わが国金融機関におけるシステムリスクの管理状況と留意点

―― 情報セキュリティ面への対応を中心として ――

考 査 局

1．はじめに

日本銀行では、かねてから金融機関の情報セキュリティを中心としたシステムリスクの管理状況[(注1)]に関心を持ち、各種のモニタリング等を行ってきた。昨年４月には、「金融機関における情報セキュリティの重要性と対応策―インターネットを利用した金融サービスを中心に―」（『日本銀行調査月報』2000年５月号に掲載）を公表し、情報通信技術（ＩＴ）の革新を背景に、システムリスクの中でも特に情報セキュリティを適切に管理する必要性が高まっている点を指摘した。その後も、情報セキュリティ面に重点を置いたターゲット考査の実施等を通じて、金融機関のシステムリスク管理状況の把握と対応促進を働きかけてきたところである。

こうした一連の活動を通じ、日本銀行としては、大手金融機関におけるシステムリスク管理の現状について、概ね適切な方向で対応が図られつつあるものと認識している。しかしながら、なお一部に改善余地が残っているだけでなく、新たな技術の導入やその活用範囲拡大に伴い、システムリスクは日々多様化・複雑化している。こうした現状に的確に対処していくためには、絶えずリスク対策を見直し、必要に応じてリスク管理体制の充実を図っていく必要があると考えられる。

そこで以下では、情報セキュリティを中心としたシステムリスク管理に関し、日本銀行が、金融機関への考査や関係者との意見交換等を通じて得た情報を踏まえ、今後の留意点を纏めた。各金融機関が、自らの抱えるリスクの大きさや費用対効果を考えながら、リスク管理の強化を図っていくうえでの参考とすることにより、金融界全体としてのレベル向上に役立つことを期待している。

2．金融機関のシステム基盤の現状と変化

まず、わが国金融機関におけるシステム基盤の現状をみると、各金融機関の業務特性やＩＴ

（注１）「情報セキュリティ」は一般に「組織固有の情報システムを正当に保護し（機密性）、真正な状態を保ちつつ（完全性）、必要時に有効に利用できる（可用性）状態を確保すること」と定義される。多くの金融機関ではこれを「システムリスク」の主体をなす部分（このほかに有効性・効率性等の視点が存在）と捉えて同リスクの一環として管理している。こうした状況を踏まえ、本稿では、情報セキュリティの問題を含め「システムリスク管理」として論じている。

投資方針等により差異があるものの、概ね下表のように整理できる(注2)。もっとも多くの場合、これら異なるシステム基盤が併存し相互に連関して動いているため、金融機関として認識すべきリスクの態様は複雑化している。

今後もＩＴ環境はめまぐるしく進化し、金融サービスに対する要求内容の高度化も続くと想定される。このため、金融機関のシステム基盤や利用技術はさらに大きな変貌を遂げていく可能性が高い。

（システム基盤の現状整理）

	カテゴリー	主なシステム	基盤として採用される背景・経緯等
コンピューターの種類に着目	メインフレーム（大型汎用コンピューター）系システム	・基幹勘定系システム（預金・為替、貸出等）	・伝統的なシステム基盤（かつてはメインフレームのみが存在）。 ・システムの信頼性優先ないし大量処理という業務特性に対応できるシステムとして選択。
	分散系システム	・資産査定・収益管理システム ・資金証券系システム	・低コストで迅速な構築が可能。 ・市場取引等の分野でパッケージソフトを導入する場合のインフラとして一般的。
ネットワークの種類に着目	クローズドネットワーク（特定の参加者のみアクセス可能なネットワーク）	・電算センター・営業店・ＡＴＭ間ネットワーク ・日銀ネット等決済システムとの対外接続ネットワーク	・高いセキュリティ水準が求められる分野での利用に有効。 ・伝統的なネットワーク。
	オープンネットワーク（不特定多数の者がアクセス可能なネットワーク）	・顧客直結型（ダイレクトチャネル）システム（インターネットバンキング等）	・24時間365日対応の不特定多数向けサービスが安価に提供可能。 ・インターネットや携帯電話がコミュニケーションインフラとして利用者の間に急速に普及。

３．システムリスク管理の基本的な枠組み

各金融機関とも、こうした状況変化に応じてシステムリスクの管理を充実・強化する必要性を認識し、今まさに対応を進めているところである。以下では、情報セキュリティを中心にシステムリスク管理の枠組みを確認したうえで、金融機関の取り組み状況を踏まえたリスク管理上の留意点について整理することとしたい。

大手銀行をはじめとする金融機関では、システムリスク管理の水準を一定以上に保つため、「リスク管理の運用サイクル」により組織的に管理しようとしている。

リスク管理の運用サイクルとは、全行的なシ

（注２）現実にはコンピューターとネットワークの種類の組み合わせによりさらに細分化されるが、大まかにいえば分散系ないしオープンネットワークを基盤としたシステムの比重が高まる傾向にある。

ステムリスク管理の基本方針や基準（これらを以下「基本方針等[注3]」という）を定め、これをシステムの開発や運用の各現場に反映していく一連のプロセスであり、一般には以下のように運営されている。

（1）基本方針等の策定・見直しと周知徹底

- 自らが抱えるシステムリスクを組織横断的に管理するため、その基本的な考え方を示すものとして、基本方針等を策定する。また、リスク分析・評価の結果や、最新のシステム技術動向を踏まえ、その有効性を定期的に点検のうえ、必要に応じ見直しを実施する。
- 併せて基本方針等を現実の業務運営面で定着させ実効あるものとするために、役職員に対する教育・啓蒙活動により周知徹底を図る。

（2）システム構築段階での対応

- システムの構築（設計・開発）段階で、基本方針等で定めた所要のリスク対策を組み込む。
- 適切なシステムリスク管理水準を確保し、システム稼働後の運用負担を軽減するためには、予めそれに必要な機能を組み込んでおくことが有効である。

（3）運用段階での対応

- システムの稼働後、基本方針等に基づいて策定された規程や手続きに従いシステムを運用する。
- 稼働済みのシステムについても、リスク分析・評価の結果やシステム基盤の変化を踏まえ、必要なリスク対策を講じる。

（4）リスクの分析・評価

- 各システムの設計や運用・利用状況が、基本方針等で定めた基準をクリアできているかといった点から、基本方針等と実態とのギャップを定期的に把握し、リスクの内容、大きさ等を分析・評価する。これによりリスクの所在を把握し、リスク対策の要否を判断する。
- こうした作業を通じて、経営陣にリスク管理の現状認識を促すとともに、人的資源の割当てや新技術の導入等を通じ、有効なリスク対策の実施につなげていくことができる。

（5）システム監査

- システム開発・運用部署や利用部署に対し、独立した内部監査部署等が業務の遂行状況を検証する。
- 検証内容としては、各部署等が基本方針等を守って事務を遂行しているか、という準拠性の検証に止まらず、現在のリスク管理体制が有効に機能しているかどうかまで踏み込むことが期待される。

以下では、こうした枠組みによるシステムリスク管理の運営上の留意点を、これまでの調査等を踏まえて解説してみたい。

4．システムリスク管理上の留意点

（1）基本方針等の策定・見直しと周知徹底

システムリスク管理の基本となる基本方針等については、ここ1～2年の間に、多くの金融

（注3）ここでいう「基本方針等」は、「セキュリティポリシー・同スタンダード」と呼ばれることが一般的であるが、実際にはセキュリティだけに止まらずシステムリスク全般にわたる内容をカバーすることが多いため、本稿ではこの呼称を使用する。

機関において整備が図られてきている。ただし、内容的には以下のような点でなお充実の余地が見受けられた。

① 基本方針等の遵守状況やリスク評価結果の検証を、どの部署が担うのかが不明確である。

② 分散系システムやオープンネットワークといった新しい技術に対応した内容が不十分である。

③ 基本方針等が各部署毎の規程・マニュアル類に反映されていない。

また、基本方針等を策定した後に、その有効性を定期的に点検する際には、以下のような点に留意する必要がある。

① リスク分析・評価やシステム監査の結果を踏まえて、基本方針等を見直す必要はないか検討する。

② 新技術を用いたシステムの採用や外部ネットワークとの接続方法変更により、自行の抱えるシステムリスクの内容に変化が生じていないかを確認する。

③ 新たな弱点が発見されたり、これを糸口に不正侵入等のリスクが顕現化することを防ぐため、最新のシステム技術の動向を極力フォローする。

なお、基本方針等を現実の業務運営面で定着させ実効あるものとするためには、役職員に対する教育・啓蒙活動を通じ、「何故これを守らねばならないか」といった基本認識を含め周知徹底することが極めて重要である。具体的には以下のような取り組みがみられた。

① 役職員各層に対する人事研修内に基本方針等に関するカリキュラムを組み込む。

② 各部署毎のシステムリスク管理者等を任命した際や、基本方針等に重要な改訂を加えた場合には、管理者等に対し基本方針等を徹底する。

③ エンドユーザーに直結する部分を抜粋し、分かり易く解説したパンフレットを作成・配布するなど、継続的に定着を図る。

（2）システム構築段階における対応

システムの構築段階における対応について、要求されるセキュリティレベルに応じて、次のような技術面・運用面に跨る対策を検討している事例がみられた。

① 認証機能、暗号化機能、不正アクセス監視機能等技術面の設計。

② 不正アクセスの検証体制等運用面の対応ルール制定。

こうした対策の実効性を担保するためには、当然のことながら、設計・開発工程やテスト段階での検証が欠かせない。この検証作業には相応のスキルと独立性が求められることから、システム部門内に専担部署を設けるなど、体制面で工夫している金融機関もみられた。

（3）運用段階での対応

メインフレーム系システムやクローズドネットワークでは、リスク対策は概ね確立している場合が多い。これに対して、分散系システムやオープンネットワークについては、アクセス管理面等において従来型のシステムリスク対策だけでは不十分な点もあり、スキルの充実を図りながら、新たな対応策を講じる必要のあるケースが多い。

以下に金融機関での取り組み事例や実情を踏まえた対応策を紹介する。

① 管理負担の軽減やスキル不足の補完

- 数多くのサーバーを導入する際に、オペレーティングシステム（コンピューターを制御する基本プログラム）等を含めその種類を極力統一している。
- オープンネットワークを利用したシステムの運行や不正アクセス等の監視業務に外部の専門業者を活用している。

② 内部牽制体制の構築

- 高権限ＩＤの利用状況を管理するため、重要ファイルへのアクセス履歴を取得し、システムの運行に従事しない部署が、不正アクセスの有無を事後検証している。

③ 関係部署で連携した障害時対応の整備

- アウトソーシングを活用したインターネット系システム等において、システム障害時に迅速な対処が可能な連絡体制を構築するとともに、広報部署等を含む関係者間で、予め対応のシナリオを整備している。

（４）リスクの分析・評価

リスク分析・評価の手法としては、リスクの所在を把握しリスク度合いをランク付けするために、各システムのリスクをその重要性と脆弱性の積（「重要性」が高く「不正や障害に対する脆弱性」の程度が大きいほど、リスクが大きくなる）として捉えることが一般的である。既に一部の金融機関では、こうした手法に則って個々のシステムのリスクをスコアリング(注4)し、これをリスク対策の優先順位付けに活用している例もみられる。

ただし、わが国の金融機関において現時点でこれを軌道に乗せている例は少なく、大方の金融機関では今後実践していくべき課題となっている。実際、本作業を進めるに当たっては、質・量とも相当のマンパワーを要するため、定期的に評価し続けるための組織的な枠組みを用意する必要がある。現時点で留意点を示せば、以下の通りである。

① 最初は大まかに把握することからスタートし、対象システムの範囲を絞るなど完全性を求めないこと。

② システムの重要性や技術基盤に応じ、適切な評価項目や評価基準を設定すること。

③ 評価レベルに格差が生じないよう、リスク統括部署等が統一的な視点でリスク評価の結果をチェックすること。

（５）システム監査

システム監査部署に期待される役割は益々大きくなっている。特に今後は、以下の３点の検証を通じ、当該金融機関のシステムリスク管理上の課題を明確化したり、経営陣に必要な提言を行うなど、リスク管理の高度化に貢献していくことが期待される。

① 基本方針等やこれに基づき講じられているリスク対策が、想定されるリスクの変化に耐え得るものとなっているか。

② リスク分析・評価について、その手法や出された結果は適切か。

③ 組織としての運用全般を通じて、セキュリティ対策の実効性が確保されているか。

（注４）ここでいう「スコアリング」は対策の優先順位付けのためにリスクの格付を行う手法であるが、定性的・主観的な評価に基づいて判断している。これに対しオペレーショナルリスク 計量化による資本賦課の枠組みにおいては、リスク顕現化による発生ロスデータに基づき最大損失額を算出することとなる。

またシステム監査要員のスキル面の制約等から自社内でリスク対策の適否をチェックすることが難しい場合には、システムの重要度を勘案したうえで外部のノウハウを活用することが考えられる。すなわち、スコアリングの結果リスクが高いと認定されたシステムや、内部におけるスキルの蓄積が不十分と判断される分野について、監査法人による外部監査、あるいは専門業者によるセキュリティ侵害テスト等のサービスを必要に応じて活用することも検討に値しよう。

5．おわりに

システムリスクの管理は、急速なＩＴ適用範囲の拡大とこれに伴うリスクの変容に合わせて、今後とも絶えず柔軟な対応が必要とされる分野である。ＩＴ化の進展が金融機関やそのシステム基盤にもたらしつつある変化としては以下のような例が挙げられる。

① インターネットの適用分野が拡大する（多様な顧客ニーズに対応したデリバリーチャネルの提供やｅビジネス分野等に活用する）。

② ＳＴＰ[注5]化による一貫処理等システム同士で連携処理する範囲が拡大する（事務効率化や人為ミス防止を図る）。

③ ハブ＆スポーク[注6]等新しいアーキテクチャーに基づいたシステムが構築される（次々に開発されるサブシステム間の連携処理を容易にする）。

こうしたシステム基盤の変化は、個別システムのダウンが他システムに連鎖したり、周辺システムに生じた事象が基幹部分に影響する可能性を高めると考えられる。こうした変化に、従来のようなシステム毎、あるいは共通のシステム基盤の存在を前提としたリスク管理により十分に対処することは難しい。異なる技術基盤に立脚したシステムが相互に連携する傾向が広がっていることを意識して、より高度かつ総合的なシステムリスク管理を図ることが求められている。

このような事態に適切に対応していくための答えを直ちに見出すことは容易でないが、環境変化に即応し、定期的・継続的にシステムリスク対策の見直しを図っていくことのできる全社的な管理体制を整備していくことが重要である。

日本銀行としても、各金融機関の金融サービスを支えるシステム基盤技術の動向や環境変化に即したシステムリスク管理の考え方について、今後ともさらに幅広い調査等を進めながら、金融機関をはじめとする関係者との間で議論を深めていきたいと考えている。

（注５）ＳＴＰ（Straight-Through Processing）とは、金融取引において約定から決済に至る一連のプロセスを、標準化されたメッセージ・フォーマットによりシステム間を連動させることによって、人手を介さずシームレスに行うことをいう。

（注６）ハブ＆スポークとは、新商品、新チャネル等の多様化するニーズに柔軟に対応するための分散技術を活用したアーキテクチャーで、複数のシステムをハブと呼ばれるサーバーを中心に接続し、連携させる仕組みをいう。