9　情報セキュリティ

－情報セキュリティ・マネジメントシステム(ISMS)に関する一考察－

辻　本　　篤

本稿は、組織の「情報セキュリティ」を支える「情報セキュリティ・マネジメントシステム」(Information Security Management System ：ISMS) を検討するものである。このシステムの基本コンセプトは、組織の情報資産を「機密性」(漏洩させない)、「完全性」(改ざんさせない)、「可用性」(故障させない)という3点に集約される。以下その導入の経緯と特徴を解説し、検討しなければならない基本的な課題を整理していく。

1. はじめに　―「情報」という組織資源

組織の運営において4大資源として管理されてきたは「人」「物」「金」「情報」。特に90年代以降、「情報」に対する扱いに注目が集まっている。世界中を接続する高速情報ネットワーク網であるインターネットの誕生は急速な情報化社会への変貌の一つとなった。これまで、限られた人のみが使用していたコンピュータが組織業務の中心となり、また一般家庭への普及、高性能化、大容量化も実現した。しかし同時に大きな社会問題も産み落とすこととなった。簡単に大量の情報を扱える状況は、情報の「漏えい」、「改ざん」、「破壊」など、世の中を震撼させる新たな脅威を生みだし、組織の存続に関わる深刻な問題も散見されるようになったのである。「情報」に対する脅威は未知であり、現在のところ絶える気配を見せない。組織や国民を守るための法律も常に後手後手にまわらざるをえない。これは情報システムの技術進化が日進月歩で進んでいくという背景があり、システムを保全するセキュリティ技術も同様である。そのため必然的に、それに関わるリスク要因も幾何級数的に増加してゆくと考えられる。

2.情報セキュリティ・マネジメントシステム(Information Security Management System：ISMS）の必要性

2.1　多発する情報漏えい

個人情報保護法（注1）が施行された2005年4月以降、個人情報の漏えい事件がメディアをにぎわすようになった。特に民間部門では顧客情報など重要情報の漏えい事件が多発している。2006年に入り、ファイル交換ソフト「ウィニー」を介した情報漏洩が多発した。たとえば、2006年には海上自衛隊の機密情報の漏えいが明らかとなった。防衛庁は、海上自衛隊の護衛艦の訓練関係の文書などの情報が含まれる多数の資料が、ファイル交換ソフト「Winny」を通じて流出したとして、調査を開始したことを明らかにしている[i]。防衛庁によると、流出した資料は、海上自衛隊の佐世保基地に配備されている護衛艦「あさゆき」の電信室所属の通信員（曹長）が所有していたと思われるファイルで、同通信員の私用PCがウイルスに感染し、Winnyを通じて流出したと報告されている。 流出したデータには、自衛艦のコールサインの一覧など、情報の重要度で「秘」とされる文書や、隊員の名簿等の個人情報が含まれているという。また、さらに重要度の高い「極秘」とされる暗号書や乱数表などについて、文書名の一覧表も流出したが、文書そのものは流出していないと報告されている。

また民間企業でも顧客情報の大規模な漏えいが発生している。最近（2011年）では、ソニー・グループの大規模な顧客情報の漏えい事件が大きな衝撃を与えた[ii]。ソニー・ピクチャーズが約100万件、ミュージックレコーが75000件、ミュージッククーポン350万件、これは、クラッカー集団LulzSecによるものとされている。グループとして1億261万3000件の漏洩として報告されている。ソニーグループの事件は、個人情報保護法施行以降、事件として発覚している中では最も大規模は事故として扱われるようになった。

2.2　ISMS適合性評価制度の創設

我が国では情報処理サービス業のコンピュータシステムが十分な安全対策を

実施しているかどうかを認定する制度として「情報システム安全対策実施事業所認定制度」があった。この制度では、集中管理されていた情報システムの施設面や 設備等の物理的な対策に重点がおかれていた。しかしこれら物的・技術的側面への対応策だけでは不十分で、人が絡むセキュリティ対策、つまり人的セキュリティを含む、組織全体のマネジメントを確立する必要性が認識されるようになった。（旧）経済産業省では「情報セキュリティ管理に関する国際的なスタンダードの導入および情報処理サービス業情報システム安全対策実施事業所認定制度の改革（平成12年（2000）7月31日）」を発表し、従来の「情報システム安全対策実施事業所認定制度」を、平成13年（2001）3月31日をもって廃止することを決定した[iii]。この制度に代わるものとして「ISMS」（Information Security Management System：ISMS（情報セキュリティ・マネジメントシステム））が登場したのである。技術的セキュリティのほかに、人間系の運用・管理面をバランス良く取り込み、新しい制度としてISMSという適合性評価制度を創設することとなった。

2.3 ISMSとは

ISMSとは、「情報セキュリティの個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用するもの[iv]」とされている。この制度の運用は、組織の業態によって異なるが、いずれにしても組織が保護すべき情報資産に関して、「機密性」、「完全性」、「可用性」を効率良く維持し、問題や課題を発見・抽出した上で、継続的に改善のプロセスを進んでゆくということが根本理念となっている。

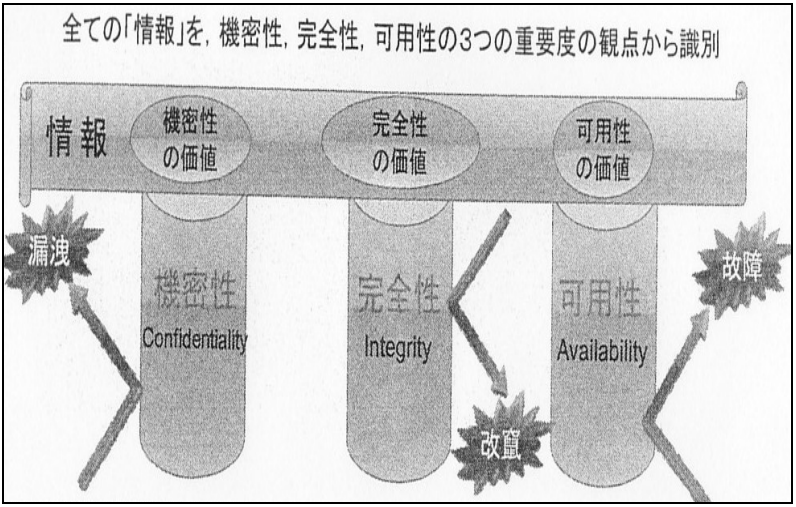

図1 「情報の価値に対する3つの観点」（静岡大学ISMS研究会（2007）[v]，p.14. より）

組織が保護すべき情報資産について、「機密性」(Confidentiality)、「完全性」(Integrity)「可用性」(Availability)をバランス良く維持し改善することが 情報セキュリティマネジメントシステム(ISMS)の基本コンセプトとされる(ISO/IEC 13335-1:2004より引用）[vi]。

「機密性」(Confidentiality)とは、認可されていない個人、エンティティ（団体等）又はプロセスに対して、情報を使用不可又は非公開にする特性であり、特定の人間だけにアクセス権を与えることを基本前提にしている。「完全性」(Integrity)とは、資産の正確さ及び完全さを保護する特性であり、情報の改ざんや破壊を防止することが基本前提になっており、「可用性」(Availability)とは、認可されたエンティティ（団体等）が要求したときに、アクセス及び使用が可能である特性であり、利用可能性を担保するものと理解される。ISMSの有効性を継続的に改善していくためには、経営管理論で一般的に述べられ、その重要性が重ねて指摘されている、PDCAサイクルを採用することが前提となる。PDCAサイクルとは、経営行動におけるPlan（計画策定），Do（導入・運用），Check

（見直し）を循環的に繰り返し実践することであり、それぞれの頭文字をとって「PDCAサイクル」と呼ばれている。特に防災や減災の分野の扱うリスクマネジメントの分野では、近年、その重要度が再評価されている。ISMSとの関係では、以下の実践が重要となると考えられる。

1. Plan　：自社の情報資産を精査して、情報セキュリティ対策の計画と目標を決定する。
2. Do　　：計画・目標を基準に対策の導入と運用を行う。
3. Check：Doで実践した対策の結果を監視して、適宜、積極的に見直しを行う。
4. Act　　：現場の情報セキュリティ担当者と経営陣で、改善・処置を行う。

このPDCAサイクルを慎重に繰り返していくことによって、当該組織の情報セキュリティレベルの向上を検討していくのである（図2参照）。

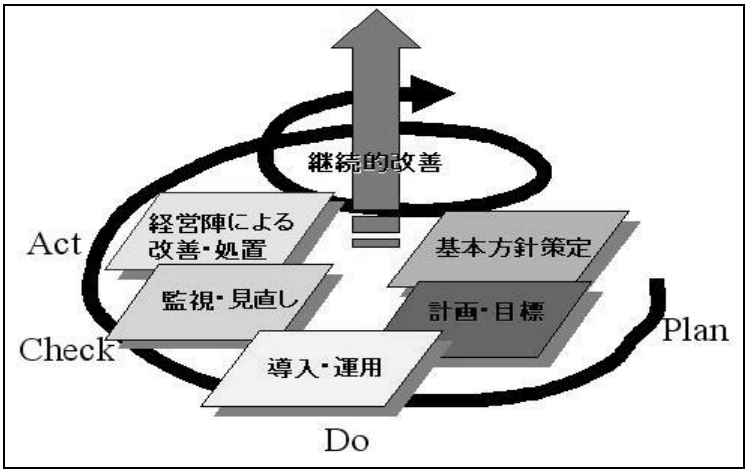

図2　情報セキュリティ対策におけるPDCAサイクルのイメージ
（「情報セキュリティマネジメントシステム(ISMS)とは」
(http://www.isms.jipdec.jp/isms/index.html) より）

3. ISMS導入・運用に関する考察

ISMSの導入・運用に関しては、そのメリットとデメリットがある[vii]。これらを慎重に検討しなければならない。それらのバランスを総合的に検証して、仮にデメリットが際立つのであれば、場合によっては運用を取りやめることも含めて、ISMSを組織制度としてどのように位置づけ、認識していくかを慎重に検討する必要がある。

現時点で報告されているメリット[viii]は、まず制度を導入することによる企業イメージの向上、同業他社との競争に打ち勝つこと、また組織を安定的に経営することである。営業上のイメージ向上、知名度の向上、顧客満足の向上、信頼性向上、競争優位性の維持、総合的な経営の安定化、これらが報告されている。特に顧客情報がそのまま経営資源として運用される業態の企業は、情報をどの程度安全に運用しているかが決め手になるので、これらのメリットの獲得は重要である。また情報資産に対するリスク（潜在するリスク、顕在するリスク、双方において）は、情報セキュリティの向上によって低減させる効果もあるとされる。また、情報資産の安全運用という大命題のほかに、この制度を導入することによって副次的効果も報告されている。社員の意識改革につながり、組織的に法令順守の精神が形成され企業倫理の向上にも役立つという。これは、ISMS制度の導入だけに見られる傾向ではない。ISMSはISO／IEC制度のひとつである。ISOシリーズとして、ISO9000シリーズ（品質管理に関するもの）、ISO14000シリーズ（環境マネジメントに関するもの）があるが、これらを導入した企業からも、社員の意識改革に役立った、企業倫理の向上に役立った、という報告がある。いわば副次的効果である。それまでの業務プロセスが刷新される際に、見落としていた改善点、問題などが浮き彫りになり、より良い業務環境の形成につながることが推察される。このことにより、社員の意識改革が促進され、その意識が集積したものが新たな企業倫理として生成され、組織に定着するものと考えられる。

しかしこのISMS制度はメリットだけではなく、デメリット[ix]も慎重にみてい

かなければならない。たとえば業務量が増加する問題である。ISMSの構築・運用のためには、文書化が義務付けられているため、利用者にとっては業務量が増加すると報告されている（ただし、適切なフォーマットを作成することで、セキュリティマネジメントは向上するとされている）。また新しい業務フローも発生する。 ISMSの要求事項に合わせて業務フローが追加・修正しなければならないことがあり、そのときは一時的に作業効率が落ちると報告されている。そのため、業務形態に対応したセキュリティ管理策を構築する必要があると指摘されている。ISO14000シリーズを導入・運用する企業からは、「外部監査を受ける前は、制度を適切に運用しているという結果を文書で示す必要があるため、数日間徹夜になることがあり、業務負担としては非常に大きい」という意見も出ている[x]。日産自動車が自身の再生を図るために、リバイバルプランを発表した。これは1999年に日産自動車のカルロス・ゴーンCOO（Chief Executive Officer：最高経営責任者）（当時）が発表した同社の経営再建計画であった。このとき取引業者数は従来の半分にすると宣言されたが、その選定のひとつの基準が、取引業者として、ISO9000や14000シリーズを取得しているか否かというものであった。ISMSは情報資産に関する組織システムである。特に情報サービスを提供する親会社は、データの整理・分析等のほとんどを子会社に任せていることが多いので、親会社よりも、子会社の方が情報セキュリティーを守っていく責任は重い。したがって親会社との取引関係を引き続き継続していくためには、子会社はISMS制度を積極的に導入し、健全に運用していることが強く求められると考えられる。

4. まとめ

現時点では、ISMSの導入・運用に関しては、メリットだけではなく、デメリットの方も慎重に検討する必要がある。特にデメリットは組織全体で時間をかけて検討していかなければならない。新たな業務負担やコスト負担は、特に中小企業においては深刻な問題としてのしかかる。システムの導入による企業イ

メージの向上、取引慣行の継続、労働意識の向上、これらの期待される効果が実現しても、組織としての負担があまりにも大きい場合、システムの導入そのものを再検討する必要があると考える。

注）

1. 「本人の意図しない個人情報の不正な流用や、個人情報を扱う事業者がずさんなデータ管理をしないように、一定数以上の個人情報を取り扱う事業者を対象に義務を課す法律のこと」（「個人情報保護法・個人情報の保護に関する法律」（@IT ,http://www.atmarkit.co.jp/aig/02security/protectionofpersonaldata.htm1））（2009年11月20日・参照）詳細は「個人情報の保護に関する法律」（首相官邸, http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/）を参照。
2. 下記URLもしくは文献から引用する際、文意を損なわれない程度に、適宜、表現を変えた箇所がある。

◆引用 URL

[i] 「海上自衛隊の「秘」情報がWinnyで流出、防衛庁が調査を開始」INTERNET Watch, http://internet.watch.impress.co.jp/cda/news/2006/02/23/10993.html（2011年5月5日・参照）

[ii] 「個人情報漏洩」, http://ja.wikipedia.org/wiki/個人情報漏洩（2011年5月5日・参照）

[iii] 「情報処理サービス業情報システム安全対策実施事業所認定制度」経済産業省, http://www.meti.go.jp/policy/netsecurity/nintei.htm（2011年5月5日・参照）

[iv] 「ISMS適合性評価制度」財団法人 日本情報処理開発協会（JIPDEC）・情報マネジメントシステム推進センター, http://www.isms.jipdec.jp/isms.html（2009年11月15日）

[v] 静岡大学ISMS研究会『実践ISMS講座』静岡学術出版事業部, 2007。

[vi] 前掲4,「情報セキュリティマネジメントシステム(ISMS)とは」http://www.isms.jipdec.jp/isms/index.html（2011年6月5日・参照）

[vii] 「ISMS」Security Akademia, http://akademeia.info/index.php?ISMS (2010年12月3日・参照)

[viii] 前掲6,「ISMS導入のメリット・デメリット」,http://akademeia.info/index.php?ISMS (2010年12月3日・参照)

[ix] 前掲6,「ISMS導入のメリット・デメリット」,http://akademeia.info/index.php?ISMS (2010年12月3日・参照)

[x] これは筆者の聞き取り調査によるものである。もちろん同制度を導入・運用するすべての組織がこのような状況を抱えていることを示すものではない。

◆参考文献

日本能率協会審査登録センター『審査委員が教えるISO27001実践導入マニュアル』日本能率協会マネジメントセンター, 2006.