教育データの利活用に係る留意事項

文部科学省

第３版（令和７年３月）

目次

○　本留意事項について 1

○　教育データ利活用の目的 3

【コラム１】教育データの利活用の参考となる考え方 5

I.　総論編（教育データを利活用する際に気を付けること） 6

１.個人情報の適正な取扱い 7

１．１ 個人情報を取り扱う際の基本理念 7

１．２ 教育委員会・学校が取り扱うこととなる個人情報等 8

１．２．１ 個人情報とは 8

【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？ 9

１．２．２ 教育委員会・学校における個人情報 10

１．３ 個人情報の取扱い区分に応じた整理 10

１．３．１ 個人情報の取扱いの概要 10

１．３．２ 個人情報の保有・取得 12

１．３．３ 個人情報の利用・提供 15

１．３．４ 個人情報の保管 22

１．４ 個人情報の取扱いの委託 22

１．５ 個人情報等利用における体制及び手続上の留意点 24

１．５．１　開示、訂正、利用停止請求 24

１．５．２　個人情報ファイル簿の作成 24

１．５．３　苦情処理、漏えい・滅失・毀損した際の対応 25

１．５．４　地方公共団体に置く審議会等への諮問 25

１．６ 個人情報保護法関連の参照文書 26

２．プライバシーの保護 26

【コラム３】ELSI（倫理的・法的・社会的課題） 27

【コラム４】プライバシー侵害が成立する代表的な裁判例　（寄稿：弁護士 森亮二） 28

３．セキュリティ対策 30

３．１ 教育情報セキュリティポリシー 30

３．２ 個人情報保護法の観点から～安全管理措置～.....33
３．２．１　組織的安全管理措置.....33
３．２．２　人的安全管理措置.....33
３．２．３　物理的安全管理措置.....33
３．２．４　技術的安全管理措置.....34
３．２．５　外的環境の把握.....34
３．２．６　自己点検及び監査.....34

II.　手順編.....35

１．取得.....36

２．利用、提供.....39

３．保管.....41

III.　事例編.....46

事例１　A 市立 B 小学校において、授業において、児童が自ら考えなどを書き込んだり他者と共有したりしながら学習を進めるためのデジタル教材を利用する.....47

事例２　A 県立 C 高等学校において、生徒が、問題を解いて習熟度に応じたフィードバックを得られるデジタルドリルを利用する.....53

事例３　A 市立 D 中学校において、生徒が、様々な学習ツールにつながるソフトウェア（学習 e ポータル）を利用する.....60

事例４　A 市立 E 中学校において、生徒に対し、アンケートなどを行うためのツール（OS メーカーが標準的に提供するソフトウェアの一部）を利用する.....66

事例５　A 市立 F 小学校において、児童の学習状況や健康情報を一覧できるツールを利用する（校務支援システム等）.....72

事例６　A 市立 G 小学校において、児童の心の健康状態を把握するツールを利用する.....76

事例７　A 市立 H 中学校において、部活動時の熱中症リスクの軽減のためにウェアラブル端末を利用する.....84

事例８　A 市立 I 中学校において、体育の授業で、生徒の技能習得と向上を促すために、動作解析ツールを利用する.....92

IV.　Q&A 編（よくあるご質問）.....100

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。.....101

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。.....103

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。 105
Q（４）教育データには、どのような個人情報が含まれますか。 107
Q（５）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。 110
【コラム５】　「△△市立〇〇中学校３年Ａ組 15 番」は個人情報？ 112
Q（６）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。 113
Q（７）教育データの利活用を行う場合、同意の取得は必要ですか。同意の取得が必要になるのはどのような場合ですか。必要な場合はどのように同意を取得すれば良いですか。 114
Q（８）新たな学習用ソフトウェア等を契約・導入する際、個人情報の取扱いに関してどのようなことに気を付ければよいですか。 116
Q（９）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（クラウドサービス）を利用する場合に、気を付けるべきことはありますか。 119
Q（10）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。 121
Q（11）教育データをシステム上で安全に管理するうえで、情報セキュリティの観点からどのようなことに気を付ければよいですか。 123

別添　国立・私立学校が留意すべき個人情報保護法の規律―早見表― 126

○　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）[1]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の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）」（個人情報保護委員会）（以下、「ガイドライン」といいます。）[2]、「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）」（個人情報保護委員会）（以下、「事務対応ガイド」といいます。）[3]、「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）（以下、「基本方針」といいます。）[4]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が、別添「国立学校・私立学校が留意すべき個人情報保護法の規律 - 早見表 - 」において本留意事項で参考となる記載を整理していますので、適宜ご参照ください。

２．構成

本留意事項は、「総論編」「手順編」「事例編」「Q&A 編」に分かれています。各文書の目的と特

---

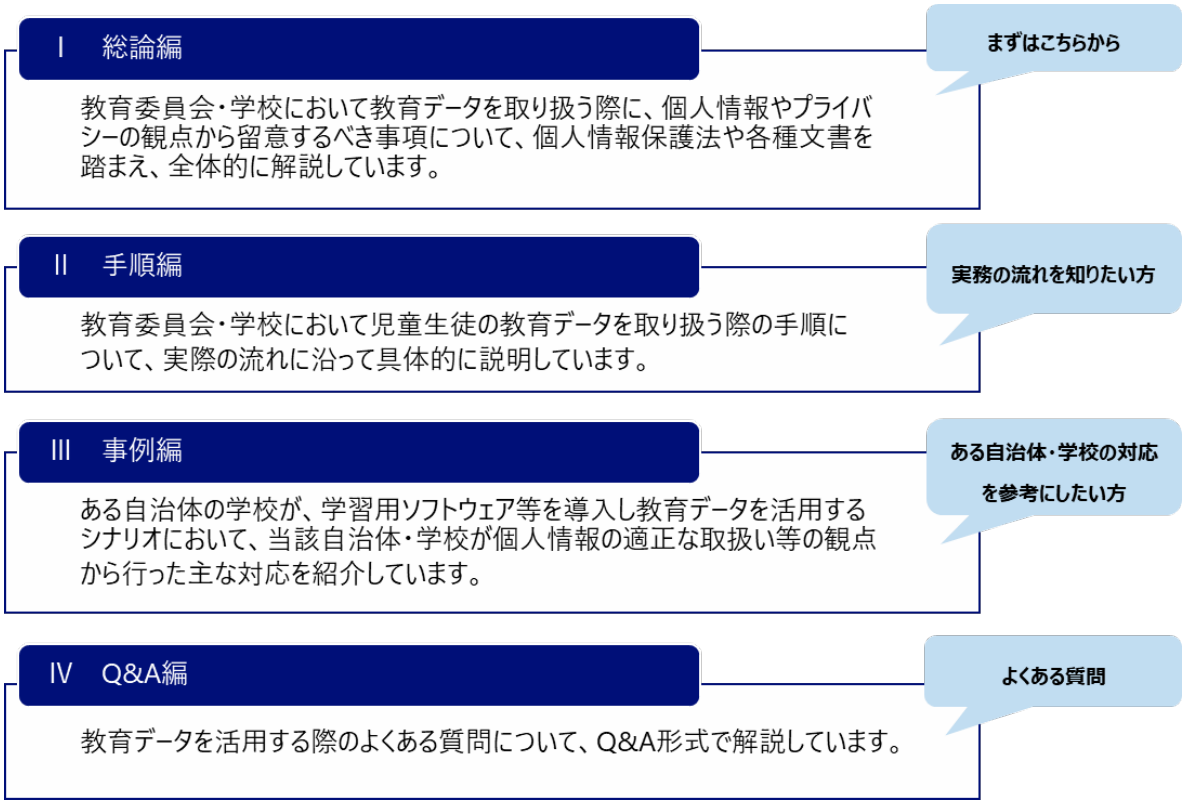
[1] Q&A 編ーQ（１）「教育データとは、具体的にどのようなものを指しますか。」も参照のこと。

[2] https://www.ppc.go.jp/files/pdf/241127_koutekibumon_guidelines.pdf
なお、ガイドライン及び事務対応ガイド（注釈２参照）は令和６年 11 月に一部改正されていますが、本留意事項は一部改正前のガイドライン及び事務対応ガイド（令和４年施行版）をもとに対象箇所を示しています。必要に応じて個人情報保護委員会から提示されている新旧対照表をご確認ください。

[3] https://www.ppc.go.jp/files/pdf/202403_koutekibumon_jimutaiou_guide.pdf

[4] https://www.ppc.go.jp/files/pdf/20220401_personal_basicpolicy.pdf

徴に従って、必要な文書を参照するようにしてください。



○　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。

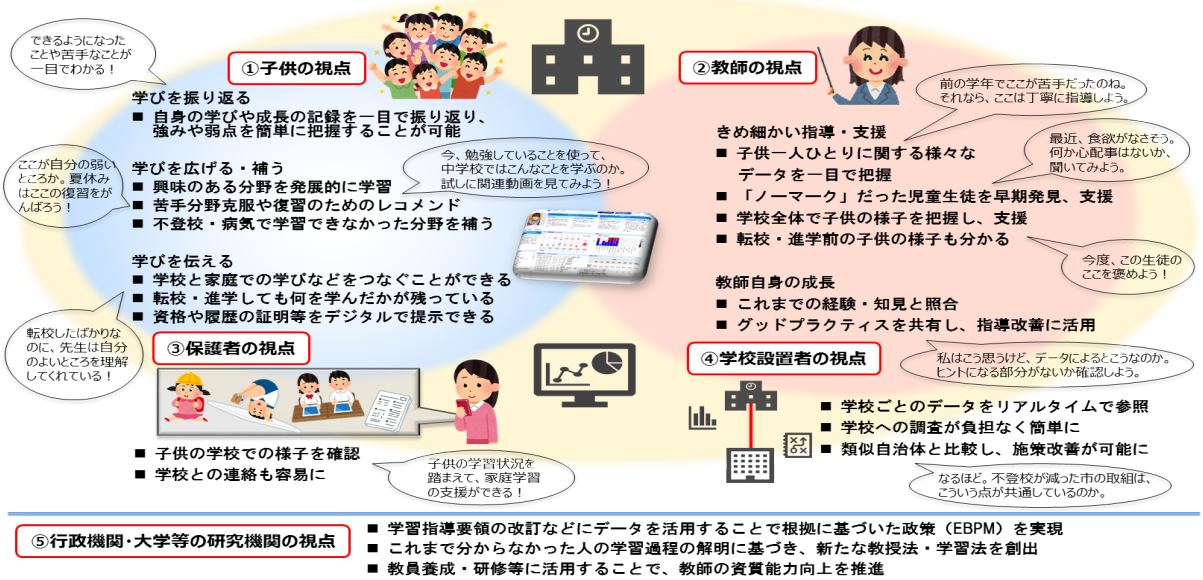
教育データを利活用する目的は、端的に言えば、全ての子供一人一人の力を最大限に引き出すためのきめ細かい支援を可能にすることです。この目的の達成に向けて、主体ごとにデータの利活用の具体的なイメージを挙げると以下のとおりです。

子　　供：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、子供、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子供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 [5]。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。（Q&A 編－Q（２）も参照のこと）

[5] 教育データを利活用する目的は、データをもとに、一人一人の力を最大限引き出すためのきめ細かい支援を可能とすることです。データの利活用はあくまでこのための手段であり、技術やデータを利活用すること自体が目的化しないようにする必要があります。



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)

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（中間まとめ）」（令和３年３月）[6]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」（令和４年１月）[7]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」（令和６年６月 21 日閣議決定）[8]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、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。

教育データの利活用に当たっては、個人情報の適正な取扱いやプライバシーの保護は大前提としな

[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/policies/priority-policy-program

がら、「教育データの利活用」と「安全・安心」の両立が実現されることが重要です。

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、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。また、こうした安全・安心な教育データの利活用はアナログデータかデジタルデータかに限らず留意する必要がありますが、本留意事項（第３版）では、１人１台端末環境によりデジタルデータの活用が進むことを念頭に、教育委員会や学校において様々な学習用ソフトウェア等を導入する様々な場面で留意すべき点についてまとめた「手順編」「事例編」を追加しています。

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。（Q&A 編－Q（３）も参照のこと）

【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[11]。

更に、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」[12]を、EU（European Union：欧州連合）では「GDPR」（General Data Protection Regulation：一般データ保護規則）[13]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。）[14]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] https://www.unicef.or.jp/about_unicef/about_rig.html

[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] 総務省は令和５年６月に、「ICT 活用のためのリテラシー向上に関するロードマップ」を公表し、参考事例として欧米におけるデジタル・シティズンシップの考え方を踏まえた取組事例を紹介している。
https://www.soumu.go.jp/main_content/000888980.pdf

[12] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188
「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原則が定められています。

[13] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
「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。

[14] 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。

I. 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。）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[15]。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、個人情報の保護に関する基本方針[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）より抜粋
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
（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

[15] プライバシーの保護が十分でなかった場合、差止請求により教育活動の継続が困難になるリスクや、国家賠償法 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。詳しくは「2．プライバシーの保護」を参照してください。
[16] https://www.ppc.go.jp/files/pdf/20220401_personal_basicpolicy.pdf

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

[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）

[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。

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[20]。

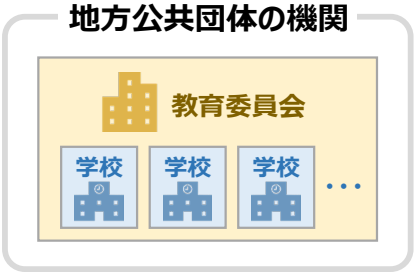
また、地方公共団体職員が職務上作成し、又は取得した個人情報であって地方公共団体職員が組織的に利用するものとして、当該地方公共団体が保有しているもののうち、行政文書等に記録されているものを「保有個人情報」[21]といいます。

【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みます。）、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」

さらに、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、個人情報保護法では「要配慮個人情報」が定義されています。「要配慮個人情報」[22]とは、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。

---

[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

[22] 個人情報保護法第２条第３項

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。（Q&A 編－Q（４）、（５）も参照のこと）

児童生徒の ● 氏名 児童生徒の氏名と紐付く ● 学年、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

なお、個人情報であったとしても、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、「Ⅰ．総論編１．３．３」を参照してください。

また、統計情報（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）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。

１．３ 個人情報の取扱い区分に応じた整理

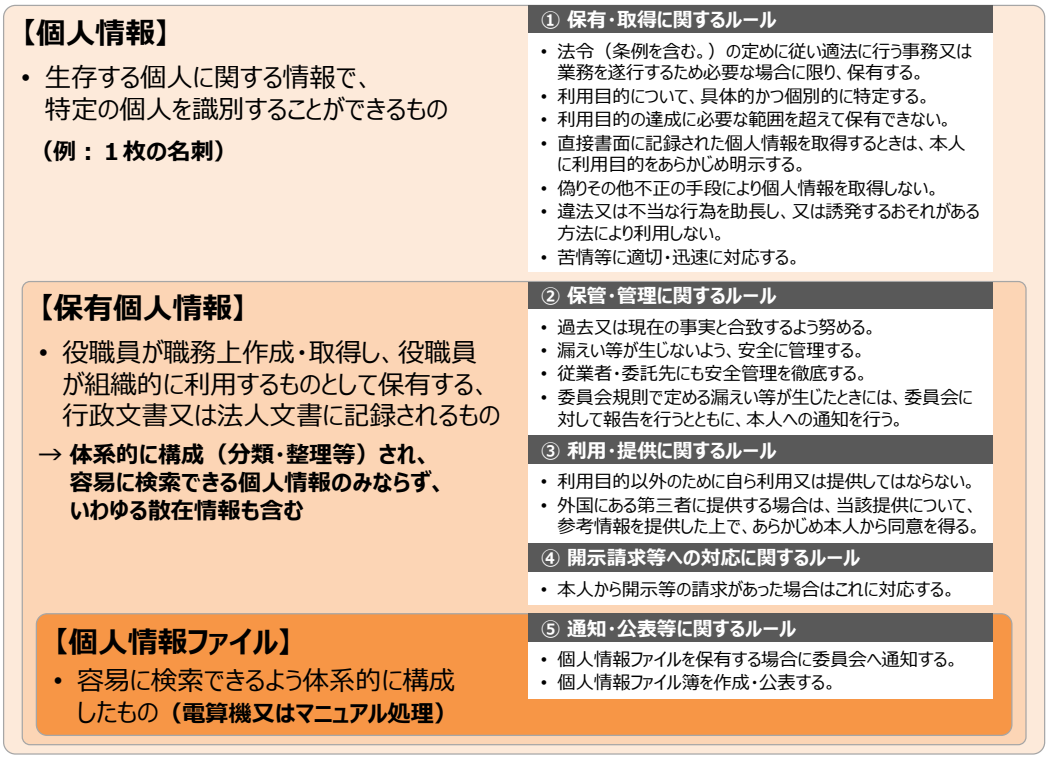
１．３．１ 個人情報の取扱いの概要

それでは、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具体的に確認していきます。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」[23]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。

[23] 個人情報保護法第２条第 11 項



図表３　個人情報保護法第５章の主な規定

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。（個人情報保護法第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**。（個人情報保護法第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。（個人情報保護法第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**。（個人情報保護法第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**。（個人情報保護法第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**。（個人情報保護法第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**。（個人情報保護法第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**。（個人情報保護法第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）

１．３．２ 個人情報の保有・取得

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[24]。

例外については、「Ⅰ．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。

言い換えると、個人情報の保有や取得は、「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範囲でなければなりません。したがって、最初に「法令の定める所掌事務又は業務」の内容を整理する必要があります。

[24] 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 [25]。そのうえで、個人情報の保有は、特定した利用目的の範囲内である必要があります。

「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 [26]。

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 [27]、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。

（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（オンラインを含みます。以下同じ。）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。（Q&A編－Q（６）も参照のこと）

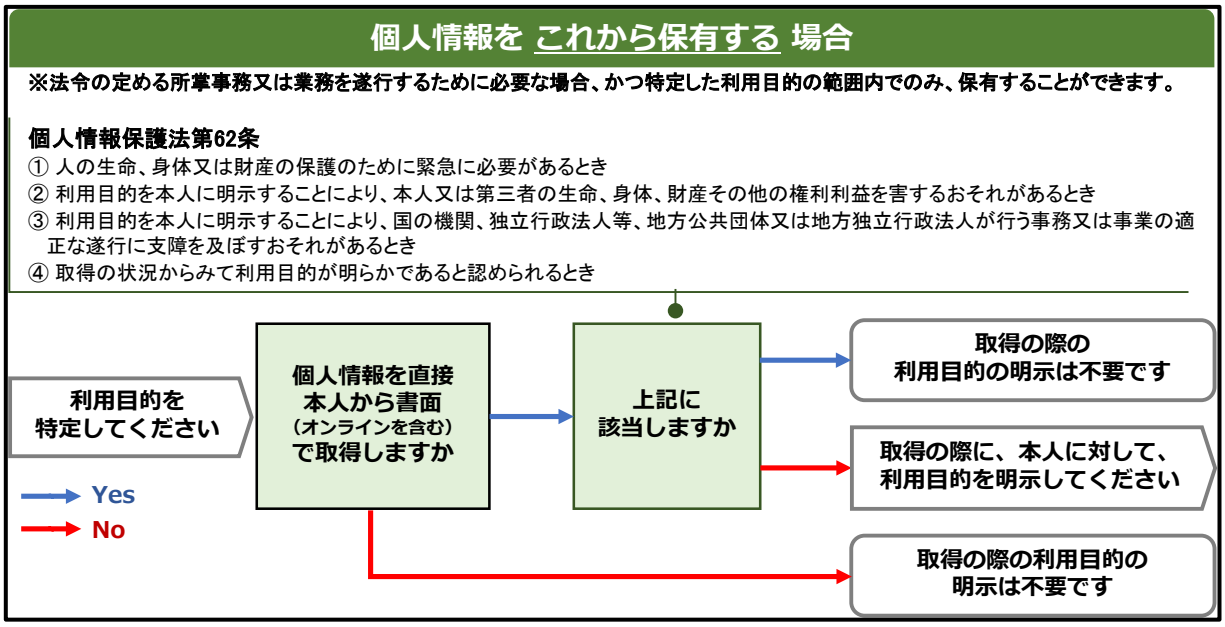
なお、利用目的を明示することにより他の権利利益を損なうおそれがある場合等、利用目的の明示を義務付けることが適当でない場合や、利用目的が明らかである場合にまで、一律にあらかじめ利用目的を明示することは合理的でない場合があり、そのような場合の例外についても定められています。例外の詳細については、図表５を参照してください。

[25] 個人情報保護法第 61 条第１項
[26] ガイドライン５－１
[27] 個人情報保護法第 82 条第１項
[28] 事務対応ガイド４-２-２

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、ここまでに解説した内容を整理すると、図表 6 のようになります。



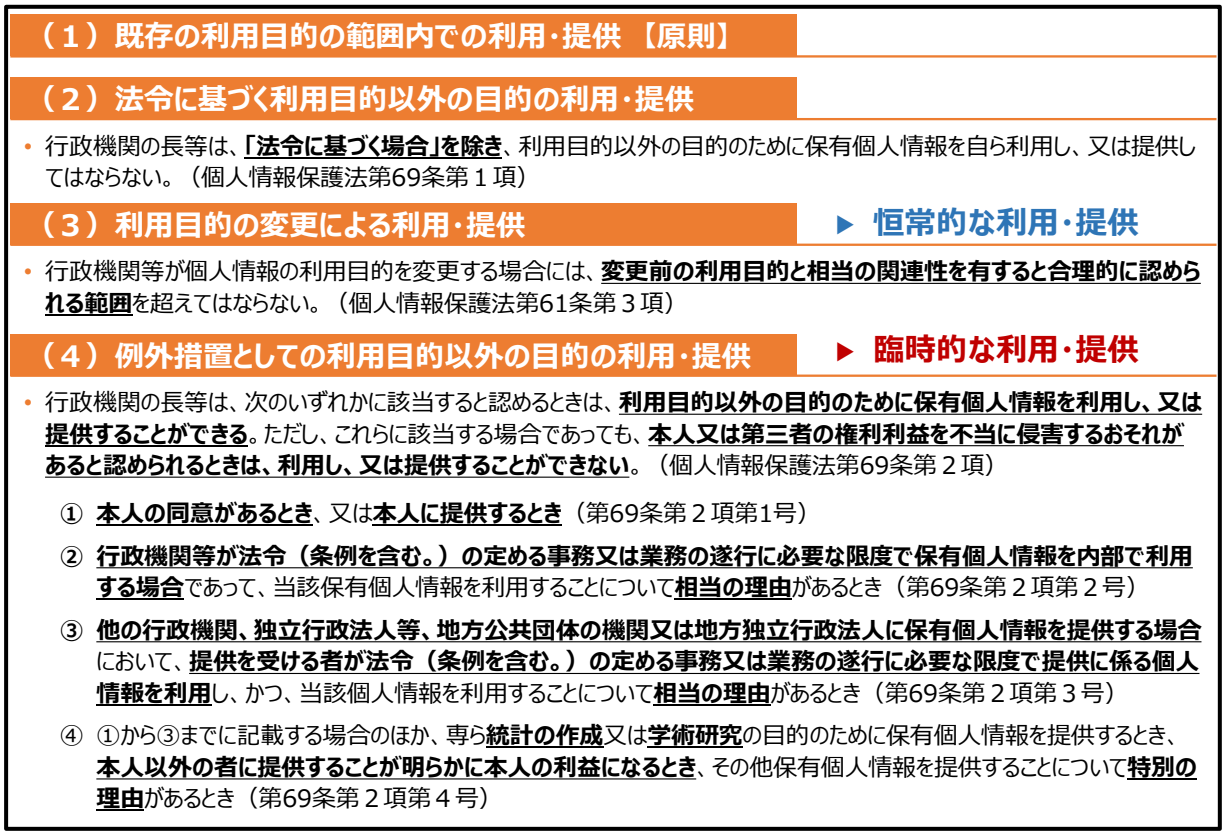
図表 6　個人情報をこれから保有する場合の流れ（フローチャート）

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、図表 7 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。

[29] 個人情報保護法第 61 条第 1 項、第 69 条第 1 項



図表７　行政機関等が個人情報を利用・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】

「Ⅰ．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関等を含む。）への提供のことを指します。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）法令（条例は含みません。以下、本項において同じ。）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・

[30] 個人情報保護法第 69 条第１項

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（昭和 22 年法律第 164 号）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]、以下のとおり考え方が示されているところです。

「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）

[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
[33] 事務対応ガイド４-２-１
[34] ガイドライン５-２-１

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。

同意の取得は、個人情報を利用目的以外の目的で利用・提供する主体が行うこととされています。例えば、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・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うことは可能です。

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]。

ただし、適正に同意が取得されていない場合は、同意が無効になる場合があります。例えば、本人の同意があっても、利用目的が具体的に特定されていない場合や、事前の説明が十分でない場合、同意が強制されている場合が該当し得ます。特に、公教育の性質上、全児童生徒に対し同意書を必須の提出物とする場合や、同意しない児童生徒が授業を受けることができない場合等はもちろん、授業に不便が生じる場合等においても、本人が完全な任意に基づいて同意しているとは限らず、実質的に同意せざるを得ない状況にある可能性があることを認識する必要があります。

また、同意した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]。

なお、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。（Q&A 編－Q（７）も参照のこと）

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

---

[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）

[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

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 当該利用・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]
③ 当該個人情報を利用・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・提供の原則禁止の例外としたものです[45]。

---

[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
[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

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、個人情報保護法の適用の対象外となります。

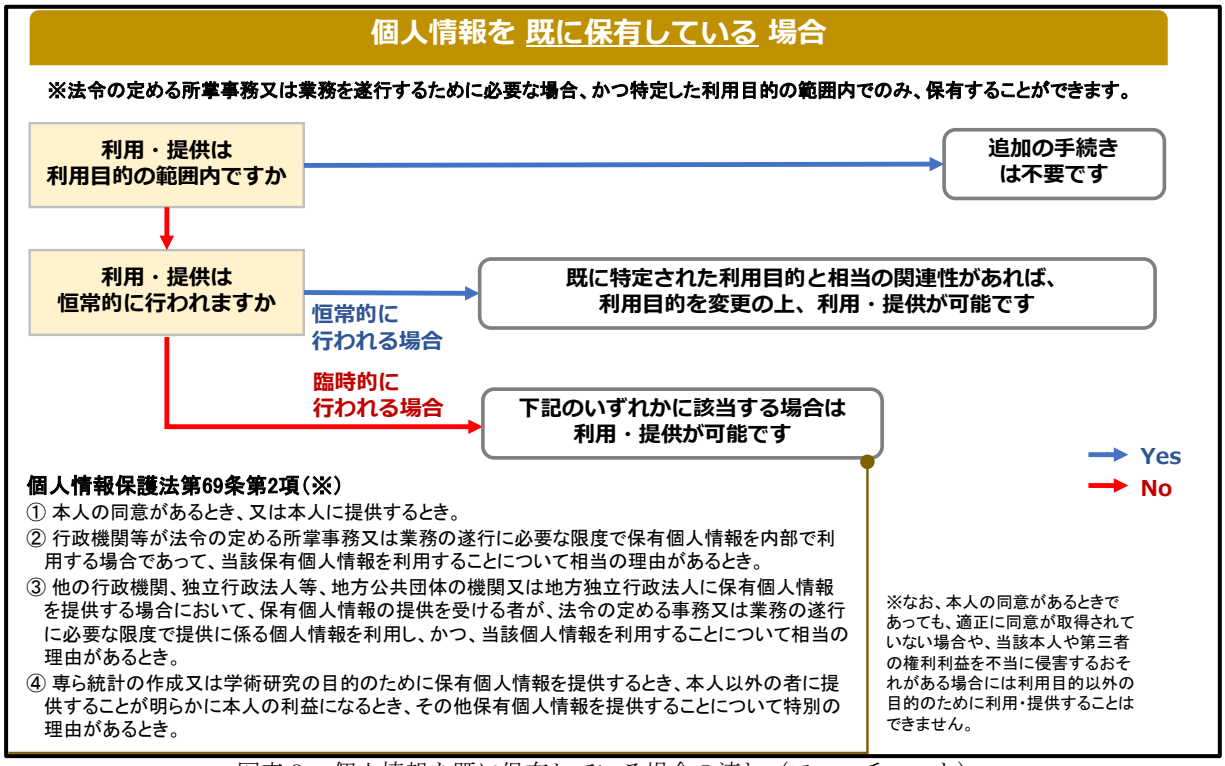
②本人以外の者に提供することが明らかに本人の利益になるときや③特別の理由があるときについても提供が可能な場合があります。

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、（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、ここまでに解説した内容を整理すると、図表９のようになります。

[46] 事務対応ガイド３-２-７
[47] ガイドライン５-５-２、事務対応ガイド４-５-２



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）

（５）提供先における適切な管理

地方公共団体の機関が保有・取得した個人情報を既存の利用目的のため当該機関以外に提供する場合、又は例外措置として利用目的以外の目的のため当該機関以外に提供する場合（他の行政機関等における利用が必要な限度で相当の理由がある場合[48]及び統計作成・学術研究や明らかに本人の利益になる場合[49]その他特別な理由がある場合）で、必要があると認めるときは、提供先における当該個人情報の利用目的や利用方法等の必要な制限を定め、その漏えいの防止等の個人情報の適切な管理のために必要な措置を講ずることを求めなければならないとされています[50]。

なお、「必要な制限」又は「必要な措置」としては、利用目的や利用方法の制限のほか、提供する個人情報を取り扱う者の範囲の限定、第三者への再提供の制限又は禁止、消去や返却等利用後の取扱いの指定、提供する保有個人情報の取扱状況に関する所要の報告の要求等が考えられます。例えば、提供先による無関係な利用を提供元の教育委員会が許容すると、教育委員会による提供が「特定した利用目的のためではない」と判断される可能性があるため、それを避けるために、提供先における利用の目的又は方法を制限することが考えられます。

地方公共団体の機関は、措置を要求した当該事項の遵守状況を把握し、その結果、措置要求が遵守されていない場合、遵守するよう求めることが必要です。

[48] 個人情報保護法第 69 条第２項第３号
[49] 個人情報保護法第 69 条第２項第４号
[50] 個人情報保護法第 70 条、ガイドライン５-５-３

１．３．４ 個人情報の保管

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 [51]。そのため、その個人情報が利用目的の達成に必要がなくなった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。

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内で、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とされています [52]。例えば、①過去のある時点の事実のみで足りる場合、②現在の事実を必要とする場合、③過去の事実と現在の事実の両方を必要とする場合があり得るため、利用目的に応じて必要な範囲で正確性を確保する必要があります [53]。

保管に当たって、必要な情報セキュリティ対策や安全管理措置については、「Ⅰ．総論編３」で解説しています。

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。

〇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

2　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。

3　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。

１．４ 個人情報の取扱いの委託

教育委員会・学校が、所掌事務の遂行のために、授業など児童生徒が一律に参加する教育活動でデ

[51] 個人情報保護法第 61 条第２項
[52] 個人情報保護法第 65 条
[53] ガイドライン５-２-４

ジタル教材等の学習用ソフトウェア等を活用することで取得される児童生徒の個人情報については、学習用ソフトウェア等を提供する民間事業者での取扱いも含め、当該教育委員会・学校で責任をもって取り扱う必要があります。そのため、この取扱いを担保するに当たっては、教育委員会・学校から民間事業者に「個人情報の取扱いを委託」することが一般的であると考えられ、望ましいことから、基本的にこうした対応が求められます。（Q&A 編－Q（８）も参照のこと）

このような学習用ソフトウェア等を利用する際をはじめ、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、個人情報の取扱いの全部又は一部を委託する場合は委託を受けた者（以下、「委託先」といいます。）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[54]。

〇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[55]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、委託先は委託された個人情報の取扱いに対して安全管理措置を講じる必要があり[56]、加えて、当該委託先事業者が個人情報取扱事業者[57]に該当する場合には、個人データの安全管理のために必要かつ適切な措置を講ずべき義務[58]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か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[59]。

また、委託元である地方公共団体の機関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[60]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

---

54 事務対応ガイド４-８-９

55 漏えい、滅失や毀損(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。

56 個人情報保護法第 66 条第２項

57 個人情報保護法第 16 条第２項

58 個人情報保護法第 23 条

59 ガイドライン５-３-１

60 事務対応ガイド４－８－９（６）に示される以下についても必要な措置を講ずることとなります。「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などを考慮し、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。」

回以上の確認を原則として行う等の必要があります[61]。

１．５ 個人情報等利用における体制及び手続上の留意点

１．５．１　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[62]。

１．５．２　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 [63]を漏れなく把握することが重要です。なお、個人情報ファイル簿を作成する必要性があるかどうかは各教育委員会において確認する必要があります[64]。

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 [65]及び条例要配慮個人情報 [66]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[67]。

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。

---

[61] 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）

[62] 個人情報保護法第５章第４節

[63] 「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。（個人情報保護法第 60 条第２項）

(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

[64] 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（個人情報保護法第 75 条第２項第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 条第２項第９号、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）第 19 条第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 条第２項１号）なお、条例で定めるところにより、個人情報ファイル簿に追加して、個人情報の保有の状況に関する事項を記載した帳簿を作成・公表することも可能とされています（個人情報保護法第 75 条第５項）。

[65] 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。本人の人種、信条、社会的身分、病歴、犯罪の経歴等が含まれます。（個人情報保護法第２条第３項）

[66] 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。

[67] 個人情報保護法第 74 条第１項第６号及び第 75 条第４項

１．５．３　苦情処理、漏えい・滅失・毀損した際の対応

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[68]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[69]。

また、地方公共団体の機関は、保有個人情報の漏えい、滅失、毀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[70]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[71]。（Q&A編－Q（10）も参照のこと）

１．５．４　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[72]。

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、対応等について審議会等に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

---

[68] 匿名加工情報と仮名加工情報の違いについては、「「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）A14-１

[69] 個人情報保護法第128条

[70] 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（平成28年個人情報保護委員会規則第３号）第43条）なお、③に関しては、「個人情報の保護に関する法律施行規則の一部を改正する規則」（令和５年個人情報保護委員会規則第５号）により、令和６年４月１日から、「不正の目的をもって行われたおそれがある当該行政機関の長等の属する行政機関等に対する行為による保有個人情報（当該行政機関の長等の属する行政機関等が取得し、又は取得しようとしている個人情報であって、保有個人情報として取り扱われることが予定されているものを含む。）の漏えい等が発生し、又は発生したおそれがある事態」となります。

[71] 個人情報保護法第68条

[72] 個人情報保護法第129条

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 [73]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）[74]
・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）[75]
・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）[76]

２．プライバシーの保護

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います。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、民事法上のプライバシー侵害となり、差止請求により教育活動の継続が困難になるリスクや、国家賠償法 [77]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、取組を推進する地方公共団体の機関への信頼が失墜し取組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

[73] https://www.ppc.go.jp/personalinfo/legal/
[74] https://www.ppc.go.jp/files/pdf/241127_koutekibumon_guidelines.pdf
[75] https://www.ppc.go.jp/files/pdf/202403_koutekibumon_jimutaiou_guide.pdf
[76] https://www.ppc.go.jp/personalinfo/legal/koutekibumon_qa/
[77] 昭和 22 年法律第 125 号

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と連携・協力、プライバシー影響評価（PIA）[78]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。

〇政策基本原則「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[79]が存在しています。「事後的でなく事前的であり、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」[80]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

[78] 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

[79] 「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 ver1.3」2023 年４月（経済産業省・総務省）（https://www.soumu.go.jp/main_content/000877678.pdf）

[80] 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）

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。

また、EU（European Union：欧州連合）の AI 規則案では、感情を推測する AI システムは、差別的な結果をもたらす可能性があると指摘されています。特に教育の場面においては、教師と子供の力関係により、特定の個人やグループの不利益につながる可能性があるとして、禁止すべきであると言及がなされています[81]。

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。

【コラム４】プライバシー侵害が成立する代表的な裁判例　（寄稿：弁護士 森亮二）

上述のとおり、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、プライバシー侵害となるリスクがあります。

ここでは、どのような場合にプライバシー侵害が成立するのかを把握するため、代表的な裁判例を紹介しています。なお、この文脈で問題になるのは、監視カメラや N システムなどの「取得・利用型」のプライバシー侵害の事案です。以下の通り、取得・利用型のプライバシー侵害については、①取得・利用する情報の性質、②取得・利用の必要性・目的、③取得・利用の態様、④取得後の情報の管理方法を総合的に判断して、プライバシー侵害かどうかが決せられるものと考えられています。

事例１　N システム事件

N システムとは、「自動車ナンバー自動読み取り装置」の略称です。①道路上に設置した端末装置のカメラで通過する車両をとらえ、②そこで得られた情報を端末装置に内蔵されたコンピュータで処理し、③自動車登録番号標の文字データのみを抽出し、④これを通信回線で各都道府県警察の警察本部に設置された自動車ナンバー照合装置に送り、⑤自動車ナンバー照合装置のコンピュータが当該データとあらかじめ登録されている手配車両のデータとを自動的に照合する、といった各機能を持つものです。車両運転者や同乗者などの車両に乗車している者の容ぼうなどの画像情報は記録されることがないとされています。犯罪捜査の重要な手掛かりとして機能することもありますが、警察による無作為的な情報収集行為がプライバシー侵害であるとして、これまで各地住民から複数の提訴を受けてきました。比較的最近の事件（東京地判平成 19 年 12 月 26 日）の違法性判断の基準は、以下のようなものです[82]。

> 憲法 13 条は，国民の私生活上の自由が警察権等の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おり，この個人の私生活上の自由の一つとして，何人も，その承諾なしに，公権力によってみだりに私生活に関する情報を収集・管理されることのない自由を有するものと解される。しかし，このような個人の有する自由も無制約のものではなく，公共の福祉のために必要のある場合には相当の制約を受けることは同条の規定するところである。よって，公権力による国民の私生活に関する情報の収集・管理が同条の趣旨に反し，国賠法上の違法性を有するか否かは，①　公権力によって取得，保有，利用される情報が個人の思想，信条，品行等に関わるかなどの情報の性質はどのようなものか，②　公権力がその情報を取得，保有，利用する目的が正当なものであるか，③　公権力によるその情報の取得，保有，利用の方法が正当なものであるか，④　公権力によるその情報の管理方法の厳格さはどの程度か，などを総合して判断すべきである。

事例２　著名人コンビニ万引き事件[83]

コンビニの防犯カメラにおける撮影行為自体が肖像権・プライバシーを侵害するものとして不法行為に当たるかが争われた事件です。本判決の示す違法性の基準は、以下のようなものです。

---

[81] https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-FullText.pdf
[82] 同じ N システムに関する事件でも、かつての裁判例の判断基準は①から③までであった。
[83] 判例タイムズ 1343 号 153 頁

本件監視カメラにおいて，本件店舗内の客を撮影し，その撮影に係る画像を報道機関に提供することによりこれを公表等することが不法行為法上違法といえるか否かは，撮影の目的，撮影の必要性，撮影の方法及び撮影された画像の管理方法並びに提供の目的，提供の必要性及び提供の方法等諸般の事情を総合考慮して，上記姿を撮影され撮影に係る画像を公表等されない利益と上記姿を撮影し撮影に係る画像を公表等する利益とを比較衡量して，上記人格的利益及びプライバシー権の侵害が社会生活上受忍限度を超えるものかどうかを基準にして決すべきである。

事例３　住基ネット事件

住基ネットについては、2002 年 8 月の稼働以降、自己情報コントロール権の侵害等を理由として、全国各地の裁判所に多数の提訴がなされてきました。その大多数において原告住民が敗訴しましたが、大阪高判平成 18 年 11 月 30 日[84]は原告住民の請求を認容し、住基ネットの違憲性を認めました。

本判決は、「行政機関において、住民個々人の個人情報が住民票コードを付されて集積され、それがデータマッチングや名寄せされ、住民個々人の多くのプライバシー情報が、本人の予期しない時に予期しない範囲で行政機関に保有され、利用される危険が相当あるものと認められる」として、原告住民による住民票コードの削除請求を認めたのでした。なお、本判決の上告審である最判平成 20 年 3 月 6 日[85]は、原審の結論を否定して、原告住民の請求を棄却しましたが、その理由について、以下のように述べています。

第一に、最高裁は、住基ネットのプライバシー侵害性について、以下のように判示しています。

A①　住基ネットによって管理，利用等される本人確認情報は，氏名，生年月日，性別及び住所から成る４情報に，住民票コード及び変更情報を加えたものにすぎないが，これらはいずれも，個人の内面に関わるような秘匿性の高い情報とはいえない。これらの情報は，住基ネットが導入される以前から，住民票の記載事項として，各市町村において管理，利用され，法令に基づき必要に応じて他の行政機関等に提供され，利用されてきたものである。

A②　住民票コードの秘匿性の程度は本人確認情報と異なるものではない。

A③　住基ネットにシステム技術上又は法制度上の不備があり，そのために本人確認情報が法令等の根拠に基づかずに又は正当な行政目的の範囲を逸脱して第三者に開示又は公表される具体的な危険が生じているとの懸念については、罰則や都道府県における審議会の設置などの措置がなされていることから、現実のものではない。

第二に、最高裁は、原審が指摘する２つの違法の理由のうち、名寄せのリスクについて以下のとおり反論しています。「原審は（中略）住民が住基カードを用いて行政サービスを受けた場合，行政機関のコンピュータに残った記録を住民票コードで名寄せすることが可能であることなどを根拠として，住基ネットにより，個々の住民の多くのプライバシー情報が住民票コードを付されてデータマッチングされ，本人の予期しないときに予期しない範囲で行政機関に保有され，利用される具体的な危険が生じていると判示する。しかし」

B①　システム上，住基カード内に記録された住民票コード等の本人確認情報が行政サービスを提供した行政機関のコンピュータに残る仕組みになっているというような事情はうかがわれない。

B②　データマッチングは本人確認情報の目的外利用に当たり，それ自体が懲戒処分の対象となるほか，データマッチングを行う目的で個人の秘密に属する事項が記録された文書等を収集する行為は刑罰の対象となり，さらに，秘密に属する個人情報を保有する行政機関の職員等が，正当な理由なくこれを他の行政機関等に提供してデータマッチングを可能にするような行為も刑罰をもって禁止されている。

B③　本人確認情報の提供が認められている行政事務において取り扱われる個人情報を一元的に管理することができる機関又は主体は存在しないことなどにも照らせば，住基ネットの運用によって原審がいうような具体的な危険が生じているということはできない。

以上のとおり、本件は、住民票コードによるデータマッチングや名寄せのリスクが主な争点となった事件でした。原審が指摘する「住基ネットにより，個々の住民の多くのプライバシー情報が住民票コードを付されてデータマッチングされ，本人の予期しないとき

[84] 判例時報 1962 号 11 頁
[85] 判例タイムズ 1268 号 110 頁、判例時報 2004 号 17 頁

に予期しない範囲で行政機関に保有され，利用される具体的な危険が生じている」という点に関して、最高裁は、そのような危険が仮に生じていればプライバシー侵害をもたらすこと自体については認めつつも、システムの仕組み上および制度上、そのような危険を回避する仕組みが採られていたことから、プライバシー侵害を否定したのです。

３．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[86]の一つである「⑤個人情報等の取扱いの安全性」の原則にしたがい、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を実施することが重要です。

このためには、主に地方公共団体が設置する学校を対象とした教育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。）や最新の「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）[87]、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ポリシーは、各地方公共団体が組織の実態に応じて自主的に策定や見直しを行うものであり、その参考として「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和６年 10 月）」（以下、「自治体ガイドライン」といいます。）が総務省において整備されています。情報セキュリティポリシーは、情報セキュリティ対策の頂点に位置するものであり、本来は地方公共団体全てを包括するポリシーでなければなりません。

一方で、地方公共団体が設置する学校においては、地方公共団体の他の行政事務とは異なる特徴を有します。例えば、学校とは地方公務員法及び教育公務員特例法に定める「服務」に服さない児童生徒が過ごす場所であり、当該児童生徒がコンピュータを活用した学習活動の実施などにおいて、日常的に情報システムにアクセスする機会があります。そのため、児童生徒においても情報セキュリティポリシーにて規定した対策について遵守するよう、職員、教員、保護者等が適切に指導を行うことが求められます。

また、学校には、指導要録、答案用紙、生徒指導等の記録、進路希望調査票、児童生徒等の住所録

[86] 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

[87] https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm

等の重要性が高い情報が保管されています。児童生徒の育成においては、学校教育に直接関わる複数の関係者により、児童生徒に関する情報が多目的で活用されます。学習においても、教職員や他の児童生徒と協働学習活動を実践する際、児童生徒が生み出す情報は本人の思考の記録であるとともに学習評価の材料となり、必要に応じて他児童生徒に開示する等多目的に活用されます。よって、学校教育においては、児童生徒の存在及び取り扱う情報の多様性・多目的性等を考慮した情報セキュリティ対策を講ずる必要があります。

このような背景を踏まえ、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、その後も改訂を行ってきました。

「教育情報セキュリティポリシーに関するガイドライン」では、以下の①～⑦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。（Q&A 編－Q（10）（11）も参照のこと）

○「教育情報セキュリティポリシーに関するガイドライン」より抜粋

第 1 編第 2 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。

⑦児童生徒の情報セキュリティ・情報モラルに関する意識の醸成を図ること

児童生徒が 1 人 1 台の学習者用端末を活用し学習活動を行うことから、教職員等からの指導を通じて、児童生徒の情報セキュリティ・情報モラルに関する意識の醸成を図ることが必要である。インターネット等の安全な利用や、コミュニケーションツールにおけるモラル習得など、児童生徒を被害者にも加害者にもしないための指導が必要である。

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[88]。

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るため、不要となった場合は削除・廃棄等の適切な対応を行う必要があります。

３．２．１　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。

３．２．２　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、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。

３．２．３　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。　（Q&A 編－Q（９）も参照のこと）

---

[88] 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）

３．２．４　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、窃取又は不正な削除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。

３．２．５　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。

３．２．６　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。

II. 手順編

本編では、実際に教育委員会・学校が学習用ソフトウェア等（ツール）を導入する際に、個人情報保護等の観点から実施すべきこと、実施が望ましいことについて、順に解説しています。教育データを利活用する際には、手順編を踏まえ、適切に行うようにしてください。

◎：個人情報保護法などの法律の規定に基づき、必ず行うべきことです。教育委員会・学校で必ず行うようにしてください。
○：教育データが活用されるのが学校であるという性質を踏まえ、行うことが望ましいとされることです。必要に応じ、各教育委員会・学校の判断で行うようにしてください。

１．　取得

留意点	具体的な対応例
［◎］ **a　利用目的（ツールを導入することで取得するデータ※の利用目的）を特定する** 教育委員会・学校は、ツールを導入することで取得するデータの利用目的をできる限り特定しなければなりません。 ツール導入時に加え、ツールの機能の追加等により取得するデータが増える際も利用目的の特定が必要なので、留意してください。 個人情報の保有は、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ます。 ※すべての項目において、「データ」は、個人情報を含むデータのことを指します。	**利用目的の例** 「Ⅲ．事例編」を参照
［○］ **b　データの取扱い等に係る整理を文書化しておく** 教育委員会は、導入するツールにおけるデータの取扱い等を内部で整理し、文書化しておくことが望まれます。	**文書化する事項例** ・　サービス概要（児童生徒の得られる教育的メリット等） ・　利用目的 ・　データ管理体制 ・　収集するデータ ・　データ取得の方法（例：児童生徒がツールに入力） ・　データ収集のタイミングと場所（例：ツール起動中に回答情報を収集、バックグラウンドで操作ログを収集） ・　利用手法（例：収集した回答情報を元に、正誤判定を実施） ・　データを保管する地理的位置及び法域（海外にサーバがある等）（例：日本） ・　第三者提供の有無、第三者提供先 ・　保存期間 ・　本人の権利（開示請求等）への対応方法 ・　問い合わせ先 ・　データ処理の根拠 ・　想定されるリスク（例：児童生徒に対して発生しうるプライバシーリスク）

留意点	具体的な対応例
［◎］ **c 児童生徒本人に対し、利用目的を明示する** 学校は、児童生徒から直接、ツールを通じてデータを取得するときは、あらかじめ、児童生徒本人に対し、データの利用目的を明示しなければなりません。	**児童生徒本人に利用目的を明示する方法例** **注）明示方法は、文書でも口頭でも可能** ・ 児童生徒に端末を貸し出す際に、利用目的を明示する ・ 児童生徒に説明会を開催し、利用目的を分かりやすく説明する ・ ツールの利用を開始する際に、利用目的をツール上の画面に表示し、説明する **注）取得の状況から見て利用目的が明らかであるときは明示が不要。明示が不要となる例：** ・ 宿題の実施状況を確認するため、宿題を提出させるとき ・ 部活動に関わる連絡を行うため、入部届で連絡先を集めるとき ・ 通学証明書発行のため、通学証明書発行申請書で通学に関わる個人情報を取得するとき
［◎/○］ **d 児童生徒に加え、保護者に対しても利用目的を明示する** ※児童生徒の発達段階によっては、利用目的の内容について児童生徒本人が理解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のみ、そうでない場合は保護者にも明示することが基本です。 ※学校教育においては保護者が利用目的を把握しておきたいと考えていることもあるので、児童生徒が 15 歳以下の場合など、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明示することが推奨されます。	**保護者に利用目的を明示する方法例** ・ 年度ごとに行う、IT ツール利用に伴う保護者向けのお知らせ文書に、データの利用目的を明確に記載する ・ 保護者向けに説明会を開催し、利用目的をわかりやすく説明する
［○］ **e 児童生徒や保護者に対し、利用目的を明示する際、利用目的に加えデータの取扱いについても説明する** 学校は、児童生徒・保護者が安心してツールを使えるよう、利用目的に加えてどのようにデータが取り扱われるかについて、説明することが望ましいです。	**利用目的に加えて説明する事項例** **（上述「文書化する事項例」の再掲）** ・ サービス概要（児童生徒の得られる教育的メリット等） ・ データ管理体制 ・ 収集するデータ ・ データの収集手法 ・ データ収集のタイミングと場所 ・ 利用手法（他のデータとの突合等） ・ データを保管する地理的位置及び法域（海外にサーバがある等） ・ 第三者提供の有無、第三者提供先

留意点	具体的な対応例
	・ 保存期間 ・ 本人の権利（開示請求等）への対応方法 ・ 問い合わせ先 ・ データ処理の根拠 ・ 想定されるリスク

２．利用、提供

留意点	具体的な対応例
［◎］　**a　利用目的以外の目的の利用･提供を行う際は適切な対応を行う** 教育委員会は、既に取得しているデータを利用目的以外の目的で利用･提供する場合は、利用目的の変更を行わなければなりません。 利用目的の変更を行う場合は、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に限ります。 ※個人情報保護法第 69 条第 2 項の要件を満たしている場合は、これらの対応は不要です（「Ⅰ．総論編 １．３．３」参照）	**利用目的を変更する例** ・　児童生徒の成績処理を行うために取得したデータを、教育委員会が学校毎の成績状況の把握のための統計作成に活用する場合
［◎］　**b　個人情報の取扱いの委託先を適切に管理する** 教育委員会は、個人情報の取扱いを委託する場合、適切な管理のために必要な措置を講じなければなりません。	**委託先を適切に管理するために行うべき事項の例** ・　委託先の選定基準等を整備し、委託先の選定や契約に当たって確認を行う ・　委託先の事業者との契約書や覚書等の文書に以下の項目を取り入れる ✓　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に関する事項 ✓　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 ✓　個人情報の複製等の制限に関する事項 ✓　個人情報の安全管理措置に関する事項 ✓　個人情報の漏えい等の事案の発生時における対応に関する事項 ✓　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 ✓　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 ✓　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 ・　上記で確認した契約内容について、以下のタイミング等で確認を行う ✓　新たに契約を行うとき ✓　契約の更新を行うとき ✓　契約内容や提供するサービスの内容に大きな変更があるとき

留意点	具体的な対応例
	・ 契約締結後は、年に一回程度適切な監査を行う （参考）個人情報の取扱いの委託先を管理するため、自治体独自で実施している取組例 ✓ 委託先の選定や契約に当たって第三者認証の認定状況を確認する ✓ 委託先の選定時にプライバシーポリシーを確認し、個人情報を適切に管理しているかを確認する
［◎］ **c 提供先が個人情報を適切に管理するための必要な措置を講ずる** 教育委員会は、保有個人情報や個人関連情報を研究者等に外部提供を行う場合、適切な管理のために必要な措置を講じなければなりません。	**必要な措置の例** ・ 提供先の選定基準等を整備し、提供先の選定や契約に当たって確認を行う ・ 提供先の事業者との契約書や覚書等の文書に以下の項目を取り入れる ✓ 利用の目的又は方法を最小限に制限する ✓ 利用目的以外の利用は行わない ✓ 個人情報を取扱う者を最小限に限定する ✓ 第三者へのデータの再提供の制限又は禁止する ✓ 終了後は、消去や返却等をする ✓ データの取扱状況に関して報告を行うことを求める ・ 上記で確認した契約内容について、以下のタイミング等で確認を行う ✓ 新たに契約を行うとき ✓ 契約の更新を行うとき ✓ 契約内容や提供するサービスの内容に大きな変更があるとき

３．保管

留意点	具体的な対応例
［◎］ **a 利用目的の達成に必要な範囲で個人情報を保有する**	**必要な範囲内で保有するための運用上の工夫例** ・ 教育委員会・学校は、利用目的の達成のために必要な情報を整理し、最小限の情報を保有する ・ 教育委員会は、あらかじめ利用目的の達成に必要な範囲で教育データを保有する際の規則（保存期間（例：卒業後○か月間）など）を定め、保存期間の経過など利用目的の達成に必要がなくなった個人情報は削除する ・ 教育委員会は、委託先においてもこれらのルールに則って運用されていることを確認する **利用目的の範囲内で保有、利用・提供を行っているか確認を行うことが望ましいタイミングの例** ・ 新たな年度が始まるとき ・ 新たに外部へ提供を行おうとするとき
［○］ **b データの正確性を確保する** 教育委員会・学校は、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に努めましょう。	**正確性を確保するための工夫例** 学校は、ツール内の児童生徒の学年、クラス、出席番号等の情報が現在の事実と合致するように、特に以下のタイミングで確実な更新を行う ・ 年度初め ・ 転出入があった場合
c 安全管理措置 **（１） 組織的安全管理措置** ［◎］**① 組織体制の整備** 教育委員会・学校は、安全管理措置を講ずるための組織体制を整備しなければなりません。	**組織体制として整備する項目の例** ・ 教育委員会においては、データの取扱いに関する責任者を設置し、各担当者の役割分担及び責任の明確化を行う ・ 学校においては、各担当者の役割分担及び責任の明確化を行う **役割分担の例** ✓ 6-1 の担任：6-1 の学習履歴 ✓ 6 年生学年主任：6 年生全クラスの学習履歴 ✓ 専科教員：授業を受け持つクラスの学習履歴 ・ 教育委員会においては、データの取扱いに係る規律への違反やデータ漏えい事案が発生している事実又は兆候を把握した場合の責任者への報告連絡体制を整備し、学校に伝達する

留意点	具体的な対応例
［◎］② **利用状況の確認** 教育委員会・学校は、あらかじめ整備された保有個人情報の取扱いに係る規律に従って保有個人情報を取り扱わなければなりません。教育委員会・学校は、これらの運用の状況を確認するため、利用状況等を確認することが望まれます。	**利用状況等を確認する方法の例** ・ 利用ログの記録 ・ 業務日誌の作成 ・ 監査の実施 ・ 不正な利用に対しアラートを実施 **利用状況等を確認する対象の例** ・ 保有個人情報の利用・出力状況 ・ 保有個人情報が記載又は記録された書類・媒体等の持ち運び等の状況 ・ 保有個人情報の削除・廃棄の状況（委託した場合の委託先での消去・廃棄を証明する記録を含む。） ・ 保有個人情報を情報システムで取り扱う場合、担当者の情報システムの利用状況（ログイン実績、アクセスログ等）
［◎］③ **安全管理措置の見直し** 教育委員会は、保有個人情報の取扱状況を踏まえ、安全管理措置の評価、見直し及び改善に取り組まなければなりません。	
［◎］**（２）人的安全管理措置** 教育委員会・学校は、教職員に、保有個人情報の適正な取扱いを周知徹底するとともに適切な教育を行わなければなりません。	**周知徹底するための方法例** ・ 保有個人情報の取扱いに関する留意事項について、教職員に定期的な研修等を行う ・ 保有個人情報についての秘密保持に関する事項を条例等に盛り込む
［◎］**（３） 物理的安全管理措置** **① 保有個人情報を取り扱う区域の管理** 教育委員会・学校は、管理区域と取扱区域について、それぞれ適切な管理を行わなければなりません。	**管理区域（庁舎のサーバ室等）の適切な管理例** ・ 管理区域に持ち込む機器等を制限する ・ 入退室管理として、IC カード、ナンバーキー等による入退室管理システムを設置する **取扱区域（教育委員会の担当部局や学校の職員室等）における適切な管理例** ・ 間仕切り等を設置する ・ 入り口から PC 画面が見えないように座席配置を工夫する ・ のぞき込み防止フィルムの画面への貼付や、スクリーンの自動ロックの設定など、のぞき込みを阻止する措置を実施する 注） ・ 管理区域：保有個人情報を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域。一般的に学校にはなく、教育委員会等に設置される

留意点	具体的な対応例
	・ 取扱区域：その他のデータを取り扱う事務を実施する区域。一般的に教育委員会の担当部局や学校の職員室が該当する
［◎］② **機器及び電子媒体等の盗難やデータの漏えい等の防止** 教育委員会・学校は、保有個人情報を取り扱う機器、電子媒体及び書類等の盗難又は紛失やデータを持ち運ぶ場合の漏えい等を防止するために、適切な管理を行わなければなりません。	**盗難や漏えいを防止するための方法例** ・ データを取り扱う部局や職員室の施錠を徹底する ・ データを取り扱う機器、データが記録された電子媒体又はデータが記載された書類等を、施錠できるキャビネット・書庫等に保管する ・ 持ち運ぶデータの暗号化、パスワードによる保護等を行った上で電子媒体に保存する
［◎］③ **保有個人情報の削除及び機器、電子媒体等の廃棄** 教育委員会・学校は、保有個人情報を削除し又は保有個人情報が記録された機器、電子媒体等を廃棄する場合は、復元不可能な手段で行わなければなりません。	**廃棄する方法例** ・ パソコンを含む情報システムにおいてデータを削除する場合、容易に復元できない手段を採用する ・ データが記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を採用する ・ データを印刷した紙媒体は、焼却・溶解・適切なシュレッダー処理等により適切に廃棄する **注）廃棄を外部に委託する場合は、廃棄した記録を証明書等により確認することが望まれます。**
［◎］**（４） 技術的安全管理措置** **① アクセス制御と認証** 教育委員会は、担当者及び取り扱う保有個人情報の範囲を限定するために、適切なアクセス制御を行わなければなりません。	**アクセス制御の例** ・ 個人情報を取り扱うことのできるシステムを限定する ・ ユーザ ID に付与するアクセス権により、個人情報を取り扱うシステムを使用できる教職員を限定する ・ パブリッククラウド上で重要な情報を取り扱う際に多要素認証を含む「強固なアクセス制御 [89]」による対策を行う **情報システムを使用する従業者の識別・認証手法の例** ・ ユーザ ID とパスワードで認証する ・ 磁気・IC カードをかざして認証する ・ 知識認証、生体認証（指紋、 静脈、顔、声紋等）、物理認証（IC カード、USB トークン、トークン型ワンタイムパスワード等）のうち、異なる認証方式 2 種類を組み合わせ、多要素で認証する

[89] 「GIGA スクール構想の下での校務 DX について～教職員の働きやすさと教育活動の一層の高度化を目指して～」（令和 5 年 3 月 8 日）p.18 にて示されている、インターネットを通信経路とする前提で、内部・外部からの不正アクセスを防御するために、利用者認証（多要素認証）、端末認証、アクセス経路の監視・制御等を組み合わせたセキュリティ対策

留意点	具体的な対応例
［◎］② **外部からの不正アクセスや漏えい等の防止** 教育委員会は、保有個人情報を取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護するための仕組みや、保有個人情報の漏えい等を防止するための措置を講じ、適切に運用しなければなりません。	**不正アクセス防止の手法の例** ・ 情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する ・ 情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入し、不正ソフトウェアの有無を確認する ・ 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする ・ ログ等の定期的な分析により、不正アクセス等を検知する
	情報システムの仕様に伴う漏えい等防止の手法の例 ・ 情報システムの設計時に安全性を確保し、継続的に見直す（情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む。） ・ データを含む通信の経路又は内容を暗号化する
［◎］**（５）外的環境の把握** ツール事業者が、外国において保有個人情報を取り扱う場合、当該外国を特定し個人情報の保護に関する制度等を把握した上で、保有個人情報の安全管理のために必要かつ適切な措置を講じなければなりません。	**注）海外にデータセンターを持つ事業者を選定する場合は、日本法が適用されない可能性があることを踏まえて慎重に検討する必要があります**
［◎］ **ｄ 個人情報ファイル簿を作成・公表する** 教育委員会は、所定の事項を記載した個人情報ファイル簿を作成して公表しなければなりません。	**個人情報ファイル簿の公表方法の例** ・ 教育委員会に備えて置く ・ ホームページで公開する
［◎］ **ｅ 請求権に適切に対応する** 教育委員会は、本人等による開示請求、訂正請求及び利用停止請求に適切に対応できるよう、請求が来た場合の手順を整備し、教育委員会・学校はそれに沿って対応しなければなりません。	**適切な対応を行うための工夫例** ・ 請求窓口や案内窓口の整備し、請求に係る手続等を分かりやすく示す ・ 自治体内の手続きに則って対応する ・ 自治体内の手続きとは別に、個別に教育分野における手続きを定め、対応する
［◎］ **ｆ インシデント発生時に適切に対応する** 教育委員会は、保有する個人情報の漏えい等のインシデントが発生した場合の手順をあらかじめ整備し、教育委員会・学校はそれに沿って対応しなければなりません。	**インシデント発生時に適切に対応するための工夫の例** ・ 教育委員会・学校は、自治体の定めるセキュリティポリシー等をもとに、インシデント発生時の対応ルールやフローを確認しておく ✓ 事実関係の調査及び原因の究明 ✓ 影響を受ける可能性のある本人への通知 ✓ 個人情報保護委員会等への報告 ✓ 再発防止策の検討及び決定 ✓ 事実関係及び再発防止策等の公表　等 ・ インシデントが発生した場合、確認した手順に沿って対応を

留意点	具体的な対応例
	行う。あわせて情報管理の責任者に相談しつつ、速やかに原因を特定し、対策を立案・実行する

III.　事例編

本編では、ある学校において学習用ソフトウェア等（ツール）を導入したシナリオに沿って、個人情報の適正な取扱い等の観点から行った主な対応について記載しています。

本資料で示す【主に実施したこと】はあくまで一例であり、実際には個人情報保護法を踏まえた対応を適切に行う必要があります。具体的に取るべき対応については、Ⅰ．総論編及びⅡ．手順編を参照してください。

事例１
A 市立 B 小学校において、授業中に、児童が自ら考えなどを書き込んだり他者と共有したりしながら学習を進めるためのデジタル教材を利用する

事例２
A 県立 C 高等学校において、生徒が、問題を解いて習熟度に応じたフィードバックを得られるデジタルドリルを利用する

事例３
A 市立 D 中学校において、生徒が、様々な学習ツールにつながるソフトウェア（学習 e ポータル）を利用する

事例４
A 市立 E 中学校において、生徒に対し、アンケートなどを行うためのツール（OS メーカーが標準的に提供するソフトウェアの一部）を利用する

事例５
A 市立 F 小学校において、児童の学習状況や健康情報を一覧できるツールを利用する（校務支援システム等）

事例６
A 市立 G 小学校において、児童の心の健康状態を把握するツールを利用する

事例７
A 市立 H 中学校において、部活動時の熱中症リスクの軽減のためにウェアラブル端末を利用する

事例８
A 市立 I 中学校において、体育の授業で、生徒の技能習得と向上を促すために、動作解析ツールを利用する

事例１

事例１　A 市立 B 小学校において、授業において、児童が自ら考えなどを書き込んだり他者と共有したりしながら学習を進めるためのデジタル教材を利用する

シナリオ

A 市教育委員会において、域内の全小学校全学年で利用するために、授業で協働的な学習を行うために、次のようなデジタル教材を導入することにした。それにあたり、A 市教育委員会及び域内の小学校の一つである B 小学校において、新たなツール導入に当たって個人情報等の観点から必要な対応を行っている。

○ 導入するツールが有する主な機能のイメージ

- 児童は端末上で、気づきやメモを残すことができる。ツール上で作成した課題等について、クラス全体で児童の回答結果や成果物を共有できる。
- 他の児童の成果物に対して、コメントや「良いね」等の評価をつけられる。

○ ツールを導入するメリット

（児童）

- 意見や気づきを書き込んだり、修正したりして、学びを記録することができる。
- 学習履歴を記録することで、自分自身の学びを振り返ることができる。
- 個人やグループの成果物をクラス内等で他者に伝えあうことで、お互いに学びを深めることができる。

（教員）

- リアルタイムで個人またはグループの学習状況を把握し、必要な声かけを行うなど、効果的な指導を行うことができる。

○ 取り扱う主な個人情報

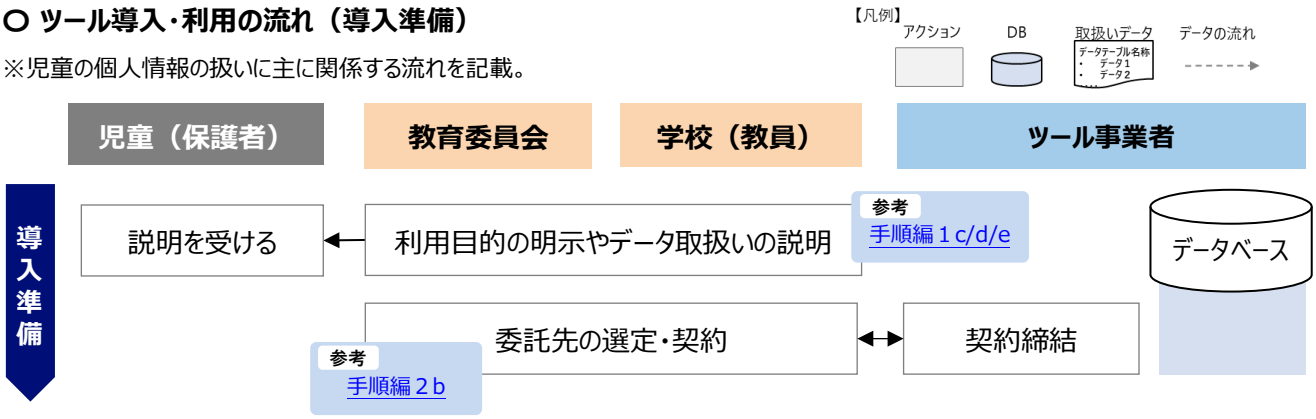
※ツールを単体で導入する場合を想定。学習 e ポータルを経由する場合は事例 3 を参照してください。

データ種別	主なデータの内容	取得方法
児童情報	ID・パスワード	ツール利用に当たって、A 市教育委員会が発行
	氏名	（あらかじめ保有）
	所属学年・クラス	
	出席番号	
教員情報	ID・パスワード	ツール利用に当たって、A 市教育委員会が発行
	閲覧権限	ツール利用に当たって、A 市教育委員会又は B 小学校が設定
	所属学年・担当クラス	（あらかじめ保有）
学習情報	児童生徒の成果物	児童生徒が、各自の端末で作成した成果物をツール上で登録
	児童生徒や教員からのコメントや評価	公開された成果物に対して、児童生徒や教員がコメント等をつける

事例１

○ ツール導入・利用の流れ（導入準備）

※児童の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜利用目的（ツールを導入することで取得するデータの利用目的）を特定する＞

- A 市教育委員会において、「学習指導に用いる」等の抽象的な利用目的ではなく、具体的に、何のデータ項目をどのように使用して指導するのか、まで検討した上で、利用目的を以下のように設定した。
  - 児童の学習状況を把握して学習指導を行うため

＜利用目的やデータの取扱いの説明をする＞

- B 小学校の教職員が、児童にプリントを配付して、特定した利用目的を明示し、データの取扱いについて説明した。
- また、小学生は 15 歳以下であり、本件についての判断能力が不十分であるため、保護者に連絡メールを配信し、同様の内容について説明をした。また、念のため保護者会においても保護者宛に口頭で説明を行った。

【プリントに記載した内容】

➢ 利用目的
- 児童の学習状況を把握して学習指導を行うため

➢ サービス概要

このツールを用いることで、授業や家庭学習で各自の端末で作成する成果物を提出したり、お互いに共有し、コメントしあったりできます。

➢ 本ツールで扱う主な個人情報
- 氏名、学籍番号
- 児童が各自の端末で作成する成果物
- 共有された他者の成果物に対するコメント

➢ データの収集手法

本人が成果物を提出したり、コメントを記入したりすることによりデータは収集されます。

➢ 第三者提供の有無

大学・研究機関等への第三者への提供はしません。

➢ 保存期間

データは、卒業して○か月後に削除します。

＜委託先の選定・契約＞

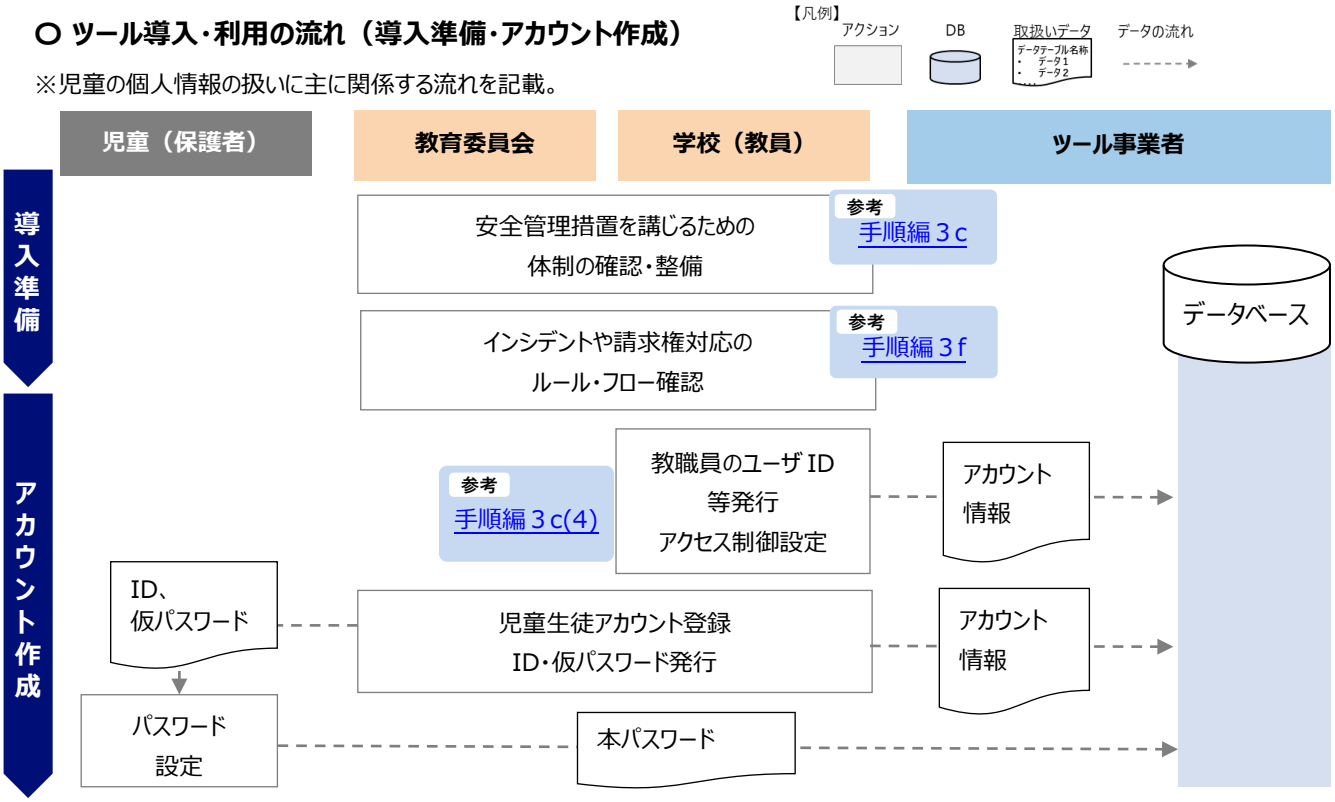
- A 市で整備している委託先の選定基準を踏まえて公告を行い、落札した事業者と A 市で契約を行った。

事例１

- 委託先との契約に当たっては、契約書に「データの利用や方法を最小限にすること」や「契約終了後はデータを削除すること」等について記載をした。 ☞契約に当たっては、「Ⅰ．総論編１．４」や「Ⅱ．手順編２b」に記載の事項も確認しましょう。

○ ツール導入・利用の流れ（導入準備・アカウント作成）

※児童の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置を講じるための体制の確認・整備＞

- 組織的安全管理措置として役割分担の明確化のため、A 市教育委員会において教育長が総括管理責任者であることを確認した。B 小学校においては、全体の管理責任者は学校長であることを確認するとともに、各クラスのデータは学級担任が責任を持つことを確認し、ツール導入に当たり、教職員にあらためて職員会議で周知した。

  ☞その他の安全管理措置として行うべき事項や留意点は 、「Ⅰ．総論編３．２」や「Ⅱ．手順編３c」も参照してください。

＜インシデントや請求権対応のルール・フロー確認＞

- A 市教育委員会において、個人情報の取扱いに係る規律への違反やデータ漏えい事案等のインシデントが発生した場合のフローを改めて確認し、各学校においてインシデントが発生している事実又は兆候を把握した場合の責任者への報告フローについて、学校に伝達した。
- B 小学校において、インシデント発生時の対応フローと役割分担を整理し、職員会議で周知した。

＜利用目的の達成に必要な範囲で個人情報を保有、利用・提供する＞

事例 1

- B 小学校において、ツールの利用に必要な児童の氏名や ID 等を入力した。児童の電話番号は、ツール利用に当たって不要だったため、ツール上に登録をしなかった。

  ポイント：データ登録が必須ではない項目については、利用目的に照らし合わせて、登録の要否を検討しましょう。

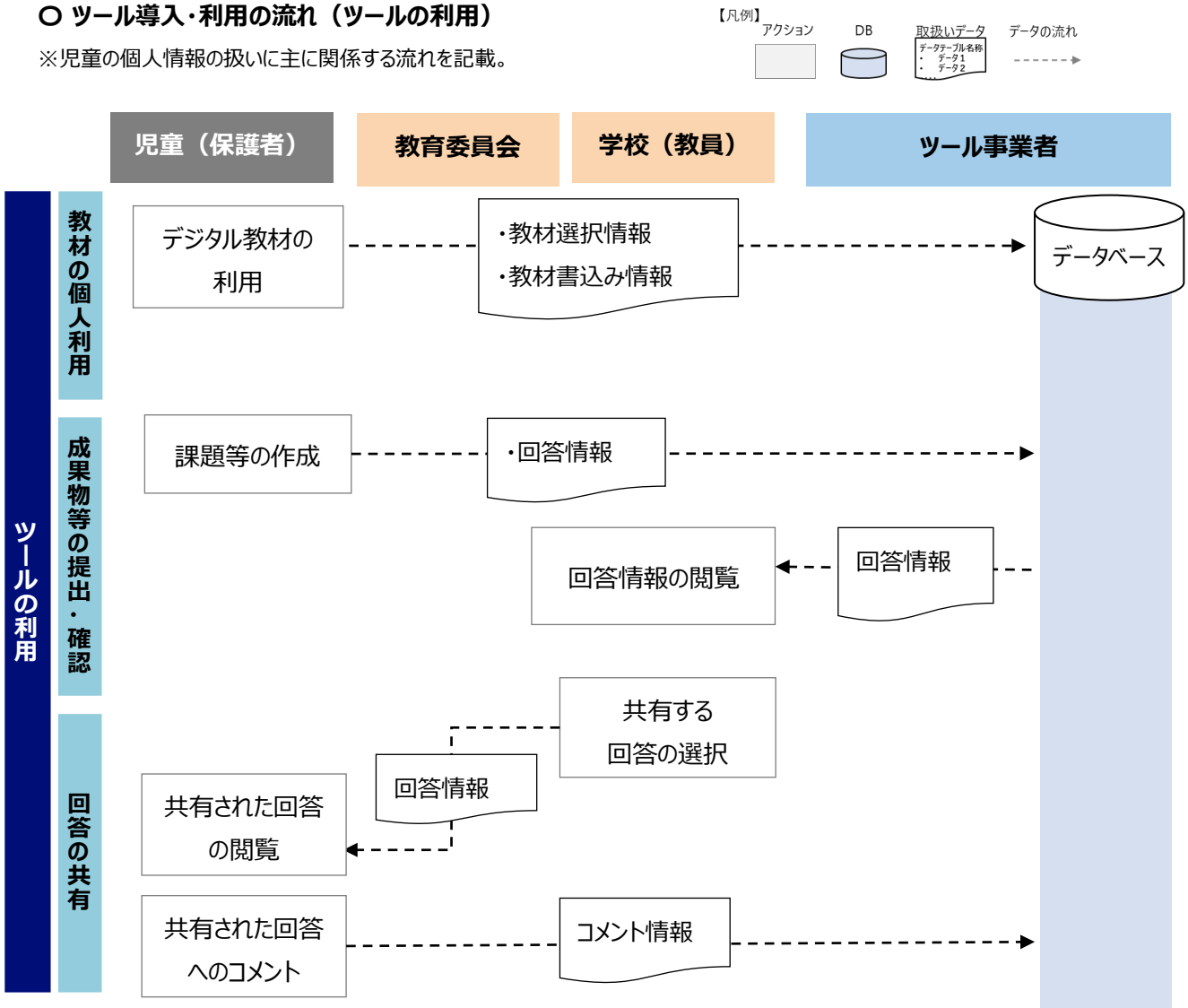
＜認証とアクセス制御＞

- B 小学校において、アカウント作成時に各アカウントでできること（閲覧、編集、アカウント登録・削除等）を整理して、必要な教職員がデータを見られるようにした。具体的には、担任教師は担任しているクラスのデータを、専科教師等は授業を受け持つクラスのデータを、学年主任は学年全てのクラスのデータを、管理職は学校内の全てのデータを閲覧・編集できるように設定した。
- アカウント登録・削除等は、管理職のみが実施できるように設定した。

  ポイント：情報漏えい等を避けるため、アカウントの権限設定に当たっては、真に必要な人のみに権限を付与し、不要な人に権限付与を行わないようにしましょう。

○ ツール導入・利用の流れ（ツールの利用）

※児童の個人情報の扱いに主に関係する流れを記載。



事例１

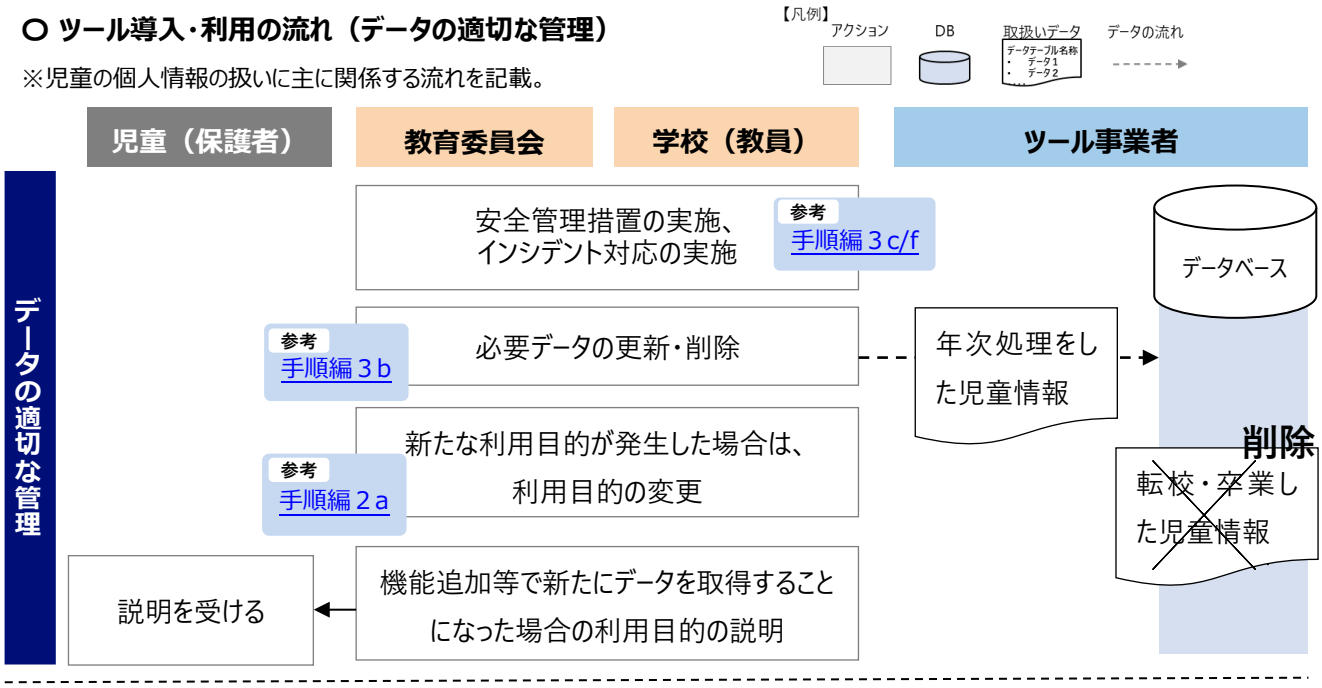
【主に実施したこと】

＜認証とアクセス制御＞

- B 小学校において、回答の共有は基本的にクラス内のみになるように設定を行った。また、一部合同授業やレベル別授業が実施される場合は、その内容のみ学年全体で共有できるような設定を行った。

○ ツール導入・利用の流れ（データの適切な管理）

※児童の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置の実施＞

- 組織的安全管理措置として、ツール導入時に確認した役割分担にしたがって、責任者が定期的に個人情報の取扱いについて確認することとした。
- 物理的安全管理措置として、 B 小学校の職員室の入り口から教職員の PC 画面が見えない配置にし、職員室が無人になる際は施錠を徹底した。
- データの取扱いについて、個人情報保護の観点から A 市の実施する研修を B 学校の教職員が受講した。

☞その他の安全管理措置として行うべき事項や留意点は 、「Ⅰ．総論編３． ２」や「Ⅱ．手順編３c」も参照してください。

＜個人情報ファイル簿を作成する＞

- A 市教育委員会において、ツールの導入に当たって、新たに個人情報を保有することとなるため、個人情報ファイル簿を作成し、自治体内の情報公開部局に報告を行った。個人情報ファイル簿は、個人情報保護法第 75 条に基づき、作成した。

＜データの正確性を確保する＞

- B 小学校で、新年度が開始するタイミングで新たに入学する児童情報を新規登録した。
- B 小学校で、転入・転出を受けて児童情報の新規登録・削除・変更の処理を行った。

事例 1

＜保有個人情報の削除及び機器、電子媒体等の廃棄＞

- A 市教育委員会は、あらかじめ定めた保存期間を過ぎたデータは、委託先のデータベースから削除させ、委託先に削除された旨の証明書を提出させた。

＜利用目的の変更による利用・提供＞

- 「児童の学習状況を把握して学習指導を行うため」に取得していた学習データを、A 市教育委員会が域内の学校のツール活用状況を把握するための統計作成に利用することにした。変更後の利用目的が変更前の利用目的と相当の関連性があると判断されたため、利用目的の変更をすることで対応した。

＜利用目的の特定＞

- 今まで学習等に活用していたツールに、新たに生活アンケート機能が追加され、新たなデータを取得することになった。そのため、新たなデータを取得する場合として、A 市教育委員会において事前に再度利用目的の特定をし、追加で B 学校から児童と保護者にプリントを配付する方法で明示を行った。

事例２　A 県立 C 高等学校において、生徒が、問題を解いて習熟度に応じたフィードバックを得られるデジタルドリルを利用する

シナリオ

A 県教育委員会において、域内の C 高等学校全学年の授業で生徒一人ひとりが自分の習熟度に合わせた問題で演習を行うために、次のようなデジタルドリルを導入することにした。それにあたり、A 県教育委員会及び域内の高等学校の一つである C 高等学校において、新たなツール導入に当たって個人情報等の観点から必要な対応を行っている。

○ 導入するツールが有する主な機能のイメージ

- 生徒一人ひとりの習熟度に合わせたフィードバックを提供する。
- 生徒本人・保護者・教員が学習履歴を確認できる。

○ ツールを導入するメリット

（生徒）

- 自分の習熟度に合った問題を解くことができる。
- 単元ごとの学習履歴を確認することで、自身の得意・不得意な分野を知ることができる。

（教員）

- 学習履歴を確認し、生徒個人やクラス全体としての習熟度を知ることができる。
- 個人間やクラス間で学習履歴の比較を行い、適切な指導を行うことができる。

（保護者）

- 子供の学習状況を確認できる。

○ 取り扱う主な個人情報

※ツールを単体で導入する場合を想定。学習 e ポータルを経由する場合は事例 3 を参照してください。

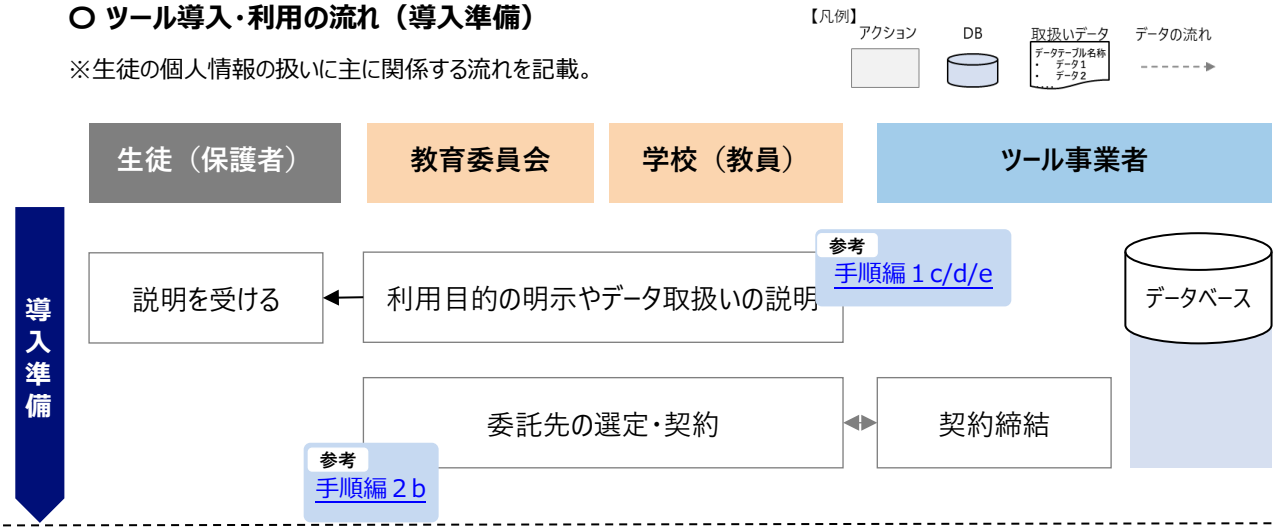
事例２

データ種別	主なデータの内容	取得方法
生徒情報	ID・パスワード	・ ツール利用に当たって、A 県教育委員会が発行 ※シングルサインオン（SSO）を用いる場合あり
	氏名	（あらかじめ保有）
	所属学年・クラス	
	出席番号	
教員情報	ID・パスワード	・ ツール利用に当たって、A 県教育委員会が発行 ※シングルサインオン（SSO）を用いる場合あり
	閲覧権限	・ ツール利用に当たって、A 県教育委員会又は C 高等学校が設定
	所属学年・担当クラス	（あらかじめ保有）
保護者情報	氏名	・ 生徒情報の管理画面から登録 ※保護者は情報を登録せずに、子供のアカウントと紐づけて利用することも可能
	住所・連絡先	
学習情報	選択した問題・解答内容（選択肢・自由記述・音声）	・ 生徒が問題にアクセス・解答をすることで情報を蓄積
	採点結果	
	操作ログ	
	教材ごとの学習履歴 学習時間	

事例２

○ ツール導入・利用の流れ（導入準備）

※生徒の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜利用目的（ツールを導入することで取得するデータの利用目的）を特定する＞

- A 県教育委員会において、「学習指導に用いる」等の抽象的な利用目的ではなく、具体的に、何のデータ項目をどのように使用して指導するのか、まで検討した上で、利用目的を以下のように設定した。
  - 生徒の学習履歴から個人及びクラス・学年での学習状況や習熟度を把握し、個別最適な学習指導を行うため

＜利用目的やデータの取扱いの説明をする＞

- C 高等学校の教職員が、生徒・保護者に対して、特定した利用目的を明示し、データの取扱いについて説明するためのメールを配信した。

【メールに記載した内容】

- 利用目的
  - 生徒の学習履歴から個人及びクラス・学年での学習状況や習熟度を把握し、個別最適な学習指導を行うため
- サービス概要

このツールを用いることで、生徒一人ひとりが自分の習熟度に合った問題を解くことができます。
また分野別の学習履歴等を確認し、容易に自分の得意・不得意な分野を把握できます。

- 本ツールで扱う個人情報
  - 氏名、学籍番号
  - 選択した問題・解答内容、採点結果
  - 操作ログ、学習履歴、学習時間
- データの収集手法

本人が問題にアクセスし、解答をすることで情報は収集されます。

- 第三者提供の有無

大学・研究機関等の第三者への提供はしません。

- 保存期間

データは、卒業時に生徒に提供するとともに、卒業して〇か月後に削除します。

＜委託先の選定・契約＞

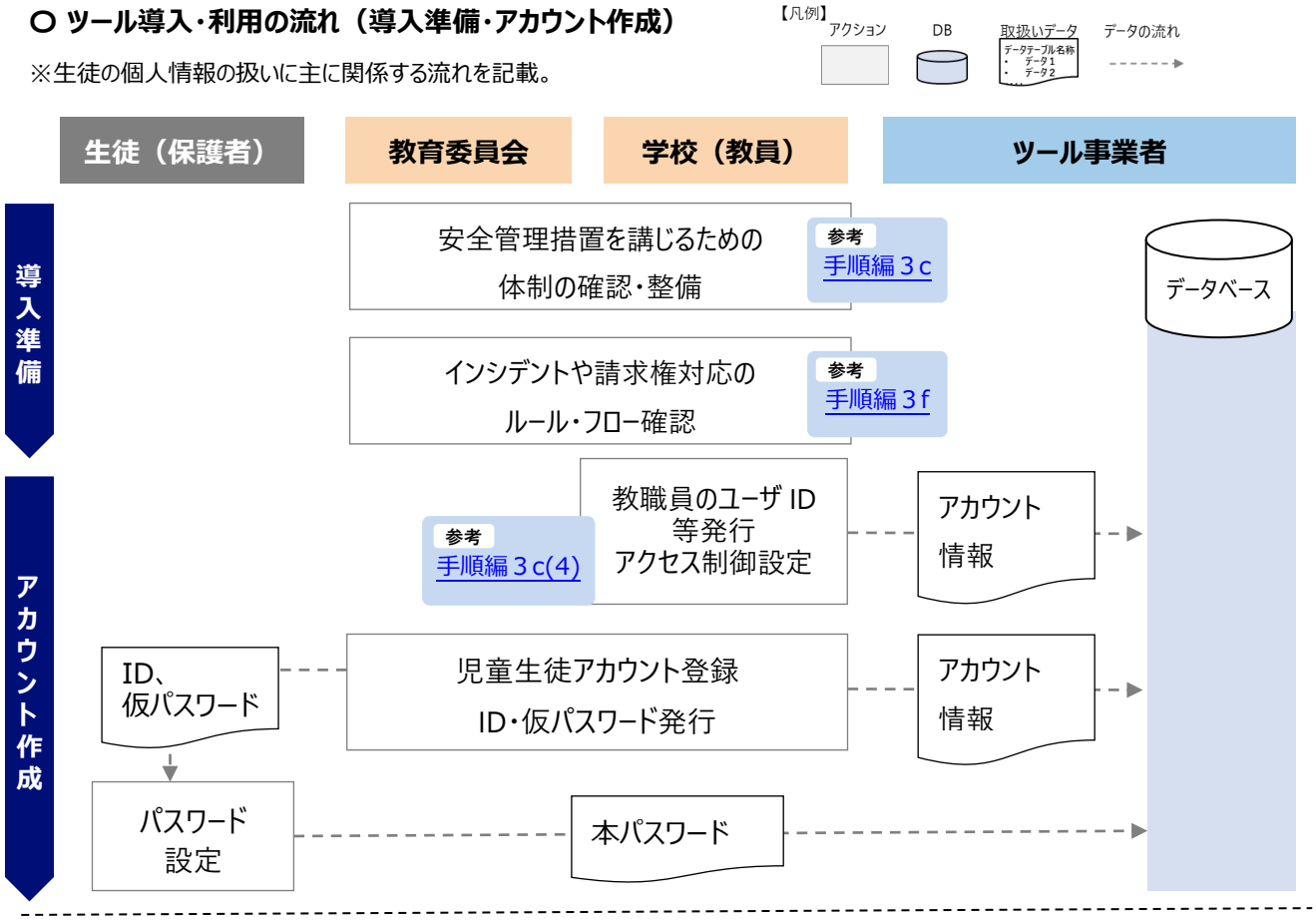
- A 県で整備している委託先の選定基準を踏まえて公告を行い、落札した事業者と A 県で契約を行った。
- 委託先との契約に当たっては、契約書に「データを独自にマーケティング利用しないこと」や「契約終了後は 3 か月程度のダウンロード期間を設けた後にデータを全て削除すること」等について記載をした。

☞契約に当たっては、「Ⅰ．総論編１．４」や「Ⅱ．手順編２b」に記載の事項も確認しましょう。

事例２

○ ツール導入・利用の流れ（導入準備・アカウント作成）

※生徒の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置を講じるための体制の確認・整備＞

- 組織的安全管理措置として、保有個人情報を適切に取り扱うため、A 県教育委員会においては各学校に保有個人情報の出力の状況について、定期的に提出を求めた。C 高等学校においては、出力を行う際は記録をするようにした。

  ☞その他の安全管理措置として行うべき事項や留意点は、「Ⅰ．総論編３．２」や「Ⅱ．手順編３c」も参照してください。

＜インシデントや請求権対応のルール・フロー確認＞

- A 県教育委員会において、個人情報の取扱いに係る規律への違反やデータ漏えい事案等のインシデントが発生した場合のフローを改めて確認し、各学校においてインシデントが発生している事実又は兆候を把握した場合の責任者への報告フローについて、学校に伝達した。
- A 県教育委員会で整理したインシデント発生時の対応フローと役割分担について、C 高等学校の職員会議で周知した。

＜利用目的の達成に必要な範囲で個人情報を保有、利用・提供する＞

- C 高等学校において、ツールの利用に必要な生徒の氏名や ID 等を入力した。

  ☝ポイント：データ登録が必須ではない項目については、利用目的に照らし合わせて、登録の要否を検討しましょう。

事例２

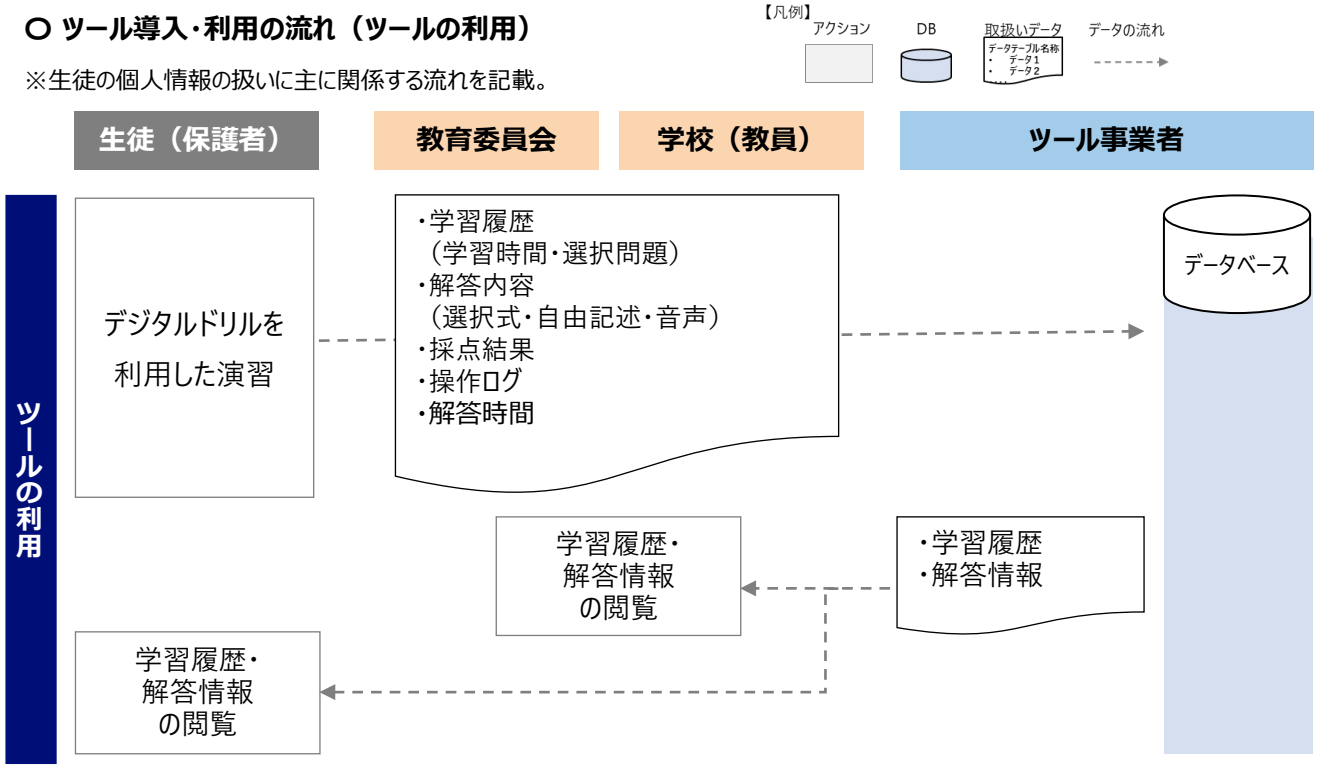
＜認証とアクセス制御＞

- C 高等学校において、アカウント作成時に各アカウントでできること（閲覧、編集、アカウント登録・削除等）を整理して、必要な教職員がデータを見られるようにした。具体的には、各教科担当の教員が当該教科の全ての解答を閲覧・編集できるように、管理職は学校内の全てのデータを閲覧・編集できるように設定した。
- アカウント登録・削除等は、管理職と主事・主任の教員のみが実施できるように設定した。

ポイント：情報漏えい等を避けるため、アカウントの権限設定に当たっては、真に必要な人のみに権限を付与し、不要な人に権限付与を行わないようにしましょう。

○ ツール導入・利用の流れ（ツールの利用）

※生徒の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

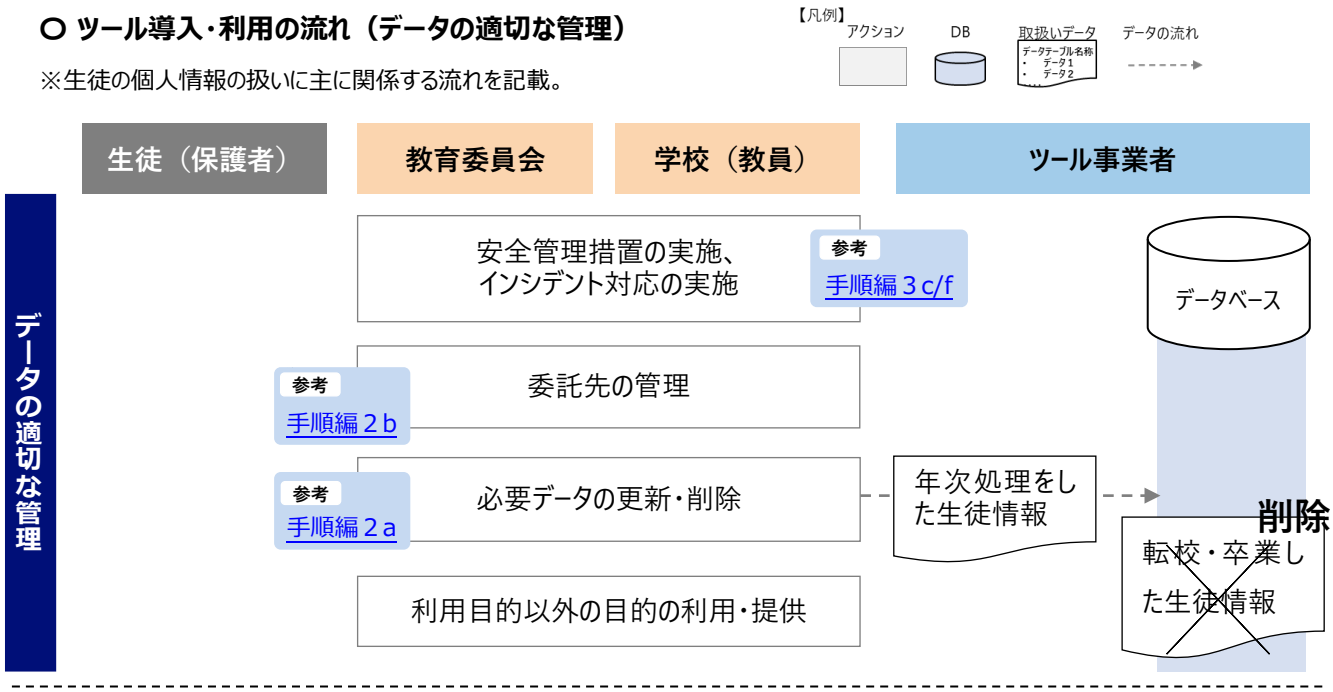
＜認証とアクセス制御＞

- C 高等学校において、生徒の学習履歴等は基本的に他の生徒は閲覧できないように設定を行った。保護者は、基本的に自身の子供の学習履歴等を閲覧できる状態とした。

事例２

○ ツール導入・利用の流れ（データの適切な管理）

※生徒の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置の実施＞

- 組織的安全管理措置として、C 高等学校の教職員のツール利用状況を確認するため、業務日誌を作成させ、システムに記録されるログイン時間との照合ができるようにした。
- 物理的安全管理措置として、C 高等学校の教職員の PC に画面の自動ロックの設定を行い、教職員の不在時に第三者から画面をのぞき込まれない対策をした。
- データの取扱いについて、個人情報保護の観点から A 県の実施する研修を C 高等学校の教職員が受講した。

☞その他の安全管理措置として行うべき事項や留意点は、「Ⅰ．総論編３．２」や「Ⅱ．手順編３c」も参照してください。

＜委託先事業者の管理＞

- A 県教育委員会は、保有個人情報に係る作業の管理体制や実施体制、保有個人情報の管理状況について、契約書に記載された内容が実施されていることを確認するため、年に 1 回、事業者へのヒアリングを行う他、委託先に対して必要か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った。

＜個人情報ファイル簿を作成する＞

- A 県教育委員会において、ツールの導入に当たって、新たに個人情報を保有することとなるため、個人情報ファイル簿を作成し、自治体内の情報公開部局に報告を行った。個人情報ファイル簿は、個人情報保護法第 75 条に基づき、作成した。

＜データの正確性を確保する＞

- C 高等学校で、新年度が開始するタイミングで新たに入学する生徒情報を新規登録した。
- C 高等学校で、転入・転出を受けて生徒情報の新規登録・削除・変更の処理を行った。
- 保護者の情報に更新があった場合は、C 高等学校から生徒経由で更新を依頼した。

＜保有個人情報の削除及び機器、電子媒体等の廃棄＞

- A 県教育委員会は、あらかじめ定めた保存期間を過ぎたデータは、委託先のデータベースから削除させた。

事例２

＜利用目的以外の目的の利用・提供（本人に提供）＞

- 「生徒の学習履歴から個人およびクラス・学年での学習状況や習熟度を分析して、適切な学習指導を行うため」に取得していた解答時間のデータを、生徒が自宅等での自主学習において学習プランを立てやすくするために、生徒本人にも提供することにした。その場合は、個人情報保護法第 69 条第 2 項第 4 号の本人に提供するときとして利用目的外の提供が可能である。

事例３　A 市立 D 中学校において、生徒が、様々な学習ツールにつながるソフトウェア（学習 e ポータル）を利用する

シナリオ

A 市教育委員会において、域内の全中学校の全学年で利用するために、様々な学習ツールにつながるソフトウェア（学習 e ポータル）を導入することにした。それにあたり、A 市教育委員会及び域内の中学校の一つである D 中学校において、新たなツール導入に当たって個人情報等の観点から必要な対応を行っている。

○導入するツールが有する主な機能のイメージ

- 学習 e ポータルにログインした生徒は、学習 e ポータルを起点に、学習等で使う各種コンテンツにアクセスできる。
- 生徒は、各種コンテンツの学習状況等を、学習 e ポータル上で確認できる。

○ ツールを導入するメリット

（生徒）

- 学習 e ポータルを起点に各種コンテンツにアクセスできるため、効率的に学習を進めることができる。
- 学習状況等を学習 e ポータル上で一元管理できるため、進捗状況や成績等を確認しやすい。

（教員）

- リアルタイムで個人またはクラスの学習状況等を把握し、効果的な指導を行うことができる。

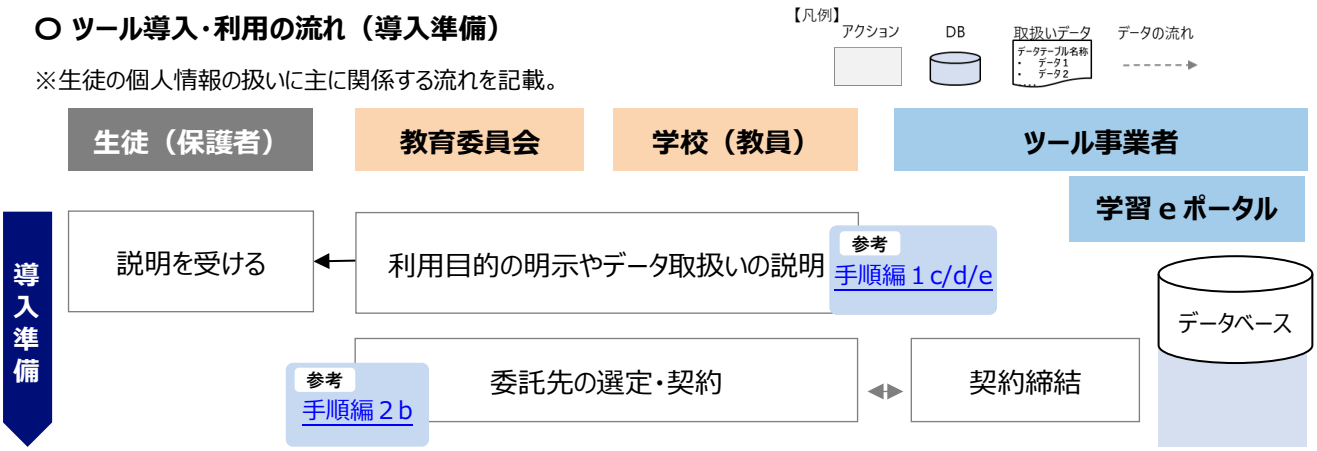
○ 取り扱う主な個人情報

データ種別	主なデータの内容	取得方法
生徒情報	ID・パスワード	• ツール利用に当たって、A 市教育委員会が発行
	氏名	（あらかじめ保有）
	所属学年・担当クラス	
	出席番号	
教員情報	ID・パスワード	• ツール利用に当たって、A 市教育委員会が発行
	閲覧権限	• ツール利用に当たって、A 市教育委員会又は D 中学校が設定
	所属学年・担当クラス	（あらかじめ保有）
学習情報	生徒の学習状況	• 生徒が学習 e ポータルと接続しているコンテンツで学習した場合
	教員からのコメント	• 学習 e ポータル上で、生徒に対し教員がコメントをつける
	アクセスログ	• 学習 e ポータル及びコンテンツにアクセスすると自動で取得

事例３

○ ツール導入・利用の流れ（導入準備）

※生徒の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜利用目的（ツールを導入することで取得するデータの利用目的）を特定する＞

- A 市教育委員会において、「学習指導に用いる」等の抽象的な利用目的ではなく、具体的に、何のデータ項目をどのように使用して指導するのか、まで検討した上で、利用目的を以下のように設定した。
  - 生徒の様々なツールを使った学習状況を一元的に把握して学習指導を行うため

＜利用目的やデータの取扱いの説明をする＞

- D 中学校の教職員が、生徒にプリントを配布して、特定した利用目的を明示し、データの取扱いについて説明した。
- また、中学生は 15 歳以下であり、本件についての判断能力が不十分であると考えられるため、保護者に連絡メールを配信し、同様の内容について説明をした。また、念のため、保護者会においても保護者宛に口頭で説明を行った。

【プリントに記載した内容】

➢ 利用目的
- 生徒の様々なツールを使った学習状況を一元的に把握して学習指導を行うため

➢ サービス概要

このツールを用いることで、学習で使う各種コンテンツにアクセスしやすくなったり、学習状況を一元管理できるようになったりします。

➢ 本ツールで扱う主な個人情報
- 氏名、出席番号
- 生徒の学習状況とそれに対する教員からのコメント
- アクセスログ

➢ データの収集手法

本人が学習ｅポータルと接続している各種コンテンツを利用することにより、データが収集されます。

➢ 第三者提供の有無

大学・研究機関等への第三者への提供はしません。

➢ 保存期間

データは、卒業して〇か月後に削除します。

＜委託先の選定・契約＞

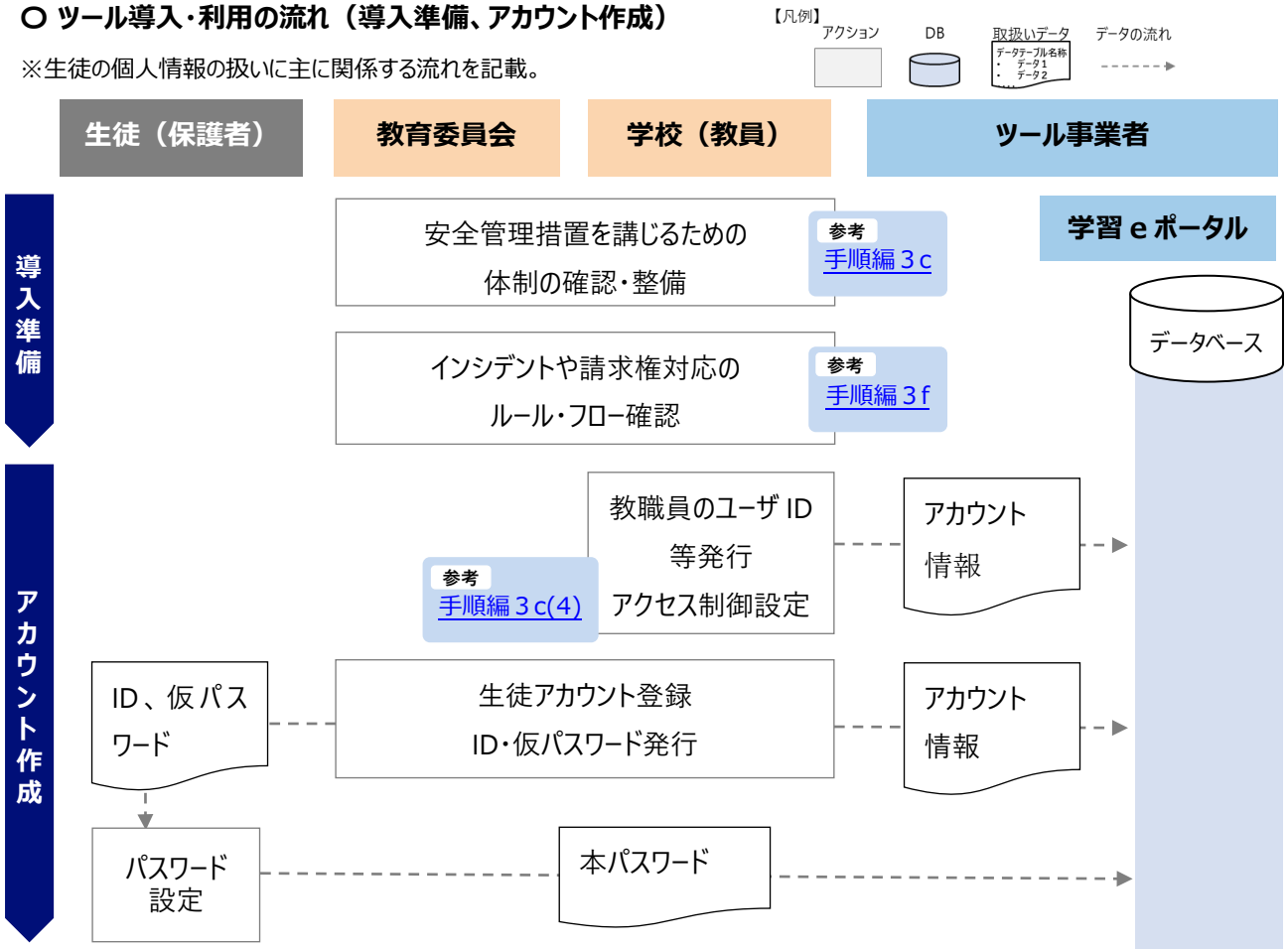
- A 市で整備している委託先の選定基準を踏まえて公告を行い、落札した事業者と A 市で契約を行った。
- 委託先との契約に当たっては、契約書に「接続する各種コンテンツに個人情報の取扱いを再委託する場合の取扱について」や「契約違反時の損害賠償責任」等について記載をした。

☞契約に当たっては、「Ⅰ．総論編１．４」や「Ⅱ．手順編２b」に記載の事項も確認しましょう。

事例３

○ ツール導入・利用の流れ（導入準備、アカウント作成）

※生徒の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置を講じるための体制の確認・整備＞

- 組織的安全管理措置として役割分担の明確化のため、A 市教育委員会において教育長が総括管理責任者であることを確認した。D 中学校においては、全体の管理責任者は学校長であることを確認するとともに、各クラスのデータは学級担任が責任を持つことを確認し、ツール導入に当たり、教職員にあらためて職員会議で周知した。

☞その他の安全管理措置として行うべき事項や留意点は 、「Ⅰ．総論編３． ２」や「Ⅱ．手順編３c」も参照してください。

＜インシデントや請求権対応のルール・フロー確認＞

- A 市教育委員会において、個人情報の取扱いに係る規律への違反やデータ漏えい事案等のインシデントが発生した場合のフローを改めて確認し、各学校においてインシデントが発生している事実又は兆候を把握した場合の責任者への報告フローについて、学校に伝達した。
- D 中学校において、インシデント発生時の対応フローと役割分担について文書で整理し、学校内のチャットで共有した。

＜利用目的の達成に必要な範囲で個人情報を保有、利用・提供する＞

- ツール事業者における ID 発行に最低限必要な情報（氏名、学年、クラス）の情報のみを事業者に提供した。

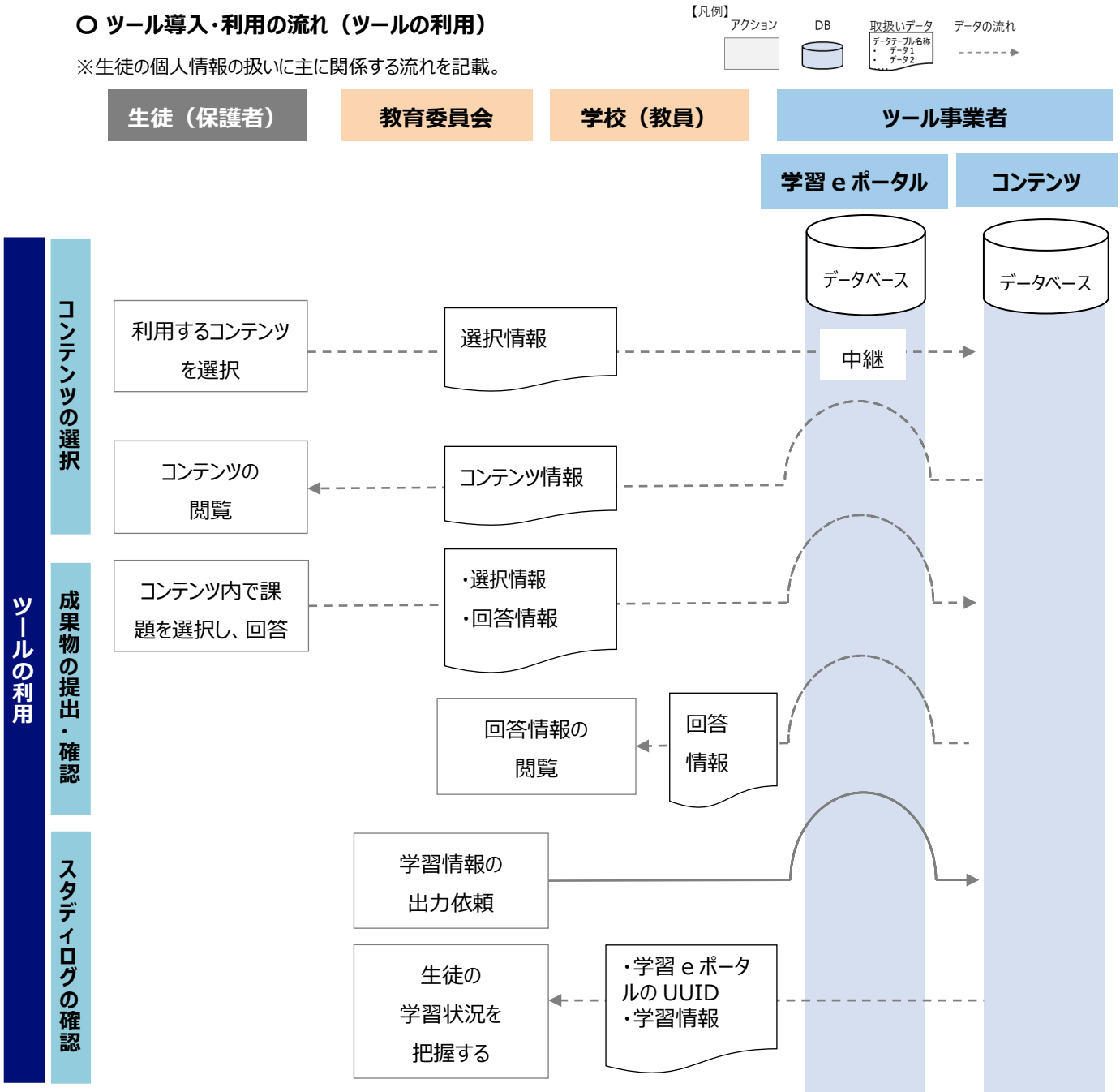
＜認証とアクセス制御＞

（詳細は、次頁参照）

事例３

○ ツール導入・利用の流れ（ツールの利用）

※生徒の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜認証とアクセス制御＞

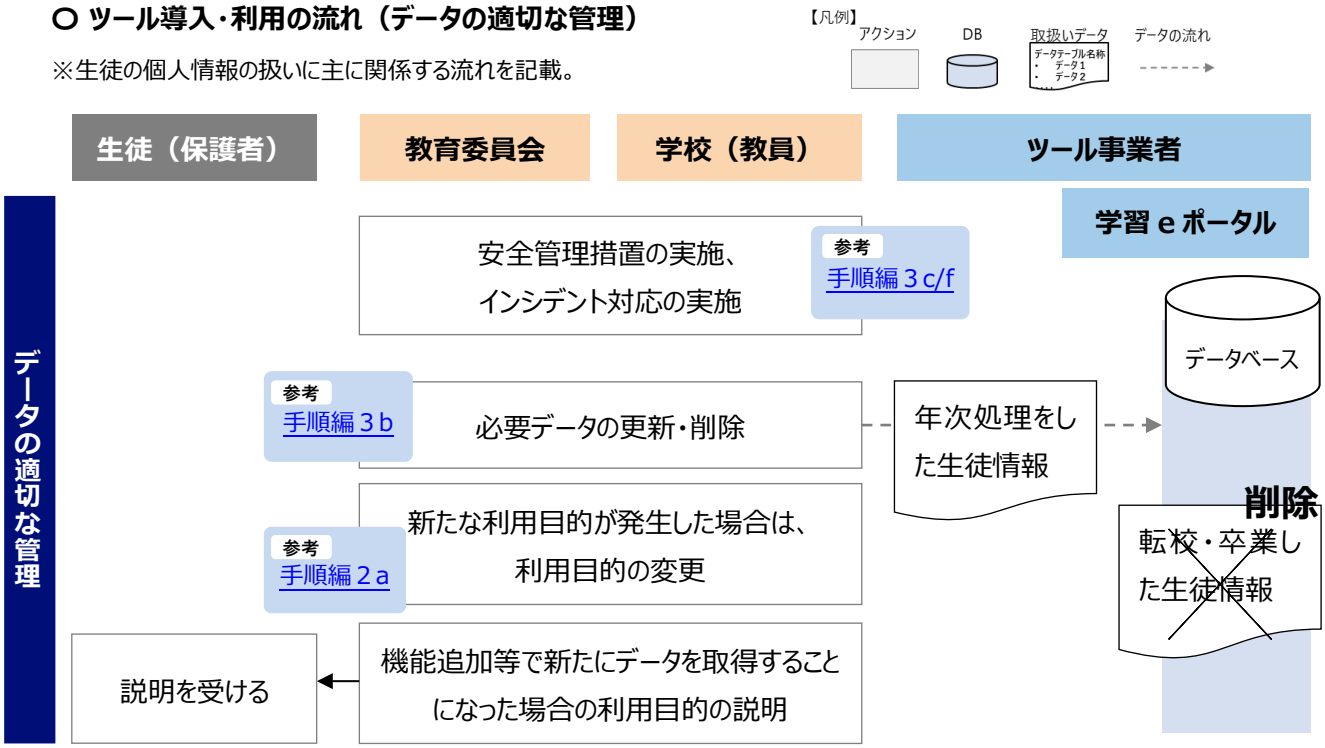
- D 中学校において、アカウント作成時に閲覧権限設定を行い、必要な教職員がデータを見られるようにした。具体的には、教員は担任しているクラスと授業を受け持つクラスのデータを、学年主任は学年全てのクラスのデータを、管理職は学校内の全てのデータを閲覧できるように設定した。
- アカウント登録・削除等は、A 市教育委員会の担当職員と D 中学校の管理職のみが実施する。

  ポイント：情報漏えい等を避けるため、アカウントの権限設定に当たっては、真に必要な人のみに権限を付与し、不要な人に権限付与を行わないようにしましょう。

事例３

○ ツール導入・利用の流れ（データの適切な管理）

※生徒の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置の実施＞

- 技術的安全管理措置として、ツール導入時に確認した役割分担にしたがって、不正と思われる利用が行われた場合は学校の ICT 担当者にアラートが届く仕組みを導入した。
- 物理的安全管理措置として、教職員のタブレットを生徒がのぞき込めないよう、のぞき込み防止フィルムを画面に貼り付けた。
- A 市教育委員会においては、学習ｅポータルのデータセンターが国内に置かれていることを確認した。

☞その他の安全管理措置として行うべき事項や留意点は、「Ⅰ．総論編３．２」や「Ⅱ．手順編３c」も参照してください。

＜委託先事業者の管理＞

- A 市教育委員会において、委託事業者が個人情報保護等について契約書に記載された内容を実施していることを確認するため、年に一度契約更新時に契約内容の確認を行う他、委託先に対して必要か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った。

＜個人情報ファイル簿を作成する＞

- A 市教育委員会において、ツールの導入に当たって、新たに個人情報を保有することとなるため、個人情報ファイル簿を作成し、自治体内の情報公開部局に報告を行った。個人情報ファイル簿は、個人情報保護法第 75 条に基づき、作成した。

＜データの正確性を確保する＞

- D 中学校で、新年度が開始するタイミングで新たに入学する生徒情報を新規登録した。
- D 中学校で、転入・転出を受けて生徒情報の新規登録・削除・変更の処理を行った。

事例３

＜保有個人情報の削除及び機器、電子媒体等の廃棄＞

- A 市教育委員会は、あらかじめ定めた保存期間を過ぎたデータは、委託先のデータベースから削除させ削除されていることを確認した。

＜利用目的の特定＞

- A 市教育委員会において、学習 e ポータルの心の健康観察機能を新たに活用することを決定した。その結果、今までは取得していなかった新たなデータを取得することになった。そのため、新たなデータを取得する場合として、A 市教育委員会において事前に利用目的の特定をし、追加で D 中学校から生徒にプリントを配布し説明、保護者に同内容のメールを配信する方法で明示を行った。

事例４　A 市立 E 中学校において、生徒に対し、アンケートなどを行うためのツール（OS メーカーが標準的に提供するソフトウェアの一部）を利用する

シナリオ

A 市教育委員会の域内の中学校では、生徒の意見を収集するためのアンケートを行うツール（OS ツールの一部）を導入している。アンケートにおいて新たに個人情報を取得することとなったため、A 市教育委員会及び域内の中学校の一つである E 中学校において、個人情報等の観点から必要な対応を行っている

○ 導入するツールが有する主な機能のイメージ

- 生徒の意見等を収集することができる

○ ツールを導入するメリット

（生徒）

- 意見を教員に対して直接伝えることができる。

（教員）

- 生徒の意見を把握し、効果的な学習指導・生活指導やクラス運営等を行うことができる。

○ 取り扱う主な個人情報

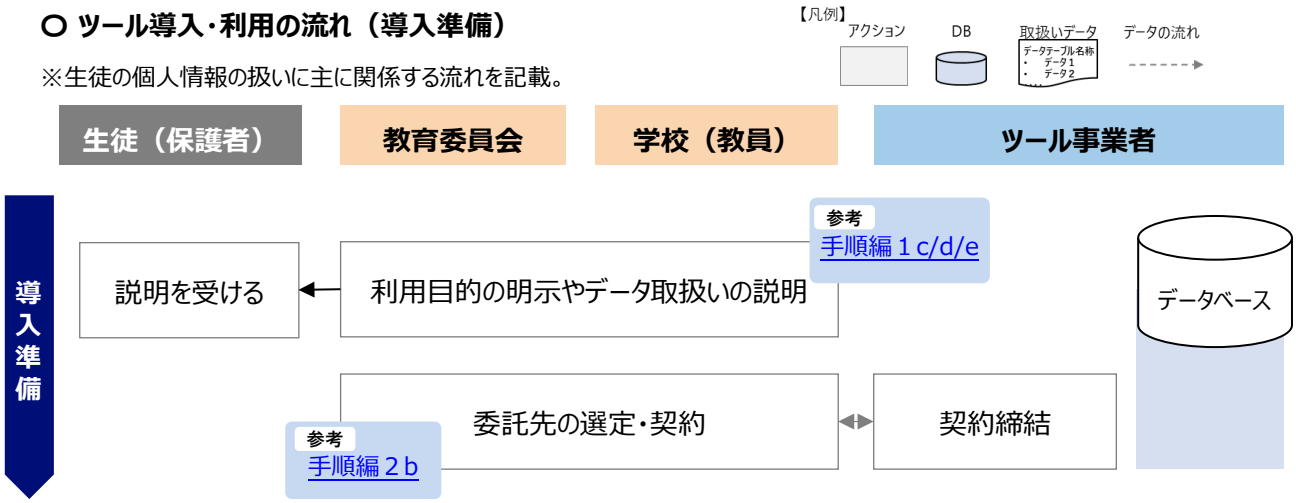
※ツールを単体で導入する場合を想定。学習 e ポータルを経由する場合は事例 3 を参照してください。

データ種別	主なデータの内容	取得方法
生徒情報	ID・パスワード	• ツール利用に当たって、A 市教育委員会が発行
	氏名	（あらかじめ保有）
	所属学年・担当クラス	
	出席番号	
教員情報	ID・パスワード	• ツール利用に当たって、A 市教育委員会が発行
	閲覧権限	• ツール利用に当たって、A 市教育委員会又は E 中学校が設定
	所属学年・担当クラス	（あらかじめ保有）
回答情報	生徒の回答	• 生徒がアンケートに回答した場合に、取得される

事例４

○ ツール導入・利用の流れ（導入準備）

※生徒の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜利用目的（ツールを導入することで取得するデータの利用目的）を特定する＞

- A 市教育委員会において、「生徒の意見を収集する」等の抽象的な利用目的ではなく、具体的に、何のデータ項目をどのように使用して指導するのか、まで検討した上で、利用目的を以下のように設定した。
  - 生徒の状況や意見を踏まえて、効果的な学習指導・生活指導を行うため。

＜利用目的やデータの取扱いの説明をする＞

- E 中学校の教職員が、生徒に対し、年度の初回のアンケートを実施する際に、アンケートの冒頭画面に特定した利用目的を明示し、データの取扱いについて説明した。
- また、中学生は 15 歳以下であり、本件についての判断能力が不十分である場合も考えられるため、保護者にプリントを配付し、同様の内容について説明をした。

【プリントに記載した内容】

➢ 利用目的

生徒の状況や意見を踏まえて、効果的な学習指導・生活指導を行うため。

➢ サービス概要

教員による効果的な学習指導や生活指導、クラス運営等のために、生徒の意見等を収集します。

➢ 本ツールで扱う主な個人情報

・ 氏名

・ 生徒の回答情報

➢ データの収集手法

本人がアンケートに回答することによりデータは収集されます。

➢ 第三者提供の有無

大学、研究機関等からの提供依頼があった際には提供することがありますが、その際、データの取扱については覚書を結んだ上で行います。

➢ 保存期間

データは、卒業して〇か月後に削除します。

事例４

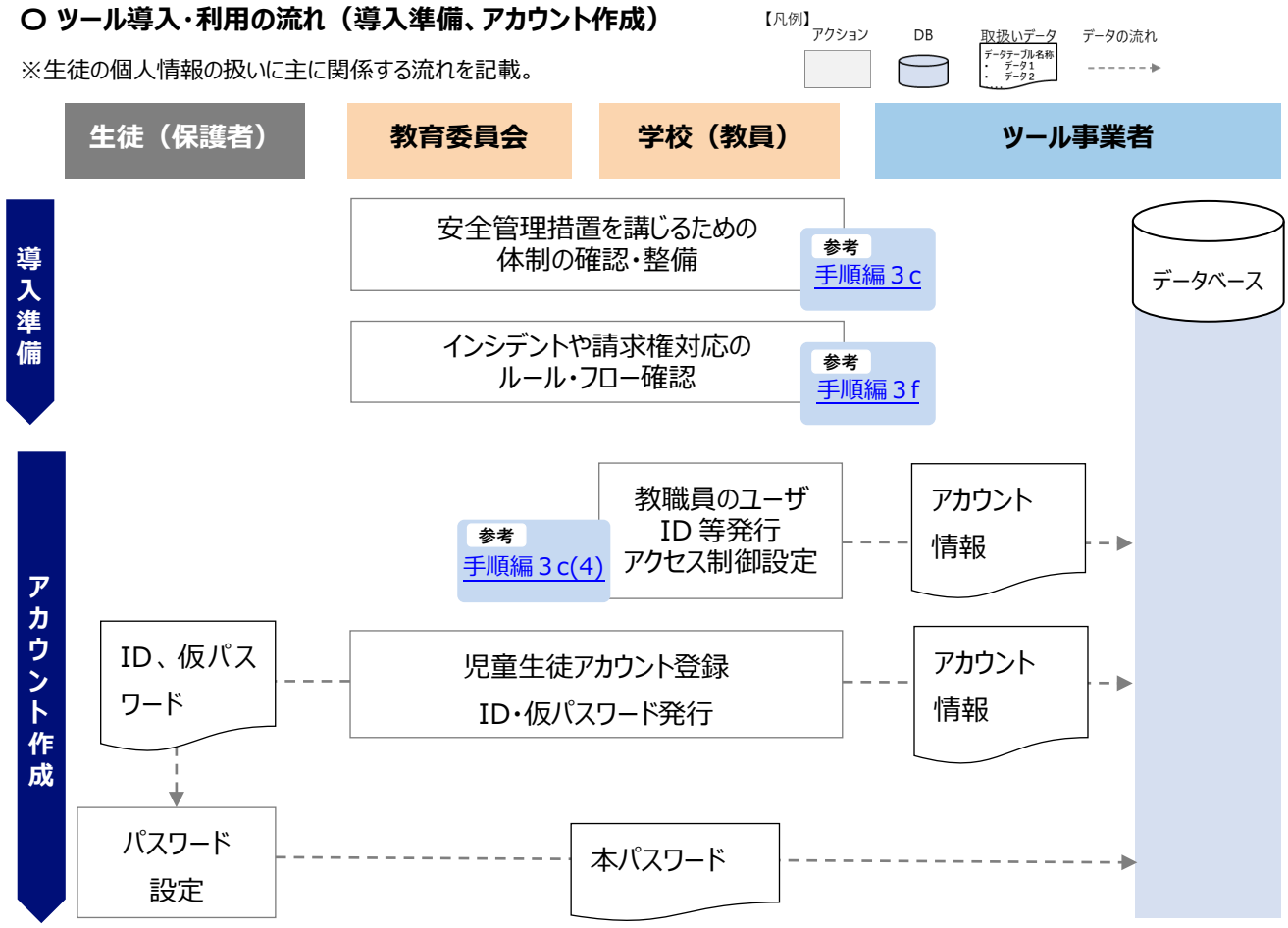
＜ツールの選定・契約＞

- A 市独自で整備している選定基準を踏まえて、導入するツールを選定し、ツール事業者と A 市で契約を行った。
- OS メーカーが標準的に提供するソフトウェア導入時に、利用規約に「データを第三者提供しないこと」や「契約終了後はデータを削除すること」、「取扱の委託を受けた目的以外の目的で利用しないこと」等について記載があることを確認し同意した。

☞契約に当たっては、「Ⅰ．総論編１．４」や「Ⅱ．手順編２b」に記載の事項も確認しましょう。

○ ツール導入・利用の流れ（導入準備、アカウント作成）

※生徒の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置を講じるための体制の確認・整備＞

- 組織的安全管理措置として役割分担の明確化のため、A 市教育委員会において教育長が総括管理責任者であることを確認した。E 中学校においては、全体の管理責任者は学校長であることを確認するとともに、各クラスのデータは学級担任が責任を持つことを確認し、ツール導入に当たり、教職員にあらためて職員会議で周知した。

  ☞その他の安全管理措置として行うべき事項や留意点は、「Ⅰ．総論編３．２」や「Ⅱ．手順編３c」も参照してください。

事例４

＜インシデントや請求権対応のルール・フロー確認＞

- A 市教育委員会において、個人情報の取扱いに係る規律への違反やデータ漏えい事案等のインシデントが発生した場合のフローを改めて確認し、各学校においてインシデントが発生している事実又は兆候を把握した場合の責任者への報告フローについて、学校に伝達した。
- E 中学校において、インシデント発生時の対応フローと役割分担を整理し、端末利用のルールと併せて周知した。

＜利用目的の達成に必要な範囲で個人情報を保有、利用・提供する＞

- アンケートの内容が、個人に紐づける必要がないものである場合、非記名式のアンケートとし、不要な情報を取得しないようにした。

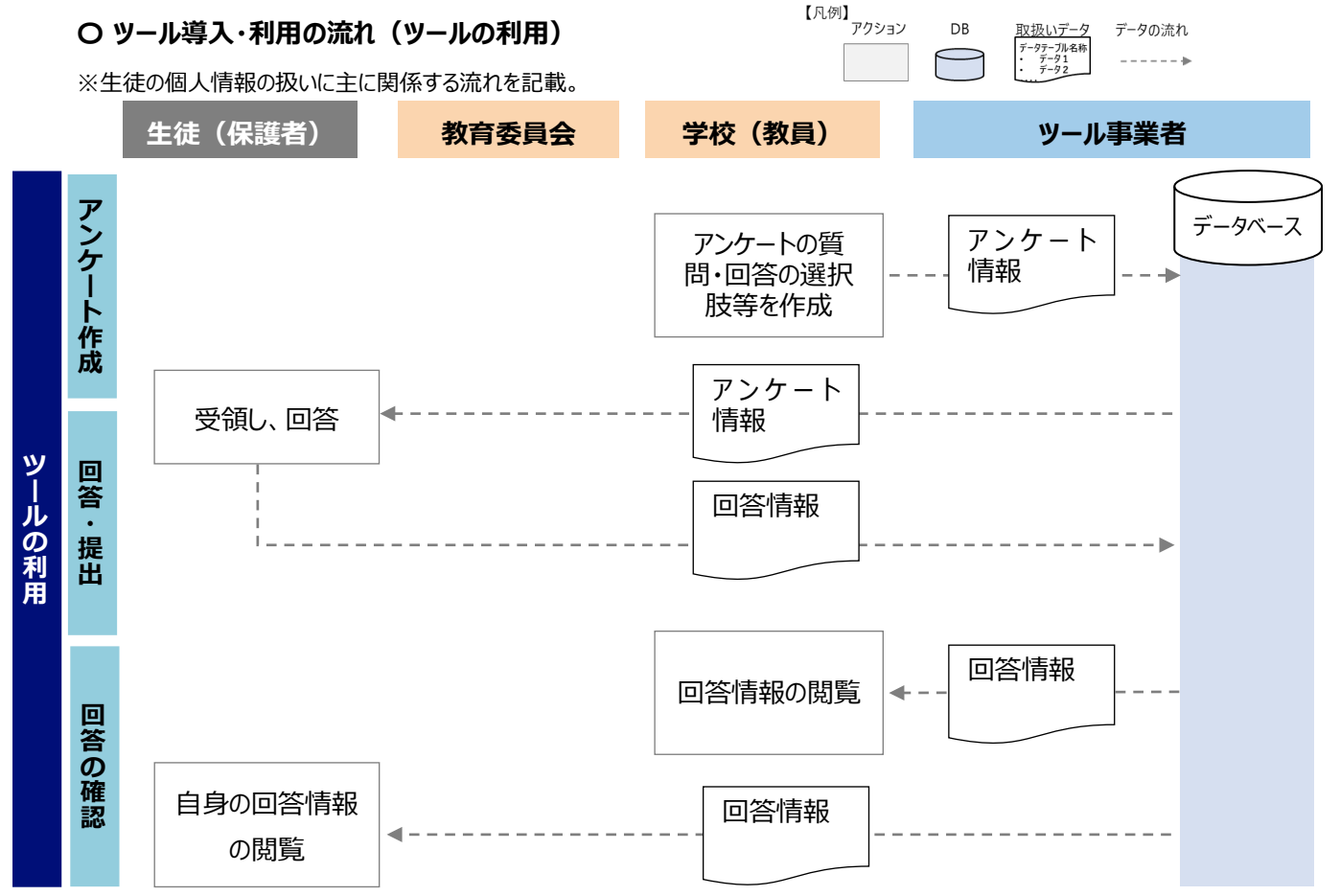
＜認証とアクセス制御＞

- A 市教育委員会において、アカウント作成時に各アカウントの閲覧権限等を整理して、必要な教職員が回答データを見られるようにした。具体的には、学級担任においては自分が担当するクラスの回答データのみを閲覧できるようにした。アカウント登録・削除等は、A 市教育委員会職員と E 中学校の管理職・ICT 担当のみが実施できるようにした。

ポイント：情報漏えい等を避けるため、アカウントの権限設定に当たっては、真に必要な人のみに権限を付与し、不要な人に権限付与を行わないようにしましょう。

○ ツール導入・利用の流れ（ツールの利用）

※生徒の個人情報の扱いに主に関係する流れを記載。



事例４

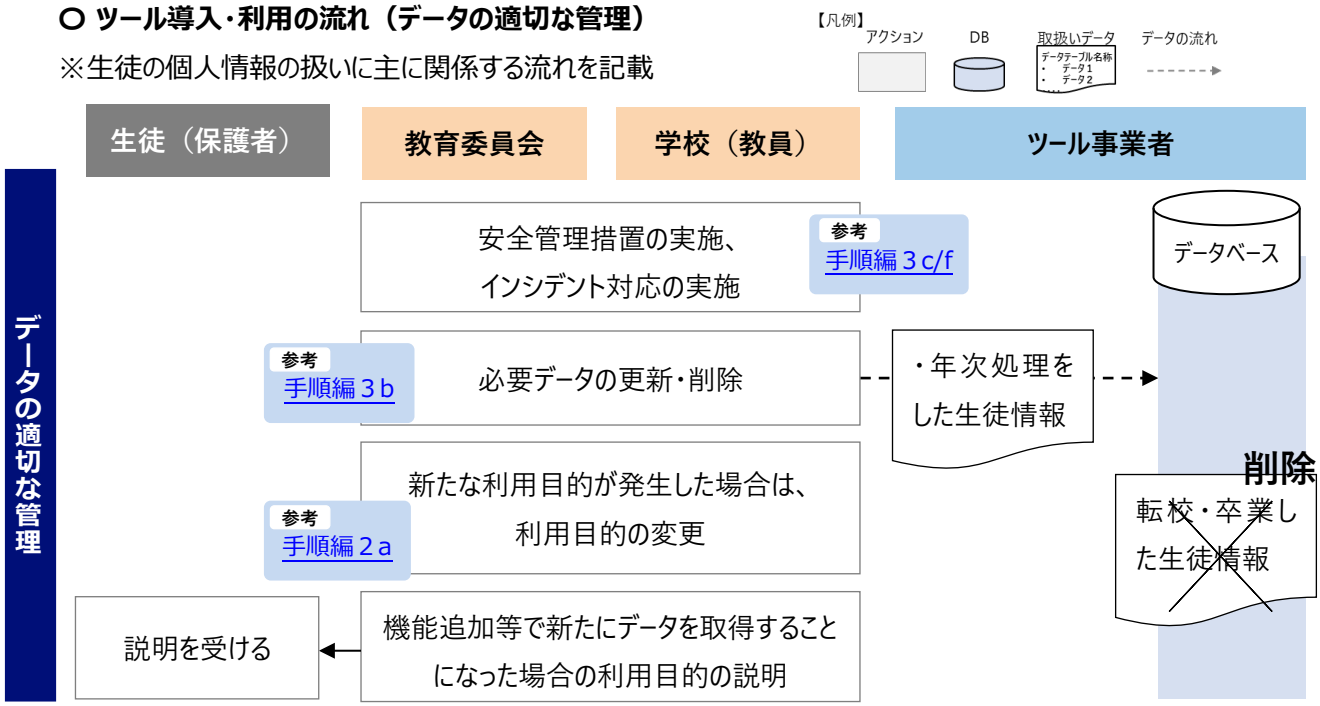
【主に実施したこと】

＜認証とアクセス制御＞

- E 中学校において、記名の回答は基本的に担任教員のみが閲覧できるようにした。ただし、学年全体に関するアンケート、全校に関するアンケートの場合は、学年の教員全員が閲覧できるような設定を行った。
- また、A 市教育委員会の域内全体に係るアンケートの場合は、E 中学校において集計を行ったうえで、A 市教育委員会に提出した。

○ ツール導入・利用の流れ（データの適切な管理）

※生徒の個人情報の扱いに主に関係する流れを記載



【主に実施したこと】

＜安全管理措置の実施＞

- 組織的安全管理措置として、OS ソフトの個人情報の取扱いについては、管理職が定期的に確認することとした。
- 物理的安全管理措置として、生徒間でのアンケートのぞき込みが発生しないよう、アンケート回答中は教職員が机間巡視を行った。
- データを削除する際は、「ごみ箱」からも削除するように気を付けた。

☞その他の安全管理措置として行うべき事項や留意点は、「Ⅰ．総論編３．２」や「Ⅱ．手順編３c」も参照してください。

＜委託先事業者の管理＞

- A 市教育委員会において、委託事業者が個人情報保護等について契約書に記載された内容を実施していることを確認するため、定期的にチェックリストを提出させた他、委託先に対して必要か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った。

＜個人情報ファイル簿を作成する＞

- A 市教育委員会において、ツールの導入に当たって、新たに個人情報を保有することとなるため、個人情報ファイル簿を作成し、自治体内の情報公開部局に報告を行った。個人情報ファイル簿は、個人情報保護法第 75 条に基づき、作成した。

事例４

＜データの正確性を確保する＞

- E 中学校で、新年度が開始するタイミングで新たに入学する生徒情報を新規登録した。
- E 中学校で、転入・転出を受けて生徒情報の新規登録・削除・変更の処理を行った。

＜保有個人情報の削除及び機器、電子媒体等の廃棄＞

- A 市教育委員会は、あらかじめ定めた保存期間を過ぎたデータは、委託先のデータベースから削除させた。

＜利用目的外の提供（学術研究目的）＞

- 「生徒の状況や意見等を踏まえて学習指導・生活指導を行うため」に取得していたアンケートの回答情報を、近隣の研究機関から指導方法の向上のための研究に提供してほしいと申し出があった。その場合は、個人情報保護法第 69 条第 2 項第 4 号の学術研究の目的として利用目的外の提供が可能なので、提供先の研究機関とデータの取扱いについての覚書を結んだ上で提供を行った。
- 提供を行うに当たっては、アンケートの回答情報に生徒の機微な情報が含まれる可能性があるため、生徒のプライバシーの保護の観点から、特定の個人を識別することができないよう、保有個人情報を加工、一部の回答はマスキングをするといった措置を講じた。

＜利用目的の特定＞

- E 中学校では、以前周知していなかった目的で、生徒を対象に新たなアンケートを行い、新たなデータを取得することになった。その場合は、新たなデータを取得する場合として、利用目的の特定から再度行う必要がある。
- そのため、新たなデータを取得する場合として、 A 市教育委員会において事前に再度利用目的の特定をし、E 中学校では新たにアンケートを行う際にアンケートの冒頭に記載する方法で生徒に対し明示を行うとともに、保護者には連絡メールを配信した。

事例５　A 市立 F 小学校において、児童の学習状況や健康情報を一覧できるツールを利用する（校務支援システム等）

シナリオ

A 市教育委員会では、域内の全小学校全学年で利用するために、児童の成績や出欠情報等に関する情報を管理するために、次のような校務支援システムを導入している。校務支援システムを引き続き使用するに当たって、A 市教育委員会及び域内の小学校の一つである F 小学校は、ツールの利用に当たって個人情報等の観点から必要な対応を行っている。

○ 導入しているツールが有する主な機能のイメージ

- 教員は、児童の個別の成績や出欠状況や健康状態を確認できる。
- 教員は、成績や出欠状況をクラスや学校単位で集計し、一覧で把握できる。

○ ツールを導入するメリット

（教員）

- 児童一人ひとりの評価・評定をデジタルで実施できる。
- 成績や出欠状況等を一覧化することで、児童の様子をきめ細やかに把握し、支援に生かすことができる。

○ 取り扱う主な個人情報

※ツールを単体で導入する場合を想定。

データ種別	主なデータの内容	取得方法
児童情報	氏名	（あらかじめ保有）
	所属学年・担当クラス	
	出席番号	
教員情報	氏名	（あらかじめ保有）
	担当学年・クラス	
	ID・パスワード	・ツール利用にあたり、F 小学校が登録・設定
学習情報	評価・評定（通知表）	・F 小学校が登録
	指導要録	・F 小学校が登録
生活情報	出欠状況	・F 小学校が登録
	保健室利用状況	

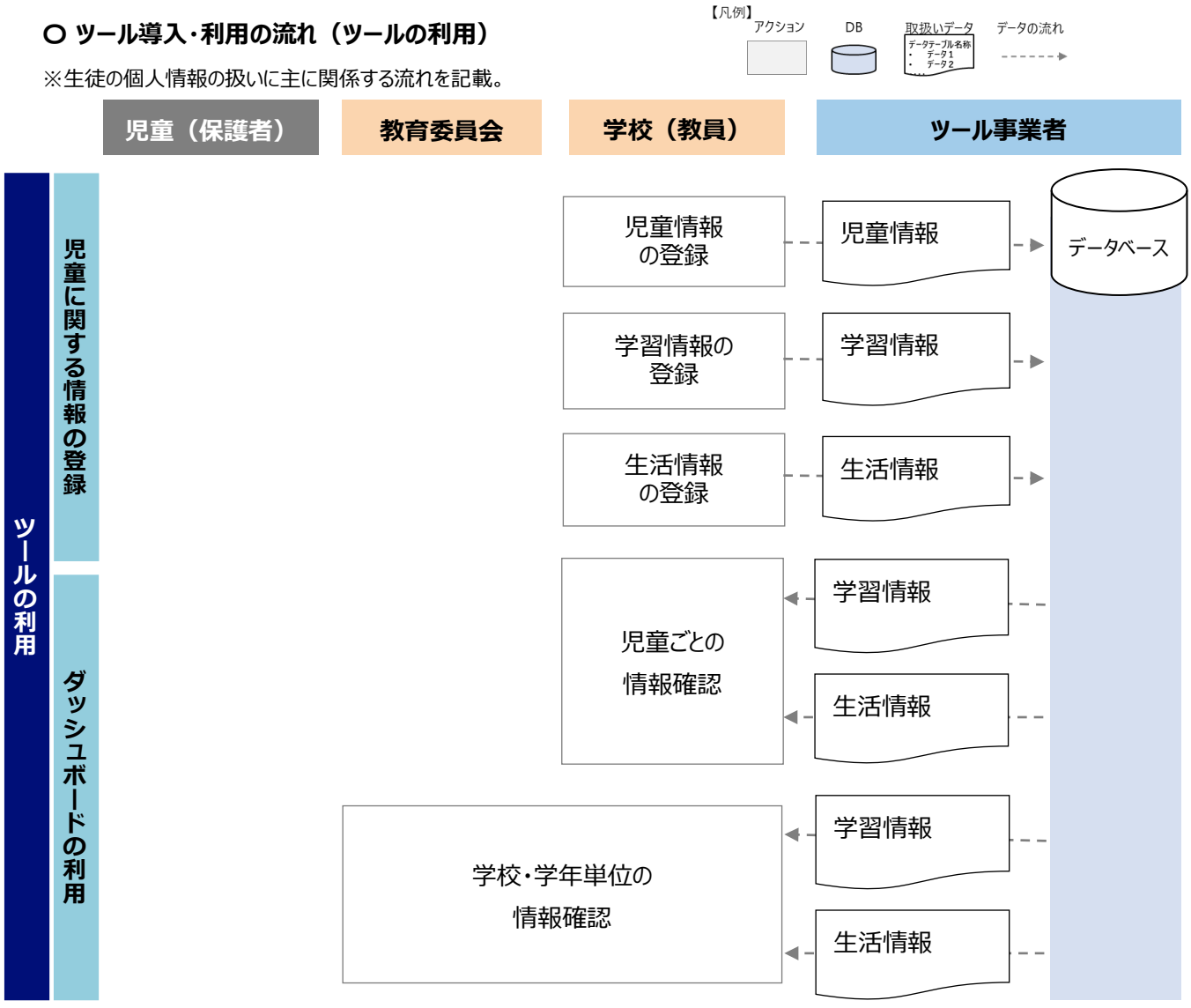
事例５

＜利用目的（ツールを導入することで取得するデータの利用目的）を特定する＞

- A 市教育委員会において、「学習指導に用いる」等の抽象的な利用目的ではなく、具体的に、何のデータ項目をどのように使用して指導するのか、まで検討した上で、利用目的を以下のように設定した。今回本システムで取り扱うデータは、既にこれまでも学校の教育活動の一環として取得しているもののみであり、新たに取得するものはないため、児童・保護者に本システムに関する利用目的の明示は特段行わなかった。
  - 成績などの学習情報を成績処理や学習指導、その後の授業準備のために利用する。
  - 出欠状況や保健室利用状況などの生活情報を、生徒指導、健康・保健指導に利用する。

○ ツール導入・利用の流れ（ツールの利用）

※生徒の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜利用目的の達成に必要な範囲で個人情報を保有、利用・提供する＞

- F 小学校では、児童の生活情報については、学習情報よりも限定された教職員のみに共有する形で、データの取扱いを整理した。具体的には、学級担任は担任しているクラスの児童の生活情報と学習情報の両方のデータを、専科教員等は授

業を受け持つクラスの児童のデータのうち、学習情報のみを、学年主任はすべてのクラスの児童の生活情報と学習情報の両方のデータを、管理職は学校内のすべてのデータの確認をできることとした（以下、この整理について「データの取扱い」という。）。

ポイント：同じ児童に関するデータであっても、閲覧・編集が必須でない項目については、利用目的に照らし合わせて、必要な範囲の情報のみを利用するようにしましょう。

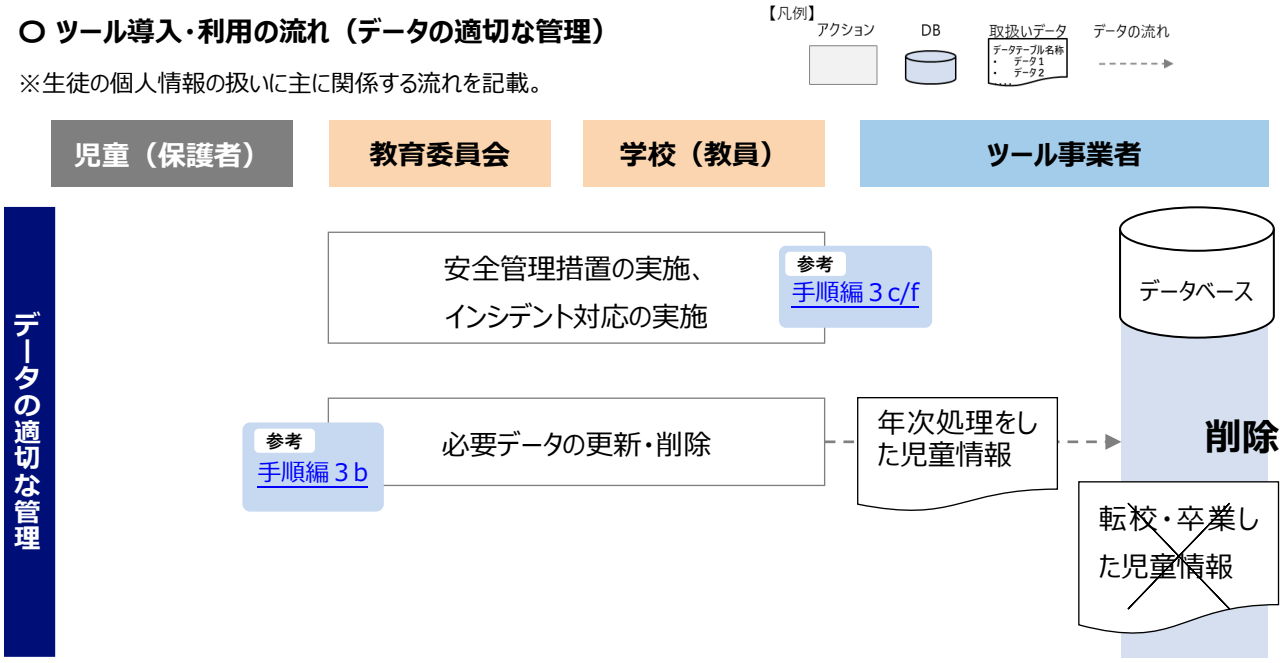
＜認証とアクセス制御＞

- F 小学校では、各アカウントができること（閲覧、編集、アカウント登録・削除等）を整理して、それぞれの教職員が必要なデータのみを見られるようにした。
- 具体的には、閲覧、編集等は、前の項目の「データの取扱い」に従って権限設定を行い、それぞれの教職員が必要な範囲の情報のみを取り扱うこととした。また、児童のアカウント登録・削除等は、管理職及び主事・主任の教職員、ICT 担当の教職員のみが実施できるように設定した。

ポイント：情報漏えい等を避けるため、アカウントの権限設定に当たっては、真に必要な人のみに権限を付与し、不要な人に権限付与を行わないようにしましょう。

○ ツール導入・利用の流れ（データの適切な管理）

※生徒の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置の実施＞

- 組織的安全管理措置として、ツール導入時に確認した役割分担にしたがって、責任者が定期的に個人情報の取扱いについて確認することとした。
- 物理的安全管理措置として、A 市教育委員会は F 小学校に対して、保有個人情報を取り扱う「取扱区域」における適切な管理を行うように指示した。F 小学校ではこれらの適切な対応を行うために、校務支援システムにアクセスができる端末の

配置場所をのぞき見が出来ない場所に変更する、出力した印刷物は不必要に持ち出さない等のルールを定め、教職員に対して職員会議で周知した。

- データの取扱いについて、個人情報保護の観点からＡ市の実施する研修をＦ小学校の教職員が受講した。

☞その他の安全管理措置として行うべき事項や留意点は、「Ⅰ．総論編３．２」や「Ⅱ．手順編３c」も参照してください。

＜委託先事業者の管理＞

- Ａ市教育委員会において、委託事業者が個人情報保護等について契約書に記載された内容を実施していることを確認するため、年に一度実地検査を行った。

＜個人情報ファイル簿の作成を検討＞

- Ａ市教育委員会は、導入しているツールを新たな方法で活用するに当たって、個人情報ファイル簿の作成を検討したが、新たな個人情報は保有しないため、作成は不要と判断した。

＜データの正確性を確保する＞

- Ｆ小学校で、新年度が開始するタイミングで新たに入学する児童情報を新規登録した。また、Ａ市教育委員会は、新たに配属された教職員情報を新規登録した。
- Ｆ小学校で、転入・転出を受けて児童情報の新規登録・削除・変更の処理を行った。

☞保存期間が法令で定められている情報（指導要録や健康診断票等）は、保存期限後に確実に削除されるよう、システムの設定や手動で管理する必要があります。

＜保有個人情報の削除及び機器、電子媒体等の廃棄＞

- Ａ市教育委員会は、卒業した児童、異動した教職員等のデータは、委託先のデータベースから削除させ、委託先に削除された旨の証明書を提出させた。

事例６　A 市立 G 小学校において、児童の心の健康状態を把握するツールを利用する

シナリオ

A 市教育委員会では、細やかな児童への生活指導や支援を行うために、域内の全小学校全学年で、児童の心の健康状態を把握するためのツールを導入することにした。それにあたり、A 市教育委員会及び域内の小学校の一つである G 小学校において、新たなツールの導入に当たって個人情報等の観点から必要な対応を行っている。

○ 導入するツールが有する主な機能のイメージ

・児童は登校時や下校時に、その時の心の健康状態を単純な記号を用いて簡便に入力する（晴・曇・雨・雷などの記号で選択する場合が多い）。また併せて、自由記述形式のコメントを入力することができる。

・教員は、児童の心の健康状態の記号やコメントを確認するとともに、クラスや学校単位で集計することができる。また、そのほかの情報等（出欠状況、保健室の利用状況、成績情報等）と併せてダッシュボードにより一覧で把握できる。

○ ツールを導入するメリット

（児童）

・一人ひとりが、自身の心身の状態の変化に気付いたり、状態を可視化することにより相談支援のきっかけをつくったりすることが期待できる。

（教員）

・心の健康状態の情報を参考に、児童の心の変化を定期的に確認し、生活指導や支援に生かすことができる。

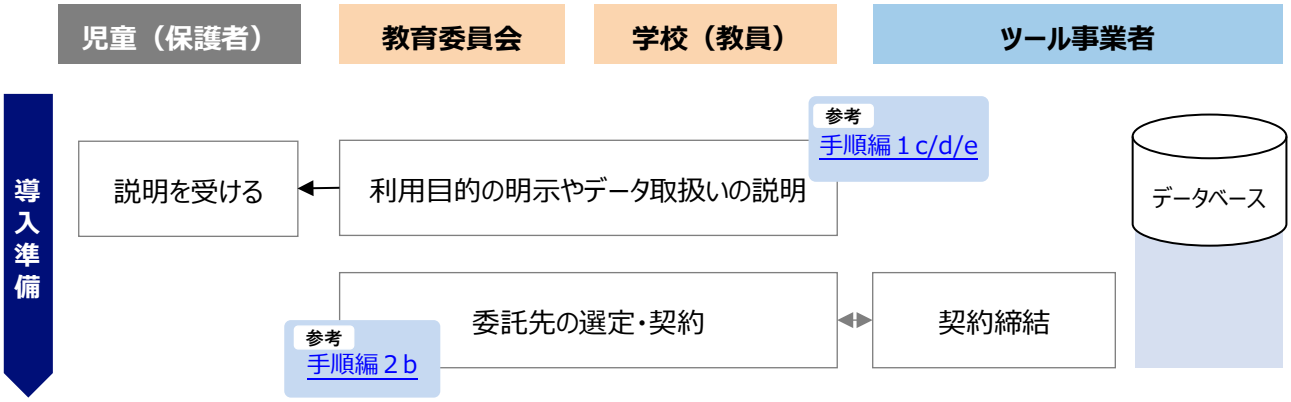
○ 取り扱う主な個人情報

データ種別	主なデータの内容	取得方法
児童情報	氏名	•ツール利用にあたり、G 小学校が登録・設定
	所属学年・所属クラス	
	学籍番号	
教員情報	氏名	•ツール利用にあたり、A 市教育委員会が登録・設定
	担当学年・担当クラス	
	ID・パスワード	
心の健康状態に関する情報	心の健康状態に関する記号	•児童が登録
	心の健康状態に関するコメント	
学習情報	評価・評定	• あらかじめ保有
	指導要録	

生活情報	出欠状況	
	保健室利用状況	

○ ツール導入・利用の流れ（導入準備）

※児童の個人情報の扱いに主に関係する流れを記載。



【主に実施したこと】

＜利用目的（ツールを導入することで取得するデータの利用目的）の特定＞

- A 市教育委員会において、「生活指導に用いる」等の抽象的な利用目的ではなく、具体的に、何のデータ項目をどのように使用して指導するのか、まで検討した上で、利用目的を以下のように設定した。

・ 児童の心の状態の変化を参考に、学校生活における日々の声掛けや生活指導に利用する。

＜利用目的やデータの取扱いの説明＞

- G 小学校の教職員が、児童にプリントを配付して、特定した利用目的を明示し、データの取扱いについて説明した。
- また、小学生は 15 歳以下であり、本件についての判断能力が不十分であるため、市のホームページにおいても説明資料を掲載するとともに、保護者にその URL にアクセス可能な Q R コード付きの連絡メールを配信し、同様の内容について説明をした。また、念のため保護者会においても保護者宛に口頭で説明を行った。

【プリントに記載した内容】

➢ 利用目的
児童の心の状態の変化を参考に、学校生活における日々の声掛けや生活指導に利用する。

➢ サービス概要
このツールを用いることで、日々の心の健康状態を参考に、学校生活におけるよりよい生活指導や、自身の振り返りに活用できます。
なお、入力された内容は、記号は全学年の教員が閲覧しますが、コメントについては学年担当の教員のみが閲覧します。

➢ 本ツールで扱う主な個人情報
・ 氏名、学籍番号
・ 児童が登校時と下校時に入力する、その時の気分を表す記号（晴・曇・雨・雷）やコメント

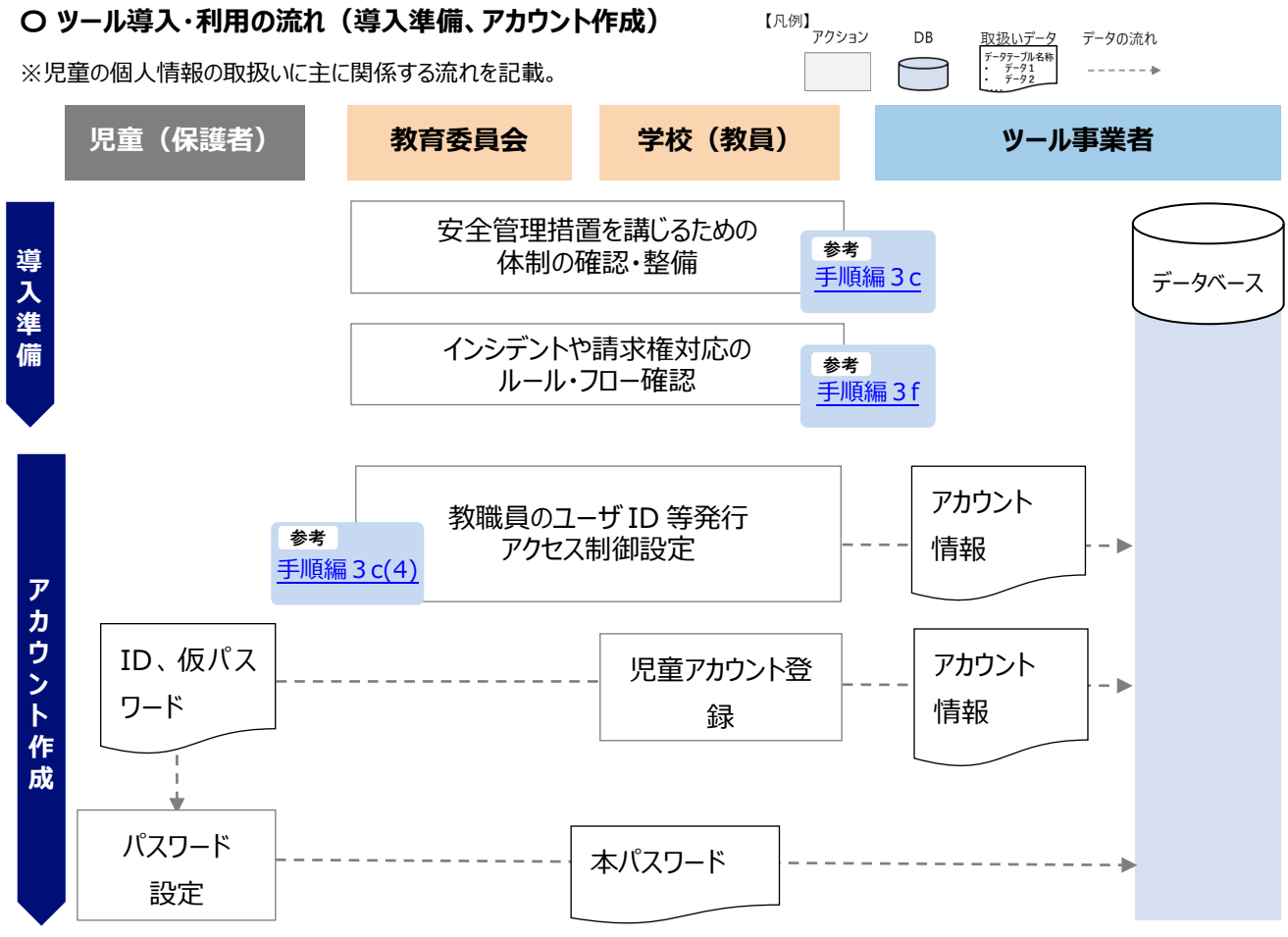
- データの収集手法
  本人が自身の気分を表す記号やコメントを入力することによりデータを収集します。なお、入力は任意であり、強制するものではありません。
- 第三者提供の有無
  大学・研究機関等への第三者への提供はしません。
- 保存期間
  記号やコメントは、３か月ごとに削除します。

＜委託先の選定・契約＞

- A 市で整備している委託先の選定基準を踏まえて公告を行い、落札した事業者と A 市教育委員会で契約を行った。
- 委託先との契約に当たっては、契約書に「データの利用やその方法を最小限にすること」や「契約終了後はデータを削除すること」等について記載をした。 ☞契約に当たっては、「Ⅰ．総論編１．４」や「Ⅱ．手順編２b」に記載の事項も確認しましょう。

○ ツール導入・利用の流れ（導入準備、アカウント作成）

※児童の個人情報の取扱いに主に関係する流れを記載。



事例 6

【主に実施したこと】

＜安全管理措置を講じるための体制の確認・整備＞

- 組織的安全管理措置として役割分担の明確化のため、A 市教育委員会において教育長が総括管理責任者であることを確認した。G 小学校においては、全体の管理責任者は学校長であることを確認するとともに、各クラスのデータはクラス担任が責任を持つことを確認し、ツール導入に当たり、教職員にあらためて職員会議で周知した。

  ☞その他の安全管理措置として行うべき事項や留意点は、「Ⅰ．総論編３．２」や「Ⅱ．手順編３c」も参照してください。

＜インシデントや請求権対応のルール・フロー確認＞

- A 市教育委員会において、個人情報の取扱いに係る規律への違反やデータ漏えい事案等のインシデントが発生した場合のフローを改めて確認し、各学校においてインシデントが発生している事実又は兆候を把握した場合の責任者への報告フローについて、G小学校に伝達した。
- G 小学校において、インシデント発生時の対応フローと役割分担を整理し、ツール利用のルールと併せて周知した。

＜認証とアクセス制御＞

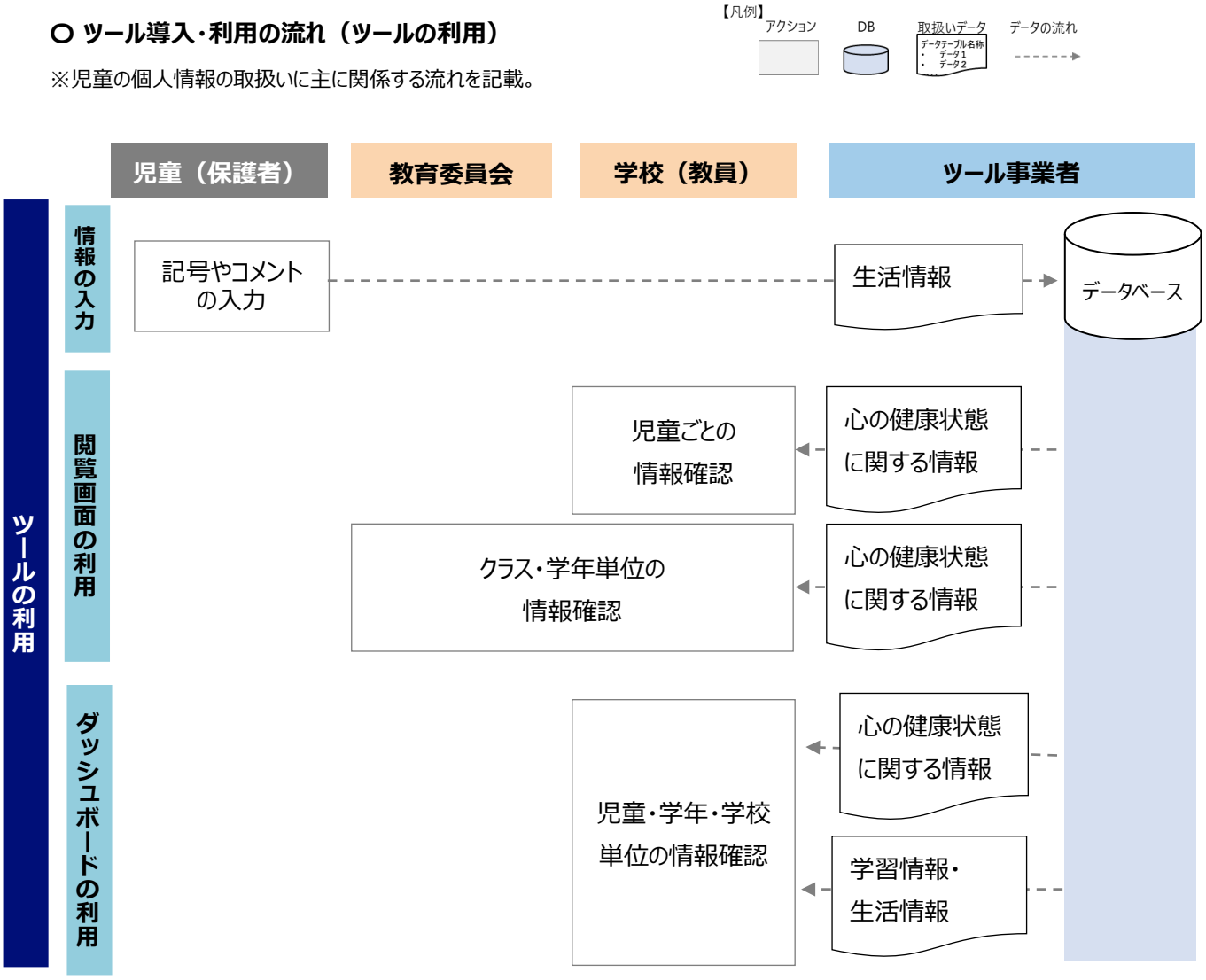
- G 小学校において、教職員のアカウント作成時に閲覧権限設定を行い、必要な教職員に限定してデータを見られるようにした。具体的には、心の健康状態の記号は全学年の教員が閲覧できるが、心の健康状態の記号やコメントについては学年担当の教員のみが閲覧できるようにした。
- アカウント登録・削除等は、管理職のみが実施できるように設定した。

  ☝ポイント：情報漏えい等を避けるため、アカウントの権限設定に当たっては、真に必要な人のみに権限を付与し、不要な人に権限付与を行わないようにしましょう。

事例 6

○ ツール導入・利用の流れ（ツールの利用）

※児童の個人情報の取扱いに主に関係する流れを記載。



【主に実施したこと】

＜利用目的の達成に必要な範囲で個人情報を保有、利用・提供する＞

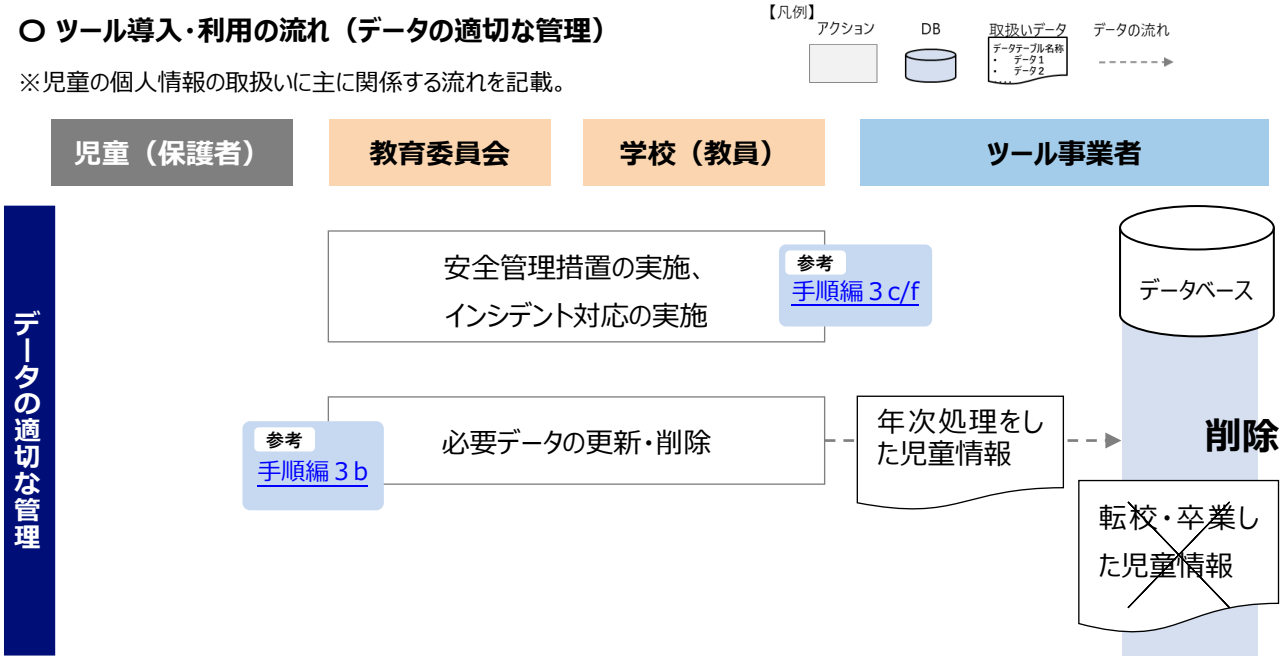
- G 小学校においては、児童の心の状態の変化を参考に、学校生活における日々の声掛けや生活指導に利用する、という利用目的の達成に必要な個人情報のみを保有した。

  ポイント：特定した利用目的の達成に必要となる個人情報を整理し、その範囲で保有するようにしましょう。

事例 6

○ ツール導入・利用の流れ（データの適切な管理）

※児童の個人情報の取扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置の実施＞

- 組織的安全管理措置として、ツール導入時に確認した役割分担にしたがって、責任者が定期的に個人情報の取扱いについて確認することとした。
- 物理的安全管理措置として、A 市教育委員会は G 小学校に対して、保有個人情報を取り扱う「取扱区域」における適切な管理を行うように指示した。G 小学校ではこれらの適切な対応を行うために、ダッシュボードが閲覧できる校務支援システムにアクセスができる端末の配置場所をのぞき見が出来ない場所に変更する、出力した印刷物は不必要に持ち出さない等のルールを定め、教職員に対して職員会議で周知した。
- データの取扱いについて、個人情報保護の観点から A 市教育委員会の実施する研修を G 小学校の教職員が受講した。また生活指導や支援はあくまで児童本人と向き合って行うことが肝要であることから、不適正な利用を防止するために、回答情報は生活指導や支援の補助的な参考情報として扱い、それのみから判断して不適切な推知をすることのないよう、併せて周知徹底した。

☞その他の安全管理措置として行うべき事項や留意点は、「Ⅰ．総論編３． ２」や「Ⅱ．手順編３c」も参照してください。

＜委託先事業者の管理＞

- A 市教育委員会において、委託事業者が個人情報保護等について契約書に記載された内容を実施していることを確認するため、年に一度契約更新時に契約内容の確認を行う他、委託先に対して必要か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った。

＜個人情報ファイル簿を作成＞

- A 市教育委員会において、ツールの導入に当たって、新たに個人情報を保有することとなるため、個人情報ファイル簿を作成し、A 市内の情報公開部局に報告を行った。個人情報ファイル簿は A 市の既定する作成手順に基づき、作成した。

＜データの正確性の確保＞

- G 小学校で、新年度が開始するタイミングで新たに入学する児童情報を新規登録した。また、A 市教育委員会は、新たに配属された教職員情報を新規登録した。
- G 小学校で、転入・転出や卒業を受けて児童情報の新規登録・削除・変更の処理を行った。

＜保有個人情報の削除及び機器、電子媒体等の廃棄＞

- A 市教育委員会は、あらかじめ定めた保管期限を過ぎたデータは、委託先のデータベースから削除させ、また削除されていることを確認した。

○ 心の健康状態を把握するツールの導入時に注意したこと

１．児童への丁寧な説明と適切な閲覧範囲の設定

A 市教育委員会は、児童の心の健康状態の記号やコメントを取得する。記号については、他の教育データ（成績情報、学習履歴情報等）と比べて、特別に機微なものではないが、他の教育データより丁寧な取扱いを意識する必要があると考えた。また、ツール上で併せて入力をするコメント（自由記述）については、病歴や信仰心といった信条[90]に関する事項など、児童の要配慮個人情報やそれに類する情報が記入されることも想定された。そのため、A 市教育委員会では以下の対応を行った。

- 児童に対してツールの利用方法を説明する際に、入力情報の閲覧範囲や活用方法についても併せて説明した。
- 情報の性質を踏まえ、他の教育データよりも閲覧範囲を限定した。（例：心の健康状態の記号は全学年の教員が閲覧できるが、コメントについては学年担当の教員のみが閲覧可）

２．入力の任意性の担保

児童に“必ず”入力をすることを求めると、児童が委縮したり、不安を抱いたりする可能性がある。A 市教育委員会では、本ツールの趣旨を踏まえると、児童に対して回答を強制することは相応しくないと考えた。

そのため A 市教育委員会では、G 小学校に対して、児童に回答を強制することの無いよう周知するとともに、運用状況の定期的な点検を求めた。G 小学校では、回答は任意であることを児童に説明するとともに、全教職員に対して、回答を強制す

[90] 「信条」とは、「個人の基本的なものの見方、考え方を意味し、思想と信仰の双方を含むものである」（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））とされている。ある特定の思想・信仰を有するという事実が記載されることは、本文における「信条」に該当するが、例えば「図書館で〇〇教の本を読んでいた」等の「信条」を推知させる情報に過ぎないものであれば、当該情報のみでは要配慮個人情報には該当しないと解される。

るような言動をしないように注意喚起を行った。（児童への説明例：「先生がみなさんの気持ちを知るきっかけにしたいが、回答したくない時は無理に入力しなくてもよい」と声掛けをする）

３．本心の入力を強要しないことの担保

児童に、本心の入力（内心を正直に入力すること）を強要するのは、内心の自由を侵害する恐れがある。

そのため A 市教育委員会では、G 小学校に対して、本心の入力を強要してはならない旨を周知するとともに、運用状況の定期的な点検を求めた。また、G 小学校では、どのように回答するかは児童に委ねられるものであることを児童に説明するとともに、全教職員に対して、本心の入力を強要するような言動をしないように注意喚起を行った。（児童への説明例：「先生がみなさんの気持ちを知るきっかけにしたいが、入力のルールは無いので、自由に入力してもらってよい」と声掛けをする）

４．情報の活用方法に関する周知徹底

心の健康状態の記号やコメントのみから児童の精神状態を判断してしまう等の不適切な利用を行ってしまうといったリスクがある。そのため A 市教育委員会は、そのような利用がなされないよう、利用目的の範囲内においてのみ活用をすることを、G 小学校の教職員に対して研修を通じて周知徹底した。

また併せて、生活指導や支援はあくまで児童本人と向き合って行うことが肝要であり、回答情報は生活指導や支援の補助的な参考情報として扱い、それのみから判断して成績評価に用いたり、家庭環境を推知したりすることのないよう、G 小学校の教職員に対して研修を通じて周知徹底した。

事例７　A 市立 H 中学校において、部活動時の熱中症リスクの軽減のためにウェアラブル端末を利用する

シナリオ

A 市教育委員会では、生徒が健康な状態で部活動を行うために、域内の中学校の一つである H 中学校において、熱中症リスクを把握するためのツールを導入することにした。それにあたり、A 市教育委員会及び H 中学校において、新たなツールの導入にあたって個人情報等の観点から必要な対応を行っている。

※生体情報は、ユーザの身体の状態を把握するために有用である一方、製品によっては医療機器と同等の精度で生体情報を取得できるものも存在する[91]。また、生体情報を分析することで、ユーザが知られたくない情報（不整脈と言った持病や相手に抱いている感情等）まで推知することが可能な場合がある。そのため、取り扱う生体情報の利用目的を適切に特定したうえで、利用目的の範囲を超えた不要な分析等を行わないことを徹底する必要がある。

○ 導入するツールが有する主な機能のイメージ

- 生徒はウェアラブル端末を装着する。ウェアラブル端末から心拍数や体温等の生体情報を取得し、熱中症リスクがある場合には通知を受け取ることができる。
- 教職員はそれらの情報をもとに声かけを行うとともに、生徒は自らの状態を把握することができる。

○ ツールを導入するメリット

（生徒）

- 熱中症にならないように、自身で運動量を調整し、休憩をとることができる。
- 自分の体調をリアルタイムで客観的に管理し、運動の負荷等を確認できる。

（教員）

- 生徒の体調をリアルタイムで把握し、適切なタイミングで運動中の休憩や声がけができる。
- 熱中症のリスクを事前に把握することで、生徒の健康や生命を守ることができる。

[91] 生体情報を計測することができるウェアラブル端末の中には、薬機法（「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律」）に基づく承認を受けて心電図等の表示が認められたものもある。

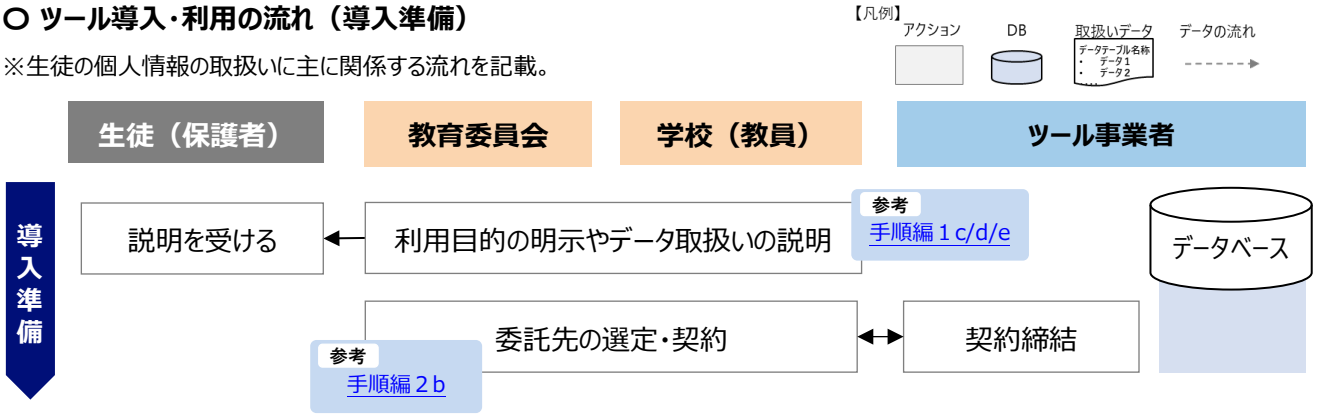
事例 7

○ 取り扱う主な個人情報

データ種別	主なデータの内容	取得方法
生徒情報	氏名、年齢、身長、体重	（あらかじめ保有）
	ID・パスワード	事業者が発行し、学校が生徒に配布
	端末情報	生徒のスマートフォンから自動で収集
	位置情報	
	加速度情報	生徒が装着したウェアラブル端末から自動で収集
教員情報	ID・パスワード	ツール利用に当たって、事業者が発行
	メールアドレス	教員がツール利用時に入力
	端末情報	教員のスマートフォン・タブレット端末から自動で収集
生体情報	心電の波形、心拍数、体温など	生徒が装着したウェアラブル端末から自動で収集

○ ツール導入・利用の流れ（導入準備）

※生徒の個人情報の取扱いに主に関係する流れを記載。



【主に実施したこと】

＜利用目的（ツールを導入することで取得するデータの利用目的）を特定する＞

- A 市教育委員会において、「部活動の指導に用いる」等の抽象的な利用目的ではなく、具体的に、何のデータ項目をどのように使用して指導するのか、まで検討した上で、利用目的を以下のように設定した。
  - 部活動時に運動中の生徒の体調や熱中症リスクを把握して適切な声がけを行い、生徒の健康を守るため。

＜利用目的やデータの取扱いの説明をする＞

- H 中学校の教職員が、生徒にプリントを配付して、特定した利用目的を明示し、データの取扱いについて説明した。
- また、中学生は 15 歳以下であり、本件についての判断能力が不十分であるため、保護者に連絡メールを配信し、同様の内容について説明をした。また、念のため保護者会においても保護者宛に口頭での説明と、同意の取得も行った。

事例 7

【プリントに記載した内容】

- 利用目的

部活動時に運動中の生徒の体調や熱中症リスクを把握して適切な声がけを行い、生徒の健康を守るため。

- サービス概要

このツールを用いることで、生徒本人や教員が、運動時の体調を管理し、熱中症を予防することができます。

- 本ツールで扱う主な個人情報
  - 氏名、年齢、身長、体重
  - 生体情報（心電の波形、心拍数、体温）
  - 加速度情報
  - 端末情報、位置情報
- データの収集手法

本人がウェアラブル端末を装着することによりデータは収集されます。なお、データの収集は部活動時のみに限ります。

- 第三者提供の有無

大学、研究機関等への第三者提供は行いません。

- 保存期間

データは、取得時から２か月後に削除します。

＜ツールの選定・契約＞

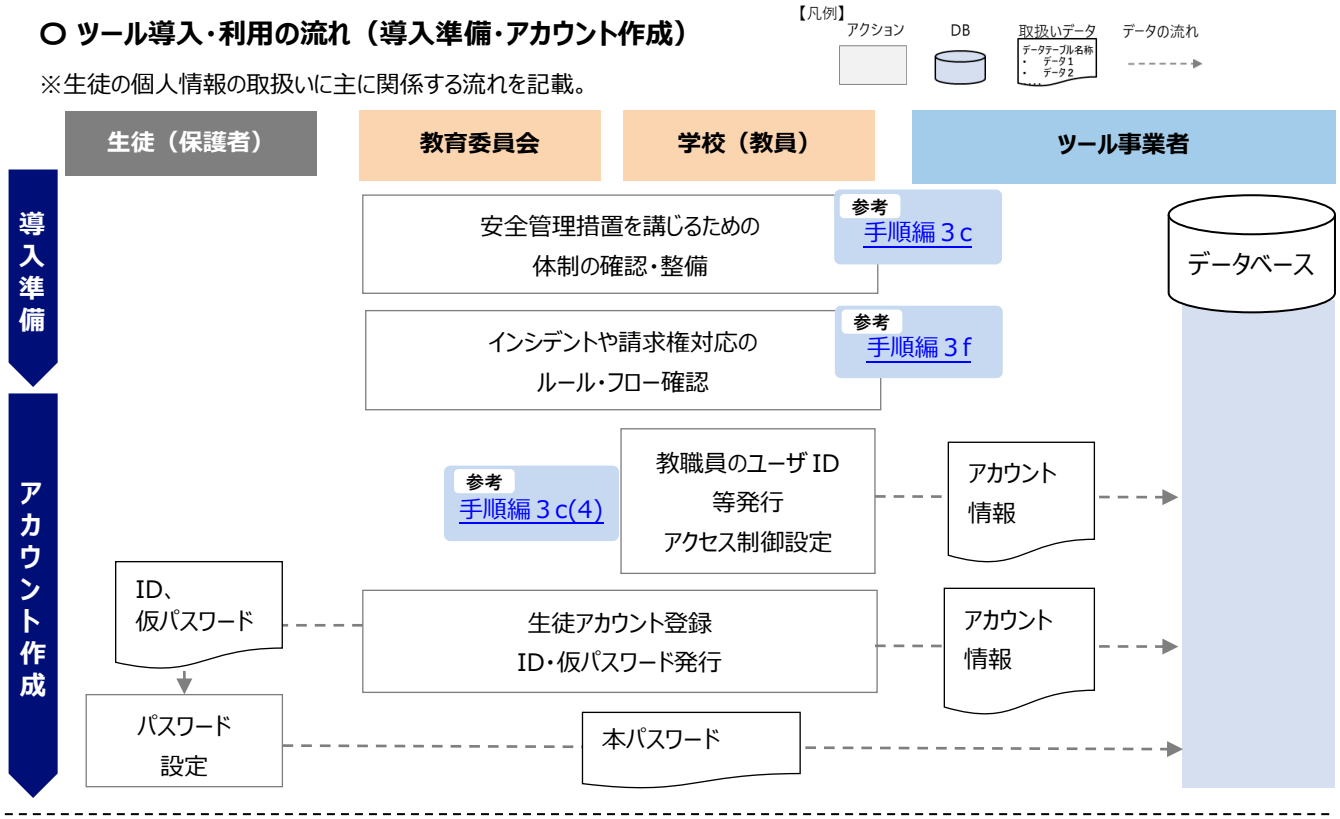
- A 市独自で整備している選定基準を踏まえて、導入するツールを選定し、ツール事業者と A 市教育委員会で契約を行った。
- 委託先との契約に当たっては、契約書に「データの利用やその方法を最小限にすること」や「データを第三者提供しないこと」、「契約終了後はデータを削除すること」等について記載があることを確認し、同意した。

☞契約に当たっては、「Ⅰ．総論編１．４」や「Ⅱ．手順編２b」に記載の事項も確認しましょう。

事例 7

○ ツール導入・利用の流れ（導入準備・アカウント作成）

※生徒の個人情報の取扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置を講じるための体制の確認・整備＞

- 組織的安全管理措置として役割分担の明確化のため、A 市教育委員会において教育長が総括管理責任者であることを確認した。H 中学校においては、全体の管理責任者は学校長であることを確認するとともに、各部活動のデータは部活動の担当教員が責任を持つことを確認し、ツール導入に当たり、教職員にあらためて職員会議で周知した。

  ☞その他の安全管理措置として行うべき事項や留意点は 、「Ⅰ．総論編３．２」や「Ⅱ．手順編３c」も参照してください。

＜インシデントや請求権対応のルール・フロー確認＞

- A 市教育委員会において、個人情報の取扱いに係る規律への違反やデータ漏えい事案等のインシデントが発生した場合のフローを改めて確認し、各学校においてインシデントが発生している事実又は兆候を把握した場合の責任者への報告フローについて、H 中学校に伝達した。
- H 中学校において、インシデント発生時の対応フローと役割分担を整理し、職員会議で周知した。
- 生徒や保護者からの開示請求等が発生した場合のフローにおいても、A 市教育委員会が確認し、H 中学校に伝達した。H 中学校では、請求権対応時の対応フローと具体策を整理し、職員会議で周知した。

事例 7

＜認証とアクセス制御＞

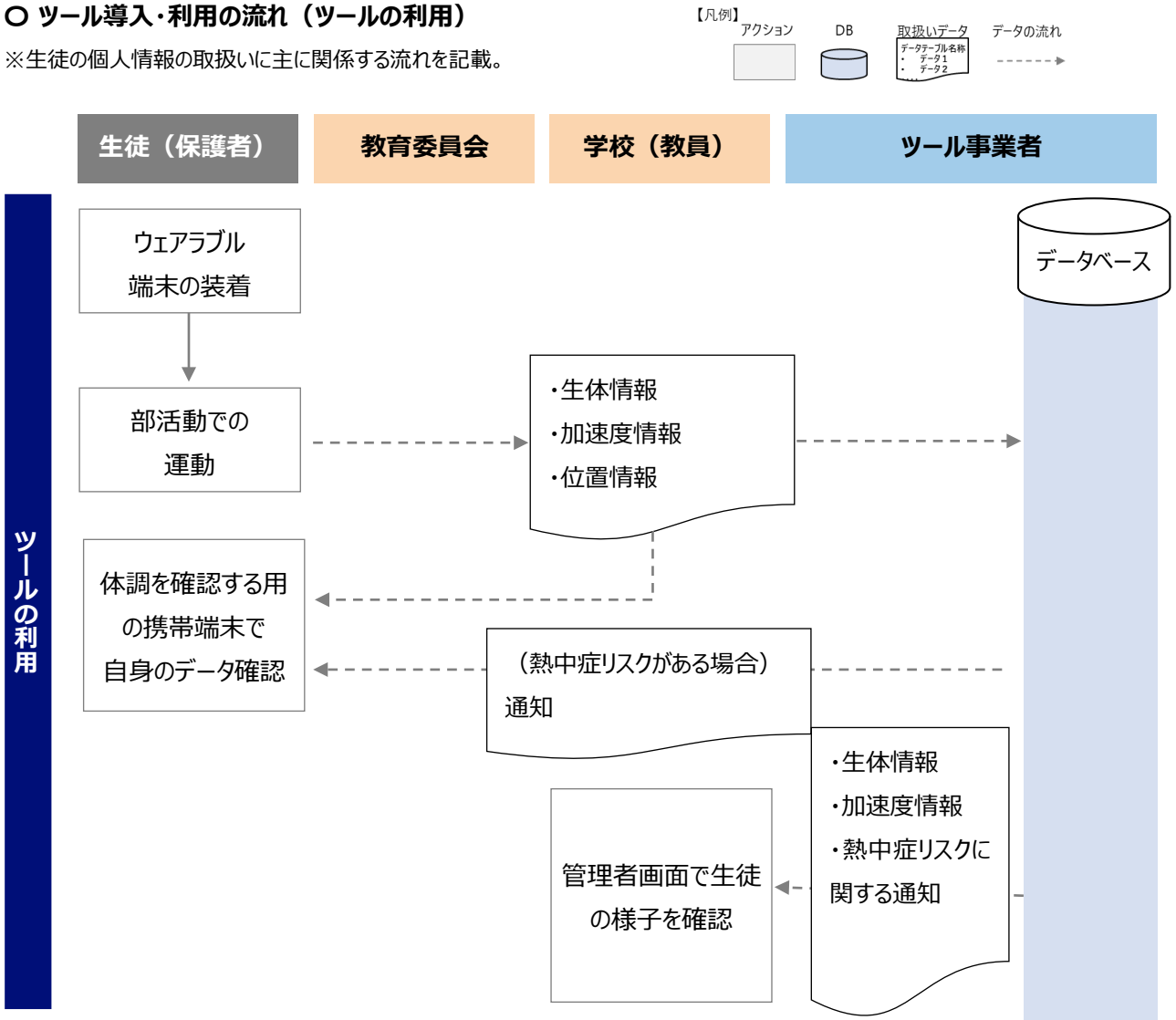
- H 中学校において、アカウント作成時に各アカウントでできること（閲覧、編集、アカウント登録・削除等）を整理して、真に必要な教職員のみがデータを見られるようにした。具体的には、部活動の担当教員は担当している部活動の生徒のデータを、管理職は部活動に参加する全生徒のデータを閲覧・編集できるように設定した。
- アカウント登録・削除等は、管理職のみが実施できるように設定した。

ポイント：情報漏えい等を避けるため、アカウントの権限設定に当たっては、真に必要な人のみに権限を付与し、不要な人に権限付与を行わないようにしましょう。

事例 7

○ ツール導入・利用の流れ（ツールの利用）

※生徒の個人情報の取扱いに主に関係する流れを記載。



【主に実施したこと】

＜利用目的の達成に必要な範囲で個人情報を保有、利用・提供する＞

- H 中学校において、熱中症リスクの分析に必要最小限かつ十分な情報のみを取得した。

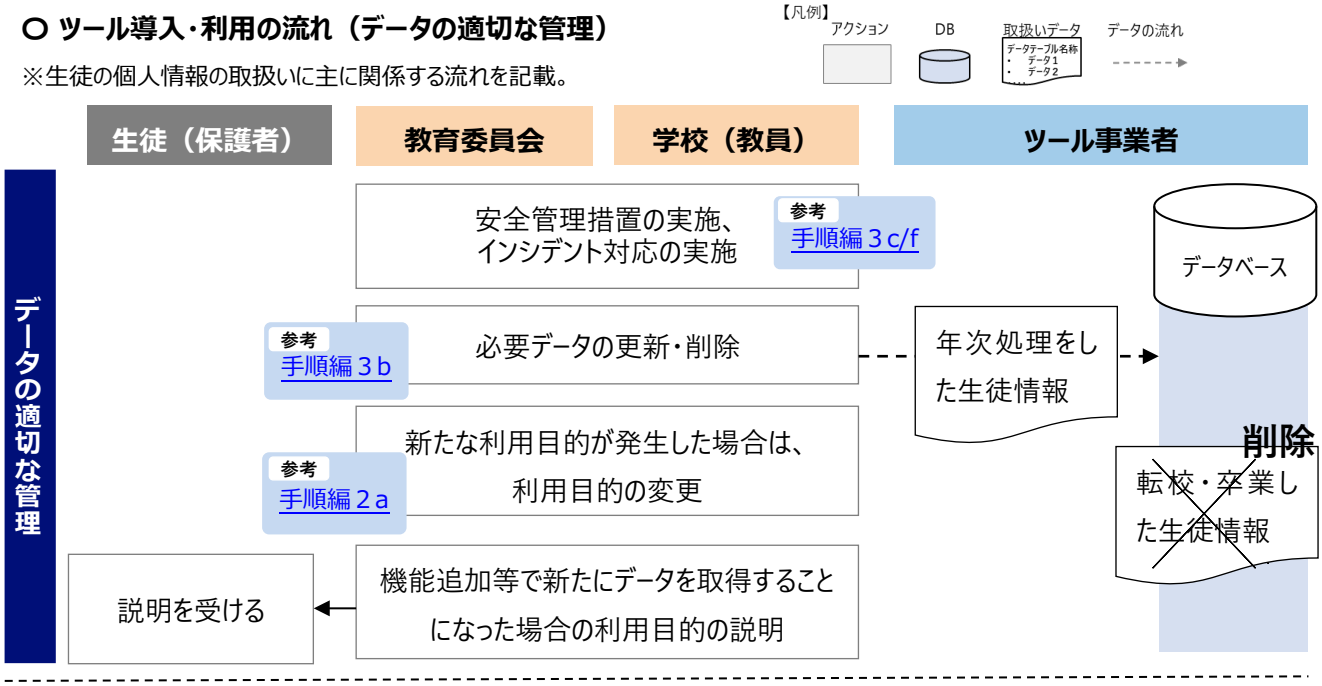
  ポイント：分析を行う上で必要となる情報を整理し、利用目的の達成のために必要最小限かつ十分な情報のみを取得するようにしましょう。

- H 中学校において、取得した生体情報で身体上疾患を推定するようなことはせず、運動中の生徒の体調や熱中症リスクを把握して適切な声がけを行い、生徒の健康を守るためだけに用いるようにした。

事例 7

○ ツール導入・利用の流れ（データの適切な管理）

※生徒の個人情報の取扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置の実施＞

- 組織的安全管理措置として、ツール導入時に確認した役割分担にしたがって、責任者が定期的に個人情報の取扱いについて確認することとした。
- 物理的安全管理措置として、生徒が教職員の携帯端末を勝手に見ることができないように、携帯端末を開くためのパスワードを設定した。また、紛失リスクを軽減するため、データは紙媒体に出力をしない、出力をした場合には不必要に持ち出さない等のルールを定め、教職員に対して職員会議で周知した。また、データの保存期間を最小限とするために、２週間に設定した。
- データの取扱いについて、個人情報保護の観点から A 市教育委員会の実施する研修を H 中学校の教職員が受講した。

☞その他の安全管理措置として行うべき事項や留意点は 、「Ⅰ．総論編３． ２」や「Ⅱ．手順編３c」も参照してください。

＜委託先事業者の管理＞

- A 市教育委員会において、委託事業者が個人情報保護等について契約書に記載された内容を実施していることを確認するため、定期的にチェックリストを提出させた他、委託先に対して必要か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った。

＜データの正確性を確保する＞

- H 中学校で、新年度が開始するタイミングで新たに部活動に参加する生徒情報を新規登録した。
- H 中学校で、転入・転出や卒業、部活動を辞める等のタイミングで、生徒情報の新規登録・削除・変更の処理を行った。

事例 7

＜保有個人情報の削除及び機器、電子媒体等の廃棄＞

- A 市教育委員会は、あらかじめ定めた保管期限を過ぎたデータは、委託先のデータベースから削除させ、委託先に削除された旨の証明書を提出させた。

○ 熱中症の予防のためのツール導入時に注意したこと

１．ウェアラブル端末の着用の任意性の担保

本ツールは心拍数や体温といった生体情報を、生徒の健康を管理するために取得するものである。健康管理において有効なツールではあるが、A 市教育委員会ではウェアラブル端末の着用を強制するほどの必要性は無いと考え、装着は任意とした。

そのため、A 市教育委員会では、H 中学校に対して、ウェアラブル端末の着用は任意であることを生徒や保護者に説明するように周知するとともに、運用状況の定期的な点検を求めた。H 中学校ではこれらの対応に加えて、全教職員に対して、着用を心理的に強制しないように注意喚起を行った。

２．必要最小限のデータ取得

本ツールでは心拍数や体温といった、熱中症把握のために必要なデータ項目の他に、血中酸素飽和度や血圧等の生体データも推計可能であった。A 市教育委員会ではウェアラブル端末で取得する個人情報の利用目的から、熱中症リスクの分析に必要な必要最低限の生体データの取得に限るよう事業者に指示した。

３．必要最小限のデータ利用に関する周知徹底

取得した心拍数や体温といった情報を用いて生徒の身体上疾患を判断する等の様々な利用されるリスク（例：不整脈等を十分な根拠に基づかない推知をしてしまうリスク、本人が知られたくない（公にしていない）症状を推知してしまうリスク、等）が想定される。そのため A 市教育委員会は、そのような利用がなされないよう、利用目的の範囲内においてのみ活用をすることを、H 中学校の教職員に対して研修を通じて周知徹底した。

事例８　A 市立Ｉ中学校において、体育の授業で、生徒の技能習得と向上を促すために、動作解析ツールを利用する

シナリオ

A 市教育委員会では、体育の授業で、生徒の技能習得と向上を促すために、域内の中学校の一つであるＩ中学校において、動作解析ツールを導入することにした。それにあたり、A 市教育委員会及びＩ中学校において、新たなツールの導入に当たって個人情報等の観点から必要な対応を行っている。

○ 導入するツールが有する主な機能のイメージ

・　生徒や教員が持つタブレット端末を用いて、生徒の運動の様子を撮影する。撮影した動画を動作解析ツールに読み込ませると、自動で解析が行われ、運動中の動作（角度、速度等）が数値化される。また、スティックピクチャー（人間を模した簡易的な図）により、関節等の動きを可視化した動画も出力される。

・　児童生徒は動画や動作解析の結果をもとに、これまでの自分の運動の様子と比較して振り返りをすることで、効率的に技能を習得し、向上できる。

○ ツールを導入するメリット

（生徒）

・　自分の運動の様子を客観的に把握し、技能習得や向上に役立てることができる。

・　生徒が自ら考えて主体的に体育の授業に取り組むことにつながる。

（教員）

・　動作解析結果の数値を参照することで、根拠をもって生徒に指導を行うことができる。

・　生徒一人一人に合わせた指導が可能になり、生徒とのコミュニケーションの機会が増える。

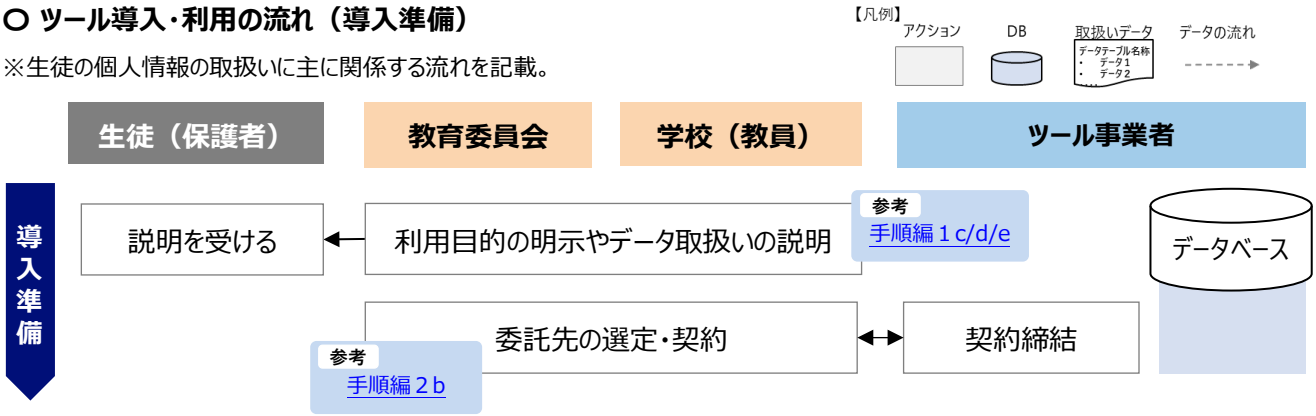
○ 取り扱う主な個人情報

データ種別	主なデータの内容	取得方法
生徒情報	氏名、身長、体重	（あらかじめ保有）
	ユーザ名	生徒がツール利用時に入力
	メールアドレス	
	端末情報	生徒のタブレットから自動で収集
	位置情報	
教員情報	ユーザ名	教員がツール利用時に入力
	メールアドレス	
	端末情報	教員のタブレットから自動で収集
	位置情報	
生体情報	動作解析結果（角度（角速度）、速度（加速度）、脊椎の湾曲率　等）	生徒・教員が持つタブレット内で、選択された動画に対するマーカーレス分析（マーカー等を装着せずに、映像データから人間の動きを分析すること）が行われて算出

事例 8

○ ツール導入・利用の流れ（導入準備）

※生徒の個人情報の取扱いに主に関係する流れを記載。



【主に実施したこと】

＜利用目的（ツールを導入することで取得するデータの利用目的）を特定する＞

- A 市教育委員会において、「体育の授業で用いる」等の抽象的な利用目的ではなく、具体的に、何のデータ項目をどのように使用して指導するのか、まで検討した上で、利用目的を以下のように設定した。
  - 体育の授業において、生徒の運動の様子を撮影した動画や動作解析の結果をもとに、生徒自身が振り返り、教員が根拠のある指導をすることで、生徒の技能習得や向上を促すため。

＊A 市教育委員会では体育の授業で用いていたが、他の利用目的として、総合的な学習（探究）の時間での利用も想定される。

＜利用目的やデータの取扱いの説明をする＞

- I 中学校の教員が、生徒にプリントを配付して、特定した利用目的を明示し、データの取扱いについて説明した。
- また、中学生は 15 歳以下であり、本件についての判断能力が不十分であるため、保護者に連絡メールを配信し、同様の内容について説明をした。また、念のため保護者会においても保護者宛に口頭での説明と、同意の取得も行った。

【プリントに記載した内容】

➢ 利用目的

体育の授業において、生徒の運動の様子を撮影した動画や動作解析の結果をもとに、生徒自身が振り返り、教員が根拠のある指導をすることで、生徒の技能習得や向上を促すため。

➢ サービス概要

このツールを用いることで、生徒本人が、運動の様子を客観的に把握し、技能習得や向上を促すことができます。
また教員が、動作解析結果の数値にもとづいた、根拠のある指導をすることができます。

➢ 本ツールで扱う主な個人情報

- 氏名、身長、体重
- ユーザ名
- メールアドレス
- 端末情報
- 位置情報
- 動作解析結果（角度（角速度）、速度（加速度）、脊椎の湾曲率　等）

➢ データの収集手法

生徒・教員が持つタブレット端末で撮影した動画をツールに読み込ませることにより、動作解析結果の数値が算出されます。
なお、データの収集は体育の授業時のみに限ります。

➢ 第三者提供の有無

大学、研究機関等への第三者提供は行いません。

➢　保存期間
データは、取得時から６か月後に削除します。

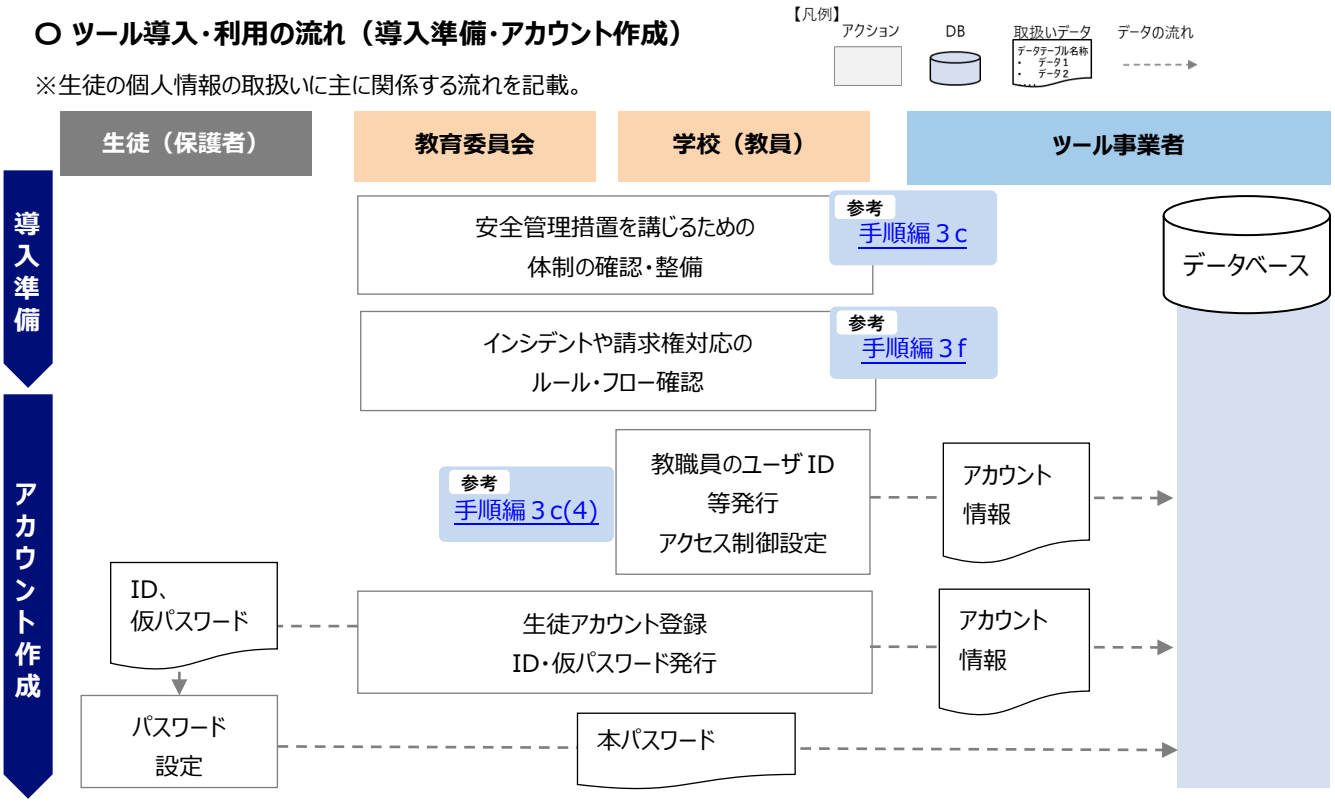
＜ツールの選定・契約＞

- A 市独自で整備している選定基準を踏まえて、導入するツールを選定し、ツール事業者と A 市教育委員会で契約を行った。
- 委託先との契約に当たっては、契約書に「データを第三者提供しないこと」や「契約終了後はデータを削除すること」等について記載があることを確認し、同意した。

☞契約に当たっては、「Ⅰ．総論編１．４」や「Ⅱ．手順編２b」に記載の事項も確認しましょう。

○ ツール導入・利用の流れ（導入準備・アカウント作成）

※生徒の個人情報の取扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置を講じるための体制の確認・整備＞

- 組織的安全管理措置として役割分担の明確化のため、A 市教育委員会において教育長が総括管理責任者であることを確認した。I 中学校においては、全体の管理責任者は学校長であることを確認するとともに、各授業のデータは体育の担当教員が責任を持つことを確認し、ツール導入に当たり、教職員にあらためて職員会議で周知した。

  ☞その他の安全管理措置として行うべき事項や留意点は　、「Ⅰ．総論編３．２」や「Ⅱ．手順編３c」も参照してください。

＜インシデントや請求権対応のルール・フロー確認＞

- A 市教育委員会において、個人情報の取扱いに係る規律への違反やデータ漏えい事案等のインシデントが発生した場合のフローを改めて確認し、各学校においてインシデントが発生している事実又は兆候を把握した場合の責任者への報告フローについて、I 中学校に伝達した。

事例 8

- I 中学校において、インシデント発生時の対応フローと役割分担を整理し、職員会議で周知した。
- 生徒や保護者からの請求が発生した場合のフローにおいても、A 市教育委員会が確認し、I 中学校に伝達した。I 中学校では、請求権対応時の対応フローと具体策を整理し、職員会議で周知した。

＜認証とアクセス制御＞

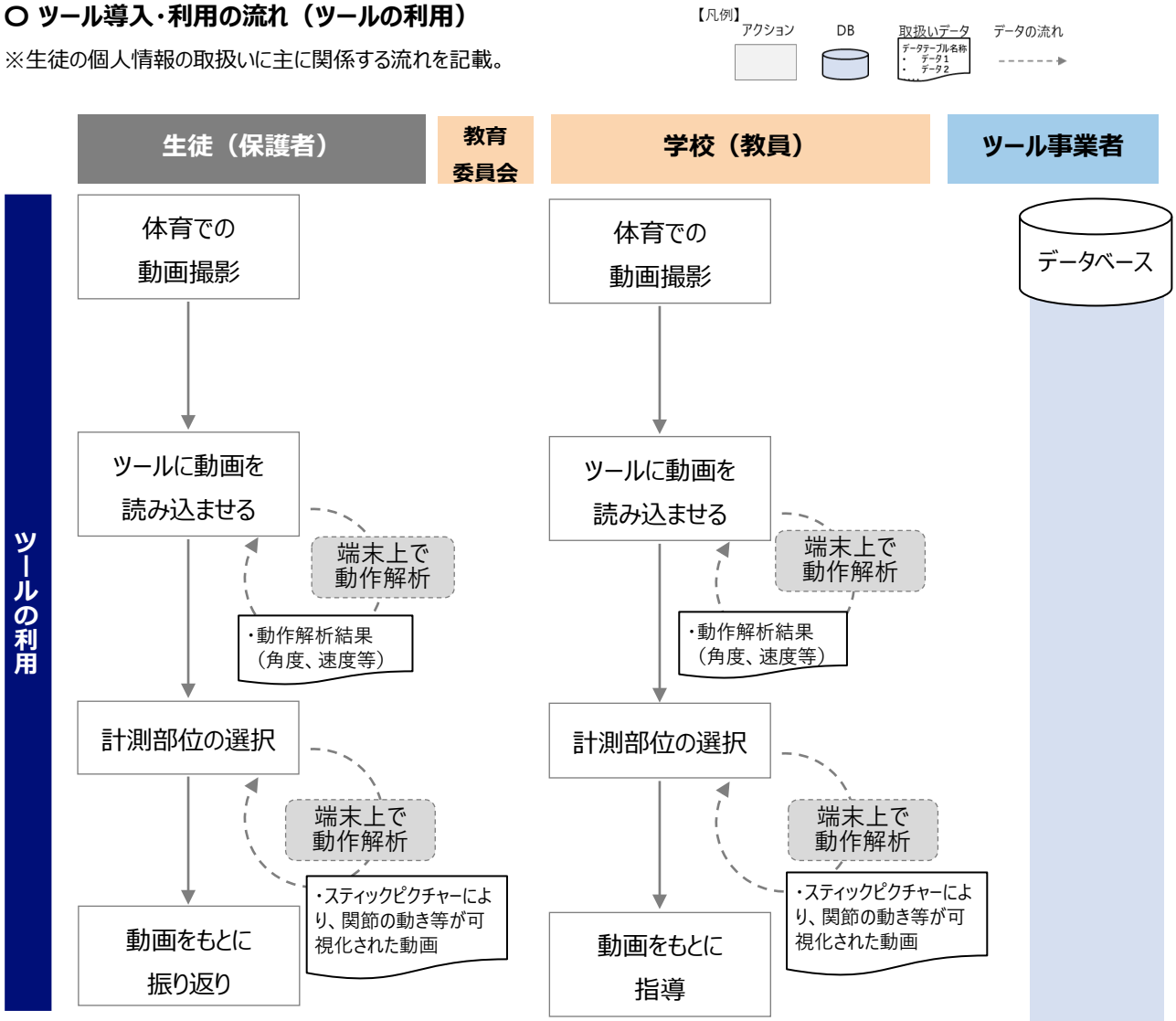
- I 中学校において、アカウント作成時に各アカウントでできること（閲覧、編集、アカウント登録・削除等）を整理して、真に必要な教職員のみがデータを見られるようにした。具体的には、体育の担当教員は担当している生徒のデータを、管理職は全てのデータを閲覧・編集できるように設定した。
- アカウント登録・削除等は、管理職のみが実施できるように設定した。

  ポイント：情報漏えい等を避けるため、アカウントの権限設定に当たっては、真に必要な人のみに権限を付与し、不要な人に権限付与を行わないようにしましょう。

事例 8

○ ツール導入・利用の流れ（ツールの利用）

※生徒の個人情報の取扱いに主に関係する流れを記載。



【主に実施したこと】

＜利用目的の達成に必要な範囲で個人情報を保有、利用・提供する＞

- Ｉ中学校において、動作の分析に必要最小限かつ十分な情報のみを取得した。

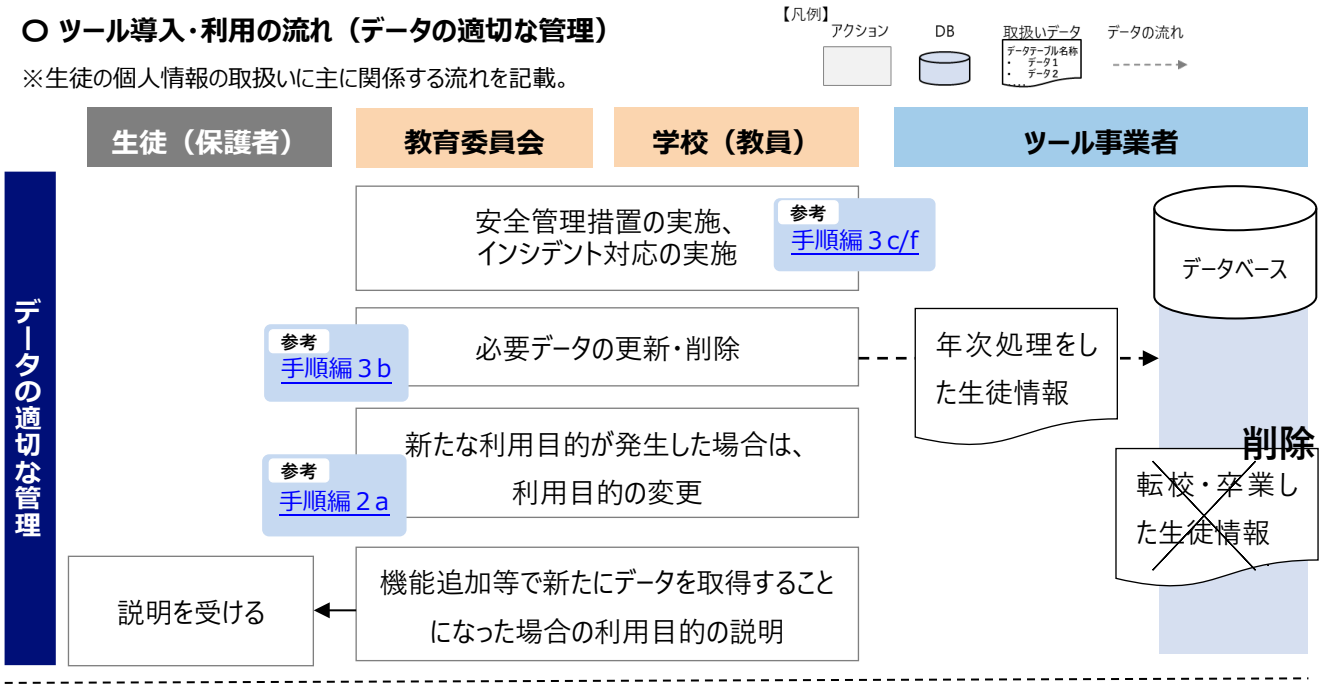
  ポイント：分析を行う上で必要となる情報を整理し、利用目的を達成のために必要最小限かつ十分な情報のみを取得するようにしましょう。

- Ｉ中学校において、動作分析の結果はあくまで参考情報であり、成績の評価とはまったく関係のない情報であると整理することで、動作分析の結果を成績の評価には用いず、教員による根拠のある指導と、生徒の技能習得や向上を促すためだけに用いるようにした。

事例 8

○ ツール導入・利用の流れ（データの適切な管理）

※生徒の個人情報の取扱いに主に関係する流れを記載。



【主に実施したこと】

＜安全管理措置の実施＞

- 組織的安全管理措置として、ツール導入時に確認した役割分担にしたがって、責任者が定期的に個人情報の取扱いについて確認することとした。
- 物理的安全管理措置として、生徒が教職員のタブレット端末を勝手に見ることができないように、タブレット端末を開くためのパスワードを設定した。また、紛失リスクを軽減するため、データは紙媒体に出力をしない、出力をした場合には不必要に持ち出さない等のルールを定め、教職員に対して職員会議で周知した。また、データの保存期間を最小限とするために、６か月に設定した。
- データの取扱いについて、個人情報保護の観点からＡ市教育委員会の実施する研修をＩ中学校の教職員が受講した。

☞その他の安全管理措置として行うべき事項や留意点は　、「Ⅰ．総論編３．２」や「Ⅱ．手順編３c」も参照してください。

＜委託先事業者の管理＞

- Ａ市教育委員会において、委託事業者が個人情報保護等について契約書に記載された内容を実施していることを確認するため、定期的にチェックリストを提出させた他、委託先に対して必要か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った。

＜データの正確性を確保する＞

- Ｉ中学校で、新年度が開始するタイミングで新たに入学する生徒情報を新規登録した。
- Ｉ中学校で、転入・転出や卒業等のタイミングで、生徒情報の新規登録・削除・変更の処理を行った。

事例 8

＜保有個人情報の削除及び機器、電子媒体等の廃棄＞

- A 市教育委員会は、あらかじめ定めた保存期間が過ぎたデータは、委託先のデータベースから削除させ、委託先に削除された旨の証明書を提出させた。

事例 8

○動作解析のためのツール導入時に注意したこと

１．動画の撮影の任意性の担保

本ツールは生徒や教員が撮影した動画を、生徒の動作を解析し、技能習得や向上を促すために活用するものである。技能習得や向上において有効なツールではあるが、A 市教育委員会では動画の撮影を強制するほどの必要性は無いと考え、撮影は任意とした。

そのため、A 市教育委員会では、I 中学校に対して、動画の撮影は任意であることを生徒や保護者に説明するように周知するとともに、運用状況の定期的な点検を求めた。I 中学校ではこれらの対応に加えて、全教職員に対して、撮影を心理的に強制しないように注意喚起を行った。

２．情報の活用方法に関する周知徹底

取得した動作分析の結果を用いて、生徒の成績をつけてしまうリスクが想定される。そのため A 市教育委員会は、そのような利用がなされないよう、利用目的の範囲内においてのみ活用をすることを、I 中学校の教職員に対して研修を通じて周知徹底した。

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 に加えて、Ⅰ．総論編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、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（デジタルデータ）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（デジタルデータ）[92]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（体力測定の結果やテストの点数等）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）

[92] 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であれば、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）も含まれます。

・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、子供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、保護者が子供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。

子供、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．子供の視点

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

・子供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。

・学校全体で子供の様子を把握し、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。

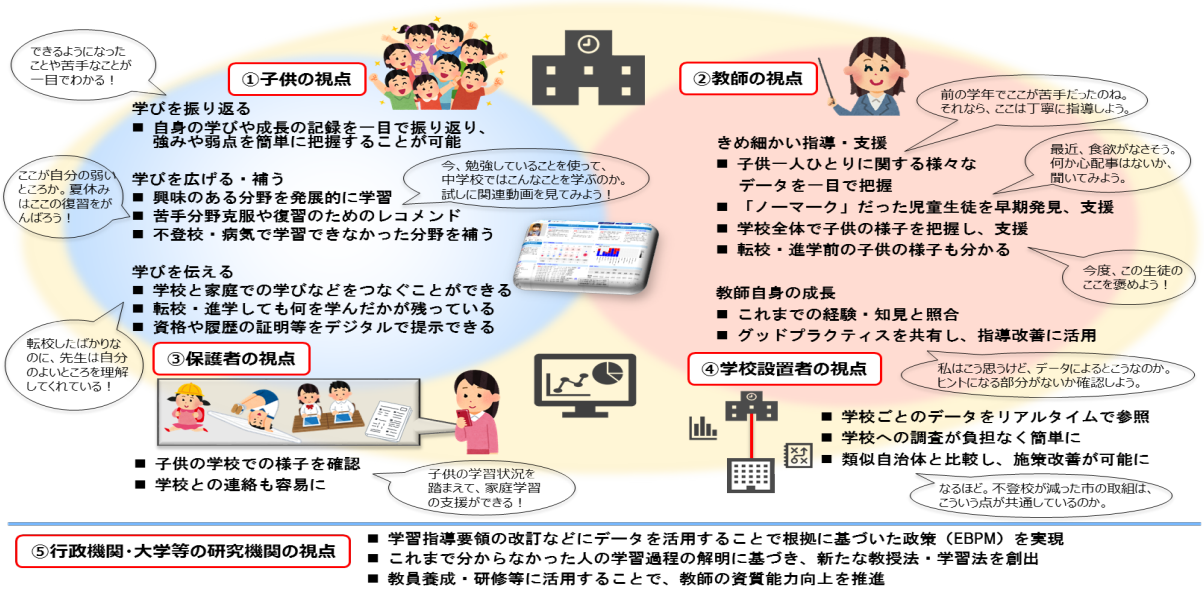
・学校との連絡が容易になる。

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）[93]

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。

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

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、本人の望まない形で教育データの利活用が行われることによって個人が不利益を受けることのないようにすることや、従来からの教師の観察や見取りと教育データで可視化される情報を両立させてバランスをとること、教育データ利活用は目的化せずにあくまで目的達成のための手段として認識することなどに留意が必要です。

さらに、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、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、「Ⅰ．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、「Ⅰ．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」[94]の７つの原則[95]の一つである

[94] 「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）

[95] 「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。

「個人情報等の取扱いに関する透明性と信頼性」の原則、主に地方公共団体が設置する学校を対象とした教育情報セキュリティポリシー[96]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、「Ⅰ．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、「Ⅰ.総論編【コラム３】ELSI（倫理的・法的・社会的課題）」を参照してください。

[96] 教育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、「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)を策定しています。
（https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm ）

Q（４）教育データには、どのような個人情報が含まれますか。

【回答】

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ような情報。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、それにより特定の個人を識別できる情報。

② 個人識別符号を含む情報。

教育委員会・学校が取り扱う教育データにおいては、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．個人情報の考え方

【回答】にあるとおり、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が、「他の情報と容易に照合することができ」るとは、地方公共団体の機関[97]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[98]。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。

---

[97] 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。（「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）」（個人情報保護委員会）３-１-１）

[98] 教育委員会が所管する公立学校については、個々の学校自体がそれぞれ一つの「地方公共団体の機関」となるわけではなく、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。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。

②の「個人識別符号」とは、当該情報単体から特定の個人を識別することができるものとして政令に定められた文字、番号、記号その他の符号をいい、これに該当するものが含まれる情報は個人情報となります。代表的なものとしては個人番号（マイナンバー）[99]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。

個人識別符号（個人の身体的特徴に関する符号）：
「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

２．教育委員会・学校における個人情報の例

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
- 学年、組、学籍番号
- 住所、生年月日、身長、体重
- 出欠席情報
- １人１台端末の利用ログ
- 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。

[99] 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）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。

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。

Q（５）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（４）」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」とは、地方公共団体の機関[100]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、個々の学校自体がそれぞれ一つの「地方公共団体の機関」となるわけではなく、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。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、氏名等と容易に紐付けることができ、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利用ログ等に関するデータ）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

[100] 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。（「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）」（個人情報保護委員会）３-１-１）

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、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[101]。

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、「Ⅰ．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[102]。

---

[101]（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）

[102]「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）」（個人情報保護委員会）３-２-７

【コラム５】 「△△市立○○中学校３年Ａ組15番」は個人情報？

「Ⅳ．Q&A 編 Q（４）」において、例えば「生年月日」や「学籍番号」のような、こ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、個人情報に該当すると解説をしました。

では、「△△市立○○中学校３年Ａ組15番」という情報は個人情報に該当するでしょうか？

○○中学校内であれば、「△△市立○○中学校３年Ａ組15番」が、「文科太郎くん」であることは、学校内にある名簿を見ればすぐに分かりますよね。名簿は、職員室にも教室の当番表にも、様々な場所にあると考えられます。その場合、「他の情報と容易に照合することができ」る情報にあると整理できるため、「△△市立○○中学校３年Ａ組15番」は個人情報に該当します。

では、△△市教育委員会においてはどうでしょうか。一見、△△市教育委員会には、児童生徒の名簿がないため「他の情報と容易に照合することができ」ない個人情報ではないのではないかと思われるかもしれません。しかし、「他の情報と容易に照合することができ」るかどうかは、教育委員会と所管の学校をまとめて一つの「地方公共団体の機関」とし、その中で照合できるかどうかで判断することになっています（「Ⅰ.総論編【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？）。つまり、教育委員会内では照合することが不可能でも、教育委員会の所管するどこかの学校において照合することができる場合は、「他の情報と容易に照合することができ」ると判断するのです。そのため、「△△市立○○中学校３年Ａ組15番」という情報は、△△市教育委員会においては「他の情報と容易に照合することができ」なくても、△△市教育委員会に属する○○中学校においては「他の情報と容易に照合することができ」、それが「文科太郎くん」であることが分かってしまうため、△△市教育委員会においても個人情報であると判断されます。

「氏名が無ければ個人情報では無い」と誤解しがちですが、仕組みを理解して情報を取り扱っていくことが大切です。

Q（６）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、児童生徒の発達段階、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は、「Ⅰ．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（オンラインを含みます。以下本 Q において同じ。）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[103]。

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。

[103] 学校や校長の名義で利用目的の明示を行う場合でも、当該個人情報が当該学校だけでなく教育委員会等での利用を想定している場合は、その旨も明示する必要があります。

Q（７）教育データの利活用を行う場合、同意の取得は必要ですか。同意の取得が必要になるのはどのような場合ですか。必要な場合はどのように同意を取得すれば良いですか。

【回答】

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利用・提供することが基本です。このように利用目的の範囲内で取り扱う場合には、利用目的を特定することは必要ですが、同意の取得は求められません。よって、教育データの利活用を行う全ての場合で児童生徒や保護者の同意が必要なわけではありません。

一方、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利用・提供する際の選択肢の一つと位置づけられています。同意を取得する場合は、教育委員会や各学校の教職員が、原則本人から（発達段階に応じて保護者から）同意を取得します。詳細は、「Ⅰ．総論編１．３．３」を参照してください。

【解説】

１．同意を取得する場合とは

上記の通り、教育データの利活用を行う全ての場合で、同意が必要となるわけではありません。

行政機関等は、法令の定める事務又は業務を遂行するため必要な場合に限り、個人情報を利用・提供することができます。その際、行政機関等は、個人情報の利用目的についてできるだけ具体的に特定し、一部の場合[104]を除き、本人に対して利用目的をあらかじめ明示しなければなりません。この通常のフローには同意の取得というプロセスは含まれておらず、そのため、同意の取得は必要ではありません。

一方で、臨時的に利用目的以外の目的のために保有個人情報を利用・提供する場合には、別のフローを取る必要があります。利用目的以外の目的で利用・提供をするには、本人の同意がある、または個人情報保護法第 69 条第２項[105]に示される場合に当てはまることが条件となるため、学校・教育委員会が利用目的以外の目的のために個人情報を利用・提供を行う場合、児童生徒や保護者の同意を取得して利用・提供するという選択肢があります。

---

[104] 個人情報保護法第 62 条第１号～第４号に示す場合
（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（同条第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（同条第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（同条第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（同条第４号）。

[105] 個人情報保護法第 69 条第２項に示される場合　①本人の同意があるとき、又は本人に提供するとき。②行政機関等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保有個人情報を内部で利用する場合であって、当該保有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。③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保有個人情報を提供する場合において、保有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。④③に掲げる場合のほか、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、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、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。

なお、学校教育は全ての児童生徒に対して平等に実施されることから、一部の児童生徒のみが同意しないことが事実上困難であることが想定されますが、そのような同意には任意性がなく、無効と判断される場合もあるため、留意が必要です。

２．どのように同意を取得するか

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・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・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[106]。

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・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。

ただし、適正に同意が取得されていない場合は、同意が無効になる場合があります。詳細は「Ⅰ．総論編１．３．３」を確認してください。

３．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 歳までの年齢以下の子供については、保護者等からの同意を得る必要があるとされています。

なお、15 歳以下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。

106 同意の取得は、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。

Q（８）新たな学習用ソフトウェア等を契約・導入する際、個人情報の取扱いに関してどのようなことに気を付ければよいですか。

【回答】

学習用ソフトウェア等（※）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。

そのため、個人情報の適切な管理を行う能力を有する学習用ソフトウェア等提供事業者を選定するとともに、委託先における個人情報の適正な取扱い、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、契約書、利用規約、個人情報保護に関するポリシー等の書面で、個人情報の取扱いに関して必要かつ適切な措置が取られているかの確認が求められます。

なお、教育委員会・学校が、所掌事務の遂行のために、授業など児童生徒が一律に参加する教育活動で学習用ソフトウェア等を活用することで取得される児童生徒の個人情報については、学習用ソフトウェア等を提供する民間事業者での取扱いも含め、当該教育委員会・学校で責任をもって取り扱う必要があるということが前提となります。この前提を踏まえると、そうした取扱いを担保するためには、教育委員会・学校から民間事業者に「個人情報の取扱いを委託」することが一般的であり、望ましいことから、基本的にこうした対応が求められます[107]。

※学習用ソフトウェア等

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．契約書等に明記すべき事項

個人情報の取扱いについては、学習用ソフトウェア等提供事業者との契約の際に、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。なお、学習用ソフトウェア等提供事業者の契約書等にこれらが示されていない、あるいは内容が不十分である場合は、別途、個人情報の取扱いに係る契約を締結する等の方策をとる必要があります。

[107] 実際には個別の事例ごとに判断されることになりますが、法律の専門家からは、委託によらず民間事業者に直接取得させることは、個人情報保護法第 20 条に照らして、民間事業者が適正に個人情報を取得しているかという観点で、違法の疑いもあるとの指摘もあったところ、民間事業者の提供する学習用ソフトウェア等を活用するに当たっては、適切に選択するよう留意してください。

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

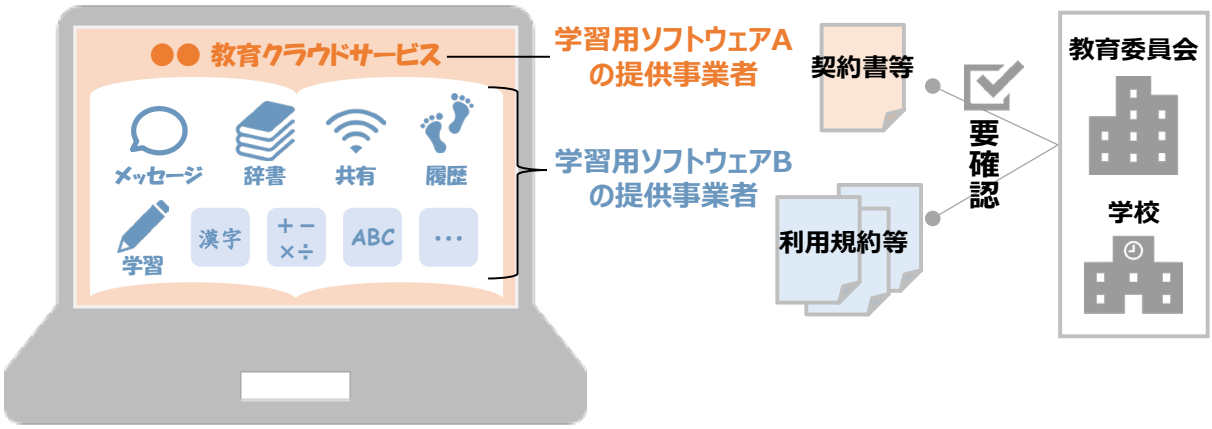
① 個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等の義務
② 再委託の制限又は事前承認等再委託に係る条件に関する事項
③ 個人情報の複製等の制限に関する事項
④ 個人情報の安全管理措置に関する事項
⑤ 個人情報の漏えい等[108]の事案の発生時における対応に関する事項
⑥ 委託終了時における個人情報の消去及び媒体の返却に関する事項
⑦ 法令及び契約に違反した場合における契約解除、損害賠償責任その他必要な事項
⑧ 契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱い状況を把握するための監査等に関する事項

このとき、「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等提供事業者が、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[109]。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ため、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。

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等提供事業者との契約や学習用ソフトウェア等提供事業者の管理の詳細については、「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）」（個人情報保護委員会）の４－８－９、最新の「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）[110]の「第２編８．外部委託」及び「第 2 編９．SaaS 型パブリッククラウドサービスの利用」等も参考にしてください。

[108] 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。
[109] 委託先は、委託に伴って委託元から提供された個人情報を、委託された業務の範囲内でのみ取り扱わなければなりません。委託先が当該個人情報を統計情報に加工することが委託された業務の範囲内である場合には、委託先は当該加工を行うことができますが、委託された業務の範囲外で委託先が当該加工を行い、作成された統計情報を自社のために用いることはできません。（「「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) A7-38）
[110] https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm



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等提供事業者の契約書等

２．個人情報の取扱いを委託する場合の留意事項

個人情報の取扱いを委託する場合は、上記に加え、「Ⅰ．総論編１．４」に示す点にも留意が必要です。

また、学習用ソフトウェア等を導入する段階で、導入しようとする学習用ソフトウェア等の安全性や信頼性を確認することが必要です。学習用ソフトウェア等の安全性や信頼性については、学習用ソフトウェア等提供事業者が、プライバシーマーク [111]や ISMS 認証 [112]といった第三者認証を取得しているか、学習者プライバシー宣言 [113]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等提供事業者に質問）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等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。

３．学習用ソフトウェア等提供事業者等に統計情報を提供する場合

統計情報は、特定の個人との対応が排斥されている限りは、個人情報保護法の適用の対象外となります。そのため、統計情報であれば、学習用ソフトウェア等提供事業者等に提供することが可能です。

111 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/）
112 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）
113 一般社団法人 ICT CONNECT 21 が設立した 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等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/）

Q（９）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（クラウドサービス）を利用する場合に、気を付けるべきことはありますか。

【回答】

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、違いはありません。クラウドの活用を念頭に置いて、留意点への対策を行っていく必要があります。

【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」[114]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、教育委員会自らがサーバ等を用意する（オンプレミス）ことがなく、初期費用を大幅に抑えられたり、より効率的・効果的に情報セキュリティを担保することが可能となったり、日進月歩で進化する新しいサービスの取り入れが容易であったりする等の利点があります。

従来のオンプレミスを前提とした ICT 環境整備を否定するものではありませんが、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ること（クラウド・バイ・デフォルトの原則）[115]も踏まえ、クラウドサービスの利用を念頭に置いて検討を進める必要があります。

また従来、重要性の高い情報のセキュリティの確保に当たっては、ネットワーク分離による境界防御型のセキュリティ対策を講じていましたが、近年では、強固なアクセス制御による対策（インターネットを通信経路とする前提で、内部・外部からの不正アクセスを防御するために、多要素認証による利用者認証、端末認証、端末・サーバ・通信の監視・制御等を組み合わせたセキュリティ対策を指す）が有効な手段として示されています。パブリッククラウド環境で重要性の高い情報を取り扱う場合には、この対策を実施することが必要です。

２．クラウドサービスの活用を念頭に置いた留意点

クラウドサービスを利用する場合には、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

---

114 サーバやソフトウェア等のシステムをユーザが管理する施設に設置し、管理運用する方式

115 「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）

するとともに、情報資産毎に許可されたクラウドを利用する教職員等及び児童生徒のみがアクセスできる環境を設定したり、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を取る必要があります[116]。特に、クラウドサービスの安全性や信頼性については、プライバシーマーク[117]やISMS認証[118]といった第三者認証を取得しているか、学習者プライバシー宣言[119]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、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[120]。

[116] 対策について、基本は「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）「第２編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、SaaS 型パブリッククラウドサービスの場合は「第２編９　SaaS 型パブリッククラウドサービスの利用」、その他の場合は「第２編８　外部委託」。学習用端末の利用については、「第２編４.５　学習者用端末のセキュリティ対策」。

[117] 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/）

[118] 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）

[119] 一般社団法人 ICT CONNECT 21 が設立した 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等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/）

[120] 「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）第２編９.２「SaaS 型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

Q（10）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[121]（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[122]や条例要配慮個人情報[123]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[124]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】

教育データが漏えい等した場合には、以下を参考に対応してください[125]。なお、個人情報保護法上の義務を守ることに加えて、主に地方公共団体が設置する学校を対象とした教育情報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

教育データの漏えい等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、漏えい等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。

２．被害の拡大防止

---

121 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。（「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）第２編２．組織体制)

122 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。本人の人種、信条、社会的身分、病歴、犯罪の経歴等が含まれます。（個人情報保護法第２条第３項）

123 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

124 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。

125 「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）」（個人情報保護委員会）４-８-11

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（教職員に指示することを含みます。）を、直ちに行います。

３．教育委員会への報告

教育情報セキュリティ管理者は、教育データの漏えい等が発生した経緯、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[126]

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[127]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[128]は60日以内）に確報を行う必要があります。

法令上で、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[129]。

---

126 個人情報保護法第68条、「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）」（個人情報保護委員会）5-4

127 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挙げられています。（個人情報保護法施行規則第43条）

128 個人情報保護法施行規則第43条第３号

129 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。（「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）」（個人情報保護委員会）４-４-１「（５）漏えい等報告の対象となる事態」）

Q（11）教育データをシステム上で安全に管理するうえで、情報セキュリティの観点から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、主に地方公共団体が設置する学校を対象とした教育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。）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、各教育委員会が教育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」（文部科学省）[130]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、「Ⅰ．総論編３」を参照するとともに、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」、「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）」（個人情報保護委員会）の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（第２編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（第２編２．）、アクセス制御（第２編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（第２編２．）、情報セキュリティインシデントの報告（第２編５．５．）、侵害時の対応（第２編７．９．）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（第２編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（第２編４．４．）、教育情報セキュリティ管理者の措置事項（第２編５．１．）、教職員等の遵守事項（第２編５．２．）、教育委員会事務局職員の遵守事項（第２編５．３．）等
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（第２編４．４．）、教育情報セキュリティ管理者の措置事項（第２編５．１．）、教職員等の遵守事項（第２編５．２．）、教育委員会事務局職員の遵守事

[130] https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm

	項（第２編５．３．）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（第２編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（第２編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（第２編６．２．）、不正アクセス対策（第２編６．５．）等
教育データ取扱いに係る教育、研修	研修・訓練(第２編５．４．）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、「Ⅰ．総論編１．４」及び「Ⅳ．Q&A 編Q（８）」を参照してください。

別添

国立・私立学校が留意すべき個人情報保護法の規律
–早見表–

文部科学省

目次

1．教育データの利活用にあたり、国立学校が留意すべき個人情報保護法の規律 126

2．教育データの利活用にあたり、私立学校が留意すべき個人情報保護法の規律 129

教育データの利活用に当たり、国立学校が留意すべき個人情報保護法の規律

参考となり得る留意事項の目次（※）	国立学校が参照すべき個人情報保護法上の主な規律	
1.3.2 個人情報の保有・取得	17 条（利用目的の特定）	• 個人情報を取り扱うに当たっては、その利用の目的をできる限り特定しなければならない
	20 条（適正な取得、要配慮個人情報の取得）	• 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 • 20 条第 2 項各号の場合を除くほか、原則として、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない
	21 条（取得に際しての利用目的の通知等）	• 個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない • 本人から直接書面（電磁的記録を含む。）に記載された当該本人の個人情報を取得する場合は、原則として、あらかじめ、本人に対し、その利用目的を明示しなければならない
	22 条（データ内容の正確性の確保等）	• 利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない
	30 条（第三者提供を受ける際の確認等）	• 27 条第 1 項各号または第 5 項各号の場合を除き、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、当該第三者の氏名又は名称及び住所並びに法人にあってはその代表者の氏名、当該第三者による当該個人データの取得の経緯の確認を行わなければならない • 確認を行ったときは、個人情報保護委員会規則で定めるところにより、当該個人データの提供を受けた年月日、当該確認に係る事項その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない • 当該記録を個人情報保護委員会規則で定める期間保存しなければならない
1.3.3 個人情報の利用・提供 ※委託との関係では 1.4 も参照	18 条（利用目的による制限）	• あらかじめ本人の同意を得た場合を除き、原則として、17 条の規定により、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない
	19 条（不適正な利用の禁止）	• 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
	27 条（第三者提供の制限）	• 個人データを提供する場合、委託や共同利用に該当しない限りは、原則として本人の同意を取得する必要がある

参考となり得る留意事項の目次（※）	国立学校が参照すべき個人情報保護法上の主な規律	
	29 条（第三者提供に係る記録の作成等）	• 27 条第 1 項各号または第 5 項各号の場合を除き、個人データを第三者に提供したときは、個人情報保護委員会規則で定めるところにより、当該個人データを提供した年月日、当該第三者の氏名又は名称その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない • 当該記録を個人情報保護委員会規則で定める期間保存しなければならない
	28 条（外国にある第三者への提供の制限）	• 外国にある第三者への個人データの提供を行う場合、次の場合を除き、あらかじめ、当該外国における個人情報の保護に関する制度等の情報を提供したうえで、本人から同意を取得しなければならない a.データ提供先事業者の所在国が、十分性認定の対象国（EU（注）、英国）である b.データ提供先事業者が、個人情報保護委員会規則で定める基準に適合する体制を整備している c.27 条第 1 項各号のいずれかに該当する場合 （注）欧州連合加盟国及び欧州経済領域(EEA)協定に基づきアイスランド、リヒテンシュタイン及びノルウェーを含む
	31 条（個人関連情報の第三者提供の制限等）	• 個人関連情報の第三者提供を行う際に、原則として、次の対応を行う必要がある １．提供先の第三者が個人データとして取得することが想定される場合、提供前に、適切に本人の同意が得られていることを確認する ２．第三者提供に係る記録を作成する
1.3.4 個人情報の保管	22 条（データ内容の正確性の確保等）	• 利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない（再掲）
1.4 個人情報の取扱いの委託	25 条（委託先の監督）	• 個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない
1.5.1 開示、訂正、利用停止請求	76 条~108 条（開示請求権~条例との関係）	• （公立学校と同様の規律なので、「Ⅰ総論編」「1.5.1 開示、訂正、利用停止請求 」を参照ください）
1.5.2 個人情報ファイル簿の作成	75 条（個人情報ファイル簿の作成及び公表）	• （公立学校と同様の規律なので、「Ⅰ総論編」「1.5.2 個人情報ファイル簿の作成」を参照ください）
	26 条（漏えい等の報告等）	• 取り扱う個人データの漏えい、滅失、毀損その他の個人データ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

参考となり得る留意事項の目次（※）	国立学校が参照すべき個人情報保護法上の主な規律	
1.5.3 苦情処理、漏えい・滅失・毀損した際の対応		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ものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。また、本人に対し、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を通知しなければならない ※公立学校と国立学校では、個人情報保護委員会への報告対象となる事態が異なる
	40 条（個人情報取扱事業者による苦情の処理）	• 個人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なければならない
3.2 個人情報保護法の観点から～安全管理措置～	23 条（安全管理措置）	• 取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない
	24 条（従業者の監督）	• 従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない

※「教育データの利活用に係る留意事項」はあくまで公立学校を対象とした留意点を整理したものであり、国立学校における個人情報の取扱いにそのまま適用されるものではないことに留意

教育データの利活用に当たり、私立学校が留意すべき個人情報保護法の規律

参考となり得る留意事項の目次（※）	私立学校が参照すべき個人情報保護法上の主な規律	
1.3.2 個人情報の保有・取得	17 条（利用目的の特定）	• 個人情報を取り扱うに当たっては、その利用の目的をできる限り特定しなければならない
	20 条（適正な取得、要配慮個人情報の取得）	• 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 • 20 条第 2 項各号の場合を除くほか、原則として、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない
	21 条（取得に際しての利用目的の通知等）	• 個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない • 本人から直接書面（電磁的記録を含む。）に記載された当該本人の個人情報を取得する場合は、原則として、あらかじめ、本人に対し、その利用目的を明示しなければならない
	22 条（データ内容の正確性の確保等）	• 利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない
	30 条（第三者提供を受ける際の確認等）	• 27 条第 1 項各号または第 5 項各号の場合を除き、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、当該第三者の氏名又は名称及び住所並びに法人にあってはその代表者の氏名、当該第三者による当該個人データの取得の経緯の確認を行わなければならない • 確認を行ったときは、個人情報保護委員会規則で定めるところにより、当該個人データの提供を受けた年月日、当該確認に係る事項その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない • 当該記録を個人情報保護委員会規則で定める期間保存しなければならない
1.3.3 個人情報の利用・提供 ※委託との関係では 1.4 も参照	18 条（利用目的による制限）	• あらかじめ本人の同意を得た場合を除き、原則として、17 条の規定により、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない
	19 条（不適正な利用の禁止）	• 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
	27 条（第三者提供の制限）	• 個人データを提供する場合、委託や共同利用に該当しない限りは、原則として本人の同意を取得する必要がある
	29 条（第三者提供に係る記録の作成等）	• 27 条第 1 項各号または第 5 項各号の場合を除き、個人データを第三者に提供したときは、個人情報保護委員会規則で定めるところにより、当該個人データを提供した年月日、当該第三

参考となり得る留意事項の目次（※）	私立学校が参照すべき個人情報保護法上の主な規律	
		者の氏名又は名称その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない • 当該記録を個人情報保護委員会規則で定める期間保存しなければならない
	28 条（外国にある第三者への提供の制限）	• 外国にある第三者への個人データの提供を行う場合、次の場合を除き、あらかじめ、当該外国における個人情報の保護に関する制度等の情報を提供したうえで、本人から同意を取得しなければならない a.データ提供先事業者の所在国が、十分性認定の対象国（EU（注）、英国）である b.データ提供先事業者が、個人情報保護委員会規則で定める基準に適合する体制を整備している c.27 条第 1 項各号のいずれかに該当する場合 （注）欧州連合加盟国及び欧州経済領域(EEA)協定に基づきアイスランド、リヒテンシュタイン及びノルウェーを含む
	31 条（個人関連情報の第三者提供の制限等）	• 個人関連情報の第三者提供を行う際に、原則として、次の対応を行う必要がある １．提供先の第三者が個人データとして取得することが想定される場合、提供前に、適切に本人の同意が得られていることを確認する ２．第三者提供に係る記録を作成する
1.3.4 個人情報の保管	22 条（データ内容の正確性の確保等）	• 利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない（再掲）
1.4 個人情報の取扱いの委託	25 条（委託先の監督）	• 個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない
1.5.1 開示、訂正、利用停止請求	32 条（保有個人データに関する事項の公表等）	• 保有個人データについて、下記１～５の情報を本人の知り得る状態に置かなければならない １．個人情報取扱事業者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名 ２．全ての保有個人データの利用目的 ３．保有個人データの利用目的の通知の求め又は開示等の請求に応じる手続、手数料の額 ４．保有個人データの安全管理のために講じた措置 ５．保有個人データの取扱いに関する苦情の申出先（認定個人情報保護団体の対象事業者である場合には、同団体の連絡先を含む）

参考となり得る留意事項の目次（※）	私立学校が参照すべき個人情報保護法上の主な規律	
	33 条~39 条（開示~事前の請求）	• 本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの電磁的記録の提供による方法その他の個人情報保護委員会規則で定める方法による開示を請求することができる • 本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの内容が事実でないときは、当該保有個人データの内容の訂正、追加又は削除を請求することができる • 本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データが第十八条若しくは第十九条の規定に違反して取り扱われているとき、又は第二十条の規定に違反して取得されたものであるときは、当該保有個人データの利用の停止又は消去を請求することができる
1.5.3 苦情処理、漏えい・滅失・毀損した際の対応	26 条（漏えい等の報告等）	• 取り扱う個人データの漏えい、滅失、毀損その他の個人データ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ものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。また、本人に対し、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を通知しなければならない ※公立学校と私立学校では、個人情報保護委員会への報告対象となる事態が異なる
	40 条（個人情報取扱事業者による苦情の処理）	• 個人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なければならない
3.2 個人情報保護法の観点から～安全管理措置～	23 条（安全管理措置）	• 取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない
	24 条（従業者の監督）	• 従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない

※「教育データの利活用に係る留意事項」はあくまで公立学校を対象とした留意点を整理したものであり、私立学校における個人情報の取扱いにそのまま適用されるものではないことに留意