博士論文

国立大学法人における組織的 IT 基盤強化策の研究
ー IT ガバナンスの観点から ー

Study on organizational enhancement of IT infrastructure in a National University Corporation
- From the view point of IT governance -

平成 29 年 3 月

永 井 好 和

山口大学大学院理工学研究科

要旨

大学では、教育・研究・運営の各分野において数多くの情報システムが導入されおり、最近では情報セキュリティに関わる脅威に常にさらされている。教育・研究上の必要性から教職員が独自に導入してきた情報システムも多く、前述の脅威への対策が充分でない可能性や、相互のコード体系の相違からデータのやり取りに困難を伴う場合もある。山口大学（以下「本学」）法人化当時、学内の情報システムの開発運用等の維持管理を大学全体として統一的に実施する体制にはなく、学内で稼働する情報システムの全貌を把握することが極めて困難であった。従って、大学執行部が学内の情報システムを掌握する仕組みを具体化することが急務であると考えられた。国立大学法人化に伴い、いずれの大学においても学長をはじめとする大学執行部のリーダーシップが求められる中、大学全体として整合性を保ちつつ効率的な IT 化を進める為に、学内情報システムを把握する必要があった。そして、全学的見地に立ち情報セキュリティ保護の視点からも検討を加えることが必要であった。しかしながら、この時点において両方の要求を満足する仕組みを備えた国立大学は見当たらなかった。そこで、これらの要求を満たす為に学内情報システム届出制度（以下「届出制度」）を考案し、本学内で実現した。具体的には、個々の情報システム（以下「届出案件」）を、学内情報基盤整備を担当する委員会（以下「委員会」）に届け出て審査を受ける仕組みである。届出を義務とする学内規則に基づき、届出案件のライフサイクルを記録し管理する為のコンピュータシステム（届出案件管理システム）を使って、委員会のもとにおかれた作業グループ（以下「WG」;ワーキンググループ）により制度が運営される。届出案件の中で所定の条件に該当する場合、WG がコンサルテーションを実施し、必要に応じて届出案件の改善を求める。本学において当制度を導入し運用することにより、以前には見過ごされていた可能性のある個別届出案件の問題点が解決される効果が認められ、当制度の学内IT基盤整備における有効性が確認された。

一方、情報セキュリティインシデントが多発する中、大学が保有する情報資産管理において、個々の業務担当者任せではなく組織体として責任ある対応ができる情報セキュリティマネジメントの仕組み（Information Security Management System、以下「ISMS」）の確立が大学にも求められている。しかも、その仕組みに従って当該組織体が実際に運営されていることが重要であり、このことを客観的に確認できる必要がある。国内では、国際規格ISO/IEC27001に準拠して構築したISMSの規格適合性を第三者機関（JIPDEC）により認定する「ISMS適合性評価制度」（以下「認証制度」）がある。当制度は、学外機関が助言型監査（審査）によ

り、対象とするISMSが前記国際規格に準拠して実質的に運用されていることを認めるものである。国立大学法人化当時、大学執行部が自大学法人の情報資産を掌握しているとは言い難く、ISMSを確立している国立大学法人は皆無であった。本学においては、ISMSの構築が進められ、前述の認証制度の下で認証を得ている。ISMSには、業務における情報セキュリティ面での行動規範を規定するISMSマニュアルが必要である。国立大学法人におけるISMS構築の為に「高等教育機関の情報セキュリティ対策のためのサンプル規程集」が提供されているが、国立大学法人が利用する場合には、自大学法人に適した形に補正する必要がある。また、ISMSの実質的運用を担保する仕組みに不十分な点も見受けられる。本論文では、本学でのISMS構築運用から得た知見をもとに学外機関による監査の重要性とその効果を示し、ISMS構築を目指す大学の為に、認証制度を活用して学外機関による監査という仕組みを含めることによって実効性のあるISMSを構築することを提案する。

Abstract

In the university, many information systems are introduced in each field of education, research, and management. Recently, those information systems are always exposed to the threat in connection with the information security. In fact, there may also be many information systems which the school staff has introduced freely for the reason required in education or research, and some of them are holding the brittleness on an information security. Moreover, a difference of a code system become a cause and may follow difficulty on an exchange of data. At the time of incorporation of Yamaguchi University, there was no system to unify the university as a whole to maintain and manage the development and operation of information systems in the university. And it was extremely difficult to grasp the whole picture. Therefore, it was considered urgent to concretize the mechanism by which the University Executive Division gains control of the information system within the university. As leadership of the university enforcement department including the president was required along with corporatization, it was necessary to grasp the in-campus information system in order to promote efficient IT development while maintaining compatibility as the whole university. And it was necessary to add consideration from the viewpoint of the whole school and from the viewpoint of information security protection. However, at this time there were no national universities with mechanisms to satisfy both requirements. Therefore, in order to satisfy these requirements, we devised the notification system of campus information system and realized it within Yamaguchi University. Specifically, it is a mechanism of submitting notice on each campus information system (henceforth a "notification matter"), introduced and worked within the campus, to the committee (henceforth a "committee") which takes charge of intramural information infrastructure maintenance, and undergoing examination by a committee. This notification system is managed by the working group (henceforth "WG") who set in the committee using the computer systems (henceforth a "notification matter managerial system") for recording and managing the life cycle of a notification matter based on the intramural rule which makes a notification duty. When a notification matter corresponds to predetermined conditions, WG make a consultation on the notification matter, and WG asks the person who submitted the notice for the required improvement of that matter. By introducing and operating this notification system at our university, the effect of resolving the problems in some notification cases that may have been overlooked before, was recognized, and the effectiveness of this system for the Improvement of IT infrastructure in the university was comfirmed.

On the other hand, since incidents related to information security are becoming more frequent, an Information Security Management System (ISMS), for managing information security matters at an organizational level, instead of at a departmental or individual level, is being requested, even in universities. Moreover, it is important that the organization is actually operated in accordance with the ISMS, and it is necessary to objectively confirm the mechanism and the activity. In Japan, there is the scheme under which the third-party organization authenticates the compatibility of the ISMS which is constructed so as to be conformable to ISO/IEC 27001. This scheme is called “ISMS Conformity Assessment Scheme”. More specifically, an organization outside the university authenticates that the ISMS subject to audit is being actually operated according to the above mentioned international standard, through an advice type audit. At the time of incorporation of a national university, it was hard to say that the university executive department grasped and controlled the information assets of its university corporation, and there were no national university corporations that established ISMS. At our university, ISMS had been developed and certified under the aforementioned certification system. ISMS requires an ISMS manual that specifies a code of conduct in terms of information security in operations. In order to construct the ISMS at the national university corporation, "A sample regulation collection for information security measures of higher education institutions” is provided, but when it will be applied to a national university corporation, it will be needed to adjust to a form suitable for the university corporation. In addition, insufficient points can be seen in the mechanism for ensuring the substantial operation of ISMS. In this paper, the importance of the audit carried out by an organization outside the university and the effects provided by it are described based on the knowledge obtained through construction and operation of the ISMS in Yamaguchi University. Then, for the other university aiming to construct its ISMS, we propose constructing the effective ISMS through including the mechanism of the audit carried out by an organization outside university by taking advantage of the ISMS Conformity Assessment Scheme.

目次

頁

第 1 章　序論

1.1 研究の背景

我が国の国立大学は 2004 年度（平成 16 年度）に実施された法人化を境にして、大学運営の環境が大きく変化した。しかしながら法人化された時点では、法人全体の視点で物事を考え部局の垣根を越えて意思決定をしていくべきとされながらも、現場教職員の意識は一朝一夕には変わらなかった。しかしながら、全学一体運営に向けた改革が絶え間なく続けられており、それまでになかった規則や仕組みが整備されて、現在では学長のリーダーシップのもとで部局を越えた意見調整がなされるようになってきている。

国立大学法人化当時企業では、J-SOX 法や内部統制及び CSR あるいは環境問題への対応等、利潤追求だけでは不十分といわれるようになり、社会に目を向けた対応に取り組み、企業あげて社会正義や公共性への意識が高まってきていた。企業内各部門で発生する様々な出来事に関する正確な情報を、より早くかつ効率的に獲得し加工する必要が高まり、IT への依存度がますます高まってきていた。情報システムのあり方が経営を左右するといっても過言ではなく、IT ガバナンスの確立と IT 基盤の更なる整備の必要性が叫ばれていた。当時企業では EA（Enterprise Architecture）の概念とともに業務と情報システムの全体最適化を進める動きがあった。2006 年 3 月には総務省から「業務・システム最適化（ガイドライン）」が発表され、中央政府においても業務の最適化が進められていた。企業では、組織の IT 化を進める上で全体最適化の為、その組織（多くの場合株式会社）全体の情報の流れを整理し分析したうえで、できる限り標準化や共通化を進めてシンプルなシステムづくりを目指すべきとされていた。システム設計の前に現状分析や情報システムへの要求定義を実施する為に、当該組織内の情報の流れをはじめとする業務の現状についてのヒヤリングが欠かせず、所属員の協力が必須であった。以下に具体的な事例として、販売在庫管理システム構築プロジェクトの事例を説明する。いわゆるウォーターフォール型開発の上流工程にあたる事例である。（ウォーターフォール型開発を構成する工程については図 3-6 を参照されたい。）システムのイメージ図は図 1-1 の通りであり、各営業拠点からの受注データや出荷指示データに基づいて工場への生産指示や出荷指示をリアルタイムで発行するシステムである。このシステムを新規に構築するプロジェクトにおいて、SE（システムズエンジニア）にとって、当該企業の業務知識のない中で現状分析や業務分析を進める為に、各事業所の担当者からの情報提供がかかせなかいのはいうまでもない。当該企業の販売管理業務についてヒヤリングしてその結果を類型化し図式化してその内容を確認

する作業は、最近ではモデリングとして一般化している。この事例では、業務全体を通しての情報処理に関しては、次の2点に大きな特徴がある。

・商品によって情報の流れ（あるいは事務処理手順）が異なる。

・情報は企業内各部署間を行き来する。

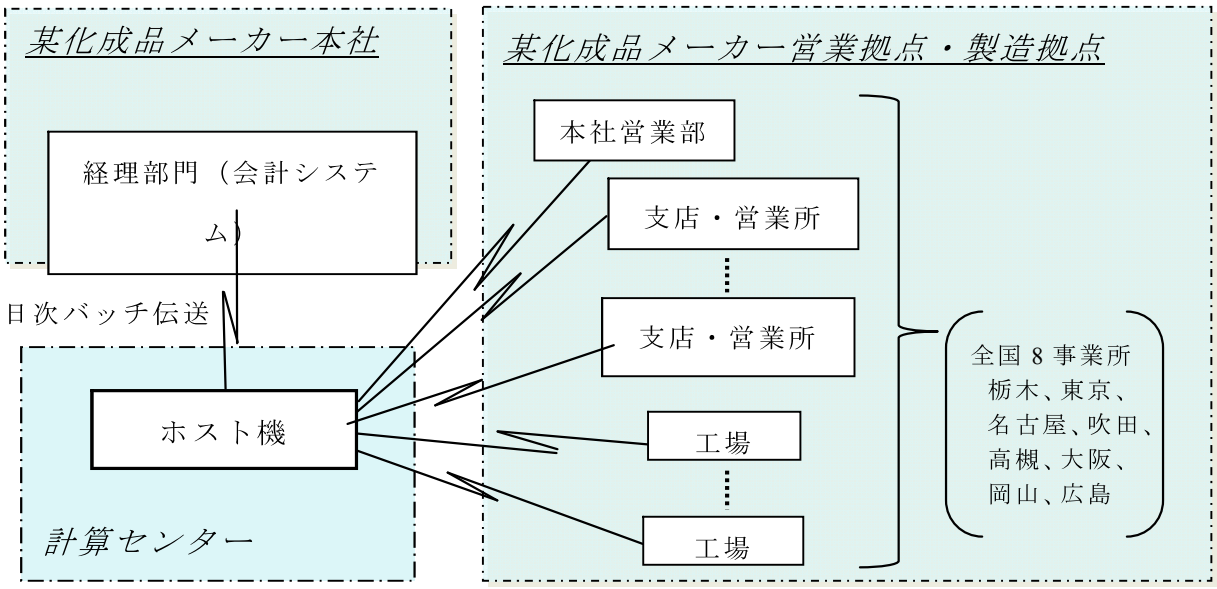

図 1-1　販売在庫管理システムイメージ図

図 1-2 はそのイメージを図式化したもので、営 とあるのが営業拠点での手続きで 工 とあるのが工場での手続きである。業務分析の過程では、図 1-2 の流れをブレークダウンして商品別の企業内の情報の流れと各部署での事務処理を時系列で図式化したが、これはモデリングにおける UML(Unified Modeling Language)でいうところの活動図（アクティビティー図）に該当する。複数部署間を行き来する情報の流れを図示することにより、現場

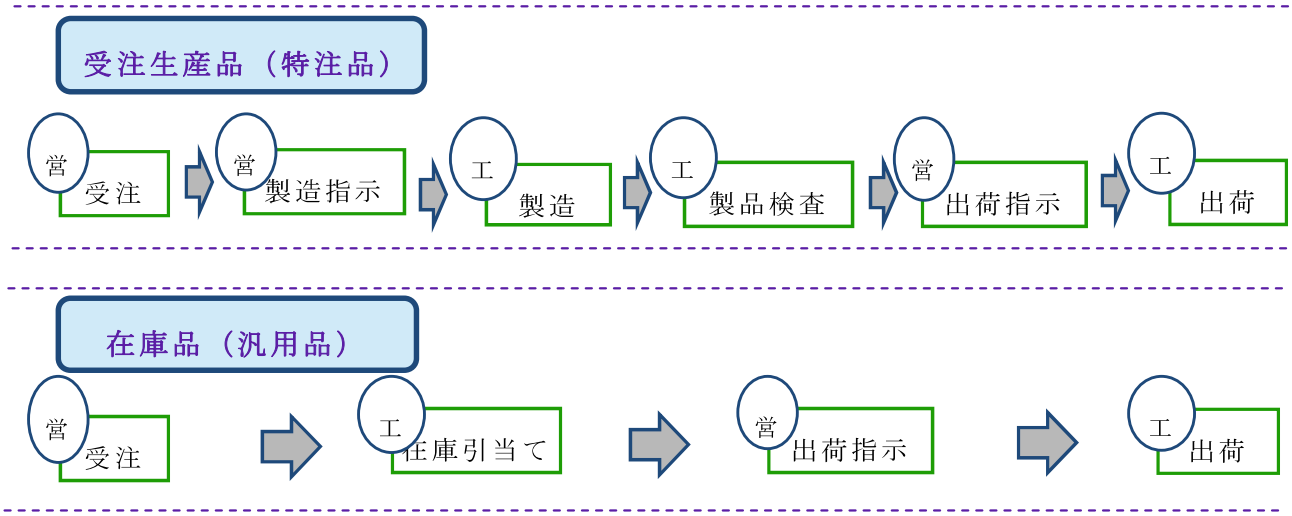

図 1-2　類型別業務フロー（イメージ図）

担当者への確認作業がスムーズにできる。業務上の各手続きについての詳しい説明は文章で表すとしても、図や文章を文書化することが、お互いの認識や理解を共有する上で極めて重要であり、システム設計以前に業務やその中の情報の流れを可視化する事が極めて重要であることを表している。これらの情報システム開発方式についての考え方は、情報システム開発方法論としてまとめている企業もある。日立製作所の HIPACE、富士通の SDEM 等の例がある。

一方、当時の国立大学では、法人化以前より各学部が独立して情報システムを管理してきており、さまざまの企業からなる企業グループのように、その不統一が散見されていた。2004 年度の国立大学法人化後、部局単位ではなく法人全体の視点での最適解が求められ、その為に部局の垣根を越えて意思決定をしていくべきであるとコペルニクス的発想の転換を要求された。天野は「法人化によって国立大学は、これまでのボトムアップ型からトップダウン型組織へと大きく変わり始めた。」と述べており、「一方ではボトムアップ型の大学運営に慣れてきた教員層、他方では文部科学省の指示と規制のもとにルーティン化した業務を執行していればよかった職員層との間に、戸惑いや変化に対する意識・認識のズレを生んでいる」と指摘している[4]。さらに「法規上トップダウン型のシステムが導入されたからと言っても、長い歴史を持ちさまざまな組織内の慣行と結び付いた従来のシステムを廃止することは簡単ではない」と指摘している[4]。前述のように、学内の情報システム管理に目を向けると、長い間に培われた学部自治の中で学部単位に情報システムが導入され、大学全体で情報システムを管理する制度はなかった。企業では ERP（Enterprise Resource Planning)を導入する等、法人組織全体の情報の流れを把握し可視化したうえで全体最適を図る場合が多かったが、本学法人化時点では、大学内全体の情報の流れを把握できる資料もなかった。大学業務を把握するべく業務の可視化を試みるにも、現状把握すら極めて困難な状況にあり、学内情報システムの稼働状況を一から把握する必要があった。しかも IT ガバナンスを確立する前提として、単に一時的にある時点での稼働状況を把握するだけではなく、日々新たに導入される情報システムを把握できる仕組みが必要である。従って、本学 IT ガバナンスを確立するには、次の 2 点の解決が喫緊の課題であった。

- 国立大学法人において稼働する情報システムを大学として掌握する仕組みが確立されていない。その為、学内で稼働する情報システムが大学全体の経営（運営）方針に沿っているのかどうかを統制することができない。
- 学内で稼働する情報システムや取り扱われるデータの標準化ができていない。

さらに、最近では、情報処理の専門家でなくてもある程度の知識があればサイバー社会の一員になることができると同時に、常に不正アクセス等の脅威に晒される環境下にある。国立大学リスクマネジメント情報（2011 年 2 月号）[8]によれば、2010 年 1 年間で 197 件ものコンピュータ不正アクセスが(独）情報処理推進機構に届け出られている。同文献には大学における情報漏洩事故等の事例も掲載されている。情報セキュリティ事故の際に緊急処置を施し、これらを未然に防止する策を講じる組織的対応が必要である。その為にも、学内の情報資産とそれらに伴うリスクを明確にするとともに、情報セキュリティ対策の状況を掌握し、情報セキュリティ事故に対しては組織的に管理し対応できる仕組みが求められる。しかしながら本学法人化時点では、この要請にこたえる組織的な仕組みはなかった。従って、本学 IT ガバナンスを確立する中で国立大学法人の情報セキュリティを維持・管理する上で以下の点の解決が喫緊の課題であった。

・国立大学法人における情報資産を CIO もしくは CISO が掌握し、それらの情報資産の安全を法人として責任をもって維持管理する仕組みが確立されていない。

1.2 研究の目的

本研究では、前節で述べた「保有する情報及び情報システムを組織的かつ安全に維持管理する仕組みがない」という問題を解消する為、「国立大学法人における IT ガバナンス確立に向けた組織面での基礎的な仕組みを考案し、実装結果を確認すること」を目的としている。ここで「基礎的な仕組み」とは、「学内の情報システムを大学執行部が把握し、全学的視点において合理的で安全と考えられる方向に導くことを可能とする仕組み」を指している。具体的には、次の 2 つの仕組みを考案し具体化するとともに、実際の大学組織の中に制度として実装して運用することにより、その仕組みが大学法人にとって有用であることを確認する。

(1) 学内で稼働する情報システムを大学として一元的に掌握できる仕組み。しかもその仕組みは、ある時点で稼働する情報システムを一時的に把握するだけではなく、新たに稼働を始める情報システムも把握可能な持続性のある仕組みである。

(2) 学内の情報資産及びそれらに伴うリスクを掌握した上で、情報セキュリティを確保し、かつそのレベルを継続的に維持・向上可能な持続性のある仕組み。しかもその持続的な維持向上が学外にも示せる仕組みを具備している必要がある。

これらの課題解決により、国立大学法人において、学長をはじめとする大学執行部による IT に関するリーダーシップを支援する仕組みが具現化され、それらの仕組みは IT ガバナンス確立の一翼を担う。

1.3 研究の概要

研究は次の 3 つのステップで進めた。

第 1 ステップ ： 学内情報システムを掌握するという組織全体の最適化の為の仕組みが IT ガバナンスの考え方にかなうものであり、法人化後の国立大学への適用が好ましい仕組みであることを確認する。

第 2 ステップ ： 学内情報システムを掌握するという組織全体の最適化の為の仕組みを検討し試行することで具現化する。

第 3 ステップ ： 学内の情報資産及びそれらに伴うリスクを把握し、情報セキュリティを維持向上させる仕組みを、学内のモデル組織で試行し具現化したうえで、学内他部署（他部局）へ広める。

第 1 ステップでは、「学内で稼働する情報システムを大学として掌握できる仕組み」は必要なのか、国立大学法人は IT ガバナンスを必要としているのか、あるいは企業同様全体最適の考え方を大学に適用できるのかどうか、について再確認する為、IT ガバナンスに関する調査を行った。この調査は、「IT ガバナンス」という用語の定義の再確認を含めて、IT ガバナンスに関する文献を参照することを中心に進めた。結果、学内情報システムを把握するという組織全体の最適化の為の仕組みが IT ガバナンスの考え方にかなうものであり、法人化後の国立大学への適用が好ましい仕組みであることを確認した。これにつては第 2 章で詳しく述べる。

第 2 ステップでは、「大学 CIO フォーラム」への出席や他大学訪問による情報収集を行い、学内では全学委員会に専門部会を設置して提案する仕組みを試行することから始めた。以下、その概要を述べる。

法人化されて間もなくのころには、IT 関連企業や国立大学の CIO に位置付けられる方々によるフォーラムが開催される等、活発な議論がなされており、研究の推進材料（事例研究材料）となった。そこで出された「大学革新のための IT 戦略提言書」[16]（以下「IT 戦略提言書」）の p.12 には、「IT を活用して組織運営効率の向上や透明性の高い経営情報の提供が実現して、初めて抜本的な組織改革が可能になる」とあり、全学的見地に立った IT 化の必要性を述べている。このことは、大学全体として整合性を保ちつつ効率的で安全な IT 化を進める為には、学内の IT 化の状況を把握するとともに、新たな情報システム導入の際に計画段階で全学的見地に立った検討を加えることのできる仕組みが必要であることを意味する。

まず、情報基盤整備を所掌する学内委員会が定める条件に合致する情報システムについて当該委員会に届け出ることにより、学内に導入されるあるいは既に導入されている情報システムを把握しようとする制度を企画し提案した。情報システム届出制度（以下、単に「届出制度」）と称し、前述の委員会を通じて学内への普及をすすめた。当制度は、事務手続きだけではなく、また専門分野の教員が片手間に相談にのるものではなく、IT の専門家（委員会の下の WG）が必要に応じて組織的にコンサルテーションを行うという特徴を持つ。このコンサルテーションは、対象となる情報システムを全学的視点において合理的と考えられる方向に導く手段とした。本学では 2004 年度から、ある条件の下で届出対象となる情報システムあるいはその導入計画の範囲を絞って当制度の試行を始めた。

国立大学法人発足当時、学部自治の下で学部ごとに導入が進められてきた学内情報システムが出力するデータは、コード体系やデータ形式もさまざまなものであった。使用するソフトウェアが基本的にフリーソフトウェアである点も、当時の企業とは大きく異なる点であった。企業ではハードソフトを問わず、製造（あるいは開発）責任の所在が不明確なものを、製品やサービスの要素として利用することは回避すべき行為とされていた。開発した情報システムの利用者から損害賠償を求められる可能性を恐れるが故である。国立大学では逆に無償であることは歓迎すべきことであり、不具合が出ても順次改善していけば許される環境であった。この点についてコンサルテーションを通して把握する為、それぞれの届出案件ごとに導入対象情報システムに関する情報（データ）を記録することを目指した。この点については「3.4.3 初期届出制度の事務フロー」において詳しく述べる。

当制度開始当初、当制度下での「届出」は任意として、届け出るか否かの判断を当該届出対象情報システムの管理者に任せるものであった。任意としていたことから、学内の全ての情報システムを把握するには至らなかったが、届出案件に対するコンサルテーションにより、各届出案件である情報システムの改善効果を確認できた。そんな中、2010 年に教職員作成のホームページが海外から改竄される事故が起きたが、このホームページを提供する情報システムは、上記届出がなされていなかった。届け出られていない情報システムにおいて情報セキュリティ事故が発生したことは、届出を義務化してリスクを軽減することの必要性を示している。最近では情報処理の専門家でなくても、ある程度の知識があればサイバー社会の一員になることができると同時に、常に不正アクセス等の脅威に晒される環境下にある。国立大学リスクマネジメント情報（2011 年 2 月号）[8]によれば、2010 年 1 年間で 197 件ものコンピュータ不正アクセスが（独）情報処理推進機構に届け出られているが、同文献には大学における情報漏洩事故等の事例も掲載されている。情報セキュリティ事故の際の

緊急処置や、前述の情報セキュリティ事故の未然防止の為に、CIO をはじめとする大学執行部が学内情報システムを漏れなく把握し、場合によっては改善するよう指導できる必要がある。前記情報セキュリティ事故を契機に届出を義務とする情報システム届出制度の運用を始めた。本論文では、義務化する前の届出制度を「初期届出制度」と呼び、義務化後の届出制度である「情報システム届出制度」と区別して、第 3 章で詳しく述べる。

第 3 ステップでは、情報セキュリティマネジメントシステム(ISMS；Information Security Management System)(以下「ISMS」)を、学内モデル組織における構築・試験運用から始め、認証制度下での認証所得後の実運用から数年にわたって、複数の部局にその適用範囲を拡大していった。

「届出制度」において届出を義務化し、届け出られた情報システムの開発や運用を承認するということは、当該情報システムにおいて何かの問題（いわゆる、情報セキュリティインシデント）が発生した場合、大学組織として責任を負うことを意味し、社会に対する説明責任を伴うことを意味する。国立大学において、学内の情報セキュリティを確保し、かつそのレベルを継続的に維持・向上させる仕組みの確立が求められることとなる。本研究の第 2 の目的である仕組みの提案が求められる所以である。

インターネットの普及が進み、情報システムが様々な脅威にさらされている中で、企業において ISMS の導入が盛んである。情報セキュリティマネジメントに関しては、国際規格（ISO/IEC27001）[1]が定められ、これに呼応して JIS 規格（JIS Q 27001）が定められている。この規格への適合性を第三者機関が評価・認証する制度（以下「認証制度」）も、（財）日本情報経済社会推進協会（JIPDEC；Japan Institute for Promotion of Digital Economy and Community）により運用されている。2016 年 9 月現在、全国で 5,000 を超える組織体がこの認証を獲得しており、国立大学においても、これを導入する動きがある。本学メディア基盤センターでは、この認証制度を活用して学内に ISMS を試験的に導入し、その効果を評価する活動を進めた。情報セキュリティ委員会に於いてモデル組織において試行することが認められ、2007 年に先行する静岡大学の事例研究から始めて、メディア基盤センターをモデル組織として ISMS の構築を進めた。2008 年には ISMS 運用を開始し、ISMS 適合性評価を受け前記国際規格（ISO/IEC27001）に適合するという認証を得た。その後効果も認められ、試行ではなく本格的に運用することとなった。そのことにより、学内の他部署（あるいは他部局）への ISMS 普及を進めることができている。現在では、国立大学法人情報系センター協議会の中に、 ISMS 適合性評価制度下での認証を受けた大学を中心として ISMS 研究会が活動しており、ISMS 導入機運の高まりを表している。他部署への

ISMS 適用範囲拡大の際、ISMS における行動規範あるいは業務の実施手順を記述する ISMS マニュアルが必要になる。2007 年には国立情報学研究所から「高等教育機関の情報セキュリティ対策のためのサンプル規程集」[10]が公開されたので、これの ISMS マニュアルとしての活用の可能性を調査研究するに至った。その結果、補充すべき事項があるものの、利用が可能であるとの結論を得た。第 4 章で詳しく述べる。

1.4 本論文の概要

本節では本論文における第 2 章から第 5 章までの章構成について簡単に述べる。

第 2 章では、本研究の第 1 ステップの内容について記述している。社会が国立大学法人に何を求めているのかという点について考察を加えた上で、情報システムに関しては IT ガバナンスの確立が必要であることを確認する。この中で、本論文で使用する IT ガバナンスという用語の定義を明確にする。

第 3 章では、本研究の第 2 ステップの内容について述べている。2 段階で「情報システム届出制度」を学内に具現化し、実際に運用することにより、この学内制度が国立大学法人にもたらす効果を確認したことについて述べる。その上で、ITガバナンスを主導する CIO やそのもとで活動する担当者の恣意的活動を排除する為に、学外の第三者機関による監査が必要であることを含めて、届出制度における今後の課題についても述べる。

第 4 章では、本研究の第 3 ステップの内容について述べている。もう 1 つの研究課題である「学内の情報資産及びそれらに伴うリスクを把握あるいは掌握した上で、情報セキュリティを確保し、かつそのレベルを継続的に維持・向上させる仕組み」として、ISMS を本学内に具現化し学内制度として運用を試行し効果を得たことを述べた上で、今後の課題について述べている。本学の事例を紹介するとともに、この制度が実際に運用されていることを客観的に評価し、CIO 等 IT ガバナンスを主導する者や組織による恣意的な活動を防止する為には、学外の第三者による監査の実施が重要であることも述べる。また、ISMS 導入に必要な ISMS マニュアルとそのテンプレートに関する考察を加える。テンプレートとして国立情報学研究所が提供する「高等教育機関の情報セキュリティ対策のためのサンプル規程集」[10]を利用する際の留意点について述べる。

第 5 章では、情報システム届出制度と ISMS という、提案する 2 つの学内制度が本学において運用され有効に機能していることを述べ、「国立大学法人における IT ガバナンス確立に向けた組織面での基礎的な仕組み」の実装結果を確認できたことを述べる。その上で、制度上の限界を含めて今後の課題や今後の展望について述べる。

第 2 章　IT ガバナンスの必要性

2.1　概要

本章では、研究の第 1 ステップとして、学内情報システムを掌握し統制するという仕組みが全体最適化という社会の要請にかなうものであり、法人化後の国立大学への適用が好ましい仕組みであることを述べる。まず次節（2.2 節）では、国立大学法人化に際して「全学的な視点に立ったトップダウンによる意思決定の仕組みと全学一体運営」が社会から求められていることを説明する。それを受けて、国立大学法人における IT に関しても学長を中心とする大学執行部が全体を掌握し統制を図ること（即ちITガバナンス）が求められていることを 2.3 節で述べる。2.4 節では、一般社会で認識されている「IT ガバナンス」という言葉に意味について、定義を含めて考察する。その上で、2.5 節では、国立大学法人が取り組むべきITガバナンスの施策について考察を加える。

2.2　国立大学法人化における IT 化の必要性

本節では、国立大学法人化の経緯について調査した結果として、国立大学法人がが「全学的な視点に立ったトップダウンによる意思決定の仕組みと全学一体運営」を求められていることを述べる。そして、大学法人の意思決定にはスムーズな情報の流れが必要であり、ITが欠かせないことを述べる。

福島真司と馬越徹による論文「国立大学法人におけるガバナンス改革の研究」[18]によれば、国立大学の自主性・自立性を持たせ、教育・研究に関する政府からの干渉を軽減しようとする議論は40年前からなされていることが判る。

文部科学省のホームページの資料に記載された「国立大学法人化の経緯」[22]によれば、平成11年4月に「国立大学の独立行政法人化については、大学の自主性を尊重しつつ大学改革の一環として検討し、平成15年までに結論を得る。」との閣議決定がなされたあと、平成15年7月に国立大学法人法等関係6法が成立し同年10月に施行されて、平成16年4月から国立大学法人に移行されている。前記の閣議決定後、文部科学省に設置された「国立大学等の独立行政法人化に関する調査検討会議」の最終報告[11]を見てみると、会議発足当初から、学長を中心に学部を超えて自主的かつ自律的な経営を行い、競争原理の中で、社会に向けて透明性を高め社会の評価を受けることが求められていることが分かる。当該最終報告書は「新しい国立大学法人像」について検討する際の視点をまとめたものであり「Ⅰ．基本的な考え方」「Ⅱ．組織業務」「Ⅲ．人事制度」「Ⅳ．目標・評価」「Ⅴ．財務会計制度」「Ⅵ．大学利用機関」「Ⅶ．関連するその他の課題」の7章で構成され

る。なかでも「Ⅰ．基本的な考え方」に「視点」や「前提」として書かれた、以下の4点が注目に値する。

◎1点目は「各大学法人が、適切な競争原理の中で効率的に運用されること。」である。

◎2点目が「国民や社会に対する説明責任（アカウンタビリティ）」である。「大学運営の実態や教育研究の実績に関する透明性の確保と社会への積極的な情報提供がなされること」が必要であるとしている。また、「これからの国立大学は、国民に支えられる大学として、国民や社会に対する説明責任（アカウンタビリティ）を重視した、社会に開かれた大学を目指す必要がある。」と述べられている。

◎3点目が「自主性・自律性」であり、「学問の府としての特性を踏まえた大学の自主性・自律性を尊重するとともに、各大学における運営上の裁量を拡大していくことが必要」と記載されている。

◎4点目が「全学的な視点に立ったトップダウンによる意思決定の仕組みと全学一体運営」である。「学問の府としての特性を踏まえた大学の自主性・自律性」を「拡大する経営面の権限を活用して、学部等の枠を越えて学内の資源配分を戦略的に見直し、機動的に決定、実行し得るよう、経営面での学内体制を抜本的に強化するとともに、学内コンセンサスの確保に留意しつつも、全学的な視点に立ったトップダウンによる意思決定の仕組みを確立することが重要である。」と述べられており、さらに「同様に、各学部等においても、全学的な運営方針を踏まえつつ、運営の責任者である学部長等を中心とした円滑な意思形成とダイナミックで機動的な運営の仕組みを導入すべきである。」としている。

「国立大学等の独立行政法人化に関する調査検討会議」の最終報告[11]では「情報」という用語が 16 箇所で使われており、学外への情報発信（公開）、国立大学法人評価委員会の評価、学術情報担当副学長の設置の 3 項目の説明に使用しているのみであるが、前述の「円滑な意思形成とダイナミックで機動的な運営の仕組み」は IT 無くしては成立しえないことはいうまでもない。言い換えると、企業でいう「経営情報システム」の構築を中期的目標にすることを国立大学に求めており、学術情報担当副学長が学長を補佐する形で「IT によって大学法人の自主的・自立的且つ効率的な運営」を支援すること求めていることを示している。

一方、国立大学法人法の条文には「情報」「情報システム」「IT」等の用語はほとんど明記されていない。ただ 1 箇所「情報」という用語が使われているのが第 30 条 2 項で、文部科学大臣が中期目標として定めるべき事項の 1 つとされている。また、国立大学法人として

の意思決定に関与する組織として、役員会・経営協議会・教育研究評議会のような組織と、学長・理事・監事・経営評議会委員・評議員等の役職が定められており、国立大学法人の評価の為に「国立大学法人評価委員会」が文部科学省におかれる等、組織の骨格が示されている。これらの組織や役職の役割を規定する部分には「情報」「情報システム」「IT」等の用語は見当たらないが、国立大学法人評価委員会の詳細については政令で定めることとなっている。これら国立大学法人の組織体系を図示すると、次の図 2-1 のようになる。国立大学法人の意思決定は理事会の議を経て学長が行うということが、国立大学法人法第 11 条に定められている。学長や理事が大学運営を迅速に行う為には、学内の活動状況に関する正確な情報が、部局（あるいは学部）の枠を越えてより早く学長や理事会（いわゆる執行部）に伝わり、執行部が正確で時宜を得た判断を下せる仕組みが必要である。またその仕組みは、執行部を中心に決定された法人としての意思を、（其の情報を知るべき）職員に正確にそしてできるだけ早く周知される仕組みでなければならない。この点において、IT が必要であり重要である。

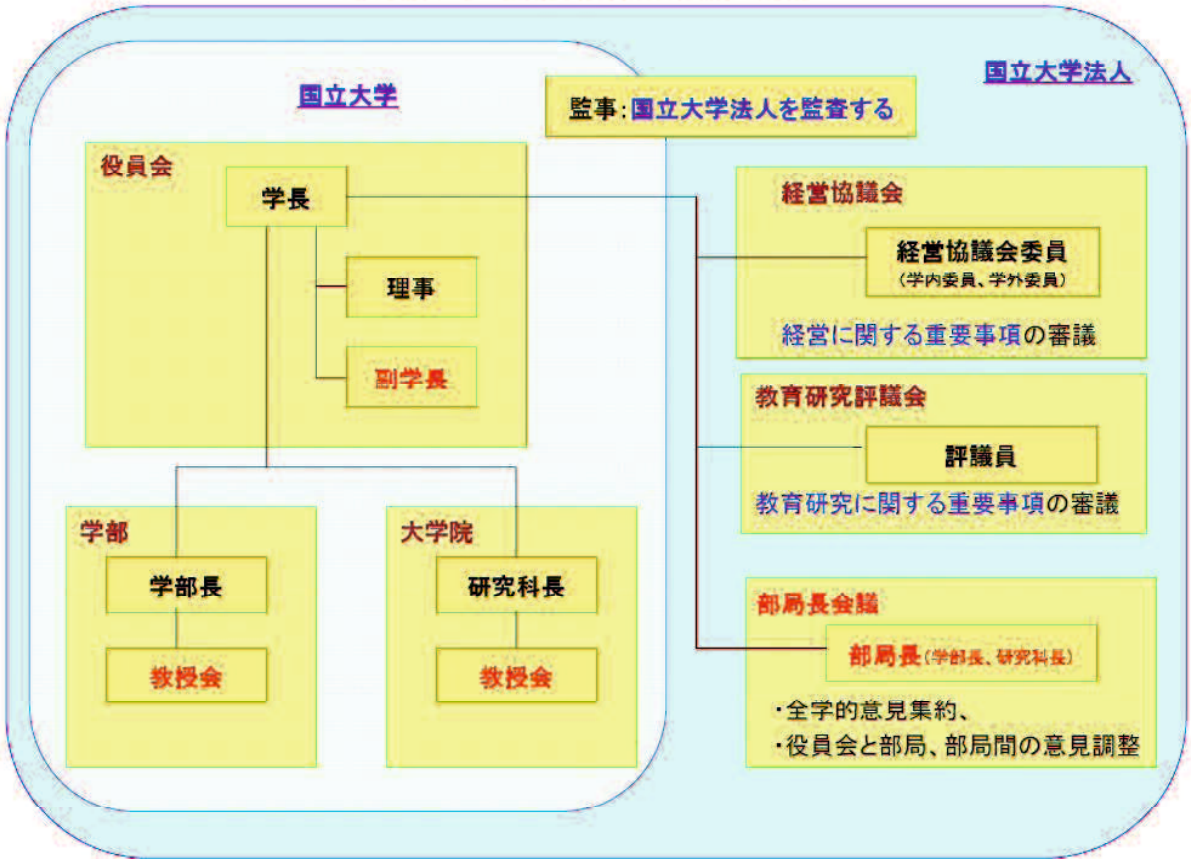

図 2-1：国立大学法人の運営組織

一方で、学校教育法に基づく教授会や部局長会議は、多くの国立大学で現在も機能しており、国立大学法人法で規定されている大学法人としての意思決定の仕組みとの調整も必要である。従来学部独自の(教授会等による)意思により各学部個別に構築されてきたIT基盤についても、全学一元的運営体制にとって有効な仕組みとするには、学部個別の仕組みを全学的視点に立って見直す必要性が生まれることが容易に推測される。

国立大学法人法では「情報」に関する記述が 1 箇所にしかないものの、IT 活用をもっと重要視し「情報」をさらに有効利用して、国立大学法人化に求められる組織づくりを推進していくことが求められている。

2.3 IT ガバナンスの必要性

国立大学法人に限らず、現代社会において、IT に無縁の社会システムはありえないといっても過言でなく、IT は社会の基盤として必要不可欠であることはいうまでもない。一方近年 IT に関する事故や事件が多発しているのも事実である。産業界では「コーポレートガバナンス」の重要性が叫ばれており、中でもIT(もしくはICT)活用の部分に着目して「IT ガバナンス」が重要視されている。2000 年前後の企業不祥事を受けるように、2004 年 4 月にはOECDから「OECD コーポレートガバナンス原則」が制定され、2006 年度秋には国内主要企業により日本 IT ガバナンス協会が設立されている。

一方、公共部門においても、行政改革の流れの中で民間の経営手法を取り入れたり、公企業を直営から間接営へ経営形態を移行する流れがある。国立大学も法人化され企業会計基準が取り入れられている。しかし、大学の中の IT 環境をみると、従来の「大学の自治」「学部の自治」の中で導入された既存の「情報システム」は大学全体を意識したものではなく、コード体系やプログラミング言語等不揃いなものが散見される。この点については、第 3 章で事例をあげて紹介する。また、蓄積されたデータが個別の学部帰属である場合、大学全体で統一的に取扱う為には、個別学部と折衝して当該学部の了承が必要であり、学部間相互にデータの整合性を確認する必要がある。従って、国立大学法人において学長が法人の業務を総理する為には、大学全体の IT 化の活動を統制する必要がある、即ちITガバナンスの確立が必要である。

2. 4 IT ガバナンスの定義

前節でITガバナンスの必要性について述べたが、本節ではITガバナンスの意味について考察する。「IT ガバナンス」とは何か、その定義を明確にする必要があるが、文献によっ

て異なる表現で定義がなされており、少なくとも以下の 5 つの定義がある。文献ごとの、これらの（5 つの）定義に共通するのは、次の点である。

- 組織体の目標や戦略のなかで、IT 戦略の策定から実施・評価までをコントロールする活動である。
- 組織としての活動である。

そして、次に記載している(1)～(5)の中で、(5)の定義のみが大学法人における IT ガバナンスを想定した定義であり、その他は、主として企業における IT ガバナンスを想定した定義である。(1)はグローバル企業である IBM 社の内部を見据えて IT ガバナンスの具体的な構成を考慮した形での定義となっている。(5)の定義は、2006 年 6 月の大学 CIO フォーラムにおいて公表された IT 戦略提言書[16]に掲載されているものである。それぞれの定義が記載されている文献を参考文献として掲載しているので、参照されたい。

(1)IT 戦略の一環であり、IT 戦略の策定から実現までの一連の活動をコントロールし、IT のあるべき姿の実現に向けた IT マネジメントプロセス、IT 標準及び IT 体制を構築する組織だった活動のことである。[9]

(2)企業が競争優位性構築を目的に、IT 戦略の策定・実行をコントロールし、あるべき方向へ導く組織能力である。[6]

(3)取締役会と経営者の責務である。それは、企業ガバナンスの不可欠の一部であり、その組織の IT が、組織の戦略と目標を維持して、そして拡張することを保証するリーダーシップ、組織的な構造及びプロセスからなる。[6]

(4)組織体・共同体が、IT を導入・活用するにあたり、目的と戦略を適切に設定し、その効果やリスクを測定・評価して、理想とする IT 活用を実現するメカニズムをその組織の中に確立すること。[24]

(5)IT を導入・活用するにあたり、全学的な目的と戦略を適切に設定し、その効果やリスクを測定・評価して、理想とする IT 活用を実現するメカニズムを全学組織の中に確立すること。[16]

大学における IT ガバナンスについては、2 つの視点により 4 分類されると考えられる。視点の 1 つは誰の為のガバナンスかという点、もう1つはガバナンスの対象が何かという点である。前者について大きく分類すると、大学外の関係者（入学希望者、学生の保護者、政府、地域社会、産業界、等）の為のガバナンスと、大学内の関係者（あるいは大学法人自身の）為のガバナンスとに分類される。後者については、「IT による（大学の）ガバナンス」と「IT（もしくは IT 化）そのもののガバナンス」とに分類される。本論文では、大学法人をその

対象とした表現になっていることから、これら 4 分類の視点に配慮して(5)の定義を採用し、「IT ガバナンス」を「IT を導入・活用するにあたり、全学的な目的と戦略を適切に設定し、その効果やリスクを測定・評価して、理想とする IT 活用を実現する為に IT を導入・活用するメカニズムを全学組織の中に確立すること。」と解釈する。

次に、前記定義の国立大学法人にとっての意味について考察を加える。国立大学においては、国立大学法人法に従って 6 年ごとの中期目標・中期計画が策定され、毎年の年度計画にブレークダウンした上で、計画が実施に移されている。中期計画及び年度計画のなかには当然 IT(あるいは IT 化)に関する事項を含むわけで、これが、前記「全学的な目的と戦略を適切に設定し・・・」の部分に当たるものとなる。

また、国立大学法人法によれば、各大学の中期計画にもとづく業務実施状況を大学評価・学位授与機構が総合的に評価することになっている。もちろん国立大学法人自らが自己評価することも求められている。2016 年現在、第三次中期計画とも言える 6 年間の中にあるが、毎年年度計画の実施状況を確認し、次年度の年度計画に反映していくよう、制度が運用されている。中期計画に関して「その効果やリスクを測定・評価して」いくことが制度化されているわけで、これは前記「IT ガバナンス」の定義の一部「その効果やリスクを測定・評価して」を具現化したものと考えられる。中期計画の中に IT に関する計画があれば、この評価の対象になる。ただ効果測定や評価に関する具体的内容については、流動的な部分がある。これは前記「IT 戦略提言書」に「利益の最大化を目標とする企業活動とは異なり、(大学における)IT の価値評価が難しい」と書かれていることからも判る。

以上のことから、「IT ガバナンス」の定義の前半部分に該当する制度は既に具現化されているものといえる。本論文においては、「IT ガバナンス」の定義の後半部分「理想とする IT 活用を実現するメカニズムを全学組織の中に確立すること。」という点に着目しており、この点について次節で述べる。

2.5 国立大学法人が取り組むべき IT ガバナンスの施策

国立大学法人化に際して、2006 年に開催された大学 CIO フォーラムによる「IT 戦略提言書」[16] の 82 頁には、「現状の課題」や「望ましい方向性」が表にまとめられている。この提言書は複数の国立大学に所属する教職員によりなされた提言であり、IT ガバナンスに関しては次の 3 項目があげられている。

(a) IT マネジメント体制の確立

(b) IT 戦略ビジョンの策定

(c) IT 導入の客観的評価の実践

これらの中で、(a)について同提言書 p.23 には、「大学 CIO を中心に IT マネジメント体制を確立する」という目標とその為の施策として、次の①～③のように記載されている。

① 早急に取り組むべき重点施策

A 大学CIO及び関連組織の設置

B 学長がトップの「IT戦略本部」の設置

C 教育・研究組織との連携

② 中期的に取り組むべき重要施策

D 大学CIOへのITガバナンスの一元化

③ 国・企業が取り組むべき施策

E 大学CIOガイドラインの整備

国立大学法人の課題に関する本論文では、「③ 国・企業が取り組むべき施策」については検討対象外である。「② 中期的に取り組むべき重要施策」は本研究の将来的な目標になりうる項目であるが、「① 早急に取り組むべき重点施策」は組織づくりに関する施策であり、IT ガバナンスの定義の後半部分「理想とする IT 活用を実現するメカニズムを全学組織の中に確立すること。」に対応する。

国立大学法人においては、文部科学省通知「独立行政法人等の業務・システム最適化実現方策について」[21]の要請に基づき、各独立行政法人等において 2005 年度中に CIO 及び CIO 補佐官が設置されている。最近では多くの大学において、形としては組織もしくは体制ができていることはいうまでもない。本学においても全学教育研究施設として該当する学部横断的組織として機構や CIO が設置され、IT 戦略提言書にいう「大学 CIO 及び関連組織」や「情報環境整備委員会」「情報セキュリティ委員会」といった委員会に相当する組織が設置されている。ここで同提言書 22 頁に掲載されている「大学 CIO 及び関連組織（機能図）」を図 2-2 として掲載して置く。同提言書では「一例」として掲載されている図であるが、この組織体系は、国立大学法人法による縦割りの運営組織の中に、IT 面での全学調整機能を補完する横割りの運営組織を取り込んでおり、前述の「① 早急に取り組むべき重点施策」3 項目「C 教育・研究組織との連携」を目指す組織となっている。ここに書かれた「IT 戦略本部」には学長が含まれていない。「B 学長がトップの IT 戦略本部の設置」に関しては、学長が「IT 戦略本部」のトップになるのか、CIO にその任を任せるのかは、今後の検討課題となっている。「① 早急に取り組むべき重点施策」の 1 項目「A 大学 CIO 及び関連組織の設置」に関して、CIO の関連組織として情報セキュリティ委員会や情報環境整備委員会が設置され、CIO 補佐官や CISO とともに IT 戦略を推進する組織を形

作っている。各教育・研究組織からその代表者が前記委員会に参加することにより、「C教育・研究組織との連携」を実現する構図にもなっている。

IT 戦略提言書では一方で課題として、教員と職員との IT 導入に関する意識にギャップがあること（同提言書 p.22）や、大学全体の IT に関する発注・調達の管理が困難で「トータルコスト」が把握できないことを指摘している。前者に関しては、次章において本研究で提案する仕組みの中で意識ギャップ解消を目指すことを述べる。後者に関しては、少なくとも大学内の情報システムを把握することが前提であり、本研究が国立大学の IT ガバナンスの基礎となると言える。

この他に次のような項目の提言がなされているが、ここではその詳細を省略する。

- 大学経営ビジョンと連動した全学的な IT 戦略ビジョンを策定する。
- 大学経営判断に資する IT 導入の客観的評価を実施する。
- 高度な IT の活用により、「カスタムメイド教育」の実現を目指す。
- 最先端学術情報基盤の整備による研究の高度化・効率化と情報発信力の強化
- IT を活用した大学経営の最適化とサービスの充実
- 全学的に統一された情報基盤を整備し、その拡張、高度化及び信頼性の向上を図る。

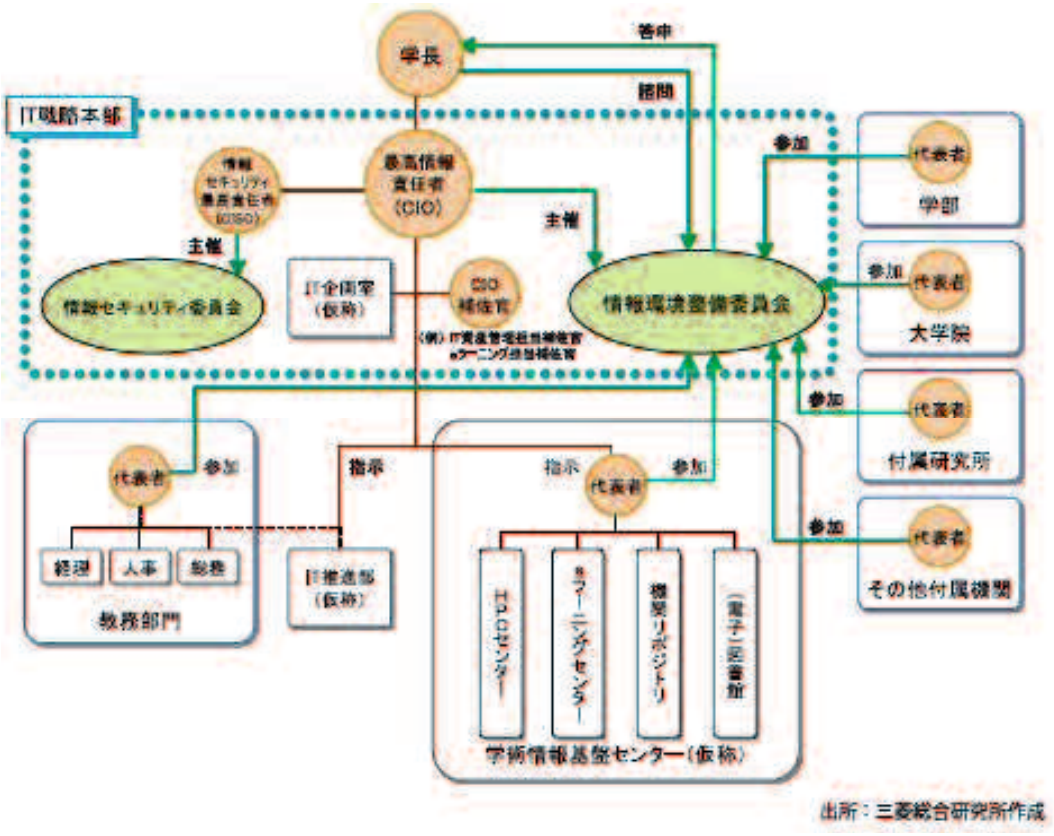

図2-2　大学CIO及び関連組織（機能図）の一例

2.6 まとめ

国立大学法人が国の制度として確立された意味を概観し、学長のリーダーシップによる大学運営におけるITの重要性について述べた。ITに関して全体最適化を図ることやITガバナンスを確立することが、国立大学法人に対する社会の要請に叶うものであり、「学内で稼働する情報システムを大学として一元的に掌握できる仕組み」も、国立大学法人に求められていることを述べた。さらに、本研究の課題を解決することにより確立される仕組みが国立大学法人のITガバナンスのレベル向上に寄与する仕組みであり、社会からの要請に叶うものであることを確認した。

第3章　学内情報システムの統一的管理（情報システム届出制度）

3.1 概要

本章では、本研究の第 2 ステップとして、第 1 章で述べた研究課題 2 項目のうちの次の項目について詳しく述べる。「学内で稼働する情報システムを大学として一元的に掌握できる仕組み（方式）」を具体化すること。しかもその仕組みは、ある時点で稼働する情報システムを一時的に把握するだけではなく、新たに稼働を始める情報システムも把握可能な持続性のある仕組み（方式）でなければならない。

本研究により考案し具体化した仕組みは、学内で稼働あるいは導入される情報システムを掌握して全学的な視野で検討することができる仕組みとして、ITガバナンスの確立に向けた活動の基礎となる仕組みである。「情報システム届出制度」と名付けて本学に実装して実際に運用することにより、学内における情報システムの 2 重開発や無駄なコストの発生を防止もしくは削減できる等、さまざまな効果を得ることができる。本研究においては、最初テスト運用を兼ねて、学内の各情報システムの管理者が任意に届出る「初期届出制度」の試行を始め、その効果を評価する。その結果を踏まえ、届け出るべき条件を整理し、その条件に該当する場合の届出を義務化すると同時に届出の手続きを簡素化して、「情報システム届出制度」として実装し運用を開始する。さらに 1 年から 2 年の運用結果を評価しより良い制度に改善していく。このように 2 段階に分けて当初予定の仕組みを制度化する。

3.2 節では本研究開始当時の国立大学の IT 化の現状を詳しく述べ、それを補足する形で、3.3 節において国立大学における情報システム調達手続きの当時の状況を述べている。3.4 節において初期届出制度について詳しく述べ、3.5 節で届出を義務化した情報システム届出制度について述べている。3.6 節ではその制度の効果と今後の課題について説明を加えている。3.7 節で本章のまとめとして、制度を運用してその効果が得られたことを示した上で、将来的の学内情報システム全体のスリム化に向けて、それぞれの情報システムの機能や入出力データの仕様を整理すること等の今後の課題について述べる。

3.2 国立大学法人 IT 化の現状

3.2.1 国立大学法人における運営組織体系

国立大学法人の運営組織体系になかに、教員と職員との IT 導入に関する意識にギャップがあることや、大学全体の IT に関する発注・調達の管理が困難で「トータルコスト」が把握できないという指摘があることを第 2 章でも述べたが、ここで補足する。「国立大学法人の財務・経営の実態に関する総合的研究[5]」73 頁に、国立大学法人の学長と理事の

方々への聞き取り調査を行った結果をまとめたものとして、「機能を『充実・強化する為の組織』を別に設置している大学が、8 割を超えている。」ことが判るとある。ボトムアップ型運営組織体系の弱体化とひきかえに強化された、トップダウン型の意思決定機構だが、縦割り組織を補完し部局間調整の為の横割り組織が必要であることを物語っている。これは、同文献第 5 章で「国立大学法人の現実と課題」が 35 頁にわたって述べられている中で、国立大学法人法が規定している縦割り組織には、学部間の調整機能を持つ別の組織（横割り組織）が必要であるとした次の 74 頁の文章からも判る。

「（中略）学長中心の本部・執行部の権限がいかに強化されても、教育研究の現場の長である部局長の了解と合意なしには、実質的な大学運営は成り立たない。単科大学は別として、複数の部局を持つ大学にとって部局長会議は、非公式とはいえ依然として、円滑で一体的な大学運営に不可欠の組織なのである。ただ、そうはいっても、従来のボトムアップ型の意思決定に中心的な役割を果たしてきた諸組織の役割の変化、意思決定過程での地位の低下は、明らかである。（中略）法人の制度設計によれば、役員会（学長・理事）、経営協議会、教育研究評議会が公的な組織だが、経営・教学のどちらについても、それだけでは大学運営が円滑に行われがたいことを、すべての国立大学法人が認識している。とりわけ大学運営の中核となるべき役員会について、大多数の大学（69％）が、経営上の重要事頓についての実質的な審議の場として、『充分に機能している』とする一方で、その機能を『充実・強化する為の組織』を別に設置している大学が、8割を超えている。（以下略）」

そして、同文献[5]69頁には作業の量と質の両面で増加するにもかかわらず、運営費が減少し、業務効率化を求められている点についての記述があり、文部科学省、国立大学法人評価委員会、大学評価・学位授与機構による、教育研究活動を含む総体的な評価の為の事務作業増を憂える声のあることを表している。事務作業量の増加を効率向上で乗り切る為にはIT活用が必須である。

3.2.2 情報化推進組織の状況

そこで IT 活用を推進する為の IT 関連組織の状況について述べる。各大学には情報化推進の為の組織が設置されており、その多くは教員組織と事務組織に跨る組織となっている。最近では CIO 及び CIO 補佐官（国立大学法人化以降は「CIO 補佐」と称している）が設置され全学的な情報化推進に向けて舵が切られている。これは文部科学省通知による要請に基づいて、各独立行政法人等において 2005 年度中に設置することになったものであり、いくつかの国立大学法人において設置されていることが、そのホームページ等で公表

されている。CIO 及び CIO 補佐官を支援する情報化推進担当組織も設置されている。前述の「IT 戦略提言書」には、1 つの例として、CIO の下に「情報環境整備委員会」と「情報セキュリティ委員会」をおき、事務組織を含む学内各部局（各部署）から代表者が参加して学内コンセンサスを図る体制が図示されている。（「図 2-2　大学 CIO 及び関連組織（機能図）の一例」を参照）

このような運営組織体系の中にあって、ほとんど全ての大学では情報関連で大きく3系統の組織が存在する。1つは学内情報基盤（学内ネットワークや研究・教育用計算機等のIT基盤）を担当する部署、1つは情報関連研究部門（学部、学科、研究科、等）、もう1つはこれらを支える事務部門である。東京大学の例でいうと（ホームページによれば）前者として、総長のもとに「情報基盤センター」があり、後者として「情報学環」「学際情報学府」が相当する。これらを支える事務組織は東京大学のホームページには記載されていないが、一般的な大学組織としても何らかの事務組織が存在することはいうまでもない。これら3系統の運営組織それぞれに、組織としての意思決定の仕組みがある。本学の事例を見ると、情報関連研究部門は教育研究組織として学部長・教授会による意思決定がなされるし、事務組織は教員組織とは別の事務局としての意思決定の仕組みを持つ。学内情報基盤を担当する部署については、業務系（事務系）情報システムを担当する部署があり、学内ネットワーク等のインフラストラクチャーを担当する組織が別に分かれている。教員組織による意思決定の仕組みと事務組織による意思決定の仕組みとが共存しているのである。国立大学情報系センター協議会での議論内容から、多くの国立大学法人においても同様であることが容易に推測される。国立大学運営に必要な当該大学内共通の情報関連課題についても、大学法人としての意思決定が必要な場合、事務系組織と教員系組織との間の調整という作業ステップが必要となる。「全学的な視点に立ったトップダウンによる意思決定の仕組みと全学一体運営」を確実なものにするには、大学全体のIT関連課題に関する意思決定の仕組みを確立する必要がある。東京大学の事例では、公開されている中期計画のなかに、「事務等の効率化・合理化に関する目標」として「電子的事務処理の推進に関する具体的方策」の記載がある。また「経費の抑制に関する目標」として「事務量の軽減や会議費の削減を図る為、学内事務分掌の見直し、会計手続きの簡略化、情報ネットワーク化、文書の電子化等を行う。」との記述も見られる。さらに、評価に関する箇所で、「東京大学の基本理念と長期的目標を具現化する自己点検・評価システムを確立する。」と「システム」の文字が見える。その他「ホームページや学内外広報誌等、多様な広報メディアを活用して広報活動の充実と活性化を図り、これらを統合するメディアミクス機能の強化を目

指す。」「総合的学術情報システムの構築に関する具体的方策」等、ITに関する記述は随所に記載されている。それぞれの中期計画推進の為の組織体が設置されているはずで、これらの中期計画は国立大学法人法第30条2項に基づく「中期目標」に対応していくものである。

本学においても全学教育研究施設として該当する機構が設置され、学部間に跨る全学的課題の為の情報化推進組織が設置されている。機構長がCIOであり、3名のCIO補佐が任命されている。また、全学的な情報化に関する課題に取り組む為、情報環境整備を担当する委員会と情報セキュリティに関する諸事項を担当する委員会が設置されており、教員・事務職員双方から選出された委員により、共同活動が進められている。ただ、教員と職員（事務系職員と技術系職員の総称）とには、その使命・職責・人事評価方法等に違いがある点、注意が必要である。本研究開始当時の本学における、それぞれの組織の特徴は次の通りである。

a. 教員組織の特徴　：

(a) 教員は基本的に専門領域に限定して活動している。（業務運営に関して、大学全体のマネジメントを意識しない場合もある。）また個人の業績に対して評価を受ける。

(b) 個々の教員の自立的な判断が尊重され、意思決定過程では多数決による決定より議論を尽くして合意形成を計るのが基本的な姿勢である。従って組織としての意思決定に時間がかかる。またトップダウンによる指示命令を全構成員に説明して周知するのにも、時間を要する。

(c) 大学の基本的な方向性や政策は、通常教員組織による委員会が決定する。ただ、法人化以後事務職員を含む委員会組織が見られ、少しずつ状況が変わってきている。

b. 事務組織の特徴　：

(a) 事務職員は、決められた業務（与えられた職責）を消化することに専念しており、企画や改善を積極的に実施する姿勢にはならない場合が多い。業務は組織的に遂行され、トップダウンでの指示命令は全体に行き渡る組織になっている。

(b) 法人化以前は、文部科学省の指示（指導）に基づき業務を進めるのが是であり、自ら他部署との意見交換をして企画し改善する習慣はあまり付いていない。ただ、法人化以降、業務の効率化や最適化が求められる中で、少しずつ変化してきている。・・・「文部科学省行政効率化推進計画」[19]（文部科学省）及び「独立行政法人等の業務・システム最適化実現方策について」[21]（文部科学省高等教育局の事務連絡）参照

(c)教員が自分で獲得してくる外部資金の用途に対して、原則口を挟めない。もちろん大学法人としてのルールに基づいて運用されることが大前提である。

先に述べたように、形式上組織面ではギャップを埋める体制ができつつあるが、構成員の意識面でも一本化された共同活動を実践する為には、組織運営上の配慮が必要である。

3.2.3 情報システムあるいは IT 化の状況

次に、国立大学の情報システムや IT 化の状況について、本学における情報システム構築・運用経験から、国立大学における情報システムの特徴を整理すると、次のような点を挙げることができる。これらは国立大学における IT 環境の統制の難しさを表している。

① 情報システム利用者の中に未成年者を含む学生がいて、情報システム管理(ライブラリ管理、データ管理、アクセス管理、等)の責任の所在が曖昧であったり、明確にすることが困難な場合がある。学生の利用は、原則当該学生を指導する教員が責任を持つこととなっており、責任者がいないわけではない。

② 学外からのアクセスや個人管理機器の持込みは可能である等、基本的に開放的である。

③ 統一になじまず、個性が重視される情報システムがある。(研究に関する部分)

④ 学内各部の必要に応じて IT 化が推進されてきた結果、開発方法やプログラミング言語等が不統一である。学内開発の情報システムには、ドキュメンテーションが不十分な為、開発者しか当該情報システムの改修や保守が出来ないケースがある。

⑤ 業務や情報の流れ全体を把握できる資料がない。

・各部署における職務分掌は文章(文字)で記述されている。

・業務手続きや手順を図示する習慣がない。

⑥ 法人全体の中で、各学部にある情報システムについて、掌握できていない。

学内情報システム全体を管理する仕組みがない。

国立大学はその発足以来学部の自治や独立性が維持されてきた。ITに関しても同様に維持・管理されてきた。このような歴史的な理由から、さまざまの情報システムをCIOのもとで一元管理しようとしても、全学にどのような情報システムが存在するのかを一覧できる資料も無く、各学部・各学科(極端な場合は研究室)に問い合わせないと把握できないケースが多い。また、各学部・各学科(極端な場合は研究室)に問い合わせても、その問い合わせの意義を十分理解してもらえず情報提供を拒否されるケースもあり、まさに「意識ギャップ」に困る場面もある。また、技術が日進月歩で変化し、情報システムもどんどん複雑化

する中で、予算要求及び執行の妥当性を(会計担当者による)会計面のチェックだけでは、二重投資や経費の妥当性を確認することには無理がある。入札による外部発注案件については、審査委員会の設置等制度が確立されているが、外部資金により学部独自に導入される中小規模の案件や内部で開発される案件については、システム面での妥当性を第三者により確認する制度が確立されているとは言いがたい。この点について、図3-1「現行の情報システム導入手続きイメージ図」を使って補足しておく。この図は、一般的な情報システムが学外から調達される際の手順の概略を表している。図の左下の「導入担当者」が起案した情報システムは「導入責任者」を通して予算が確保され、「予算責任者」の承認のもとで予算執行される。仕様策定委員会等において作成された仕様書により「契約担当部署」を通して学外委託先が決定される。対象となる情報システムによって、入札が必要な場合や不要である場合等さまざまであり、状況によっては学内教職員自らが開発して導入される場合もある。ここでは入札により調達される場合を図示している。予算執行の結果は、図の上部に記載されている「経理担当部署」に報告される。ここで注意すべき点は、起案部署・経理担当部署・契約担当部署それぞれの関心事が異なる点と、起案部署の予算執行権限が部局(学部)ごとに与えられている点である。即ち、起案部署では当該案件の機能・金額・作業条件を全て把握しているが、契約担当部署では作業条件、経理担当部署では金額、と確認の責任範囲が限定されていることである。ここに、類似の情報システムが複数の部局(学部)によって導入される可能性・危険性が潜んでいるのであり、大学全体を展望した上で、機能面(特に、情報システムの外部仕様たる機能面)の重複を検出する仕組みが必要なのである。

2 部局間を例にとって説明した図表が、図 3-2「2 部局間の情報システム導入手続き関係図」である。A 学部で A システム、B 学部で B システムの導入が計画されたとき、現行の手続きでは、両者の機能が酷似していても両方ともが導入される可能性があるといえる。学部単位の予算を持ち、学部単位に予算を執行していく中で、情報システムへの投資案件の内容をシステム面から細かくチェックし、学部間での重複や類似システムの開発、あるいは開発方法の妥当性をチェックする仕組みが必要である。

3.3 国立大学法人 IT 化の課題

3.3.1 IT ガバナンスという課題

さて、「全学的な視点に立ったトップダウンによる意思決定の仕組みと全学一体運営」を求められている国立大学法人においては、学内に散在する多くの情報システムを統一的に管理することが必要で、その為には全学的な調整や統制が重要であり、いわゆる「IT ガバ

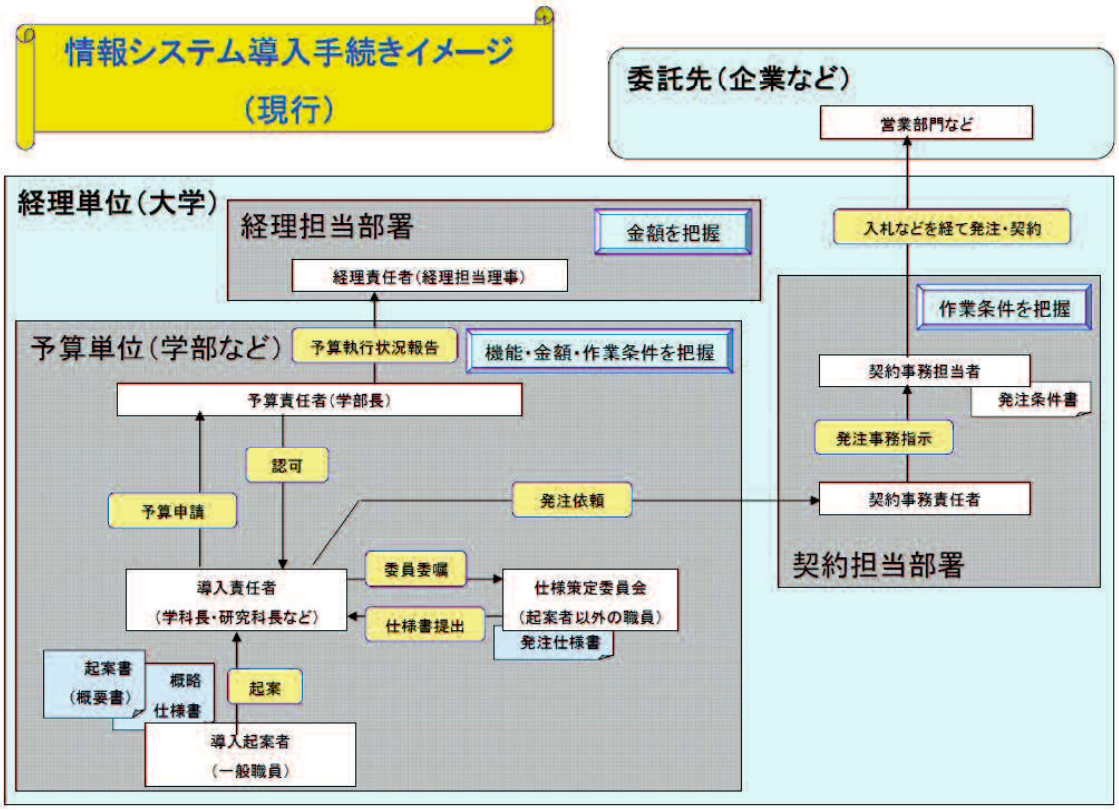

図 3-1　現行の情報システム導入手続きイメージ図

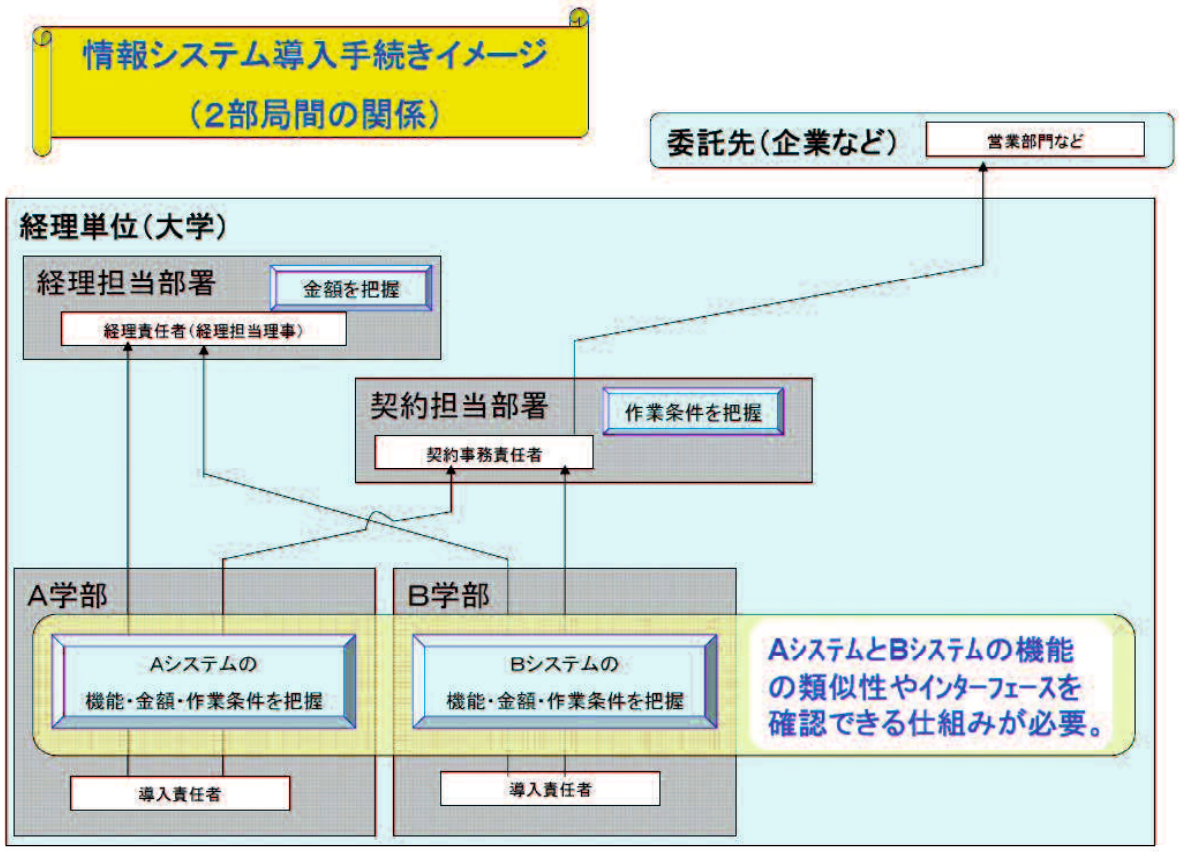

図 3-2　2部局間の情報システム導入手続き関係図

ナンス」が重要なのである。その為には「学内情報システムを掌握する仕組みの確立」が必要である。学内には既に多くの情報システムが構築されており運用されている。それらのほとんどは各部局ごとに維持管理されているものであり、設計思想や構築手法もさまざまである。プログラミング言語もさまざま、利用されているオペレーティングシステムやミドルソフトもさまざまである。類似システムが、学内に複数存在するケースも見つかっている。国立大学法人の中で稼動する情報システムを掌握できていない状況では、むしろ「学内情報システムを掌握する仕組みの確立」のほうが「既存情報システムの統合」に先行すべき課題であるが、必ずしもその仕組みが確立されているとは言えない。とりわけ学内開発の情報システムに関しては、そのほとんどを CIO に把握されていないことが表 3-1 からも分かる。表 3-1 は、2010 年度に実施した、国立大学法人情報系センターに対するアンケート回答の集計結果を表にしたものであり「CIO の方は、学内で運用されている業務情報システムをどの程度把握なさっていますか？」という質問への回答である。もちろん大学によって状況は異なる。某大規模大学の CIO の方の「各部局に任せれば良く、大学全体で管理する必要はない」という意見がある一方で、中規模大学の情報系センター長の中には「なんとか把握できる方法がないかと苦慮している」という方もある。別の単科大学の情報系センター長は「うちでは私の手元で全て把握できている」と述べている。表 3-1 や他大学へのヒヤリング状況から、必要性を感じつつも全学の情報システム全てを把握できていない大学が少なくないと考えられる。もう 1 つの課題は「情報システム維持管理体制の一元化」である。学内各部局によって維持管理されている情報システムもあれば、教員個人で管理されている情報システムもある。また、法人化以前より文部科学省主導で維持管理されてきた所謂「汎用システム」もある。「汎用システム」については、その維持管理を各国立大学法人に任せていく

表 3-1　CIO の学内情報システム把握状況

項目	回答数	比率
A. 全システムを把握	8	14.0
B. 内部開発以外を把握	12	21.1
C. 外部資金や内部開発は把握しているがそれ以外は把握していない	0	0.0
D. 入札による情報システムのみ把握	6	10.5
E. 情報系センター調達分のみ把握	11	19.3
F. その他	16	28.1
G. 無回答	4	7.0
計	57	100.0

方向と決まっており、個別の国立大学法人としての維持管理体制を確立するよう求められている。これら学内 IT 環境全般にわたり維持管理体制を一元化することによって重複開発を避けるとともに、維持管理に必要な知識・技術の蓄積により、より一層の効率化を推進すべきである。

3.3.2 コード体系の統一

情報システムを統一的に管理する上では、もう 1 つ「コード体系の不揃い」という問題がある。次に、この点について説明する。近年のオープン化やマルチベンダー化が進み、種々雑多の既存システム間の情報交換の機会が多くなるにつれ、プログラミング言語や DBMS（データベースマネジメントシステム）の種類の統一はほぼ不可能である。また、インターネットの普及により、学内外の多くの情報システム間でデータ授受が発生するとともに、学外者を含む不特定多数の人が情報システムにアクセスする機会が増加している。このような環境のもとでは、多くの情報システム間を行き交うデータの均一性がより重要になる。とりわけコード体系の標準化が大切である。大学内の情報システムについても、従来部局ごとに開発されてきた情報システム間でデータを一元的に取り扱う際に、このコード体系の違いが障害となっている。1 つの例をあげて見たい。複数学部を擁する総合大学において、7 学部に 3 種類の教務システムが存在した事実がある。コード体系が異なること、各業務システム処理用のサーバが各学部事務室にあって管理責任が各学部事務担当部署にあること、さらには扱うデータが個人情報を多く含む為データ管理担当部署外に提供しにくいこと、等が要因となって、情報システムとしての一元化（統一）も困難なものになっており、CIO の一元

表 3-2 情報システムと学部コード

項番	システム名称 / 学部	教務システム	授業料システム	財務会計システム	備考
1	教育学部	07	07	0107	
2	教育学研究科	07	81	0281	
3	人文学部	10	10	0110	
4	人文学研究科	10	80	0280	
5	経済学部	17	17	0117	
6	経済学研究科	17	82	0282	
7	理学部	22	22	0122	
8	理学研究科	27	75	0275	
9	工学部	25	25	0125	

的管理下におくこともできない状況がある。もう 1 つの例は学部コードである。学内の多くの情報システムでキー項目となる基本的なコードであるにも拘わらず、業務システムによって異なるのである。各業務システム間で、データを授受しようとする際に都度コード変換の処理を必要とすることが容易に判る。表 3-2 に具体的なコード例を示す。この状況のなかで、業務システム相互のデータ授受において、必ずコード変換が必要になり、学部や研究科を新設した場合には、業務システムごとの「学部コード」を付番する必要がある。しかも、業務システムごとに管理部署が違う為、コードを新設するつど関係部署の担当者が会議を開いて検討しコードを決定していく手間が必要となる。これらの問題は、学内においてコード体系を一元的に管理し統制する部署がないことに起因している。

3.4 初期届出制度

3.4.1 コンサルティングチームの設置

学内情報システムを一元管理する為には、学内に導入される情報システムを、定められた部署に必ず届け出てその内容を一元的に把握できる仕組みが必要である。本学では、学内における情報システム導入計画時に、学内に設置されている情報基盤整備委員会（学内情報基盤の整備を統一的に担当する全学委員会）に届け出るとともに、コンサルテーションを受けるようにする初期届出制度を構築・運営してきた。大学全体として整合性を保ちつつ効率的で安全な IT 化を進めることを目的とするものである。情報基盤整備委員会は、教員・事務職員双方が協同で学内の情報化推進や情報基盤整備について担うべく、国立大学法人化に際して設置された全学委員会であり、附属病院を含む各部局から選出される委員で構成される。各部局の長により、当該部局の情報基盤を任すことができて全学的視野で意見を出せる教職員が委員として選出される。教員と事務職員の混成委員会であり、教員の視点からも事務職員の視点からも意見を出せるよう配慮している。既に学内で稼働する情報システムについても、適宜届け出ることとした。部局を跨ぐこのような制度は、国立大学法人法第 11 条に基づく学長と理事による強力な権限の下で実施可能となったもので、学校教育法に基づく（各学部の）教授会が大学の中心的意思決定機関であった法人化前には実現されなかった。学部を跨ぐ協議と調整に多大な時間をかけなくても大学としての意思決定（合意）ができる。

図 3-3 の朱書破線の部分以外の部分は、情報システムが学外から調達される際の従来の一般的な概略手順を表している。仕様面でのチェックが学部内に閉じていることが判る。届出制度下では、情報基盤整備委員会のもとの WG として図中右下のコンサルティングチームを設置する。このチームは全学的視野に立ってコンサルテーション活動を行う。この活

動により、予算配賦の時期とは関係なく、全学的見地に立った仕様検討がなされる。「3.3.2　コード体系の統一」の関しても、対象となる情報システムのコード体系を可能な限り標準化に向かうよう方向付けをおこなう。。

コンサルティングチームは、大学の業務の分類（教育・研究担当、評価担当、ネットワーク担当、データベース担当、業務運営システム担当等）に対応する4つの専門部会から構成し、メンバーは教員と事務職員の双方から選出される。業務運営システム担当専門部会は教員 1 名のほかは事務職員・技術職員、他の専門部会は教員主体で、それぞれ数名から構成される。案件ごとの分担は各専門部会の部会長・副部会長から構成される専門部会調整会議で調整の上決定される。各専門部会の担当分野を表 3-3 に示す。

全学一体運営の為に全学的視点で情報システムを構築するとしても、必ずしも全部局共通とは限らない。各部局の特徴を十分考慮した場合、個別に開発すべき場合もある。教材作成を支援するシステムでは、学部ごとに異なる機能が必要となると考える方が自然であろう。これらの事情については、コンサルテーションする側とこれを受ける側とのコミュニケーションを密にし、十分な検討を加えて対応することにより解決に向かうことができる。このチームは、導入起案者から見て IT に関する相談窓口となる組織であり、情報システム間の機能面での重複チェックを含めた部局間調整機能を果たす。もちろんコンサルテーション内容は記録として蓄積され、以後の情報システム導入計画時に参照できるようになる。これにより組織間と時間軸双方における類似の情報システムとの比較検討がなされ、CIO をはじ

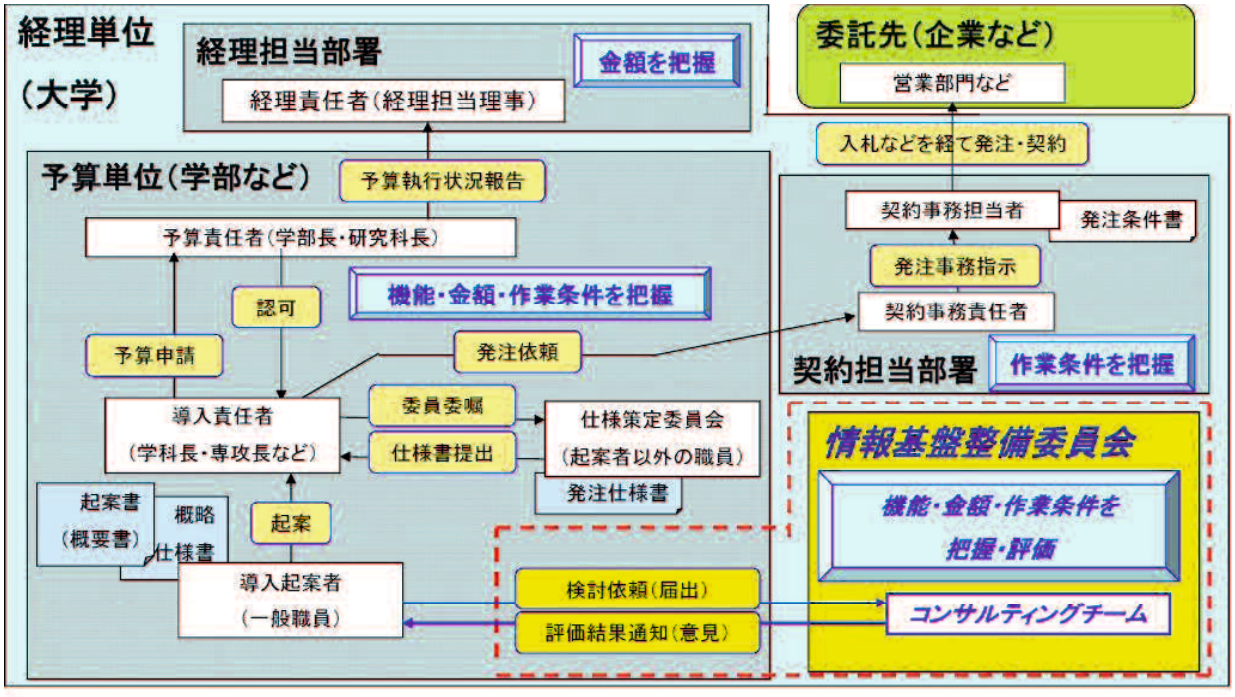

図 3-3：2 部局間の情報システム導入手続き関係図

表 3-3 コンサルティンググループの構成

グループ	担当
1. 業務専門部会	(1) 業務情報システムに関する事項
	(2) 認証・コード一元化に関する事項
	(3) 電子事務局に関する事項
2. 基盤専門部会	(1) 学内外のネットワーク・サーバの整備及び一元化、運用及び利活用に関する事項
	(2) 認証サーバの整備、運用及び利活用に関する事項
	(3) 研究用高速計算機環境の整備、運用及び利活用に関する事項
3. 教育・評価専門部会	(1) 教務システム及び教育支援システム関連の整備、運用及び利活用に関する事項
	(2) データベースシステム関連の整備、運用及び利活用に関する事項
4. コンテンツ専門部会	(1) 電子図書館の整備、運用及び利活用に関する事項
	(2) デジタルコンテンツの整備、運用及び利活用に関する事項
5. 専門部会調整会議	(1) It化に関する事項
	(2) 4専門部会間の定期的情報交換と調整
	(3) 4専門部会間共通事項

め大学経営陣は、当該委員会を通して学内情報システムの導入状況を把握し、導入前に大局的見地から意見を述べることが可能となる。コンサルテーションはチームメンバーの業務の 1 つとして位置づけて組織的に実施される為、従来の教育・研究の合間に個人的に対応するのではない。その為、コンサルテーションスケジュールの調整も組織的に行うことが可能である。コンサルテーションを受ける側の日程にあった対応ができるという利点がある。相談する側が従来の導入手続き前の予定にコンサルテーション工程を組み入れ、コンサルテーションの内容を記録し蓄積することで学内業務と位置付けている点、従来とは異なる制度である。類似機能を持つ情報システムの導入については、その開発を抑制するよう機能する点も従来の専門教員等の個人的対応と異なるところである。

3.4.2 届出対象とする情報システム

大学における各学部・各研究科にはそれぞれ特色があり、本来必要とする情報システムも異なる。一時的開発後、短期間のうちに廃棄する研究用の情報システムもある。これらまで全学的管理対象とすることは管理コストを大きくする弊害の方が多い。一方で、複数の学部・研究科に跨る分野の研究や教育の需要が多くなってきている事実もあり、これに伴って教務関連システムの複数学部間共通化の必要性は高くなっている。全学統一的な管理の範囲に含めるべき情報システムの範囲は、必ずしも学内で導入される情報システム全

てではないと考えるのが妥当である。本論文では、次のように、ある程度広範囲で継続的に利用される情報システムを届出の対象として、効率的な情報システム管理の実施を実現している。1研究室内で開発され運用される研究用シミュレータや研究室内業務情報システム等は対象外としている。

＜届出対象範囲＞

(1)　複数の学部・学科・研究室または課にまたがって利用される情報システムの導入

(2)　複数の部局等にまたがって利用される既存の情報システムの改変

上記届出範囲を含めた、初期届出制度における届出基準については付録 B を参考にして頂きたい。

3.4.3 初期届出制度の事務フロー

図 3-4 は届出手続きの流れを示したものである。まず情報システム導入起案者は届出書を作成して情報基盤整備委員会に提出する。情報基盤整備委員会（もしくは CIO）は、コンサルティングチーム内の担当専門部会にコンサルテーション開始を指示する。届出書の様式については付録 A を参照頂きたい。様式 1-1 と様式 1-2 に分かれており、ここでその内容について補足する。記入項目はいずれもコンサルテーション実施に必要な情報を記述するものであり、次の A、B、C の 3 種類に分類できる。この書類は、届け出る者が気軽に記入できることが必要であり、届け出ることを定着させることを優先する為、B、C の項目が未記入でも届出を受け付けるルールである。

A：届出事務手続きに関する情報・・・届出責任者名、届出者連絡先、情報システム導入希望時期、届出書の添付資料、検討結果（コンサルテーション結果）希望回答期限、等

B：情報システム導入計画に関する情報・・・導入計画名称、導入する情報システム名称、導入部署、導入責任者や導入担当者の連絡先、予算、導入費用見積、等

C:導入対象となる情報システムに関する情報・・・当該情報システムの機能概要、開発体制や運用体制、利用者、アクセス可能範囲、等

専門部会は届出書の内容を検討し、不足情報の入手を含めて適宜情報システム導入起案者（以下「届出者」）と打合せを行い、コンサルテーションを進める。学内外の関連部署との意見交換も必要に応じて行う。届出者や関係各部署との意見交換結果を受けて、専門部会としての意見をまとめて意見書を作成する。意見書については、付録 A の様式 2 を参照されたい。この書類は、コンサルテーションの結果を記載する為に作成するもので、届け出られた情報システムの仕様に関する意見や、その情報システムの導入計画に関する意見を記入する。届出書と重複する項目もあるが、コンサルテーションを通して変化する可能

性に配慮して、届出書及び意見書の両書類に記入する様式となっている。意見書はコンサルティングチーム内各専門部会代表者の審議と情報基盤整備委員会の審議を経て、届出者に送付される。コンサルテーションの過程で、過去の事例や他部局の事例との比較検討を行って類似の情報システムがないことを確認し、また学内ネットワーク接続上の課題や個人情報保護上の課題を中心として、情報セキュリティ面での問題の有無を指摘する等、情報システム導入計画の完成度を向上させる。情報セキュリティ面で解決すべき課題がある場合には、情報セキュリティ委員会に諮ることで解決する。この書類に記載された意見を導入計画に反映する(意見を採用する)かどうかは、予算執行権限を持つ届出責任者(あるいは導入責任者)が判断する。複数部署から同様の届出があった場合には、当該部所との調整が必要となる。情報システム導入が完了した時点で、届出者は図 3-5 に示すように、

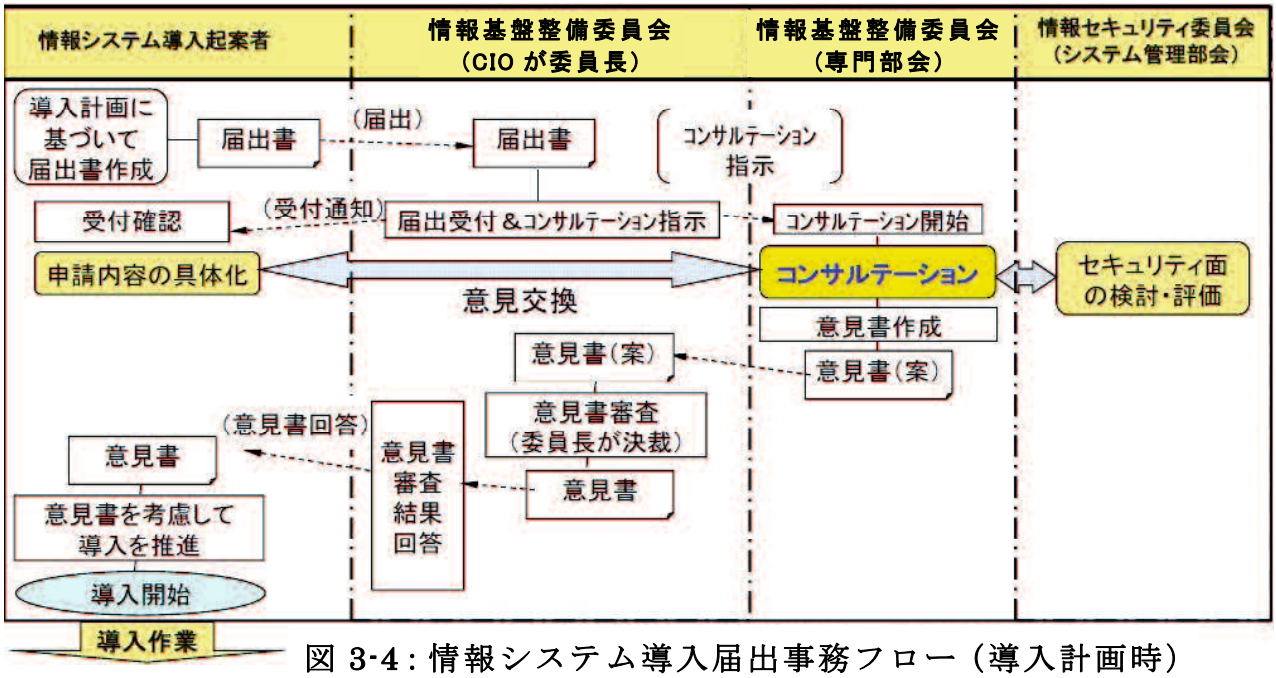

図 3-4：情報システム導入届出事務フロー（導入計画時）

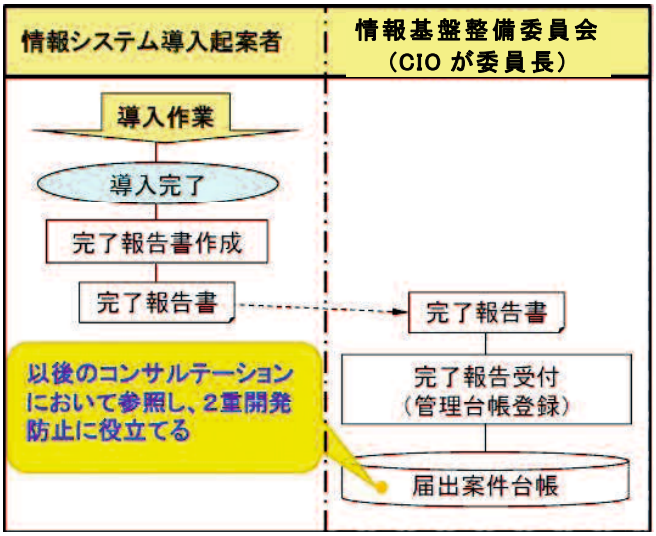

図 3-5：情報システム導入届出事務フロー（導入完了時）

導入結果に関する情報とともに完了報告書を提出する。導入計画を中止した場合は、中止することを決定した時点で、導入を中止した旨記入して完了報告書を提出するルールである。完了報告書については、付録 A の様式 3（様式 3-1、様式 3-2、様式 3-3 の 3 様式。）を参照されたい。 様式 3-1 が導入完了の事実を報告する為の書類であるが、導入計画の実施内容を記した様式 3-2 や、導入した情報システムに関する内容を記した様式 3-3 を添付して提出する。これにより、その後のコンサルテーションに向けた参考資料が蓄積される。届出案件が増えてコンサルテーション実績を蓄積し参照できる情報が整備されていくことにより、さらにコンサルテーション内容が充実していくことを目的としている。図 3-4 及び図 3-5 では、届出書や意見書は書類のイメージで記載しているが、これらは教職員が自席から Web ページに入力することを可能としており、入力データはデータベースに蓄積される。これにより、学内教職員による届出案件の状況の閲覧を可能にして学内情報共有を図っている。図 3-5 における届出案件台帳（データベース）を Web ページで学内教職員が自由に参照できるようにすれば活用の幅が広がり、届出者自らが情報システム導入計画時に類似システムの有無を確認することも可能である。届出案件に関する届出者と専門部会との間の連絡等の事務処理は、情報基盤整備委員会を所掌する事務部門の事務職員が実施している。

3.4.4 情報システムライフサイクルと初期届出制度

一般的に（いわゆるウォーターフォール型開発の場合）情報システム開発は図 3-6 のような工程に分けられ、当コンサルテーションは、図中の企画プロセスの一部に該当する。業務上、導入要求が出た情報システムは、導入に係るコストや導入プロジェクトの体制をはじめ、企画プロセスの初期段階としてその必要性や有益性を検討する為の作業が開始される。このプロセスでは、①情報システムへの要求事項を整理しまとめる「要求定義」、②要求内容を実現する為の基本的なシステムの構造、③導入する為の費用、④導入プロジェクト体制、⑤導入後の保守・運用の体制等が検討される。このプロセスの最終段階で導入の可否が判断される。新たな情報システムを開発するのか、既存の情報システムを活用するのか、活用する際に改造が必要なのかどうかについて判断するのも、このプロセスである。開発プロセスでは、具体的な導入プロジェクトを発足させ、導入に向けた実際の活動を推進することになる。業務処理設計、機械処理設計、運用設計、性能設計、信頼性設計等の設計工程のあと、新たに開発する場合や改造を伴う場合には、製造工程を伴う。プログラムの設計・製造、ハードウェアの調達、システムテスト、運用訓練、システム操作教育、データ移行等を経て、システムの運用開始の可否を判断して、運用プロセスに入る。運用プ

ロセスに入ると同時に、システム不良対策や性能向上、あるいは小さな仕様変更対応等の保守が必要となる。従来、これらのプロセス全体が各部局ごとに実施されていた為、他部局で類似の情報システム導入があっても、予算さえ確保できていれば問題にならなかったと考えられる。これらの導入プロセス全体のなかで、届出制度では、企画プロセスの段階で学内全体の状況を検討対象に加えることを可能にする。この段階でコンサルテーションの一環として他の情報システムの状況を検討対象とする為には、過去に導入された情報システムの現状を把握しておく必要がある。言い換えると、導入される情報システムについては、以後のコンサルテーションに備えて、正確な情報を蓄積しておく必要がある。一方、情報システムは運用直前にならないと、その形が確定しない。情報システム導入プロジェクトにおける曖昧性とか不確実性といわれるものである。そこで、運用開始時点（即ち導入完了時点）の状況を「完了報告」として届け出る仕組みとしている。初期届出制度は、情報システムの導入プロジェクトを各部局が責任を持って推進あるいは実施するという従来の予算執行の仕組みを維持しつつ、全学の状況をみて最適な導入に向けた検討が導入プロジェクトの早い段階でなされるよう配慮しており、届出書、意見書、完了報告書、廃止届の 4 種類の文書を使用する。これらと情報システムのライフサイクルとの関係を図 3-7 に示す。これらの届出により、情報基盤整備委員会は情報システムの誕生（導入及び運用開始）・更新・消滅（廃止）の事実を把握する。個別の情報システムの、構成管理・変更管理・プロジェクト管理・リリース管理・キャパシティ管理・セキュリティ管理等、ライフサイクル全般における維持管理については、図 3-3 中における導入起案者と維持管理部署において実施される。届出の為の文書にはコンサルテーション実施に必要な情報が記入されており、全て届出案件台帳（データベース）に記録される。実際の運用においては、届出は紙媒体ではなく

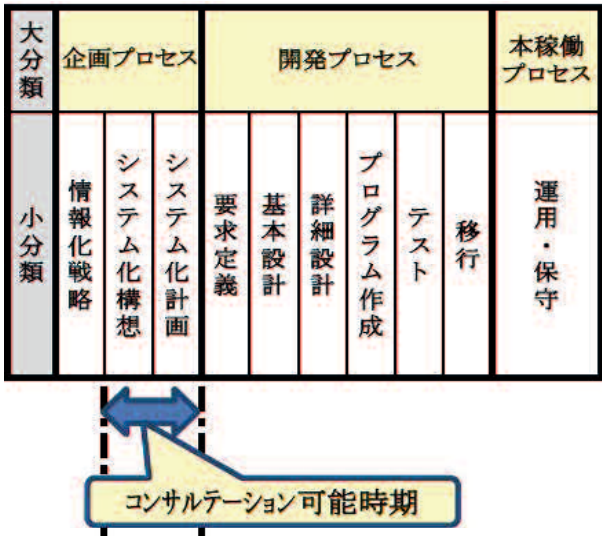

図 3-6：情報システム開発工程（ウォーターフォール型開発の場合）

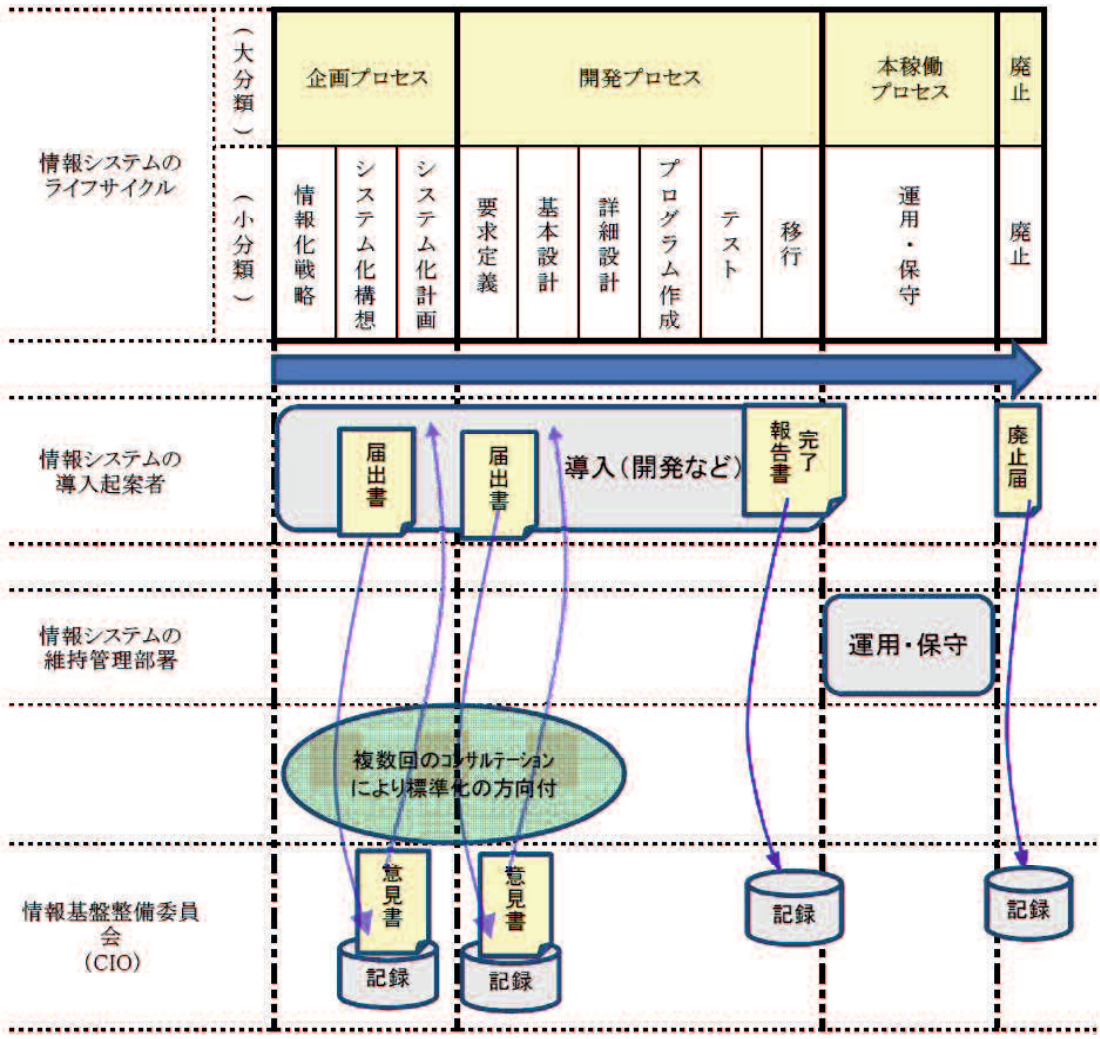

図 3-7　情報システムのライフサイクルと届出

Web ベースの届出案件管理システムにより、学内ネットワークを通して行われる。これらの情報は、もちろん届出案件のコンサルテーションに利用されるのであるが、当該情報システム導入以後の別の届出案件においても参照される。

3.4.5　初期届出制度の効果と課題

3.4.5.1　情報システム届出による効果の事例

ここで、届出事例として「M 管理システム導入計画」を紹介する。（ここでは管理対象物を便宜上 M と表現する。）本学における M の管理は従来から各部局に任されており、さまざまの法令に基づく大学全体としての各種報告書の作成に苦労していた。届出制度開始後、担当教員が（他大学から無償提供された）M 管理システムを導入して作業の効率化しようと検討を始めた。発生源データ入力の仕組みにより学内他部局を巻き込んだ情報システム導入になる為、相談したい旨の要請（届出）があった。届出に基づき全学的視野でコンサルテーションを実施し、学内の関連業務やその為の業務処理システムの状況を調査したところ、次の課題が見つかった。（M はある種の物品を表している。）

(1) 情報システム導入以前には、全学統一の M の管理がなされていない。

(2) 届出をした部局以外にも、届出案件とは別の M 管理システム（有償）の導入予定があった。

(3) 導入対象となる M 管理システムの運用体制が不明確である。

(4) 導入する情報システムの運用にあたり、求められる情報セキュリティ対策が不明確である。

そこで、情報システム導入以前に全学規模の M の管理業務を整理するよう助言した。届出があったことにより、全学的規模での業務の見直しが開始され、前述の各課題それぞれが次に述べる改善に向かった。

(1) に対しては、全学統一 M 管理は、大学全体の課題として全学委員会で検討が進められることとなった。

(2) に対しては、他部局の他システム導入との 2 重投資を防止する為、一本化に向けて調整が進んだ。

(3) に対しては、M 管理システムの運用体制については、業務形態確定後、全学一体運営の中で統一的な運用がなされるよう方向付けられた。

(4) に対しては、情報セキュリティ対策についても大学全体の情報セキュリティポリシーに沿った情報システムとなるよう、 M 管理システムの仕様の見直しがなされた。

3.4.5.2 初期届出制度の効果

本論文記載のような制度は国立大学では他に例を見ないと考えられるが、本学では実際に運用を開始しており、2010 年 12 月末日現在で 100 件の届出を受けている。そのうち 70 件についてコンサルテーションを実施している。他の 30 件は、制度開始前から運用されていた情報システムや、単なるアプリケーションソフト購入等の届出案件である。制度の学内周知とともに届出案件も増加し、それとともに、学内の情報システム名やその管理者が DB に蓄積され、CIO が把握する情報システムの範囲も増加していった。また、学内の IT の専門家によるコンサルテーションを受けることで、個別案件のもつ課題が指摘され改善されることも多い。初期届出制度により課題が解決された事例を挙げる。

(1) ユーザ認証の仕組みを独自に持つ業務システムの導入計画において、当該情報システム導入起案者はユーザ管理の作業量を認識していなかった。コンサルテーションにより、不要なユーザ管理作業の発生を回避できた。

(2) 導入予定の情報システムではファイヤーウォールへの配慮がまったくなされていなかったが、情報セキュリティへの配慮不足をコンサルテーションにより補うことができ、情報

セキュリティ事故の芽を摘み取ることができた。

(3) 高い可用性を求められるサーバであるにも拘わらず、事務机横の事務用電源からの電力供給で当該サーバを運用すれば良いと安易に計画していた。無停電電源装置の設置の必要性を指摘し、しかるべきサーバ室へ設置する計画に変更した。

従来のように情報システム導入計画が担当部局の中で閉じていたならば、IT に関する知識不足に起因する情報セキュリティ事故や 2 重投資になりかねない案件が、初期届出制度によって、未然に防止できている。この点が初期届出制度の効果である。

3.4.5.3 初期届出制度の課題

多数の情報システムについての届出を通してコンサルテーションがなされていたが、個人情報を取扱う情報システム以外については、「届出」が任意であり導入を計画する側が不要と考えると届出がなされない場合がある。情報システムの導入計画時にコンサルテーションを義務付けることやコンサルテーション技術向上の為の継続的努力等も必要である。

また、届け出られる情報システムの背後の業務手順の変更なくして情報システムの改善が出来ない場合等もあり、届出者との円滑なコミュニケーションの為にも、業務に関するある程度の業務知識を習得することも課題である。さらに、急速な IT 発展の中でコンサルテーションチームが常に知識・技術の向上を求められる点は、苦労する点でもあり、避けて通れない課題でもある。

コンサルテーショングループには、次のような指摘も少なからず寄せられていた。

- 届出手続きが煩雑である。
- 技術者の立場で書類が作られていて、ある程度 IT の知識がないと記入できない場合がある。一般ユーザでも記入できる様式にできないかどうかを検討すべきである。

これらも初期届出制度における課題であり、3.5.1 節に述べるような改善（制度改正）を実施することにつながった。

3.4.6 届出の義務化と届出制度の改革

3.4.6.1 情報セキュリティ事故対策の必要性

2010 年 9 月に、海外からのサイバー攻撃によって学内研究室のホームページが改竄される事故が発生した。当該ホームページを表示する情報システムは初期届出制度下での届出はなされておらず、情報セキュリティ技術には疎いがホームページ用のサーバ運用の能力を持つ教職員が作成したものであった。本人了解のもと当該サーバを即日学内ネットワークから遮断する対応がなされ大事には至らなかった。当該サーバ管理責任者、学内ネ

ットワーク運用担当者、CIO がすぐに相互に連絡し合えたという好条件があって即応出来たものである。このことから次の情報セキュリティ対策の必要性が判る。

(1) 稼働する情報システムの管理責任者の緊急時の連絡先を CIO が把握していること

(2) 教職員への情報セキュリティ教育、特にインターネットの脅威への対策に関する教育

(3) 充分なセキュリティ対策の実施、または対策が充分なサーバ等の安全な稼働環境への移行

(1)項は初期届出制度を活用して届出を義務化することで実現できる。(2)項のうち一般的な脅威や対策については専門家による学内講習会を実施することで対応できる。個別情報システムごとの事情に配慮した情報セキュリティ対策に関する教育（あるいは指導）は初期届出制度におけるコンサルテーションの仕組みにより対応可能である。(3)項についてもコンサルテーションの過程で、より良い方向へ誘導できる。

届出制度が求められる理由はもう 1 つある。企業を含めてすべての組織に求められている内部統制である。あずさ監査法人パブリックセクター本部は、「国立大学法人の内部監査」[3]の第 3 章で「国立大学法人においては（中略）内部統制構築の責任に関する法律上の規定はないが、学長（総長）または役員会といったマネジメント層に責任があると考えるのが妥当であろう。」と述べ「組織のマネジメントは、常に内部統制が有効に整備され、かつ有効に機能しているかどうか把握するよう努めなければならない」としている。CIO の統制活動と内部監査等の監査活動において、学内情報システムの状況を網羅的に把握する為の手段として、届出制度が必要となる。

3.4.6.2 届出制度義務化の必要性

初期届出制度が学内情報システムの改善に役立ったことを述べ、届出が任意であることから効果の範囲が限定されることや無届出情報システムにおいて情報セキュリティ事故の可能性があることも、既に述べた。初期届出制度には、次の改善を加えて網羅性を高め、必要に応じてコンサルテーションを実施することによって学内情報システム全体の安全性や信頼性を高める必要があった。

(1) 情報システムの届出対象条件を明確にし、全ての対象情報システムの届出を義務付ける。届出義務化を周知した上で、無届出情報システムについて学内ネットワークから切断する。

(2) 情報システムの開発工程の中のどの時期（工程）であっても届出可能とする。また、稼働していない情報システムに関する相談だけの届出も受け付ける。

(3) 届出の単位を、導入（開発）計画単位から情報システム単位に変更し、1 つの情報システムについて何回でも相談や届出ができる仕組み（届出案件管理システム）とする。

(4) 情報基盤整備委員会の WG が、コンサルテーション実施対象案件の届出状況やコンサルティング状況を、定期的に確認して制度を根付かせる。

届出案件ごとの届出手順は第 3 章で述べた業務の流れの通りであるが、届け出るべき事項の中で、当該情報システムの責任者と緊急時の連絡先については記入必須項目となる。届出の義務化や無届出情報システムの学内ネットワークからの切断の可能性については、学内への周知徹底が必須である。実際の切断にあたっては、当該情報システムの管理者に事前に通知し、切断に起因する事故（2 次災害）の防止への配慮が必要である。ことはいうまでもない。

3.4.6.3 届出対象

届出を必要とする情報システムとしては、従来は「学内で稼働する情報システム」としていた。クラウド化やアウトソーシング等に配慮して、本学が稼働責任を担う情報システムを含める為、「本学の経費により借用して構築する場合を含め、教育研究ならびに業務に関わって本学で構築・利用される情報システム（コンピュータシステム）」と変更する。届出を義務化する為、学内ルールとしてオーソライズする。

届出案件の中で、個人情報等重要情報を含む場合や学外に向けて情報を発信している場合には、コンサルテーションを実施することとする。

3.4.6.4 改革前後の届出状況

本学では、2011 年初めより改定後の届出制度を運用している。事務組織を通じて全教職員宛届出義務化の学内ルール施行を通知し、運用開始 3 ヶ月後には講習会を開催して周知を図った。さらに、2011 年度前期には学内ネットワークに接続されている情報システムについて一覧表を作成し、各情報システムの管理者宛送付し届出を促している。図 3-8 に示す届出案件件数推移の中で、2011 年度後期の件数は 10 月 1 ヶ月間の件数であるが、これは学外ネットワークとの通信を許している情報システムについての届出期限を 10 月末に設定したことにより多くなっている。その結果、初期届出制度以降の届出件数の推移（図 3-8 参照）には、顕著な届出の増加が現れている。なお、2010 年度後期の 13 件のうち 2 件が初期届出制度下での件数である。

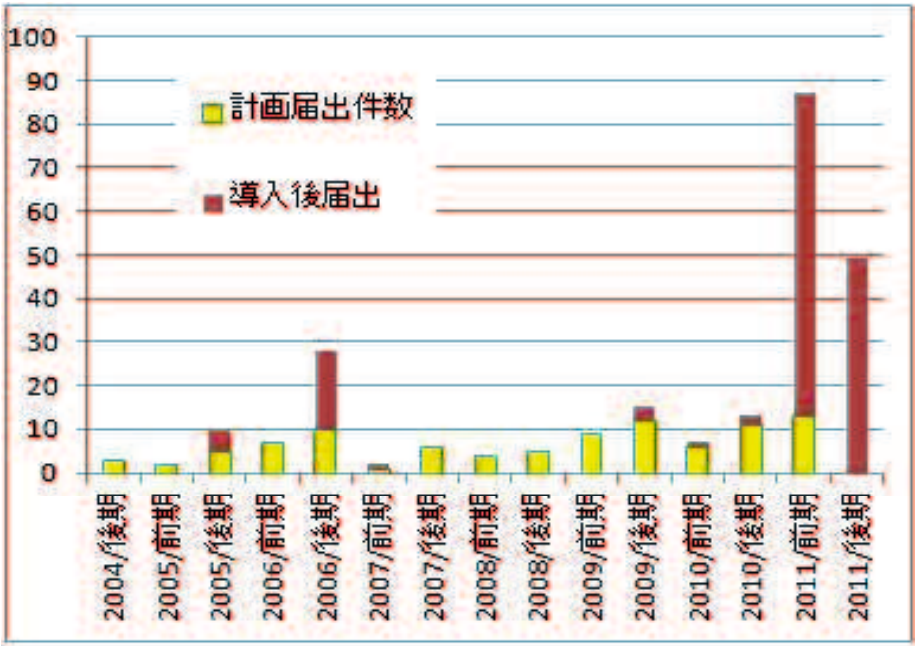

図 3-8　届出案件件数推移

3.5　情報システム届出制度

3.5.1 届出の義務化に伴う制度変更点

2010 年 9 月の情報セキュリティ事故対策として届出を義務化したことは 3.4.6 節で述べた。ここではこれらを含む、初期届出制度からの変更点について詳しく説明する。

(1) 情報システム届出条件の明確化……初期届出制度においては、複数部署で継続的に運用される情報システムを届出対象としていたが、学内周知が充分でなかったこともあり、各担当者において届出要否の判断に迷うこともあった。これを解消する為、届出対象となる情報システムの条件に関する講習会を開催して周知を図った。さらに、2011 年度前期には、前節でも述べたように、学内ネットワークに接続されている情報システムについて一覧表を作成し、各情報システムの管理者宛送付し届出を促している。届出対象となる情報システムの条件をより明確にする為、届出不要な情報システムを表 3-4 のように例示し、制度の主旨や届出方法に関する想定質問集をホームページで学内に公開することとした。

(2) 学外で稼働するが大学に稼働責任のある情報システムの届出対象への追加……近年のクラウド化の趨勢の中で、学外にサーバが設置される情報システムの増加がみられる。本学経費で導入される情報システムについては、サーバが学外にあっても大学の責任が無くなるものではない為、届出対象とした。

(3) 届出義務化の周知と、その上での無届出情報システムの学内ネットワークからの切り離し……届出が義務化されたことを事務文書として全学に通知した。その上で、学内ネ

ットワークの IP アドレスを付与しているコンピュータの中で、表 3-4 上で届出が必要とされる情報システムの担当者に対して、届出がない場合には学内ネットワークから切り離す旨通知して届出を促した。

(4) 組織の簡素化と届出案件審議の定例化……初期届出制度において複数の専門部会に跨る案件も多く、多人数の日程調整に手間取って会議招集が困難であった。そこで、コンサルテーションや審議の為の組織を簡素化した。委員会の下の 4 つの専門部会とそれらの間の調整会議を情報基盤検討部会（以下「部会」）1 つに統合して固定委員数を減らし、必要に応じて 専門知識を有する者を招聘することとして、活動し易くした。また部会開催を定期化し、毎月 1 回は必ず新しい届出案件を検討・審議するとともに、コンサルテーションの状況を確認するように改めた。

(5) 届出単位の変更……届出の単位を「導入計画」から「情報システム」に変更した。これは、CIO（もしくは CISO）が個別情報システムの管理者を把握し、情報セキュリティ面の指導や管理ができることを重視した為である。初期届出制度から追求してきた重複開発の検出は、部会やコンサルテーションの中で実施するよう変更した。

(6) 届出必須項目への情報システム関係者の緊急時連絡先の追加……異常を検知した個別情報システムを学内ネットワークから切り離したり停止させたりして他の情報システムに影響が及ばないようにする為には、当該個別情報システムの担当者との連絡が急務となる。その時に備え、緊急時連絡先を届出必須項目とした。それとともに、緊急時に責任ある判断を下せるよう、当該個別情報システムの責任者としては届出元組織の責任者の個人名も届け出るよう求めることとした。

(7) 届出書記載事項の簡素化……初期届出制度を開始するころは学内情報システムの数やそれぞれの特徴が明確ではなかった為、学内の情報の流れを把握するべく設計情報を届け出る仕組みとした。しかし、個別開発（プログラム製造等）を伴わない多くの情報システムでは設計情報を収集することに意味のないことが判ってきた。表 3-4 の項番 6 に分類されるものが典型例である。そこで、届出の際には気軽に届け出られることを優先する為、届出書記載事項を簡素化した。これら設計情報の多くを届出書から削除し、運用関連情報等の情報セキュリティ面で必要な項目を追加した。削除した項目については、必要に応じて適宜コンサルテーションの中で情報収集することとした。具体的な変更内容を表 3-5 に示す。初期届出制度において届出書により入力される具体的データ項目については、3.4.3 節及び付録 A を参照頂きたい。一方、義務化後の届出制度において届出書により入力されるデータ項目については、本学の Web ページに掲載されているが

学内限定公開となっている為、詳細(具体的なデータ項目)の掲載を割愛する。

(8) 制度運用方法の変更……その他、次の 2 点に関する変更を実施した。

a. コンサルテーション要否判断については、個人情報の有無や学内ネットワーク接続有無、あるいは届出情報の充足性等により、その必要性を部会で審議したのち、部会長が行うこととした。

b. 関連規則の改訂を行い、ホスティングやハウジングの利用条件に当制度での届出義務があることを追加した。

3.5.2 義務化後の情報システム届出状況

3.5.2.1 届出の概況

ここでは 2011 年 1 月の届出義務化以降の半年ごとの届出件数を表 3-6 に示す。またこれをグラフ化したのが図 3-9 である。届け出られた案件の中には、サーバ 1 台 1 台を届け出た事例や、教務システムのようにほぼ学内全構成員が利用する PC をその構成に多数

表 3-4 届出対象情報システム分類表

項番	情報システムを構成する主要機器	内容	利用(アクセス)範囲					
			学外公開	学内限定	事務LAN限定	研究室限定	病院LAN限定	ネットワーク接続無し
1	サーバ	個人情報有り	◎	◎	◎	○	○	○
2		個人情報無し(教育・業務用)	◎	◎	◎	○	○	×
3		個人情報無し(研究用)	◎	○	ー	○	ー	×
4	サーバ機能のない PC		×	×	×	×	×	×
5	共有ディスク		◎	○	○	○	○	ー
6	プリンタ・復号機		◎	○	×	×	×	×
7	学外設置サーバ		◎	◎	◎	◎	◎	ー

凡例	
	◎ :届出必要(原則、コンサル実施する)
	○ :届出必要(原則、コンサル実施しない)
	× :届出不要(原則、コンサル実施しない)
	ー :該当無し

表 3-5 届出書上の記載項目の変更内容

(1) 設計情報（削除項目）	
①	システム構成(ハード/ソフト、サーバ/クライアント)
②	費用関連項目(予算/開発費/資産計上額、等)
③	中期計画と導入との関連に関する説明
④	導入作業体制に関する説明
⑤	他大学や国内外との技術比較
(2) 情報セキュリティ上必要な項目（追加項目）	
①	ネットワーク関連情報(学外接続有無/通信プロトコル/IP アドレス、等)
②	取扱う情報の種類(個人情報/機密情報/知的財産、等)
③	ソフト開発者(市販/外部委託開発/学内開発、等)
④	利用時間/保守体制/緊急時連絡先

含むにもかかわらず 1 件の届出になっている事例等があり、届出件数と情報システム数あるいはサーバの数とが必ずしも一致しているわけではない点留意する必要がある。

2013 年 9 月末までの 3 年弱の間の届出総数は 516 件であり、このうち 125 件についてコンサルテーションを実施した。残る 391 件については、個々の情報システムの管理者をはじめとする諸事項を CIO が把握するにとどめた。2011 年 7 月からの 1 年に届出が集中しているのは、制度開始半年後に、学内ネットワークに接続している全てのコンピュータそれぞれの管理者宛、届け出るよう文書にて促した為である。2012 年 7 月以降は、新たに導入される情報システムを中心に届出がなされており、新たな情報システムを導入する際に届け出ることが習慣化されてきていることを表している。

表 3-6 届出件数

項番	期間	コンサルテーション有り	コンサルテーション無し	計
1	2011.1～2011.6	22	4	26
2	2011.7～2011.12	38	116	154
3	2012.1～2012.6	37	245	282
4	2012.7～2012.12	8	12	20
5	2013.1～2013.6	17	6	23
6	2013.7～2013.9	3	8	11
7	計	125	391	516

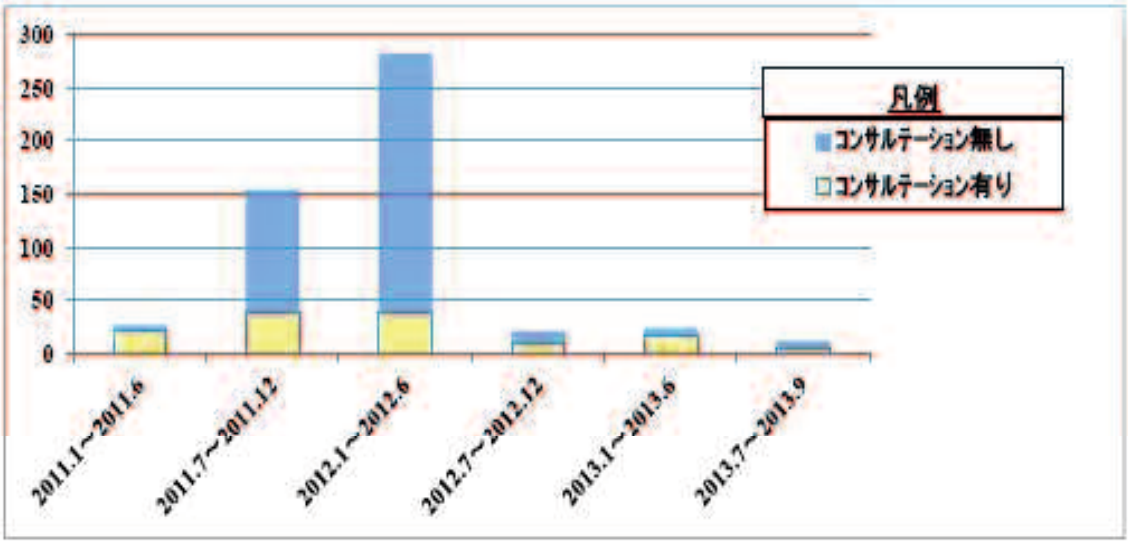

図 3-9　届出件数推移グラフ

3.5.2.2 コンサルテーションの概況

次に、コンサルテーションを通じて出された意見について述べる。125 件の届出に対する意見は合計 396 項目にのぼる。これは、各届出案件の意見書に記載された指摘事項や留意事項それぞれを 1 件と数え、全意見書に対する件数を集計した為である。大多数の場合、1 件の届出に対して複数の意見を記載している。表 3-7 は各意見（指摘事項や留意事項）を分類して集計し、その件数を表にしたものである。表 3-7 によれば、セキュリティ対策に関する意見が最も多く、認証に関する意見を合わせると 150 件(38%)にのぼる。当制度が情報セキュリティに力点を置いていることが判る。また、運用体制や連絡体制に加えて各組織の役割や責任の範囲を明確にするよう求める意見や大学全体の方針との整合性を求める意見も、91 件(23%)と多い。これは、各情報システムの維持管理をより確実なものにしたいとの委員会の意思の現れである。IT ガバナンスフレームワークのデファクトスタンダードとなっている COBIT[2]/[17]にいうドメイン PO（計画と組織）にあたり、いわば情報システムの開発や調達以前に実施すべきプロセスである。当該情報システムの導入計画段階で委員会から意見を出せることは意義深い。ここで COBIT について補足する。COBIT は Control Objectives for Information and related Technology の略である。情報システムコントロール協会(ISACA;Information Systems Audit and Control Association)と IT ガバナンス協会(ITGI;IT Governance Institute)が定めた IT ガバナンスの仕組みづくりを支えるフレームワークであり、デファクトスタンダードになっている。本論文では、Ver.4.1 を参考にしたが、現在では、Ver.5 が発行されている。COBIT では、組織における IT の活動を 4 つのドメイン（PO;計画と組織、AI;調達と導入、DS;サービス提供とサポート、ME;モニタリングと評価）に分けており、各ドメインはプロセスで構成され全体で 34 のプロセスを定義している。

ただ、COBIT は企業経営を想定しており、国立大学への適用にあたっては充分な検討が必要である。

これら意見の中で多くの届出に共通した意見内容は次の 4 点である。

①外注先を含む運用体制を明確にし、緊急時連絡先を明示的に届け出ること。(緊急時の停止可否判断をスムーズにする為)

②利用者の本人認証には、できるだけ大学推奨の認証方式を利用すること。(個別ユーザ管理による作業増を防ぐ為)

③サーバはできる限り設置環境の整ったサーバ室内に設置するか、情報系センター提供の仮想サーバやソフトウェアを活用して IT 資産増を避けること。(電力使用量削減を含むコスト削減の為)

④アプリケーション開発では、情報セキュリティ対策に充分配慮したプログラミングをすること。特に外部から入力を許可する場合には注意すること。(データ保全と情報セキュリティホール防止の為)

表 3-7 意見書記載内容一覧

項番	分類	意見内容	件数
1	組織	運用体制・連絡体制の明確化	55
2	役割分担	関係組織の責任分担の確認	20
3	全体最適	大学全体の方針との整合性確保	16
4	認証	本人認証の必要性や統一認証方式の採用	22
5	ｾｷｭﾘﾃｨ対策	アクセス制御、セキュリティ対策ソフト導入、データ保護、物理的セキュリティ、人的可用性、等	128
6	ｼｽﾃﾑ設計・開発	インターフェース確認、ドキュメント整備、テスト環境整備、等	30
7	ｾﾝﾀｰｻｰﾋﾞｽ活用	既存設備や学内サービスの活用による IT 投資削減	57
8	ｻｰﾋﾞｽ仕様確認	情報系センター等学内サービス部門との相談	35
9	手続き・手順	ルール遵守、手続き方法や書類の見直し	33
10	計		396

これらの意見書に記載された意見通りに導入や運用をする義務は明文化されているわけではない。コンサルテーション結果としての助言であり、直接的な強制力はない。意見を採用するか否かの最終判断は、届け出られた情報システムの管理責任部署によってなされる。しかしながら、意見書は情報基盤整備委員長(CIO 補佐)名で届出元に回答され、CIO の

意見を代弁し大学執行部の意向を反映したものとして扱われる。一方で、個人情報の管理に関する規則には個人情報を扱う情報システムの届出義務が明文化され、ハウジングやホスティング等の学内サービスも当制度の届出無しに利用できない規則になっている。従って万一意見に反することが要因となる事故が発生した場合には、対外的にも当該情報システムの管理責任者の責任として対処することになる。しかも、意見書はコンサルテーションを通じて届出元の希望や意向に配慮してまとめられるものであり、回答された意見を無視することは極めて困難でありまたその必要もない。当制度の優れた点である。

3.5.2.3 コンサルテーションの効果事例

届出の中では、重要な意見を出している事例もある。ここではおもな事例を 4 件紹介しておく。いずれも当制度がない状況下では得ることが極めて困難な効果である。

1 つ目は、1 学科の教育支援システムの為に新たなソフトウェアやサーバ(ハードウェア)を導入することをやめ、学内において既に提供されている既存サービスを利用するよう指導した例で、届出書と意見書を図 3-10 に示す。もし当制度が無ければ、学内に新たなサーバが設置されたと考えられ、管理コスト増や設置場所によっては空調を含めた電気使用量増を伴ったと考えられる。当制度により当該講義担当教員は Moodle 上の教材を作ることに専念できるようになり、サーバ設置や Moodle インストール等の作業が不要になった。ここで、Moodle について補足しておく。Moodle は学習管理システム (Learning Management System: LMS)あるいは学習過程管理システム (Course Management System: CMS)等と呼ばれる、eラーニングシステムの 1 つである。本学の Moodle サービスについては次の URL を参照されたい。http://www.cc.yamaguchi-u.ac.jp/guides/moodle/

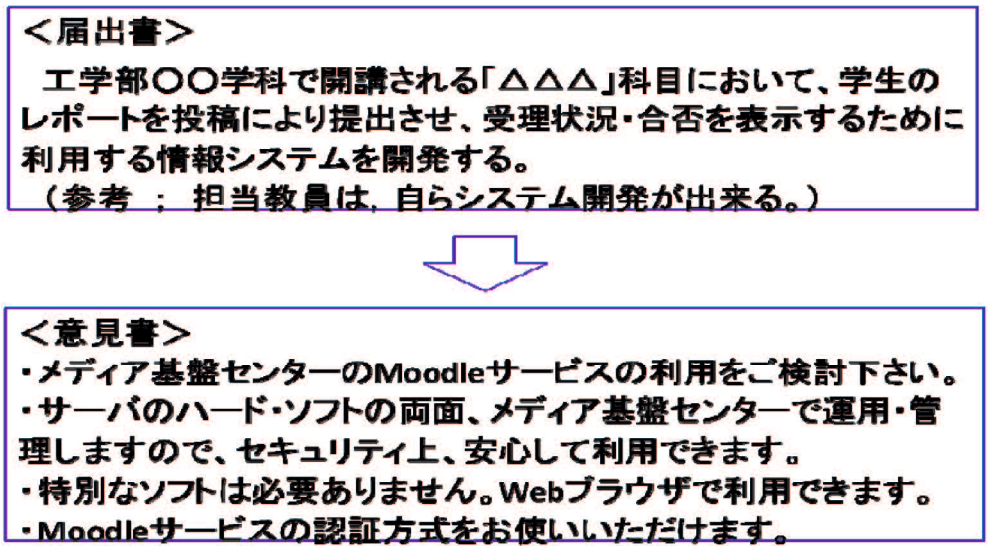

図 3-10 意見書例 1;Moodle 活用へ誘導

2 つ目は、部局における新たなデータベース(DB)サーバ運用作業を抑止しようとするコンサルテーション事例である。届出書と意見書を図 3-11 に示す。この案件では、届け出た部署において大学全体を対象とする既存 DB におけるデータ項目以外に必要とするデータ項目があり、これを補う為に新たな DB サーバを立ち上げ運用しようとしていた。大学全体としての DB に、届け出た部局が必要とするデータ項目を追加することにより、当該部局における新たなサーバ運用作業の発生を抑止しようとする意見である。この事例では、予算面から当該部局での個別 DB 構築を抑止できなかった。しかしながら、全学共用 DB への統合への働き掛けをしており、データ項目の共通化等将来の統合を可能とする DB 設計がなされる。もし当制度が無ければ、当該部局独自の DB が構築されて全学共用 DB とは別の新たなデータ構造となる可能性が極めて高く、当該 DB 個別の新たなデータ管理作業が発生していたと考えられる。

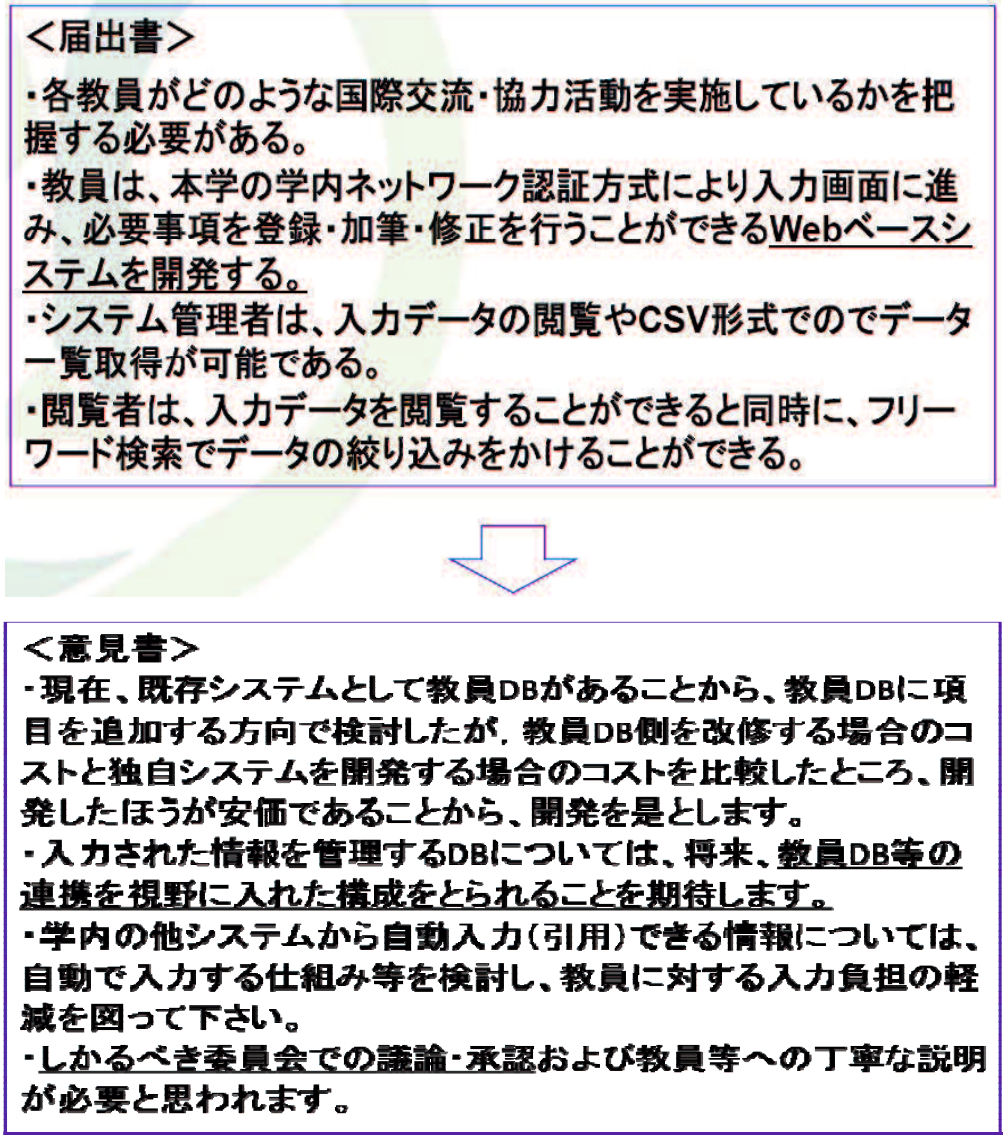

図 3-11 意見書例 2;既存 DB への統合を助言

3 つ目の事例は、情報システムの実運用環境と研究用環境を明確に分離するよう求める意見である。届出書と意見書の内容抜粋を図 3-12 に示す。大学全体の事業継続計画(BCP:Business continuity planning)を支援する情報システム研究の一部として、気象情報等を提供する情報システムを開発するという届出である。当該届出案件の主たる目的は危機管理システムの研究の為の情報システム導入にある。しかしながら、届け出られた情報システムは全学危機管理システム全体の完成に先駆けて運用に供され、BCP 発動根拠にもなりうる重要な気象データを提供することになる。一般的には、このような場合において運用テストがそのまま実運用に移行する可能性が考えられる。全学危機管理システム全体の完成に向けた研究が継続される中で、届け出られた部分は実運用に供されつつも、全体のテストにおいても使用されることが懸念される。実運用環境をテストで使用する場合、テストデータによって実運用の完全性や可用性が損なわれる可能性がある。コンサルテーションではこの点に注目して、テスト環境と実運用環境をはっきりと分離するよう、意見書の 1 番目の意見として明文化して指摘したのである。もし当制度が無ければ、研究とは別の

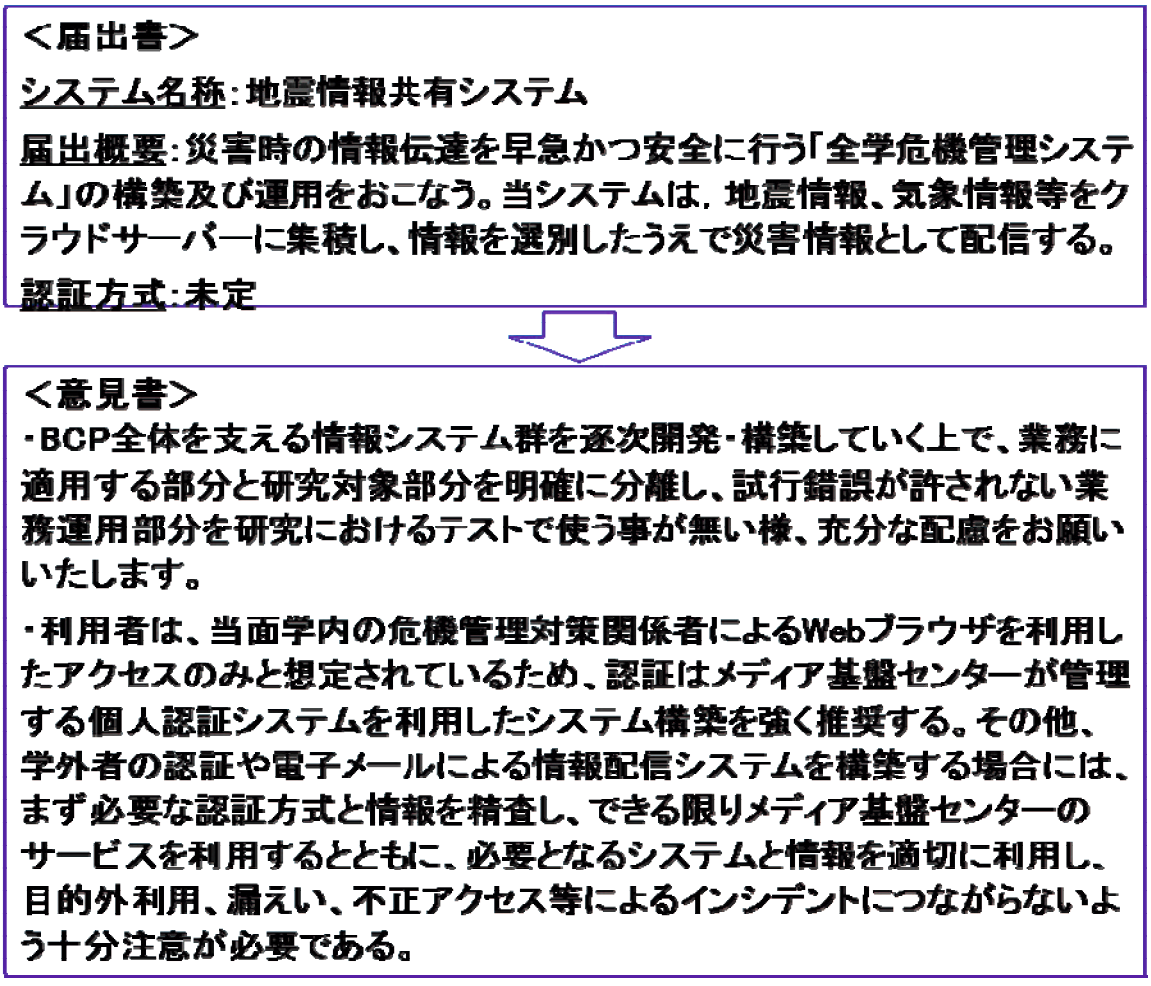

図 3-12 意見書例 3;テスト環境と実運用環境の分離

予算を確保して実運用の為の機器や体制を充分整備することなく、研究者が運用を引受けることになる可能性を否定できない。研究者個人がこれを引受けるということは、本来大学が組織的に運用すべき情報システムを個人に委ねることとなる。将来的に当該研究者に本務である研究以外の作業負荷を掛けることになりかねない。運用開始以後の運用や予算への配慮の必要性について、研究者個人だけではなく学内外の関係者に周知出来た意義は大きい。

また、意見書2番目の内容は、個人認証(本人認証)の仕組みとして既存の個人認証システムの活用を勧める意見である。当該システム独自の個人認証の仕組みを新設することは、必然的にユーザ管理作業やデータベースの維持管理作業が発生する。これを避ける為の指摘である。

4つ目の事例は、図3-13の届出書に示す通りのありきたりなホームページの届出である。インターネットからのデータ入力を許す場合には情報セキュリティ上注意すべき点が多いことを指摘した例である。この例では、学外サーバを利用することもシステム構成の選択肢としている為、指摘事項も多岐にわたっている。具体的な指摘内容は図3-13の意見書記載の通りである。フィッシングや不正アクセスさらには災害等不測の事態への対応等情報セキュリティへの配慮を促すとともに、ベンダーとのサービスレベルアグリーメント(SLA)を取りきめるよう指摘してサービス品質への配慮を促している。

<届出書>
・創立〇〇周年に向けての広報活動のために、フォトコンテストの写真募集と閲覧のできるホームページ(HP)を、学外ベンダーが自社に設置するサーバ上に開設する。
・写真募集の手段としては、HP を介して送ってもらう方法と郵送の 2 通り。
・同じホームページを介して寄付金を募る。

<意見書>
・何か重大なセキュリティ事象が発生したときに，クライアントとして迅速な対応が出来るのか，甚だ疑問です。学外サーバを利用するのであれば，その辺の担保が必要です。
・学外ベンダー側に，重大な瑕疵や倒産等の不測の事態が発生し，サーバの継続利用が不可能になった際の格納データに対する担保が不明確です。
・本学ドメインを利用せず，独自で汎用ドメインを取得する場合，寄付金募集ということもあり，フィッシングサイトとの疑念を払拭するよう，ご配慮願います。特に，JPRS（日本レジストリサービス）への登録情報及びサーバ証明書の登録情報は，適切に設定して下さい。
・緊急事態発生時等に原因究明を行うに必要なログが記録されていることが望まれます。
・アップロードされた画像のファイル形式の確認，公開フォルダへの一時保存の防止等の技術的不正アクセス防止措置を講じられる必要があります。
・当システムにアクセスできる担当者，アクセス場所等を適切に制限し，担当者，アクセス場所は個々に識別可能であるべきです。
・サーバに保存されるプログラム・データの複製を本学内に有するなど，システムの復元が可能なバックアップ体制をご検討ください。
・「本学情報セキュリティ緊急時対応基準」による全学緊急事態担当者が，緊急時に，ネットワークからの切断，システムの停止，システムの修復，原因究明等の対応が可能なように，全学緊急事態担当者に学外サーバ及びシステムへのアクセス権限を付与して下さい。
・学外サーバに関する SLA（サービスレベルアグリーメント）を作成されることを期待します。提供業者の責任および免責の範囲等を明確にするべきです。
・広報ページは迅速に情報を提供する機能が必要であり，その機能を維持するため，怠りなく運用管理およびリスク管理を行う必要があります。

図 3-13　意見書例4；学外ｻｰﾊﾞ利用時の注意事項

3.6 情報システム届出制度の効果と更なる改善

3.6.1 情報システム届出制度の効果

ここで当制度の全般的な効果として、3 点挙げる。

(1) 学内情報システム全体の安全性あるいは可用性の向上

表 3-7 の項番 1 に示すように、運用体制や連絡体制、さらに役割分担に関する意見が 75 件(意見全体の 19%)にのぼる。これらの意見により、個別情報システムの管理者の連絡先が明確な状態で運用されるようになり、万一情報セキュリティ事故が発生した場合の処置がスムーズに出来て、大学全体への影響を最小限に抑えられるよう改善されたと言える。実際、今年学内のある PC が踏み台にされて学外 Web ページへの不正アクセスが発生した際も、検知直後の当該 PC の管理者との連絡により状況把握と原因追求を、早期かつ確実に実施出来た。検知直後に当該 PC を学内ネットワークから切り離したことはいうまでもないが、類似事故防止の為の啓発活動を含めて再発防止策の策定に役立てることができた。また 3.5.2.2 節で述べたように、認証やセキュリティに関する意見が 150 件(意見全体の 38%)も出されている。この点についての具体例は前節の 3 つ目や 4 つ目に掲載しているが、認証機能の必要性を指摘しこれを組込むことにより機密性が確保される等の改善効果が出ている。これらの意見により個別情報システムの安全性や可用性を改善させ、ひいては学内情報システム全体の情報セキュリティレベルを向上させている。

(2) 情報システムそのものや開発運用体制の改善とコスト削減

表 3-7 項番 7 に記載されている 57 件(意見全体の 14%)の「センターサービス活用」は、届け出られた個別情報システムの機能がすでに学内で提供されているサービスで実現されていることを指摘し、これを活用するよう勧める意見である。新たな情報システム導入を抑制することにつながり、コスト削減効果が得られた。3.5 節で示したコンサルティング事例(図 3-10 の意見書例 1)でも、作業量を含めたコスト削減の効果をもたらしている。届出元で新たにサーバや新たなアプリケーションソフトウェアを導入した場合と、既に学内で提供されている Moodle サービスを利用した場合では、100 万円程度の差異があると推定される。あくまでも一般的なケースで推定条件を設定して比較すると表 3-8 のようになるので、参考とされたい。ただし、表 3-8 記載の数値(金額)は想定条件に基づくものであり、あくまでも試算値である。また、人件費単価(円/人時)も想定であり、組織や上記作業を実施する人によって大きく異なる点についても注意が必要である。この例は作業量減というだけではなく、作業そのものの発生を抑止できる事例があることを示している。これらの事例は、新たなシステム開発を抑制し既存の情報システムを活用したという点において、当制度が理想と

表 3-8 既存サービス利用効果試算表(参考)

項番	分類	費目		金額(千円)(注)		
		大項目	小項目	A:個別導入	B:既存サービス利用	A-B:差異
1	一時経費(導入費用)	(1)ハードウェア(サーバ)購入費		400	0	400
2		(2)UPS購入費		200	0	200
3		(3)アプリケーションソフトウェア開発費		800	0	800
4		(4)作業費(人件費)	①インストール作業	12	0	12
5			②ソフトウェア操作の学習	24	24	0
6			③利用マニュアル作成	48	0	48
7		(小計)		1,484	24	1,460
8	経常経費(月額)	(1)電気代		α	α	0
9		(2)サーバ維持管理費用	①ソフトウェア保守費	12	0	12
10			②データベース管理作業費	12	0	12
11		(3)ユーザ管理		30	0	30
12		(小計)		54	0	54

する情報システム維持管理の原則(3.6.2 節参照)に、より近づけることが出来ている。当制度の大きな効果である。

また、前述の表 3-7 項番 1 に示す、運用体制や役割分担に関する意見に加え、表 3-7 項番 6 の「システム設計・開発」や同表項番 8 の「サービス仕様確認」は、情報システムの品質向上等開発における改善をもたらしている。

(3) 学内 IT ガバナンス改善

当制度は、学内情報システムを全学的視点で統制する機能を支援する効果があった。IT 戦略提言書[16]によれば、IT ガバナンスとは「企業が競争優位性構築目的に、IT 戦略の策定・実行をコントロールし、あるべき方向へ導く組織能力」のことである。当制度のもとでは、表 3-7 項番 3「全体最適」の為の意見が 16 件(意見全体の 4%)出されている。大学組織として学内の個別情報システムを把握し、情報システム導入に際して CIO や CISO の意向を反映する為の意見を出せる仕組みになっていることが判る。あるべき方向へ導くという意味において、当制度開始以前に比べてITガバナンスのレベルを向上させていると言える。また、当該組織の構成員の意思がある程度尊重され、強制力ではなく、出された意見に基づく調整や協調によって組織体としての意思決定がなされるというガバナンスの特徴を備えているといえる。

さらに、届出により把握される情報システムやそこで取扱われるデータを情報資産として見た場合、データの種類や量、学外接続の有無や利用者のアクセス範囲、ソフトウェアの種類等届け出られた情報は、リスク評価において、当該情報システムの具体的な脅威や脆弱性を明確にする上でも役立つ。学内情報資産のリスク評価に情報を提供していることになり、情報セキュリティレベル向上にも役立っている。

3.6.2 情報システム届出制度の課題と改善

前節で述べたように当制度導入により得られた効果は大きい。ここで、今後の学内情報基盤整備への当制度活用上解消されることが望ましい課題について、当制度自体に関するものと学内情報システム全体の維持管理（あるいはITガバナンス）に関するものに分けて、以下にそれらを対応策とともに述べておく。当節で届出制度自体の課題について述べたあと、次節で学内情報システムに関する課題について述べる。

1 つ目は、届出内容を常に最新の状態に保つ為の改善が必要なことである。再新状態に保てない状況としては、次のようなケースが考えられる

① 届出内容に変更がある場合には改めて届け出る仕組みになっているが、学生（特に大学院生）の卒業や退学あるいは教職員の人事異動等に伴う運用体制（組織）変更が全て届けられない可能性がある。多くの場合、情報システム自体には変更が無く、届け出なくても当該情報システムの担当者がすぐに困ることがないからである。

② 情報システムを新たに導入する時は、学内ネットワーク接続の必要性から届け出るが、稼働停止時の「廃止」や小さなシステム改変の時の「変更」が届け出られない可能性もある。

③（学生の卒業や教職員の退職を含めて）担当者の異動に伴う引継ぎが不十分な場合（仕様書等の引継ぎ情報が不完全な場合を含めて）その後管理者不在のような状況になる可能性が考えられる。当制度の運用開始以前から稼働している情報システムの中にも、この状況にあって届出未了となっているものがある可能性もある。

④プロジェクト経費等、有期限の経費で調達された情報システムの、その期限後の運用の継続の際に担当者（あるいは責任者）不在の状態になる可能性がある。

これらに対しては、定期的に（例えば年に一度）全届出元に届出内容変更有無の確認依頼通知を出し、この通知を受けた個別情報システムの担当者から必要に応じて変更を届け出る手続きを追加すれば届出内容を最新の状態に更新できる。

2 つ目は、情報セキュリティ上の配慮から、個別届出案件に関する情報を見ることができるのが届出者と部会の委員だけという点である。届出者以外の教職員による、類似システ

ムの有無の確認や参考文献としての参照が困難である。もちろん、なかには公開できない案件もあり得るが、当制度が理想とする情報システム維持管理の原則にさらに近づける為には、届出内容の公開の範囲の再検討の余地がある。ここでいう原則とは、学内情報システム全体が、次の 2 つの条件を満たした状態で維持管理されるべきことを指している。

- 同じ機能を持つ情報システムは学内で1つのみ稼働すること。
- 同じデータの入力は学内では 1 か所のみで行われること。

届出書作成の際にその時点で既に届け出られている(あるいは既に稼働している)他の情報システムの流用の可能性を検討したり、コンサルテーションの際に他の類似案件を例示したりしてコンサルテーションを進めることができるようにする為である。

これに対しては、公開可能な範囲で、参照して意味のあるデータ項目を教職員が参照できる Web 画面を作れば良い。届出書や意見書に記載された用語をキーワードとして類似の届出案件を検索する機能も有用である。この Web 画面への表示項目は、その利便性や安全性について委員会等において良く検討し全学的合意を得る必要があるのはいうまでもない。また、個別の案件に関する情報の他部署への開示に関しても、当該届出案件である情報システムの管理部署の了承を得ることも重要である。

3 つ目は、届出義務化の際の届出書(入力)簡素化により、届出案件(情報システム)相互の共通性や流用可能性等を検討する為の情報収集を、コンサルテーション時に実施している点である。案件により(届け出られた情報システムの特徴により)収集すべき情報(データ項目)が異なり、コンサルティングチームへの負荷が大きい。次節で述べるように、学内で継続的に稼働する情報システムの標準化や学内のソフトウェアの流通促進を進めれば、標準化された部分に関する情報を収集する必要が無くなり、コンサルテーションにおいて収集すべき情報も減少していく。同じ機能の情報システムや同じデータを学内において重複させないという、当制度が理想とする情報システム維持管理の原則にさらに近づける為にも、コードやデータ形式あるいは設計ドキュメント等の標準化やソフトウェアの流通のさらなる促進が必要である。

また、情報セキュリティの観点でも、リスク評価に必要な情報が収集されることが望ましく、この視点からも届け出るべき情報(データ項目)の検討や見直しを継続していくべきであると考えている。

4 つ目として、本学における運用経験からの知見として、情報システム届出制度を他大学で適用し、活用にあたっての次の点に留意が必要であることを補足しておく。

・ 当制度を構成する為には次の 3 つが必要である。制度を運営する委員会組織、届出案件の受付・登録等を処理する届出案件管理システム、そして構成員が守るべきルールの 3 つである。

・ 届出案件管理システムは、学内構成員が自分のいる場所から届出書を入力できる仕組みを持つべきである。届出に必要なデータ項目を簡便な項目に絞り、気軽に届け出られるよう配慮が必要である。

・ 制度を運営する委員会組織には、学内ネットワークに詳しい要員を含めるとともに、情報システムの種類に応じて届出者から意見を聴く為に、適宜専門家に意見を求めることができる仕組みが必要である。

・ 構成員が守るべきルールにおいては、届出の必要な情報システムとそうでない情報システムの違いを明確にし、学内に周知すべきである。

・ CIO に情報を集中することにより、CIO 自身やコンサルテーショングループの恣意的な意見の発生の可能性も否定できない。これを防止する為にも、コンサルテーションの内容を記録し、構成員が参照できる仕組みにすべきである。また、次章で述べるようにこの制度の実施状況について学内外の監査を受ける仕組みを合わせて運用すべきである。

3.6.3 情報システムに見られる課題と対応策

当制度の当初の理想に向かって学内情報システムのあり様について考えると、国立大学法人経営情報基盤のスリム化・高度化という課題は、今なお残っている。当制度を義務化したことで、業務運営において運用されているほとんどの情報システムを把握することが出来た。(全ての届出件数 516 件のうち、業務で利用されるものが約 250 件ある。)附属病院で使用される医療情報システムを別に扱うとしても、既に届け出られた約 130 件について再整理を行い、個別情報システム相互間の情報の流れ(データの流れ)を明らかにする(可視化する)ことにより、全体としてスリム化を図ることも、学内の情報システム管理作業全体を軽減する為の課題である。その為には、次のような作業が必要になる。

・部署間を移動する情報(データ)の再整理

・類似システムの標準化・共通化の促進

・業務関連データベースの再整理

・業務手順の簡素化、文書の電子化

これらを進める為にも、当制度を活用して今後導入される情報システムを把握する必要がある。

一方で、各部局あるいは各教職員それぞれが必要に応じて情報システムを作成し運用することを避けられない現実もある。従って、情報システムあるいはソフトウェアの標準化・部品化も必要である。学内におけるソフトウェアの流通を促進し、開発された情報システムやソフトウェアがより多くの場所で活用される仕組みを確立するという課題である。その為の対応策として、開発した教職員や所属部署が何らかのインセンティブを得られる仕組みが考えられる。より多くの利用により開発コストを回収出来れば、次の前向きな作業への活力を与えることにもなる。もちろん品質確保の仕組みも必要である。従来のように「自分が作って自分で使う」だけであれば、少々の不具合はその場で修正して利用を継続することが可能であるが、他人が使うからには、利用に耐える品質が必要である。検査や不具合検出時の取扱いルールや対応の仕組みも必要になる。大学内には、研究の為に一時的に開発するソフトウェアや特殊な機能を必要とする情報システムもあり、すべての情報システムが標準通りのものにはならないが、多くの教職員や学生が継続的に利用する情報システムに対して、前述の標準化やソフトウェアの流通促進を進める為にも、当制度による学内情報システムの把握をさらに進める必要がある。

3.7 まとめ

本研究の課題の 1 つである「学内で稼働する情報システムを大学として一元的に掌握できる仕組み」としての「情報システム届出制度」を提案して本学に実装し、これを運用してその効果を得たことについて事例をあげて説明した。そのうえで「3.6.1 情報システム届出制度の効果」に、当制度の効果を次の 3 点に集約して記述した。

(1) 学内情報システム全体の安全性あるいは可用性の向上
(2) 情報システムそのものや開発運用体制の改善とコスト削減
(3) 学内 IT ガバナンス改善

これにより、「3.6.2 情報システム届出制度の課題と改善」や「3.6.3 情報システムに見られる課題と対応策」で述べたような今後の課題もあるが、本研究の課題の1つ（1.2節(1)）が解決され、ITガバナンスの観点から、組織的IT基盤強化策の1つが具体化されたといえる。

大学法人が組織体として責任を持って情報システムの維持管理を安全な状態で持続する為に、「3.6.2 情報システム届出制度の課題と改善」の 4 番目の留意点を踏まえた上で、情報システム届出制度を他大学でも活用することを提案する。

第4章　情報セキュリティマネジメントシステム（ISMS）

4.1 概要

本章では、本研究の第 2 の課題である「学内の情報セキュリティを確保し、かつそのレベルを継続的に維持・向上させる仕組み」について述べる。第 2 章で述べた IT ガバナンスの定義の中に「全学的な目的と戦略を適切に設定し、その効果やリスクを測定・評価して、理想とする IT 活用を実現するメカニズムを全学組織の中に確立すること」とある。本研究では、効果やリスクを測定・評価する仕組みが内在する情報セキュリティマネジメントシステム（Information Security Management System、以下「ISMS」）を学内において具現化することで、研究課題を解決している。本学における ISMS 構築事例を紹介し、その経験から得た知見に基づき、学外の第三者機関による監査の重要性とその効果を示す。また認証制度（http://www.isms.jipdec.or.jp/isms.html を参照）を活用して、ISMS を実効性のある仕組みとして運用することを提案する。さらに、ISMS 構築を目指す他の国立大学の為に、その国立大学が ISMS マニュアルのテンプレートとして参照することが見込まれる「高等教育機関の情報セキュリティ対策のためのサンプル規程集」[10]（以下「サンプル規程集」）の利用について考察する。

4.2 中期計画と ISMS 導入

本学では、国立大学法人化後の第一期中期目標・計画の中で、情報セキュリティレベルの向上と同セキュリティ文化の普及を目指し、情報セキュリティマネジメントの仕組み（ISMS）の導入を掲げた。その当時、情報セキュリティポリシー（以下「ポリシー」）策定済みの大学は多かったが、第三者機関により実質的な ISMS の存在を認定された大学は少なかった。山本（2012）[23]は「大学での ISMS は情報基盤センター等の IT 運営分野では ISMS と ITSMS（IT Service Management System）の統合導入等進んできているが、大学全体では内部統制分野等企業ほどには進んでいない」と述べている。当時本学では、学内で稼働している情報システムが大学として把握されていないことに加えて、大学の神経ともいうべき学内ネットワークの開発・運用が担当者任せになっている場合が多く、組織的情報セキュリティ対策の実施が困難であった。前者に関してはすでに第 3 章で述べているように、情報システム届出制度を構築・運用することで対策とした。後者に関しては ISMS の構築（ISMS 認証取得までの活動）・運用を通じて解決していったので、以下この点について述べる。

4.3 認証制度と学外監査

4.3.1 認証制度とISMSの実効性

認証制度では、ISO/IEC 27001[1]をはじめとする国際規格や対応する JIS 規格への適合性について第三者機関による認定を受ける。当認定（以下「ISMS 認証」）を受ける為には、単に基準や規則が定められているだけではなく、ISMS 適用範囲全体が基準や規則（以下「ISMS マニュアル」）どおりに活動していることが証明されなければならない。もちろん情報管理に関する規則も定められ、個々人の無用な情報秘匿は許されず、必要に応じて組織内で共有される。また、前記国際規格の第 9 章ではパフォーマンス評価の実施を求めており、ISMS 認証を受けた組織では、ISMS の当該組織における有効性を自ら評価した上で ISMS を運用している。従って継続して ISMS 認証を受けていること自体が有効な ISMS を運用していることを示している。さらに、ポリシーを業務に適用した上で実効性のある ISMS を構築しそして運用していることを、大学として社会に向けて明確にする効果を得ることができる。

4.3.2 ISMS認証における審査の意味（ISMSの実効性の証明）

ISMS 認証を受ける大学においては、ISMS 適用範囲全体が ISMS マニュアルに規定された実施手順に従って実際に運用されていることが、次の 4 段階で確認される。第 4 段階の審査が本論文にいう学外監査にあたり、ISMS 認証の実質的な意義と言える重要な点である。

① ISMS スタッフ会議…定期的に開催され、前回会議以降発生したインシデントやその対策をはじめ、作業状況を報告し合い今後の予定について情報共有を行う。スタッフそれぞれの作業状況を相互に確認し合う場である。

② 内部監査…内部監査チームにより、運用状況を確認する。各種記録や ISMS マニュアルの改訂内容（運用手順の変更内容）について机上で確認するドキュメント監査と、ISMS 適用範囲内の業務実施状況を実際に見て廻る実地監査が行われる。もちろん監査指摘事項への対応状況（改善状況）の再確認（フォローアップ）が後日なされる。内部監査は最低限年 1 回以上実施される。

③ マネジメントレビュー…ISMS スタッフと内部監査チームが経営陣に運用状況及び監査結果を報告することにより、経営陣が現場の状況を確認する場である。経営陣は今後の予定に対して指示や承認を与える。ISMS 運用における大学法人としての意思伝達（あるいは決定）の場でもある。

④　第三者機関による審査…ISMS 認証機関から派遣される審査員により、規格準拠性を中心に年 1 回の確認がなされる。審査員の確認内容に基づき ISMS 認証を継続するか取り消すかが決定される。この確認（あるいは審査）により、ISMS 適用範囲の運用状況が学外機関により客観的に確認されることになる。学外の審査員が審査することで、4.5.6 節で述べる点以外にも、学内の環境に慣れた者が気付かない不具合を発見できる利点がある。事務用 PC 画面が戸外を通る部外者からも見える方向を向いていることや、機密性の高い区域への意外な進入路が見つかる等が身近な例である。

内部監査や認証機関による審査は、助言型監査と言われており、各段階において多くの助言（あるいは指摘）がなされる。また、必ずしも情報セキュリティレベルを保証するものではないが、ISMS 適用範囲において ISMS が規格通りに現に運用され、情報セキュリティレベル向上に向かっている事実を、利害を共有しない第三者が確認することとなり、ISMS の実効性を示す。このことにより社会からの信頼も高まる。

4.4 本学の取り組みとISMSの事例

4.4.1 本学の取り組み

本学では ISMS 認証取得を目指し、当時の国際標準準拠の ISMS 認証基準に沿って情報セキュリティ対策実施手順を具体化すべく、メディア基盤センターをモデルとして ISMS 構築プロジェクトを発足させた。ISMS 認証取得をもって ISMS 構築完了（プロジェクト終了）とし、これを共通の目標として、所属員の意識統一と所属員間の情報共有を図った。本学における ISMS 構築の経緯に関しては、本学メディア基盤センターのホームページ「ISMS 広報部」の「ISMS 認証取得への道」に詳しく述べている。2008 年 10 月には ISMS 認証を取得し、文部科学省の「平成 20 年度に係る業務の実績に関する評価結果」「その他業務運営に関する重要目標」における注目事項として、次の URL に掲載されている通り、中期計画の当該項目が「達成に向けて順調に進んでいる」との評価を受けている。（http://www.mext.go.jp/a_menu/koutou/houjin/1289584.htm を参照されたい。）

このことにより、本学ホームページを通して他大学や一般社会にアピールする効果を得た。2008 年当時、国立大学法人の ISMS 認証取得大学は静岡大学と宇都宮大学に本学を加えた 3 校であったが、2015 年には表 4-1 の通り私学を含めた 15 の大学が ISMS 認証を取得している。このうち 12 校が国立大学であるが、2012 年以降の増加が目立つ。本学内においては、毎年適用範囲を拡大して、学内の情報セキュリティ文化の普及と情報セキュリティレベル向上に寄与している。本学における ISMS 適用範囲の拡大の状況については、付録 C 経営情報学会予稿「ISMS 適用範囲拡大における留意点」を参照されたい。

表 4-1 ISMS 認証取得大学一覧

項番	大学名	組織部門	登録
1	静岡大学	情報基盤センター	2003/11/25
2	日本福祉大学	（省略）	2005/3/16
3	早稲田大学	情報企画部	2007/1/24
4	宇都宮大学	総合メディア基盤センター	2007/11/25
5	日本大学	総合学術情報センター	2007/12/4
6	山口大学	（省略）	2008/10/24
7	徳島大学	情報化推進センター	2012/3/9
8	九州大学	情報統括本部	2012/3/22
9	長崎大学	情報企画課及び情報メディア基盤センター	2013/3/4
10	鹿児島大学	学術情報基盤センター	2013/4/23
11	岡山大学	情報統括センター	2013/11/12
12	横浜国立大学	情報基盤センター	2014/3/6
13	広島大学	情報メディア教育研究センター	2015/3/27
14	室蘭工業大学	情報メディア教育センター	2015/3/27
15	琉球大学	総合情報処理センター	2015/4/13

JIPDEC ホームページ（http://www.isms.jipdec.or.jp/lst/ind/search.cgi）から

（閲覧日:2015 年 10 月 17 日）

4.4.2 本学のISMSの特徴

次に、本学における ISMS 運用を通じて知ることの出来た本学の ISMS の特徴 4 点を順に説明する。

まず、組織上の ISMS 適用範囲が学内の複数部局にまたがり、適用範囲内組織の所属員（原則全員）が月 2 回集まって情報交換を行っている点である。図 4-1 に本学の 2015 年度の ISMS 運用体制図を示す。教員・技術職員・事務職員が職種や職位に関係なく対等の立場でお互いに率直な意見を述べ合い、ISMS に関する情報を共有し、日々業務改善活動を組織的に推進している。従来業務担当者の個人管理に埋没していたインシデント情報も、ISMS 運用開始後には所属員共有の情報として組織的に管理されている。具体的には、ISMS 適用範囲内組織の所属員が横断的に月 2 回 ISMS スタッフ会議として集まり、原則全てのインシデント（あるいは情報セキュリティ事象）を報告しており、類似事故の

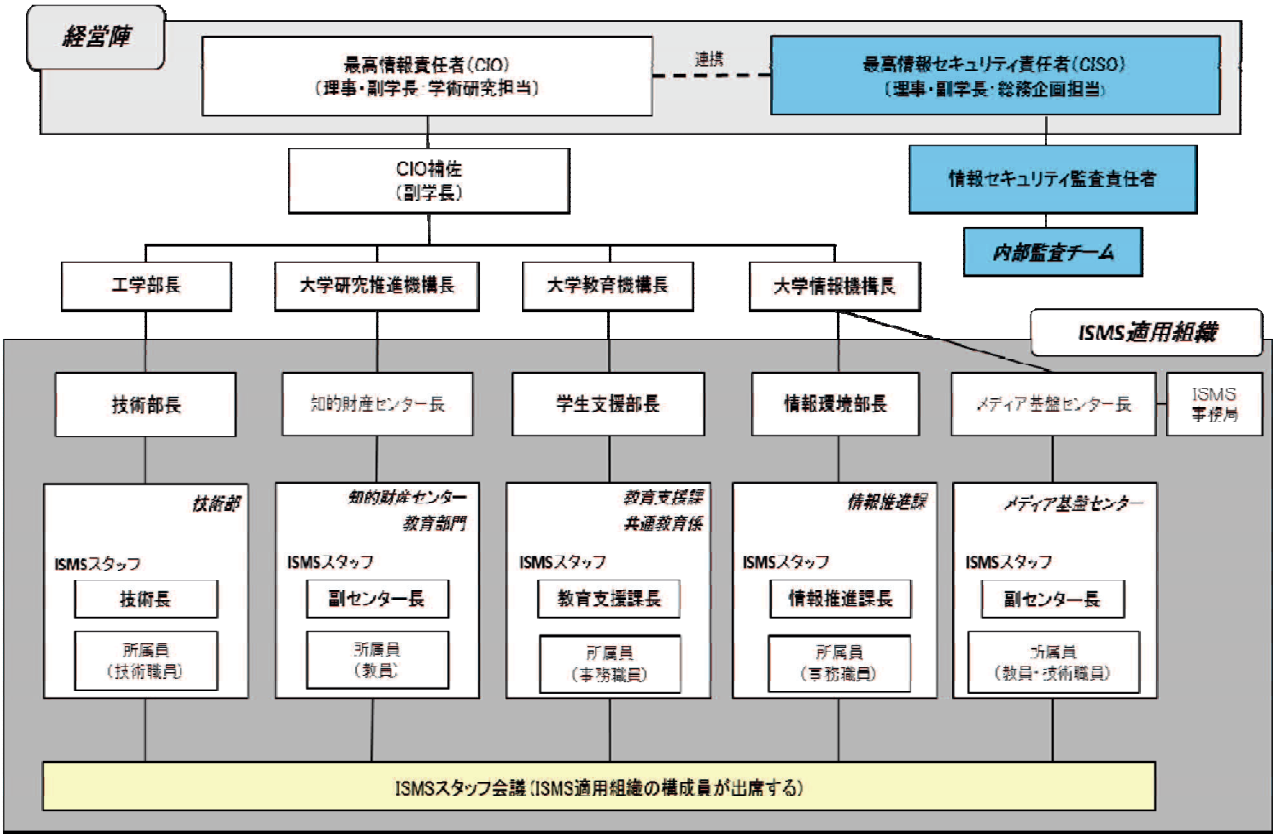

図 4-1 山口大学の ISMS 運用体制図

発生抑止に役立っている。順次適用範囲を広げることができているという、この状況は、当初 1 部門で始めた ISMS という仕組みが学内他部署にとっても有用であると評価され受け入れられたことを示している。しかしながら、他部署への適用範囲拡大の際には、言葉の解釈や立場の違いによりその導入への反対等を伴う場合もあり、粘り強く説明や説得・調整を行う必要があることを付記して置く。

二つ目は、監査室を含む複数部局から選出された監査員からなるISMS内部監査チームを構成している点である。法人化以降国立大学に設置された監査室は主として業務監査と会計監査を担当するもので、発足当初はISMSに関する内部監査が職務分掌には含まれていなかった。ISMS 構築時に、被監査組織から独立した学内組織として ISMS に関する内部監査を依頼し、監査室員の教育を行った上で試行するところから始めた。現在では人事異動等により学内における ISMS 内部監査経験者の数も増え、ISMS 適用範囲が拡大していることもあって、被監査組織外の部署に所属する ISMS 内部監査経験者 9 名による内部監査チームを編成し活動している。また、情報系教員 1 名をこのチームに加えて技術面での監査をサポートしている。マネジメントレビューや内部監査により、ISMS が実質的に運営されていることを学内他部署に対して示すことができている。

三つ目は「ISMS 講習会」を毎年実施し、学内外に向けて ISMS の啓蒙・普及を推進している点である。当初は新たに ISMS 適用範囲内組織の所属となった教職員に ISMS の初歩的知識を供与する為に始めたもので、毎回講習会受講前後に実施する確認テストで受講者の知識増を確認している。ISMS 全般に関する教育を実施し、リスクアセスメントをはじめとするISMS運用への参画を可能とする為のものであるが、学外からも受講者が集まるようになり、受講者が中心となって所属大学のISMSを構築しISMS認証を取得した大学もある。

四つ目は、国立大学情報系センター協議会の中に設置されている ISMS 研究会においてISMSの定着・普及を進めている点である。各大学間相互に、ISMSの効果や運営上の問題点等の情報を交換して、広くISMSのメリットを広げていく活動である。ISMS認証取得大学の参加は毎年増加し、その大学におけるISMSの効果が報告されている。

4.4.3 ISMS 研究会参加大学の事例

ISMS 研究会では、毎年研究発表会が開催され 2015 年秋で 13 回を数える。表 4-1 掲載の参加各大学それぞれにおいてISMSの有効性を評価しながら運用を継続していることが判る。本論文では、それらのうち徳島大学の ISMS の効果に関する発表を紹介する。その中で、佐野ほか(2014)[12]は、同大学においてISMSが有効であり、活動とりわけ評価改善プロセス(PDCA の中の P フェーズと A フェーズ)において内部監査や第三者機関による定期審査が重要な位置を占めていることを述べている。また、被監査組織外からの指摘事項への対応を通じて問題点を解決し是正することにより、業務改善が継続的に実施されると述べている。さらに、ISMSを通して業務の可視化が進み「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、間接的教育等の効果が得られた」とも述べている。

ISMS 認証取得各大学いずれにおいても全学を ISMS 適用範囲にしているわけではなく、今後の適用範囲の拡大が本学を含めて課題となっているものの、それぞれにおいて自ら策定した ISMS マニュアルに則った PDCA(Plan、Do、Check、Act)活動を実践し、学内情報セキュリティレベルを継続的に向上させている。

4.4.4 ISMS マニュアルのテンプレート化

ここで、ISMS 普及活動の一つとして実施した、本学の ISMS マニュアルのテンプレート化について述べる。このテンプレートは、企業を中心的な対象組織としている国際規格 ISO/IEC27001 を大学に適用しやすくする為、本学が ISMS 構築の際に得た知見や経験を他大学で活かすべく作成したものである。詳細については情報処理学会の研究報告[7]

を参照頂きたい。その後 2013 年に前記国際規格が全面的に改訂され、また高等教育機関向けに「サンプル規程集」[10]が公開された。そこで、大学が認証制度の下で新たにISMS を構築する際にサンプル規程集を ISMS マニュアルとして有効活用できるかどうかについて、次の二つの観点で考察を加える。一つは監査人の独立性の観点、もう一つは文書としての充足性の観点である。

4.5 サンプル規程集利用の ISMS

4.5.1 政府機関の情報セキュリティ対策のための統一基準群

国立大学においては、前述の ISO/IEC 27001 を中心とする規格の他に「政府機関の情報セキュリティ対策のための統一基準群」[15]（以下「統一基準群」）と、これに沿ったサンプル規程集が示されていて、これらを参考に情報セキュリティ管理の仕組みを構築する支援がなされている。この統一基準群は、統一規範、運用指針、統一基準、ガイドラインの 4 点の文書からなる。各文書の内容から、ガイドラインが国際規格 ISO/IEC 27001（あるいは JIS Q 27001）（以下「ISMS 規格」）附属書 A の管理策に対応するものと考えられる。統一基準群においては、監査について「第 2 部 情報セキュリティ対策の基本的枠組み」の中の「2.1.1（3）情報セキュリティ監査責任者の設置」や「2.3.2 情報セキュリティ監査」等の記述がある。2.3.2 節「遵守事項（2）監査の実施」の「基本対策事項」には「組織内における監査遂行能力が不足等している場合には、学外の者に監査の一部を請け負わせること」とされており、必ずしも第三者機関による監査もしくは審査を必須事項とはしていない。認証制度において求められる監査人の独立性の観点から、この点は改善が必要と考える。

本学の ISMS 構築時期とサンプル規程集作成時期とがほぼ同じであり、サンプル規程集を使用できなかったが、次節以降で ISMS 構築におけるサンプル規程集活用の可能性について考察する。

4.5.2 ISMS マニュアルとしてのサンプル規程集

サンプル規程集を使った ISMS マニュアルで ISMS 認証を受けた事例を筆者は知らないが、ここでは、統一基準群とサンプル規程集を利用して ISMS の定義文書（いわゆる ISMS マニュアル）を作成して構築された ISMS が、ISMS 規格に準拠・適合している（ひいては ISMS 認証を取得できる）のかどうかについて、考察を加える。

4.3 節でも述べているが、ISMS 認証は、PDCA サイクルを繰り返す業務改善活動を通じて情報セキュリティレベルの向上を図る為の情報セキュリティマネジメント体制が確立されている（即ち、実質的に ISMS が運用されている）と確認できることを前提として付与されるものである。また、ISMS 規格は汎用的であり、形態や規模又は性質を問わず全ての組織に

適用できることを意図しており、個別組織の実状に沿ったマネジメントシステムを許容している。この意味では、ISMS 規格要求事項に対して重大な漏れや不足あるいは矛盾する状況がない限り、適合と判断される。ただし、検出されたインシデントや規格不適合の可能性等の課題や問題点については着実に解決される仕組みを備えていなければならない。

サンプル規程集は2学部からなるモデル大学を想定してポリシーの事例として策定されたものであり、冒頭の「本文書について」の中で「各大学等で本文書を参考として自組織向けの規程等を作成する際には、これらの内容を参照した上で必要な修正や加除を検討して頂きたい」としており、これを利用してISMSを構築する際には、これ使って構築されたISMSを適用する組織の特徴に適した形に再編集するとともに、マネジメントシステムを実際に運用する為の文書を追加する必要がある。

ISMS 規格（具体的には、ISO/IEC 27001 の付属書 A に記載された管理策）では、これを適用する範囲の境界を、場所、設備、業務、組織、要員等それぞれの面で明示することを求めている。一方、サンプル規程集は、仮想の国立大学法人 A 大学における体制と規則を想定して検討されており、「C1001-01（目的）」に記載の通り当該大学の情報システムの運用及び管理全体に必要な事項を定めるものである。「C1001-02（適用範囲）」には人的適用範囲が、「C1001-03（定義）」には管理対象とする情報資産の定義が記載されていて、サンプル規程集は当該大学全体を適用範囲としていることが判る。施設や設備に関しても、「B2152 情報システムの構成要素に関する技術規程」で情報セキュリティレベルに応じたクラス分けを行い、全体で管理するよう要求している。

4.5.3 ISMS 運用体制と監査

ここでは、4.2節で述べた監査人の独立性に関する観点から、サンプル規程集が示す運用体制の改善点について述べる。サンプル規程集では、「本文書について」において、同文献の図4に情報システム運用管理体制が図示されており、情報セキュリティ確立に向けた、情報セキュリティマネジメントにおけるPDCAの活動サイクルを実践する組織として位置づけられている。また図4と同じページでは「ポリシーに沿った教育活動や組織の運用、さらにはその状況の監査と評価・見直しが重要」と、監査の重要性を指摘している。ただ、この運用管理体制図には、監査実行者が記載されていない。「C2401 情報セキュリティ監査規程」によれば、情報セキュリティ監査責任者が人選する監査人に、監査の実施を依頼することとしている。ISMSにおける監査では、ISMS規格を基準として熟知した上で被監査組織の活動状況を確認する必要があり、規格や規程を良く知るグループ（もしくはチーム）を情報セキュリティ監査責任者のもとに設置すべきであろう。サンプル規程集の図4に内部監

査チームを加えて補正したのが、本論文の図4-2である。ただし、さらにサンプル規程集では、学外の監査チームによる監査を実施することも許容しており、これにより監査の独立性を高めることができる。また、ISMS規格においては、大学全体を適用範囲とすることは必ずしも求めておらず、学内の一部のみを適用範囲として実質的な活動を確実に確認し、順次適用範囲を拡大していくことも可能である。この点については、経営情報学会2014年春季全国研究発表大会において、本学における適用範囲拡大事例を発表している。その予稿を付録Cとして添付するので参照頂きたい。図4-3は学外第三者機関による認証審査を加え、部分的にISMSを導入した場合を反映して図4-2を修正したものである。ISMS運用実態審査の為に学外の第三者機関が加わっていること、CIOとCISOを分離して別人としていること、そしてISMS適用範囲とそうでない部分（部署）が共存していることが図4-2と異なっている。ISMS適用範囲内では、マネジメントレビュー（経営者レビュー）や第三者機関による審査が義務付けられ、ISMSマニュアル通りの実務が実施されていることが確認されることは既に述べたが、ISMS適用範囲外ではこれが確認されるとは限らない。

4.5.4 ISMS 運用に必要な文書

サンプル規程集はポリシーの具体例であり、ISMSを実質的に構築し運用する為に追加作成の必要な文書は多い。ポリシーが実務に確実に反映される為には、適用範囲の実状に即した手順が具体化される必要があり、ポリシーに従って実務が遂行されていることを証明する為の記録文書を必要とするからである。一般的にポリシーは、基本方針、対策基準、実施手順で構成されるが、実施手順は大学全体に共通な事項に関するものと、部局別（もしくは部署別）の実状に合わせて具体的な記述で作成されるものとがある。ISMSはその適用範囲における具体的実施手順を記述した文書を含めることになる。JIPDECが公表している「ISMSユーザーズガイド」[13]にはISMS文書が例示されている。ここではそのうちの事例として、内部監査や第三者機関による審査に必要な文書について説明する。

サンプル規程集では、「C2401 情報セキュリティ監査規程」「C3401 情報セキュリティ監査実施手順」が定められている。前者においては、情報セキュリティ監査責任者が監査計画を立てて監査人を選任して監査を実施するよう記載されている。監査実施後には全学総括責任者に報告し組織的に改善に向かうよう要求している。後者には、計画・実施・報告・改善の一連の手順が詳しく記載されており、これは ISO/IEC27007:2011「情報セキュリティマネジメントシステム監査のための指針」と同様の内容であるが、ISMS 規格では監査の根拠をISO/IEC 27001 におくのに対して、サンプル規格ではポリシーをその根拠としている点が異なる。ただ、ISO/IEC 27001 の「9.2 内部監査」では、「組織自体が規定した要求

事項」への適合を求めていることから、サンプル規程集に基づいて作成された各種手順書に沿って実務がなされていることが確認されれば、内部監査において実質的に ISMS が運用されているとみなしうることを示している。

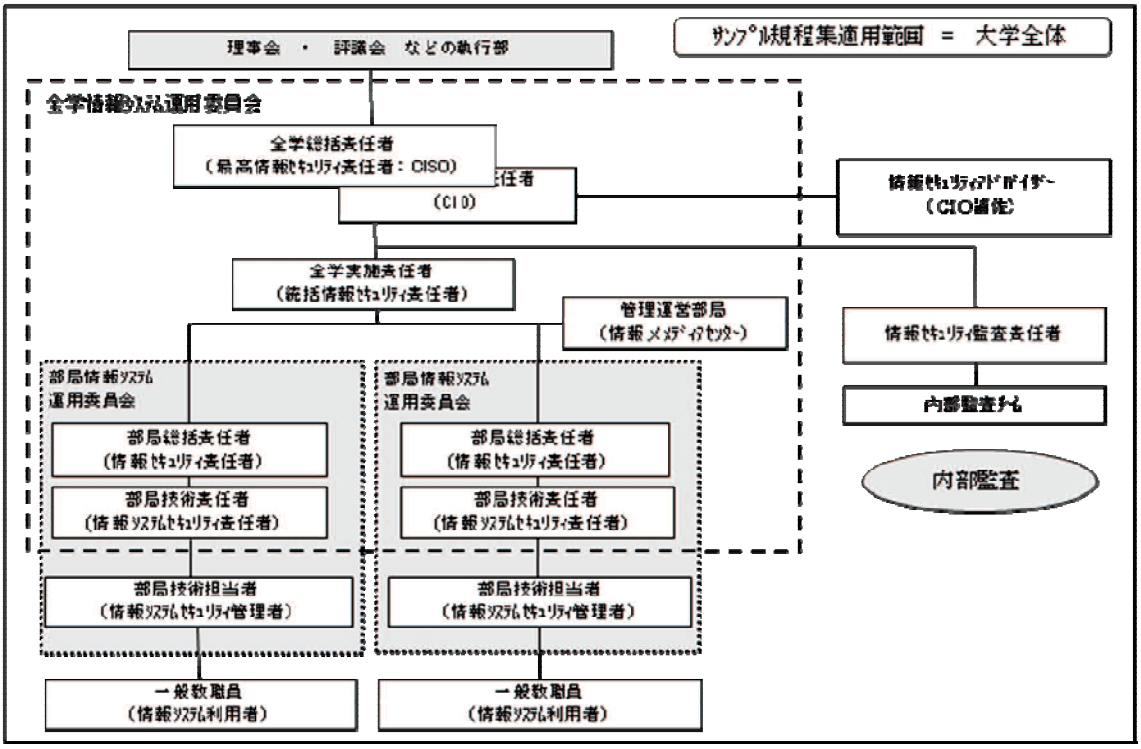

図4-2 内部監査チームを加えて補正した情報システム運用管理体制

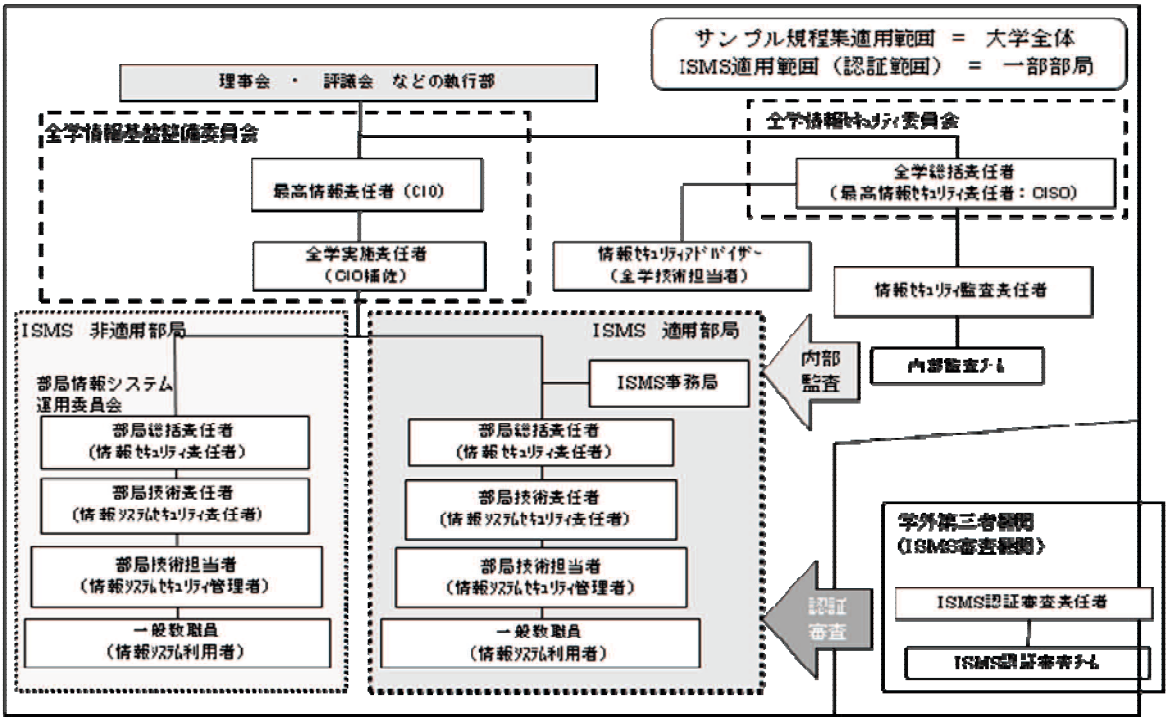

図4-3 学外第三者機関による認証審査を含むISMSを、部分的に導入した情報システム運用管理体制

もう1つ必要な文書が記録文書である。実務がポリシー通りに実施されていることを内外に証明する為には、実務の記録を残し実態を示す証拠として整理保管されなければならない。ISMS 適用範囲に限定して、各種記録文書について考察する。先に述べたように、ISMS における実務状況の確認（PDCA のうちの C フェーズ）には、自己確認を除き、大きくは内部監査・マネジメントレビュー・第三者機関審査の 3 つの作業ステップがある。これらの確認作業に役立つ記録文書の一部について、その例を「ISMS ユーザーズガイド」[16]の中から紹介する。（サンプル規程集では、参考として C3500「表 1 政府機関統一基準適用個別マニュアル群の構成」が示され、「C3501 各種マニュアル類」の項が設定されているもののその事例は提示されておらず、各大学にて策定することを想定している、あるいは各大学で策定できる旨記載されている。）

a. 適用範囲定義書…適用範囲を示す図面や文書
b. 教育訓練実施記録
c. リスクアセスメント報告書
d. リスク対応計画書／同報告書
e. 事業継続計画書
f. インシデント記録／同（対策）報告書
g. パフォーマンス評価実施記録
h. 外部委託実施記録
i. マネジメントレビュー報告書
j. 内部監査計画書／同報告書

4.5.5 ポリシー通りの運用実態を証明する仕組み

ISMS ではポリシーに従って実務が運営されていることが必要であり、そのことを内外に証明できることが求められることはすでに述べた。サンプル規程集はポリシーの事例を提供してくれるが、PDCA の各フェーズを実際に運営し、その実態を確認して学外機関が認定する仕組みまでは提供してくれない。各大学の実態に即して構築する必要がある。本学では、最初にメディア基盤センターを適用範囲として ISMS を構築したが、これに合わせてさらに前述の ISMS 認証を取得して、第三者機関による定期的な審査を受けることにより、学外に対しても ISMS が実質的に運用されている事実を証明することができている。サンプル規程集では、学内の内部監査実施まで要求しているが、第三者機関による確認行為までは要求していない。監査の独立性という観点から、別法人の審査員による実質的な ISMS 運用の証明（ISMS 認証）を受ける意義は大きい。

4.5.6 第三者機関のみがチェックできる管理策

ISMS 規格には、サンプル規程集にない要求事項がある。ISO/IEC27001 の第 5 章「リーダーシップ」の内容がそれである。ここでは経営陣への要求事項が記載されており、この要求事項を満たしているかどうかは第三者機関でないと確認できない、あるいは独立性の観点から確認の意味がない。サンプル規程集をベースに ISMS マニュアルを策定し ISMS を構築する場合には追加する必要がある。また、ISMS 規格の第 9 章「パフォーマンス評価」中の「9.2 内部監査」や「9.3 マネジメントレビュー」での要求事項への準拠性について、第三者機関による監査を実施することにより、内部監査体制や経営方針の中の情報セキュリティに関する事項等に関する示唆を得ることが可能となる。ISMS 規格には経営陣をチェックする部分を含んでおり、第三者機関による監査の実施が求められる。

最後になるが、認証制度の下で ISMS 認証取得済みの 4202 組織へのアンケート結果の報告書[14]から「質問 9 ISMS の導入及び認証取得の効果について」という質問の回答では、多くの回答者が次の 5 点を効果としていることを記しておく。

・組織の情報セキュリティ管理体制が強化できた。
・組織の情報セキュリティ対策が強化できた。
・社員の情報セキュリティに関する意識向上、教育啓発に寄与した。
・顧客からの信頼確保に貢献した。
・経営者の情報セキュリティへの関与が深まった。

4.6 まとめ

本章では、実効性のある ISMS の構築・運用について事例とともに学外監査が重要であることを述べた上で、4.4 節において、本学等の ISMS 構築・運用の事例について触れ、情報セキュリティ上の課題が解決されていくことを述べた。ただ、ISMS 適用範囲が学内の一部に止まっており、適用範囲拡大が課題であることも述べた。さらに、サンプル規程集を利用して実効性のある ISMS を構築し運用することの可能性について考察を加えた。ポリシー通りに実務が実行されていることを証明する仕組みを確立する必要があり、内部監査や第三者機関（別法人）による審査がこの仕組みに当たることも述べた。これらの仕組みを組込み、実効性のある ISMS を確立する為には、サンプル規程集に追加すべき仕組みや文書があることも述べ、その内容を示した。また、ISMS 規格に準拠できる可能性についても述べた。これらの考察から、ISMS 認証取得はサンプル規程集のみで構築された仕組みをより実質的に変える効果があることが判る。これらのことを受けて、サンプル規程集を ISMS マニュアルの中心として、ISMS における PDCA サイクル中の C フェーズに当たる内部監査

や第三者機関による審査の仕組みを加えることによりISMS 構築が可能であることを示し、これを提案する。これらの結果、「学内の情報資産及びそれらに伴うリスクを掌握した上で、情報セキュリティを確保し、かつそのレベルを継続的に維持・向上可能な持続性のある仕組み」が具体化され、本研究のもう1 つの課題（1.2 節(2)）が解決された。

一般的に、組織内の制度は、常に形骸化する可能性を内在しているが、組織外（本論文の場合、ISMS 適用範囲外組織）の眼での監査を継続することにより、実質的運用が継続されるものと考えている。また、本論文でいうISMS 認証が特定の情報セキュリティレベルを保証するものでは無く、情報セキュリティレベルの改善を推進する仕組みが組織内に構築されていることを認定するものであることにも留意が必要である。またISMS 認証を受けるには費用が必要となるが、この費用を低減するあるいはなくす方策も今後の課題とである。

情報セキュリティレベル向上の仕組みとして、学外からも信頼されるISMS がより多くの大学において構築・運用されれば、高まる情報セキュリティリスクの低減に寄与できる。

第 5 章　結論

5.1　本研究の成果;研究の意義

本論文では、国立大学における IT 基盤強化の為に組織的な活動が必要であることを述べ、IT ガバナンス確立の為に 2 つの仕組みを具現化したことを述べて、それらの仕組みを提案した。それに先立ち、ITガバナンスの確立が社会から国立大学に求められていることについても説明を加えた。

第 3 章では中規模国立大学法人において、学内 IT 化の状況を把握し、新たな情報システム導入の際、計画段階で全学的見地に立った検討を加えることが可能となる仕組みとして、「情報システム届出制度」を提案した。提案にあたって、本学で運営されている「学内情報システム届出制度」について紹介し、事例を挙げて当制度の運用によって学内情報基盤整備上の効果が出ていることも述べた。また、学内情報システムのあり様についての課題と対応策も示した。この届出制度は、学内情報基盤の維持管理に責任を持つ組織を設定している大学に適用できる。もし、本論文にいうところの制度を運営できる常設組織がない場合には、CIO の権限のもとでコンサルティングチームを編成することで提案する仕組みを構築できる。この点についても、事例を挙げて実際の運用による効果も述べた。社会が求める「全学一体運営」に向けた IT 化の活動の中で、一般的な教職員が陥りがちな情報システム導入時の不具合を専門家が未然に防ぐ可能性を格段に高めるという意味で、届出制度は有効な仕組みである。また、学内の情報システムを網羅的に把握するという意味で、内部統制に向けて有用な学内現状把握の仕組みであると言える。単なる届出だけではなく、適宜専門家によるコンサルテーションが実施されることで、学内情報システムの品質向上をもたらす点においても、提案する届出制度は有用である。

第 4 章では、実効性のある ISMS の構築・運用について事例を紹介するとともに学外監査が重要であることを述べ、サンプル規程集を利用して実効性のある ISMS を構築し運用することの可能性について考察を加えた。ポリシー通りに実務が実行されていることを証明する仕組みを確立する必要があり、内部監査や第三者機関（別法人）による審査がこの仕組みに当たることも述べ、学外機関による監査の仕組みを組み込んだ ISMS の導入を提案した。これらの仕組みを組込んで実効性のある ISMS を確立するにあたり、国立情報学研究所が公表しているサンプル規程集を使用する為には追加すべき仕組みや文書があることも述べ、その内容を示した。また、ISMS 規格に準拠できる可能性についても述べた。これらの考察から、ISMS 認証取得はサンプル規程集のみで構築された仕組み（ISMS）をよ

り実質的なものに変える効果があることが判る。これらのことを受けて、サンプル規程集をISMS マニュアルの中心として、ISMS における PDCA サイクル中の C フェーズに当たる内部監査や第三者機関による審査の仕組みを加えて ISMS を構築することを提案した。今後、情報セキュリティレベル向上の仕組みとして、学外からも信頼される ISMS が、より多くの大学において構築・運用されれば、高まる情報セキュリティリスクの低減に寄与できる。

これまで述べたように、研究目的である「国立大学法人における IT ガバナンス確立に向けた組織面での基礎的な仕組みを考案し、その実装結果を確認すること」ができた。これにより当初の本研究課題は解決され、次のようなメリットをもたらすことが判った。

① 国立大学法人において、学長をはじめとする大学執行部による IT ガバナンス面でのリーダーシップを支援する仕組みの一翼を担う仕組みが具体化される。

ⅰ) 情報システム届出制度により、二重開発や無駄なコストの発生を防止もしくは削減できる。

ⅱ) 情報システム届出制度により、大学の運営方針に沿った情報システムの開発・運用への方向付けができる

ⅲ) ISMS により、その適用範囲における情報資産を網羅的に掌握でき、それらが持つリスクとその対策を法人として統制することが可能になり、情報セキュリティレベルが年々向上する。

② 情報システム届出制度により情報システムの仕様面を、ISMS によりデータを中心とする情報資産を、それぞれ大学執行部(もしくは CIO)が掌握できる。

③ 将来における、学内情報システム全体のスリム化が可能になる。

5.2 今後の課題;IT ガバナンス確立に向けた展望

多くのコンサルテーション事例により、今後の国立大学内情報システムが必要とする IT に関する知見(とりわけ導入計画時の失敗事例)が蓄積されれば、今後の学術面・技術面の発展に寄与できる。即ち、届け出られた情報システムの導入・運用の実態を調査し比較・分析することにより、今後の学内情報基盤のさらなる整備・発展が進む。

これは次の理想に向かって情報化を推進することでもある。

- 同じ機能を持つ情報システムは学内で1つのみ稼働する。
- 同じデータの入力は学内では 1 か所のみで良い。

さらには、大学間での共通化・標準化に発展させることもできる。

また、届出制度を通じて得られた知見を一般化することにより、ICT あるいは情報セキュリティに関する実践的教材として情報関係教職員の教育に役立てることが可能である。急

速な ICT の進歩・革新の中で、I/O 機器の多様化・小型化・マルチメディア化等、学内情報システムそれぞれが今後対応すべき一般的な課題も多い。このことは必然的に学内情報システムの変化をもたらすことになり、情報基盤整備は今後とも継続される。そこで、理想とする情報システム維持管理のあり様に向かって、改めて本論文で提案した 2 つの仕組みの普及を提案するものである。組織体として責任を持って、そして統率された状態での安全・安心な情報システムの維持管理を目指している大学に、当制度を適用することは意義深い。

ただ、本研究の段階では「初期届出制度」で収集・蓄積しようとした付録 A で示すデータを、届出義務化を優先する為十分蓄積できていない。今後の課題として、この点を改善することが必要となる。

(1)学内情報システムや諸データ(コードを含む)の標準化

(2)類似機能の情報システムの 2 重開発防止

(3)情報システム管理体制の簡素化・効率化

ここで、当制度を適用する為の留意点を、本学における制度運営経験から得た知見からまとめておく。逆にいうと、これらの留意点に対応できるあるいは対応しようとしている大学にとって、当制度はより有意義な制度となると考える。

① 当制度を構成する為には次の 3 つが必要である。制度を運営する委員会組織、届出案件の受付・登録等を処理する届出案件管理システム、そして構成員が守るべきルールの 3 つである。

② 届出案件管理システムは、学内構成員が自分のいる場所から届出書を入力できる仕組みを持つべきである。届出に必要なデータ項目を簡便な項目に絞り、気軽に届け出られるよう配慮が必要である。

③ 制度を運営する委員会組織には、学内ネットワークに詳しい要員を含めるとともに、情報システムの種類に応じて届出者から意見を聴く為に、適宜専門家に意見を求めることができる仕組みが必要である。

④ 構成員が守るべきルールにおいては、届出の必要な情報システムとそうでない情報システムの違いを明示すべきである。

ちなみに、本学は文部科学省の調査資料「国立大学法人の財務分析」[20]の第 2-1 表「国立大学法人の財務分析上の分類」において「中規模病院有大学(G グループ)」に分類されており、次のような条件のもとにあることを補足する。

a) 学内の情報基盤整備を担う全学委員会を設置しており、情報基盤整備に関する学内規則を起案し制定を主導できる。
b) 前項記載の委員会を技術面でサポートする情報系センターが設置されている。
c) CIO と CISO により、情報システムの全学統一的管理を目指している。(前記分類において「大規模大学(A グループ)の中には「部局に任せれば良い」との方針の大学もある。)
d) 技術的にも時間的にも本論文でいう「コンサルティング」可能な教員が所属している。

なお、本学の教職員数や学生数等大学の概要については、本学のホームページの「大学紹介」の Web ページを参照されたい。

IT の進歩が著しいのは周知のことであるが、クラウドシステム(あるいはクラウドサービス)、BYOD(Bring your own device)、IOT(Internet of Things)の台頭とともに大学法人の責任範囲や維持管理の在り方にも時代の流れとともに大きな変化が生じている。「学内」という用語を単に地理的な範囲と捉えるだけでは不十分とも考えられる。さらには、IR(Institutional Reserch)やオープンサイエンス等、データの維持管理に関する変化の流れもあり、情報セキュリティの考え方にも変化をもたらしている。情報資産の有効活用や共同利用など、情報資産の可用性(あるいは利便性)を高める要請がある中で、機密性の維持も求められ、バランス良い情報セキュリティを必要としている。社会が求める「全学一体運営」に向け、当制度がITのガバナンスとITによる(大学の)ガバナンス整備に引き続き貢献できることを確信する。

参考文献

[1] ISO&IEC（2013）:『情報システムーセキュリティ技術ー情報セキュリティマネジメントシステムー要求事項（英和対訳版）ISO/IEC 27001:2013』、日本規格協会

[2] IT ガバナンス協会編、[2008]、「COBIT 4.1」･･･ 松尾明監訳、ISACA 東京支部翻訳

[3] あずさ監査法人パブリックセクター本部（2006）『国立大学法人の内部監査 東京大学における内部監査実践例』第一法規、pp56～57

[4] 天野郁夫（2008）『国立大学・法人化の行方 自立と格差のはざまで』東信堂

[5] 天野郁夫・他、[2007]、「国立大学法人の財務・経営の実態に関する総合的研究」、『日本学術振興会 科学技術研究費補助金 最終報告書 基盤研究（A） 課題番号15203033』、最終報告書

[6] 石島隆 著、[2005]、『情報システムの内部統制』、中央経済社、pp.8-9

[7] 市川哲彦、小柏香穂理、永井好和、小河原加久治（2011）: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（IPSJ SIG Technical Report）Vol.2011-IOT-14 No.6、pp.1-6

[8] KDS国大協サービス、『国立大学リスクマネジメント情報2011年2月号』、http://www.janu-s.co.jp/mail_magazine_html_data/pdf/2011/h2302.pdf（2012-2-11 アクセス）

[9] 甲賀憲二・林口英治・外村俊之 著、[2002]、『IT ガバナンス』、NTT出版、p.42

[10] 国立情報学研究所 学術情報ネットワーク運営・連携本部（2015）:高等教育機関の情報セキュリティ対策のためのサンプル規程集（2015 年版）、http://www.nii.ac.jp/csi/sp/ 、(2016-5-10 アクセス)

[11] 国立大学の独立行政法人化に関する調査検討会議（2002）『新しい「国立大学法人」像について;国立大学の独立行政法人化に関する調査検討会議最終報告「Ⅱ組織業務」』文部科学省

[12] 佐野雅彦、八木香奈枝、上田哲史（2014）:徳島大学情報センターにおける ISMS の効果、学術情報処理研究 No.18、pp.90-98

[13] JIPDEC ISMS 適合性評価制度技術専門部会（2014）:『ISMS ユーザーズガイドー JIS Q 27001:2014 （ISO/IEC 27001:2013）対応』、JIPDEC

[14] JIPDEC 情報マネジメント推進センター（2014）:『ISMS 適合性評価制度に関するアンケート調査報告書』、JIPDEC

[15] 情報セキュリティ政策会議（2014）:政府機関の情報セキュリティ対策のための統一基準群（2014 年度版）、
http://www.nisc.go.jp/active/general/kijun26.html、(2015-11-5 アクセス)

[16] 大学 CIO フォーラム(2006)『大学革新のための IT 戦略(「大学革新のための IT 戦略」提言書)』三菱総合研究所&Microsft、p.13

[17] 日本 IT ガバナンス協会(2008)『COBIT 実践ガイドブック』日経 BP 社、p.14

[18] 福島真司・馬越徹、[2006]、「国立大学法人におけるガバナンス改革の研究」、『桜美林大学大学院国際学研究科修士論文』、2005 年度修士論文

[19] 文部科学省、[2006]、「文部科学省行政効率化推進計画」（2006 年 8 月 29 日改定版）

[20] 文部科学省科学技術政策研究所第 1 調査研究グループ(2008)『国立大学法人の財務分析』調査資料-150 第 2-1 表、
http://www.nistep.go.jp/achiev/ftx/jpn/mat150j/pdf/mat150j.pdf(2014-2-24 アクセス)

[21] 文部科学省高等教育局、[2005]、「独立行政法人等の業務・システム最適化実現方策について」、『事務連絡』、2005.12.28 付

[22] 文部科学省(1999 以前):「国立大学の法人化の経緯」、
http://www.mext.go.jp/a_menu/koutou/houjin/03052701.htm、(2016-7-18 アクセス)

[23] 山本富夫（2012）:ISO 審査機関からみた国立大学法人の ISMS、学術情報処理研究 No.16、pp.197-199

[24] @IT 情報マネジメント編集部:「IT ガバナンス」、
http://www.itmedia.co.jp/im/articles/0302/28/news031.html、(2016-12-28 アクセス)

付録 A　初期届出制度における主要書類

ここに掲載するのは、初期届出制度の事務フローに記載のある書類の様式である。著者が起案し情報基盤整備委員会に提案した最終案である。次の3種類（6様式）のレイアウトを次頁以降に掲載する。

1. 届出書（様式１－１）……情報システム導入計画検討申請書（案）
2. 届出書（様式１－2）……導入する情報システムの概要（案）
3. 意見書（様式2）……情報システム概要・意見書（案）
4. 完了報告書（様式3-1）・・・情報システム導入完了報告書（案）
5. 完了報告書（様式3-2）・・・情報システム導入報告書（案）
6. 完了報告書（様式3-3）・・・情報システム概要書（導入完了時点）（案）

様式１－１

管理№.

情報システム導入計画検討申請書(案)

山口大学
　情報基盤整備委員会委員長　殿

標記の件、下記の情報システム導入計画を検討頂きたく、申請致します。

申請部局(部署)：
申請責任者：　　印
申請者：　　印
(　連絡先内線　：　　)

記

1.	導入計画名称	:
2.	導入する情報システム名称	:
3.	検討結果回答希望期限	: 年　月　日(　)
4.	検討結果回答先	:
5.	添付資料 (1). 導入する情報システムの概要 (2). その他補足説明資料　①. ②. ③. ④. ⑤.	

様式１－２

管理No.

導入する情報システムの概要（案）

導入計画名称	導入する情報システム名称	導入部署	運用開始予定時期	運用終了予定時期
			年　月	年　月
導入責任者	(氏名)	(TEL;内線)	(Mail ｱﾄﾞﾚｽ)	
事務担当者	(氏名)	(TEL;内線)	(Mail ｱﾄﾞﾚｽ)	
技術担当者	(氏名)	(TEL;内線)	(Mail ｱﾄﾞﾚｽ)	

システム化の概要（目的等）と 範囲 （他の情報システムとも関連あれば可能な範囲で記入）

山口大学中期目標・計画との関連 と 費用対効果

予算内訳（もしくは導入費見積り）及び予算確保の状況	総予算額
	千円

導入作業体制・運用体制

利用者（下記の中で○印）;その他の場合、利用者の条件を（ ）内に記載
教職員 ・ 学部学生 ・ 大学院生 ・ 学外者 ・ その他（ ）

アクセス可能範囲（下記の中で○印）;特定部局かその他の場合、具体的内容を（ ）内に記載
学外 ・ 学内 ・ 特定部局（ ） ・ その他（ ）

利用者の本人確認の必要性 と アクセス制限の必要性
[本人確認 ： 必要 ・ 不要]　　[アクセス制限 ： 必要 ・ 不要]

様式２

管理No.

情報システム概要・意見書（案）

<table>
<tr><td>情報システム名称</td><td>システム所掌部署</td><td colspan="3">担当部会等名</td></tr>
<tr><td></td><td></td><td colspan="3"></td></tr>
<tr><td colspan="2">システム概要・機能概要</td><td>運用（維持管理）体制</td><td colspan="2">資産計上予定額</td></tr>
<tr><td colspan="2" rowspan="4"></td><td rowspan="4"></td><td>ﾊｰﾄﾞ</td><td>千円</td></tr>
<tr><td>ｿﾌﾄ</td><td>千円</td></tr>
<tr><td colspan="2">運用費月額見込み</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">システム構成（ﾈｯﾄﾜｰｸ構成）</td><td>DBMS 名称</td><td colspan="2">他大学等との比較</td></tr>
<tr><td colspan="2" rowspan="3"></td><td rowspan="2">（ □ 市販ｿﾌﾄ
□ 自主開発
□ ﾌﾘｰｿﾌﾄ ）</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>個人認証方式</td></tr>
<tr><td colspan="2"></td><td colspan="2">国内外の技術比較</td></tr>
<tr><td colspan="2">前提サーバ・ハード構成</td><td colspan="3">前提クライアント・ハード構成</td></tr>
<tr><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">前提サーバ・ソフト構成</td><td colspan="3">前提クライアント・ソフト構成</td></tr>
<tr><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2">費用対効果</td><td colspan="3">開発工数見積</td></tr>
<tr><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="5">備　　考　（必要に応じて適宜詳細資料を添付）</td></tr>
<tr><td colspan="5"></td></tr>
</table>

様式３－１

管理No.

情報システム導入完了報告書(案)

（※開発完了時運用開始前の時点で提出してください。）

山口大学

情報基盤整備委員会委員長　殿

標記の件、下記の情報システム導入を完了致しましたので、報告致します。

申請部局（部署）：

申請責任者：　　印

申請者：　　印

（ 連絡先内線 ：　　）

記

１．　導入計画名称　　：		
２．　導入した情報システム名称　：		
３．　添付資料		
	(1). 情報システム導入報告書	
	(2). 情報システム概要書	
	(3). その他補足説明資料	①.
		②.
		③.
		④.
		⑤

様式３－２

管理No.

情報システム導入報告書(案)

情報システム名称	導入部署	導入責任者	事務担当者
		<TEL>	<TEL>
運用開始期日	年　月　日	<Mail>	<Mail>

導入作業期間(プロジェクト設置期間)	自：　年　月　日 至：　年　月　日	総費用	千円

システム化の概要(目的等) と 範囲

山口大学中期目標・計画との関連 と 費用対効果 (計画時との差異がある場合に記載)

導入費実算内訳 と 予算対比	開発完了時 資産計上総額
	千円
	運用経費予定額(月額)
	千円/月

導入ﾌﾟﾛｼﾞｪｸﾄ自己評価(進捗管理、品質管理、開発規模管理、ｾｷｭﾘﾃｨ管理、文書管理、要員管理、外注管理、など)

利用者(下記の中で○印);その他の場合、利用者の条件を( )内に記載
教職員 ・ 学部学生 ・ 大学院生 ・ 学外者 ・ その他( )

個人認証の有無	アクセス権限設定方式
有 ・ 無	

導入作業体制(プロジェクトメンバー別担当一覧)	開発工数

備　考

様式３－３

	管理No.

情報システム概要書（導入完了時点）（案）

情報システム名称	システム所掌部署	導入責任者	技術担当者
運用開始予定時期	年　月　日	<TEL>	<TEL>
運用終了予定時期	年　月　日	<Mail>	<Mail>

システム概要・機能概要	運用（維持管理）体制

資産計上額	
ハード	千円
ソフト	千円

システム構成（ネットワーク構成）	DBMS 名称	他大学等との比較
	□ 市販ソフト □ 自主開発 □ フリーソフト	
	個人認証方式	国内外の技術比較

サーバ・ハード構成	クライアント・ハード構成

サーバ・ソフト構成	クライアント・ソフト構成

システム規模				運用情報			
①	（開発言語１）	（　）		①	サービス提供日		
	プログラム本数		本	②	サービス提供時間帯		
	ソースステップ数	(行)	step	③	バッチ処理サイクル	（日次）	回
②	（開発言語２）	（　）		④		（週次）	回
	プログラム本数		本	⑤		（月次）	回
	ソースステップ数		step	⑥		（年次）	回
③	想定クライアント数		台	⑦	DB 容量		GB
④	DB 上データ項目数		項目	⑧	その他ファイル容量		GB
⑤	入力フォーム数		パイト	⑨	プログラムエリア容量		GB
⑥	出力フォーム数		種	⑩	外部接続データ		
⑦	帳票数		種				
⑧	DB 以外の入出力ファイル数		ファイル				
⑨	開発期間	～					
⑩	移行期間	～					

作成予定ドキュメント				
	業務運用マニュアル	既存流用・作成・不作成	データ仕様書	既存流用・作成・不作成
	システム操作マニュアル	既存流用・作成・不作成	（画面・テーブル定義等）	
	業務処理設計書	既存流用・作成・不作成	用語辞書	既存流用・作成・不作成
	機能仕様書	既存流用・作成・不作成	コードブック	既存流用・作成・不作成
	プログラム一覧	既存流用・作成・不作成	性能設計書	既存流用・作成・不作成
	プログラム仕様書	既存流用・作成・不作成	信頼性設計書	既存流用・作成・不作成

備考		その他（詳細別添）	

付録 B　初期届出制度における届出基準

平成16年9月10日

山口大学における情報システム導入届出基準(案)

学術情報機構

本年より国立大学法人山口大学がその活動を開始し、本学の今後6年間の活動規範となる中期計画が定められた。この中で以下の内容が定められている。

① (#115) 学術情報機構は、大学全体の情報基盤整備、情報化推進を戦略的に進める。

② (#364) システム間及び部局間での共有データ等の全学統一管理ルールを定め、ネットワークによる業務全体としての効率性向上に努める。

③ (#441) サーバーの集中化を進め、学内情報ネットワーク上のセキュリティ管理を学術情報機構で統括する。

これらの計画を達成するべく、学術情報機構において新規導入案件を把握し、学内での情報化投資の2重化を避けるとともに、持てる技術・知識を駆使して、費用対効果を意識したより良い情報化を目指したい。そこで、標記基準を設定し、情報システム導入案件把握の仕組みを用意する。

1．　目的

学内に導入される情報システムの開発・運用・維持を効率的で有効なものとすることを目的とし、その必要な届出基準を定める。これは、山口大学において利用する情報システム(以下、「情報システム」という。)が以下の原則で維持管理されることを目指すものである。

①. 1個のデータ(項目)の入力が全学で1箇所のみであること。

②. 同様の業務を処理する情報システムが全学で1個であること。

この目的の早期実現に向けて学術情報機構では、情報システムのコンサルテーションを行うものとする。

2. 適用範囲

以下の情報システムの導入に対して本基準を適用する。

(1). 複数の学部・学科または研究室にまたがって利用(運用)される新たな情報システムの導入。

(2). 複数の学部・学科または研究室にまたがって利用(運用)されている既存の情報システムの改修。

※なお、さらに情報セキュリティ対策基準に準拠する必要がある。

3．　届け出るべき事項

[導入計画時の届出]

新規導入や市販の情報システム製品の導入または情報システムの改修を計画する者(以下、「導入責任者」という。)は、以下の様式

(1).【様式1－1】「情報システム導入計画検討申請書」

(2).【様式1－2】「導入する情報システムの概要」

を情報基盤整備委員会委員長(学術情報機構長)宛に提出しなければならない。

[調査・検討]

情報基盤整備委員会の下、各専門部会は、届けられた申請書に対して当該導入計画の調査・検討及びコンサルテーションを実施し、その結果及び意見を導入責任者に【様式2】「情報システム概要・意見書」にて通知しなければならない。

[導入完了時の届出]

導入責任者は、情報システムの運用開始時に導入計画と実際の導入との比較及び情報システムに対する自己評価を実施し、以下の様式

(1).【様式3－1】「情報システム導入完了報告書」
(2).【様式3－2】「情報システム導入報告書」
(3).【様式3－3】「情報システム概要書(導入完了時点)」

を情報基盤整備委員会委員長(学術情報機構長)宛に提出しなければならない。

4. 申請書等届出先

学術情報部学術情報課情報企画係

(受付申請書類の回示ルート)

学術情報部　情報企画係 → 情報基盤整備委員会(企画調整会議) → 情報基盤整備委員会(各専門部会) →
情報基盤整備委員会(企画調整会議) → 情報基盤整備委員会委員長 → 学術情報部 情報企画係

5. 届出様式(添付資料)

(1). 導入計画時の届出様式
①.【様式1－1】「情報システム導入計画検討申請書(案)」
②.【様式1－2】「導入する情報システムの概要(案)」
(2). 導入計画時の検討・コンサルテーション結果様式
①.【様式2】「情報システム概要・意見書(案)」
(3). 導入完了時の届出様式
①.【様式3－1】「情報システム導入完了報告書(案)」
②.【様式3－2】「情報システム導入実績報告書(案)」
③.【様式3－3】「情報システム概要書(導入完了時点)(案)」

6. 附則

(1). 本基準は、平成 16 年4月1日から適用を開始する。
(2). 本基準は、平成 16 年度の活動状況により見なおすものとする。

以　上

付録 C　経営情報学会予稿「ISMS 適用範囲拡大における留意点」

ISMS 適用範囲拡大における留意点
Considerations in ISMS scope expansion

永井好和[†]　多田村克己[†‡]　小河原加久治[†‡]

Yoshikazu NAGAI[†]　Katsumi TADAMURA[†‡]　Kakuji OGAWARA[†‡]

[†] 山口大学大学情報機構メディア基盤センター

[‡] 山口大学大学院理工学研究科

[†] Media and Information Technology Center, Organization for Academic Information, Yamaguchi Univ.

[‡] Graduate School of Science and Engineering, Yamaguchi Univ.

（要旨）

山口大学（以下、「本学」）では、ISMS 適合性認証を受け、情報セキュリティ面での改善活動を進めている。当初、学内組織の一部を適用範囲としたあと、他の学内組織に拡大する場合には、さまざまの作業が発生する。各種文書の改訂作業はもちろん、新たに拡大する組織の所属員への教育が必要である。本稿では、ISMS 適用範囲拡大の際の留意点についての知見を、新規要員の教育を中心として整理し報告する。

（Abstract）

In Yamaguchi University, the improvement activities in respect of an information security are advanced in response to ISMS conformity attestation. As the first step, a part of organization had been the scope of the ISMS, then the scope expansion of ISMS is planned as the next step. When the expansion is executed, various kinds of work arise in this step. The education to the affiliation member of the organization which newly expands is required as well as the revised work of various documents. This paper reports the important matter in the case of ISMS scope expansion focusing on a new staff's education.

1. はじめに

(財)日本情報経済社会推進協議会(JIPDEC ; Japan Institute for Promotion of Digital Economy and Community)は、日本の組織体の情報セキュリティマネジメントシステム(ISMS ; Information Security Management System)が国際規格「ISO/IEC 27001」もしくは国内規格「JIS Q 27001」に適合することを認証する ISMS 適合性認証制度[1]を運営している。JIPDEC によれば、日本では 2014 年 3 月 27 日現在 4,493 の組織がこの認証を受けている[2]が、この中で大学はわずか 10 校である。そのうち国立大学 8 校は全て情報系センターを適用範囲とするもので、7 校が教員が中心となって ISMS を構築している。本学では 2008 年 10 月にメディア基盤センターがこの認証を取得し、以後毎年 1 回第三者機関による審査を受けてその認証を維持している。教員が中心となって ISMS を構築したものである。認証の有効期間は 3 年であり、今年 10 月には 2 回目の更新審査を受ける予定である。現在迄に事務組織への適用範囲拡張を 2 回実施しており、今年 4 月には 3 回目の範囲拡張作業を開始した。本稿では 2 回目の適用範囲拡張時の記録から課題を整理し、今年度の拡張に活かすと共に、広く学外にもその知見を生かして頂きたく、本

稿を執筆することとした。第 2 章で拡張作業の状況を述べ、第 3 章では課題を整理して今後の適用範囲拡張作業での留意すべき事項について説明する。最後に第 4 章で纏めを行う。

2. 今までの適用範囲拡張の状況

本学には学内共通の業務を遂行する為 3 つの学内機構が設置されており、現在 ISMS 適用範囲は、図 1 で示す ISMS 運用体制の一点鎖線で囲まれた C の範囲であり、2 つの機構に跨っている。

最初の適用範囲は図 1 の A に示す範囲である[3]。1 回目の拡張は図1の A の範囲から B の範囲への

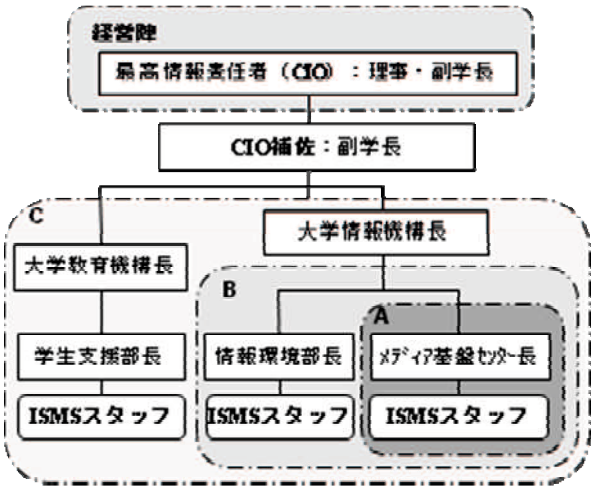

図 1 ISMS 組織体制図

拡張である。教員中心の組織であるメディア基盤センターから、事務系情報システムを維持管理する事務組織という意味で異質な組織体への拡張であった[4]。同じ機構長の指揮下にあり、学内の情報システム運営という業務内容に共通点のある組織体への拡張であった。2 回目は図 1 の B の範囲から C の範囲への拡張である。異なる機構に属する事務部門であり、教務情報を取り扱う事務組織という、業務内容の異なる組織への拡張であり、1 回目とは別の工夫を必要とした。情報系センター以外の事務組織を適用範囲に含めての適合性認証取得は、国立大学では初めてである。

2 回目の適用範囲拡張作業は、両機構長間の「導入を検討する」ことの合意から始まり、両機構数名ずつのメンバーからなる ISMS 導入検討ワーキンググループ（以下、「WG」）を中心に進めた。WG は年度初めから 10 回のミーティングを通して作業を進め、従来より ISMS を運用している教員が ISMS 構築経験を基に WG を主導する形で進めた。何よりも留意した点は、新たな作業負担を可能な限り増やさないことと、内部監査や審査と言った言葉から来る「管理される」という意識や未知の作業への不安をできる限り生じさせないことであった。表 1 に示す一連の WG 活動では、幹となる作業項目に限定して作業量を減らし、内部監査や第三者監査（以下、「審査」）では現場のありのままをチェックしてもらい、自らの業務を見つめ直す方針で臨んだ。結果、その年度の審査の際には、拡張後の適用範囲を対象とすることが出来た。ここで、内部監査迄に実施した、幹となる 4 つの作業について順次説明する。

表 1 ISMS 適用範囲拡張 WG の状況

回	主な作業	発生した課題
0	WG 設置に関する合議 (機構長・部長出席)	・現場職員への導入作業に伴う負担軽減要求
		・第三者機関による監査（審査）費用の分担明確化
		・ISMS への所属員の理解
		・ISMS 導入の効果の確認
1	WG 活動内容の確認とﾐｰﾃｨﾝｸﾞ開催の頻度	
2	ISMS 概要説明	・ISMS 初任者研修会の受講
3	ISMS の基本方針・ 適用範囲の確認	・ISMS スタッフ会議への参加
		・ISMS 文書の修正（新たに導入する組織の構成員に文書修正ができるか？）
		・業務や場所を限定する場合の適用範囲の決め方
4	情報資産洗出し	・適用範囲の境界を行き来する情報の取り扱い方確定
5	ﾘｽｸｱｾｽﾒﾝﾄ手順の確認	・ﾘｽｸｱｾｽﾒﾝﾄ実施
6	ISMS 文書改訂改訂 (ISMS 文書へのｱｸｾｽ等、具体的作業実施方法の確認を含む)	・各種情報資産へのアクセス権限の確認。特に、ISMS 文書修正作業における人的排他制御
		・拡張部分の受審開始時期
		・審査機関への変更通知 (変更点の整理)・・・事業所名称や業務内容の表現
7	ﾘｽｸｱｾｽﾒﾝﾄ結果ﾚﾋﾞｭｰ	・脅威や脆弱性の内容が人により異なる。
		・資産価値・脅威・脆弱性のレベル設定が人により異なる。

8	内部監査指摘事項対応	・指摘事項により業務のやり方を（職場環境の変更を含めて）変える場合の、現場の理解（マネージャーや予算管理者を含めて）
9	第三者監査対応準備	・改善項目の優先順位付け
10	C フェーズでの指摘対応（A フェーズ）	・新たに加わった教職員の監査に対する不安

(1) 教育・・・新たな ISMS スタッフに ISMS とは何かを理解して頂き、従来からの ISMS 基本方針を説明して、適用の可否を検討した。

(2) 適用範囲の設定・・・物理面・人材面・業務面それぞれにおける適用範囲の境界を明確にし、組織構造と所属職員の役割の再確認を実施した。

(3) 情報資産の洗出しとリスクアセスメント・・・従来からのリスクアセスメントのやり方の適用可能性を検討した上で、新たな適用範囲（以下、「新範囲」）における情報資産を洗出し、リスクアセスメントを実施した。

(4) ISMS 文書の改訂・・・従来からの ISMS 文書（マニュアルや手順書等）それぞれについて、新範囲に適用可能となる様、修正を加えた。この過程で、ISMS 適合性認証制度の為の適用宣言書記載の各管理策の適用可否を検討した。

3. 適用範囲拡張時の留意点

3.1 新範囲の特徴

大学における ISMS の特徴については文献[5]を参照頂くとして、ここでは本学での ISMS 適用範囲拡大作業の特徴について述べる。

(1) 国立大学法人内の教員中心の組織に、事務職員からなる組織を、同じ管理手順（あるいは基準）の ISMS 適用範囲に加え、1 つの組織体としての ISMS 再構築である。教員の勤務時間帯は本人の裁量に任されているが、事務職員の勤務時間帯は固定され基本的に超過勤務可能な範囲は限定的である。

(2) 新範囲の所属職員に ISMS に関する知識も関心もほぼない状況で ISMS 導入が決定されている。

(3) 作業着手から内部監査を受ける迄の期間が 4 カ月と短い。

(4) 新範囲所属員が担当する業務の一部に ISMS を適用する為、職場には ISMS による管理下にある情報（書類や電子媒体）と、そうではない情報が混在している。

3.2 課題と対策としての留意点

新範囲への ISMS 導入作業上、表 1「発生した課題」欄に示す様々な課題に対処して行った。これらの中で、今後さらに ISMS 普及を進める上で留意すべき主な事項は以下の通りである。

(1) 新範囲所属員の教育：まず何よりも大切なことは、新範囲所属職員の ISMS への理解と協力であり、その為の教育である。ISMS を運用する人たち自身が、PDCA(Plan-Do-Check-Act)を業務の中で実践できる様にならなければならないからである。その為の施策として次の 3 点を挙げる。

① 身の回りの情報セキュリティに関する意見交換の場・・・会話の中で、従来からの業務や仕事の中に潜む脅威に気づかせて、それを防止する必要性を感じてもらう。さらにどう対策すれば良いかという疑問を抱いてもらうことが重要であり、情報セキュリティを組織として管理する必要性に気づいてもらう。小人数のミーティング形式で数回実施する必要がある。

② ISMS 研修会・・・ISMS 構築の中で重要な項目について座学と演習を実施する。情報セキュリティ基礎、ISMS 概要（機密性・完全性・可用性の理解やリスクアセスメント、管理策の考え方等）、PDCA サイクル、国際規格、有効性測定等の座学ののち、リスクアセスメント演習をグループ学習の形で実施する。本学では、この研修会を年に 1 度実施して新範囲内に異動（新たな任用を含む）になった教職員全員に受講を義務付け、学内外にも案内している。

③ ISMS スタッフ会議(2 週間に一度全 ISMS スタッフが集まり意見交換する場として位置づけられる会議) への参加・・・新範囲所属職員のうち WG メンバーにオブザーバとして参加し、従前の適用範囲における ISMS の活動実態を理解してもらうと共に、新範囲における ISMS との関連を理解してもらう。

(2) ISMS 骨格作り・・・次の各項目について、WG メンバー全員で適用範囲拡張後の姿を明確にしていく。このとき大切なのは、WG メンバーが一緒になって作業を行うことである。個々の細かな作業について分担するとして

も、作業状況やその内容については WG 全員が共有する。実作業としては、ISMS マニュアルや管理策手順書等の各種文書の修正をとおして拡張後の ISMS の形を確定して行くことになるが、新組織の WG に入っていない所属員の ISMS 関連の実作業分担は期待できない。

① ISMS 基本方針の確認･･･新範囲において従前の基本方針を受け入れられるかどうかを検討する。

② ISMS 適用範囲の確定･･･人的適用範囲、物理的適用範囲、業務上の適用範囲等について検討し、ISMS 文書に反映して行く。物理的適用範囲に関して注意が必要なのは機密性のレベルによる分類で、次の 3 分類が考えられる。

a.適用範囲外の人の立入りを一切認めない場所

b.適用範囲内の人の立会の元で適用範囲外の人が立入る場所（さらに限定される場合もある）

c.適用範囲外の人も自由に立ち入れる場所

業務上の適用範囲検討においては、業務間（あるいは担当者間）を行き交う情報について、どの範囲までを範囲内とするか、良く見極める必要がある。発生・伝達・記録・保管・廃棄（消滅）のライフサイクルを明確にする必要がある。

③ 情報資産の洗出し･･･ISMS の中で管理対象となる物品や情報等、全てを一覧表にする。新範囲所属のメンバーが洗出し、従来からの ISMS 適用範囲内の WG メンバーがレビューする。

④ リスクアセスメント･･･留意点は 2 点である。

a.従前のリスク要因のレベル分けが新範囲に適用可能かどうかの見直しが必要であるが、まずは従来どおりのレベル分けでのリスク評価をするのが現実的である。

b.脅威のレベルを発生頻度で分ける場合が多いが、大地震等極めて頻度が少ないが影響が極めて甚大なリスクに対しては、一般の受容基準とは別の基準を設定するのが良い。リスク値は小さいが受容すべきでない場合がありうる。

⑤ ISMS 文書の再確認･･･従前の文書に記入されている内容を、新範囲に適用できるかどうかを見直す必要がある。特に、採用すべき管理策は、業務の違いにより従前の適用範囲と異なる可能性がある為再確認する作業は避けられない。ただ期間が短い現実の中では、内部監査により ISMS 文書と現実との差異を指摘される可能性を許容せざるを得ない。これらについては、次の PDCA サイクルで是正していくのが現実的である。また、文書修正を新範囲の所属員だけで実施するのではなく、WG の中で作業を吸収することが望ましい。

(3) 監査への不安解消･･･一般的に「監査」と聞くと怖いものという印象を持つ人が多い。ISMS の運用スケジュールに内部監査や外部審査が含まれると聞いて、ISMS そのものに拒絶反応を示す人もいる。前述の様に、早くから ISMS スタッフ会議に参加することにより、前年度の「監査」や「審査」の状況を聞いて指摘事項への対応を一緒に考えることにより、不安を和らげることができる。

4. おわりに

2 回の ISMS 適用範囲拡張作業のうち、2 回目の作業を通して得た「ISMS 適用範囲拡張に際しての留意点」について報告した。本学では、今年度 3 つめの機構への拡張を計画している。本稿で述べた留意点に配慮しながら拡張作業を進めることにより無事拡張を終えることはもちろんであるが、さらなる留意点を含む新たな知見を得ることを期待している。

参考文献

[1] JIPDEC，ISMS 適合性評価制度，http://www.isms.jipdec.or.jp/isms.html (Apr.24.2014).

[2] JIPDEC，認証取得組織数推移，http://www.isms.jipdec.or.jp/lst/ind/suii.html (Apr.24.2014).

[3] 永井好和;「国立大学における情報セキュリティマネジメントシステム運用事例」,「大学行政管理学会 第 15 回定期総会・研究集会 資料集」, 2011, pp67-68.

[4] 市川 哲彦，小柏 香穂理，永井好和，小河原加久治「[招待講演]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. IOT, [インターネットと運用技術]」, 2011-IOT-14(6), 1-6, 2011-07-08 .

[5] 静岡大学 ISMS 研究会,「10.大学の ISMS」, 井上春樹,『実践 ISMS 講座』, (株)ITSC, 2007, pp86-91.

以下余白