2.4 障害発生時連絡の情報共有に関する教訓（G4）

教訓 G4　運用者は少しでも気になった事象は放置せず共有し、とことん追求すべし

問題

A社のシステムが数時間停止し、また対応が遅れたため、公表も遅れた。

同社のオンラインサービスを提供するシステムは現用・待機ノードによる二重化冗長構成を採っており、現用ノードが故障すると、自動的に待機ノードに切り替わる仕組みとなっていた。また、同システムの運用は子会社に委託され、運用子会社の担当者はシステムの異常を検出すると診断メッセージを出力して保守ベンダに解析を依頼し、その解析結果を本社の運用部門に伝え、本社運用部門では重大な状況の場合にのみ経営層（CIO）に報告する手順となっており、このような運用手順がマニュアルに記載されていた。

ある日の夜間バッチ処理中に1台の現用ノードでメモリコントローラの障害が発生し、監視端末にエラーを示すメッセージが表示された。

運用子会社の担当者は「障害診断ツール」を使い、診断レポートを出力し、保守ベンダのSEに対し、電話と電子メールで診断レポートの内容を報告した（図2.4－1①）。

保守ベンダのSEは診断レポートの内容を見て、待機ノードが正常に稼働していると判断し、運用子会社の責任者に切替え処理が成功しているとの見解を伝えた（図2.4－1②）。

運用部門の統括責任者は「当日の業務への影響はない」と判断し、処理が切り替わっていると誤認したまま障害対応を完了し、経営陣への報告を行わなかった（図2.4－1③）。

運用部門が経営陣（CIO）へ報告すべきだと判断したのは、翌日未明の業務で一部の情報が配信できないことが判明してからだった。CIOに連絡が取れたのは翌日朝で、午前中のオンラインサービスは停止となった（図2.4－1④）。

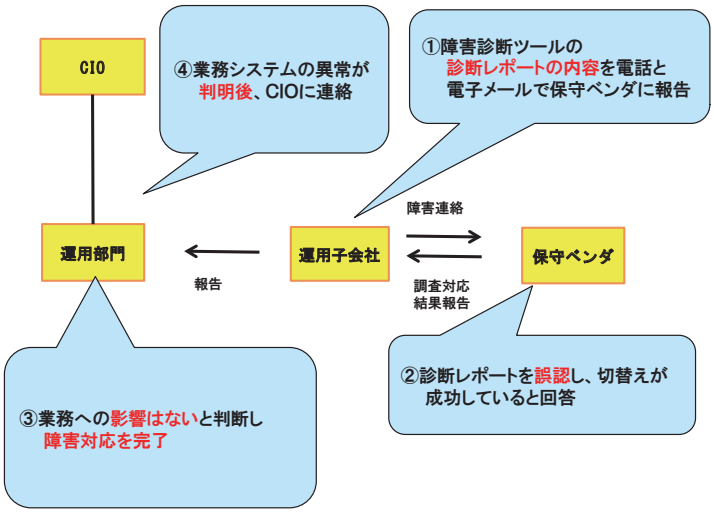

図2.4－1　障害の経緯

原因

今回の問題の直接の原因はメモリコントローラの障害が発生したことである。

これに続いて、以下のヒューマンエラーによるミスが発生した。

① 保守ベンダの SE が診断レポートを誤認した。

実際には、待機ノードが処理を引き取って継続するには、現用ノードが処理不能だと表明し、“バトン”が渡される必要があった。運用子会社の担当者は診断レポートの内容から「現用ノードは死にかけているが、待機ノードにバトンが渡っていない」らしき状況に気づいていたが、保守ベンダの SE にそのことを連絡せず、保守ベンダの SE は現用ノードからバトンが渡っていると誤認し運用子会社の責任者に報告した。

② 運用部門が主体的にシステムの状態を確認せず、運用子会社からの報告で問題なしと判断した。

③ 運用部門が経営陣に適切な報告を怠り、業務の対応の遅れにつながった。

さらに調べると、ミスが発生した根本原因は以下であることがわかった。

④ 運用子会社の担当者と保守ベンダの SE は、マニュアル通りに作業したが、それに加えて運用子会社の担当者は、現場での異常を察知したときには、その情報を保守ベンダの SE や運用子会社の責任者に伝達した上で協議すべきであった。

運用子会社には、オペレーションしている人も疑問に思ったら相談するという「顧客視点」でシステムを捉える考え方が欠けていた。

対策

A 社は障害発生時の緊急態勢・運用手順を以下のように整備し再発防止策とした。

最も重視した再発防止策は、

①「運用担当者が現場での異常を察知したときには、状況判断できる運用部門の社員にその情報を連絡して協議する態勢を作る」ことをオペレーションマニュアルに明記する。

ということである。

あわせて以下のような再発防止策も実施した。

② 障害対応を体制面で改善して強化する。

- 事象として障害と断定できない場合でも障害の可能性がある場合は、早期に上位役職者へ報告するルールを追加作成する。
- 状況判断できる運用部門の社員（プロパ）がセンターへ 24 時間常駐する。

③ 確認手順及び確認項目を明確に定義する。

- 速やかな復旧に向けた取り組みに変える。
- 装置の停止有無（コンソールメッセージの伝達方法の改善）、業務影響、障害リスクを明確に定義する。
- 障害対応の確認項目を明確に定義する。
- 障害対応時アクションリストに項目を追加する。
- エスカレーション管理台帳を整備する。

- 保守ベンダの連絡ルールを改善する。

④ ハードウェアのハングアップなどで二重化の切替えが不確定な場合には、疑わしき要素を切り離す仕組みを順次取り込む。（フェールソフト）

⑤ 必要な教育及び訓練を実施する。

効果

今回の対応後にも障害が発生しているが、報告ルールの整備などの再発防止策により、利用者に影響を及ぼす重大障害につながらずに対応できている。

教訓

運用現場ではあらかじめ想定できないようなことが起こるので、運用担当者が現場での異常を察知したときには、状況判断できる運用部門の社員にその情報を連絡して協議するような仕組みを考えておくべきである。