資料２－５

3年ごと見直しヒアリング

弁護士　森　亮二

目次

第1節　個人情報に関する権利の在り方

- 取得についての透明性の確保
- 利用停止、消去、第三者提供の停止の拡大

第2節　漏えい報告の在り方

- 漏えい報告の義務化

第4節　ﾃﾞｰﾀ利活用に関する施策の在り方

- 仮名化データの規制緩和は不適当
- スコアリングについての規制
- ターゲティング広告と個人識別符号の拡大

第5節　ペナルティの在り方

- 課徴金制度を導入すべき

第6節　域外適用等

- 域外適用の条項の追記

第7節　その他

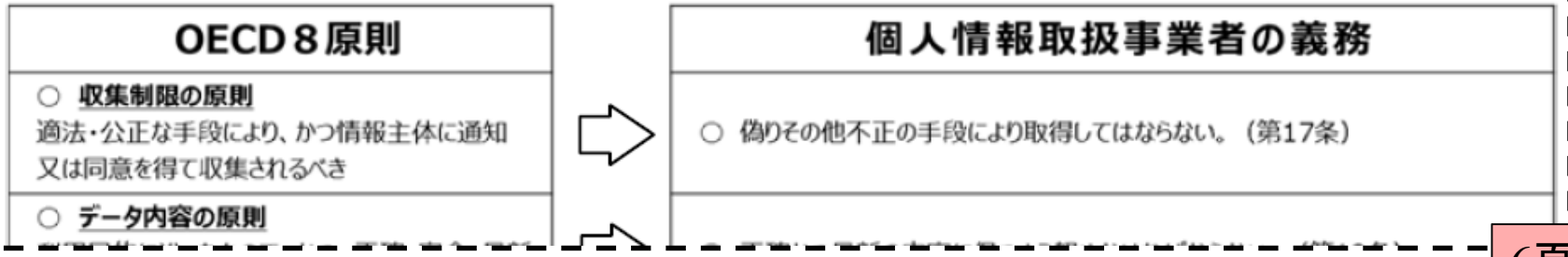
- 条例の統一化、委員会の所管の拡大
- ｸﾞﾚｰｿﾞｰﾝの解消－生成は取得と解すべきである
- ｸﾞﾚｰｿﾞｰﾝの解消－要配慮個人情報の可能性

第１節　個人情報に関する権利の在り方

取得についての透明性の確保

第1節　個人情報に関する権利の在り方

ＯＥＣＤ８原則と個人情報取扱事業者の義務規定の対応（概要）



OECD８原則	個人情報取扱事業者の義務
○ 収集制限の原則 適法・公正な手段により、かつ情報主体に通知又は同意を得て収集されるべき	○ 偽りその他不正の手段により取得してはならない。（第17条）
○ データ内容の原則	

6頁

要望等としては、事業者が個人情報を取得又は利用する際に本人の関与を求める意見等が寄せられている。

8頁

取得についての透明性の確保

第1節　個人情報に関する権利の在り方

- 現行法では、取得については、17条1項の適正取得義務、17条2項の要配慮個人情報の取得の同意、18条における利用目的の通知・公表・明示、26条の確認記録義務関係が主な規制。

- OECD原則の求める「取得の事実」の通知等を新たに規定してはどうか。

- 「こっそり取得」は、17条1項の適正義務違反となることがあるが、正面から取得の透明性を確保する義務を規定してはどうか。

- もっともどのような場合に、取得の事実を通知・明示させるかということについては、検討を要する。

利用停止、消去、第三者提供の停止の拡大

第1節　個人情報に関する権利の在り方

＜削除・利用停止に関する相談＞
（中略）事業者に対する不満等のうち、事業者が削除・利用停止に応じないことに関する不満等が最も多く寄せられている。（中略）要望等としては、削除・利用停止の義務化を求める意見や、削除・利用停止手続に伴い事業者が取得する個人情報の範囲等について規制を求める意見等が寄せられている。

9頁

必要性

「ＪＩＳ　Ｑ　１５００１個人情報保護マネジメントシステム－要求事項」においては、本人の保有個人データの利用停止、消去又は第三者提供の停止の請求を受けた場合は、原則として応じる義務があることとされており、自主的に個人情報保護法の水準を超えた対応が行われている。

許容性

12頁

利用停止、消去、第三者提供の停止の拡大

第1節　個人情報に関する権利の在り方

- 現行法では、保有個人データの利用停止、消去の請求には、16条または17条の違反が条件となっており、第三者提供停止の請求は、23条1項又は24条の違反が条件となっている。

- 消費者からの要望であり、かつJISQ15001において広く実現されている運用であることから、これらの条件なく、利用停止、消去、第三者提供の各停止請求を原則として義務化してはどうか。

事業者によっては、安全管理上の理由等から、個人情報データベース等を部門ごとに別々に管理している場合もあり、このような場合に全部門の個人データを容易に名寄せし、利用停止等ができるような体制になっているかという論点もある。

18頁

- 現行法の開示請求の場合には、「名寄せが困難なので開示しない」という拒絶がみとめられていないことと不均衡な議論ではないか。

利用停止、消去、第三者提供の停止の拡大

- JISQ15001にそろえる場合、
  - ①　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場合
  - ②　当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合
  - ③　他の法令に違反することとなる場合

  が例外となる（28条の開示請求の例外と同じ）。

第2節　漏えい報告の在り方

漏えい報告の義務化

第2節　漏えい報告の在り方

□　漏えい報告を法令上明記し、義務化すべきではないか。

- 明確な義務化がなされていないことから、漏えいの対応が遅れることにより権利利益の侵害のおそれが高まる。
- 他方で、判明した事実の報告であれば、事業者の負担は大きくない。むしろ適切なアドバイスを受けられて、プライバシー侵害による損害賠償請求等を回避することができる可能性もある。
- 件数や情報内容によって義務の有無を区別する考え方は合理的。
- 期限を明示的に設けることがいいのではないか。GDPRの判明後72時間は一つの目安。

第４節　データ利活用に関する施策の在り方

仮名化データの規制緩和は不適当

第4節　データ利活用に関する施策の在り方

ＧＤＰＲの仮名化（Pseudonymisation）については、（中略）個人データよりも負荷の軽い規律となっており、第11条(2)には、データ主体が、自己の権利の行使の目的のために、自身の識別ができるようにする付加的な情報を提供する場合を除き、第15条から第20条までの規定（※）は適用されないとされている。

※　第15条（データ主体によるアクセスの権利）、第16条（訂正の権利）、第17条（消去の権利（「忘れられる権利」））、第18条（取扱いの制限の権利）、第19条（個人データの訂正若しくは消去又は取扱いの制限に関する通知義務）、第20条（データポータビリティの権利）

34頁

仮名化データの規制緩和は不適当

第4節　データ利活用に関する施策の在り方

（２）「仮名化」の検討

○　ＥＵにおいては、個人情報としての取扱いを前提としつつ、若干緩やかな取扱いを認める「仮名化」が規定され、国際的にもその活用が進みつつある。

○　我が国においても、「仮名化」のような個人情報と匿名加工情報の中間的規律の必要性については、従前から経済界からの要望もあるところであるが、具体的なニーズの有無、開示請求や利用停止等本人関与の在り方を含めた規律の在り方等について、ＥＵの規律のレベルの実態、国際的な動向も踏まえ、具体的に検討していく必要がある。

40頁

仮名化データの規制緩和は不適当

第4節　データ利活用に関する施策の在り方

Article11　第11条

1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

1．管理者が個人データを取扱うための目的が管理者によるデータ主体の識別を要しない場合、又は、その識別を要しなくなった場合、その管理者は、本規則を遵守するという目的のみのために、データ主体を識別するための付加的な情報を維持管理し、取得し、又は、取扱うことを義務付けられない。

2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

2．本条第1 項に定める場合において、管理者がデータ主体を識別する立場にないことを証明できるときは、その管理者は、それが可能であるならば、データ主体に対し、しかるべく通知する。そのような場合、データ主体が、それらの条項に基づく自己の権利の行使の目的のために、自身の識別ができるようにする付加的な情報を提供する場合を除き、第15 条から第20 条は、適用されない。

仮名化データの規制緩和は不適当

Recital (57)
If the personal data processed by a controller do not permit the controller to identify a natural person, the data controller should not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. However, the controller should not refuse to take additional information provided by the data subject in order to support the exercise of his or her rights. Identification should include the digital identification of a data subject, for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller.

前文(57)
管理者によって取扱われる個人データが管理者による自然人の識別を許容しないものである場合、そのデータ管理者は、本規則の条項を遵守するという目的のみのために、データ主体を識別するための付加的な情報を入手することを義務付けられない。ただし、その管理者は、データ主体から自己の権利の行使をサポートするために提供される追加的な情報の取得を拒むことができない。識別には、例えば、データ管理者によって提供されるオンラインサービスにログインするためにデータ管理者から提供され、データ主体によって用いられる同一の認証情報のような認証手段を介するデータ主体のデジタル識別が含まれなければならない。

仮名化データの規制緩和は不適当

第4節　データ利活用に関する施策の在り方

Recital (64) sentence2
A controller should not retain personal data for the sole purpose of being able to react to potential requests.

前文(64) 第2文
管理者は、ありうる要求に対応するという目的のみのために個人データを保持してはならない。

仮名化データの規制緩和は不適当

第4節　データ利活用に関する施策の在り方

- そもそもGDPRにおいて、仮名化データの規律が個人データよりも負荷の軽い規律になっている、とはいえないのではないか。

  - GDPR11条1項は、GDPRの義務を果たす目的のためだけに、本人を識別できる情報を持つ必要はないという趣旨であり、

  - GDPR11条2項は、本人から事業者に対して、本人の個人データに関する請求があった場合に、本人が識別できる情報を持たない事業者は、これに対応しなくていい、ただし、本人が識別情報を提供する場合には、対応すべき、という趣旨。

  - 日本法では、本人が識別できない場合（仮名化のうえ元のDBを消去する場合等）には、原則として個人情報ではないので、そもそも個人情報にかかる義務を負わない。

仮名化データの規制緩和は不適当

- また、仮名化データについての特別な取扱いを認めるとなると、「安全な仮名化データとはどのようなものか」「仮名化データの取扱いについてどのような義務を課すべきか」という議論が当然必要となるが、これは匿名加工情報の在り方の議論と同じものではないか。

スコアリングについての規制

第4節　データ利活用に関する施策の在り方

ＡＩスコアリングについては、Ｊスコアや芝麻信用など、顧客の信用力をスコア化するサービス提供が進展している。
○　こういったＡＩ・ＩｏＴの活用の進展により、多様な分野で新たなサービス等の進展が期待される一方、ビジネス生態系の変化とともに、新たなルールの必要性について指摘する意見もある。

36頁

- AIスコアリングが貸し付けやシェアリングエコノミーにおける信用力評価に留まらず、広く様々な場面で利用されるようになると、スコアリングに用いられる指標への迎合が生じて価値の多様性が失われ、社会が固定化し、イノベーションを阻害するおそれがある。本人の同意に関わらず、利用場面を限定することを検討すべきではないか（e.g. 就職、入学、結婚等に利用しない）。

- (a)指標として用いられる情報と(b)信用力等個人の価値・能力の間の未知の相関性がAIにより明らかにされる可能性がある。不適切な指標による差別が生じないよう、指標として用いられる情報の種類（読書歴、購読する新聞等）を限定することを検討すべきではないか。

ターゲティング広告と個人識別符号の拡大

第4節　データ利活用に関する施策の在り方

ターゲティング広告では、ＰＣやスマートフォン等のブラウザごとのクッキー上に発行されるＩＤに紐付いて蓄積される情報（サイト閲覧履歴等）や、スマートフォン等のＯＳが発行する広告識別子に紐付いて蓄積される情報が使われることが多いとされる。

38頁

特に、最近は、スマートフォンの普及等により、ウェブ上の検索履歴や閲覧履歴のみならず、位置情報を含めた広い意味での行動履歴が利用され得る状況にある。このような幅広い情報を膨大に収集し、解析、利用することについて、プライバシー上懸念があるとの意見もある。

39頁

ターゲティング広告と個人識別符号の拡大

第4節　データ利活用に関する施策の在り方

○　ターゲティング広告のベースとなるウェブ技術は進化が著しく、本来、イノベーションを阻害することを避ける観点からも、まずは、自主ルール等による適切な運用が重要である。自主ルール等については、強制力や自主ルール等に参加していない者の存在など、一定の限界があるのも事実であるが、今後、可能な限り民間の自主性を活かしつつ、認定個人情報保護団体制度等を活用するなど自主ルールを執行可能な形としていくことを含め検討する必要がある。

○　クッキー等について、例えば、一定の要件に該当するものについて個人情報保護法上の個人識別符号とするなど、その位置付けを明確化することも考えられるが、クッキー等自体は、「識別子」としてセッション管理を含め広範に用いられる技術であり、利用特性も多様であることから、現行法の規定に加えて、クッキー等をあえて個別に規律する必要性含め、慎重に検討する必要がある。

41頁

ターゲティング広告と個人識別符号の拡大

第4節　データ利活用に関する施策の在り方

- ターゲティング広告の問題の一つは、多くの情報が突合されるにも関わらず、個人情報でないものとして扱われ、自主規制以外の規律がかからない点にある。

- 多くの情報が突合されれば、必然的に特定の個人を識別できる可能性が高まり、権利侵害の可能性も高まるため、何らかの規律が必要ではないか。

- 平成27年改正の際に、個人が特定されなくても個人が特定されるおそれを招くものを「（仮称）準個人情報」として、規制対象とすることが検討されたが、その際の問題意識はまったく同じであった。

- 特にその性質・特性から多量又は多様な情報を収集することとなる蓋然性が高い識別子を規制対象とすることが提案され、その要素として、①本人との密接関連性、②一意性、③共有性、④不変性を考慮すべきであるとされた。

パーソナルデータ検討会技術検討ワーキンググループ
「（仮称）準個人情報 」及び「（仮称） 個人特定 性低減データ」に関する技術的観点からの考察ついて（中間報告）」6頁

ターゲティング広告と個人識別符号の拡大

第4節　データ利活用に関する施策の在り方

- この議論はやや形を変えて、個人識別符号が導入されることとなった（個人識別性があるものだけが対象）。そこでは、①情報の機能、取扱いの実態等を含めた社会的な意味合い、②情報が一意であるか等、個人と情報との結び付きの程度、③情報の内容の変更が頻繁に行われないか等、情報の不変性の程度、④　情報に基づき、直接個人にアプローチすることができるか等、本人到達性が個人識別符号の選択基準とされた。

瓜生和久　編著 「一問一答　平成27年改正個人情報保護法」14頁

- 平成27年改正の際の問題意識に今般の問題意識を加えて、ターゲティング広告等に用いられる多量又は多様な情報を収集する機能がある識別子を個人識別符号として定義してはどうか。選定の要素としては①本人との密接関連性、②一意性、③共有性、④不変性、⑤本人到達性などが考えられる。

- 具体的には、メールアドレス、携帯電話番号、MACアドレス、スマートフォンの広告ID等がこれに該当するのではないか。

第５節　ペナルティの在り方

課徴金制度を導入すべき

第5節　ペナルティの在り方

○　個人情報保護法では、個人情報取扱事業者に課される罰則について最大でも１年以下の懲役又は50万円以下の罰金とされていることから、現行のペナルティの体系では実効性が不十分な事業者を念頭に、ペナルティの強化が必要との議論がある。
○　平成27年改正法の施行後の国際的状況を見ると、ペナルティの強化が大きな潮流となっているのは否定できない。

46頁

○　なお、域外適用との関係で、罰金等が科せられないことを踏まえ、課徴金制度の導入を求める意見（中略）もあるが、ＷＴＯ協定や環太平洋パートナーシップ協定（ＴＰＰ）で示されている、国境を越えるサービスの提供に関する内国民待遇、最恵国待遇等の原則（いわゆる無差別原則）の考え方や、外国事業者に対する法執行の在り方という視点も踏まえて、検討を深める必要がある。

54頁

課徴金制度を導入すべき

第5節　ペナルティの在り方

- 個人情報取扱事業者に課される罰則は、最大でも1年以下の懲役又は50万円以下の罰金。しかも、海外事業者には適用できない。

- このような状況では、事業者による法令順守を確保して、個人の権利利益を保護することは困難であり、課徴金制度を導入すべきである。

- GDPRとの乖離も大きいが、ルールの国際的ハーモナイゼーションも議論される今日において、このような乖離を正当化する事情があるとは思われない。

第６節　域外適用等

域外適用の条項の追記

第6節　域外適用等

域外適用については、現行法の域外適用の範囲や、執行手法について、各国主権との関係整理の視点も含めて、引き続き検討する必要がある。他の国内法の状況も勘案して検討する必要がある。

53頁

第75条
第15条、第16条、第18条（第２項を除く。）、第19条から第25条まで、第27条から第36条まで、第41条、第42条第１項、第43条及び次条の規定は、国内にある者に対する物品又は役務の提供に関連してその者を本人とする個人情報を取得した個人情報取扱事業者が、外国において当該個人情報又は当該個人情報を用いて作成した匿名加工情報を取り扱う場合についても、適用する。

域外適用の条項の追記

第6節　域外適用等

□　域外適用を定める75条は、明文上は明らかでないが、本人からの直接取得が要件となっている。そのため、本人からの直接取得のない、26条の確認記録義務は、75条の域外適用の対象外となっている。

本法4章1節で定める個人情報取扱事業者の義務等の規定のうち、17条（適正な取得）の規定が含まれていないのは、立法（規律）管轄権の基本である属地主義の考えによれば、外国事業者がわが国に所在する個人情報の本人から個人情報を取得する場合、取得過程の重要な一部はわが国で行われていると考えられるので、域外適用規定を適用するまでもなく、本法の規定が適用されると解されるからである。同様に、（中略）26条（第三者提供を受ける際の確認等）の規定が域外適用の対象とされていないのは、本条が個人情報の本人から直接に個人情報を取得した場合であることを域外適用の要件としているところ、本人からではなく第三者から個人情報を取得した場合はこの要件を満たさないからである。

宇賀克也「個人情報保護法の逐条解説」[第6版]　328頁

域外適用の条項の追記

第6節　域外適用等

- 本人からの直接取得を要件としたのは、わが国と十分な関係性のない外国事業者の取扱いに対する域外適用を認めることには、主権侵害等のおそれがあるからである 。

- しかしながら、本人からの直接取得の有無を、「わが国との十分な関係性」の基準とすることは必ずしも適当ではない。たとえば、日本向けのサービスを提供している外国事業者が、国内事業者から個人情報を取得する場合には、当該外国事業者による個人情報の取り扱いはわが国と十分な関係性を持つものと評価しうる場合がある（e.g.当該外国事業者の日本現地法人から取得する場合）。

- わが国との関係性の有無の判断基準は、「国内にある者に対する物品又は役務の提供に関連してその者を本人とする個人情報を取得した」か否かのみで判断すべきである。

- 本人からの直接取得要件を不要とすることにより、26条等の本人からの直接取得の場面でない条項を、域外適用の対象条項として75条に追記すべきである。

域外適用の条項の追記

第6節　域外適用等

- この点についてのGDPRの規定は、以下のいずれかに関連する場合に域外適用されるというもの
  - EU域内の本人に対する物品もしくはサービスの提供
  - EU域内の本人の行動の監視

- 本人からの直接取得は要件になっていない。

第３条地理的適用範囲
1．本規則は、その取扱いがEU 域内で行われるものであるか否かを問わず、EU 域内の管理者又は処理者の拠点の活動の過程における個人データの取扱いに適用される。
2．取扱活動が以下と関連する場合、本規則は、EU 域内に拠点のない管理者又は処理者によるEU 域内のデータ主体の個人データの取扱いに適用される：
(a) データ主体の支払いが要求されるか否かを問わず、EU 域内のデータ主体に対する物品又はサービスの提供。又は
(b) データ主体の行動がEU 域内で行われるものである限り、その行動の監視。

第7節　その他

条例の統一化、委員会の所管の拡大

第7節　その他

具体的には、行政機関、独立行政法人、地方公共団体、民間事業者等の法律等の統合を求める意見や、委員会が行政機関や地方公共団体における個人情報の取扱いについても所管することを求める意見等があった。この論点に関する政府としての検討に際しては、委員会としても適切に対応していく必要がある。

56頁

- 条例がバラバラなのは、実務的にはデータ利活用の大きな障害になっている。
- 委員会の所管の拡大なくしては、十分な保護を図ることができない。海外からの評価も低く、特にガバメントアクセスに対して委員会が適切な抑制を行うことは、十分性認定の維持にも不可欠ではないか。
- 1条に「プライバシーの保護」を明記して、プライバシーに対する所管を明確にしてはどうか。

ｸﾞﾚｰｿﾞｰﾝの解消ー生成は取得と解すべきである

第7節　その他

- 特に要配慮個人情報の文脈で、事業者が内部において要配慮個人情報を生成する行為が「取得」にあたるものとして、本人の同意を要するかが議論になっている。

- 事業者が内部で生成する場合であっても、外部から取得する場合であっても、権利侵害のおそれは変わらない。

- 今後、AIの浸透により、さらに容易に要配慮個人情報を生成することが可能になるため、歯止めが必要である。

- 要配慮個人情報以外にも、内部で生成される情報（たとえば従業員の評価情報）は存在するが、これらに対して、利用目的の通知等に関する18条※が適用されなくなるのは、不適当である。

※「個人情報取扱事業者は、個人情報を取得した場合は～」

ｸﾞﾚｰｿﾞｰﾝの解消ー要配慮個人情報の可能性

第7節　その他

- 要配慮個人情報の可能性、たとえば「キリスト教徒の可能性がある」という情報が要配慮個人情報に該当するかについて議論がある。

- このような可能性も、要配慮個人情報と解すべきである。

- 「可能性」、「蓋然性」等を付記しただけで、要配慮個人情報でなくなるとすると、規制の実は完全に失われる。

ご清聴ありがとうございました