JIPDEC・日本商工会議所共催「中小企業向け改正個人情報保護法実務対応セミナー」講演要旨

2016 年 12 月 9 日開催

「改正個人情報保護法への実務対応」

弁護士法人第一法律事務所　弁護士　福本　洋一氏

■はじめに

2015 年春、マイナンバー法対応についてお話した時よりも今回の個人情報保護法改正に対する関心が薄いように思うが、マイナンバー（番号）法が特殊な情報を取扱う際の規定であるのに対して、個人情報保護法は広く情報全般に関わる話であり、今回の法改正で「過去 6 ヵ月以内に 5,000 件超の個人情報を取扱う事業者に適用される」という除外がなくなり中小事業者も適用対象となってくるため、インパクトはむしろこちらの方が大きい。

中小企業にとって重要なのは 2016 年 11 月に個人情報保護委員会から 4 分冊で出された「個人情報の保護に関する法律についてのガイドライン」である。

従前は経済産業分野のガイドラインがスタンダードなものとして扱われていたが、今回はそれを取り込むような形で「通則編」が作られ、特殊な事業を行う事業者を除き中小事業者においてはこの通則編が対応事項のポイントになってくる。

その他のガイドラインは 1.外国にある第三者への提供編（外国に対してデータを提供する場合のルールについて）、2.匿名加工情報編（ビッグデータへの対応）、3.第三者提供時の確認・記録義務編（第三者提供をする時に記録をとって保存すること等）である。

■個人情報保護法の改正の概要

1.改正の沿革

2005 年 4 月の全面施行から 10 年以上が経過し、この間の情報技術の進展により古いルールになじまないビジネスや取り扱いの問題が生じた。これらに対応するため 2015 年 9 月に改正・公布され、来年春の全面施行を予定している。

2.改正の背景

今回の改正は、「大手交通系企業の IC カードの乗降データ提供事案」、「大手教育出版系企業の個人情報大量流出事案」への対応を主な目的としている。

「大手交通系企業の IC カードの乗降データ提供事案」は、ビッグデータ事業を行っている大手交通系企業が IC データの乗降データを第三者に提供したところ、「オプトアウトしていない」等の事由から騒がれ提供行為を中止せざるを得なくなったものである。

事業者は、IC カードに紐づく ID を仮 ID に置き換え、個人を特定できない形で提供したことから個人情報保護法の適用外であると考えたが、たとえば 1 日 1 本しか運行しない電車に 1 名の乗客しかいなければその乗降データで個人が特定できてしまう。つまり、現行法では「個人情報とは何か」が不明瞭であり、今回の改正ではビッグデータ事業との関係において個人情報の定義の明確化も重要な課題であった。また、曖昧な形で提供すると個人データの提供に該当するとの疑念を抱かれるので、対外的に疑念を抱かれない形で提供するためのスキームを考えるために今回「匿名加工情報」という概念を作成した。

また、「大手教育出版系企業の個人情報大量流出事案」によって、これまではいわゆる名簿屋事業を行うにあたり不要であった登録が、今回の改正で必要となり、また、データを持ち出して売却するような利得行為は犯罪とし

て取り締まられることとなった。

3．主な改正項目

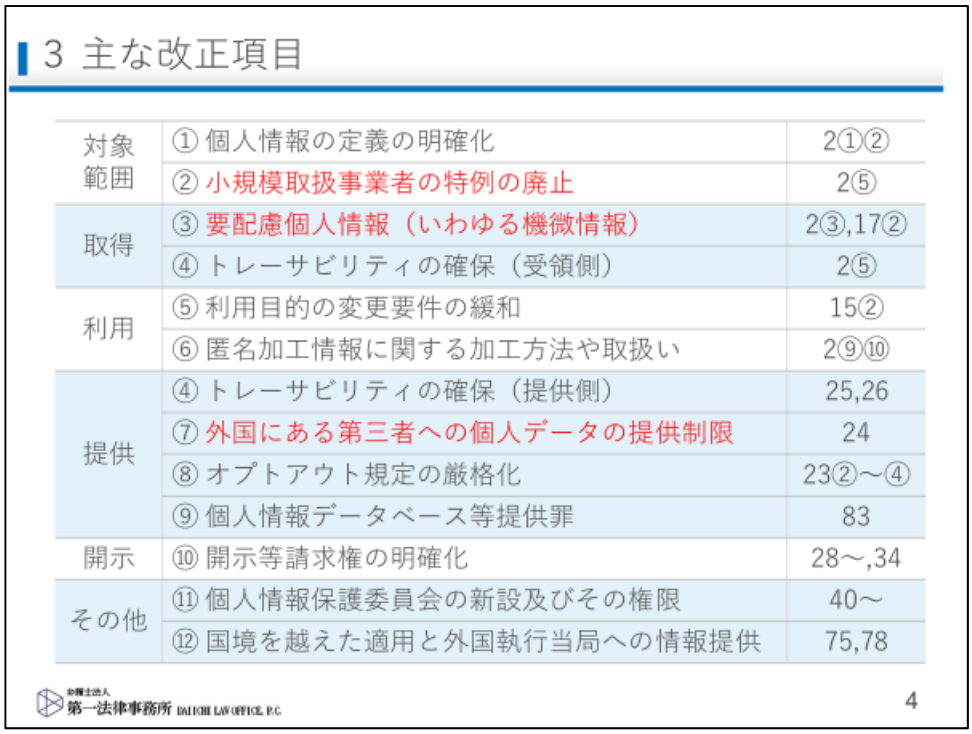

図 1.改正個人情報保護法　主な改正項目

先述の「大手交通系企業の IC カードの乗降データ提供事案」、「大手教育出版系企業の個人情報大量流出事案」によって新たに導入された制度は、名簿屋や名簿を購入して事業を行う事業者には影響するが、一般的な事業を行っている中小企業は、②小規模取扱事業者の特例の廃止、③要配慮個人情報（いわゆる機微情報）、⑦外国にある第三者への個人データの提供制限、という 3 つのポイントだけおさえておけば、それ以外は基本的に今まで通りと考えて良い。

①　個人情報の定義の明確化

今回、個人情報の定義に「個人識別符号」が加わったが、政府の見解によると個人情報の範囲が広がったのではなく、曖昧であった定義を明確化した、ということである。

個人識別符号とは、その人を特定するための ID というイメージを持っていただくと分かり易いと思う。つまり、氏名があることが個人情報の必須要件ではない。たとえばオンラインサービスで氏名を登録しなくても ID で登録・利用している場合には、当該 ID も特定の個人を識別することができる情報となりうる。

また、顔認証技術により、撮影された映像から抽出された顔認証データで管理されれば、氏名がわからなくても、特定の個人を識別することができる情報に該当する。改正前から、ガイドラインにおいて防犯カメラの映像も、顔が判別できるような解像度が高いものは、氏名が分からなくても個人情報とされている。

先述の「大手交通系企業の IC カードの乗降データ提供事案」でも ID の概念がどこまでであれば個人情報として保護すべきかを明確にすべきという議論がなされていたが、この点については法律ではなく下位の政令に委任し、その中で個別列挙して明確化することとなった。その結果、顔認識データ、指紋認識データ等のいわゆる生体認証データと、パスポート番号、免許証番号、基礎年金番号、健康保険証番号、マイナンバー等の公的な番号は、その人に 1 つしか適用されない番号なのでこれも個人情報というように明確化された。

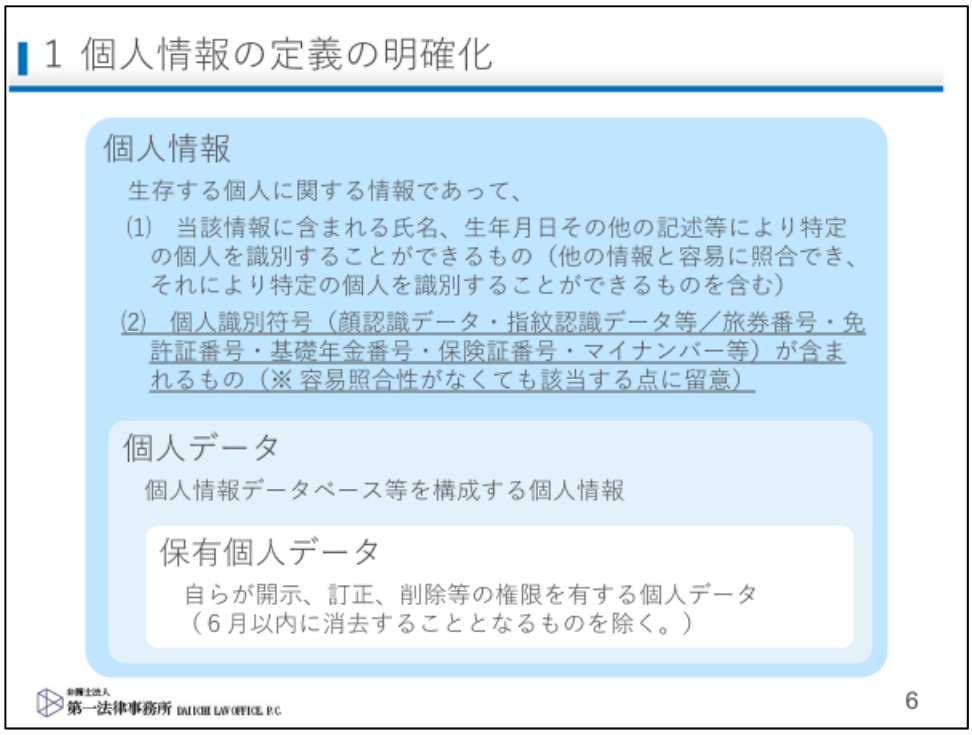

図 2.個人情報の定義の明確化

② 小規模取扱事業者の特例の廃止

これまでは過去 6 か月以内に 5,000 人を超えない個人情報しか持たない事業者は個人情報取扱事業者としての義務を負わなかったが、今回この規定が廃止され、扱う個人情報の規模に関わらず適用される。したがって、今まで個人情報取扱事業者ではなかった中小事業者は情報管理体制とともに安全管理に対する意識を持って頂きたい、というのが今回の改正で一番重要な点である。

■取得・利用段階における対応事項

1．取得・利用段階における法規制

今回新しく、適正な取得（第 17 条）の中に要配慮個人情報の取得制限が加わり、トレーサビリティの確保のため、受け取る際にも確認義務が課される。

2．利用目的の変更に対する制限の緩和

利用目的を変更する際には、「相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない」とされていた今までの規定から、「相当の」という文言が削除された。これまで変更できないと抑制的に思われていたものが本来許される範囲まで拡大するという委縮効果の軽減が目的である。

現行法を基にした経済産業分野のガイドラインでは「社会通念上本人が想定することが困難でないと認められる範囲内で変更は可能」という解説がされているのに対して、個人情報保護委員会のガイドラインでは「社会通念上、本人が通常予期し得る限度と客観的に認められる範囲内」に変わった。関連性の判断基準が本人ではなく一般人を基準とすることが明確化されたといえる。

3．要配慮個人情報

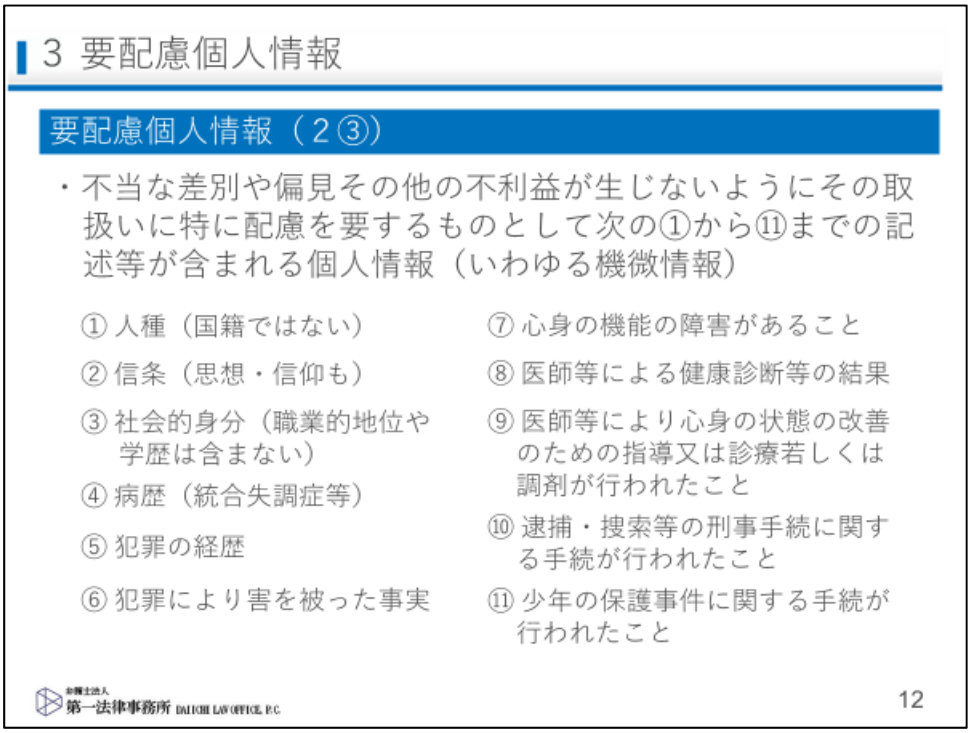

図 3.要配慮個人情報

要配慮個人情報には取得に際して本人の同意をとらなければならない、といった制約がかけられている。

一般的な企業は、⑧「医師等による健康診断等の結果」を取得することが想定されるが、労働安全衛生法上、事業者は労働者に健康診断を受けさせる義務があり、結果を取得することもあり得る。しかし、この取得は「法令に基づく場合」に該当するため、例外として本人からの同意取得は不要である。

また、要配慮個人情報を含んでいる際にはオプトアウト手続きによる第三者提供はできない（第 23 条第 2 項）。ただし、本人が SNS などで自ら公表している場合等は同意なく取得して良いという取得制限の例外も規定されている（第 17 条第 2 項）

4．トレーサビリティの確保

トレーサビリティの確保に関する規定は、あくまで名簿屋対策として入っていることに注意が必要である。①オプトアウトによる場合、②第三者提供について本人同意を得て提供される場合、③事業者でなく個人から提供される場合は確認記録が必要だが、④委託・事業承継・共同利用に基づいて提供される場合、⑤法令に基づいて第三者に提供される場合等は確認・記録が不要である。

したがって、名簿を買ってきて事業を行う事業者は別として、普通の事業者においては、本人以外から個人データを「もらう」ということがあまりないと思われるので、確認記録をしなければならない場合は限定的だと思われる。

第三者提供を受ける側の義務（第 26 条）にある「取得の経緯（直近まで）」というのは誰からもらってきたか、本人から直接もらったか、有償で買ってきたか、公開情報を集めて来たか等を確認しなければならないことを指している。

■安全管理措置における対応事項

1．安全管理措置における対応事項

今回の改正で安全管理措置について大きな変更はないが、①データ内容の正確性の確保等（第 19 条）に不要な情報は消すように、という「遅滞なく消去する努力義務」が新しく盛り込まれた。

これまでは目的外利用等の理由により本人から消去の申し立てを受けるのみだったが、裁判所から消去を命じる

ことが実現できる権利として今回の改正法で明確に定められた。努力義務ではあるものの、訴訟リスクの低減の観点からは、そもそも不要な情報は持たない方がよく、情報の安全管理の観点からも望ましい。

安全管理について大きな変更はないものの、今まで適用対象外であった中小企業が個人情報の取扱いを新たに考えなくてはならなくなった。ガイドラインの中では中小事業者向けの管理方法の例示もなされている。

安全管理について考える際には、まず、その情報の漏えいにより本人が被る侵害の程度を考えて欲しい。冒頭の「大手教育出版系企業の個人情報大量流出事案」では子供の情報も含まれ、漏洩により本人が被る利益侵害の程度は重い。自社が保有する個人情報のうち、何が本人への影響度合いが高いものかをまず考え、加えて事業の規模、性質、情報の性質、量、記録媒体、保管先等に鑑み情報漏えいのリスクを評価し、情報をどう守るか考える必要がある。

従業員数が 1、2 人くらいの中小企業であれば社内規定、個人情報管理規定といった文書の整備でなく、口頭ベースでも良いというように軽減されているが、安全管理のためにやるべきことを明確にして社内全体で理解することが大切であるという点では大企業と同じである。

2．情報漏えいの原因

冒頭の「大手教育出版系企業の個人情報大量流出事案」で行政からなされた是正勧告の中で「自社の業務の全過程において自社が保有する個人情報の利用・管理に責任を持つ部門の設置を怠っていた」ことが問題点として指摘された。

保護法では、委託先に対しては、委託元が自身と一体として監督することが求められているため、委託による場合は第三者提供の際の本人同意が必要ない。つまり、委託先は第三者ではない、ということである。したがって、委託先で漏洩が起きた際に、自社内に管理する仕組みがないことが問題であり、たとえばベンダーに一任して、そこでどういう管理がされているのかを把握していないような場合は問題である。

■提供段階における対応事項

1．提供段階における対応事項

今回の改正の対象は「提供」段階に集中している。

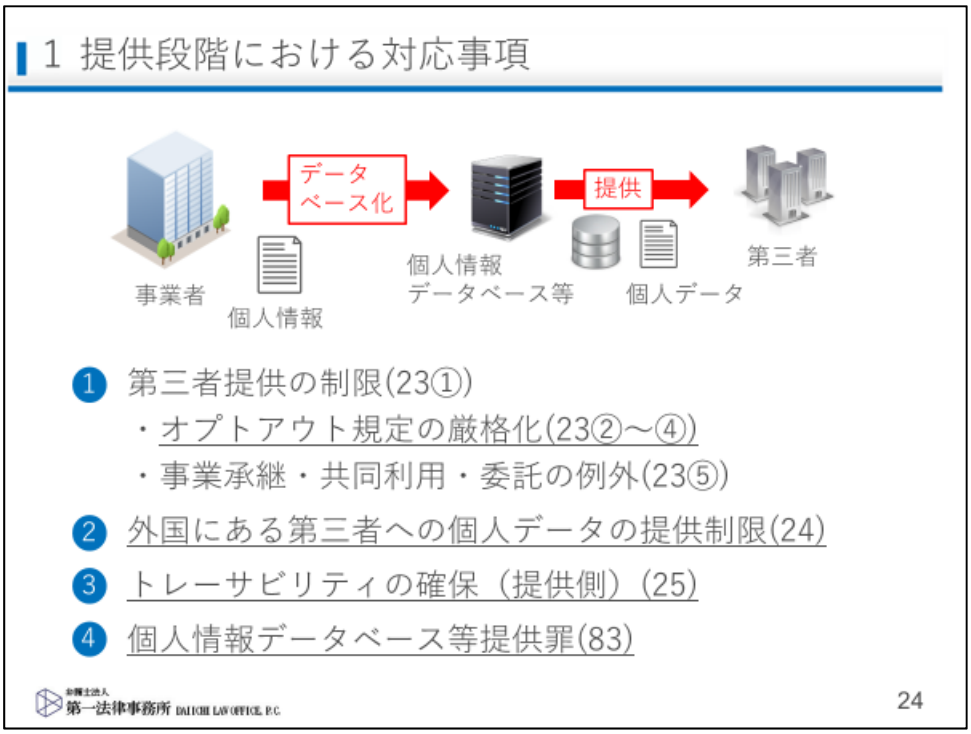

図 4.提供段階における対応事項

2．オプトアウト規定の厳格化

名簿として売却する際に個人情報保護委員会に適切に届け出をすること（第 23 条第 2 項）、個人情報保護委員会は届け出された内容を公表する（第 23 条第 4 項）ことによって不正利用を防ぐことが今回の規定の厳格化の背景にあるが、オプトアウト規定を用いて第三者に個人データを提供する事業者は限定的であると思われ、影響を受ける事業者は少ないと思われる。

3．外国にある第三者への個人データの提供制限

日本国内の個人データを海外の第三者に提供する際には移転規制がかかり、本人の同意がない限りは提供してはいけない。

第三者提供の制限には、①委託、②事業譲渡、③共同利用という 3 つの例外があり、大抵の事業者が個人データを外に提供する場合はいずれかに該当することが多く、同意の取得が問題とはならない。しかし、外国の事業者に対する提供に関してはこうした例外はない。よって、委託で外国に渡す場合や、共同利用で外国にある子会社に個人データを渡す場合でも本人の同意が必要となる。これは今回の改正の重要な点である。

しかしここで注意が必要なのは、提供先の事業者が海外で設立された事業者であることが基準である。国内の事業者がサーバーを海外に置いている場合は国内における提供に該当するので「外国にある第三者への提供」にはあたらない。

つまり、アメリカにあるデータセンターのストレージを使って自社の情報をクラウドで管理する場合、日本法人と契約して提供する場合は「外国にある第三者への提供」にはあたらないが、アメリカの法人と契約して提供する場合は「外国にある第三者への提供」にあたるので注意して欲しい。但し、外国の事業者でも日本国内にサーバーを置いていて日本国内でしかデータのやりとりがないのであれば外国にある第三者への個人データの提供にはあたらない。

したがって、拠点がどこにあるのかという議論は外国の事業者と取引する際には考えなくてはいけないが、国内事業者と取引する際にはどこにサーバーがあるかいちいちチェックする必要はない。

また、我が国と同等の水準にあると認められる外国にある第三者には、本人の同意がなくても提供して良い。EU のデータ保護指令にある「十分性がある国には提供して良い」という規定と同じ発想である。しかし、現時点で日本が「十分性がある、同等の水準にある」と認定している国はないため、この例外規定は今のところ使えない。

③「提供の当事者間で、提供先における個人データの取扱いについて、契約や内規等により、法の規定の趣旨に沿った措置の実施が確保されている第三者」とは、契約や内規により日本の保護法の規定を外国でも守ることを事業者間、あるいはグループ内で規程として取り決め、順守している場合には外国にある第三者へ提供して良い、ということである。

また、日本では JIPDEC が認定機関であるが、APEC の越境プライバシールール（CBPR）の認証を得ている第三者にも本人の同意なく提供してよい。

海外の事業者が日本国内にいる個人に対し物品や役務を提供することで個人情報を取得する場合には、海外で取り扱う場合でも国外適用があることになっている。EU が策定した一般データ保護規則（GDPR）でもこれと同様の規定があり、EU 域外から EU 域内の個人情報をとってきた場合に EU の GDPR が適用されるのと同様の発想である。しかし、EU は違反行為に対する制裁金の上限が非常に高額であるのに対し、日本のペナルティは非常に弱く、指導・助言、是正勧告による対応が可能である。

4．トレーサビリティの確保

第三者提供をする際には、提供時に記録を残すこと、提供を受ける側も受け取り時に記録を残すこととされている（第 25 条）。

5．個人情報データベース等提供罪

冒頭話した名簿屋への売却事件から個人情報データベース等提供罪が新設されたが、罰則として 1 年以下の懲役、または 50 万円以下の罰金が科される。

■開示段階における対応事項

1．開示等請求権の明確化

現行法には開示等の請求の求めを受けた時に対応する義務があったが、当時それが裁判所で実現できる権利であるのか見解がわかれており、地方裁判所の裁判例では、「開示等の請求権は裁判所で実現できる権利ではない」という判断がなされた。しかし今回の改正によって裁判所で実現できる権利であることが明確に定められた。

■匿名加工情報への対応事項

1．匿名加工情報の位置づけ

たとえば、システムテストのために実データから氏名などをカットしたものなど、個人情報の中から個人を識別できる部分を削除したものを「匿名加工情報」と考えている人も多いと思う。それは誤解で、「匿名加工情報」というのは、目的外利用や、第三者提供等のために加工された情報を指す。したがって、システムテストのために、より安全な形でそのデータを利用するために不要な情報は仮名化して使おう、という場合は安全管理措置のために加工しただけのことで、「匿名加工情報」にはあたらない。ガイドライン中にも、個人情報の安全管理措置の一環として一部の情報を削除あるいは分割して保存管理する場合、統計情報を作るために個人情報を加工する場合は含まないと明記されている。

冒頭の「大手交通系企業の IC カードの乗降データ提供事案」では、IC カードの分析用データに ID 番号が付いている。これを第三者に提供する際に変換番号に置き換え、変換番号から ID に戻せないようになっている。したがって事業者は「非個人情報」と理解していたが、元のデータと照合すれば、分析用データのどの ID が元データのどの ID かを特定することが可能であり、それは容易照合、つまり分析用データも「個人情報」であり第三者提供の際にはオプトアウトが必要という議論がなされた。

今回の改正では、対応表がなく突合できないようなものは「匿名加工情報」とし、それらは同意がなくても提供、目的外利用可能とした。したがって、ガイドラインでは個別事象の判断にゆだねることになっているが、対応表があり元のデータに戻せるようなものは「容易照合である」ということで「個人情報」に該当すると判断される可能性が高い。

2．匿名加工情報に関する加工方法や取扱い

「匿名加工情報の適正な加工」（第 36 条第 1 項）とは、氏名など特定の個人を識別することができる記述、特異な記述（1 日 1 本しか走っていない電車に 1 人しか乗っていない場合の乗降履歴等）等を削除することである。

匿名加工情報は本人の同意なく目的外利用可能であるし、第三者提供に際しても同意を得なくてもよい。しかし一定の情報を公表する必要がある。また、匿名加工情報を作成した場合、個人を識別するために他の情報と照合してはならない。

■まとめ

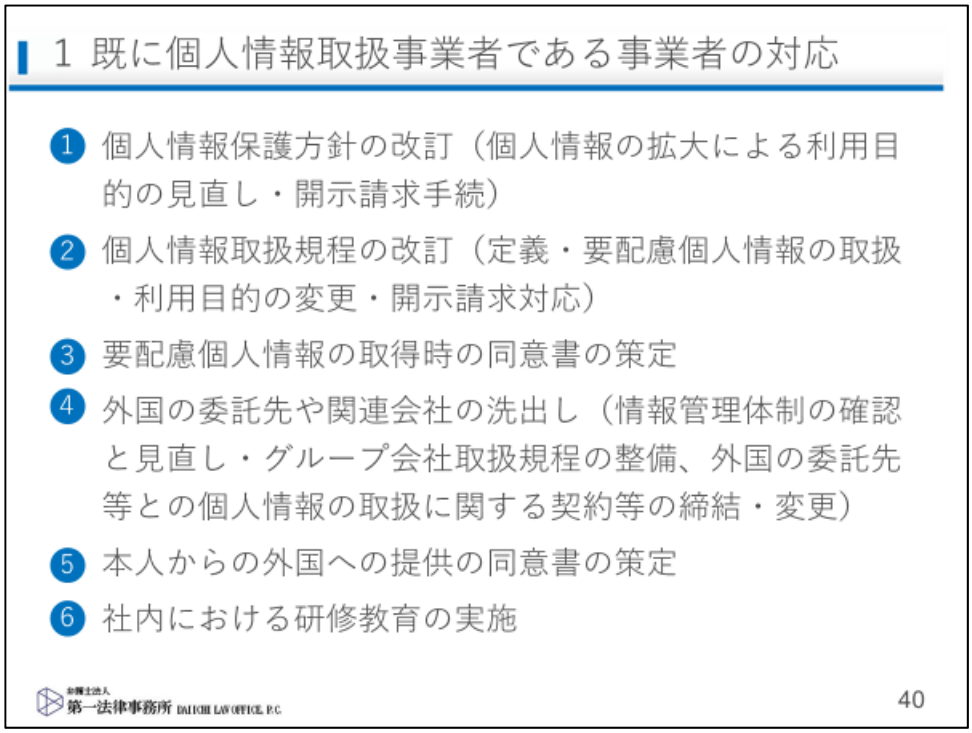

図 5.既個人情報取扱事業者の対応

1．既に個人情報取扱事業者である事業者の対応

今まで個人情報取扱事業者として対応してきた事業者は、今回の改正を受けてまず、①個人情報保護方針の改訂～⑥社内における研修教育の実施、を考えて頂きたい。

① 個人情報保護方針の改訂

今回、個人情報の概念が実質的に拡大した。

先述の通り、万引き防止のために、店内を撮影している映像から顔認証技術を用いて万引き歴のある者をリスト化して入店者と照合する場合、氏名などは取得していないが、個人識別符号であり、個人情報の利用にあたることが今回の改正で明確になった。これを自社の個人情報保護方針等で利用目的として挙げるか考えなければならない。万引き防止目的であれば、利用目的の公表の例外規定に「個人情報取扱事業者の権利・正当な利益を害するおそれがある場合は公表しなくて良い」とされているので個人情報保護方針に利用目的として追加しなくて良いケースもあるかもしれないが、マーケティング目的から顔認証データを用いて購買データと紐付けて利用する場合には新たに個人情報保護方針に利用目的を追加するか考えなければならない。

また、開示請求が裁判所で実現可能な権利となったため、適切に対応できる体制を作ることが必要である。

② 個人情報取扱規程の改訂

小規模事業者であれば「規程」の形式にこだわる必要はないかもしれないが、ルールは明確にしておく必要がある。定義・要配慮個人情報の取扱・利用目的の変更・開示請求対応については改訂しておく必要がある。

③ 要配慮個人情報の取得時の同意書の策定

主に従業員の健康診断結果等を労働安全衛生法のような法律上の根拠に基づかない形でもらうような場合には、要配慮個人情報を取得する場合に当たるので、同意書を取り、明確に義務履行したことを証拠として残しておくことが望ましい。

④ 外国の委託先や関連会社の洗出し

外国の法人格の事業者への個人情報の提供がないか洗い出しをし、該当すればそこの情報管理の体制（海外のデータセンターでの管理であるかを含む）を確認し、海外のグループ会社があれば、日本の個人情報保護法に準じた情報管理体制を構築して、グループ全体の取扱規程を整備する、といった対応が必要である。

現実的には、外国にある第三者に顧客の情報を提供する場合に本人同意を得ることは難しいと思われるので、実務では契約や規程の見直しで対応していくことになるのではないかと想定している。

⑤ 本人からの外国への提供の同意書の策定

他方、同意を得て提供する方がやり易ければ、同意書のフォーマットを作成して取得することも考えられる。

⑥ 社内における研修教育の実施

ルールを作ったという形式だけで満足せず、社員に周知することが重要である。

2．名簿業者・名簿購入事業者の対応

名簿業者・名簿購入事業者が行うべき特殊な対応として、オプトアウト・トレーサビリティへの対応が必要である。オプトアウトの公表事項として追加すべきものを追加し、オプトアウトする場合の要配慮個人情報の取得禁止、オプトアウトを使う際の予告期間の確保、個人情報保護委員会へのオプトアウトについての届け出、トレーサビリティの確保を必ず行い、社内にも周知しなければならない。

3．ビッグデータ事業者の対応

ビッグデータビジネスを行う事業者は、匿名加工情報として提供するのであれば個人情報保護方針等に明記し公表する必要があり、匿名加工情報の作成・管理・提供における取扱手順等・識別行為の禁止を内部のルールとして個人情報取扱規程に盛り込む必要がある。匿名加工情報の加工方法に関しては仮 ID に変換する際のルール、アルゴリズムなど、元データに戻せる情報が流出しないよう管理体制等を明確にする必要がある。匿名加工情報公表用に専用の公表サイトを作っておくと良いかもしれない。また、これらについても社内教育が必要である。