

本学での情報セキュリティポリシー策定と施行

お茶の水女子大学 総合情報処理センター 浅本紀子

asamoto@is.ocha.ac.jp

1. はじめに

IT革命といわれて久しいが、技術の急速な発達にともなう膨大な情報の蓄積・加工能力や、ネットワークの高速化・広域化を手にいれたわれわれは、情報セキュリティ上の新しい脅威にもさらされた。平成12年7月18日情報セキュリティ対策推進会議決定の「情報セキュリティポリシーに関するガイドライン」においては、情報セキュリティポリシーを策定し、これに基づく総合的・体系的な情報セキュリティ対策を図ることとされてしている[2]。学問研究の場である大学においても、技術に支えられた情報基盤の整備とともに、確固たるセキュリティが確保されて、はじめて自由で効率的な教育研究が可能となるはずである。残念ながらお茶の水女子大学においては、独立行政法人となった2004年4月の段階ではセキュリティポリシー作成については未着手であった。本発表は、2004年度の1年間の本学における情報セキュリティポリシーの策定と施行およびネットワーク利用ルールに関する報告である。

2. セキュリティポリシーの策定まで

2004年4月:

国立大学法人となり、本学では運営組織の変更がおこなわれた(図1)。新しい組織においては、情報セキュリティは「情報推進室」の担当となり、学術・情報機構長が担当副学長となった。情報推進室は、評議員を室長、企画広報課長を副室長とし、図書館事務長、総合情報処理センターから2名、各学部から1名ずつの室員でスタートした。

多くの大学でも同様の事情だろうが、室員となった教員のほとんどが情報の専門家ではなく、室会議では他大学の資料等を参考に、まずは自分たちが勉強するところから始まった。

2004年5月:

情報セキュリティポリシーの目次案を作成した。目次は比較的すんなりと決まったのだが、この段階で問題となったのは、次の2点である。

1.(2)対象範囲と対象者

2.(1)(2)(3)の記述の詳細度

本学は、同一敷地内にすべての教育課程の附属学校園を有している。また大学の特性として正式に所属している教職員学生以外の出入りが恒常的に存在する。議論の結果、本ポリシーの対象者は、教職員(常勤、非常勤を問わない)、学部及び大学院の学生、研究生、聴講生、附属学校生徒等の大学・附属学校の全構成員並びに本学のネットワーク又は情報資産を使用する委託業者及び来学者とすることにした。

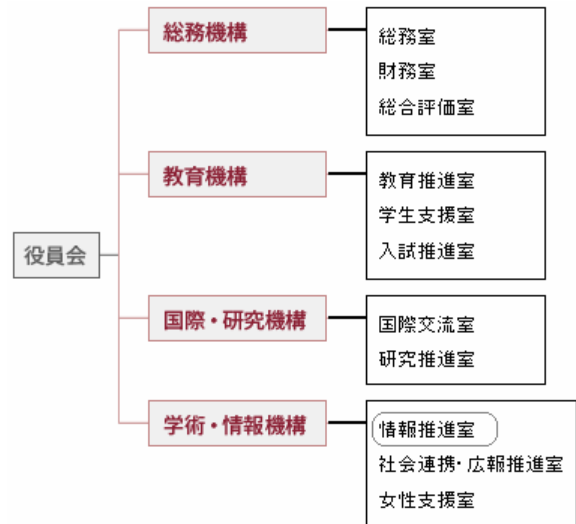


図1: 組織図

1. 基本理念と方針
 - (1) 用語の定義
 - (2) 対象範囲と対象者
 - (3) 情報の分類と管理
 - (4) 組織の構成と権限
2. 情報セキュリティ対策
 - (1) 物理的セキュリティ
 - (2) 人的セキュリティ
 - (3) 技術的セキュリティ
 - (4) 緊急対処
3. 評価と見直し

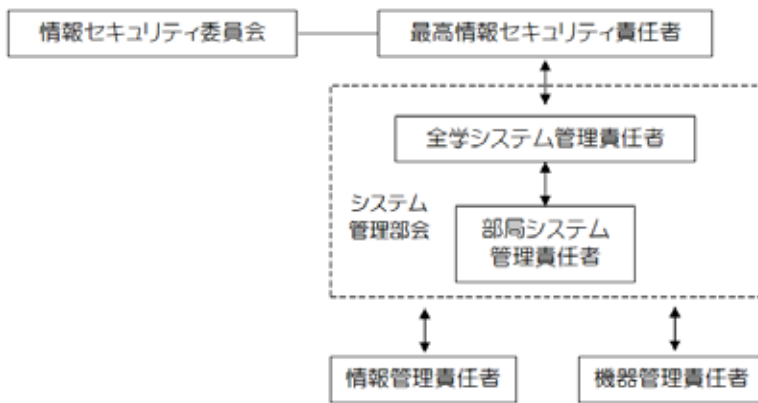


図2: 情報セキュリティ組織の構成

また、このポリシーは、全員に読んで欲しい基本方針であるため、あまり長くなることを避け、具体的な手順は、別途「セキュリティポリシー実施手順」にまとめることとし、ポリシー策定と並行して検討を進めることとした。

そして、このポリシーに基づく具体的な事項について企画・立案・実施・管理・評価・継続的検討を行なうための情報セキュリティ組織の構成を検討した。

2004年6月:

情報セキュリティポリシーの素案を作成し、必要な予算と手間の増大について、学内に説明に行ったところ、予想通り多くの反対意見がでた。ところが、6月下旬に起きたある事件で事態は急変し、全学を挙げて情報セキュリティを見直すこととなる。

2004年7月:

この月には、セキュリティポリシー実施に必要な多くの手続きをおこなった。これでやっと本学も、セキュリティポリシーについての体裁だけは整えたこととなった。

- ・ 「お茶の水女子大学情報セキュリティポリシー」を策定し、学内に公布した。
- ・ 「情報セキュリティ委員会」を発足した。
- ・ セキュリティポリシーに基づき「最高情報セキュリティ責任者」を任命した。
- ・ 「システム管理部会」を設置した。

3. セキュリティポリシー施行後

施行されたセキュリティポリシーを実現するため、緊急の課題であった「物理的セキュリティ」と「ネットワークセキュリティ」の対策を講じた。内容の性質上、ここには記さずに分科会の席上で紹介したい。

4. 現在

この1年間、学内全体の協力で、セキュリティポリシーに従っていくつかの作業をおこなってきた。かかった費用も相当な額にのぼり、学内各所に要請した手間と不自由さは甚大なものである。それにもかかわらず、情報推進室で目標とした、構成員すべてに情報セキュリティへの責任意識を認識してもらうにはまだ遠いものがあると感じている。

今後は、学内の情報基盤を、情報システムの機密性・完全性・可用性、並びに安全性の観点から分析・整理した上で、全学における本ポリシーの運用実態の調査、利用者の意見の収集をおこなう必要がある。その結果や、情報セキュリティに関する動向などによって、現行のセキュリティポリシーについて評価し、必要があればこれを更新していくことになる。

参考文献

- [1] お茶の水女子大学 <http://www.ocha.ac.jp>
- [2] 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>