システム監査学会第３８回研究大会
＜「IT監査保証の判断基準」 研究プロジェクト報告＞

オペレーショナル・レジリエンスの向上とシステム監査
Improving Operational Resilience and Systems Audits for it

発表者：静岡大学　遠藤正之

2024年６月７日２版

IT監査保証の判断基準研究プロジェクトメンバー

松尾明（主査）	公認会計士, CISA, TOGAF9認定アーキテクト
石島隆	法政大学経営大学院教授
成田和弘	有限責任監査法人トーマツ、システム監査技術者, CIA, CISA
鈴木夏彦	日本電気株式会社、システム監査技術者, CIA, CISA
牧野博文	株式会社東芝、システム監査技術者, ITストラテジスト, 情報処理安全確保支援士, ITコーディネータ, CISA
遠藤正之	静岡大学情報学部教授

発表の構成

Ⅰ．バーゼル銀行監督委員会「オペレーショナル・レジリエンスのための諸原則」

Ⅱ．金融庁「オペレーショナルレジリエンス確保に向けた基本的な考え方」

Ⅲ．バーゼルコアプリンシプル改訂版の市中協議

Ⅳ．ITレジリエンス観点でのシステム障害対策の4つの観点

Ⅴ．事例研究：2023年10月全銀システム障害

Ⅵ．オペレーショナル・レジリエンス7つの原則に対するシステム管理基準の着眼例

Ⅰ．バーゼル銀行監督委員会「オペレーショナル・レジリエンスのための諸原則」（2021年3月）

オペレーショナル・レジリエンスとは、パンデミック、サイバー攻撃、システム障害、自然災害などの混乱に際して、銀行が重要な業務を継続できる能力

（１）業務中断が起こり得ることを前提に、その影響が許容水準内に収まるよう態勢整備を求めるもの。
（２）BCP 等の個別のプロセス整備だけではなく 、業務中断による影響の軽減・緩和、初動・回復に繋げるキャパシティの確保等、包括的な検証と態勢整備を求めるもの。
（３）想定する問題事象とその対策を纏めるといったリスク管理的アプローチだけでなく 、失敗に至る原因を事前に想定し、因果関係を遡りながら脆弱性を除去するリバース・エンジニアリング的アプローチに基づくもの 。
（４）組織横断的な取り組みにあたり、経営陣のトップダウンによるコミットメントを求めるもの。

Bank for International Settlements（2021）”Principles　for Operational Resilience”及び金融庁/日本銀行（2021）による

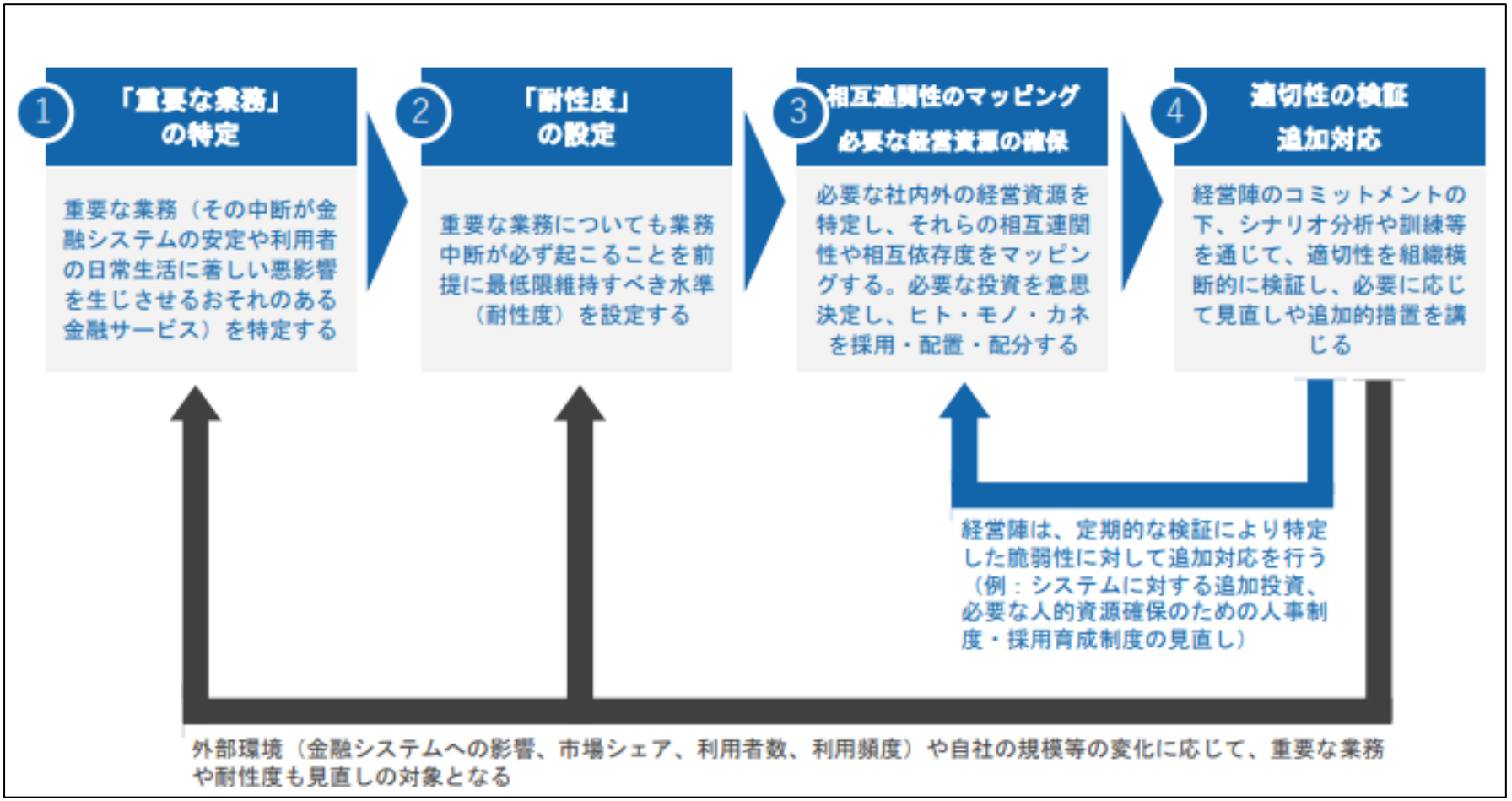
7つの原則(プリンシプル・ベース)

①ガバナンス	銀行は、業務中断時にも重要な業務の提供に及ぼす影響を最小限に抑えられるよう、既存の体制を活用し、オペ・レジリエンスに係る方針を確立、監督、実施すること。
②オペリスク管理	銀行は、オペリスク管理のための機能を応用することで、業務プロセス、人的資源、システムに対する組織内外の脅威や潜在的なリスクを常に把握すること。また、自行のオペ・レジリエンスに係る方針に沿って、重要な業務の脆弱性を速やかに評価し、リスクを管理すること。
③BCPとテスト	銀行は、BCPを整備すること。また、深刻であるが起こり得るシナリオを想定した訓練を実施し、障害時でも重要な業務を継続できるか確認すること。
④相互連関性の特定	銀行は、重要な業務を特定したうえで、オペ・レジリエンスの方針に沿って、重要な業務の提供に係る組織内外の相互連関性や相互依存関係をマッピングすること。
⑤サードパーティ依存度の管理	銀行は、重要な業務の提供に関わるサードパーティやグループ内組織への依存度を管理すること。
⑥インシデント管理	銀行は、リスクのアペタイト（選好度）や許容度に沿って、重要な業務の提供を阻害しうるインシデントを管理するための初動・回復計画を策定・実施すること。また、実際に発生したインシデントからの教訓を踏まえて、同計画を継続的に更新していくこと。
⑦サイバーを含むICTセキュリティ対応	銀行は、侵害の検知や防御、初動・回復プログラムにかかる、サイバー関連を含む頑健なICTセキュリティを確保すること。またこれらプログラムは定期的にテストされ、周囲の状況を適切に認識し、重要な業務をサポートするためのリスク管理や意思決定プロセスのための情報を提供するものでなければならない。

金融庁/日本銀行（2021）による

Ⅱ.金融庁「オペレーショナルレジリエンス確保に向けた基本的な考え方」（2023年2月）

オペレジの基本動作



金融庁（2023）

Ⅲ. バーゼルコアプリンシプル改訂版の市中協議

原則25オペレーショナルリスクに関しての改訂項目（2024年4月確定）

基準	改訂内容
必須基準１	法律、規則または監督当局は、銀行に対し、以下の事項を行うための適切なオペレーショナルリスク管理及びオペレーショナルレジリエンス戦略、方針、手続 、システム、 統制及びプロセスを有することを求める 。 (a)オペレーショナルリスクを識別、評価、監視、報告、管理、軽減すること 。 (b)脅威や潜在的な障害を特定するとともに、破壊的な事象に対応・適応し、重要な業務の遂行への影響を最小化すること。
必須基準６	法律、規則または監督当局は、銀行に対し、サイバーセキュリティを含む強固な情報通信技術ICTの枠組み、及びオペレーショナルリスク管理の枠組み及びオペレーショナルレジリエンスアプローチ と整合的なリスク管理の実施を求める 。
必須基準８	監督当局は、重要な業務を中断させるインシデントやその重要性の報告を含め、オペレーショナルリスクに影響を与える事態について、常に情報を得られるような適切な報告メカニズムを有するよう銀行に求める。

金融庁/日本銀行（2023）による

Ⅳ．ITレジリエンス観点でのシステム障害対策の4つの観点

対策種類	説明
予防	障害が起きにくい設計を行う、システム投資の計画段階からの考慮が必要
検知	システムの異常やシステムダウンの原因を、早期に発見して対処する
代替	別の手段でサービス提供を継続し、利用者への影響を最小化する
復旧	障害箇所をバイパスする暫定対処と完全な修正を行う本格対処がある

大和総研（2022）

Ⅴ．事例研究：2023年10月全銀システム障害

発生から検知

2023年10月7日（土）～9日（祝）
全銀システムの中継コンピュータを「RC17」から「RC23」へ更新する移行の第1回目として、14金融機関での移行が実施

10 月 10 日（火）朝、10金融機関で中継コンピュータがシステムダウン。
10金融機関は、いずれも中継コンピュータ内の「内国為替制度運営費付加・チェック処理」を利用。
この10金融機関と他金融機関との間でテレ為替経由でのリアルタイム送金ができない状況。

解析により、内国為替制度運営費のテーブルを参照する際にエラーが発生することが判明。

遠藤正之（2024）

代替

新ファイル転送または電子媒体での持込

しかし、対象データの多さ、金融機関側で内国為替制度運営費のデータを追加する等の準備作業が必要。

2日間で約315万件の発信に対し、約107万件の発信の持ち越しが発生（2023年12月1日の公表数字による）。

遠藤正之（2024）

復旧

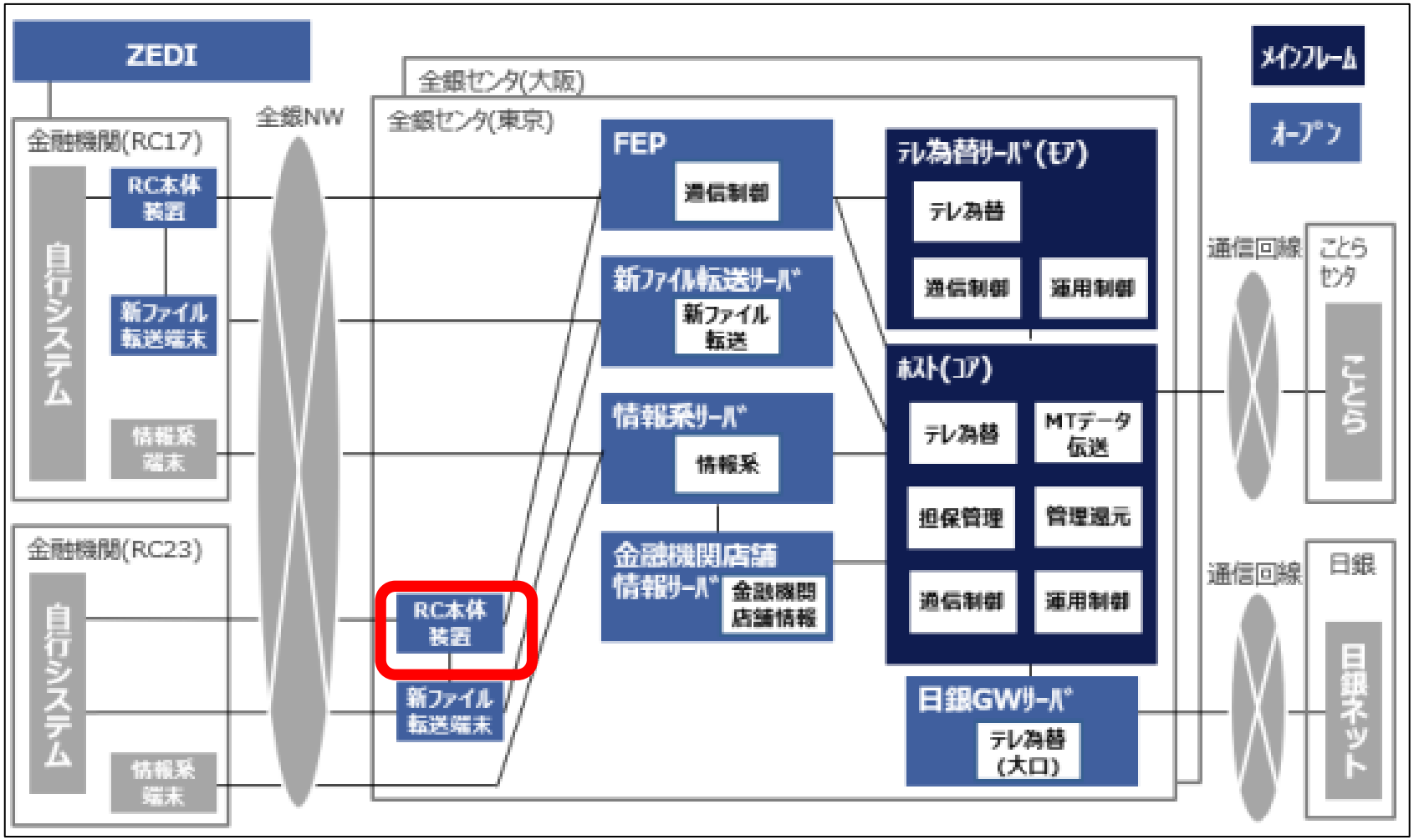
暫定対処１（10日）
内国為替制度運営費のテーブルを参照せずに、固定値にて内国為替制度運営費の金額を入力するプログラム修正を。
しかし、プログラムの改修箇所が多岐にわたり、結局翌11日のオンライン開始までにプログラム修正が間に合わず、10金融機関での他金融機関との間の送金ができない状況が翌日も継続

暫定対処２（11日）
内国為替制度運営費の金額を一律0円とするプログラム修正、翌12日から稼働。

本格対処（2024年1月から3月）
内国為替制度運営費の計算をプログラムで行う形

遠藤正之（2024）

全銀システムの概要

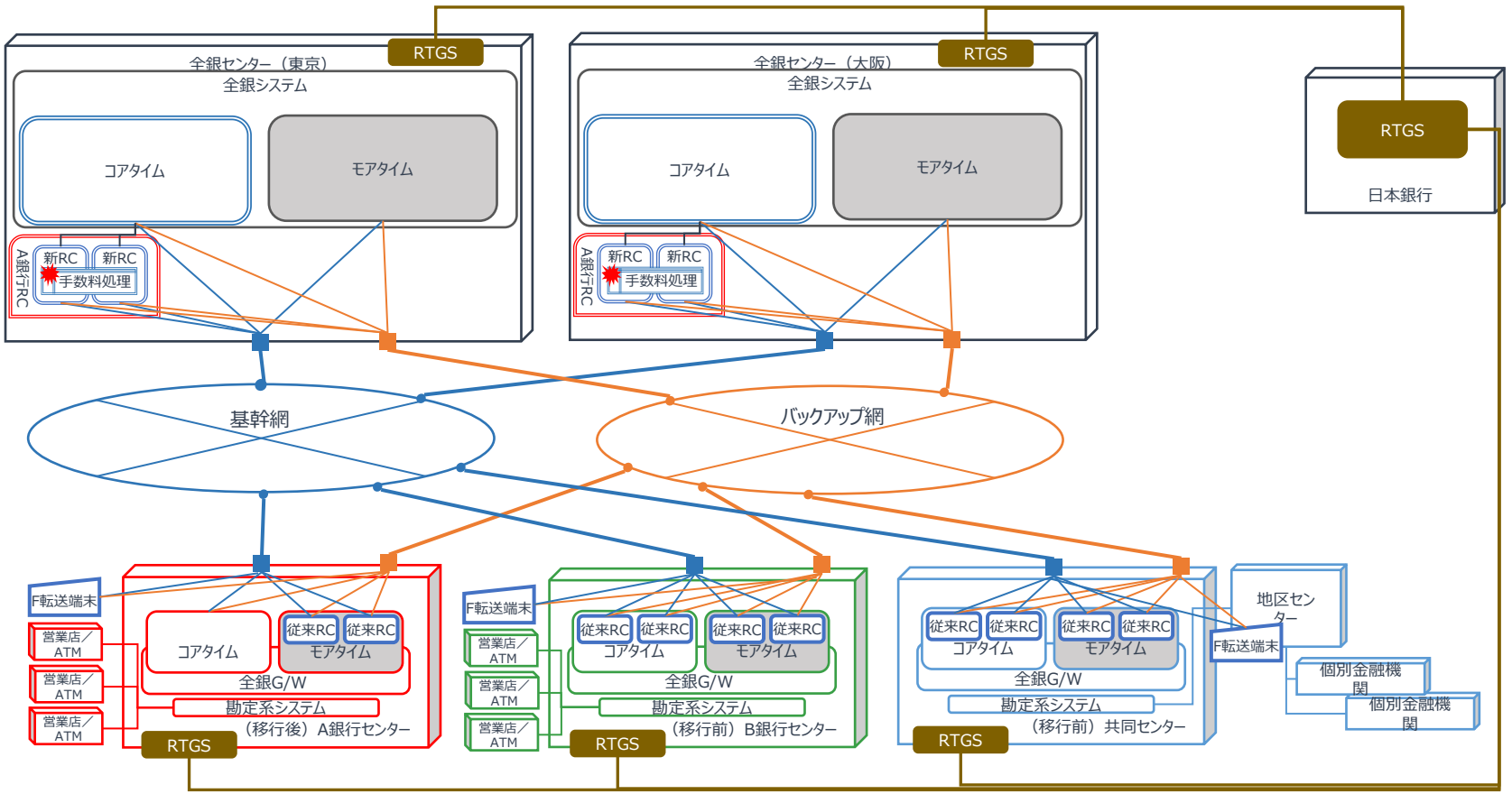


障害発生箇所は、全銀センタ（東京、大阪）のRC23（中継コンピュータ）

全国銀行資金決済ネットワーク（2023.3）

全銀システムの概要（移行中のイメージ図）

※推定含む



移行後の金融機関と移行前の金融機関が並存する形

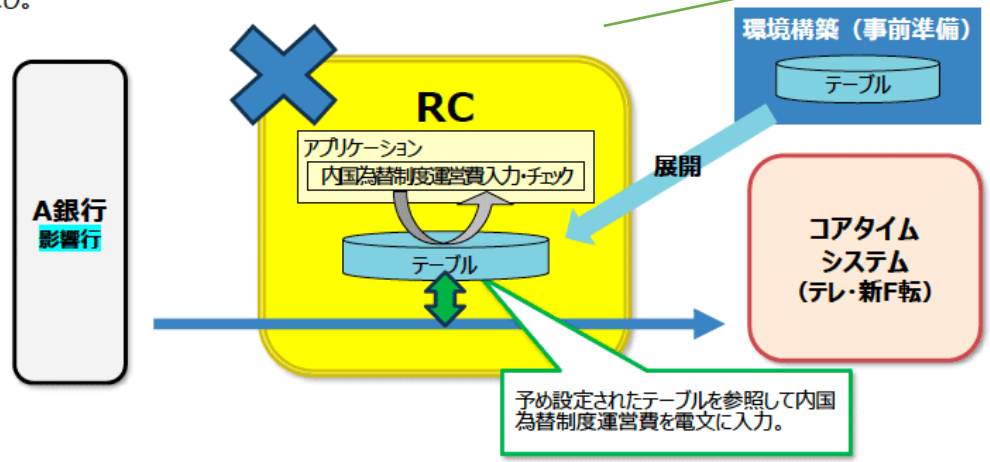
公表資料を基にプロジェクトで作成

（参考）障害原因に対する当研究プロジェクトでのディスカッション

一般社団法人全国銀行資金決済ネットワーク

障害の原因

- 電文1件ごとに、仕向機関が被仕向機関に支払う「内国為替制度運営費」（金額は種目により異なる）については、「①金融機関が予め電文に金額を入力してRCに送信」、「②予めRCに設定されたテーブルを参照して、RCが電文に金額を入力」、のいずれかの方法がある。
- 今回、②の方法を採用している10行において、「予めRCに設定されたテーブルをRCが参照する処理」でエラーが発生し、RCが異常終了した。
- なお、①の方法を取った３行は影響なし。また、JPモルガン・チェースのコアタイムシステム用のRCは、旧機種のままであった。コアタイムシステムにおける障害を踏まえて、モアタイムシステム（接続は任意）に接続していないため、結果的に影響なし。



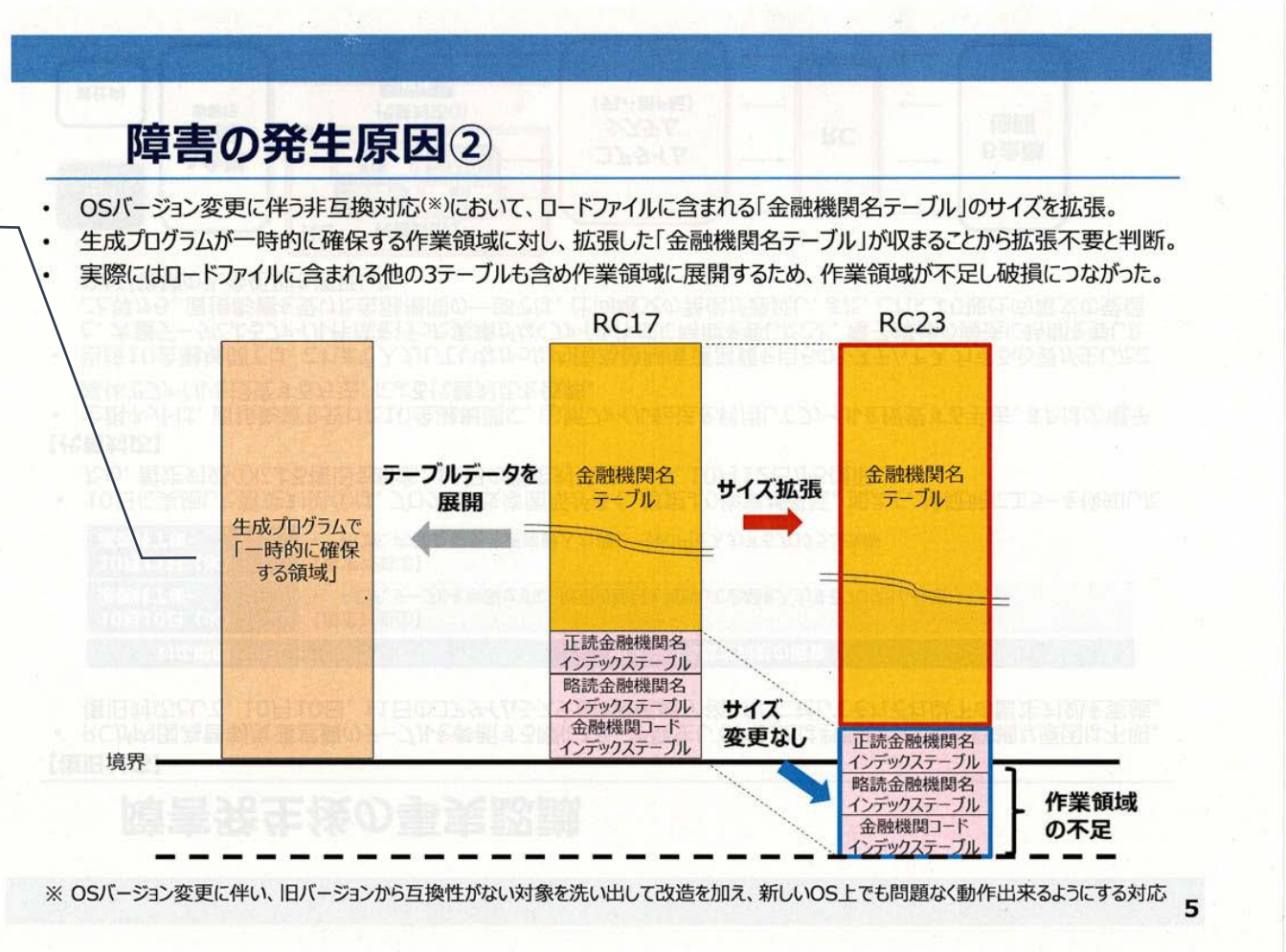
※上記は、現時点で確認できている状況。 5

- 「すべての銀行に対して正常に電文を送ることができる」ことの確認が必要だったが、テストのバリエーションが不足していた。
- 「銀行とつながり続けること」が使命のRCにビジネスロジックをいれたところにも、遠因がある
- 移行段階での実機での確認も不十分だった。

全国銀行資金決済ネットワーク（2023.10.18）

（参考）障害原因に対する当研究プロジェクトでのディスカッション

- RC内の領域設計についての認識相違
- 設計では影響があることを認識しているのにテストをしていなかったのでは。
- 領域オーバーは、コードの静的チェックや動的チェックでも見つかるのではないかという疑問？
- OSのアドレッシングモードの変更が今回の主要な変更との認識が不十分だったのでは。

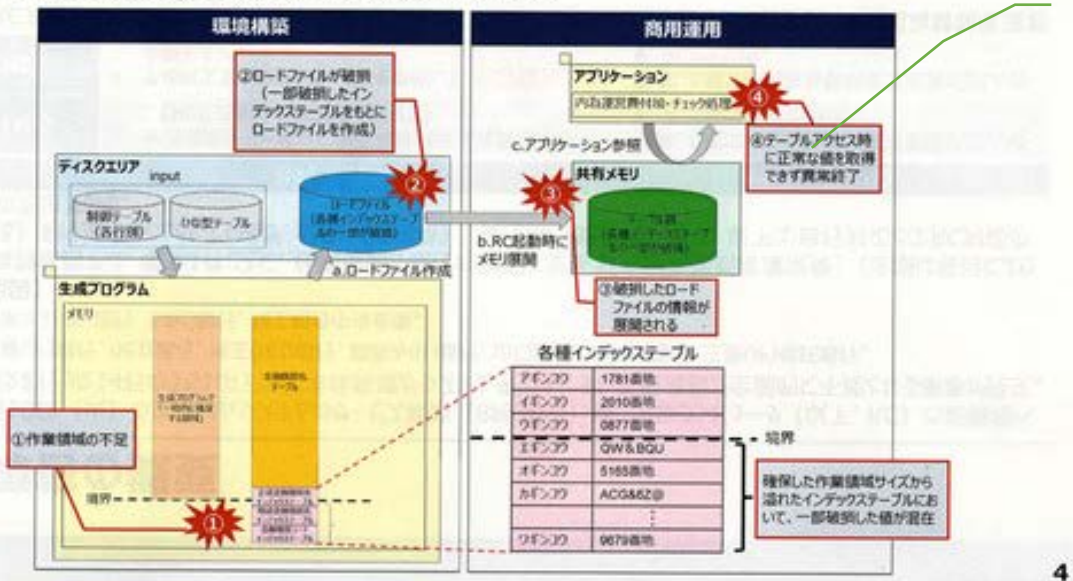


全国銀行資金決済ネットワーク（2023.12.1）

（参考）障害原因に対する当研究プロジェクトでのディスカッション

障害の発生原因①

- 環境構築時に使用する生成プログラムの不具合が原因。
- 生成プログラムのテーブル作成処理の不具合（一時的に確保する作業領域が不足、下図①）により生成したロードファイルの一部が破損（下図②）。
- 内国為替制度運営費のテーブルは、システム起動時にディスクエリアにあるロードファイルから展開（下図③）。
- テーブルアクセス時に正常な値を取得できず異常終了（下図④）。



- 環境変更に伴う制約事項が、意識されず、レビューやテストでも発見されなかった。

全国銀行資金決済ネットワーク（2023.12.1）

（参考）障害原因に対する当研究プロジェクトでのディスカッション

障害発生後の事実認識

【復旧対応】

- RCが内国為替制度運営費のテーブルを参照する際にエラーが発生していることは判明したものの、詳細な原因は不明。復旧対応として、10月10日、11日のコアタイムシステムの通信終了後、RCに対してそれぞれ以下の暫定対処を実施。

対応期間	RCに対する暫定対処の概要
10月10日（火） 通信終了後～	【暫定対処①】 ・ RCが、テーブルを参照せずに、取引の種目を判別して金額を入力するプログラム改修
10月11日（水） 通信終了後～	【暫定対処②】 ・ RCが、内国為替制度運営費入力欄に一律0円を入力するプログラム改修

- 10日に実施した暫定対処①は、プログラム改修箇所が多く、想定より作業が遅延。加えて、検証時にエラーを検知したため、暫定対処①による復旧を断念。11日の暫定対処②により、10月12日から復旧。

【代替対応】

- 全銀ネットは、直接影響を受けた10金融機関に、①新ファイル転送を利用してファイルを授受する手法、または②電子媒体でファイルを授受する方法、による代替対応を依頼。
- 当該10金融機関では、これまで入力していなかった内国為替制度運営費を自らのシステムで入力する必要が生じたこと、大量データによるファイル作成を行った実績がなくファイル作成に時間を要したこと、電子媒体の搬送に時間を要したこと等から、直接影響を受けた金融機関の一部では、仕向電文の発信が遅延し、また、これにより被仕向電文の受信および後続の入金処理も遅延した。

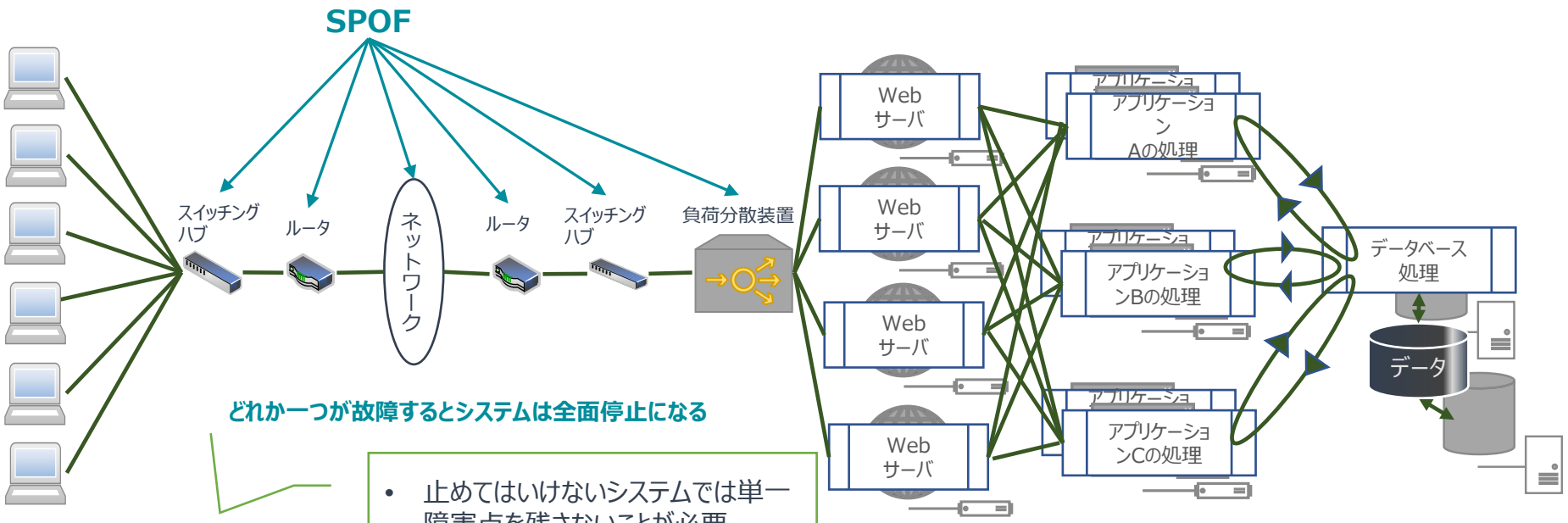
6

- 実績のある旧システムに戻す手順が準備されているべきだった
- **社会的影響の大きなシステムであるにもかかわらず、不測の事態を想定した準備が不十分だったのでは。**

全国銀行資金決済ネットワーク（2023.12.1）

（参考）単一障害点の例

単一障害点（SPOF:Single Point of Failure）の例



どれか一つが故障するとシステムは全面停止になる

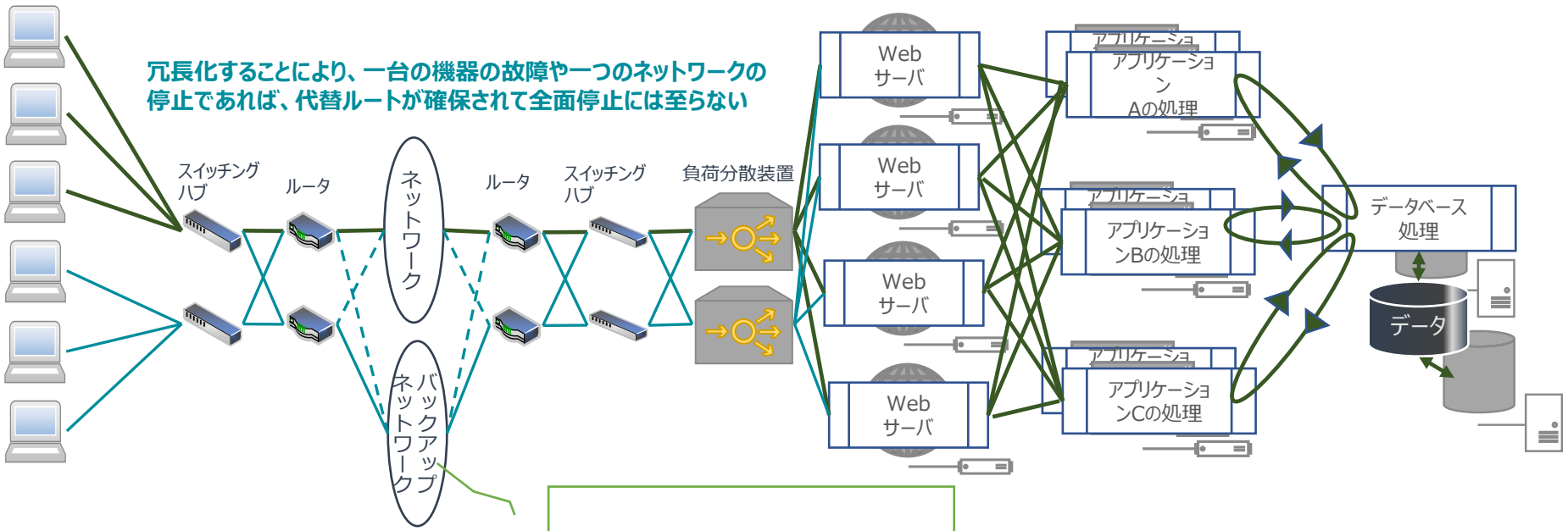
- 止めてはいけないシステムでは単一障害点を残さないことが必要
- 全銀システム障害における単一障害点は、「手数料処理」

負荷分散：並列に運用されている機器間で、負荷がなるべく均等になるように処理を分散して割り当てる

プロジェクトにて作成

（参考）単一障害点の改善例

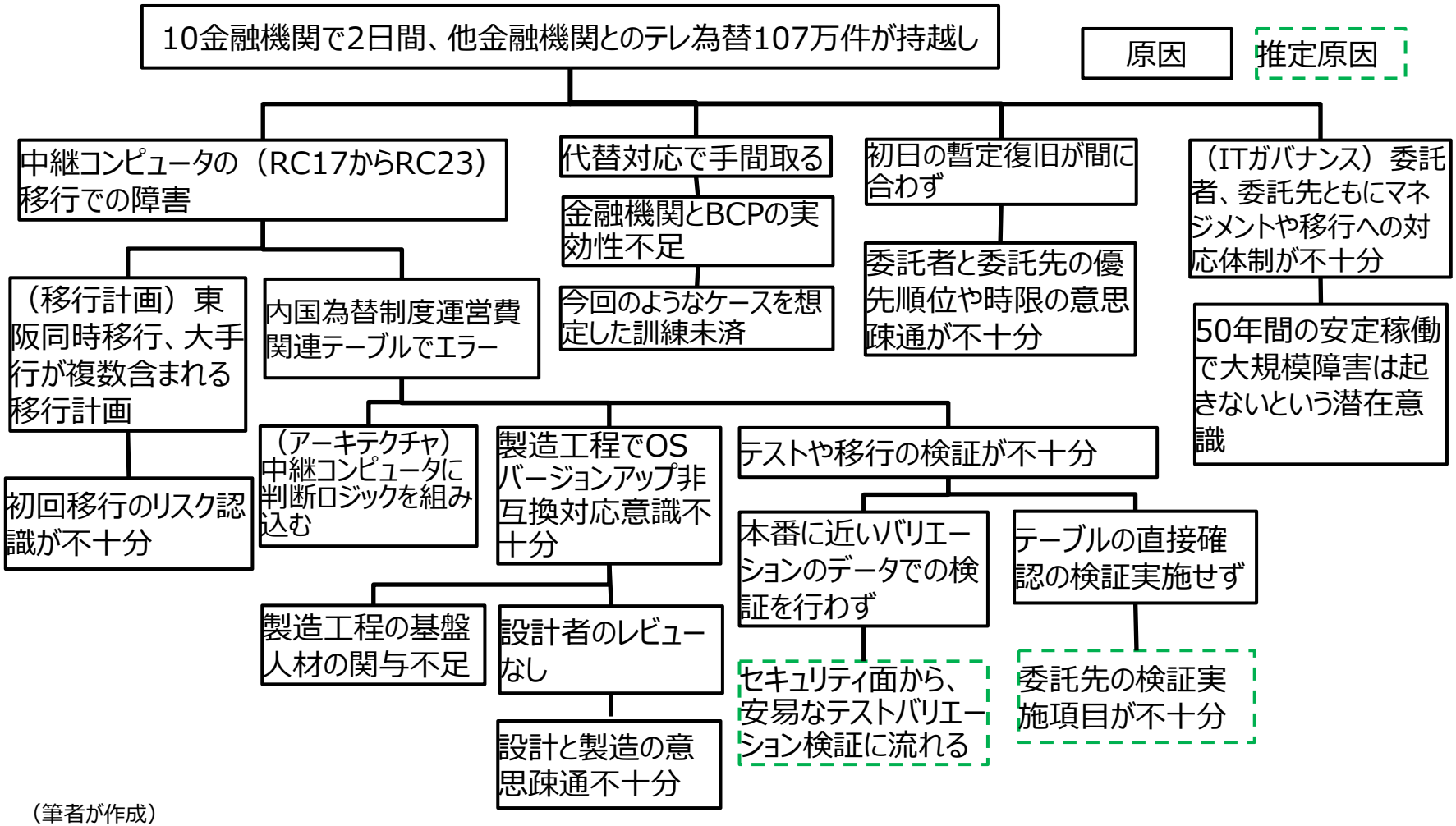
単一障害点（SPOF:Single Point of Failure）の改善例



- **リスク回避のためには旧システムの併存も検討が必要だった。**

プロジェクトにて作成

全銀システム障害の根本原因分析



（筆者が作成）

委託者、委託先とも移行のリスク認識低く、代替対応や暫定復旧対処も不十分。

予防・検知の問題点：全銀システム障害

直接的原因：内国為替制度運営費の情報に係わるインデックステーブルの生成処理の不具合により、インデックステーブルが破損していたため。
その原因：テーブルを作成する処理において、OS（オペレーションシステム）のバージョンアップに伴うサイズ拡張の認識不足により、必要なメモリの確保が不十分であった

予防・検知に関しての問題点（リスク顕在化要因）
１．データ引渡しが主役割の中継コンピュータへの複雑なロジック組み込み
２．プログラム実装時の設計仕様の確認が不十分
３．テストでのデータの網羅性が不十分で不良の検出漏れが漏れた
４．移行時のテーブル作成後の検証が行われなかった
５．移行計画に関しても、冗長構成の東京大阪の2か所の同時移行

遠藤正之（2024）

代替及び復旧の問題点：全銀システム障害

代替の問題点：新ファイル転送でのデータ授受や電子媒体でのデータ持ち込みへの変更作業を行う金融機関を巻き込んだ訓練や仕組みが不十分。
→持込や処理の時間切れが発生した。

復旧の問題点：暫定対処１のプログラム修正に当たる影響確認が不十分。
→最初からより修正箇所の少ない暫定対処２を選択する見極めができていれば、翌11日に稼働できた可能性が高い

遠藤正之（2024）

【全銀システム障害から学ぶ】金融機関のあるべき対応１

１．レジリエンスの前提として、重要な業務を定義し、優先順位付けを明確にする。
全銀システムの場合、国内の金融機関間のインフラであり、当日中の処理が要請されている。テレ為替、データ伝送、媒体持込といった複数手段のいずれかを利用して、当日中に金融機関から他の金融機関への振込を終わらせることが求められている。
また2系統の場合、1系統ずつ移行することも十分検討の余地あり。

２．予防に関する見直し。
・計画段階からシンプルな構成で運用のしやすいITシステムを構築する
・既存システムも含め、顧客影響を最小限にするために、事務処理に関する実効性のある複線化や、システムの冗長性の確保が行われているのかを、点検

遠藤正之（2024）

【全銀システム障害から学ぶ】金融機関のあるべき対応２

３．代替に関する事前点検や他組織関係者も考慮した訓練の実施。
全銀システム障害においては、障害が発生した中継コンピュータ経由での受け渡し以外に、新ファイル転送でのデータ授受や電子媒体でのデータ授受という手段が用意されていたことまでは良かったが、データ作成側の事務処理を考慮した実効性が不足。

４．代替に関する人的組織的準備。利用者視点での代替対応を行うためのタスクフォースを速やかに設置できるよう要員の使命付けをしておく。
システム障害時、システム開発担当部署は、原因箇所の把握と復旧に向けた修正への対応で手いっぱいになる。
顧客対応や広報については、システム担当部署とは別の指揮系統を取れるようなリソース配分で準備する。

５．システム更改計画の対外開示。これにより顧客も重要決済等を避けることで、影響範囲を狭めることが可能になる。

遠藤正之（2024）

【全銀システム障害から学ぶ】開発会社（委託先、再委託先）も含めた対応

１．開発段階での予防：再委託を含めた情報連携が必要。
例えば設計者が製造段階（プログラミング）のレビューにも関与するなど

２．テスト段階での予防：効率的な検証を行うために、実データ提供などの金融機関と開発会社間の協力が必要。

３．復旧：開発委託側と開発会社との共通認識が取れるような連携が必要。時限を共有して複数のプランを用意して判断することが望ましい。
（全銀システム障害の場合、全銀ネットが開発会社と復旧の優先順位の考え方について合意できておらず、代替案への切替時限等の取り決めもなく進めたため、復旧に手間取る）

遠藤正之（2024）

【全銀システム障害から学ぶ】接続する他組織も含めた対応

１．テスト段階の予防：テストでのデータ連携は、接続する金融機関の了解を得て、出来る限り本番でのデータを用いる。

２．代替：訓練の定期的な実施と参加。別ルートでの受け渡しをする際には、重複データの発生や、欠落データが発生しないように、持込側の金融機関でチェックが必要になる。代替を想定した事前の訓練が定期的に行われていれば、よりスムーズな代替手段での連携が行うことができる。

３．代替・復旧：実効性のある代替や復旧を行うため、接続する他組織との相互の連携の強化が必要。他金融機関での事業継続計画も取り込み、金融システム全体での事業継続を図ることが望まれる。システム人材の強化も必要。

遠藤正之（2024）

全銀システム障害事例のまとめ

組織内での机上での検討では、実効性に限界がある。重要な業務に関しては、開発会社や他組織も巻き込んだ検討や障害を想定した訓練を行うことで、ITシステムのレジリエンス力を高めていくことが重要

・次期全銀システムでのオープン化も見据えた改革の中で発生した障害であるという視点も必要。 大きな改革の初回は何らかのトラブルが出ることが多い。その意識がやや希薄だったのではないか。
・今後もDXにより、システムの組み換えが起こると障害が発生することは予想されるが、新技術の取込では そのようなチャレンジは必要であり、過度に障害を責めるのは、かえって保守的な発想から抜け出られなくなる点にも留意が必要。

遠藤正之（2024）

Ⅵ．オペレーショナル・レジリエンス7つの原則に対するシステム管理基準の着眼例

	7つの原則	システム管理基準の着眼例
①ガバナンス	業務中断時にも重要な業務の提供に及ぼす影響を最小限に抑えられるよう、既存の体制を活用し、オペ・レジリエンスに係る方針を確立、監督、実施すること。	• 組織体の目的及び IT 戦略の目標を達成するために、達成に及ぼす影響についてリスクを評価し、対応を行う。(I.2.4)
②オペリスク管理	オペリスク管理のための機能を応用することで、業務プロセス、人的資源、システムに対する組織内外の脅威や潜在的なリスクを常に把握すること。また、自行のオペ・レジリエンスに係る方針に沿って、重要な業務の脆弱性を速やかに評価し、リスクを管理すること。	• 情報システムに影響を与える重大事故、サイバー攻撃、災害、テロ等に対する対応策を具体化するため、影響範囲、業務の重要性及び緊急性を明確にし、復旧優先度を設定する。(Ⅱ.9.1)
③BCPとテスト	BCPを整備すること。また、深刻であるが起こり得るシナリオを想定した訓練を実施し、障害時でも重要な業務を継続できるか確認すること。	• 重大事故、災害等の発生時に、適切な措置を迅速、円滑かつ確実に実行するために、情報システムの業務継続計画を策定する。(Ⅱ.9.2) • 事業継続計画に基づいた情報システムの業務継続計画を最新の状態にして実効性を高めるために、定期的に訓練を実施し、実現可能性を検証する。(Ⅱ.9.4)

金融庁/日本銀行（2021）による

オペレーショナル・レジリエンス7つの原則に対するシステム管理基準の着眼例（続き）

	7つの原則	システム管理基準の着眼例
④相互連関性の特定	重要な業務を特定したうえで、オペ・レジリエンスの方針に沿って、重要な業務の提供に係る組織内外の相互連関性や相互依存関係をマッピングすること。	• 必要に応じて、地政学的要因やサプライチェーンに関連する要因についても考慮する。(Ⅱ.9.1)
⑤サードパーティ依存度の管理	重要な業務の提供に関わるサードパーティやグループ内組織への依存度を管理すること。	• IT戦略に基づいて外部サービスを利用するために、外部サービスの利用対象及び内容を明確にした外部サービス利用計画を策定する。(Ⅱ.8.1)
⑥インシデント管理	リスクのアペタイト（選好度）や許容度に沿って、重要な業務の提供を阻害しうるインシデントを管理するための初動・回復計画を策定・実施すること。また、実際に発生したインシデントからの教訓を踏まえて、同計画を継続的に更新していくこと。	• 利用部門と合意した目標内でインシデントを解決し、根本原因を特定して恒久的な対策を講じるために、インシデント管理及び問題管理の手順を定めて体系的に管理する。(Ⅱ.5.5)
⑦サイバーを含むICTセキュリティ対応	侵害の検知や防御、初動・回復プログラムにかかる、サイバー関連を含む頑健なICTセキュリティを確保すること。またこれらプログラムは定期的にテストされ、周囲の状況を適切に認識し、重要な業務をサポートするためのリスク管理や意思決定プロセスのための情報を提供するものでなければならない。	• 経営戦略及びIT戦略で定められた目標を達成するために、ITシステムの利活用に関するコントロールを実行し、その結果としてのパフォーマンス、コスト、リスク管理、コンプライアンス管理、社会的責任と持続性等の状況を経営者に報告するための体制を整備・運用する。(Ⅱ.1.1) • IT システムの利活用に関するリスク管理（サイバーセキュリティリスク管理を含む）のための体制が整備・運用されている。(Ⅱ.1.1達成目標６)

金融庁/日本銀行（2021）による

参考文献

Bank for International Settlements（2021）”Principles for Operational Resilience”
金融庁/日本銀行（2021）「バーゼル銀行委員会による「オペレーショナル・レジリエンスのための諸原則」の公表について」
金融庁（2023）「オペレーショナルレジリエンス確保に向けた基本的な考え方」
金融庁・日本銀行（2023）「バーゼル銀行監督委員会による市中協議文書『実効的な銀行監督のためのコアとなる諸原則』の改訂版の公表について」
青崎稔・園田章（2023）「国際的な関心が高まるオペレーショナル・レジリエンス」『週刊金融財政事情2023.2.21』
大和総研（2022）「ITレジリエンスの教科書」翔泳社
遠藤正之（2024）「全銀システム障害から学ぶITレジリエンス確保の要諦」『週刊金融財政事情2024.3.26』
全国銀行資金決済ネットワーク（2023.3）「次期全銀システム基本方針」
全国銀行資金決済ネットワーク（2023.10.18）「システム障害に係る対応状況について」
全国銀行資金決済ネットワーク（2023.12.1）「システム障害記者会見資料」