http://www.edu.pref.kagoshima.jp/　　（通巻第１７３５号）

指導資料

鹿児島県総合教育センター

情報教育 第124号

― 小，中，高，特別支援学校対象 ―
平成 24 年４月発行

一人一人の意識を高める情報セキュリティ対策の改善

学校では，児童生徒や保護者に関する多くの個人情報を取り扱っており，漏えいや紛失等があった場合の社会的影響は大きい。一たび個人情報の漏えいや紛失が起きると，学校の信頼を失うばかりか，悪用されたり，児童生徒や保護者に対して精神的苦痛を与えたりするなど，深刻な問題となることから，多くの個人情報を扱う教職員には，個人情報保護に対する高い意識が求められる。そこで本稿では，一人一人の教職員の意識を高めるための情報セキュリティ対策について述べる。

１　情報漏えいの主な原因

独立行政法人情報処理推進機構(IPA)は，平成22年１月～12月に公表された国内の情報漏えい事故の分析結果から，情報セキュリティに関する脅威として，「『人』が起こしてしまう情報漏えい」を第１位に挙げている（**表１**）。

表１　情報セキュリティに関する脅威

順位	脅　　威
第１位	「人」が起こしてしまう情報漏えい
第２位	ウェブサイトを経由した攻撃
第３位	定番ソフトウェアの脆弱性をねらった攻撃

（IPA「2011 年度版 10 大脅威」から）

また，教育ネットワーク情報セキュリティ推進委員会（ISEN）が公表している「平成22年度学校・教育機関の個人情報漏えい事故の発生状況・教員の意識に関する調査」によると，学校等における情報漏えいの原因は，車上荒らしや学校侵入などによる「盗難」，校内での取扱いが不適切で紛失や行方不明となる「管理ミス」，ルールを逸脱した「不正な情報持ち出し」，持ち出し許可を得た情報の「紛失・置き忘れ」の順となっており，管理上の問題や人為的ミスが全体の約９割を占めている（**図１**）。

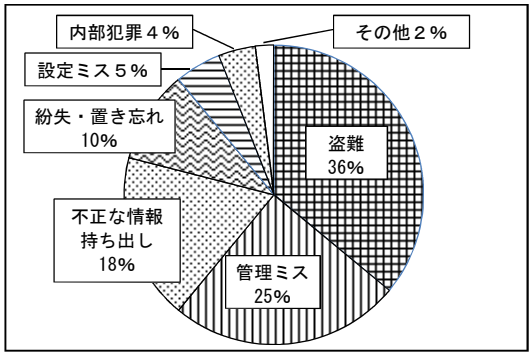

図１　個人情報漏えい事故の原因

情報セキュリティ対策は，技術的な仕組みの整備はもちろんであるが，利用者の守る意識がなければ成り立たない。そのためには，実効性のあるルールの策定とその共通理解を図り，一人一人の教職員が高い意識をもって取り組むことが重要である。

２　個人情報に対する基本的な考え方

一人一人の児童生徒にきめ細かな指導を行うためは,個人情報を収集するとともに,それらを教職員間で共有する必要がある。

しかし，児童生徒の個人情報は，児童生徒や保護者から預かっているものであり，安易に利用することは許されない。

そこで，個人情報を取り扱う際は，常に次のことを念頭におくべきである。

- 個人情報は，学校や教職員のものではなく，児童生徒や保護者のものであること。
- 個人情報は，児童生徒個人の人格尊重の基に，慎重かつ適正に取り扱わなければならないこと。
- 個人情報を取り扱う際は，関係法令や守秘義務に反しないこと。
- 個人情報を収集する際は，その範囲と利用目的，保有期間を明確にすること。
- 個々のデータでは個人を特定できない情報でも，他と照合することで個人の識別が可能であれば，個人情報として取り扱う必要があること。

３　情報セキュリティポリシー運用サイクルの確立

平成17年に「個人情報の保護に関する法律」（いわゆる個人情報保護法）が全面施行されてから約７年が経過した。

各学校では，教育委員会等が示した情報セキュリティポリシーに基づき，情報資産の適正な取扱いについて，実効性のある規定を定めなければならない。

その際，セキュリティを重視した厳格な規定を定めることは重要であるが，規定が厳し過ぎて利用者の過剰な負担となり利便性を著しく損なうと，規定が守られずに，逆にリスクを増大させることになる（**図２**）。

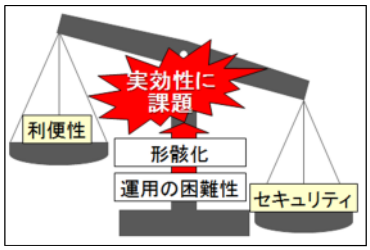

図２　利便性とセキュリティのバランス

したがって，規定を策定する際は，リスクを軽減させるだけでなく，利便性をある程度確保することも必要である。

例えば，規定が守られず，情報資産の持ち出しが日常的に行われることが多くの事故の原因となっていることから，持ち出しの原則禁止を徹底すると同時に，やむを得ず持ち出す場合の手順や，情報漏えいを防ぐための対策を明記することも大切である。

情報セキュリティ対策の実効性を高め，一人一人の教職員が共通理解して実践するためには，**図３**に示すように，情報セキュリティポリシー運用サイクルを確立することが大切である。

つまり，常に規定の運用状況を把握し，セキュリティと利便性を自校の状況に見合ったバランスになるよう，定期的な評価・見直しを行い，実効性のあるルールを策定した上で，ルールを守ることの必要性を利用者に認識させることが重要である。

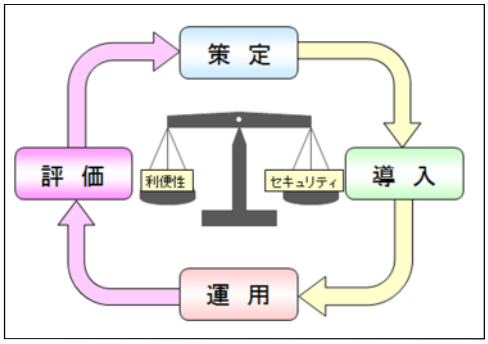

図３　情報セキュリティポリシー運用サイクル

４　情報セキュリティ対策改善のための留意点

現在では，学校の情報資産の多くが電子化されており，それらの情報は複製が容易で，漏えいや紛失の原因となりやすい。また，流出した場合の回収が困難となり，被害も大きくなるため，より一層の注意が必要となる。

そこで，紙媒体の情報資産も含め，各学校の情報セキュリティ対策を次の点に留意して改善していく必要がある。

(1)　情報資産の洗い出しと重要度による分類

学校内で保有している情報資産について，紙媒体及び電子データ等の管理表を作成し，保管場所や保存期間，担当係等を明記する。さらに，その情報資産が外部に漏えいした場合や消失した場合の影響も考慮し，重要度を**表２**のように３段階程度に分類して取扱いの規定を定める。

管理表及び取扱いの規定は，定期的に見直し，更新するとともに，全教職員への周知を図る。

表２　重要度による分類例

分類	分類基準
重要度Ａ（高）	機密文書に相当し，持ち出しを禁止する情報資産
重要度Ｂ（中）	機密文書に相当し，校長の許可により一定期間に限って持ち出しを可能とする情報資産
重要度Ｃ（低）	重要度Ａ及びＢには相当しないが，一般に公開することを前提としない情報資産

(2)　重要度に応じた取扱いの明確化

重要度Ａ及びＢに分類した情報資産の取扱いについては，次のような内容を定める。

- アクセス制限を設定した共有フォルダ等に保存する。
- 分類が分かるようにファイル名を付ける。
- 紙媒体の情報は，保管用金庫や鍵のかかる書庫等で保管する。
- 電子データは，パスワード設定や暗号化を行う。
- 保存期間を過ぎたデータは確実に破棄又は消去する。
- 複製や持ち出しを禁止する。
- やむを得ず持ち出す場合の例外規定を定め，持ち出す際の手続きや方法等について明記する。

(3)　情報資産の持ち出しに関する例外規定の明確化

重要な情報資産については，持ち出し禁止を徹底することが原則であるが，教職員は時期によって持ち出しを必要とする場合もある。

規定の不備や形骸化により，情報資産が持ち出された際に多くの事故が起きていることから，例外規定として，持ち出す際の手続きや方法を定めておき，確実に遵守させることが必要である。

特に，万一盗難や紛失等の事故が起きた場合に，情報漏えいを防ぐためには，電子データにパスワードや暗号化を施すことが重要である（**図４**）。その方法については，一人一人が確実にできるように操作手順書を作成するとともに，実際に操作を行う職員研修も必要となる。

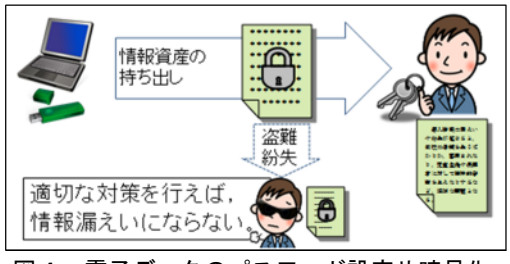

図４　電子データのパスワード設定や暗号化の重要性

５　情報資産の管理に関する規定例

各県立学校の情報セキュリティポリシーを参考に，見直したい主な既定の一例を示す。

各学校では，自校の環境に合わせて情報セキュリティポリシーを改善するとともに，誰が，何を，どのようにするのかを具体的に示した実施手順書を作成することが重要である。

(1)　情報資産の分類及び取扱いに関する規定例

○　情報資産の分類と取扱い

本校における情報資産を，個人情報保護の観点から次のように分類して取り扱う。

分類	分類基準	情報資産例	取扱制限
A	児童（生徒）の個人情報を含み，特に機密性が高い情報資産	・指導要録 ・転出入関係書類 ・入学者選抜に関する表簿 ・健康診断票 ・学習成績一覧表 ・生徒指導の記録	・持ち出し禁止 ・指定された保管場所での保管及び利用 ・紙媒体の施錠管理，電子情報のパスワードロック又は暗号化の設定
B	児童（生徒）の個人情報を含む，校長の許可により一定期間に限って持ち出しを可能とする情報資産	・定期考査結果 ・生活環境調査票 ・保健調査票	・原則持ち出し禁止 ・持ち出す場合の「情報資産の持ち出しに関する例外規定」の遵守
C	分類Ａ及びＢには相当しないが，一般に公開することを前提としていない情報資産	・緊急連絡網 ・学級通信，学校便り	・必要最小限の持ち出し可

(2)　電子情報の管理に関する規定例

○　電子情報の保存

- 校務データは「情報システム利用に関する実施手順書」に従い，アクセス権の施された共有フォルダに保存すること。
- 分類Ａ及びＢの電子情報については，他者が読み取ることができないよう「電子情報のパスワード・暗号化設定手順書」で示す方法に従い，暗号化すること。
- 分類Ａ及びＢの校務データは，原則として端末パソコンやＵＳＢメモリ等に複製してはならない。分類Ｂの校務データを持ち出す場合は「情報資産の持ち出しに関する例外規定」に従うこと。

(3)　情報資産の持ち出しに関する例外規定例

【例外規定】

業務の都合上，やむを得ず情報資産を外部に持ち出す場合は，以下のことを守ること。

- 「情報資産校外持出許可願」により，学校長の許可を得る。
- 「情報資産持ち出し記録簿」に持ち出す情報資産名，持ち出し日，返却日等を記入する。
- 保管ボックスにある所定のパソコン又はＵＳＢメモリを利用する。
- 複製するデータは必要最小限のものとする。
- 分類Ａ及びＢの情報資産については「電子情報のパスワード・暗号化設定手順書」に従い，パスワード設定又は暗号化を施す。
- 運搬時は盗難や置き忘れに十分注意する。
- 使用後は複製したデータを確実に消去し，速やかに返却する。

ＩＣＴに係る技術は日々進展しているが，環境がどんなに変化しても，それを使う教職員一人一人の個人情報保護に対する意識が最も重要であることは変わらない。

全教職員が情報セキュリティの重要性を理解し，確実に取り組むためには，学校の経営目標の中に情報セキュリティへの取組を位置付けることも必要である。

当教育センターWebサイトで情報セキュリティに関する情報提供を行っているので，参考にしていただきたい。

－参考文献－

○　『学校情報セキュリティハンドブック』
平成19年　コンピュータ教育開発センター
○　村上今雄，野間俊彦著『学校の情報セキュリティ』　平成16年　ぎょうせい

（情報教育研修課）