BOJ
Reports & Research Papers

2007年3月

リスク管理と金融機関経営に関する調査論文

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

日本銀行金融機構局

目　　次

１．はじめに

金融機関業務におけるコンピュータ・システム（以下、システム）の重要性は一段と高まっており、経営戦略上も重要な地位を占めるに至っている。このため、システム・リスク管理に対する金融機関の関心も強まっている。日本銀行は、これまで幾つかのペーパー[1]を公表し、金融機関のシステム・リスク管理上の留意点を紹介するとともに、考査やオフサイト・モニタリングなどを通じて、適切な対応を働きかけてきた。

しかしながら、考査等においては、リスク管理上適切ではない取扱いが引続き見られるほか、日本銀行へのシステム障害報告も増加しているなど、改善の余地が少なくない。こうした事例の多くは、特定の金融機関だけではなく、全ての金融機関にも共通に生じ得る内容のものである。このため、これらの事例およびその対応策を公表することは、金融機関にとって有益と考えられる。

本稿では、金融機関におけるシステム・リスク管理の現状を整理したうえで、考査等で見られたシステム・リスク管理面の要改善事例やシステム障害事例を基に、システム・リスク管理対策上の具体策を整理し、紹介する。

２．金融機関におけるシステム・リスク管理の現状と問題点

（１）体制整備や環境変化への対応面での問題

今日の金融機関経営において、システムは正確かつ効率的に業務を遂行して行くうえで必要不可欠な存在となっている。また、各金融機関のシステムは相互にネットワーク化され、全体として大きな決済システムを形成しているほか、膨大な顧客情報も処理されている。このため、ある金融機関で、システム障害による業務停止や不正アクセスによる情報漏洩といった、システムに内在するリスクが顕現化した際の影響は、極めて重大である。

こうしたことから、システム・リスクは、金融機関経営における主要なリスクの一つとして位置付けられ、各金融機関では、リスク管理の規程（情報セキュリティ・ポリシー、同スタンダード等）を整備し、これらに基づくシステム・リスク管理対策を推進している。

---

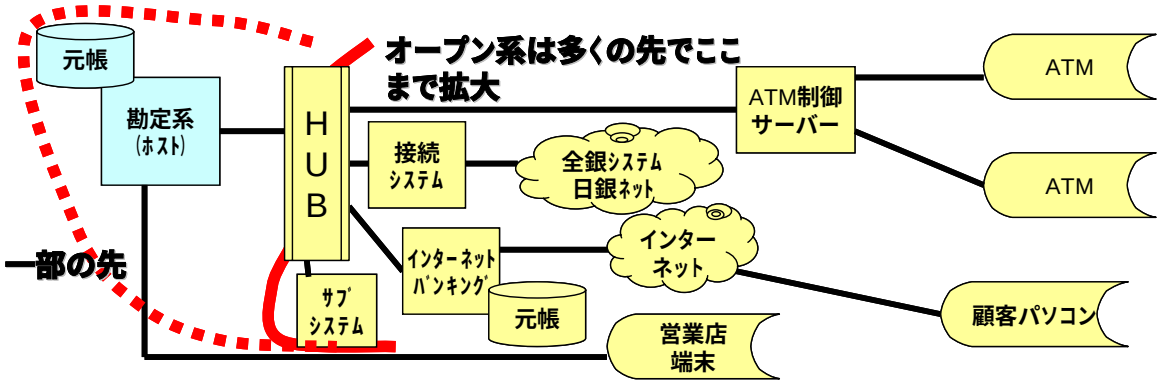
[1] 「金融機関における情報セキュリティの重要性と対応策」（2000 年 4 月）、「わが国金融機関におけるシステムリスクの管理状況と留意点」（2001 年 9 月）。日本銀行ホームページ（http://www.boj.or.jp/）参照。

その一方で、金融機関のなかには、規程やリスク管理の枠組みは定めたものの、規程に則したシステム運用が必ずしも行われていない先や、管理体制が十分に機能していない先も少なからず見受けられる。

また、最近では、システムの大規模・複雑化、技術基盤の変化や、外部委託も含めた開発・運用形態の多様化が進むなかで、金融機関におけるシステム・リスク管理において、以下のような問題点も見られるようになっている。

①システム間のデータ連携が進むなかで、システム全体が十分に把握・監視されていない結果、あるシステムの不具合や処理能力不足がシステム全体の停止や処理遅延に繋がるなど、従来よりもシステム障害時の影響が広範化している事例が見られる。

②オープン系システム[2]の利用が、勘定系システムの中心部分まで拡大するなかで、外部からの不正アクセス等情報セキュリティ面でのリスクが増大しているにもかかわらず、金融機関側のリスク対策が遅れている事例が見られる。



③システム開発・運用の外部委託が進むなかで、本来金融機関自らが行うべきシステムの基本的な要件設定やユーザー受入れテストまでも、委託先任せにする事例が見られる。

（2）システム障害の発生事例からみた分析

日本銀行が取引先金融機関から報告を受けたり、考査およびオフサイト・モニタリングを通じて把握したシステム障害の発生件数は、システムの複雑化や利用範囲の拡大を反映して、近年増加傾向にある。

---

[2] 本稿では、システムの仕様が広く知られており、複数の小型コンピュータ（サーバー）が処理を分散しながら相互に連携し、全体として機能するようなシステムを指す。

こうした障害の発生原因等を分析してみると、以下のとおり金融機関側のシステム・リスク管理を強化することにより、発生を未然に防いだり、発生した場合の影響を小さくできるものが少なくない。

①障害の発生原因を「ハードウェアに起因した障害」等下表の４種類に大別し、その内容をみると、障害の相当部分は金融機関側の適切なリスク管理により回避することが可能である。

ハードウェアに起因した障害	製造元からの与件による面が大きいが、機器の二重化や切替え訓練の実施等により、未然に防げる障害も少なからず存在
ソフトウェアに起因した障害	テスト項目の不足やテスト環境の不備に起因したものが多く、これらはテストの充実等により、防止することが可能
システム性能に起因した障害	システム資源の不足や設定不備が主な原因であり、性能・負荷テストの実施や稼動後の定期的な監視により防止することが可能
運用・保守に起因した障害	人為的なミスによるものが多く、運用手順書やプログラム登録手順書の整備により、防止することが可能

②一定の障害が発生すること自体は避けられないとしても、復旧作業時のリカバリー・ミスなど、不適切な対応が障害の長時間化に繋がっている事例が少なくない。これらについては、障害マニュアルを整備したり、実戦的な訓練の実施を通じて習熟度を高めることにより、復旧時間を短縮するなど障害発生時の影響を小さくすることが可能である。

③近年のシステム共同化の進展につれて、共同センターにおける障害の事例も目立ってきている。共同センターでの障害は、一つのプログラムの不具合や運用ミスが複数金融機関の業務を同時に停止させたり、誤処理に繋がるため、影響が大きい。リスクを削減するためには、ＳＬＡ（Service Level Agreement）の締結や立入監査などを通じた委託先管理の強化により、障害対策の改善を促すことが適当である。

３．システム・リスク管理上の要改善事例と対応策

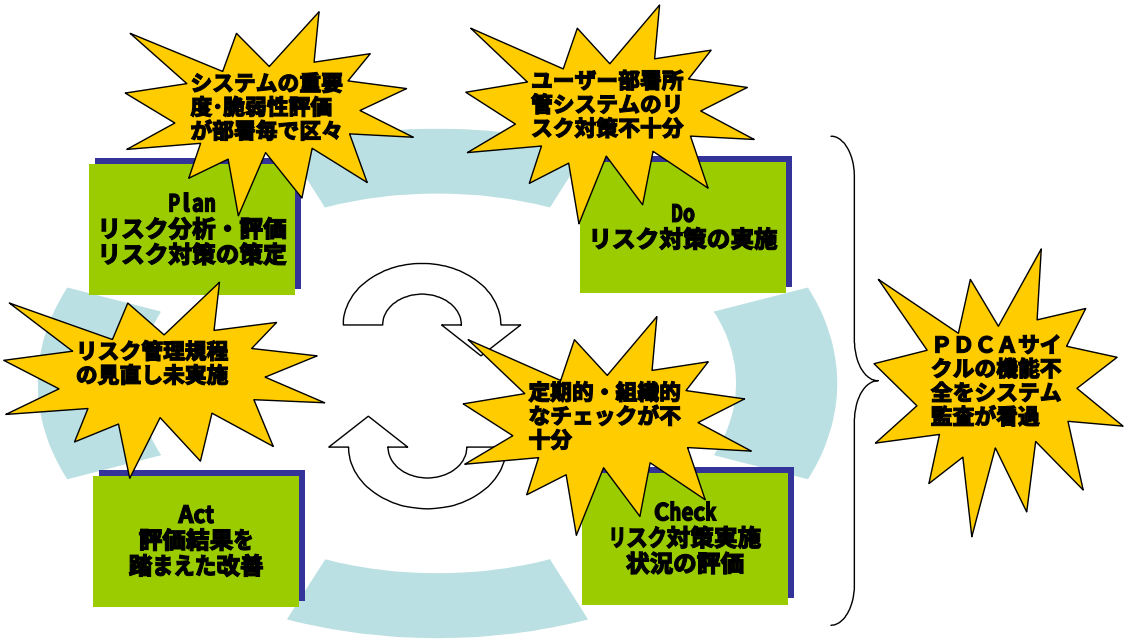
以下では、実際に考査等の場で見られた要改善事例やシステム障害事例等を基に、主な想定事例とその対応策を整理した。また、障害対策および情報セキュリティ対策を進めるうえでの具体的な確認項目として、「想定される障害事例と対応策」（別添１）および「想定される情報セキュリティ侵害に繋がる事例と対応策」（別添２）も作成した（以下で紹介した事例と対応策のうち、冒頭に星印＜★＞のあるものは、別添資料で詳細に説明）。

（１）システム・リスク管理の体制・プロセス

各金融機関では、システム・リスク管理の水準を一定以上に保つため、計画(Plan)、実施(Do)、確認(Check)、処置(Act)という「リスク管理の運用サイクル（いわゆるＰＤＣＡサイクル）」による組織的な管理を進めている。

しかしながら、実際の管理状況をみると、ＰＤＣＡが定期的に実施されていない、管理対象外のシステムがある、個別システムの重要度や脆弱性評価が不徹底であるなど、リスク対策に改善を要する事例が見られる。

事例	対応策
• リスク管理規程（情報セキュリティ・ポリシー、同スタンダード等）が最近のリスク変化を反映したものとなっていない	• 管理サイクルを定期的（年 1 回程度）に回すことにより、リスク管理規程やリスク対策の陳腐化を防ぐこと
• ユーザー部署所管であるため、管理対象から漏れている重要なシステムのリスク対策が十分ではない	• 管理サイクルの対象には、重要なユーザー部署所管システムも含めること
• 個別システムの重要度や脆弱性評価の尺度が評価部署によって異なる	• システムの重要度や脆弱性評価等リスクの分析・評価に当たっては、リスク統括部署による社内横断的なチェックなどにより、全社ベースで評価の目線を揃える仕組みを構築すること
• 管理サイクルの機能不全がシステム監査で見過ごされている	• システム監査においては、個別システムのリスク管理規程に対する準拠性等だけではなく、管理サイクルが全体として機能しているかも検証すること



（２）システム開発管理（システムの統合・共同化プロジェクトなど）

システムの開発管理においては、経営層の重要性認識が不十分な結果、プロジェクト管理体制が全社横断的なものとなっていない事例や、コンティンジェンシー・プランの整備や事務面の対応等システム面以外の作業が漏れている事例が見られる。

また、品質管理では、テスト・ケースの不足やシステム全体を通した検証が不十分な結果、プログラムの不具合が見過ごされている事例がある。さらに、性能管理でも、想定事務量の算出等システムの基本的な要件設定にユーザー部署が関与していないため、実際にシステムを稼動してみると、システムの性能が事務量をカバーし切れず、停止に繋がっている事例が見られる。

稼動判定においては、予め稼動の是非を判定する基準（以下、稼動判定基準）を設けることにより、品質・性能・運用水準を一定レベル以上に保つ仕組みを整えている先が多くなっている。もっとも、稼動判定基準の不備（客観性に欠ける、必要な判定項目が網羅されていない等）により、品質等の確認が不十分なまま、稼動を開始してしまい、トラブルが多発する事例も見られる。

（プロジェクトの管理体制）

事例	対応策
• プロジェクトへの経営層の関与が不足しているため、プロジェクトが抱えるリスクを全社レベルで十分に認識していない	• 重要なプロジェクトについては、役員会等への定期的な報告を求めるなどにより、経営層がプロジェクトのリスクを認識し、適切な指示ができる仕組みを整えること
• 要件定義、システム設計段階でのユーザー部署の関与が十分でないため、総合運用テスト段階に入ってから手戻りが発生する	• プロジェクトの推進に当たっては、システム部署だけではなく、関係者を網羅した検討組織を設置し、十分な意思疎通を図りながら進めること
• 新システムの稼動延期時に必要となる現行システムへの追加開発や、リース・保守期限の延長等の作業が洗い出されていない	• 稼動延期時に必要な作業およびその負荷を予め洗い出し、何らかの事情で稼動延期になる事態にも備えること

（品質管理）

事例	対応策
• テスト時の不具合について、同一ないし類似のロジックを用いた他プログラムに対する横並び検証が実施されていない	• テストで検出された不具合をシステム品質の向上に活かすため、他のプログラムに対する横並び検証を実施すること
★ プログラム修正の際、誤って修正対象ではない箇所も変更したが、テスト項目は本来の変更箇所の検証に限定しているため、誤修正を検出できない	★ 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用いてテストすること ★ 修正プログラムの本番登録に際し、修正前プログラムと差分を比較するなどにより、修正箇所を確認できる仕組みを構築すること

（性能管理）

事例	対応策
★ 大量振込み取引により、取引プログラム内の通番が上限値を超え、システムが停止する	★ システム内に有している各種上限値を管理するとともに、事務量を踏まえた定期的な検証を行うこと
• 想定事務量の算出等システムの性能要件設定を委託先に任せ切っているため、必要なシステム資源（ハード・ソフト）が確保されない	• システムの性能要件設定および性能・負荷テスト結果の検証は、金融機関（ユーザー部署を含む）が主体となって実施すること

（稼動判定）

事例	対応策
• 稼動判定基準が客観的な指標となっていないため、経営陣が適切な判断を下せない	• 稼動判定基準は、できるだけ数値化された客観的な指標を用いること
• 稼動判定基準に事務面の準備状況に関するチェック項目が盛込まれておらず、事務習熟が不十分なまま稼動を開始する	• 稼動判定基準は、システム面だけでなく、事務面・顧客対応面の準備状況に関するチェック項目も盛込むこと
• 外部接続先センター側のフォール・バック（元のシステムに戻す）期限後に最終稼動判定会議を設定しているため、仮に同会議で稼動を延期しても、外部接続先との接続変更は延期できない	• 外部接続先等関係先のフォール・バック期限を調査し、これを踏まえて調整したうえで、それ以前に最終稼動判定を行うこと

（コンティンジェンシー・プラン）

事例	対応策
• 新システム稼動後のコンティンジェンシー・プランは、現行のプランをそのまま使用することになっている	• 新システム稼動後はシステム構成や事務フロー等が変わるため、変更点を洗い出したうえで、現行のコンティンジェンシー・プランを見直すこと
• 新システム稼動後のコンティンジェンシー・プランに基づく訓練が実施されていない	• 新システム稼動後のコンティンジェンシー・プランは、稼動日までに訓練を実施し、その実効性を検証すること

（事務面の対応）

事例	対応策
• 営業店等の事務習熟度を測る客観的な指標がなく、習熟が遅れている店の洗い出しができていないため、当該店に対する事務指導が実施されていない	• 営業店等の事務習熟度について、理解度テスト等客観的な指標で把握できる仕組みを構築し、必要に応じ習熟が遅れている店への指導を実施すること

（３）情報セキュリティ管理

情報セキュリティ管理においては、ウィルス・チェック・ソフトウェアの定義ファイルが適切に更新されていないなど、オープン系システムの利用拡大に管理体制が追い付いていない事例が見受けられる。

また、特にシステム運用部署において、製品の制約上重要ＩＤを共用せざるを得ないシステムであるにもかかわらず、アクセス履歴（ログ）が検証されていないなど、ユーザーＩＤ・パスワード管理の不徹底から、高権限者への牽制が不十分な事例も見られている。

（ユーザーＩＤ・パスワード管理）

事例	対応策
★高権限を有する運用担当者への牽制が不十分なため、不正にプログラムを改造すれば、機密情報が入手可能である	★職務毎の権限設定や操作ログの検証等により高権限者（責任者クラス）に対しても牽制機能を確保すること

（アクセス・ログ管理）

事例	対応策
★アクセス・ログはログイン履歴しか取得しておらず、ファイルへアクセスした者を特定できない ★ログ・ファイルは編集しなければ検証が困難な形式で記録されているため、アクセス・ログの検証が実施されていない ★ログ・ファイルに、一般のユーザーＩＤでもアクセスできるため、ログの改竄・消去が可能である	★アクセス・ログの取得に当たっては、以下の点に留意すること ①アクセス・ログの内容がアクセス者の特定等不正アクセスへの牽制効果を有すること ②アクセス・ログが検証可能な形式で出力される仕組みを構築すること ③アクセス・ログの改竄等ができない仕組みを整えること

（データの暗号化）

事例	対応策
★システム導入時には暗号の脆弱性評価を実施したが、導入後、技術進歩等を織込んだ定期的な脆弱性評価を実施しないまま使用を継続したため、容易に解読可能な状態にある	★暗号技術の利用に当たっては、当該暗号の強度を定期的に評価すること ★暗号の採用に当たっては、総務省および経済産業省が公表している「電子政府推奨暗号リスト」等信頼度の高いガイドライン類を参照し、強度を保つこと

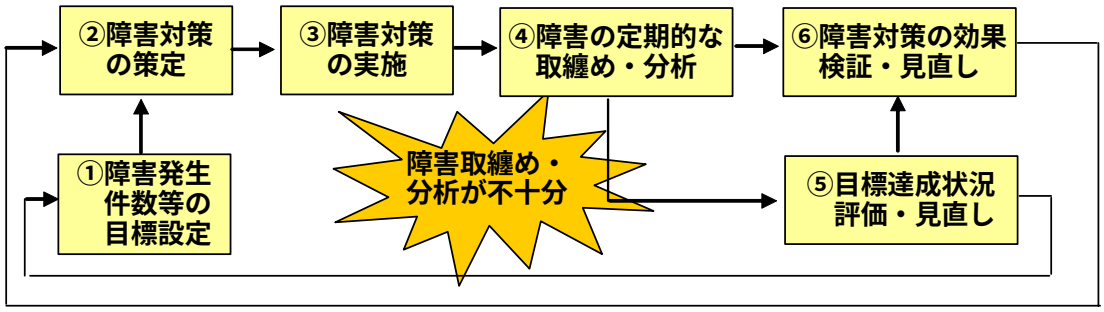
（外部不正侵入・攻撃対策）

事例	対応策
★インターネット上からのみセキュリティ侵害テストを実施しているため、ルータより内部にあるファイアウォールの堅確性が確認されていない	★セキュリティ侵害テストの実施に当たっては、システム構成を理解したうえで、漏れのないテスト内容とすること
★ファイアウォールの外部側に設置された侵入検知システム（ＩＤＳ）の監視端末を経由して、ネットワークの内部側にアクセスできる通信経路（バック・ドア）が存在する	★システムの機器構成を十分に理解し、不正な侵入を許す経路が存在しないシステムを構築すること ★システムの機器構成を変更する際は、不正な侵入を許す経路が生じていないか検証すること

（４）システム障害管理

金融機関経営において、システム障害は直接的な影響とレピュテーショナル・リスクの両面から無視できないものとなっている。このため、障害発生をいかに抑制し安定稼動を確保するか、また障害発生時にいかに迅速・的確な対応を取るかが重要な課題となっている。

障害を抑制するためには、先ず障害発生件数の上限等の目標値を設定し、当該目標達成のために必要な施策を策定･実施することが有効である。次に、発生した障害事例を分析し、その根底にある問題点を見つけ出したうえで、目標値や対策の見直しに繋げる一連の流れを確立することが重要である。



また、障害発生時に適切な対応を取るためには、障害の情報が責任者および関係者間で速やかに共有される必要がある。このため、障害発生時の連絡・報告体制を整備し、かつ適時見直すことが重要である。

しかしながら、実際の障害管理の運営をみると、障害の定期的な取纏めや分析が不十分なため、障害管理が十分に機能せず、障害削減に結びついていない事例や、障害発生時における情報の連絡・報告が後手に回り、初期対応を誤った事例が目立つ。

（障害の定期的な取纏めや分析）

事例	対応策
• 障害件数は取纏めているが、内容の分析は行っていないため、障害の根底にある問題点が洗い出されていない	• システム別・発生原因別等の障害発生傾向を分析することにより、根底にある問題点まで掘り下げたうえで、対応策を検討すること
• ユーザー部署所管システムの障害は、取纏め・分析の対象外のため、再発防止策が十分に検討されていない	• システム所管部署の如何を問わず、重要システムの障害を対象に取纏め・分析を実施すること

（障害発生時の連絡・報告体制）

事例	対応策
• 障害の報告・連絡基準が不明確であるため、システム部署内でしか情報が共有されず、顧客宛ての広報や集中決済機関への連絡など必要な対応が後回しとなる	• 障害の重要度に応じた報告・連絡基準を定め、連絡先を随時更新するなど、必要な関係先に速やかに連絡する体制を構築すること

（５）システム運用管理

システムの運用管理においては、運用・保守ミスが原因の障害が依然として多いほか、復旧作業時のリカバリー・ミスも少なからず生じており、システム運用管理面での改善の余地は大きい。リカバリー・ミスの内容をみると、障害訓練を実施していないため、障害マニュアルの不備が見過ごされたり、障害訓練不足に起因して待機系機器への切替えが失敗するなど、異例時の運用まで手が回っていない事例が見受けられる。

また、一つの運用ミスが大きな障害に繋がるケースもあり、システム・リスク管理において運用管理が果たす役割は大きい。しかし、システムの開発管理に重点が置かれ過ぎていたり、外部業者に全面委託した結果システムがブラック・ボックス化している例も見受けられる。金融機関は、運用管理の重要性を再認識する必要がある。

（運用・保守ミスに起因した障害の防止）

事例	対応策
★稼動系機器が停止し、待機系機器に切替わるはずが、待機系機器のプログラムが別の原因で先に停止していたため、切替えに失敗する	★待機系機器についても、プログラムの稼動状況を含めて監視すること
★バッチ･プログラムのリリース（本番登録）をサービス開始前営業日の業後とすべきところ、サービス開始日の日中に実行したため、エラーが発生する	★修正プログラムのリリース・タイミングや、リリース順序等に誤りを生じさせない観点から、リリース手順書等を作成のうえ、検証する体制を整備すること
★稼動系機器に障害が発生した際に、一部の機能が稼動していると、待機系機器への自動切替え処理が開始されずシステムが停止する。ネットワーク機器の場合には、不安定な状況で短時間に障害と復旧を繰返すと、制御データが大量に発生（輻輳）し、端末の応答時間が遅延する	★監視上は正常に稼動しているように見える場合でも、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

（障害マニュアルの整備・訓練等）

事例	対応策
★振込み依頼が大量に未処理となったが、コンティンジェンシー・プランが事前に作成されていなかったため、有効な代替策が実施されない	★振込み、口座振替え等大量処理を行うシステムで障害が発生した場合は、手作業量が多く顧客影響が大きいため、コンティンジェンシー・プランは、特に重点的に作成すること ★未処理明細の特定や再送信の取扱いを明確にすること
★待機系機器への切替えには、機器の自動切替え後、コマンドを入力する必要があったが、同手順が障害マニュアルに記載されていなかったため、切替えに失敗する	★障害マニュアルの整備を、個別手順の記述まで漏れのないようきめ細かく行うとともに、それに基づく実機訓練を定期的に実施し、その実効性を検証すること
★外部センターとの中継システムが停止したため、同センターに代行処理を依頼したが、持込み磁気テープの仕様が基準と異なり、処理ができない	★外部センターに代行処理を依頼する際に持込む磁気テープ等の仕様を確認するとともに、持込み手順の相互認識を一致させること

４．おわりに

日本銀行としては、各金融機関が自社システムの特性に応じたリスクの所在を認識したうえで、以上に述べた事例と対応策を自らのリスク管理の評価に活用することにより、各種リスク対策の改善に役立てて頂くことを期待している。

また、これらのリスク対策は、情報通信技術の進歩や新たな金融犯罪の出現等に合わせて、随時見直して行く必要がある。

以　　上

（本件に関する照会先）
日本銀行金融機構局
システム関連考査担当　03-3277-2992
岩佐 智仁　　河本 勝也

別添1

想定される障害事例と対応策

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え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。
	・ 稼動系機器に障害が発生した際に、一部の機能が稼動していると、待機系機器への自動切替え処理が開始されずシステムが停止する。 ネットワーク機器の場合には、不安定な状況で短時間に障害と復旧を繰返すと、制御データ（パケット）が大量に発生（輻輳）し、端末の応答時間が遅延する。	・ 監視上は正常に稼動しているように見える場合でも、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。
2．ソフトウェア		
(1)制御プログラム	・ サーバーのメモリー領域が、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、徐々にメモリー使用可能領域が減少し、稼動から数日経過した段階でシステムが停止する。 ➢ テスト段階では、頻繁にサーバーを停止しており、実運用に即した数日間連続した稼動テストを実施していない。	・ 実運用に即した数日間連続した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。
	・ 機器Aの障害が原因で、機器BとCとの通信が遮断された。機器B、C共に正常な状況のため、自動再開処理が実行されたが、プログラムの不具合から、システムが停止する。 ➢ 自動再開処理のテストでは、機器Bの障害を想定し、バックアップ機器B'とCが自動再開することを確認していたが、機器B、機器Cが共に正常な状況で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なか、直接接続していない機器から受ける影響までを洗い出したうえで、テスト項目を作成すること。

別添１

想定される障害事例と対応策

分類	想定される障害事例	対応策
２．ソフトウェア		
(2)業務プログラム	・ 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、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え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、外部接続先を含むテスト（END-TO-END のテスト）を行うこと。
	・ 休日に本番システムのソフトウェアのバージョン・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現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・アップ後の稼動確認では、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。	・ 業務処理の稼動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、業務処理を含めて稼動確認を行うこと。
	・ ATM の振込み処理では、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。このため、このデータを用いて振込み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る。しかしながら、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、被仕向け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り、被仕向け金融機関まで巻き込んだ振込みテストを実施していない。	・ 対外接続系業務においては、外部接続先を含むテスト（END-TO-END のテスト）を実施すること。 ・ 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。

別添１

想定される障害事例と対応策

分類	想定される障害事例	対応策
２．ソフトウェア		
(2)業務プログラム	・ 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することにより、不具合が発生する。 ➢ 修正後のテストが、本来の変更箇所の検証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。 ・ 修正プログラムを本番登録（リリース）する際、修正前プログラムと差分を比較するなど、修正箇所を確認できる仕組みを構築すること。
	・ 外部センター宛ての振込みデータが、障害により大量に滞留した。数時間後、復旧したが、当日決済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が処理し切れない。	・ 当日分の処理を優先して行えるような機能を付しておくこと。
	・ 取引件数の増加により、取引通番が１日の上限値を超え、超過分の取引通番については、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。	・ システム内に有している各種の上限値を管理すること。 ・ 当該上限値と取引データ等の実績値を踏まえた定期的な検証を行うこと。
３．性能関連		
(1)処理能力	・ CPU 処理能力の増強の結果、プログラムの応答時間が極めて短時間となったことから、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、応答時間を０秒と認識したため、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。

別添1

想定される障害事例と対応策

分類	想定される障害事例	対応策
３．性能関連		
(1)処理能力	・ 取引件数の増加に伴い、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行った。レスポンスが向上した結果、想定件数以上の取引をWEB サーバーが受付けた。WEB サーバーの処理能力には余裕があったため処理できたが、後続処理を行うAP サーバーは、想定件数までの処理能力しか有しておらず、AP サーバーの能力不足によりシステム全体がスローダウンする。 ➢ テストでは、「想定件数」での負荷試験は行ったものの、「(システムの) 許容最大件数」では行われていない。 また、想定件数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。 ・ 大量データを扱うオンライン処理において、データ毎に同一のエラーが発生し、大量のエラー・メッセージがCPU に命令を与える操作端末（コンソール）に表示された。このため、コンソールが表示処理に手一杯となって、CPU に応答できなくなり、システムが停止する。	・ 一部システムの能力増強を行う際に、システム全体のピーク時処理量の整合性を踏まえた性能評価を行うこと。 ・ その際に、「想定件数」に加えて、「許容最大件数」の性能負荷試験を行うこと。 ・ WEB システムにおいて、アクセスを制限できる仕組み（流量制限）を設けること。 ・ 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。
(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した。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。 このサーバーは、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延する。 ➢ テストでは、顧客を含め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。	・ 本番システム環境と同等の性能評価テストを行えない場合、設定値は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。

別添1

想定される障害事例と対応策

分類	想定される障害事例	対応策
3．性能関連		
(2)設定値	・ 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。	・新たなサービス開始に伴いリソースを試算する際、過去の使用状況を踏まえて算出すること。
	・ ディスクに記録されている取引履歴を、6 ヶ月に 1 度 MT（磁気テープ）へ退避する運用を行っている。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 ヶ月で容量を超過しシステムが停止する。	・ 取引量の変動の大きいシステムについて、システム・リソースの確認タイミングを柔軟に見直すこと。
	・ 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、稼動系機器よりも待機系機器の方が小さくなり、稼動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。	・ 稼動系機器と待機系機器の設定値に差異のないことを、システム構築時および設定変更時に確認すること。
4．運用・保守関連		
(1)運行監視	・ 稼動系機器に障害が発生し、待機系機器への切替え処理が実行されたが、待機系機器で稼動する切替え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、プログラムの稼動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、プログラムの稼動状況を含めて監視すること。

別添1

想定される障害事例と対応策

分類	想定される障害事例	対応策
4．運用・保守関連		
(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 の稼動開始が遅延する。 ➢ 前日のバッチ処理はオンライン開始の 6 時間前に完了しており、システムの立上げ開始時刻を早めることが可能であるにもかかわらず、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の復旧時間を含め、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。原因究明に時間を要し、業務開始時刻を過ぎる。原因究明後、定例バッチ処理を再実行するが、業務開始時刻を過ぎると当該バッチ処理を起動できない仕様のため、再実行できず業務開始時刻が大幅に遅延する。	・ 臨時作業を実施する際は、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。 ・ バッチ作業の自動処理が停止した場合に備えて、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。
	・ 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延が生じ、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、営業店までに留まり、事務集中センターを含めた全体で行っていない。	・ テストでは、全ての業務関連先を対象として、ピーク日事務量による確認を行うこと。
(3)障害訓練等	・ 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。 ➢ 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み、主要要員到着を待ち続け初期対応が遅延する。	・ 障害内容を自動通報する仕組みは、定期的に情報が正しいことを確認すること。 ・ 当仕組みが機能しないことも想定した連絡体制を確立すること。

別添1

想定される障害事例と対応策

分類	想定される障害事例	対応策
４．運用・保守関連		
(3)障害訓練等	・為替処理において、プログラムの不具合により、振込み依頼は受付けられるものの、被仕向け金融機関に送信できずに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、振込み依頼の受付けを停止する手順が用意されておらず、未処理件数が増加し続け影響範囲が拡大する。 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く、営業店毎に当日日付の決済を手作業で処理することも困難である。	・ 為替、口座振替え等大量取引を扱い顧客影響の大きい処理において、大量の未処理データが発生した場合の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・プランに基づく実戦的な訓練を実施し、その実効性を確認すること。
	・ 対外接続システムが停止した際、コンティンジェンシー・プランを発動し滞留データを MT に出力し対外接続先に渡すプログラムを実行した。その際、データ量が多く 2 本のテープに跨ってデータを作成したが、2 本目のテープのフォーマットが、事前に取決めている仕様と異なっているため、対外接続先では処理ができない。 ➢ MT が 2 本以上に跨るケースのテストを行っていない。	・ 持込み MT の仕様確認を行うこと。また、持込み手順を明確にし、関係者間で認識を共通化しておくこと。

別添1

想定される障害事例と対応策

分類	想定される障害事例	対応策
4．運用・保守関連		
(3)障害訓練等	・ 通信機器のハードウェア障害の発生に伴い、稼動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、待機系機器が稼動しない。 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。 ➢ システム稼動開始後、ハードウェア障害時を想定した切替え訓練を行っていなかったため、オペレーターは障害時のコマンド入力の必要性を認識していない。	・ 業務処理に必要な全ての項目を監視対象とすること。 ・ 障害マニュアルの整備を、個別手順の記述まで漏れのないようきめ細かく行うとともに、それに基づく実機訓練を定期的に実施し、その実効性を検証すること。
(4)プログラム・リリース	・ 外部接続システムに接続端末を追加登録する際、開発システム環境の端末定義を残したままリリースしたため、外部接続先との処理が不能となる。 ・ 勘定系システムにおいて稼動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えテストを実施していたが、稼動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えテストを行っていない。	・ 本番システム環境にリリースする際には、変更前の定義と変更後の定義を比較し、変更箇所を確認すること。 ・ 切替えテストは、周辺システムの稼動確認を含めて行うこと。 ・ ソフトウェアのバージョン・アップ等システム変更後は切替え訓練を実施すること。

別添1

想定される障害事例と対応策

分類	想定される障害事例	対応策
4．運用・保守関連		
(4)プログラム・リリース	・ 新サービス開始に伴うプログラム・リリースを、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した結果、先日付登録されていたデータが、新サービスに認識されない。 ➢ テストでは、当該バッチ処理の稼動確認を行っているが、登録時期を記載した手順書の確認は行われていない。	・ 修正プログラムのリリース・タイミングや、リリース順序等に誤りを生じさせない観点から、リリース手順書等を作成のうえ、検証する体制を整備すること。
	・ 営業店端末プログラムを遠隔地から保守（リモート・メンテナンス）する際に、手順書の記載ミスにより、更新ではなく消去したため、全営業店の端末が利用できない。 ➢ リモート・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テストは行っていない。	・ 作業手順書の記載内容の正当性を確認する体制を整備すること。
	・ 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てしまう。	・ ライブラリー登録時の登録情報や登録結果の検証体制を確立すること。

以 上

別添２

想定される情報セキュリティ侵害に繋がる事例と対応策

分類	想定される情報セキュリティ侵害に繋がる事例	対応策
１．管理対象システム	・ ユーザー部署が独自に導入した個人情報を扱うシステムが、システム・リスク評価の対象となっていないため、アクセス履歴（ログ）が定期的に検証されていない。	・ ユーザー部署が独自に導入したシステムに対しても、その重要度に応じ、規程に定めた統一的な基準で、情報漏洩対策等を実施すること。
	・ システム管理台帳への記載基準が明確でないため、あるサブ・システムが記載から漏れ、ウィルス・チェックの対象外となっている。	・ 設置機器と、システム管理台帳の情報を定期的に突合すること。 ・ 同台帳の記載基準を定期的に見直すこと。
	・ 本番システムに対する基本ソフトウェアの修正プログラム（パッチ）の適用は、ホスト系は運用部署、オープン系は開発部署が行う取決めとなっているが、ホスト系とオープン系を接続する機器については管理部署を明確にしていなかったため、ソフトウェア修正を長期間実施していない。	・ 開発から運用への引継ぎの際に、管理部署を明確にすること。 ・ 管理されていない機器がないか、定期的に検証する仕組みを構築すること。
２．ユーザーID・パスワード管理	・ １人の運用担当者に、あらゆるアクセス権限とプログラム・ソース・コードの参照権限が付与されており、作業に対する検証も行われていないため、当該担当者が不正にプログラムを改造したうえで、機密情報を入手することが可能となっている。	・ 相互牽制が可能なように、職務毎に権限設定を付与したうえで、アクセス・ログを定期的に検証することにより、高権限者（管理者クラスを含む）に対しても、牽制機能を確保すること。
	・ 高権限 ID・パスワードを委託先に貸与しているが、アクセス・ログの検証等牽制体制が確保されていないため、委託先が行った重要な操作を把握できない。	・ 高権限 ID・パスワードを委託先に貸与する際には、アクセス・ログの定期的な検証や、必要の都度パスワードを伝達し、作業後にパスワードを変更する運用など、牽制体制を確保すること。

別添２

想定される情報セキュリティ侵害に繋がる事例と対応策

分類	想定される情報セキュリティ侵害に繋がる事例	対応策
２．ユーザーID・パスワード管理	・ ユーザーID･パスワードをファイルに記録しているシステムにおいて、本番移行後にも開発時の設定のまま当該ファイルへのアクセスを制限していない。このため、全ユーザーがID・パスワードを参照可能となっている。	・ 開発部署から運用部署に引継ぎを行う際、ファイルのアクセス権限を含めて、本番環境用に変更すること。 ・ 特に、ユーザーID･パスワードを記録したファイルがある場合には、適切なアクセス権限を設定すること。
	・ パッケージ・ソフトウェアの制約等により、プログラムにユーザーID・パスワードを埋め込んでいるため、パスワードを長期間変更していない。	・ ユーザーID･パスワードをプログラムに埋め込まず、別ファイルに保存し、プログラムが必要な都度参照する方式（引数）とするなど、容易に変更可能な仕組みを構築すること。
	・ 人事異動が行われた際に、IT 部署に対するユーザーID の削除依頼を失念したうえ、登録状況を定期的に確認していないため、長期間にわたり、異動者が前所属のユーザーID を利用可能となっている。	・ 異動者のユーザーID を速やかに削除する体制・仕組みを整えること。 ・ ユーザーID と在籍者リストとの照合を定期的に実施し、職務上アクセスの必要のない者に権限を付与していないことを確認すること。
	・ 資金移動処理において、規程上は「データ入力は担当者、送信は管理者」と定めているが、システムの権限体系上は、管理者にデータ入力と送信の両方の権限が付与されているため、資金移動の処理を単独で行うことが可能となっている。	・ 重要な処理は、管理者であっても単独で行えない権限体系をシステムに組み込むこと。

別添２

想定される情報セキュリティ侵害に繋がる事例と対応策

分類	想定される情報セキュリティ侵害に繋がる事例	対応策
３．アクセス・ログ管理	・ 重要ファイルへのアクセス権限を複数のユーザーに付与しているが、システムへのログイン・ログアウト履歴しか取得していないため、当該ファイルへアクセスした者を特定できない。	・ アクセス･ログの内容は、誰が、どのファイルに、いつアクセスしたかを特定できるものとすること。 ・ アクセス･ログの内容が機能制約等により限定される場合には、アクセス権限（範囲）を絞り込むことにより、システムで不正行為があった場合に、実行者を特定できる仕組みを構築すること。
	・ アクセス･ログが記録されたファイルへのアクセスを制限していないため、一般のユーザーID でもアクセス・ログの改竄・消去が可能となっている。	・ アクセス・ログに対する改竄・消去を防止するため、ログ・ファイルへのアクセス権限を適切に設定すること。
	・ アクセス･ログは、編集しなければ検証が困難な形式で記録されているため、実際には検証がなされていない。	・ アクセス･ログが検証可能な形式で出力される仕組みを構築すること。
４．機器・外部記憶媒体管理	・ CPU に命令を与える操作端末（コンソール）がログインしたままの状態で放置されている。このため、同一フロア内の要員は誰でも、操作者が特定されない状況で、システムを不正に利用できる。	・ コンソールにパスワード付きスクリーン・セイバーを設定する等により、不正アクセスを防ぐ対策を講ずること。
	・ 外部記憶媒体の使用をシステム的に制限しているパソコンで、管理者の許可により一時的に制限を解除したが、使用後、担当者が再設定を失念する。管理者も設定状態の確認をしなかったため、外部記憶媒体が常時使用可能となっている。	・ 一時的に外部記憶媒体の使用を解除する際に備えて、①設定の解除および再設定手順を明確にすること、②再設定漏れを想定し、定期的にパソコンの設定を確認すること。

別添２

想定される情報セキュリティ侵害に繋がる事例と対応策

分類	想定される情報セキュリティ侵害に繋がる事例	対応策
４．機器・外部記憶媒体管理	・ パソコンでの FD 使用をシステム的に制限しているが、USB 接続の外部記憶媒体（USB メモリー、MO 等）は、何ら制限なく使用可能となっている。	・ 外部記憶媒体の使用を制限している場合、接続可能な全ての媒体について、扱いを明確にすること。
	・ マシン・エリアの出入口において、FD や MT（磁気テープ）の持出しを防止するため、「人」に対しては金属探知機でチェックを行っているが、「携行品」に対するチェックは行っていない。	・ 携行品を含め、適切なチェックを行うこと。 ・ 出入口における携行品のほか、MT 搬送用コンテナ等もチェック対象に含めること。
５．データの暗号化・暗号技術評価	・ 重要データについては、伝送経路上で暗号化しているが、データ入力・蓄積機器上では、暗号化されていないため、元データ（平文）を読み取ることが可能となっている。	・ 重要データについては、入力から、伝送経路上、蓄積まで一貫して暗号状態を保つこと。 ・ 保たれない場合には、データへのアクセスを排除または限定し得る環境を構築すること。
	・ 重要データを蓄積・伝送する際に暗号化しているが、暗号の強度（暗号アルゴリズム、鍵長等）を評価せずに、暗号化装置等を導入している。 または、導入当初の暗号の強度評価は実施しているが、導入後、技術進歩等を織込んだ定期的な強度評価を実施していない。	・ 暗号の強度について、当該システムの重要性および利用環境（インターネットのように不特定多数が接続可能か等）を考慮したうえで、採用する暗号の強度を評価すること。また、定期的に強度評価を見直すこと。 ・ 暗号の採用に当たっては、総務省および経済産業省が公表している「電子政府推奨暗号リスト」等信頼度の高いガイドライン類を参照し、強度を保つこと。
６．外部不正侵入・攻撃対策	・ セキュリティ侵害テストを定期的に実施しているが、機器構成変更時やファイアウォールのバージョン・アップ時には、実施していない。	・ システムの機器構成等を変更した場合には、直後にセキュリティ侵害テストを実施すること。

別添２

想定される情報セキュリティ侵害に繋がる事例と対応策

分類	想定される情報セキュリティ侵害に繋がる事例	対応策
６．外部不正侵入・攻撃対策	・ セキュリティ対策としては、ファイアウォールの侵害テストしか行っておらず、基本ソフトウェアに対するパッチの適用や、WEB アプリケーションの脆弱性検証を行っていない。	・ セキュリティ対策は、侵害テスト等で把握可能なネットワークの対策と、基本ソフトウェアに対するパッチの適用等ソフトウェアの両面から実施すること。
	・ セキュリティ侵害テストを、インターネット上からのみ実施しているため、侵害行為の殆どはルータで止められてしまい、ルータより内部にあるファイアウォールの堅確性が確認できていない。 また、ファイアウォールは、多段構成としているが、1 段目しかテストしていないため、2 段目以降の堅確性を確認できていない。	・ セキュリティ侵害テストは、設置している機器の役割を的確に理解したうえで、インターネット側からの侵害テストに加え、1 段目、2 段目以降のファイアウォールの堅確性も評価できる内容とすること。
	・侵入検知システム（IDS）をファイアウォールの外部側にのみ設置している。このため、ファイアウォールを通過してきた、真に危険な攻撃が検知できない。	・IDS の機能を的確に把握し、使用目的に応じて、適切な位置に設置すること。
	・ インターネットに接続している WEB サーバーにおいて、内部の保守作業用に、リモート制御用プログラム（telnet 等）を常時稼動させているため、外部からの不正侵入に悪用される可能性がある。 メンテナンス作業は月 1 回程度であり、同作業の利便性よりリモート制御機能が悪用される危険性の方が高い。	・ telnet 等リモート制御用のプロセスは、利便性と安全性の観点から、必要性を見極めたうえで稼動させること。
	・ 堅確性を高めるため、ファイアウォールを多段構成としているが、全て同一機種のため、当該ファイアウォールの脆弱性を踏まえた攻撃を受けた場合、有効な防御にならない。	・ ファイアウォールを多段構成とする場合、異なる機種で構成すること。

別添２

想定される情報セキュリティ侵害に繋がる事例と対応策

分類	想定される情報セキュリティ侵害に繋がる事例	対応策
６．外部不正侵入・攻撃対策	・ ファイアウォールより外部側のネットワークと内部側のネットワークを IDS により監視しているが、監視端末が両ネットワークで共通となっている。 監視端末とネットワークはルータで接続されているため、このルータ経由で外部側のネットワークからファイルウォールを経由せず内部側のネットワークにアクセスできる経路（バック・ドア）が存在する。	・ システムの機器構成を十分に理解し、不正な侵入を許す経路が存在しないシステムを構築すること。 ・ システムの機器構成を変更する際には、不正な侵入を許す経路が生じていないか検証すること。
	・ DoS 等サイバー攻撃に対する検知基準が、旧来の攻撃手法を基に作成されているため、陳腐化している。 このため、新たな手法のサイバー攻撃を受けた場合、検知に時間を要する、またはサーバーが停止する可能性がある。	・ 新たなサイバー攻撃手法を積極的に情報収集し、検知基準や対策の見直し要否の評価を定期的に実施すること。 ・ サイバー攻撃によるサービス停止時間を最小限に抑えるため、検知基準と攻撃への対応手順を定めること。
７．コンピュータ・ウィルス対策	・ ネットワークに接続している開発端末や、外部記憶媒体の利用が可能なスタンド・アロン端末は、 ウィルスに感染するリスクおよび他に感染させるリスクがあるが、ウィルス・チェック・ソフトウェアが導入されていない。または、定義ファイルが適切に更新されていない。	・ ウィルス・チェック・ソフトウェアの導入・運用基準を定めるにあたっては、①外部記憶媒体授受の有無、②ネットワーク接続の有無（LAN かスタンド・アロンか）により感染リスクを評価し、検証すること。
	・ ウィルス・チェックは、常駐検知機能によるチェックのほかに、全ファイルへの定期的なチェックを定めているが、以下の点ができていない。 ①定期的な全ファイル･チェックを過信して、常駐検知機能の正常稼動を確認していない ②全ファイルへの定期的なチェックを自動化したが、実施結果を確認していない	・ ウィルス･チェックの運用にあたっては、①定義ファイル更新前の新種ウィルスの侵入可能性、②常駐検知機能停止時のウィルスの侵入可能性、③常駐検知対象外のファイルの存在、に留意し、ウィルス・チェックの正常稼動・実施結果を確認すること。

別添２

想定される情報セキュリティ侵害に繋がる事例と対応策

分類	想定される情報セキュリティ侵害に繋がる事例	対応策
８．スパイウェア・フィッシング対策	・ インターネットを利用した取引において、以下のようにデザインや利便性を重要視した作りとなっているため、フィッシング詐欺の対象とされやすい。 ① アドレスバーを表示していないため、利用者が正当なサイトであることを確認できない。 ② 顧客宛の重要な「お知らせメール」に URL を恒常的に記載しているため、偽サイトに誘導するフィッシング・メールに対する顧客の警戒感が薄れる。	・ インターネット・バンキング・システムの脆弱性を、アプリケーション面からも検証すること。 ・ メールに URL を添付しないポリシーとする等、フィッシング詐欺対策を適切に策定すること。
	・ ユーザーID とパスワードのほかに、乱数表を用いた第 2 パスワードを入力する方式(チャレンジ・レスポンス方式)において、第 2 パスワードの入力画面の「取消」を実行し、再度入力画面を表示させる都度、要求される第 2 パスワードが変更される仕組みとなっている。 このため、スパイウェア等により入手した第 2 パスワードに一致する乱数表の組み合わせと同じ値が表示されるまで、「取消」を実行することで、入手したパスワードでの不正取引が可能となっている。	・「取消」処理を含めた全処理パターンについて、本人認証機能に脆弱性がないか検証すること。
	・ 異常取引検知のため、資金移動や重要情報の変更等「重要操作」の都度、その内容を電子メールで顧客に通知する仕組みとしている。 しかし、通知先メール・アドレスの変更が「重要操作」に指定されていないため、犯罪者が不正取引に先立ってメール・アドレスを変更した場合、顧客は異常取引に気づくのが遅れる。	・ 「重要操作」が実行された都度、その内容を顧客に通知する仕組みを構築すること。 ・ 顧客に通知する「重要操作」の指定に漏れが生じていないか定期的に検証すること。

別添２

想定される情報セキュリティ侵害に繋がる事例と対応策

分類	想定される情報セキュリティ侵害に繋がる事例	対応策
８．スパイウェア・フィッシング対策	・ 24 時間利用可能なインターネット・バンキングの問合せ窓口を、日中のみとしているため、顧客が夜中にフィッシング詐欺にあった場合等に、連絡・相談する窓口がない。	・ インターネット・バンキング・サービスを提供している場合、サービス時間中の顧客問合せ窓口を用意すること。また、受付時の社内関係部署間の連絡体制を整備すること。

以　上