中澤ゼミ

教育機関における情報セキュリティポリシーのあり方

A1200211　小林　香織

1 はじめに

政府は2005年を目標に，e-Japan計画において高度通信情報ネットワークの安全性及び，信頼性を確保するため，2003年までに情報セキュリティポリシーの評価･見直しの実施によるセキュリティ水準の確保を挙げ，関係省庁及び民間に対して，不正アクセスやサイバーテロの予防･見知に関する技術等の実用化を計画している．これを受けて，文部科学省においても大学における不正侵入の実態を調査し，「大学における情報セキュリティポリシーの考え方」をとりまとめた[1]．このことから，教育機関でも情報セキュリティポリシーの必要性が意識され始めている．

一方，企業では1999年頃から，情報セキュリティ管理の重要性が話題となり，多くの企業がその基本となるポリシーの策定に取り組んできた．しかし，ここにきて策定したポリシーが全く機能していないケースが増加している[3]．

そこで，本研究では企業の取り組みと失敗例，先にふれた大学の情報セキュリティポリシーの考え方を活かし，小中学校などを含めた一般的な教育機関において効果的に策定･運用するための情報セキュリティポリシーのありかたを示す．

2 情報セキュリティ

2.1 情報セキュリティ対策 [2]

情報セキュリティとは，情報資産を脅威から守り，機密性[1]，完全性[2]，可用性[3]を確保することである．そのために以下の項目について対策が必要になる．

･セキュリティ組織
･リスク管理策
　･組織的対策（情報セキュリティポリシー）
　･技術的対策

組織的対策と技術的対策を併せてリスク管理と言う．組織的対策とは情報セキュリティポリシーの策定に相当する．セキュリティ対策を考えると技術的対策以上に，組織的対策の重要性が見えてくる．いかに高価なセキュリティ製品を導入しても，正しく利用しなければ意味がない．そのため，システム管理者や利用者にいかに規則を守らせるかが鍵となる．本研究では，その対応策である情報セキュリティポリシーに焦点を当て，議論を進める．

2.2 情報セキュリティポリシー

2.2.1 情報セキュリティポリシーについて

情報セキュリティポリシーとは，情報資産を守るために行う対策や，規則をまとめたものである．一般的に，情報セキュリティポリシーは3つの階層に分けられる．最も上位に位置づけられる基本ポリシーは，組織の情報に対する目的および，目的を達成するための行動方針を示す．中間層のスタンダードでは，基本ポリシーに基づいた実際に守るべき規定，最も下位にあたるプロシジャは，スタンダードに基づいた各部署単位で作成する情報セキュリティのルールである．しかし，情報セキュリティポリシーは策定しただけでは何の意味もない．であるからには全利用者に配布し，その内容を認識した上で規則を遵守してもらう必要がある．これがポリシーを運用するということであり，運用して初めてセキュリティレベルの向上を図ることが可能になる．

2.2.2 情報セキュリティポリシー策定の手順 [2][6]

情報セキュリティポリシーを策定する手順として表1のような方法がある．

(i)　組織･体制の確立

情報セキュリティポリシーの策定，実行状況のモニタリング，セキュリティの啓蒙活動，ポリシーの見直しまでを行うことのできる組織体制を整える．また，ポリシーを組織内に通達する方**法，**使用方法を決める．

(ii)　基本ポリシーの策定

一般に，基本ポリシーは組織の構成員に周知され，外部へのアピールにも用いられる．何のためにポリシーを策定するのかといった“目的”を明確に示し，簡潔にわかりやすくまとめる必要がある．

(iii)　公的ガイドラインのリストアップ

公的ガイドライン[4]に準拠してセキュリティ対策を考えることが効率的であり，効果的である．

表1. 情報セキュリティポリシー策定の手順

1	組織･体制の確立
2	基本ポリシーの策定
3	公的ガイドラインのリストアップ
4	リスクアセスメント
5	スタンダード，プロシジャの策定

[1]許可されたものだけが情報にアクセスできること．
[2]情報の整合性が取れた状態で保存されていること．
[3]必要なとき確実に情報を利用できる状態にあること．

[4] 例としては，経済産業省の”システム監査基準“，”コンピュータウイルス対策基準”，”コンピュータ不正アクセス対策基準“などである．

(vi)　リスクアセスメント

情報資産のリストアップとセキュリティに関する脅威･被害の分析を行い，個々の情報資産に関するリスクを測定する．この手順は特に労力が必要になる．十分に時間をかけて行わないと，無駄の多い管理策が生まれることになる．

(v) スタンダード，プロシジャの策定

スタンダード，プロシジャは各項目が組織内のどのグループに適用されるか具体的にわかりやすく記述する．策定案を各グループに送り，意見を収集し，その結果を反映させる．さらに，先に挙げた脅威に対する対策を選び策定していく．

2.2.3 セキュリティ対策の運用サイクル

策定した情報セキュリティポリシーを適用範囲内の対象者すべてに配布し，配布されたものを対象者が閲覧する．閲覧した内容について同意することを要求し，同意できない対象者がいるならば意見や理由を収集する．現場の意見と現在のセキュリティ状況をポリシーと照らし合わせ，内容の妥当性を判断し，必要に応じて変更を加える．さらに，変更した内容を再び対象者に配布し，同意を得る．また，運用そのものが基準を満たしているかどうか監査し，評価を行うことも重要である．さらに，同意した者は，その規則を実行することになるので，ポリシー運用開始時および定期的に必要な情報セキュリティ教育を受けなければならない．

2.3 企業におけるセキュリティ対策の問題 [3]

2.3.1 認証取得の形骸化

現在，BS7799[5]やISMS適合性評価制度[6]といった認証を取得する企業が増える中，認証取得が形骸化している．上辺だけの目的意識で認証を取得しようという考え方に原因があるが，これは認証制度全般にいわれる問題でもある．もう一つの要因としては，BS7799 やISMSを模範にしすぎ，認証制度の要求項目をまねただけの情報セキュリティポリシーを策定していることだ．BS7799 やISMS の要求する安全対策のレベルは高く，内容も多い．現場の業務実態を考慮して策定しないと，内容を詰め込みすぎ，実行できない管理策を含んだプロシジャを策定してしまう可能性が高い．現場にとって負担が重く，運用できないポリシーでは意味がない．

2.3.2 ポリシーの形骸化

策定した情報セキュリティポリシーが役に立たないという事態も起きている．その原因は，現場の業務実体からの乖離，不十分な社員教育にある．策定の際，現場の意見を収集する作業をきちんと踏まないと，社内の反感を買いやすく，ポリシーの遵守率が下がり，ポリシーが形だけの存在になる．社員のセキュリティ教育も問題だ．教材を作り，社員を集めて講習をするなど，セキュリティ教育には労力と費用を費やすことになる．これを，負担に感じポリシーの運用が疎かになっている．

2.4 教育機関におけるセキュリティ対策の問題 [5]

一般的に，教育機関では専任のネットワーク管理者がいる所は少なく，教員や事務職員が職務の片手間に管理している場合が多い．企業のように，大学でセキュリティを専攻していた者，入社してから管理者としての教育を受けた者など専門の知識を持った管理者を雇用する余裕がないため，教員･事務職員の中に知識を持った者がいない場合は苦労することになる．

教育機関の管理者は少人数で数百人のアカウントを管理しているが，これでは企業に比べて管理者の負担が大きすぎる．

次に，コンピュータ一台に対する利用状況を見ると，ほとんどの教育機関では個人専用の端末が存在しないため，どの端末からログインしても個人環境を実現しなくてはならない．それができなければ，セキュリティの管理が煩雑になり，管理者の負担が増える．

初等教育機関特有の問題としては，生徒が有害サイトへ接続を行った際，アクセスを制限･監視するフィルタリング機能が必要になる．そのほかに，企業と比べるとネットワークセキュリティへの関心が薄い．このことは，情報セキュリティポリシー策定の取り組みが，企業よりも遅れている事実からも確認できる．

表 2. 教育機関と企業の環境

	学校の場合	企業の場合
ネットワーク管理者	教員･事務職員	専門の管理者
ネットワーク管理者の人数	少数	多数
コンピュータ	不特定多数	一人一台
ホームページの利用	情報収集，情報発信	業務以外では禁止
セキュリティ意識	一般的に低い	一般的に高い

[5] セキュリティに関する国際標準ISO/IEC17799で，客観的に情報システムのセキュリティ管理に関する適合性を評価する制度．

[6] 組織の情報セキュリティマネジメントシステム(ISMS)が，国際標準規格であるISO/IEC 17799 に準拠していることを認定する，財団法人 日本情報処理開発協会(JIPDEC)の評価制度．

3 教育機関における情報セキュリティポリシー

2.3 で述べたように，内容の詰め込み過ぎ，現場の業務実態からの乖離，不十分なセキュリティ教育は情報セキュリティポリシーの形骸化を招く要因となる．ここではその対応策を述べる．

3.1 情報セキュリティポリシーの意義

日本のセキュリティ教育は米国などに比べ 10 から 15 年ほど遅れていると言われる．アメリカではセキュリティに関する一般的な教養コースは少ないが，大学院コースでは暗号，コンピュータセキュリティ，ネットワークセキュリティなどの講義が充実している．韓国では，「セキュリティ学科」が学部に誕生し，1000 名規模の卒業生を送り出している．しかし，これらは，セキュリティの専門家に対する教育である[9]．

だが，ネットワーク全体の安全性のレベルは，最も堅牢なところではなく，最も脆弱な部分で決まる．セキュリティ技術者が最新のセキュリティ対策を行い，24 時間見張ったとしても，セキュリティ意識の低い利用者が，紙に書いた自分のパスワードを落とし，悪意を持った第三者に拾われてしまえば簡単にネットワークへの侵入を許すことになる．このようなことを防ぐために，セキュリティ技術者や専門家の教育以上に一般ユーザーへの教育が必要である．2.2.3 でも述べたように，教育機関で情報セキュリティポリシーを策定・運用することはセキュリティ教育を徹底することになる．毎年多くの者が入学し，卒業する教育機関でポリシーを策定・運用することは，社会へセキュリティ教育を受けた者を数多く輩出することになる．これは企業でポリシーを策定・運用するよりも社会的使命が大きく，ネットワーク社会全体の脆弱な部分を少しずつ強化していくことになり，延いては，ネットワーク社会全体の安全性を高めることになる．加えて，これらの教育は将来の技術者養成へのステップとしても期待できる．ポリシーの策定・運用にこのような意義を持たせれば，多少労力や費用を費やすことになっても，ポリシーの運用を疎かにしてしまうことはなくなるはずだ．

3.2 策定の方法

3.2.1 策定体制

セキュリティコンサルタントにポリシーを策定してもらうのではなく，教育の現場をよく知る教員・事務職員で策定するのが望ましい．コンサルタントから押しつけられたポリシーではなく，彼らから策定・運用に関するアドバイスを受けながら実際に運用を行う教員・事務職員が策定し，自らの意思をそこに反映させることで，目標が内在化され，現場に適したより実現可能なポリシーを作ることができる．

また，ネットワーク管理者については，ユーザーにセキュリティ教育を徹底させることでネットワーク管理者の負担を軽くすることができる．新たに管理者を雇用できない場合は，教員・事務職員の中から管理者の増員をしなければならない．その場合，多少知識がなくとも担当しながら学ぶことになるだろう．

教員・事務職員だけでポリシーを策定する際，専門の知識を持った者が策定に当たるとは限らないため，関連情報を集めるのに手間がかかるなど様々な問題がある．このような場合，異なる教育機関の担当者がお互いに相談でき，情報交換の場となる電子掲示板やオンライン・コミュニティがあれば策定もスムーズになるだろう．

3.2.2 教育機関特有の問題点への対応策[6]

策定の方法は 2.2.2 に示した手順で行うが，ここではスタンダードで取るべき教育機関特有の問題点への対応策を示す．

教育機関では企業よりも構成員の入れ替わりが頻繁に起きるため，アカウント利用情報を常に最新の状態を保つように注意しなければならない．特に，入学・卒業など大規模な構成員の入れ替わりの時期や転校・転入の際，不要なアカウントを削除する．休眠アカウント[7]は，不正アクセスの糸口になりやすいことが理由である．

アクセス制限の例としては，IDとパスワード，ICカード[8]，鍵型トークン製品（USBキー[9]）による接続制限などが考えられる．覚えるのが困難で，一定期間を過ぎれば変更しなければならないパスワードは，その重要性がわからない小学生や中学生には扱いが難しい．このような場合USBキーを使うことにより問題の解決が図れる．USBキーをパソコンに差し込むだけで利用者の認証が可能なため，パスワードの扱いになれていないユーザーにもその用途と重要性を理解させやすい．

3.3 運用の方法

3.3.1 情報セキュリティ運用管理ツールの導入[6]

完成した情報セキュリティポリシー自体は文章である．これをすべての対象者に配布し，必ず読んでもらわなくてはならない．その際，管理者が少なく組織内の人数が多い教育機関では，運用の管理作業が簡単であることが求められる．このような問題を解

---

[7] 長期間利用されていないアカウント．

[8] 半導体集積回路が組み込まれており，大きなデータを記録でき，データの暗号化も可能なため偽造に強い．

[9] Universal Serial Bus周辺機器とパソコンを結ぶデータ伝送路の差し込み口に，この鍵を挿入することでパソコン，ネットワーク，ファイルへのアクセス管理を可能にする．

表3. 情報セキュリティポリシー運用管理ツールに求められる機能

1.	すべての対象者へ配布が容易である
2.	対象者ごとに内容のカスタマイズができる
3.	内容の変更に伴い差し替えが容易である
4.	最新のバージョンに保つのが容易である
5.	内容の追加, 変更時に対象者へ通知することができる
6.	ユーザーに同意させる機能がある
7.	ユーザーごとの同意状況が確認できる
8.	同意の要求に返信しない者に注意をすることができる
9.	ユーザーが不明な点を問い合わせることができる
10.	情報セキュリティに関するテストができる

消する方法に, 情報セキュリティポリシー運用管理ツールの導入があげられる. 一般にこの管理ツールには表3のような機能が望まれる.

3.3.2 セキュリティ教育

入学の時期に合わせてすぐに, 各教育機関で定められた情報セキュリティポリシーに沿ったセキュリティ教育を行わなければならない. セキュリティ教育の内容としては, セキュリティの啓蒙, セキュリティ対策の方法, 禁止行為に関する教育などを行えば, 対象者は自分が行うべきプロシジャの意味を理解できるようになり, 遵守率も上昇する. それとともに情報倫理教育やパソコン・メールの使い方など基本的なコンピュータリテラシも扱う必要がある.

教育の方法としては次のようなものが考えられる. 生徒・学生には, セキュリティ教育を各教育課程で必修として扱えば, すべての者に教育ができる上, セキュリティの授業に対して動機付けができる. 教員に対しては, セキュリティ管理責任を研究室やクラスごとに細かく分割し, 人任せではなく自分で対策を行わなければならない状況を作り出す. 教員よりもセキュリティ対策に詳しい学生を実務責任者に据え, 教員は管理責任者になるという形もあるが, 最終的な責任は教員になくてはならない. 事務職員の場合, セキュリティ管理責任を持たない者もでてくる. このような状況ではセキュリティ知識を持つ者と持たない者の間に片寄りが生じる. そのため, 部署内でセキュリティ対策委員会を作り, 組織の構成員を定期的に交代することで, 事務職員内のセキュリティレベルの底上げを計ることが可能だ. その上で, セキュリティに関する勉強会を開けば教員・事務職員へのセキュリティ教育は効果的になる.

3.3.3 評価と見直し

組織のセキュリティ責任者は, ポリシーに添った対策がどの程度遵守されているかを評価しなければならないが, 管理者の自己満足に終始し, 評価が不完全な形で終わらないように注意すべきだ. 先に述べた, オンライン・コミュニティで異なる機関の担当者同士が互いに評価しあうシステムができれば, 外部監査のような役割を果たすことができ, 自分の教育現に近い環境にある組織のポリシーと比較し検討することが可能だ.

4 おわりに

本研究では, 教育機関における情報セキュリティポリシーのあり方について, ポリシーの策定から運用に関して議論した. 教育機関特有の問題を考慮し, 情報交換やポリシーの外部監査先を探す場としての機能を持つオンライン・コミュニティ, 管理者の負担を減らすためのセキュリティ教育の徹底や USB キーによるユーザー認証, ポリシー運用管理ツールの導入などを示し, 効果的に策定・運用するためのポリシーのあり方につて明らかにした.

ポリシーを教育機関で策定・運用することは企業で行うよりも社会的使命が極めて大きい. ネットワーク社会全体の安全性を決める鍵となることから, ポリシーの策定・運用を疎かにすることはできない. まだポリシー策定の取り組みを始めていない教育機関は, 早急に取り組みを始める必要がある. しかし, ネットワークの安全性が高まるという成果は長期間ポリシーを運用してはじめて現れてくるということを念頭に置いてポリシーを運用していかなければならない. 今後の課題としては, ポリシーの策定・運用を行う組織と実際の教育機関の組織構成が異なるため, 二つの整合性を取りながらすべての教員・事務職員にポリシーの遵守やセキュリティ教育を進めていくことが重要になる.

参考文献

[1]大学における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 年 3 月

[2]塚田孝則,”企業を守るセキュリティポリシーとリスク評価”,日経 BP 社 ,2001 年 7 月

[3] 高下義弘,” 注目テーマ　情報セキュリティ管理”,NIKKEICOMPUTER,12. 30,pp. 54-57,2003 年 12 月

[4]熊谷誠治,”誰も教えてくれなかったインターネット・セキュリティのしくみ”,日経ＢＰ社

[5]田鍋潤一郎,”ネットワークポリシに基づいた校内ネットワーク構築の試み”

[6]http://www. Atmarkit.co.jp/,株式会社 @IT

[7]http://www.allied-telesis.co.jp/index.html/,アライドテレシス株式会社

[8] 原田敬,情報処理振興事業協会セキュリティセンター,”ISO/IEC 15408 とは”

[9] 佐々木良一,杉立淳,”情報セキュリティ教育の今後”