

個人情報保護法ニュース No.23

政令・規則の整備が「中身」の議論へ

— 令和8年9月16日 第369回個人情報保護委員会 公表資料の解説 —

平素より大変お世話になっております。

令和8年7月17日に公布された「個人情報の保護に関する法律等の一部を改正する法律」(令和8年法律第56号。以下「改正法」といいます。)につき、令和8年9月16日に開催された第369回個人情報保護委員会において、政令・委員会規則で定める事項の「基本的な考え方(案)」が初めて示されました。あわせて、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)の別添「講ずべき安全管理措置の内容」の見直しの方向性も公表されています。

改正法の細目の多くは政令・委員会規則・ガイドラインに委ねられており、実務対応の内容はこれらの下位法令によって定まります。その意味で、9月16日の公表資料は、改正法の施行準備において最も重要な一次資料の一つです。

本号(No.23)では、同日公表された資料1「政令・規則の整備に向けた基本的な考え方(案)について」、参考資料1「読替表」および資料2「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)等における安全管理措置の手法の例示の追加等の検討について」の内容を、条文に即して解説いたします。なお、改正法の全改正項目については、ニュースレター(No.22)においてご報告しております。

とりわけご留意いただきたいのは、資料2に示された安全管理措置ガイドライン別添の見直しは、令和9年4月施行という、改正法本体の施行より1年以上早いスケジュールで進む点です。本号が実務対応の一助となれば幸いです。

【本号の要点】

- ① 政令・規則には、法律が定めた枠を超える内容を定める余地がない。事務局は例外事由を3つの型(自明性／公の利益／準ずるもの)に整理し、いずれについても枠を明示している。
- ② 顔特徴データは、周知事項が法律上5類型定められ、周知方法までが規則事項とされた。現在の掲示のままで足りる事業者は多くない。
- ③ 安全管理措置ガイドライン別添の見直しは令和9年4月施行。改正法本体より1年以上早く、準備期間は実質半年である。

令和8年9月
弁護士法人三宅法律事務所

* 本ニュースレターに関するご質問・ご相談がありましたら、下記にご連絡ください。

弁護士法人三宅法律事務所

弁護士 渡邊雅之(執筆者)

TEL 03-5288-1021 FAX 03-5288-1025

Email: m-watanabe@miyake.gr.jp

政令・規則の整備が「中身」の議論へ
— 令和8年9月16日 第369回個人情報保護委員会 公表資料の解説 —

【目次】

- 1 はじめに——政令・規則の検討が「中身」の段階へ
- 2 検討プロセスの現在地——令和8年8月26日・9月9日・9月16日
- 3 今回の検討項目と公表資料の構成
- 4 「基本的な考え方」の読み方——例外事由の3類型
- 5 本人の意思に反しないことが明らかな取扱い(第18条第3項第7号、第20条第2項第7号、第27条第1項第8号)
- 6 子供の個人情報の取扱いに関する規律(第35条第9項・第10項、第40条の2、第58条の3)
- 7 顔特徴データ等に関する規律(第16条第5項、第21条の2、第35条第7項)
- 8 安全管理措置に係るガイドライン別添の見直し(資料2)
- 9 実務への示唆——何を、いつまでに
- 10 参考:安全管理措置に関する社内規程の規定例
- 11 おわりに

【一目でわかる】今回の3資料と自社への当たり所

公表資料	論点	影響を受ける主な業務	決まる文書	効き始める時期
資料1 1-①	本人の意思に反しない取扱い	第三者提供全般／決済・予約・送金／越境移転／要配慮個人情報の取得	規則+GL	令和10年(本体施行)
資料1 2-①	子供の個人情報	会員サービス／教育・BtoC／広告データ連携／統計作成等特例	政令・規則+GL	令和10年(本体施行)
資料1 2-②	顔特徴データ等	入退室管理／店舗カメラ／本人認証／施設の受付	政令・規則+GL	令和10年(本体施行)
資料2	安全管理措置 GL 別添	情報システム全般／クラウド／認証基盤／インシデント対応	ガイドライン	令和9年4月(最優先)

※ 時間軸が最も短いのは資料2である。改正法対応に先行して着手する必要がある。

1 はじめに——政令・規則の検討が「中身」の段階へ

令和8年9月16日、第369回個人情報保護委員会が開催され、改正法の施行に向けた政令・委員会規則(以下「規則」という。)の整備について、初めて具体的な内容の議論が行われた。公表された資料は次の3点である。

資料	表題	内容
資料1	個人情報の保護に関する法律等の一部を改正する法律 政令・規則の整備に向けた基本的な考え方(案)について(適正なデータ利活用の推進、リスクに適切に対応した規律)	3項目について、政令・規則で定め得る範囲の考え方と論点を提示
参考資料1	個人情報の保護に関する法律 読替表(16歳未満の者の個人情報等の取扱いの規定関係)	第40条の2等による読替えの全体を条文単位で提示
資料2	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)等における安全管理措置の手法の例示の追加等の検討について	通則ガイドライン別添の現代化。ゼロトラスト・横展開対策等

これまで公表されてきた委員会資料は、いずれも「どこで決めるか」「どう決めるか」という手続面のものであった。これに対し本資料は、政令・規則に何をどこまで書き得るのかという実体面に踏み込んだ初めての資料である。いずれも「案」の段階であり、今後の意見交換会・事務局ヒアリングおよび意見公募手続(パブリックコメント)を経て変更され得るが、事務局の考え方の骨格は本資料から読み取ることができる。

出典は、個人情報保護委員会ウェブサイトの委員会開催状況(令和8年9月16日・第369回委員会。
<https://www.ppc.go.jp/aboutus/minutes/2026/20260916/>)である。

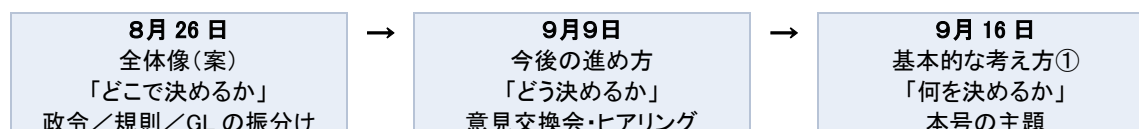
2 検討プロセスの現在地——令和8年8月26日・9月9日・9月16日

改正法の公布後、個人情報保護委員会からは資料が相次いで公表されている。本号の位置付けを明確にするため、まず時系列を整理する。

日付	委員会・事務局の動き	内容
令和8年7月10日	改正法成立(7月17日公布・法律第56号)	本体施行は令和10年7月16日までの政令指定日。罰則関係等の一部は令和9年1月17日

令和8年7月31日	「改正法の成立を受けた個人情報保護委員会の今後の取組(案)」	政令・規則・ガイドライン整備の大枠
令和8年8月19日	オプトアウト届出事業者に対する実態調査の結果および注意喚起	提供先の確認・記録・周知の実態と、求められる対応
令和8年8月26日	「政令・規則等で定める事項の全体像(案)」および「今後の進め方」(第366回委員会決定)	4分類12テーマごとに、政令・規則・ガイドラインの振り分けを提示
令和8年9月9日	「意見交換会・事務局ヒアリングの概要(案)」	マルチステークホルダー連携プロセスと当面のスケジュール
令和8年9月16日	「政令・規則の整備に向けた基本的な考え方(案)」および安全管理措置ガイドライン別添の見直し(第369回委員会)	本号の主題。基本的な考え方の第1回と、資料2

整理すれば、3つの資料は次の関係にある。



【図解】基本的な考え方の議論スケジュール(9月9日資料)

時期	議題	対象テーマ	本号での解説
9月中旬	基本的な考え方①	子供／顔特徴データ／本人関与に関する規律	◎ 第5節～第7節
9月下旬～10月上旬	基本的な考え方②	統計作成等／委託先／漏えい等	—(次回以降)
10月中旬	基本的な考え方③	連絡可能個人関連情報／オプトアウト／課徴金	—(次回以降)
10月中旬～下旬	事務局ヒアリング	上記①～③を踏まえて実施	—
11月～12月	委員会・意見交換会を随時開催	具体的内容の議論	—
令和9年1月～	意見公募手続(パブリックコメント)	政令・規則の条文案	—

なお、9月9日資料に示された当面のスケジュールによれば、基本的な考え方の議論は、9月中旬に子供・顔特徴データ・本人関与に関する規律、9月下旬から10月上旬に統計作成等・委託先・漏えい等、10月中旬に連絡可能個人関連情報・オプトアウト・課徴金が予定されている。今回の3項目は、このうち9月中旬の回に当たる。10月中旬から下旬に事務局ヒアリングが実施され、意見公募手続は令和9年1月以降の見込みである。

3 今回の検討項目と公表資料の構成

資料1は、改正法の4分類(適正なデータ利活用の推進、リスクに適切に対応した規律、不適正利用等防止、規律遵守の実効性確保のための規律)のうち、まず次の3項目について政令・規則の基本的考え方を検討するものである。他の項目やガイドライン等については、今後の委員会において順次検討するとされている。

分類	テーマ	主な委任規定
適正なデータ利活用の推進	目的外利用、要配慮個人情報取得及び第三者提供に関する規律(取得の状況からみて本人の意思に反しないため本人の権利利益を害しないことが明らかな取扱い等)	第18条第3項第7号、第20条第2項第7号、第27条第1項第8号(規則)
リスクに適切に対応した規律	子供の個人情報の取扱いに関する規律	第35条第9項第8号・第9号(規則)、同項第12号(政令)
リスクに適切に対応した規律	顔特徴データ等に関する規律	第16条第5項、第21条の2第2項第4号、第35条第7項第10号(政令)／第21条の2第1項柱書・同項第6号、第35条第7項第9号(規則)

統計作成等の特例、委託先における取扱い、漏えい等報告・本人通知の緩和、連絡可能個人関連情報、オプトアウト制度の強化、課徴金といった項目は、いずれも今回の検討対象に含まれていない。これらを重点論点とする事業者においては、次回以降の委員会資料を待つこととなるが、その分、社内における論点整理を先行させる時間があるともいえる。

4 「基本的な考え方」の読み方——例外事由の3類型

資料1を通読すると、事務局が例外事由を3つの型に整理し、それぞれについて規則・政令で定め得る範囲に明確な枠を設けていることが分かる。この構造を先に把握しておく、各論の理解が容易になる。

型A 自明性で絞る	型B 公の利益で絞る	型C 準ずるもので絞る
【枠】本人(子供の場合は法定代理人)が同意する意思を有しており、又は同意すべき立場にあり、本人にとって不測の権利利益の侵害をもたらさないことが自明である場合に限られる 【該当規定】 第18条第3項第7号 第20条第2項第7号 第27条第1項第8号 第35条第9項第8号 第35条第7項第9号	【枠】知る権利や公共の安全等の公の利益のために情報を公開することが想定される主体(法律上列举された公的機関や報道機関等に準じる主体)に限られる 【該当規定】 第35条第9項第9号 (cf. 現行規則第6条)	【枠】今後の技術進展等に機動的に対応するための例外事由であり、法律上列举された類型に準じる場合に限られる(政令のバスケット条項) 【該当規定】 第35条第9項第12号 第21条の2第2項第4号 第35条第7項第10号

いずれの型も、法律が既に定めた例外の延長線上でしか規則・政令を定め得ない構造となっている。実務上は、「規則で柔軟に手当てされるはずである」という前提に立った設計は避けるべきであり、むしろ規則は狭く、かつ具体的に定められることを想定して準備を進めることが相当である。

この点は、衆参両院の附帯決議(各第7項)が、同意不要の特例について「必要最小限」とすること、および規則によって「具体的な範囲や判断基準を明記すること」を求めていること(参議院決議はこれに加えて「恣意的な判断や濫用を防止すること」を明記する)とも整合する。

【ポイント】

- ・規則は「狭く・具体的に」定められる可能性が高い。広い包括条項を期待した設計は避ける。
- ・規則が定められた後も、自社の場面が類型に当たるかの個別判断と記録は必要である。

5 本人の意思に反しないことが明らかな取扱い(第18条第3項第7号、第20条第2項第7号、第27条第1項第8号)

(1) 本人の同意が必要とされる3場面

本項目を理解する前提として、個人情報保護法において本人の同意が必要とされる場面を確認しておく。次の3場面である。

場面	現行条文	改正により新設される号
① 目的外利用	第18条第3項	第18条第3項第7号
② 要配慮個人情報の取得	第20条第2項	第20条第2項第7号
③ 第三者提供	第27条第1項	第27条第1項第8号

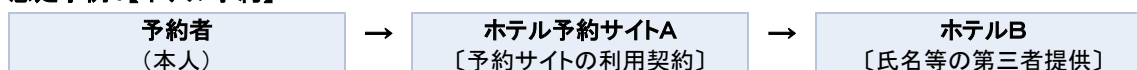
①は、あらかじめ特定した利用目的の達成に必要な範囲を超えて個人情報を取り扱う場面である。②は、信仰・病歴・犯罪歴など差別につながり得る情報を取得する場面である。③は、個人データを第三者に提供する場面であり、外国にある第三者に対する提供を含む。現行規定では、この3場面はいずれも、例外規定に該当する場合を除き本人の同意が必要とされている。

本項目の改正は、この3場面すべてに共通して、新たな例外を設けるものである。第三者提供のみの問題ではない点に留意を要する。

(2) 現行法の隘路——事務局が示す2つの想定事例

事務局は、形式的な同意取得を求めることに実質的な意味が乏しい場面として、2つの事例を挙げている。

想定事例1【ホテル予約】



想定事例2【海外送金】



事務局は、このような場合に行われる個人データの第三者提供は、契約の履行のために不可欠なものであり、本人の意思に反しないため本人の権利利益を害しないことが明らかといえると整理する。それにもかかわらず、現行規定では本人から同意を取得する必要がある。この点を改めるのが本改正である。

(3) 改正後の構造——法律に定めた①と、規則に委ねた②

改正後は、前記3場面のいずれについても、次のいずれかに該当する場合には、あらかじめ本人の同意を得ないで実施することができる。

① 法律に直接規定	② 規則で定める場合【今回の委任事項】
本人との間の契約の履行のために必要やむを得ないことが明らかである場合 → 前記2つの想定事例がこれに当たる ※「必要やむを得ない」＝必要性があり、かつ他の手段によっては契約の目的を達成することができない場合	取得の状況からみて本人の意思に反しないため本人の権利利益を害しないことが明らかである場合として個人情報保護委員会規則で定める場合 → 具体的内容が今回の論点（後記(5)）

なお、①の「必要やむを得ない」の意義について、政府は、必要性があり、かつ、他の手段によっては契約の目的を達成することができない場合であるとし、その旨を個人情報保護委員会においてガイドライン等で明確にしていくものと承知している旨を答弁している（令和8年4月21日 衆議院本会議・松本尚国務大臣）。

また、本人が16歳未満の場合には、第40条の2第1項により「取得の状況からみて本人の権利利益を害しないことが明らかである場合として個人情報保護委員会規則で定める場合」と読み替えられる（後記6(4)参照）。

(4) 規則で定め得る範囲の上限——「自明性」の枠

事務局は、規則で定め得る範囲について、次の考え方を示している。すなわち、第18条第3項第7号、第20条第2項第7号および第27条第1項第8号は、本人が個人データの第三者提供等に同意する意思を有しており、又は同意すべき立場にあり、本人にとって不測の権利利益の侵害をもたらさないことが自明である場合に限り、本人同意を不要とするものである。

そして、「本人との間の契約の履行のために必要やむを得ないことが明らかである場合」は、その自明である場合の典型例として法律で直接定められたものであり、したがって規則で定め本人同意を不要とできるのも、上記の範囲に限られる、とされている。

【判断の起点は「本人の側」にある】

- 本人から見て同意するのが当然といえるか（積極的な評価）
- × 事業者側の利便性・効率性、同意取得の負担、同意率が低い見込み
- × 本人が拒否しないであろうという消極的な評価

実務上の含意は次の3点である。第一に、事業者側の利便性や効率性は理由とならず、判断の起点は本人の側から見て同意するのが当然といえるか否かにある。第二に、本人が拒否しないであろうという消極的な評価では足りず、同意する意思を有している、又は同意すべき立場にあるという積極的な評価を要する。第三に、規則の公表後も、自社の具体的場面が規則の類型に当たるかを個別に判断し、その判断過程を記録することが求められる。規則に定められたことにより自動的に適法となるものではない。

(5) 論点1——規則で追加が検討されている2類型

法律が対象としているのは、①事業者と本人との間の契約であり、かつ②その履行のために必要やむを得ない場合のみである。事務局は、これに加えて、次の2類型を規則において追加的に規定すべきではないかとして、論点を提示している。

類型	内容	事務局が挙げる例
① 事業者と第三者との契約の履行	事業者と第三者（＝本人以外）の契約であって、状況からみて本人の意思に反しないため本人の権利利益を害しないことが明らかなものの履行のために必要やむを得ないことが明らかである場合	本人の家族が、ホテル予約サイトでホテルでの当該家族及び本人の宿泊予約を行ったため、予約サイトAからホテルBに対して当該本人の氏名等が提供される場合

② 契約の締結に先立つ提供	事業者・本人間での契約の締結に先立って、本人の要望に応じて行う提供であって、必要やむを得ないことが明らかである場合	本人が、ECサイトでの商品購入契約の締結に先立ちクレジットカード払いを要望したため、いわゆる3Dセキュア(本人認証手法)の枠組みにより、ECサイト運営事業者Aからクレジットカード会社B等に対して本人の情報が提供される場合
---------------	---	--

①は契約の「当事者」を、②は契約の「時点」を、それぞれ一段拡張するものと整理できる。なお、本人が16歳未満の子供である場合についても、上記と同様の場合を本例外の対象となるように規則で規定してはどうか、との論点が併せて提示されている(論点2)。

(6) 実務への影響

①の類型は、家族・同行者・被扶養者など、契約の当事者ではないが契約の目的に不可欠な本人の情報を扱う場面に広く及び得る。旅行・宿泊、航空・鉄道の団体予約、保険の被保険者、法人契約における従業員、家族カード等が典型である。もっとも、事務局が示した枠は、本人の意思に反しないため権利利益を害しないことが明らかなものの履行に限られており、契約が存在することのみをもって足りるものではない。

②の類型は、決済の与信照会、本人認証、eKYC、審査、見積り、在庫引当て等、契約成立前に外部へ情報を提供する場面に及び得る。ここでも枠は「本人の要望に応じて」「必要やむを得ないことが明らかである」場合であり、事業者側の判断で先回りして提供する場面は含まれにくい。

実務対応としては、自社の第三者提供等について、法律上の①に当たるもの、規則の②に当たり得るもの、いずれにも当たらないものに仕分けておくことが有益である。規則案の公表後に当てはめを開始したのでは、対応が間に合わないおそれがある。

(7) 現行実務および諸外国法制との関係

本項目は、これまで「黙示の同意」の解釈により処理されてきた領域を、法律上の例外として明文化する側面を有する。通則ガイドライン 3-3-2 は、個人情報取扱事業者が要配慮個人情報を書面又は口頭等により本人から適正に直接取得する場合、本人が当該情報を提供したことをもって、当該事業者が当該情報を取得することについて本人の同意があったものと解されるとする。また、ガイドラインに関する Q&A 7-13 は、提供する個人データの項目や提供の態様によっては、本人の同意があると事実上推認してよい場合もあると解されるとしている。

もっとも、従前の黙示の同意の解釈がそのまま規則の類型に置き換わるものではなく、規則の類型に当たるかは別途判断を要する。

諸外国法制との関係では、GDPR 第 49 条第 1 項(b)が、データ主体と管理者との間の契約の履行のために必要な場合、又はデータ主体の要求に基づき契約締結前の措置を実施するために必要な場合を越境移転の例外とし、同項(c)が、管理者と他の自然人若しくは法人との間で締結されるデータ主体の利益のために帰する契約の履行に必要な場合を挙げている。前記の類型①②は、これらに近い発想である。もっとも、日本法の例外は越境移転に限られず、国内の第三者提供・目的外利用・要配慮個人情報の取得にも及ぶ点で、適用範囲は GDPR 第 49 条より広い。

なお、事務局は、本規定により外国にある第三者への個人データの提供も本人同意なく実施可能である旨を明記している。第 28 条に基づく同意も、本例外に該当する場合には不要となり得る点に留意を要する。

6 子供の個人情報の取扱いに関する規律(第 35 条第 9 項・第 10 項、第 40 条の 2、第 58 条の 3)

(1) 現行規定はガイドライン・Q&Aのみ

事務局資料は、現行規定では、子供の個人情報の取扱い等に係る事業者の義務については、ガイドラインや Q&A における記載のみである旨を明記する。すなわち、法律本体、政令、規則およびガイドライン本体のいずれにも、未成年者や子供の個人情報の取扱いに関する規定は置かれていない。

通則ガイドラインは、個人情報の取扱いに関して同意したことによって生ずる結果を未成年者が判断できる能力を有していないなどの場合は、親権者や法定代理人等から同意を得る必要があるとする。また、ガイドラインに関する Q&A(Q1-62)は、個別具体的に判断されるべきであるが、一般的には、12 歳から 15 歳までの年齢以下の子供の場合には法定代理人等から同意を得る必要があるとする。

立法の理由として、事務局は、子供は心身が発達段階にあるためその判断能力が不十分であり、個人情報の不適切な取扱いに伴う悪影響を受けやすいことを挙げる。また、年齢基準を 16 歳未満とした根拠として、Q&A(Q1-62)および欧州の一般データ保護規則(GDPR)第 8 条を明示している。

実務上は、12 歳から 15 歳という幅のある運用が、16 歳未満という単一の基準に置き換わることとなる。13 歳あるいは 15 歳を基準としていた事業者においては、基準の見直しが必要となる。

(2) 改正の3つの柱

① 読替規定(第 40 条の2)	② 利用停止等請求(第 35 条第9 項・第 10 項)	③ 責務規定(第 58 条の3)
同意取得や通知等の対象を、本人から法定代理人へ読み替える 【例外】 (a)16 歳未満であることを知らないことについて正当な理由がある場合 (b)法定代理人が許可した本人の営業に関して個人情報を取得した場合 (c)法定代理人がない又はそのように信ずるに足る相当な理由がある場合	16 歳未満の本人及びその法定代理人は、当該本人が識別される保有個人データが取り扱われているときは、利用停止等又は第三者への提供の停止を請求できる 違法行為の有無等を問わない 法律上 11 類型の例外+政令で定める場合(第 12 号)	【第1項・事業者】当該未成年者の年齢及び発達の程度に応じて、その最善の利益を優先して考慮した上で、未成年者の権利利益を害することのないように必要な措置を講ずるよう努めなければならない 【第2項・法定代理人】子供本人の最善の利益を優先して考慮しなければならない

責務規定が事業者と法定代理人の二層構造となっている点に留意を要する。法定代理人にも最善の利益の考慮義務が課される。なお、法定代理人の関与および責務規定については、行政機関等についても同様の改正が行われる。

(3) 参考資料1(読替表)が示す影響範囲

参考資料1は、第 40 条の2等による読替えの全体を条文単位で示したものである。読替えの対象条文を列举すると、影響範囲の広さが明らかとなる。

根拠	読替えの対象条文
第 40 条の2第1項	第 18 条(目的外利用)／第 20 条第2項(要配慮個人情報の取得)／第 21 条(取得に際しての利用目的の通知等)／第 21 条の2第1項(特定生体個人情報の周知)／第 26 条第2項(漏えい等の本人通知)／第 27 条(第三者提供・オプトアウト・提供先確認)／第 28 条(外国にある第三者への提供)／第 30 条の2第1項及び第5項(統計作成等の特例)／第 32 条第1項(保有個人データに関する事項の公表等)／第 35 条第7項(特定生体個人情報の利用停止等請求)
第 40 条の2第2項	第 31 条第1項(個人関連情報の第三者提供の制限等)
第 71 条の3	第 62 条(利用目的の明示)／第 68 条第2項(漏えい等の報告等)／第 69 条第2項(利用及び提供の制限)／第 71 条(外国にある第三者への提供の制限)(いずれも行政機関等)

読替えは同意の場面に限られず、通知、公表、オプトアウト、越境移転、さらには統計作成等の特例にも及ぶ。とりわけ、第 30 条の2が読替えの対象とされている点は見落とされやすい。子供の公開要配慮個人情報を統計作成等の特例により取得する場合、同意の基準は法定代理人となる。ウェブ上の公開情報を収集してAI開発を行う事業者においては、留意を要する。

(4) 読替えにより文言が変わる箇所

読替えは、「本人」を「本人の法定代理人」に置き換えるのみではない。文言自体が変わる箇所があり、実務上はここで判断を誤りやすい。

条文	読替前	読替後
第 18 条第3項第7号等	取得の状況からみて本人の意思に反しないため本人の権利利益を害しないことが明らかである場合	「本人の意思に反しないため」が落ち、取得の状況からみて本人の権利利益を害しないことが明らかである場合となる
第 20 条第2項第9号	当該要配慮個人情報が本人、国の機関等により公開されている場合	公開主体の「本人」が「本人の法定代理人」に置き換わる
第 27 条第2項第6号・第7号	本人の求めに応じて提供を停止／本人の求めを受け付ける方法	「本人又はその法定代理人」の求めとなる(本人自身の求めも残る)
第 27 条第7項ただし書	取得の時点において本人等により公開されていたものである場合	公開主体の「本人」が「本人の法定代理人」となる
第 32 条第1項	本人の知り得る状態に置く	本人の法定代理人の知り得る状態に置く

【見落としやすい3点】

- ① 第 18 条第3項第7号等は、子供の場合「本人の意思に反しないため」の要素が落ち、判断が客観化される。
- ② 子供自身がSNS等で公開した要配慮個人情報、公開情報に係る例外(第 20 条第2項第9号)に乗らない。
- ③ 統計作成等の特例(第 30 条の2)も読替えの対象。ウェブ公開情報を収集するAI開発でも法定代理人が基準となる。

とりわけ第 18 条第3項第7号等については、子供の場合、判断の基準が「本人の意思」ではなくなり、客観的な権利利益の評価となる。前記 5(4)の「自明性」の当てはめ方が、子供の場合には一段変わることとなる。また、第 20 条第2項第9号の読替えにより、子供自身がSNS等で公開した要配慮個人情報は、公開情報に係る例外に乗らないこととなる。

(5) 利用停止等請求の例外——法律上 11 類型+政令

第 35 条第9項は 12 の例外を定める。主要なものは次のとおりである。

号	例外事由	委任
第1号	法定代理人の同意を得て取得した場合	—
第3号	人の生命・身体・財産の保護のために必要な場合	—
第8号	子供本人との間の契約の履行のために必要やむを得ないことが明らかである場合その他、取得の状況からみて子供本人の権利利益を害しないことが明らかである場合	規則
第9号	法定代理人や公的機関、報道機関等その他の者により公開されていたものである場合	規則(公開主体)
第11号	本人が 16 歳以上であると信じさせるために詐術を用いた場合	—
第12号	その他前各号に掲げる場合に準ずる場合	政令

このほか、法令に基づく場合(第2号)、公衆衛生の向上又は児童の健全な育成の推進(第4号)、国の機関等への協力(第5号)、学術研究(第6号・第7号)、法定代理人が許可した営業(第 10 号)が定められている。規則・政令に委ねられているのは、第8号・第9号・第 12 号の3つである。

実務上とくに留意を要するのは、第 11 号として「詐術を用いた場合」が法律上の例外に置かれている点である。年齢確認の設計と直結する規定である。

(6) 規則・政令で定め得る範囲

事務局は、前記3号について、それぞれ次の枠を示している。前記 4 の3類型がそのまま当てはまる。

- 第8号(規則・型A)——第 20 条第2項第7号に相当する読替後の規定に倣った例外事由であり、規則で定め得るのは、子供本人の法定代理人が保有個人データの取扱いに同意する意思を有しており、又は同意すべき立場にあり、本人に不測の権利利益の侵害をもたらさないことが自明である場合に限られる。
- 第9号(規則・型B)——第 20 条第2項第9号(現行法第 20 条第2項第7号)に倣った例外事由であり、規則で定め得るのは、知る権利や公共の安全等の公の利益のために情報を公開することが想定される主体(法律上列举された公的機関や報道機関等に準じる主体)に限られる。なお、現行規則第6条は、(a)外国政府、外国の政府機関、外国の地方公共団体又は国際機関、(b)外国において学術研究機関等に相当する者、(c)外国において第 57 条第1項各号に掲げる者に相当する者を定めており、事務局はこれを規定することでよいかと問いかけている。
- 第 12 号(政令・型C)——今後の技術進展等に機動的に対応するための例外事由であり、政令で定め得るのは、法律上の 11 類型(第1号から第 11 号まで)に準じる場合に限られる。

事務局は、法律上の 11 類型には現行法第 20 条第2項各号に倣った例外事由が含まれていることを前提に、これに加えて規定すべき場合が何か想定されるかを問いかけている(論点3)。事業者側から具体例を示す余地がある部分である。

(7) 実務対応

第一に、年齢基準の見直しである。13 歳・15 歳など独自の基準を設けていたサービスは 16 歳未満に統一し、年齢を把握していないサービスについては、把握するか、16 歳未満の利用を想定しない設計に振り分けることとなる。

第二に、本人関与の窓口の再設計である。同意取得画面、利用目的の通知・公表、開示等請求、利用停止等請求、オプトアウトの受付のいずれもが法定代理人対応となる。もっとも、第 27 条第 2 項の求めは「本人又はその法定代理人」であり、本人自身の求めも残るため、窓口では双方を受け付ける必要がある。

第三に、見落とされやすい領域への対応である。統計作成等の特例によるウェブ公開情報の取得、個人関連情報の提供(第 31 条第 1 項)における提供先での同意確認、外国にある第三者への提供(第 28 条)は、いずれも法定代理人が基準となる。広告・データ連携の契約条項にも影響する。

第四に、第 58 条の 3 への備えである。年齢及び発達 の程度に応じた配慮が努力義務とされることから、推薦アルゴリズム、課金設計、利用時間の設計等について、判断過程を記録に残す運用を開始することが望まれる。

7 顔特徴データ等に関する規律(第 16 条第 5 項、第 21 条の 2、第 35 条第 7 項)

(1) 現行規定の何が問題とされたか

事務局は、現行規定では、原則として個人情報の利用目的を自社のホームページに掲載する等して公表することにより、生体データとしての個人識別符号に該当するもの(顔特徴データを含む)も含め、事業者は個人情報を取得することが可能である旨を指摘する。令和 5 年の「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」において揭示例等が公表され、Q & A にも一定の記載があるが、いずれも法令上の義務ではない。

他方、顔特徴データ等は、(a)本人が関知しないうちに容易に、それゆえに大量に入手可能であり、(b)一意性及び不変性が高く特定の個人を識別する効果が半永久的に継続するため、取扱いが本人のプライバシー等の侵害につながる可能性があると考えられる。さらに、カメラ等の計測機器を複数の地点に設置して顔特徴データ等を入手し、これを名寄せに利用することで、本人が関知し得ないまま行動を追跡することも可能である。

そのうえで事務局は、顔特徴データ等の適正な利活用を促すため、透明性を確保した上で本人関与の強化が必要ではないか、と問題を設定している。利活用の抑制ではなく、利活用を可能とするための透明性確保という立て方である点に留意を要する。

(2) 定義(第 16 条第 5 項)と政令委任の構造

特定生体個人情報とは、特定生体個人識別符号が含まれる個人情報をいう。特定生体個人識別符号とは、個人識別符号のうち、次の 2 要件を満たす身体的特徴に係る情報として政令で定めるものを変換したものである。

- ① 特別の技術又は多額の費用を要しない方法により取得することができること
- ② 取得されていることを本人が容易に認識することができないこと

事務局は、特定生体個人情報に係る規律は、顔特徴データ等が上記の性質を有するため、その他の生体データに比べて本人のプライバシー等の侵害に類型的につながりやすいという特徴を有することとなっているとし、したがって第 16 条第 5 項の政令において規律の対象とできるのは、法定された性質等を踏まえ、個人識別符号に該当する生体データのうち上記性質を有するものに限られるとする。

そのうえで、改正法第 2 条第 2 項第 1 号に該当するものとして政令で定める生体データのうち、顔特徴データ(現行の施行令第 1 条第 1 項口「顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状によって定まる容貌」)を対象としてはどうか、との論点が提示されている(論点 1)。また、現段階において、この他に法定された性質を有し規律対象とすべきものがあるかが問われている。

(3) なぜ顔特徴データのみか——動向調査の 2 軸

事務局は、根拠として「生体データの利用に関する動向調査 最終報告書」(令和 7 年 12 月。個人情報保護委員会ウェブサイト「調査等」において公表)を示している。同調査は、①取得に要する費用等、②本人の関知なく取得される可能性の 2 軸で評価しており、その結果は次のとおりである。

生体データ	① 取得に要する費用等	② 本人の関知なく取得される可能性	規律対象の候補
顔特徴データ	A: 制約が非常に少ない	A: 非常に高い	◎ 両要件を満たす
歩容データ	C: 制約が多い	A: 非常に高い	△ ①を満たさない
声紋データ	B: 制約が少ない	B: 高い	△ ②が一段落ちる
虹彩データ	B: 制約が少ない	C: 低い	× ②を満たさない
静脈・指紋・掌紋データ	B: 制約が少ない	C: 低い	× ②を満たさない
DNA	C: 制約が多い	D: 非常に低い	× いずれも満たさない

※ ①②の評価は同報告書による。「規律対象の候補」欄は本ニュースレターによる整理である。

両軸ともにAと評価されているのは顔特徴データのみである。もっとも、歩容データは②がA、声紋データは②がBと評価されており、技術の進展により取得コストが低下した場合には、将来的に規律の対象に加えられる可能性が残る。音声による本人認証や歩容分析を利用する事業者においては、今後の動向に留意が必要である。

(4) 周知義務(第21条の2)

特定生体個人情報を取り扱うに当たっては、次の事項について、規則で定めるところにより、あらかじめ本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

区分	内容
法律上の5類型 (第1項第1号～第5号)	① 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 特定生体個人情報を取り扱うこと ③ 特定生体個人情報の利用目的 ④ 特定生体個人識別符号に変換される身体の一部の特徴に係る情報 ⑤ 開示等の請求等に応じる手続(手数料の額を含む)
規則委任事項	・その他個人の権利利益を保護するために必要なものとして規則で定める事項(第1項第6号) ・周知方法(「本人に通知」する方法及び「本人が容易に知り得る状態に置く」方法)(第1項柱書)
例外(第2項各号)	① 本人又は第三者の権利利益を害するおそれがある場合 ② 当該事業者の権利又は正当な利益を害するおそれがある場合 ③ 国の機関等の事務の遂行に協力する必要がある場合 ④ その他前3号に準ずるものとして政令で定める場合

周知事項のみならず、周知方法自体が規則事項とされている点が重要である。揭示の方法が法令により規律されることとなる。事務局は、周知義務の趣旨を、特定生体個人情報の取扱いに係る本人の不安感を緩和し、利用停止等請求権の行使等の適切な対応を図る契機を提供する点にあると整理しており、規則の内容もこの趣旨から導かれる。

(5) 論点2——周知方法および周知事項の方向性

事務局は、周知方法について、カメラやセンサー等の機器の周辺に分かりやすく揭示する等の方法により、検知対象者が十分認識できる場所に分かりやすく揭示することが重要であるとし、第21条の2第1項柱書の規則においては、いかなる手段においても容易に知ることができる周知方法を規定する必要があるとする。

この点、政府は、周知の具体的な方法については十分な透明性を確保する観点から、カメラを設置する施設の入口に周知事項を揭示する等、原則として本人が訪れると想定される場所に揭示することを規定することを想定している旨を答弁している(令和8年6月17日 参議院デジタル社会の形成及び人工知能の活用等に関する特別委員会・松本尚国务大臣)。

周知事項については、第1項第6号の規則において、不安感の緩和に繋がる周知事項や、本人がいかなる対応を取るべきかの検討に資する事項を規定する必要があるとされ、令和5年3月の前記文書およびこれを踏まえたQ&Aで示されている周知方法・周知事項を参考としてはどうかとされている。同文書が示す揭示事項の例は、次のとおりである。

区分	揭示事項の例
施設内での揭示	顔識別機能付きカメラシステムの運用主体／同システムで取り扱われる個人情報の利用目的／問合せ先／WebサイトのURL及びQRコード等
Webサイト等への掲載	導入する必要性／システムの仕組み／取り扱われる個人情報の利用目的／運用基準(登録基準、登録される情報の取得元、誤登録防止措置、保存期間等)／他の事業者への提供(委託、共同利用等)／安全管理措置／開示等の請求の手続、苦情申出先等
揭示の場所・方法	被撮影者の目線や動線を考慮し、人が出入りする際に目に付きやすい出入口(大規模施設で入口が複数ある場合には一定の大規模な入口)に揭示する。デザインやフォントを工夫し、アイコンやイラスト等を活用して分かりやすい方法で揭示する

なお、衆参両院の附帯決議(各第9項)も、同情報が取り扱われている旨および本人からの利用停止請求等の手段について、監視カメラやセンサー等の機器の周辺に分かりやすく揭示する等の方法による周知の徹底を求めており、参議院決議はこれに加えて「当該機器の検知対象者が十分認識できる場所等」を明記している。

(6) 利用停止等請求(第35条第7項)と例外の設計

本人は、当該本人が識別される特定生体個人情報に取り扱われているときは、違法行為等の有無を問わず、利用停

止等又は第三者への提供の停止を請求することができる。例外は法律上9類型および政令で定める場合(第10号)である。

このうち第9号は、契約の履行のために必要やむを得ないことが明らかである場合のほか、特定生体個人識別符号の作成の状況又は特定生体個人情報の取得の状況からみて本人の意思に反しないため本人の権利利益を害しないことが明らかである場合として規則で定める場合である。事務局は、規則で定め得るのは、本人が顔特徴データ等の取扱いに同意する意思を有しており、又は同意すべき立場にあり、本人にとって不測の権利利益の侵害をもたらさないことが自明である場合に限られるとしており、前記5(4)と同一の枠が用いられている。第10号については、政令で定め得るのは法律上の9類型に準じる場合に限られる。

また、特定生体個人情報は、オプトアウト制度に基づく第三者提供の対象から除外される。なお、事務局資料のスライドはこれを「改正法第27条第1項ただし書」と表記しているが、参考資料1の読替表においては第27条第2項ただし書に「要配慮個人情報若しくは特定生体個人情報」と規定されている。条項の表記は、公布された条文により確認されたい。

実務上の課題として、国会審議では、複数の事業者が顔特徴データを同時に取り扱う場合、利用停止請求を望む本人が個々の事業者に対して請求せざるを得ないことが指摘された。政府は、手続が本人にとって過重な負担とならないよう配慮しなければならないとしたうえで、複数の事業者が絡む場合は一元的な窓口を設置するなどを想定して進めていきたい旨を答弁している。商業施設・テナントビル等、複数事業者が関与する場面では、この議論を踏まえた設計が求められる。

(7) 実務対応

【早見】いまの掲示で足りるか

現在よくある掲示	評価	改正後に求められる内容
「防犯カメラ作動中」のみ	×	本人識別を目的とする場合は、第21条の2の5類型(事業者名・住所・代表者の氏名／取り扱う旨／利用目的／変換元の身体的特徴の内容／開示等請求の手続)を掲示する
「顔認証システム使用中」のみ	×	同上。システム名の表示のみでは足りない
利用目的を自社HPにのみ掲載	×	HP掲載に加え、機器の周辺・検知対象者が十分認識できる場所への掲示が求められる方向
入口に掲示(記載事項は5類型を充足)	△	入口のみでは足りない可能性。カメラ・センサーの周辺、動線・視認性を踏まえた掲示を検討する
入口+機器周辺に掲示し、HPに運用基準等を掲載	◎	令和5年3月文書の二層構成(施設内は主体・目的・問合せ先・URL／QR、Webは運用基準・安全管理措置等)に沿う

第一に、用途の仕分けである。本人識別を目的とする装置・ソフトウェアにより本人を識別できるようにしたものであるか否かを基準として、自社が保有するカメラを、防犯、入退室管理、本人認証、マーケティング分析等の別に一覧化する。単なる顔写真や本人識別を目的としない画像(人流・混雑把握等)は、特別規律ではなく通常の個人情報規律に服する。

第二に、掲示の作り直しである。「顔認証使用中」といった掲示のみでは第21条の2の5類型を満たさない。事業者名、住所、代表者の氏名、利用目的、変換元の身体的特徴の内容、開示等の請求等に応じる手続まで示す必要がある。掲示場所も、入口のみならず、カメラやセンサーの周辺、検知対象者が十分認識できる場所を想定する。

第三に、停止請求への対応フローの整備である。違法行為等の有無を問わず請求できるため、適法に運用していることを理由に応じないという対応は成り立たない。9類型の例外に該当するかを個別に判断する運用を要する。また、本人の顔データと保有データの照合が必要となる場面では、照合用データの取得・保管・削除のログを残し、目的外利用を技術的に遮断する設計が必要である。

第四に、契約・調達の見直しである。顔認証システムのベンダー契約に、周知文言・掲示物の提供、停止請求への対応手順、ログの保存を盛り込むほか、複数事業者が関与する施設においては、誰が掲示し誰が窓口となるかを取り決めておくことが望まれる。

8 安全管理措置に係るガイドライン別添の見直し(資料2)

(1) 位置付け——改正法とは別のルートで進む

資料2は、改正法の施行に伴う改正ではなく、現行の通則ガイドライン別添「10(別添)講ずべき安全管理措置の内容」の見直しである。改正法とは別のスケジュールで進む点に留意を要する。

検討の背景として、近年、個人情報取扱事業者及び行政機関等への機密情報等の窃取・破壊等を企図したサイバー

攻撃が一層高度化・複雑化・巧妙化し、攻撃対象も拡大し続けており、個人データ等の漏えい等の大きな要因となっていることが挙げられている。

個人情報保護委員会は、サイバーセキュリティ関係省庁・機関（内閣官房国家サイバー統括室(NCO)、警察庁サイバー警察局、情報処理推進機構(IPA)、情報通信研究機構(NICT)およびJPCERTコーディネーションセンター)との間で、個人情報保護法サイバーセキュリティ連絡会を令和6年12月から四半期ごとに7回開催してきた。令和8年1月には、同連絡会で得られた知見をまとめた「不正アクセス発生時のフォレンジック調査の有効活用に向けた着眼点」が公表されている。

事務局は、別添が平成28年11月の策定当時から内容が大きくは変わっていないことを指摘し、現代化を含めた見直しが必要との考えに至ったとする。別添は、従わなかった場合に法違反と判断される可能性がある「講じなければならない措置」と、当該措置を実践するための例を示した「手法の例示」で構成されており、その改正は実質的な義務水準の見直しを意味する。

(2) 4つの課題と対応の方向性(案)

課題	内容	対応の方向性(案)
① 取扱態様の多様化	クラウドサービスの普及、デバイスの高機能化等により、個人データ等の取扱いの態様が多岐にわたっている	組織体制・技術的措置の手法の例の明確化／クラウドサービスにおける技術的措置の手法の例等の明確化／生体認証・多要素認証の手法の例の明確化
② 境界型モデルの前提	現行の「10-6 技術的安全管理措置」は境界型セキュリティモデルを念頭に置いたものである	ゼロトラストアーキテクチャの考え方を取り入れた手法の例の明確化
③ 侵入後の横展開	侵入型ランサムウェアを代表として、ネットワークの奥深くまで侵入する事案が増えている	侵入された後の横展開対策として講じなければならない技術的措置の手法の例等の明確化
④ 構成の不明確さ	「講じなければならない措置」と「手法の例示」の対応関係・趣旨が明確でない	位置付けの整理・再構成／Q&Aにおける手法の例の別添への一本化

(3) とくに注目される3つの追加

ゼロトラスト	横展開対策	クラウド
組織内・組織外のアクセスを問わず、アクセス要求ごとに動的コンテキストを評価し、リスクに応じてアクセスの可否を判断する ※NIST「Cybersecurity Framework 2.0」等により、同アーキテクチャの考え方が取り込まれていく傾向が確認されたとされる	・特権アカウントの利用等を最小限に限定する ・侵害を受けた又はそのおそれがある情報システムの停止・隔離、アカウントの無効化等により、被害が広がらないようにする ※侵入型ランサムウェア事案を念頭に置いた記述	【利用者側】個人データが記録された電子媒体それ自体を自ら管理しない 【提供者側】サービスとして個人データを取り扱う情報システムに外部の者がアクセスする場合がある →双方を踏まえた技術的措置の手法の例を明確化

- ゼロトラスト——組織内・組織外のアクセスを問わず、アクセス要求ごとに動的コンテキストを評価し、リスクに応じてアクセスの可否を判断すること等を手法の例として示すことが考えられるとされる。事務局は、NIST「Cybersecurity Framework 2.0」(令和6年2月)等により、ゼロトラストアーキテクチャ(組織内外を問わず何も信頼せず、全てを検証するというセキュリティ概念)の考え方が取り込まれていく傾向が確認されたとする。
- 横展開対策——(a)特権アカウントの利用等を最小限に限定すること、(b)侵害を受けた又はそのおそれがある情報システムの停止・隔離、アカウントの無効化等、不正アクセス等が発生した場合でも被害が広がらないよう必要な対策を講ずること、が挙げられている。侵入の防止のみならず、侵入後に被害を拡大させないことが安全管理措置の内容として明記されることとなる。
- クラウドサービス——利用事業者からすると個人データが記録された電子媒体それ自体を自ら管理しないこととなり、提供事業者からするとそのサービスとして個人データを取り扱う情報システムに外部の者がアクセスする場合があることを踏まえ、講じなければならない技術的措置の手法の例等を明確にするとされる。

(4) 構成の再整理

第一に、重複の解消である。現行別添「10-3(2) 個人データの取扱いに係る規律に従った運用」および同「(3) 個人デ

一タの取扱状況を確認する手段の整備」の手法の例示は内容的に重複していると考えられるため、位置付けを整理し再構成するとされる。

第二に、標題と内容の不整合の解消である。現行別添「10-6(3) 外部からの不正アクセス等の防止」の手法の例示では「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」ことなどが示されているが、標題は「防止」であり、その内容は「保護する仕組みを導入し、適切に運用しなければならない」とされている。事務局は、標題および内容から検知という具体的な手法が考えられることを直ちに読み取れないとして、位置付けを整理し再構成するとしている。防止と検知が切り分けられ、ログ分析による検知が独立した措置として整理される可能性がある。

第三に、行政上の対応を行った個別事案の反映である。責任部署の設置、個人データの取扱いに係る規律の明確化と周知、安全管理措置の見直し、従業員の教育の実施方法等の見直しなど、手法の例として考えられるものの示すことができていないものについて、委員会が行政上の対応を行った個別の事案等を踏まえて追記を検討するとされている。

第四に、他のガイドライン等への波及である。別添の内容は、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)、特定個人情報の適正な取扱いに関するガイドライン(事業者編・行政機関等編)その他のガイドライン等で示される安全管理措置の内容と重複しているため、これらについても必要な見直しを検討するとされている。マイナンバーを取り扱う事業者にも影響が及ぶ。

(5) スケジュール——令和9年4月施行

時期	内容	実務上の対応
令和8年9月頃	手法の例示の追加等の方向性の公表	本資料がこれに当たる。現行の技術的安全管理措置と突き合わせる
令和8年11月頃	見直し案の委員会審議	案の内容を確認し、対応が困難な項目を洗い出す
令和8年12月頃	意見公募手続(パブリックコメント)開始	意見提出。業界団体経由を含め、年内に論点を固めておく
令和9年2月頃	パブリックコメントの結果の委員会報告、改正事項の決定	確定内容に基づく対応計画の策定
令和9年4月	改正事項の施行	規程・体制・技術的措置の改定を完了させる

改正法本体の施行は令和10年7月16日までの政令指定日であるのに対し、資料2の改正事項は令和9年4月に施行される。準備期間は実質的に半年程度であり、改正法対応に先行して着手する必要がある。なお、事務局は、上記改正事項の施行後も、情報通信技術の進展等を踏まえて安全管理措置の手法の例示について不断の検討を行いたいとしている。

9 実務への示唆——何を、いつまでに

今回の3資料は、影響する業務、内容を定める文書および時間軸のいずれも異なる。まず自社への当たり所を特定することが出発点となる。

論点	影響を受ける主な業務	内容を定める文書	着手の視点
本人の意思に反しない取扱い	第三者提供全般、決済・予約・送金、越境移転、要配慮個人情報の取得	委員会規則＋ガイドライン	提供フローの棚卸しを先行させる
子供の個人情報	会員サービス、教育・BtoC、広告データ連携、統計作成等特例	政令・規則＋ガイドライン	年齢基準と本人関与の窓口の設計
顔特徴データ等	入退室管理、店舗カメラ、本人認証、施設の受付	政令・規則＋ガイドライン	カメラの棚卸しと掲示の作り直し
安全管理措置ガイドライン別添	情報システム全般、クラウド、認証基盤、インシデント対応	ガイドライン	令和9年4月施行。最優先で着手する

時間軸が最も短いのは資料2である。改正法対応に先行して着手されたい。

【着手チェックリスト】
☐ 第三者提供フローを、(a)法律上の契約履行型、(b)規則で追加され得る2類型、(c)いずれにも当たらないもの、に仕分けた
☐ 要配慮個人情報の取得・目的外利用の場面も、同意例外の検討対象に含めた(第三者提供のみで検討していない)
☐ 16歳未満の利用を想定するサービスを特定し、年齢基準を16歳未満に統一した
☐ 統計作成等特例・個人関連情報の提供・越境移転についても、法定代理人基準となることを確認した
☐ 本人識別を目的とするカメラ・生体認証システムを一覧化した
☐ 現在の掲示物を写真等で記録し、第21条の2の5類型と突き合わせた

☐ 顔特徴データの利用停止等請求に応答するフローと、照合用データの取扱いを定めた
☐ 現行の技術的安全管理措置を、ゼロトラスト・横展開対策・クラウド・多要素認証の4観点で自己点検した
☐ 特権アカウントの棚卸しと、侵害時の停止・隔離手順を文書化した
☐ 資料2のパブリックコメント(令和8年12月頃)に向けて、意見提出の要否と担当を決めた

今後3か月の具体的な対応としては、次のとおりである。

- 令和8年9月から10月——委員会の議論を追いながら棚卸しを進める。自社の重点テーマの回に合わせて社内の論点を整理する。第三者提供フローを、(a)法律上の契約履行型、(b)規則で追加され得る2類型、(c)いずれにも当たらないもの、に仕分ける。カメラ・生体認証の一覧を作成し、本人識別を目的とするものを特定したうえで、現在の掲示物を第21条の2の5類型と突き合わせる。
- 令和8年10月から12月——事務局ヒアリングは10月中旬から下旬に実施される予定である。業界団体を通じた意見提出を検討する場合は、この時期までに主張を固める必要がある。並行して、現行の技術的安全管理措置を、ゼロトラスト・横展開対策・クラウド・多要素認証の4観点で自己点検し、対応が困難な項目を洗い出す。資料2のパブリックコメントは12月頃に開始される見込みである。
- 令和9年1月以降——政令・規則の条文案に対するパブリックコメントが見込まれる。並行して、資料2の改正事項が令和9年2月頃に決定され、4月に施行される。

改正法本体の施行までの間に、少なくとも二度の意見公募手続と一度のガイドライン施行があることとなる。施行までに2年あることを前提とした対応計画は、見直しを要する。

10 参考:安全管理措置に関する社内規程の規定例

資料2で追加が見込まれる「手法の例示」に対応するため、社内規程(個人データ安全管理措置規程、情報セキュリティ規程等)に置くことが考えられる規定例を示す。いずれも案の段階の資料に基づく試案であり、確定したガイドラインの内容および自社のシステム構成・リスク評価に応じて調整されたい。

(1) ゼロトラストの考え方に基づくアクセス制御

(アクセス制御の原則)

第〇条 個人データを取り扱う情報システムへのアクセスは、当該アクセスが社内ネットワークからのものであるか社外からのものであるかを問わず、すべて検証の対象とする。

2 前項の検証は、アクセス要求のつど、次に掲げる事項その他の動的な情報を評価して行うものとする。

- 一 利用者の識別及び認証の状況
- 二 利用する端末の状態(管理対象端末であるか、修正プログラムの適用状況、マルウェア対策の稼働状況等)
- 三 アクセス元のネットワーク及び位置に関する情報
- 四 アクセスの対象となる個人データの種類及び量
- 五 平常時の利用状況との乖離の有無

3 情報システム管理者は、前項の評価の結果に応じ、アクセスの許可、追加認証の要求、機能の限定又はアクセスの拒否を行うものとする。

(権限の最小化及び定期的な見直し)

第〇条 個人データへのアクセス権限は、業務の遂行に必要な最小限の範囲で付与する。

2 情報システム管理者は、少なくとも〇か月に一度、付与されているアクセス権限を棚卸しし、不要となった権限を速やかに削除する。

3 異動、退職又は退職の申請があったときは、〇営業日以内に権限の変更又は削除を行う。

(2) 多要素認証・生体認証

(多要素認証)

第〇条 次に掲げるアクセスについては、知識情報、所持情報及び生体情報のうち二以上の異なる要素を組み合わせた認証(以下「多要素認証」という。)を用いなければならない。

- 一 個人データを取り扱う情報システムへの社外からのアクセス
- 二 特権アカウントによるアクセス
- 三 1,000人を超える本人に係る個人データを一括して出力し、又は複製することができる操作
- 四 クラウドサービスの管理者コンソールへのアクセス

2 多要素認証に生体情報を用いる場合は、当該生体情報の取扱いについて別に定める手続によるものとする。

(3) 特権アカウントの管理と横展開対策

(特権アカウントの管理)

第〇条 特権アカウントは、その利用を必要最小限に限定し、次に掲げる措置を講ずる。

- 一 常時利用可能な特権アカウントを設けず、必要のつど承認を得て一時的に権限を付与すること。
- 二 特権アカウントを個人に紐付け、共有しないこと。
- 三 特権アカウントによる操作のログを取得し、他の利用者が改変できない方法で保存すること。
- 四 特権アカウントの一覧を少なくとも〇か月に一度棚卸しすること。

(被害の拡大防止措置)

第〇条 不正アクセスその他の情報セキュリティ上の事象を検知したときは、被害の拡大を防止するため、速やかに次に掲げる措置を講ずるものとする。

- 一 侵害を受けた又はそのおそれがある情報システム、機器又はネットワークの停止又は隔離
 - 二 侵害されたおそれのあるアカウントの無効化及び認証情報の変更
 - 三 関連するシステム間の通信の遮断又は制限
 - 四 バックアップの保全及び復旧可否の確認
- 2 前項の措置に係る判断の権限者、連絡体制及び実施手順は、別に定めるインシデント対応手順による。
- 3 第1項の措置を講じたときは、その内容、実施時刻及び判断の根拠を記録し、保存する。

(4) ログの取得・分析(検知)

(ログの取得及び分析)

第〇条 個人データを取り扱う情報システムについて、次に掲げるログを取得し、〇年間保存する。

- 一 認証の成否及び認証方式に関するログ
 - 二 個人データの参照、出力、複製、変更及び削除に関するログ
 - 三 特権アカウントによる操作に関するログ
 - 四 外部との通信に関するログ
- 2 情報システム管理者は、前項のログを定期的に分析し、不正アクセス、不正な持出しその他の異常を検知するものとする。
- 3 前項の分析の頻度及び検知の基準は、取り扱う個人データの種類及び量に応じて定める。

現行の通則ガイドライン別添では、ログの分析による「検知」が「10-6(3) 外部からの不正アクセス等の防止」の手法の例示に置かれているが、資料2は、標題及び内容から検知という手法が直ちに読み取れないとして再構成を検討している。社内規程においては、当初から「防止」と「検知」を分けて定めておくことが望ましい。

(5) クラウドサービスの利用

(クラウドサービスの利用)

第〇条 個人データを取り扱うクラウドサービスを利用するときは、利用の開始に先立ち、次に掲げる事項を確認し、記録する。

- 一 当該サービスの提供事業者が個人データを取り扱うこととなるか否か、及びその範囲
 - 二 個人データが保存される国又は地域
 - 三 提供事業者又はその再委託先の事業者によるアクセスの可否及びその管理方法
 - 四 暗号化、鍵の管理主体その他の技術的な保護措置の内容
 - 五 アクセスログの取得の可否、保存期間及び利用者による取得方法
 - 六 契約終了時の個人データの返還又は削除の方法
- 2 管理者コンソールその他の設定を変更したときは、その内容及び変更者を記録し、個人データが外部から参照可能な状態になっていないことを確認する。
- 3 利用するクラウドサービスの一覧(サービス名、利用部署、取り扱う個人データの種類、契約形態を含む。)を作成し、少なくとも〇か月に一度更新する。

なお、いわゆる「クラウド例外」(外部事業者が契約上・運用上、保存された個人データを取り扱わないこととなっている場合には第三者提供にも委託にも当たらないとする整理)による場合には、「取り扱わない」状態が契約及びアクセス制御により確保されていることを、第1項第1号及び第3号の記録により説明できるようにしておくことが必要である。

(6) 自己点検表

観点	確認事項	現状
ゼロトラスト	社内ネットワークからのアクセスを無条件に信頼していないか。アクセス要求ごとの評価が可能な構成となっているか	☐ 対応済 ☐ 一部 ☐ 未着手
多要素認証	社外アクセス・特権操作・クラウド管理者コンソールに多要素認証を適用しているか	☐ 対応済 ☐ 一部 ☐ 未着手
特権アカウント	常時有効な特権アカウントを廃し、必要のつど付与する運用としているか。棚卸しの記録があるか	☐ 対応済 ☐ 一部 ☐ 未着手

横展開対策	侵害時にシステムを停止・隔離し、アカウントを無効化する手順と権限者が定まっているか	☐ 対応済 ☐ 一部 ☐ 未着手
ログの検知	ログを取得するだけでなく、定期的に分析し異常を検知する運用となっているか	☐ 対応済 ☐ 一部 ☐ 未着手
クラウド	利用中のクラウドサービスの一覧と、保存先・アクセス可否・暗号化の記録があるか	☐ 対応済 ☐ 一部 ☐ 未着手

11 おわりに

今回の公表資料から読み取るべき点は、次の3点に整理できる。

第一に、政令・規則には、法律が定めた枠を超える内容を定める余地がないことである。同意不要の例外は「自明である場合」、公開情報に係る例外は「公の利益のために情報を公開することが想定される主体」、政令のバスケット条項は「法律上の類型に準ずる場合」と、事務局は各所において明確に枠を示している。規則により柔軟な手当てがされることを前提とした設計は避けるべきである。

第二に、顔特徴データについては、掲示の見直しが不可避であることである。周知事項が法律上5類型定められたうえ、周知方法までが規則事項とされた。事務局は検知対象者が十分認識できる場所への掲示を重視しており、国会答弁も施設入口への掲示を想定している。現在の掲示のままで足りる事業者は多くないものと思われる。

第三に、安全管理措置ガイドライン別添の見直しが最も早く、令和9年4月に施行されることである。ゼロトラスト、横展開対策、クラウド、多要素認証が「手法の例示」に加えられる。「講じなければならない措置」の周辺が書き換わる以上、監督における評価の基準が変わることを意味する。

本号で取り上げた3資料は、いずれも「案」の段階にある。意見交換会、事務局ヒアリングおよび意見公募手続を経て変更され得るが、裏を返せば、現在は事業者として意見を述べ得る時期にある。パブリックコメントの公表を待つのではなく、委員会における議論の段階から論点を追ひ、必要に応じて業界団体等を通じた意見提出を検討されたい。

なお、本ニュースレターは一般的な情報提供を目的とするものであり、個別の事案への対応については別途ご相談ください。政令・委員会規則・ガイドライン等の最新情報を適宜ご確認ください。

以上