金沢大学総合メディア基盤センターにおける ISMS

上杉喜彦 [1)]，佐藤正英 [1)]，笠原禎也 [1)]，大野浩之 [1)]，高田良宏 [1)]，井町智彦 [1)]，
森 祥寛 [1)]，東　昭孝 [1)]，Nakasan Chawanat[1)]，二木　恵 [1)]，濵　貴幸 [2)]，西川直樹 [2)]，
松平拓也 [2)]，松能誠仁 [2)]，富田　洋 [1)]

1) 金沢大学 総合メディア基盤センター
2) 金沢大学 総合技術部

mori4416@staff.kanazawa-u.ac.jp

ISMS on the Information Media Center, Kanazawa University

Yoshihiko Uesugi [1)], Masahide Sato [1)], Yoshiya Kasahara [1)], Hiroyuki Ohno [1)], Yoshihiro Takata [1)], Tomohiko Imachi [1)], Mori Yoshihiro [1)], Akitaka Higashi [1)], Chawanat Nakasan [1)], Megumi Futatsugi [1)], Takayuki Hama [2)], Naoki Nishikawa [2)], Takuya Matsuhira [2)], Nobuhito Matsuno [2)], Hiroshi Tomita [1)]

1) Information Media Center, Kanazawa University.
2) Engineering and Technology Department, Kanazawa University

概要

金沢大学総合メディア基盤センターは、2018 年 1 月に情報セキュリティに関する国際規格である JIS Q 27001（ISO/IEC 27001）に基づき、ISMS 認証を取得した。これによって質の高い情報セキュリティの維持と、その保証が可能となった。本稿では、国立大学法人の情報系センターにおける ISMS 取得に関する取組みの 1 つとして、金沢大学の例を紹介する。

1　はじめに

情報技術の発達と、あらゆるところに張り巡らされたネットワーク網の整備によって、今や、全世界で絶え間なく発生する情報セキュリティインシデントの報に接し続ける毎日となった。金沢大学総合メディア基盤センター（以下「本センター」という。）でも、金沢大学の情報系センターとして、金沢大学内のネットワーク整備やネットワークを利用したサービスを日々運用している。本センター構成員たちも、日々の工夫や、個人個人のもつ技量によって、問題が発生しないよう努めている。しかし、情報セキュリティインシデントは、思わぬ形で発生してしまう。その対応などを考えたとき、個人の力量に依存するだけでは、その場その場のインシデント対応はできても、「同じインシデントを繰り返し発生させないためにはどうしたら良いか？」「対応可能な人材を増やすにはどうしたら良いか？」「インシデント対応して解決したという成果をどのように記録に残したら良いか？」といった対応に限界がある。このような対応を行うには、より組織的な行動が必要という問題意識を持っていた。これは、多くの、さまざまな組織で共有できる意識であろう。

特に、国立大学法人の情報系センターである本センターが取扱う情報資産には、ネットワークやメールサービス、学内に設置されている共用パソコンなどの情報機器、果てはポータルサイトを始めとする金沢大学の各種サービスに関連するさまざまな情報などがある。それらの機密性、可用性、完全性の確保は極めて重要であり、組織として、質の高いセキュリティ状態の維持は、絶対に必要であるのだが、それを組織内部から内発的に改革

図 1　ISMS 認証取得した本センター入口

するだけでは限界があった。

そこで本センターでは、質の高いセキュリティを得て、それを客観的にセンター内外に示すため、情報セキュリティに関する国際規格である ISMS 認証を、本センターを適用範囲として取得することとした。この ISMS を本センター内に導入することは、セキュリティ全般に対する「考え方」を外部から取入れ、組織内部を自己改革させることと同義であり、導入にあたって、諸手を挙げての賛同が得られたわけではない。しかし、2016 年に ISMS を導入することを方針として定めたことから、本センター全体で動き出し、諸々の作業と認証を経て、本センターは、ISMS 認証を 2018 年 1 月 30 日に取得した。

この ISMS 認証には、2019 年 9 月 12 日現在、ISMS 認証を管理する情報マネジメントシステム認定センター[1]に登録されている「大学」と名がつく高等教育機関などの組織で調べると、本センターを含めて全部で 20 組織が登録されている。そのうち情報系センターが認証を取得しているのが 12 組織、学内の基幹ネットワークサービスに対して認証を取得しているのが 12 組織ある。最も早く登録されたのが静岡大学で 2003 年 11 月 25 日に初回登録、2012 年以降は毎年 1、2 件ずつ登録されている。なお、大学以外も含めると 5,956 組織が認証を取得しており、2002 年から登録されていることを踏まえると、素朴な計算をするなら 1 日 1 組織弱の登録がなされたことになる。

本稿では、全体から見れば、まだ取得数が少ない国立大学法人の情報系センターが、ISMS を取得するにあたって行った具体的な取組み内容について、本センターを例として紹介していく。

2 ISMS とは

ISMS（Information Security Management System、情報セキュリティマネジメントシステム）とは、国際標準化機構[2]によって定められた、情報セキュリティに関する国際規格「ISO/IEC 27001」[3]に基づいた仕組みである。日本では、ISO/IEC 27001 を受けて、JIS（日本産業規格）として「JIS Q 27001」にまとめられている[4]。一般に ISMS 認証を取得するとは、JIS Q 27001（ISO/IEC 27001）の規格に基づき、情報セキュリティに関する対応を組織的に正しくマネジメントしていることを ISMS 認証機関に毎年確認されていることを指す。規格の中では、

- ✓ 組織を適切にマネジメントして、国際規格に基づく確かでセキュアな組織を維持する。
- ✓ リスクアセスメントを自ら実施することで、組織を運用し、サービスを展開していくために必要なセキュリティレベルを自ら定義する。
- ✓ セキュアな組織を達成するためのセキュリティ対策プランを自ら構築する。
- ✓ 資源（人・もの・金）を配分し、組織が所有するシステムやサービスを適切に運用するとともに、継続的に改善する。

などの実施が求められている。ISMS では、これらを正しく適用することによって、セキュアな環境を維持し、リスクを適切に管理しているという信頼を利害関係者に与えることが可能となっている。同時に、組織自身が、規格に示されている情報セキュリティの要求事項を満たすだけの能力を有している客観的事実を内外に示すことができる。さらに、ISMS が要求する組織の適切なマネジメントを構築する過程で、属人的な業務の存在を明らかにし、できるだけそれを廃していく、そのきっかけを作ることができる。

3 ISMS 認証取得に向けての取組

ここからは、本センターが ISMS 認証取得に向けて実施してきた取組について述べる。ここでの内容は、本センター特有の状況を踏まえて、ISMS を実施するため

3.1 コンサルタントの活用

本センターが、ISMS を導入することを方針として定めたのは良いが、本センター職員（常勤・非常勤を問わず、本センターに所属する、もしくは本センター業務を所掌の範囲とする教員と事務職員で、ISMS の適用範囲内の者をまとめて「職員」という。以下、職員という用語は同意として使用する。）のほぼ全員が、ISMS 認証取得に向けて何をすべきか、右も左も分からない状態であった。そこで、認証取得に向けた各種支援を得るために「株式会社サン・パートナーズ[5]」と、ISMS 導入に向けたコンサルティング契約を結んだ。そのもとで、2016 年 11 月から本センター内に ISMS 認証取得のための組織を作り、JIS Q 27001（ISO/IEC 27001）に則った情報セキュリティマネジメントを実施するための体制整備とルール作成を行った。そして、

その体制とルールのもとで、コンサルタントの指導・助言を受けながら、ISMS に沿った運用を開始し、これは 2019 年 9 月 20 日現在も続いている。

3.2 ISMS のための文書作成作業

ISMS の特徴の一つが文書主義である。

ISMS の実施にあたっては、あらかじめ、従うべきルールを、JIS Q 27001（ISO/IEC 27001）の規格を満たすように、自分たちで確立する。このルールを確立するために、ISMS の適用範囲の活動について、その根拠となる文書類が、多数必要となる。ISMS に必要な文書類の内容は、JIS Q 27001（ISO/IEC 27001）の規格で厳密に定められている。その結果、作成する文書類は、種類、量ともに膨大になる。

本センターの場合は、コンサルタントから、JIS Q 27001（ISO/IEC 27001）の規格として、ISMS の要求事項を満たすマニュアルや管理策、記録類などの文書類のひな形を、コンサルティングの一環として提示された。本センター職員は、提示されたひな形をもとに、本センターで実現したい ISMS を、本センター特有の人的、組織的な特徴を踏まえて、文書類に追加・修正をしていった。その作業は、これから従うことになるルール（マニュアルや手順書など）や、推進組織などの体制構築も含まれている。

ひな形をもとにした文書作成以外にも、さまざまな関連・補足書類を作成した。中には、本センター職員毎に、署名をいれた誓約書や、本センターのシステム管理や機器管理などを行う関連業者からの契約書の締結や誓約書の提出などもある。

これらの文書類は、2019 年 9 月 19 日現在では、補足資料を含めて 87 種類あり、ISMS に従って適切に保存、管理している。

3.3 職員教育の実施

文書類を作成しただけでは、ISMS 認証を受けられない。文書類作成作業と併せて、その文書の内容を把握し、そこに書かれたとおり、正しく行動が行えるように、本センター職員に対する教育を逐次、実施しなくてはならない（どのタイミングで教育を実施するかも文書類に内容と合わせてまとめていく）。この教育によって、ISMS についての知識と、ISMS のために構築したルールについて学び、ルールに従った正しい行動ができるようにした。

教育は、当初、対面で行い、本センター全職員に受講させた。この教育は、入れ替わって本センターに新たに配属された職員だけでなく、毎年、継続して実施しなくてはならない。そこで、場所や時間を選ばず実施できるよう e ラーニング研修のための教材を用意し、それを使用して実施した。なお、この教育では、対面／e ラーニング問わず、簡単ではあるが、最後にテストを行い、職員が学んだことへの証拠とした。

また後述の内部監査を実施する内部監査員は、内部監査員研修を受講し、合格した者のみが担当できる。本センターでは、コンサルティング会社である株式会社サン・パートナーズが主催する役割別教育研修の内部監査員研修を、一部の本センター職員に受講してもらうことで、内部監査の資格者を増員していった。

4 「JIS Q 27001（ISO/IEC 27001）」に対応するための取組

ここで説明する内容は、前述の「3.2 ISMS のための文書作成作業」における文章作成作業の具体的内容の一部である。以下で説明する内容は、すべて文書として、まとめて記録、保存していかなくてはならない。JIS Q 27001（ISO/IEC 27001）では、文書類の書式自体は定めていないが、規格が要求する必要事項を過不足無く満たした文書類作成は大変難しいだろう。その点も含めて、コンサルティングを受けることは有効な手段といえる。

4.1 適用範囲と組織の状況の決定

ISMS の導入に際しては、ISMS で実施すべき取組や作業を、組織のプロセス及びマネジメント構造全体の一部として組み込み、その中で情報セキュリティを考慮することが重要である。従って、ISMS は、その組織のニーズと力量（対応可能な職員の人数や能力など）に合わせて、無理のない規模で行うことが期待されている。そのため、ISMS では、組織のマネジメント及び業務プロセスを、その周辺に取り巻くリスクと変化に対応させるように、守るべきものの境界と範囲を定め、これを適用範囲とする。この中で、組織として、自らのニーズ及び目的、情報セキュリティの要求事項、組織内で行われている業務プロセス、並びに組織

の規模及び構造を考慮して、最大限のセキュリティの確立及び実施を行っていく。適用範囲の決定は、組織として多くの情報を取扱う中で、守るべき組織マネジメントと業務プロセスを明確化でき、そのリスクや状況の変化などを有限化して適切に対応可能とする。

本センターではこのような ISMS の考え方を元に、適用範囲について「本センター全体を適用範囲とする。本センターの推進組織、関連するステークホルダーとセキュリティ上の役割・責任を明確にして、情報セキュリティの確立・向上及び継続的な改善を行う。」と定め、情報セキュリティ方針（図 2）に記載した。このような大枠での適用範囲の定め方が可能なのは、本センターが、金沢大学角間キャンパス内で独立した 2 階建ての建屋にあり、事務室、教員の研究室、システム、サービスともに建屋内にまとまっているためである。「本センター全体」という文言は、この金沢大学総合メディア基盤センターの建屋の内部全体を指している。ただし、教員の「教育」と「研究」に関しては、ISMS の管理下にするにはそぐわない点があるため、教員の研究室内については、他の部屋とは異なる形で適用している。

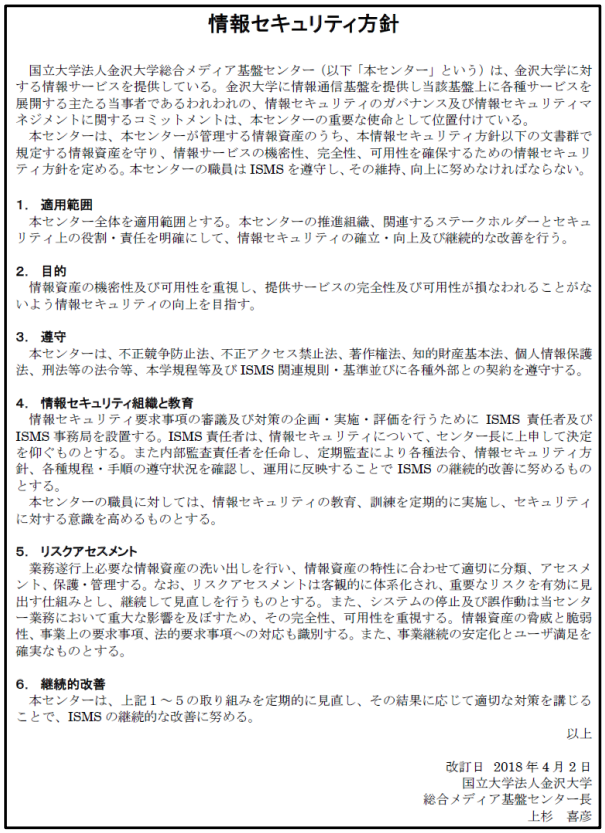
適用範囲が定まると、本センターの状況、外部及び内部の課題、利害関係者のニーズ・期待及び相互の要求事項などが明確化できる。併せて、ISMS の適用範囲に入る人員、業務も明確化でき、そこで稼働しているハードウェアやシステム、サービス及び業務プロセスなど、ISMS を導入して守るべきものと守らないものを切り分けることができた。

4.2 情報セキュリティ方針と目的の確立

ISMS では、トップマネジメントによる、情報セキュリティ方針及び情報セキュリティ目的の確立が求められている。トップマネジメントでは、当該組織が元々持っている「戦略的な方向性」と「情報セキュリティ方針及び情報セキュリティ目的」の両立を確実にするリーダーシップ及びコミットメントの実証が要求されている。

本センターは、ISMS として、情報セキュリティ方針（図 2）を確立し、毎年、情報セキュリティ目的と計画を策定している。

2017 年度及び 2018 年度は、「教育」をテーマに、情報セキュリティ目的を策定し、職員に向けたセキュリティ教育などを計画・実施した。2019 年度



情報セキュリティ方針

国立大学法人金沢大学総合メディア基盤センター（以下「本センター」という）は、金沢大学に対する情報サービスを提供している。金沢大学に情報通信基盤を提供し当該基盤上に各種サービスを展開する主たる当事者であるわれわれの、情報セキュリティのガバナンス及び情報セキュリティマネジメントに関するコミットメントは、本センターの重要な使命として位置付けている。
本センターは、本センターが管理する情報資産のうち、本情報セキュリティ方針以下の文書群で規定する情報資産を守り、情報サービスの機密性、完全性、可用性を確保するための情報セキュリティ方針を定める。本センターの職員は ISMS を遵守し、その維持、向上に努めなければならない。

1. 適用範囲
本センター全体を適用範囲とする。本センターの推進組織、関連するステークホルダーとセキュリティ上の役割・責任を明確にして、情報セキュリティの確立・向上及び継続的な改善を行う。

2. 目的
情報資産の機密性及び可用性を重視し、提供サービスの完全性及び可用性が損なわれることがないよう情報セキュリティの向上を目指す。

3. 遵守
本センターは、不正競争防止法、不正アクセス禁止法、著作権法、知的財産基本法、個人情報保護法、刑法等の法令等、本学規程等及び ISMS 関連規則・基準並びに各種外部との契約を遵守する。

4. 情報セキュリティ組織と教育
情報セキュリティ要求事項の審議及び対策の企画・実施・評価を行うために ISMS 責任者及び ISMS 事務局を設置する。ISMS 責任者は、情報セキュリティについて、センター長に上申して決定を仰ぐものとする。また内部監査責任者を任命し、定期監査により各種法令、情報セキュリティ方針、各種規程・手順の遵守状況を確認し、運用に反映することで ISMS の継続的改善に努めるものとする。
本センターの職員に対しては、情報セキュリティの教育、訓練を定期的に実施し、セキュリティに対する意識を高めるものとする。

5. リスクアセスメント
業務遂行上必要な情報資産の洗い出しを行い、情報資産の特性に合わせて適切に分類、アセスメント、保護・管理する。なお、リスクアセスメントは客観的に体系化され、重要なリスクを有効に見出す仕組みとし、継続して見直しを行うものとする。また、システムの停止及び誤作動は当センター業務において重大な影響を及ぼすため、その完全性、可用性を重視する。情報資産の脅威と脆弱性、事業上の要求事項、法的要求事項への対応も識別する。また、事業継続の安定化とユーザ満足を確実なものとする。

6. 継続的改善
本センターは、上記 1 ～ 5 の取り組みを定期的に見直し、その結果に応じて適切な対策を講じることで、ISMS の継続的な改善に努める。

以上

改訂日 2018 年 4 月 2 日
国立大学法人金沢大学
総合メディア基盤センター長
上杉 喜彦

図 2 情報セキュリティ方針

は「徹底」をテーマに、新たに情報セキュリティ目的を確立・計画・実施している。

4.3 組織の役割、責任及び権限の割り当て

トップマネジメントは、情報セキュリティに関連する役割に対して、職員に対して、責任及び権限を割り当て、その伝達を確実に行わなくてはならない。そこで、本センターでは、ISMS に基づいて業務を推進していくための推進体制組織を本学の人事組織を踏まえながら、その枠組みをこえて構築した（図 3）。図 3 右側の ISMS 推進体制という破線の枠内が、ISMS 推進のための組織となる。この体制では、まず ISMS 推進体制組織のトップとして「ISMS 経営陣」を置き、本センターのセンター長が就いた。併せて、ISMS の運用に関する必要な事項を審議する機関として、「情報セキュリティ委員会」を置き、委員長に ISMS 経営陣が就いた。次に、ISMS 経営陣のもとで、実務の統括者として「情報セキュリティ管理責任者（ISMS-CISO）」をおき、2019 年度は情報基盤部門部門長が就いた。併せて、その指示のもとで活動する「ISMS 事務局」を置いた。また、年に 1 回を目安として本センターが所有している情報資産を中心にリスクアセスメントを行うため、リスクアセス

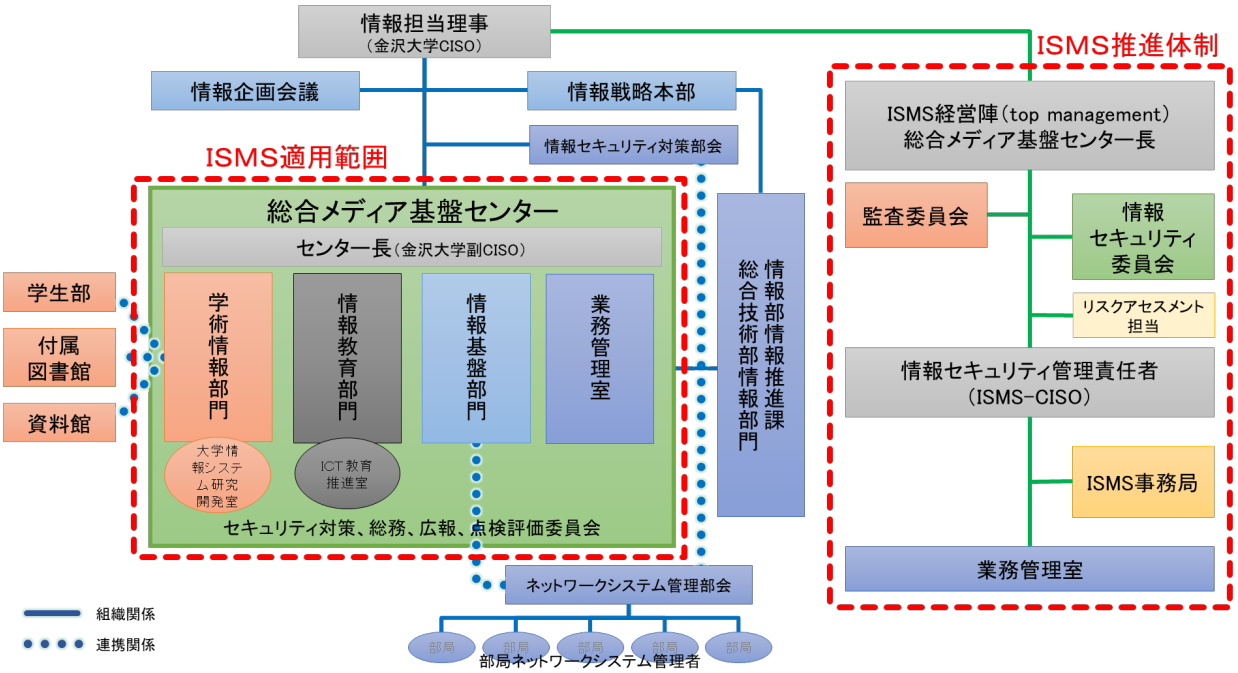


図 3　金沢大学総合メディア基盤センターにおける ISMS 推進体制

メント担当を置いた。最後に、ISMS が正しく運用されているかを組織内から監視する「監査委員会」を置き、その責任者（以下、内部監査責任者と呼ぶ。）に、2019 年度は学術情報部門部門長が就いた。内部監査責任者（とコンサルタント）のもと、原則年 1 回の内部監査を実施し、ISMS 活動の監視や改善に努めている。

4.4　マネジメントレビューの実施

トップマネジメントの役割として、組織の ISMS が、継続して、適切、妥当かつ有効に機能していることを確実に示すために、あらかじめ定められた間隔で ISMS をレビューすることを求められている。本センターでは、後述する内部監査実施時に、併せてマネジメントレビューを実施し、その内容を議事録として文書化し、保管している。

このレビューによって、組織のトップ自身が ISMS で定めたセキュリティに関する多くの取り決めについて認識し、情報セキュリティを踏まえた組織運営を意識させることができる。特に人事異動によってトップが替わったときなどでも、議事録として文書化された情報を得られることで、組織としてのセキュリティへのスタンスや対応、課題などを把握できるのは、ISMS の大きな利点であろう。

4.5　リスクアセスメントの実施

ISMS では、組織は、規格が求めている情報セキュリティを保証するために、リスクアセスメントのプロセスを定め、定期的に、もしくは必要に応じて適用することが求められている。

本センターでは、このための方策として、ISMS 導入が決まったときに、ISMS の適用範囲に入る本センターが所有している情報資産と業務プロセスを明確にして、一覧表にまとめる作業を開始した。次に、一覧表の内容それぞれについて、機密性、可用性、完全性に関するリスクを数的にアセスメント（評価）し、それを踏まえて、具体的に発生が考えられるリスクや問題などを挙げていく。最後に、数的なアセスメントの結果として、対応が必要と評価したもののみをピックアップし、そのリスクを管理する方策について検討し、その結果をまとめた。こうして完成するのがリスク対応計画である。このリスク対応計画が、組織内で承認されれば、以降、本センター職員は、日々の作業の中で、計画に沿った対応を求められていく。

このようなリスクアセスメントは、認証取得のための審査との兼ね合いから、原則 1 年に 1 回の実施が必要である。特に、リスクアセスメントでは、情報資産からリスク対応計画まで「一貫性と妥当性」が必要とされており、妥当性の観点から、アセスメントの過程で行った評価とその結果の文書化が必須である。また、ここでいう一貫性とは、適当な情報資産を 1 つ上げたときに、その資産について、数値化したリスクを示し、その値や発生

が考えられる問題を示した上で、それを防ぐためのリスク対応計画までを順を追って説明し、文書を示せることである。時には逆の流れ、このリスク対応計画を行うのは、どの情報資産のリスクを考えたからというのも示せなくてはならない。

このリスクアセスメントは、ISMS 導入に際して最も労力が必要となる。多くの場合、何をすればリスクアセスメントになるか分からず、作業が進まないことが多い。リスクアセスメントを進める方法としては、先行研究として、山口大学がその手法を提案している[6]。他には企業向けではあるが ISMS 導入に関する技術書が出版されているので、それを参照するのが良いだろう。

4.6 パフォーマンス評価と記録保存の実施

これまで、規格に対応するための作業について示してきた。ISMS では、さらに、示した作業が実施されているかどうかを評価する作業そのものも求められている。これはパフォーマンス評価などと呼ばれている作業で、ISMS 認証を取得するためには欠かせない作業である。評価事項としては、規格で要求されている作業や業務などの内容、リスクアセスメントの結果としてまとめられたリスク対応計画の内容を、項目毎にリスト化し、確認内容と確認時期、実施の可否を図る評価方法についてまとめていく、その後、定期的に項目毎の確認と記録を行う。

4.7 内部監査

ISMS では、JIS Q 27001（ISO/IEC 27001）が要求しているさまざまな事項（規格の附属書 A で定められている管理目的及び管理策や ISMS そのものが有効に実施・維持されているか否かを示す前述のパフォーマンス評価など）を確認可能な状態にし、質の高いセキュリティが維持されていることを示すために、あらかじめ定めた期間毎に内部監査を実施することが求められている。

本センターでは、その要求に従い、図 3 にも表記されている監査委員会とコンサルタントが中心となり、内部監査を、年に 1 回（2017 年 7 月、2018 年 11 月、2019 年 9 月）、企画、実施している。この内部監査では、

- ✓ 内部監査を担当している職員（以下、内部監査員と呼ぶ。）とコンサルタントから、それ以外の本センター職員へ、業務などにあたって、JIS Q 27001（ISO/IEC 27001）の規格が要求している事項に準拠したセキュリティ対応がなされているかどうかの聞き取り調査（約半日）
- ✓ 監査結果の取りまとめと報告
- ✓ 報告された事項についての対応計画検討

の 3 つについて、およそ 1.5 日程度かけて実施する。この内部監査では、規格の要求事項について厳しく確認し、それを満たしていない部分があった場合は、徹底的に指摘しなくてはならない。何故なら、内部監査を徹底することで、ISMS 認証機関による監査時に、要求事項が満たされている、もしくは満たすための作業を実施中であるという、ISMS が機能し、質の高いセキュリティが維持されている状態を示せるからである。ISMS の考え方では、そもそも認証機関に指摘されるまで、要求事項が満たされていない状態があること自体が、ISMS が機能していないと判断されかねず、それが重なれば ISMS 認証には不適合となってしまう。

また、内部監査員とコンサルタントからの指摘事項は、ISMS 経営陣と本センター職員全員に対して報告される。本センター職員は、この指摘事項を踏まえて、文章類の修正や作成、リスクアセスメントの再確認、さまざまな記録作成の不備の見直しなどを、いつまでに実施するかの計画をたて、その内容を文書に起こし、その後、計画の通り、通常業務の中で実施しなくてはならない。内部監査の最後に、内部監査委員が、これらの内容を報告書として作成し、監査が終了となる。

なお、本センターでは、内部監査の資格者を 2017 年度から 2018 年度までは 4 名だったが、2019 年度には 7 名に増員した。内部監査員を増員した理由は、内部監査員もまた本センター職員であり、通常は業務に携わっている。そのため内部監査員自身が携わっている業務を監査するのでは、監査の意味がなくなってしまう。そこで内部監査員が監査する業務が、自身の業務と重ならないように、内部監査員の人数自体を増やしている。

5 まとめ

ここまで本センターにおける ISMS 認証取得の取組について紹介したが、その内容は完全では無い。これは取組の詳細自体が、本センターのセキュリティに関わる内容となるため、書くこと自体が質の高いセキュリティへの不備をもたらす可能性がある。一方で、ISMS を構築するノウハウについても、本センターではコンサルタントを入れて、

その助言やサポートを受けているため、ノウハウ自体はコンサルタントとその会社のものであり、詳らかに開陳をする分けにはいかない。そこで本稿では、ISMS 認証取得に関して、実施すべき取組について、規格の要求事項として書かれている内容と一般論まで落とし込んで記載し、その上で、本センターでの作業をセキュリティの問題が生じない範囲で示していった。今後、ISMS 導入などが検討課題として上がっている大学などの組織において、その検討の一助になれば幸いである。

最後に、セキュリティ対応として、ISMS 認証取得とならんで話題にあがるのが CSIRT への対応である。本センターでは、ISMS 認証取得に際して、あえて CSIRT については除外をした。これは企業などのコーポレートガバナンスで言われる内部統制における考え方の「予防的統制」と「発見的統制」を踏まえて、予防的統制である ISMS の中に、発見的統制である CSIRT を組みこむと、ISMS としての枠組み自体を壊しかねないと考えたからである。そもそも、情報系センターに求められている CSIRT とは、情報系センター以外の学内各所でセキュリティインシデントが発生した際の対応であって、それ自体は ISMS の適用範囲外となることが多いだろう。逆に、ISMS の適用範囲内に発生したインシデントについて、ISMS によるインシデント対応の手続きを越えて、CSIRT による対応が求められるような場合は、逆に、情報系センター職員自体が主体とならない方が良いであろう。このような考えのもと、本センターの ISMS には CSIRT を組みこんでいない。しかし、CSIRT そのものは、セキュリティインシデントへの対応に必要なものなので、今後、ISMS とは別に議論が必要となるだろう。

参考文献

[1] 情報マネジメントシステム認定センター、https://isms.jp/（2019 年 9 月 18 日閲覧確認）

[2] 国際標準化機構（International Organization for Standardization）、https://www.iso.org（2019 年 9 月 18 日閲覧確認）

[3] ISO/IEC 27001:2013、https://www.iso.org/standard/54534.html（2019 年 9 月 18 日閲覧確認）

[4] JIS Q 27001: 2014 (ISO/IEC 27001:2013): “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（2014）

[5] 株式会社　サン・パートナーズ、http://www.sunpartners.co.jp/（2019 年 9 月 18 日閲覧確認）

[6] 市川哲彦, 永井好和, 長谷川孝博, 伊藤賢, 三池秀敏:“情報セキュリティマネジメントシステム(ISMS)における効率的な詳細リスクアセスメント実施手法の提案と情報処理センターへの適用”、学術情報処理研究 12 巻(2008)1 号 p.52-58