ディスカッション・ペーパー

金融機関のITガバナンスに関する対話のための論点・プラクティスの整理（案）

平成 31 年３月

金融庁
Financial Services Agency

目次

Ⅰ. はじめに

金融機関のビジネスは、ITシステムなくして成り立たない情報装置産業であり、金融機関間で接続され、ネットワーク化した重要インフラとなっている。

1990年代の金融機関においては、金融商品・サービスが多岐に広がり、業務プロセスも複雑化する中、ITシステムも巨大化、複雑化し、情報量、処理量も増大するとともに、システムのライフサイクルに応じて企画、開発、管理、運営ごとに業務が細分化し、外部に委託する業務も増えていった。

こうした金融機関のITシステムの進展に伴い、情報セキュリティを含むシステムリスク[1]も広範囲なものとなり、管理態勢の充実・強化の必要性が高まっていたことから、平成11年にシステムリスク管理態勢に係る検査マニュアルを策定した。また、同時期に、システム統合を伴う金融機関等の経営統合が進展し、システム統合リスク[2]に係る管理態勢の重要性も高まったことを鑑み、平成14年に「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」を策定した。

これ以降も、金融機関においては、IT技術の進展に伴い、ITシステムへの依存度はますます高まり、システムリスクもさらに多様化してきたが、システム部門から組織全体で対処すべき課題としてシステムリスク管理に係る実務を積み重ねてきた。

一方で、金融を巡る環境は、人口減少・高齢化の進展や、低金利環境の長期化等により厳しい状況が続いている。こうした中にあっても、金融機関が利用者ニーズにあった金融サービスを引き続き提供していくには、自らの体力に応じたコストの下、経営戦略を実現させるための効果を適切に生じさせるITシステムにしていくことが不可欠となる。

また、近年、デジタライゼーションの動きが加速的に進展し、電子決済等代行業者、仮想通貨交換業者等の新たなプレイヤーが金融分野に進出しており、今後、利用者の様々なニーズに対応したワンストップサービスを目指すプラットフォーム企業等も金融分野で登場しうると指摘されている。こうした中、金融機関において、情報の利活用を含むデジタライゼーションを活用した顧客起点のビジネスモデルへの変革の動きも進むと考えられる。

このように、金融機関では、ITシステムについて、システムリスク管理の対象とするのみならず、自らの経営理念を実現するために経営戦略と連携させていくことが強く求められるようになっている。当局においても、従来のシステムリスク及びシステム統合リスクにかかる管理態勢のモニタリングに留まらず、ITガバナンス[3]をいかに有効に機能させているかについて、金融機関と対話していく重要性が高まっている。

---

[1] システムリスクとは、コンピュータシステムのダウン又は誤作動等、システムの不備等に伴い金融機関が損失を被るリスク、さらにコンピュータが不正に使用されることにより金融機関が損失を被るリスクをいう。

[2] システム統合リスクとは、システム統合における事務・システム等の統合準備が不十分なことにより、事務の不慣れ等から役職員が正確な事務を誤り、あるいはコンピュータシステムのダウン又は誤作動等が発生し、その結果、顧客サービスに混乱をきたす、場合によっては金融機関等としての存続基盤を揺るがす、さらには決済システムに重大な影響を及ぼすなど、顧客等に損失が発生するリスク、また統合対象金融機関等が損失を被るリスクをいう。

[3] 本書では、経営者がリーダーシップを発揮し、IT と経営戦略を連携させ、企業価値の創出を実現するための仕組みを「IT ガバナンス」としている。

そこで、本文書では、金融機関のITに関する対話のあり方について整理するにあたり、従来のシステムリスク及びシステム統合リスクに係る管理態勢に先立ち、ITガバナンスの論点を取り扱うこととした。

II. 本文書の目的・位置づけ

金融庁では、金融モニタリング有識者会議が公表した「検査・監督改革の方向と課題」（平成29年３月）を踏まえ、検査・監督全般に共通する基本的な考え方と進め方を整理した「金融検査・監督の考え方と進め方（検査・監督基本方針）」を、意見募集の手続を経て公表した（平成30年６月）。今後、この検査・監督基本方針を踏まえ、個々のテーマ・分野ごとのより具体的な考え方と進め方を、議論のための材料であることを明示した文書（ディスカッション・ペーパー）の形で示すこととしている。

検査・監督基本方針は、金融行政の目標について、「金融システムの安定と金融仲介機能の発揮、利用者保護と利用者利便、市場の公正・透明と市場の活力の両立という基本的な目標の実現を通じて、企業・経済の持続的成長と安定的な資産形成等による国民の厚生の増大という究極的な目標を実現すること」と整理している。

これまで金融機関の IT システムについては、金融システムの安定と利用者保護の観点から、システムリスク管理態勢及びシステム統合リスク管理態勢を中心に扱われてきた。

本文書では、金融機関による金融仲介機能の発揮や健全性の確保を促していく上で、経営管理の状況等についても実効性のあるモニタリングを行うことが必要であるとの観点から、その一環としての IT ガバナンスについての考え方と進め方を示すとともに、従来のシステムリスク管理態勢及びシステム統合リスク管理態勢についての考え方についても整理している。

なお、サイバーセキュリティについては、「金融分野におけるサイバーセキュリティ強化に向けた取組方針について」のアップデート版を平成 30 年 10 年 19 月に公表しており本文書では扱っていない。

本文書の公表後も、重点的にモニタリングを行った特定の課題等について、その結果や今後の課題・着眼点等を必要に応じ公表するとともに、それを踏まえて、必要に応じ本文書の内容を充実させることも想定している。

本文書は、平成31年４月15日までの間、意見募集の手続に付し、広く意見を求める。ただし、手続期間中もその後も、金融機関や利用者をはじめとした幅広い関係者との議論を行い、継続的な改善に努めていく。

なお、検査・監督基本方針では、平成 30 年度終了後（平成 31 年４月１日以降）を目途に検査マニュアルを廃止する予定としている。

検査マニュアルには、システムリスク管理態勢及びシステム統合リスク管理態勢に関

するチェックリストが示されており、金融機関では、これを踏まえた実務が積み重ねられてきた。検査マニュアルの廃止は、これまでに定着した実務を否定するものではなく、金融機関が現状の実務を出発点に、より良い実務に向けた創意工夫を進めやすくすることを目的としている。

したがって、本文書も、より良い実務に向けた対話の材料とするためのものであり、検査や監督において、本文書の個々の論点を形式的に適用したり、チェックリストとして用いたりすることはしない。また、本文書を用いた対話にあたっては、金融機関の規模・特性を十分に踏まえた議論を行う。

本文書は、主として預金等受入金融機関や保険会社を対象としているが、これ以外の金融サービスを提供する企業が活用することを妨げるものではない。

III. ITガバナンスの高度化の必要性

１．従来の取組み

従来、金融機関のシステムリスク管理については、システム企画・開発・運用・管理、情報セキュリティ管理の局面ごとの管理態勢を中心とした、いわゆるITガバナンスを支えるITマネジメント（IT管理）に焦点を当てており、金融機関においては、システムの安定性の確保に向けた実務が積み重ねられてきた。

この一方で、金融機関の中には、ITシステムの課題認識として、システム部門・システムリスク管理部門における既存システムの維持を主眼として、システム統合やシステム障害等の個別問題への対応に留まる傾向があるところもみられた。

また、金融庁は、重要なリスクに焦点を当てた検証や、問題の本質的な改善に繋がる原因分析・解明等を目指してきたが、個別事案の部分的な事項の事後検証に焦点を当てた従来の検査姿勢が金融機関の上記の対応を助長し、内部管理の合理性・効率性の追求を阻害している面もあった。

２．環境の急速な変化及び金融機関の活動

金融を巡る環境は、人口減少・高齢化の進展や、低金利環境の長期化等により厳しい状況が続いている。このため、金融機関が利用者ニーズにあった金融サービスを引き続き提供していくには、ITシステムについても、自らの体力に応じたコストの下、経営戦略を実現させる上で適切かつ効果的な形で構築していくことが強く求められている。

また、金融機関の中には、自身で、あるいはフィンテック企業等と協業することで、イノベーションを活用した、利用者利便の向上に資する金融商品・サービスを提供する動きも出てきている。

３．企業価値を創出するITガバナンスの必要性

前述のような環境において、金融機関のIT戦略は今や金融機関のビジネスモデルを左右する重要課題となっており、さらには金融機関の将来像にも繋がる経営課題となっている。金融機関においては、経営戦略をIT戦略と一体的に考えていく必要性が増している。

こうした観点から、経営者がリーダーシップを発揮し、ITと経営戦略を連携させ、企業価値の創出を実現するための仕組みである「ITガバナンス」が適切に機能することが金融機関にとって極めて重要となっている。

仮にITガバナンスが適切に機能しなかった場合、

- ITマネジメントが阻害された結果、システムの安定稼動が損なわれる事態に繋がる可能性がある、
- 厳しい経営環境におかれているにもかかわらず、経営戦略を踏まえたITシステムのあり方を検討していないために、自らの体力に見合わない多額のシステムコストが放置されている場合には、将来的な健全性に悪影響が生じるおそれも危惧される、
- 非金融からの新たなプレイヤーに対抗すべく適切にITを活用した経営戦略を立てようとしても、企業文化や人財戦略を含めたビジネス・業務の円滑な転換を図る上で業務上の混乱が生じる、

といったことが懸念される。

このように、ITガバナンスは、利用者利便の観点だけでなく、金融システムの安定や、金融業を総体としてデジタライゼーションを適応させていくといった観点からも金融機関の経営にとって必要不可欠な仕組みとなっており、それぞれの課題に応じた形で金融機関と対話していく必要性が生じている。

Ⅳ. 金融機関におけるITガバナンス

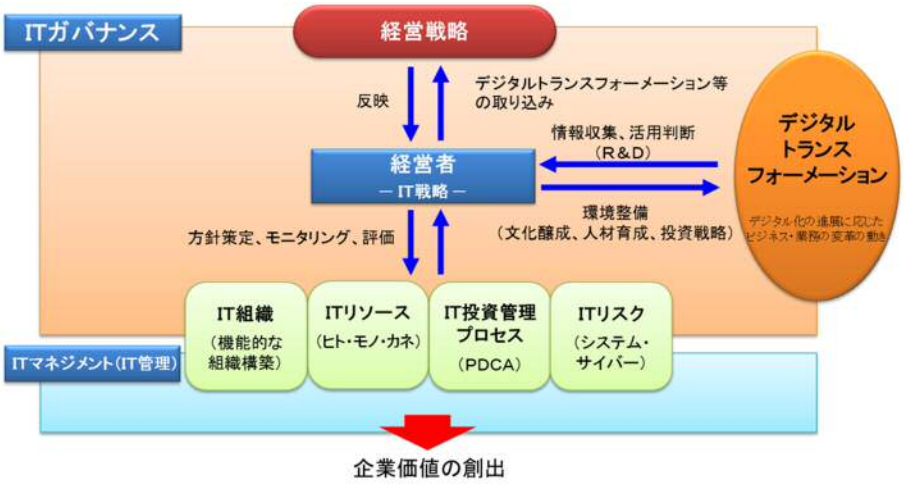
１．ITガバナンスに関する考え方

前事務年度において、金融機関と対話していくべきITガバナンスの概念を整理すべく、主な業態（主要行等、地域銀行、大手生損保）のいくつかの金融機関との対話や有識者に対するヒアリングを重ねた結果、ITガバナンスの概念として、図表１のような姿を公表した。

従来のシステムリスク管理で対象としていたシステムの安定稼働に向けたITマネジメントに留まらず、金融機関が持続可能なビジネスモデルを確保する上で必要となるITと経営戦略の連携を中心にすることや、昨今のデジタル化の進展に応じたビジネス・業務

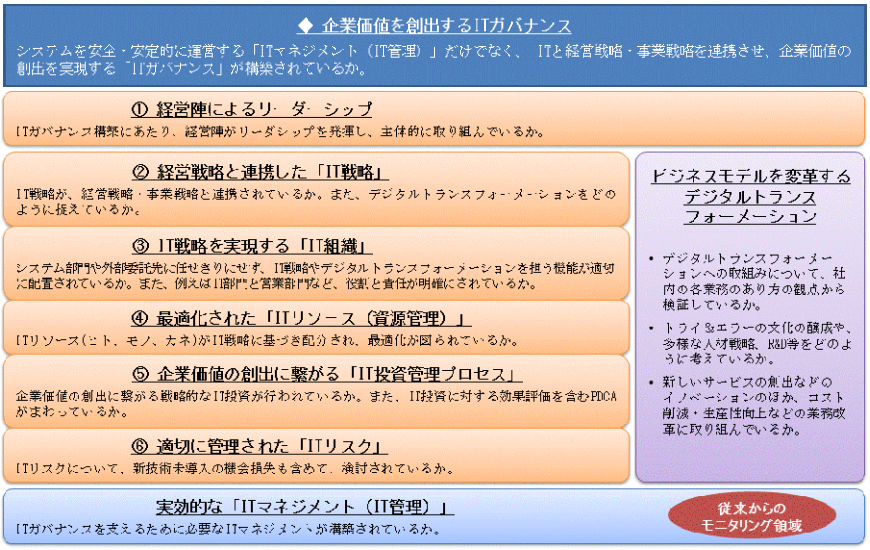
の変革の動きである「デジタルトランスフォーメーション」について、取捨選択の上、必要に応じて、経営戦略に取り込むことなどを想定したものである。

図表１「IT ガバナンスの概念イメージ」



こうした概念整理の下で、金融機関との対話に向けた論点を図表２のように整理し、有識者や金融機関との議論を重ねた。この結果を踏まえ、今回、IT ガバナンスに関する考え方や着眼点として整理した。

図表２「IT ガバナンスに関する考え方や着眼点」



２．深度ある対話に向けた基本的な考え方・着眼点

（１）経営陣[4]によるリーダーシップ

前述のように、人口減少・高齢化の進展や、低金利環境の長期化等により金融を取り巻く環境は厳しい状況が続く中、金融機関は IT システムについても、自らの体力に応じたコストの下、経営戦略を実現させる上で適切かつ効果的な形で構築していくことが強く求められている。

このため、金融機関の経営者は、自らの体力と進むべき経営戦略を踏まえて、あるべき IT システムの姿を率先して検討していくことが求められている。

さらに、デジタライゼーションが加速度的に進展する中、競合する事業者が、イノベーションを活用した利用者利便の向上に資する金融商品・サービスを提供する中、自らの経営戦略を検討する上では、現下のデジタルトランスフォーメーションで生じている動きや新たなサービスについても適切に把握した上で、採否を取捨選択していくことも不可欠となっている。

その際、経営陣がリーダーシップを発揮し、IT と経営戦略を連携させ、企業価値の創出を実現するための仕組みである IT ガバナンスを適切に機能させることが必要となる。

経営陣は、IT リテラシーの向上に努め、IT を経営にどのように活用するか、デジタル化をどのようにビジネスモデルの変革につなげるか等、創造力を働かせて積極的に議論を行い、目指す将来像を示していくことが求められている。

（２）経営戦略と連携した「IT 戦略」

フィンテック等による金融イノベーションが進展する中、金融機関においては、経営戦略を IT 戦略と一体的に考えていくことの必要性が増している。

また、デジタライゼーションの進展に応じたビジネス・業務の変革の動きに活発になっており、金融機関によるオープン API 導入に向けた環境整備が進んでいるなど、経営戦略にデジタルトランスフォーメーションを取り込む動きも広がってきている。

こうした中、金融機関において、目指す将来像や持続可能なビジネスモデルが描かれており、強化・維持する事業分野に対して、どのように IT を利活用し、デジタルトランスフォーメーションを取り込むことなどが十分に議論され、経営戦略・事業戦略が IT 戦略と一体になっていることが重要である。

また、当初、経営戦略と IT 戦略が一体的に策定されたとしても、環境変化に応じた経営戦略の見直しを含め、IT 戦略がその時々の経営の考え方に沿ったものとして適切に機能するよう、適宜点検・見直していくことが重要である。

---

[4] 経営陣とは、経営者のほか、IT システム部門を含む内部管理部門及び事業部門の責任者を含む。職掌に応じて求められる知識・経験は異なりうる一方、今日の金融機関において、IT システムを一切用いない業務は存在しないと考えられ、本稿では、特定の部門に限らず、「経営陣」としている。

この際、既存の IT システムについて、自らの体力に応じたコストの下で経営戦略を実現させるための効果を最大化するものとなっているか等を点検し、IT システムのあり方を議論することも重要である。

（３）IT 戦略を実現する「IT 組織」

金融機関においては、従来、ユーザー部門からの要望を受けたシステム部門が一元的にシステム化対応を行う組織体制が多くみられるものの、IT 戦略やデジタルトランスフォーメーションを実現するには、人財、プロセス、IT 技術の視点から適した組織能力を構築する必要がある。

特に、IT 戦略が経営戦略と連携されたものとしていくには、システムの企画・開発・運用・管理等の判断及び責任を、経営陣・システム部門・ユーザー部門がいかに分担するかは重要であり、例えば、システム開発におけるユーザー部門の役割の明確化や人事交流等により、ユーザー部門とシステム部門間のコミュニケーションを活発化させる取組みを講じている事例も見られるところである。

また、今後、新たな金融サービスの創出やデジタルトランスフォーメーションを推進するにあたっては、全社横断的に牽引する組織体制や部門の垣根を越えてシナジー効果が生まれるような組織体制を検討することが重要と考えられる。

さらに、必要に応じて、新しいことへの挑戦の推奨や失敗の許容、アジャイル型の高速な開発手法の導入、先端人財を柔軟に採用可能な人事体系の検討や先端人財を採用しやすくする工夫といった取組みにより、IT 戦略を支えるカルチャーを醸成し、IT 組織に定着させていくことも重要となる。

（４）最適化された「IT リソース（資源管理）」

IT 戦略（アウトソース戦略含む）を実現するためには、策定した戦略に基づき IT リソースを配分し、最適化を図る必要があり、その際にはヒト、モノ、カネの観点を考慮することが重要である。

システム共同化等によりシステム部門の体制が縮小化している一方で、イノベーションの進展により専門性が高まっている中、スキルを継承する人財が不足し、次世代を担う IT 人財の育成も困難になることが想定される。他の業務部門と同様にキャリアパスを明確にし、IT 戦略の実現に必要なスキルを見据えて、IT 人財を計画的に育成していくことが重要である。（ヒトの観点）

新技術（API、AI、クラウド等）を積極的に活用し、コストを大幅に削減している事例や、自らの取引データについて商流等の付加価値を見出せる形で収集し、新サー

ビスへのデータ利活用を進めている事例等がみられており、金融機関では、セキュティ面のリスク等を踏まえつつ、新技術を導入しないことの機会損失も踏まえて、その採否を考えることが重要である。こうした中、金融機関の「密結合」構造のシステムがこれらの新技術導入の阻害要因となることも考えられ、将来的には、自らのシステム構造のあり方についての議論も排除すべきでないと考えられる。（モノの観点）

既存システムの機能を維持するために IT 予算を配賦することは重要であるが、維持・制度対応の予算を所与のものとするのではなく、あくまで自らの IT 戦略に基づきながら、他の選択肢の可能性の検討や、企業価値創出のための戦略的な投資の確保など、最適な予算配賦を行うことが重要である。（カネの観点）

（５）企業価値の創出に繋がる「IT 投資管理プロセス」

IT 投資については、ROI（Return On Investment）等の指標を用いた事前評価・事後評価を行い、実証実験（PoC）後の実用化や必要に応じてサービス自体の廃止を行うなどの PDCA を回すことが重要である。一方、戦略的な IT 投資案件の判断を行う際、短期間では ROI 目標を達成することができず、戦略的な IT 投資案件が採用されないことも考えられる。

こうしたことから、経営戦略にとって中長期的に重要な IT 投資を行う場合の評価指標・手法を確立していくことが重要となる。

（６）適切に管理された「IT リスク[5]」

IT 技術の進化やイノベーション、デジタル化の進展に応じたビジネス・業務の変革の動きが活発になっており、金融機関においては、自らの経営戦略を実現させる観点から、新たな技術やサービスについても、セキュリティ面等の新たなリスクを見極めながら、採否を考えることが求められている。

このため、既存システムを漫然と利用し続けることが、競争面はもとよりコスト面においても経営におけるリスクとなりうるとの観点から、IT 戦略策定から、個々の投資判断に至るまで、新技術等にも目を配りつつ、必要に応じて、新技術等を採用することで高まるオペレーショナル・リスク等と、採用しないことで将来得られる収益やコスト削減等の機会を逸しうるリスクを比べ、適切に判断することが重要である。

[5] ここでは、例えばクラウド等の新たなサービスの利用は、短期的にはシステム更新のコストやセキュリティ面を含む従来と異なる外部委託先管理が必要になるといったオペレーショナル・リスクがある一方、中長期的には、ランニングコストの削減や BCP 面での強靭性といった面でのメリットも考えうるところ、これらへの目配りがなされないことで、将来的に得られるメリットを逸失してしまうおそれとして「IT リスク」と表現している。形式的に、定量的な測定や、投資判断時の評価項目への追記を行うというよりも、実質的に検討・判断において意識されるべきものと考えられる。

３．今後整理していくべき論点

前述の「２．深度ある対話に向けた基本的な考え方・着眼点」では、金融機関全般を対象としているが、今後、次の領域に焦点を当てた IT ガバナンスについても、有識者や金融機関との議論を重ねながら、より良い IT ガバナンスに向けた金融機関との対話のあり方を検討していく。

- 地域銀行における共同センターと自行の IT 戦略・IT ガバナンスのあり方
- メガバンクや大手生損保等のグローバルにビジネスを行う金融機関におけるグローバル IT ガバナンス
- 上記のほか、デジタライゼーション等による金融業の変化に合わせたモニタリングのあり方

４．金融機関との対話の基本的な進め方

当局のモニタリングについては、次のような進め方で金融機関との対話を実効的に行うことを基本的に想定している。

（１）多様で幅広い情報収集

金融機関との間で IT ガバナンスについて対話していくにあたっては、当局として、金融業界に直接関係があるものに限らず、広く情報収集し、常時知見の集積に努めることが求められる。具体的には、①情報の利活用やデジタルトランスフォーメーションに向けた金融・非金融における取組み、②国内外の IT 技術等に関する動向、③フィンテック企業や金融業態における IT システムに関する取組みの状況、④金融業態それぞれにおいて経営戦略の議論の繋がりうる事業環境等に関する情報、⑤海外当局等における議論の動向、⑥経済・社会環境全般の変化等について、感度良く、適時に情報を収集していく必要がある。

また、金融機関との間においても、日常のモニタリングにおいて、一般に、経営陣や社外取締役、内部監査の担当者を含む金融機関の幅広い役職員との面談等を通じてビジネス動向や内部管理上の問題意識を把握する際に、IT システムに対する姿勢や取組みも含めて、意見交換を行っておくことも情報収集の基礎となる。

（２）ベスト・プラクティスの追求に向けた対話

IT ガバナンスに関する対話においては、原則として、金融機関がベスト・プラクティスの実現に向けて主体的に創意工夫を発揮することができるよう、対話に取り組む

が、具体的には、課題に応じて対話のあり方も変わっていく。

例えば、

① IT マネジメントが阻害された結果、システムの安定稼動が損なわれる事態に繋がる可能性がある場合（利用者保護に関わる場合）には、当該金融機関のシステムリスク管理のあり方について対話することになる一方、

② 厳しい経営環境におかれているにもかかわらず、経営戦略を踏まえた IT システムのあり方を検討していないために、自らの体力に見合わない多額のシステムコストが放置されている場合には、将来的な健全性に悪影響が生じるおそれも危惧される場合（将来的な健全性に関わりうる）等には、当該金融機関との間での将来の健全性の議論の一環として対話することになるほか、

③ 非金融からの新たなプレイヤーに対抗すべく適切に IT を活用した経営戦略を立てようとしても、企業文化や人財戦略を含めたビジネス・業務の円滑な転換を図る上で業務上の混乱が生じる場合は、金融機関との間で業界としてのベスト・プラクティスの姿に関する対話が中心となると考えられる。

また、当局としては、水平的レビュー等を通じて把握した幅広い金融機関の特徴ある取組みや海外当局との情報交換等を通じて得た海外金融機関のベスト・プラクティスについての知見を、営業上の秘密に留意しつつ、金融機関に共有し、金融機関の自主的な変革のためのきっかけとなるよう取り組む。

（３）対話にあたっての留意点

モニタリングの中で、ビジネスモデル・経営戦略・IT ガバナンス等を理解した上で、それらを踏まえた対話等を重視するとしても、ビジネスモデル・経営戦略等自体は、金融機関の自主的な経営判断に委ねられるものであることから、金融機関自身の判断を尊重する必要がある。

また、対話に際して、金融機関に過度な負担が生じないように配慮する必要がある。金融機関からの情報収集についても、モニタリングにおける活用状況等を踏まえ、定期的な提出資料の内容・提出の頻度を見直すことも重要であると考えられる。

（４）当局の問題意識の発信

対話の結果として得られた有益な気づきや問題意識（問題事案から得られた教訓や先進的取組み事例の紹介を含む）については、対話の対象となった金融機関へのフィードバックに加え、金融レポートや業界団体との意見交換等の場を通じて対外的に発信していく。また、重点的にモニタリングを行った特定の課題等について、その結果や今後の課題・着眼点等を必要に応じ公表していく。

さらに、IT ガバナンス等の検討を要すると思われる課題が見つかった場合には、関係する部局や省庁と情報共有や意見交換を行う。

（５）モニタリングに関する態勢整備

実効的なモニタリングを行うためには、それを実施する当局側の態勢整備も必要となる。例えば、金融機関のビジネス、経営管理、リスク分析、IT 等に関する知識のみならず、国内外の動向・事例を含む多様で幅広い情報を収集・分析し、金融機関の潜在的リスクや課題を抽出する能力、物事の軽重を判断できる能力及び金融機関の経営陣と十分なコミュニケーションを図ることのできる対話力を持つ人財の育成や採用が重要となる。

あわせて、個別金融機関や各業態についての知見と、IT ガバナンス等に関する知識及び経験を、当局全体として高い水準で保持し、それらを十分に活用できる組織の態勢及び文化を醸成していくことが重要となる。例えば、内外の重要な問題事例についてケース・スタディとしてまとめ、考え方を深める材料とし、また、モニタリングの過程で得られた各種情報等を適切に蓄積し、将来のモニタリングに有効に活用できる態勢を整備していくことなどが考えられる。

Ⅴ. 従来のシステムリスク管理

１．検査マニュアル廃止への対応

（１）IT マネジメント（IT 管理）分野に関する取り扱い

前述の IT ガバナンスの概念イメージ（図表２）で整理されている IT マネジメント（IT 管理）は、金融機関の業務の健全性及び適切性の観点から重要なものとなっている。こうした背景の下、金融庁では、金融機関が対応すべき事項を整理し、環境や優先課題の変化に応じて見直しながら、検査マニュアルの「オペレーショナル・リスク管理態勢の確認検査用チェックリスト」の別紙（システムリスク管理態勢）に示し、検査・監督において利用してきた。

また、同チェックリストにおいて、検査官がさらに深く業務の具体的検証をする場合には、「安全対策基準・解説書」[6]等に基づき確認するとしていたことから、同基準・解説書も検査において利用してきた。

一方、各金融機関においても、同チェックリストや同基準・解説書が定着しており、

[6] 公益財団法人金融情報システムセンター（FISC）が公表している「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」の略称

関連する各種ガイドライン等も一般に複数存在することから、金融機関では、これらも参考にしつつ、システムリスク管理に係る実務を積み重ねてきている。

こうした中、IT 技術やデジタライゼーションの進展に伴い、新たなリスクが発生することも想定されることから、システムリスク管理態勢の整備はますます重要であるが、金融機関においては、検査マニュアルの廃止後も、一般に存在する各種ガイドライン等が活用され、より良い実務に向けた創意・工夫が積み重ねられることが期待される。

（2）システム統合・更改リスク管理分野に関する取り扱い

システム統合を伴う金融機関等（それらを傘下とする持株会社を含む。）の経営統合が合併や持株会社化等により進展する中、システム統合に係るリスクの管理態勢の充実・強化がますます重要なものとなっている。こうした背景の下、金融庁では、検査において特に留意すべき項目を整理し、着眼点を明確にしておくことが必要と考え、平成 14 年 12 月に「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」を公表し、検査・監督において利用してきた。

また、各金融機関においても、システム統合に焦点を当てた各種ガイドライン等が一般的に公表されていないことから、システム統合や更改する際の着眼点として、同チェックリストが活用されてきた。このため、金融機関からは、検査マニュアルの廃止後も何らかの基準等を残して欲しいといった要望も複数寄せられた。

こうしたことを踏まえ、同チェックリストのうち、重要な着眼点を本文書に残しつつ（後述に記載）、システム統合リスク管理態勢に係る基本的な考え方・着眼点の詳細を別添とすることとした。

図表３「検査マニュアル廃止後の IT システム全般の整理」

領域	概要	これまでのルール等	今後の対応
IT ガバナンス	IT システムを企業価値創出につなげるための仕組み	特になし	本文書にもとづく対話
IT マネジメント（IT 管理）	金融機関のシステム安定稼働を目的としたリスク管理	検査マニュアル及び検査マニュアル中で引用している FISC 安全対策基準・解説書	一般に存在する各種ガイドライン等
システム統合	システムリスク管理の一部で、合併等に伴うシステム統合のプロジェクト管理等	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	本文書に考え方・着眼点の概要を記載の上、詳細編を別添

２．システム統合・更改リスク管理に関する基本的な考え方・着眼点

（１）経営陣のリスク管理に対する協調した取組み

（経営統合に係るリスク管理態勢のあり方）

経営統合等に伴うシステム統合[7]において、事務・システム等の統合準備が不十分なことにより、事務の誤りやシステム障害等が発生した場合、顧客サービスに混乱をきたす、場合によっては金融機関等としての存続基盤を揺るがす、さらには決済システムに重大な影響を及ぼす等の可能性がある。

こうしたことから、統合対象金融機関等[8]の経営陣は、リーダーシップを発揮し、システム統合リスクだけでなく、経営統合全体に係るリスクを認識の上、管理態勢を整備することが必要である。あわせて、顧客対応を含む方針・計画、適切かつ必要な資源配分、問題点等に対する方策、業務及びシステムの移行判定等の重要な意思決定を行う場合等において、期限を優先するあまりリスクを軽視することがないよう、合理性や顧客利便・保護を十分に検討の上、より慎重に判断することが重要である。

（システム統合に係るリスク管理態勢のあり方）

整備された管理態勢の下、統括役員及び部門[9]は、事務・システム統合プロジェクトの管理状況を的確に把握し、適切な方策を講じるとともに、重要な問題点等については、経営陣に適時適切に報告することが必要である。

また、統合が遅延する等の不測の事態が生じた場合には、適切に対応できる体制を整備することが重要である。

（２）協調したシステム統合リスク管理態勢のあり方

（セキュリティ管理体制の整備）

セキュリティに係る管理者[10]は、重要データ（本番用顧客データ等）の適切な管理を行うとともに、統合対象金融機関等間におけるセキュリティ水準の差異を的確に把握し、統合後の業務を前提としたセキュテリィ水準を確保することが必要である。

また、IT 技術の進展等に伴う新たなリスクを洗い出し、リスク軽減のための適切な方策を講じることが重要である。

---

[7] システム統合・更改の範囲及び内容については、経営統合によるシステム統合、共同センターシステムへの移行、基幹システムの構築・更改等、金融機関の存続基盤に関わる様々なプロジェクトの形態が考えられる。したがって、後述の考え方・着眼点においては、システム統合・更改の内容等に応じて、「統合」部分を読み替えすることが可能である。

[8] 複数の金融機関等間でシステム統合を行う場合の全ての金融機関を指す。なお、システム移行や更改の場合は、該当金融機関となる。

[9] 統合プロジェクトを統括管理する部門の長を指す。システム移行や更改の場合は、プロジェクト全体を統括管理する担当役員等が該当する。

[10] 営業部店長と同等かそれ以上の職責を負う上級管理職（取締役を含む）を指す。なお、管理者の指示基づき担当部門の職員が行うことを妨げるものではない。

（協調した事務リスク管理態勢のあり方）

システム統合においては、単に事務の統合に限らず、金融商品・サービスや営業部店の統廃合等、影響範囲が多岐にわたることを認識する必要がある。システム統合における事務・システム等の統合準備が不十分なことにより、事務の不慣れ等から役職員が正確な事務を誤り、その結果、顧客サービスに混乱をきたすことも考えられる。

こうしたことから、管理者は、事務リスクの重要性を自覚し、関係部署と連携しながら、顧客対応を含むリスク軽減のための適切な方策を講じることが重要である。

（協調したシステムリスク管理態勢のあり方）

システム統合においては、事務・システムの準備不足が統合プロジェクト全体に与える影響が大きいことなどを認識する必要がある。システムの停止や誤作動が発生し、その結果、決済システムに重大な影響を及ぼす可能性も考えられる。

こうしたことから、管理者は、システムリスクの重要性を自覚し、関係部署と連携しながら、リスク軽減のための適切な方策を講じることが重要である。

（協調した業務運営態勢のあり方）

システム統合に伴い、システムオペレーション等も大きく変更になることが考えられるが、管理者は、業務運営が円滑に進むよう、関係部署と連携して、本番を想定した十分な訓練を実施することが重要である。

（外部委託業務管理態勢のあり方）

システム統合に際して、システム開発作業等に限らず、各種業務を外部委託することが考えられるが、管理者は、外部委託先任せにすることなく、委託者自らが主体的に関与し、委託業務に問題が認められた場合は、速やかに是正していくことが重要である。

（３）不測の事態への対応

システム統合においては、不測の事態（災害や事故・犯罪あるいは障害等）が発生し、計画通りに作業が進められなくなることや、統合日前後にシステム統合を延期することなどの可能性が考えられる。

このため、経営陣は、不測の事態に備えたコンティンジェンシープランを整備し、十分な訓練を実施するなど、適切な方策を講じることが重要である。

（４）監査及び問題点の是正

（内部監査）

システム統合に関する監査においては、内部監査部門が、統合プロジェクトのリスク管理状況を把握した上で、問題点が統合計画に与える影響やリスク管理態勢の実効性といった観点から、適切な頻度で内部監査を行い、重大な問題点が認められた場合は、代表取締役や取締役会が適切な措置を講じることが重要である。

（第三者機関による評価）

システム統合に係る重要事項の意思決定に際しては、第三者機関による評価を、その限界も見極めつつ、効果的に活用することも考えられる。第三者機関による評価の結果、重大な問題等が認められた場合、取締役会は適切な措置を講じることが重要である。

３．検査・監督の基本的な進め方

当局の検査・監督については、次のような進め方でリスクベースでのモニタリングを実効的に行うことを基本的に想定している。

（１）個別金融機関の実態把握

かつて検査で行われていたようなチェックリストに基づく全金融機関に対する一律で網羅的な検証では、画一的な結果に陥ってしまうため、金融機関毎にリスク特性、経営管理状況、システムリスク・システム統合リスク管理状況等の実態把握を行い、最低基準に抵触する蓋然性を把握することを重視する。特に利用者保護に与える影響の大きい金融機関については、より深い分析、密度の高い対応を行う。

（２）モニタリングの実施

モニタリングにあたっては、モニタリングの対象とする金融機関、モニタリングで検証を行う問題の範囲、モニタリングの具体的手法等の方針を定める必要がある。

モニタリングの対象とする金融機関は、リスクが高いと考えられる金融機関や、今後リスクが高まる可能性がある金融機関を中心に選定する（当局の予見が困難な問題事象が生じている可能性が高まっている場合を含む）。

モニタリングで検証を行う範囲についても、リソースの制約を踏まえれば、リスク

が高いと考えられる領域や、今後リスクが高まる可能性がある領域を中心に効率的に行う必要がある。

モニタリングの進め方は、既存の情報を分析して一定の着眼点や仮説を検討する必要がある一方、モニタリングの実施自体は、予断を持つことなく、双方向の対話や議論を通じて、事実に基づく合理的な根拠を前提として行い、かつ、検証結果に対する金融機関の真の理解や納得感を得るように努める必要がある。

もっとも、金融機関の経営陣において、システムリスク・システム統合リスク管理が適切に行われていない場合には、その経営に重大な影響をもたらし、またその信頼を大きく毀損するような事案が発生し得る。

当局による金融機関のモニタリングの基本的な目的は、多様で幅広い情報収集等を通じてリスクの顕在化に関する端緒や気づきを得た際に、それを金融機関と共有することにより、金融機関の企業価値を大きく毀損するような事案の発生を未然に防止することにある。

以上