中小私立大学における情報セキュリティ対策に関する一考察

佐伯　勇

Study of Information Security Management in Small and Medium-sized University

SAEKI Isamu

Abstract : For the last decade, Japanese government has provided basic guiding principles necessary for managing the information security. However, the information security managements do no function enough at many small and medium-sized universities. In this paper, I analyze the cause why this kind of management fails in many universities. On the basis of this result, I introduce an effective case and describe how to develop security policy gradually.

はじめに

大学の情報化進展にともない，教育・研究・事務業務の多くがコンピュータや情報ネットワークによって支えられるようになった。大学業務における情報ネットワークシステム依存度の高まりに比例して，情報セキュリティ事故の発生確率と影響が日増しに大きくなっている。個人情報保護など情報管理の厳格化が叫ばれる中，大学としても情報セキュリティを高めなければ，社会的信用を失いかねない時代となった。

日本では，内閣の高度情報通信社会推進本部の情報セキュリティ対策推進室が，2000年に「情報セキュリティポリシーに関するガイドライン」[1]を策定し，情報セキュリティを担保するために必要となる政府関連機関の情報セキュリティポリシーに関する基本的な考え方・策定・運用及び見直し方法のガイドラインを示した。各省庁などはこのガイドラインを踏まえ，情報セキュリティポリシーを策定した。その後も，2005年には内閣官房の情報セキュリティセンター（NISC）と，高度情報通信社会推進戦略本部（IT戦略本部）の情報セキュリティ政策会議が設置され，官民における統一的・横断的な情報セキュリティ対策の推進が図られている。

内閣の動きを受けて国立大学では，全国共同利用大型計算機センター長会議のもとに「大学の情報セキュリティポリシーに関する研究会」が発足し，2002年には「大学におけるセキュリティポリシーの考え方」[2]がまとめられた。2007年には，国立情報学研究所の「国立大学法人等における情報セキュリティポリシー策定作業部会」と電子情報通信学会の「ネットワーク運用ガイドライン検討ワーキンググループ」が「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」[3]を公開した。これらの報告書をもとにして，国公立大学の情報セキュリティ対策は急速に進んだ。

私立大学では，私立大学情報教育協会のネットワーク研究委員会のもとに不正侵入対策小委員会が設置され，2002年に「提言　私立大学向けネットワークセキュリティポリシー」[4]がまとめられた。

この10年間の間に，情報セキュリティ対策を行うために必要な基礎的情報は整備されてきたが，一部の大規模私立大学における先進的事例を除くと，効果的な情報セキュリティ対策を行っている私立大学はそう多くはない。私立大学情報教育協会の平成20年度私立大学情報環境基本調査（中間集計結果）によれば，セキュリティポリシーを策定し対策を実施していると

回答した私立大学は26%に留まっている。さらに，対策済みと回答した26%の大学の中には，セキュリティポリシーを策定したものの，PDCAサイクルが機能せずに実質的な効果が得られていない大学も含まれていると推測される。

中小の私立大学ではなぜ情報セキュリティ対策が進まないのか，対策を実施しようとした大学がなぜ頓挫してしまうのか。本稿では，まずこれらの要因を分析する。さらにこの結果を踏まえて，中小の私立大学で効果的な情報セキュリティ対策を講じるための指針を提案する。

1　情報セキュリティリスクの特徴

防災や防犯など大学が取り組むべきリスク管理の中で，情報セキュリティリスクは，日々新しい脅威が生まれるためリスク低減が大変困難であるという特徴がある。その理由を次に3点示す。

1.1. 新しい攻撃手法の登場

ウイルス，ワーム，ボットネット，スパイウェア，フィッシング，不正アクセス，DoS攻撃，DNSキャッシュポイズニング，SQLインジェクションなど攻撃手法が日々高度化，多様化している。これらの攻撃によりコンピュータシステムの管理者権限が乗っ取られ，不正行為が行われる事例が後を絶たない。またこれらの攻撃を自動的に行うツールがインターネット上で流通しており，誰でも比較的容易に入手可能である。

1.2. 新しいソフトウェアやサービスの登場

利便性の高いソフトウェアやサービスが次々と登場し，使用方法を誤った場合のリスクの存在を理解せずにユーザーが使用して情報漏えい事故に至るケースが多発している。たとえば，匿名性の高い状態でファイルを交換できるPeer to Peer（P2P）ファイル交換ソフトウェア，インターネット上の地図に個人的な情報を保存し公開可能なGoogle Maps，インターネット上で文書などを作成・保存し公開可能なGoogle Appsなどを使用し事故に発展した例がある。

1.3. 新しいハードウェアの登場

USBメモリ，各種メモリカード，超小型パーソナルコンピュータなど可搬型記録媒体の低価格化と大容量化が進み，膨大なデータを誰もが手軽に学外に持ち出せるようになってきた。これらの媒体の紛失，盗難，廃棄ミスなどによる情報漏えい事故が後を絶たない。

このように，情報セキュリティリスクは日々急速に拡大し続ける特徴を持ち，どのような対策を講じたとしても決してなくならないものと覚悟すべきである。

2　情報セキュリティリスクの管理方法

前節で述べたとおり，情報セキュリティリスクはどのような対策を講じても根絶できないし，時間の経過とともに増大していくという特徴を有する。しかし，情報セキュリティリスクをゼロに近づけることは不可能ではない。そのために必要なリスク管理方法を次に4点示す。

2.1. リスク分析

リスク分析とは，保護すべき情報資産を明らかにし，それらの情報資産に対するリスクを評価することである。世の中で広く用いられているリスク評価方法であるGMITS（ISO/IEC TR 13335 guideline for the management of IT security）では，リスク値を次式で定義する。

リスク値＝資産価値×脅威の程度×脅威の頻度×脆弱性の程度

組織内の全部局が利用する情報資産を洗い出してリスク評価を行い，リスクの大きいものから順に，回避，最適化，移転，保有という対応を取るよう分類する。

2.2. 全組織的な情報セキュリティ委員会の運営

セキュリティポリシーを策定し円滑な運用を行うためには，図1に示すような情報セキュリティ委員会を構成して対応する必要がある。ただし，図中の職名は大学の組織形態によって異なる可能性がある。

情報セキュリティ委員会は，全学の情報セキュリティに関して，基本的なセキュリティポリシーの策定，重要事項の決定，対外的な対応などを行う。たとえば，セキュリティポリシーの策定と改訂，セキュリティポリシー遵守の励行と違反に対する措置，教育研究活動におけるネットワーク利用ルールの制定，学内の他の機構との調整，外部との折衝などが主な任務であ

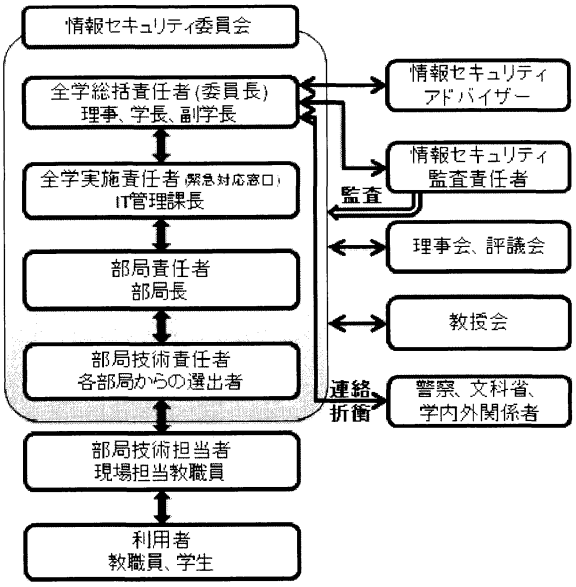

図1　情報セキュリティ委員会の例

る。また，各責任者に対して情報セキュリティに関する教育を行うとともに，一般の利用者に幅広く初心者教育を行う。

全学総括責任者である委員長は，予算と人事の権限および責任を有する学長，副学長あるいは理事に相当する者が望ましい。全学総括責任者は，いわゆる最高情報責任者（CIO）の役割となる。図1では，各部局責任者と部局技術責任者を含む大規模な委員会を学内に1つ設置する場合を示しているが，大規模大学では部局ごとに委員会を設ける二段構成とすることもある。学内外組織との交渉は委員長が，事故発生時の緊急対応は全学実施責任者が担当する。

情報セキュリティ対策には，情報システム技術や対処方法の専門的な知識と経験を必要とするため，実施規程の策定・導入から運用，評価，見直しまで専門的な助言を行う専門家を活用することが重要である。全学総括責任者が情報システムに関する専門的な知識と経験を持つため専門家の助言を必要としないような特殊な場合を除き，情報セキュリティアドバイザーを置く必要がある。さらに，情報セキュリティ委員会とは独立した情報セキュリティ監査責任者がセキュリティ対策実施状況の監査を行うが，既に学内に内部監査室などの監査組織が設置されている場合は兼務させることも可能である。

2.3. セキュリティポリシーの策定

セキュリティポリシーは，大学が所有するネットワークとネットワーク上の情報資産のセキュリティ対策

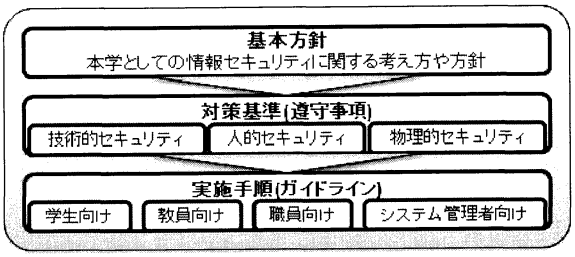

図2　セキュリティポリシーの構成モデル

について，大学が総合して体系的かつ具体的に取りまとめたものである。どのような情報資産をどのような脅威からどうように守るのかという基本的な考え方や，セキュリティを確保するための体制・組織・運用を示す規定である。セキュリティポリシーの文書構成には特に決まりがあるわけではないが，図2に示すとおり，セキュリティに対する基本方針，対策基準，実施手順で構成することが多い。

基本方針は法律でいう憲法に相当するものであり，大学としての情報セキュリティに関する考え方や方針を示したものである。基本方針は学内外に積極的に公開し，学内向けにはポリシーの周知徹底，学外向けには信頼感を与える役割を持つ。

対策基準は基本方針を具体化し，システムの利用形態や脅威などによって対策を考えやすいように分類したうえで，それぞれについて遵守すべき規定を記述したものである。攻撃に有利な情報が漏えいする可能性があるため，対策基準はその規定が必要な構成員にのみ公開すべきである。

実施手順は対策基準を現場レベルで実施するために，学生，教員，職員，システム管理者など対象者ごとに内容を抜き出し説明したものである。実施手順に関しても基本的には公への公開を避けるべきであるが，仮に第三者に見られた場合でも問題が生じないよう記述内容に配慮しておく必要がある。

2.4. PDCA サイクルの実施

PDCA は，Plan-Do-Check-Act の略で，品質改善や環境マネジメントでよく知られた手法である。セキュリティ対策は一度行ったら終わりというものではなく，セキュリティ環境の変化に応じて常に見直しと改善が求められる。図3に，情報セキュリティ対策で行われる PDCA サイクルの一例を示す。Plan でセキュリティポリシーを策定して目標を達成するための計画を立て，Do で対策を導入して教育・運用し，Check で監査して対策が計画通り行われて当初の目標を達成

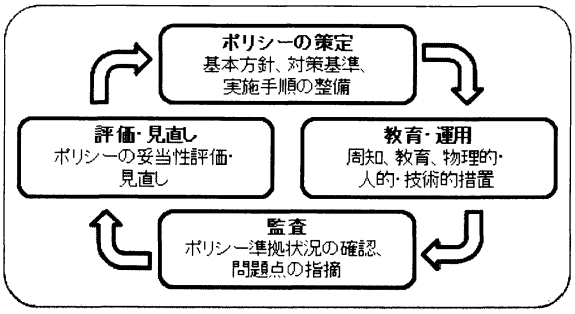

図3　PDCAサイクル

しているかを確認し，Actで評価結果をもとに業務の改善を行う。この段階でPDCAサイクルが1回転し，見直しと改善の結果に基づいて新しいサイクルに入ることになる。

3　私立大学における情報セキュリティ対策状況

前節で示したセキュリティ対策は，大学トップの強力なリーダーシップのもとに全構成員の協力が得られなければ決して成功しない。企業と比較して統治能力の低い私立大学では対策を行いにくいはずだが，実際はどのような状況であろうか。

私立大学情報教育協会では，大学の情報セキュリティ対策の自己点検・評価のツールとして，2009年に情報セキュリティ対策チェックリスト（案）[5]を公開し，平成21年度大学情報セキュリティ研究講習会において，講習会参加大学の自己評価を集計した。情報セキュリティ対策チェックリスト（案）は，情報資産の把握，組織的対応，人的対応，技術的・物理的対応の4分野から構成され，それぞれの分野に用意された詳細な設問にそれぞれ6点満点で回答する形式となっている。1〜3点は「できていない」，4点は「一部できている」，5〜6点は「できている」という評価に対応する。調査の対象は全国42私立大学と4私立短期大学である。集計結果については，現在のところ当日会場で配布された中間報告でしか公表されていないため，本稿では各項目の平均値をさらに各分野で単純平均した値を求め表1に記した。

表1から，全ての分野において自己評価が4を下回っていることが分かる。これは，大半の私立大学において，情報セキュリティ対策が十分に実施されていないことを示している。さらに，講習会会場での議論や報告などでは，対策を実施していると回答した大学でも，「作ったルールを覚えきれない」「講習会をしても人が集まらない」といった問題点が多く指摘されていた。つまり，経営陣のリーダーシップや学内の理解が十分に得られない中，先進的な大学では政府や大学業界団体の定めた基準を参照してセキュリティポリシーの策定が進められたのだが，立派なセキュリティポリシーを策定することに注力した結果PDCAサイクルが回らず，ポリシーが絵に描いた餅状態になっていると推測されるのである。

表1　情報セキュリティ対策チェックリスト自己評価

分　野	平均値
情報資産の把握	3.05
組織的対応	3.29
人的対応	3.34
技術的・物理的対応	3.20

4　中小私立大学における効果的な事例

全国の私立大学の多くが効果的なセキュリティ対策を取れない中，理工系学部のない3学部構成で入学定員800名弱のX大学の取り組みが，多くの大学の参考になると思われるのでここで紹介しておきたい。なお，X大学の取組状況は30分程度の聞き取りで入手した情報であり，今後詳細な情報を調査したいと考えている。ここでは，取り組みのポイントのみ示しておく。

（ア）将来的にはセキュリティポリシーが必要だと感じているが，現在は作成せず。
（イ）その代わりに，セキュリティ宣言を学長名でWebに掲載。
（ウ）学長を委員長とする全学的な情報セキュリティ委員会を設置。（年1回程度開催。）
（エ）4名程度で構成する小委員会を設置。最新情報の収集や教育を担当。
（オ）絶対に守るべき10カ条をA4一枚で作成。（暗黙のルールの明文化。各種機関が作成しているルールやこれまでの事故事例を参考に主観的に判断。）
（カ）教職員には講習会，学生にはオリエンテーションで説明。
（キ）事故が発生するたびに学長に報告し，小委員会で協議。迅速な対応が難しいため情報セキュリティ委員会には事後報告。
（ク）発生した事故や他大学の事故事例をもとにル

ールの項目を徐々に追加。

X大学は，セキュリティポリシーは作るものではなくて育てるものであるとの考えのもと，PDCAサイクルを回すことを最優先に，誰でも理解し守ることができるルールを定めて対策を講じている。しかし，この程度の対策でも，社会的責任やリスク低減の観点から何もしないよりはるかに有効だと考えている。X大学の担当者は次のように語っていた。

「現場の教職員から反対の声が出るようなルールは定めてはいけない。今後も情報セキュリティ事故は発生し続けるので，事故のたびに少しずつルールを追加していく。このようなパッチワーク的な対応を繰り返していると，学内で抜本的な対策を求める声が高まってくる可能性がある。そのような空気が生まれて初めて，セキュリティポリシーを定め本格的に情報セキュリティ対策を実施することができるのではないか。」

大学のような比較的統治能力の低い組織では，大学構成員が情報セキュリティ対策の必要性を強く実感しなければ，トップダウンアプローチが必要な全学的危機管理体制は実現できない。最初は誰もが反対しない最少ルールを定めてPDCAサイクルを回し続け，構成員の意識が高まるのを待つという手法は，多くの中小私立大学でも大いに参考にできるのではないだろうか。

ま　と　め

情報セキュリティ対策に関する情報やコンサルティングサービスがあふれる中，一部の先進的な中小私立大学は身の丈を遥かに超えたセキュリティポリシーを策定してPDCAサイクルを回すことができず，対策が頓挫しているようである。情報セキュリティポリシーは作るものではなく育てるものである。最初は構成員が物足りなく感じるほどの簡単なルール作りから始め，PDCAサイクルの中でセキュリティポリシーを育てていくことが最も効果的なアプローチとなる中小私立大学が多いのではないか。今後は，X大学の事例を詳細に調べ，スムーズに情報セキュリティ対策を講じるポイントをさらに整理していきたい。

参考文献

1）情報セキュリティ対策推進室，2000，『情報セキュリティポリシーに関するガイドライン』，http：//www.kantei.go.jp/jp/it/security/taisaku/guideline.html.

2）大学の情報セキュリティポリシーに関する研究会，2002，『大学におけるセキュリティポリシーの考え方』，http：//www 2.itc.nagoya－u.ac.jp/security－policy/tousin.html.

3）国立情報学研究所　国立大学法人等における情報セキュリティポリシー策定作業部会，電子情報通信学会　ネットワーク運用ガイドライン検討WG，2007，『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』，http：//www.nii.ac.jp/csi/sp/.

4）社団法人私立大学情報教育協会，2002，『提言　私立大学向けネットワークセキュリティポリシー』，http：//www.juce.jp/LINK/report/netsec 2002.pdf.

5）社団法人私立大学情報教育協会，2009，『情報セキュリティ対策チェックリスト（案）』，http：//www.juce.jp/sec/checklist 2009/juce_sec_list.pdf.

6）土居範久監修，独立行政法人情報処理推進機構，2009，『情報セキュリティ教本　改訂版　組織の情報セキュリティ対策実践の手引き』，実教出版.

7）独立行政法人情報処理推進機構，2009，『情報セキュリティ読本　改訂版　IT時代の危機管理入門』，実教出版.

8）畠中伸敏編著，2008，『情報セキュリティのためのリスク分析・評価』，日科技連出版社.

9）佐伯勇，2007，『大学における情報ネットワークセキュリティ』，甲南女子大学研究紀要人間科学編，Vol.44，pp.69–73.