エッセイ	システム監査の視点からみた情報システムに関する最近のトピックスから

会員番号299　安本哲之助（情報システム監査株式会社）（元近畿支部支部長）

最近、一昔前のメインフレームを遥かに凌ぐ高性能と、数多くの脆弱性を持つ Android とともに過ごす時間が増えた。その私がシステム監査分野に従事をはじめて 25 年が経過した。手がけはじめた当時 10 年も経過すればシステム監査は人間ドックのように重要産業分野では必須なものとして普及すると見込んできたが、その歩みは残念ながら遅々としたものであった。近畿支部 25 周年を迎えることになってようやく金融機関を始め中央省庁から定着しだしたのはよろこばしいかぎりである。

そこでこの機会に昨今のトピックスをシステム監査の視点から振り返ってみた。

● 中央省庁では情報セキュリティ分野の取り組み結果につき本格的な「年度情報セキュリティ報告書」を省庁別に作成し、平成 24 年 5 月に公表した。

この種の報告書はいままでは当該組織体限りで情報セキュリティの現況を外部に開示するのはためらわれてきたが、今回全省庁がはじめてそれぞれ開示をおこなったことは評価でき、セキュリティも国民の安心のため公表される時代になった。

また、政府は平成 24 年 4 月「情報セキュリティ対策のための統一規範」で全省庁に情報セキュリティ監査を「おこなわなければならない」とセキュリティ監査の実施をあらためて義務付けた。それまではセキュリティ監査を「実施すること」といわば推奨レベルにとどまっていたが「ねばならない」と強い語調に表現をあらため、これが真摯に定着されることをねらっており、今後の推移を見守りたい。

あわせて「重要インフラにおける情報セキュリティ確保にかかわる『安全対策基準等』策定にあったっての指針」の情報セキュリティ対策の評価の項で、自己監査による内部監査より外部監査の方が専門性や客観性が保持できることを評価している。

したがって今後各方面で外部組織による情報セキュリティ監査実施が見込まれるが、その実施の担い手としてシステム監査人が必要数充足されるかが危惧され、この面からも当協会の公認システム監査人の増強が強く望まれる。

一方、民間部門では上場企業においても年度決算報告は従前では企業の業績中心の報告であったものが、近年ではアニュアルレポートとして総合報告書の形態をとるものが増えてきた。業績以外に事業継続計画、CSR 方針、内部統制報告、情報管理（物理的セキュリティ、人的セキュリティ、技術的セキュリティ、組織的セキュリティ）

等が包含され、政府機関と同様セキュリティ分野への取り組み記述がこれからも一層充実してくるものと思われる。

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、公共系システムを中心にすでに法令で義務付けられているが、わが国でも法定化されることを期待したい。当近畿支部ではかねてより「システム監査の法制化研究会」のプロジェクト活動を推進しているが、リーダーの田淵隆明氏が、2012 年 6 月 13 日の衆議院公聴会で「システム監査の法制化」の必要性について言及されたのには、大いに注目され、この活動が実を結ぶことが切望される。

● 先般、東日本大震災で被災して、メルトダウン事故を惹起した福島第一原子力発電所における事故報告が「政府の事故調査・検証委員会」および「国会事故調査委員会」双方から公表されたが、その報告書を読み解くと、端々にシステム監査の視点からみても問題となる事象が多々検出されている。

国会事故調査委員会の黒川委員長は「福島原子力発電所事故は終わっていない。複雑に絡まった『規制の虜（Regulatory Capture)』とそれを当然と考える日本人の「思いこみ（マインドセッ ト)」があった。前例を踏襲すること、組織の利益を守ることは、重要な使命となった。この使命は、国民の命を守ることよりも優先され、安全対策は先送りされた」と報告書の締めくくりで記述している。

また、事故調査・検証委員会の畑村洋太郎委員長の締めくくりの言葉「見たくないもの、都合の悪いことは見えないものである」このことばを重くうけとめたい。

いままでシステム監査は経営や財務等のビジネス情報システムに注力して取り組まれてきたが、高度なIT技術が利用されている設備・制御系分野についても運用当事者に任せるばかりでなく、客観的な立場からシステム監査に取り組まなければならない必要性を痛感させられた。一方、サイバー攻撃においても、重要情報の詐取やネットワークそのものの撹乱以上に、電力、ガス、水道といった、国民の生命や健康に直結する社会インフラの頭脳である制御系の機能不全が危惧される。

ここでもこの分野の専門スキルを身につけたシステム監査人が量的・質的に育っているか気になるところである。