金融高度化セミナー資料

2012年5月

システムリスク管理と
障害管理体制の実効性確保

日本銀行　金融機構局

日本銀行
BANK OF JAPAN

本日の説明内容

日本銀行金融機構局の公表資料

・「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」（2007年3月）

・「金融機関におけるシステム障害に関するリスク管理の現状と課題」（2010年11月）

・「システム障害管理体制の実効性向上に向けた留意点」（2012年2月）

を基に、システムリスク管理とシステム障害管理体制の実効性確保に関する留意点を説明。

Ⅰ．システムリスク管理の具体策

Ⅱ．システム障害に関するリスク管理の現状と課題

Ⅲ．システム障害管理体制の実効性向上に向けた留意点

Ⅰ.システムリスク管理の具体策

1. システムリスク管理の観点
2. システムリスク管理における8つのポイント
3. 情報セキュリティに関する具体的な留意点

1. システムリスク管理の観点

観　点	内　容	具体的なリスクの例
安定性 （可用性）	・災害、障害等からのシステムの保護	・システム・ダウンによる業務停止
安全性 （機密性） （完全性）	・犯罪、不正行為等からのシステムの保護	・内部不正による顧客情報の漏洩 ・ハッカーによる不正アクセス
信頼性	・システムが提供する情報や機能の正確性確保	・システムの提供する情報の誤りによる業務トラブルの発生
遵守性	・法令・規制・規程の遵守	・レピュテーションの低下
有効性	・経営や戦略の策定・実現に必要な情報機能の提供	・不十分な情報に基づく経営戦略の策定
効率性	・高い生産性での情報・機能の提供	・システムの開発・運用コスト増加 ・ ステムの拡張性・柔軟性の低下

2. システムリスク管理における8つのポイント

(1)システムリスク管理の体制・プロセス

- ・経営陣の関与
  - ― リスク認識、リスク管理体制の整備
  - ― リスクや環境の変化を踏まえた同体制の見直し
  - ― システム企画(IT戦略)、システム開発、システム運用、システムリスク管理等に関する経営レベルの会議の開催
- ・企画・開発・運用・リスク管理にかかる規程の整備
  - ― 基本方針、セキュリティポリシー、同スタンダード等の整備
- ・システムリスク管理に関するPDCAサイクルの確保
  - ― EUCを含めたシステムの洗出し、重要度ランクの付与、実施基準の策定

2. システムリスク管理における8つのポイント（続き）

（2）システム企画

・案件採択に関する手順の策定

― システム化ニーズの意向集約から案件採否の決定までの手順の策定

・システム投資に関する事後評価

2. システムリスク管理における8つのポイント（続き）

（3）システム開発

- プロジェクトの進捗管理体制の整備
  ― IT部署、ユーザー部署、外部委託先間での情報共有体制
- 品質管理体制の整備
  ― テストケースの十分性確認、システム全体を通じた検証
- 性能評価体制の整備
  ― ユーザー部署も関与した想定事務量の算出とテストの実施
- 稼働判定（プログラムリリース）基準の策定
  ― 開発工程完了基準・稼働開始基準の策定

2. システムリスク管理における8つのポイント（続き）

（4）システム運用

- オペレーション管理体制の整備
  — 相互牽制体制、マニュアルの整備
- 本番データ管理体制の整備
  — 媒体管理、本番データ貸出ルールの策定
- 機器管理（キャパシティやパフォーマンスの管理）基準の策定
  — CPU、ディスクなどの使用量のほか、各種設定値の上限値に近づいた場合のモニタリング基準の策定

2. システムリスク管理における8つのポイント（続き）

（5）外部委託先管理

- 契約書・サービスレベル仕様書等による役割分担の明確化
- 各階層（経営陣、部長クラス、担当者クラス等）における会議の開催
- 立入調査の実施
- 再委託、再々委託の有無の確認

2. システムリスク管理における8つのポイント（続き）

（6）システム障害管理

- システム障害管理体制の枠組みの整備
  - ― 障害の重要度ランクの認定基準
  - ― 経営陣に対する障害報告基準
- 障害の傾向分析と再発防止策の策定
  - ― 対象業務、障害原因（ハード障害、ソフト障害、操作ミス等）、背景等を分析し、再発防止策を策定
- コンティンジェンシープランの策定
  - ― 障害シナリオの策定
  - ― 同プランの記載項目（影響範囲、復旧目標時間等）の標準化
- 障害訓練の実施
  - ― 外部委託先やユーザー部門を含めた訓練の実施

2. システムリスク管理における8つのポイント（続き）

（7）情報セキュリティ対策

- ユーザー部署を含めた情報セキュリティ対策の策定
  - ― ID・パスワード管理、アクセス制御、ログ取得基準、ウィルス対策等

- インターネット利用業務におけるサイバーテロ等外部からの攻撃への対策
  - ― Webサイトへの大量データ送信による業務妨害対策、標的型メールによるウィルス感染による情報漏洩対策

- 顧客にかかる情報セキュリティ面の対策
  - ― フィッシングサイトへの誘導または偽装メールを通じた現金詐取等への対応（可変式パスワードや電子証明書の導入等）

2. システムリスク管理における8つのポイント（続き）

（8）システム監査

- リスクプロファイルの把握
  ― 規程等の遵守状況の確認だけではなく、リスクプロファイルの抽出が適切にできているかを確認
- リスクプロファイルの変化に応じた監査の実施
  ― 監査計画を立て、効果的に監査を実施（外部監査も活用）
- 内部監査等で判明した問題点の改善状況のフォローアップ
- オープン系システムの利用拡大や新技術の採用など、システムリスクのプロファイルの変化を踏まえた監査要員の育成

3. 情報セキュリティに関する具体的な留意点

― システム開発やシステム運用等に関する留意点は、Ⅲ章「システム障害管理体制の実効性向上に向けた留意点」で紹介

（1）顧客が晒されるリスクへの対応

- フィッシングサイトや偽装メールを通じた現金搾取が発生。全銀協、全信協では「可変パスワードや電子証明書といった固定式のID・パスワードのみに頼らない認証方法の導入を図る」ことを申し合わせ

▽セキュリティ対策の一例

セキュリティ対策	対策内容
×単一要素認証	ID・パスワードのみによる認証
×複数要素認証（知識認証）	ID・パスワードの認証に加え、合言葉の入力や画像選択による認証
◎同（所有物認証＜乱数表＞）	同、乱数表で指定された数字の入力による認証
◎同（所有物認証＜トークン＞）	同、パスワード生成装置（トークン）指定された数字の入力による認証
△同（生体認証）	同、手のひら等の静脈による認証
△クライアント電子証明書	自社が顧客の端末の正当性を確認（顧客に電子証明書を配布）
（サーバ電子証明書）	（顧客が接続先の正当性を確認＜自社のシステムに電子証明書を導入＞）
（資金移動時のメールサービス）	（顧客が資金移動の発生を即時に認識）
（通信データの暗号化）	（自社・顧客間の送受信データを暗号化）

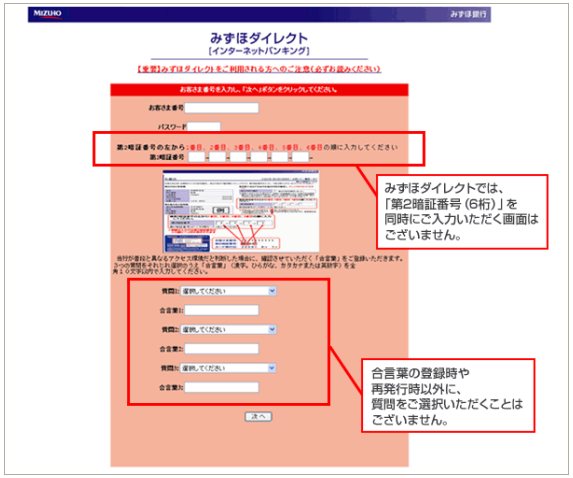
顧客認証方式
×固定式
△固定式ながら
偽造困難

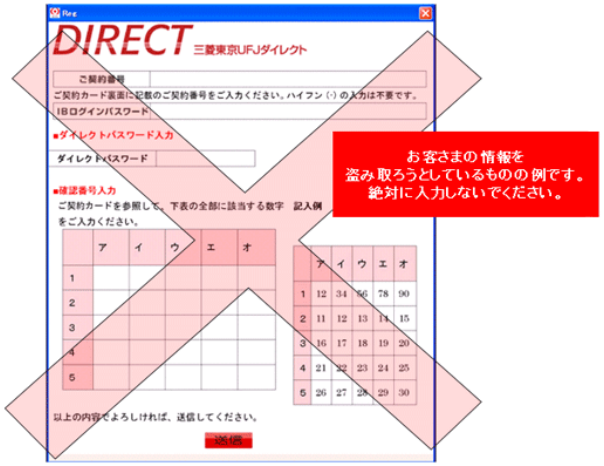
電子証明書ではあるが、顧客認証方式ではない

3. 情報セキュリティに関する具体的な留意点（続き）

（1）顧客が晒されるリスクへの対応（続き）

- 複数要素認証を導入していても、フィッシング被害が発生
- Webサイトや電子メールによる顧客への注意喚起、フィッシングサイトの監視、顧客あて電子メールへの電子署名の添付など、継続的な対応も必要





— 偽装メールの注意喚起一例（各金融機関のWebサイトから転載）

3. 情報セキュリティに関する具体的な留意点（続き）

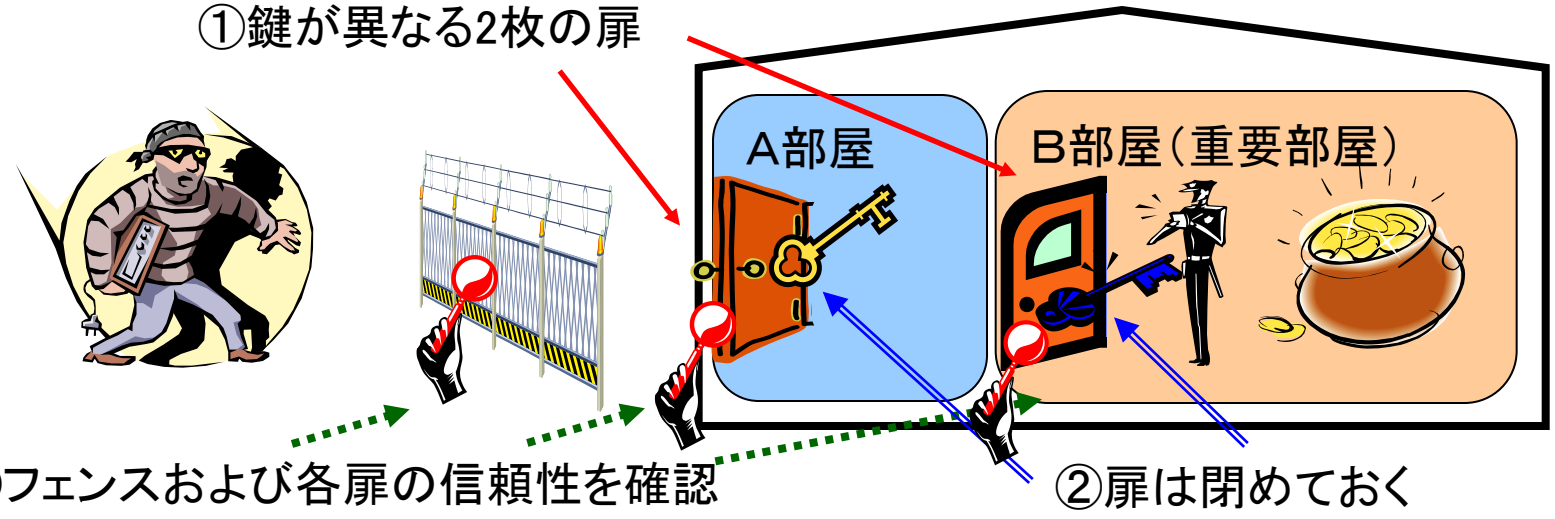
（2）業務妨害やウィルス感染への対応

＜安全な防犯基準とそれに見合う建物＞

① 扉は1枚目が破られたことを想定して2枚設置すること。その際には、鍵が異なるA扉とB扉にすること

② 扉は常時閉めておき、真の訪問者が来たときに開けること

③ ピッキング等に備えて、それぞれの鍵（扉）の信頼性確認を、警備会社に定期的に依頼すること



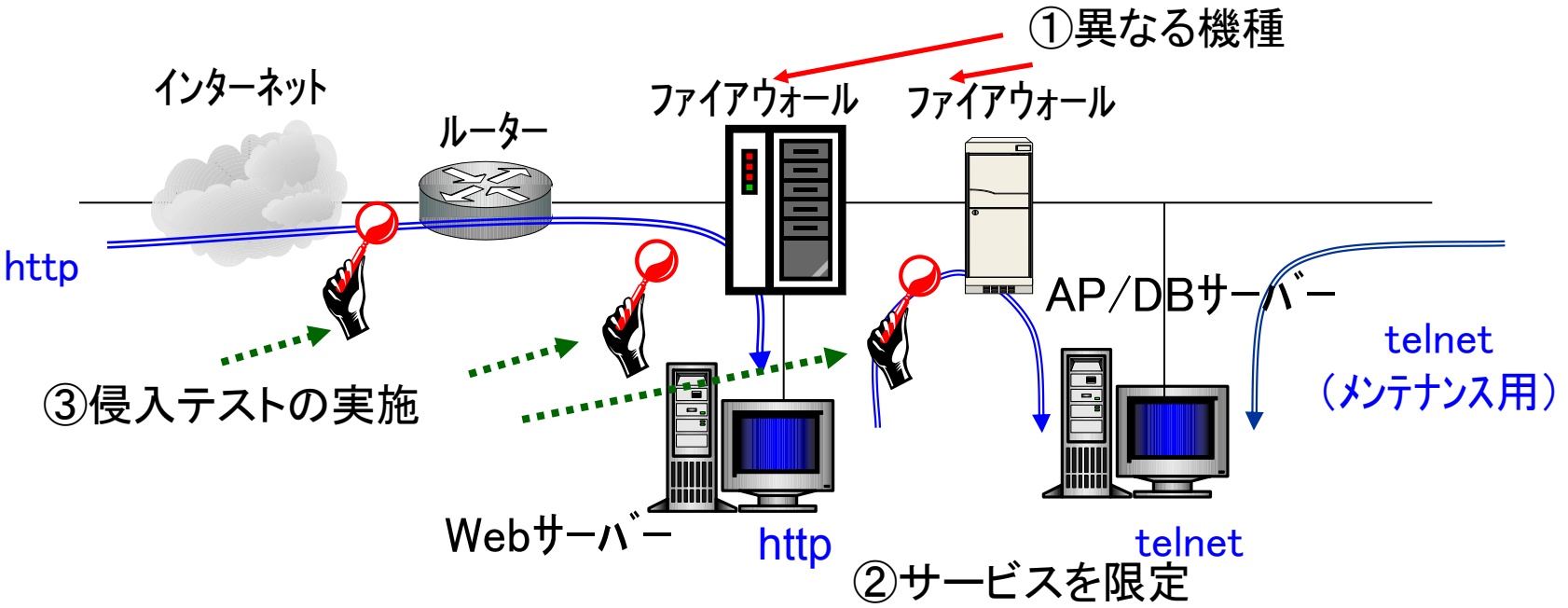
3. 情報セキュリティに関する具体的な留意点（続き）

＜セキュリティ・ポリシーに見合う正しい構成＞

① ファイアウォールは複数台設置すること。その際には、セキュリティ上の不具合に備えて、異なる機種とすること

② 利用可能なプロトコルおよびサービスを限定すること

③ ファイアウォールに対する侵入テストを定期的に実施すること



3. 情報セキュリティに関する具体的な留意点（続き）

＜犯罪者に狙われやすい建物＞

① 扉は1枚目が破られたことを想定して2枚設置。ただし同じ鍵の扉

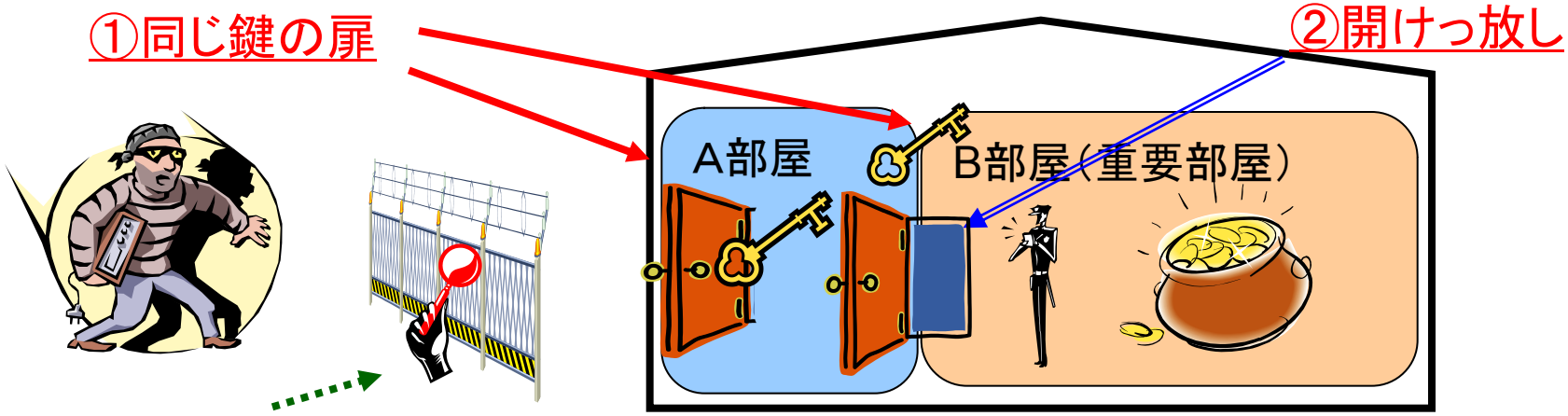
⇒ 同一メーカーから買う方が安価。修理依頼先が1先で済む。

② 内側の扉は開けっ放し

⇒ 警備員は通常B部屋にいるが、数時間おきにA部屋も巡回。A部屋の扉が閉まっていることを過信し、B部屋の扉を常時開放（B部屋の鍵を毎回開ける手間が省ける）。

③ 外にあるフェンスの信頼性のみ確認

⇒ 殆どの泥棒は、外側のフェンスを乗り越えられないため、ここさえ確認しておけば、全体が安全だと過信



3. 情報セキュリティに関する具体的な留意点（続き）

＜問題がある構成＞

① ファイアウォールが同一の機種

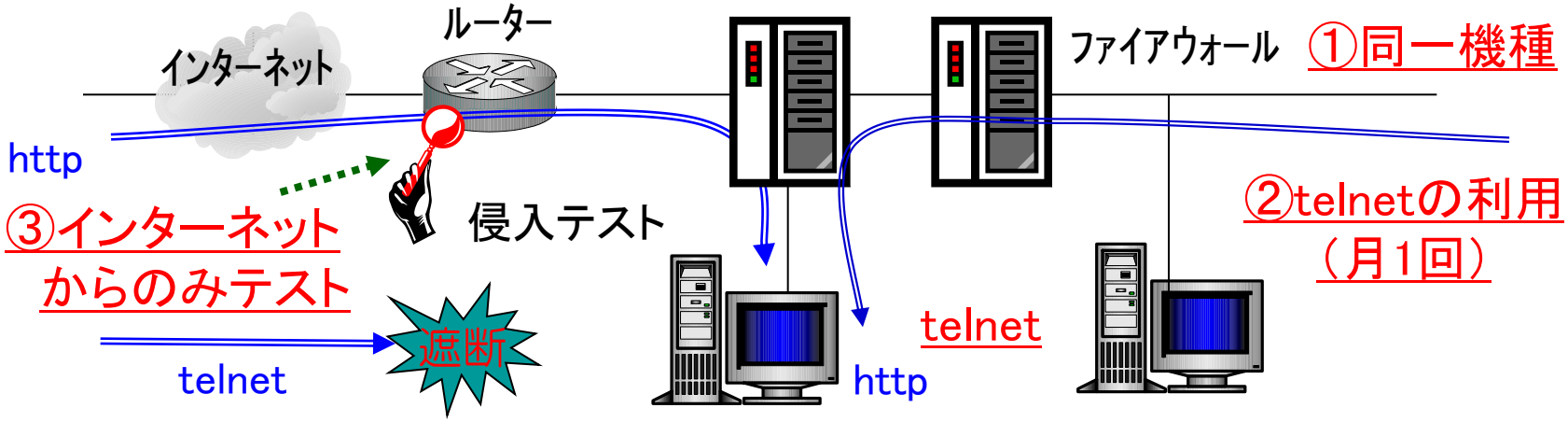
⇒ 構築当初は異なる機種。片方機種のリプレース時に、委託先が維持管理の容易性に重点を置き、同一機種に変更

② Webサーバーで不要なサービスを立上げ

⇒ 月1回のログ収集を内部から簡単に行うため（サーバー設置室に出向く手間が省ける）、常時telnetを立上げ（ログ収集を行う委託先のニーズ）

③ ファイアウォールに対する侵入テストは未実施

⇒ インターネット上からのみテストを実施。ルーターのフィルタリングで殆どのプロトコルが遮断される



3. 情報セキュリティに関する具体的な留意点（続き）

（2）業務妨害やウィルス感染への対応（続き）

① 大量データ送信による業務妨害（DDoS攻撃）への対策（例）

- ファイアウォールの設置
- DDoS対処用機器の設置
- ネットワークのリアルタイム監視
- 攻撃元からの通信遮断
- 定期的な侵害テスト

インターネットバンキング（個人・法人）、広報用ホームページそれぞれに対策が必要

② ウィルス感染への対策

- ウィルスパターンファイルの定期的な更新
  - 常に最新版に更新、数週間に1回更新
- 外部記憶媒体の利用制限
  - システム的に制限、規程で制限

職員用PCのほか、外部との媒体授受用端末（行内ネットワークに接続されていない給与振込システム用の端末等）、営業店端末、ATM、等についても対策が必要な場合もある

3. 情報セキュリティに関する具体的な留意点（続き）

（3）教育・訓練

① システム部門における情報セキュリティ確保への取り組み

・研修やセミナーへの参加等を通じたセキュリティ専門家の育成
・ 情報セキュリティに関する資格取得の奨励
・ITベンダー等との定期的な意見交換
・情報セキュリティ関係の有事対策等を専門とする組織の設置

② 業務部門、ユーザー部門における情報セキュリティ確保への取り組み

・情報セキュリティ担当部門によるメールマガジン等による情宣活動の実施
・役職員向け勉強会の開催
・セキュリティに関する理解度チェック（テスト）の実施

③ 情報セキュリティに関する訓練

・ウィルス感染を想定した訓練
・DDoS攻撃発生を想定した訓練
・情報漏洩発生を想定した訓練
・役職員宛標的型メールの送信を想定した訓練（疑似的な標的型メールを役職員宛てにテスト送信）

Ⅱ.システム障害に関する リスク管理の現状と課題

1. アンケートの概要
2. システム障害の発生状況
3. システム障害予防策の実施状況と課題
4. 調査結果等から見えてくる留意点：その1
5. 影響の大きいシステム障害の発生状況と要因
6. 調査結果等から見えてくる優位点：その2

1. アンケートの概要

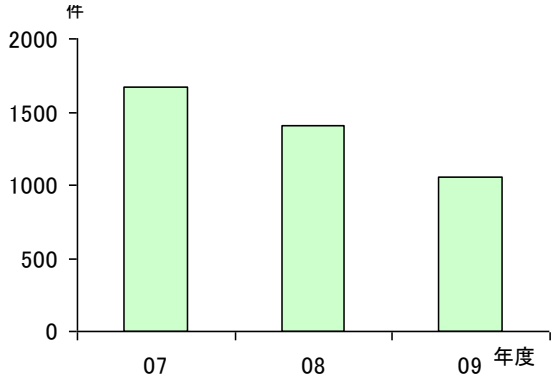
・調査時期：2010年4～6月
・調査手法：質問票によるアンケート調査
・対象金融機関：**173先**
　― 全地域銀行106行、信用金庫28金庫（システム運営業務を信金共同事務センターへ委託していない先）および都市銀行等39先
・対象システム：**勘定系システム**
　― インターネットバンキングシステム、ファームバンキングシステム、内国為替等外部接続システム、営業店システムを含む
・主な調査事項
　―― システム障害の発生状況（件数、発生要因）
　―― システム障害予防策の実施状況（発生要因別）
　―― システム障害予防策を推進するうえでの課題
　―― 影響の大きいシステム障害の発生状況（件数、発生要因）
　　・・・ 予防策が想定どおり機能しなかった要因

2. システム障害の発生状況

・ 調査対象期間（2007～2009年度）では、減少傾向。

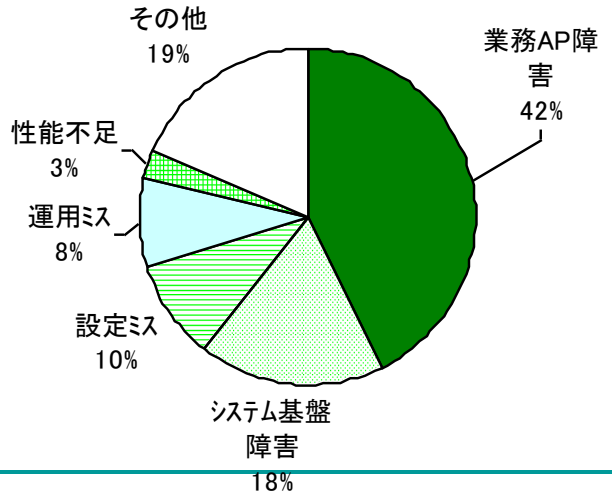
（注）「システム障害」：対顧客や決済等にかかるサービスに多少なりとも影響のあった障害

（図表1）システム障害の発生件数の推移



・ 発生要因別には、「業務アプリケーションプログラム障害（以下、「業務AP障害」）」が4割強を占め、それに「システム基盤障害 」、「設定ミス」、「運用ミス」が続く。

（図表2）システム障害発生要因別の割合（09年度）

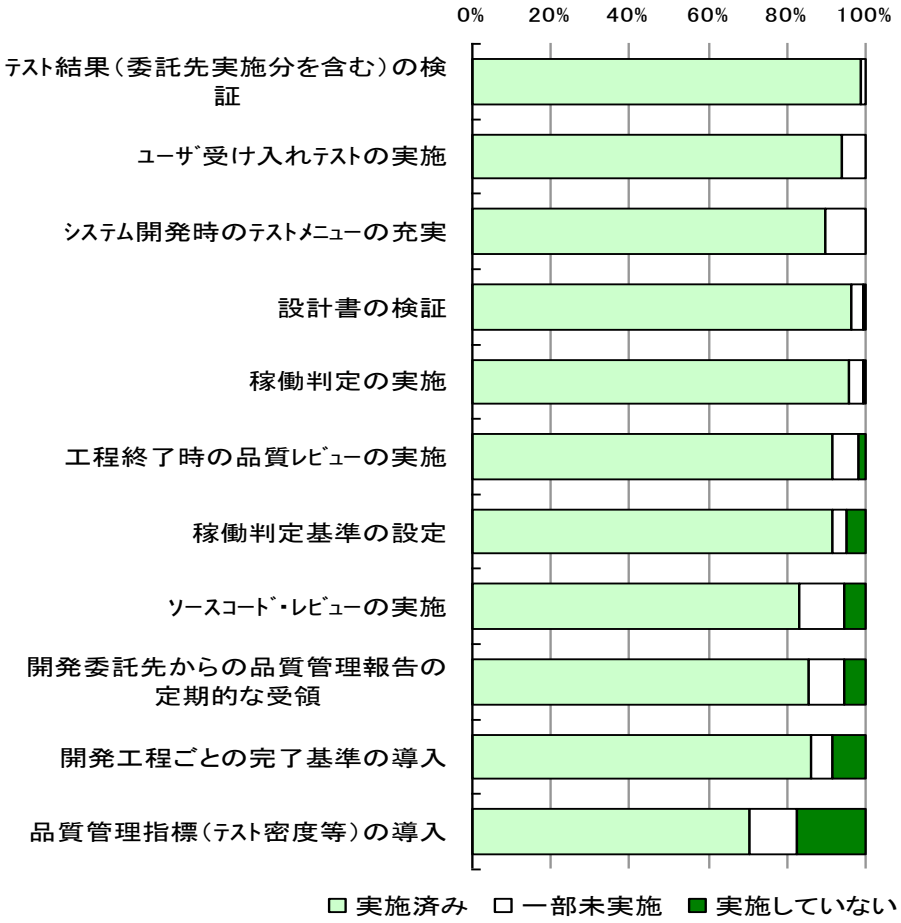


3. システム障害予防策の実施状況と課題

● **業務AP障害対策**

テスト結果や設計書の検証、稼働判定等を「実施済み」との回答が9割以上となったほか、品質管理指標の導入などを「実施済み」との回答も7～8割。

(図表3)業務AP障害にかかる予防策の実施状況

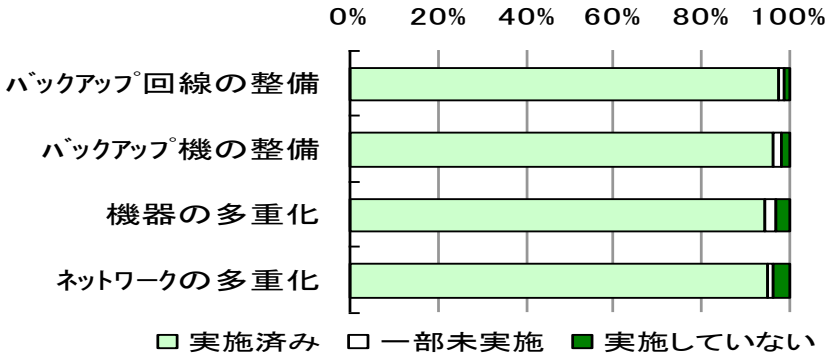


3. システム障害予防策の実施状況と課題（続き）

●**システム基盤障害対策**

バックアップ機の整備等、影響の大きいシステム障害を予防するためのインフラ整備は、「実施済み」との回答が9割超。

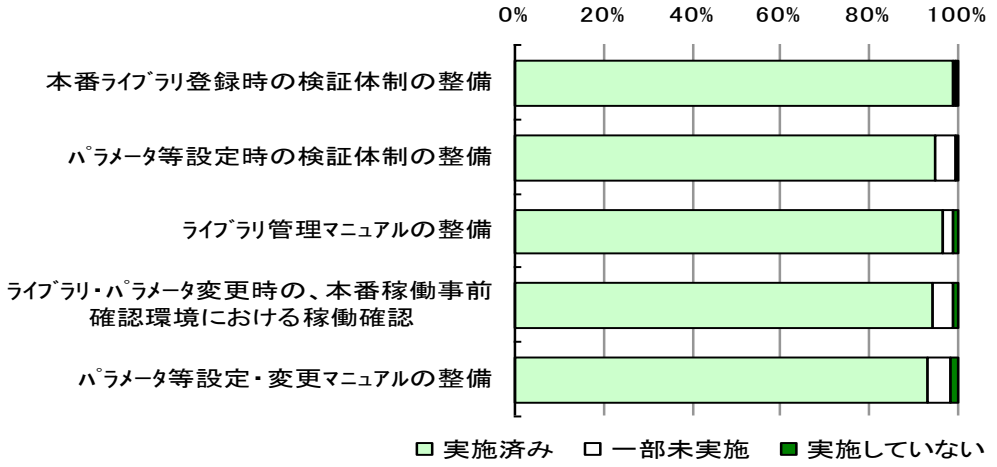
（図表4）システム基盤障害にかかる予防策の実施状況



●**設定ミス対策**

マニュアルや検証体制の整備、設定変更時の稼働前確認などは、「実施済み」との回答が9割超。

（図表5）設定ミス起因のシステム障害にかかる予防策の実施状況

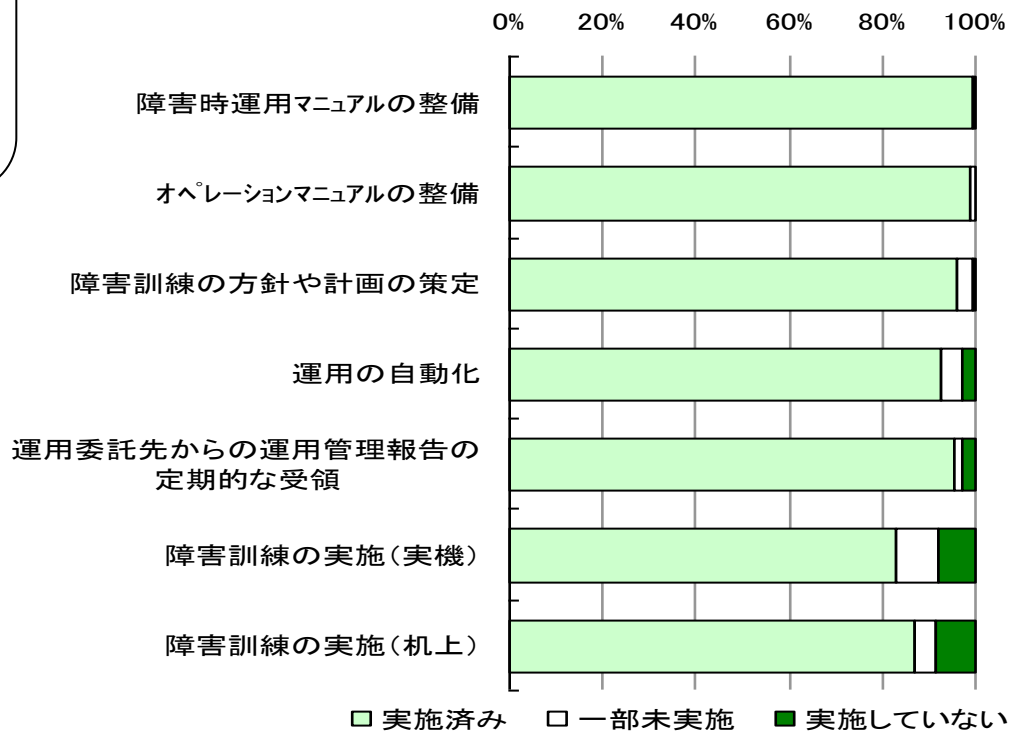


3. システム障害予防策の実施状況と課題（続き）

● **運用ミス対策**

マニュアル整備や障害訓練などは、「実施済み」との回答が約9割。

（図表6）運用ミス起因のシステム障害にかかる予防策の実施状況

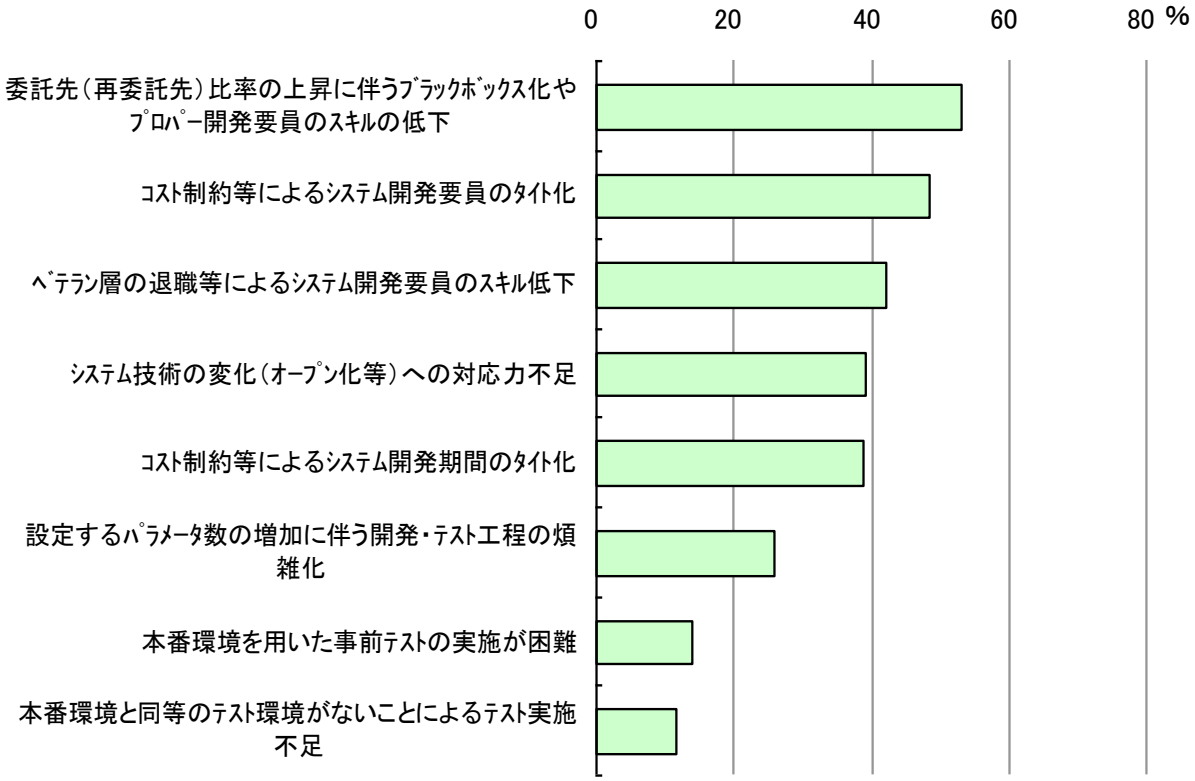


3. システム障害予防策の実施状況と課題（続き）

●システム開発面

システム開発要員のタイト化やスキルの低下を挙げる先が多い。

（図表7）システム開発にかかる課題（複数選択可）

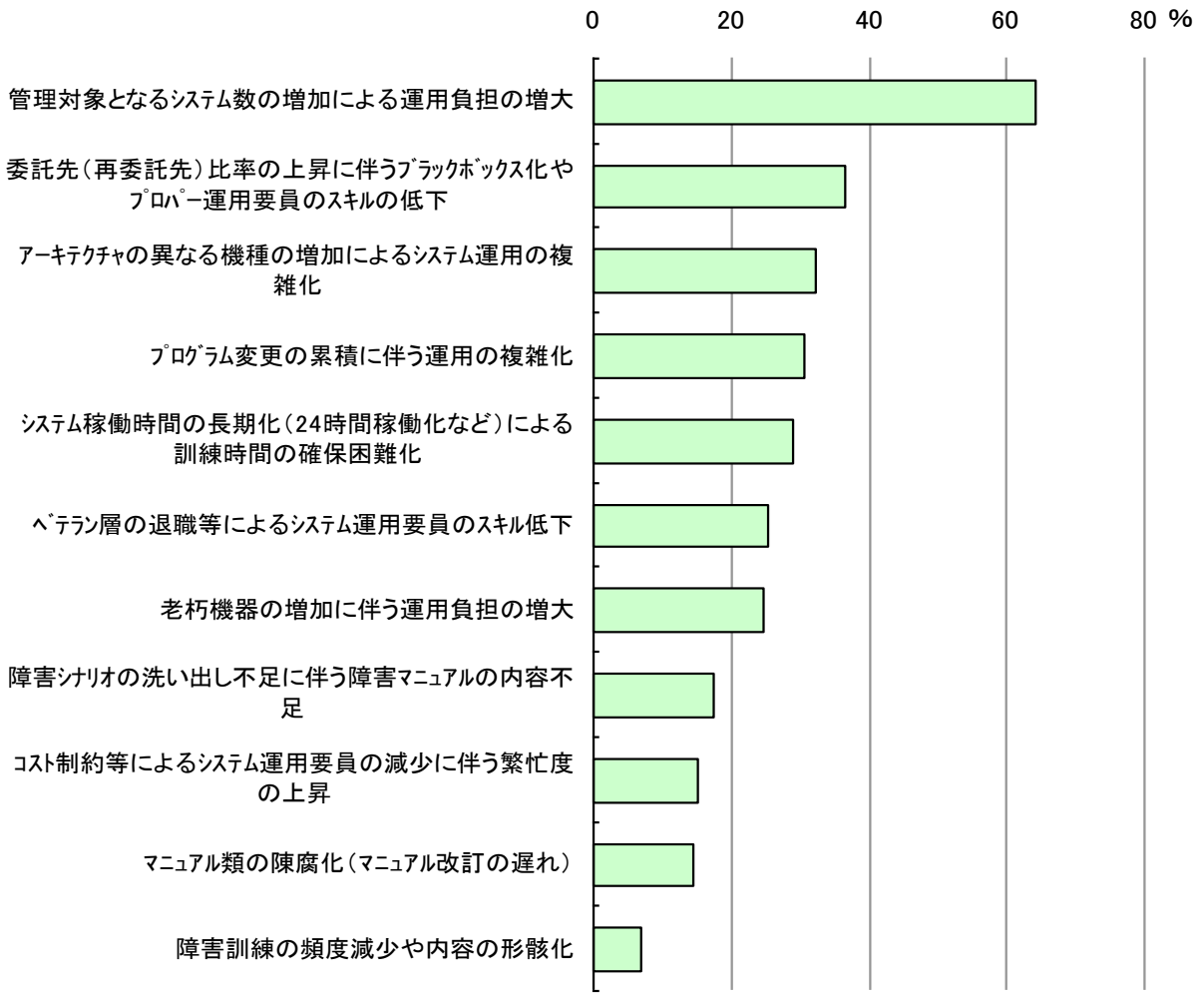


3. システム障害予防策の実施状況と課題（続き）

●**システム運用・維持管理面**

運用負担の増大や運用の複雑化、スキル低下を挙げる先が多い。

（図表8）システム運用・維持管理にかかる課題（複数選択可）



4. 調査結果等からみえてくる留意点：その1

・ システム障害の各種予防策については、「実施済み」と回答した先が多い。

・ 一方で、予防策を推進するためのシステム開発や運用･維持管理面において、

✓ 委託先比率の上昇やベテラン層の退職等によるスキルや要員数の確保の困難化

✓ 管理対象システム数の増加やシステムの技術基盤の変化等に伴う運用の複雑化といった環境変化への対応の難しさ

が課題として挙げられている。

4. 調査結果等からみえてくる留意点：その1（続き）

・システム開発や運用・維持管理業務面では、管理対象システム数の増加や複雑化等、質・量両面での変化に対し、予防策の見直しのほか、人的リソースの確保・スキルの育成など、適切に対応することが重要。

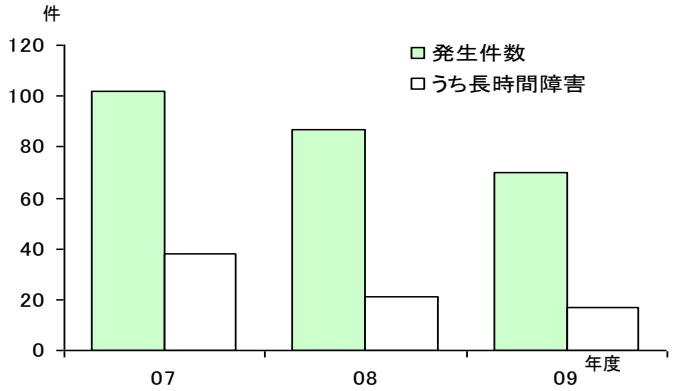
→ 例えば、システム分野の新卒採用を増やす先や、スキル向上を目的にプロパー職員をITベンダーへ出向させる先もみられる。

5. 影響の大きいシステム障害の発生状況と要因

・ 調査対象期間（2007～2009年度）では、影響の大きいシステム障害、また同障害のうち長時間障害の発生件数は減少。

（注）「影響の大きいシステム障害」：対顧客や決済等にかかるサービスの1つまたは複数が全面的に停止するに至ったシステム障害
「長時間障害」：影響の大きいシステム障害のうち、復旧までに長時間（3時間以上）を要したシステム障害

（図表9）影響の大きいシステム障害の発生件数の推移



・ もっとも、影響の大きいシステム障害のうちバックアップ機等システム構成面の予防策が機能しなかった事例が存在。

（図表10）1つまたは複数の対外提供サービスの全面停止に至った件数と原因

		合計				
			ﾊﾞｯｸｱｯﾌﾟ切替遅延・不能	縮退運転切替遅延・不能	多重化していない	その他
2007 年度	上期	49	7	4	8	30
	下期	53	6	1	3	43
2008 年度	上期	41	12	2	4	23
	下期	46	10	5	3	28
2009 年度	上期	33	13	5	4	11
	下期	37	5	5	2	25

5. 影響の大きいシステム障害の発生状況と要因（続き）

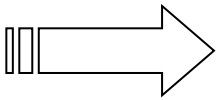
システム構成面での予防策

システムが稼働する機器を必要に応じ多重化

具体的には、

①メイン機器のほかにバックアップ機器を設ける、

②1つのシステムを複数の機器で並行稼働させ、1つの機器が稼働を停止しても残りの機器のみでシステムを稼働させる構成とする



こうした予防策にもかかわらず、影響の大きいシステム障害の発生要因をみると、

①バックアップ機や、②並行稼働のもとでの縮退運転 、への切替が遅延あるいは切替そのものができなかった、

など、想定どおりに予防策が機能しなかった事例もみられる 。

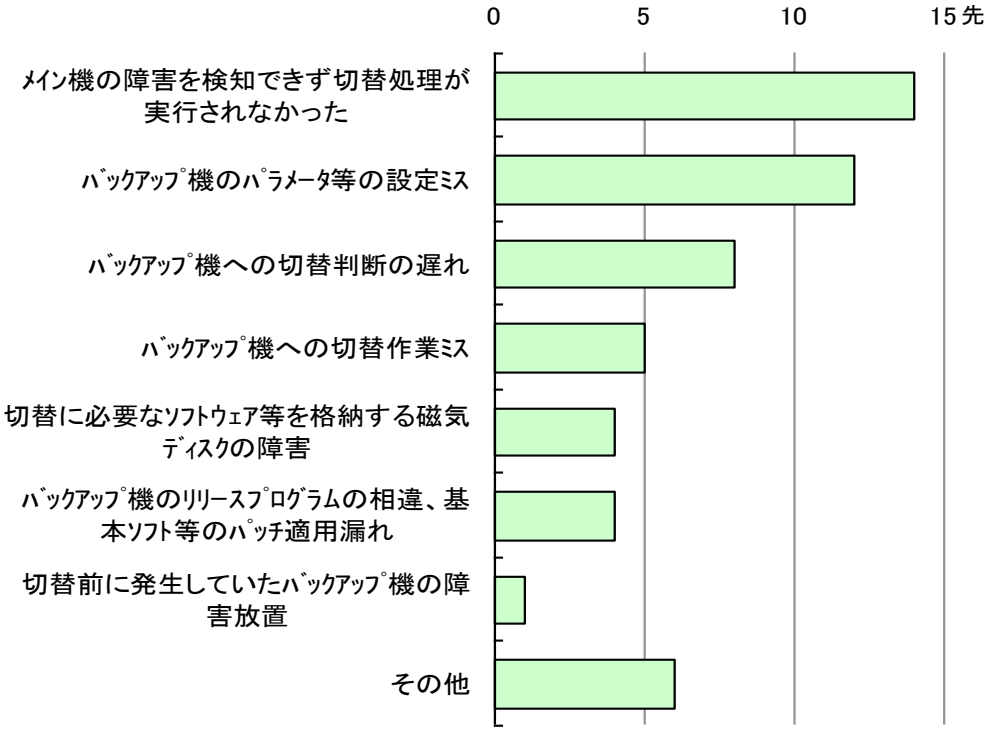
5. 影響の大きいシステム障害の発生状況と要因（続き）

●「メイン機の障害の検知漏れ」を挙げる先が多いほか、

「バックアップ機への切替にかかるパラメータ等の設定ミス」、
「切替判断の遅れ」、
「切替作業ミス」

等の人為的ミスを挙げる先がみられる。

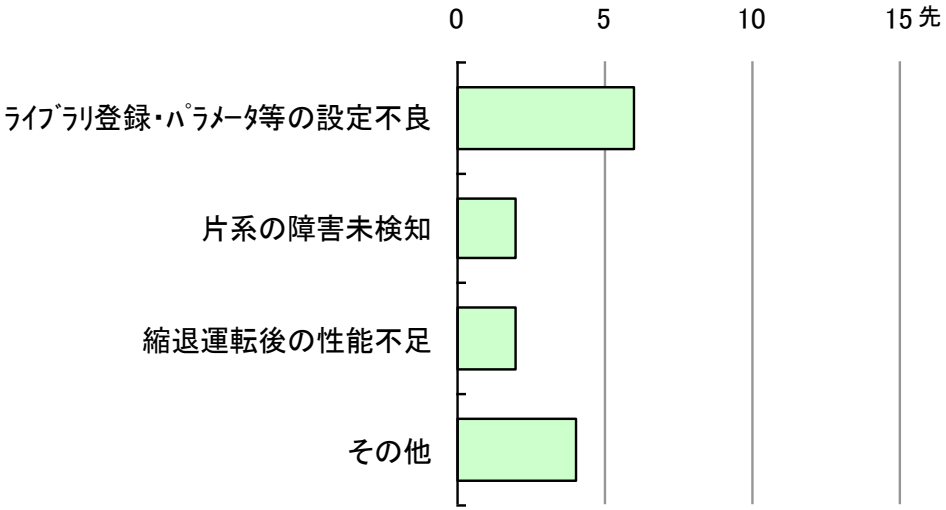
（図表11）バックアップ機への切替遅延・不能が発生した要因（対象34先の複数回答）



5. 影響の大きいシステム障害の発生状況と要因（続き）

●縮退運転への切替が遅延または行えなかった要因としては、「パラメータ等の設定ミス」を挙げる先が多い。

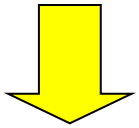
（図表12）縮退運転への切替遅延・不能が発生した要因
（対象12先の複数回答）



6. 調査結果等からみえてくる留意点：その2

・ 影響の大きいシステム障害のなかには、バックアップ機器の整備等、予防策が講じられていたにもかかわらず、それが想定どおり機能しなかった事例もみられる。

⇒ その原因として、「メイン機の障害が検知できなかった」ことや、「バックアップ機への切替にかかるパラメータ等の設定ミス 」、「同切替にかかる運用ミス 」といった人為的ミスを挙げた先が少なくない。



・ 影響の大きいシステム障害を回避するために、システム機器の多重化などの予防策が想定どおりに機能するよう、機器の稼働状況にかかる監視内容の工夫や設定ミス防止のための検証体制の見直し、運用ミス防止のための計画的な障害対応訓練を行うことが重要。

６．調査結果等からみえてくる留意点：その２（続き）

●具体策としては、例えば、

✓　システム運用部門の監視体制の整備、システムによる監視の範囲や内容の見直し

✓バックアップ機にかかる設定作業に関し、現状の検証体制がメイン機と同様に十分か否かの見極め、必要に応じた見直し

✓　万一バックアップ機への切替が必要となった場合にも適切な対処ができるよう、様々なケースごとに具体的な手順を整備、バックアップ機への切替訓練等を計画的に実施

✓磁気ディスク装置障害発生時にも切替ソフトウェアへ影響が及ばないよう、同じシステム系列に切替ソフトウェアを配置しないなど、同ソフトウェアの設置場所について配意

Ⅲ.システム障害管理体制の実効性向上に向けた留意点

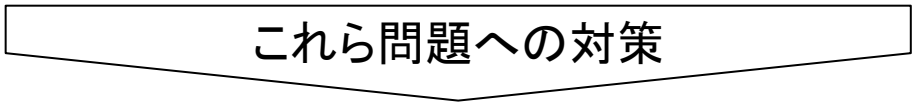
1. 最近の大規模障害を踏まえた留意点
2. システム障害管理体制の実効性向上に向けた留意点
3. 障害発生の未然防止策における留意点
4. 障害発生時の対応における留意点
5. 障害管理に対する経営陣の関与
6. 障害管理体制面の問題点と対応策
7. 想定される障害事例と対応策

1. 最近の大規模障害等を踏まえた留意点

・ これまでの対応

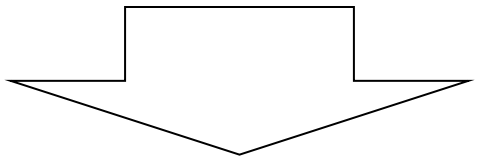
【システム障害の典型的な事例】

・システム開発の途上で生じた問題が、システム稼働後に顕在化



【システム開発中の対応】

①プロジェクト管理体制の整備、②プログラムの品質確保、③適切な稼働判定



長年のシステム開発のなか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先が多い

1. 最近の大規模障害等を踏まえた留意点（続き）

・ 最近の大規模障害等を踏まえ、留意すべき事項

【システム安定稼働後】

・ 時間の経過ともに、当該システムに対するリスク認識が低下しがちになる

・ 他方で、顧客サービスの向上のためのシステム対応や顧客行動の変化等に伴い、潜在的なリスクが蓄積しうる

・ 特に長期間安定稼働を続けているシステムは、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、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易い

これら問題への対策

顧客等への影響が大きい社会的に重要なシステム（勘定系システム等）については、長期安定稼働を続けていても、経営陣の指示のもと、障害の未然防止策の策定や障害発生時の対応体制を整備する必要

2. システム障害管理体制の実効性向上に向けた留意点

・ 日本銀行公表資料「システム障害管理体制の実効性向上に向けた留意点」（2007年2月）資料の概要

1. はじめに

2. 障害発生の未然防止策における留意点
（1）稼働中のシステムへの対応
（2）開発中のシステムへの対応

3. 障害発生時の対応における留意点
（1）障害対応体制
（2）障害対応計画（コンティンジェンシープラン）
（3）システム障害に備えた訓練

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認識
（2）障害発生の防止に向けた指示

5. おわりに

別添1：障害管理体制面の問題点と対応策・・・60項目
・個々の障害事例の背後にある管理体制面の具体的な問題点と対応策を紹介

別添2：想定される障害事例と対応策・・・54項目
・過去発生した個々の障害事例と対応策を紹介

2. システム障害管理体制の実効性向上に向けた留意点（続き）

・ 日本銀行公表資料「システム障害管理体制の実効性向上に向けた留意点」（2007年2月）資料の概要

別添1：個々の障害事例の背後にある管理体制面の具体的な問題点と対応策を紹介

Ⅰ．障害発生の未然防止対策		
1．システム稼働中の対応		
	（1）システムリスク評価	6項目
	（2）システム処理性能・設定値	2項目
	（3）委託先管理	3項目
	（4）障害抑制の具体策	
	①障害事例分析・防止策	3項目
	②操作ミスの防止策	2項目
	③障害件数目標値の設定	2項目
2．システム開発中の対応		
	（1）プロジェクト管理	2項目
	（2）システム設計・プログラム品質	5項目
	（3）システム稼働判定	4項目

Ⅱ．障害発生時の対応		
1．障害対応体制		
	（1）報告体制	4項目
	（2）初動対応	1項目
	（3）顧客・広報対応	3項目
2．障害対応計画		7項目
3．システム障害に備えた訓練		4項目

Ⅲ．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	8項目
2．障害発生の防止に向けた指示	4項目

合計	60項目

2. システム障害管理体制の実効性向上に向けた留意点（続き）

・ 日本銀行公表資料「システム障害管理体制の実効性向上に向けた留意点」（2007年2月）資料の概要

別添2：過去発生した個々の障害事例と対応策を紹介

―― 07年3月に公表した「事例からみたコンピューター・システムリスク管理の具体策」の別添を増補改訂したもの。

1．ハードウェア障害	3項目
2．ソフトウェア障害	
（1）制御プログラム	5項目
（2）業務処理プログラム	9項目
3．性能	
（1）処理能力	6項目
（2）設定値	9項目

4．運用	
（1）機器監視	1項目
（2）運用手順	8項目
（3）プログラムリリース	8項目
5．障害対応	5項目
合計	54項目

3. 障害発生の未然防止策における留意点

（1）稼働中のシステムへの対策

・ 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

▽ 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

3. 障害発生の未然防止策における留意点（続き）

（1）稼働中のシステムへの対策

・ 環境変化に対する有効な対策の一例

▽ 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
システム処理性能・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

3. 障害発生の未然防止策における留意点（続き）

（2）開発中のシステムへの対策（例）

①プロジェクト管理体制の整備

・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、認識に齟齬が生じないようにする

②プログラムの品質確保

・要件定義やシステム設計、テスト結果と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

③適切な稼働判定

・業務部署やリスク管理部署等の評価も踏まえて、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を行う

4. 障害発生時の対応における留意点

（1）障害対応体制（例）

・初動対応：　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

・連携体制：　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しない体制とする

自社と委託先の責任分担に曖昧な点をなくす

当日中に処理すべきデータの決済件数・金額等を速やかに外部接続先や当局に連絡できる体制を構築する

・顧客対応：　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なるため、予め、関係部署の責任分担を明確化したうえで、必要な情報共有を行う体制を構築する

4. 障害発生時の対応における留意点（続き）

（2）障害対応計画（コンティンジェンシープラン）（例）

・記載内容：　システム変更や組織変更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

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にくい内容となっていないことを、組織的に検証する

システム面・業務面の対応計画の整合性を確保する

（3）システム障害に備えた訓練（例）

・訓練計画：　訓練シナリオは、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・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用意する

障害発生時の連絡体制の実効性や妥当性を検証するために、対策本部の設置訓練や拠点駆付け訓練、広報対応訓練も活用する

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検証する

5. 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認識（例）

- 稼働中のシステムに関しても、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る
- システム部署や業務部署、リスク管理部署などに、潜在リスクの所在や特徴について、報告を求める
- 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

（2）障害発生の防止に向けた指示（例）

- 障害の未然防止策を充実させるために、自社分だけではなく他社分も含めて障害事例分析を行うよう指示を出す
- システム部署と業務部署が、システム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、体制を確保する
- 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

6. 障害管理体制面の問題点と対応策

障害発生の未然防止対応

（1）稼働中のシステムへの対応

①システムリスク評価

障害管理体制面の問題	想定される障害	対応策
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。
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。

6. 障害管理体制面の問題点と対応策（続き）

障害発生の未然防止対応

（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

障害管理体制面の問題	想定される障害	対応策
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。

6. 障害管理体制面の問題点と対応策（続き）

障害発生の未然防止対応

（1）稼働中のシステムへの対応

③委託先管理

障害管理体制面の問題	想定される障害	対応策
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。

6. 障害管理体制面の問題点と対応策（続き）

障害発生の未然防止対応

（1）稼働中のシステムへの対応

④障害抑制の具体策

障害管理体制面の問題	想定される障害	対応策
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。
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。

6. 障害管理体制面の問題点と対応策（続き）

障害発生時の対応

（1）障害対応体制

①報告体制

障害管理体制面の問題	想定される障害	対応策
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。

②初動対応

障害管理体制面の問題	想定される障害	対応策
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。

6. 障害管理体制面の問題点と対応策（続き）

障害発生時の対応

（1）障害対応体制

③顧客・広報対応

障害管理体制面の問題	想定される障害	対応策
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。

6. 障害管理体制面の問題点と対応策（続き）

障害発生時の対応

（2）障害対応計画（コンティンジェンシープラン）

障害管理体制面の問題	想定される障害	対応策
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。

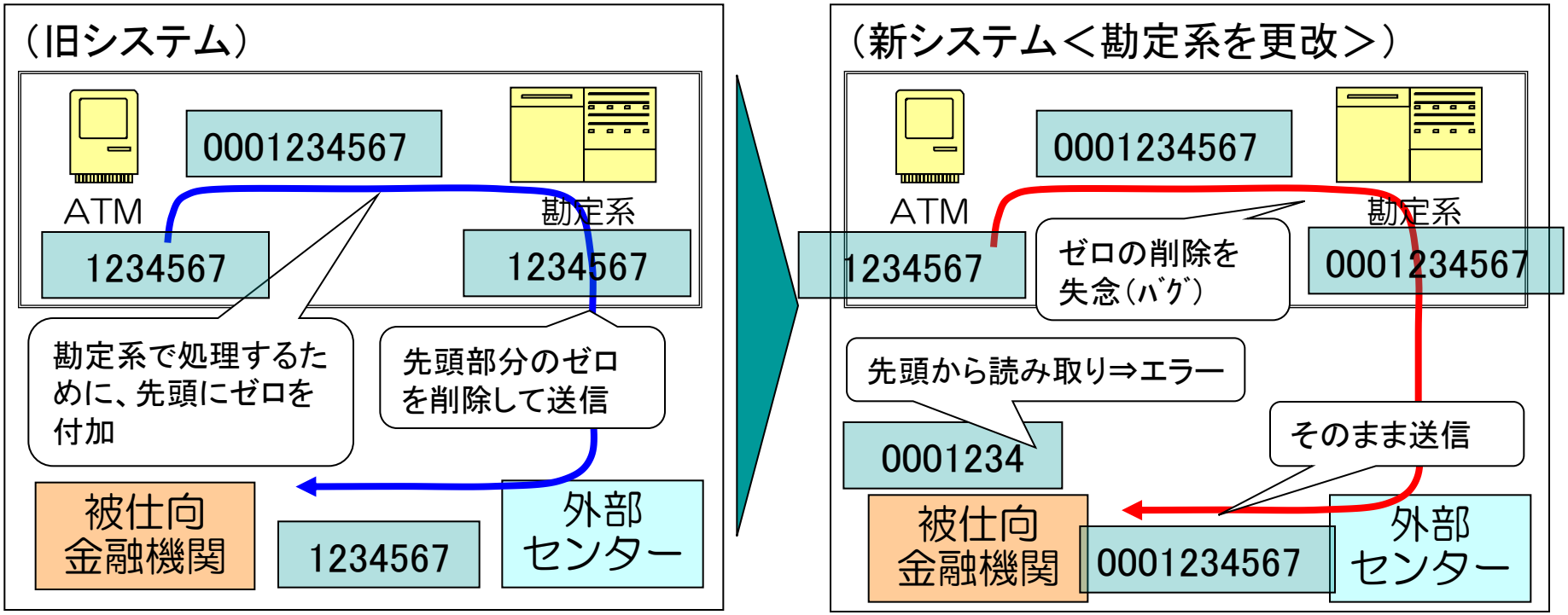
（3）障害に備えた訓練

障害管理体制面の問題	想定される障害	対応策
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。

7. 想定される障害事例と対応策

（1）ソフトウェアに関する問題

日本銀行 金融高度化セミナー「システムリスク管理の現状と課題」（2007年3月23日）資料より抜粋



問題点：新システムへの移行にあたり、被仕向金融機関を含めたテストを実施していない。

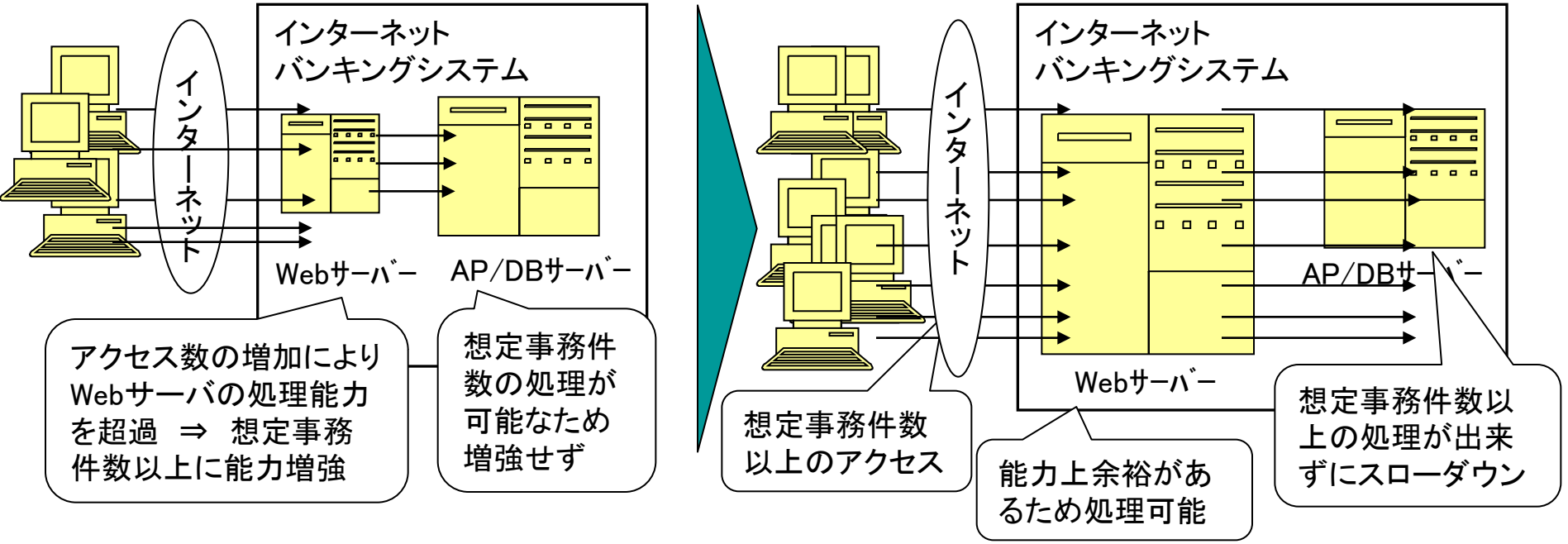
対応策：対外接続業務においては、主要な外部接続先との間でテストを行うこと。

システム間のデータ連動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

7. 想定される障害事例と対応策（続き）

（2）処理能力に関する問題

日本銀行 金融高度化セミナー「システムリスク管理の現状と課題」（2007年3月23日）資料より抜粋



問題点：「想定事務量」でのテストは行ったものの、「最大事務量」でのテストは未実施。

想定事務量を超過して取引が発生した場合に、アクセスを制御する仕組みがない。

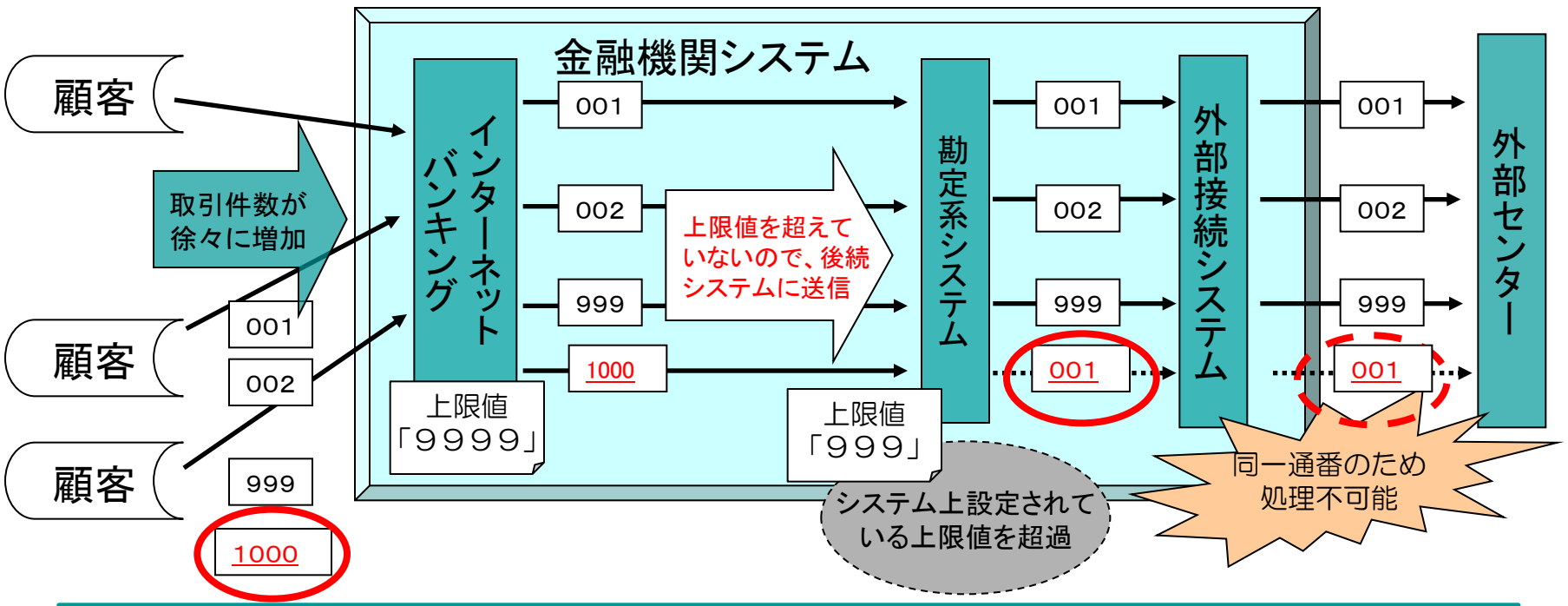
対応策：システムの一部の能力増強を行う際には、システム全体の性能評価を行うこと。

性能負荷テストは「想定事務量」に加え、「最大事務量」でも行うこと。

7. 想定される障害事例と対応策（続き）

（3）設定値に関する問題

日本銀行 金融高度化セミナー「システムリスク管理の現状と課題」（2007年3月23日）資料より抜粋



問題点：入力処理を業務プログラムの担当部署と、出力処理の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。

対応策：上限値の確認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。

上限値の管理は、OS、DBMS等に設定しているものに加え、APに設定されているデータの入出力可能件数、ワーク領域等を含めること。

ご清聴ありがとうございました

本資料に関する照会先

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、志村、熊坂

tel: 03-3664-4333

email: csrbcm@boj.or.jp