

29-J003

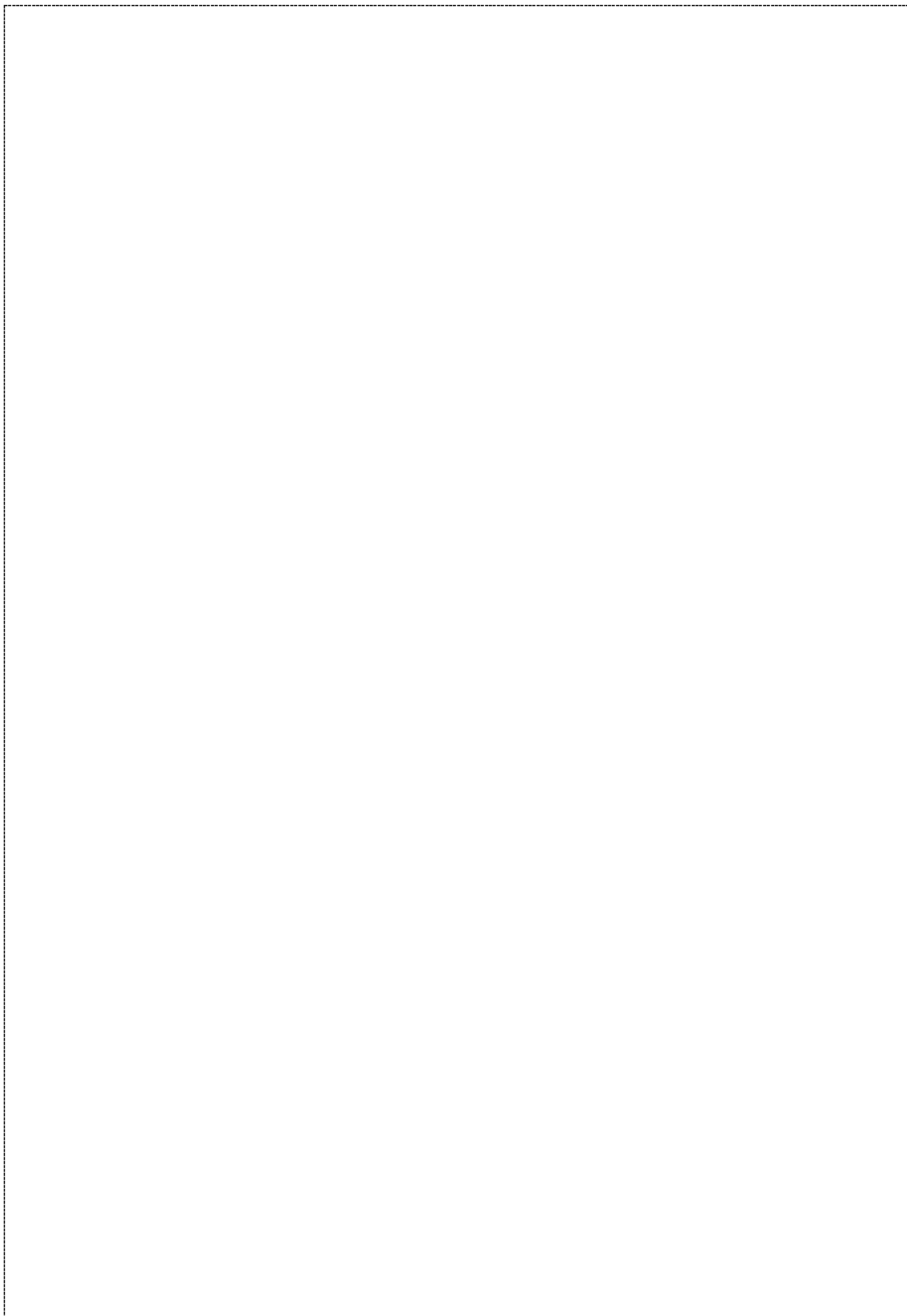
平成 29 年度  
個人情報保護タスクフォースレポート

**改正個人情報保護法  
情報サービス事業者における実務上の留意点**  
～こんなときどうする？確認のためのケーススタディ～

平成 30 年 5 月

一般社団法人 情報サービス産業協会

個人情報保護タスクフォース



## はじめに

平成 29 年 5 月 30 日に、改正された「個人情報の保護に関する法律(ここでは改正個人情報保護法といいます。)」が全面的に施行されました。改正個人情報保護法は、個人情報の定義の明確化、個人情報の有用性を確保(利活用)するための整備、個人情報の保護の強化(いわゆる名簿屋対策)等の観点から見直しがなされており、個人情報の保護と利活用の促進のバランスに配慮したものとなっております。この見直しを受けて、情報サービス産業においても従前の対応を見直していくとともに、この法律の趣旨を踏まえた、より適切な対応を行っていく必要があります。

本書は、改正個人情報保護法の施行を受け、情報サービス産業の皆様の実務で、わかりにくいけれども対応しなければならないポイントに焦点を絞り、ユースケースを設定して分かりやすく整理したものです。

具体的には、JISA 会員企業を主に個人情報の取扱いを受託する者＝委託先と想定して、「個人情報のライフサイクル」と「委託元との関係」の2つの観点から、法律やガイドラインの表現が曖昧で対応に迷うケースに焦点を当てて、実務上判断する際の参考情報を提供することを意識して作成しております。また「委託元との関係」では、「委託元と委託先との間の関係で対応しなければならない事項」と「委託先の中で対応しなければならない事項」の観点も加えています。なお、特に迷いやすいケースに絞ったため、実務上ありうるすべての事項を網羅したものではなく、ケースの中にはここで挙げた事項のほかに考慮すべき観点もあることにも留意する必要があります。

本書の内容が、改正個人情報保護法に基づいて業務を行う、JISA 会員企業の皆さまの一助となれば幸いです。

平成 30 年 5 月

一般社団法人情報サービス産業協会  
個人情報保護タスクフォース  
座長(株式会社 NTT データ)  
土屋 茂樹

## 目次

|                                                                                     |    |
|-------------------------------------------------------------------------------------|----|
| 1. 個人情報取り扱いのライフサイクルでの留意事項 .....                                                     | 1  |
| 1.1. 個人情報の定義.....                                                                   | 2  |
| ケース 1 「顧客から受領したテストデータに個人データが含まれていた、顧客自身はテストデータの当該情報を個人情報と認知していなかった」 .....           | 3  |
| ケース 2 「別々に受領したデータであったが、特定の属性データを照合すれば個人が特定できることがわかった」 .....                         | 5  |
| 1.2. 個人情報の取得.....                                                                   | 8  |
| ケース 3 「マスキングが不十分なデータをダミーデータとして受領した」 .....                                           | 9  |
| 1.3. 個人情報の管理－オプトアウト対応－ .....                                                        | 12 |
| ケース 4 「オプトアウトによって第三者提供された「個人データ」をさまざまなサービスで利用しているときに、一部のサービスのみ利用(提供)停止が要求された」 ..... | 13 |
| 1.4. 個人情報の管理－外国にある第三者への提供－ .....                                                    | 16 |
| ケース 5 「本人同意を得ていない個人データを、法改正以前から、海外企業に委託していた」 .....                                  | 17 |
| 2. 委託元との関係での留意事項 .....                                                              | 19 |
| 2.1. 委託元からの監督 .....                                                                 | 20 |
| ケース 6 「委託元から過剰とも思える監査に対応する」 .....                                                   | 21 |
| ケース 7 「再委託先の安全管理措置が不十分だった」 .....                                                    | 23 |
| 2.2. 漏えい等事案発生時の対応.....                                                              | 26 |
| ケース 8 「委託元への個人データ紛失報告が大幅に遅れた」 .....                                                 | 27 |
| 2.3. 開示請求等への対応.....                                                                 | 32 |
| ケース 9 「開示等請求を受けてはならないにも関わらず、受けてしまった」 .....                                          | 33 |
| ケース 10 「開示等請求への対応が遅れ、訴訟を起こされた」 .....                                                | 35 |
| Appendix(付録) .....                                                                  | 37 |
| 情報サービス産業における個人情報取扱実務チェックシート：【委託元への対応】 .....                                         | 38 |
| 情報サービス産業における個人情報取扱実務チェックシート：【委託先の対応】 .....                                          | 39 |
| 情報サービス産業における個人情報取扱実務チェックシート：【再委託先への対応】 ..                                           | 40 |

## 本書作成の背景と方針

本書は、平成 29 年 5 月 30 日に施行された「個人情報の保護に関する法律」(以下、個人情報保護法といいます。)への実務対応のポイントのうち、特に解釈の難しい部分を中心に、実務上、具体的に何をすればよいかを、実施の容易さも考慮しながら、優先順位付けして示すことを目指して、タスクフォースにて議論した結果をまとめたものです。

個人情報保護法に関しては、すでに多くの解説書や実務 Q&A が出版されておりますが、そうした中、本書は以下の点で特徴あるものを目指しました。

- ・ 実務において、特に対応が必要な事項を示すこと。
- ・ 情報サービス事業者、とりわけ受託業務にフォーカスすること。
- ・ 中小企業を含む全 JISA 会員企業にとって、無理なく対応できるよう、優先順位付けをして対応策を示すこと。

また、個人情報保護に関しては、「金融分野における個人情報保護に関するガイドライン」「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」等、各個別分野ごとのガイドラインも作成されており(図 1 参照)、受託者(委託先)の立場としては、委託元の業界によって、これらを確認する必要がありますが、本書は、個別分野にとらわれず、共通部分のみを扱っています。

| 対象業界                 | 主な関係法令、ガイドライン等                                                                                |
|----------------------|-----------------------------------------------------------------------------------------------|
| ・全業界                 | 個人情報の保護に関する法律、同法施行令、同法施行規則<br>個人情報の保護に関する法律についてのガイドライン<br>個人情報保護条例                            |
| ・行政機関<br>・独法<br>・自治体 | 「行政機関の保有する個人情報の保護に関する法律」、同法施行令、同法施行規則<br>「独立行政法人等の保有する個人情報の保護に関する法律」、同法施行令、同法施行規則<br>個人情報保護条例 |
| ・金融分野                | 「金融関連分野ガイドライン」※1                                                                              |
| ・医療分野                | 「医療関連分野ガイダンス」※2                                                                               |
| ・電気通信分野              | 「電気通信事業における個人情報保護に関するガイドライン」※3                                                                |
| ・その他分野               | 雇用分野、私的年金分野、ヒトゲノム・遺伝子解析研究等での業法等に基づく指針など                                                       |
| ・認定個人情報保護団体の会員       | 認定個人情報保護団体の定める指針 (2018.1.23現在で44団体)                                                           |
| ・匿名加工情報を作成する企業       | 「個人情報保護委員会事務局レポート「匿名加工情報 パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」                                     |

※1:金融分野における個人情報保護に関するガイドライン、信用分野における個人情報保護に関するガイドライン、債権管理回収業分野における個人情報保護に関するガイドラインの総称  
 ※2:医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス、健康保険組合等における個人情報の適切な取扱いのためのガイダンス、国民健康保険組合における個人情報の適切な取扱いのためのガイダンス、国民健康保険団体連合会等における個人情報の適切な取扱いのためのガイダンスの総称  
 ※3:この他、放送分野、郵便事業分野、信書便事分野でガイドラインがある

図 1 改正個人情報保護法関連の法令とガイドライン等

本書は、原則見開き 2 ページ、以下の構成で、改正個人情報保護法の論点を、実践的かつ具体的な記述で解説しています。

|               |                                                                                   |
|---------------|-----------------------------------------------------------------------------------|
| ■ ケース         | 1 個の具体的なケースを採り上げます。                                                               |
| ■ リスク         | 上記ケースに含まれるリスクを説明します。                                                              |
| ■ 個人情報保護法での規定 | 関連する個人情報保護法の条文上の規定を示します。                                                          |
| ■ 対応策         | 上記ケースにおいて、リスクを回避、低減させるための対応策を解説します。<br>基本的な対策・重要な対策から始めて、次善策や付随的な対策を記載するようにしています。 |
| 「ちょっと待って！」    | ケースに関連する別の論点や、併せて注意すべき事項、実務的な留意点など上記では採り上げきれなかった論点を、記載しています。                      |

またケースで取り上げた登場人物の相関図を図 2 に示します(登場人物及び社名は架空のものです、実在の人物や団体名等とは一切関係がありません)。

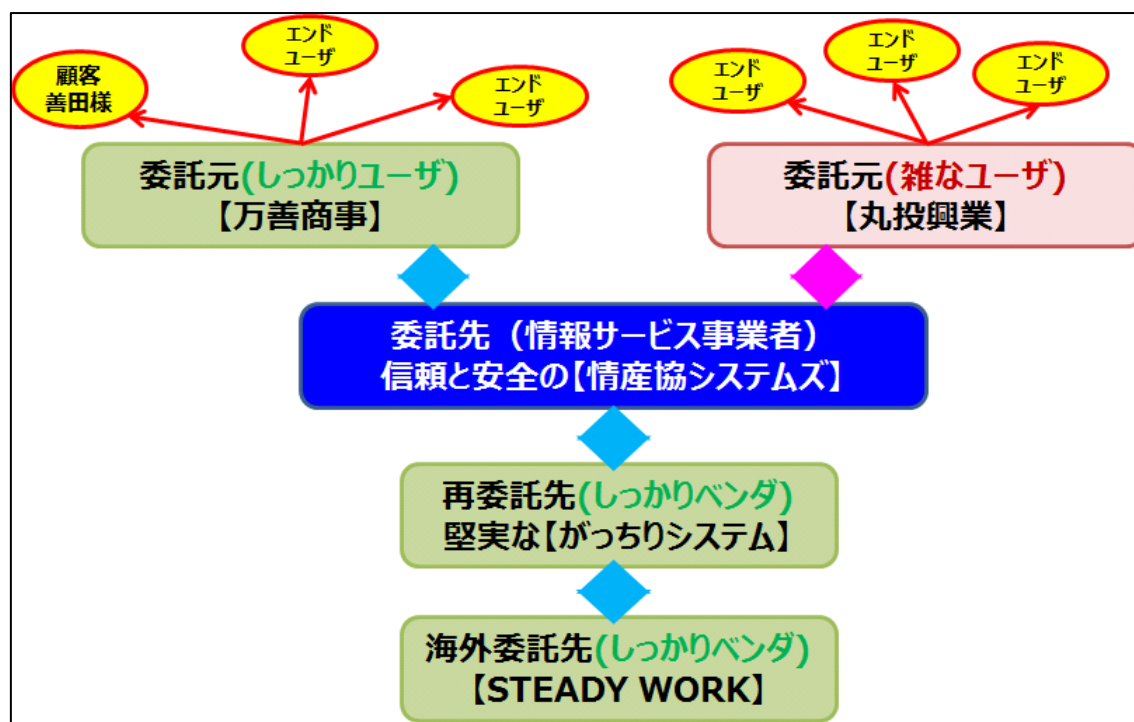


図 2 登場人物

## 想定読者

委託元から個人情報を取り扱うシステムの開発や運用を受託する「情報サービス事業者」のプロジェクトマネージャ、またはプロジェクトリーダを主な読者として想定して本ドキュメントを作成しています。

## 用語

| 用語名    | 本書における定義                                                                                                                                                                                                                                                                                                                                                               |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 委託     | <p>業務の一部を他社に代行してもらうこと。</p> <p>⇔提供：個人情報了他者に提供すること。業務の委託関係はない。</p> <p>⇔共同利用：グループ会社などで、社員の個人情報等を共同で利用すること。</p>                                                                                                                                                                                                                                                            |
| オプトアウト | <p>個人情報保護法第 23 条第 2 項に、以下の通り定義されている。</p> <ul style="list-style-type: none"> <li>・第三者に提供される個人データについて、本人の求めに応じて提供を停止することとしている場合であって、あらかじめ、以下の項目について、本人に通知し、又は本人が容易に知り得る状態に置いた上で、本人の同意を得ることなく第三者に提供すること。</li> <li>・個人データを第三者に提供する旨</li> <li>・提供する個人データの項目</li> <li>・提供方法</li> <li>・本人の求めに応じて提供を停止する旨</li> <li>・本人の求めを受け付ける方法</li> </ul>                                   |
| 個人識別符号 | <p>「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう。</p> <p>(1) 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの</p> <p>(2) 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの</p> |
| 個人情報   | <p>個人情報保護法第 2 条第 1 項により、以下のように定義されている。</p> <ul style="list-style-type: none"> <li>・生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの</li> <li>(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)</li> </ul>                                                                                                                                               |

| 用語名          | 本書における定義                                                                                                                                                                                                                                                            |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 第三者への提供      | 事業者が保有する個人データを、その事業者以外の者に提供すること。<br>「第三者」とは、その個人情報の持ち主である本人と、その個人情報を取り扱う事業者以外のすべての人（事業者）をさす。                                                                                                                                                                        |
| 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。<br>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や、6ヶ月以内に消去するもの（更新するものを除く）は除外される。                                                                                                                             |
| 本人が容易に知りうる状態 | 本人が知ろうとすれば、時間的にも、その手段においても、簡単に知ることができる状態に置いていること。具体的な事例としては以下の通り。<br>事例 1 ) ウェブ画面中のトップページから 1 回程度の操作で到達できる場所への掲載等が継続的に行われていること。<br>事例 2 ) 事務所の窓口等への掲示、備付け等が継続的に行われていること。<br>事例 3 ) 広く頒布されている定期刊行物への定期的掲載を行っていること。<br>事例 4 ) 電子商取引において、商品を紹介するウェブ画面にリンク先を継続的に掲示すること。 |
| テストデータ       | 委託元から受領したテストデータ。                                                                                                                                                                                                                                                    |
| マスキング        | マスキング対象となった個人データの個人が識別特定の不可能となった状態。                                                                                                                                                                                                                                 |
| 物理的安全管理措置    | 物理的安全管理措置には次の措置がある。<br>(1) 個人データを取り扱う区域の管理<br>(2) 機器及び電子媒体等の盗難等の防止<br>(3) 電子媒体等を持ち運ぶ場合の漏えい等の防止<br>(4) 個人データの削除及び機器、電子媒体等の廃棄<br>【例】<br>個人データが格納された媒体を移送するときは、厳重な施錠と物理鍵を別に保管する等し、万が一紛失や盗難にあったときでも内容が外部の者にわからないようにするなどの措置が必要である。                                       |

| 用語名       | 本書における定義                                                                                                                                                                                                                                                                                              |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 組織的安全管理措置 | <p>組織的安全管理措置には次の措置がある。</p> <ul style="list-style-type: none"> <li>(1) 組織体制の整備</li> <li>(2) 個人データの取扱いに係る規律に従った運用</li> <li>(3) 個人データの取扱状況を確認する手段の整備</li> <li>(4) 漏えい等の事案に対応する体制の整備</li> <li>(5) 取扱状況の把握及び安全管理措置の見直し</li> </ul> <p>【例】<br/> 取扱いを委託された個人データが漏えいや滅失などしたとき、速やかに委託元に連絡できるように連絡体制を予め整備する。</p> |
| 開示等請求     | <p>保有する個人データについて開示や訂正、消去などの申出を受けることがある。取扱いの委託を受けた個人データの場合で委託元が開示等請求窓口となっているときは、そうした申出を委託元に行うよう促す。また委託元が開示等請求を受け、自社も取扱いを受託している立場から対応することになったときは、速やかに対応する。</p>                                                                                                                                          |

## 執筆者名簿

|     |       |                                                               |
|-----|-------|---------------------------------------------------------------|
| 座長  | 土屋 茂樹 | 株式会社 NTT データ<br>技術革新統括本部 システム技術本部<br>セキュリティ技術部部長              |
| 副座長 | 室脇 慶彦 | 株式会社野村総合研究所<br>理事                                             |
| 委員  | 堀籠 雄  | SCSK 株式会社<br>法務・総務・広報・CSR グループ 法務部 副部長                        |
| 委員  | 和田 義毅 | 株式会社 NTT データ<br>技術革新統括本部 システム技術本部<br>セキュリティ技術部 情報セキュリティ推進室 室長 |
| 委員  | 山田 英二 | 株式会社 NTT データ<br>企画調整室 IT 政策推進グループ 課長                          |
| 委員  | 曾我 吉和 | 株式会社 NTT データ<br>技術革新統括本部 システム技術本部<br>セキュリティ技術部 情報セキュリティ推進室 課長 |
| 委員  | 大工原義裕 | TIS 株式会社<br>管理本部コンプライアンス統括部エキスパート                             |
| 委員  | 崎村 夏彦 | 株式会社野村総合研究所<br>ビジネス IT 推進部 上席研究員                              |
| 委員  | 佐藤 敦  | 株式会社野村総合研究所<br>品質監理本部 情報セキュリティ部長                              |
| 委員  | 高橋 知樹 | 株式会社三菱総合研究所<br>社会 ICT イノベーション本部 副本部長                          |
| 事務局 | 田原 幸朗 | 一般社団法人情報サービス産業協会<br>理事                                        |
| 事務局 | 鈴木 律郎 | 一般社団法人情報サービス産業協会<br>総務部 次長                                    |

(平成 30 年 3 月末日執筆当時)

## **1. 個人情報取り扱いのライフサイクルでの留意事項**

## **1.1. 個人情報の定義**

## ケース 1 「顧客から受領したテストデータに個人データが含まれていた、顧客自身はテストデータの当該情報を個人情報と認知していなかった」

情産協システムズは、顧客管理システムの開発を受託しており、丸投興業から、テスト用データとして、会員番号を架空の値に置き換えたデータを受領しました。丸投興業からは、当該データは個人情報を含まないとして渡され、情産協システムズも受領した時点では、顧客の氏名、生年月日等が削除されていることは確認しました。

### ■リスク：

委託元が個人情報と認識しないデータを、精査することなく受領してはいけません。もし受領した後、個人情報が含まれている情報と認識した場合には、直ちに個人情報として管理しなければいけません。

### ■個人情報保護法での規定：

- ・ 個人情報保護法 第2条第1項第1号及び第2号
- ・ 個人情報保護法施行令 第1条各号（運転免許証番号は第4号）

本ケースは、一見したところ個人情報を含んでいなかったが、精査したところ運転免許証番号が含まれていたケースです。

運転免許証番号のみでは、誰に対して付与されたのか分からず、特定の個人を識別することができないのではないかと、従って、個人情報には該当しないと判断しがちですが、法令で「個人識別情報」とされており、これを含むデータも個人情報に該当します。

### ■対応策：

- (1) 個人情報に該当するおそれのあるデータは極力、受領しない。

まず、個人情報に該当する可能性のあるデータを安易に受領しないことを考えるべきです。本ケースでは、テスト用データということですので、必ずしも実際の顧客データを使用する必要はなく、仮定のデータを用いればよかったとも考えられます。また、どうしても本番データを使用してテストを行わなければならないのであれば、委託元の稼働環境において、委託元の立会いのもとに行うなど、データを受領しない形で実施することも考えられるでしょう。

- (2) 受領データに個人情報が含まれないことを、委託元に明示してもらう。

やむを得ず、個人情報を含む可能性のあるデータを受領する場合には、委託元との

契約で、法に照らし個人情報を明記する義務を課すか、若しくは個人情報を含むデータを譲渡しない旨、明記することが有益です。

(3) ポイントとなる事項を、委託元に確認する。

個人情報に当たるか否かが微妙な場合には、以下のような観点で、委託元に確認を行うことが望ましいと考えられます。

- ・ それ自体では特定の個人を識別できないように見えても、提供される他の情報と照合すれば、識別されるようになっていないか（容易照合性がないか）。
- ・ 氏名、生年月日等は含んでいないものの、特殊な情報（たとえば、非常に高額な物品の購入歴や、希少な病歴など）が含まれており、それによって、特定の個人が識別されることはないか。
- ・ 個人識別符号に該当する情報を含んでいないか。

**ちょっと待って！**

何が個人識別符号に該当するは、個人情報保護法施行令第 1 条に列挙されています。これに対して、民間の発行するクレジットカード番号は、「個人識別符号」とされておらず、クレジットカード番号を含む情報は、他に個人を識別・特定する情報が含まれていないときは「個人情報」には該当しないことになります。ただし、クレジットカード番号のように悪用されるおそれの高い情報は、たとえ「個人情報」に該当しない場合であっても、厳重な管理が求められます。

## ケース 2 「別々に受領したデータであったが、特定の属性データを照合すれば個人が特定できることがわかった」

情産協システムズは、丸投興業の EC(電子商取引)システムの開発を受託しており、丸投興業から、テストデータとして、実際の顧客の購入履歴データを受領しました。この際、丸投興業において事前に、氏名を含む顧客属性データと、購入履歴データは分離されていたので、情産協システムズは、前者の顧客属性データは個人情報として扱わなければならないが、後者の購入履歴データは、個人情報に該当しないと認識していました。

ところが、受領後に、情産協システムズにおいて精査してみると、顧客属性データには顧客 ID が割り振られており、購入履歴データの備考欄にも、顧客 ID が残っていることが分かりました。

### ■リスク：

個人データを含まないとして譲渡されたデータであっても、個人を識別できる ID が振られたものについては、注意が必要です。同一の ID を持つ他の個人データがある場合、これらのデータが容易に照合できる可能性があるからです。個人情報を含むデータとして認識した場合には、直ちに個人情報として管理しなければいけません。

### ■個人情報保護法での規定：

- ・ 個人情報保護法第 2 条第 1 項第 1 号での個人情報の定義（「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。」）

本ケースは、顧客属性データと、購入履歴データを別々に受領しました。前者が、個人情報に当たるのは明らかです。後者の購入履歴データは、氏名等を削除することで、特定の個人が識別できないようになっていたため、一見、個人情報には当たらないようにも思えます。

しかし、顧客 ID を照合し、顧客属性データと統合することにより、委託先において、特定の個人を識別できるようになりました。このため、購入履歴データも個人情報として扱わなければなりません。

実際のケースでは、顧客属性データを分離しておきながら、両データを同じ委託先に譲渡することはないかもしれませんが、本ケースのように、顧客 ID 等を照合して、意図せずして個人を特定できる場合もあるので、注意が必要です。

## ■対応策：

ケース1の場合と同様です。

### (1) 個人情報に該当するおそれのあるデータは極力、受領しない。

まず、個人情報に該当する可能性のあるデータを安易に受領しないことを考えるべきです。本ケースでは、テスト用データということですので、必ずしも実際の顧客データを使用する必要はなく、仮定のデータを用いればよかったとも考えられます。また、どうしても本番データを使用してテストを行わなければならないのであれば、委託元の稼働環境において、委託元の立会いのもとに行うなど、データを受領しない形で実施することも考えられるでしょう。

### (2) 受領データに個人情報が含まれないことを、委託元に明示してもらう。

やむを得ず、個人情報を含む可能性のあるデータを受領する場合には、委託元との契約で、法に照らし個人情報を明記する義務を課すか、若しくは個人情報を含むデータを譲渡しない旨、明記することが有益です。

### (3) ポイントとなる事項を、委託元に確認する。

個人情報に当たるか否かが微妙な場合には、以下のような観点で、委託元に確認を行うことが望ましいと考えられます。

- ・ それ自体では特定の個人を識別できないように見えても、提供される他の情報と照合すれば、識別されるようになっていないか（容易照合性がないか）。
- ・ 氏名、生年月日等は含んでいないものの、極めて特殊な情報（たとえば、非常に高額な物品の購入歴や、希少な病歴など）が含まれており、それによって、特定の個人が識別されることはないか。
- ・ 個人識別符号に該当する情報を含んでいないか。

## ちょっと待って！

委託元から個人情報を含まない旨の保証を得たうえで受領したデータの中に、個人情報が混入しており、万一、それが委託先から流出した場合には、委託先も責任を免れません。ただし、「対応策」で示したとおり、契約上、委託元に個人情報を明示する義務を課していたのに委託元から申告がなかったという場合や、委託元から個人情報が含まれていないとの誓約を得ていた場合には、委託元に対しては責任を負わず、さらには委託元に対して賠償請求等ができることもあり得ます。また、委託先としてやるべきことはやっていれば、レピュテーション・リスクを抑えることができるものと思われます。



## 1.2. 個人情報の取得

### ケース 3 「マスキングが不十分なデータをダミーデータとして受領した」

情産協システムズは、丸投興業から、同社の顧客管理システムの開発を受託しています。

試験にあたり、丸投興業からテストデータとして、「顧客データの一部をマスキングして作成したダミーデータ」と説明を受けたものを受領しました。

情産協システムズがテストを準備しようとしたところ、受領したダミーデータのマスキングが不十分のため顧客を識別し、特定できるおそれがある、との声が担当者から寄せられました。

#### ■ リスク :

委託元からテストデータの提供を受ける場合、不十分な加工等により「個人データ」が含まれたままの状態を受領する可能性があります。

このケースで委託先の確認も不十分で、個人情報の漏えいに至った場合、委託元、委託先双方の責任が追及されるリスクがあります。

#### ■ 個人情報保護法での規定 :

- ・ 個人情報保護法 第 23 条第 1 項
- ・ 個人情報保護法 第 23 条第 5 項
- ・ 個人情報保護法 第 26 条第 1 項

本ケースでは、委託元から提供されたデータが委託元によって個人データとされていなかったため、個人情報保護法第 23 条第 5 項第 1 号により「個人データの取扱いを委託するときには第三者提供とされない」との条文が、適用されないおそれがあります。このとき、委託元は「個人データ」の第三者提供の制限に違反して委託先に個人データを提供していることになる可能性があります。

一方、データを受領した委託先は、実質的に「個人データ」となっているデータは、委託元が特定し、明示したか否かにかかわらず、その取扱いにおいて、法を順守する必要があります。

なお委託先が第三者提供を受けたときは、一定の例外を除き、法第 26 条に基づき、確認及び記録義務の対象になります。

#### ■ 対応策 :

委託元からテストデータの提供を受ける際は、予め次の事項を契約や仕様等の書面で

確認する。

- ・ 受領する予定のデータの内容と必要とする取扱い。
- ・ テストデータの内容を確認時、個人データが含まれるおそれがあるときは、速やかに委託元に返却する旨

**(参考)対応策の事例：**

- ・ システム開発に係る標準契約において個人情報保護に関する規定を設け、委託元があらかじめ書面にて個人情報を特定し明示することを求める。また損害賠償請求や本人からの開示請求等の対応に関する規定を記載する。
- ・ クラウドサービス等で個人情報と認識せずに顧客から情報を預かる場合も、個人情報と認識して預かるときに準じた対応を推奨し、一部は個人情報と認識して預かるときと同じ対応を求める。
- ・ マスキングされたデータを受領したときには、データの内容を確認し、「個人データ」が含まれるおそれがあるか確認する。

**ちょっと待って！**

テストデータなどで「個人データ」を含む可能性があるデータは、そのデータを受領する前に、委託元とともによく内容を確認しましょう。



### 1.3. 個人情報の管理－オプトアウト対応－

#### ケース4「オプトアウトによって第三者提供された「個人データ」をさまざまなサービスで利用しているときに、一部のサービスのみ利用(提供)停止が要求された」

オプトアウトによって提供された「個人データ」を使って、万善商事が販売した製品のサポート業務と製品情報を提供するシステムを、情産協システムズは受託しています。

万善商事の顧客から製品情報の提供のみを停止するよう依頼がありましたが、当該システムでは、提供機能の一部のみを停止する仕様になっていません。

##### ■リスク：

第三者提供を受けた委託先は、利用者本人から提供停止の要請があった場合は、委託元の承認を得た上で、直ちに利用停止しなければいけません。

一方、本システムの仕様のように、顧客の要請に従って利用停止してしまうと、サポート業務も停止することになり、事業継続上の問題となります。

##### ■個人情報保護法での規定：

- ・ 個人情報保護法 第23条第1項
- ・ 個人情報保護法 第23条第2項

「あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない」が、法第23条第2項において、「あらかじめ、本人に通知し、又は本人が容易に知りうる状態に置くとともに、個人情報保護委員会に届け出たとき」には、本人同意を得ずとも「当該個人データを第三者に提供することができます」。

##### ■対応策：

あらかじめ用途別に機能が停止できる、システム設計にします。すでに運用中のシステムは、計画的に改修するようにします。故意に改修を遅らせるなどせず、妥当な改修計画を立て、改修後の保守、運用計画も検討するようにしてください。

あるいは、委託元と委託元の顧客とは包括的な同意を得ているので、一方のサービスのみ停止できないことを説明し、現状を容認するか、あるいは、両方のサービスを停止するかの、いずれかで了解を得る方法も考えられます。

本ケースのように、委託元のシステム運用を受託しているケースでは、委託元の顧客本人への説明や対応、若しくは承諾については、委託元が行うのが一般的です。委託先は、委

託元に事前に上記対応が必要である旨、説明し契約を交わすことで、委託元とのトラブルを防止します。

**(参考)対応策の事例：**

3か月後の定期アップデートに合わせて、システム改修を計画し、委託先に説明し了承を得ます。また改修以前に、委託元の顧客本人から、製品情報提供停止の要請があった場合には、委託元から委託元の顧客本人に、今後の対応について説明するよう、事前に依頼しておきます。

**ちょっと待って！**

複数の委託元との間で同じような課題がある場合、個人情報漏えい事件等を契機に改修依頼が集中することが考えられます。日頃から、委託先とシステムの課題を共有し、計画的に解決することの同意を得ておきましょう。



#### **1.4. 個人情報の管理－外国にある第三者への提供－**

## ケース 5 「本人同意を得ていない個人データを、法改正以前から、海外企業に委託していた」

情産協システムズは、万善商事から情報サービスシステムの運用を受託しています。個人情報保護法の改正前から、万善商事から提供を受けた個人情報は、がっちりシステムを通じて、データ処理を委託している STEADY WORK 社（外国にある第三者）が管理するサーバに保存しています。

しかし、法の改正に伴い、がっちりシステムへの提供の形態が、本人同意が取れていないことになることが判明しました。

### ■ リスク：

外国の事業者（外国にある第三者）に個人情報を提供する場合には、「本人同意を得」ているか、その事業者が「個人情報保護委員会で定める基準に適合する体制を整備」していなければいけません。

### ■ 個人情報保護法での規定：

- ・ 個人情報保護法 第 24 条
- ・ 個人情報保護法施行規則第 11 条
- ・ 個人情報の保護に関する法律についてのガイドライン(外国にある第三者への提供編)

外国の事業者「個人データ」を委託する場合には、「本人の同意を得」なければいけません。ただし、本条にある「個人情報保護委員会で定める基準に適合する体制を整備している」場合には、本人同意が不要になります。具体的には、個人情報保護法施行規則第 11 条第 1 号において「①適切かつ合理的な方法で、②法第 4 章第 1 節の趣旨に沿った措置の実施が確保されていること」とされており、ガイドラインでは①及び②の基準が事例とともに解説されています。

このほかに、個人情報保護法施行規則第 11 条第 2 号に基づき、委託先、再委託先、又は外国の事業者が、プライバシーフレームワークへの適合性を国際的に認証している制度の認定を受けていることでも、本人同意の取得は不要になります。

### ■ 対応策：

「個人データ」を外国の事業者に提供する場合には、委託先において再委託先を適切に

管理、監督し、日本国内と同等の個人情報の管理、手続きを求めることが肝要です。従来から、外国の事業者が日本国内と同等の管理を求めている場合には、今般の改正を受けて、新たに必要になる業務や手続きはありません。

外国の事業者に対して、日本と同等の個人情報の管理、手続きを求めている場合には、契約更新時に、本人同意の取得を前提として、外国の事業者に対し日本国内と同等の管理を行うようJISAのモデル契約書で求めている条件を取り込んで契約することが考えられます。

### (参考) 自社内における対応策の事例：

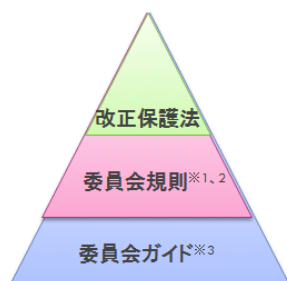
外国の事業者との契約において、JISA 個人情報保護モデル契約(第2版)で求めている条件と同等の内容を取り込む。

### ちょっと待って！

- ・ 国内外に関わらず、個人情報を外部事業者に提供する場合には、本人同意を取得することはもとより、委託先による外部事業者の管理、監督を行うことが重要です。
- ・ 外国の事業者が「個人データ」を提供する場合には、JISA 個人情報保護モデル契約(第2版)を参考にして、日本国内と同等の管理を契約書で定め、継続的に実施していくよう求めます。
- ・ 適切な体制を整備している外国の事業者を選定する指標の一つに、APEC の越境プライバシールール（CBPR：Cross-Border Privacy Rules）システムの認定を受けていることが挙げられます。

海外提供は原則としては厳しくなったが、適正な委託先の監督の実施により、**海外委託は可能**。**お客様が不可能と誤解される**場合、可能である旨をお客様に説明する必要がある。

#### ■ 海外委託に関する法令等に定められた要件



#### 【要件】

- ①海外委託する旨**本人の同意を得る**。または
- ②個人情報保護委員会規則で定める**基準**に適合、等

#### 【②の基準】

■ガイド※3で定める。

#### 【②の基準】

■ **委託先の監督を適正に実施している。**  
(選定、契約、必要に応じた監査)

※1委員会：個人情報保護委員会。個人情報の保護に関する監督を行う、日本政府内の独立組織。公正取引委員会と同レベルの位置づけ。

※2委員会規則：個人情報保護委員会の定める規則。

※3委員会ガイド：個人情報保護委員会の定めるガイドライン。

図 3 海外委託の要件

## **2. 委託元との関係での留意事項**

## **2.1. 委託元からの監督**

## ケース6「委託元から過剰とも思える監査に対応する」

先日、万善商事にて、顧客管理システムに対する不正アクセスを検知しました。不正アクセスの内容を分析した結果、顧客システムへの影響はなく、再発防止策としてネットワーク設定等の見直しも実施しました。

それ以降、万善商事から毎月のように立入監査の依頼があります。立入監査への対応には時間もコストも相応な負担がかかっています。契約書にも「乙(情産協システムズ)は甲(万善商事)の監査に協力すること」との条項がありますが、情産協システムズは、万善商事の監査は限度を超えた頻度であると思っています。

### ■リスク：

必要以上の監査を受け入れることは、受け入れ側の準備体制や対応時間等、保守費以上のコスト負担を強いられることがあります。

### ■個人情報保護法での規定：

- ・ 個人情報保護 第22条

「個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない」とされています。

### ■対応策：

委託元と次の事項で合意形成を行います。

- ・ 委託先に対する監査に求めるレベル(回数、立入検査の有無、実施内容等)を明確化します。
  - ・ 委託先(再委託先を含む)に対する監査にあたっての手続きを、JISA 個人情報保護モデル契約(改訂第2版)第9条(監査)、第10条(改善の指示)に基づき定めます。
- ※参考 JISA 個人情報保護モデル契約(改訂第2版)

<https://www.jisa.or.jp/Default.aspx?TabId=272&pdid=28-J005>

### ちょっと待って！

監査受入れのために要した費用の負担については、監査を実施する前に委託元と合意するようにしてください。

再委託先を利用する場合には、必ず委託元に対して再委託を実施する旨を報告するとともに、委託元から求められている監査および安全管理措置の実施を契約に定めてください。



## ケース7「再委託先の安全管理措置が不十分だった」

情産協システムズは、万善商事の顧客管理システムの開発及び運用を請け負っています。開発運用職務の分離のため、請け負ったシステムの運用はがっちりシステムに再委託しています。

情産協システムズとがっちりシステムは取引関係が長いことから、二者間の契約は、取引当初から見直しがされていませんでした。また、情産協システムズは日々の運用業務の管理状況の報告は受けていたものの、管理方法の詳細はがっちりシステムに任せきりにしていました。

ある日、顧客管理システムの安全管理状況について、情産協システムズががっちりシステムに行く現地監査に、万善商事が同行しました。その結果、がっちりシステムの安全管理措置の実施が不十分であることがわかり、情産協システムズは、万善商事から厳重注意を受けることとなりました。

### ■リスク：

個人情報を含む情報管理を外部委託する際に、委託先において必要な管理がなされないことにより個人情報が漏えいした場合、委託元はその責任を問われる可能性があります。

### ■個人情報保護法での規定：

- ・ 個人情報保護法 第22条

「個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない」とされています。

### ■対応策：

再委託先との契約に当たって、次の事項で合意形成を行います。

- ・ 個人情報取扱事業者として相応しい事業者であるかを選定基準とします。選定基準は2点考えられます。
  - ① プライバシーマーク取得業者であること。
  - ② プライバシーマーク取得業者ではない場合、個人情報の管理状況(個人情報の取得・利用、保管、提供、開示請求への対応に関するルールがあること、など)を確認し、妥当であると評価できること。

※参考:個人情報保護委員会 中小企業向け「これだけは!」10 のチェックリスト付  
はじめての個人情報保護法 ～シンプルレッスン～(平成 29 年 6 月)

[https://www.ppc.go.jp/files/pdf/1711\\_simple\\_lesson.pdf](https://www.ppc.go.jp/files/pdf/1711_simple_lesson.pdf)

- ・ 委託先における委託された個人データの取扱状況を把握できるようにします。

※参考 個人情報の保護に関する法律についてのガイドライン 8 (別添)講ずべき安全管理措置の内容

[:https://www.ppc.go.jp/files/pdf/guidelines01.pdf](https://www.ppc.go.jp/files/pdf/guidelines01.pdf)

※参考 JISA 個人情報保護モデル契約(改訂第 2 版)

[:https://www.jisa.or.jp/Default.aspx?TabId=272&pdid=28-J005](https://www.jisa.or.jp/Default.aspx?TabId=272&pdid=28-J005)

- ・ 委託元との契約に基づいた監査手続きが実施できるよう、契約に定めます。

※参考 JISA 個人情報保護モデル契約(改訂第 2 版)

<https://www.jisa.or.jp/Default.aspx?TabId=272&pdid=28-J005>

### **ちょっと待って!**

再委託先をする場合は、必ず委託元に対して再委託を実施する旨を報告するとともに、委託元から求められている監査および安全管理措置の実施を契約に定めてください。



## 2.2. 漏えい等事案発生時の対応

## ケース 8「委託元への個人データ紛失報告が大幅に遅れた」

情産協システムズは、万善商事の顧客の「個人データ」を取り扱うシステムの運用を受託しています。

ある金曜日夜に、情産協システムズの社員が、「個人データ」が格納されたバックアップメディアを倉庫に保管しようと、メディアをカバンに入れ、電車を使って移送しました。メディアを入れたカバンを網棚に置いたのですが、下車駅でカバンを置き忘れて下車してしまいました。

急ぎ鉄道会社に連絡し、カバンを搜索しましたが、見つかりません。

このため、上司に連絡し、上司から万善商事に紛失があったことを連絡しようとしたが、金曜日の夜から日曜日にかけて連絡が取れず、万善商事への報告は月曜日の朝になってしまいました。

一方、紛失したカバンに入っていたメディア内のデータは、日曜日のうちにインターネット上に流出してしまいました。

### ■リスク：

漏えい事案を防止するための対応が不十分であり、漏えい事案が生じてしまいました。

漏えい事案発生後の対応としては、委託先から委託元への土日夜間発生時の事案発生の第一報が滞り、翌営業日等まで経営層等への伝達が遅れてしまっています。

委託先から委託元への連絡系統が整理、更新されておらず、関係者への第一報が滞っています。

### ■個人情報保護法での規定：

- ・ 個人情報保護法 第 20 条
- ・ 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)8-3
- ・ 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)8-5

法第 20 条で「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」とされています。

ガイドライン 8-5 物理的安全管理措置では、「電子媒体等を持ち運ぶ場合の漏えい等の防止」が求められ、「個人データが記録された電子媒体又は個人データが記載された書類等を持ち運ぶ場合、(略)紛失・盗難等を防ぐための安全な方策を講ずる。」と対応が義務化されています。

ガイドライン 8-3 組織的安全管理措置では、「漏えい等の事案に対応する体制の整備」が求められ、「漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならない。」と対応が義務化されています。

#### ■ 対応策：

個人情報の取扱いを受託するときに、委託先は委託元に次の事項を要請します。

- ・ 委託先から委託元への緊急連絡ルートは 2 系統用意する。
- ・ 委託元の協力を受け、定期的な緊急時対応訓練を実施する。

委託先は、日常から、次の事項の運用を実施します。

- ・ 漏えい事案が生じないよう、「個人データ」を媒体に格納して持ち出さない、持ち出すときは暗号化し肌身離さず運搬する等、「個人データ」の移送又は送信時の物理的安全管理措置を行う。
- ・ プロジェクトメンバには最新の連絡先を複数周知し、事案遭遇当日のうちに、第一報の連絡を上長等に入れるよう、教育・啓発に努める。
- ・ ステークホルダ(委託元、個人データの本人、関係府省、プライバシーマーク事務局など)への報告は、可能な限り社内関連部署の専門家の知見を活用し、対応経験の乏しい当事者組織が単独で行うことは避けるようにする。

#### (参考) 対応策の事例：

JISA 個人情報保護モデル契約(改訂第 2 版)で求めている条件と同等の内容を取り込む。

#### ➤ 漏えい事案を生じさせないための対策

- ・ 個人データの移送は、移送途中で紛失・盗難等を生じさせないよう、極力媒体での移送は行わない。やむなく媒体で移送する場合は、施錠した搬送容器に格納し、肌身離さず運搬する。
- ・ 個人データの移送においては、移送の手段を問わず、暗号化等の措置を施し、紛失・盗難等が生じて個人データの内容を外部の者が見ることができないようにする。

#### ➤ 漏えいした時の対策

##### ◆ 発見者または当事者

漏えい事案等の遭遇時は、緊急時のプロジェクト連絡体制に従い、直ちに発生事

実を上司等に報告し指示を仰ぐ。

◆ プロジェクト

当該事案発生の報告を受けた際は、緊急時の連絡体制に従い、関係者にいち早く侵害の発生事実を伝え、対応マニュアルに従って、初動対応を行う。

〔初動対応〕

- ・優先事項:お客様およびプロジェクト等で定めた連絡先への報告
- ・被害状況の詳細な把握
- ・証拠の保全
- ・被害拡大の防止
- ・事案発生に至る経緯の洗い出し

◆ コーポレートスタッフ

状況の把握とプロジェクトへの資源投入の判断を行う。

委託元と連携し、社外の関連組織への報告等の対応を行う。

**ちょっと待って！**

漏えいが極力生じないような業務フローにしましょう。

万一漏えいしたときの対応を、関係者とあらかじめ合意しておきましょう。





### **2.3. 開示請求等への対応**

## ケース 9 「開示等請求を受けてはならないにも関わらず、受けてしまった」

情産協システムズは、万善商事の顧客管理システムの運用を受託しています。

この顧客管理システムで保有している個人データの開示請求の申出先は、万善商事となっていますが、万善商事は顧客に対して、顧客管理システムの運用を情産協システムズに委託している旨を公表しています。

ある日、情産協システムズは、万善商事の顧客(個人)の善田氏から、顧客管理システムで管理している善田氏の個人データを開示するように請求を受けました。

情産協システムズは、受託しているシステムで管理している「個人データ」であり、申し出者本人の「個人データ」であることから、リスクが少ないと判断し、善田氏に対して「個人データ」を開示しました。

後日、情産協システムズは、万善商事から、同社に無断で善田氏の請求に応じたことへのクレームを受けました。

### ■リスク：

開示等の申出があったとき、委託先は委託元が対応すべき開示等の申出を受け付けてはいけません。

### ■個人情報保護法での規定：

個人情報保護法 第 32 条 1「個人情報取扱事業者は、(略)、政令で定めるところにより、その求め又は請求を受け付ける方法を定めることができる。」とあり、政令では、「開示等の請求等を受け付ける方法として」、「開示等の請求等の申出先」を定めることができるので、開示請求をする本人は、当該の申出先に対して開示請求をしなければならないとされています。

### ■対応策：

委託先は委託元に開示等の求めを受けた場合の取扱いを予め確認、取り決め、実施内容を従業員に周知、教育します。

- ・ 委託元の窓口、連絡方法、申請様式等。

### (参考) 対応策の事例：

- ・ 委託元と委託先の役割、及び、本来と異なるルートでの対応が必要となるケースなど、例外的な対応手順も含めて、文書で確認を行う。

- ・ 委託先の裁量の範囲や、範囲を超えた場合の対処策についても確認する。
- ・ 対応の状況を委託元に定期的に報告するとともに、委託先への連絡日時等を含め、対応の状況を記録に残す。

### **ちょっと待って！**

委託された「個人データ」に対して委託先に開示請求などがあったとき、あわてて開示請求に応じるのではなく、本来開示請求などを受けることになっているか確認し、開示請求を受ける立場になりときは請求を受け取らないようにしましょう。

## ケース 10 「開示等請求への対応が遅れ、訴訟を起こされた」

情産協システムズは、万善商事の顧客管理システムの運用を受託しています。

この顧客管理システムで保有している個人データの開示請求の申出先は、万善商事となっています。

あるとき、万善商事が、同社の顧客(個人)の善田氏から、万善商事の顧客管理システムで管理している同氏の個人データを開示するように請求を受けました。

万善商事社内での請求対応が遅れたこともあり、委託先の情産協システムズから万善商事に当該個人データを送付するまでに 2 週間かかり、善田氏の開示請求から 20 日経過後に、個人データを開示しました。

その間、善田氏は、申出受領の連絡後 2 週間を経過しても回答がなかったことから、その翌日開示請求に関する訴訟を万善商事に提起しました。

訴えを起こされた万善商事は、情産協システムズに対して、情産協システムズの対応の遅れが訴訟を招いたとクレームをつけました。

### ■リスク：

開示請求対応への遅れが訴訟提起を招くおそれがあります。

### ■個人情報保護法での規定：

- ・ 個人情報保護法 第 34 条第 1 項

「本人は、(略)、請求に係る訴えを提起しようとするときは、その訴えの被告となるべき者に対し、あらかじめ、当該請求を行い、かつ、その到達した日から 2 週間を経過した後でなければ、その訴えを提起することができない。」とされています。

### ■対応策：

委託先は委託元に次の事項の契約を求めます。

- ・ 保有個人データの開示等にあたり、委託先が通常のオペレーションとは異なる作業を行う必要があるときは、委託元が当該開示等の請求を受理した後、速やかに委託先に対して連絡するなど、委託元の責任で開示等請求者に回答すること。
- ・ 委託元と委託先との間で、開示等請求の回答に関する SLA(サービスレベルアグリーメント)を確認し、かつ合意すること。このとき、SLA は、繁忙期か否かや、開示等請求を受ける個人データの抽出等の難易度などにより変わり得ることを考慮すること。

**(参考) 対応策の事例：**

- ・ 委託元と委託先の役割、及び、本来と異なるルートでの対応が必要となるケースなど、例外的な対応手順も含めて、文書で確認を行う。
- ・ 委託先の裁量の範囲や、範囲を超えた場合の対処策についても確認する。
- ・ 対応の状況は委託元に定期的に報告するとともに、委託先への連絡日時等を含め、対応の状況を記録に残す。

**ちょっと待って！**

開示等の請求への対応が遅れないよう、あらかじめ、開示等請求への対応をどのようにするか、委託元と合意しましょう。

## Appendix(付録)

## 情報サービス産業における個人情報取扱実務チェックシート：【委託元への対応】

| <input checked="" type="checkbox"/> | チェック項目                                                                                                                                                 | 本文<br>ページ |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <input type="checkbox"/>            | 個人データが含まれる可能性があるデータを委託元から受領するとき、委託元に対して、契約書等で、個人データを含む場合はどのデータが個人データに該当するかを明示する義務を課すか、あるいは個人データを含むデータを渡さない旨の特段の取り決めを求めているか。                            | 3、6       |
| <input type="checkbox"/>            | 受領したデータに個人データが含まれるか判断が難しいとき、委託元に対して、個人データを含むか確認を求めているか。                                                                                                | 3、6       |
| <input type="checkbox"/>            | 委託元が個人データを特定かつ明示せずに、個人データを含むデータを委託先に提供したとき、委託元から個人データの取扱いに関して損害賠償請求することがないことを契約書等に記載しているか。                                                             | 10        |
| <input type="checkbox"/>            | 委託元が個人データを特定かつ明示せずに、個人データを含むデータを委託先に提供したとき、当該個人データの本人に対する対応を委託元が行うことを、契約書等に記載しているか。                                                                    | 10        |
| <input type="checkbox"/>            | 委託元から取扱いの委託を受けた個人データが、オプトアウトによって第三者提供を受けた個人データであるとき、場合によっては用途別にサービス提供を停止できるようにあらかじめシステム対応することを、委託元と合意しているか。                                            | 13        |
| <input type="checkbox"/>            | 個人データについて、外国にある企業(外国の第三者)に取扱いを再委託するとき、委託元に対して、その個人データの取扱いについて海外に委託することについて本人の同意を得ているか確認する、又は再委託先の外国にある企業の個人情報の取扱い体制やその企業への監督方法について合意するなど、適切な措置をとっているか。 | 17        |
| <input type="checkbox"/>            | 個人データの取扱いの委託を受けたとき、委託元と、委託元から受ける監査のレベル(回数、立入検査の有無、実施内容等)を明確化しているか。                                                                                     | 21        |
| <input type="checkbox"/>            | 個人データの取扱いの委託を受けたとき、委託元と、委託元から受ける監査の手続きを、再委託先があるときはそれも含め、定めているか。                                                                                        | 21        |
| <input type="checkbox"/>            | 個人データの取扱いの委託を受けたとき、委託元との間で、漏えい等があったときの緊急連絡ルートを複数系統設けているか。                                                                                              | 28        |
| <input type="checkbox"/>            | 個人データの取扱いの委託を受けたとき、委託元の協力を受け、定期的な緊急時対応訓練を実施するようにしているか。                                                                                                 | 28        |
| <input type="checkbox"/>            | 取扱いを受託している個人データに対して開示等請求を受けたとき、委託先が通常の実業とは異なる作業を行う必要があるときは、委託元がその開示等請求を受理した後、速やかに委託先に対して連絡するなど、委託元の責任で請求を行った本人に回答することを、委託元に求めているか。                     | 33        |
| <input type="checkbox"/>            | 取扱いを受託している個人データに対して開示等請求を受けたとき、委託元と委託先との間で、開示等請求の回答に関する SLA(サービスレベルアグリーメント)を、繁忙期や個人データの抽出の難易度等を考慮して、確認し、かつ合意しているか。                                     | 35        |
| <input type="checkbox"/>            |                                                                                                                                                        |           |

## 情報サービス産業における個人情報取扱実務チェックシート：【委託先の対応】

| <input checked="" type="checkbox"/> | チェック項目                                                                                        | 本文<br>ページ |
|-------------------------------------|-----------------------------------------------------------------------------------------------|-----------|
| <input type="checkbox"/>            | 特段の取り決めが委託元との間で結ばれていないときは、個人データが含まれるようなデータを委託元から受領しないこととしているか。                                | 3,6       |
| <input type="checkbox"/>            | 受領する予定のデータの内容を確認し、あらかじめ特段の取り決めがないにも関わらず個人データが含まれるおそれがあるときは、速やかに委託元と協議し、そのデータを受領しないこととしているか。   | 3,6、9     |
| <input type="checkbox"/>            | 受領した後に速やかにデータの内容を確認し、あらかじめ特段の取り決めがないにも関わらず個人データが含まれるおそれがあるときは、速やかに委託元と協議し、そのデータを返却することとしているか。 | 3,6、9     |
| <input type="checkbox"/>            | 受領した後に個人データであることがわかったとき、アクセス制御など個人データに関する安全管理措置を適用することとしているか。                                 | 3,6、9     |
| <input type="checkbox"/>            | 受領した後に個人データであることがわかったとき、その個人データを含むデータを、委託元と協議し、返却することとしているか。                                  | 3,6、9     |
| <input type="checkbox"/>            | 必要があってテストデータ等として個人データを受領するときは、個人データに対する管理体制を整えてから受領しているか。                                     | 3,6、9     |
| <input type="checkbox"/>            | オプトアウトによって第三者提供を受けた個人データを用いたサービスを行うときは、用途別にサービス提供を停止できるようにあらかじめシステム対応しているか。                   | 13        |
| <input type="checkbox"/>            | 外国の企業に個人データの取扱いを委託するときは、法令に従い、あらかじめ本人から同意を得たり、適切な体制を整備している外国企業に委託するといった対応をしているか。              | 17        |
| <input type="checkbox"/>            | 取扱いを受託している個人データに対して当該個人データの本人からの開示等の請求を受けたときは、委託元に対して請求するよう促すよう社内周知しているか。                     | 33、<br>35 |
| <input type="checkbox"/>            |                                                                                               |           |

**情報サービス産業における個人情報取扱実務チェックシート：【再委託先への対応】**

| <input checked="" type="checkbox"/> | チェック項目                                                                                                                                                                   | 本文<br>ページ |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <input type="checkbox"/>            | (再)委託先が講じる安全管理措置の内容については、(再)委託先に任せきりにせず、(再)委託先に対して適切な監督を行うようにしているか。具体的には、個人データの漏えい、滅失または毀損の防止その他の個人データの安全管理のために、必要かつ適切な、組織的、人的、物理的、技術的の各観点での安全管理措置が継続的に行われていることを確認しているか。 | 23        |
| <input type="checkbox"/>            | JISA 個人情報保護モデル契約(改訂第2版)に基づき、(再)委託先との間の契約を見直し、再委託の場合は委託元からの監査と、委託先からの監査が実施できるようにしているか。                                                                                    | 21        |
| <input type="checkbox"/>            | 再委託先からの再々委託は原則禁止とし、やむを得ず再々委託するときは、必ず委託元も含めて再々委託を実施する旨の報告を求めるとともに、再委託先に対するものと同様の監査及び安全管理措置の実施を求めているか。                                                                     | 23        |
| <input type="checkbox"/>            |                                                                                                                                                                          |           |



—禁無断転載—

29-J003

改正個人情報保護法

情報サービス事業者における実務上の留意点

～こんなときどうする？確認のためのケーススタディ～

平成 30 年 5 月発行

発行：一般社団法人情報サービス産業協会

〒101-0047 東京都千代田区内神田 2-3-4 S-GATE 大手町北 6 階

TEL 03-5289-7651

URL <http://www.jisa.or.jp/>

©Copyright, Japan Information Services Industry Association, 2018

