新しい情報セキュリティシステムの条件
―既存システムの限界とその超克に関する一考察―

寺本 卓史

Abstract

On this paper, we analyze the limitation of present Information Security Management System (ISMS), and consider the method of breaking through the limitation. Though ISMS is defined as one of risk management systems, it is surrounded by the condition which is totally different from that of other risk management systems. It is caused by distinctive character of "Information System", consisted of "Information" and "Information Network". It was never recognized that "Information" is important as now. Also "Information Network" is becoming "open network" day by day. It means that "Information System" is confronted with unknown risks. However, present risk management system is made for controlling known risks. From such point of view, it can be said that the present ISMS is not enough effective against threats. At the end of this paper, we suggest several conditions to improve information security.

1. はじめに

企業活動をはじめ社会のさまざまな領域に情報通信技術(Information and Communication Technology：ICT)[(1)]によって成立する情報ネットワーク(Information Network)[(2)]が構築・活用されるようになるにつれ、情報セキュリティ(Information Security)に対する意識にも、かつてないほどの急激な変化が生じている。このことは逆説的ではあるが、既存の情報セキュリティの仕組みが十分ではないことを示していると捉えることができる。すなわち、今日的状況に十分対応できるセキュリティのシステムが求められているのである。現在の情報セキュリティは、情報セキュリティマネジメントシステム(Information System Management System：ISMS)を中心として考えられていることが一般的である。このシステムは国際認証(ISO)化され、多くの組織で用いられている。しかしながら、このシステムは基本的に、他の多くのリスクマネジメントシステムと同様、既知の危険（risk）に対応する仕組みになっており、不確実性(uncertainity)に満たされた今日の情報ネットワークには十分に対応できないことも見受けられる。したがって、こうした限界を超える新しい情報セキュリティシステムが求められているのである。

本研究ではこうした問題意識を基に、既存の情報セキュリティ制度の問題点と、その超克に関する考察を行なう。まず次の２章においては、情報セキュリティをめぐるコンテクストを読み解き、情報セキュリティが必要とされる背景について整理する。つづく３章では、情報セキュリティに要求されている事項について「二重の困難性」という観点から、既存の情報セキュリティのシステムが十分に

機能し得ない状況を分析する。さらに４章では、現在の情報セキュリティの制度としてISMSの仕組みを分析し、その問題点を抽出する。そして５章では、前章で明らかになった課題を克服する、新しい情報セキュリティの構築について提言する。最後の６章では、これまでの議論を総括する。

2. 情報セキュリティをめぐるコンテクスト

情報セキュリティ (Information Security) に対する意識の変化の背景には、以下のような情報ネットワークに関するコンテクストがある。

2. 1　情報ネットワークへの依存

近年の社会･経済活動は、ICTを用いて処理されることが多くなっている。今日のわが国企業において、何らかの情報システムを用いない企業は皆無に等しく、また情報システム自体の担う役割も、日々増大している。

例えば、2007年5月に発生した全日本空輸の情報処理システム障害は、半日以上にわたって同社便の運行を停止させ、約8万人に影響を及ぼすなど、同社の企業活動に大きな影響を与える結果となった[1]。このトラブルの原因は社内の情報ネットワークにおけるルータ (中継器) の不具合であったが、こうしたかつては小さな問題で済んでいたトラブルが、現在では企業活動全体にまで大きな影響を及ぼしかねない状況にある。

また、1984年11月に世田谷区で発生した地下電話ケーブル火災は、一般電話回線が8,900回線、公衆電話回線1,377回線、専用･特定回線3,000回線などが不通となった[2]。この事故は近隣住人の電話回線が使用不能となるなど、地域の社会･経済活動に影響を与えただけでなく、金融機関VAN事業者などのオンラインが回線専用･特定回線に収容されていたため、銀行のオンラインが停止するなど、全国的にも大きな影響を及ぼした。この事故の完全復旧には9日間かかり、推定の被害総額は45億円に上るとされている。

このように、社会･経済活動が情報ネットワークへの依存を高めるにつれ、情報ネットワーク自体の重要性が上昇している点に注目する必要がある。

2. 2　情報ネットワークの脅威の増大

情報ネットワークの中でもオープン･ネットワークの利用者が増加し、また不特定多数になるにつれ、ネットワークにおける脅威が増大している[3]。具体的には、コンピュータ･ウィルスやスパムメール、ネットワーク障害など、情報ネットワークを介して発生・伝播されるさまざまな問題の発生件数が急増している。

（年）	平成13	14	15	16	17	18
ウイルス感染被害報告件数（万件）	4.3	7.5	6.9	12.1	8.6	10.5
検挙事件数（件）	35	51	58	65	94	84

表１　ウイルス感染被害報告件数と検挙事件数

日本国内におけるウイルス被害件数は、2001年 (平成13年) には約4.3万件だったものが2006年

(平成 18 年) には約 10.5 万件となるなど、この五年余りの間にも急激に増加している [3] (表 1)。また、ウイルス流布の目的も、かつてのいたずら目的中心から、詐欺や重要情報の入手など実利目的へと変化しつつあり、悪質化している。

さらに、無差別・大量に一括送信される宣伝目的の電子メールであるスパムメールの増大も問題となっている [4]。2005 年の槙原・鵜飼・竹村による分析では、日本国内におけるスパムメールを年間約 1,410 億通と推計しており、その損失労働時間は 282 万時間となるなど経済活動に大きな損失をもたらしている。

このように、情報ネットワークは外部からの脅威のみならず、内部における脅威も情報ネットワークのオープン・ネットワーク化と共に増大している。

2．3　情報の重要性の上昇

情報ネットワークに接続されるコンピュータが増加するにつれ、脅威に晒される情報が質と量の両面において変化している。

例えば、ここ数年で急増した P2P ファイル交換ソフト [4] 利用者を標的としたコンピュータ・ウィルスによって引き起こされた、官公庁や民間企業などさまざまな組織による大量の情報漏えいが問題となっている。『情報セキュリティ白書 2007 年度版』によると、2006 年度において最も脅威の高かった問題は「Winny による情報漏えい」であったという [5]。また、2006 年において Winny などのファイル交換ソフトを使用したことによって、情報流出被害のあった組織 (企業・自治体) は全体の 3.3% であった [6]。

また、情報保護の意識の高まりと共に、情報漏えいが発生した場合の社会的影響も大きくなっている。例えば 1999 年 5 月に発生した宇治市の約 22 万人分の住民基本台帳データ流出事件の場合、一人当たりの被害額は 1 万円と裁判所で認定され、また 2004 年 2 月に発生した YahooBB の約 450 万人の個人情報漏えいの場合は 6 千円と認定されるなど、個人情報が大きな価値を持つと認識されるようになりつつある。

以上のように、情報ネットワークで重要な情報が扱われるようになり、また個人情報のように社会的な認識が変化したことなどによって、情報ネットワーク上に流出した場合に、大きな影響を及ぼしかねない情報が増大している。

3.　情報セキュリティの「二重の困難」

上記のような状況から「情報セキュリティ」の重要性が指摘されるようになっている。そして、これまでの傾向を見る限り、今後も重要性は引き続いて上昇すると考えられる。その一方で、この二十年余りで爆発的に普及した ICT については、セキュリティ対策に必要な知識や経験が未だ十分に得られていないことも多い。また、進化し続ける ICT によって情報ネットワークやそこで提供される技術やサービス自体も、日々新たなものが誕生しており、安定した技術の形態を捉えることが困難であるという特質がある (5)。すなわち情報セキュリティは、守るべき情報の重要性が増す一方で、守るべき場所となる情報ネットワークの姿が定まらないという、「二重の困難」にあるという特徴がある。「二重の困難」の原因としては、以下のものを挙げることができる。

3．1　オープン･ネットワーク化

1990 年代以前の情報ネットワークは、大型汎用コンピュータを中心とした集中管理型が殆どであり、また各々のネットワークの規模接続される端末の数や利用者も限られていたのに対し、90 年代以降は、多数の情報ネットワークが相互に接続されて世界規模のネットワーク、すなわちインターネットを形成するようになるなど、いわゆるオープン･ネットワーク化が進展した[7]。

インターネットに代表されるようなオープン･ネットワークは、それ自体が一つの生命体のような存在であり、特定の主体による直接的なコントロールが十分に行き届かないことに最大の特徴がある。したがって、情報ネットワークに関する全ての資源を管理することを前提とする集中型管理における情報セキュリティとは、対応を根本的に変える必要がある。例えば、コンピュータ・ウィルスに感染した自宅パソコンから P2P ファイル交換ソフトを経由して、所属する組織の情報を流出させてしまうといったケースは、こうしたオープン･ネットワークシステムの中における情報資産の管理の難しさを表わすものといえる。

また組織内部においても利用者が、かつての専門家のように限定されているわけではないため、ルールの遵守を前提とした仕組みを見直す必要がある。ネットワークの利用に関して、なぜ対策が必要なのか、また対策を怠った場合どのような不利益がありうるかについて、組織の構成員全体に対して周知徹底を図ることが必要となっている。さらに、利用者が不適切な操作を行なった場合においても一定の安全性を確保する「仕掛け」を設定することが必要である。

このようにオープン･ネットワークシステムにおいては、システムの構成上も、また利用者のあり方についても、集中型管理システムとは異なるアプローチでセキュリティについて管理する必要があるのである。

3．2　脅威の不確実性化

一方で、さまざまな情報が情報ネットワークを介してやり取りされることによって、それに対する脅威も増大した。自らの組織内で情報ネットワークが完結していた時代にあっては、脅威は組織内のコントロールで対応することが可能であったのに対し、今日では一組織の情報や情報ネットワークであっても、世界中の脅威に晒され、また直接関係のない脅威であっても影響を受ける可能性も見られるようになった。例えば 2006 年 5 月末から 6 月はじめにかけて発生した、領土問題に端を発した韓国から島根県庁サイトへの Dos 攻撃は、国際間の問題が情報ネットワークにも影響を及ぼすことを示すものとなった[6][8]。こうした攻撃にあった場合、直接該当する組織 (前例では島根県庁) 以外にも、情報ネットワーク的に近い位置にある組織がサービス能力の低下を余儀なくされるなどの影響を受ける恐れがある。すなわち、世界中が結びついたオープン･ネットワークにおいては、その脅威もグローバルに存在するようになったのである。

このように情報セキュリティとは、こうしたグローバルな脅威に対応することを意味している。これは、食品偽装の問題のように社内のマネジメントで解決するものではない[7]。ここに情報セキュリティ対策の最大の課題がある。しかし、さまざまな情報の流通やサービスがオープン･ネットワーク上で行われている以上、課題があるからといって情報ネットワークの利用を止めることは現実的でない。すなわち、情報セキュリティとは「二重の困難」の中で、オープン･ネットワークから撤退するこ

となく、関連するさまざまな要素のバランスを取りながら進めていくしかないのである。

4. 既存の情報セキュリティ制度

4. 1 情報セキュリティの定義

情報セキュリティとは、情報資産を取り巻く脅威から、情報資産を保護することである。情報資産とは、「組織や個人がその価値を認識している『情報』と『情報システム』のこと」であり、コンピュータに保存されていたり情報ネットワークを流通したりするデジタル・データとしての情報に止まらず、情報ネットワークやそれを構成するコンピュータ、通信機器、紙で保存されている情報の他、組織や個人で保有している文書化されていないノウハウのようなものまで、あらゆる無形資産が情報資産として括られる可能性がある。また、情報セキュリティの対象は、これら全ての情報資産に関わるハードウェアソフトウェアの技術系、人間系の全てである。

	人為的	非人為的
意図的	コンピュータ・ウイルス 不正アクセス、盗聴	―――
非意図的	データの誤操作 データの置忘れ	火災・地震等の災害 機器・通信経路の故障

表２　脅威の分類とその例

こうした資産に関する脅威としては、一般的に考えられるようなコンピュータ・ウイルスやネットワークを介した電子的不正侵入といった人為的・意図的な脅威のみでなく、誤操作によるデータ消失やデータの置き忘れなどの人為的・非意図的な脅威、さらには火災や地震などの非人為的・非意図的な脅威などをも含める必要がある [9] (表２)。

このような広範な脅威に対して、情報資産を保護することとは、「機密性 (Confidentiality) 」、「完全性 (Integrity) 」、「可用性 (Availability) 」を確保することと一般的に解釈されており、それぞれの頭文字をとって情報セキュリティの「CIA 」と呼ばれている [8]。機密性とは秘密であるべき情報が適切な状態に保たれていること、完全性とは情報が完全な形で管理されることであり、可用性とは情報を必要なときに利用できることを、それぞれ示している。

以上のように広範な脅威に対して「 CIA 」が保たれることが、情報資産が「適切な行動をとることにより、事故又は悪意にもとづく行為からデータ及び資源を保護すること」であると考えられているのである [9]。

4. 2 情報セキュリティマネジメントシステム（ISMS）

情報セキュリティの意識の高まりとともに、情報資産管理の方法として登場したのが、1995 年に英国で規格された BS7799 の Part2 を基に民間認証制度とされたのが、「 ISMS 適合性制度」であり、さらにこの制度を発展的に国際規格化されたものが「 ISO/IEC27001 」である (図１)。この ISO/IEC27001 は、ISO9001、ISO140001 に続く第三の国際認証規格であり、2005 年 11 月に発行されたものであり、現在において最も標準的な情報セキュリティマネジメントの実施手法として認識されている [10] [10]。

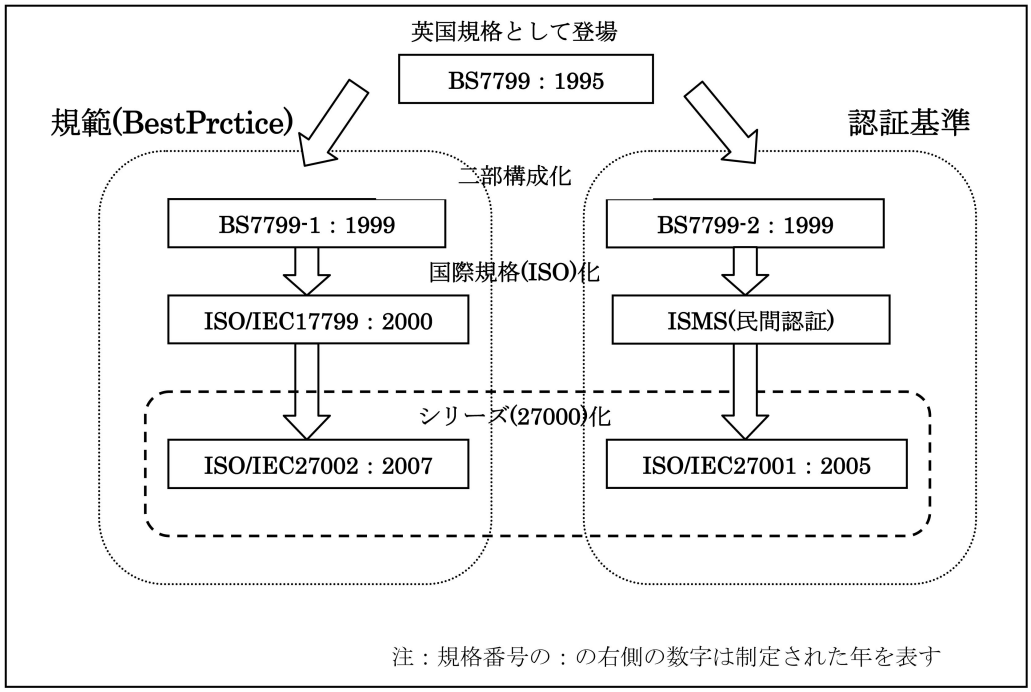

図 1　ISMS の発展の歴史

その特徴として、以下のような点を指摘することが出来る。

PDCA サイクル

ISO/IEC27001 では、マネジメントをサイクルとして捉えており、マネジメントサイクルとして計画 (Plan)、実施 (Do)、監査 (Check)、改善 (Act) からなる「PDCA サイクル」を導入している。このサイクルを繰り返すことによって、組織における不適切を継続的に発見し、より好ましい状態へと漸次的に接近することが出来るとしている。

階層化

情報セキュリティを階層化して実現しようとしている。具体的には、組織の情報セキュリティに対する基本姿勢を明らかにする「基本方針 (Policy)」、基本方針に基づいて具体的規定を定める「実施基準 (Standard)」、実施基準を満たすための詳細な手順を示す「実施手順 (Procedure)」の三階層となっており、段階的に情報セキュリティの目標設定から実施方法までを管理できるようになっている。

広範な対象範囲

ISO/IEC27001 が規定する情報セキュリティの対象とは、組織構造、方針、計画立案、責任、実践、手順、プロセス、資源など広範にわたっている。このことは、情報セキュリティの実現のためには多様な要素の連関の調整をとる必要があるとの前提に立っていることを示している。

このように、ISO/IEC27001 が規定する ISMS においては、オープン・ネットワークにおける脅威に対する対策が徹底的に考慮されている。すなわち ISMS とは、情報セキュリティに対する技術的な対策

ではなく、組織全体に渡って情報セキュリティを構築･監査し、適切なリスク･マネジメントを行なうPDCA サイクルの実施を規定しているのである。

また、「基本方針」を作成する Plan の段階においては、組織内の全ての情報資産を「棚ざらい」し、それぞれの情報資産における「脆弱性」と「脅威」、及びセキュリティ侵害が発生した場合に想定される損害の大きさから、情報資産ごとにリスク評価を行なう。そして、その評価に基づいてどのような対応策を行なうかを決定することが要求されている。このように ISMS には、組織の方針に基づきセキュリティ対策を実施するか否かも含めた決定を実施するという、経営の観点からリスク・マネジメントとしての意思決定を行なうことが、システムとして組み込まれているのである。

このリスク・マネジメントとしてのセキュリティ･マネジメントという観点は、それ以前の情報セキュリティには無かった視点である。以前の情報セキュリティとは、管理者が策定し、利用者は与件としてそれに従うものという前提で捉えられていた。すなわち情報システムは管理者にとって操作可能なものであり、適切な措置によって完全なセキュリティを確保できると考えられていた。ところが、ISMS ではセキュリティとは「完全」な状態を前提とはしておらず、「最善」の状態を模索して選択するものであり、前提において決定的な違いがある。

このように、ISMS はオープン・ネットワーク化された情報環境の中において組織がリスク･マネジメントを実施することによって情報セキュリティを維持するための仕組みを構築したものと考えることができるのである。

4．3　ISMS の課題

しかしながら、ISMS であっても現在の情報環境において、必要十分に機能しているわけではない。PDCA サイクルを繰り返すという運用方法自体に、絶えず改善を続けなければ十分に機能しないという ISMS の脆弱性を見ることもでき、また PDCA が十分に機能しない場合には、抱える問題点が顕在化する場合もある。このことは、ISMS 適合性評価制度を取得している組織であっても、情報漏えいやシステム停止などのセキュリティ侵害事例 (情報セキュリティインシデント) を起こしていることからも明らかである。また ISMS 認証の制度自体の運用においても、セキュリティ侵害事例が発生した場合においても PDCA サイクルをまわすことで問題点を解決すれば、引き続き ISMS 認証を得ることができるなど、ISMS 認証の取得イコール安全性の確保とはなっていないのが現実である [(11)]。

そこで以下では、こうした ISMS の抱える課題について、情報システムの性質と合わせて分析を行い、その問題点を探ることとする。

4．3．1　情報システムの特性

情報システムの変化速度

最初の問題は、情報システムにおける技術やサービスの登場によってもたらされる変化の速度が速いことである。ISMS が PDCA サイクルをまわすにせよ、常に新たな脅威が発生し続けるため、情報資産の評価、対応策の決定が後手にならざるを得ない。例えば、不ファイル交換ソフトである Winny の使用をきっかけとした情報流出は、2005 年末から翌年にかけて多数発生し社会問題化したが、それ以前には殆ど発生していなかった。いわば、突然ともいえるタイミングで、この問題か登場したのである。こうした変化速度の速さが、現在の ISMS のあり方に限界をもたらしている。

これは他の分野のマネジメントシステムと比較するときわめて独特なものである。例えば食品製造における品質管理は、満たすべき基準 (衛生管理基準など) が明確に定められており、この基準が急激に、また大きく変化することはない。すなわちマネジメントにおけるゴールを明確にし、そのゴールを組織の構成員によって共有することが比較的容易にできる。

それに対し情報資産にあっては、必要とされる対応策がオープン・ネットワークという外的環境によって容易に変更される。例えば、ゴールとすべきセキュリティ対策の理想状態を組織内で共有することが難しいのである。

資産価値の変容

情報資産にセキュリティ侵害事犯が発生した場合の損害の大きさも、ネットワーク環境の変化などによって、組織内の意思とは無関係に変化する。

情報は、「名寄せ」や「紐付け」によって価値が大きく変化する性質を持つ。単独では大きな意味を持たない情報であっても、他の情報と合わせることによって大きな意味を持つことがあるのである。例えば生年月日や電話番号は、それらをキャッシュカードの暗証番号とする人にとってはセキュリティ上、重大な情報である。史上最強のハッカーと呼ばれたミトニックは、一見何の変哲もない企業における部署名やそこに所属する人間の氏名といった情報を切り口に、情報システムに潜入するといった自身のテクニックを語っているが、こうした事例は企業内において全く価値の無いように見える情報であっても、つなぎ合わせることによって重大なセキュリティ侵犯を引き起こす情報となりうることを示している [11]。

また、社会的な意識の変化によって組織の持つ情報資産の価値が変化する場合もある。昨今流出が騒がれる個人情報も、以前と比べて著しく流出した際の影響は大きなものとなっている。かつては名簿の形で公開されていた住所・電話番号・氏名のような情報であっても、今日では個人の合意なしに他者が公開することは基本的に許されておらず、流出した際の損害は大きなものとなっている。また、直接的な損害以外にも、流出させた組織に対する信頼性の低下といった間接的な損害も発生し、さらには流出先からの再流出を防ぐことが出来ないなど、情報の流出が発生した際の損害の規模を正確に予測することは事実上不可能である。

以上のように、情報資産の価値は、情報流出などセキュリティ侵害が発生して初めて確定されるという性格を持つのである。これは ISMS がリスク評価において、セキュリティ侵害が発生した際の損害コストを用いているのに対し、その評価の前提となる評価指標の算出に困難があることを意味している [12]。

4. 3. 2　コストとしてのリスク対応策

次に、外的要因だけでなく ISMS の制度自体にも、セキュリティ侵害予防の観点からは問題がある。ISMS は組織にとっては、他のリスク・マネジメントと同様に、危機管理を目的とした事前対策の一つである。したがって、ISMS のリスク評価で見たように、想定される損害額を指標としてリスク対策を決定している。ところが、損害額は前述のように算出に困難性を持つ上に、さらに実際の損害より小さく算出される傾向を持つ。これは想定される損害の算出に際して、ブランド価値の低下といった、無形資産の被害を参入することが困難なことによるものである。

また、組織にとってセキュリティ対策を実施する費用は、損害を予防・減少させるコストとして意識され、利益を生み出す費用とは認識されない。すなわち、セキュリティ対策はリスク・マネジメントとしては、「純粋リスク」であり、「投機的リスク」としては扱われないことが一般的である[12]。さらに、セキュリティ対策を強化することは、セキュリティ対策という直接的コスト以外にも、運用上のコストにおいても影響を及ぼす。セキュリティ対策を施すと、技術系・人間系共にトラブルの発生や効率が低下されることが指摘されている。例えば、システムへのログインなどにおける認証の強化は、技術系のシステムの処理が複雑化することによりレスポンスの低下をもたらしたり、人間系の処理手順の複雑化に伴い作業効率の低下を引き起こしたりすることがある。

このように、ISMS によるセキュリティ対策の強化はコストの面においても、リスク評価における過少算出の傾向や、純粋リスク対策としての直接的・間接的コストの上昇という観点から、セキュリティ侵害を防ぐ十分なコストが投入されない可能性があるのである。

5. 新しい情報セキュリティの条件

前章で分析した問題点を克服するためには、情報セキュリティマネジメントの仕組みに次のような仕組みや意識、文化を取り入れることが必要であると考えられる。

5. 1. リスク概念の転換

ISMS では、既知かつ計量可能な対象、すなわち「危険」のみを管理すべきリスクとして扱ってきた。しかしながら、これまでみてきたようにこうした「狭義」のリスクでは、セキュリティ侵害に十分に対応することが出来ない。したがって、ISMS に未知や計量不可能なものも含めた「広義」のリスクを扱う仕組みを組み込む必要がある。ナイトはリスクを計量可能な「危険」、計量が不可能な「不確実性」に分類しているが、この定義にしたがえば、情報セキュリティで取り扱うべきリスクは「危険」よりも「不確実性」に当たるものが多いことが理解できよう[13]。すなわち、組織にとって想定していなかった、もしくは想定していてもリスクを計量化して管理することが難しい事態が情報セキュリティでは多く発生するのである。したがってこうした「想定外」の事態に、いかに対応するかが重要となる。

2001 年 9 月 11 日に発生した、米国企業の中にはニューヨーク世界貿易センタービルへの旅客機突撃テロの後、「事業継続計画 (Business Continuing Plan：BCP) 」を作成するところが増加した[14]。これは、それまで想定しなかったような危機にも対応できる計画を作成しておくものである。既存の ISO/IEC27001 にも BCP の策定はルールとして組み込まれているが、そこで前提となっている危機とは、リスク分析で評価の対象とした所有する情報資産に対して、既知のリスクに対する脅威が顕在化したものに限定されている。救急医療において、大規模災害などで多くの負傷者が発生した場合に、重症度と緊急性によって分別することを「トリアージ」と呼ぶが、情報セキュリティにおいても想定外の事態が発生した際に状況を迅速にトリアージし、対応できる仕組みが必要である。

5. 2. セキュリティ対策の転換

セキュリティ対策についても、これまでの情報セキュリティのあり方の転換が必要とされる。既存の仕組みは、情報セキュリティは他のリスク管理と同様コストや効率性に相反する存在として捉えられている。また、他のセキュリティと比較して、情報セキュリティはどこまで対策を実施すれば十分

であるかが明確ではなかった。これではセキュリティの重要性を共有している組織であっても、必要十分な量のコスト・手間をかけることは難しい。そのためには情報セキュリティを「投機的リスク」として認識する意識の転換が必要である。

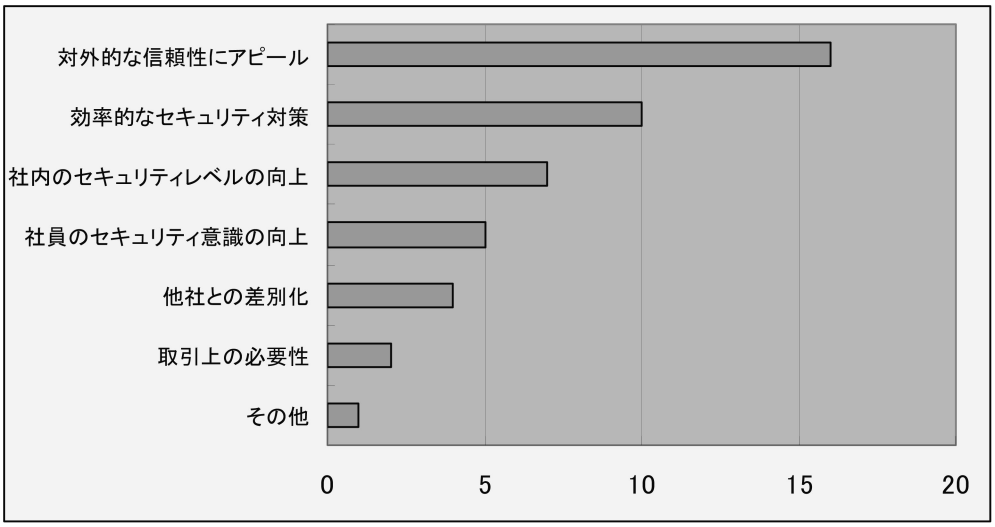

図 2　ISMS 構築のメリット (単位：%)

例えば、ISMS 認証の取得に関するメリットに関する調査では、「対外的な信頼性のアピール」が一位のメリットであり、「効率的なセキュリティ対策」や「社内のセキュリティレベルの向上」を引き離している [15] (図２)。また、2008 年４月１日より完全施行となる金融商品取引法 (通称 J-SOX 法) においても「IT 統制」が組み込まれるなど、企業価値を測る尺度として情報セキュリティが扱われるようになりつつある [16]。このように、ISMS 認証は情報セキュリティ対策というコストとして扱われるのではなく、広報的な利益をもたらすという意味合いで取得されることが多く、実態としては投機的リスクとして扱われることが多くなっている。重要なのは、情報セキュリティ対策への投入レベルを、「コスト」としての計量によって算出するのではなく、戦略としての意思決定によって求められる「投資」という認識を組織として持つことである。

5. 3.　セキュリティ文化の重視

これまで指摘したリスク概念やセキュリティ対策の転換のためには、組織におけるセキュリティ文化が重要な役割を担うこととなる。

想定外の事態に直面した時にどのような対応をとったら良いかについて、完全にマニュア化にすることは困難である。したがって、そうした事態にあってどのような対処を行なうかは、個人の判断にゆだねられることとなる。この個人の判断の基盤となるのが、組織におけるセキュリティ文化である。また、投機的リスクとしてのセキュリティ対策についても、その意思決定を支援し、また組織内における合意を形成するためにはセキュリティ文化が重要な鍵概念となる。

セキュリティ文化とは 2002 年 8 月に OECD が改訂した「情報セキュリティガイドライン」の中で述べられているもので、認識や責任、対応、倫理、民主主義といった 9 つの原則から成り立っており、全

文を通して、情報システム及びネットワーク利用に際して、参加者全員が情報セキュリティの関心と責任を持つ重要性を指摘している[17]。これまで情報セキュリティに関係ないと思っていた個人にとっても、避けて通ることはできない問題である事と定義されているのである。

組織においては、その内部において独自のセキュリティ文化を醸成し、その文化が構成員個人の意思決定の原則 (Principle) となることが、これまで見てきたような想定外の事例が頻繁に発生する今日のセキュリティをめぐる状況においては必要であろう。

6. おわりに

情報セキュリティのあり方は、この二十年の間に大きく変容した。この変容は二つのポイントに集約することが出来る。一つはコンピュータ及びネットワークのシステムが集中管理型からオープン・ネットワーク型へ大転換を遂げたこと、もう一つは利用者層の爆発的な拡大である。前者は技術的対策が中心であったセキュリティ対策に人的対策へのアプローチの転換を要求し、後者は不特定多数の利用者が安心して利用できるシステムを要求した。この矛盾するような二つの要求に対し、情報セキュリティはいまだ旧来の「純粋リスク」を前提としたリスク・マネジメントを行なっている。

名和はこのような情報セキュリティの現状を次のように指摘している。「セキュリティという概念は因果律にもとづいて組み立てられている。(中略) システムが大規模な複雑系になり、かつ多くの人によって動かされるようになった今日、セキュリティを単なる因果律によって律することが出来るのかどうか、ここに厄介な問題がある」と指摘している[18]。すなわち、現状の情報システム対応しうるシステムとして「進化」してはいないのである。

また利用者層の拡大は、これまで情報セキュリティには関係ないとされてきた一般利用者にも相応の認識と責任が求められるようになっている。すなわち、利用者全てが情報セキュリティを意識し行動することが求められているのであり、いわば情報セキュリティの「深化」が要求されているのである。

情報セキュリティにおいて今日求められているのは、このようなリスク・マネジメントしての一層の「進化」と「深化」ではないだろうか。

注

(1) 一般的に用いられる IT(Information Technology) とほぼ同じ意味であるが、コミュニケーション (Communication) を含めることで、情報技術のネットワーク性・共同性を認めた表現となっている。本章では、現状及び今後の情報ネットワークの発展において、ICT という用語が適切であると考え、用いるものとする。

(2) 情報ネットワークには、インターネット (Internet) の他にも銀行間ネットワークシステム (全銀ネット) や企業間ネットワークや企業内ネットワークなど様々な規模・種類のものがある。情報セキュリティの問題はインターネット上に限らず、これら全てのタイプのネットワークで発生しうる問題である (例えば Suica システムのトラブルなどは基本的には社内ネットワークの問題に分類される)。しかしながら、様々な情報ネットワークは、3.1. で論じるように、組織内に閉じられたものからオープン・ネットワークする傾向がある

(3) オープン・ネットワークについては、本論文 3.1. を参照。

(4) Peer to Peer(ピア・ツー・ピア) の形式を用いたファイル交換ソフトウェアのこと。ピア・ツー・ピアとは、各ユーザのコンピュータが対等・直接的に接続され、データの交換が行なわれるなど、クライアント・サーバ形式に代わる新たな仕組みとして注目される一方で、著作権侵害の問題や P2P ソフトである Winny を介して蔓延したコンピュータウイルスなどが社会問題となっている。

(5) 例えば、コンピュータソフトウェアには完成 (完全) という概念が存在しない。したがって保守によって、バグ (プログラム上の欠陥) を継続的に発見するしかないと考えられている。名和はこうしたソフトウェアについて「連続変化の法則」、「エントロピー増大の法則」、「統計的成長の法則」の 3 つの法則を指摘している [19]。

(6) Dos 攻撃 (Denial of Service) とは、Web ページへのアクセスやメール送信を、インターネットに接続したサーバに対して集中的に行なうことによって、サーバの機能を低下・停止させる攻撃のこと。詳細については、以下を参照 [20]。

(7) 食品の衛生管理においては食品安全規格である ISO22000(旧 HACCP) の規格に従うことで、一定の安全レベルと保つ事は比較的容易であると考えられる。この安全レベルを脅かすものは、未知の脅威 (例えば狂牛病といった新種の疾病など) が考えられるが、一定の安全レベルを保っていれば未知の脅威が顕在化した時に一つの組織が責められる事は少ないと考えられる。

(8) 情報セキュリティの CIA は、OECD「情報システムのセキュリティのためのガイドライン」で提示され、ISO/IEC27002「情報セキュリティを守るための実践規範」によって定められている。また、ISO/IEC27005「情報資産管理のためのテクニカルレポート」では、CIA に加え、「真正性 (Authenticity) 」、「責任追跡性 (Accountability) 」、「信頼性 (Reliability) 」の 3 つを加えた 6 点を情報資産保護の要素としている。

(9) ISO/IEC2382-8 による情報セキュリティの定義 [21]。

(10) ISO/IEC とは、国際標準化機構 (International Organaization for Standization) と国際電気標準会議 (International Electronical Comission) によって定められる規格のこと。認証規格の他にも様々な規範なども規格として標準化されている。

(11) 例えば、財団法人日本電子部品信頼性センターの実施する ISMS 認証においては、認証の一時停止･取り消しについて以下のように記述されている。「次の場合、認証組織に対して認証の一時停止又は認証の取り消しを行ないます。(中略)ISMS の不適合に対して、合理的期間内に継続的改善のための是正処置が出来ない場合／ ISMS の不適合に対して、一時停止期間内に継続的改善のための是正処置が出来ない場合」[22]。すなわち、問題が発生してもそれを解決出来れば認証の取り消しは行なわれないのである。

(12) 本論文 2.3. で述べたように、1999 年の宇治市住民基本台帳データ流出事件の場合は一人当たり１万円、2004 年の YahooBB 個人情報漏えい事件は 6 千円など、流出させた個人情報の内容が異なるとは言え、裁判で認定される被害額は大きな開きがある。また同じような情報を流出させたとしても管理体制によって認定額が異なったり、さらには裁判費用や人的コスト、営業上の損失などを含めると事前に被害額を正確に想定するのはきわめて困難である。宇治市の裁判の経緯については、以下を参照 [23]。

参考文献

〔1〕日本経済新聞、2007 年 9 月 12 日、朝刊、13 面

〔2〕石見利勝・糸井川栄一 (1985) 「1984 世田谷ケーブル火災の被害について」『日本建築学会大会学術講演梗概集』、日本建築学会、pp.353-354

〔3〕総務省 (2007) 『平成 19 年度版 情報通信白書』 オンライン版、第 1 章第 3 節 5(3) (http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h19/index.html)

〔4〕槙原博之･鵜飼康東･竹村敏彦 (2005)「spam メールの経済的損失の試算」、『RCSS ディスカッションペーパー 33 号』、関西大学阻止尾ネットワーク研究センター、pp.6

〔5〕情報セキュリティ研究会 (2007)『情報セキュリティ白書 2007 年度版』情報処理推進機構、pp.6-7

〔6〕イプシ・マーケティング研究所 (2007) 『2006 年国内における情報セキュリティ事象被害状況調査報告書』情報処理推進機構、p.75

〔7〕税所哲郎 (2006) 『情報セキュリティ・マネジメントの導入と展開』関東学院大学出版会、pp.1-2

〔8〕ITpro(2006) 「島根県ホームページに Dos 攻撃、韓国の IP アドレスから大量のアクセスとメール」 (http://itpronikkeibp.co.jp/article/NEWS/20060602/239853/)

〔9〕相戸浩志 (2003) 『よく分かる情報セキュリティ技術の基本と仕組み』秀和システム、pp.27-29

〔10〕税所哲郎　2006、前掲書、pp.22-25

〔11〕ITmedia エンタープライズ　2004「交通安全と情報セキュリティの共通点」 (http://1www.itmedia.co.jp/enterprise/articles/0412/news025.html)

〔12〕〔8〕　情報処理推進機構　2006『情報セキュリティ読本改訂版』実教出版、p.76

〔13〕〔9〕　Bearden, Gary S.　1975 ‘Reiew of “System Review Manual on Computer Security”’,”ACM SIGCSIM Installation Management Review” Association for Computer Machinery, pp.3-4

〔10〕村井純　1995『インターネット』岩波書店、pp.46-47

〔11〕Mitnick, Kein D.& Simon, Willialm L. 2002 ”The Art of Deception” Wiley,(岩谷宏訳　2003『欺術』

ソフトバンクパブリッシング、pp.23-24)
〔12〕亀井利明　2004『リスクマネジメント総論』同文館出版、pp.20-21
〔13〕Knight Frank H. 1921”Risk,Uncertainity and Profit” Houghton Miffin, (奥國領次郎訳　1969『危険・不確実性及び利潤』文雅堂銀行研究社)
〔14〕原田泉　2005『情報セキュリティで企業は守れるのか』NTT 出版、pp.86-88
〔15〕日本情報処理開発協会情報セキュリティ対策室 ISMS 事務局、2002『ISMS 適合性評価制度パイロット事業成果報告』p.4
〔16〕KPMG Japan ニューズレター 2006『日本版 SOX を超えた IT 統制』
(http://www.kpmg.or.jp/resources/newsletter/risk/ba/200606_1/01.html)
〔17〕外務省「情報システム及びネットワークのセキュリティのためのガイドライン」
(http://www.mofa.go.jp/mofaj/gaiko/oecd/security_gl_a.html)
〔18〕名和小太郎　2005『情報セキュリティ 理念と歴史』みすず書房、p.25
〔19〕名和小太郎　2005、前掲書、pp.100-101
〔20〕情報処理推進機構　2006、前掲書、pp.18-19
〔21〕日本規格協会　2004『JIS ハンドブック 64』pp.133-148
〔22〕日本電子部品信頼性センター ISMS 認証部　2007『ISMS 認証制度』p.18
〔23〕原田泉　2005、前掲書、pp.38-40