Vol.2011-IOT-14 No.6
2011/7/15

山口大学における情報セキュリティマネジメントシステム (ISMS) 構築テンプレート作成及び適用範囲拡張について

市川 哲彦[†1,†2] 小柏 香穂理[†1]
永井 好和[†1] 小河原 加久治[†2,†1]

最近の山口大学メディア基盤センターにおける情報セキュリティマネジメントシステム (ISMS) 関連活動について報告を行う．本センターにおける ISMS 構築の目的の一つに，学内外における情報セキュリティ文化の普及が挙げられる．ここ数年，他の大学においても ISMS 構築の動きが見られ，本センターへの訪問依頼や文書提供などの情報提供依頼がなされている．本センターで ISMS 構築及び運用にあたって利用している文書をそのまま提供するのが最も簡単な方法であるが，(1) セキュリティ上外部に出せない部分が存在すること，(2) 契約上コンサルティング会社との共同著作物となっている部分が存在すること，また，(3) 関連文書が山口大学法人著作物であり，本学の知財提供のルールに従う必要があること，の三点に鑑み，文書類を適宜取捨選択を行った上で，コンサルティング会社と協力の上，出版物等として販売を行うこととした．

また，学内においては，ISMS 適用範囲の拡張に関する議論が行われている．従来は，メディア基盤センターの教育・研究用サービス及び機関ネットワークを適用範囲としていたが，新たに事務部門が管轄するサーバ室を含めるよう適用範囲を再定義し，関係文書についても見直しを行う予定である．本報告では，これら二件について，現在の作業状況と今後の予定について概要を説明する．

Recent activities on the information security management system (ISMS) at Yamaguchi University: publishing ISMS document templates and extending the scoped area

Yoshihiko Ichikawa,[†1,†2] Kahori Ogashiwa,[†1]
Yoshikazu Nagai[†1] and Kakuji Ogawara[†2,†1]

This report describes the recent activities regarding the information management system (ISMS) at Yamaguchi University. One of the aims of the ISMS at our university is to support proliferation of information security culture in- and outside the university. In addition to a dozen of Japanese universities that are forerunner with respect to ISMS, several universities have been trying to establish effective ISMS, and some of them have required us to reveal ISMS documents such as manuals and records as to help them accomplish their tasks. It, however, is difficult to reveal the whole documents as is, since (1) some parts of the documents shall not be revealed due to security reasons, (2) some parts of the documents are copy-righted by our university and the consultant company that we had a contract with when we initially established our ISMS, and (3) we must follow the intellectual property provision rules of the university as the documents are owned by the university (not by the individual staff member). So, we are planning to publish ISMS doucment templates in cooperation with the consulting company that helped us build our initital ISMS.

In addition to this activity, we are now planning to extend the scoped area of our ISMS so that it includes the server room managed by non-technical staff members as well as the original area, i.e., maintenance of the educational and research computer systems and backbone computer network system managed by the technical staff members belonging to Media and Information Technology center of Yamaguchi University. We have been discussing about which parts must be changed accordingly, especially, how the scoped area shall be modified, and which parts of the ISMS manuals and procedures should be adapted. This report describes the recent progress and the future plan of these activities briefly.

1. はじめに

情報セキュリティは計算機を維持・管理する上で常に意識する事項であるが，特に個人情報保護法の施行を機会にして更に注目が集まるようになっており，組織において情報セキュリティマネジメントシステム (Information Security Management System, ISMS) を導入し，情報セキュリティの維持をより強固にする試みが盛んになった．また，一般企業だけではなく大学のような教育・研究機関においても個人情報保護やセキュリティ教育の観点から ISMS が重要視されるようになっている[1)2)]．山口大学メディア基盤センターにおいても，全学情報基盤を担う必要性に鑑み，2005 年度から ISMS の構築に取り組み始め，2008 年 10 月に ISMS 国際規格である ISO/IEC 27001 (国内規格では JIS Q 27001[3)]) の認証を

†1 山口大学メディア基盤センター
Media and Information Technology Center, Yamaguchi University
†2 山口大学大学院理工学研究科
Graduate School of Science and Technology, Yamaguchi University

取得した．

ISMS 認証取得の第一の目的は本学の情報基盤を担うメディア基盤センターのセキュリティレベルの継続的な維持であるが，その一方で，学内への情報セキュリティ文化の普及も中期計画に掲げており，また，社会貢献の一環として，国立大学法人情報処理センター協議会 ISMS 研究会[4] の活動等を通して，学外に対しての情報セキュリティ文化の普及活動も行っている．本報告で，このような学内外への普及活動としておこなっている最近の二つのアクティビティについて概略を述べる．

一つ目は ISMS 構築用テンプレートの販売である．従来より，文献[5] や関連する文書において規格自体の説明は行われてきており，また，文献[6] のように具体的な構築事例について解説した書籍もある．しかしながら，大学における構築事例はまだ少なく[⋆1]，大学における ISMS 構築の具体例について解説した資料は公開されていない．一方，近年急速に大学における ISMS 構築の動きが見られ，大学間での情報提供依頼や資料提供依頼がなされるようになってきた．このような社会の動きに鑑み，本センターでは，ISMS の構築・運用のために作成した ISMS マニュアルなどの基本文書，管理策手順書やその下位手順書，運用上必要となる各種様式などを，情報セキュリティ上問題の無い範囲で可能な限り ISMS 構築用テンプレートとして公開し，社会的なニーズに応えようと考えている．

二つ目は学内における情報セキュリティ文化の普及である．これまでは本センターの基盤システム運営を適用範囲として ISMS の構築・運営を行ってきたが，学内への普及に向けての動きも少しずつではあるが進んでいる．まず，内部監査への取り組みについて変化があった．当初より，本学の監査室のスタッフを ISMS 内部監査チームに招聘し，情報セキュリティ監査の経験の場として利用してもらっていたが，2010 年度より，正式に監査室の業務に情報セキュリティ監査の項目が入り，本センターがその適用の第一号となった．今後の情報セキュリティ監査の計画については未公開であるが，少なくとも全学的な情報セキュリティ監査のための礎をなす事に貢献できた点については，ISMS 認証取得の効果の一つとして挙げられると考えている．加えて，本センターが所属する大学情報機構の事務部門である情報環境部においても ISMS への取り組みが開始された．当初は，情報環境部のごく一部を含むように，メディア基盤センターで構築された ISMS の適用範囲を拡張することで進める予定である．本稿では特に後者の活動を取り上げる．

以降，本稿ではまず ISMS 構築用テンプレートの作成基本方針と現状について触れ，続いて，適用範囲拡張の現状について説明を行う．最後にまとめてと今後の計画について述べる．

2. ISMS 構築用テンプレート

本節では，まず ISMS 構築の PDCA サイクルにおいてどのような文書が作成されるのかを概観し，次に，実際に我々が利用している文書の一覧がこの枠組みに従ってどのように位置づけられるかを整理し，続いて，学外への提供方法について現在の計画を述べる．

2.1 ISMS の PDCA サイクルとアウトプット

ISO/IEC 27001 で規定される ISMS は PDCA サイクルからなるプロセスアプローチを採用している．PDCA サイクルは Plan (計画: 確立)，Do (実行: 導入・運用), Check (点検: 監視・レビュー)，Act (処置: 維持・改善) の 4 フェーズを繰り返しながら組織のシステムを改善しつつ維持する考え方である．具体的にどのような事項を実施すべきであるかについては規格書[3] の第 4.2 節に述べられており，P, D, C, A の各フェーズで実施すべき事項がそれぞれ第 4.2.1 項，第 4.2.2 項，第 4.2.3 項，第 4.2.4 項で説明されている．また，関連するより詳細な事項が第 5 章から第 8 章に記述されている．規格に基づき ISMS を導入・運用する組織は，規格書に書かれている要求事項を文書化された手順として具体化し，さらにそれらを確実に実施することが求められる．各組織の活動内容はサービス内容，人員，求めるセキュリティレベル等に応じて組織毎に異なっており，具体的にどのような手順を定めるのか，などは各組織が判断する事項である．従って，ISMS 構築プロセスで利用される各フェーズにおけるアウトプットは，概念的には同じものになるが，具体的にはそれぞれの組織毎に工夫がこらされたものとなる．

PDCA サイクルのフェーズ毎のアウトプットをまとめたものを表 1 に示す．実際に PDCA サイクルを進める上では，年間計画表の作成も必要であると考えているが，規格書には特に明示的に記述が無いため，本センターでは A フェーズにおいて概略の計画案を作成し，その段階で，P フェーズでの活動計画も決定している．さらに，P フェーズの最後で経営陣の運用許可を求める際には，より詳細な活動計画表をまとめている．

以下は，PDCA サイクルの各フェーズの概要である．

2.1.1 Plan(確立) フェーズ

P フェーズでは情報セキュリティポリシーの確立を行うため，組織の考え方を定めた基本方針，詳細な適用範囲，PDCA サイクルを回すために必要となる ISMS マニュアル，対策

⋆1 著者らの把握する範囲では，執筆時点では次の通りである: 南山大学 (2003 年 2 月)，京都大学 (2003 年 6 月)，静岡大学 (2003 年 11 月)，日本福祉大学 (2005 年 3 月)，國學院大学 (2006 年 1 月)，早稲田大学 (2007 年 1 月)，宇都宮大学 (2007 年 11 月), 山口大学 (2008 年 10 月)．なお，いずれも大学内の特定組織あるいはキャンパスを適用範囲とした認証取得をしており，全学での認証取得事例は著者らの把握する限りでは存在しない．

Vol.2011-IOT-14 No.6
2011/7/15

表 1 PDCA サイクルのフェーズ毎のアウトプット一覧

フェーズ	説明	アウトプット
Plan (確立)	ISMS の運用に必要となる文書の作成とリスクアセスメントに基づくリスク対応計画の作成を行う.	適用範囲，基本方針，ISMS マニュアル及び関連実施手順書，管理策実施手順書，リスクアセスメント結果，リスク対応計画，適用宣言書，経営陣の承認文書
Do (実施)	定められた手順に従った ISMS の運用を行う.	各種記録，リスク対応計画及び実施報告書，有効性測定手順書
Check (監視・レビュー)	日常的な監視に基づく予防・是正処置の立案や，管理策の有効性測定，内部監査，マネジメントレビューによる定期的な点検を行う.	予防・是正処置計画書・報告書，有効性測定結果，内部監査報告書，マネジメントレビュー結果
Act (維持・改善)	Check フェーズで指摘された改善事項や予防・是正処置を実施する．また，利害関係者にこれらの変化を伝達する.	指摘事項回答，予防・是正処置計画書・報告書，利害関係者への通知・契約の変更，(次サイクル計画書)

基準及びその実施手順を与える管理策実施手順書が作成される．P フェーズでの重要な活動の一つにリスクアセスメントがあり，この過程で組織が持っているリスクが特定され，それに基づいて，規格要求の付属書 A (Annex A) に記載されている管理目的・管理策の中で組織が必要としているものを選び出すこととなる．その結果は適用宣言書にまとめられる．適用宣言書は管理策の採否を記したものであり，外部組織に ISMS 運用の基準となる管理策の範囲を明示することで情報セキュリティ対策の概要を伝えるために利用される．また，リスクアセスメントの過程で要対応リスクの洗い出しが行われ，以降の D フェーズでのリスク対応計画作成へと引継がれる．経営陣の承認は構築した ISMS での運用許可を得るために要求されている．これら一連の作業をより詳細に表したものが図 1 である．

2.2 D(導入・運用) フェーズ

D フェーズでは P フェーズでのリスクアセスメントで要対応とされたリスクについてリスク対応計画を立案し，その実施を行う．また，管理策有効性測定方法の定義もなされ，次の C フェーズで利用される．従ってこれらに関連する書類がアウトプットとなる．また，D フェーズでは管理策実施手順書に従って，組織運用に関わる及び技術的な情報セキュリティ対策が実施され，その結果としてスタッフの異動に関連する記録，入退室記録，サーバログ，システム保守記録，イベント・インシデントの発生と対応などの記録類が作成される．この事は規格要求の 4.2.2) には明記されていないが，4.3.3) 記録の管理において一連のプロセスの内容や重大なインシデントについては記録を取ることが求められている．

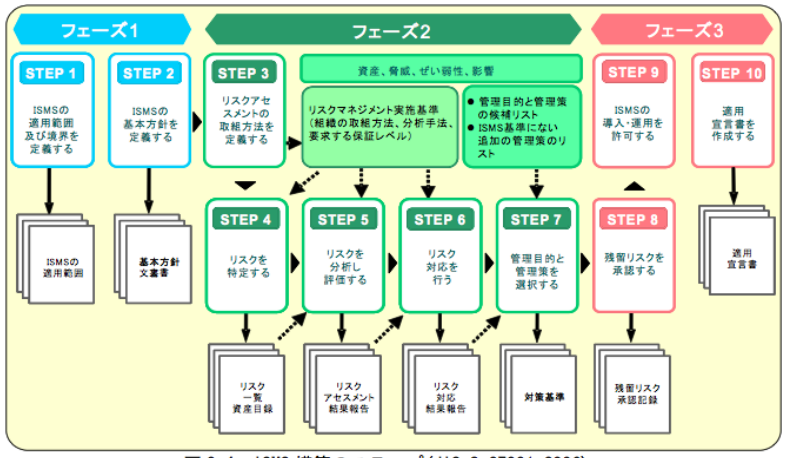

図 0-4 ISMS 構築のステップ(JIS Q 27001:2006)

図 1 P フェーズの活動と文書群: (出典: 日本情報処理開発協会, 図 0-4 ISMS 構築のステップ (JIS Q 27001:2006)，ISMS ユーザーズガイド-JIS Q 27001:2006(ISO/IEC 27001:2005) 対応-，2008)

2.3 C(監視・レビュー) フェーズ

C フェーズには，内部監査やマネジメントレビューのように予めスケジュールされた日程で実施されるレビューの他に，日常的な監視 (モニター) の結果として把握された各種イベントをトリガーとして適宜実施される予防・是正措置の立案及び実施が含まれる．また，これらのレビューや是正・予防措置に当たっては，実施管理策や各種対策の有効性を測定することが規格で求められている．内部監査 (internal audit) は適用範囲内の組織のメンバーで行う第一者監査であり，中立性を確保するためや人間関係に配慮して組織外のスタッフに依頼することもあるが，本来は内部要員からなるグループで行う相互監査である[⋆1]．第三者機関による認証審査は一部を抽出しての審査であるが，内部監査は適用範囲全体が監査の対象となる．マネジメントレビューは経営陣が ISMS の運用状況をチェックするために行われ，定期的に専用のレビュー会議を実施して行うこともあるが，日常的なコミュニケーションによるレビューも大切である．

2.4 A(維持・改善) フェーズ

A フェーズは C フェーズのアウトプットを次サイクルの P フェーズにつなげるための活

⋆1 本センターの内部監査では，学内の監査室のスタッフなどに依頼をしている．

Vol.2011-IOT-14 No.6
2011/7/15

図 2 PDCA 各フェーズの時間的な関係 (山口大学メディア基盤センターの場合)．数字は月である．

動となる．具体的には，C フェーズでなされた指摘事項を改善すること，予防・是正処置の実施を行うことが求められる．他にも，自他の事例から学んだことがらを予防・是正処置に反映させることや，利害関係者にリスク管理についての変化を伝えることも要求事項には含まれている．

2.5 PDCA サイクル

基本方針及び ISMS マニュアルの構築を別にすると，P: 要対応リスク対応及び管理策実施手順の策定，D: それらの実施，C: レビュー・モニターによる実施状況の確認と測定と評価，A: 改善，という一連の流れからなっており，これらの日常的な活動が基本方針及び ISMS マニュアルに従って回されていくことが見て取れる．勿論，基本方針や ISMS マニュアル自体も改善の対象となるため，P フェーズを再度実施する際には，リスクアセスメントや実施手順の見直しに加え，これらも適宜レビューを行う．

PDCA サイクルを図式的に表示する際には，P, D, C, A のそれぞれのアウトプットが次のフェーズのインプットとなる環状のイラストを用いることが多いが，これは時間的な関係，すなわち，各フェーズが終了してから次のフェーズが開始するということでは無い．図 2 に本センターにおける時間的な関係の実例を示す．図には明記されていないが，規格 4.2.3 b) d) で要求されている，有効性測定やリスクアセスメントの見直しは P フェーズでスケジュールを調整した上で，6 月〜7 月に実施している．

3. テンプレート作成指針

本センターの ISMS 関連文書は，A. ISMS マニュアル等，B. リスクアセスメント関連文書, C. 有効性測定関連文書, D. 手順書, E. 記録等，のような文書種別に従って整理され管理されている．文書内容がある程度把握された状態であればこの分類方法の方が文書の探索が容易であり，利用しやすいのであるが，実際に ISMS 構築をしてみると，このような編成ではどうしても文書間の上下関係，参照関係，時間的な関係が見づらいく，作業途中の見通しが悪いという問題点があると感じられた．そこで，今回テンプレートを作成するにあたっては，PDCA サイクルのそれぞれにおいて，ある程度構築の時間的な流れに従って文書を配置する方が利用しやすいのではと考えた．実際のファイル群をこのような考えに従って配置した結果の一部を図 3，4 に示す．いずれも作成中のテンプレートの目次を Web ブラウザでレンダリングした結果のスナップショットである．また，単純に資料を提示しただけでは，どのような位置づけで文書が作成されているのかが読み取りづらいので，テンプレート中の文書種単位で ReadMe ファイルを準備し，簡単な説明を付している．例えば，適用範囲に関する ReadMe は次のようになっている:

> 適用範囲は次の観点から構成されており，資料 1 「適用範囲と境界・サービスの定義.pdf」にまとめてあります．(資料 1’は pdf 文書のワード版です．)
>
> (1) 事業 (service)
> 組織内で行うどのようなサービスを対象とするかを定義します．例: 教育・研究用コンピュータシステム運用，基幹ネットワーク運用，教務システム運用．
>
> (2) 組織 (organization)
> 対象とする人的な範囲を定義します．CIO, CIO 補佐，情報セキュリティ担当者，システム運用担当者などを整理しながら，組織図を作りあげていくとうまくゆくかもしれません．資料 2 「ISMS における組織と役割.doc」にまとめてあります．
>
> (3) 所在地 (location)
> 物理的な適用範囲です．キャンパス所在地，キャンパスマップ，フロア平面図などに，具体的に適用範囲を書き込んでいきます．入退室などの管理がどのように行われているか (例: 常時施錠，IC カードによる認証，番号キーによる認証) などを記載したり，立ち入り制限の区分け (例: 関係者以外立ち入り禁止，第 3 者でも立ち入り可，物品等の受け渡し場所) などがわかるように色分けなどをすると判りやすくなります．資料 1 には平面図のサンプルとセキュリティ上公開しても問題の無い図面のみが含まれています．
>
> **(中略)**
>
> なお，規格 4.2.1 a) にある通り，適用範囲からの除外についても理由の説明が求められます．

文書をそのまま提供したのでは情報セキュリティ上の問題が発生するため，次のような方針に従って文書の一部を削除している:

P 基本方針はそのままサンプルとして提示する．他にも本学の事例や他機関の事例の中で特徴があるものなどをサンプルとして合わせて提示することを検討する．適用範囲については一部図面及びネットワーク図を除外し，サンプルと置き換える．ISMS マニュアル類は細則を含めて全体を一つの文書にまとめて ISMS マニュアルとする．リスクアセスメント結果全体は提供せず，主要残留リスク説明書と管理策適用宣言書を適宜情報を削除して提示する．管理策実施手順書 (これは対策基準でもある) 及び関連手順書は一つの文書にまとめ，関連手順書は付録とする．ただし，手順書の中で，A.9〜A.12 は技術的なセキュリティに関する箇所であるため提供はしない．導入運用許可書については TF[⋆1]の活動報告書を削除した上で提供を行う．

D 計画書や記録類のテンプレートを提示する．有効性測定方法については A.9〜A.12 以外を提供する．インシデント管理システムが稼働していればシステム及びその利用マニュアルも提示する．[⋆2]

C C フェーズに関係するものとしては，内部監査関係についてはチェクリスト等のテンプレート，マネジメントレビューのインプットの大枠だけ残してページに説明を付したもの，マネジメントレビューアウトプットのサンプル (CIO に入力サンプルとして渡しているもの)，を提供する．

A A については TF 編成案，次サイクル計画案の一部を提示する．

3.1 テンプレート提供方法

今回作成した文書は本学の業務として作成を行ったものであり，著作権は通常の研究成果物とは異なって作成者個人には帰属せず大学に帰属する[⋆3]．このような法人著作物は，スタッフ個々人の判断で外部に文書を提供することとはできないため，特許等の知的財産と同様に，本学の産学公連携・イノベーション推進機構が行う，知的財産 (以下, 知財) の外部

⋆1 本センターの ISMS で適宜タスクフォース (TF) を編成して業務を進めている．A フェーズでは，次の P フェーズで必要となる作業を整理し，その上でそれぞれのタスクを数名のスタッフからなる TF にアサインしている．「リスクアセスメント見直し」TF のように，D フェーズ以降のリスクセスメントの見直し計画の立案のみを行うものや,「法令チェック」TF のように実際に新規法令や法令改正を実施する TF が存在する．

⋆2 現在もインシデント管理システム実装プロジェクトが進行中である．

⋆3 法人著作であるため，作成者であっても著作物を利用する際には原則として大学の許可が必要となる．ただし，作成者には自身が作成に関与した部分について，研究資料は講義資料などとして利用することできるか否かについては，作成者と法人との覚書きを取り交わすことがある．本件は現在協議中である．

1. P	1 適用範囲	0 ReadMe 適用範囲.docx
		1 適用範囲と境界・サービスの定義.pdf
		1' (ワード文書)適用範囲と境界・サービスの定義.doc
		2 ISMSにおける組織と役割.doc
	2 基本方針	0 ReadMe 基本方針.docx
		1 基本方針例.pdf
	3 ISMS マニュアル	0 ReadMe ISMSマニュアル.docx
		1 ISMSマニュアル.doc
	4 リスクアセスメント	0 ReadMe リスクアセスメント.docx
		1 リスクアセスメント手法.docx
		2 主要残留リスク説明書（2010年度版）.doc
		3 メディア基盤センターISMS管理策適用宣言書.doc
	5 対策基準・実施手順	0 ReadMe 対策基準・実施手順.docx
		1 JIS Q 27001 附属書A管理策手順書.doc
	6 導入運用許可	0 ReadMe 導入運用許可.docx
		1 ISMS運用計画書.doc

図 3 ISMS 構築用テンプレート: P フェーズ関連文書

2. D	1 リスク対応計画	0 ReadMe リスク対応計画作成.docx
		1 リスク対応計画テンプレート.docx
		2 リスク対応計画 (センター経営).docx
	2 記録	0 ReadMe 記録.docx
		1 小串センターソフトウェアライセンス一覧.xls
		2 小串センター保管ファイル一覧.xls
		3 小串センター廃棄報告書.xls
		4 障害訓練計画書.doc
		5 退職・異動時のアクセス権限等確認書 .doc
		6 権限解除アクションリスト.xls
		7 新サーバ室入室・来客簿.doc
	3 有効性測定手順	0 ReadMe 有効性測定手順.docx
		1 管理策の有効性の定義と測定 (含 測定方法及び結果記入テンプレート).doc
		2 管理策有効性測定方法及び結果.docx

図 4 ISMS 構築用テンプレート: D フェーズ関連文書

販売の形式を取ることとなる．知財の販売は，本学では通常有限会社山口 TLO に委託しているが，特許と異なって ISMS 関連の市場を山口 TLO は必ずしもつかんではいないため，メディア基盤センター等が販売促進活動も行わなくてはならないという現実的な問題点がある．また，今回テンプレート化する文書の一部は株式会社 ITSC とのコンサルタント契約の上で作成されたものであるため，契約により ITSC 社が提供するテンプレートに基づいて作成された二次著作物は共同著作物として扱う必要がある．そのため本学が独自に販売を行うためには，著作権処理が必要となる．この問題を解決するため，共同著作者である ITSC 社に ISMS 構築用テンプレートの販売を委託し，同テンプレートを用い同社のコンサルテーション業務を許諾する方向で検討が進んでいる．

4. 適用範囲の拡張

従来の適用範囲，すなわち，教育・研究用コンピュータシステム及び基幹ネットワークの運用に加え，情報環境部情報推進課が行っているハウジングサービスと関係するサーバ室も適用範囲に含める方針で作業を進めている．作業計画は次の通りである:

認証範囲　現在「大学情報機構メディア基盤センター」の名称で，３センターをサイトとし,「教育・研究用コンピュータ及び基幹ネットワークシステムの管理運用」を適用範囲としている．名称及び適用範囲を変更する必要がある．

基本方針　基本方針名称を認証範囲の名称に合わせる．また，基本方針がセンターのみを対象とする文書になっているため，大学情報機構を対象とするものに変更する必要がある．

適用範囲の定義　基本的な定義を変更する

- 組織: メディア基盤センター及び情報環境部へ変更．組織図に部長及び情報推進課の関係職員を組み込む．さらに「組織と役割」にも反映させる．(CIO 補佐もセンター長に加えて部長を入れないとだめ．)
- サービス: 情報推進課によるハウジングサービスを追加
- ロケーション: 情報推進課サーバ室を追加．図面も修正
- 資産: 情報推進課サーバ室及びハウジングサービスに必要とされるものを追加
- 技術: 情報推進課サーバ室内のネットワーク設備を追加．

リスクアセスメント　大学業務用ハウジングサービスを資産として追加し，リスクアセスメントを行う．他センターのサーバ室のリスクと同様なのでコピー・ペーストした上で微調整．

手順書　ハウジングサービス及び部屋の入退室の手順書を作成する．メディア基盤センターのものを参考にして微調整．

契約書　ハウジングサービス利用者との契約書を作る．契約書が重いということであれば，利用者にサービスレベルアグリーメント (SLA) についてのアナウンスを行うのみとする．

管理策手順書　管理策手順書記載の手順で問題が無いかを確認．

文書全般　ヘッダの部分が「大学情報機構メディア基盤センター」になっているので「大学情報機構」に変更．また文書全体に「センター」,「センター職員」ということばが随所に現れているため，適宜「機構」や「ISMS スタッフ」などの名称に変更をする.「プロジェクトリーダ」も名称変更が必要．

現在はこれらの作業を順次進めている段階である．

5. ま と め

本学の ISMS 関連の活動として，ISMS 構築テンプレートの販売と適用範囲の拡張について概略を述べた．本学の ISMS 構築の結果が他大学における情報セキュリティ文化の普及に少しでも役立てばと考えている．また，今回の適用範囲の拡張は，規模自体は小さいものの，事務組織内に ISMS 適用範囲を拡げる本学では初めての試みとなる．この経験が大学情報機構にとどまらず他部署における ISMS 構築の動きにつながることを期待している．

謝辞　本研究は山口大学大学情報機構スタッフ及び株式会社 ITSC 様の多大なる協力のもとに行われております．ここに記して謝意を表します．

参 考 文 献

1) 八巻直一，藤本　徹，長谷川孝博，館野康彦，小林伸睦，野崎宏明，中山雄一，岡田吉弘，井上春樹：大学の IT コンプライアンス，静岡学術出版 (2007).
2) 電子情報通信学会編：情報セキュリティハンドブック第 5 編第 4 章，オーム社 (2004).
3) JIS Q 27001: 2006 (ISO/IEC 27001:2005): 情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステム要求事項，日本規格協会 (2006).
4) 国立大学法人情報処理センター系協議会 ISMS 研究会：Web ページ，
`http://sigisms-nipc.cc.yamaguchi-u.ac.jp/`.
5) 日本規格協会：ISMS ユーザーズガイド: JIS Q 27001:2006(ISO/IEC 27001:2005) 対応，
`http://www.isms.jipdec.jp/std/index.html`.
6) 羽生田和正，池田秀司，荒川誠実：ISMS 構築･認証取得ハンドブック―ISO/IEC 27001 対応 情報セキュリティマネジメントシステムの事例集，日科技連出版社 (2008).