博士学位論文

金融情報システムにおける経営戦略としてのリスクマネジメントの体系化及びその実践

2015 年 3 月

慶應義塾大学大学院システムデザイン・マネジメント研究科
システムデザイン・マネジメント専攻

遠藤 正之

要旨

我が国の金融事業者が運営する情報システム（以下金融情報システム）は、経済の様々な変化への対応と安定的な稼働の双方を要請される「基幹インフラ」であり、その重要性が高まっている。金融情報システムは顧客の財産情報を扱いつつ、広範囲の異質な決済ネットワークにつながるなど、複雑かつ大規模なシステムであるとともに、高度な信頼性・安定性を要求されるシステムであり、リスクマネジメントの難易度が格段に高い。

その一方で、経営戦略としての金融情報システムのリスクマネジメントにどう取り組むべきかという経営者向けのガイドラインは、未だ明確な形では示されておらず、経営者視点でのリスクマネジメントの研究も十分に行われていなかった。そこで、本論文では、経営戦略としての金融情報システムのリスクマネジメントの包括的な枠組みとして、「リスクマネジメント戦略の 6 観点(CORE-OQ)」を提案し、その枠組みについて、情報システム開発に関与する金融機関従業員を対象とした問題意識調査による妥当性検証、企業の取組みの調査による事例検証、クラウド技術、情報セキュリティ最新動向、地銀共同化、リスクアペタイト・フレームワーク等の経営環境変化への検討を行った上で、金融情報システムのリスクマネジメントの体系化と評価を行うものである。

本論文の結論となる「リスクマネジメント戦略の 6 観点(CORE-OQ)」は、経営者が金融情報システムのリスクマネジメントを行うにあたって、最低限意識すべき項目を集約したものであり、以下の 6 項目である。

１）経営トップのコミットメントと支援（Commitment）、

２）適切な組織体制整備による IT ガバナンス強化（「組織体制と IT ガバナンス」）（Organization）、

３）経営 IT リスクの適切な評価と対策の構築（「IT リスクマネジメント」）（IT Risk Management）、

４）経営戦略に合致した業務拡張性及びシステムの一貫性の確保による二重投資の排除（「拡張性一貫性確保」）（Extensibility）、

５）外部関係者の要請と IT のケイパビリティの間をつなぐ要件定義最適化（非機能要件を含む）（「要件定義最適化」）（Optimization）、

６）品質重視の仕組構築（Quality）。

以上の各項目の英字の頭文字を取って、金融情報システムのコアとなるものとの意味も込め、「CORE-OQ」(コア OQ)と命名する。

Risk management of financial information systems as a corporate strategy and practical implementation

ABSTRACT

Information systems in financial companies in Japan have been important as a critical infrastructure component that should be flexible enough to adapt to changes in the economy while also maintaining stable operations. Financial information systems therefore had to be able to manage risks with complicated transactions dealing with customers' assets and connect with a wide and diverse set of networks. However, there is a lack of effective guidelines in terms of corporate strategies for managing risks in operating financial information systems to support executive managers that are relevant not only to daily operations but also basic studies of risk management from the viewpoint of executive managers. Therefore, this thesis aims to address these gaps by presenting six indispensable and comprehensive viewpoints for managing risks within financial information systems as a means to build corporate strategy.
The six viewpoints comprise
1) **Commitment**, that accounts for the commitment and support of top management;
2) **Organization**, or the organizational system and governance for information technology (IT);
3) **IT Risk management** for the evaluation and control of risk;
4) **Extensibility** so that the system configuration can change depending on the business strategy;
5) **Optimization** that considers stakeholders' requirements and current level of IT competence; and
6) **Quality**-oriented systems (CORE-OQ).
The proposed CORE-OQ framework was tested using both data collected through a questionnaire survey of managers or affiliated members of financial companies and actual corporate activities. The framework takes various environmental changes into account, such as cloud technology, recent information security accidents, M&A case studies, and the risk appetite framework.

第1章 序論

1.1. 研究の背景と意義

我が国の金融システムは、グローバリゼーションの進展によるボーダレス化と情報通信技術の発展により、世界経済の変動からの影響を直接受けるなど大きく変貌している。それに伴い、金融事業者が運営する情報システム（以下金融情報システム）は、経済の様々な変化への対応と安定的な稼働の双方を要請される「金融機関経営の基幹インフラ」[（財）金融情報システムセンター, 2012]としての、重要性をますます増してきている。金融情報システムは顧客の財産情報を扱いつつ、広範囲の異質な決済ネットワークにつながるなど、複雑かつ大規模なシステムであるとともに、高度な信頼性・安定性を要求されるシステムであり、リスクマネジメントの難易度が格段に高い [遠藤正之、高野研一, 2013a]。その一方で、従来、経営戦略としての金融情報システムのリスクマネジメントにどう取り組むべきかという経営者向けのガイドラインは、未だ明確な形では示されておらず、経営者視点でのリスクマネジメントの研究も十分に行われていなかった。そこで、本論文では、経営戦略としての金融情報システムのリスクマネジメントの包括的な枠組みを提案し、その枠組みについて、情報システム開発に関与する金融機関従業員を対象とした問題意識調査による妥当性検証や、実際の取組みを広汎に調査することによる事例検証を行った上で、金融情報システムのリスクマネジメントの体系化と評価を行うものである。

1.2. 用語の定義

本論文は、経営学、金融、情報システムの多領域をカバーする学際的な視点からの成果であるとともに、実務家への提言もその目的としており、様々な読者を想定している。そこで、本節では、本論文での主要な用語について、様々な分野の研究者や専門家の間の認識の統一を図るため、用語の定義を行う。

1.2.1. 戦略、経営戦略

戦略には様々な定義があるが、最もシンプルなものとして、「企業が考えた競争に成功するためのセオリー」 [Barney.J., 2002]との定義を採用し、組織経営における戦略を経営戦略とする。経営戦略には、企業戦略と事業戦略が含まれる。

1.2.2. 金融情報システム

金融事業者が保有ないし、運営する情報システムのことを言う。その中でも、本論文が主要な研究対象として想定しているのは、リアルタイムの決済処理を行うシステムや、顧客の財産情報を保有し、他のシステムやネットワークと連携する大規模なシステムである。

1.2.3. リスク

リスクに関して、リスクマネジメントの国際規格である ISO31000 [『ISO31000(英和対訳版)』, 2009]では、「目的に対する不確かさの影響」と定義している。従来のマイナスの結果を産むリスク（純粋リスク）のみならず、ビジネス展開や経営戦略上の意思決定に伴ってリスク負担した結果、プラスの側面につながるような場合のリスク（投機的リスク）の双方を対象とする [亀井克之, 2011]ものである。これは、リスクには二面性があることを意識したものである。

本論文でも、システム障害発生のようなマイナスの結果を産むリスク（純粋リスク）と、ビジネスの拡大や経営戦略実現を目的とする IT 投資に代表されるようにプラスの側面につながるようなリスク（投機的リスク）の双方をリスクとして捉える。ただし、文脈によっては、マイナスの結果を産むリスクのみに焦点を当てて論じる場合もあり、その際は、「マイナスの結果を産むリスク」ないしは、「純粋リスク」との表記で明示する。

なお、金融情報システムのリスクは、オペレーショナルリスク、ビジネスリスク、戦略リスク、風評リスク、法務・規制リスク等に細分化できるが、その点は、2.3 節で説明する。

1.2.4. リスクマネジメント（広義、狭義）

リスクマネジメントとは、「リスクに関して組織を指揮し統制する調整された活動」[『ISO31000(英和対訳版)』, 2009]である。本論文では、前項で述べたリスクの二面性に対応して、リスクマネジメントを 2 種類の意味で用いている。まず、「広義のリスクマネジメント」は、マイナスの結果を産むリスク（純粋リスク）と、プラスの側面につながるリスク（投機的リスク）の両面を勘案したリスクマネジメントのことであり、経営や経営戦略とも密接に関わるものである。いかにリスクを取って収益を上げるかをマネジメントすることでもあり、経営戦略そのものとほぼ同義とも言える。本論文の表題の「金融情報システムにおける経営戦略としてのリスクマネジメント」は、金融情報システムにおける広義のリスクマネジメントを論じていることを明示したものである。一方、「狭義のリス

クマネジメント」は、システム障害、システム性能不十分、システム開発プロジェクトの失敗等のマイナスの事象を防止するための、マネジメントとして定義する。本論文では、特記ない場合は、「広義のリスクマネジメント」であるとする。

1.2.5. IT、ICT

IT（Information Technology）は、情報技術と情報技術を用いたアプリケーションやサービスの総体とする [向正道, 2013]。また、ICT（Information and Communication Technology）（情報通信技術）という言葉も最近使われるようになってきた。IT はコミュニケーションを支援することを目的の一つとしており、IT と ICT と区別をすることにそれほど意味はない [向正道, 2013]との考えに従い、本論文では、「IT」の表記で統一する。ただし、先行文献からの引用については、先行文献の表記を優先する。

1.2.6. ガバナンス、IT ガバナンス、マネジメント

ガバナンスとは、「組織が方向づけられ、統制される仕組みないしはシステムである」[経済産業省, 2010]とする。そして、IT ガバナンスは、「企業が IT に関する企画・導入・運営および活用を行うにあたって、すべての活動、成果及び関係者を適正に統制し、目指すべき姿へと導くための仕組みを組織に組み込むこと、または組み込まれた状態」 [小池聖一・パウロ他, 2011]とする。

マネジメントは、経営と管理の両方の意味があるが、本論文では、特記しない限り、管理の意味で用いる。

尚、大企業での相次ぐ不正発生の中でコーポレートガバナンスへの関心が高まり、企業統治として取締役会が行うガバナンスと、経営執行としてのマネジメントの分離が図られており、その意味でガバナンスとマネジメントを区別する考え方もあるが、本論文では必ずしもそのような区別は意識していない。

1.2.7. CEO、CIO

CEO とは、Chief Executive Officer の略。最高経営責任者。企業の経営トップのことを言う。

CIO とは、Chief Information Officer の略。最高情報責任者。IT・システム統括役員すなわち情報システム部門を統括する役員のことを言う。

1.2.8. 金融情報システムの失敗

ある金融情報システムを原因として、外部から直接評価されるリスク（マイナスの結果を産むリスク、純粋リスク）起因の事象が顕在化した場合、その金融情報システムの失敗と定義する。顕在化の典型例は、マスコミ等で取り上げられ、対外的に表面化した場合である。 [遠藤正之、高野研一, 2013a]

1.2.9. 金融情報システム開発の失敗

金融情報システム開発の失敗とは、対外的には失敗であることが表面化していない場合も含め、システム開発プロジェクトに関して、計画時の工期ないし、予算を守れないか、品質に不満があると評価されたシステム開発と定義する。また、工期及び予算を達成し、品質についても満足との評価があっても、外部から直接評価されるマイナスのリスクがマスコミ等で取り上げられて、対外的に表面化した場合（金融情報システムの失敗）も、金融情報システム開発の失敗でもあるとする。逆に、金融情報システム開発の成功とは、計画時の工期及び予算を達成し、品質についても満足と評価され、外部から直接評価されるリスクも顕在化していないシステム開発と定義する。 [遠藤正之、高野研一, 2013a]

1.3. 研究の目的と対象範囲

1.3.1. 研究の目的

本研究は、我が国の社会経済のインフラの一つである金融情報システムに関して、金融情報システムが金融機関の経営戦略へ貢献するための、リスクマネジメントの包括的な枠組みを構築することを目的とする。更に、この枠組みの普及により、金融情報システムの開発過程、運用保守局面での経営者の関与とリスクマネジメント（広義）を高度化し、金融情報システムによるビジネス価値増大につなげることを最終目的とする。

1.3.2. 研究の対象範囲

金融業には、様々な業態があり、その情報システムも多様である（2.2 節で詳述する）が、本論文の研究対象としては、金融機関等コンピュータシステムの安全対策基準・解説書（第８版） [（財）金融情報システムセンター, 2011a]が対象としている以下の情報システム及びハードウェア、ソフトウェアを対象とする。

１）顧客にオンラインサービスを提供するコンピュータシステム(業務系基幹オンラインコンピュータ・システム)、

２）他の金融機関等との決済業務に使用するコンピュータシステム(資金決済システム等)、

３）顧客データを扱うコンピュータシステム、

４）サービスを提供するために金融機関等が顧客に提供するハードウェア、ソフトウェア。

1.4. 主要な先行研究

金融情報システムのリスクマネジメントに関する先行研究は大きく分けると以下の五類型に分類できる［遠藤正之、高野研一, 2013a］。

１）問題点指摘型、

２）体制・リーダーシップ依存型、

３）事故事例分析型、

４）管理態勢構築型、

５）具体策提言型。

1.4.1. 問題点指摘型

第一の類型として、従来の金融情報システムが経営戦略と結びついていなかったという問題点を指摘し、経営者の対応を促す研究がある。問題点指摘型と言える。

奥田は、IT の発展と金融のグローバル化の影響を、欧米での金融業界の対応と対比させ、「米国の銀行のような大胆な長期的戦略に立って継続的に投資を続け、産業界全体の活力増強にも貢献したのとは程遠いのが現状である」と事務効率化や省力化が IT 投資の主目的だったと指摘し、情報・知識産業として IT 活用に向けた推進体制の整備、人材の確保養成が必要であるとしている［奥田晃司, 2005］。

また、富永は、日本銀行の IT リスク考査に関わってきた経験から、金融機関の IT リスク管理について、以下の 10 個の問題点を指摘している［富永新, 2009］。

１）攻めと守りのバランス、

２）スピードとクオリティのバランス、

３）経営効率と戦略適合性のバランス、

４）事前予防と事後対策のバランス、

５）サービス水準や利便性とコスト負担のバランス、

６）公共性と収益性のバランス、

７）時代変化に適合したルール設計と市場の自由や自己規律のバランス、

８）テクノロジー（技術）とマネジメント（人）のバランス、

９）自前（内製）とアウトソーシング（外部委託）のバランス、

１０）メインフレームとオープン・クラウド系システムのバランス。

また、金融情報システムの問題の本質として、利用者の高い要求に応え金融機関としての信頼性を確保すべく精緻な仕組みを作りこんでおり、繊細で難しいという点や、「守りの IT 投資が経費負担として重くのしかかっていることも金融機関の収益性が向上しない一因かもしれない」といった点を指摘している。更にオープン系システムとホスト系システムのリスク管理上のポイントを纏めており、大規模化、複雑化の進展や、アウトソーシングや共同化によるリスク、システム統合プロジェクトの進め方、事業継続管理まで言及し、社会全体の金融リスクに対する考え方を変革することを提言している。

1.4.2. 体制・リーダーシップ依存型

第二の類型として、CIO（Chief Information Officer、最高情報責任者、IT・システム統括役員）を中心とした体制面やリーダーシップが解決策であると結論付けたものがある。体制・リーダーシップ依存型と言える。

森は、米銀で CEO と並んで経営上大きな役割を担い、IT・システムを統括する CIO を邦銀でも確立させることで、顧客価値創造を目的とした経営戦略と整合性のある IT 戦略を CIO に策定させ、企業価値の創造を果たすべきと指摘している［森俊也, 2006]。

宮坂らは、IT システム統合プログラムのリーダーシップに焦点をあて、その中で金融情報システムの IT 統合の成功事例と失敗事例の比較分析を行っている。経営トップの自社 IT システムの理解や、経営判断による危機感の共有、IT 戦略に対する直接のコミットメント等が重要としている［宮坂美樹、山本秀男, 2010]。更に経営トップの行動がプログラムマネージャーである CIO へどのように波及していくかを変革期と定着期にかけてのリーダーシップモデルで示し、CIO の創発的行動が組織にとって重要であることを示している。

西岡は、銀行の情報システム統合の 3 事例（成功 2 事例、失敗 1 事例）を分析する中で、経営トップの関与とリーダーシップに加え、より現場に近いポジションにいる CIO がプロジェクトの鍵を握る役割を果たすとしている［西岡茂樹, 2013]。

1.4.3. 事故事例分析型

第三の類型として、金融情報システム事故事例から分析を行うものがある。事故事例分析型と命名できる。

坂東らは、金融情報システムの障害に関しての新聞報道について、7 年間の障害に関して、顧客サービス関連、業務処理関連、共通、犯罪の 4 カテゴリーで分類の上、その報道での取り扱いの大きさ（ニュース性）と障害自体の重大性レベルが必ずしも一致しないことから、その差異の原因を分析している［坂東幸一、田中健次, 2009a］。

更に、金融情報システムと通信ネットワークを比較した上で安全性を高めるための重点事項として、プログラム品質向上、過負荷対策、ハードウェアの信頼性向上、ヒューマンエラー対策、犯罪行為への対策の 5 点が改善課題であると纏めている［坂東幸一、田中健次, 2009b］。

日本銀行によれば、金融情報システムの障害発生要因をハードウェア障害、ソフトウェア障害、システム性能に起因した障害、運用保守に起因した障害の 4 種類に大別して、システムリスク管理の体制プロセスの整備、システム開発管理、情報セキュリティ管理、システム障害管理、システム運用管理の 5 つに分けて対策を提言している［日本銀行金融機構局, 2007a］。

1.4.4. 管理態勢構築型

第四の類型は、経営としての情報システム管理態勢構築を提言するものである。言わば管理体制構築型である。

大橋は、IT 投資を業務処理の効率化から、収益増大を含めた資本効率化にシフトする必要があるが、IT 投資額と資本効率との間に相関関係は無く、むしろ IT 活用の管理が資本効率には重要であるとしている［大橋利夫, 2001］。

渡辺は、金融情報システムに関わる狭義のリスクマネジメントすなわちマイナスの結果を産む情報システムリスクについて、情報システムの企画・開発・運用に関わる人材のスキル、IT アウトソーシング等の組織の開発・運用体制といった観点に着目して纏めている［渡辺研司, 2005］。具体的には、マルチベンダーに対する管理能力の欠如、業務・システム経験の欠如、IT オフショアリング、ユーザー検収における責任体制の欠如、大規模で複雑なプロジェクトを管理できる PM 人材・スキル不足等を挙げ、それらをビジネス継続マネジメントの観点で、経営戦略の課題として捉えることが重要であるとしている。

1.4.5. 具体策提案型

第五の類型は、マイナスの結果を産むリスク（純粋リスク）を低減する手法を具体的に提案するものであり、言わば具体策提案型である。最近、金融情報システムの障害事例が話題になったこともあり、このタイプのものが増える傾向にある。

益田らは、金融情報システムのシステム間のインターフェース部分の障害に対し、化学プラントプロセスで用いられる HAZOP 手法により、潜在的な危険を回避できるとしている［益田美貴，高野研一, 2010]。更にそれを発展させ、大規模な情報処理システムの業務継続計画でのビジネスインパクト分析に対し、HAZOP 手法を取り入れることを提案している［益田美貴，高野研一, 2011]。

経済産業省の「IT 経営ロードマップ改訂版」では、IT 投資が「守りの投資」が中心であるという問題意識から、先進企業の攻めの取組みを整理した 10 カ条の「IT 経営憲章」を掲げており、全産業向けではあるが、事例として金融業に関しても 4 例掲載している［経済産業省, 2010]。10 カ条は、以下の通りであるが、経営者向けのメッセージである（3.1.1 項で詳述)。

１）経営と IT の融合、
２）改革のリード、
３）優先順位の明確化、
４）見える化、
５）共有化、
６）柔軟化、
７）CIO と高度人材の育成、
８）リスク管理、
９）環境への配慮、
１０）国内企業全体の底上げ。

情報処理推進機構では、2005 年 7 月から 2010 年 1 月に発生した障害事例を分析し、障害再発防止策を記載した上で、システム開発において、経営層、事業部門、情報システム部門、IT ベンダー毎の役割を明確にし、管理フレームを導入することで、ソフトウェアの信頼性を高めることができると提言（3.1.2 項で詳述）し、金融事業者の取組み事例を

例示している [独立行政法人情報処理推進機構ソフトウェア・エンジニアリング・センター(IPA SEC) , 2011]。

日本銀行では、金融機関のシステム障害管理体制の実効性確保に向けた留意点として、「障害発生の未然防止対策」「障害発生時の対応」「障害管理に対する経営陣の関与」の 3 つの観点から取り纏めている [日本銀行金融機構局, 2012]。

情報処理推進機構では、「障害管理」の取組みが進んでいる 8 社（金融 3 社、運輸 2 社、製造 3 社）の企業事例をもとに、「障害管理の取組み」と「障害が防止できなかった備え」「障害管理フレームワーク」に関して、事業者への提言を纏めている [独立行政法人情報処理推進機構技術本部ソフトウェア・エンジニアリング・センター, 2012a]及び [独立行政法人情報処理推進機構技術本部ソフトウェア・エンジニアリング・センター, 2012b]。

米国では、金融に限定せずに情報システム全般に関して、重視すべき観点を列挙して考察するような研究が行われている。

Manfreda らは、情報システム全般に関して、トップマネジメントとシステム部門職員との関係において、9 つの要素が重要であるとしている。それは、以下である [Manfreda,A.and Stemberger,M., 2014]。

1）トップの支援、
2）相互の信頼感、
3）情報システムの価値の認知、
4）技術知識、
5）職務知識、
6）経営知識、
7）技術の役割、
8）支援の役割、
9）職務の役割。

Young らは、同じく情報システムプロジェクト全般に対して、5 つの要素が重要成功要因であるとしている。それは、以下である [Young, R.and Jordan,M., 2008]。

1）プロジェクト方法論、
2）ユーザーの関与、
3）トップマネジメントの支援、

4）ハイレベルの計画、

5）プロジェクトスタッフ。

Doll は、情報システムへのトップマネジメントの関与の重要性を論じ、以下の 4 つを挙げている [Doll,W., 1985]。

1）ステアリングコミッティー

2）計画の文書化

3）優先順位の合意

4）長期的財源。

1.4.6. 先行研究に対する本論文の特色

以上の 5 つの類型の先行研究は、本研究でもその多くが、参考とはなるものの、本論文の目的とする、金融情報システムにおける経営戦略としてのリスクマネジメントの指針を構築するにあたっては、網羅性やアプローチの論理性という観点では不十分であると考えられる。第一の問題点指摘型は、経営者が果たすべき解決策の提言が不十分である。第二の体制・リーダーシップ依存型は、事例の成功や失敗を体制面や属人的なリーダーシップに起因するものとする傾向があり、一般の経営者にとっての指針にはなりにくい。第三の事故事例分析型は、マイナスの結果を産むリスク（純粋リスク）に関して、過去に発生した事故の類型により分析をする点で参考になるが、プラスのリスク（投機的リスク）の考慮が不十分であり、経営レベルでの現状の指針となるものではない。第四の管理態勢構築型は、論点それぞれは有意義だが、管理面に重点を置く議論であるため、経営理念の浸透や、組織を構成する人材の士気向上施策等の考慮が、経営戦略としては必要であり、その点で不十分である。最後の第五の具体策提言型も一定の局面では有効であるが、経営戦略を実現する目的には、更に上位レベルの理念や方針までがつながった施策が必要と考えられる点で不十分であると考える。

本論文の問題意識は、経営者が経営戦略の一環として、金融情報システムのリスクマネジメントを行うための体系化を図ることである。そのためには、経営者がプラスのリスク（投機的リスク）とマイナスの結果を産むリスク（純粋リスク）の両面を把握して、リスクマネジメントを行う中で、金融情報システムに関しても、その特性を把握した上で、経営戦略としてのリスクマネジメントを行うことが望まれる。そのことが、金融情報システ

ムの健全な発展にもつながると考える。また、体制や属人的なリーダーシップに依存するのではなく、経営視点でリスクをマネジメントするための指針となる枠組みが必要である。

本論文はそのような金融情報システムにおける経営戦略としてのリスクマネジメントの観点を、先行研究の 5 つの類型を更に発展させ体系化する初めての試みである。このような包括的な提言はこれまで成されておらず、この課題全体の問題定義からリスクマネジメントの実践に至るまでのプロセスを明らかにすることで、学術的かつ実務的貢献を果たすものと考える。

1.5. 論文の構成

本論文は 6 つの章で構成される。各章の概略は、以下の記述の通りであるが、先行研究の 5 つの類型を取り込んだ上で、議論を発展させ、金融情報システムにおける経営戦略としてのリスクマネジメントの体系化を図っている。

「第 1 章 序論」（本章）では、論文の全体像を提示する。具体的には、研究の背景と意義、用語の定義、研究の目的と対象範囲、主要な先行研究、論文の構成について述べる。

「第 2 章 金融情報システムのリスクマネジメントの現状と課題」では、我が国金融システムとその中で特に金融情報システムの現状、金融情報システムの概観、金融情報システムに関するリスク、金融情報システムの問題構造とリスクマネジメントの課題を明らかにする。先行研究のうち、管理態勢構築型の研究の成果を金融情報システムに関するリスクに取り込み、問題点指摘型の研究のエッセンスを金融情報システムの問題構造に取り込む。

「第 3 章 リスクマネジメント戦略の構築」では、まず、経営戦略に対する金融情報システムのリスクマネジメント要求項目を、具体策提案型の先行研究、システム監査関連基準、成功事例から広く収集する。その上でそれら要求項目を整理体系化するものとして、リスクマネジメント戦略の 6 観点(CORE-OQ)を仮説設定し、開発局面と運用局面での適用について検証する。特に開発局面では、情報システム開発に関与する金融機関従業員を対象とした問題意識調査での妥当性検証を実施しており、その分析を行う。運用局面については、2011 年の大手銀行の障害を機に整備された障害管理体制の構築に関して事故事例分析型の文献を採り上げ考察する。

「第 4 章 経営戦略の実現に向けたリスクマネジメントの実践」では、第 3 章とは逆に、経営戦略の実現に向けて、金融情報システム側の貢献の視点で検討する。経営戦略、IT 戦略、金融情報システムの関係をモデル化した上で、取組み事例として、東京証券取引所

の事例と、オンライン証券 5 社の事例を検討する。リスクマネジメント戦略の 6 観点(CORE-OQ)に対する企業 CIO の評価についても言及する。

「第 5 章 金融情報システムのリスクマネジメントの体系化と評価」については、システム監査関連基準で見たリスクマネジメント、経営者から見た金融情報システムのリスクマネジメント、組織マネジメントの視点でのリスクマネジメント、最近の環境変化へのリスクマネジメントの対応を通して、リスクマネジメント戦略の 6 観点(CORE-OQ)の評価を行う。先行研究のうち、体制・リーダーシップ依存型の研究を経営者から見た金融情報システムのリスクマネジメントの考察に生かしている。

「第 6 章 結論」では、本研究の結論をまとめた上で、今後に残された課題についても明示して、論文を収束させる。

以上の 6 章建ての論文となるが、各章の関係を図示したものが図 1 である。特に第 3 章から第 5 章までで、仮説の「リスクマネジメント戦略の 6 観点（CORE-OQ)」を様々な観点で検証する構成である。その観点で、本論文を V モデルの形でまとめたのが、図 2 である。

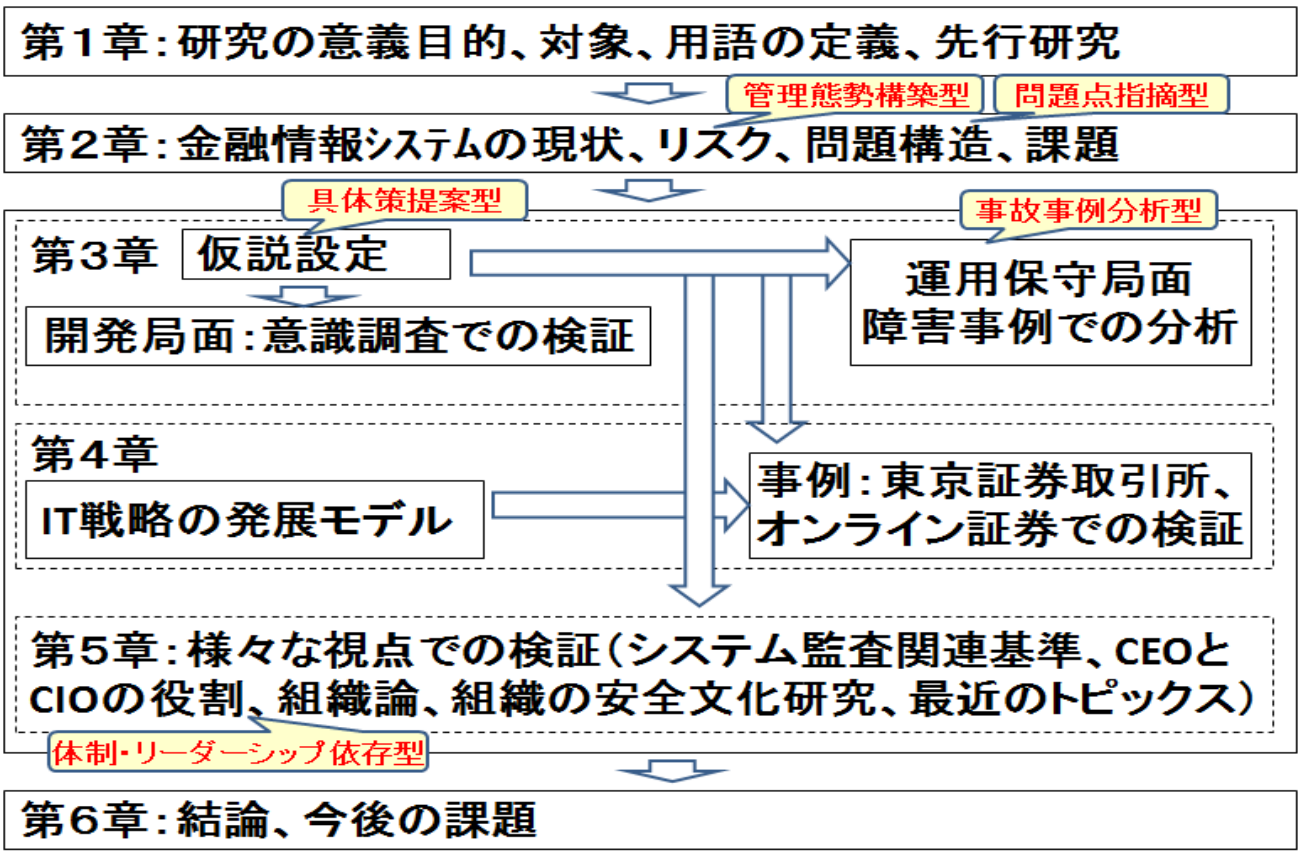


図 1 論文の構成

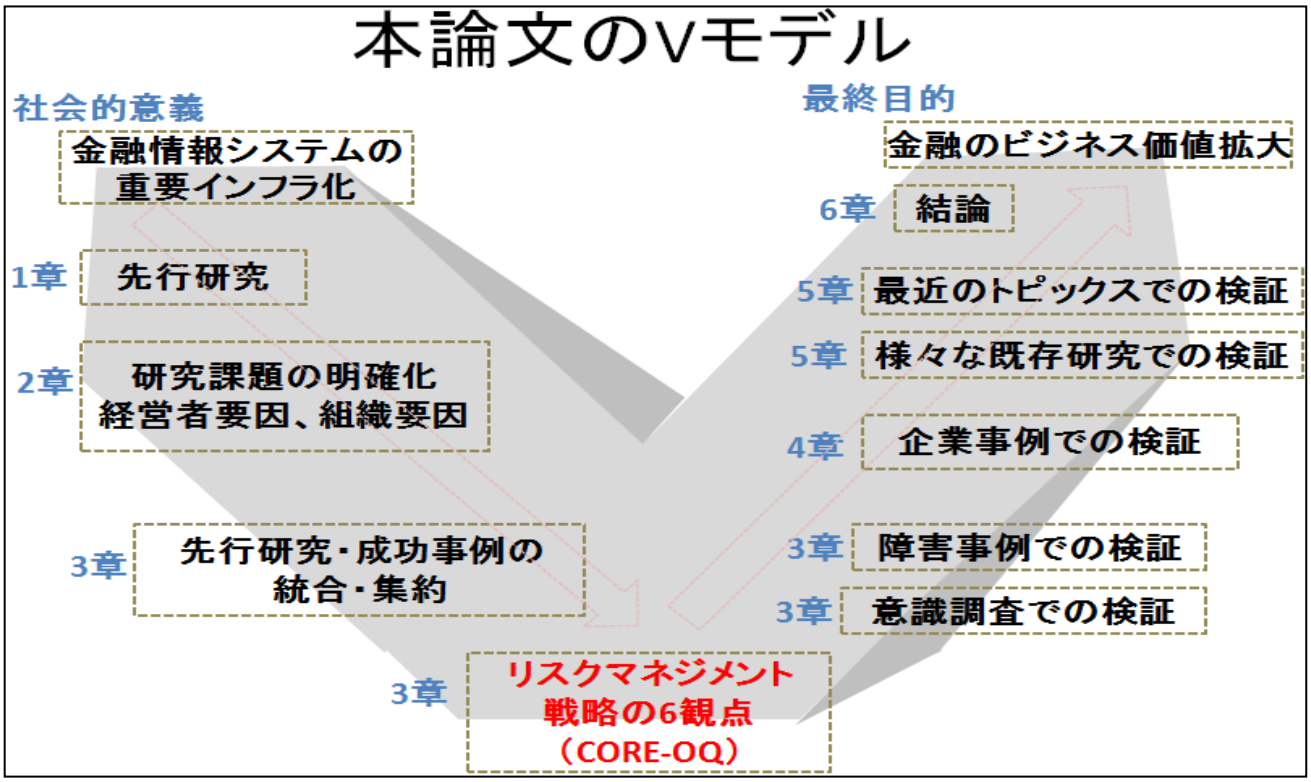


図 2 本論文の V モデル

第2章 金融情報システムのリスクマネジメントの現状と課題

2.1. 我が国金融システムと金融情報システムの現状[1]

我が国の金融システム[2]は、銀行部門と市場部門に大別することができる［日本型金融システムと行政の将来ビジョン懇話会, 2002] [金融審議会金融分科会基本問題懇談会, 2009]。

銀行部門は、銀行業務の典型である資金余剰者と資金不足者の仲介を行う間接金融を中心とした金融形態であり、産業金融モデルとも言われる。一方、市場部門は、資金余剰者と資金不足者が証券市場の価格メカニズムを通して、資金調達や有価証券売買を行う直接金融の金融形態であり、市場金融モデルとも言われる[3]。銀行部門と市場部門は、ともに国際的な金融規制強化や市場競争激化といったボーダレス化と情報通信技術発展の影響により、ビジネスモデルは大きく変貌せざるを得なくなってきている。

銀行部門（産業金融モデル）については、ボーダレス化により、バーゼル銀行監督委員会の自己資本規制・流動性規制の見直しによる国際的な金融規制が強化される一方で、情報通信技術の発展により決済インフラとしての重要性が高まっている。しかしながら、銀行の金融情報システムは、1980 年代に構築されたホストコンピュータシステムを核にして、その後の金融業務の複雑化や多様化に対応して機能別のサブシステムを付け足しており、全体として、複雑かつ大規模なシステム構成になっている。大手銀行は独力で金融情報システムの開発を行い続けているが、地方銀行では単独行でシステム投資を負担できないケースも生じ、アウトソーシングの一形態であるシステムの共同化の動きが加速してきた［岩佐智仁, 2011] [大和田尚孝, 2010a] [日本銀行金融機構局, 2009] [日本銀行金融機構局, 2014]。更に直接、顧客と決済を行うチャネルとしての、エレクトロニックバンキングやインターネットバンキングの流れも加速している。

市場部門（市場金融モデル）では、情報通信技術の発展により、1990 年代から欧米において、オプション取引や先物取引を組み合わせた様々なデリバティブ商品や証券化商品が開発された点も大きな変化である。またネットワーク高速化により、株式取引についても市場のある国内で取引をする必然性が無くなり、国際的な市場間競争が激化し、市場イン

---

[1] 本節は、「金融事業経営における情報システム開発のリスクマネジメント観点の提案」［遠藤正之、高野研一, 2013a]を元にしている。

[2] この金融システムとは、情報システムのことではなく、法制度を含めた金融全体の体系のことである。

[3] 実際には銀行での投資信託販売に見られるような「市場型間接金融」という中間形態が拡大している。［池尾和人＋財務省財務総合政策研究所, 2006]との指摘がある通り、中間的な形態もある。

フラとしての取引所システムの強化が図られていった。東京証券取引所で 2010 年 1 月に稼働した株式売買システム「arrowhead」や、大阪証券取引所で 2011 年 2 月に稼働したデリバティブ売買システム「J-GATE」はその代表例である。証券会社も取引所のシステム更改に合わせたシステム投資を行うことが求められ、システム投資の負担が経営体力を超えるような中小証券会社を中心に再編淘汰も進んでいる。証券取引所自体でも国境を越える合従連衡の動きが発生しているが、その一因は、システム投資金額増加をカバーするための規模の経済を狙った点にある。

金融システムの変化に対応して、金融情報システムへの経営や業務部門からの要求が多様化高度化するとともに、金融経済活動の社会インフラとしての重要性が増してきている。その一方で、様々な要求を満たすことや、新旧システムの混在により、情報システム自体が複雑化しており、情報システムに関するリスクマネジメント実施の難易度は高まっている。また金融情報システムのトラブルは社会的に多大な影響を与えるため、一旦事故が起こるとその金融情報システムでサービスを提供している金融事業者の経営を揺るがしかねない状況に発展する。ビジネスチャンスの喪失やサービスの信頼性低下やサービス自体の廃止に繋がり、経営者の交代、経営形態の変更に至ることもある。情報システムのリスクマネジメントの巧拙が、金融事業者の競争力の優劣に大きな影響を与えると言っても過言ではない。

2.2. 金融情報システムの概観[4]

一言で金融情報システムと言っても、実は我が国の金融情報システムは様々な業態で構築運営されている。具体的な金融情報システムの類型と内容は、毎年出版される金融情報システム白書 [（財）金融情報システムセンター, 2012]に体系的、網羅的に記載されている。

2.2.1. 個別金融機関等のシステム

個別金融機関等のシステムは、銀行、信託銀行、信用金庫・信用組合等協同組織金融機関、生命保険会社、損害保険会社、証券会社、クレジットカード会社、信販会社、消費者金融会社、ゆうちょ銀行、かんぽ生命等の情報システムである。システム構成、デリバリーチャネル等の業態別概要を表 1 に示す。

[4] 本節は「金融情報システム開発戦略におけるリスクマネジメント」[遠藤正之, 2011]を元にしている。

表 1 金融情報システムの概要(個別金融機関)

業　態	システムの構成等の概要
銀行	業務系システム群（勘定系システム、資金証券系システム、国際系システム、対外接続系システム等）、情報系システム群、事務系システム群（営業店システム、集中センターシステム等）。デリバリーチャネルは、ATM、インターネットバンキング/モバイルバンキング、コールセンター。
信託銀行	銀行と同様のシステム群に加え、財産管理系(信託)システムがある。 デリバリーチャネルは、銀行と同様。
協同組織金融機関	システム構成、デリバリーチャネルは銀行とほぼ同様。業態別に共同運営を行う。具体的には信用金庫のしんきん情報システムセンター、信用組合の全信組センター、労働金庫のユニティ、農業協同組合の全国統一システムである。
生命保険会社	業務系システム群（契約管理システム、保険料収納システム、保険金支払いシステム等）、情報系システム群、資産運用系システム群。デリバリーチャネルは、CD/ATM、インターネット、コールセンター。
損害保険会社	業務系システム群（契約管理システム、保険料収納システム、事故サービスシステム等）、情報系システム群、代理店システム、資産運用系システム群。デリバリーチャネルはインターネット、コールセンター。
証券会社	業務系システム群（注文約定処理システム、営業店事務処理システム、顧客管理システム、経営管理システム、コンプライアンスシステム等）、情報系システム群（投資情報システム、銘柄情報システム、経済金融情報システム、営業支援システム等）、その他システム群（国際系システム、対外接続系システム、ディーリング・トレーディングシステム等）。デリバリーチャネルは、ATM、インターネット、コールセンター、銀行等の金融商品仲介業者。
クレジットカード、信販会社	クレジットカード会社の場合、新規顧客受付更新システム、カード利用与信管理システム、売上処理システム・精算システム、債権管理システム。 信販会社の場合、売上処理システム、個品あっせんに関するシステム。デリバリーチャネルは、CD/ATM、インターネット、電話。
消費者金融	新規顧客受付関連システム、カード発行関連システム、債権管理関連システム。デリバリーチャネルは、自動契約機、CD/ATM、インターネット、電話。
ゆうちょ銀行	郵便貯金システム（平成 16 年から第４次オンラインシステム）
かんぽ生命保険	業務処理系システム（契約保全、保険業務全般を行うシステム）、情報分析系システム（平成 21 年から、第 5 次オンラインシステム）

(金融情報システム白書平成 25 年版［（財）金融情報システムセンター, 2012]による)

詳細の説明は本論文では行わないが、同一業態でも実際のシステムの構成はさまざまである。例えば銀行では、メガバンクが単独でシステムを構築している一方で、地域銀行の多くは、システム投資削減のためシステムを共同化し、ベンダーに基幹システムの開発運用全般を運営委託する形態を取っている。また、2.1 節では、金融事業者のリスクを銀行部門、市場部門に分けて説明したが、金融事業者は必ずしも片方のみを考慮すれば良いわけではない点にも注意すべきである。例えば、銀行部門を代表する銀行のシステム構成に

は、資金証券系システムという、市場に直結する金融情報システムが含まれている。銀行の経営者が行うリスクマネジメントは、相対取引を基本とする銀行部門のリスクのみならず、価格形成メカニズムによって取引を行う市場部門のリスクについても視野に入れる必要があることを示唆している。

2.2.2. 金融機関相互のネットワーク

金融システムのインフラとして、個別金融機関のシステムとは別に、金融機関相互の決済、情報提供のネットワークが構築されている。ネットワークの種類と概要を表 2 に示す。

表 2 金融情報システムの概要(金融機関等相互のネットワーク)

ネットワーク	システム構成の概要、ネットワークの種類
日銀ネット	当座預金系システム（日銀ネット当預系）、国債系システム（日銀ネット国債系）
全銀システム	全国銀行データ通信システム、国際的な決済等のネットワーク（CLS[5]システム、SWIFT[6]）、CD/ATM ネットワーク
国際的決済ネットワーク	日銀ネットでの外国為替円決済制度、CLS システム、SWIFT
CD/ATM ネットワーク	MICS[7]全国キャッシュサービス（業態別 9 ネットワークを接続）
保険会社ネットワーク	生命保険会社（生保共同センター）、損害保険会社（損害保険ネットワークシステム）
証券取引ネットワーク	㈱証券保管振替機構が運営するシステム（決済照合システム、株式等振替システム、一般債短期社債振替システム、投信振替システム）、㈱証券クリアリング機構が運営するシステム（金融商品取引清算・決済システム）
証券取引所	東京証券取引所や大阪証券取引所等の売買システム、清算システム、東証の相場報道システム、大証 FX システム等のシステム。
取引所以外の有価証券流通市場	店頭取扱有価証券の売買等に関するシステム（銘柄情報開示システム、適時情報伝達システム）、私設取引システム（PTS[8]）に関するシステム、債権店頭市場システム（国内債取引システム、取引情報配信システム）
金融商品取引ネットワーク	金利先物等取引のシステム（取引所システム、参加者システム）、取引所為替証拠金取引のシステム
個人信用情報機関	全国銀行個人信用情報センター、シーアイシー、日本信用情報機構

（金融情報システム白書平成 25 年版［（財）金融情報システムセンター, 2012]による）

[5] Continuous Linked Settlement
[6] The Society for Worldwide Interbank Financial Telecommunication s.c.r.l
[7] Multi Integrated Cash Service
[8] Proprietary Trading System

銀行部門と市場部門に 2 分類するという本論文の見方をすれば、市場部門の金融情報システムネットワークは、証券取引ネットワーク、証券取引所、取引所以外の有価証券流通市場、金融商品取引ネットワークである。中でも取引所以外の有価証券流通市場に関しては、平成 10 年に、証券取引の取引所集中義務が撤廃され、私設取引システム(PTS)が証券業の一つとして位置づけられ、現在2社が稼働している。これは金融のグローバリゼーションによるボーダレス化の変化が、市場部門の競争の範囲を広げているという 2.1 節の説明と連動した動きである。

2.3. 金融情報システムに関するリスク

金融事業者のリスクカテゴリーを示した先行研究としては、以下のものがある [遠藤正之, 2011]。

Michel らは、金融業におけるリスクをオペレーショナルリスク、ビジネスリスク、戦略リスク、風評リスク、法務・規制リスク、市場リスク、信用リスク、流動性リスクの 8 カテゴリーに分け、更に「リスクを防衛的な意味だけで理解してはいけない。…収益に関連してリスクを前向きに選ぶことができるということが、永続的に成功するすべての企業の経営管理プロセスの中心に位置するのである。」としている [Michel Crouhy、Dan Galai、Robert Mark, 2005]。

齋藤は、内部監査の観点からリスクを以下の 10 カテゴリーとした。すなわち戦略リスク、事業リスク、オペレーショナルリスク、財務/財務報告リスク、ディスクロージャーリスク、市場リスク、法的リスク、IT リスク、災害リスク、不正リスクの 10 カテゴリーである [齋藤正章, 2009]。

また IT リスクに絞った研究として、島田は、戦略性リスク、有効性リスク、効率性リスク、セキュリティリスク、コンプライアンスリスクの 5 種類を示している。ただしリスクの分類には明確な基準はなく、事業体ごとに決定すべきであるとも記述している [島田裕次, 2009]。

また、金融機関経営の観点からは、金融情報システムセンター（FISC）では、信用リスク、市場リスク、流動性リスク、オペレーショナルリスクを挙げている [（財）金融情報システムセンター, 2012]。

以上リスクに対する分類法は、研究者の視点によって異なるが、本論文では経営者の立場を意識した分類であるという点と、プラスの側面につながるようなリスク（投機的リス

ク）を明示的に意識しているという理由から、最初に記述した Michel らのリスクカテゴリーを導入する。

さて、金融事業者のリスクは、金融情報システムとの関係で、表 3 に示すように、二つのタイプに分類できると考える。 [遠藤正之、高野研一, 2013b] [遠藤正之, 2011]

第一のタイプは、金融情報システムが外部のステークホルダーに利用され、それ自体の可用性や信頼性に関して外部から直接評価されるタイプのリスクである。このタイプのリスクとしては、オペレーショナルリスク、ビジネスリスク、戦略リスク、風評リスク、法務・規制リスクが該当し、本論文で詳細に検討する対象となる。このタイプは、リスクのプラスマイナス両面で言えば、純粋リスクの面が多いが、投機的リスクも含んでいる。

第二のタイプは、金融システムの経営上重要なリスクに対し、金融情報システムが経営判断をサポートするタイプのリスクである。金融業はリスクを取り、それを管理することによって収益を得る [日本型金融システムと行政の将来ビジョン懇話会, 2002]と言われるが、金融事業経営の本質は、豊富な情報を用いてリスクを評価し、社会全体のリスクをコントロールすることで、収益を上げることである。第二のタイプのリスクには、市場リスク、信用リスク、流動性リスクが該当し、金融情報システムは、リスクの正確な情報をタイムリーに経営に対して提供することが要請されている。このタイプはリスクのプラスマイナス両面で言えば、純粋リスクと投機的リスク双方を含むものである。

表 3 金融事業者のリスク

金融情報システムとの関係でのタイプ	リスクカテゴリー	リスク内容（純粋リスク）
Ⅰ.金融情報システム自体が､外部から直接評価されるタイプ	オペレーショナルリスク	システム障害、情報漏洩、事務ミス、不正
	ビジネスリスク	顧客ニーズとの不適合、提供タイミングを逃す
	戦略リスク	投資途上での中断、利用されないシステム、二重投資の発生
	風評リスク	企業イメージの低下や信用の低下による競合への取引流出
	法務・規制リスク	契約が法律や規制と合致しないことで、損害を受けるリスク
Ⅱ.金融情報システムが経営判断をサポートするタイプ	市場リスク	金融市場における価格・相場の変化で資産の価値が減少する
	信用リスク	カウンターパーティの信用力劣化により資産の価値が減少する
	流動性リスク	市場で市場価格での決済や資金調達取引ができない

金融事業者のリスクを考える際に、ストック中心のビジネスで相対取引を基本とする銀行部門と、フロー中心のビジネスで市場での価格形成メカニズムによって取引を行う市場部門とでは、金融情報システムに限っても純粋リスクの重点が異なると考える。銀行部門は、相対取引で多数かつさまざまな顧客の金融ニーズに対応していることが特徴である。そのため、主体となる組織の信用が重要で、風評リスクを重視している。銀行部門の金融情報システムに関しても、事務ミス、不正、システム障害による風評リスクが、重要である。

一方、市場部門の金融情報システムは、価格形成メカニズムを提供する点で、市場へのリアルタイムのアクセスが要求される点が最大の特徴であり、それを阻害する事象の発生は、ビジネスの停止につながることから、ビジネスリスクが最も重要なリスクである。

以下では、銀行部門と市場部門のそれぞれに対して、リスクカテゴリー別に、金融情報システムが与える影響を中心に説明する [遠藤正之, 2011]。

2.3.1. オペレーショナルリスク

銀行部門のオペレーショナルリスクには、事務面での不完全さ、不正、人的ミスに起因するリスクと並んで、不適切なシステムに起因するシステムリスクを挙げることができる。システム障害による業務の中断(みずほ銀行の 2011 年 3 月の口座振替遅延、ATM 中断 [中田敦、大和田尚孝, 2011a]、ゆうちょ銀行の 2010 年 7 月の対外系ダウンと ATM 障害 [吉田洋平, 2010]）が典型例であるが、不完全なアクセスシステムに起因する情報漏洩(アリコジャパンの大量顧客情報漏洩 [中井奨, 2009])や、計算処理の誤りの発生に伴う損失発生（かんぽ生命での特約還付金の間違い [矢口竜太郎, 2008]）がこの中に含まれる。

市場部門において、オペレーショナルリスクに含まれる金融情報システムのリスクとして、市場自体の中断や、証券会社のシステム障害によるサービスの停止が挙げられる。市場自体の中断の例として、東京証券取引所の 2005 年 11 月のシステム障害による市場取引全面停止 [大和田尚孝, 2010b]が挙げられる。また、証券会社のシステム障害によるサービス停止の典型例としては、楽天証券の 2008 年 11 月のサービス停止がある [市嶋洋平, 2008]。

2.3.2. ビジネスリスク

ビジネスリスクは幅広い概念であり、金融情報システムに関係するものと、そうでないものとがある。代表例として、商品やサービス（含む情報システム）が顧客ニーズにマッ

チせず、またタイムリーな提供タイミングを逃すことにより、ビジネスとして成功しなかったり、計画した利益を得ることができなかったりするリスクが、挙げられる。後述する戦略リスクや風評リスクもビジネスリスクに含むと考えることもできる。特に、ウォーターフォール型[9]の開発の場合、金融情報システムの開発段階で要件が適切に把握できていない場合、リリース後にビジネスリスクが顕在化する可能性がある。

さらに市場部門においては、金融情報システム障害による取引停止自体が、手数料獲得の取引チャンスを失うという点で、ビジネスリスクの顕在化と考えることができ、銀行部門以上に、ビジネスリスクに直結しやすいと言える。2.3.1 項のオペレーショナルリスクの事例は、ビジネスリスクも顕在化させていると言える。

2.3.3. 戦略リスク

戦略リスクとは、戦略自体の成功と収益の不確実性が高い重要な投資のリスクである [Michel Crouhy、Dan Galai、Robert Mark, 2005]。金融情報システム開発においては、大規模な投資が発生するが、十分な効果を得られない可能性があるというリスクである。すなわち IT 戦略が経営戦略とマッチしていないため、システム開発途上での中断、二重投資の発生、また開発されてもビジネスで利用されないシステムの発生等のリスクである。銀行部門においては、スルガ銀行が、勘定系システムの刷新プロジェクトで導入決定したパッケージのカスタマイズに難航し、開発を取り止めた結果、100 億円を超える損失発生につながった事件が最近の代表例である [安藤正芳, 2007] [大和田尚孝、中井奨, 2010b]。

市場部門においては、外国為替証拠金取引（FX）サービス大手の外為どっとコムが、トラブルの多発した主力サービスそのものの停止に追い込まれた事例が典型例である [中井奨, 2010a] [中井奨, 2010b]。

一方で、優れた金融情報システムを持つことは、戦略の選択肢を増やすことができ、その意味で、戦略リスクの低減を図ることができる。例えば 2010 年に完成した東京証券取引所の株式売買システム「arrowhead」は、単なる金融情報システムというだけでなく、その高速性と信頼性を武器に、取引の拡大を可能とし [大和田尚孝, 2010b]、更に大阪証券取引所とのアライアンス戦略を可能にした点でプラスの側面につながったと言える。

[9] 設計・プログラミング・テスト等の工程を明確に分け、各工程で定められた成果物作成がすべて完了してから次工程作業に進むプロセスを取る開発手法。

2.3.4. 風評リスク

風評リスクは、その組織が信頼性に欠けると顧客、社会、市場から判断されるリスクである。信用が土台となる金融ビジネスの性格上、信頼性が損なわれることは避ける必要があるため、経営者が特に注意しているものである。金融システムに関しては、事故や障害の発生が大きく報道されることで、前述のオペレーショナルリスクを超えて影響範囲が広がる点が重要である。銀行部門について、みずほ銀行の 2002 年と 2011 年のシステム障害［日経コンピュータ, 2002] [中田敦、大和田尚孝, 2011a] [中田敦、大和田尚孝, 2011b] はその典型例である。

市場部門においては、ビジネスリスク顕在化が風評リスクに直結することが多い点に留意が必要である。例えば証券取引所の場合、市場間競争が激化しており、システム障害による取引所の信用力が低下すると、執行市場が私設取引所に移ったり、国内の上場企業の上場先がアジア市場に分散したりするといった影響が発生する。システム障害は、報道されることでこのリスクの顕在化に直結する。またオンライン証券におけるシステム障害によるサービス中断は、自社の代替手段が無いだけに、信用の低下に繋がりやすい。システム障害以外の事例としては、顧客情報の漏洩により、社会からの信用を損なうことがある。例えば 2009 年の三菱 UFJ 証券の事例［大和田尚孝、中井奨, 2010b]は、金融情報システムが顧客の財産に関わる情報を持つというリスクがクローズアップされた典型例である。

2.3.5. 法務・規制リスク

金融情報システム開発のカウンターパーティに対して、契約の不履行に関する訴訟に発展する法務リスクがある。銀行部門では、前述のスルガ銀行が勘定系システムの刷新プロジェクト取り止めに関し、日本 IBM に対して訴訟を起こしている例が挙げられる。システム開発の失敗に対し、スルガ銀行は、「開発契約は請負契約だった」と主張し、日本 IBM は「準委任契約であり自社の役割は果たした」と反論し、係争中である［大和田尚孝、吉田洋平, 2010a]。

市場部門の場合、カウンターパーティや投資家が取引で損失を発生した場合に、金融情報システムの提供者を訴えるリスクがある。東京証券取引所のシステムの不具合により、みずほ証券が誤注文の発注取消の連絡をしたにも関わらず、取引が成立して損失が発生し、訴訟に発展した例が最たるものである［大和田尚孝、吉田洋平, 2010a]。

2.3.6. 市場リスク

ここまでの 5 つのリスクは、金融情報システム自体が外部から直接評価されるタイプのリスクである。金融事業者のリスクには、それ以外に、経営判断をサポートすることで金融情報システムが間接的に関与するリスクとして、市場リスク、信用リスク、流動性リスクの 3 つが挙げられる。これらのリスクは、金融機関の収益活動から生じるものであり、純粋リスクと投機的リスクの両面がある。

市場リスクは、外国為替市場や、株式債券市場、短期金融市場等の金融市場における価格や相場の変化で資産の価値が減少するリスクのことを言う。その内訳は、金利リスク、為替リスク、価格変動リスクである。市場リスクの低減のため、金融情報システムには、マーケット情報を正確に把握することや、即時に情報伝達することが求められている。

特に、市場部門では、このリスクは日常業務の根幹となるものである。金融情報システムには、金融機関が、投機的リスクを取って資産価値を増やす一方で、損失の発生をコントロールするため、マーケット情報を正確に把握することや、即時に情報伝達することが求められる。例えば、三菱 UFJ モルガンスタンレー証券の 2010 年度決算で、デリバティブ商品の巨額損失を主因として約 1400 億円赤字となった事例は、失敗の典型例である[日本経済新聞, 2011]。

2.3.7. 信用リスク

信用リスクは、主として、融資先の信用力の劣化により、保有資産の価値が減少するリスクを言う。金融情報システムには、融資先のリスクの正確な把握による融資業務運営や、適切な担保や保証等の引当ての判断のための、サポートが求められている。銀行部門は、融資により収益を得るビジネスモデルであり、信用リスクの判断が、業務の根幹となるものである。

市場部門でも、有価証券等を保有している場合の、発行体の信用力低下や義務不履行による資産価値の減少のリスクが中心である。このようなリスクの正確な把握による適切な措置をとるために、金融情報システムのサポートが求められている。

2.3.8. 流動性リスク

流動性リスクについては、銀行部門では、資金の運用と調達の期間のミスマッチの発生や、予期せぬ資金流出で必要な資金確保が困難となる資金繰りのリスクがある。また市場の混乱等で、保有する有価証券の換金性が低下し、著しく不利な価格での取引を余儀なく

されるリスクも想定される。金融情報システムには、総合的な運用調達の管理のための情報提供が求められている。

市場部門でも、市場で市場価格での決済や資金調達取引ができず、不利な条件での換金を行うことで損失を被るリスクが中心である。特に市場の混乱やカウンターパーティの所属する国や市場の状況により、著しく不利な価格での取引を余儀なくされるケースがある。よって、それらを含めたリスク管理について、金融情報システムのサポートが求められている。

2.4. 金融情報システムの問題構造

前節まで、我が国の金融システムと金融情報システムを概観し、金融情報システムに関するリスクについて、純粋リスク顕在化の事例で説明してきた。金融情報システムは様々な業態で利用されているが、多くの純粋リスク顕在化事象が発生していることから、本節では、我が国の金融情報システムの特異性や開発動向に言及した上で、その問題構造について、整理を行う。

2.4.1. 金融情報システムの特異性と開発動向

我が国の金融情報システムの問題構造を論じる際、他の情報システムと異なる特異性を考慮する必要がある。それは、以下の四点である。

1）決済システムとして広範囲のネットワークに接続しており、可用性や大量即時処理への外部からの要求度合いが高い。

2）顧客の財産情報を扱うことから、情報セキュリティの高さを求められる。

これら二つの特異性に関しては、損なわれた場合、報道等で大きく取り上げられ風評リスクが顕在化する。

3）レガシーシステムの存在である。金融情報システムが大量データ処理を行うため、1980 年代にホストコンピュータで構築したレガシーシステムを、IT 技術の発展した現在でも使い続けることが不可避であり、新技術を用いて構築した分散系システムとレガシーシステムの間でのデータのやり取りが発生するため、保守や開発の難易度が高くなっている。

4）規制産業としてビジネスの権益が保護されている一方で、情報システムの健全性についても当局の監視下に置かれており、経営や情報システムのイノベーション採用の自由度を制約している。

また、金融情報システム開発の動向については、社団法人日本情報システムユーザー協会で、企業 IT 投資の動向調査を行っている。2011 年度の調査で、500 人月以上の金融情報システム開発に関する金融事業者 29～30 社からの回答のうち、、期限がすべて予定通りだったという回答は 48%、予算がすべて予定範囲だったという回答は 50%、品質がすべて満足を得られたという回答は 33%であった（表 4）[10] [日本情報システムユーザー協会, 2012]。残りの金融事業者では、何らかの問題が発生していることとなる。

表 4　金融情報システム開発での規模別工期予算品質達成度

工期	プロジェクト規模	回答数	予定通り完了	ある程度予定通り	予定より遅延
	100～500 人月未満	36	42%	44%	14%
	500 人月以上	29	48%	41%	10%
予算	プロジェクト規模	回答数	予定通り完了	ある程度予定通り	予定より超過
	100～500 人月未満	35	49%	37%	14%
	500 人月以上	30	50%	37%	13%
品質	プロジェクト規模	回答数	満足	ある程度満足	不満
	100～500 人月未満	35	31%	57%	11%
	500 人月以上	30	33%	57%	10%

[「企業の IT 投資動向に関する調査報告書 2012」pp.220-222 から筆者が作成]

2.4.2. 金融情報システムの問題構造とその要因

我が国の金融情報システムを、業態を超えて全体で大きく捉えると、以下の 4 つの要因が複合して、純粋リスク顕在化につながるような問題構造があると考える [遠藤正之、高野研一, 2015]。

1）IT 要因（外部要因）、

2）金融業務要因（外部要因）、

3）組織要因（内部要因）、

4）経営者要因（内部要因）。

すなわち、我が国の金融情報システムの問題は、金融情報システムの大規模複雑化により、トラブル対応力の低下や拡張性の欠如が生じ、ひいては金融の競争力低下を招くという点である。その原因となる問題点や、環境変化への不適合等の現象を筆者が洗い上げた上で、グルーピングしたものが、図 3 である。IT や金融業務という外部要因の変化に対して、システム開発の組織や経営者という内部環境が適合しきれていないという、大きな問題構造が浮かび上がってくる。

[10] 他の情報システムと比較すると金融情報システムは工期、予算、品質とも達成度合いは高い。

以下それぞれの要因別に詳述していく。

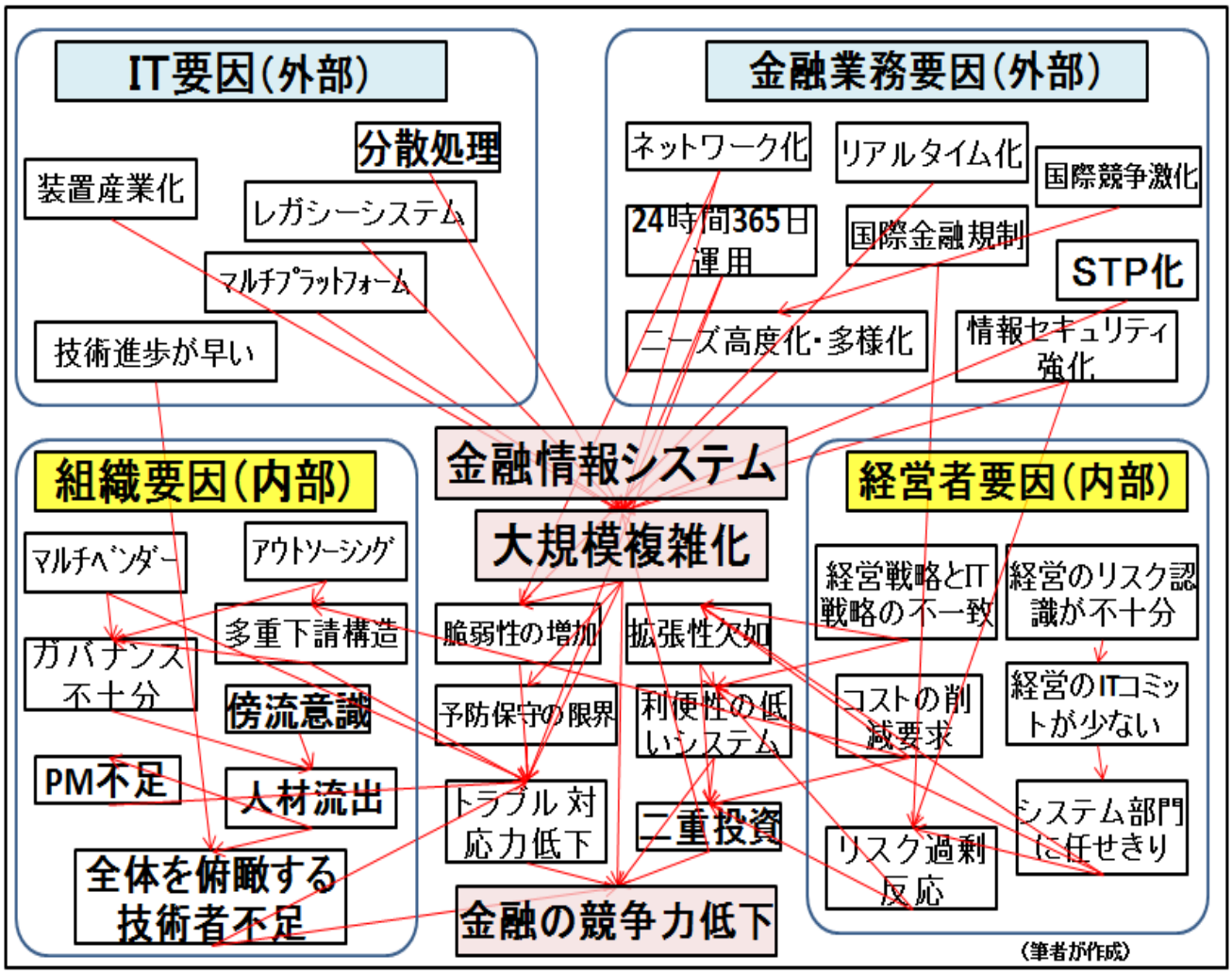


図 3 金融情報システムの問題構造図

2.4.2.1. IT 要因

第一の要因は、外部環境である IT（Information Technology）要因である。金融業が装置産業化する一方で、レガシーシステムが存在し、システムの複雑化をもたらしている。レガシーシステムの典型は、1980 年代にホストコンピュータで構築されたシステムであり、その後構築された分散系システム等との連携が、保守や開発の難易度を高めている。

2.4.2.2. 金融業務要因

第二の要因は、外部環境である金融業務要因である。金融のグローバル化、ボーダレス化と、それに伴う国際競争の激化と国際的な金融規制の導入により、高度かつリアルタイ

ムベースでの 24 時間 365 日運用のニーズが高まる一方、情報セキュリティやコンプライアンス面の要求を満たすことも必要となっている。

2.4.2.3. 組織要因

第三の要因は、内部環境要因である金融情報システムの開発組織の要因である。金融情報システムの大規模化により、シングルベンダーでの対応は困難となり、マルチベンダーでの対応が必要になった。更に委託されたベンダー自体も、複数のベンダーに再委託する多重下請構造が一般化している。そのため、ガバナンスが不十分となり、大規模プロジェクトをマネジメントするプロジェクトマネージャーや、全体を俯瞰する技術者が不足してきている。

2.4.2.4. 経営者要因

第四の要因は、内部環境要因である金融事業者の経営者要因である。経営者の金融情報システム開発におけるリスク認識が不十分な傾向に加え、障害等への過剰反応と通常開発でのコスト削減の要求が相乗して、拡張性の欠如を招き、その結果、経営戦略の変化に柔軟に対応できず、二重投資の発生や利便性の低いシステムにつながるリスクがある。

2.5. 金融情報システムのリスクマネジメントの課題

前節で述べた通り、IT 要因と金融業務要因の外部要因が不可避であるのに対し、経営者要因や組織要因の内部要因には、主体的に対応可能であると考えている。そこで本論文では、特に組織要因を含めた経営者の対応がポイントであると考え、主として経営者関与について論じていく。

金融情報システムが、大規模複雑化している中で、金融情報システムにおける経営戦略としてのリスクマネジメントが適正に行われないと、トラブル対応力の低下、金融情報システムの拡張性の欠如による二重投資の発生が生じ、ひいては金融自体の競争力低下が懸念される。次の第 3 章では、このような課題全体を捉えた上で、経営者がどのように対処すれば良いのか、リスクマネジメント戦略の構築を図っていく。

第3章 リスクマネジメント戦略の構築

第 2 章では、金融情報システムのリスクマネジメントの現状把握を行った上で、課題全体の構造を明らかにした。本章では、いよいよ本論文の中核となるリスクマネジメント戦略の構築を行う。まず、IT 投資に対するリスクマネジメント要求、システム監査関連基準からの経営者が関与すべき項目抽出、そして金融情報システム開発の最近の成功事例の成功要因を総括し、リスクマネジメント戦略を 6 観点(CORE-OQ)に集約する。その後、情報システム開発に関与する金融機関従業員を対象とした問題意識調査により、現状の開発局面での妥当性の検証を行う。最後に運用局面でのリスクマネジメントについても考察する。

3.1. IT 投資に対するリスクマネジメント要求[11]

金融事業者の経営戦略実現のためには、金融情報システムが核となる重要な構成要素であるが、その金融情報システムの構築には、適切な IT 投資を継続することが必要となる。そこで本節では、IT 投資に対するリスクマネジメント要求について考察する。

金融事業者が IT 投資を考える場合、二つの大きな命題を実現することが必要となる。第一は、競争優位性を高めるための IT 投資である。言わば「攻めの IT 投資」である。第二は、システムの信頼性実現のための IT 投資である。言わば「守りの IT 投資」である。この両面のバランスが取れることで、経営戦略の実現につながることになる。

3.1.1. 攻めの IT 投資（「IT 経営ロードマップ」）

競争優位性を高めるための「攻めの IT 投資」を適切に纏めている先行研究として、金融業に限定されず、全産業向けであるが、「IT 経営ロードマップ」 [経済産業省, 2010]がある。

「IT 経営ロードマップ」では、経営・業務・IT の融合による企業価値の最大化を目指すことを「IT 経営」と定義し、企業が IT 経営を実践するために取り組む 10 の原則を IT 経営憲章として纏めている。それは、以下の通りである。

1）経営と IT の融合…経営者は自らの経営判断に基づき、企業改革や業務改革の道具として常に IT を戦略的に活用する可能性を探求する。

[11] 本節は、「金融機関経営者が情報システム開発で果たす役割の一考察」[遠藤正之, 2012]を元にしている。

2）改革のリード…経営者は、企業改革に IT における技術革新の成果を生かし、日々の細かな改善を含め、中長期にわたり、取組みをリードする。

3）優先順位の明確化…経営者は、取り組むべき企業改革や業務改革の内容を明らかにして、その実現に向けた IT 投資の優先順位を常に明確に現場に示す。

4）見える化…経営者は、IT を活用し、競争優位の獲得に必要な情報や業務を可視化し、かつステークホルダーへの情報開示や透明性の確保に取り組む。

5）共有化…経営者は、「見える化」した情報や業務を「共有化」し、企業内での部門を超えた業務間連携、業種・業態・規模を超えた企業間連携を促す情報基盤構築やバリューチェーンの最適化に取り組む。

6）柔軟化…経営者は、IT を活用し、個々の企業の枠にとらわれず、業務やシステムの組み替えや、必要な情報を迅速かつ最適に活用できる事業構造への転換に取り組み、経営環境の急速な変化に柔軟に対応する。

7）CIO と高度人材の育成…経営者は、最適な IT 投資・IT 活用を実現するために、CIO を任命し、ともに企業改革や業務改革に取り組む。また、産学官、ユーザー・ベンダの垣根を越えて、IT を駆使した企業改革を推進できる高度人材の育成・交流を推進する。

8）リスク管理…経営者は、IT 活用がもたらすリスクと、問題が発生した際のステークホルダーや社会に及ぼす影響を正しく認識し、その管理を徹底する。

9）環境への配慮…経営者は、環境に対する企業責任を認識し、IT 活用によるエネルギー効率向上や省資源化に取り組む。

１０）国内企業全体の底上げ…経営者は、IT 投資から最大限の効果を引き出すためにも、中小企業等企業規模や業種の如何を問わず、企業の枠を超えて我が国企業全体の IT 経営の改善・普及に取り組む。

一方、経営と IT の融合が進んでいない企業の特徴として、以下 3 点を挙げている。

①経営者が IT 投資と経営戦略の関係が希薄だと考えており、経営者自身の IT 投資に対する考え方が不明確、

②経営目標実現に向けた IT 活用の基本的な「IT アーキテクチャ」[12]の不在、

[12]IT を活用すべき業務や対象市場とそのための IT アーキテクチャが、経営レベルで明確にされていること。「IT ロードマップ改訂版」では、「絵図面」と表記されている。

③「IT アーキテクチャ」を具体化するための業務設計作業（業務モデル構築）の不在。

IT 経営憲章の 10 原則は、金融事業者の IT 戦略や金融情報システムにも適用可能であるが、６）柔軟化、８）リスク管理、１０）国内企業全体の底上げの３つの観点が特に重要と考える［遠藤正之, 2012］。

６）の「柔軟化」は、「見える化」「共有化」した情報や業務を外部環境に応じて柔軟に組み替えることで、社内外のバリューチェーンのつながり力を高める活動である（図 4）。金融事業者の場合、多様な外部インターフェースに対する情報受渡しを標準化し、情報やデータの流通を促進する活動が望まれており、重要である。

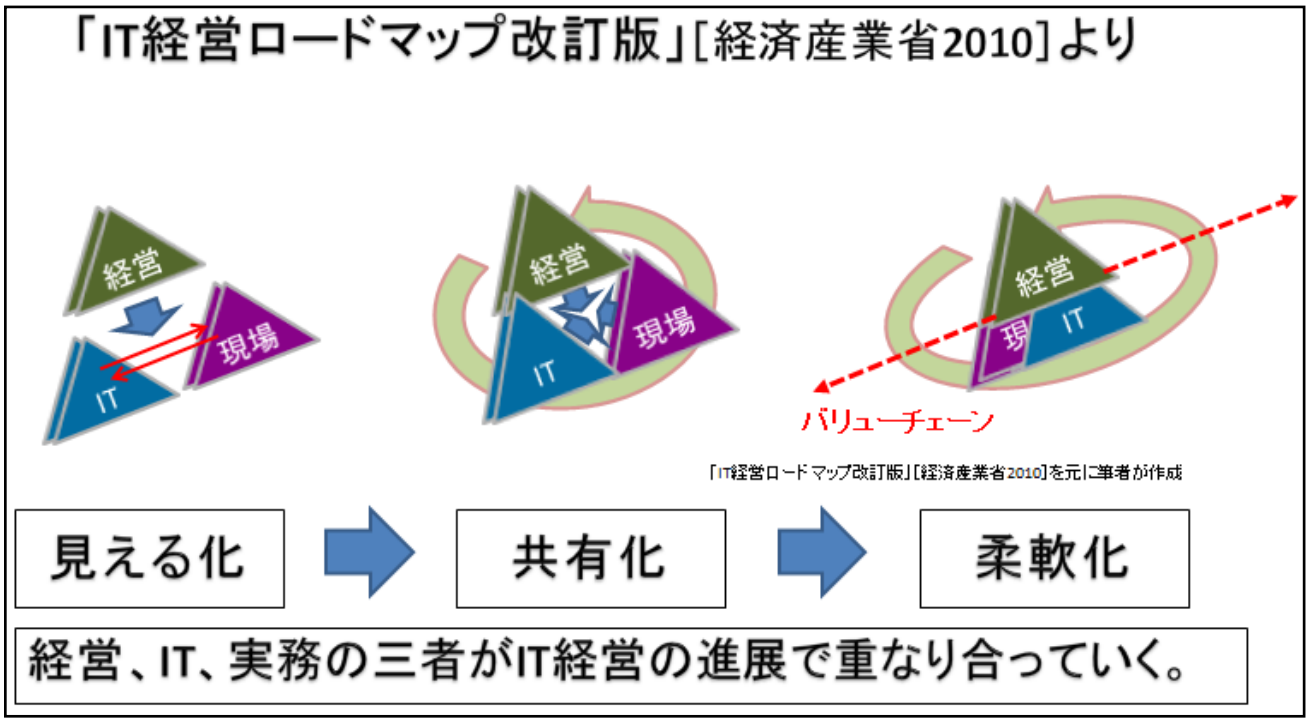


図 4「見える化」「共有化」「柔軟化」［経済産業省, 2010］

８）の「リスク管理」は、マイナスの結果を産むリスク（純粋リスク）に関する項目であるが、顧客情報の情報セキュリティを厳格に管理しつつ、多様なネットワークとの柔軟な接続の継続性、可用性を高める安定性が要請される点で、本論文の主眼とするところでもあり、重要である。

１０）の「国内企業全体の底上げ」については、金融機関は、金融機能、決済機能の利便性を高めることで、産業全体の IT 経営力向上や、国内企業全体の活性化に貢献するインフラを担っていることから、長期的な経営戦略の観点で極めて重要である。

3.1.2. 信頼性実現（「重要インフラ情報システムの信頼性向上の取組みガイドブック」）

システムの信頼性実現のための「守りの IT 投資」を高めるための要件を纏めた先行研究としては、「重要インフラ情報システムの信頼性向上の取組みガイドブック（以下「信頼性向上の取組みガイドブック」と略す)」［独立行政法人情報処理推進機構ソフトウェア・エンジニアリング・センター(IPA SEC) , 2011]が、良く纏められている。この文書も「IT 経営ロードマップ」と同様、金融業に限定されず、全産業向けであるが、事例の８社中金融業を３社採り上げている。

ここでは、情報システムの障害が引き金になって、国民生活や社会経済活動を支える重要インフラサービスに大きな影響が生じることを防止するための取組みを提言している。重要インフラサービスを支える情報システムを「重要インフラ情報システム」とし、鉄道、航空、物流とともに金融を代表的な重要インフラサービスと位置づけ、「重要インフラ情報システム」を提供する事業者のステークホルダー別に、提言を纏めている。

その中で、重要インフラ事業者の情報システム部門や外部組織、事業部門、経営層それぞれについて、期待される役割を定義している。特に、経営層に対しては、事業要件レベル（ビジネスモデルレベル）で、外部環境を把握して情報システムへの信頼性要求を作り、それが実現される過程をモニターし、実際の信頼性が十分かを評価する必要があるとし、以下の８点の役割を提言している。

１）信頼性について事業要件レベルでの外部関係者との合意、
２）１）のうち、情報システムに関係する部分の識別、
３）情報システムへの事業要件レベルでの信頼性要求のとりまとめ、
４）情報システムの信頼性提供の見込みの承認、
５）個別の開発・保守プロジェクトの承認、
６）個別の開発・保守プロジェクトの監視への参画、
７）情報システムの信頼性の評価結果と対策の承認、
８）信頼性について事業要件レベルでの外部関係者への説明。

更に、信頼性要求については、システムを社会的重要度に応じてカテゴライズすることを推奨している。また利用できるツール情報として、情報システムコントロール協会の「COBIT Ver4」や経済産業省の「システム管理基準」［経済産業省, 2004］「情報セキュリティ管理基準」、金融事業者向けとして（財）金融情報システムセンター（FISC）の「金

融機関等コンピュータシステムの安全対策基準・解説書」［（財）金融情報システムセンター, 2011a]、「個人情報保護法」、会計報告の適正性確保のための「金融商品取引法」等を挙げている。また参考となる金融業の取組好事例として、アプリケ―ションオーナー制度をいち早く導入して情報システムの利用者である業務部門の責任と役割分担を明確にした取組みと、システム開発にあたって「上流工程完璧主義」を掲げて漏れのない要件定義書作成を行い、設計への反映をフォローした取組みを紹介している。

経営層への８点の役割を金融機関に適用する場合、１）信頼性について事業要件レベルでの外部関係者との合意と８）信頼性について事業要件レベルでの外部関係者への説明が、特に重要であると考える。

なぜならば、金融情報システムは、多様な外部関係者が関与しており、外部環境の状況を経営リスクとして把握することと、外部関係者への説明責任を果たすことで、ビジネスリスクや風評リスクの低減を行うことが重要なためである［遠藤正之, 2012]。また金融情報システムの信頼性要求とそのコストに関しても、十分に専門家の意見を採り入れて経営判断することが必要になる［遠藤正之, 2012]。

3.2. システム監査関連基準からの経営者関与項目の抽出[13]

金融情報システムのリスクマネジメントにおいて、システム監査は、開発や運用を行う部署とは別に、第三者の視点での助言を行う点で、リスクマネジメントの一翼を担うものである。そして、システム監査にあたっては、明文化された複数の基準が存在している。これらの基準は、過去の様々なプロジェクトに基づいて作成されたものであり、経営者のリスクマネジメントの観点として、現実的で重要なポイントがほぼ網羅されていると考えられる。

ここでは、金融情報システムのリスクマネジメントに活用できる以下 4 件のシステム監査関連の基準について、次節から 4 基準の概要と経営者関与項目を示す。尚、後続の 5.1 節でも、各々の詳細を比較検討することとなる。

１）COBIT4.1 版［IT ガバナンス協会, 2007]、

２）システム管理基準・システム監査基準［経済産業省, 2004]、

３）金融機関等のシステム監査指針［（財）金融情報システムセンター, 2007]、

[13] 本節は「金融情報システムの開発上流工程におけるシステム監査ポイントの提言」[遠藤正之、高野研一, 2013b]を元にしている。

４）金融検査マニュアル（預金等受入機関に係る検査マニュアル）・システム統合リスク管理態勢の確認検査用チェックリスト [金融庁, 2014] [金融庁, 2002]。

3.2.1. 「COBIT4.1 版」（Control Objective for Information and related Technology)

米国に本部を置く情報システムコントロール協会[14]が設立した IT ガバナンス協会が、1996 年に初版を発行し、その後 1998 年 2 版、2000 年 3 版、2005 年 12 月 4 版、2007 年 4.1 版と版を重ね、2012 年 4 月に 5 版が発表された。5 版では事業体全体のガバナンス観点の色彩がより強まっているため、本論文では、システム監査に関連する国際的な基準として完成度が高いと考えられる 4.1 版（2008 年 6 月日本語版）で検討する。

4.1 版では IT 業務を、4 つのドメイン（領域）に分類して、ガバナンスの観点で、コントロール目標とアクティビティを整理している。ドメインとは IT ガバナンスを整備・運用する上で欠かせない領域を指す。

第一の PO(計画と組織：Plan and Organise)のドメインは、

PO1:IT 戦略計画の策定、

PO5：IT 投資の管理、

PO8：品質管理、

PO9：IT リスクの管理

に代表されるシステム開発プロジェクト構築前の 10 プロセスからなっている。

第二の AI(調達と導入：Acquire and Implement)のドメインは、

AI5：IT 資源の調達、

AI6：変更管理

に代表されるシステム開発時の 7 プロセスからなっている。

第三の DS(サービス提供とサポート：Deliver and Support)のドメインは、

DS5：システムセキュリティの保証

に代表される運用保守の 13 プロセスからなる。

第四の ME(モニタリングと評価：Monitor and Evaluate)のドメインは、PO から DS までのドメインで提示したプロセスが適切に運用されているかをモニタリングするドメインで、ME4：IT ガバナンスの提供を含む 4 プロセスからなる。

[14] ISACA：Information Systems Audit and Control Association

全体では合計 34 プロセスとなる。各プロセス内に、詳細化したコントロール目標 210 項目と経営者管理者のアクティビティ項目[15]197 項目が示される（詳細は巻末別紙 1 ご参照)。

アクティビティ項目については、CEO や CIO 等の経営者や管理者の関与に関し、4 つの類型で分類されている。関与が大きいものから、①実行責任者、②説明責任者、③協議先、④報告先の 4 類型である。アクティビティ項目の 4 類型は、その順に関与度の大きさとなるため、筆者はこの類型に対し、実行責任者を 4 ポイント、説明責任者を 3 ポイント、協議先を 2 ポイント、報告先を 1 ポイントのウェイト付けをして、開発計画に関するアクティビティに関し、プロセス毎に単純集計した。その結果の抜粋は、表 5 の通りであるが、CEO の関与度の集計値が高いプロセスは、

ME4：IT ガバナンスの提供、

PO1:IT 戦略計画の策定、

PO9:IT リスクの評価と管理、

PO5:IT 投資の管理、

AI5:IT 資源の調達の順となった。

一方、CIO の関与度の集計値が高いプロセスは、

PO9:IT リスクの評価と管理、

AI1：コンピュータ化対応策の明確化、

PO10:プロジェクト管理、

PO8:品質管理、

PO5:IT 投資の管理、

PO1:IT 戦略計画の策定の順となった。

特に 1 番目 PO9:IT リスクの評価と管理と、2 番目の AI1：コンピュータ化対応策の明確化は、ほぼ拮抗していた。また実施工程別分析でも上流工程で行うものが中心であることが確認できた。

全般に実務に近い CIO のアクティビティ項目の関与度の方が CEO より大きいが、ME4：IT ガバナンスの提供だけは、CEO のアクティビティ項目の関与度が大きくなる。

[15] コントロール目標とアクティビティ項目は一対一対応していない。

そこで具体的なアクティビティ項目を見ると、「経営層と取締役会による IT アクティビティに対する監督と推進の確立」、「IT 成果・IT 戦略・資源とリスクの管理のビジネス戦略との整合、レビュー、承認、及び周知」「成果及びポリシー、計画、手続へのコンプライアンスに関する独立した定期評価の実施」「独立した評価による検出事項の解決、およびマネジメント層による合意された改善案の確実な実施」の 4 項目に関して、CEO が実行責任者となっていることが確認できた。IT 戦略とビジネス戦略との整合を保ち、監督推進を行い、実施状況を定期評価して改善を確実に実施することが、CEO に期待されていることが読み取れる。CIO については、IT 戦略計画を策定し、システム化要件を確定させた上で、開発マネジメントに関し主導的な役割を果たす等、より実務的な関与が期待されている。

表 5 「COBIT4.1 版」で CEO,CIO の関与度の集計値が高いプロセス

CEO・CIO の関与度の集計値が高いプロセス	アクティビティ項目数（満点）	CEO	CIO	CEO+CIO 合計	主な実施工程
ME4:IT ガバナンスの提供	5（20）	**18**	14	32	上流から下流
PO1:IT 戦略計画の策定	5（20）	**11**	**18**	29	上流
PO9:IT リスクの評価と管理	10（40）	**10**	**28**	38	上流から下流
PO5:IT 投資の管理	5（20）	7	**19**	26	上流
AI5:IT 資源の調達	5（20）	7	9	16	上流から下流
PO10:プロジェクト管理	7（28）	5	**22**	27	上流から下流
PO8:品質管理	5（20）	3	**20**	23	上流から下流
AI1:コンピュータ化対応策の明確化	8（32）	0	**27**	27	上流

3.2.2. 「システム管理基準」、「システム監査基準」

経済産業省（旧通商産業省）が、情報システム監査を普及振興させるため、1985 年に制定した「システム監査基準」を、2004 年に大幅改定し「システム監査基準」と「システム管理基準」との二文書構成としたものである。「システム監査基準」が、システム監査人の行為規範であり、「システム管理基準」が、監査上の判断の尺度として用いるべき基準である。「システム管理基準」は、情報システムに係る産業全般を視野に入れ、監査項目を列挙している。金融情報システムに特化したものではないが、我が国の標準的なシステム監査関連の基準であり、検討対象とした。内容は、システム部門の管理に重点が置かれている点が特徴的である。

6 つの章に分かれており、

Ⅰ章の情報戦略が 6 節 47 項目、

Ⅱ章の企画業務が 3 節 23 項目、

Ⅲ章の開発業務が 6 節 49 項目、

Ⅳ章の運用業務が 10 節 73 項目、

Ⅴ章の保守業務が 6 節 19 項目、

Ⅵ章の共通業務が 7 節 76 項目、

合計 38 節 287 項目が基準として掲載されている（詳細は巻末別紙 2 ご参照)。

CEO と CIO の具体的関与の記載が無いため、筆者が各項を独自に「COBIT4.1 版」のアクティビティ項目の 4 類型に分類、ウェイト付け（①実行責任者 4 ポイント、②説明責任者 3 ポイント、③協議先 2 ポイント、④報告先 1 ポイント）して、単純集計し、関与度の高い項目を分析した。その結果は、表 6 の通りで、CEO については、1 番目が全体最適化、2 番目が組織体制となり、以下災害対策、委託・受託、情報化投資、事業継続計画、開発計画、コンプライアンスとなった。CIO については、1 番目が全体最適化と組織体制であり、以下委託・受託と人的資源管理が続いた。

「COBIT4.1 版」とは異なり、CIO より CEO の関与度の集計値が高い節は見出せなかった。これは、システム部門向け管理項目が中心であるというこの基準の特徴の帰結であると考える。実施工程別分析では、上流工程から対応が必要な項目が上位を占めた。CEO、CIO の両方で 1 番目となった全体最適化の詳細項目には、「IT ガバナンスの方針を明確にすること」、「情報化投資及び情報化構想の決定における原則を定めること」、「情報システム全体の最適目標を経営戦略に基づいて設定すること」といった経営戦略やガバナンスに関する項目が含まれている。

表 6 「システム管理基準」での CEO,CIO の関与度の集計値が高い節

CEO・CIO の関与度が高い章、節[16]	内訳数（満点)	CEO	CIO	CEO+CIO 合計	主な実施工程
Ⅰ.情報戦略１．全体最適化	4（16)	7	1 1	18	上流
Ⅰ.情報戦略２．組織体制	3（12)	6	11	17	上流
Ⅵ.共通業務４．災害対策	4（16)	4	5	9	上流から下流
Ⅵ.共通業務５．委託・受託	5（20)	2	8	10	上流から下流
Ⅰ.情報戦略３．情報化投資	1（4)	2	4	6	上流から下流
Ⅰ.情報戦略５．事業継続計画	1（4)	2	4	6	上流から下流
Ⅱ.企画業務１．開発計画	1（4)	2	3	5	上流から下流
Ⅰ.情報戦略６．コンプライアンス	1（4)	2	2	4	上流から下流
Ⅵ.共通業務４．人的資源管理	4（16)	1	8	9	上流から下流

[16] Ⅰ.Ⅱ.…が章。1, 2, …が節。1. 1,1. 2…が項。

3.2.3. 「金融機関等のシステム監査指針」

財団法人金融情報システムセンター（FISC[17]）が、1987 年に金融機関向けに制定し、その後、2000 年第 2 版、2007 年第 3 版、2014 年改訂第 3 版と三回の改訂を経ている。第 3 版は、個人情報保護法、金融商品取引法等の法制度の変更や、IT ガバナンスやリスクマネジメントの国際標準である COSO-ERM[18]の考え方を反映した改訂である。改訂第 3 版は、クラウドコンピューティング等の情報システムの最新状況への対応がされたものであるが、項目としては、第 3 版と不変であり、本項では、第 3 版を用いて分析する。

金融機関のシステム監査に焦点を絞って策定されており、本稿の対象である金融情報システムに適合している。情報システムの対象領域を 12 に分類し、その対象領域をシステム監査の要点項目として、169 の小項目に分類し小項目毎にチェックポイントを記載している（詳細は巻末別紙 3 ご参照)。

要点項目別の小項目内訳は、

1.情報システムの計画と管理 11 項目、

2.情報システムリスクの管理 5 項目、

3.情報セキュリティ 20 項目、

4.システム開発 26 項目、

5.システム運用 18 項目、

6.システム利用 15 項目、

7.入出力等の処理 22 項目、

8.ネットワーク 10 項目、

9.システム資産・資源管理 7 項目、

10.外部委託 4 項目、

11.コンティンジェンシープラン 23 項目、

12.ドキュメンテーション 8 項目である。

CEO や CIO の関与は記載されていないが、小項目毎に監査対象となる部門として情報システム部門、利用部門、本部各部門を明示している。その記載を参考にして、「COBIT4.1

[17] The Center for Financial Industry Information Systems

[18]米国のトレッドウェイ委員会組織委員会（COSO）が 2004 年 2 月に公表したエンタープライズ・リスクマネジメントのためのフレームワークで、8 つの統制要素、4 つの統制目標からなる。

版」のアクティビティ項目の 4 類型に分類、ウェイト付け（①実行責任者 4 ポイント、②説明責任者 3 ポイント、③協議先 2 ポイント、④報告先 1 ポイント）して、単純集計し、CEO と CIO の関与度の高い要点項目を分析した。その結果は、表 7 の通りで、CEO は、１番目が情報システムの計画と管理であり、情報システムリスクの管理、システム開発、情報セキュリティが続いた。CIO は、1 番目の情報システムの計画と管理は同じだが、以下はシステム開発、情報セキュリティ、情報システムリスクの管理と続いた。実施工程別分析では、上流工程から対応が必要な項目であることが確認できた。

CEO、CIO とも 1 番目となった情報システムの計画と管理の小項目には、「経営戦略に沿った情報システム戦略の策定」、「情報システム運営委員会」、「情報システム部門の組織」、「ユーザー部門等の組織体制」、「情報システム中長期計画の策定」、「予算計画の策定」といった項目が含まれており、経営戦略に沿った情報戦略と組織整備への関与が重要であることを示している。

表 7 「金融機関等のシステム監査指針」での CEO,CIO の関与度の集計値が高い要点項目

CEO・CIO の関与度が高い要点項目	内訳数（満点）	CEO	CIO	CEO+CIO 合計	主な実施工程
1. 情報システムの計画と管理	8（32）	14	26	40	上流
2. 情報システムリスクの管理	5（20）	7	17	24	上流から下流
3. 情報セキュリティ	8（32）	5	19	24	上流から下流
4. システム開発	14（56）	5	21	26	上流から下流

3.2.4. 「金融検査マニュアル（預金等受入機関に係る検査マニュアル）」・「システム統合リスク管理態勢の確認検査用チェックリスト」

「金融検査マニュアル（預金等受入機関に係る検査マニュアル）」は、金融庁の検査用として、1999 年に制定された。その後、頻繁に改訂がなされ、2014 年 6 月版が最新である（2014 年 11 月時点）。本マニュアルは、検査官の視点を揃えることを目的とするが、ホームページ上で公開することによって、金融機関の意識をも高め、リスクに対する態勢整備が図られることを意図したものである。その中でシステムリスク管理態勢の整備・確立状況に関し、158 項目の検査チェックポイントを制定している（詳細は巻末別紙 4 ご参照）。

項目の内訳は、

経営陣による整備項目 22 項目（方針の策定 6 項目、内部規程・組織体制の整備 11 項目、評価改善活動 5 項目）、

管理者による整備項目 21 項目（管理者の役割責任 10 項目、システムリスク管理部門の役割 11 項目）、

個別項目 115 項目（情報セキュリティ 27 項目、システム企画・開発・運用管理等 47 項目、防犯・防災・バックアップ・不正利用防止 18 項目、外部委託管理 13 項目、付保預金払戻 10 項目）となっている。

「金融検査マニュアル（預金等受入機関に係る検査マニュアル)」の分冊の位置づけで、「システム統合リスク管理態勢の確認検査用チェックリスト」 が 2002 年 12 月に制定されている。これは、2002 年 4 月に発生した大手銀行統合時のトラブルにより、金融情報システムの統合のリスク認識が社会的に高まったことを受けて制定されたものであり、システム統合リスク管理態勢に絞って、32 項目のチェック項目を示している。内訳は、
経営陣のリスク管理に対する協調した取組み 10 項目、
協調したシステム統合リスク管理態勢のあり方 16 項目、
不測の事態への対応 3 項目、
監査及び問題点の是正 3 項目となっている（詳細は巻末別紙 5 ご参照)。

CEO や CIO の関与の分析については、経営陣による整備項目の 22 項目に絞って、「COBIT4.1 版」のアクティビティ項目の 4 類型に分類、ウェイト付け（①実行責任者 4 ポイント、②説明責任者 3 ポイント、③協議先 2 ポイント、④報告先 1 ポイント）して、単純集計し、CEO と CIO の関与度の集計値を分析した。その結果は、表 8 の通りであるが、CEO、CIO とも、内部規程・組織体制の整備が 1 番目となった。2 番目以降は、CEO は方針の策定、評価・改善活動の順となり、CIO は逆に評価・改善活動、方針の策定の順となった。

なお、各項目の素点で見た場合は、方針の策定は CEO 平均が 3 点となっており、内部規程・組織体制の整備の平均 2 点を 1 点上回っており、CEO の比重が高い項目であると考えられる。実施工程別分析では上流工程が中心であることが確認できた。

表 8 「金融検査マニュアル」での CEO,CIO の関与度の集計値が高い項目

CEO・CIO の関与度が高い中項目	内訳数（満点)	CEO	CIO	CEO+CIO 合計	主な実施工程
1. 方針の策定	4（16）	12	16	28	上流
2. 内部規程・組織体制の整備	7（28）	14	28	42	上流
3. 評価・改善活動	5（20）	10	20	30	上流から下流

3.3. リスクマネジメント戦略の 6 観点(CORE-OQ)[19]

金融情報システムの問題構造（2.4 節）に対しては、IT 投資に対するリスクマネジメント要求（3.1 節）で述べたように、競争優位性を高める「攻めの IT 投資」と、信頼性を実現する「守りの IT 投資」の両面のバランスを取った経営が求められる。しかしながら、経営者に重要なポイントを絞りこんで分かりやすく伝えるガイドラインは存在していない。そこで、「IT 経営ロードマップ」での「攻めの IT 投資」の考慮点、「信頼性向上の取組みガイドブック」での「信頼性実現」言わば「守りの IT 投資」の考慮点、システム監査関連基準の項目、最近の金融情報システム開発の成功事例の成功要因を総括して、経営者向けの項目を絞り込む試みを行った。

成功要因については、表 9 にある通り、最近の金融情報システム開発の成功事例である銀行システム統合事例と取引所システム更改事例から、抽出した。この 2 事例の選定理由は、金融システムにおける銀行部門と市場部門のそれぞれを代表する事例である点と、広く知られた事例で情報が十分に公開されている点の 2 点である。

表 9 最近の金融情報システム成功事例

	銀行システム統合 [大和田尚孝, 2009b]	取引所システム更改 [大和田尚孝, 2010b]
トップの関与	CEO のリーダーシップで体制構築。開発は CIO に委任するも継続して支援	CIO を外部から調達して、その後委任し継続して支援
体制構築	経営、業務部門、システム部門三位一体のプロジェクト体制構築	体制を整備するとともに、外部要員も投入して強化
重視したポイント	データ量増加に対するキャパシティ面での可用性、信頼性確保	高速取引に対応したレスポンスを重視
グランドデザイン	EA（エンタープライズアーキテクチャー）[20]を適用	EA（エンタープライズアーキテクチャー）を導入
要件定義	計画に 6 カ月掛け、要件を整理、多様な顧客を背景に要件の優先順位の合意に注力	発注者責任の徹底、レスポンス面の重視に伴う機能を簡素化した要件定義に注力
プロジェクマネジメント	進捗管理「見える化」 各種レビューとテストの充実	開発単位別に進捗品質を管理 早期不具合発見の手法を徹底
ベンダーマネジメント	マルチベンダーをコントロール	ベンダーを巻き込んで開発

[19] 本節は、「金融事業経営における情報システム開発のリスクマネジメント観点の提案」[遠藤正之、高野研一, 2013a]、及び「金融情報システムの開発上流工程におけるシステム監査ポイントの提言」[遠藤正之、高野研一, 2013b]を元にしている。

[20] Enterprise Architecture、組織全体の情報システムの最適化を図る方法論。

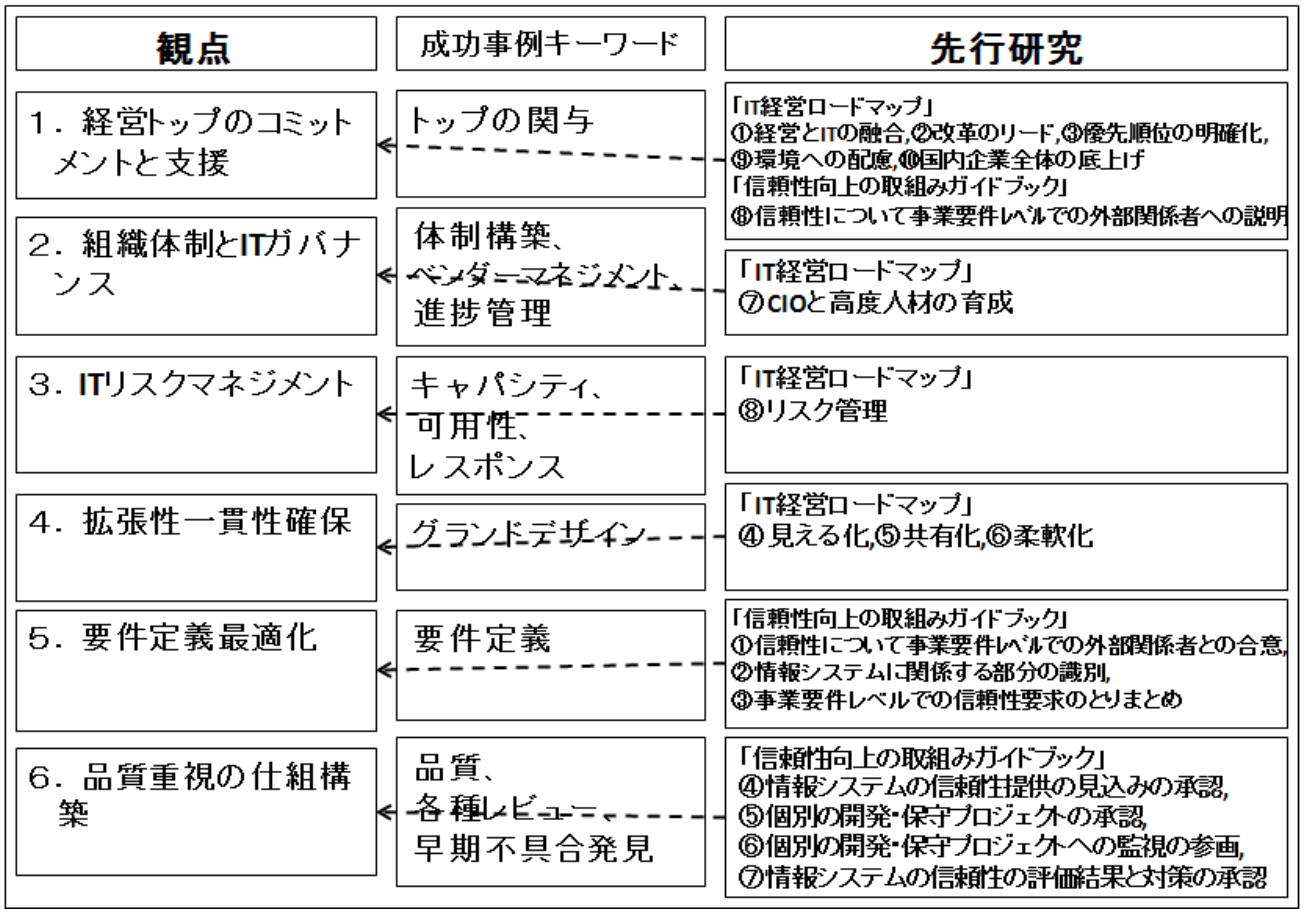


図 5 リスクマネジメント戦略の 6 観点への集約

この成功事例のキーワードに、「IT 経営ロードマップ」と「信頼性向上の取組みガイドブック」のポイントを含めて、図 5 の通り、経営者向けのポイントを整理した。

3.3.1. 経営トップのコメットメントと支援（Commitment）

観点 1 は、経営トップのコミットメントと支援（Commitment） である。経営トップが、経営戦略に沿った形での IT 戦略の優先順位を把握決定していき、利用部門と開発部門の間の組織体制を整備し、外部のステークホルダーへの説明責任を果たし、また情報システム開発部門への直接的な関与により、現場の士気を向上させることで、開発と IT 投資の成功に繋げているという点である。

これは、「攻めの IT 投資」の観点では、「IT 経営ロードマップ」での「経営と IT の融合」、「改革のリード」、「優先順位の明確化」に対応した項目であり、守りの「信頼性実現」の観点では、「信頼性向上の取組みガイドブック」の「信頼性について事業要件レベルでの外部関係者への説明」に対応している。

3.3.2. 組織体制と IT ガバナンス（Organization）

観点２は、適切な組織体制整備による IT ガバナンス強化（「組織体制と IT ガバナンス」）（Organization） である。対象となる情報システム開発に適した全社的組織体制やプロジェクト体制が構築され、システム部門においても開発における IT ガバナンスが高い状況に持っていくことである。これは、「攻めの IT 投資」の観点の「IT 経営ロードマップ」での「CIO と高度人材の育成」が対応している。

3.3.3. IT リスクマネジメント（IT Risk Management）

観点３は、経営 IT リスクの適切な評価と対策の構築（「IT リスクマネジメント」）（IT Risk Management）である。金融情報システム開発期間に発生可能性のあるリスクや、リリース後に発生可能性のあるリスクについて、開発開始時に広い視野で全般的に純粋リスクを洗い出した上で、純粋リスクの発生確率と影響度合いを分析し、対処の優先順位付けを決めているという点である。更に、適切な対策を立案し実施するとともに、継続的に純粋リスクの状況を管理し続けている点も含まれる。

これは、「攻めの IT 投資」の観点の「IT 経営ロードマップ」の「リスク管理」に対応する。

3.3.4. 拡張性一貫性確保（Extensibility）

観点４は、経営戦略に合致した業務拡張性及びシステムの一貫性の確保による二重投資の排除（「拡張性一貫性確保」）（Extensibility） である。将来の業務の拡張性やシステムの拡張性を確保できるような設計がなされ、更に将来にわたるシステムの二重投資がないように、金融情報システム全体のグランドデザインの上での位置付けが明確になったうえで、開発を行っているという点である。

これは、「IT 経営ロードマップ」の「見える化」、「共有化」、「柔軟化」に対応する。

3.3.5. 要件定義最適化（Optimization）

観点５は、外部関係者の要請と IT のケイパビリティの間をつなぐ要件定義最適化（非機能要件を含む）（「要件定義最適化」）（Optimization） である。経営及び業務部門から出た要件と、現状のシステムで構築可能な仕組みとの組み合わせに関し、業務面とシステム面で検討の上、より焦点を絞ってコストを抑えた形で、効果的な情報システム開発を行っているという点である。

これは、「信頼性向上の取組みガイドブック」の「信頼性について事業要件レベルでの外部関係者との合意」、「情報システムに関係する部分の識別」、「事業要件レベルでの信頼性要求のとりまとめ」に対応する。

3.3.6. 品質重視の仕組構築（Quality）

観点６は、品質重視の仕組構築（Quality） である。実際の情報システム開発で、設計品質や開発品質を向上するためのルールや手順の制定や、品質向上のための定期的な会議体や組織体の設置が行われているという点である。

これは、「信頼性向上の取組みガイドブック」における「情報システムの信頼性提供の見込みの承認」、「個別の開発・保守プロジェクトの承認」、「個別の開発・保守プロジェクトへの監視の参画」、「情報システムの信頼性の評価結果と対策の承認」の各項目に対応する。

3.3.7. CORE-OQ

前項までの６観点を「リスクマネジメント戦略の６観点」とし、各項目の英字の頭文字を取って、金融情報システムのコアとなるものとの意味も込め、「CORE-OQ」（コアＯＱ）と命名する（図 6）。

1．経営トップのコミットメントと支援	Commitment
2．適切な組織体制整備によるITガバナンス強化（「組織体制とITガバナンス」）	Organization
3．経営ITリスクの適切な評価と対策の構築（「ITリスクマネジメント」）	IT Risk Management
4．経営戦略に合致した業務拡張性及びシステムの一貫性確保による二重投資の排除（「拡張性一貫性確保）	Extensibility
5．外部関係者の要請とITケイパビリティの間をつなぐ要件定義最適化（非機能要件を含む）（「要件定義最適化」）	Optimization
6．品質重視の仕組構築	Quality

図６リスクマネジメント戦略の６観点「ＣＯＲＥ－ＯＱ」

ここまで説明してきた開発局面のリスクマネジメント戦略の６観点(CORE-OQ)をまとめると表 10 のようになる。

表 10 開発局面のリスクマネジメント戦略の 6 観点「CORE-OQ」

開発局面のリスクマネジメント戦略の6観点「CORE-OQ」

1．経営トップのコミットメントと支援（Commitment）	経営トップが優先順位決定、組織体制の整備に関与、社内外への発信
2．適切な組織体制整備によるITガバナンス強化（「組織体制とITガバナンス」）（Organization）	全社的組織体制やプロジェクト体制が構築され、ITガバナンスが高められている
3．経営ITリスクの適切な評価と対策の構築（「ITリスクマネジメント」）（IT Risk Management）	リスクを洗い出し、優先決め、対策を立案、実施し、継続的に管理
4．経営戦略に合致した業務拡張性及びシステムの一貫性確保による二重投資の排除（「拡張性一貫性の確保」）（Extensibility）	拡張性を確保できる設計。二重投資がないよう金融情報システム全体のグランドデザインをしている
5．外部関係者の要請とITのケイパビリティの間をつなぐ要件定義最適化（「要件定義最適化」）（Optimization）	要件と、現状のシステムの両面で検討、より焦点を絞って効果的な情報システム開発を行っている
6．品質重視の仕組構築（Quality）	設計品質や開発品質に関わるルール・手順の制定や会議体・組織の設置

遠藤正之、高野研一(2013)「金融事業経営における情報システム開発のリスクマネジメント観点の提案」より

その中で、開発局面を時系列で見ると 6 観点は必ずしも同じ時点での関与ではない点にも留意が必要である。特に 1 の「経営トップのコミットメントと支援」は一貫して全体に関わる項目である。また「IT リスクマネジメント」と「品質重視の仕組構築」は計画時の関与に加え、開発時に継続的な関与が必要な項目である（図 7）。

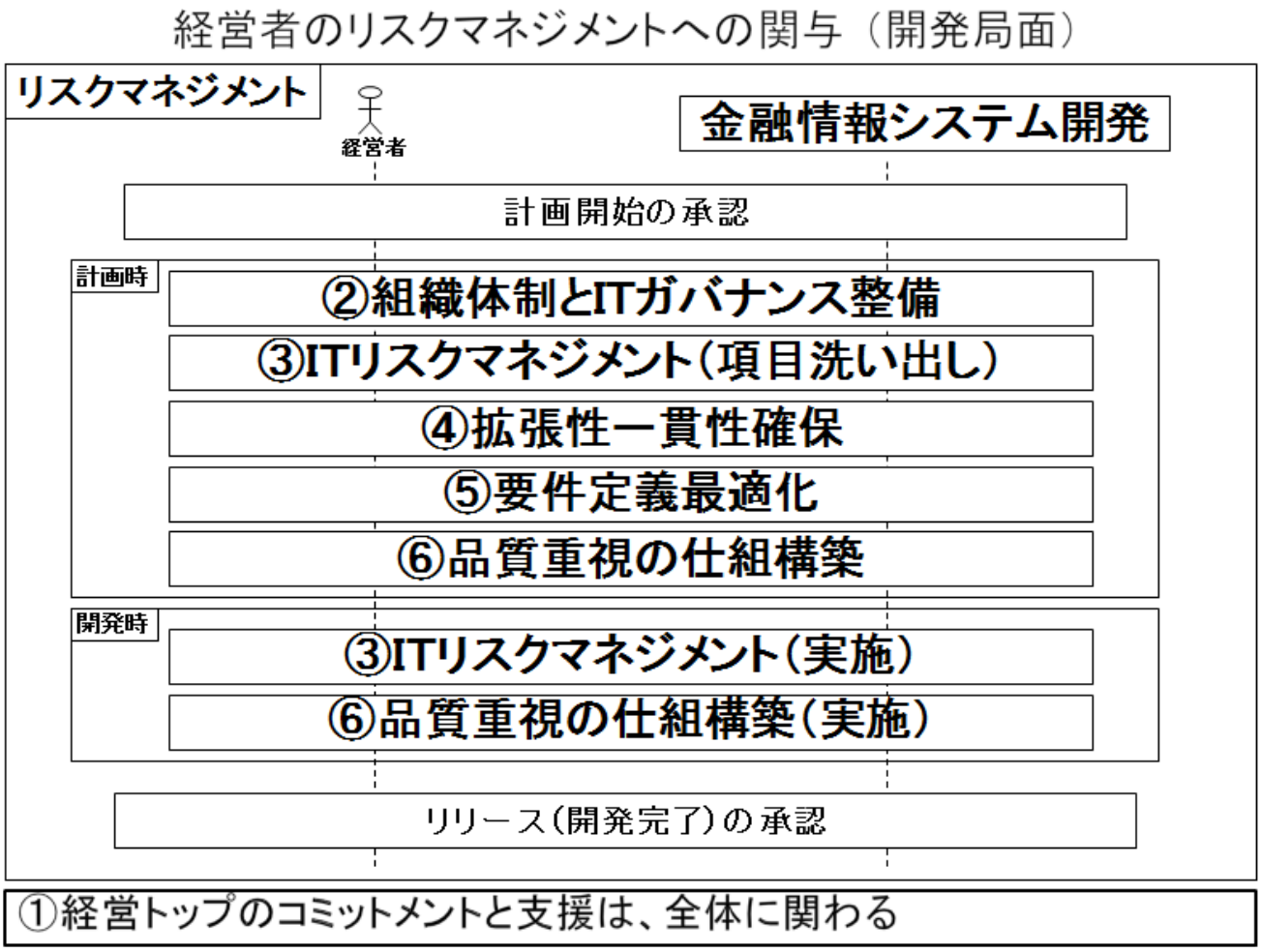


図 7 経営者のリスクマネジメントへの関与

3.4. 情報システム開発に関与する金融機関従業員の問題意識調査[21]

3.3 節のリスクマネジメント戦略の 6 観点に関して、情報システム開発に関与する金融機関従業員に問題意識調査をすることで、実際の金融情報システムプロジェクトでの有効性を確認することとした。仮説設定をした上で、インターネットを用いたアンケート調査を 2013 年 2 月から 3 月に行い、分析を行った。

3.4.1. 仮説設定

まず、金融情報システム開発でのマネジメント実施と経営者関与に関して、以下の仮説を設定した。

[21]本節は、「金融情報システム開発段階での経営者関与とマネジメント戦略に関する考察」[遠藤正之、高野研一, 2015]を元にしている。

仮説：リスクマネジメント戦略の 6 観点に関して、マネジメント実施や経営者関与が適切に行われた場合とそうでない場合のプロジェクトの成功率に差がある（目的変数「プロジェクトの成否」，説明変数「リスクマネジメント戦略の 6 観点：CORE-OQ」）。

3.4.2. 調査設計

この仮説を検証すべく、過去 5 年間に完了した金融情報システムプロジクトへのリスクマネジメント実施状況、CEO（経営トップ）の関与状況、CIO（情報システム最高責任者）の関与状況を情報システム開発に関与する金融機関従業員宛に調査することとした。

調査質問項目として、表 11 の通り、属性・自由回答 15 問（項番 1～9,16,17）、「プロジェクトの成否」（目的変数）関連 5 問（項番 10）、「リスクマネジメント戦略の 6 観点(CORE-OQ)」（説明変数）関連 55 問（項番 11～15、11 問×5）の計 75 問を用意した。

このうち、「リスクマネジメント戦略の 6 観点(CORE-OQ)」の質問の内訳は、
マネジメント実施（現状）、CEO 関与（現状）、CEO 関与（理想）、CIO 関与（現状）、CIO 関与（理想）の 5 視点に対し、同一内容の 11 問の質問を設定した。

その 11 問の明細は、
「経営トップのコミットメントと支援(Commitment)」2 問、
「組織体制と IT ガバナンス(Organization)」3 問、
「IT リスクマネジメント(IT Risk Management)」1 問、
「拡張性一貫性確保(Extensibility)」2 問、
「要件定義最適化(Optimization)」1 問、
「品質重視の仕組構築(Quality)」2 問とした。

データ収集にあたっては、経営者の関与状況の情報を幅広く多数集めることが重要であると考え、400 万人以上のモニターを擁するミクシーリサーチを利用した。一方で、情報の質を高めるため、過去 5 年間の金融情報システムプロジェクトへの経営者の関与状況を把握している金融機関勤務の情報システム開発担当者のみに予備調査で対象を絞り込んだ。調査は 2013 年 2 月 14 日から 3 月 27 日に実施し、様々な業種、年代、立場等の属性の 276 件の回答を得た。その中から同一選択肢に 8 割以上偏ったもの、各選択肢に均等に分散しているもの等 49 件を対象外とし、表 12 の通り、有効データ 227 件を分析対象とした。

表 11 調査質問項目

項番	質問内容
1	年齢，勤務年数，関与年数（5 問）
1 -1	年齢（プロジェクト関与開始時点）
1-2	勤務年数（プロジェクト関与開始時点）
1-3	金融情報システム関与年数
1-4	うち情報システム部門での関与年数
1-5	うち業務部門での関与年数
2	会社規模（社員数）
3	業種
4	プロジェクト期間
5	プロジェクト規模
6	プロジェクトタイプ（新規 or 改修）
7	開発対象業務（顧客ｵﾝﾗｲﾝ，決済，社内）
8	立場（管理職 or リーダーor 担当者）
9	関与した時期(全部 or 前半 or 後半)
10	プロジェクトの成否（5 問）
10-1	計画したコストの範囲だったか
10-2	計画した時期に予定通りに完了したか
10-3	想定した通りの品質だったか（不具合発生状況）
10-4	計画したシステム化の範囲を開発できたか
10-5	全体的にプロジェクトは成功だったか
11	情報システムのマネジメント実施（11 問）
11-1	経営戦略との関連付け（Commitment）
11-2	重要性の社内浸透(Commitment)
11-3	業務部門組織体制整備(Organization)
11-4	情シ部門組織体制整備(Organization)
11-5	IT ガバナンス良好(Organization)
11-6	IT リスクマネジメント実施(IT Risk Management)
11-7	拡張性意識(Extensibility)
11-8	グランドデザイン意識(Extensibility)
11-9	コストパフォーマンス意識(Optimization)
11-10	品質向上会議体組織設置(Quality)
11-11	品質向上ルール手順制定(Quality)
12	CEO(経営トップ)の関与状況(11 問)
12-1	情報システム全体計画への関与（Commitment）
12-2	重要性の社内外発信(Commitment)
	（12-3 以降は，11 番と同内容への関与）
13	経営トップの関与はどうあるべきか(11 問)（明細は，12 番と同内容）
14	CIO の関与状況(11 問)（明細は，12 番と同内容）
15	CIO の関与はどうあるべきか(11 問)（明細は，12 番と同内容）
16	CEO(経営トップ)の望ましい関与（自由回答）
17	CIO の望ましい関与（自由回答）

表 12 調査有効データの概要

		人数	%
性別	男性	182	80.2
	女性	45	19.8
年代	20 代	23	10.1
	30 代	86	37.9
	40 代	77	33.9
	50 代	36	15.9
	60 代以上	5	2.2
立場	情シ部門管理職以上	55	24.2
	情シ部門開発リーダー	67	29.5
	情シ部門担当者	35	15.4
	業務部門管理職以上	28	12.3
	業務部門開発リーダー	19	8.4
	業務部門担当者	21	9.3
	その他	2	0.9
業種	都市銀行	36	15.9
	地方銀行	46	20.3
	信託銀行	15	6.6
	信金信組	16	7.0
	証券会社	24	10.6
	生命保険	25	11.0
	損害保険	17	7.5
	クレジット信販	23	10.1
	取引所	5	2.2
	その他	20	8.8
会社規模	100 人未満	42	18.5
	100～299 人	41	18.1
	300～999 人	43	18.9
	1000 人～2999 人	44	19.4
	3000 人～9999 人	25	11.0
	10000 人以上	32	14.1
プロジェクト期間	3 カ月未満	13	5.7
	3～6 ヶ月未満	42	18.5
	6～12 ヶ月未満	50	22.0
	12～18 ヶ月未満	47	20.7
	18 ヶ月以上	75	33.0
プロジェクト規模	30 人月未満	45	19.8
	30～100 人月未満	75	33.0
	100～500 人月未満	66	29.1
	500 人月以上	41	18.1
プロジェクトタイプ	新規開発	82	36.1
	既存改修	111	48.9
	その他	34	15.0
対象業務（重複回答有）	顧客オンライン業務	95	41.9
	他金融機関との決済業務	94	41.4
	社内業務	110	48.5

3.4.3. 結果の分析

3.4.3.1. 仮説の検証

プロジェクトの状況とプロジェクト成功の関係は、以下の通りであり、リスクマネジメント戦略の 6 観点に関しては、その実施や関与の有無が成功割合に影響していることが確認できた（図 8～図 10）。

その際、目的変数の「プロジェクトの成否」については、調査方法の制約で回答者の主観評価としたが、確度を高めるため、コスト・納期・品質・実現範囲・全体の 5 設問を項番 10 に用意し、記憶が鮮明な直近のプロジェクトを回答させるよう工夫した。これら 5 設問の回答結果を信頼性分析した結果、クーロンバックのα係数が 0.916 となり、内的整合性は十分であると判断したため、5 問目の「全体的にプロジェクトは成功だったか」(10-5)の 1 問を指標として代表させることとした。

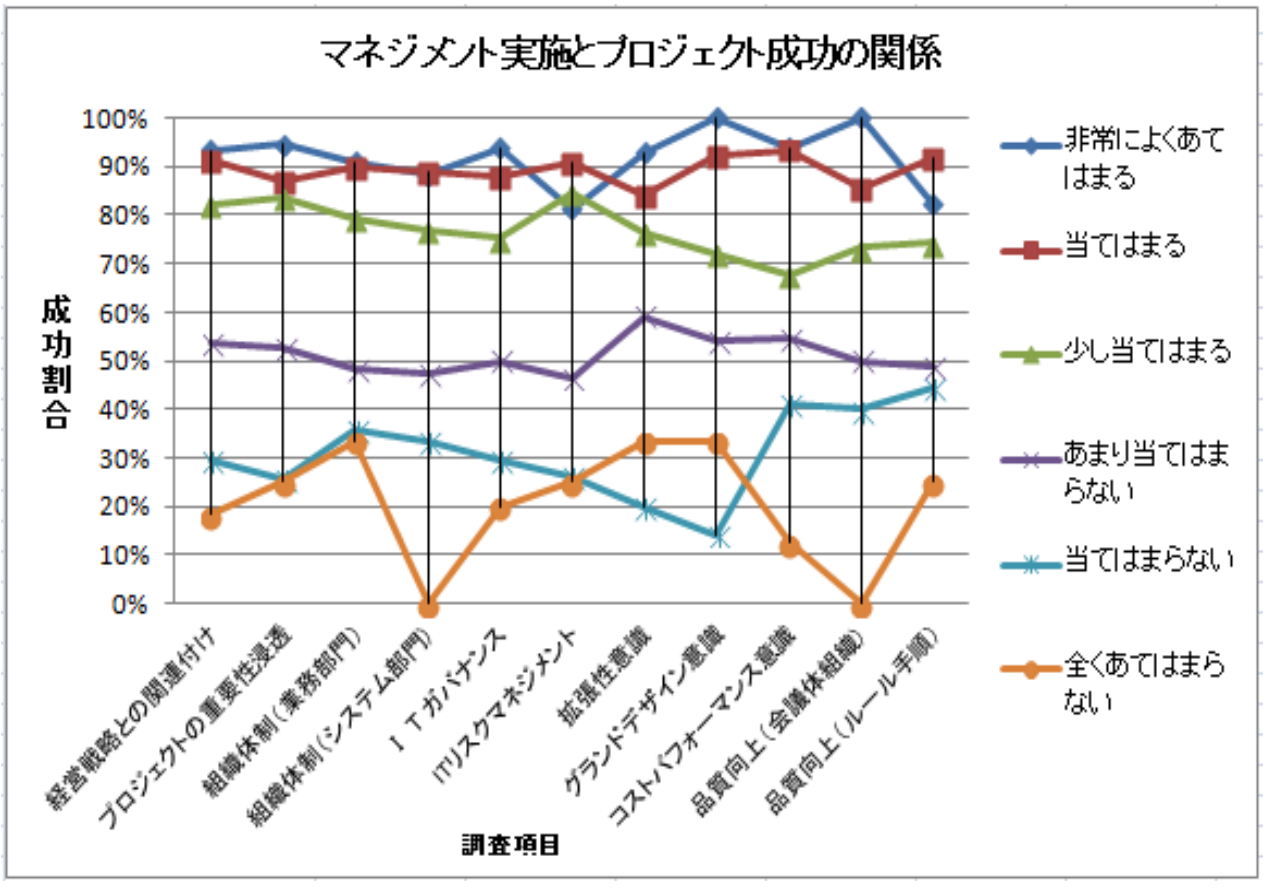


図 8 マネジメント実施とプロジェクト成功の関係

分析にあたっては、プロジェクトの成功が当てはまるとする回答（非常に当てはまる、当てはまる、少し当てはまる）と、当てはまらないとする回答（あまり当てはまらない、

当てはまらない、全く当てはまらない）に 2 分して「プロジェクトの成否」とし、Q11、Q12、Q14 の 33 問に対し、各々クロス集計を行った。これを、グラフ化したものが図 8 から図 10 である。尚、クロス集計の際に、各々カイ二乗検定を行い、「プロジェクトの成否」と各設問（33 問）との関係について、すべて 1%有意水準で確認できた。

まずリスクマネジメント戦略の 6 観点に関わるマネジメント実施とプロジェクト成功の関係に関しては、図 8 の通り、マネジメントを実施したか否かで、成功割合に大きな差があった。実施している（「非常に当てはまる」「当てはまる」）プロジェクトは 9 割程度の成功率があるのに対し、実施しなかった（「当てはまらない」「全く当てはまらない」）プロジェクトは 2 割から 3 割前後しか成功していない。

CEO（経営トップ）関与とプロジェクト成功の関係でも、マネジメント実施ほどの差ではないが、図 9 の通り、差がみられた。実施している（「非常に当てはまる」「当てはまる」）プロジェクトは 8 割以上の成功率があるのに対し、実施しなかった（「当てはまらない」）プロジェクトは 3 割から 5 割程度しか成功していない。

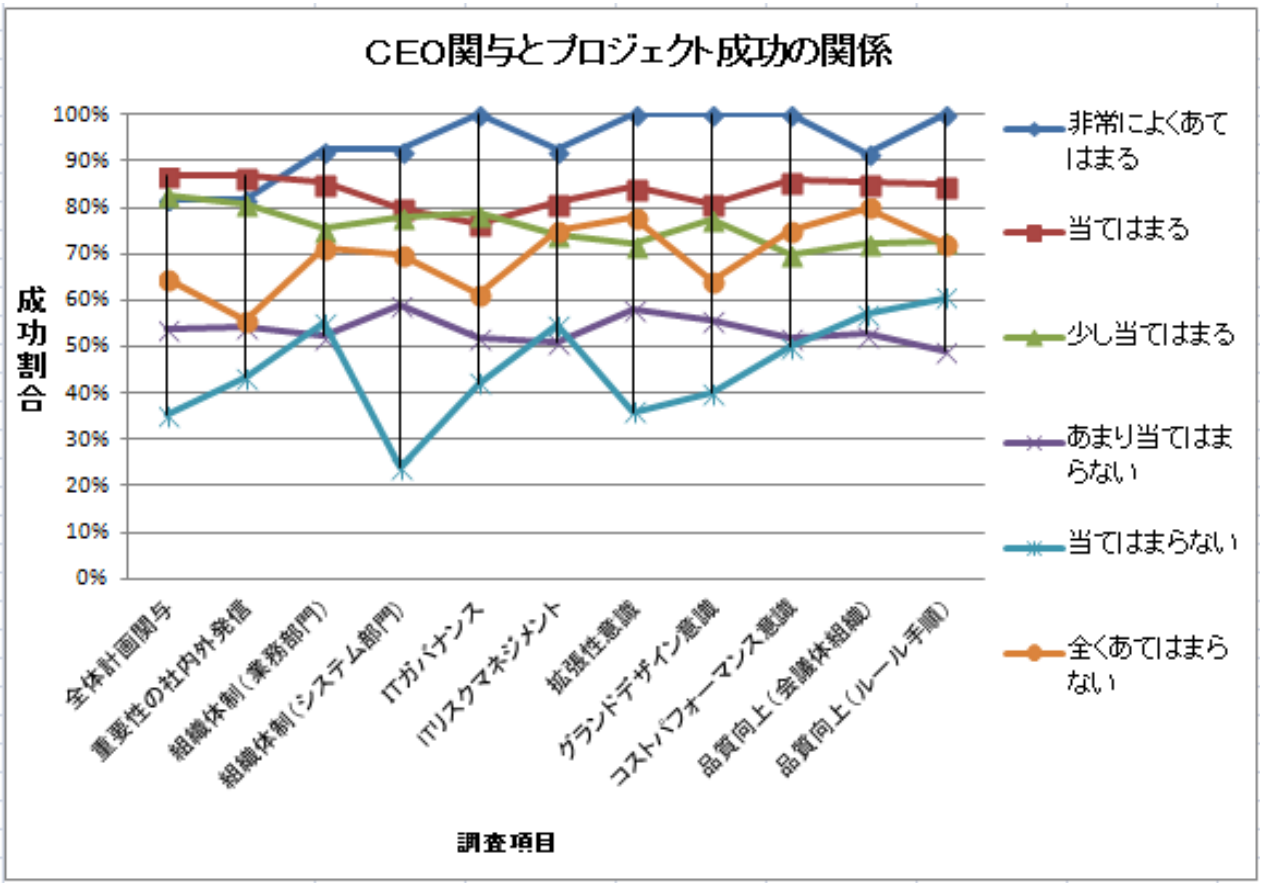


図 9 CEO 関与とプロジェクト成功の関係

CIO（情報システム最高責任者）関与とプロジェクト成功割合でも、図 10 の通り、実施している（「非常に当てはまる」「当てはまる」）プロジェクトは 8 割以上の成功率があるのに対し、実施しなかった（「当てはまらない」）プロジェクトは 3 割から 6 割程度しか成功していない。

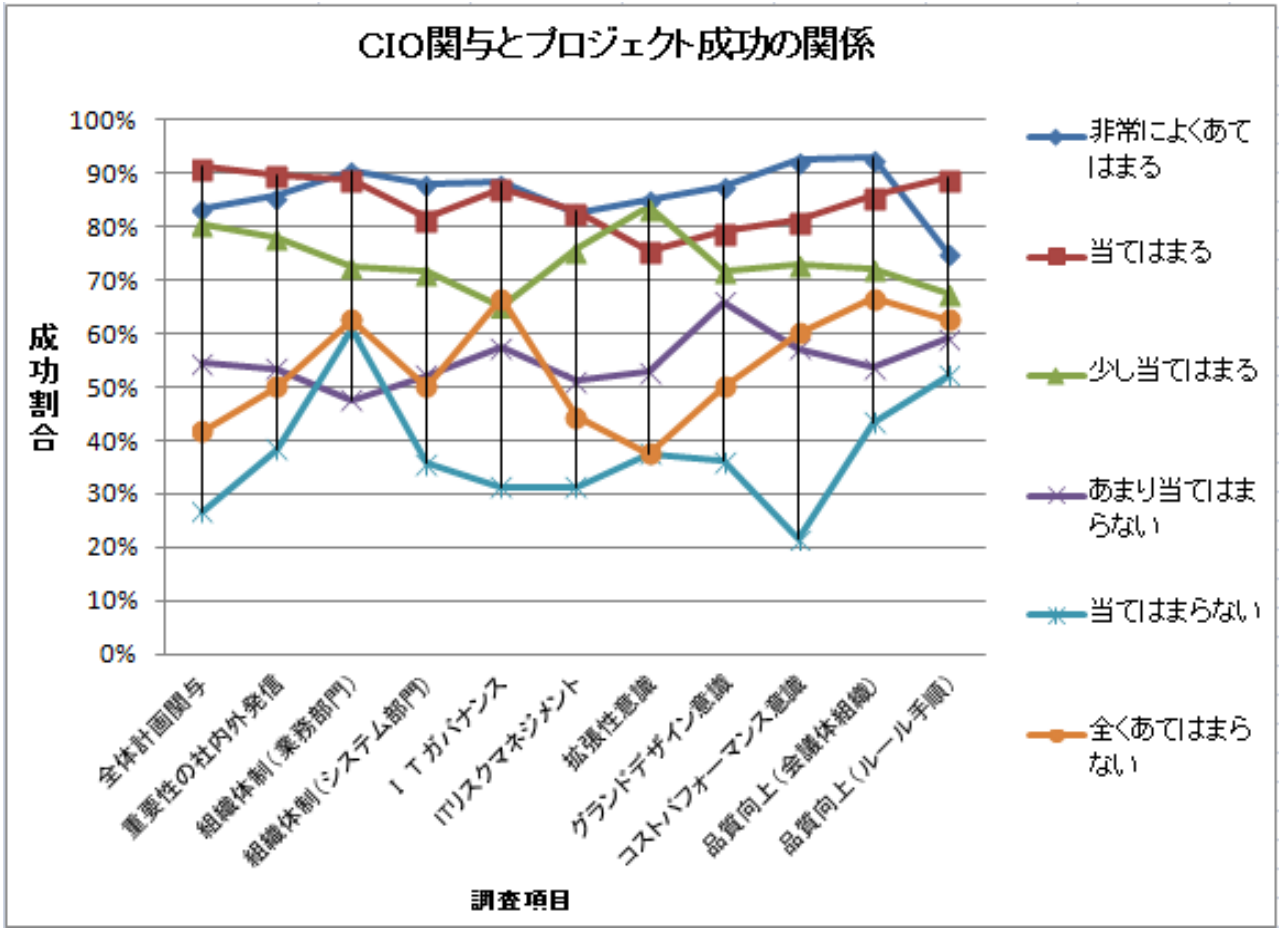


図 10 CIO 関与とプロジェクト成功の関係

CEO、CIO 関与に関しては、全く関与なし（「全くあてはまらない」）の成功率は、関与なし（「当てはまらない」）より 2 割から 3 割程度高くなっている点が特徴的であった。不適切な関与（介入）がされるよりは、むしろ全く関与が無い方が良いということを示唆していると考える。

3.4.3.2. 因子分析による考察

CEO 関与の 11 問、CIO 関与の 11 問、マネジメント実施の 11 問の合計 33 問を通して、因子分析を行った（表 13）。

その結果、3 つの因子での説明が最もあてはまりが良く、第一因子は CIO 関与、第二因子は CEO 関与、第三因子はマネジメント実施と順当な因子構成となった。

表 13　意識調査 33 問の因子分析

質問内容	因子		
	1	2	3
Q14_5_CIOのITガバナンス関与	.903		
Q14_4_CIOの情シ部門組織体制整備関与	.886		
Q14_7_CIOの拡張性意識	.834		
Q14_8_CIOのグランドデザイン意識	.832		
Q14_6_CIOのITリスクマネジメント関与	.794		
Q14_10_CIOの品質向上会議体組織設置関与	.775		
Q14_2_CIOの社内外発信	.744		
Q14_11_CIOの品質向上ルール手順制定関与	.695		
Q14_9_CIOのコストパフォーマンス意識	.687		
Q14_1_CIOの全体計画関与	.664		
Q14_3_CIOの業務部門組織体制整備関与	.602		
Q12_10_経営トップの品質向上会議体組織設置関与		.915	
Q12_5_経営トップのITガバナンス関与		.870	
Q12_7_経営トップの拡張性意識		.833	
Q12_6_経営トップのITリスクマネジメント関与		.831	
Q12_11_経営トップの品質向上ルール手順制定関与		.816	
Q12_4_経営トップの情シ部門組織体制整備関与		.794	
Q12_9_経営トップのコストパフォーマンス意識		.788	
Q12_8_経営トップのグランドデザイン意識		.745	
Q12_3_経営トップの業務部門組織体制整備関与		.632	
Q12_1_経営トップの全体計画関与		.612	
Q12_2_経営トップの社内外発信		.437	
Q11_3_業務部門組織体制整備			.821
Q11_1_経営戦略との関連付け			.803
Q11_8_グランドデザイン意識			.801
Q11_4_情シ部門組織体制整備			.780
Q11_11_品質向上ルール手順制定			.778
Q11_10_品質向上会議体組織設置			.777
Q11_2_重要性の社内浸透			.750
Q11_9_コストパフォーマンス意識			.726
Q11_6_ITリスクマネジメント実施			.718
Q11_5_ITガバナンス良好			.682
Q11_7_拡張性意識			.629

因子抽出法：最尤法　回転法：Kaiserの正規化を伴うﾌﾟﾛﾏｯｸｽ法

第一因子 CIO関与

第二因子 CEO関与

第三因子 マネジメント実施

33 問全体での因子分析の結果を受け、CEO 関与 11 問、CIO 関与 11 問、マネジメント実施 11 問の各カテゴリー内での因子分析を行って更に分析を行うこととした。その結果、CEO 関与、CIO 関与、マネジメント実施とも、3 つの因子での説明が最もあてはまりが良い結果となったが、異なる因子構成となった。

まず、CEO 関与は、表 14 の通り 3 因子で説明ができた。

第一因子は、「組織体制整備関与」、「社内外発信」、「全体計画関与」の項目から、「経営リーダーシップ因子」とした。

第二因子は、「IT リスクマネジメント関与」、「拡張性意識」、「グランドデザイン意識」、「IT ガバナンス関与」という項目が上がり、「先見性リスク認識因子」と命名した。

第三因子は、「品質向上関与」の 2 項目と「コストパフォーマンス意識」であることから、「品質コスト意識因子」と命名した。

表 14　CEO 関与質問の因子分析

CEO(経営トップ)関与質問内容	因子		
	1	2	3
Q12_3_経営トップの業務部門組織体制整備関与	.971		
Q12_2_経営トップの社内外発信	.716		
Q12_4_経営トップの情シ部門組織体制整備関与	.599		
Q12_1_経営トップの全体計画関与	.505		
Q12_6_経営トップのITリスクマネジメント関与		.880	
Q12_7_経営トップの拡張性意識		.766	
Q12_8_経営トップのグランドデザイン意識		.665	
Q12_5_経営トップのITガバナンス関与		.622	
Q12_11_経営トップの品質向上ルール手順制定関与			.957
Q12_10_経営トップの品質向上会議体組織設置関与			.870
Q12_9_経営トップのコストパフォーマンス意識			.440
因子抽出法:最尤法　回転法:Kaiserの正規化を伴うプロマックス法			

CEO関与

第一因子
経営リーダーシップ因子

第二因子
先見性リスク認識因子

第三因子
品質コスト意識因子

CIO 関与も表 15 の通り、3 因子で説明ができる結果となった。

第一因子は、「組織体制整備関与」2 項目、「IT ガバナンス関与」、「IT リスクマネジメント関与」、「社内外発信」、「全体計画関与」の各項目が含まれ、「マネジメント力因子」と命名した。

第二因子には、「品質向上関与」の 2 項目と「コストパフォーマンス意識」が挙がり、「品質コスト意識因子」と命名した。

第三因子には、「拡張性意識」、「グランドデザイン意識」が上がり、「先見性拡張性因子」と命名した。

CEO 関与で第二因子に含まれる「IT ガバナンス関与」「IT リスクマネジメント関与」項目が第一因子に含まれている点が注目される。

表 15　CIO 関与質問の因子分析

CIO関与質問内容	因子		
	1	2	3
Q14_4_CIOの情シ部門組織体制整備関与	.743		
Q14_5_CIOのITガバナンス関与	.711		
Q14_6_CIOのITリスクマネジメント関与	.664		.350
Q14_3_CIOの業務部門組織体制整備関与	.615		
Q14_2_CIOの社内外発信	.614		
Q14_1_CIOの全体計画関与	.477	.329	
Q14_10_CIOの品質向上会議体組織設置関与		.884	
Q14_11_CIOの品質向上ルール手順制定関与		.728	
Q14_9_CIOのコストパフォーマンス意識		.522	
Q14_7_CIOの拡張性意識			.861
Q14_8_CIOのグランドデザイン意識			.708
因子抽出法:最尤法　回転法:Kaiserの正規化を伴うプロマックス法			

CIO関与

第一因子
マネジメント力因子

第二因子
品質コスト意識因子

第三因子
先見性拡張性因子

マネジメント実施は、表 16 の通りとなった。

第一因子は、「経営戦略との関連付け」、「重要性の社内浸透」、「組織体制整備」2 項目が含まれていることから、「戦略組織体制整備因子」と命名した。

第二因子には、「IT リスクマネジメント実施」、「IT ガバナンス良好」、「拡張性意識」、「グランドデザイン意識」が挙がり、「先見性ガバナンス因子」とした。第一因子と第二因子は、CEO 関与の因子と各々構成項目は同一であるが、組織マネジメントを意識した因子名称とした。

第三因子には、品質向上関与の 2 項目が挙がり、「品質意識因子」と命名した。

表 16　マネジメント実施質問の因子分析

マネジメント実施質問内容	因子		
	1	2	3
Q11_1_経営戦略との関連付け	.874		
Q11_2_重要性の社内浸透	.758		
Q11_3_業務部門組織体制整備	.714		
Q11_4_情シ部門組織体制整備	.617	.331	
Q11_9_コストパフォーマンス意識	.301		
Q11_6_ITリスクマネジメント実施		.942	
Q11_5_ITガバナンス良好		.691	
Q11_7_拡張性意識		.663	
Q11_8_グランドデザイン意識		.513	
Q11_10_品質向上会議体組織設置			.889
Q11_11_品質向上ルール手順制定			.820
因子抽出法:最尤法　回転法:Kaiserの正規化を伴うプロマックス法			

マネジメント実施

第一因子
戦略組織体制整備因子

第二因子
先見性ガバナンス因子

第三因子
品質意識因子

CEO 関与と CIO 関与に関しては、CEO はリーダーシップ、CIO はマネジメントといった要素が最重要であるが、その次には、CEO はリスク認識と先見性と言った将来につながる点への関与が優先され、CIO は品質やコストと言った現実的な実務への関与が優先されるとの示唆が得られた。

マネジメント実施に関しては、経営戦略との関連付けや、組織体制の整備が成されていることが、重要であることが示唆された。

3.4.3.3. 重回帰分析による考察

前節の因子分析の結果を受け、各因子のプロジェクトの成功への影響度度合いを分析するため、被説明変数を「全体的にプロジェクトは成功」（項番 10-5）として、表 17 の通り、重回帰分析を行った。CEO 関与と CIO 関与に関しては、調整済 R2 乗の当てはまりが良くないため、あくまで参考ではあるが、以下の示唆が得られた。

まず、CEO 関与に関しては、「経営リーダーシップ因子」の影響が 10%有意となり、「先見性リスク認識因子」は有意とはならなかったが、比較的高い重回帰係数が得られた。

CIO 関与に関しては、「マネジメント力因子」の影響が 5%有意の相関性を示し、「品質コスト意識因子」は、有意とはならなかったが、比較的高い重回帰係数が得られた。

表 17　プロジェクトの成功の重回帰分析

CEO関与とプロジェクトの成功	B	ベータ	t 値	有意確率	VIF	CEO：リーダーシップ因子が有意。先見性リスク認識因子も高い重回帰係数。
（定数）	4.022		48.439	.000		
CEO経営リーダーシップ因子	.299	.213	1.782	.076	3.682	
CEO先見性リスク認識因子	.259	.185	1.282	.201	5.417	
CEO品質コスト意識因子	-.019	-.013	-.110	.912	3.794	
調整済R2乗	.126					
F値 （有意確率）	11.901					

CIO関与とプロジェクトの成功	B	ベータ	t 値	有意確率	VIF	CIO：マネジメント力因子が有意。品質コスト意識因子も高い重回帰係数。
（定数）	4.022		50.332	.000		
CIOマネジメント力因子	.369	.264	2.000	.047	4.854	
CIO品質コスト意識因子	.217	.155	1.408	.161	3.378	
CIO先見性拡張性因子	.078	.055	.491	.624	3.512	
調整済R2乗	.191					
F値 （有意確率）	18.776					

マネジメント実施とプロジェクトの成功	B	ベータ	t 値	有意確率	VIF	マネジメント実施戦略組織体制整備因子、先見性ガバナンス因子が有意。
（定数）	4.022		59.654	.000		
戦略組織体制整備因子	.601	.428	4.220	.000	4.029	
先見性ガバナンス因子	.240	.171	1.725	.086	3.844	
品質意識因子	.131	.093	1.026	.306	3.228	
調整済R2乗	.424					
F値 （有意確率）	56.46					

マネジメント実施に関しては、「戦略組織体制整備因子」が 1%有意であり、「先見性ガバナンス因子」も 10%有意が認められた。

3.4.3.4. 共分散構造分析による考察

3.4.3.1 の仮説の検証、3.4.3.2 の因子分析による考察、3.4.3.3 の重回帰分析による考察を踏まえ、プロジェクトの成功につながる要因の関係性をモデル化するため、共分散構造分析を利用した探索的パス解析を行った。プロジェクトの成功要因の候補として、3.4.3.1

で検証された CEO 関与、CIO 関与、マネジメント実施それぞれと、更にそれらを分解した 3.4.3.2 の因子分析の結果を用いてモデルを検討した。

CEO 関与、CIO 関与、マネジメント実施の相互関係については、CEO 関与と、CIO 関与については、影響しあうものの一方向の因果関係は認められなかったが、マネジメント実施と、プロジェクトの成功の因果関係は明確であった。

また CEO 関与や CIO 関与により、マネジメント実施が高まるという、因果関係が認められた。その結果、CEO 関与、CIO 関与が、マネジメント実施を経て、プロジェクトの成功につながるというパスのモデルが、最も当てはまりの指標が高くなった。

更に CEO 関与、CIO 関与、マネジメント実施の各々を因子で捉えるか、全体で捉えるかに関しても、より詳細に探索的パス解析を試みた。その結果、CEO 関与、CIO 関与に関しては、因子分析結果である 3 因子に分解したときに当てはまりの指標が高くなった。一方、マネジメント実施については、マネジメント実施設問 11 問の平均値を用いたときに最も当てはまりの指標が高くなった。

最終的に、3 因子から構成される CEO 関与と、同じく 3 因子から構成される CIO 関与が、社内のマネジメント実施に影響を与え、それがプロジェクトの成功につながるというモデルが示唆された（図 11）。

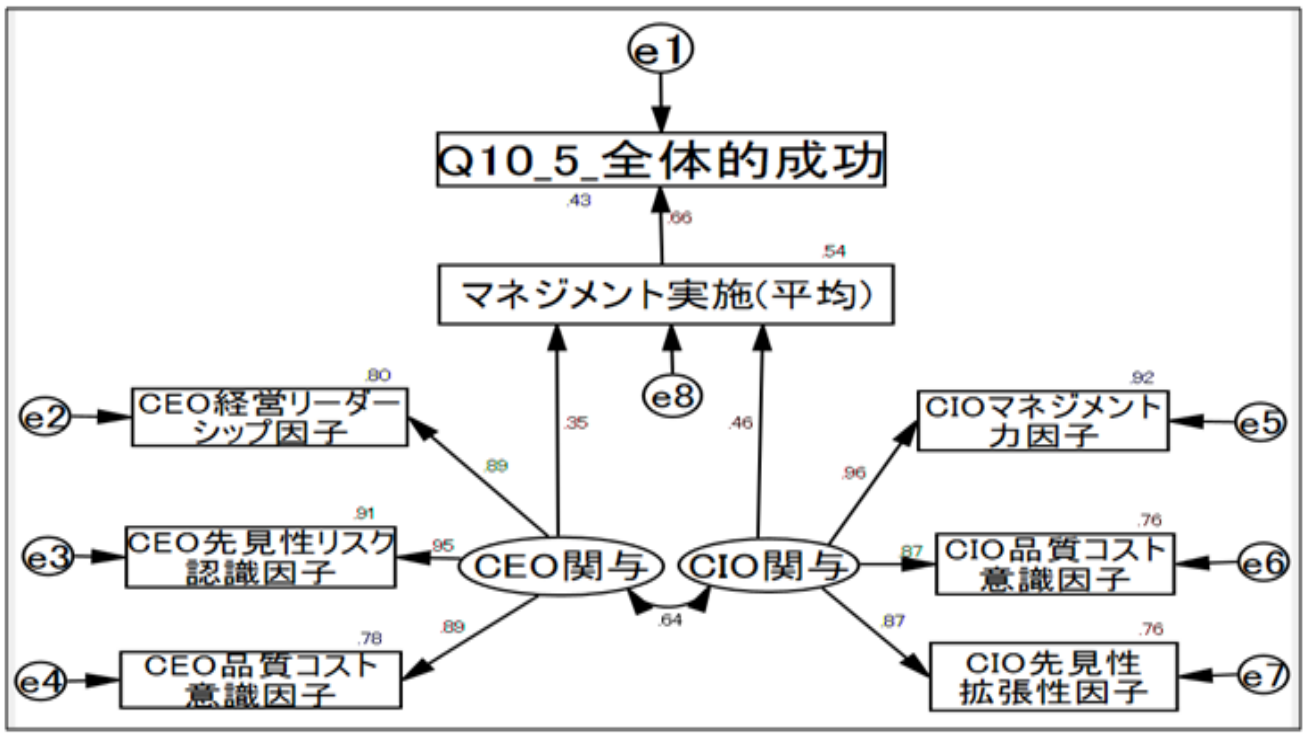


図 11　CEO 関与、CIO 関与、マネジメント実施での共分散構造分析モデル

CEO の関与では、3 因子の中で、「CEO 先見性リスク認識因子」の係数が最も高く、CIO 関与では「CIO マネジメント力因子」の係数が最も高くなった。

モデルの妥当性を示す共分散構造分析の各指標は表 18 の通りである。

表 18　共分散構造分析の指標

カイ二乗	自由度	有意確率	GFI	CFI	RMSEA
53.482	18	.000	.945	.977	.093

まず、カイ二乗、自由度、有意確率については、有意確率は 0.000 となり問題ない。

GFI（Goodness of Fit Index）については、モデルの適合度の指標であり、1 に近いほど説明力があるとされており、一般的に 0.9 以上が「説明力があるパス図」とされている。また CFI(Comparative Fit Index)は、0.95 以上が良いと言われており、両指標とも適合を示唆している。RMSEA（Root Mean Square Error of Approximation）は、モデルの分布と真の分布の乖離を 1 自由度当たりの量として表現した指標で、0.05 以下は当てはまりが良く、0.1 以上は当てはまりが悪いとされているが、本件は当てはまりが相応な範囲に入っている。以上からこのモデルは有意な適合性があるものと示唆される。

また、重回帰分析と以下 2 点の符合が確認できた。

第一は、 CEO 関与、CIO 関与がプロジェクトの成否に直接影響があるという関係を探索したものの、間接的な関係しか見出すことができなかった点である。これは、重回帰分析で、CEO 関与と CIO 関与のプロジェクトの成功への関係について、調整済 R2 乗の当てはまりが良くない点と符合している。

第二は、マネジメント実施については、平均値を用いたときに当てはまりが高くなった点である。これは、重回帰分析結果で「戦略組織体制因子」と「先見性ガバナンス因子」双方が有意であり、全体にも相応の当てはまりが認められた点と符合している。

因子分析、重回帰分析、共分散構造分析の結果から 2 点の示唆を得ることができた。

第一に、CEO 関与の「経営リーダーシップ因子」や CIO 関与の「マネジメント力因子」、マネジメント実施での「戦略組織体制整備因子」の 3 因子は全体での経営のリーダーシップや、マネジメント力によるものであり、リスクマネジメント戦略の 6 観点の中でも、経営リーダーシップやマネジメント力が、プロジェクトの成否につながる最重要な要素であることが考察できる。

第二に、CEO と CIO の役割の相違点が示唆された。すなわち、CEO は、全体計画関与、組織体制整備、社内外発信のリーダーシップに加え、先見性、リスク認識が重要である一

方、CIO は、リスクマネジメント、IT ガバナンスに加え、品質やコストを意識した実務的なマネジメントが重要であることが示唆された。

3.4.3.5. 理想と現実の差異（ギャップの分析）

意識調査の中で、経営トップ（CEO）と CIO について、現状と同時に理想の状況を調査し、その差を比較したところ、すべて有意差があった（表 19）。有意差の検定に関しては、対応のある t 検定の結果を記載した。尚、対応サンプルによる Wilcoxon の符号付き順位検定も行ったが、対応のある t 検定の結果と最大で 0.02 の差に留まり、有意に差が生じるものは無かった。

表 19 理想と現実のギャップの分析

経営トップ（CEO）	理想	現状	差	有意確率
1 経営トップの全体計画関与	3.84	3.55	0.29	0.000
2 経営トップの社内外発信	4.00	3.65	0.35	0.000
3 経営トップの業務部門組織体制整備関与	3.92	3.72	0.20	0.100
4 経営トップの情シ部門組織体制整備関与	3.98	3.75	0.23	0.003
5 経営トップのITガバナンス関与	4.06	3.77	0.29	0.001
6 経営トップのITリスクマネジメント関与	4.09	3.80	0.29	0.000
7 経営トップの拡張性意識	3.97	3.75	0.22	0.007
8 経営トップのグランドデザイン意識	4.04	3.67	0.37	0.000
9 経営トップのコストパフォーマンス意識	3.96	3.81	0.15	0.041
10経営トップの品質向上会議体組織設置関与	3.95	3.63	0.32	0.000
11経営トップの品質向上ルール手順制定関与	3.81	3.52	0.29	0.001
CIO				
1 CIOの全体計画関与	4.18	3.79	0.39	0.000
2 CIOの社内外発信	4.22	3.74	0.48	0.000
3 CIOの業務部門組織体制整備関与	4.11	3.81	0.30	0.000
4 CIOの情シ部門組織体制整備関与	4.27	4.08	0.19	0.010
5 CIOのITガバナンス関与	4.24	4.03	0.21	0.003
6 CIOのITリスクマネジメント関与	4.33	4.01	0.32	0.000
7 CIOの拡張性意識	4.31	3.96	0.35	0.000
8 CIOのグランドデザイン意識	4.31	3.92	0.39	0.000
9 CIOのコストパフォーマンス意識	4.27	3.98	0.29	0.000
10CIOの品質向上会議体組織設置関与	4.17	3.88	0.29	0.000
11CIOの品質向上ルール手順制定関与	4.14	3.76	0.38	0.000

経営トップ（CEO）に対して、差が大きい（0.3 以上）項目としては、8 の「グランドデザイン意識」、2 の「社内外発信」、10 の「品質向上会議体組織設置関与」となった。

これは、経営トップに対しては、経営戦略と長期的なグランドデザインレベルの IT 戦略への意識や、社内外への発信力や、品質向上会議体組織への関与等を期待しているものと考えられる。

CIO に対して、差が大きい（0.3 以上）項目としては、2 の「社内外発信」、1 の「全体計画関与」、8 の「グランドデザイン意識」、11 の「品質向上ルール手順制定関与」、7 の「拡張性意識」、6 の「IT リスクマネジメント関与」、3 の「業務部門組織体制整備関与」が示された。経営トップ以上に理想（期待）と現実のギャップのある項目が多いという結果であり、以下 3 点を分析できる。

第一に、情報システムプロジェクトの直接の最高責任者である CIO の実務マネジメント面への期待の高さを示したものと考えられる。

第二に、CIO に期待されるマネジメントには、「社内外発信」、「業務部門体制整備」という経営全体への影響力行使や、「全体計画」への関与に加え、「グランドデザイン意識」という将来の情報システムの構想を持つことが求められているものと考えられる。

第三に CEO と CIO の両者に共通するギャップ項目として、「社内外発信」と「グランドデザイン意識」があった。これは、情報システム開発の重要性について、情報システム開発に関与する金融機関従業員の期待ほどには発信されておらず、将来に向けたグランドデザインについても、期待ほどには経営者に意識されていないということを表しているものと言え、経営者と実務者の間のコミュニケーションがより必要な項目と言える。

3.4.4. 問題意識調査のまとめ

仮説の検証、因子分析、重回帰分析、共分散構造分析、ギャップの分析を総合して、問題意識調査全体を総括すると、以下の 5 点にまとめることができる。

第一に、全体として、リスクマネジメント戦略の 6 観点（CORE-OQ）に基づいたマネジメント実施の有効性が、金融情報システム開発に関与する金融機関従業員の視点で検証することができた。また、共分散構造分析の結果から、経営者関与の重要性は否定されないものの、マネジメント実施体制の構築が結果として成されることが、より重要であることが示唆された。

第二に、CIO に対して、期待が高まっていることが確認できた。特にギャップの分析の結果がそれを表している。具体的には、社内外への発信力や影響力の拡大に加え、品質コスト意識や具体的なルール制定等を含めた情報システム部門への実務的な関与が、CIO に求められていることが、明らかになった。その背景として、金融情報システムの変化と複雑化に対し、CEO の直接的な関与が困難になる状況があると考えられる。

第三に、CEO に対しては、CIO への使命付けがより求められているとも言える。組織における CEO と CIO の属性によるが、一般的には CIO には金融情報システムの将来像を意識して、実務を適切にマネジメントできる人材を登用し、CEO が CIO の使命付けを明確にして発信し、経営に関与させながら、支援することが有効であると考える。

第四に、重回帰分析の結果から、CEO については、経営リーダーシップ面と、先見性リスク面を意識することが重要であり、一方、CIO については、マネジメント面と、品質コスト面について特に意識することが必要であるとの示唆があった。

第五に、3.4.3.1 で、CEO や CIO の不適切な関与（介入）が、マイナスに働く可能性もあるとの示唆もあった。また、ギャップの分析において、「社内外発信」や「グランドデザイン意識」のギャップが CEO と CIO の両者に共通していた。これらは、CEO、CIO、情報システムマネジメントの相互間のコミュニケーションを図ることが、重要であることを示唆している。

最後に全体を総括すると、本意識調査の結果や、リスクマネジメント戦略の 6 観点を参考にして、CEO、CIO、情報システムマネジメントの関係や役割分担を見直すことで、現実的でかつ効果的な連携が実現できると考える。

3.5. 運用局面でのリスクマネジメント

前節までは、開発局面での考察であったが、金融情報システムが運用局面になってからのリスクマネジメントも重要である。そこで本節では、金融情報システムの信頼性実現の観点で、対外的に最も重要と考えられる障害の再発防止策に焦点をあてる。まず、2007 年から 2011 年にかけての代表的障害事例について分析する。その後、2011 年の大手銀行での障害（3.5.1.2 事例 1：M 銀行振込大幅遅延で詳述する）を受けて、日本銀行や情報処理推進機構で策定、公開された障害防止対応文献に言及した上で、考察する。

3.5.1. 障害事例[22]

2007 年から 2011 年の金融情報システムにおける代表的障害事例を分析する。銀行部門と市場部門の直近 2 事例については、経緯詳細も含めて分析し、リスクマネジメント戦略の 6 観点の適合状況を確認し、新たに追加すべき要素や、適用にあたっての留意点がないかを検討考察する。

3.5.1.1. 失敗事例での顕在化リスク

本論文では、「失敗」を金融情報システムの失敗と金融情報システム開発の失敗に分け、定義した（1.2.8 項、1.2.9 項）。

金融情報システムの失敗に関しては、ある金融情報システムを原因として、外部から直接評価されるリスク（マイナスの結果を産むリスク、純粋リスク。具体的には、オペレーショナルリスク、ビジネスリスク、戦略リスク、風評リスク、法務・規制リスク）起因の事象が、マスコミ等で取り上げられる等で対外的に顕在化した場合、失敗と定義する。

一方、金融情報システム開発の失敗とは、対外的には失敗であることが表面化していない場合も含め、システム開発プロジェクトに関して、計画時の工期ないし、予算を守れないか、品質に不満があると評価されたシステム開発と定義する。また、工期及び予算を達成し、品質についても満足との評価があっても、外部から直接評価されるマイナスのリスクがマスコミ等で取り上げられて、対外的に表面化した場合（金融情報システムの失敗）も、金融情報システム開発の失敗でもあるとする。

ここでは、金融情報システムの失敗事例について、要件で不十分なものと顕在化したリスクを示す(表 20)。リスク欄の×印が不十分な要素ないし顕在化したリスクである。尚、

[22] 本項は、「金融事業経営における情報システム開発のリスクマネジメント観点の提案」[遠藤正之、高野研一, 2013a]を元にしている。

戦略リスクについては、システム開発プロジェクト自体の頓挫や延期が発生した場合、金融情報システム開発戦略自体の失敗となり、戦略リスクが顕在化すると考えた。

表 20 最近の金融情報システム失敗事例分析

(時期、業態)失敗ないしトラブルの内容、経営への影響	6 観点						顕在化リスク				
	経営コミットメント	組織体制ガバナンス	IT リスクマネジメント	拡張性一貫性	要件定義最適化	品質重視	オペレーショナル	ビジネス	戦略	風評	法務規制
(2007 年銀行)新勘定系システムの開発が頓挫、ベンダーと訴訟中	―	―	×	×	×	―	―	×	×	×	×
(2007 年銀行)顧客情報管理の名寄せの障害。受入限度額管理ができず、一部営業店で新規口座開設停止	―	―	×	―	―	―	×	×	―	×	―
(2008 年取引所)前月リリースの派生売買システムの障害により、一部銘柄取引の停止	―	―	―	―	×	×	×	×	―	×	―
(2008 年取引所)為替取引システム停止	―	―	×	×	―	―	×	×	―	×	―
(2008 年生保)7000 件の特約還付金に計算間違い。15 年間発覚せず	―	―	×	―	―	×	×	―	―	×	―
(2008 年証券)株の平均取得単価誤算出を 5 年間放置→関東財務局の業務改善命令	―	―	×	―	×	―	×	―	―	×	―
(2008 年証券)相次ぐトラブル、7 時間のサービス停止→金融庁から 3 度の業務改善命令	―	―	×	×	―	―	×	×	―	×	―
(2009 年銀行)勘定系システムの刷新を 1 年延期	―	―	×	―	―	―	―	―	×	×	―
(2009 年取引所)5 日前に稼働したシステムがダウン	―	×	×	×	―	×	×	×	―	×	―
(2009 年生保)顧客情報約 3 万 2 千件流出→金融庁から業務改善命令、推定 429 億円の減収	―	―	×	―	―	―	×	×	―	×	―
(2010 年外為証拠金取引)ﾊﾞｰｼﾞｮﾝｱｯﾌﾟ後の半年で、15 回のトラブル。→金融庁から業務改善命令、主力サービス停止により業界首位から転落	―	―	×	―	―	×	×	×	×	×	―
(2010 年銀行)他行振込データ受渡不能、ATM で他行カード利用不可	―	―	―	―	―	―	×	―	―	×	―
(2011 年銀行)振込大幅遅延、ATM 停止→金融庁から業務改善命令、頭取更迭、銀行統合へ	×	×	×	×	×	×	×	×	×	×	―
(2012 年取引所)株式売買システムの障害により、241 銘柄の売買が午前中停止	×	×	×	―	―	×	×	×	×	×	―

(日経コンピュータ連載「動かないコンピュータ」等から筆者が分析)
注)【6 観点】×:不十分、ー:無関係ないし不明、
【顕在化リスク】×:顕在化、ー:特に顕在化せず

失敗事例については、情報の公開が限定されているため、開発時に経営者のコミットメントや IT ガバナンスの状況等を正確に把握することは困難である。ただ、金融情報シス

テムの失敗により、顕在化するリスクが極めて多いことが把握できる。経営戦略と IT 戦略が整合性を取り、経営者、業務部門、システム部門の適切な体制のもとで、コミュニケーション良く開発プロジェクトが進められていれば、リスクが顕在化する失敗とならなかったケースも多いと考えられる。

3.5.1.2. 事例 1：M 銀行振込大幅遅延

1）発生時系列推移

月曜日にテレビ局 A 社の義援金口座 a へ大量の振込が集中し、夜間バッチの 1 口座当たり処理可能件数（リミット値）を上回り、22 時 7 分に夜間バッチが異常終了した。

その後、異常終了の欠落データ復元作業が難航し、翌火曜日朝になってもバッチ処理の完了目途が立たなかった。営業店端末開局を優先するため、翌火曜日 7 時頃夜間バッチ処理を中断し、バッチ日替り処理を実施した。その結果、通常自動化されている夜間バッチ処理のシステム運行が手動に切り替わり、3 万ジョブに及ぶ膨大な作業を手作業で行うこととなり、二重振込や処理漏れといった二次的三次的なトラブルが連鎖的に発生することとなった。

翌火曜日にも、B 携帯電話事業者の義援金口座への大量振込集中により、対外接続系システムでの受け入れ可能なデータ量のリミット値を上回ったため、水曜日の朝 7 時 17 分に夜間バッチ処理の異常終了が発生した。そこで、営業店端末開局を優先するため、前日に引きつづいて夜間バッチ処理を中断し、バッチ日替り処理を実施せざるを得なくなった。

前日の処理に引き続き、膨大な手作業処理が発生し、夜間バッチ処理の大幅遅延につながり、金曜日まで遅延件数は積み上がった。この遅延に派生して、ATM の利用停止や利用制限、ダイレクトチャネルの利用制限といった対顧客宛に影響の大きい事象も発生した。

2）原因分析

リスクマネジメント戦略の 6 観点で分析したところ、すべて不十分であることが判明した。第 1 の「経営トップのコミットメントと支援」に関しては、経営者サイドでのシステム全体を指揮する人材が見当たらず、経営者へのトラブルの報告も発生から半日以上経過していた。第 2 の「組織体制と IT ガバナンス」に関しては、システムを熟知する人材の育成が不十分であると共に、事前のユーザー部門とシステム部門の情報共有が不十分であり、トラブルの対応においても関係者間の指揮命令系統が整理されず、連絡体制も不十分であった。第 3 の「IT リスクマネジメント」に関しては、未然防止観点で、為替システ

ム、夜間バッチの仕組みに対するリスク認識不十分で、定期的な見直しの仕組や実効性のあるシステム監査がワークしていなかった。第 4 の「拡張性一貫性確保」についても、バッチ処理の処理可能件数に対してのシステム部門の認識が不十分で、一旦異常終了すると膨大な手作業が発生するという点で問題があった。第 5 の「要件定義最適化」についても、手作業事務の増大に対しての対策が取られないまま、新たな機能や処理が追加されていった点で問題があった。第 6 の「品質重視の仕組構築」についても、新商品開発に当たり、バッチの負荷を確認するテストが行われないなど、非機能要件の確認が不十分で、BCP（Business Continuity Plan）の検討や、訓練が不十分なままであった点で、品質は不十分であった。

3.5.1.3. 事例 2：TS 取引所一部銘柄取引停止

１）発生時系列推移

午前 1 時半：相場情報を配信する情報通信ゲートウェイサーバー8 台のうちの 1 台でハード障害が発生。検知した運用ベンダー担当者が診断レポートを出力し、保守ベンダーと TS 取引所担当に連絡。保守ベンダーの担当 SE は、携帯電話の小さい画面で情報が不十分な状態でレポートを一人で分析し、他のサーバに処理が引継がれると誤判断した。保守ベンダーから他のサーバへ引継がれる旨の報告を受けた TS 取引所担当者は、自ら確認することなく、売買業務への影響は無いと判断し、エスカレーションもしなかった。

翌午前 7 時：オペレーターが出勤したところで、再度異常メッセージが表示され、予備系への切替引継ぎができていないことが判明。この段階で担当役員の携帯電話を呼び出すが、出勤途上で連絡取れず。

午前 8 時：担当役員が出勤し、対応を関係者と協議。

午前 8 時 40 分：システム復旧作業が進まないため、回復を断念し、一部銘柄（241 銘柄）の売買停止を決断。

２）原因分析

リスクマネジメント戦略の 6 観点で分析したところ、4 つの点で不十分であることが判明した。第 1 の「経営トップのコミットメントと支援」に関しては、待ったなしの状況にありながら、経営者サイドとの連携が不十分で対策が後手に回った。第 2 の「組織体制と IT ガバナンス」に関しては、運用トラブルが発生した場合の解析担当が保守ベンダーの SE 一人であり、組織的な対応が成されていなかった。TS 取引所側も担当一人が、連絡役

としての機能しか果たさなかった。第 3 の「IT リスクマネジメント」に関しては、未然防止観点でのバックアップ切替の仕組みができていた点は良かったが、それに慢心し、切替を見届けるという基本動作が不十分であった。第 4 の「拡張性一貫性確保」については、本件は無関係であると考えられる。第 5 の「要件定義最適化」についても、本件は運用面の問題であり無関係であると考えられる。第 6 の「品質重視の仕組構築」については、障害時運用の実態に関して、小さい携帯電話での分析を行わなければならない等、実際の障害運用状況に応じたマン・マシーンインターフェースや、再鑑を行う等の運用の検証や訓練が不十分であったと言える。

3.5.1.4. 事例研究のまとめと示唆

直近の失敗 2 事例に関し、リスクマネジメント戦略の 6 観点の状況と顕在化リスクについて、纏めた（表 21）。その結果、失敗事例では、6 観点の多くが不十分であることが、明らかになった。

表 21　失敗 2 事例のリスクマネジメント戦略の 6 観点と顕在化リスク

リスクマネジメント戦略の 6 観点		M 銀行振込大幅遅延	TS 取引所一部銘柄取引停止
6 観点	経営トップのコミットメントと支援	×経営者への障害連絡体制、手順が不十分。	×経営との連携に不備あり
	組織体制と IT ガバナンス	×システムの責任役員体制が取られなかった。	×夜間の障害対応体制に不十分な点があり
	IT リスクマネジメント	×リスク評価不適切のまま見直されず。監査も機能せず	×現場でのリスクマネジメント不十分
	拡張性一貫性確保	×バッチ処理の処理可能件数自体と担当者の認識が不十分	―
	要件定義最適化	×全体を理解できる人材が欠如、現場のトラブル対応力不十分。	―
	品質重視の仕組構築	×非機能や運用の品質確保が不十分	×障害時運用の品質確保が不十分
顕在化リスク	オペレーショナルリスク	×障害長期化	×障害が複数回発生
	ビジネスリスク	×他銀行へ取引流出	×取引の停止
	戦略リスク	×事後処理への忙殺	×システムの信頼性低下
	風評リスク	×イメージ低下大	×イメージ低下
	法務規制リスク	―	―
注)【6 観点】×:不十分、－:無関係【顕在化リスク】×:顕在化、－:特に顕在化せず			

3.5.2. システム障害管理体制の実効性向上に向けた留意点[23]

日本銀行は、金融機関の「システム障害管理体制の実効性確保に向けた留意点」を「障害発生の未然防止対策」「障害発生時の対応準備」「障害管理に対する経営陣の関与」の 3 つの観点から取り纏めている（図 12） [日本銀行金融機構局, 2012]。

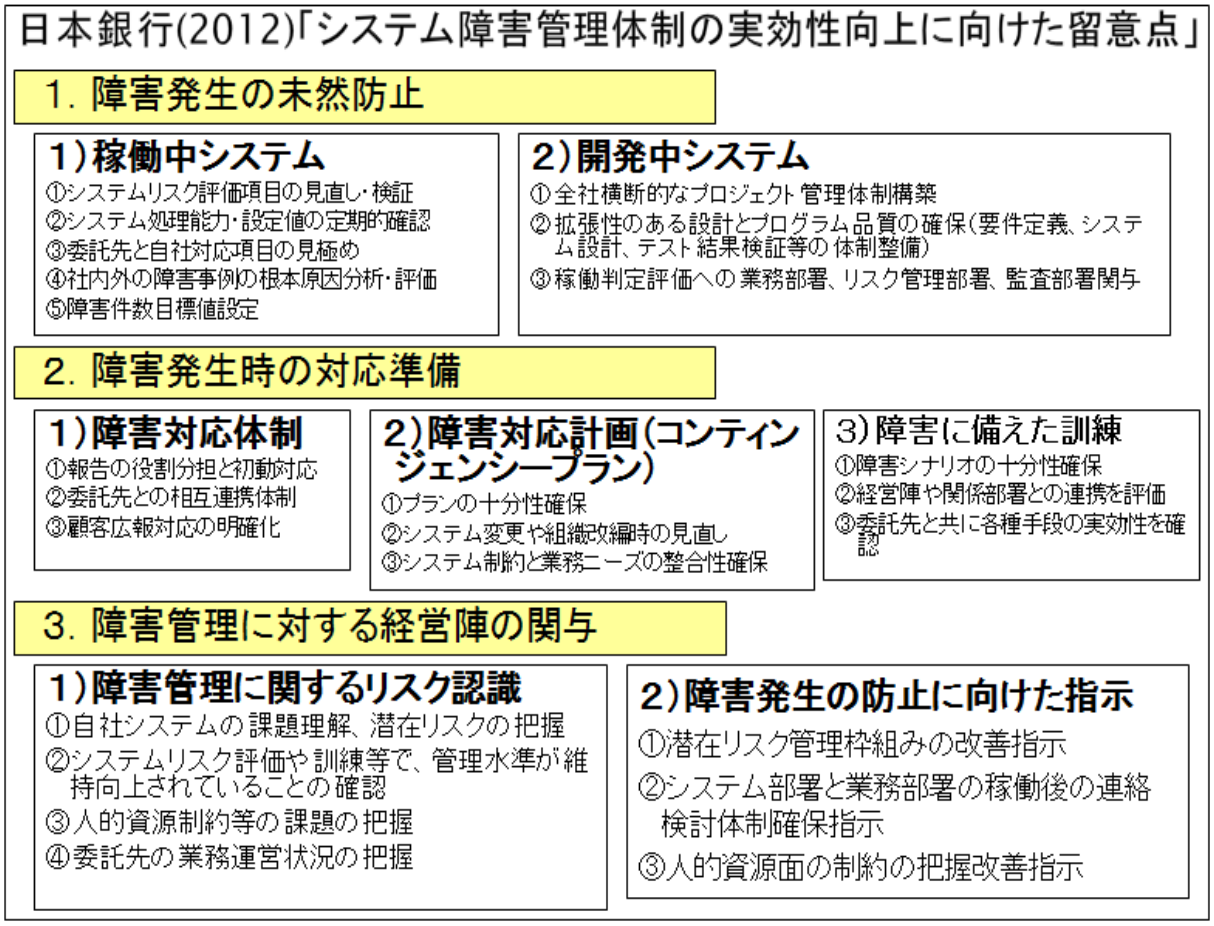


図 12 システム障害管理体制の実効性向上に向けた留意点

3.5.2.1. 障害発生の未然防止対策

障害発生の未然防止対策については、稼働中のシステムと開発中のシステムに分けて未然防止対策を挙げている。

第一に、稼働中のシステムに関して、時間の経過に伴う社内外の環境の変化により潜在リスクが蓄積することを認識し、そのリスクへの対策を適切に取ることが重要としている。環境変化については、以下 3 項目を挙げている。

[23] 本項は、「金融情報システム障害の再発防止についての一考察」[遠藤正之, 2013]を元にしている。

1）インターネット取引、携帯電話モバイル端末経由取引の増加、サービス提供時間拡大等による突発的な事務量増加、処理能力の不足、

2）接続先の拡大、重要業務を担うＥＵＣの増加によるシステム構成複雑化を起因とするシステム変更作業時の設定ミス、考慮漏れ、

3）新技術の採用、汎用端末化による外部からの不正アクセスやウィルス感染。

その上で、稼働中システムのリスク対策として以下 5 項目を挙げている。

1）システムリスク評価、

2）システム処理能力・設定値の定期的確認、

3）委託先管理、

4）障害事例分析、

5）障害件数目標値の設定。

第二に、開発中のシステムについても、以下の 3 項目の留意点を挙げている。

1）全社横断的な管理体制構築による、関係部署間の情報共有と認識相違を生じさせない。

2）要件定義やシステム設計テスト結果の検証について適切な体制を取る。環境変化に対応した拡張性とプログラム品質を確保する。

3）開発したシステムが本番稼働に耐えるかどうかを確認する。稼働判定は業務部署やリスク管理部署等の評価を踏まえて行う。

3.5.2.2. 障害発生時の対応準備

「障害発生時の対応準備」としては、「障害対応体制」「障害対応計画（コンティンジェンシープラン)」「障害に備えた訓練」の 3 点が重要としている。

1）障害対応体制…報告ルール、連絡体制、顧客広報対応を事前設定する。システム部署への過度の集中を避ける点と経営陣への報告での迅速性の重視が留意点となる。

2）障害対応計画（コンティンジェンシープラン）…システム変更や組織改変に伴う最新化、分かりにくくないかを組織的に検証するとともに、システム面、業務面のコンティンジェンシープランの整合性確保が重要としている。

3）障害に備えた訓練・検証…バックアップセンターへの切替が必要なメインシステムの停止だけでなく、機器、オンライン処理、バッチ処理、対外接続システムにおける障害の発生など複数のシナリオを用意する点、対策本部の設置訓練、拠点駆け付け訓練、広

報対応訓練等を行うことで、障害の復旧手順書、バックアップ機器、各種手段の実効性を検証することが重要としている。

3.5.2.3. 障害管理に対する経営陣の関与

「障害管理に対する経営陣の関与」としては、以下 2 点が求められている。

1）障害管理に関するリスクの認識…稼働中システムのリスクプロファイルの変化の認識によるリスク評価や、訓練、障害管理体制の実効性検証を行う必要がある。その際、想定リスクシナリオ不十分、問題意識の低下傾向、システム要員の退職による管理ノウハウが散逸等のリスクを認識することが前提となる。

2）障害発生の防止に向けた指示…潜在リスクの認識評価のための管理の枠組みや障害発生の対応体制、委託先管理体制の改善の責任があり、他社の障害事例分析、システム部署と業務部署の連絡検討体制構築、システム要員のスキル低下を防止する人材育成のため、企画・開発・運用間のバランスを取った資源配分を指示することが必要となる。

3.5.3. 「稼働品質」向上の取組み[24]

情報処理推進機構は、「情報システム障害の再発防止のための組織マネジメントの調査WG報告書」及び「障害管理の取組みに関する調査　調査報告書」において、「障害管理」の取組みが進んでいる 8 社（金融 3 社、運輸 2 社、製造 3 社）の企業事例をもとに、「障害管理の取組み」と「障害が防止できなかった備え」「障害管理フレームワーク」に関して、事業者への提言を纏めている。 [独立行政法人情報処理推進機構技術本部ソフトウェア・エンジニアリング・センター, 2012a] [独立行政法人情報処理推進機構技術本部ソフトウェア・エンジニアリング・センター, 2012b]

「障害管理の取組み」として、「稼働品質」に対する目標設定がされ、その目標達成のための活動が行われている点が共通するとしており、以下 7 点を提言している。

1）情報システムで守られるべき価値の設定、

2）情報システムの重要度の指標化、

3）情報システムの品質目標の設定、

4）具体的な品質向上施策の実施、

①運用状況の把握と対処、

[24] 本項は、「金融情報システム障害の再発防止についての一考察」[遠藤正之, 2013]を元にしている。

②開発プロセスおよび運用プロセスの標準化、

③運用視点での開発のチェック、

④IT 基盤の標準化、

⑤障害の発生分析と再発防止策の立案と展開、

5）品質向上施策の策定と実施の管理体制、

6）品質向上施策についての人的な面での取り組み、

7）情報システムの障害などの記録である。

「障害が防止できなかった時の備え」としては、以下 3 点が重要としている。

1）非常時の情報システム関係者の招集体制の取り決め、

2）非常時の情報システムの利用者（事業部門、関係会社）の行動ルールの取り決め、

3）非常時を想定した訓練の実施。

「障害管理フレームワーク」については、表 22 の通り、以下 3 項目が重要であるとしている。

1）経営者のガバナンス、

①信頼性方針の策定、

②情報システム運用状況の監視、

③障害管理目標の達成判断、

2）管理者の障害管理のマネジメント、

①障害管理目標の設定、

②運用、

③障害対応、

④再発防止、

⑤障害記録の確認、

⑥障害の予防・プロセス改善、

3）障害管理体制の構築。

表 22「障害管理の取組みに関する調査」調査報告書

「障害管理の取組みに関する調査」調査報告書（2012）

フレームワーク項目		共通的取組み
ガバナンス	信頼性方針の策定	経営層が、事業として提供している価値を、情報システムにとって最も重要な価値と設定 「情報資産の保全」(A社) 「事業に必要なITサービス品質(機密性、完全性、可用性)維持」(B社) 「公正性が損なわれず、継続してサービス提供できる」(C社)
	情報システム運用状況の監視	経営層は事業への影響の観点から運用部門が計測した運用状況を把握(定常的な会議、障害発生時のエスカレーション)
	障害管理目標の達成判断	把握した運用状況や障害件数から、目標に照らして判断
マネジメント	障害管理目標の設定、運用、障害対応、再発防止、障害記録の確認、障害の予防・プロセス改善	
障害管理体制の構築		組織形態(全社一元型、事業部門独立型)に応じたガバナンスとマネジメント
障害管理活動の有効性を高める方策		「経営層コミットメントと障害管理施策へのリソース配分」(A社) 「障害発生時のコーディネータ人材の育成」(B社) 「設計運用での冗長的な仕組み、運用文書の標準化」(C社)

そして、経営者のガバナンス、管理者の障害管理のマネジメント、障害管理体制の構築の 3 項目の相互関係を表した障害管理フレームワークの全体像は、図 13 の通りである。

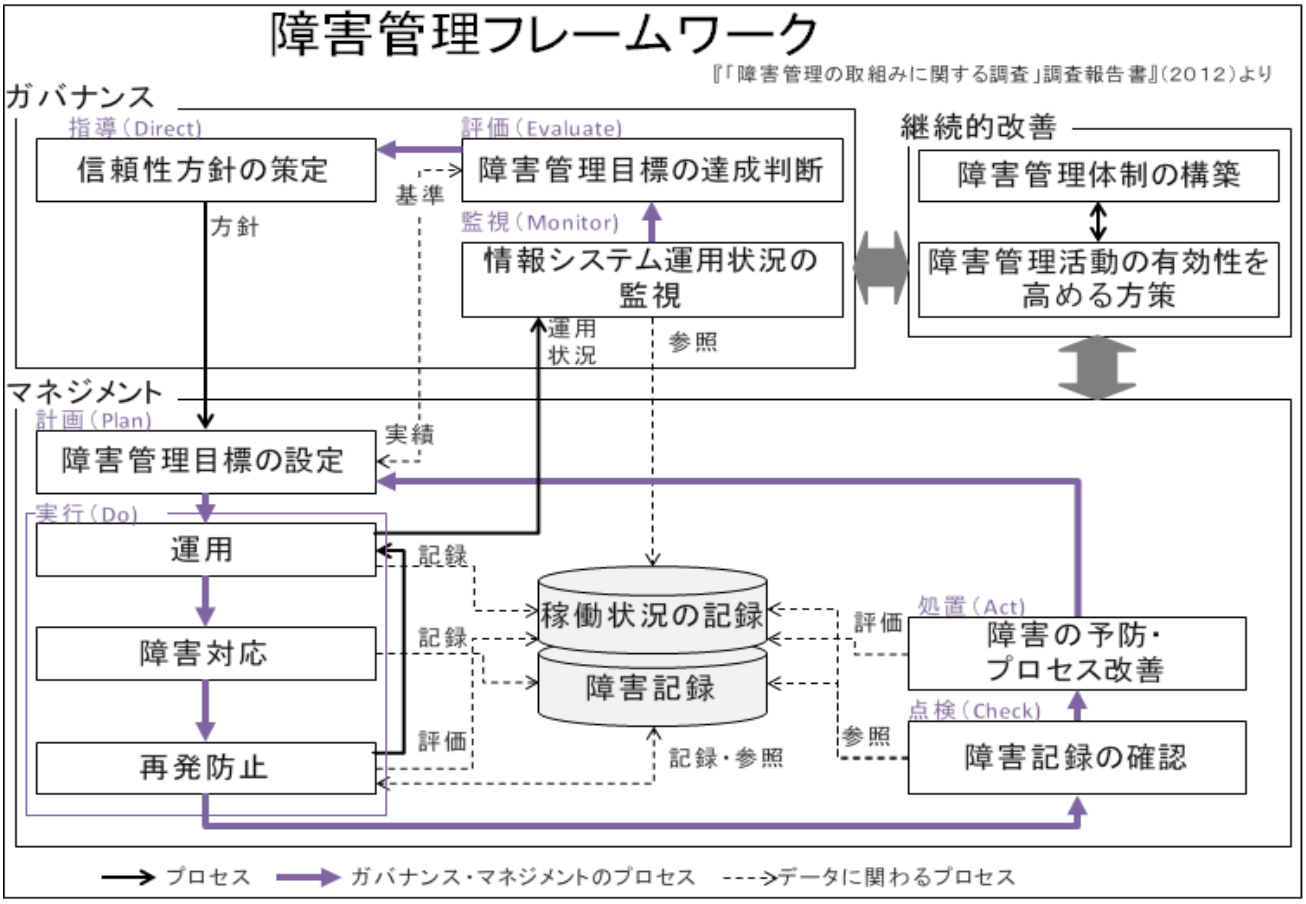


図 13 障害管理フレームワーク

3.5.4. 運用局面での CORE-OQ の適用

前節までの障害事例の分析や、障害対応策の文献での検討を踏まえ、リスクマネジメント戦略の 6 観点について、運用局面での適用が図れるかを確認する。

3.5.4.1. 経営トップのコメットメントと支援（Commitment）

観点 1 の経営トップのコミットメントと支援（Commitment） については、障害管理のリスク認識を経営トップが持ち、障害発生防止の指示を行うという未然防止面、障害発生時に組織内外への発信 を適確に行うという障害対応面で重要である。障害訓練にも参画し、実効性の確認に関与することも望まれる。

3.5.4.2. 組織体制と IT ガバナンス（Organization）

観点 2 の適切な組織体制整備による IT ガバナンス強化（「組織体制と IT ガバナンス」）（Organization） については、「守りの IT 投資」が成されており、障害発生時の全社的

組織体制や委託先との連絡体制の構築を指示し、障害に備えた訓練が定期的に実施されるなど、IT ガバナンスが高められていることが必要となる。

3.5.4.3. IT リスクマネジメント（IT Risk Management）

観点 3 の経営 IT リスクの適切な評価と対策の構築（「IT リスクマネジメント」）（IT Risk Management）については、稼働中システムのリスクや処理能力の定期的な見直しを指示し、開発中システムのリスク管理と共に、継続的にリスクの状況を管理し続けることが必要となる。

3.5.4.4. 拡張性一貫性確保（Extensibility）

観点 4 の経営戦略に合致した業務拡張性及びシステムの一貫性の確保による二重投資の排除（「拡張性一貫性確保」）（Extensibility）については、障害対応計画を考慮した設計がなされ、システムの二重投資がないように、金融情報システム全体のグランドデザイン上の位置付けが明確にされているが望まれる。

3.5.4.5. 要件定義最適化（Optimization）

観点 5 の外部関係者の要請と IT のケイパビリティの間をつなぐ要件定義最適化（非機能要件を含む）（「要件定義最適化」）（Optimization）については、経営及び業務部門から出た要件と、現状のシステムで構築可能な仕組みに加え、運用面や業務継続計画を考慮し、より焦点を絞ってコストパフォーマンスの高い効果的な情報システム開発を行っていくことが必要である。

3.5.4.6. 品質重視の仕組構築（Quality）

観点 6 の品質重視の仕組構築（Quality） については、設計品質や開発品質に加え、運用品質を向上するためのルールや手順の制定や、品質向上のための定期的な会議体や組織体の設置が行われている点が必要である。

3.5.4.7. CORE-OQ

ここまでの考察の通り、「リスクマネジメント戦略の 6 観点」(CORE-OQ)は、運用局面に拡張しても、有効な考え方であると言える。

運用局面でのリスクマネジメント戦略の 6 観点(CORE-OQ)をまとめると表 23 のようになる。

表 23 運用局面のリスクマネジメント戦略の 6 観点「CORE-OQ」

運用局面のリスクマネジメント戦略の6観点（CORE-OQ）

1．経営トップのコミットメントと支援（Commitment）	障害対策への関与、障害時の組織内外への発信
2．適切な組織体制整備によるITガバナンス強化（「組織体制とITガバナンス」）（Organization）	障害時の全社的組織体制、委託先との連絡体制の構築、障害訓練の定期的に実施
3．ITリスクの適切な評価と対策の構築（「ITリスクマネジメント」）（IT Risk Management）	リスクや処理能力の定期的な見直しによる継続的なリスク状況の管理
4．経営戦略に合致した業務拡張性及びシステムの一貫性確保による二重投資の排除（「拡張性一貫性の確保」）（Extensibility）	障害対応を考慮した設計が、金融情報システムのグランドデザイン上でも明確になっている
5．ステークホルダーの要請とITのケイパビリティの間をつなぐ要件定義最適化（「要件定義最適化」）（Optimization）	運用面や業務継続計画を考慮した上で、コストパフォーマンスの高い効果的な情報システム開発がされている
6．品質重視の仕組構築（Quality）	運用品質に関わるルール・手順の制定や会議体・組織の設置

遠藤正之（2013）「金融情報システム障害の再発防止についての一考察」発表資料を元に作成

3.5.5. リスクマネジメント戦略の構築（第 3 章のまとめ）

第 3 章では、経営レベルで金融情報システムのリスクマネジメントを行うに当たり、IT 投資の観点、システム監査関連基準の観点、金融情報システムの最近の成功事例の成功要因を集約する形で、リスクマネジメント戦略の 6 観点(CORE-OQ)を構築した。その上で、情報システム開発に関与する金融機関従業員の問題意識調査によって、開発局面において、リスクマネジメント戦略の 6 観点が適切であることを確認した。更に運用局面においての妥当性も、最近公開された障害防止対応に関する文献で確認できた。続く第 4 章では、金融情報システムの具体的事例を元に、リスクマネジメント戦略の 6 観点をいかに実践すべきかについて考察する。

第4章 経営戦略の実現に向けたリスクマネジメントの実践

第 3 章では、経営者が着目すべき項目としてリスクマネジメント戦略の 6 観点(CORE-OQ)を提示したが、その前提にあるのは、経営者が経営戦略の重要な要素として、金融情報システムをマネジメントする必要があるという視点であった。第 4 章では視点を逆転させ、金融情報システムのリスクマネジメント実施が、金融機関の経営戦略実現に対して、どのような貢献ができるかについて、実例を中心に検討を進める。まず、経営戦略、IT 戦略、金融情報システムの関係について、モデルを提示した上で、東京証券取引所の株式売買システム「arrowhead」構築プロジェクトとオンライン証券 5 社の取組み事例で考察する。

4.1. 経営戦略、IT 戦略、金融情報システムの関係[25]

本節では、「経営戦略」、「IT 戦略」、「金融情報システム」の関係に着目する。その際、3.1.1 項で検討した「IT 経営ロードマップ」での「経営」、「IT」、「現場」の三者の関係を参考にし（図 14）、「現場」を「金融情報システム」に置き換えてモデル化を図る。

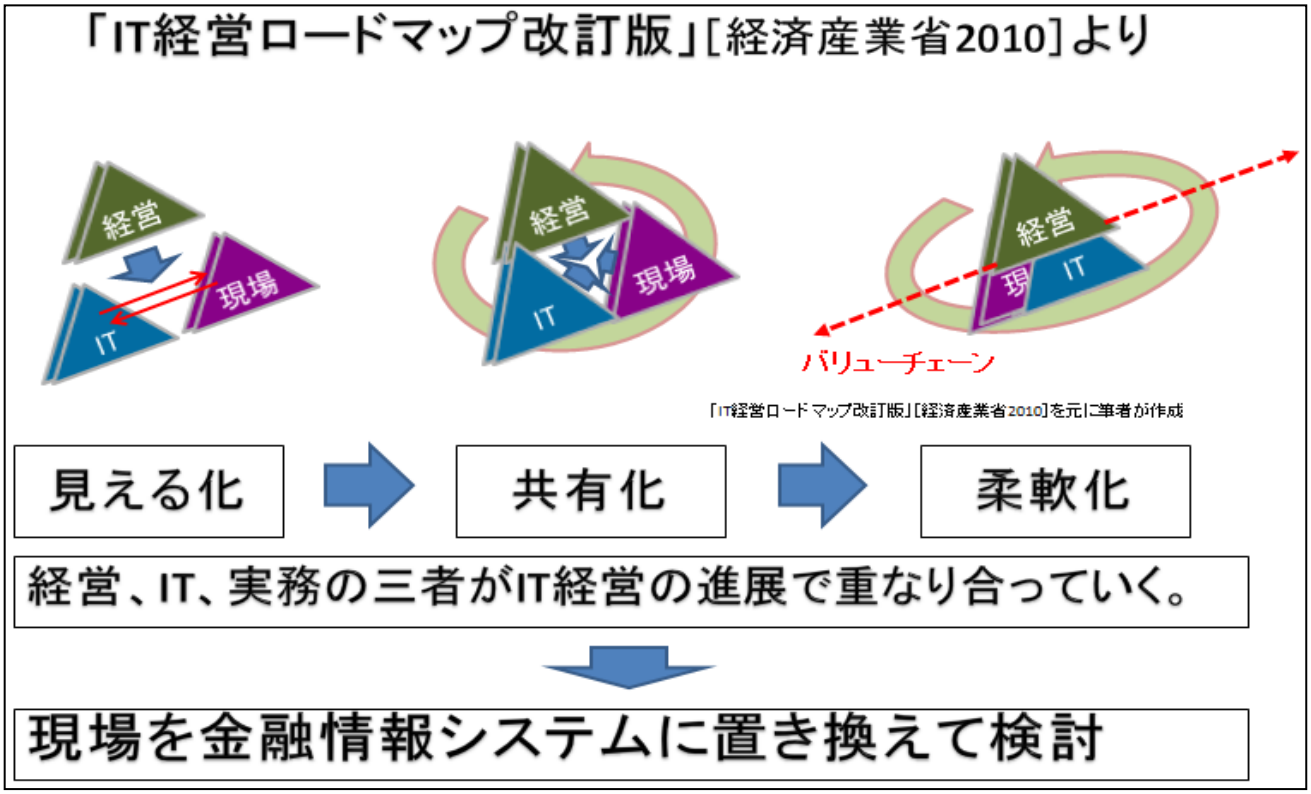


図 14「IT 経営ロードマップ」での「経営」「IT」「現場」三者の関係［経済産業省, 2010］

[25]本節は、主として「金融業の経営戦略実現に向けた情報システム貢献の考察」[遠藤正之、高野研一, 2014a]「地域金融機関における情報システム共同化に関する考察」[遠藤正之、高野研一, 2014b]を元にしている。

さて、「経営戦略」、「IT 戦略」、「金融情報システム」の三者の関係は、金融事業者によって、様々な形態をとると思われるが、考察を容易にするため、以下の三つのモデルに集約して作成した。

1）経営戦略包含型

2）IT 戦略確立型

3）金融情報システム貢献型。

これらはあくまで一般化したモデルであり、実際には、中間的な形態や異なる形態があることは言うまでもない。

4.1.1. 経営戦略包含型

第一のモデルは、「経営戦略」の中に「IT 戦略」が包含されるモデルである。金融情報システム導入の初期段階や、情報システム以外の経営戦略が主導となっている状況を想定している。

そのような状況では、IT 戦略は意識されていないことが多く、処理の正確性や情報の保存性を高めること等、事務合理化やデータ蓄積を主目的とした生産性向上、業務改善の手段として、金融情報システムが用いられる。IT 戦略は明確には存在していないが、金融情報システムの重要性は経営者にも認識されており、経営戦略から見ると、安定的な稼働が最優先の使命となる。このタイプを「経営戦略包含型」と命名した（図 15）。後述する事例では、4.2 節の東京証券取引所の 2005 年頃や、4.3 節のオンライン証券のうち、SBI 証券や楽天証券の状況が、ほぼ該当すると考える。

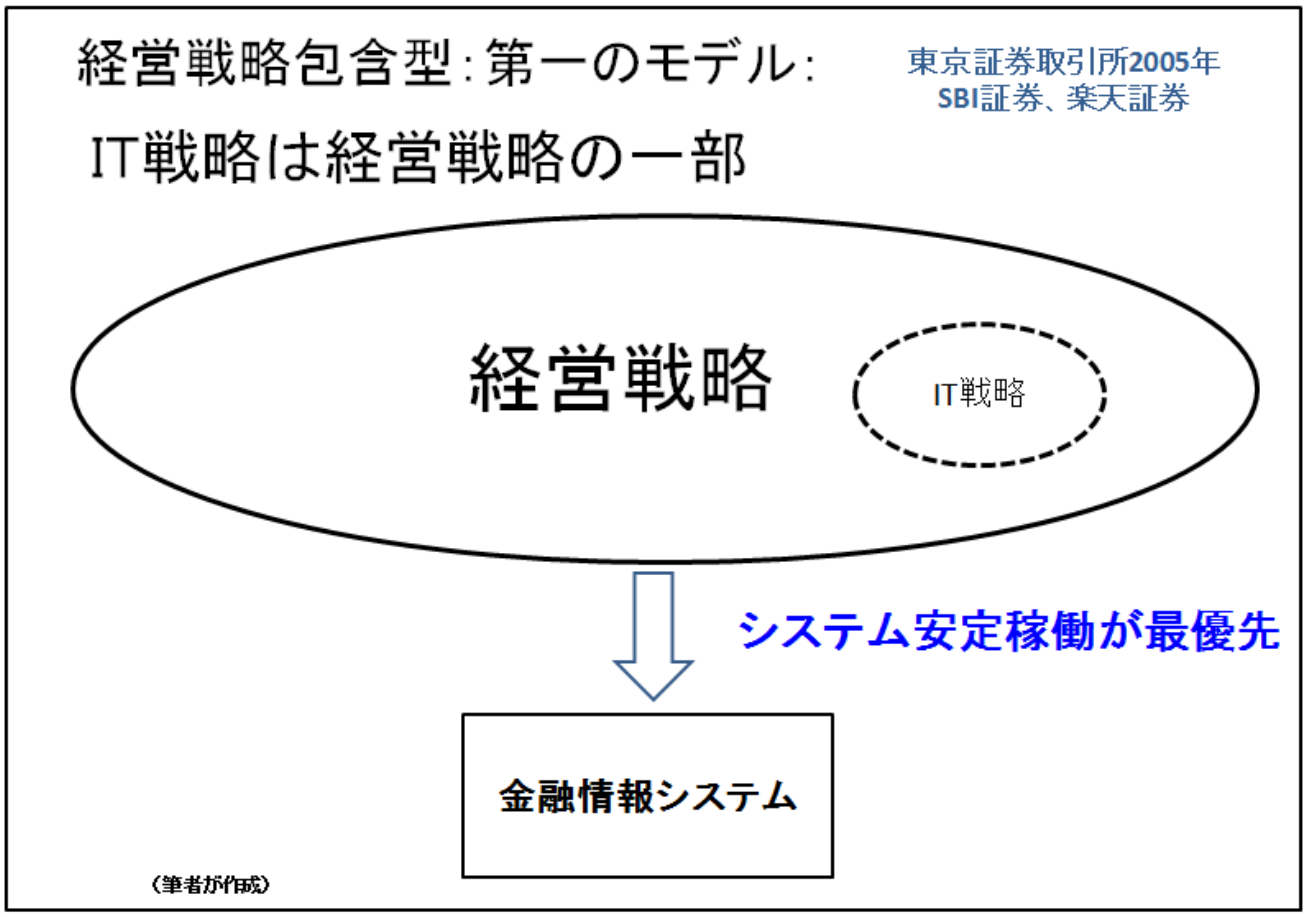


図 15 経営戦略包含型

4.1.2. IT 戦略確立型

第二のモデルは、IT 戦略が経営戦略の中から独立し、金融情報システムをどのような観点で構築保守するかについても組織体での合意がなされているタイプである。このタイプを「IT 戦略確立型」と命名した（図 16）。本節冒頭で言及した「IT 経営ロードマップ改訂版」で、「見える化」ないし、「共有化」が行われている状況である。

このタイプの「経営戦略包含型」との最大の相違点は、経営戦略とは別に、IT 戦略が策定される点であるが、「経営戦略」、「IT 戦略」、「金融情報システム」の関係は図 16 の通り、一方向の関係である。

1）「経営戦略」と「IT 戦略」の関係については、経営戦略に沿って、IT 戦略が構築されている。IIT 戦略は個別に策定されるが、あくまで経営戦略に沿った全体最適を意識したものが求められる。

2）「経営戦略」と「金融情報システム」の関係については、経営戦略から金融情報システムに対して、第一のモデルと同様の安定稼働の要求に加え、競争優位につながる機能や

性能の差別化が求められる。経営者にとって、金融情報システムが差別化の源泉となることが意識されている状況である。

3）「IT 戦略」と「金融情報システム」の関係については、IT 戦略が策定されることにより、将来の金融情報システムの姿を見据えた形での優先順位付や資源配分が成され、金融情報システム全体のグランドデザインが構築され、そのグランドデザインに基づいて個々の金融情報システムが設計構築されることになる。

後述する事例では、4.2 節での東京証券取引所の 2008 年頃や、4.3 節でのオンライン証券のうち、松井証券やマネックス証券の状況が、このモデルにほぼ該当すると考える。

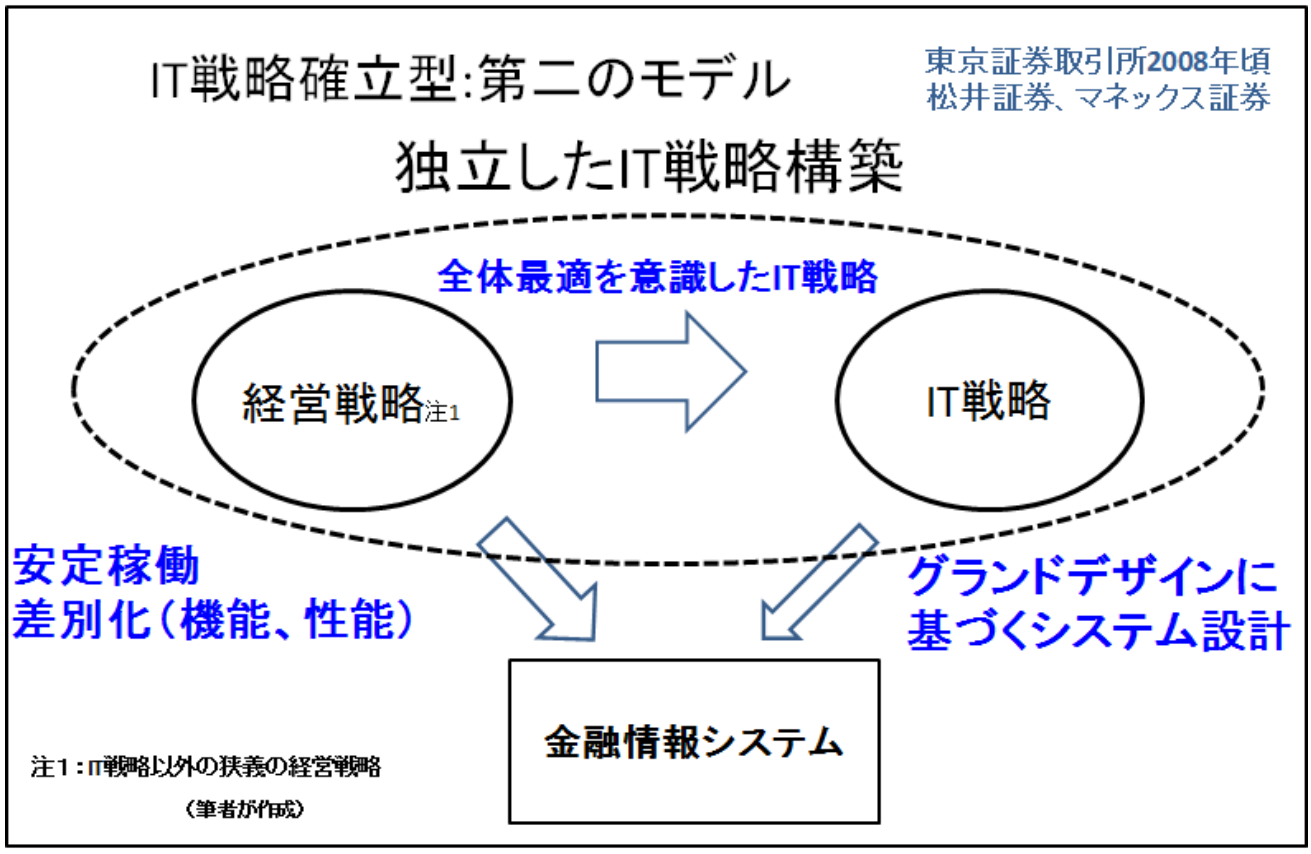


図 16 IT 戦略確立型

4.1.3. 情報システム貢献型

第三のモデルは、第二のモデルをさらに発展させ、金融情報システムや金融情報システムに関わる無形資産（インタンジブルズ）が、経営戦略や IT 戦略の選択肢を広げるようになっているステータスのモデルであり、「金融情報システム貢献型」と命名する。本節冒頭で言及した「IT 経営ロードマップ改訂版」では、「見える化」、「共有化」が進み、「柔軟化」まで到達している状況である。

ここでの、無形資産（インタンジブルズ）とは、バランスシートには計上されないが、金融情報システムを構築する人材や組織、更に情報システムそのものや、データの蓄積等を含むものである（図 17）。

このタイプと「IT 戦略確立型」との最大の相違点は、図 17 の通り、「金融情報システム」から「IT 戦略」、「経営戦略」、「IT 戦略」から「経営戦略」への作用が発生している点である。すなわち、「経営戦略」、「IT 戦略」、「金融情報システム」の関係が双方向の相互作用の関係となっている。

1）「経営戦略」と「IT 戦略」の関係については、経営戦略に沿って、IT 戦略が構築される点は、第二のモデル「IT 戦略確立型」と変わらないが、それだけでなく IT 戦略が環境変化への対応力を経営戦略に与えることができる状態となっている。IT 技術の発展を利用して、変化に対応する経営戦略が策定できる状態とも言える。

2）「経営戦略」と「金融情報システム」の関係については、経営戦略から金融情報システムに対して、第二のモデル「IT 戦略確立型」と同様、安定稼働の要求と競争優位につながる機能や性能の差別化が求められることは変わらないが、金融情報システムを利用した新規ビジネスの策定が可能となるなど、金融情報システムが戦略の源泉となりうる点が大きく異なる点である。

3）「IT 戦略」と「金融情報システム」の関係については、グランドデザインが構築され、その下で個々の金融情報システムが設計構築される点は、第二のモデル「IT 戦略確立型」と同様であるが、更に、金融情報システムを構築する中で、IT に精通した人材や、情報やデータの蓄積が成されることで、最新技術を用いた IT 戦略が可能となる点で異なっている。

後述する事例では、4.2 節での東京証券取引所の 2010 年以降の状況や、4.3 節でのオンライン証券のうち、カブドットコム証券の現在の状況が、このモデルにほぼ該当すると考える。

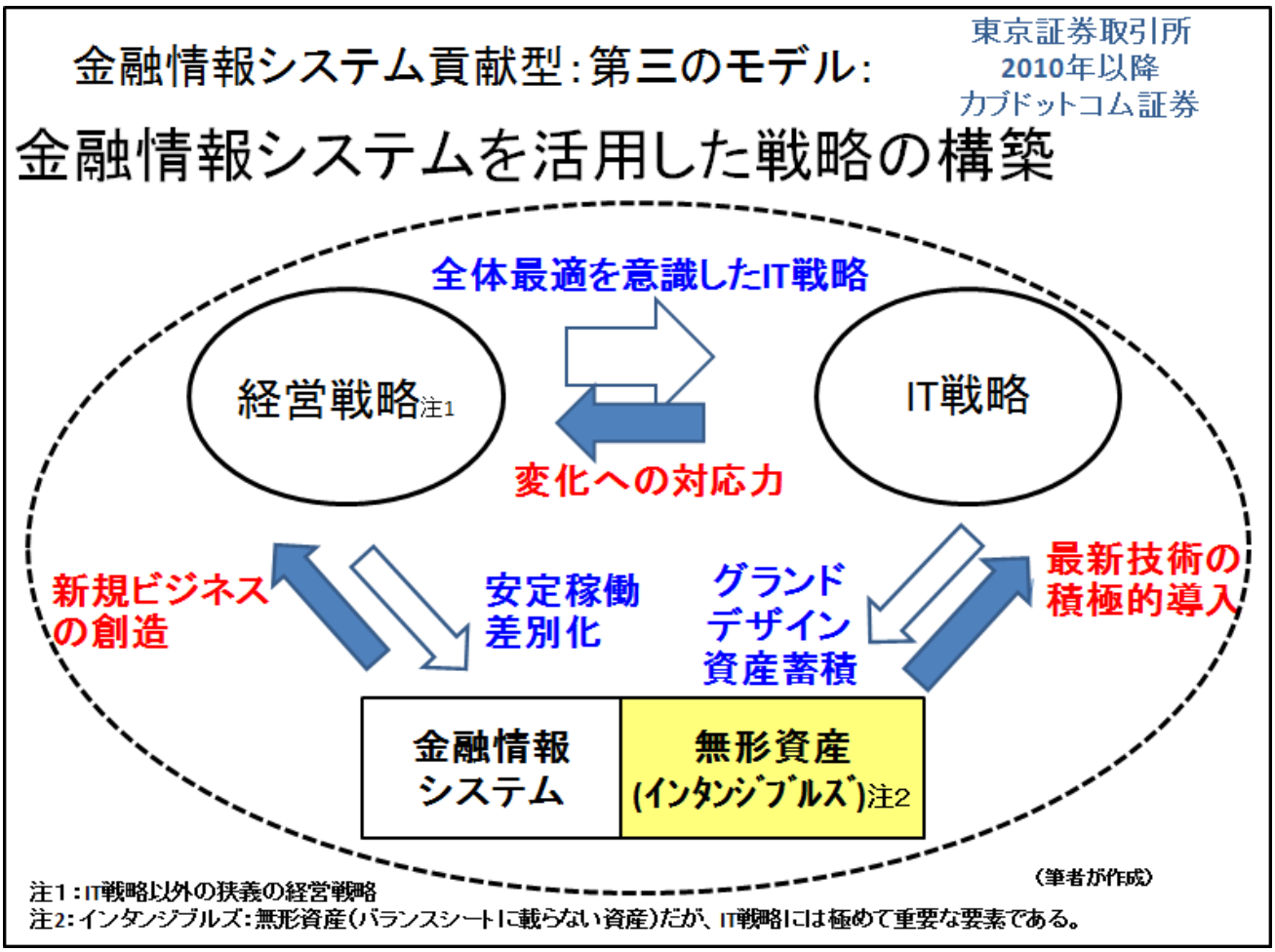


図 17 金融情報システム貢献型

以上の 3 類型を念頭に、次節からは、具体的な事例で、「金融情報システム」が「経営戦略」や「IT 戦略」へどのような作用を及ぼしているかについて、検討する。

4.2. 取組み事例（東京証券取引所の事例）[26]

本節では、東京証券取引所（Tokyo Stock Exchange　以下東証と略す）の株式売買システム「arrowhead」構築開発（2010 年 1 月リリース）の事例を採り上げる。東証の「arrowhead」構築開発は、最近の金融情報システム開発の代表的な成功事例であり、その開発プロジェクトの進展は、「経営戦略」と「IT 戦略」そして、「金融情報システム」の関係を大きく変化させるものであった。またリスクマネジメントやプロジェクトマネジメントの手法や工夫は、他の範となる好事例でもある。この事例を利用して金融情報システムが経営戦略実現に貢献

[26] 本節は、[鈴木義伯, 2010] [大和田尚孝, 2010b]、[遠藤正之, 2011]及び [Masayuki Endo,Kenichi Takano, 2013]及び 2011 年 2 月 1 日の東京証券取引所鈴木 CIO ヒアリングを元にしている。

するに至った道筋を説明するとともに、リスクマネジメント戦略の 6 観点(CORE-OQ)の適合状況について、考察する。

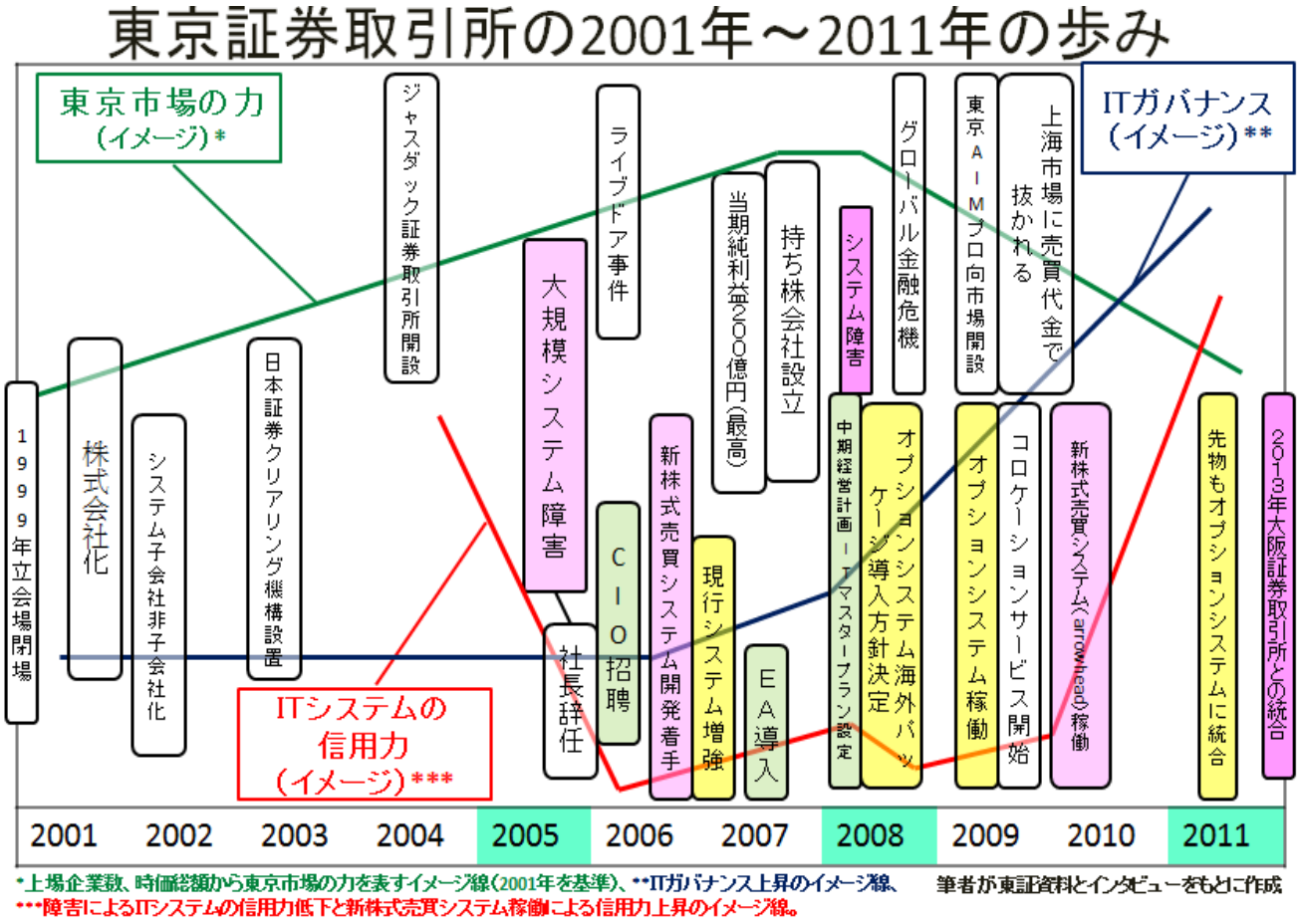


図 18 東京証券取引所の 2001 年～2011 年の歩み［Masayuki Endo, Kenichi Takano, 2013］

4.2.1. 開発経緯

4.2.1.1. 開発の概要と背景

東証の株式売買システムの開発は、2006 年前半から要件定義に着手し、2010 年 1 月にリリースする 4 年がかりのものであった。開発費用は 130 億円、開発ステップ数は 340 万ステップである。

図 18 は、東京証券取引所の 2001 年の東京証券取引所株式会社化から、2010 年の新株式売買システム「arrowhead」稼働、2011 年の先物システムのオプションシステムへの統合までの歩みの概要を時系列で表したものである。ここで着目すべきは、東京市場の力と IT システムの信用力そして、IT ガバナンスの関係である。

東京株式市場は、2005 年頃の市場活性化に伴うデータ量増加により、当時の証券取引所の株式売買システムの性能の限界に近付いたことから、2005 年の大規模システム障害につな

がり、東証の IT システムの信用力の低下を招き、その後 IT ガバナンスの立て直しを図ることが喫緊の課題となった。

一方、その後、東京市場の上場企業数は 2008 年の 2415 社をピークに、2011 年には 2290 社にまで減少し、東証上場企業の時価総額も 2006 年の 563 兆円をピークに 2011 年 1 月には 315 兆円まで減少するなど、東京市場の力は低下していく。このような外部環境下で、東証の株式売買手数料や、上場に関わる手数料による収益力も低下する。そのような中で、2010 年の「arrowhead」稼働は、IT システムの信用力向上の実現となって、新たなビジネスチャンスを生み出した。海外の取引所との取引所間競争が激化する中で、新たな競争優位の源泉となり、2013 年には、大阪証券取引所との統合を果たすという経営戦略の実現につながったのである。

この歩みの中で、一旦低下した IT システムの信用力向上には、IT ガバナンスの立て直しから 3 年の年月が必要であった点にも着目すべきである。これは、優れた IT 戦略であっても、その効果の実現には、相応の年月がかかることを示唆している。

さて、「arrowhead」開発開始時点に戻ると、開発の背景としては以下二点があった。

第一は国際的な取引所間競争の激化である。海外投資家の台頭、アルゴリズム取引の活発化による処理速度へのニーズの高まり、取引所間の M&A の動きの活発化、私設取引所との競争環境といった動きの中で、競争優位を確保することを狙ったものである。

第二の背景として、システムの信認の回復がある。2005 年から 2006 年初に東証は、3 回にわたる大規模なシステム障害や停止が発生しており、市場や金融当局から厳しい目で見られており、抜本的なシステム構築を図る必要があった。以上の二点から、失敗の許されない経営のトップ・プライオリティ・プロジェクトとして、経営トップが推進するプロジェクトとなったのである。

4.2.1.2. CIO 招聘と組織変更・意識改革

東京証券取引所生え抜きの社長が、2005 年 12 月のシステム障害の責任を取って引責辞任した後、東芝出身の西室氏が社長に就任したが、社長就任後すぐに、社外で CIO 適任者を探し、2006 年 2 月に NTT データから CIO となる鈴木氏を招聘した。更に証券界からの協力を得る必要もあり、野村証券出身の斉藤社長も招聘し、自らは会長に就任することで経営陣の強化を図った。CIO に関しては、内部要員で適切な人材がいなかったため、外部に求めざるを得なかった面があるが、金

融庁ともコミュニケーションを取ることにより、日本で最も大手のベンダーである NTT データから優秀な人材を招聘することができたことは、大きな転換点であった。

CIO に就任した鈴木氏は、証券業務や取引所業務に関しては精通していなかったが、就任直後に欧州視察を行い、取引所システムの最重要価値がスピードであることを再認識したと言う。［大和田尚孝, 2010b］。その後、鈴木 CIO が主導して、2006 年 4 月には開発プロジェクトの実施に向け、従来の業務別縦割りだったシステム担当をシステム本部に集結する組織変更を行った。また合わせて、システムの品質を確保する組織として、品質管理部を新設した。これらは、全社統一的に全体最適な開発体制を構築し、業務別の知識やノウハウの共有を進め、従来不足していた IT ガバナンスの強化を図るものであった。

体制強化と並行して、鈴木 CIO は発注者としての意識改革を進め、東証と開発ベンダーの役割分担を明確化し、要件定義と受入テストの実施は発注者の責任であるとした。しかしながら、実際には、発注する東証には要員が揃っていなかった。そこで、スキル要員を外部から補強する策を取った。また、鈴木 CIO は、システム開発の理想を追求し、それまで横行していた過去に遡及する発注契約[27]を一切禁止する改革を行った。これは、発注者が受注者に甘えることなく、責任を持って、発注の役割を果たすということの一つの現れであり、東京証券取引所のプロジェクトメンバーの発注に対する責任意識を高める狙いがあった。同時に、発注者側が段取り良く発注をすることで、受注ベンダーのモチベーションを高めることも狙っていた。更に開発運用の標準プロセスの整備を行った。開発については、工程の節目に工程会議や品質評価会議等の会議を設定し、工程ごとの進捗と品質の管理を、東証自身が行うこととした。また運用については、運用の標準であるITIL[28]を適用して整備を図った。

4.2.1.3. システムの計画とベンダー選定、EA 導入

2006 年の 4 月から新株式売買システムの検討を開始し、2006 年夏からは、要件定義に着手した。その際、顧客である証券会社等のニーズをヒアリングし、基本コンセプトをまとめ、その後の設計やベンダー選定の軸を作った。

基本コンセプトは4項目からなる。

1）高速性すなわち注文受付通知のレスポンスを 10 ミリ秒以下とする点（従来は 2～3 秒のレスポンス）、

[27] 正式に契約を締結する前にベンダーに作業を開始してもらたり製品を納入してもらうこと

[28] Information Technology Infrastructure Library

2)拡張性すなわち拡張基準を超えたとき、1週間程度での処理能力増強を可能とする点(従来は、3～6 ヶ月を要した)、
3)柔軟性すなわち多様な商品や取引ルールの追加、変更に短期間で対応可能とする点、
4)可用性すなわち 99.999%以上の稼働を確保(5 年で 10 分程度の停止時間)という点である。
可用性、拡張性、高速化を実現するため、一方で、システムの全体構成、設計を極力シンプル化し、過剰な機能を削ぎ落とす方針も初期段階で決めていた。

2006 年 6 月からはベンダー選定のための RFP(Request for proposal:提案依頼書)作成作業に取り掛かり、約 1500 頁にわたる詳細なものであったが、東証の責任で作成した。2006 年 8 月からは RFP を更に詳細化した要件定義書の策定に取り掛かった。新株式売買システムの要件定義にあたっては、鈴木 CIO は、大規模なシステム開発のマネジメントやベンダーとの折衝力強化のノウハウを持ち込む一方、社内メンバーには、上流工程で発注者である東証が責任を持って性能マネジメント計画書や仕様書を作成することを求め、発注者責任の徹底を図った。実際の作成作業の一部はベンダーの協力を得たが、責任は東証が持つことを明確化した。また要件定義書の変更時は、CIO の承認を得るルールとして、容易に変更できないということを徹底した。特に、非機能要件について漏れなくかつ実現性ある形で定義することには意を用いた。非機能要件の中でも性能要件がビジネスの競争力を高めるためには必須であり、机上で要件を確認する作業を行った。要件定義には、2006 年秋から 2007 年 1 月までの期間をかけて行った。

並行して、ベンダーの選定も行い、3 段階の審査のうえ、2006 年末に富士通を選定した。世界最速の処理レスポンスの可能性があるものの、開発中の技術を提示してきた富士通の提案を採用することは、未知の技術のユーザーになることであり、リスクもあったが、採用を決定できたのは、競争力強化のために高速性が必須であるという経営戦略に基づいた基本コンセプトが明確であったことが、一つの要因である。

株式売買システム以外の主要システムについても、システムのシンプル化のため更新計画をロードマップとして立てていった。2006 年後半～2007 年初頭にかけて、鈴木 CIO が主導で、業務部門の役員全員に対しビジネスの戦略やシステムに求めるものが何であるかをヒアリングし、その結果を踏まえて EA(Enterprise Architecture)(P.40 脚注 20 参照)の手法で将来にわたるシステムの一貫性と全体最適を図った。2007 年には、EA を本格的に IT

マスタープランへ盛込み、IT 戦略として明確化した。また開発と運用の役割分担を明確にするため、運用を行う IT サービス部と開発を行う IT 開発部に分離を行った。

4.2.2. 開発の特徴・工夫

4.2.2.1. 上流工程完璧主義とフィードバック型 V 字モデル開発

新株式売買システムの開発の特徴として上流工程完璧主義と開発工程のフィードバック型V字モデルと言われる方法がある。従来の金融情報システム開発では、上流工程である要件定義や基本設計の間違いは、終盤の運用テストや、システムテストでの発見で已むなしとしており、相応の手戻りが発生する可能性があった(V 字モデル開発)。

東証の「arrowhead」構築では、従来テストフェーズで作成していたテスト項目を、設計と並行して作成することで、設計書の検証を早期に行う手法で、品質向上を図った(W字モデル開発)。 更に前工程の要件定義や設計を次工程で確認レビューすることを意識的に行わせ、不具合を早期発見する開発モデル(フィードバック型V字モデル開発)を構築し、ベンダーにも徹底させた［鈴木義伯, 2010］。

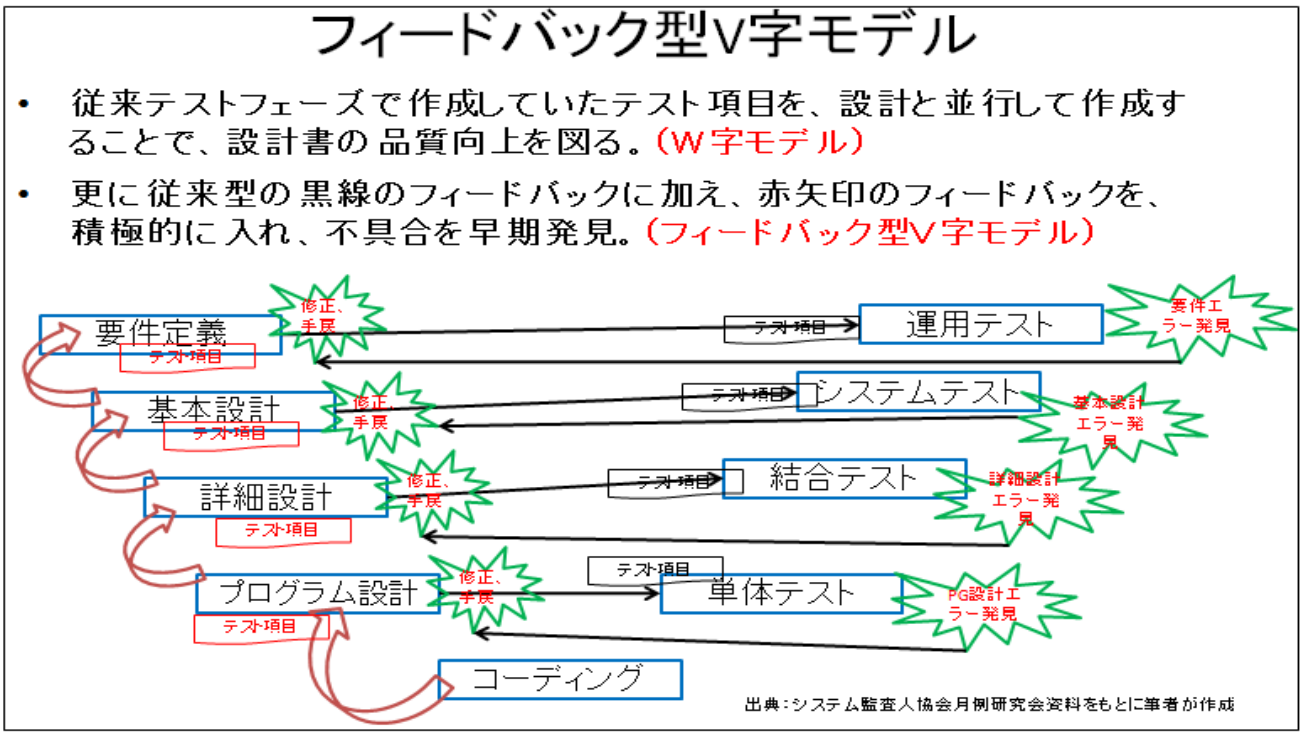


図 19 フィードバック型 V 字モデル

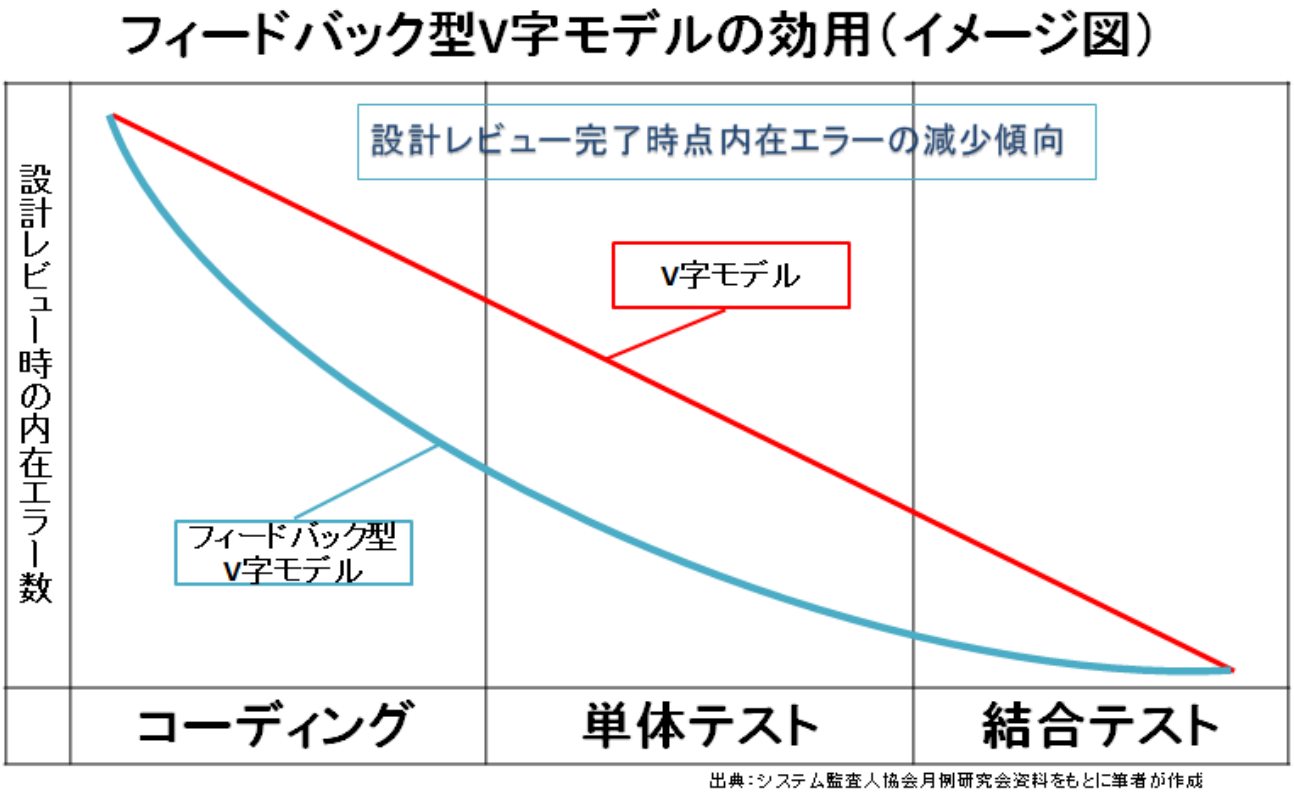


図 20 フィードバック型 V 字モデルの効用

実際に、外部接続サブシステムを除く6サブシステムで、要件定義に関わるトラブル発生のうち、多くの部分を、詳細設計段階で摘出できている。ただし、この手法はシステム開発の上流工程の要件定義や外部設計の品質が高く、その後の変更が発生しないことが前提であり、発注者の責任を明確にして基本方針に基づいて詳細な要件定義や外部設計を行ったことと表裏一体であった。

4.2.2.2. 開発テスト段階での品質管理の徹底

開発テスト段階での品質管理については、ベンダーとの連携を意識し、品質管理をベンダーを巻き込んで徹底できる仕組みの構築を図った。組織や会議体もそのために構築した。

第一に品質管理の組織を発注者側、ベンダーの双方に複数設置することで、品質強化を図った。具体的には、発注者である東証には、プロジェクト外組織である品質管理部に加え、プロジェクトチーム内組織として、品質管理グループを設けダブルチェックを行う形とした。

その際、プロパー要員では十分なスキル要員が確保できなかったため、これら組織には、開発ベンダー（富士通）以外のベンダー出身の有識者を採用する等の施策を行い、チェックの水準を高めた。一方ベンダーである富士通にもプロジェクト内の品質管理グループと、プロジェクト外の第三者部門のダブルチェック体制を要請し、実現させた。

第二に、「arrowhead」構築プロジェクトの要件の中で、競争優位のために最重要であったレスポンス性能の設計については、ベンダー任せにせず、外部の有識者を活用して、工程毎に発注者である東証が自ら実装工程まで評価を行った。

第三に、2008 年 3 月からベンダー富士通でのプログラム製造工程となり、2008 年 9 月からは、結合テストが始まった。この段階で通常であればベンダー側に任せた開発になるところ、ベンダーからの進捗報告に関し、発注者側で確認し、基準を満たさない場合は、次の工程に入れさせないという運用を厳格に行い、ベンダーにまでリスクマネジメント意識を徹底した。開発におけるリスクに関し、発生確率と影響度を掛け合わせてすべてのリスクを数値化して評価し、工程会議で一元管理することも行った。

その結果、結合テストは、当初計画では 2008 年 12 月終了であったが、8 つのサブシステムのうち、3 サブシステムが 2009 年 3 月に完了、4 サブシステムは 5 月に終了、1 サブシステムは 2009 年 8 月にようやく完了することとなった。しかしながら、この段階で品質に徹底的にこだわった結果、最終的な 2010 年 1 月のリリースについては、問題なく実現することができた。特に最重要としたレスポンス性能についても、注文応答 2 ミリ秒、情報配信 3 ミリ秒を実現し、当時のニューヨーク証券取引所の 5 ミリ秒、ロンドン証券取引所の 4 ミリ秒を上回ることができた。

4.2.3. IT ガバナンスの進化

前項の開発経緯から、東京証券取引所は、2005 年から 2010 年にかけて、「経営戦略包含型」、「IT 戦略確立型」、「金融情報システム貢献型」へと推移したと考える。

4.2.3.1. 経営戦略包含型の時期

2005 年当時は、大きなシステム障害が発生するなど、システムの安定稼働が大命題であり、それこそが経営戦略であった。IT 戦略は、経営戦略に包含されていたと言える。

4.2.3.2. IT 戦略確立型の時期

EA（Enterprise Architecture）の手法で将来にわたるシステムの一貫性と全体最適を図った。2007 年には、EA を本格的に IT マスタープランへ盛込み、IT 戦略として明確化した。これは、IT 戦略が社内外に明文化されたものであり、この時期に東証は、「IT 戦略確立型」に進化したと言える。

4.2.3.3. 金融情報システム貢献型へ

2010 年 1 月の株式売買システム「arrowhead」の稼働は、当時の世界最速レベルの取引レスポンスを実現するものであり、東京証券取引所の IT システムの信用力は一気に高まった。またこのシステムを生かすために、コンピュータセンターの一角に顧客となる証券会社のサーバを設置するスペースを貸し出すコロケーションサービスと言う新しいビジネスモデルを構築することもできた。更にシステム部門の人材も強化され、大阪証券取引所との統合により日本取引所グループが形成された点も、金融情報システムの成果と言える。この時期、「金融情報システム貢献型」に進化したと言える。

4.2.4. リスクマネジメント戦略の 6 観点(CORE-OQ)での分析

リスクマネジメント戦略の 6 観点(CORE-OQ)を、東証の「arrowhead」構築プロジェクトでの適合性を確認したのが、表 24 である。6 観点が高いレベルで実現され、開発が進んできたことが見て取ることができる。このことからも、リスクマネジメント戦略の 6 観点(CORE-OQ)が有効であることが示唆される。

表 24「arrowhead」構築プロジェクトでのリスクマネジメント戦略の 6 観点

リスクマネジメント戦略の 6 観点	「arrowhead」構築プロジェクトでの状況
経営トップのｺﾐｯﾄﾒﾝﾄと支援	CIO をヘッドハントして選任し、経営トップが支援
組織体制と IT ガバナンス	組織体制整備と意識改革の両面でのガバナンス構築
IT リスクマネジメント	信頼性に加え、高速取引へ対応するレスポンス面を重視。リスク全般の定量化と管理の実施
拡張性一貫性確保	更新計画のロードマップを策定し、EA 手法を採用
要件定義最適化	発注者責任の徹底、レスポンス面の重視に伴う機能簡素化した要件定義に注力
品質重視の仕組み構築	早期不具合発見のための手法開発、品質管理組織の充実、ベンダーを巻き込んだ性能面の開発時点での品質向上

4.3. 経営戦略に貢献する金融情報システム（オンライン証券の事例）[29]

前節での東京証券取引所の分析に続き、本節では、オンライン証券大手 5 社（SBI 証券、マネックス証券、楽天証券、松井証券、カブドットコム証券）に対してモデルの適用を図る。

[29] 本節は「金融業の経営戦略実現に向けた情報システム貢献の考察」[遠藤正之、高野研一, 2014a]を元にしている。

4.3.1. オンライン証券業界の概要

オンライン証券業は、1999 年の小口株式売買委託手数料の自由化を機に一斉に市場参入が相次いだ比較的新しい業態である。当初は、60 社以上が参入したが、競争による淘汰が進み、現在は、大手 5 社のシェアが 7 割を超えるような集約度となっている。

この業態を金融情報システムの検討対象に選択した理由は、以下 2 点である。

第 1 に金融情報システムが業務に直結しており、その優劣によって業績に変化が生じる可能性が高い業態と考えられる点である。

第 2 に、その一方で手数料引下げや新サービス導入の競争の中で、投入できる経営資源が限られる業態と考えられるためである。

さて、2013 年 3 月期の 5 社の概要は、図 21 の通りである。営業収益[30]首位は SBI 証券、やや差があって 2 位楽天証券、3 位松井証券、4 位マネックス証券が続き、5 番目にカブドットコム証券が入っている。営業の規模を表す口座数も同様の順位であり、インターネットを利用する個人の取引が中心で、口座数が営業収益につながる業態であることを示唆している。

オンライン証券各社の概要（2014年3月期）　（筆者が作成）

単位：10億円	SBI証券	楽天証券	松井証券	マネックス証券	カブドットコム証券
営業収益	74	46	40	36	23
営業利益	33	22	27	14	12
経常利益	33	22	27	14	12
当期純利益	18	13	16	8	7
口座数（万口座）	294	167	94	89	87
株式委託個人売買シェア	35.3%	15.2%	11.0%	6.5%	7.7%
短評・特色	営業収益首位、口座数トップ、金融サービス事業の中核としての位置付け。SBIマネープラザで窓口営業実施	営業収益2位。2003年から楽天グループへ。グループ全体で幅広い金融事業を展開。	営業収益3位。オンライン証券専業。	米TradeStation社を買収。	大手の一角。
IT戦略タイプ	経営戦略包含	経営戦略包含	IT戦略確立	IT戦略確立	金融情報システム貢献

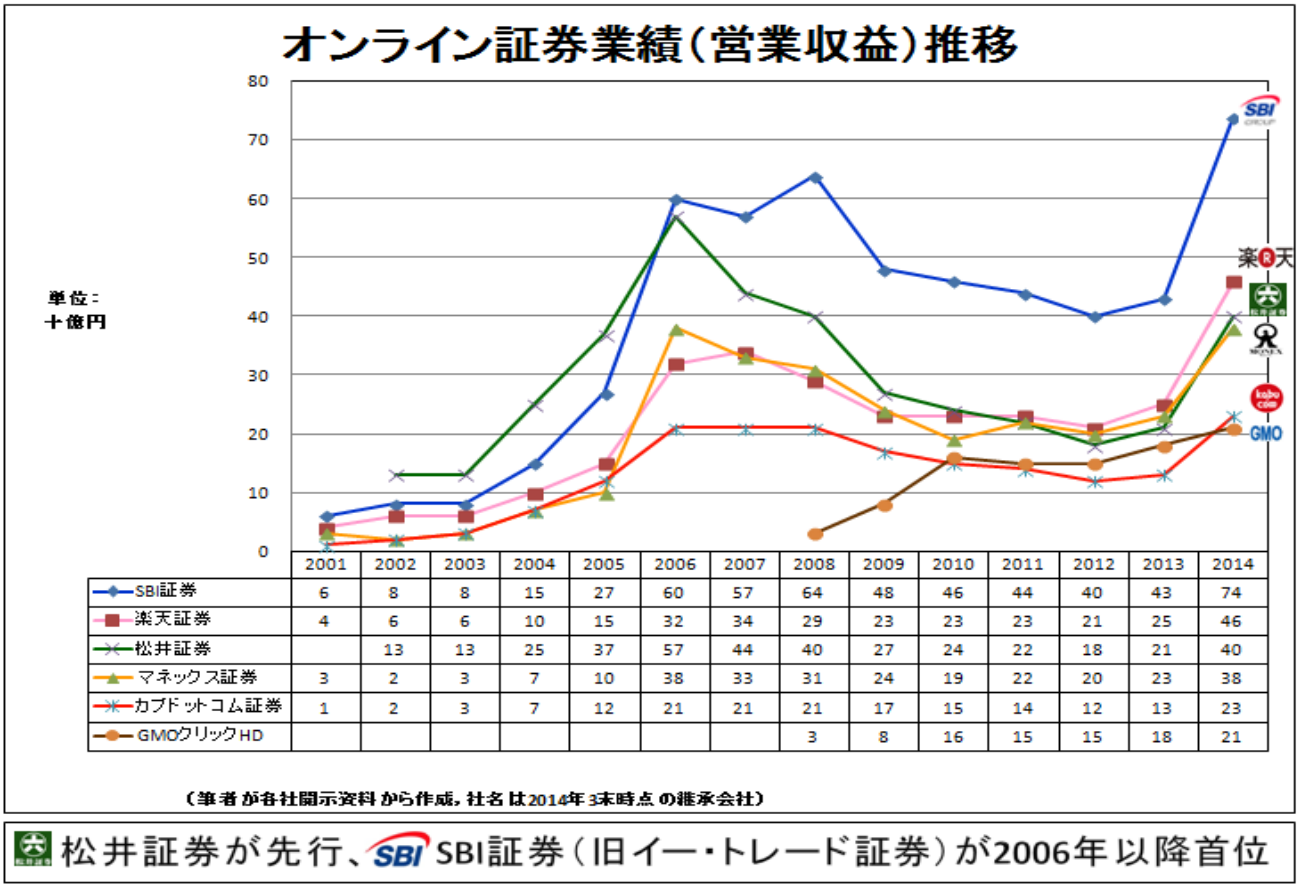
図 21 オンライン証券各社の概要

[30] 一般企業では売上高に相当する

また 5 社の業績推移を営業収益ベース（2001 年～）、営業利益率（2003 年～）で表わしたものが、図 22 と図 23 である。

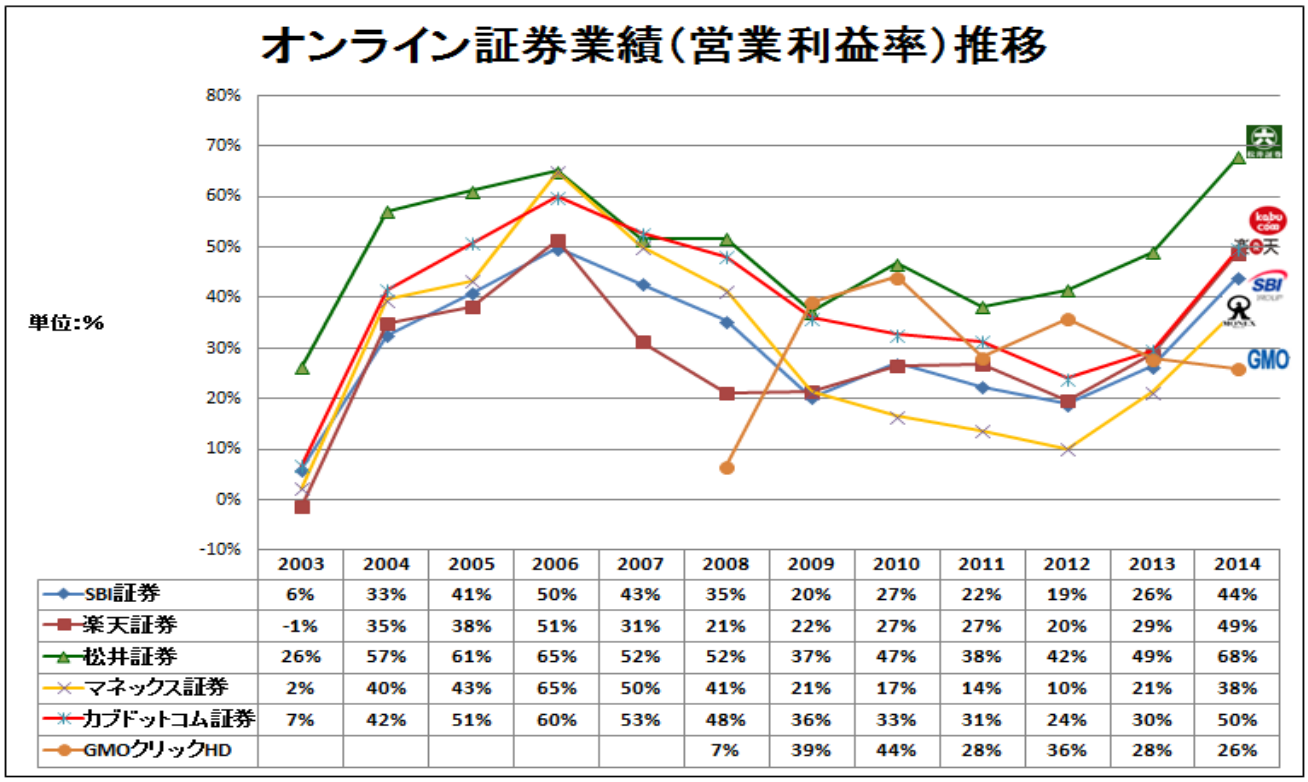
営業収益では、2005 年までは松井証券が首位であったが、2006 年以降は SBI 証券（旧イー・トレード証券）が首位を奪い、現在に至っている。松井証券は、2011 年以降は、楽天証券やマネックス証券にも抜かれ、3 位から 4 位の座に甘んじている。これは、当初は松井証券が、証券専業会社として、株式取引の熟練者をターゲットとした営業で成功した［高井文子, 2006］ものの、SBI 証券や楽天証券が、インターネット大手企業系列であることを活用したマーケティングで、市場を拡大してシェアを逆転したものである。

一方営業利益率では、松井証券が首位の座を安定して確保しており、ビジネスモデルの確立による収益力の高さを維持している。カブドットコム証券も 2 番手に付けており、収益力は高い。これは、システムの内製化によるところが大きいと推測される。なお、純利益でも松井証券、カブドットコム証券は安定している。



	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
SBI証券	6	8	8	15	27	60	57	64	48	46	44	40	43	74
楽天証券	4	6	6	10	15	32	34	29	23	23	23	21	25	46
松井証券		13	13	25	37	57	44	40	27	24	22	18	21	40
マネックス証券	3	2	3	7	10	38	33	31	24	19	22	20	23	38
カブドットコム証券	1	2	3	7	12	21	21	21	17	15	14	12	13	23
GMOクリックHD								3	8	16	15	15	18	21

図 22 オンライン証券業績（営業収益）推移



	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014
SBI証券	6%	33%	41%	50%	43%	35%	20%	27%	22%	19%	26%	44%
楽天証券	-1%	35%	38%	51%	31%	21%	22%	27%	27%	20%	29%	49%
松井証券	26%	57%	61%	65%	52%	52%	37%	47%	38%	42%	49%	68%
マネックス証券	2%	40%	43%	65%	50%	41%	21%	17%	14%	10%	21%	38%
カブドットコム証券	7%	42%	51%	60%	53%	48%	36%	33%	31%	24%	30%	50%
GMOクリックHD						7%	39%	44%	28%	36%	28%	26%

（筆者が各社開示資料から作成。社名は2014年3末時点の継承会社）

松井証券、カブドットコム証券の収益力が高い

図 23 オンライン証券業績（営業利益率）推移

4.3.2. オンライン証券における経営戦略、IT 戦略、金融情報システムの関係

オンライン証券 5 社は、同様の業務を実施しているが、IT への取り組みについては、大きな差があった。2013 年現在、SBI 証券、楽天証券の 2 社が「経営戦略包含型」、マネックス証券と松井証券が、IT 戦略に特徴がある「IT 戦略確立型」、カブドットコム証券が金融情報システムと無形資産（インタンジブル）が強く、経営戦略への貢献が大きい「金融情報システム貢献型」に分類される。

4.3.2.1. SBI 証券

「経営戦略包括型」の SBI 証券と楽天証券の共通点は、多角化事業の中での展開であること、それに関連するが、シナジー効果を高めるため顧客数の増大を図る戦略で拡大してきたことである。

SBI 証券は、設立時はソフトバンクグループの金融事業を担うところからスタートしており、その後、ソフトバンクグループから SBI グループとして独立したが、グループ内に保険、銀行、証券有人店舗を展開してきた。グループの中核事業でありながら、グループ全体の経営戦略の中に、オンライン証券事業の IT 戦略が包含されているとも言える。IT ポータ

ルでの顧客取込みを行う経営戦略が功を奏し、現在、口座数、営業収益とも他社を大きく引き離している。IT ポータルでの顧客取込みを IT 戦略として、「IT 戦略確立型」と捉える見方もある。

4.3.2.2. 楽天証券

楽天証券の場合、日本を代表するインターネット事業会社の一部門として、顧客数増大を図ってきた。業容拡大に対して情報システムの能力が追い付かず、2005 年から 2008 年にかけて IT 関連の障害が多発し、金融庁の業務改善命令を受けている。最近では、障害を起こさないアーキテクチャを構築する取組みを行う等、IT 戦略が萌芽している。

4.3.2.3. マネックス証券

「IT 戦略確立型」のマネックス証券と松井証券は、オンライン証券業に特化している点は共通しているが、全く異なる戦略を取っている。

マネックス証券は、積極的な M&A 戦略での拡大を図っている。国内 M&A で 2010 年にオリックス証券を合併し、2010 年に香港、2011 年にアメリカの会社を買収する海外 M&A を実施している。特にアメリカの Trade Station 社の買収は、その保有する金融情報システムとシステム内製化という無形資産（インタンジブルズ）を一つの大きな狙いとしていた。買収後、日本のユーザー向けに米国株取引ができる最先端のツールを提供して他社との差別化を図っている。またそのシステム開発手法であるアジャイル型開発手法[31]を日本の情報システムに移転する試みを行うとともに、無形資産（インタンジブルズ）の蓄積を図るべく、日本の情報システム開発部隊の内製化を推進する IT 戦略を取ってきている。

4.3.2.4. 松井証券

松井証券は、1999 年の開業前から営業マンを介さない個人顧客の取り込みのノウハウを持っていたことから、顧客数の増加を求めずに、収益性の高い、売買回数の多い顧客に対する利便性を高めることに注力した。すなわち手数料体系に加え、情報システムの使い勝手を対象とする顧客に合わせた形で構築し、システムの能力にも意を用いる等、IT 戦略を確立していたと言える。その結果、初期の業界では、唯一の勝ち組と言える状態となったが、その

[31] 不確実なビジネス環境の中で変化するニーズへの迅速な対応を目的としたソフトウェア開発手法で、顧客参加度合いが強く、反復漸進型で開発前の要求の固定を前提としないのが特徴である［独立行政法人情報処理推進機構ソフトウェア・エンジニアリング・センター, 2011］。

後、2006 年頃からは顧客数拡大戦略を取った SBI 証券に対し、営業収益、顧客数とも後塵を拝する状況となっている。収益力の高さではいまだ業界一であるが、持続的な競争優位を確立しているとは言い切れず、環境の変化にどのように対応していくのか興味が持たれる。

4.3.2.5. カブドットコム証券

「金融情報システム貢献型」のカブドットコム証券は、参入はやや遅れたが、CEO が SE の出身者であることもあり、金融情報システムに精通しており、金融情報システムで差別化する戦略を取ってきた。当初からシステムは運用も含め内製化するという、確固たる IT 戦略を取り、その結果、高い技術力の人材の内部蓄積に成功している。顧客に対し、システムのサービスレベルを保証し、レスポンスが遅れた場合は手数料を無料にするという施策を行っているが、これも、内製化要員が開発運用を行うことで、適切な対応ができることが背景にある。また、ソフトウェアを含む無形固定資産が、10%台で推移しており、これも内製化の確立によるものと考えられる。ただ IT 戦略は非常に優れているが、売買シェアについて上位 2 社に大きく離されている点で、IT 戦略以外の経営戦略による対応の余地があるとも考えられる。

4.3.2.6. まとめ

前節で検討した東京証券取引所は、「経営戦略包含型」から「IT 戦略確立型」を経て「金融情報システム貢献型」に移行した例である。移行の契機は、2006 年に IT に強い CIO を外部から招聘し、システム部門の改革を行い、IT 戦略を確立して、その後、構築した金融情報システム（「arrowhead」）とその開発に伴って蓄積した無形資産（インタンジブルズ）を活かして「金融情報システム貢献型」となるに至った。

それに対し、本節のオンライン証券業界は、様々なバックグラウンドを持つ事業者が競争しており、必ずしも段階的な移行をしているわけではない。1999 年代以降発展した業界であるため、開業当初は、安い手数料と軽装備のシステムでの市場シェアを獲得する戦略であったが、その後、会社毎の付加価値を高める戦略に転じて模索が続いていることは間違いなく、今後の環境変化を踏まえた戦略の対応と金融情報システムの貢献度合いに注目したい業界であると考える。

4.3.3. リスクマネジメント戦略の 6 観点(CORE-OQ)での分析

オンライン証券 5 社に関して、一部ヒアリング[32]も交え、リスクマネジメント戦略の 6 観点(CORE-OQ)に関しての適用状況を確認、分析し、図 24 に取り纏めた。

4.3.3.1. SBI 証券

経営トップのコミットメントと支援（Commitment）については、やや不明確であるが、組織体制とガバナンス（Organization）、IT リスクマネジメント（IT Risk Management）、品質重視の仕組構築（Quality）については、週次で経営戦略会議やシステム品質会議が開催されるなど整備がなされている。要件定義最適化（Optimization）の観点も整備されており、拡張性一貫性確保（Extenshibility）の観点でも、アーキテクチャを意識した検討がなされていることが確認できた。

4.3.3.2. 楽天証券

経営トップのコミットメントと支援（Commitment）及び IT リスクマネジメント（IT Risk Management）、品質重視の仕組構築（Quality）の観点は、2008 年の障害発生を機に大きく整備されており、組織体制とガバナンス（Organization）についても、システム企画部、アプリケーション開発部、プロジェクト推進部、インフラ統括部、システム運用部の充実した体制で整備がされている模様である。拡張性一貫性確保（Extenshibility）の観点でも、2014 年 5 月にデータベース基盤の刷新がされるなど、整備が進んでいる。

4.3.3.1. 松井証券

経営トップのコミットメントと支援（Commitment）については、経営戦略に基づいた IT 戦略が実施されている。組織体制とガバナンス（Organization）については、ベンダーとの情報処理サービス基本契約の形で整備がされている。要件定義最適化（Optimization）の観点も、差別化する業務の選択と集中が成されていることが確認できた。

4.3.3.1. マネックス証券

経営トップのコミットメントと支援（Commitment）については、情報システム強化を意識した M&A が行われており、明確である。組織体制とガバナンス（Organization）につい

[32] 2014 年 4 月 7 日 SBI 証券の岩吉常務(CIO)、2014 年 5 月 8 日カブドットコム証券の阿部常務(CIO)に対して実施。

ては、開発形態が異なる国内のシステム部と米国トレードステーション社[33]のシステム部門、を並列させつつ、グローバルシステム事業部が両者を統括する形となっている。また、拡張性一貫性確保（Extenshibility）の観点でも、グローバル戦略と連動したシステム戦略が実施されつつあることが確認できた。

オンライン証券各社の「CORE-OQ」取組みの分析　（筆者が作成）

	SBI証券	楽天証券	松井証券	マネックス証券	カブドットコム証券
Commitment	グループCEOは営業畑で、情報システムへの関与は少ない。	証券CEOはマーケティング担当だが障害対応でシステムも詳しい。	CEOの戦略が独自かつ明確。一日信用取引の推進。	CEOがM&Aによるグローバル戦略を推進。CTO(オランダ人)は、アジャイル型の開発を推進。	CEOがSE出身で、情報システムへの関与は強い。
Organization	システム開発部、システム運用部、品質管理部の体制。従業員484名(26年3末)だが、システム部要員は少数で、野村総研へ運用含めアウトソーシング。経営戦略会議(週次)で案件実現時期を決めている。	情報システム本部の中にシステム企画部アプリケーション開発部、プロジェクト推進部、インフラ統括部、システム運用部を持つ。従業員252名(26年2月)	システム部担当役員 従業員121名(コールセンター等155名:25年3月) SCSKと情報処理サービス基本契約締結	国内のシステム部とトレードステーション社のシステム部門は別組織で、利用部門はそれぞれに依頼をする形となっているが、グローバル・システム事業部が、両者を調整統括。従業員267名(26年2月)うち50名がシステム部。	事務システム本部の中にシステム部があり、システム部長がCIO。自社開発自社運用(汎用品はアウトソース、パッケージ商品をカスタマイズ)従業員数102名(26年3月)。システム部(約30名)の技術力が高い。
IT Risk Management	システム品質会議(週次)開催	障害対応の徹底	不明	不明	リスク管理部門が実施。CEOも関与。
Extensibility	旧アーキテクチャ部での検討結果を今後実施していく。(26年4月)	2014年5月データベース基盤の刷新。	不明	グローバル戦略	開発ロードマップによる一貫性確保。基盤システム更改による拡張性確保。
Optimization	経営戦略会議(週次)で案件実現時期を決める。	不明	選択と集中により、証券に特化。	不明	システム部主導での調整
Quality	システム品質会議(週次)開催	障害対応の徹底	不明	日興証券系ベンダー依存から内製化の進展、アジャイル開発への取組み。	品質管理チーム含め、全社的取組。

図 24 オンライン証券各社の「CORE-OQ」取組みの分析

4.3.3.2. カブドットコム証券

経営トップのコミットメントと支援（Commitment）については、社長が SE 出身であり、情報システムでの差別化を経営戦略の柱としている。具体的には、決算発表の VTR で、社

[33] 2011 年 6 月にマネックスグループが買収した米国のオンライン証券会社で、証券や FX の技術開発力に強みを持つ。

長が「情報システムが競争力の源泉でありサービス基盤そのもの」とアピールをしている。組織体制とガバナンス（Organization）についても、開業以来の内製化の中で技術力が蓄積されている。また IT リスクマネジメント（IT Risk Management）は、リスク管理部門で実施されており、品質重視の仕組構築（Quality）についても品質管理チームが組成されている。要件定義最適化（Optimization）の観点もシステム部が経営企画の役割も担う形で主導する形で整備されており、拡張性一貫性確保（Extenshibility）の観点でも、開発ロードマップが作成されている点、拡張性確保のための基盤システム更改がされている点が確認できた。

4.3.3.3. まとめ

オンライン証券大手 5 社は、各社とも情報システムが経営上重要なインフラであることを意識しており、リスクマネジメント戦略の 6 観点(CORE-OQ)については、確認できた範囲内では、整備されていた。

CIO 宛ヒアリングの結果を付記すると、リスクマネジメント CORE-OQ については、概ね違和感が無いという意見であった。その中でも、経営トップのコミットメントと支援（Commitment）と組織体制とガバナンス（Organization）が会社全体で重要であるとの認識が共通していた。

また、CIO 宛ヒアリングの中で、特に留意すべきマネジメント項目として、人事管理とベンダーマネジメントが重要であるとの指摘が共通していた。具体的には、以下 2 点である。

1）システム部員の将来のロードマップの可視化による育成計画や適切な労務管理によるモチベーションアップ施策。

2）ベンダー政策及びベンダーマネジメントの施策

これらの項目については、CIO が現場で最も苦労している点であると考えられる。リスクマネジメント戦略の 6 観点(CORE-OQ)の「組織体制とガバナンス（Organization）」の中でも、特に注意喚起すべきものであろう。

4.3.3.4. 経営戦略の実現に向けたリスクマネジメントの実践

本章では、リスクマネジメント戦略の 6 観点(CORE-OQ)に加え、「経営戦略」「IT 戦略」「金融情報システム」の関係に着目し、金融情報システムのリスクマネジメント実施が金融

機関の経営戦略実現にいかに貢献するかについて考察してきた。その中で、以下 2 点の示唆があった。

1）リスクマネジメント戦略の 6 観点(CORE-OQ)が、金融機関 CIO の視点でも違和感なく、経営レベルの指針として、十分に有効である。

2）東証及びオンライン証券の事例により、金融情報システムが、経営戦略に貢献するためには、リスクマネジメント戦略の 6 観点(CORE-OQ)が高いレベルで実施されていることが伺える。

第 4 章の実例での検討に続き、次の第 5 章では、リスクマネジメント戦略の 6 観点(CORE-OQ)を、別の様々な視点で検討し、体系化を図っていく。

第5章 金融情報システムのリスクマネジメントの体系化と評価

第 4 章までで、リスクマネジメント戦略の 6 観点(CORE-OQ)を中心に、金融情報システムのリスクマネジメントについて、検討分析してきた。第 5 章では、更にシステム監査関連基準の詳細記述での分析、CEO と CIO の役割分担の検討、組織マネジメントの視点での検討を行う。最後に、最近の環境変化のトピックス 5 点を採り上げ、それらへの対応を検討することで、金融情報システムのリスクマネジメントの体系化を図り、リスクマネジメント戦略の 6 観点(CORE-OQ)を評価することとする。

5.1. システム監査関連基準で見たリスクマネジメント[34]

リスクマネジメント戦略の 6 観点(CORE-OQ)が適切であることを確認するため、3.2 節で紹介した以下のシステム監査関連の基準の詳細記述にどのように対応しているかを調査分析する。

1）COBIT4.1 版 [IT ガバナンス協会, 2007]、
2）システム管理基準・システム監査基準 [経済産業省, 2004]、
3）金融機関等のシステム監査指針 [（財）金融情報システムセンター, 2007]、
4）金融検査マニュアル（預金等受入機関に係る検査マニュアル）・システム統合リスク管理態勢の確認検査用チェックリスト [金融庁, 2014] [金融庁, 2002]。

合わせてリスクカテゴリーについても、主目的として考慮されているオペレーショナルリスク以外のリスクであるビジネスリスク、戦略リスク、風評リスク、法務・規制リスクへの言及記載を確認する。

5.1.1. COBIT4.1（Control Objective for Information and related Technology)

「COBIT4.1 版」は、米国の IT ガバナンス協会が発行した基準である（3.2.1 項参照）。リスクマネジメント戦略の 6 観点(CORE-OQ)に関して、本基準を調査したところ、表 25 の通り、6 観点すべてが記載され、特に「組織体制と IT ガバナンス」、「IT リスクマネジメント」、「拡張性一貫性確保」、「要件定義最適化」の 4 観点が複数のプロセスで記述されていることが確認できた。とりわけ「組織体制と IT ガバナンス」の項目は全 34 プロセスのうち、8 プロセスに記述されており、重視されている（詳細は巻末別紙 1 ご参照）。尚、6 観点には

[34]本節は「金融情報システムの開発上流工程におけるシステム監査ポイントの提言」[遠藤正之、高野研一, 2013b]を元にしている。

分類できないが、CEO の関与が必要なアクティビティ項目として、ME1：IT 成果のモニタリングと評価のプロセスの項目が見出された。

表 25「COBIT4.1 版」とリスクマネジメント戦略の 6 観点(CORE-OQ)との対応

6 観点	プロセス	CEO の関与アクティビティ項目例
1. 経営トップのコミットメントと支援	PO1:IT 戦略計画の策定	ビジネス目標と IT 達成目標の関連付け
2. 組織体制と IT ガバナンス	PO1:IT 戦略計画の策定	IT 戦略計画、IT 実行計画策定
	PO4:IT プロセスと組織及びそのかかわりの定義	IT 戦略委員会の設置、利害関係者及びベンダーとのリレーションシップの確立、IT 組織構造の確立、IT プロセスフレームワークの策定
	PO10:プロジェクト管理	IT 投資のためのプログラム/ポートフォリオ管理フレームワークの定義
	ME4:IT ガバナンスの提供	IT 成果、IT 戦略、資源とリスクの管理のビジネス戦略との整合のレビュー承認周知、経営層による IT アクティビティに対する監督と推進の確立
3. IT リスクマネジメント	PO9:IT リスクの評価と管理	リスクマネジメントの整合性に関する判断 リスク対応実行計画の維持及びモニタリング
	DS5:システムセキュリティの保証	IT セキュリティ計画の定義と維持
4. 拡張性一貫性確保	PO1:IT 戦略計画の策定	プログラムポートフォリオの分析とプロジェクトおよびサービスポートフォリオの管理
	PO5:IT 投資の管理	プログラムポートフォリオの維持
5. 要件定義最適化	PO1:IT 戦略計画の策定	重要な依存関係及び最近の成果の特定
	PO2 情報アーキテクチャの定義	情報モデル、データディクショナリ、および分類スキームを活用した、最適化されたビジネスシステムの計画策定
6.品質重視の仕組構築	PO8:品質管理	品質管理システムの定義 、品質管理システムの確立と維持
6 観点以外	ME1：IT 成果のモニタリングと評価	モニタリングアプローチの確立、ビジネス目標をサポートする測定可能な目標の特定と収集

以上の分析から、「COBIT4.1 版」は、経営戦略やビジネスを意識したガバナンス重視のシステム監査関連基準であるが、記載の CEO 関与項目がリスクマネジメント戦略の 6 観点(CORE-OQ)に集約されていることが確認できた。

リスクカテゴリーに関しては、「戦略計画の策定」「戦略との整合」と言うキーワードで戦略リスクが強く意識され、「ビジネスと IT の整合」でビジネスリスク、「コンプライアンス」で法務・規制リスクに言及がある一方で、風評リスクに関しては、記載が見当たらなかった。

5.1.2. システム管理基準、システム監査基準

「システム管理基準」は、日本の経済産業省制定の基準である（3.2.2 項参照）。リスクマネジメント戦略の 6 観点(CORE-OQ)に関する調査結果は表 26 の通り、6 観点すべてが監

査項目として記載されていることを確認できた（詳細は巻末別紙 2 ご参照)。また、「組織体制と IT ガバナンス」、「IT リスクマネジメント」、「要件定義最適化」に関しては、複数の項で CEO 関与項目の記載が確認できた。一方、「経営トップのコミットメントと支援」、「拡張性一貫性の確保」、「品質重視の仕組構築」については、それぞれ 1 つの項での記述にとどまった。また 6 観点以外の CEO 関与項目は見出せなかった。

以上から「システム管理基準」は、情報システム部門の視点で策定されたシステム監査関連基準であるが、CEO 関与の項目がリスクマネジメント戦略の 6 観点(CORE-OQ)に集約されていることが確認できた。

リスクカテゴリーに関しては、「情報戦略」「全体最適化計画との整合性」というキーワードで戦略リスクが強く意識され、「コンプライアンス」の記載で法務・規制リスクが意識されていた。一方、風評リスクについては、「障害の報告体制」という関連項目の記載に留まり、ビジネスリスクに関しては記載が見当たらなかった。

表 26「システム管理基準」とリスクマネジメント戦略の 6 観点(CORE-OQ)との対応

6 観点	章、節、項	CEO関与の監査項目例
1. 経営トップのコミットメントと支援	Ⅰ.情報戦略1. 全体最適化 1.1全体最適化の方針・目標	IT ガバナンスの方針を明確にすること 情報システム全体の最適目標を経営戦略に基づいて設定すること
2. 組織体制と IT ガバナンス	Ⅰ.情報戦略2. 組織体制 2.1情報システム化委員会	全体最適化計画に基づき、委員会の使命を明確にし、適切な権限及び責任を与えること
	Ⅰ.情報戦略2. 組織体制 2.2情報システム部門	情報システム部門の使命を明確にし、適切な権限及び責任を与えること
	Ⅵ.共通業務2. 進捗管理 2.2評価	業務の工程終了時に、計画に対する実績を分析評価し、責任者が承認すること
	Ⅵ.共通業務4. 人的資源管理 4.1責任・権限	要員の責任及び権限は、業務の特性及び業務遂行上の必要性に応じて定めること
3.IT リスクマネジメント	Ⅰ.情報戦略5. 事業継続計画	情報システムに関連した事業継続の方針を策定すること
	Ⅰ.情報戦略6. コンプライアンス	法令及び規範の管理体制を確立するとともに、管理責任者を定めること
	Ⅵ.共通業務4. 災害対策 7.2 災害時対応計画	リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること
4. 拡張性一貫性の確保	Ⅰ.情報戦略3. 情報化投資	情報化投資計画は、経営戦略との整合性を考慮して策定すること
5. 要件定義最適化	Ⅰ.情報戦略4. 情報資産管理の方針	情報資産の管理方針及び体制を明確にすること
	Ⅱ.企画業務1. 開発計画	開発計画は、組織体の長が承認すること
6. 品質重視の仕組構築	Ⅵ.共通業務3.品質管理	品質管理計画は、方法、体制等を明確にすること

5.1.3. 金融機関等のシステム監査指針

「金融機関等のシステム監査指針」は、金融機関出資の財団法人金融情報システムセンターで策定された基準である（3.2.3 項参照)。リスクマネジメント戦略の 6 観点(CORE-OQ)に関する調査結果は表 27 の通り、6 観点すべてを大項目レベルの記載で確認できた（詳細は巻末別紙 3 ご参照)。特に「組織体制と IT ガバナンス」、「IT リスクマネジメント」、「品質重視の仕組構築」の 3 観点は、複数記載されていた。尚、6 観点以外の CEO 関与項目は小項目レベルでも見出せなかった。

表 27「金融機関等のシステム監査指針」とリスクマネジメント戦略の 6 観点(CORE-OQ)との対応

6 観点	要点項目、大項目[35]	CEO関与の小項目例
1. 経営トップのコミットメントと支援	1.情報システムの計画と管理 1.1.情報システム戦略	A.経営戦略に沿った情報システム戦略の策定 B.情報システム運営委員会
2. 組織体制と IT ガバナンス	1.情報システムの計画と管理 1.2.全社的な情報システム組織	A.情報システム部門の組織 B.ユーザー部門等の組織体制
	1.情報システムの計画と管理 1.3. 情報システム計画	A.情報システム中長期計画の策定 B.情報システム短期計画の策定と実施
	4.システム開発 4.1.運営と要員管理	B.システム開発業務の運営管理
	4.システム開発 4.7.プロジェクトマネジメント	A.プロジェクト計画の策定 B.プロジェクト計画の内容 C.プロジェクト要員
3.IT リスクマネジメント	2.情報システムリスクの管理 2.1.情報システムリスクの管理	A.情報システムリスク管理体制 B.情報システムリスクの識別と評価 C.情報システムリスク対策 D.法令・規制の遵守
	3.情報セキュリティ 1.全社的なセキュリティ管理体制	A.セキュリティポリシー B.セキュリティスタンダード C.セキュリティ管理体制
4. 拡張性一貫性の確保	1.情報システムの計画と管理 1.6.投資及び予算管理	A.予算計画の策定
5. 要件定義最適化	2.情報システムリスクの管理 2.3.情報システムの最新技術及び金融犯罪の動向に関する調査と研究	A.情報システムの最新技術及び金融犯罪の動向に関する調査と研究
6. 品質重視の仕組構築	4.システム開発 4.7.プロジェクトマネジメント	D.進捗・コスト・品質管理
	9.システム資産・資源管理 9.2.容量管理	A.キャパシティプランニング

[35] 1.2.…が要点項目、1.1,1.2…が大項目、A,B…が小項目。

以上から「金融機関等のシステム監査指針」は、金融機関向けのシステム監査関連基準であるが、CEO 関与の項目がリスクマネジメント戦略の 6 観点(CORE-OQ)に集約されていることが確認できた。

リスクカテゴリーに関しては、「情報システム戦略」「法令遵守」という項目で戦略リスク、法務・規制リスクが意識されていた。「広報活動の準備」という風評リスクの記述もあったが、ビジネスリスクへの言及は見当たらなかった。

5.1.4. 金融検査マニュアル（預金等受入機関に係る検査マニュアル）

「金融検査マニュアル」は、金融庁が策定した検査用の基準である（3.2.4 項参照)。リスクマネジメント戦略の 6 観点(CORE-OQ)に関する調査結果は、表 28 の通り、6 観点すべてを大項目レベルの記載で確認できた。また小項目にあたるチェック内容でも、6 観点すべてが複数のチェック内容で CEO 関与項目として、記載されていた（詳細は巻末別紙 4 別紙 5 ご参照)。

特に、「組織体制と IT ガバナンス」と「IT リスクマネジメント」が、大項目レベルで複数の項目で確認できた。また 6 観点以外の CEO 関与項目として、「システム統合リスク管理態勢の確認検査用チェックリスト」から、運営体制の明確化というチェック内容を見出すことができた。

以上から「金融検査マニュアル」は、監督官庁から発信された統制を意識した基準であるが、CEO 関与の項目がリスクマネジメント戦略の 6 観点(CORE-OQ)に集約されていることが確認できた。

リスクカテゴリーに関しては、「戦略目標の明確化」「マネーローンダリング」という項目で戦略リスク、法務・規制リスクが意識され、外部委託管理で「レピュテーション」との風評リスク関連の記載があったが、ビジネスリスクへの言及はなかった。

表 28「金融検査マニュアル」リスクマネジメント戦略の 6 観点(CORE-OQ)との対応

6 観点	大項目、中項目[36]	CEO関与のチェック内容抜粋
1. 経営トップのコミットメントと支援	Ⅰ.1. 方針の策定 Ⅰ.1.2.戦略目標の明確化	・システム戦略方針を含むか ・システム開発の優先順位 ・情報化推進計画 ・システムに対する投資計画
2. 組織体制とIT ガバナンス	Ⅰ.1. 方針の策定 Ⅰ.1.3.システムリスク管理方針の整備周知	・担当取締役及び取締役会等の役割・責任 ・システムリスク管理に関する部門の設置
	Ⅰ.2. 方針の策定 Ⅰ.2.3.システムリスク管理部門の態勢整備	・業務の遂行に必要な知識と経験を有する人員を適切な規模で配置 ・システムリスク管理部門から各業務部門に対する牽制機能が発揮される態勢を整備しているか
3.IT リスクマネジメント	Ⅰ.3. 評価改善活動 Ⅰ.3. 1 システムリスク管理の分析・評価	システムリスク管理の状況を的確に分析し態勢上の弱点や改善すべき点を検討し、原因を検証しているか
	Ⅲ. 3. 防犯防災バックアップ不正利用防止 Ⅲ. 3. コンティンジェンシー・プランの策定	災害等でコンピュータシステムが正常に機能しなくなった場合に備えたコンティンジェンシー・プランを整備しているか。
4. 拡張性一貫性の確保	Ⅲ. 2. システム企画・開発・運用管理 Ⅲ. 2. 1 企画・開発態勢	・投資対効果を検討しシステムの重要度及び性格を踏まえ、報告しているか。 ・中長期の開発計画を策定しているか
5. 要件定義最適化	Ⅲ. 2. システム企画・開発・運用管理 Ⅲ. 2. 1 企画・開発態勢	・信頼性が高く効率的なシステム導入を図る企画開発のための内部規程・業務細則等の整備 ・横断的な審議機関を設置しているか
6. 品質重視の仕組み構築	Ⅲ. 2. システム企画・開発・運用管理 Ⅲ. 2. 1 企画・開発態勢	・テスト計画を作成し、適切かつ十分にテストを行っているか ・テストやレビュー不足が原因で、長期間顧客に影響が及ぶような障害が発生しないようなテスト実施態勢を整備しているか
6 観点以外	Ⅱ. 協調したシステム統合リスク管理態勢のあり方 Ⅱ. ⅳ.協調した業務運営態勢のあり方	・運営体制の明確化(システム統合後のデータ受付、オペレーション、作業結果確認、データやプログラムの保管管理の職務分担を定め統合後の運営体制を明確にしているか

5.1.5. 監査の基準での考察

5.1.5.1. リスクマネジメント戦略の 6 観点（CORE-OQ）での考察

システム監査関連の 4 基準の分析の結果を、リスクマネジメント戦略の 6 観点(CORE-OQ)に関する項目の記載という切り口で纏めたのが表 29 である。

システム監査関連 4 基準の分析とそれを纏めた表 29 から、筆者は以下の 4 点を見出した。

[36] Ⅰ.1. , Ⅰ.2.…が大項目、Ⅰ.1.1. , Ⅰ.1.2.…が中項目。

表 29 システム監査関連の基準に関するリスクマネジメント戦略の 6 観点

		COBIT4.1 版	システム管理基準	システム監査指針	金融検査マニュアル
6 観点	経営トップのコミットメント	○	○	○	○
	組織体制と IT ガバナンス	◎	◎	◎	◎
	IT リスクマネジメント	◎	◎	◎	◎
	拡張性一貫性の確保	◎	○	○	○
	要件定義最適化	◎	◎	○	○
	品質重視の仕組構築	○	○	◎	○
注)◎:複数記載あり、○:記載あり（複数記載は、CEO 関与の観点で COBIT のプロセス、システム管理基準の章、システム監査指針・金融検査マニュアルの大項目レベルでカウント）					

第一に、各基準とも、CEO の関与度が特に高い項目として、経営方針の確定、ガバナンスの確立、組織の整備に関する項目を含んでおり、それらを抽出することができた。特にガバナンス関連の項目は各基準とも充実していた。リスクマネジメント戦略の 6 観点(CORE-OQ)のうち、「経営トップのコミットメントと支援」及び「組織体制と IT ガバナンス」に集約できるものである。

第二に、リスクの評価と管理の項目については、CIO が CEO よりも関与度が高い項目として、どの基準でも採り上げられていた。リスクマネジメント戦略の 6 観点(CORE-OQ)の「IT リスクマネジメント」の観点に集約できるものである。基準ごとに重点が異なっていたが、金融事業者向けの基準である「金融機関等のシステム監査指針」で情報セキュリティ項目の関与度の集計値が高かった点が特徴的であった。これは、金融事業が顧客の資産負債に関わる重要情報を取り扱っており、情報漏えいや紛失の事故が大きく報道されるという特質を反映したものと考えられる。

第三に、「拡張性一貫性の確保」、「要件定義最適化」、「品質重視の仕組構築」の各観点については、切り口や記載の濃淡はあるものの、既存の基準の中で採り上げられていることが確認できた。

第四に、リスクマネジメント戦略の 6 観点(CORE-OQ)以外の項目として、2 点を抽出することができた。一つ目は、「COBIT4.1 版」に記載された「IT 成果のモニタリングと評価」の項目であり、稼働開始後のシステムの評価についての経営者の関与の重要性を示唆するものであった。二つ目は、「金融検査マニュアル」の分冊である「システム統合リスク管理態勢の確認検査用チェックリスト」から抽出した、協調した業務運営態勢のあり方の項目であり、システム統合後の業務側の運営体制整備が重要であることを示唆するものである。

5.1.5.2. リスクカテゴリーでの考察

次に、金融機関のシステム監査人が監査を実施する観点でリスクカテゴリー（1.2.3）に関して、オペレーショナルリスク以外のリスクであるビジネスリスク、戦略リスク、風評リスク、法務・規制リスクが、金融情報システム自体が外部から直接評価されることを、確認するため、整理したのが表 30 である。

リスクマネジメント戦略の 6 観点（CORE-OQ）がすべての基準で網羅されていたのに対し、こちらは、基準により相違が発生した。オペレーショナルリスクについては、どの基準も当然のように十分意識されていたが、経営者が重視しているビジネスリスクの観点は COBIT だけが意識しており、日本の監査に関連する基準では明確に意識されていなかった。また風評リスクについては、どの基準もやや間接的な記載であった。さらに金融事業者の経営者が本業として関心を持っている市場リスク、信用リスク、流動性リスクについての記載は見出せなかった。経営者が着目するリスクへの記述が不十分であるという点で、経営者のリスクマネジメントに直接活用するには、やや物足りない面があることが伺える。

したがって、金融機関のシステム監査人が監査を実施する観点では、ビジネスリスクが意識された「COBIT4.1 版」と実務的な項目が網羅された「金融機関等のシステム監査指針」を組み合わせ、更に「システム管理基準」や「金融検査マニュアル」の要素を補完することが望ましいのではないかという示唆が得られた。

表 30 システム監査関連の基準でのリスクカテゴリー

		COBIT4.1 版	ｼｽﾃﾑ管理基準	ｼｽﾃﾑ監査指針	金融検査ﾏﾆｭｱﾙ
リスクカテゴリー	オペレーショナルリスク	◎	◎	◎	◎
	ビジネスリスク	○	－	－	－
	戦略リスク	◎	◎	○	○
	風評リスク	－	△	○	△
	法務・規制リスク	○	○	○	○
注）◎：複数記載あり、○：記載あり、△：関連項目記載あり、－：記載なし (複数記載は、CEO 関与の観点で COBIT のプロセス、システム管理基準の章、システム監査指針・金融検査マニュアルの大項目レベルでカウント)					

5.1.6. システム監査関連基準での検討のまとめ

リスクマネジメント戦略の 6 観点(CORE-OQ)に関しては、今回検討した事例とシステム監査関連の基準の分析の範囲では、経営者が着目すべきリスクマネジメントの項目を集約するものとして多様な観点から検討した結果、ほぼその妥当性が示唆されたと考える。ただし、CEO 中心の関与項目と CIO 中心の関与項目があること、金融事業者の経営者が重視するビ

ジネスリスクや、風評リスク等の観点が既存の基準に盛り込まれていないという示唆もあり、監査関連基準を利用する際の留意点と言える。

5.2. 経営者から見た金融情報システムのリスクマネジメント

前節では、システム監査関連の 4 基準を比較する形で CEO と CIO の関与項目について、検討してきた。本節では、更に議論を進め、先行研究からの示唆も採り入れ、CEO と CIO が行うべき金融情報システムのリスクマネジメントについて論じる。

さて、過去にも CEO と CIO の情報システム関与については、多くの研究が成されてきた[遠藤正之、高野研一, 2015]。

Doll は、「情報システムは技術者に任せておくにはあまりにも重要である」[Doll,W., 1985]と述べており、

Watson は、「情報システム管理者と CEO の関係が、情報システムマネジメントの重要課題の判断に影響を与える」 [Watson, R, 1990]としている。

Jarvenpaa らは、「トップマネジメントが情報システムのマネジメントに参加、関与することで、情報システムが発展する」 [Jarvenpaa,S.and Ives,B., 1991]とし、

Earl は、「情報システムの成功要因の第一は、トップマネジメントの関与である」 [Earl,M., 1993]とし、

Young らは「プロジェクトの重要成功要因の中でトップのサポートが最も重要である」[Young, R.and Jordan,M., 2008]とするなど、多くの研究者が情報システムの CEO の関与が重要であるとしている。

また、Banker らの「銀行や金融のように、差別化戦略を取る企業の多くは、CIO が CEO に直接報告している」 [Banker,R.et al., 2011]のように、CIO の関与も等しく重要視されている。

我が国の金融情報システムにフォーカスしても、経営者関与の重要性を指摘する研究は数多くなされている。

例えば，奥田は、「最も重要なポイントは，情報・知識産業としての本質を理解できるトップマネジメントの存在である」 [奥田晃司, 2005]とし、

森は、以下のように述べている。「情報戦略と経営戦略に精通し、それらを融合させ，経営上大きな役割を担う人的資源である CIO を確立していくとともに、（中略）経営戦略の立案実行に積極的に関与させることが求められる」 [森俊也, 2006]。

宮坂らは、「IT 統合は（中略）企業経営における最重要課題であることを経営トップ自らが認識しなければならない」 [宮坂美樹、山本秀男, 2010]としている。

冨永は、「本来は、CEO が CIO となることが理想的である。(中略)現実的には、現場感覚と経営センスを有する CIO を養成あるいは探し出し、IT 戦略やシステム統制を任せるところから始めるべきだろう。」 [富永新, 2009]とし、

渡辺は「IT・システムリスクへの取組みは（中略）経営戦略上の課題として取り組むべきものである」 [渡辺研司, 2005]とする等の指摘である。

以上の先行研究から、経営トップ（CEO）と CIO がいかに、情報システムに関して連携することが重要であることが、改めて認識できる。その一方で、経営トップ（CEO）が自ら行うべきことと、CIO に委任しサポートする要素とがある点について意識すべきとの示唆もある。経営トップで会社全体に責任を持つ CEO と情報システム部門の責任者である CIO の役割は自ずと異なっており、より明確に分けて考えることが必要である。リスクマネジメント戦略の 6 観点「CORE-OQ」（コア OQ）に関しても、CEO（経営トップ）が主として果たす役割と、CIO が主として果たすべき項目があると言える。また、6 項目の比重も均等ではない。そこで、経営トップが自ら行うべき事項と、CIO に委任しサポートする事項があるという点を図 25 に図示した。これに沿って、CEO と CIO それぞれについて説明していく。

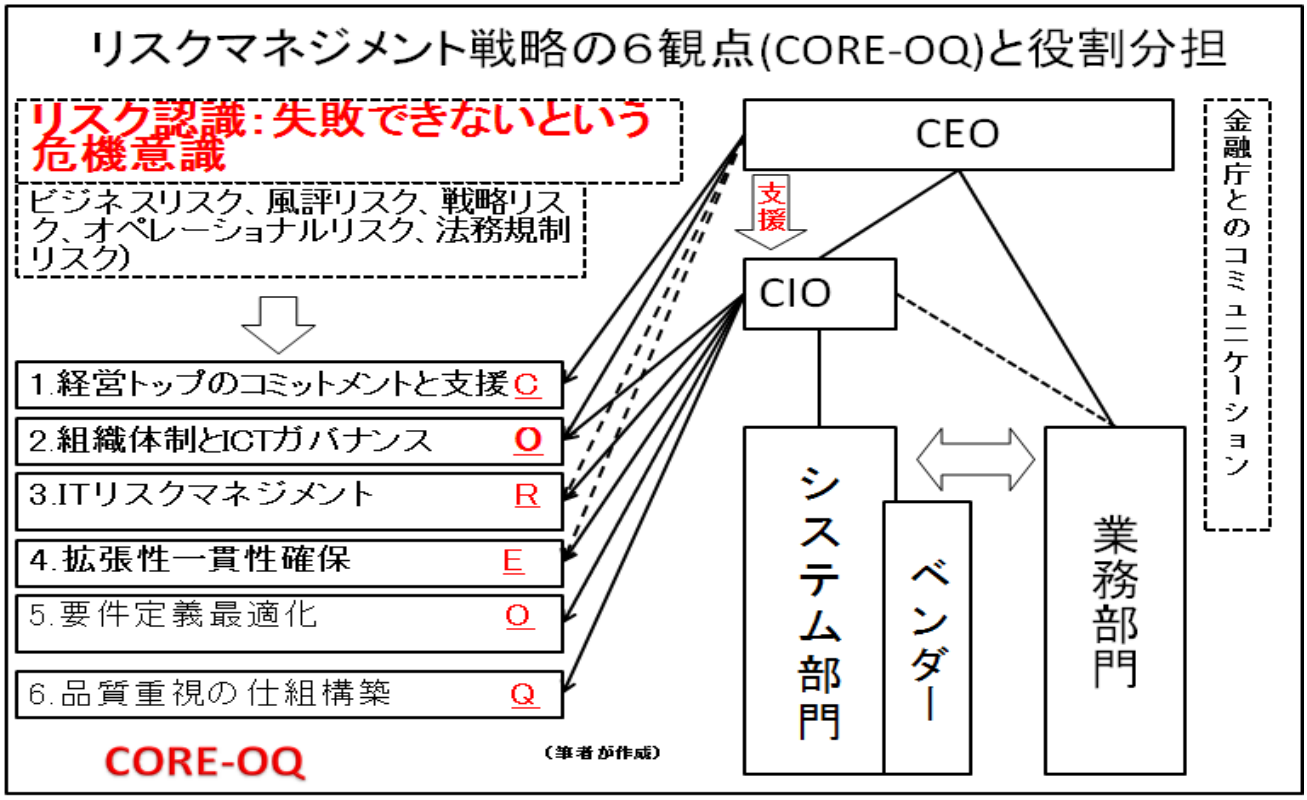


図 25 リスクマネジメント戦略の 6 観点(CORE-OQ)と役割分担

5.2.1. CEO の役割

CEO（経営トップ）にとっては、金融情報システムへのコミットメントとして、CIO の選任や、社内体制構築が最重要である。また、全社的に重要な大規模プロジェクトでは、CIO が最後まで一貫してやりきれるような使命を与え、CEO が支援し続けることが必要である。プロジェクトのサイクルを意識した、CIO の起用を行うことが望まれる。

CEO（経営トップ）が、「経営トップのコミットメントと支援」のうち、「経営トップのコミットメント」として、直接的に関与すべき項目としては、第一に経営戦略を明確化すること、第二にプロジェクト期間を全うする CIO を指名付けし、その上で経営参画をさせるなど継続的に支援をすること、第三に情報システム構築に適した社内体制を整備するため、リーダーシップを発揮することが挙げられる。

第一の経営戦略の明確化については、その企業の将来にわたる戦略を明確化し、共有するとともに、IT 戦略に求めるものや優先順位を明確にすることが必要である。このプロセスの過程で、経営者が必然的に金融情報システムの開発にコミットメントすることになる。

第二の CIO の指名付けと経営参画をさせるなど継続的に支援する点については、そのプロジェクト完了までの明確な責任と権限を与えると共に、経営に参画させることで社内でのステータスを高めることが期待される。

第三の社内体制の構築にあたり、リーダーシップを発揮する点は、CIO 以外の経営陣及び業務部門とシステム部門の連携体制を構築することで、CIO をサポートすることが必要である。

次に経営トップが「経営トップのコミットメントと支援」のうち、「支援」として間接的に関与する項目としては、第一に CIO への金融情報システム開発と運用執行の委任、第二に「拡張性一貫性確保」のベースとなる長期的視野の CIO との共有、第三に IT リスクマネジメントへの関与である。

第一の CIO への金融情報システム開発と運用執行の委任については、開発体制、プロジェクトガバナンス構築、プロジェクトリスクマネジメントの仕組構築等について執行を CIO に委任し、経営トップは社内での反対を抑えるといったサポートを行う立場が望ましい。

第二の長期的視野の CIO との共有については、長期的視野でのコスト、効果への目配り（EA、要件最適化、品質重視）を支援サポートするという点である。

第三の IT リスクマネジメントへの関与については、リスク認識を CIO と共有することと、特に重要なリスクについて把握し、経営判断につなげることが重要である。

5.2.2. CIO の役割

CIO については、CEO からの委任を受け、責任を持って金融情報システム以下の観点を担う必要がある。CIO の役割分担の中心となるのは、第一に「組織体制と IT ガバナンス」のシステム部門の開発体制整備、第二に「IT リスクマネジメント」のリスクの継続的管理、第三に「拡張性一貫性確保」、「要件定義最適化」、「品質重視の仕組構築」に関して、現状の保有システムと IT 戦略を意識した金融情報システムのポートフォリオマネジメントの主導である。

第一の「組織体制と IT ガバナンス」のシステム部門の開発体制整備は、システム開発と運用保守を含め、社員及びベンダーの体制を整備し、短期的に経営や業務のニーズを実現しながら、中長期的な視点で、インタンジブルである人的スキルやノウハウの蓄積を図ることが重要である。

第二の「IT リスクマネジメント」のリスクの継続的管理に関しては、洗い上げたリスクを評価し、優先順位を付けてトラッキングするとともに、ハードソフトの経年経過や環境変化に伴うリスクが無いかを定期的に洗い上げて、重要なリスクについては、CEO にも共有することが必要である。

第三の金融情報システムのポートフォリオマネジメントの主導に関しては、経営戦略、IT 戦略に沿って、長期的な視野での推進が必要な、システムのインフラの整備や、開発手順や進捗管理、品質管理の標準化施策への資源配分を行うことが望まれる。

また経営トップ、CIO が、共に関与すべき項目もある。それは、金融情報システムは、金融システムのインフラであることを考慮し、経営する金融業全体の安定性、影響点、国際競争力にも配慮した仕組みで、開発を進めるというポリシーを持ち、それを判断軸にするという点である。

5.3. 組織マネジメントの視点でのリスクマネジメント

金融情報システムのリスクマネジメントを IT 戦略と整合する形で、適確に実施するには、組織マネジメントの要素も重要である。本節では、金融情報システムに関する組織マネジメントの観点について、組織論と組織の安全文化の先行研究を通して検討を行う。

5.3.1. 組織論からの視点

組織マネジメントを学術的に体系化しているのが、組織論である。この組織論と呼ばれる学問領域には、「ミクロ組織論」と「マクロ組織論」の 2 つの捉え方があり、それぞれに 3 つの側面がある［野田稔, 2005］。

5.3.1.1. ミクロ組織論

第一のミクロ組織論は、組織の中の個人の行動や、個人と個人の関わり方に焦点を当てるものである。その中に以下の 3 側面がある。

1）リーダーシップ、

2）個人の行動、

3）集団の行動。

1）リーダーシップ論には、強いリーダーシップを発揮するカリスマ的リーダーシップや、変革的リーダーシップから、部下を手助けするサーバントリーダーシップまで、様々なリーダーの類型がある。リーダーより従う側であるフォロワーが重要であるとするフォロワーシップに関する議論もある。金融情報システムと経営者の関わりにおいては、経営

者が、M&A に伴うシステム統合を行うタイミングのような重要な変革期においては、強いリーダーシップを発揮することが求められる。一方平常時においては、組織体制を整備し、システム部門の社内での重要性を社内外に認識させるような、サーバントリーダーシップが求められる。これは、リスクマネジメント戦略の 6 観点(CORE-OQ)の「経営トップのコミットメントと支援」そして、「組織体制と IT ガバナンス」の項目に該当する。

2）個人の行動とは、組織における個人の動機付け（モチベーション）やコミットメントに関するものである。個人のモチベーションを高めるためには、外発的な動機付けと内発的な動機付けがあると言われる。外発的な動機付けは、昇給等の金銭的な見返りや昇進昇格によるものであるが、与えることができる給与も昇進対象のポストも有限であり、その効果にも限界がある。金融情報システムのリスクマネジメントでも、この方式には同じく限界がある。一方で、内発的な動機付けは、有能さと自己決定の感覚が動機付け要因であるとされ、自己が有能で自己決定的であると感じている人は、さらなる有能さと自己決定の感覚を求めて意欲を燃やし努力を投ずるのである［二村敏子, 2004]。この内発的な動機付けを高めることで、仕事全般に対するコミットメントを高めることができる。金融情報システムに関しても、情報システム部員の内発的動機づけを高めるためには、経営戦略や IT 戦略を経営者と共有することが大きな要素となる。これは、リスクマネジメント戦略の 6 観点(CORE-OQ)の「経営トップのコミットメントと支援」の項目に該当する。

3）集団の行動とは組織の意思決定や、構成メンバー間のコミュニケーションに関するものである。組織においては、組織メンバーが適切な意思決定を行う際に、コミュニケーションが重要な要素となる。組織メンバー間の意識の整合性を取ることで、その意思決定が効果的となるのである。その際、判断の基準となる組織メンバーの認知の枠の存在を意識し、受け手の感情に配慮したコミュニケーション手段を取る必要がある。金融情報システムにおいても、経営者と業務部門、情報システム部門間での視点や認知の枠組みが異なることを意識した、コミュニケーションが必要となる。これは、リスクマネジメント戦略の 6 観点(CORE-OQ)の全部の項目に関係するものである。

5.3.1.2. マクロ組織論

第二のマクロ組織論は、組織構造やその機能や調整、組織間のネットワークに焦点を当てるものであり、以下の 3 側面からなる。

1）組織構造、

２）組織機能、

３）組織ネットワーク。

１）組織構造とは、組織のデザインや複雑性に焦点をあてるものである。古くは職能性組織と事業部制組織やカンパニー制組織、最近ではネットワーク組織といった組織形態や機能型組織とプロジェクト型組織、マトリックス型組織等の組織デザインを考える分野である。金融情報システムにおいては、情報システム部門は開発プロジェクトを遂行するためのプロジェクト型組織となっている一方で、業務部門は機能型組織や顧客カテゴリー別の組織となっていることが多い。そのために、業務部門のニーズが情報システム部門に対して、1 対 1 対応であることはまれであり、複数の部署からのニーズが発生することになる。そのために、ニーズの優先順位を一元的に決定するための組織や会議体が必要となる。これは、リスクマネジメント戦略の 6 観点(CORE-OQ)の「経営トップのコミットメントと支援」そして、「組織体制と IT ガバナンス」の項目により支援されるものである。調整の対象としては、「要件定義の最適化」があてはまる。

２）組織機能とは、組織メンバーの職能、ラインとスタッフの役割、組織内の調整メカニズムを議論するものである。組織が大規模になるにつれて、組織メンバーの役割分担が明確となり、分業が進むようになる。更に指揮命令系統についても組織が拡大すると、リーダーが、自身のライン配下のメンバーの状況を把握することが困難になり、そのためのスタッフ組織を必要とするようになる。組織の複雑化が進み、組織メンバー間の調整メカニズムが必要になる。小規模な組織では、相互のコミュニケーションや、直接的な管理監督により調整が成されるが、より大きな組織では、目標やビジョンの共有と業務の標準化による調整メカニズムが必要となる。金融情報システムにおいても同様であり、特に社員以外のベンダーと仕事を分担することが多く、標準化が非常に重要となる。これは、リスクマネジメント戦略の 6 観点(CORE-OQ)の「品質重視の仕組構築」が該当する。

３）組織ネットワークについては、グループ経営や、組織間ネットワークから組織を見る側面である。昨今、金融事業においては、持株会社形式での M&A が多数発生しており、金融情報システムの統合や接続が必要になってきている。また、金融情報システムの分野でもオフショア開発に代表される遠隔地での開発が行われており、この観点が重要である。リスクマネジメント戦略の 6 観点(CORE-OQ)では、「組織体制と IT ガバナンス」が該当する。

5.3.1.3. 組織論からの視点のまとめ

ミクロ組織論の 3 側面、マクロ組織論の 3 側面に関して検討したが、組織論の観点でもリスクマネジメント戦略の 6 観点(CORE-OQ)は適切な項目を含んでいることが確認できた。

5.3.2. 組織の安全文化研究からの視点

前項の組織論からの視点に続き、本項では、組織の安全文化研究の視点でリスクマネジメント戦略の 6 観点(CORE-OQ)について、検討する。ここで採り上げるのは、既存研究や製造業を中心とした安全性向上の実践活動を通して、組織の安全文化の構成要因を体系化した高野の研究である。金融業においても、大規模障害の発生を防止するという信頼性実現が求められており、共通する点があると考える。高野が提唱する具体的な構成要因は、以下の組織の安全文化の 8 軸（8 つの視点）である［高野研一, 2013］（図 26）。

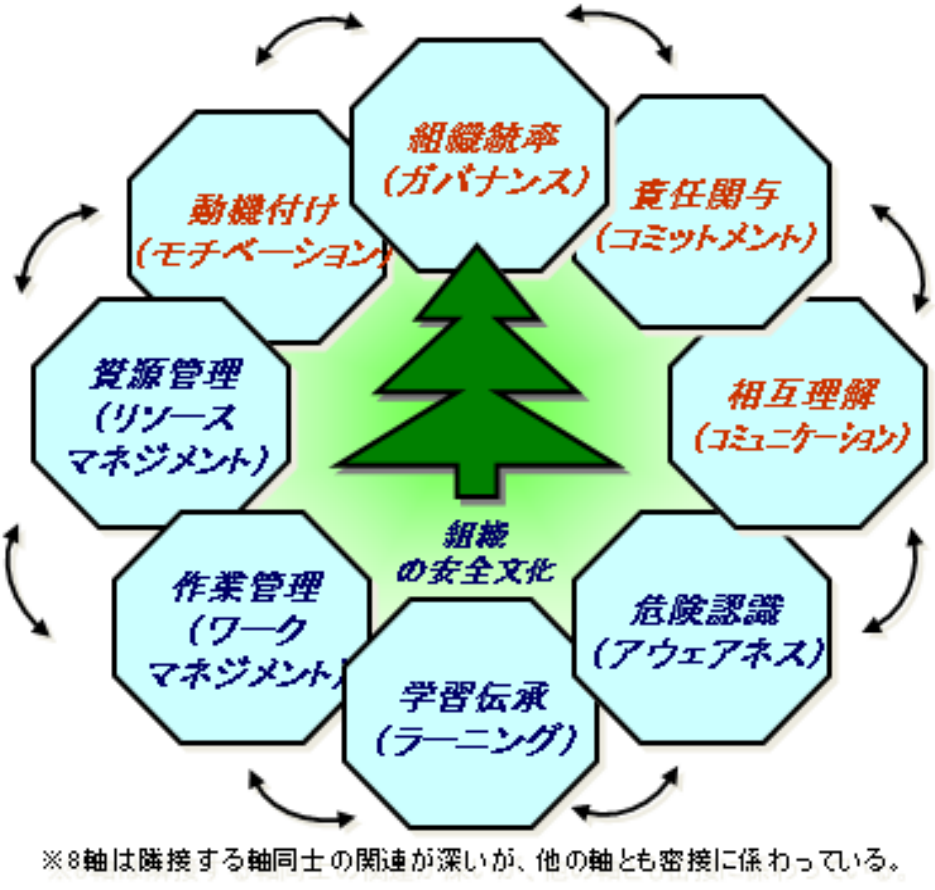


図 26 組織の安全文化の 8 軸（8 つの視点）［高野研一，2013］

1）組織統率（ガバナンス）、

2）責任関与（コミットメント）、

3）相互理解（コミュニケーション)、
4）危険認知（アウェアネス)、
5）学習伝承（ラーニング)、
6）作業管理（ワークマネジメント)、
7）資源管理（リソースマネジメント)、
8）動機付け（モチベーション)。

5.3.2.1. 組織統率（ガバナンス）

組織統率（ガバナンス）とは、組織内で安全優先の価値観を共有し、これを尊重して組織管理を行うことで、コンプライアンス、安全施策における積極的なリーダーシップを含んでいる。金融情報システムでも組織のガバナンスは重要であり、リスクマネジメント戦略の 6 観点の「組織体制と IT ガバナンス」に合致するものである。

5.3.2.2. 責任関与（コミットメント）

責任関与（コミットメント）とは、組織の経営トップ層及び管理者層から一般職員まで、また規制者、協力会社職員までが各々の立場で職務遂行にかかわる安全確保に責任を持ち、自主的かつ積極的に関与することである。金融情報システムでのリスクマネジメント戦略の 6 観点「経営トップのコミットメントと支援」に合致する項目である。

5.3.2.3. 相互理解（コミュニケーション）

相互理解（コミュニケーション）とは、組織内及び組織間（規制者、同業他社、協力会社）における上下、左右の意思疎通、情報共有、相互理解を促進し、これに基づき内省することである。特にマイナス情報についての共有を行うことである。5.3.1 項のミクロ組織論でも挙げられており、金融情報システムでもリスクマネジメント戦略の 6 観点のすべての項目に関係する。

5.3.2.4. 危険認知（アウェアネス）

危険認知（アウェアネス）とは、個々人が各々の職務と職責における潜在的リスクを意識し、これを発見する努力を継続することにより、危険感知能力を高め、行動に反映することである。特にマイナス情報についての共有をおこなうことである。金融情報システム

でも障害発生の未然防止や、開発プロジェクトにおける QCD[37]（品質、コスト、納期）目標の未達成を防止する観点で重要であり、リスクマネジメント戦略の 6 観点では、「IT リスクマネジメント」と合致する。

5.3.2.5. 学習伝承（ラーニング）

学習伝承（ラーニング）とは、安全重視を実践する組織として必要な知識（失敗経験の知識化等）、そして背景情報を理解し実践する能力を獲得し、これを伝承していくために、自発的に適切なマネジメントに基づく組織学習を継続すること。またそのための教育訓練を含むものである。金融情報システムでも情報システム開発に関わる技術やスキルの蓄積が組織全体のインタンジブルズ（無形資産）の蓄積に非常に重要である。リスクマネジメント戦略の 6 観点では「組織体制と IT ガバナンス」に合致する項目である。

5.3.2.6. 作業管理（ワークマネジメント）

作業管理（ワークマネジメント）とは、文書管理、技術管理、作業標準、安全管理、品質管理など作業を適切に進めるための実効的な施策が整備され、個々人が自主的に尊重することである。金融情報システムにおいても、文書による管理や作業の標準化、共有化、品質管理は重要であり、リスクマネジメント戦略の 6 観点では「品質重視の仕組構築」に合致する項目である。

5.3.2.7. 資源管理（リソースマネジメント）

資源管理（リソースマネジメント）とは、安全確保に関する人的、物的、資金的資源の管理と配分が一過性で無く適正なマネジメントに基づき行われていることである。金融情報システムにおいても、開発要員や運用保守の要員を適切に調達すること、そしてハードウェアやソフトウェアについても、適切な調達管理が重要である。オンライン証券の CIO ヒアリングでも、その点を指摘されている。リスクマネジメント戦略の 6 観点では「組織体制と IT ガバナンス」に合致する項目である。

5.3.2.8. 動機付け（モチベーション）

動機付け（モチベーション）とは、組織としてふさわしいインセンティブ（やる気）を与えることにより、安全性向上に向けた取り組みが促進されるとともに、職場満足度を高

[37] Q は品質（Quality）、C はコスト（Cost）、D は納期（Delivery）の略であり、システムプロジェクトの成功要因の 3 要素として説明されることがある。

めることである。5.3.1 項のミクロ組織論でも挙げられている項目であるが、金融情報システムにおいても、経営トップの適切な関与により、経営戦略や IT 戦略を経営者と共有することが大きいと考える。リスクマネジメント戦略の 6 観点では「経営トップのコミットメントと支援」に合致する項目である。

5.3.2.9. 組織の安全文化研究からの視点のまとめ

組織の安全文化研究での高野の組織の安全文化の 8 軸（視点）に関して検討したが、リスクマネジメント戦略の 6 観点(CORE-OQ)が、対応する適切な項目を含んでいることを確認することができた。

5.3.3. 情報システムでの組織マネジメント研究

前項までは、一般の組織論や組織の安全文化研究の視点で考察したが、本項では情報システムに焦点を絞った組織マネジメントに関する最近の研究について、検討する。

5.3.3.1.「IT マネジメントの新機軸」（向正道）

向は、企業の IT マネジメントに関して、経営者、事業部門、情報システム部門の間のコミュニケーションの問題点の一つとして、情報システムの現状や課題を経営者が理解できる文書の不在を指摘し、その解決策として、具体的な事例となるフォーマットを提案している［向正道, 2013]。更に情報システム部門は経営や事業部門との約束を守る点、すなわち QCD（品質、コスト、納期）の目標実現のみならず、経営や事業部門が期待している点、システム活用によるビジネスへの直接貢献や、システムがビジネスの制約とならないことなどでの貢献が必要であるとしている。

向の検討、提言はまさに、組織論における「コミュニケーション」、組織の安全文化研究における「相互理解（コミュニケーション)」の具体的施策を提言するものである。また経営者への期待だけでなく、情報システム部門が自ら経営や業務部門に貢献する姿勢を指摘している点は傾聴に値する。

5.3.3.2. 情報システムを成功に導く経営者の支援行動（栗山敏）

栗山は、情報システム構築プロジェクトは不確実性があるが、経営者が不確実性にタイムリーに対応するためには、意思決定機関としてステアリングコミッティーが有効に機能することが必要であると指摘している。［栗山敏, 2013]。そして、情報システムプロジェクトを成功に導く経営者の支援行動として、以下の 4 点を挙げている。

1）計画化（Planning）関連。具体的には、情報システム導入の可否の承認、QCD 目標の決定、戦略目的の決定周知徹底がある。

2）組織化（Organizing）関連。具体的には、必要メンバーのアサインによるプロジェクトチーム編成、人材の計画的育成がある。

3）指揮（Leading）関連。具体的には、ステークホルダーのモチベーションへの配慮、経営者とプロジェクトメンバーとの共通言語確立、経営者の積極的学習、リーダーシップの発揮がある。

4）統制（Controlling）関連。具体的には、戦略目標達成のために、柔軟に QCD 目標の修正ないし、要件圧縮の受容がある。

栗山の検討対象は、情報システム一般であるが、これらの項目は、金融情報システムでもあてはまる項目である。ただ、金融情報システムは 2.4.1 項で述べたように、可用性要求や情報セキュリティ要求が厳しいという点で、より強い経営者の支援行動が必要になると考える。

5.4. 環境変化とリスクマネジメント戦略の 6 観点の評価

ここまで様々な視点で検討してきたが、最近、金融情報システムをめぐる環境は著しく変化しており、ここまで十分に検討しきれなかった分野について検討し、リスクマネジメント戦略の 6 観点での対応のスコープに収まるかを確認し、評価する。具体的には、クラウド技術、情報セキュリティ環境、開発手法・組織の多様化、地域金融機関の共同化、リスクアペタイト・フレームワークの 5 点について検討する。

5.4.1. クラウド技術

最近の IT の進展すなわちクラウド技術の利用による金融情報システムへの影響である。クラウドの金融情報システムでの利用については、最近進んできているが、まだ顧客が利用するオンラインシステムや、決済が行われる大規模なシステムでの利用には至っていない。

しかしながら、今後、中小規模金融機関を含め、ハードソフトの保有コストを削減する目的と、開発スピードの速さを求める点から、普及が進む可能性がある。最近、財団法人金融情報システムセンターにおいて、利用方法に関する有識者の意見取り纏めが行われ 2014 年 11 月に「金融機関におけるクラウド利用に関する有識者検討会報告書」として公開された。［（財）金融情報システムセンター, 2014]。

その中での、クラウドのメリットとリスクの例は表 31 表 32 の通りであるが、その利用には経営者の関与による判断とリスク軽減策の実施が、従来の情報システム導入以上に必要となる。なぜならば、従来の情報システム以上にコスト削減や納期短縮等のメリットが大きい反面、自社でのシステムと異なるリスクが発生するからである。リスクマネジメント戦略の 6 観点では「経営者のコミットメントと支援」及び「IT リスクマネジメント」が、より高いレベルで適切に行われることが必要である。

表 31 クラウドのメリット（例） [（財）金融情報システムセンター, 2014]

メリット	内容
コスト削減	資源共有型スキームで規模の経済が働くスケールメリットによってシステムのコスト削減が見込まれる。
納期・システム開発期間の短縮	ユーザーが IT インフラを自前で調達・構築するプロセスと比べて、リソースの導入・構築に係る手間が大幅に減少するため、サービスインまでの納期やシステム開発期間を短縮できる。
システム運用負担の軽減	システムメンテナンス等の運用を事業者に任せることによってユーザーの運用負担を軽減できる。
拡張性・柔軟性	スモールスタートや一時的な使用、即時撤退などが可能となり、機会損失の抑制や先行者利得の確保に寄与する可能性がある。
オンデマンドセルフサービス	ユーザー自身でサーバー等の利用や停止をコントロールできるため、無駄な資源利用を排除できる。
利便性や機能の向上	新技術導入スピードが速いため、ユーザーの利便性や機能向上の効果が大きい。またモバイル端末や SNS（ソーシャル・ネットワーキング・サービス）等との親和性が高く、社内外環境とのデータ交換や情報共有も容易にできる。
業務継続性	隔地に分散する複数の資源の利用が前提となっているサービスの場合、拠点被災等に対する業務継続性が高い。

表 32 クラウドのリスク（例） [（財）金融情報システムセンター, 2014]

リスク	分類	内容
法制度の違いによる影響	法制度	プライバシー保護等の要請が国（法域）によって異なることに伴い、トラブルが生じた場合の対応や個人データの移転に支障が生じる可能性がある。
情報漏洩リスク	技術	サービス終了時にハードウェアの物理的な破壊・消磁を通じたデータの完全消去が困難なため、残存したデータが漏えいするリスクがある。
	技術	オンプレミスの環境と異なり、ネットワークでのデータ伝送をベースとした仕組みであるため、データ伝送中のデータが漏えいするリスクがその分大きい。
リアルタイム性、可用性への懸念	運用	他ユーザーのトラフィックが高まった場合、自ユーザー分の処理に係るリソースが不足することにより、レスポンスの悪化やシステムの停止につながる可能性があり、求められるサービスレベルが保証されない懸念がある。
インシデント対応の不十分性	ガバナンス	クラウド事業者は、コスト節約や機動的なサービス開始を重視するため、標準化されたものより踏み込んだユーザーサポートを行うことに消極的な場合がある。この結果、ユーザーによるリスク管理上必要な情報の開示やインシデント対応が十分に行われない可能性がある。

5.4.2. 厳しい情報セキュリティ環境

最近の情報セキュリティは、大きく変化している。特にネット上の情報セキュリティリスクの拡大とその対策の必要性が高まったことである。「情報セキュリティ白書 2014」では、2013 年度の情報セキュリティのトピックスとして、以下の 10 点を挙げている［独立行政法人情報処理推進機構技術本部セキュリティセンター, 2014]。

１）インターネットバンキングを狙った攻撃が多発、被害額は過去最悪、

２）Web 改ざん被害が過去最悪、フィッシング詐欺も横行、

３）パスワードリスト攻撃による不正利用が頻発、

４）政府機関をターゲットとした水飲み場型攻撃、

５）内部者による情報漏洩、

６）「サイバーセキュリティ戦略」の決定、

７）サイバーセキュリティの国際連携、

８）制御システムの情報セキュリティシステムへの取り組み、

９）情報セキュリティ人材育成への取り組み、

１０）パーソナルデータ保護と利活用への取り組み。

この中でも１)のインターネットバンキングは、まさに金融情報システムの事象であり、２)、３)、５）も金融情報システムでの事象を含んでいる。

１）のインターネットバンキングへの攻撃に関しては、2013 年 6 月以降不正送金被害が急激に増加した結果、年間被害額が、過去最悪だった 2011 年と比較して、件数で約 8 倍の 1315 件、金額で約 4.6 倍の 14 億 600 万円となった。更に 2014 年上半期は、被害額ベースで、2013 年 1 年間を上回る 18 億 5200 万円となっている（表 33)。更に不正の被害が多くの地方銀行や信用金庫・信用組合に拡大している点や法人名義口座に係る被害が拡大している点も 2014 年上半期の特徴である［警察庁, 2014]。

表 33 インターネットバンキングに係る不正送金［警察庁, 2014]

期間	件数	被害額
2014 年上半期	1,254 件	約 18 億 5200 万円
2013 年下半期	1,098 件	約 11 億 9300 万円
2013 年上半期	217 件	約 2 億 1300 万円

２）の Web 改ざん被害についても、銀行を装ったメールや広告による偽サイトへ誘導するフィッシング詐欺が横行している。

3）のパスワードリスト攻撃についても、ID とパスワードの使い回しをしている利用者が狙われている。漏洩したパスワード等を利用して、利用者のコンピュータを乗っ取り、標的となるコンピュータに DDos 攻撃[38]と呼ばれるサイバー攻撃を仕掛ける懸念もある。

5）の内部者による情報漏洩については 2014 年 2 月に横浜銀行の ATM 保守管理業務の委託先の社員による顧客カード情報の不正取得が発生した点は、記憶に新しい。

このような被害発生に対し、金融機関としても、情報セキュリティに関するルールを変更するなど対応しているが、高度化する攻撃に対しては、専門の CSIRT[39]組織等の組成も必要であり、経営資源を適切に配分する経営判断が生じる。リスクマネジメント戦略の 6 観点では「経営者のコミットメントと支援」及び「IT リスクマネジメント」がより高いレベルで適切に行われることが必要である。また、セキュリティ対応の非機能要件を取込んだ金融情報システム開発を行う必要があり、「要件定義の最適化」にも関係することとなる。

5.4.3. 開発手法・開発組織の多様化

ビジネスの変化の激しさを反映した開発方法の多様化として、ウォーターフォール型開発（P.21 脚注 9）以外の反復型（イテレーション型）開発[40]や、アジャイル型開発（P.92 脚注 31）のニーズが高まっている点である。ウォーターフォール型開発は、日本国内では開発の 96.5%で適用されているとの調査があるが、米国ではウォーターフォール型開発は、13%に過ぎないとの調査結果となっている [独立行政法人情報処理推進機構ソフトウェア・エンジニアリングセンター, 2012c] [独立行政法人情報処理推進機構技術本部ソフトウェア・エンジニアリングセンター, 2012d]。これは、日本では、ユーザー企業がベンダー企業に開発を外部発注する契約形態が主流であるのに対し、米国では、ユーザー企業が主体となる内製化の開発形態が主流であることが、一因であると言われている。ただ、日本でもユーザーニーズの変化の激しいオンライン証券会社等では、ウォーターフォール型ながら、開発サイクルを短期にすることで、変化に柔軟に対応しているケースもある。そ

[38] DDos(Distributed Denial-of-Service)攻撃とは、攻撃者が乗っ取った複数のコンピュータを利用して、集中的に標的コンピュータに処理能力を超える大量のデータを送りつけ、故意に過負荷の状態の陥れる攻撃である。

[39] Computer Security Incident Response Team

[40] ソフトウェアシステムを徐々に開発し、使用可能なシステムを段階的にリリースする開発手法。反復ごとに設計が修正され、新たな機能が追加されていく開発手法。

のような流れを踏まえると、いずれ日本でも非ウォーターフォール型開発のシェアが上昇すると考えられているが、現状では、非ウォーターフォール型開発のリスクマネジメントの標準は必ずしも確立しておらず、その採用にあたっては、経営者の判断を要するとともに、管理にあたっても経営者ないしは、業務部門の開発過程への関与が必要となる。

またプロジェクトメンバーの組織形態の変化もリスクマネジメントでの考慮が必要である。特に一箇所で対面打合せをしながら開発する形態から、ネットワーク接続された遠隔地で、電話会議等も利用しながらも、主として文書ベースでのコミュニケーションによる開発が行われるようになってきた。典型例は、中国をはじめとしたアジア諸国でのオフショア開発である。

このような開発手法や開発組織の多様化に対しては、組織自体の IT ガバナンスが保たれていることが必要であり、リスクマネジメント戦略の 6 観点での「組織体制と IT ガバナンス」及び「IT リスクマネジメント」「品質重視の仕組構築」の項目での対応となるが、より経営者が、自社における各手法のメリットとリスクに関して、十分理解することが重要になると考える。

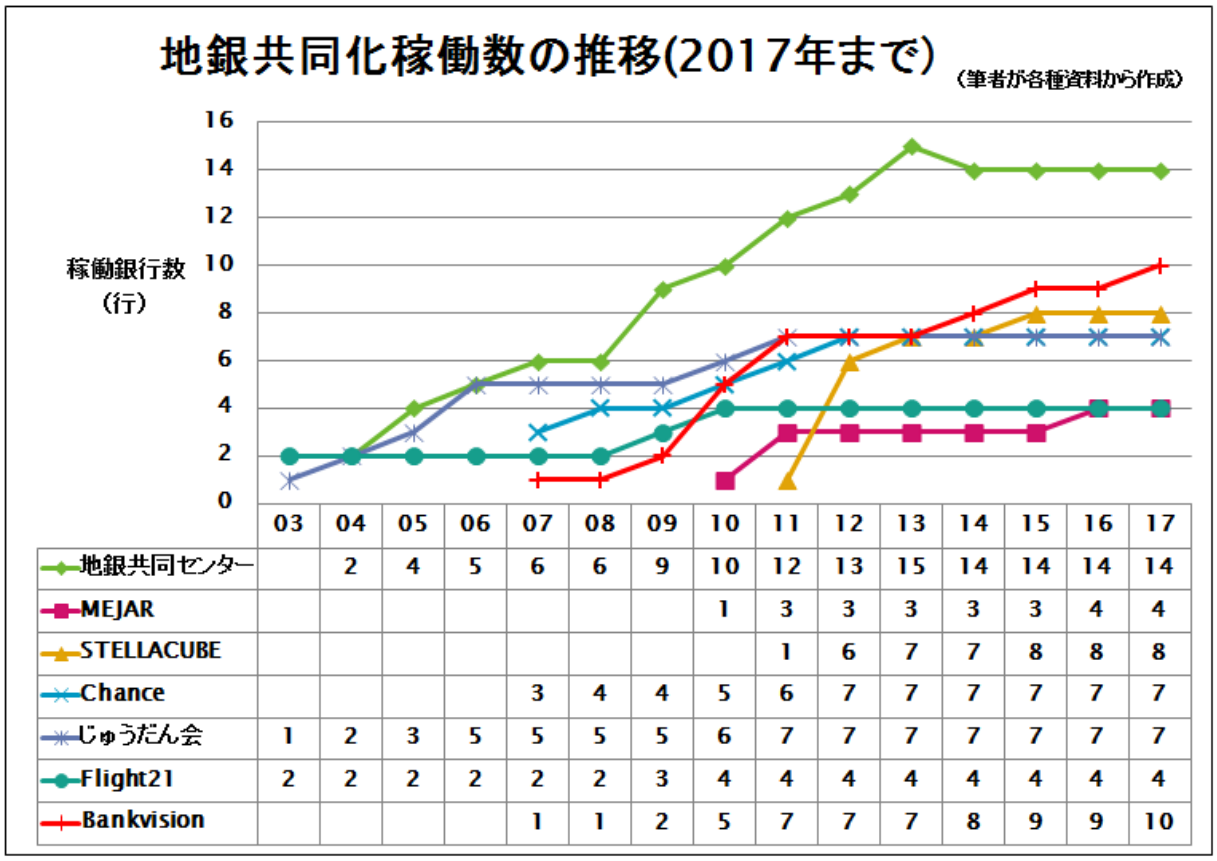
5.4.4. 地域金融機関の共同化[41]

地域金融機関を中心とした、共同化の動きもリスクマネジメント上、考慮が必要である。我が国の地域金融機関の共同化は、1977 年に九州の相互銀行 8 行で稼働した相銀九州共同オンラインセンター（現システムバンキング九州共同センター：ＳＢＫ）に始まる。続いて信用金庫業界の共同化が行われるなど、当初は、中小規模の金融機関の共同化が行われてきた。しかし、1999 年頃になると大手中堅規模の地方銀行を巻き込んだシステム共同化の動きが活発となる。これは、1990 年代後半の金融システム危機の後、都市銀行の再編が進行する中で、地方銀行は地域に根ざした基盤を各々が保有することから、大きな再編は免れたものの、新規 IT 投資の負担の削減が経営課題となったことに呼応したものである。

その中でも、ＮＴＴデータが京都銀行と進めた「地銀共同センター」は、地銀中堅を巻き込んだ 15 行（現在は 14 行）による共同利用型センターとなった。また八十二銀行のシステムを展開する「じゅうだん会」（日本列島を縦断する共同化との趣旨、7 行）、福岡銀

[41] 本項は「地域金融機関における情報システム共同化に関する考察」[遠藤正之、高野研一, 2014b]を元にしている。

行と広島銀行の共同化である「Flight21」(4 行)、三菱東京 UFJ 銀行（当初東京三菱銀行）のシステムを利用する「Chance プロジェクト」(7 行)、日本ユニシスが百五銀行で実現した Windows 上でフルバンキング行う「Bankvision」(8 行)等が続いている（図 27 ご参照）。



	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
地銀共同センター		2	4	5	6	6	9	10	12	13	15	14	14	14	14
MEJAR								1	3	3	3	3	3	4	4
STELLACUBE									1	6	7	7	8	8	8
Chance					3	4	4	5	6	7	7	7	7	7	7
じゅうだん会	1	2	3	5	5	5	5	6	7	7	7	7	7	7	7
Flight21	2	2	2	2	2	2	3	4	4	4	4	4	4	4	4
Bankvision					1	1	2	5	7	7	7	8	9	9	10

図 27 地銀共同化稼働数の推移

2013 年 11 月に日本銀行が実施したアンケートでは、全 105 行の地方銀行第二地方銀行のうち、67%が勘定系システムで共同システムを利用しており、更に今後の稼働予定を含めるとその比率は高まる。

各システム共同化の特徴を表 34 にある通り、より詳細に見てみると、ベンダー主導の共同化（地銀共同センター、STELLACUBE、Bankvision）、メガバンク主導の共同化（Chance）、大手地銀主導の共同化（MEJAR、Flight21）、地銀主導の共同化（じゅうだん会）といった色分けができる。

表 34 各システム共同化の特徴

	ベンダー	特徴	参加行
地銀共同センター	NTTﾃﾞｰﾀ(ﾊｰﾄﾞは日立)	ＮＴＴデータが京都銀行のシステムを元に共同化しているもので、最大勢力	京都、千葉興業、岩手、池田泉州、愛知、青森、北越、福井、秋田、四国、足利、鳥取、西日本シティ、大分
MEJAR	NTTﾃﾞｰﾀ(ﾊｰﾄﾞは富士通)	地銀トップの横浜銀行が主体、2011 年に上位地銀の一角である七十七銀行が参加表明	横浜、北海道、北陸、七十七
STELLACUBE	NTTﾃﾞｰﾀ(ﾊｰﾄﾞは日立)	2008 年 3 月に勘定系パッケージ STAR シリーズ（富士通メインフレーム）の後継として発表	東京都民、富山、但馬、長野、東北、神奈川、仙台、きらやか
Chance	日本 IBM(ｿﾌﾄは銀行)	三菱東京 UFJ 銀行のシステムを地銀に適用するもの。参加行は中位の有力地銀	常陽、百十四、十六、南都、山口、北九州、もみじ
じゅうだん会	日本 IBM(ｿﾌﾄは銀行)	八十二銀行のシステムを共同化するもの	八十二、阿波、山形、武蔵野、琉球、筑波、宮崎
Flight21	日本 IBM	福岡銀行と広島銀行のシステム共同化によるもの	福岡、広島、熊本、親和
Bankvision	日本ﾕﾆｼｽ	百五銀行との共同開発。世界初の Windows フルバンキングである点が画期的	百五、紀陽、山梨中央、鹿児島、スルガ、北國、大垣共立、十八、筑邦、佐賀

また、表 35 に示す通り預金量順に共同化の陣営と稼働時期を分析すると以下の三点が読み取れる。

第一に、ベンダー主導の共同化、地銀主導の共同化、メガバンク主導の共同化が先行してきた。これは経営体力がやや弱い銀行群から共同化が進んだことを示唆している。

第二に、大手地銀 4 行（横浜、千葉、福岡、静岡）は、経営戦略の自由度の高い自営ないしは、自行が主導権を取れる共同化を指向している。ただ、相応の余力があったこともあり、陣営の取組み時期は異なる。まず福岡銀行が、先行して広島銀行との共同化を 2002 年～2003 年に実現し、横浜銀行は 2010 年にようやく勘定系システムのリリースを迎えている。千葉銀行は、新たな共同化スキームとして、日本 IBM と組んで、ゆるやかな連携である「TSUBASA」プロジェクトを主導しているが、勘定系以外のサブシステムでの共同化が先行しており、勘定系システムのリリースは、2016 年となる。また静岡銀行は、長らく自営での運営を進めてきたが、2014 年 1 月に日立製作所が開発するオープン系のプラットフォームで稼働する勘定系システムの採用を決定し、そのパッケージを第二地銀 3 位で今まで自営だった京葉銀行に適用する計画である。

第三に中堅以下の銀行では、共同化を主導するごく少数の言わば「リーダー行」（表 35 下線付）と追随する言わば「フォロワー行」に分かれるが、「フォロワー行」は、概ね「リーダー行」より預金量が小さい銀行である点が見て取れる。

表 35 地銀預金量順の共同化の状況（抜粋）

銀行名	所在地	預金残高 26年3末(億円)	共同化	銀行名	所在地	預金残高 26年3末(億円)	共同化
横浜銀行	神奈川県	118,683	MEJAR(10年1月)	群馬銀行	群馬県	59,853	自営
千葉銀行	千葉県	101,219	TSUBASA(16年)	北陸銀行	富山県	57,120	MEJAR(11年5月)
福岡銀行	福岡県	84,245	Flight21 (02年1月)	中国銀行	岡山県	56,900	TSUBASA(17年)
静岡銀行	静岡県	82,343	自営⇒日立(17年)	十六銀行	岐阜県	50,372	Chance(07年7月)
常陽銀行	茨城県	74,909	Chance(07年1月)	足利銀行	栃木県	49,579	地銀共同センター (11年7月)
七十七銀行	宮城県	71,329	MEJAR(16年)	伊予銀行	愛媛県	48,194	自営
西日本ｼﾃｨ銀行	福岡県	65,166	地銀共同センター (13年1月)	山口銀行	山口県	47,738	Chance(10年5月)
京都銀行	京都府	62,992	地銀共同センター (04年1月)	東邦銀行	福島県	47,245	PROBANK (03年9月)
広島銀行	広島県	61,881	Flight21 (03年1月)	池田泉州銀行	大阪府	46,173	地銀共同センター (05年1月)
八十二銀行	長野県	60,013	じゅうだん会 (02年3月)	南都銀行	奈良県	45,971	Chance(08年5月)

（筆者が各種資料から作成）

21位 百五銀行 三重県 42,351億円 Bankvision(07年5月)

従来の地方銀行の経営は、県毎に営業エリアを棲み分けるビジネスモデルであり、その前提の下、共同化が進んできた。経営判断上のポイントは二つあったと考える。

第一に、共同化は、容易に後戻りができない決定であり、参画の決定要因は、リーダー行やベンダーへの信頼感がベースとなると考えられる。

第二に、システムを共同化するためには、システムのみならず、業務戦略面も開示して、経営戦略をも共有することが必要となるため、競合する銀行とは組むことができないという点である。一例として、北都銀行荘内銀行の経営統合後の共同化の事例がある。秋田県第二位の地銀である北都銀行は、山形県第二位の地銀である荘内銀行と 2009 年に持株会社フィデアホールディングス傘下に経営統合され、荘内銀行が加盟する「地銀共同化センター」への参加を希望したが、秋田銀行（秋田県一位の地銀）に反対され、希望がかなわず、荘内銀行も含めて、新しく「Besta cloud」陣営を作ることとなった。

現在は、地方銀行の経営は厳しさを増しており、その再編の進展は必至の情勢である[42]。特に、県内に複数の地銀が存在するケース等営業エリアが競合する場合に、システム共同化が、経営統合検討時に重要な要素となることが増えるものと思われる。また、システムの老朽化や複雑化によるメンテナビリティの悪さがリスクとなってきており、その点の解消を行いつつ、投資額を抑えるような共同化の動きも増加すると思われる。

このような地方銀行の再編とシステム共同化の取り扱いに関しては、リスクマネジメント戦略の 6 観点での「経営トップのコミットメントと支援」によるものとなるが、「組織体制と IT ガバナンス」及び「IT リスクマネジメント」の観点も重要となる。その際、経営者がいずれの情報システムが自社の将来の経営戦略にとって有効であるかを理解した上で、判断することが必要になると考える。

5.4.5. リスクアペタイト・フレームワーク

リスクアペタイト・フレームワーク（Risk Appetite Framework）は、最近大手金融機関を中心に適用が図られているリスクマネジメント及びガバナンスの考え方である。リスクアペタイトとは、「リスク選好」のことであり、リスクを積極的に取ることを前提にした用語であり、リスクアペタイト・フレームワークは、「経営陣がグループの経営戦略等を踏まえて、進んで受け入れるリスクの水準について対話・理解・評価するためのグループ内共通の枠組み」[金融庁, 2014]と定義される。2013 年の FSB（金融安定理事会）[43]で、金融機関のリスクガバナンス態勢を整備するためのポイントとして、「取締役会の独立性・専門性の確保」、「監査機能の充実」に加えて、「リスクアペタイト・フレームワークの構築」を挙げたことが、注目される契機となった［碓井茂樹, 2014]。

従来のリスクマネジメントと異なる大きな特徴は、以下三点である［大山剛, 2014]。

第一に、リスクのスコープを広く捉える点である。従来は計量化が困難との理由で、取り上げられないこともあった「戦略リスク」や「風評リスク」等を含めたすべてのリスクを取り扱う点である。

---

[42] 2014 年 11 月 4 日には、横浜銀行と東日本銀行、11 月 7 日には、肥後銀行と鹿児島銀行の統合が報道された。いずれも持株会社傘下での統合だが、利用している共同センターが異なるため、いずれ、システム共同化の見直しが発生する可能性を含んでいる。

[43]Financial Stability Board。主要国・地域の中央銀行、金融監督当局、財務省、主要な基準策定主体、IMF（国際通貨基金）、世界銀行、BIS（国際決済銀行）、OECD（経済協力開発機構）等の代表が参加し、金融システムの脆弱性への対応や金融システムの安定を担う当局間の協調の促進に向けた活動を行っている。

第二に、「フォワードルッキング」でのリスク量の把握をする点である。従来のリスクマネジメントが、過去データに基づいて統計的に将来のリスクを予測する形だったのに対し、現状分析の上で、近い将来に起こり得るリスクを予測するというアプローチをとる。その際、組織がリスクテイクすることで、収益を生み出すことが前提となっており、経営者の経営判断のロジックを反映する必要がある。したがって、経営戦略に密接に繋がる概念として、リスクマネジメントを捉えることになる。

第三に、リスクテイク方針の透明化ないし見える化である。リスクテイク方針をステートメントとして定め、関係者間で共有することとなる。金融一般で言えば、格付を維持しうる範囲でリスクテイクして収益力を高める等の方針を定めることが一例である。金融情報システムに関しては、変化の激しい分野では、若干の不具合がある点は覚悟の上で、スピーディーなサービス提供を図るといった方針を定めて、関係者間で共有することが一例である。

日本の金融機関においては、収益管理する部門とリスク管理部門が異なること、経営陣がその判断ロジックの透明化に抵抗することから、まだ実際の運営には困難も予想される。情報システムに関しても、現状では、開発形態がベンダー宛発注型中心であることから、発注者側でのリスクテイクが直接的に行いにくい点もネックとして考えられる。今後は、収益管理部門とリスク管理部門の一体化を進めることや、情報システム部門の内製化を進めることでリスクを取りやすくすること、「取締役会の独立・専門性の確保」に沿った経営と執行の分離により、経営執行の判断ロジックを文書で明記すること等、組織改革、意識改革を進めることが必要であると考える。また、「監査機能の充実」に沿った金融情報システムへの内部監査、外部監査機能の充実も求められる。

以上のリスクアペタイト・フレームワークを金融情報システムのリスクマネジメントに適用する場合、リスクマネジメント戦略の 6 観点での「経営トップのコミットメントと支援」すなわち、金融情報システムのリスクを経営トップが理解し、その上で判断することが重要となる。更にリスク管理部門の位置付けの変化や内製化の進展等、「組織体制と IT ガバナンス」や「IT リスクマネジメント」の観点も重要である。経営者が、リスクと収益性を勘案し、どの情報システムに対して、経営資源をどの程度配分して投資することが、長期的な経営戦略、IT 戦略にとって有効であるかを判断することが必要となると考える。

5.4.6. まとめ

ここまで環境変化の代表例として、クラウド技術、情報セキュリティ環境、開発手法・開発組織の多様化、地域金融機関の共同化、リスクアペタイト・フレームワークを検討し、リスクマネジメント戦略の 6 観点(CORE-OQ)の有効性を確認してきた。それらを表に纏めたのが、表 36 である。

いずれも、より深い経営者の関与が必要とはなるが、リスクマネジメント戦略の 6 観点(CORE-OQ)のスコープ内には入る。リスクマネジメント戦略の 6 観点(CORE-OQ)は、これ以外の環境変化に対しても、柔軟に対応することができる可能性が高いとの示唆が得られた。

表 36 環境変化とリスクマネジメント戦略の 6 観点(CORE-OQ)

環境変化	ﾘｽｸﾏﾈｼﾞﾒﾝﾄ戦略の 6 観点(CORE-OQ)	留意点
クラウド技術	経営者のコミットメントと支援 IT リスクマネジメント	利用には経営者の関与による判断とリスク軽減策の実施が、従来の情報システム導入以上に必要。
情報セキュリティ環境	経営者のコミットメントと支援 IT リスクマネジメント 要件定義の最適化	高度化する攻撃に対しては、専門の CSIRT 組織等の組成も必要であり、経営資源を適切に配分する経営判断が生じる。
開発手法･組織の多様化	組織体制と IT ガバナンス IT リスクマネジメント 品質重視の仕組構築	自社における各手法のメリットとリスクに関して、十分理解することが重要。
地域金融機関の共同化	経営トップのコミットメントと支援 組織体制と IT ガバナンス IT リスクマネジメント	経営者がいずれの情報システムが自社の将来の経営戦略にとって有効であるかを理解した上で、判断することが必要。
リスクアペタイト･フレームワーク	経営トップのコミットメントと支援 組織体制と IT ガバナンス IT リスクマネジメント	経営者が、情報システムのリスクとビジネスの収益性の両面を理解して、判断することが必要。

第6章 結論

6.1. 本研究の結論

第 1 章から第 5 章までの検討考察と評価により、金融事業の経営者に向け、リスクマネジメントの重要な要素を、リスクマネジメント戦略の 6 観点(CORE-OQ)として、経営レベルで集約体系化することができた点が、本研究の貢献である。

すなわち、6 つの観点の中に、経営レベルで重要なリスクマネジメントの要素がすべて包含されていることを、確認することができた。そこで、本研究の結論として、纏めたリスクマネジメント戦略の 6 観点(CORE-OQ)を提示する。

6 観点の項目自体は、3.3 節の記載と、同一であるが、内容には、その後の章での検討を盛り込んで追加している。具体的にはシステム監査関連基準からの示唆、オンライン証券 CIO インタビューからの示唆、環境変化への対応からの示唆を盛り込んだ。

6.1.1. 経営トップのコメットメントと支援（Commitment）

観点 1 は、経営トップのコミットメントと支援（Commitment） である。経営トップが、経営戦略に沿った形での IT 戦略の優先順位を把握決定していき、利用部門と開発部門の間の組織体制を整備し、外部のステークホルダーへの説明責任を果たし、また情報システム開発部門への直接的な関与により、現場の士気を向上させることで、開発と IT 投資の成功に繋げているという点である。

経営トップ（CEO）に求められる具体的な点として、3 点を挙げる。

第一に、経営統合に際して、明確なシステム統合の方針を早期に決断し、業務部門のベクトルを合わせることが重要である。

第二に、攻めの IT 投資に関して、リスクアペタイト・フレームワークの考え方にも沿って、クラウド技術や非ウォーターフォール開発手法のように、有効である反面、新たなリスクをはらむ新技術や開発手法・組織形態を、長期の視点で適切に利用するように CIO を方向づけし、現場の意識を高めることが重要である。

第三に、信頼性確保の IT 投資に関しては、システムの安定性維持や、情報セキュリティに関わる必要な投資や体制確保を行うべく、CIO を支援することが必要である。

6.1.2. 組織体制と IT ガバナンス（Organization）

観点 2 は、適切な組織体制整備による IT ガバナンス強化（「組織体制と IT ガバナンス」）（Organization） である。対象となる情報システム開発に適した全社的組織体制やプロ

ジェクト体制が構築され、システム部門においても開発運用での IT ガバナンスが高い状況に持っていくことである。

この観点については、具体的な事項を 4 点追加して挙げる。

第一に、自社人材の労務管理を行うとともに、長期的な育成計画や将来のロードマップを可視化して、モチベーションを高め、組織全体のスキルすなちインタンジブルズを高めていくことが重要である。

第二に、協力会社であるベンダーのマネジメントについても、よりビジネスに貢献するモチベーションを高める仕掛けを盛り込むことが重要である。

第三に、IT 投資の成果とモニタリングを継続的に行うことで、投資の有効性をフォローする仕掛けを作っていくことが必要である。

第四に、組織の専門化の進展に対し、経営者の直接関与だけでなく、内部監査組織や外部監査人を活用したガバナンスを図ることが必要である。

6.1.3. IT リスクマネジメント（IT Risk Management）

観点 3 は､経営 IT リスクの適切な評価と対策の構築(「IT リスクマネジメント」)(IT Risk Management）である。金融情報システム開発期間に発生可能性のあるリスクや、リリース後に発生可能性のあるリスクについて、開発開始時に広い視野で全般的に純粋リスクを洗い出した上で、純粋リスクの発生確率と影響度合いを分析し、対処の優先順位付けを決めているという点である。更に、適切な対策を立案し実施するとともに、継続的に純粋リスクの状況を管理し続けている点も含まれる。

この観点については、プロジェクトに限定されない、情報システム部門全体ひいては、社内全体での長期的な観点でのリスクマネジメントを 3 点追加する。

第一に、情報セキュリティに関しては、十分な備えが必要である。自社のみで対応できない高度なスキルや情報が必要な場合もあり、業界全体での連携を図ることも必要である。

第二に、新技術や、新開発手法に関しては、メリットを殺さないように留意しながらも、リスクの軽減策を適切に講じていくようなマネジメントが必要となる。

第三に、経営統合等の際のリスクマネジメントについても、統合相手とのコミュニケーションを行い、標準化を早期に行うことが必要である。

6.1.4. 拡張性一貫性確保（Extensibility）

観点４は、経営戦略に合致した業務拡張性及びシステムの一貫性の確保による二重投資の排除（「拡張性一貫性確保」）（Extensibility） である。将来の業務の拡張性やシステムの拡張性を確保できるような設計がなされ、更に将来にわたるシステムの二重投資がないように、金融情報システム全体のグランドデザインの上での位置付けが明確になったうえで、開発を行っているという点である。

この観点については、具体的な事項として以下を追加する。それは、システムの老朽化や複雑化によるメンテナビリティの低下に関しての解決策の検討である。

6.1.5. 要件定義最適化（Optimization）

観点５は、外部関係者の要請と IT のケイパビリティの間をつなぐ要件定義最適化（非機能要件を含む）（「要件定義最適化」）（Optimization） である。経営及び業務部門から出た要件と、現状のシステムで構築可能な仕組みとの組み合わせに関し、業務面とシステム面で検討の上、より焦点を絞ってコストを抑えた形で、効果的な情報システム開発を行っているという点である。

この観点については、具体的な事項として以下を追加する。それは、運用局面も考慮して、情報セキュリティ面やレスポンス等の非機能要件の取込み漏れが無いように、開発の初期の段階で確認する仕掛けを作っておくことが重要であるとの点である。

6.1.6. 品質重視の仕組構築（Quality）

観点６は、品質重視の仕組構築（Quality） である。実際の情報システム開発で、設計品質や開発品質を向上するためのルールや手順の制定や、品質向上のための定期的な会議体や組織体の設置が行われているという点である。

この観点については、以下 3 点を意識した品質確保策の検討を追加する。

第一に開発手法の多様化の意識、

第二にネットワーク型組織やオフショア開発の考慮、

第三に内部監査、外部監査の有効な活用の 3 点である。

6.1.7. CEO と CIO への提言

最後に、金融情報システムに関わっている CEO と CIO への提言を行って、論文全体のまとめとしたい。

6.1.7.1. CEO への提言

CEO については、観点 1「経営トップのコミットメントと支援（Commitment）」と観点 2「組織体制と IT ガバナンス（Organization）」が重点的に実施すべき項目である。特に、以下の 3 点を考慮いただくことが重要であると考える。

第一に、長期的な経営戦略を明示するリーダーシップと、先見性が重要である。これにより、それにマッチした IT 戦略や情報システムのグランドデザインを構築することが可能になる。

第二に、CIO を選任し、攻めの IT 投資、信頼性確保の IT 投資の両面や、人材育成に関して使命付けを行い、経営参画させるなど、支援することが重要である。

第三に、情報システムを意識した、全社組織体制の構築や人材の育成にリーダーシップを発揮することが重要である。

6.1.7.2. CIO への提言

CIO については、観点 2「組織体制と IT ガバナンス（Organization）」、観点 3「IT リスクマネジメント（IT Risk Management）、観点 4「拡張性一貫性確保（Extensibility）」、観点 5「要件定義最適化（Optimization）」、観点 6「品質重視の仕組構築（Quality）」が実施すべき項目であるが、特に以下の 3 点を考慮いただくことが重要であると考える。

第一に、品質面やコスト面といった実務を意識した金融情報システムのポートフォリオマネジメントに関してのリーダーシップが重要である。

第二に、システム部門の組織体制構築とベンダーマネジメントやシステム部門要員のモチベーション向上に関して、リーダーシップを発揮することが重要である。

第三に、CEO と情報システム部門の相互間のコミュニケーションを図り、CEO には、情報システムの現状と将来像を示し、情報システム部門には、長期的な経営戦略の方向性を伝えるようにすることが望まれる。

6.1.7.3. 提言の総括

優れた金融情報システムを構築して、運用するには、相応の年月が必要である。4.2 節で示した東京証券取引所の取組み事例がその一例である。他の経営事項とは異なり、情報システムへの投資は、すぐに経営の成果が目に見えるものではないが、長期的にはその優劣が大きく経営を左右するものであるという点を、改めて認識いただきたいと考える。10

年後、20 年後の組織や社会の変化を考えた長期ビジョンや経営戦略の方向性を示すことで、その戦略と方向性の合致した情報システムを構築、運用することが重要である。またそのような将来像を理解して、組織の情報システムの全体像を俯瞰できる人材を育成することも経営にとって、肝要である。本論文で構築したリスクマネジメント戦略の 6 観点（CORE-OQ）を、経営の一助としていただければ、誠に幸いである。

6.2. 今後に残された課題

本論文の研究で、今後に残された課題として、以下 2 点を挙げる。

第一に、この分野は、今後も継続的なブラッシュアップが必要であるという点である。

前節までで結論付けた、リスクマネジメント戦略の 6 観点(CORE-OQ)は、金融情報システムが置かれた環境変化に柔軟に対応できる抽象度の高いものではあるが、今後も金融と IT の変化は継続するものであり、経営者の関与により、組織運営を最適化することが重要である。ただ、5.4 節で述べたような環境変化の進展や、新たな変化も生じると考えられる。また、大きな経営の枠組みでは、ガバナンスとマネジメントの分離が進み、社外取締役による監視が重視される潮流があり、金融情報システムに関しても、経営者関与の視点について、ガバナンスとマネジメントの両面での検討が必要になることも予想される。結論として、本論文は現時点での最適な体系化ではあるが、今後の環境変化によって絶えず内容をブラッシュアップして行くことが必要であると言える。

第二に、金融情報システムの中で、今回の事例は証券取引所、銀行統合、オンライン証券、地方銀行共同化等限られたものであり、生命保険、損害保険、証券会社（オンライン証券以外)、クレジット信販等の業態は、詳細の検討を行うことができていない。また一事業体のシステム以上に重要な、決済のネットワークである日銀ネット、全銀システムや SWIFT のような国際的決済ネットワークについても十分に検討することができなかった。今後これらについても、視野に入れて検討を行い、研究を継続して参りたいと考える。さらに、その先には、情報システム全般のリスクマネジメントへ理論を拡張していくことも目指したいと考える。

参考文献

（財）金融情報システムセンター. (2014). 『金融機関におけるクラウド利用に関する有識者検討会報告書』. 参照日: 2014 年 11 月 22 日, 参照先: 金融情報システムセンター（FISC): https://www.fisc.or.jp/isolate/?id=759&c=topics&sid=190

（財）金融情報システムセンター. (2011a). 『金融機関等コンピュータシステムの安全対策基準・解説書（第８版）』. 財団法人金融情報システムセンター.

（財）金融情報システムセンター. (2007). 『金融機関等のシステム監査指針第３版』. 財団法人金融情報システムセンター.

（財）金融情報システムセンター. (2010). 『平成 23 年版金融情報システム白書』. 財経詳報社.

（財）金融情報システムセンター. (2011b). 『平成 24 年版金融情報システム白書』. 財経詳報社.

（財）金融情報システムセンター. (2012). 『平成 25 年版金融情報システム白書』. 財経詳報社.

（財）金融情報システムセンター監査安全部. (2011). 「外国為替証拠金取引（ＦＸ）大手会社のオンライン障害にみる安全対策の考察」. 『金融情報システム H23 年冬号』.

（財）金融情報システムセンター監査安全部. (2008). 「新設銀行のシステム障害に関する障害とコンティンジェンシープランに見る安全対策の考察」. 『金融情報システム H20 年冬号』.

（財）金融情報システムセンター調査部. (2010ｂ). 「株式執行市場の多様化と証券サービスの動向」. 『金融情報システム H22 年秋号』.

（財）金融情報システムセンター調査部. (2008). 「金融機関における勘定系システムの現状」. 『金融情報システムH20 年冬号』.

（財）金融情報システムセンター調査部. (2010a). 「金融情報システムの最適化」. 『金融情報システム H22 年冬号』.

（社）日本内部監査協会. (2012). 『IT 監査と IT 統制』. 同文舘出版.

（社）日本内部監査協会. (2007). 『ここから始める IT 監査』. 同文舘出版.

『ISO31000(英和対訳版）』. (2009). (財)日本規格協会.

Banker,R.et al. (2011). “CIO　REPORTING STRUCTURE, STRATEGIC POSITIONING, AND FIRM PERFORMANCE,” . MIS Quarterly, Vol.35 (No.2), pp.487-504.

Barney.J. (2002). “GAINING AND SUSTAINING COMPETITIVE ADVANTAGE,Second Edition”『企業戦略論』ダイヤモンド社. (岡田正大, 訳) Pearson Education,Inc.

Doll,W. (1985). “Avenues for Top Management Involvement in Successful MIS Development,” . MIS Quarterly, Vol.9 (No.1), pp.17-35.

Earl,M. (1993). “Experiences in Strategic Information Systems Planning,”. MIS Quarterly, Vol.17 (No.1), pp.1-24.

IT ガバナンス協会. (2007). 『COBIT4.1 版（日本語版）』. IT ガバナンス協会.

Jarvenpaa,S.and Ives,B. (1991). “Executive Involvement and Participation in the Management of Information Technology,”. MIS Quarterly, Vol.15 (No.2), pp.205-227.

Manfreda,A.and Stemberger,M. (2014). “Factors causing the relationship gap between top management and IS personnel,”. Jounal of Enterprise Information Management, Vol.27 (No.2), pp.107-121.

Masayuki Endo,Kenichi Takano. (2013). “A Study of Project Management of Information Systems in the Financial Sector in Japan”. APCOSEC2013.

Michel Crouhy、Dan Galai、Robert Mark. (2005). “The Essentials of Risk Management”（訳者代表三浦良造『リスクマネジメントの本質』共立出版,2008 年). McGraw-Hill.

Schubert,K. (2004). “CIO Survival Guide” John Wiley & Sons,Inc(『次世代 CIO』). (渡部洋子, 訳）日経 BP ソフトプレス.

Watson, R. (1990). “Influences on the IS Manager's Perceptions of Key Issues: Information Scanning and the Relationship With the CEO,”. MIS Quarterly, Vol.14 (No.2), pp.217-231.

Young, R.and Jordan,M. (2008). “Top management support:Mantra or necessity?,”. International Journal of Project Management, Vol.26, pp.713-725.

システム障害特別調査委員会（委員長　甲斐中辰夫）. (2011). 「調査報告書」.

ピーター・ウェイル、マリアン・ブロードベント. (2003). 『IT ポートフォリオ戦略論』(監訳マイクロソフト株式会社コンサルティング本部）. ダイヤモンド社.

ロブ・ファイヌマン、カイ・ハン・ホー、エードー・ローズ・リンデグレーン、ピート・ベルトマン. (2010). 『IT 監査の基礎と応用』. 中央経済社.

阿部吉伸. (2010). 「カブドットコム証券の IT 経営」『日本システム監査人協会第 159 回月例研究会』講演資料.

安藤正芳. (2007). 「動かないコンピュータ、スルガ銀行」. 『日経コンピュータ 2007 年 1 月 8 日号』, 100-102 頁.

羽川茂雄. (2013). 「地域金融機関における基幹系システムのリスク回避策～事例紹介～」. 『金融情報システム』, H25 (夏).

碓井茂樹. (2014). 「金融機関のリスクガバナンス-変革の潮流」『GMS2014 日本金融監査協会特別講演』. 参照日: 2015 年 1 月 5 日, 参照先: http://goodway.co.jp/fip/doc/gms2014/gms2014_a4.pdf

益田美貴, 高野研一. (2011). 「ビジネスインパクト分析への HAZOP 手法の適用」『安全工学』Vol.50 No.5、pp.292-301. 安全工学会.

益田美貴, 高野研一. (2010). 「金融情報システムへの HAZOP 手法の適用」『安全工学』Vol.49No.2、pp.104-114. 安全工学会.

遠藤正之. (2012). 「金融機関経営者が情報システム開発で果たす役割の一考察」. 『国際戦略経営研究学会第 5 回全国大会報告要旨集』, pp.13-16.

遠藤正之. (2011). 「金融情報システム開発戦略におけるリスクマネジメント」. 中央大学大学院戦略経営研究科研究論文（非公開）.

遠藤正之. (2013). 「金融情報システム障害の再発防止についての一考察」. 『国際戦略経営研究学会第 6 回全国大会（新潟大学）報告要旨集』, pp.93-96.

遠藤正之、高野研一. (2014a). 「金融業の経営戦略実現に向けた情報システム貢献の考察」. 『日本情報経営学会第 68 回大会予稿集』, pp.185-188.

遠藤正之、高野研一. (2013a). 「金融事業経営における情報システム開発のリスクマネジメント観点の提案」. 『日本情報経営学会誌』, Vol.33, (No.3), pp.86-97.

遠藤正之、高野研一. (2013b). 「金融情報システムの開発上流工程におけるシステム監査ポイントの提言」. 『システム監査』, Vol.27 (No.1), pp.13-40.

遠藤正之、高野研一. (2015). 「金融情報システム開発段階での経営者関与とマネジメント戦略に関する考察」. 『日本情報経営学会誌』, Vol.35 (No.2).

遠藤正之、高野研一. (2014ｂ). 「地域金融機関における情報システム共同化に関する考察」. 『日本情報経営学会第 69 回大会予稿集』, pp.191-194.

奥田晃司. (2005). 「ICT と金融システム」（大橋正和、堀眞由美編著『ネットワーク社会経済論-ICT 革命がもたらしたパラダイムシフト-』紀伊國屋書店）.

梶本政利、原田要之助. (2008). 「経営を支える IT の実現に‘COBIT’を生かす」. 『日経コンピュータ 2008 年 10 月 15 日号』, 92-98 頁.

葛谷幸司. (2010). 「大規模システム開発におけるプロジェクト管理の実際」『日本システム監査人協会第 158 回月例研究会』講演資料.

岩佐智仁. (2011). 「システム共同化に関する現状と課題」. 『金融情報システム』, H23 (春).

亀井克之. (2011). 『リスクマネジメントの基礎理論と事例』. 関西大学出版部.

吉田洋平. (2010). 「動かないコンピュータ、ゆうちょ銀行」. 『日経コンピュータ 2010 年 9 月 1 日号』, 92-94 頁.

吉田洋平. (2008). 「動かないコンピュータ、東京証券取引所」. 『日経コンピュータ 2008 年 3 月 1 日号』, 156-158 頁.

吉田隆之. (2013). 「今、求められるセキュリティ人材」『ISACA 東京支部 2013 年 11 月例会』講演資料.

吉武一. (2009). 「情報システム監査」（齋藤正章、蟹江章編著『組織運営と内部監査』放送大学教育振興会）.

久保敏幸. (2013). 「地域金融機関様における勘定系システムへの取り組み事例～課題と方向性～」. 『金融情報システム』, H25 (夏).

宮坂美樹、山本秀男. (2010). 「IT システム統合プログラムのリーダーシップに関する考察」. 『国際プロジェクトプログラムマネジメント学会誌』, 5 (1), pp.103-115.

玉置亮太. (2008). 「動かないコンピュータ、東京金融取引所」. 『日経コンピュータ 2008 年 8 月 15 日号』, 88-90 頁.

金田雅子. (2009). 「金融機関におけるプロジェクト監査への取り組み事例」『日本システム監査人協会第 148 回月例研究会』講演資料.

金融審議会金融分科会基本問題懇談会. (2009). 「今次の金融危機を踏まえたわが国金融システムの構築」. 金融審議会金融分科会基本問題懇談会.

金融庁. (2002). 「システム統合リスク管理態勢の確認検査用チェックリスト」.

金融庁. (2014). 「金融検査マニュアル（預金等受入金融機関に係る検査マニュアル）」.

金融庁. (2014). 「平成 26 事務年度　金融モニタリング基本方針（監督・検査基本方針）」. 参照日: 2015 年 1 月 5 日, 参照先: 金融庁: http://www.fsa.go.jp/news/26/20140911-1/01.pdf

金融庁. (2014 年 7 月). 金融モニタリングレポート. 参照日: 2014 年 11 月 23 日, 参照先: 金融庁報道発表資料: http://www.fsa.go.jp/news/26/20140704-5/01.pdf

栗山敏. (2013). 『情報システムを成功に導く経営者の支援行動』. 白桃書房.

経営情報学会システム統合特設研究部会. (2005). 『成功に導くシステム統合の論点』. 日科技連出版社.

経済産業省. (2010 年 3 月). 「IT 経営ロードマップ改訂版」. 参照日: 2015 年 2 月 8 日, 参照先: 経済産業省 IT 経営ポータル IT 経営協議会:
http://www.meti.go.jp/policy/it_policy/it-keiei/action/conference/roadmap_revised.pdf

経済産業省. (2004). 「システム管理基準」「システム監査基準」.

警察庁. (2014). 「平成 26 年上半期のインターネットバンキングに係る不正送金事犯の発生状況について」. 参照日: 2014 年 11 月 24 日, 参照先: 『広報資料』:
https://www.npa.go.jp/cyber/pdf/H260904_banking.pdf

原田要之助. (2014). 「情報セキュリティマネジメントの変遷と課題」. 『情報セキュリティ総合科学』第 6 号 pp.93-111.

向正道. (2013). 『IT マネジメントの新機軸』. 日経 BP 社.

高井文子. (2006). 「「支配的な通念」による競争と企業間相違形成」. 『日本経営学会誌』, 第 16 号, pp80-94.

高野研一. (2013).「組織ルール､施策の形骸化を防ぐ安全文化の高め方」. 著: (株)技術情報協会,『ヒューマンエラー対策事例集』pp.149-155. 技術情報協会.

根本直子. (2010). 『残る銀行、沈む銀行』. 東洋経済新報社.

根来龍之、経営情報学会. (2010). 『ＣＩＯのための情報・経営戦略－ＩＴと経営の融合』. 中央経済社.

根来龍之、早稲田大学 IT 戦略研究所. (2005). 『デジタル時代の経営戦略』. メディアセレクト.

佐々木良一. (2008). 『IT リスクの考え方』. 岩波書店.

佐々木良一. (2013). 『IT リスク学』. 共立出版.

坂東幸一、田中健次. (2009a). 「金融情報システム事故に関する新聞報道の分析と評価」. 『日本信頼性学会誌』, 31 (1), pp.77-91.

坂東幸一、田中健次. (2009b). 「新聞報道による情報システム事故の信頼性・安全性の分析」. 『日本信頼性学会誌』, 31 (6), pp.412-419.

市嶋洋平. (2008). 「動かないコンピュータ、楽天証券」. 『日経コンピュータ 2008 年 12 月 15 日号』, 108-110 頁.

小池聖一・パウロ他. (2011). 『経営者のための IT ガバナンスの実務』. 中央経済社.

小田利勝. (2007). 『SPSS による統計解析入門』. プレアデス出版.

松原実穂子. (2014). 「2013 年のサイバーセキュリティを振り返って」『ISACA 東京支部 2014 年 1 月例会』講演資料.

松島桂樹. (2007). 『IT 投資マネジメントの発展』. 白桃書房.

松嶋登, 水越康介. (2005). 「制度とビジネス・モデルの革新：松井証券(1)」. 首都大学東京 GBS リサーチペーパー、VB-05-01.

情報処理推進機構ソフトウェア・エンジニアリング・センター. (2008). 『IT プロジェクトの見える化～総集編～』. 日経 BP 社.

森俊也. (2008). 『イノベーション創発の戦略経営論 : 環境認識・トリガーの特定・トリガーの戦略化』. 創成社.

森俊也. (2006). 『大競争時代における銀行組織のマネジメント』. 創成社.

星恒夫. (2013). 「勘定系システム更改の課題と対応　地域金融機関様向けの日本ユニシスの取り組み」. 『金融情報システム』, H25 (夏).

西岡茂樹. (2013). 「企業合併に伴う情報システム統合のリスクに関する考察 : 三銀行の事例分析に基づく」. 『日本情報経営学会誌』, Vol.34 (No.1), pp.52-63.

太田康夫. (2009). 『金融消滅-再規制が生み出す新しい世界』. 日本経済新聞社.

大橋一成、濱田秀夫、隅田慶子. (2001). 「リスクの観点からみた金融統合の効果と影響」.

大橋利夫. (2001). 「金融機関の効率化と IT の役割の変化」. オフィス・オートメーション.

大山剛. (2014). 「リスクアペタイト・フレームワークとは何か」.『企業リスク 2014/07』, pp.68-73.

大山剛. (2013). 「リスクアペタイト・フレームワーク構築の現状」. 『金融財政事情 2013 年 10 月 14 日号』, pp.28-33.

大和田尚孝. (2010a). 「システム共同化加速で進む淘汰」. 『金融ビジネス Summer2010』, 92-93 頁.

大和田尚孝. (2011). 「地域金融機関におけるＩＴソーシング戦略再考」.『金融情報システム』, H23 (春).

大和田尚孝. (2013). 「地域金融機関における勘定系システムの今後」. 『金融情報システム』, H25 (春).

大和田尚孝. (2009a). 「動かないコンピュータ、東京工業品取引所」. 『日経コンピュータ 2009 年 7 月 8 日』, 98-100.

大和田尚孝. (2010b). 『システム改革の正攻法』. 日経 BP 社.

大和田尚孝. (2009b). 『システム統合の「正攻法」』. 日経 BP 社.

大和田尚孝、吉田洋平. (2010a). 「動かないコンピュータ裁判」. 日経コンピュータ 2010 年 1 月 20 日号, 38 頁.

大和田尚孝、中井奨. (2010b). 「トラブルの損失計算式」.『日経コンピュータ 2010 年 3 月 3 日号』, 24-37 頁.

地域金融機関 IT 研究会. (2013). 「地域金融機関における勘定系システムの今後のあり方～勘定系システムの更改問題を中心に～」. 『金融情報システム』, H25 (秋).

池尾和人. (1999). 「戦後日本の金融システムの形成と展開、そして劣化」. 大蔵省財政金融研究所研究部.

池尾和人. (2003). 『銀行はなぜ変われないのか』. 中央公論新社.

池尾和人. (2010). 『現代の金融入門』. 筑摩書房.

池尾和人＋財務省財務総合政策研究所. (2006). 『市場型間接金融の経済分析』. 日本評論社.

中井奨. (2009). 「動かないコンピュータ、アリコジャパン」. 『日経コンピュータ 2009 年 10 月 14 日』, 70-72 頁.

中井奨. (2010a). 「動かないコンピュータ、外為どっとコム」. 『日経コンピュータ 2010 年 10 月 27 日号』, 92-94 頁.

中井奨. (2010b). 「動かないコンピュータその後」.『日経コンピュータ 2010 年 12 月 22 日』, 26-43 頁.

中田敦、大和田尚孝. (2011b). 「みずほ銀障害の全貌　復活の鍵は CIO 人事」. 『日経コンピュータ 2011 年 6 月 9 日号』, 20-27 頁.

中田敦、大和田尚孝. (2011a). 「動かないコンピュータ、みずほ銀行」. 『日経コンピュータ 2011 年 4 月 28 日号』, 38-41 頁.

長谷川建一. (2010). .「ネット証券に見るマーケティングとシステム開発」.『日本情報経営学会誌』, Vol.30 (No.4), pp3-12.

田沢務. (2006). 『金融大統合時代の IT 戦略』. NTT 出版.

渡辺研司. (2005). 「金融ビジネスにおける情報システムリスク・マネジメント体制の構築」. 早稲田大学大学院情報生産システム研究科.

渡邊真治. (2009). 『金融業の情報化と組織に関する経済分析』. 多賀出版.

島田直貴. (2013). 「勘定系システムの課題と今後の方向」. 『金融情報システム』, H25 (春).

島田裕次. (2009). 「IT リスク評価のアプローチ」（堀江正之編著『IT のリスク・統制・監査』同文舘出版）.

湯浦克彦. (2006). 『IT ガバナンスの構造』. エスアイビー・アクセス.

独立行政法人情報処理推進機構. (2014). 「情報セキュリティ上の脅威が事業経営に与える影響」. 参照日: 2014 年 11 月 24 日, 参照先: 『情報処理推進機構情報セキュリティ』: http://www.ipa.go.jp/security/manager/know/meaning/effect.html

独立行政法人情報処理推進機構セキュリティセンター. (2014). 「2014 年版情報セキュリティ 10 大脅威」. 参照日: 2014 年 11 月 24 日, 参照先: 情報処理推進機構情報セキュリティ: http://www.ipa.go.jp/files/000037151.pdf

独立行政法人情報処理推進機構ソフトウェア・エンジニアリング・センター. (2011). 「非ウォーターフォール型開発 WG 活動報告書」. 参照日: 2014 年 11 月 24 日, 参照先: 情報処理推進機構ソフトウェア高信頼化: http://www.ipa.go.jp/files/000004565.pdf

独立行政法人情報処理推進機構ソフトウェア・エンジニアリング・センター(IPA SEC) . (2011). 「重要インフラ情報システムの信頼性向上の取組みガイドブック」. 参照日: 2013 年 11 月 10 日, 参照先: http://sec.ipa.go.jp/reports/20110330.html

独立行政法人情報処理推進機構ソフトウェア・エンジニアリングセンター. (2012c). 『ソフトウェア開発データ白書 2012-2013』. 独立行政法人情報処理推進機構.

独立行政法人情報処理推進機構技術本部セキュリティセンター. (2014). 「情報セキュリティ白書 2014 概要説明資料」. 参照日: 2014 年 11 月 24 日, 参照先: 『情報処理推進機構情報セキュリティ』: http://www.ipa.go.jp/files/000040704.pdf

独立行政法人情報処理推進機構技術本部ソフトウェア・エンジニアリング・センター. (2012a). 「情報システム障害の再発防止のための組織的マネジメントの調査WG報告書」. 参照日: 2013 年 7 月 8 日, 参照先: http://www.ipa.go.jp/files/000004616.pdf

独立行政法人情報処理推進機構技術本部ソフトウェア・エンジニアリング・センター. (2012b). 『「情報管理の取組みに関する調査」調査報告書』. 参照日: 2013 年 7 月 28 日, 参照先: http://www.ipa.go.jp/files/000004667.pdf

独立行政法人情報処理推進機構技術本部ソフトウェア・エンジニアリングセンター. (2012d). 「非ウォーターフォール型開発の普及要因と適用領域の拡大に関する調査調査報告書」. 参照日: 2014 年

11 月 24 日, 参照先: 『情報処理推進機構ソフトウェア高信頼化』:
http://www.ipa.go.jp/files/000004635.pdf
二村敏子. (2004). 『現代ミクロ組織論』. 有斐閣.
日経コンピュータ. (2002). 『システム障害はなぜ起きたかーみずほの教訓』. 日経 BP 社.
日本銀行金融機構局. (2012). 「システム障害管理体制の実効性向上に向けた留意点」. 参照日: 2014 年 7 月 21 日, 参照先: www.boj.or.jp/research/brp/ron_2012/data/ron120216a.pdf
日本銀行金融機構局. (2009). 「金融機関におけるシステム共同化の現状と課題」. 参照日: 2014 年 8 月 17 日, 参照先: http://www.boj.or.jp/research/brp/ron_2009/data/ron0906c.pdf
日本銀行金融機構局. (2010 年 11 月). 「金融機関におけるシステム障害に関するリスク管理の現状と課題」. 参照日: 2014 年 8 月 17 日, 参照先:
http://www.boj.or.jp/research/brp/ron_2010/data/ron1011a.pdf
日本銀行金融機構局. (2007a). 「事例からみたコンピュータ・システム・リスク管理の具体策」. 参照日: 2014 年 8 月 17 日, 参照先: http://www.boj.or.jp/research/brp/ron_2007/data/ron0703a.pdf
日本銀行金融機構局. (2007b). 「地域金融機関におけるシステム・プロジェクト管理の現状について」. 参照日: 2014 年 8 月 17 日, 参照先: http://www.boj.or.jp/research/brp/ron_2007/data/ron0709a.pdf
日本銀行金融機構局. (2014). 「地域金融機関におけるシステム外部委託先管理に関するアンケート（2013 年 11 月）調査結果」. 参照日: 2014 年 8 月 17 日, 参照先:
http://www.boj.or.jp/research/brp/ron_2014/data/ron140331b.pdf
日本型金融システムと行政の将来ビジョン懇話会. (2002). 「金融システムと行政の将来ビジョン」. 参照日: 2014 年 9 月 27 日, 参照先: http://www.fsa.go.jp/news/newsj/13/singi/f-20020712-1.pdf
日本経済新聞. (2011 年 4 月 21 日). 「三菱モルガン 1400 億円赤字」. 『日本経済新聞』4 頁.
日本証券業協会証券教育広報センター、高橋文郎. (2011). 『新・証券市場 2011』. 中央経済社.
日本情報システムユーザー協会. (2012). 「企業の IT 投資動向に関する調査報告書 2012」. 日本システムユーザー協会.
梅本剛正. (2005). 『現代の証券市場と規制』. 商事法務.
富永新. (2009). 『わが国金融機関への期待』. 生産性出版.
福島良治. (2011). 「金融仲介機関のリスク管理とガバナンス」（早稲田大学大学院ファイナンス研究科、首藤惠編著『金融サービスのイノベーションと倫理』中央経済社）.

堀内昭義、花崎正晴. (1998).「なぜ日本は深刻な金融危機を迎えたのか―ガバナンス構造の展望―」.『経済経営研究 Vol. 19, No. 1』.

目次康男. (2009).「動かないコンピュータ、丸三証券」.『日経コンピュータ 2009 年 1 月 1 日号』, 98-100 頁.

野田稔. (2005).『組織論再入門』. ダイヤモンド社.

矢口竜太郎. (2008).「動かないコンピュータ、かんぽ生命保険」.『日経コンピュータ 2008 年 9 月 15 日号』, 12-14 頁.

淀川高喜. (2013).『実践 IT 戦略論』. 日経 BP 社.

鈴木義伯. (2010).「東証新売買システム（arrowhead)の開発経緯について～上流工程の取り組みとその効果～」『日本システム監査人協会第 153 回月例研究会』講演資料.

拝原正人. (2009).『プロマネ失敗学』. 日経 BP 社.

齋藤正章. (2009).「リスクマネジメントと内部監査」（齋藤正章、蟹江章編著『組織運営と内部監査』放送大学教育振興会）.

研究業績

１．定期刊行誌掲載論文（主論文に関連する原著論文）

[１]遠藤正之、高野研一.「金融事業経営における情報システム開発のリスクマネジメント観点の提案」.『日本情報経営学会誌』, Vol.33, (No.3), pp.86-97. (2013 年 5 月).

[２]遠藤正之、高野研一.「金融情報システムの開発上流工程におけるシステム監査ポイントの提言」.『システム監査』, Vol.27 (No.1), pp.13-40. (2013 年 11 月).

[３]遠藤正之、高野研一.「金融情報システム開発段階での経営者関与とマネジメント戦略に関する考察」.『日本情報経営学会誌』, Vol.35 (No.2). (2015 年予定)

２．国際会議論文（査読付きの full-length papers）

[４]Masayuki Endo, Kenichi Takano. “A Study of Project Management of Information Systems in the Financial Sector in Japan”. APCOSEC2013. (2013 年 9 月).

３．国内学会発表

[５]遠藤正之.「金融機関経営者が情報システム開発で果たす役割の一考察」.『国際戦略経営研究学会第 5 回全国大会報告要旨集』, pp.13-16. (2012 年 9 月).

[６]遠藤正之*、高野研一.「金融情報システム開発でのリスクマネジメント観点の一考察」『日本情報経営学会第 65 回全国大会予稿集』, pp.57 -60. (2012 年 10 月).

[７]遠藤正之.「金融情報システム開発局面における経営者のリスクマネジメントの一考察」.『日本経営工学会平成 25 年度春季大会予稿集』, pp.120 -121. (2013 年 5 月).

[８]遠藤正之.「金融情報システム障害の再発防止についての一考察」.『国際戦略経営研究学会第 6 回全国大会（新潟大学）報告要旨集』, pp.93-96. (2013 年 9 月).

[９]遠藤正之*、高野研一.「金融情報システム開発への経営者関与に関わる一考察」.『日本情報経営学会第 67 回全国大会予稿集』, pp. 184-187. (2013 年 9 月).

[10]遠藤正之*、高野研一.「金融業の経営戦略実現に向けた情報システム貢献の考察」.『日本情報経営学会第 68 回全国大会予稿集』, pp.185-188. (2014 年 5 月).

[11]遠藤正之*、高野研一.「地域金融機関における情報システム共同化に関する考察」.『日本情報経営学会第 69 回全国大会予稿集』pp.191 -194. (2014 年 11 月).

謝辞

本博士論文は、多くの方々のご指導、ご支援による研究の成果であります。特に、下記の方々からは一方ならぬご指導、ご支援を賜っており、ここに深く感謝の意を表します。

指導教授であり、本博士論文の主査である、システムデザイン・マネジメント研究科（以下 SDM）の高野研一教授には、後期博士課程入学の相談時から 3 年以上にわたり、研究の方向付けや、論文の構成、記述内容に関するアドバイスまで、懇切丁寧にご指導いただきました。また、投稿する学会の選択や研究支援プログラムへの推薦等、研究活動すべてにわたるご支援をいただきました。

副査を務めていただいた SDM の春山真一郎教授には、ご専門のソフトウェア開発の視点でのご指導を日頃からいただくとともに、本博士論文の重要な論点等の改善点をアドバイスいただき、より独自性が明確になるように改善することができました。

同じく副査を務めていただいた SDM の白坂成功准教授には、有志の開発方法論ゼミでご指導をいただくとともに、本博士論文での論理構成等の見直しに関して、アドバイスいただき、論文の論理性を高めることができました。

学外から副査を引き受けていただいた法政大学イノベーション・マネジメント研究科の石島隆教授は、IT 統制やシステム監査の専門家として、論文に欠けている要素を適確にご指摘賜り、論文の厚みを増すことができました。また、研究開始の契機となる 6 年前の科目履修生時代から、様々の場で、専門家のご紹介や研究内容のご指導を賜りました。

SDM の前野隆司研究科委員長には、CIO インタビューに持参する署名入りのご著書を提供いただく等、様々な局面でご支援いただきました。狼嘉彰顧問、手嶋龍一教授、小木哲朗教授、当麻哲哉准教授、神武直彦准教授、ヒジノ・ケン ビクターレオナード准教授からは、研究発表会の場で、適確なご指摘をいただき、その後の研究に反映することができました。日比谷孟俊顧問からは、公聴会の場で、研究の意義に関して暖かいコメントやアドバイスをいただきました。

西村秀和教授、中野冠教授、谷口智彦教授、保井俊之特別招聘教授、五百木誠准教授、湊宣明准教授らからも、ご指導や励ましの言葉を掛けていただく等ご支援いただきました。

同じ研究室の先輩である東瀬朗助教からは、統計処理方法やアンケート調査全般に関して、大塚有希子氏からは、プロジェクトマネジメントやビジネスアナリシスに関して、一方ならぬご指導やご支援をいただきました。

また SDM の都丸孝之、勝間田実三、佐藤みずほ、佐伯政男、三島邦子、堀越繁明、菅沼貞雄、河村智行、藤原茂樹、木下聡子、西尾未稀、宇野研一、伊藤研一郎、片方恵子、渡邊雅紀、岡本幸久、安部和秀、貴島文緒の諸氏らからは、研究内容や研究の進め方に関して有益なアドバイスや情報をいただくなど、多くの支援をいただきました。

博士共同研究室で机を並べて研究させていただいた方々からも、研究の情報や有形無形の励ましや刺激をいただき、大変心強く研究を進めることができました。

修士（専門職）時の指導教授である、中央大学戦略経営研究科（以下 CBS）の山本秀男研究科長には、修士時代の研究論文に関して丁寧な指導をいただき、後期博士課程進学後も聴講や勉強会でご指導いただき、公聴会でも適確なご指摘をいただきました。CBS では、修士時の副査である河合忠彦教授、杉浦宣彦教授や、藤沼亜起教授、遠山亮子教授、露木恵美子教授、池田唯一客員教授らにもご指導、ご支援をいただきました。また CBS の伊東明、木村剛、松森実、内村光良、近藤亜子、山中理惠、江原伸治、福田貴量、上岡恵子の諸氏らからは研究や学会発表への様々なアドバイスや支援をいただきました。

日本情報経営学会、国際戦略経営研究学会、日本経営工学会での発表に対して、近畿大学の井戸田博樹教授、奈良産業大学の西岡茂樹教授、電気通信大学の由良憲二教授、M&I リサーチの奥田幸治氏、流通経済大学の蜂谷博教授、高崎経済大学の藤本哲教授、多摩大学の原田保教授、早稲田大学の吉見憲二助教、静岡大学の田中宏和教授、明治大学の歌代豊教授、中央大学の丹沢安治教授、リコージャパンの室勝弘氏、青山学院大学の玉木欽也教授、静岡大学の八巻直一教授、早稲田大学の光圀光七郎教授、日揮の佐藤知一氏らから有益な指摘やコメントをいただき、その後の研究へ多くの示唆をいただきました。

日本情報経営学会とシステム監査学会への投稿を査読いただき、適確で丁寧なご指摘ご指導をいただいた、匿名の先生方からも、非常に有益な気付きをいただきました。

長時間の CIO インタビューに応じていただいた東京証券取引所の鈴木義伯様、SBI 証券の岩吉直樹様、カブドットコム証券の阿部吉伸様にも、実際の企業経営をされる立場からの多くの知見をいただきました。

在学中に著者が所属していた三菱東京 UFJ 銀行システム部の関係各位にも業務と研究の両立について、様々なご配慮とご支援をいただきました。

また、本研究は、慶應義塾大学大学院博士課程学生研究支援プログラムによる支援を 3 年連続で受けており、研究支援センターの関係の方々や、様々なご支援をいただいた学生部の皆様、SDM 研究科秘書の皆様にも感謝申し上げます。

ここに書ききれなかった方々にも等しく感謝申し上げます。

最後になりますが、両親や妻の父からも暖かく見守っていただきました。そして、研究者としては先輩でもある妻雪枝に、多くの叱咤激励と配慮をいただいたことを記し、謝辞を締めさせていただきます。

2015 年 2 月

遠藤 正之

別紙1 COBIT4.1版

リスクマネジメント(RM)戦略の6観点…C:経営、Or:組織ガバナンス、R:ITリスク、E:拡張性、Op:要件定義最適化、Q:品質重視
リスクカテゴリー…O:オペレーショナルリスク、B:ビジネスリスク、S:戦略リスク、Re:風評リスク、L:法務・規制リスク
経営者関与ポイント…4点(R):実行責任者、3点(A):説明責任者、2点(C):協議先、1点(I):報告者

COBIT4.1版　コントロール目標	アクティビティ	CEO	CIO	CEO+CIO	RM戦略の6観点	リスクカテゴリー	CFO	企業幹部	ビジネスオーナー	OP責任者	設計責任者	開発責任者	IT管理責任者	PMO	ｺﾝﾌﾟﾗ・監査・ﾘｽｸ・SEC担当	導入チーム	研修部門	ｻｰﾋﾞｽｲﾝｼﾃﾞﾝﾄ構成問題管理担当	取締役会	合計
PO1 IT 戦略計画の策定		11	18	29			7	11	11	10	8	10	8	7	6	0	0	0	0	107
1.1 IT 価値の管理																				
1.2 ビジネスとIT の整合	ビジネス達成目標とIT 達成目標の関連付け	2	4	6	C	B	1	4	2											13
1.3 現在の能力と成果の評価	重要な依存関係および最近の成果の特定	2	4	6	Op	O	2	4	2	2	2	2	2		2					24
1.4 IT 戦略計画	IT 戦略計画の策定	3	4	7	Or	S	2	2	1	2	2	2	2	1	2					23
1.5 IT 実行計画	IT 実行計画の策定	2	3	5	Or	O	1		2	2	2	2	2	4	1					21
1.6 IT ポートフォリオの管理	プログラムポートフォリオの分析と、プロジェクトおよびサービスポートフォリオの管理	2	3	5	E	O	1	1	4	4	2	4	2	2	1					26
PO2 情報アーキテクチャの定義		4	11	15			8	8	10	2	16	12	2	0	13	0	0	0	0	86
2.1 企業の情報アーキテクチャモデル	企業情報モデルの構築と保守		3	3	Or	O	2	1	2		4	2	2		2					18
2.2 企業ﾃﾞｰﾀﾃﾞｨｸｼｮﾅﾘおよびﾃﾞｰﾀ構文規則	企業データディクショナリの構築と保守		1	1	Op	O			2		4	4			2					13
2.3 データ分類体系	データ分類体系の確立と保守	1	2	3	Op	O	2	3	2	1	2	2			4					19
2.4 インテグリティの管理	データオーナに対する情報システム分類手続とツールの提供	1	2	3	Op	O	2	3	2	1	2	2			4					19
	情報モデル、データディクショナリ、および分類スキームを活用した、最適化されたビジネスシステムの計画策定	2	3	5	Op	O	2	1	2		4	2			1					17
PO3 技術指針の決定		0	15	15			5	5	0	9	20	9	4	6	8	0	0	0	0	81
3.1 技術指針計画の策定	技術インフラストラクチャ計画の策定と維持		3	3	E	O	1	1		2	4	2	2		2					17
3.2 技術インフラストラクチャ計画	技術標準の策定と維持		3	3	E	O				2	4	2	1	1	1					14
3.3 将来の動向および規制のモニタリング	技術標準の公開		3	3	E	O	1	1		1	4	1	1	1	1					14
3.4 技術標準	技術進歩に関するモニタリング		3	3	Op	O	1	1		2	4	2		2	2					17
3.5 IT アーキテクチャ委員会	新しい技術の(将来的)(戦略的)使用の定義		3	3	Op	O	2	2		2	4	2		2	2					19
PO4 ITプロセスと組織及びそのかかわりの定義		4	14	18			8	10	5	11	11	8	14	8	8	0	0	0	0	101
4.1 IT プロセスフレームワーク	委員会の設置、利害関係者およびベンダーとのリレーションシップの確立を含む、IT 組織構造の確立	2	3	5	Or	O	2	2		2	2	2	4	2	1					22
4.2 IT 戦略委員会	IT プロセスフレームワークの策定	2	3	5	Or	O	2	2		2	2	2	4	2	2					23
4.3 IT 運営委員会	システムオーナの明確化		3	3	Or	O	2	2	2	4	1	1	1	1	1					18
4.4 組織におけるIT 部門の配置	データオーナの明確化		2	2	Or	O	1	3	2	1	4	1	1	1	2					18
4.5 IT 組織の構造	監督業務および職務の分離を踏まえた、IT 担当者の役割および責任の確立と導入		3	3	Or	O	1	1	1	2	2	2	4	2	2					20
4.6 役割と責任																				
4.7 IT の品質保証の責任																				
4.8 ﾘｽｸ,ｾｷｭﾘﾃｨおよびｺﾝﾌﾟﾗｲｱﾝｽに関する責任																				
4.9 データおよびシステムのオーナシップ																				
4.10 監督																				
4.11 職務の分離																				
4.12 IT スタッフの配置																				
4.13 主要IT 担当者																				
4.14 契約社員に関するポリシーおよび手続																				
4.15 リレーションシップ																				
PO5 IT 投資の管理		7	19	26			12	16	6	6	6	6	8	9	5	0	0	0	0	100
5.1 IT セキュリティの管理	プログラムポートフォリオの維持	3	4	7	E	O	4	4	2					1	1					19
5.2 IT 予算内での優先順位の決定	プロジェクトポートフォリオの維持	1	4	5	E	O	2	4	2		2	2		2	1					20
5.3 IT 予算編成プロセス	サービスポートフォリオの維持	1	4	5	E	O	2	4	2	2				2	1					18
5.4 コスト管理	IT 予算編成プロセスの確立と維持	1	3	4	E	O	2	2		2	2	2	4	2						20
5.5 便益管理	ビジネスにおけるIT 投資、コスト、および価値の特定、周知、およびモニタリング	1	4	5	E	O	2	2		2	2	2	4	2	2					23
PO6 マネジメントの意図と指針の周知		3	12	15			4	3	1	4	2	4	10	0	6	0	0	0	0	49
6.1 IT ポリシーおよび統制環境	IT 統制環境およびフレームワークの構築と維持	1	4	5	Or	O	2	1	1	2		2	2		2					17
6.2 企業のITﾘｽｸおよび内部統制のﾌﾚｰﾑﾜｰｸ	IT ポリシーの策定および保守	1	4	5	Or	O	1	1		2	2	2	4		2					19
6.3 IT ポリシーの管理	IT コントロールフレームワークおよびIT 目標と指針の周知	1	4	5	Or	O	1	1					4		2					13
6.4 ポリシーの展開				0																0
6.5 IT 目標と指針の周知				0																0
PO7 IT 人材の管理		0	6	6			2	0	0	6	6	6	8	6	2	0	0	0	0	42
7.1 要員の募集および保持	IT スキル、職位定義書、給与支払い区分、個人的な業績ベンチマークの特定		3	3	Or	O	2			2	2	2	4	2						17
7.2 要員の能力	IT 人材に関する人事ポリシーおよび手続の実施(募集、採用、調査、報酬、研修、評価、昇進、および解雇)		3	3	Or	O				4	4	4	4	4	2					25
7.3 役割に応じた人材配置				0																0
7.4 要員の研修				0																0
7.5 個人に対する依存				0																0
7.6 要員の人事認可手続				0																0
7.7 従業員の業績評価				0																0
7.8 職務の変更および解雇				0																0
PO8 品質管理		3	20	23			2	3	5	9	9	9	9	9	10	0	0	0	0	88
8.1 品質管理システム	品質管理システムの定義	2	4	6	Q	O		2	1	1	1	1	1	1	2					16
8.2 IT IT 標準および品質の実践基準	品質管理システムの確立と維持	1	4	5	Q	O	1	1	1	2	2	2	2	2	2					20
8.3 開発および調達標準	品質標準の策定と組織全体への周知		4	4	Q	O	1		1	2	2	2	2	2	2					18
8.4 顧客中心	継続的改善に向けた品質計画の策定および管理		4	4	Q	O			1	2	2	2	2	2	2					17
8.5 継続的改善	品質目標へのコンプライアンス状況の測定、モニタリング、およびレビュー		4	4	Q	O			1	2	2	2	2	2	2					17
8.6 品質の測定,ﾓﾆﾀﾘﾝｸﾞ,およびﾚﾋﾞｭｰ				0																0
PO9 IT リスクの評価と管理		10	28	38			14	14	33	26	19	19	19	2	17	0	0	0	0	201
9.1 ITﾘｽｸﾏﾈｼﾞﾒﾝﾄとﾋﾞｼﾞﾈｽﾘｽｸﾏﾈｼﾞﾒﾝﾄの整合	リスクマネジメントの整合性に関する判断(リスクの評価など)	3	2	5	R	O	4	2	4	1					1					17
9.2 リスクをめぐる状況の明確化	関連する戦略的ビジネス目標の理解		4	4	R	O	2	2	2	2					1					13
9.3 イベントの特定	関連するビジネスプロセス目標の理解		2	2	R	O			2	4					1					9
9.4 リスク評価	社内のIT 目標の特定とリスク背景の明確化		4	4	R	O			4		2	2	2		1					15
9.5 リスクへの対応	目標に関連するイベントの特定[イベントの一部はビジネス指向(ビジネスはA)、一部はIT 指向(IT はA、ビジネスはC)	1	3	4	R	O			3	4	4	4	4		2					25
9.6 リスク対応実行計画の維持およびモニタリング	イベントに関連するリスクの評価		3	3	R	O			3	4	4	4	4		2					24
	リスク対応策の評価	1	3	4	R	O	1	3	3	4	4	4	4		2					29
	コントロールに関するアクティビティの優先順位付けおよび計画	2	3	5	R	O	2	3	4	4	2	2	2		2					26
	リスク対応実行計画の承認および資金の確保			0	R	O	3	3	4	1	1	1	1		1					15
	リスク対応実行計画の維持およびモニタリング	3	4	7	R	O	2	1	4	2	2	2	2	2	4					28
PO10 プロジェクト管理		5	22	27			4	13	5	8	8	9	6	26	14	0	0	0	0	120
10.1 プログラム管理フレームワーク	IT 投資のためのプログラム/ポートフォリオ管理フレームワークの定義	2	4	6	Or	O	2	3						2	2					15
10.2 プロジェクト管理フレームワーク	IT プロジェクト管理フレームワークの確立と維持	1	4	5	Or	O	1	1	1	2	2	2	2	4	2					22
10.3 プロジェクト管理のアプローチ	IT プロジェクトのモニタリング、測定および管理システムの確立と維持	1	4	5	Or	O	1	1		2	2	2	2	4	2					21
10.4 利害関係者の関与	ﾌﾟﾛｼﾞｪｸﾄ憲章,日程,品質計画,予算,ｺﾐｭﾆｹｰｼｮﾝ管理計画,及びﾘｽｸﾏﾈｼﾞﾒﾝﾄ計画の作成		2	2	Or	O		2	2	2	2	2	2	4	2					20
10.5 プロジェクト範囲の記述	プロジェクトの利害関係者の協力および関与の確保	1	4	5	Or	O		3	2					4	2					16
10.6 プロジェクトの各フェーズの開始	プロジェクトおよびプロジェクトに関する変更の効果的なコントロールの保証		2	2	Or	O		2		2	2	2		4	2					16
10.7 統合プロジェクト計画	プロジェクトの保証およびレビュー方法の定義と導入		2	2	Or	O		1				1		4	2					10
10.8 プロジェクトの資源				0																0
10.9 プロジェクトのリスクマネジメント				0																0

別紙1 COBIT4.1版

リスクマネジメント(RM)戦略の6観点…C:経営、Or:組織ガバナンス、R:ITリスク、E:拡張性、Op:要件定義最適化、Q:品質重視
リスクカテゴリー…O:オペレーショナルリスク、B:ビジネスリスク、S:戦略リスク、Re:風評リスク、L:法務・規制リスク
経営者関与ポイント…4点(R):実行責任者、3点(A):説明責任者、2点(C):協議先、1点(I):報告者

COBIT4.1版　コントロール目標	アクティビティ	CEO	CIO	CEO+CIO	RM戦略の6観点	リスクカテゴリー	CFO	企業幹部	ビジネスオーナー	OP責任者	設計責任者	開発責任者	IT管理責任者	PMO	コンプラ・監査・リスク・SEC担当	導入チーム	研修部門	サービスインシデント構成問題管理担当	取締役会	合計
10.10 プロジェクトの品質計画				0																0
10.11 プロジェクト変更コントロール				0																0
10.12 保証方法に関するプロジェクト計画				0																0
10.13 プロジェクトの成果の測定、報告、およびモニタリング				0																0
10.14 プロジェクトの終了				0																0
AI1 コンピュータ化対応策の明確化		0	27	27			3	24	20	17	15	19	2	32	11	0	0	0	0	170
1.1 ビジネスの機能的および技術的要件の定義と保守	ビジネスの機能的および技術的要件の定義		2	2	Op	O		2	4	2	4	4		4	1					23
1.2 リスク分析報告	要件のインテグリティ/通用性を目指したプロセスの確立		2	2	Op	O				2		2		4	2					12
1.3 実現可能性調査および代替対応策の策定	ビジネスプロセスリスクの特定、文書化、および分析		4	4	R	O		4	4	4	2	4		4	2					28
1.4 要件および実現可能性の決定および承認	提案されたビジネス要件の導入に関する実現可能性調査/影響評価の実施		4	4	Op	O		4	4	2	2	2		4	2					24
	提案されたソリューションにおけるIT 運用便益の評価		4	4	E	O	1	4	4	1	1	1		4						20
	提案されたソリューションにおけるビジネス便益の評価		4	4	E	O		4		2	2	2	1	4						19
	要件承認プロセスの作成		3	3	Op	O		2		2	2	2		4	2					17
	提案されたソリューションの承認		4	4	Op	O	2	4	4	2	2	2	1	4	2					27
AI2 アプリケーションソフトウェアの調達と保守		0	3	3			0	0	9	6	8	23	2	24	12	0	0	0	0	87
2.1 概要設計	ビジネス要件の概要設計仕様への変換			0	Op	O			2		2	4		4	2					14
2.2 詳細設計	詳細設計およびソフトウェアアプリケーションの技術的要件の策定		2	2	Op	O			2	2	2	4		4	2					18
2.3 業務処理統制および可監査性	設計における業務処理統制の組み込み			0	E	O			4	2		4		4	4					18
2.4 アプリケーションのセキュリティおよび可用性	調達した自動化機能のカスタマイズおよび導入			0	ー	O			2	2		4		4	2					14
2.5 調達したｱﾌﾟﾘｹｰｼｮﾝｿﾌﾄｳｪｱの構成および導入	アプリケーション開発プロセスの管理に関する正式化された方法論およびプロセスの策定		1	1	Or	O				2	2	3	2	4	2					16
2.6 既存システムの大幅なアップグレード	プロジェクトのソフトウェア品質保証計画の策定			0	Q	O			1		2	4		4	2					13
2.7 アプリケーションソフトウェアの開発	アプリケーション要件の追跡および管理			0	Q	O						4		4						8
2.8 ソフトウェアの品質保証	ソフトウェアアプリケーションの保守計画の策定		1	1	ー	O				2		4		2						9
2.9 アプリケーション要件の管理				0																0
2.10 アプリケーションソフトウェアの保守				0																0
AI3 技術インフラストラクチャの調達と保守		0	9	9			4	0	1	10	8	8	10	0	2	0	0	0	0	52
3.1 技術インフラストラクチャの調達計画	調達手続/プロセスの定義		3	3	Or	O	2			2	2	2	4		1					16
3.2 インフラストラクチャ資源の保護と可用性	インフラストラクチャの要件について承認済みのベンダーと協議		3	3	Or	O	2		1	4	2	2	4		1					19
3.3 インフラストラクチャの保守	インフラストラクチャの保守に関する戦略および計画の策定		3	3	Or	O				4	4	4	2							17
3.4 実現可能性テスト環境	インフラストラクチャコンポーネントを構成		3	3	ー	O				4	2				1					10
AI4 運用と利用の促進		0	5	5			0	0	6	4	0	4	0	0	1	6	6	0	0	32
4.1 運用上のソリューションの計画	ソリューションを運用可能にする戦略の作成		3	3	Op	O			3	4		4			1	4	2			21
4.2 ビジネス部門の管理者への知識の移転	知識移転の方法論の作成		2	2	E	O			3							2	4			11
4.3 エンドユーザへの知識の移転	エンドユーザ向けの手続マニュアルの作成			0	ー	O			4			4			2	2				12
4.4 運用ｽﾀｯﾌおよびｻﾎﾟｰﾄｽﾀｯﾌへの知識の浸透	運用スタッフおよびサポートスタッフ向けの技術サポート文書の作成			0	ー	O				4		2			2					8
	研修の整備と実施			0	ー	O			3	3		4					4			14
	研修結果の評価と必要に応じた文書の改訂			0	ー	O			3	3						4	4			14
AI5 IT 資源の調達		7	9	16			6	0	0	9	1	9	16	4	6	0	0	0	0	67
5.1 調達のコントロール	会社レベルの調達ポリシーと整合されたIT 調達ポリシーおよび手続の策定	1	3	4	Or	O	2			1	1	1	4		2					15
5.2 サービスプロバイダとの契約の管理	認可されたサービスプロバイダのリストの作成/保守			0	Or	O							4							4
5.3 サービスプロバイダの選定	提案依頼(RFP)プロセスを使用したサービスプロバイダの評価および選定	2	3	5	Or	O	2			4		4	4	4	2					25
5.4IT 資源の調達	組織の利益を保護する契約の策定	4	3	7	Or	O	2			4		4	4		2					23
	確立された手続を遵守した調達		3	3	ー	O				4		4	4		2					17
AI6 変更管理		0	3	3			0	0	1	4	2	4	2	2	2	0	0	0	0	20
6.1 変更の標準と手続	変更要求の一貫した記録、評価、優先順位付けのための仕組みの策定および導入		3	3	Or	O			1	4	2	4	2	2	2					20
6.2 影響評価、優先順位付け、および認可	ビジネス上の必要性に基づく変更の影響評価および優先順位付け		1	1	ー	O			4	4	2	4	2	4	2					23
6.3 緊急変更	緊急変更や重要な変更の実施における、承認されたプロセスの遵守		1	1	ー	O			1	4	1	4			2					13
6.4 変更の状況追跡および報告	変更の承認		1	1	ー	O			2	4		4								11
6.5 変更の終了および文書化	変更の関連情報の管理と周知		3	3	ー	O			1	4	2	4	1	4	2					21
AI7 ソリューションおよびその変更の導入と認定				0																0
7.1 研修	導入計画の策定とレビュー		3	3	ー	O		2	1	2	2	4		2	2					18
7.2 テスト計画	テスト戦略(開始基準と終了基準)および運用テストの計画策定方法の確立およびレビュー		3	3	ー	O		2	2	2	2	4		2	2					19
7.3 導入計画	ビジネス要件および技術的要件のリポジトリと認定されたシステムのテストケースの作成と保守		3	3	ー	O						4								7
7.4 テスト環境	テスト環境におけるシステムの変換テストと統合テストの実施		1	1	ー	O		1	4	2	2	4		1	2					17
7.5 システムおよびデータの変換	テスト環境の準備および最終受け入れテストの実施		1	1	ー	O		1	4	3	2	4		1	2					18
7.6 変更のテスト	合意された認定基準に基づいた本番環境への移行の推奨		4	4	ー	O		1	3	4	2	4		1	2					21
7.7 最終受け入れテスト				0		O														0
7.8 本番環境への移行				0		O														0
7.9 導入後レビュー				0		O														0
DS1 サービスレベルの定義と管理		0	3	3			0	2	2	2	1	2	2	1	2	0	0	4	0	21
1.1 サービスレベル管理フレームワーク	IT サービス定義のためのフレームワークの策定		3	3	Or	O		2	2	2	1	2	2	1	2			4		21
1.2 サービスの定義	IT サービスカタログの作成		3	3	ー	O		1	2	2	1	2	2	1	1			4		19
1.3 サービスレベル・アグリーメント	重要なIT サービスについてのSLA の定義		2	2	ー	O	1	1	2	4	1	4	4	2	2			4		27
1.4 オペレーショナルレベル・アグリーメント	SLA 履行のためのOLA の定義		1	1	ー	O			2	4	1	4	4	2	2			4		24
1.5 サービスレベル達成状況のモニタリングと報告	包括的なサービスレベル成果のモニタリングと報告		1	1	ー	O			1	4		1	1		1			4		13
1.6 ｻｰﾋﾞｽﾚﾍﾞﾙ・ｱｸﾞﾘｰﾒﾝﾄおよび請負契約の見直し	SLA とその請負契約の見直し		1	1	ー	O	1		2	4		4	4		2			4		22
	IT サービスカタログの見直しと更新		3	3	ー	O		1	2	2	1	2	2	1	1			4		19
	サービス改善計画の策定		3	3	ー	O		1	1	4	1	4	2	2	1			4		23
DS2 サードパーティのサービスの管理		0	10	10			5	0	5	14	3	14	15	8	8	0	0	0	0	82
2.1 すべてのｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞとのﾘﾚｰｼｮﾝｼｯﾌﾟの特定	サードパーティとのサービスのリレーションシップの特定と分類		1	1	Or	O			2	4	2	4	3	2	2					20
2.2 サービスプロバイダとのリレーションシップの管理	サービスプロバイダの管理プロセスの定義と文書化		3	3	Or	O	2		1	4	1	4	4	2	2					23
2.3 サービスプロバイダにかかわるリスクの管理	サービスプロバイダの評価および選定に関するポリシーと手続の確立		3	3	Or	O	2		2	2		2	4	2	2					19
2.4 サービスプロバイダの成果のモニタリング	サービスプロバイダにかかわるリスクの特定、評価および低減		3	3	Or	O	1			4		4	4	2	2					20
	サービスプロバイダからのサービス提供状況のモニタリング		4	4	ー	O			3	4		4	4	2	2					23
	すべての利害関係者に対するサービスのリレーションシップの長期的達成目標の評価	2	4	6	ー	O	2	2	2	2	2	2	4	2	2					26
DS3 性能とキャパシティの管理		0	11	11			0	0	5	20	4	12	10	9	3	0	0	0	0	74
3.1 性能とキャパシティの計画策定	IT 資源の性能とキャパシティのレビューに関する計画策定プロセスの確立		3	3	Or	O				4	2	2	2	2						15
3.2 現状の性能とキャパシティ	IT 資源の現行の性能とキャパシティのレビュー		2	2	Op	O			1	4		2	2	2						13
3.3 将来の性能とキャパシティ	IT 資源の性能とキャパシティの予測		2	2	Op	O			2	4	2	2	2	2						16
3.4 IT 資源の可用性	IT 資源に関する不適合を特定するギャップ分析の実施		2	2	Op	O			1	4		4	2	2	1					16
3.5 モニタリングと報告	IT 資源が利用不能になる潜在的リスクに備えた緊急時対応計画の策定		2	2	R	O			1	4		2	2	1	2					14
	IT 資源の可用性、性能とキャパシティの継続的なモニタリングと報告		1	1	ー	O			1	4		1	1	1	1					10
DS4 継続的なサービスの保証		0	5	5			4	4	4	8	6	6	4	4	6	0	0	0	0	51
4.1 IT 継続フレームワーク	IT 継続フレームワークの作成		3	3	Or	O	2	2	2	4	4	4	2	2	4					29

別紙1 COBIT4.1版

リスクマネジメント（RM)戦略の6観点…C：経営、Or：組織ガバナンス、R：ITリスク、E：拡張性、Op:要件定義最適化、Q：品質重視
リスクカテゴリー…O：オペレーショナルリスク、B：ビジネスリスク、S：戦略リスク、Re：風評リスク、L：法務・規制リスク
経営者関与ポイント…4点（R)：実行責任者、3点（A)：説明責任者、2点（C)：協議先、1点（I)：報告者

COBIT4.1版　コントロール目標	アクティビティ	CEO	CIO	CEO+CIO	RM戦略の6観点	リスクカテゴリー	CFO	企業幹部	ビジネスオーナー	OP責任者	設計責任者	開発責任者	IT管理責任者	PMO	コンプラ・監査・リスク・SEC担当	導入チーム	研修部門	サービスインシデント構成問題管理担当	取締役会	合計
4.2 IT 継続計画	事業影響分析とリスク評価の実施		2	2	R	O	2	2	2	4	2	2	2	2	2					22
4.3 重要なIT 資源	IT 継続計画の策定と保守	1	2	3	—	O	2	2	1	4		2	2	2	2					20
4.4 IT 継続計画の保守	復旧目標に基づくIT 資源の特定と分類		2	2	—	O				4		2	1	2	1					12
4.5 IT 継続計画のテスト	IT 継続計画を常に最新の状態で維持するための変更管理手続の策定と実施		1	1	—	O				4		4	4	4	1					18
4.6 IT 継続計画に関する研修	IT 継続計画の定期的なテスト		1	1	—	O			1	4		2	2	1	1					12
4.7 IT 継続計画の配付	テスト結果に基づく追加対応計画の作成		2	2	—	O			1	4	2	4	4	4	1					22
4.8 IT サービスの復旧および再開	IT 継続計画に関する訓練の計画と実施		1	1	—	O			4	4		2	4	1	1					17
4.9 遠隔地におけるバックアップ保管施設	IT サービスの復旧と再開の計画策定		2	2	—	O	1	1	2	4	2	4	4	4	2					26
4.10 再開後のレビュー	バックアップの保管と保護に関する計画の策定と実施		1	1	—	O				4		2	2	1	1					11
	再開後のレビュー実施手続の確立		2	2	—	O			1	4		2	2		2					13
DS5 システムセキュリティの保証		1	9	10			2	3	5	10	8	5	1	1	10	0	0	0	0	55
5.1 IT 財務管理フレームワーク	IT セキュリティ計画の定義と維持	1	3	4	R	O	2	2	2	2	2	2	1	1	4					22
5.2 IT セキュリティ計画	ID(アカウント)管理プロセスの定義・作成・運用		3	3	R	O		1	2	4	4	1			2					17
5.3 ID 管理	潜在的および実際のセキュリティインシデントのモニタリング		3	3	R	O			1	4	2	2			4					16
5.4 ユーザアカウントの管理	ユーザのアクセス権・特権の定期的見直しと確認		1	1	—	O			3	2					4					10
5.5 セキュリティのテスト、監視、モニタリング	暗号鍵の保持・保護のための手続作成と改訂		3	3	—	O				4			1		2					10
5.6 セキュリティインシデントの定義	ネットワーク間の情報フローを保護する技術的・手続的なコントロールの導入・維持		3	3	—	O			2	2	4	4			2					17
5.7 セキュリティ技術の保護	定期的な脆弱性評価の実施		3	3	—	O	1		1	2	2	2			4					15
5.8 暗号鍵の管理				0		O														0
5.9 不正ソフトウェアの阻止、発見、および是正				0		O														0
5.10 ネットワークのセキュリティ				0		O														0
5.11 機密データの交換				0		O														0
DS6 コストの捕捉と配賦		0	12	12			8	6	6	8	8	8	16	8	0	0	0	0	0	80
6.1 サービスの定義	提供サービス/サポートされているビジネスプロセスへのIT インフラストラクチャの対応付け		3	3	E	O	2	2	2	2	2	2	4	2						21
6.2 IT 財務管理	すべてのIT費用(要員的費用,技術的費用など)の特定と,これらの費用のITサービスへの単位原価での対応付け		3	3	E	O	2			2	2	2	4	2						17
6.3 コストモデルの策定とコスト請求	IT 会計および原価管理のプロセスの確立と保守		3	3	E	O	2	2	2	2	2	2	4	2						21
6.4 コストモデルの保守	課金に関するポリシーと手続の確立と保守		3	3	E	O	2	2	2	2	2	2	4	2						21
DS7 利用者の教育と研修		0	3	3			0	2	4	2	2	2	2	2	2	0	4	0	0	25
7.1 教育と研修のニーズの特定	ユーザの研修ニーズの特定とその分析		3	3	Op	O		2	4	2	2	2	2	2	2		4			25
7.2 教育と研修の実施	研修プログラムの作成		3	3	—	O		2	4	2	1	2	2	2	1		4			23
7.3 受講研修内容の評価	啓蒙活動と教育研修の実施		3	3	—	O		1	2	2	1	2	2	2	1		4			20
	研修評価の実施		3	3	—	O		1	4	2	1	2	2	2	1		4			22
	最良の研修実施方法およびツールの特定と評価		4	4	—	O		1	4	2	2	2	2	2	2		4			25
DS8 サービスデスクとインシデントの管理				0																0
8.1 サービスデスク	分類(重大度と影響力)とエスカレーション(機能と階層)の手続の作成		2	2	—	O			2	2	2	2	2		2			4		18
8.2 顧客からの問い合わせの登録	インシデント/サービス要求/情報要求の発見と記録			0	—	O												4		4
8.3 インシデントエスカレーション	問い合わせの分類、調査、および診断		1	1	—	O				2	2	2			1			4		12
8.4 インシデントのクローズ	インシデントの解決、回復、およびクローズ			0	—	O			1	4	4	4			2			4		19
8.5 傾向分析	ユーザへの通知(最新の進行状況など)		1	1	—	O			1									4		6
	マネジメントレポートの作成	1	1	2	—	O			1	1			1		1			4		10
DS9 構成管理				0																0
9.1 構成リポジトリとベースライン	構成管理の計画策定手続の作成			0	—	O			2	3	2	1	2		2			4		16
9.2 構成管理アイテムの特定と管理	初期構成情報の収集とベースラインの確立			0	—	O				2	2	2			1			4		11
9.3 構成のインテグリティのレビュー	構成情報の検証と監査(未承認ソフトウェアの発見を含む)			0	—	O	1			3			1		1			4		10
	構成管理用リポジトリの更新			0	—	O				4	4	4			1			4		17
DS10 問題管理				0																0
10.1 問題の特定と分類	問題の特定と分類		1	1	—	O		1	2	3	2	2			1			4		16
10.2 問題の追跡と解決	根本原因の分析の実施			0	—	O				2		2						4		8
10.3 問題のクローズ	問題の解決			0	—	O			2	3	4	4		4	2			2		21
10.4 変更管理、構成管理、および問題管理の統合	問題の状況の確認		1	1	—	O		1	2	4	2	2		2	2			4		20
	改善のための提案事項の提示と関連する変更要求の作成			0	—	O			1	3	1	1		1				4		11
	問題の記録保持			0	—	O			1	1		1			1			4		8
DS11 データ管理				0																0
11.1 データ管理におけるビジネス要件	データの保管と保持に関する要件を取り入れた手続の定義		3	3	—	O			1	2	4				2					12
11.2 データの保管および保持の調整	メディアライブラリの管理手続の定義、維持、および導入		3	3	—	O				4	2	2	1		2					14
11.3 メディアライブラリ管理システム	メディアと機器の安全な廃棄手続の定義、保守、および導入		3	3	—	O			2	4			1		2					12
11.4 廃棄	計画に基づくデータのバックアップ		3	3	—	O				4										7
11.5 バックアップと復元	データ復元のための手続の定義、維持、および導入		3	3	—	O			2	4	2	2			1					14
11.6 データ管理におけるセキュリティ上の要件				0		O														0
DS12 物理的環境の管理		1	2	3			2	2	2	4	2	0	2	2	2	0	0	0	0	21
12.1 サイトの選定と配置	要求される物理的保護レベルの定義			0	—	O			2	4	2				2					10
12.2 物理的なセキュリティ対策	サイト(データセンター、オフィスなど)の選定と委託	1	2	3	Or	O	2	2	2	4	2		2	2	2					21
12.3 物理的アクセス	物理的環境に関する対策の実施			0	—	O			1	4	1	1			2					9
12.4 環境的要因からの保護	物理的環境の管理(保守、モニタリング、報告を含む)			0	—	O				4	2									6
12.5 物理的施設の管理	物理的アクセスを許可および維持する手続の定義と導入		2	2	—	O			1	4	1	1	1		2					12
DS13 オペレーション管理				0																0
13.1 オペレーション手続と指示	オペレーション手続(マニュアル、チェックリスト、シフト交代計画、引き継ぎ文書、エスカレーション手続など)の定義/変更			0	—	O				4					1					5
13.2 業務のスケジュール策定	作業負荷とバッチジョブのスケジュール策定			0	—	O			2	4	2	2								10
13.3 IT インフラストラクチャのモニタリング	インフラストラクチャと処理のモニタリングおよび問題の解決			0	—	O				4					1					5
13.4 機密文書と出力デバイス	物理アウトプット(紙、メディアなど)の管理と保護			0	—	O				4					2					6
13.5 ハードウェアの予防的保守	スケジュールとインフラストラクチャへの修正または変更の適用			0	—	O			2	4	2	2			2					12
	認証デバイスを侵害、損失、盗難から保護するためのプロセスの導入/確立		3	3	—	O				4			1		2					10
	予防的保守のスケジュール策定と実施			0	—	O				4										4
ME1 IT 成果のモニタリングと評価				0																0
1.1 モニタリングアプローチ	モニタリングアプローチの確立	3	4	7	—	O	4	2	1	2	1	2	1		2					22
1.2 モニタリングデータの定義と収集	ビジネス目標をサポートする測定可能な目標の特定と収集	2	3	5	—	O	2	2	4	4		4								21
1.3 モニタリング方法	スコアカードの作成		3	3	—	O				4	2	4	2							15
1.4 成果評価	成果の評価		3	3	—	O		1	4	4	2	4	2							20
1.5 取締役会およびマネジメント層への報告	成果の報告	1	3	4	—	O	1	4	4	4	2	4	2		1					26
1.6 是正措置	成果改善策の明確化とモニタリング		3	3	—	O			4	4	2	4	2		2					21
ME2 内部統制のモニタリングと評価				0																0
2.1 内部統制フレームワークのモニタリング	IT 内部統制活動のモニタリングとコントロール		3	3	—	O				4		4	4		4					19
2.2 監督レビュー	セルフ評価プロセスのモニタリング		3	3	—	O		1		4		4	4		2					18
2.3 コントロール例外事項	独立したレビュー、監査、および検査の成果のモニタリング		3	3	—	O		1		4		4	4		2					18

別紙1 COBIT4.1版

リスクマネジメント(RM)戦略の6観点…C:経営、Or:組織ガバナンス、R:ITリスク、E:拡張性、Op:要件定義最適化、Q:品質重視
リスクカテゴリー…O:オペレーショナルリスク、B:ビジネスリスク、S:戦略リスク、Re:風評リスク、L:法務・規制リスク
経営者関与ポイント…4点(R):実行責任者、3点(A):説明責任者、2点(C):協議先、1点(I):報告者

COBIT4.1版　コントロール目標	アクティビティ	CEO	CIO	CEO+CIO	RM戦略の6観点	リスクカテゴリー	CFO	企業幹部	ビジネスオーナー	OP責任者	設計責任者	開発責任者	IT管理責任者	PMO	コンプラ・監査・リスク・SEC担当	導入チーム	研修部門	サービスインシデント構成問題管理担当	取締役会	合計
2.4 コントロールセルフ評価	サードパーティによるコントロールの確実性を保証するためのプロセスのモニタリング	1	3	4	―	O	1	1		4		4	4		2					20
2.5 内部統制の保証	コントロールの例外事項を特定し、評価するためのプロセスのモニタリング	1	3	4	―	O	1	1	1	4		4	4		2					21
2.6 サードパーティにおける内部統制	コントロールの例外事項を特定し、是正するためのプロセスのモニタリング	1	3	4	―	O	1	1	1	4		4	4		2					21
2.7 是正措置	主要な利害関係者への報告	1	4	5	―	O	1	1							1					8
ME3 外部要件に対するコンプライアンスの保証		0	4	4			0	0	2	1	1	1	2	1	4	0	0	0	0	16
3.1 外部法規制、および契約のコンプライアンス要件の特定	法律、契約、政策、および規制上の要件を特定するプロセスの策定と実行		4	4	R	L			2	1	1	1	2	1	4					16
3.2 外部要件への対応の最適化	IT のポリシー、標準、および手続に対するIT アクティビティのコンプライアンスの評価	1	4	5	―	O	1	1	1	4	4	4	4	4	4				1	33
3.3 外部要件に対するコンプライアンスの評価	IT のポリシー、標準、および手続に対するIT アクティビティのコンプライアンスの積極的な保証に関する報告		4	4	―	O			2	2	2	2	2	2	4					20
3.4 コンプライアンスの積極的な保証	コンプライアンス要件に応じて、IT のポリシー、計画、および手続を整合するインプットの提供		4	4	―	O			2	2	2	2	2		4					18
3.5 報告の統合	法的要件に関するIT 部門の報告と、その他のビジネス部門からの類似報告との統合		4	4	―	O				1	1	1	4	1	4					16
ME4 IT ガバナンスの提供		18	14	32			9	7	2	3	3	3	3	3	14	0	0	0	0	79
4.1 IT ガバナンスフレームワークの確立	経営層と取締役会によるIT アクティビティに対する監督と推進の確立	4	2	6	Or	O	2	2							2					12
4.2 戦略との整合	IT 成果、IT 戦略、資源とリスクの管理のビジネス戦略との整合、レビュー、承認、および周知	4	4	8	Or	S	1	1							2					12
4.3 価値の提供	成果、およびポリシー、計画、手続へのコンプライアンスに関する独立した定期評価の実施	4	2	6	Or	O	2	1		1	1	1	1	1	4					18
4.4 資源の管理	独立した評価による検出事項の解決、およびマネジメント層による合意された改善案の確実な実施	4	2	6	Or	O	2	1		1	1	1	1	1	4					18
4.5 リスクの管理	IT ガバナンス報告の作成	2	4	6	Or	O	2	2	2	1	1	1	1	1	2					19
4.6 成果の測定																				0
4.7 独立した保証																				0

別紙2 システム管理基準

リスクマネジメント（RM）戦略の6観点…C：経営、Or：組織ガバナンス、R：ITリスク、E：拡張性、Op:要件定義最適化、Q：品質重視
リスクカテゴリー…O：オペレーショナルリスク、B：ビジネスリスク、S：戦略リスク、Re：風評リスク、L：法務・規制リスク
4点（R):実行責任者、3点（A):説明責任者、2点（C）：協議先、1点（I）：報告者

システム管理基準	CEO	CIO	CEO+CIO	CFO	企業幹部	RM戦略の6観点	リスクカテゴリー
Ⅰ．情報戦略(47)							
1．全体最適化（18）	7	11	18	6	9		
1.1 全体最適化の方針・目標（6）	4	4	8	2	2	C	S
(1)ITガバナンスの方針を明確にすること。							
(2)情報化投資及び情報化構想の決定における原則を定めること。							
(3)情報システム全体の最適化目標を経営戦略に基づいて設定すること。							
(4)組織体全体の情報システムのあるべき姿を明確にすること。							
(5)システム化によって生ずる組織及び業務の変更の方針を明確にすること。							
(6)情報セキュリティ基本方針を明確にすること。							
1.2 全体最適化計画の承認（3）	2	4	6	2	4	Or	O
(1)全体最適化計画の立案体制は、組織体の長の承認を得ること。							
(2)全体最適化計画は、組織体の長の承認を得ること。							
(3)全体最適化計画は、利害関係者の合意を得ること。							
1.3 全体最適化計画の策定（7）	1	3	4	2	3	Or	S
(1)全体最適化計画は、方針及び目標に基づいていること。							
(2)全体最適化計画は、コンプライアンスを考慮すること。							
(3)全体最適化計画は、情報化投資の方針及び確保すべき経営資源を明確にすること。							
(4)全体最適化計画は、投資効果及びリスク算定の方法を明確にすること。							
(5)全体最適化計画は、システム構築及び運用のための標準化及び品質方針を含めたルールを明確にすること。							
(6)全体最適化計画は、個別の開発計画の優先順位及び順位付けのルールを明確にすること。							
(7)全体最適化計画は、外部資源の活用を考慮すること。							
1.4 全体最適化計画の運用（2）	1	3	4	1	1	－	O
(1)全体最適化計画は、関係者に周知徹底すること。							
(2)全体最適化計画は、定期的及び経営環境等の変化に対応して見直すこと。							
2．組織体制（9）	6	11	17	4	3		
2.1 情報システム化委員会（5）	2	3	5	2	2	Or	S
(1)全体最適化計画に基づき、委員会の使命を明確にし、適切な権限及び責任を与えること。							
(2)委員会は、組織体における情報システムに関する活動全般について、モニタリングを実施し、必要に応じて是正措置を講じること。							
(3)委員会は、情報技術の動向に対応するため、技術採用指針を明確にすること。							
(4)委員会は、活動内容を組織体の長に報告すること。							
(5)委員会は、意思決定を支援するための情報を組織体の長に提供すること。							
2.2 情報システム部門（2）	2	4	6	1		Or	O
(1)情報システム部門の使命を明確にし、適切な権限及び責任を与えること。							
(2)情報システム部門は、組織体規模及び特性に応じて、職務の分離、専門化、権限付与、外部委託等を考慮した体制にすること。							
2.3 人的資源管理の方針（2）	2	4	6	1	1	Or	O
(1)情報技術に関する人的資源の現状及び必要とされる人材を明確にすること。							
(2)人的資源の調達及び育成の方針を明確にすること。							
3．情報化投資（6）	2	4	6	4	4	E	O
(1)情報化投資計画は、経営戦略との整合性を考慮して策定すること。							
(2)情報化投資計画の決定に際して、影響、効果、期間、実現性等の観点から複数の選択肢を検討すること。							
(3)情報化投資に関する予算を適切に執行すること。							
(4)情報化投資に関する投資効果の算出方法を明確にすること。							
(5)情報システムの全体的な業績及び個別のプロジェクトの業績を財務的な観点から評価し、問題点に対して対策を講じること。							
(6)投資した費用が適正に使用されたことを確認すること。							
4．情報資産管理の方針（4）	1	3	4	2		Op	O
(1)情報資産の管理方針及び体制を明確にすること。							
(2)情報資産のリスク分析を行い、その対応策を考慮すること。							
(3)情報資産の効率的で有効な活用を考慮すること。							
(4)情報資産の共有化による生産性向上を考慮すること。							
5．事業継続計画（5）	2	4	6	2	4	R	O
(1)情報システムに関連した事業継続の方針を策定すること。							
(2)事業継続計画は、利害関係者を含んだ組織的体制で立案し、組織体の長が承認すること。							
(3)事業継続計画は、従業員の教育訓練の方針を明確にすること。							
(4)事業継続計画は、関係各部に周知徹底すること。							
(5)事業継続計画は、必要に応じて見直すこと。							
6．コンプライアンス（5）	2	2	4	2	4	R	L
(1)法令及び規範の管理体制を確立するとともに、管理責任者を定めること。							
(2)遵守すべき法令及び規範を識別し、関係者に教育及び周知徹底すること。							
(3)情報倫理規程を定め、関係者に教育及び周知徹底すること。							
(4)個人情報の取扱い、知的財産権の保護、外部へのデータ提供等に関する方針を定めること。							
(5)法令、規範及び情報倫理規程の遵守状況を評価し、改善のために必要な方策を講じること。							
Ⅱ．企画業務(23)							
1．開発計画（9）	2	3	5	2	3	Op	O
(1)開発計画は、組織体の長が承認すること。							
(2)開発計画は、全体最適化計画との整合性を考慮して策定すること。							
(3)開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果等を明確にすること。							
(4)開発計画は、関係者の教育及び訓練計画を明確にすること。							
(5)開発計画は、ユーザ部門及び情報システム部門の役割分担を明確にすること。							
(6)開発計画は、開発、運用及び保守の費用の算出基礎を明確にすること。							
(7)開発計画はシステムライフを設定する条件を明確にすること。							
(8)開発計画の策定に当たっては、システム特性及び開発の規模を考慮して形態及び開発方法を決定すること。							
(9)開発計画の策定に当たっては、情報システムの目的を達成する実現可能な代替案を作成し、検討すること。							
2．分析（8）	1	3	4		3	Op	O
(1)開発計画に基づいた要求定義は、ユーザ、開発、運用及び保守の責任者が承認すること。							
(2)ユーザニーズの調査は、対象、範囲及び方法を明確にすること。							
(3)実務に精通しているユーザ、開発、運用及び保守の担当者が参画して現状分析を行うこと。							
(4)ユーザニーズは文書化し、ユーザ部門が確認すること。							
(5)情報システムの導入に伴って発生する可能性のあるリスク分析を実施すること。							
(6)情報システムの導入によって影響を受ける業務、管理体制、諸規程等は、見直し等の検討を行うこと。							
(7)情報システムの導入効果の定量的及び定性的評価を行うこと。							
(8)パッケージソフトウェアの使用に当たっては、ユーザニーズとの適合性を検討すること。							
3．調達（6）	1	3	4	2	2	E	O
(1)調達の要求事項は、開発計画及びユーザニーズに基づき作成し、ユーザ、開発、運用及び保守の責任者が承認すること。							
(2)ソフトウェア、ハードウェア及びネットワークは、調達の要求事項を基に選択すること。							
(3)開発を遂行するために必要な要員、予算、設備、期間等を確保すること。							
(4)要員に必要なスキルを明確にすること。							
(5)ソフトウェア、ハードウェア及びネットワークの調達は、ルールに従って実施すること。							
(6)調達した資源は、ルールに従って管理すること。							
Ⅲ．開発業務（49）							
1．開発手順（4）		2	2		1	Op	O

別紙2 システム管理基準

リスクマネジメント（RM）戦略の6観点…C：経営、Or：組織ガバナンス、R：ITリスク、E：拡張性、Op:要件定義最適化、Q：品質重視
リスクカテゴリー…O：オペレーショナルリスク、B：ビジネスリスク、S：戦略リスク、Re：風評リスク、L：法務・規制リスク
4点（R):実行責任者、3点（A):説明責任者、2点（C）：協議先、1点（I）：報告者

システム管理基準	CEO	CIO	CEO・CIO	CFO	企業幹部	RM戦略の6観点	リスクカテゴリー
(1)開発手順は、開発の責任者が承認すること。							
(2)開発手順は、開発方法に基づいて作成すること。							
(3)開発手順は、開発の規模、システム特性等を考慮して決定すること。							
(4)開発時のリスクを評価し、必要な対応策を講じること。							
2．システム設計（15）		2	2		1	Op	O
(1)システム設計書は、ユーザ、開発、運用及び保守の責任者が承認すること。							
(2)運用及び保守の基本方針を定めて設計すること。							
(3)入出力画面、入出力帳票等はユーザの利便性を考慮して設計すること。							
(4)データベースは、業務の内容及びシステム特性に応じて設計すること。							
(5)データのインテグリティを確保すること。							
(6)ネットワークは、業務の内容及びシステム特性に応じて設計すること。							
(7)情報システムの性能は、要求定義を満たすこと。							
(8)情報システムの運用性及び保守性を考慮して設計すること。							
(9)他の情報システムとの整合性を考慮して設計すること。							
(10)情報システムの障害対策を考慮して設計すること。							
(11)誤謬防止、不正防止、機密保護等を考慮して設計すること。							
(12)テスト計画は、目的、範囲、方法、スケジュール等を明確にすること。							
(13)情報システムの利用に係る教育の方針、スケジュール等を明確にすること。							
(14)モニタリング機能を考慮して設計すること。							
(15)システム設計書をレビューすること。							
3．プログラム設計（5）		1	1			ー	O
(1)プログラム設計書は、開発の責任者が承認すること。							
(2)システム設計書に基づいて、プログラムを設計すること。							
(3)テスト要求事項を定義し、文書化すること。							
(4)プログラム設計書及びテスト要求事項をレビューすること。							
(5)プログラム設計時に発見したシステム設計の矛盾は、システム設計の再検討を行って解決すること。							
4．プログラミング（4）		1	1			ー	O
(1)プログラム設計書に基づいてプログラミングすること。							
(2)プログラムコードはコーディング標準に適合していること。							
(3)プログラムコード及びプログラムテスト結果を評価し、記録及び保管すること。							
(4)重要プログラムは、プログラム作成者以外の者がテストすること。							
5．システムテスト・ユーザ受入れテスト（13）		2	2		2	ー	O
(1)システムテスト計画は、開発及びテストの責任者が承認すること。							
(2)ユーザ受入れテスト計画は、ユーザ及び開発の責任者が承認すること。							
(3)システムテストに当たっては、システム要求事項を網羅してテストケースを設定して行うこと。							
(4)テストデータの作成及びシステムテストは、テスト計画に基づいて行うこと。							
(5)システムテストは、本番環境と隔離された環境で行うこと。							
(6)システムテストは、開発当事者以外の者が参画すること。							
(7) システムテストは、適切なテスト手法及び標準を使用すること。							
(8)ユーザ受入れテストは、本番同様の環境を設定すること。							
(9)ユーザ受入れテストは、ユーザマニュアルに従い、本番運用を想定したテストケースを設定して実施すること。							
(10)ユーザ受入れテストは、ユーザ及び運用の担当者もテストに参画して確認すること。							
(11)システムテスト及びユーザ受入れテストの結果は、ユーザ、開発、運用及び保守の責任者が承認すること。							
(12)システムテスト及びユーザ受入れテストの経過及び結果を記録及び保管すること。							
(13)パッケージソフトウェアを調達する場合、開発元が品質テストを実施したことを確認すること。							
6．移行（8）		2	2		2	ー	O
(1)移行計画を策定し、ユーザ、開発、運用及び保守の責任者が承認すること。							
(2)移行作業は文書に記録し、責任者が承認すること。							
(3)移行完了の検証方法を移行計画で明確にすること。							
(4)移行計画に基づいて、移行に必要な要員、予算、設備等を確保すること。							
(5)移行は手順書を作成し、実施すること。							
(6)移行時のリスク対策を検討すること。							
(7)運用及び保守に必要なドキュメント、各種ツール等は開発の責任者から引き継いでいること。							
(8)移行は関係者に周知徹底すること。							
Ⅳ．運用業務（73）							
1．運用管理ルール（4）		1	1			ー	O
(1)運用管理ルール及び運用手順は、運用の責任者が承認すること。							
(2)運用管理ルールは、運用設計に基づいて作成すること。							
(3)運用手順は、運用設計及び運用管理ルールに基づいて、規模、期間、システム特性等を考慮して作成すること。							
(4)運用設計及び運用管理ルールに基づいて、担当責任者を定めること。							
2．運用管理（16）		1	1		1	ー	O
(1)年間運用計画を策定し、責任者が承認すること。							
(2)年間運用計画に基づいて、月次、日次等の運用計画を策定すること。							
(3)運用管理ルールを遵守すること。							
(4)ジョブスケジュールは、業務処理の優先度を考慮して設定すること。							
(5)オペレーションは、ジョブスケジュール及び指示書に基づいて行うこと。							
(6)例外処理のオペレーションは、運用管理ルールに基づいて行うこと。							
(7)オペレータの交替は、運用管理ルールに基づいて行うこと。							
(8)ジョブスケジュール及びオペレーション実施記録を採り、ジョブスケジュールとの差異分析を行うこと。							
(9)オペレーション実施記録は、運用管理ルールに基づいて一定期間保管すること。							
(10)事故及び障害の影響度に応じた報告体制及び対応手順を明確にすること。							
(11)事故及び障害の内容を記録し、情報システムの運用の責任者に報告すること。							
(12)事故及び障害の原因を究明し、再発防止の措置を講じること。							
(13)情報システムのユーザに対する支援体制を確立すること。							
(14)情報セキュリティに関する教育及び訓練をユーザに対して実施すること。							
(15)情報システムの稼動に関するモニタリング体制を確立すること。							
(16)情報システムの稼動実績を把握し、性能管理及び資源の有効利用を図ること。							
3．入力管理（5）		1	1			ー	O
(1)入力管理ルールを定め、遵守すること。							
(2)データの入力は、入力管理ルールに基づいて漏れなく、重複なく、正確に行うこと。							
(3)入力データの作成手順、取扱い等は誤謬防止、不正防止、機密保護等の対策を講じること。							
(4)データの入力の誤謬防止、不正防止、機密保護等の対策は有効に機能すること。							
(5)入力データの保管及び廃棄は、入力管理ルールに基づいて行うこと。							
4．データ管理（10）		1	1			ー	O
(1)データ管理ルールを定め、遵守すること。							
(2)データへのアクセスコントロール及びモニタリングは、有効に機能すること。							
(3)データのインテグリティを維持すること。							
(4)データの利用状況を記録し、定期的に分析すること。							
(5)データのバックアップの範囲、方法及びタイミングは、業務内容、処理形態及びリカバリの方法を考慮して決定すること。							
(6)データの授受は、データ管理ルールに基づいて行うこと。							

別紙2 システム管理基準

リスクマネジメント（RM）戦略の6観点…C：経営、Or：組織ガバナンス、R：ITリスク、E：拡張性、Op:要件定義最適化、Q：品質重視
リスクカテゴリー…O：オペレーショナルリスク、B：ビジネスリスク、S：戦略リスク、Re：風評リスク、L：法務・規制リスク
4点（R):実行責任者、3点（A):説明責任者、2点（C）：協議先、1点（I）：報告者

システム管理基準	CEO	CIO	CEO+CIO	CFO	企業幹部	RM戦略の6観点	リスクカテゴリー
(7)データの交換は、不正防止及び機密保護の対策を講じること。							
(8)データの保管、複写及び廃棄は、誤謬防止、不正防止及び機密保護の対策を講じること。							
(9)データに対するコンピュータウイルス対策を講じること。							
(10)データの知的財産権を管理すること。							
5. 出力管理（7）		1	1			ー	O
(1)出力管理ルールを定め、遵守すること。							
(2)出力情報は、漏れなく、重複なく、正確であることを確認すること。							
(3)出力情報の作成手順、取扱い等は、誤謬防止、不正防止及び機密保護の対策を講じること。							
(4)出力情報の引渡しは、出力管理ルールに基づいて行うこと。							
(5)出力情報の保管及び廃棄は、出力管理ルールに基づいて行うこと。							
(6)出力情報のエラー状況を記録し、定期的に分析すること。							
(7)出力情報の利用状況を記録し、定期的に分析すること。							
6. ソフトウェア管理（9）		1	1			ー	O
(1)ソフトウェア管理ルールを定め、遵守すること。							
(2)ソフトウェアへのアクセスコントロール及びモニタリングは、有効に機能すること。							
(3)ソフトウェアの利用状況を記録し、定期的に分析すること。							
(4)ソフトウェアのバックアップの範囲、方法及びタイミングは、業務内容及び処理形態を考慮して決定すること。							
(5)ソフトウェアの授受は、ソフトウェア管理ルールに基づいて行うこと。							
(6)ソフトウェアの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。							
(7)ソフトウェアに対するコンピュータウイルス対策を講じること。							
(8)ソフトウェアの知的財産権を管理すること。							
(9)フリーソフトウェアの利用に関し、組織体としての方針を明確にすること。							
7. ハードウェア管理（6）		1	1			ー	O
(1)ハードウェア管理ルールを定め、遵守すること。							
(2)ハードウェアは、想定されるリスクに対応できる環境に設置すること。							
(3)ハードウェアは、定期的に保守を行うこと。							
(4)ハードウェアは、障害対策を講じること。							
(5)ハードウェアの利用状況を記録し、定期的に分析すること。							
(6)ハードウェアの保管、移設及び廃棄は、不正防止及び機密保護の対策を講じること。							
8. ネットワーク管理（6）		1	1			ー	O
(1)ネットワーク管理ルールを定め、遵守すること。							
(2)ネットワークへのアクセスコントロール及びモニタリングは、有効に機能すること。							
(3)ネットワーク監視ログを定期的に分析すること。							
(4)ネットワークは、障害対策を講じること。							
(5)ネットワークの利用状況を記録し、定期的に分析すること。							
(6)ネットワークを利用したサービスについて、組織体としての方針を明確にすること。							
9. 構成管理（4）		1	1			ー	O
(1)管理すべきソフトウェア、ハードウェア及びネットワークの対象範囲を明確にし、管理すること。							
(2)ソフトウェア、ハードウェア及びネットワークの構成、調達先、サポート条件等を明確にすること。							
(3)ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、影響を受ける範囲を検討して決定すること。							
(4)ソフトウェア、ハードウェア及びネットワークの導入並びに変更は、計画的に実施すること。							
10. 建物・関連設備管理（6）		1	1			ー	O
(1)建物及び関連設備は、想定されるリスクに対応できる環境に設置すること。							
(2)建物及び室への入退の管理は、不正防止及び機密保護の対策を講じること。							
(3)関連設備は、適切な運用を行うこと。							
(4)関連設備は、定期的に保守を行うこと。							
(5)関連設備は、障害対策を講じること。							
(6)建物及び室への入退の管理を記録し、定期的に分析すること。							
Ⅴ. 保守業務（19）							
1. 保守手順（3）		1	1		1	ー	O
(1)保守ルール及び保守手順は、保守の責任者が承認すること。							
(2)保守手順は、保守の規模、期間、システム特性等を考慮して決定すること。							
(3)保守時のリスクを評価し、必要な対応策を講じること。							
2. 保守計画（3）		2	2		2	ー	O
(1)保守計画はユーザ及び保守の責任者が承認すること。							
(2)変更依頼等に対し、保守の内容及び影響範囲の調査並びに分析を行うこと。							
(3)保守のテスト計画は、目的、範囲、方法、スケジュール等を明確にすること。							
3. 保守の実施（3）		1	1		1	ー	O
(1)システム設計書、プログラム設計書等は、保守計画に基づいて変更し、ユーザ及び保守の責任者が承認すること。							
(2)プログラムの変更は、保守手順に基づき、保守の責任者の承認を得て実施すること。							
(3)変更したプログラム設計書に基づいてプログラミングしていることを検証すること。							
4. 保守の確認（5）		1	1		1	ー	O
(1)変更したプログラムのテストの実施は、保守のテスト計画に基づいて行うこと。							
(2)変更したプログラムは、影響範囲を考慮してテストを行うこと。							
(3)変更したプログラムのテストは、ユーザが参画し、ユーザマニュアルに基づいて実施すること。							
(4)変更したプログラムのテストの結果は、ユーザ、運用及び保守の責任者が承認すること。							
(5)変更したプログラムのテストの結果を記録及び保管すること。							
5. 移行（3）		1	1		1	ー	O
(1)移行手順は、移行の条件を考慮して作成すること。							
(2)変更前のプログラム及びデータのバックアップを行うこと。							
(3)運用及び保守の責任者は、他の情報システムへ影響を与えないことを確認すること。							
6. 情報システムの廃棄（2）		1	1		1	ー	O
(1)旧情報システムは、リスクを考慮して廃棄計画を策定し、ユーザ、運用及び保守の責任者の承認を得て廃棄すること。							
(2)旧情報システムの廃棄方法及び廃棄時期は、不正防止及び機密保護の対策を考慮して決定すること。							
Ⅵ. 共通業務（76）							
1. ドキュメント管理（9）	0	2	2	0	2		
1.1 作成（5）		1	1		1	Or	O
(1)ドキュメントは、ユーザ部門及び情報システム部門の責任者が承認すること。							
(2)ドキュメント作成ルールを定め、遵守すること。							
(3)ドキュメントの作成計画を策定すること。							
(4)ドキュメントの種類、目的、作成方法等を明確にすること。							
(5)ドキュメントは、作成計画に基づいて作成すること。							
1.2 管理（4）		1	1		1	Or	O
(1)ドキュメントの更新内容は、ユーザ部門及び情報システム部門の責任者が承認すること。							
(2)ドキュメント管理ルールを定め、遵守すること。							
(3)情報システムの変更に伴い、ドキュメントの内容を更新し、更新履歴を記録すること。							
(4)ドキュメントの保管、複写及び廃棄は、不正防止及び機密保護の対策を講じること。							
2. 進捗管理（6）	1	3	4	1	2		
2.1 実施（3）						Or	O
(1)進捗計画に基づいて方法、体制等を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。							

別紙2 システム管理基準

リスクマネジメント（RM）戦略の6観点…C：経営、Or：組織ガバナンス、R：ITリスク、E：拡張性、Op:要件定義最適化、Q：品質重視
リスクカテゴリー…O：オペレーショナルリスク、B：ビジネスリスク、S：戦略リスク、Re：風評リスク、L：法務・規制リスク
4点（R):実行責任者、3点（A):説明責任者、2点（C）：協議先、1点（I）：報告者

システム管理基準	CEO	CIO	CEO+CIO	CFO	企業幹部	RM戦略の6観点	リスクカテゴリー
(2)ユーザ、企画、開発、運用及び保守の責任者は、進捗状況を把握すること。							
(3)進捗の遅延等の対策を講じること。							
2.2 評価（3）						Or	O
(1)業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。							
(2)評価結果は、次工程の計画に反映すること。							
(3)評価結果は、進捗管理の方法、体制等の改善に反映すること。							
3. 品質管理（4）	1	3	4	1	1		
3.1 計画（2）	1	2	3	1	1	Q	O
(1)品質目標に基づいて品質管理の計画を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。							
(2)品質管理計画は、方法、体制等を明確にすること。							
3.2 実施（2）		1	1			Q	O
(1)業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。							
(2)評価結果は、品質管理の基準、方法、体制等の改善に反映すること。							
4. 人的資源管理(13)	1	8	9	2	2		
4.1 責任・権限（3）	1	3	4	2	2	Or	O
(1)要員の責任及び権限は、業務の特性及び業務遂行上の必要性に応じて定めること。							
(2)要員の責任及び権限は、業務環境及び情報環境の変化に対応した見直しを行うこと。							
(3)要員の責任及び権限を周知徹底すること。							
4.2 業務遂行（4）		1	1			Or	O
(1)要員は、権限を遵守すること。							
(2)作業分担及び作業量は、要員の知識、能力等から検討すること。							
(3)要員の交替は、誤謬防止、不正防止及び機密保護を考慮して行うこと。							
(4)不測の事態に備えた代替要員の確保を検討すること。							
4.3 教育・訓練（4）		2	2			Or	O
(1)教育及び訓練に関する計画及びカリキュラムは、人的資源管理の方針に基づいて作成及び見直しを行うこと。							
(2)教育及び訓練に関する計画及びカリキュラムは、技術力の向上、業務知識の習得、情報システムの情報セキュリティ確保等から検討すること。							
(3)教育及び訓練は、計画及びカリキュラムに基づいて定期的かつ効果的に行うこと。							
(4)要員に対するキャリアパスを確立し、業務環境及び情報環境の変化に対応した見直しを行うこと。							
4.4 健康管理（2）		2	2			Or	O
(1)健康管理を考慮した作業環境を整えること。							
(2)健康診断及びメンタルヘルスケアを行うこと。							
5. 委託・受託（25）	2	8	10	5	2		
5.1 計画（3）	1	3	4	2	1	Or	O
(1)委託又は受託の計画は全体最適化計画に基づいて策定し、責任者が承認すること。							
(2)委託又は受託の目的、対象範囲、予算、体制等を明確にすること。							
(3)委託又は受託は、具体的な効果、問題点等を評価して決定すること。							
5.2 委託先選定（3）	1	2	3	2	1	Or	O
(1)委託先の選定基準を明確にすること。							
(2)委託候補先に必要な要求仕様を提示すること。							
(3)委託候補先が提示した提案書の比較検討を行うこと。							
5.3 契約（8）		1	1	1		Or	O
(1)契約は、委託契約ルール又は受託契約ルールに基づいて締結すること。							
(2)コンプライアンスに関する条項を明確にすること。							
(3)再委託の可否について明確にすること。							
(4)知的財産権の帰属を明確にすること。							
(5)特約条項及び免責条項を明確にすること。							
(6)業務内容及び責任分担を明確にすること。							
(7)契約締結後の業務内容に追加及び変更が生じた場合、契約内容の再検討を行うこと。							
(8)システム監査に関する方針を明確にすること。							
5.4 委託業務（7）		1	1			Or	O
(1)委託業務の実施内容は、契約内容と一致すること。							
(2)契約に基づき、必要な要求仕様、データ、資料等を提供すること。							
(3)委託業務の進捗状況を把握し、遅延対策を講じること。							
(4)委託先における誤謬防止、不正防止、機密保護等の対策の実施状況を把握し、必要な措置を講じること。							
(5)成果物の検収は、委託契約に基づいて行うこと。							
(6)業務終了後、委託業務で提供したデータ、資料等の回収及び廃棄の確認を行うこと。							
(7)委託した業務の結果を分析及び評価すること。							
5.5 受託業務（4）		1	1			Or	O
(1)受託業務の実施内容は、契約内容を遵守すること。							
(2)受託内容の進捗状況を把握し、リスク対策を講じること。							
(3)成果物の品質管理を行うこと。							
(4)契約に基づき、受託業務終了後、提供されたデータ、資料、機材等を返却又は廃棄すること。							
6. 変更管理（6）	0	4	4				
6.1 管理（3）		3	3			Or	O
(1)変更管理ルールを定め、ユーザ、開発及び保守の責任者が承認すること。							
(2)仕様変更、問題点、ペンディング事項等の変更管理案件が生じた場合、他システムの影響を考慮して決定すること。							
(3)変更管理案件は、提案から完了までの状況を管理し、未完了案件は定期的に分析すること。							
6.2 実施（3）		1	1			Or	O
(1)変更管理案件は、変更管理ルールに従って実施すること。							
(2)変更管理案件を実施した場合に、関連する情報システムの環境も同時に変更すること。							
(3)変更の結果は、ユーザ、開発、運用及び保守の責任者が承認すること。							
7. 災害対策（13）	4	5	9	4	2		
7.1 リスク分析（3）	2	3	5	2	1	R	O
(1)地震等のリスク及び情報システムに与える影響範囲を明確にすること。							
(2)情報システムの停止等により組織体が被る損失を分析すること。							
(3)業務の回復許容時間及び回復優先順位を定めること。							
7.2 災害時対応計画（6）	2	2	4	2	1	R	O
(1)リスク分析の結果に基づき、事業継続計画と整合をとった災害時対応計画を策定すること。							
(2)災害時対応計画は、組織体の長が承認すること。							
(3)災害時対応計画の実現可能性を確認すること。							
(4)災害時対応計画は、従業員の教育訓練の方針を明確にすること。							
(5)災害時対応計画は、関係各部に周知徹底すること。							
(6)災害時対応計画は、必要に応じて見直すこと。							
7.3 バックアップ（2）	2	3	5	2	1	−	O
(1)情報システム、データ及び関連設備のバックアップ方法並びに手順は、業務の回復目標に対応して定めること。							
(2)運用の責任者は、バックアップ方法及び手順を検証すること。							
7.4 代替処理・復旧（2）	2	2	4	2	1	−	O
(1)ユーザ及び運用の責任者は、復旧までの代替処理手続き及び体制を定め、検証すること。							
(2)ユーザ及び運用の責任者は、復旧手続き及び体制を定め、検証すること。							

金融機関等のシステム監査指針：チェックポイント集一覧表

リスクマネジメント(RM)戦略の6観点…C:経営、Or:組織ガバナンス、R:ITリスク、E:拡張性、Op:要件定義最適化、Q:品質重視
リスクカテゴリー…O:オペレーショナルリスク、B:ビジネスリスク、S:戦略リスク、Re:風評リスク、L:法務・規制リスク
経営者関与ポイント…4点(R):実行責任者、3点(A):説明責任者、2点(C):協議先、1点(I):報告者

要点項目	大項目	小項目	経営者				RM戦略の6観点	リスクカテゴリー	システム監査対象部門					システム監査の着眼点				
			CEO	CIO	CFO	企業幹部(ユーザー部門)			情報システム部門			本部各部門	利用部門	有効性	効率性	信頼性	安全性	遵守性
									企画	開発	運用							
1.情報システムの計画と管理(11)	1.情報システム戦略	A.経営戦略に沿った情報システム戦略の策定	2	4	1	2	C	S	◎			○		◎				
		B.情報システム運営委員会	2	3	2	2	C	S	◎	○	○	○	○	◎				
	2.全社的な情報システム組織	A.情報システム部門の組織	2	3	2	2	Or	O	◎	○	○			◎	○	○	○	○
		B.ユーザー部門等の組織体制	2	3	2	2	Or	O				◎	◎	◎	○	○	○	○
	3.情報システム計画	A.情報システム中長期計画の策定	3	4	2	2	Or	O	◎			○		◎	○			
		B.情報システム短期計画の策定と実施	2	3	1	1	Or	O	◎			○		◎	○			
	4.有効性評価	A.情報システム部門における評価					ー	O	◎	○	○			◎	○	○	○	○
		B.ユーザー部門等における評価					ー	O				◎	◎	◎	○	○	○	○
	5.最新技術の調査と研究	A.最新技術の調査と研究		3	1	1	Op	O	◎	○	○	○		◎	○	○	○	○
	6.投資及び予算管理	A.予算計画の策定	1	3	2	2	E	O	◎	○	○			○	◎			
		B.実績管理					ー	O	◎	○	○			○	◎			
	合計		14	26	13	14												
2.情報システムリスクの管理(5)	1.情報システムリスクの管理	A.情報システムリスク管理体制	1	4	2	1	R	O	◎	○	○	◎		○	○	○	◎	○
		B.情報システムリスクの識別と評価	3	2	4	2	R	O	◎	○	○	◎		○	○	○	◎	○
		C.情報システムリスク対策	1	4	1	1	R	O	◎	○	○	◎		○	○	○	◎	○
	2.法令遵守	A.法令・規制の遵守	1	4	1	1	R	L	◎	○	○	◎	○					◎
	3.情報システムの最新技術及び金融犯罪の動向に関する調査と研究	A.情報システムの最新技術及び金融犯罪の動向に関する調査と研究	1	3			Op	O	◎	○	○	◎		○	○	○	◎	○
	合計		7	17	8	5												
3.情報セキュリティ(20)	1.全社的なセキュリティ管理体制	A.セキュリティポリシー	1	3	2	2	R	O	◎	○	○	◎	○				◎	○
		B.セキュリティスタンダード	1	3	2	2	R	O	◎	○	○	◎	○				◎	○
		C.セキュリティ管理体制	1	3	2	2	R	O	◎	○	○	◎	○				◎	
		D.セキュリティ教育・研修		3		2	Op	O	◎	○	○	◎	○				◎	
		E.障害・事故・犯罪等の対応					ー	O	○	○	◎	○	○				◎	
	2.建物・設備等の安全対策	A.建物・設備等の安全対策		1		1	R	O	○	○	◎	○	○				◎	
		B.入退館(室)管理		1		1	R	O	○	○	◎	○	○				◎	
	3.パソコン、サーバー等の管理	A.パソコン等の管理					ー	O	◎	◎	◎	◎	◎				◎	
		B.サーバーの管理					ー	O	◎	◎	◎	◎	◎				◎	
	4.機密情報管理	A.機密情報の管理					ー	O		◎	○	○					◎	
		B.機密情報の暗号化					ー	O		◎	○						◎	
		C.暗号鍵の管理					ー	O	○	◎	○	○	○				◎	
	5.アクセスコントロール	A.アクセスコントロールの方針と手続き					ー	O	○	◎							◎	○
		B.アクセスコントロール設計					ー	O		◎							◎	
		C.ユーザーIDの管理					ー	O	◎	◎	◎	◎	◎				◎	○
		D.パスワード管理					ー	O	◎	◎	◎	◎	◎				◎	○
		E.アクセスの監視					ー	O			◎						◎	
	6.コンピュータウイルス等不正プログラム対策	A.コンピュータウイルス等不正プログラム対策	1	3			R	O	◎	◎	◎	◎	◎				◎	
	7.顧客データ保護	A.顧客データ管理					ー	O	○	○	◎	○	○				◎	○
		B.個人データの取扱方針と管理	1	2		2	R	O	○	○	◎	○	○				◎	○
	合計		5	19	6	12												
4.システム開発(26)	1.運営と要員管理	A.職務の分離		3	1	1	R	O		◎							◎	
		B.システム開発業務の運営管理	1	2			Or	O		◎					◎	○		
		C.システム開発要員の管理					ー	O		◎					◎	○	○	○
		D.開発環境の整備		1			Or	O		◎							◎	
	2.標準と手続き	A.標準と手続きの制定		1			Op	O		◎					○	◎		○
		B.標準と手続きの維持管理					ー	O		◎					○	◎		○
	3.システム開発ライフサイクル(SDLC)	A.システム分析		1		1	E	O		◎	○	○	○	◎	○	○	○	○
		B.開発検討		1		1	E	O		◎				○	◎	○	○	○
		C.システム設計		1			E	O		◎				○	○	◎	○	○
		D.プログラム設計					ー	O		◎					○	◎		○
		E.プログラミング					ー	O		◎					○	◎		○

別紙3 金融機関等のシステム監査指針

リスクマネジメント（RM)戦略の6観点…C：経営、Or：組織ガバナンス、R：ITリスク、E：拡張性、Op:要件定義最適化、Q：品質重視
リスクカテゴリー…O：オペレーショナルリスク、B：ビジネスリスク、S：戦略リスク、Re：風評リスク、L：法務・規制リスク
経営者関与ポイント…4点（R)：実行責任者、3点（A)：説明責任者、2点（C)：協議先、1点（I)：報告者

要点項目	大項目	小項目	経営者				RM戦略の6観点	リスクカテゴリー	システム監査対象部門					システム監査の着眼点				
			CEO	CIO	CFO	企業幹部（ユーザー部門）			情報システム部門			本部各部門	利用部門	有効性	効率性	信頼性	安全性	遵守性
									企画	開発	運用							
4.システム開発	3.システム開発ライフサイクル(SDLC)	F.システムテスト					―	O		◎					○	◎	○	○
		G.移行		1		1	Op	O		◎	○	○	○		○	◎	○	○
		H.移行後レビュー					―	O		◎	○	○	○	◎	○	○	○	○
	4.システム変更管理	A.システム変更					―	O		◎	○	○	○		○	◎	○	○
		B.プログラム変更作業					―	O		◎					○	◎	○	○
		C.一時的プログラム変更					―	O		◎					○	◎	○	○
	5.障害対策	A.障害対策		1			R	O		◎						◎	○	
	6.パッケージソフトウェア取得	A.調査・分析		1			Op	O		◎				◎	○	○	○	○
		B.導入					―	O		◎				○	○	◎	○	○
		C.フォローアップ					―	O		◎				◎	○	○	○	○
	7.プロジェクトマネジメント	A.プロジェクト計画の策定	1	2		1	Or	O		◎	○	○	○	◎	○	○	○	○
		B.プロジェクト計画の内容	1	2		1	Or	O		◎					◎	○	○	
		C.プロジェクト要員	1	2			Or	O		◎					◎	○	○	
		D.進捗・コスト・品質管理	1	2			Q	O		◎					◎	○	○	
		E.プロジェクトの評価					―	O		◎				○	◎	○	○	
	合計		5	21	1	6												
5.システム運用(18)	1.運営と要員管理	A.職務の分離		2			R	O			◎						◎	
		B.システム運用業務の運営管理					―	O			◎				◎	○		
		C.システム運用要員の管理					―	O			◎				◎	○	○	○
	2.標準と手続き	A.標準と手続きの制定					―	O			◎				○	◎		○
		B.標準と手続きの維持管理					―	O			◎				○	◎		○
	3.運用管理	A.オペレーション管理-スケジュール管					―	O			◎				○	◎	○	○
		B.オペレーション管理-作業管理					―	O			◎				○	○	◎	○
		C.オペレーション管理-管理記録					―	O			◎				○	○	◎	○
		D.システム運用状況の監視					―	O			◎					◎	◎	○
		E.ファイル管理					―	O			◎				○	○	◎	○
		F.プログラム管理					―	O			◎				○	○	◎	○
		G.機器管理					―	O			◎					◎	◎	○
		H.外部接続管理					―	O			◎					◎	◎	○
		I.障害対策-発生管理					―	O			◎					◎	◎	
		J.障害対策-原因究明・対策					―	O			◎					◎	◎	○
		K.重要帳票管理					―	O			◎					◎	◎	○
		L.カード管理					―	O			◎					◎	◎	○
		M.CD/ATM等及び無人店舗の管理					―	O			◎					◎	◎	○
	合計		0	2	0	0												
6.システム利用(15)	1.運営と要員管理	A.ユーザー部門等における運営管理					―	O				○	◎	◎			○	○
		B.ユーザー部門等の要員管理					―	O				○	◎		◎	○	○	
		C.教育・訓練					―	O				○	◎		◎	○	○	
		D.防災・防犯					―	O				○	◎				◎	○
		E.機器の保守					―	O				○	◎			○	◎	○
	2.ユーザー業務手続きとマニュアル	A.ユーザー業務手続きとマニュアルの維持管理					―	O				○	◎			○		◎
	3.業務管理	A.端末機等操作の管理					―	O					◎				◎	○
		B.データファイルの取扱管理					―	O					◎				◎	○
		C.重要帳票の管理					―	O					◎				◎	○
		D.顧客の認証媒体やキャッシュカード等の管理					―	O					◎				◎	○
		E.顧客のパスワードや暗証番号の管理					―	O					◎				◎	○
		F.CD/ATMの管理					―	O					◎				◎	○
		G.無人店舗の管理					―	O					◎				◎	○
		H.その他の店舗形態の管理					―	O					◎				◎	○
		I.渉外用パソコン等の管理					―	O					◎				◎	○
	合計		0	0	0	0												
7.入出力等の処理(22)	1.入出力業務管理体制	A.職務の分離					―	O					◎				◎	
		B.業務管理					―	O					◎				◎	
	2.入力原票	A.入力原票の作成					―	O					◎					◎
		B.入力原票の承認					―	O					◎					◎
		C.入力原票の訂正					―	O					◎					◎
		D.入力原票の保存					―	O					◎					◎

別紙3 金融機関等のシステム監査指針

リスクマネジメント（RM)戦略の6観点…C：経営、Or：組織ガバナンス、R：ITリスク、E：拡張性、Op:要件定義最適化、Q：品質重視
リスクカテゴリー…O：オペレーショナルリスク、B：ビジネスリスク、S：戦略リスク、Re：風評リスク、L：法務・規制リスク
経営者関与ポイント…4点（R)：実行責任者、3点（A)：説明責任者、2点（C)：協議先、1点（I)：報告者

要点項目	大項目	小項目	経営者				RM戦略の6観点	リスクカテゴリー	システム監査対象部門					システム監査の着眼点				
			CEO	CIO	CFO	企業幹部（ユーザー部門）			情報システム部門			本部各部門	利用部門	有効性	効率性	信頼性	安全性	遵守性
									企画	開発	運用							
7.入出力等の処理	3.入力処理	A.データ入力					―	O		◎		○	◎			◎	○	○
		B.外部企業等からの入力データの受入れ					―	O		◎	○	○	◎			◎	○	○
		C.入力原票がない場合のデータ入力					―	O		◎		○	◎			◎	○	○
	4.処理の一貫性の制御	A.処理の正確性確保					―	O		◎	○	○	◎			◎		○
		B.ファイル間の整合性確保					―	O		◎	○	○	◎			◎		○
		C.複数システム間のインタフェース					―	O		◎	○		◎			◎		
	5.エラーデータ	A.エラーデータの修正					―	O		◎		○	◎					◎
		B.エラーデータの分析					―	O		◎		○	◎			◎		
	6.出力処理	A.出力情報の検証					―	O				○	◎			◎		
		B.出力情報の訂正					―	O				○	◎			◎	○	○
		C.出力情報の配布					―	O			○	○	◎			◎	○	○
		D.外部企業等へのデータ送付					―	O			○		◎			◎	○	○
		E.出力情報の保存、廃棄					―	O					◎			○	◎	○
		F.出力情報の有用性					―	O			○	○	◎	◎	○			
	7.マスターファイル	A.マスターファイルの更新					―	O			◎					◎	○	
		B.マスターファイルの完全性及び正確性の確保					―	O			◎					◎	○	
	合計		0	0	0	0												
8.ネットワーク(10)	1.ネットワーク管理	A.ネットワーク管理体制		1			Or	O			◎	○	○		○	○	◎	
		B.ネットワーク管理に係る手続き					―	O			◎	○	○		○	○	◎	
		C.ネットワークの構成管理					―	O			◎	○	○		○	○	◎	
		D.障害対策					―	O			◎	○	○		○	○	◎	
	2.セキュリティ管理	A.アクセスコントロール					―	O			◎	○	○		○	○	◎	
	3.インターネットセキュリティ	A.インターネットセキュリティ					―	O			◎	○	○		○	○	◎	
		B.ホームページ					―	O			◎	○	○			○	◎	○
	4.電子メール	A.電子メール					―	O	○	○	◎	○	○		○	○	◎	○
	5.オープンネットワークを利用した金融サービス	A.不正取引を防止する機能					―	O			◎	○	○			○	◎	○
		B.顧客への対応					―	O				◎	◎			○	◎	○
	合計		0	1	0	0												
9.システム資産・資源管理(7)	1.資産管理	A.ハードウェア資産管理					―	O			◎			○	○		◎	
		B.ソフトウェア資産管理					―	O			◎			○	○			◎
	2.容量管理	A.キャパシティプランニング	1	2			Q	O			◎			○	◎			
	3.性能管理	A.性能測定とチューニング					―	O			◎				◎	○		
	4.データベース管理	A.データベース管理					―	O		○	◎				○	○	◎	
	5.パッチの適用と管理	A.パッチの適用と管理					―	O			◎				○	○	◎	
	6.構成管理	A.構成管理					―	O			◎				○	○	◎	
	合計		1	2	0	0												
10.外部委託(4)	1.外部委託計画	A.外部委託計画の策定	1	2			Or	O	◎			○		○	○	○	◎	
		B.外部委託先の選定		1			E	O	◎	○	○	○		○	○	○	◎	
		C.外部委託契約の締結					―	O	◎	○	○				○	○	○	◎
	2.外部委託業務管理	A.外部委託業務の管理					―	O		◎	◎			○	◎	◎	◎	○
	合計		1	3	0	0												
11.コンティンジェンシープラン(23)	1.情報システムのコンティンジェンシープランの策定と維持管理	A.コンティンジェンシープランの策定		2		2	R	O	○			◎				○	◎	
		B.コンティンジェンシープラン策定のための体制		2		2	R	O	○	○	○	◎	○			○	◎	
		C.リスク分析と評価		2		2	R	O	○			◎				○	◎	
		D.復旧手順の作成					―	O	○			◎				○	◎	
		E.教育・訓練					―	O	○	○	○	◎	○	○		○	◎	
		F.コンティンジェンシープランの維持管					―	O	○	○	○	◎	○	○		○	◎	
	2.緊急事態に対する準備	A.緊急時対応組織の準備					―	O	○			◎				○	◎	
		B.人員及び資産の安全確保					―	O	○			◎				○	◎	
		C.通信手段の確保及び情報収集					―	O	○			◎				○	◎	
		D.緊急用資源と搬送手段の確保					―	O	○			◎				○	◎	
		E.緊急時の業務運営の方法					―	O	○			◎				○	◎	
		F.災害対策システムーバックアップサイト等の対応					―	O	○	○	○	◎				○	◎	
		G.広報活動の準備					―	Re	○			◎				○	◎	
		H.損害状況評価の方法					―	O	○			◎				○	◎	

別紙3 金融機関等のシステム監査指針

リスクマネジメント（RM)戦略の6観点…C：経営、Or：組織ガバナンス、R：ITリスク、E：拡張性、Op:要件定義最適化、Q：品質重視
リスクカテゴリー…O：オペレーショナルリスク、B：ビジネスリスク、S：戦略リスク、Re：風評リスク、L：法務・規制リスク
経営者関与ポイント…4点（R)：実行責任者、3点（A)：説明責任者、2点（C)：協議先、1点（I)：報告者

要点項目	大項目	小項目	経営者				RM戦略の6観点	リスクカテゴリー	システム監査対象部門					システム監査の着眼点				
			CEO	CIO	CFO	企業幹部（ユーザー部門）			情報システム部門			本部各部門	利用部門	有効性	効率性	信頼性	安全性	遵守性
									企画	開発	運用							
11.コンティンジェンシープラン	3.対策本部における対応	A.初期対応の手順					―	O	○			◎				○	◎	
		B.暫定対応の手順					―	O	○			◎				○	◎	
		C.本格復旧の手順					―	O	○			◎				○	◎	
	4.コンピュータセンター等における対応	A.初期対応の手順					―	O	○	○	○	◎				○	◎	
		B.暫定対応の手順					―	O	○	○	○	◎				○	◎	
		C.本格復旧の手順					―	O	○	○	○	◎				○	◎	
	5.営業店等における対応	A.初期対応の手順					―	O				◎	○			○	◎	
		B.暫定対応の手順					―	O				◎	○			○	◎	
		C.本格復旧の手順					―	O				◎	○			○	◎	
	合計		0	6	0	6												
12.ドキュメンテーション(8)	1.ドキュメンテーションの標準化	A.ドキュメンテーション標準の制定と管					―	O		◎	○	○			○	◎		○
		B.電子媒体によるドキュメンテーションの標準					―	O		◎	○	○			○	◎	○	○
	2.ドキュメントの作成	A.ドキュメントの作成					―	O		◎					○	◎		
		B.ドキュメントの作成管理					―	O		◎					○	◎		
		C.プロトタイプ開発等におけるドキュメントの作成					―	O		◎					○	◎		
	3.ドキュメントの管理	A.ドキュメント管理手続きの制定					―	O		◎	○	○	○				◎	○
		B.ドキュメントの内容の更新					―	O		◎					○	◎		
		C.ドキュメントの機密性					―	O		◎	○	○	○				◎	
	合計		0	0	0	0												

別紙4 金融検査マニュアル（預金等受入機関に係る検査マニュアル）

リスクマネジメント(RM) 戦略の6観点…C：経営、Or：組織ガバナンス、R：ITリスク、E：拡張性、Op:要件定義最適化、Q：品質重視

リスクカテゴリー…O：オペレーショナルリスク、B：ビジネスリスク、S：戦略リスク、Re：風評リスク、L：法務・規制リスク

経営者関与ポイント…4点（R）：実行責任者、3点（A）：説明責任者、2点（C）：協議先、1点（I）：報告者

金融検査マニュアル（預金等受入機関に係る検査マニュアル）								
大項目	中項目	CEO	CIO	CFO	企業幹部	合計	RM戦略の6観点	リスクカテゴリー
Ⅰ．経営陣によるシステムリスク管理態勢の整備・確立状況								
1．方針の策定	①【取締役の役割・責任】	4	4	4	4	16	C	O
	（ⅰ）取締役							
	（ⅱ）取締役会							
	（ⅲ）システム担当取締役							
	②【戦略目標の明確化】	4	4	2	4	14	C	S
	③【システムリスク管理方針の整備・周知】	2	4	2	2	10	R	O
	④【方針策定プロセスの見直し】	2	4	2	2	10	Or	O
	合計	12	16	10	12	50		
2．内部規程・組織体制の整備	①【内部規程の整備】	2	4	2	2	10	Or	O
	②【システムリスク管理部門の態勢整備】	2	4	2	2	10	Or	O
	（ⅰ）設置と役割付与							
	（ⅱ）管理者の配置と権限付与							
	（ⅲ）人員の配置							
	（ⅳ）業務部門への牽制機能							
	③【各業務部門及び営業店等におけるシステムリスク管理態勢の整備】	2	4	2	4	12	Or	O
	（ⅰ）内部規程等周知遵守態勢の整備							
	（ⅱ）システムリスク管理の実効性確保							
	④【取締役会等への報告・承認態勢の整備】	2	4	2	2	10	Or	O
	⑤【監査役への報告態勢の整備】	2	4	2	2	10	Or	O
	⑥【内部監査実施要領及び内部監査計画の策定】	2	4	2	2	10	Or	O
	⑦【内部規程･組織体制の整備プロセスの見直し】	2	4	2	2	10	Or	O
	合計	14	28	14	16	72		
3．評価・改善活動								
⑴ 分析・評価	①【システムリスク管理の分析・評価】	2	4	2	2	10	R	O
	②【分析・評価プロセスの見直し】	2	4	2	2	10	R	O
⑵ 改善活動	①【改善の実施】	2	4	2	2	10	Or	O
	②【改善活動の進捗状況】	2	4	2	2	10	Or	O
	③【改善プロセスの見直し】	2	4	2	2	10	Or	O
Ⅱ．管理者によるシステムリスク管理態勢の整備・確立状況								
1．管理者の役割・責任	①【システムリスク管理規程の整備・周知】	－	－	－	－	－	－	O
	②【システムリスク管理規程の内容】	－	－	－	－	－	－	O
	③【管理者による組織体制の整備】							
	（ⅰ）システムリスク管理部門の態勢	－	－	－	－	－	－	O
	（ⅱ）研修・教育態勢と専門性人材の育成	－	－	－	－	－	－	O
	（ⅲ）取締役会等及びオペレーショナル・リスク管理部門への報告態勢	－	－	－	－	－	－	O
	（ⅳ）セキュリティ管理者の設置	－	－	－	－	－	－	O
	（ⅴ）システム管理者の設置（含むEUC）	－	－	－	－	－	－	O
	（ⅵ）データ管理者の設置	－	－	－	－	－	－	O
	（ⅶ）ネットワーク管理者の設置	－	－	－	－	－	－	O
	④【システムリスク管理規程及び組織体制の見直し】	－	－	－	－	－	－	O
2．システムリスク管理部門の役割・責任								
⑴【システムリスクの認識・評価】	（ⅰ）システム全般のリスク認識・評価	－	－	－	－	－	－	O
	（ⅱ）EUC等のリスク認識・評価	－	－	－	－	－	－	O
	（ⅲ）定期的又は適時のリスク認識・評価	－	－	－	－	－	－	O
	（ⅳ）システム処理能力に関するリスク認識・評価	－	－	－	－	－	－	O
	（ⅴ）新商品導入時又は商品内容変更時のリスク認識・評価	－	－	－	－	－	－	O
	（ⅵ）インターネット等を利用した取引のリスク認識・評価	－	－	－	－	－	－	O
⑵【システムリスクのモニタリング】	（ⅰ）適切な頻度でのモニタリング	－	－	－	－	－	－	O
	（ⅱ）取締役会等及びオペレーショナル・リスク管理部門への報告	－	－	－	－	－	－	O
⑶【システムリスクのコントロール及び削減】	（ⅰ）システムリスクのコントロール	－	－	－	－	－	－	O
	（ⅱ）システムリスクの削減	－	－	－	－	－	－	O
⑷検証・見直し	システムリスク管理方法の定期的な検証・見直し	－	－	－	－	－	－	O
Ⅲ．個別の問題点								
1．情報セキュリティ管理								
⑴セキュリティ管理者等の役割・責任	①【セキュリティ管理者の役割・責任】							

別紙4 金融検査マニュアル（預金等受入機関に係る検査マニュアル）

リスクマネジメント(RM) 戦略の6観点…C：経営、Or：組織ガバナンス、R：ITリスク、E：拡張性、Op:要件定義最適化、Q：品質重視

リスクカテゴリー…O：オペレーショナルリスク、B：ビジネスリスク、S：戦略リスク、Re：風評リスク、L：法務・規制リスク

経営者関与ポイント…4点（R）：実行責任者、3点（A）：説明責任者、2点（C）：協議先、1点（I）：報告者

金融検査マニュアル（預金等受入機関に係る検査マニュアル）								
大項目	中項目	CEO	CIO	CFO	企業幹部	合計	RM戦略の6観点	リスクカテゴリー
	（ｉ）企画、開発、運用、保守にわたるすべての管理	－	－	－	－	－	－	O
	（ii）システムリスク管理部門への報告	－	－	－	－	－	－	O
	（iii）ﾌｨｼﾞｶﾙｾｷｭﾘﾃｨ、ﾛｼﾞｶﾙｾｷｭﾘﾃｨ	－	－	－	－	－	－	O
	（iv）ｼｽﾃﾑ、ﾃﾞｰﾀ、ﾈｯﾄﾜｰｸ管理上のｾｷｭﾘﾃｨ	－	－	－	－	－	－	O
	②【システム管理者の役割・責任】							
	（ｉ）適正なスクラップ・アンド・ビルド	－	－	－	－	－	－	O
	（ii）各業務部門、営業店等及びｺﾝﾋﾟｭｰﾀｾﾝﾀｰ	－	－	－	－	－	－	O
	（iii）社外に持ち出すコンピュータの管理	－	－	－	－	－	－	O
	③【データ管理者の役割・責任】							
	（ｉ）内部規程・業務細則等の制定、周知徹底	－	－	－	－	－	－	O
	（ii）データ保護、データ不正使用防止について適切かつ十分な管理	－	－	－	－	－	－	O
	④【ネットワーク管理者の役割・責任】							
	（ｉ）内部規程・業務細則等の制定、周知徹底	－	－	－	－	－	－	O
	（ii）ネットワークがダウンした際の代替手段考慮	－	－	－	－	－	－	O
⑵【不正使用防止】	（ｉ）接続相手先が本人若しくは正当な端末であることを確認する態勢	－	－	－	－	－	－	O
	（ii）操作履歴を監査証跡として取得、定期的チェック	－	－	－	－	－	－	O
	（iii）アクセス権限の管理明確化	－	－	－	－	－	－	O
⑶【コンピュータウィルス等】	不正な侵入の防止と侵入時の発見除去態勢	－	－	－	－	－	－	O
⑷【インターネットを利用した取引の管理】	（ｉ）顧客からの苦情相談等を受け付ける態勢	－	－	－	－	－	－	O
	（ii）システムダウン、不具合時の補完態勢	－	－	－	－	－	－	O
	（iii）サービス提供主体の誤認防止対策	－	－	－	－	－	－	O
	（iv）当該金融機関の情報、サービス提供内容の開示	－	－	－	－	－	－	O
	（ｖ）マネーローンダリング防止等の観点	－	－	－	－	－	－	L
	（vi）顧客情報漏洩、顧客データ改ざん書換の防止態勢	－	－	－	－	－	－	O
	（vii）顧客取引履歴の一定期間保存	－	－	－	－	－	－	O
	（viii）利用者自身が使用状態を確認できる機能	－	－	－	－	－	－	O
	（ix）フィッシング詐欺対策等の不正防止策	－	－	－	－	－	－	O
⑸【偽造・盗難キャッシュカード対策】	（ｉ）ATMｼｽﾃﾑ等のセキュリティレベルの評価、対策	－	－	－	－	－	－	O
	（ii）不正払戻し防止、情報漏えい防止	－	－	－	－	－	－	O
	（iii）異常な取引に関する基準、把握時の対応	－	－	－	－	－	－	O
2. システム企画・開発・運用管理等								
⑴【システム開発・運用部門の相互牽制態勢】	システム開発部門運用部門の分離分担、相互牽制	－	－	－	－	－	－	O
⑵ システム企画・開発態勢	①【企画・開発態勢】							
	（ｉ）内部規程・業務細則等の整備	－	－	－	－	－	－	O
	（ii）横断的な審議機関設置、検討	－	－	－	－	－	－	O
	（iii）中長期の開発計画策定	－	－	－	－	－	－	O
	（iv）リスクの継続的洗い出しと維持・改善のための投資	－	－	－	－	－	－	O
	（ｖ）投資効果検討と必要に応じた取締役会報告	－	－	－	－	－	－	O
	（vi）開発案件の企画・開発・移行の承認ルール	－	－	－	－	－	－	O
	（vii）本番システムの変更案件の承認後実施	－	－	－	－	－	－	O
	②【開発管理】							
	（ｉ）開発に関わる書類やプログラムの作成方式の標準化	－	－	－	－	－	－	O
	（ii）ﾌﾟﾛｼﾞｪｸﾄ責任者を定め、取締役会、ｵﾍﾟﾚｰｼｮﾅﾙﾘｽｸ管理部門の進捗状況チェック	－	－	－	－	－	－	O
	③【内部規程・業務細則等の整備】							
	（ｉ）設計、開発、運用に関する内部規程・業務細則等の策定、見直し	－	－	－	－	－	－	O
	（ii）設計書等は開発書類作成の標準規約制定、準拠作成	－	－	－	－	－	－	O
	（iii）開発の監査証跡を残すようなシステム	－	－	－	－	－	－	O
	（iv）マニュアル、開発書類等の第三者宛分かりやすさ	－	－	－	－	－	－	O
	④【テスト等】							
	（ｉ）テスト計画作成と適切かつ十分なテスト	－	－	－	－	－	－	O
	（ii）テスト実施態勢の整備	－	－	－	－	－	－	O
	（iii）ユーザー部門も参加する総合テストの実施	－	－	－	－	－	－	O
	（iv）内容を理解できる役職員による検収	－	－	－	－	－	－	O
	⑤【システム移行の決定】							
	（ｉ）責任者の明確化	－	－	－	－	－	－	O
	（ii）移行計画策定と各部門の役割と責任の明確化	－	－	－	－	－	－	O

別紙4 金融検査マニュアル（預金等受入機関に係る検査マニュアル）

リスクマネジメント(RM) 戦略の6観点…C：経営、Or：組織ガバナンス、R：ITリスク、E：拡張性、Op:要件定義最適化、Q：品質重視
リスクカテゴリー…O：オペレーショナルリスク、B：ビジネスリスク、S：戦略リスク、Re：風評リスク、L：法務・規制リスク
経営者関与ポイント…4点（R）：実行責任者、3点（A）：説明責任者、2点（C）：協議先、1点（I）：報告者

金融検査マニュアル（預金等受入機関に係る検査マニュアル）								
大項目	中項目	CEO	CIO	CFO	企業幹部	合計	RM戦略の6観点	リスクカテゴリー
	（iii）移行判定基準策定と当該基準での移行決定	−	−	−	−	−	−	O
	⑥【システム移行後の検証】							
	（ｉ）稼働後一定期間をおいて移行後のレビュー実施	−	−	−	−	−	−	O
	（ii）ユーザー要件充足、費用対効果等の検討、評価	−	−	−	−	−	−	O
	（iii）レビュー結果の改善計画への反映	−	−	−	−	−	−	O
	（iv）レビュー結果の各部門責任者への報告	−	−	−	−	−	−	O
	（v）新商品導入後、ユーザー部門でのサンプルチェック実施	−	−	−	−	−	−	O
	⑦【人材の育成】	−	−	−	−	−	−	O
⑶ システム運用態勢	①【職務分担の明確化】							
	（ｉ）職務分担の明確化	−	−	−	−	−	−	O
	（ii）運用担当者の担当外ﾃﾞｰﾀﾌﾟﾛｸﾞﾗﾑへのアクセス禁止	−	−	−	−	−	−	O
	②【システムオペレーション管理】							
	（ｉ）スケジュール表、指示表等による実施	−	−	−	−	−	−	O
	（ii）承認後の作業スケジュール表、作業指示書による実施	−	−	−	−	−	−	O
	（iii）全ての記録とチェック項目を定めた点検	−	−	−	−	−	−	O
	（iv）重要オペレーションの複数名実施、自動化	−	−	−	−	−	−	O
	（v）レポート出力機能や作業履歴取得保存機能	−	−	−	−	−	−	O
	（vi）開発担当者によるオペレーションの原則禁止	−	−	−	−	−	−	O
	③【本番データ管理】							
	（ｉ）データ貸与の方針、手続きの明確化	−	−	−	−	−	−	O
	（ii）方針、手続きに従った運用等の本番データ管理	−	−	−	−	−	−	O
	④【システム障害の管理】							
	（ｉ）重要な障害発生時、関係部門と連携し、取締役会等に報告する態勢	−	−	−	−	−	−	O
	（ii）最悪のシナリオを想定して必要な対応を行う態勢	−	−	−	−	−	−	O
	（iii）関係業務部門への情報提供方法、内容の明確化	−	−	−	−	−	−	O
	（iv）外部委託先を含めた指揮命令系統明確化と応援体制明確化	−	−	−	−	−	−	O
	（v）記録簿記入と、システムリスク管理部門への報告態勢	−	−	−	−	−	−	O
	（vi）運用外部委託先からの報告態勢	−	−	−	−	−	−	O
	（vii）障害内容の定期的分析と対応策	−	−	−	−	−	−	O
	（viii）障害の影響の極小化するためのｼｽﾃﾑ的な仕組み	−	−	−	−	−	−	O
⑷ システム監査	（ｉ）独立した内部監査部門による定期的システム監査	−	−	−	−	−	−	O
	（ii）精通した要員による内部監査実施やｼｽﾃﾑ監査人等による外部監査活用	−	−	−	−	−	−	O
3. 防犯・防災・バックアップ・不正利用防止								
⑴【防犯対策】	（ｉ）防犯組織の整備と責任者明確化	−	−	−	−	−	−	O
	（ii）入退室管理・重要鍵管理等、適切かつ十分な管理	−	−	−	−	−	−	O
⑵【コンピュータ犯罪・事故等】	留意した態勢と点検等の事後チェック	−	−	−	−	−	−	O
⑶【防災対策】	（ｉ）防災組織の整備と責任者の明確化	−	−	−	−	−	−	O
	（ii）業務組織に即した防災組織と役割分担責任者明確化	−	−	−	−	−	−	O
	（iii）防火・地震・出水に対する対策確保	−	−	−	−	−	−	O
	（iv）重要データ等の避難場所の確保	−	−	−	−	−	−	O
⑷【バックアップ】	（ｉ）バックアップの取得と管理方法明確化	−	−	−	−	−	−	O
	（ii）分散保管、隔地保管等	−	−	−	−	−	−	O
	（iii）バックアップ取得周期の文書化	−	−	−	−	−	−	O
	（iv）重要システムでのｵﾌｻｲﾄﾊﾞｯｸｱｯﾌﾟｼｽﾃﾑ準備	−	−	−	−	−	−	O
⑸【コンティンジェンシープランの策定】	（ｉ）コンティンジェンシープランの整備、実効性の確保	−	−	−	−	−	−	O
	（ii）取締役会の承認	−	−	−	−	−	−	O
	（iii）「金融機関等におけるコンティンジェンシープラン策定のための手引書」の参照	−	−	−	−	−	−	O
	（iv）システム障害やバッチ遅延等のリスクシナリオの想定	−	−	−	−	−	−	O
	（v）決済に及ぼす影響や顧客に与える被害の分析	−	−	−	−	−	−	O
	（vi）システム障害事例等でのシナリオの見直し	−	−	−	−	−	−	O
	（vii）全社レベル、外部委託先と共同での訓練の定期的実施	−	−	−	−	−	−	O
4. 外部委託管理								
⑴ 外部委託業務の管理	①【外部委託先の選定】レピュテーションの観点等	−	−	−	−	−	−	O（Re）
	②【委託契約の内容】	−	−	−	−	−	−	O
	③【外部委託先のモニタリング】	−	−	−	−	−	−	O
	④【外部委託先への監査】	−	−	−	−	−	−	O

別紙4 金融検査マニュアル（預金等受入機関に係る検査マニュアル）

リスクマネジメント(RM) 戦略の6観点…C：経営、Or：組織ガバナンス、R：ITリスク、E：拡張性、Op:要件定義最適化、Q：品質重視

リスクカテゴリー…O：オペレーショナルリスク、B：ビジネスリスク、S：戦略リスク、Re：風評リスク、L：法務・規制リスク

経営者関与ポイント…4点（R）：実行責任者、3点（A）：説明責任者、2点（C）：協議先、1点（I）：報告者

金融検査マニュアル（預金等受入機関に係る検査マニュアル）								
大項目	中項目	CEO	CIO	CFO	企業幹部	合計	RM戦略の6観点	リスクカテゴリー
	⑤【問題点の是正】	－	－	－	－	－	－	O
⑵ システム関係の業務委託先の検証	①システムリスクの認識・評価	－	－	－	－	－	－	O
	②委託者の監査、外部監査の定期的な実施、報告	－	－	－	－	－	－	O
	③セキュリティレベル	－	－	－	－	－	－	O
	④ユーザーレビュー、ユーザーテストの実施	－	－	－	－	－	－	O
	⑤品質管理部著による客観的評価態勢	－	－	－	－	－	－	O
	⑥運用状況の定期的な報告	－	－	－	－	－	－	O
	⑦システム障害等発生時の連絡態勢の制定	－	－	－	－	－	－	O
	⑧他の金融機関への影響等の判断と対応態勢	－	－	－	－	－	－	O
5. 付保預金の円滑な払戻しのための整備状況等								
⑴ 預金保険法遵守	第55 条の2第4項及び第58 条の3第1 項	－	－	－	－	－	－	O
⑵名寄せの整備	①適切に維持・登録される態勢整備	－	－	－	－	－	－	O
	②正しい登録、登録状況の検証	－	－	－	－	－	－	O
⑶ 保険事故発生時	事故発生時のシステムの整備	－	－	－	－	－	－	O
⑷ 新商品やシステム更改	修正、更改に関わるシステムの整備	－	－	－	－	－	－	O
⑸手順書・マニュアル整備	①保険事故発生から磁気テープ等を預金保険機構に提出するまで	－	－	－	－	－	－	O
	②預金保険機構からデータを受け取った後の作業	－	－	－	－	－	－	O
	③上記②のデータを用いずに払戻を行う作業	－	－	－	－	－	－	O
	④事故発生後の預金等変動のデータを預金保険機構に提出する作業	－	－	－	－	－	－	O
	⑤預金者等に対する債権と支払対象預金等との相殺及び預金等債権の買取り等	－	－	－	－	－	－	O
6. システム統合に係るリスク管理態勢	「システム統合リスク管理態勢の確認検査用チェックリスト」	－	－	－	－	－	－	O

別紙5 システム統合リスク管理態勢の確認検査用チェックリスト

リスクマネジメント(RM)戦略の6観点…C:経営、Or:組織ガバナンス、R:ITリスク、E:拡張性、Op:要件定義最適化、Q:品質重視
リスクカテゴリー…O:オペレーショナルリスク、B:ビジネスリスク、S:戦略リスク、Re:風評リスク、L:法務・規制リスク
経営者関与ポイント…4点(R):実行責任者、3点(A):説明責任者、2点(C):協議先、1点(I):報告者

項目		リスク管理態勢のチェック項目	CEO	CIO	CFO	企業幹部	合計	RM戦略の6観点	リスクカテゴリー
Ⅰ. 経営陣のリスク管理に対する協調した取組み	ⅰ. 経営統合に係るリスク管理態勢のあり方	1. 経営統合に係るリスクに対する認識	4	2	2	2	10	R	O
		2. 協調体制の整備	4	2	2	2	10	Or	O
		3. 顧客対応の重要性に対する認識等	4	2	2	2	10	Or	O
		4. 統合方針の確立	4	2	2	2	10	C	O
		5. ビジネスモデルの確立	4	2	2	2	10	C	O
		6. 統合計画及び実行計画の策定	4	2	2	2	10	C	O
		7. 統合プロジェクトの管理	4	2	2	2	10	Or	O
		8. 統合プロジェクトの移行判定	4	2	2	2	10	Q	O
	ⅱ. システム統合に係るリスク管理態勢のあり方	1. システム統合に係るリスク管理体制の整備	3	4	2	2	11	Or	O
		2. システムの移行判定	3	4	2	2	11	Q	O
	合計		38	24	20	20	102		
Ⅱ. 協調したシステム統合リスク管理態勢のあり方	ⅰ. セキュリティ管理体制の整備	セキュリティ管理体制の整備	4	2	1	2	9	R	O
	ⅱ. 協調した事務リスク管理態勢のあり方	1. 管理者の役割	2	2	1	4	9	R	O
		2. 事務部門の組織整備	2	2	1	4	9	Or	O
		3. 用語の統一と事務規定の整備	2	2	1	4	9	Op	O
		4. 金融商品・サービス体系の整備	2	2	1	4	9	Op	O
		5. 営業部店網の整備	2	2	1	4	9	Or	O
		6. 顧客データの整備	2	2	1	4	9	Op	O
		7. 営業部店における対応	2	2	1	4	9	Or	O
	ⅲ. 協調したシステムリスク管理態勢のあり方	1. 管理者の役割	2	4	1	2	9	R	O
		2. 企画・開発・移行の体制	2	4	1	2	9	Or	O
		3. システム開発の管理	2	4	1	2	9	Or	O
		4. 規定・マニュアルの整備		4		4	8	−	O
		5. テスト等	2	4	1	2	9	Q	O
	ⅳ. 協調した業務運営態勢のあり方	1. 運営体制の明確化	2	2	1	4	9	−	O
		2. 業務運営の検証	2	2	1	4	9	Q	O
	ⅴ. 外部委託業務管理態勢のあり方	外部委託業務管理	2	4	1	4	11	−	O
	合計		32	44	15	54	145		
Ⅲ. 不測の事態への対応		1. 統合計画遅延時の対応	4	3	1	3	11	R	O
		2. コンティンジェンシープランの整備	4	3	1	3	11	R	O
		3. 統合日前後における不測の事態への対応	4	3	1	3	11	R	O
	合計		12	9	3	9	33		
Ⅳ. 監査及び問題点の是正	ⅰ. 内部監査	1. 内部監査体制の整備	4	2	1	3	10	Or	O
		2. 内部監査の手法及び内容	4	2	1	3	10	Or	O
	ⅱ. 第三者機関による評価	第三者機関による評価の活用	4	2	1	3	10	Or	O
	合計		12	6	3	9	30		