個人情報保護の国内外動向と日本企業から見た課題

2015年1月28日, 2月3日

国際社会経済研究所
小泉　雄介
y-koizumi@pd.jp.nec.com

１．個人情報保護の国際動向

２．個人情報保護の国内動向

３．日本企業から見た課題と今後の見通し

全世界的なデータ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** ・2014年3月　EU規則案欧州議会修正案の採択（理事会は未決）
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** ・**2012年3月　FTCのプライバシー・フレームワーク　公表**
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への参加が認められる
日本	・2003年　個人情報保護法 制定 ・2013年12月 「パーソナルデータの利活用に関する制度見直し方針」 ・**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」**

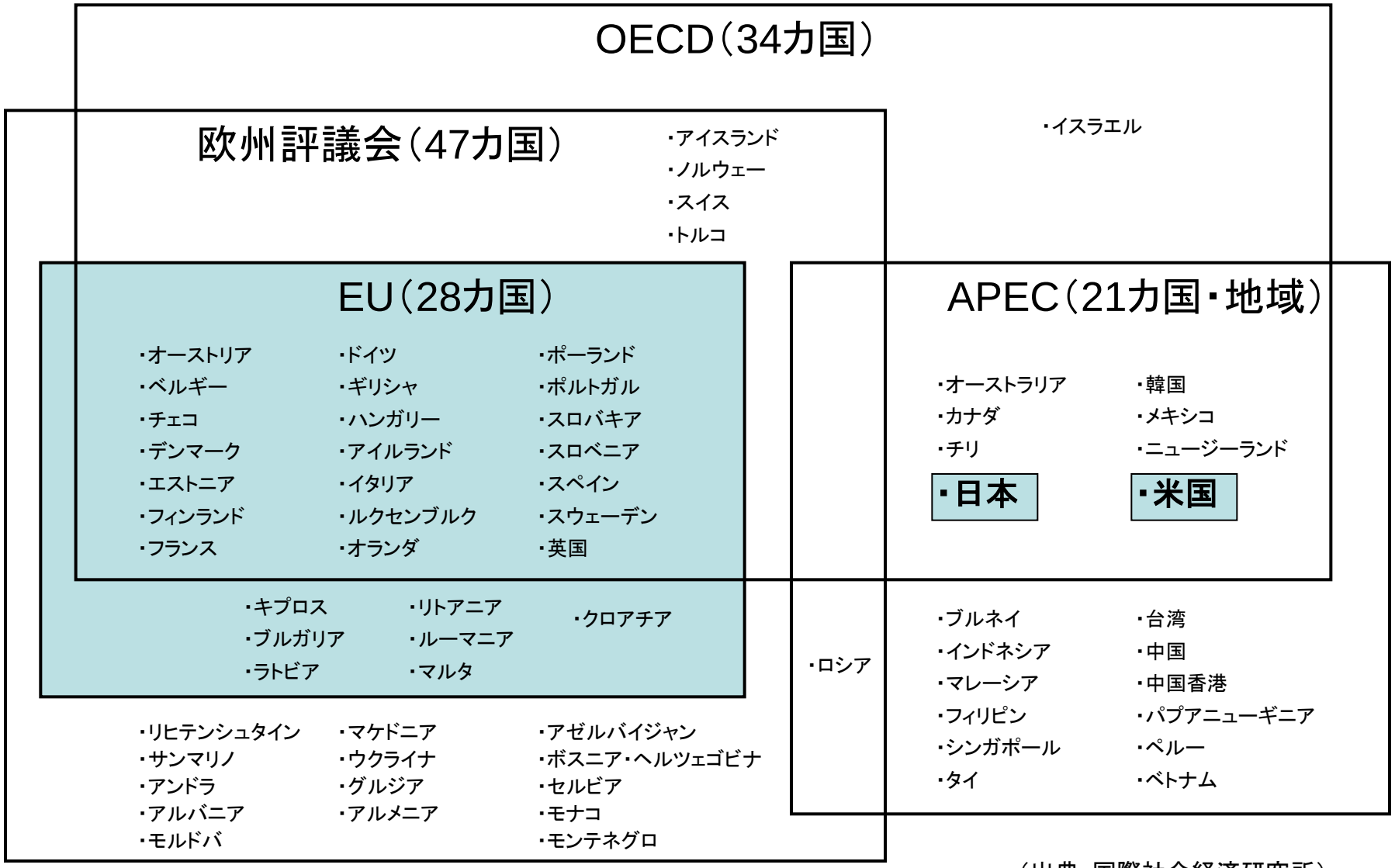
「忘れられる権利」など

Do Not Track など

FTC 3条件など

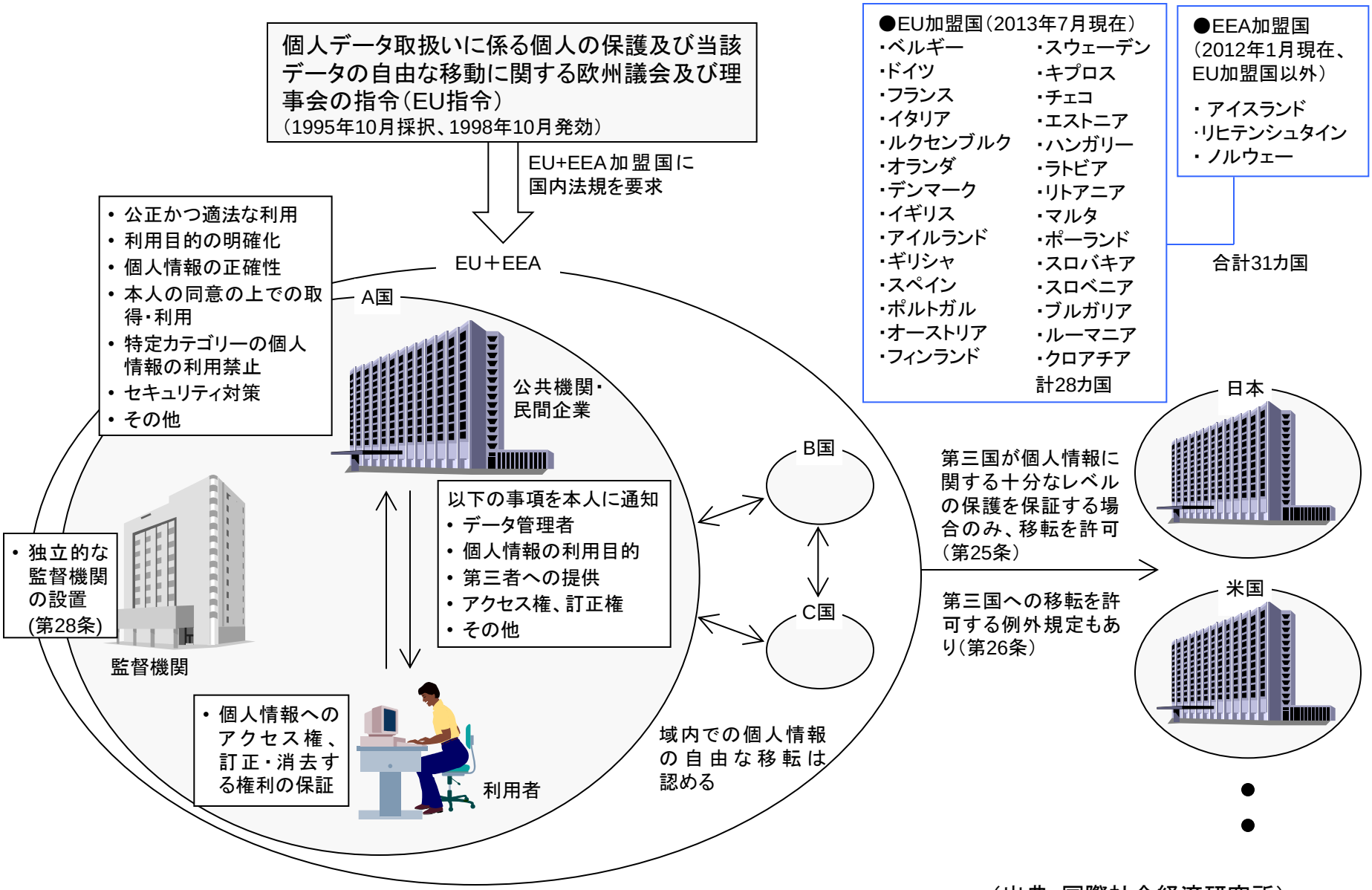
（出典：国際社会経済研究所）

各国際機関・統合体の加盟国　～日本の位置づけ～



（出典：国際社会経済研究所）

EU： EUデータ保護指令の概要



（出典：国際社会経済研究所）

EU： 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**。

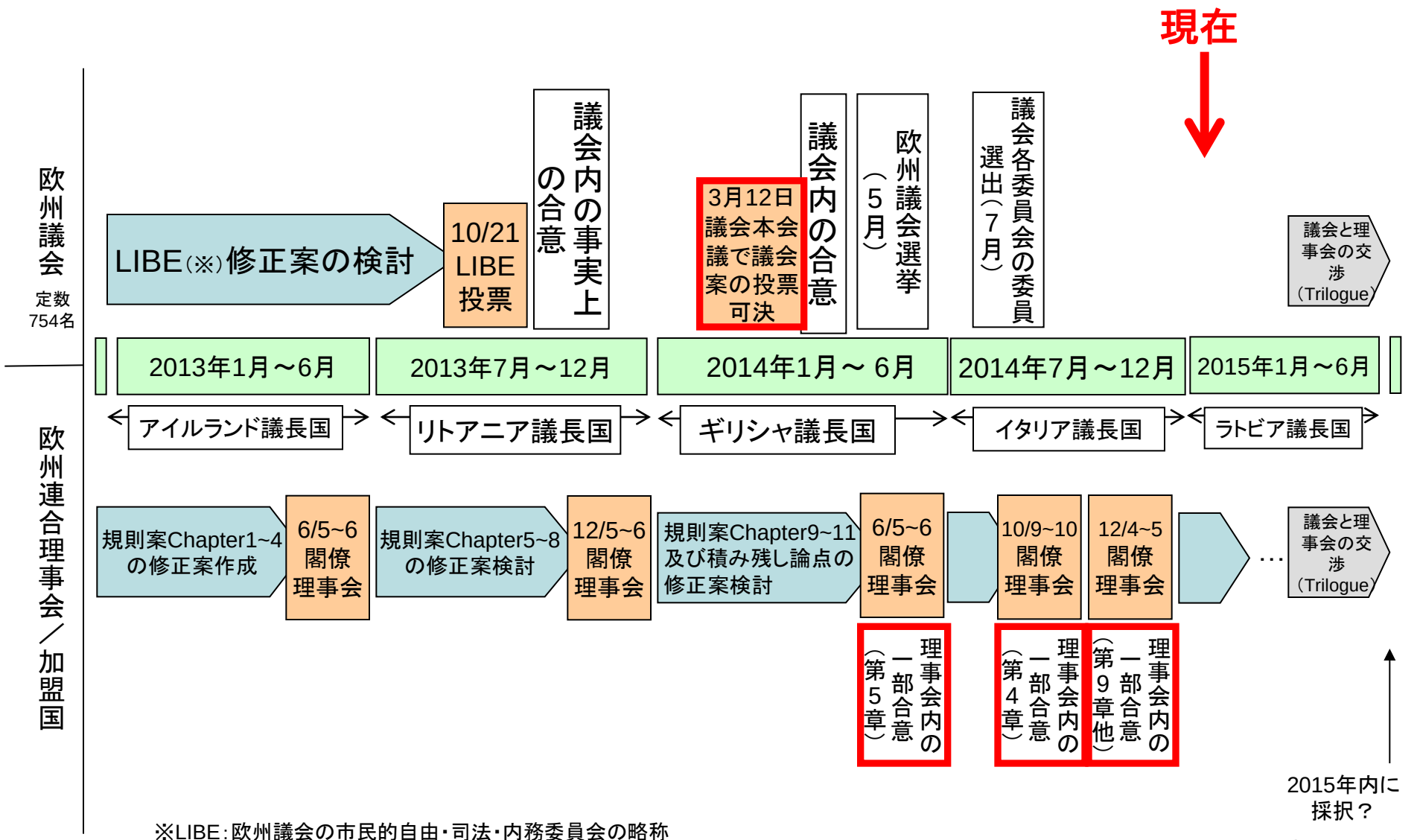
〇米国：
  - 全世界から個人データを収集する米国の多国籍企業（「データの蛸」）。ex. Google, Facebook
  - PATRIOT法により、令状無しに米国企業の国外現地法人からもデータ収集できる米国政府。

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

（出典：国際社会経済研究所）

EU： 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： EUデータ保護規則案（2012年1月）の全体構成

- 第1章　一般的条項（第1条～第4条）
- 第2章　諸原則（第5条～第10条）
- 第3章　データ主体の権利
  - 第1節　透明性とモダリティ（第11条～第13条）
  - 第2節　情報提供と、データへのアクセス（第14条～第15条）
  - 第3節　訂正と消去（第16条～第18条）
  - 第4節　異議申し立ての権利、プロファイリング（第19条～第20条）
  - 第5節　制限（第21条）
- 第4章　管理者と処理者
  - 第1節　一般的義務（第22条～第29条）
  - 第2節　データセキュリティ（第30条～第32条）
  - 第3節　データ保護評価と事前オーソライズ（第33条～第34条）
  - 第4節　データ保護オフィサー（第35条～第37条）
  - 第5節　行動規範と認証（第38条～第39条）
- 第5章　個人データの第三国又は国際組織への移転（第40条～第45条）
- 第6章　独立の監督機関
  - 第1節　独立的な地位（第46条～第50条）
  - 第2節　義務と権限（第51条～第54条）
- 第7章　協力と整合性
  - 第1節　協力（第55条～第56条）
  - 第2節　整合性（第57条～第63条）
  - 第3節　欧州データ保護評議会（第64条～第72条）
- 第8章　救済、責任及び制裁（第73条～第79条）
- 第9章　特定のデータ処理状況に関する条項（第80条～第85条）
- 第10章　委任法令と実施法令（第86条～第87条）
- 第11章　最終条項（第88条～第91条）

EU： 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（規則案）

規制強化

・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、違反時の通知義務や罰則等々）

・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）

規制緩和

・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

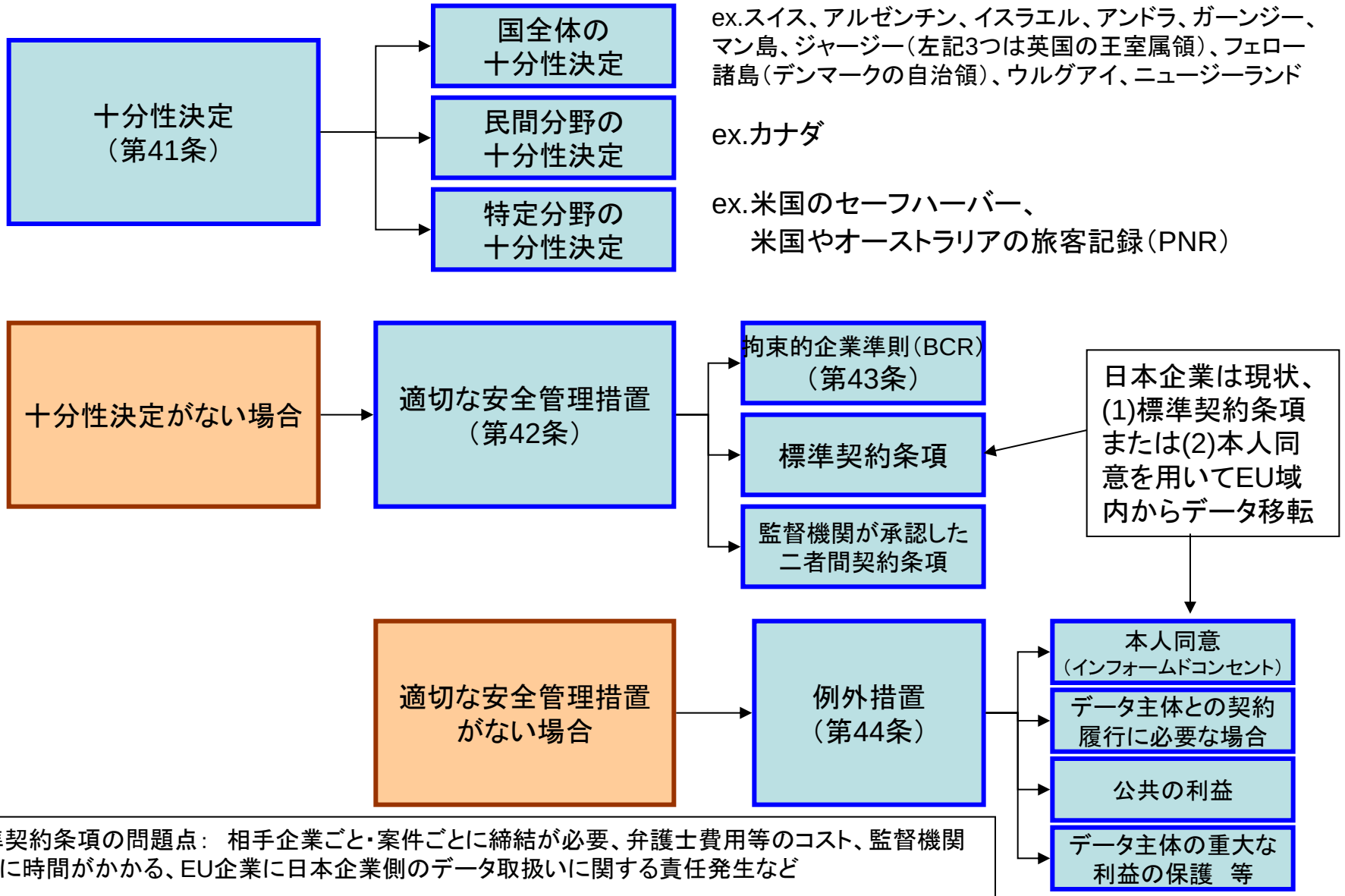
・EU域内事業拠点を含め、強化規則対応のための多大な負荷

＜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： 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）

EU： 第三国へのデータ移転方法

【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。（2011年7月時点で2716社（Not Currentを含む））

  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、

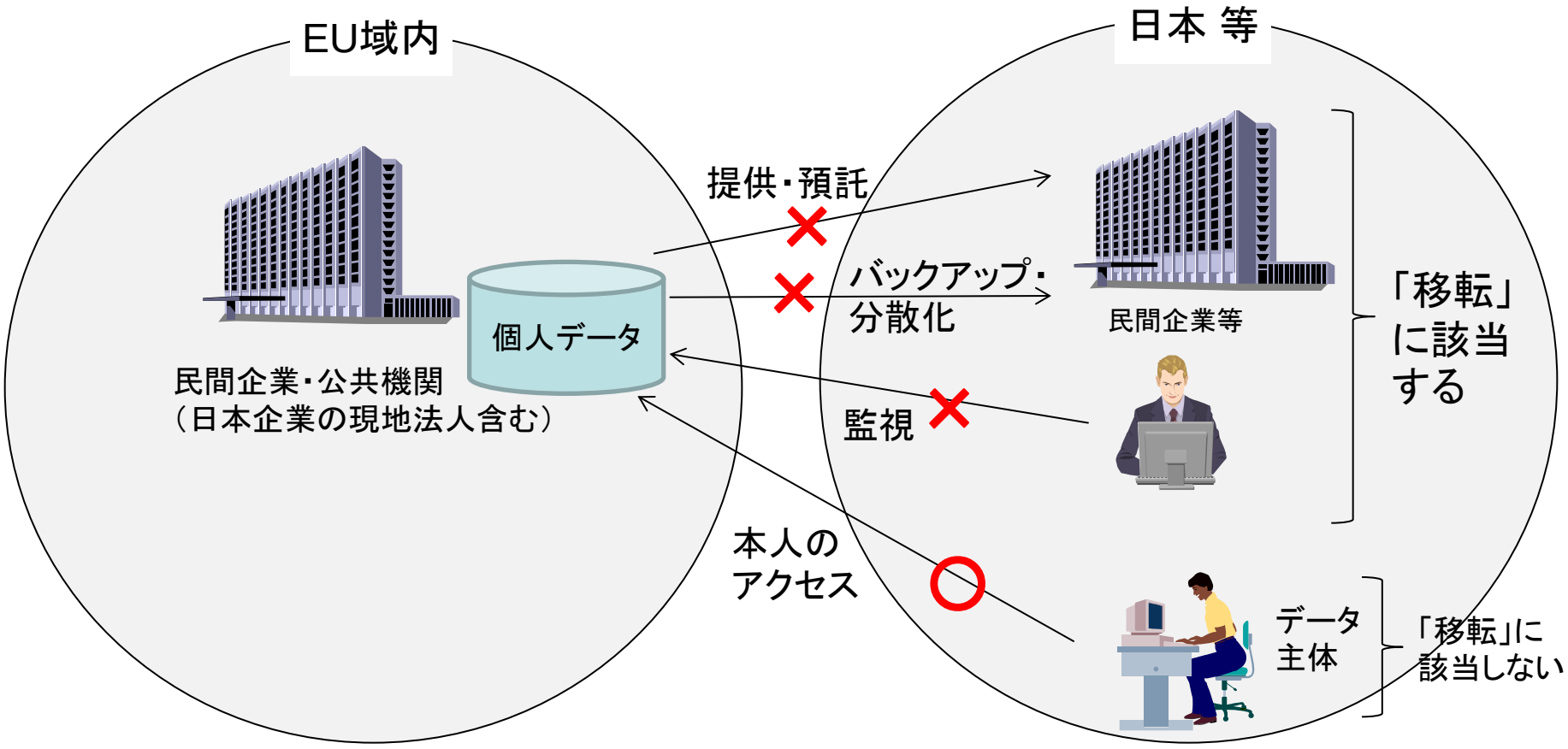
- 拘束的企業準則（Binding Corporate Rules：BCR）（第26条第2項）：

  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（モデル契約条項）（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： 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。

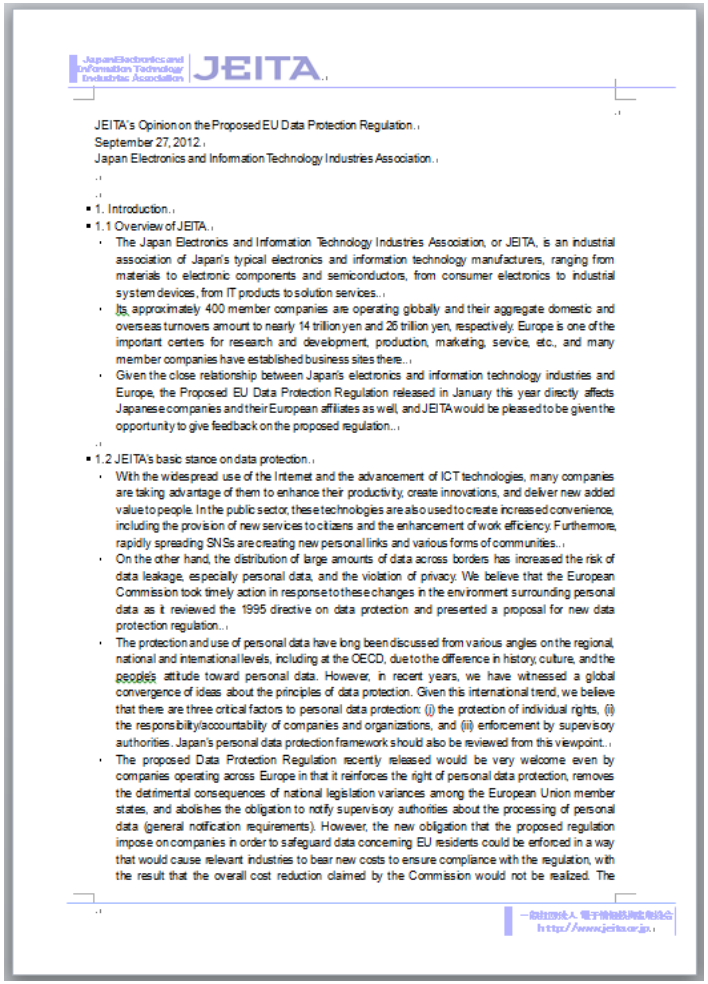


（出典：国際社会経済研究所）

EU： EU規則案に対するJEITA意見書(1/2)

〇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
- 個人データ漏洩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'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

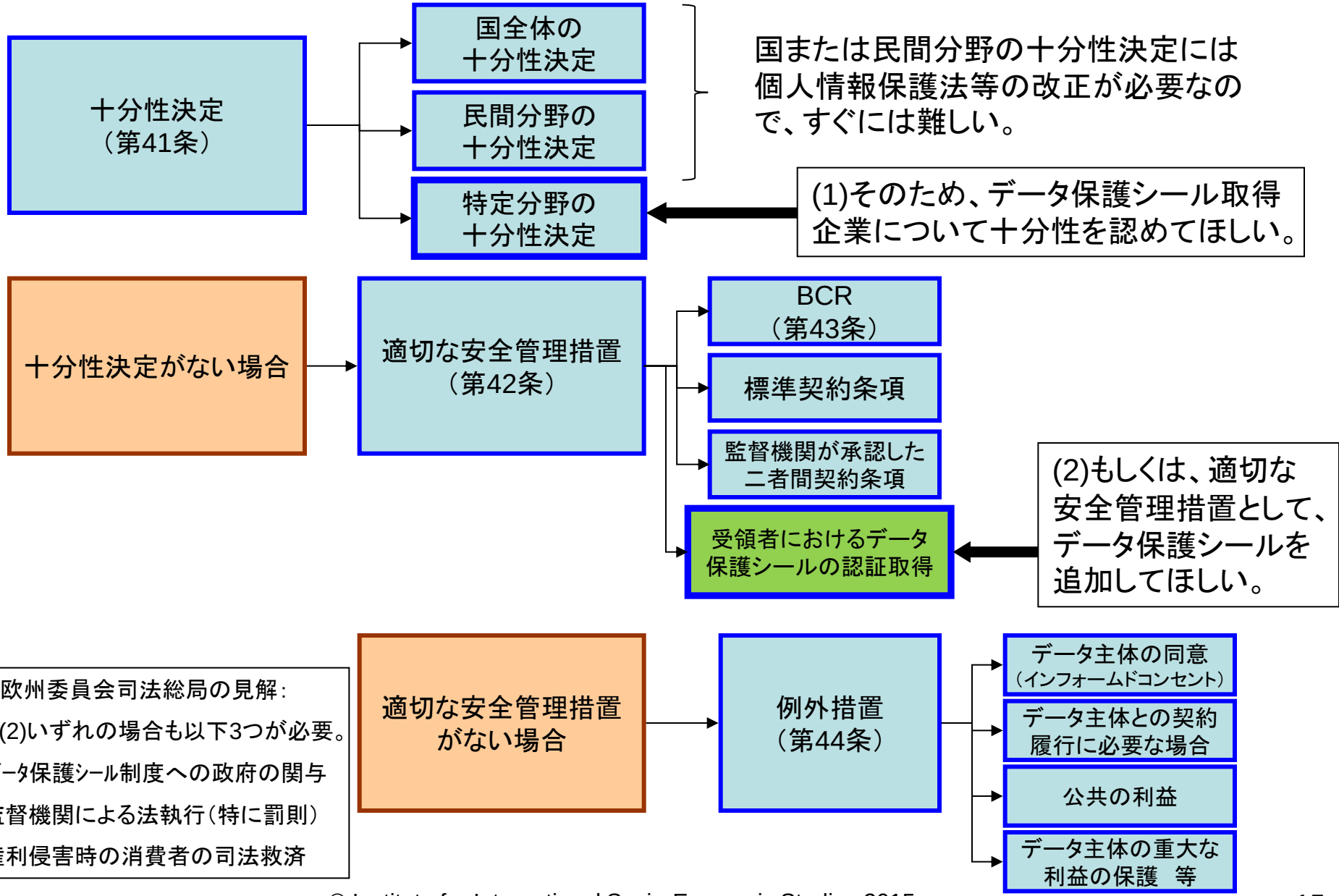
EU： EU規則案に対するJEITA意見書（2/2）

- 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。）

EU： 第三国移転へのシール制度活用（JEITA意見書より）



EU： 欧州議会および欧州連合理事会修正案における受容

- 欧州議会採択案（2014年3月）、欧州連合理事会修正案（2014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、BCRや標準契約条項と同列で、「データ保護シール」が追加された。

→ 欧州議会採択案：

– 「有効な欧州データ保護シール（EU域内の管理者および第三国の受領者におけるもの）」

→ 欧州連合理事会修正案：

– 「認証メカニズム／データ保護シール（第三国の受領者におけるもの）」および「行動規範（第三国の受領者におけるもの）」

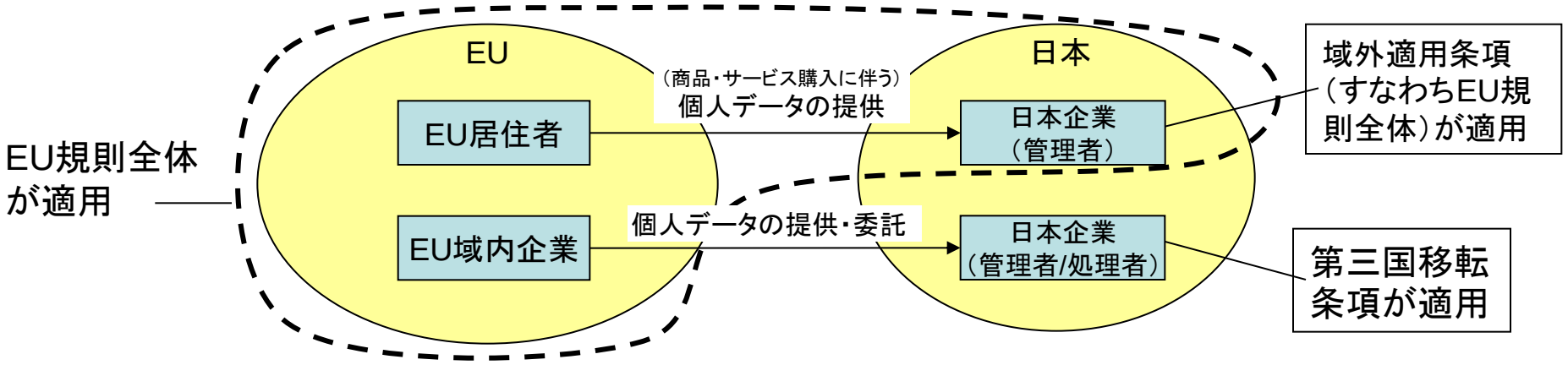
EU： EU規則案第3条2項（域外適用）

● 現行の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。

● EU規則案での改定内容

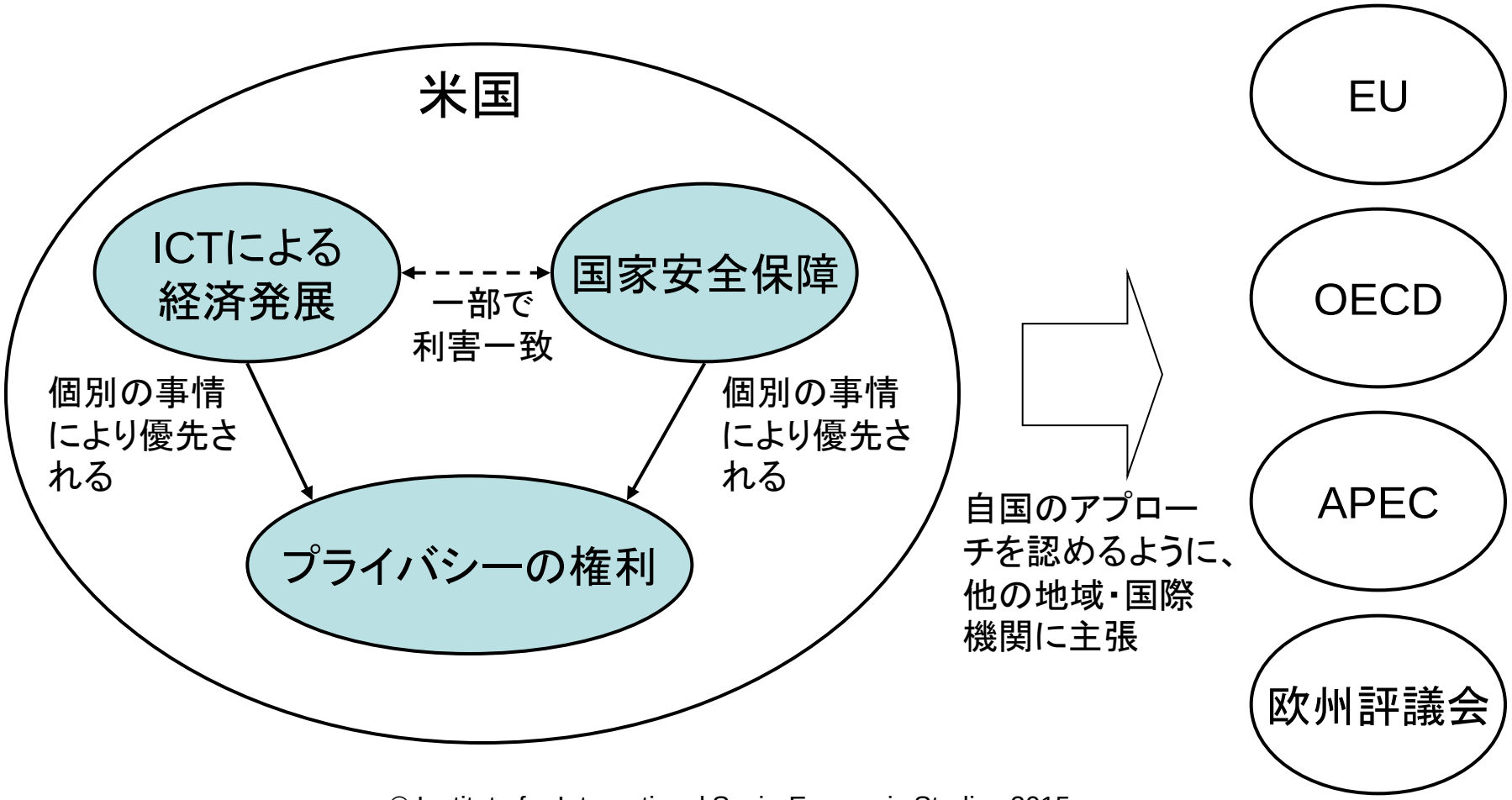
- **<u>EU域外企業であっても、以下の場合、EU居住者のデータを取扱う管理者に対してはEU規則が適用される</u>**（第3条第2項）。
  - ① EU居住者に商品やサービスを提供している場合
  - ② EU居住者の個人の行動をモニターしている場合
- 具体的には、オンラインサービス事業者、パーソナルクラウド事業者、オンライン広告事業者、スマートフォンアプリ事業者等が対象になりうる。



（出典：国際社会経済研究所）

米国： プライバシーの基本的な考え方（仮説）

- プライバシー／データ保護に対する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。）



米国： プライバシー・フレームワーク（1/2）

- 従来のフレームワーク
  - 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。

米国： プライバシー・フレームワーク（2/2）

- 近年の動向

①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。通称ホワイトペーパー。
- 商務省のドラフト報告書（グリーンペーパー： 2010年12月）がベース。
- **「消費者プライバシー権利章典」7原則**を含む。
  - 内容的には米国のFIPPs（公正な情報取扱い8原則。OECDの8原則とほぼ同じ）を現代風にアレンジしたもの。
  - **民間分野に対する「原則」を規定しているが、細かい「ルール」までは規定していない**。
    - **原則（権利章典）については立法勧告**を行っている。
    - **ルールについては各関係者で集まって業界ごとの行動規範**を作り（マルチ・ステークホルダー・プロセス）、自主規制を行う。
  - EUデータ保護規則案とは「原則」は共通する部分も多いが、**「ルール」が法規制なのか、自主規制なのかの面で異なる**。ただし、ルールに対する「法執行」は、米国の方が厳しいとも言われている。

②FTC「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。FTCのドラフト報告書（2010年12月）がベース。
- **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。

米国： 消費者プライバシー権利章典

1. 個人のコントロール

   消費者は、企業が自分からどのような個人データを収集し、どのようにそれを利用するかについてコントロールを行使する権利を有する。

2. 透明性

   消費者は、プライバシー及びセキュリティ・プラクティスに関して容易に理解でき、アクセスできる情報の提供を受ける権利を有する。

3. コンテキストの尊重

   消費者は、自分が個人データを提供したコンテキストと整合的な仕方で、企業がデータを収集し、利用し、提供することを期待する権利を有する。

4. セキュリティ

   消費者は、個人データのセキュアかつ責任ある取扱いを受ける権利を有する。

5. アクセスと正確性

   消費者は、使用可能なフォーマットで、またデータのセンシティビティ、及びデータが不正確であった場合に消費者が負の影響を受けるリスクに適合した仕方で、個人データにアクセスし、修正する権利を有する。

6. 焦点を絞った収集

   消費者は、企業が収集及び保持する個人データに合理的な制限を設ける権利を有する。

7. 責任（Accountability）

   消費者は、企業が消費者プライバシー権利章典への遵守を保証するための適切な措置を伴って、それらの企業による個人データの取扱いを受ける権利を有する。

米国： ビッグデータ報告書

- 大統領行政府「Big Data: Seizing Opportunities, Preserving Values」（2014年5月）
  - オバマ大統領から2014年1月に依頼を受け、ポデスタ大統領顧問が商務省、エネルギー省等の協力のもと作成。
  - ビッグデータ技術が経済・社会・政府活動に及ぼす影響に関する包括的なレビュー。
- ビッグデータは経済成長等に寄与する一方で、「プライバシー」と「社会的差別」という2つの問題をもたらしうると指摘。
- 以下6点を勧告。

①消費者プライバシー権利章典を前進させること

- 商務省は、ビッグデータの開発と、それが消費者プライバシー権利章典に与える影響について、関係者や市民からのパブコメを求める適切な諮問手続きを取るべきである。そして、関係者の検討用に、また大統領から議会に提出するために、法案ドラフトを作成するべきである。

②全米的なデータ違反基準を定めた法案を通過させること

③プライバシー保護を非米国市民にも拡大すること

④学校で収集された生徒のデータは教育目的のみで利用されることを保証すること

⑤ビッグデータ分析による差別を防止するための技術的専門知識を拡大すること

⑥電子通信プライバシー法（ECPA）を修正すること

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の存在が発覚して以来、米欧セーフハーバー・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。
  - 「米国の大規模な監視プログラムは、セーフハーバーの下で移転されるデータが、セーフハーバー原則の例外事項として規定された国家安全保障上の厳格な必要性や適切性を超えて、米国政府機関によってアクセスされ利用される結果をもたらしかねない」と指摘。
  - 13の勧告を提示。そのうち、「米国政府機関によるアクセス」に関する勧告は以下。
    12. 自己認証をした企業のプライバシーポリシーには、セーフハーバーの下で移転されたデータについて、政府機関が米国法の下で収集したり利用できる範囲についての情報を掲載するべきである。とりわけ、企業はプライバシーポリシーにおいて、どのような場合に国家安全保障や公共の利益、法執行上の要件を満たしてセーフハーバー原則の例外が適用されるのかを明示するようにすべきである。
    13. セーフハーバーで想定されている国家安全保障上の例外は、厳格に必要な又は適切な範囲でのみ適用されることが重要である。
  - 同日発行の他のコミュニケーションにおいて、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。
- 2014年6月、欧州委員会副委員長（当時）のReding氏は13の勧告のうち12個について米国はポジティブな対応をしてきたが、13番目の（米国政府によるアクセスに関する）勧告への対応は不十分と発言。
- 2014年12月現在、欧州委員会がセーフハーバーの見直しプロセス中。

OECD： プライバシーガイドライン見直し

- OECDプライバシーガイドライン（1980年採択）
  - 有名な**プライバシー8原則**を含む。日本の個人情報保護法の基盤ともなっている。

• 収集制限の原則	• データ内容の原則
• 目的明確化の原則	• 利用制限の原則
• セキュリティ保護措置の原則	• 公開の原則
• 個人参加の原則	• 責任の原則

  - ソウル閣僚宣言（2008年）において、「技術、市場、利用者行動の変化と、デジタル・アイデンティティの重要性の拡大の観点」から、**ガイドラインの見直し**が要求された。
  - OECDガイドラインは人権保護よりも**経済発展を目的**としているのが大きな特徴。
- OECDプライバシーガイドライン改定版
  - OECD情報セキュリティ・プライバシー作業部会（WPISP）において見直しを実施し、**2013年7月のOECD理事会で改定版を正式採択**。
  - **8原則自体は変更せず、**ガイドラインに**以下の項目を追加**。
    - **データ管理者の義務**:
      - 企業による**プライバシー・マネジメント・プログラム**の導入
      - セキュリティ違反時の通知
    - **加盟国の義務**:
      - 十分な権限を持った**プライバシー執行機関（DPA）**の設置
      - 国家プライバシー戦略の開発
      - 教育と普及啓発の実施
      - データ管理者以外のアクター（個人等）の役割の考慮
      - **国際的取り決めの開発の促進**（ex. 米欧Safe Harbor, EUのBCR, CBPR, CoE条約108号）
      - 国際比較可能な統計手段の開発の促進

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1月28日、各加盟国の署名に付された。
  - 2014年12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

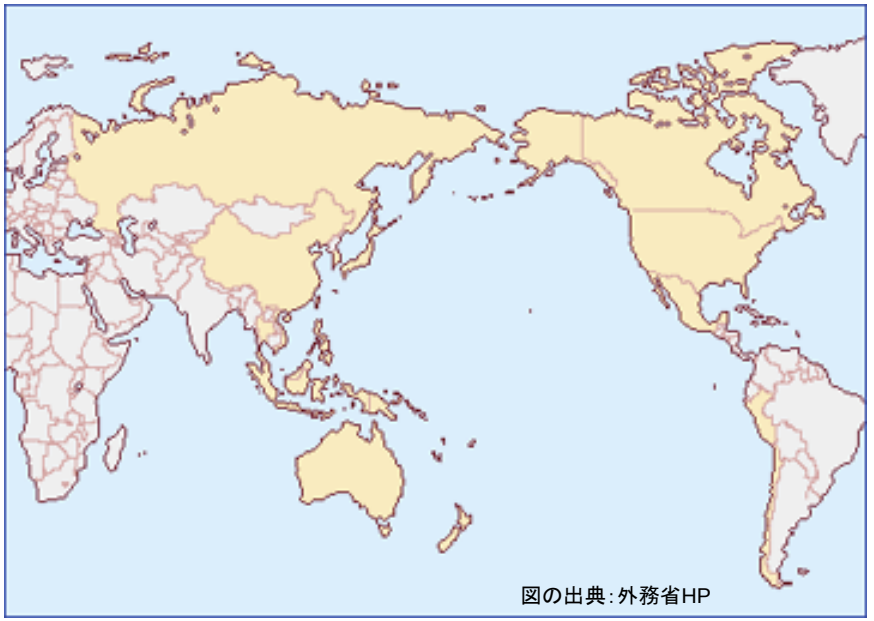
  - 2010年から同条約の見直し(Modernisation)に着手。**2014年12月にデータ保護アドホック委員会が見直し案を承認**。今後、閣僚委員会で審議および採択予定。
  - **CoE条約108号の批准は、EU指令/規則案において第三国が十分性決定を受ける際の判断材料となる**。欧州委員会がCoEに対して明言したとのことである。

「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。

APEC： 越境プライバシールール（CBPR）

- 越境プライバシールール（CBPR）
  - **APEC内で、企業・組織が国境を越えて個人データを移転するためのルール**。
  - 2013年6月に日本が参加申請し、2014年4月に承認（米国、メキシコに続き3カ国目）。
  - 検討経緯
    - 2006年からAPECのECSG（電子商取引運営グループ）において検討を開始。2007年に閣僚会合の承認によって設置された「APECデータプライバシー・パスファインダー」において、開発が進められた。
    - **2011年11月**のAPEC閣僚会合及び首脳会議において取りまとめられ、公表された。



  - **企業の越境個人データに係るプライバシーポリシーとプライバシー・プラクティスに対して、APECが認定した各国の責任団体（Accountability Agent：AA）が第三者認証を行う**。
    - 責任団体（AA）は公的機関でも民間団体でも良い。
  - **ポリシーに対するコミットメントに違反した企業に対しては、各国のプライバシー執行機関（いわゆるDPA）が法執行を行う**。このプライバシー執行機関はCBPRの要件と整合的な国内法令の下で法執行を行う能力が必要。また、参加国のプライバシー執行機関の少なくとも1つは、下記のCPEAに参加していることが必要。
- 越境プライバシー執行のための協力取決め（CPEA）（2010年発効）
  - APEC内で、各国のプライバシー執行機関のネットワークを通じて、プライバシー法令の国境を越えた執行協力を行うための取決め。
  - これまで、オーストラリア、カナダ、中国香港、ニュージーランド、米国、日本の執行機関が参加。

シンガポール： 新たな個人データ保護法

- 略称PDPA。2012年10月に議会を通過。**2013年1月に制定**。
- 外国企業（日本企業含む）との関係では、下記2つがポイント。
  - 同法はシンガポール内でデータを収集、利用または開示する全ての企業に適用される。これにはシンガポール内でオペレートする外国企業も含まれる。
  - いわゆる「**第三国移転条項**」があり、要件を満たさない限り、国外へのデータ移転を禁止。

    「第26条：シンガポール外への個人データ移転

    企業が移転される個人データに対して**PDPAの下での保護と同等な保護の基準を提供する**ことを保証するという、PDPAに規定された要件を遵守する場合にのみ、当該企業はシンガポール外の国または領域に個人データを移転することができる。」
- 通信情報省規則（2014年7月2日施行）
  - **第三国移転の要件として、当該企業には法的拘束力のある義務**が求められている。法的拘束力のある義務として、以下が挙げられている。
    - 法律
    - 契約（受領者にPDPAと同等な保護基準を求めるもの）
    - 拘束的企業準則（BCR）
    - その他の法的拘束力のある文書
  - これらの法的拘束力のある義務に加えて、下記の条件を満たすことも求められている。
    - 第三国移転に対する本人同意
    - 当該企業と個人との契約履行に必要な場合　等
  - EUのような十分性決定の仕組みは（同規則では）示されていない。

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）
  - 「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; 救済的策でなく予防的
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

出典URL：http://privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-japanese.pdf

- EUデータ保護規則案、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. FTC報告書「（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。」

国際的潮流に見るパーソナルデータ保護の3つの要素

〇個人の権利

・アクセス請求権

・訂正請求権

・消去/利用停止請求権　等

〇企業・組織の責任

・プライバシー・バイ・デザイン

・プライバシー・バイ・デフォルト

・プライバシー影響評価

・安全管理措置

・データ保護オフィサー

・データ漏洩時の報告　等

〇法執行

・データ保護監督機関
（第三者機関）

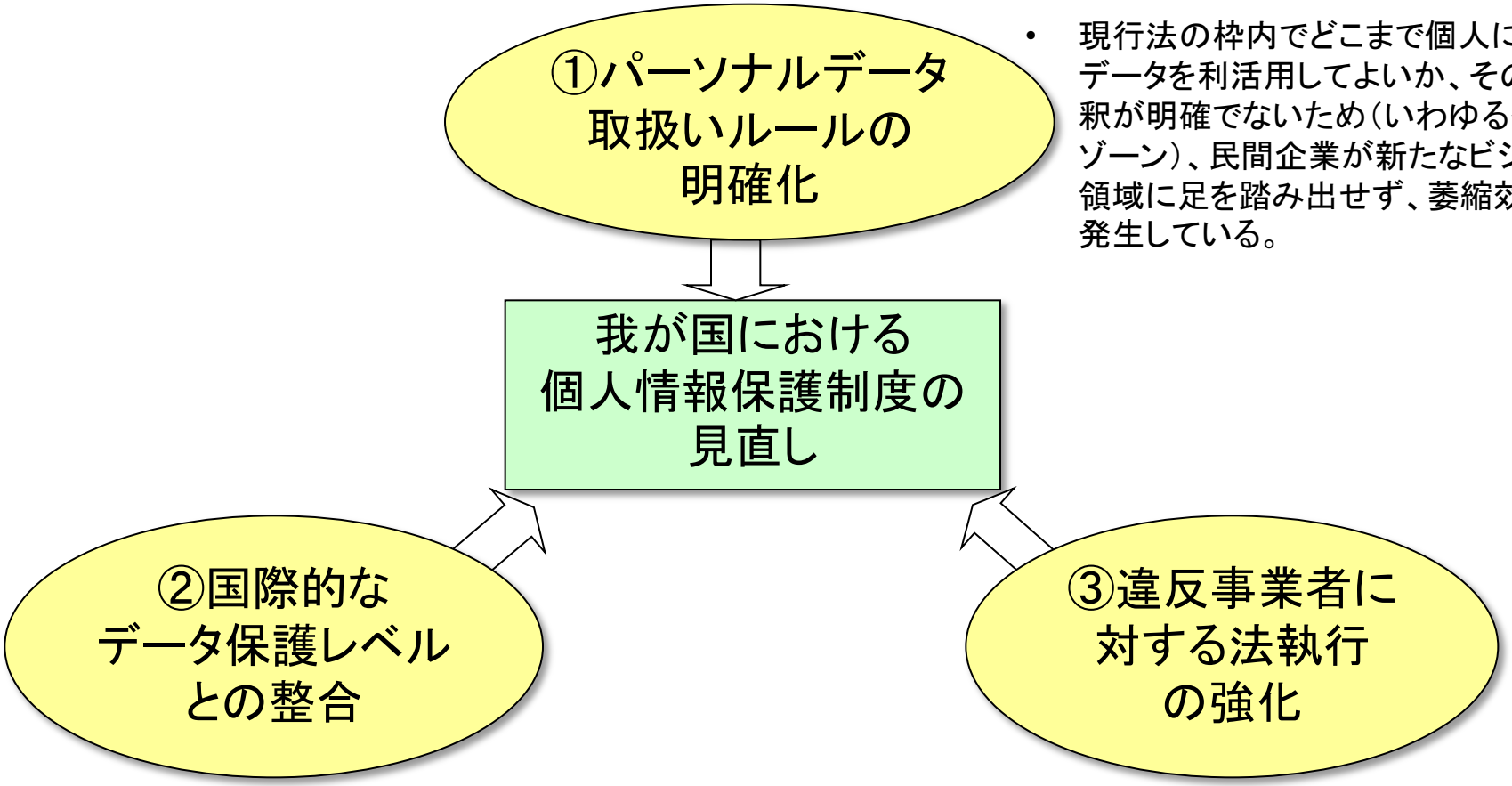
・罰則を含む制裁措置　等

1. 個人情報保護の国際動向

2. 個人情報保護の国内動向

3. 日本企業から見た課題と今後の見通し

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）

改正法案の骨子案(1/2)

○ 匿名加工情報(仮称)←(個人特定性低減データ)
- 匿名加工情報を作成する際には予め個人情報保護委員会への届出必要。
- 匿名加工基準は(自主規制ルールではなく)委員会規則で定める。
- 匿名加工情報を第三者提供する場合は、その旨を公表し、提供先に匿名加工情報であることを明示する。

○ 利用目的の制限の緩和
- 利用目的変更のオプトアウトは、取得時に「利用目的の変更がありうる」旨を通知又は公表することが必要。
- 利用目的変更時には委員会への届出が必要。
- 委員会は届出内容を公表、本人への通知や公表方法が不適切な場合は勧告・命令。

○ 要配慮個人情報(仮称)←(機微情報)
- 病歴も要配慮個人情報に含まれるが、医療機関における取扱いに配慮し、病歴については例外措置を設ける。

○ 第三者提供に係る確認及び記録
- 事業者は個人情報データベース等の提供を受ける時は、提供元が当該データベースを取得した経緯等を確認し、所定事項の記録を作成し、一定期間保存する。
- 事業者は個人情報データベース等を第三者提供した時は、所定事項の記録を作成し一定期間保存する。

改正法案の骨子案(2/2)

○ 個人情報データベース提供罪の新設

○ 第三者提供のオプトアウト

- 委員会への届出必要。
- 委員会は届出内容を公表、本人への通知や公表方法が不適切な場合は勧告・命令。

○ 開示等請求権

- 個人は、開示等請求に係る訴えを提起する前に、事業者に対して当該請求が必要。

○ 個人情報保護委員会

- 委員会は事業者に対する報告徴収・立入検査の権限を事業所管大臣等に委任可能。

○ 個人情報保護指針←(自主規制ルール)

- 認定個人情報保護団体が個人情報保護指針を作成する場合は、消費者代表者等の意見を聴くよう努め、委員会に届出が必要。
- 委員会は指針の変更等を命じることが可能。

○ 外国の第三者への個人データ提供

- 本人同意を得るか、委員会が「十分性」を認定するか、提供先事業者が一定要件を満たす保護体制を整備していることが必要。
- 上記3点目については、現行の各企業の適切な移転手続きが合法であることを明確化する。

1. 個人情報保護の国際動向

2. 個人情報保護の国内動向

3. 日本企業から見た課題と今後の見通し

日本企業から見た課題と今後の見通し

① 越境データ移転
- EU等の海外企業からのデータ移転
- 海外企業へのデータ移転　→現行の適切な移転は改正法でも合法

② ビッグデータと個人情報保護
- 骨子案では「利用目的変更のオプトアウト」を導入したが、保護レベルの国際的調和の観点からは難点あり

③ プロファイリングと社会的差別
- 「プロファイリング」は大綱では今後の検討課題とされている
- 米欧ではプロファイリング自体は許すが、個人の権利利益の侵害や社会的差別につながるものは許さないという考え方
- 「社会的差別」は大綱・骨子案において機微情報の関連で触れられているが、プロファイリングの結果として生じる差別については今後の課題

④ いわゆる名簿屋対策
- 改正法案骨子案では「業規制」ではなく、「行為規制」で対応
- 米国では「データブローカー」として、業規制が検討されているが、日本の感覚からすると緩やかな内容

⑤ 自主規制ルール
- 大綱における「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」の考え方が後退

ビッグデータと個人情報保護： EUおよび米国FTCの見解

- EU指令第29条作業部会の見解
  - 「ビッグデータの発展の個人データ保護への影響に関するステートメント」（WP221, 2014年9月16日）
  - EUデータ保護指令（95/46/EC）その他の関連EU法令は、ビッグデータ運用における個人データの処理にも適用される。
  - 関係者の中には、ビッグデータオペレーションにおける将来的な発展が実現されるように、EU法令の下の幾つかのデータ保護原則（特に目的制限の原則とデータ最小化の原則）は実質的に見直されるべきと主張する者もおり、個人データの利用が当該個人に害を与えるリスクのレベルの方に焦点を当てるべきと主張する者もいる。
    - 目的制限の原則：データ管理者は個人データを、特定され、明示的で、かつ正当な目的のみで収集しなくてはならず、それらの目的と不整合な仕方でデータを処理してはならない。
    - データ最小化の原則：個人データは、収集された目的や処理される目的との関係において、十分かつ適切でなければならず、過剰なものであってはならない。
  - しかし現状では、EUデータ保護の原則がビッグデータの発展において、もはや有効・適切でないと信じるいかなる理由もない。
- 米国FTCの見解
  - 「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）
  - 企業は、データが収集された時点とは実質的に異なる仕方で消費者データを利用する場合には、事前に肯定的で明示の同意を得なければならない。

ビッグデータと個人情報保護： 英国ICOの見解

- 英国ICO（データ保護監督機関）の見解
  - 「ビッグデータとデータ保護」（2014年7月28日）
  - ビッグデータは、異なるルールで行われるゲームではない。すなわち、英国のデータ保護法は、ビッグデータ分析における個人データ処理にも同様に適用される。
    - 透明性： 企業・組織は、データの収集の時点でデータの利用方法について説明する必要がある。企業・組織は消費者への通知内容を簡便な仕方（ex.動画等）で伝える革新的な方法を見出すべき。個人データではなくて匿名化データが使われているといったことも知らせるべき。
    - 目的制限： 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、当初の目的とは整合的でない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。当初目的と整合的であ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、すなわち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どうか、データの使われ方が個人の合理的な期待の範囲内であるかということである。
      - 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。
    - 匿名化： ICOはデータの匿名化を推奨する。匿名化を適切に行えば、データはもはや個人データとみなされず、データ保護の義務の対象外となりうる。しかし、ビッグデータ分析の文脈では、有効な匿名化には困難が伴いうるため、企業・組織は堅固なリスク評価を実施すべき。ICOの見解では、匿名化の要件は、再識別化のリスクを消滅させることではなく、再識別化のリスクが極めてありえないレベルまで軽減されたことを保証することである。技術的措置（データマスキング、仮名化、アグリゲーション、バンディング）や法的・組織的安全保護措置が考慮に入れられるべき。

プロファイリングと社会的差別

- プロファイリングとは
  - ある個人に関する多くのデータを（様々なデータソースから）集積し、これらのデータをアルゴリズムで分析することによって、個人を一定のカテゴリーにセグメント分けすること。
  - プロファイリングによって、当該個人の行動（購買活動・業務パフォーマンス等）を予測したり、既知でない属性（嗜好・返済能力・健康状態等）を推定したりすることが可能になる。
    - 米国ビッグデータ報告書ではカテゴリーの例として、以下を挙げている。
      - “Ethnic Second-City Strugglers” （人種上の第二都市住人）
      - “Retiring on Empty: Singles” （引きこもり：独身）
      - “Tough Start: Young Single Parents” （養育問題：子連れの片親）
      - “Credit Crunched: City Families” （信用危機：都市家族）
      - “Rural and Barely Making It” （地方でぎりぎりの生活）

        ※和訳出典：次世代パーソナルサービス推進コンソーシアム

  - プロファイリングに関与する企業
    - オンライン広告企業
    - データブローカー

プロファイリングと社会的差別

- ビッグデータ分析による（想定される）社会的差別の事例（米国ビッグデータ報告書、FTCデータブローカー報告書等より）
  - 人種的バイアス：黒人を示す名前（Jermaine等）を含むWeb検索は、白人を示す名前を含むWeb検索よりも、arrest（逮捕）という語を含む広告表示が多いという研究結果。
  - 価格差異化：幾つかの小売店では、同一商品を地域によって異なる価格で販売。所得水準が高い地域の住民に、所得水準が低い地域の住民よりも低価格で提供。
  - 融資差別：米国ではかつて「Redlining（赤線引き）」という、居住地域に基づく融資差別が存在。すなわち、アフリカ系アメリカ人やラティーノ、アジア人等が多く住む居住地域の住民に対し、住所のみで融資内容を決定するという差別である。これは1975年の住宅抵当貸付公開法で禁止されたが、ビッグデータ分析によって新たな「Redlining」が生じる恐れがある。
  - 例えば「家庭での喫煙者」というカテゴリーにセグメント分けされた人は、空気清浄器の広告対象となるのみならず、信用力が低い／保険リスクがあるとみなされたり、雇用や入試において不適切な候補者とみなされたりする恐れがある。
  - 店舗への来店時に、「購入する見込みのない消費者」とセグメント分けされた人は、他の消費者に比べて差別的な扱いを受ける恐れがある。
  - オンライン学習で収集された生徒の学習履歴データが、教育目的のみならず、後に消費者プロファイルの開発に使われたり、本人に不利益な決定に使われたりする恐れがある。

【ご参考】プロファイリングに対する規制：FTCデータブローカー報告書

- 2014年5月発行。“Data Brokers: A Call for Transparency and Accountability”
- 代表的なデータブローカー9社のデータ収集・利用に関する調査に基づく報告書。
  - Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, Recorded Future
- データブローカーに対する法規制を議会に勧告。（2012年3月FTC報告書でも勧告）
- データブローカーの概要
  - 消費者の個人情報を収集して、集積・分析し、第三者に販売・提供する企業。ビッグデータ経済における重要な参加者とされる。
  - 広範なデータソースから消費者の個人情報を収集。一般に消費者とは直接やり取りを行わないので、消費者はしばしばデータブローカーの存在自体に気が付いていない。
  - データブローカーの3類型

    （1）FCRA（公正信用報告法）の規制対象となる企業
    - 1970年制定のFCRAは消費者報告機関による信用、雇用、保険、住宅供給等の目的でのデータ提供を規制

    （2）FCRAの対象とならず、マーケティング目的でデータを保持する企業

    （3）FCRAの対象とならず、マーケティング以外の目的でデータを保持する企業
    - 詐欺の検出・身元確認（リスク軽減）、人物の検索等
- 現行法（FCRA）の対象とならない（2）と（3）の企業について、「A.マーケティング商品」「B.リスク軽減商品」「C.人物検索商品」という括りで分析。

【ご参考】プロファイリングに対する規制：FTCデータブローカー報告書

A.マーケティング商品を販売するデータブローカー（9社のうち5社が該当）

- 顧客企業は、例えば消費者の興味・関心についての情報を購入し、マーケティング（ex.オンライン広告）で利用可能。メールアドレスの購入も可能。
- 消費者データを分析した商品も販売。ある商品に関する広告媒体や出稿地域のサジェスト等。
- 2~3社は分析結果から消費者毎の「マーケティングスコア」を作成して、消費者をランク付け。
- 消費者による本人データへのアクセスは限定的。
  - 5社のうち2社のみが本人データの訂正可能。
  - 5社のうち4社はオプトアウト可能。
  - ただし消費者がこれらの権利について得られる情報は限定的で、中央化されたポータルは存在しない。

B.リスク軽減商品を販売するデータブローカー（9社のうち4社が該当）

- 顧客企業は、消費者の身元を確認したり、詐欺を検出できる。例えば、金融企業は口座開設申請者の実在性確認をしたり、社会保障番号が不正利用されていないことを確認できる。
- 消費者による本人データへのアクセスは限定的。
  - 4社のうち2社は本人データへのアクセス可能。
  - 4社のうち1社のみが訂正可能。

C.人物検索商品を販売するデータブローカー（9社のうち3社が該当）

- 人物検索サイト上で、様々な人物（取引先・顧客・友人・恋人等）の情報を入手できる。
- 消費者は同じサイト上で本人データにアクセス可能（無料又は有料）。データ公開のオプトアウト可能。訂正も或る程度可能。

【ご参考】プロファイリングに対する規制：FTCデータブローカー報告書

- 議会への法規制の勧告内容

A.マーケティング商品を販売するデータブローカーに対する法規制

(1) 消費者が本人データに容易にアクセスでき、オプトアウトの権利も行使できるようにすること。

(2) 生データ（氏名、住所、年齢、所得層等）のみならず推定データも利用していることを明確に開示すること。

(3) データソースの名称やカテゴリを開示すること。

(4) データソースとなる企業（消費者と直接的な取引のある企業）は、データブローカーへのデータ提供やオプトアウトについて、消費者に目立つ通知を与えること。

B.リスク軽減商品を販売するデータブローカーに対する法規制

(1) 金融企業等がリスク軽減商品を利用することで、取引相手の消費者が不利な影響を受ける場合には、当該金融企業等はデータブローカーを消費者に開示すること。

(2) データの正確性や安全性を担保しつつ、消費者によるアクセスや訂正を可能とすること。

C.人物検索商品を販売するデータブローカーに対する法規制

(1) 消費者が本人データにアクセスできるようにすること。

(2) 消費者が本人データの利用をオプトアウトできるようにすること。

(3) 消費者がデータソース上の本人データを訂正できるように、データソースを開示すること。

(4) オプトアウト後も同姓同名の検索結果が表示される可能性等、オプトアウトの制約事項を開示すること。

- データブローカーへのベストプラクティスの勧告

(1) 商品開発のあらゆる段階でプライバシーに配慮する、プライバシー・バイ・デザインを実施すべき。

(2) 特にマーケティング商品において、未成年者データの収集を避けるような措置を講じるべき。

(3) 顧客企業（データ利用者）が消費者データを資格決定（信用、雇用、保険、住宅購入等）や非合法な差別の目的で利用しないような合理的な予防措置を講じるべき。