

パーソナルデータ保護法制に 向けた最近の動向

産業技術総合研究所
セキュアシステム研究部門
高木 浩光

個人情報売買解禁へ？

● 日経新聞報道 2012年11月29日

- 「民間の個人情報売買解禁へ 政府、新事業創出を後押し」

「政府が経済対策に盛り込む**規制改革案**が明らかになった。企業や病院などが持つ**個人情報**を匿名化したうえで他の企業に**売買できる新ルール**をつくり、新商品の開発や新規ビジネスの創出を後押しする。

政府が30日に閣議決定する経済対策（略）情報の出し手として患者データを保有する病院や、POSデータを持つスーパーなど流通業を想定（略）

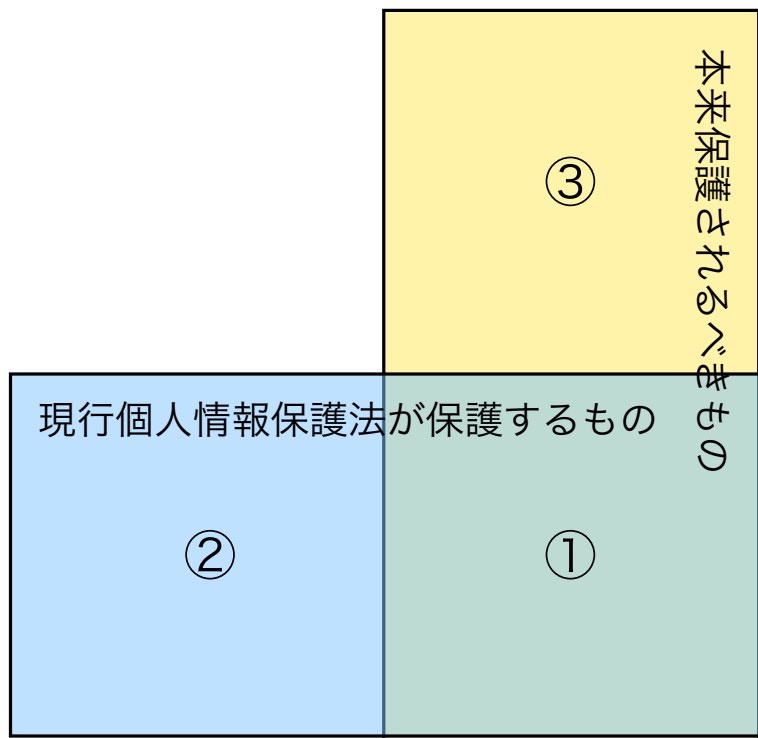
情報の出し手側が**住所の一部や氏名、電話番号など個人を特定できる情報を削除したデータを作成**。その情報を製造業などが買い取り、地域や年齢層に応じた新商品の開発や市場調査に生かせるようにする。**複数の機関や企業から個人情報を集めて加工・分析し、企業に情報提供する新たなビジネス**が生まれる可能性もある。（略）

個人の間では**情報流出への不安も強い**とみられ、政府は**2013年秋をメドに個人情報**をどこまで隠せば「匿名化」とみなせるかを明確にしたルールをつくる方針だ。早ければ13年の臨時国会に個人情報保護法改正案を提出する。」

ここ半年の動き

- 総務省 パーソナルデータの利用・流通に関する研究会
 - 情報セキュリティ対策室 10月設置、6月報告書
 - 個人情報保護法を超越した保護・利活用の制度を提案
 - 妥当な落とし所へ制度を変えようとする方向性
- 経産省 IT融合フォーラム パーソナルデータWG
 - 情報経済課 11月設置、5月報告書
 - 消費者と事業者の信頼関係の構築 有効な同意の確保へ
 - 現行法の下、事業者に誠実なサービス提供を促す方向性
- 内閣府 規制改革会議 創業等WG
 - 内閣総理大臣諮問 1月設置、3月～5月WG、6月答申
 - 氏名住所削除で匿名データとみなそうとするが失敗
 - 現行法を無視してガイドラインで合法化を目指す方向性

現行法と期待される将来



「世界最先端IT国家創造宣言」

● 内閣 IT総合戦略本部, 6月14日

- 「「ビッグデータ」のうち、特に利用価値が高いと期待されている、個人の行動・状態等に関するデータである「パーソナルデータ」の取扱いについては、その利活用を円滑に進めるため、**個人情報及びプライバシーの保護との両立を可能とする事業環境整備を進める**。また、環境整備に当たっては、プライバシーや情報セキュリティ等に関するルールの標準化や国際的な仕組み作りを通じた利便性向上及び国境を越えた円滑な情報移転が重要であり、OECD等国際交渉の場を活用し、国際的な連携を推進する。既に、スマートフォンの利用者情報の取扱いなど先行的にルール策定が行われた分野については、取組の普及を推進する。

また、**速やかにIT総合戦略本部の下に新たな検討組織を設置し**、個人情報やプライバシー保護に配慮したパーソナルデータの利活用のルールを明確化した上で、**個人情報保護ガイドラインの見直し、同意取得手続の標準化等の取組を年内できるだけ早期に着手するほか、新たな検討組織が、第三者機関の設置を含む、新たな法的措置も視野に入れた制度見直し方針（ロードマップを含む）を年内に策定する**。

さらに、2014年以降に、制度見直し方針に示されたロードマップに従って、国際的な連携にも配慮しつつ、順次パーソナルデータ利活用環境を整備し、利活用を促進する。

規制改革会議 創業等WG

● 答申より

- 「**ビッグデータの利用を阻害する理由の一つとして個人情報保護法に起因する問題**が指摘されており、例えば、事業者にとって、個人情報の利用のルールが明確でないため、どのような利用であれば適正といえるかの判断が困難である、事業者が消費者の反発によるリスクを感じ個人情報の利用を躊躇しているといった旨の指摘がある。

遊休・無形の資産たるビッグデータの利用を促進する観点から、**国際先端テストの視点も踏まえ**、どの程度データの加工等を実施すれば個人情報に当たらず、**個人情報保護法の制限を受けることがなくなるのかを明確化するためのガイドライン**を策定する等、いわゆる匿名化された情報の個人情報保護法上の取扱いの明確化を行う。」

国際先端テストの結論（消費者庁）

- 「匿名化情報の利用に関する日本と欧米の制度の比較」
 - 「例えば、上記「X1234」が週3日以上ワインを飲んでいる」という事例について（略）事業者が「X1234」を氏名等の識別情報と結び付ける「対応表」を保有しているのであれば、「週3日以上ワインを飲んでいる」という属性情報を含め、「個人データ」に該当することになる一方、「対応表」を廃棄するなどして識別情報と結び付かないように管理しているのであれば、当該属性情報は「個人データ」には該当しないこととなる。（略）

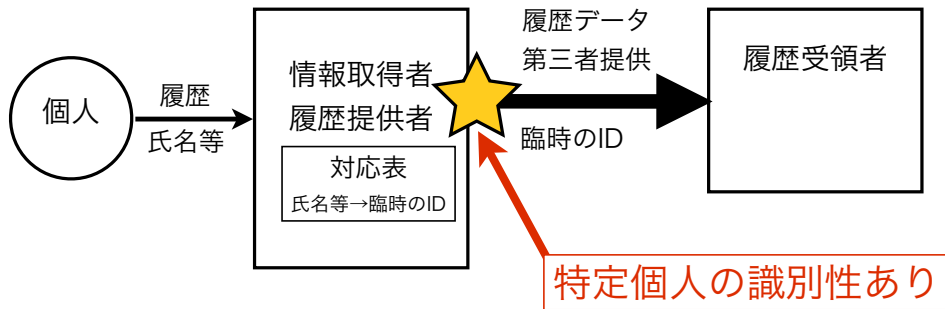
このように、日本の法制度は、欧米と比較して匿名化情報の利用に関して厳しい規制を設けているものではなく、（略）例えば「対応表」を廃棄するなど、特定個人を識別できないような対応を事業者が施すことにより（欧米と同様）、属性情報や履歴情報の利活用を図っていくことは可能である。」
 - この意味するところは……。

「個人情報」の定義（現行法）

- 個人情報保護法での定義
 - この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述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を含む。）をいう。
- 法解釈上の論点
 - 「識別することができる」は誰によって識別という話か？
 - 提供者基準（消費者庁及び経産省ほか政府説、鈴木説）
 - 受領者基準（岡村説）
 - この解釈は特に、照合により識別できるかにおいて重要となる

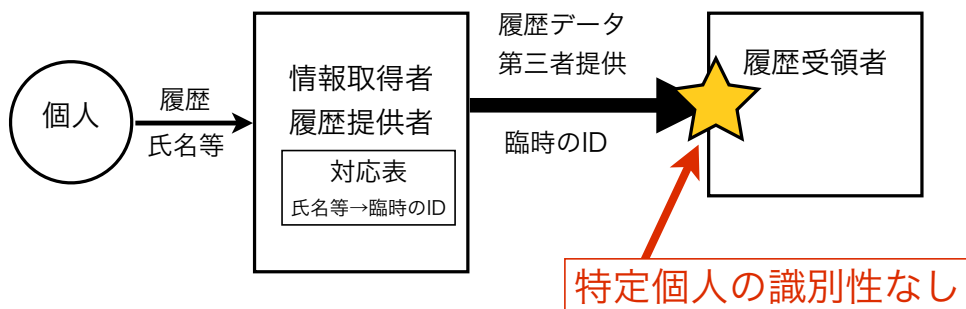
提供者基準 個人識別性

● 政府説



- 消費者庁の規制改革会議への回答はこれに依拠している
 - 提供する時点で「対応表を廃棄」していれば、特定個人の識別性はないことになる
 - データを提供する時点でそのデータが提供者において照合できるか
 - 提供先で照合できるかは関係ない

受領者基準 個人識別性



- 岡村説ほか
 - 一部の事業者がこれを正当性の理由にしつつある

岡村説

● 岡村久道, 個人情報保護法 新訂版, 商事法務, 2009

- p.76より「このような基準を前提にすると、情報を保有する事業者Aが、これをマーケティング等に自ら利用する場合には、Aにとって識別性が具備されているか否かを基準にすれば足りる。これに対し、Aにとって識別性を具備する情報を、これを具備しないBに提供する場合には、第三者提供の制限（法23条1項）違反とならないものと考えらるべきである。Bにとどまらず通常人からみても誰の情報なのか識別できない以上、その提供によって、本法が想定する権利利益侵害のおそれが本人に通常発生するとは認められないからである。また、かく解さなければ、本人の権利利益を図るため、特定の個人を識別しうる部分を番号・符号に置き換える方法を用いて匿名化したデータを第三者提供することすら許容されなくなりがねない。これと反対に、Aにとって識別性を具備しない情報を、これを具備するBに提供するケースは、理論上は想定できても、実際に発生しうるか疑問である。」
- 実際に生じ得る「権利利益侵害のおそれ」を重視する実質論に基づく説とみられる

● 「実際に発生しうるか疑問」は誤りと言わざるを得ない

- 最近では一部の事業者で該当する行為が行われている

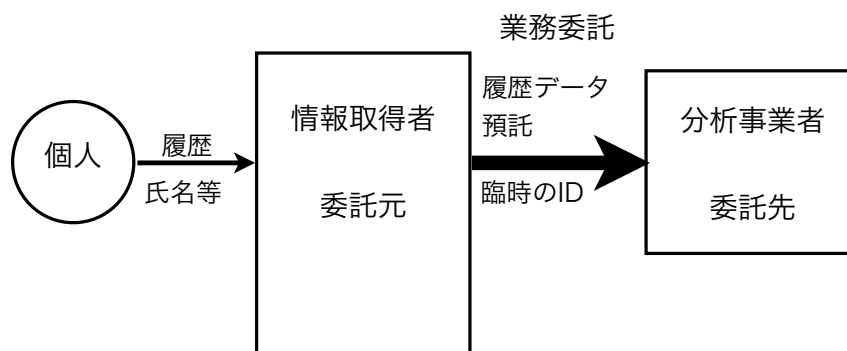
● X（識別性あり） Y（識別性なし） Z（識別性あり）を想定していない

- X Zによって「権利利益侵害のおそれ」が生ずるので、前半のA Bで「権利利益侵害のおそれが本人に通常発生するとは認められない」とされているのと矛盾

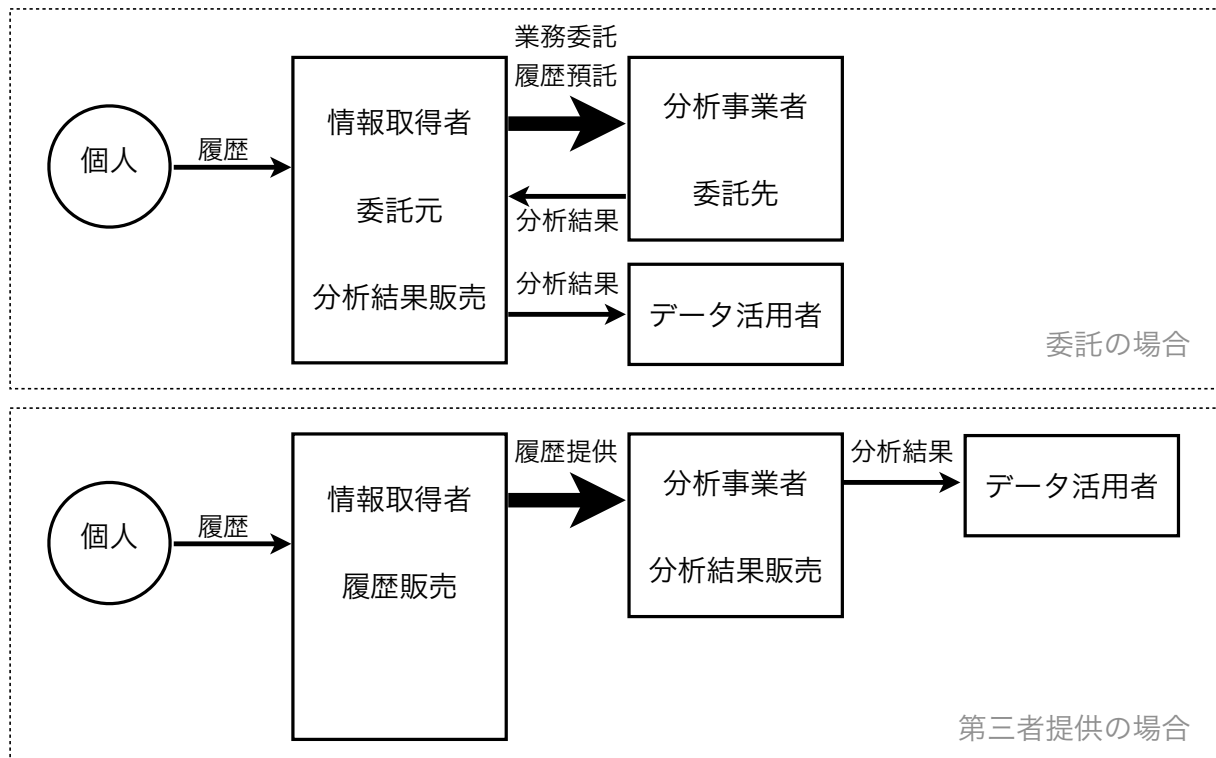
業務委託との混同に注意

● データ分析の業務委託の場合（政府説での理解）

- 委託契約の下で履歴データを提供（預託）する
- データから氏名等を削除して臨時のIDを付して渡すのが通例
 - その意図は、安全管理措置として事故時の被害を軽減するためであり、個人データの提供に当たらず（個人情報に該当しなくする）ためではない
 - 委託先は委託元と一体であるから委託先においても個人データ



履歴データの分析処理と活用



履歴データ第三者提供の現行と将来

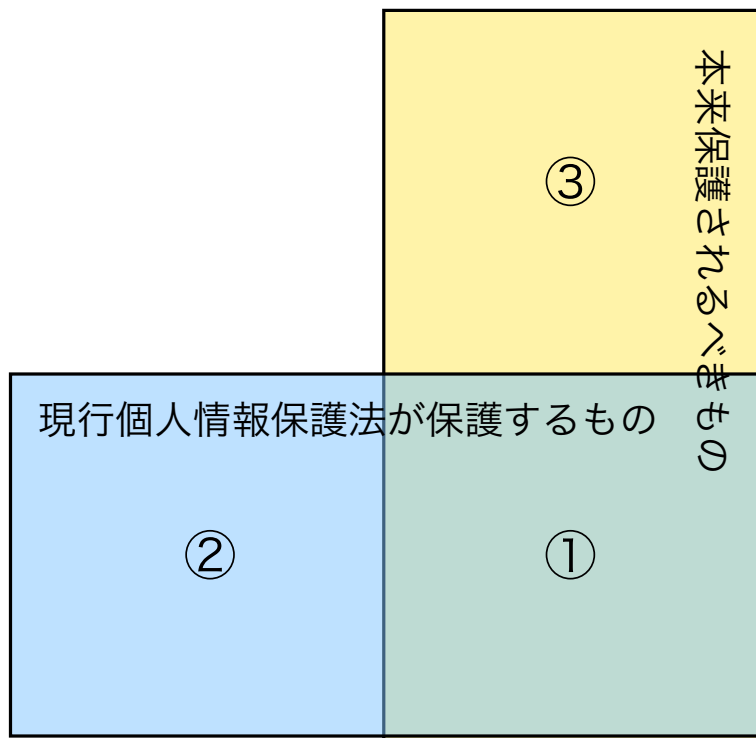
	提供するデータの構成	現行の個人情報保護法での解釈	本来あるべき保護の形	利用価値
a	イベント1件ずつバラバラのデータ (個人毎の識別子が無い)	個人情報に該当しない	保護の必要なし	小
b1	個人毎のイベントのリストであり、個人毎の識別子が付されているが、提供の都度それがランダムに付番されなおすデータ	個人情報に該当しない (※消費者庁国際先端テスト結果結論における「対応表を廃棄する場合」に相当)	保護されるパーソナルデータ (※総務省パーソナルデータ研究会による) FTC3要件を満たすなら保護対象外としてよい?	中～大 (提供の区切り期間の長さによる)
b2	個人毎のイベントのリストであり、個人毎の識別子が付されており、複数回の提供をまたがって識別子が共通であるデータ	個人情報に該当する (※提供元において「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」となるもの) に当たる)	保護されるパーソナルデータ (※総務省パーソナルデータ研究会による) FTC3要件を満たすなら保護対象外としてよい?	大
c	何らかの匿名化処理が施されたデータ	?	?	小～大

前提：氏名、生年月日及び、住所、電話番号等の連絡先情報が排除されているデータについて

現行法の不備

- 前表において
 - b1かb2かで、無断第三者提供が合法か違法かに分かれる
 - b1も本来保護すべきデータであるのに合法
 - b2でも自由に利活用してよい場合があるかもしれないのに違法
 - b1とb2では、プライバシーインパクトは変わらない
 - 注：b1ならば、対応表を捨てなければならないので、複数回に渡って提供する場合において、結果として、同一人として識別できる履歴の期間が短くなることから、プライバシーインパクトを小さくする効果があるかのようなのであるが、以下の脱法的手段が存在するため、プライバシーインパクトはb2と変わらない
 - 例えば毎日1回データを提供するとき、その都度、対応表を廃棄して新たな臨時IDを付して提供するが、提供する履歴データは過去履歴の全部（数日、数か月、数年前のデータを含む全部）とすることで、現行法で合法とした上で、b2と変わらない利用価値が得られる
 - 現行法の線引きは実質論的期待からかけ離れている

現行法と期待される将来



総務省パーソナルデータ研究会報告書

- 「実質的個人識別性」の導入
 - p.24 「ここで、プライバシーの保護というパーソナルデータの利活用の基本理念を踏まえて実質的に判断される個人識別性を、概念上明確にするため、「実質的個人識別性」と呼ぶ（略）*54。」
 - 脚註54 「なお、個人情報保護法の「個人情報」の要件である個人識別性も「特定の個人を識別することが『できる』」として蓋然性・可能性を要件として規定されており（諸外国等のidentifi[able]、link[able]なども同様。）、その該当性判断に当たっては法の趣旨に従って判断することが必要となるため、同様の実質的な判断を行うことは文言上は除かれてないと考えられる。しかしながら、（略）引き続き検討していくことが必要であると考えられる。」
- 実質的個人識別性のある「保護されるパーソナルデータ」の例示
 - 継続的に収集される購買・貸出履歴、視聴履歴、位置情報等
 - 個人のPCやスマートフォン等の識別情報
 - 「実質的に特定の個人と継続的に結びついており」

FTC3要件とは？

- 総務省パーソナルデータ研究会で言及
 - 規制改革会議答申でも言及
 - 以下を条件に「保護されるパーソナルデータ」から除外する
 - 1. 適切な匿名化措置を施していること。
 - 2. 匿名化したデータを再識別化しないことを約束・公表すること。
 - 3. 匿名化したデータを第三者に提供する場合は、提供先が再識別化をすることを契約で禁止すること。
 - FTCレポート2012でも類似の記述あり
 - (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form, that data will fall outside the scope of the framework.
 - A company that violates its policy against re-identifying data could be subject to liability under the FTC Act or other laws.

非識別化の意義

- 「非識別化」の多義性
 - k-匿名化のようにひとりの人に対応しないデータにすることを指すのかそれとも、単にlinkableでなくすることなのか
- linkableでなくする解釈の場合
 - 本人リーチする目的の場合と、しない目的の場合がある
 - 本人リーチする目的の場合
 - 行動ターゲティング広告に利用する目的など
 - 「保護されるパーソナルデータ」であるべき
 - 「対応表」が存在する
 - 本人リーチしない目的の場合
 - 統計データに加工して利用する目的など
 - FTCでは3要件を満たせば will fall outside the scope of the framework とされている
 - 「対応表」を必要とする場合と必要としない場合がある

個人識別性の範囲

- 少なくとも4つがある
 - 特定個人識別性（氏名生年月日その他の記述により特定の...）
 - 米国消費者プライバシー権利章典
 - 特定の消費者、コンピュータその他デバイスに合理的にリンクできるもの
 - 実質的個人識別性（総務省パーソナルデータ）
 - 継続的に収集される履歴、位置情報等を含む
 - 不特定個人識別性
 - 特定の個人は識別されていないが、ひとりひとりが別々の人として識別されている

特定個人識別性 _____

米国消費者プライバシー権利章典(?) _____

実質的個人識別性 _____

不特定個人識別性 _____

