ISMS 認証取得後の活動について

Our activities after the ISMS certificated

佐野雅彦†，上田哲史†
Masahiko SANO†, Tetsushi Ueta†

sano@tokushima-u.ac.jp, ueta@tokushima-u.ac.jp

†徳島大学情報化推進センター

† The Center for Administration of Information Technology, The University of Tokushima

概要

情報化推進センターは，平成 24 年 3 月に情報セキュリティマネジメントシステム（ISMS）を取得した．これは，我々が管理・運用する情報システムを，適切に運用するための活動及び体制を国際標準規格の下で確立するプロジェクトであった．ISMS を取得した時点では，その物理的な適用範囲は情報化推進センター棟に限定しており，本来含めるべき情報化推進センター蔵本分室を適用外としていた．今回，適用外としていた蔵本分室を適用範囲に含めるため, ISMS の変更審査を受審（変更審査は 9 月）するため活動を行ったので，その事例を紹介する．

キーワード：

ISMS，変更審査，事例紹介

1. はじめに

徳島大学情報化推進センターは，平成 22 年 7 月に，学内の情報化推進をより強力に支援するため，高度情報化基盤センターから改組された．改組後の大きなミッションとして，コンピュータシステムの更新（平成 24 年 3 月稼働）と，センターか管理する情報システムを適切に運用するための仕組みの再構築があった．とくに後者のミッションは ISMS の仕組みに類似する部分が多く，このミッションのアウトプットとして ISMS の取得を行うこととなった [1].

平成 23 年 5 月に ISMS 取得活動を開始した際には，常三島地区の情報化推進センター棟および蔵本地区の情報化推進センター蔵本分室（附属図書館蔵本分館内）を ISMS の物理的な適用範囲として準備を進めてきたが，附属図書館蔵本分館が改修工事中（平成 23 年 9 月～平成 24 年 5 月）であったため，議論の末，ISMS 取得時点（登録日は 2012 年 3 月 9 日）ではこれを適用範囲外とし，改修工事後にその適用範囲を変更することより，本来の対象範囲に含めることとした．平成 24 年 3 月には ISMS（ISO/IEC 27001:2005・JIS Q 27001:2006）を取得した．

本稿では, ISMS 取得後半年余りで ISMS の適用範囲変更（拡大）を行った，我々の活動事例を紹介する．

2. ISMS 取得後

平成 24 年 1 月の ISMS 本審査受審後，平成 23 年度末までは，マネジメントレビュー結果による是正項目への対応と本審査結果への対応が主であった．とくに，マネジメントレビュー結果からの是正項目「マニュアル等の整備不足」は，これまでの属人的なセンター運用体制から業務マニュアルによる組織的運用体制への移行を図るうえで重要な課題であった．しかし，同時進行していた「情報化推進センターコンピュータシステム」更新プロジェクトが導入段階に入っており，新システム用の業務マニュアルが次々と必要になり，業者作成分 170 を含む 250 超のマニュアル（7 月末時点）を整備する結果となった．加えて平成 24 年 4 月には，ISMS 構築チームの主要メンバー5 名中 3 名が移動となり，大幅なリソース減となった．これらのため，従来システムに対するマニュアル整備は進まず，新システム稼働の喧騒が一段落（6 月以降）してからの取組となり，本来予定していた 4 月末

から遅れる結果となった.

ISMS 取得までは，ある意味，「ISMS とるぞー，おぉー」的な勢いにまかせた面があり，短期間で ISMS を取得できたはいいが，本当の苦労はこれからという事態がまさに具現された状態である．この状況下で，以降に述べる適用範囲変更を行った（本稿執筆時点では変更審査受審前）.

3. 適用範囲変更のための活動

冒頭部で述べたように, 本センター蔵本分室は ISMS 取得後に変更審査により適用範囲に含める方針のため，平成24年5月に審査機関と連絡をとり変更手続きのための前準備に入った（定期審査の時に行う選択肢もあった）. 本学の場合，ISMS の認定範囲の変更には審査機関側に変更届を提出し，変更届から 3 か月以内に変更審査を受審する手順であることから，前述の是正事項の対応も含め，9 月上旬の受審とし，6 月上旬に変更届を提出した.

適用範囲変更のための作業は, ISMS の PDCA サイクルを P（計画）から開始することと言える．これは，JISQ27001:2006, 4.2.1 ISMS の確立 a)で規定される，「ISMS の適用範囲及び境界を定義する」[2] に該当するためである．この P（計画）においては，図-1 に示すように，適用範囲及び境界の変更により洗い出される新たな情報資産のリスクアセスメント，リスク対応のための管理目的及び管理策の選択という流れを経て，D（実行）サイクルへ移行する.

今回の適用範囲変更では, 図-1 に示す ISMS 基本方針やリスクアセスメントに対する組織の取組み方には変更を加えなかった（必要性がないと判断した）ため，実質的には新たな適用範囲及び境界の策定，情報資産の洗い出し，脅威の洗い出し，リスク評価といった P の残る部分についての作業を行った．また，蔵本分室で提供されるサービスも認定済みの範囲で提供しているものと同じであるため，サービス上の変化はない．よって，適用宣言書自体には変更は生じなかったが，各種規定類，下位手順書・マニュアル等は該当部分を変更している.

3.1. リスクアセスメント

情報化推進センター蔵本分室は，図-2 に示す 2 部屋構造であり，入口手前から，受付・執務室，NW 室として運用されてきた．予備的なリスクアセスメント行ったところ，受付領域，執務領域の分離が必要と判断したが，しかし予算と住環境悪化の問題から，境界の明示と簡易パーテーションによる分離とした．その際，受付領域は一般人が立ち入る領域であるが，執務領域，NW 室は職員あるいは特別に許可された場合のみの立ち入りを許可するリスク対応策とした．そのほかいくつかの対策を事前に行い，ある程度対応済みとなった時点で，ISMS 手順に従ったリスクアセスメントを実施し，問題点が小さくなるように配慮した．なお，確認された問題点は是正あるいは予防措置として対処する計画としている．余談であるが, 蔵本地区は電源事情が常三島地区より悪く（これもリスク), 時間帯による電圧変動幅が大きく±10%程度の変動は普通である．このため，蔵本分室には以前から AVR（交流定電圧電源装置）を介して UPS を接続している（リスク対応）.

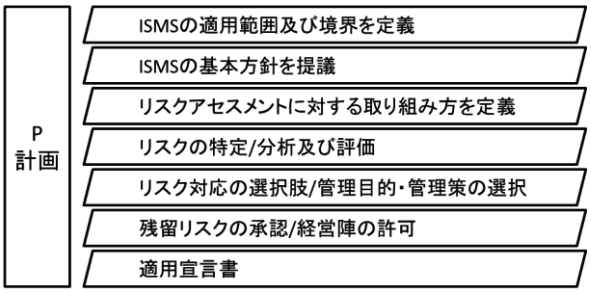

図-1　ISMS の Plan（計画）のフェイズ

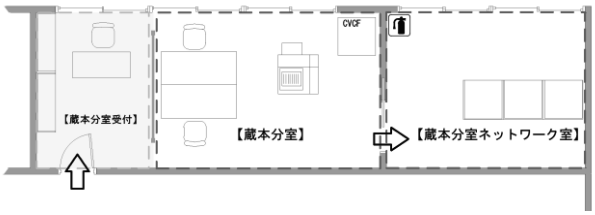

図-2　蔵本分室概略図

3.2. 内部監査ほか

内部監査は 7 月 9 日から 13 日の間で実施された. これはヒアリングと実施確認を主体とするもので，今回は適用宣言書の管理策実施状況の確認を中心に行われた．蔵本分室に関する内部監査からの指摘事項は，入退出管理の記録不備や業務記録の不備が主であった．今後，マネジメントレビューを経て，改善プロセスに取り組む.

4. おわりに

本稿では，ISMS 取得後の活動のうち，ISMS の適用範囲変更の例を取り上げた．これは ISMS の PDCA の P からサイクルを回すことに他ならない．幸い認定取得時の経験から，人的リソースが大幅に削減された現在の状態でも，短期間で PDCA サイクルを一巡することが可能になったと思われる．あとは 9 月の変更審査待ちである.

参考文献

1) “組織評価と ISMS,” 情報処理学会研究会報告, Vol. 2012-IOT-16 No.41.
2) “JIS Q 27001:2006,” 日本規格協会.