社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＤＳＭ－33　(11)
2004／5／14

大学におけるISMS準拠のセキュリティポリシ策定に関する一考察

松浦 健二† 上田 哲史† 佐野 雅彦† 大恵 俊一郎†

†徳島大学高度情報化基盤センター 〒770-8506 徳島市南常三島２－１

E-mail: †{matsuura, tetsuhi, sano, oe}@ait.tokushima-u.ac.jp

あらまし 現在セキュリティ対策は，個人情報保護のみならず，知的財産の管理保護や情報資産の活用といった側面からも重要であり，大学組織においても取り組まれているところである．特に，ポリシ文書はセキュリティ規範となるものであり，その運用においてはISMS認証制度などに準拠した運用体制の確保とサイクリックな監査が行われる事が望ましい．徳島大学では，ISMS準拠のセキュリティ対策とポリシの策定を目的として，全学展開による活動を行っている．また，そのための運用システムを開発した．そこで本稿では，大学におけるISMS規格準拠のセキュリティ運用手法を考察する．

キーワード セキュリティポリシ，ISMS，情報資産，リスクアセスメント

A Study on Polishing up the Security Policy Documents in accordance with Information Security Management System

Kenji MATSUURA† Tetsushi UETA† Masahiko SANO† and Shun'ichiro OE†

† Center for Advanced Information Technology, Tokushima University

2-1 Minamijosanjima, Tokushima, 770-8506 Japan

E-mail: †{matsuura, tetsushi, sano, oe}@ait.tokushima-u.ac.jp

Abstract Since lots of security incidents have occurred nowadays because of a lax policy or lacking it, the security policy for a social organization is very important and has attracted a great deal of public attention. As for every university, it will play important roles especially in not only protecting the campus networks but also making best use of intellectual properties. Hence, Tokushima University is now tackling to enact this document in accordance with ISMS (Information Security Management System) regulation. Before releasing this document, the security-information management system has been developed in order to manage information assets of the university. Analysis of this database provides critical points of the current security. Although this ongoing project has not completed, this paper describes our findings both of how to manage the organization and how to develop the system.

Keyword Security Policy, ISMS, Information Assets, Risk Assessment

1. まえがき

個人情報の漏洩事故・事件は2004年に入ってからも続出し，深刻な社会問題となっているが，多くは当該組織の杜撰な情報管理や情報セキュリティ対策の甘さに起因しており，組織における情報セキュリティポリシの構築が重要だと認識されつつある．一方，全国の国立大学は，2004年4月から各大学のオリジナリティを確保しながら，独立法人として一斉にスタートを切った．法人化後はこれら大学機関において教員の個性ある研究結果などの知的財産に加え，所属教職員と学生の個人情報，学生の成績などについて，情報セキュリティの確保が重要な課題としてクローズアップされている．

これまで大学においては，本来セキュリティとトレードオフの関係にあるはずの利便性について，その確保のみに注目し，研究と教育に対して利便性が最大限発揮される運用方法が優先されていた．悪く表現すると，教育と研究の名目においては多少の脅威やリスクは眼をつぶる，もしくは不問とする傾向にあった．特にネットワーク研究などを含む工学系学部を抱える場合，研究基盤のインフラとして研究者が自由にネットワークを活用したいとの要望を受けて，敢えて不十分

なセキュリティ対策の放置を容認している場合もあると考えられる．こうした現状に対し，経済産業省や，情報処理推進機構（IPA），情報セキュリティ対策推進会議などの活発な啓蒙活動に加え，電子情報通信学会・情報処理学会・電気学会は，「高等教育機関におけるネットワーク運用ガイドライン」を平成15年1月29日初版公開し，大学等研究教育機関におけるセキュリティ確保についての方針を打ち出した[1].

一方，文部科学省では，平成13年6月15日の情報セキュリティポリシ策定に対する通達を行い，引き続き，国立情報学研究所が事務局となって，大学の情報セキュリティポリシーに関する研究会を設立，平成14年3月29日「大学における情報セキュリティポリシの考え方」を公開した[2]. さらに翌15年8月29日には，全国国立大学を対象として，「情報セキュリティセミナー」を実施し，単なる文書・規定を策定するだけでなく，実行性を伴うよう組織作りや監査制度を設けるよう提言している．

このように大学ネットワークにおける継続的なセキュリティ対策への要求が高まる中，徳島大学においても，セキュリティポリシの構築を行った．コンサルティング会社の支援を受け，上記ガイドラインや方針に則った上で，客観性，具体性を損なわない，全学レベルのポリシ策定を志向した．本稿ではその概要と開発した運用システムについて述べる*．徳島大学では，セキュリティポリシの策定と技術的な対策に加え，人的・物理的セキュリティを重視した総合的な対策が必要であるとの観点から，ISMS（Information Security Management System）に準拠した施策を講じている**．本学は，医学系・工学系・総合科学系などの複数学部が複数のキャンパスに散在している特徴をもつ．したがって本稿は，このような状況下でキャンパスネットワークを統合的に運用している場合の，ISMS準拠のセキュリティ対策としてのケーススタディを述べる事に主眼を置き，技術的な内容よりも寧ろ，その運用方法を中心に考察する．

2. キャンパスLANにおけるセキュリティ対策

2.1. ネットワーク運用特性

徳島大学は，地理的に分散化された二つのキャンパスと大学本部の合計3地区に散在し，それらは1GBで相互接続されている．また，医学部・歯学部・薬学部・工学部・総合科学部の5学部と各大学院，学内共同利用施設・研究センター，付属図書館等の，粒度・特性の異なる組織で構成される特徴をもつ．

これまで，本学におけるキャンパスネットワーク（通称TUNES）は，高度情報化基盤センターの管理する基幹ネットワークと相互接続する支線ネットワークによって構成される．支線は，各部局のボランティアである支線管理者によって，自主的かつ自由に運用・発展してきた経緯を持つ．つまり，各支線でWWWサーバやメール・メーリングリストなどの公式サーバ運用を行い，支線下のプライベートネットワークや無線LANの構築などはある程度自由度を保ちながら，かつ安定的にネットワーク運用を行う必要があった．

2.2. 保護・管理する情報の定義

組織の性格上，コンピュータとネットワークの使用は不可欠であり，扱う情報も膨大であるため，管理・保護すべき情報の定義は重要である．本学においては，セキュリティポリシによって保護すべき対象は，個人情報のみと定義した．具体的には個人の氏名，住所などのプライバシ情報を始め，成績などの学務情報，ID，パスワード，電子メイル資源，すなわちそれらの漏洩改竄が当事者や組織の財産や生命に重大な影響を与えるものである．

知的財産については研究・教育者個人の管理とし，管理対象外とした．これは本学におけるセキュリティポリシの適用範囲の判断として大きな特徴である．ポリシ策定時点では大学側において知的財産に関する明確な定義が形成されておらず，研究結果の組織への帰属性やインセンティブの定義が不明のうちは個人で管理すべきと判断した．しかし，本学に限らず，インターネット黎明期にUNIXサーバを中心とした自由度の高いネットワークを構築してきた多くの組織では，知的財産を情報セキュリティの保護範囲に含めるために失う自由が極端に大きくなると予想され，したがって当面は範囲外に設定すると考えられる．

情報資産は，これら個人情報を記録・保持している情報システムと位置づけ，さらに情報システムはこれを構成するシステム機器とシステム情報とした．

2.3. ISMS準拠のセキュリティ対策実施

2.1節のような経緯をもって発展運用されてきたキャンパスネットワークに対し，ISMS認証基準に準拠した手法を導入する．また，本基準は，以下の三つの特性を保持する事で，情報セキュリティにおける情報の安全保護の側面のみならず，情報活用の側面から今後の大学運営にとって重要な意味を持つ．

・**完全性（Integrity）**：情報及び処理方法が正確である事，および完全である事を保障する．

・**機密性（Confidentiality）**：アクセスを許可された者

---

* 本施策は，STNet社によるコンサルティングによって実施している．

** ISMS(Ver.2)は，英国BS7799-2:2002に準拠する形で，JIPDEC(日本情報処理開発協会)により平成15年4月21日に公開．
http://www.isms.jipdec.jp/doc/JIP-ISMS100-20.pdf

だけが当該情報にアクセスできる事を確実にする．

・**可用性（Availability）**：認可された利用者が必要時に，情報および関連資産にアクセスできる事を確実にする．

本規格の大学における先行事例として，平成 15 年度に南山大学（全学規模），静岡大学（総合情報処理センター），京都大学(大学院医学研究科医療経済学分野）が取得済みである．しかし，平成 16 年 4 月時点で取得を公表している全事業者のうち，大学機関は上記の 3 機関のみである．

2.4. セキュリティ対策実施上の課題

2.1 節で特徴付けられる本学のような大学において，キャンパスネットワークをこの認証基準に準拠させるべくトップダウン的な施策を講じる際には，以下の課題を考慮する必要がある．

(1) 自由度と統一性のトレードオフ

これまで発展的に運用されてきた支線の自由度をある程度確保しつつ，全体のセキュリティ水準を一定に保つ必要がある．このためまず，基幹ネットワークから末端ノードまでを含めて，情報資産の洗い出しを行う事が望ましい．その上で，規定上は統一性を確保しつつ，支線毎に自由度を持たせた施策をとる．

(2) 情報保護と情報活用の両立

知的財産や個人情報の安全な管理と同時に，その積極的な活用を図るための，情報システムの冗長性分析やリスク分析，およびリスク対応計画などを実施する必要がある．

(3)部局組織と支線構成の差異

徳島大学は，5 学部と学内共同利用施設等から構成されるが，各組織間の構成員数の粒度や構成員の特性等において，部局間で格差が激しい．例えば，工学部と歯学部では，学生も含めた構成員において，数千人オーダーの差が生じる．しかし，支線の構成は，ある程度の粒度で運営せざるを得ないため，部局構成と支線構成が一致しない．つまり，ISMS の対策上は，組織構成と資産管理上の組織が一致すべきであるが，現状に即した対応策が必要になる．そこで，本アプローチでは，組織単位として支線単位の対策を講じる方針をとり，その支線は３１に集約された．

(4) 業務上の運用組織とシステム運用上の組織の差異

一般の業務フローと，システム運用上の階層構造の相互関係は，組織が大きくなるに従い，矛盾を生じてくる．例えば，システム運用上の担当者と，システム運用上の権限を有する人物が異なる場合などである．具体的には，システム管理者は，アウトソーシング先の提携企業の担当者であるが，ソフトウェアシステムの運用責任者は学内の教員，さらに，そのシステムを利用する業務上の責任者は，別の学内の教員になっている場合などが該当する．このため，運用フローを見直す必要性はあるが，ISMS 上は，システムの管理運用責任者の観点に統一して記述する等の一貫性を確保する事が必要である．

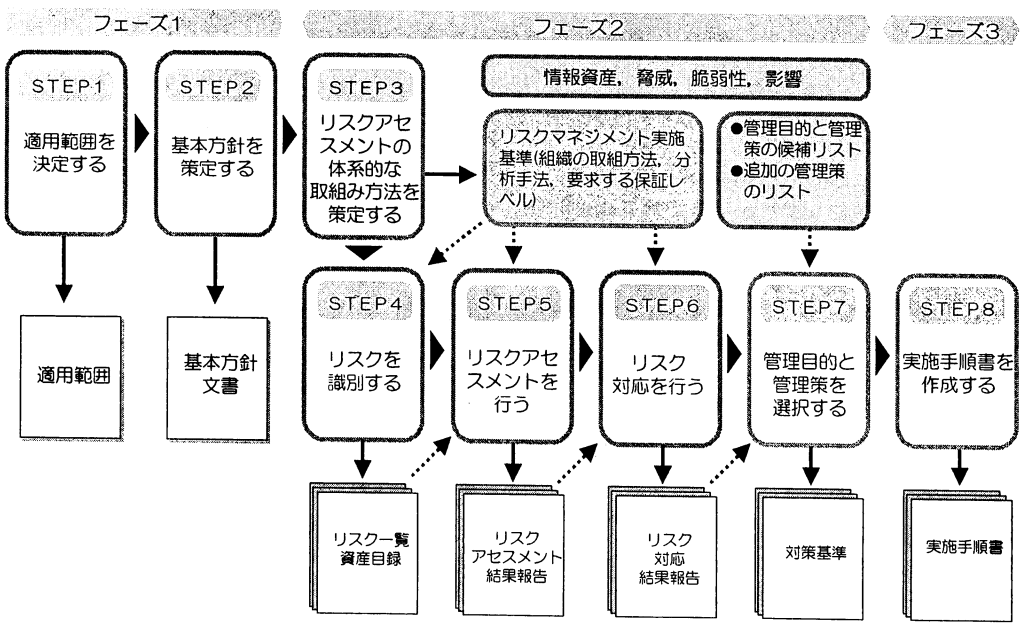

図 1　ISMS に即したセキュリティ対策実施手順

図２　開発した運用システムの表示例

3. ポリシ策定手順とその運用

3.1. ISMS 認証基準に即した運用フロー

図１は，ISMS の標準的なセキュリティ対策の運用フローを示している．徳島大学においては，大学の情報セキュリティポリシに関する研究会の公開文書に即したポリシ文書を原案として，かつ図１に概ね即したフローでの対策を講じる手法を導入した．

フェーズ１ではまず，適用範囲として，高度情報化基盤センター内の各システムおよび基幹ネットワークにする方式と，支線以下まで含めた全学システムを対象とする方式があった．ISMS では手法的に以下の二つのアプローチがある．

① 詳細リスク分析アプローチ

② ベースラインアプローチ

①では各リスク分析項目に対し，詳細に分析して，個々のリスクを網羅的に対策を講じる．このため，きめ細かな対策がとれるが，組織が大きくなればそれだけ膨大な時間と労力が必要になる．②は，国際標準規格などに記載されている項目のうち，所属組織に必要な項目のみを抽出し，そのポイントに絞って分析と対策を講じる手法である．対策費用面等で非効率な側面が生じる可能性はあるが，対策の一貫性が保て，基準を明確化できる側面もある．

前節の２方式のうち，本施策は，後者の全学展開活動が前提であり，前述のようなキャンパスネットワーク特性を考慮する必要がある．特に，大学組織の性格上，毎年数千人の学生が入れ替わり，かつ様々なシステムが乱立可能な状況下での対策という特性を考慮しなければならない．そこで，図中フェーズ２の STEP4 以降では，②のベースラインアプローチを採用した．

また，STEP1 の適用範囲は，STEP2 における基本方針に文書として明記し，その文書と STEP7 により策定される対策基準を組み合わせ，全体としてセキュリティポリシ文書として策定する事とした．同時に，各部局共通の実施手順書を策定し，必要に応じて，各部局独自に，実施手順書の加筆・修正を行える事とした．

基本方針や文書策定，組織作り，体系的な取組手順

が決まれば，一般には以下の手順に従い，対策を講じる．本学もこれに準じた．

a) 情報資産の洗い出し
b) 資産目録策定
c) リスクアセスメント
d) リスク対応計画
e) 計画実施
f) 適用宣言
g) 評価・見直し

3.2. セキュリティ対策上の特徴

(1) 情報資産目録作成上の特徴

情報資産の洗い出しにおいては，様々なレベルでの収集が考えられるが，本学においては，TUNES ネットワーク上で複数人により利用されるシステムを洗い出し，資産目録を構成する方針をとった．つまり，この目録に登録された情報・システム・機器は，大学組織として保護管理対象とする．一方，教職員が個々人で利用する PC 端末等は，個人のセキュリティ教育を実施した上で，個人の責任分界とした．また，情報資産の洗い出し時は，情報，システム情報，システム機器に分類した．また，情報資産は，管理責任がどこにあり，その情報のインプットとアウトプットが明確に判断できるような二次情報も含めて収集した．

(2) リスクアセスメントの特徴

作成された資産目録に対しては，リスク値を算出する．一般に，リスク値の算出式は次式となる．

リスク値＝重要度×脅威×脆弱性

ここで，本学においては，各値の最大値 3 ポイント整数値（リスク値の最大値 27 ポイント）とした．支線管理者と情報資産洗い出しの委員を担当者として選出された．この担当者が洗い出された情報資産項目を整理して，担当者に再度フィードバックし，担当者が入力の必要な項目に対してリスクポイントを入力する方式をとった．抽出されたリスク値に対しては，整合性や相対的なレベルの統一性などを分析・調整した．

(3) ポリシ文書の特徴

図 1 中の STEP5 までで，部局毎の特徴が出るため，その対応計画を策定し，実施する．さらに，適用宣言書にて，手続き的なセキュリティ対策の初回対策が完了する事になる．策定，導入，運用，見直しの循環は一般に PDCA (Plan-Do-Check-Action)サイクルと呼ばれ，これを継続的に循環させることが重要である．

ここで，徳島大学では，策定予算執行の関係上，PDCA サイクルのうち策定過程においては通常よりも大幅に短縮する必要があった．このため，ポリシ文書のレビューと策定は，情報資産目録作成からリスク分析，適用宣言書までの一連の対策活動と並行実施する事とした．また，ポリシ文書は，STEP2 の基本方針と，STEP7 の対策基準を結合した 2 部構成とした．

ここで本文書は，文献[2]と ISMS 認証基準(Ver.2)のそれぞれの内容を対応付けければならない．図 3 は，その対応上の部分的な例である．そこで本文書は，両文書の必要項目を網羅的に参照対応付けられるような内容とした．更に，実用性を考慮して，多種多様な立場の読者が，自分に必要な部分に集中して読む事ができるように，冗長敵記述を敢えて容認し，内容が文書全体に分散配置されないよう工夫した．また，文書の記述レベルの一貫性をもたせるため，実情の業務運用フローよりも寧ろ，業務の責任が誰に帰着するのか，という観点から記述する事とした．

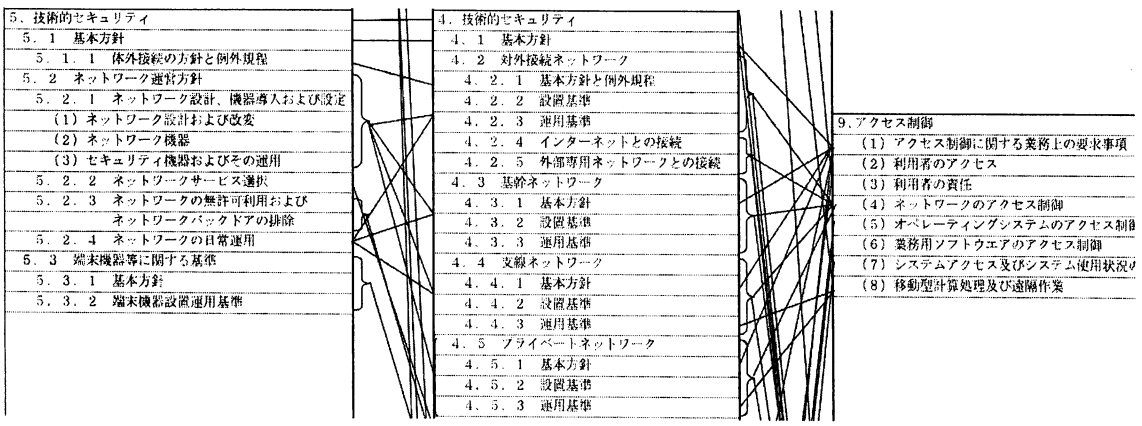

図 3　大学における情報セキュリティポリシーの考え方，徳島大学情報セキュリティポリシ，および ISMS ver 2.0 相互の網羅する項目の対応の一例．

4. 運用システム構築と運用

4.1. 運用システムを用いた対策の概要

実際に，前章の対策フローを支援する運用システムを開発した．本章で，本システムを解説しながら，作業フローの概要について述べる．

最初に組織作りを行うために，支線管理者と資産調査委員を中心とするキックオフミーティングを開催した．ミーティング参加者が各部局の責任者となり，末端システム管理者までを含めた教職員により，情報資産洗い出し以後の作業が行われた．

具体的には，情報資産洗い出し時は 31 の支線に及ぶ支線管理者により構成されるメーリングリストとBBS によるコミュニティを形成し，セキュリティに関する WG メンバが作業支援を行った．結果として，大学構成員約 8,000 名に対し，洗い出された情報資産は，約 800 項目に集約された．

4.2. 運用システムの概要

この間，図 1 におけるセキュリティ対策の運用フローで最も重要な，情報資産の洗い出しとリスク分析のためのシステムを開発した．本システムは，一般的なセキュリティレベルを確保（学内限定アクセスで，認証および暗号対策を講じた）した WWW-DB 連携システムとして PHP と RDBMS を用いて開発した．図 2 は，そのシステムの部分的なスナップショットである．

本システムを通じて，情報資産を登録・削除・編集できる他，そのリスク値算出の根拠情報の入力などが可能である．また，入力されたデータを元に，図 1 STEP4 に示される情報資産目録や，同 STEP5 のリスクアセスメントのデータが自動的に集計される．

4.3. システムを通じたリスクアセスメントの結果

リスク値は，既に述べたとおり，最大値２７までとるが，要対策となる閾値として１０を選択した．この数値は，現実的にはかなり厳しい値であり，実際ほとんどの部局における資産目録項目が，要対策となった．この原因には，特殊な事情を除き，多くは以下の２点に特徴付けられた．

（１） 入退室・施錠管理策

（２） マニュアル整備

これらの対策は ISMS 認証基準上常識的であっても，一般に大学の体質として，これまで注力されてきていなかった事項である．このような典型的な要因と対策を含めて，リスク対応計画を以下の観点から構築する必要がある．

（A） 低減：管理策を講じる

（B） 移転：リスクを外部に移転する

（C） 回避：リスク発生の可能性を削減する

これらの結果も反映させて，適用宣言書を作成した．ここで，本システム内に蓄積された情報資産およびリスクアセスメントデータを元に，翌年度以降の継続的な作業軽減が図れる．つまり，各部局のセキュリティ対策の担当者は，前年度までに抽出された情報に対する差分だけをメンテナンスすればよいためである．また，この情報は，担当者が変わっても容易に理解できるよう，なるべく典型的な例と，特殊な例をシステム入力時の例として具体的に FAQ としてまとめ，公開した．これは，記述レベルの統一の側面からも必要不可欠であった．

5. むすび

情報セキュリティ対策では，技術的セキュリティが注目を集める事が多い．しかし，それ以外の人的セキュリティや物理的セキュリティが原因で，事故・事件が発生している例が少なくない．このため，人的・技術的・物理的セキュリティに代表される各項目を統合的かつ，総合的に分析・対策を講じることが重要である．その際，完全性・可用性・機密性の３つの側面から多面的に分析する必要がある．

そこで本稿では，近年の情報セキュリティ対策への要求を受けて徳島大学において実施している ISMS 準拠の活動について報告した．これは，分散キャンパスという特徴を有し，医学系・工学系などの様々な分野の学部を有する大学における ISMS 準拠のセキュリティポリシ策定と，その実施策のケーススタディである．特に，大学において曖昧になりがちな，責任の所在をはっきりさせる意味で，本手法は最も効果的である．今後は，実際に ISMS 認証取得に向けた対策と，運用システムの改善を実施する予定である．

謝辞 本プロジェクトは平成 15 年度徳島大学学長裁量経費の援助を受けた．ここに深甚なる謝意を表する．

文 献

[1] 情報セキュリティ対策推進会議，“情報セキュリティポリシのガイドライン，” 2000. http://www.kantei.go.jp/jp/it/security/index.html

[2] 大学の情報セキュリティポリシーに関する研究会，“大学における情報セキュリティポリシーの考え方，” 2002. http://www.kudpc.kyoto-u.ac.jp/Security/

[3] 打川和男，情報セキュリティポリシーの実践的構築手法，オーム社，2003.

[4] 日本工業標準調査会，情報技術－情報セキュリティマネジメントの実践のための規範，JIS X 5080，2002.

[5] British Standards, Information Security Management Systems – Specification with Guidance for Use, BS7799-2:2002, 英和対訳版，