

# 情報セキュリティポリシー - の策定について

長嶋 豊，中島 賢治\*，大淵 寛\*\*，中原 勝俊\*\*\*，汐除 時也\*\*\*\*

情報処理センター長，\* 副センター長，\*\* 情報処理センター，

\*\*\* 電子制御工学科，\*\*\*\* 長崎大学経理部

## 1. はじめに

最近、インターネットやブロードバンド技術の普及とともに、広く自由なサイバー空間が享受できるようになった。その反面、コンピュータウイルスやプライバシー侵害など、多種多様なネット犯罪が激増しており、深刻な状況は収まるところを知らない。一方、政府は「e-JAPAN重点計画2003」を定め、

世界最高水準の高度情報通信ネットワークの形成、

人材の育成と教育・学習の振興、

電子商取引等の促進、

行政・公共分野の情報化、

高度情報通信ネットワークの安全性と信頼性の確保、

に集中的に取り組むとしている。

及び は高等専門学校にも深い関連があり、特に、 は情報セキュリティ確保の重要性が示されている。

情報セキュリティとは、「セキュリティ上の危険や脅威から情報資産を保護し、機密性、完全性、可用性の観点で正常な機能・状態を保持することにより、情報システムや情報の信頼性を高め、利用者が安心して情報システムを利用できるようにすること」と定義されている。

しかし、現在のインターネット社会は安全性が保証されないため、情報セキュリティは自己責任が原則とならざるをえない。しかし、関連する領域は技術、法律、制度、規格など多岐に渡るため、完全なセキュリティ対策を一高専で立てるのは困難な状況であった。

数年前から政府は情報セキュリティに関する啓蒙活動を盛んに行ってきたが1) - 3)、大学や高専が参考にできる材料に乏しく、必要性は認識されながらも策定には至っていなかった。

平成14年3月、大型計算機センターを設置している7大学の関係者が共同で「大学における情報セキュリティポリシー - の考え方、以下大学編と略す」を刊行し、大学等における情報セキュリティポリシー（以下ポリシーと略す）の基本的な指針が示された。本校では、「大学編」をモデルにした「情報セキュリティポリシー - 」の策定、「利用者用実施手順」の策定、「情報処理センターシステム管理者用実施手順」の策定を行い、今年度から運用をはじめた。本報では特に、ポリシーについての策定経緯や概要及び今後の課題等について報告する。

## 2. 情報セキュリティポリシー - 策定

### 2.1 ポリシー - の策定準備

情報処理センターでは、平成14年度の重点目標として「ポリシー - の策定」を掲げ、前年度から関連情報の収集を行ってきた。昨年8月には本省主催情報セキュリティセミナー、11月には国立情報学研究所と九州大学共催情報セキュリティポリシー - 入門講座へ出席した。昨年度当初はギガビットLAN切替の残務等から、ポリシー策定の着手が遅れ、結局ポリシー策定作業部会を9月に発足させ、草案作りを開始した。

一方、学内のポリシーに対する意識向上を図るために、教官会議向けポリシー紹介資料を作成、配布した。「情報セキュリティポリシーとは、本校における全ユ - ザの膨大な情報資産と佐世保高

専 LANを構成する情報システム全てを、どのような体制で、責任者はだれで、どのように守るか、組織体の意志としての方針・目標であり、基本方針 - 対策基準 - 実施手順を整備しておくこと」であることを説明した。サービス提供や操作性、コストとセキュリティの関係が相反することにも言及した。

まず、「大学編」をモデルとして、ポリシーに相当する「基本方針」と「対策基準」を作成した。現在運用しているポリシーと実施手順の体系図を図1に示し、今年8月文部科学省主催の情報セキュリティセミナーで示されたポリシー最新体系図を図2に示す。従って、今年度の評価・改善では、「マニュアル」について規定する必要がある。

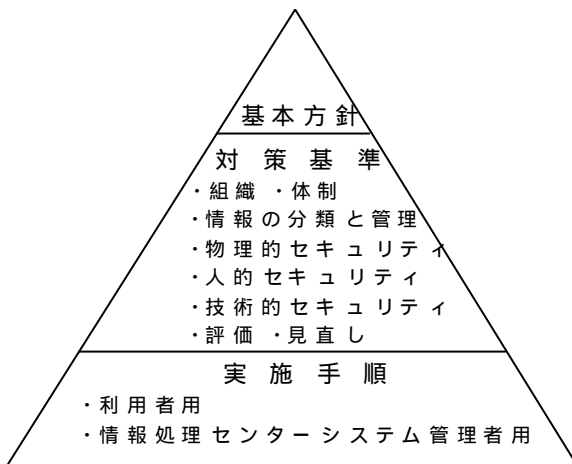


図1 現行の情報セキュリティポリシー - 体系

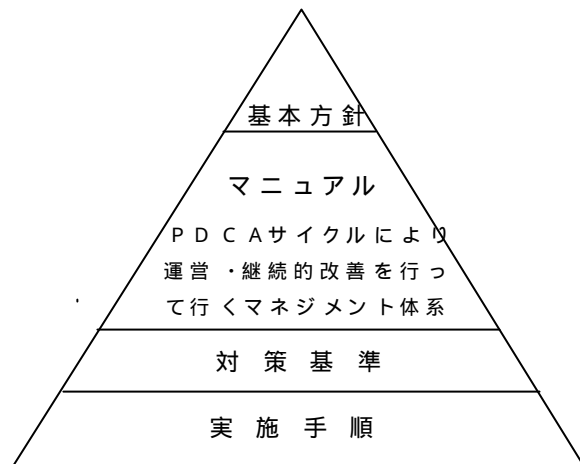


図2 今後の情報セキュリティポリシー - 体系

「大学編」では、要件がどの程度重要であるかを明確にするために、次の4種類の表現が使用されている。

しなければならない：最低限実施すべきこと。

すべきである：可能な限り早期に実施すべきである。

することが重要である：即座に実施しなくても優先的に実施すべきであることを示す。

する事がのぞましい：実施または考慮することが望ましい。

ポリシー策定に当たっては、具体的に実践していることや実現可能な内容について規定したので、できるだけ の表現を使用した。更に、ポリシー - 及び実施手順は策定後も常に計画・運用・評価・改善（Plan - Do - Check - Action：P D C Aと略す。）を図るべき性格のものであり、最初から完成度の高い内容を狙わない方針とし、策定に当たった情報処理センタ - 委員会や情報セキュリティ委員会等でその旨説明を行った。

## 2.2 情報セキュリティポリシーの基本方針

### (1) 基本方針

第1部の基本方針では、本ポリシー - の目的や定義、対象範囲及び、実施手順を別途策定することについて規定した。

### (2) 対策基準 - 組織・体制の確立 -

第2部の対策基準のうち、組織・体制の確立には最も時間を割いて議論をし、「大学編」を編纂した研究会の金澤正憲主査や国立情報学研究所、九州大学等にも本校の実情を説明、確認を行った。ポリシー - の策定と運用については、先ず学内トップ層の理解が必要不可欠であり、トップダウンで推進できるように考え、「最高情報セキュリティ責任者」には校長を選任した。更に、運営委員会



## (7) 評価・見直し

策定したポリシーをPDCAサイクルで定期的に評価・見直しするために必要な措置を規定した。

以上から構成したポリシー案は平成15年2月情報処理センター委員会では了承され、翌3月の運営委員会時に第1回情報セキュリティ委員会を開催して、ポリシーの概要説明・審議の上、正式に本校情報セキュリティポリシーとして決定した。

## 3. 情報セキュリティポリシーの運用

本学構成員にポリシーを遵守してもらうために、全教職員へは「ポリシー」と「利用者用実施手順」を周知する必要から、印刷、製本し配布した。全ページに複写防止用透かし文字を加えて印刷し、転・退職時や改訂時にポリシー等を回収しやすくするために、全冊に管理番号を付し、受領印を押してもらいながら配布した。

運用に際して以下の措置を講じた。

- (1) 学生に対しては、情報セキュリティポリシーを策定したこと、第1弾として、実施手順の重要事項を情報処理担当教官へ配布、講義時の参考教材として使用することを依頼した。
- (2) 技術的セキュリティとして、メールサーバに加えてWebサーバへもウイルス対策ソフトをインストールした。更に、第1演習室及びCAD室(各49台)全端末にウイルス対策ソフトをインストールするとともに、全教職員へも対策ソフトをできるだけ使用するように依頼した。
- (3) 物理的セキュリティとしてLAN管理室に電子錠を設置した。近々光ファイバー端子室兼事務室にも取り付ける予定である。更に、保安上の問題から、夜8時より朝7時まで及び土日は終日ロックアウトするようになり、校舎主要出入口にも電子錠が設置された。その結果、ホームルームや教官室、研究室、実験室の情報資産の管理が行き届くようになった。
- (4) 8月11日に情報公開された、史上最強のウイルス「MSプラスト」対策では、情報処理センター演習室及びCAD室へのOSの脆弱性を修正するパッチ当て作業を休日返上で実施した。さらに、教職員や学生向けに、メールはもちろん、掲示や印刷物を使用して対策の徹底を要望した。対策専用ソフトをCD-ROMに書き込み、学科等システム管理責任者やボランティアの教室系技官の方々の協力を得て、各学科の措置を担当してもらった。専攻科生に貸し出しているノート型パソコンや個人登録してる学生のパソコンの処理は、各自でセンターに持参してもらい、全てについて対策を施した。その結果、MSプラスト被害の報告はなかった。
- (5) その他、スパムメール対策を行って、1週間に3000件以上の不要メールをサーバで除去しているが、不十分であり一層の対策が必要である。

## 5. おわりに

情報セキュリティポリシーを策定し、運用を開始するまでの経緯や概要について報告した。ポリシーは、PDCAサイクルでスパイラル的にセキュリティを向上させることが求められるので、これから運用を通して問題箇所を評価・改善する予定である。

今後の課題としては、

- (1) 学生への情報セキュリティ教育の徹底する。次年度からは、ユーザIDの自動的な付与はやめ、簡易テスト等である一定以上の情報セキュリティレベルをクリアしてから付与する。
- (2) 教職員への情報セキュリティ教育・研修を実施する。
- (3) 公式ホームページ上の掲示板やコンテンツに関してセキュリティ上の問題点を見直す。
- (4) IDS(侵入検知システム)等の導入と運用などセキュリティを確保するために必要な予算措置に取り組む。

- (5) 中期計画・中期目標に沿った運用を行う。
- (6) 平成14年11月28日版(改訂部分見え消し)資料2)及び情報セキュリティポリシーに基づく対策の実施に関する参考資料、平成14年12月25日付)を参考にした評価・修正等、平成15年8月29日付、文部科学省主催情報セキュリティセミナーの指導に沿った改善を行う。
- (7) ポリシーが遵守されているかの監査を実施する。

#### 参考文献等

- 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ーに関するガイドライン、平成12年7月18日及びA省情報セキュリティポリシー例、平成12年10月
- 2) 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ーに関するガイドライン(改訂部分見え消し)、平成14年11月28日、及びA省情報セキュリティポリシー例(改訂部分見え消し)、平成14年11月
- 3) 文科省政策課情報化推進室；文部科学省情報セキュリティセミナー、平成13年7月30日
- 4) 金澤正憲主査他；大学の情報セキュリティポリシーに関する研究会編；大学における情報セキュリティポリシーの考え方、平成14年3月29日
- 5) ネットワークセキュリティセミナー実行委員会編；第6回情報セキュリティセミナーテキスト、平成14年9月25、26日
- 6) 国立情報学研究所、九州大学情報基盤センタ共催；平成14年度情報セキュリティポリシー入門講座資料、平成14年11月8日
- 7) 高野茂；文科省情報化推進室長；情報セキュリティポリシーに基づく対策の実施に関する参考資料、平成14年12月25日
- 8) ネットワーク社会における情報の活用と技術[情報教育テキスト]、岡田正、高橋参吉、藤原正敏編、実教出版、平成15年2月
- 9) 国立情報学研究所情報セキュリティポリシー関連資料、2003.3
- 10) 九州大学経理部編；国立学校情報セキュリティポリシー実施手順書(事務用標準版)、平成14年3月(CD-ROM版)
- 11) URL集
  - <http://www.sinet.ad.jp/info/policy/index.html>
  - <http://www.jpccert.or.jp/>
  - <http://www.ipa.go.jp/>
  - <http://www.netsecurity.ne.jp/>
  - <http://www.ieice.org/jpn/netguide00294.html>
  - <http://www.jnsa.org/policy/guidance/index.html>