



# システムの開発管理・リスク管理への 取組みについて

---

2007年3月23日

みずほ銀行

IT・システム統括部



## 資料概要

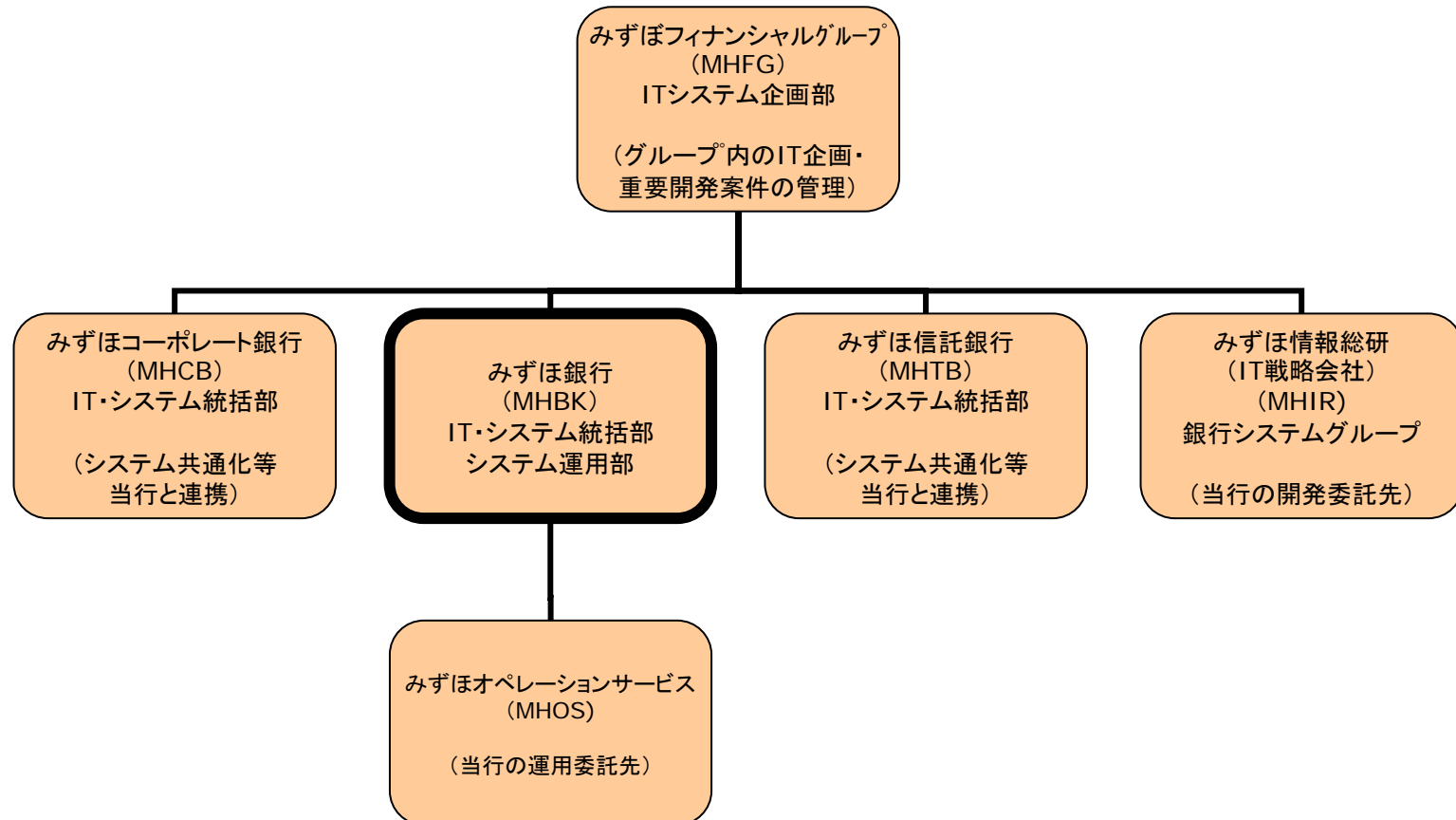
---

- I. システム開発管理への取組みについて
  - ・ 当行と当行グループの主なシステム組織の関係／  
当行のシステム組織と役割／IT戦略委員会
  - ・ システム開発の案件管理の運営方法
  - ・ 案件着手報告会／リリース協議会
  - ・ プロジェクト審査／主な審査ポイント
  
- II. システムリスク管理への取組みについて
  - ・ システムリスク管理体系／システムリスク管理室の役割  
／モニタリング・コントロール
  - ・ システム障害の管理／システム障害報告／傾向分析

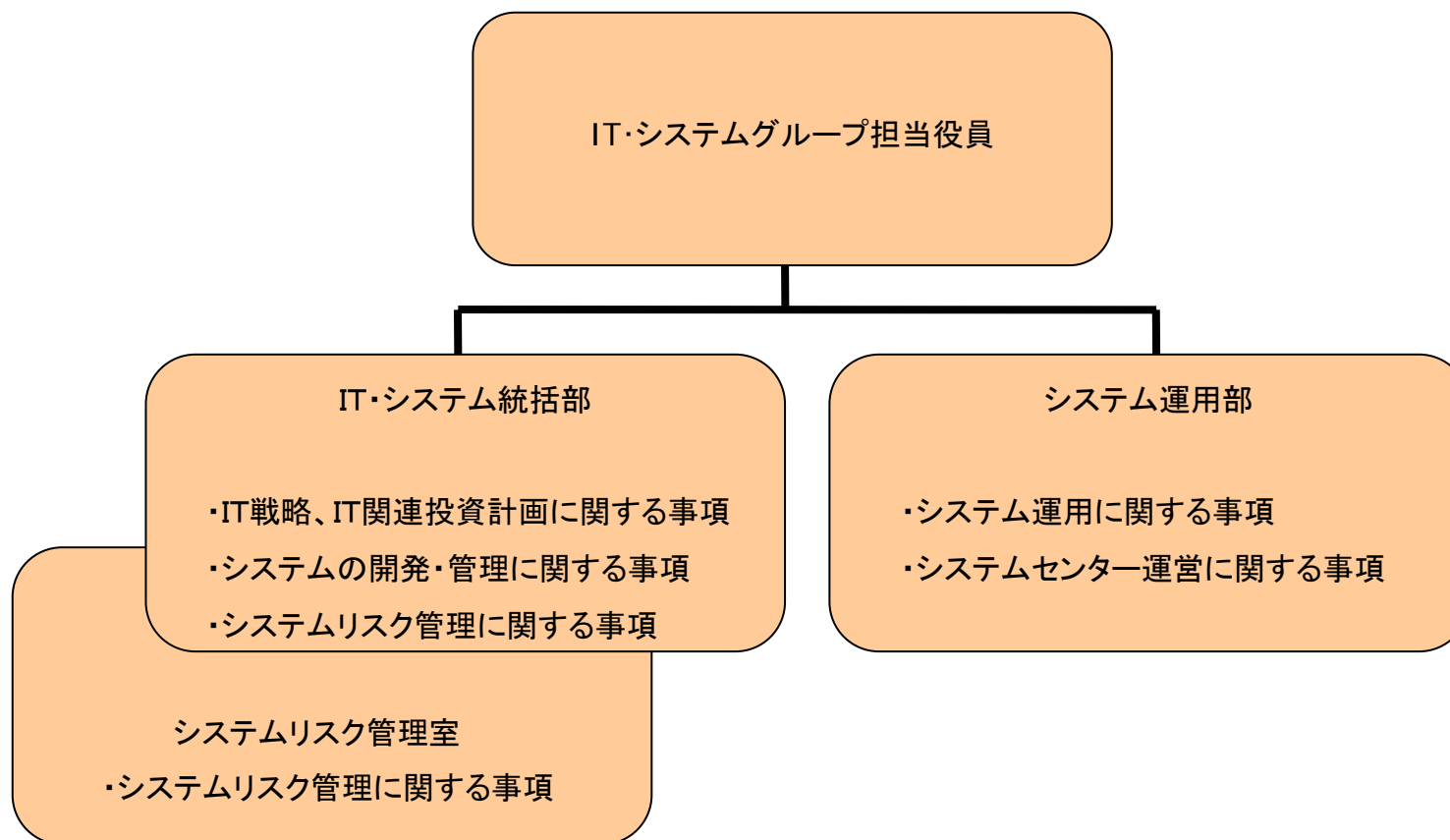
終わりに

# I. システム開発管理への取組みについて

## 当行と当行グループの主なシステム組織の関係



## 当行のシステム組織と役割





## IT戦略委員会(経営レベル)

---

### ○ 位置付け・目的

- ・ 各担当役員の担当業務を横断する全行的な諸問題について総合的に審議・調整を行う経営政策委員会のひとつ。

#### (主な審議・調整事項等)

- ・ IT戦略の基本方針・IT関連投資計画。IT関連投資計画の運営方針。IT関連投資案件にかかる投資方針、投資効果の評価。
- ・ 特定の大型プロジェクト案件の実行計画に関する事項、進捗状況の管理、及びリスク管理状況の把握、関与(リリース判定等)。
- ・ システムリスク管理に関する事項。

### ○ 構成

- 委員長: 頭取が指名する副頭取執行役員
- 副委員長: IT・システムグループ担当役員
- 委員: 企画、リスク管理、事務、財務・主計、コンプライアンス統括、内部監査部門、支店業務部門、個人、法人、プロダクト部門、人事(各グループ担当役員)
- オブザーバー: 監査役
- 事務局: IT・システム統括部、経営企画部

### ○ 開催頻度 定例開催のほか必要に応じ適宜開催 (月1回以上開催)



## システム開発の案件管理の運営方法（1／2）

---


- 経営にインパクトのある重要な開発案件について、開発プロジェクトの計画段階からリリースまでの一連の進捗の管理を行う。
  - 案件管理を行うための仕組み（ツール）として、工程管理基準・進捗管理基準、実行計画書、チェックリストを位置付ける。
  - 工程管理基準・進捗管理基準において、各工程における作業内容、成果物、関係者の役割分担等を明確化する。
  - 実行計画書において、開発プロジェクトにおけるヒト、モノ等のリソース確保、推進体制やスケジュール、管理手法等の計画の妥当性を評価するために必要な情報をまとめる。実行計画書は、要件定義・基本設計の工程で作成し、開発着手時に開発着手の権限者（経営レベル）の承認を得る。  
実行計画書に記載された進捗管理方法に基づき行い（会議録・報告書等のエビデンスを残す）、各工程の終了・次工程への進行を工程管理基準・進捗管理基準で定めた権限者（IT部門内）が承認する。
  - チェックリストにおいて、計画承認フェーズ、進捗管理フェーズ、リリース判定フェーズ毎の評価項目及びその基準を定め、確認を行う。
  - グループ全体の経営上重要な開発案件については、持株会社も含めた管理体制を構築。



## システム開発の案件管理の運営方法（2／2）

---

- 開発着手
  - 開発着手の決裁手続きを決裁権限に則り実施し、経営の承認を得る。事前に「案件着手報告会」でIT・システムグループ担当役員に報告し、「IT戦略委員会」で経営レベルの審議・調整を行う。実行計画書・チェックリスト・プロジェクト審査記録を作成する。
  - 進捗管理  
重大な実行計画の変更のある場合は変更についての決裁を得る。
- リリース判定
  - リリース決裁手続きを、決裁権限に則り実施し、経営の承認を得る。事前に「IT戦略委員会」で経営レベルの審議・調整を行う。
  - リリース決裁手続き（及び「IT戦略委員会」）に先立ち「リリース協議会」を開催し、チェックリスト、プロジェクト審査記録、テスト完了状況、リリース計画、コンティンジェンシープラン、運用引継ぎ状況、ユーザー部門準備状況、リリースを承認する際の妥当性評価、等を明記した資料を用意してIT・システムグループ担当役員に協議する。



## 案件着手報告会 リリース協議会

---

### ○ 目的

- ・ 開発着手について経営レベルの承認を得る前に、実行計画書等を用いて案件内容を報告する(案件着手報告会)。
- ・ リリースについて、リリース条件の充足状況を関係者で確認する(リリース協議会)。
- ・ 対象は、担当役員決裁以上の案件。

### ○ メンバー

- ・ IT・システム担当役員 IT・システム統括部長(副部長) システム運用部長  
システムリスク管理室 企画チーム プロジェクト総括チーム プロジェクト推進チーム 開発会社の所管部署 開発依頼部(ユーザー部)

### ○ 開催頻度

適宜 (週1回程度)





## プロジェクト審査

---

- システムリスク管理室が、実行計画書、システムテスト計画書、リリース事前協議書の審査を行い、プロジェクト審査記録書を作成する。審査は審査ポイントに沿って行う。
- プロジェクト審査記録書は案件着手報告会、リリース協議会、IT戦略委員会に提出され、報告、協議、審議・調整の材料として活用される。



## プロジェクト審査記録書

---

<b>案件名</b> (審査工程 審査実施日)	
<b>総評</b> 評価  補足説明	<b>改善指摘事項</b> 指示事項 (次工程着手の条件) 指導事項 (期限までの整備完了を要する) 追記・補記事項 (ドキュメント整備) 依頼事項その他 (今後の検討課題)
その他	審査結果 (指摘事項項目数)  フォローアップ (整備終了日、検証者)



## 主な審査ポイント(実行計画)

---

1. プロジェクトでの開発目標、案件内容が明確に定義されていること
2. 主要機能が明確に定義されていること(要件の充足、効果の妥当性、採用技術の実績、セキュリティ機能、前提条件・制約事項、実現見送り事項、ユーザー部門等関連部署との合意)
3. 開発体力(要員計画)・投資額が明確になっていること
4. システム概要が明確に定義されていること(ハード・ソフト・ネットワーク構成、信頼性、障害対策、災害対策、拡張性、代替策の検討)
5. 開発推進体制(委託先との役割分担を含む)が妥当であること
6. 移行計画が明確に定義されていること(方針・範囲・時期・方法)
7. コンティンジェンシープランに関する基本的な考え方が明確になっていること
8. スケジュールが明確になっていること(工程・イベント・全体・個別・期間の重複の影響)
9. 本番運用方針が明確になっていること
10. その他(他のグループ会社との関係が明確になっていること。EUCとの関連が明確になっていること。未確定事項が明確になっていること等)



## 主な審査ポイント(テスト計画)

---

1. 関連システム、テスト体系(分類)、テスト目的・範囲・項目が明確に定義されていること
2. 前提条件・制約事項が明確になっていること(テスト出来ない部分、しない部分についての代替方法、省略事由の妥当性、前工程(結合テスト)での品質評価の反映(結合テスト終了未済の場合の影響)、未確定事項の整理と評価)
3. テストスケジュールが明確になっていること
4. テスト環境が明確になっていること(テスト環境と本番環境の相違点)
5. テスト手法・検証方法が明確になっていること(目的に合ったテストデータ・テストケース・負荷のかけ方・テストケース洗い出し方法・テスト店属性の設定方法)
6. テスト完了基準(終了・完了条件)が明確に定義されていること
7. テスト使用ツールが明確になっていること
8. テスト実施体制・役割分担・テスト管理(進捗管理、変更管理、バージョン管理、テストデータ管理等)が明確になっていること
9. その他(他のグループ会社との共通案件についてはシステム全体計画での位置付けが明確になっていること、EUCとの関連が明確になっていること等)



## 主な審査ポイント(リリース事前協議)

---

1. リリース案件及び概要と規模が明確になっていること
2. リリースの目的・効果が明確になっていること
3. 前提条件・制約事項が明確になっていること
4. テスト内容(結果)の整理と評価がされていること
5. 懸案事項が明確になっていること
6. テスト期間中の障害発生状況と対応状況が妥当・適切であること
7. リリース準備状況
8. 切替・移行作業が明確になっていること
9. コンティンジェンシープランの内容が明確・妥当であること
10. データの保管状況
11. 他のグループ会社との関連が明確になっていること
12. EUCとの関連が明確になっていること
13. その他



## Ⅱ. システムリスク管理への取組みについて システムリスク管理体系

---

- ・ システムリスク管理の基本方針
- ・ 情報セキュリティポリシー
  
- ・ システムリスク管理の基本方針細則
- ・ システム案件管理基準
- ・ システム障害報告基準
- ・ オフサイトバックアップシステムの切替・切戻し共通基準
  
- ・ グループ会社システムリスク管理運営要領
- ・ システム案件管理運営要領
- ・ 外部委託管理要領
- ・ システムリスク評価運営要領
- ・ 情報セキュリティスタンダード
- ・ 情報セキュリティスタンダード付属書(ITセキュリティ管理編)
  
- ・ 諸手続(プロシジャー)



## システムリスク管理室の役割

---

- システムリスク管理に関する諸規程、基準、運営要領等の制定、改廃
  - ・システムリスク管理の基本方針、システムリスク管理の基本方針細則、
    - \* 情報セキュリティポリシー、\* 情報セキュリティスタンダード、  
情報セキュリティスタンダード・ITセキュリティ管理編、システム障害報告基準、  
システムリスク評価運営要領、外部委託管理要領  
( \* 印 コンプライアンス統括部情報管理室)
  
- 開発案件などの審査の実施
  - ・プロジェクト審査、システムリスク審査、新規業務・新商品の審査、  
個別運用ルールの審査 等
  
- システムリスク評価の実施と報告
  - ・重要度評価、システムリスク評価報告
  
- システム障害管理の実施と報告
  - ・システム障害の管理、発生状況の定例報告、障害傾向分析
  
- オペレーショナルリスク管理、報告
  
- 行内教育
  - ・支店長・副支店長・営業課長研修、本部次長研修 等



## モニタリング／コントロール

---

### ○本番稼働中のシステム

- システムインベントリーへの登録、定期的な見直し(年2回)
- システムの重要度評価の実施(年1回、随時)
- システムリスク評価の実施(モニタリング)(年1回、随時)
- リスクに対する対策(コントロール)の実施

### ○開発途上のシステム

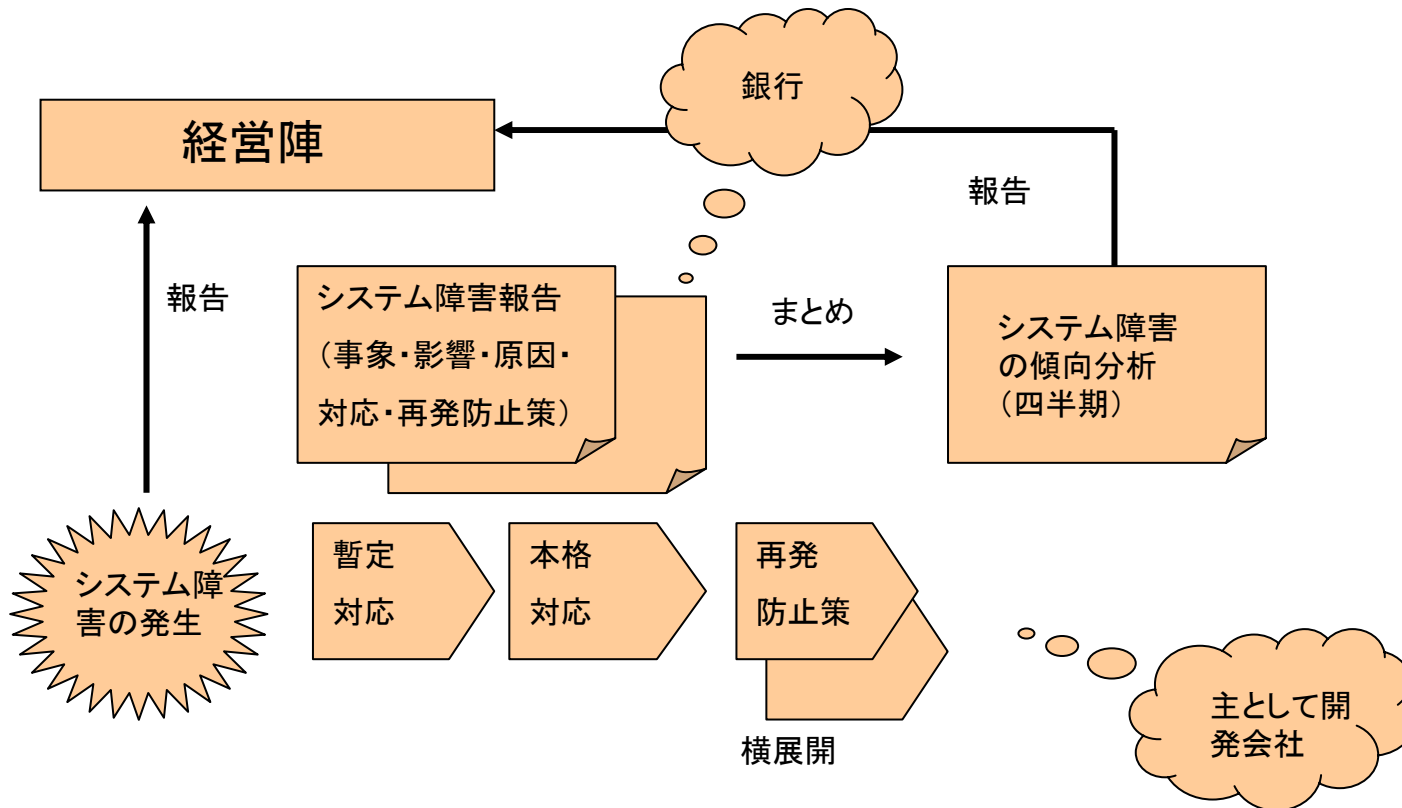
- プロジェクトリスクの管理(随時)

### ○システム障害発生への対応

- システム障害への対処(暫定対応・本格対応)
- システム障害報告(記録・分析)
- 再発防止策の策定と実施(横展開)



## システム障害の管理について





## システム障害報告（1／5）

---

標題（件名、システム名）	起票部署印、確認印、承認印
日時	原因
事象	本格対応
影響	再発防止策
暫定対応	オペリスク

## システム障害報告（2／5）

### ○ 標題

- ・ 発生した障害の内容、特徴を件名として簡潔に記入する
- ・ システム障害が発生したシステム名、(システム番号)、業務名を記入
- ・ オンラインか、オフラインか、本番障害かテスト・机上発見か
- ・ 影響の大きさに応じて障害ランクを記入

原因システムと異なる場合がある

机上発見に努める

### ○ 日時

- ・ 障害が発生(検知)した(西暦)年月日(曜日)、時刻(24時間表記の時・分)
- ・ 暫定対応等によりシステム(又は業務)が復旧した(西暦)年月日(曜日)、時刻(24時間表記の時・分)
- ・ 障害発生から復旧に要した時間(24時間表記の時・分)

短縮化する工夫

### ○ 事象

- ・ 障害事象の内容を具体的にわかりやすく記入
- ・ 発見経緯を記入
- ・ システムダウンか、誤作動か、不正利用か

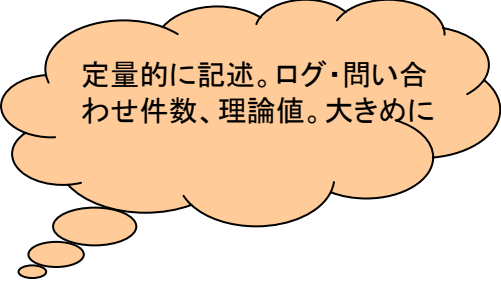
極力わかりやすい言葉で

## システム障害報告（3／5）

---

### ○ 影響

- ・ 影響範囲〔行外・顧客（お客さま）、行内、IT部門内〕を選択する
- ・ 情報漏えいの有無
- ・ 影響内容、影響を与えた時間等を具体的かつ定量的に記入
- ・ ユーザー部署の窓口担当者、連絡先
- ・ 影響規模〔顧客（お客さま）数、取引件数、取引金額、部店数、口座数等〕を数字で記入



定量的に記述。ログ・問い合わせ件数、理論値。大きめに

### ○ 暫定対応

- ・ システムの復旧及び業務の復旧・継続のために行ったシステム上の対応（緊急修正、再処理、追加処理など）を具体的に記入（システム対応）
- ・ 業務の復旧・継続のために行った業務上の対応を具体的に記入（業務対応）

## システム障害報告（4／5）

初期障害か、潜在障害か

### ○ 原因

- ・ システム障害の原因となったシステム名、プログラム番号、プログラム名等を記入する
- ・ 当該プログラムの障害を起こしたバージョンの登録日を記入
- ・ プログラム中の障害を起こしたロジックがリリースされてから障害が顕在化（又は発見）されるまでの期間を月数で記入（潜在期間）
- ・ 障害を引き起こした原因を分類する（ハード、ネットワーク、メーカーソフト、自行開発ソフト、開発側作業ミス、運用ミス、外部要因等）
- ・ 自行開発ソフトウェア障害、開発側作業ミス、運用ミスの場合、直接の原因、直接原因を誘発させた間接原因、直接原因・間接原因を誘発させた真の原因を特定し、内容を記述する
- ・ 直接・間接・真の原因を仕込んだ工程、発見すべき工程を特定する

分析

## システム障害報告（5／5）

### ○ 本格対応

- ・ 本格対応の内容を具体的にわかりやすく記述する
- ・ プログラム対応予定本数、対応日を記入する

妥当性の検証

### ○ 再発防止策

- ・ 直接原因、間接原因、真の原因排除のための今後の仕組みとして開発工程や運用手順、ユーザー教育・ルール等にかリキュラムとして組み込むものの内容とその実現方法、計画について具体的に記述する。今後の同原因の障害を防止するため、開発工程、運用、操作手順等に組み込むべき具体的な仕組みを記述する
- ・ 再発防止策を実施する予定日を記入する(システムリスク管理室が適宜トレースする)

横展開による類似障害の未然防止

ルール化、チェックリストに追加、実行の確認、審査ポイントへの追加、総括

### ○ オペリスクデータ

- ・ 当該障害の対応コスト(みなし計算)、(発生した場合のみ)実損額、(該当があれば)回収金額を記入する



## システム障害の傾向分析（1／6）

---

- 総件数
- 目標件数
- ランク別
- 業務分野別
- 原因区分別
- 初期障害率
- 特記事項（新たな傾向・現象を早めに把握して対応）



## システム障害の傾向分析（2／6）

総件数 目標件数

---

### ○ 総件数

- ・ ハード障害
- ・ ネットワーク障害
- ・ 机上発見
- ・ メーカーソフト障害
- ・ 自行開発ソフト障害
- ・ 開発側作業ミス
- ・ 運用ミス
- ・ 外部障害

### ○ 目標件数

- ・ 品質管理上の目標値を設定（月次・半期）  
（リスク管理上の評価基準）
- ・ 自行開発ソフト障害、開発側作業ミス、運用ミス、メーカーソフト障害  
（OS・PP等を除く）を対象
- ・ 目標達成状況につき経営報告（定期、 随時）
  - － 目標未達の場合は対策の実施と対策の妥当性評価を実施





## システム障害の傾向分析（3／6）

### ランク別 業務分野別


---

#### ○ ランク別（影響の大きさ）

- ・ 行外・顧客（お客さま）
- ・ 行内
- ・ IT部門内

#### ○ 業務分野別（原因システム）

- ・ 勘定系
- ・ 対外接続系
- ・ 情報系
- ・ 証券・市場系



## システム障害の傾向分析（4／6） 原因区分別（1/2）

---

（行内）

- ハード障害
- ネットワーク障害
- メーカーソフト障害
- 自行開発ソフト障害
- 開発側作業ミス
- 運用ミス

（行外）（外部障害）

- ハード障害、ネットワーク障害、ソフト障害、社会インフラ停止（停電など）、災害、セキュリティ突破、運用ミス、原因不明



## システム障害の傾向分析 (5/6)

### 原因区分別 (2/2)

---

#### ○ 自行開発ソフト障害

- ・ 直接原因 (要件定義ミス、基本設計ミス、詳細設計ミス、プログラムミス、設定ミス、作業ミス、JCLミス、等)
- ・ 間接原因 (ドキュメント不備、影響調査不足、思い込み、失念・不注意、レビュー不備、テスト不備、等)
- ・ 真の原因 (ルール未整備・不備、スキル不足、コミュニケーション不足、等)
- ・ 作込工程 (要件定義、基本設計、詳細設計、プログラム作成、運用マニュアル作成、移行・本番作業 等)



## システム障害の傾向分析（6／6） 初期障害率

---

- 自行開発ソフト障害を対象
- リリース後の初期障害か潜在障害か
- 初期障害率の分母
  - 投入量（工数）
  - 開発量（リリース本数）



おわりに

---