では困る。リストにただ『○』や『×』だけを書き込めばよいわけではなからうし、その結果をどう分析して改善案に結びつけていけばよいかについて、なんらかの指針がほしい。

4. 統制マトリックス法の提案

著者らは、前章で述べたシステム監査の問題点を解決し、システム監査の導入・実施を円滑に行うためには、内部統制の一層の整備とその文書化を進めることが第一歩であると考えます。

本章で提案する「統制マトリックス法」は、広義のシステム監査の一部として、内部統計の設定や文書化、分析を行うための手法である。

4.1 統制マトリックスの枠組み

統制マトリックス法は、一言でいうと、システム監査に関する知識やノウハウを整理し、監査実務に活用するための枠組みである。具体的には、統制マトリッ

クスとよぶ二次元の表形式のワークシートを用いて、
観点… 監査（内部統制）上の着眼点（内部統制によって達成すべき望ましい状態）、
局面… 業務の状態（業務の流れを細かい作業単位に分割したもの）、

の二つの断面から、ある業務に対する内部統制を分類整理し、このマトリックスを用いて、システムに対して十分な内部統制が設定されているかを分析したり、内部統制が確実に実施されているかを監査したりする。

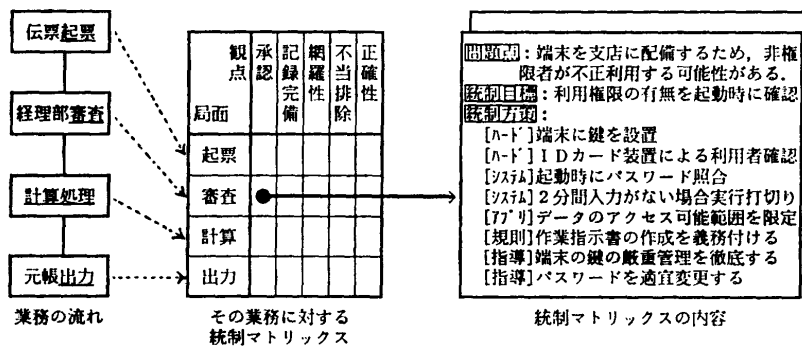
ここで、二次元のマトリックス形式を用いているのは、①業務における単位作業のそれぞれについて、複数の観点から総合的に検証する必要があること、②業務の流れ（手順）を考慮することによって、管理のめれや冗長性を検出しやすくすること等の理由による。

例えば、ある業務に対して内部統制を設定する際には、局面として、まず、業務の流れに沿って、単位作業を列挙する。次に、局面ごとに、そこで実施すべき内部統制を、

- ① 統制目的（達成すべき状態／避けるべき状態）、
- ② 統制点（何をどう管理するかの手針）、
- ③ 統制内容（具体的な規則、手法、ツール等）、
- ④ 費用対効果（ある技法や手法を実施する費用と、それによって期待できる効果）

等を一組とした箇条書きで書き込む。ほとんどの場合は、ある観点、ある局面について、複数の統制項目が設定されるので、マトリックスのひとつの箱に対してこの①～④の組が複数組存在することになる。

図2に統制マトリックスの例を示す。これは、簡単な経理業務をマトリックスで表したものである。



注) ここでは、ペーパーレス会計システムの中で、「伝票の画面審査（画面に表示された伝票データを見て審査し、承認／差戻しの判定を入力する）」という作業について、オンライン端末を本支店の主管部門に設置した場合に、不正利用を防止するための内部統制について論じている。

図2 統制マトリックスの概念
 Fig. 2 Concept of control matrix.

4.2 統制マトリックスにおける観点

システム開発者や利用者部門の管理者が業務に対して内部統制を設定したり、システム監査人が業務を監査する際には、様々な視点から業務に対する統制の充足度を検証する必要がある。ここで、内部統制の基本は、正当な権限を持った作業（ないしソフトウェア）だけが、正しい入力だけを対象に、正確に処理を行い、結果の出力を定められたとおりに利用すること、そして、誰が、いつ、何をを行ったかをきちんと記録しておくこと（これを監査証跡という）である。

そこで、統制マトリックス法では、内部統制を、5種類の『観点』、すなわち、

- 承認… データや処理内容が承認をうけているか（処理権限、検閲等）
- 記録… データや処理履歴が完全かつ正確に記録されているか（証跡、バックアップ等）
- 網羅性… 処理すべきデータをもれなく迅速に処理しているか（紛失／遅延防止等）
- 不当排除… 不当なデータを処理したり、権限のない者が処理していないか（不正、重複処理等）
- 正確性… 処理内容に誤りはないか（処理結果の正確性、処理時期の適時性等）

という分類基準によって分類整理する。ただし、各観点は互いに完全に独立ではなく、一つの内部統制事項が複数の観点到属するという場合もある。

これらの観定の相互関係を図式化すると図3のとおりであり、業務に対する内部統制の分類基準としては、この5種類で十分であるといえる。さらに細かい分類が必要ならば、各観点を細分化して中分類、小分類

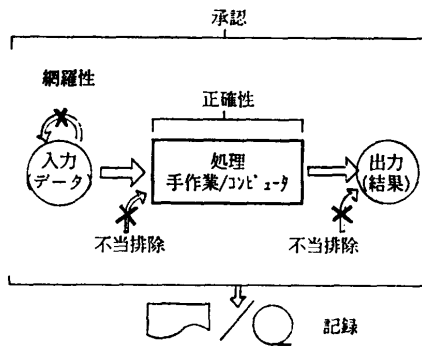


図3 五つの観点の相互関係

Fig. 3 Relationship among five viewpoints of internal controls.

類を設けてもよいが、あまり細分化しすぎると、表が複雑になる上、分類作業自体にノウハウが必要になり、分類にかなりの労力を費やす必要が生じてしまう。

業務に対する内部統制をこのように観点別に分類整理することによって、システム監査に関する知識やノウハウを利用しやすい形で蓄積することができる。また、実際の監査実務においても、観点別に検討を行うことによって、蓄えられた知識を有効に活用できるし、検討もれや統制/監査内容の偏りを検出・防止するためにも有効である。

4.3 統制マトリックスにおける局面

統制マトリックスでは、業務処理の手順を、『局面』とよぶプロセスに分割し、業務全体を局面の流れとして捉えるプロセスフローアプローチをとっている。

局面としては、あらかじめ、起票、データ入力、データ編集(更新)、書面審査、画面審査、磁気記録保存管理、書類保存管理、帳票出力、帳票配付、書類回付、データ通信、データ検索、データ突合わせ、データ消込み、データ抽出分類、計算処理、という典型的な作業項目を定めており、実際に業務フローを作成する際には、これら既定の局面を組み合わせる形で作成する。

ここであらかじめ局面の種類を限定しているのは、それによって、知識蓄積の段階で、観点別だけでなく、局面(作業内容)別にも知識整理を行うことが可能になり、知識の可用性が増すことと、局面分割の可能性を限定することによって誰が書いても同じようなフロー図になるというプロダクトの質的均一化が期待できること、の二点の理由による。著者らが経験した適用事例では局面の種類は、上に挙げた16種類で十分であったが、システムの対象分野によっては種類の

追加が必要になる可能性もある。

4.4 統制マトリックス法における内部統制の方策の分類

内部統制は、規則や手順等の形で業務処理手続きの中に組み込まれるが、その有効性は、それが『必ず』、『完全に』実施されるかどうかにかかっている。

そこで、統制マトリックス法では、統制方策が確実に実施されるか、結果的に有効に機能する確率が高いか、という視点から、統制方策を次の5段階に分類することとした。

[ハード]: ハードウェアによる統制。

端末機の鍵等、物理的手法によるもの。

[システム]: システム・ソフトウェアによる統制。

本人確認・利用記録等、OSやアクセス管理システム等のシステムソフトウェアによるもの。

[アプリ]: アプリケーションソフトウェアによる統制。

エラーチェックや確認メッセージ等アプリケーションソフトウェア(業務システム等)の中に自前で機能を組み込むもの。

[規則]: 明文化された規則や手続きによる統制。

人手で行う管理のうち、各種の規則、規程、職務分掌等による明文化された規定があるもの。

[指導]: 明文化されていない規則や手続きによる統制。

人手で行う管理のうち、明文化されておらず、業務指導や個々の管理者の判断、担当者の誠意に委ねられているもの。

これらのうちでは、[ハード]の区分の統制方策が、実施の確実性が最も高く、望ましい。以下、[システム]、[アプリ]、[規則]、[指導]の順に、その実施の確実性が低下する。また、各レベルの特徴として、①[システム]レベルの統制は、出来合いのソフトウェアを導入すれば実施できるが、内容的に画一化されやすい、②[アプリ]レベルのものは、組み込みに手間が掛かるが、きめ細かな統制が可能である、③[規則]レベルや[指導]レベルのものは、管理者個人の管理方針によって効果のばらつきが大きい等があげられる。

4.5 統制マトリックスの全体構成

統制マトリックスとは、横方向に5種類の観点に対

応する列が並び、縦方向に局面別の行が並んだ二次元の表形式のワークシートである。したがって、ある局面についてマトリックスを横に眺めると、5種類の観点別に分類された内容が一覧できる。一方、ある観点についてマトリックスを縦に眺めると、業務の流れの中で、ある特定の観点からの管理はどうかが一覧できる。

5. 統制マトリックスの利用方法

統制マトリックスは、まず、文献等の知識やノウハウを分類整理するための知識整理用ワークシートとして使える。これを『汎用統制マトリックス』とよぶ。

さらに、システム監査人や統制設計者の実務においては、業務に設定されている現行の統制を分析整理し、リスクや問題点を徹底的に分析するための分析用ワークシートとしての使い方、新たな統制を設定するための設計・検証用ワークシートとしての使い方等がある。これらの使い方をするためのマトリックスを、『実務用統制マトリックス』とよぶ。

実務用統制マトリックスを作成するには、まず対象業務の局面フロー図を作成して、これをマトリックスの縦軸とし、次に汎用統制マトリックスの中から、同じ局面／観点の要素を引用／加工しながら書き込んでいけばよい。この作業は、作業者の経験の有無にあまり影響されず、ある程度高い生産性と品質が保証できる。

以下では、統制マトリックスの具体的な利用方法を4種類示す。

5.1 監査に関する知識整理の枠組みとして

諸文献や実験経験者から得た専門知識や細かいノウハウを、観点・局面別に分類して汎用統制マトリックスに登録することによって、体系的に整理蓄積できる。また、監査基準書等に一般論として書かれている知識を、観点や局面別に分析し直すことによって、実務に応用しやすい形に変えることができる(図4)。

実際、監査の専門家のノウハウのうち、最も重要であり、かつ難しいのは、文献等に一般論として書かれた知識をどの局面でどのように利用すればよいかという部分である。

統制マトリックスを用いれば、専門家のノウハウを他人が利用しやすい形で蓄積できるため、実務中の利用だけ

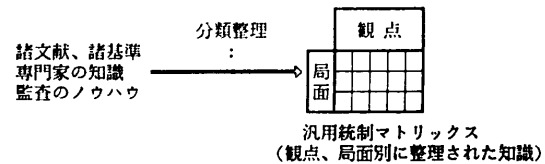


図4 統制マトリックスの利用例-1(知識の蓄積)
Fig. 4 Example of control matrix usage (1):
Classifying auditing/control knowledge.

でなく、監査人相互の情報交換や、監査人の養成にも有効である。

5.2 業務統制手続きを新設する際の道具として

ある業務に対して新たに統制手続きを設定する場合には、まず、業務の流れを局面モデル化し、汎用統制マトリックスを参考にしながら、各局面に対する内部統制を設定して、その業務専用の実務用統制マトリックスを作成する(図5)。

この過程では、この業務固有のリスクや運用上の問題点が洗い出されるが、それらがマトリックスの形で整理して保存しておけば、将来、業務を取り巻く環境や業務自体の順に変更が生じた場合に、その業務に対する内部統制についての設計者の意図を伝えるための貴重な資料となる。従来は、変更が繰り返される過程で統制の当初の主旨が徹底せず、効果が薄められてしまうケースが多々見られたが、このような手順をとればその心配をする必要がなくなる。

5.3 業務変更によって業務統制手続きを改定する際の道具として

ある業務の手続き等を一部変更したりする際には、まず現行の業務について統制マトリックスを作成する。次に、変更後の業務手順において統制手続きとその効果がどう変わるかをマトリックスに書き加える。そして、マトリックス上で、業務手続きの変更による統制面への影響を評価し、新たな統制手続きを設定す

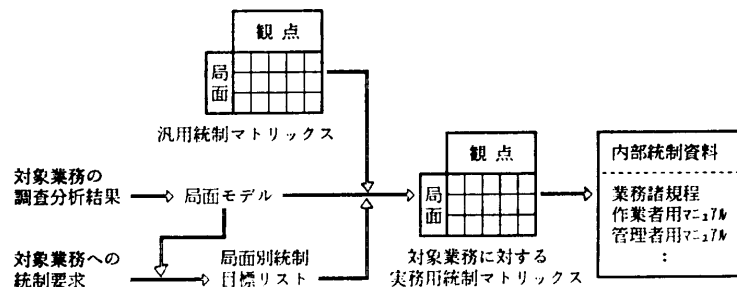


図5 統制マトリックスの利用例-2(統制手続きの新規設定)
Fig. 5 Example of control matrix usage (2):
Designing internal controls.

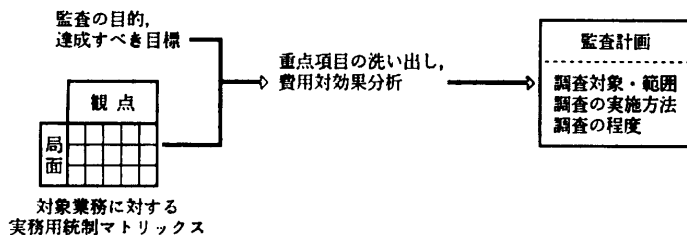


図 6 統制マトリックスの利用例-4 (監査の計画・実施)

Fig. 6 Example of control matrix usage (4):
Making auditing plan.

る。

最初に現状の統制マトリックスを作る段階で、現行の統制手続きを設定した際のマトリックスが残っていれば、作業が非常に簡単になる。また、変更のたびにマトリックスを蓄積しておき、それらを適宜遡って比較検討するように義務付けておけば、何度かのシステム改造によって統制もれが生じるという潜在的なリスク発生への心配も少なくてすむ。

5.4 監査を計画・実施するときの道具として

ある業務を監査する際には、その業務に対して設定されている統制手続きを調べ、調査分析すべき対象や、調査の方法、程度等を決定しなければならない。

この際に、その業務に対する統制マトリックスが用意してあれば、監査対象に対する事前調査の手間が大幅に省力化できる。また、監査用のチェックリスト等を統制マトリックスの形式でまとめておけば、縦横の比較検討等を通じて監査結果を多面的に分析することが容易にできる (図 6)。

6. 統制マトリックスについての検討

統制マトリックス法の適用事例としては、ある会社が情報システムを再構築するに当たり、要件定義の段階でシステム監査の立場から運用時の内部統制を検証、充実させるために適用した²⁾。これは前出の 5.2~5.3 節の用途に相当する。この場合には、利用者に、従来行っていた内部統制をマトリックス形式で整理、文書化してもらい、それをもとに開発側が加わって統制方策の検討と見直しを行った。また、会計システムのペーパーレス化に当たって、複数の処理方式が候補に挙がったので、各方式での誤処理や不正の防止方策をマトリックスで整理したところ、比較検討の焦点が明確になった。

これらの検討過程で作成された実務用統制マトリックスは、今後システム改造時やシステム監査実施時に

活用する予定である。

この事例を踏まえて統制マトリックス法の特徴を整理すると、以下のとおりである。

(1) 統制マトリックスを使うと、特定の観点と局面のもとでの統制の目的、望ましい状態、統制の方法等を考えることになり、論点や内容を現実的に表現できる。また、作成者だけでなく、マトリックスを利用する者にとっても、イメージがわかりやす

く、分かりやすい。

(2) システム監査に関する知識や実務上のノウハウは、現実問題の特殊な局面で考慮すべき注意事項や、様々な例外的事情等が多い。統制マトリックスを使えば、これらをうまく整理することができる。

(3) 各統制項目 (目的や方策等) を、いつ (局面)、なぜ (観点) 行うのかが明確に表現できる。このため、ある統制方策の位置付けが明確になり、システムや業務規則を変更する影響が把握しやすい。

(4) ひとつの局面に対して、複数の観点から検討を加えるので、統制もれの発生を防止/最小化しやすい。さらに、前後の局面との対比によって、ある局面での統制の重要度や効果等が容易に評価できる。

(5) 一方、統制マトリックスを縦横に対比・分析することによって、ある業務全体に対する統制の整合性を巨視的視野で吟味することができる。

(6) 統制のもれやムダは、新しい情報システムの導入や、組織変更、職務分掌の変更等によって発生する機会が多い。これらの変更の際に、新旧業務手続きの統制マトリックスを作成して検討することにより、もれやムダの発生が最少化できる。

(7) 汎用統制マトリックスは、最初から完璧なものである必要はない。とりあえずできるだけ詳しいマトリックスを作っておき、実績を重ねていく過程で、知識を逐次付け加えて充実させていけばよい。

7. おわりに

システム監査に関しては、全体的傾向として、理論的基盤、実務的基盤ともに未だ脆弱である。システム監査を普及するためには、システム監査の理論を体系的に整理する研究を進めるとともに、経験者の実務ノウハウを活かした手法やツールを開発し、さらに監査人を養成するための手立てを考える必要がある。

本論文で述べた統制マトリックス法は、このための

一手法であるが、今後は、以下のような点についてさらに研究を進めていく予定である。

- (1) 統制マトリックス法を多くの事例に適用し、実用可能性の評価と改良に努める。
- (2) 現在は、主に運用時の内部統制を対象にしているが、今後は企画・開発業務の統制へと広がっていく。
- (3) 監査や統制コストをできるだけ抑えるためにも、システム監査の実務を支援するツールを開発する。
- (4) 現在のシステム監査は、欧米の企業風土を基調にした部分が多い。わが国にシステム監査を定着させるために、組織としての行動を重視する日本の社会慣行に適合した監査・統制方法を、さらに検討していく。

参 考 文 献

- 1) 青山監査法人システム監査部(編): 高度情報化時代のシステム監査の方法, 中央経済社, 東京(1984).
- 2) 高橋光裕, 坂内広蔵: ペーパーレス会計システムにおける運用統制方策の検討, 電力中央研究所依頼研究報告, Y87502 (1988).
- 3) 通商産業省機械情報産業局(監修): システム監査白書 1989, コンピュータ・エージ社, 東京(1989).
- 4) 通商産業省機械情報産業局(監修): システム監査基準解説書, 日本情報処理開発協会, 東京(1985).

5) (米国) 内部監査人協会: 「システムの可監査性および統制の研究」報告書(日本語版), Vol. 1: 総括報告, Vol. 2: データ処理統制の実態報告, Vol. 3: データ処理監査の実態報告, 日本 IBM (1978).

6) 日本情報処理開発協会: 「わが国におけるシステム監査の現状—システム監査普及状況調査結果—」, 01-R 018 (1990).

(平成2年12月13日受付)

(平成3年9月12日採録)



高橋 光裕 (正会員)

1959年生。1983年慶應義塾大学工学部管理工学科卒業。1985年同大学院修士課程修了。同年(財)電力中央研究所入所。現在に至る。ソフトウェア開発の見積り予測技術、システム監査の研究に従事。ソフトウェア科学会会員。



坂内 広蔵 (正会員)

1948年生。1972年東京工業大学応用物理学科卒業。1974年同大学院修士課程修了。同年(財)電力中央研究所入所。ソフトウェアテスト、保守、開発技法の研究に従事。現在同所知識処理研究室長。1983年8月から1年半 University of California, Berkeley 校客員研究員。日本OR学会, IEEE 各会員。