学術情報処理研究
No.18 2014 pp.90–98

徳島大学情報センターにおける ISMS の効果

Effects of ISMS on the Center for Administration of Information Technology, Tokushima University

佐野雅彦†，八木香奈枝†，上田哲史†

Masahiko SANO†,Kanae YAGI†, Tetsushi UETA†

sano@ipc2.tokushima-u.ac.jp, yagi@ipc2.tokushima-u.ac.jp, ueta@tokushima-u.ac.jp

†徳島大学情報センター

† The Center for Administration of Information Technology, Tokushima University

概要

徳島大学情報センターでは，平成 24 年 3 月に国立大学法人内の組織としては 4 番目に ISMS 認証を取得した．ISMS 認証は情報セキュリティマネジメントの国際標準として知られており，国内の多数の組織が取得している．また，ISMS は情報セキュリティポリシーを運用する仕組みとしても効果的である．本センターは ISMS 構築後約 3 年経過したことから本センターにおける ISMS の効果について検証と考察を行った．その結果，本センターの ISMS 導入および運用の効果が確認された．本論文ではその詳細について述べる．

キーワード

ISMS, 効果，運用事例

1. はじめに

組織の情報セキュリティ対策として情報セキュリティポリシーを策定し運用することは現代社会では不可欠である．平成 25 年の文部科学省の調査結果[1]では，国立大学法人では 100%，公立，私立大学全て含めると 67%，平成 24 年の経済産業省の調査結果[2]では有効回答数の 57%の民間企業が策定済みとされており，約 6 割程度の組織で情報セキュリティポリシーが策定されている（本学は平成 16 年に策定済み）．

情報セキュリティポリシーは継続的改善を含む適切な運用と運用状況の監視および監視結果からの改善が不可欠であり，このような活動の繰り返しにより，組織の現状に適したポリシーとしてその有効性の維持あるいは向上を図ることが可能となる．

情報セキュリティ対策や情報セキュリティポリシーの構築や運用に関する仕組みは，情報セキュリティマネジメントシステム（**I**nformation **S**ecurity **M**anagement **S**ystem 以下 ISMS）として知られており，その国際標準として ISO/IEC 27000 シリーズの規格がある．その中核となる ISO/IEC 27001 は ISMS の構築とその運用に重点が置かれており，ISMS の確立，導入，運用，監視，レビュー，維持及び改善するためのモデルとして提供されている[3]．ISMS 認証は，第三者である ISMS 認証機関が審査対象組織の ISMS が ISO/IEC 27001 の規格要求事項に適合していることを評価する，第三者適合性評価制度である．

徳島大学情報センター（平成 26 年度より情報化推進センターから改組）では，平成 24 年 3 月に国立大学法人内の組織としては 4 番目に ISMS 規格（ISO/IEC 27001:2005 / JIS Q 27001:2006，以下 ISMS 規格）の認証を取得した．この主たる理由は，高度情報化推進センターから情報化推進センターへの改組の成果として，情報システムや情報セキュリティに対する本センターの管理運用体制が良くなったことを学内外の利害関係者に分かりやすい形で提示するためである[4]．事実，国際標準規格という所謂「お墨付き」は外部評価において好評価が得られている[5]．

ISMS 規格への準拠や ISMS 認証取得が国立大学法人やその情報系センターにもたらすメリットについては明らかではないが，本学を含め各大学の目指す方向性は似通っている[6]．しかし相違点も多く，各組織

の背景（組織文化）が反映されたISMSの構築といえる[7]. これら事例はISMS構築を目指す組織における大きな判断材料となる.

本論文では，国立大学法人におけるISMSの事例の一つとして本センターにおけるISMSの効果について，ISMS導入と運用状況を検証し，評価と考察を述べる．続く2章では本センターのISMSの導入，3章では運用状況，4章ではその評価，5章では本センターにおけるISMSの効果について考察，6章では今後の課題と展望について述べ，最後に7章で纏める.

2. ISMSの導入

2.1 ISMS導入理由

本センターにおけるISMSの導入背景には，研究主体のセンターからサービス主体のセンターへの方針転換および全学情報サービスへの関与の強化を求められたことにある．しかしながら，本センターの業務体制は属人的でかつ人員不足であり，他の要因も含め上記要求を満たせないことを外部評価により指摘された[5]. 我々は，これを改善する取組みとして，外部コンサルタントの協力により運用業務を 4 つの視点（システム運用管理，正常確認管理，障害運用管理，システム保全管理）で作業分解し，運用業務プロセスを再設計する業務改善プロジェクトを立ち上げた. このプロジェクトでは，属人的業務からの脱却を図り，学内に対してセンターの評価を向上させる目的があった．なお，運用業務における人員不足については，最終的にSE4名を補充する体制で対応している.

この業務改善プロジェクトの推進において，管理するサービスや情報資産の洗い出し，運用手順の明確化・作成など作業はISMSの管理策を支える下位作業手順の構築でもあることに気づいた我々は，改革の目に見えるアウトカムの一つとしてISMS認証を取得することとした.

2.2 ISMSの構築プロセス

ISMS 認証取得プロジェクトは平成 23 年度中に認証取得することを目標に，平成23年5月から開始した．同10月の書類審査，同11月の予備審査を経て翌平成24年1月の本審査で合格し，平成24年3月に登録証が発行された. 実質8ヶ月半のプロジェクトであった．このISMS認証取得プロジェクトは前節で述べた本センター内の業務改善プロジェクトと並行して実施した.

我々の ISMS 構築では，ISMS 関係の文書は ISMS 認証取得プロジェクトで作成し，ISMS で特定した管理策の下位手順・マニュアル関係を業務改善プロジェクトでカバーする形でISMS構築プロセスを進行させた．幸い，業務改善プロジェクトにおいてその途中からISMSを考慮することは，文書管理以外は比較的容易であった．文書管理については残念ながらISMS関係文書と運用業務系文書が異なる管理となった.

我々の ISMS 構築プロセスは ISMS 規格の「4.2.1 ISMSの確立」に従って実施した．具体的には，文献[10]に解説されている 10 ステップから構成された手法を適用した．なお，我々はISMSの構築においてコンサルタントは導入しなかった．これは，我々が徳島大学情報セキュリティポリシーを策定する際に，ISMSについて検討した経験[8]があったことと，業務改善プロジェクトで既に外部コンサルタントを導入していため，経費面から困難と判断したためである．また，ISMS構築の期間短縮のため市販テンプレートを購入して参考とした（当時，山口大学で開発中のISMS 構築テンプレート[11]も検討したが，採用にはならなかった）.

本センターのISMS認証範囲は表1に示すとおり取得時から2回変更している（組織については3.4節に記載）. ISMS認証ではその対象範囲を組織の事情に合わせて設定できる．これは，同様の情報セキュリティに関する規格JISQ15001（プライバシーマーク）とは異なり，スモールスタートによりISMS運用を開始し，ISMS運用の経験を積み，その後対象範囲を拡大する方法を選択できることを意味する．本センターでも，取得時はセンター棟がある建物のみを物理的範囲とし，その後，分室を加えて対象サービス範囲を拡大する手法を採用している.

ISMS構築時のリスクアセスメントには，静岡大学のマインドマップを用いた手法 [9]を参考に，ベースラインアプローチ[10]的な手法を採用した（認証取得後は，詳細リスク分析手法に順次移行）．このリスクアセスメントの結果，本センターのISMSでは，ISMS規格の付属書 A の 133 の管理策から，電子商取引関係を除いた131の管理策を選択している. 各管理策では業務改善プロジェクトにおいて策定されたマニュアル類を下位手順書として参照している.

ISMS 文書の構築には，ISMS 文書を一つの文書として文書管理を簡素化する静岡大学の例[9]があるが，本センターでは表2に示す文書群で構成している. また，下位手順書となる業務改善プロジェクトで策定した手順/台帳/様式等はおよそ 250 程度ある．ISMS 構築前の本センターは属人的な運用体制であったため，明確に文書化された手順書は少なく，ISMSの要求事項を満たすために多くの手順書を策定する必要があった．事実，審査機関による書類審査では，74件もの問題点を指摘[5]された．その内訳は，ISMS規格本文に関して26件，付属書 A の管理策に関して48件であった．前者はISMSのPDCに関係する部分（A を

含まない）に該当し，後者は業務改善プロジェクトでは想定していなかったものが主であった．上記問題点は，担当者および関係者を総動員して対応し，本審査までに改善した．この対応内容を ISMS 運用の一部として記録しておいたところ，本審査時には良い方向に作用したと思われる．

2.3 ISMS 運用・評価・改善プロセス

ISMS 認証の取得には ISMS の PDCA サイクルが少なくとも一巡している必要がある．ISMS の運用（Do）は ISMS の構築 (Plan)において選択/導入した管理策に従って運用することである．本センターの場合，管理策は業務改善プロジェクトで策定した手順書やマニュアルを下位手順書として運用される．

ISMS 規格では，ISMS 構築時に選択/導入した管理策の有効性を測定して評価（Check）しなければならない．管理策の有効性測定方法は ISMS の構築時に予め定めておく必要がある．しかし，本センターには既存の有効性測定の仕組みはなく，購入したテンプレートを参考に業務改善プロジェクトの成果を踏まえて有効性測定を行うものとした．この有効性測定では定量的評価を主としているが，定性的評価となる場合においては内部監査の結果を用いて評価を行っている．逆に，有効性測定結果を ISMS 内部監査の情報としても利用している．

ISMS の内部監査には内部監査用チェックシートを予め策定しておき，表 2 に示す内部監査管理規定に基づいて実施する．このチェックシートは ISMS 規格の要求事項から抽出した 173 項目，選択した 131 の管理策から抽出した 130 項目，合計 303 項目のチェック項目（質問事項等）で構成されている．前者は主として ISMS 推進責任者や経営陣を対象とし，後者は部門等責任者を対象としている．内部監査により明らかになった問題点（不適合等）は是正処置や予防措置あるいはリスク対応として発生した場所に改善要求される．これら内部監査で指摘された事項は次回内部監査で必ずチェック対象に含め，内部監査結果のフォローアップができるように工夫している．なお，ISMS 運用初期の内部監査では，外部経験者を監査リーダとして内部監査を実施した．センター教職員 2 名の ISMS 内部監査研修受講後は，前述の 2 名を含む 4 名によるセンター内での相互監査方式としている．

ISMS 構築当初は内部監査と管理策の有効性評価は年 1 回であったが，ISMS 認証審査において有効性評価を年 1 回とすることの妥当性について意見が出された．このため，現在では年 2 回の管理策の有効性評価と内部監査を実施している．ただし，年 1 回で十分と判断される事項は実施時期を考慮しながら分散化している．

マネジメントレビュー（以下 MR）は，上記結果や是正処置，予防処置，リスク対応等様々な情報をインプットとして経営陣（本センターではセンター長）のレビューを受け，新たな方針をアウトプットするプロセスである．ISMS ではこの MR は重要である．

改善プロセスでは，MR のアウトプットや是正処置，予防処置等を元に改善処置を実施する．また，これらの結果は次の PDCA サイクルの P（計画）へ入力され，ISMS が期待する PDCA サイクルの循環となる．

表 1 ISMS の適用範囲の変化

審査種類（時期）	ISMS 適用範囲/所在/人員数
認証審査（H24.1）	徳島大学キャンパス情報ネットワークの管理運用ならびに各種全学情報システムの運用支援 / 情報化推進センター棟 / 15 名
変更審査（H24.9）	同上 / 情報化推進センター棟，蔵本分室 / 同上
定期審査 変更審査（H25.1）	全学情報ネットワークシステムの運用管理，ハウジング・ホスティングシステムの運用管理，教育用システムの運用管理及び専門技術アドバイスサービス / 同上 / 同上

表 2 策定した主要な ISMS 文書と関連文書

ISMS 規定文書：22
COM-B01 文書管理規程
COM-B02 是正処置管理規
COM-B03 予防処置管理規程
COM-B04 内部監査管理規程
ISMS-A01 情報セキュリティ基本方針書
ISMS-A02 ISMS マニュアル
ISMS-B05 教育・研修管理規程
ISMS-B06 リスクアセスメント管理規程
ISMS-B07 情報セキュリティ運営管理規程
ISMS-B08 人的セキュリティ管理規程
ISMS-B09 セキュリティ事件・事故管理規程
ISMS-B10 物理的・環境的管理規程
ISMS-B11 通信・運用管理規程
ISMS-B12 アクセス管理規程
ISMS-B13 システムの開発および保守管理規程
ISMS-B14 適合性管理規程
ISMS-B15 事業継続管理規程
ISMS-B16 管理策有効性評価管理規程
ISMS-C02 監視・見直し手順書
ISMS-C02 マネジメントレビュー手順書
ISMS-C06 リスク対応計画手順
ISMS-C09 セキュリティ事件・事故手順
上記に関連する台帳等：48
業務に関する文書/台帳/様式等：246

3. ISMS の運用状況

3.1 運用状況

本センターの ISMS の運用状況について述べる．ISMS の運用開始は平成 23 年 10 月からであり，現時点(平成 26 年 7 月)で 6 周期目の PDCA 運用である．

認証取得 1 年目（2, 3 周期）では，ISMS 認証取得時における残課題への対応や表 1 で示した ISMS 適用範囲の拡大などがあったが，とにかく PDCA サイクルを回すことを主目的とした活動期間であった．このため，内部監査において不適合事項が相当数あった．これは，ISMS 取得前の運用期間が短く，業務改善プロジェクトで策定した業務フローや手順の問題点の洗い出しが不十分であったことが原因である．そして ISMS 認証取得後に実質的な ISMS 運用が行われた結果，様々な問題点が表面化したといえる（詳細は文献[12]を参照）．なお，取得後 1 年経過時点での定期審査では，「ISMS は運用され維持されております」との評価であった．

認証取得 2 年目（4, 5 周期）では，1 年目に表面化した問題点を改善しつつ，ISMS の運用の質の向上を図った．1 年目の内部監査による指摘事項の原因を 5 種類（記録，報告，実行，手順，策定）に分類して根本原因の追究と改善を図った結果，2 年目の定期審査では「ISMS を維持し改善しています」との評価を受けることができた．図 1，図 2 にそれぞれ，内部監査の状況，有効性評価の状況をグラフで示す．累計事項は各監査対象で発生した指摘事項の累計である．分類事項は全ての指摘事項を管理策毎に分類して集計したものである．この結果から見ると，1 年目よりも 2 年目が改善されていることが確認できる．図 1-1 では，1 年目から 2 年目にかけて不適合（軽）が改善して減少している．一方，観察事項は増加している．これは不適合事項が改善により観察状態に移行したケースがあったためである．観察となった理由は改善策の効果確認に時間を要したためである．図 1-2 は上記指摘事項を管理策毎に 5 種類の原因分類毎に計数したグラフである．このグラフからは，手順（手順の実行不備）以外は改善されていることが確認できる．

運用 3 年目では，平成 25 年度末の BCP 対応による情報資産の刷新と平成 26 年度に実施した改組を踏まえ，ISMS を維持しながら本年度実施する ISMS 認証の更新と新規格への対応を予定している．

上記 BCP 対応では，東南海地震による津波を想定した可用性向上を図ったキャンパス間 NW，主要サーバを収容するための仮想化基盤群，およびキャンパス間 NW が機能喪失した際の広域無線/衛星無線から構成されるシステムを構築・導入した．また，平成 26 年度の改組は，情報マネジメント室，情報基盤・セキュリティ室，ICT 推進室の 3 室で構成していた本センターの内部組織を，情報統括部門，ICT サービス部門として再編し，新たに事務組織を事務室として加えたものである．

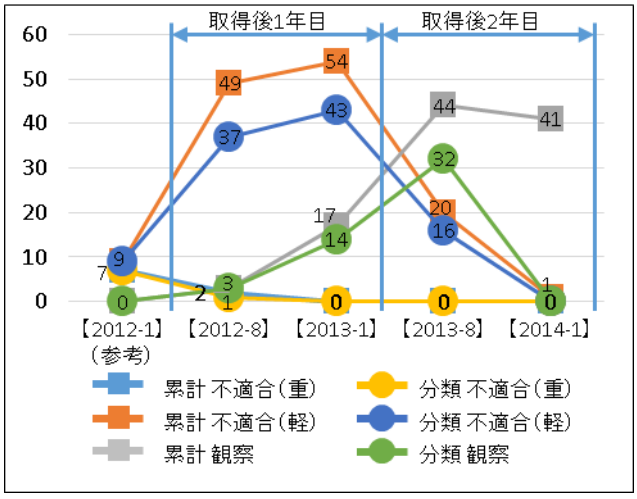

図 1-1 ISMS の運用状況（内部監査の指摘累計数）

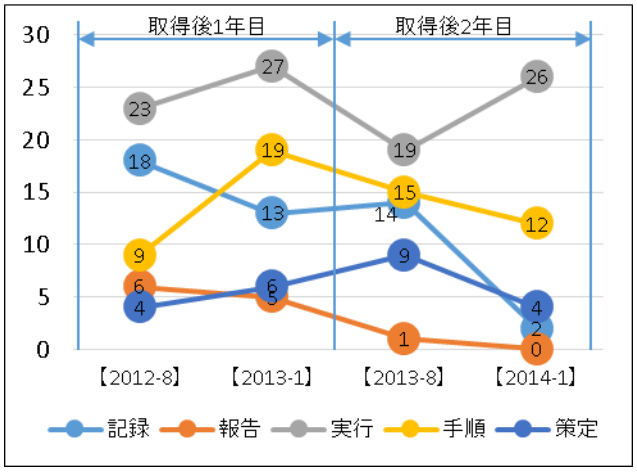

図 1-2 ISMS の運用状況（内部監査の分類別指摘数）

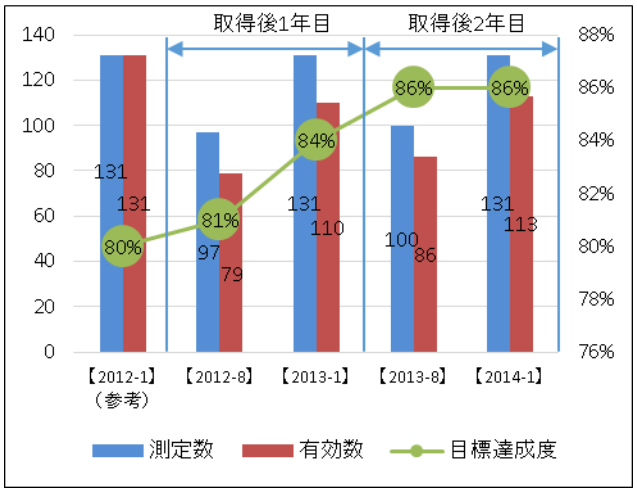

図 2 ISMS の運用状況（有効性評価）

3.2 合理化・省力化

ISMS の運用は通常の業務に加えて規格要求事項の手順が増えるため確実に業務増となる．ISMS では運

用記録が重要であるが，これら記録の作成に手間がかかると通常業務を圧迫し，結果として，記録不十分でISMS 規格の要求事項を満たさなくなる．本センターでは，2.1 節で述べた業務改善プロジェクトにおいて業務を明確化し，通常の業務記録・報告が実施されるように業務フローを設計・実装した．しかし実運用における業務記録の負担は大きく，記録不十分となり，内部監査において手順未実施あるいは記録不十分との指摘となった[12]．このことは，2.1 節で述べた目的の達成が不十分であることを意味した．

上記指摘の改善策として，まず，最も業務頻度が高い受付管理（受付番号の発行を含む）と作業記録管理を省力化するツールを Microsoft ACCESS を用いて作成した．これにより管理番号発行と記録入力の手間は大きく改善され，図 1-2 に示すとおり，記録に関する指摘は減少した．次に，運用業務における各種管理台帳のうち，頻繁に利用するものを ACCESS 上に順次構築し，情報共有のための省力化を図った．表 3 は現時点で ACCESS 上に構築している業務管理のツール及び台帳類である．このようにして，本センターでは実運用業務に ISMS が要求する事項を組み込み，ツール類を活用して合理化・省力化することにより，ISMS の運用が可能となった．

以上のことから，通常業務に ISMS の要求事項を埋め込み一体化した状態において，ツール類による合理化・省力化が本センターの ISMS の運用に有効であることが確認できた．

一方，ISMS 規格本文の運用は，記録や台帳などの共有すべき対象範囲が狭いことから，現時点では合理化・省力化が進んでいない．ただし，情報資産のリスクアセスメントや是正処置/予防処置等についてはツール類の導入あるいは構築が必要と考えている．

ツール類を用いた合理化・省力化以外には，業務そのもの見直しが効果的である．幸い ISMS では，ISMS 構築時に業務を可視化（業務フローを明確化）し，ISMS 運用にて定期的に見直す機会があるため，業務フローや業務そのものを合理化・省力化しやすい環境にある．本センターでも，コールセンターの受付フローや障害対応フロー等，運用業務を中心とした業務フローや手順の改善が実施された．

3.3 関連業務

本センターの ISMS に関連した業務を以下に示す．

（1）大学の情報セキュリティポリシーの運用

本学の情報セキュリティポリシーに本センターの ISMS の経験を反映している．これは，セキュリティポリシー本体や手順の策定・更新のほか，情報セキュリティポリシーの内部監査におけるチェックシートや実施方法（助言型内部監査など）についても ISMS の運用経験を反映している．逆に本大学の情報セキュリティポリシーの運用から得られた情報も本センターの ISMS へ反映している．

（2）利用者教育

ISMS には利用者教育が含まれる．本センターでは，学内貢献を踏まえ，新入生に「情報科学」の講義の一部を利用して情報セキュリティに関する導入教育を実施している．また，新入生以外の学内利用者にはセミナーを開催することで利用者教育としている．

（3）部局管理者の支援

本学では情報セキュリティポリシーに従い部局毎に情報セキュリティ管理者を設置している．この管理者の支援において，ISMS 運用で得られた経験を活用している．

3.4 センター組織

ISMS 認証取得時（平成 24 年 1 月），本センターは表 4-1 の人員で構成され，ISMS 適用範囲中（表中の灰色部分），他組織との兼務者 3 名（センター長，副センター長）を除くと実員 12 名の体制であった．ISMS の構築・運用は情報基盤・セキュリティ室 2 名が主担当で行い作業補助を他の室で分担した．ISMS 構築後は情報基盤・セキュリティ室が ISMS 推進責任者を兼務して ISMS を運用している．なお，本センターでは特定 ISMS 事務局を設置しておらず，ISMS 推進責任者が各室に業務を分散している．表 4-2 は平成 26 年 4 月に改組した現在の人員構成である．この改組後，情報統括部門の教員 1 名と技術職員 1 名で ISMS の運用を行っている．なお，ISMS 構築及び運用における人員割当ては表 4-3 に示すとおりである．

表 3 本センターで作成した省力化ツール類

受付履歴管理（記録/管理番号発生/TODO 管理）
作業記録管理（記録/管理番号発生/TODO 管理）
ハードウエア管理台帳 / ソフトウエア管理台帳 IP アドレス管理台帳 / ライセンス管理台帳 文書管理台帳 / ML 管理台帳

表 4-1　平成 24 年 1 月の人員構成

部署名等 （ISMS 適用範囲 15 名）	人員内訳*						
	専教	兼教	技職	技補	SE	事務	事補
センター長		1					
副センター長		1				1	
情報マネジメント室	1				2		
情報基盤・セキュリティ室	2					1	
ICT 推進室	2		1	2	2	2	

（*専教：専任教員，兼教：兼任教員，技職：技術職員，技補：技術補佐員，SE：派遣 SE，事務：事務職員，事補：事務補佐員）灰色部分が ISMS 適用範囲，事務職員はセンターに兼務

表 4-2　平成 26 年 4 月の人員構成

部署名等（ISMS 適用範囲 18 名）	人員内訳*						
	専教	兼教	技職	技補	SE	事務	事補
センター長	1						
情報統括部門	2		1				
ICT サービス部門	2			2	5		
事務室						3	2

（*専教：専任教員，兼教：兼任教員，技職：技術職員，技補：技術補佐員，SE：派遣 SE，事務：事務職員，事補：事務補佐員）灰色部分が ISMS 適用範囲

表 4-3 ISMS 構築時/運用時の人員割り当て

	専教 A	専教 B	技職	SE 2 名
ISMS 構築時（H24.1 時点）				
・ ISMS 規定構築				
ISMS 規定策定	◎	○		
下位規定整合調整	○	◎	△	△
・ 関連業務手順構築				
業務フロー/手順策定（業務改善 PJ）		◎	○	○
ISMS 運用（H26.4 時点）				
・ ISMS 本体運用		◎	○	

◎:主担当．○補助．△必要時補助

専教:専任教員，技職:技術職員，SE:派遣 SE

4. 評価

4.1 ISMS 運用経費

ISMS の運用に要した経費を項目で表 5 に示す．表 5 では ISMS 認証取得及び維持等の直接的経費と ISMS の規格要求事項を満たすために要した間接的経費に分けて記載した．なお，これらの経費にはセンター教職員の人件費は含まない．

（1）直接的経費

直接的経費は ISMS 認証を取得・維持するために不可欠である．本センターでは，定期審査時期以外に適用範囲拡大を 1 回実施したため，余分な経費が発生している．定期審査時に適用範囲変更を実施した場合では登録証再発行等の費用が発生するが，変更審査を実施するよりは低く抑えることができる．加えて，本センターではまだ実施していないが，ISMS 認証の更新（ISMS 認証の有効期限は 3 年間）や規格変更に伴う移行がある．一度 ISMS のノウハウを得た後，ISMS 認証を更新しない方法も考えられるが，定期的な外部審査という要求は組織内の ISMS の形骸化防止に最も効果が期待できる．本センターでは直接的経費は予算化しており，ISMS 認証取得/更新時を除き，審査 1 回あたり 50 万程度を想定している．

（2）間接的経費

直接的経費ほど明確ではない．これは，ISMS の要求事項を通常業務に組み込んでいるため，明確な分離が困難なことが理由である．表 5 では主に情報セキュリティの向上や ISMS 運用（関連する実業務を含む）の改善に関係したものを記載している．たとえば表中の「入退出管理」は，ISMS 規格の A.9.1 で要求されるが，情報セキュリティを考慮すれば自明であり，対応前では問題があった箇所あるいは見過ごしていた箇所である．よって，ISMS 規格の要求事項でもあるが実運用としても必要な事項であるといえる．また，本センターで開発したツール類も，主として実運用業務を合理化・省力化するためのものであるが，結果として ISMS 運用に寄与している．これらのことから，間接的経費は組織が導入する管理策とその基準により異なるといえる．

表 5 ISMS 運用及び関連する経費の項目

直接的経費
ISMS 認証取得及び維持費等
・ISMS 認証取得費用（予備審査等含む）（H24.3）
・ISMS 変更審査費用（H24.9）
・ISMS 定期審査費用（取得後 1 年目）（H25.1）
・ISMS 定期審査費用（取得後 2 年目）（H26.1）
適用範囲変更（サービス拡大）
・ISMS 更新審査費用（予定）
・ISMS 移行審査費用（予定）
ISMS 研修費等
・ISMS 一般研修（4 名）（H23/H24 各 2 名）
・ISMS 内部監査研修（2 名）（H24/H25 各 1 名）
・ISMS 新規格移行研修（1 名）（H25）

間接的経費
業務改善プロジェクト経費
・外部コンサルタント及び SE2 名（H23 年度）
物理的・環境的セキュリティ改善
・防犯ガラス，受付シャッター設置（H24/H25 年度）
・入退出管理（IC カード管理）設置（H24/H25 年度）
・監視カメラ増設設置（H25 年度）
通信・運用管理改善
・監視用大型ディスプレイ設置（H25 年度）

前述した直接的経費および間接的経費に関係するセンター内の人的労力は，ISMS 構築期間中（5 ヶ月間）では情報基盤・セキュリティ室の教員 2 名が作業の中心（表 4-3 参照）であり，その教員の業務の 3 割

から 4 割を占めている．これは，教育や研究その他を除くと殆どが ISMS 構築に要していることになる．コンサルタントを導入することで負担を減らすことは可能であるが，実効的な ISMS の構築には，経験上，相当の関与が必要と推測する．一方，ISMS の管理策を支える実運用業務については，業務改善プロジェクトにおいて SE2 名とコンサルタントを導入した．これは間接的経費に含めている．

ISMS 構築後は，管理策の有効性評価のための作業や ISMS 本体を運用（委員会，有効性評価，内部監査，MR，是正処置/予防処置/リスク対応，ISMS 認証維持など）のための人的労力が発生している．3.2 節で述べた合理化・省力化ツールは派遣 SE が業務の一部として開発・改変している．

4.2 業務可視化

ISMS の導入効果として業務の可視化がある．本センターでは，業務改善プロジェクトにおいて属人的運用からの脱却を目指しており，マニュアルや業務フローによる可視化は必須である．しかし，平成 23 年度に実施した業務改善プロジェクトでは，各種事象エスカレーションや決済フローまでは定義したが，運用業務全体のマネジメントプロセスまでは踏み込んでいなかった．我々はこの部分に ISMS のマネジメントプロセスを組み込むことで，本センターの運用業務フローを可視化した．このようにして可視化された事項は複数あるが，その例として，週次受付履歴数（コールセンター業務記録）を図 3-1，週次作業記録件数を図 3-2 のグラフにそれぞれ示す（期間は 2013.8 から 2014.6）．

このような業務の可視化は 3.2 節で述べたように，ツールによる効果が大きい．これは過去の記録の検索や未処理の抜き出しなどが簡単に行え，他の DB 化した管理台帳との連携も容易となることが理由である．ISMS 導入以前では，このような業務件数の把握は個人でメールや Excel による管理に留まり，全体像の把握は手間を要するかあるいは不明であった．このため，個人は目一杯業務を行っているが，センター全体では不明という状況となり，学内に対して本センターの貢献を具体的に示すことが困難であった．業務の可視化はこのような状況を防止する効果がある．

本センターでは，毎朝の会議で日々の様々な事項についての意見交換と情報共有を行っている（会議内容は CMS 上に記録）．また，毎週金曜日の朝の会議では週次の進捗管理も行っている．

これらの活動から，インシデントやアクシデント発生時の対応やその予防，潜在的リスクやセキュリティ違反の発見，作業進捗管理，間接的教育などの効果が得られた．

4.3 対外的効果

本センターにおける ISMS を導入したことによる対外的効果は，学内への効果と学外への効果に分かれる．

（1）学内への効果

大学の情報基盤を国際標準のマネジメントプロセスで管理していることによる安心，信頼感の向上がある．これには，本センターで提案する各種情報化施策に対する部局側の理解や，部局等への情報セキュリティ内部監査（情報セキュリティポリシーにおける内部監査であり，本センターは平成 24 年度から毎年 10 部局等を対象に 4 年で一巡する予定で助言型内部監査を実施）への理解などに効果があった．また，情報セキュリティマネジメントに関するアドバイス（その多くは助言型内部監査で行われる）も，本センターの ISMS 運用を実例として，より具体的に実施することが可能となった．加えて，ISO 規格の取得は学内の組織評価において評価対象となっている．

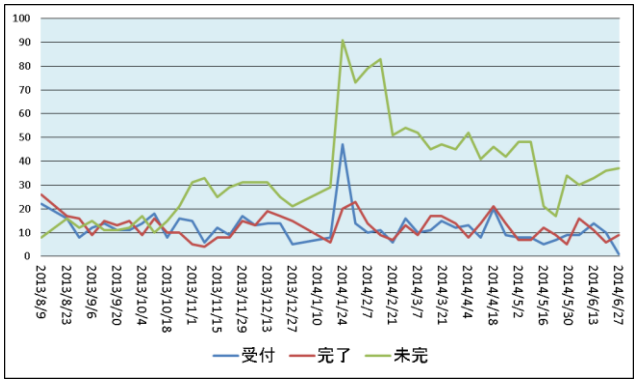

図 3-1 週次受付履歴数

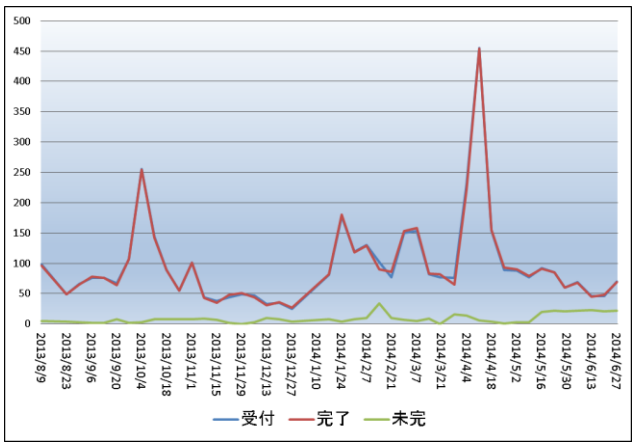

図 3-2 週次作業記録数

（2）学外への効果

まず，我々が ISMS 運用から得られた知識・経験により，業務に関係する外部業者の対応の妥当性を判断できるようになり，業者の言いなりになるケースが減ったことが挙げられる．例えば，業務データをクラウドに預けるとすると相手方にも ISMS や情報セキュリ

ティポリシーを要求することとなるが，相手方のそれらが妥当かどうかを判断できる知識と経験を有することができる．

次に，本センターでは実施していないが，BCP を考慮した組織間でバックアップデータの持ち合いやデータ連携した業務を行う際の，相手方に示す情報セキュリティに関する目安としての効果が期待できる．また，外部評価においても ISMS 認証は分かりやすい指標の一つとなり，好評価である[5].

5. 考察

3 章の運用状況および 4 章の評価を踏まえ，ISMS 導入の効果について考察する．

5.1 本センターにおける考察

（1）ISMS 導入のメリット

まず，別途実施していた業務改善プロジェクトの成果も含まれるが，運用業務の可視化により，以前の属人的な業務運用体制からの脱却が図れたことである．これには様々な効果があり，BCP における人的リスクを抑える効果や，4.2 節で述べた効果がある．とくに，情報共有度の向上により，セキュリティ事象の発生を早期に把握し，事件事故を未然に防ぐ可能性が向上した．

次に，ISMS 運用における定期的な見直しは，業務フローや運用手順を改善する機会となり，業務フローや運用手順の改善や合理化・省力化の効果があった．

また，組織評価や学内への説明および各種支援において効果があった．これに関連して，学内の情報セキュリティポリシー運用において，ISMS 運用経験のフィードバックや経験を踏まえた部局への支援が可能となった．これらにより，学内への貢献度が高まったといえる．

（2）ISMS 導入のデメリット

デメリットは端的に言えば ISMS 経費といえる．ISMS 認証を維持するための直接的経費は最低限の必要経費であるが，間接的経費は管理策やセキュリティ水準の設定により左右される．ISMS 運用に要する人的労力は確実に増加するため，ISMS 推進担当者や教育担当者などの業務負担は増加する．人員交代（移動）が少ない場合は良いが，交代が増えると，移動後の新人教育の手間が増加する．

4.3 節で述べた効果を考慮しない場合，ISMS 運用経費を下げることも可能であるが，ISMS 運用を形骸化させないためには，外部監査が別途必要と思われる．

（3）費用対効果

上記（1）および（2）によるが，本センターの場合，メリットがデメリットを上回っていると判断しており，費用対効果は妥当レベルであると判断している．なお，文献[13]では，2008 年における ISMS 取得事業者へのアンケート結果において，「半数が妥当と解答している一方，4 割強が高いと回答している」と報告されている．

5.2 他組織への適用に関する考察

本事例を参考に，他組織が ISMS 認証あるいは ISMS の構築・運用を行うことについて考察する．なお，ここでは ISMS の構築・運用を行うことと ISMS 認証取得とは別の事項として取り扱う．

ISMS 規格に準じた ISMS を構築する場合，それまでの業務（サービス）を明確にし，その業務手順を見直す必要がある．本センターの場合は 2.1 節で述べた理由から外部コンサルタントを導入して業務見直しを図り，その上で ISMS の規格要求事項の組み込みをおこなった．既に業務が可視化されている場合は ISMS 規格要求事を既存業務フローに旨く組み込むことになると推測する．この組み込みが旨くできるかどうかで，運用における実効性が変わると思われる．

ISMS 規格要求事項に該当する既存業務がない場合は新たな業務となる．例えば，ISMS の付属書 A の管理策は情報セキュリティを広範囲にカバーしているため，新たに業務が発生する場合がある．

ISMS は，スモールスタートが可能であるため，最小限の範囲で開始し，順次拡大する手段が選択できる．比較的固定された人員が配置でき，対象人員が少ない場合はこの手法が効果的と考える．本センターでは表 4-3 に示した様に特定人員を中心に構築した．

一方，人員移動が頻繁となる組織においては，時間をかけた構築は難しいと思われるため，費用を要するが，経験者やコンサルタントのアドバイスで既存業務の見直しを含め一気に構築するほうが得策と思われる．また，ISMS 運用時は ISMS 事務局を設置し，推進責任者や ISMS 担当者の負担を減らす工夫が必要である．

組織内で ISMS 内部監査を行う場合には．自身の業務を監査しないように割り当てをすることや，監査の要点を外部研修等で習得することが望ましい．なお，審査機関による定期審査結果をフィードバックすることで，経験上，一定の内部監査の質を確保できると判断している．

6. 課題と展望

本センターの ISMS の運用は，構築から 3 年経過した．ISMS 認証については，ISMS 認証の更新と ISMS の新規格(ISO/IEC27001:2013)への移行を予定している．この移行は ISMS 認証の更新時に新規格で更新す

ることも可能である. いずれにしても新規格発行から 2 年以内の移行が必要となる（旧規格は 2015 年 10 月に失効する）.

センター業務では，これまで，日常の運用業務を中心に合理化・省力化の改善を進めてきた．これは，ISMS 構築による業務の可視化と ISMS 構築・運用が契機となった合理化・省力化である．これらには，既に述べたように, ツール類の導入や業務フローの合理化および運用手順の改善による省力化が含まれる.

今後は, ワークフローシステムによる決済業務の効率化や各種管理台帳の DB 化による連携が課題である．とくに，ワークフローシステムの導入により稟議の決済など記録が自動的に保管されるので，ISMS 規格が要求する記録について意識しなくてもすむ. また, ISMS 本体の運用については，是正措置や予防処置の支援ツールや, リスクアセスメントの支援ツールの導入あるいは構築による効率化が課題である.

今後の展望としては, 本センターの ISMS 運用経験を学内にフィードバックし, 他の学内組織においても ISMS 認証の取得あるいは ISMS に準拠した運用体制の構築を支援し, 本学情報セキュリティポリシーの実質的な運用促進を図りたいと考える.

7. おわりに

本論文では, 国立大学法人徳島大学情報センターにおいて ISMS を導入した効果について述べた. 国立大学法人の情報系センターとしては，ISMS 認証を取得するメリットは一般企業等と比較すると小さいとされるが，業務の可視化や学内貢献，利害関係者との関係改善など様々な効果が確認された．また，5 章では本センターの事例を参考に他組織に展開することについても考察した. 費用対効果は本センターとしては妥当と判断しているが, これは各組織で判断が分かれるところである.

本センターは ISMS を構築して約 3 年となるが，改善すべき課題は多く，今後も PDCA サイクルの推進する必要がある．ISMS の PDCA は，運用業務における PDCA と関連しており, 両者が乖離して ISMS が形骸化しないように，実利のある ISMS 運用としたい.

最後に，本センターの ISMS 事例が参考になれば幸いである.

謝辞

本センターの ISMS 導入及び運用について，様々な意見・助言を頂きました各位に御礼申し上げます.

参考文献

[1] 平成 25 年度学術情報基盤実態調査: 文部科学省, 2014.3.25 公表

[2] 平成 23 年情報処理実態調査報告書: 経済産業省, 2012.7.18 公表

[3] 日本規格協会：JIS Q 27001:2006 (ISO/IEC 27001:2005)，日本工業標準調査会，2006

[4] 上田哲史, 佐野雅彦 : 徳島大学情報化推進センターにおける ISMS 構築について, 情報処理学会研究報告，Vol.2011-IOT-14, No.5, pp.1-2, 2011

[5] 上田哲史，佐野雅彦 : 組織評価と ISMS，情報処理学会研究報告，Vol.2012-IOT-16, No.41, pp.1-6, 2012

[6] 市川哲彦，上田哲史，長谷川孝博，三原義樹 : 事例紹介：情報系センターの情報セキュリティマネジメントシステムにおける事務系組織の役割, 情報処理学会研究報告，VOl.2012-IOT-16, No.40, pp.1-6, 2012

[7] 市川哲彦，永井好和，長谷川孝博，三池秀敏 : 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，情報処理学会研究報告，Vol.2009-IOT-6, No.6, pp.1-6, 2009

[8] 松浦健二，上田哲史，佐野雅彦，大恵俊一郎 : 大学における ISMS 準拠のセキュリティポリシ策定，信学技法，TM2004-11, pp.1-6, 2004

[9] 長谷川孝博，井上春樹，八巻直一 : ISMS 文書の低コストかつ高効率な管理運用手法，情報処理学会研究報告，Vol.2009-IOT-6, No.7, pp.1-6, 2009

[10] ISMS ユーザーズガイド-JISQ27001:2006，日本情報処理開発協会，2006

[11] 市川哲彦，小柏香穂理，永井好和，小河原加久し治：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，情報処理学会研究報告，Vol.2011-IOT-14, No.6, pp.1-6, 2011

[12] 佐野雅彦，八木香奈枝，上田哲史 : 徳島大学情報化推進センター ISMS 活動事例，学術情報処理研究集会発表論文集，No.17, pp.17-20, 2013

[13] 水沼彩子，澤近俊輔ほか : ISMS 認証取得及びその継続における課題と解決策について，情報処理学会研究報告，Vol.2009-CSEC-46, No.12, pp.1-8, 2009