2112MizuhoKaizen.pdf
2021.12 ブログ：金融庁の某銀行・業務改善命令について、の詳細（）
（→ http://www.1968start.com/M/blog/index2.html#2112 ）

金融庁の某銀行・業務改善命令について

2021.12　中所武司

■本件のきっかけ

金融庁は 11/26 に、今年８回のシステム障害を起こしたみずほ銀行と持ち株会社に対し、銀行法に基づく２度目の業務改善命令を出した。

みずほ銀行については、これまで、2002 年と 2011 年の大規模システム障害などについて、教科書やブログで取り上げてきたので、下記の金融庁の業務改善命令について、調べてみた。

・みずほ銀行及びみずほフィナンシャルグループに対する行政処分について：
https://www.fsa.go.jp/news/r3/ginkou/20211126/20211126.html

■業務改善命令の内容要約とコメント（→★）

Ⅰ．みずほ銀行への業務改善命令の内容

1. 当行が策定したシステム障害に係る再発防止策の速やかな実行
2. 以下の内容についての業務改善計画の策定と速やかな実行
   ・システム障害に係る**再発防止策**
   ・システムの安定稼働等に必要となる**経営管理態勢の整備**
   ・システム障害の真因を踏まえた**業務の改善**
3. システム障害の発生原因等を踏まえた経営責任の明確化。

Ⅱ．処分の理由

1. 令和３年２月から９月の間に、顧客に影響を及ぼすシステム障害を計８回発生。
   ２月 28 日の障害：
   ・システムに高い負荷がかかる月末にデータ移行作業を実施（リスクの検討不十分）
   ・多数のＡＴＭが稼働を停止し、ＡＴＭへの通帳やカード取込みを発生
   ８月 20 日の障害：
   ・全営業部店での一定時間の店頭取引停止
   ９月 30 日の障害：
   ・復旧対応における法令遵守態勢に係る問題

2. 短期間に複数のシステム障害を発生させ、
   ・個人・法人の顧客に重大な影響を及ぼし、
   ・社会インフラの一翼を担う金融機関の役割を十分に果たせず、
   ・日本の決済システムの信頼性を損ねた

3.　今回の一連のシステム障害の直接の原因

・開発や障害対応における**品質の検証不足**

・保守・運用に係る問題点の放置、**委託先への管理不十分**
新基幹システム安定稼働のための**保守管理態勢の不備**

・**危機対応の検証（訓練や研修）不十分**

→★原因が具体的に述べられていないので、結果論だけでの判断なのか、あるいは、
個々の障害の直接的原因を特定した分析結果なのかが不明。
後者ならよいが、前者ならまともな再発防止策をとれるかが心配。

4.　このような原因（システム運営態勢を弱体化）の背景

・執行部門は、
ＩＴ現場の実態を十分に把握・理解せずに、安定稼働していると誤認し、
障害発生時も影響範囲が局所的になりやすいとの特性を過信し、
安定稼働に必要な事項（有事の被害極小化に必要な取組みを含む）を十分に洗い出さず、
新システムを開発フェーズから保守・運用フェーズへと態勢を移行させ、
保守・運用に必要な人員の配置転換や維持メンテナンス経費の削減等を推進した。

・執行責任者は、
安定稼働していると誤認して、システムリスク管理態勢の実態を把握しないまま、
人員の再配置、ベンダーからの業務の引継ぎを行った。

→★執行部門と執行責任者の責任を分けて記述しているが、
第一義的な責任は、ＣＩＯ（情報システム部門担当の役員）にある。
適任ではないＣＩＯが任命され、執行部門がその不適切な報告を鵜呑みにしたのか、
ＣＩＯが、執行部門での問題化を恐れて、意図的に虚偽の報告をしたのか、
いずれの場合も、お粗末な話。

→★ベンダーからの業務の引継ぎについて言及しているが、
3. の直接の原因でも、委託先の管理不十分としている。
金融庁の調査において、真の原因を明確にするためには、結果論ではなく、
ベンダー側のプロジェクトマネージャーたちのヒアリングを実施すべき。

→★ソフトウェア工学的観点では、
ユーザ側とベンダー側のプロジェクトマネージャー達の間で
プロジェクト管理の重要項目（＊）に関する情報共有の有無が疑われる。

（＊）本文の最後の全体的コメントに記載。

5. こうした対応が、障害の予兆管理や障害からの復旧に係る対応力といった、
IT 現場における業務対応力の脆弱化を招く一因となったものと認められる。

6. 取締役会は、
・障害分析や予兆管理の状況、障害に係る訓練の実態、
・ＩＴ人材の適正配置の状況
などの継続的な報告させるようなシステムリスク管理態勢を整備せず、
複雑なシステム等の運用管理に係る脆弱な実態を把握しておらず、
執行責任者に対し、適切な指示等を行える態勢となっていない。

→★4. の背景でのコメントとして、第一義的な責任は、ＣＩＯにある、と述べ、
「執行部門がその報告を鵜呑みにした」か、「意図的に虚偽の報告をした」かの、
いずれの場合も、お粗末な話と述べたが、取締役会には報告されていなかった。

7. みずほ銀行の経営を管理すべき持株会社に、以下のガバナンス上の問題点あり。

・業務執行を担う経営陣が、適切な資源配分を目指す構造改革を推進した結果、
コストの最適化が強調され、システムを安定稼働させるための人材の配置転換や
維持メンテナンス費用の削減が実施された

・取締役会において、構造改革に伴うシステムリスクに係る
人員削減計画と業務量の状況について、十分に審議を行っていない

・執行責任者が、高度な専門性が求められる**ＣＩＯの人選**の指針を策定していなかった。

・執行部門は、リスク委員会が、トップリスクとして選定した「大規模なシステム障害」に対して、
対応しなかった

・監査委員会が、重点監査テーマとして「IT 関連ガバナンス態勢」を設定し、
内部監査グループから改善提言無しとの報告を受けた際に、
具体的な指示を行っていない

→★持ち株会社に対しても、経営的視点で、同様の管理責任を指摘している。
特に、高度な専門性が求められるＣＩＯの人選の指針がなかったとの指摘がある。
4. の背景に関するコメントで、第一義的な責任を負うＣＩＯとして、
適任ではない者が任命された可能性に触れたが、その通りだったことになる。

8. ６月 15 日に公表されている再発防止策には、
その後、８月及び９月に発生した４回のシステム障害の発生原因の一部が含まれず、
限定的なものだった。

9. 金融庁は、ガバナンス上の問題の真因は、以下の通りであると考えている。
（１）システムに係るリスクと専門性の軽視
（２）IT 現場の実態軽視
（３）顧客影響に対する感度の欠如、営業現場の実態軽視

（４）言うべきことを言わない、言われたことだけしかしない

　これらの真因の多くは、2002 年及び 2011 年のシステム障害にも通底する問題である。
システム障害に関する過去の教訓を踏まえた取組みの継続がないという点、あるいは、
環境変化への適切な対応が図られていないものがあるという点において、
自浄作用が十分に機能しているとは認められない。

→★まったくの情けない話。

10. したがって、当行及び当社においては、
（１）システム障害に係る再発防止策
　　（システムリスク管理態勢の整備、障害発生時の顧客影響を極小化対策、
　　適切な資源配分に係る改善策を含む）
（２）システムの安定稼働等に必要となる経営管理態勢の整備に係る具体的な取組み
（３）一連のシステム障害の真因として挙げた
　　・システムに係るリスクと専門性の軽視、
　　・IT 現場の実態軽視、
　　・顧客影響に対する感度の欠如や営業現場の実態軽視、
　　・言うべきことを言わない、言われたことだけしかしない姿勢
　　といった企業風土を改め、各々の役職員が顧客影響に対する感度を高めていくなど、
　　組織的行動力を強化し、行動様式を変革していくための具体的な取組み

に係る業務改善計画を策定し、これを速やかに実行するとともに、
当該業務改善計画について継続的に再検証及び見直しを実施していく必要がある。

■ソフトウェア工学的観点でのコメント：３件

【１】全体の印象としては、この業界によくある話：

　ソフトウェアシステムを含むＩＴ技術に詳しくない最高幹部が、コスト削減のみに固守し、
それに逆らえない現場が、品質を軽視した結果ということになる。
　同様のことは、以下の 2007 年の学会講演でも指摘した。

（参考）http://www.1968start.com/M/paper/ses2007.html
「ソフトウェア工学：４０年目の現実」（基調講演），
ソフトウェアエンジニアリングシンポジウム 2007，情報処理学会（Aug. 2007）．
（海谷、山本（編）：ソフトウェアエンジニアリング最前線２００７，近代科学社）

・その言及部分：プレゼン資料の４ページ目
　http://www.1968start.com/M/paper/0708chusho.pdf
＜抜粋＞
●コスト重視の弊害：**品質よりコスト重視**
　品質を度外視したコスト削減要求が増加。

品質は見えないが、コストは見える。
テスト作業の不足。品質レビューやリスク管理の形骸化。
↓
●解決策：**品質のためのコスト重視**
コストを度外視した不良削減要求が増加。
品質は見えないが、コストはかかる。
テスト作業の充実。品質レビューやリスク管理の重点化

【２】4.で述べたプロジェクト管理の重要項目

（参考）http://www.1968start.com/M/lecture/SE3index.html
拙著「ソフトウェア工学（第３版）」（朝倉書店、2014 年）参照

＜「3.4 プロジェクト管理」から引用＞
『プロジェクト管理の知識体系ＰＭＢＯＫの１０項目の知識エリア』
- 統合管理　　：ステークホルダの期待に応えて要求を達成
- スコープ管理　　：目標達成のための作業設定と成果物の検証
- 時間管理　　：各工程の工数を見積もり，進捗を管理
- コスト管理　　：各工程のコストを見積り、実績管理
- 品質管理　　：品質評価方法を決め，適宜，評価を実施
- 人的資源管理　　：スキルを有する要員の計画を立て、その確保
- コミュニケーション管理：情報収集，配布，保管，検索実施
- リスク管理　　：納期，予算，品質のリスク予測と対応策
- 調達管理　　：外注先選定や契約内容などの外注管理
- ステークホルダ管理：利害関係のある関係者との意思疎通

【３】みずほ銀行のシステム障害に関する過去のブログ

- 2021.3　「みすほ銀行のシステム障害は単純なプログラムミス」
http://www.1968start.com/M/blog/index2.html#2103

- 2018.7　「IT 事件史（2011 年）：みずほ「悪夢」再び　震災で混乱」を読んで
http://www.1968start.com/M/blog/index.html#1807c

- 2018.6　「IT 事件史（2002 年）：みずほ銀が大規模システム障害」を読んで
http://www.1968start.com/M/blog/index.html#1806c

- 2011.4　「みずほ銀行の振込み処理トラブル」
http://www.1968start.com/M/blog/old.html#1104b

＜本ブログの抜粋：2002 年のトラブルに関する部分＞

拙著： ソフトウェア工学（**第２版**)、朝倉書店 (Mar.2004)からの抜粋
（注：2014年発行の**第３版**では、＜あとがき＞のみで言及）

＜2.5節 インタフェースの問題＞

「**2002年春に発生した某銀行オンラインシステムのトラブル**の遠因は，合併前の3銀行のシステムが独自仕様で構築されていたことである．そのため，合併後の連携処理部分でインタフェース不良が発生して大きな事故となってしまった．」

＜あとがき＞

「現在の技術では，人間はプログラムの開発時に設計ミスをするし，検査ではテスト漏れによりそのミスを見逃してしまうというヒューマンファクタの問題が残されており，ソフトウェア危機は果てしなく続くようにみえる．前世紀末の西暦2000年問題も**新世紀初頭（2002年4月）の某銀行の情報システム障害**も危機的状況を思わせるには十分であったが，ソフトウェア革命はまだ達成されてはいない．」

以上