

システム障害の予防策立案のための リスクの捉え方 —運用と開発 未知との遭遇—

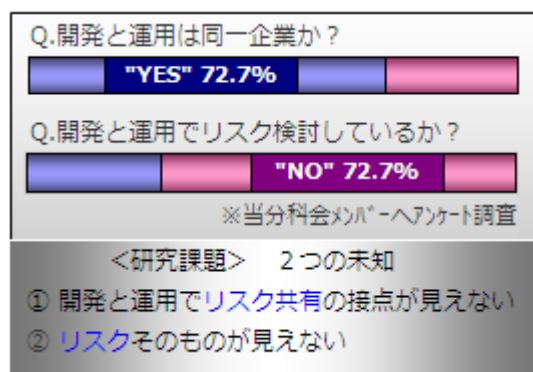
アブストラクト

1. なぜシステム障害は防げないのか？

深夜3時30分。突如、寝室に携帯電話の着信音が鳴り響く・・・システム障害を告げる恐怖の着信音・・・。

システム開発から運用までの各局面で発生するシステム障害により、開発者と運用者の深夜の着信が鳴り止むことはない。その根本原因について、我々はある仮説を立てた。それは、開発と運用を主とした様々なステークホルダが抱えるリスクの共有ができていないからではないかというものである。図表1の調査結果は開発部署と運用部署が同じ屋根の下にいるにも関わらず、双方の把握したリスクが共有されていない可能性が相当程度あることを示唆させる結果となった。

図表1 開発／運用部門のリスク共有調査



2. システム障害が引き起こすリスクとは？（リスクへのアプローチ）

当分科会ではシステム障害を未然に防ぎたいという切なる願いのもと、業種が異なる開発者7名、運用者8名の総勢15名が一同に介した。方向性や研究範囲の分からない暗闇の中、各々が抱えるリスクという漠然とした何かを捉える為、その手段を模索した。リスク特定のアプローチは次のとおりである。

- (1) **問題点の洗い出し**：開発者と運用者が別々の観点からリスクについて検討することで不明瞭となっているリスクの定義や適用範囲、ターゲットを明確にする。
- (2) **リスクの可視化**：リスクアセスメント手法を確立する為、開発情報、運用情報から各工程で潜在するシステム固有のリスクを洗い出し、評価するまでのプロセスを定義する。
- (3) **診断ツール開発**：評価プロセスを踏襲したリスク診断ツールを開発する。ガイドに沿って設問に回答することで、システムのどこにリスクが潜んでいるか、視覚的に捉えることを可能とする。
- (4) **リスクアセスメントの実践**：リスクアセスメント手法の有用性を検証するためにリスク診断ツールを実際の現場に適用する。検証結果を分析し、手法とツールの改善することで評価精度を高める。

図表2 リスクの定義と評価プロセス



3. システム障害を撲滅する為に・・・

当分科会で研究したリスクアセスメント手法の独自性として、以下の3点が挙げられる。

I. リスクレベルの特定と予防策立案

開発情報と運用情報から各フェーズのリスク要因をカテゴライズする。次に発生確率、影響度、重要度、難易度の観点からリスクレベルを特定し、障害予防策の立案と実現性の検討を行う。

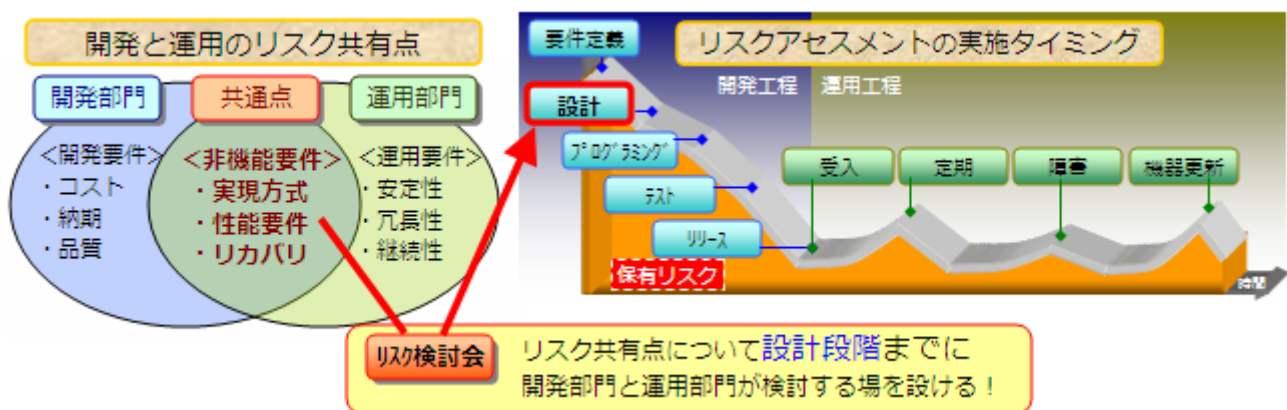
II. タイムリーなリスクの抽出と管理

リスク評価の実施タイミングを開発工程は各フェーズ、運用工程は各イベントと定め、保有リスクを可視化することで開発から運用まで一貫したリスク管理を行う。

III. 開発部門と運用部門のリスク共有

運用者の観点で捉えたリスクを開発工程で開発部門と運用部門が合同で検討することで、共通点のリスクヘッジを行う。開発フェーズで対応しきれない残存リスクは受入時に運用フェーズへ引き継ぐ体制をつくり、継続してリスク管理を行う。

図表3 リスクの共有と管理



4. 研究成果の有用性評価

リスクアセスメント手法の有用性について、実在するプロジェクトでリスク診断ツールを活用してリスク診断を行った。判定結果について、整合性、実用性、妥当性の観点から検証した。(図表4参照)

図表4 リスク診断ツールの検証結果 (アンケート結果のまとめ)

- ①リスク判定結果と過去の障害事例データとの整合性 △改善の余地あり
⇒過去の障害事例データが示すハイリスク要因をリスク判定結果に反映させる為、更なるデータ収集が必要
 - ②リスク判定結果と予防策の実用性 ◎良好
⇒リスクに対して発生し得る障害が予測されており、現実的かつ実用的な予防策立案になっている
 - ③リスク要因の優先順位の妥当性 ○兼ね良好
⇒リスクカテゴリ別に優先度の高いリスクをキャッチアップするように改善し、重要なリスクが認識しやすくなった
- ※アンケート対象業種 金融(クレジット)/損保/流通/製造関係(計8社)

5. 障害を未然に防止する為の提言

当分科会で研究したリスクアセスメント手法は、リスクを的確に捉えて、効果的な予防策立案の方法を提示した。この成果が障害撲滅への第1歩となることを確信している。当分科会の研究成果を貴社のリスクマネジメントにご活用頂き、最適なリスク対策を講じることで、開発者、運用者、経営者、全ての関係者に静寂な夜を送って頂きたい。

＜障害防止のための3つの提言＞

- ①システム評価者は、開発と運用のシステム情報をあらかじめ定義し、データ管理を継続すること
- ②開発/運用部門は、優先度が低くなりがちな非機能要件について、開発工程でリスク評価を行うこと
- ③経営層は、リスクに対する予防策の費用対効果を検討し、予防策の対応可否を決断すること