

VII 情報セキュリティ・個人情報保護のケーススタディ

ケース1

定期考査が近づき、学校で考査問題を作成し始めたところ、時間的に遅くなったのと、翌日が土曜日でもあったので個人のUSBメモリに保存し、持ち帰って仕事の続きをしようと考えたが・・・。

問題点

- ・
- ・
- ・

対策

- ・
- ・
- ・

効果等

- ・
- ・
- ・

ケース2

A教諭の机上は、あまり整理ができていない。今日は「生徒の進路希望調査用紙がない。」と大騒ぎをしている。私は、またかと呆れてしまった・・・。

問題点

- ・
- ・
- ・

対策

- ・
- ・
- ・

効果等

- ・
- ・
- ・

ケース3

パソコンで定期考査の評価をしている途中に生徒指導が必要となり、パソコンの入力画面もそのまま指導に行った……。

問題点

- ・
- ・
- ・

対策

- ・
- ・
- ・

効果等

- ・
- ・
- ・

ケース4

ホームルーム担任の生徒の保護者から電話で、最近の家庭での様子や学習について相談を受けた。その際、メモ書きした用紙をパソコンで打ち直し、個人票にファイルした後、うっかりメモ用紙を丸めてゴミ箱に投棄してしまった……。

問題点

- ・
- ・
- ・

対策

- ・
- ・
- ・

効果等

- ・
- ・
- ・

ケース5

年度末の大掃除で書類の整理のため、健康診断書など個人情報のファイルを段ボールに入れ、事務室に置いておいたところ、一部がなくなっていることが判明した。誤廃棄による紛失の可能性が疑われるが・・・。

問題点

- ・
- ・
- ・

対策

- ・
- ・
- ・

効果等

- ・
- ・
- ・

コーヒータイム

次の問いに答えてください。

- 1 職員連絡表や定期考査問題など、分類2の情報外部記憶媒体で持ち出す際に、暗号化する必要はない。
(はい、いいえ)
- 2 清掃分担表や補習計画など、分類3のみの情報が入っているUSBメモリ等は個人の机の引き出しに保管してもよい。
(はい、いいえ)
- 3 私物のパソコンで業務を行うのは危険であるため、職場のパソコンを自宅に持ち帰り業務を行ってもよい。
(はい、いいえ)
- 4 職員は情報漏洩や紛失などの事故を起こした場合、自分で対処すれば所属長に報告する必要はない。
(はい、いいえ)
- 5 紙媒体の文書については、個人情報を含んでいても施錠された場所に保管する必要はない。
(はい、いいえ)

(注) 分類については、県教育委員会事務局、教育機関及び県立学校の情報資産管理表で決められています。市町村立小・中・高等学校においても参考にしてください。

～ ケースの解答例 ～

ケース1

- 問題点
- ・校務で使用するU S Bメモリの登録や情報資産持ち出しの申請ができていない可能性がある。
 - ・個人のU S Bメモリを職場のパソコンに接続することにより、コンピュータウイルスに感染するリスクが高まる。
 - ・U S Bメモリには、他にも重要な情報資産が保存されている可能性があり、情報管理に問題がある。
 - ・定期考査用問題はどの分類に属するかや分類によるU S Bメモリの取扱いの違いを知らずに、情報を暗号化せずに持ち帰っている可能性がある。
- 対 策
- ・情報セキュリティポリシーに関する研修を定期的実施し、情報資産の分類や分類による取扱いの違いを確認する。
 - ・校務で使用する外部記憶媒体の使用登録申請書や情報資産を持ち出すメディア申請書の提出を徹底する。
 - ・情報の暗号化についての研修を実施する。
- 効果等
- ・情報資産の流出や紛失の恐れが無くなる。
 - ・情報セキュリティの意識の醸成が図られる。
 - ・情報資産の重要度の評価ができる。
- 法令等
- ・地公法第34条（秘密を守る義務）
 - ・徳島県個人情報保護条例（以下、「個人情報保護条例」という。）第10条（適正管理） 等

ケース2

- 問題点
- ・クリアデスクができていない。
 - ・個人情報の紛失・漏えいのおそれがある。
 - ・「またか」と呆れられるように、これまでも個人情報の適切な管理ができていなかったことが推測される。
- 対 策
- ・キャビネット等を増設し、クリアデスクに取り組める環境を整える。
 - ・事前に処理方法をマニュアル化しておき、紛失・漏えいなどへの防止策を徹底しておく。
 - ・情報セキュリティに関する知識を身につけるための研修を実施する。
- 効果等
- ・個人の情報セキュリティの向上だけでなく、職場環境の改善にもつながる。
 - ・マニュアル化することで組織としての情報セキュリティも高まる。
 - ・ネット上への個人情報流出などのトラブルを防止することができる。
- 法令等
- ・地公法第34条（秘密を守る義務）
 - ・個人情報保護条例第10条（適正管理） 等

ケース3

問題点・クリアスクリーンができていない。

- ・評価資料が漏えいしたり、紛失したりするおそれがあった。
- ・日常的に重要書類を紛失させる可能性が高い。

対 策・日ごろからクリアデスク、クリアスクリーンを徹底する。

- ・緊急を要する事態であっても、重要書類の管理等は教職員間で注意し合う。
- ・研修によって情報漏えい防止の意識を確立する。

効果等・情報の漏えい・紛失のリスクが低くなる。

- ・クリアデスクにより書類の整理整頓ができ、職場環境が良くなる。
- ・クリアデスクによる教職員間の風通しも良くなる

法令等・地公法第34条（秘密を守る義務）

- ・個人情報保護条例第10条（適正管理）

等

クリアデスクとは

重要な書類などが紛れてしまわないように机の上を整理整頓すること。また、部活動などで長時間席を離れるときや退校時に、机上へ重要な書類・USBメモリ（分類2以上の情報資産を含むもの）を置かずに、施錠できる引き出しなどにそれらを片付けることを指します。

クリアスクリーンとは

席を離れたときにパソコンの画面を見られないように、また、勝手に操作されないようにロックすることを指します。スクリーンセーバーを解除するときパスワードの入力が必要となるように設定してください。また、席を離れるときは、必ず画面ロック（Windows キー + L）で必ず画面をロックするようにします。

ケース4

- 問題点
- ・ゴミ箱に捨てた用紙には個人情報が入力されており、清掃時に生徒の目に触れる可能性があった。
 - ・「うっかり」捨てたことから分かるが、個人情報に対する危機管理意識が希薄である。
 - ・紙媒体もデジタル媒体と同様に取扱う必要があり、この場合は分類2に属すると思われる情報なので、パソコンに入力後は、シュレッダーにかけるなど、情報漏えいしないように確実に処分する必要がある。
- 対策
- ・校内研修等で、個人情報の保護等に関する研修を実施する。
 - ・児童生徒の個人情報等、守るべき情報は何か共通理解が必要である。
 - ・不要となった個人情報の入力された用紙は、シュレッダーにかけることを全教職員が徹底する。
- 効果等
- ・情報の漏えいが無くなる。
 - ・厳正な情報管理に努めようとする共通認識ができる。
 - ・情報漏えいを防ぎ、生徒や保護者が不利益を被ったり、生徒や保護者からの教職員に対する信頼を失うことを防ぐ。
- 法令等
- ・地公法第34条（秘密を守る義務）
 - ・個人情報保護条例第10条（適正管理）
- 等

ケース5

- 問題点
- ・大掃除とはいえ個人情報に対する危機管理意識が希薄である。
 - ・紙媒体もデジタル媒体と同様、厳格な取扱いが必要であり、本来、施錠できる場所に保管する必要がある書類なのに、注意が行き届かない状態で段ボールに入れて保管している。
 - ・管理する責任者が、その役割を果たせていない。また、責任の所在が明確でない。
- 対策
- ・校内研修等で、個人情報の取扱いに関する研修を実施する。
 - ・個人情報の整理などは、責任者の監督の下、複数の教職員で当たる。
 - ・不要な個人情報の入力された用紙は、シュレッダーにかける。
- 効果等
- ・情報の漏えいが無くなる。
 - ・厳正な情報管理に努めようとする共通認識ができる。
- 法令等
- ・地公法第34条（秘密を守る義務）
 - ・個人情報保護条例第10条（適正管理）
- 等

コーヒータイム

1 (いいえ) 2 (はい) 3 (いいえ) 4 (いいえ) 5 (いいえ)

分類1	徳島県情報公開条例第8条第1号から第7号に該当する情報が含まれている情報資産のうち、セキュリティ侵害が個人並びに団体及び組織の生命、財産等へ重大な影響を及ぼすおそれのあるもの (例えば、成績会議資料、証明書関係など)
分類2	徳島県情報公開条例第8条第1号から第7号に該当する情報が含まれている情報資産のうち、分類1以外のもの (例えば、定期考査問題、職員連絡表など)
分類3	分類1及び分類2以外の情報資産 (例えば、学校祭関係、清掃分担表など)

(注) 各所属の情報資産管理表で確認してください。

◇分類別管理方法など

	分類1	分類2	分類3
管理方法	暗号化して施錠された場所に保管	暗号化して施錠された場所に保管	規程なし
外部への持出	持ち出し禁止	暗号化して持出可能	暗号化して持出可能
電子メールなど	暗号化もしくはパスワードを設定して送信	暗号化もしくはパスワードを設定して送信	規程なし

(注) 紙媒体も同様に厳格な取扱いが必要です。

[参考]

— USBメモリの取扱い手順 —

分類2に属する定期考査問題について

- 1 外部記憶媒体使用登録申請書を提出する。(未登録のUSBメモリは使用不可)
※外部記録媒体は、保管責任者(副校長又は教頭)が一元的に管理する。
- 2 保管は、暗号化して施錠された場所に保管する。
- 3 情報資産持ち出しメディア申請書を提出する。
- 4 暗号化して持ち出す。

(注) 過失により個人情報盗まれ、紛失し、又は流失させ、公務の運用に支障を生じさせた教職員は減給又は戒告の懲戒処分を受ける可能性があります。