特定領域研究「日本の技術革新－経験蓄積と知識基盤化－」第 2 回国際シンポジウム研究論文発表会　論文集
平成 18 年 12 月 16 日

E－2

情報システムの発展とシステム監査の乖離リスク
－情報システム運用の多様化に伴う脆弱性の増加－

Development of information systems and misfit risk in systems auditing -Emerging vulnerabilities along with diversification of information systems operation-

渡辺　研司[1]・堤　啓太[2]・山崎　光子[2]
WATANABE Kenji[1]・TSUTSUMI Keita[2]・YAMAZAKI Mitsuko[2]
[1]長岡技術科学大学　工博・[2]長岡技術科学大学
[1]Nagaoka University of Technology, Dr. Eng・[2] Nagaoka University of Technology

ネットワーク型社会・経済・情報システムリスク・事業継続マネジメント
Networked Society & Economy・Information Systems Risk・Business Continuity Management

１．はじめに

現代における社会経済は、情報技術の発展とその採用によって、ネットワーク型社会へと変化してきた。そして今では、企業間でデータをやり取りすることによって、商品取引プロセスをリアルタイムで完了させたり、サプライチェーンで情報を共有することで全体最適化を図ったりというようなことが日常的に行われるようになっている。しかしその一方で、ひとつの企業で発生したシステム障害が、ネットワークでつながっている他の企業やサプライチェーン全体に伝播し、特定の場所で起きたはずの障害が広い地域に時間さえもまたがって影響を及ぼしてしまうというような事故･事件が散見されるようになった。このような状況においては、情報システムに対してそういった障害のリスク対策を行い、その対策が確実に行われているかどうかを評価する必要がある。しかし、情報システム評価としてよく用いられている制度であるシステム監査では、一箇所の障害が広域に影響を及ぼすという観点は未だ採用されておらず、未だシステム障害は連日発生している現状にある。そこで本研究では、システム監査の変遷を、それを取り巻く技術革新という観点から整理し、システム監査と社会で採用されている情報技術の間の現状における乖離について、考察を展開することを目的とする。

２．システム監査の変遷

システム監査は、経済産業省によって定められたシステム監査基準および、システム管理基準などの基準を用いて行われる活動である。表 1 にシステム監査基準の変遷を示した。システム監査基準は、2006 年 10 月現在までに二回の改訂が行われている。最初および第一回改訂までのシステム監査基準では、その目的は「情報システムの安全性、信頼性、効率性の確保」となっており、当時はまだ低かった情報システムの安全性･信頼性･効率性を確保するための基準であった。その後第二回目の改訂によって、その目的は「組織体の情報システムにまつわるリスクに対するコントロールが適切に整備・運用されているかを評価し、IT ガバナンスの実現に寄与する」ことに変更された。こうした一連の改訂とその目的の変更の背景には、次項において述べるいくつかの情報システムにまつわる障害事例が大きく関連している。

表１　システム監査基準の変遷[1)]

1951年7月	企業における内部統制の大綱
1953年2月	内部統制の実施に関する手続き要領
1980年3月	日本情報処理開発協会がシステム監査基準(試案)公表
1983年12月	産業構造審議会情報産業部会中間答申でシステム監査基準の策定を提言
1985年1月	システム監査基準策定
1996年1月	システム監査基準第一回改訂
2004年10月	システム監査基準第二回改訂、システム管理基準公表

３．技術発展とシステム障害

システム監査基準は、これまでに二度の改訂が行われているが、その背景には、情報技術の発展・普及とそれに伴って発生したシステム障害が大きく関わっている。１９８５年に策定されたシステム監査基準は、企業内での電算機の利用範囲拡大により、信頼性に関する問題が数多く浮上したためである。当時のメディア[2)]によれば、コンピュータを使ったシステムの故障は２０日に一度は起きていたとされており、広がる電算機利用に対して信頼性を高めることが急務となっていた。１９９６年に行われた第一回目の改訂は、情報環境変化への対応、国際化への対応、災害対策への対応といった点が新たに追加された。これらは、ネットワーク技術の発展とその情報システムへの利用が広がったことが技術的背景にある。さらに、１９９５年1月に発生した阪神大震災によって企業の情報システムが打撃を受けたことが改訂に大きな影響を与えたと推測される。第二回目の改訂は２００４年に行われ、IT ガバナンスという観点からの変更と、技術革新に伴う新たなリスクへの対応のための管理項目が加えられた。改訂時、企業は情報システムを経営戦略の要として位置づけており、情報技術は企業が存続する上で必須のものとなるほどに発展していたといえる。この改訂は、以前の監査基準と比べると大きな変更が加えられたが、それは情報システムの位置づけの変化を踏まえて行われたものだと考えられるが、ここにおいても改訂の前にシステム障害が発生している。その中でも重要なのは、いわゆる２０００年問題および、２００２年のみずほ銀行大規模システム障害である。２０００年問題は、情報システムを構築する際に、先を見越した設計を行わなければならないという教訓を残した。みずほ銀行のシステム障害は、自社の情報システムについて経営者がしっかりと把握し、コントロールしなければならないということを社会に伝えた。この二つの事例は、組織内の IT ガバナンスを実現し、リスクコントロールに努めなければシステム障害が発生するということを示している。第二回目の改訂においても、過去の問題点を内容に反映しているといえる。

これらのことから、システム監査基準改訂の背景には、システム障害と技術発展が密接に関わっているといえよう。

４．現在のシステム監査の問題点

２００４年にシステム監査は改訂されたが、依然としてシステム障害は発生し続けている。社会に大きな影響を与えた事件として、２００５年１１月に発生した東京証券取引所(以下東証)のシステム障害が挙げられる。これはシステム監査を行っているにも関わらず、障害発生を未然に防止することができなかった事件である。障害の主な原因はソフトウェアのバグだが、その背後にはベンダーへの過度な依存という構造的問題が隠れている。システム監査の基準には委託の項目があり、アウトソーシングの実施についても監査が行われるが、このような構造的な問題を監査で解決することは難しい。通常、システム監査の基準は、確認作業として行われることが多く、今回のケースのような構造的問題にアプローチすることはできない。そのため、現在のシステム監査によるリスクコントロールだけでは、情報システムリスクへの対応は不十分であるといえる。

５．積極的な情報システムリスクマネジメントの必要性

システム監査は、あくまでも自社のシステムが最低限の基準を満たしているかをチェックするための補完的要素、あるいは外部への保証として使われるべきであり、監査の基準を満たすだけで満足してはならない。各企業はシステム監査に加え、自発的に MOT(Management of technology)の一環としての情報システムリスクマネジメントに取り組む必要がある。情報システムは企業活動の根底を支える重要な要素となっているため、リスク対策は事業継続に不可欠である。

６．おわりに

企業は新しい技術を積極的に取り入れることによって、自らを発展させてきた。しかしその発展に伴うリスクへの対応はシステム監査だけでは追いつかず、企業としての社会的責任が果たせない状況にある。企業は、システム監査のみならず、自発的に MOT としての情報システムリスクマネジメントに取り組み、事業継続に勤めなければならない。

注

１）吉田洋、「システム監査機銃の変遷と今後の課題」 『経営総合科学』Vol.85（2005 年 9 月）pp.21-34, 愛知大学経営総合科学研究所
２）朝日新聞 1985 年 1 月 25 日朝刊, 朝日新聞社