

急がれる法定システム監査の実施 - 社会的責任が問われるコンピュータ事故・犯罪の増大化に対応して -

Practice of Legal System s Aud its

~ To Defend from Com puterCrim e /AccidentDam ages SocialResponsibility ~

松田 貴典

Matsuda Yoshinori

松田技術士事務所

概要

IT (Information Technology: 情報技術) 活用の進展は速く、予期できない事故・犯罪が容赦なく人々を襲い、健全な情報化を脅かす混沌とした国際情社会に向かいはじめている。また、ソフトウェアの不正コピー事件やコンピュータウイルスのばら撒き事件、ネットワーク取引システムの障害など社会を震撼させるコンピュータ事故・犯罪も多発し始めている。もし、企業や事業体が情報システムのセキュリティ対策を実施していないことにより社会不安を引き起こすことになれば、その企業や事業体は存続を危ぶまれるばかりか社会的責任や法的責任を問われることになる。このことから、これまで情報システムの信頼性や安全性を担保するシステム監査から、一步踏み込んだ情報システムの社会的責任を担保するシステム監査が求められるのである。そして、このシステム監査を、もはや内部監査の一環としての任意監査ではなく、実施を法的に義務付ける「法定システム監査」にすべき時期にきている。

キーワード：IT (情報技術)、法定システム監査、コンピュータ事故・犯罪、社会的責任、情報システムの脆弱性、国際的責務

1. はじめに

「システム監査を“法定システム監査”と位置付け、強制実施すべき時期は熟している」といえば、賛同者もいるが反対論者も多い。この背景に、システム監査(以下、監査)の実施を義務付ける法定システム監査(強制システム監査: 以下、法定監査)とすることが、健全な監査の普及や啓蒙を推進するより監査ビジネスの拡大を支援することにならないかとの懸念がある。

この議論は、学会をはじめ諸研究会において、真正面きって議論されたことは少ない。それは、前述の如く、監査の普及や啓蒙活動

に最も効果的な手段は何かと問えば、「先ず法定監査が必要」と異口同音に語られるが、この回答はあまりにも短絡的であること。また、内部監査の一環として捉えられている監査を法定化する事に、経営者自身がその必然性に疑問を感じていることなどがその理由として考えられる。さらに、内部管理の手続き(手法)に属する監査が、法律によって規制されるならば、情報戦略や情報活用に独自性を失うことにもなりかねず、創造豊かな情報化の発展は望めなくなることも考えられる。その上、監査内容にあらゆる省庁と関連する要件が多く、一省庁の判断で法定化することも問題があるように思える。例えば、監査を

IT (Information Technology: 情報技術) の効率的活用や情報産業の発展に寄与すべき視点で見る経済産業省、公共企業や自治体情報通信システムの健全な発展と安全性・信頼性の確保の視点や個人情報の保護などの視点で健全化を求める総務省、コンピュータ犯罪を取締りその減少を求める警察庁、金融機関での金融情報システムや証券情報システム、国際間金融取引の安全性など求める財務省、健全な情報システムの活用やIT人材育成の視点を求める文部科学省、基幹の情報通信システムが耐震構造で安全に設置される施設の建設を求める国土交通省など、どの省庁からみても監査の視点は挙げられ、情報通信システムの安全性・信頼性・効率性の向上に重要な視点である。したがって、どの省庁にも関与したことを一つの省庁で推し進めることは難しいと考えられる反面、ITが広く普及し社会システムの中核機能を果たしていることから、監査の法定化は避けておれない状況といえる。

現代は、規制緩和の時代である。この時代に監査の法定化を進め、規制緩和と逆行することはタブーであるといった風潮はある。規制緩和は「善」で、これに反することは「悪」と言った風潮もおかしいものである。グローバルなネットワーク時代で、且つ、インターネットが国際的なビジネス取引の情報基盤になろうとしている時代に、情報システムの信頼性、安全性、効率性を求める監査が法定監査として位置付けられ、健全な情報化を求めことにいささかの迷いもない。

2. 法定監査による抑制が期待できるコンピュータ犯罪・事故

警視庁が発表したハイテク犯罪状況では、ネットワークを利用した犯罪の検挙数は、平成11年に247件で、平成12年では484件と実に倍増である。反面、電磁的記録を対象とした犯罪は、半減以下に減少している。ま

た、特徴としてインターネットオークションを利用した事件が多発しており、その内、詐欺事件が31件、著作権違反が7件である。不正アクセス事件も下半期に増加しており、下半期のみで23件にもなっている⁽¹⁾。また、ハッカーやクラッカーの侵入事件も多発している。悪質なクラッカーはネットワークを通じてサーバーコンピュータに侵入し、ファイルを破壊したり、データの改ざんしたりし始めている。

一方、近年、社会を震撼させたコンピュータ犯罪・事故が多発しはじめている。以下のコンピュータ犯罪・事故は、被害を受けた企業の損失だけでは済まされず、社会から非難をあび、社会的責任を問われた事件でもある。

2.1 拡がる社会的責任事件

(1) 繰り返し発生するソフトウェア違法コピー事件

1999年12月、米国のアドビシステムズ社など7社が、東京の環境調査会社をソフトウェアの違法コピーによる損害賠償訴訟をおこした。そして2000年4月に和解が成立し、環境調査会社は正規にソフトウェアを購入する金額を上まわる和解金を支払うことに同意した。

2001年5月16日に、マイクロソフト社、アップルコンピュータ社、アドビシステムズの三社がパソコン用業務ソフトウェアを不正に複製したとして、東京の司法試験予備校を相手に1億1000万円の損害賠償などを求めた訴訟で、東京地方裁判所は原告側の主張をほぼ認め「正規品の小売価格と同額の損害賠償をすべきだ」として、約8千500万円の支払いを命じた。判決によると、予備校は1999年5月当時、マイクロソフト社の表計算ソフトウェアの「エクセル」や、アップル社の画像処理ソフト「マックドロー」、アドビシステム社の編集ソフトウェア「ページメーカー」など無断で違法にコピーし、教材作成

などの業務に利用していた。なお、違法コピーが発覚後、同社は正規にソフトウェアを購入している（2001年5月17日付日本経済新聞）。

これらは、企業という社会的な責任のある組織の中で行われた不正コピーについて、民事上の不法行為を認定した判決であった。また、違法コピー事件としては、1996年の9月に、大阪市のソフトウェア会社が、マイクロソフト社、ロータス社、ジャストシステム社の三社に対して総額約1億4000万円の損害賠償金を支払うなどの内容にて和解が成立している。この和解内容は、正規のライセンス料金の約2倍の賠償金支払いのほかに、

違法コピーを認め謝罪文を提出する、今後違法コピーを行わないことを確約する、少なくとも3年間は三社の全製品に関する著作権協会の検査を受け入れる、などであった（1996年9月11日付日本経済新聞）。

（2）不正アクセスにより機密情報の漏洩

インターネットの脆弱性を突いて、中央省庁のホームページ（以下、HP）にハッキングやクラッキング攻撃を受けた事件が、2000年1月に発生した。HPを狙った不正アクセスは、中央省庁のほか日本銀行や人事院の事務局にも及んでおり、公務員試験の情報の消去など、短時間によるサイト攻撃を受けていた。一方、米国で、重大なデータ窃盗事件が発生した。2000年の9月頃にマイクロソフト社のコンピュータシステムにハッカーが侵入し、開発中のパソコンOS「ウィンドウズ・ミレニアム・エディション（ME）」の設計情報が盗まれた可能性があるとして米紙が報じた。同紙によると侵入者は電子メールに「QAZトロージャン」と呼ばれる特殊ソフトウェアを埋め込み、これを通じて極秘製品情報を取り出したとされている（1999年10月28日付日本経済新聞）。重要なことは、マイクロソフト社のOSの機密情報が盗まれたこと

により、「OSのメーカーであってもセキュリティ機能の弱点を突かれることが発生する」事実を、あらためて社会に暴露したことである。

不正アクセスにより、企業や国家機密のデータが窃盗され、スパイ行為が実施されることも予測される。スパイ行為により、競合他社に画期的なアイデアが盗まれ数億円に及ぶ取引の契約を失うこともある。また、官公庁の入札価格が事前に漏洩し、みすみすの商談を失うことにもなりかねない。データ窃盗は決してインターネット等のネットワークから発生するばかりではない、設計図や仕様書が電磁的記録に複製され社員から持ち出されることも過去には多く発生している。しかし、グローバルネットワーク時代となり、ネットワークを介したデータ窃盗は国内のみならず、海外からも起こってくることになり、ネットワークセキュリティ対策の強化が望まれる。

（3）情報資産を破壊するコンピュータウイルス事件

不正アクセスとならんで、非常に脅威となっているコンピュータ犯罪に、コンピュータウイルス（以下、ウイルス）がある。1980年代の後半に、我が国ではじめてウイルスが発見されて以来、パソコンや通信ネットワークやインターネットの増大化とともに、ウイルスの被害が急増しはじめている。

近年、最も話題となったウイルスは1999年に発見された「メリッサ」ウイルスである。マイクロソフト社の日本語文書ワープロ「ワード（Word）」のマクロ機能を利用して、電子メール及び情報管理のソフトウェアである「アウトブック（Outbook）」を介在に、ワードファイルなどを添付した電子メールを交換することにより瞬く間に広がった。受信したメリッサウイルスに感染のワードファイルをクリックすると、メーリングリストに登録されている最大50人分のアドレスに自動送信

するため、急速に広がった。さらに、メリッサウイルスが沈静化しないまま、このメリッサを上まわる強力なウイルスが現れたのである。このウイルスは「ラブレターワーム (VSB/LoveLetterworm)」と呼ばれ、2000年5月4日に発見された。ラブレターワームの感染力は恐ろしく、世界20カ国で確認され、およそ4500万台のコンピュータに被害を及ぼした。また、2000年9月に発見されたW2MTX (PE MTXA) は2ヶ月間で約900件の感染が報告されている。

ウイルスの新種は止まることなしに出現し、被害率は極めて高くなってきている。2001年7月17日に海外で発見された新種のウイルス「Sircam (サーカム)」は、過去最悪のペースで広がっていることが、IPA (情報処理振興事業協会) から報告された。サーカムは11日間で届出が520件に達したとのことである。また、サーカムに続いて、新たなウイルス「コード・レッド」が猛威をふるい、世界のインターネットサーバーに感染している。コード・レッドは、自己増殖の強いワーム型のウイルスであり、電子メールを感染媒体せず、インターネットに接続しているサーバーに直接、自己コードを送り込みサーバー上のメモリーで活動を開始する。さらに、感染後は不正アクセスを可能にするバックドア (裏口) を作成し、第三者が感染先を自由自在に悪用できる亜種の「コード・レッド」も出始めている (平成13年8月7日付、読売新聞)。

ウイルスの特徴は、一般に、新しく発見されるウイルスほど強力で感染力が強く、大きな被害が全世界に急速に広まること、また、原ウイルスをもとにさらに悪化させた亜種が模倣して出現する。その上に、ウイルス作成の犯人を突き止めること極めて難しいことである。

(4) システム障害事件

2001年の6月29日に米国店頭株式市場 (ナスダック) で、売買注文のネットワークシステムに異常が発生し、米東部時間午後2時半 (日本時間30日午前3時半) ごろから約1時間20分にわたって取引システムが停止した。ナスダックは非常措置として、取引の終了時刻を通常より1時間遅らせた。ナスダックは取引終了後、「ナスダックの基幹システムが、米通信事業者ワールドコム社の技術者の手違いによりダウンした」との声明を発表した。また、ワールドコム社は通信システムのダウンが同社の手がけた定期検査の途中で起きたことを認めた (2001年6月30日付日本経済新聞)。

一方、これより数ヶ月前の2月26日の午前に、サッカーの2002年ワールドカップ (W杯) 日韓大会のチケット販売をインターネットによる受付を実施したところ、アクセスが殺到し英文にて「大量の申込みがあったため、チケットショップを閉めなければならなくなりました。申し訳ありません。できるだけ早く復旧いたします」という文字が表示され、申込みができない状態となった。インターネット販売は、システムトラブルで当初の15日開始から延期され、24日の夜から始まったばかりで、わずか1日半で停止した。今大会のチケット販売はW杯史上初めてのインターネット販売となった。前回のフランス大会では、チケットが代理店などを通じて観戦者の手にはいるまでの過程で、チケットの横流しや転売が横行した。フリーガン (暴徒化したサポーター) 対策やブラックマーケットへの流出を防ぐために、チケットの購入者がそのまま観戦者になる「直売方式」が裏目に出ることになる (2001年2月16日付読売新聞)。

2.2 増える社会的責任を問われるコンピュータ事故・犯罪

これらの事件は、IT (情報技術) の高度

化とその脆弱性が密接に関連しているコンピュータ事故・犯罪ではあるが、社会に与えた影響も大きい。しかし、これらの大半は、監査によりその発生がかなりコントロールされるか、被害の拡大が抑制されることが期待できる事故・犯罪である。以下、その内容を考察する。

(1) 「ソフトウェア資産」の認識が薄い繰り返しのソフトウェア違法コピー事件

ソフトウェア不正コピー事件を背景に、情報システムのオープン化とEUC(End User Computing)に伴い、パソコンが急速に普及し、ソフトウェア資産管理の重要性の認識が、その普及についていけなかったことにある。また、ソフトウェアに代表される情報資産の複製が、違法行為であることの社内教育や指導が周知徹底なされていなかったと考えられる。しかし、最も問題があることに、経営者自身が、ソフトウェアの不法な複製に対する違法性の認識の薄いことにある。コンピュータソフトウェアの権利団体のBSA(Business Software Alliance:本部米国ワシントンDC)によると、2000年日本のソフトウェアの違法コピー率は37%(昨年は31%)で損害額は約16.7億ドル、また、2000年の世界全体の違法コピー率は昨年より1ポイント上昇し、37%で、損失額は約118億ドルを上るものと推計している⁽²⁾。法治国家である日本においても、ソフトウェアの違法コピーの問題は跡を絶たない。この時の評に、「パソコンソフトウェアの違法コピーの問題は、表面化することはめずらしいうえ、違法の確証を得るのが難しく刑事事件として摘発された例は無い」としている。

これを契機に、企業や組織では、従業員に対して知的財産権の価値認識と管理意識を植え付けようとする動きが出始めている。企業行動指針や就業規則に規定をもうけ、社内教育は啓蒙に動きは始めている。

(2) 公共性の高い情報システムでの情報漏洩は社会的責任が問われる

前述のように、近年、インターネットを通じて企業の機密情報の不正アクセスや、他人のパスワードを盗んでのクラッキング、データ窃盗、データ改ざん、なりすまし犯罪、コンピュータウイルスのばら撒き等、さまざまなコンピュータ・犯罪が増加している。この種の犯罪の特徴は、一度発生するとすぐに模倣されて繰り返し繰り返し発生し、その範囲はインターネットの普及に相俟って、企業から組織、団体、個人へと広がることである。これは非常に憂慮すべきことである。不正アクセス等のインターネット犯罪の攻撃を許すことは、直接的には情報資産の消失や業務の停止を引き起こすことになる。実際に、2000年5月に発見され、世界20カ国で確認されたラブレターワームの場合、約47億ドル(約5000億円)の損害が発生したとされている。また、感染したウイルス駆除の費用や失われた情報資産を修復する時間的損失も大きい。しかし、こうした情報資産の消失や修復のための時間的なロス、企業等の内部で留まっている間は、一時的な金銭的損害ですむことになるが、銀行システムや公共企業体システム等の社会的情報システムにおいて、情報漏洩やサービスの停止が発生すれば、社会的な信用の失墜を招くことになる。もちろん、企業の情報システムにおいても、度重なるトラブルや長期的な業務の停止は、対外的な信用のみならず、企業の収益をじわじわと蝕むことになる。インターネットが社会システムの基盤となった今日、これらの問題は決して、一企業体としての問題として済まされず、社会的責任が問われる時代になってきている。そしてこの社会的責任はますます増大し、グローバル化が進むことによりその責任は国際的に問われることになる。

(3) 設計ミスによるシステム障害は人的災

害

インターネットの拡大に伴って、コンピュータ犯罪や事故は他のリスクと複雑に関連して、今後ますます増加してくる。クレジット情報の盗用やデータの改ざん、電子通貨の偽造等はコンピュータ犯罪になるが、罪の意識のない犯罪（愉快犯等）や新手の犯罪も起こってくる。例えば、インターネット上の Web や図書から写真や図柄を、無断で複製し自社の情報サービスに利用することは、著作権侵害になるが、安易に行われることが多い。また、企業の機密情報や誹謗・中傷の情報をインターネットの電子掲示板（ニュースグループ）に流して、故意に企業を混乱に陥れたり、SPAM メール（迷惑メール）やメール爆弾、ウイルスをサイトに送りつけて、混乱させたりして業務を妨害する等、インターネットの情報伝達力を悪用した犯罪がおこってくる。しかし、こういったケースで被害を被るのは、サイバービジネスを実施する個人や事業者のみではない、利用者にも被害が及び被害者である事業者が加害者化し、利用者から多額の損害賠償を請求されることにもなりかねない。昨年の 2 月に東京のある証券会社がインターネットによる株取引を開始した。この時インターネットで取引した 87 件が顧客の指定通りに処理できず、数億円の補償金を払ったとされている。

通常、オンラインシステムを設計するときには、オンライントランザクション（取引データなど）の発生ピーク時に合わせて、余裕をもったシステム設計やサーバーシステムの選択を行う。この設計を間違っシステム開発し実施した時には、オンライントランザクションの処理の待ち行列が発生し、一定限度をこえると完全にサーバーシステムの機能不全が起こってしまうことになる。まさしく人的な災害ともいえる。

3. 求められるシステム監査の法定化と

情報システム脆弱性の視点

IT の高度化により、企業や社会はその恩恵（効用）を受け、豊かな情報社会を満喫しているが、情報システムは、IT に内在する本質的な弱さ（脆弱性）により、さまざまな脅威にさらされ、その現実化により被害を被っている。

脆弱性には、経営管理・組織的側面の脆弱性（以下、経営組織的脆弱性）、国際・社会的側面の脆弱性（以下、国際社会的脆弱性）、情報技術（IT）的側面の脆弱性（以下、情報技術的脆弱性）、法・倫理的側面の脆弱性（以下、法倫理的脆弱性）の四つの側面があり、それぞれに監査の視点は異なってくる⁽⁵⁾。以下、情報システムの脆弱性と監査の重要な視点を述べる。

3.1 情報技術的脆弱性とシステム監査

コンピュータ事故・犯罪を綿密に分析すると、実は情報技術的脆弱性が基底にあり、その上で、経営組織的脆弱性や国際社会的脆弱性、法倫理的脆弱性と結びついて脅威の現実化が起こり、被害が生じる。また、IT の進歩により情報技術的脆弱性は常に変化する。この情報技術的脆弱性がもとで、組織の牽制機能が働かない環境になり、さらに、法律や管理制度が弱いとコンピュータを悪用した犯罪や予想外の事故を引き起こすことになる。そこで、情報システムの安全性に重点をおいた情報技術的脆弱性の監査が求められるのである。これを「セキュリティ監査」と呼ぶことにする。

セキュリティ監査の重要な視点の一つに、コンピュータシステムのセキュリティ対策の実施状況がある。例えば、大規模な金融・証券の情報システムや社会公共的なシステムはコンピュータシステムの二重化やバックアップセンターの維持（契約）を実施している。監査では、この実施状況を点検・評価する。

しかし、セキュリティ認識の薄い企業等ではコンピュータシステムのセキュリティ対策費用は、売上の拡大や利益を生まない投資として考えがちであるが、この考えには問題点が多い。近年、セキュリティ投資を控えたことで、経営者に対して社会的責任を問われることが多発しており、情報システムのシステムダウンや情報資産の消失等が企業等の危機事態を招くことにもなりかねない。さらに、企業や国際間のネットワーク全体を「仮想の個」として捉えなければならない。それは、自己の情報システムの脆弱性が足がかりとなって、ネットワーク全体の脆弱性を発生させることになるからである。情報資産保護のためのセキュリティ対策が、企業等のトップマネジメントの重要な施策であることを、トップマネジメント自らもって認識させることが、監査の重要な役割である。そして、監査は情報システム全体の安全性に主眼をおいたセキュリティ監査が必要となる。

3.2 法倫理的脆弱性とシステム監査

情報資産に関連して法倫理的脆弱性には大きく二つの細部側面で脆弱性が発生する。一つは、情報を如何に保護するか側面である。情報は貴重な資産である、それがため、情報が不正にアクセスされて複製されたり、改ざんや窃盗されたりする機会が増大する。これらの不法行為から如何に情報資産を保護していくか重要な問題である。また、ソフトウェアや情報資産が取引の対象となることで、知的財産権ビジネスや取引手段としてのITの法的な問題を検討しておかなければならない。もう一つの側面は、ITが如何に適正にしかもルールやマナーにもとづいた活用の仕方がなされているかである。自社の情報システムの活用が、時としてその意思なく他人の情報システムに迷惑をかけたたり、法的侵害を犯す結果になったりすることである。他システムへのウイルス侵入の踏み台にされるなど

典型的な事例である。この二つの側面は、情報システムの活用方法によって、法的な被害者にも加害者にもなるということである。

近年、情報データの不正なアクセスや侵害など、法倫理的脆弱性に起因した問題が広がりはじめている。そのほとんどは、コンピュータ犯罪やプライバシーの侵害など法的な問題を引き起こす要因となっている。これは、ITの持つ本質的な脆弱性が経営組織的脆弱性や国際社会的脆弱性を誘引し、犯罪を引き起こすことになるためである。コンピュータ犯罪の発生する環境は、組織の牽制機能の弱体化や内部統制の不備により生まれてくる。さらに、国際的なネットワークを利用した犯罪は、国家間の法律の不均衡や国際協力体制の脆弱性に起因することが多い。その一方で情報倫理の問題として取り扱われるべき多くの事件が発生している。

一方、消費者を対象としたサイバービジネスが激増し、事業者との間でのトラブルも増加している。そこで、サイバービジネスを立ち上げる場合に、消費者保護の視点で考慮しておかなければならない代表的な法律に、平成13年6月1日より施行された「特定商取引」（特定商取引に関する法律：旧改正訪問販売法）と平成13年4月1日より施行された「消費者契約法」「金融商品販売法」がある。それぞれの法律において、保護・規制の対象やルールの機能は異なる。しかし、いずれの場合にあっても、企業（事業者）を規制し、消費者を保護するという立場では共通しているが、特定商取引法は事業者の行為を規制する行政上のルールであるのに対して、消費者契約法は特定の販売方法や業種を規制するものではなく、消費者の取引の適正化を図る民事上のルールである。

これらの事例は、ITに関連した法律の一例にすぎない。監査では主として自社の情報資産の保護と他人の情報資産の侵害やプライバシーの侵害等の保護と侵害の両面から、

法的な視点にたった法的セキュリティ監査が、今後、ますます重要になってくる。

3.3 国際・社会的側面脆弱性とシステム監査

情報システムは、通信技術の進歩により、企業内部から企業間の情報通信システムへ進展してきた。いわゆる情報化の点から線、面への展開である。そして、この面の拡がりには企業間から国際間のネットワーク取引に拡がりはじめている。

国際・社会的側面脆弱性は、主として情報システムを仲介したネットワーク取引から発生する。ビジネス社会でのネットワーク取引は今後ますます増加し、産業界でのネットワーク取引は、CALS や EC に発展していくことになる。また、金融機関での EFT (Electronic Funds Transfer: 電子資金移動) は、企業間決済から、個人決済に進み、電子マネーによる決済へと進んでおり、やがて、ネットワークによる企業間ネットティング (相互決済) や個人決済の国際化が起こってくる。

インターネットによるサイバービジネスは、個人であっても簡単にネットワークビジネスの確立ができる。しかし、ネットワークシステムの不稼働リスクや決済業務の停止・不能リスク、決済不能による連鎖倒産 (システムミックリスク)、時差による国際的な決済不能 (ヘルシュタットリスク) 等さまざまな脅威が実現する国際的な脆弱性が発生してくる。また、官公庁や役所システムである電子政府 / 自治体システムが個人情報の保護や社会的安全性の確保ができていないかのセキュリティ監査がもとめられる。もし、これらのシステムの不稼働や機能が十分に発揮できていないならば、却って、手続きの複雑化やコスト負担の増大化を招くばかりでなく、社会的混乱を招きシステムを否定することになる。

今後、グローバル企業の監査は、国際・

社会的視点に目を向けた視点で、国際間で調整をとりながら進めなければならない。

4. システム監査に関連する主な基準・指針および法律・制度とその強制力

表1は、1974年以降での監査およびセキュリティに関連する主な基準 / 指針と法律 / 制度等について、年代別にまとめたものである。監査に関連して如何に多くの基準や指針があり、如何に多くの省庁と関与しているかが分かるであろう。システム監査基準は、1983年12月の産業構造審議会の中間答申において、システム監査ガイドラインの必要性の指摘を受け、通商産業省機械情報産業局長の私的諮問機関である「情報化対策委員会システム監査部」にて審議・策定され、1985年の1月に公表された。その後、ITの進展に伴い、情報システムのオープン化やダウンサイジング化、1995年の阪神・淡路大震災による情報システム安全対策の強化など、情報環境の急激な変化に対応すべく、1996年1月に改訂された。

一方、他のセキュリティ諸対策基準では、1977年の4月に電子計算機システム安全対策基準が策定され、情報環境の変化にともない、数回の改訂がなされ1995年に「情報システム安全対策基準」として公表されている。その他、「コンピュータウイルス対策基準」(1990年に策定、95年に改訂)、「ソフトウェア管理ガイドライン」(1995年に策定)、「コンピュータ不正アクセス対策基準」(1996年)がある。また、財団法人金融情報センター (FISC) では、「金融機関等コンピュータシステムの安全対策基準」(1985年)や「金融機関等のシステム監査指針」(1987年)が公表され、その後、金融機関等を対象としたシステム監査実践例集や手順例集、オープン化に伴う「金融機関等の小型・分散システムにおけるシステム監査実施のための手引」(1994年)

や「共同センター加盟金融機関のシステム監査実施手引書」（1998年）など、ITの高度利用と時代のニーズに対応して、それぞれの関係省庁の管轄範囲で関連基準等が公表されている。

これらの基準／指針や制度は、ITの進展やコンピュータ関連犯罪・事故の発生にもなって必然的に制定されたり改訂されたりしてきたが、その実施や適用の強制力は、各省庁により大きく差異がある。例えば、金融機関の場合、情報システムの社会公共性が高く、その不稼働は、一般市民からクレームとなるばかりでなく、国際的な信用の失墜を招くことにもなり、情報システムの安全対策の実施率は非常に高い。

プライバシーの保護に関しては、1985年に行政機関に対して「行政機関の保有する電子計算機に係る個人情報の保護に関する法律」が制定されているが、民間に対する法律は、一部割賦販売法や貸金業の規制に関する法律等、全体をカバーするものではなく、行政機関の指導基準や自主規制による実施がなされているに過ぎない。

一方、EU構成国は、1995年7月24日に「個人データ処理に係る個人の保護および当該データの自由な移動に関する欧州議会および理事会の指令」（Directive of the European personal data and on the Free movement of such data）採択し、この指令に適合するように3年（1998年10月）以内にデータ法を改正または新たに法律を制定し施行した。EU指令の第25条では、第3国へのデータ移動に関しては、十分なレベルのデータ保護措置（adequate level of protection）が講じられている場合に限られており、わが国でもこの条項への対応が迫られ、1998年にプライバシーマーク制度や個人情報保護マーク制度を制定している。また、2000年に個人情報保護基本法の大綱案が出された状況である。

毎年のように制定された基準や指針、改正や制定された法律や制度は、情報システムの健全化には十分に有効に機能するものである。しかし、法律以外その実施や施行は決して強制されていない。それにもまして、コンピュータ事故・犯罪はますます増加の傾向にある。これらの基準や指針、制度の実施は、監査の法定化により、かなり推進されるばかりか、指導性の高い監査は、企業等のトップマネジメントへのセキュリティへの認識を高めることになる。また、監査の法定化により、情報システムユーザから見れば、最も効果的な基準や指針を選択するところなり、より有効な基準や指針に改訂され統合されていくことになる。

5．おわりに

情報システムの健全化の手法には監査のほかに、リスクマネジメントやセキュリティマネジメント等がある。これらの手法は、健全な情報化社会に充分貢献できると考えられてきた。しかし、IT活用の進展は速く、予期できない事故・犯罪が容赦なく人々を襲い健全な情報化社会を脅かす混沌とした国際情報化社会に向かいはじめている。その一方で、国際企業間の競争は激化し、企業等が生き残りをかけたITの戦略活用が求められている。しかし、社会公共性の高い情報システムにおいては、その安全性に対する対策不足がトラブルを引き起こし、企業等の存続を危ぶまれるばかりか社会的責任や法的責任を問われることになりかねない。このことから、これまで情報システムの信頼性や安全性を担保する監査から、一步踏み込んだ情報システムの社会的責任を担保する監査が求められるのである。そして、この監査を、もはや内部監査の一環としての任意監査ではなく、実施を法的に義務付ける「法定監査」にすべき時期にきている。

筆者は全ての情報システムを対象に全て

の脆弱性視点で監査の法定化を求めている。簡潔に言うならば、監査対象は、社会性、国際性、遵法性を持つ情報システムであり、その情報システムによる事故や犯罪が社会的責任を問われるシステムということになる。また、ここに掲げた脆弱性視点は、監査により十分に効果が得られる視点である。さらに、対象となる事業者や企業等と言うならば、金融・証券会社、病院、運輸鉄道企業、学校等であり、対象なる業務システムといえば、バンキングシステムや電子カルテシステム、電子政府システム、電子商取引システム、ソフトウェアライセンス管理システムなど社会公共性の高いシステムや情報システムのトラブルが危機的な事態を招くシステムといえる。しかし、今後、監査の対象システムや範囲等を決定することは、情報システムの規模、範囲、機密性、社会性、国際性等を勘案して十分な議論が必要である。一般的な概念で決めるものではないと考える。

この時代に、監査の法定化を遅らすことは、プライバシー保護の法制化やネットワーク取引の安全性等の強化を求める国際社会から非難を受けることになる。安全性、信頼性、遵法性を担保する監査はより強力に実施しなければならないし、また、監査の効果を高めるために、独立・客観性はより一層の法的な保証のもとで、推し進める必要がある。そして、監査の法定化は行政を巻き込んで討議しなければならない重要な問題である。

敢えてお断りしておくが、筆者は監査のビジネス展開を問題にしているのではない。また、監査ビジネスの範囲や監査人の職業資格化を求めているのでもない。ITの高度化がもたらす21世紀のグローバル情報化社会の健全化に、監査の果たすべき役割は何かを問うているのである。グローバル時代の情報社会において、情報システムの安全性、信頼性、遵法性を確保するには、現状では、監査の法定化が最も効果的であり、それが日本の国際

情報化社会への責務と考える。

[参考文献]

- (1) 警察庁編；「警察白書」（平成12年版），（2000）
- (2) BSA (Business Software Alliance) ホームページ：
<http://www.bsa.or.jp/news/2001/010525.htm>
- (3) 通商産業省機械情報産業局監修；「システム監査基準解説書」，（財）日本情報処理開発協会発行，（1996）
- (4) 財）日本情報処理開発協会編；「情報化白書」，コンピュータエージ社，（2001）
- (5) 松田貴典著；「情報システムの脆弱性」，白桃書房，（1999）
- (6) 岡村久道編；「インターネット訴訟2000」，ソフトバンクパブリッシング社，（2000）
- (7) 松田貴典著；「システム診断とシステム監査」，日本経営診断学会年報，第32集，（2000）

表1 年別システム監査およびセキュリティに関連する主な基準/指針と法律/制度等

年	基準/指針	関連法律/制度ほか
1977	電子計算機システム安全対策基準策定	
1984	電子計算機システム安全対策基準改訂	
1985	システム監査基準の策定 金融機関等コンピュータシステムの安全対策基準 (FISC:財務省)	著作権法改正 (プログラム著作物など)
1986	情報システム安全対策指針 (警察庁)	システム監査試験の実施
1987	金融機関等のシステム監査指針 (FISC:財務省) 地方公共団体コンピュータセキュリティ対策基準 (総務省)	刑法改正 (コンピュータ犯罪に対応:電磁的記録の不正作出,コンピュータ使用詐欺など)
1988	民間部門の個人情報保護の取扱指針	プライバシー保護法 (行政機関保有の情報)
1989	情報システム安全対策ガイドライン コンピュータウイルス等不正プログラム対策指針 (警察庁)	
1990	コンピュータウイルス対策基準策定	コンピュータウイルス被害届出制度 不正競争防止法改正 (営業秘密など)
1991	電気通信事業者における個人情報保護に関するガイドライン (総務省)	システム監査企業台帳制度
1994	金融機関等の小型・分散システムにおけるシステム監査実施のための手引」 (FISC:財務省)	
1995	情報システム安全対策基準改訂 (電子計算機システム安全対策基準を改め名称変更)	ソフトウェア管理ガイドライン (日本情報処理開発協会) EU 指令 (個人情報保護の関する EU 指令)
1996	システム監査基準の改訂 コンピュータ不正アクセス対策基準	コンピュータ不正アクセス届出制度
1997	情報システム安全対策指針改訂	著作権法改正 (送信可能化権など)
1998	共同センター加盟金融機関のシステム監査実施手引書」 (FISC:財務省)	プライバシーマーク制度 (日本情報処理開発協会) 個人情報保護マーク制度 (日本データ通信協会:総務省) セキュリティマーク制度 (電子商取引実証推進協議会)
1999	JIS X5070:ISO/IEC15408 (セキュリティ製品国際評価の国際標準基準)	不正アクセス禁止法 (不正アクセスの禁止) 児童ポルノ等児童保護法 (ネット頒布等禁止) 住民基本台帳法 (基本台帳ネットワーク関連)
2000	ISO/IEC17799 (セキュリティマネジメントシステムの認証の国際標準基準) セキュリティポリシーに関するガイドライン (各省庁向け)	電子署名認証法 (電子署名の効力認証など) 個人情報保護基本法制の大綱案 セキュリティマネジメントシステム評価制度 (SMS:安全対策事業所認定制度の後継)
2001		消費者契約法/特定商取引法 (6月まで,旧改正訪問販売法)/金融商品販売法 (以上,電子商取引の健全化に関連する法)

		律) 情報セキュリティアドミニストレータ試験実 施
--	--	---------------------------------

注：基準/指針/制度のうち、省庁が記載していないものは経済産業省に関連するものである。

出典：表は「システム監査白書」(1999-2000)、「情報化白書」(2001)を参考に作成した。