日本DPO協会
勉強会資料

CBPR認証の意義と近時の取得動向について
～改正個人情報保護法への対応など～

2022年3月17日
（一財）日本情報経済社会推進協会
常務理事　坂下哲也

自己紹介

JIPDEC

- （一財）日本情報経済社会推進協会（**JIPDEC**）　常務理事
  【所管】電子情報利活用研究部・認定個人情報保護団体
  - 芝浦工業大学　情報通信工学科　非常勤講師（通信システム設計論）
- 日頃やっている業務
  - 電子情報の保護と利用に関する基盤整備の企画・推進
    - G空間（地理空間情報）、IoT（Internet of Things）、ブロックチェーン（分散型台帳技術）、PDS（Personal Data Store）、デジタル・トランスフォーメーションなど
  - データの利用やプライバシー保護に関する制度研究など
- 政府委員等
  - デジタル庁における入札制限等の在り方に関する検討会委員
  - 宇宙政策委員会専門委員
  - 国立研究法人審議会臨時委員（JAXA部会部会長）
  - 準天頂衛星システム事業推進委員会委員
  - シェアリングエコノミーサービス検討会議委員
  - ISO／IEC JTC1 SC27／WG5（Information Security, Cybersecurit／プライバシー技術）委員など

- 最近の著作
  - **「信頼に基づくデータ流通の基盤に関する考察」（畠山久志監修『デジタル化社会における新しい財産的価値と信託』、商事法務、2022）**
- その他
  - （一社）JcoMaaS理事、（一社）ピープルアナリティクス＆HRテクノロジー協会理事　など。

はじめに

- 令和2・3年改正個人情報保護法の施行まで2週間余りとなりました。
- 今回の改正では海外へ個人データを移転する際の情報提供などについて事業者が行う必要がある点が追加されています。
- 当協会認定個人情報保護団体では、2017年からAPEC／CBPRの認証機関（AA：アカウンタビリティエージェント）を務めておりますが、問い合わせや申請も増えてきました。
- 本日は、現在のCBPRの状況や、域外移転に関係する制度状況などを報告させていただきます。
- 皆様のご参考になれば幸いです。

アジェンダ

- 令和２年改正個人情報保護法　ガイドラインの概要
- 認定個人情報保護団体とCBPR
- 企業において確認して欲しい点

令和２年改正個人情報保護法ガイドラインの概要

令和２年改正個人情報保護法　ガイドラインの概要(1)

テーマ	法・政令・規則改正の内容	ガイドラインの改正内容
利用停止等	一部の法違反の場合に加えて、本人の権利又は正当な利益が害されるおそれがある場合にも拡充する	• **本人の権利又は正当な利益が害されるおそれがある場合**について、利用停止等が認められる事例や認められない事例を含め解釈を具体的に記載 ➢ 利用停止等が認められる事例…ダイレクトメール送付停止を求めたにもかかわらず、繰り返し送付される場合 ➢ 認められない事例…電話会社からの料金支払いを免れるため、課金に必要な情報の利用停止等を請求する場合
漏えい等報告・本人通知	漏えい等が発生し、個人の権利利益を害するおそれがある場合（要配慮個人情報、財産的被害が発生するおそれがある漏えい等）に、委員会への報告（速報・確報の２段階）及び本人通知を義務化する	• **委員会への報告を要する事態**について、事例を含め解釈を具体的に記載するとともに、**委員会への速報・確報の時間的制限の考え方**等を記載 ➢ 財産的被害が発生するおそれがある漏えい等に該当する事例…ECサイトからクレジットカード番号が漏えいした場合 ➢ 速報の時間的制限の目安として、事態の発生を知った時点から概ね3日～5日以内（確報については、規則において原則30日以内と規定）
不適正利用の禁止	違法又は不当な行為を助長する等の不適正な方法により個人情報を利用してはならない旨を明確化する	• **不適正な方法による個人情報の利用に該当すると考えられる場合**について、事例を含めて解釈を具体的に記載 ➢ 該当する事例…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

令和２年改正個人情報保護法　ガイドラインの概要(2)

テーマ	法・政令・規則改正の内容	ガイドラインの改正内容
認定団体制度の充実	現行制度に加え、企業の特定分野（部門）を対象とする団体を認定できるようにする	• 今般の法改正も契機に、**認定団体の望ましい取組の方向性**を示すためのガイドラインを認定団体編として新設 • 制度の目的・意義に加え、①求められる具体的な業務（苦情処理、情報提供等）、②自主ルールの策定等、③漏えい等報告等について記載
公表事項等	安全管理のために講じた措置を法定公表事項に追加する	• 安全管理の観点から公表すべき事項として、個人データの取扱いに関する責任者を設置している旨、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ている旨等を記載 • 外国の制度等を把握した上で、安全管理措置を講ずべき旨を明確化 • 現行法で義務付けられている利用目的の規定に関し、本人が合理的に予測等できないような個人データの処理（ex.いわゆる「プロファイリング」）が行われる場合、本人が予測できる程度に利用目的を特定しなければならない旨を明確化
仮名加工情報	「仮名加工情報」を創設し、利用を内部分析等に限定することを条件に、利用目的の変更の制限等を緩和する	• **仮名加工情報の加工基準等**について、事例を含め解釈を具体的に記載 ➢ 仮名加工情報の加工基準に従った加工の事例…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：氏名を削除

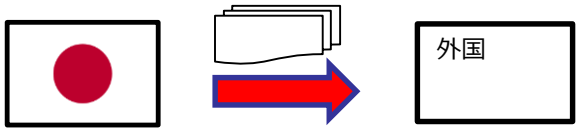
令和２年改正個人情報保護法　ガイドラインの概要(3)

テーマ	法・政令・規則改正の内容	ガイドラインの改正内容
個人関連情報	提供先において個人データとなることが想定される情報の第三者提供について、本人同意が得られていること等の確認を義務付ける	• **同意取得の主体**、**同意取得の方法**等について、事例を含め解釈を具体的に記載 ➢ 同意取得の主体…原則、情報を利用する主体となる提供先が同意を取得する ➢ 同意取得の方法…同意取得にあたっては、対象となる個人関連情報の範囲を示した上で、明示の同意を要する
越境移転	• 本人同意に基づく越境移転： 同意の取得時に、本人への情報提供を求める • 体制整備要件に基づく越境移転：移転先による個人データの適正な取扱いの継続的な確保のための「必要な措置」及び本人の求めに応じた情報提供を求める	• **同意取得時の情報提供、体制整備要件に基づく越境移転時に移転元が講ずべき「必要な措置」**について、事例を含め解釈を具体的に記載 ➢ 同意取得時に提供すべき情報の考え方…本人がリスクを適切に把握できるよう、 ✓ 移転先が所在する外国の名称、 ✓ 個人情報保護制度等に関して、我が国の制度や我が国事業者に求められる措置との本質的な差異 についての情報提供を求める ➢ 体制整備要件に係る「必要な措置」… ✓ 年一回程度、移転先における個人データの取扱状況及びこれに影響を及ぼすおそれのある外国制度の有無等を確認、 ✓ 契約違反等の問題が生じた場合には、その是正を求める ✓ 問題が解消されず適正な取扱いの継続的な確保が困難となった場合は、個人データの提供を停止

※　その他、開示方法、第三者提供記録の開示、オプトアウト規定、域外適用等の改正法に係る解説を追加するなどの所要の改正を実施
※　個人情報保護員会HP　ガイドライン・QA等：https://www.ppc.go.jp/personalinfo/legal/#anc_Guide

越境移転について

■ 外国にある第三者への個人データの提供時に、**移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等**を求める。

現　行	改正後
	各要件に基づく移転時、それぞれ以下を義務付け
外国にある第三者に個人データを提供できる要件 本人の同意	本人からの同意取得時に、以下の情報を提供（§24②） ・ 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**
基準に適合する体制を整備した事業者	① 移転元に対し以下の「必要な措置」を求める ・ 移転先における**適正取扱いの実施状況等の定期的な確認** ・ 移転先における適正取扱いに**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」に関する情報を提供（§24③）
我が国と同等の水準国（ＥＵ、英国）	

※この他、「法令に基づく場合」等の例外要件あり。
個人情報保護委員会の資料をJIPDECで一部編集

第24条の定める内容

■ 第24条の内容

- **外国にある第三者への個人データの提供する際には、**移転先事業者における個人情報の取扱いについて、**取得する本人へ情報提供の充実**を行わなくてはならない。

■ 要件

- その１
  - **外国にある第三者に個人データを提供する際に、個人の同意を取る。**
  - その時に、①移転先の所在国の名称、②当該外国における個人情報の保護に関する制度、③移転先が講ずる個人情報の保護のための措置を伝えなくてはならない。
- その２
  - **個人情報保護委員会が認めた基準に適合する体制を整備した事業者**に提供する場合、
    - 事業者は、①移転先における適正取扱いの実施状況等の定期的な確認、②移転先における適正取扱いに問題が生じた場合の対応を行わなくてはならない。
    - 本人から求めがあれば、「必要な措置」に関する情報を提供しなくてはならない。
- 例外
  - 個人情報保護委員会が日本と同水準の保護制度を持っているEUや英国への移転は除く。

第27条の定める内容

■ 27条及び政令第8条の概要及び改正内容

- 令和2年の改正に伴い、第27条・政令第８条の規定に基づく『**外的環境の把握を含む保有個人データの安全管理のために講じた措置を、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とされました。
  - 但し、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については、その必要ありません。

■ 27条の内容

- 外的環境の把握として、外国において個人データを取り扱う以下のような場合、外国の個人情報の保護に関する制度等を把握する必要があります。
  - 外国にある支店・営業所に個人データを取り扱わせる場合
  - 外国に支店等を設置していない場合であっても、外国にある従業者に個人データを取り扱わせる場合
  - 外国にある支店等や従業者が、日本国内に所在するサーバに保存されている個人データにアクセスして、これを取り扱う場合
  - 外国にある第三者に個人データの取扱いを委託する場合
  - 委託先が外国にある第三者に個人データの取扱いを再委託する場合
  - 委託先や再委託先が、日本国内に所在するサーバに保存されている個人データにアクセスして、これを取り扱う場合
  - 外国にある第三者の提供するクラウドサービスを利用する場合
    - 日本国内に所在するサーバに個人データが保存される場合においても同様
    - 但し、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は、個人データの第三者への「提供」には該当しません
- 外国の制度等を把握して安全管理措置を講じる場合には、「保有個人データの安全管理のために講じた措置」として、支店等、従業者、委託先が所在する外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を本人の知り得る状態に置く必要があります。
  - なお、個人データが保存されるサーバが所在する国を特定できない場合には、サーバが所在する外国の名称に代えて、サーバが所在する国を特定できない旨及びその理由、及び、本人に参考となるべき情報を本人の知り得る状態に置く必要があります。

第28条の定める内容

■ 28条の概要及び改正内容

- **外国にある第三者への個人データの提供する場合には、**原則として、外国にある第三者への個人データの提供を認める旨について、本人の事前同意を得ることが義務付けられている。令和２年改正により、本人の同意を得ようとする場合等についての情報提供の充実が定められました。

■ 28条の内容

- 原則：外国にある第三者に個人データを提供する場合には、あらかじめ本人の同意を得なければならなりません。

  ※改正により、同意を得ようとする場合には、①移転先の外国の名称、②当該外国における個人情報の保護に関する制度に関する情報、③移転先が講ずる個人情報の保護のための措置に関する情報を伝えなくてはならないとされました。

- 例外：以下のいずれかの場合には、本人の同意を得る必要はない。

  ①日本と同等の水準にあると個人情報保護委員会規則で定める外国にある第三者に提供する場合

  ②個人情報取扱事業者が講ずべき措置に相当する措置（相当措置）を継続的に講ずるために必要な個人情報保護委員会で定める体制を整備している者に提供する場合

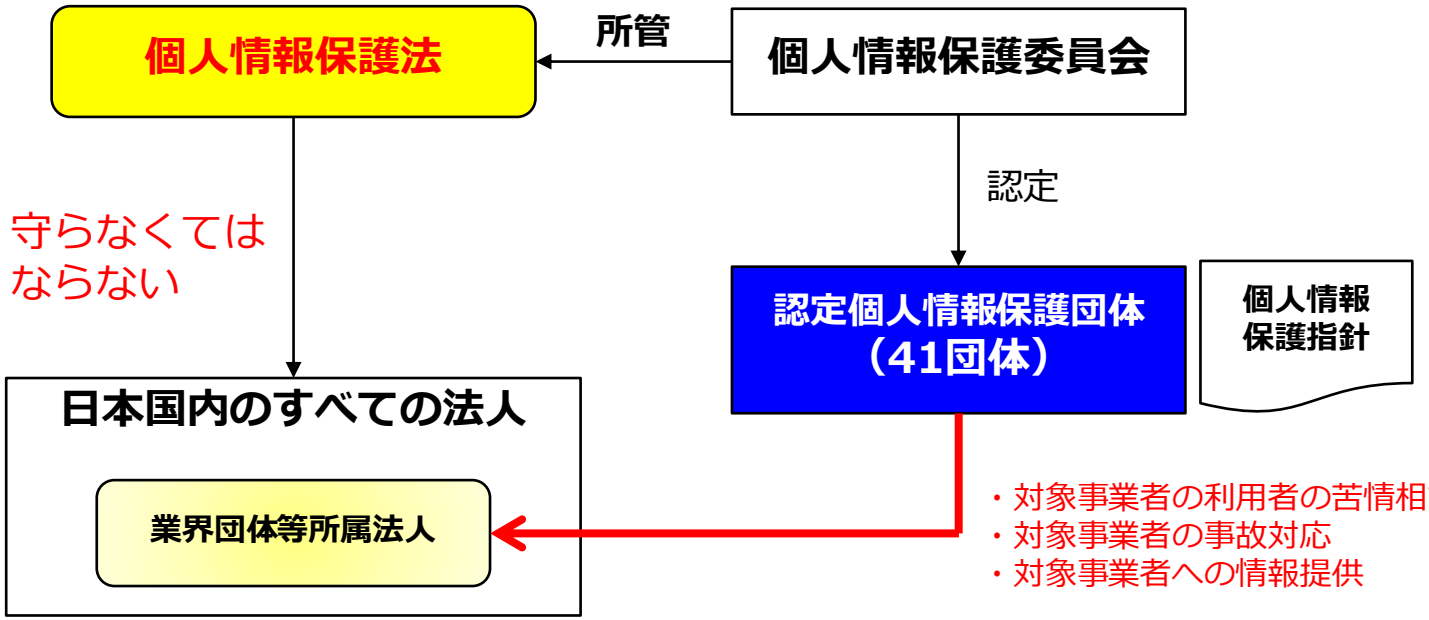
  ③特定の条件に該当する場合

  ※ 改正により、提供する者は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とらなければならず、また、本人から求めがあれば必要な措置に関する情報を提供しなければならないとされました。

認定個人情報保護団体とCBPR

認定個人情報保護団体

- 認定個人情報保護団体は、個人情報保護法を所管する個人情報保護委員会より認定を受ける。
- 認定を受けた認定個人情報保護団体は指針（グループ内のルール）を作成し、傘下の企業に遵守を求める。（指針作成は努力義務）
- また、**消費者等との苦情の仲介や、事故対応**を行う。
- 更に、当協会は**APEC／CBPR（越境プライバシールール：Cross-Border Privacy Rules）の認証**も実施。（認証企業：3社）



（認定個人情報保護団体一覧：https://www.ppc.go.jp/personalinfo/nintei/list/）

APEC（アジア太平洋経済協力）の取り組み

■ **APECプライバシーフレームワーク**（2004年10月採択）21エコノミー

APEC加盟エコノミーにおける整合性のある個人情報保護への取組を促進し、情報流通に対する不要な障害を取り除くことを目的として制定。

- 人口では世界の41.4%、GDP（国内総生産）では57.8%、貿易額では47%

■ **CPEA（越境執行協力協定）** 2009年11月 11エコノミー

- エコノミー内での情報の取得と管理について、国内の法規や指針を対象に参加国で対応
- 米国、日本、韓国、シンガポール、カナダ、メキシコ、豪州、台湾、フィリピン、ニュージーランド、香港

■ **CBPR（越境プライバシールールシステム）** 2011年11月 9エコノミー

- 運用するための仕組みとしての CBPRシステム（APEC越境プライバシールールシステム、APEC Cross Border Privacy Rules System）
- 米国、日本、韓国、シンガポール、カナダ、メキシコ、豪州、台湾、フィリピン

プライバシー執行機関間の有効な越境的協力

■ **AA（アカウンタビリティ・エージェント）** 5エコノミー（2021年12月時点）

米国、日本、韓国、シンガポール、台湾

APECの方針

- APEC地域の参加エコノミー間の要求事項であるが、同じ手続き等を適用することが推奨されている。
- APEC CBPR認定とは（APECサイト）
  http://cbprs.org/business/
  - **CBPRシステムは、APEC地域の参加エコノミー間で個人情報を交換するために、単一フレームワークを提供することで参加エコノミー間の差異を埋める。**
- Policies, Rules and Guidelines（APEC文書）
  http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf
  - **CBPRの要求事項ではないが、APEC参加エコノミー域外へ転送する際でも、同じプライバシーポリシーと手順を適用することを推奨する（P4 脚注10）。**
  -

CBPR取得のメリット

- 官民連携したCBPR認証を取得することにより、事業運営においてCBPRシステムに適合した越境データの取り扱いを行っていることを示すことを対外的にアピール可能**【認証シール】**
- CBPR認証取得企業ならば、越境データ移転において個人情報がより安全に取り扱われているという認識が、ステークホルダーにて醸成されていくことが期待される。CBRP認証取得事業者が優位な立場を得られる**【データトラスト訴求】**
- 他国企業で調達条件に入るケースもあり、越境データ移転のトラストが重要視される傾向へシフト**【調達要件】**
- 認証事業者に対して、APEC域内からの苦情・相談等について、必要に応じてアカウントエージェントが調整を行う**【苦情対応】**

審査プロセス

■ CBPR認証審査の手続き：　約４ケ月間

項目	実施内容
①審査前 申請受付	・申請書類の受け取り ・審査費用の受領
②文書審査	・APEC質問表、JIPDEC質問表の確認 ・確証資料による実績確認
③ヒアリング（コロナ禍はリモート）	・不明点の確認、追加資料の確認 ・指摘事項の改善状況の確認
④現地審査	・経営者、実務担当者へのインタビュー ・安全管理措置の現場確認
⑤認証審査会 （リモート会議）	・外部有識者３名（学識者、弁護士、消費者団体）による審査結果の妥当性評価
⑥審査後 認証付与	・契約書の締結 ・運用管理費の受領

各国の状況

■ AA（アカウンタビリティ・エージェント：認証機関）の状況

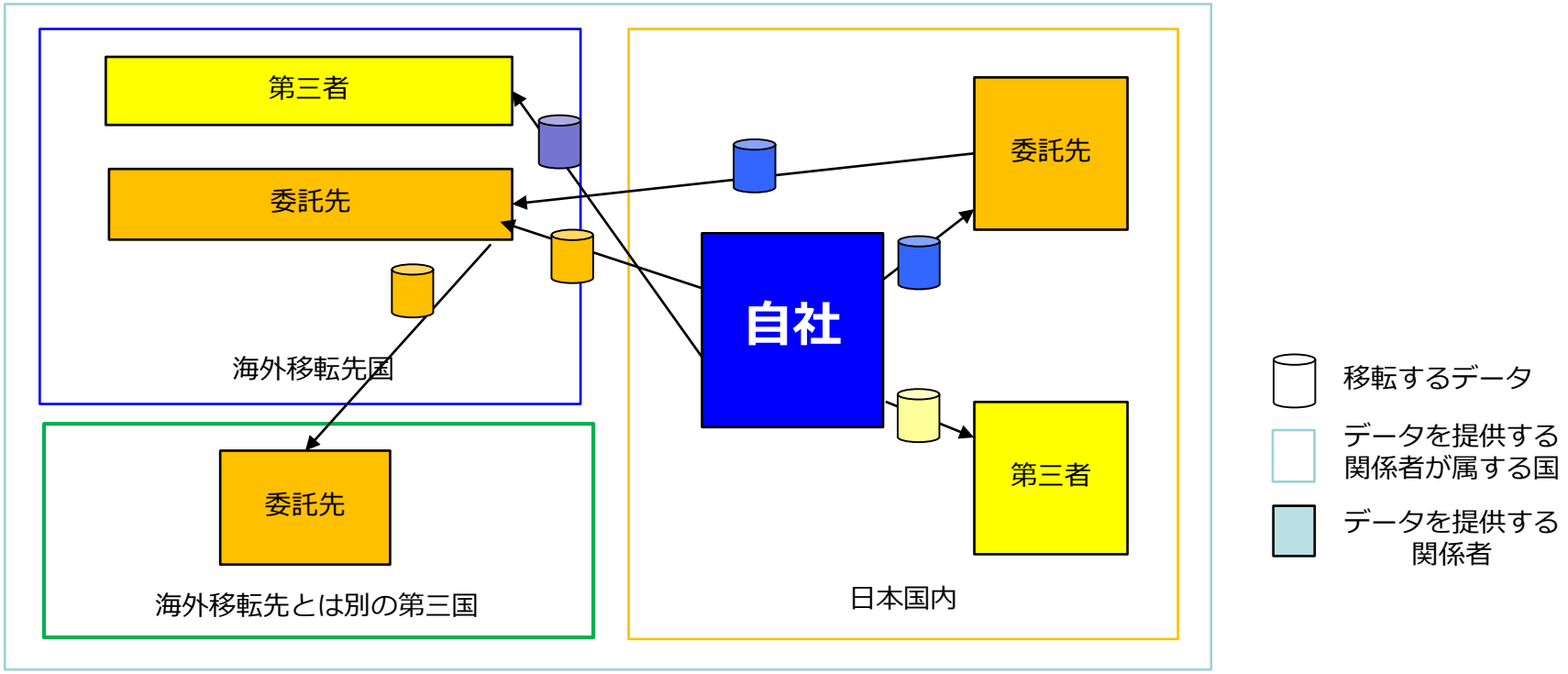
国名	ＡＡ名	CBPR認証　取得事業者数	PRP認証　取得事業者数
米国	TrustArc	３２	２２
	Schellman	1	4
	NCC Group	3	3
	HiTrsut	―	―
	BBB National Programs	3	2
シンガポール	IMDA	6	2
韓国	KISA	―	―
台湾	資訊工業策進会	―	―
日本	**JIPDEC**	**3**	**―**
合計		４8社	３３社

※日本の認証取得事業者
インタセクトコミュニケーションズ、Paidy、YahooJapan
その他審査中１社、申請準備中２社。

改正法施行前に企業で確認する点

事業者からの相談から気付く点

- 当協会認定個人情報保護団体では、対象事業者であっても、対象事業者以外であっても、データ利用等についての問い合わせに対応している。
  - 対象事業者ではない事業者の域外移転についての相談で目立つ点
    - 自社の個人データについて、『何が、どこにあるのか』を可視化できていない。
      - データをマッピングする事を推奨している。



作成したデータマッピングのイメージ図

データマッピングをしないと何が困るのか。

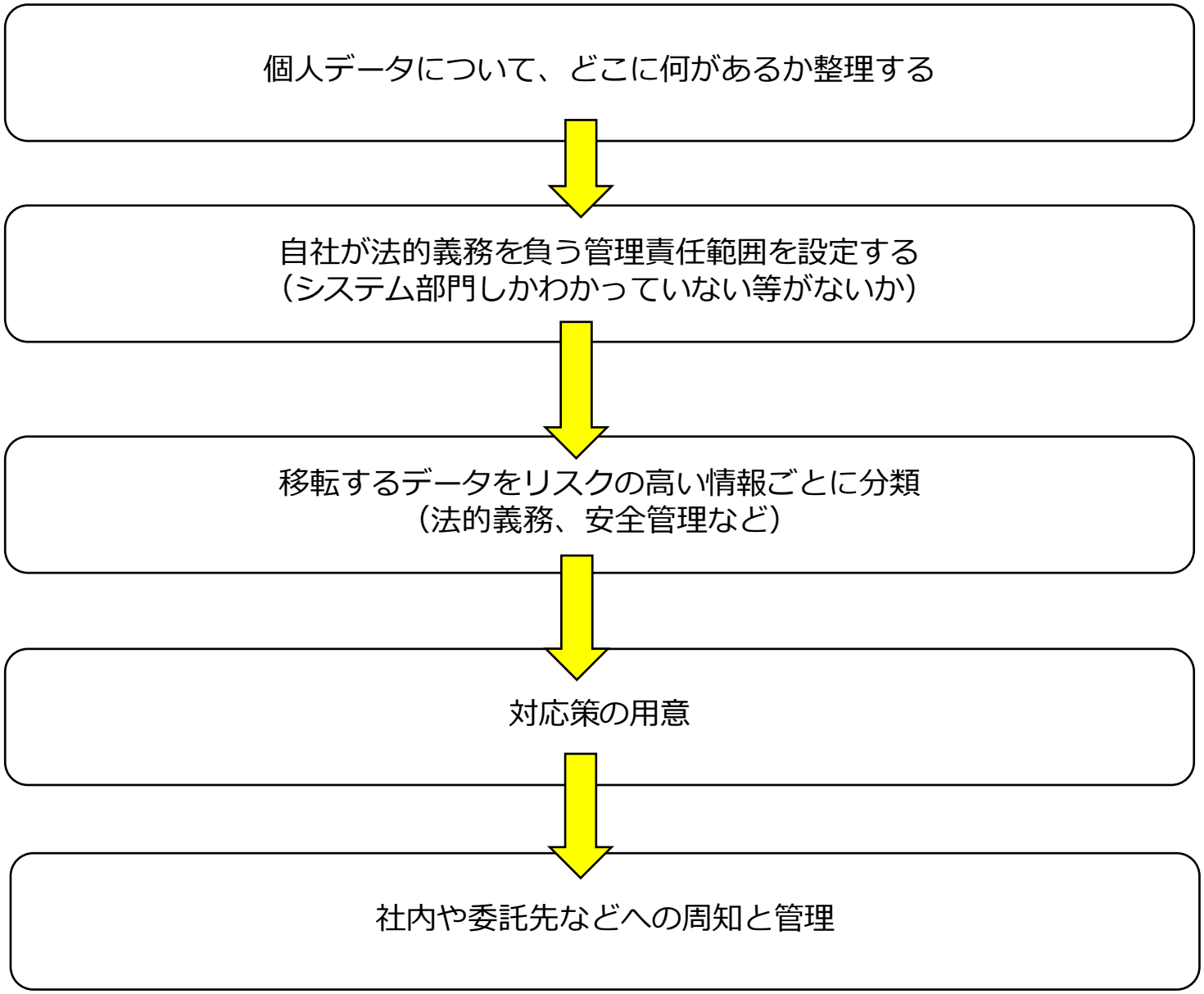
■ 実際の事例

- 知らない間に国内の委託先を通じて、海外第三国へ個人データが渡っていたことによって、顧客に海外事業者から無断で連絡が届き、お客様から同意違反であると問い合わせが届いた。

- 委託先が契約を無視してセキュリティ対策が不十分な海外の再委託先へ個人データを移転していたので、再委託先で情報漏洩が起こった。

- クラウド事業者のサーバー設置先が、日本と同等レベルのプライバシー保護が達成できない国だったため、政府機関から注意を受けた。

データマッピングの仕方の例



ありがとうございました