令和５年７月

個人情報漏洩防止研修

総務部

学校における個人情報の持出し等による漏えい等の防止について（通知）　18 文科総第９号

平成 18 年４月 21 日

資料１

個人情報の持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ー対策について

（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、ウイ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。

３　ファイル交換ソフト（Winny 等）について

最近発生している情報漏えい事案では、学校外で利用したパソコンにファイル交換ソフト（Winny 等）がインストールされており、コンピューターウィルスに感染したことによりパソコンに保存されていたファイルが漏えいする例が多数発生している。

このため、学校外で利用されるパソコンにファイル交換ソフト（Winny 等）がインストールされていないことの確認を徹底する。 特に、自宅で利用する個人用のパソコンについては、以下の点に留意する。

1　ファイル交換ソフトは、安易にインストールしないこと。

2　ファイル交換ソフトの有無を点検し、これがインストールされたパソコンでは、児童生徒等の個人情報を扱わないこと。

3　当該パソコンに、児童生徒等の個人情報等が保存されているか否かを点検し、保存されている場合は、適切に削除する等の措置をとること。

4　ウィルスに感染した場合には、直ちに情報流出を遮断する措置を講ずること。