

教育委員会等の学校設置者及び教職員の皆様へ

令和 7 年 6 月 25 日
個人情報保護委員会学校における個人情報の漏えい等事案を踏まえた
個人情報の取扱いに関する留意点について（注意喚起）

学校においては、その業務の性質上、幼児・児童・生徒（以下併せて「生徒」といいます。）の個人情報が、日常的かつ頻繁に取り扱われる環境にあります。また、取り扱われる個人情報の項目も、健康診断結果や病歴等の要配慮個人情報¹、成績や家庭環境に関する情報等、プライバシー性の高い個人情報や仮に悪用された場合にこどもの権利利益に大きな影響を及ぼしかねない個人情報が多くなっています。

令和 4 年 4 月から私立学校を含む個人情報取扱事業者の漏えい等報告が義務化され、また、令和 5 年 4 月から個人情報保護法が地方公共団体にも適用されることとなり、学校現場における、生徒の個人情報に関する漏えい、滅失等の事案（以下「漏えい等事案」といいます。）についても、多数の報告を受けています。そこで、当委員会は、これまでに受領した報告に基づき、学校現場において生じやすい漏えい等事案について、その発生原因や再発防止策について、別紙²のとおり、取りまとめました。

教育委員会等の各学校の設置者及び教職員の皆様におかれましては、別紙の内容を御覧いただき、漏えい等事案が発生しやすい状況についての理解を深め、日常の業務における生徒の個人情報の取扱いや、ルール及び対策の見直しに役立てていただきますようお願いいたします。

¹ 「要配慮個人情報」とは、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」といいます。）上の用語で、「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報」をいいます（個人情報保護法第 2 条第 3 項）。

² 今回、小学校、中学校及び高等学校等の現場において発生した個人情報の漏えい等事案について、個人情報保護委員会が教育委員会から受領した漏えい等報告を基に分析を行いました。

特に留意していただきたい事項は、以下の点です。

- ・ 教育・研修等による個々の教職員の意識向上も大切ですが、人間の注意力にも限界はあります。したがって、教育委員会等の各学校の設置者や学校の管理職の皆様におかれましては、個人の意識向上に偏った対策ではなく、組織的な側面や技術的な側面から、漏えい等を防止できないかについて、別紙の漏えい等事案の典型例を御参照いただき、教育委員会等の各学校の設置者や学校全体として実施できる内容を御検討いただきますようお願いいたします。
- ・ 最近では、学校でも ICT の活用が進み、情報共有ツール等のデジタルツールの使用における個人情報の漏えい等事案が多く見受けられます。このような事案では、一度の事象で、多くの生徒の個人情報が漏えいしてしまう点で問題が大きくなる場合もありますので、予防のための対策を御検討いただきますようお願いいたします（例えば、研修等を通じて情報セキュリティに関する意識の醸成を図ること、教職員の皆様が専門家等から技術的なサポートを受けられやすくするような環境作り等が考えられます。）。
- ・ （公立学校の場合）教育委員会を含む行政機関等の保有する個人情報の取扱いについては、個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）（以下「事務対応ガイド」といいます。）「4－8（別添）行政機関等の保有する個人情報の適切な管理のための措置に関する指針」があります。同指針にも記載されているとおり、「個人情報の適切な管理に関する定めの整備」「管理体制の整備³」「教育研修」は、行政機関等に求められる基本的な事項になりますので、これらの事項が不十分である場合には、速やかな対応をお願いいたします。

以 上

³ 事務対応ガイド 4-8-2 において、各行政機関等に総括保護管理者を置くこと、保有個人情報を取り扱う各課室等に保護管理者を置くこと、保有個人情報を取り扱う各課室等に保護担当者を置くこと等を定めています。教育委員会及び学校においても、現場の状況に応じて、管理体制を整備し、責任及び役割を明確にした上で、個人情報の適切な管理のために必要な措置を講じていただくことが重要です。

学校現場において発生しやすい個人情報の漏えい等事案に関する原因と再発防止策

1 学校現場において漏えい等事案の発生が多い理由

学校における漏えい等事案が多く発生する主な理由については、以下のようなものが挙げられます。

(1) 取り扱う個人情報が多いこと

学校では、生徒の氏名・生年月日・住所などの基本的な個人情報、生徒の健康に関する情報、生徒の成績・進路に関する情報、生徒の家庭環境に関する情報等、多くの種類の情報を日常業務において取り扱っています。したがって、学校は、個人情報について、漏えい等事案が発生する機会が多い場所であるといえます。

また、生徒の人数分の個人情報を取り扱う環境にあるため、ヒューマンエラーに起因するものであっても、一度の漏えい等事案において、外部に流出等する個人情報に係る本人数が多くなりやすい傾向にあります。

(2) 業務スペースが広いこと

学校では、教職員が多くの場所に移動して執務をしなければなりません。事務等を行う職員室、生徒に指導を行う教室、行事等を行う体育館や講堂等、様々な場所に移動するため、個人情報が記録された媒体を置く場所が固定されにくいという問題があります。特に紙媒体に個人情報が記録されている場合、紙媒体の置き忘れや移動中の紛失などが発生するリスクが高まります。

また、学校は、当然のことながら、生徒や保護者等の学校の職員以外の多数の人が利用する場所であるため、業務スペースとして内部であるか又は外部であるかの区別がつきにくく、外部の人から個人情報を閲覧される機会が多くなります。

(3) データの共有範囲の問題

最近の学校では、生徒が1人1台の端末を有し、アプリケーションを使って課題のやり取りを行ったり、教員から生徒に対し連絡事項を伝えたりする機会が多くなっています。また、学校から、保護者に対しても、アプリケーション上で連絡事項を伝える機会が多くなっています。

このような状況の下、教職員は、教職員間のみで共有すべきデータと、生徒や保護者に対しても共有するデータの両方を、日常的に取り扱わなければならないため、教職員間のみで共有すべき生徒の個人情報を、誤って生徒や保護者に対しても共有してしまうような事象が生じやすい状況にあります。

(4) 紙媒体の取扱いが多いこと

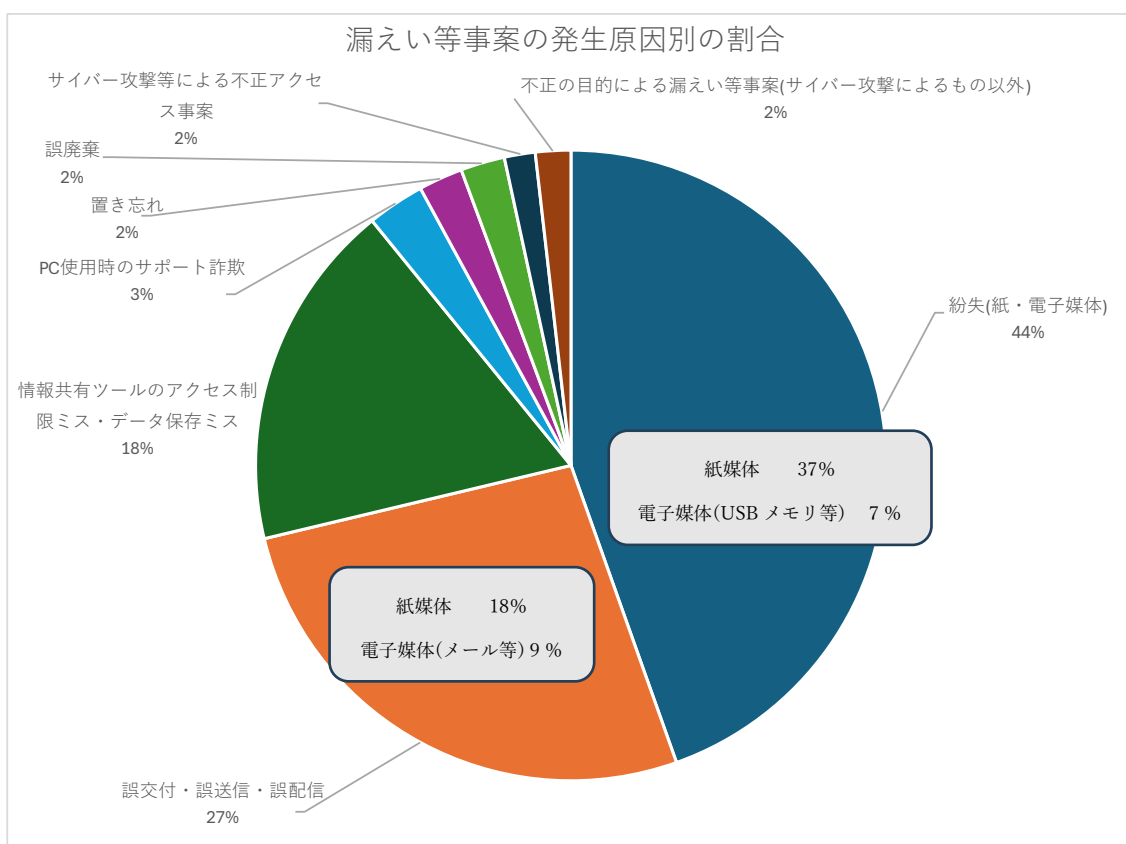
学校では、生徒の教育目的や保護者への連絡目的等で、一般に紙媒体の取扱いが多くなりがちです。そのため、個人情報が記録された紙媒体の紛失や誤交付、印刷ミス等による漏えい等事案が生じやすい状況にあります。

2 学校現場で発生しやすい漏えい等事案の分析結果

注) 令和5年4月から令和7年4月までにおいて、小学校、中学校、高等学校及び特別支援学校の現場において発生した漏えい等事案について、個人情報保護委員会が、教育委員会や私立学校等から受領した漏えい等報告（約 450 件）を基に、発生原因別の割合等を分析したもの。

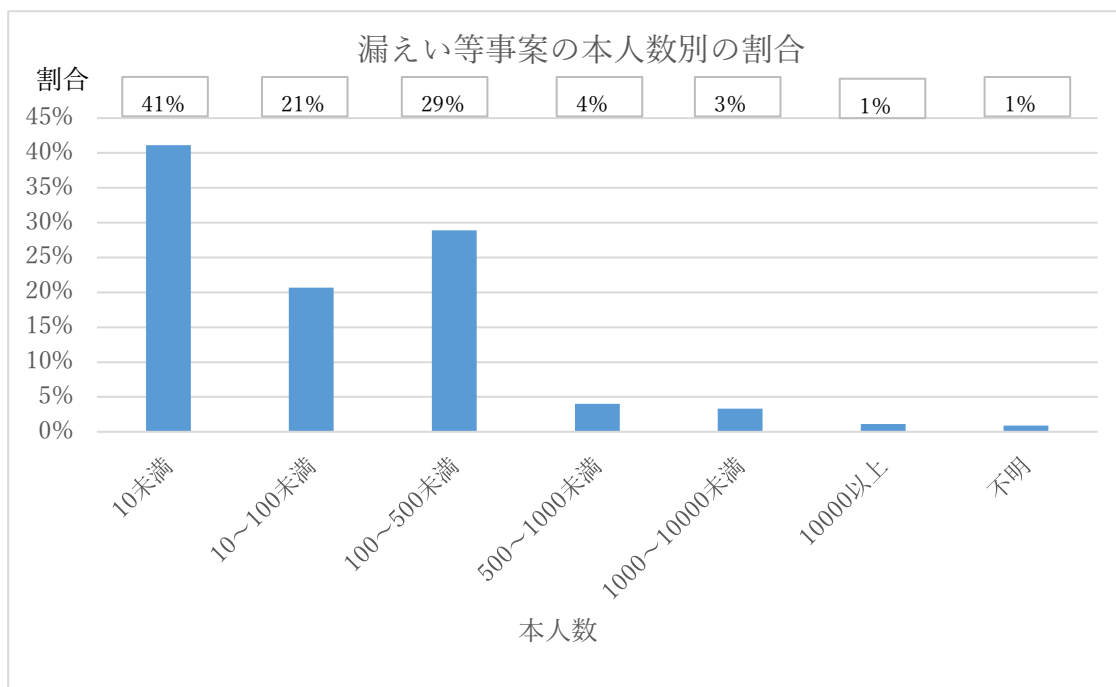
なお、本分析は、学校現場で発生しやすい漏えい等事案に着目するものであるため、教育委員会の事務において生じた事案や委託先等の民間事業者において発生した不正アクセス事案の影響を受けた漏えい等事案は除外している。

- (1) これまでに受領した漏えい等報告を基に、以下のとおり、発生原因別の割合をグラフ化しました。

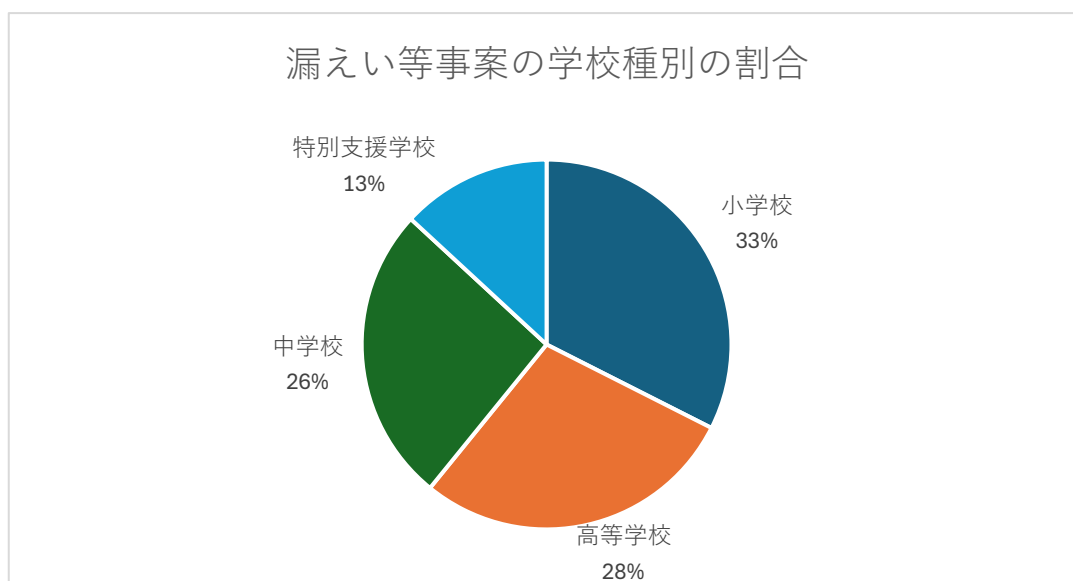


紛失による漏えい等事案が一番多くなっていますが、情報共有ツール等デジタルツールの使用に伴う操作ミスも一定の割合で生じている点から、最近の学校における ICT 活用の浸透がうかがえるところです。

- (2) 以下は、本人数別の発生割合をグラフ化したものです。誤交付事案等、本人数が10人未満のものも多いですが、情報共有ツールの誤設定による事案や紛失事案等で本人数が100人以上になっている事案も多くなっています。



- (3) 以下のグラフは、個人情報保護委員会に報告された漏えい等事案が発生した学校種別の割合を、グラフ化したものです。これを見ると、学校種別に偏ることなく漏えい等事案が発生していることが分かります。



3 学校現場において生じやすい漏えい等事案と再発防止策の例

以下においては、漏えい等事案のタイプ別に分析しています。個人情報保護法上、行政機関等については法第 66 条第 1 項において安全管理措置が規定され、事務対応ガイドの「4－8（別添）行政機関等の保有する個人情報の適切な管理のための措置に関する指針」において具体的な措置について規定しています。また、個人情報取扱事業者については法第 23 条において安全管理措置が規定され、個人情報の保護に関する法律についてのガイドライン（通則編）（以下「ガイドライン」といいます。）の「10（別添）講ずべき安全管理措置の内容」において具体的な措置について規定しています。

以下では、事案類型ごとに、問題となり得る事務対応ガイドの規定（公立学校の場合）及びガイドラインの規定（私立学校の場合）を記載しています。実際の漏えい等事案については、個別の事情により問題となる事項は変わりますが、参考にしてください。

(1) 紛失（紙媒体）（事務対応ガイド 4-8-5(6) (9) 等、ガイドライン 10-3(2)、10-5(1) (3) 等）

学校では、生徒の学習用や保護者にお便りなどを配布する必要性等から、特に紙媒体の利用が多く、また、現在はデジタル化されている資料も過去分は紙で保存されています。そのため、紙媒体の紛失は、漏えい等事案の件数としては多くなっています。

また、修学旅行や校外学習等、業務上、校外に持ち出す必要がある場合、業務が多忙のため自宅に持ち帰って作業するために校外に持ち出す場合などもあり、校外での紛失事案も見受けられます。

【事案例】

- 職員室内保管庫に保管してあったはずの生徒数百名の緊急連絡カードが所在不明となった。
- 学年末試験の成績一覧表が校外で拾われた。
- 休日に自宅で業務を行うためテスト答案を校外に持ち出し、飲食した後、帰宅途上でカバンごと紛失した。
- 数年分の指導要録が所在不明となった（新校舎への引っ越しの際に誤廃棄した可能性が高い。）。
- 修学旅行中に、教員用しおりや、生徒のアレルギー情報等が記載された名簿を紛失した。

【発生原因】

- ・ 校外に持ち出し中の管理不備。
- ・ 職員室内の管理不備。
- ・ 新校舎への引っ越しに伴う紛失の可能性。

【再発防止策例】

- ・ 個人情報に記載された書類を保管するキャビネットの鍵の管理の一元化。

- ・家庭状況調査ファイルの使用記録簿を作成し、管理職は退勤前に記録簿を確認。
- ・校外に個人情報を持ち出す際のルールの確認・徹底。
- ・事案を共有し、校内研修を実施。
- ・修学旅行しおり等、校外に持ち出すことが前提となっている資料に掲載する情報の見直し。

(2) 紛失（電子媒体）（事務対応ガイド 4-8-5(4)(6)(9)等、ガイドライン 10-3(2)、10-5(1)(2)(3)等）

電子媒体を紛失することにより、大量の個人情報について一度に漏えい又は漏えいのおそれが発生することがあります。また、電子媒体の紛失事案については、そもそもその電子媒体の使用や校外持ち出しについて、セキュリティポリシー等の規程に違反していることが多く見受けられます。

【事案例】

- 生徒の個人情報が入った USB メモリを教諭の机で保管していたが、数日間出勤しなかった間に紛失した。
- 生徒の成績データ等が入った私物 USB メモリを校長の許可なく校外に持ち出し、カバンに入れたまま飲食し、紛失した。
- 生徒の傷病情報等が入った私物 PC を職員室前の生徒配布用メールボックス上に置き忘れたところ、当該 PC が無くなった。
- 児童の教育支援計画の一部を写した画像を保存したデジタルカメラを入れたカバンが、自転車ごと盗難に遭った。

【発生原因】

- ・情報セキュリティポリシー等に従わない私物 USB メモリの使用。
- ・情報セキュリティポリシー等に従わず、許可なく校外に USB メモリを持ち出し。
- ・電子媒体そのものや、電子媒体を入れたカバン等の管理の問題。

【再発防止策例】

- ・情報セキュリティポリシー等の規程の再周知。校内研修の実施。
- ・業務の見直し等により校外に個人情報を持ち出す機会の削減を図る。
- ・USB メモリの保管・管理は、校長及び教頭が厳重に行い、貸出及び返却の際は書面による管理者の承認・確認を行う。
- ・USB メモリを原則使用禁止とする。
- ・個人情報を含む資料を保存した USB メモリについてはパスワード設定を徹底。

(3) 誤交付（事務対応ガイド 4-8-5(7)等、ガイドライン 10-3(2)、10-5(3)等）

個人情報が記載された書類の誤交付は、学校現場だけで生じやすい事象というわけではありません。ただし、学校では、生徒の健康に関する個人情報等の要配慮個人情報を扱うため、本人数の少ない漏えい事案についても漏えい等報告の対象事態であることが多くなっています。また、学校では紙媒体の取扱いが多いために誤交付が生じやすい環境であるともいえます。

【事案例】

- 生徒Aの保健調査票や尿検査の結果通知書を生徒Bに誤交付した。
- 児童調査票等が入った連絡袋を取り違え、生徒Aに渡すべきものを生徒Bに、生徒Bに渡すべきものを生徒Aに渡すことにより、個人情報漏えいした。
- 教員が業務で使用する資料（個人情報を含む。）をまとめたファイルを児童の机上に置いていたところ、誤って当該児童が自宅に持ち帰った。

【発生原因】

- ・ 検尿結果を配布する際に、封筒の中身をよく確認しなかった。
- ・ 提出物ファイルが個々の家庭とやり取りするための連絡帳ファイルと同色の紙ファイルであり、両者を混在してしまった。
- ・ クラス担任が不在のため、クラス副担任が同じ名字2名の生徒の中身を十分に確認せず封入して交付した。
- ・ 資料等の保存・整理が不十分の状態で複数の案件や業務・学習指導を同時進行的に進めていたため、書類が混在してしまい、生徒等に交付すべきではない書類を誤って交付するに至った。

【再発防止策例】

- ・ 個人情報を含む書類を封入する際には、確認を徹底する。
- ・ 机上の整理整頓、文書等の管理を徹底させる。
- ・ 封筒の宛先と文書の宛名が突合しやすいよう外折りにする。
- ・ 個人情報を含んだ文書を教室に安易に持ち込まない。
- ・ 個人情報を含む書類の保管は、施錠可能な職員室の保管棚に入れる。

(4) 誤送信・誤配信（事務対応ガイド 4-8-5(7)等、ガイドライン 10-3(2)、10-6(4)等）

メールの誤送信については、学校現場以外でも見受けられる事象です。ただし、学校現場では、近時、生徒や保護者等ともメール配信システムや端末への配信等を行うことが増えていることから、生徒端末への誤配信や欠席連絡アプリ上での送信ミスなどの特有の事象も生じています。

【事案例】

- 一斉メール配信システム使用時に誤って個人情報が含まれたファイルを添付した。
- メール宛先入力の際、誤って教職員と同姓の生徒のアドレスを入力した。
- BCCで送信するべきところをToやCCで送信した。
- 本来持ち出しが禁止されている成績データを、自身の個人アドレスに送付したつもりがメールアドレスを誤って送信した。
- 生徒指導に関する情報を、誤って生徒が使用する一人一台端末に配信した。
- 欠席連絡アプリ上で、本来1人に送信する情報を多数に誤送信した。

【発生原因】

- ・ メール送信時や一斉メール配信システム使用時等における、添付ファイルや宛

先の確認不足。

【再発防止策例】

- ・メール送信に関するルールの策定。
- ・一斉メールを送信する際の確認の徹底。
- ・職員に対する事案の共有、研修や注意喚起を定期的実施。
- ・考査や成績処理について余裕を持って業務を行えるよう、日程や方法の見直しを図る。

(5) 情報共有ツールのアクセス制限ミス・データの保存ミス（事務対応ガイド 4-8-5(7)、4-8-6(1)等、ガイドライン 10-3(2)、10-6(1)等）

近年、学校でもデジタルツールを使用する必要のある業務が増加しています。また、学校においては、情報の共有範囲は職員間だけにとどまらず、生徒や保護者に共有すべきケースも多いことから、情報共有ツールにおける誤投稿やアクセス制限のミス、個人情報が含まれるファイルの保存場所のミス等により、個人情報が漏えいするケースが少なくありません。これらの事象の背景としては、デジタルツールの仕様や設定に関する理解が不十分なまま使用されていることがあります。

【事案例】

- オンラインフォームを使用したアンケートを実施した際に設定を誤った（結果の概要を表示する機能を誤って有効にしたため、回答者同士で回答が閲覧できる状態となった。教員用の共同編集権限を生徒にも付与した等）。
- オンラインフォームを使用して試験の自己採点結果を生徒に入力してもらう際に、教員用 URL を誤って掲載したため、生徒が他の生徒の結果を閲覧できる状態となった。
- オンライン学習管理システムを利用し答案・成績を生徒に返却しようとしたところ、クラスを間違えて送信した。
- コラボレーションツールを利用していたところ、チャットの投稿場所を間違え、生徒を含む学年全体に情報を送信した。
- 担当教諭間で情報共有をするはずが、誤って、個人情報が記録されたファイルを教員及び生徒の共有フォルダに保存してしまった。

【発生原因】

- ・プライベート設定にすべきところを誤って公開設定にした等の設定ミス。
- ・保存先の共有範囲の理解不足。
- ・対象のファイルやアップロード先の確認不足。
- ・デジタルツールの仕様や設定に関する理解不足。

【再発防止策例】

- ・オンラインフォーム等のツール利用時の校内マニュアルを作成し、教職員に研修を実施。
- ・教育委員会から全学校に対して、個人情報の取扱いや ICT 活用の留意事項について指導の徹底を図る。

- ・学習用クラウドサービスの操作について、教育委員会と学校それぞれの権限を再整理。
- ・コラボレーションツールの公開範囲の設定を定期的に点検。
- ・オンライン学習管理システムに掲載する文書を限定。

(6) PC 使用時のサポート詐欺（事務対応ガイド 4-8-6(7)等、ガイドライン 10-3(2)、10-6(3)等）

サポート詐欺は、インターネット使用時に注意すべきものです。学校現場だけの問題ではありませんが、サポート詐欺に遭って遠隔操作ソフトをインストールしてしまい、PC 端末に保存された生徒の個人情報に漏えいのおそれが生じたという漏えい等事案も少なくありません。

【事案例】

- 公用 PC（又は私用 PC）でインターネットにつなぎ検索等をしていたところ、トロイの木馬への感染を示す警告画面と連絡先が表示された。連絡先へ電話し、指示に従って PC を操作。遠隔操作ソフトをインストールし、遠隔操作が行われた。

【発生原因】

- ・サポート詐欺とは知らずに、攻撃者の指示に従い、PC 端末に遠隔操作ソフトをインストールした。

【再発防止策例】

- ・インターネット閲覧用と業務用で、PC 端末を分ける。
- ・職員への注意喚起・事案共有。
- ・資産管理ソフトの導入（遠隔操作ソフトダウンロード URL をアクセス禁止リストに入れる等）。
- ・一般ユーザーはソフトウェアをインストールできないようにする措置を導入。

(7) 置き忘れ（事務対応ガイド 4-8-5(6)(9)等、ガイドライン 10-3(2)、10-5(1)(3)等）

学校現場では、教職員が、職員室、教室、体育館等、多くの場所に移動して執務を行うため、紙媒体の置き忘れが生じやすい環境です。置き忘れが生じた場合、生徒に閲覧させることが予定されていない情報を閲覧されてしまう可能性があり、個人情報の漏えい等事態が生じやすくなります。

【事案例】

- 学年集会が行われた場所に生徒の家庭環境等を含む個人情報が記載された紙媒体を置き忘れたところ、生徒がスマホで撮影した。
- 教室の教卓上に生徒の個人情報が記載された資料を置き忘れたところ、生徒が閲覧した。
- 面談を教室で実施した際、生徒用の机の中に家庭環境調査簿を置き忘れたところ、生徒が閲覧した。

【発生原因】

- ・紙媒体の置き場所に関する管理不備。

【再発防止策例】

- ・家庭環境調査簿は職員室外に持ち出さない。
- ・職員打合せ等で、個人情報が含まれている書類の取扱いについて再度確認する。
- ・生徒情報が記載された文書を執務室外に持ち出す際には、封筒等に格納して厳封する。

(8) 誤廃棄（事務対応ガイド 4-8-5(6) (9) 等、ガイドライン 10-3(2)、10-5(1) (3) 等）

誤廃棄は学校現場に限らず生じる事象ですが、学校では、健康診断票、学習用教材、指導要録の誤廃棄等の事案があります。

【事案例】

- 廃棄書類をシュレッダー廃棄した際、生徒の健康診断票も誤って廃棄してしまった。
- 過去の指導要録が所在不明であるが、おそらく誤廃棄した可能性が高い。

【発生原因】

- ・紙媒体の管理不備。

【再発防止策例】

- ・所定の場所への保管を徹底する。
- ・研修において、全職員に事案や個人情報の適切な取扱いについて周知する。
- ・書類使用後は速やかに保管場所に返却することを徹底する。

(9) サイバー攻撃等による不正アクセス事案（事務対応ガイド 4-8-6(1) (2) (7) 等、ガイドライン 10-6(1) (2) (3) 等）

サイバー攻撃等の外部の第三者による不正アクセスによる漏えい等事案は、民間の個人情報取扱事業者においても頻繁に起きているものです。学校現場では、アカウントの乗っ取り事案が多く見受けられるため、多要素認証等により防御を行う対策が考えられます。

【事案例】

- クラウドストレージサービスを利用していたところ、職員のアカウントが、第三者に不正に利用され、ファイルの閲覧、操作、ダウンロード等が行われた。
- クラウド型学習支援システムの管理用アカウントが攻撃者に不正に利用され、個人情報が漏えいした。

【発生原因】

- ・ID 及びパスワードの管理に問題があった。
- ・初期パスワードからの変更がなされていなかった。

【再発防止策例】

- ・多要素認証の導入。
- ・特に配慮を要すべき個人情報の保管場所と運用方法を再確認。
- ・重要な個人情報の保管場所について監査を実施。
- ・より高度なセキュリティレベルで運用可能なシステムへの移行。
- ・セキュリティ設定を再チェックする。
- ・セキュリティ意識向上のための研修の実施。

(10) 不正の目的による漏えい等事案（サイバー攻撃によるもの以外）（事務対応ガイド 4-8-6(1) (2) (7) 等、ガイドライン 10-3(2) (5)、10-6(1) (2) 等）

学校関係者ではない第三者による不正アクセス事案以外に、生徒や教職員による不正アクセスや不正な持ち出しによる漏えい等事案も少なからず発生しています。教職員だけでなく生徒に対する情報モラル教育も軽視できない状況が見受けられます。

【事案例】

- 教員が所持していた生徒用アカウント一覧表を生徒が不正に入手し、他の生徒のアカウントに不正アクセスした。
- 教員が校務用 PC の管理を生徒に任せ、PC のパスワードを教えていたところ、生徒が教員だけしか見てはいけない資料を閲覧した。
- 生徒が、教員の ID・パスワードを不正に利用し、個人情報にアクセスした。
- 授業資料をプロジェクターに投影させた際、教員専用のデータ保存領域のアクセスコードがプロジェクターに表示されたため、これを生徒に閲覧・利用された。
- 校務員が、生徒の個人情報が記載されている教員用の資料を無断でコピーし、生徒に閲覧させた。
- 教員が退職時に生徒のデータを不正に持ち出した。

【発生原因】

- ・個人情報が記載されている紙媒体の管理の不備。
- ・ID 及びパスワードの管理の不備。
- ・生徒や教職員の情報モラルの問題。

【再発防止策例】

- ・授業関係資料と生徒の個人情報の保存領域の分離と運用の徹底。
- ・ログイン ID・パスワードの厳正な取扱いの徹底。
- ・アカウント管理体制の見直しとルールの明文化。
- ・パスワード等のデータの印刷やコピーの禁止。
- ・教員に対する情報リテラシー教育等の実施。
- ・生徒に対する情報モラル教育の推進。

以 上