経営情報と情報システム監査

菊池 豊彦*

1993年に入り、コンピュータ業界のトップ達は一斉に「今年はソフトウェアとサービスの時代」と宣言した。ソフトウェアとサービスを企業化する、あるいはビジネスにすると言う目標は正しい。しかしその内容は時代遅れである。情報社会の現代では、「システムインテグレーションとシステム監査の時代」、すなわちシステム監査等を企業化しなければならない時代である。

そこで当論文ではまずシステム監査とは何かを解説している。次に、システム監査を実施する人材の育成方法を検討し、その育成内容が実質的に経営情報学でのコアカリキュラム（専門学科で教えるべき最小限のカリキュラム）と等価である事を指摘するのがこの論文の趣旨である。

1．情報化社会とコンピュータセキュリテイ

情報システムのハードウエアやソフトウェア、およびその運用などの技術が急激に進歩してきた。それによって情報システムの適用分野が急速に拡大し、その適用内容も高度化している。それらに加えて社会的環境の変化等の相乗的な効果を含め、この十年内で本格的な情報社会が到来した。

この結果情報システムへの依存度が非常に高まる事になり、情報システムが正常に稼働している間はシステムからの恩恵を十分に受ける事が出来るが、いったん情報システムに異常が発生するとその影響は非常に大きなものになる。

特に集中処理の時代からネットワーク化による分散処理の時代に入る事により、システムの異常原因やそれによる影響が多様化、広域化、さらに複雑化する事になる。

この様に情報システムが多様化し高度化するに伴い、情報システムに関連する種種の脆弱性が顕著になってくる。その結果情報システムの利用に伴って発生する可能性のあるリスクとして大別して〝事故、災害〟、〝コンピュータ犯罪〟そして〝プライバシー侵害〟等があげられる。

情報システム監査が注目されている背景に、これらのリスクが現実のものとなり、種種の社会的混乱が引き起こされる事があげられる。そこで、まずこれらリスクの発生の歴史を若干説明する。

まず地震の例である。1978年6月に発生した宮城県沖地震では被害地域における多くの情報システムが影響を受けた。被害は、建物の崩壊によるコンピュータや関連設備などの転倒や位置ずれ(横すべり)が起きる等、大小さまざまであった。

それまでは、地震による被害が実際に情報システムにまで及ぶケースがなかったため我が国

* 東京情報大学助教授，システム監査技術者

1993年1月18日受理

は地震多発国でありながら、クチでは防災対策の確立が言われていても実際には十分にその整備が進んでいなかった。この宮城県沖地震の発生を契機として、物理的に安全性をチェックあるいは評価する為に通商産業省が1977年に公表した電子計算機システム安全対策基準（1984年に改訂）が大きくクローズアップされた。

その後1985年１月に公表された通商産業省の〝システム監査基準〟においても、この安全対策基準を活用するように〝注〟がつけられている。さらに1991年５月に通商産業省から全面的に改訂された電子計算機システム安全対策基準が公表された。

次は電話回線事故の例である。1984年11月東京都世田谷区で地下ケーブル埋設工事中に火災が発生し、電話回線８万９千回線、データ通信専用回線72回線そしてテレックスなど専用回線４千回線が不通となった。

重要性の高いものから順次回復させ事故から９日目に全面復旧したが、その間都市銀行のオンラインシステムが全面ストップし、大きな社会問題になった。

金融機関のオンラインバンキング、ＪＲの〝みどりの窓口〟、航空会社の座席予約システムなどは日常の社会生活に普及，浸透している。それらシステムへのわれわれの依存度を考えると、これらシステムに一旦障害やエラーなどが生じると大混乱になる。そうなると単に一つの企業、一つの地域だけの問題ではなく大きな社会不安の原因とも成り得るのである。

ところで、一般に〝コンピュータ犯罪〟とは、コンピュータが直接的あるいは間接的に何らかの形で介在した社会悪行為と定義されている。情報システム関連資産を狙った犯罪、金銭や物品を狙い、その為の手段としてコンピュータを利用する犯罪等がその主要な例である。社会的な影響を考えてか、コンピュータ犯罪を公表するケースは全世界にわたって非常に少ない。米国では1960年代に出現し、1970年代から増加したと言われている。日本では米国から10年遅れて、1970年代に出現し、1980年代に入って増加し始めている。公表されたコンピータ犯罪の中から幾つかの例を説明する。

まず、1973年に米国で発生したイクイティファンディング事件がある。これは会社ぐるみの詐欺事件である。ロサンゼルスのイクイティファンディング生命保険会社で、経営者および従業員の計23名が共謀して６万４千件の架空保険証券を偽造し、再保険として譲渡し資金を調達していた事件である。

６万４千件の保険証券を偽造するということは、それだけのニセの契約書を作る事であり、コンピュータを利用して始めて可能な事である。

一方国内に目を向けると、1981年にある都市銀行の支店のオンライン端末オペレーターの女子行員とその愛人が、あらかじめ設定した架空名義口座に１億８千万円のニセ入金操作を行い、現金５千万円小切手８千万円を引き出すと言った事件が発生している。さらに、1989年には地方銀行の支店で、支店長と支店長代理がオンラインシステムを役席キーでオフラインに切替え、ホストコンピュータと端末機を切り離して端末機の印字機能のみを使用し、約50億円にのぼる定期預金証書を偽造、発行していた事が発覚した。　他にも、情報システムの持つ特有な脆弱性として次のものが挙げられる。

(1)　情報システムを使った業務処理量が大幅に増加している。したがって短時間に膨大な業務量が処理されるので、たとえ短時間でもシステムにトラブルが発生すると膨大な量のデータが異常な状態に置かれる。その為対応が非常に難しくなる。

(2)　システムで処理する内容、数字や文字、音声および画像等の複合したマルチメディアの使用、処理する場所の広域化など情報処理方式が非常に多様化かつ複雑化している。従ってシステムに異常が発生する原因もまた多様化かつ複雑化してくるので、発生可能な原因を全て検討し、対応する事が非常に困難になってきている。

(3)　本格的な分散処理時代への突入により、データベースなどへのアクセスガシステムを設置している場所への侵入といった物理アクセス

によるよりも、大規模なネットワークを通しはるか遠隔地から全く自由に端末を通して、他人に知られる事無く行えるようになった。さらに国と国をまたがっての遠隔地からのアクセスが可能になった事から、その対応は非常に複雑でかつ難しくなって来ている

(4) プログラムやデータの記憶媒体の物理的特徴やその記憶方式は、これまでのものとは大きく異なっている。例えば磁気テープ、磁気ディスク等の記憶媒体には多量のデータやプログラムを記録する事が出来るから、これら媒体の運用管理は細心に実行し間違っても紛失や廃棄をしてはならない。

さらにこれら媒体への記録は電磁気の原理で行っているので、直接目で見る事が出来ない。したがってそれらの内容を消失させたり、変更させたり等を何一つ証拠を残さず実行できる。エラーによるにせよ、あるいは犯罪によるにせよこの種の行為を検出したり、その影響を取り除く事は困難な作業である。

(5) いろいろなソフトウェアツールの出現により特別な技術を持たなくても特定のデータ処理は実行出来るようになった。

それでも多くのデータ処理は、コンピュータ処理やアルゴリズム等の専門的な知識が必要であり、これら知識の無い人たちにとっては情報システムはブラックボックスそのものである。つまり情報システム内で専門家が行う事故や不正などを発見するのが困難である

(6) コンピュータが使用されていない時代の内部統制は、一般に職務の分離つまり組織化とそこに働く多数の人達の間での内部牽制機能で実現されてきた。しかし情報システムの導入およびその進化は、小人数でかつ職務の分離が十分になされていない組織で膨大なデータを多数の処理方式で処理出来る状況をつくってしまった。つまり内部牽制機能が、これまでのものとは異質になってきているのである。この状態に対応出来る方策が必要不可欠になってきている。

以上幾つかの脆弱性を挙げたが、システムのこれらの脆弱性が原因で発生する数々の脅威から情報システムを中心とした情報処理活動に関連する種種の資産を守る事をコンピュータセキュリティといっている。

2．情報システムの有効性と戦略性

情報が企業経営において非常に重要な役割を果たすようになっている。その結果、従来の人事管理、生産管理、財務管理などの管理分野と並んで、情報を資源として管理する〝情報資源管理〟という考え方が生まれた。現在では情報資源管理が非常に重要性を持つようになってきている。その背景には、社会の情報化が存在している。

この社会の情報化は当然、現代社会の大きなトレンドとかかわりを持つものである。例えば一橋大学商学部の宮川公男先生の考え方に依れば、現代の大きなトレンドは次に説明する幾つかのキーワードで示され、これらのキーワードが全て社会の情報化の原因となっているのである。

(1) 変化の加速化

東京、ニューヨーク、そしてロンドンと言った世界市場での、例えば円相場がラジオやテレビを通して時時刻刻放送されるくらい、相場の変化の振幅が大きくなってきている。またワープロの新製品の寿命がたった3か月程度といったように、技術の進歩も非常に大きく変化している。

この様に、円相場は絶えず変化しているし、ワープロも絶えずモデルチェンジしている。それらの変化の加速化は、当然それらの情報の価値を増加させることになる。

(2) 経済、社会の成熟化

社会が豊かになるにつれて消費者のニーズも多様化あるいは個性化してきている。従ってこれら多様性あるいは個別性を明確に区別するための情報が必要とされる。

さらに成熟化の1つの例として耐久消費財の需要を見るとほとんど新規需要ではなく買い替え需要が主体となっている。買い替え需要のほ

うが、むしろ消費者のニーズが多様であり個性的になっているといえよう。この様に、社会の成熟化に伴って大幅な変化が生じる事になる。従ってそれらの変化を知るための情報に対するニーズが大幅に高まることになる。

(3) 相互依存の複雑化

例えば、全く異なった業種の企業が新たに市場に参入すると言った様に、あらゆる業界で業種の壁が低くなったり消滅したりしている。この様に今までは無関係であったものが関係を持つ事になると、そのものについての情報が必要になる。更にこれらの相互依存の関係が複雑になればなるほどその要素である相互依存関係に関する情報がますます必要となる。

(4) 国際化

情報技術と通信技術の結合に依って、いろいろな情報が地球的規模で伝達出来る様になってきた。当然、情報の価値も増大する事になる。

以上の様に、社会のトレンドに従って情報化が進むにつれてコンピュータの設置台数が大幅に増加すると共に通信サブシステムによるネットワークが充実し、その結果各々の情報システムが巨大化していくことになる。

この事は情報システムへの投資がどんどん巨大化する事を意味する。従ってシステム資源の有効利用やコスト対パフォーマンスの向上等を積極的に推し進める必要がある。つまり情報システムの効率性や有効性の確保が強く要請されるようになった。

当初、情報システムは人員削減や経費削減などの〝コスト削減〟のための道具として広く活用されてきた。従って情報システムを導入する事により、いくらコストダウン出来るかが最大の目標であった。

やがて情報システムは非定常業務にも使用される事になり、その結果効果的な意思決定の促進や機会損失の極小化などの〝収益の増加〟にも役立つ道具として活用されるようになった。

この様に情報システム構築の目標が変化する間に、情報処理技術や通信技術そして情報システムによる社会基盤の整備等が大きく進展した。特に半導体つまりＬＳＩの実用化によるパソコンやワークステーションの普及、デジタル通信の実用化に伴うコンピュータネットワークの整備等により社会の情報化が急激に実現した。

この様にしてやがて情報システムを企業競争の重要な手段として使い、競合他社に対して優位を確立しようとする目的が設定されるようになった。企業の〝経営戦略の情報化〟としての情報システムの使用である。

戦略情報システム (Strategic Information System) とは、社会の情報化に伴う市場環境の変化に対応し、さらに市場競争の一層の激化に打ち勝つ為のシステムである。競争優位に立つ為の経営戦略の具体化、更に種種の情報技術でそれら経営戦略を情報戦略として具体化し、最後にそれらを情報システムとして開発し、運用するのである。

従って戦略情報システムでは、与えられた経営戦略をその時点でのいろいろな最新の情報技術を用いて如何に忠実に情報戦略として具体化しているかが最大のポイントである。この様に現代では、営業活動を有利に展開出来る事を意図した情報システム、つまり〝有効性〟と〝戦略性〟を重視した情報システムが注目をあびている。

最後に現代の情報システムに要求される５種類の機能を、これまでのまとめとして要約する。まず情報システムは自己の持つ種種の脆弱性が原因で発生するであろう障害、事故、エラー、ミスそして犯罪等に対応出来る機能を備えていなければならない。これは、情報システムの持つ〝信頼性〟および〝安全性〟に関する機能である。

次に情報システムがコストや費用の削減にどのくらい役立っているか、また収益の増加にどのくらい貢献しているかを示すのが情報システムの持つ〝効率性〟および〝有効性〟に関する機能である。

最後に情報システムが経営戦略を如何に情報

戦略に具体化しているかを示すのが〝戦略性〟である。

3．通産省〝システム監査基準〟の趣旨

現在のシステム監査基準は、1985年11月に通商産業省が公表したものである。その目的は、同基準の趣旨のところで次の様に説明されている。つまり、

〝情報化の進展に伴い、すでに経済、社会の多くの分野がコンピュータシステムに大きく依存する状況に至っている。また情報処理技術と通信技術の発達やその結合よるネットワーク化の展開により、情報化は今後さらに広範にかつ深く浸透していくものと考えられる。その結果、システムが停止、悪用あるいは有効に機能しなくなった場合には、組織体の経営活動に支障をきたすことはもちろんのこと、国民生活全般にも影響を及ぼす恐れがある。したがって、コンピュータシステムの信頼性、安全性、効率性を確保し、情報化基盤を整備することは、今後わが国が健全な情報化社会を構築していくうえで必要不可欠な課題といえる。〟

以上からシステム監査は、情報システムの信頼性、安全性、効率性を高め、情報化社会の健全化に資する事を目的にしている。

現実には単一の情報システムが監査対象であるので、これらの目的は密接に関連しており、全く独立的なものではないが、信頼性、安全性、および効率性の定義は、〝システム監査基準解説書〟によると次の通りである。

(1) 信頼性を高める
・システムの品質を高める事
・エラー、事故の発生を未然に防止する事
・万一エラーや事故が発生した場合には、影響を最小限にくい止め、迅速に回復する事

(2) 安全性を高める
・自然災害からシステムを保護する事
・不正アクセスや破壊行為からシステムを保護する事

(3) 効率性を高める
・システム資源を最大限に活用する事
・コスト対パフォーマンスの向上を図る事

そして、1990年代になって社会の急激な情報化に伴い、システム監査の目的もさらに次の2項目が実質的に加えられている。

(4) 有効性を高める
・組織体の収益の増加に寄与する事

(5) 戦略性を高める
・経営戦略を情報戦略として具体化する事。さらにシステム監査そのものの定義もやはり同じ趣旨により次の様に説明されている。つまり、

〝システム監査は、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実効性の担保およびシステムの有効性を図る上で、効果的手段と考えられる。〟

まず監査とは、監査検査もしくは観察審査の略と考えられ、英語ではＡＵＤＩＴと言い、独立かつ客観的な立場で、特定の目的のための調査、分析を行い、その結果について意見を表明する事である。この一般的な定義を参考にして前述の趣旨のポイントをまとめると、次の4点になる。

(1) 監査の独立性の確保

情報システムに関係する人が自ら情報シテスムおよび関連業務に付いて、例え一般の監査手続きと同様の精緻な方法で実施しても、それはシステム監査とは言えない。監査が本来的に持つ特性としての〝監査対象から独立した客観的立場〟から行われる必要がある。ここでは独立した第三者をシステム監査人と名付けている。

(2) 情報システムの総合的点検、評価

監査の対象とするシステムは、電子計算機を中核とする情報システムである。そして、システムへの入力データの作成から処理、記憶、伝送、出力情報の利用までの関連業務が全て対象となる。したがって情報部門の業務にとどまらず、データ作成、情報を利用するユーザー部門の関連業

務も含むのである。

ともかく、ある目的を遂行するために構成される情報機能を、システムと言う視点から全体にわたって点検、評価するものである。

(3) 関係者への助言、勧告

点検、評価の結果を監査報告書にまとめて、関係者全員に対して監査対象となった情報システムの全体的状況と問題点を明快に知らせ、問題点の改善の為の助言や勧告を行う。

監査報告書の提出をもって終了するのではなく、報告書に記載した改善の為の助言や勧告を実現させるためのフォローアップ体制を整備して、改善の円滑な推進を図るのもシステム監査人の任務である。

(4) セキュリティ対策の実効性の担保とシステムの有効活用の促進

〝実効性の担保〟とは、企画、開発中の情報システムのセキュリティ対策が十分に妥当のものであるか否か、また運用中の情報システムのセキュリティ対策の程度およびその実効性について点検、評価し妥当と認められない時は、システムの信頼性と安全性の向上の為の策定を行う。

又、〝有効活用の促進〟とは、情報システム化の目的の達成度合いについて点検、評価し、妥当と認められない場合は改善、勧告する。

ところで、〝情報システム監査基準〟は、情報システムを監査する為のガイドラインであり、監査に当たっての必要事項を網羅的に示したものである。

システム監査基準は次の3章から構成されている。まず、〝一般基準〟であり、システム監査おいて基本となる目的、対象、システム監査人、監査時期、監査計画および監査手順などのシステム監査の総括的事項を記述している。次に、〝実施基準〟であり、システム監査人が監査を行うに当たっての観点と内容について定めたもので、監査基準の中核の章である。最後は、〝報告基準〟であり、システム監査結果を取りまとめるに当たっての必要な事項および監査結果に基づく処置について定めた章である。

4．監査の概要

監査の一般的知識を得る為に、ここでその概要を説明する。

(1) 監査の種類

監査は、その内容、主体、法的規制、そして内部・外部等の視点から分類される、

(ア) 監査内容による分類

・会計監査――会計処理および会計記録の信頼性、正確性などを高める為に、独立した第3者がその適否を点検、評価し意見を表明する。
・業務監査――業務活動において、資源の有効利用、経営方針や経営計画への準拠性、その他業務処理の信頼性、安全性、効率性などの観点から点検、評価し、意見を表明する
・経営監査――経営管理の組織・制度・運営などについて、その準拠性、合法性そして経営能率度の観点から点検、評価し意見を表明する。

(イ) 監査主体による分類

・公認会計士監査――商法および証券取引法に基づき、財務諸表が法令や定款に従って適切に作成されているか否かを、処理の妥当性をふまえ、外部の利害関係者の為にその信頼性を監査。
・監査役監査――商法に基づいて監査役が取締役の職務の執行を監査すると共に、営業の報告を求め会社の業務や財産状況を監査、つまり会計監査と業務監査を行う。
・内部監査人監査――監査役とは異なり、監査部や検査部等の部門に属する専門スタッフにより、経営者や管理者の為に会計業務および業務活動全般を監査する事

(ウ) 法的規制による分類

・法定監査――公認会計士監査、監査役監査など法令の定めるところにより強制的に行う監査
・任意監査――内部監査人監査のように、企業

や組織体などの自由意思によって任意に行う監査

(ニ) 内部・外部による分類

・内部監査――企業や組織体内部において、独立的な立場の内部監査人が行う監査
・外部監査――公認会計士監査のように、組織外部の独立した人が監査主体となって行う監査

(2) システム監査の位置づけ

一般には〝システム監査人によりコンピュータを中核とする情報システムを監査対象とする内部監査であり、経営者や管理者の為に行われる任意監査である〟と理解されているが、次の様な位置づけも可能である。

・情報システムの企画、開発、運用という〝業務〟を対象としているから、システム監査は業務監査の範疇にはいる。
・会計監査や業務監査で監査対象になる会計処理、業務処理そして経営管理等がコンピュータ化されているならば、それらの対象は全てシステム監査の対象でもある。
・システム監査は、会計監査におけるＥＤＰシステム監査よりも広範囲の概念である。なお日本公認会計士協会でのＥＤＰシステム監査の定義は次の如くである。

〝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為システムに組みこ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有効性と妥当性を検討・評価する事〟

5．システム監査の実施手順

システム監査の実施手順は大別して、

(1) 計画段階
(2) 実施段階
(3) 報告段階

から成り立っている。各段階における具体的な内容は、対象としている組織体や情報システム毎に異なったものになる。ここでは、システム監査基準に従って説明する。

(1) 計画段階

計画段階は次の３ステップから成る。

・事前準備
・基本計画作成
・個別計画作成

・事前準備

あらかじめ内部統制の整備状況や実施状況、対象業務の内容、情報システム構成や対象部門の組織構成等の調査をして、次の各計画作成の為の情報を収集する。

・基本計画作成

基本計画書は、監査を効率的に実施しかつ監査の効果を高める為に作成される。すなわち、当該年度に実施すべきすべての監査対象の実行可能性を検証した後に基本計画を策定する。基本計画は、年間監査実行計画とも考えられ、次の項目を記載しなければならない。

－当該年度に実施する監査対象
－重点監査テーマ
－実施体制
－年間スケジュール

・個別計画作成

基本計画で示した個々の監査対象毎に、具体的な監査活動を示したものが個別計画になる。従って基本計画書で示した監査対象の個数だけ個別計画書が存在する。

個別計画はまさに実行計画そのものであるから、工数、費用、期間等監査を実施するにあたって必要とされる要件は、全て記述されていなければならず、次の項目が記載されなければならない。

－対象
－目的
－範囲および手続き
－時期および日程
－責任者および業務分担
－報告時期

又、具体的な監査時期として、一般基準では次の様に定めている。

・システムの企画、開発業務の監査は各業務の実施に即して適時行う事。
・運用業務の監査は一定の期間ごとに実施する事
・システムの大幅変更については、開発業務に準じて監査を行う事。

(2)　実施段階

次に、個別計画ごとに監査を実施する事になるが、監査精度および監査効率の向上のため一般基準で次のように監査手順を定めている。

〝システム監査は、個別計画に基づき
・予備調査
・本調査
・評価・結論
の手順により行う〟

・予備調査

システム監査の実施を効率的に行う為に、対象業務の実態を事前に把握するものである。事前に情報システムに関する内部統制の手続き、制度、規則等に関連する資料の提出を被監査部門に要求したり、自分でも収集する。さらに、質問書を被監査部門に提出して、必要事項を記入してもらい回収する。そして**内部統制が整備され、機能しているか**を評価する。

・本調査

監査目的に照らして、対象業務の実態を調査、分析、検討する。その方法としては、現地調査、意見聴取、そして監査技法の利用などがある。

具体的には、情報システムに関連する内部統制手続きがシステムの企画、開発、運用において十分に準拠されているか、また有効に機能しているかを証拠(監査証跡と言う)に基づいて検討する。これを**準拠性テスト**と言う。次に情報システムの処理結果の正確性、妥当性、信頼性などについて、準拠性の程度に応じて合理的な範囲で証拠を収集し、検討する。これを**実証性テスト**と言う。

(3)　報告段階

実施手順の最後のステップは評価・結論である。これは調査結果を踏まえて、対象業務の実態を監査目的に照らしあわせ妥当であるかどうか判断する事である。このステップで注目すべき点は、システム監査基準の報告基準として、その監査結果を報告書として取りまとめるように規定している事である。

さらに次に示すように正確、明瞭、簡潔、を目的として、その報告内容をも規定している。

・報告書には次の項目を記載する事
　監査責任者
　作成日
　対象
　目的
　範囲および手続き
　実施期間
　実施分担および分担者
　監査結果の概要
　　－信頼性の状況
　　－安全性の状況
　　－効率性の状況
　　－有効性の状況
　　－戦略性の状況
　指摘事項
　改善勧告
　　－緊急改善
　　－通常改善
・監査結果の概要にはシステムの信頼性、安全性、効率性、有効性、戦略性についての評価を記載すること
・指摘事項には、監査の結果に基づく問題点を記載すること
・改善勧告には、指摘事項に基づき重要と認められる改善事項を記載すること。また必要に応じた改善案を併記すること(なお、緊急改善とはシステムに重大な欠陥が生じており、そのまま放置出来ないと判断される事項であり、通常改善とは重大な欠陥ではないが、システムの改善が図れると判断される事項である)

ところでこの報告書は、個別計画毎に作成す

るとともに重大な過失や不正といった特別な場合を除き、事前に被監査部門との意見交換などを行い、その結果の十分な確認をする。しかる後に結論を下すように勧めている、 さらに、このようにまとめられた報告書は、報告書に基づく適切な処置を講ずる事ができる権限者に提出する。権限者は、報告書に記載されている改善事項を承認するならば、被監査部門に改善事項を実施するように指示する。

一方システム監査人は、自分が書いた報告書に記載された改善勧告を実現させる為の努力を払わなければならない。そして、被監査部門での改善事項の実施状況をフォローアップしなければならない。

6．システム監査と内部統制

システム監査は、情報システムに関連する内部統制が有効に整備され、正しく運用されているかを客観的立場から総合的に点検・評価するものである。

内部統制は具体的には、情報システムの信頼性、安全性、効率性、有効性、そして戦略性を確保したり、向上したりする為の企画業務、開発業務そして運用業務における組織、管理体制、業務方針、業務計画、種種な手続きや基準、マニュアルやドキュメンテーションおよびそれら業務の評価システムなどを全て包含したものである。

内部統制を機能面からみると、

(1). 予防牽制機能(不正や誤りなど、発生可能性のある行動や機会を事前に封じこませる手続きや方法

(2). 検知回復機能(不正や誤りなどの発生をすみやかに検出すると共に、回復のための処置をとらせる仕組みや機能)

等からなり、両機能は補完しあうことにより効果を発揮する。

この様な内部統制が十分に確立、整備されていればシステム監査として、

(1). これらの内部統制を如何に尊守しているか、

(2). 処理結果は妥当か、

などの検討に焦点がしぼられ、システム監査は、効率的かつ容易に実施出来る。

したがって、「システム監査人は、内部統制組織の信頼性の程度を勘案して〝試査〟の範囲を合理的に決定しなければならない」事になる。ここで、〝試査〟は記録や事実の一部を抜き取り検査によって全体の信頼性、妥当性を推定する監査技術である。これは全部の資料を検査して全体の信頼性、妥当性を立証する〝精査〟に対応するものである。現代の監査は、対象が余りにも複雑化したため全ての監査資料を〝精査〟する事が時間、コスト的に見合わないという認識のもとに、内部統制組織の程度を前提にして〝試査〟の範囲を決めて実施される。

ところで、情報システムに内部統制が必要である理由は、情報システムの持つ次の主要な特性に依っている。

(1). 情報システムの企画、開発、運用などの業務は、種種多様な技術の組み合わせで成り立っており、各業務間、各工程間を通じて一貫した統制、標準化の下にシステムが開発され運用されなければならない。

(2). 情報システムの開発、運用を担当する部門では、技術レベル、経験年数などの異なる多数の要員により共同作業が行われる為、担当や責任範囲などを明確にし、また属人的にならない様に手法を標準化し、統一しておく必要がある。

(3). 開発業務は、プロジェクト制で進められる事が多いが、一時的に編成され開発終了後は解散されるので、プロジェクト管理、システムの品質管理、標準化、文書化などが明確に規定され、周知徹底されなければならない。

(4). 情報の蓄積および処理機能が特定の場所や人に集中し易いので、その対策が必要である。

(5). コンピュータ化されると共に、監査証跡が失われ易くなりまた従来の手作業ベースとする内部統制手続きがプログラムに集中化する傾向がある。

(6). 物理的、空間的に離れた場所から情報の入出力が可能の為、手作業ではありえなかった情報の改ざんや不正アクセス、あるいは操作ミスや

故障などが発生する可能性が高い。
(7). 処理手続きや統制手続きなどの実施が記録として残らない場合がある。
(8). 何一つ証拠を残さずにに不正を遂行しうる可能性があると共に、解読出来ない形で多くの情報が記録、保管される。
(9). 人間の介在が減少するため、誤りに気づかないまま大量のデータを処理する危険性がある。

最後に、これらのシステムの特性に対応した内部統制の一般例を次に示す（これら内部統制を点検・評価するのがシステム監査である)。

・組織、権限に関する規定
　－組織・業務規定（組織図を含）
　－職務権限規定
・企画に関する規定
　－計画書作成、承認、変更に関するマニュアル
　－種種設備、ハードウェアやソフトウェア等の購入、導入規定
　－ユーザー調査規定
・開発に関する規定
　－開発手順、開発マニュアル
　－システム設計マニュアル
　－プログラム設計マニュアル
　－プログラミングマニュアル
　－テストマニュアル
　－開発用機器使用マニュアル
　－プロジェクト管理マニュアル
・運用に関する規定
　－操作手順書作成、修正、使用マニュアル
　－障害対策マニュアル
　－システム保守規定
　－入退室管理規定
　－ユーザーマニュアル
・文書、ソフトウェアに関する規定
　－プログラム登録、管理規定
　－データ保管、管理規定
　－一般文書保管規定
　－機密保護マニュアル
　－システム機器使用状況報告書マニュアル
・外注に関する規定
　－外注委託規定
　－外注管理規定
　－検収条件規定
　－進捗、セキュリティ等管理規定
・標準化に関する規定
　－入出力レイアウト
　－画面レイアウト
　－コード、ファイル設計
　－プログラム作成作業標準化規定
　－システム操作手順標準化規定

等。

7．情報経営学とシステム監査人育成カリキュラム

システム監査人としては、つぎの知識・能力を持っている人を就かせる必要がある。
(1). システムの企画・開発に関する知識
(2). システムの運用に関する知識
(3). 監査に関する能力
(4). システム監査実施に当たっての関連知識

その上、システム監査の実施を円滑に進めその結果の信頼性を高めるために、監査の実施や評価に当たっては常に公正不偏の態度を保持し、かつ特に業務上知り得た事項に対して守秘義務を尊守すると言う高度な倫理感も要求される、又、システム監査の遂行には業務知識も当然の事として要求される。

他方、日本情報処理開発協会が発行した「システム監査Ｑ＆Ａ１10」によると、前述の内容をより具体的に次の様に説明している。

(1)　情報システムの構成、機能に関する知識。
　(ア) ハードウエア
　・コンピータアーキテクチャ
　・中央処理装置
　・外部記憶装置
　・入出力装置
　・通信制御装置
　(イ) ソフトウェア
　・オペレーティングシステム

・ファイル編成
・サービスプログラム
・応用プログラム
・プログラム言語の種類と特徴
・オンライン処理と伝送制御
(ウ) 情報処理システム
・システム処理パターン
・システム構成
・システム評価

(2) 情報処理システムの企画、開発及び運用に関する知識
(ア) 情報処理システム計画
・長期、短期計画の策定方法
・システム計画の内容
(イ) 調査・分析
・現状分析方法
・要求分析方法と要求定義法
・影響分析方法
(ウ) 開発の可能性
・開発資源の見積もり法
・開発体制組織
・効果の測定法
(エ) システム設計
・システム設計手順
・システム概要と詳細設計
・機能評価法
(オ) プログラム設計
・プログラム仕様
・プログラム手順と技法
・支援ツール
(カ) テスト
・テスト計画とテストデータ作成法
・テストの方法と手順
・テスト結果の評価法
(キ) システム操作
・操作体制
・操作手順
(ク) 入力データの作成
・作成手順
・入力データのチェックとエラー処理
(ケ) データやプログラムの管理
・取扱及び受け渡し方法
・保管及び廃棄方法
・変更、追加、削除の手順
(コ) ファシリティ管理
・入退室管理手順
・ファシリティの保守と監視
(サ) 出力情報の管理
・取扱及び引渡方法
・出力情報の保管、廃棄、活用方法
(シ) 外部委託
・委託契約の内容と手順
・進捗状況の管理
(ス) 要員管理
・要員計画と作業環境
・技術習得及び職業倫理
(セ) 標準化と文書化
・標準化の制度と運用体制
・文書化の種類と方法
(3) 監査に関する能力
(ア) 監査計画の立案
・目標設定
・計画の妥当性の検討
(イ) 監査の実施
・監査対象の現状分析方法
・監査方法の知識及びその適用
・監査内容及び内部統制の評価法
(ウ) 監査結果の取りまとめ
・総合評価手順
・指摘事項の的確性
・改善勧告の妥当性
(4) 関連知識
(ア) システム監査基準
・一般基準
・実施基準
・報告基準
(イ) コンピュータセキュリティ
・セキュリティ対策の方法
・リスク分析
・データ分析
(ウ) 人事・組織管理

・人事・組織管理の一般知識
・職務分析関連
・人事考課関連
・教育・訓練関連
・人間関係関連

(エ) 経営管理、財務管理
・経営管理及び財務管理の知識
・財務分析関連
・原価計算関連

(5) 関連法規
・監査関連法規
・労働関連法規
・セキュリティ関連法規

(6) 他監査との連携・調整
・公認会計士監査関連
・監査役監査関連

以上がシステム監査人として必要な知識の概要であり、これはとりもなおさずシステム監査人を育成する為の教育カリキュラムの大要でもある。このカリキュラムの特徴は、

(1) 情報処理の基礎と応用に関する系統的な学問分野。

(2) 経営、人事・組織、財務等の基礎と応用に関する系統的な学問分野

の両分野を包含するものである。そしてこれは、まさに経営情報学に於けるコアカリキュラム（専門学科で教えるべき最小限のカリキュラム）を示すものである。

そこで、特に(1)項に関して参考文献(4)、(5)ベースに大学の経営情報学部における情報学のコアカリキュラムの私案をここに示す（カリキュラム名は全て仮定の名前である）

(1) 技術文書構成論

コンピュータを勉強と研究の道具として使う為の、コンピュータリテラシーと情報科学の基本として大切な良い日本語の技術文書作成技術等の教育で、次の内容より成る。

・ワードプロセッサ
・電子メール
・表計算（データ解析能力の育成）

(2) プログラミング序論

次の目的を持つ
・問題解決手法とアルゴリズム化を秩序だてて考える能力を育成
・プログラムの設計、コーディング、デバック、テスト、文書化について、良質のプログラム書法の習得
・計算機のハード、ソフト等の技術の発展、プログラムの図式化法等、計算機科学を更に学んで行くための基礎の習得
・ファイル、データベースの基礎

(3) 計算機システム序論
・計算機システムの基本概念を機械語のレベルで習得
・コンピュータアーキテクチャの基本概念の習得

(4) オペレーティングシステム一般
・オペレーティングシステムの役割
・ＣＰＵアーキテクチャとオペレーティングシステムのインタフェース
・多様なレベル・形態の計算機結合方式

(5) ソフトウェア工学序論
・ソフトウェア開発サイクル
・各段階での文書化技術
・各段階での使用可能な技術

(6) コンピュータセキュリティ
・セキュリティ一般
・リスク分析
・安全性／信頼性設計
・プライバシーと知的所有権

以上、プログラミング序論などは学部で２年間に渡って教育する必要がある

参考文献

1）日本情報処理開発協会編
・〝システム監査基準解説書〟（1987）
・〝システム監査Ｑ＆Ａ110〟（1987）
・〝シスメム監査実施の手引き〟（1989）
2）菊池豊彦著〝情報システム監査の最前線〟（1992）日本電気文化センター

3)宮川公男〝情報資源管理におけるシステム監査の役割〞 システム監査 Vol3, No2 (1990)
4)野口正一、他〝大学等における情報系専門教育の改善への提言〞
情報処理 Vol32, No10 (1991)
5)村岡洋一〝情報科学カリキュラムの一例〞
情報処理 Vol33, No2 (1992)