校務の情報化と学校情報セキュリティポリシー

－　校務情報化の運用基盤としての情報セキュリティ　－

三木市立教育センター　所長　梶本　佳照
me730457@ns.miki.ed.jp

キーワード：情報セキュリティ，安全保障，情報漏えい，校務の情報化，情報セキュリティポリシー

１．はじめに

情報セキュリティとは，どういう意味なのか。セキュリティとは，「安全」，「安心」，「安全保障」の意味があり，「情報セキュリティ」の分野では，それを「セキュリティ」と言っている。すなわち，情報セキュリティとは情報資産を安全に守るという意味である。情報資産には，デジタルデータやアナログデータを問わず会議の記録，児童生徒の住所や氏名，成績，健康調査結果，教職員の住所，サーバの設定資料といった有形のものと職員の会話の内容といった無形のものがある。

ＯＥＣＤが 1992 年に発表した情報セキュリティに関するガイドラインにおいて「情報セキュリティの目的は，情報システムに依存するものを，可用性(Availability)，機密性(Confidentiality)，完全性(Integrity)の欠如に起因する危害から保護すること」であると定義されている（表 1)。この機密性，完全性，可用性は情報セキュリティの３要素と呼ばれ，情報セキュリティを考える上での重要な概念になっている。言い換えると「情報を安全に守る」ということは，「情報の漏えい」「情報の改ざん」「情報の破壊・消失」から守ることと考えるとわかりやすい。

国の施策としても情報セキュリティ対策に力をいれており，「ＩＴ新改革戦略」（2006/1/19）では，「(２)安心してＩＴを使える環境の整備　５．個人の情報セキュリティリテラシー向上のための，初等中等教育からの情報セキュリティ教育を推進する。」と述べられている。

表１　情報セキュリティの３要素（情報セキュリティハンドブックより）

機密性：	情報へのアクセスを許可された人だけが情報を使うことができるようにすること。たとえば，機密情報はその情報を見る権限のある人しか見ることができないようにすることである。
完全性：	情報および情報の処理方法が正確であり，完全であるようにすること。情報が完全であるとは，たとえば情報が改ざんされたり，情報システムが勝手に変更されないようにすることであり，情報の正確さとは，たとえば誤って削除されたり変更されるようなことがないようにすることである。
可用性：	情報へのアクセスを許可された利用者が，必要なときはいつでも情報や情報システムにアクセスできるようにすることであり，たとえば，自然災害やシステムダウンにより，情報が使えなくなることを防ぐことである。

２．校務情報化と情報漏えい

「校務の情報化」とは，学校内の文書や子どもに関する情報がデジタルデータ化され，コンピュータやネットワークを活用して処理したりやり取りしたりして職員間で相互に共有できるとともに再利用できる状態である。さらに情報のやり取りは一つの学校内にとどまらず，ネットワークを通じて教育委員会及び各学校間でも行われ，お互いが連携している状態である(図１)。

このように単にコンピュータを使って文書を作成したり，統計処理を行ったりしている状態に比べて格段にデジタルデータとして扱う種類やネットワークを介した情報のやり取りも増える。その中には，外部に漏れてはいけない児童生徒や教職員の個人情報が多く含まれている。

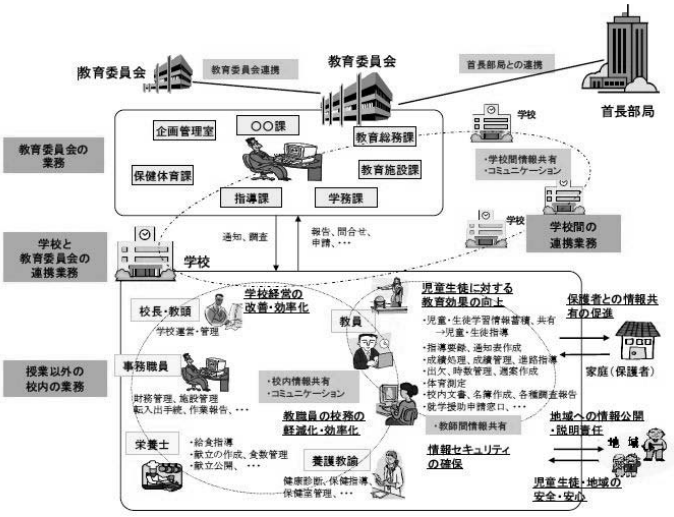

図１　校務情報化のあるべき姿（校務情報化の現状と今後の在り方に関する研究報告書より：JAPET）

紙媒体からの情報漏えいについても，どの職場でもメモ用紙がよく使われるが，学校では一度印刷された紙の裏を再利用されることがよくある。図２は市内の学校へのアンケート調査結果である。メモ用紙の表に書かれた内容は，情報資産として認識されているかもしれないが，メモ用紙の裏に個人情報が残っていたらどうなるのであろうか。一度学校内で再確認することも必要である。

３．情報漏えい対策の手順

３．１ 情報を守るための整理項目

情報を守るには,次の項目を整理して考えていく必要がある。

・何から何を守るか　・どのようにして守るか

・誰が行うのか　・使えるリソース（人，物，金）はどの程度あるのか。

３．２ 情報資産の洗い出しとリスク対応

「何から何を守るか」の「何を守る」については,「情報資産の洗い出し」が必要になってくる。このことにより，守るべき情報資産には，どういうものがあるのか具体的に整理することができる。

その次に,「何から」をはっきりさせるために，それぞれの情報資産について，盗難や紛失，破損，流出など，どのような脅威があるかを考え，その大きさと脆弱性を評価する（表２，３）。これらをもとにその情報資産のリスクを評価していく。リスク評価の仕方には，次のような式を使うこともできる。

リスク評価＝情報資産の重要度×脅威の評価×脆弱性の評価

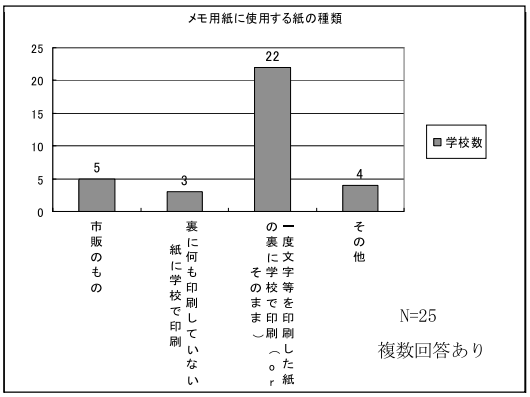

図２ メモ用紙に使用する紙の種類

リスク評価を明確にした後に，そのリスクへの対処法を考え実施していくとよい（表４）。この対処法が学校情報セキュリティポリシーの実施手順の原案になっていく。

表２　学校内の守るべき資産リストと脅威　一部

(文　書	保存年限	重要度	守るべき情報資産	情報セキュリティ脅威例					脅威
指導要録（学籍）	２０	大	○	11	12				中
除籍簿（学籍）	２０	大	○	11	12				小
学級編制関係	１	小							
園児・児童・生徒名簿	５	大	○	2	4	6			中
入学・卒業児童・生徒報告書	１	大	○	2	4	6			小

表３　脅威の具体的内容　一部

個人情報漏洩関連の脅威	
1	個人所有パソコンの盗難，紛失による漏洩
2	USBメモリ等のメディア及び書類等の盗難、紛失での個人情報漏洩
3	学校ホームページの個人情報掲載による漏洩
4	メール誤送信による漏洩
5	学校内パソコンのウイルスやスパイウェア感染による漏洩
6	情報機器処分時のデータ消し忘れによる漏洩

表４　リスクへの対応策　一部

リスク	対応策
USBメモリの盗難・紛失による情報漏えい	ファイルへのパスワード設定や暗号化 USBへの認証化
サーバのハードディスクトラブルによる情報消失	バックアップの実施

４．学校情報セキュリティポリシー策定における留意点

４．１ 学校情報セキュリティポリシーは，市内の学校全体で共通になっているか。

市内の学校ごとに考え方が違う状態であると情報セキュリティの実現が難しくなる。基本方針，対策基準の作成においては，教育委員会が主導して，学校情報セキュリティポリシーの意味と内容を研修しながら同一のものを策定することが良い。実施手順も各学校で行われている業務内容はほぼ同じなので,数校の推進校と教育委員会で実施手順のひな形を作成しそれをもとに各学校で部分修正を加えるのが現実的である。

４．２ ひな形や他の市のコピーをそのまま使うのではなく,意味を理解しているか，学校の実情に合っているか。

ひな形を使うことが悪いのではなくその意味を理解することなく使うことが問題なのである。また，学校の実情に合わない部分は修正して使うことも大切である。しかし,修正する場合，守りにくいからという理由で安易に情報セキュリティのレベルが下がることがないように特に注意しなければならない。

４．３ 学校長のリーダーシップのもと学校全体として学校情報セキュリティ策定の意味を理解しているか。

学校長の積極的な関与とリーダーシップは，学校情報セキュリティ対策を実施していく上で重要な要素である。情報セキュリティの維持のためには職員全員が約束を守っていくことが必要である。そのためには学校長が「情報の漏えい」「情報の改ざん」「情報の破壊・消失」は学校経営上,重要な損失になることを理解しリーダーシップを発揮していく必要がある。

【参考文献】

（１）独立行政法人情報処理推進機構，情報セキュリティ教本，実教出版，2007 年 4 月

（２）学校情報セキュリティハンドブック，財団法人コンピュータ教育開発センター，2007 年 3 月