情報セキュリティのマネジメント体制を具体化
ISMS 認証（ISO/IEC 27001）取得

情報メディア基盤センター　上繁　義史

1. はじめに

長崎大学の情報セキュリティ維持において，情報メディア基盤センターと学術情報部情報企画課の果たす役割は大変重要なもので，数々のセキュリティインシデント（情報セキュリティに係わる事故）に対応してきました。

その中で平成 22 年度から始まった第 2 期中期目標及び中期計画の中で，大学の情報セキュリティに関して以下の文言が加わりました。

第 2 期中期目標
「情報マネジメント体制を整備し，情報セキュリティを向上させる。」
第 2 期中期計画
情報資産の安全管理を高めるための体制を整備するとともに，高度情報セキュリティに対応した人材を育成する。」

そこで，情報メディア基盤センターと情報企画課と共同でセキュリティ体制や活動を確認しながら文書化することにより，情報セキュリティの管理体制（情報セキュリティマネジメントシステム（Information Security Management System; ISMS））を明確化していくこととなりました。

ISMS の国際規格として ISO/IEC 27001 があり，ISMS の計画・運用・チェック・改善（いわゆる PDCA サイクル）の設計及び運用の規準となっています。これに従うことが本学における ISMS の明確化の早道と考え，平成 22 年度より準備活動を開始し，平成 25 年 3 月 ISMS 認証の取得に至り，本学の情報セキュリティの管理体制の明確化を達成しました。平成 25 年度はこれを受け，ISMS 活動の平準化を進めてまいりました。認証の継続に関する審査を受審し（平成 26 年 1 月）これにも合格しました。

本稿では，2 章で ISMS の概要をご紹介します。3 章～6 章で平成 22 年度以降の活動を振り返りながら，平成 25 年度までの ISMS に関する諸活動について報告し，7 章では ISMS 活動の学生教育への展開について報告します。

2. ISMS の概要

個別のセキュリティ上の問題を場当たり的な発想で対処していると，組織としての一貫したセキュリティレベルを保つことができません。そこで，組織としてのマネジメントが必要となります。そのためにまずは自らがもつ様々な情報資産についてリスク評価を行い，必

要なセキュリティレベルを確保できているかを判定します。判定の結果不十分とされた事柄を中心に，組織の持つ資源（人的資源や情報資産など）を適切に配分して，継続的にセキュリティレベルの維持・向上をはかるためのマネジメント体制を作り上げます。このような情報セキュリティに関するマネジメント体制を ISMS といいます。

（1） ISO/IEC 27001

ISO/IEC 27001 は ISMS の構築や ISMS の PDCA サイクルに基づく運用などに関する国際規格であり，本文である要求事項と日常の運用手順に関する管理策から構成されています。要求事項は ISMS の骨格にあたるもので，ISMS の構築を行うのに，必要な文書の種類や PDCA サイクルの各段階において，どのようなことが実施されなければならないかをまとめたものです（下図参照）。ISMS の認証を受けるには，要求事項の全てを満たさなければなりません。また，管理策は情報セキュリティ維持に関係する人員，場所，機材，書類，記録媒体ほかを管理するための目的と具体化するための考え方が 133 箇条に渡って書かれていて，組織の状況に合わせて，具体的な管理の手法をマニュアル化していくことが求められています。こちらは組織の実情に応じて取捨選択したり，133 箇条以外の管理策を追加したりすることができます。

図　ISO/IEC 27001:2005 の要求事項の構成

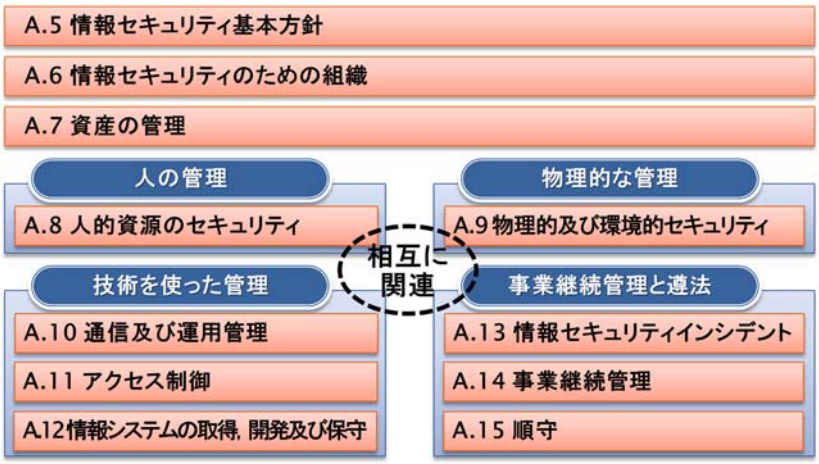

図　ISO/IEC 27001:2005 の附属書 A の構成

3. 平成 22 年度～ISMS に関する調査及び先行的なマニュアル整備

（1） 先行事例の調査

まずは ISMS の理論的な概念について，情報企画課のメンバーとともに調査を行い，並行して先行事例の調査を行いました。先行事例として，平成 22 年 4 月時点で既に ISO/IEC 27001 の認証を取得していた国立大学法人 静岡大学，宇都宮大学，山口大学の状況を，当時の公開記事などから調査しました。

特に山口大学については，平成 22 年 6 月に訪問調査を行いました。その際に静岡大学と TV 会議システムで結び，ISMS の構築，認証取得，運用に関する取り組みについてインタビューを行いました。ここで得た重要な知見は，ISMS が単に大学のセキュリティ維持のための方法であるのにとどまらず，「大学としての社会的責任」や「今後大学が被るリスクに対する保険」として必要不可欠なものである，という認識に立つことでした。

インタビューの結果を受ける形で，情報セキュリティマネジメントシステム構築ワーキンググループ（ISMS 構築 WG）を組織し，情報セキュリティに関する現状分析，本学の情報セキュリティのマネジメント体制構築と実施に関する検討を開始しました。WG のメンバーは筆者を含めた情報セキュリティ専門部会委員 4 名で構成しました。

（2） 先行的なマニュアル整備

ISMS では様々なマニュアルを作成し，周知することが要求されていたことから，先行的に統合認証システム（平成 23 年 3 月より稼働）など，一部のシステムについて，センター及び情報企画課向けのマニュアルを作成しました。

4. 平成 23 年度～ISMS 構築の本格活動開始

（1） 学外の ISMS 研修への参加

ISMS を構築するには，上述のように ISO/IEC 27001 の要求事項を満たすように行うのが早道であるとの考えから，ISMS のより詳細な知識（構築のノウハウや具体的な PDCA サイクルの運用など）について，さらに知見を得るべく，第 4 回 ISMS 研修会（山口大学主催，平成 23 年 5 月）に参加いたしました。そこでは ISMS 構築に関する演習を交えたより具体的な知見を得ることができ，後の ISMS 構築におおいに役立ちました。

（2） ISMS の具体的な検討

平成 23 年夏以降，山口大学での研修を参考に，具体的な ISMS 構築のための検討に着手しました。まずは以下について検討を開始しました。

- 適用範囲 : ISMS を適用する物理的・人的・ネットワーク的な範囲をどのように設定するか。
- 実施体制 : センターと情報企画課がどのように連携するか。また実施体制の中で，学内

委員会等との関係をどのように位置づけるか。

- 情報資産の内容：ISMS を適用する情報資産の範囲をどのように設定するか。

5. 平成 24 年度～ISMS の実践，認証取得

（1） ISMS の構築

平成 23 年度に引き続き情報資産のセキュリティリスク分析を行いつつ，並行して ISMS 全体に関するマニュアル群の作成を行いました。平成 24 年度中の認証取得を目指していたので，コンサルタント（トーマツ）の助言を受けながら，文書のブラッシュアップを図っていきました。10 月に素案がまとまり，実施の準備として，情報メディア基盤センター全教員と情報企画課職員を対象とした内部研修を 11 月に実施しました。ここでは，ISMS の概要と遵守するマニュアル群について解説を行いました。後にテストを実施し，定着度の確認を行いました（要員への教育も ISO/IEC 27001 の要求事項に含まれています）。同時に ISMS の目的や基本方針，実施体制などをまとめた「ISMS 基本方針」をセンターの Web を通じて公開しました（最新版は附録参照）。

（2） ISMS の実践

平成 24 年 11 月より ISMS の PDCA サイクルを実施しました。主だった活動としては以下のようなことが挙げあられます。

- 業務の中でのセキュリティ活動（データセンターやネットワークの維持等）の実施と記録
- セキュリティ事故の確認（検出）・対応・記録
- ISMS スタッフ会議を通じての情報共有
- 内部監査
- センター長によるマネジメントレビュー（経営層からの活動のレビュー）
- ISMS 文書の更なるブラッシュアップと修正内容の周知

（3） ISMS の認証に関する審査

上述の活動の上で，ISO/IEC 27001 の認証審査を BSI ジャパン社に依頼して，平成 25 年 1 月に受審，無事に合格に至りました。その結果，平成 25 年 3 月 4 日に正式に ISO/IEC 27001 認証取得組織として登録されるに至りました。認証登録の名称は「情報企画課及び情報メディア基盤センターが提供する大学総合情報サービス」で，有効期間は 3 年間です。

ちなみに，本学の ISMS の登録状況は一般財団法人日本情報経済社会推進協会（JIPDEC）の Web 上で検索することができます。


bsi.

Certificate of Registration

図　ISO/IEC 27001:2005 認証の証明書（BSI ジャパン社交付）

6. 平成 25 年度～ISMS 活動の平準化，継続審査対応

この年度では，ISMS 活動をさらに浸透させるために，継続的に実践を進めました。新たな ISMS スタッフに対する教育，通常業務の中でのセキュリティ維持の取り組み，内部監査，マネジメントレビュー，ISMS の改善といった一連の活動を通じて，ISMS を担当するスタッフも認証取得以前と比べてもセキュリティについて意識するようになったという声も聞かれました。スタッフの声を要約すると，以下のようにまとめられます。

- 事務室内の配線及び机上の整理が進んで，職場環境が良くなった。
- 情報セキュリティに関するマニュアル類の整備を進めることで，スタッフ間での確実な共有ができるようなり，セキュリティ活動が効率的に行えるようになった。
- 管理策の検討を通じて，自分たちのセキュリティ活動を総合的に見直すことができ，業務に関する有用な気づきが多くなった。
- 外部業者に対して，ISMS に基づくセキュリティ上の要求を行うことで，お互いに適度な緊張感を持ちながら協業できるようになった。

ISMS の認証は毎年中間審査（サーベイランス審査）があり，平成 26 年 1 月に受審しました。そちらの結果も良好で，ISMS 認証の維持が認められています。

7. ISMS の副次効果～学生教育へのフィードバック

ISMS 構築の経験は，教養教育における情報セキュリティに関する教育にフィードバックされています。学部 1 年前期の必修科目である「情報基礎」では，講義資料（本センターで作成）の 1 章を情報セキュリティに充てていますが，その中で日常のセキュリティ対策に

関する内容を充実させることができました。

また，本センターが責任部局となっている全学モジュール「情報社会とコンピューティング」のモジュールⅠ科目「情報社会の安全と安心」（学部 1 年後期）において，情報セキュリティに特化した授業を展開しています。その中では，グループ学習による ISMS 構築の演習を行っており，情報資産のリスクアセスメントやリスク対応，管理策の作成などを実践的に学習できるようになっております。

8. まとめ

本稿では，ISMS の活動全体を振り返り，情報メディア基盤センターと情報企画課による情報セキュリティ体制の明確化の過程と，学生へのセキュリティ教育の現状について，報告しました。今後の活動としては，ISO/IEC 27001 が平成 25 年 10 月に改訂されたことに伴い，本学の ISMS も平成 26 年度中にそちらに対応を図っていくとともに，更なるセキュリティ体制の改善を図ることです。また，ISMS は情報メディア基盤センターと情報企画課だけで取り組めば良いというものではありません。学内には様々な情報資産があることから，ISMS の経験に基づく，情報セキュリティの啓発を進めたいと考えます。

（附録）ISMS 基本方針

この基本方針は平成 26 年度時点の最新版です。（以前のものが既に有効でないため）

ISMS 基本方針

制定：平成24 年11 月 9 日
改訂：平成25 年 1 月21 日
改訂：平成26 年 4 月 1 日
ICT 基盤センター長

1. 目的

学術情報部情報企画課及びICT 基盤センターは，長崎大学における情報基盤の中核組織であり，管理運営を担っている各種業務系・教育研究系システム及びネットワークシステムの安定　的な運用を行うために，情報セキュリティマネジメントシステム（以下，ISMS という）の活動を行います。

また，本基本方針においてISMS の適用範囲及び責任体制を定めて，ISMS の行動規範とします。

2. 基本方針

(1) 情報セキュリティを確保するために，責任体制を構築し，マニュアルを定め遵守するとともにISMS の運用に携わる者に必要な教育等を行います。

(2) 関係法令及び本学の規則，情報セキュリティポリシーを遵守し，情報セキュリティの確保を行います。

(3) 情報資産のリスクに対しては，適切な規準を用いて評価する仕組みを定め，定期的なリスクアセスメントを実施することにより，情報セキュリティの確保を行います。

(4) 本学の公共性及び教育・研究機関としての特殊性を考慮し，特にシステムの継続的な運用を行います。

(5) 情報セキュリティの確保を行うために，定期的に内部監査を行い，改善を行うことでISMS の信頼性の向上を継続的に行います。

3. 適用範囲

(1) 対象組織：情報企画課及びICT 基盤センター

(2) 対象業務：対象組織が提供する大学情報総合サービス

(3) 対象資産：対象組織が保有する情報資産（紙媒体も含む）

4. 責任体制

(1) ISMS 監督者

ICT 基盤センター長は，ISMS 活動の最高責任者として，その業務を総括する。

(2) ISMS 管理責任者

情報企画課長は，ISMS 管理責任者としてISMS 活動に関する管理運営を担う。

(3) ISMS スタッフ

情報企画課の職員は，ISMS スタッフとしてISMS 活動の実務を担う。

(4) 内部監査責任者

内部監査責任者は，本学の職員よりISMS 監督者が指名し，ISMS に関する基本方針，マニュアル，規程，手順について定期的な内部監査の実施を担う。