

# システム診断とシステム監査

## 情報システムの脆弱性視点からのアプローチ

Information Systems Diagnosis and Information Systems Audit  
An approach from the Viewpoint of Vulnerability of Information Systems

松田技術士事務所

松田 貴典

Matsuda Consulting Engineer Office Matsuda Yoshinori

### 1. はじめに

近年のIT (Information Technology: 情報技術) の発展はめざましく、企業や官公庁等 (以下、企業等) の情報システムの高度化をもたらし、ITを経営戦略の実現に積極的に活用するようになってきた。その一方で、インターネットをはじめとするグローバルネットワークは、国際的なビジネス社会を形成する情報通信インフラストラクチャ (情報通信基盤) を確立することになる。グローバルネットワーク時代における情報システムは、ビジネス活動の企画・設計から調達、開発、生産、管理、保守に至る諸活動を支援するCALS (Commerce At Light Speed: 光速商取引)<sup>注1)</sup>をはじめ、電子決済を含めた一連のビジネス活動の電子化を実現するとともに、EC (Electronic Commerce: 電子商取引) の時代を導くことになる。

この時代になるとIT活用は無限の可能性と効用が期待できる反面、投資効果の予測が難しくなる。また、ITと経営戦略との関係は、これまでは企業等における戦略の実現にITを活用するという考え方であったが、現在ではITを前提に経営戦略を立案していくという考え方に進化している。そして、ITなしに競争優位の実現は難しく、時には企業等の生き残りができない時代となってきている。即ち、ITと経営戦略の主従関係は既に逆転しており、それゆえ、自社にとってのITは何かを十分に調査・分析し選別するとともに、ITに連動して組織や業務をダイナミックに変革させることが重要である。さらに、IT投資は、基幹業務が確立された後は、将来のキャッシュフロー向上のための戦略投資に向けられなければならない。

情報システムの健全化の手法には、リスクマネジメントやセキュリティマネジメントのほかに、システム監査（以下、監査）がある。これらの手法は、健全な情報化社会に充分貢献できると考えられてきた。しかし、IT活用の進展は速く、現在では、予期できない事故・犯罪が容赦なく人々を襲い健全な情報化社会を脅かす混沌とした国際情報化社会に向かいはじめている。その一方で、国際企業間の競争は激化し、企業等が生き残りをかけたITの戦略活用が求められており、その失敗は企業等の存続を危ぶまれるばかりか社会的責任や法的責任を問われることになる。このことから、これまで情報システムの信頼性や安全性を担保する監査から、一歩経営に踏み込んだ情報システムの戦略性や有用性の評価が求められている。これはまさしく、経営者にとっては、ITの戦略活用を推し進める強力なシステム診断（以下、診断）を要求するものであり、その一方で、情報システムの信頼性・安全性・適法性を担保する監査が強く求められている。そして、この監査を、もはや内部監査の一環としての任意監査ではなく、実施を法的に義務付ける「法定監査」にすべき時期にきている。

## 2. システム監査の法制化とシステム診断の役割

### (1) システム監査と診断の役割

監査は、情報システムの「信頼性、安全性及び効率性」の向上を図り、情報化社会の健全化に資することを目的として、「監査対象からの独立」し「客観的立場」で「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・勧告」するとともに「フォローアップ」する一連の活動である<sup>(1)</sup>。現在のようにITの高度化と戦略活用の進展にともない、監査ではその視点である信頼性、安全性、効率性の範囲の拡大や監査機能の強化が進められている。例えば、「情報化投資は適性で十分な効果が上がっているのか」の視点や「情報システムが経営戦略に連動して有用に機能しているか」の視点など、「有効性」や「有用性」の視点である。この結果、これまでの重要な監査視点である「効率性」を、その視点の範囲を拡大化した「有効性」や「有用性」に改訂することを指摘し、有用性の視点をさらに細分化した、戦略性、有効性、生産性、採算性の視点を挙げている<sup>(2)</sup>。まさしく適切な指摘であり、今後この視点は、IT活用の高度化に伴いますます重要になってくる。

これまで、監査についてはいく度となくその「監査」の呼称の改訂が叫ばれてきた。それは監査のもつ意義や定義に限界が感じられたからである。もともと、「EDP 監査」な

るものがあつた。これは、商法や証券取引法に基づく会計監査の実施にあたって、コンピュータ化された会計システムを対象とした監査証跡の確保や見読可能な信頼ある帳票の出力およびコントロールの組み込み状況の監査である<sup>(3)</sup>。一方、「System Auditing」を「システム監査」と訳し、EDP 監査とは一線を引く「EDP システム監査」がシステム監査として位置付けられた経緯がある。このように、システム監査の手法や手続きは、会計監査を基本に確立されてきたこともあり、監査の用語が定着した。

しかし、現在のように、高度に進化した情報社会では、監査は会計システムのみを対象にしていない。独自の「システム監査概念」を確立させるとともに、経営問題として監査を捉えて行かなければならない。欧米では既に監査を「Information Systems Audit and Control」と表現し、情報システムの高度化にともなう監査（監査と訳することに問題はあるが）及びコントロール（統制）の強化を図ってきた。そして、情報システムのより品質の向上及びより安全性・信頼性の向上にその視点をシフトさせている。これは IT の高度化に伴い、“Information Systems (IS)”を戦略的な活用にまで押し上げ、その効用を画期的に広げる一方で、金融システムをはじめとする社会的な使命をもつ情報システムは、公認情報システム監査人(CISA: Certified Information Systems Auditor)等に監査を一部義務付けている。

前述したように、これまでITは企業等の経営戦略の実現手段(ツール)として見られ、戦略が明確化されないと経営に役立つ情報システムの確立ができないとされてきた。しかし、現在のITは、戦略の実現手段としての位置付けのみならず、戦略そのものになり始めている。コンピュータのパーソナル化やモバイル化、インターネットによるEC社会の実現等は、情報戦略を誘導し、新たなビジネス創造をもたらしている。このような状況の中で、情報システムの戦略活用を監査に求めることに問題があると考えられる。むしろ法制化を進める上で適切ではなく、もはや監査で点検・評価する次元を超えており、情報システムの診断に委ねることが、健全な情報化の進展にふさわしいと考える。また、当然のことであるが、企業等の情報システムに対する期待(目的)は同じであっても、監査と診断での視点やアプローチは異なるはずである。

診断では、ITを経営の側面から経営者に助言・指導するだけでなく、IT戦略の内容に主眼をおいた継続的なコンサルティングアプローチをすべきである。コンサルティングアプローチとは、問題解決の手法を通して、経営や業務の改善・改革を継続的に実施するアプローチである。また、それはITの戦略的機能を分析・評価したアプローチであり、

常にITと経営戦略との融合を図るものである。一方、監査では、情報システムの安全性、信頼性及び適法性に視点を置き、ITがもたらす脆弱性に向けた断続的なリスク/セキュリティアプローチである。リスク/セキュリティアプローチとは、問題点の発見や点検手法を通して、脅威の実現リスクの発見やセキュリティ確保を主眼においた断続的なアプローチである。それゆえ、監査と診断の役割と範囲を明確に分離し、監査については、法定監査として実施が義務化されなければならない。また、診断では情報システムをより戦略的活用を推し進める視点に置き、監査とその役割を補完しつつ、情報システムの健全化を推し進めることが、グローバルネットワーク化時代に最も必要なことと考える。

筆者は、これまで、監査視点の拡大化と監査人の立場をより強化するため、「参画型」の監査を提言してきた。高度化する情報システムの健全化をより高めるには、これまでの独立・客観性を踏襲する監査では、その機能を十分に果たせないとして、参画型の監査を主張してきた。参画型の監査とは、情報システムの開発や運用での安全性、信頼性に関与して、一部マネジメント業務を管理者とともに進め、その中で直接に監査を行うものである。例えば、牽制機能を強化する組織体制の提案、具体的なセキュリティシステムの設計など、マネジメントが実施しなければならない業務を、監査人が一部実施しながら進める監査である。この結果、より直接的な指導効果を求めることになるが、監査としての独立・客観性を見失うことになる。しかし、参画型の監査も新たな監査スタイルとも言えよう。しかし、今、監査のスタイルや監査の役割を拡げることは監査の法制化を遅らすことにもなり兼ねない。監査の法制化を遅らすことは、プライバシー保護の法制化やネットワーク取引の安全性等の強化を求める国際社会から非難を受けることになる。安全性、信頼性、適法性を担保する監査はより強力に実施しなければならないし、また、監査の効果を高めるために、独立・客観性はより一層の法的な保証もとで、推し進める必要がある。

今日、最も重要な要件で討議しなければならないのが、監査の法制化の問題である。この問題は、個別には主張されているが、行政を巻き込んで討議しなければならない重要な問題となってきた。

### **3．情報システムの脆弱性のシステム診断とシステム監査**

#### **(1) 情報システムの脆弱性の監査と診断の役割**

情報システムは、ITの技術革新とともに高度化し、企業環境のみならず家庭環境をも変革させ「豊かな情報化社会」をもたらした。しかし、豊かな情報化社会の裏では、情

報システムが高度化すればするほど、コンピュータ事故、災害、犯罪等の脅威が現実のものとなって、大きな被害をもたらす脆弱な社会を生むことになる。脅威の実現化は企業にとってその存続を危ぶませることになり、個人にとって日常の家庭生活ができなくなってしまうことになる。この誘因となるのが「情報システムの脆弱性」(Vulnerability of Information Systems, 以後、脆弱性)である。脆弱性は、ITが持つ本質的な特性により発生し、避けることができない欠陥となって情報システムに内在する。欠陥は、ハードウェアの故障やソフトウェアのバグ(bug)などを指すだけではない、企業や社会へ悪影響を及ぼす機能的な障害をも含んでいる。そして、脆弱性のコントロールの弱い部分から脅威が現実化する。

企業等は、事業や業務の「目的」を達成するために、ITにより確立された情報システムを活用する。その目的とは、経営目標の達成や業績の向上等様々な成果の成就である。すなわち、企業等の執行諸機能を情報通信システムにて実行することで、それが持つ本質的な特性によりその「効用」を享受できる<sup>(4)</sup>。しかし、この効用とは裏腹に、情報システムの事故や災害、犯罪等により多大な被害を受ける脆弱性を内在させることになる。通常、脆弱性はコントロールされているがこのコントロールを超えた時、事故や犯罪の脅威が現実化するのである。

脆弱性はこれまで技術的側面、組織的側面、社会的側面にて分類され、森宮<sup>(5)</sup>が指摘するように、情報システムの脆弱性を分析し、理論的に吟味することが不十分であったと言える。これまで論述してきたように、ITが合理化や省力化の手段ではなく、戦略の実現化や経営の戦略そのものになりつつある今日、脆弱性を単なるITの「弱さ」の側面で捉えることは問題が多い。その上、IT投資やIT活用の失敗が、企業の競争離脱や存続が危ぶまれることになることを鑑みれば、脆弱性の視点はより経営管理や組織的側面で捉えなければならない。そこで、脆弱性を新たに 経営管理・組織的側面、 国際・社会的側面、 情報技術(IT)的側面、 法・倫理的側面の四つに類型化し、監査及び診断の視点をしめした<sup>(6)</sup>。このように脆弱性を分類した理由は、第一に、これまで分類されてきた技術的側面、組織的側面、社会的側面の脆弱性の研究成果を活用できること。第二にITが密接に関連して影響を及ぼす側面をより拡大化して捉える必要があること。即ち、情報基盤としてのテクノロジーの側面、ITの企業等活用としての経営、組織的な側面、外部的な関連としての国際、社会的な側面、そしてそれぞれの側面に密接に関連する法律、倫理的な側面で捉えることが、効用との関係で脆弱性をより明確化できること。そして第

三に、脆弱性をより明確化することで、事故や犯罪が何に起因して発生しているか明らかになり、その対応（対策）が立てやすくなることである。

表1は脆弱性類型化とその側面からの監査と診断の視点の事例である。効用は企業等の執行諸機能を情報システムにより執行されることによる得られる成果である。また、効用とは裏腹に内在する脆弱性の視点を、主として診断の対象をとる「有用性」と、主として監査の対象となる「安全性・信頼性・適法性」で区分した。

一方、前述のように、監査と診断を組み合わせ有効に機能するには、それぞれが同じ脆弱性の側面から情報システムへアプローチすることは望ましい姿ではない。監査はITの脆弱性の側面から安全性、信頼性、適法性の視点を中心に客観的な立場でアプローチをおこない、また、診断は経営管理・組織的な脆弱性の側面から有用性の視点でコンサルティングアプローチをおこなう。その上で密接に関連する国際社会的脆弱性と法・倫理的側面の脆弱性の視点に向けてアプローチするのである。図1はこのアプローチの方向性を示したものである。

脆弱性の分類は、監査や診断の役割や範囲を明確に分けるためのものではない。監査や診断がどの脆弱性側面でどのような視点からアプローチをかけ、どの方向に向けるべきか示すためのものである。その結果、互いの機能を相互に補完しながら、漏れの無い、有効で効率的な監査と診断が期待できるのである。以下、個々の脆弱性の側面について事例を中心に視点とアプローチを述べる。

## （2）経営管理・組織的側面の脆弱性

経営管理・組織的側面の脆弱性（以後、経営組織的脆弱性）は、企業等の業務を情報システム化することにより発生する。しかし、経営組織的脆弱性は、その情報システムを実務現場に適用し、日々運用していくことから発生する。例えば、経営管理には、内部統制の欠如による脆弱性の発生が重大である。内部統制の欠如は、結果的に、情報システムに対する信頼性の欠如、情報システムへの不信感となって現われ、情報システムが経営管理や情報戦略に役立つ機能が果たせなくなる。また、コンピュータや情報システムにより、組織は少数精鋭化となり、少人数による広範な大量データの処理が可能になる。反面、不正データの入力や処理が行われる機会を増大させることになり、結果的には内部牽制機能の弱体化が起こってくる。これが情報化によるブラックボックス化の組織的脆弱性の一例である。

近年、情報をより現場に開放して、戦略的な活動をさせる EUC (End User Computing) やモバイルシステムが普及している。これは、幅広い情報を現場に提供し、より新鮮な情報による競争優位と差別化を図るものである。診断ではこの推進にトップマネジメントの側面からアプローチしなければ、成功は難しい。例えば、近年話題となっている企業間での EDI (Electronic Data Interchange: 電子データ交換) や SCM (Supply Chain Management) の実現、企業内においては BPR (Business Process Re-engineering: リエンジニアリング) など情報の活性化の実践的手法は、経営管理や組織管理に有効な IT 活用がなされているかの視点で診断することが求められる。また、適正な IT の戦略投資やその効果の測定も、無駄な投資を抑制する反面、継続的な企業の存続に必須と言える。そこで、診断では、IT の戦略投資や効果の経営組織的脆弱性を、有用性の視点でコンサルティングアプローチするのである。

情報システムの脆弱性は IT を活用することで画一的に発生するものではない。個々の企業等が活用する IT の機能、範囲、情報アーキテクチャ (情報処理の基本的考え方) のレベル、情報システムの進展度等により固有の脆弱性が内在することになる。また、脆弱性のコントロールの強弱により、脅威の現実化するリスクが異なるし、被害の大きさも変わる。IT のビジネス活用は戦略の実現を優先するあまり脆弱性の問題が無視されるきらいがある。特にこのことを企業のトップマネジメントは理解し難く気付かないことが多い。そこで、診断では、経営組織的脆弱性からのコンサルティングアプローチが必要なのである。

### (3) 国際・社会的側面の脆弱性

情報システムは、通信技術の進歩により、企業内部から企業間の情報通信システムへ進展してきた。いわゆる情報化の点から線、面への展開である。そして、この面の拡がり企業間から国際間のネットワーク取引に拡がりは始めている。

国際・社会的側面の脆弱性 (以後、国際社会的脆弱性) は、主として情報システムを仲介したネットワーク取引から発生する。ビジネス社会でのネットワーク取引は今後ますます増えており、産業界でのネットワーク取引は、CALS や EC の世界に発展していくことになる。また、金融機関での EFT (Electronic Funds Transfer: 電子資金移動) は、企業間決済から、個人決済に進み、電子マネーによる決済へと進んでおり、やがて、ネットワークによる個人決済の国際化が起こってくる。

例えば、インターネットによるサーバービジネスは、個人であっても簡単にネットワークビジネスの確立ができる。しかし、簡単にビジネスが模倣され、急激にビジネスを失うことになる。また、ネットワークシステムの不稼働リスクや決済業務の停止・不能リスク、決済不能による連鎖倒産（システミックリスク）、時差による国際的な決済不能（ヘルシュタットリスク）等さまざまな脅威が実現する脆弱性が発生してくる。そこで、診断は、インターネットをはじめとする情報通信システムが、豊かな情報化社会や国際社会に貢献しているかの有用性の視点での診ることになる。また、官公庁や役所システムが如何に市民や国民に役立つシステムになっているか、電子政府のシステムが社会のコスト削減につながっているか等が診断項目として挙げられる。もし、これらのシステムの不稼働や機能が十分に発揮できていないならば、却って、手続きの複雑化やコスト負担の増大化を招く脆弱性が生まれるのである。これらの脆弱性への対応は、診断のみならず監査においても、リスク分析に主眼をおいたリスクアプローチをすべきである。ただし、診断は主として投機的リスクを対象とし、監査は主として純粹リスクを対象とする。

#### （４）法・倫理的側面の脆弱性

法・倫理的側面の脆弱性（以後、法倫理的脆弱性）には大きく二つの細部側面で脆弱性が発生する。一つは、情報を如何に保護するかの側面である。情報は貴重な資産である、それがため、この情報が不正に複製されたり、不正にアクセスして改ざんや窃盗されたりする。これらの不法行為から如何に情報資産を保護していくか重要な問題である。また、ソフトウェアや情報資産が取引の対象となることで、知的財産権ビジネスや取引手段としてのITの法的な問題を検討しておかなければならない。

もう一つの側面は、ITが如何に適正にしかもルールやマナーにもとづいた活用の仕方がなされているかである。自社の情報システムの活用が、時としてその意思なく他人の情報システムに迷惑をかけたり、法的侵害を犯す結果になったりすることもある。これら情報資産の保護と侵害の両面は、法倫理的脆弱性として考慮すべき重要な視点のひとつである。

近年、情報は人、モノ、金に次ぐ第四の経営資産と言われている。この情報資産を戦略的に活用することで、競合企業からの競争優位が展開できる。また、ソフトウェアに対して知的財産権としての価値が認識され、その価値が積極的に取引活用されることが多くなり、その知的資産活用が活発化しはじめている。具体的にはソフトウェア著作権ビジネスやビ

ジネス・モデル特許の戦略的マーケティングである。

一方、情報データの不正なアクセスや侵害は、情報システムの脆弱性が法倫理的脆弱性問題に広がりはじめている。そのほとんどは、コンピュータ犯罪やプライバシーの侵害など法的な問題の起こす要因となっている。これは、ITが経営組織的脆弱性や国際社会的脆弱性を誘引し、犯罪を引き起こすことになる。コンピュータ犯罪の起こる環境は、組織の牽制機能の弱体化であり、内部統制の不備によるものである。さらに、国際的なネットワークを利用した犯罪は、国家間の法律の不均衡や国際協力体制の脆弱性に起因することが多い。その一方で情報倫理の問題として取り扱われるべき多くの事件が発生している。

例えば、日本ケミファ事件（1982年）、ネットワークねずみ講事件（1992年）、テーエスデー事件（1995年 風説の流布：証券取引法違反）、ドクター・キリコの診察室事件（1998年：自殺相談）、行政機関ホームページハッカー事件（2000年）等、インターネットの普及にともなって急速に増え始めている。情報倫理は情報を取り扱う人間のあり方の外周問題である。狭義には情報システムにかかわる人々の規範であり、情報作法と言えよう。倫理の立場で言うならば、高度情報通信社会なかで、何が良くて何が悪いのか倫理的に判断を下しつつ、その振る舞い方は倫理的正誤の知識を「学ぶ」ことによって得るのである。そして、いつの時代にも通用すべき絶対的な倫理というものはなく、倫理は歴史的に相対的であるといえる。だからこそ、歴史的に通用する倫理的正誤の知識を学ぶために、情報倫理教育が必須である。

この法倫理的脆弱性において、監査では主として情報資産の保護と侵害の両面から、法的な保護に主眼をおいた法的セキュリティアプローチをおこない、診断においては情報資産の管理・運用及びその教育に主眼をおいたコンサルティングアプローチをおこなう。

#### **（５）情報技術的側面の脆弱性**

コンピュータや通信システムが持つIT本来の脆弱性である。コンピュータ事故・犯罪を綿密に分析すると、実は情報技術的脆弱性が基底にあり、その上で、経営組織的脆弱性や国際社会的脆弱性、法倫理的脆弱性と結びついて脅威の現実化が起こり、被害が生じる。また、ITの進歩により情報技術的脆弱性は常に変化する。この情報技術的脆弱性がもとで、組織の牽制機能が働かない環境になり、さらに、法律や管理制度が弱いとコンピュータを悪用した犯罪や予想外の事故を引き起こすことになる。この結果、情報システムの安全性、信頼性、適法性に重点をおいた情報技術的脆弱性の監査が求められる。

この脆弱性の重要な視点の一つに、コンピュータシステムのセキュリティ対策の実施状況がある。例えば、大規模な情報システムや社会公共的なシステムはコンピュータシステムの二重化やバックアップセンターの維持（契約）を実施している。しかし、情報化が進んでいない企業等ではコンピュータシステムのセキュリティ対策費用は、売上の拡大や利益を生まない投資として考えがちであるが、この考えには問題点が多い。近年、セキュリティ投資を控えたことで、経営者に対して社会的責任を問われることが多発しており、情報システムのシステムダウンや情報資産の消失等が企業等の危機事態を招くことにもなりかねない。さらに、企業や国際間のネットワーク全体を「仮想の個」として捉えなければならない。それは、自己の情報システムの脆弱性が足がかりとなって、ネットワーク全体の脆弱性を発生させることになるからである。情報資産保護のためのセキュリティ対策が、企業等のトップマネジメントの重要な施策であることを、トップマネジメント自らもって認識させることが、監査の重要な役割である。そして、監査は情報システム全体の安全性に主眼をおいたセキュリティアプローチが必要となる。

その一方で、情報システムの有用性の視点での診断が重要になる。情報システムの機能が十分に発揮されているか、常に情報システムの効率化や有効利用について検討改善しているか、情報化されて業務システムが利用者にとって使いやすく、オンラインレポンスや処理パフォーマンスに問題はないのかといった視点での診断の実施が必要である。

#### 4．おわりに

情報システムの脆弱性を四つの側面で類型化し、情報システムの脆弱性に対する診断と監査の基本的なあり方について論述した。しかし、高度にコンピュータ化した情報化社会はITの進展とともに進化し、脆弱性は複雑に変化する。それは情報システムの効用が、情報処理の効率化や業務の合理化の域を終えて、IT活用による企業等戦略の実現、競争優位の展開等、有用性へのインパクトとなってきたことである。その結果、情報システムの脆弱性の視点は安全性、信頼性、効率性から、適法性、有用性にも及ぶことになる。このような情報システムの脆弱性が拡がる中で、情報システムの健全化を担保する監査と有用性を点検・評価しコンサルティングする診断との機能や役割は明確に異なり、アプローチも変えるべきである。そして、監査をできる限り早期に法制化し、実施を義務化させなければならないと考える。

敢えてお断りしておくが、筆者は診断人や監査人の知識、能力を問題にしているのではな

い。また、ビジネスや業務の範囲を限定しようともしていない。ITの高度化がもたらす21世紀のグローバル情報化社会の健全化に、診断と監査の果たすべき役割は何かを問うているのである。グローバル時代の情報社会において、情報システムの安全性、信頼性、適法性を確保するには、現状では、監査の法制化が最も効果的であり、それが日本の国際情報化社会への責務と考える。反面、診断はこれまでの立場では十分に成果をあげられるとは考え難く、これまで監査で提言してきた参画型のアプローチが必要である。そしてこれらの手法や手続きが相互補完しながら効果的・効率的な情報システムの健全化と有用化を実現しなければならない。ここに新たな「システム監査」と「システム診断」という概念の確立が求められるのである。

[ 1 ] CALS は、最初 Continuous Acquisition and Life-cycle Support: 生産・調達・運用支援統合情報システムの略で、現在は Commerce At Light Speed: 光速度取引となるまで、CALS の簡略前の用語は4回の変更がなされている。

#### [ 参考文献 ]

- ( 1 ) 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」 (財)日本情報処理開発協会発行 1996
- ( 2 ) 武田道雄, 上園忠弘著 「監査役によるシステム監査のためのチェックリスト」 システム監査 Vol.8 1995
- ( 3 ) 日本公認会計士協会編 「EDP監査の進め方」 (財)大蔵財務協会 1976
- ( 4 ) 森宮康著 「情報システムのリスクマネジメントとシステム監査」 システム監査学会編 「システム監査の理論と実践」 1994
- ( 5 ) 松田貴典著 「情報システムの脆弱性」 白桃書房 1999
- ( 6 ) 青山監査法人システム監査部編 「システム監査の方法」 中央経済社 1985
- ( 7 ) 宇佐美博 富山茂著 「システム監査の手法と実務」 日刊工業新聞社 1991