金融高度化セミナー「システムリスク管理の現状と課題」における質疑応答の模様

（問）システムリスク管理におけるセキュリティ・ポリシーの見直しはどの程度のサイクルで行っているか教えて欲しい。また、今般改訂された金融検査マニュアルの内容を踏まえた見直しは行っているか？

（横浜銀行）セキュリティ・ポリシーの見直し頻度は特に規程化していない。新検査マニュアルへの対応としては、セキュリティ・ポリシーの下部規程には手を入れる必要があると認識しており、現在内容を検討中である。

（みずほ銀行）当行では、上位の規程であるシステムリスク管理の基本方針について、原則年１回の見直しを定めている。新検査マニュアルへの対応については、基本方針レベルの変更を検討しており、本年４月に反映する予定。

（問）近年、金融機関におけるコンピュータ・システムの管理や運用では、外部委託のウエイトが高まっているが、外部委託を行う場合にリスク管理面で注意すべき点は何か？

（日本銀行）外部委託には、全面委託や部分委託など様々な形態があるが、リスク管理上のポイントは２点あると思う。まず、委託先との間で「何を委託しているのか」の確認をしっかりと行い、システム管理・運用面での「役割」と「責任」の分担を明確化することである。もう一点は、その役割分担のもとで、委託先が予め定められた内容のサービスを適切に提供しているかどうかを、自らが事後的に検証できる手段、例えば、定期報告、立ち入り調査等を用意しておくことである。

（横浜銀行）当行でも外部委託を相当活用しているが、開発、運用、保守の各段階において、サービス仕様書等でお互いの役割と責任を明確化し、定期的な報告を求めながら、必要に応じて委託先の仕事振りを検証している。

（みずほ銀行）従来に比べると、委託先の管理は難しくなっているというのが実感。システムの開発・運用の委託だけでなく、行内のユーザー部署における業務の委託も増加しており、システム障害の内容も最近複雑化、多様化している。リスク管理部署としては、まずはリスクの所在を明らかにし、そのうえで委託先の効果的な管理手法を検討することになると思う。

（問）横浜銀行では、システムのリスク評価（CSA）を年１回実施しているとの

説明があったが、どの程度の陣容で行われているのか？

（横浜銀行）CSA は、IT 統括部・管理グループのスタッフ４名で行っている。ただし、評価対象は、自行構築システムのうちシステム・情報面で重要度が高いと判断されるものとしており、当行の全てのシステムを対象としているわけではない。それでも評価対象は相当数になるので、２年前の最初の CSA 実施には２か月程度の時間を要した。

（問）システム障害を未然に防止するポイントは何か？

（横浜銀行）システムの開発、運用、保守には、外部委託先、ユーザー部署を含めて、様々な人たちが関与している。システム障害のリスクはその間隙をぬって顕現化するものである。お互いのコミュニケーションを適切にとり、リスクの所在や対処方法を共有することが重要だろう。

（みずほ銀行）システムの開発段階で「不具合を作り込まない」ことが大切だと思う。加えて、立ち会い体制や相互検証によるダブル・チェックを強化するなどシステム開発管理面での工夫を通じて、システムの不具合を早期に検知することにより、障害発生を未然に防止できるケースもある。顧客取引や決済システムへの影響を極力回避する努力が必要。

（日本銀行）システム障害をゼロにすることはできない。やや逆説的になるが、システム障害が起こり得ることを前提に体制を整える必要がある。万が一障害が発生した場合には、その原因をよく分析し、二度と同じ障害を発生させないことが重要。システム障害には様々な情報が隠されている。「障害から学ぶ」という姿勢も大事ではないかと思う。

以　上