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

第2版（案）

2023 年 4 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・デジタル技術の進展に伴い、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システムを整備・維持していくことが不可欠となる。

また、IT・デジタル技術の進展によって、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、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登場し始めている。今後、金融機関において、デジタル技術を活用した顧客起点のビジネスモデルへの変革がより一層進むものと考えられる。

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。

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、

---

[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。

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」（2017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（2018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。

本文書の初版を 2019 年６月に公表した後、2020 年から 2022 年にかけて、IT ガバナンス等に関する調査結果レポートと事例集を毎年作成し、公表した。2022 年 6 月には、メガバンク及び地域金融機関の DX（デジタルトランスフォーメーション）[4]に関する取組みや IT 人材の確保・育成等を重点テーマとして対話を行い、今後の課題等を含め、その調査結果を公表した。

また、2022 事務年度においても、金融機関と IT ガバナンスの発揮に向けた建設的対話を行った。本文書初版の公表後、当時、整理すべきとされた論点は、その後の年次の調査結果レポートで議論したうえ、DX の取組みに相応の進捗が見られるなどの状況の変化があったことから、今回、本文書に DX の考え方・着眼点を盛り込み、その内容を充実させることとした。

2019 年 12 月に廃止された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

[4] デジタルトランスフォーメーションとは、デジタル技術を活用して、顧客や社会ニーズをもとにサービスやビジネスモデル等を変革し、競争上の優位性を確立することを指す。広義で解釈されることも多く、デジタル化、デジタイゼーション、デジタライゼーションと混同されやすいが、本来、ビジネスの変革を実質的に目指した取組みが該当する。

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。

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整備していくことが強く求められている。

上記に加え、利便性の向上だけではなく、地域経済の活性化、少子高齢化社会への対応、デジタル社会の推進などの社会的課題の解決の観点も相まって、金融機関が金融・非金融の領域を超えたサービスを拡充し、地域のデジタル化支援を行うことが求められるようになるなど、金融業界を取り巻く環境は、大きく変化している。

こうした環境変化に対応するため、金融機関は新しいデジタルサービスの創出やビジネスモデル変革に向けた取組みを近年急速に進めている。具体的には、コロナ禍を契機に高まった非対面サービスに対するニーズを満たすとともに、既存の金融サービスに対するペインポイント[5]を解消するような顧客起点のサービス設計が求められている。

例えば、グループ外の金融機関や非金融の事業者とも業務提携し、「共創する」ことにより、各種サービスを組み合わせた利便性・付加価値の高い顧客体験を生み出したり、新規事業領域を拡大させたりする事例がみられる。こうした事業拡大の動きは、金融機関の強みである信用によって得られる顧客データや決済システムを活かした事業領域が中心となっている。さらに、金融機関が取り組んだデジタル化の知見を活かして、取引先企

[5] ペインポイントとは、顧客がサービスを利用する際に感じる課題や悩み、不満をいう。カスタマーエクスペリエンス（顧客体験価値）を向上させるには、ペインポイントを洗い出し、それを解消させることも重要である。

業の業務効率化とデジタル化を支援するコンサルティング[6]も広がっている。こうした新規事業によって金融機関の顧客に新たな付加価値がもたらされ、金融機関の企業価値が向上することは、我が国経済の持続的な好循環を実現するうえでも重要だと考えらえる。

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、企業文化や人材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社会のデジタル化の動きに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。

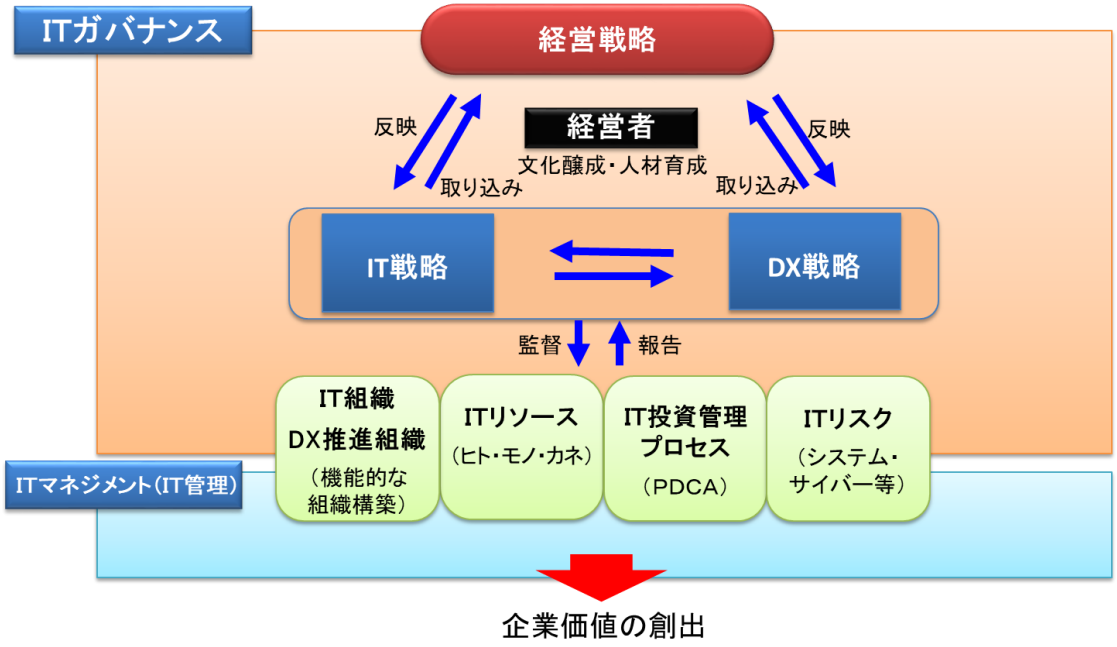
[6] 例えば、中小企業向けの ICT（Information and Communication Technology）コンサルティングが挙げられる。業務の現状分析を行い、効率化に有用なデジタルツールやクラウドサービスの提案、導入・活用支援を行うものである。取引先企業の資金繰り支援や融資、事業承継等のサービスにつながる場合もある。

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

本文書の初版に基づき、金融機関との建設的対話を行った結果を踏まえ、IT ガバナンスの概念を図表１のように整理している。

図表１．IT ガバナンスの概念



IT ガバナンスとは、経営者が IT と経営戦略を連携させ、企業価値を創出する仕組み全体を指していることから、内部統制のみならず、ビジネスの収益を向上させる成長戦略の実現も含まれている。また、新たな取組みが全て成功するわけではないので、失敗を恐れずチャレンジを促すような企業文化の醸成が本質的に重要である。

金融機関との建設的対話の結果、経営戦略、IT 戦略及び DX 戦略の関係について、グッドプラクティスを以下のとおり導出した。まず、金融機関が持続可能なビジネスモデルを確立するための経営戦略（全社的な事業戦略含む）が策定され、将来に向けた事業ポートフォリオの見直し、カルチャーの変革、IT・デジタルの素養を持った人材の育成方針等が明確になる。それと連携する形で基幹系システム更改や次世代システムアーキテクチャ等の方針を定めた IT 戦略が決定され、さらに経営戦略と IT 戦略に基づいて、既存業務の革新やビジネスモデル変革等の DX 戦略[7]が計画される。一方で、DX 戦略を実現する

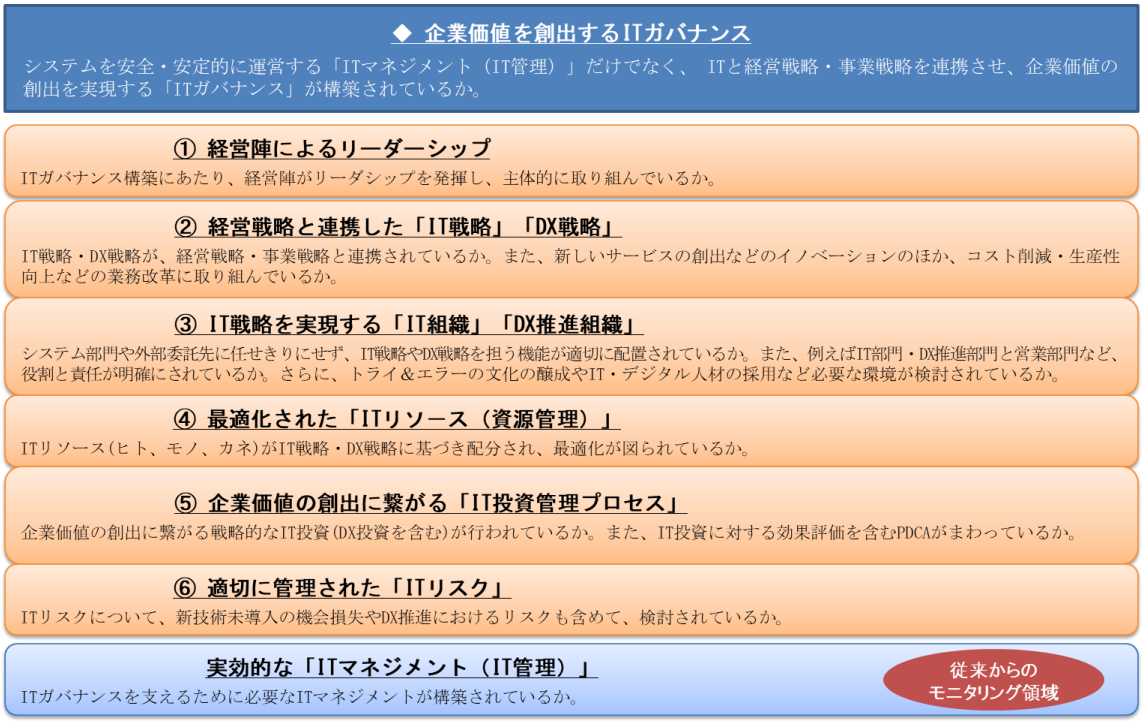
[7] DX 戦略とは、収益性向上やビジネスモデル変革等の経営戦略を実現するため、デジタル技術を活用した業務革新や事業開発等に関する方針・計画を定めたものをいう。IT 組織が策定する IT 戦略とは異なり、将来の事業領域を構想しながら、各段階で必要なリソース、新技術の実装方法、収支等について総合的に策定することから、明確に区別して定義した。ただし、図表１のように、経営戦略、IT 戦略及び DX 戦略は相互に作用し合う関係にあり、あえて区別せずに一体的に策定される場合もあ

ために、インフラやデータ活用基盤のあり方といった IT 戦略が決まる場合もある。

加えて、IT ガバナンスには、IT 組織・DX 推進組織[8]、IT リソース、IT 投資管理プロセス、IT リスクが要素として含まれるが、これらは、対話の結果に基づくと、IT 戦略と DX 戦略を実現させる上での共通する仕組みである。規模が比較的大きい金融機関では、IT 戦略は IT 部門が策定・管理の主体となる一方、DX 戦略は DX 担当部門や事業部門が中心となって推進する体制を整備し、投資を効果的に実行するプロセスを構築している。また、金融機関の規模・特性に応じて、DX を IT 戦略に含み、かつ IT 組織と DX 推進組織が一体となった組織体制の方が効率的な場合もある。

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及び IT ガバナンスに関する考え方や着眼点を図表２のように整理した。

図表２．IT ガバナンスに関する考え方や着眼点



2021 事務年度の IT ガバナンス調査結果レポートでは、DX に関して金融機関が辿っている遷移をもとに、DX の進化系をイメージしながら、そこに到達するためのロードマップを示した。また、DX の着眼点を仮置きし、取組みが先行している金融機関との対話を通じて深堀することにより、DX を成功させるために重要な要素（成功要因）について整

るなど、様々なアプローチがある。

[8] DX 推進組織とは、DX 戦略に係る案件の企画・立案、投資予算と要員の確保、プロジェクト管理、サービス設計等を主管する組織をいう。基幹系など既存システムの開発・運用・保守を担う IT 組織と責任権限が異なることから、別途定義した。

理している。足元の数年間で、非対面サービスの割合が増加し、地域金融機関においてもペーパーレス化やスマホアプリ開発、店頭タブレット等の施策が求められていることが分かった。また、メガバンクにおいては、DX に関する取組みが個別に進展し、差がつき始めている。

特に、金融プラットフォーム事業や非金融領域の新規事業、データ利活用によるサービス等は、デジタル技術の活用と外部事業者との共創がビジネスの要点となっている。例えば、AI 技術であれば、自然言語処理・画像処理・音声認識等の各分野で先端技術が数多く研究開発されており、それを製品化するベンチャー企業や実装を支援する IT ベンダーも複数存在している。非常に多い選択肢の中から、経営戦略に最も適合する製品と外部事業者を見極めて組成するには、金融機関自ら確かな知見を組織内に獲得・蓄積し、意思決定プロセスを確立しなければならない。

つまり、IT ガバナンスの整備・充実を継続的に図ることが、新しいビジネスを創造し、発展させるための仕組みとして欠かせない点を改めて強調しておきたい。また、IT ガバナンスが有効に機能しなければ、IT コストの効果を最大限に引き出せない上、収益性も含め、将来的な事業経営に悪影響が生じるおそれがある。顧客利便性と信頼性の高い先進的なサービスを提供し、企業価値を創出するため、金融機関の規模・特性等に応じた創意工夫を期待したい。

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[9]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、金融機関の経営陣は、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。

また、経営陣は、デジタル活用が顧客ニーズを起点としたサービスの提供に欠かせない手段であることについて役職員の理解を得、将来の DX の到達点を示し、組織全体を導いていく必要がある。経営陣が DX 戦略についてリーダーシップを発揮し、例えば、情報発信を続けることで、ステークホルダーの信頼と共感を得ながら、組織内の戦略の実現に向けた機運やモチベーションを高めることが重要である。

さらに、システム改革だけでなく、業務改革と人事制度改革も併せて進めることで、デジタル活用のアジリティ確保や全社的な意識変革が促される。DX に関する取組みが

[9] 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。

全て成功するわけではないので、失敗を恐れずチャレンジを奨励する企業文化が求められている。

一方、サイバー空間における脅威が増大する中、金融機関に対するサイバー攻撃によって、顧客情報の漏えい、顧客資産の不正出金や業務停止などの被害が発生している。DX を安心・安全に推進していくには、デジタル活用に伴うサイバーリスクを評価するとともに、リスクに見合ったサイバーセキュリティ管理態勢を構築し、適切にリスクコントロールすることが求められる。

経営陣は、IT リテラシーとデジタルリテラシーの向上に努め、IT・デジタル技術を経営にどのように活用してビジネスモデル変革につなげるのか、デジタル活用の恩恵を享受するうえでの前提となるセキュリティをどのように確保するのか、IT リスク（サイバーリスクを含む）をどのように管理するのか等、バランスを考えながら創造力を働かせて議論を行い、目指す将来像を明らかにしていく必要がある。[10]

（２）経営戦略と連携した「IT 戦略」・「DX 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。

IT 戦略では、基幹系システムの更改、情報系システムの高度化、クラウド活用、情報セキュリティ等の方針を定めるとともに、ビジネスと DX 推進を支えるシステムアーキテクチャのあり方[11]を検討することが重要である。システムアーキテクチャの将来像として、メインフレームとオープン系基盤、オンプレミス[12]とクラウド等の最適な組み合わせを示し、さらにデータ活用基盤・API 連携等についても検討することが考えられる。

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、適宜見直していく必要がある。

また、デジタル化の進展による社会環境変化に対応するため、経営戦略と IT 戦略に基づいて、メガバンクや大手の地域金融機関では DX に関する戦略を策定する動きがみられる。DX 戦略では、収益性の向上やビジネスモデル変革に向けて、チャネル改革、業務革新、店舗のデジタル化、顧客接点拡大、商品・サービスのクロスセル、新規事業開発といった戦略領域を定め、中長期を見据えたロードマップを策定すること

---

[10] DX 推進に伴う新たなリスクへの備え、経営層のリーダーシップの発揮など、金融機関に期待する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（Ver. 3.0）」（金融庁、2022 年 2 月、https://www.fsa.go.jp/news/r3/cyber/torikumi2022.html）を参照。

[11] 老朽化したレガシーシステムを使い続けると、維持保守費の増大につながるだけでなく、DX の足枷となる可能性がある。ビジネス要件の変化に柔軟かつ迅速に対応できるよう、システム構成を全体最適化することなどが考えられる。なお、システム再構築の手法には、リホスト、リライト、リプレース等があるが、中長期の IT コスト、開発言語の将来性、ブラックボックス化の解消、ハードウェア価格の動向といった観点で多面的に評価して選択することが重要である。

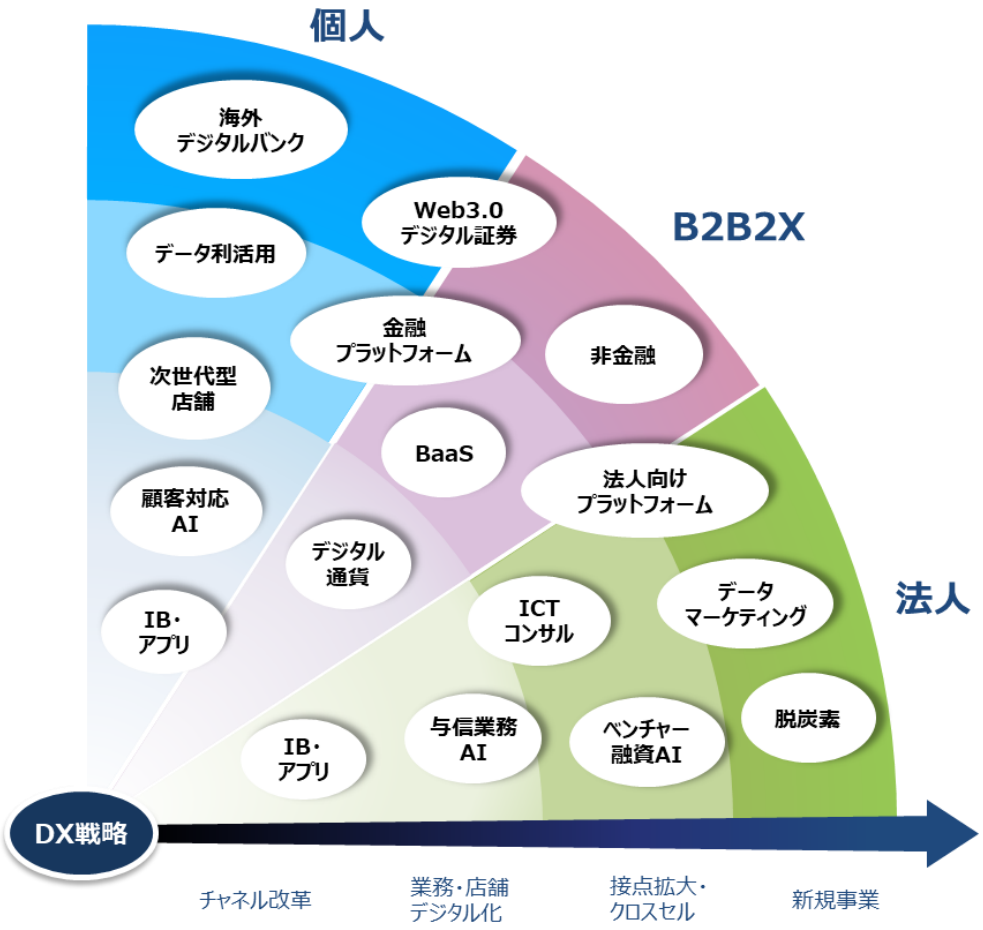
[12] システムの稼働に必要なソフトウェア、ハードウェア（サーバーやネットワーク等）を自社で保有する利用形態のこと。

が重要である。

図表３のように金融・非金融、個人向け・法人向けといったサービスの境界が曖昧になってきていることから[13]、これを上手く融合させることで、新たなビジネス創出を金融機関は模索している段階にある。絶え間なく変化し続ける顧客のニーズとペインポイントを常に調査分析し、実装に必要なデジタル技術を持つ IT ベンダーや相応の顧客基盤を有する事業者と手を組むことが考えられる。

投資余力が限定的な場合、単独で実行すると過剰投資になる恐れがある。そうした状況下では、他行と連合して共通要件を見定めつつ、各種機能の共同利用や適したプラットフォームに相乗りすることが考えられる。

図表３．DX による業務革新と事業領域の拡大イメージ



※B2B2X：企業が他の企業へサービスを提供し、サービスを受けた側の企業がさらに消費者（BtoBtoC）や企業（BtoBtoB）へ提供する取引形態のこと

[13] 例えば、BaaS（組込型金融）は、金融機関が銀行口座関連のサービスを提供することで、非金融の事業者が抱える最終消費者（エンドユーザー）に組込型金融を実現するものである。 金融機関は提携先の事業者を通じて、これまで接点のなかった新たな顧客層を獲得することができる。最終消費者が個人の場合もあれば、法人の場合やその両方の場合もあり、金融機関の強みを活かした総合的なサービスの開発、共創が始まっている。

（３）IT 戦略を実現する「IT 組織」・「DX 推進組織」

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 DX 戦略を実現するには、企画・開発を担う責任者、組織（部門、子会社等）、会議体のあり方、IT・デジタル人材と情報セキュリティ人材[14]を確保・育成する観点から、適した組織能力を設計し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。

今後、新たな金融サービスの創出や DX を推進するにあたっては、経営陣を中核にした推進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。また、IT・デジタル技術を活用した既存事業の構造改革では、事業部門に可能な限り権限委譲し、小さく始めて改善を繰り返すアジャイル・アプローチによって、柔軟かつ迅速に対応する事例がみられる。そうした場合には、IT 組織がアジャイル開発の手法やポリシー、ツール選定、開発環境等について標準化を行い、各事業部門で管理不能な開発にならないよう支援する必要がある。

DX は迅速なソリューションの提供が鍵であるため、IT 子会社や IT ベンダーと共同するなどして、案件の企画から実装まで短期間で行える体制作りが重要である。企画・設計のみならず、プロジェクト管理や開発・テスト工程を金融機関が主体的に実施するなど、内製化の動きも広がっている。

さらに、DX 推進には、金融業務と IT・デジタルの知識を習得した様々な職種の専門人材が必要なことから、スキル定義とキャリアパスの明確化、専門人材の報酬体系や教育研修など人事制度上の工夫が求められている。新しい事業への挑戦の推奨やアジャイル開発手法の導入、AI・データサイエンス等に携わる先端人材の中途採用といった取組みにより、IT 戦略と DX 戦略を支えるカルチャーを醸成し、組織全体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

[14] 情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための役割を担う人材を指す。

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した一方で、IT・デジタル技術や開発手法の進展により専門性が高まっている中、スキルを継承して次世代を担うIT人材が不足している。また、DX推進の中核となるデジタル人材[15]、特に金融業務とITスキルを兼ね備えた人材は獲得競争が激化していることから、中途採用で充足できなくなっている。他の業務部門と同様にキャリアパスを明確にし、IT戦略とDX戦略の実現に必要なスキルを具体的に定義し、IT人材とデジタル人材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」

戦略的なIT投資額及びそれに含まれるDX案件の投資額について、中期計画と年度予算を定め、全社的な戦略案件の起案から審議、投資意思決定までが迅速に実行できるようなプロセスを整備することが重要である。

投資後の進捗管理においては、将来収益が得られる案件や事業であれば、ROI（Return On Investment：投資収益率）等の指標を用いて評価を行い、進捗状況に応じてリソースの増強やサービスの縮小・撤退を判断するPDCA[16]を回す必要がある。一方で、実証実験（PoC）の段階や中期的な観点で対応が必要な戦略案件は、収益化の目途が立つまでの間、特性に応じたKPI（定量的指標）を設定して計画対比をモニタリングすることも考えられる。

---

[15] デジタル人材とは、DX推進において必要なスキルを習得した専門人材であり、ビジネスアーキテクト、データサイエンティスト、UI/UXデザイナー等の職種の総称である。DX推進組織のみならず、営業企画などの事業部門やIT組織にデジタル人材が所属している場合もある。

[16] PDCAとは、Plan（計画）、Do（実行）、Check（評価）、Action（対策）のサイクルを継続的に回して改善することをいう。一定金額以上の投資・進捗管理においては、慎重かつ合理的な意思決定ができる枠組みが欠かせないと考えられる。

近年、IT・デジタルの新技術がますます多様化、高度化しており、経営戦略に最も適合する技術・製品を見極めるには、研究開発と実証実験が欠かせなくなっている。一度採用すると容易に代替できない技術もあることから、最新技術の継続的な情報収集と外部専門家の活用等によって選定プロセスを強化し、確かな知見を獲得することが重要である。

また、戦略的な IT 投資の割合を増やす目的で、非戦略領域の維持保守コストを抑制・削減する取組みが広くみられる。システムの安定性・堅牢性を重視しながら、DX 戦略を支えるシステムアーキテクチャへの更改やインフラ強化を図ることが中長期の競争優位性を築くと考えられる。

（６）適切に管理された「IT リスク[17]」

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。地域社会の課題解決に向けて、取引先企業や IT ベンダーも DX に取り組んでいる状況を鑑みると、デジタルサービスの創出はあらゆる産業で一層進展するものと見込まれる。

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 戦略と DX 戦略の策定から個別案件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。

また、DX 推進におけるリスクとしては、新商品・新サービスに係るリスク、システム障害リスク、情報セキュリティリスク（サイバーリスク含む）、外部事業者との連携に伴うリスク[18]等が想定される。DX 推進の恩恵を享受するうえで、これらのリスクの低減及び管理が求められる。

まず、新商品・新サービスを検討する際には、企画・設計段階からセキュリティ要件を組み込む「セキュリティバイデザイン」を実践し、サービス全体の流れの中で、連携先も含めて脆弱性を洗い出し、リスクに見合った堅牢なサイバーセキュリティ対

[17] 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。

[18] 外部事業者との連携に伴うリスクには、経済安全保障上の懸念、マネロン・テロ資金供与リスク、パートナー事業者の撤退リスク（事業継続への影響）等が含まれる。

策を導入することが重要である。

併せて、新商品・新サービスのリスク分析では、根拠法令等コンプライアンス上の問題がないことをまず確認したうえで、リスクの洗い出しと対応策の検討、残余リスクの評価等を行う必要がある。DX 関連の新サービスは、戦略領域にある周辺システムで開発、運用、提供されることが多いため、当該システムに対するシステムリスク管理態勢の評価やクラウド活用に伴う審査等が必要になる。IT 子会社や銀行業高度化等会社[19]、外部事業者など連携先と共同でシステム障害発生時の顧客対応・業務継続・復旧体制を整備しなければならない。

個人情報・顧客情報の管理態勢についても、外部事業者に情報連携する場合には、業者側で情報漏洩等のインシデントが発生するリスクを認識し、十分な対応策を講じる必要がある。また、データ利活用による顧客への新たな価値の提案や AI 分析等が行われているが、データの品質・信頼性が低い場合には誤った出力結果となるリスクがある。蓄積した元データを適宜補正・加工することによって、セキュリティを確保しながら品質を高める必要がある。

３．その他の論点

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、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継続していく。

- 地域銀行における共同センターの次世代構想と自行の IT ガバナンスのあり方
- 大手金融機関におけるグローバル IT ガバナンス
- 上記のほか、DX 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

[19] 銀行業高度化等会社とは、情報通信技術その他の技術を活用した銀行業の高度化もしくは当該銀行の利用者の利便の向上に資する業務（または資すると見込まれる業務）を営む会社をいう。

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DX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、企業文化や人材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。

なお、対話の中で、金融機関が IT・デジタル技術を活用して新たに行おうとしている取組みに関して、規制・監督上の課題・悩みを抱えていることを把握した場合には、「FinTech サポートデスク」や「FinTech 実証実験ハブ」、「金融機関システム・フロントランナー・サポートデスク」の活用の慫慂を含め、金融法令の解釈の明確化等の支援を行うことが必要である。

（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材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」[20]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、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・デジタル技術や DX 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[21]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

[20] 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

[21] 金融機関に活用されている各種ガイドライン等として、公益財団法人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」及び「金融機関等のシステム監査基準」、情報システムコントロール協会（ISACA）の「control objectives for information and related technology（COBIT）」、経済産業省（METI）の「システム管理基準」及び「システム監査基準」などが想定される。

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	一般に存在する各種ガイドライン等を参考にしつつ、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[22]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。

[22] 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。

こうしたことから、統合対象金融機関等[23]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[24]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[25]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。

（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）

---

[23] 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。

[24] 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。

[25] 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。

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