個人情報の保護に関する法律準拠の為の行動規範

CSAJC cloud security alliance SM Japan Chapter

CSA cloud security alliance®

日本版提供に際しての告知及び注意事項

本書「個人情報の保護に関する法律準拠の為の行動規範（CoC　JP）」は一般社団法人日本クラウドセキュリティアライアンス（CSAジャパン）が公開するものです。

以下の変更履歴（日付、バージョン、変更内容）をご確認ください

変更履歴

日付	バージョン	変更内容
2021 年 11 月 17 日	1.0	初版発行
2023 年 01 月 27 日	1.1	追補版発行

用語については特に定めのない限り個人情報保護法及び関連法令やガイドラインにおける各用語の定義と同一と致します。

CSAジャパンは、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1. 責任の限定

CSAジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1) 本書の内容の真正性、正確性、無誤謬性

(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと

(3) 本書の内容に基づいて行われた判断や行為がもたらす結果

(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2. 二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1) 本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。

(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。

(3) CSAジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。

(4) 転載、再掲、複製の作成と配布等について、CSAジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

3. 本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。

(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守さ

せるものとします。また、当該責任者は、本書の電子ファイルを適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。

(3) 本書をダウンロードした者は、CSAジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。

(4) 本書を印刷した者は、CSAジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

4. 原典がある場合の制限事項等

本書がCloud Security Alliance, Inc.の著作物等の翻訳である場合には、原典に明記された制限事項、免責事項は、英語その他の言語で表記されている場合も含め、すべてここに記載の制限事項に優先して適用されます。

5. その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSAジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、本書または本書の提供場所に記載の問合せ先までお願いします。

追補版作成に際しての謝辞

「個人情報の保護に関する法律準拠の為の行動規範（COC-JP）追補版」の作成は、CSAジャパンの「クラウドプライバシー・ワーキンググループ」に参加するメンバーを中心とした、CSAジャパン会員の有志により行われました。

作業は全て、個人の無償の貢献としての私的労力提供により行われました。なお、企業会員からの参加者の貢献には、会員企業としての貢献も与っていることを付記いたします。

以下に、執筆にされた方々の氏名および所属先（企業会員からの参加の場合のみ）を記します。（氏名あいうえお順・敬称略）

サルギシャン アレクサンドル：ファイルフォース株式会社

新貝 知晃：株式会社日立システムズ

竹内 智子：株式会社クレスコ・デジタルテクノロジーズ

谷本 茂明

津嶋 紀宏：株式会社日立システムズ

前川 浩司：BSIグループジャパン株式会社

松本　優子

山本 博崇

山崎 万丈

目次

I. 序論 5
II. 背景 6
実践規範 8
第1章　個人情報の適正取得（第17条、第18条、第20条、第21条、第30条） ***9***
第1節　個人情報取扱事業者が個人情報を適正に取得するには次のルールを守る必要がある 9
第2節　改正（令和2年）ポイント整理 14
第3節　法の条文（令和2年改正との対比表） 17
第2章　漏えい等報告・本人通知の義務化（第26条） ***19***
第1節　漏えい等事案が発覚した場合に講ずべき措置 19
第2節　報告・本人通知が必要となる場合 19
第3節　報告・本人通知を要しない場合 20
第4節　報告・本人通知義務の主体 20
第5節　個人情報保護委員会への報告 21
第6節　本人への通知 22
第3章　個人情報の提供（第27条、第28条、第29条、第30条） ***23***
第1節　外国にある第三者への提供 23
第4章　個人関連情報、および第三者提供の制限等について（第2条第7項、第16条第7項、第31条） ***28***
第1節　個人関連情報および個人関連情報取扱事業者（第2条第7項、第16条第7項） 28
第2節　個人関連情報の第三者提供の制限（第31条） 29
第5章　匿名加工情報関連（第2条、第16条、第43条、第44条、第45条、第46条） ***31***
第1節　匿名加工情報に係る規程内容の概要 31
第2節　匿名加工情報に係る具体的な行動規範とそのポイント 32
第3節　まとめ 36
第6章　仮名加工情報関連（第2条、第16条、第41条、第42条） ***37***
第1節　仮名加工情報に係る規定内容の概要 37
第2節　仮名加工情報に係る規定内容のポイント 38
第3節　まとめ 43
第7章　域外適用(第166条) ***45***
第8章　罰則（第19条、第173条、第177条、第179条） ***46***
第1節　不適正な利用の禁止(第19条) 46
第2節　措置命令・報告義務違反の罰則について法定刑を引き上げ（第173条、第177条） 47
第3節　法人に対する罰金刑を引き上げ(第179条) 48
第4節　罰則の改正まとめ 48

I. 序論

個人情報保護は、全世界的にはリスクベースの評価になってきている。個人情報の管理者は、彼らが処理する個人データの適切な保護レベルを組織内で決定し実施する責任を負う。その決定においては、最先端技術、実装費用、データ処理の性質、範囲、内容および目的を勘案し、また個人の権利及び自由に対する主張の可能性および深刻さが変動するリスクを考慮する必要がある。その結果、クラウド事業者（CSP）は、彼らが処理する個人データに求められる保護レベルを自ら決定する責任を負う。

またデータの有効活用とプライバシーの確保を巡って各国の個人情報保護法の制定が活発化しており、日本国の法制度も、各国との個人情報の越境移転を見越した、EUとの個人情報保護法（GDPR)との十分性認定をはじめとする、法制度のアップデートが求められており、2019年に「個人情報保護法 いわゆる3年ごと見直し制度改正大綱」が定められ、令和2年と令和3年に見直しが行われた。

2021年に各種ガイドライン（保護法とガイドラインを総称して個人情報保護法等と表記する)が個人情報保護委員会より出されており、CSAジャパンは、これらの法令の準拠のための「個人情報の保護に関する法律準拠の為の行動規範」を作成した。

2018年に発行された「CSA GDPR準拠の為の行動規範（CSA CoC（PLA[V3]))と同様に、CSPとクラウド利用者に個人情報保護法準拠のためのソリューションを提供し、CSPが提供するデータ保護レベルに関する透明性ガイドラインを提供することを目指している。

「個人情報の保護に関する法律準拠の為の行動規範（COC-JP）」は、実質的に以下を提供するものである:

あらゆる規模および所在場所のCSPにとっての、個人情報保護法に遵守し、
利用者に提供している個人データ保護レベルを、体系化された方法で明示するための例示と解説。

「個人情報の保護に関する法律準拠の為の行動規範（COC-JP）」及び「追補版」は、主に法的要件に重点を置いているため、Cloud Control Matrix（CCM）やSTAR認証（またはSTAR評価証明またはSTARセルフアセスメント）などの他のCSA作成の実践規範および認証と組み合わせてこの規範を採用することを提案し、情報セキュリティの必要な要件をCCM/ISMSなどとの対比を本文中に記載している。

このような状況において、Cloud Control Matrixまたはそれと同等のもの（例えば、ISO 27017またはISO 27018による補完を伴うISO 27001）といった情報セキュリティの技術標準の採用や、それらに関連する認証スキーム（例えば、STAR認証、STAR評価証明、STARセルフアセスメント、ISO 27001、またはSOC2）は、CSPがセキュリティプログラムまたは情報セキュリティ管理システム（ISMS）を実装し、これらのリスクアセスメントで概説された脅威から利用者のデータを適切に保護している証拠を提供する。

「個人情報の保護に関する法律準拠の為の行動規範（COC-JP）」は、個人情報保護法等のクラウド分野に関連する要件を反映し、CSA Security, Transparency and Assurance Registry（STAR）の一部を構成する。

「個人情報の保護に関する法律準拠の為の行動規範（COC-JP）」の対象読者には、CSP、クラウド利用者と潜在利用者、クラウド監査者、およびクラウドブローカーのように、クラウドコンピューティングおよび個人データ保護法制に関心のあるすべての利害関係者が含まれる。

最後に、「個人情報の保護に関する法律準拠の為の行動規範（COC-JP）」に対するいかなる認証も、管理者（Controller）または処理者（Processor）が個人情報保護法等を遵守する責任を軽減するものではなく、国の個人情報保護委員会の任務および権限を損なうものではないことに注意することが重要である。

II. 背景

欧州では2016年5月にREGULATION（EU）2016/679（“GDPR”）が発効し、2018年5月25日以降すべてのEU参加国において直接適用されることになった。更に、個人データの越境移転に必要なSCC（標準契約条項）の改訂が2021年7月に実施された。米国でもカリフォルニア州消費者プライバシー法（CCPA：the California Consumer Privacy Act）やカリフォルニアプライバシー権法（CPRA: the California Privacy Rights Act of 2020）に加え、連邦データプライバシー法案としてCOPRA（Consumer Online Privacy Rights Act）（消費者オンラインプライバシー法）という法案が審議されている。

このように消費者のプライバシーにかかわる法制化は世界的なトレンドであり、プライバシーという権利を法的に認める流れにある。

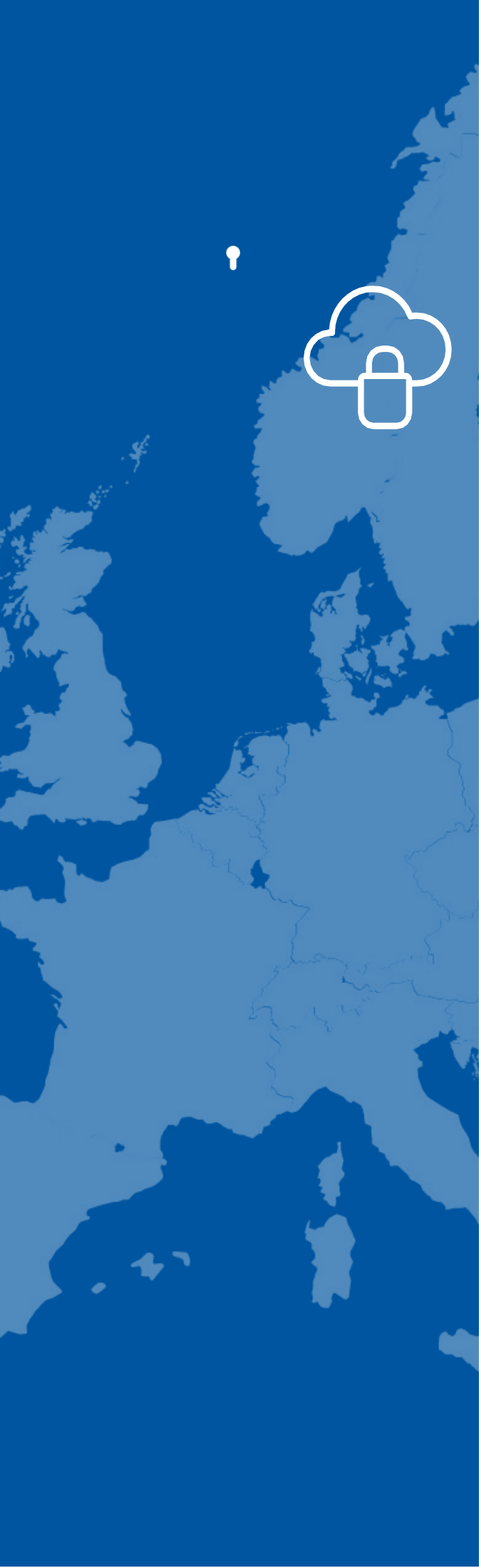
日本では個人情報全般に関する扱いを個人情報保護法等によって定めてきていたが、欧米に比べあいまいな部分も多く、企業活動の国際化やクラウドコンピューティングの進展に伴う国境をまたいだデータの移動・処理・保管が常態化した中で各国法制度との差を埋める（GDPRに求められる十分性認定）活動などが必要になってきている。

そのため、今回の追補版では「個人関連情報」や「仮名加工情報」といった新しい概念、第三国移転など改正された部分を中心に解説を行っている。

表0-1　定義の整理

<table>
<tr><td>個人情報
生存する特定の個人を識別できる情報
個人識別符号が含まれるもの</td></tr>
<tr><td>個人データ
個人情報を検索できるように体系的に構成したもの</td></tr>
<tr><td>保有個人データ
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のできる権限を有する個人データ</td></tr>
</table>

日本では個人情報保護法の制定により、個人情報は利用目的の特定・管理下にある情報の安全管理・削除訂正などの要請対応に関する事項が定められているが、経済活動活性化のためにより踏み込んだ議論が必要であるとCSAジャパンクラウドプライバシーワーキンググループは認識し本書を取りまとめた。



実践規範

第1章　個人情報の適正取得
（第17条、第18条、第20条、第21条、第30条）

社会活動を通して個人情報を入手する機会は少なくない。

不適切な方法で個人情報を入手すると、個人情報保護法違反、処罰の対象になる可能性がある。結果として社会的信用を失ったりするリスクがある。これまで対象が一定規模の事業者とされてきたが、情報利活用の推進に伴い、私たちの社会生活における個人情報の取り扱いのケースも該当する場合があるので注意が必要。

個人情報の取得時のルールについて、事例とともに解説する。

第1節　個人情報取扱事業者が個人情報を適正に取得するには次のルールを守る必要がある

① 取得する個人情報の**利用目的を特定**すること（第 17 条 1 項 2 項）
② 個人情報の取り扱いは特定した**利用目的に制限**される（第 18 条）
③ 特定した個人情報と**利用目的を公表**すること（第 21 条）
④ **不正な手段で入手しない**こと（第 20 条 1 項）
⑤ **本人の同意**を明らかにすること（第 20 条 2 項）
⑥ **取得時の確認・記録義務**（第 30 条 2 項）

個人情報の取得のたびに利用目的の通知・公表することを避けるため、企業・組織の多くは「個人情報保護方針」や「プライバシーポリシー」をWebサイトで公表している。

事例　Amazon.co.jp プライバシー規約[1]

Amazon.co.jpプライバシー規約

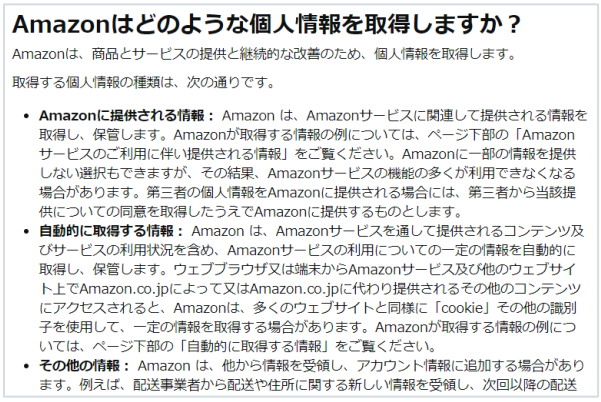
最終更新日: 2022/4/1

改定前のプライバシー規約はこちらをご参照ください。

Amazon.co.jp では、個人情報を細心の注意を払って慎重に取り扱い、利用および共有させていただいています。本プライバシー規約（以下「本規約」といいます。）は、本規約を参照するAmazonのウェブサイト、端末、製品、サービス、オンラインストア及び実店舗（以下「Amazonサービス」といいます。）を通じたAmazon（Amazon.com, Inc.を含め、Amazon.com Services LLC及びその国内外の関係会社をいいます。）による個人情報の取得及び取扱いに関する方針を説明するものです。**Amazonサービスをご利用いただいた場合、本規約に同意していただいたものとみなされます。**

目次

- 個人情報の管理者
- Amazonはどのような個人情報を取得しますか？



Amazonはどのような個人情報を取得しますか？

Amazonは、商品とサービスの提供と継続的な改善のため、個人情報を取得します。

取得する個人情報の種類は、次の通りです。

- **Amazonに提供される情報：** Amazon は、Amazonサービスに関連して提供される情報を取得し、保管します。Amazonが取得する情報の例については、ページ下部の「Amazonサービスのご利用に伴い提供される情報」をご覧ください。Amazonに一部の情報を提供しない選択もできますが、その結果、Amazonサービスの機能の多くが利用できなくなる場合があります。第三者の個人情報をAmazonに提供される場合には、第三者から当該提供についての同意を取得したうえでAmazonに提供するものとします。
- **自動的に取得する情報：** Amazon は、Amazonサービスを通して提供されるコンテンツ及びサービスの利用状況を含め、Amazonサービスの利用についての一定の情報を自動的に取得し、保管します。ウェブブラウザ又は端末からAmazonサービス及び他のウェブサイト上でAmazon.co.jpによって又はAmazon.co.jpに代わり提供されるその他のコンテンツにアクセスされると、Amazonは、多くのウェブサイトと同様に「cookie」その他の識別子を使用して、一定の情報を取得する場合があります。Amazonが取得する情報の例については、ページ下部の「自動的に取得する情報」をご覧ください。
- **その他の情報：** Amazon は、他から情報を受領し、アカウント情報に追加する場合があります。例えば、配送事業者から配送や住所に関する新しい情報を受領し、次回以降の配送

（おさらい1）　個人情報保護法における個人情報取扱事業者の定義変更も再確認する：

個人情報保護法の2017年（H29年施行）改正前は、小規模事業者を個人情報取扱事業者の例外と規定されていたが、改正によって小規模事業者に対する例外措置が撤廃され、事業者の規模を問わないようになっている。

2017年（H29年施行）改正前の個人情報保護法では、個人情報取扱事業者の例外として「個人情報によって識別される特定の個人の数の合計が過去6か月以内のいずれの日においても5000を超えない者」と小規模事業者を除外する規定があったが、法改正によって撤廃され、自治会や同窓会といった私たちの日常の生活により近い小規模の非営利組織も個人情報取扱事業者に該当するようになっているので注意が必要。[2]

[1] Amazon.co.jp プライバシー規約　最終更新日: 2022/4/1
https://www.amazon.co.jp/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ （2022/10/24 時点）
[2] マイナンバーセキュリティ全般「改正個人情報保護法」ポイント解説 2017 年（H29 年）改正 https://www.daj.jp/news/170322_01/

（おさらい2）「個人情報保護法二条」にて定義されている個人情報を再確認する：

「個人情報」は下記のように定義されており、2017年（H29年施行）改正にて「二」が追加されている。

◆個人情報の定義の一：特定の個人を識別することができるもの

- 生存する特定の個人が識別できれば、文字情報の「名刺」、画像の「顔写真」はそれぞれ個人情報
- 複合的な情報から特定の個人を識別できれば個人情報
- 他の情報と容易に照合ができ、それにより特定の個人を識別することができれば個人情報
- （念のため）居住地や国籍を問わず、日本にある個人情報取扱事業者及び行政機関等が取り扱う個人情報は、個人情報保護法による保護の対象となり得る。

◆個人情報の定義の二：個人識別符号が含まれるもの

個人識別符号は 2 種類に大別され、個人情報保護委員会政令に以下のように示されている。[3]

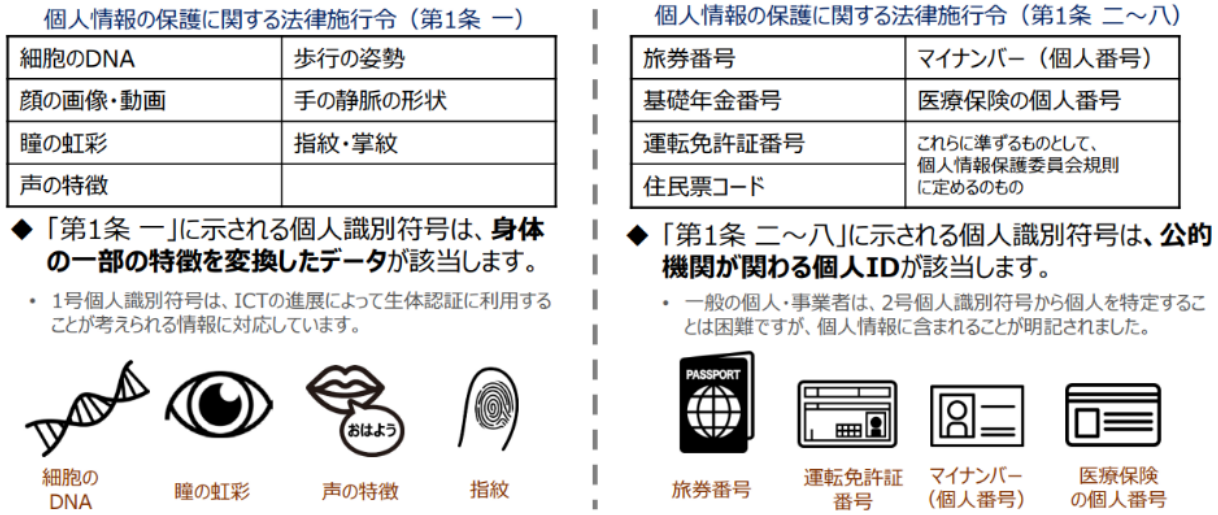


図 1−1

（おさらい3） 個人情報は広義であるため規制対象が異なることを確認する：

個人情報／個人データ／保有個人データの違いと規制[4]

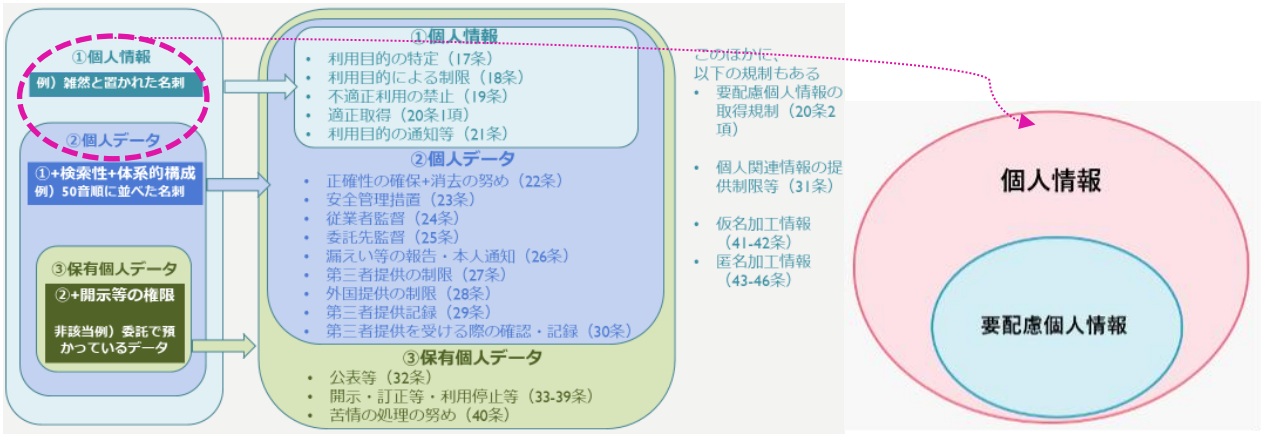


図1−2

[3] 総務省 ICT スキル総合習得教材「個人情報の保護と匿名データの利活」https://www.soumu.go.jp/ict_skill/pdf/ict_skill_2_4.pdf
[4] IT をめぐる法律問題「弁護士水町雅子の IT 情報法ブログ」https://cyberlawissues.hatenablog.com/entry/2022/05/26/170605

（おさらい4） 個人情報保護の関連法体系、および、制度改正背景と課題を確認する:

個人情報保護法でイメージしにくい関連法体系と改正時期については個人情報保護委員会より令和3(2021)年に共有されている以下資料がある。[5]

図 1-3

図 1-4

[5] 個人情報保護法令和 2 年改正及び令和 3 年改正案について
https://www.meti.go.jp/shingikai/sankoshin/shomu_ryutsu/bio/kojin_iden/life_science/pdf/001_03_02.pdf

表1-1 「個人情報の適正取得」に関する法条文（抜粋）とガイドライン[6]

改正（令和2年）後の法条文	ガイドライン
（利用目的の特定） 第 17 条（第 1 項） 個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。	・個人情報が個人情報取扱事業者において、どのような事業の用に供され、どのような目的で個人情報を利用されるのか本人にとって一般的かつ合理的に想定できるよう**具体的に特定**すること。 ・個人情報を**第三者に提供することを想定している場合**は、利用目的の特定に当たり、その旨が**明確に分かるよう特定**しなければならない。
（利用目的の変更） 第 17 条（第 2 項） 個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と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。	（利用目的の特定）により特定した利用目的は、**変更前の利用目的と関連性を有すると合理的に認められる範囲**、すなわち、変更後の利用目的が変更前の利用目的からみて、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（当初の利用目的と変更後の利用目的を比較して予期できる範囲）で変更することは可能である。
（利用目的による制限） 第 18 条（第 1 項） 個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。	・個人情報取扱事業者は、第 17 条第 1 項により特定した**利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合は、あらかじめ本人の同意を得なければならない**。 当該同意を得るために個人情報を利用すること（メールの送信や電話をかけること等）は、当初特定した利用目的として記載されていない場合でも、目的外利用には該当しない。 ・**「取得」の際の同意の要否ポイントを再確認**すると、実務上は、個人情報を取得する際には本人同意が必要であるとの誤解も少なくないが、個人情報保護法は、**利用目的の範囲内であれば**、取得の際の本人同意を必要とせず、利用目的の通知または公表を求めるに留まる。（個人情報保護法第 18 条 1 項 2 項）
（公表） 第 21 条（第 1 項） 個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。	「公表」とは、広く一般に意思を知らせること（不特定**多数の人が知りえるよう発表**すること）をいい、公表に当たっては、事業の性質及び個人情報の取扱状況に応じ、**合理的かつ適切な方法**によらなければならない。 例えば ホームページ・ポスター・パンフレット
（適正な取得） 第 20 条（第 1 項） 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してはならない。	・新ガイドラインより「**不正手段**」とされる方法 ✓ 窃盗、脅迫 ✓ 十分な判断能力のない子供等からの取得 ✓ 第三者提供制限違反に加担して個人情報の提供を受ける ✓ 不正な手段により取得させた個人情報の提供を受ける ✓ 提供者が不正な手段で取得した個人情報と知りながら提供を受ける ・個人情報を不正に取得した場合は、本人は個人データの利用の停止や消去を請求することができ、個人情報取扱事業者は原則として応じる義務がある。
（本人の同意） 第 20 条（第 2 項） 個人情報取扱事業者は、次に掲げる場合を除くほか、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。 (1) 法令に基づく場合 (2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。 (3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。 (4) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。 (5) 当該個人情報取扱事業者が学術研究機関等である場合であって、当該要配慮個人情報を学術研究目的で取り扱う必要があるとき（当該要配慮個人情報を取り扱う目的の一部が学術研究目的	・個人情報については、偽りその他不正の手段によって取得する場合を除き、取得そのものは本人の同意は必要とされていない（個人情報保護法第 20 条 1 項）。これに対し、要配慮個人情報の取得は、原則（1）～（8）を除き本人の事前同意が必要となる。 ・通常の個人データには、オプトアウト方式による第三者提供が認められているが、これに対して、**要配慮個人情報に該当する個人データは、オプトアウト方式による第三者提供が認められない**。要配慮個人情報に該当する個人データを第三者提供する場合、事前に本人の明示的な同意を得ることが必須となる。 参考：「オプトアウト方式」とは、本人の明示的な同意がなくとも、提供停止の求めを受けるまでは個人データの第三者提供を行う方式を意味する（個人情報保護法第 27 条 2 項本文） ・行政機関が個人情報ファイルを保有しようとする場合、個人情報保護委員会に当該個人情報ファイルに関する一定の事項を通知しなければならない（個人情報保護法第 74 条 1 項）。 その際、個人情報ファイルに記録される個人情報に要配慮個人情報が含まれる場合は、その旨を通知事項に含める必要がある（同項 6 号）。 ・要配慮個人情報を取り扱う事業者は、個人情報保護法令及びガイドラインの規定を遵守する必要がある。

[6] 個人情報の保護に関する法律についてのガイドライン（通則編）https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

<table>
<tr>
<td>である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。)。
(6) 学術研究機関等から当該要配慮個人情報を取得する場合であって、当該要配慮個人情報を学術研究目的で取得する必要があるとき(当該要配慮個人情報を取得する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。)(当該個人情報取扱事業者と当該学術研究機関等が共同して学術研究を行う場合に限る。)。
(7) 当該要配慮個人情報が、本人、国の機関、地方公共団体、学術研究機関等、第 57 条第 1 項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合
(8) その他前各号に掲げる場合に準ずるものとして政令で定める場合</td>
<td>✓ 誤って要配慮個人情報を受領した場合は、すぐに返送・廃棄
✓ 要配慮個人情報を加工することは可能
・要配慮個人情報の取扱いルールに違反した場合、個人情報保護委員会による行政処分や行政指導、さらに刑事罰の対象となる可能性がある。</td>
</tr>
<tr>
<td>(確認義務)
第 30 条(第 1 項) 個人情報取扱事業者は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、次に掲げる事項の確認を行わなければならない。ただし、当該個人データの提供が第 27 条第 1 項各号又は第 5 項各号のいずれかに該当する場合は、この限りでない。
当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名
当該第三者による当該個人データの取得の経緯
(第 2 項) 前項の第三者は、個人情報取扱事業者が同項の規定による確認を行う場合において、当該個人情報取扱事業者に対して、当該確認に係る事項を偽ってはならない。</td>
<td>個人情報取扱事業者は、第三者から個人データの提供を受ける際は、当該第三者による当該個人データの「取得の経緯」を確認しなければならない。
「取得の経緯」を確認する趣旨は、提供を受けようとする個人データが適法に入手されたものではないと疑われる場合に、当該個人データの利用・流通を未然に防止する点にある。
「取得の経緯」の具体的な内容は、個人データの内容、第三者提供の態様などにより異なり得るが、基本的には、取得先の別(顧客としての本人、従業員としての本人、他の個人情報取扱事業者、家族・友人等の私人、いわゆる公開情報等)、取得行為の態様(本人から直接取得したか、有償で取得したか、いわゆる公開情報から取得したか、紹介により取得したか、私人として取得したものか等)などを確認しなければならない。
あくまで、個人データを提供した「第三者」による取得の経緯を確認すれば足り、そこから遡って当該「第三者」より前に取得した者の取得の経緯を確認する義務はない。</td>
</tr>
<tr>
<td>(記録義務)
第 30 条(第 3 項) 個人情報取扱事業者は、第 1 項の規定による確認を行ったときは、個人情報保護委員会規則で定めるところにより、当該個人データの提供を受けた年月日、当該確認に係る事項その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。
(第 4 項) 個人情報取扱事業者は、前項の記録を、当該記録を作成した日から個人情報保護委員会規則で定める期間保存しなければならない。</td>
<td>・個人情報取扱事業者は、記録を、文書、電磁的記録(電磁的方式(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。)で作られる記録をいう。以下同じ。第 2 条第 1 項第 1 号参照)又はマイクロフィルムを用いて作成しなければならない。
個人情報取扱事業者は、作成した記録を規則で定める期間保存しなければならない。
保存期間は記録の作成方法によって異なる。具体的には、次の表のとおりである。(対象となる複数の本人の記録を一体として作成した場合、保存期間は記録ごとに異なることがある。)
<table>
<tr><td>記録の作成方法の別</td><td>保存期間</td></tr>
<tr><td>契約書等の代替手段による方法により記録を作成した場合</td><td>当該記録の個人データの提供をした日から 1 年間</td></tr>
<tr><td>一括して記録を作成する方法により記録を作成した場合</td><td>当該記録の個人データの提供をした 3 年を経過する日までの間</td></tr>
<tr><td>上述以外の場合</td><td>3 年</td></tr>
</table>
</td>
</tr>
</table>

第2節　改正（令和2年）ポイント整理

（適正な取得）に係る法改正についてポイント、および、ケーススタディを整理[7]

ポイント1　不適正取得は利用停止・消去・第三者提供停止請求の義務対象（改正）

表1-2

前提	・**「利用停止等請求・第三者提供停止請求」**とは、本人からの請求により、保有個人データを利用しないか、消去するか、第三者提供を停止しなければならないという対応 ・**対応が必要な場合は、以下の違法行為がある場合**に限られる 権利利益を害する恐れ・不適正利用・目的外取扱い・**不適正取得**・第三者提供制限違反・外国提供違反
法改正	・本人の権利又は正当な利益が害されるおそれがある（利用が不要になった場合、重大な漏えい・滅失・毀損等発生時（第 22 条の 2 第 1 項本文該当時）など）場合に、利用停止、消去又は第三者提供停止義務が新設されている ・事業者としては、幅広に本人の希望通りに対応することが望まれる ✓　不適正利用時にも、利用停止又は消去義務がある ✓　対象が拡大され「6か月以内に消去する短期保存データ」も開示義務の対象になっている
必要な対応	個人情報取扱事業者は対応フローチェック → フロー改訂 → プライバシーポリシー改訂 → 従業者教育等

ポイント2　オプトアウトで取得された個人データのさらにオプトアウト提供は規制対象（改正）

表1-3

前提	・オプトアウトとは：本人の同意なく個人データを第三者提供する構成 ・個人データを提供すること等を公表等しておき、本人から拒否がなければ同意がなくても第三者提供できる仕組み
法改正	・オプトアウト禁止の場合が拡大されている ・具体的には以下の場合は、オプトアウトによる個人データの提供/取得禁止 さらにオプトアウトで取得した個人データをさらにオプトアウトで提供してはならない
経緯	・元々の個人情報保護法では、オプトアウトは対象に限定なく幅広く認められていた。 ・平成 27 年改正での「要配慮個人情報」新設を受け、「要配慮個人情報」はオプトアウト禁止に拡大
必要な対応	・自社で、禁止される類型をオプトアウトで取得/提供しているものがあるか確認 →禁止対象は提供/取得不可なので、個人データなしで業務を行うか、異なる方法で個人データを提供/取得できるか検討する

ポイント3　要配慮個人情報取得制限の例外_個人の権利利益不当侵害のおそれある場合を除く学術研究目的での取扱い（令和3年改正）

表1-4

前提	学術研究機関等とは：大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者をいう（個人情報保護法第 16 条第 8 項）。 ・個人情報保護法がこれまで適用除外されてきたが、令和 3 年改正で適用除外されなくなった。GDPR 適用上はこれで有利になるとも考えられる。 ・報道機関、著述を業として行う者、宗教団体、政治団体についてはこれまで通り個人情報保護法が適用除外される（個人情報保護法第 57 条第 1 項）。
法改正	◆要配慮個人情報の取得制限の例外 本人同意のない要配慮個人情報取得は原則禁止だが、学術研究機関の場合、民間事業者と違って、以下の場合にも可能（第 20 条第 2 項第 5・6 号） ・学術研究目的で取り扱う必要があるとき（当該要配慮個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。） ・**学術研究機関等から当該要配慮個人情報を取得する場合**であって、当該要配慮個人情報を学術研究目的で取得する必要があるとき（当該個人情報取扱事業者と当該学術研究機関等が共同して学術研究を行う場合に限る） ※第 5・6 号ともに、目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがあ る場合を除く

[7] 個人情報保護法令和 2 年改正 2020 年 2021 年のポイント解説 改正法 2022 年 4 月施行 2020.1（2022.5 改訂） 弁護士 水町 雅子 http://www.miyauchi-law.com/f/200325pii2020kaiseigaiyou.pdf

	◆ 第三者提供制限の例外 **本人同意のない要配慮個人情報取得は原則禁止だが、学術研究機関の場合、民間事業者と違って、以下の場合に可能**（第 23 条第 1 項第 6･7 号） ・ 学術研究の成果の公表又は教授するためやむを得ないとき ・ 学術研究目的で提供する必要があるとき（当該個人データを提供する目的の一部が学術研究目的である場合を含む）（当該個人情報取扱事業者と当該第三者が共同して学術研究を行う場合に限る） ・学術研究機関等である第三者が当該個人データを学術研究目的で取り扱う必要があるとき（当該個人データを取り扱う目的の一部が学術研究目的である場合を含む） ※第 5･6･7 号ともに、個人の権利利益を不当に侵害するおそれがある場合を除く

ポイント4　提供先が個人データとして取得することが想定されるときの提供規制（新設）

表1-5

前提	・個人データを外部提供することは、一定の場合にしか認められない（第 27 条）。 ・個人データでなければ、外部提供に当たって特に法規制はなかった
法改正	・自分にとって個人データでなくても、個人情報でなくても、**提供先が個人データとして取得**することが想定されるときは、提供が規制される（改正法第 31 条）→「個人関連情報」 ・提供元が現に認識している場合及び同種の事業を営む事業者の一般的な判断力・理解力を基準にして通常想定できる場合をいう ・契約で定めるのがよいが契約していても個人データとしての利用・取得の可能性ある場合は確認要 ・提供できる場合は、次の場合に限定 ✓ 第 27 条 1 項各号（法令に基づく場合等） ✓ 本人同意が得られていることを確認した場合 ・記録・保存義務あり（改正法第 31 条第 3 項で準用法第 30 条第 3･4 項。改正法第 31 条第 3 項では第 30 条第 2 項も準用。） ・外国への提供であっても同様
経緯・背景	・リクナビの Cookie 情報の外部提供を踏まえての規制新設。Cookie 等規制のための改正ともいえる。 ・改正法では Cookie でなくても「個人関連情報」であれば規制対象。
必要な対応	個人情報取扱業者が自社で、個人関連情報を提供している場合、本人同意の取得、記録の作成・保存対スキーム・フロー検討

ポイント5　漏えい時の行政制裁_個人データ/個人関連情報提供時に取得経緯等を偽った場合（新設）

表1-6

前提	・行政制裁がなされるか ・個人情報保護法に基づく行政制裁等（広義を含む）
法改正	・助言・指導（個人情報保護法第 147 条） ・勧告（個人情報保護法第 148 条 1 項） ・命令（個人情報保護法第 148 条 2･3 項） ・厳密な意味での行政制裁ではないが、立入検査・報告徴収（個人情報保護法第 146 条 1 項） ・ 過料 **・個人データ/個人関連情報の提供時に取得の経緯等を偽った場合**（個人情報保護法第 185 条 1 号）
経緯・背景	不適切事案のレベル感によって、行政制裁等のレベルも変わってくる可能性 ・1 件のメール誤送信、1 枚の名刺を社内で紛失したという場合 ・大量の個人情報を漏えいした場合、あるいは、従業者が悪用したという場合 ・個人情報の内容、量、態様、影響度合い、講じていた安全管理措置（個人情報保護法第 23 条）の内容など ・漏えいに限らず、不適切事案全般に対して行政制裁等 ・重い行政制裁は、事業廃止命令や業務停止命令、業務改善命令等（発出された事例あり） ・なお、不適切な行為がなくても、報告徴収・立入検査等がなされる可能性はある
必要な対応	不適切な行為を防止するよう体制・規程・従業者監督・委託先監督その他の運用を徹底 ・技術的対策も十分に行う ・インシデント発生後は速やかに被害を最小限に抑える方策を取り、真摯に対応する ・保険加入等も検討

ケーススタディ　名簿屋から適法に個人情報を購入する_適正取得

表1-7

前提	名簿購入自体は違法ではない
購入者側の法的問題	購入者には、適正取得義務（第 20 条）、確認義務・記録義務（第 30 条）等が課せられている。 名簿屋による取得の経緯等を確認する必要があり、違法な取得方法を疑われる名簿を購入していたら、購入者自体が個人情報保護法違反になりうる（個人情報保護法ガイドライン（確認記録義務編）14P）
名簿屋側の法的問題	名簿屋にも、同様に、適正取得義務（第 20 条）、確認義務・記録義務（第 30 条）があり、当然適法に名簿を取得する必要がある。加えて、名簿売却に係る第三者提供規制（オプトアウトが殆どの可能性あり？オプトアウトの場合届出＆公表等）、利用目的規制（利用目的の特定等（第 17・18 条）・公表等（第 21・32 条））が課せられている。
購入者の主な義務	**適正取得** 個人情報を偽りその他不正の手段により取得していないか、その名簿は大丈夫か、確認必要 （適正な取得） 第 20 条　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してはならない。 2　個人情報取扱事業者は、次に掲げる場合を除くほか、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。（略） **確認義務・記録義務** 個人データの提供を受ける際は、**取得の経緯等を確認し、記録・保存**しなければならない 第三十条 個人情報取扱事業者は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、次に掲げる事項の確認を行わなければならない。ただし、当該個人データの提供が第二十七条第一項各号又は第五項各号のいずれかに該当する場合は、この限りでない。 一　当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名 二　当該第三者による**当該個人データの取得の経緯** 2　前項の第三者は、個人情報取扱事業者が同項の規定による確認を行う場合において、当該個人情報取扱事業者に対して、当該確認に係る事項を偽ってはならない。 3　個人情報取扱事業者は、第一項の規定による確認を行ったときは、個人情報保護委員会規則で定めるところにより、当該個人データの提供を受けた年月日、当該確認に係る事項その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。 4　個人情報取扱事業者は、前項の記録を、当該記録を作成した日から個人情報保護委員会規則で定める期間保存しなければならない。
購入者の確認方法	① 氏名等の確認方法 ■ 例）口頭/書面で申告を受ける、登記/HP を確認、法人番号から名称・住所を確認、信用 DB、有報等を確認 ② 取得の経緯：取得先の別（顧客としての本人、従業員としての本人、他の個人情報取扱事業者、家族・友人等の私人、公開情報等）、取得行為の態様（本人から直接取得、有償取得、公開情報、紹介、私人として取得） ■ 例）契約書を確認、本人の同意を得ていることを誓約する書面の取得、HP、同意書面を確認 ■ 適法に入手されたものではないと疑われるのに提供を受けた場合、第 20 条 1 項違反のおそれ ■ あくまで提供者の取得経緯を確認すれば足り、それより前に取得した者の取得経緯を確認する必要はない ③ 提供者が法を遵守していることについても確認することが望ましい ■ オプトアウトの場合は、オプトアウト届出が公表されていることを確認し記録しなければならない

（参考1）　個人データへのリスク対策

個人データが第三者に閲覧されないうちに全てを回収した場合は漏えいに該当しないため不要、また、高度な暗号化その他の個人の権利利益を保護するために必要な措置が講じられている場合も不要となる。すぐに取り返すことと、電子政府推奨暗号リスト（CRYPTREC）に載っているような暗号化を実施して保存しておくことが重要。

（参考2）　個人情報の提供・取得とクラウドサービス

クラウドを通じて個人情報を取り扱うに当たっては、個人情報保護法の規制を受ける場合がある。クラウドサービスにおいて、利用者の保有する情報は、クラウド事業者の管理するサーバに保管されることとなる。

クラウド事業者の管理するサーバへの個人情報データの移動が、個人情報保護法上の「提供」に該当するか否かがまず問題となる。

「クラウドサービスの利用が、本人の同意が必要な第三者提供又は委託に該当するかどうかは、保存している電子データに個人データが含まれているかどうかではなく、クラウドサービスを提供する事業者において個人データを取り扱うこととなっているのかどうかが判断の基準となる。

「契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等が考えられる。」と説明されている。

クラウド事業者がユーザーの保存した個人データを取り扱うこととなっている場合には、「提供」に当たることとなる。クラウドサービス提供事業者の管理するサーバへのデータの移動が、個人情報保護法上の第三者への「提供」に該当する場合、原則として、あらかじめ本人の同意を取得することが必要となる。

第3節　法の条文（令和2年改正との対比表）[8]

表1-8

改正後	改正前（条文番号変更の場合は条文内容省略）
（利用目的の特定） 第 17 条（第 1 項）　個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。	3　個人情報取扱事業者等の義務 3-1　個人情報の利用目的（第 15 条・第 16 条、第 18 条第 3 項関係） 3-1-1　利用目的の特定（第 15 条第 1 項関係）
（利用目的の変更） 第 17 条（第 2 項）　個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と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。	3-1-2　利用目的の変更（第 15 条第 2 項、第 18 条第 3 項関係）
（利用目的による制限） 第 18 条（第 1 項）　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。	3-1-3　利用目的による制限（第 16 条第 1 項）
（公表） 第 21 条（第 1 項）　個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない	3-3-3　利用目的の通知又は公表（第 18 条第 1 項関係）

[8] 個人情報の保護に関する法律についてのガイドライン（通則編）（平成 28 年個人情報保護委員会告示第 6 号）の一部改正の新旧対照表
https://www.ppc.go.jp/files/pdf/211116_guidelines01_shinkyu.pdf

改正後	改正前（条文番号変更の場合は条文内容省略）
（適正な取得） 第 20 条　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してはならない。 2　個人情報取扱事業者は、次に掲げる場合を除くほか、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。 一　法令に基づく場合 二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。 三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。 四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。 五　当該個人情報取扱事業者が学術研究機関等である場合であって、当該要配慮個人情報を学術研究目的で取り扱う必要があるとき（当該要配慮個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）。 六　学術研究機関等から当該要配慮個人情報を取得する場合であって、当該要配慮個人情報を学術研究目的で取得する必要があるとき（当該要配慮個人情報を取得する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（当該個人情報取扱事業者と当該学術研究機関等が共同して学術研究を行う場合に限る。）。 七　当該要配慮個人情報が、本人、国の機関、地方公共団体、学術研究機関等、第五十七条第一項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合 八　その他前各号に掲げる場合に準ずるものとして政令で定める	**（適正な取得）** 第 17 条　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してはならない。 2　個人情報取扱事業者は、次に掲げる場合を除くほか、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。 一　法令に基づく場合 二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。 三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。 四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。 五　当該要配慮個人情報が、本人、国の機関、地方公共団体、第 76 条第 1 項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合 六　その他前各号に掲げる場合に準ずるものとして政令で定める場合
（確認義務） 第 30 条（第 1 項）　個人情報取扱事業者は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、次に掲げる事項の確認を行わなければならない。ただし、当該個人データの提供が第 27 条第 1 項各号又は第 5 項各号のいずれかに該当する場合は、この限りでない。 　当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名 　当該第三者による当該個人データの取得の経緯 （第 2 項）　前項の第三者は、個人情報取扱事業者が同項の規定による確認を行う場合において、当該個人情報取扱事業者に対して、当該確認に係る事項を偽ってはならない	3-7-6　提供先の第三者における確認義務（第 26 条第 1 項関係）
（記録義務） 第 30 条（第 3 項）　個人情報取扱事業者は、第 1 項の規定による確認を行ったときは、個人情報保護委員会規則で定めるところにより、当該個人データの提供を受けた年月日、当該確認に係る事項その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。 （第 4 項）　個人情報取扱事業者は、前項の記録を、当該記録を作成した日から個人情報保護委員会規則で定める期間保存しなければならない。	3-7-7　提供先の第三者における記録義務（第 26 条第 3 項関係）

第2章　漏えい等報告・本人通知の義務化（第26条）

改正法（令和2年）では、個人情報取扱事業者の責務として、個人データの漏えい等（滅失、毀損を含む）が発生し、個人の権利利益を害するおそれが大きい場合に、速やかに個人情報保護委員会への報告[9]及び本人への通知[10]をすることが義務化された。

これにより、個人情報保護委員会が個人情報取扱事業者に対し、速やかに適切な指導・監督を行うことができ、二次被害発生・拡大の防止につながる。また、本人が漏えい等の事態の発生を早く知ることで、保有個人データの利用停止・消去等の請求[11]をしやすくなる。

ここでは、漏えい等事案が発覚した場合に講ずべき措置、報告・本人通知が必要となる場合と要しない場合、報告・本人通知義務の主体、個人情報保護委員会への報告、本人への通知について記述する。

第1節　漏えい等事案が発覚した場合に講ずべき措置

ガイドライン[12]では、漏えい等事案の内容等に応じて、次に掲げる事項について必要な措置を講じなければならないとされている。

① 事業者内部における報告及び被害の拡大防止
② 事実関係の調査及び原因の究明
③ 影響範囲の特定
④ 再発防止策の検討及び実施
⑤ 個人情報保護委員会への報告及び本人への通知

第2節　報告・本人通知が必要となる場合

個人の権利利益を害するおそれが大きいものとして規則第7条にて4つの類型（報告対象事態）を定め、ガイドライン[13]にて、それぞれの報告対象事態において報告を要する事例を挙げている。

なお、後述の4つの類型（報告対象事態）①から③については**1件以上**の個人データの漏えい等が発生した**おそれ**がある場合でも報告・本人通知の対象となる。

報告対象事態における「おそれ」については、その時点で判明している事実関係に基づいて個別の事案ごとに蓋然性を考慮して判断することになる。漏えい等が発生したおそれについては、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がこれに該当する[14]。

【4つの類型（報告対象事態）】

① 要配慮個人情報が含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態
   - 病院における患者の診療情報や調剤情報を含む個人データを記録した USB メモリーを紛失した場合
   - 従業員の健康診断等の結果を含む個人データが漏えいした場合

② 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
   - EC サイトからクレジットカード番号を含む個人データが漏えいした場合
   - 送金や決済機能のあるウェブサービスのログイン ID とパスワードの組み合わせを含む個人データが漏えいした場合

[9] 規則第 8 条、ガイドライン（通則編）3-5-3（個人情報保護委員会への報告）
[10] 規則第 10 条、ガイドライン（通則編）3-5-4（本人への通知）
[11] 第 33 条 5 項、6 項
[12] ガイドライン（通則編）3-5-4（漏えい等事案が発覚した場合に講ずべき措置）
[13] ガイドライン（通則編）3-5-3-1（報告対象となる事態）
[14] ガイドライン（通則編）3-5-3-1（報告対象となる事態）

③ 不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態（内部不正による漏えい等も含む）

- 不正アクセスにより個人データが漏えいした場合

※漏えいが発生したおそれがある事態に該当し得る事例

(ア) 個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において外部からの不正アクセスによりデータが窃取された痕跡が認められた場合

(イ) 個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において、情報を窃取する振る舞いが判明しているマルウェアの感染が確認された場合

- ✧ 単にマルウェアを検知したことをもって直ちに漏えいのおそれがあると判断するものではなく、防御システムによるマルウェアの実行抑制の状況、外部通信の遮断状況等についても考慮する[15]。

(ウ) マルウェアに感染したコンピュータに不正な指令を送り、制御するサーバ（C&C サーバ）が使用しているものとして知られている IP アドレス・FQDN への通信が確認された場合

(エ) 不正検知を行う公的機関、セキュリティ・サービス・プロバイダ、専門家等の第三者から、漏えいのおそれについて、一定の根拠に基づく連絡を受けた場合

- ランサムウェア等により個人データが暗号化され、復元できなくなった場合
- 個人データが記載又は記録された書類・媒体等が盗難された場合
- 従業者が顧客の個人データを不正に持ち出して第三者に提供した場合

例えば、個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において、通常の業務で必要としないアクセスによりデータが窃取された痕跡が認められた場合が考えられる。

④ 個人データに係る本人の数が 1,000 人を超える漏えい等が発生し、又は発生したおそれがある事態（本人の数が確定できない漏えい等において、漏えい等が発生したおそれがある個人データに係る本人の数が最大 1,000 人を超える場合も該当）

- システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となり、当該個人データに係る本人の数が 1,000 人を超える場合

第3節　報告・本人通知を要しない場合

以下の場合には報告・本人通知の義務から除外される。漏えい等による被害拡大防止の観点からも、個人データをすぐに回収（第三者閲覧不可の状態に）できる体制・ルールを整えておくことや、高度な暗号化等の秘匿化[16]を含む安全管理措置を講じておくことが重要となる。

- 個人データを第三者に閲覧されないうちに全てを回収した場合（閲覧が不可能な状態とするまでの間に第三者が閲覧していないことがアクセスログ等から確認された場合も含む）[17]は、漏えいに該当しない。
- 漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合等、「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている場合については、報告を要しない[18]。

第4節　報告・本人通知義務の主体

漏えい等報告・本人通知の義務を負う主体は、漏えい等が発生し、又は発生したおそれがある個人データを取り扱う個人情報取扱事業者である。

ただし、委託先において漏えい等事案が生じた場合には、原則として委託元と委託先の双方が報告する義務を負う。委託先が委託元に対して、当該事態が発生したことを速やかに（概ね3～5日以内）通知した場合は、委託先は報告義務を免除される[19]とともに、本人への通知義務も免除される[20]。委託元が報告や通知内容等を管理できるよう、漏えい等の報告に関する事項を委託契約に盛り込んでおくことが望ましい。

---

[15] QA 1-6 個人データの漏えい等の報告等（第 26 条関係）A6-14
[16] QA 1-6 個人データの漏えい等の報告等（第 26 条関係）A6-16
[17] QA 1-6 個人データの漏えい等の報告等（第 26 条関係）A6-1
[18] ガイドライン（通則編）3-5-3-1（報告対象となる事態）
[19] ガイドライン（通則編）3-5-3-5（委託元への通知による例外）
[20] ガイドライン（通則編）3-5-4-1（通知対象となる事態及び通知義務の主体）

なお、クラウドサービス提供事業者に関して、Q&A A6-19[21]に次の通り記載されている。

> **クラウドサービス提供事業者が、個人データを取り扱わないこととなっている場合において、報告対象となる個人データの漏えい等が発生したときには、クラウドサービスを利用する事業者が報告義務を負います。この場合、クラウドサービス提供事業者は、第26条第1項の報告義務を負いませんが、クラウドサービスを利用する事業者が安全管理措置義務及び同項の報告義務を負っていることを踏まえて、契約等に基づいてクラウドサービスを利用する事業者に対して通知する等、適切な対応を行うことが求められます。**

第5節　個人情報保護委員会への報告

原則として、個人情報保護委員会のホームページの報告フォームに入力する方法[22]により「速報」と「確報」の二段階に分けて行う[23]。速報の時点で全ての事項を報告できる場合には、1回の報告で速報と確報を兼ねることができる。

なお、報告先が事業所管大臣となるときは、事業所管大臣が報告方法を定めている場合にはその方法により、定めがない場合には報告書を提出する方法により報告する[24]。

また、個人情報取扱事業者が法人である場合、いずれかの部署の従業者が当該事態を知った時点を基準に報告期限を判断するため、組織内で迅速に報告・連絡できる体制やルール（対応フロー等）を整備しておくことが重要となる。

- 速報

  時間的制限：報告対象の事態を知ってから「速やかに」
  （個別の事案によるものの、当該事態を知った時から概ね3～5日以内）

  報告内容：報告事項のうち、報告をしようとする時点において把握している内容
- 確報

  時間的制限：報告対象の事態を知ってから30日以内
  （不正の目的をもって行われたおそれがある漏えい等の場合は60日以内）

  報告内容：全ての報告事項
  （合理的努力を尽くしても全ての事項を報告できない場合、判明次第、報告を追完）

【報告事項】

① 概要
② 漏えい等が発生し、または発生したおそれがある個人データの項目
③ 漏えい等が発生し、または発生したおそれがある個人データに係る本人の数
④ 原因
⑤ 二次被害またはそのおそれの有無およびその内容
⑥ 本人への対応の実施状況
⑦ 公表の実施状況
⑧ 再発防止のための措置
⑨ その他参考となる事項

[21] QA 1-6 個人データの漏えい等の報告等（第 26 条関係）A6-19
[22] 漏えい等の対応とお役立ち資料 ｜ 個人情報保護委員会 https://www.ppc.go.jp/personalinfo/legal/leakAction/
[23] 規則第 8 条、ガイドライン（通則編）3-5-3（個人情報保護委員会への報告）
[24] QA 1-6 個人データの漏えい等の報告等（第 26 条関係）A6-24

第6節　本人への通知

個人データの漏えい等の事態を知った後、「当該事態の状況に応じて速やかに」本人への通知を行う必要がある[25]。個別の事案において、通知により本人の権利利益が保護される蓋然性や通知による弊害等を勘案して判断するものとされ、具体的な時間的制限は示されていない。

本人に通知する事項は、個人情報保護委員会への報告事項のうち、以下5項目とされており、「本人の権利利益を保護するために必要な範囲において」[26]行うものとされている。

【通知事項】

① 概要
② 漏えい等が発生し、または発生したおそれがある個人データの項目
③ 原因
④ 二次被害またはそのおそれの有無およびその内容
⑤ その他参考となる事項

通知の様式は法令上定められていないが、本人にとって分かりやすい形（文書の送付、電子メールの送信等）で通知を行うことが望ましいとされている。

ただし、本人への通知が困難（保有個人データに連絡先が含まれていない等）である場合は、本人の権利利益を保護するために必要な代替措置（事案の公表や問合せ窓口の設置・公表等）を講ずることによる対応が認められる。

[25] 規則第 10 条、ガイドライン（通則編）3-5-3（本人への通知）
[26] ガイドライン（通則編）3-5-3-3（通知の内容）

第3章　個人情報の提供（第27条、第28条、第29条、第30条）

第1節　外国にある第三者への提供

第1項　外国にある第三者の解釈

国内の第三者と外国にある第三者では定義が違い、また規制内容にも差異が認められる。

外国にある第三者においては、委託・事業承継等が発生した場合・共同利用等による提供であっても例外とはならず、第三者扱いのままである。このため原則本人の同意が必要となる。また、オプトアウトによる第三者提供も認められない。これは個人情報保護法第28条（外国にある第三者への提供の制限）において、以下のように記述されているからである。

> （前略）前条第一項各号に掲げる場合を除くほか、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得なければならない。この場合においては、同条の規定は、適用しない。

一方、別の例外が存在しており、この例外が該当すると外国にある第三者扱いしなくてよい、ということになる。結果として第27条（第三者提供の制限）が適用され、国内の第三者にあたるかどうかを評価する。

すなわち、個人情報の提供をするにあたり

- それが外国の第三者にあたる場合には、本人の同意が必要である（海外にある委託先の場合でも、外国にある第三者への提供である旨の通知と同意が必要である）
- 外国の第三者にあたらない場合には、第27条が適用される

この外国の第三者の例外の条件であるが、「個人情報の保護に関するガイドライン（外国にある第三者編）」の総論[27]に以下のように記載されている。

> 個人情報取扱事業者は、個人データを外国にある第三者に提供するに当たっては、第28条第1項法に従い、次の（1）から（3）までのいずれかに該当する場合を除き、あらかじめ「外国にある第三者への個人データの提供を認める旨の本人の同意」を得る必要がある。
>
> （1）当該第三者が、我が国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の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号。以下「規則」という。）で定める国にある場合（※1）
>
> （2）当該第三者が、個人情報取扱事業者が講ずべき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）次の①から⑦までのいずれかに該当する場合（第27条第1項各号関係）
>
> （中略）
>
> 上記（1）の場合、当該第三者が所在する国は、第28条第1項における「外国」に該当しない。また、上記（2）の場合、当該第三者は、第28条第1項における「第三者」に該当しない。したがって、これらの場合には、第28条第1項の適用がないため、個人情報取扱事業者は、当該第三者への個人データの提供に際して、「外国にある第三者への個人データの提供を認める旨の本人の同意」を得る必要はない。

上記（1）から（3）については、同文書の上記引用部分以降で詳述されているので参照されたい。

[27] 引用：https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/#a2（2022/11/11 参照）

第2項　外国にある第三者への提供に関する規制

改正法（令和2年）における、外国にある第三者に個人データを提供する要件を整理すると、以下の通りとなる。[28]

外国にある第三者への提供

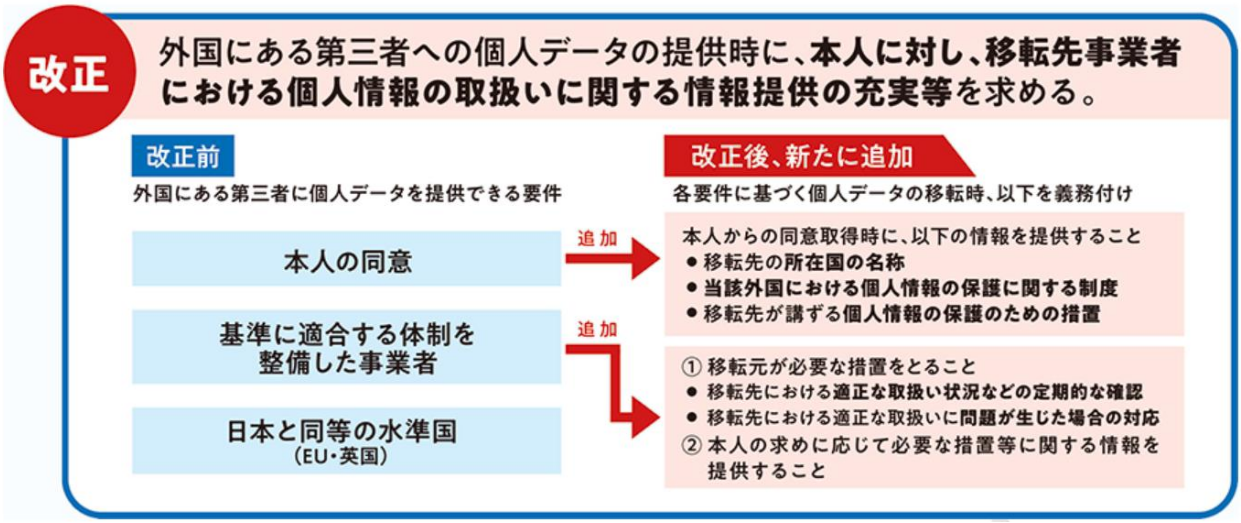


図3-1　外国にある第三者への提供（改正前後のポイント）

以下、改正法（令和2年）によって新たに追加された義務について記載する。

（a） 本人の同意

> 第28条
> 2　個人情報取扱事業者は、前項の規定により本人の同意を得ようとする場合には、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、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報を当該本人に提供しなければならない。

【追加された条文の解釈】

本人の同意を根拠に外国にある第三者に提供する場合には、同意取得時に本人に対し以下の情報を提供することが義務付けられた。

- 移転先の所在国の名称
- 当該外国における個人情報の保護に関する制度
- 移転先が講ずる個人情報の保護のための措置

まず移転先の所在国の名称を提供することが義務付けられている。ただし、国名が特定できない場合は、その理由も含めて本人に伝えるとともに、外国の範囲が決まっていればその情報を提示する。

そのうえで、当該外国における制度や措置を調査して本人に提供する必要がある。この改正の趣旨は、個人データの越境移転に伴うリスクについて、本人の予測可能性を高めることにあるため、日本の個人情報保護法との違いをコンパクトに提示すると分かりやすい。個人情報保護委員会がまとめているサイト「外国における個人情報の保護に関する制度等の調査」があるので、参考にするとよい。[29]

[28] 引用：https://www.ppc.go.jp/news/kaiseihou_feature/#gaikoku　（2022/11/11 参照）
[29] 引用：https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/#gaikoku（2022/11/11 参照）

（b） 基準に適合する体制を整備した事業者

第28条
3　個人情報取扱事業者は、個人データを外国にある第三者（第一項に規定する体制を整備している者に限る。）に提供した場合には、個人情報保護委員会規則で定めるところにより、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供しなければならない。

【追加された条文の解釈】

移転先の第三者が基準適合体制を整備していることを根拠に、個人データの越境移転を行った場合には、移転先の第三者による個人データの適正な取扱いを継続的に確保することを、移転元に求めている。具体的には、次の2点である。

① 移転元が必要な措置を取ること
・移転先における適正な取扱い状況などの定期的な確認
（注）「定期的に確認」とは、年に1回程度又はそれ以上の頻度で確認することをいう。
・移転先における適正な取扱いに問題が生じた場合の対応

② 本人の求めに応じて必要な措置等に関する情報を提供すること
（注）規則第18条（第3項）に具体的に提供しなければならない情報（次の(1)～(7)）についての記載があるので参照されたい。これらの情報を、本人に対し遅滞なく情報提供しなければならない。[30]
(1) 当該第三者による第 28 条第 1 項に規定する体制の整備の方法
(2) 当該第三者が実施する相当措置の概要
(3) 第 1 項第 1 号の規定による確認の頻度及び方法
(4) 当該外国の名称
(5) 当該第三者による相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその概要
(6) 当該第三者による相当措置の実施に関する支障の有無及びその概要
(7) 前号の支障に関して第 1 項第 2 号の規定により当該個人情報取扱事業者が講ずる措置の概要

なお、第28条第1項「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者」は、規則第16条に規定されている。

規則第16条
法第28条第1項の個人情報保護委員会規則で定める基準は、次の各号のいずれかに該当することとする。
（1）個人情報取扱事業者と個人データの提供を受ける者との間で、当該提供を受ける者における当該個人データの取扱いについて、適切かつ合理的な方法により、法第4章第2節の規定の趣旨に沿った措置の実施が確保されていること。
（2）個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること。

「適切かつ合理的な方法」は、個々の事例ごとに判断されるべきであるが、個人データの提供先である外国にある第三者が、我が国の個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずることを担保することができる方法である必要がある。

[30] 引用：https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/#a6-2-2（2022/11/11 参照）

例えば、次の事例が該当する。[31]

事例1） 外国にある事業者に個人データの取扱いを委託する場合
提供元及び提供先間の契約、確認書、覚書等
事例2） 同一の企業グループ内で個人データを移転する場合
提供元及び提供先に共通して適用される内規、プライバシーポリシー等

したがって、CSPに個人データの取扱いを委託する場合は、CSPとの間で締結する委託契約がこの事例に該当する。ただし、CSPが海外のクラウド事業者の場合は、第32条第1項第4号及び政令第10条第1号の規定により、個人データを保管している当該国における個人情報の保護に関する制度を把握した上で安全管理措置を実施することが求められる。また、本人の適切な理解と関与を促す観点から、その国の制度についても、本人の知り得る状態に置くといった対応が望ましい。（「第3項 保有個人データの安全管理のために講じた措置」参照）

第3項　保有個人データの安全管理のために講じた措置

第32条第1項第4号及び政令第10条第1号の規定を記述する。

第32条（第１項）
個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。
（1） 当該個人情報取扱事業者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名
（2） 全ての保有個人データの利用目的（第 21 条第４項第１号から第３号までに該当する場合を除く。）
（3） 次項の規定による求め又は次条第１項（同条第５項において準用する場合を含む。）、第 34 条第１項若しくは第 35 条第１項、第３項若しくは第５項の規定による請求に応じる手続（第 38 条第２項の規定により手数料の額を定めたときは、その手数料の額を含む。）
（4） 前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの

政令第10条（保有個人データの適正な取扱いの確保に関し必要な事項）
法第32条第１項第４号の政令で定めるものは、次に掲げるものとする。
（1） 法第 23 条の規定により保有個人データの安全管理のために講じた措置（本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置くことにより当該保有個人データの安全管理に支障を及ぼすおそれがあるものを除く。）
（2） 当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先
（3） 当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先

[31] 引用：https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/#a6-1（2022/11/11 参照）

政令第10条で定めるものとして、「(1) 法第23条の規定により保有個人データの安全管理のために講じた措置」が追加された。この「保有個人データの安全管理のために講じた措置」について、ガイドラインには、以下の項目毎に事例が記載されている。[32]

【安全管理のために講じた措置として本人の知り得る状態に置く内容の事例】

（基本方針の策定）
事例） 個人データの適正な取扱いの確保のため、「関係法令・ガイドライン等の遵守」、「質問及び苦情処理の窓口」等についての基本方針を策定
（個人データの取扱いに係る規律の整備）
事例） 取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について個人データの取扱規程を策定

（組織的安全管理措置）
事例1） 個人データの取扱いに関する責任者を設置するとともに、個人データを取り扱う従業者及び当該従業者が取り扱う個人データの範囲を明確化し、法や取扱規程に違反している事実又は兆候を把握した場合の責任者への報告連絡体制を整備
事例2） 個人データの取扱状況について、定期的に自己点検を実施するとともに、他部署や外部の者による監査を実施

（人的安全管理措置）
事例1） 個人データの取扱いに関する留意事項について、従業者に定期的な研修を実施
事例2） 個人データについての秘密保持に関する事項を就業規則に記載

（物理的安全管理措置）
事例1） 個人データを取り扱う区域において、従業者の入退室管理及び持ち込む機器等の制限を行うとともに、権限を有しない者による個人データの閲覧を防止する措置を実施
事例2） 個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するための措置を講じるとともに、事業所内の移動を含め、当該機器、電子媒体等を持ち運ぶ場合、容易に個人データが判明しないよう措置を実施

（技術的安全管理措置）
事例1） アクセス制御を実施して、担当者及び取り扱う個人情報データベース等の範囲を限定
事例2） 個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入
（外的環境の把握）
事例） 個人データを保管している A 国における個人情報の保護に関する制度を把握した上で安全管理措置を実施

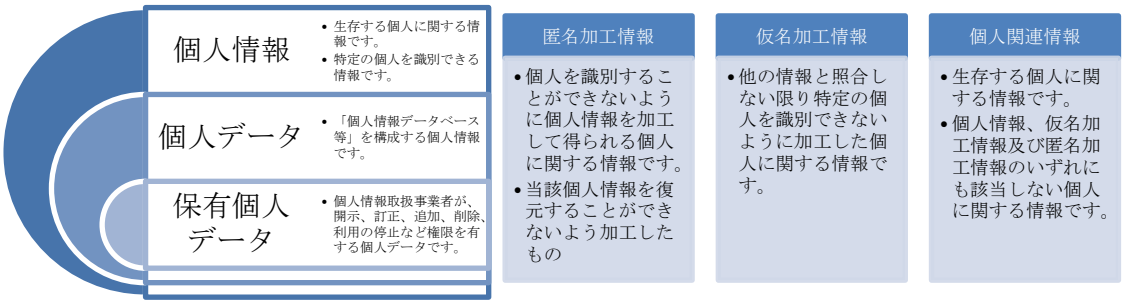
[32] 引用：https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a3-8-1（2022/11/11 参照）

第4章　個人関連情報、および第三者提供の制限等について（第2条第7項、第16条第7項、第31条）

第1節　個人関連情報および個人関連情報取扱事業者（第2条第7項、第16条第7項）

2022年4月施行の改正個人情報保護に関する法律では、「個人関連情報」という個人に関する情報の類型が新設されました（図4-1）。個人情報保護に関する法律において「個人関連情報」とは「生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないものをいう。」[33] と定義されています。個人情報保護法ガイドライン（通則編）では、「個人関連情報」の定義を解釈され、個人を識別することができる氏名、生年月日、住所など情報は個人情報であり、個人関連情報に該当しません。個人関連情報に該当する事例としては、Cookie等の端末識別子を通じて収集された、ある個人のウェブサイトの閲覧履歴やある個人の位置情報、購入歴などが挙げられています。[34] ただし、個人関連情報のデータ性質および量につきましては留意が必要と考えられます。例えば、位置情報やウェブサイト閲覧情報などの個人関連情報が連続的に蓄積されるによって個人を識別できるようになる場合は個人情報に該当します。つまり、個人関連情報を個人情報として取得する際に、本人の同意を得ることが求められます。

表4-1　個人関連情報の第三者提供にあっての記録事項



個人関連情報を取り扱っている事業者につきましても、個人情報保護に関する法律において「この章、第6章及び第7章において「個人関連情報取扱事業者」とは、個人関連情報を含む情報の集合物であって、特定の個人関連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その他特定の個人関連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（第31条第1項において「個人関連情報データベース等」という。）を事業の用に供している者をいう。ただし、第2項各号に掲げる者を除く。」[35]と定義されています。個人情報保護法ガイドライン（通則編）では、「個人関連情報取扱事業者」の定義「「個人関連情報取扱事業者」とは、個人関連情報データベース等を事業の用に供している者のうち、国の機関、地方公共団体、第2条第9項に規定する独立行政法人等（別表第2に掲げる法人を除く。）及び第2条第10項に規定する地方独立行政法人を除いた者をいう。」[36]ように解釈されています。

[33] 第 2 条（第 7 項）
[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（通則編）平成 28 年 11 月（令和 3 年 10 月一部改正）個人情報保護委員会　p. 22.
[35] 第 16 条（第 7 項）
[36] 個人情報の保護に関する法律についてのガイドライン（通則編）平成 28 年 11 月（令和 3 年 10 月一部改正）個人情報保護委員会　p. 22-23.

第2節　個人関連情報の第三者提供の制限（第31条）

改正個人情報保護法においては個人関連情報の第三者提供が制限されています。改正個人情報保護法では提供先で個人情報となる「個人関連情報」の第三者提供の場合は新たに下記の2つを義務化しています。

- 同意確認義務：提供元は、提供先が「個人関連情報」の提供を受けて、個人情報と突合、照会する場合、いわば「個人情報」として取得することが想定されるとき、提供先において事前に本人同意が得られていることを確認しなければなりません。[37]
- 確認記録義務：提供元は、上記による確認を行ったときは定めた事項[38]に関する記録を作成しなければなりません。[39]

個人関連情報の提供にあたる本人の同意の取得につきましては、最終的な利用者となる提供先の第三者であるが、本人の権利利益の保護の観点から、提供元の個人関連情報取扱事業者が代行することが認められています。[40]　ただし、提供元が同意取得代行する場合は個人関連情報に限って、「委託」に該当せずに、委託に伴う義務が発生しません。本人の同意取得主体を問わず、個人データとして取得する提供先、対象となる個人関連情報の項目、利用目的等の情報について本人に示すことが求められています。

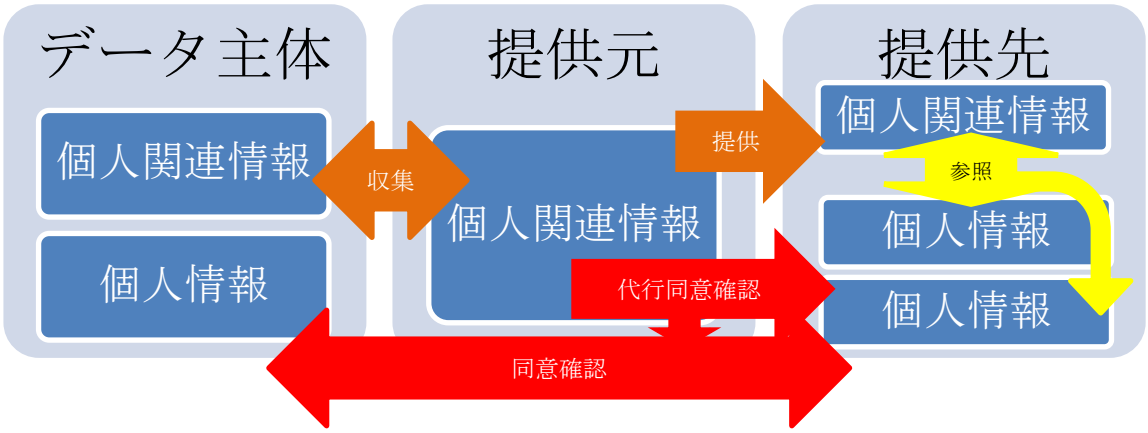


図4-1　個人関連情報取り扱いフロー

個人関連情報の提供先が外国にある第三者であるときに、当該外国の名称、当該外国における個人情報の保護に関する情報、当該第三者が講ずる個人情報の保護のための措置に関するなどの情報を本人に提供されていることを確認することが求められています。（第 31 条（二）　参照）

個人関連情報取扱事業者は、改正個人情報保護法（第31条第1項）の規定による本人の同意取得の確認を行った場合は、その記録を作成しなければなりません（第30条第3項）。その記録の作成する媒体、方法、事項、保存期間または記録事項の省略などにつきましては「個人情報の保護に関する法律についてのガイドライン（通則編）」においては詳しく説明されています。[41]（表4-2　参照）

[37] 第 31 条（第 1 項）。個人情報の保護に関する法律についてのガイドライン（通則編）平成 28 年 11 月（令和 3 年 10 月一部改正）個人情報保護委員会　p. 90.
[38] 個人情報の保護に関する法律についてのガイドライン（通則編）平成 28 年 11 月（令和 3 年 10 月一部改正）個人情報保護委員会　p. 104.
[39] 第 31 条（第 3 項）。個人情報の保護に関する法律についてのガイドライン（通則編）平成 28 年 11 月（令和 3 年 10 月一部改正）個人情報保護委員会　p. 100.
[40] 個人情報の保護に関する法律についてのガイドライン（通則編）平成 28 年 11 月（令和 3 年 10 月一部改正）個人情報保護委員会（3-7-2-2）p. 93-94.
[41] 個人情報の保護に関する法律についてのガイドライン（通則編）平成 28 年 11 月（令和 3 年 10 月一部改正）個人情報保護委員会（3-7-2-2）p. 100-108.

表4-2 個人関連情報の第三者提供にあっての記録事項

記録媒体	文書、電磁的記録、マイクロフィルム		
作成時期	提供の都度または提供する前		
作成方法	一括して記録を作成する方法(*1)	契約書等の代替手段による方法	その他の場合(*2)
記録事項	①本人の同意(*3)　②提供した年月日　③提供先の氏名又は名称（法人の場合はその代表者の氏名）　④当該個人関連情報の項目		
保存期間	最後に当該記録に係る個人関連情報の提供を行った日から起算して３年を経過する日までの間	最後に当該記録に係る個人関連情報の提供を行った日から起算して１年を経過する日までの間	３年

(1) 継続的に提供する場合は、一括して記録を作成することができる。
(2) 規則第27条第3項の要件を満たさない書面も、記録事項が記載されていれば記録として認められます。
(3) 外国にある第三者への提供にあっては、情報の提供についても記録します。

第5章　匿名加工情報関連
（第2条、第16条、第43条、第44条、第45条、第46条）

第1節　匿名加工情報に係る規程内容の概要

個人情報保護法では、「個人情報の有用性」と「個人の権利利益の保護」のバランスを図ることを目指しているが、ここでは「個人情報の有用性」を推進するための方策として導入された概念である「匿名加工情報」を対象として、係る法的要件とその対応方法を記載する。

「匿名加工情報」とは、「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、復元できないようにしたもの」である。また、匿名加工情報は、一定のルールのもとで、第三者提供や目的外利用の同意を得ることなく利用が可能な情報である。

個人情報保護法では、匿名加工情報に関連して、以下の5項目の内容を規定している。[42]

① 匿名加工情報の作成のための適正な加工（第43条第1項関係）
② 匿名加工情報に係る安全管理措置（第43条第2項、第6項、第46条関係）
③ 作成時の公表（第43条第3項関係）
④ 匿名加工情報の第三者提供（第43条第4項、第44条関係）
⑤ 識別行為の禁止（第43条第5項、第45条関係）

上記条文で対象としている既定は、個人情報取扱事業者（作成者）と匿名加工情報取扱事業者（受領者）についての法的要件を記載したものである。（「図5-1　匿名加工情報の作成者・受領者が遵守すべき規定」参照）

また、今回取り上げた条文では、「個人情報保護委員会規則で定める基準に従い、・・」といった表現でしばしば個人情報保護員会の定める規則[43]が参照されており、当ガイドでは、あわせてこちらからも引用している。（以下、規則という。）

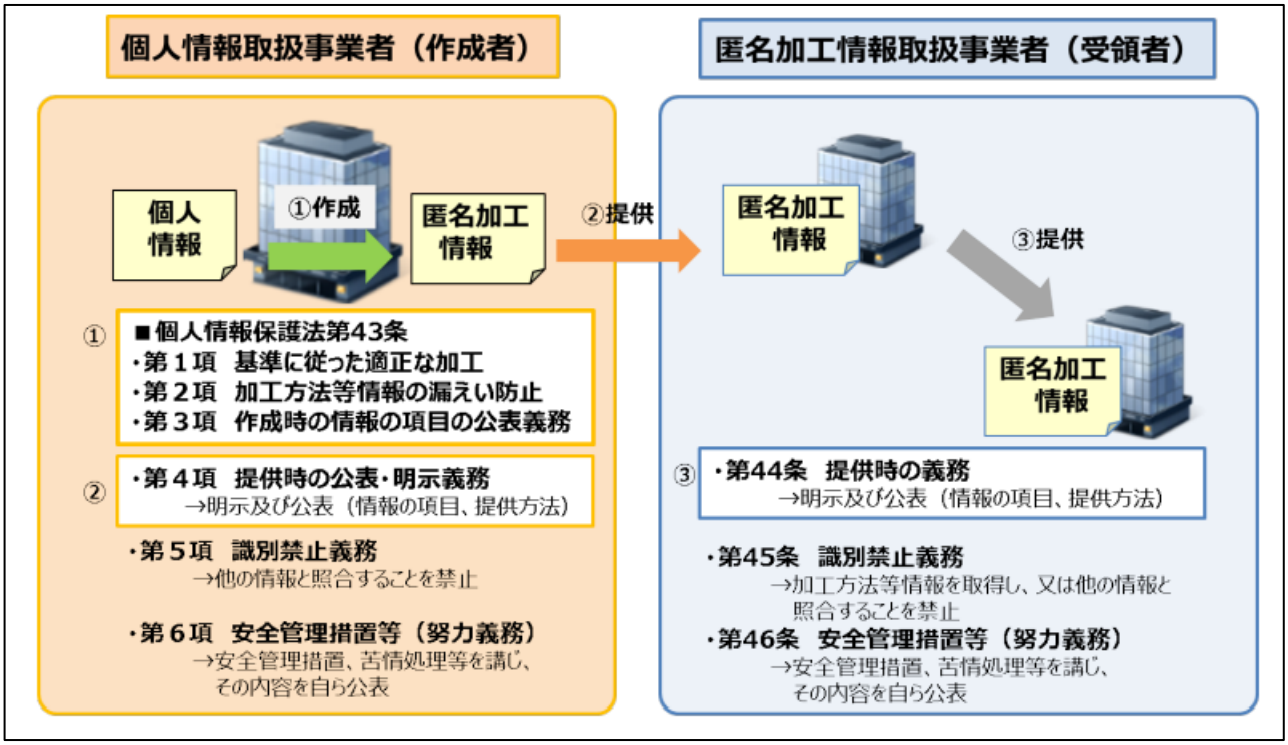


図5-1　匿名加工情報の作成者・受領者が遵守すべき規定[44]

[42]「個人情報の保護に関する法律についてのガイドライン（仮名加工情報・匿名加工情報編）（2016/11 月）（2021 年 10 月一部改正）」
[43]「個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第 3 号）
[44]「個人情報保護委員会事務局レポート　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（2017 年 2 月）」

第2節　匿名加工情報に係る具体的な行動規範とそのポイント

ここからは、上記の各条文について、各組織で対応を検討する上での具体的な行動規範やそのポイントについて記載する。

第1項　匿名加工情報の作成のための適正な加工（第43条第1項関係）

個人情報取扱事業者は、匿名加工情報を作成するときは、特定の個人を識別できないように、かつ、その作成に用いる個人情報を復元できないようにするために、規則第19条各号に定める基準に従って、当該個人情報を加工しなければならないとされている。

表5-1　匿名加工情報の作成のための適正な加工（抜粋）

項目 [該当条文]	事業者の対応	ガイドライン（補足）
匿名加工情報の適正な加工（第 36 条 1 項）	個人情報取扱事業者は、匿名加工情報を作成するとき、特定の個人を識別すること及びその作成に用いる個人情報を復元することができないようにするため、以下に挙げる個人情報保護委員会規則で定める基準（規則第 19 条の各号）に従い加工しなければならない。 1. 特定の個人を識別することができる記述等の削除 2. 個人識別符号の削除 3. 情報を相互に連結する符号の削除 4. 特異な記述等の削除 5. 個人情報データベース等の性質を踏まえたその他の措置	1. 特定の個人を識別することができる記述等の削除 事例）氏名、住所、生年月日が含まれる個人情報を、以下のように加工する 1）氏名を削除する 2）住所を削除、又は、○○県△△市に置き換える 3）生年月日を削除。又は、生年月に置き換える 2. 個人識別符号の削除 政令で定める以下のもの （1）生体情報（DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋）のデジタルデータで特定の個人を識別できるもの （2）旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー、各種保険証の番号等の公的機関が割り振る番号 3. 情報を相互に連結する符号の削除 事例）サービス会員の情報について、氏名等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、その管理用 ID を削除する。 4. 特異な記述等の削除 事例 1）症例数の極めて少ない病歴を削除する。 事例 2）年齢が「116 歳」という情報を「90 歳以上」に置き換える。 5. 個人情報データベース等の性質を踏まえたその他の措置 特定の個人の識別ができないようにするための匿名加工の手法 -項目削除、一般化、トップコーディング等 （別表参照）

下表には、先に挙げた事例に出てくる主な匿名加工の手法についてサマリーした。[45]

表5-2　匿名加工の主な手法

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。 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。 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。 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。

[45] 個人情報保護委員会事務局、匿名加工情報の加工基準について https://www.soumu.go.jp/main_content/000462276.pdf

手法名	解説
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）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。

（※）匿名加工情報の作成に当たっての一般的な加工手法を例示したものであり、その他の手法を用いて適切に加工することを妨げるものではない。

一般に、データを匿名化する際の処理の流れは、以下のようになる。[46]

① 利用用途の定義
② 対象データセットの選定
③ 対象データセットにおける識別子、準識別子、機密属性の定義
④ データセットの加工
⑤ （参考）ツールによる評価

上記処理の補足として、⑤の具体的なツールは、参考文献 [4]では、オープンソースのARX（https://arx.deidentifier.org/）といった匿名加工ツールを用いるとされているが、ARXは、主に研究者・技術者向けに用いられており、実務者が使うには一般的ではない。

また、匿名加工情報ツールは、表5-2の加工手法への対応の他、各ツール独自の機能や活用支援サービスと共に、いくつかの会社から提供されている。

各社からは、匿名加工情報ツールの機能の一部として、各種支援サービス（AIによる支援サービスや適切な活用に向けた支援サービスなど）などが行われているが、各事業者にとっては、匿名加工情報のスキル育成も重要な課題である。一般財団法人日本情報経済社会推進協会（JIPDEC）では、認定個人情報保護団体対象事業者を対象とした匿名加工情報の取り扱いに関する支援も行われており、今後、このような支援やガイドラインによるスキル育成の進展も期待される。

第2項　匿名加工情報に係る安全管理措置（第43条第2項、第6項、第46条関係）

ここでは、匿名加工情報に係る安全管理措置として、2.1 加工情報等情報の安全管理措置と2.2 匿名加工情報の安全管理措置について記載されている。

（a）加工情報等情報の安全管理措置

個人情報取扱事業者は、匿名加工情報を作成したときは、加工方法等情報の漏えいを防止するために、規則で定める基準に従い、必要な措置を講じなければならない。

当該措置の内容は、対象となる加工方法等情報が漏えいした場合における復元リスクの大きさを考慮し、当該加工方法等情報の量、性質等に応じた内容としなければならないが、具体的に講じなければならない項目及び具体例について、以下を参照いただきたい。

[46] 引用：ラクスエンジニアリングブログ、実際の匿名化：データ匿名化 第 6 回、2019 年 9 月
https://tech-blog.rakus.co.jp/entry/20190930/kamisen

表5-3 加工情報等情報の安全管理措置（抜粋）

項目 [該当条文]	事業者の対応	ガイドライン（補足）
加工方法等情報の安全管理措置 （第 36 条第 2 項）	個人情報取扱事業者は、匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号並びに加工の方法に関する情報の漏えいを防止するため、以下に挙げる個人情報保護委員会規則で定める基準（規則第 20 条の各号）に従い加工しなければならない。 1. 加工情報を取り扱う者の権限及び責任の明確化 2. 加工方法等情報の取扱いに関する規程類の整備等 3. 加工方法等情報を取り扱う正当な権限を有しない者による取扱いを防止するために必要かつ適切な措置	1. 加工情報を取り扱う者の権限及び責任の明確化 具体例） ・加工方法等情報の安全管理措置を講ずるための組織体制の整備 2. 加工方法等情報の取扱いに関する規程類の整備等 具体例） ・加工方法等情報の取扱いに係る規程等の整備とこれに従った運用 ・従業員の教育 ・加工方法等情報の取扱状況を確認する手段の整備 ・加工方法等情報の取扱状況の把握、安全管理措置の評価、見直し及び改善 3. 加工方法等情報を取り扱う正当な権限を有しない者による取扱いを防止するために必要かつ適切な措置 具体例） ・加工方法等情報を取り扱う権限を 有しない者による閲覧等の防止 ・機器、電子媒体等の盗難等の防止 ・電子媒体等を持ち運ぶ場合の漏えい等の防止 ・加工方法等情報の削除並びに機器、電子媒体等の廃棄 ・加工方法等情報へのアクセス制御 ・加工方法等情報へのアクセス者の識別と認証 ・外部からの不正アクセス等の防止 ・情報システムの使用に伴う加工方法等情報の漏えい等の防止

(b) 匿名加工情報の安全管理措置

個人情報取扱事業者又は匿名加工情報取扱事業者は、匿名加工情報の安全管理措置、苦情処理等の匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。第36条（第6項）では個人情報取扱事業者の第39条では匿名加工情報取扱事業者の安全管理措置について記載している。

表5-4 匿名加工情報の安全管理措置（抜粋）

項目 [該当条文]	事業者の対応	ガイドライン（補足）
匿名加工情報の安全管理措置等 （第 36 条第 6 項）	個人情報取扱事業者は、匿名加工情報の安全管理や適正な取扱いを確保するために必要な措置（苦情の処理等）等を自ら講じ、かつ、その内容を公表するよう努めなければならない。	当該安全管理等の措置については、個人情報と同様の取扱いを求めるものではないが、事業の性質、匿名加工情報の取扱状況、取り扱う匿名加工情報の性質、量等に応じて、合理的かつ適切な措置を講ずることが望ましい。
匿名加工情報の安全管理措置等 （第 39 条）	匿名加工情報取扱事業者は、匿名加工情報の安全管理や適正な取扱いを確保するために必要な措置（苦情の処理等）等を自ら講じ、かつ、その内容を公表するよう努めなければならない。	匿名加工情報には識別行為の禁止義務が課されていることから、匿名加工情報を取り扱う者が不適正な取扱いをすることがないよう、その情報が匿名加工情報である旨が一見して明らかな状態にしておくことが望ましい。

なお、安全管理措置の詳細については、個人情報保護全般について記載された以下の各条を参照頂きたい。

第23条： 安全管理措置
第24条： 従業者の監督
第25条： 委託先の監督
第40条： 個人情報の取扱いに関する苦情処理について

第3項 作成時の公表（第43条第3項関係）

表5-5 匿名加工情報作成時の公表（抜粋）

項目（該当条文）	事業者の対応	ガイドライン（補足）
匿名加工情報の作成時の公表 （第 43 条第 3 項）	個人情報取扱事業者は、匿名加工情報を作成したときは、個人情報保護委員会規則（規則第 21 条）で定めるところにより、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ない。 1 匿名加工情報を作成した後、遅滞なく、インターネットの利用その他の適切な方法により行う。 2 個人情報取扱事業者（A）が他の個人情報取扱事業者（B）の委託を受けて匿名加工情報を作成した場合は、（B）が公表する。また、当該公表により（A）が当該項目を公表したものとみなす。	【個人に関する情報の項目の事例】 事例）「氏名・性別・生年月日・購買履歴」のうち、氏名を削除した上で、生年月日の一般化、購買履歴から特異値等を削除する等加工して、「性別・生年・購買履歴」に関する匿名加工情報として作成した場合の公表項目は、「性別」、「生年」、「購買履歴」である。 「公表」とは、広く一般に自己の意思を知らせること（不特定多数の人々が知ることができるように発表すること）をいう。 また、ここでの「遅滞なく」とは、直後でなくても認められることを意味する。ただし、少なくともその利用又は第三者提供の前に、作成したことを一般に十分に知らせるに足る期間を確保しなければならない。許容される具体的な期間は、業種及びビジネスの態様によっても異なり得るため、個別具体的に判断する必要がある。

なお、公表に係る考慮点等の詳細については、個人情報保護全般について記載された以下を参照頂きたい。

第21条： 取得に際しての利用目的の通知等

第4項 匿名加工情報の第三者提供（第43条第4項、第44条関係）

個人情報取扱事業者又は匿名加工情報取扱事業者は、匿名加工情報を第三者に提供するときは（匿名加工情報をインターネット等で公開する場合も）、提供に当たりあらかじめ、インターネット等を利用し、匿名加工情報に含まれる個人に関する情報の項目や匿名加工情報の提供方法を公表するとともに、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を電子メール又は書面等により明示しなければならない。

また、上記の項目や加工方法が同じである匿名加工情報を復・継続的に第三者へ同じ方法により提供する場合には、最初に匿名加工情報を第三者提供するときに個人に関する項目を公表する際に、提供期間や又は継続的に提供されることとなる旨を明らかにしておくことにより、その後の公表は先の公表により行われたものと解される。

なお、第43条（第4項）は個人情報取扱事業者（作成者）に、第44条は匿名加工情報取扱事業者（受領者）についての法的要件を記載したものである。

表5-6 匿名加工情報の第三者提供（抜粋）

項目（該当条文）	事業者の対応	ガイドライン（補足）
匿名加工情報の第三者提供 （第 43 条第 4 項）	個人情報取扱事業者が、当該匿名加工情報を第三者に提供するときは、以下の対応が必要。 1. あらかじめ、第三者に提供され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その提供の方法について公表す	（1）第三者に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 事例）「氏名・性別・生年月日・購買履歴」のうち、氏名を削除した上で、生年月日の一般化、購買履歴から特異値等を削除する等加工して、「性別・生年・購買履歴」に関する匿名加工情報として作成して第三

	るとともに、当該第三者に対して、当該提供に係る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。 ※公表は、インターネットの利用等により行う。 2. 当該第三者に対して、当該提供に係る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。 ※明示は、電子メール送信、書面交付等により行う。	者提供する場合の公表項目は、「性別」、「生年」、「購買履歴」である。 (2)匿名加工情報の提供の方法 事例 1)ハードコピーを郵送 事例 2)第三者が匿名加工情報を利用できるようサーバにアップロード
匿名加工情報の第三者提供 (第 44 条)	匿名加工情報取扱事業者が、他者が作成した匿名加工情報を第三者に提供するときにも、上記、第 36 条(第 4 項)で定められた個人情報取扱事業者と同様の対応が求められる。	

第5項　識別行為の禁止(第43条第5項、第45条関係)

匿名加工情報を取り扱う場合には、当該匿名加工情報の作成の元となった個人情報の本人を識別する目的で、他の情報と照合したり加工方法等情報を取得してはならない

表5-7　識別行為の禁止(抜粋)

項目(該当条文)	事業者の対応	ガイドライン(補足)
識別行為の禁止 (第 43 条第 5 項)	個人情報取扱事業者は、個人情報に係る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。	【識別行為に当たらない取扱いの事例】 事例 1)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。 事例 2)匿名加工情報を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こと。 【識別行為に当たる取扱いの事例】 事例 1)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こと。 事例 2)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こと。
識別行為の禁止 (第 45 条)	匿名加工情報取扱事業者は、個人情報に係る本人を識別するために、当該個人情報から削除された記述や加工の方法に関する情報を取得したり、当該匿名加工情報を他の情報と照合したりしてはならない。	

第3節　まとめ

ここまで、現状の匿名加工情報に係る法的要件とその対応方法を記載してきたが、最後に2022年4月施行予定の改正法検討の中で挙げられた、データ利活用に関する施策の在り方について追記する。

匿名加工情報については、既に一定程度の活用が進みつつあるものの、「利用方法が分からない」、「自社　データへのニーズがあるのか分からない」、「分析するための人材がいない」等の意見がみられ、したがって、委員会として、具体的な利活用モデルやベストプラクティス等の発信を進めていくことが重要との認識になっている。[47]

これらの状況を踏まえ、令和2年 改正個人情報保護法では、仮名加工情報が新設された。仮名加工情報自身の説明と、これを含めた個人情報保護法に関連して定義されている情報に関する比較については、仮名加工情報の項を参照されたい。

[47]「個人情報保護法いわゆる 3 年ごと見直し制度改正大綱(2019 年 12 月 13 日)」p.21 他

第6章　仮名加工情報関連（第2条、第16条、第41条、第42条）

第1節　仮名加工情報に係る規定内容の概要

当節では、令和2年改正個人情報保護法（2022/4/1施行）において、データの利活用を推進するために新設された「仮名加工情報」について記載する。仮名加工情報は、図6-1に示すように、「他の情報と照合しない限り特定の個人を識別できないように加工された個人に関する情報」で、以下の特徴を有する。

・原則として事業者内部での利用に限定。利用目的の特定・公表により利用できる（利用目的の変更を本人の同意なく行うことが可能）

・匿名加工情報に比べて、加工しやすく、また、利用用途も広がり、様々な分析に活用できる

・個人の各種請求（開示・訂正等、利用停止等の請求）や漏えい時の報告への対応義務が緩和されている

前項でも記載した通り、個人情報保護法では、「個人情報の有用性」と「個人の権利利益の保護」のバランスを図ることを目指しているが、ここでは「個人情報の有用性」を推進するための方策として、イノベーションを促進する観点から、「仮名加工情報」が創設された。

個人情報保護法では、仮名加工情報に関連して、以下の8項目の内容を規定している。[48]

① 仮名加工情報の適正な加工（第41条第1項関係）
② 削除情報等の安全管理措置（第41条第2項関係）
③ 利用目的による制限・公表（第41条第3項・第4項関係）
④ 利用する必要がなくなった場合の消去（第41条第5項関係）
⑤ 第三者提供の禁止等（第41条第6項関係）
⑥ 識別行為の禁止（第41条第7項関係）
⑦ 本人への連絡等の禁止（第41条第8項関係）
⑧ 適用除外（第41条第9項関係）

本章では、上記の8項目のうち、特にポイントとなる事項について、個人情報の保護に関する法律についてのガイドライン（詳細は脚注48を参照のこと。以降、本章では単にガイドラインと記す）などを参考に概説・補足し、匿名加工情報との比較なども含め記載する。

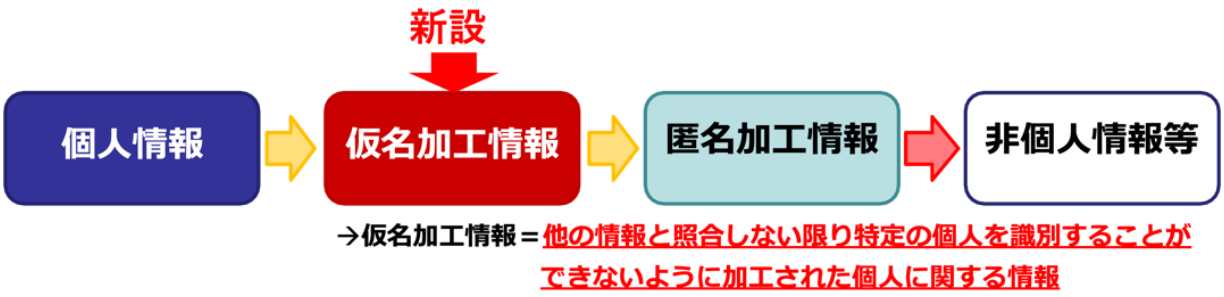


図6-1 仮名加工情報の位置づけ[49]

[48]「個人情報の保護に関する法律についてのガイドライン（仮名加工情報・匿名加工情報編）（2016/11 月）（2021 年 10 月一部改正）
https://www.ppc.go.jp/personalinfo/legal/guidelines_anonymous/#a2-2-2-2

[49] 引用：JIPDEC セミナー、抜け漏れ再チェック！全面施行直後、改正個人情報保護法の実務対応ポイント、2022 年 7 月 1 日

第2節　仮名加工情報に係る規定内容のポイント

①　仮名加工情報の適正な加工（第41条第1項関係）

・第41条（第1項）

個人情報取扱事業者は、仮名加工情報を作成するときは、他の情報と照合しない限り特定の個人を識別することができないようにするために必要なものとして個人情報保護委員会規則で定める基準に従い、個人情報を加工しなければならない。

（概説）

今回の改正で、「仮名加工情報」の概念が創設された。仮名加工情報とは、個人情報や個人識別符号について、図6-2に示すように、その一部を削除することや復元可能な規則性が無いよう置換することで、特定の個人を識別することができないよう加工した情報である。

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
（置換えの場合、元の記述を復元できる規則性を有しないこと）

図6-2 仮名加工情報の具体例[50]

規則第31条（＋ガイドライン）からは、図6-3の例のように加工方法が具体的に示されている。

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又は置換

事例 a）会員 ID、氏名、年齢、性別、サービス利用履歴が含まれる個人情報を加工する場合に次の措置を講ずる。
1）氏名を削除する
事例 b）氏名、住所、生年月日が含まれる個人情報を加工する場合に次の 1 から3 までの措置を講ずる。
1）氏名を削除する。
2）住所を削除する。又は、〇〇県△△市に置き換える。
3）生年月日を削除する。又は、日を削除し、生年月に置き換える。

※氏名の削除後、当該個人情報に含まれる他の記述等により、なお特定の個人を識別することができる場合には、当該記述等によって特定の個人を識別することができなくなるよう加工する必要がある。

② 個人情報に含まれる個人識別符号の全部を削除又は置換

⑥ 個人情報に含まれる記述等のうち、当該記述等が不正に利用されることにより、財産的被害が発生するおそれがあるものを削除又は置換

例：クレジットカード番号、送金や決済機能があるウェブサービスのID・パスワード等

図6-3 仮名加工情報の加工法の具体例[51]

[50] 引用：NTTデータ先端技術株式会社、改正個人情報保護法の概要、https://www.intellilink.co.jp/column/security/2021/082300.aspx
[51] 引用：JIPDECセミナー、抜け漏れ再チェック！全面施行直後、改正個人情報保護法の実務対応ポイント、2022年7月1日

より具体的な加工方法の例を図6-4に示す。同図に示すように、他の情報と照合しない限り特定の個人を識別できないように加工する(ここでは、氏名情報だけ加工している)。

■ 個人情報

取引ID	会員ID	氏名	日時	店舗ID	店舗名	担当者ID	商品ID	商品名	数量	価格	年齢
10032	224523	田中一郎	2016/8/2 18:25	KN013	みなとみらい店	101	151	王様のカフェラテ	1	132	46
10033	224523	田中一郎	2016/8/2 18:25	KN013	みなとみらい店	101	22	タマゴサンド	1	286	46
10034	225412	佐藤幸子	2016/10/4 7:13	CB002	西船橋駅前店	305	288	近江屋チョコレート(ホワイト)	4	209	46
10035	231622	鈴木博	2016/11/30 11:59	TK101	錦糸町店	211	793	バンドウクジラぬいぐるみ(大)	1	16500	46
10036	231622	鈴木博	2016/11/30 11:59	TK101	錦糸町店	211	151	王様のカフェラテ	1	132	46
10037	231622	鈴木博	2016/11/30 11:59	TK101	錦糸町店	211	22	タマゴサンド	1	286	46
10038	231622	鈴木博	2016/11/30 11:59	TK101	錦糸町店	211	287	近江屋チョコレート(ビター)	4	209	46
10039	225412	佐藤幸子	2016/12/10 1:58	MI301	溜池山王店	112	793	王様のカフェラテ	1	132	46
10040	224523	田中一郎	2016/12/10 5:55	KY023	横浜駅前店	104	151	王様のカフェラテ	1	132	46

■ 仮名加工情報

他の情報と照合しない限り特定の個人を識別できないように加工

取引ID	会員ID	氏名	日時	店舗ID	店舗名	担当者ID	商品ID	商品名	数量	価格	年齢
10032	224523	ABC	2016/8/2 18:25	KN013	みなとみらい店	101	151	王様のカフェラテ	1	132	46
10033	224523	ABC	2016/8/2 18:25	KN013	みなとみらい店	101	22	タマゴサンド	1	286	46
10034	225412	DEF	2016/10/4 7:13	CB002	西船橋駅前店	305	288	近江屋チョコレート(ホワイト)	4	209	46
10035	231622	GHI	2016/11/30 11:59	TK101	錦糸町店	211	793	バンドウクジラぬいぐるみ(大)	1	16500	46
10036	231622	GHI	2016/11/30 11:59	TK101	錦糸町店	211	151	王様のカフェラテ	1	132	46
10037	231622	GHI	2016/11/30 11:59	TK101	錦糸町店	211	22	タマゴサンド	1	286	46
10038	231622	GHI	2016/11/30 11:59	TK101	錦糸町店	211	287	近江屋チョコレート(ビター)	4	209	46
10039	225412	DEF	2016/12/10 1:58	MI301	溜池山王店	112	793	王様のカフェラテ	1	132	46
10040	224523	ABC	2016/12/10 5:55	KY023	横浜駅前店	104	151	王様のカフェラテ	1	132	46

図6-4 仮名加工情報の加工例(氏名情報だけ加工した場合の例)[52]

(匿名加工情報との比較)

従来の匿名加工情報と仮名加工情報を比較した場合、以下のように特徴づけられる。

- 匿名加工情報:「当該個人情報を復元することができないように加工したもの」
- 仮名加工情報:「他の情報と照合しない限り特定の個人を識別することができないよう加工したもの」

(補足)

仮名加工情報には、図6-5に示すように、「仮名加工情報(個人情報)」と、「仮名加工情報(非個人情報)」がある。

- 「仮名加工情報(個人情報)」とは、仮名加工情報の作成元となった個人情報や当該仮名加工情報に係る削除情報等を保有している等により他の情報と照合することで特定個人が識別できる状態にあるもので、これは個人情報の範疇に位置付けられる。
- 「仮名加工情報(非個人情報)」はその逆で、個人情報ではなく、匿名加工情報と同様に個人に関する情報の範疇に位置付けられる。

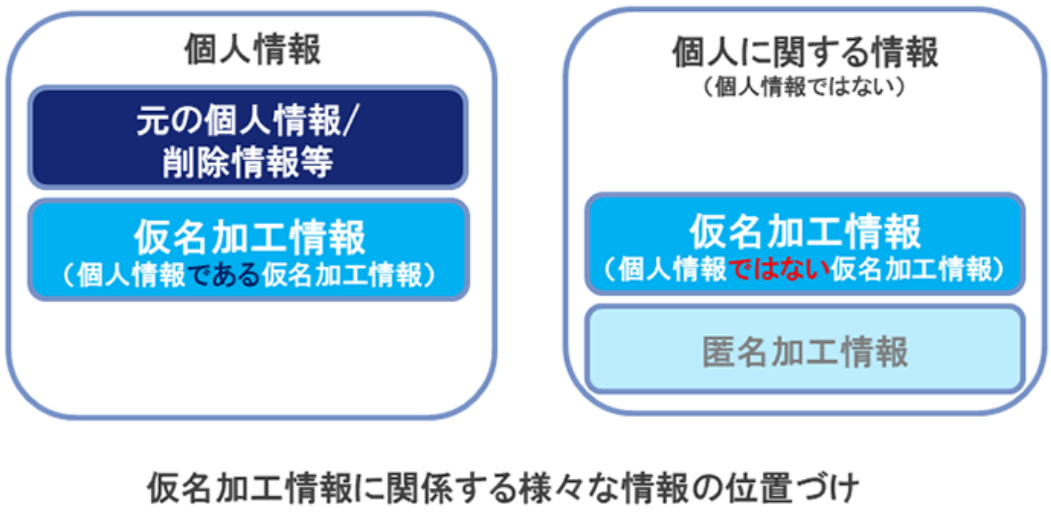


図6-5 仮名加工情報の具体例に関係する様々な情報の位置づけ[53]

[52] 引用:JIPDECセミナー、抜け漏れ再チェック!全面施行直後、改正個人情報保護法の実務対応ポイント、2022年7月1日

[53] 引用:NTT データ先端技術株式会社、改正個人情報保護法の概要、https://www.intellilink.co.jp/column/security/2021/082300.aspx

- 仮名加工情報と容易照合性

図6-6に示すように、仮名加工情報には、容易照合性の有無により、個人情報に位置付けられるものとそうでないものがある。容易照合性とは、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できるものである。

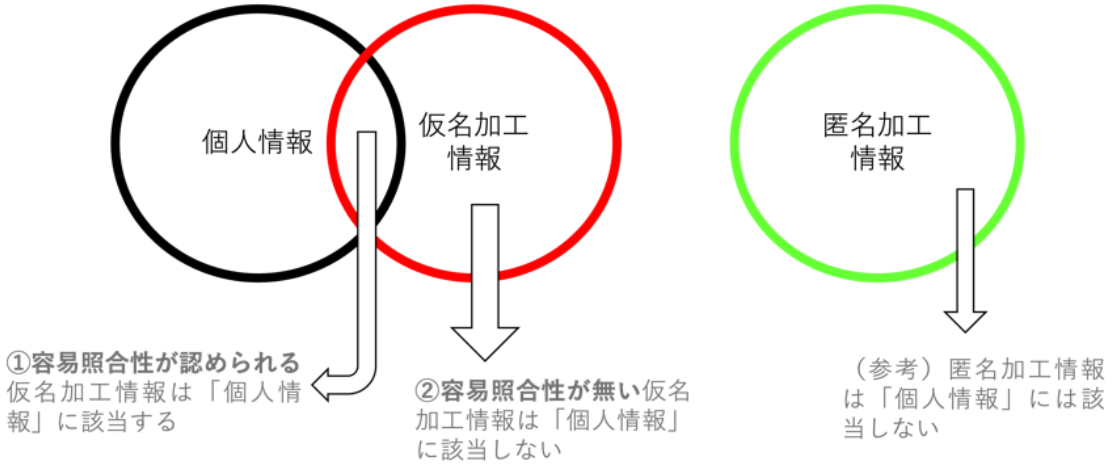


図6-6　個人情報と仮名加工情報、匿名情報との関係

②　削除情報等の安全管理措置（第41条第2項関係）

・第41条（第2項）

個人情報取扱事業者は、仮名加工情報を作成したとき、又は仮名加工情報及び当該仮名加工情報に係る削除情報等を取得したときは、削除情報等の漏えいを防止するために必要なものとして個人情報保護委員会規則で定める基準に従い、削除情報等の安全管理のための措置を講じなければならない。

（概説）

削除情報等の安全管理措置として、仮名加工情報に係る削除情報等の漏えいを防止するための安全管理措置を講じなければならない。

ここで、削除情報等とは、「仮名加工情報の作成に用いられた個人情報から削除された記述等及び個人識別符号並びに前項の規定により行われた加工の方法に関する情報」である。具体的には、氏名等を仮IDに置き換えた場合における置き換えアルゴリズムに用いられる乱数等のパラメータまたは氏名と仮IDの対応表等のような加工方法に関する情報が該当し、「氏名を削除した」というような復元につながらない情報は該当しない。

（引用：JIPDECセミナー、抜け漏れ再チェック！全面施行直後、改正個人情報保護法の実務対応ポイント、2022年7月1日）

③　利用目的による制限・公表（第41条第3項・第4項関係）

・第41条（第3項・第4項）

仮名加工情報取扱事業者（個人情報取扱事業者である者に限る。）は、第18条の規定にかかわらず、法令に基づく場合を除くほか、第17条第1項の規定により特定された利用目的の達成に必要な範囲を超えて、仮名加工情報（個人情報であるものに限る。）を取り扱ってはならない。

仮名加工情報についての第21条の規定の適用については、同条第1項及び第3項中「、本人に通知し、又は公表し」とあるのは「公表し」と、同条第4項第1号から第3号までの規定中「本人に通知し、又は公表する」とあるのは「公表する」とする。

（概説）

・利用目的の制限（ガイドラインより）

個人情報取扱事業者である仮名加工情報取扱事業者は、法令に基づく場合を除くほか、第17条第1項の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報である仮名加工情報を取り扱ってはならない。利用目的を変更した場合には、原則として変更後の利用目的を公表しなければならない。具体的には、図6-7の通り。

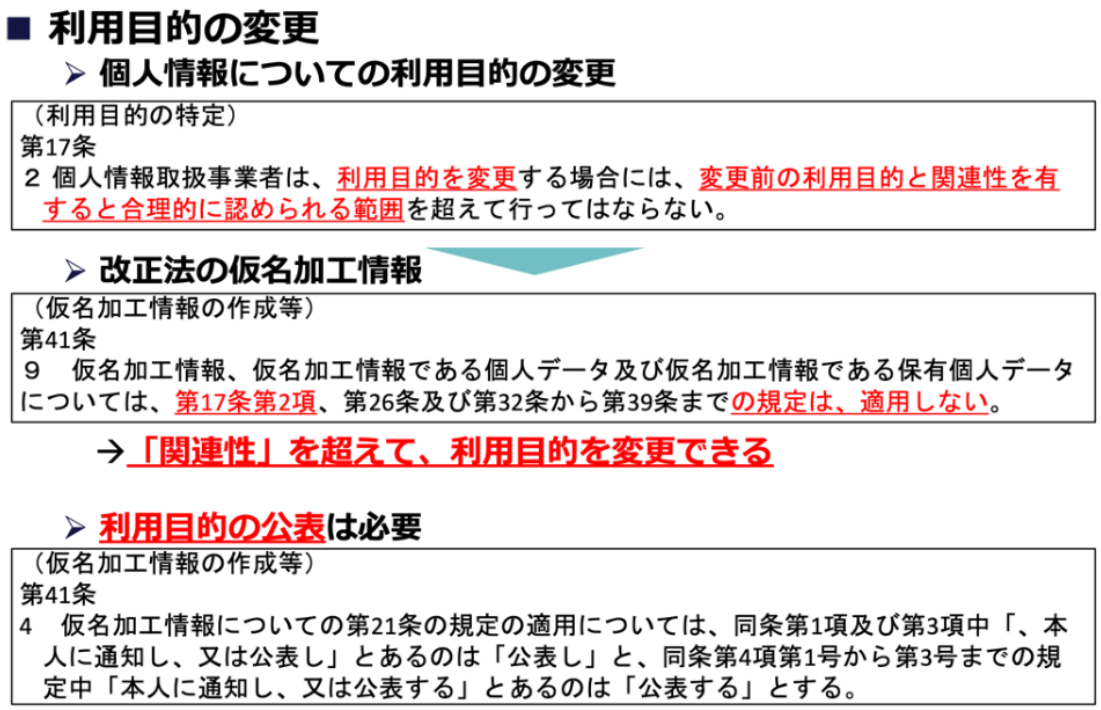


図6-7 仮名加工情報における利用目的の変更[54]

・利用目的の公表

通常の個人情報は、利用目的を本人への通知又は公表のいずれかの方法が必要とされるが、仮名加工情報は、公表のみで良い。

④ 利用する必要がなくなった場合の消去（第41条第5項関係）

・第41条（第5項）

仮名加工情報取扱事業者は、仮名加工情報である個人データ及び削除情報等を利用する必要がなくなったときは、当該個人データ及び削除情報等を遅滞なく消去するよう努めなければならない。この場合においては、第22条の規定は、適用しない。

（概説） ガイドラインより

個人情報取扱事業者である仮名加工情報取扱事業者は、保有する仮名加工情報である個人データについて利用する必要がなくなったとき、当該仮名加工情報である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。また、保有する削除情報等について利用する必要がなくなったときは、当該削除情報等を遅滞なく消去するように努めなければならない。

・具体的な事例1：仮名加工情報である個人データについて利用する必要がなくなったとき

[54] 引用：JIPDECセミナー、抜け漏れ再チェック！全面施行直後、改正個人情報保護法の実務対応ポイント、2022年7月1日

事例）新商品の開発のため、仮名加工情報である個人データを保有していたところ、当該新商品の開発に関する事業が中止となり、当該事業の再開の見込みもない場合

・具体的な事例2：削除情報等について利用する必要がなくなったとき

事例）仮名加工情報についての取扱いを終了し、新たな仮名加工情報を作成する見込みもない場合

⑤ 第三者提供の禁止等（第41条第6項関係）

⑥ 識別行為の禁止（第41条第7項関係）

⑦ 本人への連絡等の禁止（第41条第8項関係）

・第41条（第6項抜粋版）

仮名加工情報取扱事業者は、第27条第1項及び第2項並びに第28条第1項の規定にかかわらず、法令に基づく場合を除くほか、仮名加工情報である個人データを第三者に提供してはならない。

・第41条（第7項）

仮名加工情報取扱事業者は、仮名加工情報を取り扱うに当たっては、当該仮名加工情報の作成に用いられた個人情報に係る本人を識別するために、当該仮名加工情報を他の情報と照合してはならない

・第41条（第8項）

仮名加工情報取扱事業者は、仮名加工情報を取り扱うに当たっては、電話をかけ、郵便若しくは民間事業者による信書の送達に関する法律（平成14年法律第99号）第2条第6項に規定する一般信書便事業者若しくは同条第9項に規定する特定信書便事業者による同条第2項に規定する信書便により送付し、電報を送達し、ファクシミリ装置若しくは電磁的方法を用いて送信し、又は住居を訪問するために、当該仮名加工情報に含まれる連絡先その他の情報を利用してはならない。

（概説）

表6-1に示すように、仮名加工情報では、第三者提供の禁止、識別行為の禁止、本人への連絡等の禁止が定められている。

表6-1 仮名加工情報における禁止項目

禁止項目	概要
第三者提供の禁止	「仮名加工情報」は第三者に提供できない（ただし、法令によって第三者提供が認められている場合や、第三者提供に該当しないとされている場合には「仮名加工情報」を第三者にわたすことはできる）
識別行為の禁止	「仮名加工情報」を、特定の個人を識別するためにほかの情報と照合（照らし合わせる）ことは禁止されている
本人への連絡等の禁止	「仮名加工情報」を、情報の本人に連絡をとるなどの目的で利用することは禁止されている

⑧ 適用除外（第41条第9項関係）

・第41条（第9項）

仮名加工情報、仮名加工情報である個人データ及び仮名加工情報である保有個人データについては、第17条第2項、第26条及び第32条から第39条までの規定は、適用しない。

（概説） ガイドラインより

仮名加工情報（個人情報であるもの）、仮名加工情報である個人データ、仮名加工情報である保有個人データのそれぞれの取扱いは、表6-2に示すように規定が適用されない。

表6-2 適用除外の対象となる情報

情報	適用除外対象規定	内容
仮名加工情報(個人情報であるもの)	利用目的の変更(第 17 条第 2 項関係)	仮名加工情報(個人情報であるもの)は、利用目的の変更の制限に関する第 17 条第 2 項の規定は適用されないため、変更前の利用目的と関連性を有すると合理的に認められる範囲を超える利用目的の変更も認められる。
仮名加工情報である個人データ	漏えい等の報告等(第 26 条関係)	仮名加工情報である個人データについては、第 26 条の規定は適用されないため、仮名加工情報である個人データについて漏えい等が発生した場合でも、第 26 条に基づく報告や本人通知は不要である。
仮名加工情報である保有個人データ	本人からの開示等の請求等(第 32 条～第 39 条関係)	仮名加工情報である保有個人データについては、第 32 条から第 39 条までの規定は適用されないため、仮名加工情報である保有個人データについては、これらの規定に基づく本人からの開示等の請求等の対象とならない。

第3節 まとめ

本章では、令和2年 改正個人情報保護法にて新設された仮名加工情報について、その利用のためのポイントを記載してきた。個人情報を取り扱う組織として、仮名加工情報新設の趣旨や活用時のポイントと各種対応義務の緩和とそれでもなお存在するリスク等を踏まえたうえで、自社での運用を検討し、うまく活用していただきたい。なお、個人情報保護委員会から提供されている個人情報保護委員会事務局レポート[55]では、仮名加工情報について想定され得るユースケースや、情報の項目に応じて考慮すべき事項とリスクに対応した具体的な加工方法、利活用に当たり検討すべき事項等について紹介されているので参照されたい。

本章のまとめとして、表6-3に個人情報保護法に関連して定義されている、他の情報との比較表を記載する。これらの情報の違いを理解し、適材適所に活用することで、さらなる個人情報の活用を推進し、個人情報保護法が目指している、「個人情報の有用性」と「個人の権利利益の保護」のバランスを図り、個人情報保護と情報活用の両立を目指すことが肝要である。

また、一部の情報を削除あるいは分割する等の加工をする場合または個人情報から統計情報を作成する場合は、リスクを考慮して取り扱うことも忘れてはならない。

本章の記載が、新事業や新サービスの創出、国民生活の利便性の向上に向けた個人情報の有効活用の一助となれば幸いである。

表6-3 個人情報関連情報の比較

情報	情報の定義	取り扱い	使い方
個人情報	生存する個人に関する情報であって、特定の個人を識別できるもの	個人情報の取得に際しては、利用目的を特定し、本人の同意を得る等の対応が必要[56]	以下の事例にように、利用目的を具体的に特定する必要がある 事例) ○○事業における商品発送、関連するアフターサービス、新商品に関する情報のお知らせのため
仮名化情報	氏名等特定の個人を直接識別できる記述を置き換える又は削除することで、加工後のデータ単体から特定の個人を識別できないよう加工した情報	・利用目的の変更を本人の同意なく 行うことが可能 ・万が一漏えい等が生じた場合であっても、報告等を行う必要がない	匿名加工情報や統計情報と比べて個人ごとの特徴を詳細に残して加工することができるため、より詳細な分析を比較的簡便な加工方法で実施できる ①事業者が持つ一つ一つのデータベースに含まれる個人情報を仮名加工情報に加工し利用目的を変更する事例 ②事業者が持つ複数のデータベースに含まれる個人情報からそれぞれ仮名加工情報を作成し利用目的を変更したうえで同一の個人ごとに突合して利用する事例

[55]「個人情報保護委員会事務局レポート 仮名加工情報・匿名加工情報信頼ある個人情報の利活用に向けて ―事例編―(2022 年 3 月)(2022 年 5 月更新)」

匿名化情報	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、復元できないようにしたもの	本人の同意を得ることなく目的外利用及び第三者提供を可能とすることにより、事業者間におけるデータ取引・連携を含むパーソナルデータ利活用を促進	新事業や新サービスの創出、ひいては、国民生活の利便性の向上が期待される以下のような事例 ①ポイントカードの購買履歴や交通系 IC カードの乗降履歴等を複数事業者間で分野横断的に利活用することにより、新たなサービスやイノベーションを生み出す可能性 ②医療機関が保有する医療情報を活用した創薬・臨床分野の発展や、カーナビ等から収集される走行位置履歴等のプローブ情報を活用したより精緻な渋滞予測や天候情報の提供等により、国民生活全体の質の向上に寄与する可能性
統計情報	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データ	統計情報の作成において、ある項目の値を所定範囲ごとに区切る場合、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	集団の傾向又は性質などを数量的に把握

第7章　域外適用（第166条）

域外適用の強化[57]により、日本国内にある者に係る個人情報等を取り扱う外国事業者についても、国内事業者と同様に、罰則によって担保された報告徴収・命令の対象となった。

以下の通り、ガイドラインにて「域外適用の対象となる事例」および「域外適用の対象とならない事例」を挙げている。

【域外適用の対象となる事例】

- 外国のインターネット通信販売事業者が、日本の消費者に対する商品の販売・配送に関連して、日本の消費者の個人情報を取り扱う場合
- 外国のメールサービス提供事業者が、日本の消費者に対するメールサービスの提供に関連して、日本の消費者の個人情報を取り扱う場合
- 外国のホテル事業者が、日本の消費者に対する現地の観光地やイベント等に関する情報の配信等のサービスの提供に関連して、日本にある旅行会社等から提供を受けた日本の消費者の個人情報を取り扱う場合
- 外国の広告関連事業者が、日本のインターネット通信販売事業者に対し、当該インターネット通信販売事業者による日本の消費者に対するキャンペーン情報の配信等のサービスの提供に関連して、当該インターネット通信販売事業者が保有する日本の消費者の個人データと結び付けることが想定される個人関連情報を提供する場合
- 外国のアプリ提供事業者が、日本の消費者に対するサービスの提供に関連して、新サービスの開発のために、日本の消費者の個人情報を用いて作成された仮名加工情報を取り扱う場合
- 外国のインターネット通信販売事業者が、日本の消費者に対する商品の販売又はサービスの提供に関連して、傾向分析等を行うために、日本の消費者の個人情報を用いて作成された匿名加工情報を取り扱う場合

【域外適用の対象とならない事例】

- 外国にある親会社が、グループ会社の従業員情報の管理のため、日本にある子会社の従業員の個人情報を取り扱う場合
  - 日本にある子会社が外国にある親会社に対して従業員の個人データを提供するためには、第 28 条に従い、本人の同意を取得するなど外国にある第三者に個人データを提供するための措置を講ずる必要がある。

[57] 第 166 条、ガイドライン（通則編）8（域外適用）

第8章　罰則（第19条、第173条、第177条、第179条）

第1節　不適正な利用の禁止（第19条）

今回の改正では個人情報保護法第19条において、個人情報取扱事業者について個人情報の不適正な利用の禁止が定められた。

旧法では、個人情報の不適正な利用の禁止、つまり、違法・不当な行為を助長・誘発するおそれがある方法によって個人情報を利用することが、明文で禁止されていませんでした。そのため、旧個人情報保護法の規定に照らして違法ではないとしても、違法又は不当な行為を助長し、又は誘発するおそれのある方法により個人情報を利用するなど、本法の目的である個人の権利利益の保護に照らして、適切でない方法で個人情報が利用されている事例が存在しました。このような背景から、今回の改正では、個人情報取扱事業者が不適正な方法で個人情報を利用することが禁止されました。不適正な方法で個人情報を利用した場合、利用停止等（個人情報保護第30条）の対象になります。

法の記載は以下の通りである。

> 第19条 個人情報取扱事業者は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない。

個人情報保護委員会のリーフレットでは以下のような図（図8-1）で表している。[58]

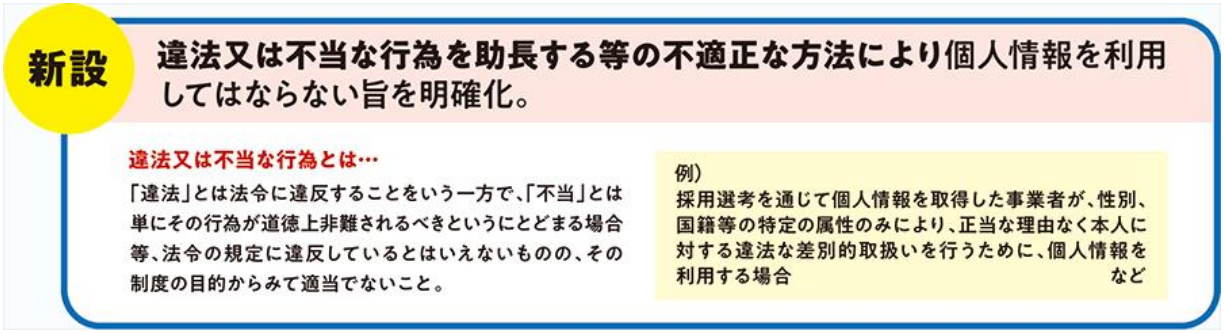


図8-1

個人情報保護委員会では下記の通り事例を示している[59]。

【個人情報取扱事業者が違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用している事例】

事例1. 違法な行為を営むことが疑われる事業者（例：貸金業登録を行っていない貸金業者等）からの突然の接触による本人の平穏な生活を送る権利の侵害等、当該事業者の違法な行為を助長するおそれが想定されるにもかかわらず、当該事業者に当該本人の個人情報を提供する場合

事例2. 裁判所による公告等により散在的に公開されている個人情報（例：官報に掲載される破産者情報）を、当該個人情報に係る本人に対する違法な差別が、不特定多数の者によって誘発されるおそれがあることが予見できるにもかかわらず、それを集約してデータベース化し、インターネット上で公開する場合

事例3. 暴力団員により行われる暴力的要求行為等の不当な行為や総会屋による不当な要求を助長し、又は誘発するおそれが予見できるにもかかわらず、事業者間で共有している暴力団員等に該当する人物を本人とする個人情報や、不当要求による被害を防止するために必要な業務を行う各事業者の責任者の

[58] 参考文献：改正個人情報保護法　特集 ｜個人情報保護委員会不適正利用の禁止
https://www.ppc.go.jp/news/kaiseihou_feature/#futekisei
[59] 参考文献：個人情報の保護に関する法律についてのガイドライン（通則編）
https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a3-2

名簿等を、みだりに開示し、又は暴力団等に対しその存在を明らかにする場合

事例4. 個人情報を提供した場合、提供先において第 27 条第 1 項に違反する第三者提供がなされることを予見できるにもかかわらず、当該提供先に対して、個人情報を提供する場合

事例5. 採用選考を通じて個人情報を取得した事業者が、性別、国籍等の特定の属性のみにより、正当な理由なく本人に対する違法な差別的取扱いを行うために、個人情報を利用する場合

事例6. 広告配信を行っている事業者が、第三者から広告配信依頼を受けた商品が違法薬物等の違法な商品であることが予見できるにもかかわらず、当該商品の広告配信のために、自社で取得した個人情報を利用する場合

以上、個人情報取扱事業者は、違法又は不当な行為（※1）を助長し、又は誘発するおそれ（※2）がある方法により個人情報を利用してはならない。

（※1）「違法又は不当な行為」とは、法（個人情報の保護に関する法律）その他の法令に違反する行為、及び直ちに違法とはいえないものの、法（個人情報の保護に関する法律）その他の法令の制度趣旨又は公序良俗に反する等、社会通念上適正とは認められない行為をいう。

（※2）「おそれ」の有無は、個人情報取扱事業者による個人情報の利用が、違法又は不当な行為を助長又は誘発することについて、社会通念上蓋然性が認められるか否かにより判断される。この判断に当たっては、個人情報の利用方法等の客観的な事情に加えて、個人情報の利用時点における個人情報取扱事業者の認識及び予見可能性も踏まえる必要がある。例えば、個人情報取扱事業者が第三者に個人情報を提供した場合において、当該第三者が当該個人情報を違法な行為に用いた場合であっても、当該第三者が当該個人情報の取得目的を偽っていた等、当該個人情報の提供の時点において、提供した個人情報が違法に利用されることについて、当該個人情報取扱事業者が一般的な注意力をもってしても予見できない状況であった場合には、「おそれ」は認められないと解される。

第2節　措置命令・報告義務違反の罰則について法定刑を引き上げ（第173条、第177条）

個人情報の保護に関する法律等の一部を改正する法律の一部施行に伴い、令和2年12月12日から個人情報の保護に関する法律（個人情報保護法）の法定刑が引上げられた。

なお、施行日以前の行為に対する罰則の適用については、改正前の個人情報保護法の規定が適用される。

主な変更点は以下の2点である（※1）

- ✓ 委員会による命令違反・委員会に対する虚偽報告等の法定刑が引き上げ
- ✓ 命令違反等の罰金について、法人に対しては行為者よりも罰金刑の最高額が引き上げ

以下に改正前との比較のために新旧比較表（表8-1）を記載する。

表8-1

改正後	改正前
第 173 条　第百四十五条第二項又は第三項の規定による命令に違反し た場合には、当該違反行為をした者は、1 年以下の懲役又は 100 万円以下の罰金に処する。	第 82 条 【新設】
（削除）	第 84 条 第 42 条第 2 項又は第 3 項の規定による命令に違反し た者は、6 月以下の懲役又は 30 万円以下の罰金に処する。
第 174 条 次の各号のいずれかに該当する場合には、当該違反行為をした者は、50 万円以下の罰金に処する。 一 第 40 条第 1 項の規定による報告若しくは資料の提出をせ ず、若しくは虚偽の報告をし、若しくは虚偽の資料を提出し、又は当該職員の質問に対して答弁をせず、若しくは虚偽	第 85 条 次の各号のいずれかに該当する者は、30 万円以下の罰金に処する。 一 第 40 条第 1 項の規定による報告若しくは資料の提出をせ ず、若しくは虚偽の報告をし、若しくは虚偽の資料を提出

の答弁をし、若しくは検査を拒み、妨げ、若しくは忌避したとき。 二 第 56 条の規定による報告をせず、又は虚偽の報告をしたとき。 る。 第 182 条 次の各号のいずれかに該当する者は、10 万円以下の過料に処する。 一 第 26 条第 2 項(第 26 条の 2 第 3 項において準用する場合を含む。)又は第 55 条の規定に違反した者	し、又は当該職員の質問に対して答弁をせず、若しくは虚偽の答弁をし、若しくは検査を拒み、妨げ、若しくは忌避した者 二 第 56 条の規定による報告をせず、又は虚偽の報告をした者。 第 88 条 次の各号のいずれかに該当する者は、10 万円以下の過料に処する。 一 第 26 条第 2 項又は第 55 条の規定に違反した者

第3節　法人に対する罰金刑を引き上げ(第179条)

今般の改正では、法人の代表者又は法人若しくは人の代理人、使用人その他の従業者(以下本項において「従業者等」という。)がその法人又は人の業務に関して罰則の対象となる行為を行った場合には、行為者に加え、その法人や人にも罰金刑が科されることになった。

以下に改正前との比較のために新旧比較表(表8-2)を記載する。

表8-2

改正後	改正前
第 179 条 法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、次の各号に掲げる違反行為をしたときは、行為者を罰するほか、その法人に対して当該各号に定める罰金刑を、その人に対して各本条の罰金刑を科する。 一 第 173 条及び第 174 条 1 億円以下の罰金刑 二 第 177 条 同条の罰金刑	第 87 条 法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、第 83 条から第 85 条までの違反行為をしたときは、行為者を罰するほか、その法人又は人に対しても、各本条の罰金刑を科する。 (新設) (新設)

第4節　罰則の改正まとめ

第1項　個人情報保護委員会の見解

今般の改正における「罰則」について個人情報保護委員会では「ペナルティの在り方」、「改訂前後の法定刑の比較」、「罰金対象の事例」及び「FAQ」を以下の通り示している(図8-2、参考文献3)。

【ペナルティの在り方】

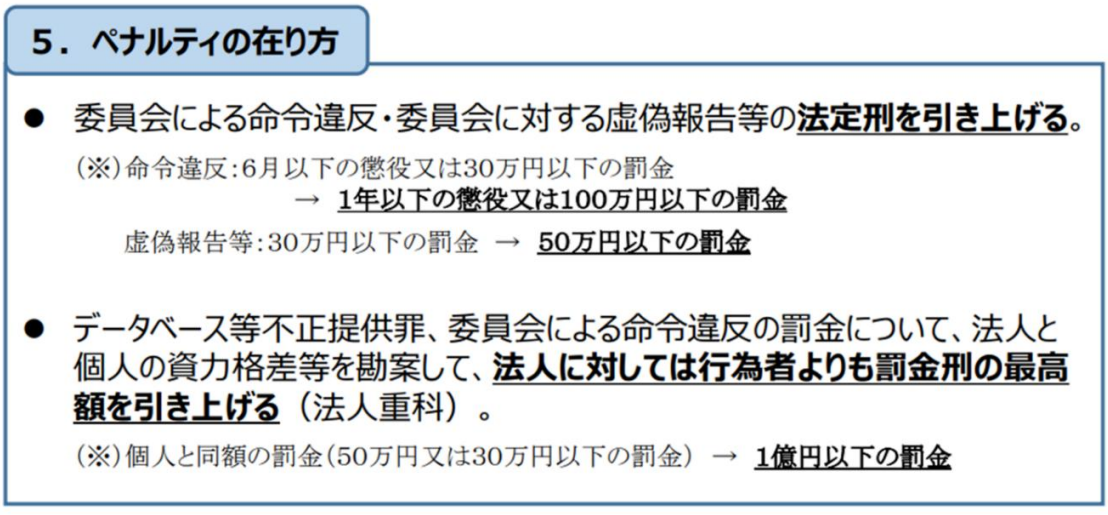


図8-2 (参考文献3)個人情報の保護に関する法律等の一部を改正する法律(概要)から抜粋[60]

[60] 引用:https://www.ppc.go.jp/files/pdf/200612_gaiyou.pdf

改正前後の法定刑の比較(表8-3)

表8-3　令和2年 改正個人情報保護法について[61]

		懲役刑		罰金刑	
		改正前	改正後	改正前	改正後
個人情報保護委員会からの命令への違反	行為者	6月以下	**1年以下**	30万円以下	**100万円以下**
	法人等	-	-	30万円以下	**1億円以下**
個人情報データベース等の不正提供等	行為者	1年以下	1年以下	50万円以下	50万円以下
	法人等	-	-	50万円以下	**1億円以下**
個人情報保護委員会□への虚偽報告等	行為者	-	-	30万円以下	**50万円以下**
	法人等	-	-	30万円以下	**50万円以下**

【罰金対象の事例】 - 個人情報取扱事業者が不正の手段により個人情報を取得 –

表8-4　個人情報の保護に関する法律についてのガイドライン（通則編）P.35-36　から抜粋[62]

事例 1)	十分な判断能力を有していない子供や障害者から、取得状況から考えて関係のない家族の収入事情などの家族の個人情報を、家族の同意なく取得する場合
事例 2)	第 23 条第 1 項に規定する第三者提供制限違反をするよう強要して個人情報を取得する場合
事例 3)	個人情報を取得する主体や利用目的等について、意図的に虚偽の情報を示して、本人から個人情報を取得する場合
事例 4)	他の事業者に指示して不正の手段で個人情報を取得させ、当該他の事業者から個人情報を取得する場合
事例 5)	第 23 条第 1 項に規定する第三者提供制限違反がされようとしていることを知り、又は容易に知ることができるにもかかわらず、個人情報を取得する場合
事例 6)	不正の手段で個人情報が取得されたことを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合

【FAQ索引】

Q11-1 個人情報取扱事業者等が個人情報保護法に違反した場合、どのような措置が採られるのですか。
A11-1 個人情報取扱事業者、個人関連情報取扱事業者、仮名加工情報取扱事業者又は匿名加工情報取扱事業者(以下「個人情報取扱事業者等」という。)が、個人情報保護法の義務規定に違反し、不適切な個人情報、個人関連情報、仮名加工情報又は匿名加工情報(以下本項において「個人情報等」という。)の取扱いを行っている場合には、個人情報保護委員会は、必要に応じて、当該個人情報取扱事業者等その他の関係者に対して報告徴収・立入検査を実施し(第 143 条)(※)、当該個人情報取扱事業者等に対して指導・助言を行い(第 144 条)、また、勧告・命令を行う(第 145 条)ことができます。

[61] 引用:https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/
[62] 引用:https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000223339

個人情報保護委員会からの報告徴収・立入検査に応じなかった場合や、報告徴収に対して虚偽の報告をした場合等には、刑事罰（50 万円以下の罰金）が科される可能性があります（第 177 条）。また、個人情報保護委員会の命令に個人情報取扱事業者等が違反した場合には、個人情報保護委員会は、その旨を公表することができ（第 145 条第 4 項）、加えて、当該命令に違反した者には、刑事罰（1年以下の懲役又は 100 万円以下の罰金）が科される可能性があります（第 173 条）。

なお、個人情報取扱事業者若しくはその従業者又はこれらであった者が、その業務に関して取り扱った個人情報データベース等（その全部又は一部を複製し、又は加工したものを含む。）を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときは、刑事罰（1年以下の懲役又は 50 万円以下の罰金）が科される可能性があります（第 174 条）。

さらに、法人の代表者又は法人若しくは人の代理人、使用人その他の従業者（以下本項において「従業者等」という。）がその法人又は人の業務に関して、上記の罰則の対象となる行為を行った場合には、両罰規定により、行為者に加え、その法人や人にも罰金刑が科される可能性があります（第 179 条）。

具体的には、従業者等が法人の業務に関して、①第 173 条又は第 174 条に掲げる違反行為を行った場合、当該法人には、1億円以下の罰金刑が科される可能性があり、②第 177 条に掲げる違反行為を行った場合、当該法人には 50 万円以下の罰金刑が科される可能性があります。また、従業者等が人の業務に関して、第 173 条、第 174 条及び第 177 条に掲げる違反行為を行った場合には、当該人に対して、当該違反行為を定める各条文に規定する罰金刑が科される可能性があります。

（※）第147条に基づく権限の委任が行われた場合には、事業所管大臣（各省庁）も報告徴収・立入検査を実施する権限を有することとなります。[63]

第2項　過去事例

過去、日本において「罰則」に係わる事例が発生している。所謂「内定辞退予測サービス「リクナビ問題」」及び「不適切な国外データ保存（LINE問題）」が発生している。

リクナビ問題は、令和元年（2020年）8月、個人情報保護委員会が初めての勧告を行った事案である。それまでは個人情報保護委員会が漏えい等報告を受けた事案や報告徴収・立入検査を行った事案の数は増加傾向にあった。この事案は、当時は個人情報保護委員会からの指導等により違法状態が是正された。

第3項　罰則効果と課題

リクナビ問題以前には勧告・命令及び罰則については、新法の中間整理公表時点での適用事例は存在しなかった。また、個人情報保護法の改訂では、罰則を違反行為に対する最終的な実効性確保の手段とし、法人に対してもいわゆる両罰規定を設けていた。しかし、罰金刑の効果は刑罰を科せられる者の資力によって大きく異なる。なので、法人に対して行為者と同額の罰金を科したとしても、罰則として十分な抑止効果が期待できないことも詳らかになった事案であると言える。なので、今般の法改正における法人処罰規定に係る重科の導入を含め、必要に応じた見直しを行う切っ掛けとなったと言える。

一方、課題も明確になってきている。主な課題は下記2点である。

① 安全管理措置義務違反などのように、違反行為があっても利得が発生していない場合があり、課徴金による抑止がなじまないケースが多い。
② 諸外国の個人情報保護法制においては違反行為に対して高額の制裁金を課すことによって規制の実効性を確保している例がある（GDPR の制裁金）。また、今般の罰金引き上げ（1 億円）では効果が薄いのではないか？との疑問が呈されている。

上記2点の課題に対して、現時点では個人情報保護法違反による罰金の執行事例もない。これを踏まえて、今回の改正においては罰則の強化は法定刑の引上げにより対処することとしている。しかし課徴金制度の導入は行っていない。なので、今後は課徴金制度の導入については、我が国の法体系、執行の実績と効果、国内外事業者の実態、国際的な動向を踏まえつつ、引き続き検討を行っていくものとされている。

第4項　GDPRにおける罰則の比較

海外における個人情報取り扱い規定としてGDPRを例に、今般の改正法における罰則強化の効果を比較評

[63] 引用：https://www.ppc.go.jp/all_faq_index/faq1-q11-1/（令和4年4月更新）

価する。以下、GDPRについての記述は「日本貿易振興機構（ジェトロ）ブリュッセル事務所　海外調査部 欧州ロシア CIS 課」が纏めた資料を引用させて頂いている。

GDPRでは少なくとも1,000万ユーロ（約12億円）、義務違反のケースによっては2,000万ユーロ（約23億円）が制裁金の最低額として設けられており、事業規模によってはさらに多くの支払いを要求される。それに比して日本での改正法罰金（1億円）は金額的に効果が期待できるか？が問題視されている（上記項番3ご参照）。

GDPRの制裁金の上限は、二つの類型があり、のいずれかとなります。

① 前事業年度の企業の全世界年間売上高の 4%以下または 2000 万ユーロのいずれか高い方(第 83 条(5))
② 前事業年度の企業の全世界年間売上高の 2%以下または 1000 万ユーロのいずれか高い方(第 83 条(4))

表8−5

制裁金の上限額の基準	義務違反の類型
企業の全世界年間売上高の 4%、または、2,000 万ユーロのいずれか高い方(第 83 条(5))	● 個人データの処理に関する原則を遵守しなかった場合(第 5 条) ● 適法に個人データを処理しなかった場合(第 6 条) ● 同意の条件を遵守しなかった場合(第 7 条) ● 特別カテゴリーの個人データ処理の条件を遵守しなかった場合(第 9 条) ● データ主体の権利およびその行使の手順を尊重しなかった場合(第 12-22 条) ● 個人データの移転の条件に従わなかった場合(第 44-49 条) ● 監督機関の命令に従わなかった場合(第 58 条(1)および(2))
企業の全世界年間売上高の 2%、または、1,000 万ユーロのいずれか高い方(第 83 条(4))	● 16 歳未満の子どもに対する直接的な情報社会サービスの提供に関する個人データの処理には、子に対する保護責任を持つ者による同意または許可が必要という条件に従わなかった場合(第 8 条) ● GDPR 要件を満たすために適切な技術的・組織的な対策を実施しなかった、またはそのような措置を実施しない処理者を利用した場合(第 25 条、第 28 条) ● EU 代理人を選任する義務を怠った場合(第 27 条) ● 責任に基づいて処理行為の記録を保持しない場合(第 30 条) ● 監督機関に協力しない場合(第 31 条) ● リスクに対する適切なセキュリティレベルを保証する適切な技術的・組織的な対策を実施しなかった場合(第 32 条) ● セキュリティ違反を監督機関に通知する義務を怠った場合(第 33 条)、データ主体に通知しなかった場合(第 34 条) ● 影響評価を行なわなかった場合(第 35 条) ● 影響評価によってリスクが示されていたにも関わらず、処理の前に監督機関に助言を求めなかった場合(第 36 条) ● データ保護責任者（DPO）*を選任しなかった場合、または、その職や役務を尊重しなかった場合(第 37～39 条)

少なくとも1,000万ユーロ（約12億円）、義務違反のケースによっては2,000万ユーロ（約23億円）が制裁金の最低額として設けられており、事業規模によってはさらに多くの支払いを要求されます。

GDPRに違反する最大のリスクは、こうした制裁金の大きさだといえる。

以下に、過去、GDPRの違反を指摘されてICOから制裁金支払いの通告を受けた事例をご紹介する。

【事例①】 Marriott International：制裁金9,920万396ポンド（約135億円）

ホテル事業を営む大手企業Marriott International社は、約3億3,900万件の個人情報を流出させたことでICOから9,920万396ポンド（約135億円）の制裁金を科せられています。

この大規模な情報流出は、Marriott International社が買収したStarwood社のシステムに起因するものです

が、Starwood社の買収時に十分なデューデリジェンス（買収先企業の精査）を実行していなかったものと判断し、Marriott International社が制裁対象となりました。

【事例②】 British Airways：制裁金1億8,339万ポンド（約250億円）

約50万人の顧客データを漏えいさせたとして、航空事業を営むBritish Airways社はICOから制裁金1億8,339万ポンド（約250億円）を科す旨の通告を受けました。British Airways社の不完全なセキュリティ対策により氏名や住所、カード決済や予約内容が流出したものです。

ここ挙げたMarriott International社とBritish Airways社に科せられた制裁金が、GDPRに違反したもののうち特に高額な事例として認知されています。

【事例③】 Google：制裁金5,000万ユーロ（約62億円）

大手IT企業であるGoogleは、個人情報の利用目的がユーザーへ明確に提示されていないこと、およびユーザーの同意を一括取得していたことがGDPRに抵触するとして、フランスのデータ保護機関であるCNILから5,000万ユーロ（約62億円）の制裁金を科せられました。

ユーザーが個人情報にまつわる確認・変更を行うにあたり、目的を果たすまでの操作が煩雑である点が主に問題であると指摘されています。

【参考資料】
「「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）」
（日本貿易振興機構（ジェトロ）ブリュッセル事務所　海外調査部 欧州ロシア CIS 課）
https://www.jetro.go.jp/ext_images/_Reports/01/dcfcebc8265a8943/20160084.pdf
https://www.iij.ad.jp/global/column/column47-2.html
https://privtech.co.jp/blog/law/gdpr-ico.html