個人情報保護・プライバシーに関する国内外動向

2017年6月21日

（株）国際社会経済研究所
主幹研究員　小泉 雄介
y-koizumi@pd.jp.nec.com

講師略歴

〇小泉　雄介

株式会社 国際社会経済研究所　主幹研究員　http://www-i-ise-com.onenec.net/jp/about/researcher/koizumi.html

- 専門領域：
  - 個人情報保護/プライバシー、監視社会、電子政府（国民ID制度）、新興国/途上国市場調査
- 略歴：
  - 1998年　（株）NEC総研入社
  - 2008年7月　日本電気（株）パブリックサービス推進本部に出向
  - 2010年7月　（株）国際社会経済研究所（旧NEC総研）に復帰
- 主な著書
  - 『国民ID　導入に向けた取り組み』（共著、NTT出版、2009年）
  - 『ブログ・SNS利用者の実像』（共著、NEC総研、2006年）
  - 『現代人のプライバシー』（共著、NEC総研、2005年）
  - 『経営戦略としての個人情報保護と対策』（共著、工業調査会、2002年）
- 主な論文・解説
  - 「ICT世界の潮流パートⅤ：諸外国における国民IDカードとeID」（日刊工業新聞2017年6月）
  - 「英国における監視カメラと顔認識の動向」（画像ラボ2017年3月号）
  - 「プライバシー影響評価（PIA）の海外動向と日本への応用」（日本データ通信2017年3月号）
  - 「EUデータ保護規則案の動向と個人データ越境移転」（ITUジャーナル2015年11月号）
  - 「マイナンバー制度とは」（日本経済新聞2013年4月7日「今を読み解く」に掲載）
  - 「EUデータ保護指令の改定と日本企業への影響」(『CIAJ Journal』2012年6月号)
  - 「国民ID制度の概要と海外の最新事情」（共著、『CIAJ Journal』2011年1月号）
  - 「オーストリアの電子IDカードと市民カード」（共著、『情報化研究』情報産業振興議員連盟、2008年）　等

1. 改正個人情報保護法

2. EU・米国の動向

個人情報を取り巻く環境変化

① 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

- 個人データ収集手段の高度化：

  スマートフォン、監視カメラ／ボディカメラ／ドローン、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、AIスピーカー）、ソーシャルロボット等
- 個人によるデータ公開・共有化の拡大： SNS等
- 越境データ流通の増大： クラウドコンピューティング等

  ⇔ データローカライゼーションの動き

② 米国プラットフォーム企業等の「ビッグブラザー」化と、政府機関による監視

- Google、Facebook、Amazon等
- スノーデン事件で明らかになった米国NSAによるデータアクセス

③ 全世界的にデータ保護制度の見直し・整合化が進められている

- EU、OECD、APEC、日本、米国 等

④ さらに近年では（個人情報を含め）質の高い大量のデータこそが人工知能（AI）の強化の鍵とされる

全世界的な個人情報保護制度見直しの動き

EU	・1995年　EUデータ保護指令　採択 ・2012年1月　EUデータ保護規則案　公表 ・**2016年4月　EUデータ保護規則（GDPR）　採択** ・2018年5月　EUデータ保護規則（GDPR）　適用
米国	・1974年　プライバシー法（連邦行政機関を対象）　制定 - 民間分野は自主規制中心（医療、金融、教育等を除く） ・**2012年2月　消費者プライバシー権利章典　公表** ・2015年10月　米欧セーフハーバー　欧州司法裁判所で無効判決
OECD	・1980年　プライバシーガイドライン　採択 ・**2013年7月11日　プライバシーガイドライン改定**
APEC	・2004年　APECプライバシー・フレームワーク　採択 ・2011年　越境プライバシールール（CBPR）　採択 ・2014年4月　日本のCBPRへの参加承認（現在、米・メキシコ・日・加の4国）
日本	・2003年　個人情報保護法 制定 ・2015年9月　改正個人情報保護法　成立 ・**2017年5月　改正個人情報保護法　施行**

（出典：国際社会経済研究所）

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、2015月9月改正）
   (2) 行政分野
      - 行政機関個人情報保護法（1988年公布、2003年改正、2016年5月改正）
      - 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（特別法）
      - 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）

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
        - 累計で16,000社以上が認証を取得
        - JIS Q 15001は改定作業中
      - APEC越境プライバシールール（CBPR）制度（2016年国内運用開始）
      - 等

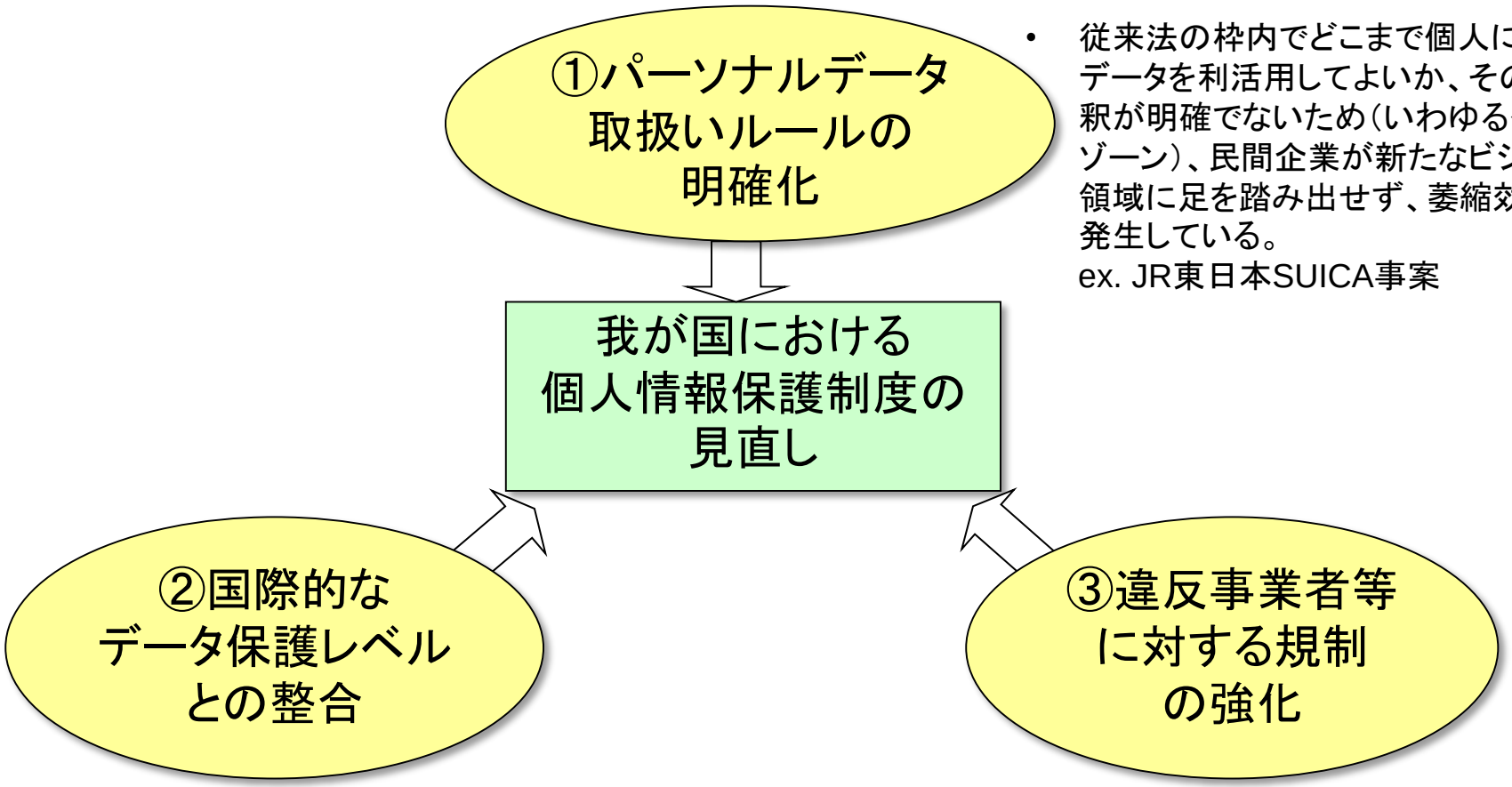
改正個人情報保護法の検討経緯

- 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　改正個人情報保護法案の国会提出
- 2015年9月3日　改正個人情報保護法の成立
- 2016年1月　個人情報保護委員会の設置
- 2016年8月　政令案・個人情報保護委員会規則案の公表、パブコメ実施　→10/5公布
- 2016年10月　個人情報保護法ガイドライン案の公表、パブコメ実施　→11/30官報掲載
- 2017年2月　個人情報保護法ガイドラインQ&Aの公表
- 2017年5月30日　改正個人情報保護法の全面施行

○ 今後の予定

- 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

日本における個人情報保護制度見直しの要因



- 従来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。
  ex. JR東日本SUICA事案

- 日本の個人情報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。

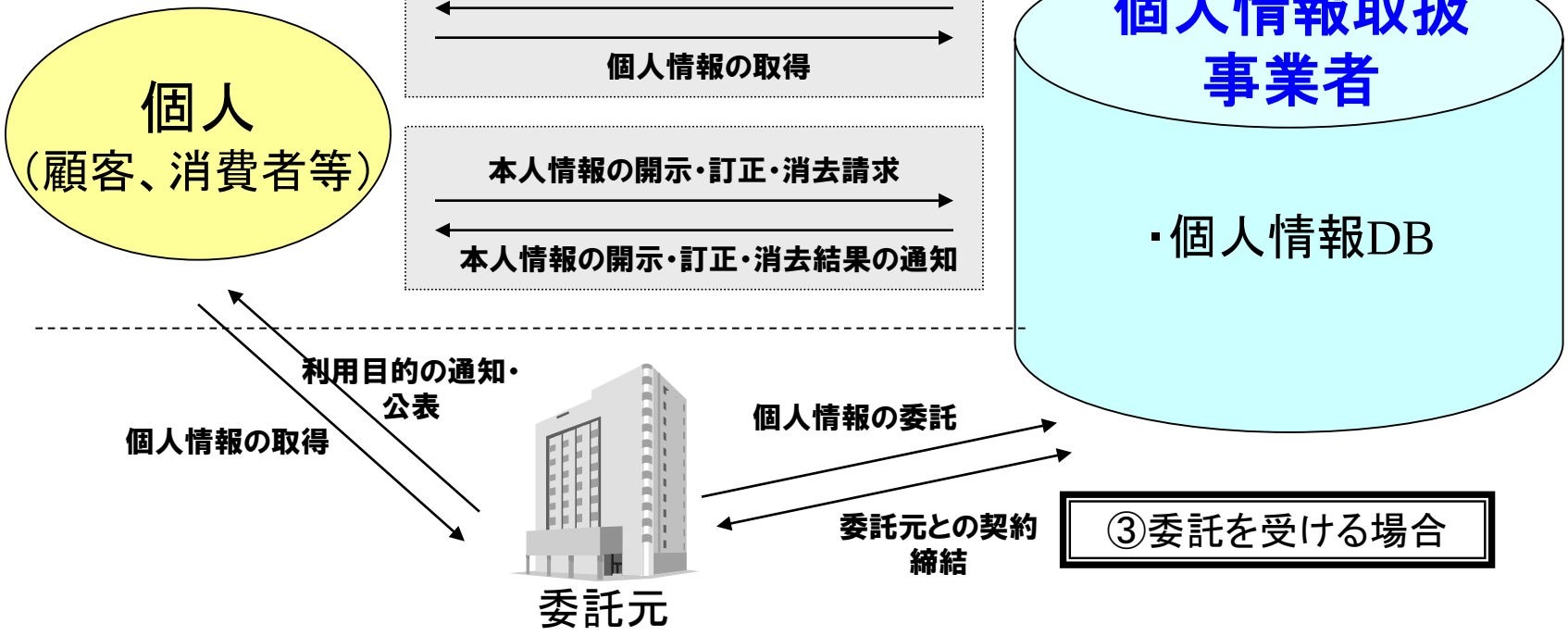
（出典：国際社会経済研究所）

個人情報保護の基本的考え方

1．個人（顧客）とのインターフェース・・・取得、開示・訂正等

①取得
- 利用目的の特定
- 適正な取得
- 利用目的の通知・公表
- 個人情報保護方針の公表

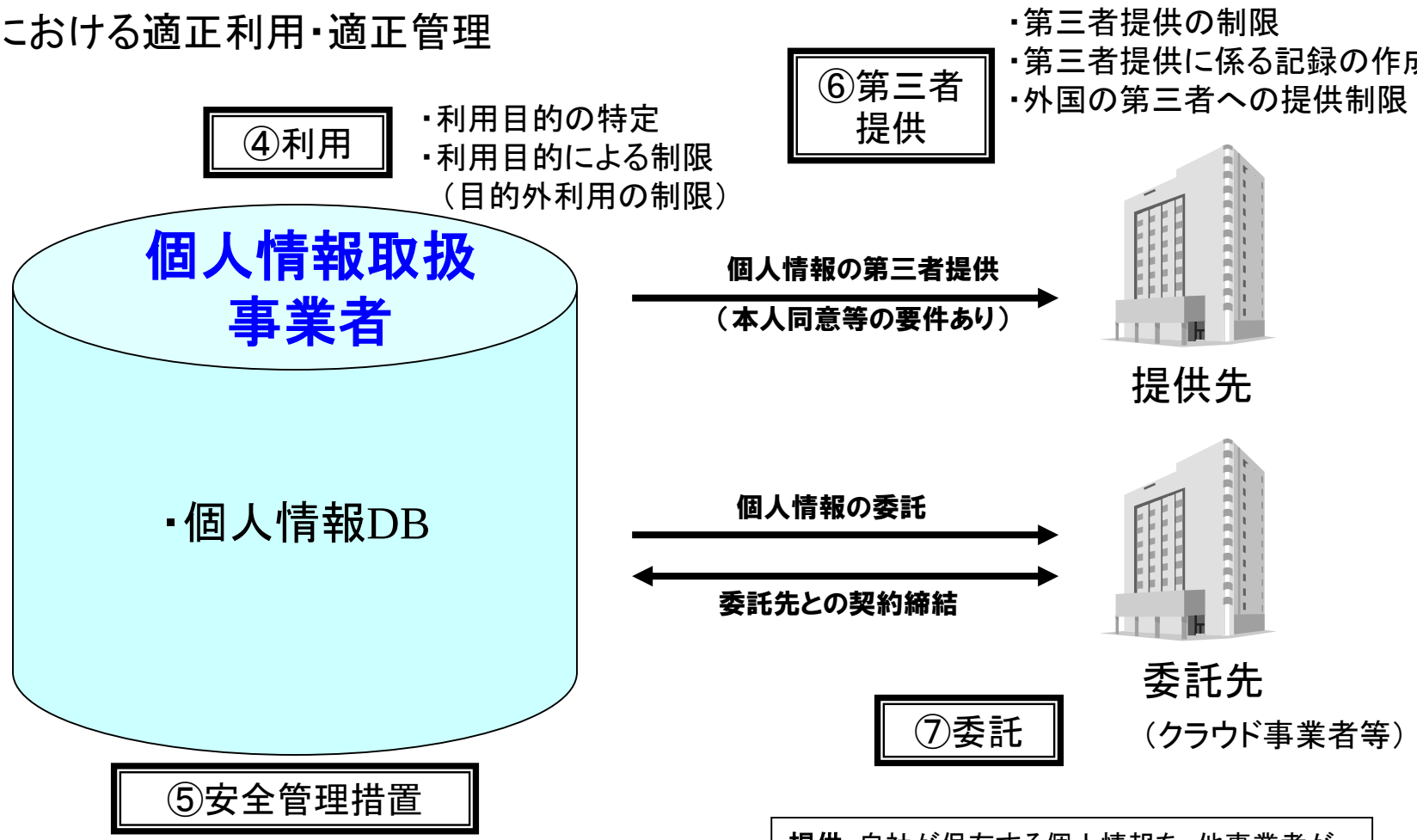
②開示・訂正等
- 開示
- 訂正・追加・削除
- 利用停止・消去



・個人から個人情報を取得する場合は、その利用目的をあらかじめ特定し、利用目的を本人に通知または公表した上で取得する。
・本人からの個人情報の開示請求や訂正請求等には、原則として対応する。

個人情報保護の基本的考え方

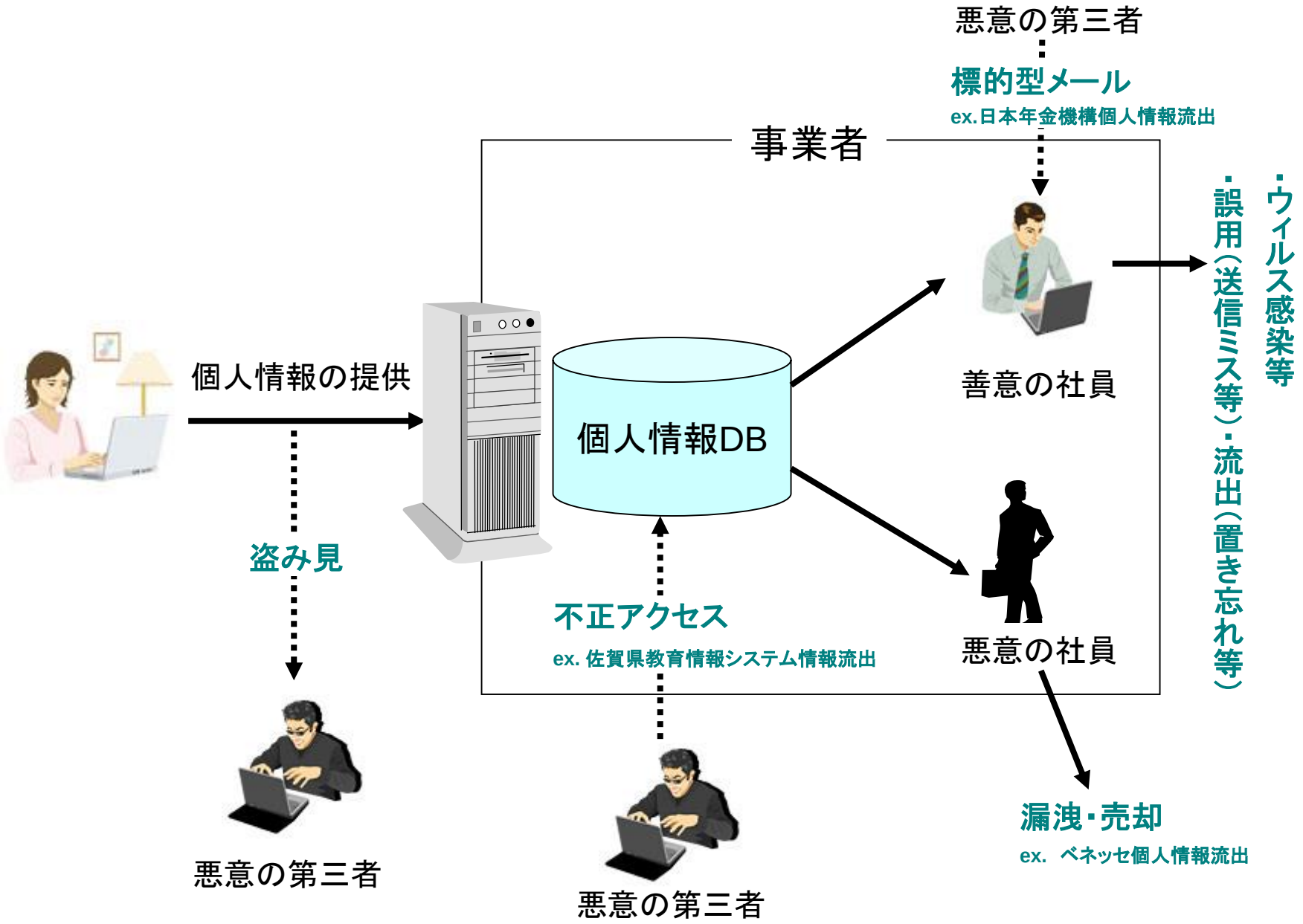
2. 業務における適正利用・適正管理



提供：自社が保有する個人情報を、他事業者が利用できるようにすること。他事業者は独自の利用目的で利用できる。

委託：自社が保有する個人情報を、他事業者に、情報処理を委託するなどのために預けること。他事業者は独自の利用目的では利用できない。

安全管理措置を怠った場合のリスク



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）

- 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）
- 外国への個人データ移転（外国の第三者への個人データ提供、域外適用、外国執行当局への情報提供）（第24条、75条、78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）

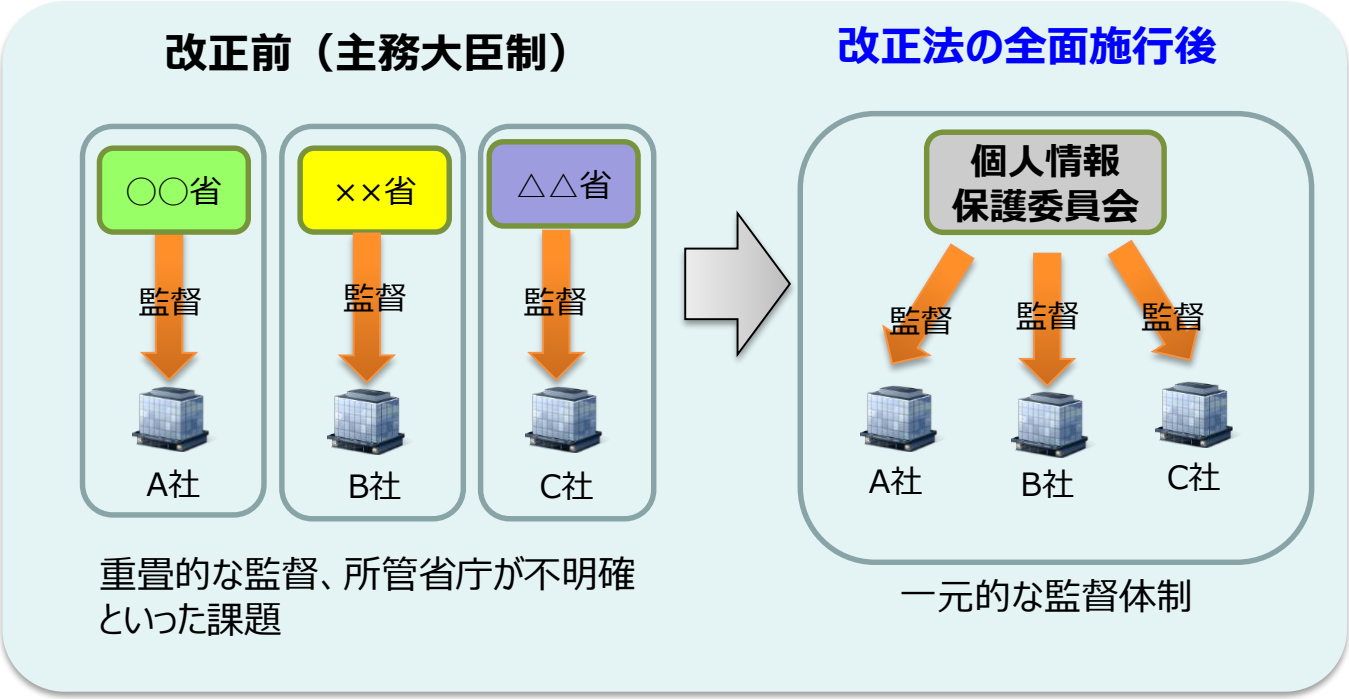
③いわゆる名簿屋対策（＝規制強化）

- 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）

個人情報保護委員会の新設

- 主務大臣が有している監督権限を改正法の全面施行時に個人情報保護委員会へ一元化。
- 事業者に対して、必要に応じて報告を求めたり立入検査を行うことができる。また、実態に応じて、指導・助言、勧告・命令を行うことができる。

民間事業者の監督体制



公的機関の監督体制*

行政機関個人情報保護法
（対象：国の行政機関）

独立行政法人
個人情報保護法
（対象：独立行政法人等）

個人情報保護条例
（対象：地方公共団体等）

※公的機関の監督体制は、個人情報保護法の改正前後で変更はない。

出典：個人情報保護委員会資料

個人情報の定義の明確化

- 従来の個人情報保護法：「個人情報」のみ

※厳密には、管理態様によって「個人情報」「個人データ」「保有個人データ」に分けられる。

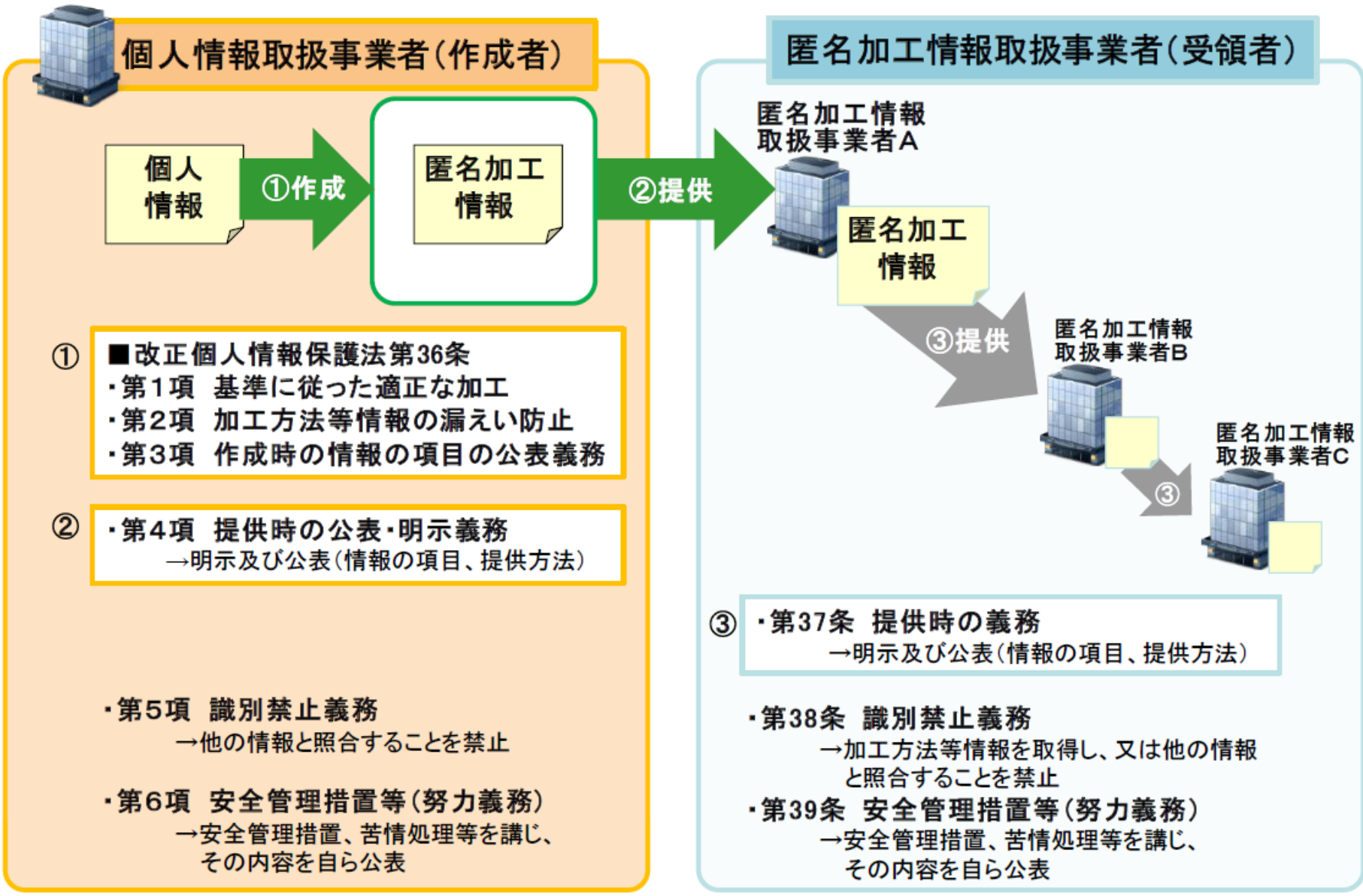
※従来法における「個人情報」の定義：「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」

- 改正個人情報保護法：　下記の3類型となった

事業者の義務 小 → 大

保護対象となる情報の類型		内容	備考
「匿名加工情報」 （※個人情報ではない）		・個人情報に一定の匿名加工措置を講じることで、特定個人を識別できないようにした情報（個人情報に復元できないようにしたもの） ・本人同意なく第三者提供が可能	・第三者提供をする旨を公表する。 ・提供先における再識別行為の禁止。 ・匿名加工基準は個人情報保護委員会が作成。
「個人情報」	従来型の個人情報	・氏名 ・生年月日や連絡先（住所・電話番号・メールアドレス等）、勤務先情報と、氏名を組み合わせた情報 ・防犯カメラに記録された本人が判別できる映像情報 等	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場合も個人情報に該当。
	個人識別符号	・身体的特徴（指紋データ、顔認識データ（顔特徴データ）、DNAデータ、声紋データ等） ・公的に付番された番号（パスポート番号、運転免許証番号、健康保険証番号等）	現行法でも個人情報に該当するが、改正法で定義を明確化した。
「要配慮個人情報」		・本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実 ・その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するもの（健康診断の結果、診療記録、調剤録、非行事実等）	・原則として、取得時に本人同意が必要。 ・第三者提供におけるオプトアウトは不可。

匿名加工情報



出典：個人情報保護委員会資料

匿名加工情報

- 匿名加工情報の作成方法（個人情報保護法ガイドラインより）
  - 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（氏名を削除、住所を○○県△△市に置換、生年月日を生年月に置換 等）
  - 個人識別符号の全部を削除（顔特徴データを削除、免許証番号を削除 等）
  - 個人情報と他の情報とを連結する符号を削除（顧客管理用IDを削除、または仮IDに置換 等）
  - 特異な記述等を削除（「116歳」という属性を「90歳以上」に置換、症例数の極めて少ない病歴を削除　等）
  - その他、自宅や職場を推定できる位置情報の削除など

- 匿名加工情報の例　（ex.小売店における販売データ）

顧客管理用ID	氏名	住所	生年月日	店舗	日時	商品	数量	・・・

匿名加工

（削除）	（削除）	市町村まで	生年月まで	店舗	日時	商品	数量	・・・

- 匿名加工情報に係る事業者の義務
  - 作成時・提供時の公表（匿名加工情報の情報項目、第三者提供の方法）
  - 再識別行為の禁止（個人情報に戻してはならない）
  - 個人情報保護委員会が定める匿名加工基準の遵守　等

匿名加工情報

- 匿名加工情報に関する個人情報保護委員会事務局レポート（2017年2月）
  - 認定個人情報保護団体や事業者団体が匿名加工情報の作成に関する自主的なルールを検討したり、民間事業者が実際に匿名加工情報を作成したりする際に参考となる事項、考え方を示すもの。
  - 以下の5つのユースケースを例示
    - 購買履歴の事例（ID-POSデータ）
    - 購買履歴の事例（クレジットカード利用情報）
    - 乗降履歴の事例
    - 移動履歴の事例
    - 電力利用履歴の事例

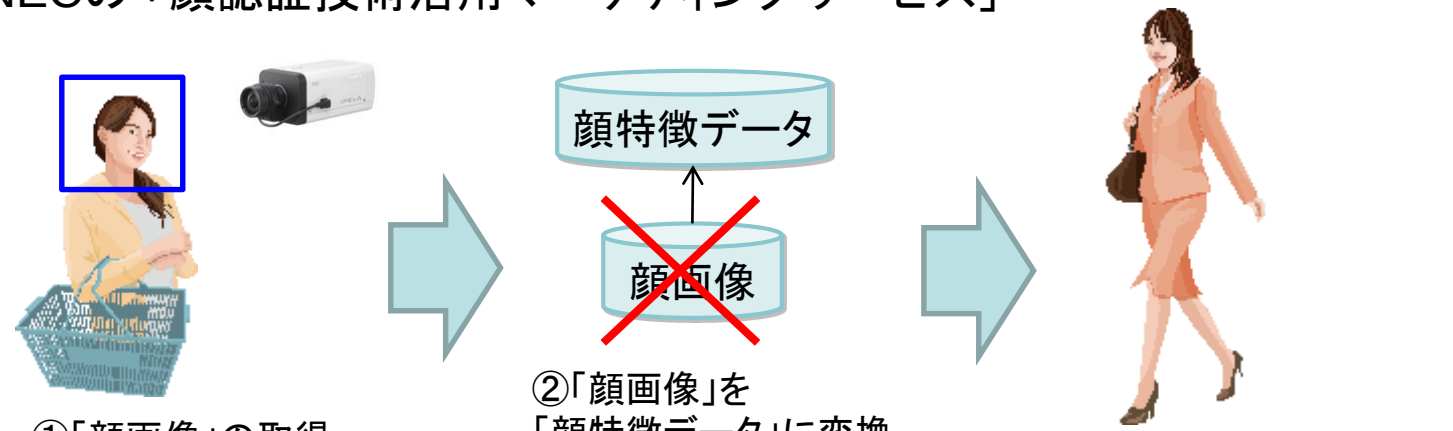
- 実際の事例
  - KDDIグループ会社：

    訪日外国人向けのアプリ「TRAVEL JAPAN WiFi」で得られる情報（国籍、訪問先、滞在時間など）の匿名加工を検討。
  - ソフトバンク：

    プライバシーポリシーの中で匿名加工情報の利用目的や第三者提供の目的、匿名加工方法について言及。

個人識別符号： 顔特徴データ

○NECの「顔認証技術活用マーケティングサービス」



①「顔画像」の取得

②「顔画像」を「顔特徴データ」に変換（＝数値化）

③「顔画像」の削除

④「顔特徴データ」の利用（リピート顧客の識別）

○大阪駅ビルにおける顔認識技術の実証実験

- 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、通行人の顔映像を顔特徴データに処理した後、顔特徴データ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ていた。
- 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）

○万引き犯を識別する防犯カメラ・顔認識システム

- 来店客の顔特徴データに対して、「万引き犯」「盗撮犯」といったフラグを立てて登録し、照合した場合に警備員のスマホにアラートを送ることが可能な防犯カメラ・顔認識システム。大手書店チェーン、ドラッグストアチェーン、百貨店等で導入が進んでいる。

防犯カメラ・顔認識技術の利活用における課題

- 防犯カメラと顔認識技術の結合に対するプライバシー懸念
  - 公共空間での匿名性の喪失:

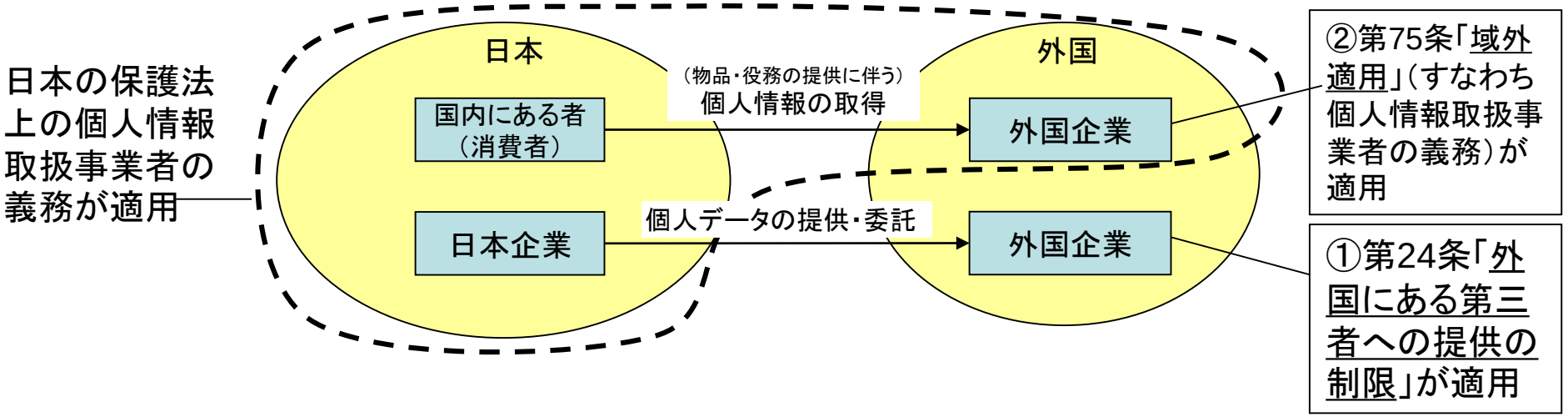
    ボディカメラで撮った顔画像をSNS等の写真データベースを用いて照合する。これにより、路上・駅・ショッピングセンターといった場所で、通りすがりの人物がどこの誰かを特定できてしまう。
  - 現実世界(オフライン世界)での個人の追跡:

    さらに、警察・自治体や企業が顔画像や顔特徴データを共有するようになれば、カメラのネットワークが様々な場所での個人の動きを容易に追跡可能となる。
  - 誤照合・差別待遇:

    ある人の顔画像が万引き犯と誤って登録された場合、個人にとって不利な情報が長期的に保存される恐れがある。
- 顔認識技術を店舗や駅等で利用するに当たっての課題
  - コンプライアンスの問題:「どのように法律(個人情報保護法)を守ればよいか」
  - 社会的受容性の問題:「消費者の漠然とした不安感に対処し、消費者から反発を受けない(炎上しない)ためにはどうしたらよいか」
- 札幌市役所の事例(2017年3月)
  - マスコミの「顔認証実証実験」との誤認報道により、札幌駅前通地下広場での人流センサーを用いた実証実験を中止。
- 政府の取組み
  - IoT推進コンソーシアム／総務省／経済産業省「カメラ画像利活用ガイドブック」(2017年1月)
  - 個人情報保護委員会:カメラ画像利活用の在り方に関する事務局レポートを作成中

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）



外国にある第三者への提供の制限

- 個人情報取扱事業者が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）できるのは、以下の場合に限られる。

  - （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の規則で定める国の場合
    →当面、予定なし。

  - （2）第三者が、個人情報保護委員会の規則で定める基準に適合する体制を整備している場合
    - 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ケース
      → 委託元と委託先の間で適切な契約、確認書、覚書等を取り交わしていること　または、
      → 委託元の日本企業がAPECの越境プライバシールール（CBPR）の認証を得ていること　または、
      → 委託先の外国事業者がAPECの越境プライバシールール（CBPR）の認証を得ていること
    - 事例2）同一の企業グループ内で個人データを移転するケース
      → 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が適切であること　等

  - （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

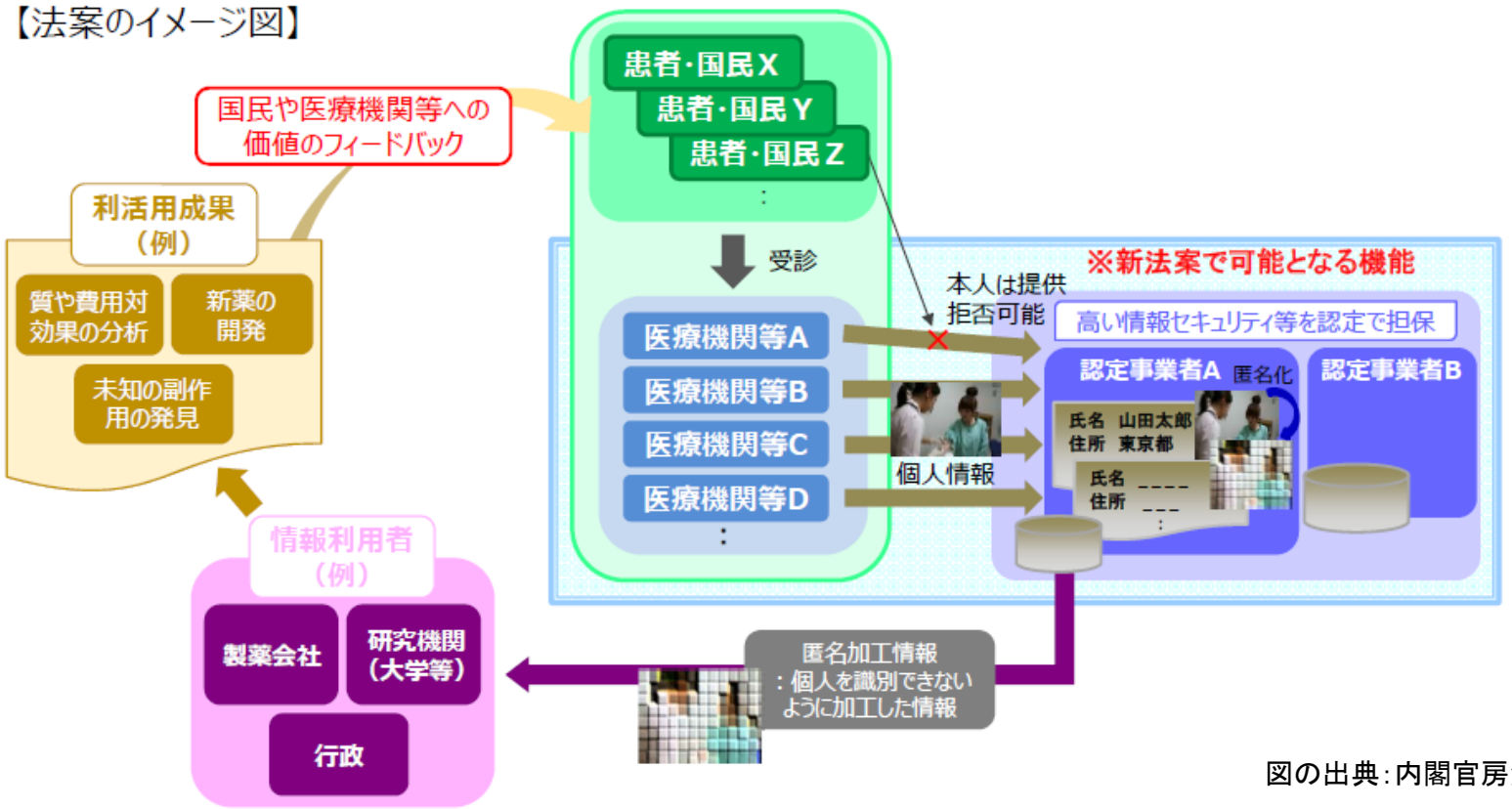
個人情報の利活用に関連した法律

- 「改正個人情報保護法」
  - 第1条で「個人情報の有用性に配慮しつつ、個人の権利利益を保護する」と謳うものの、全体としては「利活用」の要素は少ない。
  - 個人情報利活用のために「個人情報保護法の特例措置」が検討された。
    → 下記の「匿名加工医療情報」に関する法律（★）

- 「官民データ活用推進基本法案」（議員立法：2016年10月に法案提出、12月7日に成立）
  - インターネット等を通じて流通する多様かつ大量の情報を適正かつ効果的に活用することにより、急速な少子高齢化の進展への対応等の我が国が直面する課題の解決に資する環境をより一層整備することが目的。
  - 基本的施策として、「行政手続等におけるICTの利用」、「国及び地方公共団体等が保有する官民データの容易な利用」、「国の施策と地方公共団体の施策との整合性の確保」等について必要な措置を講ずる。
  - 官民データ活用の推進に関する施策を推進するため、IT総合戦略本部に、内閣総理大臣を議長とする官民データ活用推進戦略会議を置く。
- 同基本法の下の個別法
  - 「医療分野の研究開発に資するための匿名加工医療情報に関する法律案」（2017年3月10日法案提出、4月28日成立）（★）
  - その他、個人関与の下でデータ流通・活用を進める仕組みも検討（情報銀行、PDS）

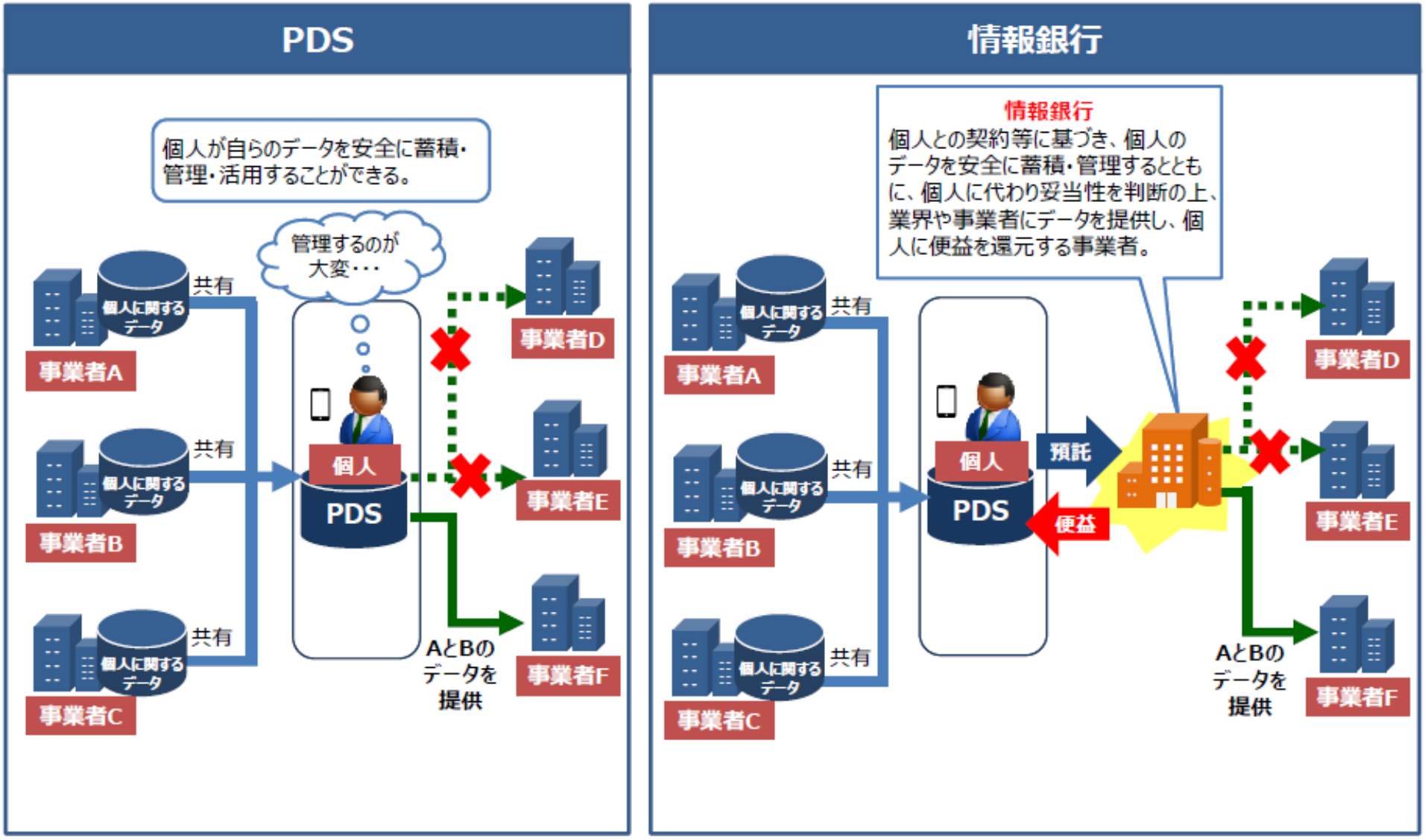
医療分野の研究開発に資するための匿名加工医療情報に関する法律

- 国の施策としては、医療機関が保有するデータを大量に集めて分析させ、医療行政や研究機関・製薬企業等の利用に供することで、医学研究の向上や医療関連事業の発展に役立てたい。
- しかし、改正個人情報保護法の下では、医療機関が保有する病歴・検査結果等の要配慮個人情報は、事前の本人同意なく（オプトアウトで）提供できない。
- そこで、個人情報保護法の特例措置として、国が一定の要件を満たすとして認定した事業者（認定匿名加工医療情報作成事業者）に対しては、医療情報のオプトアウトによる提供を可能とする。



図の出典：内閣官房資料

【ご参考】 PDS(パーソナルデータストア)と情報銀行

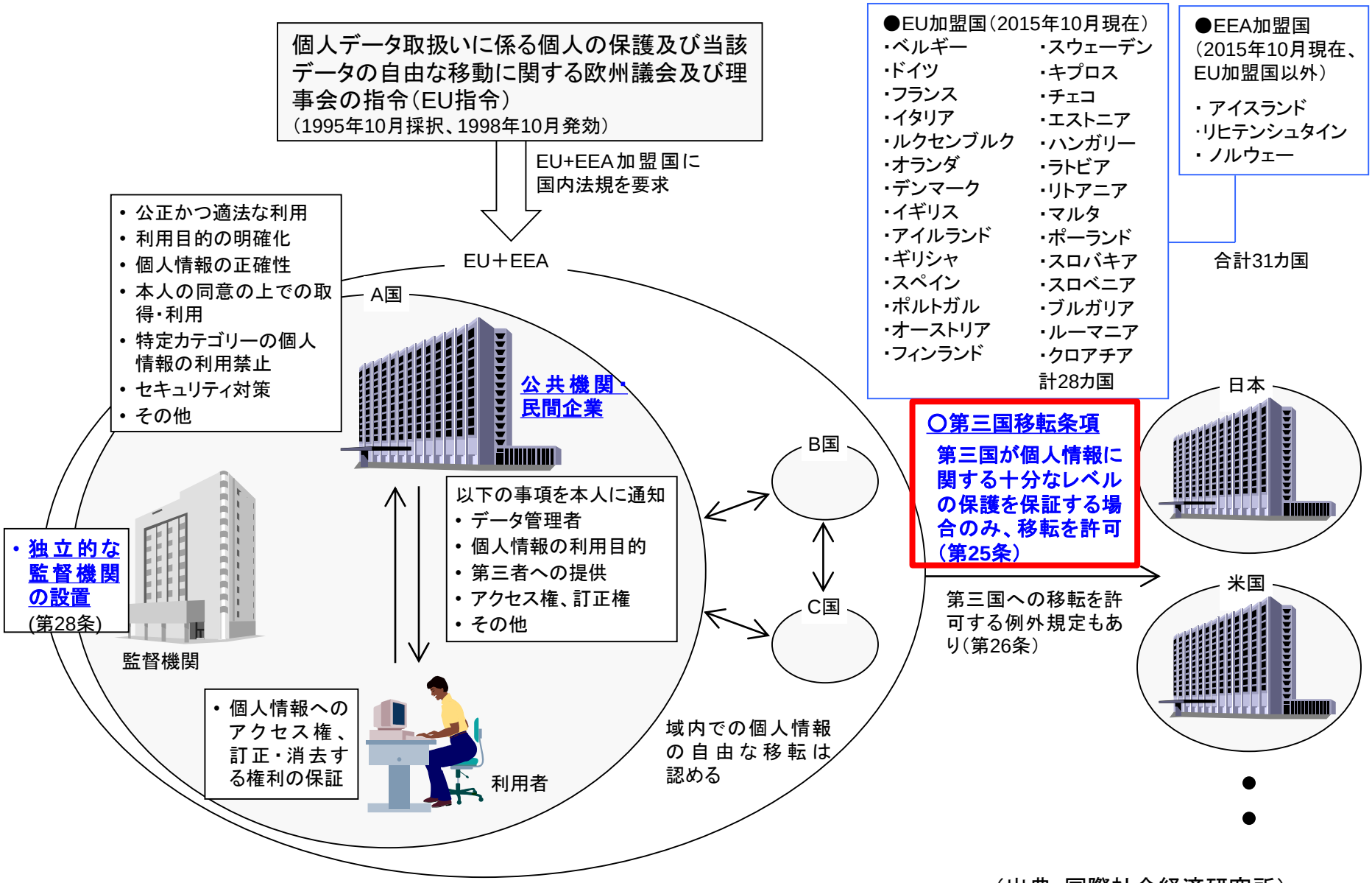


（出典：IT総合戦略本部 データ流通環境整備検討会 AI、IoT時代におけるデータ活用ワーキンググループ 2016年9月資料）

1. 改正個人情報保護法

2. EU・米国の動向

現行のEUデータ保護指令の概要



（出典：国際社会経済研究所）

EUデータ保護指令改定の背景

- 今回の改正は、指令の採択から20年近く経ち、インターネット等の急速な技術的進歩やグローバル化の進展によって発生してきた、以下のような新たな課題に対処するためのもの。

① **急速なICT技術の進歩とグローバル化の進展と、それによるリスクの拡大**
- クラウドコンピューティングに代表される国境を越えたデータ流通の増大
- SNSなど、個人データの公開・共有化の拡大
- 行動ターゲティング広告、GPS携帯電話など、個人データ収集手段の高度化

② **現行のデータ保護スキームに対する企業の不満の増大**
- 多国籍企業にとって負担が大きい非効率・非整合的な規制の緩和要求の増大
  - 従来、各加盟国ごとに異なる国内法や、各国の監督機関の決定を遵守する必要があった。
  - 管理者は原則として全てのデータ処理内容を監督機関に通知する義務があった。
  - BCR（拘束的企業準則）の承認には3つの監督機関のレビューが必要だった。

- **①については、とりわけEU市民や規制当局にとっての懸念は下記2つの国家群**。

〇米国：
- 全世界から個人データを収集する米国の多国籍企業（「データの蛸」）。ex. Google, Facebook
- スノーデン事件で明るみに出たPRISMにより、米国IT企業からデータ収集できる米国政府。

〇データ保護法の整備されていない新興国：
- 低賃金で欧州企業からデータ処理の委託（オフショアリング）を受ける企業。

→EUデータ保護規則には、（特に米国企業に対する）非関税障壁の側面もある

（出典：国際社会経済研究所）

EUデータ保護規則(GDPR)の主要スケジュール

● これまでの経緯と今後のスケジュール

- (1995年10月　EUデータ保護指令の採択)
- 2012年1月　欧州委員会による**EUデータ保護規則案の公表**
- 2016年4月14日　**欧州議会で正式採択**
- 2016年5月4日　EU官報で公布
  http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- 2016年～17年:　準備期間
  - 諮問機関(EU指令第29条作業部会)によるガイドラインの作成
  - 2016年12月13日に第一弾として、以下を公表。パブコメを経て4月5日に採択。
    - データポータビリティの権利に関するガイドライン(WP242)とFAQ
    - データ保護オフィサー(DPO)に関するガイドライン(WP243)とFAQ
    - 主たる監督機関に関するガイドライン(WP244)とFAQ
  - 2017年4月4日には、第二弾として以下を公表。
    - DPIA(データ保護影響評価)に関するガイドライン案(WP248)
  - 2017年内に、以下に関するガイドラインの作成を予定。
    - 認証、同意、プロファイリング、透明性、データ違反報告、データ移転
- 2018年5月25日:　**新規則のEU加盟国(+EEA加盟国)への直接適用**(application)

EUデータ保護規則(GDPR)での主な改正点

- 規制緩和となった点:
  - 指令から規則への格上げにより、加盟国に直接適用(加盟国間のルール差が消失)
  - 個人データ取扱事務の監督機関への届出義務廃止　等

- 規制強化となった点:
  - 外国企業への域外適用(Facebookなど、EU市民に直接サービス提供の場合)
  - 忘れられる権利
  - データポータビリティの権利
  - データ違反時(漏洩時など)の報告義務
  - データ保護影響評価の義務
  - 罰則強化(違反時に最大で2000万ユーロまたは年間世界売上の4%の罰金)　等

- EU域内からのデータ移転規制について:

  → ほぼ内容変わらず

  ※ JEITA(電子情報技術産業協会)／JISA(情報サービス産業協会)等のロビー活動によって、認証制度を用いたデータ移転手段は追加された。

GDPR：忘れられる権利とデータ・ポータビリティの権利

○ 第17条　消去する権利（「忘れられる権利（Right to be forgotten）」）

- 現行EU指令の第12条にも自分の個人データを消去する権利が規定されているが、これを精緻化。
- 現行では、データが不正確だったり不法に収集された等の理由がないと消去できないが、新規則では**本人が同意を撤回した場合にも、管理者に消去してもらう権利を保障**。
- また、管理者が個人データを公開している場合、管理者は、**当該個人データを処理している他の管理者に対して、データ主体が当該個人データへのリンクやコピーの消去を求めていることを通知するための合理的な措置（技術的な措置を含む）を取らないといけない**（利用可能な技術や実施にかかるコストは考慮した上で）。

○ 第20条　データ・ポータビリティの権利

- 個人がサービス提供者から自分の個人データを一定の機械可読フォーマットで入手し、他のサービスに移転する権利を保障。
- ex. 個人がSNSサービスを他のサービスに切り替える場合

GDPR：忘れられる権利（第17条）

●GDPRに「忘れられる権利」が導入されたきっかけ

- Facebookの会員だったオーストリアの法学生Schrems氏が、同社に自分に関する全ての個人データの開示請求を行ったところ、彼が自覚している以上の個人データがサイトに収集されており、彼が削除したはずの個人データまで保存されていた。

- このような事態を防ぐため、EU規則では、以下が導入された。
  - SNSサイト等の管理者が収集したり処理する**個人データを最小限に留めること**の義務。（第5条個人データ処理原則）
  - **デフォルト設定においてデータが公開されない**ようにする義務。（第25条データ保護バイ・デフォルト）
  - 個人が自分の個人データの消去を請求し、かつそれらを保持する正当な理由が無い場合、管理者が当該データを消去する義務。（第17条忘れられる権利）

- GDPRの下では、Facebookは消去請求のあったデータを直ちに、かつ完全に消去する義務が生じることになる。

現行EU指令の下での「忘れられる権利」

- スペイン人によるGoogle検索結果への申立て
  - 2010年、スペイン在住のコステハ氏が、自分の氏名をGoogle検索すると検索結果に自分に関する過去の記事（※）が表示されるとして、現地新聞社にその記事の削除を、**Google SpainおよびGoogleに検索結果での記事の非表示を求め**、スペインデータ保護局に救済の申立てをした。
    - ※コステハ氏の未払い社会保険料徴収のために差押・不動産競売手続が行われるとの公告を載せた、現地紙の1998年当時の記事。
  - スペインデータ保護局は、新聞社への請求は却下したが、Google SpainおよびGoogleに対する請求は認めた。Google両社は判断取消しを求めてスペイン高等裁判所に提訴。2012年3月、スペイン高等裁判所は欧州司法裁判所に先決裁定を付託。
- 欧州司法裁判所の裁定結果（2014年5月）
  - 検索エンジン事業者はEU指令に言う「管理者」に該当するのか？

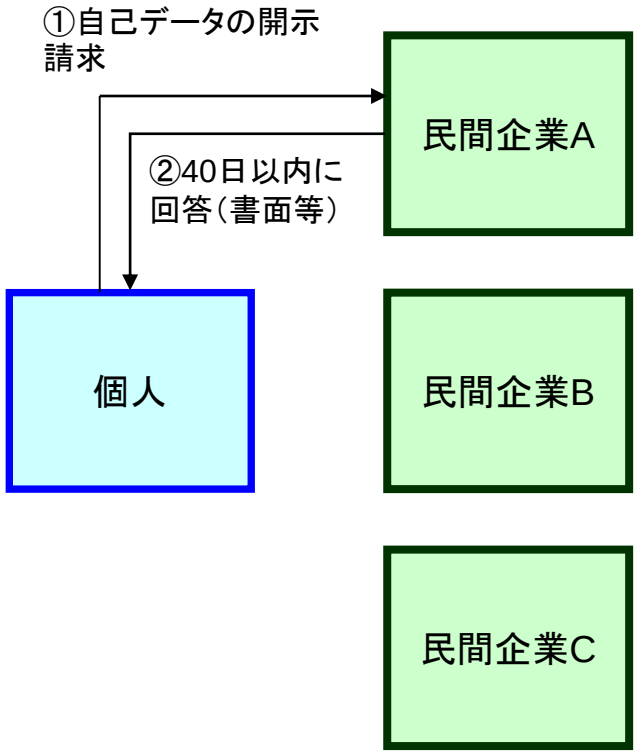
⇒検索エンジンの動作は、ネット上の情報を自動的に索引付けし、一時的に蓄積し、特定の優先順位に従って利用できるようにするものであるため、そこに個人データが含まれていれば、**この一連の動作はEU指令にいう「個人データの処理」に該当**する。従って、**検索エンジン事業者には「管理者」として検索結果の消去請求に応じる義務**が生じる。

参考文献：今岡直子「『忘れられる権利』をめぐる動向」

- Googleの対応
  - この裁定を受け、Googleは「Google.es」「Google.fr」等、EU域内ドメインからの検索結果に限って消去請求に対応（検索結果を削除）。
  - 2015年6月、フランス当局は「Google.com」を含む全世界サイトから検索結果を削除するように命令。

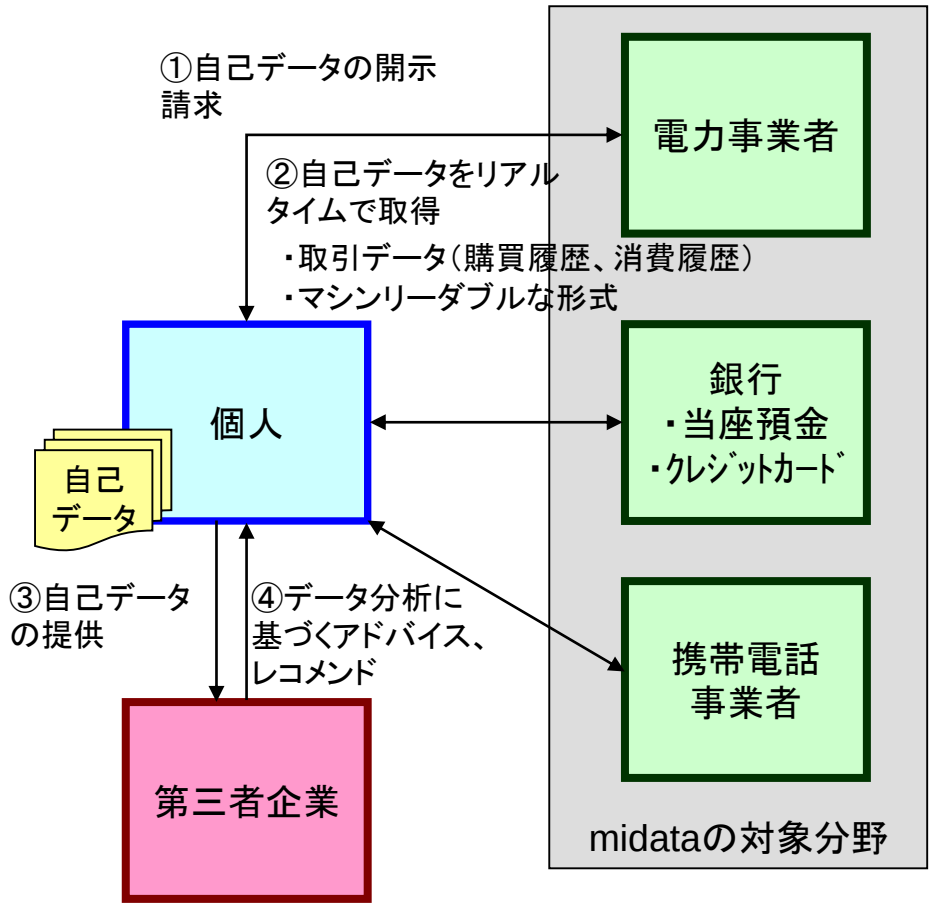
データ・ポータビリティの権利の事例： 英国midata

○英国での従来の自己データ開示制度



- 企業に対する自己データの開示請求は法的権利として認められているが、**取得に最大で40日間かかる**（データ保護法の規定）
- **電子的形式で取得する権利は認められていない**
- **国民の半数以上が開示請求権を知らない**

○ midataの枠組み



- 個人が開示請求をした際、**自己データをリアルタイムで取得することが可能に**なる
- 第三者企業も利用できるような、**一定のマシンリーダブルな形式の電子データ**を取得可能

出典：国際社会経済研究所

GDPR：データ違反時（漏洩時等）の報告（第33条、第34条）

○ 第33条　個人データ違反の監督機関への通知

- 個人データ違反（personal data breach、※紛失・盗難・漏洩・不正利用等）があった場合、それが個人の権利と自由にリスクをもたらしそうにない場合を除き、管理者は不当な遅滞なく、実行可能な場合には**個人データ違反に気づいてから72時間以内に**、監督機関に当該個人データ違反について通知（報告）するものとする。72時間以内になされない場合には、監督機関への通知は合理的な正当化と共になされるものとする。
- 通知項目は、漏洩データ等の対象人数・データ項目、データ保護オフィサーの連絡先、起こりうる結果（影響）、管理者が取る予定の対応策等。

○ 第34条　個人データ違反のデータ主体への連絡

- 個人データ違反が個人の権利と自由に高いリスクをもたらしそうである場合、管理者は不当な遅滞なく、データ主体に当該個人データ違反について連絡するものとする。
- ※第34条3項では、管理者が適切な技術的及び組織的保護措置を取っており、これらの措置（暗号化等）が個人データ違反の影響を受けるデータに適用されていた場合や、データ主体の権利と自由への高いリスクが具体化されないことを保証するような実質的措置を取っている場合には、データ主体への連絡は必要ないとされている。

GDPR:データ漏洩時等の報告(第33条、第34条)

●GDPRに「データ違反時の報告・連絡」が導入されたきっかけ

- 2011年4月、SCEのPlayStation Networkがサイバー攻撃され、全世界(EU含む)の数千万人分の個人データ(氏名、住所、クレジットカード情報等)を含むデータベースが不正アクセスされた。SCEがその事実を利用者に知らせるまでに、一週間もかかった。

- このような事態を防ぐため、EU規則では、企業に対して以下のことを義務付けた。
  - データ違反を防止し回避するための安全管理措置を強化する義務。(第32条安全管理措置)
  - 実行可能な場合は、データ違反が発見されてから72時間以内に監督機関に報告するとともに、不当な遅滞なく個人にも連絡する義務。(第33条、34条)

GDPR:データ保護影響評価(第35条)、課徴金(第83条)

○ 第35条　データ保護影響評価

- 個人の権利や自由に高いリスクをもたらしそうな個人データ処理(**プロファイリング**、**特別カテゴリーの個人データの大規模処理**、**有罪判決・犯罪に係わる個人データの大規模処理**、**公共空間の大規模なモニタリング**等)について、データ保護影響評価(※PIAに該当)を義務付け。

○ 第83条　行政罰を科すための一般条件

- 監督機関は、本規則の違反に対し、最大で**2000万ユーロ**、又は企業の場合には最大で**前年度の年間世界売上(total worldwide annual turnover)の4%**の課徴金を科すことができる。

GDPR：データ保護影響評価（DPIA）に関するガイドライン

- EU指令第29条作業部会（EU各国のDPAおよび欧州データ保護監察官（EDPS）で構成）はGDPR施行のためのガイドラインを検討。

- 2017年4月4日には、DPIA（データ保護影響評価）に関するガイドライン案が公表された。
  - 「Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/6792」（WP248）
  - 5月23日までパブコメを実施。

- 同ガイドラインでは、DPIAを行うべきデータ処理活動のクライテリアとして、次頁以下の10クライテリアを開発。データ処理活動がこれらのうち、2つ以上のクライテリアに適合する場合にはDPIAが必要。

DPIAを行うべきデータ処理のクライテリア（１/３）

クライテリア	説明
1.評価（Evaluation）またはスコアリング	プロファイリングや予測を含む。とりわけ、「データ主体の業務実績、経済状況、健康、個人的嗜好、興味、信頼、行動、所在又は移動に関連する側面」から得られるもの。 • 銀行が顧客を信用照会データベースを用いてスクリーニングする場合 • バイオテクノロジー企業が病気・健康リスクを評価し予測するために顧客に直接的に遺伝子検査を行う場合 • 企業がWebサイトの利用やナビゲーションに基づいて行動・マーケティングプロファイルを構築する場合　など
2.法的または同様に重大な影響を与える自動意思決定	データ主体に「自然人に関する法的な効果」を生じさせるか、「同様に自然に重大な影響を与える」ような意思決定を目的とした処理の場合（第35条3項(a)）。 • 処理が個人の排除や差別を導くかもしれない場合　など • 個人にほとんど影響を与えない、あるいは何ら影響を与えない処理については、このクライテリアに該当しない。
3.体系的監視	データ主体を観察したり監視したり管理したりするための処理。 • 「誰でも立ち入ることの出来る場所における体系的監視」（第35条3項(c)）を通じて取得されたデータ　など • このタイプの監視をクライテリアとしているのは、誰が自分のデータを取得しており、どのように利用されるのかデータ主体が気づかないような状況で個人データが取得される恐れがあるため。また、頻繁な人通りのある公共空間（または誰でも立ち入ることの出来る場所）においてそのような処理を受けることを個人が回避できない恐れがあるため。

DPIAを行うべきデータ処理のクライテリア（2/3）

クライテリア	説明
4.センシティブデータ	• 第9条で規定された特別な種類のデータ（例えば個人の政治的思想に関する情報） • 有罪判決や犯罪に関する個人データ • 一般的に個人の権利利益に対する潜在的なリスクを増すとみなされる可能性のあるデータ。例えば、電子通信データ、位置データ、金融データ • 純粋に個人的な活動や家庭活動の過程で個人によって処理された情報。例えば、個人文書管理・電子メールサービス・日記・ノート・その他さまざまなライフログサービスのためのクラウドサービスで処理される情報など
5.大規模に処理されるデータ	データ処理が大規模に実施されているかを決定する際には、とりわけ以下の要素が考慮されるべき。 ・関係するデータ主体の数（絶対数、または人口等に占める割合） ・データの分量および／またはデータ項目の範囲 ・データ処理活動の期間 ・データ処理活動の地理的範囲
6.照合・結合されるデータセット	様々な目的および／または様々な管理者によって実施される複数のデータ処理活動から得られたデータセットの照合や結合であって、データ主体の合理的な期待を超えるような方法で行われたもの。

DPIAを行うべきデータ処理のクライテリア（3/3）

クライテリア	説明
7.脆弱なデータ主体に関するデータ	データ主体と管理者の間のパワー不均衡のため、このタイプのデータ処理はDPIAが必要となりうる。 • 雇用主によるデータ処理が人事管理と関連している場合、従業員はそれに反対することに重大な困難が伴うことがある。 • 子どもは自分のデータの処理について理解した上で反対したり同意することはできないと考えられる。 • 特別な保護を必要とするような脆弱な人々、例えば精神疾患者、亡命希望者、高齢者、患者など。
8.革新的な利用、技術的または組織的なソリューションの適用	新たな技術の利用によって、個人の権利利益に高リスクをもたらす恐れのある新たな形態のデータ取得や利用が生じえるため。 • 物理的アクセスコントロールのための指紋と顔認識の統合利用など。 • IoTアプリケーションは個人の日常生活やプライバシーに重大な影響を及ぼしうるため、DPIAが必要であるかもしれない。
9.EU外部への越境データ移転	移転先の国、オンワードトランスファーの可能性、例外条項に基づく移転の可能性等について考慮する。
10.データ処理が「データ主体による権利行使やサービス・契約の利用を妨げる」場合	• 人々が通行せざるを得ない公共エリアで実施されるデータ処理 • サービス利用や契約締結をコントロールする目的のデータ処理（銀行による信用照合データベースでの顧客のスクリーニングなど）

DPIAクライテリアの適用例

データ処理の例	該当するクライテリア	DPIAが必要か否か
病院が患者の遺伝子データと健康データを処理する場合	4. センシティブデータ 7. 脆弱なデータ主体に関するデータ	必要
高速道路における運転行動を監視するためにカメラシステムを利用する場合。管理者は、自動車をsingle out（識別）し、ナンバープレートを自動認識するためにインテリジェントビデオ分析システムの利用を想定。	3. 体系的監視 8. 革新的な利用、技術的または組織的なソリューションの適用	
企業が従業員の仕事場やインターネット行動など、従業員の行動を監視する場合。	3. 体系的監視 7. 脆弱なデータ主体に関するデータ	
民間企業が連絡先名簿のプロファイルを作成するために、ソーシャルメディアで公開されているプロファイル情報を収集する場合。	1. 評価またはスコアリング 5. 大規模に処理されるデータ	
登録者に一般的なオンラインマガジンを送信するためにメーリングリストを利用する場合。	（いずれも該当しない）	必ずしも必要でない
eコマースサイトが、同サイトでの過去の購入履歴に基づき、年代物の車の部品の広告を表示する場合。	1. 評価またはスコアリング（体系的・大々的ではない）	

GDPR：適切な安全管理措置による移転（第46条）

○ 第46条　適切な安全管理措置による移転

- 欧州委員会による十分性認定がない第三国への個人データ移転は、以下の安全管理措置がある場合に可能。
- ①監督機関の個別のオーソライズが不要な場合
  - 公的機関間での法的拘束力のある文書
  - BCR（拘束的企業準則）
  - 欧州委員会に採択されたSCC（標準契約条項）
  - EU加盟国の監督機関に採択された標準契約条項
  - **第40条に則り承認された行動規範**（第三国の受領者におけるもの）
  - **第42条に則り承認された認証制度**（第三国の受領者におけるもの）
- ②監督機関の個別のオーソライズが必要な場合
  - 管理者または処理者と第三国の受領者の間の契約条項
  - 公的機関の間での行政的取り決めの中の条項（行使可能なデータ主体の権利を含むもの）

- **従来のEU指令に基づく「SCC」は、欧州委員会によって修正、置換又は廃止されるまで、効力を持ち続ける**。従来のEU指令に基づく「BCR」は、当該監督機関によって修正、置換又は廃止されるまで、有効である。

EUから第三国への個人データ移転方法（現行）

【現行のEUデータ保護指令の規定】

- 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**（2015年に無効判決、2016年よりPrivacy Shield）

- 欧州委員会は2000年に、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ついて個人情報の「十分なレベルの保護」を行っていると認める決定を行った。（セーフハーバー決定）
- 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。

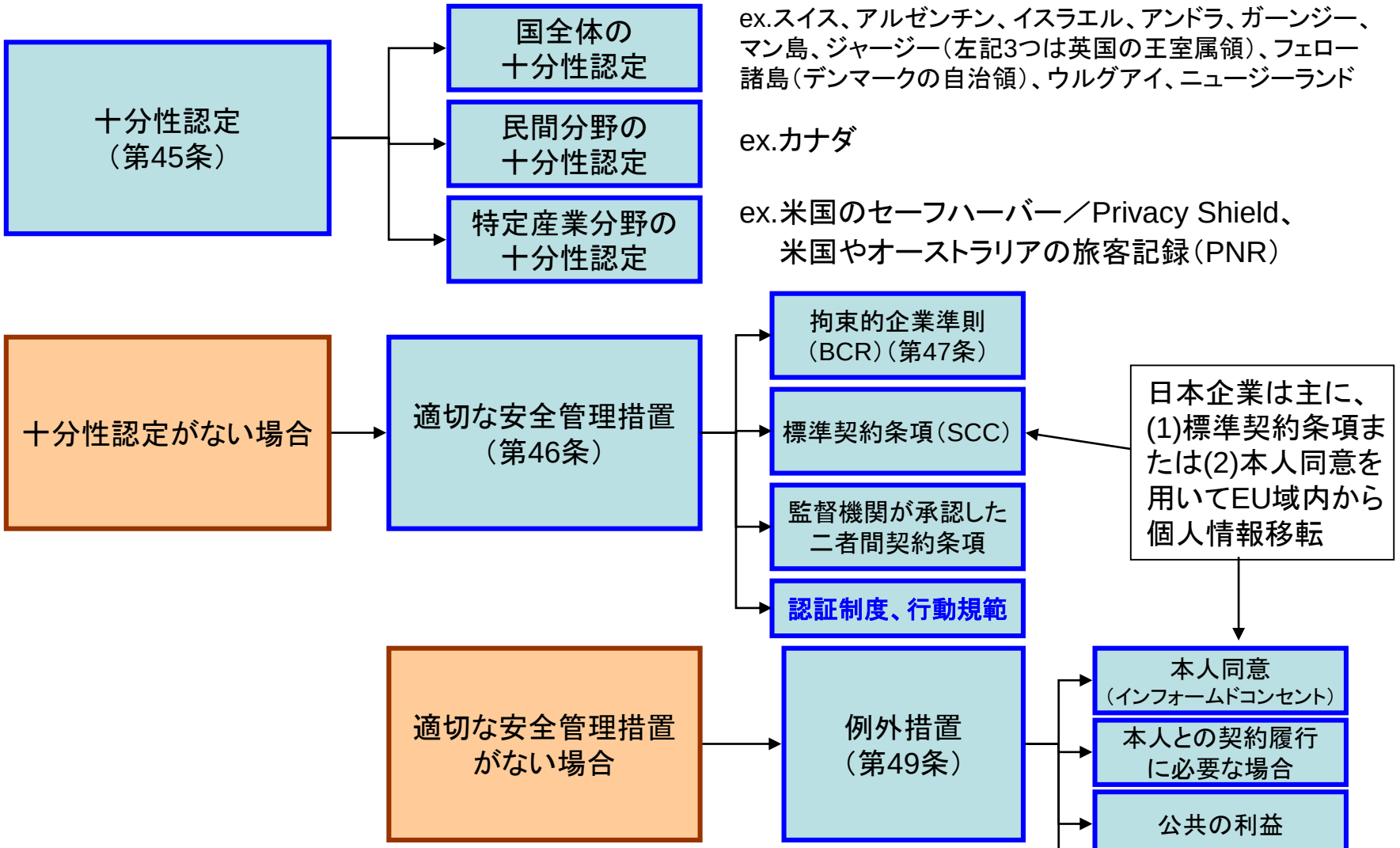
③ 例外規定として、

- **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。
- **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。
- 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から第三国への個人データ移転方法（GDPR）



(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からの個人データ移転等に当たって注意すべきケース

I. 自動車の車載機器から得られる位置データ・プローブデータや電化製品の利用履歴データ・保守データを、データ分析や研究開発のために欧州現地法人で集めて利用する場合。これらのデータは使用者の氏名を伴わなくても、機器IDが付されている場合にはEUにおいて個人で0田とみなされうる。また、氏名や機器IDを伴わなくても、位置データや利用履歴データは集積することにより個人データとみなされうる。このような場合、欧州現地法人はGDPRを遵守した取扱いを行わないといけない。

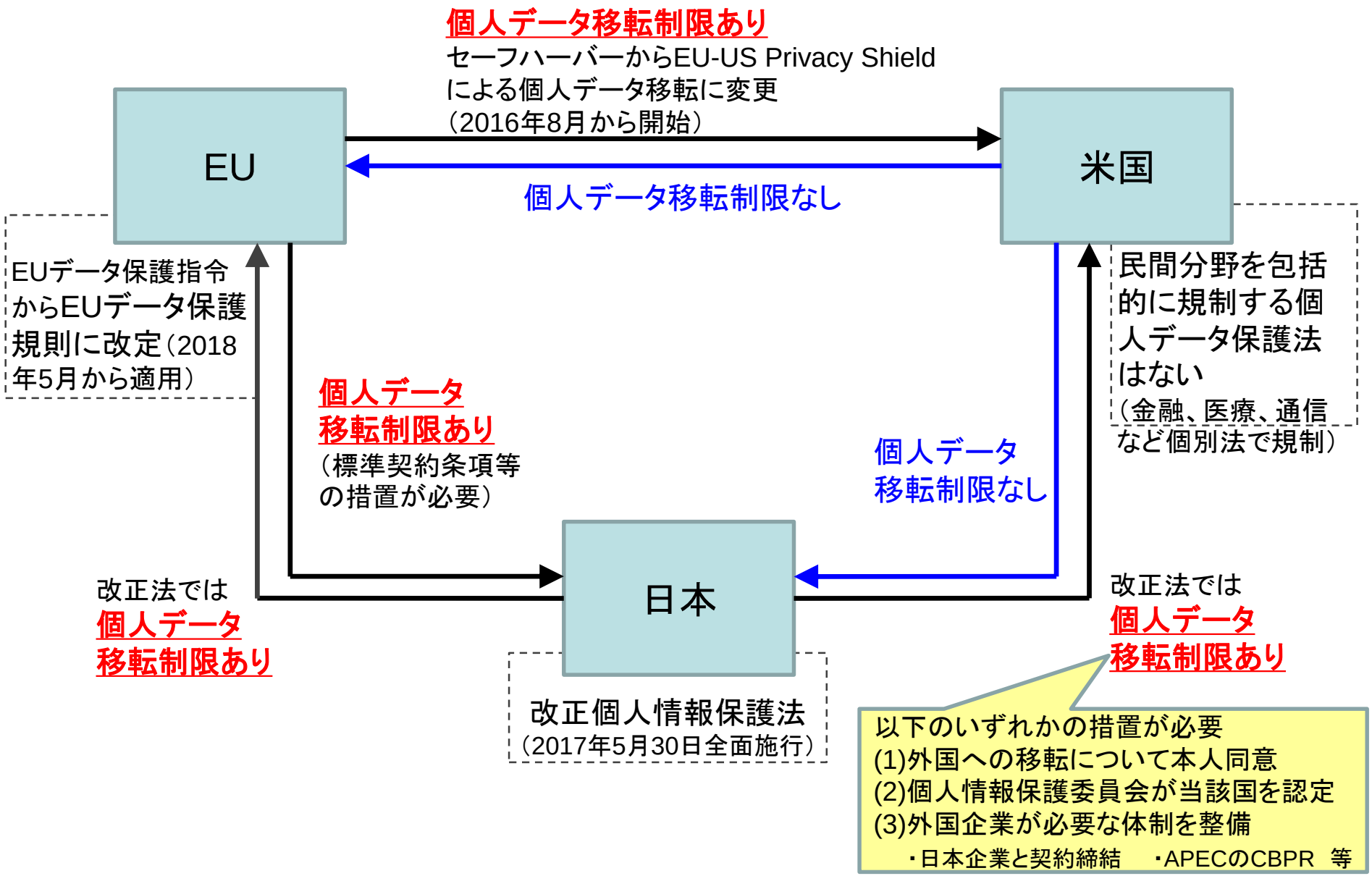
II. 店頭や街角の防犯カメラから得られる顔画像や顔特徴データをデータ分析や研究開発のために欧州現地法人で集めて利用する場合。EUでも、顔画像が個人情報に該当するのみならず、顔特徴データも個人データと解釈されている。これらのデータを取得する場合、欧州現地法人はⅠと同様にGDPR全般を遵守しないといけない。この場合は特に、事前にデータ影響保護評価を行う義務が生じる。また、本人から顔画像や顔特徴データの開示請求があった場合の対応方法についても考慮が必要。

III. 上記Ⅰ・Ⅱのデータを日本の本社に送信して分析等を行う場合。これは個人データの第三国移転に当たるため、欧州現地法人との間でSCCを結ぶなどの措置を取らないと、違法となってしまう。

IV. 上記Ⅰ・Ⅱのデータを EU域外のクラウド事業者に預ける場合。日本では、ホスティングなどクラウド事業者に個人データを単に預ける行為（IaaS）は、個人情報保護法にいう「委託」に基本的には当たらない。しかしEUでは単に預ける行為も個人データの処理の委託とみなされ、域外事業者への「移転」に該当するため、SCC締結など第三国移転のための措置を取らないといけない。EU離脱後は英国もEU域外国となるため、注意が必要。

V. 個人データの第三国移転には、データを提供したり委託したりするケースのみならず、データに第三国からのアクセス許可を与えることも該当する。例えば、EU域内の医療機関が保有する病理画像に日本国内から病理医がアクセスするような場合。

越境データ移転： 日米欧データ移転の全体像



日米欧における個人データ移転

- 米国には、（前頁の図のように）米国からEUや日本等の外国へのデータ移転制限がないにもかかわらず、事実上、米国企業に大量の個人データが集まっている。

- 米国に個人データが集まるのは次の理由である。
  - 個人からデータを集めるGAFA （BtoC）
  - 企業からデータを集めるクラウド事業者 （BtoB）

  あくまでビジネスの優位性の問題であって、制度の問題ではない。

  （あえて制度上の優位性を挙げれば、米国には民間企業一般を規制する個人情報保護法がない。）

- 2017年6月には公正取引委員会が「データの集積によって、独占や寡占（競争の制限）をもたらし得る企業結合や、市場における地位を利用した消費者・中小企業からのデータの不当な収集（搾取）、あるいは不当な「囲い込み」に対しては、独占禁止法による対応が必要」として、論点を整理した報告書を公表。

- データの国外移転を防ぐため、ロシア、中国のようにデータローカライゼーション政策（後述）を取る国もあるが、日本がそのような国際世論から叩かれるような政策を取ることは現実的ではない。

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／規則における第三国移転条項
- アジア諸国(EUと同様な第三国移転条項がある国)
  - 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(**相手国の個人情報保護レベルに関わらず移転を禁じる**)
  - **ロシア**:2014年7月成立(2016年9月施行)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。
  - **中国**:2016年11月成立のサイバーセキュリティ法において、重要情報インフラ事業者に対して国内で取得されたデータの国内保管義務を規定。
  - **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という。
  - 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り、このことがDL政策を取る国に格好の口実を与えている。

【ご参考】G7におけるデータローカライゼーションへの言及

- G7 情報通信大臣共同宣言（2016年4月29・30日）
  - ⅱ. 情報の自由な流通の促進と保護
  - **情報の自由な流通の促進と保護**のため、我々は、以下の取組を奨励する。
  - a) インターネットのオープン性及び越境情報流通の促進
  - 我々は、引き続き、インターネットのグローバルな本質を維持し、越境での情報流通を促進し、また、インターネット利用者が、自らの選択に基づきオンラインの情報、知識及びサービスにアクセスすることを許容するようなICT 政策を支持する。我々は、公正な公共政策の目的を考慮した場合に**正当化することのできない、データローカライゼーション要求**に反対する。
  - b) プライバシー及びデータ保護の促進
  - 我々は、プライバシー及びデータ保護についての高い基準を満たすため、各国の法域をまたがる効果的なプライバシー及びデータ保護を一層促進するような政策枠組みの整備に努める。また、我々は、プライバシー及び個人データ保護を設計段階全体を通じて考慮した、**プライバシーバイデザインなどのプロアクティブな方法を歓迎**する。

- G7 伊勢志摩首脳宣言（2016年5月27日）
  - 我々は，プライバシー及びデータの保護やサイバーセキュリティを尊重しつつ，インターネットの開放性，透明性及び自由を確保するため，**情報の自由な流通**及びデジタル・エコノミーの全ての主体によるサイバー空間への公平かつ平等なアクセスを促進することにコミットする。

越境データ移転： 最近の状況

- EUから日本への個人データ移転について、現状では不自由な状況にあるが、日本政府は日EU間の「相互の円滑なデータ移転を図る枠組みの構築」を目指して2016年からEU側と協力対話を続けている。
- 他方、欧州委員会は2017年1月10日に越境データ移転に関するコミュニケーション「Exchanging and Protecting Personal Data in a Globalised World」を発行し、十分性認定については日本と韓国を優先的に検討するとしている。
  - ただし「EUのデータ保護ルールは、FTA交渉のサブジェクトにはなりえない。第三国とのデータ保護に関する対話と貿易交渉とは、別々のトラックで行わなければならない」と同文書で明言している。
- 3月20日にはCeBITの中で世耕経産大臣、アンシプ欧州副委員長、ヨウロバー欧州委員、熊澤個人情報保護委員等が日EU間のデータ流通の円滑化について意見交換を行い、共同プレスステートメントを発表。データに関するハイレベルでの対話、専門家対話、関係省庁が連携した取組を推進する。
  - 具体的には、日EU・ICT政策対話、日EU産業政策対話、日・EUビジネス・ラウンドテーブル等の既設の対話と並行して、データ・エコノミーの側面に焦点を当てた専門家会合の開催。
- また、日本はAPECの越境プライバシールール（CBPR）制度に2014年より参加し、2016年6月からは国内でJIPDECを認証機関としてCBPR認証制度の運用が開始されている。

米欧セーフハーバーを巡る動き

- 米国PRISM問題とセーフハーバー・スキーム
  - **2013年6月にスノーデン氏の証言によりPRISMの存在が発覚**。これにより、セーフハーバー・スキームの「十分性」について議論が再熱。
    - PRISM：米国政府による米国インターネット企業からの個人データ収集プログラム
  - **2013年11月27日に欧州委員会**は「セーフハーバーの機能に関する欧州議会および理事会へのコミュニケーション」を発行。**米国に対して2014年夏までに改善策を示すように要請**。
  - 2014年3月には欧州議会がセーフハーバー協定の停止を求める決議案を採択。
  - 欧米間でセーフハーバー見直し作業が続けられてきたが、2015年10月の欧州司法裁判所によるセーフハーバー無効判決によって、この作業が加速されるとともに、見直しのハードルが上げられることとなった。

EU-US Privacy Shield

- 2013年6月にスノーデン氏の証言により米国PRISMの存在が発覚し、セーフハーバーの有効性が揺らぐ。

- 2015年10月の欧州司法裁判所による「米欧セーフハーバー無効判決」を受け、米欧間で新たな枠組みを交渉。2016年2月にPrivacy Shieldに大筋合意。同年8月から運用開始（商務省サイトで受付）。

- 「EU-US Privacy Shield」では、セーフハーバーと同等な内容に加え、以下の3点が追加。

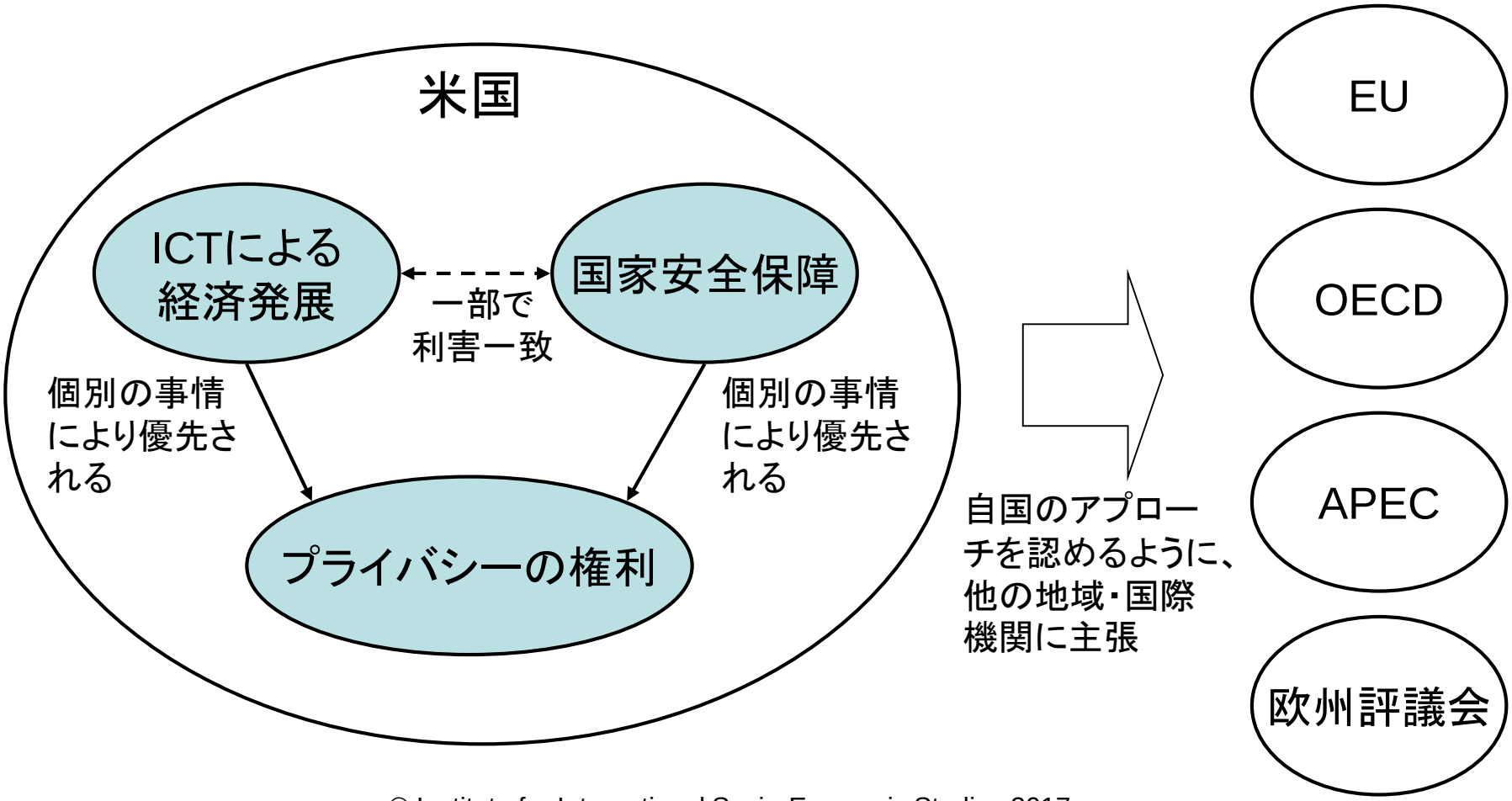
  ①米国企業に対する執行強化
  - 商務省が企業の遵守状況を定期的にモニター

  ②米国政府に対する規制強化
  - 米国政府はEUから移転された個人データに対する無差別な大量監視を行わない
  - 米国政府による国家安全保障目的でのデータアクセスに対するオンブズパーソン新設
  - 米国政府に対する米欧共同での年次レビュー
    →2017年秋に第1回レビュー予定

  ③EU市民に対する有効な権利保護
  - 米国企業のEU市民からの苦情への一定期間内の回答義務
  - EU市民による自国DPA（データ保護監督機関）への苦情申立、DPAから米国機関への苦情照会 等
    →第29条作業部会およびEU各国DPAのウェブサイトに市民用入力フォームを公開予定

米国における個人データ保護の基本的な考え方（仮説）

- 個人データ保護に対する功利主義的／プラグマティックなアプローチ
  - 企業のデータ利用によって個人が実際に不利益を被ることがなければ（何をやっても）よい。
  - 安全保障や経済発展など、米国の国益にかなう要素があれば、プライバシー／データ保護よりもそちらが優先される。（その方が、米国民の利益にもなるでしょう、という考え方。）



【ご参考】 欧州における個人データ保護の権利

- 欧州において、**個人データ保護の権利**は、「欧州連合基本権憲章」第8条や「欧州連合の機能に関する条約」第16条で認められた**基本的人権の1つ**。
- 個人が実際に不利益を被っているか否かは、データ保護にとって本質的な要素ではない。すなわち、当人が何らかの不利益を被っていなくても、個人データ保護の権利を行使することができる。
（義務論的アプローチ）
  - ただし、欧州でも個人データ保護の権利は絶対的な権利ではなく、公共の利益との関係も考慮されなければならない。

- 他方、米国では、企業等のデータ利用によって個人が実際に不利益を被ることがなければ（何をやっても）よいという考え方。いわば、**経済政策と個人データ保護がセット**になっている。

米国の個人情報保護制度

- 個人情報保護制度の概要
  - 行政分野は1974年プライバシー法、及び2002年電子政府法により規制。
  - 民間分野は、HIPAA（医療保険）、電子通信プライバシー法、金融サービス近代化法、FCRA（公正信用報告法）、児童オンラインプライバシー保護法などの**個別法により個別分野を規制するセクトラル方式**。
  - 個別法により規制されない、大多数の民間企業に対しては、**自主規制**を推奨。**企業のプライバシーポリシーに虚偽の記載があれば、FTC法の第5条（不公正な競争方法及び不公正・欺瞞的な行為又は慣行の禁止）によってFTCが法執行を行う**。

- FTC（連邦取引委員会）による法執行の例

Googleに対する法執行（2012年8月）	GoogleとFTCは、閲覧履歴収集に関するグーグルの虚偽説明および前回の同意内容への違反を理由として、制裁金2,250万ドルをFTCに支払うということで同意。
Facebookに対する法執行（2011年11月）	同社のプライバシーポリシーに違反して個人データを第三者に提供していたとして、同社に対して包括的なプライバシープログラムの導入と、外部監査人による20年間に渡る評価を命令。
Googleに対する法執行（2011年10月）	Google Buzzのサービスが同社のプライバシーポリシーに違反していたとして、同社に対して包括的なプライバシープログラムの導入と、外部監査人による20年間に渡る評価を命令。

【ご参考】トランプ政権の動き

- FCC（連邦通信委員会）が制定したブロードバンド・プライバシー規制を撤廃
  - 4月3日、トランプ大統領は、オバマ前大統領時代（2016年10月）にFCCが承認した「ブロードバンドその他の通信サービスの顧客のプライバシー保護に関する規則」を廃止する法案に署名した。
  - 同規則は未施行であったが、ISPに対して、GoogleやFacebookといったウェブサイト以上に顧客のプライバシー保護を要求するものであった。
  - すなわち、ISPに対して、広告やマーケティングの目的で、顧客の正確な位置情報・金融情報・医療情報・子どもの情報・Web閲覧履歴を利用する場合は、事前に同意を取得しなければならないとするものであった。
  - 同規則の廃止は、AT&T、コムキャスト、ベライゾンといったISPにとっては勝利であり、プライバシー擁護団体にとってはダメージである。
  - オバマ政権時代の規則を廃止しようとする一連の動きの1つ。
  - （出典：Reuters記事を抄訳）