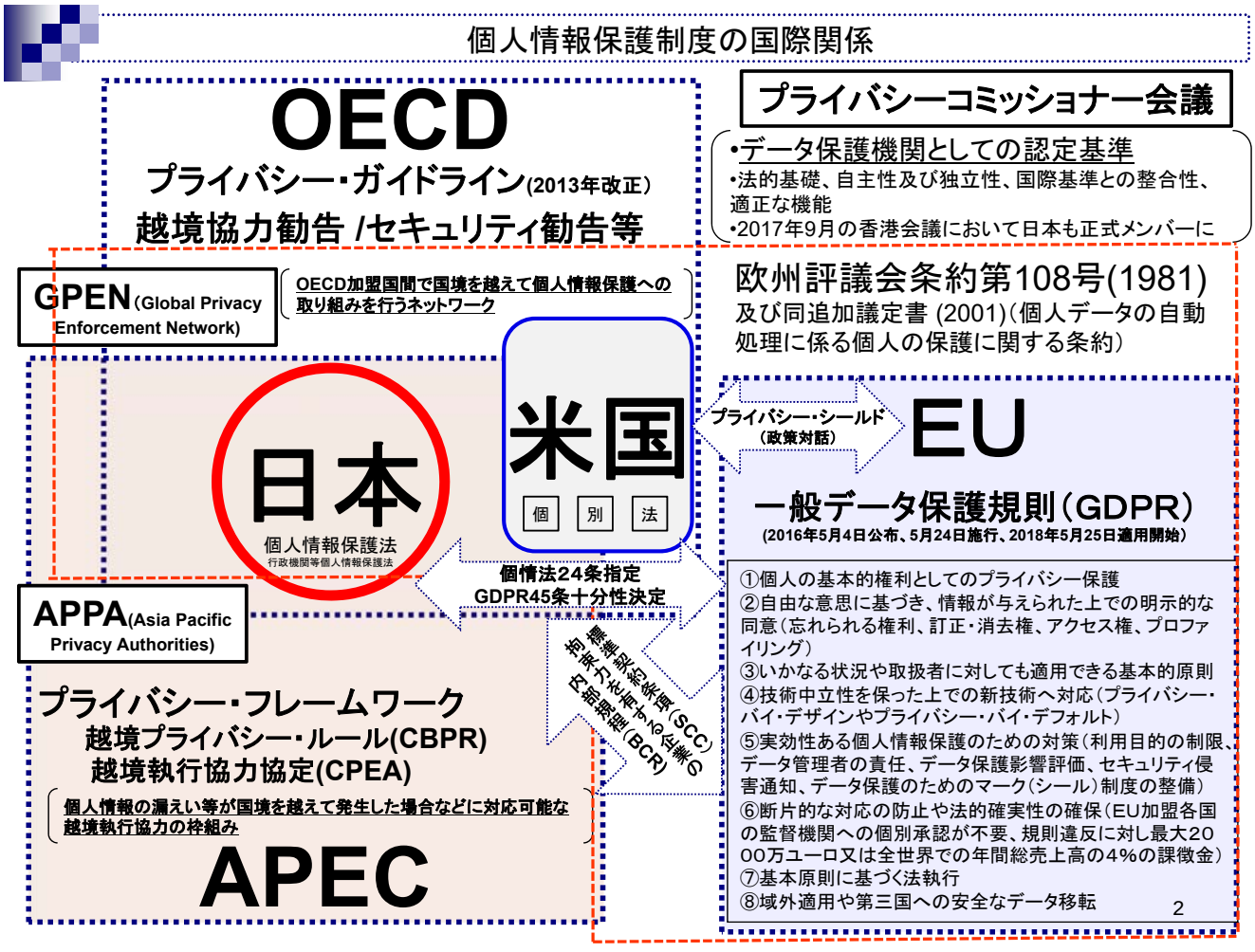
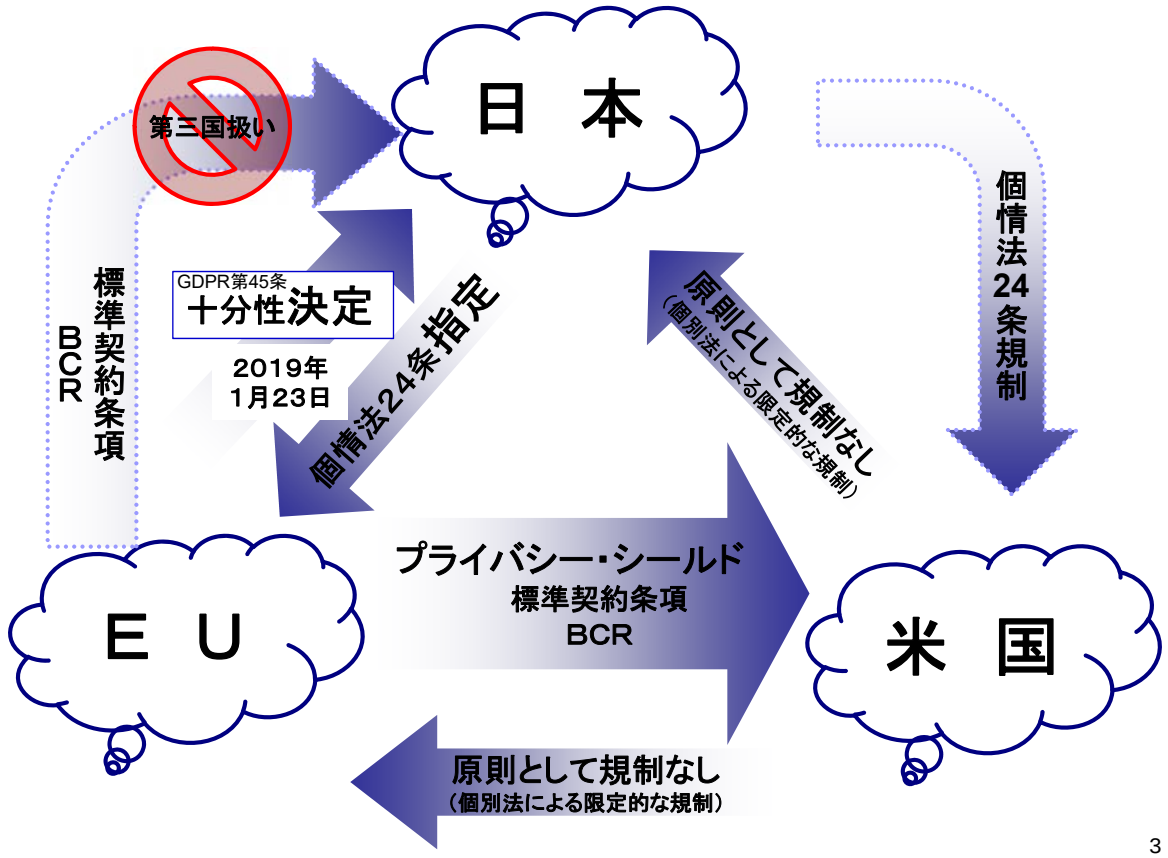
データ移転をめぐる国内外における制度的枠組みの構図

The Current International Structure and Framework for Onward Data Transfer

慶應義塾大学　総合政策学部　教授
新保 史生



個人データの移転をめぐる国際的な制度



©2019 SHIMPO Fumio

個人情報法第24条の構造（外国の第三者への個人データの提供）

■ 個人情報取扱事業者は、

① 外国（本邦の域外にある国又は地域をいう。以下同じ。）

（個人の権利利益を保護する上で⑤我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。以下この条において同じ。）にある

② 第三者

（個人データの取扱いについてこの節の規定により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ために必要なものとして⑥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を除く。以下この条において同じ。）に

個人データを提供する場合には、

⑦前条第1項各号に掲げる場合を除くほか、

あらかじめ ③ 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。

④ この場合においては、同条の規定は、適用しない。

外国／外国にある第三者とは

① 外国とは

- 本邦の域外にある国又は地域

② 外国にある「第三者」とは

- 個人データを提供する個人情報取扱事業者と当該個人データによって識別される本人以外の者が外国にある第三者であること （個人、事業者、外国政府など）

第三者に該当

- 外国の法人格を取得している当該企業の現地子会社
- 提供元の個人情報取扱事業者と法人格が別の関連会社や子会社

- 日本の法人格を有する当該事業者の外国支店等は第三者には当たらない（同一法人格内での個人データの移動）
- 外国法人が個人情報取扱事業者に該当する場合（日本国内に事務所を設置している場合、日本国内で事業活動を行っている場合）

④ この場合においては、同条の規定は、適用しない。 （同条＝23条）

委託、事業承継又は共同利用（法第23条第5項各号に掲げる場合）に伴って、外国にある第三者に個人データを提供するときであっても、法第24条が適用される
（原則、**③本人同意**が必要：記録義務も免除されない）

③ 本人同意に基づく提供 （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）

24条の同意不要 ↓ 23条が適用される

⑤ **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への提供** — 除く

⑥ 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を整備している第三者への提供 — 除く

- ※必要な体制が整備されているかについては、個人情報保護委員会に対して事前の届出等は不要

本人同意 / オプトアウト / 委託 事業承継 共同利用

① 提供先において個人情報取扱事業者の義務に相当する措置を講じていること

② 提供先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（アジア太平洋経済協力（APEC）の越境プライバシールール（CBPR）システム）

本人同意不要

⑦ 法第23条第1項各号に該当する場合（第三者提供に係る義務の適用除外規定） — 除く

①法令（外国法令は含まず）、②生命・身体・財産、③公衆衛生、④法定事務

日EU間の相互の円滑な個人データ移転を図る枠組みの発効

「個人情報保護法第24条に係る委員会規則」の内容

個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国

外国指定に当たっての5つの判断基準 （日本による指定の基準）

- ①個人情報保護法に定める個人情報取扱事業者の義務に関する規定に相当する法令その他の規範があること、また、これらを遵守する態勢が認められること
- ②独立した個人情報保護機関が存在し、当該機関が必要な監督を行うための執行態勢を確保していること
- ③個人情報の適正な活用と個人の権利利益保護に関する相互の理解、連携及び協力が可能であること
- ④個人情報の保護を図りつつ相互の円滑な移転を図る枠組みの構築が可能であること
- ⑤我が国としてその外国を指定する必要性が認められること

個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国等
（平成31年個人情報保護委員会告示第１号）

欧州経済領域協定に規定された国（個人情報保護法第24条指定国）

- ◆ *アイスランド*
- □ アイルランド
- □ イタリア
- □ 英国
- □ エストニア
- □ オーストリア
- □ オランダ
- □ キプロス
- □ ギリシャ
- □ クロアチア
- □ スウェーデン
- □ スペイン
- □ スロバキア
- □ スロベニア
- □ チェコ
- □ デンマーク
- □ ドイツ
- ◆ *ノルウェー*
- □ ハンガリー
- □ フィンランド
- □ フランス
- □ ブルガリア
- □ ベルギー
- □ ポーランド
- □ ポルトガル
- □ マルタ
- □ ラトビア
- □ リトアニア
- ◆ *リヒテンシュタイン*
- □ ルーマニア
- □ ルクセンブルク

欧州経済領域（EEA)EU28カ国＋ ◆ 3カ国

個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール

（GDPR45 条決定による効力発生日から適用：2019年1月23日）

(1) 要配慮個人情報（法第2条第3項関係）

(2) 保有個人データ（法第2条第7項関係）

(3) 利用目的の特定、利用目的による制限
（法第15条第1 項・法第16 条第1 項・法第26 条第1 項・第3 項関係）

(4) 外国にある第三者への提供の制限（法第24条・規則第11条の2関係）

(5) 匿名加工情報（法第2条第9項・法第36条第1項・第2項関係）

変更の内容

- 近年の個人データの流通の国際化や、情報セキュリティ対策の重要性等を踏まえ、以下の内容を追加する変更

① 国際的な整合性への対応

- 法第6条に基づき、個人情報保護委員会が、国際的に整合のとれた個人情報に係る制度を構築するために必要な措置を講ずること

② 個人データに対する不正アクセス等への対応

- 情報セキュリティ対策として、個人情報保護委員会とNISC等の各省庁・関係機関との連携を行うこと

③ グローバルな視点での監督

- 経済・社会活動のグローバル化及び情報通信技術の進展に伴って増大する、個人情報を含むデータの国境を越えた流通及び利用に関して、個人情報保護委員会が多角的な視点で対応すること

（2）事業者の保有する個人情報の保護の推進

② 個人データの円滑な国際的流通の確保のための取組

- 個人情報保護委員会は、個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している国との間で、相互に円滑な個人データの移転を図るために、国際的に整合のとれた個人情報に係る制度を促進する方法としての枠組みを構築するための措置を講ずることとする。
- 個人情報保護委員会は、個人情報保護法を所管する機関として、外国から移転される個人情報の適正な取扱いを確保する観点から、法第6条に基づき、日本と当該外国との間の制度及び運用の差異を埋めるために必要な措置を講ずる権限を有している。個人情報保護委員会は、必要に応じ、法及び政令で規定された規律（例えば、要配慮個人情報や保有個人データの定義に係る規律等）を補完し上回る、拘束力のある規律、すなわち、国内の個人情報取扱事業者に対して執行可能な、より厳格な規律を設けることを含め、一層の個人情報の保護を行う権限を有している。
- また、個人情報保護委員会は、当該外国当局との執行協力及び法制度の理解に関する対話を行うこととする。

（4）個人情報の保護及び円滑な流通を確保するための国際的な取組

- 1の（3）の国際的な協調の観点から、個人情報保護委員会において、個人情報の保護を図りつつ、国際的なデータ流通が円滑に行われるための環境を整備するため、国際的な協力の枠組みへの参加、各国執行当局との協力関係の構築等に積極的に取り組むものとする。
- また、個人情報保護委員会は、情報通信技術の進展や個人情報を含むデータの国境を越えた流通の増大を受け、法第75条の趣旨を踏まえ、必要に応じて海外執行当局と連携し、国内にある者に対して物品や役務の提供を行う外国事業者における個人情報の適正な取扱いを確保するため、適切な対応を行うものとする。

（5）個人データに対する不正アクセス等への対応

- 1の（4）の情報セキュリティ対策の観点から、個人情報保護委員会は、個人情報取扱事業者の保有する個人データの外部からの不正アクセス等による漏えい等のリスクの低減、事案への適切な対応を図るため、内閣官房内閣サイバーセキュリティセンター（NISC）等の関係省庁及び情報セキュリティ関係機関と緊密に連携する。

European Union（欧州連合）一般データ保護規則（GDPR）

GDPRとは

General Data Protection Regulation

- 正式名称、「一般データ保護規則（個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則）」
- 2016年5月24日に施行、2018年5月25日からEU加盟国への適用開始
- EUの個人情報保護制度は、個人の基本的権利として個人データを保護する特徴を有する制度
  - 1993年11月1日に欧州連合条約（マーストリヒト条約）が発効し欧州連合（EU）が発足
    - 欧州域内で国ごとに異なる法制度（規制）のレベルを一定にするための取り組み
    - 個人データ保護のための取り組みは、「個人データ保護95/46/EC指令」(1995)が端緒

European Union（欧州連合）一般データ保護規則（GDPR）の検討過程

1995年：「EU個人データ保護指令」の採択
1998年：同履行期限
2009年：EU個人データ保護指令の見直しに関する検討開始
2010年11月：見直しの基本的方向性に関する文書公表
2012年1月25日：「EU個人データ保護規則」案の公表
2012年～：理事会及び議会で審議
2013年10月21日欧州議会市民的自由・司法・内務委員会(LIBE)採択

個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則（**一般データ保護規則**）

規則の特徴

①EU域内における規制の単一化・簡素化
国内法制化の不要な「規則」に変更
一つの国からの承認を得れば、他国の当局からの承認は不要
データ保護当局間の調査協力のメカニズム

②より強固な個人データ保護ルールの整備
事業者　プライバシー・バイ・デザインの原則
個人データ漏えい時の通知義務
個　人　消去権（忘れてもらう権利）
プロファイリングへの異議を申し立てる権利
データ・ポータビリティの権利
同意の明示（オプト・イン原則）

③データ保護に関するグローバルな課題への対応

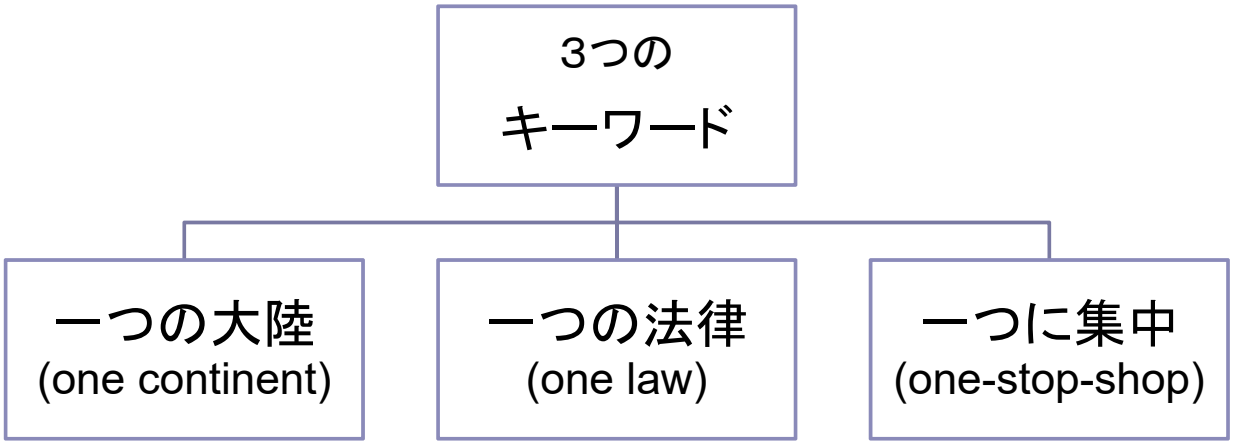
- **規則とは？（指令と規則の違い）**
  - **規則 (Regulation)、指令 (Directive)**
  - **決定 (Decision)、勧告 (Recommendation)**

□　指令とは、EU加盟国に対して示された提案を、国内法へ転換することを義務づける効力を有するもの
□　その効力は、EU域外の国に直接影響を及ぼすものではないが、各国の国内法の規定によっては間接的に域外の国にも影響が及ぶことがある
□　各国で法制度が異なることから、欧州域内における法制度（規制）の基準を統一化することが必要なため、そのために必要な一定の枠組みや基準を明確に示し、各国がそれを履行する際の要求事項を定めたもの

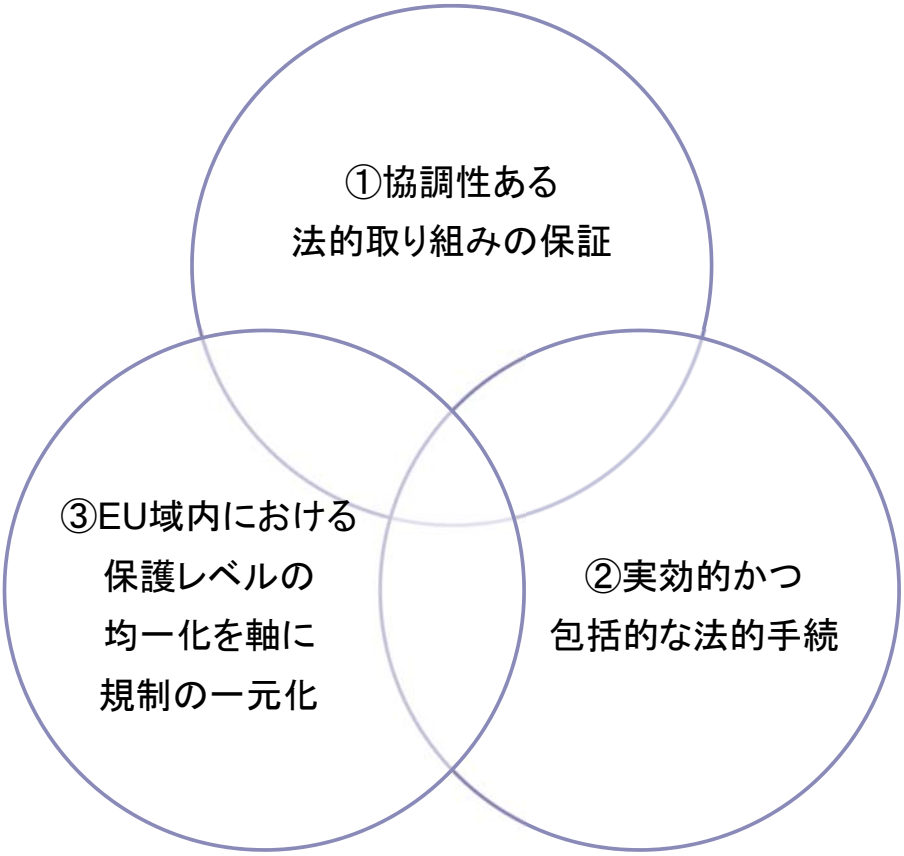
- 検討過程における議論
  - 2009年から検討を開始し、「忘れてもらう権利」や「プライバシー・バイ・デザイン」などの新たな取り組みの導入の必要性について議論
  - 2011年には、規則案が非公式に公表されて各国による水面下の検討・交渉が行われる
  - EU加盟各国から寄せられた意見（コメント）は、約3000件
  - 意見に基づき2013年3月までにとりまとめが行われる予定が、2013年5月29日まで延期（この段階で、ベルギー、チェコ、デンマーク、エストニア、ハンガリー、スウェーデン、スロベニア、イギリスの8カ国（EU加盟国は27カ国）が反対意見を表明）

一般データ保護規則　（ＧＤＰＲ）の特徴

（個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則）



GDPRの３つの目標



GDPR制定の主たる目的（４つの目的）

①包括的な取り組みの充実

②個人の権利保障の強化

③域内市場の一層の活性化及びデータ保護ルールの執行の向上

④グローバル化への対応強化

GDPRの８つの主なポイント

①個人の基本的権利としてのプライバシー保護

②自由な意思に基づき、情報が与えられた上での明示的な同意（忘れられる権利、訂正・消去権、アクセス権、プロファイリング）

③いかなる状況や取扱者に対しても適用できる基本的な原則

④技術中立性を保った上での新技術へ対応（プライバシー・バイ・デザインやプライバシー・バイ・デフォルト）

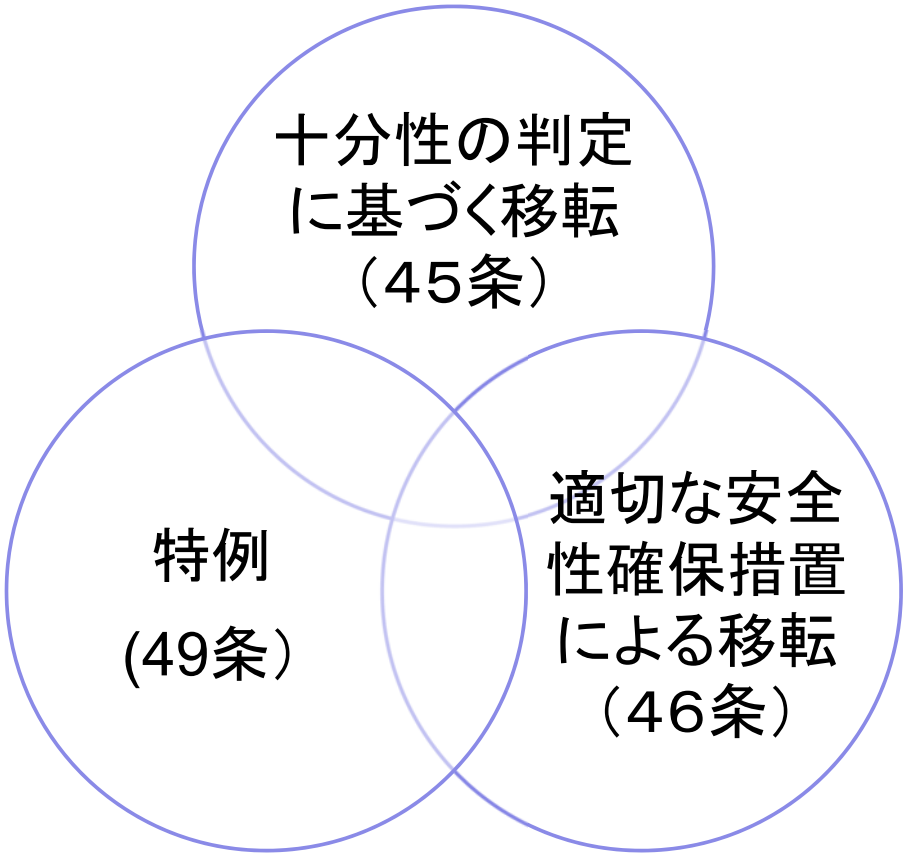
⑤実効性ある個人情報保護のための対策（利用目的の制限、データ管理者の責任、データ保護影響評価、セキュリティ侵害通知、データ保護のためのマーク（シール）制度の整備）

⑥断片的な対応の防止や法的確実性の確保（EU加盟各国の監督機関への個別承認が不要、規則違反に対し最大2000万ユーロ又は全世界での年間総売上高の4%の課徴金）

⑦基本原則に基づく法執行

⑧域外適用や第三国への安全なデータ移転

GDPRが定める越境データ移転に関する制度



（１）十分性の判定に基づく移転　（４５条）

(a)十分なレベルのデータ保護基準に適合

- アルゼンチン、アンドラ、イスラエル、ウルグアイ、カナダ、ガーンジー(英領)、ジャージー(英領) 、スイス、ニュージーランド、ハンガリー（第三国から現在はEU加盟国に）、フェロー諸島（デンマーク自治領）、マン島(英領)、日本

(b)プライバシー・シールド（米国のみ）

（２）適切な安全性確保措置による移転　（４６条）

(a)公的機関間における法令に基づく移転

(b)拘束的企業準則（BCR）

(c)標準データ保護約款

(d)行動規範（業界団体等が策定）

(e)認証（シールプログラム）