教育データの利活用に係る留意事項

文部科学省

第１版（令和５年３月）

目次

Ⅰ. 本留意事項について

本留意事項は、教育委員会・学校において教育データの利活用が進む中で、セキュリティや個人情報等に関して心配の声があることを受け、教育データを利活用するに当たっての安全・安心を確保するために、教育委員会・学校が留意すべき事項を整理したものです。

１．取り扱う内容

本留意事項は、初等中等教育段階の**公立学校**の教職員、教育委員会の職員等が、児童生徒の教育データ（デジタルデータ）を取り扱う際に、留意すべきポイントをまとめています。

教育データには個人情報が含まれる場合がありますが、本留意事項においては、児童生徒を本人とする個人情報を対象としています（保護者や教職員等を本人とする個人情報は対象とはしていません。）。

なお、教育データを利活用するに当たって現時点で想定される留意点を整理したものであり、個人情報等の適正な取扱いに関して網羅的に整理したものではありません。今後、教育データの利活用が進むにつれて、新たな課題や、論点についての議論が深まっていくことも想定されます。そのため、本留意事項も改訂を行っていく予定です。

本留意事項は、個人情報の適正な取扱いを確保し、また初等中等教育段階の**公立学校**の教職員、教育委員会の職員等対象者の利用に資するものとするため、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。）の規定、「個人情報の保護に関する法律についてのガイドライン（行政機関等編）」[1]（個人情報保護委員会）（以下、「ガイドライン」といいます。）、「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）」[2]（個人情報保護委員会）（以下、「事務対応ガイド」といいます。）、「個人情報の保護に関する基本方針」[3]（平成 16 年４月２日閣議決定、令和４年４月１日一部変更）（以下、「基本方針」といいます。）及び「実証事業ガイドライン（こどもに関する各種データの連携にかかる留意点等）」[4]（デジタル庁）等を参考にしつつ、個人情報保護委員会事務局から助言を受けたうえで作成したものです。

なお、個人情報保護法の対象規定が一部異なることから、国立大学法人や公立大学法人の設置する学校及び私立の学校については、今回の留意事項の対象とはしていません。

２．構成

本留意事項は、教育データ利活用の目的について説明した後、個人情報の取扱い等、安全・安心に教育データを取り扱う際に留意すべき事項について解説しています。加えて、教育データを利活用する際のよくある質問について Q&A 形式で解説しています。

---

[1] https://www.ppc.go.jp/personalinfo/legal/guidelines_administrative/
[2] https://www.ppc.go.jp/files/pdf/220428_koutekibumon_jimutaiou_guide_shinkyu.pdf
[3] https://www.ppc.go.jp/files/pdf/20220401_personal_basicpolicy.pdf
[4] https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/e91b13a9-fcee-4144-b90d-7d0a5c47c5f0/2f9dd9b9/20221221_news_children_outline_01.pdf

II.　教育データ利活用の目的

１．教育データの利活用はなぜ必要なのか

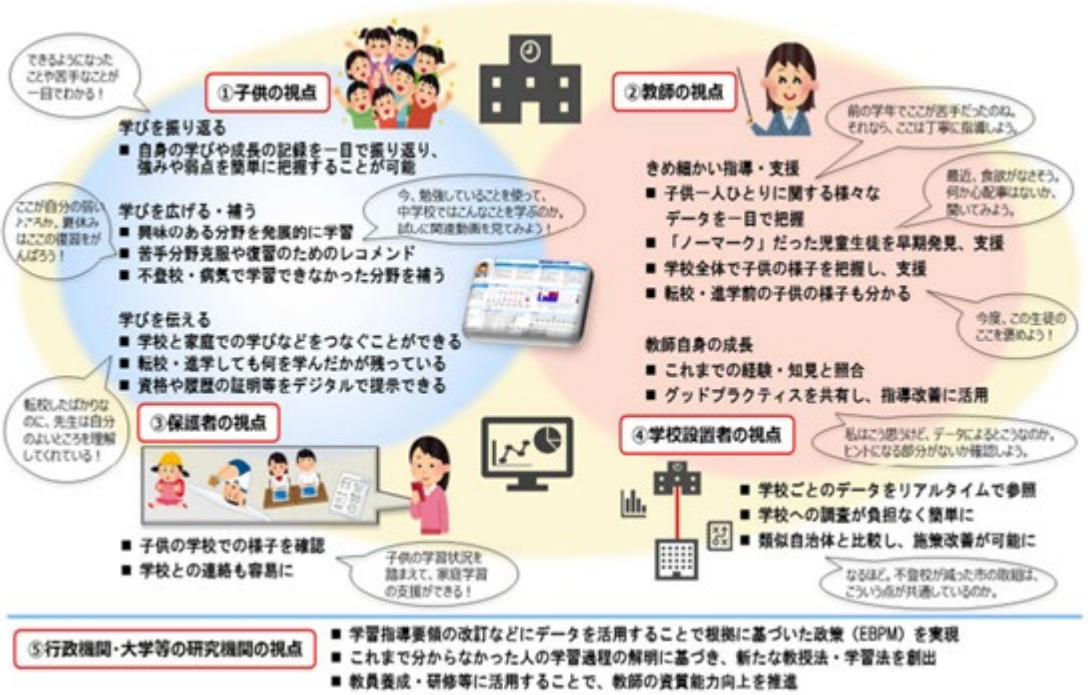
「教育データの利活用」と聞くと、「今、なぜ教育データの利活用が必要なのか。」、「教育データを利活用するとどのようなよいことがあるのか。」等の疑問がわいてくる方もいらっしゃるのではないでしょうか。

教育データを利活用する目的は、端的に言えば、全ての子供一人一人の力を最大限に引き出すためのきめ細かい支援を可能にすることです。この目的の達成に向けて、主体ごとにデータの利活用の具体的なイメージを挙げると以下のとおりです。

児 童 生 徒：これまでの自らの学びを振り返ったり、学びを広げたり、伝えたりすることが可能になります。
教　　師：よりきめ細かい指導や支援が可能となり、自身の経験や知見を照合することで自身の成長にもつながります。
保　護　者：子供の学校での様子を確認する等の学校との連携が容易となります。
学校設置者：類似の地方公共団体との比較や施策の改善がより容易となります。
研究機関等：具体的な個人等を特定できないデータを大学等の研究で利活用することで根拠に基づいた政策立案やより効果的な教授法・学習法の創出等、我が国全体の教育水準の向上につながることも期待されています。

このように、教育データを利活用することで、児童生徒、教師、学校設置者等の可能性を最大限に引き出すことが可能となります。

これまでも学校ではアナログな形でデータの活用等は行われていました。一方、GIGA スクール構想の推進により児童生徒１人１台端末が整備され、学校における端末を使用した学習が急速に普及してきています。この端末を活用した学習によって、例えば端末の利用ログやデジタルドリルの回答時間等、紙を活用した学習では得られなかった児童生徒の学びに関するデジタルデータが利活用できるようになっています。このため、上記の目的を達成していくために教育データの利活用が求められているのです。



図表１　教育データの利活用の将来像

（出典）「教育データの利活用に係る論点整理（中間まとめ）」文部科学省（令和３年３月）[5]

教育データの利活用については、文部科学省が「教育データの利活用に係る論点整理」[6]（令和３年３月）において教育データの定義、目的、原則や利活用イメージ等を示すとともに、デジタル庁・総務省・経済産業省・文部科学省が「教育データ利活用ロードマップ」[7]（令和４年１月）において学校内外における教育データの利活用に向けた論点や方向性を公表しているほか、「デジタル社会の実現に向けた重点計画」[8]（令和４年６月７日閣議決定）に記載される等、政府全体において推進する方針が打ち出されています。

２．本留意事項のねらい

上記のように、教育データの利活用は、子供の資質・能力の育成等で大きな役割を果たすことになるため、教育委員会・学校において教育データの利活用を推進していくことが求められています。

一方、各地方公共団体において教育データの利活用が始まりつつある中で、デジタルデータは複製や移転等が容易であることもあり、個人情報の適正な取扱いの確保やプライバシー

[5] 「教育データの利活用に係る論点整理（中間まとめ）」文部科学省（令和３年３月）（https://www.mext.go.jp/content/20210331-mxt_syoto01-000013887_1.pdf）の「３．教育データの利活用の目的（将来像の具体的イメージ）」

[6] https://www.mext.go.jp/content/20210331-mxt_syoto01-000013887_1.pdf

[7] https://www.digital.go.jp/assets/contents/node/information/field_ref_resources/0305c503-27f0-4b2c-b477-156c83fdc852/20220107_news_education_01.pdf

[8] https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/d130556b/20220607_policies_priority_outline_05.pdf

の保護の観点からデータを利活用することへの心配の声があります。

この心配は、「データ利活用はどこまで何が許されているか分からない」等の不安感に起因すると考えられます。このまま漠然と不安な状態だと、データの利活用を全く行わなかったり、データの利用を必要以上に制限したりする等、データの利活用がしづらい状態になってしまい、可能なはずの支援もできない状況となってしまいます。

このため、今回、文部科学省において、教育データ利活用に当たって、各教育委員会・学校において教育データの利活用を進めていく際の参考として、安全・安心を確保する観点から留意すべきポイント等をまとめました。

教育委員会・学校において、教育の質の向上のために教育データを利活用していく過程で、必要な場面に応じて、本留意事項を活用し、安全・安心に教育データを利活用いただきたいと思います。

【コラム１】教育データの利活用の参考となる考え方

児童生徒の権利については、国連で「子どもの権利条約」[9]が採択されています。ここでは「子どもにとって最もよいこと」等の４つの原則や、「児童の最善の利益が主として考慮されるものとする」こと、「すべての児童に対し、教育及び職業に関する情報及び指導が利用可能であり、かつ、これらを利用する機会が与えられる」こと等が定められています[10]。

加えて、児童生徒の「デジタル・シティズンシップ」という考え方があります。デジタル・シティズンシップとは、今後、児童生徒自身がデジタルデータを日常的に道具として活用していく際に必要となる、デジタル技術の利用を通じて社会に積極的に関与し、参加する能力のことです。

加えて、児童生徒の個人情報の適正な取扱いの確保についても配慮する必要があります。個人情報の取扱い一般については、OECD（Organisation for Economic Co-operation and Development：経済協力開発機構）が「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」[11]を、EU（European Union：欧州連合）ではGDPR[12]（General Data Protection Regulation：一般データ保護規則）を定めています。また、日本でも「個人情報等の適正な取扱いに関係する政策の基本原則」（以下、「政策基本原則」といいます。）[13]が定められ、取扱いの安全性、本人関与の実効性、取扱いに関する透明性と信頼性等が７つの原則とされました。

---

[9] 「子どもの権利条約」（https://www.unicef.or.jp/kodomo/kenri/1_1j8j.htm）

[10]国連・子どもの権利委員会では「デジタル環境との関連における子どもの権利についての一般的意見25号(2021年)」を発表しています。

[11]「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」（https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2)ここでは「１ 収集制限の原則」、「２ データ内容の原則」、「３ 目的明確化の原則」、「４ 利用制限の原則」、「５ 安全保護の原則」、「６ 公開の原則」、「７ 個人参加の原則」、「８ 責任の原則」の８原則を定めています。

[12]「General Data Protection Regulation」(https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679)ここでは「１ 個人データの取扱い」の「a 適法性、公正性及び透明性」、「b 目的の限定」、「c データの最小化」、「d 正確性」、「e 記録保存の制限」、「f 完全性及び機密性」、「２ 管理者のアカウンタビリティ」等が定められています。

[13] 「個人情報等の適正な取扱いに関係する政策の基本原則」個人情報保護委員会（令和４年５月 25 日）(https://www.ppc.go.jp/files/pdf/kihongensoku.pdf)。「１ 個人情報等の取扱いの必要性・相当性」、「２ 個人情報等の取扱いに関する適法性」、「３ 個人情報等の利用目的との関連性・利用の適正性」、「４ 個人情報等の取扱いに関する外延の明確性」、「５ 個人情報等の取扱いの安全性」、「６ 個人情報等に係る本人関与の実効性」、「７ 個人情報等の取扱いに関する透明性と信頼性」の７つの原則が定められています。

III.　総論編（教育データを利活用する際に気を付けること）

１．個人情報の適正な取扱い

１．１ 個人情報を取り扱う際の基本理念

教育委員会・学校において教育データを取り扱う場合には、個人情報等の適正な取扱いを確保することが必要です。個人情報の取扱いに当たっては、個人情報の保護と有用性に関する個人情報保護法の考え方を十分に踏まえて、個人情報の保護と適正かつ効果的な活用のバランスを考慮した取組みが求められます。

個人情報の適正な取扱いに当たっては、公立学校の教育データについて、学校の組織編制、教育課程、学習指導、生徒指導及び職業指導といった法令（条例を含みます。以下同じ。）[14]に定める所掌事務や業務を遂行するために必要な場合に限って保有したうえで、個人情報保護法における利用目的の特定及び明示、変更等の整理を行う必要があります。

なお、個人情報の取扱いに当たっては個人情報保護法[15]に準拠していれば十分というわけではなく、プライバシーの保護も求められます。個人情報保護法第３条においては、個人情報がプライバシーを含む個人の人格と密接な関連を有するものであり、個人が「個人として尊重される」ことを定めた憲法第 13 条の下、慎重に取り扱われるべきことを示すとともに、個人情報を取り扱う者は、その目的や態様を問わず、このような個人情報の性格と重要性を十分認識し、その適正な取扱いを図らなければならないとの基本理念を示しています。

詳細は、基本方針[16]を参照してください。

〇個人情報の保護に関する基本方針（平成16年4月２日閣議決定、令和4年4月１日一部変更）

１ 個人情報の保護に関する施策の推進に関する基本的な方向

（２）法の基本理念と制度の考え方

法第３条は、個人情報がプライバシーを含む個人の人格と密接な関連を有するものであり、個人が「個人として尊重される」ことを定めた憲法第 13 条の下、慎重に取り扱われるべきことを示すとともに、個人情報を取り扱う者は、その目的や態様を問わず、このような個人情報の性格と重要性を十分認識し、その適正な取扱いを図らなければならないとの基本理念を示している。

行政機関、地方公共団体の機関、独立行政法人等、地方独立行政法人及び個人情報取扱事業者等の個人情報等を取り扱う各主体（以下、「各主体」という。）においては、この基本理念を十分に踏まえるとともに、官民や地域の枠又は国境を越えた政策や事業活動等において、以下に掲げる考え方を基に、法の目的を実現するため、個人情報の保護及び適正かつ効果的な活用の促進に取り組む必要がある。

２ 国が講ずべき個人情報の保護のための措置に関する事項

[14] 例えば、教育委員会・学校においては、地方教育行政の組織及び運営に関する法律（昭和 31 年法律第 162 号）や学校教育法（昭和 22 年法律第 26 号）等の法令が含まれます。

[15] そのほか各地方公共団体において、個人情報保護法の規定に基づき策定される個人情報保護法施行条例において、「条例要配慮個人情報」（個人情報保護法第 60 条第５項）を規定されていることがあります。

[16] https://www.ppc.go.jp/files/pdf/300612_personal_basicpolicy.pdf

（1）各主体における個人情報の保護等個人情報等の適正な取扱いの推進

③ 官民や地域の枠を越えて各主体が取り扱う個人情報の保護等個人情報等の適正な取扱いの推進

官民及び地域の枠を越えたデータ利活用として、健康・医療・介護、教育、防災及びこども等の準公共分野、スマートシティ等の相互連携分野や公的基礎情報データベース（ベース・レジストリ）の整備等については、法の規律が異なる各主体間における個人情報等のデータ連携等が行われることとなる。

各主体間における個人情報等のやりとりがより複層的になることにより、個人情報等の取扱いについて責任を有する主体が従来以上に不明確になるリスクがあり、これに対応した制度設計や運用を行う必要がある。そのため、個人情報等を取り扱う各主体のみならず、データ連携等を推進する者においても、データガバナンス体制の構築等に取り組むことが重要である。

１．２ 教育委員会・学校が取り扱うこととなる個人情報等

１．２．１ 個人情報とは

個人情報保護法における「個人情報」とは、生存する個人に関する情報で、以下の①又は②に該当するものをいいます。

①当該情報に含まれる氏名等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものも含まれる。）

②個人識別符号が含まれるもの

個人情報には、それのみで特定の個人を識別できる氏名等の情報のみならず、他の情報と容易に照合することができ、それにより特定の個人を識別できる生年月日や住所等の情報も含まれます。

なお、ここでいう「他の情報と容易に照合することができ」とは、地方公共団体の機関[17]において通常の事務や業務における一般的な方法で、他の情報と容易に照合することができる状態をいいます。

教育委員会が所管する公立学校については、個々の学校自体が地方公共団体の機関に該当するのではなく、当該学校を所管する教育委員会が地方公共団体の機関に該当します。そのため、この「他の情報と容易に照合することができ」る範囲については、基本的に学校単位

[17] 個人情報保護法において、「地方公共団体の機関」とは、知事、市区町村長、教育委員会、公安委員会、選挙管理委員会、監査委員等の執行機関のほか、公営企業管理者（病院事業管理者を含む。）、警察本部長及び消防長等が該当するとされています。（事務対応ガイド３－１－１）

ではなく教育委員会単位で考える必要があります[18]。

個人情報に該当するかどうかを判断する際、その情報が公開されているかどうかは関係しません。したがって、ある個人が自らインターネットやSNSに公開している情報であっても、それが特定の個人を識別できるような情報であれば、個人情報に該当します。

なお、②の「個人識別符号」の代表的なものとしては、個人番号（マイナンバー）[19]や健康保険証の記号・番号、パスポート番号があります。また、ソフトウェア等本人を認証できるようにする容貌や指紋も、生体情報を変換した符号として「個人識別符号」に該当します。その他にどのような情報が「個人識別符号」に該当するかは、脚注を参照してください[20]。

また、地方公共団体職員が職務上作成し、又は取得した個人情報であって地方公共団体職員が組織的に利用するものとして、当該地方公共団体が保有しているもののうち、行政文書等に記録されているものを「保有個人情報[21]」といいます。

---

[18] 例えば、ある情報について、学校内では氏名等と照合することが不可能で、特定の個人を識別することが困難であるとしても、所管の教育委員会に問い合わせる等の方法により容易に照合することができ、特定の個人を識別することができる場合は、個人情報に該当します。また、同様に、教育委員会内では照合することが不可能でも、学校において照合することができる場合は、個人情報に該当します。

[19] マイナンバーの取扱いは法令（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号））により用途が厳しく制限されているため、学校で取り扱うことは基本的に想定されず、教育委員会で取り扱う場合も限られています。

[20] 個人識別符号とは、単体で特定の個人を識別することができるものとして政令（個人情報の保護に関する法律施行令（平成15年政令第507号））で定められた文字、番号、記号その他の符号をいいます（個人情報保護法第２条第２項）。本文で記載したほかに「個人識別符号」の代表的なものは、以下の身体の特徴のいずれかを電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、特定の個人を識別するに足りるものとして個人情報保護委員会規則で定める基準に適合するものです。「細胞から採取されたデオキシリボ核酸（別名 DNA）を構成する塩基の配列」「虹彩の表面の起伏により形成される線状の模様」「発声の際の声帯の振動」「声門の開閉並びに声道の形状及びその変化」「歩行の際の姿勢及び両腕の動作、歩幅その他の歩行の態様」「手のひら又は手の甲若しくは指の皮下の静脈の分岐及び端点によって定まるその静脈の形状」「指紋又は掌紋」等

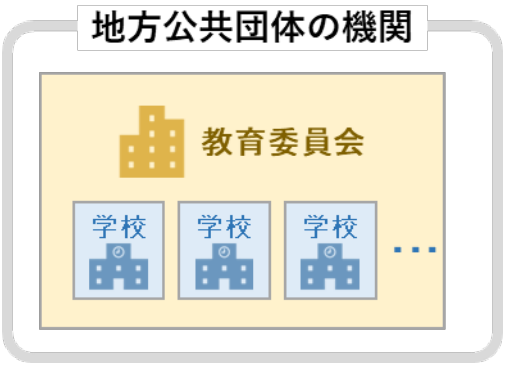
[21] 個人情報保護法第60条第１項

【コラム２】個人情報保護法における「地方公共団体の機関」とは？

個人情報保護法において、「地方公共団体の機関」とは、知事、市区町村長、教育委員会、公安委員会、選挙管理委員会、監査委員等の執行機関のほか、公営企業管理者（病院事業管理者を含む。）、警察本部長及び消防長等が該当するとされています。

この「教育委員会」には、教育委員会そのものだけでなく、教育委員会とその所管する学校全てが含まれます。

この際、個々の学校自体がそれぞれ一つの「地方公共団体の機関」となるわけではありません。学校は、その学校を所管する教育委員会の中の一組織であり、教育委員会と所管する学校全体で一つの「地方公共団体の機関」となります。



図表２　個人情報保護法における「地方公共団体の機関」

１．２．２ 教育委員会・学校における個人情報

教育委員会・学校においては、例えば以下のようなデータは、基本的に個人情報に該当すると考えられます。個人情報のうち、教育委員会や学校の職員が職務上作成し又は取得した個人情報であって、組織的に利用するものとして教育委員会や学校が保有しているもののうち、行政文書等に記録されているものについては、保有個人情報に該当します。

児童生徒の
- 氏名

児童生徒の氏名と紐付く
- 年組、学籍番号
- 住所、生年月日、身長、体重
- 出欠席情報
- １人１台端末の操作履歴
- テストの評点
- 学習アプリの回答結果、回答時間

※あくまで一例

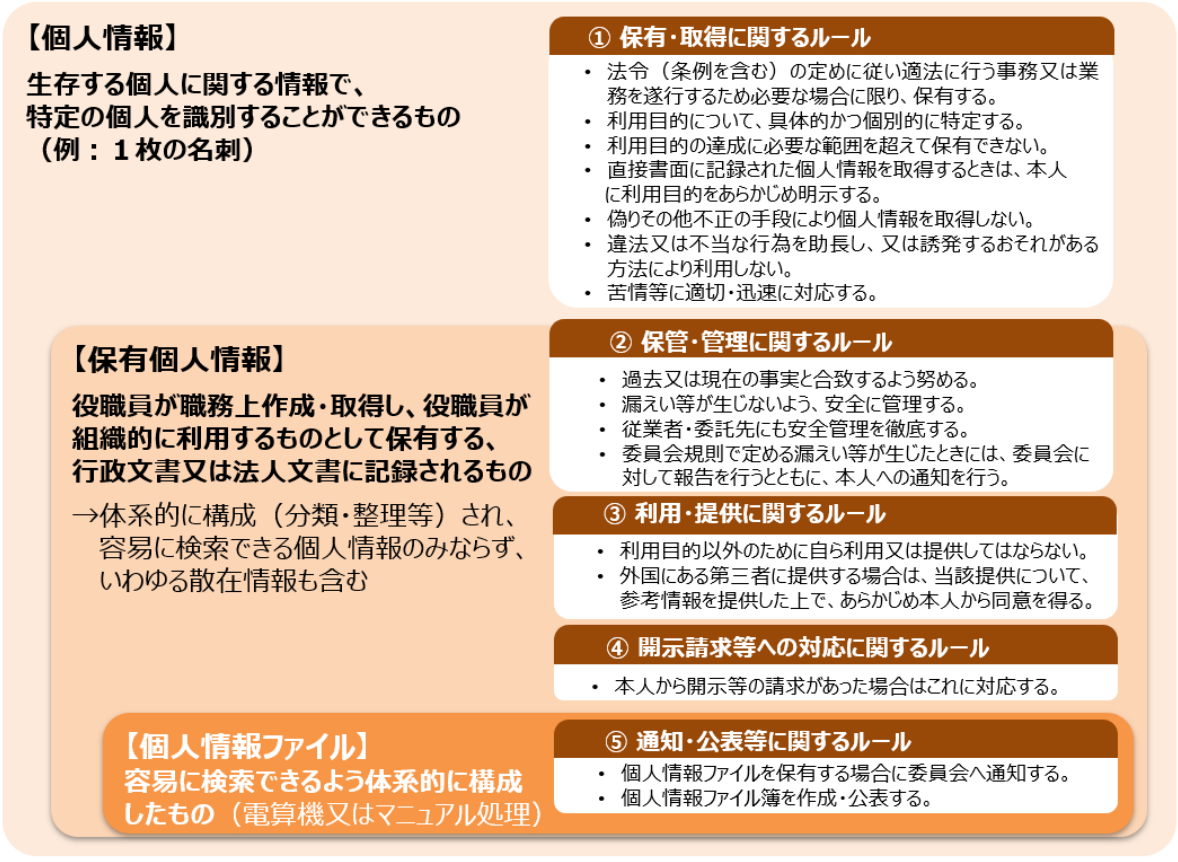
１．３ 個人情報の取扱い区分に応じた整理

１．３．１ 個人情報の取扱いの概要

それでは、具体的に、個人情報を取り扱う際に遵守すべき個人情報保護法の規定について確認していきます。教育委員会・学校については、個人情報保護法上「地方公共団体の機関」[22]に該当し、行政機関等の義務等に関する個人情報保護法第５章の規定を遵守する必要があります。

代表的な規定の内容は、図表３のとおりです。

例えば、「個人情報を保有する際には利用目的を具体的かつ個別的に特定すること」「特定した利用目的以外のために自ら利用又は提供してはならないこと」「苦情等に適切・迅速に対応すること」「本人からの開示等の請求があった場合はこれに対応すること」等、個人情報を保有・取得するときから、保管・管理、利用・提供するときにかけて、様々なルールが決められています。



図表３　個人情報保護法第５章の主な規定

[22] 個人情報保護法第２条第 11 項

１．３．２ 個人情報の保有

また、地方公共団体の機関が個人情報を保有・取得・利用・提供する際には、図表４の規律が適用されます。これらの規定は、教育委員会・学校にも適用されます。

保有に関する規律

- 行政機関等は、**法令（条例を含む）の定めに従い適法に行う事務又は業務を遂行するため必要な場合に限り**、個人情報を保有することができる。（法第61条第1項）
- 行政機関等は、**個人情報の利用目的について**、当該個人情報がどのような事務又は業務の用に供され、どのような目的に使われるかをできるだけ**具体的かつ個別的に特定しなければならない**。（法第61条第1項）
- 行政機関等は、**特定された利用目的の達成に必要な範囲を超えて、個人情報を保有してはならない**。そのため、個人情報が保有される個人の範囲及び個人情報の内容は、利用目的に照らして必要最小限のものでなければならない。（法第61条第2項）

取得・利用・提供に関する規律

- 行政機関等は、**本人から直接書面（電磁的記録を含む。）に記録された当該本人の個人情報を取得するとき**には、本人が認識することができる適切な方法により、**本人に対し、利用目的をあらかじめ明示しなければならない**。（法第62条）
- 行政機関の長等は、**違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない**。（法第63条）
- 行政機関の長等は、**偽りその他不正の手段により個人情報を取得してはならない**。（法第64条）
- 行政機関の長等は、利用目的の達成に必要な範囲内で、**保有個人情報が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**。（法第65条）
- 行政機関の長等は、「法令に基づく場合」を除き、**利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない**。（法第69条第1項）

図表４　行政機関等が個人情報を保有・取得・利用・提供する際の規律（原則）

以上のように、地方公共団体の機関が個人情報を保有するに当たっては、法令の定める所掌事務又は業務を遂行するために必要な場合に限り、かつ利用目的を適切に特定する必要があり、その特定した利用目的の範囲内で保有個人情報を利用・提供することが原則です[23]。

例外については、「Ⅲ．総論編１．３．３」において解説しています。

（１）　法令の定める所掌事務又は業務の整理

地方公共団体の機関が個人情報を保有する場合は、法令の定める所掌事務又は業務を遂行するために必要な場合に限り、利用目的をできる限り特定しなければならないと規定されています。つまり、地方公共団体の機関は、法令の定める所掌事務又は業務のうち、個人情報を保有することによって遂行しようとする具体的な事務又は業務の遂行に必要な場合に限り、個人情報を保有することができます。そのため、まず、利用目的を特定する前に、「法令の定める所掌事務または業務」についての整理が必要となります。

[23] 個人情報保護法第 61 条第１項、第 69 条第１項

「法令の定める所掌事務又は業務」については、事務対応ガイドに以下のとおり記載されています。

○事務対応ガイド４－１（保有に関する制限（個人情報保護法第 61 条））より抜粋

各行政機関等の所掌事務又は業務には、当該行政機関等の設置の根拠となる法令において「所掌事務」や「業務の範囲」を定める条文に列挙されている事務又は業務のほか、「権限」を定める条文上で規定されている事務又は業務や、作用法上規定されている事務又は業務が含まれる。地方公共団体においては、地方自治法第２条第２項に規定する「地域における事務」もこれに含まれる。また、地方自治法以外にも、地方公共団体の機関の職務権限については地方教育行政の組織及び運営に関する法律（昭和 31 年法律第 162 号）、警察法（昭和 29 年法律第 162 号）、地方公営企業法（昭和 27 年法律第 292 号）等の各法律に規定されている。なお、所掌事務又は業務の根拠となる法第 61 条第１項の「法令」には、条例が含まれるほか、規則等の地方公共団体が法令に基づき定める法規が含まれる（ガイドライン５－１（保有に関する制限）を参照のこと。）。

その一例として、以下に「地方教育行政の組織及び運営に関する法律」の第 21 条を抜粋しています。

○地方教育行政の組織及び運営に関する法律（昭和 31 年法律第 162 号）（抄）

（教育委員会の職務権限）

第 21 条　教育委員会は、当該地方公共団体が処理する教育に関する事務で、次に掲げるものを管理し、及び執行する。

一　教育委員会の所管に属する第三十条に規定する学校その他の教育機関（以下「学校その他の教育機関」という。）の設置、管理及び廃止に関すること。

二　教育委員会の所管に属する学校その他の教育機関の用に供する財産（以下「教育財産」という。）の管理に関すること。

三　教育委員会及び教育委員会の所管に属する学校その他の教育機関の職員の任免その他の人事に関すること。

四　学齢生徒及び学齢児童の就学並びに生徒、児童及び幼児の入学、転学及び退学に関すること。

五　教育委員会の所管に属する学校の組織編制、教育課程、学習指導、生徒指導及び職業指導に関すること。

六　教科書その他の教材の取扱いに関すること。

七　校舎その他の施設及び教具その他の設備の整備に関すること。

八　校長、教員その他の教育関係職員の研修に関すること。

九　校長、教員その他の教育関係職員並びに生徒、児童及び幼児の保健、安全、厚生及び福利に関すること。

十　教育委員会の所管に属する学校その他の教育機関の環境衛生に関すること。
十一　学校給食に関すること。
十二　青少年教育、女性教育及び公民館の事業その他社会教育に関すること。
十三　スポーツに関すること。
十四　文化財の保護に関すること。
十五　ユネスコ活動に関すること。
十六　教育に関する法人に関すること。
十七　教育に係る調査及び基幹統計その他の統計に関すること。
十八　所掌事務に係る広報及び所掌事務に係る教育行政に関する相談に関すること。
十九　前各号に掲げるもののほか、当該地方公共団体の区域内における教育に関する事務に関すること。

（2）　利用目的の特定

地方公共団体の機関が個人情報を保有するに当たっては、法令の定める所掌事務又は業務を遂行するために必要な場合に限り、かつ、利用目的はできる限り特定しなければなりません[24]。

「その利用目的をできる限り特定」するとは、個人情報がどのような事務又は業務の用に供され、どのような目的に使われるかをできるだけ具体的かつ個別的に特定するということです。その際の利用目的は、具体的な利用行為が当該利用目的の範囲内であるか否か、合理的かつ明確に判断できるものでなければなりません[25]。

なお、特定した利用目的については、保有個人情報の開示を行う場合に開示請求者に対して通知しなければならないことから[26]、内部において適切に整理・管理する必要があります。そのため、利用目的の特定の方法として、利用目的について内部的に整理したものを文書化しておくといった対応等が考えられます。

また、地方公共団体の機関は、特定された利用目的の達成に必要な範囲を超えて、個人情報を保有してはならないとされています[27]。そのため、その個人情報が、利用目的の達成に必要がないと判断される場合には、廃棄・削除等の適切な対応が必要となります。

なお、教育委員会・学校における教育データについては、指導要録や出席簿等、学校教育法等の法令で保存期間が定められているものがあるため、それらについては法令に基づく保存期間を設定する必要があることに留意する必要があります。

[24] 個人情報保護法第 61 条第１項
[25] ガイドライン５－１
[26] 個人情報保護法第 82 条第１項
[27] 個人情報保護法第 61 条第２項

○学校教育法施行規則（昭和 22 年文部省令第 11 号）（抄）

第 28 条　学校において備えなければならない表簿は、概ね次のとおりとする。

一　学校に関係のある法令

二　学則、日課表、教科用図書配当表、学校医執務記録簿、学校歯科医執務記録簿、学校薬剤師執務記録簿及び学校日誌

三　職員の名簿、履歴書、出勤簿並びに担任学級、担任の教科又は科目及び時間表

四　指導要録、その写し及び抄本並びに出席簿及び健康診断に関する表簿

五　入学者の選抜及び成績考査に関する表簿

六　資産原簿、出納簿及び経費の予算決算についての帳簿並びに図書機械器具、標本、模型等の教具の目録

七　往復文書処理簿

1　前項の表簿（第二十四条第二項の抄本又は写しを除く。）は、別に定めるもののほか、五年間保存しなければならない。ただし、指導要録及びその写しのうち入学、卒業等の学籍に関する記録については、その保存期間は、二十年間とする。

2　学校教育法施行令第三十一条の規定により指導要録及びその写しを保存しなければならない期間は、前項のこれらの書類の保存期間から当該学校においてこれらの書類を保存していた期間を控除した期間とする。

（3）　利用目的の明示

地方公共団体の機関が、本人から直接書面（オンラインを含む。）に記録された当該本人の個人情報を取得するときは、あらかじめ、本人に対し、その利用目的を明示する必要があります。なお、本人から直接書面（オンラインを含む。）で取得しない場合には、利用目的を明示する必要はありません。

利用目的の明示の方法は、児童生徒本人にお便りやメール等であらかじめ示しておく方法のほか、教室における掲示や集会での説明等の口頭による方法も考えられますが、いずれにせよ、本人が利用目的を認識することができるよう、適切な方法により行うことが必要です。ホームページ等の端末の画面においてあらかじめ必要な情報を掲載しておく場合も考えられますが、この場合には、本人が送信ボタン等をクリックする前等にその利用目的が本人の目に留まるようその配置に留意することが望ましいとされています[28]。

もっとも、学校教育においては、保護者が、児童生徒を本人とする個人情報を含む教育データの利用目的を把握しておきたいと考えていることもあります。そのため、学校の実態や利用する個人情報の種類に応じて、保護者に対しても利用目的を明示することは、より丁寧な対応となります。

なお、利用目的を明示することにより他の権利利益を損なうおそれがある場合等、利用目

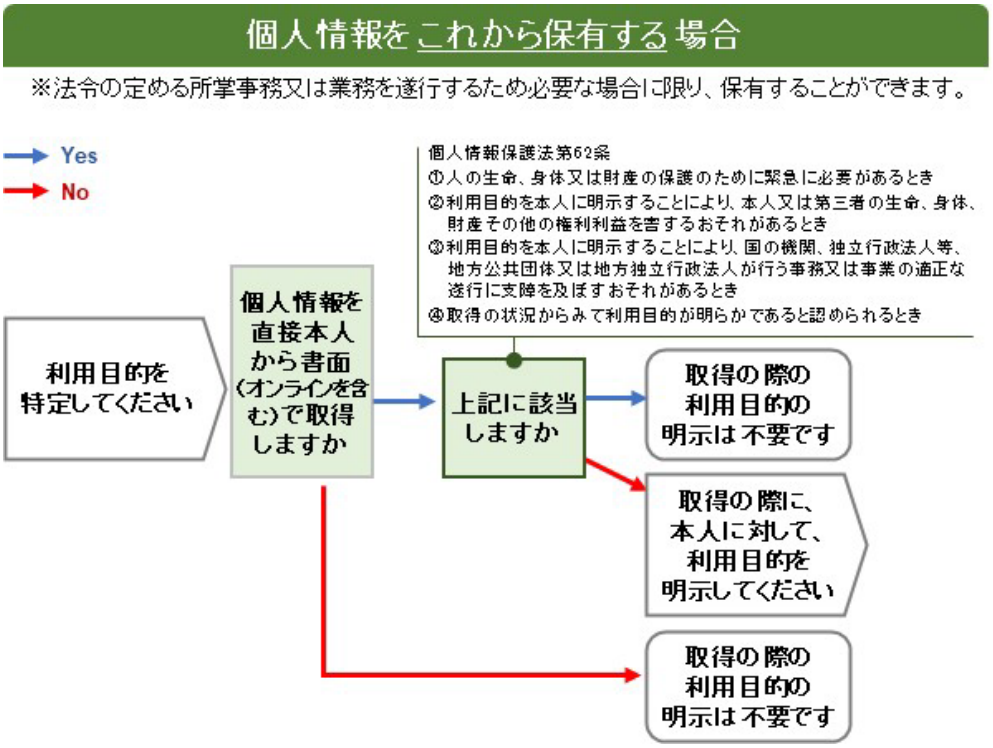
[28] 事務対応ガイド４－２－２

的の明示を義務付けることが適当でない場合や、利用目的が明らかである場合にまで、一律にあらかじめ利用目的を明示することは合理的でない場合があり、そのような場合の例外についても定められています。例外の詳細については、図表５を参照してください。

利用目的の明示の例外（個人情報保護法第 62 条第１号～第４号）
①　人の生命、身体又は財産の保護のために緊急に必要があるとき（第１号） ②　利用目的を本人に明示することにより、本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがあるとき（第２号） ③　利用目的を本人に明示することにより、国の機関、独立行政法人等、地方公共団体又は地方独立行政法人が行う事務又は事業の適正な遂行に支障を及ぼすおそれがあるとき（第３号） ④　取得の状況からみて利用目的が明らかであると認められるとき（第４号）

図表５　利用目的の明示の例外（個人情報保護法第 62 条第１号～第４号）

個人情報をこれから保有する場合の手続きについて、ここまでに説明した内容を整理すると、以下のフローチャートのようになります。

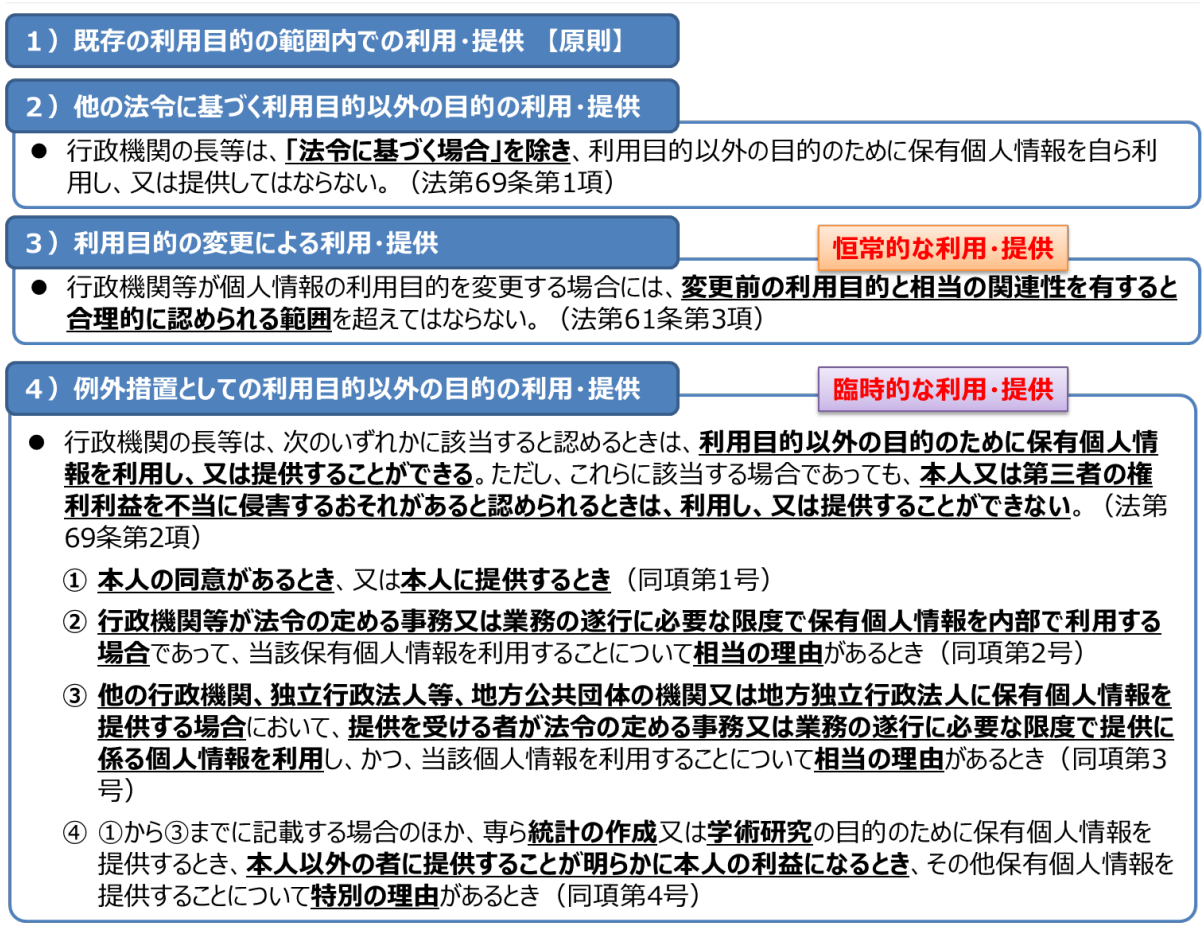


図表６　個人情報をこれから保有する場合の流れ（フローチャート）

１．３．３ 個人情報の取得・利用・提供

地方公共団体の機関が個人情報を保有するに当たっては、法令の定める所掌事務又は業務を遂行するために必要な場合に限り、かつ利用目的を適切に特定する必要があり、その特定した利用目的の範囲内で保有個人情報を利用・提供することが原則であるとされています[29]。

ただ、例外的に、以下の（２）（３）（４）に該当する場合には、既存の利用目的以外の目的で利用・提供することが認められます。



図表７　行政機関等が個人情報を保有・取得・利用・提供する際の規律（原則）

（１）　既存の利用目的の範囲内での利用・提供【原則】

「Ⅲ．総論編１．３．２」でも記載しているとおり、地方公共団体の機関において、個人情報は、特定した利用目的の範囲内で内部利用・外部提供することが原則とされています。なお、教育委員会・学校が内部利用するとは、利用目的を特定した教育委員会・学校の機関内部で利用することを指し、外部提供とは当該機関以外（同じ地方公共団体内部の別の行政機

[29] 個人情報保護法第 61 条第１項、第 69 条第１項

関等を含む。）への提供のことを指します。この場合において、例えば、教育委員会・学校内での利用は内部利用になりますが、教育委員会から首長部局への提供は外部提供に当たることとなります。

（２）　他の法令（条例は含みません。以下、１．３．３（２）において同じ。）に基づく利用目的以外の目的の利用・提供

地方公共団体の機関は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならないとされています[30]。

これは、個人情報が、特定された利用目的以外の目的のために利用・提供された場合、本人の予期しない利用・提供による不安・懸念を生じさせるのみならず、悪用によるプライバシーの侵害や財産上の権利侵害等をもたらす危険性を増大させるため、原則として利用目的以外の目的のための利用・提供を禁止しているという趣旨です。

しかし、法令に基づく場合は当該禁止の原則から除かれることとされています。具体的には、児童福祉法に基づく要保護児童対策地域協議会[31]等の法律に基づく連携体制が考えられますが、そのような体制の下で利用・提供が可能な個人情報の範囲等については、各法律において規定される連携体制の内容や連携によって達成される目的、連携に当たり必要な個人情報の内容や性質等を踏まえて、適切に判断される必要があります。

（３）　利用目的の変更による利用・提供

利用目的を変更せざるを得ない場合が生じることは一般に想定されるため、地方公共団体の機関の事務及び事業の適正かつ円滑な運営を図りつつ、個人の権利利益を保護し、利用目的に一定の柔軟性を持たせるために、利用目的の変更の規定が設けられています。

利用目的を変更する場合には、変更後の利用目的が変更前の利用目的と「相当の関連性」を有すると「合理的に認められる」範囲を超えて行ってはならないとされており[32]、ガイドラインにおいて以下のとおり考え方が示されているところです。

---

[30] 個人情報保護法第 69 条第１項
[31] 児童福祉法第 25 条の２
[32] 個人情報保護法第 61 条第３項

「相当の関連性」、「合理的に認められる」
「相当の関連性」： 当初の利用目的からみて、変更後の利用目的を想定することが困難でない程度の関連性を有することをいう[33]。 「合理的に認められる」： 社会通念上妥当であると客観的に認識されるとの趣旨であり、行政機関等の恣意的な判断による変更を認めるものではない[34]。

図表８　「相当の関連性」、「合理的に認められる」の考え方

なお、利用目的の変更は、当初の利用目的と変更後の利用目的を比較して、社会通念上、一般人の判断において、通常予期し得る限度と客観的に認められる範囲内をいい、どの程度の関連性を有するかは総合的に勘案して判断されます。

（４）　例外措置としての利用目的以外の目的の利用・提供

例外措置として、以下ア～ウのいずれかに該当する場合は、臨時的に利用目的以外の目的のために利用・提供を行うことができます。なお、利用目的以外の目的のための利用・提供を恒常的に行うことを個人情報の取得前から予定している場合は、そのような利用・提供が可能となるように利用目的を設定しておくべきです。

ア　利用目的以外の目的の利用・提供（本人の同意がある場合又は本人に提供する場合）

あらかじめ本人の同意がある場合においては、個人情報の利用目的以外の目的のための利用・提供を行うことができるとされています。この場合の本人の同意は、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法によらなければなりませんが、必ずしも書面によることを要しないため、口頭等でも取得することができます。

また、個人情報が利用目的以外の目的のために利用・提供されることについて本人が同意したことによって生じる結果について、未成年者等である本人が判断できる能力を有していない等の場合は、親権者又は法定代理人等から同意を得る必要があります。教育委員会・学校においては、こういった場面が多いと考えられます。本人が同意したことによって生じる結果について自分で理解・判断できると考えられる子供の具体的な年齢は、個人情報の種類や場面ごとに個別具体的に判断されるべきですが、一般的には 12 歳から 15 歳までとされています[35]。

---

[33] 事務対応ガイド４－２－１

[34] ガイドライン５－２－１

[35] 「法定代理人等から同意を得る必要がある子どもの具体的な年齢は、対象となる個人情報の項目や事業の性質等によって、個別具体的に判断されるべきですが、一般的には 12 歳から 15 歳までの年齢以下の子どもについて、法定代理人等から同意を得る必要があると考えられます。」（「「個人情報の保護に関する法律についてのガイドライン」に関する Q&A」個人情報保護委員会（令和４年５月）A１-62）。

なお、本人の同意があるときであっても、当該本人や第三者の権利利益を不当に侵害するおそれがあるときには利用目的以外の目的のために利用・提供することはできません[36]。

また、地方公共団体の機関の判断により本人に提供することは、利用目的以外の目的でも可能です。

イ　利用目的以外の目的の利用・提供（相当な理由がある場合）

利用目的以外の目的のための利用・提供をすることができない原則の例外として、

①地方公共団体の機関が法令の定める所掌事務又は業務の遂行に必要な限度で個人情報を内部で利用する場合であって、当該個人情報を利用することについて相当の理由があるとき[37]

② 他の行政機関、独立行政法人等、地方公共団体の機関又は地方独立行政法人に個人情報を提供する場合において、個人情報の提供を受ける者が、法令の定める事務又は業務の遂行に必要な限度で提供に係る個人情報を利用し、かつ、当該個人情報を利用することについて相当の理由があるとき[38]

が規定されています。

なお、いずれの場合も、本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、この限りでないとされています[39]。

「相当の理由があるとき」とは、地方公共団体の機関の恣意的な判断を許容するものではなく、少なくとも、社会通念上、客観的にみて合理的な理由があることが求められます。相当の理由があるかどうかは、個人情報の内容や当該個人情報の利用目的等を勘案して、地方公共団体の機関が個別に判断することとなりますが、例外的に利用目的以外の目的のための利用・提供が許容される場合について規定した趣旨から、例外としてふさわしい理由であることが求められます[40]。

以上を踏まえ、利用目的以外の目的の利用・提供を行う場合は、以下の観点について整理する必要があります。なお、①から④の観点については、全ての観点を考慮して検討することが求められます。

①当該内部利用及び外部提供が「臨時的」なものであること[41] ②法令の定める所掌事務又は業務の遂行に「必要な限度」であること[42]

[36] 例えば、本人の同意があったとしても、その同意が強制されたものである場合、保有個人情報の中に本人の情報の他に第三者の情報も含まれている場合等は、本人又は第三者の権利利益を不当に侵害するおそれがあるものと考えられます。
[37] 個人情報保護法第 69 条第２項第２号
[38] 個人情報保護法第 69 条第２項第３号
[39] 個人情報保護法第 69 条第２項柱書
[40] 事務対応ガイド４－５－２
[41] 事務対応ガイド４－２－１
[42] 個人情報保護法第 69 条第２項第２号及び第３号

③当該個人情報を内部利用及び外部提供することについて「相当の理由」があるとき[43]
④本人又は第三者の権利利益を不当に侵害するおそれがないこと[44]

ウ　利用目的以外の目的の提供（統計作成･学術研究等）

利用目的以外の目的のための利用・提供をすることができない原則の例外としては、①専ら統計の作成又は学術研究の目的のために保有個人情報を提供するときや、②本人以外の者に提供することが明らかに本人の利益になるとき、③その他保有個人情報を提供することについて特別の理由があるときに利用目的以外の目的での外部提供が可能な場合があります。なお、いずれの場合も当該本人や第三者の権利利益を不当に侵害するおそれがあるときには利用目的以外の目的のために利用・提供することはできません。

①専ら統計の作成又は学術研究の目的のために保有個人情報を提供するときは、提供した保有個人情報が特定の個人が識別することができない形で用いられることが通常であり、個人の権利利益が侵害されるおそれが少なく、かつ、公共性も高いと考えられることから、利用目的以外の目的のための利用及び提供の原則禁止の例外としたものです[45]。

この場合の「統計情報」とは、複数人の情報から共通要素に係る項目を抽出して同じ分類ごとに集計して得られるデータであり、集団の傾向又は性質等を数量的に把握するものです[46]。統計情報は、特定の個人との対応関係が排斥されている限りにおいては、「個人に関する情報」に該当するものではありません。

また、②本人以外の者に提供することが明らかに本人の利益になるときや③特別の理由があるときについても外部提供が可能な場合があります。

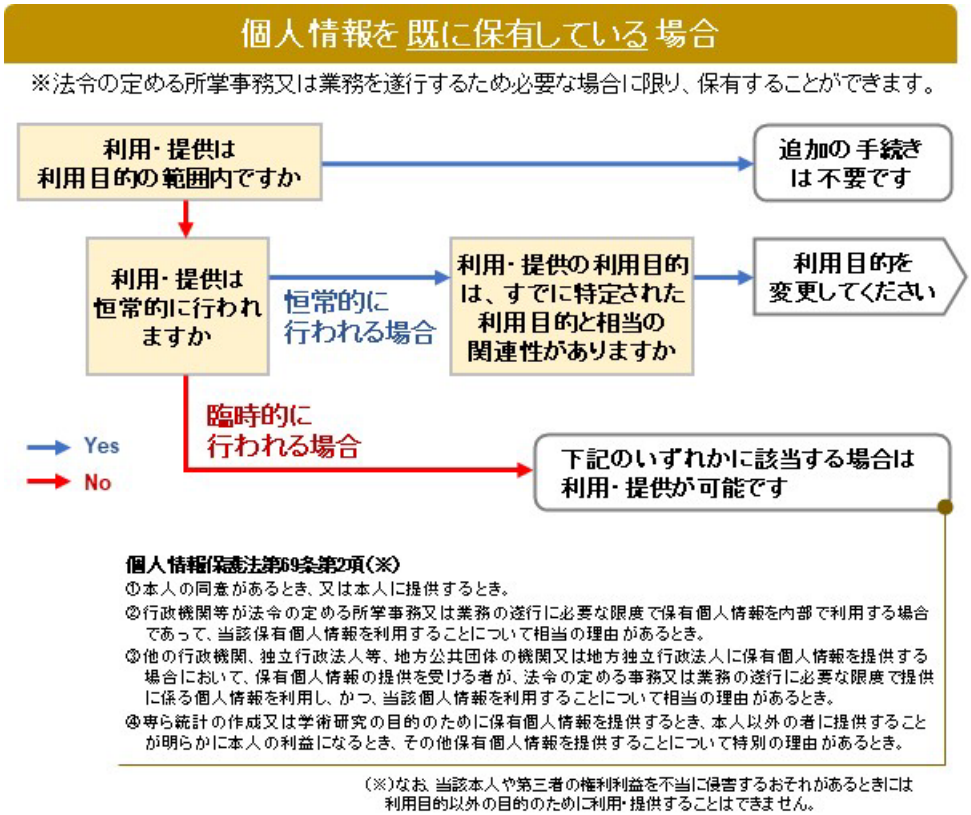
②本人以外の者に提供することが明らかに本人の利益になるときについては、緊急に輸血が必要な場合に当該個人の血液型を医師に知らせる場合等、本人の生命、身体又は財産を保護するために必要がある場合や、本人に対する金銭の給付、栄典の授与等のために必要がある場合等が含まれます。もっとも、適用の判断においては、個人情報を提供することの効果等を踏まえて、提供の必要性や相当性等について十分に考慮する必要があります。

③特別の理由については、本来地方公共団体の機関において厳格に管理すべき保有個人情報について、個人情報保護法第 69 条第２項第３号に規定する者（他の行政機関、独立行政法人等、地方公共団体の機関又は地方独立行政法人）以外の者に例外として提供することが認められるためにふさわしい要件として、個人情報の性質、利用目的等に則して、「相当の理由」よりも更に厳格な理由が必要です。具体的には、（ア）地方公共団体の機関に提供する場合と同程度の公益性があること（イ）提供を受ける側が自ら当該個人情報に相当する個人情報を取得することが著しく困難であること（ウ）提供を受ける側の事務が緊急を要すること

[43] 個人情報保護法第 69 条第２項第３号及び第３号
[44] 個人情報保護法第 69 条第２項柱書
[45] 事務対応ガイド４－５－２
[46] 事務対応ガイド３－２－７

（エ）当該個人情報の提供を受けなければ提供を受ける側の事務の目的を達成することが困難であること等の理由が必要となります[47]。

個人情報を既に保有している場合の手続きについて、ここまでに説明した内容を整理すると、以下のフローチャートのようになります。



図表９　個人情報を既に保有している場合の流れ（フローチャート）

１．４ 個人情報の取扱いの委託

個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないよう、必要な措置を講じる必要があります。また、契約書に、次の事項を明記するとともに、委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認する必要があります[48]。

○個人情報の取扱いを委託する際に契約書に明記すべき事項
①　個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等の義務

[47] 事務対応ガイド４－５－２、ガイドライン５－５－２
[48] 事務対応ガイド４－８－９

② 再委託の制限又は事前承認等再委託に係る条件に関する事項
③ 個人情報の複製等の制限に関する事項
④ 個人情報の安全管理措置に関する事項
⑤ 個人情報の漏えい等[49]の事案の発生時における対応に関する事項
⑥ 委託終了時における個人情報の消去及び媒体の返却に関する事項
⑦ 法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項
⑧ 契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項

また、委託事業者は委託業務に関して安全管理措置を講じる必要があり[50]、加えて、当該事業者が個人情報取扱事業者[51]に該当する場合には、個人データに関する安全管理措置を講ずべき義務[52]も負うこととなります。そのために、地方公共団体の機関は、委託先に対する必要かつ適切な監督の一環として、個人情報保護法に従った個人データの適切な取扱いが確保されるように、定期的な監査を行う等、委託先に対して必要且つ適切な監督を行うとともに、委託先に対して必要な助言や指導を行うことが考えられます[53]。

また、委託元が取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければならず、委託する業務に係る保有個人情報の秘匿性等その内容やその量等に応じて、作業の管理体制及び実施体制や個人情報の管理の情報について、少なくとも年１回以上の実地調査を原則として行う等の必要があります[54]。

１．５ 個人情報等利用における体制及び手続上の留意点

（1） 開示、訂正、利用停止請求

個人情報保護法は、本人が、地方公共団体が保有する自己に関する個人情報の正確性や取扱いの適正性を確保するうえで重要な仕組みとして開示請求、訂正請求及び利用停止請求（以下、「開示請求等」といいます。）の仕組みを設けており、何人も、地方公共団体の機関に対

[49] 漏えい、滅失やき損(例えば、ランサムウェアにより暗号化されてしまった等も含みます。)が含まれます。以下、「漏えい等」といいます。
[50] 個人情報保護法第 66 条第２項
[51] 個人情報保護法第 16 条第２項
[52] 個人情報保護法第 23 条
[53] ガイドライン５－３－１
[54] 委託先において、保有個人情報の取扱いに係る業務が再委託される場合には、委託先に同様の措置を講じさせるとともに、再委託される業務に係る保有個人情報の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが実地検査等の措置を実施します。保有個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様です。保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を記します。保有個人情報を提供し、又は業務委託する場合には、漏えい等による被害発生のリスクを低減する観点から、提供先の利用目的、委託する業務の内容、保有個人情報の秘匿性等その内容等を考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講ずる必要があります。（事務対応ガイド４－８－９）

し、その地方公共団体の機関が保有する自己を本人とする保有個人情報の開示請求等をすることができます[55]。

（2） 個人情報ファイル簿の作成

個人情報ファイル簿は個人情報保護法第 75 条第１項に基づき、地方公共団体の機関に対して、その作成及び公表が義務付けられているため、個人情報ファイル簿の作成に当たっては、対象となる個人情報ファイル[56]を漏れなく把握することが重要です[57]。

なお、地方公共団体の機関においては、記録情報に要配慮個人情報[58]及び条例要配慮個人情報[59]が含まれているときは、その旨も個人情報ファイル簿に記載する必要があります[60]。

作成した個人情報ファイル簿については、公表しなければならないことに留意が必要です。

（3） 苦情処理、漏えい・滅失・き損した際の対応

地方公共団体の機関は、地方公共団体における個人情報、仮名加工情報又は匿名加工情報の取扱いに関する苦情の適切かつ迅速な処理に努める必要があります[61]。

また、地方公共団体の機関は、保有個人情報の漏えい、滅失、き損その他の保有個人情報の安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定める事態[62]が生じたときは、当該事態が生じた旨を個人情報保護委員会に報告する必要があります。また、本人に対し、当該事態が生じた旨を通知する必要があります[63]。

（4） 地方公共団体に置く審議会等への諮問

地方公共団体の機関は、個人情報の適正な取扱いを確保するため専門的な知見に基づく意

---

[55] 個人情報保護法第５章第４節

[56] 「個人情報ファイル」とは、保有個人情報を含む情報の集合物であって、次に掲げるものをいいます。（1）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 （2）前号に掲げるもののほか、一定の事務の目的を達成するために氏名、生年月日、その他の記述等により特定の保有個人情報を容易に検索することができるように体系的に構成したもの（個人情報保護法第 60 条第２項）

[57] なお、１年以内に消去する記録情報のみを記録する個人情報ファイル（個人情報保護法 75 条２項６号）や 1000 人に満たない個人情報ファイル（個人情報保護法第 75 条２項９号、令 19 条２項）等については、個人情報ファイル簿の作成・公表が不要です。（個人情報保護法第 75 条２項１号）

[58] 不当な差別や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人種や信条、病歴、犯罪の経歴、健康診断等の記述等が含まれる個人情報のことをいいます。（個人情報保護法第２条第３項）

[59] 各地方公共団体において条例で独自に定めている要配慮個人情報のことをいいます。

[60] 個人情報保護法第 74 条第１項第６号及び第 75 条第４項

[61] 個人情報保護法第 128 条

[62] 個人情報保護委員会への報告対象事態としては、①要配慮個人情報が含まれる保有個人情報（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下同じ。）の漏えい等が発生し、又は発生したおそれがある事態、②不正に利用されることにより財産的被害が生じるおそれがある保有個人情報の漏えい等が発生し、又は発生したおそれがある事態、③不正の目的をもって行われたおそれがある保有個人情報の漏えい等が発生し、又は発生したおそれがある事態、④保有個人情報に係る本人の数が 100 人を超える漏えい等が発生し、又は発生したおそれがある事態が掲げられています（個人情報保護法施行規則第 43 条）。

[63] 個人情報保護法第 68 条

見を聴くことが特に必要である場合には、条例で定めるところにより、審議会等に諮問することができます[64]。

上記の「個人情報の適正な取扱いを確保するため専門的な知見に基づく意見を聴くことが特に必要」な場合とは、具体的には、定型的な案件の取扱いについて、専門的知見に基づく意見を踏まえて国の法令やガイドラインに従った運用ルールの細則を事前に設定しておくことで個人情報の適正かつ効果的な活用が図られる場合等（個人情報の保護に関する法律についてのQ&A（行政機関等編））が挙げられ、個人情報保護制度の運用やその在り方についてサイバーセキュリティに関する知見等の専門的知見を有する者の意見も踏まえた審議が必要であると合理的に判断される場合を指します。また、安全管理措置等、個人情報を取り扱うに当たって必要な各種の措置及び個人情報及びプライバシーに係るリスク分析、評価、対応等について意見を聴くことも想定されます。

ただし、利用目的以外の目的での利用・提供を行うことが可能かどうかについて、地方公共団体の機関が、個別の事案の個人情報保護法に照らした適否の判断について審議会等への諮問を行うことは、法の規律と解釈の一元化という個人情報保護法の趣旨に反するものであるため、審議会等への諮問は行えないことに留意が必要です。

１．６ 個人情報保護法関連の参照文書

その他、個人情報保護法の各規定の解釈等については、個人情報保護委員会ウェブサイト[65]で公表されている以下の資料を参照してください。また、その他各地方公共団体の個人情報保護法施行条例については、各地方公共団体の例規集を参照してください。

【地方公共団体の機関に係るガイドライン等】

・個人情報の保護に関する法律についてのガイドライン（行政機関等編）[66]
・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）[67]
・個人情報の保護に関する法律についてのQ&A（行政機関等編）[68]

２．プライバシーの保護

また、教育データを取り扱う場合には、「プライバシー」の考え方も念頭に置く必要があります。

プライバシーという概念は世の中に広く認識されており、また、国民の私生活上の自由が公権力の行使に対しても保護されるべきことを規定している憲法第13条が、個人の私生活上

[64] 個人情報保護法第129条
[65] https://www.ppc.go.jp/personalinfo/legal
[66] https://www.ppc.go.jp/files/pdf/220908_koutekibumon_guidelines.pdf
[67] https://www.ppc.go.jp/files/pdf/koutekibumon_jimutaiou_guide.pdf
[68] https://www.ppc.go.jp/personalinfo/legal/koutekibumon_qa/

の自由の一つとして、何人も、個人に関する情報をみだりに第三者に開示又は公表されない自由等を認める判決等もみられます。他方で、いわゆる「プライバシー権」として主張される内容は、個人情報の取扱いに直接関係しないものも含め、極めて多様かつ多義的なものになっており、判例等から一義的な定義を見出すことは困難です。この点、個人情報保護法では、個人情報の取扱いに伴い生じるおそれのある個人の人格的、財産的な権利利益に対する侵害を未然に防止することを目的として、個人情報の取扱いに関する規律と本人関与の仕組みが具体的に規定されています。

プライバシーの保護に当たっては個人情報保護法に準拠していれば十分というわけではありません。個人情報の取扱いが、個人情報保護法に照らして外形上問題がなかったとしても、プライバシーの保護が十分でなかった場合、国家賠償法[69]に基づく国家賠償請求等のリスクが発生するおそれがあります。さらに、取組みを推進する地方公共団体の機関への信頼が失墜し取組みを続けることが困難になってしまうリスクも懸念されます。

この点、個人情報保護法第３条においては、個人情報がプライバシーを含む個人の人格と密接な関連を有するものであり、個人が「個人として尊重される」ことを定めた憲法第 13 条の下、慎重に取り扱われるべきことを示すとともに、個人情報を取り扱う者は、その目的や態様を問わず、このような個人情報の性格と重要性を十分認識し、その適正な取扱いを図らなければならないとの基本理念を示しています。

プライバシーの保護においては、個人情報保護法を遵守するのみならず、各主体の自律的な取組みと連携・協力、プライバシー影響評価（PIA）[70]の手法を用いることや、個人データの取扱いに関する責任者を設置すること等によるデータガバナンス体制の構築等が必要と考えられます。

プライバシーに関しての記述として、政策基本原則のうち、「７.個人情報等の取扱いに関する透明性と信頼性」において以下のとおり述べられており、「プライバシー・バイ・デザイン」の考え方も重要になるとされています。

○政策基本原則「７．個人情報等の取扱いに関する透明性と信頼性」より抜粋

個人情報等の取扱いに当たっては、事後における対処療法的な対応ではなく、プライバシーを含む個人の権利利益の保護を事業等の設計段階で組み込み、事後の改修等費用の増嵩や信用毀損等の事態を事前に予防する観点から、全体を通じて計画的にプライバシー保護の取組を実施する「プライバシー・バイ・デザイン（Privacy by Design）」の考え方が重要である。

「プライバシー・バイ・デザイン」には７つの原則[71]が存在しています。「事後的でなく事

[69] 昭和 22 年法律第 125 号

[70] 個人情報等の収集を伴う事業の開始や変更の際に、プライバシー等の個人の権利利益の侵害リスクを低減・回避するために、事前に影響を評価するリスク管理手法

[71] 「DX 時代における企業のプライバシーガバナンスガイドブック　ver1.2」2022 年２月（総務省・経産省）（https://www.meti.go.jp/policy/it_policy/privacy/guidebook12.pdf）

前的であり、救済策的でなく予防的であること」、「プライバシー保護の仕組みが、事業やシステムのデザイン及び構造に組み込まれること」及び「プライバシーに係る情報は生成される段階から廃棄される段階まで、常に強固なセキュリティによって守られなければならない」等が定義されています。

これらの定義を踏まえると、プライバシー保護の仕組みを初期段階から予防的に構築し、取組み全体に渡り、情報の収集（生成）から廃棄までの全ての段階で機能しているということが重要です。

また、プライバシーに関わる社会的状況やプライバシーの捉えられ方の変化等により、当初想定していなかったプライバシーに関する問題が発生する可能性もあり、この場合、最初にプライバシー・バイ・デザインを実施しているから十分であるということには必ずしもなりません。このため、プライバシー・バイ・デザインによる仕組みの構築とそれを不断に見直し、改善していくプロセスを併せて検討していくことが求められます。

【コラム３】ELSI（倫理的・法的・社会的課題）

プライバシーの保護に関連して、ELSI（Ethical, Legal and Social Issues：科学技術の社会実装に際しての倫理的・法的・社会的課題）という考え方があります。

教育データの利活用に関する技術が日進月歩であることや、教育データの利活用の事例が積み重なっていくことを考慮すると、現在は想定していなかった課題が今後随時発生していくことが考えられます。こういった状況を踏まえると、今後、教育データの利活用が進むにつれて、新たな課題や、論点についての議論が深まっていくことも想定されます。

例えば、「EdTech の ELSI 論点 101」[72]においては、教育データの利活用の進展により想定される ELSI の論点の例として、「過去の問題行動がすべて記録蓄積されていくと、たとえそこから成長を見せていても、その児童・生徒のことを適切に評価できなくなるのではないか？」「成績の可視化が序列化を助長しないか？」等が挙げられています。

上記のような課題は、教育データの利活用が進むにつれて出てきた新たな課題であり、現時点で決まった解があるわけではありません。そこで、こういった新たな課題が出てきた場合には、各学校や地域で議論しながら、全体として納得できる解を探していく必要があります。また、文部科学省においても、今後順次、新たな課題についての議論を進めて、本留意事項の改訂を行っていく予定です。

[72] 教育データの利活用に関する有識者会議(第 13 回)会議資料「【資料 2-1 参考資料】滋賀大学加納教授提出資料(EdTech の ELSI 論点 101)」(https://www.mext.go.jp/kaigisiryo/content/20221011-mxt_syoto01-202318_2-12.pdf)

３．教育データを取り扱う際のセキュリティ対策

教育データを取り扱う場合は、政策基本原則の７つの原則[73]の一つである「個人情報等の取扱いに関する透明性と信頼性」の原則にしたがい、事後における対症療法的な対応ではなく、プライバシーを含む児童生徒の権利利益の保護を事業等の設計段階で組み込み、事後的な費用の増大や児童生徒のプライバシー侵害を事前に予防するために、全体を通じて計画的にプライバシー保護の取組みを実施することが重要です。

このためには、各地方公共団体の教育委員会で策定している教育情報セキュリティポリシーや「教育情報セキュリティポリシーに関するガイドライン」[74]（文部科学省）、個人情報保護法の規定に基づき、必要な情報セキュリティ対策や安全管理措置を行う必要があります。

３．１ 教育情報セキュリティポリシー

情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいいます。地方公共団体における情報セキュリティは、各地方公共団体が保有する情報資産に自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものです。

しかし、学校においては、コンピュータを活用した学習活動の実施等、教職員はもとより、児童生徒が日常的に情報システムにアクセスする機会がある等、地方公共団体の他の行政事務とは異なる特徴があります。このため、文部科学省では平成 29 年 10 月に、主に地方公共団体が設置する学校を対象とした情報セキュリティポリシー（以下、「教育情報セキュリティポリシー」といいます。）の策定や見直しを行う際の参考として、教育情報セキュリティポリシーの考え方及び内容について解説した「教育情報セキュリティポリシーに関するガイドライン（平成 29 年 10 月版）」を策定しました。さらに、令和元年 12 月、令和３年５月、令和４年３月に改訂を行っています。

「教育情報セキュリティポリシーに関するガイドライン」では、以下の①～⑥を基本理念としています。詳細や各理念に関係する対策基準は、「教育情報セキュリティポリシーに関するガイドライン」を参照してください。

○「教育情報セキュリティポリシーに関するガイドライン」文部科学省（令和４年３月）
第３章　地方公共団体における教育情報セキュリティの考え方
①組織体制を確立すること
学校における情報セキュリティ対策の考え方を確立させるためには、情報セキュリティの

[73] 各府省等の国の行政機関において政策の規格立案・実施に取り組むことが期待される７つの原則は、以下のとおりです。
①個人情報等の取扱いの必要性・相当性、②個人情報等の取扱いに関する適法性、③個人情報等の利用目的との関連性・利用の適正性、④個人情報等の取扱いに関する外延の明確性、⑤個人情報等の取扱いの安全性、⑥個人情報等に係る本人関与の実効性、⑦個人情報等の取扱いに関する透明性と信頼性

[74] https://www.mext.go.jp/content/20220304-mxt_shuukyo01-100003157_1.pdf

責任体制を明確にしておく必要がある。教育情報セキュリティポリシーの実行管理の最終責任を有する最高情報セキュリティ責任者（CISO：Chief information Security Officer）については、本ガイドラインにおいては、情報セキュリティインシデントが発生した際の危機管理等の観点から、自治体ガイドラインと同一の者（副市長等）が担うこととした。教育委員会・学校においては、首長部局の情報政策担当部局と密に連携し、情報セキュリティ対策を講ずる必要がある。また、学校は、教員を中心に構成され、教員は、児童生徒の教育を司ることがその職務の中心であることから、学校における情報システムの開発、設定の変更、運用、見直し等の権限や情報セキュリティの遵守に関する教育、訓練等については、基本的に教育委員会において責任を持つことを明確にした。

②児童生徒による重要性が高い情報へのアクセスリスクへの対応を行うこと

学校においては、コンピュータを活用した学習活動の実施等、児童生徒が日常的に情報システムにアクセスする機会があることに、その特徴がある。実際、児童生徒による、学校が保有する重要性が高い情報に対する不正アクセス事案も発生している。このため、本来は児童生徒が見ることを想定していない重要性が高い情報等にアクセスするリスクを回避することが必要である。

③標的型及び不特定多数を対象とした攻撃等による脅威への対応を行うこと

学校においては、学校ホームページや教職員によるメールの活用、さらには、学習活動におけるインターネットの活用等が行われていることから、地方公共団体のいわゆる行政部局と同様に、標的型及び不特定多数を対象とした攻撃等による脅威に対する対策を講ずることが必要となる。

④教育現場の実態を踏まえた情報セキュリティ対策を確立させること

成績処理等を自宅で行うことを目的として、教員が個人情報を自宅に持ち帰る場合がある。一方で、個人情報が記載された電子データを紛失することにより懲戒処分等を受けた教員は平成 27 年度で 62 名（文部科学省「平成 27 年度公立学校教職員の人事行政状況調査」）も存在することを踏まえ、平成 29 年のガイドライン策定時に教員が個人情報を外部に持ち出す際のルールについて、考え方を明確にした。また、児童生徒が活用する情報システムにおいては、児童生徒の扱う情報そのものが個人情報となる場合があり、これら情報を完全に匿名化することは困難であることから、児童生徒が活用する情報システムであっても重要性が高い情報を保持する場合、暗号化等の対策を講ずることとした。なお、通信経路の暗号化を必須とし、データへの適切なアクセス制限を行った上で、データそのもの及びデータ格納先の暗号化については運用を考慮して対策を講ずることが必要である。

⑤教職員の情報セキュリティに関する意識の醸成を図ること

学校は、成績や生徒指導関連等の重要性が高い情報を取り扱うことから、研修等を通じて、教職員の情報セキュリティに関する意識の醸成を図ることが必要である。

⑥教職員の業務負担軽減及び ICT を活用した多様な学習の実現を図ること

情報セキュリティ対策を講じることによって校務事務等の安全性が高まるとともに、教員

の業務負担軽減へとつながる運用となるよう配慮する必要がある。また、学校は、児童生徒が学習する場であることに鑑み、授業において ICT を活用した様々な学習活動に支障が生じることのないよう、配慮する必要がある。

３．２ 個人情報保護法の観点から～安全管理措置

個人情報を含む教育データを取り扱う際には、個人情報等の適正な取扱いを確保するために、個人情報等の安全管理のための必要かつ適切な措置を講じる必要があります。具体的には、個人情報等の取扱いに係る責任者の設置等の組織的安全管理措置、個人情報等の取扱いに携わる職員や関係者への教育訓練等の人的安全管理措置、個人情報等を取り扱う端末の制限等の物理的安全管理措置、個人情報等へのアクセス制限やログの管理等の技術的安全管理措置、保有個人情報が外国において取り扱われる場合に当該外国の個人情報の保護に関する制度等を把握する外的環境の把握をリスクに応じて講じることが求められます[75]。

（1） 組織的安全管理措置

まず、組織的に個人情報の取扱いに関する責任者を設置すること等によるデータガバナンス体制の構築等を行う必要があります。教育委員会・学校においては、各学校長等を管理責任者とし、管理責任者が個人情報等を取り扱う担当者を指定することが必要です。また、教育長等を総括管理責任者として置くことが必要です。

（2） 人的安全管理措置

個人情報を取り扱う教職員には、個人情報等のデータを取り扱っている自覚や、高い規範意識が求められるため、これらの意識醸成が必要です。例えば、総括管理責任者である教育長や教育委員会が、個人情報の適切な管理のための研修を教職員に対して行うことが考えられます。

（3） 物理的安全管理措置

個人情報を取り扱う区域の管理や、機器及び電子媒体等の盗難等の防止、電子媒体等を持ち運ぶ場合の漏えい等の防止、個人情報の削除及び機器、電子媒体等の廃棄等の措置が考えられます。また、災害等に備えた措置についても講じることが考えられます。その他、個人情報等を取り扱う端末を持ち出す場合には十分なセキュリティを確保すること、USB メモリ等の外部記録媒体の接続は制限することも考えられます。なお、クラウドサービスを利用する場合は教育委員会が自ら果たすべき安全管理措置の一環として必要かつ適切な措置を講じる必要があります。

[75] 政府情報システムのためのセキュリティ評価制度（ISMAP）による審査をクリアしたクラウドサービスリストが公開されており、当該リストに掲載のサービスを活用することも考えられます。
（https://www.ismap.go.jp/csm）

（４）　技術的安全管理措置

管理責任者は、個人情報等へのアクセス制御のための措置を講じるとともに、個人情報等へのアクセス状況の記録や情報の改ざん、窃取又は不正な消去の防止のための措置を講じることが考えられます。

特にアクセス状況の記録については、アクセス記録機能を、データを利用する情報システムに実装したうえで、定期的なログの確認を行うことが考えられます。アクセスの記録は、ログイン時刻やアクセス時間、ログイン中の操作内容等が特定できるようにすることが重要であり、これらを記録したアクセスログへのアクセス制限を行い、不当な削除や改ざん、追加等を防止する対策を講じることも考えられます。

また、管理責任者は、不適切なアクセスの監視のために、例えば、一定以上の情報がダウンロードされた場合に警告表示を設定することや当該設定を定期的に見直すことが考えられます。また、情報システムの管理者権限を必要最小限とすることが考えられます。

さらに、外部からの不正アクセスを防止するため、ファイアウォール設定等による経路制御等の必要な措置や、不正プログラムによる個人情報等の漏えい等の防止のためのソフトウェアの脆弱性の解消、不正プログラムの感染防止措置等について必要な措置を講じることも考えられます。

（５）　外的環境の把握

海外のクラウドサービスを利用する等、個人情報が海外で取り扱われる場合は、個人情報が取り扱われる外国の特定や外国の個人情報の保護に関する制度等の把握を行ったうえで、安全管理のために必要かつ適切な措置を講ずる必要があります。

（６）　自己点検及び監査

教育委員会に監査責任者を置き、安全管理措置の実施状況を定期的に監査し、総括管理責任者に報告することが考えられます。総括管理責任者はその報告内容を評価し、適切な管理のための措置・改善を行う PDCA サイクルを回すことが考えられます。

また、管理責任者は、個人情報等の記録媒体、処理経路等について、定期的に点検を行い、その結果と併せて、個人情報の開示請求や個人情報等の取扱いに関する苦情等を、総括管理責任者に報告することが考えられます。報告を受けた総括管理責任者は、事案に応じて児童生徒や保護者に対する説明等の対応も検討することが必要となります。

IV.　Q&A 編（よくあるご質問）

本編では、教育データ利活用に関してよくある質問と回答を記載しています。実際に教育データの利活用を行う際には、各 Q&A だけでなく、総論編Ⅲの関連箇所も参照してください。

Q（１）教育データとは、具体的にどのようなものを指しますか。

【回答】

本留意事項においては、教育データとは、初等中等教育段階の公立学校における児童生徒の教育・学習に関するデータ[76]を指します。教育データは、その内容によって、大きく分けて①行政系データ、②校務系データ、③学習系データと整理することができます。

【解説】

本留意事項においては、「教育データ」を（１）対象（２)内容という観点から、以下のように整理します。

１．対象

初等中等教育段階の公立学校における児童生徒の教育・学習に関するデータを対象とします。なお、個々の子供の学びによる変容を記録し、活用していく観点から、定量的データ（テストの点数等）だけではなく、定性的データ（成果物、主体的に学習に取り組む態度、教師の見取り等）も対象とします。

２．内容

教育データは内容ごとに、概ね、以下のように区分できます。

① 行政系データ

国や地方公共団体が統計・調査等により収集・蓄積しているデータで、行政職員や教職員が取り扱う情報です。

（例）

・児童生徒数・教員数等の情報
・端末整備の状況
・教育に関する統計調査等

② 校務系データ

学校運営に必要な児童生徒の学籍情報等のデータであり、教職員が学校・学級の管理運営、学習指導、生徒指導、生活指導等に活用する情報です。

（例）

・学籍情報（学年・組・番号等）

[76] 学校教育として活用されるデータ全般を指しており、学校教育として行われているものは家庭等の学校の外で行われているもの（例：宿題や家庭学習等）を含みます。

・出席簿
・指導要録に記載のある成績情報
・進路指導情報（面談記録等）

③　学習系データ

ワークシートや学習ドリル、アンケート等の学習に関するデータであり、教職員や児童生徒が日々の学校における教育活動において活用する情報です。

（例）

・端末の利用ログ
・学習の記録（確認テスト結果等）
・アンケートの回答結果
・活動の記録（動画・写真等）

Q（２）教育データの利活用を行うと、どのようなメリットがあるのでしょうか。

【回答】

教育データを利活用することで、児童生徒が興味のある分野を掘り下げる等学びを広げることができたり、教師がきめ細かい指導・支援に生かすことができたり、保護者が児童生徒の学校の様子を確認しやすくなったりすると考えられています。

また、教育委員会においては所管の学校のデータを把握したり、他の地方公共団体と比較したりすることもできる等、教育データの利活用は、学校現場においても教育行政においても、大きなメリットがあると考えられます。

【解説】

教育データを利活用することで、全ての子供たちの力を最大限に引き出すためのきめ細かい支援が可能になります。

児童生徒、教師、保護者、学校設置者といった主体ごとの視点で、教育データの利活用の具体的なイメージや考えられるメリットを挙げると、以下のとおりです。

１．児童生徒の視点

ア．学びを振り返る

・自身の学びや成長の記録を一目で振り返り、強みや弱点を簡単に把握することができる。

イ．学びを広げる・補う

・興味のある分野を発展的に学習することができる。
・苦手分野克服や復習のためにどのようなことをすればよいか把握できる。
・不登校・病気で学習できなかった部分を補うことができる。

ウ．学びを伝える

・学校と家庭での学びをつなぐことができる。
・転校・進学先に学びの記録を持っていくことができる。
・資格や履歴の証明等を電子データで提示できる。

２．教師の視点

ア．きめ細かい指導・支援

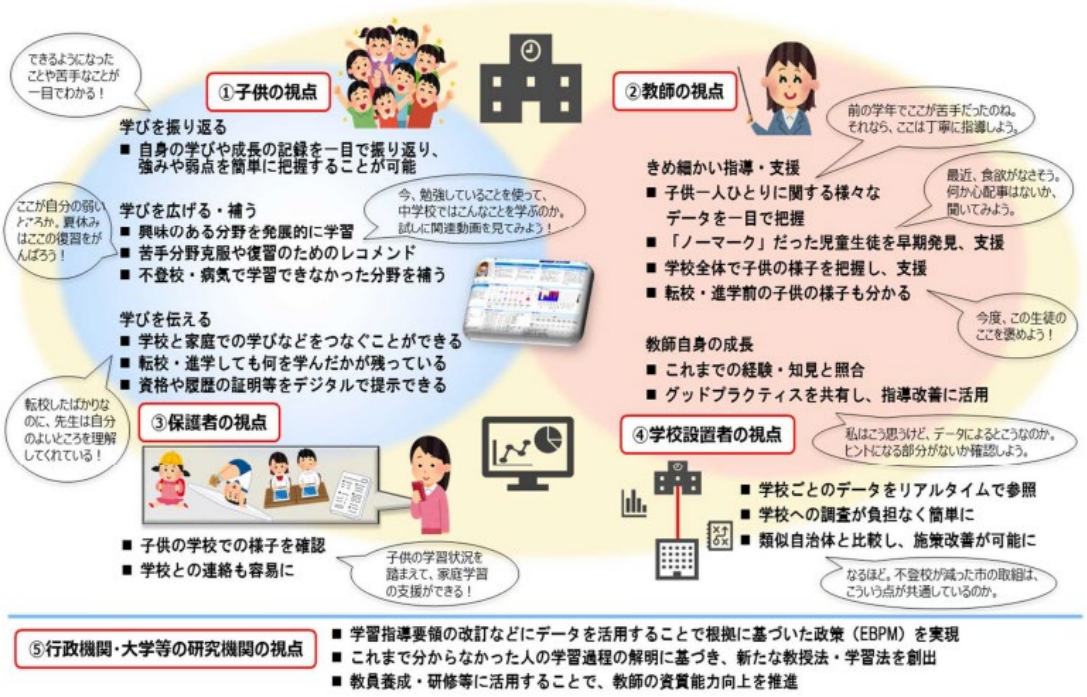
・児童生徒一人一人に関する様々なデータを一覧的に表示して把握できる。
・これまでは見えにくかった児童生徒の課題を早期に把握し、支援できる。
・学校全体で児童生徒の様子を把握し、支援できる。
・転校・進学前の子供の学びの記録や様子が分かる。

イ．教師自身の成長

・これまでの経験・知見と照合できる。
・好事例を共有し、指導の改善に活用できる。

３．保護者の視点
・子供の学校での様子を確認できる。
・学校との連絡が容易になる。

４．教育委員会の視点
・学校ごとのデータをリアルタイムで見ることができる。
・学校への調査が負担なく簡単にできる。
・他の地方公共団体と比較して、改善が可能になる。



図表 10　教育データの利活用の将来像

（出典）「教育データの利活用に係る論点整理（中間まとめ）」文部科学省（令和３年３月）[77]

さらに今後、具体的な個人等を特定できない大規模な教育データを利活用することで、エビデンスに基づく学習・指導や、政策立案を行うことができると考えられています。例えば、全体の状況や傾向等を把握し、現場の教育実践の向上や国・地方公共団体等の政策立案につなげたり、大学等の研究機関において効果的な学習・教育方法の検証をしたりすることも可能になります。

[77] 「教育データの利活用に係る論点整理（中間まとめ）」文部科学省（令和３年３月）（https://www.mext.go.jp/content/20210331-mxt_syoto01-000013887_1.pdf）「３．教育データの利活用の目的（将来像の具体的イメージ）」

Q（３）教育データを利活用するときには、どのようなことに気を付ければよいですか。

【回答】

教育データには、個人情報が含まれる場合があります。児童生徒を本人とする個人情報を含む教育データを利活用する場面では、個人情報保護法の規定に基づき、必要な手続きを行います。また、児童生徒のプライバシーにも配慮した細やかな対応が必要となります。

加えて、教育委員会・学校において、教育データの利活用が安全・安心に行われるための仕組みやルール作りや、教職員等への研修を行う必要があります。

【解説】

１．個人情報の適正な取扱い

児童生徒の教育データには、個人情報が含まれる場合があります。児童生徒を本人とする個人情報を取り扱う場合は、保有する際にその利用目的をあらかじめ特定したり、場合によっては特定した利用目的を本人である児童生徒に明示したり、安全管理措置を講じる体制を整備したりする等、個人情報保護法や各地方公共団体の個人情報保護法施行条例等に基づいた適正な取扱いが求められます。詳細は、「Ⅲ．総論編１．３」を参照してください。

２．プライバシーの保護

教育データの取扱いに当たっては、個人情報保護法を遵守していれば十分というわけではなく、プライバシーの保護も求められます。プライバシーの保護の観点から、個人の教育データの利活用は、本人の理解や納得のうえで行われる必要があり、本人の望まない形で行われることによって、不利益を受けることのないように気を付けていく必要があります。

プライバシーの保護についての詳細は、「Ⅲ．総論編２」を参照してください。

３．教育データのセキュリティの確保

上記のように、教育データには、児童生徒を本人とする個人情報等が含まれる場合があるため、安全・安心に取り扱う必要があります。そのためには、個人情報保護法や、個人情報保護委員会が公表している「個人情報等の適正な取扱いに関係する政策の基本原則」[78]の７つの原則[79]の一つである「個人情報等の取扱いに関する透明性と信頼性」の原則、各教育委員会

[78] 「個人情報等の適正な取扱いに関係する政策の基本原則」個人情報保護委員会（令和４年５月 25 日）（https://www.ppc.go.jp/files/pdf/kihongensoku.pdf）

[79] 「１ 個人情報等の取扱いの必要性・相当性」、「２ 個人情報等の取扱いに関する適法性」、「３ 個人情報等の利用目的との関連性・利用の適正性」、「４ 個人情報等の取扱いに関する外延の明確性」、「５ 個人情報等の取扱いの安全性」、「６ 個人情報等に係る本人関与の実効性」、「７ 個人情報等の取扱いに関する透明性と信頼性」の７つの原則が定められています。（https://www.ppc.go.jp/files/pdf/kihongensoku.pdf）

等で策定している教育情報セキュリティポリシー[80]に従う必要があります。具体的には、教育委員会・学校において、教育データの利活用が、安全・安心に行われるための管理体制やルールを定めるほか（データガバナンス体制）、教職員等への研修等を行います。詳細は、「Ⅲ．総論編３．１」を参照してください。

４．さらなる課題への対応

教育データの利活用について、現時点で想定される留意点は主に上記のとおりですが、教育データの利活用に関する技術が日進月歩であることを考慮すると、現在は想定していなかった課題が今後発生していくことが考えられます。こういった新たな課題が出てきた場合には、各学校や地域で議論しながら、全体として納得できる解を探していく必要があります。詳細は、「Ⅱ．教育データ利活用の目的【コラム１】」を参照してください。

[80]各教育委員会が情報セキュリティポリシーの策定や見直しを行う際の参考として、文部科学省において「教育情報セキュリティポリシーに関するガイドライン」（令和４年３月）を策定しています。
（https://www.mext.go.jp/content/20220304-mxt_shuukyo01-100003157_1.pdf）

Q（４）新たな学習用ソフトウェアを契約・導入するときは、どのようなことに気を付ければよいですか。

【回答】

契約の際には、学習用ソフトウェア（※）提供事業者の契約書、利用規約、個人情報保護に関するポリシー等で、学習用ソフトウェアの安全性や信頼性、個人情報の取扱いに関する規定等を確認する必要があります。

また、学習用ソフトウェア提供事業者に、児童生徒を本人とする個人情報の取扱いを委託するに当たっては、個人情報保護法を遵守する必要があります。

※学習用ソフトウェア

児童生徒が学習する際に使用するソフトウェア（デジタル教科書等の学習資料・学習コンテンツ、AI ドリル等の習得学習教材、画像・映像編集ソフトウェア等）に加え、学習支援を行うソフトウェア（児童生徒の学習活動を共有、学習の進行状況を管理する等）を含みます。

【解説】

１．契約の際に気を付けること

学習用ソフトウェアを導入する段階で、導入しようとする学習用ソフトウェアの安全性や信頼性を確認する（後述（１）参照）必要があります。また、学習用ソフトウェア提供事業者に、児童生徒を本人とする個人情報の取扱いを委託するに当たっては、個人情報保護法を遵守した取扱いとなっているかについても、事前に確認（後述（２）参照）しておく必要があります。

具体的には、まず、学習用ソフトウェア提供事業者の契約書（教育委員会と学習用ソフトウェア提供事業者との間の契約書）、利用規約（学習用ソフトウェアの利用者が守るべき事項等が記載された利用規約）、個人情報保護に関するポリシーの内容を確認します。

また、個人情報の取扱いの委託を行う際には、下記に加え、「Ⅲ．総論編１．４」を参照してください。

（１）学習用ソフトウェアの安全性や信頼性の確認

学習用ソフトウェアの安全性や信頼性については、学習用ソフトウェア提供事業者が、プライバシーマーク[81]や ISMS 認定[82]といった第三者認証を取得しているか、学習者プライバシ

[81] 一般財団法人日本情報経済社会推進協会（JIPDEC））のプライバシーマーク制度 （https://privacymark.jp/）
[82] 情報マネジメントシステム認定センター（ISMS-AC）の ISMS 適合性評価制度 （https://isms.jp/isms.html）

一宣言[83]を行っているか、といった点が信頼性の確認に役立つと考えられます。また、過去に情報流出が発生していないかをインターネットや新聞記事等を通じて調査（必要に応じて直接学習用ソフトウェア事業者に質問）すること（仮に発生していた場合には、学習用ソフトウェア提供事業者に改善状況や再発防止策を確認すること）も、安全性や信頼性の確認に役立ちます。

（２）学習用ソフトウェア提供事業者における個人情報の取扱いの確認

個人情報の取扱いについては、学習用ソフトウェア提供事業者との契約の際に、学習用ソフトウェア提供事業者の契約書、利用規約、個人情報保護に関するポリシー等で、以下の事項が明記されているかについて確認する必要があります。

○個人情報の取扱いを委託する際に契約書に明記すべき事項
①個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等の義務
②再委託の制限又は事前承認等再委託に係る条件に関する事項
③個人情報の複製等の制限に関する事項
④個人情報の安全管理措置に関する事項
⑤個人情報の漏えい等[84]の事案の発生時における対応に関する事項
⑥委託終了時における個人情報の消去及び媒体の返却に関する事項
⑦法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項
⑧契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱い状況を把握するための監査等に関する事項

また、個人情報の保管期間や削除方法、児童生徒本人への開示をどのように行うか等の点についても、あらかじめ取扱いを決めておくことが大切です。

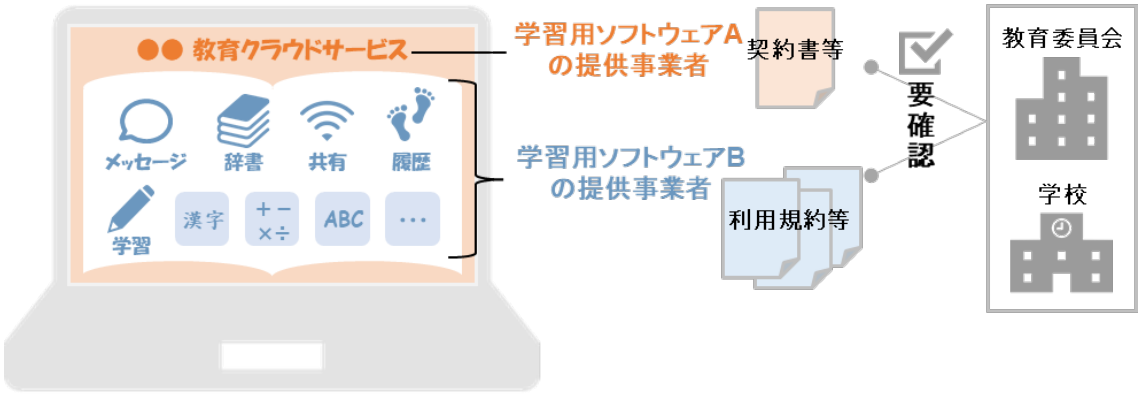
上記の「①個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等の義務」については、例えば、学習用ソフトウェア提供事業者が、取得した個人情報を含む教育データを自社のマーケティングのために分析する等、その事業者自身のために利用することが契約書に記載されていないか等を確認する必要があります。このような利用は通常、教育委員会・学校にとって、法令の定める所掌事務又は業務の遂行に必要であるとはいえないと考えられ、教育委員会・学校からの委託の範囲を超えると考えられるので、教育委員会・学校が委託を行う場合にはその範囲や内容を慎重に検討することが求められます。

[83] 一般社団法人 ICT CONNECT 21 が、令和２年５月 28 日に設立した GIGA スクール構想推進委員会が、令和３年に策定した、学習者が様々な教育サービスを安全・安心に使えるように、学習用ソフトウェアの提供企業が教育委員会／学校／大学／保護者に向けて、児童生徒/学生の個人情報についての正しい取扱いを宣言するための宣言書（https://giga.ictconnect21.jp/declare/）です。

[84] 漏えい、滅失やき損(例えば、ランサムウェアにより暗号化されてしまった等も含みます。)が含まれます。

また、例えば、プラットフォーム機能を持つ学習用ソフトウェア A を介して、別の学習用ソフトウェア B を利用する場合（図表 11 参照）には、教育委員会・学校は、A の提供事業者との間の契約書等の内容を確認するのはもちろんですが、B の提供事業者が定める利用規約等の内容も確認する必要があります。

学習用ソフトウェア提供事業者との契約や学習用ソフトウェア提供事業者の管理の詳細については、事務対応ガイド４－８－９、「教育情報セキュリティポリシーに関するガイドライン」[85]の「第５章１．８」等も参考にしてください。



図表 11　教育委員会・学校が確認すべき学習用ソフトウェア提供事業者の契約書等

[85] 「教育情報セキュリティポリシーに関するガイドライン」文部科学省（令和４年３月）（https://www.mext.go.jp/content/20220304-mxt_shuukyo01-100003157_1.pdf）

Q（５）教育データをシステム上で安全に管理するうえで、どのようなことに気を付ければよいですか。

【回答】

教育委員会・学校において、教育データを安全に管理するための仕組みやルール作り、教職員への研修等を行うことが重要です。そのうえで、教育データを取り扱う者一人一人が、その仕組みやルールを守る必要があります。なお、教育データの取扱いを外部に委託する場合には、適切な委託先を選ぶとともに、委託先の監督も必要になります。

【解説】

教育データを安全・安心に取り扱うためには、個人情報保護法、各教育委員会等で策定している教育情報セキュリティポリシーに従って、教育委員会・学校において、教育データを安全に管理するための仕組み・ルール作りや、実際にデータを取り扱う者への研修等を行う必要があります。なお、各教育委員会が情報セキュリティポリシーの策定や見直しを行う際の参考として、文部科学省において「教育情報セキュリティポリシーに関するガイドライン」[86](令和４年３月)を策定しているため、参考にしてください。

具体的には、例えば、以下のようなことが必要です。詳細は、「Ⅲ．総論編３」を参照するとともに、各教育委員会等が策定したセキュリティポリシーや事務対応ガイド４－３－１－１（１）の記載を参照してください。

■教育データを安全に管理するために必要になることの例	「教育情報セキュリティポリシーに関するガイドライン」の参照箇所
教育データを安全に管理するための体制整備	組織体制（１．２．）等
教育データの取扱い状況を確認する方法の整備	組織体制（１．２．）、アクセス制御（１．６．２．）等
教育データの流出が発生した場合に備えた体制の整備、ルール作り	組織体制（１．２．）、情報セキュリティインシデントの報告（１．５．３．）、侵害時の対応（１．７．３．）等
教育データが保管されている場所の厳重な管理	管理区域の管理（１．４．２．）
教育データが記録されている機器、電子媒体（例：パソコン）の盗難等を防止するための対応	教職員等の利用する端末や電磁記録媒体等の管理（１．４．４．）、教職員等の遵守事項（１．５．１．）等

[86] https://www.mext.go.jp/content/20220304-mxt_shuukyo01-100003157_1.pdf

教育データが記録されている電子媒体等を持ち運ぶ場合の情報流出を防止するための対応、持ち運びのルール作り	教職員等の利用する端末や電磁記録媒体等の管理（１．４．４.）、教職員等の遵守事項（１．５．１.）等
教育データの削除、廃棄（例：保存年数を超えた教育データの削除）	教職員等の利用する端末や電磁記録媒体等の管理（１．４．４.）等
教育データにアクセスできる者の限定	アクセス制御（１．６．２.）等
外部からの不正アクセスを防止するための対応	アクセス制御（１．６．２.）、不正アクセス対策（１．６．５.）等
教育データ取扱いに係る教育、研修	研修・訓練（１．５．２）等

図表 12　教育データを安全に管理するために必要になることの例

なお、教育データの管理を外部に委託する場合には、まず信頼できる適切な委託先を選ぶことが必要です。そのうえで、委託先との契約については、「Ⅲ．総論編１．４」及び「Ⅳ．Q&A 編 Q（３）」を参照してください。

Q（６）教育データを取り扱う際に、インターネットにつながるシステムを利用する場合とそうでない場合で、気を付けるべきことに違いはありますか。

【回答】

インターネットに接続するシステムを利用する場合でもそうでない場合でも、基本的に、気を付けるべきことに違いはありません。どちらの場合でも、安全に教育データを管理する必要があります。ただし、クラウドサービスを利用する場合には、クラウドサービスの特性に起因する留意点もあります。

【解説】

１．クラウドサービスの特徴

１人１台端末の整備に伴って、インターネットにつながるシステムやサービスを利用する機会は従前と比べて増加しています。

従来主流だったのは、いわゆる「オンプレミス」と呼ばれるサービス形態でしたが、オンプレミス型には、サーバの維持管理コストやセキュリティ面のほか、ソフトウェアがインストールされたハードウェアが手元にないとサービスが利用できない等の課題がありました。

一方で、クラウドサービスは、サーバを自前で用意する必要がないためコスト削減につながったり、サーバ（データセンター）の管理を厳重に行っているためセキュリティ面での安全性が高かったり、インターネットを介してサービスを利用するため時間や場所の制約がほとんどなかったりする、等の利点があります。

クラウドとオンプレミスはそれぞれに特徴がありながらも、政府全体としては、上記のように多くの利点があるクラウドの利用を推進するという方針が示されています（クラウド・バイ・デフォルトの原則[87]）。

また、文部科学省においても、「教育情報セキュリティポリシーに関するガイドライン」（令和４年３月）において、教育現場におけるクラウドの活用を推進しています[88]。校務系データ等の機密性の確保に当たっては、旧来はネットワーク分離による制御を中心とした境界防御型の手段で対応されていましたが、近年では、端末への対策を中心とした、接続するネットワークを限定しないアクセス制御認証型（ゼロトラスト）への移行又は組込みも有効

[87] 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」(2021 年（令和３年）３月 30 日 各府省情報化統括責任者（CIO）連絡会議決定)「２ 基本方針 ２．１ クラウド・バイ・デフォルト原則」(https://cio.go.jp/sites/default/files/uploads/documents/cloud_policy_20210330.pdf)

[88] 「教育情報セキュリティポリシーに関するガイドライン」文部科学省（令和４年３月）(https://www.mext.go.jp/content/20220304-mxt_shuukyo01-100003157_1.pdf) 第５章「教育現場におけるクラウドの活用について」「１．９　クラウドサービスの利用」

な手段として推奨されています。これらの手段を用いれば、クラウドを活用する場合も、十分なセキュリティ確保が可能となります。

２．クラウドサービスの特性に起因する留意点

教育データは安全に管理する必要があり、このことは、インターネットにつながるシステムを使用する場合とそうでない場合とで違いはありません。

ただし、クラウドサービスを利用する場合には、クラウドサービスの特性[89]を踏まえた留意点があります。具体的には、信頼できるクラウドサービス提供事業者のシステムを利用するとともに、アクセス権限を一定の範囲の者に限定したり、データの暗号化等による安全管理措置を講じたりする等外部からの不正アクセスを防止する等の対策が必要です[90]。

また、海外のクラウドサービスについては、管理する教育データやシステムについて、一部の日本の法令が適用されない場合や、「法的なトラブルが生じた場合に利用する裁判所（管轄裁判所）」が日本国外となってしまう場合がありますので、同サービスの利用については慎重な対応が求められています[91]。

[89] クラウドサービスの特性の詳細については、「教育情報セキュリティポリシーに関するガイドライン」の「１．９クラウドサービスの利用（3）クラウドサービスの特性に起因する留意点」を参照してください。

[90] 対策の詳細については、「教育情報セキュリティポリシーに関するガイドライン」を参照してください。主にオンプレミスのシステムの場合については「１．６　技術的セキュリティ」、クラウドサービスを利用する場合については「１．９　クラウドサービスの利用」、学習用端末の利用については「1.12　１人１台端末におけるセキュリティ」を参照してください。

[91] 詳細は、「教育情報セキュリティポリシーガイドライン」の第５章「教育現場におけるクラウドの活用について」「１．９．１　学校現場におけるクラウドサービスの利用について」「（３）クラウドサービスの特性に起因する留意点」及び「１．９．３ パブリッククラウド事業者のサービス提供に係るポリシー等に関する事項」【解説】(10)③を参照してください。

Q（７）万が一、教育データが流出してしまった場合や意図せずに削除されてしまった場合に、どのような対応が求められますか。

【回答】

直ちに、学校における教育情報セキュリティ管理者[92]（校長等）に報告し、被害の拡大防止の措置を取ることが求められます。教育情報セキュリティ管理者は、流出や削除等（漏えい、滅失やき損（例えば、ランサムウェアにより暗号化されてしまった等も含みます。）が含まれます。以下、「漏えい等」といいます。）が発生した原因を調査・分析し、教育委員会に報告するとともに、再発防止のために必要な対応をとる必要があります。

なお、法令で求められる場合(要配慮個人情報[93]や条例要配慮個人情報[94]が１件でも漏えい等した場合、個人情報に不正アクセスがあった場合、漏えい等が生じた個人情報について本人の数が 100 人を超える場合等)には、教育委員会[95]が個人情報保護委員会への報告と本人への通知を行うことが必要となります。

【解説】

教育データが流出してしまった場合や意図せずに削除されてしまった場合には、以下を参考に対応してください[96]。なお、個人情報保護法上の義務を守ることに加えて、教育委員会・学校のセキュリティポリシー等において独自のルールを定めている場合には、そのルールにも従ってください。

１．学校内部での報告

教育データが流出してしまった場合や誤って削除されてしまった場合、又は、そのおそれがあると思われる場合には、その事態を認識した教職員は、直ちに、教育情報セキュリティ管理者（校長等）に報告します。

このとき、自らの判断で事態の解決を図るのではなく、速やかに教育情報セキュリティ管理者に報告し、その指示を仰ぐことが重要です。また、流出や誤削除に該当するかどうか等の判断に迷う場合にも、少しでも疑わしいと思った時点で、速やかに報告することが望ましいです。

---

[92] 学校の情報セキュリティ対策に関する権限及び責任を有する者です。通常は校長を充てることが想定されます。詳細は「教育情報セキュリティポリシーに関するガイドライン」文部科学省(令和４年３月)の「１．２．組織体制」を参照してください。

[93] 不当な差別や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人種や信条、病歴、犯罪の経歴、健康診断等の記述等が含まれる個人情報（個人情報保護法第２条第３項）

[94] 各地方公共団体において条例で独自に定めている要配慮個人情報

[95] 個人情報保護法第 68 条（漏えい報告等）の主体は、「行政機関の長等」です。「行政機関の長等」には、行政機関の長、地方公共団体の機関、独立行政法人等及び地方独立行政法人が該当します。（個人情報保護法第 63 条）公立学校においては、「地方公共団体の機関」である教育委員会が個人情報保護委員会への報告・本人への通知を行うことになります。

[96] 事務対応ガイド４-８-11

２．被害の拡大防止

教育情報セキュリティ管理者は、被害の拡大防止又は復旧のため、外部からの不正アクセスや不正プログラムの感染が疑われる端末等のネットワークを切断する等の対応を、直ちに行います（教職員に指示することを含む）。

３．教育委員会への報告

教育情報セキュリティ管理者は、教育データの流出や誤削除が発生した経緯、被害状況等を調査し、直ちに教育委員会に報告します。なお、５．にあるような事態が発生した場合には、事態を知った後速やか（概ね３～５日以内）に、教育委員会から個人情報保護委員会への報告が必要となることに留意してください。

４．再発防止策

教育情報セキュリティ管理者は、教育データの流出や削除の発生した原因を分析し、再発防止のために必要な対策を実施するとともに、教育委員会に再発防止対策を報告します。

５．教育委員会から個人情報保護委員会への報告・本人への通知[97]

児童生徒の健康診断の結果等の、要配慮個人情報や条例要配慮個人情報が１件でも漏えい等した場合、児童生徒を本人とする個人情報に不正アクセスがあった場合、漏えい等が生じた個人情報について児童生徒本人の数が 100 人を超える場合等、個人情報保護法で求められる場合[98]には、教育委員会は、個人情報保護委員会への報告と児童生徒本人への通知を行うことが求められます。個人情報保護委員会への報告は、事態を知った後速やか（概ね３～５日以内）に速報を、30 日以内（不正の目的をもって行われたおそれがある保有個人情報の漏えい等が発生し、又は発生したおそれがある事態である場合[99]は 60 日以内）に確報を行う必要があります。

法令上では、個人情報保護委員会への報告及び児童生徒本人や保護者への通知を要しない場合であっても、事案の内容、影響等に応じて、事実関係及び再発防止策を公表したり、児童生徒本人や保護者への連絡をしたりすることも検討してください[100]。

---

[97] 個人情報保護法第 68 条。詳細については、ガイドライン５-４、事務対応ガイド４-４を参照してください。

[98] 個人情報保護委員会への報告対象事態としては、①要配慮個人情報が含まれる保有個人情報（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下同じ。）の漏えい等が発生し、又は発生したおそれがある事態、②不正に利用されることにより財産的被害が生じるおそれがある保有個人情報の漏えい等が発生し、又は発生したおそれがある事態、③不正の目的をもって行われたおそれがある保有個人情報の漏えい等が発生し、又は発生したおそれがある事態、④保有個人情報に係る本人の数が 100 人を超える漏えい等が発生し、又は発生したおそれがある事態が掲げられています（個人情報保護法施行規則第 43 条）。

[99] 個人情報保護法施行規則第 43 条第３号

[100] 事務対応ガイド４-４-１「（５）漏えい等報告の対象となる事態」では、「行政機関等における個人情報の適正な取扱いを確保する必要があることから、行政機関等は、法に基づく報告の対象とならない場合であっても、国民等の不安を招きかねない事案（例えば、公表を行う漏えい等が発生したとき、個人情報保護に係る内部規程に

Q（８）個人情報とは、どのようなものが該当しますか。

【回答】

教育委員会・学校においては、例えば児童生徒の氏名や生年月日、出欠席情報、テストの評点や学習アプリの回答履歴等が個人情報に該当すると考えられます。

【解説】

１．「個人情報」とは

個人情報保護法における「個人情報」とは、生存する個人に関する情報で、以下の①又は②に該当するものをいいます。

① 氏名等その情報のみにより、特定の個人を識別することができる[101]ような情報。（ア）又は、生年月日等その情報のみでは特定の個人を識別できなくても、他の情報と容易に照合することができ、それによって特定の個人を識別できる情報。（イ）

② 個人識別符号を含む情報。

個人情報には、それのみで特定の個人を識別できる氏名等の情報（ア）のみならず、他の情報と容易に照合することができ、それにより特定の個人を識別できる生年月日等の情報（イ）も含まれます。

例えば、「児童生徒の氏名」は、氏名から特定の児童生徒を識別することができるため、個人情報（ア）と言えます。

一方、例えば「生年月日」や「学籍番号」は、あくまで数字や番号であり、それ自体に特定の児童生徒が特定できるような情報が含まれているわけではありません。しかし、そのような、その情報のみでは特定の児童生徒を識別できないような情報についても、他の情報と容易に照合することができ、それにより特定の個人を識別することができる場合は、個人情報（イ）に該当します。

先ほどの「学籍番号」を一例に考えてみましょう。

学籍番号それのみでは、それが誰の学籍番号なのかは分かりません。しかし、学校においては通常、学籍番号と特定の児童生徒の氏名の対応関係を把握しているため、それらを容易に紐付け、学籍番号から特定の児童生徒を識別することが可能です。こういった場合は、その学校を所管している教育委員会管内においては、その学籍番号は個人情報（イ）に該当す

対する違反があったとき、委託先において個人情報の適切な管理に関する契約条項等に対する違反があったとき等）については、当該事案の内容、経緯、被害状況等について、速やかに委員会へ情報提供を行うことが望ましい。」とされています。

[101] 「特定の個人を識別することができる」とは、社会通念上、一般人の判断力や理解力をもって、生存する具体的な人物と情報との間に同一性を認めるに至ることができることをいいます。

ることになります。
このように、その情報のみでは特定の個人を識別することができない場合でも、他の情報と容易に照合することができ、それにより特定の個人を識別することができる場合は、その情報は個人情報として扱うことが求められるため、注意が必要です。

なお、ここでいう「他の情報と容易に照合することができる」[102]とは、例えば、各学校において通常の事務や業務における一般的な方法で、他の情報と容易に照合することができる状態をいいます。児童生徒の氏名等それ単体で特定の個人を識別できる情報を削除する等加工し、学籍番号等の番号や符号で管理したとしても、それだけでその学籍番号等が個人情報に当たらなくなるわけではありません。学校においては、通常、名簿等を使って氏名等の情報と照合することで、学籍番号等の番号や符号から、特定の児童生徒等を識別することができるため、この場合は、その番号や符号についても、個人情報に該当します。

また、個人情報に該当するかどうかを判断する際、その情報が公開されているかどうかは関係しません。したがって、ある個人が自らインターネットや SNS に公開している情報であっても、それが特定の個人を識別できるような情報であれば、個人情報に該当します。

なお、②の「個人識別符号」については、代表的なものとしては個人番号(マイナンバー)[103]や健康保険証の記号・番号、パスポート番号があります。また、ソフトウェア等で本人を認証できるようにする容貌や指紋も、生体情報を変換した符号として「個人識別符号」に該当します。その他にどのような情報が「個人識別符号」に該当するかは、脚注を参照してください[104]。

２．教育委員会・学校における個人情報

---

[102] 教育委員会が所管する公立学校については、個々の学校自体が地方公共団体の機関に該当するものではなく、当該学校を所管する教育委員会が、地方公共団体の機関に該当します。そのため、「他の情報と容易に照合することができる」範囲については、基本的に学校単位ではなく教育委員会単位で考える必要があります。（例えば、ある情報について、学校内では氏名等と照合することが不可能で、特定の個人を識別することが困難であるとしても、所管の教育委員会に問い合わせる等の方法により容易に照合することができ、特定の個人を識別することができる場合は、個人情報に該当します。また、同様に、教育委員会内では照合することが不可能でも、学校において照合することができる場合は、個人情報に該当します。）

[103] マイナンバーの取扱いは法令（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号））により用途が厳しく制限されているため、学校で取り扱うことは基本的に想定されず、教育委員会で取り扱う場合も限られています。

[104] 個人識別符号とは、単体で特定の個人を識別することができるものとして政令（個人情報の保護に関する法律施行令（平成 15 年政令第 507 号））で定められた文字、番号、記号その他の符号をいいます（個人情報保護法第２条第２項）。本文で記載したほかに「個人識別符号」の代表的なものは、以下の身体の特徴のいずれかを電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、特定の個人を識別するに足りるものとして個人情報保護委員会規則で定める基準に適合するものです。「細胞から採取されたデオキシリボ核酸（別名 DNA）を構成する塩基の配列」「虹彩の表面の起伏により形成される線状の模様」「発声の際の声帯の振動」「声門の開閉並びに声道の形状及びその変化」「歩行の際の姿勢及び両腕の動作、歩幅その他の歩行の態様」「手のひら又は手の甲若しくは指の皮下の静脈の分岐及び端点によって定まるその静脈の形状」「指紋又は掌紋」等

教育委員会・学校においては、例えば以下のようなデータは、基本的に個人情報に該当すると考えられます。個人情報のうち、教育委員会や学校の職員が職務上作成し又は取得した個人情報であって、組織的に利用するものとして教育委員会や学校が保有しているもののうち、行政文書等に記録されているものについては、保有個人情報に該当します。

児童生徒の
- 氏名

児童生徒の氏名と紐付く
- 年組、学籍番号
- 住所、生年月日、身長、体重
- 出欠席情報
- １人１台端末の操作履歴
- テストの評点
- 学習アプリの回答結果、回答時間

※あくまで一例

教育データは多種多様であるため、一概に整理することは困難ですが、校務系データ（例：学籍情報（学年・組・番号等）等）や、学習系データ（例：学習の記録（確認テスト結果等）等）は、個人情報に該当する場合が多いと考えられる一方、行政系データは、統計情報等特定の個人を識別できない情報が多く含まれています。

上で挙げたものは、あくまで一例であり、個人情報に該当するかどうかは、取り扱う教育データの内容や状況に照らして、個別具体的に判断する必要があります。

３．個人情報はどのように取り扱わなければならないか

児童生徒を本人とする個人情報を取り扱う場合は、個人情報保護法や各地方公共団体の個人情報保護法施行条例等に基づいた適正な取扱いが求められることになります。詳細は「Ⅲ．総論編１」を参照してください。

Q（９）学級名や学籍番号のみを含んだ成績等のデータで、児童生徒の氏名と紐付けて管理されていないデータは、個人情報に該当しますか。

【回答】

教育委員会・学校においては、基本的に個人情報に該当すると考えられます。

【解説】

「Ⅳ．Q&A 編 Q（８）」において解説しているとおり、個人情報には、それのみで特定の個人を識別できる氏名等の情報のみならず、他の情報と容易に照合することができ、それにより特定の個人を識別できる情報も含まれます。

ここでいう「他の情報と容易に照合することができる」とは、例えば、各地方公共団体の機関において通常の事務や業務における一般的な方法で、他の情報と容易に照合することができる状態をいいます。

教育委員会が所管する公立学校については、個々の学校自体が地方公共団体の機関に該当するものではなく、当該学校を所管する教育委員会が地方公共団体の機関に該当します。そのため、この「他の情報と容易に照合することができる」範囲については、基本的に学校単位ではなく教育委員会単位で考える必要があります。（例えば、ある情報について、学校内では氏名等と照合することが不可能で、特定の個人を識別することが困難であるとしても、所管の教育委員会に問い合わせる等の方法により容易に照合することができ、特定の個人を識別することができる場合は、個人情報に該当します。また、同様に、教育委員会内では照合することが不可能でも、学校において照合することができる場合は、個人情報に該当します。）

学校においては、通常、学級名や学籍番号と特定の児童生徒の氏名等との対応関係を把握しているため、それらを容易に照合し、学級名や学籍番号を通じて、成績等のデータから特定の児童生徒を識別することが可能です。

したがって、成績等のデータに氏名等が含まれておらず、「学級名」や「学籍番号」等のその情報からは一見特定の児童生徒を識別することはできない情報しか含まれていない場合であっても、基本的には、その成績等のデータは、個人情報に該当します。

なお、氏名等と容易に紐づけることができ、特定の児童生徒を識別することができる情報は、学級名や学籍番号のような情報に限られません。

例えば、1 人 1 台端末の利用ログ（端末番号とその端末の操作履歴等に関するデータ）等、一見して誰の情報であるかが分からないような情報であっても、教育委員会・学校が、児童生徒と端末の対照表等を確認することで、端末を使用する児童生徒の氏名等と容易に照合することができ、それにより、利用ログから、特定の児童生徒を識別することが可能である場合は、1 人 1 台端末の利用ログは個人情報に該当します。

また、成績情報、進路指導情報、学習の記録等について、氏名等をマスキングしたり、データ上で氏名等を別のIDに置き換えたりして加工した情報であっても、それらの加工を行う前の元データと容易に照合することができる場合は、加工後のデータについても、個人情報に該当します[105]。

このように、教育委員会・学校で取り扱う児童生徒に関する情報の多くは、たとえその情報のみで特定の児童生徒を識別することができる情報ではないとしても、基本的に個人情報に該当すると考えられます。

なお、教育データに個人情報が含まれる場合であっても、必ずしも必要な利用や提供を行うことができないというわけではありません。個人情報の利用・提供については、「Ⅲ．総論編１．３．３」を参照してください。

また、統計情報は、特定の個人との対応関係が排斥されている限りにおいては、個人情報保護法の適用の対象外となります[106]。

[105] 「(略) 個別の事案ごとに判断されますが、顧客データについて氏名等の一部をマスキングしたに過ぎない場合、当該加工後の情報は、加工前の個人情報との容易照合性等を踏まえると、通常、個人情報に該当することが多いと考えられますので、ご留意ください。」(令和３年８月２日付「「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、外国にある第三者への提供編、第三者提供時の確認・記録義務編及び匿名加工情報編）の一部を改正する告示」等に関する意見募集の結果について」【別紙２－4】意見募集結果（匿名加工情報編）№26）

[106] 事務対応ガイド３-２-７

Q（10）教育データの利用目的を明示するときは、①「誰が」②「誰に対して」明示すればよいですか。

【回答】

①「誰が」

教育委員会や各学校の教職員が行います。

②「誰に対して」

本人である児童生徒に対して、利用目的を明示する必要があります。また、学校の教育活動への理解を得る観点から、学校の実態や教育データの種類に応じて、保護者に対しても利用目的を明示すると、より丁寧な対応となります。

【解説】

※利用目的の明示の詳細については、「Ⅲ．総論編１．３．２」を参照してください。

１．「誰が」利用目的を明示するか

個人情報保護法上、利用目的の明示は、個人情報を本人から直接書面（オンライン含む）で取得する主体（地方公共団体の機関である教育委員会）が行うこととされています。

そのため、学校が、児童生徒を本人とする個人情報を本人から直接書面（オンライン含む）で取得する場合は、各学校の教職員や校長等が、学校や校長の名義で利用目的の明示を行うことも可能です。

また、教育委員会が、自ら児童生徒を本人とする個人情報を本人から直接書面（オンライン含む）で取得する場合には、教育委員会の名義で利用目的の明示を行う必要があります。この際、名義は教育委員会として、実際は所管の学校を通じて明示を行っても構いません。

２．「誰に対して」利用目的を明示するか

個人情報保護法上は、利用目的は、本人である児童生徒に対して明示する必要があります。

もっとも、学校教育においては、保護者が、児童生徒を本人とする個人情報を含む教育データの利用目的を把握しておきたいと考えていることもあります。そのため、学校の実態や利用する個人情報の種類に応じて、保護者に対しても利用目的を明示することは、より丁寧な対応となります。

Q（11）同意の取得を行う場合、①「誰が」②「誰から」同意を取得すればよいですか。

※このQでは、同意の取得を行う場合について解説しています。

なお、個人情報の利用に当たっては、法令（条例を含みます。以下、本Qにおいて同じ。）の定める所掌事務又は業務を遂行するため必要な場合に限り、かつ特定した利用目的内で内部利用・外部提供することが基本です。同意は、利用・提供が臨時的に行われる場合において利用目的の範囲外で内部利用・外部提供する際の選択肢の一つと位置づけられています。詳細は、「Ⅲ．総論編１．３．３」を参照してください。

【回答】

①「誰が」

教育委員会や各学校の教職員が行います。

②「誰から」

同意は、本人から取得するのが原則とされています。

しかし、児童生徒の発達段階によっては、同意したことによって生じる結果について、自分で理解・判断できないことも考えられます。自分で理解できる場合は本人から、できない場合は保護者から、同意を取得するのが基本です。なお、同意したことによって生じる結果について自分で判断できると考えられる子供の具体的な年齢は、個人情報の種類や場面ごとに個別具体的に判断されるべきですが、一般的には12歳から15歳までとされています。

【解説】

※このQでは、同意の取得を行う場合について解説しています。

なお、個人情報の利用に当たっては、法令の定める所掌事務又は業務を遂行するため必要な場合に限り、かつ特定した利用目的内で内部利用・外部提供することが基本です。同意は、利用・提供が臨時的に行われる場合において利用目的の範囲外で内部利用・外部提供する際の選択肢の一つと位置づけられています。詳細は、「Ⅲ．総論編１．３．３」を参照してください。

１．「誰が」同意を取得するか

個人情報保護法上、同意の取得は、個人情報を利用目的以外の目的で利用又は提供する主体（地方公共団体の機関である教育委員会）が行うこととされています。

そのうえで、学校が児童生徒を本人とする個人情報を利用目的以外の目的で利用又は提供する場合は、学校の教職員や校長等が学校や校長の名義で同意の取得を行うことも可能です。

また、教育委員会が、児童生徒を本人とする個人情報を利用目的以外の目的で利用又は提供する場合には、教育委員会の名義で同意を取得する必要があります。この際、名義は教育委員会として、実際は所管の学校を通じて同意の取得を行っても構いません。

２．「誰から」同意を取得するか

同意は、本人から取得するのが原則とされています。つまり、児童生徒を本人とする個人情報を、利用目的の範囲外で利用・提供する場合には、児童生徒本人から同意を取得することが原則です。

しかし、児童生徒の発達段階によっては、同意したことによって生じる結果について自分で理解・判断できないことも考えられます。自分で理解・判断できる場合は本人から、できない場合は保護者から、同意を取得することが基本です。

なお、同意等について自分で理解・判断できると考えられる子供の具体的な年齢は、個人情報の種類や場面ごとに個別具体的に判断されるべきですが、一般的には 12 歳から 15 歳までとされています。

なお、12 歳から 15 歳までの児童生徒が同意したことによって生じる結果を自分で判断できると考えられるか判断がつきにくい場合に、児童生徒本人のみならず保護者の同意も併せて取得しておくことは、より丁寧な対応となります。

以上のとおり、最終的には個人情報の種類や児童生徒の発達段階に応じて、誰から同意を取得するかを個別具体的に判断する必要があります。もちろん、実際の学校現場で児童生徒一人一人について判断をすることは現実的ではありませんので、基本的には学年や学校全体として判断を行うことで問題ありません。