

V 個人情報保護のケースと関連する法令等

中学3年の学級担任をしているA教諭は、家事や子育て等で遅くまで学校で仕事ができないので、生徒の成績等のデータが入った個人用のUSBメモリを自宅に持って帰り、自宅のパソコンを使用して進学事務等をするようになった。

ところが、ある日、バッグに入れて持ち運びしていたUSBメモリを探したが、見あたらなかった。

よく考えてみると、一昨日、自宅で仕事をした時にUSBメモリを使用し、その後は使用していなかったことまでわかった。そこで、昨日からの自分の行動をすべてチェックし、心当たりの場所を何度も探してみたが、やはり見つからなかった。

翌日、学校長に生徒のデータが入ったUSBメモリを紛失したことを報告した。

(1) ポイントを整理してみましょう！

- ◇A教諭は3年生の担任で、進学事務などの校務と家事の両立をしなければならず、多忙な毎日を過ごしていた。
- ◇A教諭は、多忙なため、学校で仕事を処理しきれず、自宅に持って帰るようになった。
- ◇A教諭は、登録したものではないUSBメモリに、生徒の個人情報を保存して持ち帰っているなど、「情報セキュリティポリシー」を守れていない。
- ◇USBメモリを学校と自宅のパソコンに接続しているので、学校のネットワークが、コンピュータウィルスに感染する可能性がある。
- ◇もし、個人情報がインターネット上に流出した場合は、データを完全に回収することは不可能であり、回復困難な不利益が生じる。
- ◇USBメモリの管理が十分でなく、情報持ち出しに対する危機管理意識が希薄で、情報セキュリティに関する知識が身につけていない。

(2) どのような責任が問われる可能性があるのでしょうか？

◇身分上の責任

◇民事上の責任

(3) 関連する法令等にはどのようなものがあるのでしょうか？

◇地方公務員法第32条、第33条（前出）

（秘密を守る義務）

第34条 職員は、職務上知り得た秘密を漏らしてはならない。その職を退いた後も、また、同様とする。

（罰則）

第60条 左の各号の1に該当する者は、1年以下の懲役又は3万円以下の罰金に処する。

二 第34条第1項又は第2項の規定に違反して秘密を漏らした者

◇徳島県個人情報保護条例

(適正管理)

第10条 実施機関は、個人情報取扱事務の目的を達成するために必要な範囲内で、その保有する個人情報に過去又は現在の事実と合致するよう努めなければならない。

2 実施機関は、個人情報の漏えい、滅失又はき損の防止その他の個人情報の適正な管理のために必要な措置を講じなければならない。

3 実施機関は、保有する必要がなくなった個人情報を確実かつ速やかに廃棄し、又は消去しなければならない。ただし、歴史的文化的価値を有する資料として保存する必要があると認められるものについては、この限りでない。

(職員の義務)

第11条 実施機関の職員は、職務上知り得た個人情報をみだりに他人に知らせ、又は不当な目的に使用してはならない。その職を退いた後も、同様とする。

(事業者の責務)

第45条 事業者は、個人情報の保護の重要性を認識し、個人情報の取扱いに伴う個人の権利利益の侵害の防止に関し必要な措置を自主的に講ずるとともに、個人情報の保護に関する県の施策に協力しなければならない。

2 事業者は、第6条第3項に規定する個人情報を特に慎重に取り扱わなければならない。

3 事業者のうち、県が資本金、基本金その他これらに準ずるものを出資している法人であって規則で定めるものは、その取り扱う個人情報の保護に関し実施機関に準じた措置を講ずるよう努めなければならない。

(罰則)

第58条 実施機関の職員若しくは職員であった者又は第12条第3項の業務に従事している者若しくは従事していた者が、正当な理由がないのに、個人の秘密に属する事項が記録された保有個人情報を含む情報の集合物であって、一定の事務の目的を達成するために特定の保有個人情報を電子計算機を用いて検索することができるように体系的に構成したもの(その全部又は一部を複製し、又は加工したものを含む。)を提供したときは、2年以下の懲役又は100円以下の罰金に処する。

◇民法第709条、第710条 (前出)

◇国家賠償法第1条 (前出)

◇教職員の懲戒処分の方針 (標準的な処分量定)

(4) 対応策について検討してみましょう！

◇適切な初期対応を行う (事実関係の把握等)。

◇管理職を中心に組織的に対応する (情報・意思決定の一元化、取材対応等)。

◇不安や動揺の広がりを防ぐため、保護者・児童生徒等への説明責任を果たす。

◇所管の教育委員会へ報告し、指導・助言を受ける。

◇学校・家庭で、徹底的にUSBメモリを探す。

◇インターネット上に生徒の個人情報流出がないか監視し、流出の可能性があった場合は、至急プロバイダに削除依頼する等、関係機関への対応を行う。

◇「情報セキュリティポリシー」の内容を十分理解する研修を実施し、個人情報漏えいの危険性を周知し、取り扱う者としての意識を高める。

◇原則として、学校から個人情報は持ち出さないようにし、やむを得ず持ち出す場合は、情報管理者の許可を得るなどのルールを明確化し、紛失・漏えい防止策を徹底する。

◇電子ファイルの暗号化やパスワードの設定など、情報を管理する上で必要な基本的知識の習得ができていないか、全教職員を対象に調査し、必要な研修を行う。

(5) セルフチェックしてみましょう！

	項 目	ア	イ	ウ
1	学校で取り扱う情報の多くが個人情報であり、守秘義務があることを理解している。			
2	「教職員の懲戒処分の指針（標準的な処分量定）」で示された個人情報の盗難紛失又は流出した場合の処分を理解している。			
3	個人情報は持ち出さないことを原則とし、やむを得ず持ち出す場合は、管理職への報告等、決められたルールを守っている。			
4	個人情報の盗難や流出等を防ぐためクリアデスクに心がけ、個人情報の入った文書等は、鍵のかかる場所に保管している。			
5	個人情報の入った文書や電子メール等は、誤送付・誤送信しないよう、宛先を厳重にチェックしている。			

(ア：はい イ：どちらとも言えない ウ：いいえ)

☆参考

徳島県教育委員会情報セキュリティポリシーの概要について

情報セキュリティポリシーは、すべての教職員が理解して実行することが大切です。情報は水と同じで、どこかに穴があればそこから漏れ出します。漏れたら最後、もとに戻すことはできません。

重要なポイントは、答案・成績表・住所録など紙に印刷されたものや電子媒体に保存されたものは、「情報資産」であるということです。このような「情報資産」を保護するため、徳島県教育委員会では情報セキュリティに関する対策に取り組んでいます。

組織人として、公務員（教職員）として、情報セキュリティに対する意識を高め、「情報資産」を守っていくことが大切です。

『徳島県教育委員会情報セキュリティポリシーにおける基本方針』（抜粋）

（情報セキュリティポリシー対策の根本的な考え方を表しています。）

第10条 教職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシーを守らなければならない。



『徳島県教育委員会情報セキュリティ対策基準』（抜粋）

（基本方針を実現するために、何をしなければならないか示しています。）

- ・所属長を「情報セキュリティ管理者」として、所属内に情報セキュリティ委員会を設置しなければなりません。
- ・教職員等は、業務以外の目的で、情報資産を外部へ持ち出したり、電子メールを送信したり、インターネットにアクセスしてはいけません。



『〇〇学校情報セキュリティ実施手順』

（各所属で、具体的な業務において、どのような手順に従って実行していくかを示しています。）

- ・情報セキュリティ管理者…所属長（学校長）が務めます。
- ・情報セキュリティ委員会…所属内での情報セキュリティの要となる組織です。
- ・情報資産の分類……………個々の情報の重要度を分類1～3に分けて管理します。
- ・情報資産の管理方法……………情報資産の保管・保存場所や取扱について規定します。
- ・教職員の遵守事項……………パソコン・外部記録媒体・ネットワーク・情報資産の取扱において、各個人が遵守すべきことを規定しています。
- ・研修体制……………情報セキュリティに関する研修を明確に位置づけます。
- ・評価と見直し……………自己点検・自己改善と実施手順の見直しを行うことを規定します。