清泉女学院における情報セキュリティマネジメントシステム研究

江尻正一*、　芝山　豊*、　長田尚子**

A Study of an Information Security Management System in Seisen Jogakuin College

Shouichi EJIRI*, Yutaka SHIBAYAMA* and Naoko OSADA**

1. はじめに

情報セキュリティマネジメントシステム(ISMS: Information Security Management System)の本格的な標準化は、最初に 1995 年イギリスにおいて、情報セキュリティの実践集“User Code of Practice”(1989 年英国貿易産業省発行)を基にして英国規格協会(BSI: British Standards Institution)が英国規格 BS 7799-1 として規格化されたことに始まる。その 5 年後にはその BS 7799-1 がそのまま、国際標準化機構(ISO: International Organization for Standardization)と国際電気標準会議(IEC: International Electro-technical Commission)によって国際規格 ISO/IEC 17799 として採用される。その後、2000 年にホームページ改ざん、個人情報流出などのトラブルが多発し、さらに 2001 年 9 月 11 日の同時多発テロにより、さらなる情報セキュリティの強化を求める世界動向の中、国際規格 ISO/IEC 17799 は 2005 年に大幅改訂され、2007 年に ISO/IEC 27000 シリーズとなった。これが現時点での ISMS の規格となっている。日本では、ISO/IEC 27000 シリーズを JIS Q 27000 シリーズとして採用して標準化を行っている。また、ISMS 認証制度については、2002 年 4 月から第三者機関による ISMS 適合性評価制度、2003 年 4 月からは情報セキュリティに関する監査人に対する情報セキュリティ監査制度が運用開始されている。

そのような状況の中、清泉女学院は他大学と比べても大いに立ち遅れていた学内情報システムを改善すべく、2010 年学内 ICT 基盤の設計・構築を検討し、学内ネットワーク基盤、施設・設備ならびにこれらに付随する業務の一元化・集中化する方向で統合的に再構築し、運用を行っている。実際の運用において、様々な部門で情報セキュリティに関する管理・運用についての取り決め及び共通理解が少しずつだが、必然的に要求される状況となっている。特に本学には情報セキュリティポリシー、学内ネットワーク利用規程、本学メール利用規程が無く、それらの策定・施行が急務となっている。

そこで本研究では、情報セキュリティ規程体系の効率的な整備を主軸に置き、今後の清泉女学院における ISMS の段階的確立を目指すことが重要であると考え、その有り方について基礎的な事柄から研究し、まとめたものである。

第 2 章では、情報セキュリティに関する用語を再確認することにより基本的な ISMS について簡潔に記述し、より具体的な説明は清泉女学院を適用例として以降の章で扱う。次に第 3 章では清泉女学院における情報セキュリティに関する規程の現状等に触れる。以上から、第 4 章では清泉女学院における ISMS の段階的確立計画を提案し、第 5 章以下ではそれについて考察、推測される結果および今後の課題等について述べる。

* 清泉女学院大学人間学部心理コミュニケーション学科
** 清泉女学院短期大学国際コミュニケーション科

2. ISMS とは

2.1 情報セキュリティ

まずは、情報セキュリティの意味について再確認する。JIS Q 27001 によると情報セキュリティとは、次の 3 大要素 CIA を維持することで、2007 年以降、更に 3 つの要素、真正性、責任追跡性、信頼性の特性が含められている。これら 6 つの特性について以下に列記する。

(1) 情報の機密性(confidentiality)

認可されているものだけが情報にアクセスでき、認可されていないものは情報にアクセスできないように施された特性で、入退室管理やメール文書の暗号化などが例として挙げられる。

(2) 情報の完全性/保全性(integrity)

情報が正確であること及び完全であることを保護する特性。例としてデジタル署名による改ざん防止策などがある。

(3) 情報の可用性(availability)

認可されたものが、必要時に情報にアクセス及び使用が可能となる特性。認可された人が必要時に情報にアクセスできない場合、業務の停滞を招きかねない。もしも何らかの障害が生じた場合でも可用性を保持できるようにシステムを冗長的に構成するなどによって業務の停滞を回避することできる。

(4) 情報の真正性/認証性(authenticity)

アクセスしたものは偽ではなく、明確に真であることが証明できる特性。適用対象はユーザー、プロセス、システム、情報等である。なりすまし防御のパスワード認証、デジタル署名が挙げられる。

(5) 情報の責任追跡性(accountability)

情報が誰によって、どのような操作がされたかの証跡を残す特性及び操作されていないことを証明できる特性。アクセスログを記録することなどがある。

(6) 情報の信頼性(reliability)

システムやプロセスが無矛盾に一貫して動作することを保証する特性。二重化による故障対策、サーバの負荷監視などがある。

2.2 情報セキュリティポリシー

(1) 規程体系

通常、組織の規程体系は理念・方針等の上位層から細則・マニュアル等の下位層へとブレイクダウン形式の階層構造を持つ。本論文では、規程体系は、図のように三つの基本層に分類できるとした。上位層は経営者などによる「方針(policies)」、中間層は「基準/標準(standards)」で、規程、標準、基準等と呼ばれるものを含み、下位層は「手順(procedures)」で細則、手順、ガイドライン、マニュアル等と呼ばれるものを含む。

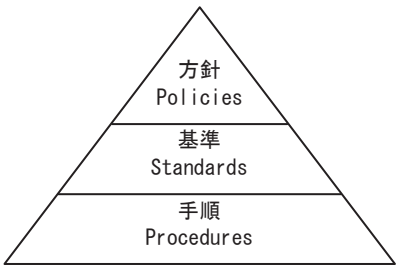

図.1 規程体系の階層性

(2) ISMS

ISMS とは、管理システム全体の中で、リスクに対する取り組み方に基づいて、情報セキュリティの確立、導入、運用、監視、レビュー、維持及び改善を担う体系のことである。なお、認証基準 JIS Q 27001: 2006 は、PDCA サイクルによって ISMS が改善されることを推奨している。

情報セキュリティの規程体系としては、一般的に上位層に「情報セキュリティ基本方針」、中間層に「情報セキュリティ対策基準」、下位層に「情報セキュリティ実施手順」が位置する。

表 1　清泉女学院における ISMS に関する主な規程(2011 年 2 月 1 日現在)

	ISMS 仕様 (ISO/IEC 27002: 2007)	情報セキュリティ規程体系			
		方針層	基準層		手順層
1	リスクアセスメントおよびリスク対応	−	「情報セキュリティ実施規程」暫定施行予定 (April 1,2011)		
2	セキュリティ基本方針	発表予定 (Mar.2,2011)		−	−
3	情報セキュリティのための組織	−		情報セキュリティ委員会(未)	連絡者会議(未)
4	資産の管理	−		固定資産及び物品管理規程他	
5	人的資源のセキュリティ	−		就業規則他	
6	物理的及び環境的セキュリティ	−		パーソナル・コンピュータ使用規程	
7	通信及び運用管理	−		SJC-net 利用規程(申合せ)他	ガイドライン
8	アクセス制御	−			
9	情報システムの取得、開発及び保守	−			
10	情報セキュリティインシデントの管理	−			
11	事業継続管理	−		自己点検及び自己評価規程	
12	順守	−		個人情報の保護に関する規程他	ガイドライン

3. 清泉女学院における ISMS に関する規程の現状

次に清泉女学院の規程について、ISMS 仕様 ISO/IEC 27002: 2007 に基づいて本学規程集及び平成 22 年度学生便覧の調査を行い、その対応・体系関係が分かるように表 1 にまとめた。但し、今回調査した規程集、学生便覧には危機管理、ホームページ運営などに関する記載がなかったため、それらの規程は表に反映されていない。また、2011 年 2 月 2 日教授会で検討予告された「情報セキュリティ基本方針」、「情報セキュリティ実施規程（暫定)」並びに「情報セキュリティ委員会」については近々施行予定であるとして表中に記した。

ISMS 仕様の各項目について、清泉女学院のセキュリティ規程整備状況を以下に列記する。

(1) リスクアセスメントおよびリスク対応

予想リスクの特定、分析・評価そして対策の手順を定めたリスクマネージメントを統一的に扱う価値判断、実施規程が無く、多くの場合、各リスクに対して個人に任せられている状況である。

(2) セキュリティ基本方針― 管理方針

セキュリティ基本方針が存在していなかったため、2010 年学内 ICT 整備に伴って、同年 7 月情報セキュリティポリシー策定検討チームが編成され、翌年 2 月学長にその結果を答申した。同年 3 月学長より情報セキュリティ基本方針が発表される予定である。

(3) 情報セキュリティのための組織― 情報セキュリティのガバナンス

情報セキュリティポリシー策定検討チーム答申を受けて、2011 年 4 月 1 日より、初の情報セキュリティ委員会が発足する予定である。

(4) 資産の管理― 情報資産の目録と分類

「固定資産及び物品管理規程」「文書管理規程」等はあるが、情報セキュリティの観点がほとんどなく、特に情報資産の概念に基づく大幅な見直しが必要である。

(5) 人的資源のセキュリティ― 従業員の雇用／異動／解雇に伴うセキュリティ

既存の「就業規程」他の見直し以外に情報セキュリティ教育規程、契約事項に関する運用細則を検

討する必要がある。

(6) 物理的及び環境的セキュリティ― コンピュータ機器の保護

平成 2 年 7 月 11 日施行の「パーソナル・コンピュータ使用規程」や「情報処理室利用(学生便覧)」があるが、それ以上に重要な情報資産である学籍簿、情報サーバ室などを扱う部門でのセキュリティ規程等の策定が急務である。

(7) 通信及び運用管理 ― システムおよびネットワークにおける技術的セキュリティの管理

ネット利用やシステム運用管理の検討が継続している状況である。

(8) アクセス制御―ネットワーク／システム／アプリケーション／機能やデータへのアクセス権制限

2010 年秋学期より学内サーバへのアクセスが開始されたばかりで、メール利用規程も含めて策定検討中である。

(9) 情報システムの取得、開発及び保守― アプリケーションへのセキュリティ組込み

OS やアプリケーションソフトの技術的脆弱性へのパッチ対応、デジタル署名、暗号化などの管理策については明文化されていない。

(10) 情報セキュリティインシデントの管理― 違反の予測と、違反に対する適切な対処

インシデント報告についても規則は存在しない状況である。

(11) 事業継続管理 ― 業務上の重要なプロセスとシステムを保護し、保守し、復旧する

危機管理マニュアルの周知・改善や各部門緊急対応マニュアルの策定が必要とされる。

(12) 順守 ― 情報セキュリティポリシー／規格／法律／規定の順守の徹底

「個人情報の保護に関する規程」「自己点検及び自己評価規程」などがあるが、情報セキュリティ関連法令順守の徹底や情報セキュリティ監査については別規程として定めていない。なお、平成 17 年 4 月 1 日より施行された「個人情報保護の方針<ガイドライン>」の名称は、規程体系に多少混乱を生じさせる危惧がある。

以上、ISMS 仕様に基づいて判断すると、清泉女学院規程は未整備状態で再構築の必要性があることが認められた。

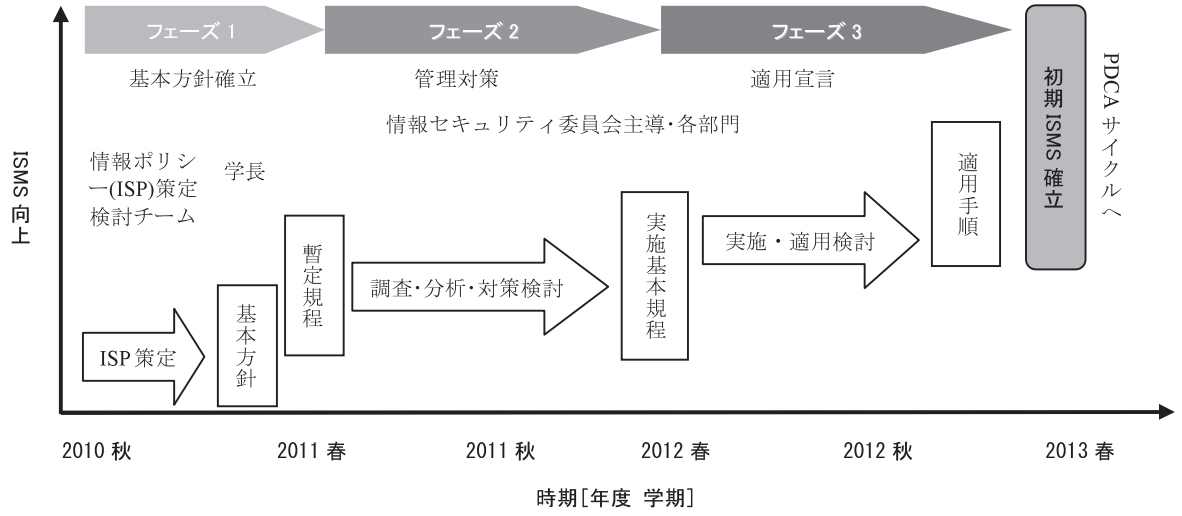

図 2　清泉女学院 ISMS 確立-ロードマップ案-

4. 清泉女学院における ISMS 確立

4.1 実施計画案

以上の事及び日々の研究・教育・校務等の活動に対して更に重大な新規活動を加えることは人材、ノウハウ、時間が乏しい小規模大学においては多大な負担を被ると考えられる。そこで、数年間をかけて段階的に ISMS について検討を重ねてから ISMS の初期確立を目指すことを提案する。

図 2 は、ISMS 適用性評価制度のマネジメント枠組みに準じて、最短の 2013 年度確立を想定した場合のロードマップである。時系列的に記述すると以下のようになる。なお、情報セキュリティ基本方針、情報セキュリティ実施規程並びに情報セキュリティ委員会規程の内容については次節にて解説する。

＜フェーズ 1＞2010 年度

・7 月、学長により情報セキュリティポリシー策定検討チーム発足。構成員は、図書館長、事務局長、総務部長、学生支援課長、情報システム委員長および情報システム委員の 6 名。

・2 月、情報セキュリティポリシー策定検討チーム、学長に答申。答申内容は、ISMS 確立計画案、情報セキュリティ基本方針提言､情報セキュリティ実施規程施行及び情報セキュリティ委員会設置依頼。

・3 月、学長、情報セキュリティ基本方針発表。情報セキュリティ実施規程並びに情報セキュリティ委員会規程の教授会審議。

＜フェーズ 2＞2011 年度

・４月、情報セキュリティ実施規程暫定施行、情報セキュリティ委員会発足。

・情報セキュリティ委員会、情報セキュリティ基本方針、実施規程及び規程体系の研修会実施。

・調査・分析・対策について検討会を行う。また、必要に応じて規程等の見直し検討を行う。

・初期情報資産調査。洗い出しと資産価値のレベル分け。実施手順検討。

・初期リスク評価、脅威、脆弱性対策、影響調査。実施手順検討。

・２月、暫定規程を本格的な実施基本規程として見直しを行う。また、必要に応じて各実施規程、手順策定。

＜フェーズ 3＞2012 年度

・4 月、情報セキュリティ実施基本規程施行。

・実施基本規程、他規程などに基づき実施・適用する。

・情報セキュリティ委員会、情報セキュリティ規程体系の整備を行う。

・各部門、規程、手順策定。

・2 月、必要に応じて情報セキュリティに関する規程等を改善する。

以上により、2013 年度、初期 ISMS を確立させ、以降の年度は PDCA サイクルに沿って ISMS の向上を図る。

4.2 情報セキュリティ規程体系案

清泉女学院の情報セキュリティ規程体系として、上位の基本層に学長による「情報セキュリティ基本方針」を配置し、その直下に情報セキュリティ対策実施基準として「情報セキュリティ実施規程」を基準層に配置させた。すべての情報セキュリティに関する規程、手順、ガイドラインは、この「情報セキュリティ実施規程」下に整合性を有して再配置することを提案する。（図 3 参照）なお、基準層に位置する規則名については、ときに基準・標準・規定・規程と呼ばれるが、本研究では清泉

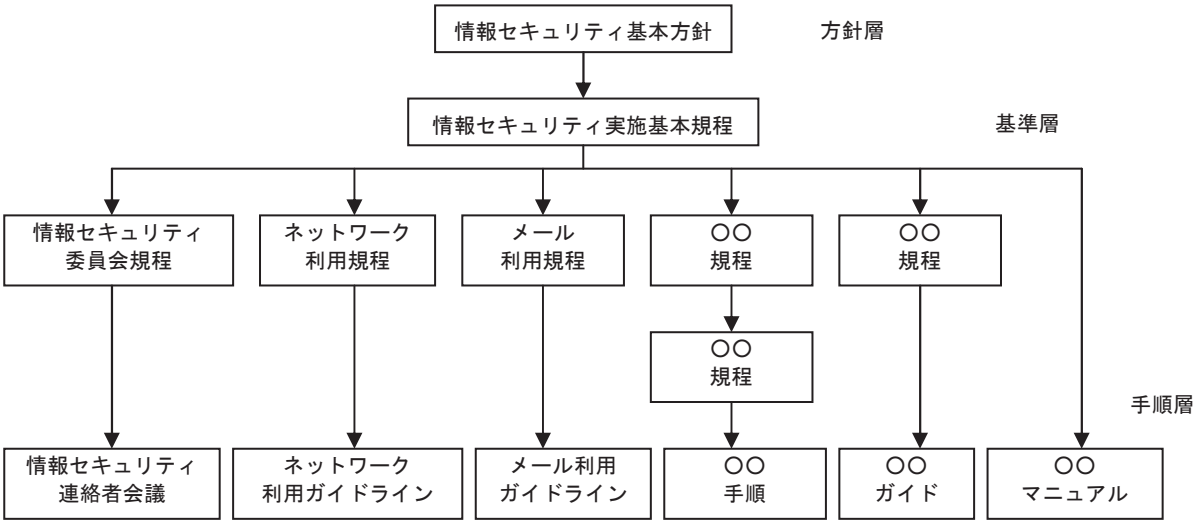

図３　情報セキュリティ規程体系

女学院の用法に則して規程と統一的に記した。

以下に提案・説明する(1)情報セキュリティ基本方針、(2)情報セキュリティ実施規程及び(3)情報セキュリティ委員会については、フェーズ 1 で作成し、フェーズ 2 以降において実施し、必要におじて見直しを行うものとする。

(1) 情報セキュリティ基本方針

上位層に位置する基本方針は、組織全体及び関係する団体、個人に対する、学長による取組み姿勢の宣言で、目的、範囲、義務、罰則等を含む必要がある。表 2 には、2011 年 2 月に情報セキュリティポリシー策定検討チームが学長に答申した基本方針(案)を記載した。検討チームにおいては、特に御茶ノ水女子大学セキュリティポリシー及び早稲田大学情報セキュリティポリシーを参考に、清泉女学院の構成員全体に広く理解できるように簡潔な基本方針案を策定した。

表 2　清泉女学院･情報セキュリティ基本方針（案）2011/02/08 作成

第 1 条　(目的)　本学･情報セキュリティ基本方針の目的は、以下の事柄を実施することにより、本学の教育および研究等の活動がより安全に安定的になるように支えるものである。
1　情報資産の管理・運用を明確化する。
2　本学の情報資産を利用するすべての構成員等に対して、情報セキュリティの必要性および責任と義務について明確化し、相互に理解を深める。
3　全学的な情報セキュリティ基盤の確立・維持・改善を図る。
4　事故予防および事故に対する迅速かつ適切対応を図る。
第 2 条　(用語の定義)　本基本方針において「情報資産」とは、以下の有形・無形のものを意味する。
・本学で扱うすべての情報(データ、文書、図画、電磁気的記録及び会話も含む)
・それらの情報を取り扱うための機器及び設備(PC、通信機器、記憶媒体、ソフトウェア、通信サービス、ネットワーク)
・その他、本学が情報資産と認めるもの
・以上の情報資産を扱う人材(専任教職員、兼任教員、臨時職員、在学生、聴講生、委託業者及び来学者も含む全構成員)
第 3 条　(適用範囲)　本基本方針は、本学で取り扱うすべての情報資産に適用する。
第 4 条　(規程体系)　情報セキュリティ関連の規程体系は、唯一の「基本方針」、基本方針に基づく「実施規程」、さらに実施

規程を具体的に展開して個別に定めた「実施手順」から成り、関連するすべての規程、ガイドライン、マニュアル等は整合性を保って本規程体系に含まれる。

第 5 条　(組織)　情報セキュリティに関して、立案、策定、管理、運用、評価、改善並びに教育を行うために、以下の情報セキュリティ組織体制を設ける。なお、仔細につい ては「情報セキュリティに関する実施規程」で別途定めるものとする。

1　全学の情報資産に関する総括的な意思決定、学内外に対する責任並びに基本方針の周知、教育を担う機関として「情報セキュリティ委員会」を設置する。

2　情報資産を管理・運用し、その状況及び結果等を情報セキュリティ委員会に報告及び提案等を行う「情報セキュリティ連絡者会議」を設置する。情報セキュリティ連絡者会議は各部門の責任者から成る。

3　本学情報資産の管理を総括し責任を負う「情報管理総括責任者」を置き、情報セキュリティ連絡者会議を総括する。

4　各部門における情報資産の総括管理責任として各「部門情報管理統括者」を設置する。緊急時には当該部門に対して緊急措置を取る権限を持つ。

5　当該の情報資産を取り扱う者はすべて、当該情報資産の情報管理の責任者である。

6　情報資産の管理・運用が適切に行われているかの監査を行う機関として「監査部会」を設置する。

第 6 条　(権限と管理)　情報資産に対する権限は、本学の教育、研究及び業務上必要な者のみに必要な権限のみを与える最小権限の原則を基本とし、機密性を確保する。情報の内容の正確性と整合性を保ち、完全性を確保する。また、必要な情報を適時に利用できるようにするため可用性を確保する。

2　情報及び情報資産を作成、利用、保存、移送、保護、提供及び消去、破棄する場合は、情報の重要度評価に基づき、格付け区分及び取扱制限を明示し、それに従って適正に管理・運用する。仔細については「情報セキュリティに関する実施規程」、各所管の実施手順等で別途定めるものとする。

第 7 条　(監査)　監査部会は、情報資産が各所管で適正に管理・運用されているかを監査し、情報セキュリティ委員会に報告しなければならない。

第 8 条　(事故)　情報セキュリティ事故に関する事項については、「情報セキュリティに関する実施規程」で別途定めるもとする。

第 9 条　(教育)　本学のすべての構成員は、情報セキュリティ教育を定期的に受け、情報資産の管理・運用方法について理解しなければならない。

第 10 条　(罰則)　本基本方針及び情報セキュリティに関連する個々の規程に違反する行為を行った本学構成員は、その程度に応じて就業規則又は学則･規程に定めるところにより懲戒を受ける場合がある。

第 11 条　(見直し)　情報セキュリティ委員会は、本基本方針の見直しの必要性有無を検討し、必要があると認めた場合は見直しを行う。

(2) 情報セキュリティ実施規程

方針を具現化して､組織全体に対して統一的な基本規程となるためには､教授会承認が必須である。教授会承認後、全構成員に周知徹底すべく働きかけが必要である。なお、実施規程案の本文記載については割愛した。

(3) 情報セキュリティ委員会

ISMS の向上を大いに支援する継続的な活動組織として情報セキュリティ委員会の設置を提案する。委員会の組織及び構成は、情報セキュリティ委員会規程案の第 2 条にあるように、各部門の統括代表者からなり、全学を統括できる立場の学長が委員長とする。なお、規程案記載は割愛した。

5. 結果と考察

情報セキュリティ規程体系の観点からすると表 1 の対応規程に示したとおり、清泉女学院の規程は既存規程を見直し更に新規規程を策定して、全体的に再整備する必要があるが、多大な労力と実践課題が生じると考えられる。そのため、短期間の初期 ISMS 確立を目指さず、2,3 年後を視野に入れた中長期的な計画に基づき、段階的に各情報セキュリティ規程、手続きを策定・整備して、初期 ISMS 確立を目指すべきと考える。但し、この活動は情報セキュリティ委員会がどれだけ主導的に的確に指導するかに依存する。情報セキュリティ委員会の活動が停滞すれば、初期 ISMS の確立は頓挫し、ダブルスタンダードを生じさせる危険性がある。

情報セキュリティ委員会のモチベーションを維持する手段として、実際に取得するかは別にして、ISMS 適合性評価制度を利用して ISMS 認証取得を目指すことが挙げられる。第三者認証機関による審査やそのための研修・制度改善は ISMS 早期確立に役立つと推測される。

6. おわりに

本研究では、小規模短期大学/大学の清泉女学院で如何に ISMS が早期に確立できるかを現状から検討した。検討結果として ISMS の段階的確立計画を提案、紹介することとなった。今回、計画及び基本規程等の基礎的研究報告とし、フェーズ 2･3 以降での各タスクにおける詳細研究は今後の課題とした。また、近年、急速にクラウドコンピューティング化が進んでいる。新しい世界に接続できる ISMS を如何に確立できるかが極めて大きな課題である。

謝辞

本研究は、清泉女学院・情報セキュリティポリシー策定検討チームでの情報セキュリティに関する議論がきっかけとなって発展したものです。同検討チーム員の八重田修氏、西村健一氏そして仲條正典氏にあらためて深謝いたします。

引用･参考文献/URL

1. 平野芳行･吉田健一郎「ISO/IEC 27001:2005 (JIS Q 27001:2006) 詳解　情報セキュリティマネジメントシステムー要求事項」日本規格協会(2006).
2. 相田浩志「情報セキュリティの基本と仕組み」秀和システム(2010).
3. 片貝理絵子 “情報セキュリティ規程体系の効率的な整備事例” IBM PROVISION No.49, p.66 (2006).
4. 日本情報処理開発協会(JIPDEC)/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/
6. ISO (International Organization for Standardization)/ISO Standards by TC http://www.iso.org/iso/iso_catalogue/catalogue_tc.htm
7. 私立大学情報教育協会(JUCE)/情報セキュリティ対策の自己点検・評価について　http://www.juce.jp/sec-check/
8. 「平成 22 年度大学セキュリティ研究講習会」私立大学情報教育･情報セキュリティ研究講習会運営委員会(2010).
9. 清泉女子大学･情報環境センター　http://campus.seisen-u.ac.jp/
10. お茶の水女子大学/セキュリティポリシー　http://www.ocha.ac.jp/Security_Policy.pdf
11. 早稲田大学 情報セキュリティポリシー　http://www.waseda.jp/mnc/RULES/Security_Policy.html
12. Tim Mather, Subra Kumaraswamy and Shahed Latif「クラウド セキュリティ ＆ プライバシーーリスクとコンプライアンスに対する企業の視点」オーム社(2010).

（受付日：2011 年 2 月 23 日）

SUMMARY

This research concerns the establishment of information security management systems at tertiary institutions using the international standards ISO/IEC 27000 family. The present study reports the application of this research at Seisen Jogakuin College (SJC) in Nagano. The establishment plan was derived from an analysis of the present state of information security. First, a road map for the establishment of an information security management system at SJC is presented. Second, revisions to SJC’s information security rules are proposed as a hierarchy of information security rules. In addition to the road map and rule revisions, the policy and each rule employed at SJC will be discussed.