基礎から振り返る 個人情報保護法の実務対応

2025年2月19日（水）

Seko Syuhei
世古 修平（66期）
当会会員

【略歴】
2014年
デロイト トーマツ コンサルティング
合同会社 入社
2017年
PwCコンサルティング合同会社 入社
2020年
LINEヤフー株式会社 入社
インハウスハブ東京法律事務所 入所
2022年
法律事務所LEACT 入所

CONTENTS

第1 個人情報の基礎

1 個人情報保護法はなぜ難しい?

個人情報の保護に関する法律（個人情報保護法）が難しい理由は、大きく分けて4つあります。

1つ目は、日常用語でいう「個人情報」の定義と、法律用語でいう「個人情報」の定義に乖離があることです。非法律家の方に対して誤解がないように説明することは難しいと感じます。

2つ目は、個人情報保護法を理解する前提として、技術理解が求められ、新しい技術・仕組みへのキャッチアップが必要であることです。「個人データ」の定義に「データベース」が登場していることからも分かるように、データベースについての理解はこの法律の根幹に関わります。

3つ目は、余白の広さです。個人情報保護法が対象とするデータテクノロジー領域は、その展開が早いことにも起因し、重要な情報が法律には何も書いていないことが多々あります。実務におい

図1

※出所：ストレッチ専門店 Dr.stretch　https://doctorstretch.com/reserve/contact/

ては、個人情報保護法以外に、個人情報の保護に関する法律についてのガイドライン※1（ガイドライン）や「個人情報の保護に関する法律についてのガイドライン」に関するQ&A※2（FAQ）、パブリックコメント、海外法や社会情勢に基づいた判断が求められます。

4つ目は、裁判例の少なさです。他の法分野ですと、偏った独自説は訴訟手続や裁判例によって是正されますが、個人情報保護法においてはそのような機会が少ないです。

2 個人情報の定義を正確に理解しよう。

個人情報保護法は、「個人情報」について、階層的に定義を置いています。一番広い定義として「個人情報」があり、個人情報のうち一定の条件を満たしたものを「個人データ」と呼びます。そして、「個人データ」のうち一定の条件を満たしたものを「保有個人データ」と呼びます。

I 「個人情報」の定義

個人情報保護法2条1項をご覧ください。

> 第二条
> 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、次の各号のいずれかに該当するものをいう。
> 一　当該情報に含まれる氏名、生年月日その他の記述等（中略）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。）
> 二　個人識別符号が含まれるもの

まず、「生存する個人に関する情報」であることが個人情報の要件です。この点、ガイドラインは、「個人に関する情報」とは、「個人の属性に関して、事実、判断、評価を表す全ての情報」として、非常に広く定義しています。例えば、私が買ったもの、私が読んだウェブサイト、私に対して企業が付与したロイヤルティーについてのランク情報などは、全て個人に関する情報です。また、「評価情報、公刊物等によって公にされている情報」も個人に関する情報に含まれます。

その上で、個人情報保護法2条1項は、「次の各号」への該当性を求めています。1号について掘り下げて説明しますが、まずは、1号本文について、具体例として 図1 のサービス申込みフォームをご覧ください。前提として「名前」、「電話番号」、

※1 https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/　※2 https://www.ppc.go.jp/personalinfo/faq/APPI_QA/

「希望店舗」といった項目は、全て「個人に関する情報」です。その上で、これらの情報が1号本文にも該当するかを検討します。このとき、どうしても「氏名」や「生年月日」に注目してしまいがちですが、条文には「もの」全体が個人情報に該当すると書いてあります。したがって、「もの」に含まれるのであれば、構成要素である、「希望店舗」、「希望日時」、「希望コース」も、個人情報に該当するということです。

続いて、1号括弧書きですが、具体例として、図2-1の「ユーザー登録情報」と「利用履歴情報」のテーブルを想定します。ユーザー登録情報は氏名を含みますので、全体が個人情報となります図2-2。一方で、利用履歴情報は氏名を含みませんので、個人情報になるのか問題となります図2-3。この答えが、1号の括弧書きに書いてあります。企業は一般にデータを活用する上で、ユーザーに対してIDを割り振りますが、ユーザーIDはテーブル間での照合を容易にする機能を果たしています。そのため、ユーザー登録情報のテーブルが個人情報であることは当然の前提として、利用履歴情報のテーブルも、個人情報であるユーザー登録情報のテーブルと「容易に照合することができ」るため、括弧書きにより個人情報に該当することになります図2-4。

以上を踏まえると、企業における実務的な対応としては、ユーザーIDにひも付く個人に関する情報は、基本的に全て個人情報と考えることになります。

図2-1

ユーザー登録情報

ユーザーID	氏名	電話番号	メールアドレス
00001			
00002			

利用履歴情報

ユーザーID	Aサービス利用履歴情報
00001	
00002	

図2-2

ユーザー登録情報

ユーザーID	氏名	電話番号	メールアドレス
00001			
00002			

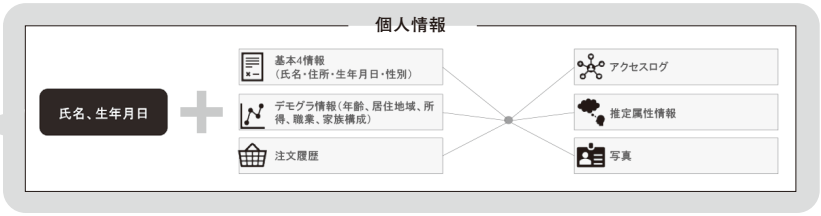
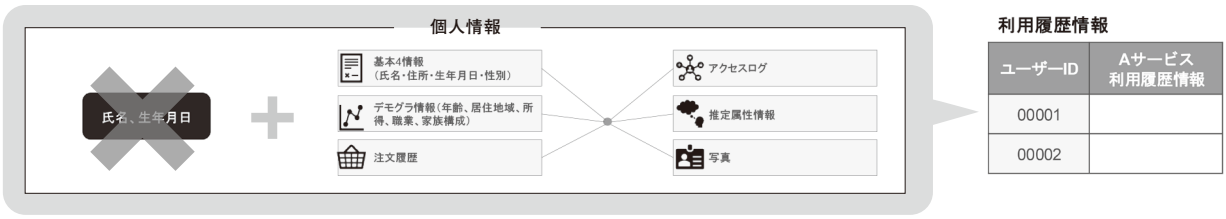


図2-3



利用履歴情報

ユーザーID	Aサービス利用履歴情報
00001	
00002	

図2-4

ユーザー登録情報

ユーザーID	氏名	電話番号	メールアドレス
00001			
00002			

利用履歴情報

ユーザーID	Aサービス利用履歴情報
00001	
00002	

こちらも個人情報

Ⅱ「個人データ」の定義

個人情報保護法16条1項及び3項をご覧ください。「個人データ」の定義を規定しています。

「個人情報」と「個人データ」の区別について知っていると何がよいかというと、例えば、漏えい等が生じた場合には個人情報保護委員会への報告が必要になりますが、報告が必要になるのは「個人データ」であって、「個人情報」ではありません。したがって、個人情報が漏えいしただけでは、原則として報告は不要ということが分かります*。

第十六条
（略）「個人情報データベース等」とは、個人情報を含む情報の集合体であって、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。）をいう。
一　特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
二　前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの
（略）
3　この章において「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う。

Ⅲ「保有個人データ」の定義

個人情報保護法16条4項をご覧ください。「保有個人データ」については、後述します。

第十六条
4　この章において「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことができる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの以外のものをいう。

*ただし、「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」に注意（ガイドライン通則編3-5）

第2 実務対応

この章では、クライアントからよく寄せられる以下の8つの相談について、ケースごとに解説します。

1 相談①：プライバシーポリシーを作成してください。

これだけ世間的に普及し、ほぼ全ての事業者が持っていそうなプライバシーポリシーですが、実は日本にはプライバシーポリシーの作成を義務付ける法律はありません。それでもなぜ、事業者がプライバシーポリシーを作成するのかというと、個人情報保護法32条が、「次に掲げる事項について、本人の知り得る状態に置かなければならない」とのルールを定めており、政令の10条で「データの安全管理のために講じた措置」「苦情の申出先」「認定個人情報保護団体の名称」等をその要素として定めているからです。

続いて、何をプライバシーポリシーに書けばい

いのかですが、大きく3つに整理することができます。1つ目は、「事業者のデータの取扱い」です。取得してから最終的に消去するまでのライフサイクルを踏まえた、各段階での取扱いを書きます。例えば、保有個人データの適正な取扱いの確保に関して必要な事項がこれに当たります。2つ目は、「本人の権利」です。本人に法律上認められた権利とその行使方法を書きます。3つ目は、「その他の事務的な事項」です。事業者への連絡方法や、最終更新日、プライバシーポリシーの更新手続を書きます。

2 相談②：個人情報が漏えいしてしまいました。

Ⅰ 外部弁護士に求められる役割

企業におけるインシデント対応において、外部弁護士に求められる役割は、以下の3つです。

1つ目は、冷静にインシデント対応の全体像を描くことです。漏えい等が発生した場合、インシデント対応チームは個人情報保護委員会への報告という時間的な制約に追われることになります。しかし、内部の実務担当者は、目の前のインシデントをどうにかするために手いっぱいなことが多いです。そんなとき、外部者としての冷静な目線で、報告までの道筋を描いてあげましょう。

2つ目は、官公庁とのコミュニケーションをサポートすることです。ほとんどのクライアントは、官公庁とのコミュニケーションに慣れておらず、又は苦手意識を持っていることが多いです。このようなときに、発生した事象や対策について、事業者として必要な主張を行うサポートが求められていると思います。

3つ目は、社内担当者間のコミュニケーションを取り持つことです。一般的には法務部門がリードしてインシデント対応を行うことが多いですが、広報・渉外部門や、経営・事業部門、技術部門など、関係部門ごとの思惑に振り回されることも少なくありません。そのようなときに、客観的な立場で関係者の間を取り持ち、会社としての方向性を調整することが重要です。

Ⅱ インシデント対応の何が辛いか—法律についての誤解

インシデント対応で生じる法律の誤解について、大きく4つに分けてお話しします。

1つ目は、個人情報の定義から生まれる誤解です。日常用語でいう「個人情報」の定義と、法律用語でいう「個人情報」の定義に乖離があるので、ここでミスコミュニケーションが生まれてしまうことがよくあります。普段から定義部分だけでも浸透を図りたいところです。

2つ目は、漏えいの定義から生まれる誤解です。「漏えい」とは、個人データが外部に流出することをいいますが、典型事例以外だと、一瞬、「あれ？これって漏えいだっけ？」 と迷うパターンが結構あります。報告が必要な要件を理解しておいて、社内対応を迷わせないことが重要です。

3つ目は、漏えい元基準に関する誤解です。ユーザー登録情報が被害に遭った場合に、個人データの漏えいに該当するという結論は違和感がないと思いますが、利用履歴情報が被害に遭った場合はどうでしょうか。ここについては、個人情報保護委員会から答えが出ていて、「対象となった情報が個人データに該当するかどうかは、当該個人データを漏えい等した個人情報取り扱い事業者を基準に考えることになります」とされています。つまり、漏えい先にとって、その情報が個人データか否かは関係がなく、漏えい元が個人データとして管理するデータが漏れたら漏えいなのです。よって、利用履歴情報が単独で被害に遭った場合も漏えいに該当しますので、注意が必要です。

4つ目は、発生した「おそれ」のある事態についての誤解です。報告対象になるのは、実際に漏えいが発生した場合だけではなく、漏えいが発生したおそれがある場合も含まれます。おそれがある場合について、ガイドラインは、「その時点で判明している事実関係からして、漏えい等が疑われるものの漏えい等が生じた確証がない場合」と

説明しますが、よく分かりませんよね。ここは、個人情報保護委員会と事業者がよく対立するところでもあります。「当該事案は漏えいのおそれがない」ということについて個人情報保護委員会と交渉するときには、説明のロジックを準備するにあたって技術系のコンサル企業やセキュリティーベンダーにリポート等を書いてもらうことも役立ちます。

Ⅲ インシデント対応の何が辛いか —実務上の落とし穴

インシデント対応で生じ得る実務上の落とし穴について、大きく4つに分けてお話しします。

1つ目は、経営層の反対です。法律上、報告義務が発生するケースはそれなりに広く、実際にはそれほど大きな影響がないようなものにも報告義務が課されるケースがあります。平常時にインシデント対応訓練をして、こういうことが起こったら報告・通知をしなきゃいけないんだということを経営層に理解しておいてもらうことが重要です。

2つ目は、我々弁護士側の技術理解の不足です。発生した事案やその原因を調査するのは技術部門ですが、漏えい等の報告を進める上で法務や外部弁護士はそれを解釈して言い換える必要があるためです。これを解決するためには、法務部門か技術部門のどちらかが壁を乗り越えて、越境していかないといけません。広く浅く知識を得るために、資格試験を勉強してみるのもよいと思いますし、私が試験委員をしている情報処理技術者試験という国家試験もぜひ受けてみてほしいです。

3つ目は、グループ間共有です。ピラミッド構造をしたグループ会社において、親会社の管理するインフラ上でインシデントが発生したとします。グループ会社間では、相互に個人データの受委託関係が発生しているのが通常ですし、保険的に共同利用の定めを置いていることも多いです。さらに、グループ外の会社との受委託関係がある場合もあり、こうなると、被害に遭ったのはどこの保有個人データなのかが不明確になりがちです。このような中で、片っ端から、これは委託なのか、共同利用なのか、それは誰の保有個人データなのか、定義していく作業は非常に大変です。ぜひ、事前にデータの流れを把握して、その流れが個人情報保護法上どのように位置付けられるのかを検討し、社内的に整理しておいてほしいです。

4つ目は、部門間連携です。緊急事態では部門間での利害対立が表面化しがちですが、法律上やらなければいけないことは決まっています。インシデントが起こったら、時間枠を押さえて定例会議を設け、関係者に情報共有することをクライアントに提案するのがいいと思います。

3 相談③： SaaSにデータを入れていいですか。

SaaSや生成AIサービスを使いたいという相談は定期的に来ます。SaaSを利用するとき、社外に個人データを提供するには、法的な根拠が必要になります。なお、前記相談②Ⅱで漏えい元基準をご説明しましたが、ここでも同じく提供元基準が採用されています。つまり、氏名自体をSaaSに入れないとしても、自社にとって個人データである情報をSaaSに入れようとするのであれば、提供には法的な根拠が必要だということです。

この提供の段階で選択し得る法的根拠は、図3のとおり、主として3つあります。

1つ目は、第三者提供です。これは、提供先にデータをあげてしまうことですので、適用されるプライバシーポリシーは提供先のものになります。また、原則として、本人から第三者提供についての同意取得が必要になりますし、提供元は、提供先、SaaSに対して特段監督義務を負うことはありません。第三者提供は、同意を漏れなく適法に取得できるかが鍵です。事前に同意を取得して、個人データを取得し、その上で第三者提供するようなケースであれば、同意の取得率は100%ですが、他方で、過去に取得済みのデータについて、後から同意を取りに行って第三者提供する場合には、どうしても同意の取得に漏れが出てきます。同意の取り方については、後記相談④で詳述します。

図3

1	■ 第三者提供 提供先にデータをあげてしまう（＝管理権限が提供先に移る） その後の適用プラポリは、提供先 同意取得が必要だが、提供元に監督義務は残らない	自社プラポリ	同意取得	監督義務
2	■ 委託 提供先にデータを預ける（＝管理権限は提供元に残る） その後の適用プラポリは、提供元 同意取得は不要だが、提供元に監督義務が残る	自社プラポリ	同意取得	監督義務
3	■ 「取り扱わないこととなっている場合」（クラウド例外） 提供先にデータを預ける（＝管理権限が提供元に残る） その後の適用プラポリは、提供元 同意取得等は不要だが、提供元に監督義務は残らない	自社プラポリ	同意取得	監督義務

2つ目は、委託です。これは、提供先にデータを預けるだけなので、適用されるプライバシーポリシーは自社のままです。第三者提供の同意取得は不要ですが、預けた者の責任として、監督義務が自社側に残ります。個人データの取扱いの委託は、個人情報保護法の独自の概念なので、SaaS利用契約など、民法上の業務委託契約以外にも該当し得ます。

3つ目は、事業者が個人データを取り扱わないこととなっている場合です。クラウド例外と呼ばれることもあります。委託は、具体的な作業、業務の存在が前提にありますが、その一部にAWSとかGCPといったクラウドインフラにデータをストレージだけしたいという場合がありますよね。そのような連携においては、提供元はクラウドサービス側に監督義務を負いません。FAQのA7-53[※3]を見ると、提供先が個人データを取り扱わないときは「提供」に該当しない、つまりクラウド例外に該当するとされています。もっとも、クラウド例外の場合には、自ら果たすべき安全管理措置の一環として適切な安全管理措置を講じる必要があるとされているので、クラウド例外は自社環境の拡張であると理解するのもよいかもしれません。

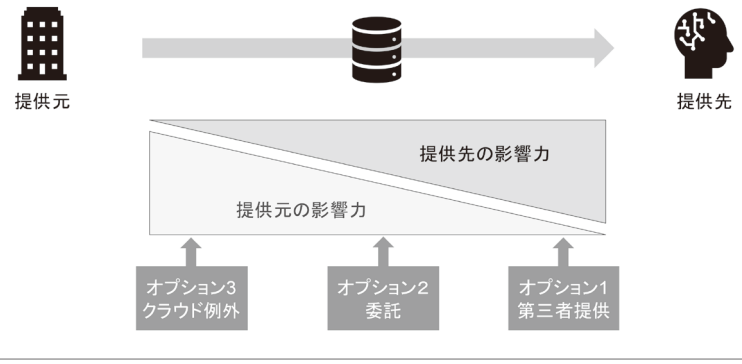
もう少し別の見方をしてみましょう。この3つのオプションは、図4のとおり、データに対する提供元、提供先それぞれの影響力の度合いが異なります。一番提供元の影響力が強いのはクラウド例外です。なぜなら、提供先はデータを取り扱わないからです。続いて委託。これは、預けるけれども、提供先は提供元の監督に服しますので、この3つの中では中間地点というイメージです。そして、一番提供先の影響力が強いのが第三者提供です。現状、SaaSの利用がこれらのどれに分類されるかについては、混迷を極めているところではありますが、クラウド例外はあくまで例外ですので、基本的には、SaaS利用は委託であると整理することをお勧めします。

4 相談④：今のプライバシーポリシーで、協力会社に個人データを提供できますか。

前記相談③で、個人データを提供するには法的な根拠が必要であることと、選択し得る法的根拠は主として3つあることをご説明しましたが、ここで、第三者提供で整理する必要がある典型ケースを2つご紹介します。

1つ目が、提供先で独自利用が想定されて、委

図4



※3 https://www.ppc.go.jp/personalinfo/faq/APPI_QA/#q7-53

託で整理ができないケースです。委託先はあくまで委託された業務の範囲内でデータを取り扱うものなので、もしそこから離れた委託先の独自利用が想定される場合には、委託では整理ができません。2つ目は、提供先での突合が予想されて、委託と整理できないケースです。これは、「混ぜるな危険」と呼ばれるもので、後記相談⑤で詳述します。

以下では、これらのケースで必要となる適法な第三者提供の同意取得の方法について説明します。

●同意取得の場所

1つ目は、プライバシーポリシーの中で同意を取得する方法です。多くの企業がこの方法を採っています。

2つ目は、フォーム等の末尾で同意を取得する方法です。個別の案件で取得した情報を第三者に提供したい場合、情報の入力画面の一番下などに、同意の文言と一緒に送信ボタンを設けるケースがよく見られます。

●同意取得の方法

ガイドライン上は、同意取得に当たっては「必要と考えられる合理的かつ適切な内容」を示す必要があるとされていますが、基本的には、目的（何のために提供するのか。）、主体（誰に対して提供するのか。）、客体（何の情報を提供するのか。）の3つを示す必要があると考えています。

例えば、図5のプライバシーポリシーでは、「以下の場合を除き、第三者に提供いたしません」として、第三者提供する場合の具体的な場面を挙げており、「広告を配信するために」という目的と、「ハッシュ化したメールアドレス等を」という客体と、「広告配信事業者に」という主体を明示しています。

他方で、利用目的の記載のみで同意と評価できないかという相談を受けることがあります。例えば、利用目的のところに、「広告、宣伝、マーケティングのために個人情報を利用します。」と書かれていることをもって、これは単なる利用目的の明示ではなくて、広告、宣伝、マーケティングのための第三者提供同意としても判断できないかという相談です。これは、同意の対象を確定できないので、第三者提供同意として判断することはできません。もしこれを許してしまうと、同じように列挙されているあらゆる利用目的について第三者提供同意が取れていることになってしまい、妥当ではないからです。

5 相談⑤：広告配信にメールアドレスを使っていいですか。

ここで広告配信と言っているのは、主として広告領域におけるカスタマーマッチの話を想定しています。この手の相談は、実際に多いにもかかわ

図5

（5）個人情報の第三者提供

当社は、以下の場合を除き、お客様の個人情報を第三者に提供いたしません。

・お客様の同意を得た場合
・利用目的の達成に必要な範囲内において、個人情報の取扱いを第三者に委託する場合
・当社お客様相談室へのお申し出に対応するために必要な範囲で、お申出者様の個人情報を、当社サプライヤーに提供する場合
・本条(6)に記載の者と共同して利用する場合
・お客様の趣味嗜好に応じた商品・サービスに関する広告を配信するために、ハッシュ化したメールアドレス等を、広告配信事業者（Google LLC、Meta Platforms, Inc.、X Corp.など）に提供する場合
・法令に基づき、警察などの公的な機関から、適法に個人情報の提供を求められた場合
・その他個人情報保護法などの法令で認められる場合

※出所：https://www.coca-cola.com/jp/ja/legal/privacy-policy

らず誤解が多い領域なので、掘り下げて説明します。

Ⅰ カスタマーマッチの仕組み

図6-1 図6-2 図6-3 図6-4 をご覧ください。

自社が世の中の潜在顧客に対して、広告を配信したいと考えたとします。このとき、自社は、まず自己が持っているユーザー（既存顧客）のデータの一部（図6-1でいう▨の部分です。）をハッシュ化して別データにします（図6-1でいう■の部分です。）。そして、ハッシュ化した個人データを他社（プラットフォーマー）に提供します図6-2。他社（プラットフォーマー）は、受け取ったデータを自社が保有している個人情報データベース等にぶつけます。そうすると、他社（プラットフォーマー）の個人情報データベース等には存在するが、広告を配信したいと思っている自社の個人情報データベース等には存在しないユーザーというのが浮き上がります（図6-3でいう、テーブルで白色のままになっている部分です。）。ここをターゲットユーザーとして（図6-4でいう■の部分です。）、効率的に広告配信ができますよというのが、カスタマーマッチの一例です。

図6-1

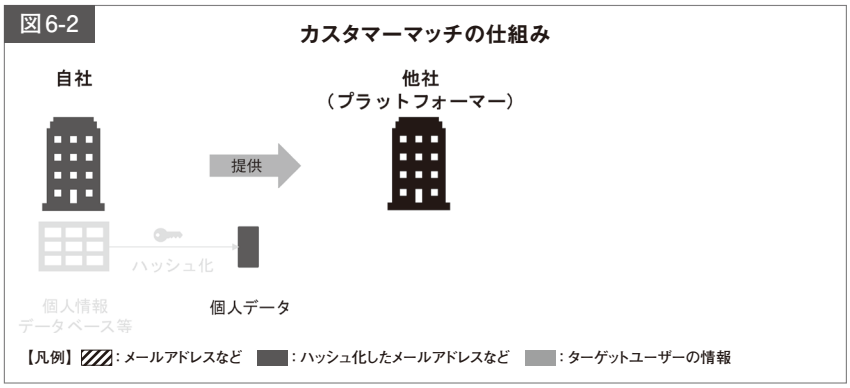

図6-2


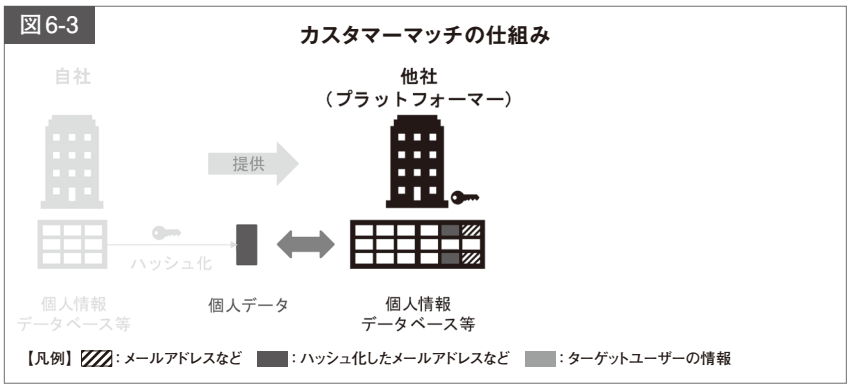
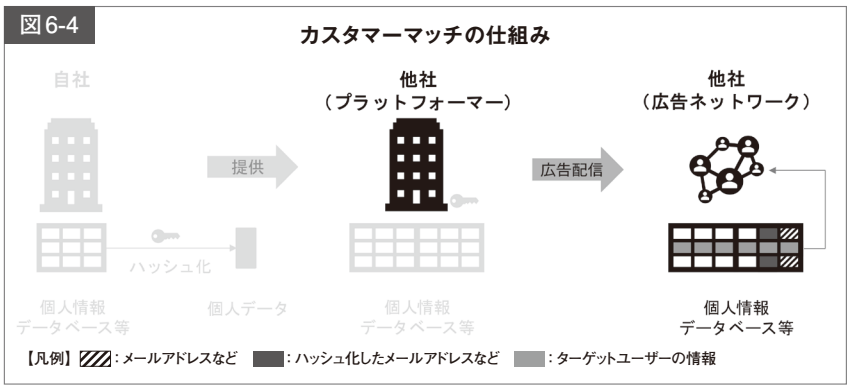
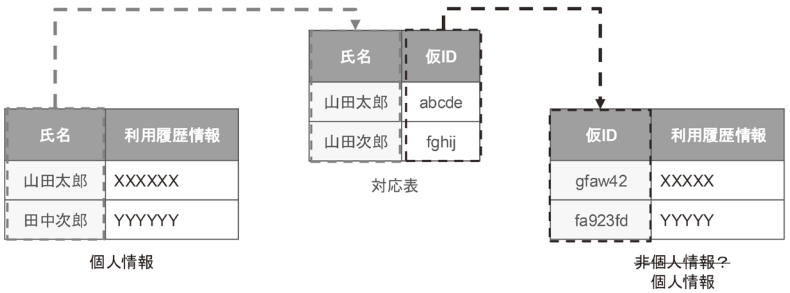
図6-3


図6-4


Ⅱ ハッシュ化の位置付け

ハッシュ化とは、入力された情報を別のランダムなデータに変換する関数・機構のことです。例えば、今日、「山田太郎」というデータをハッシュ化して得られた内容は、明日再度、「山田太郎」というデータをハッシュ化したとしても、同じものになります。

図7



入力したときに得られるデータは、今日も明日も同じなので、ハッシュ関数をそのまま残しているのであれば、それは対応表を残していることと実質的に変わらないからです。いつでも同じ結果が得られるということは、乱数等のパラメータがあれば対応表があるのと同じです。したがって、図7の一番右側のテーブルを非個人情報にしたいのであれば、ハッシュ関数等も破棄する必要があるということです。

続いて、ハッシュ化しても引き続き個人情報ですよという話を、FAQのQ15－14[※4]に沿ってご説明します。なお、このFAQでは、個人情報から匿名加工情報を作成する話をしているのですが、これは個人情報から匿名加工情報ではない単なる非個人情報を作るときにも同様に当てはまる議論です。

Q15－14前半は、氏名をハッシュ化するなどして仮IDに置き換えた場合に、これが非個人情報になるのか、また、非個人情報なら第三者提供の同意がなくても他社に送ってよいのか、そして、基になった個人情報と、個人情報と匿名加工情報の対応表と、匿名加工情報の3つがあったとして、個人情報と匿名加工情報の対応表を破棄する必要があるのか、という質問です。

A15－14は、個人情報と匿名加工情報の対応表は、破棄する必要があると回答しています。なぜなら、図7のとおり、3つのテーブルが社内にあった場合、一番左のテーブルから対応表を参照することができますし、さらに対応表から一番右のテーブルも容易に照合することができます。したがって、一番右のテーブルを非個人情報にしたいのであれば、対応表は削除する必要があるということです。

次に、Q15－14の後半は、対応表は破棄するとして、この対応表を作る基になったハッシュ関数等は残しておいてもいいですか、という質問です。

A15－14は、「再度同じ置き換えを行うことによって、本人を識別することができるので、破棄する必要があります」と回答しています。なぜなら、ハッシュ関数に「山田太郎」というデータを

Ⅲ 混ぜるな危険

図6-2に戻って説明しますが、カスタマーマッチの実施に際しては、最初に自社は、他社（プラットフォーマー）に対して個人データを提供することになります。この提供が、同意のいらない委託でいけますか、それとも同意が必要な第三者提供ですか、というのが「混ぜるな危険」のお話です。

FAQのQ 7－41[※5]では、「委託に伴って提供されたデータを、本人ごとに突合することはできますか。」という質問に対して、解決方法が2つ示されています。

解決方法の〈1〉は、通常の第三者提供です。委託では混ぜられませんよ、継ぎ足せませんよという話だったので、だったらもう自社で第三者提供の同意をユーザーから取得してしまって、他社に提供するということです。よくあるのは、図5で説明したように、「広告を配信するために」という目的と、「ハッシュ化したメールアドレス等を」という客体と、「広告配信事業者に」という主体を明示して、第三者提供の同意を取得するようなパターンです。

解決方法の〈2〉は、委託と整理した上で、提供先で本人の同意を取得するパターンです。A7-41では、委託先で取る同意が何の同意かについては明示的には書かれていませんが、業界的には、突合することについての同意をいうとするのがメジャーな解釈です。GoogleやMetaなどの大手プラットフォーマーは、たいてい自社のプラ

※4 https://www.ppc.go.jp/personalinfo/faq/APPI_QA/#q15-14　※5 https://www.ppc.go.jp/personalinfo/faq/APPI_QA/#q7-41

イバシーポリシーで、「情報を関連付けることがあります」みたいなことを記載しています。これが、FAQのA7−41でいう同意として有効であれば、どの会社も第三者提供同意なしにプラットフォーマーにデータを送信できるわけです。

ここで考えていただきたいのは、我々は今までプラットフォーマーからプライバシーポリシーの再同意を取られたことがあったかということです。私はあまりそういう記憶がありません。また、解決方法〈2〉でいく場合、それはあくまで委託ということになりますが、プラットフォーマーは、委託の範囲以上にいろいろ使っているように思います。そうだとすると、プラットフォーマーのプライバシーポリシーの記載をもって、解決方法〈2〉で整理できるどうかは、各社のリスク判断になります。私は、解決方法〈2〉でいくとしても、事後的でいいから第三者提供同意を取っておいてほしいとお願いすることが多いです。

6 相談⑥：ユーザーから位置情報を取得してもいいですか。

Ⅰ 位置情報の具体例

●GPS

衛星との通信時間を利用して距離を計測し、携帯端末の緯度経度情報を取得することができます。

●Bluetooth

「Bluetooth」発信機からの電波を携帯端末が受信することで位置を把握できます。デパートの売場のように縦にエリアが重なっている場所、緯度経度的には一緒のものだったとしても、ある程度の位置情報がわかります。

●IPアドレス

ネットワーク情報に基づいて大まかな位置情報を推定することができます。

Ⅱ 位置情報の注意点

位置情報の個人情報該当性について、ガイドラインは、ある位置情報が単独では個人情報に該当しなくても、それが積み重なることで特定の個人を識別できる場合があり、その場合には個人情報に該当すると説明しています。特定個人識別性の要件を氏名到達性、つまり使命にたどり着けるかどうかで理解してしまう人が一定数いますが、ここは文字通り、特定の個人を識別できるかどうかから判断しなければなりません。

また、位置情報の取得については、まずOS側での同意が必要ですし、電気通信事業者は位置情報の取得に際して同意取得等が求められています。その他の場合でも、情報の機微性を考慮して基本的には同意を取ることが望ましいです。また、スマホアプリの場合は、GoogleやAppleなどのプラットフォーマーは自社の規約において、アプリが位置情報を取得するのであれば同意を取得するよう求めてくる場合もあります。同意の取得方法については、GDPRのガイドラインや電気通信事業法のガイドライン等を参照されるとよいと思います。

7 相談⑦：開示請求が来てしまったのですが…。

開示請求は、法律上に記載のある本人に認められた権利の1つです。開示請求についての悩ましい論点を4つ解説します。

Ⅰ 開示請求の対象

開示請求権の対象は、保有個人データです。本人から直接取得した個人データはもちろんのこと、自社でユーザーに対して付与したペルソナ情報や評価情報、第三者から取得してユーザーに追加した属性情報なども対象になります。

Ⅱ 全開示請求への対応

開示請求で一番悩ましいものが、全てのデータを開示してくださいという請求です。データの洗い出しや確認に多大な手間と時間がかかります。FAQのA9−7[※6]は、「個人情報取扱事業者に対し、本人が開示を請求する範囲を限定させる権利を認めるものではありません」と書いていますので、最終的には全て対応せざるを得ませんが、実務上では、以下の方法で負担を軽減することが可能です。

- ユーザー自身がマイページ上で登録情報を確認できるようにしておいて、請求するまでもなくご自身で情報を確認できるようにしておく方法
- 開示に対する専用フォームを作成しておいて、開示が必要な範囲を事前にヒアリングしてしまう方法
- 本人の開示の目的等を踏まえて、事業者側から開示範囲を提案する方法
- すぐ開示できるデータ、開示までに時間がかかるデータの2段階に分けて対応する方法

Ⅲ 本人確認

事業者は、開示に際して本人確認を行うことができます。もっとも、実際には本人確認の途中で本人と連絡が取れなくなることが結構多いです。その後のトラブルを避けるため、1つ目に、本人確認の手続を進めるうえで、本人が対応する必要がある内容を明確に伝えること、2つ目に、本人から返答がなくなった後も、必要に応じて1回程度はリマインドを行うこと、最後に、対応の証跡を残しておくことが重要です。これは、「必要な手続きが完了していないため対応を中断している」ということを説得的に説明できるためです。

Ⅳ 手数料

個人情報保護法32条は、開示について、手数料の定めを置くことを認めています。開示請求の内容は様々で、純粋な権利行使のようなものもあれば、別の意図に基づいていて、事業者側が大きな負担を強いられることもあるため、手数料は定めておくのがお勧めです。

8 相談⑧：チェックシートはどう回答したらいいですか。

そもそも、チェックシートはなぜ使われているのでしょうか。個人情報保護法25条を見てみると、委託元には委託先を監督する義務があります。さらに、ガイドラインでは監督のために必要な措置が3つ挙げられており、その1つとして個人データの取扱い状況の把握という項目があります。この把握のためにチェックシートが使われているのです。

もし、チェックシートへの作業負担を軽減したいなら、事前に自社で回答済みの文書を用意するのがよいです。チェックシートを用意するのもよいですし、DPA（Data Processing Agreement）と呼ばれる文書形式にまとめてしまうのもよいと思います。そして、それでも利用企業独自の形式のチェックシートの対応を求められる場合には、オプション費用を取るケースもここ数年はいくつか出てきています。

ただ、ここはどうしても、案件を受注したい営業部門とチェックシートの対応に負担感を感じる法務部門との間での調整になるので、最終的には、会社として、チェックシートへの対応を求められることが多いかと思います。最近は、これらのセキュリティーチェックを効率化するSaaSも登場していますので、利用してみるのもよいかもしれません。

※6 https://www.ppc.go.jp/personalinfo/faq/APPI_QA/#q9-7