資料1－1

第二次いわゆる3年ごと見直しへのコメント

弁護士・ひかり総合法律事務所
理化学研究所革新知能統合研究センター客員主管研究員
国立情報学研究所客員教授
大阪大学社会技術共創研究センター招へい教授
国立がん研究センター研究所医療AI研究開発分野客員研究員
板倉陽一郎

アジェンダ

- 1　個人の権利利益のより実質的な保護の在り方
  - 1.1　個人情報等の適正な取扱いに関する規律の在り方
  - 1.2　第三者提供規制の在り方
  - 1.3　こどもの個人情報等に関する規律の在り方
  - 1.4　個人の権利救済手段の在り方
- 2　実効性のある監視・監督の在り方
  - 2.1　課徴金，勧告・命令等の行政上の監視・監督手段の在り方
  - 2.2　刑事罰の在り方
  - 2.3　漏えい等報告・本人通知の在り方
- 3　データ利活用に向けた取組に対する支援等の在り方
  - 3.1　本人同意を要しない公益に資するデータ利活用等の在り方
  - 3.2　民間における自主的な取組の推進
- 4　その他
  - 4.1　個人情報保護政策の在り方
  - 4.2　いわゆる3年ごと見直しの在り方
  - 4.3　行政機関等の規律の在り方

1　個人の権利利益のより実質的な保護の在り方
1.1　個人情報等の適正な取扱いに関する規律の在り方

- 個人情報取扱事業者における個人情報・個人データに係る義務の対象を「**個人データ（当該個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む。）**」（規則7条3号）に統一すべき
  - Webスキミングへの対応のために，漏えい等報告等の対象を広げた規則改正によるものであるが，既にGL通則編では安全管理措置の対象ともなっている（3-4-2）
    - なお，「従前からの解釈を明確化したもの」とされているが（パブコメ回答29番），義務の対象という重要な点についての上乗せであり，委任の範囲を逸脱していると思われることはとりあえず措く
  - 現状，「個人情報」が義務の対象である規定（17条～21条）が，対象を「個人情報」としている趣旨は「**いずれ個人情報データベースに記録され「個人データ」となるものであっても，取得段階では「個人情報」の状態であることによる**」（園部・藤原第三次改訂版149頁）のであるから，**個人データ（個人データ予定個人情報を含む）という概念が許されるのであるなら，「個人情報」すべてに義務を掛けるのは過剰**である。
  - 不適正利用禁止（19条）の対象が「個人情報」であり，「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」（2023年3月）21頁によると，
    - 「不法行為の成否を評価するに当たり考慮される要素は、個人情報保護法上も不適正利用の禁止規定（法第 19 条）や適正取得規定（法第 20 条第 1 項）の解釈などにおいて、考慮すべき」
    - 「顔識別機能付きカメラシステムを利用するに当たっては、個人情報保護法を遵守するのみならず、肖像権やプライバシー保護の観点からも留意する必要があるし、そのような観点を個人情報保護法の適用においても考慮すべきである」
  - とされる。これは，**不法行為に該当するような個人情報の取扱い全てについて，個人情報保護委員会の監視・監督が及ぶことになるが，（現時点で）「個人情報」を義務の対象としていることの趣旨を逸脱している**。
  - GDPR2条1項”…intended to form part of a filing system.”とも平仄は合う

1.1　個人情報等の適正な取扱いに関する規律の在り方（続）

- 適正取得・不適正利用
  - 義務の対象を個人データ（個人データ予定個人情報を含む）とする前提で，「カメラシステムの利用について」も踏まえて事例を追加することは必要であり望まれる。
- 個人関連情報
  - 義務の対象を個人データ（個人データ予定個人情報を含む）とする前提で，現在の個人関連情報は「個人情報」に含まれるとした方が簡便ではないか。
    - 概念が多すぎるという経済界の要望にも沿う。
  - 電気通信事業法における外部送信規律は，個人情報保護法に取り込み，統一的に把握できるようにすべき（細かい概念が異なる等は事業者における対応が困難）。
- 生体データ等
  - GDPR9条1項は生体データを特別カテゴリデータとしている
  - 医療やゲノムについては適切な立法がなされるべきであり，それを踏まえてもなお個人情報保護法側で概念を変更しなければならないのかという必要性は吟味されるべき

1.2　第三者提供規制の在り方

- 前提として，GDPR上の適法化事由（6条1項(a)-(f)）と単純に比較する議論は筋が悪い
  - **日本法は取扱いが原則適法，GDPRは取扱いが原則違法**であり，前提が全く異なる（が，それを踏まえてもなお）
- 契約に基づく提供は，**契約の本来的な趣旨（役務の提供等）に必須の範囲**については認められるべき
  - 複雑な決済スキームについて同意があると考えるのは欺瞞（であるが，必要性は高く，行政規制による許容性も認められる）
  - 契約や約款に書き込めば本来的な趣旨となるわけではないことは注意。
- オプトアウト
  - 二重オプトアウト禁止（27条2項「この項本文の規定により提供されたもの」）の企業情報データベース等への影響は精査すべき。
  - American Privacy Rights Act of 2024（草案）における「一元化されたメカニズム」（Sec6.(b)）は参考になる（「容易に知り得る」の形骸化への対応にも資する）。

1.3　こどもの個人情報等に関する規律の在り方

- 「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について、未成年者、成年被後見人、被保佐人及び被補助人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」（GL2-16）という定式化は**そもそも意思能力と行為能力（に相当するもの）を混同しており理論上おかしい**。
  - 「とりあえず親の同意を取ろう」（未成年者）「とりあえず親族の同意を取ろう」（高齢者）という，本人の権利利益の保護と関係のないスタンプラリーになってしまっている（高齢者の場合，ほとんどは法定代理人ですらない）。
  - 同意を含む取扱いについての代理を認めるのであればきちんと立法すべき（必要に応じ本人確認の手続等も）
    - 詳細は板倉陽一郎・藤村明子「こどもデータ及び教育データの取扱いにおける同意に関する考察」情報通信学会誌41巻3号（2024年）25頁。
- こどもや家庭への支援や，教育データの利活用は，そもそもそれぞれの法律で必要な情報・データの取扱いが定められるべき（医療における一次利用も同様）。
  - **個人情報・個人データを用いた政策が立案される際に，最初から個人情報保護法に負担がかかることを想定して立案することは間違い**。必要な情報・データの取扱いはそれぞれの分野で適切に立法される必要がある（**そのために「個人情報等の適正な取扱いに関係する政策の基本原則」（令和4年5月25日）がある**）。感染症法15条，56条の41などは実践例。
  - AIにおける個人情報・個人データの利用についても，著作権法における適用除外規定等との平仄を併せた上で，AIそのものに関する法令で定められることが筋ではないか。

1.4　個人の権利救済手段の在り方

- 差止請求
  - 利用停止請求は拡大された（35条1項，19条・35条5項）が，裁判例は現れていない。一人だけ利用停止されても全体としての違法な取扱いは改められない。
  - 消費者契約法・特商法・景表法・食品表示法と並びで適格消費者団体による差止請求を認める余地がある。
    - オプトアウトについて一元化されたメカニズムが用意される場合，これを代替行使することも認めてよいのではないか。
- 集団的被害回復制度
  - 裁判手続特例法令和4年改正（2023年10月1日施行）により，慰謝料請求は可能になっている（財産的損害の存在又は故意が必要）が，利用例が見られない。
- いずれにせよ，適格消費者団体，特定適格消費者団体への機能強化は不可欠の前提であり，財政支援等が望まれる。

2　実効性のある監視・監督の在り方
2.1　課徴金，勧告・命令等の行政上の監視・監督手段の在り方

- 課徴金
  - 第一次いわゆる3年ごと見直しでは否定的であったが，以下の理由により**導入に賛成する**。
    - 破産者マップ（類似サイトを含む。以下同じ。）のように，明らかな個人データの不適切な取扱いにより利益を得ようとする（得ている）ものが実際に存在すること
    - ビッグ・テックに対しても，金銭的なペナルティは効果的であること（外国会社未登記に係る過料）
  - 違法な取扱いによる利益の吐き出しが主たる目的であり，**過失による漏えい等では基本的には利益は存在しないので，対象とはいえない**。
    - ただし**安全管理措置を全く行わないことによって価格優位を実現して利益を得ていたというような極限的な場合**が考えられないではない。
    - 主観的要件（景表法8条は「知らず、かつ、知らないことにつき相当の注意を怠つた者でないと認められるとき」を除外している）の導入も考えられる。
  - 事業者は全体としては課徴金の導入は避けたいのであるが（当然であろう），個人情報やセキュリティの担当部署としては適切な予算配分のきっかけになるのではないか。この点では，**経営陣と担当部署は利害が対立する**。
- 公表
  - 公表についての規律がないが（規律があるものとして取引透明化法6条3項，6項），事業者に対する事実上のペナルティである以上，規律を定めるべきである。
- その他の監視・監督手段
  - 破産者マップのような明らかな違法サイトについて，個人情報保護委員会が，検索エンジン運営者，ドメイン事業者，CDN等への措置命令・課徴金納付命令が行えるようになることは効果的であり望ましい。

2.2　刑事罰の在り方

- 公表されている唯一の告発事例が奏功していない
  - 個人情報保護委員会「破産者等の個人情報を違法に取り扱っている事業者に対する個人情報の保護に関する法律に基づく対応について」（令和5年1月11日）。
  - 国際的な事案について，データ保護機関のネットワークも利用すべきであるし，告発事案についてはその後も捜査機関との協力を進めて欲しい。
- 個人情報データベース等提供等罪（179条）の客体が「個人情報データベース等」であることで、被害者は客観的に被害を把握できない
  - 捜査段階で、被害者に「個人情報データベース等」の立証を厳密に求めることで、ほとんど使えなくなっている（報道されているのも数件）。

2.3　漏えい等報告・本人通知の在り方

- 「おそれ」（施行規則7条1号）
  - **コストを掛けて調査すればするほど「おそれ」の範囲が拡大して（対象の本人の人数が増えて），本人通知のコストが上がるというのはインセンティブ構造としておかしい**。
    - 本人通知は本人の権利利益保護のために行われるべきであって，事業者へのペナルティとして行われるべきではない。
- 漏えい元基準
  - 26条の「個人データ」該当性は，提供元基準にならって漏えい元基準が採用されているが，個人データの一部であって，特定の個人の識別もできず，単体では意味すらないような部分が漏えい等しても，本人通知まで行わなければならないというのは不合理である。漏えい報告の場面は事前判断ではないので，リスクに応じた対応で十分である。
  - 他方で，**（漏えい元基準の不合理性に乗じて）提供元基準まで放棄させようという議論があるが，第三者提供の場面は，事業者が事前にリスクを判断しなければならないので，明らかに不適切**である。
- 報告の活用
  - 速報の分析活用が望ましい。同じような漏えい等報告が速報として多数個人情報保護委員会に届く場合，同種の攻撃や，ウイルスについて迅速なアラートに結び付けて欲しい。そうでなければ，攻撃されて，事業自体の停止等によるダメージを受けつつも速報を提出する事業者が報われない。
- 公表（前掲）
- 第三者提供と漏えいの関係
  - 「個人情報取扱事業者が自らの意図に基づき個人データを第三者に提供する場合（※）は、漏えいに該当しない。」（GL通則編3-5-1-1）とされるが，**意図に基づいていても，違法な第三者提供が漏えいに該当しない（＝報告義務等がない）というのは不合理**であり，二分論でなくともよい
    - 板倉陽一郎「個人情報保護法の観点から」指宿信・板倉陽一郎編『越境するデータと法』（法律文化社，2023年）202頁の中で，同論点に触れた（207頁）。

3　データ利活用に向けた取組に対する支援等の在り方
3.1　本人同意を要しない公益に資するデータ利活用等の在り方

- 「公益」は基本的には個別法によって定められるべき。
  - こども・教育・医療・災害対策等における個人情報・個人データの取扱いはそれぞれの法令で必要な情報・データの流れが記載されることによって定められるべき。
    - 医療については二次利用についても次世代医療基盤法その他で立法される流れであり，望ましい。なお，学術研究機関等ではない医療機関による研究は個人情報保護法の学術研究例外と別に医療関係法令で定める方が実態に即すのではないか。
- 「公益」に関する一般条項を求める議論
  - GDPRにおける「適法な利益」（6条1項(f)）に相当する一般条項を求める声があるがそもそもの日本法とGDPRの原則の違いを踏まえていない。
  - **既に日本法には「人の生命、身体又は財産の保護のために必要がある場合」（27条1項2号等），「公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合」（同3号等）が存在**し，解釈の積み重ねもある。どちらかというと実務的に困難なのは後段（「本人の同意を得ることが困難であるとき」。）
  - 後段を，「**本人の同意を得ることが困難である等，本人の同意を得ないことについて相当の理由がある場合**」などとしてはどうか（事案によっては，本人に連絡が付く限り絶対に同意を得ようとせよというのは明らかに不合理）。

3.2　民間における自主的な取組の推進

- PIA，DPOなどについては，適切なインセンティブが設けられるべきであるが，GDPRのアンチテーゼとして改正される予定の英国法（Data Protection and Digital Information Bill）の動向にも着目すべき。

4　その他
4.1　個人情報保護政策の在り方

- 3年ごと見直しのたびに新たな制度や概念が入るが，（法の究極目的である）本人の権利利益の保護との関係でどのように効果的であるのか（利活用施策については，権利利益の保護を後退させずに推進できているのか）の検証が必ずしも行われていない。
  - 消費者基本計画（令和2年3月21日閣議決定，令和3年6月15日改訂）では，「工程表においては、今期消費者基本計画の対象期間中の取組予定及び KPI（重要業績評価指標：Key Performance Indicator）を明示し、国民の意見を反映させるための取組を進めるとともに、消費者委員会の意見を聴取した上で毎年度改定する。」とされ（23頁），これに沿って消費者委員会による検証・評価・監視が行われている。

4.2　いわゆる3年ごと見直しの在り方

- いわゆる3年ごと見直しを廃止するという議論があるが強く反対する
  - **法改正にはエネルギーがいる。廃止したら法改正を前提とした議論は避けられるようになる。平成27年改正まで，10年以上放置したことの反省を忘れるべきではない**。
  - 他方で，「3年」が適切であるかは議論してよい。
    - 法律・政令・規則・一般GL・個別分野GLを改正しているとすぐに次の改正の議論が必要になる。これに加えて，いわゆる3年ごと見直し以外の改正（直近では令和3年改正）や，関連分野の法改正（例えば，電気通信事業法における外部送信規律の導入等）により，事業者の対応が負担（限界）であることも理解はできる。
- いわゆる3年ごと見直しに係る検討の回は，個人情報保護委員会を公開で開催すべき（第105回個人情報保護委員会（令和元年5月17日）ヒアリング再掲）
  - あらゆる事業者等に影響のある法律の改正に関する議論であり，全くの非公開で開催して正統性（legitimacy）が保てるのか，疑問がある。原則公開で開催すべきではないか。
  - 個人情報保護委員会本会の公開に支障があるのであれば，専門委員による専門委員会を公開として議論することも考えられるのではないか。

4.3　行政機関等の規律の在り方

- 行政機関等の規律についても3年ごと見直しで改正されることが望ましい
  - 行政機関等の規律について，**行政機関等における個人情報の取扱いの観点で正面から議論されなくなって久しい**（平成27年個情法改正⇒平成28年行個法等改正も，令和2年3年ごと見直し⇒令和3年一元化も，基本的には**ハネ改正**）
  - （その結果）行政機関等のDX化，デジタルプラットフォームやスマートシティの施策を想定した規律ではない。例えば，
    - 原則，散在情報規制（個人情報・保有個人情報・個人情報ファイル）
    - 匿名加工情報の提供は提案募集手続に限られる
    - 仮名加工情報は自ら作成することを前提としていない
    - 外部提供に係る確認記録義務がない
    - 本人からの請求は開示前置
      - 板倉陽一郎「デジタル改革関連法成立後のプラットフォームビジネスとパーソナルデータ」千葉恵美子編著『デジタル社会の進展と法のデザイン』（商事法務，2023年）282頁参照
- 規律移行法人の範囲についても議論が必要（金融，交通等）