金融検査結果事例集別冊３

〔システムリスク管理態勢〕

平成23年７月

金融庁検査局

＜別冊３目次＞

【別冊３〔システムリスク管理態勢〕】

１．システム投資計画や戦略目標に関する指摘

①【取締役の役割・責任、戦略目標の明確化、システムリスク管理方針の整備・周知】

（規模・特性等）

・　地域銀行、中小規模

【検査結果】

・　システム開発案件については、所管部署であるシステム部門がシステム開発計画書としてとりまとめ、半期毎に常務会へ報告している。

　しかしながら、常務会は、同部門に対し、中期経営計画等に照らして優先的に実施すべき開発案件の判断基準を示していない上、開発を実行又は取り下げした案件の妥当性について検証していない。このため、不正取引の検知など重要性の高い施策に係るシステム開発が行われていない。

　また、他行との共同開発案件の管理については、同部門による他行との調整等が不十分となっていることから、共同開発の進捗が十分なものとなっていない。

②【戦略目標の明確化】

（規模・特性等）

・　主要行等及び外国銀行支店

【検査結果】

・　近年、銀行業界においては、勘定系システムの再構築やバッチ処理の効率化について、検討に数年を要するのが一般的になっている中、大量データ処理を起因とした現行勘定系システムの構造の複雑化・肥大化及び運用の硬直化が課題となっている。

　こうした中、当行は、現行システムが抱える障害発生・復旧対応などの具体的なリスク課題について、外部評価やリスクの洗出しを行わないまま、現行システムへの投資は制度変更対応のための改修にとどめている。

　このため、大量の取引が集中した場合の処理可能な範囲（制限値）が各々の取引毎に相違していることを所管部署が認識しておらず障害の復旧に時間を要している。

（規模・特性等）

・　地域銀行、大中規模

【検査結果】

・　取締役会は、システム子会社の副社長を委員長として、子銀行頭取以下関係役員が参加するＩＴ戦略委員会を設置し、効率的なＩＴ投資の実現に向け、グループ全体の案件を審議する体制としている。

　しかしながら、ＩＴ戦略委員会は、子銀行のシステム更改に係る進捗管理を行うにとどまっており、グループ全体として検討が必要な、業務に精通したシステム人材確保の方針やシステム企画・開発における品質の向上のための方針、中長期的な情報システムの戦略等について十分な検討を行っておらず、これらシステム開発体制の強化や維持などの方針が、システム開発を担うシステム子会社の経営戦略に反映されていない。

【別冊３〔システムリスク管理態勢〕】

（規模・特性等）
・　主要行等及び外国銀行支店
【検査結果】
・　中期システム開発計画について、経営会議は、開発期間及び費用が大幅に増加することが判明したことから、開発対象システムの削減による計画の見直しを行うこととし、システム開発担当部門に検討を指示している。
　しかしながら、経営会議は、企画部門が策定中のシステム投資計画との整合性や、システム開発に係る関係各社のシステム開発人員調整に係る検討を、同部門に指示していない。

（規模・特性等）
・　保険会社
【検査結果】
・　当社は、インターネットによる募集受付を本格化しつつあり、システムの安定的な安全稼動は、当社の重要課題である。
　しかしながら、取締役会は、システム基盤系など数年に亘る取組が必要な課題について、システムリスク管理計画の策定等、進捗管理を行う態勢を構築していない。また、取締役会は、システムリスク管理部門がシステム基盤の維持などの安全対策といった課題を先送りしてきた状況を看過している。
　さらに、同部門は、当社と同業他社の安全対策の水準・動向の比較等による現状の安全対策上の問題を把握しておらず、当該問題を取締役会等に報告していない。
　こうしたことから、契約管理上の重要な機能を担うシステムの基本ソフトやデータベースソフトについて、保守契約が期限切れとなっているにもかかわらず、当社は、延長保守契約も締結しないまま継続使用している。このため、システム障害が生じ、同システムが復旧できない場合には、既存契約の継続手続を行うことができなくなり、顧客に無保険期間を発生させるなど、顧客に重大な影響を与える可能性がある。

（規模・特性等）
・　主要行等及び外国銀行支店
【検査結果】
・　システムリスク管理部門は、システム化案件に対し、合目的性やリスク認識に立った優先順位付けを実施していない。このため、当初計画していたシステム開発案件について、同部門は、毎期多数の案件を繰り延べ・中止しており、その中には事故・事務ミス防止を目的とした案件や期限までの対応を必須としている案件も含まれている。
　しかしながら、同部門は、取締役会等に対し、繰り延べ・中止を妥当とする判断理由等を報告していない。

（規模・特性等）
・　主要行等及び外国銀行支店
【検査結果】

【別冊３〔システムリスク管理態勢〕】

・　取締役会は、システムリスク管理態勢について、ＩＴガバナンス規程を策定し、当該規程においてシステム開発等の骨格をなすＩＴ戦略やＩＴ中期経営計画を策定するとしている。

　しかしながら、ＩＴ戦略等の策定は未だ検討段階となっているほか、取締役会は、システム開発に係る標準的な手続等の基本事項を定めた規程を策定していない。

（規模・特性等）

・　主要行等及び外国銀行支店

【検査結果】

・　頭取をはじめとする経営陣は、システムの統合後の合理化効果を生むためには開発体制・手法やセキュリティ水準等を早期に一本化することが必要であると認識している。

　しかしながら、実際の統合時点では既存システムを併存させているため、開発体制等の一本化は限定的なものにとどまっており、当初計画していた統合後の合理化効果は未だ実現していない。

　また、「統合と同時にＩＴ戦略については積極的に投資する」とした統合計画時の基本理念についても、システム統合プロジェクト開発に資源をとられ、新たなＩＴ戦略は必要最小限なものにとどまっている。

（規模・特性等）

・　主要行等及び外国銀行支店

【検査結果】

・　頭取をはじめとする経営陣は、経営の最重要課題である合併や中核システム構築に経営資源を投入したことから、システムリスク管理態勢構築への取組が経営統合以降と遅れ、開発リスクが及ぼす経営戦略への影響や脅威についてリスクとして認識しておらず、整備状況や遅延に対して報告を求めていない。

　また、経営陣は、経営資源の配分や開発リスク等の管理状況を横断的・多角的に検討するために必要とされる経営会議を補完する機関も設置していない。このため、経営陣は、システムリスク管理態勢整備の遅延やシステム開発の業務定義課題等を十分に把握しておらず、対応策の議論や適切な指示を行っていない。

（規模・特性等）

・　主要行等及び外国銀行支店

【検査結果】

・　頭取をはじめとする経営陣は、コスト削減による競争力強化と利益確保等に傾倒し、必要なシステム開発や事務の人材確保等のシステムに関する中長期計画の策定が遅れ、短期的かつ暫定的な対応にとどまっている。このため、システムの複雑化による顧客ニーズや新商品に対するシステム対応力の低下、少数熟練者への業務運営の依存によるリスクの増大等の事態を招いている。

　こうした中、経営陣は、システム中長期計画を策定してプロジェクト管

理態勢を組成し推進しているものの、計画に係る全体予算についての出資関係会社の了解を得ていないほか、出資関係会社に要請しているプロジェクト参加メンバーの着任が遅れているなど、プロジェクトを推進するための体制を十分に整備していない。

（規模・特性等）

・　主要行等及び外国銀行支店

【検査結果】

・　当行及び子会社の全ての情報システムに適用するシステム戦略について、システム部門は、新たな戦略が子会社の基幹システムに大きな影響を与えることを認識しているにもかかわらず、当行が導入済みのシステムについて処理速度が劣化している問題を共有していない。

（規模・特性等）

・　地域銀行、中小規模

【検査結果】

・　当行は、勘定系及び情報系等のシステムに係る管理について、加盟行が共同運営する共同センターに委託している。

　こうした中、加盟行の脱退等に伴い、当行分担金の増加が見込まれることや、サブシステム経費が増加傾向にあることなど、中長期収益計画に影響を及ぼす可能性があるにもかかわらず、頭取をはじめとする経営陣は、これらの問題を把握しておらず、システムリスク戦略方針が明確となっていない。

（規模・特性等）

・　主要行等及び外国銀行支店

【検査結果】

・　頭取をはじめとする経営陣は、システム統合など、システムに係る諸問題の協議・検討機関として情報システム戦略委員会を設置しているものの、開催頻度が低いうえ、諸問題を各委員が適時適切に共有する場となっていない。

【別冊３〔システムリスク管理態勢〕】

２．コンティンジェンシープランに関する指摘

○【コンティンジェンシープランの策定】

（規模・特性等）

・　主要行等及び外国銀行支店

【検査結果】

・　経営管理部門は、システム更改等の機会に応じて危機管理体制に関する規程などの見直しを行い、いくつかの業務を業務継続の優先度の高い重要業務と決定している。

　こうした中、同部門は、決済業務等の業務継続の優先度の高い業務に対し、バックアップとして災害対策システムを保有していない中で、現金による仮払い等の暫定策の策定などについて検討しておらず、障害発生時に仮払いを前回実績の振込データ等により対処するといった検討を行っていない。

　このため、同部門が策定しているコンティンジェンシープランは、業務システムが被災した場合や長期のシステム障害に陥った場合においても、システムの復旧を待って決済業務等を行うことを前提とした旧態依然としたものとなっている。

（規模・特性等）

・　主要行等及び外国銀行支店

【検査結果】

・　危機管理態勢に関する経営陣の関与について、当行は、「危機管理方針」に基づき、「対策本部」を設置し、情報収集や対応方針の決定、対策の指示等を行うとともに、報告体制についても、システムリスク統括責任者を通じて、頭取に報告することとしている。

　こうした中、以下の問題点が認められる。

・　システム障害発生時の報告態勢について、同責任者は、頭取に対して十分な情報を報告しておらず、また、経営陣も、障害の原因や最大リスク等の障害の実態把握を迅速かつ正確に行っていない。

　こうしたことから、重大な障害が発生しているにもかかわらず、頭取は、「対策本部」を障害発生後速やかに立ち上げていない。

・　緊急事態発生時の営業店情報等の報告態勢について、経営陣は、「シナリオ別対応計画」において、同責任者が収集した営業店情報等を経営陣に報告することとしているが、経営陣は、同計画、同計画に基づく訓練や見直しの実効性についてフィジビリティ（実行可能性）を含めた十分な検証や改善指示等を行っていない。

　このため、同計画のシナリオが不十分な上、同計画に基づく障害発生時の対応訓練等は、営業店担当部門や事務部門を訓練対象としないまま実行されたことから、同責任者は障害発生時の営業店情報や業務運営の状況について、経営陣への報告を適切に行っていない。

　また、同計画の事務局も、発生事象の背景にある原因や最大リスク等の確認・検証等を行っておらず、経営陣が適切な判断を確保するために必要な報告を行っていない。

・　当行とシステム開発委託先及びシステム運用委託先の連携態勢について、

【別冊３〔システムリスク管理態勢〕】

経営陣は、３社間における連携体制の構築をシステムリスク管理部門等に委ね、十分に関与していない。

このため、システム障害を想定した３社合同での実地訓練がこれまで実施されていないことや、緊急時における、当行とシステム開発委託先の指揮命令系統が不明確であるといった問題点を、経営陣は看過している。

こうした中、二次障害リスクの情報が、一次障害発生当初よりシステム開発委託先に伝えられていたにもかかわらず、システムリスク管理部門は、同情報を認識していないほか、影響調査が勘定系システムの担当者へは連携されていないなどの問題が発生している。

（規模・特性等）

・　主要行等及び外国銀行支店

【検査結果】

・　システムのコンティンジェンシープラン（以下「ＣＰ」という。）の整備について、当行は、基本方針等において、緊急事態の要因及び緊急事態の発生を想定した緊急時対応体制の定期的訓練を年１回以上実施するとしており、これまでも運営要領に則った訓練を行ってきたとしている。

こうした中、システムリスク管理部門等は、リスクシナリオの検討を十分に行っておらず、以下のような問題が認められるなど、ＣＰの実効性が確保されていない。

・　当行は、現行システムの運用において、障害が起こりうる課題を認識していたものの、課題に基づくＣＰの見直しを行っていない。

・　障害シナリオの検討が不足していることから、ＣＰにおいて地震発生時のバックアップ切替対応以外のシナリオを想定していない。

・　システムリスク管理部門は、ＣＰを毎年定期的に見直しているとしているが、システム開発委託先が作成したＣＰについては、目次の項目レベルの確認にとどまっている。

・　ＣＰにおいて、当行とシステム開発委託先との担当部署間の連携体制を記載しているものの、両社の報告・指示命令系統が明確なものとなっていない。

・　当行及びシステム開発委託先並びにシステム運用委託先は、災害訓練等を実施しているものの、夜間処理が大幅に遅延した場合を想定した訓練等を行っていない。

以上の問題のため、システム障害の大幅遅延が発生しており、さらに、影響を受ける後続の処理代替プラン等がなかったことから、障害が拡大・長期化している。

（規模・特性等）

・　主要行等及び外国銀行支店

【検査結果】

・　システム障害や災害等を想定した「業務継続計画」について、総務部門は、想定シナリオに基づく訓練を年１回実施することとしており、その結果を経営会議に報告している。

しかしながら、同部門は、同計画の策定を所管部署任せとしており、実効性の確認を行っていない。このため、発生したシステム障害について、既に実施された想定シナリオとほぼ同様の状況であるにもかかわらず、適切な障害告知が行われていないとの苦情を受けて事後的に対応しているなど、同計画は有効に機能していない。

（規模・特性等）

・　地域銀行、中小規模

【検査結果】

・　システム障害への対応について、システムリスク管理部門は、サブシステムの障害発生件数が増加傾向にあるにもかかわらず、勘定系システムを除き、障害の原因分析や未然防止策の策定を行っていない。また、取締役会は、システム障害を想定した実効性のあるコンティンジェンシープランを策定していない。

（規模・特性等）

・　主要行等及び外国銀行支店

【検査結果】

・　リスク管理部門は、一部のグループ会社を除き、グループ各社におけるコンティンジェンシープランの策定状況の把握や内容の適切性に係る検証を行っていない。また、同部門は、当行における緊急時対応に係る規程において、緊急時にグループ会社から報告を受けた場合の当行の連絡体制や方法などの具体的な対応を定めていないほか、緊急時を想定した訓練を行っていない。

（規模・特性等）

・　地域銀行、中小規模

【検査結果】

・　災害時等における基幹システムのバックアップについて、システムリスク管理部門は、検討を十分に行っておらず、センター被災時の代替策を策定していない。また、同部門は、システム復旧後のバックアップデータの反映方法や、バックアップデータの搬出前に障害が発生した場合のデータの復元方法について、対応策を十分に検討していない。

（規模・特性等）

・　保険会社

【検査結果】

・　システムリスク管理部門は、コンティンジェンシープランについて、バックアップシステムの稼働を前提として策定しており、速やかに稼働しなかった場合を想定しておらず、緊急業務の手作業への移行判定基準やマニュアル等を整備していない。

また、同部門は、東京及び大阪以外の保険課が被災した場合の支払い等の対応策を明確に規定していないうえ、初動時の連絡網や職員の召集基準も明確にしていない。

【別冊３〔システムリスク管理態勢〕】

（規模・特性等）

・　主要行等及び外国銀行支店

【検査結果】

・　グループ全体としてのコンティンジェンシープラン（以下、「ＣＰ」という。）について、取締役会は、問題発生時又は発生が予想される場合には、「危機管理対策本部」を設置して重要な基本方針や施策を協議することとしている。

しかしながら、取締役会は、当該対策本部の位置付け、設置する障害のレベル、統括部署、子銀行への連絡体制、全体の責任体制を明確にしておらず、ＣＰは実効性に欠けたものとなっている。

こうした中、子銀行で発生したシステム障害において、ＣＰの発動が遅延したうえ、対策本部として「危機管理対策本部」と「システム障害対策本部」を併設したり、子銀行と当社要員が兼務において、各々の役割が不明確なものとなり、復旧作業や顧客対応などにおいて、持株会社として適切な対応を行っていない。

その結果、障害を拡大させることとなり、為替未送信が発生しているなど、顧客に大きな影響を及ぼすシステム障害となっている。