Vol.2009-IOT-6 No.6
2009/6/27

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構築の実例

市川哲彦[†1]　永井好和[†1]
長谷川孝博[†2]　三池秀敏[†3]

個人情報保護法の施行を機会に，従来から重視されていた組織の情報セキュリティの在り方について更に注目が集まるようになり，情報セキュリティマネジメントシステム (Information Security Management System, ISMS) の構築・運用が盛んになった．ISMS は適切な情報セキュリティレベルを維持するための組織的な取り組みのシステムであるため，効率の良い導入・運用を行わないと組織にとってオーバヘッドとなり，組織の本来の業務の支障となる可能性がある．本論文では，本学における ISMS 構築・運用の一連のプロセスを紹介し，それらを実施する上で我々が得た知見について議論を行う．

A case study of supporting information security management systems at Yamaguchi University

Yoshihiko Ichikawa,[†1] Yoshikazu Nagai ,[†1]
Takahiro Hasegawa [†2] and Hidetoshi Miike[†3]

Information security has become one the most important concerns for our society. Information security management systems (ISMSs) are human- and computer- systems to support required security levels. Since the main part of ISMSs comprises human activities, reducing the overhead for supporting ISMSs is a critical issue in order to support ISMSs effectively. This papaer describes the ISMS support processes in our university, and also addresses our know-hows concerned mainly with utilization of information processing systems and methodologies

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)]) の認証を取得した．

ISMS は適切な情報セキュリティレベルを維持するための組織的な取り組みのシステムであるため，効率の良い導入・運用を行わないと組織にとってオーバヘッドとなり，組織の本来の業務の支障となる可能性がある．そのため，ISMS の構築・運用の各フェーズにおいて各種方法論の活用や情報処理システムを効果的に利用することが求められる．なお本論文では，特定用途で情報の加工を行うためのコンピュータシステムのことを情報処理システムと呼び，コンピュータや人を含めた組織的な活動の仕組みを情報システムと呼んで区別することにする．

本論文の目的は，山口大学メディアキバンセンター (以下，本センターと呼ぶ) における ISMS 構築・運用の一連のプロセスを紹介し，それらを実施する上で我々が得た知見を，情報処理システムの活用や方法論的な工夫を中心にして説明することである．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が，各組織の活動内容は組織毎に異なっているのが当然であるため，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となる．本センターは，大学の活動の基盤となるコンピュータネットワークや各種サーバ類，さらに，プリントサービスや教室システムなどのサービスを学内に提供する組織であ

†1 山口大学メディア基盤センター
Media and Information Technology Center, Yamaguchi University
†2 静岡大学情報基盤センター
Center for Information Infrastructure,, Shizuoka University
†3 山口大学大学院理工学研究科
Graduate School of Engineering, Yamaguchi University

る．主たる利用者が学生や教職員という点では一般的な企業とは異なるかもしれないが IT インフラの整備と付随するサービスの実現という点では，自治体やサービスプロバイダーなどとも共通する部分があると考えられる．このことから，本センターでの ISMS 構築の実際の様子や，一連のプロセスにおける情報処理システム活用のノウハウはは参考になるのではと期待している．

以下では，まず本センターにおける ISMS 構築の経緯について述べ，続いて ISMS 構築プロセスにおけるアウトプットがどのようなものであるかを説明する．アウトプットの種類については特徴があるわけではないが，規格で要求される事項を利用する様式に反映させることもまた極めて重要なノウハウである．[*1] 引き続き，各フェーズを実施するにあたって利用した方法論や，それらを実施するにあたってどのようなツールを利用したかについて説明を行う．最後にまとめと今後の課題について述べる．

2. 山口大学メディア基盤センターにおける ISMS 構築の経緯と体制

国立大学は 2004 年度より国立大学法人へと組織が変更され，それに伴い 6 年間を 1 期とした中期目標およびその実現のための中期計画の策定と，各年度毎の年度計画の作成が求められるようになった．これらはその 6 年間における大学の活動指針を与えるものであり，その達成度は文部科学省に設置された国立大学法人評価委員会によって評価がなされる．本学では情報セキュリティに関する注目が集まっていることから，2004 年度〜2009 年度の中期目標として「学内情報セキュリティーの基本方針を定め，情報の安全確保に努める。」が掲げられ，また，そのための具体的な方策の一つとして学内の情報基盤を運営しているメディア基盤センターにおける ISMS 構築の検討が開始された．2006 年度から本格的な構築プロセスに入り 2008 年 10 月に JIS Q 27001:2006 (ISO/IEC 27001:2005) に基づく認証を取得した．

ISMS の構築と運営は，組織内に ISMS 推進事務局を置き，そこが中心となって行われるのが一般的である．大学では各種委員会の下にワーキンググループ (working group, 以下 WG) を設置して実務的な側面を担当することが多いため，当初は WG を構成することも検討した．ところが，準備段階で WG メンバーであるスタッフとそれ以外のスタッフとの間で理解度に大きな差が出てしまい，活動がはかどらない問題が発生した．そこで構成員が 20 名程度と比較的小規模であることを考慮し，通常 WG の下に置かれるタスクフォース (task force, 以下 TF) を ISMS 事務局の下に柔軟に編成することし，全スタッフが全てのフェーズにおいて必ずなにがしかの作業に参加する体制にした．ISMS 事務局が TF の編成や進捗フォローなどを細かく行わなくてならないということや教育コストが高いという問題もあるが，全員参加体制での ISMS 構築が可能であることから，(1) 基本方針・手順等の周知が徹底できる，(2) ISMS に係わることで一連のプロセスの理解が深まる，(3) 特定スタッフへの負荷の集中を避けることができる，というメリットがある．適用範囲が小さいからこそ実施できる体制ではあるが，大学における情報処理センターなどの小・中規模の部門などでは有効な手法であると考えられる．

3. 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．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組織毎に異なっているのが当然であるため，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となる．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．

本節では，PDCA サイクルのフェーズ毎のアウトプットについてまず説明し，続いて本センターにおける ISMS 構築・運用で作成した具体的な様式について説明を行う．アウトプットとして何が求められるかは規格要求事項に含まれているため，作成される文書などの種類は組織によるばらつきはあまり無いものと考えられるが，それらの様式を定め，アウトプットをより的確かつ効率良く生成できるようにすることが ISMS の構築・運用では極めて重要なスキルである．従って，本節の記述は単なる様式の説明ではなく，我々が構築・運用得た知見そのものであると言える．

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．なお，本セ

⋆1 なお，一部の文書は (株)ITSC 社のコンサルティングに基づいて作成している．従って，公開ができない部分もある点をご了承いただきたい．

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，実施基準・詳細手順等を定めた手順書，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，リスク対応計画実施報告
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，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.	予防・是正処置計画書，利害関係者への通知・契約の変更

ンターでの ISMS 運用では年度計画の策定は A フェーズにおいて行うこととし，P フェーズでの活動計画などもすべてこの段階で決定を行うこととしている.

3.1 PDCA サイクルにおける各フェーズとそのアウトプット

3.1.1 Plan(確立) フェーズ

ISMS の構築を行う際にまず行うのが適用範囲 (scope) と境界 (boundary) の定義である．適用範囲は，誰が (組織)，何を (事業)，何処で (所在地)，何を用いて (資産[⋆1] および技術) 行っている活動か，によって定義される．またこの範囲の内側と外側を区切るものが境界となる．内側の組織は第一者，外側は第三者，第三者でも特に契約関係などがあれば第二者となる．組織間の境界の内と外，それから物理的な境界の内と外では管理方法が異なるため，適用範囲の設定の仕方によって実施されるセキュリティ対策は大きく異なってくる.

次に基本方針を策定する．基本方針はリスク管理の目的や方向性・原則，遵守すべき法律や契約，リスク評価の基準，適用範囲，が矛盾無く記述され，かつ経営陣が承認した文書である．規格要求の 4.2.1) が P フェーズにに関して記述した箇所であるが，ここでは，基本方針についてのみ言及されており，通常セキュリティポリシーを確立する際に必要とされる，管理基準 (standard) や詳細手順 (procedure) については言及されていない．しかしながら，4.2.1) のリスクアセスメントの項で言及されている管理策 (control) の実施に必要となる各種手順書や，D，C，A の 3 フェーズについての要求事項を説明した 4.2.2)〜4.2.4) で直接・間接に言及されている教育訓練 (詳細は 5.2.2)，内部監査 (詳細は 6)，マネジメントレビュー (詳細は 7)，予防・是正処置 (詳細は 8) などを実施するための手順書も備える必要がある．そのため，P フェーズで以降の 3 フェーズを円滑に実施するための体制を整えるためには，これらの必要となる手順までを整備し，ISMS マニュアルとして整理しておく必要がある．管理すべき文書および文書管理方法についての要求は，規格要求の 5 にまとめられている.

P フェーズの柱となるのがリスクアセスメントである．リスクアセスメントでは (1) そのためのアプローチと受容基準を定め，(2) 資産を洗い出し，(3) 定められた手法にもとづいてリスクを分析・評価し，(4) リスク対応 (risk treatment) を検討する，という手順を踏む．リスクアセスメントアプローチは文献[4] にいくつか例が記載されているが，その中のマトリックスアプローチが一般的である．リスクアセスメントのより詳しい説明については第**??**節にて行う．リスクアセスメントの結果として，組織がどのようなリスクにどう対応すべきかが明確になる.

最後に規格要求の付属書 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し，適用宣言書にまとめる．これらの結果とこの結果に基づく ISMS の導入と運用については，経営陣によって承認を得ることが要求されるため，許可書の準備もまた必要となる．以上を整理すると，P フェーズのアウトプットは，適用範囲，基本方針，ISMS マニュアル，リスクアセスメント結果，適用宣言書，経営陣による導入・運用許可書，となる.

規格要求では，リスクアセスメントの結果必要とされるリスク対応計画の立案や，後の C フェーズで必要とされる管理策の有効性測定方法の定義は，それぞれ 4.2.2 a) 及び 4.2.2 d) で定義されており，D フェーズで実施することとなっている．本センターの事例では，これらを P フェーズの一部として実施した．これは，年間計画や予算要求が関係するため，早期に計画を立案し実施体制を整えることが重要と判断したためである.

3.1.2 Do(導入・運用) フェーズ

D フェーズでは，リスク対応計画の立案と実施，管理策の実施手順書に定められた手順の実施，管理策有効性測定方法の定義，がなされる．また，規格要求の 4.2.2) には明記されていないが，記録の管理 (4.3.3)) 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ため，入退室やシステム保守などの日常的な活動

⋆1 資産 (asset) は規格書では「組織にとって価値を持つもの」と定義されており，組織を構成するスタッフ，業務を遂行する上でで利用されるコンピュータなどの機械，ソフトウェア，電力など組織が提供を受けているサービス，電子メイルや通信基盤など組織が提供しているサービス，紙媒体や電子媒体で管理されている情報，などが全て含まれる.

やインシデントの管理が求められる．既に述べたとおり，本センターではリスク対応計画の立案と管理策有効性測定方法の定義は，P フェーズにおいて実施している．また，何をどのように記録するかについてもあらかじめ決めておく必要があるため，本センターの事例では P フェーズにおいてこれらを定めている．

3.1.3 Check(監視・レビュー) フェーズ

C フェーズは監視とレビューという二種類の活動から構成されている．レビューは定期的に実施される活動であり，管理策有効性測定，内部監査，マネジメントレビューが該当する．監視 (monitor) はいつとは決めずに随時実施する活動であり，インシデントに対しての是正処置の計画や，予見されるインシデントに対しての予防処置の計画などが含まれる．内部監査 (internal audit) は組織内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相互に行う相互監査である．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レビューものの他に，日常的なコミュニケーションによっても行われる．以上をまとめると，このフェーズのアウトプットは，監視からは予防・是正処置計画書が，また，レビューからは管理策有効性測定結果，内部監査結果，経営者の判断や指示を与えるマネジメントレビュー結果が含まれる．

3.1.4 Act(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 P フェーズにつなげるための活動となる．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．本センターの事例では，これらに加えて，次の PDCA サイクルの計画と，次の P フェーズの活動計画の立案も A フェーズで行っている．これらは企画書では特に求められていないが，円滑に PDCA サイクルを実施するために常に次フェーズ以降の実施計画を立案しておくことが必要不可欠であるたえ，次の P フェーズのインプットを作る A フェーズで実施をすることとした．

3.2 本センターで利用した各種様式

上述の通り，各フェーズを進めるに当たっては，さまざまなインプットやアウトプットを作成する必要がある．概念的にどのようなものを作成すれば良いかは既に述べた通りであるが，実際に組織の中でそれらを作成する際には，言葉だけでは具体的にイメージすることが難しく，業務を遂行するに当たって適切な様式の定義を行う必要がある．本節では，特に本センターにおいて工夫を行った点を中心説明を行う．なお，今回の ISMS 構築は (株)ITSC 社によるコンサルティングの基で最初の PDCA サイクルを実施したため，一部については共同での開発となる．

3.2.1 P フェーズ

P フェーズを進める上で最も時間的なコストがかかるのが資産の洗い出しとリスクアセスメントである．資産の洗い出しは次の手順で行った: 1. 業務手順書や業務フロー図を元に，各業務において (i) 入って来る情報，(ii) 出て行く情報, (iii) アクセスする情報, (iv) 保管情報, (v) 利用する資産，をピックアップしリストする; 2. 資産の重要性に配慮して取捨選択する; 3. グルーピングによりアセスメント対象とする資産数を減らす．なお，本センターの例では業務フロー図などは必ずしも整備されていなかったため，担当者が自身の業務内容を考慮して資産をピックアップしている．

資産の洗い出しは電子スプレッドシートに記入項目を決定して書き込むことで簡単に作成できるように見えるが，実際には次の二点を考慮に入れる必要がある．まず，上述の手順にもあるが資産は個別に扱われるのではく適宜グルーピングされるという点が挙げられる．例えば教室内には同様のパーソナルコンピュータ (以下 PC) が複数台設定される．これは，同じ場所で，同じ用途で利用されており，持っているリスクもほぼ同じである．従って，帳簿上個別に扱われているものであっても，一グループにまとめて資産として管理すれば ISMS の目的であるリスク管理という観点からは問題はない．更に本センターの例では，同一サービスを構成する資産は一つにまとめるという方法を採用した．これにより，例えば電子メイルサービスを構成する，複数台のサーバ類やアプライアンスを一つの資産として管理することができる．従って資産を洗い出す上では，このようなグループ構成を念頭に置き，大分類，中分類，小分類といった分類階層を作成した上でリストアップ作業を進め，その中で適宜グルーピングを進めるのが作業量削減につながり効果的である．

次に，資産の価値はその資産に依存する他の資産の価値に左右されるということも重要である．[⋆1] そのため，資産価値はリスク対応の必要性を決定する重要な尺度であるため，こ

⋆1 ここで資産の価値は経理上の簿価や市場における取引の価値ではなく，その資産の組織に取っての重要度，すなわち，その資産になにがしかのトラブルが発生した時の影響度の大きさを表す．例えば，全学に認証サービスを提供している LDAP サーバの市場価値と，全学の電子メイルユーザにスパムフィルタリング機能を提供しているアプライアンスの市場価値が同じであっても，前者の方が資産としての価値は高いと見なすのが適切である．

の依存関係を適切に把握することが，後段のリスクアセスメントで必須である．例えばサーバ類はそのオペレータたるスタッフに依存している．従って，多くの重要なサーバ類のオペレータをしているスタッフはそれだけ資産価値が高いことになる．また，認証サーバやファイルサーバなども教育システム，ネットワークシステムなどの他の資産にサービスを提供しているので，それだけ資産価値が高くなる．これらの依存関係の中には電力への依存など，ほぼ自明と言えるものもあるが，必ずしもすべてが自明ではなく，依存関係も変化するものであるため，資産表のレベルで管理できるようにすることが望まれる．上記のような観点から，資産表の見出しは，大分類，中分類，小分類，資産名，資産が依存する資産，担当者(責任者)，保管形態，設置場所，保管期限，廃棄方法, 資産の利用者，資産に依存している資産，関係法令，としている．[⋆1] リスク対応については，比較的長期間にコストをかけて実施すべきリスク対応計画は別葉に落としているが，簡単なものはこのようにリスクアセスメント結果に直接書き込む形式としている．

3.2.2 D フェーズ

D フェーズでは記録管理やインシデント管理が重要である．入室記録などの各種帳票はこれまでも利用されてきたものを多少修正してそのまま利用している．問題となったのは，インシデント管理であり，日常的に発生する数多くのトラブルをどこまでどのような形式が記録するかが議論された．現在は従来より利用しているインシデント等のイベントを学内外に広報するためのシステムをそのまま利用して管理しており，今後はワークフローに対応したシステムに移行する予定である．

3.2.3 C フェーズ

予防・是正処置は随時計画・実施されるものであるため，計画書の定型様式を作成して対応している．内部監査とマネジメントレビューはチェックの範囲が ISMS 全般にわたるため，いかに効率よくインプットとアウトプットを作成するかが問題となる．内部監査では規格要求事項に対してチェックシートを作成し，予備的な自己監査の後，監査人による本監査を行う方式を採用し，本監査の効率を高めている．チェックシートの記入例を図 1 に示す．1〜3 は事前に内部監査チームが記入して提示を行うので，被監査組織側が 4〜5 を内部監査実施前に回答する．6〜9 は監査当日に内部監査チームが記入するものであるが，書面で確認できるものは事前に確認し，必要があれば当日再確認を行う．なお，実際にはこれらを横方向に並べた電子スプレッドシートを用いて監査を行っている．

1	規格要求事項	4.2.1 a)
2	チェック項目	適用組織と関係する外部組織が適切に記載されているか.
3	確認のための補足事項	組織図を用意いただき，ISMS 適用予定範囲と適用範囲外とする組織の境界を明確にした図を用意してください.
4	確認資料・確認方法	組織図
5	自己点検回答	ドキュメント 03-1「ISMS における組織と役割」組織体制図参照
6	自己点検者	市川
7	評価	A (適合)
8	監査対象者コメント	同ドキュメントの全学組織図も参照
9	監査者コメント	特になし.

図 1 内部監査用チェックシートの例: 1〜3 は事前に内部監査チームが記入して提示; 4〜5 は被監査組織側が内部監査実施前に回答; 6〜9 は監査当日に内部監査チームが記入. (注意: 実際にはこれらを横方向に並べて監査を行っている)

	項目	説明
1	ISMS の構築・運用状況報告	
2	内部監査結果報告	
3	利害関係者からのフィードバック	利用者からの希望など
4	予防・是正措置の状況	
5	有効性測定結果	
6	教育・訓練	
7	前回マネジメントレビューへのフォローアップ (省略)	
8	ISMS に影響を及ぼす学内外の変化	技術的な変化，法令の変化等
9	ISMS 改善のための提案	スタッフから改善提案や CIO への希望
10	その他改善のための提案	
11	その他関連事項	

図 2 マネジメントレビューインプット

マネジメントレビューの項目立ては規格要求 7.2 を参考に図 2 のようにまとめた．これに CIO 講評を加えたものがマネジメントレビュー会議の議事次第となる．CIO は，このレビュー会議での報告を受けインプット内容の評価を行い，最終的な指示内容の作成を行う．インプット内容の評価については，確認事項をあらかじめ準備し CIO には確認内容にそった所見を記入してもらっている．これを図 3 に示す．さらにここから指示事項だけを抜き出したものが最終的なマネジメントレビューのアウトプットである．改善指示は次の 5 種類

これは，前者にトラブルが発生すると，教育・研究などのほぼ全てのサービスが停止してしまうが，後者のトラブルは業務効率を著しく低下はさせるものの完全なサービス停止にはいたらず，組織への影響度は相対的に低い，ためである．簿価や市場価値は，むしろ事故原因の発生頻度や脆弱性の評価に反映される．

⋆1 実際には管理の都合上その他の項目も含まれている．

	項目	確認事項	所見
1	ISMS の構築･運用状況報告	・ 構築はスケジュール通りか・ 適用範囲は適切か. ・ 資産表は適切に管理されているか. ・ リスクアセスメント方法や結果は適切か. ・ リスク対応計画は適切か，また，計画通り実施されているか.	・ 文書作成を進めること。今後のスケジュールが不明. ・ 概ね適切。他部署との責任や役割の境界を明確にすること. ・ 資産表を完成させること. ・ 残留リスクを明らかにすること。基準の見直しを検討すること. ・ 適切
2	内部監査結果報告	・ 内部監査結果に対する改善はなされているか. ・ 内部監査は適切か. ・ 認証機関からの指摘にたいする改善はなされているか.	・ PDCA サイクルの中で確実に対処すること. ・ 適切. ・ PDCA サイクルの中で確実に対処すること.
3	利害関係者からのフィードバック	・ 利害関係者の要求事項を自らのサービスに反映させているか.	・なされている.

図 3 マネジメントレビューアウトプット (1): インプットの評価 (一部)

(a) ISMS **の有効性改善**		
事項 (関係インプット項目)	**指示分類**	**指示内容**
規格に合致した手順の文書化 (1)	改善	必要書類を本審査までには確実に完成させること.
手順の確実な実施 (1,4)	評価	手順に従った自主的な改善活動が実施されている．内部監査結果などを踏まえ引き続き改善をされたい.
有効性測定 (4)	提案	副センター長レビューが未実施のサイトがあるので実施を検討すること.
ISMS スタッフ教育 (6)	維持	スタッフの ISMS 教育がなされている。引き続き，レベルが向上するよう努力を行うこと.
スタッフ教育 (6)	提案	それぞれの職能に必要な教育を行っているのかが不明である．ISMS 以外の教育訓練についてもマネジメントレビューのインプットに含めると良い.
訓練 (6)	改善	事業継続計画を作成し訓練を行うこと.
年度計画 (1)	提案	これまでの年度計画の実施状況の報告及び本審査後から次のサーベイライスまでのスケジュールおよび次年度の年度計画の提案があると良い.

図 4 マネジメントレビューアウトプット (2): 指示内容 (一部抜粋)

に分類している:

- 評価: 現状特に問題は見られず，また，活動内容等が目的に合致しているため，評価に値する事項
- 維持: 現状特に問題は見られないので，引き続き現状を維持すべき事項
- 提案: 特に問題は見られないが，更なる向上のために指示する提案事項
- 改善: 問題が見られるので今後は改善を行うべき事項
- 回答: スタッフからの提案事項に関しての回答．予算や職員増強などの資源の割当てへの決定事項や関連する指示内容を含む.

アウトプットの結果の一部を図 4 に示す.

3.2.4 A フェーズ

A フェーズについては特別工夫した点は無いが，既に述べたとおり次の PDCA サイクルの計画と P フェーズの TF 編成はこの段階で行っている.

4. まとめと今後の課題

ISMS はコンピュータシステムの活用を含む人的なシステムであるため，ワークフローを整理し，各フェーズでどのようなアウトプットが必要かを明確にし，かつ，それらをいかに効率よく確実に生成するかが構築・運用の鍵となる．そこで，本論文では山口大学メディア基盤センターにおける ISMS 構築で得た知見に基づき，ISMS を構成する PDCA サイクルの各フェーズにおいてどのような様式を用意し，また，どのような工夫を行ったかについて説明を行った．このような事例研究は個別の ISMS 構築の現場では行われているものであるが，事例として整理された形で公表されるケースは必ずしも多くは無い．ISMS の認証取得をするかどうかは別にしても，本センターにおける事例を参考にして，今後の情報セキュリティレベルの維持の参考になればと考えている.

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) TR X 0036-3:2001: IT セキュリティマネジメントのガイドライン－第 3 部: IT セキュリティマネジメントのための手法，日本規格協会 (2001).