Vol.2012-IOT-16 No.40
2012/3/16

事例紹介: 情報系センターの情報セキュリティマネジメントシステムにおける事務系組織の役割

市 川 哲 彦[†3] 上 田 哲 史[†4] 長谷川 孝博[†1]
三 原 義 樹[†2] (五 十 音 順)

国立大学法人の情報系センターにおける情報セキュリティマネジメントシステム (ISMS) の構築が徐々に拡がりつつあるが，適用範囲を情報基盤運営としているため教員組織が適用範囲の中心になることが多い．しかしながら，大学における情報セキュリティの維持を考える上で，多くの情報システムの運営に直接的に関わり，また，個人情報など非常にセンシティブな情報の取扱いを行っているのは大学事務局であるため，より幅広い大学における ISMS の有効性を確保するためには，事務組織の関わり方を検討することは非常に重要である．そこで，本報告では，ISMS 構築と認証取得を行っている静岡大学情報基盤センター，宇都宮大学総合メディア基盤センター，山口大学メディア基盤センター，徳島大学情報化推進センターにおける事例を紹介し，大学における情報系センターを核とした ISMS 構築及び展開の方向性を検討する上での資料とすることを目的とする．

A preliminary case study: roles of administrative bureaus in and thier responsibilities for the information security management systems of information processing centers at national universities

Yoshihiko Ichikawa,[†3] Tetsushi Ueta,[†4]
Takahiro Hasegawa[†1] and Yoshiki Mihara[†2]
(in the order of the Japanese syllabary)

Information security management has been an inevitable issue at educational organizations, and several information processing centers at national universities in Japan have built and maintained information security management systems (ISMSs) to address the issue. Since these ISMSs are basically designed for information security of IT infrastructures and they are maintained mainly by educational staff, the scoped area of the ISMSs comprise educational organizations and just some (or none) of organizations in administrative bureaus. Administrative bureaus, however, play an important role in information security for information systems as well as sensitive privacy information, and investigating their appropriate roles in and responsibilities for ISMSs at universities is inevitable in securing effectiveness of and extending the scope of ISMSs. In order to provide practical information for the exploration, this report illustrates four cases in the following organizations: Center for Information Infrastructure at Shizuoka University, Media Network Center at Utsunomiya University, Media and Information Technology Center at Yamaguchi University, and Center for Administration of Information Technology at the University of Tokushima. We hope that this study of these diverse cases leads to ISMSs including various activities at universities.

1. はじめに

近年，社会における情報セキュリティに関する意識は継続的に高まり続けており，情報セキュリティマネジメントシステム (Information Security Management System, ISMS) の必要性が様々な形で協調されるようになっている．例えば，国立大学法人評価委員会は，その中期目標及び中期計画の素案についての意見[1)] において次のような指摘をし，情報セキュリティ対策に取り組む体制の確立と ISMS を動かすための PDCA サイクルの確立を求めている:

> 情報セキュリティ政策会議 (内閣官房長官) が策定した「第 2 次情報セキュリティ基本計画」及び、同基本計画の達成に向けた具体的な年度計画として定められた「セキュア・ジャパン 2009」において、独立行政法人等の情報セキュリティ対策の推進を図ることが求められている。
> (中略)
> 国立大学法人も「独立行政法人等」に含まれており、中期目標及び中期計画を通じて情報セキュリティ対策に取り組むことが求められていることから、中期目標及び

†1 静岡大学情報基盤センター
Center for Information Infrastructure, Shizuoka University
†2 宇都宮大学総合メディア基盤センター
Media Network Center, Utsunomiya University
†3 山口大学メディア基盤センター
Media and Information Technology Center, Yamaguchi University
†4 徳島大学情報化推進センター
Center for Administration of Information Technology, the University of Tokushima

ⓒ 2012 Information Processing Society of Japan

中期計画素案に情報セキュリティ対策に係る事項の記載のない下の法人に対し、中期目標及び中期計画の修正を求める。

一方，大学における ISMS の構築・運用活動も継続的に行われてきており，多くの大学において情報セキュリティポリシーが策定され，また，国際規格である ISO/IEC 27001[2)⋆1]の認証取得も，著者らの知る限りでは，南山大学 (2003 年 3 月)[3),4)]，京都大学 (2003 年 6 月)，静岡大学 (2003 年 11 月)[5)]，日本福祉大学 (2005 年 3 月)，國學院大學 (2006 年 1 月)，早稲田大学 (2007 年 1 月)，宇都宮大学 (2007 年 11 月)[6)]，山口大学 (2008 年 10 月)[7)]，徳島大学 (2012 年 2 月)[8)] において行われている．

情報系センターを核とした ISMS では，利用者認証，ネットワークシステム，ホスティング／ハウジングサービスなどの情報基盤の運営業務を対象とすることが多く，そのため，これらの運用に関わるセンター教員を中心として ISMS が構築されているケースが多い．とはいえ，センター活動は事務組織のサポート無しでは考えられないし，また，基幹となる情報システム運営を行うと同時に個人情報を含む非常にセンシティブな情報を取り扱っているのは事務局組織であるため，情報基盤だけではなく大学全体の情報管理のための ISMS への展開を考える上では，事務局組織の ISMS における役割と責任をどう捉えるかは非常に重要な課題である．そこで本報告では，上述の大学の中から国立大学法人における情報系センターを中心として ISMS 構築を行っている静岡大学，宇都宮大学，山口大学，徳島大学の４つをとりあげ，適用範囲における事務組織の関わり方について比較検討を行うことを目的としている．

以下の構成は次の通りである．まず第 2 節では，ISO/IEC 27001 における適用範囲の定義について説明を行う．これを踏まえ，次の節では各大学の ISMS における適用範囲について特に組織とサービスの概要を比較する．続いて，各大学の特徴と今後の展開について述べる．最後にまとめと今後の課題について議論する．

2. 適用範囲の定義

ISO/IEC 27001 では「4.2.1 a) ISMS の確立」において，適用範囲は事業，組織，所在地，資産，技術の５つの観点から定めるとしており，例えば，山口大学メディア基盤センターでは，次のように定めてている:[⋆2]

- **事業 (business)**　教育・研究用コンピュータの管理運用，基幹ネットワークシステムの管理運用及び業務用情報システムの運用支援．ISMS の定義文書中では事業を構成するサービス一覧が定義されている;
- **組織 (organization)**　山口大学大学情報機構メディア基盤センター及び情報環境部情報推進課．関連文書では「センター等」と略している．詳細は次節以降にて触れる;
- **所在地 (location)**　３キャンパス内のメディア基盤センター及び情報推進課．定義文書ではセキュリティレベルの分けた上で，図面上で適用範囲の詳細を識別可能にしている;
- **資産 (assets)**　事業を推進する上で必要とされる資産;
- **技術 (technology)**　大学基幹ネットワーク.

本報告では，これらのうち事業及び組織の，特に事務組織の関与の仕方に注目し，各センターにおける適用範囲の定義．その背景などの基本的な考え方，今後の展望などを比較する．

大学名	組織部門名称	登録範囲	初回登録日 (有効期限)	認証機関
静岡大学	情報基盤センター	学術ネットワークハブ拠点の管理・運営ならびに学内ネットワークおよび各種情報基盤サービスの管理・運営・提供 (静大情セ-ISMS- 2009 年 9 月 15 日発行)	2003/11/25 (2012/11/24)	JACO
宇都宮大学	総合メディア基盤センター	センター運営管理業務（情報ネットワークセキュリティ基盤，統合認証，教育研究・学術情報サービス，授業支援）	2007/11/15 (2013/11/14)	JQA
山口大学	大学情報機構メディア基盤センター及び情報環境部情報推進課	教育・研究用コンピュータの管理運用，基幹ネットワークシステムの管理運用及び業務用情報システムの運用支援 (山口大学メディア基盤センター適用宣言書: 口大情環 第 43 号, 2011/6/29)	2008/10/24 (2014/10/23)	JACO
徳島大学	情報化推進センター	徳島大学キャンパス情報ネットワークの管理運用ならびに各種全学情報システムの運用支援 (情報化推進センター適用宣言書 ISMS-B06-D04 2011/11/25)	2012/3/9 (2015/3/8)	JACO

表 1　静岡大学・宇都宮大学・山口大学・徳島大学の ISMS 登録情報 (注: 徳島大学の初回登録日及び有効期限の情報は本報告執筆時点での予定である．)

3. 情報処理センター系 ISMS の適用範囲とその特徴

本報告の対象とする四大学の ISMS の基本情報を表 1 に示す基本情報は Web ページ[9)] か

⋆1 先行規格の BS7799-2 及びその日本語版である ISMS 認証基準 (Ver 1.0, Ver. 2.0) b を含む.
⋆2 実際には図面などを用いてより詳しく定義し，境界，セキュリティレベル，セキュリティ対策等を明記している.

ⓒ 2012 Information Processing Society of Japan

大学名	組織部門名称	登録範囲	初回登録日 (有効期限)	認証機関
日本福祉大学	-	学生 (大学・大学院) の入学前の資料請求、入試管理、学籍管理、履修成績管理、卒業後の情報管理 (2010 年 10 月 20 日付適用宣言書 第 4 版).	2005/3/16 (2014/3/5)	BSIJ
國學院大學		渋谷キャンパスにおける学修・学生支援、入試・学生募集、広報活動、卒業生・保護者との協力支援、生涯学習、コンピュータシステム管理、資料・情報の収集管理、研究開発の運営・研究支援及び管理部門の業務 (2008 年 10 月 1 日付適用宣言書 第 2 版)	2006/1/30 (2012/1/12)	BSIJ
早稲田大学	メディアネットワークセンター	早稲田大学メディアネットワークセンター (MNC) におけるシステム開発、運用業務 (2006 年 10 月 3 日付適用宣言書 第 1 版)	2007/1/24 (2013/1/23)	BSIJ

表 2 参考: 日本福祉大学・國學院大學・早稲田大学の ISMS 登録情報

らも取得することができる[*1]．以下では，各大学の ISMS 適用範囲を順に説明する．参考までにその他の大学の基本情報で Web ページ[9] から取得可能なものについても，表 2 にまとめておく．

3.1 静岡大学情報基盤センター

図 1 に，静岡大学情報基盤機構組織構成を示す．2009 年の機構設立当初より，情報戦略や全学情報基盤を審議する情報戦略委員会、実施組織として情報基盤センター、事務組織として学術情報部情報企画課が機構配下に設置されている．機構長は、研究・情報担当理事である情報化統括責任者（CIO）が兼務し、現時点では情報基盤センター長も兼務している．機構と情報基盤センターのそれぞれ CIO 補佐と特任教授が配置され，センターの運営を補助している．浜松キャンパスと静岡キャンパスは，それぞれ約 6000 人規模であり，2003 年〜2011 年までの ISMS 適用範囲人員は、情報基盤センター教職員 12 名程度で構成されていた．2011 年の認証審査において，情報基盤機構の事務組織である情報企画課 (現在の構成員数 6 名) を取り込み，2012 年現在の ISMS 適用範囲人員は 20 名である．情報企画課のリスクアセスメントや文書作成などの ISMS 構築作業は，そのほとんどをエリア内に閉じて完了し，センターの ISMS 文書類との統合を行うことで完了できた．基幹系業務システム（人事給与、財務会計等の事務システムを運用する仮想サーバ）は，センターの基幹ネットワークシステムと同様に，2010 年 3 月に構築を完了した商用プライベートクラウドセンターに移設完了している．課長，係長を含む情報企画課スタッフの 3 名は，毎週行われるスタッフ会議（センタースタッフは全員参加）に参加しており，予算執行や事務手続き等における情報共有と連携処理が実現できている．2003 年の ISMS の認証当初から懸案であった事務組織（情報企画課）の取込を完了できた今，当センターでは新たに IT サービスマネジメントシステム（ITSMS）の構築に取り組んでいる状況にある．

*1 徳島大学の情報は執筆段階では未登録である．

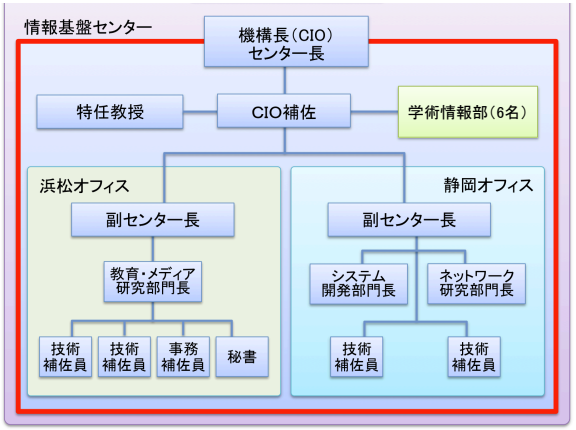

図 1 静岡大学情報基盤センターの ISMS における組織構成

3.2 宇都宮大学総合メディア基盤センター

適用範囲の組織委構成図を図 2 に示す．センター長を指揮系統のトップとする「事務室」が組織されている大学組織でよく見られる「○○部□□課××係がセンターも所掌する」とは根本的に異なる．当然，室長以下のセンター事務職員も ISMS の対象範囲内にあり，図には表れにくいが，センターに関わる全構成員（学生アルバイト，常勤・非常勤，専任・兼任を含む）が，ISMS の対象とあり，教育や監査の対象になっている．現在の ISMS の適用範囲の組織は 21 名からなる．

3.3 山口大学メディア基盤センター

山口大学メディア基盤センター等で運用されている ISMS の組織図を図 3 に示す．文献[10] でも簡単に紹介しているが，2011 年 10 月の更新審査から適用範囲の事業範囲を拡張し，従来から範囲内であってメディア基盤センターの業務に加え，情報環境部情報推進課が行っているサーバ室運用，学内業務システム用のハウジングサービス，及び情報環境部が管轄する

ⓒ 2012 Information Processing Society of Japan

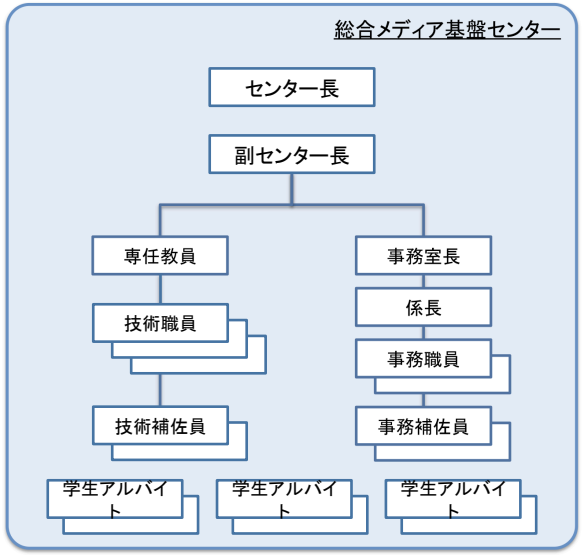

図 2　宇都宮大学総合メディア基盤センターの ISMS における組織構成

一部システムの運用までが含まれるようになっている．これに伴い，メディア基盤センターの組織に加え，CIO 補佐として情報環境部長，情報セキュリティ管理者として情報推進課課長，更に、情報セキュリティ担当者として同課課員 6 名が適用範囲に加わった．

従来より ISMS 関連文書の管理に関しては情報環境部情報推進課情報基盤係が担当しているが，情報基盤係は適用範囲内ではなく，メディア基盤センターから業務内容に関する覚書に従って業務委託された “第二者” という扱いとなり，PC 教室や解放端末スペースを管理を学生支援部・図書館・生協や，各建物に設置されたネットワーク機器室の維持管理を担当する学部等と同様の位置づけにある[*1]．

内部監査は本来適用範囲内のメンバーで内部監査チームを編成するのであるが，山口大学メディア基盤センター等の ISMS では，客観性を担保すること，学内他部局への ISMS の普及を容易にすること，及び学内に情報セキュリティ監査のノウハウを蓄積することを意図して，敢えて学内他部局の職員に依頼をしている．この体制は ISMS 構築当初から続いて

*1 情報基盤係とは文書管理に関する覚書が取り交わされている．

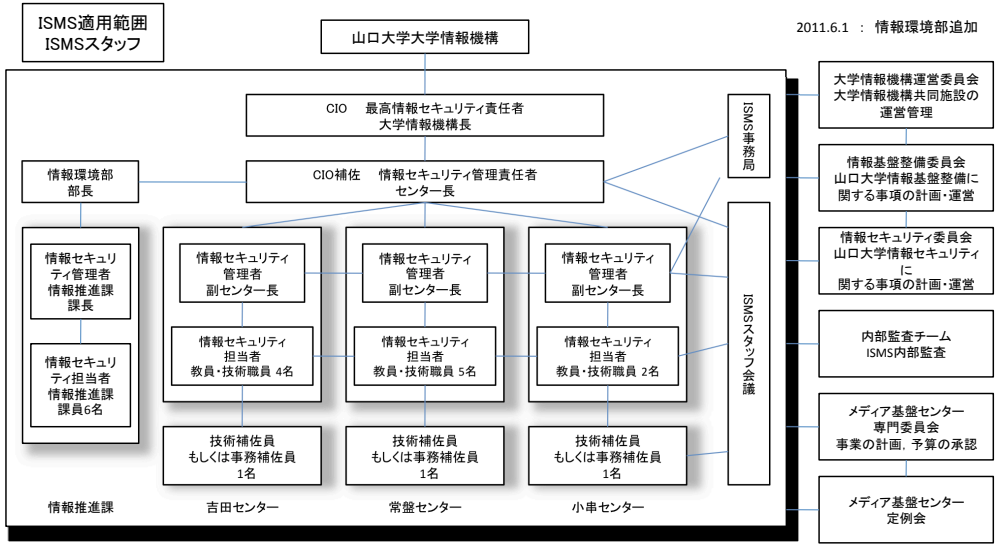

図 3　山口大学メディア基盤センター等の ISMS における組織構成

おり，2011 年は，附属病院，大学教育機構，教育学部の教育職員，及び全学の情報セキュリティ監査を担当する業務監査・指導室の事務職員からなる内部監査体制の下で監査が実施された．

3.4　徳島大学情報化推進センター

ISMS 適用範囲を図 4 に示す．センター規則で規定された職の全員には適用されておらず，今回の認証ではセンター長，副センター長，およびセンター棟・分室[*2]で実務にあたる職員 12 名の合計 15 名に適用している．すなわち，規則上室員となっていても，ISMS 物理的境界内で執務しない事務情報部所属の職員 (図中ではアスタリスクで示している) は除外することとした．

副センター長は事務情報部部長であり，全学の情報施策のスムーズな実施のための事務側の調整を主に行っている．

*2 今回の認証では蔵本地区分室は改装工事のため適用範囲外とし，工事終了後改めて追加審査を受ける予定である．

ⓒ 2012 Information Processing Society of Japan

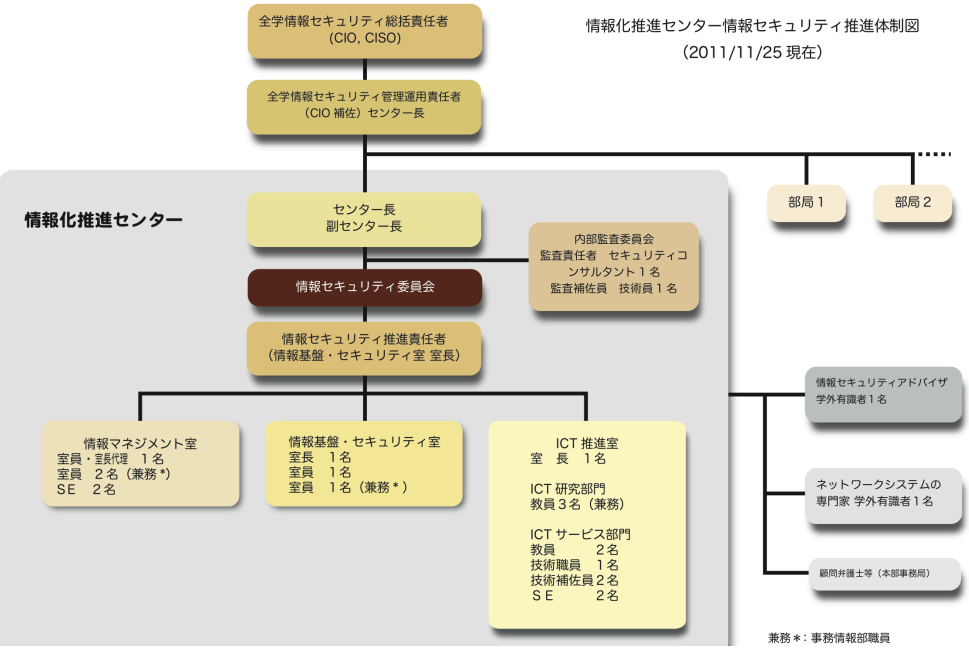

図 4　徳島大学情報化推進センターの ISMS における組織構成

ISMS の拡張展開となりうるもっとも自然な対象部局は情報部であるが，現在のところその可能性については議論されていない．

4. 事務組織の関わり方に関する議論

上記の四つの大学の事例は，大学の通信ネットワークや認証などを主たる適用範囲としていること，その運用に関わる教育情報処理センター系組織を中心として適用範囲が構成されていること，さらに，大学全体の CIO が (適用範囲に入るかどうか違いはあるが) 直接的に ISMS の統括を行っていることが共通点として挙げられる．一方，事務組織の関わり方に関してはいくつかの観点から— (1) ISMS の構築・運用に必要ば事務サポートが適用範囲に組み込まれているか，(2) 業務系システムの運用及び運用支援サービスが適用範囲に入っているか，さらに，(3) 教務系情報システムが適用範囲に入っていか— 違いが見て取れる．

ISMS を構築・運用する上で，手順の文書化と挙証データとしての各種記録の管理は必要不可欠であり，また，的確な進捗管理を行い遺漏無く計画が進むよう支援する体制も極めて重要である．従って，ある程度は各種ツール類の活用で軽減されるにしても，大学の事務組織のサポートは不可欠である．宇都宮大学の事例では，構築当初から適用範囲内に事務組織が含まれており，さらに現在では，事務室がセンター長直轄となっている．また，静岡大学では 2011 年より適用範囲に学術情報部の一部を取り込み連携を強化している．山口大学では窓口業務などは適用範囲内であるが，ISMS 関連文書の管理，予算・物品管理，ISMS 事務局会議の支援などは適用範囲外の情報基盤係に依頼をしている．徳島大学では，事務情報部の所掌となっており，担当事務補佐員はセンターからの委託の職員の形を取ってルールに従ってもらっており，窓口業務以外の ISMS 関連業務に事務は関与はない．

業務系システムのサポートが適用範囲内であるかどうかについても違いが見られる．静岡大学では業務系システムをクラウド環境に移行し，業務系システムの支援も適用範囲に入っている．山口大学や徳島大学ででは，業務系サーバ室の運用や運用支援が適用範囲に含まれているが全てが対象ではない．

表 2 に示す日本福祉大学や國學院大學，及び表には示していないが南山大学の事例ではいずれも教務系システムを含む適用範囲となっている．一方，情報処理系センターが基盤システムを適用範囲としてスタートしている ISMS では大学毎の違いが見て取れる．徳島大学では教務系システムもサーバ系統はセンターが全面的にサポートをしている．山口大学の ISMS では，教務系システムへののハウジングサービス提供は行っているが，システム運用には関与していない．

5. おわりに

情報処理センター系組織を中心として ISMS の構築及び ISO/IEC 27001 (JIS Q 27001) の認証取得をしている静岡大学，宇都宮大学，山口大学，徳島大学に関して，事務組織の関わりという観点からその適用範囲の比較を行った．いずれも，大学経営陣からの支援を受け情報基盤の運営を中心に適用範囲を構成している点は共通しているが，ISMS の構築・運用に必要不可欠な事務サポートの実現の仕方や，業務系システムの適用範囲への取り込み方などでは違いが見られる．

現在，いくつかの大学においても情報処理センター系の組織を中心とした ISMS 構築の動きがみられる．各組織毎に立ち上げの経緯や大学内での役割分担などに違いがあるので，

ⓒ 2012 Information Processing Society of Japan

本報告で紹介したいくつかの事例が少しでも構築・運用の参考になればと期待している．今後は，紹介した事例の類型化や，適用範囲の拡大に関する検討状況などを引き続き調査したいと考えている．

参 考 文 献

1) 国立大学法人評価委員会：国立大学法人の中期目標及び中期計画の素案についての意見（案），国立大学法人評価委員会総会（第 30 回）配付資料別紙資料 1-5，p. http://www.mext.go.jp/b_menu/shingi/kokuritu/gijiroku/attach/1286693.htm (2009).
2) JIS Q 27001: 2006 (ISO/IEC 27001:2005): 情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステム要求事項，日本規格協会 (2006).
3) アイソス編集部：事例 ISMS は学生サービス向上の大前提–情報資産価値を最大化するために導入 南山大学 (特集 BS7799-2 規格詳細と事例)，月刊アイソス， Vol.8, No.6, pp.58–67 (2003).
4) 電子情報通信学会編：情報セキュリティハンドブック第 5 編第 4 章，オーム社 (2004).
5) 八巻直一，藤本　徹，長谷川孝博，館野康彦，小林伸睦，野崎宏明，中山雄一，岡田吉弘，井上春樹：大学の IT コンプライアンス，静岡学術出版 (2007).
6) 永井　明：ISMS 確立及ひ認証取得までの経緯と今後，第 2 回国立大学法人情報系センター ISMS 研究会 (2008).
7) 市川哲彦，永井好和，長谷川孝博，三池秀敏：山口大学における情報セキュリティマネジメントシステム構築の実例，情報処理学会インターネットと運用技術研究会報告，Vol.2009-IOT-6, No.6 (2009).
8) 上田哲史，佐野雅彦：徳島大学情報化推進センターにおける ISMS 構築について，情報処理学会インターネットと運用技術研究会報告，Vol.2011-IOT-14, No.5 (2011).
9) 一般財団法人日本情報経済社会推進協会 (JIPDEC) 情報マネジメントシステム推進センター：ISMS 認証組織情報検索，p.http://www.isms.jipdec.or.jp/lst/ind/index.html.
10) 市川哲彦，小柏香穂理，永井好和，小河原加久治：山口大学における情報セキュリティマネジメントシステム (ISMS) 構築テンプレート作成及び適用範囲拡張について，情報処理学会インターネットと運用技術研究会報告，Vol.2011-IOT-14, No.6 (2011).

ⓒ 2012 Information Processing Society of Japan