改正個人情報保護法の政令・規則の整備に向けた意見
―「政令・規則の整備に向けた基本的な考え方」に対して―

２０２６年１１月４日
（一社）日本経済団体連合会
デジタルエコノミー推進委員会企画部会
データ利活用戦略ワーキング・グループ

本年７月に成立した「個人情報の保護に関する法律等の一部を改正する法律」の施行に向け、個人情報保護委員会事務局から、政令・規則の整備に向けた基本的な考え方①（2026 年 9 月 16 日）、②（同 10 月 1 日）、③（同 10 月 14 日）が示された。これらについて、下記のとおり意見を述べる。

今回の改正は、AI 開発をはじめとするデータ利活用の推進と、リスクに応じた個人の権利利益の保護との両立を図るものである。政令・規則は、その趣旨が実務で生かされるよう、リスクベースの考え方に立ち、事業者が予見可能性をもって判断できる形で定めるべきである。

なお、政令・規則の検討にあたっては、現段階から具体的なユースケースを想定しておく必要があることから、本意見にはガイドライン・Q&A において示すべき考え方も一部含めている。今後、経団連としても、必要に応じて具体的な事例を提供していく。

記

Ⅰ．基本的な考え方①

1. 適正なデータ利活用の推進

1-①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

（1）例外の規定方法と適用範囲（p.15 論点１）

- 「第三者との契約」と「契約締結に先立つ場合」の２類型を追加する方向に賛同する。
- 規則は限定列挙ではなく、判断基準（考慮要素）を示す書き方をすべき。限定列挙にすると、想定外の正当なケースが漏れてしまう。衆参両院の附帯決議（第七項：具体的な範囲や判断基準を規則で明記）の要請には、この書き方でも十分に応えられる。

- 具体例はガイドライン事項ではあるが、「第三者との契約」に含まれ得る例として、少なくとも以下が読める規則の書き方とすべき。このほかにも事例は多々あると考えられるため、都度追加していくなど充実を図るべき。
  - 友人や婚約者による予約
  - 法人契約による従業員の出張手配
  - ギフト配送での受取人情報の提供
  - 企業保険における被保険者の加入の場合
- なお、この２類型の追加で必要十分かどうかは、現時点では判断しきれない。事例を積み上げる中で不足が判明した場合は、規則の見直しも視野に入れるべき。

2. リスクに適切に対応した規律

2- ① 子供の個人情報の取扱いに関する規律

(1) 利用停止等請求の例外となる取扱い（p.23 論点１）

- 利用停止等請求の例外である第８号（改正法第 35 条第９項第８号：子供本人との契約の履行に必要やむを得ない場合、または規則で定める「子供本人の権利利益を害しないことが明らかな場合」）を、大人と同様とする方向に賛同する。
- 子供向けサービスの提供に不可欠な取扱い（アカウントの維持・本人認証・決済・不正対策など）が第８号で読めることは、ガイドラインで明確化すべき。

(2) 利用停止等請求の例外事由の追加（p.23 論点３）

- 第 12 号（改正法第 35 条第９項第 12 号：法律上の 11 類型の例外に準ずるものとして政令で定める場合）に関し、次の場面が各号（第１～11 号）で読めるか整理すべき。認められない場合は第 12 号で整理すべき。
  - 不正防止や子供の安全確保のための最小限の保持（利用停止措置を受けた者の再登録防止、年齢確認の記録など）
  - 法令対応・紛争対応のための保存

(3) 法定代理人の同意と年齢確認（論点外）

- 改正法第 35 条第９項第１号（法定代理人の同意を得て取得した場合の例外）の射程を示すべき。特に、合理的な手続を踏んだが事後に同意の欠如が判明した場合の扱いを明確化すべき。

- 法定代理人からの同意取得の在り方、年齢確認についても、衆参両院の附帯決議（第八項：柔軟な手法の許容）に沿った柔軟な手法を、ガイドラインで認めるべき。

2- ② 顔特徴データ等に関する規律

(1) 特定生体個人情報の対象範囲（p.31 論点１）

- 対象（改正法第 16 条第 5 項：特定生体個人情報の定義。容易取得性・感知不可性を満たす身体的特徴として政令で定めるもの）を、顔特徴データに限定する方向に賛同する。
- ただし、単なる顔画像や、識別を目的としない途中処理（人物マスキング等）が対象外であることを明確化すべき。ドライブレコーダーや通常の防犯カメラまで対象だと受け取られるような過剰反応を防ぐ必要がある。

(2) 周知方法と周知事項（p.31 論点２）

- 周知方法（改正法第 21 条の 2 第 1 項：周知方法・周知事項を規則で定める）は、掲示と URL・QR コードを組み合わせた階層的な周知とする基本的な方向性に賛同する。
- そのうえで、移動式カメラについても、周知方法・周知事項が現実的に実施可能な形となるよう、ウェブサイトでの公表を含め事業者が手段を選べることを委員会規則（またはガイドライン）で明確に定めるべき。現在の検討は固定式カメラを前提としているように見受けられる。車載・ドローン・ロボット等の移動式カメラで顔特徴データを取得し、本人を識別できるようにする場合には、機器周辺への掲示が十分に機能しない。
- 16 歳未満の場合の「法定代理人が容易に知り得る状態」（改正法第 40 条の 2 による読替え後の周知義務）について、事前に法定代理人へ個別に通知することは現実的でないため、ウェブサイトへの掲載も含まれることを明確化すべき。

(3) 周知義務の例外（p.32 論点３）

- 登録型の顔認証サービスのように、同意取得時にすでに周知事項を説明している場合は、重ねての周知は不要と整理すべき（改正法第 21 条の 2 第 2 項第 4 号：周知義務の例外として政令で定める場合）。

(4) 利用停止等請求の例外となる取扱い（p.33 論点４）

- 利用停止等請求の例外である第 9 号（改正法第 35 条第 7 項第 9 号：契約の履行に必要やむを得ない場合、または規則で定める「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場合」）を、本人の権利利益を害しないことが明らかな取扱いに関する論点 1（基本的な考え方① p.15）と同様とする方向に賛同する。

(5) 利用停止等請求の例外事由の追加（p.33 論点 5）

- 利用停止請求への対応として、照合から除外（再取得・再登録の防止）するための最小限の情報保持が認められることを、明確化すべき（改正法第 35 条第 7 項第 10 号：法律上の 9 類型の例外に準ずるものとして政令で定める場合）。

Ⅱ．基本的な考え方②

1. 適正なデータ利活用の推進

1- ① 統計作成等の特例

- 統計作成等の特例は、AI 開発・統計作成を後押しする今回の改正の柱。同意を取るより使いやすい制度でなければ利用されず、匿名加工情報と同様に、十分に活用されないおそれがある。規則は原則的な要件にとどめ、具体はガイドライン・Q&A で柔軟に示すべき。
- 特例に係る義務違反は課徴金納付命令の対象外とならない方向であることも踏まえ、出口で規律を担保する以上、入口の要件はリスクベースで柔軟なものとし、事業者が萎縮せず特例を活用できるよう、予見可能性の高い形で定めるべき。

(1) 統計作成等の担保措置（p.19 論点 1）

- 担保措置を「必要かつ適切な措置」として規定し、具体的な措置はリスク評価に基づき事業者が選択できる方向に異論はない。特定の措置（例えば、特定の PETs や組織体制等）や、新たな様式によるリスク評価・記録を一律に義務付けず、各事業者の既存の安全管理の取組みを活用できるようにすべき。
- 措置の水準は現行法第 23 条（安全管理措置義務）と同様のリスクベースであり、一律の上乗せではないことを、ガイドライン等で明確化すべき。不明確なままだと「同意を取る方が楽」となり、特例が使われない。求める水準は、データの量・機微性・利用態様に応じて考えるべき。特定分野の事情に基づく厳格な措置を、全分野に一律に及ぼすべきではない。

- その上で、ガイドライン等で、最低限必要な措置と、要件を満たすと評価される代表的な実施例を示すべき。抽象的な要件だけでは事業者が適合性を判断できず、過剰な対応や特例の利用見送りにつながる。
- プライバシーマーク（JIS Q 15001）、ISMS（情報セキュリティの管理体制）、ISO/IEC 27701（プライバシーの管理体制）、PIA（プライバシー影響評価）の実施、分野別の既存ガイドライン（例：医療分野の「医療情報システムの安全管理に関するガイドライン」）への準拠などは、担保措置を講じていることの有力な根拠となる旨を示し、既存の基準と重複する基準は設けるべきではない。
- 復元防止・目的外利用防止は、結果責任ではなく措置義務と整理すべき。技術的に完全な防止は困難であり、「復元が一切できないこと」の証明までは求めるべきでない。情報の性質、利用環境及び合理的に予見されるリスクに応じ、ガードレール設計等の合理的な措置を講じてその内容を記録していれば、要件を満たすこととすべき。万一復元等が生じても、遡って特例の要件を欠くことにはならない旨を明確化すべき。
- 診療記録等の非構造化データや自由記述欄に含まれる氏名等を、完全に検出・削除することは技術的に困難。統計作成上の必要性、利用可能な技術、検出精度等を踏まえた合理的な対応を認めるべき。
- 「利用する必要がなくなった個人情報等の遅滞なき消去」については、再学習・検証・説明責任のために必要な範囲での保存が認められることを明確化し、保存できる条件、必要性の定期的な見直し及び消去時期の判断基準を示すべき。AI の品質管理や説明責任には一定期間の保存が欠かせず、不要後の消去の確保とも両立できる。

（2）特例の対象となる行為の範囲（p.20 論点２）

- 本人への直接の働きかけを伴う手法を除外する方向自体に異論はない。ただし、除外対象は「特例に基づき取得・受領した情報を用いて、特定の本人に直接働きかける行為」と具体的に定義すべき。「個人に直接影響を及ぼす手法」という抽象的な書きぶりでは、通常の AI 開発手法まで萎縮しかねない。
- 本人同意や利用目的の範囲内など、別の根拠で行う働きかけの反応データを特例データと併せて用いることは妨げられない旨を、明確化すべき。
- 学習済みモデルが結果として特定個人の情報を記憶し得る場合も、合理的な措置を講じている限り直ちに特例の対象外とはならないこと、及びその判断の目安を示すべき。
- 特例に基づく統計情報・AI モデルの作成と、作成したモデル等を別途適法な根拠（本人同意等）で活用すること（例：保健事業、レコメンド等の自社サービ

ス、統計に基づく属性別の施策等）は別の行為であり、後者は制限の対象外であることを明確化すべき。作成したモデルの利用は特例の対象外であり、従来どおりの規律によると考えられる。統計作成等の概念が狭隘なものとならないよう求める衆議院の附帯決議（第三項）の趣旨にも沿う。データの取得・分析と成果物の利用とでは本人への影響が異なるため、段階を分けて整理することで予見可能性が高まる。

- 初回の AI モデル開発に限らず、新たなデータを用いた追加学習・評価・更新といった継続的な改善も特例の対象となり得ることを、具体的なユースケース（例：複数の主体が保有する攻撃情報を用いたサイバー防御 AI の開発・改善）とともに、ガイドライン・Q&A で示すべき。

(3) 公表方法（p.22 論点 3）

- 公表方法の要件を全て同時に満たすことを求めるべきではない。透明性・検索性が確保される限り、方法は事業者の選択に委ねるべき。プライバシーポリシーやプライバシーセンターでの掲載や、一覧ページからリンクで辿れる構成も認めるべき。
- 「クローリング等を防止する措置を講じていないこと」は要件とすべきでない。クローリングへの対応は、各社のセキュリティやウェブサイト運用の方針に基づき判断すべき事項。セキュリティ上、ドメイン全体で防止措置を講じている企業もあり、当該ページだけ外す対応は負担が大きい。検索性はキーワードや委員会指定サイトで確保できる。仮に設けるとしても「一般的な検索エンジンで検索可能」程度にとどめるべき。
- 「特定のキーワード」は、委員会が定型文言として早期に示すべき。
- 「必要な期間をおいている」の意味を明確化すべき。提供開始前の待機期間を求める趣旨であれば、特例が機動的に使えないため、不要又は最小限とし、掲載継続期間を含めて目安を示すべき。
- 公表は自社サイトでの公表を基本とし、委員会が指定するウェブサイトでの公表は、それに代わる任意の選択肢にとどめるべき。指定サイトでの公表の義務付けや併用は求めるべきでない。指定サイトへの掲載に情報の提出や確認を要すると、公表が実質的な届出制となる。他の公表義務では方法が事業者の裁量に委ねられており、本特例だけ方法を具体的に定めるのはバランスを欠く。また、自社のプライバシーポリシー等での説明と二重の手間になるうえ、利用する事業者が多くなれば、指定サイトはかえって利用者にとって検索しづらくなる。運用にあたっては、事業者が即時に登録でき（審査によるリードタイムが

生じない）、自社ページへのリンク登録で足りる形とし、指定サイトへの掲載完了を取扱いの開始・変更の前提とすべきではない。

- 多数の提供元（保険者等）から受領する場合には、提供先が一括して公表できる方法を認めるべき。

(4) 公表事項（p.22 論点４）

- 規則で追加する公表事項は、本人による取扱いの把握と権利行使に必要な範囲に限定すべき。公表事項が広範になるほど、特例の利用が困難となる。
- 「行おうとする統計作成等の内容」（改正法第 30 条の 2 第 1 項の法定公表事項）は、「〇〇分野の AI モデル開発」程度の抽象度で足りることを示すべき。
- 公表事項の「対象情報の内容に関する事項」についても概要（データ項目や性質はカテゴリ単位、取得の経緯は類型的な記載）で足り、データ項目の網羅的な列挙は求めないこととすべき。項目を全て公表すると、研究開発や事業等の内容が推知され、営業秘密の観点からリスクが高く、特例を使う大きな阻害要因となる。例えば、医療分野であれば、「氏名・連絡先等の情報を削除した、病名等の医療情報」といった記載で足りるとすべき。サイバー防御に関わる情報など、詳細を公表すると攻撃や検知回避を招くおそれがある情報は、技術的な詳細ではなく類型・概要による説明で足りるとすべき。
- 代表者氏名等は、既存の会社情報への参照等で代替できるようにすべき。また、取扱予定期間が確定できない場合は、期間の目安や決定基準による記載を認めるべき。
- 「本人の権利行使のために必要な事項」の範囲と、これを誰が特定するのか（データの性質や取扱いの実態を踏まえ、提供元・提供先が特定するとの理解でよいか）を、具体例とともに示すべき。

(5) 公表事項の簡易な変更（p.23 論点５）

- 提供元の名称等を簡易な変更の対象とする方向に賛同する。このほか、データ項目の削減、取扱いの実質が変わらない組織再編に伴う承継、合理的な範囲での取扱予定期間の延長、公表済みの目的の範囲内での AI モデルの改善についても、簡易な変更の対象とすべき。
- 統計作成等の内容が同一のまま新たな提供元が加わる場合も、既存の公表への追記で足りるなど、手続を簡素化すべき。データの性質、取得の適法性、目的及び本人へのリスクが実質的に同等である場合を想定しており、新たな提供に必要な合意・公表まで省略する趣旨ではない。

- 提供元が倒産・解散等により変更の公表に協力できない場合の、承継先による対応や代替的な手続を示すべき。

(6) 第三者提供時の記録事項（p.25 論点６）

- 公表事項と重複する記録事項は、公表内容の写しを保存することで記録に代えられるようにすべき。公表終了後に内容を確認できなくなるとの懸念は、写しの保存で解消できる。
- 「提供された個人データの本人を特定するに足りる事項」は、提供対象のデータ群、提供時点、対象範囲及び既存の管理記録等で追跡できる場合には、本人ごとの記録の省略・簡素化（データセット単位の記録等）を認めるべき。あわせて、本人からの開示・利用停止等への対応が確保される条件を示すべき。仮名化等で識別性を下げたデータの提供時に、本人ごとの特定事項の記録を求めると、データ最小化に反し、かえって再識別のリスクを高めかねない。
- 継続的・反復的な提供については、一括・包括的な記録の作成を認めるとともに、提供元・提供先間の合意書等への記載をもって記録に代えられるようにすべき。担保措置の概要や合意・公表の実施等の要件に係る事項は、合意書や管理記録を参照し、必要時に確認できる方法で足りるとすべき。

(7) 保険制度を横断した運用と医療分野のガイドライン（論点外）

- 健康保険組合（個人情報取扱事業者）と市町村国保・後期高齢者医療広域連合（行政機関等）とで、要件・公表・記録の運用をそろえ、保険制度を横断した統計作成を可能とすべき。
- 参議院の附帯決議（第四項）を踏まえた医療分野のガイドラインの改正等は、規則の整備と同時期に進めるべき。

2. リスクに適切に対応した規律

2- ①委託先における個人データ等の適正な取扱い

- 実務で活用される制度とすべき。要件が過度に詳細であれば利用されず、委託先に全ての義務がかかる現状が続くだけとなる。
- どのような場合に制度の対象となるかを事業者が判断できるよう、具体的な事例をガイドライン等で充実させるべき。改正法の説明資料（2026 年 7 月公表）では「委託元の指示に従って機械的に入力作業を行う場合」等が例示されていたが、クラウド・SaaS の利用など、より実務に即した事例も示すべき。

(1) 契約に定める取扱いの方法（p.40 論点１）

- 「取扱いの方法」として定める事項は、委員会案の４項目（対象となる個人情報等、処理の内容、取扱いの始期及び終期、取扱いの行われる国又は地域）で足り、これ以上の追加は不要。
- 「対象となる個人情報等」の注１の「その項目等」は、カテゴリ単位（顧客の連絡先情報、購買履歴など）の特定で足りるとすべき。基本契約で包括的に委託する実務では、その都度の個別特定は困難。
- 「処理の内容」は処理の類型と目的で足り、そのうち「評価・加工の基準」（注２）は、委託元が示す仕様で足りるとすべき。使用ツールや作業手順などは、細目的な事項（p.39 の第４項目）として、委託先の裁量に委ねられることを明記すべき。
  - GDPR に係る EDPB ガイドラインにおける「本質的な手段」と「非本質的な手段」の区別と同様に、評価・加工の具体的な分析手法などの細目は、非本質的な手段として委託先の裁量に委ねられるべき。
  - SaaS 等の定型サービスに委託する場合、取得先・提供先や評価・加工の基準等は、委託元が取扱いの範囲を理解し指示できる程度の類型的な記載で足りるとすべき。
- 「取扱いの始期・終期」は、契約期間や「委託業務の終了まで」との定め、自動更新条項で足りるとすべき。
- 「取扱いの行われる国又は地域」は、クラウド等で処理地域が変わり得る実態を踏まえ、幅のある特定を認めるべき。例えば、利用リージョン（「〇〇地域内のデータセンター」等）、候補国の列挙、委託元が承認した国の一覧、変更時の事前通知・承認手続の定めなどが考えられる。物理的なサーバーの所在地や全処理工程の特定までは、一律に求めるべきではない。

(2) 契約において所定の事項を定める方法（p.40 論点２）

- 書面（電磁的記録を含む）によることとし、一部を委託元が別途書面で特定できるとする方向（注４）に賛同する。基本契約で大枠を定め、個別契約・発注書・仕様書・管理画面の設定等で委託元が具体化する方法を、広く認めるべき。
- クラウド等の標準約款であっても、委託元が内容を確認し、選択・同意したものであれば「委託元の指示」と評価できることを明確化すべき。
- 既存の委託契約・基本契約の定めで要件を満たし得る場合はそのまま適用を認めるなど、変更覚書の締結や契約改定が広範に必要とならない制度設計とすべき。令和２年改正時の越境移転対応では、契約見直しに相応の実務負荷が生じ

た。同様の負荷が生じないよう配慮すべき。改定が必要となる場合でも、覚書等による補完を認め、十分な経過期間を設けるべき。

(3) その他契約において定める事項（p.41 論点３）

- 委員会案に列挙された事項を超えて、定めるべき事項を追加すべきではない。事項が増えるほど、既存契約の改定や新規契約の交渉の負担が増え、制度が使われなくなる。
- 列挙された事項は、通常の委託契約・データ処理契約（DPA）に定められている水準の規定で足りるとすべき。漏えい等の報告、取扱いの停止、返還・消去などは、既に多くの契約に定めがある。
- 各事項の具体的な方法は、当事者間の合意に委ねるべき。特に「取扱いに関する記録」は、全ての処理ログの提供ではなく、委託元の求めに応じた提供や定期報告で足りるとすべき。
- 取扱記録や「安全管理のために講じた措置に関する情報」の提供は、委託先が標準的に提供する第三者認証・保証報告書（ISO/IEC 27001 認証、SOC 2 報告書等）や管理画面等の活用で足りることを明確化すべき。これらを確認し、不足する情報を補完することが委託元による監督に当たることも、ガイドライン等で示すべき。全ての委託元向けに個別様式で記録を作り直して常時提供することは、SaaS 等の定型サービスでは過大な負担となる。

2- ②漏えい等報告及び本人通知義務

- 漏えい等報告は、「漏えいした可能性を完全に否定できなければ報告」という現行の運用を見直し、委員会が早急に把握すべき事案に重点化すべき。
- 「おそれ」の考え方、報告の在り方、本人通知の在り方それぞれについて、リスクベースで判断できるようにすべき。

(1) 本人通知義務の緩和（p.46 論点１）

- 「二次被害の防止等のために措置を本人が講じられるようにする必要性が少ない場合」かどうかの判断基準を規則で示し、漏えい等（その「おそれ」を含む）の発生時に、事業者がその基準に沿ってリスクベースで判断できるようにすべき。
- 「それ単体ではおよそ意味を持たない情報のみ」という言葉を厳しく解釈すると、該当事案がほとんどなく、本人通知を緩和した改正の趣旨が活かされない。

衆参両院の附帯決議（第十項：具体的な対象範囲や判断基準を規則で明記）を踏まえ、客観的な基準を伴う形で、次の場合や判断の考え方も規定すべき。

- 委託先・共同利用者・グループ会社など、漏えい元の管理下にある者や守秘義務を負う者との間でのみ共有する識別子は、「外部と共用性のない」ものとして扱うこと。
- 「外部と共用性のない」社内識別子などの情報と、それ自体では本人に到達できず二次被害のおそれもない情報（車両の稼働データ、機器のログ等）のみが漏えいした場合。
- 漏えい元が保有する他の情報と照合しない限り、特定の個人を識別できない情報のみが漏えいした場合（例：氏名・住所・連絡先等を削除した匿名の履歴書など、本人への連絡・接触もできない情報）。
- 同一顧客の情報を既に保有するグループ会社等への誤送信など、受領者にとって新たな情報とならない場合。
- 契約者番号・内部管理番号等についても、番号の名称ではなく利用実態（事業者と本人のみが知り得るか、他の情報との照合や認証への悪用のおそれがあるか）で判断すること。
- 既に利用されていない識別子やメールアドレス（退職者の社用メールアドレス、従業員番号等）のみが漏えいした場合。
- 本人等により適法に公開され、漏えい時にも同じ内容が同じ範囲で閲覧可能な情報（公開済みの従業員紹介ページ等）のみが漏えいした場合。ただし、非公開情報との結合等によりリスクが増す場合は除く。

- 端末識別子やハッシュ化したメールアドレス等のうち、事業者固有の方法で生成し、他者が照合できないものは、「共用性のない識別子」と扱うべき。
- IDFA のように共用性のある識別子であっても、それのみが漏えいした場合は、それ自体では本人への連絡や二次被害にもつながりにくい。その識別子の持つ特性を踏まえ、「本人の権利利益の保護に欠けるおそれが少ない場合」として考えるべき。
- 本人への通知に代わる措置は、社外への公表を前提とせず、情報の性質やリスクに応じた柔軟な方法（事案の性質に応じた公表、問合せ窓口の設置、対象者に限定した周知等）を認めるべき。例えば、外部と共用性のない従業員 ID のみが漏えいした場合は、従業員向けポータル等での周知で足りることをガイドラインで示すべき。権利利益の保護に欠けるおそれが少ない事案でも社外公表が前提だと、レピュテーションへの配慮から個別通知を選ぶ事業者が増え、事業者・本人の双方にとって合理的でない。

(2) 第三者の確認を受ける体制及び手順（p.47 論点２）

- 確認の対象は、責任者の設置や事案対応手順（事実確認・本人通知・再発防止）の整備など、基本的な事項に限定すべき。
- 確認手続は、チェックリスト等の書面による簡易なものとし、更新も過度な負担とならないようにすべき。

(3) 漏えい等報告の合理化の対象事案（p.48 論点３）

- 本人の数が１名の事案を対象とし、一定の範囲で速報を免除し、一定期間ごとに取りまとめた確報を許容する方向に異論はない。その上で、これらの取扱いと、対象が規則第７条第１号から第３号（p.51）のいずれかに該当する１名の事案であることを、規則上明確に定めるべき。
- 加えて、本人が住所変更を届け出ないなど、事業者に帰責性がない事情で生じた誤送付も、合理化の対象として扱われることを明確化すべき。

(4) 体制及び手順の確認主体（p.48 論点４）

- 認定個人情報保護団体を確認主体とすることに異論はない。ただし、認定団体の対象事業者でない企業や、認定団体のない業種も多く、それだけでは制度を使える事業者が限られる。
- そこで、プライバシーマーク、ISMS（ISO/IEC 27001）、ISO/IEC 27701 等の第三者認証の審査・認証機関や監査法人等、必要な専門性と独立性を有する者も確認主体に加えるべき。既存の認証・監査で確認済みの範囲（責任者の設置、初動対応、本人通知、再発防止等）は活用し、不足する部分のみを追加で確認する形とすべき。確認項目、有効期間及び更新の扱いも明示すべき。
- 併せて、認定団体の負担への配慮や機能強化への支援も要望する。

(5) サイバー対処能力強化法等との整合性（p.49 論点５）

- サイバー対処能力強化法によるインシデント報告の基準との整合性を確保する方向性に賛同する。サイバー攻撃に起因する漏えい等の「おそれ」（p.44㋒）は、攻撃の痕跡がある場合や一定の蓋然性が高い場合に限るべき。可能性を否定できないことのみをもって報告対象としない旨を、規則・ガイドラインで明確化すべき。
- 併せて、サイバー攻撃に起因しない「おそれ」（紛失した媒体が後に発見された場合や、クラウドの公開設定の誤り、ウェブサービスの特殊な URL に個人情

報が一時的に表示された場合などで、アクセスログが一部欠けていても、URLの特殊性・非到達性や公開時間等から、第三者による閲覧やクローリングがなかったと合理的・技術的に説明できる場合等）についても、同様に蓋然性に基づく基準へ見直すべき。

- サイバー対処能力強化法に加え、電気通信事業法等の他法令に基づく報告も含め、窓口・様式・提出情報の一元化を進めるべき。一度提出した共通情報が関係機関で共有され、各制度の報告に充当される仕組みとすべき。「おそれ」の判断に必要な事実・証跡、報告期限、追加報告の方法も可能な限りそろえ、法目的により差が残る事項は対応表で示すべき。

（6）違法な第三者提供の報告対象化（p.50 論点６）

- 違法な個人データの第三者提供を報告対象とする場合には、漏えい等報告の趣旨（意図しない事態について委員会が早急に把握し、必要な措置を講じること）や、法第 26 条第 1 項の「個人データの安全の確保に係る事態」との関係を整理した上で、対象を限定的に定めるべき。その際、目的外利用等の他の違法行為との均衡も考慮する必要がある。
- 具体的には、本人同意も法定の例外もない第三者提供（法第 27 条第 1 項、第 28 条第 1 項違反）に限定すべき。外国にある第三者への提供時の情報提供（法第 28 条第 2 項・第 3 項）や確認・記録義務（法第 29 条・第 30 条）など、手続的義務の不備まで含めると、グローバルなクラウドを利用する企業や中小企業を含め、厳密な対応は困難。
- このうち、「内容や件数を問わず報告対象」とするのは、違法性を認識しつつ行った提供や不正の目的がある提供など、悪質な事案に限定すべき。システムエラーやオペレーションミスで同意の取得・記録ができていなかった事案は、実態として漏えいに近い。現行の漏えい等報告の基準（規則第 7 条各号）に準じて扱えば、過失による事案も捕捉しつつ、1 件の同意漏れまで全件報告する過大な負担は避けられる。
- 同意の有無や範囲について本人と見解が分かれる場合は、事業者が合理的な根拠に基づき同意を得たと判断していた限り対象外であることを、明確化すべき。実際に、顧客から苦情の傍論として「同意していない」と主張される事案は多い。基準が不明確なままだと、事業者は安全策として報告せざるを得ず、誠実に対応する事業者ほど負担を負うことになる。

- 同意の有効性や、委託・共同利用・第三者提供の区別など、法的評価に合理的な疑義がある場合は、必要な事実確認と法的評価を経て報告対象と合理的に判断できた時点を「知った時」とするなど、判断基準を示すべき。
- 事業者が自ら発見し、提供先での削除等の是正を終えた事案については、報告内容の簡素化等、自主的な発見・是正を妨げない運用上の配慮を要望する。

（7）委託元と委託先の報告の重複解消（論点外）

- 委託先で漏えい等が生じ、委託先が委託元への通知より先に速報を提出した場合は、委員会は既に事実関係を把握しているため、委託元の速報は不要とすべき。確報は委託元・委託先の連名で提出できることとすべき。事実関係を十分に把握できていない委託元が遅れて速報を出しても、迅速かつ効率的な報告にならない。新制度で義務が免除される委託先については、委託元に代わって速報を提出できるかどうかもあわせて整理すべき。

Ⅲ．基本的な考え方③

1. 不適正利用防止

1-①連絡可能個人関連情報の不適正利用及び不正取得の禁止

（1）対象となる記述等の範囲（p.15 論点）

- 現時点で追加的に規定すべきものは特段ない。仮に将来追加する場合は、新たな技術により個人への連絡手段が現実に生じた場合に限り、当該技術を利用する事業者と議論を尽くすべき。
- その上で、第 4 号の「Cookie ID 等」の「等」の範囲は慎重に整理すべき。注の広告識別子、SNS の ID、オンラインサービスのアカウント ID、IMEI 等まで一律に含めると、規律の射程が著しく広がる。住所・電話番号・メールアドレスは、誰が取得しても連絡に使えるのに対し、Cookie ID 等はそれ自体を取得しても直接連絡できる事業者は限られ、情報の性質が異なる。特に IMEI 等の端末識別番号は、通常、それ単体で特定の個人への情報伝達に利用できるものではない。
- 法第 2 条第 8 項各号の「特定の個人に対する連絡等に利用することができるものに限る」との限定を踏まえ、どのような場合に該当し、どのような場合に該当しないかを、ガイドライン・Q&A で具体例とともに示すべき。例えば、有効期限が切れた Cookie ID、使われていない電話番号、転居により連絡できない住所は該当しないと考えられる。加えて、自社サービス内でしか通知できないア

カウント ID も、当該事業者以外が取得しても連絡に使えないため、該当しないものと整理すべき。

- なお、連絡可能個人関連情報の不適正利用及び不正取得の禁止については、悪質な事案を対象とするものであることをガイドライン・Q&A で明確にすべき。その際、現行法第 19 条（不適正利用の禁止）のガイドラインと同様に具体的な事例を示すなど、適法・適正に事業を行う事業者の事業活動が萎縮しないよう、適切な判断基準を示すべき。

2. 規律遵守の実効性確保のための規律

2- ①課徴金の導入

- 課徴金は、衆参両院の附帯決議（第十二項：過度な萎縮の防止、明確なガイドラインの策定、運用の透明性の確保）を踏まえ、対象をできる限り限定し、判断に迷う曖昧さを残さない形で定めるべき。曖昧さが残ると、法令遵守に真摯に取り組む企業ほどガバナンス・コストをかけるため、データ利活用に取り組まなくなる。政令・規則、その後のガイドラインも含め、判断に迷いが生じないようにすべき。
- 統計作成等の特例に係る義務違反も課徴金の対象となるが、制裁だけが強化され特例のメリットが損なわれないよう、バランスに配慮すべき。

（1）課徴金納付命令の対象（p.46 論点１）

- 第三者提供の制限違反について、本人に直接影響を与えることが一般的に想定されない情報のみを提供した場合を対象外とする、リスクベースの方向に賛同する。
- 統計作成等の特例に係る義務違反は対象外を設けない案とするのであれば、何が特例の義務違反に当たるかを明確にすべき。
- 学習済み AI モデルについては、出力に個人情報が含まれたことのみをもって、モデルに個人データが保持されている（過学習させた）とは判断しない旨を、ガイドラインで明確化すべき。
- 適正な方法で学習を行い、パラメータしか残っていない場合、個人データは保持されていないと考えられ、その旨も併せて明記すべき。

（2）課徴金納付命令の対象外となる情報（p.47 論点２）

- 対象外となる（＝①、②、③のいずれも含まれない）場合の具体例を、ガイドライン等で示すべき。対象外となる場合が限定的に過ぎると、リスクベースで対象外を設けた意味が実務上なくなる。
- 「③ その他の以下の記述等」の範囲は、明確かつ限定的に定めるべき。
  - 「特定の個人に対する連絡等が可能となる記述等（Cookie ID 等）」を連絡可能個人関連情報と同様に広く解すると、対象外となる場合がほぼなくなる。
  - 「特異な記述等（症例数の極めて少ない病歴等）」の「極めて少ない」のような定性的な表現は、客観的な基準に置き換えるべき。
  - 「多数の事業者において取得されている共用性のある ID 等」について、事業者固有の方法（ソルトの付与等）で生成し、他者が照合できない識別子は含まれないことを明確化すべき。
  - 「蓄積された位置情報、購買履歴等」は、どの程度の量・期間で「蓄積」に当たるのかを示すべき。併せて、氏名・住所等を除いた購買履歴のみを提供する場合は対象外となり得ることを、明確化すべき。
- 「③ その他以下の記述等」の判断に当たっては、少なくとも仮名加工情報の加工基準を満たす程度に加工したデータの提供は、対象外となることを明確化すべき。

(3) 課徴金額の算定方法（p.50 論点３）

- 課徴金額は、違反行為から「直接的に得られた財産的利益」（p.48）に限られることを、規定上明確化すべき。資料の事例はいずれも売却等で対価が明確だが、実際にはデータを活用したサービス全体で収益を得ることが多い。サービス全体で得た売上・利益まで算定されれば、過大な金額となる。
- 対価を得ていない場合には課徴金の対象とならない（勧告・命令の対象にとどまる）ことも、明確化すべき。
- 適法な部分と違法な部分が混在する取引（事例②のように、一部の本人・項目については同意を得ていた場合）は、違反行為に対応する部分に按分して算定する考え方を示すべき。
- 事例③のような場合でも、AI の価格のうち、違反（個人データの保持）に起因する部分と、正当な AI 開発による付加価値とを区別すべき。AI を実装したことによる付加価値全体が対価とみなされると、AI 開発に取り組む企業が萎縮する。

(4) 対価額の推計（p.51 論点４）

- 対価額の推計に関する規定を設ける場合、算定の考え方及び計算方法を明確かつ十分に示すべき。弁明の機会において事業者が算定方法や根拠に具体的に反論する上で重要。

(5) 課徴金の減額のための報告方法（p.52 論点５）

- 違法な第三者提供が漏えい等報告の対象とされた場合には、当該漏えい等報告をもって減額のための報告とみなすなど、両制度の手続を一本化すべき。

(6) 消滅及び事業譲渡等の場合の加算及び減額（p.54 論点６）

- 存続法人等に対する課徴金の減額の引継ぎには賛同する。また、課徴金を逃れる目的で違反行為を行った法人を消滅させる場合に、存続法人等へ加算を適用することにも異論はない。
- 消滅法人の過去の課徴金対象行為が事後的に判明した場合など、存続法人等に当該違反行為の帰責性がない場合もあり得る。加算の引継ぎは機械的に行うのではなく、事案ごとに考慮できるようにすべき。

以　上