システム監査法制化の現状と今後の方策

システム監査法制化研究会
主査　　田淵　隆明

【1】はじめに

近年、公共分野などにおいて、プログラムの誤りなどに起因するトラブルにより、広範囲にわたる経済的損失や人的被害が頻発している。また、今般の東日本大震災に起因する福島第一原子力発電所の事故(メルト・ダウン、メルト・スルー・水素爆発など。一部の専門家からは断続的な再臨界の可能性も指摘されている)においても、全電源喪失の考慮をスルーしていたり、電源車の電圧が異なり使用できなかったなど、先進国にあるまじきお粗末な失敗であり、第三者による「システムの監査」が実施されていたら事前に問題点がクローズ・アップされ、今回の大惨事を防ぐことができたとの指摘も少なくない。

諸外国の例を見ると、システム「監査の法制化」については、米国、韓国、台湾などでは、公共系のシステムを中心にシステムの監査が法令で義務付けられており、我が国にも近い将来、システム監査の法制化が導入される可能性がある。我が国の産業の競争力の確保、及び、国民生活の発展に寄与するために、そして、我が国のサスティナブルな社会の形成のためにも、システム監査の法制化の実現は極めて重要な施策である。

一方、「主婦年金救済策」、「個人情報保護法」の拡大解釈による副作用に象徴されるように、制度導入・改正のもたらす負の側面については、事前に様々な簡単から検討しておくべきであり、諸外国の先進事例も含めて研究されるべきである。

【2】これまでのシステム監査法制化研究会の活動のまとめ

(1)公共系のシステム監査について

米国、韓国、台湾では、公共系の一部システムについて、情報システムに関する監査が法制化されている。このことを踏まえで次のような議論が行われていた。

・原子力など、システムの誤作動による被害が甚大な分野では特に重要である。
(昨年の段階で、メンバーの方から「原子力」というキーワードが指摘されていた。)

・「有価証券報告書」の資産の管理の箇所において、システム監査の状況について記載を求めることも一計である。ただし、このことは、「公共性」を重視し、「金融商品取引法」ではなく「会社法」の改正とするべきである。

【提言】公共分野・医療分野におけるシステム監査の法制化を推進するべきである。

【提言】会社法を改正し、公共性の大きい「大会社(資本金 5 億円以上または負債 200 億円以上)、かつ、公開会社」においては、「会計監査人」とパラレルな地位での「システム監査人」を設置し、「監査役会」(監査役設置会社)または「監査委員会」(委員会設置会社)に、監査報告を行うことを法制化するべきである。

⑵ソフトウェア　--- 製造物責任法の不備
・現状、民法上ソフトウェアは「動産」ではない。
製造物責任法第 2 条における「製造物」とは「製造または加工された動産」とあるため、ソフトウェアには製造物責任法が適用されない。

・カーナビはPL法の対象にはならない。
理由はメカニズム(メカニックス)と一体でないから。
カーナビは単に運転者に情報を与えるだけ。たとえプログラムが
暴走しても、人体や器物に直接危害を加える訳ではない。
この観点からは、一般ビジネスアプリやゲームソフトと同類。

・PL法の対象になる例を出すとすれば、プリウスで問題となった制御システム等。

・「産業用ロボットコントローラ、湯沸かし器用マイコン回路、エンジン制御モジュール等のプログラムなど、ハードウェアに組み込まれた制御系ソフトウェア」については、ハードウェアに製造物責任法が適用されるため、当該のソフトウェアにも間接的に製造物責任法の効果が及ぶ。また、個別開発ソフトウェアの場合は、仕様書による縛りが効く。しかし、「スマートフォン等の組込系ソフトウェアや、個別開発ではないパッケージ・ソフトウェア」の場合は、製造物責任法が適用されず、当該ソフトウェアの瑕疵に起因するユーザの損失については、その立正責任が民法 415 条に依拠することとなり、立証責任がユーザ側に帰することとなる。

・ドイツ、フランスなどでは、「ソフトウェア」は「製造物」である。これは映画の DVD などと同様に、コンテンツして扱われているためである。つまり、映画の CD,DVD と同様の扱いである。なお、ダウンロードの場合もこれに準ずるものとされている。

【提言】製造物責任法第 2 条を改正し、「製造物」の中に、「ソフトウェア」を追加する。

(3)その他：中国の会計基準
・中国の「新企業会計準則」について報告を受けた。

※EU 委員会は、「新会計準則」について、「暫定的に同等性」を認定し、本年中に同等性認定の継続の可否を判断する予定。我が国において、これは全く手薄な分野であり、システムへの影響についての議論が全く不十分である。

【3】我が国におけるシステム監査法制化の動き

バブル崩壊後の 1990 年代、金融不祥事等の経済犯罪が多発し、我が国においてもシステム監査の法制化の必要性が各方面から提言されるようになり、2005 年頃までは、政府内でもシステム監査の法制化を進める動きがあった。しかし、近年はセキュリティ分野、個人情報保護以外はあまり進展がない。実は、SAAJ 本部においても 2008 年頃まではその動きがあり、記者発表も行われたが、現在は消極的である。

残念ながら、現在、日本の産業界には所謂「J-SOX 後遺症」が蔓延している。特に、2006 年頃に吹き荒れた J-SOX の意味の取り違えによる「3 点セット」ビジネスの影響は大きく、産業界全体が”羹に懲りて膾を吹く”という状況を呈している。その結果、IFRS 対応も含めて、制度の変更に対する IT 投資・業務改革などの立ち上げが遅延する背景にもなっていると思われる。

医療分野では、薬事法に基づく医用電気機械への EMC 規制(2007/10～)があり、動作確認の第三者による保証が義務付けられている。しかし、他の分野では、セキュリティ分野と BCP 分野を除き、あまり浸透していないのが現状である。

IT に関して言えば、状況は深刻である。「データが消失する」、「データが重複する」などの不具合は、社内での検査において比較的高い確率でトラップすることができる。問題は、微妙に数値が異なるような場合であり、本来の値が 12,345 であるべきところが、12,354 になってたことを不具合と認識できないことも少なくない。本来的にはこのような業務処理に関する事項においても外部監査を義務化するべきであるが、前途は険しいと言わざるを得ない。

※1.会計分野では、インプット値からアウトプット値を想定するのが容易ではない、「退職給付システム」、「連結会計システム」などは特にリスクが高い。
→日本公認会計士協会の IT 委員会報告第 3 号などでは、具体的に見落としやすい例として、「退職給付システム」、「連結会計システム」が挙げられている。

※2.特に、技術者のスキル、及び、モラルの低下、「重要性の原則」という用語の濫用など、ソフトウェアの品質の劣化を惹起する条件は蔓延しており、早急なる対策が望まれる。

こうした「日本社会の劣化」とも言われる深刻な事態の原因としては、「ゆとり教育」(1966 年 4 月 2 日以降～2007 年 4 月 1 日までに生まれた者に適用)による日本人全体の学力の低下があることは当然のことであるが、2003 年度の税制改正の「プログラム準備金制度」の廃止に伴う「システム・インテグレータ認定制度」が 2003 年 3 月期をもって廃止されたことにより、高度情報処理の有資格者を優遇するインセンティブが失われたことが挙げられる。この制度下では、高度情報処理の有資格者を多数確保し、IT ベンダのスキルを高水準に保つことが強力な税制優遇に直結していた。これが失われたことは慙愧に堪えない。

※プログラム準備金制度: 4億円を限度として、売上の10%までをシステムの保守等に要する準備金の積立を損金算入できる制度。利益の 10%ではなく売上の 10%に注意。

【4】システム監査を法制化する具体的方法

今回の東日本大震災に起因する福島第一原子力発電所の事故や、金融機関の大規模なシステム・トラブルを受け、システム監査の法制化の必要性が、再び各方面から指摘され始めている。公共系は勿論のこと、大企業についてもシステム・トラブル/機能不全の発生時の社会に対する影響が甚大であることから、第三者によるシステム監査の義務化を行うべきである。例えば、「会社法」を次のように改正することで実現可能である。

(取締役会等の設置義務等)
第 327 条 ---- 第 6 項を追加
6. 委員会設置会社は、システム監査人を置かなければならない

(大会社における監査役会等の設置義務)
第 328 条 ---- 第 3 項及び第 4 項を追加
3. 大会社(委員会設置会社を除く。)は、システム監査人を置かなければならない。
4. 公開会社でない大会社は、システム監査人を置かなければならない。

(システム監査人の資格等)
第 338 条の 2
システム監査人は、システム監査技術者その他政令で定める者でなければならない

なお、他の法律との齟齬が問題となり、運用上の解釈の曖昧さや「個人情報」の拡大解釈の弊害が各方面から指摘されている「個人情報保護法」については、その見直しの必要性が各方面から指摘されている。特に、単なる「個人を特定できる情報」と病歴・障害などの「保護するべき個人情報」の区別や、下位法令体系の整備は急務である(※)。

※内閣府令の「施行令」や省令の「施行規則」が制定されておらず、ガイドラインのみが存在する。また、プライバシー・マークの定義する「個人情報」は、個人情報保護法の規制対象とする「個人情報」よりも範囲が広く、運用・解釈上の困難さが頻発している。我が国の産業競争力の回復のためにも、同法の見直しは急務であろう。

【5】本研究における今後の課題

※当日、発表します。

【6】参考資料

(1)海外の薬事制度について (2008)
http://www.pref.kyoto.jp/yakumu/resources/1201507232393.pdf

(2)「めだか」(SAAJ 会報 201011)
http://skansanin.com/saaj/medaka/201011medaka2.pdf

(3) 日本公認会計士協会IT委員会研究報告第 31 号「IT委員会報告第3号「財務諸表監査における情報技術(IT)を利用した情報システムに関する重要な虚偽表示リスクの評価及び評価したリスクに対応する監査人の手続について」Q&A
http://www.hp.jicpa.or.jp/specialized_field/31_6.html
→特に Q28 に注意。

(4)神尾博「計算・通信・制御機能の融合とシステム監査」(システム監査学会 2005.12)
〈一部引用します〉

５．急務となる制御系のシステム監査基盤の確立

制御系のシステム監査は、現在ではほとんど行われていないと言っても過言ではない。しかしながらこれまで述べてきたように、(旧来の情報システムに) 制御系を融合したシステムも急速に増加しており、このまま放置すると、大局高所からシステム全体の総合的な評価を下すといった、システム監査の根幹である機能すら果たすことが出来ない事態にも陥りかねない。

また交通やエネルギーなどの社会的インフラを担う分野においては、保証型監査を前提とした法定システム監査への要求の高まりも予測され、その場合はたとえば情報系のみのデータの入出力に限らず、制御系でのデータや各種信号の入出力の正確性・確実性の検証も、併せて要求される可能性も高い。

(5)あずさ監査法人

AZInsight Volume41 2010/09「中国子会社への IFRS 適用について」

－新企業会計準則の概要と実務上の留意点

(6)ドイツ気象庁

Informationen des Deutschen Wetterdienstes(DWD) – Kernkraftwerksunfalle in Japan

http://www.dwd.de/

→Ausbreitung Japan の mehr をクリックすると、放射能の拡散予測が見られる。

(7)3 号機で再臨界の可能性の指摘

http://2r.ldblog.jp/archives/4359572.html

福島第一原発のふくいちライブカメラで青い光を確認か？

(8)黄色い雨「東京で黄色い雨を観測」

http://www.asyura2.com/11/genpatu9/msg/243.html

(9)経済産業省アイデアボックス

システム監査の法令化(YE ツイッター氏) --- SAAJ 東京の方

http://201002.after-ideabox.net/ja/idea/00376/

〈一部引用します〉

近年の情報システムに関わるトラブルの頻発は、情報システムが社会的なインフラとなった今日では、その当該企業のみならず社会全体に大きな影響を与え、特に金融機関はもとより、航空・運輸業界、電気・ガス・水道業界等におけるシステム障害記事、直近ではメーカーである自動車会社の組込みシステムの問題による被害記事が新聞に掲載されない日はないという状況です。

★ここに経済産業省が公表のシステム監査規準／管理規準等を基準とする「システム監査」の法令化を提案します。直近では、情報セキュリティについての議論が活発になってまいりましたが、その重要性は一部のセキュリティに限定されず、戦略性・安全性・信頼性・有効性全般を網羅する「システム監査」を義務付ける必要があると考えます。内部統制におけるIT統制も財務報告の信頼性に偏った監査となり、その厳格な実施において疑問の声もあります。

今や、システム監査は会計監査の前提としてのみならず、そのトラブル発生が社会的影響度において、また会計監査よりもその被害や影響力が大きいことを冷静に考慮すべきです。情報システムの障害による被害は今後益々大きくなりその対策は重要なものとなるでしょう。この対策として、第三者による「システム監査」が唯一の有効な手段だと考えます。会計監査

や内部統制と同様に「システム監査の法制化」を提案いたします。
尚、カテゴリーもあえて情報セキュリティと区別する為に「9．その他のIT政策」にさせていただきました。「システム監査」のカテゴリを新規に作成いただければ幸いです。

(10)日本情報産業新聞　2006/03/17
http://www.josan.jp/dantai080317.htm
日本システム監査人協会が情報システム監査の普及に提言書

〈一部引用します〉
日本システム監査人協会(SAAJ)は、情報システム監査の普及や制度のあり方、監査の基準などを明確にしてシステム現場への浸透を図るため 10 項目の提言を明らかにした。システム監査を取り巻く問題点と期待を明らかにし、今後のあるべき姿を描いて具体的な活動として展開していく。例えばシステムの企・開発・運用・保守を行っているシステム管理者が監査を意識したコントロールを行えるよう、システム管理者や若い世代を見据えた取組みを推進するなどだ。内部統制/IT 統制が重要になっている現在、監査の重要性を認識させるいい機会といえる。
今回の提言は大きく、システム監査の「普及」「制度」「基準」「技術・視点」「監査人」「その他」の 6 分野について 10 項目にまとめたもの。これに当り、システム監査の現状や問題点を洗い出すために会員及び関連する団体や企業へのアンケートを実施、その回答を受けて策定した。
システム監査の普及では、内部統制や企業の社会的責任の増加、システムの安全性と信頼性の重要度が増していくことなどから普及は進んでいくとしている。
ただし、システム管理者がシステム監査を意識してコントロールしていないことが多いことから、現場を知る管理者やこれからシステム監査に従事するであろう若い世代に向けた認知度向上を推進する必要があるとしている。また、システム監査と情報セキュリティ監査の関連とその違いを明確にすることにした。
制度の面を見ると、今後は法制化・制度化が進むことが考えれられており「法制化が必要」との声が過半数を占めている。一方で「法制化は不要」との声もあり、同協会では対象範囲を絞った法制化など、検討チームを設けて検討を進める考えを示した。
システム監査の基準では、管理基準だけでは対応できないシステム環境での対応基準モデルの策定を手がけていく。ほかにはシステム監査人の人材像、例えば役割や要求されるスキルなどを検討して整理することで、同協会が実施している「公認システム監査人制度」とその認定取得者の価値を向上させ、普及を図っていくとしている。システム監査の重要性は今後も増していくことが分かっており、協会の取組みを強化、推進することを明確にした。
日本システム監査人協会　http://www.saaj.or.jp/