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、処理したりやり取り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にしている。

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」が起こ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）。

機密性	許可されない利用者が，情報にアクセル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

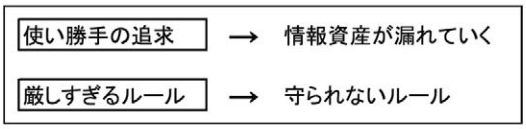

図２　情報セキュリティのバランス

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。原因を間違う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。

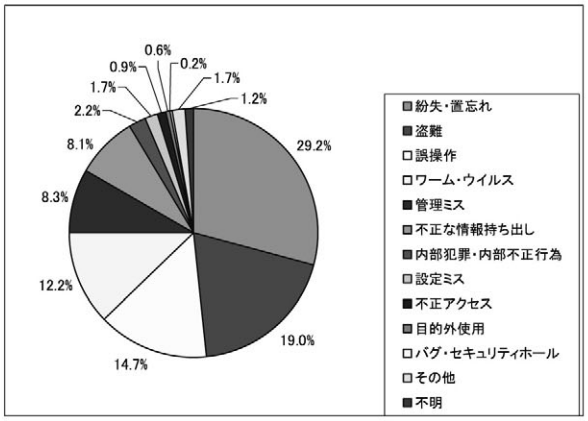

図２　情報漏えい原因比率【件数】

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。

３．３ 情報漏えい防止に向けて

「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」から情報漏えいを防ぐためには、デジタルデータのみならず紙からの情報流出への対策も考えておく必要があることがわかる。また、情報流出の大きな原因は、人であるため人的ミスを防ぐ対策を考えていく必要がある。

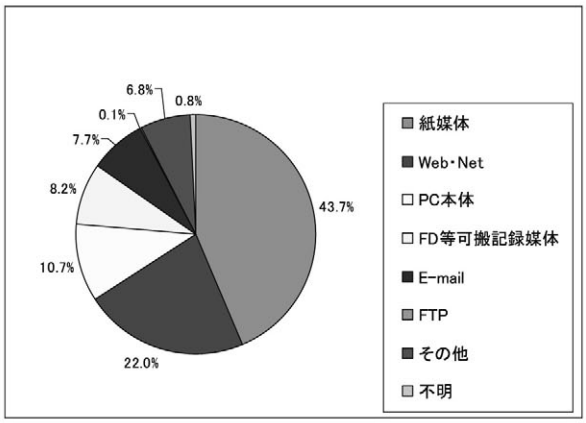

図３ 情報漏えい経路（媒体）比率【件数】

４．情報セキュリティ意識の向上に向けて

４．１ 人の意識面から

（１）職員全員のセキュリティ意識の底上げを行う。

全職員の意識がある程度高まっていないと、セキュリティへの取り組みが進まないので情報モラル（情報倫理・法への理解＋情報安全・情報セキュリティ）研修会を全職員対象に実施した。

（２）研修の内容

実際の「車上荒しによるデータFD盗難事例」をもとに「自分ならどうするか」、「問題だと思う点は何か」ということをワークシートに書くことから研修を始めた。このことにより、情報漏えい事例を自分のこととして考えることができた（図４、５）。

４．２ システム面から

（１）ログオン時にラストユーザネームを非表示

Windows ログオンは、USB のセキュリティＫｅｙに加えてユーザ名＋パスワードによる認証を用いるようにした(図６)。

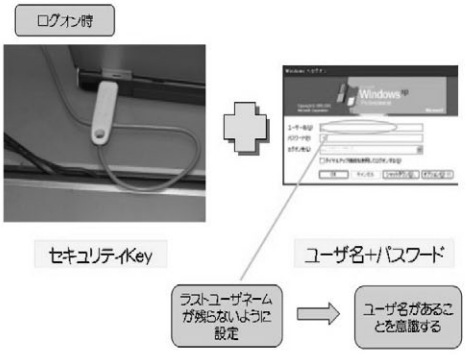

図６ ログオン時の工夫

Q 問題だと思う点を2つ以上書いてください N=138 上位10	人	%
校外に持ち出した	104	75.4%
車外から見える位置に荷物を置いていた	91	65.9%
個人情報管理の意識の低さ	35	25.4%
必要のない年度のデータを持ち出した	26	18.8%
荷物を残して車を離れた	25	18.1%
直帰しなかった	17	12.3%
盗難に気付くのが遅かった	12	8.7%
個人情報をFDに入れていた(コピーされ易い・持ち出し可能)	9	6.5%
FDのデータを保護していなかった	7	5.1%
前年度のデータを削除していなかった	6	4.3%

図４ 問題だと思う点（重複回答有）

Q 自分ならどうしますか? N=138 上位10	人	%
校外に持ち出さない	76	55.1%
持ち出した場合は、常に身に付ける・目の届くところに置く	55	39.9%
持ち帰る場合は直帰する	31	22.5%
荷物を車外から見える位置に放置しない	26	18.8%
不必要になった情報(前年度分等)は削除する	20	14.5%
荷物を残して車から離れない	14	10.1%
データファイル・フォルダにロックをかける	12	8.7%
持ち出した場合は、厳重に管理する(金庫等に保管)	12	8.7%
持ち出しできないところ(施錠できるところ等)に保管する	9	6.5%
FDやCD-R等のメディアに保存しない	8	5.8%

図５ 自分ならどうするか（重複回答有）

（２）ログオンしているユーザ名を表示

ログオンしている状態で、ログオンしているユーザ名をコンピュータの画面上に表示するようにした(図７)。これは、導入しているシステムの機能を利用して表示させた。職員に対するアンケート調査の結果、６４％(N=44)が役立っていると答えた。その理由を考察すると、ユーザ名の表示により「誰が使っているのかわかる。自分が使っているのが確認できる。責任を持って仕事ができる。」というようにコンピュータを使っていることに対して自覚が生まれるようである。

図７ ユーザ名の表示

５．まとめと課題

校務情報化のためには、情報セキュリティへの対策が重要でありそれには、意識面とシステム面の両面が大切である。そして、これらは別々のものではなくシステムを使っていくにつれて意識面も高まるように両方が補完しあうように工夫することが大切である。さらに、情報セキュリティポリシーを作成し、組織として統一的に情報セキュリティを実現することが望まれる。

参考資料：情報セキュリティ読本 改定版（独立行政法人 情報処理推進機構） 実教出版, 2007
よくわかる事例で学ぶ情報セキュリティ FOM出版, 2006