信託セミナー

個人情報の保護と活用を巡る近時の動向と実務対応等について

三浦法律事務所弁護士　日　置　巴　美

— 目　次 —

はじめに

本日は、「個人情報の保護と活用を巡る近時の動向と実務対応等について」というテーマで、個人情報保護法に則り、どのような形であればデータを利活用できるのか話をさせていただきたいと思います。これを守らなければいけない、あれを守らなければいけないというような感覚ではなく、法令、あるいは本人との契約、B to Bでの契約がありますが、それらの下、どうすればデータを活用できるのかということについて、いろいろイメージしていただくのが今回の話の趣旨です。

はじめに、今どのような理由でデータが注目されているのかをまとめています。基本的には、データを活用しなければ、国内・国際競争で既存のビジネスの優位性を保持し、何か技術を持っていたとしてもそれを活かすこと自体が危ぶまれているというのが現状ではないかと思います。新しいサービスを創出するときや、既存のビジネスを変えていくときにも、データを活用できます。

また、例えば戦略的な人事・労務管理において、今の配置ではなく、この人にはこの適性があるからこちらへ配置したほうがよいのではないかとか、ここはシステム、AI を使

って代替した方が生産性、作業効率がよくなるのではないかといったことがあります。その分の空いた労働力を別のところに適正配置していく、新しい業務を考えるようなことに使っていくことで、データにより競争力を高めていこうということがあるかと思います。

他方、攻めの利用を進めるあまり、違法又は不当にデータを取り扱ってしまうことで生じる法的又は炎上リスクがあります。そうすると、本人から「それはおかしいのではないのか」ということを言われる可能性があり、そうしたリスクが顕在化することにも常に注意しなければならないと思います。違法な場合のみならず、個人情報保護法はミニマムのルールであることから、不当な取り扱いにも気を配れとされる場面が発生しています。

データの取扱いの巧拙がビジネスのみならず企業の勝負を決めるのではないか、ということが一つ言えるかと思います。「個人情報・プライバシー」に無関係な企業は存在しません。新規産業や新規ビジネスモデルを展開するために、攻守揃った総合的なデータ戦略を構築することも一つではないかと思います。後ほどお話しますが、個人情報の取扱いをどの部署で行っているのか、それ以外の部署がデータの利活用やデータの保護を気にしているのかなどについては、企業により濃淡も含めて異なるのではないかと思います。

データの利活用と保護は、戦略を立てる部署や、事業部、総務部、法務部といった部署と連携しながら進めていかなければ、インシデント対応においてもそうですが、全社総合的なデータの利活用あるいは保護は難しいと考えています。総合的なデータ戦略について一つひとつの企業が考えていくことが、今重要になっているのではないかと問題提起する次第です。

1.　データ保護と活用のトピックス

資料３頁で最近のデータ保護と活用のトピックスについて簡単な図にまとめています。個人情報を活用する際には個人情報保護法が一つの指標となり、基本となります。データの利活用環境を整えることを目的とされた平成27年の改正が記憶に新しいかと思います。これは、保護・利活用両面からの法改正であると謳われていました。

匿名加工情報の制度の創設や、利用目的変更、個人情報の明確化といったように、保護と利活用両面が考えられています。保護しなければデータの活用はおよそあり得ません。本人が嫌だと思えばデータは出さないわけですから、保護と利活用の両面を考えての法改正という環境整備がされています。個人情報を使うときには、いずれも個人情報保護法の枠内で対応する必要があり、その基礎の上で、例えばAI・データの利用に関する契約や、PDS（パーソナルデータストア）、情報銀行、データ取引市場の台頭なども最近はトピックスとされています。

人事の戦略構築やコストカット、付加価値を生む仕事への業務配置の変更もあると思いますが、信用スコアリングといったデータによって生まれる付加価値、あるいはフェイスブックのデータ流用、ケンブリッジ・アナリティカの問題や、マリオットホテルのデータ漏えいのように、大規模なデータ漏えい事案もあり、安全面や炎上リスクにも関係してくるところには、すべて個人情報保護法が関係しているかと思います。

AI・データの利用に関する契約については、

何年か前から政府がソサエティ5.0や第４次産業革命を謳い、その実現に向け複数の政府検討会を立ち上げ､報告書を適宜出しています。その中で経済産業省が､「AI・データの利用に関する契約ガイドライン」を策定しています。本ガイドラインでは、企業の機械から出るようなデータやセンシングデータの話もありますが、パーソナルデータを使う場合も関係します。パーソナルデータの取得・利用・提供については個人情報保護法で規律されているので、それも踏まえた上でどうやって契約をするのか、どういうデータ共有モデルを作るのかということにも触れられています。

例えばAIの学習用データを取得する際、そのデータが個人情報であれば個人情報保護法の規律がかかるので、やはり同法が問題となります。例えばPDS、情報銀行、データ取引市場においても、原則として本人の同意がなければデータの共有はできないというように、やはり個人情報保護法が関係します。

データ取引市場であれば一般社団法人データ流通推進協議会、オムロンや日立、NEC、インテージ、ウフルなど、老舗の製造業からメーカーまでと、データ活用を前面に出しているような企業が一緒に組んで対応している例が一つあります。

また、みずほ銀行などが出資しているJ-DEX（日本データ取引所）もあるかと思います。情報銀行については、総務省や経済産業省でも認定スキームが検討されていましたが、ヤフーなどのIT関連企業で構成されている一般社団法人日本IT団体連盟で、パーソナルデータを安全に預けられると認定して、より本人が安心してデータを出せるようにデータを流通させようという仕組みがつくられているのが最近の動きかと思います。

ここまでの話は、個人情報保護法を中心として、不正競争防止法、著作権法といった法令との関係というミニマムなルールを基礎としたお話です。次に、本人との関係として、例えば信用スコアリングなどを見ていただければ分かると思いますが、プライバシーや人権の問題、個人情報保護法の問題、レピュテーションリスク、炎上リスクといったものも問題になるかと思います。

その他、プライバシーポリシーのようなステートメント、本人との契約にも留意すべきです。活用の幅を確保するためには、やはり本人との利用規約や契約上データを活用しうる幅を、個人情報保護法の利用目的制限も含めて決めていくことが必要になります｡また、匿名化や統計化すれば使える余地をきちんと契約上残しておくことも重要になります。

また、B to Bにおける契約関係では、例えば個人情報を一次取得した場合、取得者がデータを他者に渡す際にはやはり本人の同意が要るとか、委託であれば同意は要らないが監督しなければならないという義務もあります。どういった形であれば法律に抵触せずにデータを共有して使っていくことができるのかを考える意味で、法律が関係してきます。そしてやはり炎上リスク、レピュテーションリスクも見なければいけません。その他、データとその派生物や、データから分かるノウハウ、暗黙知のようなものや、明確になっているものもあるかもしれません。そうしたものを、どう守るのかという知的財産的な側面からの戦略も重要になってくると思います。以上が、データを取り巻く環境における注意点、ポイントになると考えています。

2．個人情報保護法の「匿名加工情報制度」

それでは、以上お話したデータ利活用のいずれの局面にも関わりうるものとして、個人情報保護法のうち「匿名加工情報制度」を中心にご説明したいと考えています。例えばAI・データの利用に関する契約において、その対象となるデータを個人情報保護法上は匿名加工情報にしてくださいという指定をする、データを流通させるときにいったん匿名加工情報にして提供するというように、分析してデータからの付加価値を得たいときに、その分析対象を個人情報の生データのまま使うのではなく、匿名加工情報に加工してデータを使うことも考えられます。そこで、まずは、匿名加工情報制度について見ていきます。

もう一つ見ていくべきは、なぜ匿名加工情報を活用するニーズが生まれるのかという点です。個人情報保護法の元々の制度との対比で、匿名加工情報を使うほうがよいのか、それとも個人情報のまま使うのがよいのかということがあります。各社のニーズや、そのときの契約、本人との規約の関係もありますが、どういった形で個人情報保護法を含みながらデータ利活用の体制を整備し、データフローを確立するのかということについてお話ししたいと思います。

匿名加工情報制度は平成27年改正で導入されていますが、なぜこういう制度が導入されたのかという背景も説明しつつ、個人情報保護法の理解も深めていただくために、３つのポイントをお話しします。

１つ目は、保護対象となる「個人情報」です。個人情報とは何かというと、特に問題とされるのが「容易照合性」と提供先基準・提供元基準です。そもそも個人情報に該当しなければ、パーソナルデータであったとしても個人情報保護法の規律の範囲外になるので、個人情報保護法にいう本人の同意という話も出てきません。したがって、個人情報に該当しないなら自由に使えそうだという話になると、まずは個人情報とは何かということが俎上に上がります。

２つ目が、「目的外利用、第三者提供と同意」です。個人情報保護法では、個人情報の利用目的を定めその範囲内で使いなさい、その目的達成に必要でない取扱いを今後するのであれば本人の同意を得なさいということで、利用目的制限を設けています。もう一つは「第三者提供の制限」です。仮に誰かにデータを渡しますという利用目的が定められていたとしても、それについては本人の同意を別途取りなさいという規制です。

したがって、本人を関与させる仕組みが取られており、数十万、数百万単位でデータを持っている場合は、その本人の同意を取ること自体が時間的にも費用的にもかなりのコストになります。かつ本人に「いやだ」と言われたときに、そのデータを除く手間やコストもかかるためで、大きなデータ流通、データ利活用の障壁になると言われていました。

３つ目は、本人同意のコスト、時間的・費用的なコストを考えなくてもよい仕組みを作れないかということで、平成27年の個人情報保護法改正で創設された「匿名加工情報制度」です。匿名加工情報は、個人情報保護法２条９項に定義がありますが、その定義とともに、取扱いのルールも、必要最低限定められています。

ただ、本人関与や、利用目的の制限はないので、ある程度取扱いルールに則ってさえい

ればフリーに使えるというのが、匿名加工情報です。ただし、この一定のルールの中に、適正な加工や識別行為の禁止などがあるので、実際に事業者が持つニーズ、データを使ってダイレクト・マーケティングしたいという場合には、識別行為の禁止義務に違反し得るし、ニーズによりこの制度が使えないという話が出てきます。

翻ると、本人同意の問題があるので、匿名加工情報制度を使いたいが、匿名加工情報にも一定のルールがあるので使えないかもしれないという場合があります。その場合は、個人情報保護法の枠の中で、どうやって利活用の幅を持たせるのかを考えていく必要がある、というのが本日の話の大筋になるかと思います。したがって、本日の話を踏まえて、自社ニーズがこうすれば満たせるという観点でご検討いただければと思います。

3.　保護対象となる個人情報―個人情報とは―

個人情報は、生存する個人に関する情報であり、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です。これには、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みます。

前者としては、氏名や生年月日・住所を組み合わせたものや、単体では氏名・顔画像といったものがあります。個人情報と紐づく情報は履歴情報などと言われますが、そういったものも他の情報と容易に照合することができ、それにより特定個人を識別することができることとなれば、単体で特定個人を識別できなくても個人情報とされています。

さらに、「特定の個人を識別することができるもの」として、平成27年改正で個人識別符号というものが新設されています。これは、明確化の趣旨で、そもそも個人情報だったけれども判断に迷わないように政令で対象が定められたものです。例えば指紋認証データ、顔認識データ、旅券番号、免許証番号が該当します。

ただ、やはり特定の個人を識別できるものとは何かと言われると、抽象的であり、判断に迷うケースは多いのではないかと思われます。判断基準について、資料５頁の枠外部分にあるとおり、個人情報とは「特定の個人を識別することができるもの」です。

情報単体としては、例えば顔写真とか映像といったもの、複数の情報を組み合わせて保存されているものとして氏名・住所・生年月日・電話番号がセットになっているものがあります。そういった情報であれば社会通念上特定の個人を識別することができると判断される、それが個人情報です。社会通念上と申し上げたとおり、一般人の判断力や理解力をもって、生存する具体的な人物と情報との間に同一性を認めることができるだろうとされる情報が個人情報だと言われています。

典型例としては、正面から顔が判別できる画像、映像と、氏名があります。個別判断が必要な例としては、先ほど申し上げた、性別、生年月日、住所、電話番号、勤務先、役職等が組み合わされていれば、「〇〇社のあの社長だ」と分かってしまうので、そういったものも個人情報だと言われています。

もう一つ注意が必要なのは履歴です。購買履歴や位置情報、移動履歴は、その情報が蓄積されればされるほど、行動習慣といったものが明らかになるために、具体的な人物が浮

き彫りにされてしまいます。例えば毎日深夜に同じ場所にいるということは、そこが家であることが分かるでしょうし、そこから勤務地が分かれば、その履歴から「○○社の○○さんだ」と分かってくることがあり得ます。

したがって、詳細な情報になればなるほど、それは特定個人を識別することができるものとして個人情報に該当する可能性があることになります。履歴だけであれば分からないから自由に使えるという考え方だと、少し難しい問題に当たってしまう可能性があることを覚えておいていただければと思います。

先ほど申し上げた利用目的の制限や、第三者提供といった規制がありますが、前者は個人情報の取扱いに、後者は個人データ、データベースに含まれている個人情報について、本人同意という義務が発生します。例えば病歴や健康診断結果といった要配慮個人情報については取得の同意が要りますし、第三者提供する場合の例外たるオプトアウト手続が使えませんので、提供取得の同意の取り方が難しくなってくるという規律があります。

そういった規律がかかるのは、基本的には個人情報であって、その該当性が問題となります。個人情報に該当しなければ、規律の話は出てきません。このため、本人同意が関係なくなるという点からは、匿名加工情報制度が一つ有用かと思われます。

4.　保護対象となる個人情報―容易照合性と提供先基準・提供元基準―

特定個人を識別することができるものだけでも、かなり幅が広そうだとお感じになったのではないかと思いますが、さらに個人情報と紐づく情報について、容易照合性という要件があるのですが、ここの要件に該当するかしないかということでかなり厳しい判断がされています。

このため、個人情報かどうかを悩むよりも、概ねパーソナルデータは個人情報に該当しているのだという方向で進んだほうが、ビジネスジャッジとしては無駄なコストがかからない場合があるという観点も含め、容易照合性の要件を見ていきたいと思います。

容易照合性とは、情報を取り扱う者が、特別の調査を行うことや、特別の費用を要することなく、通常行っている業務における一般的な方法で、他の情報と照合が可能な状態にあることをいいます。さらにこれは、その事業者ごとの相対的な判断となるので、外部で特定個人を識別できなくても、自社内の特定個人の情報とマッチさせながら使っているようなケースでは、個人情報に該当すると言っているのが、この容易照合性の基準になります。

資料６頁の「例えば」以下の部分をご覧ください。CIF 番号、会員 ID、口座番号でも構わないのですが、本人を識別するために付している ID で本人一人の情報、例えばＡさんの情報を分散管理しているというときに、その基本情報となる属性情報と、履歴情報を分散して、それを ID で繋ぎ照合しながら使っているときには、容易照合性の要件からすべての氏名等が入っていないデータセットも含め、個人情報に該当します。

また、例えばデータを分散管理するときに、最初から一つのデータセットを格納して分離するケースと、Ａの項目についてはＡデータベースに、Ｂの項目についてはＢデータベースにという形で、システム上入力時からすべて分散格納するようなケースもあると思いま

す。全体で管理しているのは１部署であるとか、社内であれば誰でも管理状況として取り扱いうるとか、全体として取扱いうるようなケースです。このようなケースでも、全体として個人情報に該当します。

これは最初の取得段階から一部だけ氏名等のデータを入れない状態で他社に提供しているのだから、これは個人情報の第三者提供ではないと言われることがありますが、当局からは基本的にはそういったものも容易照合性がありコントロール下だろうと言われることがあるので、ご注意いただいたほうがいいと思います。

このように、個人情報該当性はかなり厳しい判断がなされていて、パーソナルデータは個人情報に大体該当すると考えると、どういった法規制があり、また、その法規制の中でどういったことができるのかを見ていかなければいけないという発想になります。

また、平成15年の個人情報保護法が成立した際、この容易照合性はどこを基準に判断するのかという議論がありました。個人データを提供する側の個人情報取扱事業者では履歴情報だけ提供し、属性情報・基本情報は提供しない。この履歴情報だけを提供するときに、第三者は提供された履歴情報から特定個人を識別することはできないといったケースがあり得ると思います。

第三者にとっては、それは安全な情報、本人の権利・利益を侵害しない情報だから、出してもいいだろうという考え方がありました。個人情報取扱事業者は第三者提供の同意を取得するという義務を負っているが、履歴情報だけ提供し、第三者にとって個人を識別できないようなら本人同意は要らないのではないかという提供先基準が謳われたことがあります。

個人情報保護法はもともと内閣府から消費者庁に所管が移っている法令ですが、消費者庁では提供先基準は取っていません。提供元で個人情報該当性を判断し規律がかかるというのを対外的に発表しています。個人情報該当性が個人情報取扱事業者を基準として判断されるのであれば、本人の同意を得ないと第三者提供できないのが基本だとされているわけです。

ただ、申し上げたとおり、提供された第三者にとっては、それは個人にリーチし得ない情報であれば活用してもいいのではないかという気持ちが残ります。そこで、どういった形で対応していくか考えたときにできたのが、先ほど申し上げた匿名加工情報制度であるとも言えます。

匿名加工情報は、特定の個人を識別することができず、かつ作成の元となった個人情報を復元することができないように加工した情報であり、履歴情報などの提供に適しています。個人情報保護法の規律だと提供元基準が取られていて、第三者提供する際には、履歴情報であったとしても本人の同意を得なければならなかったものが、匿名加工情報を作成するための適正加工基準に則って加工するなど、個人情報保護法の匿名加工情報制度のルールを守っていただければ、本人の同意なく、第三者に同じようなデータが提供できるようになっています。

5.　目的外利用、第三者提供と同意

個人情報には、一連の取扱いに次のような義務が課せられます。今後、匿名加工情報を使うのか、個人情報のまま個人情報の取扱い

ルールに則ってデータの利活用をしていく方がいいのかを考えていただくためにも、個人情報保護法の個人情報の取扱いルールを確認したいと思います。

個人情報保護法は、取得、利用、保管、提供、本人対応といった個人情報を取得して活用していく一連の取扱いの場面ごとにルールを定めている法律です。

個人情報を利用し続ける限りは、最初に目的を設定し、変更する幅が決められています。その変更幅にも入らない目的で使いたいときには、目的外利用の制限が課せられていて、本人の同意を得なければならないとされています。

次に、取得の際には適正な態様で個人情報を取得しなければなりません。例えば、本当はBの目的で使いたいが、それを隠して本人が喜ぶようなAの目的だけを説明してデータを取得するという詐術的な行為なども、適正取得違反になり得ます。また、例えば店舗内のカメラを防犯目的以外で使いたいのに、防犯カメラ作動中などと表示するのみで、ずっと人をトレースしているようなケースでは、カメラのデータの取得というのも、適正取得違反になりかねません。

次に、個人データの場合には正確性の確保等です。そして、安全管理措置義務。データの取扱いを委託した場合には委託先の監督義務が発生するので、かなり重いコストを払うことになり得ます。契約書のレビューや実際の監査において、コスト面でかなり注力していかないと対応できません。また、最近も「宅ふぁいる便」といった色々なデータ漏えいの話が出ていますが、外部委託している場合でも、委託先でどういうシステム管理をされているのか見ておかないと、後々本人から損害賠償請求、あるいはＢ to Ｂであれば他社から損害賠償請求されることにもなりかねません。

その次の項目は、第三者提供の制限です。基本的には個人情報取扱事業者が他者（公開も含む）に対して、ある一定の主体だけではなく、広くデータを見せてしまうようなケースも含めて、本人の同意が必要になるのが原則です。その他第三者が外国にある場合については、さらに別途の制限が課せられています。また、第三者提供に関しては確認・記録作成義務が制定されています。

最後に、本人対応です。開示請求、訂正請求、あるいは利用停止・提供停止について対応し、また、苦情処理もしなければいけません。以上が個人情報保護法に定められた個人情報の一連の取扱いのルールになります。

ここまで見ると分かるとおり、実際は運用コストがかなりかかります。１年に１回、社員が個人情報を使っているのかどうか、どういう目的で使っているのか、どういう管理体制になっているのかなどをチェックしていくだけでもかなり大変です。

また、個人情報の取扱いに関する情報が社内共有され、上に報告される体制を取っていないと、法令順守のチェック対応やセキュリティインシデントが発生した際に適切な対応が取れないこともあります。データによっては金融庁に報告しなければならない、クレジットカードであれば早めにIPA（独立行政法人　情報処理推進機構）等と情報共有しなければいけないといったいろいろな話があるので、体制整備と内部運用をしていくだけでもコストがかなりかかります。

目的外利用と第三者提供の同意が問題となる場面は少なくありません。どういったときにデータを他社と共有したいのか考えると

き、データをただ単に販売するという先ほどの情報取引、データ取引市場だけではなく、分析まで考えてみると、自社内で分析までの人員を確保できている会社はそんなに多くはないと私は理解しています。

したがって、技術力のあるところにデータを提供し、解析してもらい、そのアウトプットを返してもらうときにも、そのデータに個人情報が含まれていれば第三者提供の制限がかかってきてしまうことが原則です。委託のスキームが取られ、共同利用の話がよく出てくるのは、第三者提供の本人同意という原則があるからだということになりますが、本人同意の制約を越えるためには、今申し上げた委託のスキームもあります。

資料９頁の右下の枠をご覧ください。委託先である個人情報取扱事業者Ｂはもともとの個人情報取扱事業者Ａが定めた利用目的内でしかデータを使うことができません。例えばＡにとってもＡが保有している以外のデータがたくさん集まるほうが、よりリッチな分析結果が出るのではないかと思われます。しかし、例えばＡがＢにデータ分析を委託していて、個人情報取扱事業者Ｃがデータ分析をＢに委託するとした場合、ＢでＡのデータとＣのデータを合わせて取扱うことはできません。それはＡからＣに第三者提供、ＣからＡに第三者提供しているのと同じ仕組みになるからです。この点については、個人情報保護委員会のQ&A の5-26-2⑵の例では、それは委託の範疇を越えていてＡもＣも目的外利用になると明確にされています。

委託のスキームは、やはり特定された利用目的の範囲内で使われます。Ａにとっての利用目的、Ｂにとっての利用目的、Ｃにとっての利用目的という制限がかかってくるので、必ずしも委託のスキームによれば何でもできるわけではありません。このため、先ほど申し上げた匿名加工情報が使えるのではないかという話が出てきます。もちろん、委託のスキームにもいい面はありますが、データを１カ所に集めて解析して、いろいろなアウトプットを出したいときには、匿名加工情報を使い、技術力のあるところにデータを提供していくことが一案と考えられます。

6.　匿名加工情報制度の創設

先ほどから申し上げているように、個人情報取扱事業者が履歴情報だけを外に出したいというときは、元の個人情報を加工します。匿名加工情報も個人情報を加工して特定の個人を識別できず、作成の元となった個人情報を復元することができないようにしたものなので、加工という面では同じです。

それでは、なぜ個人情報と匿名加工情報という別々の類型に分かれるのでしょうか。資料10頁をご覧ください。

加工した個人データは、加工しても個人情報・個人データに該当し得ます。加工後の情報からなお特定の個人を識別できる情報、例えば先ほど申し上げた詳細な位置情報、移動履歴というようなものが該当します。あるいは容易照合性があり特定の個人を識別できるもの、具体的な人物が明らかになるものということで、加工前と加工後の情報をIDにより連携させる場合や、詳細な履歴があり履歴を対比、対照すれば加工前の情報と加工後の情報が照合可能な状態のものは、加工したとしても依然として個人情報に該当します。

匿名加工情報とは、特定の個人を識別できず、個人情報を復元できないように加工した

ものであり、個人情報保護委員会規則の適正加工基準に従った加工が必要です。また、識別行為の禁止義務などの一定の義務が課せられているため、個人情報該当性の容易照合性の要件は関係なく、匿名加工情報に該当します。

7. 匿名加工情報（2条9項）と取扱いルール（4章2節）の創設

ここからは、具体的に匿名加工情報とは何かという点、どう対応するかという点をお伝えするため、適正加工基準や、取扱いルール全般についてご覧いただきたいと思います。資料11頁をご覧ください。本人が個人情報を個人情報取扱事業者Aに提供すると、Aは個人情報を取得するので､利用目的を特定して、かつ、その利用目的の範囲内でデータを取り扱います。こういう目的で使いますということを公表し、あるいは本人に対して明示・通知をしている状況になります。

ただ、実際使っていると、他のニーズも出てくるので、違う目的で使いたいと思うこともあります。その場合、目的変更可能であるか、目的外利用の同意を得られるのでなければ、個人情報保護委員会規則で定める基準に従い、個人情報に適正な加工をします。そうすると、加工された個人情報は匿名加工情報になり、まずは作成した匿名加工情報の項目を公表していただく必要があります。

かつ、それを第三者に提供する場合には、その項目も公表する必要があります。提供する際には、匿名加工情報であることを明示していただく義務もあります。個人情報保護委員会規則では「インターネットの公表その他の」と書かれており、インターネット以外の方法も取り得そうです。

例えば社員の情報を匿名加工情報にして、あるいは健康保険組合の中にある健康関連の情報を匿名加工情報にして活用するとき、基本的に企業のウェブサイトで公表されても、本人はわざわざ自社のウェブサイトや健保組合のウェブサイトを見ません。しかし、個人情報保護委員会としては対外的に公表することが重要であり、イントラネットへの掲示では足りず、インターネットで公表するよう言っているようですので、匿名加工情報を作成したときにはインターネット上で公表していただくことが必要になってきます。

こうして適正な加工をして匿名加工情報を個人情報から作り、作った情報については公表します。提供についても義務がかかってくる中で、匿名加工情報では、削除した記述等や加工方法の漏えいをまずは防止していただくという安全管理措置義務が課せられています。ただ、注目していただきたいのは、安全管理措置義務が、匿名加工情報自体の保存、管理に課せられているのではありません。削除した情報を安全に管理して、それが誰かに漏えいしてしまいその匿名加工情報から元の本人が識別されないようにしてくださいというように、加工等情報に対して安全管理措置義務がかかっています。かつ、取扱いについては、本人を識別するために他の情報と照合することが禁止されています。それにより、データが流通・活用する中で、本人を特定してデータが悪用されないようにし、本人に権利・利益の侵害が生じないようにしていることになります。

実際に特定の個人を識別できない、かつ元の情報を復元できないのであれば十分、基本的に本人の氏名等にリーチできないものです

ので、本人には具体的な損害が生じないことがほとんどです。ですから、個人情報が適正に加工されたのであれば、元の情報に戻すことを作為的にしない限りは、本人の権利・利益を侵害しないということで、匿名加工情報は自由な取扱いが認められているということがお分かりいただけるかと思います。

ルールに則っていれば、基本的にはレピュテーションリスクの関係や本人の損害は生じ得ないというのがこの制度を使う一つのメリットだと思います。例えばSuicaが個人情報保護法違反ではないかということで炎上したと思います。こうしたことが起こり得ないという意味でも、匿名加工情報制度は一つ活用の選択肢になるかと思われます。

匿名加工情報を作るときに、特定個人を識別することができないように、また作成の元となった個人情報を復元することができないようにするために、実際何をしたらいいのかについては、データ分析やデータの取扱い専門家でなければ、なかなか分かりません。そこで、明確なルールがないと困るということで、個人情報保護指針を用いることが推奨され、認定個人情報保護団体制度で細則を定めてよいことになっています。業界ごとに取扱っているデータが異なり得るので、団体ごとに細目を作り、匿名加工情報を活用できるようにしていただくというのも含めて、個人情報保護法が予定する匿名加工情報制度です。

一度、個人情報から匿名加工情報を作成すれば、特定の個人を識別してしまわない限りは、匿名加工情報として転々流通することもできますし、作成した社が自ら取扱うこともできるとなっていますが、そのような取扱いが認められていることの理由としては、本人が識別されないことが大きいです。この制度のポイントとしては、適正な加工と、識別行為の禁止という2つです。本日はこの肝となる制度を、重点的にお話ししたいと考えています。

8. 加工方法にかかる検討プロセスの全体の流れ

資料12頁をご覧ください。適正な加工と識別行為の禁止義務も併せて検討しながら、取扱いニーズを満たすのか、自社で匿名加工情報を使っていけるのかをご検討いただくことが本日の一つの目的になります。信託協会様の方でも「匿名加工情報の取扱いに関するルール」を策定されています。こちらも参考になるので、後ほど、再度ご確認いただければと思います。

以下のスライドでは、個人情報保護委員会、経済産業省、国立情報学研究所からそれぞれ公表された匿名加工情報に関するレポートをまとめています。適正加工しつつ有用なデータを作成するため、本人を識別して本人に不測の事態を生じないため、そしてそうしたリスクを回避するために考えられたプロセスが、1）ユースケース等の明確化、2）個人属性情報（識別子、属性）、履歴の仕分、3）個人識別等に係るリスクの抽出、4）個人識別等に係るリスクを踏まえた具体的加工方法の検討となります。

本プロセスを踏んでいただくと、基本的には本人識別のリスクは非常に低くなります。かつ、本プロセスは併せて個人情報保護法に定める適正加工基準も満たすように作られているので、この順番でご覧いただければ、基本的には匿名加工情報が作れ、かつ、識別行為の禁止義務にさえ反しないようにしていた

だければ、自由なデータの利活用が確保される形になっています。

1)　ユースケース等の明確化

ユースケース等の明確化の目的は、加工の対象となるデータの項目と加工方法をリスクに応じて絞り込むためとされています。どういったデータの内容にするのかは、何をしたいのかにもよるわけです。

まず、ニーズとして、匿名加工情報の作成者における業務・サービスの概要、データ流通の範囲、匿名加工情報の利用目的などがあります。目的により使いたいデータが変わるので、特定個人を識別できないように、元のデータを復元できないようにするときには、目的に応じて情報を削る方向になります。

例えば詳細な位置情報があったとします。住所・地番・マンション名・何号室などのデータがあるとして、その情報が詳細になればなるほど、本人にリーチする可能性は非常に高くなります。したがって、加工するときには削るか、あるいは、他の情報に置き換えてしまうのです。詳細な住所であれば市町村までにするといった形で加工することが考えられます。

しかし、住所や地域が必要なデータの解析ニーズもあり得ます。できるだけ住所を残したいとなると、他の情報に含まれている例えば生年月日、職業、年収といった情報を削る判断につながると思います。

したがって、ここで申し上げているデータの匿名加工情報の利用目的をまず明確にしていただく必要があります。かつ、他社に出すとその分、その元のデータを保有する事業者もいるので、参照して突合すれば元の本人を識別してしまうかもしれないということで、他社に出すときにはまた別の観点から参照リスクあるいは同じような情報との参照リスクを考えていただき、加工しなければならないことになってきます。

利用目的や他社への提供があるのかという観点でどういう加工をしたらいいのかを逆算していくということです。詳細は、先ほど申し上げた信託協会「匿名加工情報の取扱いに関するルール」も参照していただきたいと思います。

2)　個人属性情報（識別子、属性）、履歴の仕分

個人属性情報（識別子、属性）、履歴の仕分の目的は、個人識別等に係るリスクの抽出を効率的に行うこと、規則19条の加工基準に対応することです。この目的に合致するようにするためには、まずその個人情報が法律上も削らなければいけないのか、識別リスクがあるのかを見なければいけないので、個人属性情報なのか、それとも履歴情報なのかという仕分けをしていただきます。

個人属性情報は、個人情報に係る本人の基本的な属性に関わる情報の項目です。例示としては、氏名、生年月日、住所、郵便番号、マイナンバー、パスポート番号、固定電話番号、携帯電話番号、CIF 番号、口座番号、クレジットカード番号、電子メールアドレス、職業、年収、預金額・借入額、家族構成というもので、単体または併せて使うことにより特定個人を識別しうるものと考えていただければと思います。

属性情報には基本的にはある一定期間変わらないものが入ってきます。変わらない情報は、やはりそれだけ参照しうる情報が世間にあふれていますし、各社が持っているかもし

れないという点で本人につながりやすい情報になってくるので、ここは属性情報として、履歴情報とは別の観点から加工が必要になってくることになります。

履歴情報とは、個人の行動に伴い発生する行動の履歴に関わる情報の項目で、取引日時、取引金額、利用店舗、利用 ATM、あるいはウェブ閲覧履歴などです。自社ウェブサイトを閲覧した際に、サードパーティ Cookie などを入れていたり、JavaScript などを入れていると思いますが、そういったシステムから履歴を突合していくことができるので、ウェブ閲覧履歴もこちらに該当すると思います。

経済産業省は規則19条の適正加工基準で、例えば個人属性情報や履歴情報が規則19条の何号に該当するから加工しなければいけないというのを明示しているのですが、個人情報保護委員会事務局のレポートでは、その明示はありません。携帯電話番号が個人情報に単体で該当するのか、クレジットカード番号はどうなのかという点を明確にしないという趣旨があるのだと思いますが、経済産業省では明確にしているが、個人情報保護委員会はその辺りを曖昧化しながら、電話番号等も削除しなさいという例示を出しています。

3)　個人識別等に係るリスクの抽出

個人識別等に係るリスクの抽出では、今申し上げたユースケース等の特定や個人属性情報・履歴情報の仕分けをしていただき、それらを踏まえて適切な加工方法を採用することと、規則19条の基準に対応することが目的となります。

個人識別等に係るリスクで想定されるものとしては、例えばその情報自体で個人を特定できる、その情報自体が個人情報であること（個人属性情報の一部。氏名、画像といったものや個人識別符号（例えば運転免許証の番号、マイナンバー、パスポート番号といったもの））などがあります。その情報自体が個人情報であることは個人属性情報の一部であり、個人識別符号のほうが、どちらかというと分かりやすいかと思います。

また、他のデータ項目との組み合わせにより、個人の特定につながる可能性があります。例えば氏名はないけれども、生年月日、住所、電話番号等が一緒になっているような情報も該当します。

あとは、本人にアクセスすることができる項目があります。携帯電話番号、メールアドレス、あるいは会員 ID、SNS の ID といったものが入ります。多くの事業者が収集しており、異なるデータセット間で個人を特定するための識別子として機能する可能性があります。多くの事業者が収集しているものとしては、例えばサービス ID、アカウント ID、例えば各社共通のポイントカードの ID は、加盟店であれば各社が持っている可能性があります。

最後に、個人の特定につながる特異な記述等があることです。例えば116歳であるといった情報も消さなければ特定リスクにつながることになります。それだけで個人が誰かということが、他の付加情報を参照すればすぐ分かってしまうので、これは個人識別等のリスクがあると判断されます。このように、情報が特定個人を識別するのか、そういうリスクがあるのかを見ていきます。

4)　個人識別等に係るリスクを踏まえた具体的加工方法の検討

個人識別等に係るリスクを踏まえた具体的

加工方法の検討として、具体的な加工方法を考えていくことになりますが、ここにあげているのは基本的な加工の手法であり、個人情報保護委員会の事務局レポートの代表的な加工方法を一部抜粋したものを記載しています。

例えば、項目削除とは、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項目を削除するもので、年齢のデータを全ての個人情報から削除するというようなことです。あとは使用したATMという項目があれば、全員のデータから削除するというようなことがあります。

レコード削除とは、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レコードを削除するものです。例えば、特定の年齢に該当する個人のレコードを全て削除することがあります。セル削除とは、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特定のセルを削除するもので、特定の個人に含まれる年齢の値を削除するといったことが含まれます。

例えば購買履歴のデータで、「きゅうり」や「なす」などいろいろなものがいろいろな人のデータの項目に含まれているとします。八百屋で買ったものを全部くくり出すと「野菜」という分類になるので、「きゅうり」を買った人も「なす」を買った人も、その全ての情報が「野菜」に置き換わるのが一般化です。あとは小学校1年生から6年生までと、中学校1年生から3年生までを、小学生、中学生というようにグルーピングすることも、この一般化に該当します。

トップ（ボトム）コーディングとは、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大きすぎるまたは小さすぎる値をまとめるものです。80歳、89歳というような高齢者のデータがあれば、80歳以上のデータの数値はすべて80歳以上とまとめてしまい、何人分について同じようなレコードができるようにするものです。

その他、丸め（ラウンディング）は、加工対象となる個人情報データベース等に含める数値について、四捨五入して得られる数値に置き換えることとするものです。小数点以下の秒といった単位の情報が残ってしまうと、それだけで他の情報、同じ情報とマッチングするキーになってしまうIDの性質、識別子の性質を帯びてしまうので、そういったものがマッチングのキーにならないように、ある程度抽象化した数値に置き換えようとするものです。

こういった代表的な手法を組み合わせて、匿名加工情報の具体的な加工がなされていきますが、ここで注意していただきたいのは、ここに書いているものは基本的に一例として示されているということです。したがって、絶対に氏名であればこうしなければならない、生年月日であればこうしなければならないということを列挙していないという前提で、参考としてお聞きいただければと思います。

例えば、個人属性情報について、個人情報保護委員会のレポートによると、氏名であればそれ自体個人を特定できる情報なので全部削除しなさいとされていますが、ここは例えば仮IDに置き換えることも考えられます。

このように、全部削除すること、場合によっては他の情報に置き換えることも考えられます。例えばイニシャルにするといったことも考えられるわけです。生年月日となると、住所や性別との組み合わせにより個人の特定につながる可能性があるので、原則として年

か日のいずれかを削除する、必要に応じて生年月、年齢、年代等に置き換えるという丸め（ラウンディング）を使っていただきます。

あるいは超高齢であることが分かるのであれば、その年齢を削除してしまうことでセル削除していただくことや、トップコーディングで80歳以上とまとめていただくといったことで加工することにより、特定の個人をそのデータセットから識別できないようにするのが、匿名加工情報の作成、適正加工となります。

具体的に作業してみないと分からないところもありますが、例えば郵便番号は下４桁を削除する、携帯電話番号も全部削除、サービスIDも削除しなさいということ、職業は一般的なカテゴリーに丸めなさい、例えば保険会社を金融業に丸めるといったことを組み合わせていくことにより、匿名加工情報を作成することになります。

したがって、この例からどういった情報なら活用できるのかをイメージしていただければと思います。家族構成を必ず残さなければいけないのであれば、性別のように他の項目を少し削る。また、携帯電話番号は要らないということになるかもしれませんのでその場合はこれを削る。家族構成のほうは残し、年収は丸めていただくなどということをしながら匿名加工情報を作成して、かつ、そのデータを活用することでニーズを満たせるのかを確認していってもらうことかと思います。

履歴情報の使い方も考えておかなければいけません。性質的に一番近いと思われる購買履歴について説明します。（スライド20頁の）項目としては、先ほど申し上げた履歴情報に該当します。

例えば信託の情報であれば、どういった形で、どういった商品を提供されている方なのかというものが該当します。日常の買い物についての購買情報であれば、購入店舗や購買時刻に関する情報と、他のデータセットに含まれる位置情報等との組み合わせにより出てきます。信託であればこういう財産を信託している、こういう形で運用している、どの店舗で対応しているといった情報になるかと思います。

ここに、先ほどの属性情報であれば、職業、年収、家族構成などが入ってきます。そこから特定個人を識別できないように気を付けていく加工が必要になってくると思います。

この履歴情報の加工では、属性情報の何を残しているかにより履歴情報のどこを削るかという話にもなりますし、どういった母集団の情報なのかによって特定リスクは変わってくるので、例えばＡ社も持っていてＢ社も持っている情報、Ｃ社も持っている情報となれば、加工する程度が高く、データの粒度は粗くなります。

閉じた情報、Ａ社しか持っていない情報であれば、ある程度リッチな状態で情報を外部に出したとしても、外部で個人を識別するリスクは、参照する情報がないから本人識別につながらないという趣旨ですが、これは低い。

このように、参照リスク、属性情報との組み合わせも見つつ、履歴情報は加工していくことが求められています。具体的な加工の話になってくると難しいかと思うのですが、イメージを持っていただければと思います。

また、仮名化というものがあります。仮名化とは、氏名等の直接個人を特定可能な記述等を、他の符号や番号等に置き換えることです。仮IDを付すことも許されており、例えば氏名や生年月日といったものを組み合わせ

てハッシュ化し、IDを作ることもできますが、その際注意しなければならない点があります。

何度か複数回にわたり匿名加工情報を作成した際、最初に作った情報、２番目に作った情報、３番目に作った情報に同じ仮IDが付されていれば、統合して分析することもできるので、リッチな情報を使えるため、仮IDを付したいというニーズもあるかもしれません。しかし、リッチな情報になればなるほど特定個人識別、再識別するリスクは高まると言われているので、仮IDを付すときには次のことに注意していただく必要があります。

複数のテーブル間を連携し、つなぐために使われる仮IDですが、同じ事業者に複数回にわたり匿名加工情報を提供するケースでは、いろいろな情報を一つのIDでまとめてしまうと識別リスクが高まります。

個人情報保護委員会は、そうすると識別リスクが高まるのだから、定期的に仮IDを変えることが望ましいと言っています。A社にもB社にもC社にも匿名加工情報を提供し、仮IDが全社ともに同じとなると、A社とB社とC社に出したデータは内容が違うけれども、A社とB社とC社が結託して全部情報を集めると特定個人を識別できたということでは困る。法の趣旨を潜脱することもあり得る、それに至らなくても、その識別リスクも考え、事業者ごとにIDは付け替えることが望ましいということです。

適正加工義務違反になるのか、あるいはもらったほうが識別行為の禁止義務に該当するのかという話はありますが、１回目、２回目、３回目の情報に同じ仮IDを付し、これを全部組み合わせれば特定の個人を識別できる、あるいは元の個人情報を復元することができると分かっているのに３回に分けたとすれば、適正加工義務違反になり得ます。

その意図はなかったけれども、出した先で個人情報になったらどうなるかというと、それは識別行為の禁止義務にも違反していたのではないか、という場合があります。また、使っているうちに個人情報になっているのだったら、それはもう匿名加工情報としてではなく、個人情報保護法上の個人情報保護の義務が発生してしまうので、匿名加工情報を提供された方としては知らぬ間に個人情報保護法の義務に違反している可能性もあるわけです。したがって、仮IDの取扱い方が望ましいと言われている措置ですが、気を付けないといけないということを覚えておいていただければと思います。

9.　適正な加工（法36条１項、規則19条）

今まで申し上げた1）から4）までの匿名加工情報の加工方法に係る検討プロセスの全体の流れを満たして対応していただければ、基本的には個人情報保護法36条１項、個人情報保護規則19条の適正加工の基準は満たされるように設計されています。しかし、本当に満たされているのかというのと、自社ニーズを満たすための加工を考えるためには、基準を別途ご覧いただき、検討したほうがよいかと思います。資料21頁以下に適正加工基準について記載しています。

一つ目として、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又は一部を削除することがあります。氏名、生年月日、役職等々が複数組み合わさっているようなデータの加工の方法について説明されています。

加工対象の項目と加工方法例として、団体や特定個人を識別することができる氏名や画像等は、削除したり、仮IDを置き換えるという話が出てきます。氏名以外の基本4情報であれば、削除したり、住所を市町村に置き換えていただく必要が出てきます。

本人到達性のあるメールアドレスやSNSのIDは削除してくださいとされていますが、この点も19条1号の基準で対応しなければならないケースがあることになります。これらの措置によっても、組み合わせにより特定の個人を識別することができる場合はあり得るので、具体的なデータの含まれる項目や粒度、どれだけ情報が詳細なのかをご覧いただきながら、必要な措置を検討していただく必要があります。この加工によっても識別リスクがある場合には、この後説明する5号の加工が必要になるのが、この基準の建て付けになっています。

会員IDのような実際にID連携に用いられている情報は消してくださいと言っているのが19条3号の基準になります。ここで、ダイレクトに本人に到達できるようなデータの使い方は、匿名加工情報では想定していないことが分かると思います。IDを消してしまえば、元情報や他の情報との連携が取れなくなります。例えば、各社共通ポイントカードの会員IDは、いろいろな業種、いろいろな社が持っているわけです。

それを用いて、匿名加工情報に仮に各社共通ポイントカードの番号が付いていれば、匿名加工したといって外に出すと、「これは各社共通の○○ポイントの番号だ」ということで、特定個人の情報、個人情報と突合することができてしまいます。したがって、そういったものは消しましょうと言っているのが、先ほどの1号又は3号になります。

最後に、5号は、履歴情報の加工の話です。履歴情報をどうやって加工していくのかということですが、基準だけご覧いただくと、前各号（1号から4号）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とされています。

この個人情報データベース等は、例えばこの一定地域内の人の情報や、この会社の顧客データだと母集団の情報が分かってしまうと、参照すべき個人情報がどこにあるのかも何となく認識できます。そうすると、何を見れば分かるのかという情報については、ある程度削ってもらわないと、外に出したときに、もしかしたら本人識別してしまうかもしれないリスクが伴うのが、この5号の前提にある意識です。

そのために何をするのかということですが、例えば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められる記述等との差異で、例えば小学4年生なのに190センチの子がいたら、その母集団の中では誰かというのが分かってしまいます。そういった情報を丸めてトップコーディング160センチ以上にするという形で加工してくださいということです。

その個人データベース、加工対象にしようとしているデータの集団、塊があり、その中の外れ値を見て、情報の性質を見ることが一つあります。もう一つは、何度か参照リスクと言っていますが、参照情報の入手が容易で

ある場合、公開情報や広く販売されているような情報があるのかどうか、それが入手困難なのかということと、参照情報が表形式になっていてマッチングしやすいのか、それとも散在情報の形を取っていてマッチングにはある程度の技術が必要なのかという点を勘案して、参照しやすいのかどうかというところを考えます。参照しやすければ識別につながりやすいし、参照しにくければ識別にはつながりにくいということで、参照リスクが高い場合は加工をしてください、参照リスクが低い場合は加工までは必要ない、とされています。

イメージが湧きにくいかもしれませんが、５号は、データベースの内容や性質を見て、識別するリスクが高いならデータを削ったり、置き換えなどが必要と言っている。ここは技術者などが得意なところではあるので、専門家に対応していただく必要があるかと思います。

10．匿名加工情報の例（ID-POSデータ）

実際にID-POSデータの例で、１つ目が顧客属性テーブルで、会員ID、氏名、生年月日、性別、住所、電話番号というデータがあります。

２つ目が取引情報のテーブルで、取引ID、会員ID、日時、店舗ID等の履歴が並んでいます。最後に購買履歴（顧客別）のテーブルがあるときに、これを全体として一つの社が使っているデータのセットになります。

加工方法は、まず電話番号は１号措置として、削除等をしていただきます。次に、会員IDについては、実際にその社の中でデータを連携している、この各テーブルを連携しているので、消すあるいは置き換えるという措置が必要になってきます。この電話番号と会員IDを用いて、全て鍵付きハッシュ関数で仮IDを付していただくような方法もあるかもしれません。ハッシュ化する元の情報、電話番号と会員IDを組み合わせたものがシードと言われますが、そのシードが外に漏れないようにしていただくのが、先ほど安全管理の話になります。

履歴と言われるものは、先ほどのデータベースの性質を勘案して、何を削除していくのかを検討していただくことになってきます。加工により作成される匿名加工情報には、仮ID、日時、年代、性別、住居エリア、店舗名、商品名、数量、金額を含むようなことができると考えられます。

11．識別行為の禁止（36条５項、38条）

こうして実際に作成した匿名加工情報には、識別行為の禁止義務が課されており、本人を識別するための他の情報との照合が禁止されています。例えば、データ取引の対象とするため、また、信用スコア算出のためのアルゴリズムを構築するために匿名加工情報を用いた場合、個人と関係のない情報（金融商品等の取引高といったもの）とともに傾向を統計的に分析することは、識別行為の禁止義務には違反しません。しかし、保有する個人情報と匿名加工情報の共通する記述、履歴が複数個一緒であれば、およそこの個人情報とマッチするのであろうと、この人の情報だというのが分かってしまうので、そういうものを照合キーとして利用してデータを分析することは、識別行為禁止義務に違反すると言われています。

また、匿名加工情報作成の元となった個人

情報と照合することも、当然できません。こういった規制があるので、匿名加工情報を利用しようとする際は、識別行為の禁止義務に違反しないように、まずは利用ニーズに対応しうるかを検討していただきます。会員 ID によってこの人の情報だということが分かり、その分析結果を元の個人情報に戻したいということは基本的にできないということです。

したがって、ダイレクトで One to One マーケティングがしたいというときには、匿名加工情報をそのまま使うことはできず、クラスター分析の結果をもってＡさんに何かしらの金融商品を紹介することならできます。

信用スコアを算出するためのアルゴリズムであれば、本人が誰かということは必要ないので、学習させた AI に、個人情報を新たにインプットして成果物を出すということならできます。

本人に、元の個人情報に戻したいというときには使えないということだけ覚えていただければと思います。ここでもやはり、利用ニーズを特定しておくことが重要だとお分かりいただけるかと思います。

12.　業務委託

続いて、業務委託についてです。匿名加工情報の適正加工基準をご覧いただいたときに、果たしてこれは自社の中で対応しうる部署があるのか、と思われた方もいらっしゃると思います。ですから、活用に際しては業務委託についても考えたほうがよいかもしれません。加工・活用のいずれの場合でも業務委託は認められます。ただ、その代わり、個人情報のような、個人情報取扱委託のようなスキームはありません。ですから、匿名加工情報の作成を委託した場合は、提供する自社と作成を委託された側の両者が共有で匿名加工情報の作成者になります。委託する場合は匿名加工情報を第三者提供するということで、公表と明示が必要になります。

このように､委託スキームはないけれども、普通の匿名加工情報のルールに従って対応していただくことが想定されています。委託に際しては、共有であれば、委託元も委託先も匿名加工情報の作成者になるので、公表義務を両者が負うということがあるので注意していただく必要があります。基本的には、委託先にどこまで自由にデータを使わせるのかということも、契約上縛っていただくことになるし、自分のノウハウや営業秘密といったものを渡すことになるので、個人情報保護法上は利用目的の制限はないかもしれないが、制限を課していくために契約内容を工夫するなどという話が出てくるかと思います。

13.　参考―データ活用の類型―

資料27頁に記載している個人に対する One to One マーケティング、行動ターゲティング広告といったいろいろなニーズを満たして実現するためには、先ほどまでご説明した個人情報として取扱うこと、匿名加工情報として取扱うこと、それとも統計のレベルでいいのかということを考えながら、また、管理コスト、技術力、人をどれだけ割けるのかとかいうことを組み合わせながら、目的達成のためにどういうルールを使うのか、実際にそういうことができる環境にあるのかを検討していただくことが、データの利活用に求められていると思います。

14. PDS・情報銀行・データ取引市場の台頭

ここからは参考情報ですが、これまでの話は、PDS（パーソナルデータストア）なども関係するかと思います。PDS、情報銀行、データ取引市場において匿名加工情報を使うこともあり得ると思います。ただ､PDSの場合、匿名加工情報にするという話より、本人がどこにデータを提供するのかなどを管理するツールなので、本人関与のルールづくり等々を考えていくのかと思います。

また、PDS、情報銀行、データ取引市場が、果たしてビジネスとなり得るのかという点が、注目されるかと思います。本人関与や、ルール、データの使用、どういったデータにするのかという点と、関与する者、どういうステークホルダーを登場させるのかという仕組みづくりはもちろんですが、実際にデータの価値の算定は、やはり難しいです。

資料28頁に三菱 UFJ 信託銀行の実証実験の例を記載していますが、こういうスキームがしっかりと成り立つためには、やはりデータの価値をどう算出するのかという問題があります。皆が共通認識を持たないと、価値がないものをもらっても、それにコストをかけても仕方ないという話が出てくるので､本人･企業双方のメリットはどこなのかを測りながら、共通認識を作っていくところがまず重要になるのかと思います。

15. データ活用を検討する際のポイント

最後に、実務でいろいろな企業の相談を受けながら、データ活用を検討する際のポイントを簡単にまとめています。

まず、当たり前のことですが、データ取扱いの現状把握が重要です。どの部署が、どのようなデータを、どのような目的で利用しているのかを、まずは把握していただくということです。

IT 人材はいるのかというのと、実際いないとしてもその後の採用の見通しは立てられているのかということがあります。IT 人材の採用は、人材が枯渇しているということだけではなく、見合うだけの条件を提示できるかという点もなかなか難しいと言われています。ですから、採用見通しが立てられるのかということがポイントになります。

データをクラウド上で分析するような仕組みがあるところもありますが、データ利用のインフラと、その関係の契約はどうなっているのかということが問題となります。個人情報のまま格納している場合、セキュリティ面はどうなっているのか、監査はどうやって行うのか。また、インシデントが発生したときの保証の問題も重要になってきます。

あとは保険関係として、セキュリティインシデントに対する保険があります。サイバーエッジ特約のようなものを付けていると思いますが、インシデント時に試算する実際の企業の賠償額の見込みに比して、そのカバーする額は非常に僅少なケースも多い印象です。とりあえず保険に入っているというレベルでは、実際に漏えいインシデントが発生した際にその保険だけで対応できる場合は、ほぼないのではないかと思います。そこで、こうしたクラウドなどのインフラに関する契約もきちんと見ていかないと、どこかから後々大きな損害賠償請求をされたときなどに対応できなくなることもあり得るので、データを活用するときには、しっかり見ていただいたほう

がいいと思います。

もう一つは、最初に、データを活用するにも、保護するにも、いずれにせよ全社的な総合的戦略の策定が重要になることを申し上げました。どこの部署で何をやっているのか分からないというようなことや、把握できる部署がないといったことが結構あります。経営企画が走ってしまい、いろいろなことを考えてくるけれども、法務部は後から「対応できますか」と聞かれて困るなどということもよく聞かれます。

したがって、戦略、法務、システムといった関係するプレーヤーが全部連携しうる仕組みをまず作るところから始める方が効率的ではないかと思います。

次に、守秘義務その他商慣習上又は契約上の制約があります。金融業の方々はオンプレミス（自社運用）でデータを管理してこられたと思います。これがクラウドに移行してきている中、外部委託が契約上入っていないケースをよく見ますが、それがオンプレミスの当然の所与の前提だという共通認識が顧客との間にできていて、果たしてこれを外部委託していいのか、契約を巻き直したほうがいいのかなどという話にもなるので、それは契約内容との関係ですが、少し気にしたほうがいいように思います。

また、当然この目的以外に使わないことが契約上固まっていれば、その顧客データを何か統計化して勝手に活用することも、後々契約上の責任あるいはレピュテーションリスクが問われることになるので、契約上の制約等々も見ておいたほうがいいかと思います。

諸外国の法令については、GDPR や中国のサイバーセキュリティ法など、データをどこでどう使えるのかということも関係してくるので、注意しなければなりません。

もう一つ、将来的な注意点として、やはり本人がデータを出さなければ、個人情報、パーソナルデータは活用できませんので、信用、信頼、その他本人との関係は重要になります。また、プロファイリングに関して本人との対応が求められたりすることがあります。例えば自由なプライバシーの問題、人権等の話と、自由な意思決定が確保されるのかという話、判断基準の納得感、エビデンスや透明性を確保できるのかという話も、日本国内法では規制はありませんが、注意しておかないとデータ活用のボトルネックになりかねません。

そして、データポータビリティの問題があります。１社が集めてきたデータの保存形式や項目が各社ごとに違うわけですが、Ａ社のデータとＢ社のデータを合わせたいと思ったときは、データの保存形式や項目を合わせた方が対応しやすい。データポータビリティの規制やニーズの話が進むかもしれません。本人から他にデータを移したいと言われ、それに対応していくときには、各社共通したデータの仕様を考えなければならないという話も出てくると思います。

それにより、もしかしたら個社にデータをまとめておくよりも、市場規模が拡大することもあるので、こういったデータポータビリティに対応することもあるのではないかということも、ご検討いただいてはどうかと思います。

ご清聴、ありがとうございました。

本稿は、平成31年１月29日に開催した信託セミナーにおける三浦法律事務所弁護士日置巴美氏の講演内容を取りまとめたものである。

（ひおき・ともみ）

個人情報の保護と活用を巡る近時の動向と実務対応等について

平成31年1月29日　第5回信託セミナー
弁護士　日置　巴美

三浦法律事務所
Miura&Partners

Miura&Partners

はじめに

データを活用しなければ、国内・国際競争の中で、既存のビジネス優位性の保持、そして技術力を活かすことが危ぶまれている。
他方、攻めの利用を進めるあまり、違法、炎上のリスクが顕在化することに常に注意しなければならない。

- **ビッグデータの活用と新規ビジネスの創出**
- **共同事業に伴うデータの利用権限の設定や知的財産の取扱い**
- **セキュリティ・インシデントへの対応**
- **戦略的な人事・労務管理**
- **グローバルなビジネス展開と現地法令**

データの取扱いの巧拙がビジネスのみならず企業の勝負を決める。

「個人情報・プライバシー」に無関係な企業など存在しない。新規産業、新規ビジネスモデルを展開するため、攻守揃った総合的なデータ戦略を構築することが肝要

Miura&Partners

略歴

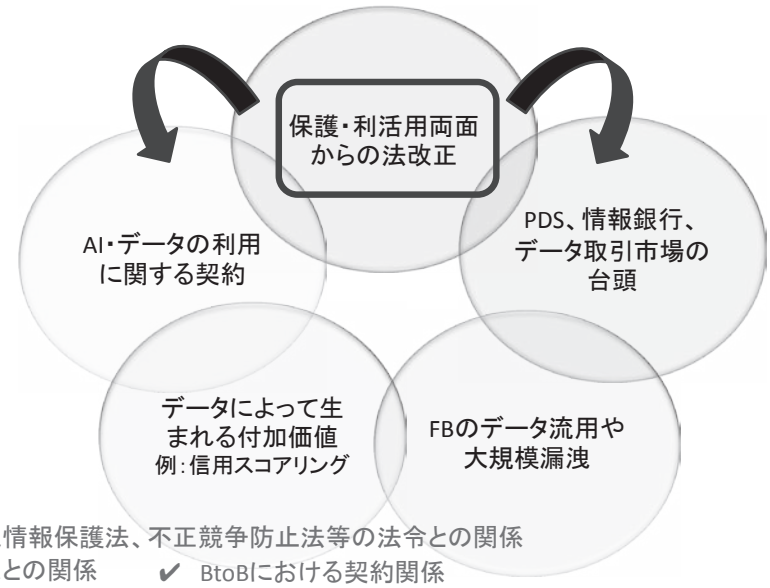
2010年　国会議員政策担当秘書（～2013年、一部期間を除く）
2013年　消費者庁消費者制度課政策企画専門官（個人情報保護推進室併任）（～2015年）
2014年　内閣官房情報通信技術（IT）総合戦略室参事官補佐併任（～2015年）
2016年　個人情報保護委員会事務局参事官補佐
2016年　弁護士法人内田・鮫島法律事務所（～2019年）
2017年　東京大学政策ビジョン研究センター客員研究員（シニア・リサーチャー）（～現在）
2018年　株式会社Data Sign社外取締役（～現在）
2018年　情報ネットワーク法学会監事（～現在）
2019年　三浦法律事務所（～現在）

✔内閣官房情報通信技術（IT）総合戦略室において、2015年の「個人情報の保護に関する法律」（平成15年法律第57号）の改正及びその後の政令・規則改正等の施行準備に携わる。
✔国立情報学研究所「匿名加工情報の適正な加工の方法に関する報告書 2017年2月21日版」共同執筆
✔独立行政法人経済産業研究所「企業において発生するデータの管理と活用に関する研究」（18-J-028）共同執筆

2

Miura&Partners

データ保護と活用のトピックス



✔ 個人情報保護法、不正競争防止法等の法令との関係
✔ 本人との関係　　✔ BtoBにおける契約関係

3

Miura&Partners

個人情報保護法の「匿名加工情報制度」

保護対象となる「個人情報」

- 個人情報とは？
- 「容易照合性」と提供先基準・提供元基準

目的外利用、第三者提供と同意

- 利用目的制限（15条、16条）
- 第三者提供の制限（23条、24条）

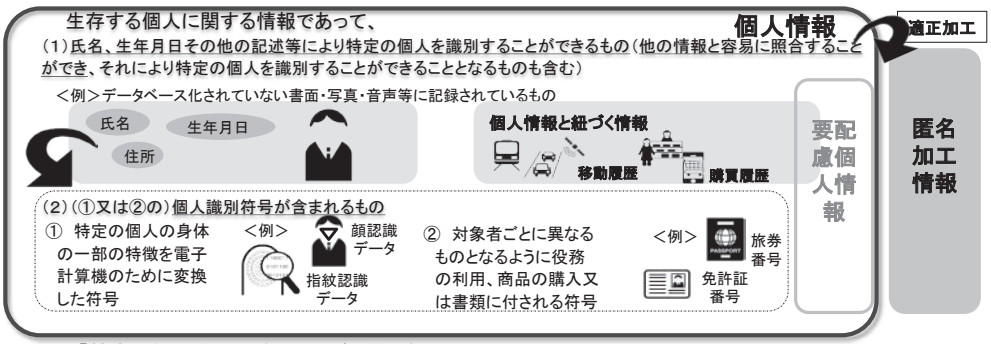
匿名加工情報制度の創設

- 匿名加工情報（2条9項）と取扱いルール（4章2節）の創設

4

Miura&Partners

保護対象となる個人情報　個人情報とは？



○「特定の個人を識別することができるもの」

個人情報とは、特定の個人を識別することができるものをいう。

「情報単体又は複数の情報を組み合わせて保存されているものから、社会通念上そのように判断できるもの」であるとされ、その判断基準について、「一般人の判断力や理解力をもって、生存する具体的な人物と情報との間に同一性を認めるに至ることができる」か否かによるとされる。

典型例：氏名

　正面から顔が判別できる画像、映像

個別判断が必要な例：

　性別、生年月日、住所、電話番号、勤務先、役職等が組み合わさった情報

　購買履歴、位置に関する情報などが蓄積されることで行動習慣が明らかとなる情報

5

Miura&Partners

保護対象となる個人情報　容易照合性と提供先基準・提供元基準

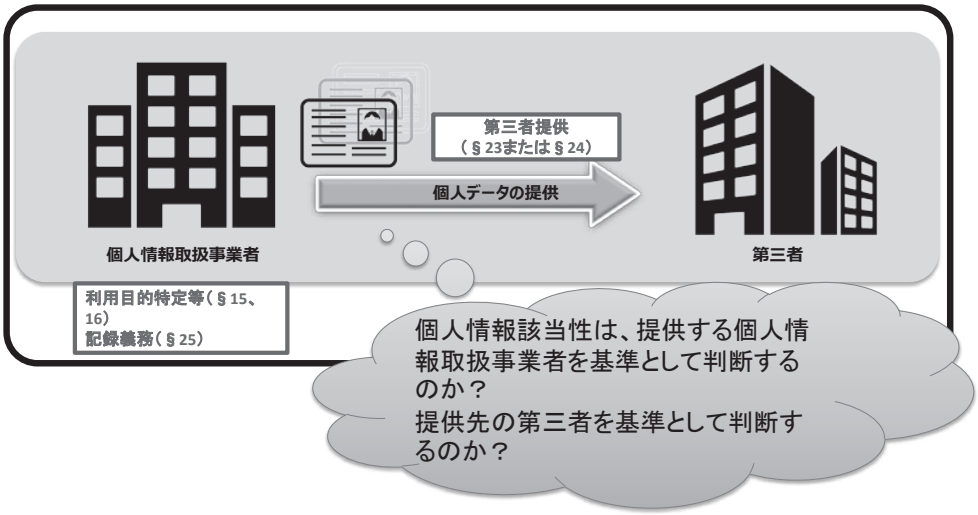
容易照合性（§２Ⅰ①かっこ書）：
情報を取り扱う者が、特別の調査を行うことや、特別の費用を要することなく、通常行っている業務における一般的な方法で、他の情報と照合が可能な状態にあることをいう。
そのような状態にあるといえるか否かは、実際に情報を取り扱う個人情報取扱事業者を基準として、当該個人情報取扱事業者における事情（保有する各情報にそれぞれどのような項目が含まれ、どのような内容であるか、これにアクセスできる者の存否、社内規定の整備等の組織的な体制、情報システムのアクセス制御等の技術的な体制等が挙げられるが、これに限られない）を総合的に勘案して判断される。

例えば・・・
○氏名等を含む情報を取得し、その蓄積される情報の保存については、項目ごとに区分して別々に行っているとしても、氏名等を含む情報とIDを付してそれぞれ連携させていたとする。この場合、区分された情報のうち、それのみでは特定の個人を識別することができないものがあったとしても、IDによって他の特定の個人を識別することができる情報と連携しているなどの事情から容易照合性が認められ、これによって特定の個人を識別することができるのであれば、そのような情報も個人情報に該当する。
○情報取得の段階で、項目ごとに区分した情報を別々に管理できるようにしていたとしても、取得される情報の項目を設定すること、取得した情報を制御すること等ができるのであれば、安易に容易照合性を否定することはできない。

6

Miura&Partners

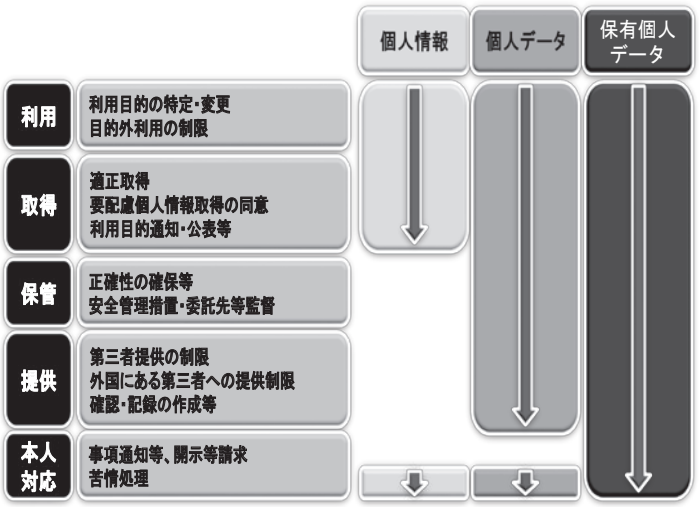
保護対象となる個人情報　容易照合性と提供先基準・提供元基準



7

Miura&Partners

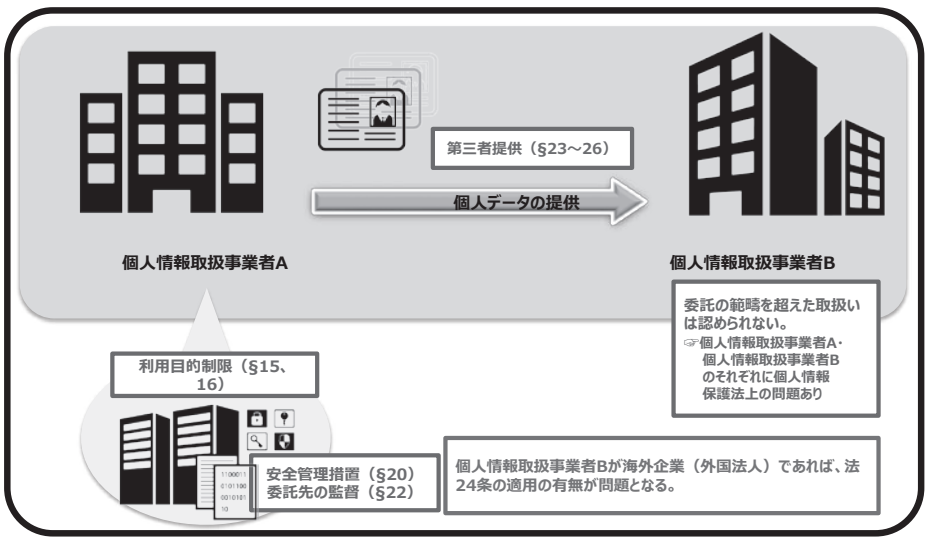
目的外利用、第三者提供と同意



8

Miura&Partners

目的外利用、第三者提供と同意



9

Miura&Partners

匿名加工情報制度の創設

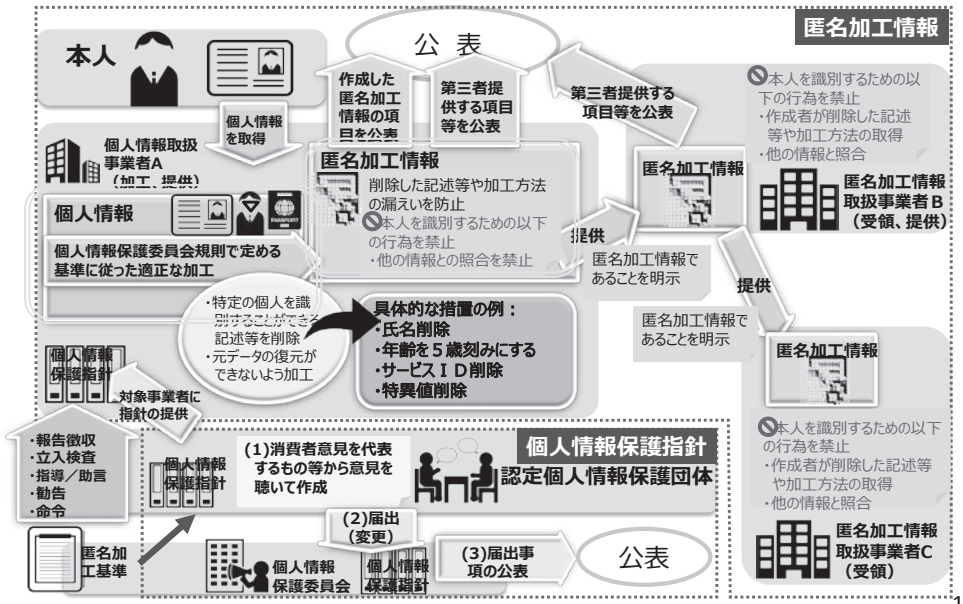
●加工後の情報から、なお特定の個人を識別できる（具体的な人物が明らか）なもの　（例：詳細な位置情報）
●「容易照合性」があり、特定の個人を識別できる（具体的な人物が明らかとなる）もの
（例：加工前・後の情報をIDによって連携させる場合
履歴によって加工前の情報と照合可能な場合）
→ **依然として、個人情報に該当する。**

●特定の個人を識別できず（具体的な人物が明らかとならず）、個人情報を復元できないように加工したもの
●個人情報保護委員会規則の適正加工基準（施行規則19条に定めるもの）に従う必要がある
●「識別行為の禁止義務」（法36条５項）があり、「容易照合性」はない
→ **匿名加工情報に該当する。**

10

Miura&Partners

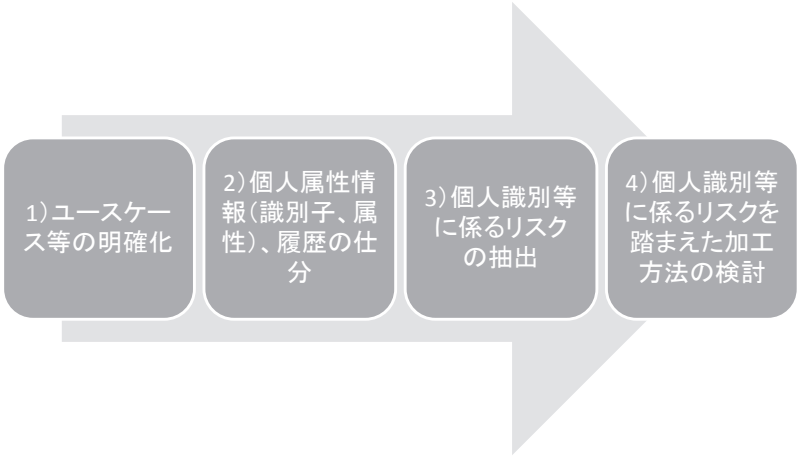
匿名加工情報（2条9項）と取扱いルール（4章2節）の創設



11

Miura&Partners

加工方法にかかる検討プロセスの全体の流れ



✔適正な加工(36条1項)のみならず、識別行為の禁止義務(同条5項、38条)も併せて検討する。
✔信託協会「匿名加工情報の取扱いに関するルール」が参考になる。

12

Miura&Partners

参考　1)ユースケース等の明確化

目的

- 加工の対象となるデータの項目と加工方法をリスクに応じて絞り込むため

確認事項

- 匿名加工情報の作成者における業務・サービスの概要
- 匿名加工情報の作成に用いる個人情報データベース等の項目、規模等(個人情報データベース等によって識別される個人の人数、データ項目の内容(カテゴリーなどの離散値、年齢などの整数値、振込金額などの連続値、データの項目の内容および取り得る値の集合、最小値、最大値など))
- 匿名加工情報に含める必要のあるデータの項目、規模(データ件数)
- 匿名加工情報の利用目的
- データの流通範囲
- 提供するデータの期間
- 匿名加工情報の提供の継続性
- 過去に匿名加工情報を提供したことがある事業者か否か

13

Miura&Partners

参考　2)個人属性情報(識別子、属性)、履歴の仕分

目的

- 3)個人識別等に係るリスクの抽出を効率的に行うこと、規則19条の加工基準に対応すること

仕分項目

- 個人属性情報(個人情報に係る本人の基本的な属性に関わる情報の項目)
  氏名、生年月日、住所、郵便番号、マイナンバー、パスポート番号(旅券番号)、固定電話番号、携帯電話番号、CIF番号、口座番号、クレジットカード番号、電子メールアドレス、職業(勤務先名等)、年収、預金額・借入額、家族構成　　など
- 履歴情報(個人の行動に伴い発生する行動の履歴に関わる情報の項目)
  取引日時、取引金額、利用店舗・利用ATM、ウェブ閲覧履歴　　など

14

Miura&Partners

参考　3)個人識別等に係るリスクの抽出

目的

- 1)、2)を踏まえて適切な加工方法を採用すること、規則19条に対応すること

想定されるリスク

- その情報自体で個人を特定できる(個人属性情報の一部)
- その情報自体が個人情報である(個人識別符号、個人属性情報の一部)
- 他のデータ項目との組み合わせにより、個人の特定につながる可能性がある(個人属性情報の一部)
- 本人にアクセスすることができる(個人属性情報の一部)
- 多くの事業者が収集しており、異なるデータセット間で個人を特定するための識別子として機能する可能性がある(個人属性情報の一部、履歴情報)
- 個人の特定につながる特異な記述等がある(個人属性情報の一部、履歴情報)

15

Miura&Partners

参考　4）個人識別等に係るリスクを踏まえた加工方法の検討

①　匿名加工に用いられる代表的な加工手法

手法名	解説
項目削除	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項目を削除する 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。
レコード削除	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レコードを削除す るもの。例えば、特定の年齢に該当する個人のレコードを全て削除すること。
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特定のセルを削 除するもの。例えば、特定の個人に含まれる年齢の値を削除すること。
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。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。

16

Miura&Partners

参考　4）個人識別等に係るリスクを踏まえた加工方法の検討

①　匿名加工に用いられる代表的な加工手法（続き）

手法名	解説
レコード一部抽出	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一部のレコードを(確率的に)抽出すること。いわゆるサンプリングも含まれる。
項目一部抽出	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項目の一部を抽出すること。例えば、購買履歴に該当する項目の一部を抽出すること。
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。
丸め(ラウンディング)	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、四捨五入等して得られた数値に置き換えることとするもの。
データ交換（スワッピング）	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。例えば、異なる地域の属性を持ったレコード同士の入れ替えを行うこと。
ノイズ（誤差）付加	一定の分布に従った乱数的な数値等を付加することにより、他の任意の数値等へ と置き換えることとするもの。

「個人情報保護委員会事務局レポート：匿 名 加 工 情 報 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 」図表4-3 代表的な加工手法（一部抜粋）

17

Miura&Partners

参考　4）個人識別等に係るリスクを踏まえた加工方法の検討

② 情報の項目と想定されるリスク及び加工例

項目	想定されるリスク	加工例（「削除」は置き換えも含む）
個人属性情報		
氏名	それ自体で個人を特定できる	全部削除
生年月日	住所（郵便番号）、性別との組合せにより、個人の特定につながる可能性がある。	・原則として、年か日の何れかを削除する。必要に応じて生年月、年齢、年代等に置き換える。【丸め】 ・超高齢であることがわかる生年月日や年齢を削除する。【セル削除／トップコーディング】
住所	生年月日、性別との組合せにより、個 人の特定につながる可能性がある。 本人にアクセスすることができる。	・原則として、町名、番地、マンション名等の詳細を削除する。【丸め】 ・レコード総数等に応じて、県単位や市町村単位へ置き換える。【丸め】
郵便番号	生年月日、性別等との組合せにより個 人の特定に結びつく可能性がある。	下4桁を削除する。【丸め】

18

Miura&Partners

参考　4）個人識別等に係るリスクを踏まえた加工方法の検討

② 情報の項目と想定されるリスク及び加工例（続き）

項目	想定されるリスク	加工例（「削除」は置き換えも含む）
個人属性情報		
携帯電話番号	多くの事業者が収集しており、異なるデータセット間で個人を特定するための識 別子として機能し得る。 本人にアクセスすることができる。	全部削除【項目削除】
サービスID、アカウントID	多くの事業者で共用される ID の場合 は、個人を特定するための識別子として 機能する。	全部削除【項目削除】
職業	住所や年収等との組合せにより、個人 の特定につながる可能性がある。	勤務先名を職種等のカテゴリーに置き換える。【一般化】
年収	職業や住所等との組合せにより、個人の特定につながる可能性がある。 超高収入の場合、それ自体から個人を特定できる可能性がある。	・具体的な年収を収入区分へ置 き換える。【丸め】 ・超高収入の値を削除する。 【セル削除/トップコーディング】

19

Miura & Partners

参考　4）個人識別等に係るリスクを踏まえた加工方法の検討

② 情報の項目と想定されるリスク及び加工例（続き）

項目	想定されるリスク	加工例（「削除」は置き換えも含む）
履歴情報		
購買履歴	購入店舗や購買時刻に関する情報と 他のデータセットに含まれる位置情報等 との組合せにより、個人の特定につながる可能性がある。 特異な物品の購買実績と居住エリア 等との組合せにより、個人の特定につながる可能性がある。	・購入店舗や購買時刻の詳細な 情報を削除する。【丸め】 ・特異な購買情報（超高額な利 用金額や超高頻度の利用回数 等）を削除する。 【セル削除/トップコーディング】

「個人情報保護委員会事務局レポート：匿名加工情報 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」図表4-4　情報の項目と想定されるリスク及び加工例（一部抜粋）

20

Miura & Partners

適正な加工（法36条1項、規則19条）

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又は一部を削除すること（当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）

【加工対象項目×加工方法例】
i　単体で特定の個人を識別することができるもの（氏名、顔画像）
　→　削除、仮IDへの置き換え
ii　氏名以外の基本4情報（住所、生年月日、性別）
　→　削除、住所を市区町村へ、生年月日を年までに置き換え（複数項目での調整可。詳細に残したい項目があれば、その他の項目を削除するなど）
iii　現在所属する・過去に所属した会社、学校等の団体、職歴、学歴であって、具体的な名称等を含むもの
　→　具体的名称を削除・一般化
iv　本人到達性のあるメールアドレス、SNSのID
　→　削除
v　本人到達性のある電話番号（スマートフォン、自宅の電話番号、職場の電話番号）
　→　削除
vi　クレジットカード番号
　→　削除

※　これらの措置によっても、組み合わせによって特定の個人を識別することができる場合がある。項目削除、一般化、丸め（ラウンディング）等の加工をさらに行うことや、上記項目のすべての組み合わせが一意にならないように加工することが考えられる（先にこの加工を行うことも認められる）。
※　この加工によってもリスクが認められる場合、5号の加工が必要であることに注意

21

Miura&Partners

適正な加工（法36条1項、規則19条）

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（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）
例）運転免許証の番号の削除
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（現に個人情報取扱事業者において取り扱う情報を相互に連結する符号に限る。）を削除すること（当該符号を復元することのできる規則性を有しない方法により当該個人情報と当該個人情報に措置を講じて得られる情報を連結することができない符号に置き換えることを含む。）
例）会員ID（メールアドレスを利用している場合は、これを含む）を削除等する。
④特異な記述等を削除すること（当該特異な記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）
社会通念上“特異”な記述（年齢が110歳であること）を削除・置き換えする。

22

Miura&Partners

適正な加工（法36条1項、規則19条）

⑤前各号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

（ⅰ）「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」に関する措置

加工対象情報内に含まれる個人情報間の記述の際を踏まえ、レコード削除、置き換え（トップ（ボトム）コーディング、一般化）を行う。

（ⅱ）「その他の個人情報データベース等の性質」に関する措置

“参照リスク”、“本人に関する情報（その組み合わせを含む）が一意か”を踏まえ、そのいずれかのリスクを低減するための加工が求められる。

- 参照情報の入手が容易である場合：公開情報、広く市販等されているもの（ネット上の名簿、SNS等にアップロードされた公開プロフィール等
- 参照情報の入手が困難である場合：会社の同僚、本人がよく利用する店舗の店主等、関係の近い者のみが知り得る情報

×

- 参照情報が表形式になっていて、一意な情報と直ちに単純な機械的なマッチングが可能
- 参照情報が文章の形式でその中から該当する項目の情報を探しでしてマッチングを行う必要がある（ブログのエントリーから特定の商品の購入を探し出す）

一意性を失わせる加工としては、セル削除、レコード削除、項目削除がある。

参照リスクの低減には、丸め（ラウンディング）、一般化、ミクロアグリゲーション、トップ（ボトム）コーディング、ノイズ付加等がある。

23

Miura&Partners

匿名加工情報の例（ID-POSデータ）

○加工によって作成される匿名加工情報には、仮ID,日時、年代、性別、居住エリア、店舗名、商品名、数量、金額を含むことができる。

顧客属性テーブル

会員ID	氏名	生年月日	性別	住所	電話番号
224523	田中 一郎	1972年4月4日	男	神奈川県横浜市中区富士見町X-X-X	045-222-XXXX
225412	佐藤 幸子	1993年12月9日	女	千葉県船橋市西船Y-Y-Y	090-444-YYYY
231622	鈴木 博	1963年8月23日	男	東京都墨田区押上Z-Z-Z	03-1234-ZZZZ

取引情報テーブル

取引ID	会員ID	日時	店舗ID	店舗名	担当者ID	商品ID	商品名	数量	…
10032	224523	2016/8/2 18:25	KN013	みなとみらい店	101	151	午後のミルクコーヒー	1	…
11252	225412	2016/10/4 07:13	CB002	西船橋駅前店	305	288	近江屋チョコレート（ホワイト）	4	…
10125	231622	2016/8/30 11:59	TK101	錦糸町店	211	793	バンドウクジラぬいぐるみ（大）	1	…
…	…	…	…	…	…	…	…	…	…

購買履歴（顧客別）テーブル

会員ID	取引ID	日時	店舗ID	店舗名	担当者ID	商品ID	商品名	数量	金額	商品ID	商品名	…
224523	10032	2016/8/2 18:25	KN013	みなとみらい店	101	151	午後のミルクコーヒー	1	150	188	ふんわりつぶアンパン	…
224523	10125	2016/8/3 7:09	KN051	富士見店	004	874	BUSSコーヒー（無糖）	2	240	-	-	-
225412	10252	2016/8/5	KN043	横浜駅前店	017	342	フレッシュYシャツ（紺）	1	8980	321	慶事用ネクタイ（銀）	…
224523	…	…	…	…	…	…	…	…	…	…	…	…

24

Miura&Partners

識別行為の禁止（36条5項、38条）

匿名加工情報を取り扱うに当たっては、「識別行為の禁止義務」に注意する必要がある。
匿名加工情報は、作成者、受領者ともにこの義務に反しない限り、様々な用途を設定し、利用することが可能。
「識別行為の禁止義務」とは、匿名加工情報の作成に用いられた個人情報の本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ことをいう。

例えば、データ取引の対象とするため、また、信用スコア算出のためのアルゴリズムをつくるために匿名加工情報を用いる場合、
・個人と関係のない情報（例：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（○）
・保有する個人情報と匿名加工情報の共通する記述等を選別し、これを照合キーとして利用してデータを分析する（×）
・匿名加工情報を、作成の元となった個人情報と照合すること（×）
等、識別行為の禁止義務による制限がある。
匿名加工情報を利用しようとする際は、これに留意し、まずは、利用ニーズに対応しうるかを検討する必要がある。

25

Miura&Partners

業務委託

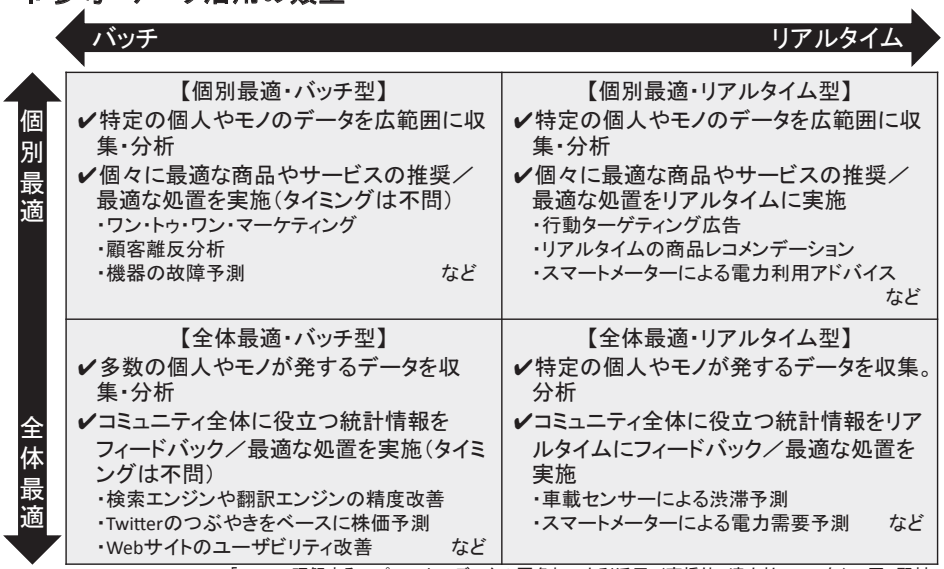
✔加工、活用に当たって、業務委託は認められるか？

✔委託に際して注意すべきポイントは何か？

26

Miura&Partners

参考　データ活用の類型



「Q&Aで理解する！パーソナルデータの匿名加工と利活用」（高橋他、清文社、2017年）17頁、野村総合研究所 IT ロードマップセミナーSPRONG2012「ビッグデータの真実　～ビッグデータの誤解を解く～」を基に作成された図

27

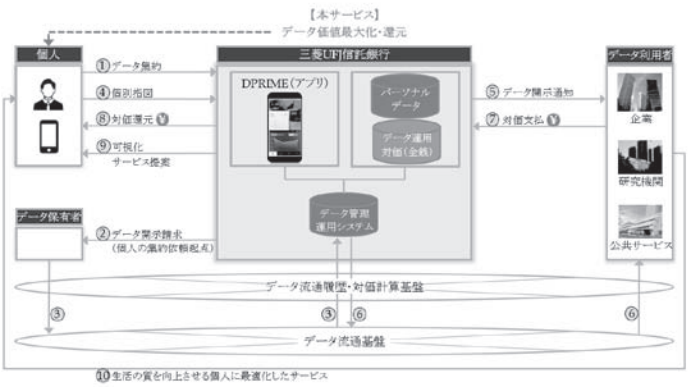
Miura&Partners

PDS・情報銀行・データ取引市場の台頭

PDS（Personal Data Store）	他者保有データの集約を含め、個人が自らの意思で自らのデータを蓄積・管理するための仕組み（システム）であって、第三者への提供に係る制御機能（移管を含む）を有するもの。
情報銀行（情報利用信用銀行）	個人とのデータ活用に関する契約等に基づき、PDS等のシステムを活用して個人のデータを管理するとともに、個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上、データを第三者（他の事業者）に提供する事業。
データ取引市場	データ保有者と当該データの活用を希望する者を仲介し、売買等による取引を可能とする仕組み（市場）。

「平成30年版　情報通信白書」図表1-2-1-1
（出典）IT総合戦略本部 データ流通環境整備検討会「AI、IoT時代におけるデータ活用ワーキンググループ　中間とりまとめ」（2017）

【本サービスの具体的スキーム】



2018年7月18日
三菱UFJ信託銀行株式会社
「新たなデータ管理サービス提供に向けた実証実験の開始について」

28

Miura&Partners

データ活用を検討する際のポイント

データ取扱いの現状把握

- どの部署が、どのようなデータを、どのような目的で利用しているか？
- IT人材はいるか。採用の見通しは立てられるか。
- データ利用のインフラと契約はどうなっているか。
- 統括しうる部署はあるか、戦略、法務、システム等、関係するプレーヤーが連携しうるか。

守秘義務その他商慣習上又は契約上の制約

諸外国の法令

将来的な注意点　-　信用、信頼その他本人との関係

- プロファイリングと、本人への対応
- データポータビリティ

29

Miura&Partners

ご清聴いただき、ありがとうございました。
https://www.miura-partners.com/
tomomi.hioki@miura-partners.com

30