EU一般データ保護規則（GDPR）とパーソナルデータ利活用の動向

2018年3月20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

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（EU指令）　採択 ・2012年1月　EU一般データ保護規則案　公表 ・2016年4月　EU一般データ保護規則（GDPR）　採択 ・**2018年5月　EU一般データ保護規則（GDPR）　適用予定**
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） ・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 ・2016年8月　セーフハーバー強化版のPrivacy Shield運用開始
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・韓の5ヵ国）
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）

【ご参考】 欧州・米国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。
  （功利主義的／プラグマティックなアプローチ）

EU一般データ保護規則(GDPR)の経緯

● 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一般データ保護規則(GDPR)案の公表**
  - 2013年10月　欧州議会司法委員会による修正案の採択
  - 2014年3月　欧州議会による議会修正案の採択
  - 2015年6月　EU理事会による理事会修正案の合意
  - 2015年12月15日　三者合意(EU理事会、欧州議会、欧州委員会)
- 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
- 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
- 2018年5月25日:　**GDPRのEU加盟国への直接適用**(application)

GDPRのガイドラインについて

- 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。
- 第29条作業部会が既に採択したガイドライン
  - データポータビリティの権利に関するガイドライン（WP242）（2017年4月5日）
  - データ保護オフィサー（DPO）に関するガイドライン（WP243）（2017年4月5日）
  - 主たる監督機関に関するガイドライン（WP244）（2017年4月5日）
  - DPIA（データ保護影響評価）に関するガイドライン（WP248）（2017年10月4日）
  - 課徴金に関するガイドライン（WP253）（2017年10月3日）
  - データ侵害通知に関するガイドライン（WP250）（2018年2月6日）
  - 自動化された意思決定とプロファイリングに関するガイドライン（WP251）（2018年2月6日）
  - 十分性のリフェレンシャルに関する作業文書（WP12の第1章の更新）（WP254）（2018年2月6日）
  - BCRに関する作業文書（WP256）（2018年2月6日）
  - 処理者向けBCRに関する作業文書（WP257）（2018年2月6日）
- パブコメに（1月23日まで）付されていたガイドライン案（ファイナライズ中）
  - 同意に関するガイドライン案（WP259）
  - 透明性に関するガイドライン案（WP260）
- パブコメ中のガイドライン案（それぞれ3月26日、3月30日まで）
  - 第49条（第三国データ移転の例外措置）に関するガイドライン案（WP262）
  - 認証機関の認定に関するガイドライン案（WP261）

EUデータ保護指令からGDPRへの改定の背景

- GDPRへの改正は、EU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**。

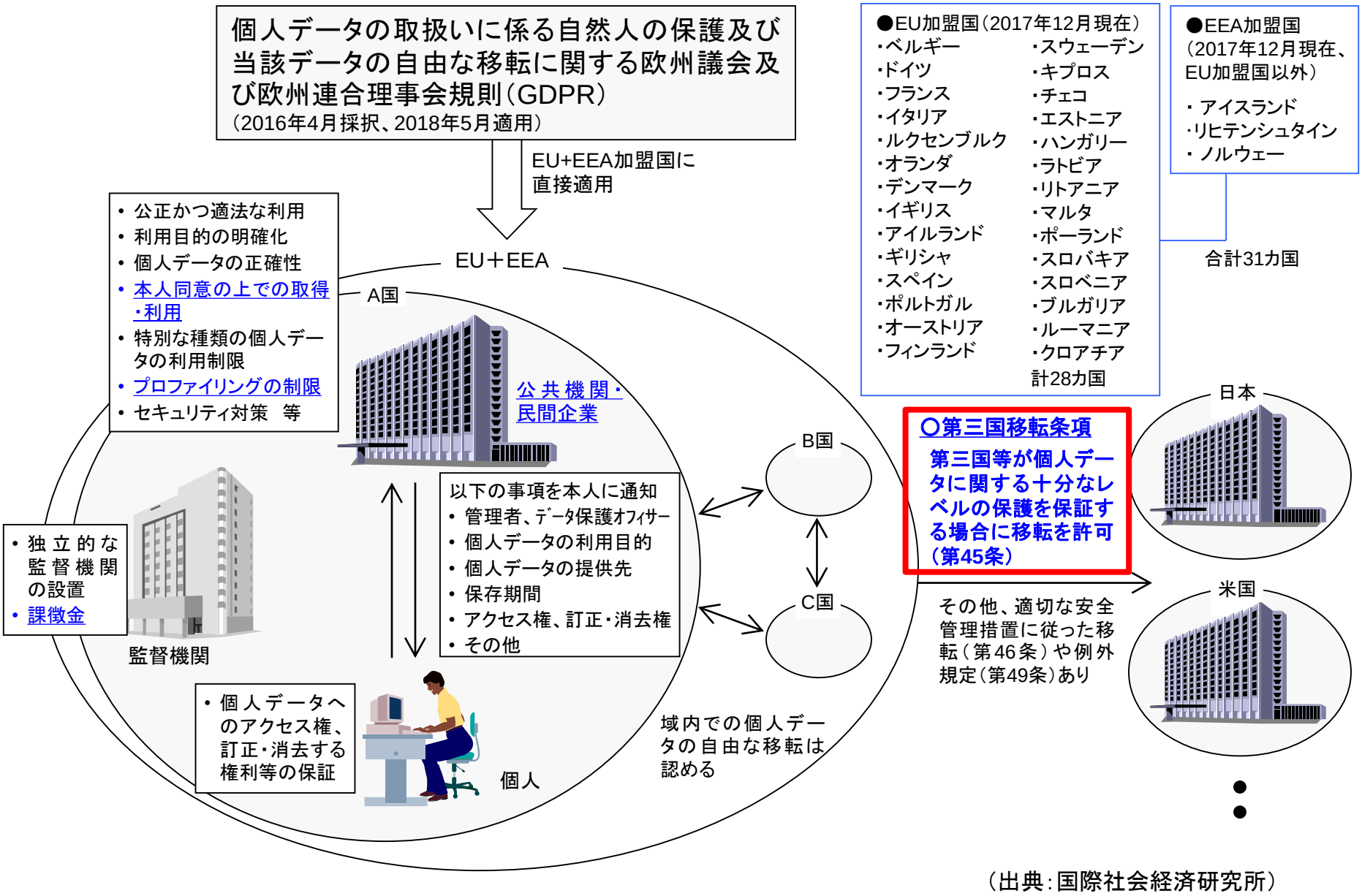
〇米国：
- 全世界から個人データを収集する米国の多国籍企業（「データの蛸」）。ex. Google, Facebook
- スノーデン事件で明るみに出たPRISMにより、米国IT企業からデータ収集できる米国政府。

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一般データ保護規則（GDPR）の概要図



（出典：国際社会経済研究所）

GDPRの概要（EU指令からの改正点）

0. 全般

– **「指令（Directive）」から「規則（Regulation）」に格上げ**
  - 規則への格上げにより、EU法を加盟国へ直接適用し、**EU域内でのデータ保護ルールを一元化**。
  - 従来のEU指令の下では、アイルランド・英国の国内法やその運用は緩く、ドイツ・フランスは厳しいというEU内の温度差があった。

※ EUの規制については、「規則」、「指令」、「決定」、「勧告」、「見解」の5 種類がある。左ほど強制力が強い。

※「指令」は、含まれている目的が国内法に置き換えられたときにのみ各国に効力を持つ。また、国内法への置き換えに際し、加盟国にはある一定の裁量権が与えられている。また指令は、定められた期間内に国内法に置き換えられなければならないということも決められている。

※「規則」は、欧州連合の加盟国の法令を統一するために制定され、加盟国に直接の効力を持ち、個々の国に効力をもたらすための国内法を必要としない。また、すべての国内法に優先する。
http://www.neca.or.jp/control/green/PDF/kank0610.pdf

– 加盟国がGDPRの内容よりも厳しい国内法や緩やかな国内法を制定することはできない。（GDPRで国内法制定が認められている場合を除く。）
  - GDPRの中で加盟国における具体的ルール制定が認められている分野：

    表現・情報の自由（第85条）、公式文書へのアクセス（第86条）、国民識別番号の処理（第87条）、雇用の場面での処理（第88条）、科学/歴史研究目的・統計目的（第89条）、公益のためのアーカイブ目的（第89条）、守秘義務（第90条）等。

GDPRの概要（EU指令からの改正点）

1．個人データ保護の権利の強化

①「自己情報コントロール権」の強化

- 曖昧でない（unambiguous）同意の取得（第7条、第4条(11)）（※当初案explicit →unambiguous）
- 透明・平易で容易にアクセス可能なプライバシーポリシーの提供（第12条）
- 消去する権利（「忘れられる権利」）（第17条）
- データポータビリティの権利（第20条）
- 子どもに対する特別な配慮（同意取得やプライバシーポリシー）（第8条、第12条）

② 個人が権利行使する手段の改善

- 監督機関（DPA）の独立性と権限の強化（第52条、第57条、第58条）
- 司法的救済措置の向上（第77条～第79条）
- 監督機関による課徴金（第83条）

③ データセキュリティの強化

- プライバシー強化技術の利用促進、認証制度／シール制度の促進（第32条、第42条、第43条）
- データ侵害時の監督機関及び本人への迅速な報告・連絡義務（第33条、第34条）

④ 管理者（controller）や処理者（processer）の説明責任の強化

- データ保護オフィサー（DPO）の設置義務（第37条）
- プライバシー・バイ・デザイン原則の導入（第25条）
- データ保護影響評価（DPIA）の実施義務（第35条）

※「管理者」：個人データ処理の目的、条件及び手段を決定する自然人、法人、公的機関、その他のあらゆる組織。
※「処理者」：管理者の代わりに個人データを処理する自然人、法人、公的機関、その他のあらゆる組織。
※「処理（processing）」：個人データに対して実行されるあらゆるオペレーション。収集、保存、変更、利用、開示、消去等の総称。

GDPRの概要（EU指令からの改正点）

2. EU域内での（デジタル単一市場実現のための）データ保護ルールの一元化
   - 単一のEU規則を各加盟国に直接的に適用すること（前述）
     - 加盟国毎のルールに合わせなくてよいので、企業にとって年間23億ユーロのコスト削減（EU試算）
   - データ処理に係る監督機関への通知義務の廃止
     - 企業にとって年間1億3千万ユーロのコスト削減（EU試算）
   - 「ワンストップショップ」としての監督機関（第56条、第60条）
     - 多国籍企業と監督機関とのやり取りは、主要拠点の国の監督機関に一本化
   - 監督機関同士の協力と、整合性メカニズムの導入（第61条、第63条）
   - EU指令の第29条作業部会を、独立的な「欧州データ保護評議会（EDPB）」に格上げ（第68条）

3. グローバル環境でのデータ保護ルールの詳細化
   - EU規則が第三国の管理者に適用される範囲の拡大（域外適用）（第3条第2項）
   - 欧州委員会による第三国の十分性決定（十分性認定）の基準の明確化（第45条）
   - 十分性決定のない第三国へのデータ移転に関するルールの簡素化・多様化（第46条、第47条、第49条）
     - BCR（拘束的企業準則）については、1つの監督機関の承認さえ貰えば、EUの他の監督機関は一括でその結果を追認することになった
   - 第三国の行政機関からのデータ開示要求への対応（第48条）

個別条項： 適用範囲（第2条）

- GDPRは、全部又は一部が自動的手段による個人データ処理に適用される。また、自動的手段以外のデータ処理のうち、ファイリングシステムの一部である処理（またはファイリングシステムの一部にすることが意図された処理）にも適用される。（第2条1項）
  - ファイリングシステムとは、特定の基準に従ってアクセスできる、あらゆる構造化された個人データの集合をいう。

- 以下のデータ処理はGDPRの適用除外となる。（第2条2項）
  - EU法の適用を受けない活動における個人データの取扱い。
  - EU条約第5編第2章（共通外交・安全保障政策）の適用を受ける活動を行う際の加盟国による個人データの取扱い。
  - 全面的に個人的な又は家庭内の活動における自然人による個人データの取扱い。
  - 公共の安全（public security）への脅威に対する保護及び防止を含む、犯罪の防止、捜査、探知、起訴、又は刑事罰を科すために所管官庁が行う個人データの取扱い。

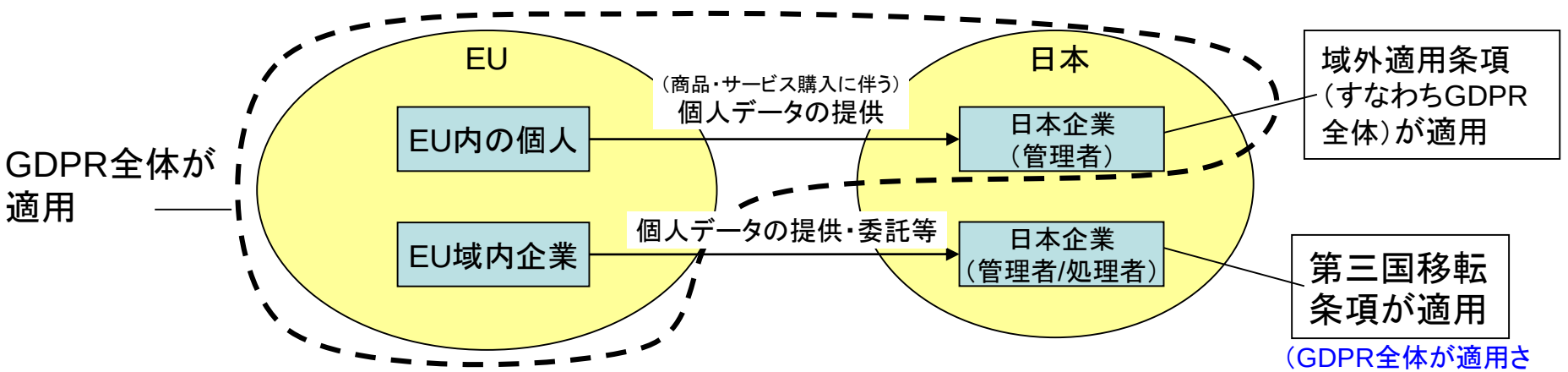
個別条項： 域外適用（第3条2項）

● 従来のEU指令の規定

- 管理者がEU域内に事業所を持つか、EU域内の設備でデータ処理を行う場合のみEU指令の対象となる。

● GDPRでの改定内容（追加規定）

- **EU域外企業であっても、以下の場合、EU域内にいる個人のデータを取扱う管理者に対してはGDPRが適用される**（第3条第2項）。
  - ① EU域内にいる個人に商品やサービスを提供している場合（無償の場合を含む）
  - ② EU域内での個人の行動をモニターしている場合
- 具体的には、オンラインサービス事業者、パーソナルクラウド事業者、オンライン広告事業者、スマートフォンアプリ事業者等が対象になりうる。
  - Ex. フランス在住のフランス人等に提供している「おもてなし」アプリ



個別条項： 個人データの定義(第4条(1))

- EU規則での「個人データ(personal data)」の定義は、やや簡略化して言うと、

> 「**識別された自然人**」、又は「管理者その他の者によって合理的に利用される可能性の高い手段によって、直接的若しくは間接的に**識別されうる自然人**」に関する**全ての情報**

- どこまでが「個人データ」か？ (フランスのデータ保護監督機関CNILの意見)
  - IPアドレスは、ISPに聞けば誰が利用したIPアドレスか分かるので個人データである。
  - 携帯電話の端末ID、パスポート番号、メールアドレス、遺伝子情報、指紋情報については、EUでは全て個人データである。ISO/IEC29100でも個人データと定義されている。
    - 註：ISO/IEC29100「Information technology - Security techniques - Privacy framework」。ISO/IEC29100ではPIIとして、社会保障番号、パスポート番号、口座番号、電話番号、正確な位置情報、生体認証データが例示されている。
  - カルフールのサービスカードの顧客IDなど、企業ごとの顧客IDも、当該企業のDBで氏名につながるデータの場合には、個人データである。

- **匿名化されたデータは個人データに該当しない**。

「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には、データ保護の諸原則は、適用されるべきでない。」(前文(26))

EUにおける匿名化

- EU指令第29条作業部会の「匿名化技術に関する意見書」
  - 「Opinion 05/2014 on Anonymisation Techniques」（WP216）（2014年4月10日採択）
  - データ保護の観点から既存の匿名化技術の有効性と限界について分析し、個々の匿名化技術に固有の、識別化（identification）に関する残存リスクを考慮することにより、これらの技術を取扱う際の勧告を提供するもの。
  - 「有効な匿名化の3基準」を提示。（十分条件）
    - (i) Singling out：個人を識別（single out）できないこと
      cf. ネット上での行動ターゲッティング広告はSingling outの例
    - (ii) Linkability：同一人物の記録と連結（link）できないこと　cf.「照合性」
    - (iii) Inference：ある個人に関する情報であると推定できないこと　cf.「特異な記述」
  - この3基準に基づき、各匿名化技術の堅固性（robustness）について評価。

有効な匿名化の3基準 / 匿名化技術	(i) 個人を識別（single out）することが可能か	(ii) 同一人物の記録と連結することが可能か	(iii) ある個人に関する情報であると推定することが可能か
仮名化	× 可能	× 可能	× 可能
ノイズ付加	× 可能	○ おそらく不可能	○ おそらく不可能
置換	× 可能	× 可能	○ おそらく不可能
アグリゲーションまたはk-匿名性	○ 不可能	× 可能	× 可能
l-多様性	○ 不可能	× 可能	○ おそらく不可能
差分プライバシー	○ おそらく不可能	○ おそらく不可能	○ おそらく不可能
ハッシュ化／トークナイゼーション	× 可能	× 可能	○ おそらく不可能

- フランスCNILの意見：「データの提供元がいわゆる「対応表」を持っている場合には、匿名化とは言えない。（世の中のどこかに対応表が存在する限り、そのデータは匿名化データではない。）」

個別条項： 仮名化（第4条（5））

- 「仮名化（pseudonymisation）」:

  「追加の情報が分離して保管され、識別された又は識別され得る自然人に個人データが帰属しないことを保証する技術的及び組織的措置をとることによって、当該追加の情報を利用せずに個人データがもはや特定のデータ主体に帰属しないような方法で、個人データを処理することをいう。」（第4条(5)）

- 大まかにいうと、仮名化は個人情報から個人を識別するデータ項目（氏名、住所、ID等）を削除し、代わりに仮名IDを付加する処理のこと。仮名IDと元データとの「対応表」は維持される。

- 仮名化された個人データは、（仮名化後も）個人データとみなされる。（前文26）
  - GDPR（および従来のEU指令）では、個人データの識別性を低減する加工した際、「追加の情報（対応表）」が加工元の企業等に存在する限りは（匿名化ではなく）仮名化とみなされる。
  - 日本の改正個人情報保護法の「匿名加工情報」に近い概念。ただし、匿名加工情報がもはや個人情報でないのに対し、EU法令では仮名化データも個人データとみなされる点が異なる。

- GDPRにおける仮名化の位置付け
  - 技術的な安全管理措置の一手段（第6条、第25条、第32条、第40条、第89条）。
  - 仮名化による義務緩和はない。（ドラフト段階では検討されていたが）

個別条項： 透明性（第12条）、同意（第7条）

- 透明で適切なプライバシーポリシーの提供（第12条）
  - 従来のEU指令にも本人への利用目的等の通知義務があるが、**企業のプライバシーポリシーが煩雑で分かりにくい**現状を踏まえ、管理者に対して新たに「透明性」の義務を追加。
    - 第29条作業部会は階層型のプライバシーポリシーを推奨。
    - プライバシーポリシー等での標準アイコンの使用も可能。

- 曖昧でない（unambiguous）同意の取得（第7条）
  - 前項に関連して、プライバシーポリシーが分かりにくいため**本人の同意が形式的なものに陥っている**現状を踏まえ、管理者に対して曖昧でない（unambiguous）同意を取得することの義務、また同意を撤回できる権利を保障する義務を追加。
    - いわゆる**「黙示の同意」は認められない**。（本人の積極的行為が必要。）
      - プライバシーポリシーへの同意を、サービスの契約約款への同意と一括で求めてはならない。
      - Web上の「同意ボックス」にデフォルトでチェックを入れてはならない。

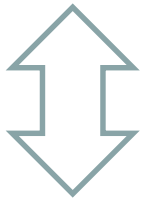
【ご参考】同意に関するGDPRの関連条文

GDPR第 4 条 定義

(11) データ主体の「同意」とは、強制を受けず、特定的に、情報提供を受けたうえでかつ曖昧でないデータ主体の意思表示であることを意味する。その意思は、当該データ主体が、宣言又は明らかな積極的行為によって、自己に係る個人データの取扱いに合意(agreement)して表すものとする。

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

出典：JIPDECのGDPR仮日本語訳



※EUデータ保護指令の定義と比較すると、GDPRでは「unambiguous」（曖昧でない）という語が追加された。

EUデータ保護指令　第2条 定義

(h) 「データ主体の同意」とは、データ主体が自己に関する個人データが取り扱われることへの同意を表明することによって、自由になされた特定のかつ十分に情報を提供された上での意思表示をいう。

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

出典：堀部政男研究室仮訳

【ご参考】同意に関するガイドライン案：有効な同意の諸要素

- EU指令第29条作業部会「同意に関するガイドライン案」（WP259）
- 第4条11項の定義では、データ主体の同意は以下を意味する。
  - 強制を受けない意思表示
  - 特定的な意思表示
  - 情報提供を受けた上での意思表示、かつ
  - 曖昧でない意思表示（その意思表示によってデータ主体は、宣言又は明らかな積極的行為によって、自己に係る個人データの取扱いに合意を表明するもの）

- 権力の不均衡（Imbalance of power）
  - GDPRの前文43では、管理者が政府機関である場合には管理者とデータ主体の関係に明確な権力の不均衡が存在することが多いため、政府機関が同意に基づいてデータ処理を行うべきでないことが示唆されている。
  - 権力の不均衡は、雇用の場面でも生じる。雇用主と従業員との依存関係に鑑みれば、従業員が同意の拒否による有害な影響の恐れもしくは実際のリスクを経験することなく、雇用主のデータ処理への同意を拒否することは難しい。例えば、職場でのカメラ監視等のモニタリングシステムの導入や、評価フォームの記入に対して、従業員が同意へのプレッシャーを感じることなく、「強制を受けずに」同意を行うことは難しい。そのため、第29条作業部会は、雇用主が同意に基づき従業員の個人データを処理することは問題があると考える。
    - ただし、従業員の同意をデータ処理の合法性の根拠としうるケースもある。例えば、職場での勤務風景をTVスタッフが撮影する場合、雇用主は従業員に対して彼らの姿を撮影してよいかどうか同意を求めることができる。

【ご参考】同意に関するガイドライン案：有効な同意の諸要素

- 同意の粒度
  - あるサービスが複数の目的のデータ処理を伴う場合は、全てのデータ処理について一括で同意を取るのではなく、データ主体がどの目的について同意するかを自由に選べるようにするべきである。
  - GDPRの前文43では、データ主体に個々のデータ処理への個別の同意を許さないような場合、当該同意は「強制を受けない」ものとはみなされないと明記されている。
    - また、前文32では「同意は、同一の目的で実施される全てのデータ処理をカバーするべきである。当該データ処理が複数の目的を有する場合には、同意は全ての目的に対してなされるべきである」と言われている。
    - 例えば、小売店が顧客に対して、マーケティング用の電子メールを送信する目的とともに、グループ内の他の企業に提供する目的で個人データ利用の同意を求めたとする。これらを1つの同意で求めた場合、2つの目的に対して個別の同意を取っていないので、当該同意は有効なものではない。
- 曖昧でない意思表示
  - 同意はデータ主体による「宣言」または「明らかな積極的行為」を必要とする。
    - EUデータ保護指令では「意思表示（その意思表示によってデータ主体は自己に係る個人データの取扱いに合意を表明するもの）」という定義だったが、GDPRではこの定義をベースに、有効な同意は「曖昧でない意思表示（その意思表示によってデータ主体は、宣言又は明らかな積極的行為によって、自己に係る個人データの取扱いに合意を表明するもの）」を必要とすることが明確された。
  - 「宣言」
    - 書面での宣言、（記録された）口頭での宣言、電子的手段による宣言。
  - 「明らかな積極的行為」
    - Webサイト上で同意ボックスをチェックすることなど。
      - 同意ボックスが予めチェックされているのは無効。オプトアウトボックスをチェックさせることも無効。
    - サービスの一般的な契約約款への包括的同意では不十分（「明らかな積極的行為」とはみなさない）。
    - 電子的手段による同意（明らかな積極的行為）
      - 例：タッチスクリーンのスワイプ、スマホカメラの前で手を振ること、スマホを8の字に動かすことなど。
      - 例：同意の文言を含む契約約款をスクロールダウンすることは、「明らかな積極的行為」とはみなされない。同意に関する文言が見過ごされている可能性があるため。

【ご参考】同意に関するガイドライン案：明示的な同意の取得

- GDPRでは、「明示的な同意」は、以下のような重大なデータ保護リスクが生じうる状況で（処理の合法性の根拠の1つとして）必要とされている。
  - 特別な種類のデータの処理（第9条）
  - プロファイリングを含む自動化された意思決定（第22条）
  - 適切な安全管理措置がない場合の第三国データ移転（第49条）

- 「通常」の同意との違い
  - GDPRでは「明らかな積極的行為」が通常の同意の前提条件とされている。このようにGDPRでは、EUデータ保護指令に比べ、通常の同意において既に高い基準が設定されているため、「明示的な」同意において更に何が必要とされるのかを明確化する必要がある。
  - 同意が明示的であることの確証を得る1つの方法は、同意を書面で得ること。さらに、当該書面にデータ主体の署名を求めることもありうる。
  - ただ、全ての場面で、書面での同意や署名された同意が求められる訳ではない。オンライン環境では、以下による明示的な同意の取得も可能。
    - 電子的フォームへの入力
    - 電子メールの送信
    - 署名付き文書のスキャンのアップロード
    - 電子署名の利用　等
    - 2段階の同意確認も、1つの方法。例えば、オンラインでの同意の意思表明後に電子メールが送られ、メール内のリンクをクリックすると、同意がコンファームされる。

【ご参考】同意に関するガイドライン案：同意の撤回

- 同意の撤回方法
  - 同意が電子的手段（マウスのワンクリック、タッチスクリーンのスワイプ、キーボード入力等）で取得された場合は、それと同程度に容易な方法で、同意を撤回できなければならない。
  - 同意が特定のユーザインターフェース（Webサイト、アプリ、ログインアカウント、IoTデバイス、電子メール等）で取得された場合には、同じインターフェースで同意を撤回できなければならない。
  - データ主体は不利益を被ることなく、同意を撤回できるべきである。すなわち、同意の撤回は無料で、またサービスレベルを下げることなく可能でなければならない。
  - 管理者は同意に先立ち、同意を撤回する権利についてデータ主体に情報提供しなければならない。
- 同意が撤回された場合
  - 同意が撤回された場合、管理者は同意に基づくデータ処理を停止しなければならない。当該データの処理（保存など）を正当化する他の合法的な根拠がない限り、管理者は当該データを消去または匿名化しなければならない。

第7条 同意の条件

3. データ主体は、いつでも同意を撤回する権利があるものとする。また、同意の撤回は撤回前の同意に基づく取扱いの合法性に影響を与えない。データ主体は、同意を与える以前にその旨が通知されていなければならない。同意の撤回は、その付与と同程度に容易なものでなければならない。

第17 条 消去の権利（忘れられる権利）

1. データ主体は当該データ主体に関する個人データについて管理者に不当に遅滞することなく消去させる権利を持つものとする。管理者は、次に掲げる根拠のいずれかが適用される場合、個人データを不当に遅滞することなく消去する義務を負うものとする。

(a) 個人データが収集された又はその他取扱いの目的に関して、当該個人データがもはや必要ない場合。

(b) データ主体が、第6 条第1 項(a)号又は第9 条第2 項(a)号による同意に基づく取扱いの同意を撤回し、かつ取扱いに関して他の法的根拠がない場合。

（以下省略）

出典：JIPDECのGDPR仮日本語訳

個別条項： 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）」）

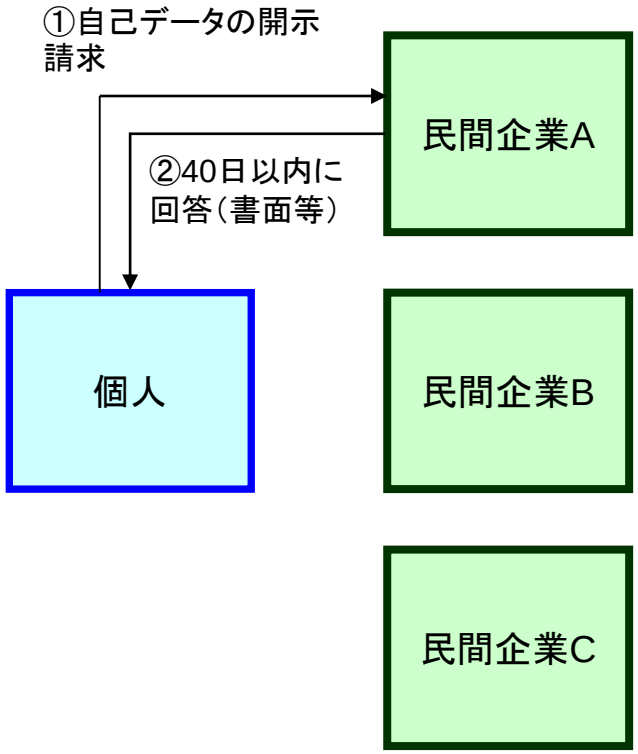
- EU指令の第12条にも自分の個人データを消去する権利が規定されているが、これを精緻化。
- EU指令では、データが不正確だったり不法に収集された等の理由がないと消去できないが、新規則では**本人が同意を撤回した場合にも、管理者に消去してもらう権利を保障**。
- また、管理者が個人データを公開している場合、管理者は、**当該個人データを処理している他の管理者に対して、データ主体が当該個人データへのリンクやコピーの消去を求めていることを通知するための合理的な措置（技術的な措置を含む）を取らないといけない**（利用可能な技術や実施にかかるコストは考慮した上で）。

○ 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（管理者）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する権利。また、そのデータを他のサービスに移転する権利。
  - ex. 個人がSNSサービスを他のサービスに切り替える場合
- 管理者側で作成した推測データ・派生データ（評価結果など）は対象にならない。

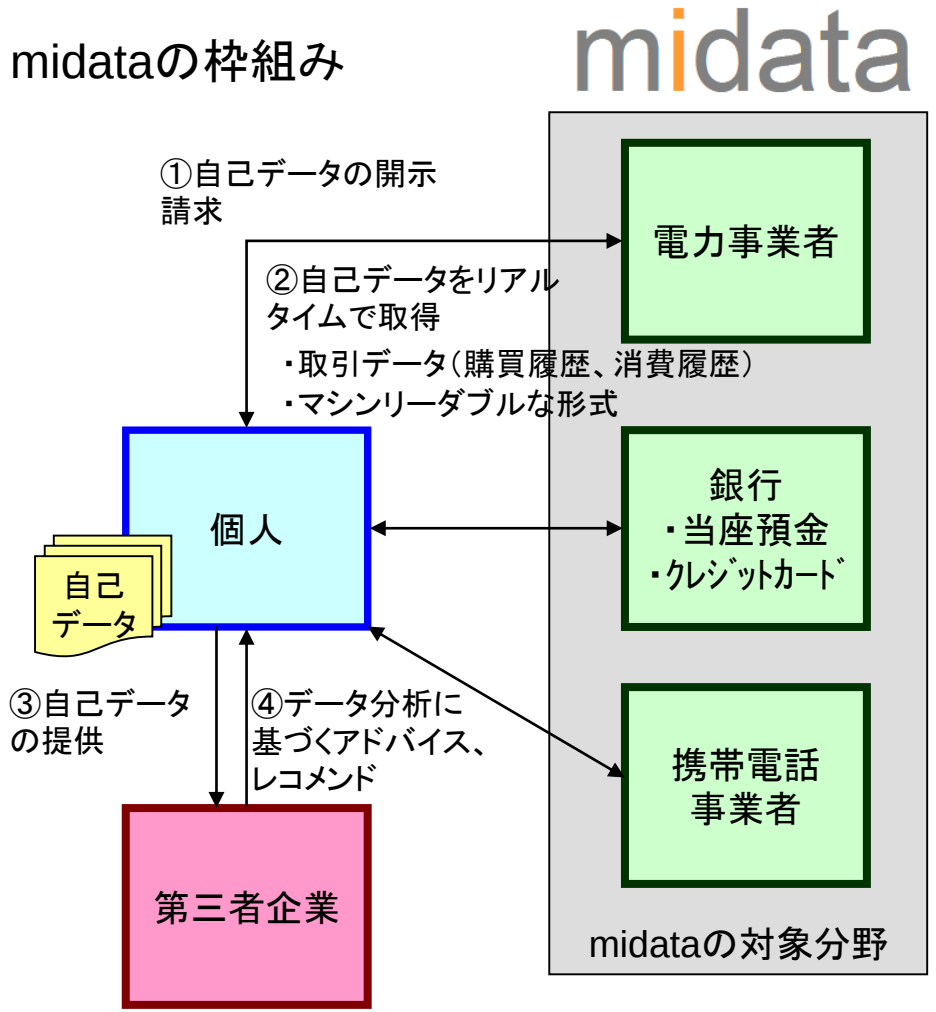
データ・ポータビリティの権利の事例： 英国midata

○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

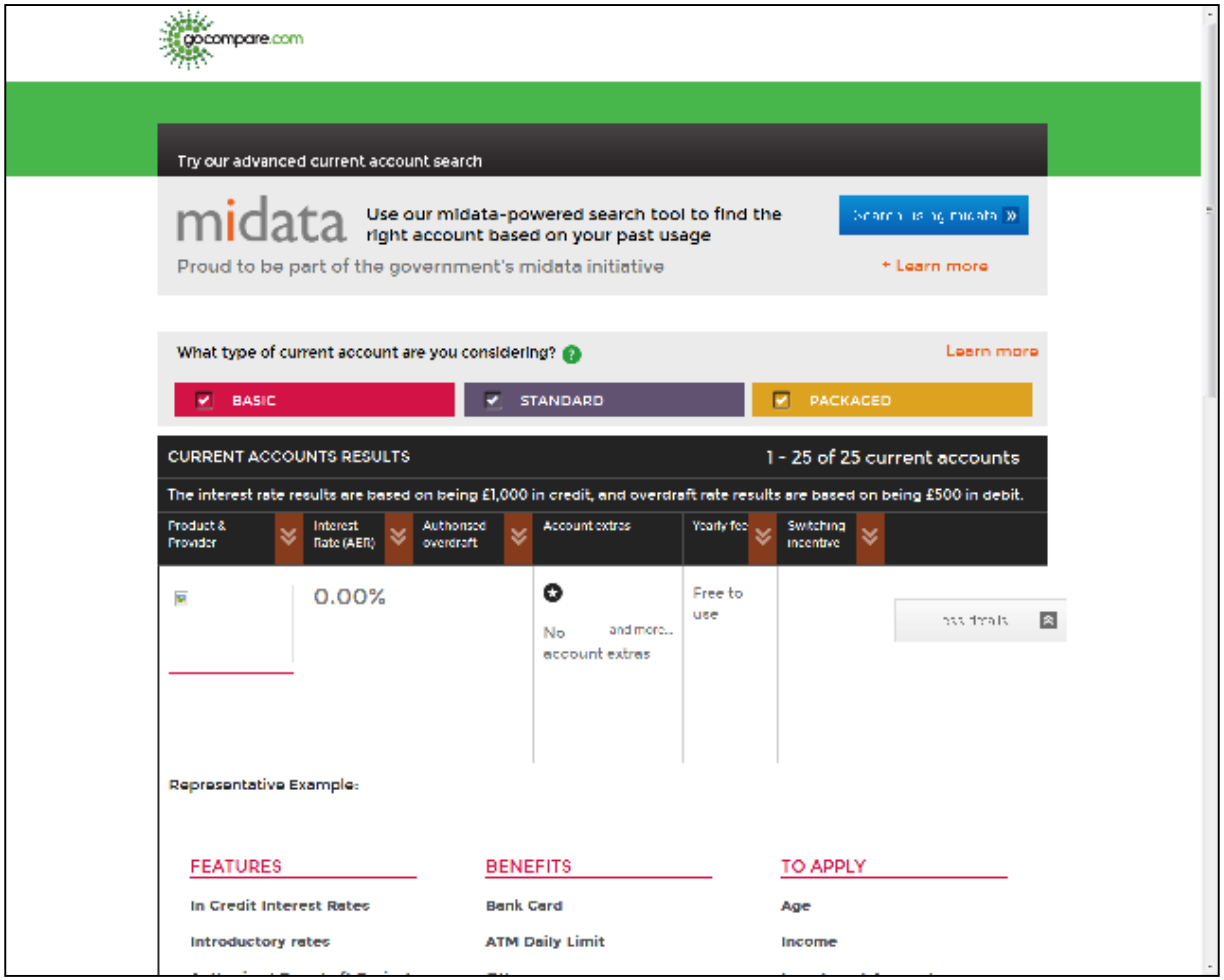


- 個人が開示請求をした際、**自己データをリアルタイムで取得することが可能に**なる
- 第三者企業も利用できるような、**一定のマシンリーダブルな形式の電子データ**を取得可能

出典：国際社会経済研究所

英国midata： 比較サイトGocompare.com

- 2015年3月にサービス開始
- 銀行から自分の取引データ（midata）をダウンロードし、本サイトに送信することにより、各種金融商品を比較し、最適な商品のレコメンドを受けることが可能



個別条項： プロファイリング（第22条等）

- GDPRではプロファイリング（※）を以下の3つの場面で規制
  - ※プロファイリングとは：「個人を一定のカテゴリーに分類したり、個人の遂行能力・興味・行動等について分析や予測をするために、個人に関する情報を集めて、その特徴や行動のパターンを評価すること」（第29条作業部会ガイドライン（WP251））

プロファイリングの種類	説明（GDPRでの位置付け）	例（第29条作業部会ガイドライン（WP251）記載のもの）
①プロファイリング一般	第4条4項で定義。個人データ処理の1つとして（他の個人データ処理と同様に）様々な義務。	・データブローカーが様々な情報源から個人データを取得し、整理して、個人に関するプロファイルを作成し、セグメント分け（し、顧客企業に販売）する場合
②プロファイリングなどの自動化意思決定（第22条）	プロファイリングなど完全に自動化された意思決定であって、本人に法的効果または同様の重大な影響をもたらすもの。第22条で原則として禁止。	・個人の運転習慣が長期に渡ってモニターされ、「常習的なスピード違反か」「直近に他の交通違反を起こしていないか」等に基づいて（自動的に）罰金額が決められる場合 ・ローンの審査がアルゴリズムを用いて行われ、担当者による評価を経ずに、審査結果が自動的に個人に通知される場合 ・オンラインでのクレジットカード申請の自動的な拒否 ・人間が介在しない電子リクルーティング
③ダイレクトマーケティング目的でのデータ処理（プロファイリングなど）（第21条）	ダイレクトマーケティンク目的での個人データ処理（プロファイリングなど）に対して、本人はいつでも異議を唱える権利を持つ（第21条2項）。 （公共の利益や正当な利益の目的での個人データ処理（プロファイリングなど）に対して異議を唱える権利もある（第21条1項）。）	・利用者の近くのレストランをレコメンドする携帯アプリが、取得したデータから利用者の食事の好みや生活習慣などをプロファイリングし、携帯電話に広告を送る場合。

【ご参考】GDPRの条文（第22条）

第22条 プロファイリングを含む自動化された個人意思決定

- 1. データ主体は、当該データ主体に関する法的効果をもたらすか又は当該データ主体に同様の重大な影響をもたらす、プロファイリングなどの自動化された処理のみに基づいた決定に服しない権利を持つ。
- 2. 第1項は次に掲げるいずれかの決定には適用されない。
  (a) データ主体とデータ管理者間の契約締結、又は履行に必要な決定。
  (b) データ主体の権利及び自由並びに正当な利益を保護するための適切な対策が定められた管理者が従うEU 法又は加盟国の国内法によって認められた決定。
  (c) データ主体の明示的な同意に基づく決定。
- 3. 第2項(a)号及び(c)号で定める状況に関して、データ管理者は、データ主体の権利及び自由並びに正当な利益を保護するための適切な対策を実施し、少なくとも管理者側で人を介在させる権利、当該データ主体の観点を表明する権利、及び決定に同意する権利を実施するものとする。
- 4. 第2項で定める決定は、第9条第2項(a)号又は(g)号が適用されず、データ主体の権利及び自由並びに正当な利益を保護するための適切な対策が機能していないならば、第9条第1項で定める特別な種類の個人データに基づいてはならない。

出典：JIPDECのGDPR仮日本語訳（訳語を一部変更、下線を記入）

【ご参考】自動化意思決定とプロファイリングに関するガイドライン：定義

- EU指令第29条作業部会「自動化された意思決定とプロファイリングに関するガイドライン」（WP251）

A. プロファイリング（Profiling）

第4条(4)：

「プロファイリング」とは、自然人に関するある一定の個人的な側面を評価するために、特に、自然人の業務実績、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の分析又は予測をするためになされる、個人データの利用から成る個人データのあらゆる形態の自動的な処理をいう。

- 上記定義により、プロファイリングは以下の3つの要素から成る。
  - 自動的な形態の処理（を伴ったもの）。（人間の関与を必ずしも排除しない。）
  - 個人データに対して実施される処理。
  - 自然人に関する個人的な側面を評価する処理。

※ 欧州評議会の2010年の勧告では、プロファイリングを以下の3段階に分けて記述している。
  - ①データ収集。
  - ②相関関係を特定するための自動的な分析。
  - ③相関関係を個人に適用し、現在または将来の行動の特徴を特定すること。

- プロファイリングは、「個人を一定のカテゴリーに分類したり、個人の遂行能力・興味・行動等について分析や予測をするために、個人に関する情報を集めて、その特徴や行動のパターンを評価すること」を意味すると概括されている。

【ご参考】自動化意思決定とプロファイリングに関するガイドライン：定義

B. 自動化された意思決定（Automated decision-making）

- 「自動化された意思決定」は「プロファイリング」と一部重なる場合もあるが、異なる概念である。
  - 例： スピードカメラのみに基づいて科される罰金は自動化された意思決定であるが、プロファイリングは伴わない。
  - 例： 個人の運転習慣が長期に渡ってモニターされ、「常習的なスピード違反か」「直近に他の交通違反を起こしていないか」といった要素に基づいて罰金額が決められる場合、プロファイリングに基づく意思決定となる。
- 自動化された意思決定は以下のデータに基づいてなされる。
  - 関係する個人から直接的に提供されるデータ（質問フォームへの回答など）
  - 個人を観察することで得られるデータ（アプリを通じて収集される位置データなど）
  - 既存のプロファイル情報から推測されたデータ（信用スコアなど）

C. GDPRにおける「プロファイリング」の扱い

- 「プロファイリング」という概念は、以下の3つの使われ方がなされうる。
  - (i)プロファイリング一般
  - (ii)プロファイリングに基づく意思決定（人間が関与するもの）
  - (iii)プロファイリングなどの、自動化された意思決定（第22条）
- (iii)には、GDPR第22条が適用される。（同ガイドラインの中心テーマ）
- (i)(ii)には、GPDR全般（一般原則）が適用される。

【ご参考】自動化意思決定とプロファイリングに関するガイドライン：第22条関連

○ 第22条は以下を意味する。

- ①「データ主体に法的効果または同様の重大な影響をもたらす、プロファイリングなどの完全に自動化された意思決定」を原則的に禁止する。（第22条1項）
- ② この原則にはいくつかの例外がある。（第22条2項）
- ③ 例外の適用に当たっては、データ主体の権利及び自由並びに正当な利益を保護するための適切な対策を実施するものとする。（第22条3項）

○ 第22条2項で挙げられた3つの例外

(a) データ主体とデータ管理者間の契約締結、又は履行に必要な決定。

- 管理者は、それが目的を達成する最も適切な方法だという理由から、自動化された意思決定を使用したいと思うかもしれない。人間が定常的に関与することは、処理されるデータ量の観点から非現実的であるか不可能であるかもしれない。
- このような自動化された意思決定が必要と示すためには、よりプライバシー侵害的でない手段を採用しうるかどうかを考慮しなければならない。もし他の手段によって同じ目的に到達できるのであれば、このような自動化意思決定は契約履行等に「必要」とはみなされない。

(b) データ主体の権利及び自由並びに正当な利益を保護するための適切な対策が定められた管理者が従うEU 法又は加盟国の国内法によって認められた決定。

- 前文71で挙げられている例は、以下のために自動化された意思決定を使用することがEU法または加盟国法で定められている場合。
  - 詐欺の監視や防止
  - 脱税の監視や防止
  - サービスのセキュリティの保証

(c) データ主体の明示的な同意に基づく決定。

【ご参考】自動化意思決定とプロファイリングに関するガイドライン：第22条関連

○ 第22条1項の「自動化された処理のみに基づいた」の意味：

– これは、意思決定プロセスに人間の関与がないことを意味する。

○ 第22条1項の「法的効果」または「同様の重大な影響」の意味：

「法的効果」

– 自動化された意思決定がデータ主体に「法的効果」をもたらす例として、以下。
  - 契約を解除されること。
  - 法令で定められた社会保障給付金（児童手当や住宅手当等）の受給資格を得たり、拒否されること。
  - 入国を拒否されたり、市民権を拒否されること。

「同様の重大な影響」

– 前文71で挙げられている例は、「オンラインでのクレジットカード申込みの自動的な拒否」および「人間が介在しない電子リクルーティング」。

– この条件を満たすには、当該処理の効果が些細なものであってはならず、注目に値するほど十分に大きいか重要なものでなければならない。換言すれば、当該意思決定は以下の可能性がなければならない。
  - 個人の環境や行動、選択に重要な影響を与えること。
  - データ主体に長期的または永続的な影響を与えること。
  - 極端な場合、個人の排斥や差別につながること。

– 十分に「重大」な影響であるか否かの閾値を正確に示すことは難しいが、以下の決定はこのカテゴリーに入りうる。
  - 信用度など、当人の金融的環境に影響を与える決定
  - 当人の医療サービスへのアクセスに影響を与える決定
  - 当人の雇用機会を否定する決定、または当人を重大な不利な状況に追いやる決定
  - 大学入学など、当人の教育へのアクセスに影響を与える決定

【ご参考】自動化意思決定とプロファイリングに関するガイドライン：第22条関連

○ データ主体の権利： 情報提供を受ける権利（第13条、第14条）

- 管理者が第22条1項にいう自動化された意思決定を行う場合は、
  - データ主体にその旨を告知しなければならない。
  - 関連するロジック（logic involved）について意味ある情報を提供しなければならない。
  - 当該処理の意義（significance）および予測される結果について説明しなければならない。
- また、当該処理が第22条1項の狭い定義に当てはまらない場合でも、上記の情報を提供することはグッドプラクティスである。
- 特にプロファイリングに基づく意思決定である場合には（第22条1項の定義に当てはまるか否かに関わらず）、当該処理が「プロファイリングを目的としていること」および「生成したプロファイルに基づいて意思決定を行うことを目的としていること」をデータ主体に明確に示さなければならない。

- 「関連するロジックについての意味ある情報」：
  - 機械学習の発展により、自動化された意思決定プロセスやプロファイリングがどのように行われているかを理解することは難しくなっている。
  - 管理者は、意思決定の背後にある理由付けや依拠するクライテリアについてデータ主体に伝えるシンプルな方法を見出すべきである。また、データ主体に提供される情報は意味あるものであるべきである。

- 「当該処理の意義および予測される結果」：
  - 例： ある保険会社は、顧客の運転行動のモニタリングに基づいて、自動車保険の保険料を自動決定している。この自動化された意思決定の「意義」と「予測される結果」として、保険会社は「危険な運転は高い保険料支払いにつながる可能性がある」と説明し、架空ドライバーの保険料を比較するアプリ（急加速したり、ブレーキが遅いドライバーなど）を提供。また、図面を使って、どのように運転習慣を改善すれば保険料が下がるかを説明。

【ご参考】自動化意思決定とプロファイリングに関するガイドライン：その他

○ 子どもと自動化された意思決定

- 前文71で、データ主体に法的効果または同様の重大な影響をもたらすプロファイリングなどの完全に自動化された意思決定は、子どもに適用しないものとするとされている。条文本文（第22条）には子どもに関する言及はないものの、第29条作業部会は子どもに対するこのような自動化意思決定を正当化するために第22条2項の例外を適用しないことを推奨する。

○ データ保護影響評価（DPIA）との関連

- 第35条3項(a)では、プロファイリングなどの自動化意思決定に対するDPIAの実施義務が規定されている。

○ 特別な種類の個人データ（第9条）との関連

- プロファイリングによって派生したデータや推測データに「特別な種類の個人データ」（要配慮個人情報に相当）が含まれる場合がありうる。この場合、「特別な種類の個人データ」として処理しなければならない。
  - 例：食品購買履歴から当人の健康状態を推測する場合。
  - 例：ある調査研究では、Facebookの「いいね！」の履歴と他の情報を組合せることで、男性利用者の性的指向の88%、利用者の民族的素性の95%、利用者がキリスト教徒かイスラム教徒化の82%を正確に予測することができた。

個別条項： データ侵害時の報告（第33条、第34条）

○ 第33条　個人データ侵害の監督機関への通知

- 個人データ侵害（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**個人データ侵害に気づいてから72時間以内に**、監督機関に当該個人データ侵害について通知しなければならない。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なければならない。
  - 処理者は、個人データ侵害に気付いた後、不当な遅滞なしに管理者に通知しなければならない。
- 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。
  - 暗号化した個人データが漏洩した場合、それが最新の技術で暗号化されており、バックアップが存在するならば、監督機関への通知（およびデータ主体への連絡）は必要ない。
  - データ侵害が複数のEU加盟国の個人の個人データに影響する場合は、管理者は主たる監督機関（EU域内の主たる事業所がある国の監督機関）に通知すればよい。

○ 第34条　個人データ侵害のデータ主体への連絡

- 個人データ侵害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侵害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）が個人データ侵害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。

個別条項： データ保護影響評価（第35条）

○ 第35条　データ保護影響評価（DPIA）

- 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（プロファイリングなどの自動化意思決定、特別な種類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29条作業部会のDPIAガイドラインでは、以下の9つのクライテリアを用意し、そのうち2つのクライテリアに適合する個人データ処理についてはDPIAが必要としている。
  - 1. 評価（Evaluation）またはスコアリング
  - 2. 法的または同様に重大な影響を与える自動意思決定
  - 3. 体系的監視
  - 4. センシティブデータや高度に個人的な性質のデータ
  - 5. 大規模に処理されるデータ
  - 6. データセット間の照合や結合
  - 7. 脆弱なデータ主体に関するデータ
  - 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
  - 9. 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

【ご参考】DPIAに関するガイドライン：DPIAを行うべきデータ処理のクライテリア

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。 • 金融機関が顧客を信用照会データベースやマネーロンダリング・テロリスト対策データベース、詐欺犯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、「同様に自然人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。

【ご参考】DPIAに関するガイドライン：DPIAを行うべきデータ処理のクライテリア

クライテリア	説明
4.センシティブデータや高度に個人的な性質のデータ	• 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） • 第10条で規定された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.データセット間の照合や結合	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。

【ご参考】DPIAに関するガイドライン：DPIAを行うべきデータ処理のクライテリア

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.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	• 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）

EU指令第29条作業部会「DPIA（データ保護影響評価）に関するガイドライン」（WP248）

【ご参考】DPIAに関するガイドライン：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や高度に個人的な性質のデータ 5. 大規模に処理されるデータ 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を利用。	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	
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データを収集する場合。	1. 評価またはスコアリング 4. センシティブデータや高度に個人的な性質のデータ 5. 大規模に処理されるデータ 6. データセット間の照合や結合	
ある機関が国家レベルの個人信用格付データベースまたは詐欺データベースを作成する場合。	1. 評価またはスコアリング 2. 法的または同様に重大な影響を与える自動意思決定 4. センシティブデータや高度に個人的な性質のデータ 9. 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	
研究プロジェクトや臨床試験において脆弱なデータ主体に関する仮名化されたセンシティブデータのアーカイブを作成する場合。	4. センシティブデータや高度に個人的な性質のデータ 7. 脆弱なデータ主体に関するデータ 9. 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	
「医師その他の医療専門家や弁護士による患者や顧客から取得された個人データ」の処理（前文91）。	4. センシティブデータや高度に個人的な性質のデータ 7. 脆弱なデータ主体に関するデータ	必要でない
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。	5. 大規模に処理されるデータ	
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	

個別条項： データ保護オフィサー（第37条）

- 管理者および処理者は、以下の場合に、データ保護オフィサー（DPO、データ保護責任者）の指名が必要。

  (a) 個人データ処理が公的機関・団体によって行われる場合。ただし、司法能力をもとにした裁判所の行為を除く。

  (b) 管理者や処理者の中心的業務が、その性質、適用範囲や目的によって、大規模にデータ主体の定期的かつ系統的な監視を必要とする個人データ処理である場合。

  - 大規模な処理の例：

    病院による患者データの処理、公共交通機関における旅客の移動データ、ファストフードチェーンの顧客の位置データ、金融機関の顧客データ、検索エンジンによるターゲット広告のためのデータ処理、電気通信事業者によるデータ処理。

  - 定期的かつ系統的な監視の例：

    電気通信ネットワークの運用、電気通信サービスの提供、電子メールのretargeting、データ駆動型マーケティング活動、信用評価等のためのプロファイリング・スコアリング、モバイルアプリ等による位置追跡、顧客ロイヤルティプログラム、行動ターゲット広告、ウェアラブル端末による健康データの監視、CCTV、スマートメーター・スマートカー・HA等のIoT機器。

  (c) 管理者や処理者の中心的業務が、特別な種類のデータや有罪判決及び犯罪に関する個人データを大規模に取扱う場合。

- 企業グループについては、DPOが各事業所から容易アクセスできるならば、グループで1人のDPOの指名でもよい。
- 上記の場合以外でも、EU法又は加盟国の国内法で要求されているならば、DPOを任命しなければならない。

個別条項： 課徴金（第83条）

○ 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。
- 軽微な違反の場合には、課徴金の代わりに懲戒発令を行うことも可能。（前文148）
- 課徴金を科すか否かの決定、また課徴金の額は、以下の項目を考慮して判断される。（第83条2項）
  - 違反の性質、重大さ及び期間。（当該データ処理の性質又は目的並びに影響を受けたデータ主体の数及びデータ主体の受けた損害の程度を考慮する。）
  - 違反が故意か、過失か。
  - データ主体の受ける損害を軽減させるために管理者又は処理者がとった行動。
  - 管理者及び処理者の責任の程度。（第25 条及び第32 条による管理者又は取扱者によって実施された技術的及び組織的対策を考慮する。）
  - 管理者又は処理者によるあらゆる関連する以前の違反。
  - 違反の是正及び違反により起こり得る悪影響軽減のため、監督機関との協力の程度。
  - 違反によって影響を受ける個人データの種類。
  - 監督機関への違反通知措置。特に管理者又は処理者が違反を通知したか否か、もし通知したのならその程度。
  - 同じ対象事項に関して、関連する管理者又は処理者に対して事前に命令された第58 条第2 項で定める措置（勧告や命令）における、それら対策への遵守。
  - 第40 条による承認された行動規範又は第42 条による承認された認証メカニズムの固守。
  - 事案の状況に適用される悪化又は軽減要素。例えば直接又は間接に、違反から得られた財政上の利益又は避けられた損失。

EUから第三国への個人データ移転方法（GDPR）

- 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や地域等
  - 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。（2018年2月に、WP12を更新するWP254が発行された。）

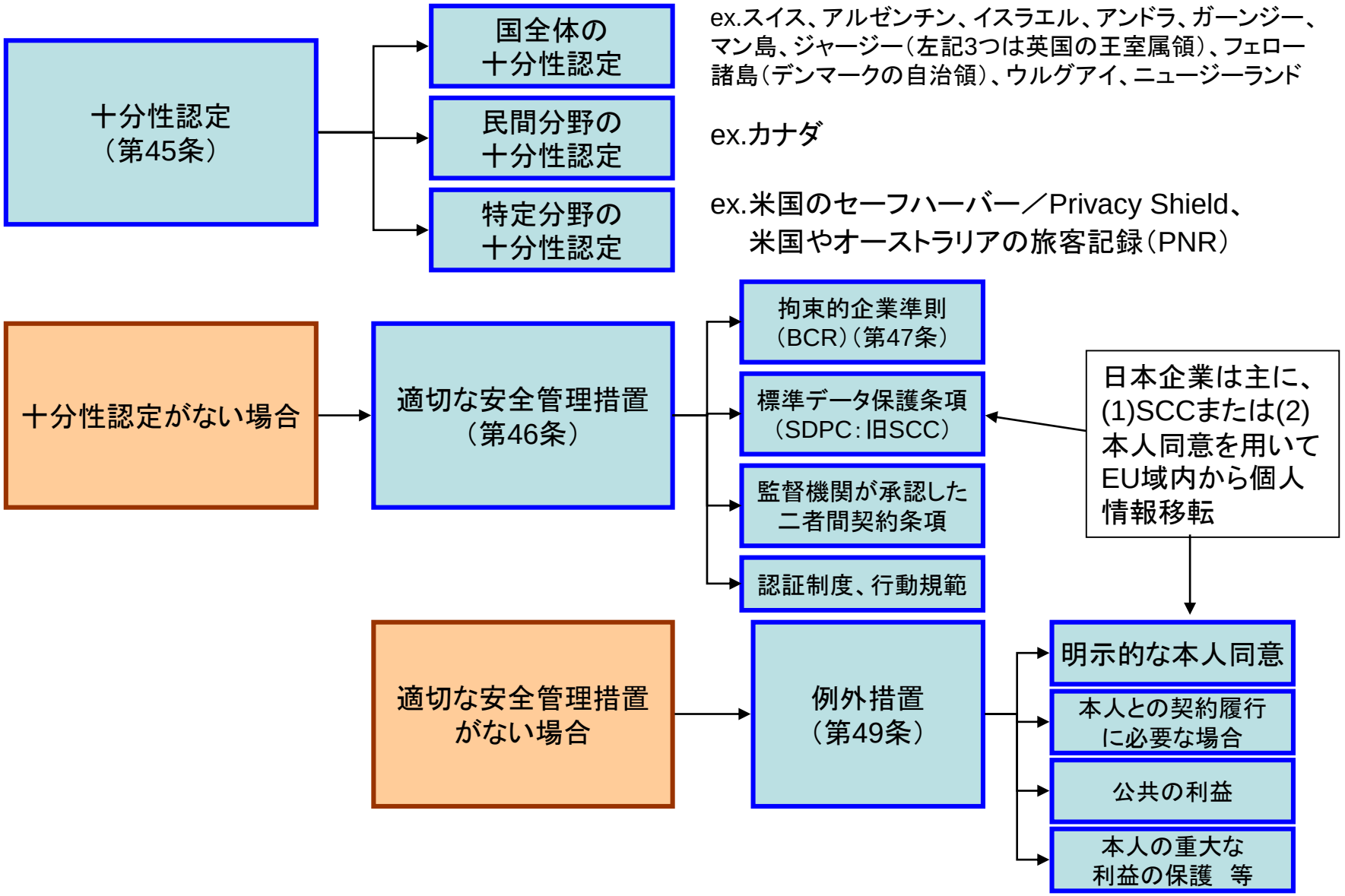
② 米国については特例として、**セーフハーバー・スキーム**
  - セーフハーバー7原則を遵守すると自己宣言する米国企業については、欧州域内からの個人データ移転を認めるもの（セーフハーバー決定）。
    - 形式上は「十分性認定」の1つとされている。
  - 2015年に欧州司法裁判所により無効判決を受け、2016年より後継のPrivacy Shieldが開始。

③ 十分性認定がない場合は、以下の「適切な安全管理措置」が必要
  - **標準データ保護条項（Standard Data Protection Clauses：SDPC：旧SCC）**（第46条第2項c）：
    欧州委員会が策定。EU指令時代のSCCは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47条）：
    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。
  - さらにGDPRでは、「認証制度」、「行動規範」による移転手段が追加された。

④十分性認定も、適切な安全管理措置もない場合には、以下の例外措置がある
  - **本人が明示的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49条）

→日本企業は主に、(1)SCCまたは(2)本人同意を用いてEU域内から個人情報移転

EUから第三国への個人データ移転方法（GDPR）



【ご参考】第49条に関するガイドライン：第49条の位置付け

- EU指令第29条作業部会「第49条（第三国データ移転の例外措置）に関するガイドライン案」（WP262）
- 第29条作業部会は長年、第三国データ移転に関して階層型アプローチを支持
  - 第三国が十分なレベルの保護を提供しているか（十分性認定：第45条）
  - 十分性認定がない場合、管理者は適切な安全管理措置を検討すべき（適切な安全管理措置：第46条）
  - 管理者はデータ移転にあたり、これら第45条と第46条の可能性をまず追求すべきであり、それらがない場合のみ、第49条の例外措置を使用すべき。
- 第49条の位置付け
  - 第45条（十分性認定）または第46条（適切な安全管理措置）に則ってデータ移転を行うのが一般原則であり、第49条（例外措置）を用いるのは原則の免除（exemption）である。
  - 欧州法に固有な原則に従い、例外がルールとなることのないように、第49条の例外措置は厳格に解釈されなければならない。
  - 第49条で移転した場合、移転された個人情報には十分な保護や適切な安全管理措置が保証されず、DPAによる事前許可も必要ないため、データ主体の権利・自由へのリスクを高める恐れがある。
- 特定の種類の個人データの移転制限（第49条5項）
  - また、十分性認定が存在しない場合、EU 法や加盟国の国内法は、公共の利益に関する重大な理由により、特定の種類の個人データに関して第三国や国際機関への移転を明確に制限することができる。

【ご参考】第49条に関するガイドライン：明示的な本人同意による移転

- 第49条1項で挙げられた7つ（(a)～(g)）の例外措置のうち、(a)では以下を規定。

  「十分性の決定及び適切な安全対策がないことによってデータ主体に関する当該移転から生じ得るリスクについての情報が提供された後、データ主体がその提案された移転に明示的に同意した場合」

- 以下3つの要素が重要。

  ①明示的な同意：

  – 「同意」および「明示的な同意」の詳しい要件については「同意に関するガイドライン」（WP259）を参照のこと。

  ②同意は個々のデータ移転に対する特定の同意でなければならない

  ③当該移転から生じ得るリスクについての情報を提供しなければならない：

  – 通常のケースで必要とされる要件（管理者の身元、処理の目的等）に加え、以下の情報をデータ主体に提供しなければならない。
    - データの受領者、または受領者の種類
    - データが移転される第三国
    - 同意が当該移転の合法的根拠であること
    - データが移転される第三国は欧州委員会から十分性認定を受けていないこと
    - 十分性認定や適切な安全管理措置がないため、データ主体にはリスクが生じ得ること

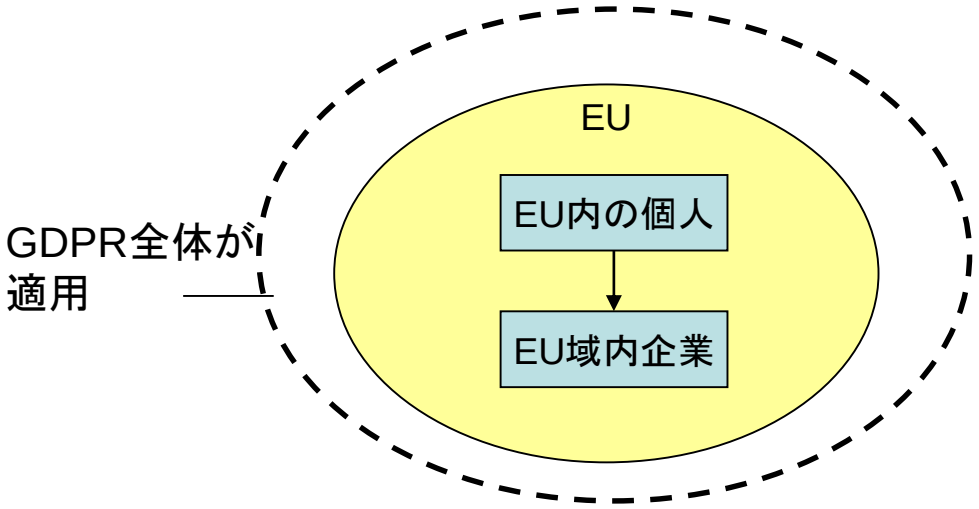
- GDPRでは、同意という例外措置の使用には高い敷居が設けられている。このような高い敷居、および同意をいつでも撤回できる権利に鑑みると、同意は第三国移転に対する長期的に有効なソリューションにはなりえないかもしれない。

EUから日本への個人データ移転： 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。
- 2017年7月3日には、個人情報保護委員会（PPC）と欧州委員会が協力対話を行い、日EU間の相互の円滑な個人データ移転を図る枠組みとして、相互に双方の保護水準が十分であることを認める相互認証を目指し、2018年の早い時期に成果を出すことを目標にお互い努力していくことについて確認。
- 2017年12月14日にPPCと欧州委員会は、日EU間の個人データ移転について会談を行い、双方の制度間の関連する相違点に対処するための、法令改正を行わない形での解決策について確認し、2018年第一四半期に、最終合意することを想定し、委員レベルで会談をもつことで一致。
- 上記「解決策」は、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を行う日本企業に対する上乗せガイドライン（個人情報保護委員会告示として個人情報保護委員会の監督権限が及ぶもの）となる見込み。
  - ①要配慮情報の範囲
  - ②保有個人データの範囲
  - ③利用目的の特定
  - ④日本から外国への個人データの再移転
  - ⑤匿名加工情報

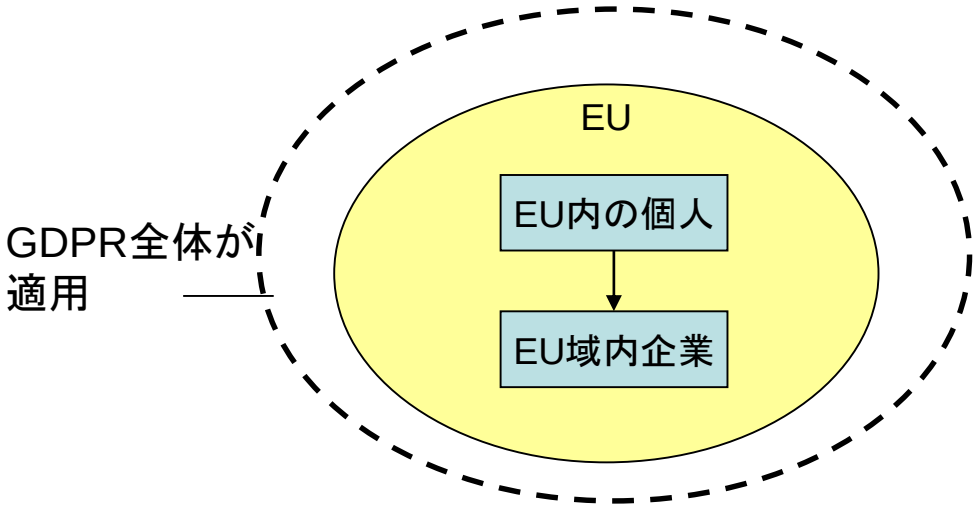
EUの個人データ取扱いに当たって注意すべきケース

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において個人データとみなされうる。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。



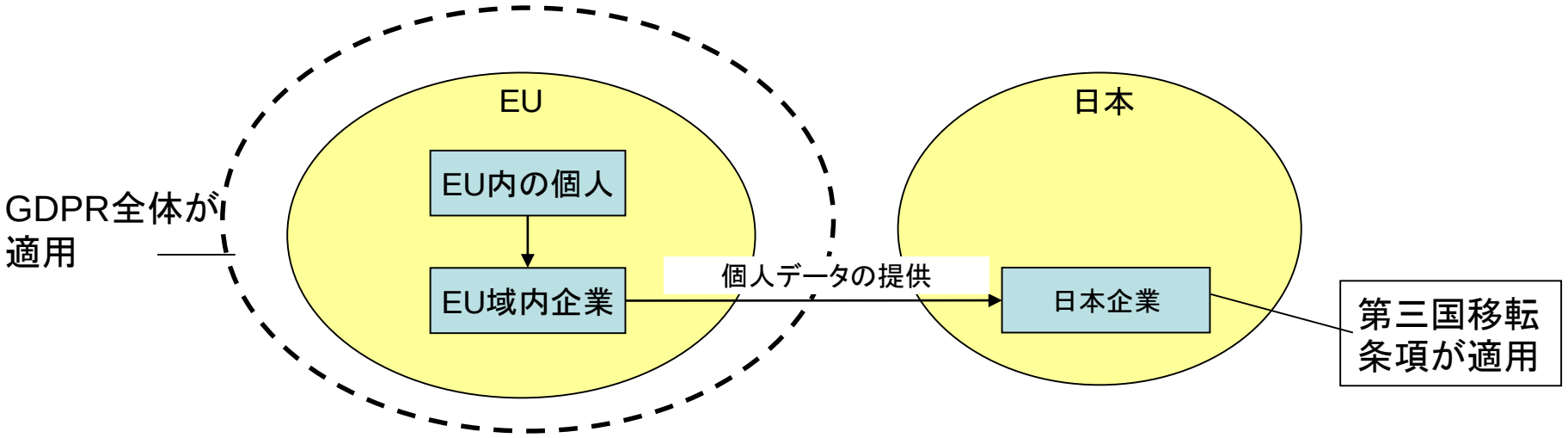
EUの個人データ取扱いに当たって注意すべきケース

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では、顔画像が個人情報に該当するのみならず、顔特徴データは「特別な種類の個人データ」に該当する。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、顔特徴データの取得に当たっては本人の明示的同意等が必要となる。



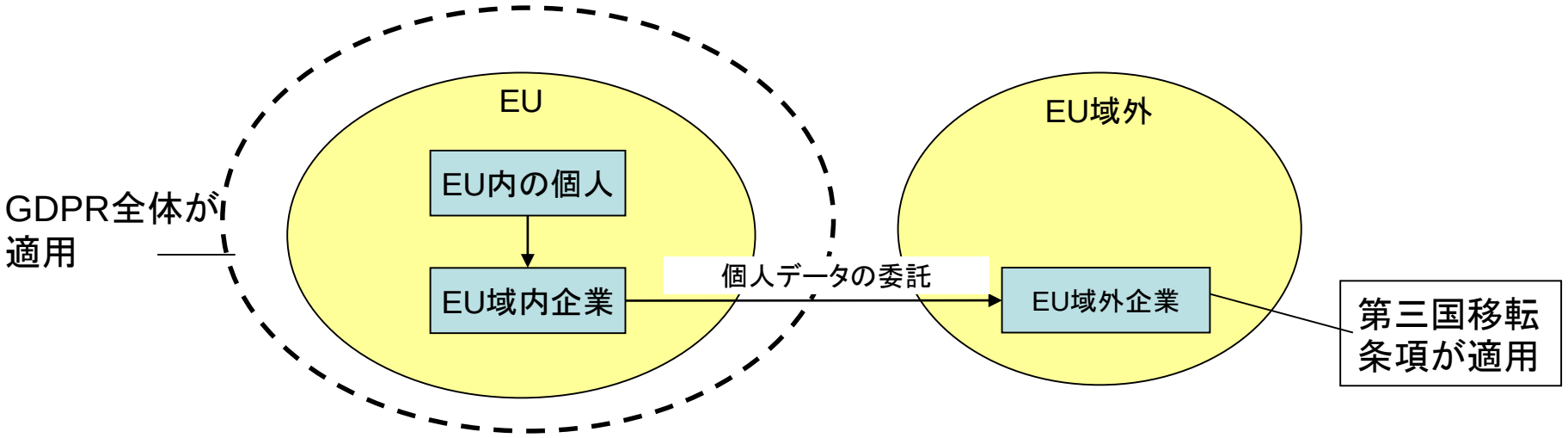
EUの個人データ取扱いに当たって注意すべきケース

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、（十分性認定までは）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いけない。



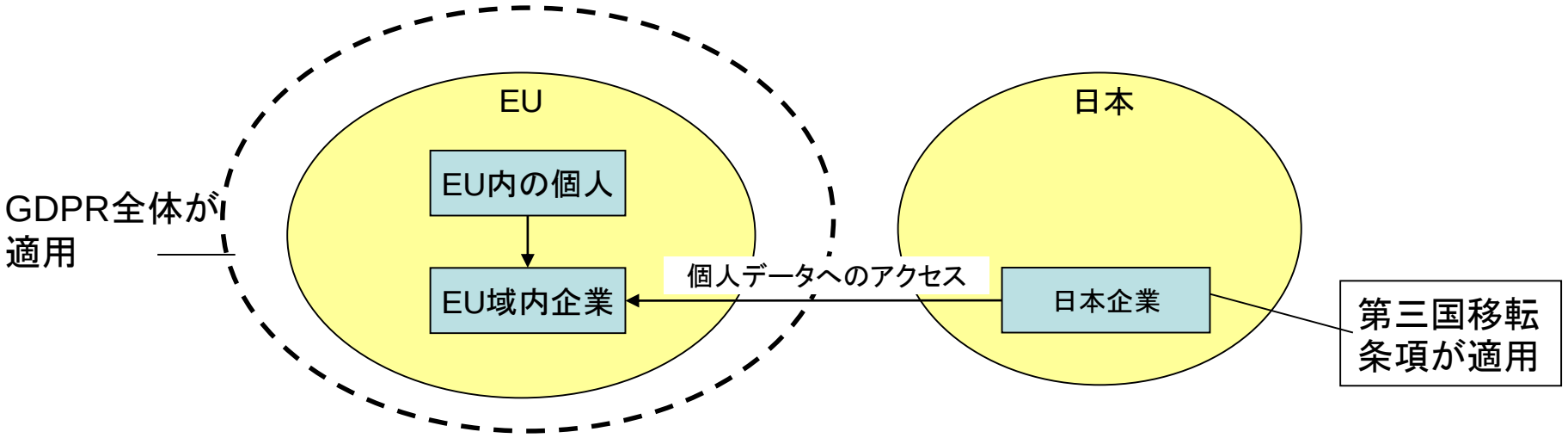
EUの個人データ取扱いに当たって注意すべきケース

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。



EUの個人データ取扱いに当たって注意すべきケース

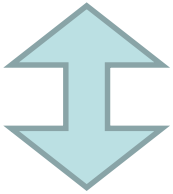
V. 個人データの第三国移転には、データを提供したり委託したりするケースのみならず、データに第三国からのアクセス許可を与えることも該当する。例えば、EU域内の医療機関が保有する病理画像に日本国内から病理医がアクセスするような場合。



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／一般データ保護規則(GDPR)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、韓国、台湾、香港　等
  - 日本(改正個人情報保護法)



- 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(2017年6月施行)のサイバーセキュリティ法において、重要情報インフラ運営者に対して国内で取得された個人情報と重要データの国内保存義務を規定。これらのデータを国外に持ち出す場合には、本人同意およびセキュリティ評価が必要。
  - **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。

【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。

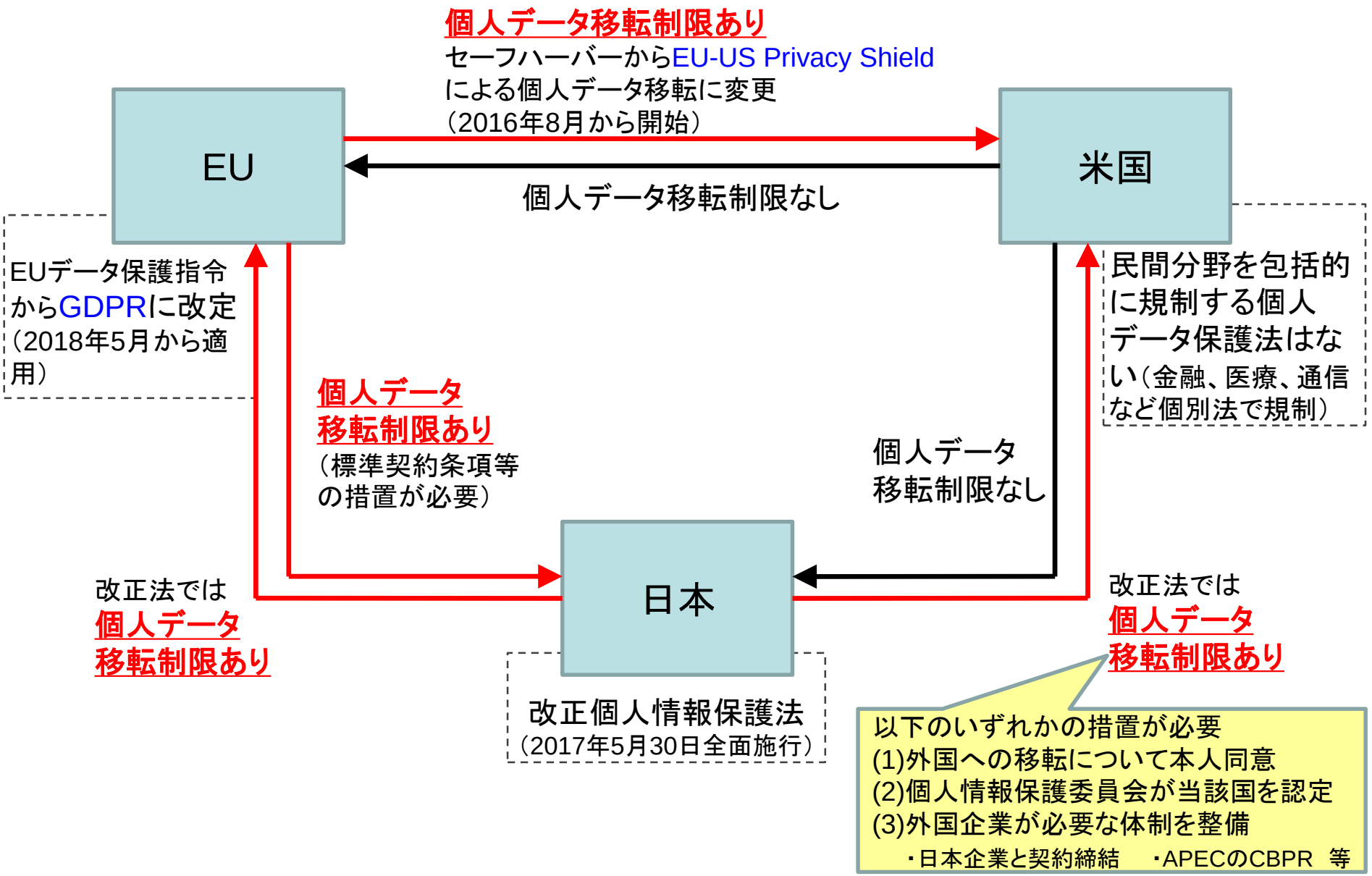
- G7 伊勢志摩首脳宣言（2016年5月27日）
  - 我々は，プライバシー及びデータの保護やサイバーセキュリティを尊重しつつ，インターネットの開放性，透明性及び自由を確保するため，**情報の自由な流通**及びデジタル・エコノミーの全ての主体によるサイバー空間への公平かつ平等なアクセスを促進することにコミットする。

日本国内へのデータ保存が要求されるケース

- 強制力はないが、ガイドラインや政府報告書等において、国内へのコンピュータ設備設置が要求されているケースがある。

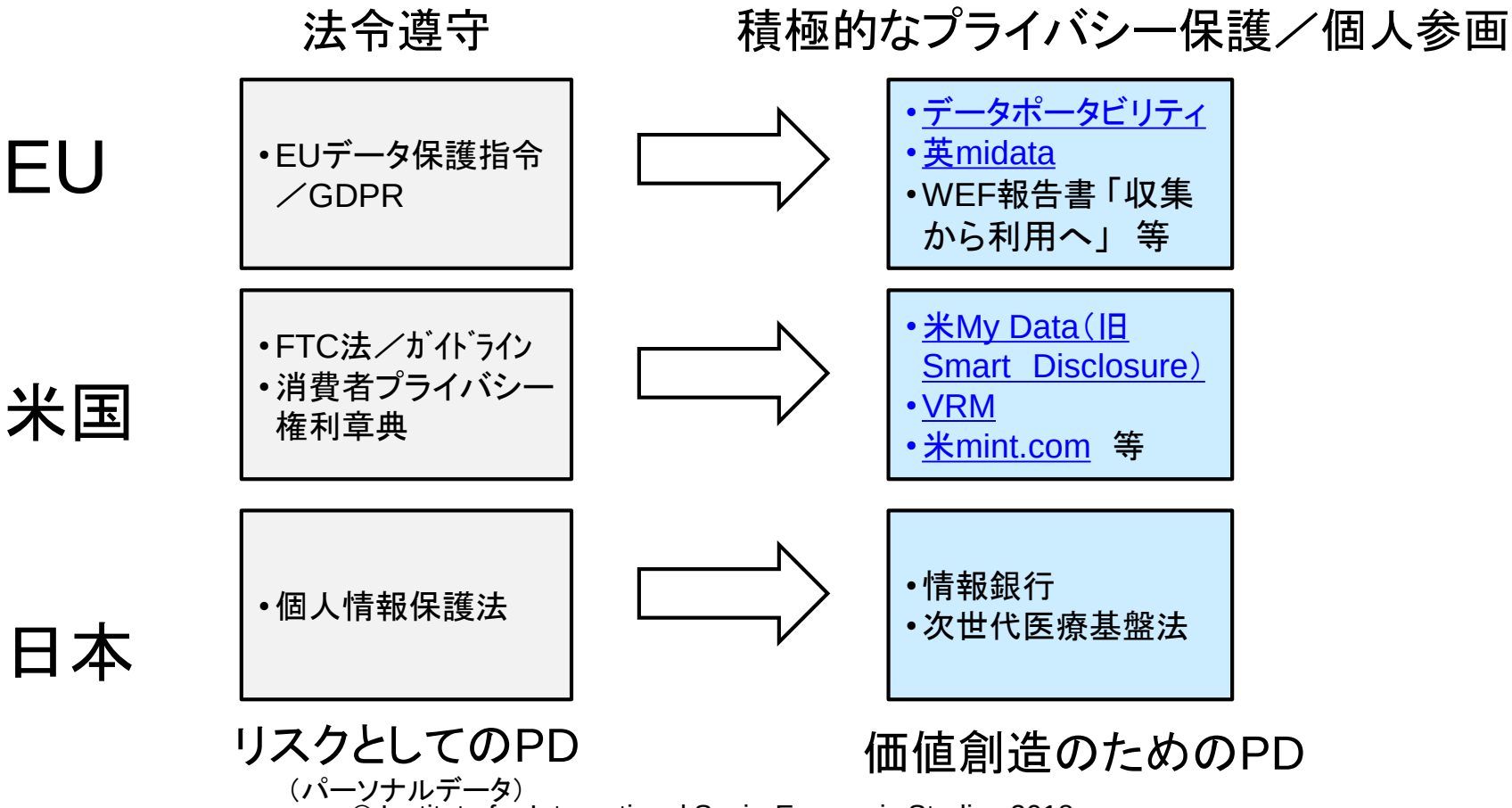
- 医療情報：
  - 「医療情報を受託管理する情報処理事業者向けガイドライン」（経済産業省、2012年）
    - 医療情報を受託管理する情報処理事業者を対象に、安全管理上の要求事項を記述したもの。
    - 「法令により作成や保存が定められている文書を含む場合には、医療情報システム及び医療情報が国内法の執行が及ぶ範囲にあることを確実とすることが必要である。」
      - 診療録は医師法により5年間の保存義務あり。
- 自治体関連情報：
  - 「自治体クラウド推進本部 有識者懇談会とりまとめ」（総務省、2011年）
    - 「・・・SLA等を確実に担保するためには、契約の規定でデータセンターの設置場所やアクセス区域を国内に限定する必要がある。また、民事裁判管轄・準拠法についてもサービス提供契約に特約が置かれることが一般的であるが、国内でなければ事実上の限界が生じる場合がある。」
  - 「自治体クラウド開発実証に係る標準仕様書」（地方自治情報センター、2010年度）
    - 「自治体クラウドのサービスを提供する場合、サービス提供者は、その取り扱う情報の重要性・機密性から日本国内法が適用される国内にデータセンターを設置する必要がある。」

【ご参考】 日米欧データ移転の全体像

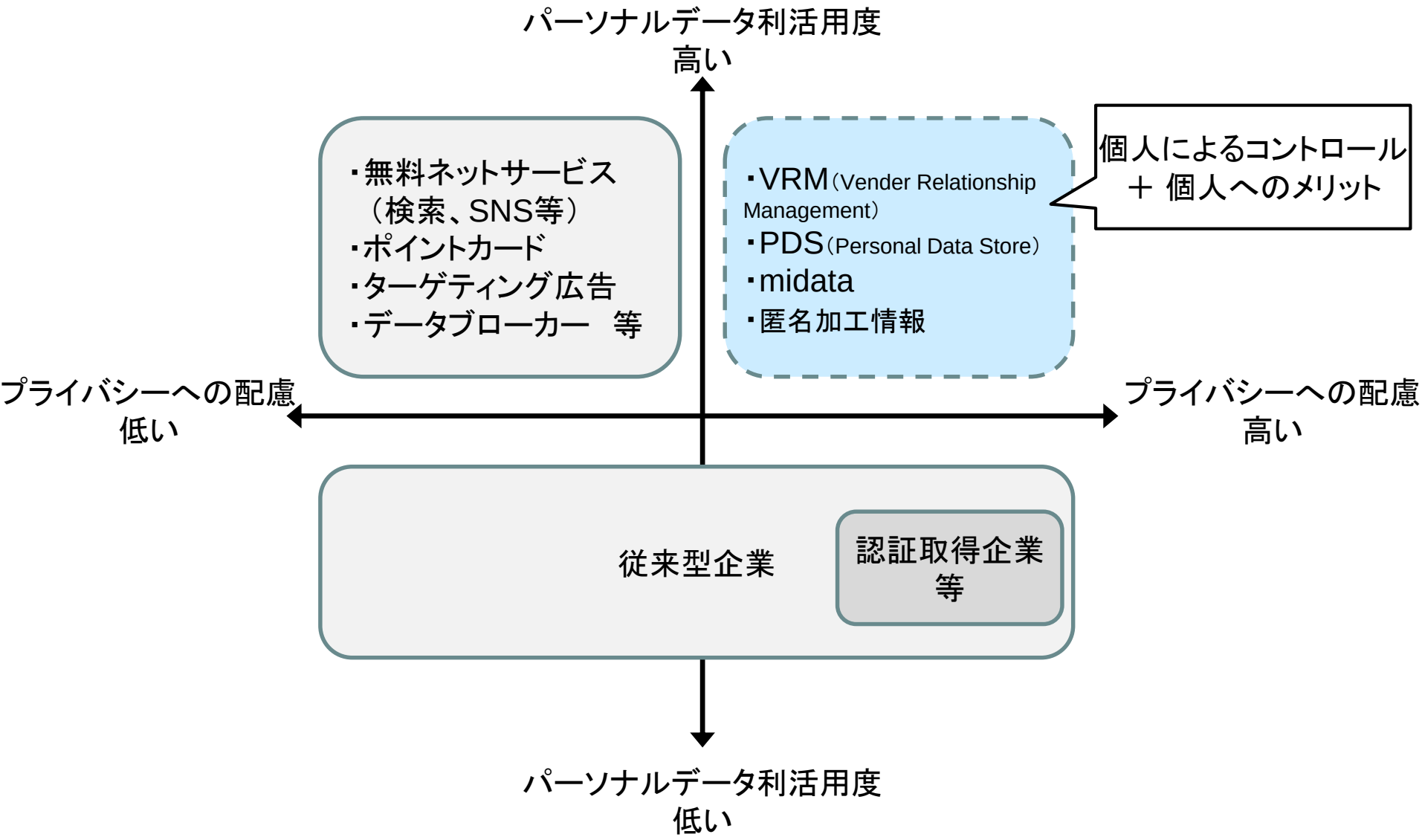


競争戦略としてのプライバシー保護（1/2）

- 従来は、企業における「データ利活用」と「プライバシー保護」は二律背反的な関係になりがちだった
  - 「法律さえ守っていれば何をやってもよい」
- 今後は**単なる法令遵守を超えて、データを利活用しつつ積極的にプライバシー保護を提供する取組みが重要に**
  - データ利用方法の透明性向上、自己情報コントロール手段の提供（PDS）、プライバシー・バイ・デザイン　等
  - 各種の漏洩事件等を通じた消費者意識の高まりも背景に（レピュテーションリスクへの対応）



競争戦略としてのプライバシー保護(2/2)



【ご参考】プライバシー現実主義者、原理主義者

- 米国のアラン・ウェスティン博士（自己情報コントロール権としてのプライバシー権の提唱者）とHarris Interactive社による米国市民に対する意識調査
  - 「**プライバシー原理主義者**（Privacy fundamentalist）」：プライバシー問題を非常に重視しており、自分のプライバシーの多くが失われていると感じる傾向にあり、**これ以上プライバシーが侵害されることに強い抵抗感**を感じている。
  - 「**プライバシー現実主義者**（Privacy pragmatist）」：プライバシーを重視し，自分の個人情報を企業や政府機関による誤用・濫用から守ることに高い関心を持つが、個人情報の利用目的が明確であり、**自分が恩恵を受けることができ、個人情報の誤用を防止するための措置が取られている場合には、個人情報の提供を厭わない**。
  - 「プライバシー無関心者（Privacy unconcerned）」：プライバシーに無関心で、他人が自分の個人情報をどう利用するかについてあまり心配していない。
- 市民の6割強が利益と保護のバランスが取れていれば個人情報を提供する「プライバシー現実主義者」、3割弱が個人情報の提供に消極的な「プライバシー原理主義者」。
  - 自分の個人情報に無頓着な「プライバシー無関心者」は少数派。

	プライバシー無関心者	プライバシー現実主義者	プライバシー原理主義者
2003年	10%（↓）	64%（↑）	26%
1999年	22%	54%	25%

出典：www.prnewswire.com、ITpro記事

プライバシー・バイ・デザイン

- プライバシー・バイ・デザイン（Privacy by Design：PbD）
  - 「設計段階からプライバシー保護を組み込む」というシステム開発・サービス開発の1つの「哲学」。企業や組織が果たすべき責任の1つ。
  - 実践手段として**PIA（プライバシー影響評価）**やPET（Privacy Enhancing Technology：プライバシー強化技術）を伴うもの。
- カナダの前オンタリオ州情報・プライバシーコミッショナーであるAnn Cavoukian博士によって1990年代に提案された概念。Cavoukian博士は下記7つの基本原則を提唱。

1. 事後的ではなく事前的、救済策的でなく予防的
2. 初期設定としてのプライバシー
3. デザインに組み込まれるプライバシー
4. 全機能的 — ゼロサムではなく、ポジティブサム
5. 最初から最後までのセキュリティ — すべてのライフサイクルを保護
6. 可視性と透明性 — 公開 の維持
7. 利用者のプライバシーの尊重 — 利用者中心主義を維持する

和訳の出典： 堀部政男/JIPDEC編『プライバシー・バイ・デザイン』

プライバシー・バイ・デザイン

- **EUのGDPR**、**米国FTC報告書（2012年）**や、**OECDガイドライン改定版**の補足説明覚書等に盛り込まれた。

- プライバシー・バイ・デザインが近年これらのフレームワークに盛り込まれている背景（仮説）
  - ICTの発展により、個人データ漏洩・濫用時の影響・被害が甚大化。
  - 技術進歩に法律制定・法規制が追い付かなくなりつつある。
  - **企業の個人データ取扱いが複雑化し、個人が自分のデータの取扱われ方について、プライバシーポリシーを読んでも必ずしも理解できなくなっている**。（同意原則の形骸化）

cf. 米国FTC報告書（2012年）

「（プライバシー・バイ・デザインを通じて）消費者から負担を取り除き、企業に消費者データを責任ある仕方で取り扱う義務を課すことによって、**消費者に長くて分かりにくいプライバシー通知を読ませることなく、消費者に基本的なプライバシー保護を提供するべき**である。」

プライバシー・バイ・デザイン事例： 空港のボディスキャナー（米国）

●課題：

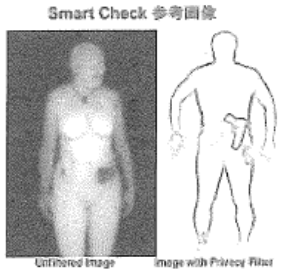
- 服を着たままで武器携帯等をチェックできるが、裸に近い画像が撮影されてしまう。

●PbDによる解決策：

- 裸に近い画像を外形表示に変換。
- 搭乗客が見えない別室で別の係員が画像を確認する。
- 不安な搭乗客は従来の金属探知機による検査を選べる。

【ビジネス慣行】
●不安や不信を抱く旅行者には、この検査を拒否し、これまでの金属探知機などによる検査を選ぶ自由が与えられる

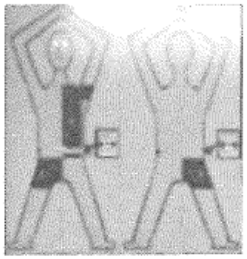
【技術】
●裸に近い画像を外形表示に変換して表示される
●画像は保存せず破棄される



確認

異常の有無を通知

【技術】
●変換された画像をさらにあいまいにした画像で確認する



【物理設計】
●監視員は搭乗客が見えない場所（別室）で分析し、搭乗客と画像を見比べることができない
●搭乗客と同性の監視員が作業
●携帯電話持ち込み禁止

出典： 堀部政男/JIPDEC編『プライバシー・バイ・デザイン』

米国Smart Disclosure： Blue Button

- 概要
  - 官民連携イニシアティブ。該当する連邦政府機関のサイト上で「Blue Button」をクリックすると、自分の個人医療データ（PHR）をダウンロードできる。
  - 退役軍人、Medicare（※）受給者、兵役者は以下のサイトから、これら連邦政府機関が保有する自己データをダウンロードしたり、自分の医療機関に自己データを提供したり、個人医療アプリなど様々なデータ利用サービスで自己データを利用することが可能。
    - 退役軍人： MyHealtheVet サイト
    - Medicare受給者： MyMedicare サイト
    - 兵役者： TRICARE サイト
  - 対象者は合計で約100万人。
- Blue Buttonへの参画者
  - 連邦政府機関では、退役軍人省、保健福祉省CMS、国防総省、人事管理庁が参加。
  - 米国の大手医療保険者や医療機関も自発的に導入を開始（UnitedHealthCare、Aetna、Walgreens）。
- 法的根拠
  - HIPAA（Health Insurance Portability and Accountability Act、医療保険の携行性と責任に関する法律）のプライバシールールでは、幾つかの例外を除き、プライバシールールがカバーする医療保険と医療機関によって保有される自己の医療記録および請求記録を調査し、レビューし、コピーを受領する権利を個人に与えている。

※Medicare：65歳以上の高齢者向けの健康保険。

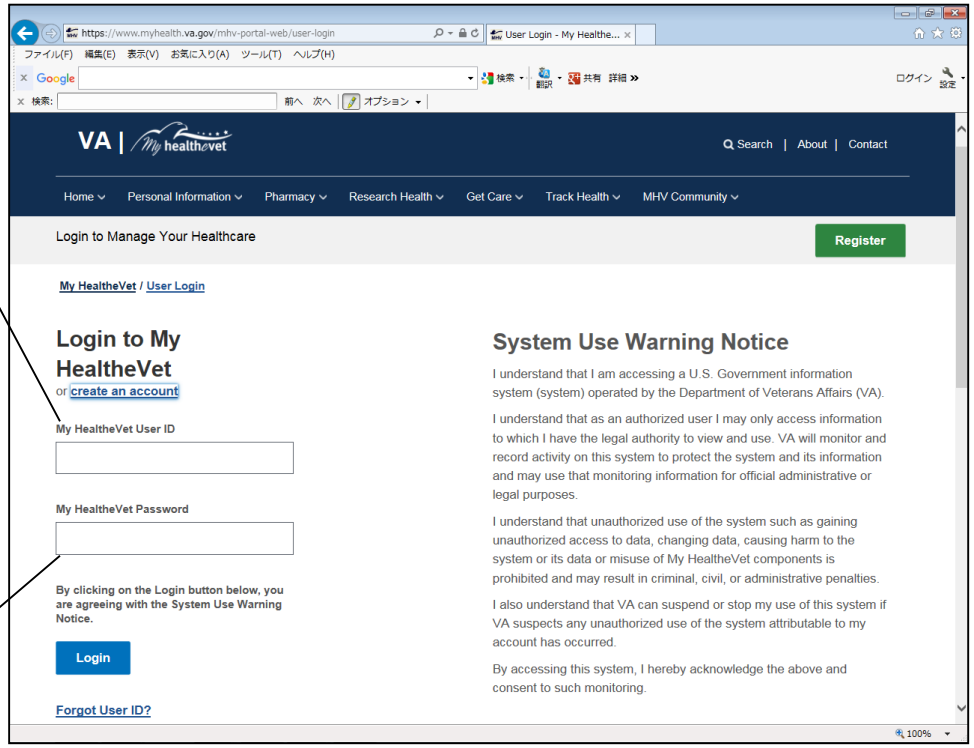
米国Smart Disclosure： Blue Button

○ MyHealtheVet（退役軍人向けサイト）

個人医療記録（PHR）のダウンロード方法

①MyHealtheVetのアカウント登録をする。
・オンライン登録時に本人確認のために「氏名」「SSN（プレミアム登録時にのみ必要）」「生年月日」「性別」が必要。また、「連絡先（eメール、電話）」「希望するIDとパスワード」「秘密の質問と回答」も登録。

②MyHealtheVetにID／パスワードでログインする。
・IDはアルファベットと数字の組合せで6～12文字。
・パスワードはアルファベットと数字と特殊記号（!, #, %等）の組合せで8～12文字。



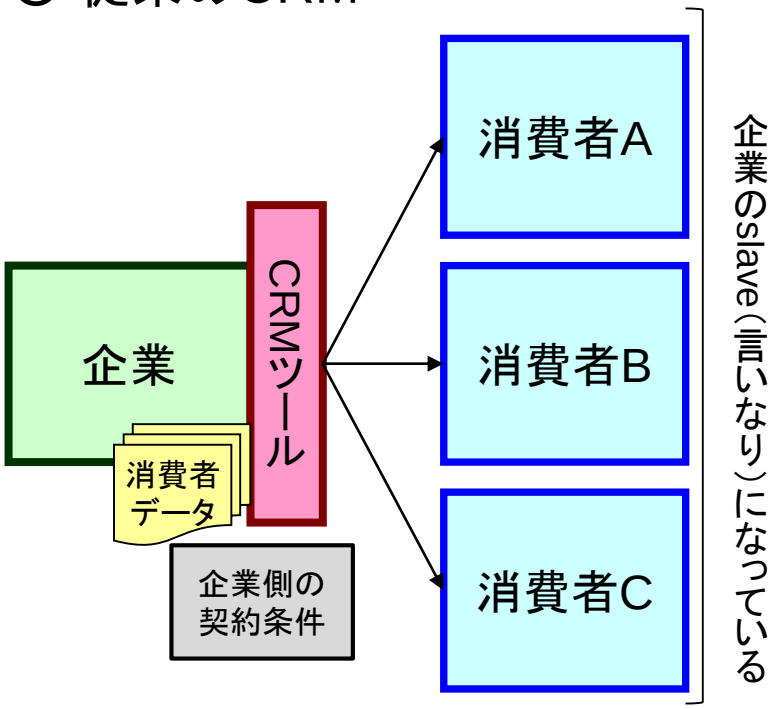
- PHRは、「PDF」「テキストファイル」「カスタマイズ可能なBlue Buttonファイル（XML）」のいずれかの形式でダウンロード可能。ダウンロードするPHRの期間や情報カテゴリを指定可能。
- ダウンロード可能なPHRに含まれるデータは以下。
  - 兵役中の医療記録・医療事象・検査結果
  - 緊急連絡先、医療チーム、保険者向けの情報
  - 処方箋なしに購入できる薬品、アレルギー、 ダイエット記録、運動記録等の日常的な記録
  - 血圧、血糖値、コレステロール、心拍数、体温、体重、痛みの程度等のバイタル測定値データ
- 「既往歴」「緊急連絡先」「投薬情報」は、本人がPHRに入力可能。
- さらに「VA Patient」としてプレミアム登録した利用者は、以下も閲覧できる。
  - 個人医療記録に基づき退役軍人省や国防総省が付加した情報
  - 処方箋の記録

Blue Button Download My Data

※Blue Button
官民連携イニシアティブ。該当する連邦政府機関のサイト上で「Blue Button」をクリックすると、自分の個人医療記録（PHR）をダウンロードできる。対象者は退役軍人、Medicare受給者、兵役者。

米国Project VRM： CRMからVRMへ

○ 従来のCRM



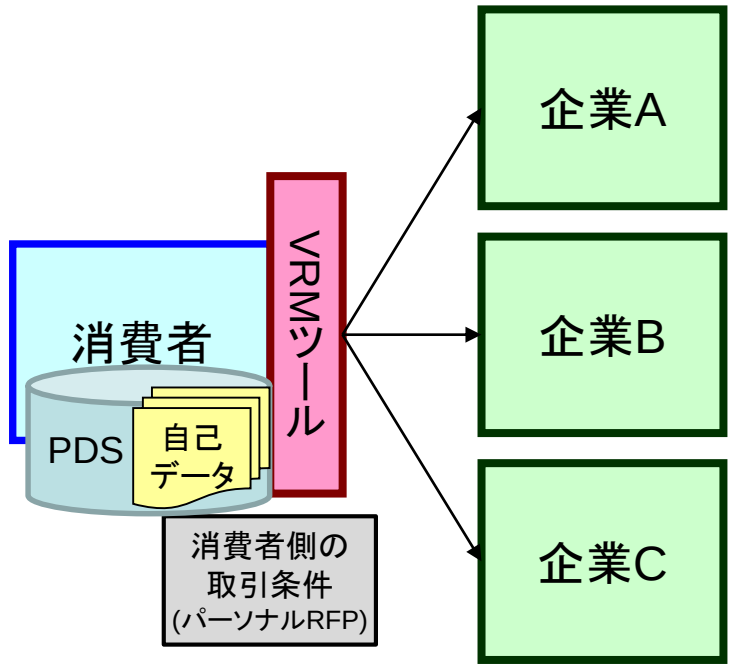
・Attention Economy（消費者の「注意」の経済）

- 企業は消費者データの分析や広告等に巨額を投じ、消費者は企業の提示する契約条件に従属

•企業が主権者として、消費者を「ターゲット」にし、「惹きつけ」、「獲得」し、「囲い込み」、「管理」する。

•企業は「奴隷所有者」的な発想で消費者を扱う。

○ あるべき姿（VRMによる補完）



・Intention Economy（消費者の「意思」の経済）

- 消費者自身による購買意思や取引条件の提示（パーソナルRFPとしての提示）

•消費者が主権者として、企業から「独立」できる。

•消費者は「エンパワーされた参加者」として企業との取引関係をコントロールできる。

•企業も消費者の正確なニーズを知ることができる。

※詳細は「パーソナルデータ利活用に関する海外事例調査報告書」をご参照ください。
（https://www.i-ise.com/jp/information/report/pdf/IISE2013.pdf）

出典：国際社会経済研究所

米国Mint.com： オンライン家計簿サービス

○ Mint.comのサービスの全体像

①Mintアカウント作成

・メルアド、PW、ZIPコードの登録

②取引データ自動収集の設定

・金融アカウントのID／PWの入力

個人
（ユーザ数
1000万人以上）

Mint.com
（Intuit社が
運営）

③Yodlee経由で
金融企業から取引
データを自動収集

Yodlee
（アカウント・アグリゲーション企業）

※Mintが支払う
手数料は年間
200万ドル

銀　行

クレジットカード
会社

証券会社

保険会社

提携先
約1800社

○保有データ
・メルアド
・ZIPコード
・金融取引データ
・金融資産データ
等

④サービスの提供（無料）

・毎月の支出額をカテゴリー別に管理

・口座残高、ローン残高、保険口座、証券口座の管理

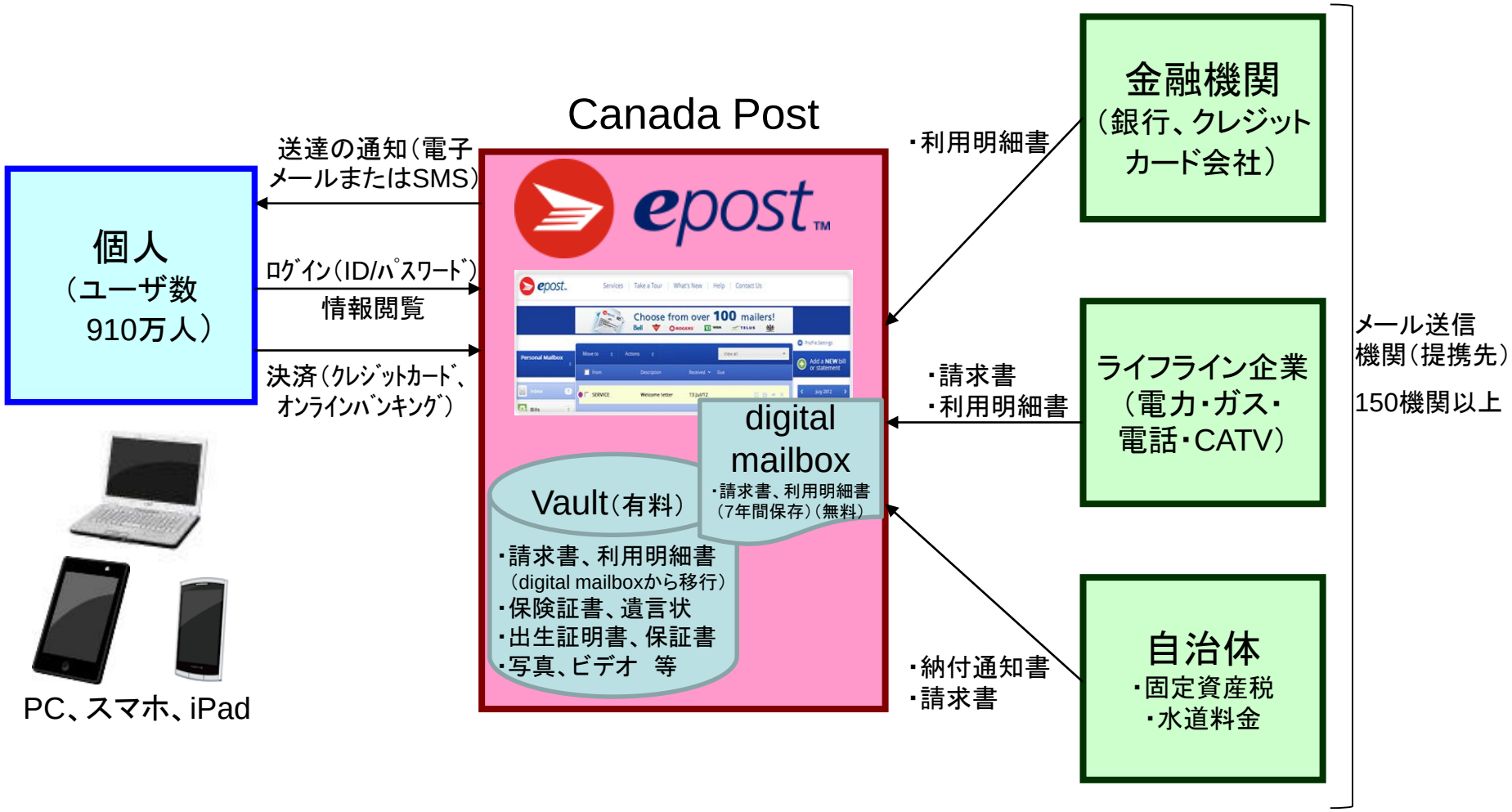
・ユーザに合った預金口座、クレジットカード、各種保険、証券商品等のレコメンド（※新規契約時に金融企業から手数料がMintに支払われる）

・ユーザ集団のカテゴリーごと支出額平均値が分かる

・予算設定機能、ゴール設定機能　等

出典：国際社会経済研究所

カナダepost： 電子送達サービス



※PDSというよりは、日本のかつての「電子私書箱」構想に近い。
※従来紙で郵送されてきたものを電子送達しようというサービスなので、データを二次利用しようという発想は少ない。

出典：国際社会経済研究所

説明者の略歴

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/マイナンバー制度）、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
  - 「米国における顔認識技術とプライバシー保護」（画像ラボ2018年2月号）
  - 「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）　等