プライバシー・パーソナルデータ問題
～JEITAの活動を中心に～

2014年3月14日
国際社会経済研究所
小泉　雄介
y-koizumi@pd.jp.nec.com

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（2013年7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（2012年1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）

【ご参考】EUデータ保護指令改定の背景

- EUデータ保護規則案（2012年1月公表）。
  今回の改正は、指令の採択から15年以上経ち、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
- PATRIOT法により、令状無しに米国企業の国外現地法人からも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（中国など）：
- 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データ保護規則案には、（特に米国企業に対する）非関税障壁の側面もある

EUデータ保護規則案の日本企業への影響

現行指令

・第三国(日本)への
データ移転制限は継続
(データ保護の十分性認定に至らず)

指令改定

規則強化

・ﾃﾞｰﾀ保護の権利強化
(忘れられる権利、ﾃﾞｰﾀﾎﾟｰﾀﾋﾞﾘﾃｨ、違反時の義務や罰則等々)

・強化規則の域外適用
(現行指令はEU域内設備でﾃﾞｰﾀ処理を行う場合のみ適用が、域外企業へも適用に)

規則緩和

・EU域内ルールの一元化
・ﾃﾞｰﾀ処理の監督機関への届出義務廃止
・BCR手続きの簡素化　等々

＜産業界にとっての問題点＞

・ﾃﾞｰﾀ移転制限によるｸﾞﾛｰﾊﾞﾙな事業活動の制約(例外規定対応への多大なコスト負担等の負荷含む。ex. ｸﾞﾛｰﾊﾞﾙ人材活用の為の従業員ﾃﾞｰﾀの日本本社への移転対応など)

・事業活動の抑制や萎縮により革新的サービスの提供の妨げ

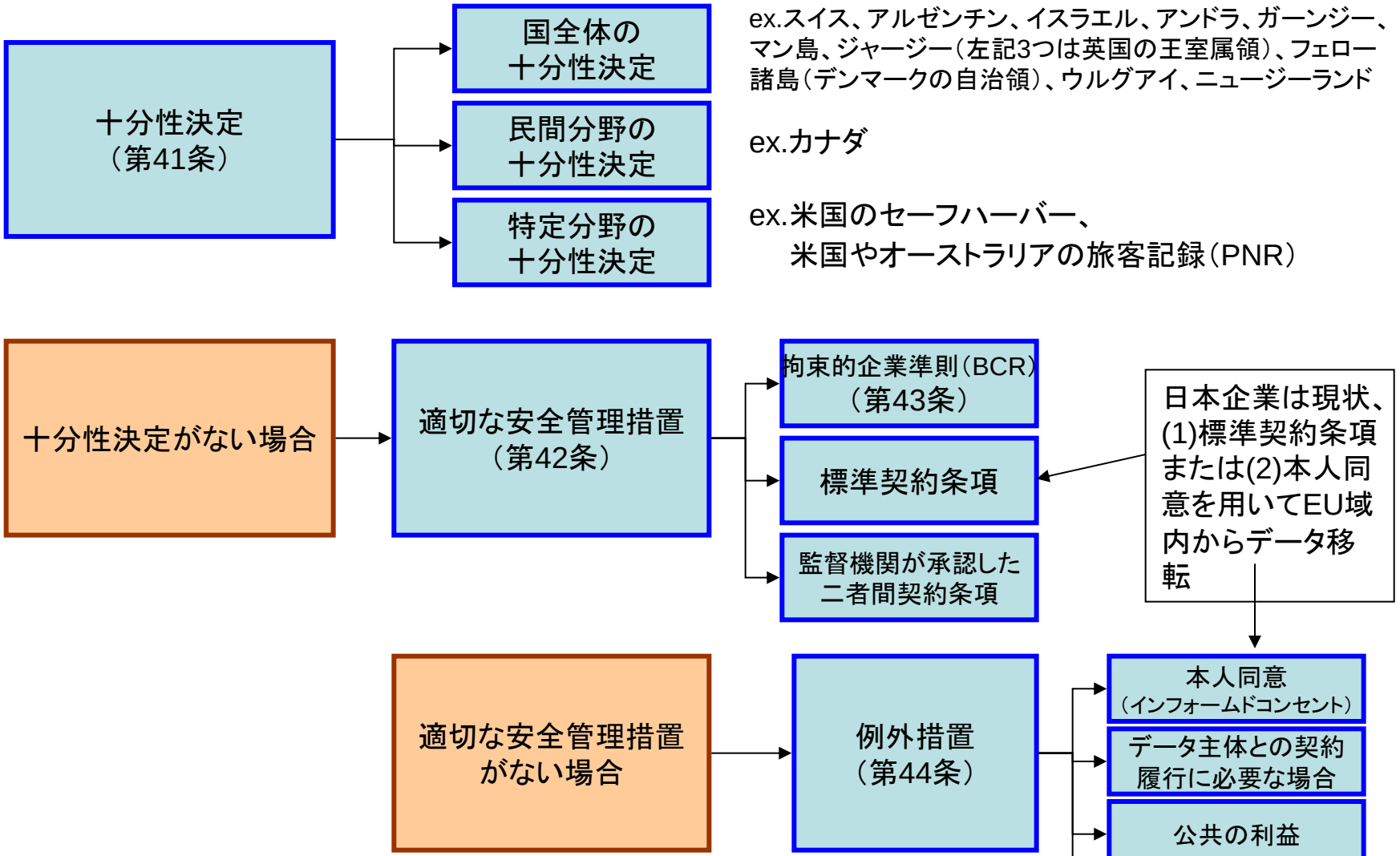
・EU域内事業拠点を含め、強化規則対応のための多大な負荷

＜EU域内日本企業拠点にも利益＞

・規則対応や手続きの簡素化によるコスト削減含む負荷の軽減

(出典:JEITA個人データ保護専門委員会)

EU規則案における第三国へのデータ移転方法



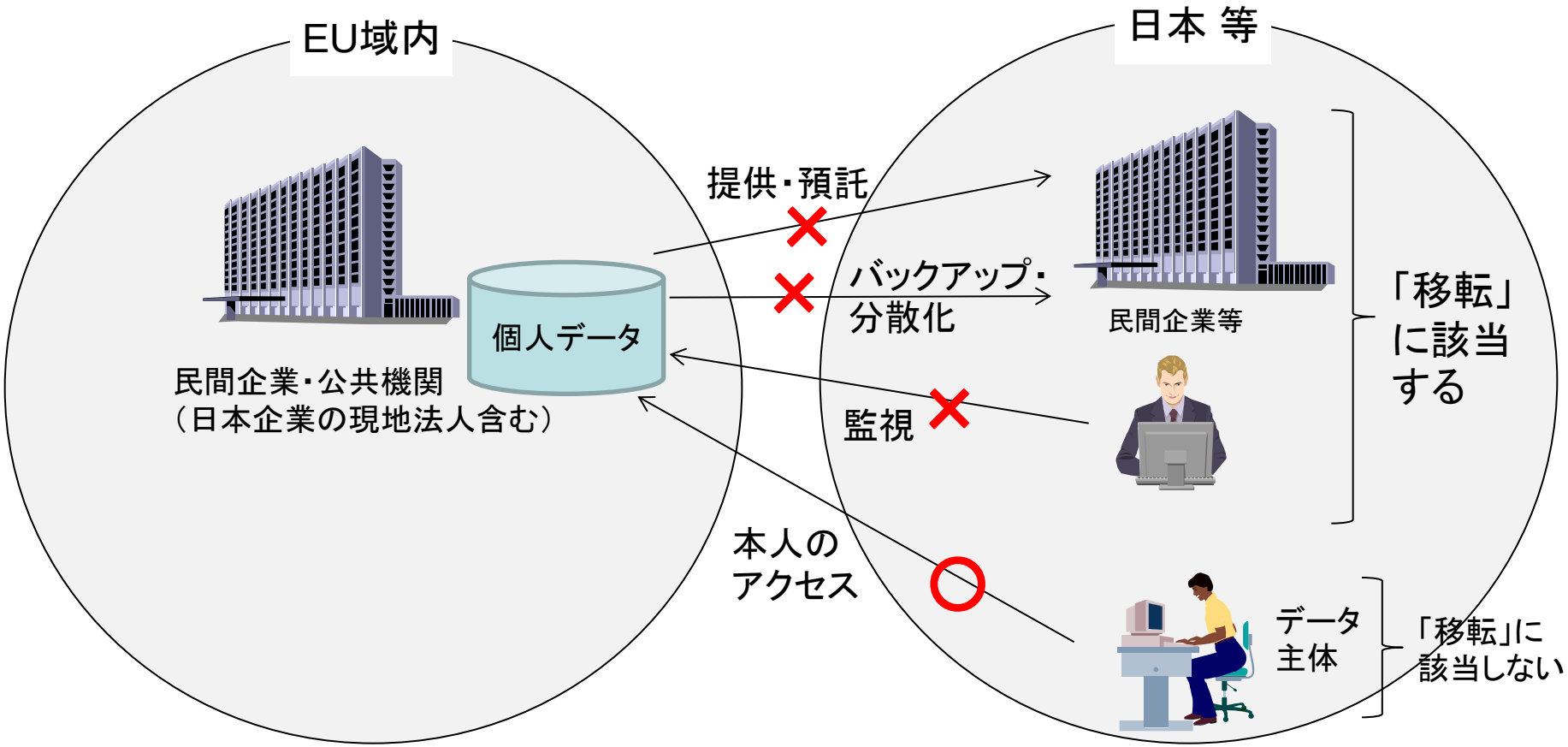
(1)標準契約条項の問題点：　相手企業ごと・案件ごとに締結が必要、弁護士費用等のコスト、監督機関の承認に時間がかかる、EU企業に日本企業側のデータ取扱いに関する責任発生など

(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

（出典：国際社会経済研究所）

第三国データ移転の「移転」とは何か

- EU指令に言う「移転」の定義
  - 「管理者（EU域内の企業等）が、第三国に所在する第三者に個人データを利用可能（available）とするために取る行為」の総称

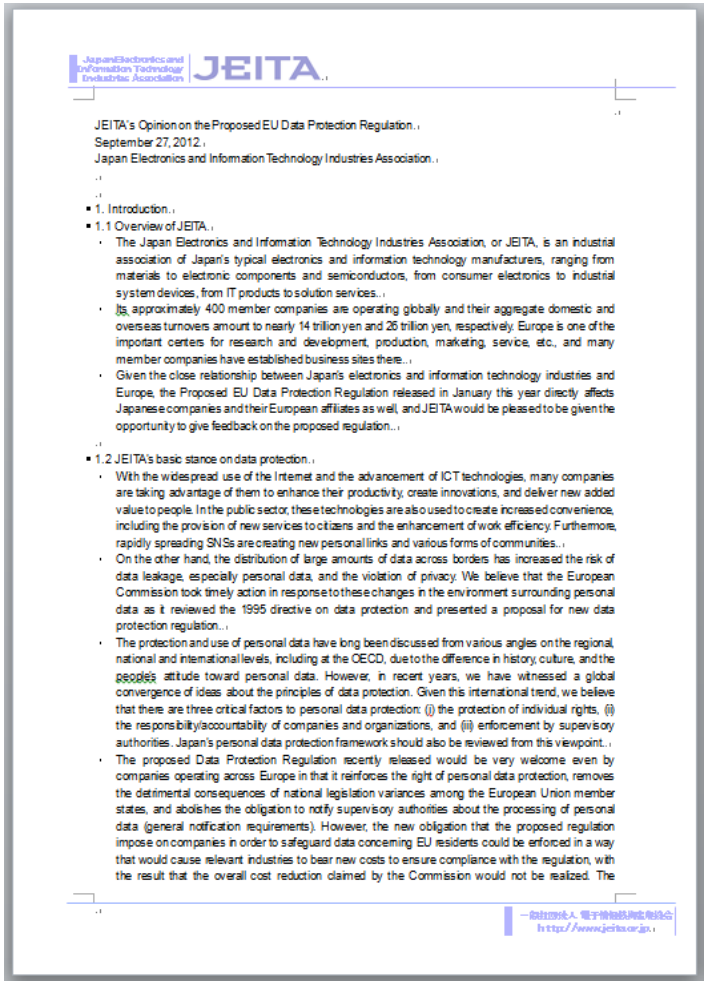


（出典：国際社会経済研究所）

EU規則案に対するJEITA意見書(1/2)

○以下の項目に対する日本産業界としての意見・要望(2012年9月)

- 第三国移転と適切な安全管理措置
- 従業員データの第三国移転
- 域外適用の除外条件
- 個人データの定義
- ポリシーの透明性と本人同意
- 従業員データの合法的処理
- 大規模災害時のデータ処理
- 忘れられる権利
- データ・ポータビリティの権利
- 個人データ違反の監督機関への通知
- プライバシー影響評価
- プライバシー・バイ・デザインと処理のセキュリティ
- 監督機関による課徴金
- 認証メカニズム、データ保護シール



JEITA

JEITA's Opinion on the Proposed EU Data Protection Regulation.
September 27, 2012.
Japan Electronics and Information Technology Industries Association.

1. Introduction.
1.1 Overview of JEITA.

- The Japan Electronics and Information Technology Industries Association, or JEITA, is an industrial association of Japan's typical electronics and information technology manufacturers, ranging from materials to electronic components and semiconductors, from consumer electronics to industrial system devices, from IT products to solution services.
- Its approximately 400 member companies are operating globally and their aggregate domestic and overseas turnovers amount to nearly 14 trillion yen and 26 trillion yen, respectively. Europe is one of the important centers for research and development, production, marketing, service, etc., and many member companies have established business sites there.
- Given the close relationship between Japan's electronics and information technology industries and Europe, the Proposed EU Data Protection Regulation released in January this year directly affects Japanese companies and their European affiliates as well, and JEITA would be pleased to be given the opportunity to give feedback on the proposed regulation.

1.2 JEITA's basic stance on data protection.

- With the widespread use of the Internet and the advancement of ICT technologies, many companies are taking advantage of them to enhance their productivity, create innovations, and deliver new added value to people. In the public sector, these technologies are also used to create increased convenience, including the provision of new services to citizens and the enhancement of work efficiency. Furthermore, rapidly spreading SNSs are creating new personal links and various forms of communities.
- On the other hand, the distribution of large amounts of data across borders has increased the risk of data leakage, especially personal data, and the violation of privacy. We believe that the European Commission took timely action in response to these changes in the environment surrounding personal data as it reviewed the 1995 directive on data protection and presented a proposal for new data protection regulation.
- The protection and use of personal data have long been discussed from various angles on the regional, national and international levels, including at the OECD, due to the difference in history, culture, and the people's attitude toward personal data. However, in recent years, we have witnessed a global convergence of ideas about the principles of data protection. Given this international trend, we believe that there are three critical factors to personal data protection: (i) the protection of individual rights, (ii) the responsibility/accountability of companies and organizations, and (iii) enforcement by supervisory authorities. Japan's personal data protection framework should also be reviewed from this viewpoint.
- The proposed Data Protection Regulation recently released would be very welcome even by companies operating across Europe in that it reinforces the right of personal data protection, removes the detrimental consequences of national legislation variances among the European Union member states, and abolishes the obligation to notify supervisory authorities about the processing of personal data (general notification requirements). However, the new obligation that the proposed regulation impose on companies in order to safeguard data concerning EU residents could be enforced in a way that would cause relevant industries to bear new costs to ensure compliance with the regulation, with the result that the overall cost reduction claimed by the Commission would not be realized. The

JEITA: 一般社団法人 電子情報技術産業協会

http://home.jeita.or.jp/press_file/20121214172407_QmZqTgt0AW.pdf

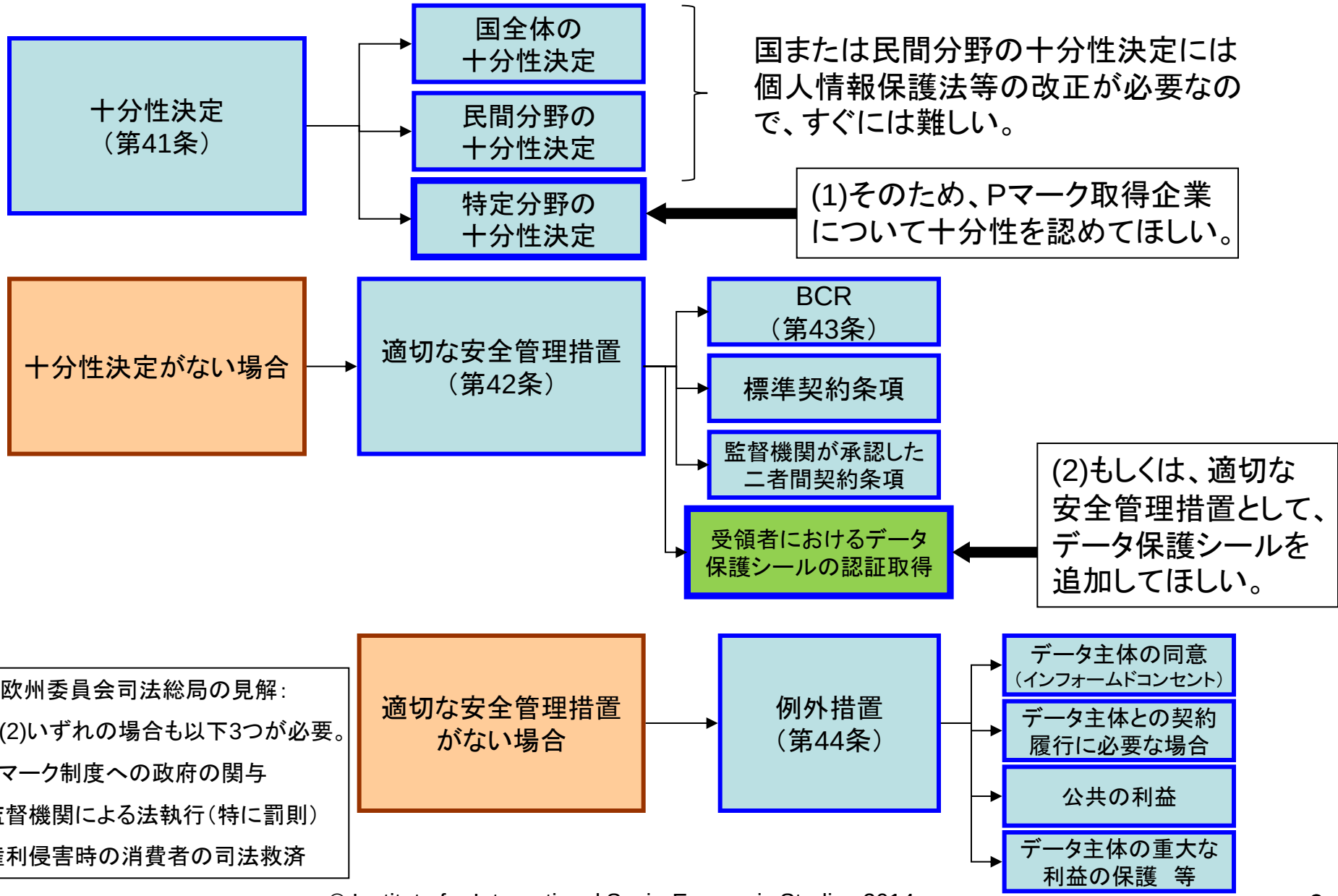
EU規則案に対するJEITA意見書（2/2）

- 2012年11月と2013年6月の2回、訪欧ミッションを実施
  - 第1回は欧州議会議員、欧州委員会司法総局を中心にロビーイング
  - 第2回は欧州連合理事会（加盟国代表部）、在欧業界団体を中心にロビーイング

- 日本における個人情報保護制度は、欧米に比べ、単一的な監督機関がない、罰則規定が緩い、司法救済の規定がないなど「十分なレベル」にないと思われる部分があるため、意見書作成にあたっての寄り所が難しかった。
- すなわち、日本はEUや米国と同等な立場に立っていないため、「日本では一定のデータ保護の原則に基づいて、きちんと保護しているから、規則案のこの部分は譲歩してほしい」と言うことが難しかった。

- ちなみに、米国では、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これまで自主規制が推奨されてきたが、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。
- EUと考え方は違うが、筋は通っているため、EUとしても米国の意見を傾聴せざるを得ない。（もちろん、欧米間の経済的相互関係の大きさや、米国の国際的発言力も大きな要因だが。）

第三国移転へのシール制度活用（JEITA意見書より）



欧州議会修正案： 主な修正条項

- 第3条2項（域外適用）
- 第4条2a項（仮名データ）
- 第6条（処理の合法性）
- 第7条（同意の条件）
- 第13a条（標準化された情報通知ポリシー）
- 第17条（忘れられる権利）
- 第23条（データ保護バイ・デザインとデータ保護バイ・デフォルト）
- 第31条（個人データ違反の監督機関への通知）
- 第32a条（リスクの尊重）
- 第33a条（データ保護遵守レビュー）
- 第39条（認証）
- 第41条（十分性決定がなされた国への移転）
- 第42条（適切な安全管理措置による移転）
- 第43a条（EU法によってオーソライズされない移転又は開示）
- 第79条（行政罰）

欧州議会修正案：
2013年10月21日に欧州議会LIBE委員会で可決、
2014年3月12日に欧州議会本会議で可決。

欧州議会修正案： 第42条（適切な安全管理措置による移転）

○ 第42条

- ※十分性決定のない第三国へのデータ移転を可能とする「適切な安全管理措置」として、（BCRや標準契約条項と同列で）「管理者および受領者における欧州データ保護シール」を追加。

- ※従来のEU指令に基づく「BCR」は、本規則の施行（entry into force）から2年後に失効することを規定。

欧州議会修正案における「仮名データ」の扱い

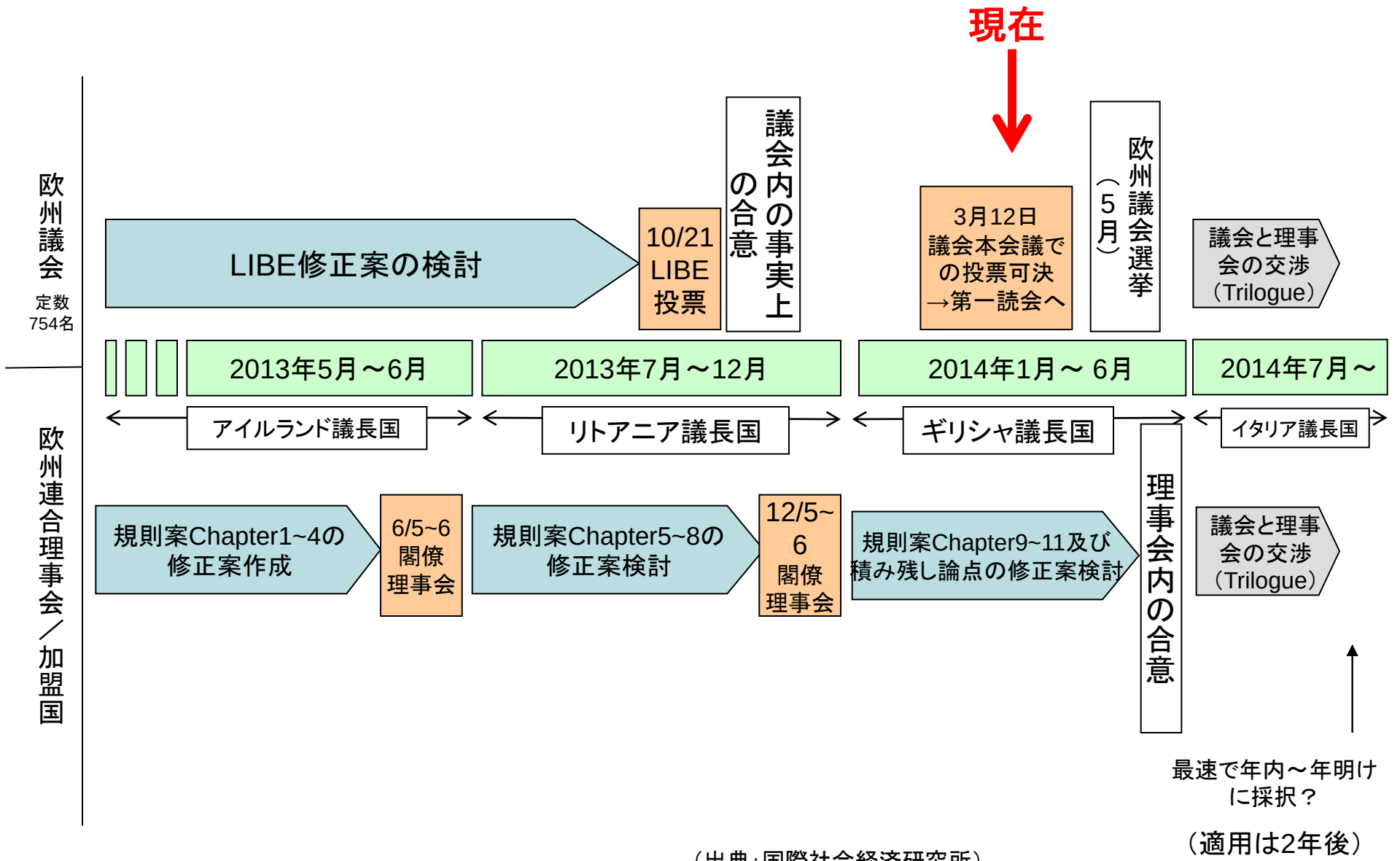
○ 第4条2a項 【新規追加】

- 「仮名データ（pseudonymous data）」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）ことができない個人データを意味する。その条件とは、当該追加情報をデータ主体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。

- ※**仮名データは個人データの1類型**であるが、管理者や処理者が仮名データの処理を行う場合には通常の個人データの処理を行う場合に比べて、**様々な義務が緩和**されている。
  - 仮名データに限った処理は、第6条にいう「データ処理の合法性」において、データ主体の合理的な期待に適合した処理とみなされる。【前文（38）】
  - 仮名データ処理に基づく「プロファイリング」は、データ主体の利益・権利等に重大な影響を与えるとはみなされない（ので、本人の明示的な同意等は必ずしも必要とされない）。【前文（58a）】
  - 仮名データに限った処理の場合、データ主体から自己データに関するアクセス請求等があった場合に、必ずしも管理者は請求に応じなくてよい。【第10条】

- ※その他、仮名データに関しては、以下のような規定がある。
  - 医師に代わって健康医療データを処理する処理者は、可能な限り匿名化されたデータ又は仮名化されたデータのみを受領し、処理するものとする。【前文（122a）】
  - データ保護影響評価の項目の一つとして、仮名化等の個人データ保護メカニズムのリストアップが挙げられている。【第33条】
  - 健康医療データを研究目的で、データ主体の同意なく処理する場合には、匿名化または仮名化が必要である。【第81条】

EUデータ保護規則案の審議スケジュール（推定）



（出典：国際社会経済研究所）

欧州評議会(CoE): 個人データ保護条約

- **欧州連合(EU)とは全く別の国際機関**。EUの加盟国27カ国すべてを含む47カ国から成る。
  - 欧州評議会のミッションは、**人権の向上**、民主主義、法の支配の3つ。
- 「個人データの自動処理に係る個人の保護のための条約第108号」
  - 1980年、閣僚委員会により採択。1981年、各加盟国の署名に付された。
  - 2014年3月現在、46ヶ国(非加盟国ウルグアイを含む)が批准。
  - **データプライバシーの領域において(欧州評議会の非加盟国を含め)全世界に適用可能な、唯一の法的拘束力を持った国際的法律文書**。
  - データ保護の基本原則として、下記を提示。

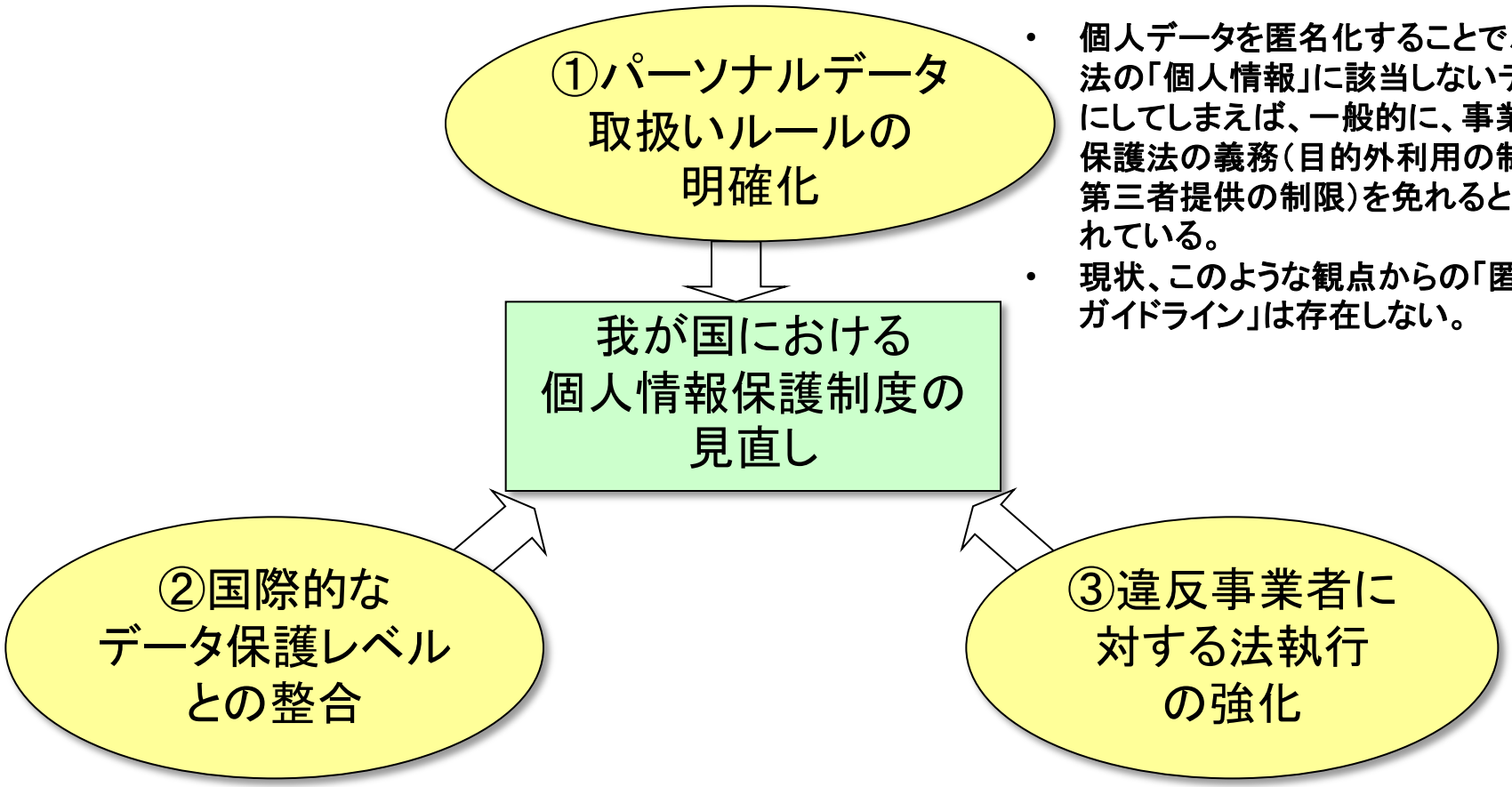
• 各国の義務	• データの内容
• 特定カテゴリのデータ	• データセキュリティ
• データ主体に対する追加的な安全措置	• 例外と制限
• 制裁と救済	• さらなる保護

  - 2010年から同条約の見直し(Modernisation)に着手。2012年11月に同条約見直し案を諮問委員会が採択。今後、**2014年6月に改定予定**。
  - **CoE条約108号の批准は、EU指令/規則案において第三国が十分性決定を受ける際の判断材料となる**。欧州委員会がCoEに対して明言したとのことである。

「EUデータ保護規則案　第41条:十分性決定がなされた国への移転
第2項　保護のレベルの十分性は、欧州委員会によって、以下を考慮することで評価されるものとする。
(c)当の第三国(・・・)が行っている国際的なコミットメント」

  - この「国際的なコミットメント」が「主にCoE条約108号」を指す。モロッコはCoE非加盟国だが、EUから十分性決定を受けるために、条約108号への参加申請を行っている。

日本における個人情報保護制度見直しの要因



- 個人データを匿名化することで、保護法の「個人情報」に該当しないデータにしてしまえば、一般的に、事業者は保護法の義務（目的外利用の制限、第三者提供の制限）を免れると考えられている。
- 現状、このような観点からの「匿名化ガイドライン」は存在しない。

- 日本のデータ保護法制は国際的には「十分なレベルにない」と見られている。
- 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）

匿名化データと第三者提供に関する論点

- 下記の2つの大きな論点が存在（していた）

（1）連結可能匿名化（※1）されたデータを第三者に「提供」するに当たって、本人同意は必要なのか？

⇒ 「提供事業者基準説」 vs「受領者基準説」

（2）連結不可能匿名化（※2）されたデータであっても、提供先で再識別化されるリスクは残存するが、そのようなリスクにどう対処すべきなのか？

⇒ 際限ない「容易識別性」の拡大への対処

※1：匿名化を行った事業者等が対応表（本人と、新たに付された符号・番号との対応表）を保有する匿名化。≒「仮名化」。

※2：対応表を残さない匿名化。≒「無名化」。

※※匿名化に関しては、2013年12月にパーソナルデータに関する検討会の技術検討WGから、「識別非特定情報」と「非識別非特定情報」という新たな区分も示されている。

【ご参考】匿名化データと第三者提供、本人同意の関係（現行指針等）

（1）連結可能匿名化データ（＝対応表あり）

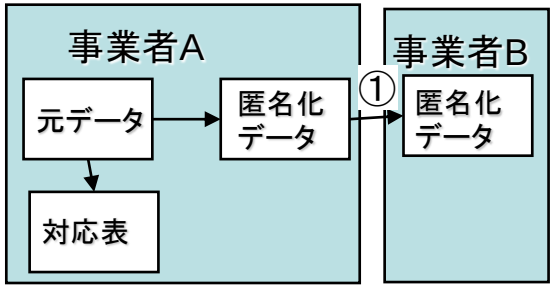
＝**事業者Aにおいては個人情報に該当**（事業者Bにおいては個人情報に該当しない）

・なぜなら、事業者Aにおいては**「容易照合性」**があるため

⇒**匿名化データの第三者提供①に当たって、本人同意が必要**

（いわゆる「提供事業者基準説」。経済産業省、消費者庁見解）

※ただし、研究機関間で臨床研究等の目的で提供する場合は同意不要（厚生労働省）



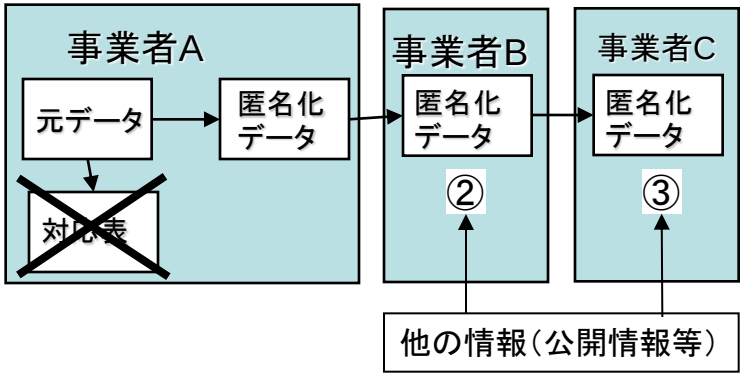
（2）連結不可能匿名化データ（＝対応表なし）

＝**事業者Aにおいても、個人情報に該当しない**

→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**

・ただし、**事業者B（②）や事業者C（③）において、他の情報と照合することで個人が識別できる可能性がある**（経済産業省、厚生労働省見解）

⇒**「安全に匿名化がされた状態」について、指針化を待つ**必要



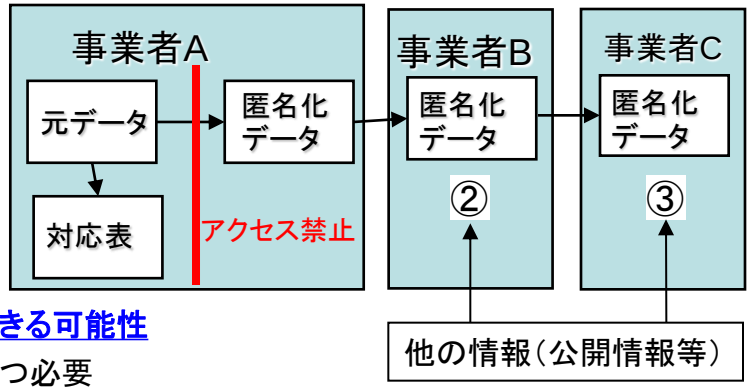
（3）事業者A内で元データと匿名化データの双方へのアクセスが厳格に禁止されている場合

＝**「容易照合性」がないので、匿名化データは個人情報には当たらない**

（経済産業分野ガイドラインQ&Aに依拠した場合）

⇒「連結不可能匿名化」と同じ扱いになり、**本人同意なく第三者提供可能**と考えられる。

⇒ただし、事業者Bや事業者Cにおいて**他の情報と照合することで個人が識別できる可能性がある**ため、（2）と同様、「安全に匿名化がされた状態」について、指針化を待つ必要



（出典：国際社会経済研究所）

「匿名化データ取扱いルール」の明確化

- 前々頁（P16）の論点への対処法として、以下の2つの方向が考えられる。
- ①**「容易照合性」の議論を棚上げし、仮に容易照合性があったとしても一定の制度的措置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する方向性**
  ⇒ 「個人が特定される可能性を低減したデータ」
- ②あくまで**「再識別化不可能化（又は十分困難化）」を目指す方向性**（非個人情報化）

①の場合、匿名化データの提供先は「信頼できる」特定の相手に限定される

- パーソナルデータ検討会では、**法改正により「日本版FTC 3条件」を導入**することが検討された。

日本版FTC 3条件
- 事業者が、適切な匿名化措置を行うこと
- 事業者が、匿名化したデータを再識別化しないことを約束・公表すること
- 事業者が、匿名化したデータを第三者に提供する場合は、提供先が再識別化をすることを契約で禁止すること

- 事業者が**この3条件を満たす場合**には、**匿名化データの第三者提供時の本人同意は不要**とする。

②の場合、匿名化データの不特定多数への提供が可能となる

- k-匿名化など匿名化技術によって再識別化が困難なレベルまで匿名化する。
- この場合、再識別化リスクが残存する問題に対処するために、**事業者自身によるリスク評価**（プライバシー影響評価の一環として）も含め、**事業者が取るべき「合理的な」匿名化措置のプロセスをガイドライン上で規定するべき**。

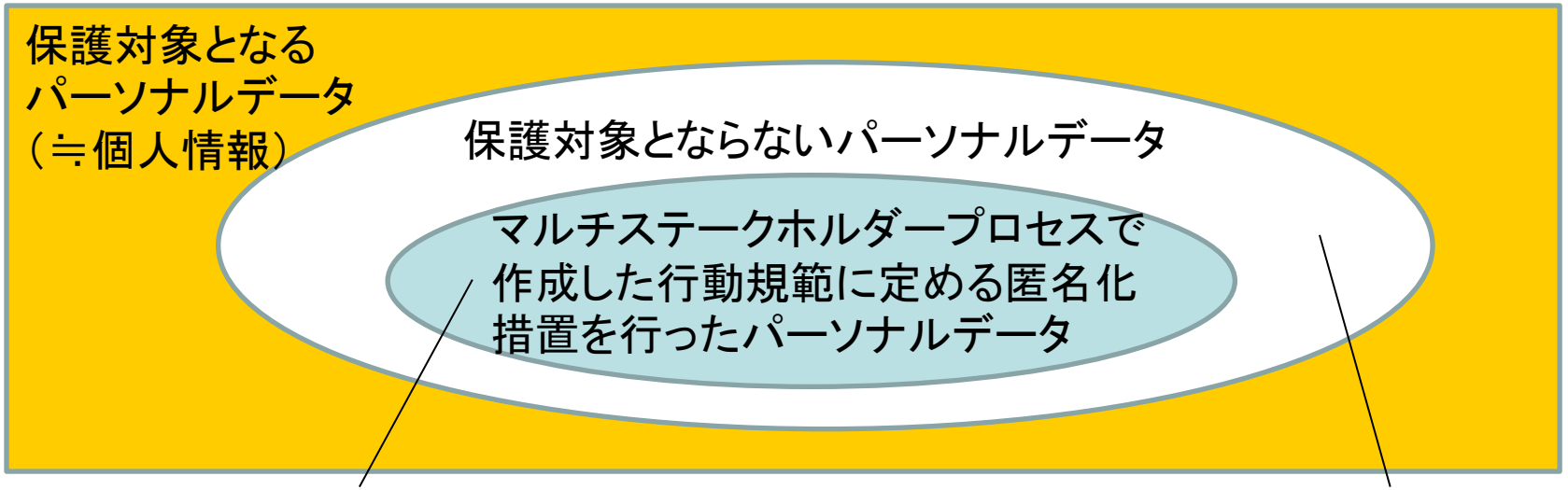
「合理的な匿名化措置」とは何か

- パーソナルデータ検討会技術検討WG報告書（2013年12月）での指摘
  - 「いかなる個人情報に対しても、識別非特定情報や非識別非特定情報に加工できる合理的な匿名水準を汎用的に達成可能な技術は存在しない。ケースバイケースで識別非特定情報や非識別非特定情報に加工することが必要である。」（p20）

- 「個人情報保護法等の見直しに関するJEITA意見書」（2013年10月）での意見
  - どこまで匿名化を行えばよいかはケースバイケースで判断せざるを得ない面が存在するため、**ガイドラインにおいて事業者が取るべき合理的な匿名化措置の「プロセス」を、リスク評価も含めて規定する**ことによって、事業者によるデータ保護に向けた積極的な取り組み（プライバシー・バイ・デザイン）を促すべきである。
    - 体制整備、教育、文書化、リスク評価（再識別化テスト等）、ポリシーでの説明、インシデント発生時の対応手順、プロセスの見直し等
  - **このリスク評価（PIA）は、基本的には事業者による自主評価である**が、我が国では何らかの機関による「お墨付き」を通じて法的な不確実性の排除を求める風土があるため、**リスク評価に関する第三者認証制度**についても併せて検討すべきと考える。

「匿名化ガイドライン」は誰が作るのか

- 一義的には「第三者機関」の役割だが、一案として、事業者が自主的に行っているパーソナルデータ保護の取組みを活かすためにも「マルチステークホルダープロセス」を活用すべき。
  （1）ガイドライン（行動規範）は、マルチステークホルダープロセスで策定する。
  （2）法律よりもやや厳しいルール（行動規範）を策定する（PIAの実施等を含む）。
  （3）事業者はそれを守ることで、直接的な法執行を受けない等のインセンティブを受けられるような建て付けとする（「執行セーフハーバー」）。
  （4）行動規範を遵守していることは、FTC法第5条的な法律がない日本では、第三者認証によって担保する。



※左図はP18の②の場合の措置を表すが、①の場合も別途考えられる。

匿名化措置を必要とする企業は行動規範を守らないといけないが、第三者機関の法執行を一定条件で免れる。

匿名化措置を必要としない企業は行動規範を守らなくてよい。