金融高度化セミナー資料

2011年1月28日

システム障害管理とバックアップセンターの実効性確保

日本銀行　金融機構局

日本銀行
BANK OF JAPAN

本日の説明内容①

- 日本銀行金融機構局の公表ペーパー

・「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）
・「バックアップ・コンピュータセンターの実効性確保にかかる課題と対応策」（2010年3月）

を基に、システム障害管理、バックアップセンターの実効性確保に関する留意点を説明。

Ⅰ．システム障害管理の現状と課題

― システム障害に関するアンケート調査と、調査結果等からみえてくる留意点等

Ⅱ．金融機関のバックアップ・コンピュータセンターの実効性確保にかかる課題と対応策

― 具体的事例に基づく、システム面を中心としたバックアップセンター運用上の課題と対応策

本日の説明内容②

（参考）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 ・システムの拡張性・柔軟性の低下

Ⅰ.システム障害管理の現状と課題

1. システム障害管理について

── 日本銀行公表ペーパー「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）より

① システム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可能

システム障害	リスク管理策
ハードウェアに起因した障害	機器の二重化、定期保守、切替え訓練の実施等
ソフトウェアに起因した障害	レビュー、テストの充実等
システム性能に起因した障害	性能・負荷テストの実施、定期的な監視
運用・保守に起因した障害	運用・障害マニュアル、プログラム登録手順書等の整備、運用訓練の実施

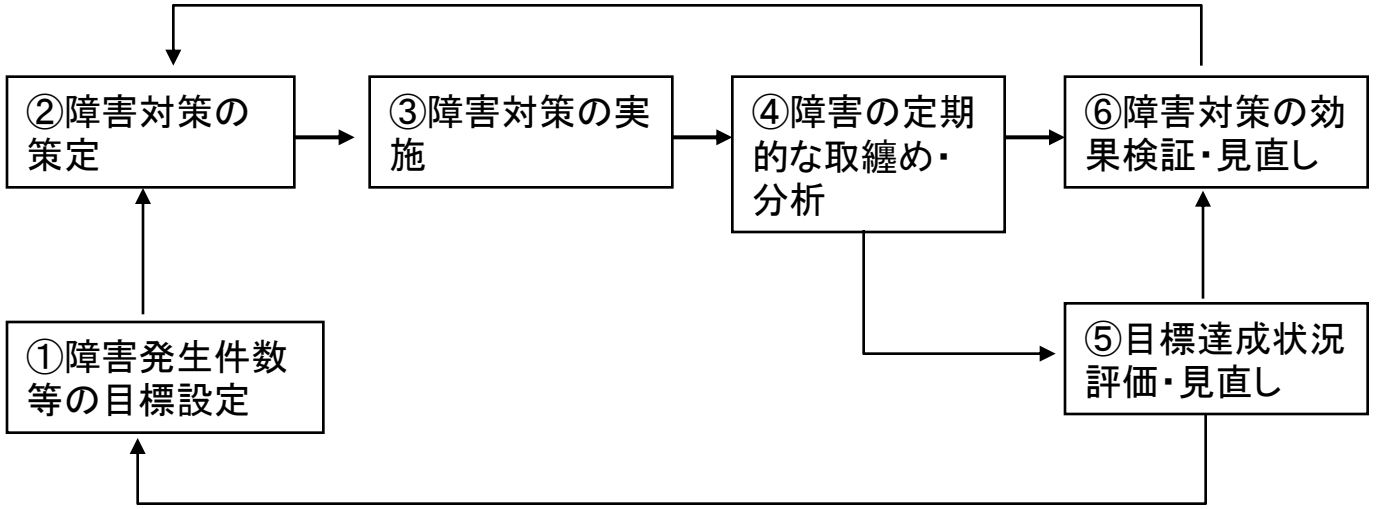
1. システム障害管理について

―― 日本銀行公表ペーパー「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）より

②システム障害管理のためのPDCA

―― 障害を抑制するためには、まず障害発生件数の上限等の目標を設定し、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。

―― 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。



1. システム障害管理について

―― 日本銀行公表ペーパー「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）より

③ システム障害事例の分析にあたっては、自社事例のみならず、他社事例を参考とすることも有益

―― 日本銀行公表ペーパー「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）では、考査等の場でみられた要改善事例やシステム障害事例等を基に、想定される障害事例と対応策を記載しているので参考にして頂きたい。

―― 公開情報の活用（各種報道・公表情報等）

2. システム障害に関するアンケート調査
（1）概　要①

- 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。

2. システム障害に関するアンケート調査
（1）概　要②

- 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

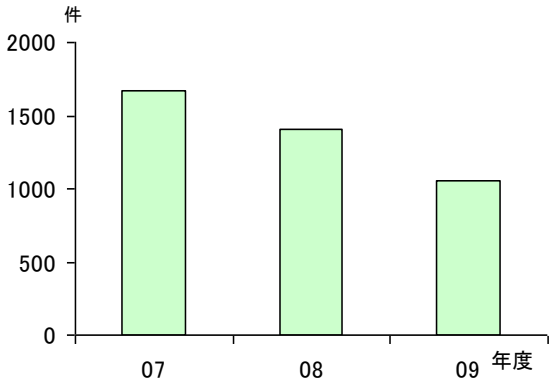
  ―― 影響の大きいシステム障害の発生状況（件数、発生要因）
  　　・・・　予防策が想定どおり機能しなかった要因

2. システム障害に関するアンケート調査
（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。

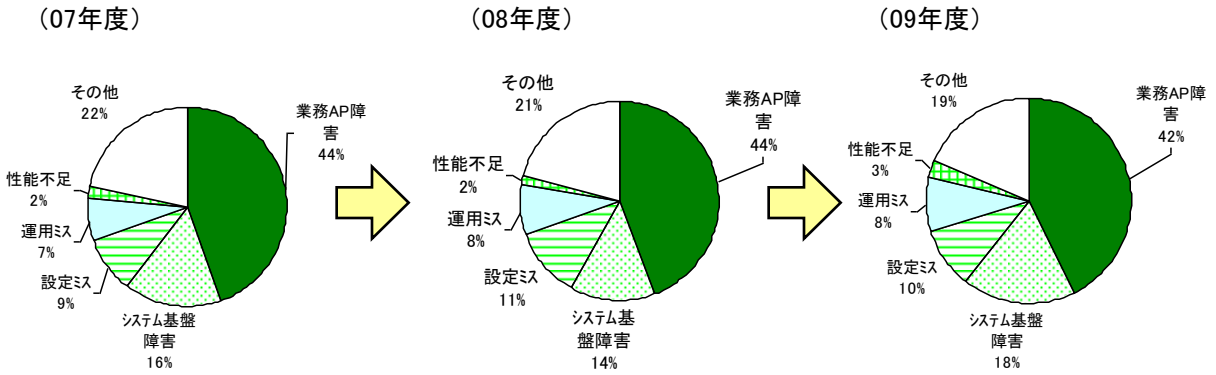
（注）「システム障害」：対顧客や決済等にかかるサービスに多少なりとも影響のあった障害

（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とその変化

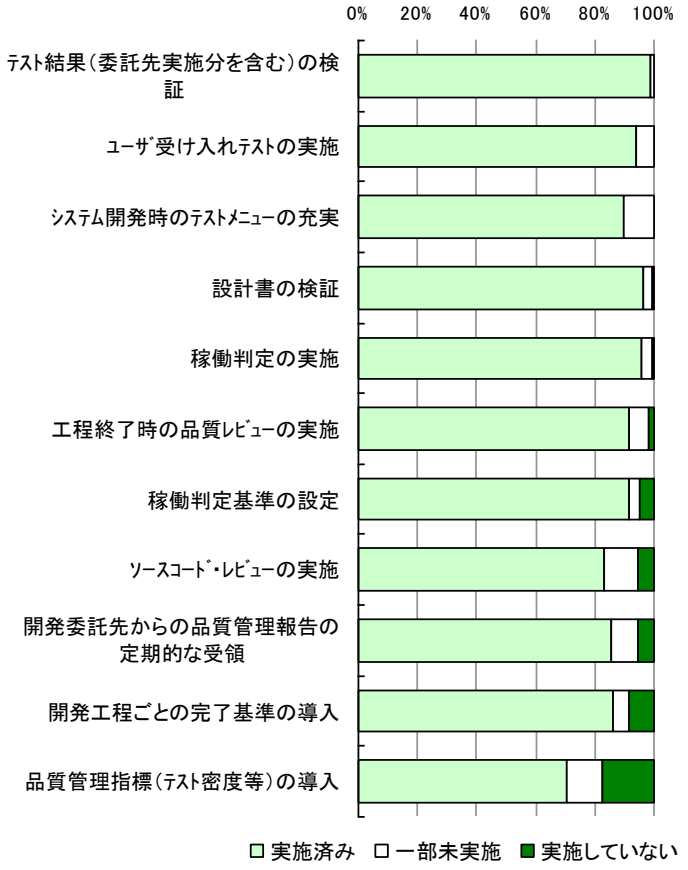


2. システム障害に関するアンケート調査
（3）システム障害予防策の実施状況①

● **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

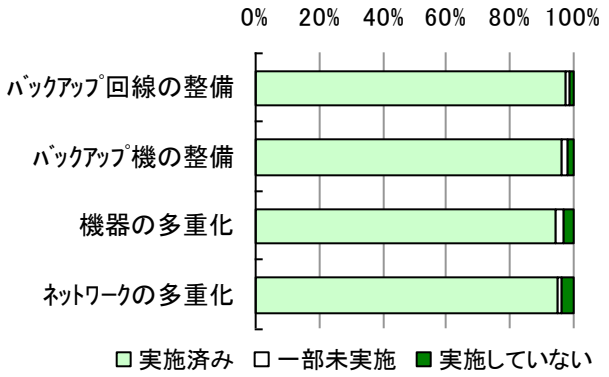


2. システム障害に関するアンケート調査
(3)システム障害予防策の実施状況②

●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。

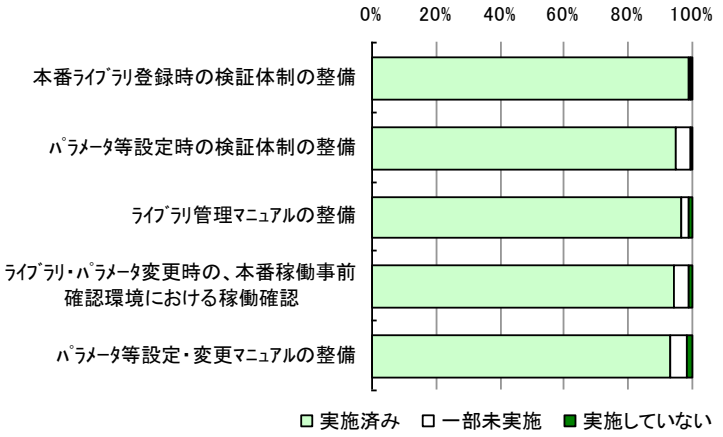
(図表4)システム基盤障害にかかる予防策の実施状況



●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

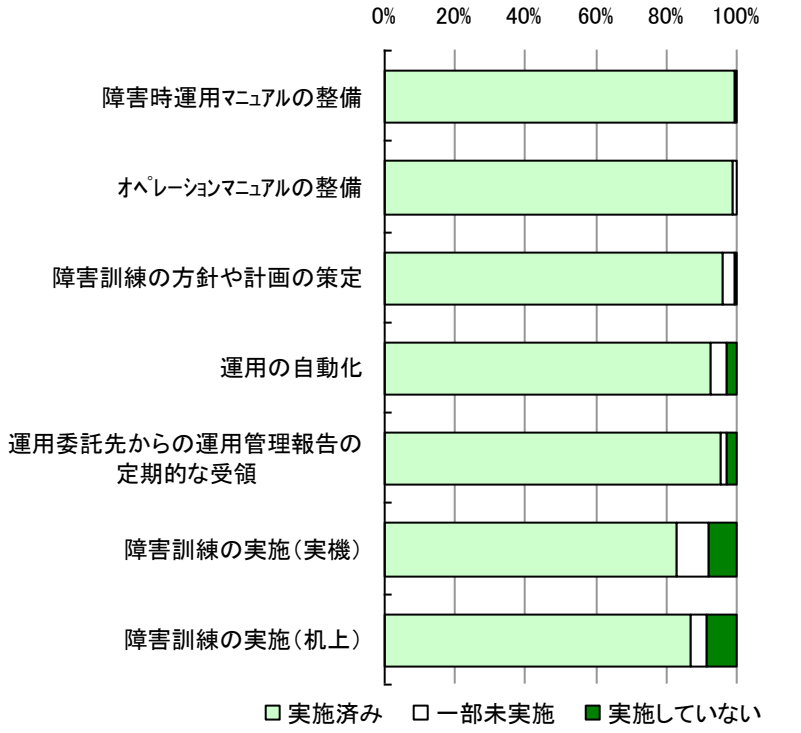


2. システム障害に関するアンケート調査
（3）システム障害予防策の実施状況③

● **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

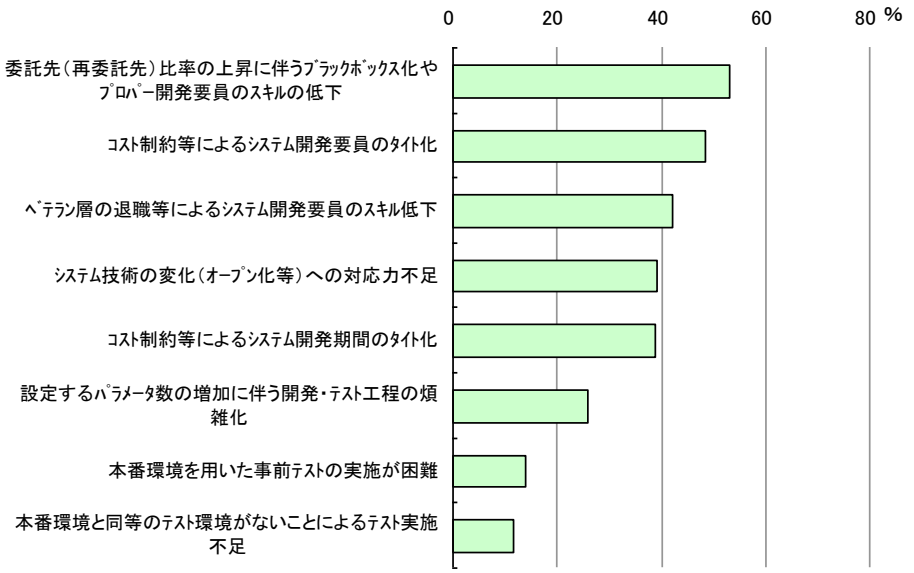


2. システム障害に関するアンケート調査
（4）予防策を推進するうえでの課題①

●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）

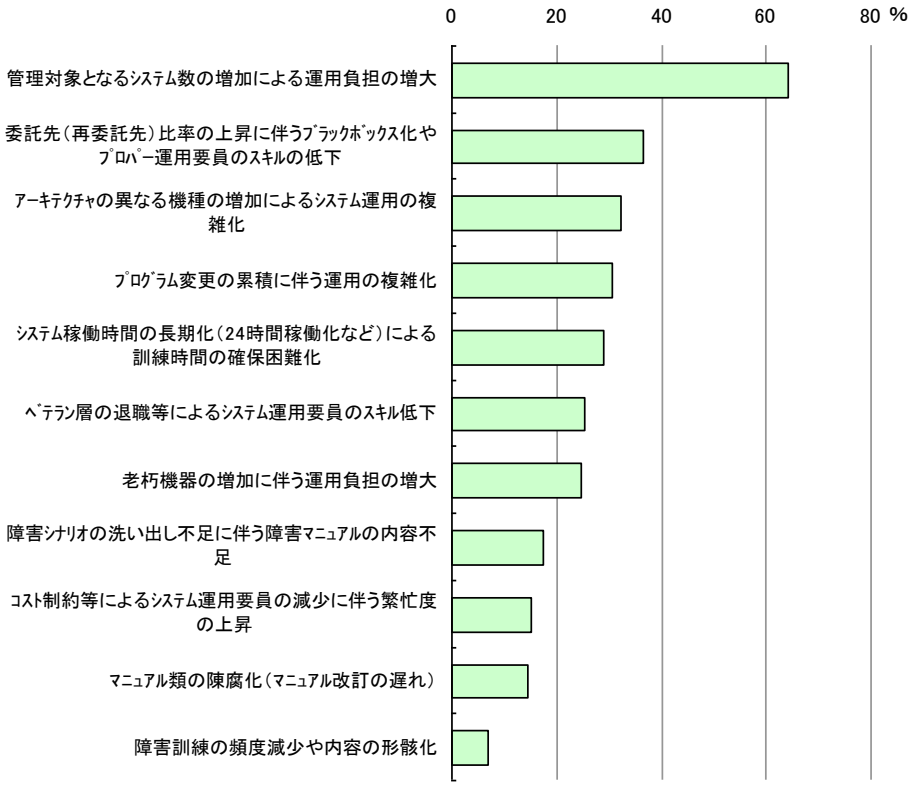


2. システム障害に関するアンケート調査
（4）予防策を推進するうえでの課題②

●システム運用・維持管理面

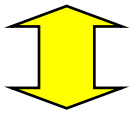
運用負担の増大や運用の複雑化、スキル低下を挙げる先が多い。

（図表8）システム運用・維持管理にかかる課題（複数選択可）



2. システム障害に関するアンケート調査
（5）調査結果等からみえてくる留意点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。

2. システム障害に関するアンケート調査
（5）調査結果等からみえてくる留意点②

- 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。

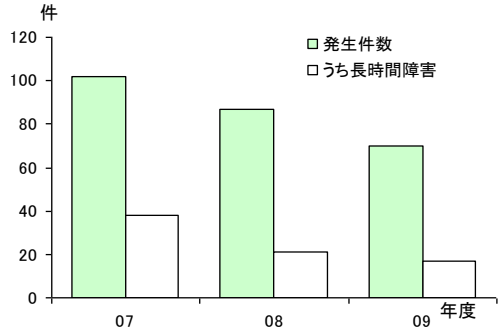
2. システム障害に関するアンケート調査
（6）影響の大きいシステム障害の発生状況

・ 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

・ 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9）影響の大きいシステム障害の発生件数の推移



（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

2. システム障害に関するアンケート調査
(7)予防策が想定どおり機能しなかった要因①

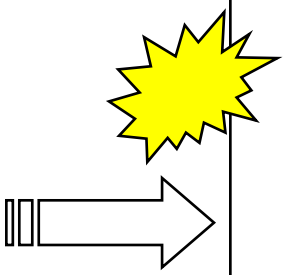
システム構成面での予防策

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 。

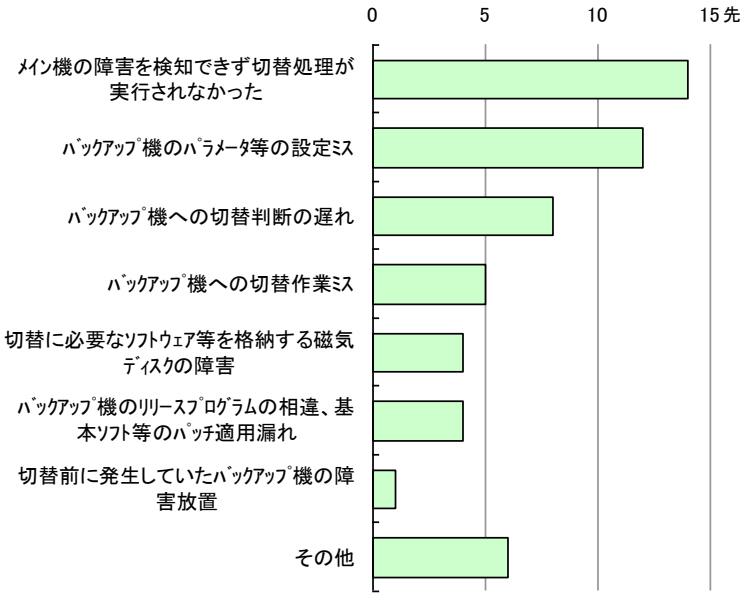
2. システム障害に関するアンケート調査
（7）予防策が想定どおり機能しなかった要因②

●「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。

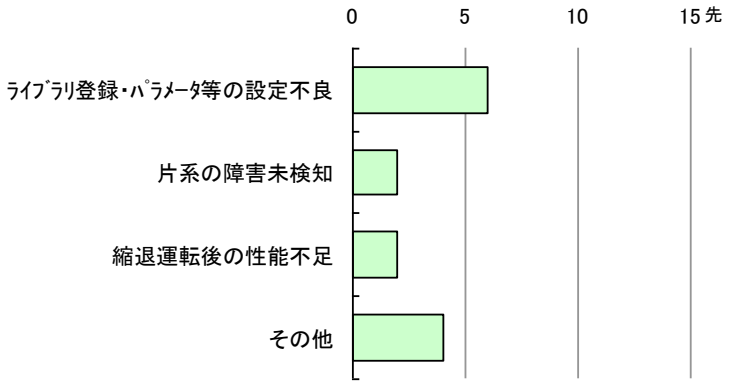
（図表11）バックアップ機への切替遅延・不能が発生した要因（対象34先の複数回答）



2. システム障害に関するアンケート調査
（7）予防策が想定どおり機能しなかった要因③

●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。

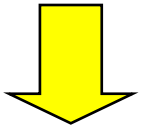
（図表12）縮退運転への切替遅延・不能が発生した要因（対象12先の複数回答）



2. システム障害に関するアンケート調査
（8）調査結果等からみえてくる留意点①

・ 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。

2. システム障害に関するアンケート調査
（8）調査結果等からみえてくる留意点②

●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

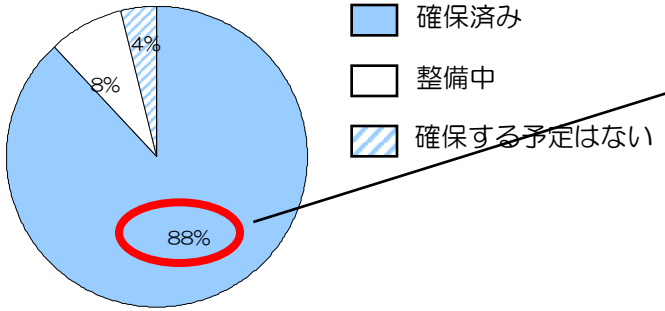
✓磁気ディスク装置障害発生時にも切替ソフトウェアへ影響が及ばないよう、同じシステム系列に切替ソフトウェアを配置しないなど、同ソフトウェアの設置場所について配意

Ⅱ．金融機関のバックアップ・コンピューターセンターの実効性確保にかかる課題と対応策

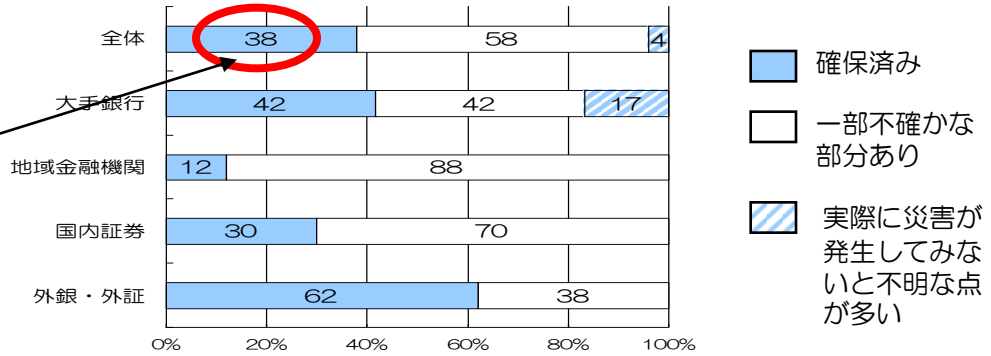
1. 現状

- 各金融機関では、平常時のシステム品質の向上やシステム障害時の対策に加え、災害時等に備えた業務継続体制の整備に努めている。
- 現在では、既に多くの金融機関が、コンピュータ・センターが機能しなくなった場合に備えたバックアップ・コンピュータセンター（以下、「バックアップセンター」）を確保。
- もっとも、バックアップセンターを確保していても、業務継続体制の実効性確保の面では、なお課題があると考えている先が多い。

▽バックアップセンターの確保状況（08年）



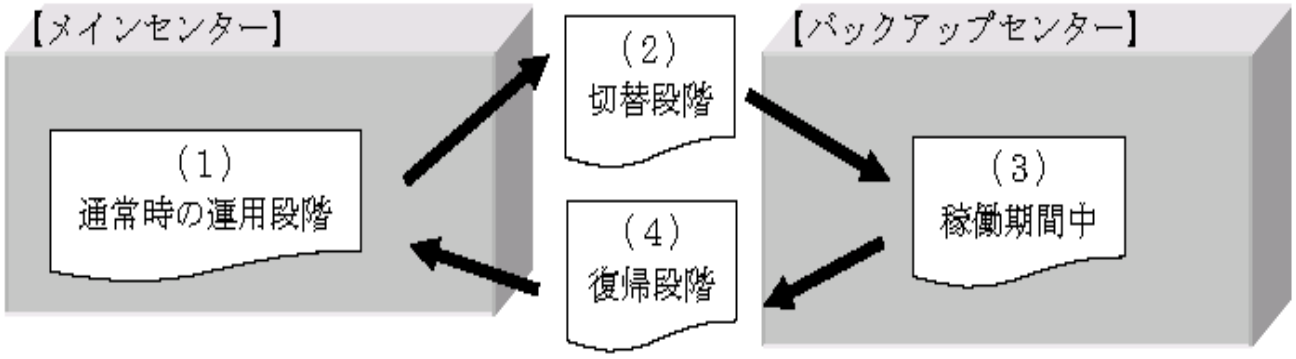
▽業務継続の実効性確保（08年）



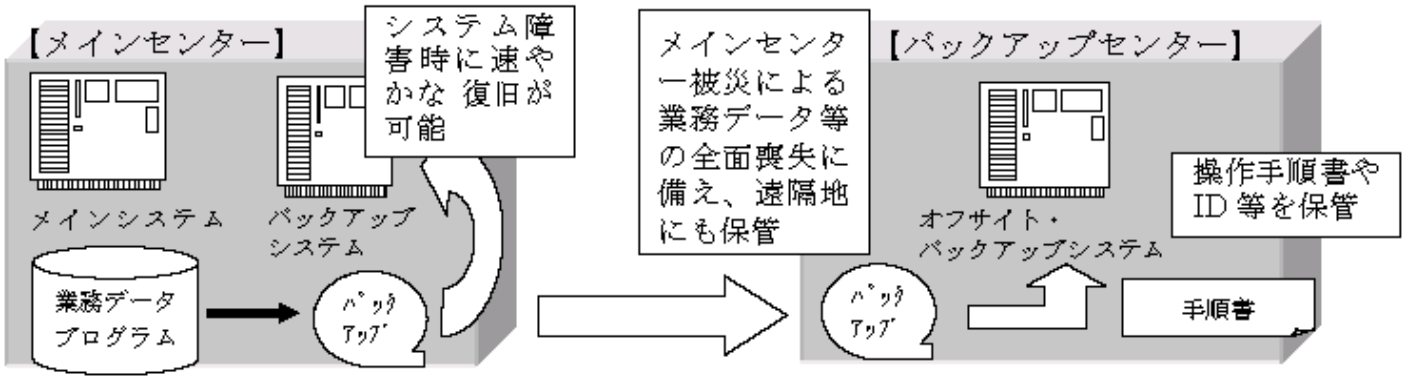
――「業務継続体制の整備状況に関するアンケート（2008 年11 月）調査結果」（日本銀行金融機構局）より抜粋

2. 課題と対策
（1）バックアップセンターの管理に関するフェーズ分け

- 以下、下図のとおり、フェーズを4段階に分け、課題と対策を解説。

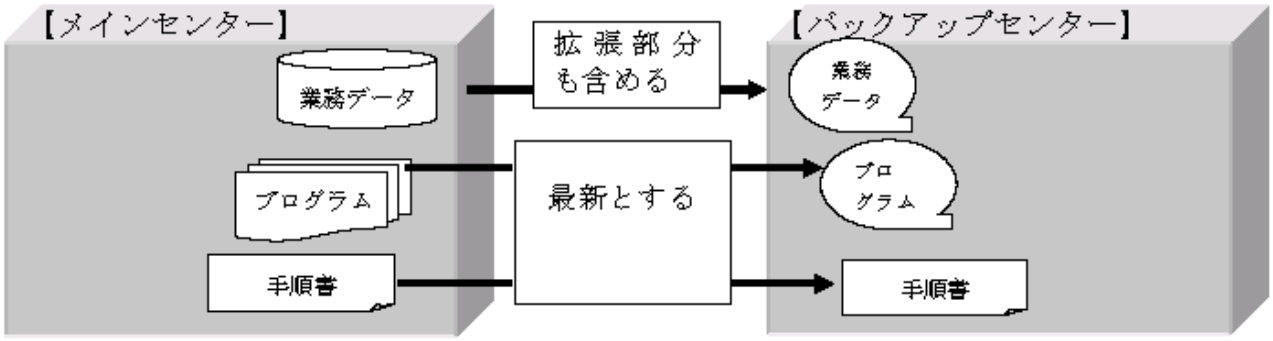


2. 課題と対策
（2）バックアップセンター稼働に向けた通常時の運用段階①



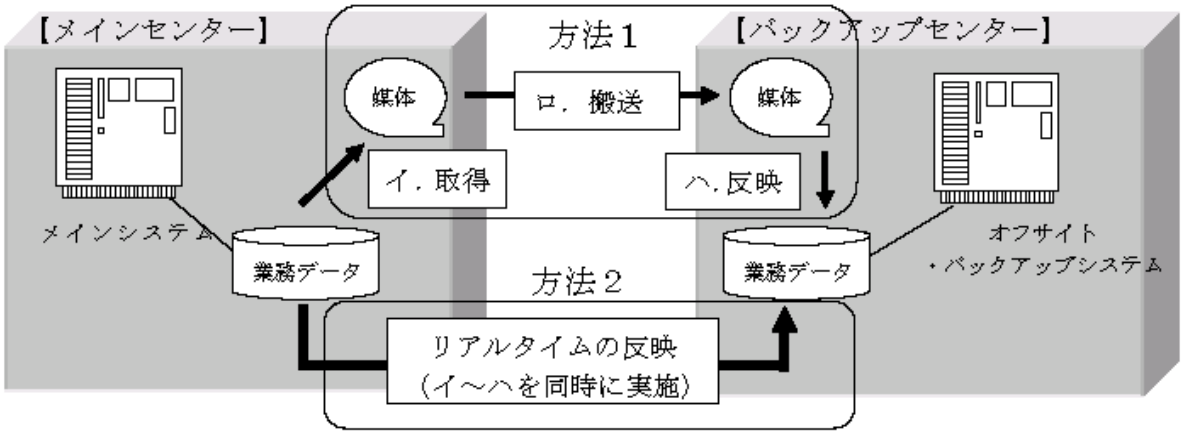
検討を要する事例	課題・対策
・バックアップデータの取得目的は、センター切替を伴わないシステム障害対応用に限定。メインセンター被災を想定していないため、バックアップデータの遠隔地保管は行っていない。	・メインセンターが被災した場合、預金残高等が復元できず、業務継続に極めて重大な支障が生じる。 ➢地震や火災などメインセンター全体が被災するシナリオを想定し、重要な業務データ等はメインセンターと同時被災しない遠隔地に保管する。
・バックアップセンターの立上げに必要なIDやパスワードがメインセンターに保管され、切替時には持ち出して使用することを想定した管理になっている。	・メインセンター被災時に建物内に立ち入れない場合、バックアップセンターの立上げができない。 ➢バックアップセンターの立上げや運行に必要なID等は同センターで直ちに利用できるよう管理する。

2. 課題と対策
（2）バックアップセンター稼働に向けた通常時の運用段階②



検討を要する事例	課題・対策
・業務データのバックアップは、毎日最新分を取得しているが、プログラムは変更頻度が少ないことからバックアップの取得を月に1度としている。	・業務データとプログラムの整合性が確保されない場合、システムが正常稼働せず、顧客取引や残高明細を復元できない。 ➢業務データとプログラムは整合性をとってバックアップを取得しておく。
・データベース拡張後に、バックアップ取得対象範囲の見直しをしていない。	・拡張分のデータが、バックアップセンターに反映されず、一部顧客の業務が再開できない。 ➢データベースの拡張等メインセンターにおけるシステム変更時には、バックアップ取得対象範囲の十分性を確認する。

2. 課題と対策
（2）バックアップセンター稼働に向けた通常時の運用段階③



検討を要する事例	課題・対策
・業務継続計画を見直し、「重要業務は当日中に復旧させること」としたが、バックアップの取得・反映方法の見直しを行っていない。	・バックアップデータの取得・反映に時間がかかり、業務継続計画で求めている時間内に業務復旧ができない。 ➢業務データのバックアップ取得から反映までに要する時間を試算のうえ、適切な反映方法を確定する。

2. 課題と対策
（3）バックアップセンターへの切替段階①－１

バックアップセンターに設置しているシステムの処理能力や各種機能は、メインセンターのそれと比較して劣る場合が多い。

バックアップセンター切替後に起こり得る諸制約
- 営業店における手作業処理の増加、
- 顧客が利用できるATMの台数が制限される、等々

こうした制約を把握しないまま切替を行った場合、切替当初は想定していなかった事務処理の発生により業務部署に過度な負担が生じたり、想定以上に顧客利便性が低下する可能性。

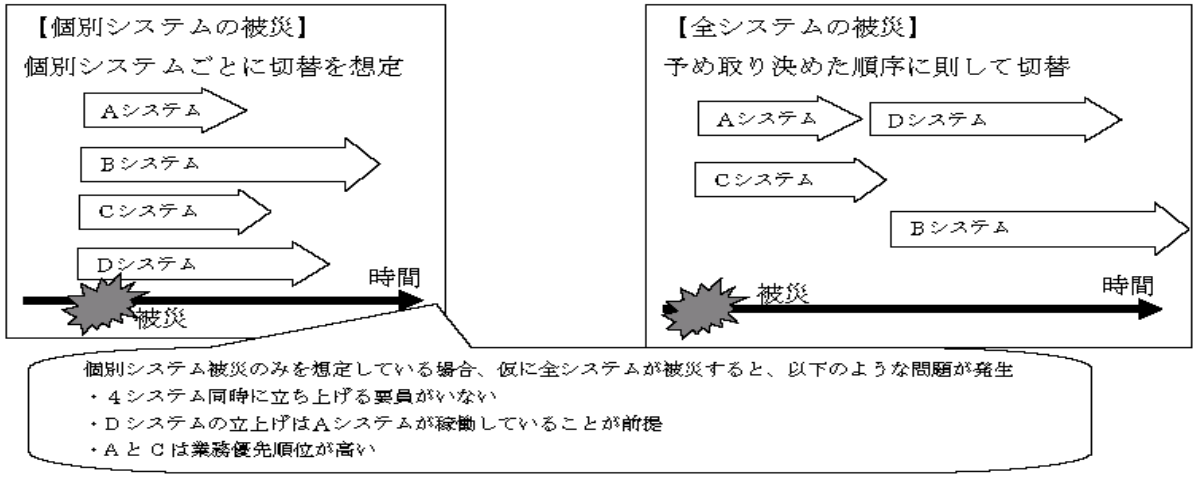
一方で、バックアップセンターの立上げに際して関係部署がその場で協議しながら切替判断を行う場合には、調整に時間を要し、業務の再開に予想外の時間を要する可能性。

2. 課題と対策
（3）バックアップセンターへの切替段階①－２

検討を要する事例	課題・対策
・切替基準が、システム処理能力等の制約や、バックアップセンターからメインセンターへの復帰のための所要期間を踏まえたものになっていない。	・バックアップセンターでの運用面の制約を踏まえずに切り替えた場合、想定外の制約の下で長期の異例運用を余儀なくされ、顧客に大きな影響を与える可能性がある。 ➢バックアップセンターの諸制約の洗い出しやメインセンターへの復帰所要期間の試算を予め行い、これを踏まえた切替基準を定める。
・共同センターのシステムを利用している先において、切替基準や権限者を定めていない。	・共同センターにおいて複数金融機関のシステムを共同運行している場合には、各社毎の事情に応じた切替判断ができないことも想定される。 ➢共同センターの運営体制や契約関係を踏まえ、運営会社や加盟各社等との間で、切替にかかる基準や権限、意思決定手続等を予め明確にする。

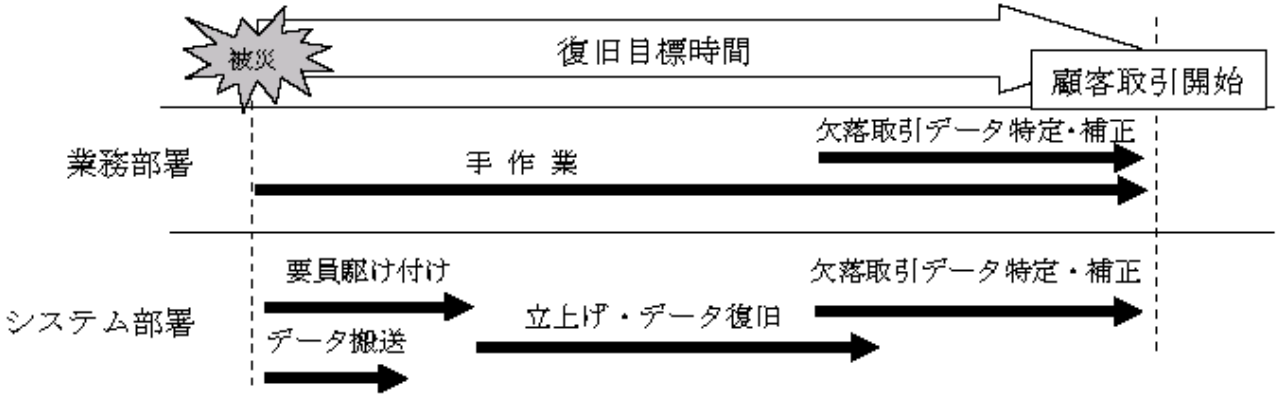
2. 課題と対策
（3）バックアップセンターへの切替段階②

▽システムの被災範囲による対応事例



検討を要する事例	課題・対策
・メインセンターの全面被災時における切替は、個別システム毎の切替手順書を用いることにしている。	・システム全体で見たときの立上げ順序が考慮されていないため、稼働開始に時間を要する。 ➢バックアップセンターへの切替作業は、業務の優先度、切替作業に従事可能な要員数、システム資源制約（コンピュータの処理能力等）等を踏まえ、全体の切替手順を事前に作成しておく。
・個別システム毎の切替を想定しているが、周辺システムとの連動が考慮されていない。	・連動するシステムからデータが入力されないため、切替を行った個別システムが稼働しない。 ➢個別システムの切替を想定する場合、周辺システムやネットワーク環境（アドレスの変更等）との連動関係も考慮した手順とする。

2. 課題と対策
（3）バックアップセンターへの切替段階③



検討を要する事例	課題・対策
・業務部署では業務毎に復旧目標時間を定めているが、バックアップセンターの切替時間（システム復旧時間）を勘案していない。	・業務部署が想定した時間内にシステムが復旧しない可能性がある。 ➢業務部署の復旧目標時間は、システム部署が担当する切替作業や、欠落取引データの特定・補正作業等の所要時間を考慮したものとする。
・欠落取引データは、営業店端末の取引履歴を基に特定し、反映作業を行うこととしているが、その他のチャネルでの取引については考慮されていない。	・顧客サービス・取引再開後に預金残高の不整合に伴うトラブルが発生する可能性がある。 ➢欠落取引データが発生する可能性がある営業店端末、自社・提携ATM、インターネットバンキング等の取引を含めて、反映方法等を取り決める。

2. 課題と対策
（4）バックアップセンターの稼働段階

検討を要する事例	課題・対策
・バックアップセンターの処理能力が、メインセンターのシステムより劣っているが、その制約について考慮した運用が想定されていない。	・全てのATMを稼働させた場合、メインコンピュータの能力不足により、ATMの応答時間が遅くなり、実用に堪えない。 ➢処理能力を踏まえて営業店端末やATM等の稼働台数を制限する。また、帳票出力等の夜間処理がオンライン開局までに完了しないことが想定される場合、作成する帳票を制限する。
・バックアップセンターにおける運用体制は、切替作業および稼働開始直後に必要な要員についてのみ想定している。	・運用要員が不足し、システムを安定的に稼働できない。 ➢システムの運行監視などを手作業で行わざるを得ない場合には、システム操作時における複数人による目視検証など、堅確性の確保にも配慮する。
・共同委託型のバックアップセンターには、利用が想定される全社が同時に利用できるシステムが装備されていない。	・バックアップセンターへの切替を実施しようとしたが、他社が利用中のため、システムを利用した業務継続ができない。 ➢メインおよびバックアップセンターともに複数社で共用する場合には、バックアップセンターが全社同時に利用できることを確認する。 ➢メインセンターは共用せず、バックアップセンターのみ共用する場合には、各社のメインセンターがそれぞれ遠隔地にあり、同時に被災するリスクが小さいことを確認する。

2. 課題と対策
（5）メインセンターへの復帰段階

検討を要する事例	課題・対策
・メインセンターへの復帰に際して、リハーサルを行うことを想定していない。	・メインセンターに復帰する際には、利用実績の少ない手順書や移行ツールを使用することになるため、想定時間内にメインセンターへの復帰ができない可能性がある。 ➢復帰作業が想定時間内に正常に行われ、かつ復帰後のシステムが正常に稼働することを、通常時から確認する。

3. まとめ

- メインセンターに設置したシステムが災害等により停止した際に、バックアップセンターが想定どおりに稼働しなかった場合の経営への影響は大。

⇒ バックアップセンターの実効性確保は、リスク管理として極めて重要。

経営の適切な関与の下での組織一体的な取り組み

・システム部署の対応のほか、業務部署における対応（バックアップオフィスの整備や要員の確保等）

・リスク管理部署や監査部門における目線を替えた有効性の検証

・社内横断的な定期協議の場を設け、問題点の洗い出しや改善策の検討を行う体制を整備

・また、
⇒ バックアップセンターの運用体制は、一旦整備した後も、組織変更の都度、あるいは、事務量の増加やシステムの更新に合わせて、必要な追加・調整を行う
⇒ 各種訓練（連絡訓練、参集訓練、システム切替訓練等）を定期的に実施し、対応策を見直す

3. まとめ（続き）

- なお、バックアップセンター運用に当たって必要となる管理の水準や体制は、それぞれのビジネスモデルや提供しているサービスの内容、同センターの利用方法（単独か共同委託か）等によっても異なる。

⇒ 上記で述べた対策を直接当てはめるのではなく、自社の置かれた環境と役割を踏まえた対応策を検討。

⇒ 共同委託型のバックアップセンターを利用している金融機関におかれても、主体的に対処すべき課題として認識したうえで、委託先との対話を深めるとともに、自社内の運用方法の確立やマニュアルの整備等に役立てて頂きたい。

以 上

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