第９９回月例研究会報告

№561　日高祐子

開催:2003 年 9 月 30 日(火)
場所:中央大学　駿河台記念会館　520 会議室
講師:金融庁検査局　総務課　特別検査官　市川雅也氏
テーマ:「システムリスク検査
--金融機関等における多様化する情報システムリスクへの対応について--」

当日、受付前には長蛇の列ができ、また会場内は三人掛けテーブルに三人が着席してもまだ収容できず、遅くに到着された方は椅子を持ち込んでの参加となる盛況振りであった。昨今の状況において、システム監査を考える場合の、当講義テーマと講師への関心の高さが窺えた。

講義要旨

１.金融庁について

金融庁の任務は、金融機関の安全を確保し、預金者・保険契約者・有価証券投資者の保護と金融の円滑を図ることである。この任務遂行の為、金融庁「監督局」は金融機関に説明を求め行政処分等を行う。また、同「検査局」は金融機関に出向き検査を実施する。

２.事務ガイドラインと銀行法

金融庁ホームページには、「事務ガイドライン」が掲載されており、かなりの頻度で改訂がなされている。当ガイドライン「経営姿勢」の項目では、システムに関わるリスクを経営陣が如何に認識しているかを問い、この認識が充分でないと基本方針が具体化されないと考えられている。また同「経営管理」の項目では、顧客に関する情報管理について、これが適切に行われていることを《検証できる体制》があることが求められており、顧客情報の漏洩が行われていないことを《証明できるかどうか》という観点で、検査がなされる。しかしながら、検査局による立入検査は「健康診断と捉え、健康体であっても更に病気がないかを検証し、悪いところがあれば是正するというスタンスで望んで欲しい。」と力説された。

３.金融検査マニュアルとシステムリスクの定義

「金融検査マニュアル」では、リスクを信用リスク・市場性リスク・流動性リスク・事務リスク及び　システムリスクの５種類に分類し、認識している。システムリスクとは、コンピュータシステムのダウン等により、顧客等に損失が発生するリスクであるが、昨今システムリスクへの対応は多様化を極めている。

４.システムリスク管理態勢の確認検査項目

数々のシステムリスク管理態勢の確認検査項目の内、特に当講義において強調された部分は、

・経営陣のリスク管理への関与、すなわち「コンピュータ関連は IT 部門に任せている。」という状態ではなく、「システムリスク管理の基本方針」等が経営のレベルで討議されているか?

・セキュリティスタンダード等の評価基準が存在し、且つ日々改訂されているか?

であり、また外部委託管理については、「事務ガイドライン」の平成 15 年 6 月末改訂において「章」への格上げがなされているとのことである。

５.システム統合リスクについて

経営陣がシステムの専門家であることは稀であるが、システム統合が何故必要なのかを理解でき、「システム統合が順調に進んでいるか？」を経営陣が判断できる基準がなければならない。往々にしてセキリティレベルの低いところからリスクは発生するが、例えば、各工程完了の承認ルールにおいて差異がある場合、品質にばらつきが生じることとなる。業務要件の確定から工程の承認ルールの統合等、経営陣が必要であることを認識すべき項目は多々ある。また、不測事態への対応としては、統合計画に比して遅延した場合等の見直し基準、発動権限者及び発動基準、システム統合の中止・延期に関わる判断基準の存在が経営陣の判断のために必要である。

大切なことは、顧客の目でリスクが考えられており、顧客に対してきちんとした対応ができることである。最後に、システム統合時においては、内部監査体制を整備することは非常に難しく第三者機関による評価、すなわち外部監査がミニマムスタンダードとされていることを付加された。

以上