IT 利活用推進のための
情報セキュリティマネジメントシステム構築及び運用について

大宮（おおみや）　則彦（のりひこ）[1]

【要旨】

情報財産の価値は、ＩＴ利活用により最大化が追求できる。しかし、機密性や技術的な制約等から最大化が困難であった。２１世紀に入りネットワーク、ＰＣ等が急速に一般的にも浸透し、技術的な制約が排除されつつある。残る最大の課題は、効率性、利便性の向上を図りつつ情報セキュリティを如何に確保するかにある。情報セキュリティマネジメントシステムの構築及び運用をベースとして、関係者の理解と協力を背景にしたＩＴ利活用推進について考察する。

キーワード：情報財産、ＩＴ利活用、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

１．　はじめに

政府が 2003 年に打ち出した「e－Japan 戦略Ⅱ[1]」の中で、２１世紀においても日本が世界の中で輝いた存在であり続けるためには、IT 利活用の推進が重要であることを強調している。しかし、現在 IT 利活用推進の前には大きな壁が立ちはだかっている。それは、IT 利活用における安全性について、関係者から信頼を得なければならないという壁である。関係者からの信頼は一朝一夕には得られない。組織の情報セキュリティ確保への取り組みについて、客観的かつ合理的な説得材料を提示しつつ理解を得なければならない。そして、何よりも重要なことは、信頼されるに足る実績を積むことにある。この壁を乗り越えるための有効な方法がある。情報セキュリティマネジメントシステム（以下、ISMS）を標準的な規格に則り構築及び継続運用し、その取り組みについて第三者評価機関から認証を取得することである。本学は、2002 年度より全学的な ISMS を構築し運用を開始した。また、2003 年 3 月には、国内の大学としては初めてとなる、「BS7799[2]：Part2」と「ISMS 適合性評価制度[3]」の認証をそれぞれ取得した。関係者に対してこれらの取り組みを説明した結果、関係者からの理解が得られ、2003 年度には長年の懸案であった学外からの各種サービスを開始することができた。今回の取り組みを通して得た知識や考え方を、本論文の中でわかりやすく提示したい。そして、今後 IT 利活用推進を目指す皆様の参考になれば幸甚である。

---

[1] 南山大学　総務部事務システム課

[2] BSI（英国規格協会）によって規定される、組織形態を問わない情報システムセキュリティ管理のガイドラインのことを指す。２部で構成されている。Part1 は「情報セキュリティマネジメントシステム（ISMS）の実施基準」、Part2 は「情報セキュリティマネジメントシステムの仕様」について記載されている。このうち Part1 は、2000 年に ISO と国際電気標準会議（IEC）より ISO 番号（ISO/IEC17799）が与えられ、国際標準化されている。Part2 は ISO 化に向けた検討が進められているところであるが、現在では世界的に情報セキュリティ管理に関する事実上の標準規格となっている。

[3] 財団法人日本情報処理開発協会（JIPDEC）が、2002 年 4 月から本格運用を開始した情報セキュリティマネジメントシステムに関する適合性評価制度。

２．　ISMS構築の取り組み動機について

2000 年度に本学では IT を軸として、教員・学生サービスの向上及び事務処理の効率化を図った。特に、情報流通においては革新的な取り組みを行った。従来は、事務職員が教員と学生の間に入って、情報流通における触媒的な役割を担ってきた。2000 年度以降は、IT の力を借りて極力事務職員が教員と学生の間に介在しなくても、情報がスムースに流通できるようにした。例えば、休講の伝達においては、従来教員から伝達を受けた事務職員が、掲示用の紙に休講情報を記載し、休講掲示板に貼り付けた。学生は、その掲示板まで足を運び、休講情報を確認していた。2000 年度以降は、教員が Web システムから休講情報を入力すれば、自動的かつ瞬時（20 分以内）に大学の HP、携帯電話用休講情報サイトそして、学内のプラズマディスプレイにそれらの情報が反映されるようになった。学生は、いつでもどこでも好きな方法で休講情報を確認することが可能となった。事務職員の介在が不要となったのである。このような取り組みを大学事務のいろいろな局面で展開した。

大学における主な利用者は、教員と学生である。利用環境の制約から従来は、教員や学生に直接情報入力や情報検索といったサービスを提供できなかった。それが、インターネットや PC の普及により、事務室に限定することなく IT 利活用環境を教室や研究室に拡大することができるようになってきた。しかし、2000 年当時、１点クリアすることができない壁があった。IT を利活用して学外から各種サービスを利用できるように試みたのだが、情報セキュリティに関する安全性について関係者からの理解が得られず断念したのである。これが、今回 ISMS を構築しようとした発端である。IT 利活用における安全性について関係者の理解及び協力が得られなければ、IT 利活用の推進はできないということを痛感した。理解を得るためには、合理的な説得ができなければならないが、組織の情報セキュリティレベルを客観的かつ合理的に証明することは非常に困難であることも同時に痛感した。この問題を克服する手段は、ISMS を標準規格に則り構築・運用し、その取り組みについて第三者評価機関より認証を取得することと考えた。関係者に対して、利用する業務やサービスにおける情報セキュリティ確保の確実性について、第三者評価機関よりの認証取得という事実で安心感を与えることができれば、関係者の理解及び協力が得られると考えたのである。

３．　情報セキュリティについて

情報セキュリティについてここで改めて定義を明確にしておきたい。

情報セキュリティとは、通常「情報財産を構成する３要素、機密性、完全性、可用性を維持すること。」[2] と定義されている。機密性と可用性については、あまり理解において齟齬は生じないと思われる。ここでは、完全性について意味を確認しておく。完全性は、「情報及び処理方法が、正確であること及び完全であることを保護すること。」[2] と定義されている。しかし、それだけでは完全性のカバーする範囲が狭くなる。完全性を広義に解釈し「情報財産が持つ本来の目的・役割を維持すること。」と捉えるのである。完全性に対する広義の解釈は、情報セキュリティ確保の過程における機密性偏重志向からの脱却に貢献する重要な要素となる。

４．　ISMSについて

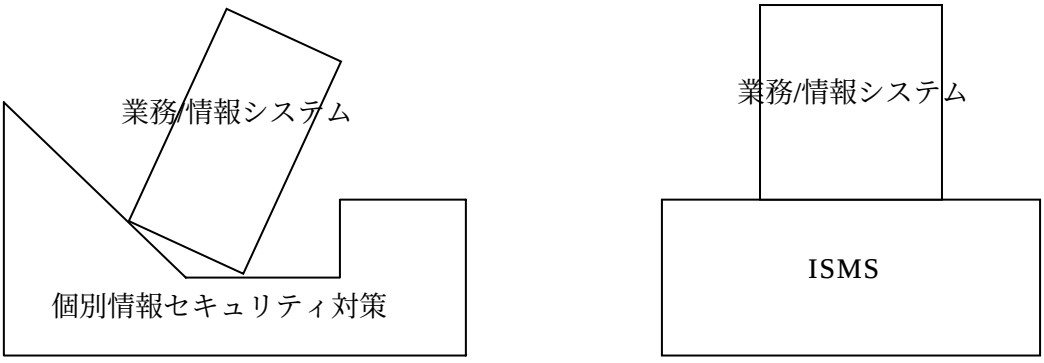
情報セキュリティ確保を確実にするためには、情報セキュリティ確保を管理する仕組みが必要となる。この仕組みのことを、情報セキュリティマネジメントシステム、ISMS と呼ぶ。

ISMS は構築しただけでは何の意味もない。PDCA（Plan-Do-Check-Act）サイクルで

継続して運用することが重要となる。『BS7799：Part2』も『ISMS 適合性評価制度』も、認証時の重要な審査ポイントは、組織内で情報財産が保護される仕組みが、継続して確実に運用されているか否かにある。ISMS の内容および継続運用が保証されれば、対外的にも対内的にも、『当該組織が保有する情報財産は確実に保護される仕組みを持ち、日々の運用もしっかりしている。』と言えるのである。

５．　ISMSの位置付けについて

従来、情報セキュリティというと後ろ向きのイメージが強かった。投資をする際にも費用対効果を説明しにくいという話をよく耳にする。しかし、これは、大きな誤解に基づいている。ISMS 単独では情報財産が保有する価値の有効活用はできない。同じように、業務や情報システムだけでも、リスクに対して無防備となることから、情報財産が保有する価値の最大化は望めない。業務や情報システムが ISMS を有効利用してはじめて、業務や情報システムが保有する各種の価値を最大化できる。従って、ISMS はすべての業務および情報システムのインフラと捉えることができる。きっちりとした ISMS が構築・運用できなければ、その上で稼動する各種業務や情報システムは非常に脆弱になる。結果、組織の信用が失墜し、利用者や顧客離れに繋がる恐れがある。そのイメージを、図 1 に示す。



ISMS 構築以前　　ISMS 構築後

図1　ISMS の位置付け

左側が、対症療法的に情報セキュリティ対策を行っている従来の情報セキュリティに対する姿勢をイメージした図である。右側が標準規格に則り ISMS を構築し、関係者の理解と協力を得ながら運用している ISMS のイメージである。右側の ISMS の上で稼動している業務や情報システムにおいては、安定かつ安全な状態での運用が可能となる。

ISMS 構築および運用について経営陣に対して説得する場合、必ず ISMS の上に構築する業務や情報システムとセットで行う必要がある。ISMS の導入だけを切り離して行うために、費用対効果が説明しずらくなる。業務や情報システムを稼動させるためには、ISMS は必須事項として捉えるべきである。

６．　IT 利活用までの流れについて

高度情報化社会においては、情報が非常に重要な財産となっている。情報を有効に利活用することが、大きなビジネスチャンスの創造や、同業他社との差別化等にもつながる。特に、IT を利活用することにより、情報財産が持つ本来の価値の最大化が追求しやすくなる。しかし、その背後にはリスクがつきまとう。機密情報漏洩、情報システムダウン、ホームページ改ざんなどの情報セキュリティ事故である。もし、これらのリスクが顕在化すると、組織の信用が失墜し、大きな負の財産を背負うことになる。このような事態に陥らないためにも、情報セキュリティの継続的な確保が必要となる。

情報セキュリティの継続的な確保のためには、関係者の理解と協力が絶対条件である。何故ならば、関係者特に ISMS の運用当事者である現場の人間にとって、ISMS にどんなメリットがあるかが最大の関心事だからである。現場にとって ISMS の運用が何のメリットもなければ、現場のモチベーションは上がらない。現場の協力が得られなければ、情報セキュリティの確保は覚束ない。従って、情報財産の価値を最大化するための IT 利活用の内容策定に際しては、現場と共同歩調をとるべきである。外部の攻撃から情報財産を守るため、あるいは認証を取得するために ISMS を構築し運用するといった説明を、現場の人間にしてはならない。それらは、中間目標にすぎないからである。最終目標は、あくまでも IT の利活用推進に設定し、その過程の中で ISMS の構築及び運用というステップをクリアしていくのである。IT 利活用実現までのステップを表 1 に示す。

表 1 IT 利活用に至るまでのステップ

ステップ	説　明
Ⅰ	現場と連携して、IT を利活用した情報財産価値の最大化に関する目標を設定する。
Ⅱ	組織の情報セキュリティレベルを把握する
Ⅲ	組織の目指す情報セキュリティレベルと比較し、不足しているあるいは、脆弱な部分の対策を行う。
Ⅳ	第三者評価機関に審査を依頼し、認証を取得する。
Ⅴ	関係者に対して情報セキュリティ確保に関する取り組みの説明を行い、安心感の醸成を図る。
Ⅵ	情報財産の価値を最大化するために IT の利活用を推進する。

表１内のステップⅡ及びⅢが、ISMS 構築及び運用に該当する。

組織は今非常に困難な状況に置かれている。そのような中で、ISMS は、組織に対して戦略的な行動を安心して起こすことのできる環境を提供する。ISMS を前向きに捉え、現場から受け入れられる積極的な目標を設定の上、ISMS の構築及び運用に取り組むことを推奨する。

7. ISMS構築手法

ISMS 構築には、２つのアプローチが必要である。１つは情報セキュリティポリシーの策定であり、もう一つがリスクマネジメントである。前者がトップダウンアプローチであるのに対し、後者はボトムアップアプローチである。両者は、別々のアプローチであるにもかかわらず、互いに密接な連携が必要である。両者を絡み合わせながら、最終的に整合性のとれた ISMS に収束させていかなければならない。イメージを図 2 に示す。

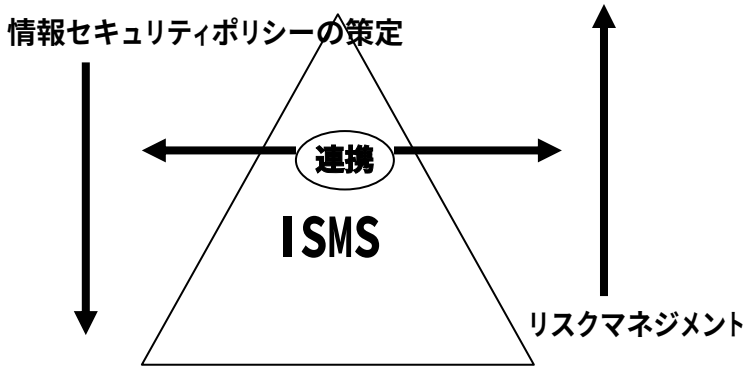


図 2 ISMS 構築イメージ

まず２つのアプローチについて個別に説明し、最終的にどのように両者の整合性を図るかについて解説する。

新たな IT 利活用推進を目標として設定した場合、IT 利活用に関係する新しい業務や情報システムについても ISMS 構築対象に含めるべきである。

７．１．　　情報セキュリティポリシーの策定

情報セキュリティポリシーは、ISMS の仕様や運用方法をドキュメントによって表現するものである。情報セキュリティポリシーの最終目標は、「組織の構成員が、情報財産を適切に扱い確実に保護できるようにすること。」である。ドキュメント体系は階層構造を有し、最上位層から基本方針/体制、ISMS 仕様書、実施基準、利用手引書/運用手順書、実施記録の順となっている。（図 3 参照）

ここで注意する点は、ドキュメント毎の対象範囲についてである。最上位に位置する基本方針から実施基準までは、組織全体で共通なドキュメントとすべきである。一方、利用手引書/運用手順書より下位の部分については、各部門/対象者固有のドキュメントとなる。

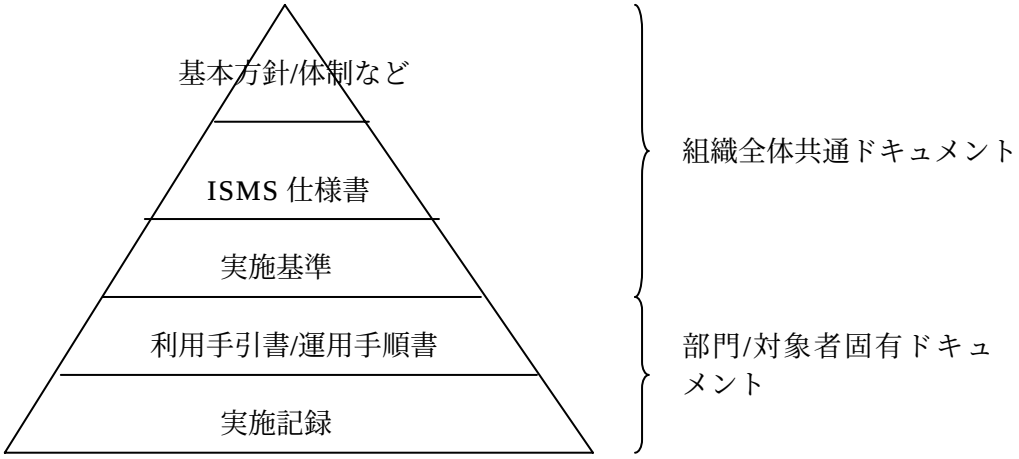


図3　情報セキュリティポリシー階層図

では、上位レベルから順に内容について説明する。ここでは、リスクマネジメントとの関係についても言及する。何故ならば、ISMS は単純な情報セキュリティポリシーとリスクマネジメントとの構造体ではなく、二つはもつれあった糸のような関係にあるからである。故に、ドキュメント毎にリスクマネジメントとどのような関係にあるかを説明する。

（１） 基本方針、体制など

ISMS 導入の目的、適用範囲（対象者、情報財産の種類等）、基本方針、体制及び責任、罰則等について記述する。組織が情報セキュリティ確保に取り組む姿勢を表明する役割を果たす。経営のトップクラスから組織全体に対して公布するような形式が望ましい。トップダウンで ISMS が組織全体に浸透していくからである。

リスクマネジメントとの関係であるが、本ドキュメントは全くリスクマネジメントとは関係がない。関係がないとは、リスクマネジメントの結果によってこのドキュメントに影響は生じないということである。

認証取得対象範囲を限定的にしたとしても、本ドキュメントの対象範囲は限定的にすべきではない。本ドキュメントは、組織全体に対して共通的な位置付けでなくてはならない。

（２） ISMS 仕様書

本ドキュメントによって、当該組織の ISMS の全体像が俯瞰できるようにする。内容は、国際規格（BS7799：Part2）または国内規格（ISMS 認証基準）に則って作成する。

本ドキュメントは、リスクマネジメント開始前、あるいはリスクマネジメントと並行的に策定が可能である。ISMS 構築目標に設定した IT 利活用のための新たな業務や情報システムも含めて策定対象範囲とする。

リスクマネジメントの結果、リスク対策が必要と判断された場合、本ドキュメントに反映しなければならない場合がある。それには、２つのケースがある。１つ目は、既存業務及び情報システムについてリスクマネジメントを行った結果、追加のリスク対策が必要と判断された場合である。もう１つのケースは、新たな IT 利活用を軸として業務や情報システムを稼動させようとした場合に、新たなリスク対策が必要と判断された場合である。

（３） 実施基準

情報セキュリティを確保するための詳細管理策を、業務のまとまり（プロセス）単位で記述する。詳細管理策は、大きく２つに分類できる。１つは法的観点等から組織にとって不可欠であると考えられる管理策、一般的にコンプライアンス（適合性）と言われている。もう１つは、最良慣行（ベストプラクティス）と考えられる管理策である。これらについても、国際規格（ISO/IEC17799）または国内規格（ISMS 認証基準）に記載されている。組織内で共通的な内容を記述する。次のレベルのドキュメントである「利用手引書/運用手順書」を策定する際のガイドとなる。

このレベルのドキュメントは、かなりリスクマネジメントとの関係が深い。何故ならば、リスクマネジメントの結果選択される詳細管理策と、本ドキュメントで記載する詳細管理策は同じレベルの内容だからである。

（４） 利用手引書/運用手順書

各部門あるいは利用者が、実際に情報財産を取り扱う方法について詳細に記述する。作成者は、ISMS 仕様書あるいは実施基準に則り作成する。対象範囲は、作成した部門あるいは対象者を限定したものとなる。一般的な表現は避け、極力実態に沿って詳細に表現する。本ドキュメントの内容とレベルに、ISMS の成否がかかっていると言っても過言ではない。現場の理解および協力の大きさが、本ドキュメントの質に大きく影響する。

従来このレベルのドキュメントは、情報セキュリティポリシーの範疇に入れられてはいなかった。敢えて本ドキュメントを情報セキュリティポリシーの中に入れる理由は、情報セキュリティポリシーの作成目標を「組織の構成員が、情報財産を適切に扱い確実に保護できるようにすること。」に設定しているからである。従って、情報セキュリティポリシーの中で、一番重要な位置を占めているとも言える。

特に、個人情報保護を確実にするためには、本レベルのドキュメントを如何に関係者に対して周知徹底できるかが非常に重要なポイントとなる。

参考のため、本学で作成した情報財産利用手引書（教員用）抜粋を附録に掲載する。

（５） 実施記録

本ドキュメントは、ISMS を実際に運用していく過程で蓄積される成果物である。従って、ISMS 構築時に作成する必要はない。

７．２． リスクマネジメント

組織が保有する情報財産を洗い出し、情報財産毎に想定したリスクを分析し、リスクの評価を行い、組織が許容できないリスクについては事前にコントロールする。これにより、情報セキュリティに関する事故を未然に防いだり、あるいは情報セキュリティ事故の影響を最小限に抑えたりすることが可能となる。これが、リスクマネジメントである。きっち

りとした組織的なリスクマネジメントを行えば、見えないリスクに怯えることもなく、情報セキュリティ対策投資の最適化が図れる。

（1）　前準備

リスクマネジメントを行う前に、共通的に行っておくことがある。国際規格あるいは国内規格に則って、リスクを想定することである。

国際規格あるいは国内規格には、2種類の要求事項が記載されている。1つは、組織が必要性を判断して選択する性質の要求事項であり、８６項目ある[4]。もう1つが、あらゆる組織について汎用的に必要性が認められる要求事項であり、選択の余地はなく対策することが義務付けられている。項目数としては、４１項目ある[5]。

要求事項は、何らかの必要性があって存在している。必要性の発生がリスクによるものと考えれば、要求事項からリスクが想定できる。表2に、詳細管理策から想定したリスクの例を4つ示す。

表2　詳細管理策からのリスク想定（例）

管理策区分	詳細管理策	想定リスク
装置の設置及び保護（注1）	装置は、環境上の脅威及び危険からのリスク並びに許可されていないアクセスの可能性を軽減するように設置又は保護すること	環境からの影響または不正アクセスを受ける所に、必要な保護をしないまま重要な装置が設置されているリスク
暗号化（注1）	取り扱いに慎重を要する又は重要な情報の機密性を保護するために、暗号化を用いること	重要なデータが暗号化されていないまま要員に取り扱われ、データが漏洩するリスク
情報の取り扱い手順（注1）	許可されてない露呈又は誤用から情報を保護するために、情報の取り扱い及び保管についての手順を確立すること	重要な情報の取り扱い・保管の手順が明確でない状態での運用リスク
セキュリティ基本方針との適合（注2）	管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正しく実行されることを確実にすること 組織内のすべての範囲について、セキュリティ基本方針及び標準類に適合することを確実にするために、定期的に見直すこと	組織の情報セキュリティ活動が情報セキュリティポリシーに準拠していることを検証しないまま情報セキュリティ活動を実施しているリスク

（注1）　組織が必要性を判断して選択する性質の要求事項

（注2）　あらゆる組織について汎用的に必要性が認められる要求事項

（2）　レベルの設定

リスクマネジメント実施上で必要となる要素のレベルを設定する。表3に設定例を示す。

---

[4] 情報セキュリティマネジメントシステム適合性評価制度、ISMS 認証基準（Ver．２．０）附属書「詳細管理策」7．～１０．

[5] 情報セキュリティマネジメントシステム適合性評価制度、ISMS 認証基準（Ver．２．０）附属書「詳細管理策」3．～6．１１．１２．

表3　レベル設定例

要素名	レベル	内　　容
財産価値評価	1	見られても、壊されても全く問題がない情報財産
	2	見られてもいいが、壊されてはいけない情報財産
	3	見られても、壊されてもいけない情報財産
	4	見られたり、壊されたりすることによって、組織全体にダメージを与える可能性がある情報財産
脅威	１～５	情報財産に与えるダメージの大きさ（１→大きさ→５）
脆弱性	１～５	脅威が発現する可能性（１→可能性→５）
リスク評価値	１～１００	財産価値評価×脅威×脆弱性
許容値	４０	組織として許容できる範囲の数値を設定する。例えば、４０とした場合、４０までは許容するが４０を超えるリスク評価値については何らかのリスク対応を行う必要がある。 この値は、リスク対応を行うか否かの分岐点であるが、ある程度主観的な設定になることは避けられない。

（3）　情報財産の洗い出しと財産価値評価

リスクマネジメントは、通常対象範囲を限定して、その範囲内の情報財産を明確にした上で着手する。情報財産の洗い出しは、業務単位とする。データの発生から始まって、業務の流れに従って情報財産を洗い出す方法を推奨する。同一情報財産が複数回出現しても構わない。洗い出した情報財産は、表４の区分に従い分類する。

表4　情報財産分類区分

大区分	小区分	説　　明
情報	電子媒体	HD、FD などの電子媒体内に存在する情報財産
	電子外媒体	紙などの電子外媒体上に存在する情報財産
	要員帰属情報	記憶や会話など人に帰属する情報財産
業務/情報システム	ハードウエア	サーバ、PC、プリンタなど
	ソフトウエア	OS、DB などの汎用製品
	施設/設備	建物、空調、マシンルーム、ネットワークなど
	業務/サービス	アプリケーションプログラムも含む
人的財産	人	人に危害が及ぶ場合

情報財産価値を評価する場合、業務の流れを意識して価値を見積る。例えば、同じアカウント/パスワードであっても、重要な業務の場合とそうでない場合では、価値は異なる。

この段階での成果物は、財産評価一覧表である。イメージは、業務単位に情報財産が分類され、財産価値評価レベルが設定されている表である。

（4）　情報財産の整理

重複して洗い出された情報財産を１つに集約する。その場合、財産価値評価レベルの高い方に集約する。整理は、情報財産分類区分に従い行う。

次のステップである現状リスクアセスメントの前準備としての作業のため、財産価値評価レベル１の情報財産については除外してもよい。

（5）　現状リスクアセスメント

整理した情報財産毎にリスクを想定し、その場合の脅威レベルと脆弱性レベルを評価する。ここで注意する点は、現時点で実装されている詳細管理策を考慮してリスク評価を行

うことである。以下に、リスク、脅威、脆弱性、詳細管理策についての基本的な考え方を示し、それを踏まえてリスク評価する上でのポイントを指摘する。最後に実践的なリスクアセスメントについて例示を交えて解説する。

ア.　リスク

リスクとは、脅威が何らかの脆弱性によって発生する確率や起きた時のダメージの大きさを総合的に表現した語句である。リスクは、情報財産、脅威および脆弱性で構成された文章で表現する。例えば、「DB サーバの故障のために、情報システムが停止する。」というような文章である。情報財産に対応させるリスクは、「前準備」で想定した内の組織が必要性を判断して選択する性質の８１項目である。

選択の余地はなく対策することが義務付けられている４１項目のリスクについては、ある特定の情報財産とリンクさせる必要はない。何らかの詳細管理策を選択して、リスクが許容できるレベルまで低減されていることが確認できなければならない。MUST リスクアセスメントと呼んで、他のリスクと区別してリスクアセスメントを行う必要がある。

イ.　脅威

情報財産に対して障害や損害を与える事象である。情報財産は、機密性、完全性、可用性の 3 要素で構成されている。脅威とは、この 3 要素に対して何らかの影響・ダメージを直接的に与える事象である。よって、脅威の種類は、機密性脅威、完全性脅威、可用性脅威の３つである。情報財産と脅威の関係を図４に示す。

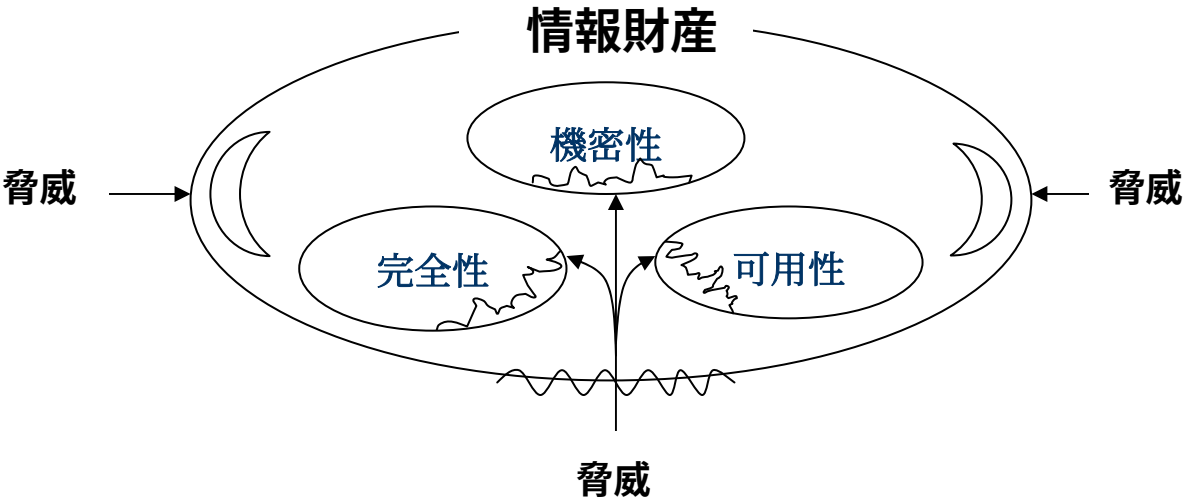


図4　情報財産と脅威の関係（イメージ）

「地震によって、建物が倒壊する」というリスクについて考えてみる。情報財産を建物とした場合、脅威は建物の 3 要素に損害を与える事象であるので、「建物の倒壊」という事象である。完全性と可用性にダメージを与えている。地震は、いや正確には地震の揺れや地震によって発生する地割れなどが「建物の倒壊」という脅威を引き起こす。一般的に、地震自体を脅威として捉えがちであるが、地震は直接的な被害を情報財産にはもたらさないので、脅威ではない。脅威を情報財産に対して直接的にダメージを与える事象と捉えれば、リスク分析をシンプルにすることが可能となる。表５にリスクと脅威の関係を例示する。

表5　リスクと脅威の関係

リスク	情報財産	脅威種別	脅威
地震によって建物が倒壊する	建物	完全性/可用性	建物の倒壊

ウ.　脆弱性

脆弱性とは、脅威が発現する原因である。逆に考えれば、脆弱性を取り除けば、脅威自体発生しなくなる。先程の例で考えると、建物が倒壊する原因が脆弱性であるので、建物の倒壊に繋がる地震災害を洗い出せばよい。それらの関係を表６に示す。

表6　リスクと脅威/脆弱性の関係

リスク	情報財産	脅威	脆弱性
地震によって建物が倒壊する	建物	建物の倒壊	地震による激しい揺れ
			地震による地割れ
			地震によるがけ崩れ
			地震による津波

ここまでが、リスク分析である。まだ、脅威レベルも脆弱性レベルも設定する必要はない。情報財産毎にリスクを想定し、そのリスクを脅威と脆弱性に分けるところまで行う。

エ.　詳細管理策

詳細管理策には、4 種類ある。抑止、防備、検出（発見）、回復（修復）の 4 つである。抑止は、脅威自体の発生を防ぐ対策であり、残りの 3 つは脅威が発生した後の対策である。先程の例であれば、免震対策を施すことが抑止になり、耐震構造の家にすることは防備になる。地震計の設置は、検出であり、自衛隊やボランティア組織との緊密な連携が、災害からの迅速な回復になる。脆弱性を脅威の発生原因と捉えれば、抑止は脆弱性への対策であり、残りの 3 つは脅威への対策となる。脅威が脅威で無くなったり、脅威による情報財産への影響を軽減したりする対策である。ことわざで表現すれば、脆弱性への対策は「転ばぬ先の杖」であり、脅威への対策は「備えあれば憂いなし」となる。上記までの内容を、表７にまとめた。

表7　詳細管理策の分類

種類	効　果	対 象	ことわざ
抑止	脅威の発生を未然に防ぐ	脆弱性	転ばぬ先の杖
防備	脅威の影響を極力抑える	脅威	備えあれば憂いなし
検出	脅威の発生を検知する		
回復	障害から早期回復する		

現状において実装されている詳細管理策を、4 つに分類する。それによって、対策のバランスが判断できる。例えば、ほとんど脅威を発生させないような対策を行っているにもかかわらず、脅威対策もしっかり行っていれば、過剰対策となる。逆に、検出ばかりに力を入れた管理策では、対策の強化が望まれる。ここまでが、リスク評価をする前準備となる。

オ.　リスク評価ポイント

ここからは、前述した内容を踏まえながら、リスクを評価する流れ及びポイントについて、例を挙げながら説明する。

まず、「DB サーバ内のディスクに障害が発生して、データが破壊される。」というリスクを分析した結果を表８に示す。

表8　リスク分析

情報財産	脅威	脅威種別	脆弱性（脅威発生原因）
データ	データ破壊	可用性/完全性	DB サーバ内のディスクに障害が発生する

データを情報財産とした場合、脅威は、データの可用性と完全性にダメージを与える「データ破壊」であり、脆弱性は、データ破壊を引き起こす原因の「DB サーバ内のディスク障害」である。

次に、詳細管理策について現状分析する。まず、脆弱性への対策であるが、「DB サーバ内のディスクに障害が発生する」こと自体を防ぐ方法を洗い出す。方法としては、設置場所内の温度や湿度管理の徹底や一定期間安全性を担保するための定期点検整備等がある。これが、抑止効果である。次に、脅威発生後の対策として、防備を洗い出す。ディスクが二重化されていれば、ディスク障害が発生したとしても直接データ破壊につながらない。脅威が脅威でなくなる対策である。検出については、毎日ディスクアナライズを実行し、軽微なレベルでディスク障害を発見できれば、大事にはいたらないかもしれない。最後に回復についてであるが、データ破壊という事態にかりになったとしても、前日のバックアップがあれば最悪前日の状態までは戻すことができる。回復訓練が定期的に行われていれば、回復に要する時間も最短に抑えることができる。

上記までの内容を表９にまとめた。

表9　脅威/脆弱性と管理策との関連

管理策の内容	脅威/脆弱性区分	管理策の種類
DB サーバ設置場所の温度/湿度管理	脆弱性	抑止
DB サーバ定期点検整備	脆弱性	抑止
ディスクの二重化	脅威	防備
定期的なディスクアナライズの実施	脅威	検出
定期的なデータバックアップ取得	脅威	回復
障害回復訓練の実施	脅威	回復

このような対策の効果を総合的に加味しながら、脅威レベル、脆弱性レベルを評価する。評価は、ある程度主観的にならざるを得ない。しかし、リスクが国際基準や国内基準に則り洗い出され、かつ詳細管理策も世間一般的に網羅されていることが重要なのである。今までは、すべてが主観的であったことを考慮すれば、飛躍的に客観性がアップしたと言える。

実際にサンプルを用いて、リスク評価のイメージを示す。表１０にリスク評価で使用するリスクアセスメントシートを掲載する。想定リスクをここでは２項目にしているが、本来は横方向に８６項目記述する。では、表の作成方法を以下に説明する。（①～⑥）

① 情報財産毎に財産価値評価レベルを設定する。

② 想定したリスクについて分解した脅威と脆弱性を記述する。この場合、情報財産と関係するリスクについてのみ対象とする。

③ 詳細管理策は、脅威と脆弱性に対応させて記述する。種別も記入する。

④ 関係する想定リスク毎に、管理策の効果算定を行う。効果算定とは、その管理策によって、どの程度脅威あるいは脆弱性の危険度が減じられるかを測定するのである。効果は、３段階で表現する（◎：効果大、○：効果あり、△：あまり効果なし）。なお、当該リスクと関係のない場合は、「―：該当せず」を記入する。
ここで、重要なポイントは、組織における要求事項である。例えば、ノンストップシステムを要望しているのか、あるいは１日だけならダウンしてもよいシステムなのかが明確になっていることが重要である。この要求事項に従って、管理策の効果を評価することになる。情報セキュリティポリシーで組織固有の要求事項を明確化しておくことが望ましい。

⑤ 情報財産毎に、脅威、脆弱性そして、実装されている詳細管理策の効果を総合的に評価して、脅威レベルと脆弱性レベルを設定する。

⑥ リスク評価値を算出する。リスク評価値は、財産価値評価レベル、脅威レベル、脆弱性レベルの３つの積で求める。

表10 リスクアセスメントシート(例)

情報財産	財産価値評価レベル	脅威レベル	脆弱性レベル	リスク評価値	脅威	脆弱性	詳細管理策		想定リスク	
							種別	内容	特に重要な財産が取り扱われたり、保管されたりするオフィス、施設等が他のものと区別なく対策もされないまま一律に管理されているリスク	環境からの影響または不正アクセスを受ける所に、必要な保護をしないまま重要な装置が設置されているリスク
建物	4	3	2	24	倒壊	地震の揺れ	抑止 防備	耐震構造 免震構造	◎ ◎	―
						がけ崩れ	抑止	地質調査	○	―
						老朽化	抑止	定期点検 整備	○	―
マシンルーム	4	3	2	24	侵入	不審者	抑止	入退室管理	◎	―
							抑止 検知	ビデオカメラ	○	―
					破壊	地震一般	「建物」参照		◎	―
						高温・火災	防備	消火器設置	△	―
								防火扉	○	―
								ハロゲンガス	◎	―
							検知	火災報知機	○	―
DBサーバ	4	3	3	36	破壊	建物倒壊	「建物」参照		―	◎
						地震一般	「建物」参照		―	◎
							防備	ボルト固定	―	◎
						高温・火災	「マシンルーム」参照		―	◎
						侵入者	抑止	入退室管理	―	◎
						故障	抑止	定期点検	―	◎
							防備	コールドスタンバイ	―	◎
							回復	保守契約締結	―	◎
							回復	危機管理マニュアル整備	―	○
							回復	障害回復訓練	―	○
							検知	連絡体制確立	―	○
					盗難	「侵入者」の項参照			―	◎
					停止	停電	防備	CVCF/UPS設置	―	◎

◎:効果大、○:効果あり、△:あまり効果なし、―:該当せず

（6） リスク対応

リスクアセスメントによって求めたリスク評価値と組織が設定した許容値を比較する。リスク評価値が許容値を超えた場合、下記に示す選択肢からリスク対応を選ぶ。リスク評価値が許容値以内であれば、リスクを意識的に保有することになる。残存リスクと呼ばれている。また、たとえリスク評価値が許容値を超えていても、そのままリスクを保有することもある。この決定については、経営トップクラスの判断が必要となる。

ア．リスクを低減する（適切な詳細管理策を採用する）

イ．リスクを回避する（リスクと関係のある業務や事業を中止する）

ウ．リスクを移転する（保険契約を締結する）

（7） 管理目的および詳細管理策の選択

リスク低減を選択した場合、適切な詳細管理策を選択して、リスク評価値を許容できるレベルまで低減しなければならない。ここでポイントとなる点は、費用対効果である。費用の制約から選択できる詳細管理策が限定される。しかし、許容値を満足できるリスク評価値にしなければならない。このバランスが難しい点である。業務経験者や IT 専門技術者の判断が重要になる。

（8） リスクの再評価

詳細管理策の選択後、再度想定したリスクについて脅威および脆弱性の再評価を行う。リスク評価値が許容できるレベルをクリアしたかを最終確認する。

リスク評価する時点で留意すべき点がある。それは、情報財産を取り扱う場所についてでである。情報財産を非常に安全性の高い場所で扱うこと自体が詳細管理策となる。例えば、1 万円札を金庫のような機密性の高い建物の中で取り扱う場合と、公共の面前で取り扱う場合を比較すると、同じ１万円という情報財産に対して管理策の選択内容が大幅に異なる。前者は金庫への入退室管理を行うぐらいでよいが、後者は警備員を配置するとか保険をかけるとか、いろいろな管理策が必要となってくる。1 万円札を盗られるという脅威に対する脆弱性のパターンが前者と後者で全く異なるからである。情報財産を取り扱う場所も含めて詳細管理策の選択および評価を行う必要がある。

リスクマネジメントの目的は、情報財産毎にその取り扱うシチュエーションも考慮した適切な取り扱い方法の明確化である。これにより、組織が保有する情報財産が確実に保護されることを目指すのである。

７．３． 情報セキュリティポリシーとリスクマネジメントとの融合

（1） 融合方法

情報セキュリティポリシーとリスクマネジメントを個別に見てきたが､本来の作業は両者を同時並行的に進め、必要の都度整合性を図る手法となる。最終的に一貫性があり、かつ統合された ISMS の構築および運用を目指すのである。

まず、リスクマネジメントの結果から情報セキュリティポリシーに対して、新たな要求事項が発生するケースを説明する。例えば、本学のケースでは、新たに学外からサービスを行う場合、従来のアカウント/パスワードによる本人確認に加え乱数表によるチャレンジレスポンス方式の導入が決定した。学外からのアクセスを想定すると、なりすましによる不正アクセスのリスクが高まる。この対策のため、乱数表によるチャレンジレスポンス方式を導入すれば、なりすまし防止効果はかなり上がると考えた。これは、リスクマネジメントの結果、導かれた対策である。乱数表によるチャレンジレスポンス方式の記述を、ISMS 仕様書及び実施基準に反映した。また、学外からできるサービスについて、利用者に説明するためのパンフレットも新たに作成して配布した。

逆のケースもある。実施基準や ISMS 仕様書が不明確なために、リスクマネジメントができないケースである。この場合、ISMS 仕様書や実施基準を先に固めなくてはならない。例えば、物理的なエリアを隔離して情報財産の安全性を確保する場合、幾つかのセキュリティ境界を利用することが要求されている。領域毎に保護基準を設定することを、セキュリティエリア管理レベルと呼ぶ。セキュリティエリア管理レベルが未設定であると、情報財産をどこに保管するかという詳細管理策が選択できない。このため、リスクマネジメントを行う前に、セキュリティエリア管理レベルを情報セキュリティポリシー上で明確に設定しておかなければならない。

世間一般において、情報セキュリティポリシーの策定が取り上げられているが、リスクマネジメントを伴わない情報セキュリティポリシーは、実世界において何ら機能しない。何故ならば、ボトムアップからの要求事項が反映されていないからである。現場や利用者から受け入れられる ISMS は、現場や利用者が扱う情報財産に対してきっちりとしたリスクマネジメントが行われ、その結果を情報セキュリティポリシーに反映させてある。その情報セキュリティポリシーが、多様化する雇用形態や複雑化する利用環境に対応しつつ、現場や利用者が保有する情報財産の保護に大きく貢献するのである。

（2） 融合確認方法

両者の融合状態を確認する方法として、第三者評価機関による審査以外に IT レベルの確認テスト[6]がある。ISMS が有効に機能しているか否かを調査するために実施する。目的は、国際規格（BS7799：Part2）や国内規格（ISMS 認証基準）に基づくマネジメントシステムの管理策が、IT 領域においてどの程度の情報セキュリティレベルを具現化しているかを明確にし、今後の対策計画に反映させることである。IT レベルの確認テストは、認証取得と合わせ、管理と技術の両面において名実ともに情報セキュリティの確保された組織とすることに寄与する。

ただし、この確認は一過性のものであることを十分認識しておかなければならない。IT 領域における変化は目まぐるしく、ある日 OK であっても、次の日も OK である保証はない。結果に一喜一憂することなく、情報システムが持つ脆弱性の本質について検討・分析のきっかけを作るという位置付けであることを認識しておく必要がある。この認識の上に立って、定期的に IT レベルの確認テストを実施する運用を推奨する。

8． ISMS継続運用のポイントについて

情報セキュリティ確保を継続的に確実にするためには、人に対しての教育及び情報財産を扱う際のルールの徹底などがとても重要である。本学では、2003 年 6 月からスタートした Can@home（キャンアットホーム：南山大学専用学外利用サービス）[7]を利用する希望者には、理解度確認テストで 90%以上の正答率を課している。これで、利用する人に対して一定レベルの情報セキュリティ能力や知識が確保できると考えている。方法としては、まず利用希望者には、ｅ－Learning 上で情報セキュリティに関する基礎知識やサービスを学外から受けるための仕組み、手続き方法、ルール等について学習してもらう。その上で、

---

6 代表的なテストには、ペネトレーション（侵入）テストがある。

7 大きく、学生用サービスと教員用サービスの２つがある。前者は、学生が学外から教務関係手続きを行うことをサポートしたサービスである。具体的な業務には、個人時間割表チェック、単位数集計表チェック、定期試験個人時間割表チェック、単位認定実例集検索、授業科目登録、成績確認、卒業見込シミュレーションがある。後者には、休講・補講情報登録、個人担当表確認、定期試験監督割当表確認、時間割確認、受講者名簿検索などがある。利用時間帯は、基本的に 7：00～23：00 である。

理解度確認テストを受験してもらい、90%以上正答した人のみに Can@home の利用を許可している。具体的には、学外からアクセスする場合に必要となる乱数表の発行を合格者のみに行っている。発想の転換を行ったわけである。従来は、IT 利活用のために利用者への教育を一生懸命行った。しかしながら、あまり効果は上がらなかった。まず、説明会を開催してもあまり人は集まらなかった。集まった人間についても、理解度の確認までは行えなかった。このような状況を打破するため、IT 利活用の条件として、情報財産取り扱いに関する知識を設定したのである。つまり、IT を利活用したければ、条件をクリアしなさいとしたわけである。利便性の高いサービスであれば、利用者は一生懸命自己の情報セキュリティレベルのアップに励む。先程の理解度確認テストの受験状況を見ていると、何度も 90%以上をクリアしようとチャレンジしている。涙ぐましささえ感じる状況である。

利便性と情報セキュリティの確保がトレードオフの関係にあるというのは、ミクロのレベルだけの話である。マクロのレベルにおいては、両者は相乗効果の関係にあると言える。何故ならば、利便性を上げれば、先程の例のように利用者の情報セキュリティレベルを意図的に上げることが可能である。また、情報セキュリティレベルを上げれば、情報財産の持つ価値を十分に引き出すことが可能となり、各種の利便性向上に取り組める。実際、本学では、ISMS 構築・運用および認証取得を契機として、Can@home という大学が持つ情報財産（個人情報）の有効活用を図ったサービスを稼動できた。利便性と情報セキュリティを上手に絡めて、ISMS を運用することが継続的な運用のポイントになる。

もう一つ、ISMS が関係者に浸透するポイントとしては、組織的な取り組みがある。特に、経営のトップクラスの参画及び理解は必須要件である。このためにも、経営のトップクラスに対して、ISMS は全ての業務/情報システムのインフラであり、IT 利活用の前提であることを理解して頂く必要がある。それができれば、情報セキュリティ確保のための必要な投資や人的資源の再配分等への理解・承認がスムースに行われる。

９．　ISMS継続運用のメリットについて

ISMS は、すべての業務および情報システムの基盤である。基盤がしっかりしていれば、その上に構築する業務や情報システムには、次に示すメリットが享受できる。

（１）　情報セキュリティ対策投資の最適化

従来は、見えない脅威に怯え必要以上の情報セキュリティ対策をしがちであった。ISMS では、情報財産に対するリスクアセスメントを行い、リスクを明確化し許容できるリスクレベルまで低減するような管理策を施す。リスクマネジメントから導かれた最適な管理策を実施することにより、情報セキュリティ対策にかかる投資の最適化が実現できる。今回の Can@home を稼動させる上で、情報セキュリティ確保の方法について議論を重ねた。暗号化の強化、本人確認の強化を中心にした議論であったが、最終的には費用対効果、利便性等を考慮して、乱数表によるチャレンジレスポンス方式及び業務単位でのアクセス制御の導入が決定された。専門家も交えた実務者会議及び経営のトップクラスが参画した最高意思決定機関を通しての議論は、投資内容決定プロセスの透明化にも寄与できたと感じた。

（２）　情報財産取り扱い方法の統一化および徹底

従来は、主観的な判断基準で情報財産の取り扱い方法を決めていたが、ISMS では客観的な判断基準に則った取り扱い方法の徹底を関係者に求めている。

学生の個人情報を例にとって説明する。学生の個人情報は重要であり、機密に属することの認識については誰もが同じ意見である。しかし、その取り扱い方になると、担当者個々の判断に頼りがちであった。ある管理者は、事務室内であれば画面上に学生個人情報が表示されていても問題はないと判断しても、別の管理者は、無人で表示されている

ことが機密漏洩につながると判断することもある。一事が万事である。このような状態を回避するためには、情報財産毎に木目細かく取り扱い方法を指示する必要がある。ISMS 構築・運用においては、きっちりとした客観的な判断基準に則った取り扱い方法を関係者に対して示すことができ、かつ実践できるようになる。これが、ISMS 構築・運用における大きなメリットである。実際、本学における教務関係の情報財産の取り扱い方法について、統一および徹底を図っている。特に、関係者毎に保有する教務関係の情報財産を明確化し、どのように扱うべきかの徹底を図った。それが、情報セキュリティポリシー内の利用手引書である。関係者毎に教育方法を変え、情報財産の適正な取り扱いを徹底している。教員については、「情報財産利用手引書（教員用）」の配布、情報セキュリティに関する説明会に加え e-Learning 上での知識修得及び理解度確認テストの実施も行っている。学生については、e-Learning 上での知識修得及び理解度確認テストを実施している。事務職員については、情報セキュリティに関する説明会に加え、各課室単位で情報セキュリティミーティングを複数回開催し、教育の徹底を図った。特に、新たに配属された職員（専任、非常勤問わず）については、情報セキュリティ講習会の受講を義務付けている。このように、具体的にかつ対象者も特定して教育することが重要なポイントである。今までは、個人的な依頼レベルであったが。ISMS では基準やルールになり、組織的な対応が可能となった。ここが大きな違いであり、メリットである。今までの内容を、従来と ISMS 稼動後とを対比させる形で表１１にまとめた。

表11　ISMS 継続運用のメリット（情報財産の取り扱い方法の統一化）

比較ポイント	従来	ISMS 稼動後
判断基準	主観的	客観的（基準書）
指導内容	抽象的（例：この資料はとても重要だから、しっかり保管しておくこと。）	具体的（例：この資料は財産価値評価レベル４であるので、セキュリティエリア管理レベル A で保管すること。）
徹底度	低い	高い（組織的）
対象者と情報財産との関係	不明確	明確（手引書）

大学では、学生の個人情報を扱う機会および関係者が多様化している。このような中で、学生の個人情報を保護することは、IT セキュリティだけでは限界がある。ISMS は、IT セキュリティばかりでなく人的管理セキュリティも対象としている。従って、情報セキュリティを確保するという点においては、非常に確実かつ有効な手段であると考える。

（３）　説明責任の達成

国際規格あるいは国内規格に則って ISMS を構築し継続運用することにより、教務関連業務で扱う情報財産を第三者が審査する制度によって適切に管理されていると証明できた。大学設置基準に代表される教育・研究への『第三者評価制度』に相当する客観性を、本学ではこの ISMS の認証取得によって事務的な分野にも導入したこととなる。その意義は非常に大きいと言える。この認証取得によって学内関係者はもちろんのこと、広く社会に対する説明責任も果たせるものと考える。

（４）　情報システムが持つ利便性の有効活用

ISMS は、適切な情報セキュリティ対策を施すことによって、情報システムが持つ利便性を最大限に引き出すことを可能とする。実際、Can@home が学生に対してどの程度利

便性をもたらしたかを検証してみる。
成績確認、授業科目登録などは授業開始の 3 週間前から行うので、わざわざそのためだけに大学に来なければならなかった。帰省中の学生は、休みを繰り上げて戻ってくる必要があった。Can@home によって自宅に居ながらにしてそれらの事務手続きが可能となり、休みを有効利用できるようになった。Can@home の実績[8]を表１２に示す。

表12　成績表を大学まで受け取りに来た学生の割合比較

従来（2002年度）の来学率	Can@home 稼動後の来学率
７５％	５７％

2003 年度春学期の成績発表において、学生は学外から自分の成績確認を Can@home を利用してできるようになった。従来の来学率と Can@home 稼動後の来学率の差１８％、つまり１５００名程度の学生が自宅から成績確認を行ったと推測できる。それを裏付ける数字がある。成績発表の日に学外から１４００名以上の学生がアクセスを行ったログが残っている。
また、本学では多数の学生が海外へ留学する。留学先においてリアルタイムに成績確認と単位認定実例集の検索も可能となり、履修計画策定の支援に貢献している。海外から Can@home の利用に関する相談が寄せられていることもその証である。
Can@home が従来あった場所と時間の制約を取り払ったことは、学生に大きな利便性を提供した。インターネット、Web システムを利用した教務システムには潜在的な利便性があったのであるが、関係者からの理解を得ることができず、利便性を十分に引き出せなかった。それが、ISMS 継続運用を通して関係者からの理解と協力を得た結果、情報システムが本来持つ利便性の開花に成功した。

（５）　情報セキュリティ確保への組織的な取り組み

情報セキュリティ確保に関する技術的な取り組みは、非常に専門的であったので一部の専門技術者に負荷が偏りがちであった。代表的な業務に、外部からの不正アクセスを監視する業務がある。多様化している不正アクセスへの対応は、市販製品の導入だけでは解決しない。これらをいかに管理・運用していくかが鍵となる。IT セキュリティに関する高度な技能を有する人材は限定的であるため、学内関係者のみで常時監視及び対策を行うことは人的負荷という面で難しい問題があった。
この問題について、ISMS 運用レビュー[9]を行った結果、組織的に対応することが決定された。その決定を受けて、現在ネットワーク監視業務及び不正アクセス抽出作業について外部委託の可能性を模索している。

---

[8] 2003 年 8 月現在、Can@home 用乱数表所持者は３２００名に達した。本学の学生数の３６％に当たる数字である。

[9] 情報セキュリティマネジメントシステム適合性評価制度、ISMS 認証基準（Ver．２．０）では、マネジメントレビューと規定している。ISMS が継続的に適切性、妥当性及び有効性を保持するために、経営陣によるレビューが義務付けられている。

１０．おわりに

厳しい競争社会の中で、個性輝く存在をアピールしていくためには、危機意識を背景にした特色ある戦略を展開していかなければならない。指針としては、組織が保有する情報財産の価値にスポットをあて、利益あるいは費用対効果の最大化を追求することがあげられる。IT を利活用することにより、本指針に沿いつつ競争力の維持・向上に最適な戦略展開がスムースに行われると考える。例えば、ブロードバンドネットワークやモバイル PC は、情報財産の利活用において存在した時間と場所の障壁を取り除いた。このような IT 基盤整備によって、従来不可能であった業務の効率化や高度化が可能となってきた。

ブロードバンドネットワークを軸としたユビキタス社会が現実化してくると、情報セキュリティの確保はより一般的かつ緊急な課題となる。その証拠に、先日一般市民まで巻き込んだウイルス騒動（Blaster）が発生した。情報セキュリティ確保の重要性及び必要性の認識が、日本社会の中に浸透したことは間違いない。組織、個人が所有する情報財産を確実に保護するしくみを、如何に早く、簡単に、かつ安価に構築できるかが重要なポイントなのである。

本稿では、ISMS を導入する考え方、ISMS の構築方法、ISMS のメリットなどに触れた。すべては、より広く、一般的に ISMS の構築及び運用が浸透し、元気に安心して暮らすことのできる便利な日本社会〔1〕が実現することを念頭に置いて記述したものである。しかし、まだまだ未知の部分が多い分野である。特に、リスクマネジメントについては、より多くの事例を通してよりアプローチしやすい手法が確立されることを望む。また、認証基準については、管理手法における標準化は進んできてはいるが、IT セキュリティに関する標準化は遅れている。IT セキュリティは、取り扱う範囲も広大でありかつ専門的である。さらに、日進月歩ならぬ秒進分歩と表現されるほど進化の激しい分野でもある。このような理由から標準化が困難と思われるが、管理面プラス技術面も含めた標準化及び認証制度の実現は、より関係者への説得力も向上する。と同時に、日本における情報セキュリティ技術及びレベルの向上にも寄与するものと考える。是非、IT セキュリティにおける標準化および認証制度の確立も視野に入れた、より一層の ISMS 関連制度の充実を望むものである。

参考文献

〔1〕 “e－Japan 戦略Ⅱ”、IT 戦略本部、（オンライン）、入手先 http://www.kantei.go.jp/jp/singi/it2/kettei/030702ejapan.pdf

〔2〕 情報セキュリティマネジメントシステム適合性評価制度－ISMS 認証基準（Ver. ２．０）－、財団法人日本情報処理開発協会、平成１５年４月２１日、p9

（附録）

情報財産利用手引書（教員用）抜粋

情報財産利用手引書（教員用）

（略）

3．　情報財産を扱う上で留意する点

1）会話

公共の場所で機密に属する内容を話してはならない。

2）FAX

基本的に機密に属する情報を FAX で送信してはならない。どうしても、送信する必要がある場合は、相手が送信先にいることを確認後、かつ誤送信の心配が無い状態で送信すること。

3）WWW ブラウザ/電子メール

① 機密を要するメッセージを送信する時は、機密が漏れる危険性に注意し、必要に応じて暗号化する。特に通信販売におけるクレジットカード番号またはオンラインバンキングサービス等の電子取引における認証情報は、信用できる販売者に限り、必ず暗号化して送信すること。また、不特定多数が利用する PC で認証情報を入力することは、絶対避けること。

② 試験問題・個人成績等機密性が高く、流出等により社会問題となるような情報については、電子メールでの送受信は行わないようにする。また、機密を要する情報を扱う可能性のある教職員は学内のメールをむやみに学外のプロバイダ等へ転送しないようにすること。

4）郵送

機密情報を郵送する場合は、必ず封印された書留封書を用いること。

5）研究室内での管理

① 短時間でも研究室を出る場合は、必ず施錠する習慣を身に付ける。その場合でも、机の上には重要な情報を放置しない。

② PC の画面は、10 分程度でスクリーンセーバが稼動するように設定することが望ましい。さらに、パスワードロックをかければさらに安全性は高まる。

6）研究室外の管理

① 機密情報については、極力複写はとらない。

② 機密情報の記載されている媒体（紙、FD、PC など）を処分する場合は、第三者に情報が漏洩しないよう配慮する。紙の場合は、溶解処分用の箱に入れる。FD の場合は、データを消去するか、FD に鋏を入れる。PC の処分は、機密情報が格納されている状態で廃棄はしない。

③ 機密情報を研究室外に持ち出す場合は、封筒、かばん等に入れる。

以上