

システムリスク管理態勢の全体最適化

—関連法令への個別対応からの脱却—

これまで金融機関では、金融庁などが定めるいくつかのガイドラインに基づいてシステムリスク管理態勢の整備を進めてきた。しかし複数のガイドラインに長期にわたって個別に対応してきた結果、管理態勢に無駄や漏れが生じているケースがある。本稿では、これらの問題点を整理した上で、全体最適化されたリスク管理態勢をどう作るべきか提言する。

システムリスク管理の現状

一般にシステムリスク管理とは、システムに係るリスクが顕在化して障害を引き起こすことを防ぐために、リスクを評価して必要なコントロール（統制活動）を実施することである。金融機関では、関連法令に対応したガイドラインやFISC（財団法人金融情報システムセンター）が中心となって策定した業界の自主基準などに基づいてシステムリスク管理態勢の整備を進めてきた。これらのガイドライン等は、法整備の動向や金融機関を取り巻く環境の変化に合わせて継続的に改定されている。

リスクには「脅威に対するぜい弱性」と「目標に対するギャップ」の2つがある。前者はシステムの「安全性」「信頼性」に対するリスクであり、後者は「有効性」「効率性」に対するリスクである。この2つの種類のリスク管理の前提として、関連法令や社内ルールについての「遵守性」が求められる。

「安全性」「信頼性」のリスク管理は、2007年に施行された金融商品取引法など各種の関連法令が施行される前から業界の自主基準の中で求められており、早い時期からリスク管

理態勢を整備したため、他業種と比べてもリスク管理のレベルは高い。

一方、「有効性」「効率性」のリスク管理は、金融庁の1997年の「金融検査マニュアル」で初めて求められたもので、「安全性」「信頼性」と比較して整備が遅れているのが現状である。

金融機関のリスク管理の問題点

金融機関では、「安全性」「信頼性」のリスク管理について、ガイドライン等に基づいて運営態勢の整備や社内ルールの作成、業務プロセスの構築などを行ってきた。しかし、同じリスクに対して複数のガイドライン等が管理態勢の整備を求めていることが原因で、次の2つの問題が生じている。

1つは、同じリスクに対するコントロールの実施が複数の社内ルールで規定されているために、複数の社内ルールの間で矛盾や不整合が生じていることである。リスクの状態に変化があった場合、当該のリスクに関するコントロールを規定したすべての社内ルールを修正する必要があるが、リスクとルールの関係を正確に把握することが難しいために修正漏れが起きやすくなっている。これを防ぐためには、ルールを整理することのほか、漏れ



なく修正するための仕組みを導入しておく必要もある。

もう1つは、システム部門の負荷が増大することである。同じリスクに対して異なる運営態勢を構築している結果、システム部門はリスクの状況を複数のリスク管理部門に報告する必要があり、その調査および報告の業務負荷が増大している。

「有効性」「効率性」に対するリスク管理にも問題がある。取り組みの開始が遅れたことに加えて、リスクが顕在化した場合の影響が「安全性」「信頼性」に比べて小さいために、そもそも取り組みの優先順位が低いことである。しかし、金融商品取引法も内部統制強化だけでなく経営戦略や事業目的の確実な遂行や業務の適正かつ効率的な遂行を求めており、「有効性」「効率性」のリスク管理態勢の整備にも積極的に取り組む必要がある。

管理態勢全体最適化の手順

金融商品取引法への対応が一段落した現在、金融機関はあらためて自社のリスク管理態勢の整備状況を見直し、全体最適を実現すべき時期を迎えている。

それは以下のような手順で進めることが効果的である。

- ①網羅性のある「コントロール基準」を作成
ガイドラインの根拠となっている関連法令に対して「遵守性」を確保するため、ガイドラインでコントロールの実施を求められてい

るすべてのリスクを網羅し、かつ重複を排除した「コントロール基準」（どういう統制をどのように実施するかを規定したもの）を作成する。

②コントロール基準の適用条件を規定

リスクを「脅威に対するぜい弱性」と「目標に対するギャップ」に分け、対応するコントロール基準の適用条件（適用単位、適用対象の情報資産）を規定する。

③コントロール基準を社内規定へ反映

ガイドラインに準拠しかつ網羅性を確保したコントロール基準に基いて、社内規定、マニュアルを策定する。

④効率的な社内ルールによる運営

コントロール基準を効率的に適用できるように社内ルールを見直す。例えば、システムリスク管理状況の報告ルール（報告する証跡の内容や、コントロールセルフアセスメントシートのフォーマットなど）はリスクの種類によらず統一する。また、金融商品取引法に対応したぜい弱性評価と、その他の法制度に対応したぜい弱性評価は同時期に実施し、それぞれのリスク管理状況の調査結果を互いに利用できるようにする。

以上のような手順で管理態勢の全体最適を実現することにより、関連法令に準拠した効果的な管理態勢の整備が可能になる。リスク管理部門では社内ルールの維持に係る負荷の削減や管理業務の効率化が、システム部門では運営業務の効率化が可能になる。 ■