Vol.2012-IOT-16 No.41
2012/3/16

組織評価とISMS

上田哲史[†1]　佐野雅彦[†1]

徳島大学情報化推進センターでは，ISMS 導入にむけ，2011 年度当初から準備を始め，最終的に 2012 年 1 月に認証機関より適合判定を受けた．ISMS 取得は，並行して行われた新コンピュータシステム調達（2012 年 3 月稼働予定）との 2 大事業であり，クラウド導入に関するデータセンターの利用，SLA 締結におけるセキュリティ要件の管理において重要な役割を果たす．時期を同じくして本センターは組織評価（外部評価）を受審したが，評価資料における組織，人的セキュリティ，経営陣の責任等の体制構築，情報セキュリティ対策および関連プロジェクトなど各種取り組みの情報は ISMS 受審には大いに役立った．情報セキュリティ関係業務は本センターの主業務であるため，ISMS をターゲットに取りまとめた資料は，組織評価資料の作成に多いに貢献した．本稿では情報系センターの組織評価における ISMS の価値や必要性と，大学における情報マネジメントの関係について述べる．

Organizational Evaluation and ISMS Activities

Tetsushi Ueta[†1] and Masahiko Sano[†1]

Center for Administration of Information Technology, The University of Tokushima has received a recommendation from the audit organization for receiving an ISO/IEC 27000 standard. We started the preparations for obtaining ISO from April 2011, and finally the final check by the auditor has done in January 2012. Obtaining ISMS certification is not only an implementation of work flows regarding the security management system but also providing smooth operations and safe communications in the information systems in the campus. In parallel with acts of ISMS, we have received an organizational evaluation by out-campus knowledgeable people on November 2011. In this audit, our improvement activities related with ISMS has been highly regarded in the report by the Evaluation Committee members. The documents on the evaluation play very effective role in the audit of ISMS since it is a powerful fact book on the organization structure, personnel security, owner's responsibilities,and information security activities of the organization. In this report, we discuss a relationship between ISMS activities and the organizational evaluation and conclude that both evaluations complementarily affect each other.

1. はじめに

大学の各部局における組織評価は，自律的評価（自己点検）と他律的評価（外部評価）に大別され，ともに組織活動の改善につなげる監査プロセスといえる．後者は特に，その部局が設立目的に合わせた活動を実施しているかについて，利害関係のない第三者による客観的な評価を評価となるため，組織活動の PDCA の監査フェーズとして効果の高いイベントとなり得る．

徳島大学情報化推進センター（以下，センター）では，2010 年 7 月の改組の際，運営の柱に情報マネジメント体制，および情報セキュリティ体制の確立を謳っている．前者の当面の大きな課題は 2012 年 3 月稼働予定のコンピュータシステム調達であり，後者はセンターにおける ISMS (Inoformation Security Management System) の認証取得である．クラウドを導入するため，SINET データセンター以外のデータセンターの契約，SLA(Service Level Agreement) 締結において情報セキュリティポリシーや，技術的セキュリティ水準・要件の再整備を要するため，ISMS は必然でもあった．

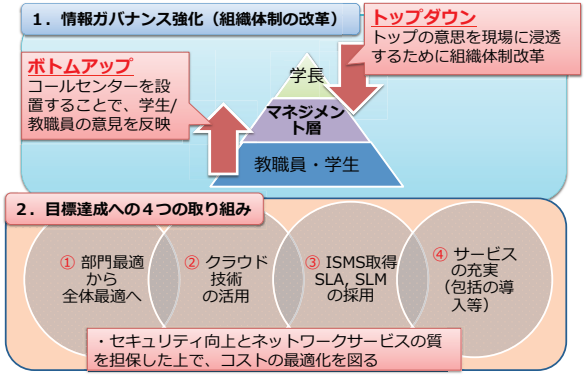

図 1　徳島大学情報ガバナンス体制と情報施策

†1 徳島大学情報化推進センター
Center for Administration of Information Technology, The University of Tokushima

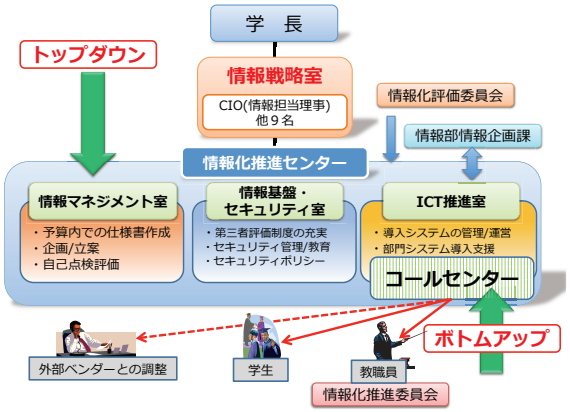

図 2　情報化推進センターの組織と情報ガバナンス

徳島大学においてセンターの改組は，大学における情報ガバナンス体制の一つの具現であった．学長直下の情報戦略室がまずは大学情報施策の方針を決定し，情報化推進センターは施策の実装部隊となっている．図 1 は情報ガバナンス概要と，ユーザへのサービスを充実させるための急ぐべき施策を挙げている．また，図 2 はセンター内組織の所掌と，コールセンターおよび情報化推進委員会によるボトムアップ体制を記述している．これらの詳細については本稿では割愛する．

改組後の運用がわずかに一年あまりであったが，学長より早々の組織評価の実施が指示された．センター内部の情報マネジメント体制のチェックのみならず，新たに敷いた全学の情報ガバナンス体制の有効性もこの機会に評価される．

ところで，情報施策の円滑な推進，各種情報システムの安全な運用，安心の情報ネットワーク基盤の運用には，情報セキュリティに関するセンター内部の PDCA が必須である．ISMS も内部監査および認証機関による審査などの監査が周期的に入り，システムの健全性がチェックされ，改善サイクルがスパイラルアップされる構造である．本センターのような部局において改善対象の事業項目は，情報マネジメント業務，情報セキュリティ業務を完全に包含するため，組織評価と ISMS 両者の監査プロセスの類似性は極めて高い．

本稿では，ISMS 認証取得の経過を述べるとともに，組織評価における情報マネジメントおよび情報セキュリティ活動に関する評価，学内外から ISMS 取得がセンターのどのような位置づけに映るかなど，組織評価と ISMS との関係を報告する．

2. 背　　景

2.1 改組と情報セキュリティ体制

2010 年度内に ISMS 取得に関する予算等の承認を得た．準備としては

- ISMS 講習会の企画・参加
- セキュリティレベルの大雑把な分類とそれに見合う物理境界の設定
- 不要物品廃棄
- 部屋のレイアウト変更

などを徐々に行った．ISMS 文書に関する具体的な作業を始めたのは 2011 年 5 月になってからのことである．

改組前 (2010 年 7 月以前) の体制では，業務は属人化しており，責任区分が曖昧でマニュアルや記録が無いなど，その場凌ぎの管理運営がなされていた．これは決して手抜きであった訳ではなく，個人個人は相応のスキルを持って業務に当たっていたが，全学に均一なサービスを提供するという視点に立った業務改善の検討が十分に行われていなかった[⋆1]．しかし，結果として管理はずさんとなり，例えば，基幹ネットワークに接続される L3, L2 スイッチの設定管理情報や保守管理情報等は整備されておらず，担当者以外は VLAN が学内でどのように巡っているかは不明な状況であった．このような状況下でも全学的にはセキュリティ的破綻を生じなかったのは，大学情報セキュリティポリシー[1)] が施行されており，セキュリティ教育や情報セキュリティ監査が定期で実施され，人的セキュリティが保たれていたためと思われる．

改組後，セキュリティ専門サービス企業に依頼し，全学のネットワークの管理現況の調査，ならびに管理運営に対して監査を実施した．ネットワークの設定，管理の全体像は明らかとなったが，ISMS 的な規定や手順は全く整備されていない状況であるため，当然ながら監査結果として「大幅な管理体制の改善」が要求された．これを受け，情報戦略室方針としてネットワーク管理体制改善プロジェクトを 2011 年 5 月より動かし，改善にあたることとした．また，改善の視覚化という意味で，並行して ISMS 取得にもあたるよう，トップダウ

⋆1 実際，改組前のセンターは研究部局の位置づけであり，教員は研究教育に重きを置いていた．

ンの指示があった[⋆1]．

プロジェクトにおける業務改善は，情報セキュリティに関する PDCA サイクルそのものであり，ISMS 実装に向けた実装のシナリオとして最適であった．まずはプロジェクトとしては，センターの行うネットワーク管理業務の範囲を再定義した．具体的には旧体制では基幹ネットワークの管理のみをセンターで行う定義であったが，これを全学に拡張した．一方，無限責任は取れないため，各部屋のコンセントまで，また，NAT やファイアウォールを挟みプライベートネットワーク相当のものをローカルに運営している場合は範囲外とした．

センター範囲内のサーバの設置は申告制とし，同時に毎年監査アプライアンスによるプラットフォーム脆弱性診断を行うこととした．また，全学のクライアントのセキュリティ担保のため，包括契約によりウィルス対策ソフトウェアを配布することとした．

2.2 コンピュータシステム調達における ISMS の関与

センターの 2012 年 3 月稼働予定のコンピュータシステム調達において，キーワードはクラウドである．学生のメイルはパブリッククラウド，教職員のメイルはプライベートクラウド，その他重要な情報システムはオンプレミスでサーバを準備するなど，ハイブリッドクラウド[2] と呼ぶべき構成である．

ここ数年メイルサービスに関しては停電以外の原因による事故でのサービス中断が頻発していたため，可用性向上に極めて効果的であると期待される．また，センター教職員が 24 時間 365 日，特定のサービスの保守維持にあたることは不可能であり，それをクラウドで代替担保することは合理的である．このときプロバイダとのインタフェースにおけるセキュリティの要件が，ISMS の様々な要求事項のクリアに相当する．

コンピュータシステム調達に関しては，SLA の策定において，大学の情報セキュリティポリシー，ISMS の規格要求事項（特に A.10 通信及び運用管理，A.11 アクセス制御，A.12 情報システムの取得，開発及び保守）のチェックが十分に行われ，また，仕様等にも反映された．

3. ISMS 実装

3.1 初 期 準 備

情報セキュリティを所掌するセンター内の部門は，情報基盤・セキュリティ室（教員 2 名）であり，ISMS についてもこの部門が中心となりとりまとめた．また，ICT 推進室室員の協力を得た．計画にあたっては文献[3),4)] を参照したが，具体性に乏しいため，規定書や管理台帳のひな形は市販のもの[5)] を利用し，参考にすることとした[⋆2]．また，各手順書のひな形は独自に開発した．

上述したとおり，本学には平成 18 年から情報セキュリティポリシー[1)] を施行しており，この策定段階においても ISMS を念頭に置いていた．情報セキュリティコンサルタントも付けた十分な策定体制を置き，ISMS の各管理策がポリシーのどの項目でカバーされるかのひも付けも検討していたため，ポリシーは ISMS 的尺度からも内容的に十分なものとなっている．この時の経験を活かし，まずはポリシー本文（基本方針，技術基準）および 11 種類の手順書の項目の精査から始めた．

静岡大学の長谷川孝博氏に外部情報セキュリティアドバイザとして参画してもらい，リスク分析からリスク対応計画にかかる作業のノウハウを学ぶことができたこの過程で情報資産の全容が改めて明らかとなり，そのグルーピングとリスク評価を落ち着いて行うことができた．リスク対応計画に入れるべき緊急の対象も出てきたため，審査前に早々に手を打ち始めた:

- 故障リスクを抱える CVCF（大型電源装置）はスポット保守を複数回行ったうえ，以上動作時の警報鳴動器を事務室に備え付けた．
- CPU 負荷が上がるとダウンするメイルサーバは，別途サーバ等を設置し，負荷分散を行った
- 包括契約によりウイルス対策ソフトウェアが導入された．

3.2 書 類 審 査

文書レビューは 2011 年 9 月末から実施された．査読結果は 10 月中旬に通知され，内容は**「不適合が懸念される事項 74 件」**という途方もないものであった．主に文書全体に具体的手順化（要求事項の実装）が圧倒的に不足していた．にも関わらず，初動審査への前進は認められていた．

リスクアセスメントに関するノウハウを十分受けていたことより，基本方針，人的セキュリティ，組織の要求事項についてはほとんど指摘は無かったが，それ以外の項目についてはほぼ須く指摘があった．

著者らは，リスクアセスメントまでの計画プロセスは何度かの講習[7)] 等で理解はしていたものの，管理策の適用と，適用宣言書を編纂するあたりから ISMS の要求事項の本質的

⋆1 本学学長は元大学病院長であり，ISO 認証は経営体制の改善に有効との理解があったためと思われる．

⋆2 山口大のひな形[6)] はリリース前であった

な意図を解釈することが難しくなり始め，それがISMSマニュアルや各規定書の詰の甘さに如実に現れることとなった．

しかし，むしろこの74件の懸念事項は，具体的にわれわれが要求事項の充足に対してどう動くべきかの詳細かつ具体的な指針となり，初動審査に向けてスケジュールを立て，分担しながら，また，適宜話し合いながら書類の改訂，追加を行なうことができた．

監査責任者を，上記プロジェクトのコンサルタントにお願いした．情報セキュリティ監査受審経験があり，客観性も確保でき適任であった．

4. 組織評価

経過としては，ISMS初動審査より先に組織評価プロセスに入った．

センター関連規則として，情報化評価委員会規則（センター長制定）を定めている．この委員会はセンターの外部評価を所掌し，目的は「センターの多面的な活動状況を外部から客観的に評価するとともに，評価の結果及び評価に関する資料を公開し，もってセンターの発展及び活性化に資することで，徳島大学全体の情報化の推進に寄与する」とされている．

第1回のセンター情報化評価委員会を2011年11月に開催することを決めた．評価委員は学外から情報分野に精通した専門家4名，学内からは学部長5名の計9名にお願いした．

4.1 評価の実施方法

評価対象は，2010年7月から2011年10月までのセンターの活動状況とした．評価の方法は，(1) 詳細な活動内容を記した情報化評価委員会資料（以下，評価資料）の査読結果，(2) ヒアリングと視察による評価を総合的に鑑みることとした（このスタイルは認証取得における文書審査，初動・本審査のスキームに良く似ている）．

4.2 評価の実施経過

2011年9月7日 徳島大学情報化推進センター情報化評価委員会および徳島大学情報化推進センター自己点検・評価委員会の設置．

9月30日，10月7日，10月13日 自己点検・評価委員会の開催．

10月1日 情報化評価委員会委員の委嘱．

10月19日 情報化評価委員会資料の各委員への事前送付．

11月8日 平成23年度第1回情報化評価委員会の開催．
議題：徳島大学情報化推進センターの評価について

11月18日 情報化評価委員会委員からの評価結果報告書の提出，とりまとめ．

12月2日 情報化評価委員会委員長からの総括的評価結果報告書の提出．

12月7日 平成23年度第2回情報化評価委員会の開催（メール審議）
議題：徳島大学情報化推進センター情報化評価委員会報告書（2011）について

情報化評価委員会は最短でも2年周期で実施することが申し合わされているため，定期的な業務の内部評価，見直しは自己点検・評価委員会（自組織内委員会）により実施される必要がある．本年度はこの組織評価により自己点検・評価委員会の評価活動も兼ねることとした．

評価資料の作成には，他の業務と並行して鋭意執筆され，一ヶ月を要した．その際図表や説明文は，情報戦略室会議資料，情報化推進委員会資料を利用することができた．教員の業績等は業績管理データベースから無手順で得られる．規則や統計をまとめて評価資料はA4 PDFで89ページとなった[*1]．また，ヒアリング実施日には評価資料の抜粋を記したプレゼンテーション資料(28ページ）を用意した．

5. 組織評価におけるISMS

評価委員会では，概要に関する説明のあと，約1時間をかけて質疑が交わされた．途中一旦現地視察に入り，最後に質疑を再開した．その際の質疑内容は記録され，評価結果報告書に採録されている．

組織評価結果は，多くの委員から改組による情報ガバナンス体制が概ね確立されていると評価されていた．そのトップダウンの意思決定から施策決定までの即応性，またコールセンターを通じたボトムアップな意見の集約体制構築（図1参照）が高評価であったものの，情報施策の相談や周知など，コミュニケーションや広報についての問題点もまた多く指摘された．時期的にBCPに関する提言や要望も多く含まれている．

実際はサービス機関としてのセンターの在り方に対し，多くの評価，意見や批判があったが，これらからISMSや情報セキュリティに関するものを以下に列挙する．(適切に編集してあるが，本文で触れていない機能等にも触れられている点はご容赦願いたい.)

- ISMS認証取得については評価できるが，これによって例えば，大学における情報セキュリティが向上したのかについて検討が必要である．
- 新入生に対する情報科学に関する授業を支援していることは評価できるが，最近，情報セキュリティに関する問題のインパクトが大きいため，全学生，教職員に対する情報セキュリティに関する教育について支援の可能性を検討する必要がある．
- 情報基盤・セキュリティ室においては，短期間で，大学全体のネットワークの掌握，セ

*1 http://www.ait.tokushima-u.ac.jp/selfcheck/evalait2011.pdf

キュリティ監査，脆弱箇所の改善を行った上で，ISMS 取得を実現しつつある

- ウェブサーバ統合プロジェクトにより，大学のトップサイトだけでなく各部局のサイトも統合を進めており，セキュリティ向上，人的なものも含めたコスト削減，デザイン統一，情報の信頼性や単一性の向上といった広報的にも重要な効果を挙げている
- 新コンピュータシステムにおいて学外からも含めて仮想デスクトップサービスを実現し，利便性とセキュリティの向上を同時に実現している
- いくつかの情報系センターで，電気設備の点検に伴う停電時においても，システムを停止させない取り組みが試みられている．ネットワークやシステムが一日 24 時間週 7 日間常に動いていることは，センターのサービス向上に大いに寄与すると考えられる．
- メールサーバのパブリッククラウド移行，ISMS 認証取得，ソフトウェア包括契約の導入等の取り組みは先進的と評価できるものの，次期システムへの移行が完了する来春以後，その導入状況を見て改めて評価する必要がある．
- 情報セキュリティについては，既にポリシーレベル，実施手順レベルでの対策が講じられていると思われるので，今後は運用段階において，インシデントの発生状況やそれを減ずるための対策が有効に働いているのかについて，定量的指標をもとに適宜評価する仕組みの導入を望む
- 新入生を対象とした「情報科学入門」の授業運営を支援し，学生の指導に寄与されていることに対しては，高く評価するとともに，心より感謝する．
- 情報戦略室の中期的ビジョンやセンターの活動方針・状況について，学内全体への徹底した広報（FD）が必要ではないだろうか? 情報セキュリティについての学生・教職員への教育も強化する必要があると思われる．
- 大学全体の情報管理のコスト削減，セキュリティー強化に対する姿勢などソフト面の充実は理解できたが，非常時のデータのバックアップ体制を含めたハード面の充実，情報における大学構成員の倫理違反に対する対応などについては十分かどうか判断できなかった．
- センターの管理範囲について，部局ネットワークと端末ネットワークを分けて構築されている．端末のネットワークは部局で管理しコールセンターが支援するということになっているが，最近セキュリティに関する問題が多いため，各部局への一層の支援をお願いしたい．
- 新しい組織体制として，情報マネジメント室，情報基盤セキュリティ室および ICT 推進室での各役割業務を達成するため，活動目標を立てて，次期コンピュータシステムの導入，ISMS 認証取得，定常的業務の安定化など，スタッフが精力的に極めて多くの業務に取り組んでいることは高く評価できる
- ウェブサーバなどの統合化，ソフトウエアの包括契約，セキュリティ対策の充実，クラウドの導入など，これから情報化社会の推進に向けた積極的な取り組みや，情報セキュリティの改善に向けた取り組みは大変重要と思われる事項であり積極的な取組は評価できる．
- 情報セキュリティ対策についても学生教職員への周知を徹底させるためにも各部局との密なる連携が求められる．
- 情報化社会の推進に向けた新しい取り組みの必要性やメリット，デメリットや情報セキュリティ問題などを専門家でない一般教職員に分かりやすく説明するなどの場を設けることも重要と思われる．
- 情報を扱うセンターは，今後の震災に対する備えとして，教育データの保存場所を含むバックアップ体制の点検を含む機器管理体制の充実も望まれる．

6. 再び ISMS

6.1 準　　備

書類審査結果の検討と併せて，133 の管理策のうち，電子商取引等に関わる 2 管理策を除く 131 管理策は適用する旨の適用宣言書を策定した．

内部監査は初動審査の直前に行われたが，初めての内部監査であるため，要求事項に関する全ての項目について，監査責任者からのヒアリング形式で担当者に実施した．時期的にまだ手順書が十分整備されていない状況下であったため，これらの未整備が指摘事項として取り扱われた．

6.2 初 動 審 査

11 月下旬に初動審査が現地ヒアリングの形で実施された．初動審査による確認のほとんどは，ISMS 文書査読における 74 個の懸念事項の是正確認である．これらのほとんどは，要求事項の意図と大きく外れることなく解釈，実装できていた．しかしながら，中には審査員に解釈の解説を部分的に聞いて汗顔となる項目もあった．

組織評価において現地視察がプログラムされていたため，よってこの初動現地視察用に改めて準備することは少なく済んだ．

初動審査の結果，4 件の不適合懸念事項が示された．

- 内部監査の不備

- 情報資産目録の不備
- 持ち出しクライアントに関する対策不備
- 環境的セキュリティの懸念

最後の項目は，医歯薬学部系キャンパスのセンター分室のことであり，初動審査時は改装工事のため，物理的境界（管理区域）としてのセキュリティ要件を満たすことができない状況であった．審査後，センター内情報セキュリティ委員会にて今回の適用範囲からは除外することが申し合わされた．内部監査の不備とは，内部監査の際，法規制に関するチェックが行われていなかったことである．そのため，後に追加的内部監査を実施した．また，規定の改訂や目録，台帳の整備，マニュアルの編纂を引き続き実施した．

有効性の測定や BCP 対策等も実施し，情報セキュリティ委員会により未処理であった残留リスクの承認も行った上で，内部監査の結果と併せていよいよマネジメントレビューに臨んだ．マネジメントレビューインプット情報から，手順書の不備は是正措置として処理するようセンター長から指示が出た．また，書類の電子化についても検討するよう意見があった．

ところで，アンチウィルスに関しては，特定の OS にしか対策できないソリューションであったため，他の OS のサーバ等の脆弱性による脅威が懸念されていた．センター長は予防措置手順を踏んで，より多くの OS をサポートする包括契約によるウィルス対策の策定を打ち出した．これは早く検討が進み，2012 年 12 月には全学で包括的に複数 OS のウィルス対策が実現する見込みとなった．

6.3 ISMS 本審査

2012 年 1 月 16 日および 17 日に本審査を受審した．初動審査における不適合懸念事項の対処を確認し，教育の実施，補足監査の実施，実際に発生したインシデントの対応[⋆1]，記録すべき外部との事象，情報セキュリティ委員会の議事概要，マネジメントレビューの結果等を説明した．

センター長，情報マネジメント室，情報基盤・セキュリティ室，ICT 推進室の各室長，監査責任者それぞれにヒアリングが実施された．目録，台帳などのエビデンスの確認，現地確認などが行われた．結果として「適合」判定をうけることができた．改善の余地として有効性測定を一年に一回と限定している点および内部監査における指摘事項の内容レベル分けの点の２点，指摘があった．前者は都度の測定，後者は適切な是正内容の適切なグルーピングと管理により克服できると考えている．

⋆1 ISMS 範囲内で発生した事故ではない．

初動審査および本審査がスムーズに進行したのは，組織評価において評価資料の編纂段階で組織，人的セキュリティ，経営者の責任などの項目について自然と整理が付いていたことが良い影響を与えた．本審査所見総括においては，外部評価結果に関する直接的コメントは残されていないが，審査中においては評価資料は組織概要を知るにおいて審査員の有効な参考書となっていた．

7. おわりに

以上，ISMS 取得への取り組みを概観した．当たり前ではあるが本センターの業務そのものが ISMS と密接に関係しており，ISMS の実装を通じて業務フローの作成やマニュアルの整備，連絡網の整備ができ，業務の抜本的な改革が実現されていると実感している．

ISMS 取得活動と同時に受審した外部評価について述べた．時系列的順序としては組織評価を行った後に ISMS 初動審査・本審査となったことは，組織評価の項目の一部に ISMS に関わる活動が含まれる構造上，評価のための資料作成，提示としては無駄が無かったように思われる．

参考文献

1) 徳島大学情報セキュリティポリシー, 改訂版, July (2011).
2) NEC プレスリリース, “徳島大学向け ICT 環境を NEC がハイブリッドクラウドで構築〜低コストで高い運用性・耐障害性を実現〜,” 2011 年 11 月 21 日. http://www.nec.co.jp/press/ja/1111/2101.html
3) ISMS ユーザーズガイド—JIS Q 27001:2006(ISO/IEC 27001:2005) 対応—, 財団法人 日本情報処理開発協会編 (2008).
4) ISMS ユーザーズガイド—JIS Q 27001:2006(ISO/IEC 27001:2005) 対応, リスクマネジメント編—, 財団法人 日本情報処理開発協会編 (2008).
5) ISMS サンプル文書集, TS-ISM, CD-ROM (2009).
6) ISMS 構築用テンプレート，ITSC, DVD, ISBN978-4-903859-67-5 C3084, (2011).
7) 第 4 回情報セキュリティマネジメントシステム (ISMS) 研修会資料, 山口大学, May 18–19, (2011).
8) “徳島大学情報化推進センターにおける ISMS 構築について,” 情報処理学会研究報告, Vol. 2011-IOT-14, No. 5, July 15 (2011).
9) 徳島大学情報化推進センター評価報告書, 徳島大学情報化推進センター情報化評価委員会編，Dec. (2011).