# 情報セキュリティ対策

## 要　点

　教職員が「車上荒らし」に遭い、個人用パソコンや、児童生徒の成績資料が記録されているにもかかわらず、パスワード設定等の保護対策が講じられていない記憶媒体などを亡失する事故等が、報道されることがあります。
　そうした事故を防ぐために、個人情報管理の重要性を認識して、次のような個人情報保護・管理対策の点検と徹底が必要となります。

（１）日頃から、文書、パソコンあるいは電子データ等に記載・記録されている内容が個人情報に当たらないか、常に意識して取り扱うこと。
（２）原則として、個人情報はパソコン内のハードディスクには保存せず、記憶媒体（ＵＳＢフラッシュメモリー等）に保存して厳重に管理すること。
（３）保有する必要がなくなった個人情報については、確実に、かつ、速やかに廃棄し、または消去すること。
（４）個人情報が記録されている文書やデータ等、特に児童生徒の成績に関する資料は校外に持ち出さないこと。
（５）やむを得ず個人情報が記録されている文書やデータ等を校外に持ち出す場合は必要最小限にとどめ、肌身離さず、寄り道などせず、たとえ短時間であっても絶対に自動車内等に放置しないこと。車の施錠を過信せず、トランクなど目の届かない場所に置いておいても決して安全ではないことを理解すること。

## 知っておくべき内容

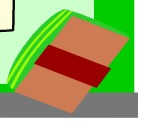
（１）「ファイル交換ソフト」がインストールされているパソコンは、業務には使用しないこと。
　※　ファイル交換ソフトがインストールされているパソコンは、外部記憶媒体にのみデータを保存している場合や作業中にケーブルをはずしている場合でもデータが流出する危険がある。
（２）インターネットに接続する個人のパソコンをやむを得ず業務に使用する場合、個人情報はパソコンのハードディスクには保存しないとともに、ウィルス対策ソフトのパターンファイルを常に最新の状態に保っておくこと。
（３）パソコン起動時や記憶媒体ごと、あるいはファイルごとのセキュリティ対策（パスワード設定、情報の暗号化、指紋認証システムの利用等）を必ず実行し、万が一、亡失しても第三者が容易にその内容を知りえない措置を講じておくこと。

## 教職員に求められること

「車上荒らし」により個人情報の流失等の事故は、教育への信頼を著しく損ねることとなります。各学校においても、「車上荒らし」やインターネットを通じての「情報流出」あるいは「校内への侵入・盗難」など、様々な事態を想定して対策を講じておくことが必要です。

### 関係法令等

１　個人情報保護法



## 個人情報の持ち出し等による漏えい等の防止について（対策例）

### 1　個人情報等の持ち出しについて

(1) 学校から個人情報等を持ち出す場合には、情報管理者の許可を得るなどのルールを明確化し、漏えい等（データの滅失、き損など）への防止対策を徹底する。
(2) 電子メールにより非公表の情報を学校外へ送信する場合も、当該情報にパスワードを設定した上で送信するなど、必要に応じて保護対策を行う。
(3) 個人情報の持ち出しによる漏えい事案では教職員の認識不足によって発生する例が多いことから、漏えいの危険性について教職員一人ひとりへ的確に周知を図るとともに、必要に応じて教育研修を実施する。
(4) 大学等の教育研究活動において、学生等が個人情報を取り扱う場合においても、教職員と同様に安全管理措置等について周知し、適正な取扱いが確保されるよう必要な措置を講ずる。

### 2　学校外で利用するパソコンのセキュリティ対策について

(1) 学校内で利用するパソコンのセキュリティ対策はもちろんのこと、学校外で業務に利用するパソコンについても、ウィルス対策ソフトがインストールされていることを確認するとともに、パターンファイルが最新の情報に更新されていることを確認する。
(2) ＯＳ等の脆弱性が改善されるよう、最新の修正プログラムを適用する。
(3) 秘密情報、個人情報等の関係者のみが閲覧すべき情報については、パスワードで保護するなど、アクセス制限の措置を行う。

**教育情報セキュリティ10か条**

「福島県教育委員会教育情報セキュリティポリシー等の施行について」（抜粋）
（平成31年3月13日付け30教総第704号教育長通知より）

ＩＣＴの活用は、日々の業務遂行に不可欠になってきていますが、誤った認識による操作により、大量の児童生徒、施設利用者の個人情報や各所属が管理する機密情報を瞬時に流出させる恐れがあり、一度流出させてしまった情報の回収は極めて困難です。

**1　適切な情報の管理（持たない、持ち込まない、持ち出さない）**
**2　私物の機器、ソフトウェアは原則禁止**
**3　パソコン・ネットワークの業務目的外使用禁止**
**4　外部記録媒体を使用する場合は適切に**
**5　離席時の画面を放置禁止**
**6　セキュリティ対策ソフトウェアは有効に**
**7　適正なパスワード管理**
**8　メールの取扱は注意（誤送信、メールからの情報漏洩、不審メール）**
**9　セキュリティ事故発生時の対応手順を確認**
**10　ソフトウェアは許可を得て取得、適切に使用**