

# 学校における情報セキュリティの現状と課題

## —情報リスクの分析と実効性のあるセキュリティポリシーの検討—

鳴門教育大学 助教授 藤村 裕一

fujimura@naruto-u.ac.jp

キーワード：情報セキュリティ、セキュリティポリシー、情報リスク、情報セキュリティ教育

### 1. 学校情報セキュリティ検討委員会の目的と活動

本研究は、CECの学校情報セキュリティ検討委員会での調査・検討を中心にまとめたものである。

本委員会は、昨年度の校務情報化モデル要件調査委員会技術標準化分科会において課題として残されたことと、個人情報保護法の施行と共に高まった情報セキュリティ向上の機運を受けて、学校で情報化を推進する際の情報セキュリティの確保に関する問題について検討するために設置された。ここでは、学校現場における情報セキュリティを確保するため、国や地方公共団体、民間企業と異なる、学校の実態に合わせた情報セキュリティポリシーの策定を、中心課題とした。

これまでにも、学校現場の教員や研究者が、学校向けの情報セキュリティポリシーを策定し、普及を図ろうとしてきた。しかし、実際にはそのいずれもが普及に至っていない。そこで、本委員会では、「実効性の確保」を最大の課題として、セキュリティポリシーの策定とその普及策の検討を行った。

### 2. 学校における情報セキュリティポリシーの現状と実効性を確保するための方策

本委員会では、千葉県印西市、鹿児島県国分市、京都府京田辺市、千葉県立学校、福島県立学校・教育機関、前橋市における情報セキュリティポリシーに関して、調査・研究を行った。その結果、情報の分類と管理方法については、様々な工夫が見られると共に、教職員個人の責任については規定されているが、情報セキュリティ管理者やシステム管理者の役割・責任については規定されていないものが多いことが判明した。

また、そのような情報セキュリティポリシーの下での情報リスクの実態を、A市において調査した。(2005年、調査対象職員数=10,296人) 図1、2は、その一部である。これからも、学校における情報リスクの高さが推測される。

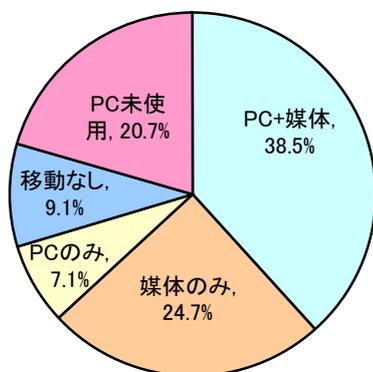


図1 記憶媒体や個人所有パソコンの学校・自宅間での持ち歩き

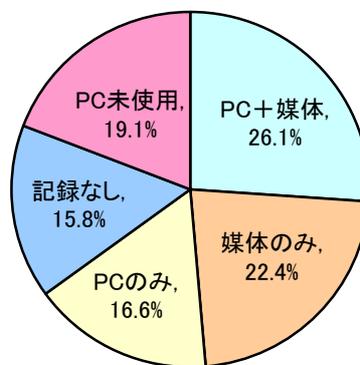


図2 記憶媒体や個人所有パソコンに、児童生徒・保護者等の個人情報記録されているか

これらの調査から、本委員会が策定を目指す学校情報セキュリティポリシーや、普及・実効性確保方策に取り入れるべきと考えた主な方策は以下の通りである。

#### (1) 管理者向けには網羅的なもの、一般教職員向けには簡潔・明瞭なもの2種類を

情報セキュリティポリシーは、情報管理責任者や管理組織に関する規定、システム管理に関する規定、一般教職員の情報管理に関する規定など、非常に範囲が広く、分量も膨大になる。当然、管理・監督責任のある教育委員会や校長・教頭などの情報管理責任者相当の者と、システム管理者は、それらの全体を熟知していなければならない。

しかしながら、一般の教職員がそのような詳細・かつ膨大な規定を受け取っても、専門用語ばかりでわからない上に、その量ゆえに読む気すら起きないことが想定される。それに対し、今回調査した中で、A3用紙1枚(A4見開き2ページ)など、一般教職員向けに、必要な情報に絞って分かりやすく提示しているところでは、比較の実効性の確保に貢献していることがわかった。そこで、本委員会でも、管理者向けの網羅的な情報セキュリティポリシーと、

その中から必要最低限の規定に絞り、簡潔・明瞭にした一般教職員向けのものの2種類を策定することとした。

## (2) 改善の最大のターゲットを一般教職員に

今回調査したいずれの情報セキュリティポリシーも、その最大のターゲットを一般教職員に据えている。その背景には、個人情報の紛失・盗難・漏洩、ウイルス感染の拡大など、事故・問題事例の多くが一般教職員によるものであり、最も情報リスクが大きいのも、一般教職員だからであるということがわかった。そこで、本委員会でも、改善の最大のターゲットを、一般教職員とすることにした。

## (3) 実効性を確保するため、教育委員会経由で、情報セキュリティポリシーのひな形と手順書を配付

これまで、多くの学校向け情報セキュリティポリシーが策定されながら、普及してこなかった背景には、情報教育担当者など、非公式で狭いチャンネルからの普及を図ってきたこともあると考えられた。そこで、本委員会では、CECから直接学校に普及を図るのではなく、教育委員会などの公的チャンネルを通し、行政の仕組みを生かして普及を図ることとした。

また、そのような普及のためのチャンネルを通しつつ、各学校で適切に情報セキュリティポリシーを策定・運用・改善を図っていくことができるようにするため、そのままだでも利用に耐えうる情報セキュリティポリシーのひな形と、一般の教職員にもよくわかるよう、各学校の実態に合わせた情報セキュリティポリシーの策定の仕方をコンパクトかつ具体的に解説した手順書(図3)を作成し、配付することとした。

**STEP 3: リスク対応策を考えましょう!**

STEP 1: 方針の策定  
STEP 2: リスク評価  
STEP 3: リスク対応策  
STEP 4: 運用  
STEP 5: 見直し

**■リスク対応策とは?**

- リスク対応策とは、リスクが顕在化した際に発生しうる被害を軽減するための対策を指します。
- リスク対応策には、日常業務で使用するハードウェアでの対応と、業務で使用するパソコンやネットワークなどの機器に導入されるソフトウェアでの対応の二つがあります。
- セキュリティポリシーの作成に取り組みされている教育委員会や学校ごとの事情も踏まえて、ソフト面とハード面の両方のリスク対応策を組み合わせたセキュリティポリシーを作成します。

**■リスク対応策の実施にはしるべがある**

- 一般的に知識を身に付ける必要があります。
- 例えば、対応策の中でソフトウェアに絡んでいると、ルールが無効になる可能性があります。ルールが有効になるように設定する必要があります。
- 具体的には教員個人が所有しているパソコンの対応ソフトウェアのインストールや設定のサポートが重要で、学校側でサポートしている必要があります。これではルールを作っても効果が期待できません。
- 現状を踏まえて、出席を取り対応策の実効性を確保する必要がある場合があります。

**■リスク対応策を個別に実施しましょう**

- 具体的なリスク対応策の実施は、まずSTEP 2で洗い出された最優先の課題(知照の必要性)から始まり、その上で最優先と見なされた各リスクに対する対応策を決定します。
- 方針は、ハード面での対応、ソフト面での対応、両者の組み合わせで初期、中期の3段階あります。
- 知照の対応策は、学校で、具体的な対応策の検討に入ります。この段階では具体的なネットワーク等の脆弱性やセキュリティポリシーの内容を踏まえながら対応策を決定します。

**「ハード面での対応」**

**「ソフト面での対応」**

**「ネットワーク面での対応」**

**「リスク対応策の実施ステップ」**

**■リスク対応策の優先度**

- STEP 2で洗い出された学校に特有のリスク順を示した「リスク対応策シート」を示した上で、以下の通り、リスクごとに対応策は優先度決定されるので、教育委員会や学校側の事情も踏まえて選択していく必要があります。
- 以下に示した対応策以外にも、各自で考えつくものをワークショップで検討してみましょう。

**「リスク対応策シート」**

リスク名(個人情報保護関連)	対応策	対応策例	採用の優先度
個人所持パソコンの盗難、紛失による漏洩	→	持ち出し禁止 (S)	1
→	持ち込みパソコンへのセキュリティ対策 (H)	→	2
→	持ち込みパソコンのウイルス対策 (S)	→	3
→	持ち込みパソコンのバックアップ (S)	→	4
→	持ち込みパソコンのパスワード設定 (S)	→	5
→	持ち込みパソコンの暗号化 (S)	→	6
→	持ち込みパソコンの物理的保護 (S)	→	7
→	持ち込みパソコンの定期的な更新 (S)	→	8
→	持ち込みパソコンの定期的なバックアップ (S)	→	9
→	持ち込みパソコンの定期的なセキュリティチェック (S)	→	10
→	持ち込みパソコンの定期的なセキュリティアップデート (S)	→	11
→	持ち込みパソコンの定期的なセキュリティパッチ適用 (S)	→	12
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断 (S)	→	13
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の対応 (S)	→	14
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の報告 (S)	→	15
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の公表 (S)	→	16
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の公表 (S)	→	17
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の公表 (S)	→	18
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の公表 (S)	→	19
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の公表 (S)	→	20

**「リスク対応策の実施ステップ」**

リスク名(個人情報保護関連)	対応策	対応策例	採用の優先度
個人所持パソコンの盗難、紛失による漏洩	→	持ち出し禁止 (S)	1
→	持ち込みパソコンへのセキュリティ対策 (H)	→	2
→	持ち込みパソコンのウイルス対策 (S)	→	3
→	持ち込みパソコンのバックアップ (S)	→	4
→	持ち込みパソコンのパスワード設定 (S)	→	5
→	持ち込みパソコンの暗号化 (S)	→	6
→	持ち込みパソコンの物理的保護 (S)	→	7
→	持ち込みパソコンの定期的な更新 (S)	→	8
→	持ち込みパソコンの定期的なバックアップ (S)	→	9
→	持ち込みパソコンの定期的なセキュリティチェック (S)	→	10
→	持ち込みパソコンの定期的なセキュリティアップデート (S)	→	11
→	持ち込みパソコンの定期的なセキュリティパッチ適用 (S)	→	12
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断 (S)	→	13
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の対応 (S)	→	14
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の報告 (S)	→	15
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の公表 (S)	→	16
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の公表 (S)	→	17
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の公表 (S)	→	18
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の公表 (S)	→	19
→	持ち込みパソコンの定期的なセキュリティ脆弱性診断結果の公表 (S)	→	20

図3 手順書『セキュリティポリシーの作成マニュアル ～明日から始められるセキュリティポリシーの作り方～』の一部

## (4) 情報セキュリティポリシーの妥当性を確保するため、JIS X5080:2002 準拠に

情報セキュリティポリシーには、実に多様なものが存在し、闇雲に条項を列挙するだけでは、妥当性を確保することは困難である。そこで、企業向けに策定され、広く一般化している JIS X5080:2002 に準拠し、学校現場の組織・実態に合わせて主語と目的語を改訂する作業を行うこととした。ただし、JIS X5080 は、今後改訂される見込みであり、公表された後は、さらにその改訂内容を反映させる予定である。

## (5) ハードウェア等による情報セキュリティの必然的確保策の紹介

企業と異なり、ITや法令の専門家が存在することが少ない学校現場では、一般教職員に難しい専門用語を説明して理解させたり、職務命令等によって遵守を強制したりすることは大変困難である。そこで、昨年度の校務IT化モデル要件調査委員会技術標準化分科会でも推奨したサーバのみにデータを保存し、ローカルには保存を不可能とするシステムと、ハードウェア認証とソフトウェア認証の組み合わせることなど、ハード面での情報セキュリティ対策も紹介することとした。これにより、今後、一般教職員が特に意識することなく、情報セキュリティを強化されることが期待される。しかしながら、この実現のためには、一定の予算が必要となるため、ハード面での対策を標準・前提とするのではなく、手順書の中で紹介するにとどめた。

## 3. 実証実験を通じた改善へ向け

今年度は、情報セキュリティポリシーのひな形と手順書の第1版を作成することで終了する。

しかし、今回作成した手順書が、果たして各学校での情報セキュリティポリシー策定を推進する支援となりうるか、また、ひな形が学校の実態に適合し、実効性を発揮できるものであるかを検証することが必要である。

そこで、平成18年度に、今回作成したひな形と手順書を、複数の実証実験地域(教育委員会単位を想定)において、1年間運用し、その効果と改善すべき点を明らかにして、第2版を策定していくことを計画している。第2版においては、改訂版のひな形を手順書に組み込み、『学校情報セキュリティ策定の手引き』(仮称)を作成して行きたいと考えている。また、この冊子を、教育委員会向けの「普及戦略ガイド」と共に、全国の教育委員会を通して配付していくことを、現在検討しているところである。

本委員会の活動を通して、JIS X5080:2002のような、学校現場において標準となる情報セキュリティポリシーの指針を示すことができれば幸いである。

参考文献: JIS X5080:2002 情報技術—情報セキュリティマネジメントの実践のための規範(2002)、日本規格協会