論　説

ビッグデータの利活用における パーソナルデータ取扱い上の法的留意点

鈴　木　　優*
村　上　諭　志**

抄　録　本稿は，ビッグデータを利活用するに際して，事業者がパーソナルデータの適切な保護の観点から留意すべき事項を平易に解説するものである。一般にビッグデータの価値はその情報量の規模に比例し，それ故，ビッグデータを取り扱う事業者の中には，より多くの情報を収集することのみに注力し，いわゆる情報コンプライアンスを疎かにする傾向がないわけではない。しかしながら，プライバシーの適正な保護と情報コンプライアンスが要請される現代社会においては，データ収集から利活用に至る全ての局面において，個人情報保護法及びその各種ガイドライン等の法令を遵守する必要性は一層高まっている。昨年，個人情報保護法が全面的に改正・施行され，パーソナルデータの利活用促進が叫ばれているなか，法令のクリアランスを含めて適切に応じる企業姿勢が重要である。

目　次

1．はじめに

ビッグデータ[1)]は，ビジネスや社会に革新的なイノベーションをもたらすポテンシャルを持つ，重要な「資源」である。現代社会では，ビッグデータの利活用を通じて，消費者にとってより良いサービスが実現され，企業における業務の迅速化・効率化が図られ，社会システムのより効率的な運営が図られることなどが期待されている。このようなビッグデータの利活用への期待が膨らむ背景には，我々の日常生活から生じる様々な情報を収集するスマートフォンや膨大な情報をリアルタイムで格納できるクラウドの登場，そして，データの分散処理技術[2)]の発達がある。このデータ分散処理技術は，多数のサーバを用いて膨大なデータを分散処理できるようにするばかりでなく，そのデータを高速かつ低コストで処理することを実現した。

近年のデータ分析技術の発展は，分析処理できるデータの範囲をも拡大した。すなわち，新たなデータ分析技術は，従来の技術では分析が困難であった，ブログ，Facebook，twitter等のソーシャル・ネットワーク・サービス（SNS）に投稿された画像及び映像等の構造化されていない情報，いわゆる「非構造化データ」を大量に分析処理することを可能にした。このように非構造化データを分析対象に加え，これを構造化データと統合して様々な角度で分析すること

* 弁護士　Masaru SUZUKI
** TMI総合法律事務所　弁護士　Satoshi MURAKAMI

により，事業者が顧客の購買動向等をより正確に把握することが可能になった[3]。例えば，マーケティングの領域においては，顧客の購買履歴や趣味嗜好のデータに基づき商品・サービスをリコメンドする機能，及び顧客の趣味嗜好に沿った広告を掲載するターゲティング広告等が登場した。また，顧客の所在する場所を示す位置情報ないしはその移動履歴を利用して，顧客に対するサービス向上に繋げる試みも行われている。例えば，ある事業者が個人の位置情報から構成される移動データを第三者に販売し，当該第三者がそのデータを活用して消費者の位置から近い店舗に関する広告をリアルタイムで配信するサービス，宿泊施設内でのセンサーで宿泊客の行動を把握することで，業務の自動化や宿泊客に対するサービスの向上に繋げる仕組みなどがある。

これらのビッグデータを用いたビジネス（以下「ビッグデータビジネス」という。）においては，気象や海況データのように個人と全く関係がない場合を除き，個人のプライバシー保護の観点から生じる課題を克服する必要がある。すなわち，ビッグデータビジネスでは，住所・年齢・職業・性別等の属性情報，趣味や嗜好に関するデータ，保有する資産や健康状態に関するデータ，ウェブの閲覧履歴や商品・サービスの購買履歴等が収集されることが多く，これらの情報は，特定の個人を識別することが可能な情報ないしは顧客のプライバシーに関わる情報（以下，本稿では，個人情報及び個人のプライバシーに関わる情報を「パーソナルデータ」と総称する。）である[4]。万が一企業が顧客のプライバシーの保護を全く考慮することなく，ビッグデータビジネスにパーソナルデータを利用するとすれば，その顧客に疑念を抱かれるに留まらず，社会全体から批判を向けられるリスクがある（いわゆる「炎上リスク」）。それ故，ビッグデータビジネスを成功に導くためには，プライバシーの保護の観点から法令に従い適切な配慮を行うことにより，顧客及び一般社会との間で信頼関係を構築することが大切である。この点，パーソナルデータの一部は，「個人情報の保護に関する法律」（以下「個人情報保護法」または単に「法」という。）で保護される[5]。しかしながら，個人情報保護法上の規制のみ留意すれば良いのではない。プライバシーの重要性が認知されている現代社会においては，cookie情報や特定の個人を識別できないIoTデータ等の個人情報保護法でカバーされないパーソナルデータであっても，プライバシーの観点から保護すべき情報については，事案に応じて事前に情報主体の同意を取得したり，パーソナルデータの取扱いを詳細に公表するなどの適切な対応が求められる（詳細は，後記2．5）。

本稿は，事業者がビッグデータを利活用するに際して，パーソナルデータの取扱上の留意点を検討するものである。なお，本稿において，便宜上，ビッグデータとして取り扱われるデータをまず大きく「個人情報ではないパーソナルデータ」と「個人情報」に分け，そのうえで，後者の「個人情報」に該当する情報を「個人情報」として利用する場合，「匿名加工情報」として利用する場合，「統計データ」として利用する場合の３種に分類する。

2．日本の個人情報保護法制に照らしたビッグデータ利活用の在り方

2．1　個人情報ではないパーソナルデータと個人情報の分類

ビッグデータを利活用するにあたっては，まず，自らが取得するパーソナルデータが法の規制を受ける個人情報であるのか，それとも個人情報ではないのかを理解することが検討の出発点となる。個人情報保護法でカバーされないパーソナルデータであっても，適切に対応すべき

ことは前述のとおりであるが，法律上の規制がかからないのであれば，利活用の自由度も高まるといえる。したがって，ビッグデータを取得して何をしたいのかを検討し，その結果を得るためにそもそも特定の個人を識別できる個人情報を取得しなくてもよいのであれば，そのような情報を取得しないという選択肢も十分に検討されるべきである。したがって，ここでは，まず個人情報の定義を確認しておきたい。

(1) 個人情報とは

「個人情報」とは，生存する個人に関する情報であって，その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，又は個人識別符号が含まれるものをいい，それ単体では特定の個人を識別することができなくても，これと容易に照合することができる他の情報を補うことによって，特定の個人を識別することができる情報も個人情報に含まれる[6)]。また，平成29年の改正（以下「平成29年改正」という。）では，これまでグレーゾーンとなっていた「個人識別符号」が個人情報に含まれることが明確化された。「個人識別符号」とは，次のいずれかに該当する文字，番号，記号その他の符号であって，特定の個人を識別することができるものとして政令で定めるものをいう[7)]。

① 特定の個人の身体の一部の特徴をコンピュータで用いるために変換した符号
② 個人ごとに異なるものとなるように役務の利用，商品の購入，又はカードその他の書類に付与される符号

①の具体例としては，顔認識データ，音声認識データ，指紋認識データ，DNA等が，また，②の具体例としては，パスポート番号，運転免許証番号，個人番号（マイナンバー）等が挙げられる。

(2) 実務的に個人情報該当性が問題となるケース

上記の個人情報の定義を踏まえ，たとえば，以下のような場合に個人情報該当性が問題となりうる。

1）購買データ/POSデータ

スーパーマーケット等の小売店において，店舗における販売戦略の分析のために，売れた商品，時間，店舗名，個数，値段等の購買データを取得している場合がある。また，レジにおける販売員が見た目で推測した購入者の性別，年代等を入力しているケースもある。これらのデータは，通常特定の個人を識別できる情報ではないことから，個人情報に該当しないといえよう。一方，ポイントカードや会員カードを通じて，各個人の購買データを取得する場合もある（ID-POSデータ）。このような場合には，上記購買データとポイントカードや会員カードにおける登録データを容易に照合することができるため，ポイントカードや会員カードにおいて個人情報を登録させている場合には，購買データについても個人情報に該当することになる。なお，リアル店舗ではなく，インターネットを通じたe-コマースにおいては，必然的に配送先等の個人情報を取得することになるため，各個人の購買データとして管理している場合には，個人情報に該当する。

2）IoT機器や監視カメラを通じて取得される観測データ

店舗における監視カメラを通じて店舗内の様子を撮影して店舗効率化やマーケティングに利用する場合や，家庭内に設置された機器のセンサーを通じて生活者の行動を把握するような場合がある。

前者の監視カメラの事例の場合，個人の顔を撮影して保存している場合には，解像度にもよるが基本的には当該情報で特定の個人を識別できる場合が多いといえ，その情報は個人情報に

該当するといえる。一方で，あえてモザイクをかけた状態で撮影されたデータを保存したり，顔から推定される年齢，性別等の属性情報を瞬時に判別したうえで，顔の部分を削除して，付された属性情報のみを保存するような場合には，個人情報を取得していないともいいうる。

後者の家庭内での機器のケースでは，機器の仕様次第であるが，たとえば生活者の顔画像等は取得せず，家電を利用した回数等のみを取得しているケースでは，個人情報を取得していないといえる。一方で，当該機器を設置した生活者の情報を別途取得している場合（たとえば，機器に付された番号で当該機器の購入者の氏名・住所が分かる場合や，位置情報を取得している場合等）には，これらの情報と機器から取得される情報が容易に照合できる場合があり，そのような場合には，機器から取得される情報についても個人情報に該当しうる。

3）ウェブ閲覧履歴データ

近時，cookie等を通じてウェブの閲覧履歴を取得し，ウェブ閲覧者の趣味・嗜好を分析し，各個人にマッチした広告を配信するターゲティング広告技術の進展が目覚ましい。このようなウェブ閲覧履歴については，それ単体では，特定の個人を識別することができないが，会員制のサイト等で，氏名等の個人情報を入力しているような場合には，当該登録情報とウェブ閲覧履歴を容易に照合できることが通常であり，そのような場合には，ウェブ閲覧履歴は個人情報に該当しうる。また，cookie情報とオフラインで取得した情報を掛け合わせることによりターゲティングの精度を向上させる等各事業者において様々な手法が構築されており，データの項目がリッチになればなるほど個人の識別リスクは高まるといえる。この分野における個人情報該当性の判断については，各事業者における実際の取扱いに応じた検討が必要となる。

2. 2 「個人情報」として利用する場合

上記2. 1での検討を踏まえ，取得する情報が個人情報に該当する場合には，当該情報にかかる個人情報保護法の規制を遵守する必要がある。この2. 2では，取得した個人情報を，そのまま個人情報として利用する場合について検討する。この類型では，仮にデータを匿名化するとデータの利用目的が達せられなくなる場合やデータの匿名化ないし統計処理が現実的でない場合等が想定される。例えば，介護施設が利用者から取得した介護データを第三者に委託して分析し，その分析結果に基づきその利用者に対するより良い介護サービスを提供しようとする場合には，取得した介護データを匿名化することは意味をなさない。このようなビジネスモデルにおいては，個々の利用者を識別できることが重要な要素となるからである[8)]。このようにビッグデータが個人情報を含む場合には，その取得，保管・管理，利用等のそれぞれの局面で，個人情報保護法が定める規制を遵守しなければならない。

(1) 個人情報の取扱い（提供以外）に関する規制

1）取得に関する規制

まず，個人情報の取得に際して，個人情報取扱事業者は個人情報を取扱うに際して，その利用目的をできる限り特定しなければならない[9)]。また，個人情報取扱事業者は，偽りその他不正の手段により個人情報を取得することが禁止されている[10)]。さらに，個人情報取扱事業者は，取得に際してあらかじめその利用目的を公表している場合を除き，原則として，速やかに，その利用目的を本人に通知し，または公表しなければならないこととされている[11)]。加えて，本人から直接書面（電磁的記録を含む）に記載された個人情報を取得する等の場合には，あらか

じめ本人に対してその利用目的を明示する必要がある[12]。ただし，以上とは異なり，対象となるデータが要配慮個人情報に該当する場合には，原則として，あらかじめ本人の同意を得ないで，要配慮個人情報を取得してはならない[13]。要配慮個人情報は，平成29年改正により新設された概念であり，本人の人種，信条，社会的身分，病歴，犯罪の経歴，犯罪により害を被った事実その他本人に対する不当な差別，偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう[14]。政令において医師等による健康診断その他の検査の結果等も要配慮個人情報に含まれることとされているので[15]，ヘルスケアデータを活用する際には留意が必要である。

２）利用，管理に関する規制

次に，個人情報の利用，管理に関する規制について述べるが，取得以後の取扱いに関する規制は，個人情報ではなく個人データに課せられる。個人データとは，個人情報データベース等を構成する個人情報をいい[16]，個人情報データベース等とは，これに含まれる個人情報を，容易に検索することができるように構成した個人情報の集合物をいう[17]。個人情報取扱事業者は，個人データを利用目的の達成に必要な範囲において，個人データを正確かつ最新の内容に保つとともに，利用する必要がなくなったときは，当該個人データを遅滞なく消去するよう努めなければならない[18]。また，その取り扱う個人データの漏えい，滅失または毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない[19]。このほか，従業者の監督[20]，委託先の監督を行わなければならない[21]。

個人情報の提供を行わない場合の個人情報に係る規制は上記のとおりであり，個人情報を取得した企業が自社でその情報を利活用する場合には，その利活用があらかじめ通知または公表した利用目的の範囲内にとどまっている限りにおいて，本人の同意を取得する必要はなく（ただし，前述のとおり要配慮個人情報を除く。），特段利活用の障害になる規制は多くないといえよう。この場合には，自社において個人情報をどのような目的で使う戦略なのか，事前の利用目的の設定が重要になる。

一方で，ビッグデータの利活用においては，そのデータを第三者に対して販売するビジネスモデルもあり，その場合，個人データの第三者提供に関する規制がかかるため，当該規制のクリアランスが必要となる。

(2) 個人データの提供に関する規制

個人データを第三者に提供する際には，原則として，本人の同意を得なければならない[22]。したがって，個人データを第三者に提供する場合には，まず本人の同意を取得することを検討することになる。ここで，留意する必要がある点として，個人データにおける一定の項目（例えば，氏名）を削除する等の匿名化を行い，提供先が特定の個人を識別できない形で個人データを提供するような場合であっても，後述の匿名加工情報といえない限り，本人の同意が必要になるということが挙げられる（提供元基準説）。一方で，この第三者提供規制には，後述１）から３）のような例外があり，当該例外事由に該当するか否か（例外規定の利用）を検討することは有益である[23]。

１）委　託

利用目的の達成に必要な範囲内において，個人データの取扱の全部又は一部を委託することに伴い，個人データを提供する場合には，本人の同意は不要である[24]。この例外は，従来から実務において広く利用されており，ビッグデータ利活用の側面においても，データの分析を委託する場合等に利用される。もっとも，平成29

年改正により導入された個人情報の国外移転規制があり[25]，委託先が外国企業である場合には，直ちにはこの例外に該当しないため，留意が必要である（後記ウ参照。）。

２）共同利用

個人データを含むデータを広く共有する方法の一つに「共同利用」[26]の手法がある。すなわち，特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって，以下の各事項について，提供にあた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いているときには，第三者提供に該当しない。より具体的には，提供元の企業のウェブサイトにおいて掲載されるプライバシーポリシーに以下の各事項を記載するのが通常である。

① 特定の者との間で共同して利用される個人データが当該特定の者に提供される旨
② 共同して利用される個人データの項目
③ 共同して利用する者の範囲
④ 利用する者の利用目的
⑤ 当該個人データの管理について責任を有する者の氏名または名称

このような個人データの共同利用は，通常，グループ企業間で用いられることが多い。しかしながら，共同利用の方式を用いることで，後述の匿名加工情報の制度を利用しなくても，本人の同意を得ることなく，複数事業者間で個人データをシェアすることができることから，ビッグデータの利活用の共通の目標を掲げる企業間でも共同利用を行うことは有益と思われる。

３）オプトアウト

第三者に提供される個人データについて，本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって，次の①ないし⑤の事項について，個人情報保護委員会規則で定めるところにより，あらかじめ本人に通知し，または本人が容易に知り得る状態に置くとともに，個人情報保護委員会に届け出たときは，あらかじめ本人の同意を得ることなく，個人データを第三者に提供することができる（オプトアウトによる第三者提供[27]）。このオプトアウトについては，平成29年改正において，個人情報保護委員会への届出が要求され，また個人情報保護委員会は届出を受けた場合に，当該届出を公表することとされており[28]，規制が強化されているため，実務的には，本人の同意を取得しえないような場合のほかは利用しづらい状況にあるといえる。

① 第三者への提供を利用目的とすること
② 第三者に提供される個人データの項目
③ 第三者への提供の手段または方法
④ 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること
⑤ 本人の求めを受け付ける方法

なお，要配慮個人情報については，第三者提供の際に，オプトアウトを用いることができないこととされている[29]。

また，平成29年改正により，個人データのトレーサビリティを確保する観点から，個人情報取扱事業者は，第三者に個人データを提供する場合には，表１に記載のような提供先である第三者の氏名等の一定事項を記録し，原則として作成してから３年間保存しなければならないこととされた[30]。また，第三者から個人データの提供を受ける場合にも，提供者の氏名や個人データの取得経緯等の一定事項を確認したうえ，同事項を含む表２に記載の事項を記録し，原則として作成してから３年間その記録を保存しなければならない[31]。この記録義務についても，個人データの第三者提供の際のコスト要因の一つになりうる。

(3) 個人データの国外移転規制

以上にかかわらず，平成29年改正により，個人データの提供先となる第三者が外国にある場

表１　提供者の要記録事項

	提供年月日	受領者の氏名，名称等	本人の氏名その他本人を特定するに足りる事項	個人データの項目	本人の同意を得ている旨
オプトアウトによる提供	○	○	○	○	
本人同意による提供		○	○	○	○

表２　受領者の要記録事項

	提供年月日	提供者の氏名，住所，代表者の氏名←確認事項	取得の経緯←確認事項	本人の氏名その他本人を特定するに足りる事項	個人データの項目	委員会によりオプトアウトが公表されている旨	本人の同意を得ている旨
オプトアウトによる提供	○	○	○	○	○	○	
本人同意による提供		○	○	○	○		○

合には，個人情報取扱事業者は，原則として，あらかじめ外国にある第三者への提供を認める旨の本人の同意を取得する必要があり，外国にある第三者に対しては，上記の委託，共同利用やオプトアウトに基づく場合であっても，本人同意を得ないまま個人データを提供することはできないこととされている[32]。

同条に定める例外としては，①提供先となる第三者が，日本と同等の水準にあると認められる個人情報保護制度を有している国として個人情報保護委員会規則で定める国にある場合，②提供先となる第三者が，個人情報取扱事業者が講ずべきとされている措置に相当する措置を継続的に講ずるために必要な体制として個人情報保護委員会規則で定める基準に適合する体制を整備している場合，③（法令に基づき提供を行う場合等の）個人情報保護法23条１項各号に該当する場合が挙げられるが，①について，本稿の脱稿時点で定められている国は存在しない。もっとも，個人情報保護委員会と欧州委員会は，2018年にEUにおいて施行されるGDPR（General Data Protection Regulation：一般データ保護規則）における域外移転規制に関連して，日本を十分な保護レベルを有する国として認定すること，および日本の個人情報保護法においてEU各国を上記①の日本と同等の水準にあると認められる個人情報保護制度を有している国として定めることを協議しており，この点の改正動向については留意が必要である[33]。②については，提供先となる第三者において，個人情報保護法４章１節の規定により個人情報取扱事業者が講ずべきとされている措置に相当する措置の実施が担保されるよう，当該第三者との間で締結される契約，確認書，覚書等において当該第三者に義務を課すことなどが考えられ[34]，実務上もこの方法が広く採用されている。したがって，たとえば，海外企業にデータ解析を委託する場合には，当該企業への提供について本人の同意を取得していない限り，上記のような委託先が日本の個人情報保護法上の義務を遵守する旨の覚書を当該委託先と締結することを検討すべきである。

2. 3 「匿名加工情報」として利用する場合

ビッグデータビジネスにおいては，特定の個人を識別できないようデータを加工して匿名加工情報としたうえ販売する方法が考えられる。この匿名加工情報の制度は，平成29年改正において，パーソナルデータの利活用を促進することを主眼として導入された。個人情報を加工して匿名加工情報とした場合には，上記個人情報にかかる利用目的の制限がかからず，また，第三者提供にあたり，本人の同意が不要となる点が大きなメリットとなる。次に，小売店における個人データを含む購買データを匿名化して，商品・サービスの開発や向上を目的とする企業にデータを提供するビジネスモデルを例にとって，匿名加工情報を利活用する方法について説明する。このようなケースでは，データを利用する企業において商品・サービスの購入者を特定できる情報までは必ずしも必要としないことが多い。そのため，小売店ないしデータ加工会社において，後述のような適切な加工を施した上で，民間企業にデータを提供することがデータの有効な活用方法として期待されている。

(1) 匿名加工情報の作成方法

匿名加工情報とは，個人情報保護法２条９項各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって，当該個人情報を復元することができないようにしたものをいう[35]。この定義のとおり，匿名加工情報となるためには，①特定個人が識別できないように加工すること（非識別化），及び②当該個人情報を復元できないようにすること（復元不能）が必要である。同法に従い適切に加工された匿名加工情報は，個人情報における個人識別性の要件を満たさないものとなるので，もはや個人情報に該当しない[36]。なお，匿名加工情報の基本的な要件である非識別化及び復元不能とは，あらゆる手法によって特定することができないよう技術的側面から全ての可能性を排除することまでを求めるものではなく，少なくとも一般人及び一般的な事業者の能力，手法等を基準として当該情報を個人情報取扱事業者または匿名加工情報取扱事業者が通常の方法により特定できないような状態にすることを求めるものに過ぎない[37]。

具体的に，匿名加工情報を作成する際には，以下の基準に従って，個人情報を加工しなければならない[38]。

① 個人情報に含まれる特定の個人を識別することができる記述等の全部または一部を削除すること

例：購入者の氏名を削除，住所は都道府県までとし，生年月日は削除して，年代に置き換え，購入時間は，午前中等に丸める。

② 個人情報に含まれる個人識別符号の全部を削除すること

例：旅券番号，免許証番号を削除。

③ 個人情報と当該個人情報に措置を講じて得られる情報とを連結する符号を削除すること

例：サービス会員の情報について，氏名などの基本的な情報と購買履歴を分散管理し，それらを管理用IDを付すことにより連結している場合に，その管理用IDを削除。

④ 特異な記述等を削除すること

例：年齢について80歳以上は，80歳以上というカテゴリーにまとめる。

⑤ 前記①ないし④に掲げる措置のほか，個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等との差異その他の当該個人情報データベース等の性質を勘案し，その結果を踏まえて適切な措置を講

ずること

このプロセスから明らかなように，データの匿名化作業は，それに含まれる情報の項目と量を減少させる行為にほかならず，ビッグデータの特徴の一つである多様性を一定程度減じる結果となる。一般論として，データの内容が抽象的になればなるほど高解像度が減少するため，そのデータの価値は低下する。そのため，パーソナルデータの利活用とプライバシー保護のバランスを図るためには，データの特性や利用目的に応じて匿名化を行うことにより，データの価値の低減をある程度軽減する方法が適切である[39]。匿名化の代表的な手法には，表３記載のものがある[40]。個人情報を匿名化するにあたっては，個人情報に含まれる情報の項目や匿名加工情報として利用を考えている用途等を検討し，安全性や有用性の観点からこれらの手法を適宜組み合わせて加工することになる[41]。例えば，項目削除／レコード削除／セル削除や一般化は，上記①や②の特定の個人を識別できる記述の削除に有効であるし，トップ（ボトム）コーディングは，上記④の特異な記述の削除に有効であるといえよう。

(2) 識別行為の禁止

匿名加工情報の取扱いに際して特に注意すべき主要な点が，識別行為の禁止ルールである。すなわち，個人情報取扱事業者は，匿名加工情報を作成して自ら匿名加工情報を取り扱うに当たっては，当該匿名加工情報の作成に用いられた個人情報に係る個人を識別するために，当該匿名加工情報を他の情報と照合してはならない[42]。また，匿名加工情報を受領した者についても，匿名加工情報を利用するときは，元の個人情報に係る本人を識別するために，削除した記述など若しくは個人識別符号若しくは加工方法に関する情報を取得し，または当該匿名加工情報を他の情報と照合してはならない[43]。

この規制はあくまで再識別を目的とした照合行為を禁止するものであり，識別目的ではない

表３　匿名化の代表的な手法

手法名	解説
項目削除／レコード削除／セル削除	加工対象となる個人情報データベース等に含まれる個人情報の記述等を削除するもの。例えば，年齢のデータを全ての個人情報から削除すること（項目削除），特定の個人の情報を全て削除すること（レコード削除），又は特定の個人の年齢のデータを削除すること（セル削除）。
一般化	加工対象となる情報に含まれる記述等について，上位概念若しくは数値に置き換えること又は数値を四捨五入などして丸めることとするもの。 例えば，購買履歴のデータで「きゅうり」を「野菜」に置き換えること。
トップ（ボトム）コーディング	加工対象となる個人情報データベース等に含まれる数値に対して，特に大きい又は小さい数値をまとめることとするもの。 例えば，年齢に関するデータで，80歳以上の数値データを「80歳以上」というデータにまとめること。
ミクロアグリゲーション	加工対象となる個人情報データベース等を構成する個人情報をグループ化した後，グループの代表的な記述等に置き換えることとするもの。
データ交換（スワップ）	加工対象となる個人情報データベース等を構成する個人情報相互に含まれる記述等を（確率的に）入れ替えることとするもの。
ノイズ（誤差）の付加	一定の分布に従った乱数的な数値を付加することにより，他の任意の数値へと置き換えることとするもの。
疑似データ生成	人工的な合成データを作成し，これを加工対象となる個人情報データベース等に含ませることとするもの。

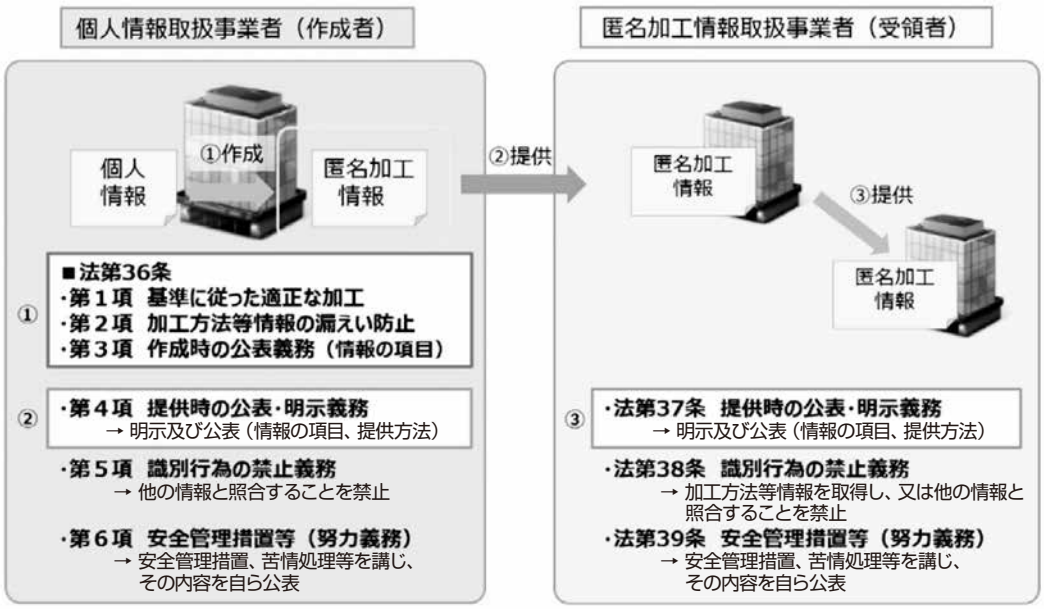

図１　匿名加工情報の作成者・受領者が順守すべき規定[50)]

他の情報との照合まで禁止するものではない。例えば，複数の匿名加工情報を組み合わせて統計情報を作成する場合，及び匿名加工情報を個人と関係のない情報（例として，気象情報，交通情報，金融商品等の取引高）とともに傾向を統計的に分析する場合等は，詳細な統計情報の取得を目的とするものであり，再識別を目的とするものではない。したがって，これらの事例は個人情報保護法により禁止される識別行為に該当しない[44)]。ビッグデータ解析のプロセスにおいては他の情報と統合する行為が行われるが，このような統合行為が再識別を目的とするものでない限り，個人情報保護法36条５項の「本人を識別するため」の要件を満たすものではなく，同条項の違反にはあたらない。また，複数の匿名加工情報を組み合わせて統計情報を作成すること，匿名加工情報を個人と関係のない情報とともに傾向を統計的に分析することも同じく禁止されるものではない[45)]。

他方で，禁止される識別行為に該当する場合として，保有する個人情報と匿名加工情報について，共通する記述等を選別してこれらを照合する行為，及び自ら作成した匿名加工情報を当該匿名加工情報の作成の元となった個人情報と照合する行為がある[46)]。自社内で個人情報データベースを保有する場合に第三者から提供された匿名加工情報に含まれる基本属性等を元に当該データベース内の個人データと紐付ける行為等は，識別行為の違反に該当するので注意を要する。

(3) その他匿名加工情報の作成者に係る主な規制

匿名加工情報を作成したときは，削除した記述など及び個人識別符号並びに加工方法などの情報の安全管理措置を講じなければならない[47)]。

また，匿名加工情報を作成したときは，当該匿名加工情報に含まれる個人に関する情報の項目を公表しなければならず[48)]，それを第三者提供するときは，提供する匿名加工情報に含まれる個人に関する情報の項目及び提供方法について公表するとともに，提供先に当該情報が匿名加工情報である旨を明示しなければならない（図１参照）[49)]。

2. 4 「統計データ」として利用する場合

複数人の情報から共通要素に係る項目を抽出して同じ分類ごとに集計して得られる統計情報は，特定の個人との対応関係が排斥されている限り，個人情報保護法上の「個人に関する情報」に該当せず，同法による規制を受けない[51]。したがって，もともとパーソナルデータであったものを統計データに加工したうえ，当該データを販売する場合には，個人情報にかかる規制も匿名加工情報にかかる規制もかからない。もっとも，形式上「統計データ」となっていればよいというものではなく，「統計データ」として個人情報保護法の規律の外におくためには，実質的にも個人との対応関係が十分に排斥できるような形で統計化されていることが重要であるといえる。この統計データとしての利用は，個人に関する情報ではないため，特定の個人にリーチすることを想定しておらず，そのような利用には向かないが，収集した情報に基づいて全体的な傾向を把握すること等を目的とするのであれば，有効活用も可能であろう。

2. 5 炎上リスクの低減化

個人情報保護法における規制は上記のとおりであるが，個人情報保護法でカバーされないパーソナルデータであっても，プライバシーの観点から保護すべき情報については，適切な対応が求められることは前述のとおりである。近時は，インターネットの発展により，消費者等の個人も自らの意見を自由に発信できるようになり，その結果，不適切な企業の言動が炎上している例は枚挙に暇がない。パーソナルデータの利活用の場面においても，このような炎上事例は多数存在し，このことがビッグデータの利活用の足かせになっている側面も否定できない。したがって，ビッグデータの利活用に際しては，個人情報保護法の規制を遵守することに加えて，個人のプライバシーに配慮した施策を講じることを検討するべきである。これらの施策として採りうる措置は，その利用形態においてどのような手法が実現可能か，また有効かの観点から検討されるべきであり，以下では，考えられる具体的な手法を参考までに示す。

(1) 本人の同意取得

パーソナルデータの取扱いについて同意を取得することは，炎上対策のもっとも効果的な手法であるといえよう。もっとも，同意の取得にあたっては，どのようにデータが取り扱われるのかについての説明が重要である。

(2) パーソナルデータの取扱いの詳細を公表

パーソナルデータの取扱いについて詳細に公表することが考えられる。炎上の原因の最たるものは，自分の知らないところで，自分の情報が利用されていることであると考えられる。どのように取り扱われるかを認識したうえで自分の情報を提供している消費者から炎上の火の粉が上がる可能性は高くない。また，この公表の手法についても検討されるべきで，たとえば，店舗における情報収集にあたっては，企業のウェブサイトに掲載していても実質的な閲覧の機会が保証されていないため，店舗での見えやすい位置に掲示することを検討するべきである。

なお，ここでの取扱い手法の内容は当然に合理的な内容であるべきで，その内容自体が不合理であれば，逆に炎上を招きかねないため，注意を要する。

(3) オプトアウト

パーソナルデータの取扱いについて反対する本人からは当該取扱いを停止する手段（オプトアウト）を設けることも考えられる。なお，ここにいうオプトアウトは，プライバシー保護の観点から企業が任意に実施する措置であって，

法23条２項にいう第三者提供停止のオプトアウトを意味しているわけではない。

3．おわりに

上記のとおり，個人情報保護法上の規制を中心に，パーソナルデータ取扱いの法的な留意点を記載した。紙面の都合上，触れられなかったが，今年５月11日〈x-apple-data-detectors://4〉には，昨年成立した医療分野の研究開発に資するための匿名加工医療情報に関する法律（次世代医療基盤法）の施行も予定されており，同法のもとで匿名化された医療情報の利活用が促進されることも予想される。このような社会的潮流のなか，いち早くパーソナルデータの適法，適切かつ有効な活用を実現することが各事業者にとっての課題であろう。本稿がそのような課題を解決するための一助になれば幸いである。

注　記

1) ビッグデータの定義は論者によって異なるが，①取れるデータ量が巨大であること（Volume），②様々な生活要素のデジタル化による多様性（Variety），③利用者の反応を取得する速度・頻度の向上（Velocity），④データの矛盾や不確実性を排除した正確性（Veracity）の４つの要素が取り上げられるため，本稿においてもこの定義に従う。なお，データの高解像（上記の④），多様性（上記の②），及び高頻度生成（上記の③）がビッグデータの基本的な特性であるとして，これらの要素を持つデータを収集した結果としてデータ容量が巨大になるとする見解もある。鈴木良介「ビッグデータビジネス」（日本経済新聞出版社，2012年）19頁及び20頁。
2) データベースを作動させるソフトウェアの一種であるHadoopが典型である。これは，「アパッチ・ハドゥープ」と呼ばれることもあるが，これはハドゥープの最も一般的なバージョンがアパッチ・ソフトウェア・ファウンデーションによってサポートされているためであり，現在は，インテル，マイクロソフトを始めとして様々なベンダーがそれぞれのバージョンのハドゥープを開発している。
3) データ量の多さ故に，多少不正確なデータが混入したとしてもその影響を軽微に留めることができるため，ビッグデータはその正確性，真実性を担保することができる。小林孝嗣「ビッグデータ入門　分析から価値を引き出すデータサイエンスの時代へ」（インプレスジャパン，2014年）29頁。
4) ビッグデータの対象がおよそ個人と関わりのない情報（気象状況等）であれば，個人情報保護の問題は生じない。岡村久道「個人情報保護法第３版」（商事法務・平成29年６月）323頁。
5) 本稿において「個人情報保護法」の用語を用いる場合，平成29年に全面施行された改正個人情報保護法を指す。
6) 法２条１項
7) 法２条２項
8) 民間企業や研究施設が介護施設（ないしは中間のデータ販売会社）から介護データを取得して利用する際には，個々の利用者の個人情報を必要としない場合もある。このケースでは，個人情報の第三者提供に係る利用者の同意がなくとも，介護施設ないしデータ販売会社の下で介護データを匿名化ないし統計処理して，民間企業等に提供することができる。データの匿名化については，本稿2．3を参照。
9) 法15条
10) 法17条
11) 法18条１項
12) 法18条２項
13) 法17条２項
14) 法２条３項
15) 個人情報保護法施行令２条２号
16) 法２条６項
17) 法２条４項
18) 法19条
19) 法20条
20) 法21条
21) 法22条
22) 法23条１項
23) 法令に基づく場合等一定の公益目的の場合についての例外（法23条１項各号）も存在するが，ビッグデータ利活用の場面で適用されることはほとんどないと思われるため，割愛する。
24) 法23条５項１号

25） 法24条
26） 法23条５項３号
27） 法23条２項
28） 法23条４項
29） 法23条２項柱書
30） 法25条１項本文，同２項
31） 法26条
32） 法24条
33） 平成30年４月25日付で，「個人情報の保護に関する法律についてのガイドライン（EU域内から十分性認定により移転を受けた個人データの取扱い編）（案）」が公表され，パブリックコメントに付されている。そこでは，個人情報保護委員会は，日本と同等の水準にあると認められる個人情報保護制度を有している国としてEUを指定し，欧州委員会も日本が個人データについて十分な保護水準を確保していると決定した，とされている。
34） 「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」３-１
35） 法２条９項柱書
36） 前掲注４）岡村119頁
37） 「個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）」２-１，前掲注４）岡村121頁
38） 法36条１項，個人情報保護法施行規則19条
39） 佐藤一郎「ビッグデータと個人情報保護法　データシェアリングにおけるパーソナルデータの取扱い」（情報管理Vol.58，No.11）831頁
40） 前掲注37）15頁。匿名加工情報の作成手法は，これらの手法に限られるものではなく，その他の手法を用いて適切に加工することも可能である。
41） 大角良太＝高橋克巳「Q&Aで理解する！パーソナルデータの匿名加工と利活用」（清文社，2017年）77頁
42） 法36条５項
43） 法38条
44） 前掲注37）３-６
45） 同上
46） 同上
47） 法36条２項
48） 法36条３項
49） 法36条４項
50） 個人情報保護委員会事務局，パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて
https://www.ppc.go.jp/files/pdf/report_office.pdf（参照日：2018.3.27）
51） 前掲注37）２-１

（原稿受領日　2018年２月15日）