RCSSディスカッションペーパーシリーズ
第34号　2005年12月

Discussion Paper Series
No.34　December, 2005

ISSN 1347-636X

銀行システム監査の強化のための人材育成と行内組織の整備

長　岡　壽　男

RCSS

文部科学省私立大学学術フロンティア推進拠点
関西大学ソシオネットワーク戦略研究センター

Research Center of Socionetwork Strategies,
The Institute of Economic and Political Studies,
Kansai University
Suita, Osaka 564-8680 Japan
URL : http://www.rcss.kansai-u.ac.jp/
http://www.socionetwork.jp/
e-mail : rcss@jm.kansai-u.ac.jp
tel. 06-6368-1177
fax. 06-6330-3304

銀行システム監査の強化のための人材育成と行内組織の整備

長 岡 壽 男

RCSS

文部科学省私立大学学術フロンティア推進拠点
関西大学ソシオネットワーク戦略研究センター

Research Center of Socionetwork Strategies,
The Institute of Economic and Political Studies,
Kansai University
Suita, Osaka 564-8680 Japan
URL : http://www.rcss.kansai-u.ac.jp/
http://www.socionetwork.jp/
e-mail : rcss@jm.kansai-u.ac.jp
tel. 06-6368-1177
fax. 06-6330-3304

銀行システム監査の強化のための
人材育成と行内組織の整備

長岡壽男*

要約

銀行の情報システムは、当該銀行の営業戦略、顧客サービス、事務管理などあらゆる部門と密接な関わりを有している。さらに、1990 年代中頃以降からのポスト第三次オンラインシステム時代では、業務の多様化、技術の進歩、システムの高度化に対応していくことが強く求められている。システム監査部門は、こうした情報システムの評価を適確に行い、経営者に公正な意見具申を行う責務がある。

したがって、システム監査体制を整備することは、いまや、銀行における経営戦略上の重要なテーマとなっている。本稿では、銀行におけるシステム監査の強化のために、人材の育成・結果監査から予防監査・トップ・マネジメントとの連携・システム監査組織の見直しという提案を行っている。

キーワード：システム監査、監査人、システム監査領域、システム監査体制

Restructuring of personnel training and internal organization to strengthen banking system audit

Hisao Nagaoka

Abstract

The information system of concerned bank has close relations in all sections like the business strategy, customer services, and the management of affairs etc.

In addition, it is strongly requested to correspond to the diversification of business lines, the advance in technology, the upgrade of the system in the post-third-generation on-line system age since about the middle of 1990's. System audit section adequately evaluates such an information system, and there is an obligation to report on a fairly opinion to the top management.

Therefore, it is an important theme in the management strategy in the bank now to maintain the organization of system audit. In this paper, it proposes personnel training, preventive audit from result audit, cooperation with top-management, and review of

* 関西大学ソシオネットワーク戦略研究センター委嘱研究員。

system audit organization for strengthening system audit in the bank.

はじめに

現代の銀行における情報システムは、営業戦略、顧客サービス、事務管理などすべての面で密接な関わりを有している。したがって、システム監査人は、情報システムの稼動状況を、客観的に評価するとともに、的確に意見具申していくことが、何よりも強く求められている。

とくに、情報通信技術の急速な進展の結果、新しい情報技術の吸収や、時代に即応した管理技術の習得が、円滑なシステム運営上欠くことのできないものとなっている。開発や運営体制の不備が、システムの事故や障害に繋がる事例も多い。このためにも、システム監査体制の充実を図り、世間から信頼を得る銀行の実現に努力を傾注していくことが、戦略としても必要であると考えられる。

筆者は、これまでに、大西、長岡（2003)、長岡（2003)、Nagaoka(2004)、長岡、増本、上田(2004)、Nagaoka（2005）において、システム監査について論じてきた。

また、システム監査についての先行研究としては、松田貴典（1999)、木村剛(2001)、吉田洋(2002)、監査法人トーマツ編（2003)、先端リスク研究会編(2003)、石島隆（2005）の文献が挙げられる。

松田貴典(1999)は、情報システムが開発されれば、そこに必ず脆弱性が存在するとの考えに立って、脆弱性に起因するリスクを体系的に整理・分析している。情報システムの稼動とともに、リスクを的確に把握し、これを抑制していくことがシステム監査において重要な責務となっている。特に、予防監査の必要が唱えられており、今後想定される脆弱性を、事前に評価していくことが、益々必要となろう。脆弱性という視点から、システム監査の着眼点をも明らかにしている。

木村剛(2001)は、自己責任原則のもとでの、金融機関が内部監査体制を確立するための指針を明示している。金融検査マニュアルに沿った金融検査の課題と今後の内部監査のあり方について、国際的な流れとともに解説している。各金融機関において、それぞれ内部統制体制を構築してきたが、如何に機能を発揮せしめるかが今後の課題となっている。

吉田洋(2002)は、情報システム監査についてのフレームワーク、研究領域、歴史的発展経緯など基礎的な概念と、システム監査の着眼点を明らかにしている。技術進歩に見合った監査手法が考案されるべきであるが、技術に振り回されていては、一般理論の構築が困難になるとの指摘は、現在のシステム監査に当てはまることといえる。システム監査についての体系的かつ理論的な研究領域が示されている。

監査法人トーマツ編(2003)は、経営者に対して、情報セキュリティの課題をどのように把握し、対応して行くかを、豊富な監査事例・経験をもとに明示している。金融機関におけ

る情報システムの事故には、経営者の理解があれば、未然に防止できたものもあったと考えられる。この意味からも、本書の狙いとする経営者への啓蒙は重要である。また、情報セキュリティ・マネジメントは、システム監査と表裏一体と考えられ、監査の立場からも研究対象として理解を深める必要がある。セキュリティ・マネジメントの適否は、今後の情報化戦略の重要なポイントになると考えられる。

先端リスク研究会編(2003)は、金融検査マニュアルの指摘する態勢の組成に、金融機関はどのように進めるべきか、経営者は何をなすべきかを明らかにしている。また、ベストプラクティスのために、いくつかの提言を試みている。システムリスクに挑むことは、まさしく金融機関における重要な戦略課題であり、リスク抑制のための具体的なマネジメントが強く求められている。

石島隆(2005)は、情報技術を利用した情報システムの内部統制評価の重要性を指摘している。しかし、多年その重要性について提唱されてはいるが、充分な対応が出来ていないのが実情である。それは、評価を行う人々に情報技術の知識が備わっていないことに起因する。ただ、情報技術が全てではなく、必要とあれば専門家の知識を借りればよい。要は、情報システムの内部統制にかかるコーポレートガバナンスにおける位置づけ、会計情報システムの仕組み、内部統制評価の留意点などを理解していることが重要であり、これらを体系的かつ具体的に明示している。内部統制のレベルアップに資するものと考えられる。

本稿では、こうした先行研究等を踏まえて、銀行のシステム監査を強化するための、人材育成と行内組織の整備について、具体的な提案を以下に論じている。

1・システム監査の役割

① システム監査の定義

銀行の経営戦略は、情報システムと密接な関係にある。情報システムが、経営戦略の目標達成のため、有効に機能の発揮が出来ているか吟味する必要がある。また、その管理体制が適切か否かといったことも重要な課題となる。こうした意味から、システム監査は、経営者の意向を受けて、全行的なリスク管理の実態を把握し、これを適時報告していくことが求められる。

財団法人金融情報システムセンター（The Center for Financial Industry Information Systems :以下 FISC と略す）では、システム監査の役割は、「情報システムリスクの管理状況をモニタリングすることであり、さらには、経営者への有益な情報提供手段となること」[1]とし、経営者へのリスク・マネジメントに寄与することに、重要な使命があると指摘している。同センターにおけるシステム監査の定義は、「情報システムの有効性、効率性、信頼性、遵守性、および安全性の達成を妨げようとする情報システムリスクの管理体制が適切かつ効果的であるかを、監査対象から組織的に独立したシステム監査人が把握、評価し、

その結果を経営者に報告するものである。」としている[2]。なお、経済産業省の「システム監査基準」では、「システム監査とは、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および評価し、組織体の長に助言および勧告するとともにフォローアップする一連の活動」と定義している[3]。

② システム監査の展開

これまでの過程をみると、情報システムの監査は、会計監査や事務検査における補完的意味合いにおいて実施されてきたと考えられる。初期の段階では、コンピュータ監査とか、EDP(Electronic Data Processing)監査として実施されてきた。銀行では、検査部門の内部組織として、EDP 監査を担当する専任者が配置されており、各部門の検査に付随して業務に当たった。この段階では、まだシステム監査というより、システムの稼動状況や正確性、管理状況などをチェックする検査が主であった[4]。

銀行が独立したシステム監査部門を設置するようになったのは、昭和 60 年代(1985 年以降)に入ってからで、一部の都市銀行等から始められた。なお、被監査部門から独立したシステム監査体制を構築しているところは、銀行においては 86.5%、協同組織の金融機関では、70.8%との調査結果がある(FISC による平成 13 年 3 月調査)[5]。

ところで、1985 年 1 月、当時の通商産業省(現経済産業省)は、システム監査のガイドラインとして「システム監査基準」を公表した。これが、今日のシステム監査体制が築かれる端緒になったと考えられる。また、同じ年に、同省の外郭団体である日本情報処理開発協会は、「システム監査基準解説書」を公表し、翌年から「情報処理システム監査技術者試験」が実施されることになった。

また、金融機関に対しては、1987 年に FISC が「金融機関等のシステム監査指針」を公表し、これがその後の金融機関におけるシステム監査の指針となっている。とくに経済環境の激変に伴い、1999 年 4 月金融監督庁(現金融庁)は、「金融検査マニュアル」を公表し、当局の監督行政の方針が、これまでの「当局指導型の検査」から「自己責任原則による経営を補強する検査」へと転換された。この中でシステムリスク管理のあり方ついても触れられており、さらなるシステム監査の強化が求められた[6]。

なお、銀行の監査には、内部監査と外部監査があるが[7]、監督官庁によるものには、金融庁による検査や、日本銀行法に基づく日本銀行による考査を随時受けている。一方、内部監査人による監査では、FISC の「金融機関等のシステム監査指針」、「金融機関等コンピュータシステムの安全対策基準」などを参考にしながら、自行の監査目的に沿った、システム監査が実施されている。

③ 金融監督機関における動き

金融機関の情報システムの安全性を確保するために、内部統制の充実は不可欠である。内部統制の一般的なフレームワークは、1992 年 9 月米国で発表されたトレッドウェイ委員会組織委員会（Committee of Sponsoring Organizations of The Tredway Commission）のレポート「内部統制の統合的枠組み」(以下 COSO レポート)がある。この COSO レポートの考え方は、その後の金融機関における内部統制を評価する上で、スタンダードといわれている[8)]。

バーゼル銀行監督委員会[9)]は、このレポートを基にして、1998 年 9 月「銀行組織における内部管理体制のためのフレームワーク」を公表した。この中で、「有効な内部管理体制は、銀行経営にとって必須の要素であり、また銀行組織の安全かつ健全な業務のための基礎となるものである」と述べている。このような金融機関の内部管理体制への関心が高まったのは、相次ぐ事故や不祥事の原因が、適切な内部管理体制の欠如によることを背景としている。

さらに、同委員会は、2000 年 7 月「銀行組織の内部監査、および監督当局と内部･外部監査人との関係」という市中協議ペーパーを公表した。特筆すべきは、「銀行組織における適切な内部管理は、組織の管理システムを評価する独立した有効な内部監査によって補強されねばならない」と表明していることである。

わが国においても、先述のとおり、1999 年 4 月、当時の金融監督庁が「金融検査マニュアル」を公表した。これにより、金融監督行政の方向転換が明らかになった。金融機関の経営者は、監査役を含めた内部監査体制を充実させることにより、自らの責任において、業務の健全性と適切性を確保するため努めるものとしている。さらに、2001 年 4 月、金融庁は、先述した「金融検査マニュアル」を改訂し、その内容を充実させた。また、2002 年 4 月には、「より強固な金融システムの構築に向けた施策」を公表し、金融機関等の内部監査体制等について重点的に検証するため、民間の専門家を登用した専門班による検査を行う方針が出されている[10)]。

こうした監督行政の動きに沿って、各金融機関においても内部監査の充実に努めているところである。また、こうした公表レポート、マニュアルや指針の考え方は、わが国の金融機関における内部統制充実のための柱となっている。システム監査に当たっても、こうした考え方を踏襲し、具体的な作業を行っている。

なお、新しい動きとして、2004 年 12 月に金融庁が公表した「金融改革プログラム一金融サービス立国への挑戦—」[11)]の項目のひとつに、「金融機関のガバナンスの向上とリスク管理の高度化を通じた健全な競争の促進」が取り上げられている。ガバナンスの実効性、社会的責任の取り組み、行動規範の確立、内部監査の充実など活力ある金融システムの構築に欠かせない具体策が示されており、各金融機関が進むべき方向が明らかになっている。また、こうした動きの中で、各金融機関の参考に供するため、2005 年 7 月、金融庁検査局は、「金融検査指摘事例集」[12)]を公表している。

2・システム監査の対象領域と実務

システム監査を学ぶに際して、システム監査論、内部統制論、情報技術論等の書を紐解くことになる。しかし、こうした分野からのアプローチ以外に、いくつかの観点から学んでいくことも必要である。また、すでに公表されている公的文書や指針、マニュアルに基づき、それらに記載された考え方を忠実に実行していくことも、金融機関において求められている。特に、システム監査に際しては、独自の監査手順やマニュアルを活用するが、その際、先述のように、FISC の指針や基準書を参考にすることも多い。しかも、システム監査の対象領域は、近年広がる一方であり、監査に際し実務上の視点からだけでなく、マネジメント全般の幅広い視野からものを見ることが求められている。システム監査が、経営にとって有効であるか否かは、情報システムに係るマネジメント全般に亘る適確な意見具申ができるか否かに係っている。ここでは、システム監査の対象領域の拡大と共に、意識しておかなければならない視点について、主要なものを取り上げ、以下に論じる。

① 金融情報システムセンター（FISC）の監査指針

システム監査の対象は、情報システム全般であるが、FISC の監査指針では金融機関の情報システムおよび関係する活動全体を捉え、13 の領域に区分している。さらに、大項目、小項目に分類し、システム監査に必要とする約 1,000 にのぼるチェックポイントを示している。

なお、13 の対象領域をコントロールする部署も多様化している。情報システム部門、本部各部門、支店などの利用部門があるが、これらの部門において、情報システムのリスクが適切にコントロールされているか、システム監査を通じて評価し、リスク・マネジメントに寄与することに狙いがある。さらに、小項目に対応させて、システム監査の着眼点として、有効性、効率性、信頼性、遵守性および安全性の五つのコントロール目標を掲げており、それぞれが達成されているか否かを評価するものとしている[13)]。

なお、小項目の着眼点のうち、安全性項目が過半数の 98 あり、以下信頼性項目の 45 と続く。システム監査の狙いが、安全性にあることが良く分かる。

また、チェックポイントが 1,000 以上あるからといって、これをひとつずつチェックしていくことは、実務上不可能である。各金融機関においては、その時々に重要と考えた監査テーマに沿って、独自の監査マニュアルを基に、システム監査を実施している。その際、FISC の「金融機関等のシステム監査指針」を参考にすることが多く、その意味では、金融機関におけるシステム監査部門の必携の書として、活用されているといえる。

② 銀行業務の領域

次に、システム監査にあたり、銀行業務システムの内容を十分に理解していることが望まれる。個々のシステムの特性や、機能および障害発生時の影響などを理解し、円滑な稼動や安全対策上の問題点などを的確に助言できることが求められる。なお、各システムの特性とシステム監査における視点をまとめると下記の表１のようになる。

銀行における主要システムの特性などを表示したが、どの銀行も同様のシステムを構築しているとは限らない。対外系システムは、もともと外部接続の拡大・進展とともに、勘定系システムの負担を軽減させるため、または、リスク分散をはかるために、分離独立させた経緯がある。したがって、小規模のシステムを保持している金融機関では、勘定系システムにおいて対外接続を処理しているところもある。

国際系システムも、海外店を保有していない金融機関では、当然のことながら、海外店システムを保有していない。限定された国際業務機能のみによる小規模なシステムで対応している。

営業店・集中系システムも、銀行によって採用している端末機器や処理業務が異なり、個別行においてそれぞれ特色のあるシステムを構築している。営業店システムは、顧客サービスの向上、円滑な事務処理、および情報管理などを目的としている。集中系システムは、事務センター等で事務を一括集中処理することにより、効率化･厳正化を図ると共に、顧客サービスの向上に結び付けることを狙いとしている。なお、最近では、事務センター部門ではパートタイマーの採用が進んでおり、入力事務や端末システムの運用業務に従事させている。このため、正職員と異なる職員の人事管理に、特別の配慮が必要である[14]。

表１・各種銀行システムの特性

システムの名称	システムの機能	障害事例など	社会への影響
勘定系システム	① 全業務の顧客取引と口座管理。 ② 他のシステムとのデータ授受。 ③ 全店の端末機器と接続。	① 世田谷ケーブル火災事故。 ② 阪神大震災による被災。 ③ システム統合時のトラブル。	① 顧客取引の停止。 ② 決済取引の停止または遅延。 ③ 顧客サービスの休止。 ④ 業界システムへの影響。
対外系システム	① 業界の決済システムとの接続。 ② ATM＊網やEB＊＊の接続と管理。	① 回線障害による支障。 ② 地震や台風による断線や停電。 ③ 雷による瞬断。	① 決済の支障。 ② 顧客サービスの休止。 ③ 業界システムへの影響。

	③ ネットバンキングの管理。		
国際系システム	① 国際業務取引の処理。 ② 海外店取引の処理。	① 爆破事故等のテロ行為。 ② 風水害および停電。 ③ 現地職員のストライキ。	① 国際間決済に支障。 ② 海外店取引に支障。 ③ 国際間協力体制。
証券系システム	① 証券取引と証券運用。 ② 証券管理業務。	① 取引所システムの停止。 ② 交換所の業務停止(地震、台風等)。	① 決済の停止または遅延。 ② 取引の遅延または代替方法の選択。
営業店・集中系システム	① 顧客サービスの向上。 ② 事務の効率化。	① 回線障害。 ② 端末機等機器障害。 ③ 交通障害、ストライキによる遅延。	① 顧客取引に支障。 ② 事務処理の遅延。
その他（インターネット、モバイル、EUC＊＊＊）	① デリバリーチャネルの多様化 ② 分散処理	① 「スパイウェア」による不正引き出し。 ② 情報流失。 ③ パソコンの紛失・盗難。	① 不正取引による信用失墜。 ② 個人情報漏洩。 ③ 企業秘密の流失。

注：＊　ATM（Automatic Tellers Machine）

＊＊　EB（Electronic Banking）

＊＊＊　EUC（End User Computing）

ところで、システム監査に際し、こうしたシステムの特性を把握し、目的に沿った監査が出来ることが必要である。近年では、各種商品開発が進み、業務も多様化している。さらに、ネットバンキングのように、技術的にもサービスの面でも発展途上にあるものについては、サービスの向上とともにセキュリティの強化を図らねばならない。かかる領域におけるシステム監査の実施は、現段階において格別に力を注がねばならないテーマとなっている。具体的な措置としては[15]、「スパイウェア」対策や情報漏洩対策などが挙げられる。

③　システムに関する各種マネジメント領域

システム監査に際し、金融検査マニュアルの考え方とFISCの監査指針によるチェックポイントの活用、さらに業務システムの理解を踏まえて、有効な監査が可能と思われる。ただし、監査人は経営に資する提言ができる見識が必要である。監査人は、単に情報システムに関するシステム監査技術に止まらず、経営全般やシステム関連のマネジメントについて、見識を広めることが望まれる。なお、システムにかかる各種マネジメント論、技術論、制度論などは、それぞれがまったく独立したものではなく、随所に重複した部分があり、同じテーマについて、視点を変えて論じられていることも多々ある。ある目的に沿って論じられる過程で、重複または不可欠な論点は、経営や技術上重要な問題と解されよう。システム監査人は、平素から幅広くマネジメント全般に関心を持ち、知識の蓄積に努めることが必要であり、このことが監査の質的内容を高める上で有効となる。

システム監査との関係において、各種マネジメント領域における関連部門、規定、指針などを下表2にまとめた。システム監査を、より有効なものにするために、内部監査人は学ぶべきテーマは多く、表2はその一例である。

情報技術の進歩と適用業務の拡大は、止まるところを知らない。それだけに、システム監査人の教育や育成は、重要な課題となっている。

一般に、システム部門の勤務経験者は、業務を通じてシステム開発･運営等について、ある程度の理解があろう。また、改めて知識を整理するにも、過去の経験が役立つと思われる。ただし、システムも業務も絶えず変化しており、これに即応していく心がけが何よりも必要である。

ところで、表2のマネジメント領域は、あるところで同じテーマを論じていたり、また、極めて隣接していること等重複している部分がある。たとえば、コーポレートガバナンスとコンプライアンスおよびCSR（Corporate Social Responsibility）が挙げられる。コーポレートガバナンスは、企業の経営戦略に沿った効果的な活動と企業倫理や法令遵守の管理がなされているかを、企業のステークホルダーが監視することといえる[16]。コンプライアンスは、法令遵守について、組織的体制の確立と推進･管理を目的としている[17]。CSRは、企業憲章の展開において、コンプライアンスも目的として取り上げる事例が多い[18]。このように、相互に密接な関係があり、重複しているところがある。

なお、コーポレートガバナンスとIT（Information Technology）ガバナンスであるが、基本的に別の概念とする考えがあるが、ここでは、コーポレートガバナンスの一部と見なす考えをとりたい[19]。ITガバナンスは、企業の戦略目的に沿って、ITが策定･実施されているか、リスクを最小化するための管理･運営がなされているかを見る仕組みと考えられる。

セキュリティ・マネジメントとリスク・マネジメントも、同じ対象を異なる角度･視点

から見ていることになる。前者は、情報の安全を守る立場から、ものを見ており、当然リスクの分析や対応、危機管理を含んでいる。後者は、リスクの実態を把握し、リスクの低減策を講じ、もしリスクが発生した場合、危機管理の体制を準備するものである。相互に内容を包含し合っていると考えられる[20]。

コンピュータ・システム・リスクについては、過去の事故事例を紐解くことも大事である。過去の事故に対して、一体何を学んだのかと思われるような事故がその後発生している。教訓として活かすことが、何よりも求められている。事故例を参考にして、自行においては、どのような体制になっているのか、充分な対応が出来るのか、絶えず自問自答していく姿勢が望まれる[21]。

また、各種の認証取得は、それぞれの領域のマネジメントが、適切に管理・運営されているかを、公的機関を通じて一定の基準を上回っていると評価されれば、認証を受けるものである。ISO(International Organization for Standardization)9000 シリーズは、事務等の高い品質を保証するものであり、BS(British Standard)7799 は、英国において情報セキュリティ・マネジメント規格として発行したものである。プライバシー・マーク制度は、1998 年より運用を開始しており、事業者の個人情報の取扱いが適切であることを、プライバシー・マークを付与することにより、個人情報の保護に関する国民の意識向上を図ることを目的としている[22]。いずれも、市場において信用を得る手法の一つといえよう。認定取得のためには、管理体制･手順などの標準化をはじめ、テーマごとに組織的な見直しが行われる。この作業が重要であり、担当職員の意識を高めると共に、その後の組織全体における、管理水準の維持に結びつくものと考えられる。要するに、認証取得が最終的な目的ではなく、高い管理水準の維持に繋がることが重要なのである。

アウトソーシングは、必ずしも情報システムに限らないが、システム部門において活用されることが多い。基本的には業務委託契約を結び、アウトソーサーに業務を委託するが、常に順調または円滑にことが運ぶとは限らない。アウトソーシングリスクを抑制するためにも、契約にあたって、万全を期さねばならない。特に、情報の漏洩事件において、外部派遣社員等が関わっている事例が見られ、事故防止の観点から、契約内容に対応策を盛込むことが重要である。さらに、委託者側において、システム企画力の空洞化を未然に防ぐ対応が必要である。システム企画部門を行内組織として残し、進歩する技術動向の的確な把握とともに、管理技術の低下をきたさぬよう努めさせねばならない。アウトソーサーに委託した内容について、委託者が理解できないとか、問題の指摘能力がなければ、受託者の思うが侭のシステムになってしまう。委託者として、アウトソーシングリスクを認識し、コントロールすべきことを適切に処理していくことが不可欠である[23]。

表２で、情報システムに関する主なマネジメント領域を一覧にしたが、これらはシステム部門だけで管理されているのではない。システム監査にあたっては、関係する部門が多く、そうした広がりを意識した監査が求められる。また、監査対象となる手続、指

針、規程、マニュアルおよび法律などについては、充分な事前準備が必要である。こうした幅広い視点からものを見ることにより、監査の質的内容を高めることが出来よう。

表２・システムに関係する主要マネジメント領域

システムに関係する主要マネジメント領域	システム部門	関係本部	営業店	外部	規定･指針･規準など
システム・マネジメント	◎	○	○	○	
企画	◎	◎			企画書、予算書
開発	◎				仕様書、手順書
運営	◎				マニュアル
ファシリティ管理	◎	○			保管規定、保存規定
ドキュメント、手続	◎	◎	○		文書規定、事務手続
IT ガバナンス	◎	◎	○		企画書、予算書
セキュリティ・マネジメント	◎	○	○	○	セキュリティ・ポリシー、各種管理規定
システムリスク・マネジメント	◎	○	○		各種管理規定
安全対策	◎	◎	○		安全対策規準、規定
緊急災害復旧対策	◎	◎	◎		コンティンジェンシープラン
コンプライアンス	○	◎	○		コンプライアンス・マニュアル
知的財産マネジメント	◎	◎			知財活用・管理規定
個人情報保護	◎	◎	◎		個人情報管理規定
CSR 企業の社会的責任)	○	◎	○	○	経営理念、行動規範
ISO9000 シリーズ	◎	◎	◎		ISO 規準
BS*7799 認証制度	◎	○	○		認証取得規準
プライバシー・マーク付与	○	◎	◎		認証取得規準
アウトソーシング	◎	◎		◎	外部委託契約、遵守規定、SLA**等

注　表示の意味は、◎は「関係度大」、○は「関係あり」を示している。

＊　BS7799 は、Part-1 と Part2 がある。前者は、「情報セキュリティ・マネジメントのための実践規範」で、後者は、「情報システム・マネジメントシステムのための要

求仕様」である[24]。

＊＊　SLA(Service Level Agreement)。

④ 法務の領域

システム監査に関係する法律は幅広く、ここでは全般的な問題は差し置いて、最近の施行されたもののうち、関係の深い重要なものについて取り上げておきたい。

ⅰ）知的財産権の保護制度

知的財産は、企業が持っている知識、情報、スキルなどの総称である。銀行における知的財産といえば、たとえば顧客情報、情報システムおよびブランドなどであるが、管理面と活用面において、組織的な体制を築き、経営目的に沿った活動が期待される。日本政府も知財立国の名の下に、企業の競争力を高めるべく、これまでに法律や制度の見直しを進めてきた。

銀行において、知的財産権に係る活用面の動きには、情報システムに関するビジネス特許が注目されるようになった。最近では、金融機関による特許出願件数は、急速に増加している[25]。このほか、ソフトウェアに関係する、特許権、著作権および意匠権など知的財産の保護に関する動きは活発になろう。

一方、管理面では、保有する知的財産権の侵害を防ぐ活動が必要となっている。さらに、近年多発している企業秘密である個人情報の漏洩問題がある。また、不正競争防止法の適用を受けるには、一定水準以上の適切な管理体制が整備されていなければならない。いずれにしても、知的財産権の保護に関する環境整備や法務部門の強化が望まれている。

なお、信託銀行では、これまで無体財産は信託の対象になっていなかったが、信託業法第４条の改正により、すべての財産について信託の受託が可能となった(2004 年 12 月 3 日公布、同年 12 月 30 日施行)。また、信託業の担い手が拡大されることになった。こうした自由化の結果、信託を通じて顧客サービスの拡大・進展が期待されている。たとえば、信託手法による知的財産のファイナンスなど、新しいビジネスが芽生えてくると思われる。当然、こうした分野の情報システムの構築も進められることになり、その結果として、システム監査の対象となるであろう[26]。

ⅱ）個人情報保護法

2005 年 4 月 1 日より、全面施行された個人情報保護法は、金融機関に個人情報の取扱い事業者としての義務を課している。特に、個人データの収集に際して、業務上必要な範囲内で、利用･提供の目的を明確にして顧客の同意を得ることが原則となっている。利用につ

いても、業務上必要の範囲で、しかも、顧客の同意を得た範囲でのみ利用できる。なお、当然のことながら、センシティブデータの収集は、原則禁止されている。

管理体制については、整備項目を定め責任者の設置、守秘義務の再確認、従業員の教育徹底、取扱いルールの作成などが定められている。このほか、苦情処理体制の整備、本人からの開示請求に対する遅滞無き開示体制の整備、情報漏洩時での事実関係の迅速な公表と本人への速やかな通知等が定められている。

金融機関では、個人情報保護の趣旨に沿って、組織内の管理体制を整備しており、保護体制に遺漏の無いよう努めている。しかしながら、個人データの流失事件が相次いで発生している現状に鑑み、システム監査の立場からも、管理体制の改善について積極的な提言が求められよう。なお、アウトソーシングが進み、業務を委託するケースが増加している。このため、業務委託先への厳しい管理・監督責任を求める必要がある。「委託先評価表」の作成や、場合によっては、アウトソーシング先の企業にもシステム監査の実施を求めることとなろう[27]。

iii）預金者保護法（偽造・盗難カード法）

これまで、民法 478 条の規定や、カード取引規定において[28]、免責とされてきた偽造・盗難カードの補償問題は、これまでの「原則補償しない」から「原則補償」へと、法の組み換えが行われることになった。

今般、偽造・盗難キャッシュ・カードによる被害を、金融機関が補償する預金者保護法が成立し（2005 年 8 月 3 日）、2006 年 2 月施行されることになった。補償の程度は、預金者の過失の有無によることになるが、過失が無ければ、金融機関の全額補償が基本的な考え方である。なお、過失かどうかは、金融機関による立証責任が課せられている[29]。

金融機関としても、さらなる安全対策の強化と預金者への防犯に対する啓蒙を図ることが必要である。法律問題であると同時に、顧客を巻き込んだ管理問題でもあり、早急の対策を取らねばならない。これの契機に、キャッシュ・カードから IC(Integrated Circuit)カードへの切り替えに、弾みがつくものと考えられる。

3・システム監査強化のための具体例

現在の金融機関で、速やかに解決しなければならない問題について、システム監査の立場から下記の 3 点を取り上げておきたい[30]。

① 情報の紛失・漏洩

金融庁が、個人情報保護法の施行に合わせて、金融機関に対し個人情報の管理体制を

一斉点検させた結果を公表している(2005年4月1日時点の点検結果)[31]。これによれば、1,069機関のうち、287機関(26.8%)において、個人データの紛失が明らかとなった。紛失の資料の類型は、書類が215機関、コムフィッシュ163機関と多く、そのほかCD-ROM(Compact Disk-Read Only Memory)やフロッピーディスクの紛失があげられている。これらの個人情報先数は、約678万先で、うち紛失・所在不明が約677.8万先である。そのほか、誤送信・誤送付よるものが約2,000先、盗難が1先となっている。平素から厳正な管理を求められている金融機関においてさえ、このような状況にある。こうした事態に鑑みて、顧客への対応と再発防止のための内部体制の整備が早急に求められている。具体的には、行内に委員会組織を立ち上げ、委員長にはトップ・マネジメントに着いてもらうほか、その委員には情報、事務、コンプライアンス等の各担当役員を含めることが必要である。委員会に権限を与え、強力なリーダーシップのもとで、管理体制を早急に構築しなければならない。各部門およびアウトソーシング先も含めて、その職務分担、チェック体制、責任等、実施に当たって明確に規定することも重要である。なお、これらの推進体制や管理体制については、外部のコンサルタントや監査人等の意見も出来るだけ聴取しておきたい。

一般に情報の紛失・漏洩には、過失によるものと故意によるものとがある。前者には、文書の保存・保管ルールの不徹底による紛失、文書の廃棄、文書の外部持ち出し・紛失、パソコンの盗難・紛失、磁気テープの紛失、アドレスの読み違いによる誤送信といったものがある。これらの過失事故への対策は、平素からの職員への教育と意識徹底が不可欠である。もちろん、管理体制も見直す必要がある。特に、最近の職員は、総合職、一般職、嘱託(定年退職者の再雇用等)、パートタイマー、アルバイト、外部派遣職員、アウトソーサー職員等により構成されている。職務遂行に当たっての意識、責任感、忠誠心は区々であり、人事管理や人事教育、事務研修において、何をしっかり教育すべきか、受講者によって明確に焦点を絞ることも必要である。画一的な人事管理、教育から、対象者に合わせた指導や研修が求められている。外部社員については、平素から相手企業と綿密なコミュニケーションを図り、些細な事でも気になるところは、芽の小さいうちに摘み取る心構えが大事である。

一方、後者には職員・外部派遣職員による個人データの検索入手後、名簿業者などへの販売、データの入った文書・パソコンの盗み出し、そして愉快犯による悪戯行為などがある。これに対しても、上述のように、さらなる職員の人事管理と行動管理が必要であろう。業務のアウトソーシングが進み、外部職員による業務処理が増えている。しかも、外部職員による事故が増加している状況から、効率性や経費削減という観点からだけではなく、厳正化や顧客サービスの視点から業務を見直すことも必要である。アウトソーシングに当たっては、委託契約において法曹専門家の意見を踏まえて、責任の所在を明確に定めることや、損害賠償についても契約で明らかにしておかねばならない。また、損害保険の付保も検討に値するであろう。

② キャッシュ・カードの偽造対策

キャッシュ・カードの偽造問題は、今に始まったことではない。1980 年代にいくつかの偽造事件が発生している。旧日本電信電話公社(現 NTT)の職員が、通信回線からカードの取引信号音を盗聴･解析し、預金者の暗証番号を割り出して、犯行に及んでいる。また、ある銀行への派遣プログラマーが、預金者の口座情報を検索し、これをコピーする手口で、預金の引き出しを行った事件がある。さらに、顧客の暗証番号等の個人情報を盗み出した、メーカーの元銀行担当技術者が、磁気エンコーダーで情報を入力し、エンボッサーを用いてニセのカードを作った事件もある[32]。このようなことから、キャッシュ・カードの中に、暗証番号を記録しておくことは改められ、1988 年以降、暗証番号の記録域にゼロを入れることになっている。そのとき以前のカードを所有し、今日まで一度も使用していなければ、現在においても暗証番号がカードに記録されていることになる[33]。

今日の問題は、何らかの方法で、預金者のみが承知している暗証番号を探り出し、偽造カードを作成して、盗難を行う事件が多発していることである。たとえば、最近、「スキミング」により　ゴルフ場を舞台に暗証番号を探り出し、偽造カードを作成し、顧客の預金口座から、ATM を利用して預金の引き出しを行っていたグループが逮捕されている[34]。

スキミング被害が社会問題化し、預金者保護のための法律も生まれたが、カードが偽造されること自体が、銀行の「製造物責任」ともいえる考え方に立っている。顧客の無過失が証明できれば、全額補償されることになる。今後、金融機関としても、顧客と共に盗難･偽造に対処する方法を実践していく必要がある。

現在、考えられる対処策について、下記の表 3 にまとめた。偽造カードの対処策は、暗証番号の厳重な管理が、もっとも大事であるが、「スキミング」などの技術を悪用するケースもあり、無過失の被害が発生している。生体認証技術も活用されているが、たとえば、指紋認証などは、指紋の偽造が出来るとの専門家の意見がある[35]。犯罪の技術も、日々進化し、これとの対応を迫られている。

なお、現在 IC カードを導入している銀行は 6 行で、2005 年度中に 18 行が導入予定である[36]。生体認証装置を備える銀行も増えており、すでに、調査金融機関 350 のうち、5.7%が実施中で、16％が導入予定である[37]。既存のキャッシュ・カードの枚数が多く、これらの IC カードへの切替や、全ての ATM へのソフト組込などにより、コストが嵩むことから、これまで、金融機関では慎重な対応がとられてきたといえる。しかし、偽造カード問題の解決のため、今後、IC カード化への動きが一層進むと思われる。ただ、利用促進に当たっては、機能の説明を十分に行い、顧客の意向を確認の上、進めることが必要である。

表３・金融機関と預金者の偽造カード対策

当事者	対処策	緊急度
金融機関が行う諸施策または管理策	①　類推されやすい暗証番号の変更を顧客に要請。（生年月日、電話番号、自家用車の番号、単純な連続番号は不可）	(A)
	②　預金契約の約款文言の変更。（預金者保護法に則した変更）	(A)
	③　取引限度額の設定可能の対応。（一日当りの利用限度額を、銀行が設定）	(A)
	④　ATM 利用明細の自宅送付、またはメール送信。（利用明細書の厳正な管理）	(A)
	⑤　カードの有効期限導入。（切替時からの設定）	(B)
	⑥　一日の引き出し限度額の任意設定。（個人の申出による設定）	(A)
	⑦　生体認証の採用。（手の平と指によるものあり）	(B)
	⑧　IC カードの採用。（切替が進行中）	(B)
	⑨　ATM 画面表示の工夫により、外部から認識不明の表示。	(A)
	⑩　遮光フィルターの採用や隠しカメラの設置。	(A)
	⑪　長期間 ATM 不使用の預金者には、窓口誘導により対応。	(B)
預金者が行う管理策	①　暗証番号の厳正かつ適切な管理。（他人に知られない管理）	(A)
	②　類推されやすい暗証番号の変更。（生年月日、電話番号、自動車番号などの変更）	(A)
	③　適時、預金残高の確認。（不審な出金のチェックにより、リスクを抑制する）	(A)
	④　利用限度額の設定管理。（多額の引出不可の設定）	(A)
	⑤　生体認証や IC カードへの切換え申出。	(B)
	⑥　利用明細をシュレッダーで処理。（手がかりを、他人に与えない）	(A)

（出典: 金融情報システム白書(2005)pp.5-13 参照のうえ筆者編集作成。また、日本経済新

聞 2005 年 1 月 26 日、同 2005 年 2 月 13 日、および日経金融新聞 2005 年 2 月 3 日なども参考にした。なお、各項目ごとに、緊急度の高いものを A、段階的に進めるものに B の符号を付した。）

③　ネットワーク犯罪

ネットバンキングは、新しい業務分野であり、その利便性により、多くの顧客に利用されている。しかし、新しい技術だけに、セキュリティ面で、まだまだ問題も抱えている。最近の事例には、「スパイウェア」を悪用し、不正引き出しの事件が発生している。

2005 年 7 月に、イーバンク銀行、みずほ銀行およびジャパンネット銀行において、同様の不正引き出し事件が発見されている[38]。この事件では、被害者のパソコンから、キーボードで入力した情報を自動的に記録し、ネットを通じて第三者に流す「スパイウェア」が発見されている。それによりパスワードを盗み出し、犯人が預金者になりすまして、預金を引き出したとみられている。

なお、現在の対策としては、次のものが挙げられている[39]。

a)　利用しているプロバイダーや携帯電話会社以外の取引制限。
b)　複数の「合言葉」を登録し、接続ごとに違った言葉を求める認証方式。
c)　使用パソコンの事前登録。
d)　振込み限度額の設定。
e)　被害補償のための損害保険加入。

このうち、a, c, d, e は、速やかに対応を図るべきと考える。d については、法人と個人とで利用金額に差があることから、顧客のニーズを確認のうえ対応しなければならない。利便性を充分に考慮することが求められている。

なお、最近では、金融機関のセキュリティ対策も進歩しており、たとえば、ネットバンキングのパスワードを、最大 32 桁まで自由に設定できる銀行がある。また、使い捨てパスワードを生成する装置を貸し出す銀行もある[40]。使いやすく、安全なものが普及すると考えられる。

偽造キャッシュ・カードは、銀行が原則補償することになったが、ネットバンキングに於ける犯罪は、別の問題である。今後の対応策が望まれている。

4・システム監査の体制強化の具体的措置

上述してきたとおり、システム監査人として学ぶべきことが多く、しかも多様な諸問題に対応するため、体制を一層充実させる必要がある。その考慮点を以下に論ずる。

①　業務の多様化に耐えうる人材の育成

銀行情報システムの歴史的な発展過程をみると、初期段階における、業務のバッチ処理システムから、勘定系のオンラインシステムへと進化した。その後、業務の国際化に伴い、国際系システムや、証券業務の充実による証券系システムなどが開発された。集中管理型システムばかりでなく、現在では、EUC など分散型システムも多用されるようになっている。このことは、新しいシステムリスクを抱えることになったといえる。

システム監査に際しても、利用部門の多様化、情報システムの高度化、広範囲にわたる諸規定・マニュアル等を対象としなければならない。これに対応できる、監査体制の充実、有能な人材の確保が望まれている。当初、検査部門の付属的な立場から小規模な組織でスタートしているが、現時点では、その重要性に鑑みて充分な要員と体制が必要となっている。また、監査人自身においても、日々進歩するシステム技術について研鑽に努めると共に、経営、業務や法務に関して幅広く知識を深めることが求められている。なお、自己研鑽のみでは限界があり、研修会や学会への参加、海外留学などの機会を与える必要がある。そのためには、システム監査部門への特別な教育投資予算枠を設けるとともに、教育や研修のための休暇制度など強制的に与えることも必要であろう。要は、強化部門としてのシステム監査組織に、他部門からの優秀かつ充分な人材の投入と、集中的な教育投資が不可欠であろう。

② 結果監査より予防監査への移行

監査というと、事後的なチェックや評価を行うと見られているが、これは誤った考え方である。結果監査は、監査し易いという利点があるが、開発プロジェクト等のトラブル防止の意味では遅すぎる。むしろ今後は、「予防監査」ともいえる、情報システムの企画･開発の段階から参画して、その都度、意見具申していくことが必要である。プロジェクトの上流工程におけるリスク量が、全体の約 70％という指摘もあり、監査の対象としても考慮する必要がある[41]。

また、システム関連のプロジェクトが大きいほど、開発の過程での計画変更は、担当者に大きな負担をかける。もしも、開発過程途中での大幅な変更が必要となれば、開発期間の延長やコストの増加は避けられない。こうした事態が生じないように、開発当初から、システム監査部門もプロジェクトに参画しておくことが望ましい。そのためには、システム監査部門の要員に、プロジェクトに参画させられるだけの余裕が必要となる。アウトソーシングの活用による合理化の結果、捻出された要員から適当な人材を配置換えすることも一考に値する。

なお、システム監査人の立場から見ても、開発当事者との日頃のコミュニケーションが出来ている結果、相互の信頼関係が築けること、実効的な助言･勧告・提案が、適時可能となることから、有効に作用するものと考えられている。

③　トップ・マネジメントとの連携

システム監査の評価･提言は、その都度トップ・マネジメントに伝えられる。必要とあれば、遅滞無く改善・改革に、トップ・マネジメント自ら行動してもらうことが重要である。このためにも、監査人としては、公正･中立の立場から、的確に意見具申することが望まれる。トップ・マネジメント側での、迅速かつ的確な対応こそ、組織全体の活性化に結びつくものと思われる。あわせて、その場限りで終わらせることなく、システム監査人が指摘した事項のフォローアップも、欠かすことの出来ないものである。

一方、トップ・マネジメント側に、真摯な姿勢が無ければ、監査人の努力も生きてこないことになる。組織として機能していく体制は、いつにトップ・マネジメントに依存しているといえる[42)]。

なお、往々にしてトップ・マネジメントが情報システムに疎いことから、システム専担者に全てを任せてしまうケースがある。情報システムに対する理解がなければ、これからの経営者は務まらない。そのために、経営者に対する教育･研修も必要である。重要なのは、事の軽重を見極めることや、平素からシステムに関心を持ち続け、意思決定の場には必ず参加することである。その場合、判断に迷いがあれば、外部専門家等の意見や知識を活用することも大事である。

④　システム監査組織の見直し

システム監査の組織は、単に技術監査に止まらず、業務・マネジメントの観点からも評価できる体制が必要である。このため、一般監査、システム監査及び外部監査などの担当者が共同して監査に当たる、いわゆる混成チームによる監査も、今後は、必要になると思われる。

歴史的には、検査部門などに付属したシステム検査からスタートしている事例が多い。現在では、システム監査として、独立した組織を採るところが増加している。このことは、システム監査の重要性が評価されている結果である。

しかし、システム監査の対象が高度化、複雑化、多様化するにつれて、総合的な見地から監査意見を出すことが必要になってくる。この意味からも、各分野の専門家による共同作業や、外部監査人も含めた監査が求められよう。独立した一組織で、全てをこなす事はむつかしくなっており、監査テーマにより柔軟な混成組織による監査体制が、今後は必要となると考えられる。

5．監査体制強化を妨げる問題

システム監査体制を強化するために、金融検査マニュアルの考え方を尊重しつつ、各銀行では平素から体制の整備に努めている。しかし、最近の顧客情報漏洩事件が多発している現状などに鑑み、経営陣や幹部が、自行の管理体制にどれほど関心を持っているのか疑わしいところがある。組織や体制は確かに設けられているが、充分に機能しているとは思えない。「しっかりやってくれている」との思い込みや、自己満足で終始しているようにも思われる。

システム監査が機能しない理由を、組織・体制の面からさらに挙げると、ｉ）適正配置といいながら、優秀・適格な要員がシステム監査部門に少なく、人数だけが一応揃っている、ii）システム監査の総合力が求められている時代に、依然として、硬直的な体質を頑なに維持している、iii）下流工程の枝葉末節な部分の監査に終始し、リスク量の多い上流工程の監査に力を注がない、iv）上席者や周囲に気を遣い、的確･公正な意見具申の出来ない雰囲気がある、ｖ）人材育成制度は設けられているが、上席者や仲間に遠慮があり、運用しにくい職場環境にある、vi）経営陣は、システム監査の重要性は認識しているが、結果的には任せきりとなっているなどがある。

また、監査技術の問題もある。システム監査技術が伴わないために、問題の発見に力及ばぬことがある。たとえば、銀行の事例ではないが、誤入力のデータ訂正が出来ないとか、大量データに対してシステムの能力に限界があるなど、最近、大きく報道されたシステム障害事件があった[43]。こうした事故事例について、システム監査人は、鋭敏に反応し、自行ではどのようになっているのか、直ちに検証するぐらいの姿勢が求められる。システム監査の立場から、「他山の石」として参考にする姿勢がなければ、こうした事例も活かされない。

このように、システム監査体制の強化を妨げる、いくつかの問題点を指摘した。これら諸問題に対する適切なマネジメントが、システム監査を有効に機能せしめることになると考えられる。

以上のごとく、本稿では、システム監査を強化するための人材育成と組織の整備について論述し、この視点から問題提起を行った。なお、この研究を発展させるため、システム監査論、内部統制論、情報システム、マネジメント、組織論など総合的な観点からの分析が、求められることになる。本論文を踏まえて、学際的な研究が、さらに必要になると考える。

謝辞

本稿は、関西大学経済･政治研究所主催第 169 回産業セミナーにおいて、発表したものを基にしている。本稿作成にあたり、鵜飼康東関西大学ソシオネットワーク戦略研究センタ

一長より、ご指導を賜った。また、上田昌史氏(関西大学 RCSS、PD)、増本貴士氏(神戸学院大学研究員)、井口洋氏(元関西大学大学院商学研究科非常勤講師)より、示唆に富む助言を頂いた。竹村敏彦氏（関西大学 RCSS,PD）からは、度々、懇切な助言を頂いた。さらに、兼石一郎氏(元 D&I 情報システム株式会社常務取締役、現 IT コンサルタント)より、実務に即した適切なアドバイスを頂いた。ここに記して謝す。

なお、もし本文中に誤りがみられるとすれば、それは全て筆者の責任に帰すことであり、明記しておきたい。

注

1）金融情報システムセンター(2000)第 1 部 p.3。
FISC では、「情報システムリスク」という言葉を使っている。これは、狭義のオペレーショナル・リスクと考えたい。オペレーショナル・リスクのうち、システムリスク、事務リスク、人事管理･不正にかかるリスク、顧客取引にかかるリスク、法務・コンプライアンスにかかるリスク、災害リスク、規制･制度変更リスク、運営リスク等が、情報システムリスクに含まれる。(先端リスク研究会(2003)pp.82-87 参照。)

2）金融情報システムセンター(2000)第 2 部 p.1。

3）経済産業省「システム監査基準」による定義である（平成 8 年 1 月 30 日改定より引用)。なお、吉田洋(2002)pp.3-8 において、システム監査の定義について詳しく解説されている。
また、日本システム監査人協会(2002)pp.31-39 においても、定義、目的、効果などシステム監査の必要性が明解に論じられている。

4）木村剛(2001)p.9 において、ルールからの逸脱、誤謬･不正などを発見し、これを是正あるいは除去するのが「検査」であり、それに加えて、実態にそぐわなくなっているルールなどを発見し、是正･除去することまでの機能を含むのが「内部監査」であると解説している。つまり、「内部監査」においては、不正･誤謬の摘発だけで終わるのではなく、内部管理体制の評価と改善という重要な役割が求められている。
また、先端リスク研究会編(2003)pp.71-73 において、「検査から監査へ」について、明解に論じられている。

5）金融情報システムセンター(1990)p.218,p.327 参照。都市銀行での、実施事例が紹介されている。
また、金融情報システムセンター(2003)pp.20-21 において、平成 13 年 3 月時点でのアンケート結果が紹介されている。

6）平成 11 年 7 月金融監督庁（現金融庁）「預金等受入金融機関に係る検査マニュア

ル」いわゆる「金融検査マニュアル」を公表した。金融検査の基本的な考え方と、法令等遵守態勢の確認検査用チェックリストやリスク管理態勢の確認検査用チェックリストなどが示されている。

また、木村剛(2001)pp.91-136 で、この点について明解に解説されている。

7）監査の分類には、監査の内容による分類、監査主体による分類、監査主体の立場による分類、法的規制による分類がある。鈴木正也(1988)p.19-20 および監査法人トーマツ編(2003)pp.196-197 参照。

8）1985 年に「不正な財務報告に関する国家委員会」が米国で組織された。委員長の名をとって、一般に「トレッドウェイ委員会」と呼ばれている。この委員会が 1992 年に公表した内部統制のフレームワークは、「COSO レポート」として知られている。www.atmarkit.co.jp/aig/04biz/coso.html(2005/09/10 照会参照)

なお、COSO レポートは、内部統制のフレームワークに関する、デファクト・スタンダードといわれている（木村剛(2001)p.28 参照)。この COSO レポートについては、鳥羽至英、八田進二、高田敏文共訳(1996)がある。

9） 1975 年に G10 諸国の中央銀行総裁会議により設立された銀行監督当局の委員会の名称である。同委員会は、ベルギー、カナダ、フランス、ドイツ、イタリア、日本、ルクセンブルグ、オランダ、スエーデン、スイス、イギリス、米国の銀行監督当局ならびに中央銀行の上席代表により構成される。なお、委員会は通常バーゼルの国際決済銀行(Bank for International Settlements: BIS)において開催される。

(www.jiten.com/dicmi/docs/k26/20957s.htm 参照。2005/09/10 照会)

１０）大西基彦、長岡寿男(2003)pp.2-5 参照。

１１）平成 16 年 12 月 24 日金融庁公表「金融改革プログラム一金融サービス立国への挑戦一」。 http://www.fsa.go.jp/news/newsj/16/f-20041224-6.html(2005/08/04 照会)

１２）平成 17 年 7 月 27 日金融庁公表「金融検査指摘事例集」。
http://www.fsa.go.jp/news/newsj/17/f-20050727-2.html(2005/08/04 照会)

１３）金融情報システムセンター(2000)第 3 部チェックポイント集を参照。

１４）正職員の場合、採用時から一定の教育を重ねて受けており、就業規則の遵守について体得している。パートタイマーについても、基礎的な教育は行われており、就業時に、必要とする諸規則を徹底している。しかし、職務についての、忠誠心や責任感について、正職員と比較して見劣る場合がある。そのため、情報管理について、取扱範囲や責任について、明確に指導する必要がある。

１５）金融情報システムセンター(2000)、チェックポイント 9-3-A、9-3-B のインターネットセキュリティ参照。また、監査法人トーマツ編(2003)pp.251-272 参照。

１６）浜辺陽一郎(2005)pp.87-92 参照。

石島隆(2005)p.8 参照。

１７）浜辺陽一郎(2005)p.6 参照。
岡本享二(2005)p.41 参照。

１８）ソニー「Annual Report 2005」p.34 参照。このなかで、企業の社会的責任（CSR）について、コンプライアンス体制の強化を掲げている。

１９）甲賀、林口、外村(2002)p.2 では、コーポレートガバナンスとＩＴガバナンスは、別の概念としている。一方、石島(2005)p.10 において、ＩＴガバナンスは、コーポレートガバナンスの一部と考えている。

２０）大木栄二郎(2001)pp.83-86 参照。

２１）事故事例については、FISC が定期的に機関誌「金融情報システム」で紹介している。

また、那野比古(1985)も参考になる。この他、システムの脆弱性について、松田貴典(1999)がある。

インターリスク総研編(2002)は、多くのリスク事例を体系的に整理しており、実務に役立つものと考える。銀行における事故事例とその教訓については、長岡寿男(2003)pp.18-25、Nagaoka(2005)pp.17-24 がある。

２２）ＫＰＭＧビジネスアシュアランス(2004)p.15 参照。

２３）金融情報システムセンター(2000)のチェックポイント、要点項目 11：外部委託を参照されたし。
また、2001 年 4 月、金融検査マニュアルの改訂では、委託業務の所管部門などによる管理状況を、内部監査の対象とすべきことが明確化されている。さらに、2005 年 4 月の個人情報保護法施行に伴い、金融庁のガイドラインでは、外部委託に係る取扱規定を整備し、委託先における方針・個人データの取扱状況の点検および監査を行う必要があるとしている。外部委託を行う金融機関において、外部委託先の適切な管理状況の把握、検査を行うべしとしている（金融情報システム白書(2005)p.37 参照）。

２４）金融情報システムセンター(2002)pp.112-113 参照。

２５）金融情報システムセンター(2002)pp.157-158 参照。平成 13 年 7 月―平成 14 年 6 月の一年間の金融機関における出願公開件数は 330 件で、前年の 30 件を大幅に上回っている。

２６）長岡、増本、上田(2005)pp.5-13.参照。

２７）金融情報システムセンター(2000)、チェックポイント、要点項目:外部委託を参照。金融情報システムセンター(2005)、pp.36-37 参照。

２８）・民法 478 条（債権の準占有者に対する弁済）
「債権の準占有者に対してした弁済は、その弁済をした者が善意であり、かつ、過失がなかったときに限り、その効力を有する」

・また、カード規定には、次のように示されている。

(暗証番号等)

（1）カードは他人に使用されないよう保管してください。また、暗証は他人に知られないようにしてください。

（2）当行が、カードの電磁的記録によって、支払機･自動サービス機または振込機等の操作の際に使用されたカードを当行が交付したものとして処理し、入力された暗証と届出の暗証との一致を確認して預金の払戻し、その他当行所定の取引の取扱いをしたうえは、カードまたは暗証につき偽造、変造、盗用その他の事故があっても、そのために生じた損害については、当行および提携先は責任を負いません。ただし、この払戻しまたはその他当行所定の取引の取扱いが偽造カードによるものであり、カードおよび暗証の管理について預金者の責に帰すべき事由がなかったことを当行が確認できた場合の当行の責任については、この限りではありません。

（3）当行の窓口においてカードを確認し、払戻請求書、諸届その他の書類に使用された暗証と届出の暗証との一致を確認のうえ取扱いました場合にも前項と同様とします。

（出典：旧大和銀行のダイワキャッシュサービスカード規定より引用）

２９）日本経済新聞 2005 年 08 月 04 日朝刊 3 ページ。金融情報システムセンター(2005)pp.11-13 参照。

３０）情報の漏洩問題事件は、銀行においても多発している。また、キャッシュ・カードの偽造事件も社会問題化している。このため、預金者を保護する法律が生まれている。これらの管理強化が、現在の銀行において重要なテーマとなっている。また、ネットワーク犯罪は、近時発生している事件であり、如何に管理すべきか注目されている。この観点から、3 点に絞って取上げている。

３１）平成 17 年 7 月 22 日付け、金融庁「金融機関における個人情報管理態勢に係る一斉点検の結果等について」を参照。
http://www.fsa.go.jp/news/newsj/17/f-20050722－4.html（2005.08.04 照会）

３２）那野比古(1985)pp.45-48,pp87-90 参照。
日本経済新聞 2005 年 04 月 14 日朝刊 7 ページ参照。

３３）日本経済新聞 2005 年 04 月 14 日朝刊 7 ページ。

３４）柳田邦男(2004)pp.107-116 において、事件の内容が明記されている。また、最近のキャッシュ・カードに関する事故事例も数多く紹介されている。本書は、偽造カードについて、預金者保護の立場から、問題の深刻さを世に明らかにし、預金者保護法成立へのインパクトを与えたと考えられる。

３５）日本経済新聞 2005 年 08 月 17 日朝刊より参照。

３６）日本経済新聞 2005 年 04 月 16 日朝刊 7 ページ参照。

３７）日本経済新聞 2006 年 2 月 10 日参照。日本経済新聞社が 2005 年 11 月 29 日―12 月 13 日に実施したアンケート調査により、350 金融機関から回答があったもの。

３８）日経産業新聞 2005 年 07 月 15 日 24 ページ参照。

３９）日本経済新聞 2005 年 07 月 10 日朝刊 3 ページ参照。

４０）日本経済新聞 2006 年 2 月 5 日参照。

４１） 先端リスク研究会(2003), pp.301-304.参照。

４２）中央青山監査法人経営監査グループ(2002)pp.194-196。ここでは、経営監査のベストプラクティスの事例として、UFJ、トヨタ、ソニーの内部監査体制が紹介されている。しかし、このなかで内部統制組織を確立していたとされる UFJ において、金融庁に対する検査忌避行為が見られ、これを指示した一部の経営者や幹部が刑事告発された(日本経済新聞社編(2004)pp.142-159 参照)。

４３）東京証券取引所において、2005 年 12 月、みずほ証券が誤発注を行い、注文の取消が出来ず、その結果市場が混乱した。また、2006 年 1 月、ライブドア問題で、システム能力の限界から、取引の停止を行った（日本経済新聞 2006 年 2 月 5 日、同 2 月 7 日参照)。

参考文献

石島隆(2005)、『情報システムの内部統制』中央経済社。

インターリスク総研編(2002)、『実践リスクマネジメント』経済法令研究会。

大木栄二郎(2001)、『経営戦略としての情報セキュリティ』工業調査会。

大西基彦、長岡寿男(2003)、「日本の金融機関におけるシステム監査の現状と課題」関西大学ソシオネットワーク戦略研究センター、ディスカッションペーパー第 10 号。

岡本享二(2005)、『CSR 入門』日本経済新聞社。

監査法人トーマツ編(2003)、『セキュリティ・マネジメント戦略』日本経済新聞社。

木村剛(2001)、『新しい金融検査と内部監査』経済法令研究会。

金融情報システムセンター(1990)、『金融機関等のシステム監査実践例集』金融情報システムセンター。

金融情報システムセンター(2000)、『金融機関のシステム監査指針』金融情報システムセンター。

金融情報システムセンター(2002)、(2005)、『金融情報システム白書』財経詳報社。

金融情報システムセンター(2003)、「金融情報システム」増刊 53 号、通巻 263 号、金融情報システムセンター。

KPMG ビジネスアシュアランス(株)(2004)、『情報セキュリティ監査制度』中央経済社。
甲賀憲二、林口英治、外村俊之(2002)、『IT ガバナンス』NTT 出版。
鈴木正也(1988)、『システム監査概論』学文社。
先端リスク研究会編(2003)、『システムリスクに挑む』金融財政事情研究会。
中央青山監査法人経営監査グループ(2002)、『コーポレートガバナンスと経営監査』東洋経済新報社。
鳥羽至英、八田進二、高田敏文共訳(2001)、『内部統制の統合的枠組み』白桃書房。
長岡寿男(2003)、第 1 部「銀行業情報システム投資の歴史と現状」pp.1-57、鵜飼康東編、『銀行業における情報システム投資の経済分析』多賀出版。
Nagaoka.H(2004),「Strategy of Information System for Japanese Banking Industry」RCSS of Kansai University, Discussion Paper Series No.18.
長岡寿男、増本貴士、上田昌史(2004)、「知的財産権のマネジメント―権利保護関係の視点からの分析―」関西大学ソシオネットワーク戦略研究センター、第 25 号、pp.3-13.
Nagaoka.H,Ukai.Y,Takemura.T(2005),"Past and Present of Information Systems in Banks" and "Information System Strategy of Nationwide Banks" in Ukai.Y (ed.) *Economic Analysis of Information System Investment in Banking Industry,* Springer-Varlag,Tokyo,Japan,pp.3-52.
那野比古(1985)、『コンピュータパニック』中公文庫。
日本経済新聞社編(2004)、『UFJ 三菱東京統合』日本経済新聞社。
日本システム監査人協会編(2002)、『情報システム監査実践マニュアル』工業調査会。
浜辺陽一郎(2005)、『コンプライアンスの考え方』中公新書。
松田貴典(1999)、『情報システムの脆弱性』白桃書房。
柳田邦男(2004)、『キャシュカードがあぶない』文藝春秋。
吉田洋(2002)、『情報システム監査』税務経理協会。