

情報セキュリティと校務情報化

－ 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、情報漏えい、校務情報化、情報セキュリティポリシー

1. はじめに

校務情報化が一人一台 PC の普及にあわせて進みつつある。校務情報化は、児童生徒情報も含めて校務情報をデジタルデータとしてコンピュータ及びネットワークを活用し、処理したり取り出したりするものである。このことにより、校務の負担軽減を図るとともに教育の質を高めることを目標としている。

デジタルデータは、紙などに記録されたアナログデータと比べて遥かに大量のデータをコンパクトに持ち運びできるとともにネットワークを通じて簡単に送信することができる。また、データがデジタルファイルになっていると加工、処理が行い易い。

反面これらのことは、「情報の漏えい」「情報の改ざん」「情報の破壊」が起りやすくなりデータの取扱いに注意が必要なことにもつながる。そして、それから守ることが重要になってくる。紙に印刷された状態であれば情報が見える形になっているのであるが、デジタルデータになると情報が見えない形になってしまう。このため従来とは違った対策が新たに必要になってくる。

これらのことから校務情報化を進めるにあたっては、情報セキュリティへの対応が欠かせないものになってくる。次に、三木市における情報セキュリティへの取り組みを紹介する。

2. 情報セキュリティの考え方

情報セキュリティとは、「情報の機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)を維持すること」(図1)と定義され、この3つの要素がバランスよく保たれていることが望まれている。

そして、使い勝手を追求すると情報資産が漏れていくことにつながり、厳しすぎるルールを作成するとそれは守れないルールになり実行性が乏しくなる(図2)。

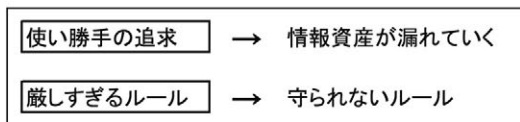


図2 情報セキュリティのバランス

機密性	許可されない利用者が、情報にアクセスできないようにすることで、情報を守ること。
完全性	組織内で処理されたデータが正しいこと、ネットワーク上で第三者によって改ざんされることなく確実に相手に送信されることなどを保証すること。
可用性	許可された利用者が確実に情報にアクセスできるようにすること。停電やサーバなどのハードウェアの故障で必要な情報にアクセスできなかったり、極度の処理の集中による負荷で、著しく応答が遅れたりしないようにすること。

図1 情報セキュリティの目的

3. 情報漏えいの原因及び経路

3.1 情報漏えいの原因

情報漏えい対策を行うためには、その原因を調べることが大切である。原因を間違えると情報漏えい対策は、効果をなさなくなる。日本ネットワークセキュリティ協会「2006年情報セキュリティインシデントに関する調査報告書」(図2)によると「紛失・置忘れ」の29.2%を始めとして「盗難」、「誤操作」、「管理ミス」、「不正情報持ち出し」、「内部犯罪・内部不正行為」、「設定ミス」、「目的外使用」といった内部の人的原因の合計が83.8%を占めている。一方、「ワーム・ウイルス」、「不正アクセス」、「バグ・セキュリティホール」といった外部からの原因は、13.3%である。

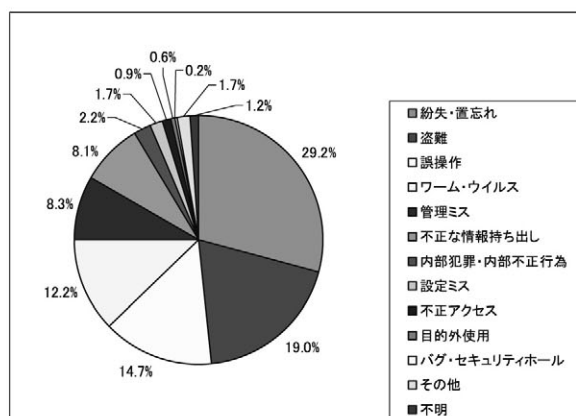


図2 情報漏えい原因比率【件数】

3.2 情報漏えいの経路

同じく報告書から情報漏えいの経路を調べてみると「紙媒体」が43.7%であり情報漏えいの半数近くが紙の印刷物からであることがわかる(図3)。次に「Web・Net」が22.0%、「PC本体」が10.7%と続いている。

