BOJ
Reports & Research Papers

2012年2月

リスク管理と金融機関経営に関する調査論文

システム障害管理体制の実効性向上に向けた留意点

日本銀行金融機構局

目　　次

（本件に関する照会先）

日本銀行金融機構局 考査企画課 システム・業務継続グループ

岩佐 智仁、泉 晋、林田 雄介

E-mail ： csrbcm@boj.or.jp

１．はじめに

今日では、資金決済、顧客情報の管理、インターネット取引を始め、金融機関業務の多くがコンピューター・システム（以下、システム）を経由して行われている。このため、金融機関は、システムの安定稼働の確保が極めて重要な課題であると認識し、システム障害の未然防止策や、障害発生時の対応策の充実に取組んでいる。

しかしながら、ある金融機関のシステムに生じた障害が、自らの顧客に止まらず決済システムにも大きな影響を与える事例が引き続きみられる。システム障害の典型的な事例は、システム開発の途上で生じた何らかの瑕疵（プログラミングミス、システム構成の設計ミス等）がシステム稼働後に顕在化し障害に至る、というものである。こうした障害を防止するためには、プロジェクト管理体制の整備、プログラムの品質確保、入念な稼働テストの実施などに取組むことが重要であり、近年では、多くの金融機関がこうした点を十分に認識してシステム開発に当たっている。

もっとも、システム開発さえ適切に行われれば障害が発生しないという訳ではない。システムが安定稼働を始めると、時間の経過とともに当該システムに対する組織としてのリスク認識が低下しがちになるが、他方で、顧客サービス向上のための周辺システムの追加や顧客行動の大きな変化等により、システムへの負荷が大きくなり、潜在的なリスクが蓄積することもある。この場合、リスクシナリオの見直しやシステムの処理能力の増強などが必要となるが、こうした中間管理を適切に行わないと、障害が発生する可能性が高まる。

特に、長期間安定稼働を続けているシステムについては、それが故に、潜在リスクが長期間に亘って蓄積し得る一方で、マニュアル類の更新や定期的な障害対応訓練などリスク管理水準を維持するインセンティブが後退しやすい面がある。万一、資金決済や為替業務を担う重要システムにおいて障害が発生した場合には、影響範囲が大きく復旧まで長時間を要する大規模障害となりかねないだけに、十分な注意が必要である。

こうした認識のもと、本稿では、システム障害管理体制の実効性向上に向けた留意点を、「障害発生の未然防止対策」「障害発生時の対応」「障害管理に対する経営陣の関与」の３つの観点から取りまとめた。また、金融機関で近年みられた個々の障害事例の背後にある障害管理体制面の問題事例をもとに、「障害管理体制面の問題点と対応策」を取りまとめ、別添１として添付している。さらに、2007 年３月公表の「事例からみたコンピュータ・システム・リスク管理の具体策」に添付した「想定される障害事例と対応策」についても、その後の障害事例を踏まえて追加・改訂し、別添２として添付している。

システム障害の発生を完全に防止することは、これに要するコストや障害が偶発的に発生することを考慮すると現実的ではない。しかしながら、経営陣の関与のもとで、障害発生の原因分析や予兆管理、あるいは迅速な障害復旧を可能とする体制の整備に継続的に取組むことを通じ、システムリスクの顕在化を抑制する、あるいはリスクが顕在化した場合の影響を極小化することは、極めて重要である。金融機関や、業務を請負うシステム関連会社等が、本稿を参考にしつつ、こうした体制整備に取組むことを期待する。

２．障害発生の未然防止対策における留意点

（１）稼働中のシステム

稼働中のシステムについては、時間の経過とともに、社内外の環境変化により潜在リスクが蓄積することを認識し、そのリスクへの対策を適切にとることが必要である。環境変化としては、例えば、①インターネット取引、携帯電話等モバイル端末経由取引の増加や、ATM 等のサービス提供時間の拡大等に伴う顧客行動の変化、②接続先の拡大や業務部署所管システム(EUC:End User Computing)の増加によるシステム構成の複雑化、③新技術の採用や ATM・営業店端末の汎用端末化(パーソナルコンピューターの採用）等によるシステム技術面からのリスクプロファイルの変化、などが考えられる。

図表 １ 社内外の環境変化と想定リスク（例）

環境変化の一例	想定される主なリスク
インターネット取引、携帯電話等モバイル端末経由取引の増加や、ATM 等サービス提供時間の拡大等に伴う顧客行動の変化	・インターネット取引等を通じた突発的な事務量の増加や、サービス時間の延長に伴う夜間・休日における事務量の増加による、システム処理能力の不足など
接続先の拡大や重要業務を担う EUC の増加等によるシステム構成の複雑化	・システムの全体像が適切に把握できないことによる、システム変更作業時の設定ミスなど
新技術の採用や ATM・営業店端末の汎用端末化等によるシステム技術面からのリスクプロファイルの変化	・自社と他社のシステムが接続されることによる、インターネットバンキングに対する外部からの不正アクセスや、ATM や営業店端末のウィルス感染など

稼働中のシステムに対するシステムリスク評価については、こうした社内外の環境変化に伴うリスクプロファイルの変化を適切に把握できるよう、評価項目を定期的に見直したうえで行い、各システムに潜むリスクの軽減に向けた対策を取りまとめる必要がある。特に既存システムを利用して新規事務や新規サービスの提供を始める場合には、新商品委員会等の枠組みにおいて、システム面からも問題がないかを確認することが考えられる。

また、業務部署（システムのユーザー部署）と連携のうえ、環境変化を踏まえて事務量の想定を見直し、システムの処理能力や設定値の妥当性を定期的に検証する必要がある。こうした検証と検証結果に応じた処理能力の増強等を行うことで、事務量がシステム開発当初の予測値の上限を超え、コンピューター本体等の物理的な処理能力の不足や、プログラムに設定している上限値への抵触により、処理が遅延・停止することを避けることが可能となる。

なお、システムの維持管理や運用作業等をシステム関連会社に委託している場合でも、例えば事務量見通しの作成等は、取組方針や顧客需要等を踏まえて自社で行うことが適当である。

このほか、障害抑制に向けた具体策としては、可能な範囲で、障害情報を他社分も含めて幅広く収集し、その原因分析を行い、同様の障害を自社システムで発生させないよう、対策を講じることも有効である。また、障害抑制に向けた各種施策の実効性の向上を企図し、一定期間に発生する障害件数等に上限目標値を設定・管理する施策も考えられる。この際、全体の障害件数のほか、障害ランク別、業務別等にも目標値を設定し、とりわけ顧客や決済システムに影響を及ぼす重大障害の発生件数の減少に努めることが重要である。

図表 ２ 稼働中のシステムへの有効な対策（例）

項目	有効な対策例
システムリスク評価	・時間の経過とともに社内外の環境変化に伴い蓄積され得る潜在リスクを想定し、評価項目を見直してリスク評価を実施
システム処理能力・設定値	・業務部署とも連携のうえ、インターネット取引等の拡充に伴う顧客行動の変化等を踏まえて、定期的に事務量を予測 ・オンライン処理のレスポンスタイムやバッチ処理の所要時間の定期的な確認
委託先管理	・委託先への依存度が高まる中であっても、自社による対応が適当と考えられる項目（事務量の想定等）の見極め
障害事例分析・防止策	・社内外の障害情報を広く収集し、障害の影響範囲、システム別・発生原因別の観点等を踏まえて根本原因を多面的に分析・評価
障害件数目標値の設定	・障害件数にかかる障害ランク別の上限目標値の設定と、当該目標の達成に必要な施策の策定・実施

（２）開発中のシステム

開発中のシステムに関する留意点としては、①大規模なプロジェクトについては、全社横断的な管理体制を構築し、関係部署間で情報共有を十分に行い、認識相違が生じないようにすること、②要件定義やシステム設計、テスト結果の検証等について適切な体制を整備し、稼働後に生じ得る環境変化を考慮したシステムの拡張性と、十分なプログラム品質を確保すること、③開発したシステムが本番稼働に耐え得るものかどうかを確認するシステムの稼働判定は、業務部署やリスク管理部署等の評価をも踏まえて行うこと、などが挙げられる。

こうした体制整備は、要件定義の不備やプログラムの不具合等による誤った結果の出力や、システム処理の遅延・停止等の障害を防止することに有効である。

これらの取組みについては、長年のシステム開発の中で各種のノウハウが蓄積されており、適切に対応している金融機関が多い。しかしながら、とりわけ障害が発生した場合の影響が大きいシステムについては、その開発工程に十分な障害予防策が盛込まれていることを、今後とも確認する必要がある。

３．障害発生時の対応における留意点

（１）障害対応体制

障害の発生を未然に防止する対策をとっていても、障害を完全に防止することは難しい。したがって、障害の発生を想定した対応体制を整備しておくことが重要である。なお、障害対応体制を定めていても、実際に障害が発生した際に有効に機能しないと、影響範囲が拡大し、復旧までに長時間を要することになるため、留意が必要である。

障害対応体制整備のひとつとして、障害発生時における経営陣への報告や委託先との連携体制、および当局への連絡体制等を事前に取決めておくことが重要である。この際、例えば、障害発生時の各種対応負担が原因究明・復旧策の検討を担うシステム部署に過度に集中する体制となっていないか、自社と委託先の責任分担に曖昧な点はないか、当日中に処理すべき決済件数・金額等を速やかに当局や外部接続先に連絡できる体制となっているか、などを確認する必要がある。

特に、初動対応に問題があり、経営陣が報告を受けるタイミングが遅延すると、関係部署への指示も遅れることになる。したがって、例えば、障害の影響度合いが不明な場合、経営陣は、まず障害発生の事実にかかる報告を先行して受け、不明な点は判明次第報告を受けるようにするなど、報告の迅速性を重視することが有効である。さらに、訓練等を通じて、こうした思考・行動様式を組織的に浸透させる取組みも重要である。

また、顧客・広報対応については、苦情対応や対外情報発信等の統制に混乱が生じると、対応負担をさらに高め組織対応力を損なう要因ともなり得るため、予め、関係部署の責任等を明確化したうえ、必要な情報共有を行う体制を構築しておく必要がある。

（２）障害対応計画（コンティンジェンシープラン）

コンティンジェンシープランについては、システム変更や組織改編等があった場合に適宜見直しを行い、最新のシステム構成・組織体制等と齟齬がないようにする必要がある。また、システム面・業務面に関するコンティンジェンシープランが、特定の者にしか理解できないような分かり難い内容となっていないかも、

組織的に検証する必要がある。

システム面・業務面のコンティンジェンシープランの整合性が取られていない事例が引き続きみられる。例えば、業務面の対応を取決めるに当たり、システム面の制約を踏まえていない事例や、反対に、障害復旧案がシステム面からしか検証されておらず、業務面のニーズを考慮していない事例などが挙げられる。このため、業務部署とシステム部署の連携のもとで、障害時の対応計画を作成する必要がある。

（３）障害に備えた訓練

システム障害に関する訓練計画を策定する際には、バックアップセンターへの切替えが必要なメインシステムの全面停止だけでなく、機器、オンライン処理、バッチ処理、対外接続システムにおける障害の発生など複数のシナリオを用意する必要がある。さらに、障害発生時の連携体制の実効性や妥当性を評価するために、対策本部の設置訓練や拠点駆付け訓練、広報対応訓練等を活用することも重要である。また、訓練の実施に当たっては、障害の復旧手順書やバックアップ機器等、障害時に利用する各種手段の実効性等を委託先とともに入念に検証する必要がある。

４．障害管理に対する経営陣の関与

（１）障害管理に関するリスクの認識

経営陣は、稼働中のシステムに関しても、インターネット取引等サービスの拡充や、それに伴う顧客行動の変化、接続システム構成の変化、新システム技術の採用などの社内外の環境変化に伴い、リスクプロファイルが変化し得ることを認識すべきである。そのうえで、システム部署や業務部署、リスク管理部署などの関係部署に、新たな潜在リスクの所在や特徴について報告を求める必要がある。また、経営陣は、監査部署も活用しつつ、障害対応等において、システム部署内の各セクション（企画・開発・運用）と業務部署等の関係部署間で、適切な協働・連携がとれる体制になっているかを確認するほか、障害管理の体制整備を図るうえで、人的資源や物的資源等の経営資源に制約が生じていないかを確認する必要がある。

特に、長期間安定的に稼働しているシステムについて、①時間経過の中で潜在リスクが長年に亘って蓄積し、想定しているリスクシナリオが不十分となり得ること、②長期間安定稼働を続けているが故に、障害対応、訓練、マニュアル整備等に対する問題意識が低下しやすくなること、③当該システムを熟知しているシステム要員の退職等から管理ノウハウが散逸しかねないこと、などの事情により長い目でみると却って対応体制が弱体化する可能性もある。

このため経営陣は、少なくとも、障害が発生すると顧客等への影響が大きいと考えられるシステムについては、その社会的重要性に鑑み、安定稼働を続けていても、システムリスク評価や訓練等を通じた障害管理体制の実効性検証に意識的に取組む必要がある。さらに、組織改編に伴う関係部署の変更や人事異動等に伴う要員（キーパーソン）の交代後も、ノウハウが維持されていることを確認する必要がある。

（２）障害発生の防止に向けた指示

経営陣は、関係部署から受けた報告等を踏まえ、システムの安定確保に向けて、その潜在リスクを認識・評価するための管理の枠組みや障害発生時の対応体制、委託先管理体制を改善するうえで責任がある。例えば、障害の未然防止策を充実させるために、自社分だけでなく他社分も含めて障害事例分析を行うよう指示することが考えられる。また、システム部署と業務部署が、システム開発中だけでなく、稼働開始後も十分に連携をとり得るよう、役員の役割分担も工夫しながら、連絡・検討体制を確保する必要がある。さらに、システム要員のスキル低下、企画・開発・運用間でのバランスを欠いた資源配分、管理ノウハウの散逸等の事象を認めた場合には、これらの問題を主体的に改善・解消する必要がある。

そのうえで、経営陣は、既存システムの継続使用の妥当性を評価し、システム見直しの要否等を検討することも求められる。

５．おわりに

金融機関のシステムは、近年、技術革新の進展等を背景に一段と多様化しており、リスクの所在を特定・認識する作業は、必ずしも容易でない状況となっている。また、望ましい障害管理のあり方は、各金融機関固有のリスクプロファイルに大きく依存する面がある。さらに、本稿で取上げた対応策は、高度な技術力等を要しない基本的な事項も多いが、リソース制約や繁忙度の高まりの中で、こうした基本的事項を徹底することが難しくなってきていることも事実である。こうした中で、各金融機関には、経営陣の適切な関与のもとで、システム障害管理に必要な施策を主体的かつ着実に実践していくことが求められる。

日本銀行としては、金融機関等が、本稿で紹介した留意点を念頭におきつつ、自社システムの特性等に応じたリスクの所在を的確に認識し、システム障害管理体制の実効性向上に向けて一層主体的に取組むことを期待している。

以　　上

障害管理体制面の問題点と対応策（例）

別添 1

Ⅰ．障害発生の未然防止対策

分類	障害管理体制面の問題点	想定される障害	対応策
1．稼働中のシステムへの対応			
（1）システムリスク評価			
	・新たな業務を開始したり、当局や各種団体が公表しているリスク評価基準が変更されているにもかかわらず、自社のリスク評価項目を見直していない。	・環境変化に伴って新たに生じたリスクを原因とする障害が発生する。	・少なくとも評価実施の都度、社内外の環境変化や当局・各種団体が公表しているリスク評価基準等を踏まえ、評価項目の妥当性を検証すること。
	・インターネットやモバイル端末を利用したサービスの開始・拡充、ATM の稼働時間拡大等に伴う顧客行動の変化による取引件数の増加を始めとするシステムへの影響を把握していない。	・取引件数がシステムの処理能力や設定値の上限を超過し、システムが停止する。	・新商品委員会等の枠組みの活用を通じて、業務部署と連携しながら、新たなサービスの提供や環境変化に伴う事務量の増加（大量取引の発生等を含む）につき見通しを策定したうえ、システムの処理能力や設定値の妥当性を確認すること。
	・システム間連動処理の拡大や商品サービスの多様化等に伴うシステム構成の変化（複雑化）を把握していない。	・外部接続先の障害を原因として自社システムが停止する。	・システムの全体構成や外部接続先を含めたシステムの連動状況等を、各システムの所管部署の十分な連携のもとで、正確に把握すること。
	・基幹システムへのインターネット技術の採用や、ATM・営業店端末の汎用端末化（パーソナルコンピューターの採用）等により、システム面のリスクプロファイルが変化しているにもかかわらず、従来のリスク対策を見直していない。	・外部からの不正アクセスによるシステム等の停止や ATM・営業店端末のウィルス感染等によるシステム障害が発生する。	・システム変更時において、ATM や営業店端末等の利用方法に変化がない場合でも、採用技術の変更に伴うリスクを的確に見極め、対策を講じること。
	・業務部署所管システム（EUC：End User Computing）に重要業務を担うシステムが含まれているにもかかわらず、EUC を一律リスク評価の対象外としている。	・EUC に障害が発生した際、障害原因の特定や復旧対応に長時間を要し、重要業務が滞る。	・重要業務を担っている EUC を特定し、その管理の枠組みを構築すること。
	・リスク評価項目に、システム運用（操作の標準化や手順書の整備等）に関するものを含めていない。	・操作ミスによるシステム停止が発生しやすい中、障害復旧手順書の不備により、復旧対応が長期化する。	・システムリスク評価の項目には、システム企画・開発面のほか、システム運用面の項目も含めること。

障害管理体制面の問題点と対応策（例）

別添１

分類	障害管理体制面の問題点	想定される障害	対応策
１．稼働中のシステムへの対応			
（２）システム処理能力・設定値			
	・事務量の増加やシステム処理方式の変更等を背景に、システムの負荷が全体的に高まっているにもかかわらず、この事実を認識していない。	・レスポンスの悪化やバッチ処理終了時刻の遅延が生じたり、システムが停止する。	・顧客サービスに与える影響等を把握する観点から、レスポンスタイムやバッチ処理時間等を定期的に確認し、リソース増強の要否等を検討すること。
	・業務部署が稼働開始後の性能要件の検討や性能テストに関与する体制となっていないため、システムの維持管理に際し、事務量の突発的な増加や将来の変化が考慮されない。	・事務量の突発的な増加時に、システムの処理能力や設定値を超過し、システムが停止する。	・稼働開始後の性能要件の検討等に当たっては、業務部署が主体的に関与すること。例えば性能テストにおいては、特異日や特異値に着目して行うほか、事務量の突発的な増加や将来的な変化を考慮すること。
（３）委託先管理			
	・システム開発作業等について、委託先への依存を高めるあまり、事務量の見通しの策定など、本来自社が主体的に取組む必要のある作業まで委託先に一任している。	・委託先が策定した事務量見通しが過少であるため、リソースの増強等の対応がなされず、処理の遅延やシステムの停止が生じる。	・事務量見通しの作成等、自社による対応が適当な作業については、自らが主体的に行うこと。
	・基本ソフトウェア等の不具合に関する重要情報の入手方法に関して、自社と委託先間で役割分担を取決めていないほか、情報を共有する体制が構築されていない。この結果、当該情報は自社だけではなく、保守委託先にも届いていると誤認している。	・基本ソフトウェアの作成会社から提供される重要な不具合情報が委託先に提供されず、本来対策を講じる必要のある不具合が、自社システムで顕在化する。	・重要情報の入手については、委託先に任せきりにせずに、自社と委託先の役割分担を明確にしたうえで、連絡を密にすること。
	・システムの運用作業を外部に全面的に委託し、自社の関与が大きく薄れた結果、システム運用に関するノウハウが自社で蓄積されず、適切なリスク対策を検討・実施できなくなっている。	・自社による委託先管理が不十分となり、委託先がコスト削減のためシステム要員の削減や操作手順の簡略化等を過度に行った結果、操作ミスが発生する。	・システム運用など、外部に全面委託している業務についても、その管理体制の適切性を評価できる体制を構築・維持すること。

障害管理体制面の問題点と対応策（例）

別添 1

分類	障害管理体制面の問題点	想定される障害	対応策
1．稼働中のシステムへの対応			
（4）障害抑制の具体策			
① 障害事例分析・防止策			
	・プログラムの不具合箇所等直接的な原因の分析・修正は行っているものの、障害の根底にある問題点を特定していない。	・自社で過去発生した障害と類似の障害が再発する。	・再発防止策は、障害の影響範囲、システム別・発生原因別の観点等を踏まえ、根本原因を分析・評価した結果に基づき策定すること。
	・障害防止策を検討するに当たり、対象とする障害を自社システムで発生した障害に限定している。	・他社や関連会社で発生した障害と類似の障害が自社システムで発生する。	・障害防止策は、可能な範囲で他社の障害情報も広く収集のうえ、策定すること。
	・EUC に重要業務を担うシステムが含まれているにもかかわらず、EUC で発生した障害は報告・分析の対象外としている。	・EUC の不具合が原因で重要業務の処理が停止する。	・重要業務を担うシステムで発生した障害は、EUC にかかるものも含め、システムの所管部署にかかわらず、報告・分析の対象とすること。
② 操作ミスの防止策			
	・操作ミスに関して適切な防止策を講じていない。	・手順書等の記載内容を誤解して操作した結果、システムが停止する。	・作業指示書の適切性検証や、操作時の相互検証の徹底、自動化対応等、操作ミスを防止するための体制を整備すること。
	・基本ソフトウェアのバージョンアップ等システム変更の際に、操作手順書を見直していない。	・システム変更に伴って操作手順書に不備が生じ、操作ミスが発生しシステムが停止する。	・通常時や障害発生時に利用する操作手順書は、システム変更の都度見直すこと。
③ 障害件数目標値の設定			
	・障害件数の管理を通じて、障害抑制策の実効性を客観的に評価していない。	・各種の障害防止策を講じているにもかかわらず、障害が多発する。	・障害件数の上限目標値等の指標を用いて、障害抑制に関する施策の実効性を客観的に評価すること。
	・障害件数の目標値が障害ランク別や業務別に定められていない。	・障害の総件数は目標値を達成しているが、特定のシステムにおいて、短期間に複数の障害が発生している。	・障害件数の目標値は、障害ランク別、業務別、システム別に定めること。

障害管理体制面の問題点と対応策（例）

別添１

分類	障害管理体制面の問題点	想定される障害	対応策
２．開発中のシステムへの対応			
（１）プロジェクト管理			
	・プロジェクトの推進に当たり、統括部署や部署横断的な会議体を設置していないなど、全社横断的なプロジェクト管理体制を構築していない。	・システム部署と業務部署の相互検証体制が不十分なまま重要プロジェクトを推進した結果、稼働開始後にシステムの不具合が多発する。	・特に重要プロジェクトの管理体制を構築する際には、プロジェクトに内在するリスクを漏れなく把握する観点から、システム開発、事務・顧客対応、広報対応の進捗状況等を把握するための社内横断的な統括部署を設置し、関係部署の相互検証体制を整備すること。
	・業務部署の関与が要件定義段階に止まり、要件定義をもとにシステム部署が作成した設計書等を業務部署が確認する体制としていない。	・システム部署が業務要件を誤認したまま設計し、稼働後の処理結果が要件と異なるものとなる。	・プロジェクトの推進に当たっては、システム部署と業務部署等、関係部署を網羅した検討組織を設置し、各段階において十分な意思疎通を図ること。
（２）システム設計・プログラム品質			
	・システムの設計に当たり、事務量増加に伴う設定値の変更や接続先の拡大等を柔軟に行えるような拡張性を考慮していない。	・設定値の変更や接続先の拡大にかかるシステム変更作業が増加・複雑化するため、プログラムの不具合を見落としやすくなり、システムが停止する。	・システム設計に当たっては、稼働後に生じ得る環境変化を考慮のうえ、システムの拡張性を確保しておくこと。
	・テストで発生した不具合への対応が、「不具合を修正すること」に止まっており、不具合が発生した背景の分析・評価を適切に行っていない。	・プログラムの品質が確保されない状況で稼働を開始し、障害が多発する。	・テストで発生した不具合について、①不具合の原因となった不備がどの工程で生じたものであるかの分析（不具合が特定の工程に集中していないことの確認）、②不具合件数とテスト件数の分析（不具合件数の減少が、テスト件数自体の減少によるものではないことの確認）、③顧客等への影響度を踏まえた「重要度」の観点からの分析（全体の障害件数は減少しているが、顧客に影響を与える障害が増加していないことの確認）等を行うこと。
	・不具合解消のためのプログラム修正が、連動する他のシステムに影響を及ぼす可能性を調査していないほか、修正後の確認は修正したシステムのみで行っている。	・テストで発生した不具合の修正方法が不適切なため、連動するシステムが停止する。	・不具合発生の連鎖を防止するため、関連システムへの不具合の影響調査を漏れなく行うこと。

障害管理体制面の問題点と対応策（例）

別添１

分類	障害管理体制面の問題点	想定される障害	対応策
２．開発中のシステムへの対応			
（２）システム設計・プログラム品質			
	・発見された不具合の水平展開手順（他処理に類似の不具合がないかの確認）を定めていない。	・テストで発見されたものと類似の不具合が残存し、稼働開始後に同種の障害が発生する。	・テストで発見された不具合をシステム品質の向上に活かすため、水平展開の取扱手順を定めること。
	・システムの性能評価に当たり、月末日のデータしか検証していないなど、業務特性を踏まえた確認を行っていない。	・月末日以外の営業日で事務量がピークとなり、CPU使用率が上限に近づいた結果、レスポンスが大幅に悪化する。	・システムの性能評価は、業務部署とも連携し、事務量動向等の分析方法の妥当性を確認のうえ行うこと。
（３）システム稼働判定			
	・稼働判定項目に、業務部署の事務処理体制や業務要件の充足状況を含めておらず、システム部署の対応状況のみをみて稼働判定を行っている。	・システム稼働直後から、事務ミスが頻発したり、業務部署のニーズに合わない帳票が出力される。	・稼働判定に業務部署、リスク管理部署、監査部署等の関係部署も関与する体制を構築し、稼働判定を全社的に行うこと。
	・稼働判定項目に、システム稼働後に必要なドキュメントの整備状況を定めていないほか、障害訓練を稼働日までに実施していないなど、円滑なシステム運行の確保に関する確認を行っていない。	・オペレーターが利用する操作手順書や、臨時作業指示書の記載内容が曖昧なため、誤操作を誘発し障害が発生する。	・稼働判定項目には、稼働後に必要となるドキュメントや、障害訓練の実施状況等、システム運行に関する内容を含めること。
	・稼働判定項目に、基幹系システム以外の周辺系システム等に関する評価を含めていない。	・周辺系システムに障害が発生し、これに連動する基幹系システムが停止する。	・稼働判定項目は、基幹系システムに限定せず、関連システムも対象とすること。
	・稼働判定項目が、例えば事務処理体制の評価について、「事務処理水準に問題がないこと」など抽象的な内容となっており、「営業店テストにおける個人・店舗ごとの打鍵ミスの件数」など具体的な基準を含むものとなっていない。	・システム稼働後に、事務習得が十分ではない特定店で事務ミスが多発する。	・稼働判定基準の策定に当たっては、なるべく数値基準を用い、数値基準の採用が適当でないものは客観性が保たれるよう関係部署で判定基準を明確にすること。

障害管理体制面の問題点と対応策（例）

Ⅱ．障害発生時の対応

分類	障害管理体制面の問題点	想定される問題事象	対応策
1.障害対応体制			
（1）報告体制			
	・障害対応にかかる関係部署の役割や相互連携体制等を明確に定めていない。	・障害発生時における経営陣への報告、当局や関連会社への連絡等に混乱が生じ、復旧までに長時間を要する。	・障害の復旧対応をシステム部署が担う一方、経営陣・当局等との連絡調整は経営企画部署が担うなど、関係部署の役割分担等を明確にすること。
	・障害復旧にかかる自社と委託先の責任分担を明確に定めていない。	・障害復旧に当たり、自社が対応すべき作業の一部を「委託先で対応するもの」と思い込み、同作業が放置され、障害の影響範囲が拡大する。	・障害復旧を迅速に行えるよう、自社と委託先の責任分担を明確にしたうえで、相互連携体制を整備すること。
	・緊急対策本部等の具体的な設置場所や、夜間・休日に障害が発生した場合の要員の召集体制を定めていない。	・緊急対策本部を速やかに設置できないほか、夜間・休日の障害発生時に要員が集まらないことにより、復旧作業が遅れる。	・緊急対策本部の具体的な設置場所や、夜間・休日の障害発生を想定した対応要員の召集体制を事前に定めること。
	・各部署では障害に伴う未処理の決済データの発生状況を把握できる状況にあるが、これらを組織全体として集約する方法がない。	・未処理の決済データにかかる復旧処理の見通しがつかず、影響を受けた顧客等に対して復旧までに要する時間等を説明できない。	・円滑な決済を確保する観点から、未処理の決済データについては、特定・集約方法や社内報告体制、復旧手順、顧客説明等、一連の対応体制を確立すること。
（2）初動対応			
	・障害発生時における経営陣への報告体制、当局や関連会社への連絡体制等において、迅速性の観点を考慮していない。	・経営陣等に障害情報が迅速に報告されず、適時のタイミングで経営陣から関係部署に復旧策にかかる必要な指示が行われなかったため、障害の影響範囲が拡大する。	・障害報告は迅速性の観点から「第１報は発生の事実、不明な点は判明次第」とするなど、初動対応手順を明文化し、経営陣から関係部署に迅速に指示が行われる体制を整備すること。
（3）顧客・広報対応			
	・法人・個人の顧客対応を担う部署を、緊急対策本部のメンバーに含めていない。	・障害の影響範囲や、復旧までに要する時間が、緊急対策本部のメンバーでは共有されているものの、顧客にはその情報が伝わらない。	・顧客からの照会等に組織的・効率的に応じられるよう、顧客対応を行う部署を緊急対策本部のメンバーに含めたうえで、役割分担を明確化し、相互連携体制を整備すること。
	・障害が顧客等に及ぼす影響の範囲、照会状況等を迅速に把握する体制を整備していない。	・障害の影響範囲を顧客からの苦情により初めて把握するなど、顧客対応が後手に回る。	・システム部署や業務部署等の関係部署が緊密に連絡を取合い、顧客対応の方針等を速やかに策定できるよう、障害発生時の情報収集体制を整備すること。

障害管理体制面の問題点と対応策（例）

別添１

分類	障害管理体制面の問題点	想定される問題事象	対応策
１.障害対応体制			
（３）顧客・広報対応			
	・障害発生時の広報対応の方針が不明確であり、経営陣等の会見やマスコミ対応、WEB による情報発信等、各種広報手段を網羅した統一的な対応を定めていない。	・記者会見、ホームページ、コールセンター等の情報発信手段ごとに、発表内容が異なる。	・顧客やマスコミ等に対する情報発信が統一的・効率的に行えるように、責任部署や関係部署の役割を明確化し、相互連携体制等を整備すること。
２.障害対応計画（コンティンジェンシープラン）			
	・システム面のコンティンジェンシープランで想定される障害発生時刻が限定的であるなど、同プランの十分性が確保されていない。	・ATM サービスの終了の間際に障害が発生すると、復旧までに相当の時間を要する。	・オンライン開始処理と夜間バッチ処理が近接する時間帯、内為入力締切時刻に近接する時間帯等、システムの運行上重要と考えられる時間帯に障害が発生するケースを想定したプランを策定すること。
	・復旧策が、滞留データの一斉送信など、システム的に処理し易い方法のみとなっており、業務的な観点から処理の優先順位を検討していない。	・為替データが滞留した際の障害対応において、当日決済データ、高額データ等、業務的に優先すべきデータの処理が遅れる。	・システム部署と業務部署の連携のもと、業務面のニーズも踏まえた復旧策を策定し、それに応じたシステム面の手当てを行うこと。
	・障害の対応方針が、業務面のニーズ（取引再開時刻等）のみで策定されており、システム面の制約等を踏まえていない。	・システムの復旧作業が、想定時間内に終わらず、取引が当初予定時刻に再開しない。	・復旧の優先順位等、障害の対応方針の策定に当たっては、業務面のニーズに対するシステム面の制約等を考慮すること。
	・障害復旧時間の見積もりに当たり、復旧策の検討に要する時間や復旧後の後続処理時間を含めていない。	・復旧に要する時間が見積もり時間を大幅に超過し、顧客サービスが予定の時刻に開始できない。	・復旧策の検討時間等を障害復旧の見積もり時間に含めたうえ、訓練等を通じて見積もり時間の妥当性を確認すること。
	・処理する事務量が多いにもかかわらず、システム障害時における手作業の実効性を確認していない。	・事務量の多さから、手作業では時間内に処理できない。	・手作業による復旧を予定している場合には、事務量を踏まえてその実効性を確認すること。
	・既存のコンティンジェンシープランが、最新のシステム構成や組織体制等の実態に見合ってない。	・障害の復旧手順に不備があり、新たな障害が発生する。	・コンティンジェンシープランが、システム構成の変化や組織改編等に伴う関係部署の変更状況、人事異動に伴うキーパーソンの交代等を正確に反映していることを、定期的に確認すること。

障害管理体制面の問題点と対応策（例）

別添 1

分類	障害管理体制面の問題点	想定される問題事象	対応策
2.障害対応計画（コンティンジェンシープラン）			
	・障害の復旧手順書の作成・管理が、そのシステムの担当者に任せきりになっているため、特定の者しか理解できない内容となっている。	・障害対応において、手順書の理解に手間取り、復旧が遅延する。	・復旧手順書は、組織的な管理のもと、経験の浅いシステム要員でも理解できるよう、作業の目的や手順等を具体的かつ明確にすること。
3.障害に備えた訓練			
	・訓練シナリオが、メインシステムの全面停止によるバックアップセンターへの切替等に限定されているなど、シナリオの十分性を検証していない。	・バックアップセンターへの切替えを必要としない障害において、障害復旧作業を速やかに行うことができない。	・訓練シナリオは、①機器障害（バックアップ機器への切替え）、②オンライン処理障害（ATM や営業店端末の障害）、③バッチ処理障害（給与振込、口座振替等の障害）、④外部接続先側の障害、⑤誤操作による障害、など複数の選択肢を用意すること。
	・オンライン処理障害等主要な障害シナリオの訓練が、長期間実施されていない。	・オンライン障害が発生したが、復旧作業に手間取り、復旧までに時間を要する。	・訓練計画には、主要な障害シナリオに即した訓練の定期的な実施を盛り込むこと。
	・訓練の参加部署がシステム部署に限定されており、経営陣への報告体制や関係部署との連絡体制等を確認していない。	・復旧作業や経営陣への報告対応等、障害発生時における種々の役割がシステム部署に過度に集中しているため、その対応負担から経営陣との情報共有に時間を要し、結果的に復旧対応が大幅に遅延する。	・障害発生時を想定して整備した社内外の連絡体制や各組織の役割分担の実効性・妥当性を、訓練等を通じて計画的に点検・評価すること。その際、①災害対策本部の設置訓練、②拠点駆付け訓練、③広報対応訓練、なども適宜活用すること。
	・訓練は机上のみで行い、開発機や本番機等の実機を利用した訓練を実施していない。	・障害発生時に手順書に基づき復旧操作を行ったが、記述内容に誤記があったため、復旧できない。	・実機を利用した訓練により、手順書類の実効性、機器の有効性を確認すること。開発機でしか訓練を行わない場合は、本番機と開発機の差異を洗い出しておくこと。

障害管理体制面の問題点と対応策（例）

別添１

Ⅲ．障害管理に対する経営陣の関与

分類	障害管理体制面の問題点	対応策
１．障害管理に関するリスクの認識		
	・経営陣は、自社システムの課題等に対する理解が不足しており、システムリスク管理の基本方針の策定・承認プロセスに主体的に関与していない。	・経営陣は、システムリスク管理に主体的に関与するうえで、自社システムの課題等について理解が不足している場合には、関係部署からサポートを受けるほか、委託先からの情報収集等に努めることにより、その知見を高めること。
	・経営陣は、長期間安定稼働を続けている決済業務等の重要業務を担うシステムに、社内外の環境変化に伴い潜在リスクが長年に亘って蓄積している可能性があることを認識していない。	・経営陣は、安定稼働の期間の長さにかかわらず、特に重要なシステムについては、その潜在リスクの洗い出しや、管理の枠組みの実効性確認を定期的に行うよう、リスク管理部署等に求めること。
	・経営陣は、①インターネットやモバイル端末の普及に伴う事務量の増加や顧客行動パターンの変化、②システムの増加や重要業務へのEUCの採用などシステム構成の変化、③ATMや営業店端末の汎用端末化に伴う採用技術の変化など、社内外の環境変化に伴う自社システムへの影響を認識していない。	・経営陣は、社内外の環境変化に伴う潜在リスクの所在や障害管理上の課題、リスク対策の実施状況等を把握するため、システム部署や業務部署、リスク管理部署などの関連部署に対して、これらの情報を適切に報告するよう求めること。
	・経営陣は、システム部署の人的資源制約の強まりを背景に、システムの企画・開発・運用の部署間の連携が図り難い状況であることを認識していない。	・経営陣は、人的資源の制約等、システム部署が抱える課題を的確に把握するため、システムの企画・開発・運用部署と十分に意思疎通を図ること。
	・経営陣は、長期間安定稼働を続けており、かつ稼働開始後に大きな追加・変更作業を行っていないシステムについては、その設計・仕様を十分に理解する要員が減少する可能性があることを認識していない。	・経営陣は、長期間安定稼働を続けているシステムのうち、特に重要なシステムについては、その設計・仕様を十分に理解している要員が継続的に確保されていることを確認すること。
	・経営陣は、長期間安定稼働を続けているシステムについては、障害訓練の定期的実施や各種手順書のアップデートなどリスク管理水準の維持・向上の面で、管理のインセンティブが後退するリスクを認識していない。	・経営陣は、長期間安定稼働を続けているシステムであっても、重要なシステムについては、障害訓練・手順書整備等リスク管理水準の維持・向上が図られていることを確認すること。
	・経営陣は、重要なシステム開発プロジェクトの品質状況等を適切に評価するうえで、必要となる情報の入手に努めていない。	・経営陣は、プロジェクトに内在するリスクを把握する観点から、進捗状況およびシステムの品質・性能に関する情報について適切な報告を求めること。
	・経営陣は、委託先の業務運営状況に対する関心が低く、委託先の不十分なリスク管理状況を長期間見過ごしている。	・経営陣は、自社による委託先管理の十分性を評価するため、委託先管理を担う部署に対し、委託先の業務運営状況について適切な報告を求めること。

障害管理体制面の問題点と対応策（例）

別添 1

分類	障害管理体制面の問題点	対応策
2．障害発生の防止に向けた指示		
	・経営陣は、関係部署から障害管理上の課題等の報告を受けているが、これらを踏まえ、経営として新たな課題を見出し、その改善・解消等に向けた働きかけを行っていない。	・経営陣は、関係部署から受けた報告等を踏まえ、例えば、システム部署と業務部署がシステム開発中だけではなく、稼働後も十分な連携をとるよう、必要な組織体制を整備するほか、システムの安定性の確保に向けて、潜在リスクの管理体制や障害発生時の事後対応体制、委託先管理体制の改善等を促すこと。
	・経営陣は、障害の未然防止に対する認識が弱く、その原因分析や防止策にかかる取組状況が不十分であるにもかかわらず、改善に向けた働きかけを行っていない。	・経営陣は、障害の根本原因に対する分析・対応策の策定や、他社で発生した障害にかかる事例分析を行うよう指示するなど、障害の発生防止の徹底を図るべく、PDCA サイクルが適切に機能するよう取組むこと。
	・経営陣は、業務委託比率が上昇する中、ベテラン層の退職等に伴う後継者育成の困難化や、コスト制約による開発要員のタイト化が、障害管理体制の実効性に及ぼす影響を認識していない。	・経営陣は、障害管理体制の改善等を図るうえで、人的資源の面（システム要員<関連会社の要員を含む>の育成・確保）に制約がないかどうかを確認すること。また、制約を認めた場合、システム要員の計画的な育成策を講じるほか、企画・開発・運用の配置・処遇を見直すなど、問題の改善・解消に向け、所要の施策を講じること。
	・経営陣は、システムの老朽化・要員のスキル低下等に歯止めがかからない状況であるにもかかわらず、現行システムの継続使用を前提とし、既存システムの見直しの要否等を検討していない。	・経営陣は、障害管理体制の改善等に当たり、必要に応じて、既存システムの見直しの要否等を検討すること。

以 上

想定される障害事例と対応策（例）

別添２

分類	想定される障害事例*	対応策
１．ハードウェア		
	・ ハードウェア障害に伴い待機系機器への自動切替処理が開始されたが、ハードウェアの制御用ソフトウェア（ファームウェア）の不具合により切替えに失敗し、システムが停止する。 ➢ ファームウェアの不具合の修正プログラムが、製造元から提供されていたにもかかわらず、保守委託先が修正情報を認識していない。	・ 保守委託先と不具合修正プログラムの情報収集方法を取決めること。 ・ 保守委託先が上記方法に則して情報を収集しているか定期的に確認すること。
	・ 稼働系機器に障害が発生したが、一部の機能が動いていたため、障害が検知されずに、待機系機器への自動切替処理が開始されない。また、ネットワーク機器で本事象が発生した場合には、不安定な状況で短時間に障害と復旧を繰返すことにより、制御データ（パケット）が大量に発生（輻輳）し、端末のレスポンスが悪化する。 ➢ ハードウェア障害を想定したテストにおいて、自動切替処理が正常に機能しないケースをテストしていない。	・ 障害が発生している場合には監視上は異常がなくても、強制的に待機系機器に切替える手順を確立し、その実効性を事前に確認すること。 ・ 機器の稼働状況に加えて、業務処理プログラムの応答状況も、監視すること。
	・ 待機系のコンピューター本体の起動に必要なシステム情報と、稼働系の同起動に必要なシステム情報が、同一の磁気ディスク内に格納されている。この磁気ディスクに障害が発生したため、稼働系・待機系ともに停止する。 ➢ トラブルが生じると、システム全体が障害となる箇所（単一障害点）を洗い出していない。 ➢ コンピューター本体以外の主要な機器（磁気ディスク装置、ネットワーク機器等）に障害が発生した場合を想定したテストを行っていない。	・ 稼働系と待機系の機器が、同時に障害とならないシステム構成とすること。 ・ 主要な機器に障害が発生したことを想定し、待機系機器が有効に機能することを確認すること。
２．ソフトウェア		
（１）制御プログラム		
	・ 基本ソフトウェアの不具合により、業務プログラムの処理完了後もサーバーのメモリー領域が解放されない状況になっている。このため、徐々にメモリーの使用可能領域が減少し、稼働から数日経過した段階でシステムが停止する。 ➢ テスト段階で、実運用に即した数日間連続の稼働テストを実施しておらず、頻繁にサーバーの起動・停止を繰り返すことで、都度メモリーが開放されていたため、本事象を発見できない。	・ 実運用に即した数日間連続のテストを実施すること。 ・ メモリー使用状況を監視すること。

＊「・」は障害事例、「➢」は問題点を示す（以下同じ）。

想定される障害事例と対応策（例）

別添２

分類	想定される障害事例	対応策
２．ソフトウェア		
（１）制御プログラム		
	・ 機器 A の障害により、機器 A、B、C 間の通信が遮断された（A は B と接続、B は A と C に接続、C は B と接続している）。機器 A のバックアップ機器 A’に切替わった後、自動再開処理が実行されたが、C のプログラムに不具合が生じ、通信が再開されない。 ➢ 自動再開処理のテストでは、機器 B の障害を想定し、機器 A、バックアップ機器 B’、C の通信が自動再開することを確認していたが、機器 B、C がともに正常な状況で、機器 A が障害となった時の自動再開テストを実施していない。	・ システム構成が複雑化している中、直接接続していない機器から受ける影響をも洗い出したうえで、テスト項目を作成すること。
	・ システムの運行時間を制御するプログラムにおいて、2 月 29 日にシステムの自動起動が失敗する。 ➢ 業務処理プログラムのテストは念入りに行ったが、制御プログラムの正当性を確認するテストを実施していない。	・ 日付処理を行う制御プログラムの正当性を確認するために、閏日等の特異日のテストを行うこと。
	・ パッケージソフトの有効期限を初期値のまま放置したため、当該期限を越えた時点でシステムが停止する。 ➢ 業務処理プログラムの各種設定値（上限値等）は管理しているが、パッケージソフトの設定値は管理していない。	・ パッケージソフトの使用に際しては、有効期限等の設定値を仕様書等により確認すること。
	・ 基本ソフトウェアに関する不具合の情報は、同ソフトウェアの契約者である自社に送付されているが、その情報をシステムの保守を委託している先に開示していない。このため、当該委託先は所要の対応をとることができず、不具合が顕在化する。 ➢ 不具合情報などの専門的な情報は、委託先にも当然伝わっているものと思い込んでいる。	・ 不具合の情報については、委託先と適時適切に共有するほか、不具合の解消に向けたシステム対応の要否等を検討すること。
（２）業務処理プログラム		
	・ 元加処理は、毎月第 1 営業日に実行する必要があるが、月初 1 日が休日と重なる場合に不具合が発生し、第 1 営業日の処理が実行されない。 ➢ テストは、月初 1 日が平日の場合しか実施していない。	・ 休日と月初・月末等の組合せを踏まえて、実日付を意識したテストを実施すること。
	・ 合併時における店舗コード読替プログラムの不具合により、存在しない店舗コードの仕向け電文が作成されたため、外部接続先で処理ができない。 ➢ 合併前に店舗コード読替えプログラムを実行し電文が作成されることは確認しているが、外部接続先とのテストは、店舗コードの読替えが不要なデータのみで行っている。	・ 適切なデータ・パターンを用いて、主要な外部接続先との間でテストを行うこと。 ・ プログラム内でデータの読替処理を行っているケースにおいては、テスト等で読替後の値が正しいことを確認すること。

想定される障害事例と対応策（例）

別添２

分類	想定される障害事例	対応策
２．ソフトウェア		
（２）業務処理プログラム		
	・ 休日に本番システムの業務処理プログラムのバージョン・アップを実施したが、翌営業日に本番システム環境に限って顕在化する不具合が発生し、業務処理が行えない。 ➢ 開発システムでは、バージョン・アップ後に業務処理が正しく行えることを確認していたが、本番システムのバージョン・アップ後の稼働確認では、システムの立上げ確認のみ実施し、業務処理の確認を行っていない。	・ 業務処理の稼働を開発システムで確認済であっても、本番システムのバージョン･アップ作業を実施した後は、開発システムと本番システムの差異がもたらす影響を検証すべく、必要に応じて業務処理を含めて稼働確認を行うこと。
	・ ATM の振込み処理では、入力された最大桁数に満たない口座番号には、先頭部分にゼロを付加する仕様としている。このデータを用いて振込依頼データを外部センターに送信する際には、先頭部分のゼロを削除する必要があったが、新システム移行後に、ゼロを削除せずに外部センターに送信したため、被仕向金融機関側で口座相違エラーとなる。 ➢ 新システムへの移行に当たり、被仕向金融機関を含めた振込テストを実施していない。	・ 対外接続系業務においては、主要な外部接続先との間でテストを行うこと。 ・ システム間のデータ連携時にミスが生じないよう、外部接続先の仕様を踏まえたうえで、システムを構築すること。
	・ プログラムを修正する際、誤って修正対象ではない箇所も変更してしまい、不具合が発生する。 ➢ 修正後のテストが、本来の変更箇所に限定したものとなっているため、誤ったプログラム変更を検出できない。	・ 重要プログラムについては、修正箇所以外も対象とした標準的なテスト項目を予め用意すること。
	・ 外部センター宛ての振込データが、障害により大量に滞留した。数時間後に復旧したものの、当日決済分のデータを優先的に処理する機能がないため、当日中に送信すべきデータを処理し切れない。 ➢ 障害復旧時の業務要件として、滞留したデータを再送信するというシステム的な観点しか考慮しておらず、当該決済への影響を極小化するという業務的な観点を含めていない。	・ 決済日や決済金額を把握する機能を設けること。 ・ 決済日や決済金額に応じて優先処理できる機能を設けること。
	・ 取引先のシステム更改に伴い、同先から持ち込まれるデータ・フォーマットが変更されたが、当該データを処理する自社システムの見直しを行っていなかったため、処理が異常終了する。 ➢ 自社システムの変更の際には、組織横断的にその影響を洗い出していたが、取引先等関連先のシステム変更の際には、そうした洗い出しを行っていない。	・ 取引先がシステムを更改する場合、持ち込まれるデータ・フォーマットの変更の有無や、変更内容を事前に確認し、自社システムの見直しの要否を検討すること。

想定される障害事例と対応策（例）

別添２

分類	想定される障害事例	対応策
２．ソフトウェア		
（２）業務処理プログラム		
	・ システム稼働開始後の事務量が徐々に増加した結果、個別取引毎に割振られる通番が１日の上限値を超過。この際、超過分の通番が再び「1 番」から重複して付されたためエラーが発生し、システムが停止する。 ➢ 事務量の推移を把握する管理体制を構築していないほか、テストにおいて上限値を超過した場合の影響を確認していない。	・ システム内に設定している各種の上限値を管理すること。また、その適切性を定期的に見直すこと。 ・ 事務量が上限値に近接してきた場合に警告を表示する機能を設けるほか、仮に超過した場合でも、欠落データの発生やシステム全体が停止することがない構成・設定とすること。
	・ システムの仕様変更の際、そのシステムと連動している他システムへの影響の洗い出しが漏れていたため、他システムの取引が不能となる。 ➢ 仕様変更が生じたシステムについては、稼働確認を行ったが、そのシステムと連動している他システムとのテストは実施していない。 ➢ 各システムを担当する部署が異なっているにもかかわらず、システム変更に際し、部署間を跨る確認体制を整備していない。	・ 仕様変更に伴う影響調査は連動する他システムについても実施するほか、変更がない場合でも必要に応じて無影響確認テストを実施すること。 ・ テスト項目の作成に当たっては、システム間の連携・処理プロセスを部署横断的に確認し、直接接続していないシステムや機器で障害が発生した場合の影響範囲を洗い出すこと。
３．性能		
（１）処理能力		
	・ CPU 処理能力を増強した結果、プログラムの応答時間が大幅に短縮されたことから、応答時間を検証するプログラムの小数点以下の有効桁数が不足し、応答時間が０秒となった。そのため、プログラムが実行されていないと認識され、バッチ処理が異常終了する。 ➢ CPU 増強の目的が、オンライン処理の時間短縮であったため、テスト段階では、オンライン処理部分のみを確認し、バッチ処理の確認は行っていない。	・ CPU 増強などシステム変更時の影響確認テストは、バッチ処理を含めるなどシステム全体を対象に実施すること。
	・ 新規サービスの開始に伴い、稼働開始から暫くの間、システムリソースの使用状況を注視していたが、CPU の使用率には問題がなかったものの、ログの格納領域が不足し、システムが停止する。 ➢ CPU のみに着目しており、磁気ディスクの使用状況を監視していない。	・ システムリソースは、CPU 使用率だけでなく、メモリーや磁気ディスク、回線使用率なども監視対象とすること。

想定される障害事例と対応策（例）

別添２

分類	想定される障害事例	対応策
３．性能		
（１）処理能力		
	・ 事務量の増加に伴い、顧客が直接アクセスする WEB サーバーの処理能力が不足したため、増強を実施。これにより、想定件数を超える取引を受け付けた場合でも、WEB サーバーでは処理対応が可能となった。一方、後続処理を行うアプリケーション・サーバーでは処理能力を増強しなかったため、想定件数を超える取引件数に処理能力が追いつかず、システム全体がスローダウンする。 ➢ テストでは、「想定事務量」での負荷テストは行ったものの、「（システムの）許容最大事務量」では行われていない。 ➢ 想定事務量を超過して取引が発生した場合に、顧客のアクセスを制限できる仕組み（流量制限）を有していない。	・ 一部システムの能力増強を行う際には、処理能力に関するシステム全体の整合性を踏まえて、性能評価を行うこと。 ・ 性能負荷テストは「想定事務量」に加え、「許容最大事務量」でも行うこと。 ・ WEB システムでは、アクセスを制限できる仕組み（流量制限）を設けること。
	・ 大量データの一括処理において、データ 1 件毎に同一の不具合が発生し、全件分のエラー・メッセージをシステムの操作端末（コンソール）に表示する処理が実行された。システムは、この表示処理に殆どの CPU 処理能力を費やし、他の処理がタイムアウト等により実行できなくなり、システム全体が停止する。 ➢ 同一不具合発生時におけるエラー・メッセージの出力を抑制していない。	・ 同一のエラー・メッセージが大量に発生した場合、表示するメッセージを抑制するなど、システム停止に繋がらない仕組みを構築すること。
	・ 新規顧客の獲得や預金量の増加を目的とした優遇金利等のキャンペーン実施に伴い、事務量が突発的に増加。もっとも、これに見合うシステムの処理能力が確保されておらず、システムが停止する。 ➢ 業務部署で企画された新商品が、システムに与える影響を確認していない。	・ 取引の繁閑差の大きい業務システムについては、システムの性能・容量にかかるモニタリングを頻繁に行うこと。 ・ 新商品の導入に当たっては、業務部署とシステム部署が連携して、システムに与える影響を確認すること。
	・ 開発期間中における性能テスト･負荷テストでは、要件定義書における性能要件を十分に達成していた。しかしながら、開発環境と本番環境の構成の違いが原因となり、本番稼働初日に十分な性能が確保できずに、営業店端末の応答時間が低下する。 ➢ 開発環境におけるテストにおいて、実運用と同等のデータ件数、処理順番等になっていない。 ➢ 開発環境と本番環境の違いがもたらす影響を把握していない。	・ 本番環境でのテストを行えず、開発環境でテストを行う場合は、本番環境との相違点やテスト方法等を十分に踏まえた確認・評価を行うこと。

想定される障害事例と対応策（例）

別添２

分類	想定される障害事例	対応策
３．性能		
（２）設定値		
	・ 限定した顧客と接続する WEB システムにおいて、新たなサービスの開始に伴いアクセスが集中。WEB サーバーの CPU やメモリー等ハードウェアのリソースには余裕があるが、取引履歴（ログ）の記録可能領域が不足しシステムが停止する。また、同サーバーはリソースに余裕があり、監視対象外となっているため、障害対応の初期動作が遅れる。 ➢ テストでは、実運用に即した性能評価を行っていない。また、取引ログの記録可能領域を想定値ぎりぎりの値としている。	・ 本番環境と同等の性能評価テストを行えない場合、設定値は十分に余裕を持った値とすること。 ・ 障害が発生した場合、システム全体に深刻な影響を与える可能性のある機器は、監視対象とすること。
	・ リソースの使用率が一定の水準を超過した際に警告を発する仕組みとしているが、新たなサービスの提供に伴い、一挙に限界値を超過した結果、警告発出を経ずにシステムが停止する。 ➢ 新サービスの導入等、事務量の増加が見込まれる場合に、既存システムへの影響を考慮していない。	・ 新規サービス・商品導入に当たっては、これらが既存システムに及ぼす影響を事前に検証すること。
	・ 磁気ディスクに記録されている取引履歴を、6ヶ月に1度磁気テープ（MT）へ退避する運用を行っている。磁気ディスクの使用率は、退避の 3 ヶ月後に問題ないことを確認している。しかしながら、事務量の増加に伴い 5 ヶ月目に容量を超過しシステムが停止する。 ➢ 事務量を把握する間隔が、事務量の増加傾向を踏まえたものになっていない。	・ 取引量の増加が見込まれる商品等については、導入後も、事務量の増加傾向を踏まえ設定値を定期的に見直すこと。また、見直しに当たっては、リソースにかかる過去の使用状況に加え、将来的な使用率見通しも考慮すること。
	・ 事務量増加に対応してファイル容量の拡張を行う際、待機系機器の設定値（ファイル容量）の見直しを失念した。このため、取扱い可能なファイル容量が、稼働系機器よりも待機系機器の方が小さくなり、稼働系機器障害時に待機系機器へのファイル引継ぎができず、切替えが失敗する。 ➢ 稼働系機器については適切な管理を行っているが、待機系機器については十分な注意を払っていない。	・ 稼働系機器と待機系機器の設定値等に差異がないことを、システム開発や設定変更のタイミングのほか、定期的に確認すること。
	・ ATM の稼働日の設定作業において、1月2日を「祝日・サービス取扱日」とすべきところを、「祝日」とのみ設定。「祝日」の場合の初期設定値は「サービス停止日」となっており、ATM が稼働しない。 ➢ 業務プログラムは重要視しているものの、パラメータ等の設定値については十分な注意を払っていない。	・ システムに設定されている各種パラメータの初期設定値を正確に把握すること。

想定される障害事例と対応策（例）

別添２

分類	想定される障害事例	対応策
３．性能		
（２）設定値		
	・ 業務処理プログラムに設定されている上限値には、入力可能データ件数のほか、出力可能データ件数がある。入力されたデータ件数は上限値を下回っていたものの、出力されたデータ件数が上限値を上回っていたため、処理が途中で中断する。 ➢ 入力処理を行う業務プログラムの担当部署と、出力処理を行う同担当部署が異なる中、上限値の確認を相互に行っていない。	・ 上限値の管理は、オペレーティングシステム、データベース管理ソフト等に設定しているものに加え、業務処理プログラムに設定されているデータの入出力可能件数、作業領域への収録可能件数（ワーク領域）等を含めること。 ・ 上限値等は、データの入力から出力までの一連の流れを踏まえて確認すること。
	・ 利息計算に利用される有効桁数が、数十年前のシステム構築時から見直されないまま、利息額が当該桁数を超過し、プログラムが異常終了する。 ➢ 事務量の推移は適切に把握し、その処理プログラムに関する上限値は都度見直ししていたものの、利息計算等に係る「桁数の上限値」は管理していない。	・ 事務処理プログラムの上限値だけでなく、各種計算に使用される有効桁数にも配慮すること。
	・ パッケージソフトを利用して、手数料を徴収するシステムを構築した際、手数料を定義している領域の値がパッケージソフトの初期値である「99999」と設定されていたが、業務処理プログラムはこれを初期値と認識せず、徴求すべき手数料と判断し、多額の手数料を徴収する。 ➢ パッケージソフトの各種設定値の意味を正しく理解しないまま導入し、導入後のテストにおいても、業務的な観点（手数料が通常では考えられないほど多額になる点）からの確認を行っていない。	・ パッケージソフトやデータベース管理ソフトの仕様を、初期値・設定値を含めて正確に把握し、テスト時には、業務的な観点から異常値の有無の検証を行うこと。
	・ 廃止した店舗の定義情報を削除する際、業務処理プログラム上の定義は削除したが、データベース上の定義を削除しなかったため、両者間で不整合が発生し、システムが停止する。 ➢ 同一システム内におけるデータの流れを把握できていない。 ➢ 作業実施後のテストによる作業内容の確認を行っていない。	・ 定義情報の削除・設定はシステム全体の整合性を踏まえて行うこと。また、当該削除等の適切性にかかる確認テストの要否を検討すること。

想定される障害事例と対応策（例）

別添２

分類	想定される障害事例	対応策
４．運用		
（１）機器監視		
	・ 稼働系機器に障害が発生し、待機系機器への切替処理が起動したが、待機系機器で稼働しているはずの切替処理に必要なプログラムが別の原因で停止していたため、切替えに失敗する。 ➢ 待機系機器に対しては、ハードウェアの状況は常時監視しているが、プログラムの稼働状況は監視していないため、プログラムが停止していることを事前に検知できない。	・ 待機系機器についても、プログラムの稼働状況を含めて監視すること。
（２）運用手順		
	・ ハードウェア障害により早朝のシステム立上げに失敗。障害検知後、障害マニュアルに沿い復旧作業を行うが、業務開始時刻に間に合わず全ATMの稼働開始時刻が遅延する。 ➢ 復旧作業にかかる想定所要時間を事前に把握していない。 ➢ 前日のバッチ処理はオンライン開始の6時間前に完了するが、システムの立上げ開始時刻はオンライン開始の 2 時間前としている。	・ システムの立上げ開始時刻は、立上げに失敗した場合に備え、復旧に要する時間を勘案しても余裕をもって業務開始に間に合う時刻に設定すること。
	・ 臨時バッチ処理と業務開始に必要な定例バッチ処理が競合し、両方のバッチ処理が異常終了した。業務開始時刻を過ぎて漸く原因が判明し、定例バッチ処理を再実行することとしたが、業務開始時刻を過ぎると当該バッチ処理が起動しない仕様となっていたため、再実行できず、業務開始時刻が大幅に遅延する。 ➢ 定例バッチ処理の仕様を理解しておらず、異常終了した場合の対応も検討していない。 ➢ 臨時作業が定例作業に与える影響を確認していない。	・ バッチ処理が異常終了した場合に備えて、再実行するために必要な条件を明示した作業手順書を用意すること。 ・ 臨時作業を実施する際は、予め並行する他の作業への影響有無、実行タイミング等の条件を確認すること。
	・ 新システム移行後の最初の事務量ピーク日に、事務集中センターにおける処理に遅れが生じ、取引の一部が当日中に完了しない。 ➢ ピーク日の事務量を想定したテストは、営業店のみを対象にしており、事務集中センターを含めた主要拠点が参加するテストを行っていない。	・ 大規模更改案件等におけるテストでは、主要な業務関連拠点を対象として、ピーク日事務量による確認を行うこと。
	・ システム変更後に見直したATMの立上げ作業手順書に記載ミスがあったため、誤って全ATMを停止させてしまい、全ATMで取引が不能となる。 ➢ 見直した手順書の実効性・正確性を、稼働確認の実施等を通じて確認していない。	・ 手順書を見直した場合、利用前に、その実効性を確認すること。

想定される障害事例と対応策（例）

別添２

分類	想定される障害事例	対応策
４．運用		
（２）運用手順		
	・ システムを起動する際、複数のバッチ処理が順次実行される仕様となっており、各処理には起動時刻が設定されている。その際、1 本目の処理に時間を要したことで、その処理が完了する前に2本目の処理が開始されてしまい、2本目の処理が異常終了する。 ➢ システムの起動処理に関する仕様を正しく理解していない。	・ 起動処理などの重要処理については、その処理内容・処理条件を把握したうえで、適切な処理順序が確保されるよう設定すること。
	・ 機器障害の復旧作業時に、誤って正常に稼働している機器の電源を切断したため、多数の営業店の端末が停止する。 ➢ 障害が発生すると業務に影響を及ぼす惧れがあるにもかかわらず、営業時間中に作業を行っている。 ➢ 機器接続図が正確でないほか、機器構成を正しく理解していない要員が作業を行っている。	・ 本番稼働時における保守作業に際しては、相互検証体制のもと、行うこと。また、作業手順については、予め関係者で確認しておくこと。 ・ 作業時間は、作業が失敗した場合の影響を考慮して決めること。 ・ 機器接続図などの仕様書を、最新に保つこと。
	・ 開発機でのテストにおいて、誤って本番のネットワーク定義を使用したため、外部のセンターと開発機が接続されてしまい、本番取引が停止する。 ➢ 作業の際には複数人で作業するなどの相互検証体制を整備していない。 ➢ 本番環境と開発環境が同一ネットワーク上に存在している。	・ 重要な作業は複数人で行い相互検証すること。 ・ 開発での作業ミスにより本番環境に影響が出ないよう、本番環境と開発環境は可能な限り分離すること。
	・ 全ATMが停止中に行うべきメンテナンス作業を、一部ATMの稼動時間中に実施したため、当該ATMが停止する。 ➢ 作業の前提条件を明確にしていない。 ➢ 作業が対象機器以外に与える影響を確認していない。	・ 保守作業実施の際は、作業の前提条件についても確認しておくとともに、本番業務への影響と万一の場合の対処方法を確認しておくこと。
（３）プログラムリリース		
	・ 本番プログラムリリースの際、開発時の設定情報を残したままリリースしたため、プログラムが正常に稼働しない。 ➢ リリースの際、設定情報の内容を確認していない。	・ 本番プログラムのリリースに当たっては、開発時の設定情報が残っていないか確認すること。

想定される障害事例と対応策（例）

別添２

分類	想定される障害事例	対応策
４．運用		
（３）プログラムリリース		
	・ 勘定系システムにおいて、稼働系機器と待機系機器のソフトウェアのバージョンが異なっている。このため、待機系機器への切替えが行われると、ATM 制御システム等の周辺システムが待機系機器と接続できず、ATM 等が全面停止する。 ➢ システム構築当初は、周辺機器を含めて切替テストを実施していたが、稼働系機器のソフトウェアのバージョン・アップ実施後、周辺機器を含めた待機系機器への切替テストを行っていない。	・ ソフトウェアのバージョン・アップ等、システムを変更した場合には、切替テストや切替訓練を通じて、周辺システムの稼働状況も確認すること。
	・ 新サービス開始に伴うプログラムリリースを、本来、前営業日の業務終了後に実施すべきところ、サービス開始当日に実施。このため、先日付で登録していたデータが新サービスで認識されない。 ➢ プログラムリリースの手順書に、登録条件を記載していない。	・ 修正プログラムのリリース・タイミングや、リリース順序等にかかる誤りを防止する観点から、リリース手順書を作成すること。
	・ 営業店端末プログラムの更新に当たり、頻繁に利用している「システムセンターからの保守（リモート・メンテナンス）機能」を利用したが、手順書の記載ミスにより、「更新」すべきところ、「消去」した。保守後に稼働確認を行わなかったため、翌営業日になって全営業店の端末が利用できない。 ➢ メンテナンスは、頻繁に行われる作業のため、開発システム環境での作業手順書の確認は行っていないほか、保守後の稼働確認を行っていない。	・ 作業手順書の記載内容の正当性を検証すること。 ・ 保守が意図したとおりに行われたことを、稼働確認等により検証すること。
	・ 修正プログラムを本番系ライブラリーに登録する際、登録情報の一部を誤指定したことにより、当該プログラムではなく別のプログラムが実行される。 ➢ ライブラリー登録手順書に、プログラムの付属情報の登録方法を記載していない。 ➢ 登録結果を検証する仕組みがない。	・ ライブラリー登録時の登録情報や登録結果を検証すること。
	・ 業務処理プログラムとシステムの運行を司る制御プログラムを同一日にリリースする際、本来、オンライン停止後にリリースする必要のある制御プログラムを、業務処理プログラムのリリースとあわせ日中に行ったため、システムが停止する。 ➢ リリース手順や、リリースに係る制約条件等を確認しないまま作業を実施している。	・ 同一日に複数のリリースを実施する場合には、リリースの時間帯にかかる制約の有無を確認すること。また、リリース手順書等にリリース・タイミングを明記のうえ、同手順書等に従いリリースを行うこと。

想定される障害事例と対応策（例）　別添２

分類	想定される障害事例	対応策
４．運用		
（３）プログラムリリース		
	・ ATM の新プログラムを、サービス開始数日前に一斉にリリースしたところ、事前のプログラムリリースに対応していない ATM が一部残存していたため、新プログラムが稼働を開始してしまい、当該 ATM が停止する。 ➢ ATM の機種によっては、リリース作業に制約が生じることを留意していない。	・ プログラムのリリース方法・手順や手段については、予め運用手順を定め、当該手順書に従って実施すること。特に ATM などの場合、機種によりリリース方法等が異なるケースがあることに留意すること。
	・ 現行システムの開発と次期システムの開発を並行して進めている状況下、現行システムに対して、次期システム用に開発していたプログラムをリリースしてしまい、現行システムが停止する。 ➢ 同時並行で進んでいるプロジェクトがある中で、プログラムのバージョン管理体制が整備されていない。	・ 稼働開始時期が異なる複数のシステムで開発を同時並行的に進める場合には、プログラムのライブラリー管理やバージョン管理をより慎重に行うこと。
５．障害対応		
	・ 障害発生時に、関係者の携帯電話に自動通報する仕組みを構築しているが、主要要員の電話番号が間違って登録されており自動通報されない。 ➢ 自動通報機能のテストを行っていない。 ➢ 運用拠点に集まったメンバーは、全員に自動通報されているものと思い込んでいる。	・ 障害内容を自動通報する仕組みでは、登録情報に誤りがないことを定期的ないし要員異動の都度確認すること。 ・ 自動通報が機能しないことを想定した連絡体制も整備すること。
	・ 為替処理にかかるプログラムの不具合により、振込依頼は受け付けられる一方、被仕向金融機関宛ての送信が不能となり、未処理データが大量に発生する。 ➢ コンティンジェンシープランには、振込依頼の受け付けを停止する手順が用意されていない。 ➢ 未処理データを営業店・決済日別に仕分けする仕組みがないため、各営業店が当日日付の自店分決済データを抽出し、手作業で処理することも困難である。	・ 為替や口座振替等、障害時の顧客への影響が大きい取引で未処理データが大量発生した場合を想定したコンティンジェンシープランを、策定すること。 ・ コンティンジェンシープランに基づき未処理明細の特定や再処理方法を明確にすること。 ・ 障害発生箇所により対応が異なるため、想定されるケースに応じたきめ細かなプランを策定すること。 ・ コンティンジェンシープランに基づく実践的な訓練を実施し、その実効性を確認すること。

想定される障害事例と対応策（例）

別添２

分類	想定される障害事例	対応策
５．障害対応		
	・ 対外接続システムが停止したため、コンティンジェンシープランを発動し、滞留データを対外接続先に引き渡すべく MT を作成。この際、データ量が多く、2 本の MT に跨ってデータを作成することとなったが、データが 2 本に跨る場合の MT のフォーマットの一部が、事前に取決めている仕様と異なり、対外接続先で処理ができない。 ➢ MT が 2 本以上に跨るケースのテストを、対外接続先との間で行っていない。	・ 対外接続先との間で授受する MT の仕様に問題がないことを、仕様書やテスト等により確認すること。
	・ 通信機器のハードウェア障害の発生に伴い、稼働系機器から待機系機器への通信経路の切替えが自動的に行われた。しかしながら、オペレーターがアプリケーション・レベルの接続再開コマンドの実行を失念したため、待機系機器が稼働しない。また、通信経路の接続状況は監視対象としているが、アプリケーション・レベルの接続状況は監視対象外としているため、業務処理に支障が生じていることを把握するまでに時間を要する。 ➢ システム稼働開始後、ハードウェア障害時を想定した切替訓練を行っていなかったため、オペレーターが障害時のコマンド入力の必要性を認識していない。	・ 障害マニュアルの整備は、個別手順の記述も含めて行うとともに、訓練を定期的に実施し、その実効性を検証すること。 ・ 重要なシステムについては、業務処理に必要な全ての項目を監視対象とすること。
	・ 障害情報の発信ツールとしてホームページの使用を予定している。もっとも、ホームページへの掲載業務等は外部委託しており、緊急時の外部委託先との連携体制が不十分なため、障害発生の事実や各種サービスの停止のお知らせ等をホームページに掲載するタイミングが、大幅に遅延する。 ➢ 緊急時を想定した委託先・関係先との連絡体制を整備していない。	・ システムの運用を外部委託している場合には、緊急時に備え、運用の機動性を確保すべく、委託先との連携体制等を整備すること。

以 上