

学位論文内容の要旨	
学位論文題目	国立大学法人における組織的 IT 基盤強化策の研究 — IT ガバナンスの観点から —
氏名	永井 好和
要旨	
<p>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ており、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。そこで、大学全体として整合性を保ちつつ効率的な IT 化を進めるために、学内情報システムを全学的見地に立って情報セキュリティ保護の視点からも検討を加えた上で把握することを可能とする、学内情報システム届出制度を提案する。個々の情報システム(以下「届出案件」という)を、学内情報基盤整備を担当する委員会(以下「委員会」という)に届け出て審査を受ける仕組み(以下「届出制度」という)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という)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。筆者所属大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た。</p> <p>当制度における届出は、2010 年まで各情報システムの管理者の任意であったが、2011 年 1 月から義務化された。届出義務化後 2 年半を経て、500 件以上の届出案件と 120 件余りのコンサルテーションにおける意見が蓄積された。これらを整理することにより、頻繁に出される意見や指摘内容が明確になり、当制度が学内情報基盤整備に有効であることを確認した。本論文では、コンサルテーション事例を紹介し、学内情報基盤の更なる改善を進める為、当制度を活用することを提案する。</p> <p>一方、情報セキュリティインシデントが多発する中、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 (JIPDEC¹⁾) により認定する「ISMS 適合性評価制度」²⁾ (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。</p> <p>本論文では、山口大学での 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ために、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。</p>	

学 位 論 文 内 容 の 要 旨	
学位論文題目	Study on organizational enhancement of IT infrastructure in a National University Corporation - From the view point of IT governance -
氏 名	NAGAI Yoshikazu
<p>Abstract:</p> <p>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 may become a cause and may follow difficulty on an exchange of data.</p> <p>Then, we propose a notification system of campus information system, in order to advance efficient IT-ization and maintaining compatibility as the whole university, which makes it possible to grasp the situation of intramural IT-izing, and to add examination also from the viewpoint of information security protection. It is the mechanism of submitting notice on each 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.</p> <p>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.</p> <p>When a notification matter corresponds to predetermined conditions, WG make a consultation on the a notification matter, WG asks the person who submitted the notice for the required improvement of that matter.</p> <p>Since the effect that the problem of the individual information system, which may have been overlooked before, was solved by introducing and working this notification system in a writer affiliation university, was accepted.</p> <p>We had already mentioned above that the notification of each information system was optional with the administrator of it until the end of 2010, but it has been mandatory since the beginning of 2011. After a two-and-a-half years after the mandating, we could get more than 500 cases of the notification and more than 120 cases of the consultation. By organizing these cases, the opinions or issues which are pointed out frequently have become clear, and we have confirmed that the Notification System is effective to improve the campus information infrastructure. In this paper, we show some examples of consultation in the Notification System, and we propose to proceed further improvements of campus information infrastructure with help of the Notification System.</p> <p>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</p>	

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.

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 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.

学位論文審査の結果及び試験，試問の結果報告書

(論文博士用)

山口大学大学院理工学研究科

報告番号	理工博乙 第 141 号	氏名	永井 好和
最終試験担当者	主 査 多田村 克己 審査委員 浜本 義彦 審査委員 小河原 加久治 審査委員 王 躍 審査委員 長 篤志		
【論文題目】 国立大学法人における組織的 IT 基盤強化策の研究 - IT ガバナンスの観点から -			
【論文審査の結果及び試験，諮問の結果】 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．特に独立行政法人化前の国立大学においては，教育・研究上の必要性から学部・学科および個人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類似のシステムが稼働して組織全体の最適化の観点からは無駄を多く含んでいた．国立大学の法人化により，全学的な視点に立ったトップダウンによる意志決定の仕組みと全学一体運営が求められるようになり，情報システムにおいても大学全体としての最適化を図る必要があったが，そもそも学内に存在する情報システムをマネジメント層が掌握する仕組みを持たないため，IT 基盤強化の計画さえ立てられなかった． 一方，情報セキュリティインシデントが多発する中，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 (Information Security Management System, ISMS) の仕組み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．国立大学法人においてこの要求を実現するためには，情報資産をCIO(最高情報責任者)もしくはCISO(最高情報セキュリティ責任者)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る必要がある．この実現のため，国立情報学研究所(NII)から国立大学向けのサンプル規程集が公開されているが，規定を整備したことでセキュリティ管理が可能になるわけではないため，実用度の高いISMSを備えた国立大学はいまだに限られている． 本研究では，国立大学法人における組織的IT基盤強化策として，大学経営層が学内の情報システムを継続的に掌握できる仕組みとして機能する制度，およびISMS構築を目指す国立大学法人に対して，リスクを測定・評価して，理想とするIT活用を実現する仕組みをそれぞれ考案した．前者は，国立大学法人で初めて導入された制度であり，10年以上運用が続けられている．後者は，国際規格ISO/IEC27001に準拠して構築したISMSに対して第三者機関から適合認証を受けているISMS構築先進大学として，実用上の効果が確認されているものを提案している．本論文で提案するこれらの仕組みは，他の国立大学法人においても経営層のリーダーシップのもと適用可能なものである． 本論文の構成と内容は以下のとおりである． 第1章では，研究着手時点での国立大学法人におけるIT化の状況と，民間企業におけるそれとを対比させながら，本研究の背景と目的を概説し，本論文の概要を述べている． 第2章では，IT ガバナンスの定義を明確化し，国立大学法人におけるIT化およびそれに付随す			

る IT ガバナンスの必要性について述べ、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かなうものである事を述べ、3 章と 4 章で提案する仕組みの必要性を明確化している。

第 3 章では、IT ガバナンス実現の基礎となる学内情報システムの統一管理を実現するための情報システム届出制度を提案している。具体的には、初期制度を構築し、山口大学におけるその実装結果を分析して導入効果を明らかにしている。さらに、前述の分析結果に基づき届出者側の費用対効果に注目した改良を実施した新しい制度を提案し、実装結果を示してその有効性を示している。さらに、他の国立大学法人での制度導入が容易になるよう、整備すべき規則、関係部署の機能と役割、届出書式の例、情報の伝達手順と記録方法に関して明らかにしている。

第 4 章では、山口大学での ISMS 構築および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、今後 NII のサンプル規程集をベースにすることによりコスト押さえながら ISMS 構築を目指す大学のために、ISMS マニュアルの整備と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。具体的には、ISMS 構築のために NII のサンプル規程集には不足している事項を明らかにした上で、追加すべき仕組みや文書体系を提案している。さらに、実効性の高い ISMS 構築には、学外からの第三者による監査が必須であることを、学外監査により得られるメリットを具体的に示しながらその効果について述べている。そして、構築した ISMS の実効性を第三者に明示する必要性から、ISMS マニュアルの整備が必要であることを示している。

第 5 章では、結論として本研究により得られた成果をまとめるとともに、今後の研究課題および展望について述べている。

公聴会には学外遠隔会場も含め 20 名の参加があり、活発な質疑応答がなされた。その主な質問内容は、

- (i)現状分析及び提案システムの実装先がいずれも山口大学のみである理由、および他大学の状況調査や他大学への実装検討の有無
 - (ii)提案された仕組みの導入効果を客観的な数値で表すことの可否
 - (iii)IT ガバナンスの観点から、提案された仕組みでも解決できない課題の有無
 - (iv)提案された仕組みを IT 関係のスタッフが十分でない小規模大学に適用することの可能性
 - (v)情報システム届出制度とそれを監視する仕組みとしての ISMS の適用範囲の関連性
- についてであり、いずれの質問に対しても申請者からの的確な回答がなされた。

以上より本研究は独創性、信頼性、有効性、実用性ともに優れており、博士(工学)の論文として十分に値するものと判断した。

論文内容及び審査会、公聴会での質問に対する応答などから総合的に判断して、最終試験は合格とした。

なお、査読のある関連論文の発表状況は下記のとおりである。(下記以外 国際会議プロシーディングス 3 編)

- 1) 永井好和, 酒井清彦, 小河原加久治, 学内情報システム届出制度の提案 -国立大学における学内情報システムの統制に向けて-, 大学行政管理学会, 第 15 号, pp. 41-51, 2012.
- 2) 永井好和, 石橋英二, 多田村克己, 小河原加久治, 学内情報システム届出制度の効果と課題 -国立大学における学内情報システムの統制に向けて-, 大学行政管理学会誌, 第 17 号, pp. 55-66, 2014.
- 3) 永井好和, 多田村克己, 小河原加久治, 外機関による監査を含む情報セキュリティマネジメントシステムの提案, 大学行政管理学会誌, 第 19 号, pp. 97-107, 2016.