学校で扱う個人情報の性質と個人情報保護対策

日本大学法学部非常勤講師
松澤 幸太郎

１．はじめに

学校において効果的な個人情報保護への取り組みをするためには，第一に実際に学校で取り扱われている個人情報がどのようなものかを認識すること，第二に学校で生じる可能性のある事故等の傾向を理解し，それを踏まえて対策を講じること，が必要である。

この点から本稿では，学校の関係する個人情報に関する最近の報道をいくつか分析しつつ，学校における個人情報保護対策のポイントを整理する。

２．個人情報の取り扱いに関する最近の報道

	事件例
1	高校で，生徒の住所や病歴などの個人情報が記入された健康記録表と，身体測定個人記録票を紛失していることが分かった。紛失したのはいずれも学校独自の書類で，健康記録表には住所，電話番号，健康保険証番号，既往症などが記入されており，健康状況など保健調査の欄もある。身体測定個人記録票は，身長や体重，視力など5項目が記載されていた。 書類を保管する棚の鍵は同校の養護教諭だけが所有。棚が壊された形跡はなく，発見当時，鍵が開いていたという。同校は教諭が鍵をかけ忘れた可能性もあるとみている。
2	教諭の乗用車が車上荒らしの被害にあい，車内から全校生162人についての音楽，家庭科の評価などの個人情報が入ったUSBメモリが盗まれた。
3	高校の生徒2人の学習に関する記録などが，インターネットの掲示板に掲載された。同校が，掲示板の管理者に削除を求め，情報は削除された。情報の内容は，実名，学習活動を評価した「総合所見」で，1人については，５段階評価の成績が掲載されていた。 同校では，職員が使用するパソコンやフロッピーは，各個人の鍵付きの机やロッカーで保管しており，情報は校内サーバーで管理し，ID番号を知る者でなければ画面を開くことが出来ない体制を取っていた。またパソコンやフロッピーの盗難はなかった。
4	養護学校の教員が，ウイルスに感染したパソコンのファイル交換ソフト「Share（シェア）」を通じ，担任を務める小学部児童1人の個人情報の記載された資料を流出させた。資料には本人の氏名と障害名，保護者の氏名，住所，電話番号などが記されていた。
5	養護学校の教諭が車上荒らしに遭い，高等部の生徒と全職員の住所録のほか，生徒の年間指導計画書や保護者との懇談記録など個人情報の入った記憶媒体が入ったショルダーバッグが盗まれた。
6	学校教員が，同校に情報公開請求した者の個人情報が書かれた公開請求書の写しを同校の同窓会長に手渡していた。同窓会長は請求書に記載された電話番号をもとに女性に連絡し，「使用目的を明らかにしないと情報は出せない」などと告げていた。この教員は「違法とは認識していたが，請求書を直接見せたほうが請求の内容が相手に分かりやすいと思った」と釈明している。

３．学校における対策のポイント

（1）学校が取り扱う個人情報の性質の観点から

以上の事例を参考に考えると，学校が取り扱う個人情報には次のような性質があると考えられる。

① センシティブ情報である場合があること

先の事例1から4まででは，障害名，成績，健康記録等の個人情報が漏洩している。これら障害名等の情報は，一般にいわゆるセンシティブ情報とされるものであり[1]，取り扱いに特別の配慮が必要とされ，地方公共団体の条例等においては，他の個人情報とは異なる取り扱いを定めている事例もある。

我が国の個人情報保護制度のもとでは，学校

には，個人情報の保護に関する法律や行政機関の保有する個人情報の保護に関する法律等ではなく，各地方自治体の個人情報保護条例が適用される場合も多い[ii]。各学校は，自らに適用される法令等が何かを確認の上，そこにおいて，上記のような，いわゆるセンシティブ情報の扱いがどのように規定されているかを確認し，対策をとる必要がある。

② 学校であることを理由に提供されたものである場合があること

事例1から4にある障害名，成績，健康記録等，また事例5にある保護者との懇談記録は，特段の必要がなければ他人に提供する性質の情報ではない。このような情報が学校に提供されているのは，保護者等の提供者が学校を信頼している，あるいは提供しないとする選択肢が事実上存在しないからである。

他方で学校には，事例5にある住所録のような，通常の公私の諸機関において保有している情報も多くある。個人情報保護制度がある以上，これら住所録のような個人情報も適切な取り扱いが求められることはいうまでもない。しかしながら現実の学校における個人情報保護対策においては，学校内にあるすべての個人情報について，均一の取り扱いをすることが求められる訳ではなく，また可能でもない。各個人情報の性質に応じ，またそれぞれの情報の本人等と学校の関係に応じた取り扱いをすることがむしろ適切である。この意味で，学校において対策を講じる際には，それぞれの個人情報について，どのような経緯で当該個人情報が学校に提供され，保有されることになっているのかを踏まえた対策が必要である。

③ 不適切な扱いがされた場合に大きな影響がある可能性のある情報であること

学校の取り扱う個人情報には，それが不適切な取り扱いをされるならば，情報の本人に大きな影響を与えるものがある。たとえば事例の2及び3にある学校の成績は，生徒の将来の進学・就職等に関わる重要な判断の基礎とされるものである。また事例1及び4の健康に関する情報は，それが不適切な形で第三者に提供されるなどされた場合には，生徒の進学・就職に止まらず，そのほかのプライベートな生活にまでも影響を与える可能性があり，また状況によっては，さらに生徒の家族等にまで影響を与える可能性も否定できない。学校においては，このような個人情報を扱っていることに留意しつつ，対策を考える必要がある。

(2) 事件の態様の観点から

次に，先に挙げた事例に対して学校としては，次のような対策を取ることが考えられる。

(イ) 個人情報の紛失

1の事例では，書類を保管していた棚の鍵の閉め忘れにより，中に保管していた書類が紛失している。鍵を閉め忘れることは，確かに問題であるが，よくあることである。この事例においては，実際には，鍵を閉め忘れたことによって，中に保管されていた書類が何者かに持ち出されたことが問題であるから，この点に対しての対策を考える必要がある。

具体的な技術的対策としては，扉を閉めた段階で自動的に施錠される棚を利用する方法や，扉を閉め忘れたとしても，そのことに他の関係者が気づくところを保管場所とするなどの対応が考えられる。

また，この事例では，書類を保管する棚の鍵は同校の養護教諭だけが所有しているということであった。このような対応は，鍵を不必要に多数の者が保有しないという観点からは適切であるが，結局担当者のみが責任を負うことになり，その他の者のチェックが効かないこと，また担当者が休暇を取るなどした際の対応をどうするのか，等の観点からは，若干の懸念がある。

一般に情報セキュリティが確保された状況とは，

- ○ 機密性：アクセスを許可された者だけが，情報にアクセスできることを確実にすること
- ○ 完全性：情報及び処理方法が正確であること及び完全であることを保護すること
- ○ 可用性：認可された利用者が，必要なときに，情報及び関連する資料にアクセスできることを確実にすること

が確保された状況をいうとされる。この事例においては，完全性と可用性の観点において，改善の余地があるのではないかと考えられる。具体的な対策としては，鍵の管理者を複数にする，あるいは，鍵を個人管理ではなく，学校として管理する方法などが検討され得ると思われる。

（ロ）外部持ち出しへの対処

2及び5の事例は，個人情報の記録された媒体が盗難された事例である。この場合盗難にあったこと自体については，基本的には，不可抗力と考えざるを得ない。しかしながらこれらの事例を，より広く，個人情報を学校の外部に持ち出した際に情報を紛失した事例と考えるならば，同様の事例は数多く生じている。

このような場合に対する対策としては，個人情報の学外への持ち出しを禁止することも考えられる。しかしながら現実の学校における教員等の執務状況を考えると，これは非常に困難である。そこで次善の策としては，個人情報の学外への持ち出しが必要な状況を可能な限り減らしつつ，個人情報を持ち出す場合に取るべき対策を定め，それを遵守することとする等の対策を考えることができる。具体的な技術的対策としては，可搬性の記録媒体を用いる場合には，パスワードを設定する方法や，記録されるファイルにパスワードをかけるあるいは暗号化する方法などが考えられる。またこの他にも，可搬性記録媒体を利用する代わりに，セキュリティ対策の施された環境にあるネットワーク上のストレージを利用する方法等も考えられ，さらに情報漏洩時に漏洩する情報を最小限にするために，ファイルを細分化し，媒体に記録する方法等も考えられる。

なお，これらの技術的対策を適用する場合には，業務遂行への影響や，対策の予算等を十分に勘案しながら，適切なものを選択する必要がある。また防止対策を定める際には，情報漏洩等の防止策とともに，情報が紛失等した際に当該情報を用いて行う業務が滞ること等を避けるために，情報のバックアップを取ることや，そのバックアップ情報も管理すること等についても定めておくことが適当である。

（ハ）生徒の情報のインターネットへの公開

3の事例は，生徒の個人情報が掲示板に掲載されたのに対して，当該情報の削除を掲示板の管理者に求め，情報が削除されたという事例である。

特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（プロバイダ責任制限法）上，一定の場合に，掲示板の管理者等は，権利を侵害された者の求めに応じて，掲示板に記載された書き込みを削除することができることになっている。本事例では，これに従った対応が関係する掲示板の管理者によってなされたものと考えられる。

本事例においてインターネットに生徒の個人情報が公開されたこと自体は，学校が行ったものではないので，このことについて学校が責任を問われることはないと考えられる。しかしながら，この事例において漏洩している個人情報は，学校から漏洩した可能性のあるものであり，このように漏洩した情報が不適切な利用・提供をされていることが発見された場合，そのことによってそもそもの漏洩自体が問題とされる可能性がある。このような事態を避けるためにも，事例のように，漏洩した情報が不適切な利用・提供をされていることがわかった場合には，削除の依頼等，迅速な対処をすることが適切である。

また本事例の報道では，情報機器及び媒体は管理されており，ネットワークも管理されていたとされている。このように適切なセキュリティ対策が取られていたという内容の報道となったのは，報道関係者からの取材に対する学校側の回答によると思われる。個人情報保護対策においては，保護者等を含む外部からの照会等に対する対応も重要な点であり，学校としては，自ら採用している個人情報保護対策等を的確に説明することができるようにしておくことも有用であると思われる[iii]。

（ニ）ファイル交換ソフトへの対処

4の事例においては，ファイル交換ソフトを通じて個人情報の漏洩が生じている。これについて，文部科学省の「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」とする通知（以下文科省通知）[iv]は，次の対策を推奨している。

- ファイル交換ソフトは，安易にインストールしないこと。
- 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，生徒等の個人情報を扱わないこと。
- ファイル交換ソフトのインストールされているパソコンに，生徒等の個人情報等が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。
- ウイ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。

ファイル交換ソフトによるもののほかにも，ウイルスソフトやスパイウェア等の悪意のあるソフトウェア（マルウェア）により，個人情報を含む重要情報の漏洩等が生じる可能性がある。個人情報保護対策の重要なポイントの一つは，適切なセキュリティ対策を講じることであり，学校においても適切なセキュリティ対策を講じる必要がある。

なおこの点について文部科学省は「情報管理体制チェックリストの参考例」を公開している[v]。当該チェックリストにおいては，基本的なポイントとして以下の事項が上げられている。

① 漏洩しては困る情報を取り扱うパソコンには，ファイル交換ソフト（Winny）を導入しない。
② 職場のパソコンに許可なくソフトウェアを導入しない，またはできないようにする。
③ 職場のパソコンを外部に持ち出さない。
④ 職場のネットワークに，私有パソコンを接続しない，または，できないようにする。
⑤ 自宅に仕事を持って帰らなくて済むよう作業量を適切に管理する。
⑥ 職場のパソコンからUSBメモリやCD等の媒体に情報をコピーしない，またはできないようにする。
⑦ 漏洩して困る情報を許可無くメールで送らない，または，送れないようにする。
⑧ ウイルス対策ソフトを導入し，最新のウイルス定義ファイルで常に監視する。
⑨ 不審なファイルは開かない。

このチェックリストは，チェックリスト自体にも記載してあるとおり，各学校の現実の状況やルールに応じ，利用すべきものと思われる。なお学校にサーバーを設置している場合などには，それについてもセキュリティ対策を考える必要がある。

（ホ）個人情報の不適切な提供

6の事例では，学校教員が，同校に情報公開請求した者の個人情報が書かれた公開請求書の写しを同校の同窓会長に手渡していた。同窓会は学校と異なる第三者組織であることから，通常個人情報保護制度においては，提供に際して本人の同意が必要となる。

本事例において，当該学校教員はこのような報道にまで発展することになるとは考えていなかったというのが実際であると推察されるが，現実にはこのように報道等の対象となる場合もある。学校としては，個人情報の取り扱い方法とともに，実際に不適切な扱いをした場合にどのような影響が生じることになるのかも併せて学校の教職員に周知する必要がある。

4．おわりに

個人情報の保護に関する法律も定めるとおり，個人情報保護は，個人の権利及び利益を保護するために行われるものであるから，対策においても各個人情報の主体である個人の立場を考えながら対策をする必要がある。この意味で先に述べた学校が保有する個人情報の性質を認識しつつ，学校は個人情報保護対策を取る必要があり，また学校は教職員等がこの点を十分認識するよう，周知すべきである。

また，学校が関係する個人情報保護についての報道をみると，個人情報保護そのものに関する問題というよりは，情報セキュリティに関する問題であることが多い。この点から学校における個人情報保護への取り組みにおいては，情報セキュリティをどのように確保するか，という点に留意すべきである。

なおこの点に関連して，学校における個人情報保護対策への取り組みにおいては，関係する教職員の認識も重要であり，この点についても，研修を行う等，何らかの対策が必要である。

---

i 一般にセンシティブ情報とは，思想・信条及び宗教に関する事項や，人種・民族・門地・本籍地・身体あるいは精神の障害・犯罪歴等社会的差別の原因となる事項に関する情報等があげられる。

ii 学校に関わる個人情報保護制度の概要については，拙稿『学校における個人情報保護のあり方』i-Net第8号（2003年9月）参照。

iii もっとも本事例との関係では，現実に個人情報の漏洩は生じていることから，今後このような事件が生じないようにするための体制の整備が望まれる。

iv http://www.mext.go.jp/b_menu/koukai/kojin/info/001.htm

v http://www.mext.go.jp/b_menu/koukai/kojin/info/s007.htm