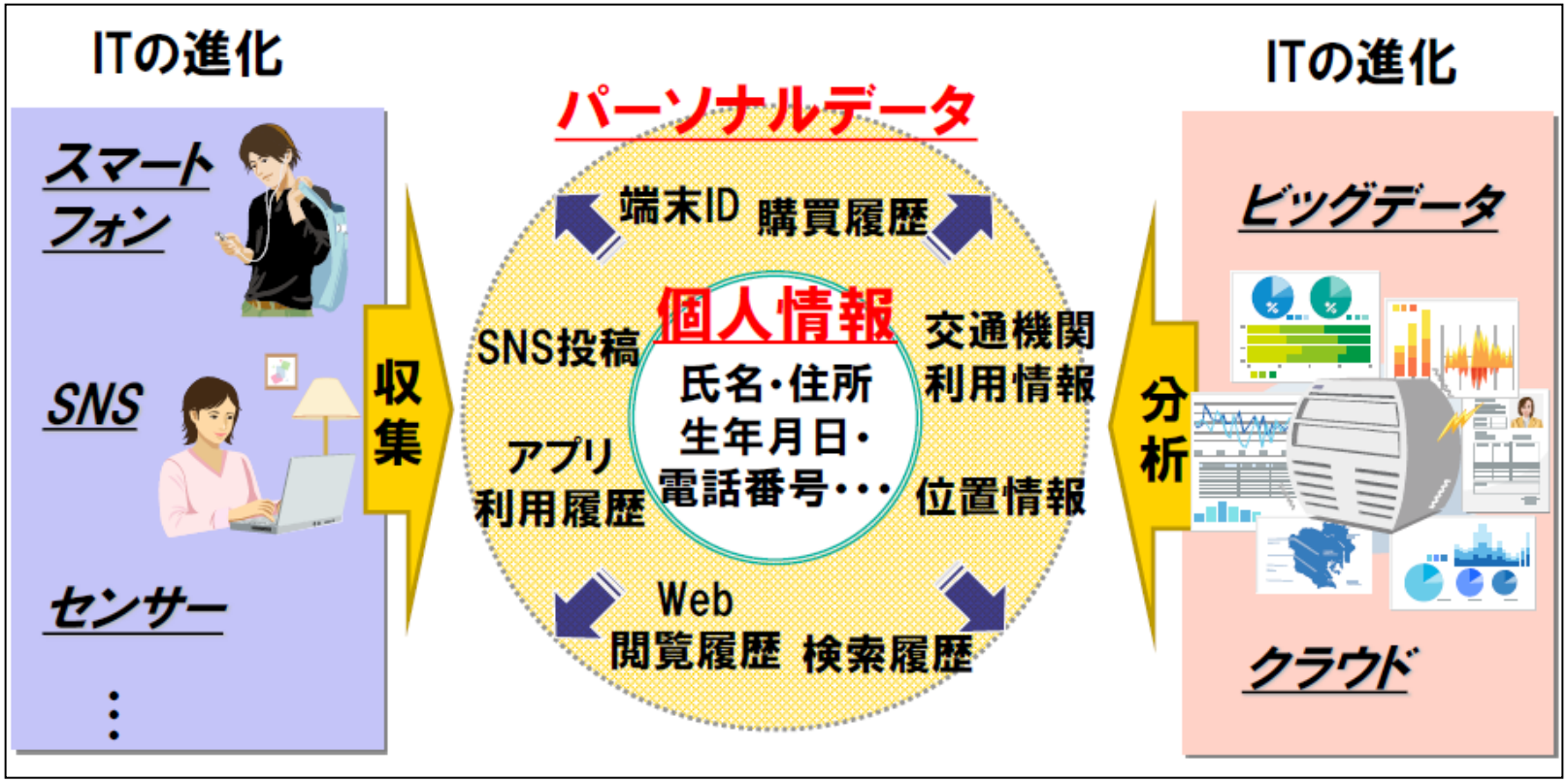
個人情報保護についての基礎および最新動向

2015年11月17日
国際社会経済研究所
小泉　雄介
y-koizumi@pd.jp.nec.com

目　次

個人情報を取り巻く環境変化

- 急速なICT技術やグローバル化の進展と、個人の権利利益を侵害するリスクの拡大
  - スマートフォン、監視カメラ、IoT機器（ウェアラブル端末、スマートメーター、車載センサー）等、個人データ収集手段の高度化
  - SNSなど、個人によるデータ公開・共有化の拡大
  - クラウドコンピューティング等による越境データ流通の増大 ⇔ データローカライゼーションの動き
- EU、米国、OECD、欧州評議会など、世界的にデータ保護制度の見直しが進められている



図の出典：NEC　徳島大介氏資料

日本の個人情報保護制度

1. 個人情報保護に関する法令

(1) 民間分野

- 個人情報保護法（2003年公布、2005年施行） → 改正法が2015年9月3日に成立。
  - 監督機関は各事業者を管轄する各省庁 → 改正法では個人情報保護委員会に一元化
  - 近年、改正のニーズが高まっていた

(2) 行政分野

- 行政機関個人情報保護法（1988年公布、2003年改正、2005年施行）
- 各自治体の個人情報保護条例（約1800自治体）

(3) 関連する法令

- 社会保障・税番号（マイナンバー）法（2013年5月31日公布、2015年10月5日より順次施行）
  - セクトラルモデル（分野別番号モデル）のID番号制度
  - 社会保障・税分野におけるデータ保護監督機関（特定個人情報保護委員会）の設置（2014年1月）
  - 番号制度に関わる行政機関・自治体にプライバシー影響評価（PIA）の実施義務
  - 行政職員に対する罰則強化（最大刑が「2年の懲役刑又は100万円の罰金刑」から「4年の懲役刑と200万円の罰金刑の併科」に。また、法人に対する両罰規定を新設）

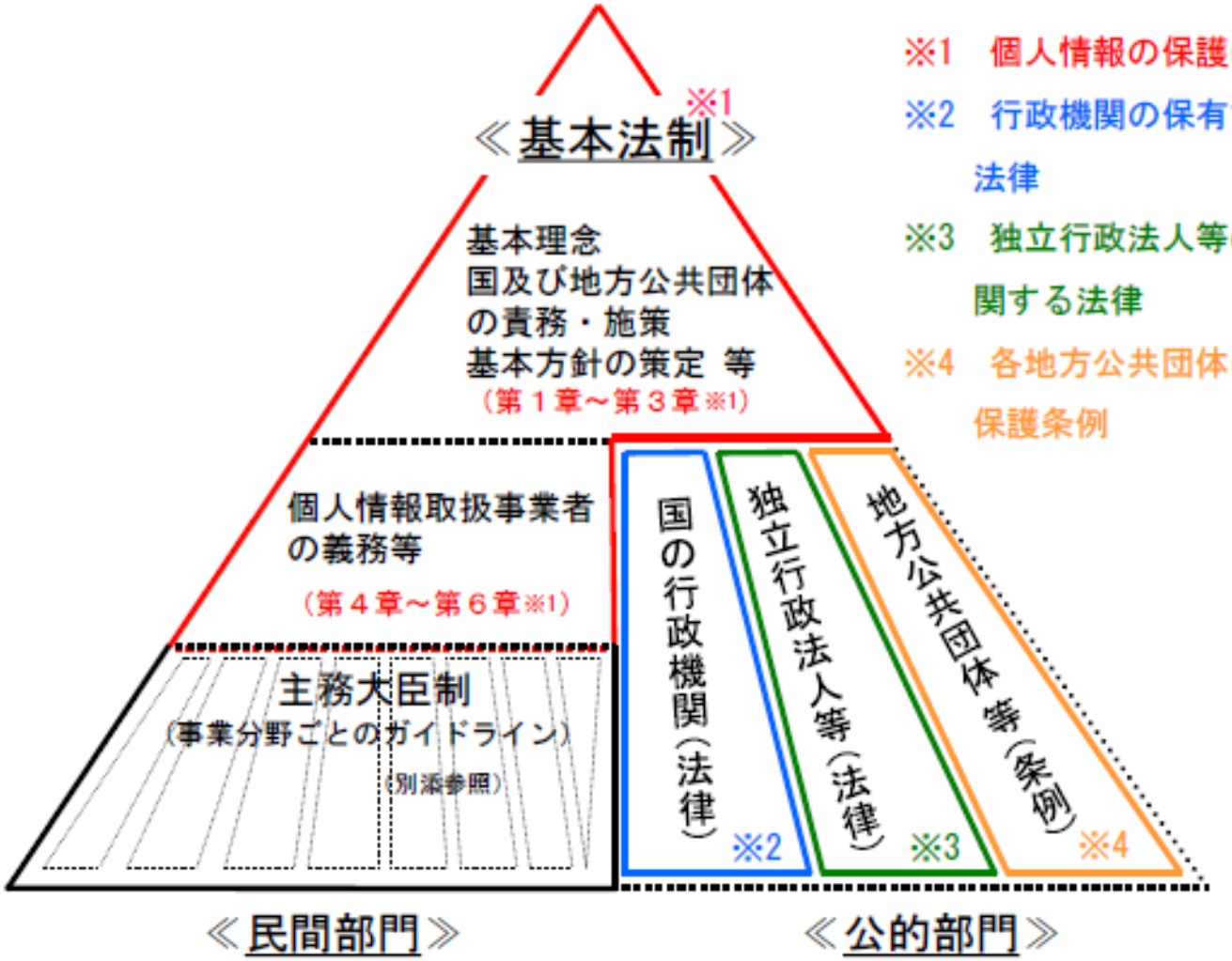
2. 個人情報保護に関する自主規制

(1) 第三者認証制度

- プライバシーマーク制度（1998年運用開始）
  - JIS Q 15001：2006をベースとする制度
  - EUデータ保護指令を参照して制定
  - 累計で16,000社以上が認証を取得

（出典：国際社会経済研究所）

日本の個人情報保護に関する法体系イメージ（現行法）



※1　個人情報の保護に関する法律

※2　行政機関の保有する個人情報の保護に関する法律

※3　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

※4　各地方公共団体において制定される個人情報保護条例

出典：消費者庁資料

個人情報保護法改正法案の検討経緯

- 2013年6月 「世界最先端IT国家創造」宣言
  - 「IT総合戦略本部の下に新たな検討組織を設置し、・・・パーソナルデータの利活用のルールを明確化した上で、個人情報保護ガイドラインの見直し・・・等の取り組みを年内できるだけ早期に着手するほか、第三者機関の設置を含む、新たな法的措置も視野に入れた、制度見直し方針を年内に策定」
- 2013年9月　IT総合戦略本部 パーソナルデータに関する検討会　検討開始
- 2014年6月　パーソナルデータの利活用に関する制度改正大綱
- 2014年12月　パーソナルデータの利活用に関する制度改正に係る法律案の骨子案
- 2015年3月10日　個人情報保護法改正法案の国会提出
- 2015年9月3日　個人情報保護法改正法の成立

〇 今後の予定

- 2016年1月　個人情報保護委員会の設置
- 2016年1月以降　政令、委員会規則の制定
- 2017年　改正法全面施行（見込み）
  - 改正法は3年毎に施行状況を検討し、必要な場合は所要の措置を講じる

【ご参考】 個人情報保護法（現行法）の成立背景

- 改正住民基本台帳法（1999年8月成立）の審議の過程で、公明党が改正住民基本台帳法の施行の前提条件として、個人情報保護法の制定を要求し、住民基本台帳法改正法案の附則に「この法律の施行にあたっては、政府は、個人情報の保護に万全を期すため、速やかに、所用の措置を講ずるものとする」という項目が追加された。

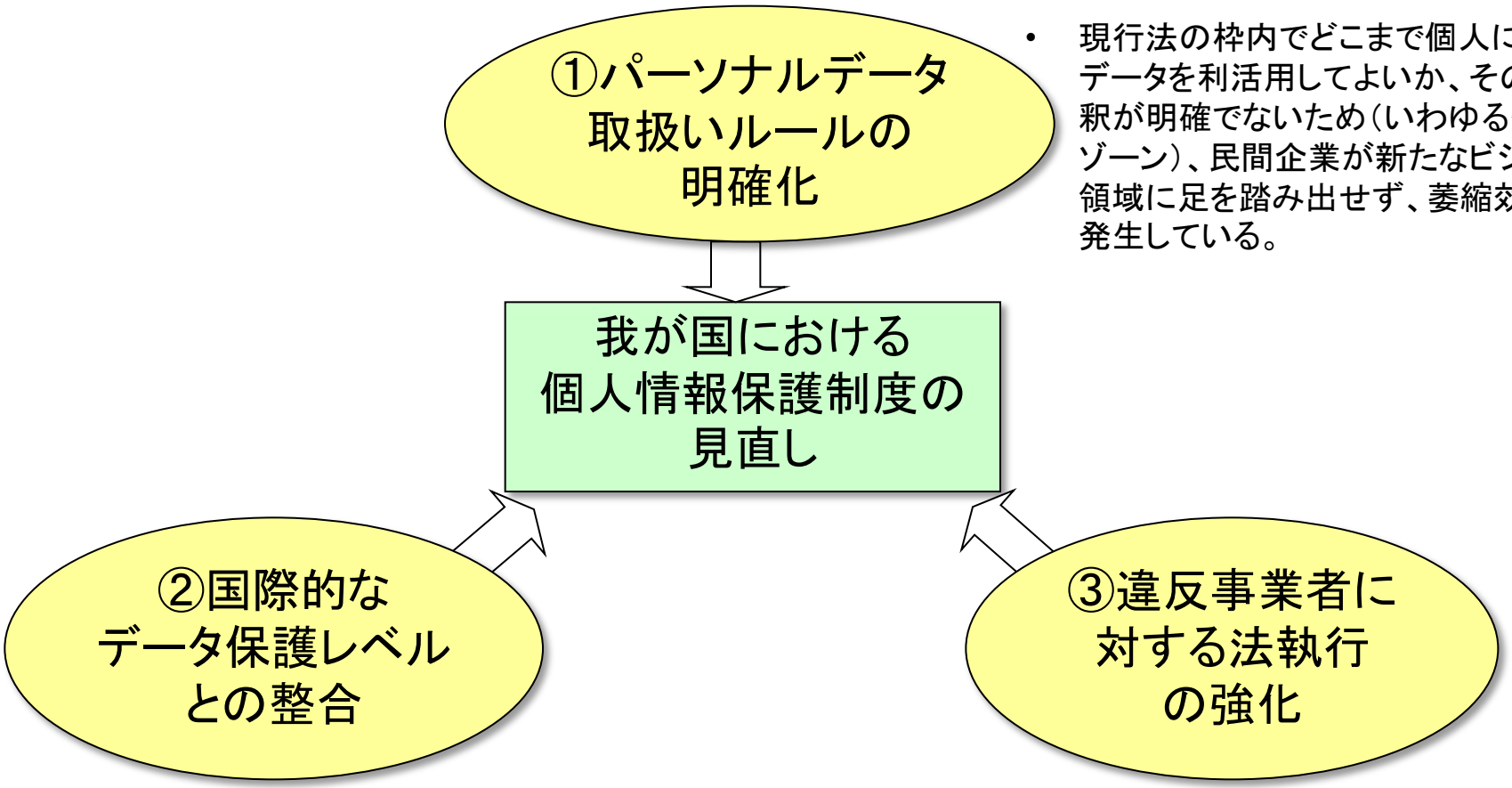
- 1999年7月、高度情報通信社会推進本部が個人情報保護検討部会を設置。同年12月、同本部は「我が国における個人情報保護システムの確立について」を決定。

- 2000年1月、高度情報通信社会推進本部は法律専門家や司法関係者等で構成する個人情報保護法制化専門委員会を設置し、法案づくりに着手した。
- 2000年10月、個人情報保護法制化専門委員会は「個人情報保護基本法制に関する大綱」を発表。

- 2001年3月、「個人情報の保護に関する法律案」が閣議決定され、3月27日に国会に法案提出された。
- 2001年の通常国会会期中での成立は見送り、継続審議となった。2001年秋の臨時国会でも見送り、継続審議。
- 2002年の通常国会でも見送り、臨時国会で廃案（12月13日）。

- 2003年3月27日に修正法案が閣議決定され、国会提出。2003年5月23日成立、5月30日公布。
- 2005年4月1日、個人情報保護法が全面施行。

日本における個人情報保護制度見直しの要因



- 現行法の枠内でどこまで個人に関するデータを利活用してよいか、その法解釈が明確でないため（いわゆるグレーゾーン）、民間企業が新たなビジネス領域に足を踏み出せず、萎縮効果が発生している。

- 日本のデータ保護法制は国際的には「十分なレベルにある」とは見られていない。
- EUはデータ保護指令において、十分な保護レベルにない第三国への個人データ移転を禁じているため、日本企業は特例的な方法を用いてデータ移転をしている。
- 第三国へのデータ移転禁止条項はシンガポールやマレーシア、台湾、香港等の保護法でも導入。

- 電話勧誘業者や名簿業者、スマホアプリ事業者、海外事業者等によって個人情報が濫用。
- 保護法には違反事業者に対する罰則規定があるが、これまで罰則適用は1件もない。
- 違反事業者に対する法執行の甘さは結果的に利用者の不安や不満を引き起こし、法令を遵守する大多数の事業者までが皺寄せを受ける羽目に。

（出典：国際社会経済研究所）

個人情報保護法改正のポイント

①パーソナルデータ利活用のための改正（＝規制緩和）

- 匿名加工情報（個人特定性低減データ）の導入（第36条～39条）
- 利用目的の変更を可能とする規定の整備（第15条第2項）
- 民間団体（認定個人情報保護団体）による自主規制ルールの作成（第53条）

②海外制度との国際的調和のための改正（≒規制強化）（≒EU十分性認定のため）

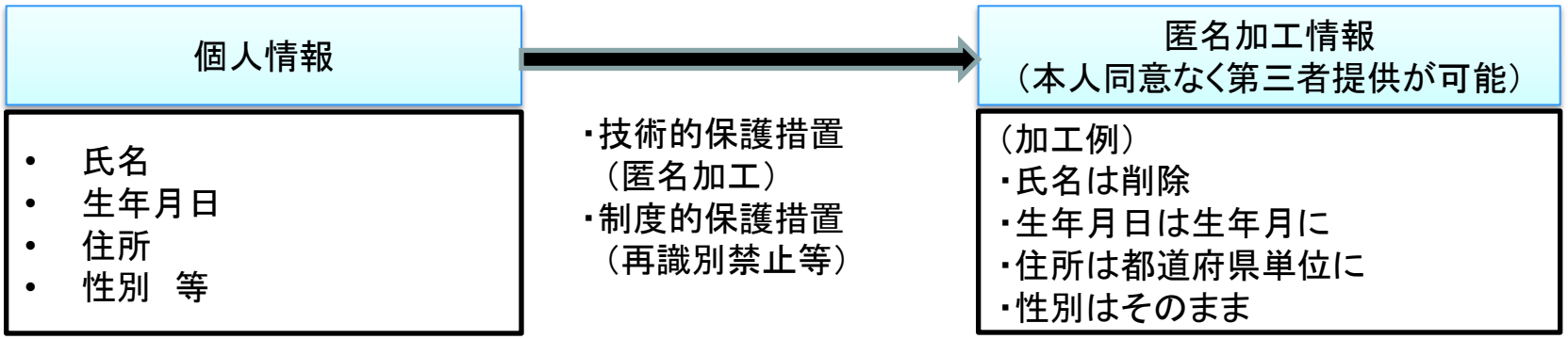
- 個人情報の定義の明確化（第2条第1項～2項）
- 要配慮個人情報（機微情報）の導入（第2条第3項）
- 個人情報保護委員会の新設（第50条～65条）
- 域外適用、外国執行当局への情報提供、第三国データ移転（第75条、78条、24条）
- 取り扱う個人情報が5,000人以下の事業者の除外規定削除（第2条第5項）

③いわゆる名簿屋対策（＝規制強化）

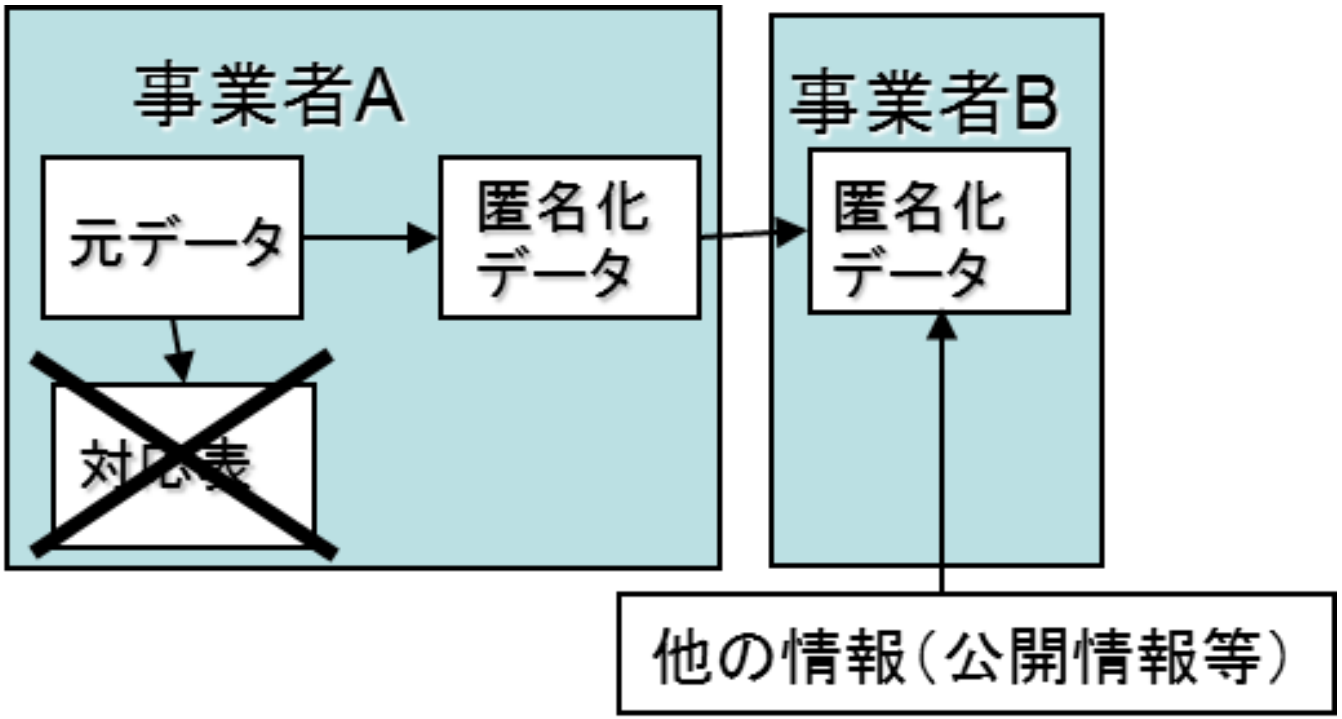
- 第三者提供のオプトアウトの届出義務（第23条第2項）
- 第三者提供に係る確認・記録の作成義務（第25条、26条）
- 個人情報データベース等提供罪の新設（第83条）

匿名加工情報の導入

- 現行の個人情報保護法の下では、「匿名化」されたデータであっても、データ提供先で「他の情報と照合する」ことで個人が再識別されるリスクが残存するため、「非個人情報」と断定することが難しい（→本人同意のない二次利用が難しい）
  - 現行法における個人情報の定義：「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（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。）をいう。」
  - JR東日本Suica問題、医療ビッグデータ（レセプトデータ二次利用）等で問題が顕在化
- この課題への対処法として「匿名加工情報」が新設された
  - 一定の制度的保護措置（提供先での本人を識別するための行為の禁止、第三者提供する旨の公表等）を取ることで個人のプライバシーに与える影響を少なくし、本人同意なく第三者提供と目的外利用を可能とした。
- 今後の課題
  - 国際的整合性（EU十分性認定への影響）
    - EUデータ保護規則案ではPseudonymous dataが日本の匿名加工情報に相当するが、Pseudonymous dataは個人データの一部であるため、二次利用に当たって本人同意が必要になる。他方、日本の匿名加工情報は個人情報ではないため、本人同意なく二次利用が可能である。
    - 日本の匿名加工情報は米国消費者プライバシー権利章典法案のDe-identified dataに相当する。



【ご参考】匿名化データと第三者提供（現行法）



・図の場合、事業者Aにおいて匿名化データは、「容易照合性」がないので、個人情報に該当しない。
・したがって、匿名化データの第三者提供に当たって、基本的に本人同意は不要のはず。
・ただし、事業者Bにおいて、<u>他の情報と照合することで特定個人を識別できる可能性</u>がある。

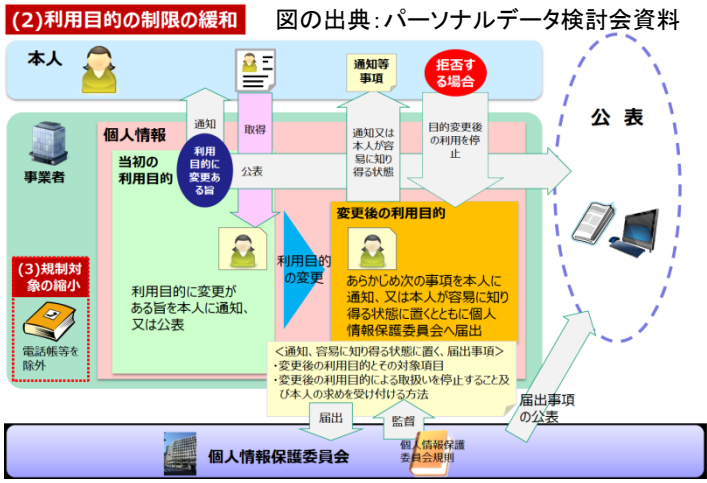
⇒そのため、事業者Aは匿名化データを第三者提供することに及び腰になってしまう。

匿名加工情報に関連する条文の日米欧比較

	日本 個人情報保護法改正法 （2015年9月）	EU データ保護規則案 欧州連合理事会案（2015年6月）	米国 消費者プライバシー権利章典法 案（2015年2月）
匿名加工情報（またはそれ相応のデータ）の定義	**※「匿名加工情報」は個人情報ではない。** ●第2条（定義） 第9項　この法律において「匿名加工情報」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて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て得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。 一　第1項第一号に該当する個人情報：　当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。 二　第1項第二号に該当する個人情報：　当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。	**※「匿名データ」は個人データではなく、EUデータ保護規則が適用されない。** **※より匿名加工情報に近い「仮名化データ」は個人データとみなされ、EUデータ保護規則が適用される。** 【匿名データ】 ●前文23 ・・・データ保護の諸原則は、匿名データ（anonymous data）には適用されるべきでない。匿名データとは、識別された自然人若しくは識別可能な自然人とは関係しない情報のこと、又はデータ主体がもはや識別可能でない仕方で匿名化されたデータのことである。それ故、本規則は、統計・研究目的での処理を含め、このような匿名データの処理には関与しない。 【仮名化データ】 ●第4条（定義） (3b)「仮名化（pseudonymisation）」とは、以下のような条件において、追加情報の利用なくしては、特定のデータ主体に結び付ける（attribute）ことができないようにする個人データの処理を意味する。当該追加情報を識別された又は識別可能な人に結び付けないことを保証するために、当該追加情報が分離して保管され、技術的かつ組織的措置の下にあることである。 ●前文23 ・・・仮名化されたデータ（pseudonymised data）（それは追加情報の利用によって自然人に結び付けることが可能である）等のデータは、識別可能な自然人に関する情報としてみなされるべきである。	**※「非識別化データ」は日本の匿名加工情報の元となった「FTC 3条件」の考え方に基づくものであり、個人データではない。** 【非識別化データ】 ●第4条（定義） (a)個人データ (2)例外： (A)非識別化データ（De-identified data）：対象エンティティが（直接的に又は委託先を通じて）以下の全ての措置を行っている場合、「個人データ」には以下のデータは含まないものとする。 (i)特定個人又は端末に実際にリンクすることができないと合理的に期待できる仕方でデータを加工する。 (ii)個人又は端末を識別しようとしないことに公けにコミットし、そのような識別を防止するための管理策を講じる。 (iii)契約上の禁止又はその他の法的に執行可能な禁止によって、対象エンティティが当該データを開示する全てのエンティティに対して当該データを特定個人又は端末にリンクしようとしないようにさせ、また同様なことを全てのさらなる開示に際して要求する。 (iv)当該データを開示する全てのエンティティに対して、特定個人又は端末にリンクしようとしないことに公けにコミットするように要求する。

利用目的の変更

- インターネット業界の要望を受けて、大綱（2014年6月）に「利用目的の変更時の手続を見直す」と記載。
- 骨子案（2014年12月）に「利用目的の制限の緩和」として、個人情報取得時に利用目的変更がありうることを通知または公表し、利用目的変更時にオプトアウトの通知または公表を行えば、事前同意なく利用目的の変更が可能とされた。
- これに対して、消費者団体や有識者から、「消費者に対する騙し討ちのための規定だ」「OECDガイドライン違反になる」「EU十分性認定の阻害要因になる」等の強い懸念が噴出。



- 骨子案の「利用目的の制限の緩和」に対しては経済団体（JEITA）も下記3点から懸念を表明、自民党・公明党に対して意見陳述。（2015年2月）
  （http://home.jeita.or.jp/press_file/20150303101433_IYph27MSl0.pdf）
  - ①消費者との信頼関係を損なう。
  - ②諸外国のデータ保護原則に合致しないとみなされる恐れがある。
  - ③むしろ、現行の利用目的変更規定（第15条2項）を柔軟に解釈すべき。
- 自民党が「個人情報保護法改正に関する提言」を公表（2015年2月11日）。
- 改正法案で「利用目的の制限の緩和」は項目ごと削除された。
  - 代わりに第15条2項の利用目的変更規定における「利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない」の「相当の」を削除することで決着。

個人情報の二次利用（利用目的の変更）はどこまで許されるのか

別紙　更なるデータ利活用を検討すべきケース

①不特定多数の人に同意を取ることが現実的ではない場合

＜例＞

- 様々な駐車場の防犯カメラのデータを大量に読み込み、多様な駐車場の駐車枠を識別して、駐車場内で自動駐車を制御する人工知能エンジンの開発を行うケース。

＜例＞

- 大量の顔画像を収集し、読み込み、防犯のための顔画像を認識する人工知能エンジンの開発・高度化を行うケース。

②最終的には匿名加工するが、分析段階では個人情報である方が精度が高い場合

＜例＞

- 別々の機関が保有する、事故車の損傷データと当該事故車のドライバーの負傷状況を掛け合わせることで、車の損傷状況を把握してドライバーの損傷程度を自動的に検証し、救急手段を選択する緊急サービスの改善に用いるケース。

例えば、防犯カメラで防犯目的で取得した顔画像を、顔認識エンジンの高度化の目的に拡大して利用することは許されるのか？

（出典：経済産業省産業構造審議会商務流通情報分科会情報経済小委員会2015年9月資料に加筆）

利用目的変更(二次利用)に関する諸外国の指針(1/3)

○ 米国

- FTC「急速に変化する時代における消費者プライバシーの保護」(2012年3月公表)

※ 同報告書はホワイトハウス「ネットワーク化された世界における消費者データプライバシー」(2012年2月公表:消費者プライバシー権利章典を含む)と整合的・補完的なものであり、ホワイトハウス報告書が民間企業に対する個人データ保護「原則」を規定しているのに対し、FTC報告書では民間分野に要求する「ルール」(自主規制)の内容を規定している。

– 同報告書の中で、「選択の簡略化」として、企業は当該取引のコンテキストや消費者との関係と整合的な、若しくは法令によって要求されたり特別に許可されているプラクティス(一般的に受容されたプラクティスcommonly accepted practices)において消費者のデータを収集したり利用したりする場合は、消費者に事前に選択を提供する必要はない(すなわち、本人の許諾なく二次利用が可能)、としている。

– この「一般的に受容されたプラクティス」として、以下の5つを挙げている。

- (1)製品やサービスの遂行
- (2)内部オペレーション(※これに「製品・サービスの改善」を含めるかは賛否両論)
- (3)詐欺の防止
- (4)法令順守と公共目的
- (5)本人へのマーケティング

利用目的変更(二次利用)に関する諸外国の指針(2/3)

○ EU

- EU指令第29条作業部会「目的制限に関する意見書」(WP203)(2013年4月2日)
  - 目的制限の原則は、管理者によるデータ利用に制限を設けることでデータ主体を保護するとともに、管理者にある程度の柔軟性を提供するものである。目的制限の概念は以下の2つの部分から成る。
    - 個人データは特定され、明示的かつ正当な目的で収集されなければならない。(目的の特定)
    - 個人データは当該目的と矛盾する(incompatible)やり方で更なる処理(二次利用)をされてはならない。(矛盾しない利用)
  - 異なる目的での更なる処理(二次利用)は、必ずしも「矛盾した利用」を意味しない。矛盾しているか否かはケースバイケースでの評価が必要。評価に当たっては、以下の要素が考慮に入れられるべきである。
    - 収集時の目的と更なる処理の目的との関連性
    - 個人データが取得されたコンテキストと、更なる利用に対するデータ主体の合理的な期待
    - 当該個人データの性質と、更なる処理がデータ主体に与える影響
    - 管理者が取る安全管理措置

利用目的変更(二次利用)に関する諸外国の指針(3/3)

○ 英国

- ICO「ビッグデータとデータ保護」(2014年7月28日)
  - ビッグデータ分析は、個人データの目的変更(re-purposing)を伴いうる。ある目的でデータを収集した企業・組織が、当初の目的とは矛盾した(imcompatible)目的で当該データを利用することを意図するのであれば、当該企業は事前にその旨を個人に知らせ、同意を得る等をしなければならない。
  - 当初目的と矛盾するか否かを決める主要な要素は、新たな目的がフェアであるかどうかである。すなわち、①新たな目的が個人のプライバシーにどのように影響を与えるか、また②データの利用方法が個人の合理的な期待の範囲内であるかが考慮されなければならない。
    - 例えば、個人がSNSに掲載した情報が、当該個人の健康リスクや金融上の信用力の評価に使われたり、当該個人への商品のマーケティングに使われたりすることは、合理的な期待の範囲内にないとみなされる。

利用目的の制限に関連する条文の日米欧比較

	日本 個人情報保護法 改正法（2015年9月）	EU データ保護規則案 欧州連合理事会案（2015年6月）	米国 消費者プライバシー権利章典法案 （2015年2月）
利用目的の特定、利用目的の制限	●第15条（利用目的の特定） 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、その利用の目的をできる限り特定しなければならない。 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。 ●第16条（利用目的による制限） 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。	●第5条（個人データ処理に関する諸原則） 第1項 (b)個人データは、特定され、明示的、かつ正当な目的で収集されなければならず、これらの目的と矛盾する（incompatible）やり方で処理されてはならない。公共の利益や第83条に則り科学的、統計的、歴史的目的を達成するための個人データの更なる処理は、当初の目的と矛盾するとはみなされないものとする。 **※理事会案では、個人データの「更なる処理（いわゆる二次利用）」に当たって、更なる処理の目的が当初目的と矛盾しない（compatible）か否かの基準を記載している。** ●第6条（処理の合法性） 3a.更なる処理の目的が当該データが収集された際の当初の目的と矛盾しないか否かを確認する（ascertain）ためには、データ主体が同意を与えていない限り、管理者はとりわけ以下を考慮に入れるものとする。 (a)データが収集された際の目的と更なる処理の目的の間の関連性（link） (b)データが収集されたコンテキスト (c)個人データの性質、とりわけ第9条にいう特別なカテゴリの個人データが処理されるか否か (d)更なる処理によってデータ主体が受けうる影響 (e)適切な安全管理措置の有無	**※コンテキストの観点から合理的な範囲であれば個人データを利用することが可能である。また、一定の目的（列挙された例外）での利用も可能である。** **※利用目的等の重大な変更に当たっては、個人に同意等のコントロール手段を与えなければならない。** ●第104条（焦点を絞った収集と責任ある利用） (a)一般則：　対象エンティティはコンテキストの観点から合理的な仕方でのみ、個人データを収集、保持、利用してよい。個人データの収集、保持、利用のプラクティスを決める際には、プライバシーリスクを最小化する方法を検討するものとする。 (b) 当該個人データが当初に取得された目的が果たされた場合、合理的な期間内に個人データを消去、破壊又は非識別化するものとする。 (c)例外：　以下の場合は、本条の規定は個人データの収集、作成、処理、保持、利用、開示を禁じない。 (1)「列挙された例外」で規定された目的での処理の場合 (2)「高められた透明性」と「個人のコントロール」を提供する場合 (3) プライバシーレビューボードの監督下で分析を実施する場合 ●第4条（定義） (n)「列挙された例外」は以下を意味する。 (1)詐欺の防止又は検出 (2)児童搾取や重大暴力犯罪の防止又は検出 (3)端末、ネットワーク又は設備のセキュリティ保護 (4)対象エンティティの権利若しくは財産の保護、又は顧客の同意に基づく顧客の権利若しくは財産の保護 (5)対象エンティティと個人の間の合意（サービス規約、利用規約、ユーザ合意、犯罪活動のモニタリングに関する合意を含む）のモニタリング又は実行 (6)顧客との取引記録の処理（合理的な期間内又は法的に要求される期間内） (7)法的要求事項の遵守又は正当な政府の要求への対応

個人情報の定義（骨子案）

個人情報の定義

事業者

個人情報

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**

氏名　住所　生年月日

次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が含まれるもの（個人情報であることを明確化）


指紋データ


顔認識データ


旅券番号


免許証番号


携帯電話番号

(1) 特定の個人の身体の一部の特徴を電子計算機のために変換した符号

(2) 対象者ごとに異なるものとなるように役務の利用、商品の購入又は書類に付される符号

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

個人情報と紐づく移動履歴

個人情報と紐づく購買履歴

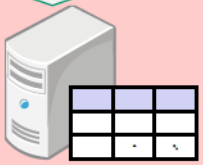
体系的に構成

個人情報データベース等

個人情報を体系的に構成

個人データ

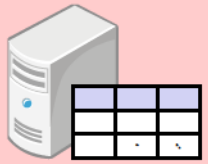
個人情報データベースを構成する個人情報



保管

保有個人データ

個人データのうち、開示等の権限を有し、政令で定める期間以上保管するもの



図の出典：パーソナルデータ検討会資料

【ご参考】 国会での審議

●第189回衆議院内閣委員会第2号（3月25日）

- ○平副大臣
- 「ビッグデータ時代が到来をしている中で、個人の行動、状態等に関するパーソナルデータの利活用が求められる一方で、個人情報の範囲が曖昧となっており、企業がその利活用をちゅうちょしている状況にあるという認識は、全く我々も一緒でございます。
- そのような中で、現行法の個人情報の定義に含まれると考えられるパーソナルデータのうち、特に事業者や消費者団体から明確化の要請の高かったもの、すなわち、身体の一部の特徴をデータ化したものや、サービスの利用や個人に発行される書類に割り振られたものに関し、特定の個人を識別できるものとして政令で定めるものを個人情報として明確化することとしております。
- 具体的には、例えば、身体の一部の特徴をデータ化したものについては、指紋認識データとか顔認識データなどを想定しております。また、サービスの利用や個人に発行される書類に割り当てられたものについては、免許証番号や旅券などを想定しているところでございます。」

●第189回衆議院内閣委員会第4号（5月8日）

- ○向井審議官（内閣官房）
- 「単に機器に付番されます携帯電話の通信端末IDは、個人識別符号には該当しないと考えられます。
- 一方、マイナンバー、運転免許証番号、旅券番号、基礎年金番号、保険証番号、これらは個人識別符号に該当するものと考えております。
- また、携帯電話番号、クレジットカード番号、メールアドレス及びサービス提供のための会員IDについては、さまざまな契約形態や運用実態があることから、現時点におきましては、一概に個人識別符号に該当するとは言えないものと考えております。」

個人情報の定義に関連する条文の日米欧比較

	日本 個人情報保護法改正法 （2015年9月）	EU データ保護規則案 欧州連合理事会案（2015年6月）	米国 消費者プライバシー権利章典法案 （2015年2月）
個人情報の定義	●第2条（定義） 第1項　この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。 一　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（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。） 二　個人識別符号が含まれるもの 第2項　この法律において「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。 一　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 二　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	●第4条（定義） (1)「個人データ（personal data）」は、①識別された自然人、又は②識別可能な自然人（データ主体）に係る全ての情報を意味する。識別されうる自然人とは、直接的若しくは間接的に、とりわけ名前や識別番号、位置データ、オンライン識別子といった識別子を参照することによって、若しくは当該人物の肉体的、生理学的、遺伝的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な1つ以上の要素を参照することによって、識別されうる自然人のことである。	●第4条（定義） (a)個人データ (1)一般則：「個人データ」は、対象エンティティの管理下にあるあらゆるデータであって、合法的な手段では一般に公開されていないデータのうち、特定個人にリンクされている（be linked）データ若しくは対象エンティティによって実際にリンク可能なデータ、又は個人に関連付けられている端末若しくは日常的に使用されている端末にリンクされているデータを意味する。個人データには以下を含むがこれらに限定されるものではない。 (A)姓名 (B)住所、メールアドレス (C)電話番号、FAX番号 (D)社会保障番号、納税番号、パスポート番号、運転免許証番号等の政府発行ユニーク識別番号 (E)指紋、声紋等の生体識別子 (F)以下を含むユニークな継続的識別子：ネットワーク端末をユニークに識別する番号、商業発行の識別番号・サービスアカウント番号（金融口座番号、クレジットカード番号、デビットカード番号、ヘルスケアアカウント番号、小売アカウント番号等）、ユニークな自動車識別子（自動車識別番号、ナンバープレート番号等）、個人のサービスアカウントへのアクセスに必要な情報（セキュリティコード、アクセスコード、パスワード等） (G)個人のコンピュータや通信端末のユニークな識別子またはそれらに関する情報 (H)収集され、作成され、処理され、利用され、開示され、保存され、又は維持されているデータであって、上記のいずれかにリンクされているデータ又は対象エンティティによって実際にリンク可能なデータ (2)例外： (A)非識別化データ（De-identified data）（略） (B)削除データ （略） (C従業員情報 （略） (D)サイバーセキュリティデータ （略）

顔認識(facial recognition)サービスの分類

①顔検出(Facial Detection):

- 映像内の顔の存在を検出し、顔の位置を同定する処理。

②顔映像からの属性推定(Categorisation):

- 顔映像から**年代や性別**といった属性を推定する処理。

③顔照合(狭義のFacial Recognition):

※「**特徴情報**」とは、顔映像から抽出された個々人にユニークな特徴を示す数値データ。

- 顔映像から抽出した**特徴情報**(前頁の顔認識データに該当)を用いて、複数の顔映像が**同一人物の顔であることを照合**する処理。
  - (1) 個人を「特定」しないが、**「識別」して追跡**する場合
  - (2) 個人を**「特定」**する場合(Facial Identification)

※「特定」「識別」は、パーソナルデータ検討会技術検討WG報告書の用語。
「特定」:ある情報が誰の情報であるかが分かること。
「識別」:ある情報が誰か一人の情報であることが分かること。

④顔認証(Facial Authentication):

- ID/パスワード等に代わる**個人認証手段**(アクセスコントロール手段)として、顔映像を照合する処理。

顔認識サービスの事例

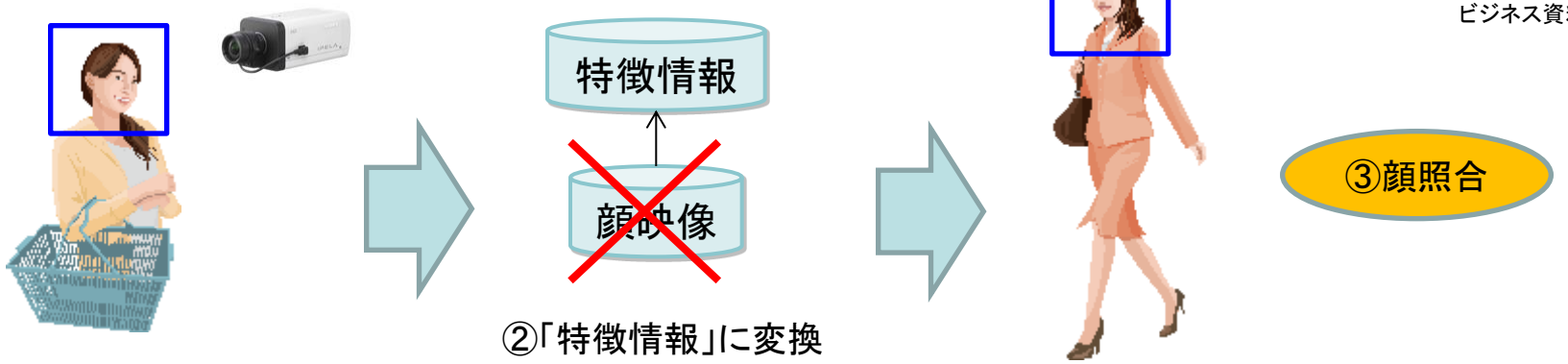
○JR東日本ウォータービジネスの次世代自動販売機

②属性推定

– カメラの顔認識により推定した性別・年代や、時間帯・気温・天候を判定材料に、お薦めの飲料品を提示。

（図の出典：JR東日本ウォータービジネス資料）

○NECの「顔認証技術活用マーケティングサービス」



①「顔映像」の取得

②「特徴情報」に変換（＝数値化）

③「顔映像」の削除

④「特徴情報」の利用（リピート顧客の識別）

○次世代コンビニ「ローソン パナソニック前店」

②属性推定

– パナソニックのカメラを店内に6台配置し、棚の商品を手に取ったが元の棚に戻したときのような「顧客が買わなかった時のデータ」も取得。

– 「何月何日何時、30代後半の男性が、新商品のパンを買わなかった」といったデータが蓄積される。（出典：THE PAGE 2014年2月15日記事）

（図の出典：株式会社ローソンのHP）

顔認識サービスの事例

○大阪駅における顔認識技術の実証実験　③顔照合

- 情報通信研究機構（NICT）は2014年4月から2年間、大阪ステーションシティにおいて、映像センサー（90台のカメラ）から施設内の状況を映像データとして取得し、通行人の顔映像を特徴情報に処理した後、特徴情報で行動を追跡することにより、シティ内の人の流量や滞留の度合い等を把握し、災害発生時の安全対策等への利用可能性を検証する実証実験を計画。
- しかし、新聞報道後に「勝手に顔を撮ってほしくない」といった市民からの抗議が寄せられたため、4月開始は事実上断念することになったという。（毎日新聞2014年3月6日記事より）

○FacebookのTagSuggest機能　③顔照合

- 利用者がアップロードした写真に人物が含まれる場合、既に当該利用者と「友人」関係にある人については、その人が誰であるかの「タグ」を「サジェスト」する機能。
- 2012年にFacebookはこの機能を一時中断したが、2013年に再開された。

○万引き犯やクレーマーを識別する防犯カメラ　③顔照合

- 来店客の顔データに対して、「万引き犯」「クレーマー」といったフラグを立てることが可能な防犯カメラシステムに対して、「顔データを無断共有している」という報道がなされたが、提供元企業から本人同意の上で共有しているとの反論がなされている。

顔認識データの個人情報保護法上の扱い

- 現行法および改正法
  - 「顔映像」は「個人情報」に該当
    - 経済産業分野ガイドライン等において「防犯カメラに記録された情報等、本人が判別できる映像情報」は個人情報に該当すると例示。
  - 「防犯カメラ」の扱い
    - 経済産業分野ガイドライン等において、一般に**防犯目的のためにビデオカメラを設置**し撮影する場合は、「**取得の状況からみて利用目的が明らかである**と認められる場合」（個人情報保護法第18条4項4号）に該当し、その**利用目的を公表等する必要がない**とされている。
    - ただし、**カメラを防犯以外の目的で利用する場合**には、「取得の状況からみて利用目的が明らか」とは認められない可能性が高いため、**当該利用目的を公表または本人に通知する必要**がある（経済産業分野ガイドライン）。

- 改正法
  - 「特徴情報」の扱い
    - 現行法では「特徴情報」が**単体で個人情報なのか否かはグレーだった。**
    - 骨子案や国会審議では、**「顔認識データ」（＝特徴情報）は単体で個人情報（個人識別符号）として例示**されている。

    ⇒前述の「③顔照合」や「④顔認証」が該当

顔認識データの個人情報保護法上の扱い

- 属性推定時（性別・年代等）の顔画像の一時的保持（推定後消去）は、「個人情報の取得」に該当するのか？（現行法および改正法）
  - 属性推定のための顔画像の撮影が「個人情報の取得」に当たるとすれば、利用目的の公表・通知が必要。
  - ただこの場合でも、撮影した（そして削除する）顔画像は（個人情報データベースを構成する）個人データには当たらないため、安全管理義務や開示・訂正義務等は発生しない。

- 属性推定データ（性別・年代等）は、改正法の「匿名加工情報」として取扱う必要があるのか？
  - 匿名加工情報については、「匿名加工基準に従う」「匿名加工情報に含まれる項目の公表」「第三者提供の方法等の公表」「本人を識別するために他の情報と照合してはならない」等の義務が発生する。
  - 属性推定データの第三者提供や目的外利用を意図しないのであれば、あえて匿名加工情報として取扱う必要はないと考えられる。

国内における顔認識データ利活用に向けた課題

カメラ映像の利用目的	取得されるデータ	現行の個人情報保護法での利用	改正後の個人情報保護法での利用	産業界への影響
防犯利用	・顔画像	○ （利用目的の通知・公表が不要） 顔画像は個人情報に該当するが、カメラの防犯利用は「取得の状況からみて利用目的が明らか」な場合として、利用目的を本人に通知又は公表する必要はない		・法改正による影響は少ない。
商用利用等（属性推定）	・顔画像（下記を推定後、消去） ・年齢・性別推定データ	× （通知・公表が必要） 年齢・性別推定データは個人情報に該当しないが、これらを推定するための顔画像の一時的保持（推定後消去）は「個人情報の取得」とみなされる恐れがある。		・カメラによる消費者の属性推定は自動販売機、デジタルサイネージ、小売店レジ等で拡がりつつある。 ・利用目的の通知・公表等の手段が課題となる。
商用利用等（顔照合/リピート顧客追跡）	・顔画像（下記を数値化後、消去） ・顔特徴データ	△ 顔特徴データが個人情報に該当するかどうかは現行法の指針では不明	× （通知・公表が必要） 顔特徴データは個人データに該当する（※）ため、利用目的を本人に通知又は公表する必要がある	・カメラによる消費者の顔照合／リピート顧客追跡は、今後の利活用が期待される分野である。 ・利用目的の通知・公表等の手段が課題となる。 ※顔特徴データは通常、個人情報データベースを構成する「個人データ」であるため、属性推定時の顔画像（単なる「個人情報」）よりも多くの義務が課される（開示義務等）。

（出典：国際社会経済研究所）

顔データに関する法解釈上の論点： 日英仏比較

	日本（改正法）	英国	フランス
顔画像の扱い	保護法上の個人情報に該当	保護法上の個人情報に該当	保護法上の個人情報に該当
顔特徴データの扱い	保護法上の個人情報に該当	保護法上の個人情報に該当	保護法上の個人情報に該当
属性推定時の一時的な顔画像データ取得の扱い	個人情報の取得に該当する恐れあり	個人情報の取得に該当（ただし、反対意見も有り）	個人情報の取得に該当
顔画像データの第三者提供	店舗等から警察への提供には、原則として令状不要	店舗等から警察への提供には、原則として令状不要	店舗等から警察への提供には、原則として令状不要
利用目的等の公表・通知方法（Web公表のみの可否）	（特に規定なし）	現地での掲示が必要	現地での掲示が必要
本人による開示請求への対応方法	（特に規定なし）	本人による開示請求に当たっては、個人識別情報（顔写真、服装情報、身分証コピー等）の提出が必要	（特に規定なし）

顔認識データと自主規制ルール

- 昨年6月の大綱では「マルチステークホルダー・プロセスを活用した機動的な自主規制ルールの策定と、委員会による認定」の考え方が制度改正の1つの目玉

  ⇒改正法では、「認定個人情報保護団体による個人情報保護指針の作成」（現行法にも存在）に自主規制ルールの考え方が統合
- 自主規制ルールが必要になる事業領域例
  - 匿名加工情報の加工方法（改正法にて言及あり）
  - 顔認識技術の商用利用　等
- 顔認識技術の商用利用（個別の運用方法で悩む場面が発生）
  - 利用目的の「通知または公表」の方法
    - Web公表で良いのか？　（おそらくNG）
    - 現地での掲示が必要な場合、どこに掲示をすればよいのか？（カメラの位置 or 入口？）
    - 防犯用途のカメラや商用利用のカメラが複数存在する場合、どうやって区別するのか？
  - 商用利用での撮影を望まない顧客への対応をどうすればよいか
  - 取得した顔特徴データに対する利用停止請求があった場合にどうすればよいか　等
- このような詳細ルールについては（個人情報保護委員会が作成するレベルのものではないため）、顔認識製品を提供するITベンダーやそれを利用するユーザ企業がイニシアティブを取って、自主規制ルールで明確化していく必要がある。

顔画像等に対する法令・ガイドライン等での義務や勧告

法令・ガイドライン等 / 項目	改正個人情報保護法	杉並区防犯カメラの設置及び利用に関する条例	東京都公安委員会「街頭防犯カメラに関する規程」	NICT報告書（映像センサー使用大規模実証実験検討委員会報告書）	英国ICOガイドライン In the picture: A data protection code of practice for surveillance cameras and personal Information	EU指令第29条作業部会 Opinion 02/2012 on facial recognition in online and mobile services	米国FTCレポート Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies	米国自主規制ルール Stakeholder Draft of Guidelines for the Collection and Use of Facial Recognition
利用目的の特定	○			○	○	○		
利用目的による制限	○	○	○	○	○	○	○	○
適正な取得	○							
取得に際しての利用目的の通知等	○	○	○	○	○	○	○	○
データ内容の正確性の確保	○				○			
安全管理措置	○	○		○	○	○	○	○
従業者の監督	○				○			
委託先の監督	○				○			
第三者提供の制限	○	○	○	○	○	○		○
保有個人データに関する事項の公表等	○			○	○		○	○
開示	○	○			○	○		
訂正等	○							
利用停止・消去	○							○
苦情の処理	○	○			○			
その他				撮影されたくない人への対応方法			・センシティブな場所に設置しない ・撮影されたくない人への対応方法	

第三国(外国)への個人データ移転制限のある諸国

- EU
  - EUデータ保護指令における第25条(いわゆる第三国移転条項)
  - 「第三国が個人データに関する十分なレベルの保護を保証する場合のみ、移転を行うことができる」

- アジア諸国
  - シンガポール、マレーシア、台湾、香港　等
  - 日本(改正法)

- データローカライゼーション
  - ロシア:2014年7月成立の法律(No.242-FZ)においてロシア市民の個人データはロシア国内のデータベースに保存することが義務付けられた。
  - ブラジル:NSAスノーデン事件を受けて、同様な条項を含む法案を審議していたが、2014年4月に可決された法案ではこの条項は削除された。
  - EU加盟国でも、イタリア、ギリシャはデータローカライゼーション政策を取っている。
  - データローカライゼーションの原因は、世界的に個人データ保護制度のハーモナイズが取られていないことと考えられる。特に米国では個人データ保護よりも国家安全保障(政府機関によるサーベイランス)が優先される傾向がある。

EUデータ保護指令の概要

個人データ取扱い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指令（EU指令）
（1995年10月採択、1998年10月発効）

EU+EEA加盟国に国内法規を要求

●EU加盟国（2015年10月現在）
- ベルギー
- ドイツ
- フランス
- イタリア
- ルクセンブルク
- オランダ
- デンマーク
- イギリス
- アイルランド
- ギリシャ
- スペイン
- ポルトガル
- オーストリア
- フィンランド
- スウェーデン
- キプロス
- チェコ
- エストニア
- ハンガリー
- ラトビア
- リトアニア
- マルタ
- ポーランド
- スロバキア
- スロベニア
- ブルガリア
- ルーマニア
- クロアチア

計28カ国

●EEA加盟国（2015年10月現在、EU加盟国以外）
- アイスランド
- リヒテンシュタイン
- ノルウェー

合計31カ国

EU＋EEA

A国

- 公正かつ適法な利用
- 利用目的の明確化
- 個人情報の正確性
- 本人の同意の上での取得・利用
- 特定カテゴリーの個人情報の利用禁止
- セキュリティ対策
- その他

公共機関・民間企業

以下の事項を本人に通知
- データ管理者
- 個人情報の利用目的
- 第三者への提供
- アクセス権、訂正権
- その他

- 独立的な監督機関の設置（第28条）

監督機関

- 個人情報へのアクセス権、訂正・消去する権利の保証

利用者

域内での個人情報の自由な移転は認める

B国

C国

○第三国移転条項

第三国が個人情報に関する十分なレベルの保護を保証する場合のみ、移転を許可（第25条）

第三国への移転を許可する例外規定もあり（第26条）

日本

米国

（出典：国際社会経済研究所）

EUから第三国への個人データ移転方法

【現行のEU指令の規定】

- 下記の場合にEU域内の管理者から第三国の管理者（又は処理者）へのデータ移転が可能。

① 十分性認定：欧州委員会が十分なレベルの個人データ保護を保証していると認定した国等（第25条）

- スイス、カナダ、アルゼンチン、イスラエル、アンドラ、ガーンジー、マン島、ジャージー（左記3つは英国の王室属領）、フェロー諸島（デンマークの自治領）、ウルグアイ、ニュージーランド。
- 認定に当たっては「個人データの第三国移転：EUデータ保護指令第25条及び第26条の適用（WP12　5025/98）」に基づいて評価。

② 米国については特例として、セーフハーバー・スキーム

- セーフハーバー原則を遵守すると自己宣言する米国企業に対して「十分なレベルの保護」を行っていることを認める協定。
- 自己宣言した企業は米国商務省のサイト（Safe Harbor List）に掲載。（2015年10月時点で約4500社）

  ex. Google, Amazon, Facebook, Microsoft, Apple等
- セーフハーバー原則は「通知」「選択」「第三者提供」「セキュリティ」「データの完全性」「アクセス」「執行」の7つ。

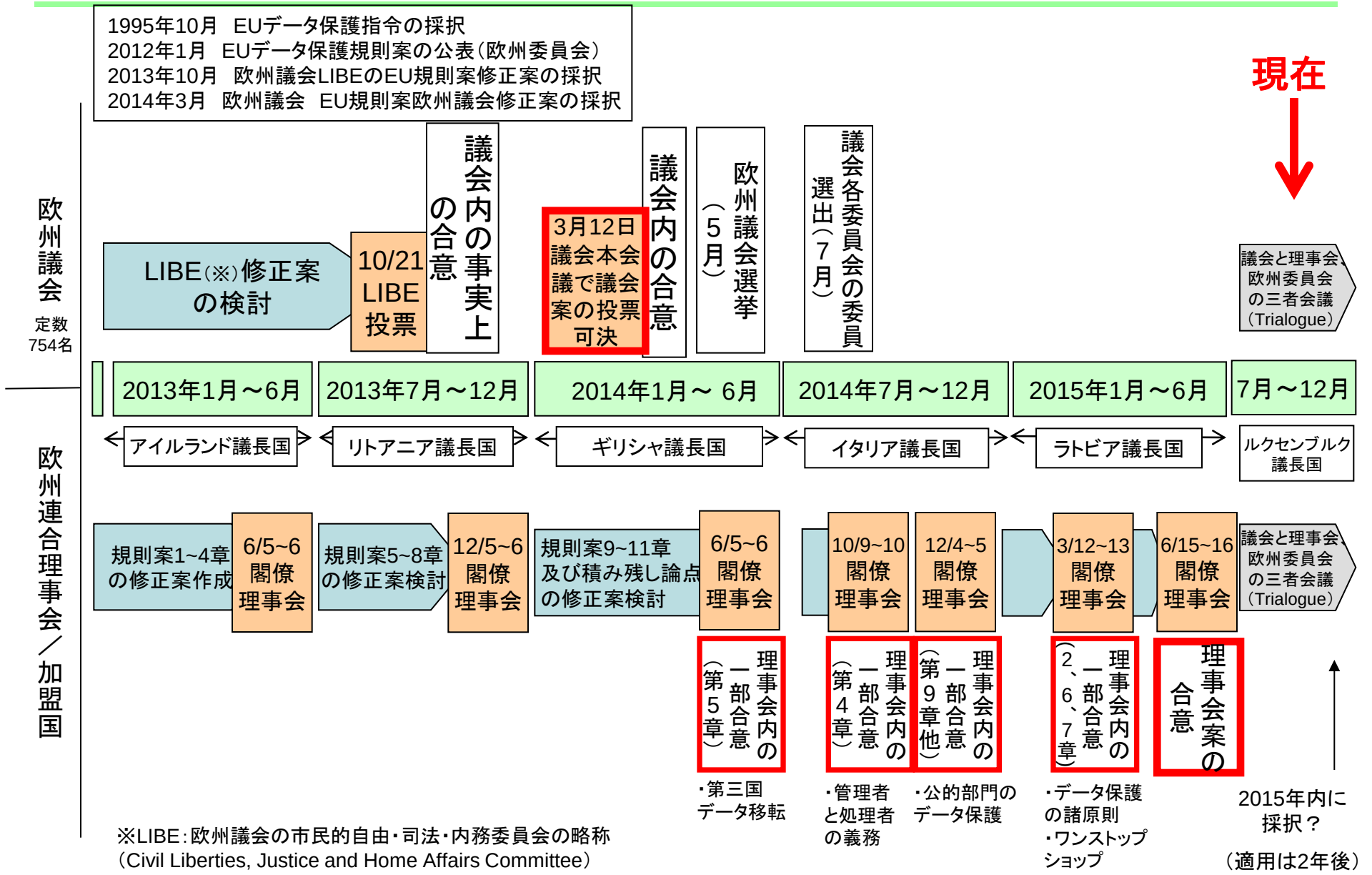
③ 例外規定として、

- 拘束的企業準則（Binding Corporate Rules：BCR）（第26条第2項）：

  多国籍企業、企業グループ内部での個人データ移転を対象。監督機関が承認。
- 標準契約条項（Standard Contractual Clauses：SCC）（第26条第4項）：

  欧州委員会が策定。2001年様式、2004年様式、2010年様式がある。
- その他、データ主体が明確な同意を与えている場合や、データ主体及び管理者間の契約の履行のために必要な場合等（第26条第1項）

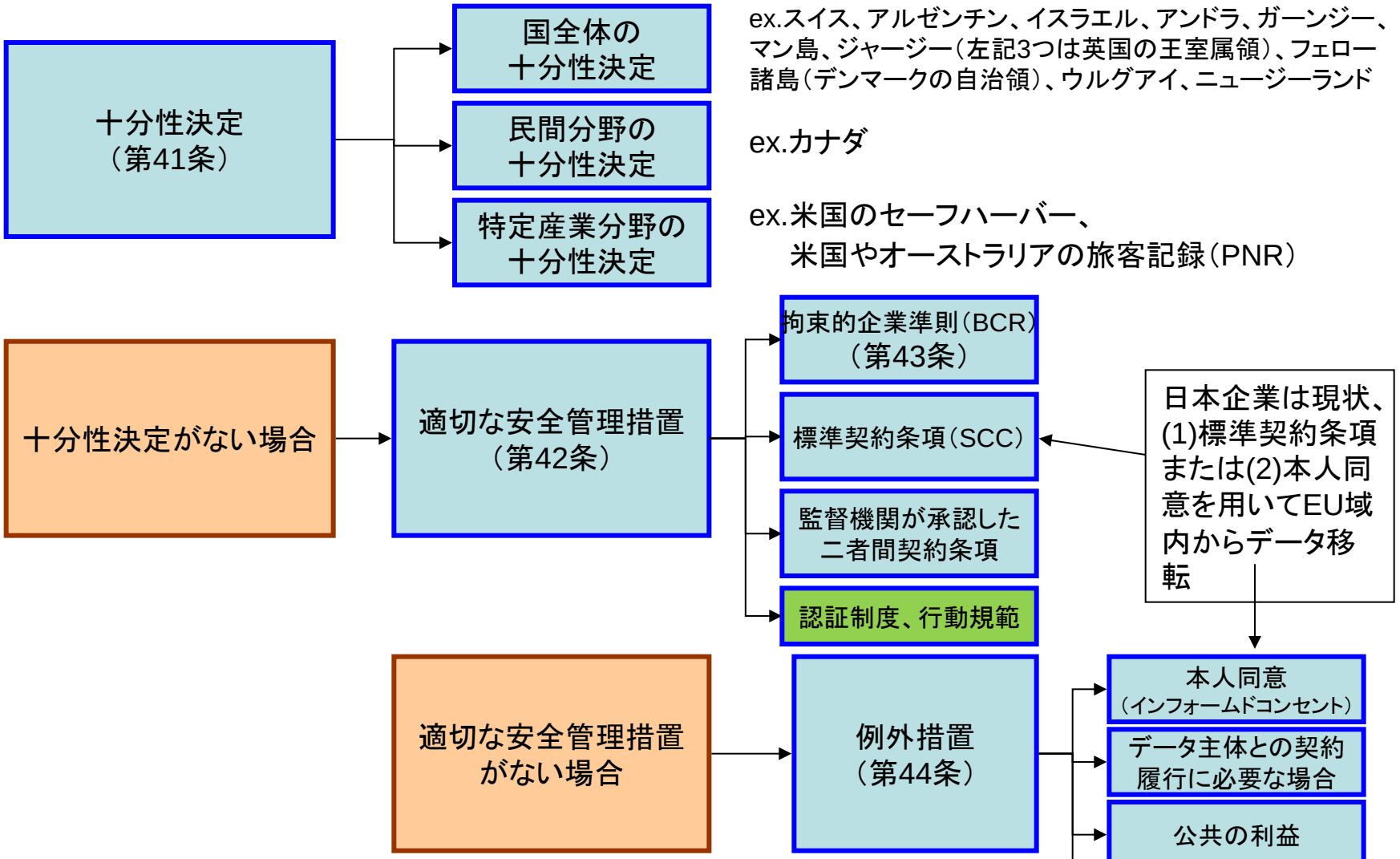
EUデータ保護規則案の審議スケジュール（推定）



※LIBE：欧州議会の市民的自由・司法・内務委員会の略称
（Civil Liberties, Justice and Home Affairs Committee）

（出典：国際社会経済研究所）

EUデータ保護規則案における第三国へのデータ移転方法



(1)標準契約条項の問題点： 相手企業ごと・案件ごとに締結が必要、弁護士費用等のコスト、監督機関の承認に時間がかかる、EU企業に日本企業側のデータ取扱いに関する責任発生など

(2)本人同意の問題点： 消費者全員の同意取得は困難、従業員データでも国により労組の同意が必要

EUからのデータ移転に対する日本産業界の対応

- 十分性認定の取得
  - 日本政府は2015年度より欧州委員会と十分性認定に向けた対話を開始する予定となっている。産業界としても十分性認定取得を強く希望。

- 認証制度を用いたデータ移転と日欧認証制度の相互承認
  - JEITA/JISAにて、EU機関にEU規則案に対する日本産業界の要望を伝えるため、2012年11月、2013年6月、2015年9月の3回、訪欧ミッションを実施。
  - JEITA/JISA等の産業界の要望に応える形で、欧州議会案（2014年3月）、欧州連合理事会案（2015年6月）で共に、「適切な安全管理措置による第三国へのデータ移転」（第42条）の1つの措置として、「認証制度/データ保護シール」によるデータ移転が追加された。
  - JEITA/JISAでは引き続き、日本の認証制度やAPECの越境プライバシールール（CBPR）等とEUの認証制度との相互承認（mutual recognition）を新たなEU規則案の枠組みに組み込んでもらえるよう、要望を続ける予定。

- 従来スキームの利用（現状維持）
  - 標準契約条項（SCC）と拘束的企業準則（BCR）
    - BCR取得企業は日系企業では無く、外資系企業のみ。日本企業は通常、標準契約条項を用いて欧州企業（現地法人含む）からデータ移転を行っている。
    - 現行のEU指令に基づく標準契約条項は、規則案の欧州連合理事会案では「欧州委員会によって修正、置換又は廃止されるまで有効」、欧州議会案では「規則の施行から5年後まで有効」。
  - 本人同意
    - 本人同意に基づく従業員データ移転の妥当性については欧州内でも議論がある。
      - 当初の欧州委員会のEU規則案第7条4項には「本人同意は、データ主体とデータ管理者の地位の間の従属関係に重大な不均衡が存在する場合には、データ処理のための法的根拠を与えないものとする」という条項があった。（その後、議会案および理事会案では削除されている。）

欧州司法裁判所の米欧セーフハーバー無効判決

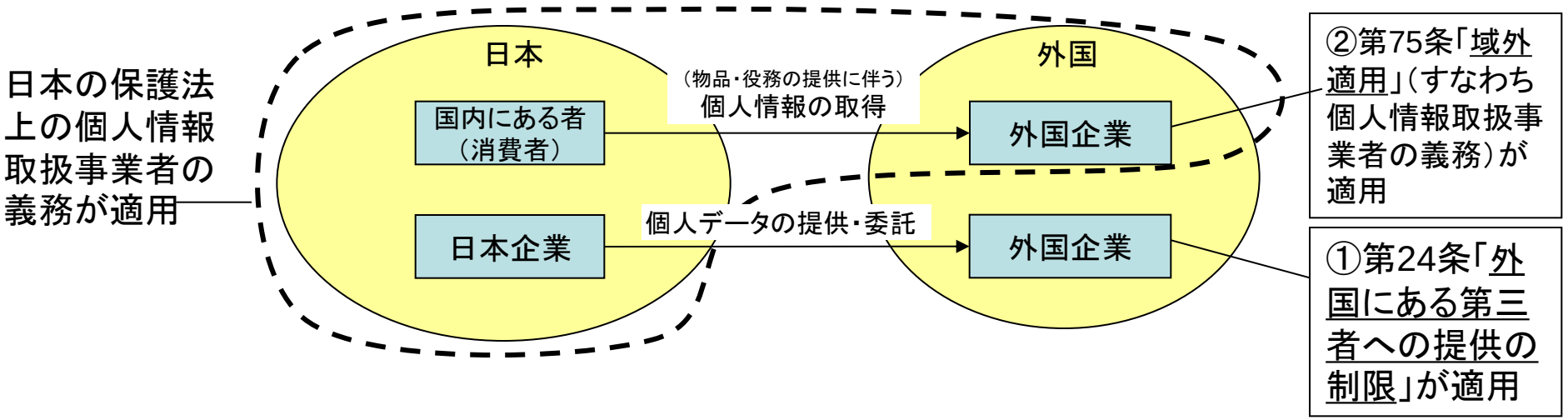
- Schrems氏によるFacebookに対する苦情申し立て
  - オーストリア国民のSchrems氏は、自分がユーザとしてFacebookに提供した個人データが同社のアイルランド子会社から米国内のサーバに移転され処理されたことについて、2013年にスノーデン氏によって暴露された米国NSA等の活動に鑑みて、米国の法律やプラクティスは米国の公共機関によるサーベイランスから個人データを十分に保護できないとして、アイルランドのDPAに苦情申し立てを行った。
- アイルランドDPAによる苦情申し立ての却下
  - これに対し、アイルランドのDPAは、セーフハーバー・スキームの下で、米国は移転された個人データに十分なレベルの保護を保証しているとして、苦情申し立てを却下した。
- 欧州司法裁判所の判決（2015年10月6日）
  - 欧州司法裁判所の2015年10月6日の判決では、「或る第三国が個人データの十分な保護レベルを保証しているとする欧州委員会の決定は、欧州連合基本権憲章やEUデータ保護指令の下での各加盟国DPAの権限を消去したり低減するものではない」との判断が示された。
- 同判決の内容
  - 「欧州委員会が決定を行っていたとしても、各加盟国のDPAは、苦情申し立てを受けて、第三国への個人データ移転がEU指令に規定された要件を遵守しているか否かを、完全な独立性でもって、調査することができなければならない。」
  - 「セーフハーバー・スキームは単に自己宣言した米国企業に適用されるのみであり、米国の公共機関はそれに従っていない。米国における国家安全保障や公共の利益、法執行の要件はセーフハーバー・スキームより優先されているため、米国企業はセーフハーバーで規定された保護ルールが国家安全保障等の要件とコンフリクトする場合には、保護ルールの方を放棄しなければならない。」

欧州司法裁判所判決への反応

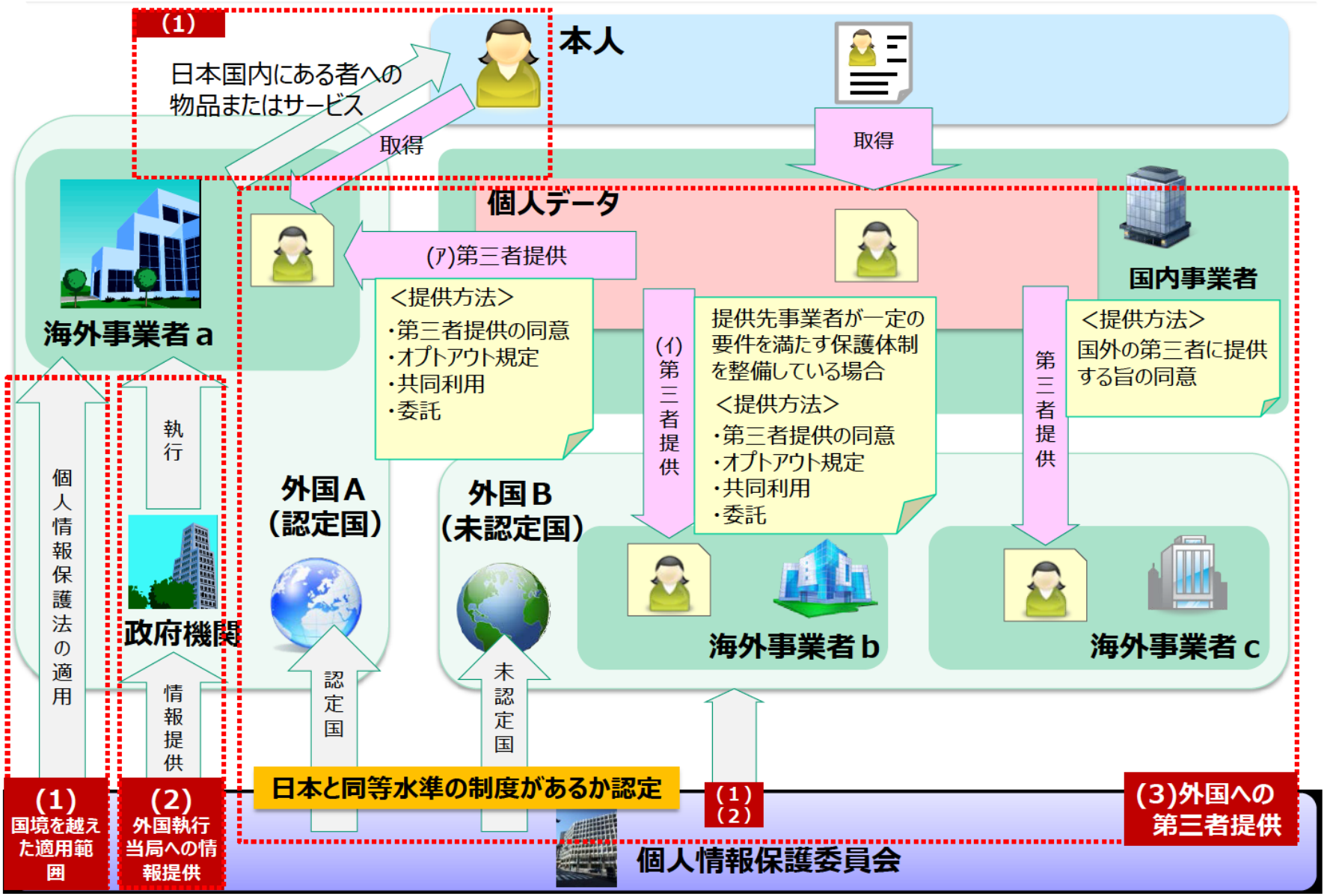
組織	反応
欧州委員会	司法担当のJourova委員は、11月にセーフハーバー改定版の交渉のために訪米し、企業が当面の米国へのデータ移転を実施するための法的なガイドラインを作成すると発表。（2015年10月9日）
欧州議会	欧州議会のLIBE（市民的自由・司法・内務委員会）は、欧州委員会が2000年に米欧セーフハーバー協定の決定を行ったことについて非難。また、欧州委員会が米国とセーフハーバー改定版の交渉を続ける計画であることも非難した。ラポーターのアルブレヒト議員曰く「欧州委員会の決定によって、どうやって米国の法的環境を変更できるというのか」。（10月12日）
欧州委員会司法総局	データ保護課のジャンカレリ課長は欧州議会LIBEの前で、直近の欧州委員会のプライオリティは米国に移転される個人データの保護と、十分な安全管理措置による移転の実現手段の明確化、EU法令の均一性であると発言。（10月12日）
在欧・米国の業界団体	DigitalEurope、CCIA Europe、AmChamEU、EuroISPA、BSA、JBCE、ITI、米国商工会議所等の23の業界団体は連名で、欧州委員会に対して、各加盟国のDPAに調和の取れた対応を取るよう働きかけるように要請した。また、スノーデン事件以来、米欧間で交渉してきたセーフハーバー改定版について早期に取りまとめるように要請。（10月13日）
EU指令第29条作業部会	EU加盟国やEU機関に対して米国政府とデータ移転を可能にする政治的・法的・技術的解決（セーフハーバー改定版を巡る現在の交渉も解決の一部になりうる）を見出すための対話を行うように要求し、2016年1月末までに米国政府と適切な解決を見出せ（ずかつ第29条作業部会による移転ツールの評価結果が芳しく）ない場合には、EU各国のDPAはあらゆる必要かつ適切な措置を講じる（協調した執行措置を含む）との声明を発表。また第29条作業部会は、欧州司法裁判所の判決が他の移転ツール（SCCやBCR）に及ぼす影響について分析中であるが、その結果が出るまでは暫くSCCやBCRを使用しうるとの見解を示した。（10月16日）
アイルランドDPA	アイルランドの高等裁判所はアイルランドのDPAに対し、Facebookが米国に移転した欧州市民の個人データが米国政府のサーベイランスから適切に保護されているか調査するように命じた。（10月20日）
ドイツのDPA	シュレースヴィヒ＝ホルシュタイン州のDPAは「セーフハーバーが無効ならば、同様の理由で、米国企業との標準契約条項（SCC）に基づくデータ移転も無効」と主張する声明を発表。（10月14日） ドイツ連邦と各州のDPAは共同で、BCRやSCCに基づく米国へのデータ移転について新たな承認は行わないとの声明を発表（10月26日）
欧州議会	欧州議会の決議において、欧州司法裁判所の判決に賛同するとともに、欧州委員会に対しセーフハーバーの代替手段と、判決の他の移転手段への影響に関して検討し、2015年末までに報告するように要請した。（10月29日）

個人情報保護法の改正： 外国への個人データ移転

- 諸外国へのデータ移転に関連し、個人情報保護法の改正法で新設された条項は下記3つ
  - 外国にある第三者への提供の制限（第24条）①
  - 域外適用（第75条）②
  - 外国執行当局への情報提供（第78条）



【ご参考】 骨子案における説明図



図の出典：パーソナルデータ検討会資料

外国にある第三者への提供の制限

- 個人情報保護法改正法　第24条（外国にある第三者への提供の制限）（新設）
  - 「個人情報取扱事業者は、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、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。」

- 外国の第三者に個人データを提供（オプトアウト、委託、事業承継、共同利用を含む）できる場合
  - （1）当該国が、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として個人情報保護委員会規則で定める**国の場合
  - （2）第三者が、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**者の場合
  - （3）**外国にある第三者への提供を認める旨の本人同意**があるか、以下の場合
    - 法令に基づく場合
    - 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
    - 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
    - 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

域外適用、外国執行当局への情報提供

- 個人情報保護法改正法 第75条（適用範囲）（新設）
  - 「第15条（※利用目的の特定）、第16条（※利用目的による制限）、第18条（※取得に際しての利用目的の通知等）（第二項を除く。）、第19条から第25条まで（※データ内容の正確性の確保等、安全管理措置、従業者の監督、委託先の監督、第三者提供の制限、外国にある第三者への提供の制限、第三者提供に係る記録の作成等）、第27条から第36条まで、第41条、第42条第1項、第43条及び次条の規定は、国内にある者に対する物品又は役務の提供に関連してその者を本人とする個人情報を取得した個人情報取扱事業者が、外国において当該個人情報又は当該個人情報を用いて作成した匿名加工情報を取り扱う場合についても、適用する。」

- 個人情報保護法改正法　第78条（外国執行当局への情報提供）（新設）
  - 「委員会は、この法律に相当する外国の法令を執行する外国の当局（以下この条において「外国執行当局」という。）に対し、その職務（この法律に規定する委員会の職務に相当するものに限る。次項において同じ。）の遂行に資すると認める情報の提供を行うことができる。
  - ２ 前項の規定による情報の提供については、当該情報が当該外国執行当局の職務の遂行以外に使用されず、かつ、次項の規定による同意がなければ外国の刑事事件の捜査（その対象たる犯罪事実が特定された後のものに限る。）又は審判（同項において「捜査等」という。）に使用されないよう適切な措置がとられなければならない。
  - ３（略）　４（略）」

外国の事業者への個人データ移転について

- 事例①:
  - ある日本企業Aが外国企業Bのクラウド型アプリケーションサービス（SaaS）と契約。社員がWebメール、グループウェア、文書ソフト、オンラインストレージなどの機能を利用。
- この場合、日本企業から外国企業への個人情報の取扱いの委託に当たるため、（第75条の域外適用ではなく）第24条の「外国にある第三者への提供の制限」が適用される。
  - 日本企業A（委託元）には「委託先監督義務」が発生。
    - 委託先の適切な選定
    - 委託契約の締結
    - 委託先における個人データ取扱状況の把握
  - 外国企業B（委託先）は第24条（外国にある第三者への提供の制限）の要件を満たす必要。
    - 個人情報保護委員会規則で定める国にある企業　or
    - 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企業
- 国外にデータがある限り、外国企業Bには、（第24条を除き）日本の個人情報保護法は適用されない。
  - もし外国企業Bが利用規約で準拠法を外国法と規定していて、Bが日本の個人情報保護法違反に当たるが、当該外国法の違反には当たらない行為を行った場合、Bを日本の保護法で罰することはできない。逆に日本企業Aが「委託先監督義務違反」とみなされる恐れがある。

外国の事業者への個人データ移転について

- 事例②:
  - 日本の消費者Cが外国企業Dのソーシャルネットサービスの会員となり、個人情報を提供。

- この場合、外国企業は日本の消費者から個人情報を直接取得しているため、第75条の域外適用が適用される。
  - 外国企業Dには第75条に挙げられた個人情報取扱事業者の義務が発生。
- 消費者Cと外国企業Dの間で係争が起こった場合の準拠法は、外国企業Dの設定する利用規約に依存する(カリフォルニア州法など)。
  - ただし、個人情報保護法違反に当たる場合(適切な安全管理措置を講じていない場合等)には、個人情報保護委員会が助言、勧告等を行うことができる。