［研究ノート］

現代の情報システム化実践とシステム監査の関わりについての一考察

A Study on Relationship between Contemporary IS and Systems Audits

松田　貴典
Yoshinori Matsuda
大阪成蹊大学
Osaka Seikei University

概　要

第４次産業革命に突入したといわれる近年、情報システム化実践の変化によりビジネスのあり方を大きく変容させた。そして、システム監査のあり方に大きく影響し、多様化の方向に向かっている。

その一方で、予測もできないコンピュータ事故や犯罪が激増し、情報システムの安全対策や信頼性の向上対策について強く求められるようになった。それ故に、実効ある情報セキュリティ対策やリスク対策等の向上とともに、対策の実効性を高めるシステム監査の普及が求められている。

筆者はシステム監査を研究するなかで、特にシステム監査のあり方に大きく影響を及ぼしたと考える近年のコンピュータ事故や犯罪等を取り上げて、システム監査との関わりについて考察するとともに、その問題点について筆者の視点で論述した。

キーワード：脆弱性、個人情報保護の監査、コンプライアンスの監査、デジタルフォレンジックス

はじめに

わが国で、はじめて「システム監査」の用語が使われたのは、1974 年（昭和 49 年）で、日本情報処理開発協会（現：日本情報経済社会推進協会：JIPDEC）が米国に EDP 監査の視察団を派遣したときであった [1]。一方、日本公認会計士協会は、業務の EDP 化で監査証跡が確保できないことを懸念して 1967 年（昭和 42 年）に「EDP システム内部統制質問書」発表し、経済団体連合会等から意見を求めた。その後、1976 年（昭和 51 年）に日本公認会計士協会が「EDP 監査の進め方」を出版し、「コンピュータ犯罪・不正を防止するために」を目的として、EDP 監査の実施をはじめた [2]。

1987 年（昭和 62 年）３月にシステム監査学会が設立され、同年 12 月に日本システム監査人協会が発足し 30 年が経過した。システム監査は「情報システムの信頼性、安全性、経済性（有効性）への寄与」から、「情報報システムにまつわるリスクに対するコントロールのリスクアセスメントに基づく対応と ICT（Information and Communication Technology：情報通信技術：注１）ガバナンスの実現への寄与」へと、その目的を経営レベルに拡げた。

そこで、本稿では、まず、情報システムを俯瞰しながら、システム監査の研究や実践に影響をどのように及ぼしたのか、システム監査学会の研究テーマからその関わりについて考察した。そのうえで、筆者が特に印象深く重要視すべき事故や犯罪、制度等を取り上げて、システム監査の考え方や実践への影響を及ぼした事項について論述した。

１．情報システムの発展とシステム監査への影響の俯瞰

コンピュータを電子計算機と訳し、ビジネス活用された 1960 年（昭和 35 年）頃は、その活用形態を「EDPS（Electronic Data Processing

投稿受理日	2017 年 3 月 17 日
再投稿受理日	2017 年 11 月 5 日

System：電子計算機データ処理システム）」と呼んだ。その後、コンピュータを経営や意思決定支援に活用し、MIS（Management Information System：経営情報システム）やDSS（Decision support system：意思決定支援システム）の概念が確立した。コンピュータの活用技術は一層発展し、OA（Office Automation：事務の自動化）やFA（Factory Automation：工場の自動化）と拡がり、ネットワークを活用しての企業間競争を優位に展開するSIS（Strategic Information System：戦略情報システム）の構築も試みられるようになった。そして、今日では、ビッグデータの活用やAI（Artificial Intelligence：人工知能）やIoT（Internet of Things：モノのインターネット）を駆使したビジネス情報システムへと大きく変容した。

総務省は2000年前半に「e-Japan」構想を打ち上げ、2000年後半には「u-Japan」の実現に向けた国家戦略を打ち立てている。情報化は、Uの「Ubiquitous」、「Universal」、「User-oriented」、「Unique」の意味を加えて、その構想の実現にむけて推進されている。

ICTを活用して構築される情報システムが発展することで、企業等にとってはICTへの投資額も大きくなってくる。そこで、経営者からみれば、構築された情報システムへ投資は適正であり有効に活用されているのか、情報システムは安全に運用され信頼できるのか、客観的に点検・評価・助言が得られないか考えることは至極当然のことである。ここにシステム監査の求められる必然性がある。表1は、1960年から10年毎に情報システムの発展とシステム監査の研究テーマ及び課題等の変遷をまとめたものである。

主なシステム監査テーマ（キーワード）は、学会誌「システム監査」から網羅的に選出した。そのテーマの多くは、情報化の実践にともない、情報処理形態やその時代に普及した関連事項である。学会の設立当初は、情報システム開発の信頼

表1　年代別情報システムの発展とシステム監査の研究テーマ及び課題等の変遷

年代	1960年～	1970年～	1980年～	1990年～	2000年～	2010年～
情報処理形態及び関連事項	EDPS バッチ処理システム	MIS/DSS 経営情報システム	OA/FA	SIS/EUC 戦略情報システム	ユビキタス VR、AI活用	クラウドコンピューティング、ビッグデータ、IoT
システム監査対象等	EDP会計 コンピュータ犯罪等	オンラインシステムの信頼性等	オンラインリアルタイムシステム、ソフトウェア開発等	情報システムの戦略活用、2000年問題	経営改革・SCM、BPR他、SNS等	クラウドコンピューティング、ビッグデータ活用等
主なシステム監査の研究テーマ(キーワード)	EDP化された会計システム等のEDP監査	オンラインシステムの信頼性・安全性に向けた監査	・システム監査と内部統制 ・コンピュータ犯罪の傾向 ・システム開発ライフサイクル ・リスクメネジメント ・ソフトウェア開発をめぐる法的問題等	・戦略的情報システムの監査 ・企画開発業務の監査 ・阪神淡路大震災(震災と安全) ・情報システムの安全対策 ・オープン環境下でのシステム監査等	・システム監査とリスクマネジメント ・SNSの情報論理 ・インターネット社会におけるシステム監査 ・情報システムの脆弱性とリスク対策 ・ITガバナンスとシステム監査等	・クラウド時代でのシステム監査 ・東日本大震災でのシステム監査 ・想定外の脆弱性時代のシステム監査等 ・ビッグデータ時代のシステム監査 ・マイナンバー制度でのシステム監査等
システム監査への期待や問題	EDP化された経理・会計帳簿システム等の信頼性の向上等	オンラインシステムの信頼性・効率性（ダウン対策など）、コンピュータ犯罪防止など）等	情報通信システムの開発の信頼性と生産性の向上、システム監査の研究、セキュリティ対策の研究等	経営戦略・業務改革手法（BPR等）、ソフトウェア資産・知的財産権管理、地震対策、ディザスター・リカバリー、2000年問題等	ビジネス問題と情報システムの脆弱性研究（ICT活用とセキュリティ）、情報セキュリティ関連法、BCP、システム監査の普及等	クラウドコンピューティング、コンプライアンス問題、情報システムの多様化とシステム監査の多様性の対応等

性や生産性にシステム監査がどのような関わるべきかの研究が進められた。その一方で、情報ステムの脆弱性に関連する事件も発生し、少し遅れながらも研究テーマに取り上げられた。しかし、脆弱性を組織全体の視点から定義する場合と、プログラムの欠陥や設計ミスなどの視点から定義する場合があり、システム監査等での監査対象や範囲の設定で混乱を起こすことなる。

2．システム監査の実施の前提となる情報システムの脆弱性

2.1　情報システムの脆弱性を惹起させた事件

（1）三和銀行オンライン詐欺事件

1981 年 (昭和 56 年) 3 月 25 日に三和銀行 (現、三菱東京 UFJ 銀行）茨木支店の女性行員 A が、同支店のオンライン端末を不正に操作して巨額の現金他を騙取した横領・詐欺事件である。女子行員 A は、銀行の開店とほぼ同時に、同支店の端末を操作して大阪の吹田支店、豊中支店、東京の新橋支店、虎ノ門支店の計 4 支店に開いた架空名義の口座へ、合計 1 億 8 千万円を架空入金した後に、伊丹空港から飛行機で東京に向かい、更に東京の新橋支店、虎ノ門支店からも現金を引き出した。女子行員 A は現金 5 千万円と小切手 8 千万円相当の合計 1 億 3 千円を詐取し、全額を主犯の B 男性に渡し、フィリッピンの首都マニラに逃亡した。

（2）本裁判で指摘された脆弱性

本事件では、1982 年（昭和 57 年）7 月 27 日、大阪地方裁判所にて、被告人 A（女性行員）に懲役 2 年 6 月、被告人 B（男性）に懲役 5 年の実刑判決が言い渡された。

本判決で、「本件犯行はコンピュータ・システムの弱点を利用したものであり、今日、これらのシステムは、金融機関は勿論、多方面に普及しており、社会生活上や経済取引上欠くべからざるものである。システム自体に内在する弱点とはいえ、これを取り扱う者によって容易に悪用されるうるものであることを明らかにし、その結果、システムに対する社会の信頼を失わせるとともに、同種の事犯を誘発しかねないものであり、社会に与える影響は無視できない。」とした。この事件と判決から、以下のようなコンピュータ・システムの問題点と脆弱性が認識され、刑法改正の契機になった。

①銀行オンラインシステムは、全国のどの支店の ATM（Automatic Teller Machine：現金自動預払機）からも現金の預金や払出が可能であることの効用は、どの支店からの ATM から悪用（遠隔操作等）されるリスクがある。

②情報システム化は運用・活用面での脆弱性を拡大し、コンピュータを操作する者による犯罪を引き起こすリスクが高まり、また、組織全体の運用管理やセキュリティへ対策の不考慮が、コンピュータ犯罪をひき起こすリスクを高めることになる。

③ 1987 年（昭和 62 年）の刑法改正で、電子計算機使用詐欺罪（刑法 246 条の 2）が新設された。

2.2　情報システムの脆弱性とその分析の重要性

（1）情報システムの脆弱性

情報システムの進展は豊かな情報化社会を形成したが、その豊かさに反作用して「脆弱な情報社会」を作ることになる。情報システムの脆弱性 (Vulnerability of Information Systems：以後、「脆弱性」と言う。）は、コンピュータ事故や犯罪等を引き起こす誘因となる。脆弱性とは、『情報システムの構築に伴い、その「効用」に比して不可避的に発生し、潜在化（内在化）する「欠陥」である』[3]。

IT（Information Technology: 情報技術：注 1）の機能の高度活用により、組織や業務の範囲（適用、内容)、量（データや処理)、質（スピード、ミスや判断・意思決定能力等）の向上をはかることができるが、IT 本来がもつ特性が「欠陥」となり複雑に変化し潜在化する。例えば、記録媒体が紙から電磁的記録に変ることで、情報を即座に可視可読できなくなる。反面、情報の集積力は大きく向上するが、電磁的記録への不正な改ざんを引き起こす要因となる。そして、脆弱性は、IT の本質的な特性に起因して、無知、無法、無規制、無対策等のコントロール（統制）欠如とマネジメント（管理）の失敗等で「さらなる脆弱性」が発生する。高度に情報化が進んだ近年は、脆弱性を①情報技術的側面の脆弱性、②経営管理・組織的側面の脆弱性、③国際・社会的側面の脆弱性、④法・倫理的側面の脆弱性に分類し、システム監査やセキュリティマネジメント等の前提要件としなければならない。企業や組織等での多様な情報システムにおいては、脆弱性は互いに関連し多様な脆弱性が潜在化することになる。システム監査やリス

クマネジメント等を実施するためには、まず前提となる対象情報システムの脆弱性分析 [注 2] からはじめなければならない [4]。

（2）脆弱性分析からのシステム監査の実施の重要性

企業等はコンピュータを活用して独自の情報システムを構築する。それは合理化であり、差別化であり、経営戦略の実現に欠かせないものである。情報システムの健全化の手法としては、客観的な立場で健全化を助言・勧告するシステム監査やセキュリティ監査等があり、健全化を直接的な対策で実施するセキュリティ対策やリスクマネジメント等がある。そして、これらの健全化を進めるにあたって最も重要なことは、その前提となる脆弱性分析の実施である。前述したように脆弱性は情報化することで、その組織の中に潜在化し、組織における統制機能が弱いと脅威の顕在化が起こり、被害が発生する。脅威の顕在化の可能性がリスクである。

（3）システム監査には狭すぎる総務省定義の「脆弱性」視点

総務省は脆弱性を以下のように定義している。「脆弱性とは、コンピュータの OS やソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のこと」をいう。脆弱性はセキュリティホールとも呼ばれている。脆弱性が残された状態でコンピュータを利用していると、不正アクセスに利用されたり、ウイルスに感染したりする危険性がある。また、情報セキュリティに対する脆弱性となるのはシステム上の問題点だけでなく、機密情報の管理体制が整っていないなどといった人間の振る舞いに関する問題点も脆弱性となりうる。こうした脆弱性をシステム的なものと区別して「人為的脆弱性」と呼ぶこともある [5]。

ところが、企業や組織等での多様な情報システムには、多様な脆弱性が発生する。システム監査の対象は、脆弱性をソフトウェアやプログラムの欠陥、セキュリティホールや管理体制上の「人為的脆弱性」を指していうのは、情報システムの安全性である情報セキュリティ問題のみを意識しているためである。システム監査では、情報システムの安全性のみが監査視点になるのではない。総合的な情報システムを対象に、信頼性や効率性、有効性なども視点となる。総務省が定義する脆弱性では、システム監査の前提となる脆弱性視点として、あまりにも狭すぎることになる。

3．個人情報漏洩事件と法・制度およびシステム監査への影響

3.1　個人情報漏洩事件とその影響

個人情報漏洩事件は、その保護や対策の考え方に重大な影響を及ぼすことが多い。個人情報は多くの企業にとって重要な情報であり、特に、消費者を対象とするビジネスにおいて、個人情報の漏洩を引き起こした企業にとって致命的となる。ただ、問題点は、個人情報の漏洩を引き起こした企業等で、法の解釈と対応で大きく差がでたことである。以下、重大な社会問題を引き起こした個人情報漏洩事件とその論点を記述した。

①地方自治体の住民基本台帳データ漏洩事件

1999 年（平成 11 年）月に京都府宇治市が住民基本台帳データを利用して乳幼児検診システムを開発企画した際に、住民票データ 22 万人分が流出しインターネットで販売された事件である。3 市民が市と業者及び元請業者に損害賠償請求を起こした裁判で、市に対して、4 万 5 千円（3 人 ×1 万 5 千円）の支払を命ずる判決が出された。1 人当たり 1 万円 5 千円の内訳は、慰謝料 1 万円、弁護士費用 5 千円であった。また、業者（システム開発会社）及び元請業者に対しても市と同じ判決が出された。

この事件がもたらした問題の一つは、インターネットを悪用して個人情報の販売を行ったことである。重要な個人情報の価値が認識され販売の対象となり、インターネットを通じて販売されることの怖さを感じさせた。二つは、個人情報のうち基本情報の漏洩では、少なくとも 1 万円の慰謝料の支払いが起こることで、基本情報の価値を社会的に概念付けした。三つは、集団訴訟のリスク（最悪のシナリオ）が発生しうることである。被害者が原告となって訴訟が起こせば、被害者が勝訴することを例証した。（宇治市住民基本台帳データ大量漏洩事件控訴審判決　大阪高裁平成 13 年 12 月 25 日）

②コンビニエンスストア等の会員情報漏洩事件

2003 年（平成 15 年）6 月にコンビニエンスストアの「ローソン」からカード会員情報 56 万人分が流出した。全会員 115 万人に対して 500 円の商品券と社長からの謝罪文を配布した。同年 8 月に信販会社アプラスからクレジット顧客情報 7 万 9110 人分がダイレクトメール

会社に流出した。対象者に 1000 円の商品券とお詫び状を配布した。

この事件がもたらした問題は、個人情報の漏洩事件をおこした企業等は、いち早く謝罪し、500 円から 1000 円程度の商品券等をお詫びとして配布することで、社会的に問題の解決を図ることとした。裁判になることを懸念しての商品券等を配布することで、個人情報漏洩事件の解決の一つのモデルを作った。個人情報漏洩を金銭で解決を図ろうとする企業姿勢には、社会的に非難されるべきである。

③通信販売会社での顧客データ漏洩を社会的責任とした対応

2004 年（平成 16 年）3 月に通販会社「ジャパネットたかた」の顧客データ約 50 万人分が流出し、内容に住所、氏名、生年月日、電話番号が入っていた。この事件を引き起こした「ジャパネットたかた」は、お詫び金を配布せずに、再発防止対策を最優先に実施するために、通信販売のビジネスを中断した。個人情報の漏洩させた企業は、それを「企業の社会的責任（CSR）」として捉えて、ビジネスを 49 日間中断した。その結果、企業には約 150 億円の減収となった [6]。

この事件では、個人情報漏洩は企業の社会的責任と捉え、社長自らセキュリティ対策の指揮をとった。この企業行動がかえって好感度の社会評価をうけるとともに、後に企業のレピュテーション（Reputation：評判）を高めて売上利益の向上につながった。一般に、セキュリティ対策は、利益を生まない投資と考えられていたが、戦略投資として売上・利益の向上をもたらすことを示した [7]。

④ JR 福知山線事故での負傷者収容病院の対応

2005 年（平成 17 年）4 月 25 日の午前 9 時 20 分ごろ、兵庫県尼崎市で起きたＪＲ福知山線電車脱線事故は大変痛ましく、負傷者を収容した二つの病院において、負傷者の個人情報の取扱いが大きく分かれた。A 病院は、負傷者の家族や関係者からの問い合わせに対して、個人情報保護の観点から一切回答をしなかった。他方 B 病院は、病院の玄関前に負傷者の氏名を張り出し、家族や関係者に対して明らかにした。この事件がもたらしたことは、二つの病院の個人情報の取り扱いの差異が起こった。個人情報保護法の解釈とともに、個人情報の取り扱い方や保護の方法に統一的な考え方がなく、企業や組織体によりバラバラな保護の考え方になってしまった。

⑤ JR 東日本 Suica の利用履歴情報の販売

2013 年（平成 25 年）7 月 1 日より、JR 東日本が、IC 乗車券「Suica」の利用履歴のビッグデータが販売開始された。データを販売した相手は日立製作所で、Suica のデータを駅エリアのマーケティングに活用していく狙いがあった。発売直後から「個人情報保護の観点で問題があるのではないか」という指摘があって、同年 7 月 25 日には販売中止を決めた。Suica のデータ販売に関する第一報の段階で「個人情報を含まない形で販売」と報じられていたが、中止の背景には、プライバシーに敏感な消費者の心理が読み切れなかったことにある。（読売新聞　2013 年 7 月 18 日付）。

取り扱うべき範囲の曖昧さ（グレーゾーン）のため、企業が情報の利活用を躊躇しはじめた。しかし、ビッグデータ時代の到来に、企業の国際的な競争力を高め、個人情報を戦略的に利活用できるようにすることが、時代に求められたことである。このことが、個人情報保護法の改正をおこなう契機となった。

⑥ベネッセコーポレーション顧客情報流出事件

2014 年（平成 26 年）7 月 9 日に、「進研ゼミ」等を運営するベネッセコーポレーションの「個人情報流出事件」が発覚した。流出した情報は進研ゼミなどの顧客の情報であり、子供や保護者の氏名、住所、電話番号、性別、生年月日等、2070 万件が流出した。ベネッセコーポレーションは、派遣社員のエンジニアが情報を持ち出し、名簿業者に売却したことを認めた。ベネッセコーポレーションの顧客情報漏洩問題で、流出したデータは少なくとも 3 つのルートで名簿業者など約 10 社に拡散した。（日本経済新聞　2014 年 7 月 10 日付）。

個人情報の漏洩経緯を追跡するためには、トレーサビリティの確保が重要となる。個人情報の第三者提供に係る確認及び記録の作成義務を、名簿業者等に義務付ける個人情報保護法改正のきっかけとなった事件である。

3.2　個人情報保護法及び番号法の改正とシステム監査への影響

（1）個人情報保護法及び番号法の改正とその対応

2015年9月3日「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律（略称：番号法）」がセットで改正され、2017年5月30日に施行された。そして、その主な改正点は、①個人情報の定義の明確化（身体的特徴等が該当、要配慮個人情報：いわゆる機微情報に関する規定の整備）、②適切な規律の下で個人情報等の有用性を確保（匿名加工情報に関する加工方法や取扱い等の規定の整備等）、③個人情報の保護を強化（名簿屋対策、トレーサビリティの確保等）、④その他（本人同意を得ない第三者提供：オプトアウト規定）の届出、取扱う個人情報が5,000人以下の小規模取扱事業者への対応）等である。特に、取扱う個人情報が5,000人以下の小規模事業者にも法の対象としたことは、企業規模に関わりなく個人情報保護の重要性を示したことである。

個人情報保護法の改正に背景の一つに、個人情報の定義が「特定に個人の識別できるもの」規定されていたが、近年個人情報があふれ他の情報と照合することで個人と紐づけされることが可能になってきたこと、さらに個人の識別符号、人種や病歴など要配慮個人情報として配慮する必要がでてきたことである。二つは、ビッグデータの利活用である。匿名加工情報に関する加工方法や取扱い等の規定を整備することで、消費者の購買履歴や乗降履歴などのデータを本人の同意なくビジネスに活用できるようにしたことである。

しかし、個人情報保護法及び番号法が改正された後も、個人情報の漏洩事件は減少していない。また、匿名化されたビッグデータの提供についても、企業等はプライバシーに敏感な消費者の心理を配慮して手探りの状態である。企業等のビッグデータの活用は、成長戦略の一つとして位置づけられている一方で、より厳格なプライバシーの保護が求められている。

筆者は、ビッグデータの活用とプライバシーの保護のバランスをとった対応に、「外部監査人による保証型のシステム監査」が非常に有効であると考える。それは、ビッグデータの提供にあたって一定の信頼性を保証し、プライバシーの保護にあたっての一定の安全生を担保することができるのである。

（2）個人情報保護マネジメントとシステム監査

個人情報の保護は、主に、JIS Q 15001で規定し、その実行は個人情報保護マネジメントシステム（Personal information protection Management Systems：PMS）の推進である。

個人情報保護マネジメントシステムとは、JIS Q 15001が規定している個人情報を保護の体制を整備し、定められた通り実行、定期的な確認、継続的に改善するための管理の仕組みをいう。管理の原則はISO27001と同様にマネジメントシステムの考え方を取り入れて、PDCAサイクルを通じて改善を実施し、スパイラルアップさせることを基本としている。そして、監査はC（点検）に位置づけられ、日常での「運用の確認」と「監査」の実施が求められている。

そこで、筆者は、個人情報保護のシステム監査を以下のように対応すべきと考える。

①個人情報漏洩リスクに対する脆弱性分析は、定期的に実施し、自社の個人情報保護ガイドライン及び規定やマニュアル等に反映しているか確認する。前節に記載するような漏洩事件が発生した時には、脆弱性分析を随時に実施する。

②教育システムや医療情報システム等の個人情報の漏洩が、重大なプライバシー侵害を及ぼす恐れのある情報システムは、システム監査の実施を義務化（法定化）すべきである。

③個人情報保護には、個人のプライバシー等の権利利益を保護する取組みを「宣言」し、適正に実施されていることを保証する外部監査人による「保証型監査」の実施をする。

④経営の視点でのシステム監査が重要となる。

- 「ガバナンスと戦略目標の実現」に寄与するシステム監査であること
- 個人情報の漏洩や紛失は、社会的責任（SR）を問われることになり、法的なコンプライアンス側面でのシステム監査であること

⑤消費者等からえたビッグデータの活用及び匿名化したデータの販売には、システム監査により匿名性を担保されるべきである。

4．サイバーショッピングをモデルにしたコンプライアンスのシステム監査

4.1　サイバーショッピングで法的問題

（1）サイバーショッピングでのコンピュータ犯罪

総務省の通信動向利用調査によれば、わが国のインターネット利用者数は、2016年末時点で1億8400万人、人口普及率は83.5.%となった[8]。インターネット空間を活用した電子商取引において、特に消費者を対象としたサイバーションピン

グはスマートフォンの急激な普及により大きく拡大した。

一般に、サイバーショッピングは、運営する事業者と購入する消費者間で、さまざまな法的問題が複雑に関連して発生する典型的なビジネスモデルと言える。例えば、クレジット情報の盗用やデータの改ざん、電子通貨の偽造等のハイテク犯罪、犯罪意識のない犯罪（愉快犯等）や新手の犯罪も起こってくる。また、事業者側から見れば、Webページを消費者からのアクセスを増やすために、人気俳優の写真や他人の図柄等を無断で自社の情報サービスに再利用することもある。そして、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に流し、故意に企業を混乱に陥れる等、インターネットの情報伝達力を悪用した犯罪が起ってくる。

サイバーショッピングでの法的問題は、法・倫理的脆弱性と密接に関連してくる。現行法制下において発生する一連の法的な問題点は、予測もされなかった事態を引き起こし、社会問題になることも多々ある。

下記事件は、昨年発生したサーバーショッピングでの典型的な違法行為となった事件である。大企業においても、今なお、違法行為が起こしているのが現状である。

（2）違法な誇大広告となるディー・エヌ・エー（DeNA）事件

IT大手のディー・エヌ・エーは2016年（平成28年）11月29日、ヘルスケア情報を扱う医療系サイトの「WELQ」に掲載していた全ての記事を、同日21時に非公開にしたと発表した。理由については、「医療情報に関する記事の信憑性について多数の意見が寄せられた」ことである。同年12月1日には、子育てや旅行、グルメなどに関する8つのサイトを、無断転用の恐れ（著作権法違反の恐れ）があるとして、公開をやめると発表した。

同社の調査では、マニュアルや外部ライターへの指示で、他サイトからの無断転用の推奨と読み取れる点が確認されたこと、原稿の正確性などについて「一切負わない」としていたなど、公開を継続することはできないと判断し、メディア運営を抜本的に見直すとしている。東京都は同社の化粧品や健康食品の原稿に誇大広告とみなせる内容があり、「医療品医療機器法違反（誇大広告）」の疑いで調査を始めた。（読売新聞　2016年12月2日付、12月8日付）

4.2　サイバーショッピングでのコンプライアンスのシステム監査

（1）サイバーショッピングのビジネスプロセスにける法制度

消費者が安心してサイバーショッピングを楽しむためには、事業者のインターネットサイトの信頼性向上や、ネットワークビジネス・プロトコルの安全性等を高めることである。

一般的なサイバーショッピングでは、4つのビジネスプロセス（広告宣伝→通信による契約→商品発送→決済）で構成される。まず、第1のビジネスプロセスは、「広告宣伝」である。消費者は、ホームページに掲載された写真や絵、説明をたよりに商品内容を知ることになる。したがって、掲載された内容に虚偽や誤認させるものであってはならない。また、商品を実際に手に取るのは、事業者からの商品を実際に手渡された時で、発注した商品と実際に受け取った商品に欠陥や違いがあれば、返品や交換、取り消しが容易に可能となる手続きの内容が掲載されていなければならない。

第2のビジネスプロセスは、「通信による契約」である。葉書や文書による契約では時間的な遅延（delay）が存在するが、通信の場合には瞬時に行われることになる。インターネットのトラブルや遅延がないわけではないが、通信の契約の成立が何時の時点なのか明確にする必要がある。例えば、発注メッセージを送信した時点なのか、事業者のサーバー到達した時点なのかなど、契約の成立時点の法的な問題が発生する。第3のビジネスプロセスは商品発送である。形のある商品の場合には、物理的な輸送や郵送が発生し、商品の引き渡しと受領確認が必要となる。コンテンツビジネス（情報や音楽商品の取引）の場合には、即時に発送と受領確認が可能となる。第4のビジネスプロセスは「決済」である。受領した商品が正しく欠陥がなければ、決済の手続きを行わなければならない。現在は、決済に多様な手段があり、輸送業者が配送と同時に事業者からの依頼で決済をうける「代引き決済」のほか、振込、現金送金のほか、近年多くなってきた電子決済等がある。決済では、事業者が商品を発送したにもかかわらず、支払いを受けられないリスクが発生したり、消費者が商品の発注とともに支払いを済ませたにもかかわらず商品が受け取れないといったリスクも発生する。

表1は、サイバーショッピングを4つのビジネスプロセスに展開し、そのビジネスプロセスにおける主要な法・制度上の問題例と関連する法制を示したものである。

（2）コンプライアンスのシステム監査

表1で示したように、サイバーショッピングでは、有店舗や対面取引とは全くことなる法・制度上の問題が発生し、サイバーショッピングを実施する事業者にはコンプライアンス監査が求められる。それは、事業者がサイバーショッピングの開発を行い運営するビジネスであるが、法的な問題は、事業者、消費者ともに発生する。企業や組織のなかで、コンプライアンス問題への対策を自ら実施することは難しいことである。その理由として以下のことが挙げられる。

①情報システム開発ではマーケティング上、戦略的に活用することを優先し、法的な問題に気付かないことや法的な問題のシステム分析をせずに開発をすることが多い。

②消費者が思いもよらない操作をおこない、想定外の法的問題を引き起こすことがある。逆にいえば、問題が発生してから、システム上の欠陥に気付く。

③システム上の欠陥に気付いても、その修正や変更を設計から遡って実施することが難しい場合が多い。

④情報は無形の財産（知的財産）であり、無形であることで価値の認識が薄く、使用・移転等の

表1　サイバーショッピングのビジネスプロセスでの法・制度上の問題例と関連する法・制度

ビジネスプロセス	法・制度上の問題例	関連する法・制度
広告宣伝	HP（ホームページ）、Web の信頼性を高める 事業責任者、連絡先等の広告表示義務 迷惑メールへの対応（2002 年特定商取引法、省令の改正） ：消費者の広告受取り拒否、再送の禁止等	特定商取引法、省令の改正 金融商品販売法 特定電子メールの送信適正化等の法
	広告表示の制限 ：不当な表示（優良誤認、有利誤認、誤認されるおそれ） ：虚偽・誇大広告の禁止（「医者に行かないで癌が治る」）など	不当景品類及び不当表示防止法 都道府県の執行力強化 健康増進法 医療品医療機器法他
	大量広告等の情報発信の規制 ：ウイルス、メール爆弾等によるサイトの通信不能など	刑法（ウイルス作成罪、電子計算機等業務妨害罪）等
	他人の著作物の HP 等への不正流用 他人の顔写真の不正貼り付け タレントブロマイドの不正使用	著作権法 肖像権侵害、名誉毀損 パブリシティ権侵害等
	通信販売できない商品 ：ポルノ、毒薬、私的宝くじ等 ：不正に複製された著作物（コンテンツ商品）等 （原則、通販はクーリングオフが不能）	風俗営業法、民法（公序良俗違反）、児童買春･児童ポルノ規制法､薬事法､刑法（富くじ罪等）、特定商取引法他
	悪徳商法（インターンネットねずみ講、マルチ商法勧誘等）	無限連鎖防止法
	インターネット・オークション（古物競り斡旋業）の営業として行う場合、公安委員会に届出と認定申請等が必要 オークション詐欺（偽ブランド、商品の未送付等）	古物営業法 刑法（詐欺罪）
	ドメインネームの不正登録・使用 サイバースクワッティング等	不正競争防止法 JP 裁定（JPNIC）
通信による契約	消費者からの発注、誤操作（錯誤無効制度の特例） 契約の成立時点（電子隔地間取引は、原則到達主義） 正しい発注者であること（成りすまし・事後否認） 通信データの改竄、変質等。契約での消費者の保護 消費者の利益を一方的に害する条項の無効	電子消費者契約民法特例法 電子署名認証法 不正アクセス禁止法 刑法（コンピュータ犯罪等） 消費者契約法他
商品発送	コンテンツ商品の配信、ダウンロード等 他人のビジネスコンテンツの配信（他人の音楽・プログラム配信、コンテンツの無断公開など）は違法	著作権法（送信可能化権侵害） 電気通信事業法
決済	決済:電子決済､電子マネーの利用（認証技術の向上が必須）、クレジット決済、振込み、代引きなど エスクロー制度：決済不能（商品発送後決済されない）、商品の不着（決済しても商品が不着）のリスク回避する制度	電子署名認証法 不正アクセス禁止法 民法、エスクロー制度、運送会社の決済サービス制度他

手続き忘れ等により知的財産の侵害の恐れがでてくる。

⑤企業等でのコンプライアンスへの侵害行為は、個人でも起こしやすい。個人が起こした問題であっても、その被害や責任は計り知れないものとなる。そして、その責任は企業等で負うことになる。

事業者にとって法的な問題は、企業法務全体に関連することであるが、サイバーショッピングを含めた情報システムの中に法的問題への対応を組み込まなければならない部分が多く、その対応は難しい。それ故、事業者は情報システムの企画・設計・開発の段階からビジネスプロセスからの法的問題の洗い出しと対策のガイドラインの作成を行い、情報共有と教育を徹底しておくことが重要である。

そのうえで、情報システム設計・開発の段階から法的問題に対するコンプライアンスのシステム監査の実施が求められる。そして、その実施にあたっては、「法とICT」の両面からアプローチする必要があり、法律知識をもつ者とシステム監査人とのプロジェクト体制で実施することも必要である。事前に自社のサイバーショッピングの管理基準を制定し、コンプライアンスのシステム監査の実施にあたることが重要である。

5．監査手法として求められるデジタルフォレンジックス

5.1　デジタルフォレンジックスが注目された事件

デジタルフォレンジックス（Digital Forensics）に関連して、話題となった大阪地検特捜部主任検事証拠改ざん事件がある。2010年（平成22年）9月21日に、大阪地方検察庁特別捜査部のM主任検事が、障害者郵便制度悪用事件で証拠物件のフロッピーディスクを改ざんしたとして証拠隠滅の容疑で逮捕された。同年10月1日には、当時の上司であった大阪地検元特捜部長O及び元副部長Sが、主任検事による故意の証拠の改ざんを知りながら、これを隠したとして犯人隠避の容疑で、それぞれ逮捕された事件である[9]。この事件で求められたのがPCデータの復元・解析技術である。デジタルデータの証拠を調査し、消されたデータを復元するデジタルフォレンジックス技術により証拠データを抽出した。

デジタルフォレンジックスが注目されたのはこの事件がきっかけではない。既に、2006年のライブドア事件や2011年に発覚したオリンパス事件などで活用されていた技術である。

5.2　デジタルフォレンジックス技術と監査

（1）デジタルフォレンジックス技術

フォレンジック（Forensic）とは、科学的な手法を用いて法的な証拠を得るための鑑識調査や情報解析に伴う技術をさし、これまでは犯罪捜査や司法現場で実施していた。近年、サーバーやパソコンのほか、携帯電話やスマートフォンなどのモバイル端末、デジタル家電などの電子機器の普及に伴い、デジタルデータの蓄積が法的証拠をして重要な意義を持つようになり、デジタルフォレンジックスは、コンピュータや電子機器等に残る記録媒体のデータを収集・分析し、その法的な証拠性を明らかにする技術を指すようになった。

なお、デジタル証拠の完全性を維持するという要求に応じるために、ACPO（Association of Chief Police Officers：英国警察長協会）により発行された4つの指針に準拠している[10]。

①法執行機関またはそれらの代理人は、後に法廷で要求され得るコンピュータまたは記録媒体に保持されているデータにいかなる変更も施すべきでない。

②コンピュータまたはストレージ・メディアに保持されている原データにアクセスする必要があると判断する例外的事情のある場合、その者はそうする資格がなければならず、それらの行為の妥当性と意味合いを説明し、証拠を示すことができなければならない。

③電子的証拠に基づいてコンピュータに適用される全ての過程の監査記録または他の記録は、作成され保存されるべきである。独立した第三者はそれらの過程を調査し同様の結果を得ることができるべきである。

④捜査の担当者（the case officer）は法とこれらの原則が遵守されることを確実にする全ての責務がある。

（2）監査証拠を保全するデジタルフォレンジックス

電磁的記録データ（デジタルデータ）を改竄された場合、そのデータを復元させた技術が、デジタルフォレンジックス技術である。これは、監査証拠の保全でもある。また、デジタルフォレンジックスは、不正アクセスや機密情報漏洩など、コン

ピュータや通信ネットワークに直接関係する犯罪における捜査手法として注目されているが、企業や組織になかでも、ICT の高度利用にともなって、外部からの侵入やデータの改竄がないか、システム監査の証拠集め、情報セキュリティ監査や安全対策の面からも重要な技術となってきている。ディスクフォレンジックによりアンチウイルスソフトやセキュリティ機器で検知できないマルウェアを見つけることができる。特にマルウェアの検知の方法を応用して、発見されにくい標的型マルウェアや、ファイルをもたないマルウェア（ファイルレスマルウェア）の検出が有効である。

6．おわりに

情報システムの高度化と多様化で、より客観的に評価し助言や勧告をするシステム監査は、「多様性」を求められている。

本稿は、まず、情報システムの発展とシステム監査の関係を俯瞰した。そして、筆者が、特にシステム監査の実効性に大きく影響を及ぼしたと考える近年のコンピュータ事故や犯罪等を取り上げて、システム監査との関わりについて考察するとともに、その論点について論述した。論述した情報システムの脆弱性をはじめ、個人情報の保護、サイバーショピングの法･制度問題、デジタルフォレンジックス等は、システム監査に重要な影響を及ぼした関連事項の一部である。その一方で、予測もできないコンピュータ事故や犯罪が激増し、情報システムの安全対策や信頼性の向上対策について強く求められるのである。筆者は､情報セキュリティ対策やリスク対策等の向上とともに、システム監査の実効性を高めるためには、コンピュータ事故や犯罪がどのように影響するのか、特に法的な問題について調査・分析し、継続的なシステム監査技術の向上に努めていく。

【注釈】

[注 1] IT と ICT はともコンピュータと通信を活用した技術・産業・サービスの総称であるが、ICT は「Communication(通信)」を要素として明示的にした名称である。日本政府は 2000 年半ばまで、IT を使っていたが、以降 ICT を使うようになった。筆者は IT と ICT をほぼ同義に使っているが、峻別しているのは使われた時代に合わせるためである。

[注 2] 脆弱性分析とは、情報システムを構成する要素が、どのようなコントロールがなされ、その状態を分析することである。 手順は、①情報システムの構成要素（ハードウエア、ソフトウェア、設備機器等）を明確化、②それらの機能の洗い出し、機能がどのように活用（どのような業務でどのように使用）されているか評価、③コントロールの状態調査、④脆弱性の評価である。

【参考文献】

[1] 宇佐美博著 「システム監査の歴史について」 愛知大学情報処理センター 2001
[2] 日本公認会計士協会編 「EDP 監査の進め方」 (財）大蔵財務協会 1976
[3] 松田貴典著 「情報システムの脆弱性」 白桃書房 1999
[4] 松田貴典著 「ビジネス情報の法とセキュリティ」 白桃書房 2005
[5] 総務省ホームページ「脆弱性」 2017.8.20 http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/11.html
[6]「減収 150 億円！ ジャパネットの「責任の取り方」 日経電子版「出世ナビ」 https://style.nikkei.com/article/DGXMZO2017.8.28
[7] 松田貴典編 芝隆･辻野武･城順平･金子清美･黒木啓良著 「コーポレートレピュテーション戦略」 工業調査会 2007
[8] 総務省「通信動向利用調査結果（平成 28 年)」 2017.8.20 http://www.soumu.go.jp/menu_news/s-news/01tsushin02_02000112.html
[9] 大阪地検特捜部主任検事証拠改ざん事件 ウィキペディア https://ja.wikipedia.org/wiki/ 2017.3.10
[10]「デジタルフォレンジックス」ウィキペディア https://ja.wikipedia.org/wiki/ 2016.12.18