2004－DSM－35　(6)
2004／9／24

大学におけるセキュリティポリシー導入の一事例

鳩野逸生[1]　田村直之[1]　伴好弘[1]
{hatono, tamura ,ban}@kobe-u.ac.jp

最近のインターネットおよび高性能な情報機器の普及に伴い，情報セキュリティ・インシデントの発生件数も増加の一途をたどっている．

そのようなインシデントを起こさないためには，セキュリティポリシーの策定やそれに基づいた監査・運用体制を確立し，厳格に実行することが必要である．

本稿では，神戸大学におけるセキュリティポリシー導入を例として，大学におけるセキュリティポリシー導入上の問題点を分析し, 円滑に導入を進めるための手順について考察する．

A CASE STUDY OF INTODUCING AN INFORMATION SECURITY POLICY AT A UNIVERSITY

Itsuo Hatono[2]　Naoyuki Tamura[2]　Yoshihiro Ban[2]
{tamura,hatono,ban}@kobe-u.ac.jp

The rapid spread of the Internet and high performance computers also increases the number of security incident. In order to prevent such incident, important points are, of course, the establishment and strict enforcement of security audit/management system based on a security policy.

In this paper, first, we report a case study of introducing a security policy in authors' university. After that, we also discuss the issue of introducing that to universities.

[1]神戸大学 学術情報基盤センター
[2]Information Science and Technology Center, Kobe University

1 はじめに

最近のインターネットの高速化，情報機器の性能向上により社会のあらゆる所に計算機やネットワークが利用されるようになってきている．一方で，情報セキュリティ・インシデントの発生件数は増加の一途を辿り，しかも深刻化している．最近多発している顧客情報の漏洩事件などがその典型であると言える [1].

そのようなインシデントを防止するためには，セキュリティ・ポリシーの策定やそれに基づいた監査・運用体制を確立し，厳格に実行することが必要である [2, 3]. 平成 12 年 7 月に内閣安全保障・機器管理室/ 情報セキュリティ対策推進室では,「情報セキュリティポリシーに関するガイドラインの概要」を定め，政府関連組織へのセキュリティポリシーの策定を促している [4]. また，情報資産を適切に保護するための基準は, BS 7799, ISO 17799 などで標準化され, 認定機関による認証が行われている [5]. しかし，大学における導入の動きは鈍いのが実状である．

本稿では，著者らの大学で導入中の情報セキュリティポリシーの考え方を述べるとともに，大学におけるセキュリティポリシー導入の手順について述べる．本学におけるセキュリティポリシーは, 2004 年 10 月 1 日を持って全面実施の予定である．

2 導入の経緯

著者らは，以上の状況を受け，情報セキュリティポリシー制定の必要性を著者らの大学の総合情報処理センター広報等で訴えて来た [6]. しかし, 大学における情報センターの地位は決して高くなくセキュリティポリシー導入の動きにはつながらなかった.

その中で，2003 年 6 月に本学において休講掲示板システムのクラック事件が発生した．事件そのものはごくありふれたものであったが，サーバに全学生を含むユーザ ID と暗号化されたパスワードが格納されていたため，前ユーザのパスワードの付け替えを実施せざるを得なかった．また，踏み台にされて攻撃を仕掛けた先が外国の政府機関であったため，大きく報道されるという事態に至った [7]. これを契機に，大学の執行部より, 本学における情報セキュリティ対策を抜本的に見直せ，との指示があり, 情報セキュリティポリシー制定の着手に至った.

3 情報セキュリティポリシー導入の問題点

一般に，セキュリティポリシーの導入にあたっては，以下の手順で行われる．

(1) 策定のための組織

(2) 目的の明確化 (基本方針の策定)

(3) 守るべき情報の分類

(4) リスクの分析

(5) リスクに応じた対策基準の策定

(6) 手順・マニュアル・ガイドラインの文書化

本学における導入において，(1) に関しては，学術情報基盤センターおよび企画部情報企画課 (事務部門における情報統括部門) を中心として学内からワーキンググループを学長の私的諮問機関として編成して，原案を策定し，学長提案とすることとなった. 基本方針, 対策基準に関しては, 大学の情報セキュリティポリシーに関する研究会による雛形 [8] をベースに検討を開始した．以下の節で概要について述べる[3].

4 基本方針

基本方針は，(1) 目的, (2) 用語の定義, (3) セキュリティポリシーの体系, (4) 対象，(5) 運用体制, (6) 情報システム等の利用に際しての原則, (7) 情報システムおよびネットワーク機器管理の原則，(8) 教育・研究，(9) セキュリティ監査, (10) セキュリティポリシーの更新，(11) セキュリティポリシーの公開の各項目で本セキュリティポリシーにおける原則を述べている[4].

[3]実施前であり，公開範囲を議論していないため基本方針の公開も現時点ではできない.

[4]2004 年 10 月以降に公開予定

5　組織

本ポリシーにおいて, 実施のための組織は,「最終的な責任体制を明らかにする」という観点で構成した. 最高情報セキュリティ責任者 (学長) をおき，各部局に，部局システム管理責任者 (部局長) をおいている．その間に情報セキュリティ委員会 (部局代表による全学委員会) およびシステム管理部会 (学術情報基盤センタースタッフが担当) をおき，それぞれセキュリティポリシーの策定・更新および実施を担当することとしている.

6　情報の分類

情報の分類にあたっては，分類のための「指標」を明らかにしておく必要がある．大学の構成員のほとんどは,「教員」,「職員」,「学生」で構成される. それぞれ，大学との関わり方が異なっているため，一括して取り扱うことは効率的でないと思われる．また，大学の活動の中で組織的に取り扱う情報を，学籍情報 (学生の履修・成績情報等) とその他事務局で取り扱う情報として分類した．以下に，情報の詳細な分類について示す.

- 教員が取り扱う情報
  - 教育に関係する情報
    - 講義等における情報 (試験・成績情報を含む)
    - 教務関連情報の取り扱い
  - 研究に関係する情報
    - 知的財産に関係する情報
    - 契約等による機密情報
    - 個人情報
- 事務に係る情報
  - 「独立行政法人等の保有する情報の公開に関する法律」による開示・不開示により詳細分類
- 学籍に係る情報
  - 同上
- 学生が作成する情報

教員に関しては，定型的な仕事が少なく共通の「情報目録」を作ることは困難であると考えられるため，教員が行う「主な活動に関連した情報」として分類した.

7　対策基準の策定

7.1　対策基準の骨子

対策基準および手順を作成するあたっての方針は以下の通りである.

- 学内に存在する全ての情報機器・システム, ネットワーク機器は, 教職員によって管理されなければならない.
- 違法行為 (著作権侵害等を含む) を行わせない (行わない).
- 学外公開サーバの管理責任の明確化とインシデント発生時の緊急対応義務を明確にする.
- 学外公開サーバを許可制へ移行する.
- どの情報をどのように守るべきかを職務に即して定義し，周知徹底を計る.
- 当面は管理者，エンドユーザに過大な負担をかけないレベルに留める.

7.2　情報分類と対策基準

本稿におけるセキュリティポリシーにおいて, 対策基準を作成するにあたって，前節で分類した情報を以下に示す属性を持つかで, 対策基準で実現するセキュリティレベルを割り当てた.

- 個人情報
  - 学籍情報, 人事情報等全学レベルで集積された情報
  - 学科，研究室，特定の講義受講者単位で集積された情報
  - その他
- 業務上秘匿すべき情報
  - 試験・入試等

  - 契約による秘密情報
  - その他

- 知的財産として価値を持つ情報 (将来的に価値を持つ可能性がある情報を含む)

各情報部類における定量的なリスク分析は, 現状の大学の組織では分析に必要な情報を集めることが困難であると判断したため行わなかった. 上記の情報に属するものは, 原則として関連する第 3 者に情報を漏洩しないという観点で対策基準・手順を作成した.

7.3 サーバ管理

サーバ機器は, 以下のように分類し, それぞれ管理の手順を定めた.

対外公開サーバ: 学外への情報の提供または学外との情報の交換を行うことを目的としたサーバ

学内サービス用サーバ: 大学本部あるいは部局が, 学生または教職員に教育・研究・事務上の公式サービスを提供するためのサーバ

機密情報サーバ: 大学の運営上「機密」に属する情報や, 共同研究等で「契約により機密にすべき」情報を保持するサーバ

その他: その他, 上記の範疇に入らないサーバ.

この中で対外公開サーバに関しては, 十分な技術を持つスタッフによる運用体制を義務づけるとともに, インシデント発生時の即応体制が義務づけられる. 学内サービス洋サーバも, 学内サービスに係る重要なものに対しては対外公開サーバに準じた体制が義務づけられている.

7.4 その他

クライアント機器, ネットワーク機器, 人的セキュリティ, 技術的セキュリティに関する対策基準および手順は, 文献 [8] を参考に本学の現状に適応可能なレベルに緩和することにより作成した[5].

[5] 一部承認待ちの手順が存在する.

8 セキュリティポリシー制定の経緯

本節では, 神戸大学における情報セキュリティポリシー制定の学内手続きの手順について以下に記す.

2003 年 8 月 セキュリティポリシー策定 WG 編成

2003 年 10 月 基本方針・対策基準の原案を作成し, 部局長会議へ上程, 部局への提示, 意見収集.

2003 年 12 月 部局長会議, 評議会で情報セキュリティ委員会を先行承認. 情報セキュリティ委員会で, 基本方針・対策基準の策定作業を続行.

2004 年 2 月 情報セキュリティ委員会で基本方針・対策基準の承認.

2004 年 3 月 部局長会議・評議会で基本方針・対策基準を承認. 2003 年 4 月より発効. 2004 年 10 月までに必要な手順を整備し, 本格実施と決定.

2004 年 7 月–9 月 情報セキュリティ説明会を各部局で実施

2004 年 7 月 対外公開サーバの申請開始

2004 年 10 月 Firewall ルールへの変更の実施 (予定)

9 制定上の問題点

セキュリティポリシーの制定にあたって数多くの問題点が発生しているが, 本節では, 各大学で共通していると思われる点を列挙する.

- 事務方とのコラボレーション

  セキュリティポリシーは, 大学における正式な規定として制定される必要がある. それには, 複雑な手続きが必要である. その手続きの大部分は, 事務方のみによって行われるため, 処理を行う事務方に十分に内容を理解してもらう必要がある[6].

[6] 本学においては, 企画部情報企画課の全面的なサポートを得られた.

- 大学の活動として作成された情報の帰属

  事務職員が職務として作成する情報は，大学に帰属するものと考えてよいと思われる. この場合，大学がそれらの情報の取り扱いについてコントロールすることに関して合理性があると判断できる．しかし，教員が教育・研究活動の一環として作成する論文や講義資料等は，帰属が極めて曖昧である[7]. この場合，情報の取り扱いについて大学からの強制力はなく,「努力目標」とならざるを得ない．この点に関しては，知財関連部署との協力が不可欠である.

- 情報管理規定の不備

  大学内で取り扱う情報の機密取り扱いに関する明確な規定が存在してない．本セキュリティポリシーでは,「独立行政法人等の保有する情報の公開に関する法律」を根拠としたが，この法律は外部に対する「情報公開」を対象としたものである．情報セキュリティポリシーにおいては，学内部署間における機密取り扱いも対象とするため，根拠とするには内容が不足していると考えられる．情報セキュリティポリシー導入を契機に,「情報管理規定」導入が望まれる.

- 実施体制の不備

  今回のセキュリティポリシーの制定・実施に対し，多大の業務増が見込まれるのに対し，非常勤 1 名分のみの補充しか行われなかった.

- 利便性を落とさずに管理が不備なサーバを減少させ，セキュリティレベルをあげるためには, 代替となる情報サービスの整備が不可欠であるが，今回の実施にあたっては予算の手当がつかず，十分な整備ができなかった[8].

[7] 著作権法の職務著作という観点からすると, 教員が作成する情報のほとんどは，職務著作とは見なせないと考えられる.

[8] 1 年後のシステム更新で増強予定.

10 今後の計画

現在，ようやく実施に漕ぎ着けた段階で，これからの実施に伴って多くの問題点が発生してくるものと思われる．これに対し，実施のための人員は十分でないという大きな問題点を抱えているが，当面は可能な範囲で実施して行かざるを得ない．これと並行して,

- セキュアな情報基盤サービスの整備
- セキュリティ維持を目的とした業務見直し
- 人材育成

をなどを推進していく必要がある．しかし，これらは，今後，大学が予算上厳しい運営を迫られることは必至であることを考えると, 大学における IT 基盤整備や業務見直しの一環として行われるべきことであることは明らかであり，より全学的な取り組みが必要であると思われる.

11 終わりに

本稿では，本学が今年度導入した情報セキュリティポリシーの概要および導入経緯を述べるとともに，大学がセキュリティポリシーを導入するにあたって障害となる事項について考察した．今回本学が導入したセキュリティポリシーは，一般的に見て十分な内容を持っているとは言い難い．今後，実施状況を監視しながら，来年 4 月からの個人情報保護法への対応を行っていく予定である.

参考文献

[1] 情報処理振興事業協会 セキュリティセンター. 情報セキュリティインシデントに関わる調査 調査報告書. IPA/ISEC, 2002. (http://www.ipa.go.jp/security/fy13/report/incident_survey/incident_survey.pdf)

[2] 森・塩谷・新川, セキュリティポリシーの考え方, (株) エスシーシー, 2001.

[3] T.P. THomas(三輪監訳), セキュリティポリシーの作成と運用, ソフトバンク, 2001.

[4] 内閣安全保障・危機管理室, 情報セキュリティ対策推進室, 情報セキュリティポリシーに関するガイドライン, 2002. (http://www.kantei.go.jp/jp/it/security/)

[5] (http://www.c-cure.org/, http://www.isms.jipdec.or.jp/).

[6] 鳩野, ネットワークセキュリティに対する提言, 神戸大学総合情報処理センター広報 MAGE, Vol. 23, 2002. (http://www.istc.kobe-u.ac.jp/contents/Kouhou/mage/mage31/)

[7] 田村, 鳩野, 伴, 大学におけるインシデント対応の一事例, 情報処理学会研究報告 2003-DSM-30, Vol.2003, No.96, pp.19–24, 福井大学, 2003.

[8] 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ティーの考え方, 2001. (http://www.kudpc.kyoto-u.ac.jp/Security/toshin2001.html)