『地域政策研究』（高崎経済大学地域政策学会） 第８巻 第１号 2005 年７月 69 頁～ 90 頁

我が国の情報セキュリティの現状とその対策に関する考察

筑 後 一 郎

A Theoretical Consideration of Current Information Security in Japan and Measures to Take

Ichiro CHIKUGO

目 次

Summary

In this research, to prevent any information-leakage, which has been seen often these days, I had carried the examination based especially on organizational approach.

In Ⅰ, we discussed the problem of information-leakage which is caused by the inadequate organizational, and picked up some principal information-leakage incident as examples to analyzed.

In Ⅱ, we pointed out that the developmental process of information orientation, although the enterprise and the self-governing community as for developmental process differs, the fundamental organizational problem pointed out does not differ. Furthermore, addition to the investigation and analysis of information security consciousness, not necessarily is the primary factor of the information-leakage been observed, and rather that the consciousness with the hard side is stronger.

In Ⅲ, we introduced several security management systems in order to prevent information-leakage, especially based on the framework of "support person" which Sauer has pointed out, and we tried to create the framework to organizationally prevent the information-leakage.

Based on that, we have concluded with some additional information, based on the examples of plans formed to increase the organizational security consciousness in IV.

はじめに

近年、情報化の進展に伴って、個人情報を管理することが容易になってきた。企業・自治体を問わず、情報のオンライン化、データ・ベース化の推進により個人・機密情報の管理が容易になりつつある。一方、本来は適切に管理されなければならないはずの個人・機密情報が、各方面で漏洩・紛失したという情報漏洩事件が多く発生しており、その報道も後を絶たない。ここでいう個人・機密情報とは、たとえば顧客に関わる情報や、住民票にまつわるデータ、または当該組織における機密性の高い情報等をいう。そうした個人・機密情報には氏名、住所、電話番号、生年月日などの個人属性を示す情報が多く含まれており、もしこれが外部に流出したとなれば様々な面で悪用されかねないという問題をはらむわけである。

そのため、個人・機密情報が一度流出してしまうと、企業・自治体を問わず、組織に大きな損害をもたらすこととなる。こうした問題は、金銭的に解決できるものではなく、個人情報を漏洩してしまったがために、当該組織に対する不安の増長や信用の失墜は、回復するまでに多くの時間がかかることはあえて指摘するまでもないことであるが、残念ながら今もなお多くの組織で個人・情報が漏洩したという報道が後を絶たないのである。

一方で、各組織に存在するコンピューター・システムには、ウイルスや外部からの進入を防止するためのセキュリティ・システムが整ってきた。すなわち、ウイルス感染防止に不可欠であるワクチンや、インターネット等の外部から進入を防止するためのファイア・ウォール（fire wall）の設置は進んでいる。情報漏洩の原因としては、こうしたシステムの不備や弱点を突いて、何者かが情報を取得し漏洩させるというシステム不備が原因の場合と、組織内部の何者かが情にアクセスし、それを外部に流出させるという組織が原因の場合と、大きくは２つの原因があると言われている。ところが、ウイルスや外部進入による情報漏洩はそれほど発生していないにもかかわらず、組織の内部者が情報を漏洩している事件は増加を続けているのが現状なのである。

このような背景をふまえ、2005 年 4 月より、いわゆる「個人情報保護法」の完全施行[1)]に至った。個人情報の保護に関し、法である程度規定するまでに至ったのは、こうした背景があることによる。

そこで本稿では、現在個人・機密情報が漏洩するリスクがはらむ我が国において、そうした情報をどのような形で組織的に防ぐ方策を見いだすか、過去に発生した情報漏洩事件やデータ等を用いながら、とくに組織的観点からのアプローチをもとに明らかにするものである。まずⅠでは、情報漏洩が起こる背景を、地方自治体と企業の３つのケースで検討し、その上で組織的観点からの問題について析出する。Ⅱでは、その問題点を受けて、情報化の発展過程とそれに伴う組織的なセキュリティの意識についてアンケート結果をふまえた上で検討する。Ⅲでは、セキュリティ保護が叫ばれるようになる前からの世界的な動きを背景にして、情報セキュリティを組織で確立するためのフレーム・ワークを呈示する。Ⅳでは、情報セキュリティを後ろ向きではなく、前向きに整備し、強みへの転換に成功した事例を検討し、考察を加えた上でむすびにかえたいと思う。

Ⅰ　情報漏洩とは

（1）情報が漏洩する背景

個人・機密情報は、はじめにでも述べたように、組織外の者が流出させる場合と、組織内の者が流出させる場合の、２つのパターンが存在する。まず第 1 に、組織外の者が情報を流出させるパターンであるが、これは当該組織のコンピューター・システムのハードウェアやソフトウェアに対し、適切な外部進入阻止対策を施していなかったために、外部の者から情報を読み取られ、流出してしまうということである。たとえば、2003 年 11 月に、（財）コンピュータソフトウェア著作権協会が保持していた著作権等の相談窓口で収集した個人情報（氏名、住所、職業、相談内容など）を、インターネット上で誰でも読み取れる状態で放置し、その情報を漏洩してしまった事件[2)]や、2005 年 5 月に株式会社カカクコムの掲示板がウイルスの侵入に遭い、メールアドレスが不正に流出した事件[3)]などがあげられる。この２つの事件に共通しているのは、コンピューター・システムの管理を適切に行っていなかったために、外部に情報を流出させてしまう結果となったことである。一般に、このような問題は、コンピューター・システムを適切に管理すること（たとえば、ウ

イルス・ワクチンを導入したり、ファイア・ウォールを設置したり、定期的に外部からの侵入がないか通信ログ（log）を確認したりする、など）で、ある程度防ぐことが可能となった。そのため、組織外の者が情報を漏洩・流出させる事件は、それほど多く発生していない。

一方、組織内の者が情報を漏洩させるパターンは、組織内部の人間が、事業遂行に必要な情報を得るための権限を持って（あるいは組織で適切な権限管理がなされなかったために）、組織内に蓄積される情報を取り出し、それを外部に流出させるものである。近年、多くの組織が情報漏洩事件として報道されるのがこのパターンであり、社会問題となっているものである。このパターンでの情報漏洩は、必ずコンピューター・システムの内部に漏洩させる者が存在し、情報を漏洩させて、組織に対し多大な損害を与えるものである。本稿では、とくに組織内部者が情報を漏洩するパターンに注目し、以下、代表的な３つの事件を（２）と（３）で要約することにする。

（２）地方自治体の情報漏洩事件（高木（2004））[4)]

自治体レベルでの大規模な情報流出事件は、京都府宇治市の事件が最初である。1998 年、宇治市が発注した乳幼児検診システムの開発にあたり、発注元の孫請け企業が約 21 万人分の住民基本台帳と外国人登録台帳の電子データを受け取った。そのデータを孫請け企業の派遣社員が高磁気ディスク（MO ; Magnet Optical disk）へ複写し、大阪府の名簿業者に約 26 万円で売り渡した。

1999 年 5 月、京都新聞の記者が宇治市に対し「情報が漏洩しているのではないか」との問い合わせで発覚した。流出したデータには、個人連番の住民番号、住所、氏名、性別、生年月日、転入日、転出先、世帯主名、世帯主の続柄等の個人情報が記録されていた。それら情報が漏洩したのは宇治市の監督不行届きが原因であるとして、宇治市議ら市民３名がプライバシー侵害による損害賠償を提訴し、2001 年 12 月、京都高裁が情報漏洩の損害を 1 人 15,000 円と算定し、判決を下した。その後最高裁まで争われたが、宇治市の上告を棄却し、上記内容で損害賠償裁判は終結した。

この事件では、市民全員の住民データがすべて外部に流出してしまった事件として非常に重要な事件となった。以後、地方自治体で情報管理が厳しく問われるようになり、総務省が各自治体に対し対策を講じるよう指示するようになる。

（３）企業の情報漏洩事件（高橋（2004））[5)・6)]

企業の情報漏洩事件は非常に多い。なかでも、情報通信産業や通信販売業といった、情報化社会には不可欠な企業が大規模な情報漏洩事件を起こしている。

まず情報通信事業の事件として、ソフトバンク BB 社（以下、SBB 社と記す）の情報漏洩事件が大規模な漏洩事件として報道された。当初、SBB 社は、自社の行う情報通信サービスの顧客名簿が 242 名分漏洩したとして 2004 年 1 月に発表した。その後、顧客情報を用いて恐喝しようとし、情報漏洩を行った犯人が逮捕されたが、同年２月、漏洩した情報はほぼすべての顧客分と退会顧客の名簿併せて約 452 万人分であることが発覚した。国内ではこれが最悪の情報漏洩事件となっ

た。

SBB 社は、情報漏洩に対する顧客へのお詫び（約 40 億円分の金券を発送した）と、情報漏洩の問い合わせ窓口のための人件費や、情報漏洩防止のためのシステム改修に乗り出し（約 400 億円）、社長が記者会見で陳謝した。しかし、その後 IP（Internet Protocol）電話サービスの通話記録が約 9 万人分流出していたことも後に判明し、同年 7 月、総務省が SBB 社に対し行政指導を行うこととなった。総務省が民間企業に対し、適切に情報管理を行うよう指導したことは、極めて異例なことだった。

また、通信販売業として有名なジャパネットたかた社（以下、たかた社）は、2004 年 3 月、全国紙の新聞記者から 149 名分の顧客情報が漏洩しているのではないかとの指摘を受け、情報漏洩が発覚した。漏洩した情報は、氏名、性別、住所、電話番号、生年月日、年齢の各個人情報である。原因は、各個人情報が記録された磁気テープが内部者により持ち出され、漏洩したことが分かった。そのためたかた社は、事態が収束するまで 49 日間営業を自粛し、地元の警察署に磁気テープを盗まれたとして告訴した。その後、たかた社の元社員が倉庫内の物品を窃盗したとして逮捕され、情報漏洩事件についても追及したが、結局情報漏洩に関する事件では不起訴となった。たかた社は最終的に、51 万人分の顧客情報が漏洩し、それに伴う営業損失は約 150 億円にのぼることが明らかとなった。

井上（2005）は、たかた社の社長にインタビューし、セキュリティに対する人材を社内で確保していなかった点、漏洩当時は情報システムの運用を専門企業に委託していたが、セキュリティ対策に関してはほとんど施していなかった点が漏洩した根本原因であることを指摘したと述べている。すなわち、組織的に情報セキュリティを堅固にするための施策を打てなかったことが、情報漏洩を引き起こした最大の問題点であったということである。

（4）情報漏洩事件の組織的観点

上述した情報漏洩事件は、すべて組織の内部者が漏洩に関わった事件である。すなわち、組織的に情報セキュリティが確立しておらず、適切な情報管理がなされなかったために内部者が情報を漏洩させてしまった事件といってよい。注目する点として、上記 3 件の情報漏洩事件は、情報そのものを情報提供会社へ売り渡したり、情報を持っていることで恐喝事件を起こしたりといった、情報をカネに変えようとする行為が共通している点である。情報は、その性質からすぐにカネに代えられるだけの価値を持ち合わせた資源である。本来ならば、組織の重要な資産である情報に対し、漏洩させないようにすることはもちろんであるが、適切に管理するだけの人材や資金を投じるべきものである。ところが上記の事件では、そうした対策は取られなかった。そのため、大規模かつ重大な情報漏洩事件を引き起こしてしまったのである。

情報漏洩対策は、コンピューター・システムの適切な管理と同程度に、組織内での情報セキュリティ対策が必要となる。もし一度でも情報漏洩事件を起こしてしまったら、次に掲げる「コスト」

を組織が負担することになると思われる。すなわち、情報漏洩事件が発覚した以後のセキュリティ対策費、臨時コールセンター等の人件費、被害者に対するお詫び料や損害賠償、売り上げの減少、信用の失墜、などである。

金銭的なコストとしては、たとえば宇治市の情報漏洩事件に対し、もし漏洩された市民全員が損害賠償を請求したと仮定すると、判決通りの支払いとして約 31.5 億円の支出が求められる。また、SBB 社では判明している損失だけで約 440 億円、たかた社では 150 億円ものコストが発生したことになる。金銭的なコストだけでも相当の負担が生じることになるため、場合によっては一度情報漏洩事件を引き起こしてしまうと、その組織自体の存在を危ぶまれることとなる。

また、金銭的コスト以上に、信用の失墜というコストは計り知れない。当然のことながら、一度信用を失うと、それを回復するまでに相当の時間が必要である。そのため、一度でも情報漏洩を引き起こしてしまうと、金銭的コスト以上に組織の信用に関わる問題に発展し、回復を図ることが極めて困難である。その意味では、情報セキュリティに対する組織的かつ包括的な対策が必要であると考えられる。すなわち、情報漏洩を引き起こさないための包括的アプローチとして、組織的観点からの考察が不可欠であると考えられるのである。Ⅱでは、こうした組織的観点からの考察と、アンケート調査による情報セキュリティの組織的浸透度について検討する。

Ⅱ　情報化の発展とセキュリティ意識

（1）情報化の発展過程

我が国における情報化―とくに、業務をコンピューター化すること―が行われた背景には、次の理由が考えられる。第 1 に、情報化が進んだ背景には、インターネット（internet）やイントラネット（intranet）の普及に伴うネットワーク化が大いに貢献したことが指摘できる。1990 年代までのコンピューター・システムとは、大型の汎用コンピューターが大量のデータを処理するように作られていた。そのため、情報を処理するための専門の人員が確保され、また集約することも高度な知識・技術が必要であった。また、各汎用コンピューターはそれぞれ独自のデータ処理機能を形作っていたために、非常に限定的で柔軟性のないデータとして各システムに格納されていたのである。

1990 年後半に入り、インターネットが驚異的な速度で普及し始めた途端に、これまでの主力だった大型汎用コンピューターが徐々に影を薄め、かわりに分散化させてデータを蓄積するためのサーバー（server）・システムが登場するようになった。すなわち、ネットワークによってデータを分散して保存・蓄積することが可能となったために、情報の加工が各組織により自由にできるようになったことが、現在の情報化に大きく寄与したわけである。一方、サーバーに蓄積された情報は、ネットワークで相互交換を容易にするために、比較的柔軟なデータへと変わっていった。ネットワークをつうじてやりとりされるデータが、それぞれのシステムで適応できるように加工することも容易になったのである。そのため、データを漏洩してしまうと、漏洩したデータを第三者が容易に加工

して配布できるようになる懸念が生じることとなる。

また、データの分散化により、当該組織成員がクライアントを用いて情報にアクセスできるようになったことも大きな変化である。先述したように、大型汎用コンピューターでは、データを加工できる人員はごく一握りのシステム要員に限られたわけであるが、データの分散化によって様々な加工を組織内部の人間が行うことを可能にした。そのため、データ分散による自由な情報加工を促すきっかけにはなったが、進化する情報システムに対応できず、組織的な情報セキュリティの確立が立ち後れてしまったことは否定できないと思われる。

（2）発展過程の相違

上述した事実をふまえ、島田（2001）は、民間企業と自治体では異なった情報システムの変遷があると指摘する。**図表・1** のように、組織文化、人的資源管理、調達、予算に分け、民間企業と自治体の情報システム発展過程の変遷を対比している。ただし、この表はあえて民間企業と自治体とを比較するために作られた表である点に注意する必要がある。

島田によれば、第 1 に、組織文化の比較では、民間企業がリスク・テーキング指向、外部指向、横割指向であるのに対し、自治体組織では安全性指向、内部指向、縦割指向であるといったように、大幅に異なる。民間企業は、情報システムの開発や改良はリスクをある程度加味し、システム構築を行うのに対し、自治体組織では安全性、すなわち情報システムの開発・改良に対して慎重である点が指摘できる。自治体では、情報システムの技術革新に対しては冒険をせず、他で評価が定まった技術についてのみ導入し、リスクを引き受けて失敗するよりも、安全で無難な方法によるシステム構築を推進する姿勢を示したものである。

また、縦割指向に関しては、情報が組織をあまねく行き渡るものであり、本来、縦割組織の都合で、当該組織にしか通用しないシステム構築を行ってはならないにもかかわらず、自治体内での各組織のみで通用するシステムを構築する傾向が強い。

内部指向については、自治体職員の交流が同質になっていることについて示したものである。すなわち、自治体職員の交流は、同様の仕事をこなす公務員同士での交流が多いため、異質な民間企業との情報交換や交流などの場がそれほど多くないことが指摘される。この内部指向は、公務員が民間企業との交流によって生じる懸念がある癒着を防ぐことが大きな理由となっているのであるが、現実にはその種の問題の対策を取ることは可能であると思われる。一般に、情報システムの技術革新が民間企業は早いため、そのノウ・ハウを取得することに大きな障害があることは、情報システムの発展にとって必ずしも有意義であるとはいえない。

第 2 に、人的資源管理での比較を行うと、民間企業と自治体では、ジョブ・ローテーション（job rotation）の長短による影響が大きい。それは、民間企業では専門性を高めるために、それぞれの職種で長い時間をかけて専門性を高める傾向がある。一方、自治体組織では、ジョブ・ローテーションが比較的早く、ゼネラリスト指向であるために、自治体における情報部門での専門性が高まらな

図表・1　民間企業と自治体の相違点

	民 間 企 業	自 治 体
組織文化	リスク・テーキング指向 外部指向 横割指向	安全性指向 内部指向 縦割指向
人的資源管理	スペシャリスト指向	ゼネラリスト指向
調　　達	多くは随意契約	多くは競争入札
予　　算	複数年度も可	原則として単年度

出所）島田達巳『情報システムのアウトソーシング―企業・自治体比較を焦点にして―』組織科学、Vol.35, No.1, 2001, pp.34

いといった問題があるという。換言すれば、自治体の情報部門は、情報システムの横断的・利用者指向的システムを開発する資源に乏しく、結果として情報システム企業の主導によるシステム構築が行われがちであるわけである。そのため、自治体では情報システムに関する仕様の策定を自らが行うことができず、導入したシステムについての評価もあいまいのままでシステムが構築され、結果として導入したシステムがシステム開発業者寄りのものになってしまい、利用する人間に対して難解なシステムになってしまうことが往々にしてあると指摘している。

第３に、調達するための契約方式について比較すると、民間企業は情報システム構築のための交渉力が強く、かなり精度の高い仕様策定の上で競争入札を行うのが一般的であるが、自治体組織では安全性の指向が強いために、事業者を選定するのにあたって、実績があり、信用のある企業に発注する随意契約のパターンを取ることが多い。そのため、情報システム開発企業は、実績づくりのために現実的には考えられないほど安価な入札を行い、後になって自治体組織が要求する追加システムの構築契約をつうじて利益を上げることを目指し、システム開発企業の意のままにシステムが構築されてしまうことが多く見受けられる。そのため、先述したように利用者にとって難解なシステムとなり、事後の評価も困難なシステムとなってしまうのである。

第４に、予算編成の観点からの比較であるが、民間企業はプロジェクトを組んで長期にわたりシステムを開発することができるだけの仕組みになっているが、自治体組織はほとんどが単年度で予算執行が収束するようなシステムになっており、大規模なシステム構築であるにもかかわらず、単年度で完了できるようにシステムを構築しなければならない限界がある。したがって、システムの開発は、単年度の予算配分の範囲内で遂行することを余儀なくされ、戦略的な志向に基づいた効果的・効率的なシステム構築や導入を困難にしている。

以上のように、民間企業と自治体では、４つの相違点があることを島田は指摘しているのであるが、とくに組織要員の観点で検討すると、確かに安全性を追い求め、内部完結型の各組織事情のみ

のシステムを構築することが限界点として指摘されることは理解できる。ところが、Ⅰで指摘したように、民間企業でも情報漏洩事件が発生している原因を探れば、どちらも情報システムについて専門的知見や技術を持ち合わせた組織成員が存在しないか、そのような組織成員を育てる仕組みがなかったために引き起こされたことが原因である。換言すれば、島田の指摘する相違点は確かに情報システムの構築に影響を及ぼす要因であるものの、組織の持つ資源を守るために必要な情報漏洩を防止するための根本的な観点については検討がなされていない。情報システムの構築をリードするために、それらシステムについて精通した組織成員を、組織がどのように調達するか、あるいは育てるかについて検討する必要があるのである。

（3）情報セキュリティの意識

前項で指摘したように、情報システムのセキュリティを高めるためには、情報システムに精通した組織成員の情報スキルの研鑽と育成が不可欠であると考えられる。そこで、ここでは国（総務省、2004）が行った情報セキュリティの意識調査について検討する。

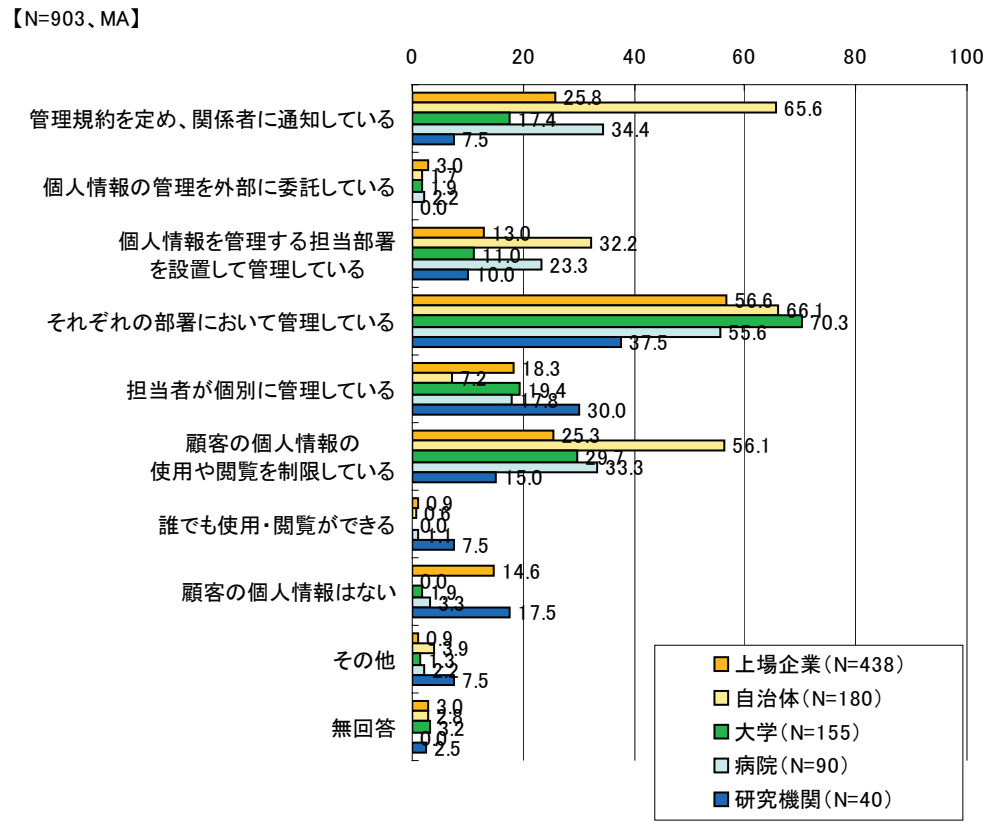
本アンケートでは、主に上場企業、自治体、病院、大学、研究機関の各団体に無作為でアンケートを送付し、回収した結果を示したものである[7)]。

個人情報の管理状況や、その方法について尋ねた調査結果を見ると、個人情報を管理する部署を設置して、包括的に管理している団体はあまり多くない。情報技術が進化しているにもかかわらず、多くは各組織に任せたままの運用になっており、組織的に情報漏洩を防ぐための組織づくりを行っていないことがうかがえる（**図表・2**）。一方、組織面・制度面でどのような対策を取っているかという点について質問した結果をみると、自治体組織を除き、個人情報の取り扱いに関する方法論が未だ明確に示されていないことが示されている。自治体以外の組織では、個人情報保護に関し「何も実施していない」と回答する割合が高いことや、事業体内での個人情報保護に関する教育が進展されていない点、さらに個人情報保護管理責任者の設置がきわめて低調である点などで、組織面・制度面での対策があまり進んでいないことがうかがえる（**図表・3**）。

先述したように、企業組織でも、自治体組織でも、専門的知見や技術を兼ね備えた組織成員が存在しない点を指摘したが、それを補うためにセキュリティ専門業者の助言や技術を取り入れるという方法も、一時的ではあるが情報の漏洩防止に効果的であると考えられる。その専門業者の利用動向を見ると、どの組織形態でも「専門業者を利用していない」という回答が過半数を超えることがわかる（**図表・4**）。組織内で情報漏洩防止のための人員も割けず、それをカバーするために外部のセキュリティ専門業者を利用することも低調であるという点は、今日多くの情報漏洩事件が発生し、報道されるという現象を如実に示す理由であると考えられる。

一方、各組織が国や地方自治体に対し、情報漏洩を防止するための施策としてどのようなものを望んでいるかについて見てみると、社員教育への助成や情報セキュリティに関する講習会等の開催といったソフト的―換言すれば、組織指向的対策よりも、セキュリティ侵害事案を取り締まる法整

図表・２　個人情報の管理方法

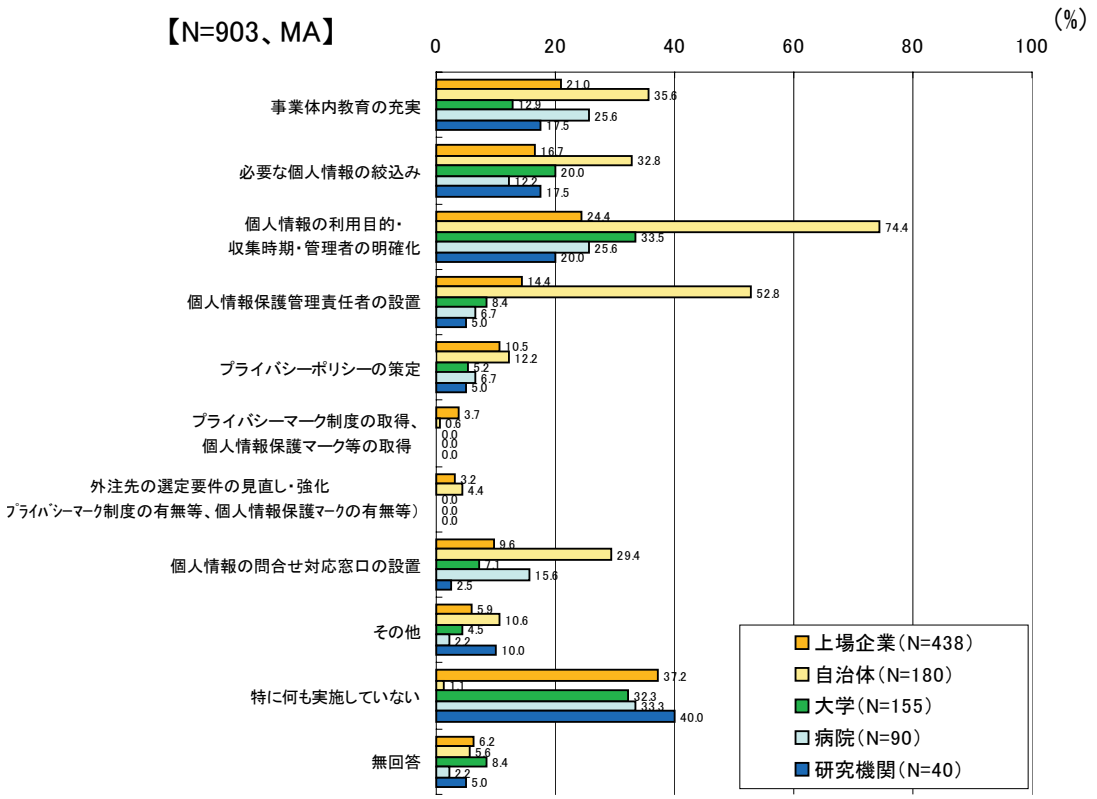


出所）総務省『情報セキュリティに関する実態調査』2004, pp.60。

備や、機器・ソフトウェア購入のための助成、セキュリティ・サービスを利用するための助成について推進してほしいという意見が多くあげられた（**図表・５**）。本来、組織を包括した情報セキュリティを構築することが最も望ましいのであるが、各組織の意識はハード面での充実を指向することが中心になっているようである。

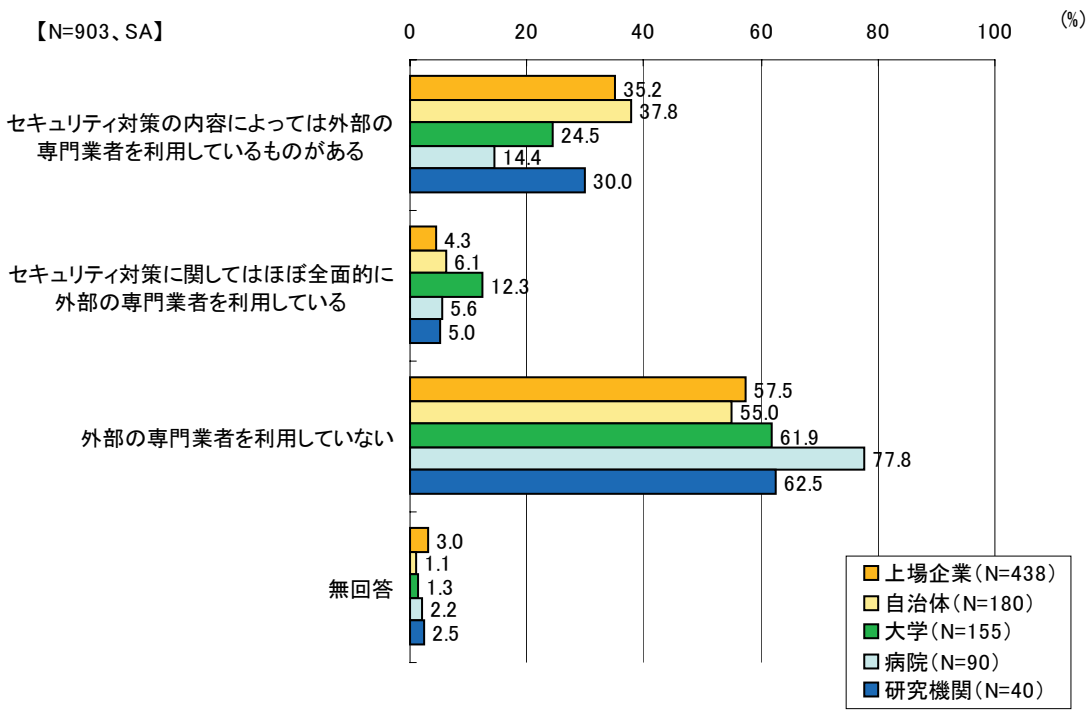
本アンケートで明らかになったことは、組織面・制度面に関する情報の保護に関する施策は、多くの組織で未だに注目されていないという点、組織的な情報の保護にいたる前に、ハード的な情報保護にようやく意識が向いた状況であるという点、各組織では、どのように情報を保護するかの意識が希薄で、それに伴う外部業者の助言や利用に至っていない点などがあげられると思われる。すなわち、情報システムに対する組織的保護施策が追いつかず、情報漏洩事件が多く発生しているのではないかという背景がうかがえるのである。情報漏洩を防ぐためには、情報システムを各組織が一定のコンセンサスを持って防ぐ手だてを講じなければならないのであるが、それについてⅢで検討することにする。

図表・３　個人情報保護に対する組織面・制度面での対策



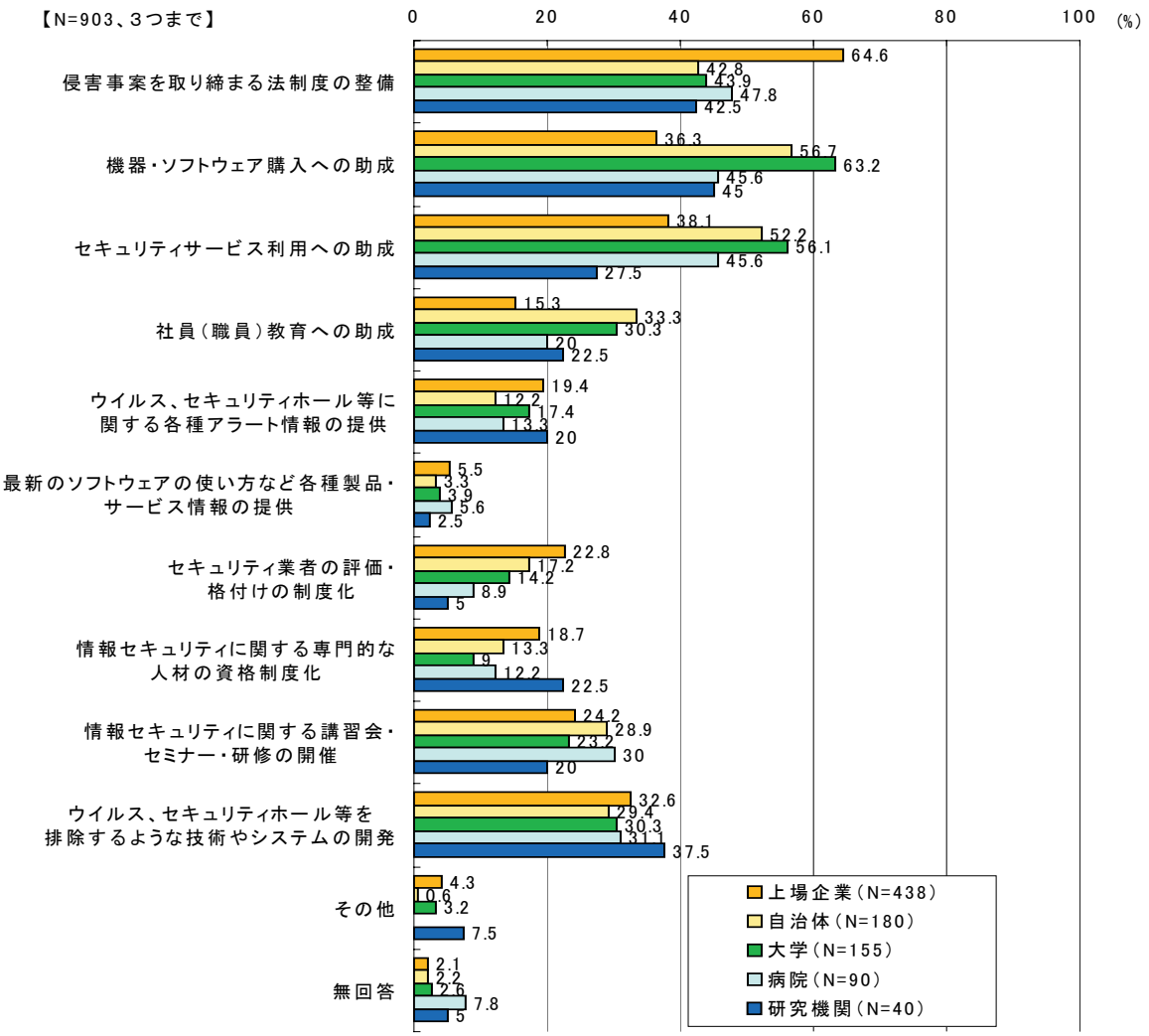
出所）総務省『情報セキュリティに関する実態調査』2004, pp.61。

図表・４　セキュリティ対策業者の利用有無



出所）総務省『情報セキュリティに関する実態調査』2004, pp.63。

図表・５　政府・地方自治体の支援施策への要望



出所）総務省『情報セキュリティに関する実態調査』2004, pp.203。

Ⅲ　情報漏洩を組織的に防ぐために

（1）情報セキュリティ保護の状況

情報漏洩はなぜ引き起こされるのか。この点については、組織的情報セキュリティの保護が不可欠であるのに、様々な問題から情報セキュリティ保持のための人材が確保できず、また組織的にも情報セキュリティを保護するための仕組みが整備されていないため、組織を問わず情報漏洩が発生しているという背景を指摘した。今日、情報漏洩事件が多く発生しているにもかかわらず、各組織では対策が進んでいるとは言い難い状況であり、情報システムに立脚したシステムでの管理を指向している組織が多数見受けられる点が主な要因ではないかと考えられる。一方で情報システムや、それに伴う技術のスピードに各組織が追いつけない状況であることも浮き彫りとなった。各組織は、情報セキュリティ保護のために、あまりに多くの知識や技術が必要で、その対策に膨大な時間や費用がかかるために躊躇しているのではないかと思われるのである。しかしながら、情報セキュリティ保護のための施策は、今日の我が国の状況をふまえると、あまり多くの時間をかけて検討するだけの余裕はないと考えられる。それは、すでに個人情報保護法の完全施行が始まった点や、情報漏洩に対する社会の厳しい目が向けられている点、情報漏洩で失う資源があまりに多い点など、多くのリスクをはらんでいることが理由である。すなわち、情報漏洩はもはや「対岸の火事」という出来事ではない。いつ、各組織に降りかかるか分からないリスクをできる限り低減させる必要があるのである。

情報セキュリティを規定するために、世界各国で様々な提言やシステムが構築されている。古くは OECD8 原則[8)] と呼ばれる情報セキュリティの基礎原則に始まり、ISO/IEC17799（BS7799）[9)]、JIS X 5080[10)] 等の規格が誕生し、セキュリティ保護に関する様々な提言が行われた。

例えば、OECD（1992）では、情報漏洩の防止を規定するための情報セキュリティについて、「情報の機密性、完全性、可用性を維持すること」と規定している。機密性とは、当該情報にアクセスを許された者だけが情報にアクセスできること、完全性とは情報・処理方法が正確かつ完全であることを保護すること、可用性とは認証された者が必要なときに情報や関連する資産にアクセスできることを示している。換言すれば、当該情報にアクセスするための資格を管理し、認証された者が必要な時にいつでも情報関連資産に正確・完全に情報を扱うことができることが情報セキュリティであると定義したのである。ここでの視点として、「認証された者」という部分が重要である。各組織には様々な情報資産が蓄積・利用されているのであるが、不必要かつ情報の漏洩が懸念されるものまでを全員が共有する必要はない。たとえば顧客や住民などの個人に関わる情報は、必要な「認証された」者だけが扱えればよい。すなわち、不必要かつ漏洩しては困る情報には、適切なアクセス権限の管理が組織的に必要となるのである。

その 10 年後、OECD（2002）は、組織で情報を保護するために不可欠であるマネジメント、す

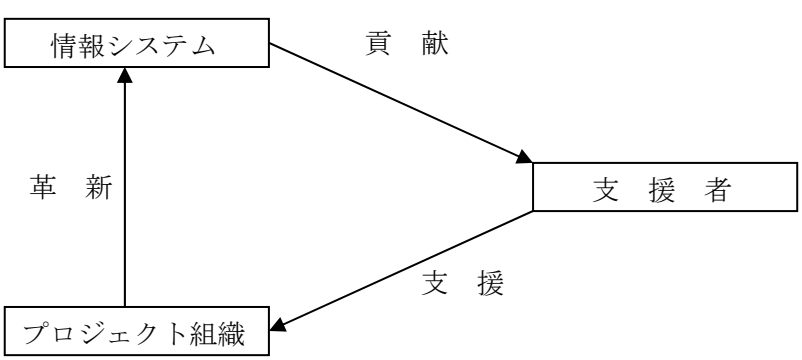
なわちセキュリティ・マネジメントについても定義した。セキュリティ・マネジメントとは、「情報システム、ネットワーク・セキュリティ・ポリシー、慣行、（効果）測定、手順が、セキュリティの首尾一貫した方式（coherent system）を作成するために調整・統合されるもの」であるという。すなわち、セキュリティ・マネジメントを遂行するためには、ただ組織の細則（policy）を策定するだけでなく、全組織的に調整・統合されて浸透するものでなければならない。そのため、組織横断的なマネジメント・システムの構築が不可欠であることを指摘しているのである。

（2）情報システムの効果的な構築

情報システムの組織横断的な策定をめぐって、Sauer（1993）のフレーム・ワークは重要な指摘を与えている。彼によれば、オーストラリアにおける巨大な情報システム（Mandata）開発についての失敗に関する事例研究をもとに、3つの要素が依存していることを指摘した（**図表・6**）。これによると、「情報システム」は、「プロジェクト組織」の活動によって構築されるものの、プロジェクト組織は各種の資源が必要となる。そこで、構築された、あるいは構築されつつある情報システムが貢献する限りにおいて、資源を投入してくれる「支援者」の役割を重視する。支援者はプロジェクト組織を支え、プロジェクト組織がその支援をもとに情報システムを革新し、革新をはかったシステムが、やがて支援者に対して貢献をもたらすという仕組みである。

言い換えれば、情報システムはプロジェクト組織が作成するものの、支援者の存在なくしては貢献することがないわけであるから、支援者はプロジェクト組織に対して積極的に働きかける必要がある。この支援者のなかには、情報システムを活用するユーザーのほか、情報システムの構築を手助けする情報技術者や情報システム企業などが含まれると考えられる。Sauer は、こうした依存関係に基づいてシステム構築を行うべきであると主張しているのである。

図表・6　Sauer 依存の三角形モデル



出所）Sauer, Chris, Why Information Systems Fail: A Case Study Approach, Alfres Waller Ltd., 1993. 澤田芳郎・鈴木整・宇都宮肇訳『情報システムはなぜ失敗するのか　事例研究アプローチ』日科技連出版社、1995、pp.45。

Sauer の指摘した三角形モデルをふまえた上で、我が国の情報システムの状況を検討すると、「支援者」にあたる層が薄いことに課題を見いだすことができると思われる。というのも、各組織における「支援者」にあたる各ユーザーや、情報システム企業の協力を受けにくいことが、Sauer の言うところの情報システムの「失敗」を意味しているからである。彼は「支援者から支援を与えられなくなった」場合を、情報システムが「失敗した」と定義している。それは、各ユーザーや情報システム企業、あるいはシステム技術者からの支援・助言がないままに作られていくシステムがあまりに多いことで、当該システムが「情報システム」として機能不全を起こしているからにほかならない。こうした問題を回避するために、組織横断的なマネジメント・システムの構築が求められるのである。

（3）情報セキュリティを組織で確立するために

セキュリティ・マネジメントは、組織横断的で一貫したシステムである必要がある。世界的に情報セキュリティの保護が叫ばれるようになったことから、わが国でも（財）日本情報処理開発協会（Japan Information Processing Development Corporation ; JIPDEC）が、JIS X 5080 の内容を踏襲した ISMS（Information Security Management System）と呼ばれる情報セキュリティ・マネジメント・システムを策定した。それによると、ISMS とは、組織が「保護すべき情報資産、リスク・マネジメントに対する組織の取り組み方法、管理目的および管理策の内容、保護すべき情報資産に要求される保証の度合い、以上 4 つの事項を明らかにすることである」と定義している。これら 4 点を明らかにすることにより、情報リスク管理が有効かつ効率的な状態に維持できているという証明になると言う。

ISMS は、これまでのハード的なセキュリティ保護モデルをさらに拡張し、組織が 4 つの要素について明らかにすることを求めたものである。情報資産、組織の取り組み、管理目的・管理策、情報資産の保証の 4 点は、情報セキュリティを保護するために必要な視点を包括している。資産を洗い出し、その資産をどのように管理するか、組織内での取り組みを明文化することで情報資産を保証するというこの仕組みは、各組織が情報セキュリティを保護するために必要な視座を与えていると考えられる。

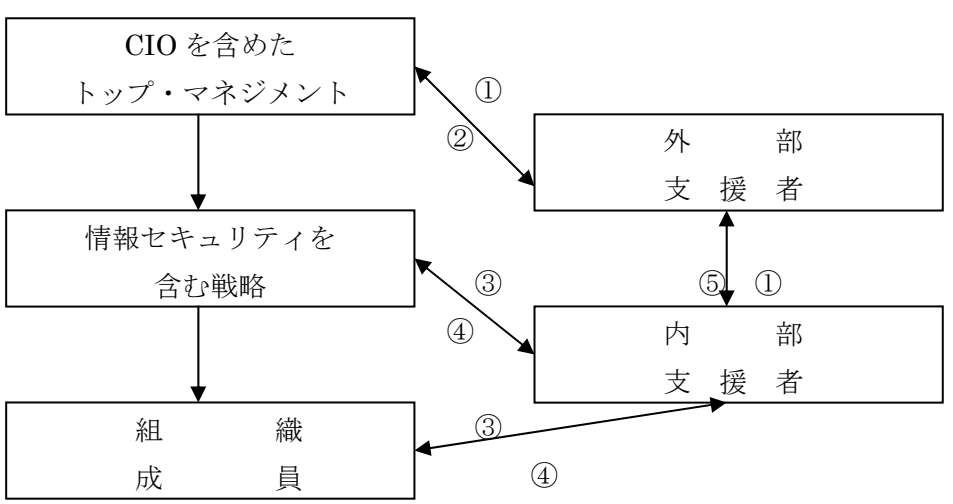
一方、わが国以外での流れとして、アメリカにおける CIO（Chief Information Officer）の考え方が浸透している。CIO とは、吉川（2004）によれば、1996 年頃に米国総務庁（General Services Administration ; GSA）と米国行政管理予算局（Office of Management and Budget ; OMB）に設置された CIO カウンシルの協働プロジェクトとして、認可を受けた大学が大学院レベルでの高度な教育コースを設置したことが始まりだという。これら大学院を CIO 大学と呼び、Carnegie Mellon University のほか 7 つの大学が認定を受けた。現在では、CIO は大学院レベルで高度な講義を受け、リーダーシップ、戦略と立案、IT（Information Technology）マネジメント、IT の習得とプログラム・マネジメントなどといった各種 IT 教育プログラムを習得することができるよう、カリキュラムが

組まれている。わが国でも、2004 年頃から早稲田大学、金沢工業大学、大阪市立大学、名古屋商科大学等で CIO プログラムの設置に動いており、情報セキュリティ意識の高まりを背景に、全国に広まりつつある。

アメリカではすでに 10 年近くの歴史があるため、情報システムに明るい意思決定に携わる組織成員が増えつつあるが、わが国ではその取り組みがまだ始まったばかりである。そのため、CIO といった専門的人材を育成することは、しばらく時間がかかるだろうと考えられている。すなわち、組織内での人材育成には、これからも多くの時間をかけて育てていかなければならず、個人情報保護法が完全施行になった今、それを待った上での情報セキュリティ保護を推進する、といった動きでは手遅れである。

そのため、情報セキュリティに対して広範な知識と技術が必要だと思われる資源を、一時的に外部の専門組織の力を借りて構築・整備し、それらシステムの意思決定のための人員を確保する必要がある。また、トップ・マネジメントから情報セキュリティ保護を含めた戦略を策定し、それが組織にまで浸透する流れのなかに、Sauer の指摘するところの内部支援者（各ユーザーや情報セキュリティ部署、システム構築部署）と外部支援者が互いに関与し、協力するための仕組みと、その結果をフィードバックさせる仕組み構築することが求められる。さらに、戦略的に組織へ情報システムを浸透させるために、情報セキュリティを含めた組織横断的情報システムの構築を戦略と結びつけることが不可欠である。上述した内容をフレーム・ワークとして考えると**図表・7**のようになる。

図表・7　情報セキュリティを意識したシステム構築フレーム・ワーク



①知識・技術の提供
②取引関係の構築
③情報システムへの関与
④組織・情報システムにフィードバック
⑤協力関係の構築

このように、情報セキュリティを保護しながら、効率的なシステムを構築するためには、「支援」する当該成員や企業が積極的に関わるための組織づくりを遂行する必要があると考えられるのである。内部支援者と外部支援者が有機的に結びつき、それぞれが互いに関与し、情報システムに影響を与えるならば、セキュリティを保護した情報システムでありながら、システムの有効性をも含めた情報システムを構築することが可能になると考えられる。Ⅳでは、内部と外部の支援者が有機的に関与し、情報システムを構築している事例を取り上げる。

Ⅳ　情報セキュリティを組織の強みへ

Ⅲでとりあげた情報システムの効果的な管理と構築は、それほど多くの企業で行われているわけではない。本章では、先進的な取り組み事例としてキヤノンソフトウェアをとりあげることにする。

キヤノンソフトウェアは、カメラ、複写機といった製品向けの組み込みソフトを主に作成している企業である。同社は、単にセキュリティ対策の方針や手続きなどの手順を決めるだけではなく、「どうしたら現場が対策を徹底できるか」という点を中心に活動してきたという（井上（2005））。

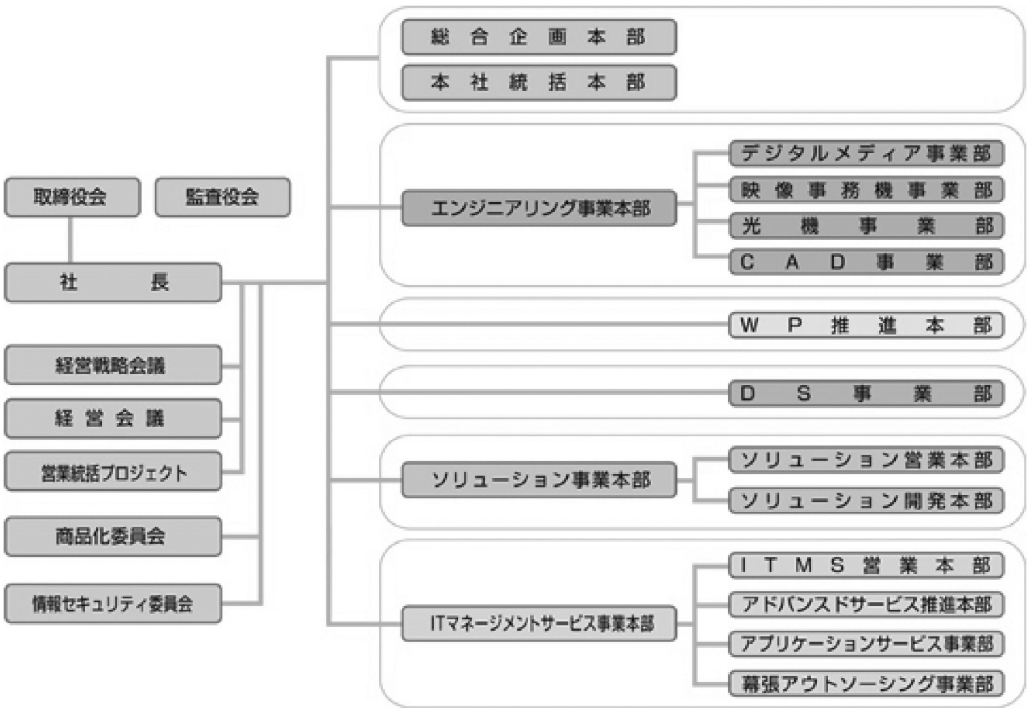
同社は、まずトップ・ダウンでセキュリティ保護活動を推進した。ソフトウェア開発企業としては初めて、2002 年に JIPDEC の ISMS（Ver.1.0）と、BS7799 の認証を取得した。その一方で、「セキュリティ活動を現場にポジティブに受け入れられるためにはどうしたらよいのか」という点に着目し、当時の CISO（情報セキュリティ統括責任者 ; Chief Information Security Officer）が企業ブランドの一部として「セキュリティ活動」を売りにするための顧客満足度調査に着手した。

それとともに、同社では、現場の管理職で構成する「情報セキュリティ委員会」を組織した（**図表・8**）。これは、社長直属の組織であり、経営戦略会議や商品化委員会などといった、企業活動を左右する組織と同格の扱いとなっている。情報セキュリティ委員会は、どこかで情報が埋もれてしまうことを防ぐため、現場ミーティングを習慣化させている。このミーティングは月に 1 度行われ、数人から数十人の課単位で、外部派遣社員も含めたミーティングを開き、浮かんできた疑問や課題をレポートにまとめ、情報セキュリティ委員会に提出するという。ここで提出された課題や疑問を整理して、翌月のミーティングで返答するという活動を行っている。また、機密書類を山積みにしたまま席を離れる社員や、コンピューター・システムを誰でも閲覧可能な状態にしている社員に対し、「セキュリティ推進部」の社員が巡回し、それぞれ注意を促しているという。

このように、コンピューター・システムだけでなく、いわゆる組織に内在する広い意味での「情報セキュリティ」を遵守する徹底的な取り組み（**図表・9**）により、親会社のキヤノンをはじめとし、セキュリティに関する顧客満足度は他の企業と比較にならないほどの評価を受けるまでになったとのことである。

キヤノンソフトウェアの取り組みは、単に情報システムだけで完結することのない組織的情報セキュリティ・システムを実現している。情報セキュリティについて話し合う組織をトップ・マネジ

図表・8　キヤノンソフトウェアの組織図



出所）キヤノンソフトウェア　ホームページより取得
（http://www.canon-soft.co.jp/company/organization.html）

図表・9　キヤノンソフトウェアの情報セキュリティ

現場が前向きに取り組める目標の設定	・セキュリティを「売り」にする企業戦略 ・顧客満足度調査へ「セキュリティ遵守度」の項目を設定
現場にセキュリティ関連の活動を浸透	・2 ヶ月に一度、セキュリティ関連のミーティングを現場で実施 ・業務に即したガイドラインを全社で共有し、社内教育で確認 ・事故が発生した際の連絡先カードの携行を徹底
危機感・緊張感の醸成	・毎月、ミーティング日に CISO が自社内外の事故等を紹介するメールを全社員に送信 ・セキュリティ推進部の社員が現場の見回り、外出時にセキュリティ上問題のあった社員に注意を喚起

出所）井上健太郎『個人情報保護法完全対策』日経情報ストラテジー、日経 BP 社、2005.02、pp.41 の図表を一部修正。

メントの直下に置き、情報セキュリティの責任者を設置した上で、組織全体に情報セキュリティの保護が行き渡るための施策を工夫している。たとえば、外部派遣社員を含めた協力者である社員から、巧みに組織内に蓄積する問題点を引き出すことに成功している点があげられる。これは、組織に属する個人が日頃考えている問題や、自分では気がつかなかった「セキュリティ意識」の醸成に役立っていると考えられる。また、情報セキュリティの保護を徹底させるため、各部署に情報セキュリティ担当者が抜き打ちで見回っている点も、社員が普段何気なく扱っている情報がいかに機密性の高いものであるかを改めて認識させることに結びついている。重要なのは、徹底がなされていないからといって叱責するのではなく、あくまでも情報セキュリティを保護するために必要な施策であるということを情報セキュリティ担当社員が説いて回ることにあるという。言い換えれば、地道にセキュリティ意識を高めるために、外部・内部を問わず社員全体がともに考え、トップ・マネジメントと結びついてセキュリティ保護意識の向上をはかっていることが、セキュリティ保護に関する顧客満足度を大いに高めている原因となっているのである。

むすびにかえて

本稿では、情報化の進展により新たに発生した情報漏洩の防止について、組織的アプローチから検討を行った。情報システムは、その技術や運用の方法が速いスピードで変化するものであるため、対策が追いつかないまま機密情報が至るところで漏洩し、結果として問題が深刻化してから法が整備された感は否めない。ただ、別の側面から言えば、法を策定することにより、各組織に対して情報の保護に関する意識に対して警鐘を鳴らしたとも見て取ることができるわけである。

情報セキュリティは、組織に属する各個人の意識がきわめて重要であるという点はこれまで検討してきたとおりである。一方で、情報の不正取得を企てる者は、その手口が巧妙化しつつあることも問題点として浮かび上がっている。本稿ではとくに、組織的観点からの考察に力点を置いたため、こうした情報の不正取得に関するリスクに関しては言及をほとんどしなかった。また、組織内で情報の高度技術者を確保・育成することは、今後の当該組織の強みを発揮する意味でも重要な行為者になることが想定される。この点についても、本稿ではあまり触れることができなかった。

今後は、情報技術やそれをとりまく組織の活動について、さらに踏み込んだ研究が必要であると認識している。これら課題点については、今後の課題としてむすびにかえたいと思う。

（ちくご　いちろう・高崎経済大学大学院地域政策研究科博士後期課程）

注）

1）「個人情報の保護に関する法律」が正式名称である。2005 年 4 月で施行に至ったのは、第 1 章（総則）、第 2 章（国及び地方公共団体の責務等）、第 3 章（個人情報の保護に関する施策等）に加え、第 4 章（個人情報取扱事業者の義務等）、第 5 章（雑則）、第 6 章（罰則）の 3 章分の施行である。詳しくは、内閣府ホーム・ページ（http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html）を参照されたい。

２）この事件は、Web アプリケーションである CGI（Common Gateway Interface）の設定が不完全で、その結果外部から読み取れるようになっていたために情報が抜き出され、外部に流出した事件である。詳しくは、下記ホーム・ページを参照されたい。
http://www.itmedia.co.jp/news/0311/12/njbt_01.html
http://japan.internet.com/ecnews/20040520/3.html
３）カカクコムのホーム･ページに、データ･ベース用のウイルスが仕掛けられ、そのウイルスの活動により、カカクコムのサービスが停止に追い込まれた事件である。このことについては、カカクコムだけでなく他のホーム・ページにも飛び火したが、とくに利用者の多いカカクコムのサービス停止が大々的に報道された。この事件の顛末については、カカクコムホーム・ページを参照されたい。
http://www.kakaku.com/info/200505/
４）この事件に関しては、下記ホーム・ページも参照されたい。
http://www.bmi.or.jp/jbms/jbms-notice/sain/20021216uzishi.htm
http://www.truste.001.jp/privacy/damage.html
５）ＳＢＢ社に関する情報は、下記ホーム・ページも参照されたい。
http://itpro.nikkeibp.co.jp/free/NCC/NEWS/20040227/140606/
http://itpro.nikkeibp.co.jp/free/NCC/NEWS/20040227/140656/
http://itpro.nikkeibp.co.jp/free/NC/NEWS/20040227/140662/
http://itpro.nikkeibp.co.jp/free/NC/NEWS/20041130/153281/
http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20040301/140727/
６）たかた社における情報は、下記ホーム・ページも参照されたい。
http://internet.watch.impress.co.jp/cda/news/2004/03/09/2371.html
http://internet.watch.impress.co.jp/cda/news/2004/10/07/4906.html
７）調査期間は 2004 年２月～３月にかけての 22 日間であり、いずれも基幹業務システムの管理者が回答している。当該アンケートの概要については、総務省（2004）、pp.3 を参照されたい。
８）1980 年５月、OECD の理事会で採択された「プライバシー保護と個人データの国際流通についての勧告」の中に記述されている８つの原則」のことである。８原則とは、収集制限の原則、データ内容の原則、目的明確化の原則、利用制限の原則、安全保護の原則、公開の原則、個人参加の原則、責任の原則のことを指す。
９）イギリスにおける汎業界向けの情報セキュリティに関するガイドラインをベースとしたガイドラインのこと。２部構成となっており、第１部で規定について書かれている。それによると、セキュリティポリシー、セキュリティ組織、資産の分類と管理、要員セキュリティ、物理的セキュリティ、通信と運用管理、アクセス制御、システム開発と保守、事業継続管理、法律等への準拠の、10 の管理エリアについて確立するよう規定している。
１０）日本工業標準調査会が「情報技術－情報セキュリティマネジメントの実践のための規範」という規格名称で策定したセキュリティ・マネジメント標準のことである。

引用文献

・井上（2005） 井上健太郎『個人情報保護法完全対策』日経情報ストラテジー、日経 BP 社、2005.2、pp.34-42。
・島田（2001） 島田達巳『情報システムのアウトソーシング―企業・自治体比較を焦点にして―』組織科学、Vol.35, No.1, 2001, pp.32-43。
・総務省（2004） 総務省『情報セキュリティに関する実態調査』2004。
・高木（2004） 高木篤夫『「個人情報」の値段』日経情報ストラテジー、日経 BP 社、2004.6、pp.181。
・高橋（2004） 高橋正和『事故発生の損失額は？』日経情報ストラテジー、日経 BP 社、2004.8、pp.260-263。
・吉川（2004） 吉川和宏『CIO 大学』日経情報ストラテジー、日経 BP 社、2004.7、pp.17。
・OECD（1992）OECD Guidelines for the Security of Information Systems, 1992。
http://www.oecd.org/document/19/0,2340,fr_2649_34255_1815059_1_1_1_1,00.html
・OECD（2002）OECD Guidelines for the Security of Information Systems and Networks TOWARDS A CULTURE OF SECURITY, 2002, pp.12。
・Sauer（1993） Sauer, Chris, Why Information Systems Fail: A Case Study Approach, Alfres Waller Ltd. , 1993, pp.25-32.

主要参考文献

・秋山知子・清嶋直樹『情報ガバナンスを再構築せよ』日経情報ストラテジー、日経 BP 社、2003.3。
・清嶋直樹『中央官庁の「CIO 補佐官」は機能するか』日経情報ストラテジー、日経 BP 社、2004.8。

・島田達巳「自治体の情報システム―民間企業との比較分析―」白桃書房、1989。
・島田達巳「地方自治体における情報化の研究―情報技術と行政経営―」文眞堂、1999。
・島田達巳「自治体のアウトソーシング戦略―協働による行政経営―」ぎょうせい、2000。
・杉山泰一『誤算の研究』日経情報ストラテジー、日経 BP 社、2004.7。
・総務省『平成 16 年版　情報通信白書』ぎょうせい、2004。
・総務省『平成 17 年版　情報通信白書』ぎょうせい、2005。
・松井啓之「地方自治体における情報化の失敗に関する事例分析」組織科学、Vol.38 No.2、2004。
※なお、ホーム・ページ URL は、すべて 2005 年 7 月 1 日現在のものである。