メディア基盤センター年報（2007年度） より

1.　巻頭言（センター長）

2007年度、メディア基盤センターは日常業務（ネットワークの維持管理、各種サービスの提供、窓口業務等）以外に、主として以下のような活動を行ってきた。

1） センター活動の透明化：業務・試行・開発・研究等のセンタープロジェクトへの申請と報告

2） 情報セキュリティマネジメントシステム（ISMS）の構築＆認証取得に向けた取り組み

3） 情報セキュリティ講習会の開催（セキュリティ委員会との共催）

4） 迷惑メール対策の継続とメールの配送遅延対策

5） 2009年3月機器更新（電子計算機システム）に向けた仕様策定支援

6） センターの広報改善プロジェクトの推進（HPの改定等）

7） 講義室等のネットワーク高セキュリティ化推進

8） デジタルコンテンツプロジェクト（eラーニング研究会の発足等）

9） 平成21年度（2009年度）概算要求への準備（ネットワークの老朽化対策）

この中で2007年度の目玉となったプロジェクトは、2）ISMSの構築＆認証取得に向けた取り組み、4）迷惑メール対策の継続とメールの配送遅延対策、及び8）デジタルコンテンツプロジェクト（eラーニング研究会の発足）などである。以下、主な取り組みの概要を説明する。

2）「ISMS構築＆認証取得の取り組み」は、2005年度より前センター長及び大学執行部の強い意向により始められ、大学全体の危機管理・リスク管理の一環として、特に情報セキュリティ管理の推進においてメディア基盤センターが先陣的な役割を果たすべくスタートしている。

2005年度は、静岡大学の先進的な取り組みなど他大学の構築事例等の調査や、ISMSに関する職員研修、準備ワーキングの設置など準備が進められていた。

2006年度からISMS構築＆認証取得に向けた本格的な取り組みを開始した。特に、ISMS事務局の発足や外部コンサルティング会社の企画競争公募等を実施し、ISMS構築体制を整備した。

2007年度は、前年度に引き続きISMS構築をセンターの主要なプロジェクトとして位置づけ、2008年度認証取得（ISO27001）＆運用に向けて以下のような活動を実施した。

・ISMS構築プロジェクトの継続（予算確保）、
・ISMS適用範囲の設定、
・ISMS基本方針、ISMSマニュアル等の上位文書の策定、
・情報資産の洗い出し＆整理、
・各種マニュアル等の文書作成＆文書管理、

等を進めた。なお、ISMS構築を推進するに当たって、ISMS事務局の事務補佐員を期限付きで採用した（2007年6月より当面2年間）。

４． 情報セキュリティマネジメントシステム（ISMS）の構築（担当・市川） 情報セキュリティへの社会的な意識の高まりを受け，一般企業のみならず大学においても情報セキュリティへの組織的な取り組みが普及しつつある。本学でも全学の情報セキュリティポリシーの策定が既になされており，各部署への普及が中期計画にも謳われている。このような背景と，また，本センターが大学における情報基盤を支えている点に鑑み，我々は他部局に先駆けて2005年度よりISMS構築を開始した。活動は2007年度から本格的となり，国際的な規格であるISO/IEC 27001（JIS Q 27001）の認証取得を一つの目標として構築活動を行っている。2005年度は独自の調査・研究にもとづく構築が主体であったが,2007年度からは前年度末に契約をした外部コンサルタントとも協力しながらISMS構築を行っている。

2007年度には次のような活動を行っている:

a. コンサルティング会社による予備調査とその対応

内部監査で用いるチェックシートの一部を利用し，本センターのISMSの状況をチェックし改善点の洗い出しを行った。初期段階であったため様々な改善点が指摘され，これらは，本センターのスタッフの活動にフィードバックされた。規模の大きなものとしては，サーバ室内の配線のやり直しやラックの耐震工事などが実施されており，また，小さなものでは，事務室内のレイアウト変更などがなされている。クリアデスククリアスクリーン，文書ラベリングなどについても指摘されたが実践までには至っていない事項もあるが，予備調査の実施がスタッフの意識向上にはつながったのは確実である。

b. ISMS上位文書の整備

ISMSは文書化された手順に従って行われるため，トップの意志を表明したISMS基本方針はもとより，基本的な手順を書き表したISMSマニュアル等，参照される各種細則の文書化が必須である。これらISMS上位文書に相当する内容は，これまでにも或る程度は規則化されていたものの，暗黙の了解で進められていた事項や，また，各スタッフが独自にマニュアル化を行っていて共有されていないものも多かったため，コンサルティング会社の提供した雛形をベースとして本センターの組織体制やサービス内容に併せてISMS上位文書の整備を行った。多忙なスタッフが空いた時間を使って文書作成を行わなくてはならないことや，ISO/IEC 27001 の要求事項についての教育が進んでいなかったため，なかなか完成度があがらないという問題もあるが，徐々に作成が進むにつれパズルのピースがそろい全体像が見え始めたと言える。

c. 資産洗い出し

ISMS構築で管理すべき資産を洗い出して目録化することが求められている。ここで資産とは一般的な財産としての資産ではなく，情報セキュリティを維持する上で考慮しなくてはならない資源のことであり，情報(紙媒体や電子媒体のデータ)，PCやサーバなどの装置，OSなどのソフトウェア，電源・空調などのユーティリティ，提供しているサービスや提供を受けているサービス，スタッフ，部屋，など多岐にわたる。我々は各スタッフが担当している業務の一覧をベースに，それらの遂行に当たって入ってくるデータ，出て行くデータ，途中

で参照・更新・保管するデータ，業務を実施する上で利用する装置や装置が必要とするユーティリティやサービス，の一覧を作成し，さらにそれらを提供するサービスの単位でグループ化を行った。この作業は4月に開始したが一通り作業が終わったのは10月であり，かなりの労力が必要とされた。

d. リスクアセスメント

資産の洗い出しに続いてここの資産に関してのリスクアセスメントを行う必要がある。これはそれぞれの資産の価値，関係する脅威，脅威がつけ込む脆弱性を特定し，考えられる情報セキュリティインシデントの可能性を数値的に評価すること，また，その評価結果に対してどのような対策を実施するかを決定するプロセスである。10月頃より作業がスタートし，当初は2007年内には一通り終了させる予定であったが，実際には年度末でも完成せず，作業完了は翌年度に持ち越しになった。スタッフから出されたさまざまな意見を基に，効率的にリスクアセスメントを進めるための手法の検討を行い，改めて作業をやり直しているため，2月3月でおおむね半分ほどを終わらせることができた。この手法については学外で発表する予定であり，本学における試みが他大学・他機関においても活用されることを期待している。

e. ISMS教育

ISMSではスタッフの情報セキュリティについての意識を向上させるため，スタッフ教育を計画的に実施することが求められている。本センターでは，2007年の末に全スタッフを対象としたISMS構築講習会を開催した。講師は外部コンサルタントである。二日間の日程で，ISMS認証規格に基礎とリスクアセスメント実習を行った。本来はもう少し早い段階で実施できると文書整理や情報資産洗い出しなどの活動がより円滑に進められたのではないと考えられるが，全スタッフを二日間拘束すると業務遂行に支障がでるおそれがあるため，敢えて学生が冬休みに入った後に実施した。実習は数名のグループに分かれて行われ，参加したスタッフ全員が積極的に取り組み，活発な議論が行われた。

f. 模擬内部監査

ISMSの認証審査はサンプリング審査であるため，構築したISMSの全てが検査されるわけではない。従って，基本的に文書や実施状況を含めてすべての事項をチェックする内部監査はISMSのPDCAサイクルを回して行く上で非常に重要な役割を果たす。本年度は内部監査チームの教育とISMS構築の一つのマイルストーンとして模擬的な内部監査を実施した。この内部監査には外部コンサルタントがオブザーバとして協力し，内部監査用チェックシートの一部を用いて実施を行った。模擬とはいえ，規格要求事項との適合性や管理策の実施状況をチェックし，また一部であるがサイトツアー（現地視察）を実施することで様々な指摘事項が挙げられた。特に文書類については個々の文書の完成度の問題，整合性，手順の不備が指摘され，これらへの対応を実施する過程でISMS認証審査にむけて大きな一歩を踏み出すことができたと言える。

その他にも，認証審査を受審する第三者機関の検討なども行い，2008年度の認証取得に向け着々と歩を進めている。なお，リスクアセスメントを進めるにあたっては外部コンサルタントの協力が必要であったが，対面での会議は一月に一回のペースであったためタイムリーなコンサルティングを受けることが難しいという問題があった。そこで，コンサルティング会社の本社が静岡にあることから，静岡大学総合情報処理センターに協力をしていただき，TV会議で本学と静岡大学を結んでコンサルタントとの会議を実施した。これにより非常に効率よくリスクアセスメントを進めることができた。ここに謝意を表したい。

参考資料