情報ネットワークにおける情報管理とセキュリティポリシー

亀田彰喜　勝木太一

概　要

近年、拡大する情報ネットワークの進展によって私たちの生活は非常に便利になり、情報ネットワーク無しでは成り立たない社会になりつつある。その反面、情報ネットワークにおける不正アクセスによるデータベースの破壊や個人情報の漏えいなどの問題が多発している。情報が漏えいし、それが悪意を持った者の手に渡ると機密情報や個人情報が不適正に取り扱われ、企業に対して大きな損害をもたらし、企業経営にも大きな影響を与える。医療現場においても、患者の住所や受診履歴などの個人情報の漏えい等により、個人の権利が侵害される危険性もある。

このような問題の対策として、教育現場での情報倫理に対する教育、法律の改正や新しい法律の整備による規制や、組織における情報資産のセキュリティ対策についてはセキュリティポリシーによる管理等が挙げられる。法による規制では、情報ネットワーク上での犯罪を法律により取り締まるというものである。多様化する情報犯罪を既存の法律を改正させることや、法律の整備により、情報資産をこのような脅威からいかに守るか。そして、セキュリティに対する対策や情報管理における体制等についても取り上げてみた。

1．はじめに

世界初のコンピュータ ENIAC が1946年に誕生して以来、コンピュータは進歩し、情報ネットワークは当初の予想をはるかに超えて大きな進歩を遂げた。すなわち、今日の社会は情報ネットワークを基盤として情報を処理することによって成り立ち、維持されているといっても過言ではない。

当初は、バッチ処理中心の時代で、情報処理は一般人から隔離されたコンピュータセンターで専門技術者によって行われており、関係のない者をコンピュータセンターに近づけないための対策が必要であった。コンピュータセンター内で起こった出来事が、外部にはほとんど伝わらない時代であったので、セキュリティがあまり重要視されることはなかった。

しかし、今日のような情報ネットワークの時代となると、外部の顧客やユーザが直接操作する情報システムが増加してきた。それとともに、一般市民の生活の中に情報システムが根を降ろしており、社会性を帯びた情報システムが増えてきている。また、今日のように情報ネットワークが主流となることでネットワークにおけるトラブルが目立ち始め、ネットワークにおけるセキュリティがクローズアップされるようになった。情報ネットワーク中心の社会となることで、情報システムあるいはネットワークの機能が停止すると社会の

機能がストップすることから、セキュリティの重要性が強く認識されるようになった。

さらに、ネットワークの国際化が進むにつれて、地球上のどこからでもアクセス可能となり、時間的にも距離的にも格差がゼロという情報ネットワーク環境ができ上がった。インターネットが普及するにつれて、いつでも、どこからでも、誰でも、簡単にインターネットにアクセスでき、どこからでも情報を入手できるという環境が生まれた。

このような情報環境の中では、情報化の進展に伴いセキュリティの範囲も広がってきている。そして、セキュリティを一部の人に任せておけばよい時代は終わり、一般の人々もセキュリティに関する知識を身につけておかなければ、本人が知らないうちに情報面で被害者にまた、加害者になる可能性がある。

そのため、現実に起きている情報ネットワークや情報管理においての諸問題を取り上げ、その諸問題に対する抑制対策を考えていく。

2．情報ネットワークにおける情報管理の現況および実態

情報ネットワークの進展にともない、私たちの生活は便利になるとともに、企業においても、顧客情報や社員の個人情報、自社製品の情報や競合他社の製品情報などのほとんどが情報ネットワークによって管理されている。また、医療機関においても電子カルテの導入が進み、患者の個人情報が情報ネットワークを介して管理されるようになった。

しかし、情報ネットワークの進展により便利になった反面、現在の情報化社会においては様々な社会問題が起きてきている。それは、情報ネットワーク上における不正アクセスによって引き起こされるデータベースの破壊や個人情報の漏えいなどの問題である。情報が漏えいし、それが悪意を持った者の手に渡ると機密情報や個人情報が不適正に取り扱われ、企業に対して大きな損害をもたらし、経営にも大きな影響を与える。医療機関においては、患者の電話番号や受診履歴などの個人情報の漏えいにより、個人の権利や利益が侵害される危険性もある。このように情報ネットワークの進展による利便性は非常に良くなったが、その反面、危険性も同じように大きくなっていることを認識しておかなければならない。

さらに、情報ネットワークや情報管理に関するトラブルは手口が多様化および巧妙化し、完全に防ぐことは不可能であるといえるかもしれない。しかし、完全に防御することは困難であっても危険性をできるだけ減らすことは可能である。

近年また、科学技術の面においても、各国で科学技術関連の開発が盛んにおこなわれるようになり、その結果、大量の研究成果が発表され、研究情報として保存されるようになった。この大量の研究情報の中から必要な情報を容易にしかも迅速に見つけ出し、その情報を分析し加工することは、さらに深く研究する上で必要条件となった。そのためには、情報を収集し、それらを検索しやすい形態に加工し、さらに活用が可能となる状態にしてお

くことの重要性が認識されるようになった。そのため、現代社会において市場情報や競合他社の情報を早く的確に収集・検索・分析・立案・蓄積・提供・伝達することが、企業の命運を握っているといっても過言ではない。

情報を管理するにあたっては、情報を迅速に検索し、収集し、さらに情報を加工し、その情報を活用することが求められる。情報を他人に知られないように、秘密裏に管理するだけが情報管理ではなく、情報をさらに加工しやすいように加工し、積極的に情報を活用することも情報管理の重要な役割である。しかし、情報を漏らさないようにする情報管理と、情報を積極的に共有化して活用していく情報管理とは、おたがいがトレードオフの関係になることが多く、そのバランスを考えることも情報管理であるといえる[1)]。

情報管理においては企業や医療ではその対応がそれぞれ異なったものになる。企業では顧客情報や社員の個人情報、病院では患者の病名や通院歴、過去にかかった病気など医療機関によって扱う情報の種類や機密性のレベルも異なる。そのため、情報管理における現況はそれぞれの企業や組織において大きく異なる。

（1）企業における情報漏えい

これまで、企業が発展していくためには、経営資源として、人材、資金、物資の三つが重要であると言われてきた。しかし、高度情報化社会が進む現在においては「情報」が第四の経営資源として重要な役割を占めるようになってきた。この「情報」を効率的に活用するために様々なところでコンピュータが導入されている。地球規模の情報化社会の到来により、情報の重要性はますます高くなったといえる。この情報化社会の進展により、情報量は飛躍的に拡大し、欲しい情報が大量の情報に埋もれて見つけ出すことができない場合も少なくない。大量の情報の中から、的確かつ迅速に必要な情報のみを見つけ出し、その情報を分析し扱いやすいように加工することは、この情報化社会を生き抜くために必要な条件になりつつある[2)]。

一方、情報化社会はわれわれに快適な生活や大きなメリットをもたらすだけでなく、個人情報の漏えいの危険性も同時にもたらす。さらに、インターネットという情報ネットワークは、快適で便利な情報化社会をもたらしたと同時に、ハッカーやクラッカーによる個人情報や秘密情報などの漏えいや破壊の危険性も増大させた。そこで、これらの危険から情報を守るために、情報通信技術に関する技術面と管理面の両方を考慮した情報セキュリティ対策を含めた情報管理が必要となる。

企業における情報流出の事例としては、2011年４月17日から４月19日にかけてＳ社のゲーム機「プレイステーション３」用サービスのシステムが不正侵入を受け、Ｓ社が運営するプレイステーションネットワークから日本を含む世界でおよそ7,700万人分の利用者の個人情報が流出した。また、同じ時期にＳ社の子会社である Sony Online Entertainment のサービスにおいてもおよそ2,460万件の個人情報が流出し、Ｓ社グループ全体で合計１億人以

上の個人情報が流出したことになり、過去最悪の件数となった。

プレイステーション３とは2006年発売のＳ社・コンピュータエンタテインメント（SCE）の据え置き型家庭用ゲーム機である。高性能パソコンに引けを取らない性能を持つほか、通信機能を備えており、インターネットを介してオンラインゲームや映画も楽しむことができる。また画像や動画などのデータを蓄積して処理する「ホームサーバー」としての役割を果たすよう設計されている。全世界の累積販売台数は５千万台を超えている。

同社のサービスに入る場合、まずインターネットに接続し、SCE 側に名前や情報、生年月日などの個人情報を登録してアカウントを所得する必要がある。また SCE のネットワーク上には「プレイステーションストア」と呼ばれる店舗があり、ゲームやビデオ、コミックなどを購入し楽しむことができ、購入方法の１つとしてクレジットカード決済があり、今回はカード番号や購入履歴などが流出した可能性もある。Ｓ社の発表によると、流出したとみられる個人情報のうち、名前や住所、生年月日などの情報は暗号化していなかったが、クレジットカード番号は暗号化していた。

この事件の原因は不正アクセスに対して、アプリケーションサーバーの脆弱性に対処していなかったことにある。脆弱性とは外部からの不正なアクセスなどによって不正に利用できてしまう欠陥のことで、プレイステーションネットワークでは、アプリケーションサーバーと呼ばれるプログラムに既知の脆弱性があった。

まず犯人はアプリケーションサーバーの脆弱性を突き、通信ツールをプレイステーションネットワーク内に不正に通信ツールを設置し、設置したその通信ツールによって個人情報が保管されているデータベースサーバーへのアクセス情報を入手し、そして、このアクセス情報を使って、外部からデータベースに不正アクセスし個人情報をダウンロードした[3)]。

このような事件に対しては、一般的に対処は難しく、わかっていても対処するためのプログラムがなかったり、システム更新ができなかったりなどの問題で対処できないこともある。しかし、Ｓ社の業務執行役員である担当責任者によると「わかっていて更新できなかったのではなく、脆弱性に対処していなかった」とのことである。つまり放置していたことになる。巨大なネットワークを運営しているにもかかわらず、脆弱性に対処していなかったのはあまりに無責任であるといえる。

更に、サイバー攻撃の事件としてはＭ社の事件がある。Ｍ社は、2011年８月11日に社内のサーバー45台と従業員が利用するパソコン38台のあわせて83台がコンピュータウイルスに感染し、情報漏えいの危険性が判明した。

サイバー攻撃が発覚したのは、Ｍ社の監視システムが８月11日に社内のサーバー異常を検知したため。標的型メール攻撃により感染した。標的型メール攻撃とは、その名の通り特定のターゲットを狙う攻撃のことで、企業内のパソコンを狙っている。しかし、企業内のパソコンはインターネットに直接接続しているわけではなく、社内だけに限定したネットワークにつながっている。そのためインターネットからの直接攻撃はできず、送信者を

偽装し、実在する信頼できそうな組織や個人からのメールのように見せかけ、メールの添付ファイルを使って感染させる方法である。今回のメールでも実在する内閣府の人物の名前と、その人物のメールアドレスを偽装して送られていた。

漏えいした可能性のある情報は、原子力発電所の設計や設備および耐震性などに関する情報、防衛省からの受注データ（装備品関係）、管理報告書の一部（80式空対艦誘導弾等の性能データ）、戦闘機やヘリコプターに関する資料（過去の戦闘機開発の経緯などをまとめた社内の説明用）、営業系サーバーにおけるパスワード等のキーログ、社員約2,000人の個人情報などがある[4)]。

標的型メール攻撃は、業務連絡を装ったり、震災や原発事故に関連した内容に関するものであったりと、思わずメールを開いてしまうような仕掛けとなっている。いわゆるソーシャルエンジニアリング（人間の心理的な隙や、行動のミスにつけ込んで機密情報を入手する方法のこと）の手口であり、タイトル・本文・添付ファイルのタイトルが巧妙に作られているものがほとんどである。

また、標的型メール攻撃への対策を完璧に行うのは難しいとされている。しかし、M社の一番の問題は、８月にウイルス感染の被害が出ていたのに、発表が大幅に遅れて対策が後手に回ってしまったことである。怪しいファイルを開いてしまった時点で、サーバー管理者と上司に報告することが重要である。標的型メール攻撃は誰でも騙されるという前提のもとで、被害にあったら報告しウイルス感染してないか、他のパソコンに波及していないか、情報がどこまで流出しているのかを確かめる必要がある。

（２）医療機関における情報漏えい

情報技術の進展に伴い、医療の分野においても情報化が進んでいる。それとともに、医療機関における医療情報の管理が求められている。その中でも最近は、医療機関における情報の流出が多発し問題となっている。特に情報ネットワークを介した患者の個人情報の流出や、ノートパソコンやUSBの紛失・盗難による個人情報の漏えいがほとんどである。そして、それらの多くは医療機関の中でも研究を主体とする大学病院で流出する事態が増えている。医療における個人情報は、医療技術の研究のためには欠かせない情報であるが、患者の個人情報は人権尊重という観点から取扱いには十分な注意が必要である。

医療における個人情報流出の特徴は、紛失したパソコンが個人所有のノートパソコンであることが多く、患者のデータの保存された自分のノートパソコンを、診療にあたって複数の医療機関の間を持ち歩いている点である。さらに、医療機関によって患者の個人情報の管理体制がそれぞれで異なっている場合が多く、カルテが電子化されている病院もあれば、されていない病院もある。

大学病院の医師にとってみれば、ノートパソコンにデータを保存して各医療機関を移動しながらデータの処理や研究をするにはノートパソコンが非常に便利なツールである。し

かし、そのノートパソコンには重要な患者の個人情報が詰まっており、情報漏えいの観点から見れば危険性が非常に高く、扱いにおいては慎重さが求められる[5]。

医療機関における個人情報の流出も完全に無くすことは困難であるが、もし個人情報の流出が起きると莫大な損害賠償を請求される場合もあり、それでなくても患者の信頼を失うことにつながる。医療機関における情報流出は、一個人の責任ではなく組織全体での対処が必要である。

病院における情報の流出事例としては、富山市のH病院の事例がある。2006年３月８日、職員の私物パソコンがウイルスに感染し、手術室使用履歴などを含む患者の個人情報、2,873件がＰ２Ｐファイル共有ソフトのWinnyネットワークに流出したことを明らかにした。

流出したのは、1997年９月から2004年12月に手術を受けた患者2,873件の氏名、性別、年齢、生年月日および手術の情報などを記したExcelファイルで、住所や電話番号、病名は記入されていない。

原因は、職員が業務作業などに利用していた私物パソコンがウイルスに感染したためであった。H病院では、診療情報を電子化した2005年以降、患者情報の持ち出しを許可登録制とするほか、私物のパソコンの院内の持ち込み禁止、Winnyの使用禁止といった措置を取ってきた。しかし、職員のパソコンがウイルスに感染したのはその前の2004年12月だった[6]。

さらにまた、K大学病院の事例もある。2011年６月27日、同病院のスポーツ医学総合センターで診察を受けた患者約２万４千人の個人情報が入ったUSBメモリが所在不明になったと発表した。

同病院によるとUSBメモリには、平成３年９月から23年４月に同センターを受診した24,459人の患者の名前や生年月日、電話番号、病名などが入っていた。USBメモリはIDとパスワードがない限り内容は見られないようになっている。USBメモリは外来受付の奥の棚に保管されており、看護師が使用しようとしたところ無くなっていたという。USBメモリはデータのバックアップ用として使用していたが、同病院は情報流出の危険性から原則的にバックアップを控えるように指示していた。ただ、データの移行期間であったため使っていた[7]。

３．情報ネットワークにおけるセキュリティ対策

（１）情報倫理に対する教育

現在ではインターネットが地球規模で普及し、一般の個人の日常生活においても情報ネットワークを利用し多くの情報に接し、簡単に情報を入手できるようになった。また現代社会においては、データベースの破壊や情報ネットワークの損壊は、経済および社会生活に多大の被害と損害を与えることになる。そのため、情報の改ざんや破壊といった情報を作

為的に操作する行為に対して、何らかの対策が必要である。それにはまず個人レベルでの情報意識の向上である。このようなことを早くから認識させ、情報技術に関与する者に対する倫理意識を身に付けさせる必要がある。そのために初等中等教育において情報教育が導入され進められつつあるが、単に情報技術だけを習得させるのではなく、情報の重要性に対する認識を深めさせ、それに対する情報倫理意識を持たせる教育を進める必要がある。

情報倫理とはコンピュータを使用し、情報ネットワークを利用するにあたっての倫理問題である。情報技術を扱う専門家は当然として、少しでも情報に触れるユーザも社会の共通の意識として今後さらに認識しなければならない問題であり、情報システムや情報ネットワークの信頼性と安全性に関わる重要な問題でもある。そのため、情報技術に関する専門家の間では倫理綱領を設け、情報倫理に対する意識を高めている。

それは情報の専門家として、事実やデータの尊重、ユーザに対するリスクへの配慮、秘密情報の守秘などであり、情報システムや情報ネットワークの管理者においては、システム運用上でのユーザへの配慮を行うとともに、システムの利用規定などを作成および実施し、情報倫理の認識のもとに業務に携わることである。また一般のユーザに対しても、社会人として他人の人格とプライバシーの尊重、知的財産権や知的成果の尊重、情報システムや情報ネットワークシステムの利用規則の遵守が求められる。

そこで、これからの情報化社会を担っていく若い世代に対する情報倫理教育というのがこれからの課題となる。その一つとして、中学校および高等学校のうちから情報教育として、情報倫理教育の取り組みが導入されつつある。

文部科学省が1999年３月１日に提示した新学習指導要領では、情報倫理を情報モラルとして取り扱っている。そこでは、新たに現代の情報化社会に対応すべく、はじめて中学校および高等学校に情報教育のための設備の充実と、インターネットが利用可能な教育環境が進められてきた。これからも、中学校、高等学校で情報技術の教育が実施されていくが、現在社会で問題になっている情報倫理、すなわち情報モラルの教育も重要視されている。中学校学習指導要領では、授業でインターネットを利用するとともに実際に例を通して、情報倫理としての個人情報や著作権の保護および発信した情報に対する責任について指導することが求められている。

また高等学校においては、新たに必修教科として「情報」が新設され、情報発信に当たっての個人の責任、プライバシーや著作権への配慮などを扱うものとすると情報モラルについて具体的な指導内容について触れている。さらに、情報教育において著作権やプライバシーの保護、情報発信者の責任などの情報モラルの必要性及び情報のセキュリティ管理の重要性についても理解させることと、基本的な知識を習得させるとともに、情報モラルについての教育も強く求めている[8)]。

このように、中学校および高等学校において新学習指導要領に基づき情報教育が導入されており、次の情報化社会を担っていく若い世代が情報に対する倫理意識を養うことがよ

り一層望まれている。学習指導要領は年々改正されており、刻一刻と変化する情報化社会に対して、有意義な教育を行うことにより、社会に出る前から情報倫理を正しく身につけていくことが抑制方法となる。

（2）法による規制

情報倫理に対する教育のところで、中学校、高等学校から情報倫理の教育を行うことで認識を高める方法を述べたが、やはりそれだけではネットワーク上でのトラブルを防ぐことはできない。そのような犯罪などを取り締まるため、法律により規制し、違反した場合は罰則を与える。我が国では著作権法、個人情報保護法、刑法、不正アクセス行為の禁止等に関する法律で規制している。

著作権法とは、著作物の創作者である著作者に著作権や著作者の人格権を付与することにより、利益を保護する法律である。同時に、著作物に密接に関与している実演家、レコード製作者、放送事業者および有線放送事業者に対して著作隣接権を付与し、これらの者の利益も保護している。無体物であるプログラムの保護については、1984年に著作権法が改正されて、著作権法による保護の対象となった。しかし、著作権法による保護では、保護の対象が表現でありノウハウやアルゴリズムは保護の対象とならない。このため、著作権法によるプログラム保護の限界が問題とされている。さらに、1986年の著作権法改正では、データベースも保護の対象とされた。これは、データベースで創作性を有するものは著作物として保護するというものである[9)]。

個人情報保護法（行政組織の保有する電子計算機処理に係る個人情報の保護に関する法律）は1988年に成立した。しかし、この法律は、行政組織の保有する電子計算機処理に関する個人情報を対象としており、民間企業が収集し保有している個人情報を対象としていない。民間企業を対象とした個人情報保護法としては、「個人情報の保護に関する法律」が2003年に成立し、2005年４月より完全に施行された。この法律によれば、「個人情報とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別できるものを含む）をいう。」と定義している。

また、刑法にもコンピュータ関連の犯罪を取り締まるための条文がある。刑法は犯罪とそれに対する刑罰の関係を規律する法である。コンピュータや、インターネットなどが現在のように使われるようになったのはここ数年で、それより前の時代の刑法ではコンピュータ関連の犯罪を取り締まるための条文は未整備であった。このため、時代の変化による必要性から新たに関連条文が整備されてきている。刑法の中のコンピュータに関わる不正を取り締まる主要な改正点は、主に次の三つである。

第一は磁気記録に文書性を認めて、電磁的記録不正作出及び併用（第百六十一条の二）を新設して、事務処理を誤らせる目的で電磁波的記録を不正に作った者は処罰されること

となった。刑法第七条の二で電磁的記録とは、電子的方式、磁気的方式その他、人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものとある。

第二はコンピュータを損壊したり、電子データを改ざん・消去したりするなどして業務を妨害するような行為に対して電子計算機損壊等業務妨害（第二百三十四条の二）である。これは磁気記録を破壊するなどしてコンピュータ業務を破壊するなどしてコンピュータ業務を妨害した者は処罰されるというものである。

第三は虚偽の情報や不正な指令を与えることによって不正に利益を入手する行為、いわゆるコンピュータ詐欺に対する電子計算機使用詐欺（第二百四十六条の二）である。従来は人をだますのが詐欺であったものを、人と対面することなくコンピュータと対面して同じことをすればコンピュータ詐欺罪で処罰されることとなった[10]。

また、増加するコンピュータウイルスを悪用した犯罪などを取り締まるための刑法改正案「情報処理の高度化等に対処するための刑法等の一部を改正する法律案」が2011年６月17日に可決し、2011年７月から施行された。すなわち、コンピュータに不正な指令を与える電磁的記録の作成する行為等を犯罪とする内容の、不正指令電磁的記録に関する罪として新設された。刑法上で電磁的記録とは、①人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する、②前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録」の２種類である。コンピュータウイルス等の不正なプログラムが想定されるため、「ウイルス作成罪」ともよばれている。

不正アクセス行為の禁止等に関する法律は、通信回線を介して情報システムに不正アクセスする行為を禁止するために、1999年８月に成立し2000年２月13日より施行された。この法律は、他人のIDやパスワードを使用して情報システムに侵入する行為を禁止するとともに、他人のIDやパスワードを無断で提供して、不正アクセス行為を助長する行為を禁止するものである。不正アクセスにより具体的な被害が生じているかを問わず、不正アクセス行為をしたものや秘密情報を漏らした者は、懲役または罰金によって処罰されることになった。

例えば、不正に入手した他人のユーザ名とパスワードを使ってサーバーに侵入すると、不正アクセス行為の禁止等に関する法律の第３条（不正アクセス行為の禁止）第１項、第２項の違反になる。また、不正に入手した他人のユーザ名とパスワードを他人に知らせると、不正アクセス行為の禁止等に関する法律の第４条（不正アクセス行為を助長する行為の禁止）の違反になる。そのほかにも、Webサーバーのセキュリティホールを利用してサーバーに侵入すると、不正アクセス行為の禁止等に関する法律の第３条（不正アクセス行為の禁止）第１項、第２項の違反になる[11]。

また、医療分野では情報化社会における問題である不正アクセスに対して厚生労働省は法的な対応として「医療・介護関係事業者における個人情報の適切な取扱いのためのガイ

ドライン」を2004年12月24日に公表した。これは2005年４月１日に個人情報保護に関する法律の施行に先駆けて、医療・介護事業者に対し個人情報の取扱いに対する指針を示したものである。この医療・介護関係事業者における個人情報の適切な取扱いのためのガイドラインは、医療機関や医師は医療における個人情報の性質や利用方法から、特に適正な取扱いの厳格な実施を確保する必要であると指摘している。そして、法の趣旨を踏まえ医療・介護関係事業者における個人情報の適正な取扱いが確保されるよう、遵守すべき事項は法の規定により厳格に遵守し、遵守することが望ましい事項は法に基づく義務ではないが、達成できるように努めることと具体的に示している[12)]。

このように、すでに法律は整備されているが、犯罪は情報ネットワークが普及し拡大するごとに多様化し巧妙化してきている。それら全てに事前に対応することは不可能であるが、ネットワーク犯罪が発生した時にはすみやかに法律の改正や新しい法律の整備を行うことで、できる限りの被害を無くすことにつながる。

前述したように、情報倫理に対する教育と法による罰則と規制では、情報倫理に対する教育や既存の法律や新たに法律を作ることで情報の犯罪自体を減らす方法であった。しかし、実際にこのようなトラブルにあわないようにするために重要なことは、情報を取扱う各々が他人事であると思わずにしっかりと情報セキュリティに対して意識を持ち、対処することである。特に、現在の情報化社会では、一人一台のパソコンを与えられるのがほとんどであり、アクセスできる限度には違いがあるとしても各々がネットワークに接続しており、一人の責任で組織全体が大きな損害を負う可能性も少なくないといえる。そのため組織としてだけでは無く、一人ひとりの注意が必要である。

前述の富山市のＨ病院の事例でも挙げたように、多くの情報漏えいの原因が私有または私用パソコンから漏えいすることが多く、そのほとんどがファイル共有ソフトである Winny からの流出である。ファイル共有ソフトとはインターネットを利用して不特定多数のユーザ間でファイルを共有できるソフトウェアである。ウイルスに感染すると、パソコン内のデータファイルが世界中の利用者に公開され、入手できる状態になり、公開フォルダにコピーされてしまう。つまり、パソコン内の送受信メールや Word などの情報が全て流出してしまうことになる。そのような事態になってしまわないためにも、しっかりと対策をたてることが必要である。

個人としての具体的な対策として、仕事用のパソコンに許可無くソフトウェアを導入しない、そして持ち出さない。職場のネットワークに私有のパソコンを接続しない。仕事用のパソコンから USB メモリなどの記憶媒体に情報をコピーしない。漏えいしては困る情報を許可無くメールで送らない。私有のパソコンでどうしても使う場合においては、漏えいしては困る情報を取り扱うパソコンには Winny などのファイル共有ソフトを導入しない。ウイルス対策ソフトを導入し、最新のウイルス定義ファイルで常に監視する。もし、不審なファイルを見つけたとしても絶対に開かないなどが挙げられる。また、私有パソコ

ンや組織の情報の取扱いについて定めている場合は、必ずそれに従わなければならない。

組織においても、委託先を含む組織で用いるパソコンについてのファイル共有ソフトの使用について、個人情報や機密情報などが保存されているパソコンでは使用禁止などといった使用条件などをしっかりと定めることが必要である。私有のパソコンについても、扱う情報の範囲や期間などを明確にし、その上で許可制にする、許可された利用範囲を管理者が確認できるようにするなどの仕組みが必要である。また、大学病院等においては個人情報や機密情報を持ち出したりすることへのルールを定め、やむを得ず持ち出す場合には、厳重な管理を義務付ける必要がある。さらに、重要な情報はアクセス制限を設け、必要な人にしかアクセスできないように設定する。重要な情報はコピーの制限を設ける。さらに暗号化して管理するといった対策や、私有のパソコンからのネットワーク接続に制限をかけるといった方法が考えられる。

また、ウイルスによって狙われやすい脆弱性（外部からの不正なアクセスなどによって不正に利用できてしまう欠陥）に対しても、最新のウイルス対策ソフトウェアをこまめにインストールし、常に最新の状態にしておくことが必要である。また、ファイアウォールやウイルス対策ソフトウェアなどの基本的なセキュリティソフトウェアを利用することにより保護することが大切である。

4．情報管理における体制

（1）企業における情報管理体制

企業が保有する情報の中には、自社の技術情報、経理に関する情報、取引に関する情報、顧客に関する情報、従業員の個人情報などのように様々なものがある。これらは、人材、資金、物資と並ぶ企業の資産の一つとして重要なものである。情報化社会が進むにつれて、情報が漏えいしたときの損害は大きくなり、情報の管理方法はより重要なものになっている。

個人情報を扱う企業として情報漏えいの対策をすることは当然の責務である。S社の情報漏えいの事例のように、注意をしていたけれど脆弱性を突かれたのではなく、脆弱性に対処していなかったということは問題外である。脆弱性は一般的に対処が難しいと言われるが、常に最新のプログラムを適用し、最新の状態にしておくことが一番の対策である。

企業の規模が大きくなれば、従業員の人数も多くなり情報管理もそれだけ難しくなる。そのため、企業全体としてのセキュリティポリシーが不可欠になる。セキュリティポリシーを整備する上で大切なことは、企業においての情報資産を明確にし、そして判断基準や実施すべき対策を明確にすることである。セキュリティポリシーは制定しているだけでは意味がないため、必要なことを明確にして全てのユーザに正しく内容を把握してもらい、遵守させることが必要である。

（2）医療機関における情報管理体制

医療機関においても、情報技術の進展に伴い医療情報の情報化が進んでいる。その一例がカルテの電子化があり、患者の住所や氏名などの個人情報から通院歴や病歴などの医療情報までもが情報化され、医療機関内での利用や研究においての利便性の向上とともに危険性も大きく増加したといえる。特に医療情報においては、その性質や利用方法により、特に適切で厳格な情報管理が求められる。

医療機関は厚生労働省が公表した医療・介護関係事業者における個人情報の適切な取扱いのためのガイドラインや、個人情報保護法の内容に沿って、個人情報に関する「宣言」や「規則」を定め、その「宣言」や「規則の概要」を院内に提示することが求められている。

医療機関における個人情報の安全管理としては、院内における情報ネットワークシステムへのアクセスを制限することや職員のユーザ ID やパスワードをアクセスログに記録しておき、定期的にチェックし、不正アクセスに対処する必要がある。

また、医療機関におけるトラブルのほとんどを占めるネットワークを介しての個人情報の流出やノートパソコンの紛失・盗難に対しては、ノートパソコンのパスワードを設定し、ファイル交換ソフトを使わないようにするなど、ウイルス対策をしっかりとする。そして、ファイアウォールによるネットワークのセキュリティ体制を整えるといった対策が重要である。

個人情報保護法や医療・介護関係事業者における個人情報の適切な取扱いのためのガイドラインの施行により個人情報に対する意識が過剰になったと言われているが、医療の研究も重要であるが患者の個人情報を守ることも重要なことは言うまでもない。このような現状でも情報に関するトラブルは起きている事実を他人事とせず、しっかりと対策することが重要である[13)]。

（3）情報セキュリティポリシーによる管理体制

現在の企業や組織は、情報化への依存による利便性の向上と引き換えに、大きな危険性を抱え持つことになった。この情報化社会において企業や組織にとって、情報セキュリティに対するリスクマネジメントは最も重要な経営課題のひとつであるといえる。特に、個人情報や顧客情報を取り扱う場合には、これを保護するということが企業や組織にとっては社会的責務である。

かつての情報システムを利用した業務は、中央集中型のホストコンピュータに一部の人間がアクセスし、情報処理業務を行うことが一般的であり、外部との情報交換、報道発表等は紙面や口頭で行うことが一般的であった。しかし、現在パソコンが急激に普及し、個人がパソコンを利用して情報処理業務を行い、また個々の端末から全世界的なネットワークに接続できる環境となった。これにより、情報活動や情報サービスの効率化が図られることとなり、内部からだけでなく外部からのアクセスが極めて容易になった。また、基本ソフトウェア及び分散管理の普及や情報システムへのアクセスが増加することにより、こ

れまで以上に十分に情報セキュリティの確保が困難な状況になってきている。こうした情報を適切に管理できれば、利便性と安全性の確立につながる。

情報を適切に管理する上で大切なことは、このような情報セキュリティ対策は画一的なものではなく、企業や組織にとっては社会的責務である。つまり、業務形態、ネットワークやシステムの構成、保有する情報資産などを踏まえた上で、その内容に見合った情報セキュリティの対策を行うことは、絶対に必要なことであるといえる。

セキュリティポリシーとは、企業や組織における情報資産のセキュリティ対策について具体的にとりまとめたものである。どのような情報資産をどのような脅威からどのように守るのか、セキュリティ対策基準や個別具体的な実施手順などを含んでいる。具体的には、どの情報を誰にアクセス許可して誰にアクセス許可しないのか、どの操作を誰に許可して誰に許可しないのか、外部からの侵入にどのようにして防ぐのか、それらが正常に機能しているかを管理することが求められる。

ここでＳ大学におけるセキュリティポリシーの事例として情報システム運用基本規程を取り上げてみる。

Ｓ大学情報システム運用基本規程[14)]

Ｓ大学（以下「本学」という。）は、インターネットに常時接続された基幹ネットワークシステム、情報処理教育システム、各研究分野で構築されたシステム、教育研究活動を支援するための業務システム等、多様な情報システムを所有している。これらのシステムは、情報化社会における人材の育成、研究者間における研究資源の共有や成果の発信、地域社会への成果の発信、効率的な大学運営に資するものであり、きわめて重要な役割を担っている。

一方、情報システムへの不正侵入、さらにはデータの改ざんやシステムの妨害といった脅威が増大している中、これらの情報システムには高度な安全性と信頼性が求められている。

これからも本学が、学術研究・教育活動を発展させていくためには、情報システムの計画的な整備に加えて、情報資産のセキュリティを確保していくことが不可欠である。

このような情報セキュリティの重要性を大学の全構成員が十分意識して情報資産を守っていくとともに、不測の緊急事態にも適切に対応できる体制を確立するため、情報システム運用基本規程（以下「基本規程」という。）を定める。

（情報システムの目的）

第１条　本学情報システムは、本学の理念を実現するため、本学のすべての教育研究活動および運営の基盤として設置し、および運用する。

（適用範囲）

第２条　この基本規程は、本学情報システムを運用し、管理し、または利用するすべての者に適用する。

（利用者の義務）

第３条　本学情報システムを利用する者または運用の業務に携わる者は、この基本規程に沿って利用し、別に定める運用および利用に関する実施規程を遵守しなければならない。

（定　　義）

第４条　この基本規程において、次の各号に掲げる用語は、それぞれ当該各号の定めるところによる。

（１）情報システム

情報処理および情報ネットワークに係るシステムで、次のものをいい、本学情報ネットワークに接続する機器を含む。

ア　本学により、所有または管理されているもの

イ　本学との契約または他の協定に従い提供されるもの

（２）情報ネットワーク

情報ネットワークには次のものを含む。

ア　本学により、所有または管理されているすべての情報ネットワーク

イ　本学との契約または他の協定に従い提供されるすべての情報ネットワーク

（３）情報セキュリティ

情報資産の機密性、完全性および可用性を維持することをいう。

（全学総括責任者）

第５条　本学情報システムの運用に責任を持つ者として、本学に全学総括責任者を置き、理事長がこれを任命する。

２　全学総括責任者は、基本規程およびそれに基づく実施規程の決定や情報システム上での各種問題に対する処置を行う。

（管理運営部局）

第６条　本学情報システムの総括的な管理運営部局は図書情報センターとする。

２　図書情報センターが行う事務は別に定める。

（部局総括責任者）

第７条　各部局に部局総括責任者を置き、学部長、国際教育センター長および事務局次長を充てる。

２　部局総括責任者は、部局における運用方針の決定および情報システム上での各種問題に対する処置を担当する。

（情報ネットワーク管理者）

第８条　本学情報ネットワークに情報ネットワーク管理者を置き、図書情報センター長を充てる。

２　情報ネットワーク管理者は公立大学法人Ｓ大学情報ネットワークシステムを管理する。

（特定情報システム管理者）

第９条　本学情報システムのうち情報セキュリティが侵害された場合に影響が大きい情報システムを特定情報システムとし、部局総括責任者が指定する。
２　特定情報システムに特定情報システム管理者を置き、部局総括責任者が任命する。
３　特定情報システム管理者は、手順の決定および特定情報システム上での各種問題に対する処置を担当する。
（見 直 し）
第10条　基本規程および実施規程等を整備した後には、各規定の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行う。
２　本学情報システムを運用し、管理し、または利用する者は、自らが実施した情報セキュリティ対策に関連する事項に課題および問題点が認められる場合には、当該事項の見直しを行う。

このように、セキュリティポリシーを整備する上で大切なことは、情報セキュリティ担当者だけがネットワークやコンピュータなどに対する情報セキュリティ対策を心掛ければよいというわけではないということである。情報資産を共有する全ての社員や職員が適切な情報セキュリティ意識を持たなければ、ウイルスや情報漏えいなどから企業や組織の情報資産を守るのは困難である。

さらにメリットとして、セキュリティポリシーを導入することで、情報資産が何であるのかを明確にでき、判断基準や実施すべき対策などを明確にすることによって、各々がセキュリティ意識を向上させる効果がある。それによって取引先や顧客などに対して、企業や組織としての信頼性も向上する。

しかし、セキュリティポリシーは制定しているだけでは意味がなく、企業や組織内外を問わず、関わる全てのユーザにその内容を把握してもらい、その上で規約を守ってもらう必要がある。こうして初めて運用しているといえるのである。また、情報セキュリティに関わる問題は刻一刻と変化しているため、それにあわせてPDCAサイクルによって計画（Plan）、運用（Do）、評価・見直し（Check）、改善（Act）、そしてまた計画、運用と繰り返し持続していくことが必要である。

しかし、どれだけ対策をしていても完全にトラブルを防ぐことは非常に困難である。このようなトラブルがあった場合について、2007年８月30日に独立行政法人の情報処理推進機構セキュリティセンターは個人情報が漏えいした時の対応策を公示している。個人情報の流出やノートパソコンなどの紛失・盗難の場合の対応策として、発見および、報告、初動対応、調査、通知・報告・公表等、抑制措置と復旧、事後対応の６つの個人情報事後対策を示している[15)]。

具体的には、まず紛失・盗難もあった場合は、本人の事件の発見と報告が求められる。そして、紛失、盗難を確認後、個人情報の内容と量、そしてアクセスの制限の有無や暗号

化について確認する。また、ネットワーク上での個人情報流出の場合は、パスワードの変更や、アカウントの停止等の初動処置をとることが必要である。個人情報の漏えいに関しては、特に事件後の初動処置の対応が重要である。

パソコンの盗難による個人情報の流出は、多くの事業所や職場で起こり得ることであり、個人情報の管理責任者が普段から情報管理について強く指導していても、徐々にマンネリ化、形骸化しがちである。一度、外部に個人情報流出やパソコン等の盗難事件がおきてから慌てても手遅れであるので、技術的な対策とともに職員相互の啓発が必要である。

5．おわりに

情報化社会が進みインターネットは、非常に便利な反面、不正アクセスや情報の漏えいや情報の破壊などの危険性も増加させた。情報犯罪の手口は巧妙化が進んでおり、今日のようなインターネット社会においては社会問題となっている。このような問題の抑制対策として、情報倫理に対する教育、法による規制、個人による技術対策、セキュリティポリシーによる管理が考えられる。

情報倫理に対する教育では、新学習指導要領により情報教育が進められているが、情報技術の習得とともに、情報を扱うにあたっての倫理教育を行い、情報倫理に対する意識を高めるというものである。具体的に中学校および高等学校の新学習指導要領に情報倫理や情報モラルについての教育を強く求めており、次の情報化社会を担っていく若い世代が情報に対する倫理意識を養うことがより一層望まれている。

法による規制では情報ネットワーク上での犯罪を取り締まるために、法律によって取り締まるもので、著作権法、個人情報保護法、刑法、不正アクセス行為の禁止等に関する法律が規制されている。情報に関する犯罪は最近のものであり、以前は刑法では情報問題に関して取り締まっていなかったが、改正されて取り扱われるようになった。また、医療機関においては医療における個人情報の性質や利用方法から、厚生労働省は医療・介護関係事業者における個人情報の適切な取扱いのためのガイドラインを公表した。これは、医療・介護事業者に対し個人情報の取扱いに対する指針を示したものである。多様化する情報犯罪に対して法律の改正や新しい法律の整備を行うことで、できる限りの被害を無くすことにつながる。

個人による技術対策では、情報を取り扱う個人が情報セキュリティに対して意識を持ち、対策することである。実際にファイル共有ソフトなどにより個人のパソコンから情報が流出することも多く、医療情報の流出に関してはパソコンの盗難や紛失を含めて、個人の問題がほとんどであるといえる。犯罪で狙われやすい脆弱性に対して常に最新のプログラムを適応する。そして、ファイアウォールやウイルス対策のソフトウェアなどのセキュリティ

ソフトウェアを利用して保護することが重要であるといえる。また、技術面だけでなく、私有のパソコンを仕事用に使わない、ファイル共有ソフトを使用しないといったことも含まれる。情報のトラブルを他人事と考えずに行動することが大切である。

セキュリティポリシーによる管理では、組織における情報資産のセキュリティ対策について、どのような情報資産をどのような脅威からどのように守るのかを、セキュリティ対策基準や個別具体的な実施手順などを具体的にとりまとめた管理体制である。セキュリティポリシーを整備する上で、情報セキュリティ担当者だけでなく、情報資産を共有する全ての社員や職員が適切な情報セキュリティ意識を持たなければ、ウイルスや情報漏えいなどから情報資産を守るのは困難である。そして、そのためには、PDCA サイクルによってセキュリティ対策をとることが重要である。

【参考文献】

1）田中一雄『情報管理概論』白桃書房、2005、13-22。
2）村山博・大貝清俊『高度知識社会における情報管理』、コロナ社、2003、1-6。
3）読売新聞、2011年 5 月 2 日『Ｓ社7700万件情報流出、原因は「脆弱性への未対応」』。
4）日本経済新聞、2011年 9 月20日『M社にサイバー攻撃か』。
5）亀田彰喜・勝木太一『情報倫理の観点からみた医療情報の管理』、Review of Economics and Information Studies Vol.10 No. 3 ・ 4 、2010、41-52。
6）医療法人社団　H病院、http://www.h-uro.com/。
7）K 大学病院、http://www.hosp.keio.ac.jp/。
8）亀田彰喜・勝木太一『情報教育における情報倫理』、Review of Economics and Information Studies Vol.10 No. 3 ・ 4 、2010、1-10。
9）和田英夫・原田三郎・日笠寛治・鳥居壮行『情報の法と倫理』、北樹出版、1999、118-120。
10）渡辺喬一『個人情報保護法のしくみと実務対策』、日本実業出版社、2005、114-132。
11）鳥居壮行『情報セキュリティ』、オーム社、1998、49-70。
12）日経メディカル編『医療機関のための個人情報保護法対応マニュアル』、日経 BP 社、2005、35-38。
13）羽生正宗『病・医院経営のための個人情報保護対策』、ビジネス教育出版社、2005、77-78。
14）Ｓ大学情報システム運用基本規程、2012。
15）田中功『情報管理の基礎知識』、海文堂、1993、13-14。