グローバルなネットワークサービスと個人情報保護法上の課題

～欧州個人情報保護を中心として～

2014年10月26日

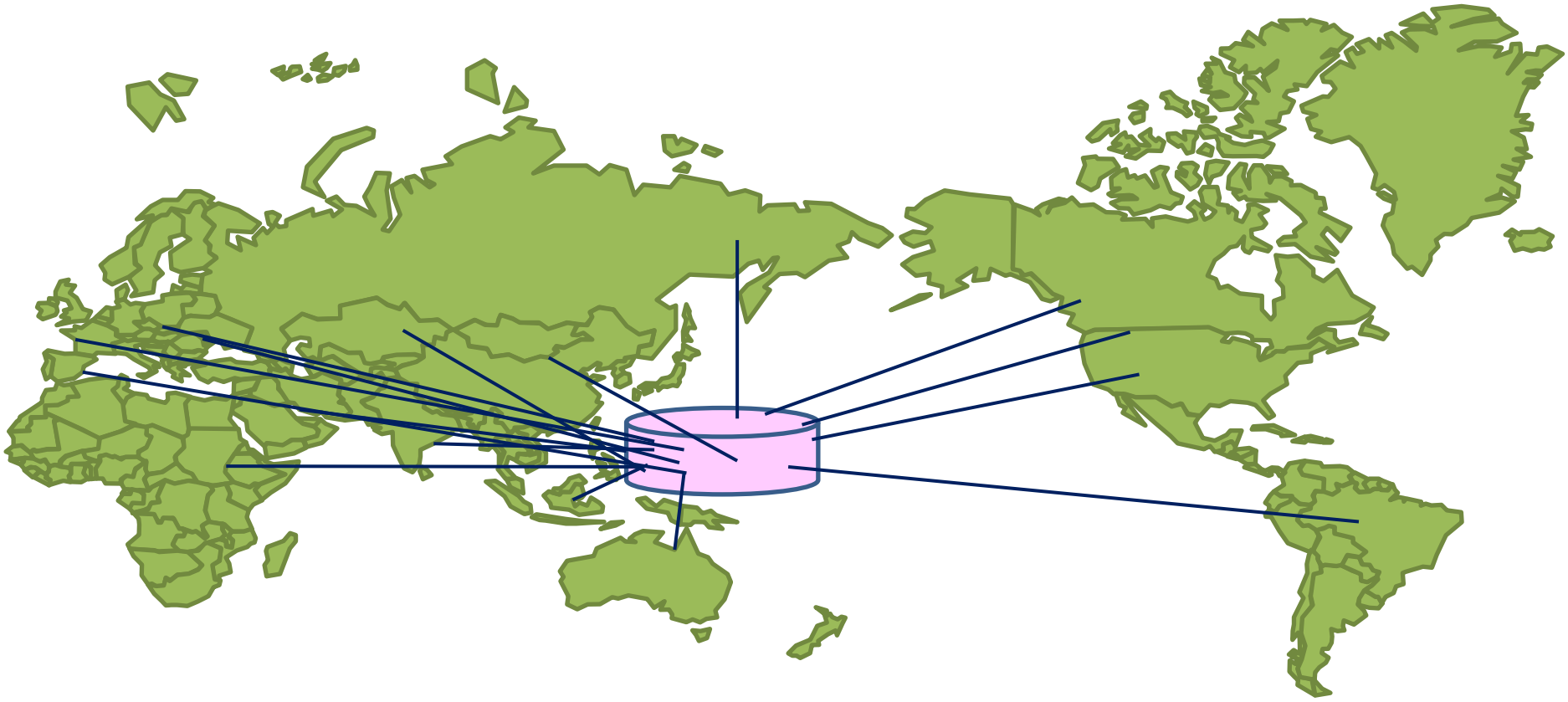
金子　啓子

目次

1. 背景

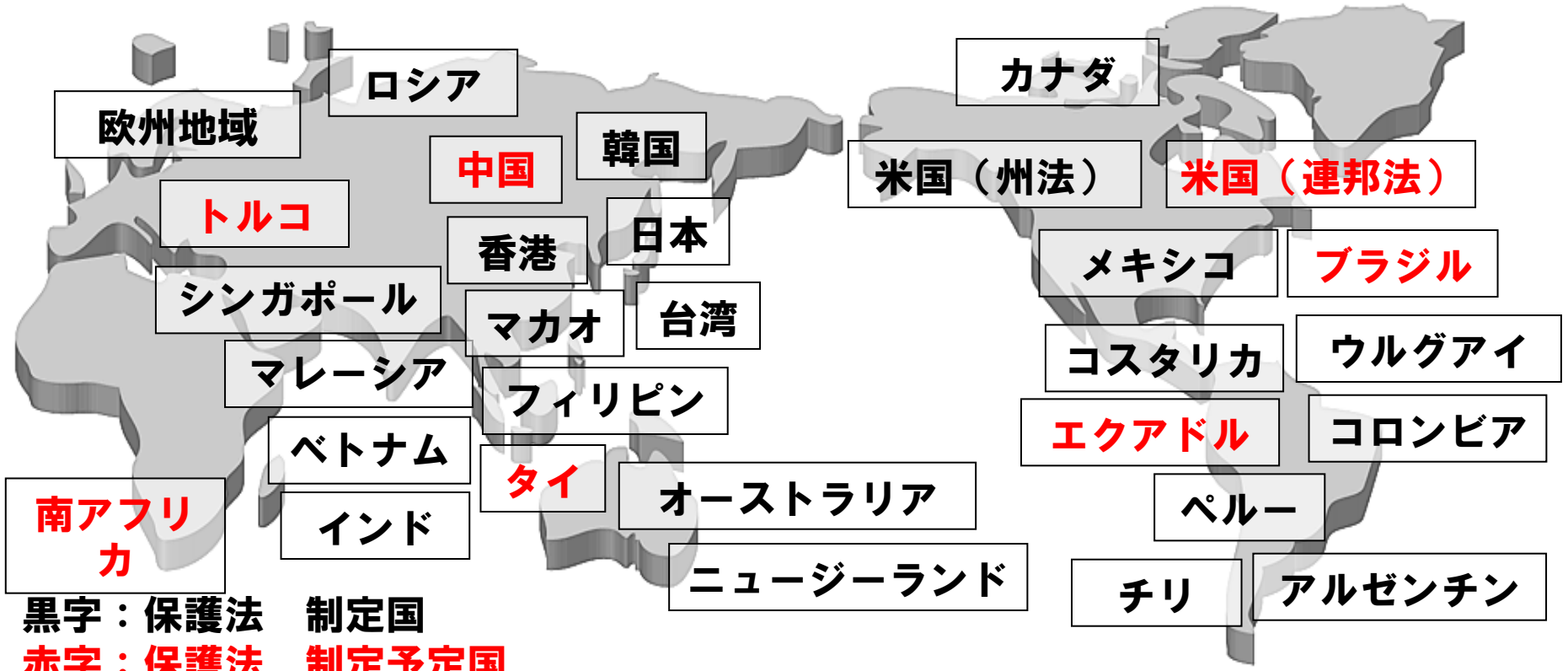
ｸﾞﾛｰﾊﾞﾙなｸﾗｳﾄﾞｻｰﾋﾞｽ

一元的なサービス提供、データ管理。（言語対応はあり）
　　例えば：Google，Apple，Facebook，・・・
サービスの均一化、事業の効率化のために、統一的対応を志向



各国の個人情報保護法令

- ネットワーク社会の進展に対応して、各国で個人情報保護法の制定・改定の動き
- 99カ国で個人情報保護法が制定されている。



黒字：保護法　制定国
赤字：保護法　制定予定国

どうするか

世界の個人情報保護法のモデルは・・・

- OECDプライバシーガイドライン （1981年）
- EU個人情報保護指令 （1995年）
  - 域外移転制限の相互主義が圧力に
  - 米国とのセーフハーバー協定で、同様の言明を求められる

欧州個人情報保護指令に適合したポリシーで高位平準化アプローチ

主要事業者の対応

	Google	Apple	Amazon	IBM	Samsung
日本語・英語（米国想定）	統一内容	ほぼ同一内容	ほぼ同一内容	統一内容	統一内容
UK（欧州）	英語 同一サイト	英語 同一サイト	別サイトだが、 ほぼ同一内容	統一内容	別サイトだが、 ほぼ同一内容

グローバル対応（推測）	統一内容	ぼぼ統一内容	ほぼ統一内容	統一内容	ほぼ統一内容

２．欧州個人情報保護法

欧州個人情報保護法の特徴

（1） EUレベルと各国のせめぎあい

- 指令→実際の適用は各国法
  - 28条　各国は、Supervisory Authority設置義務
    DPA(Data Protection Agent)
  - 29条　EUレベルのワーキングパーティーの設置
    - メンバー：各国のDPA/EUの機関/EC委員会　の各代表
    - 役割（30条）
      - 各国での統一的適用に向けて、各国法の適用にあたっての諸問題を調査
      - 委員会に、EU内と第三国の保護レベルに関する意見書
      - 委員会に、改正や保護手段の追加を提案
      - 委員会に、EUレベルでの行為規範についての意見書

欧州個人情報保護法の特徴

（2） 実質的義務より手続きに負担

指令　18条（概訳）

第1項　加盟国は、コントローラに、部分的にでも自動化された処理を行う前に、DPAに通知することを義務付けねばならない。

第4条第1項(c)　域外企業の代表者の登録

第26条　移転契約の登録

欧州個人情報保護法の特徴

（3） 域外移転制限と相互主義

指令　25条（概訳）

1．個人情報の第三国への移転（transfer)は、その国が十分な保護を保証する（ensure）場合に限る。

アンドレア、アルゼンチン、オーストラリア、カナダ、スイス、フェロー諸島、ガンジー島、イスラエル、マン島、ジャージ島、ニュージーランド、ウルグアイ。
（2014年5月　現在　12か国）

背景：米国との立場の違い

2.1 概要

「コントローラ」「取扱い」概念

- コントローラ:
  個人情報の利用目的と取扱手段（means of the processing ）を決める者 （EU指令　第2条（d））

- プロセッサ:
  コントローラのために個人情報を取扱う者（同（e））。

- 取扱:
  個人情報に対する（自動的かどうかに関わらず）オペレーションであり、収集、記録、保存、編集、変更、仕様、開示、削除等が含まれる。（ 同　第2条（b））

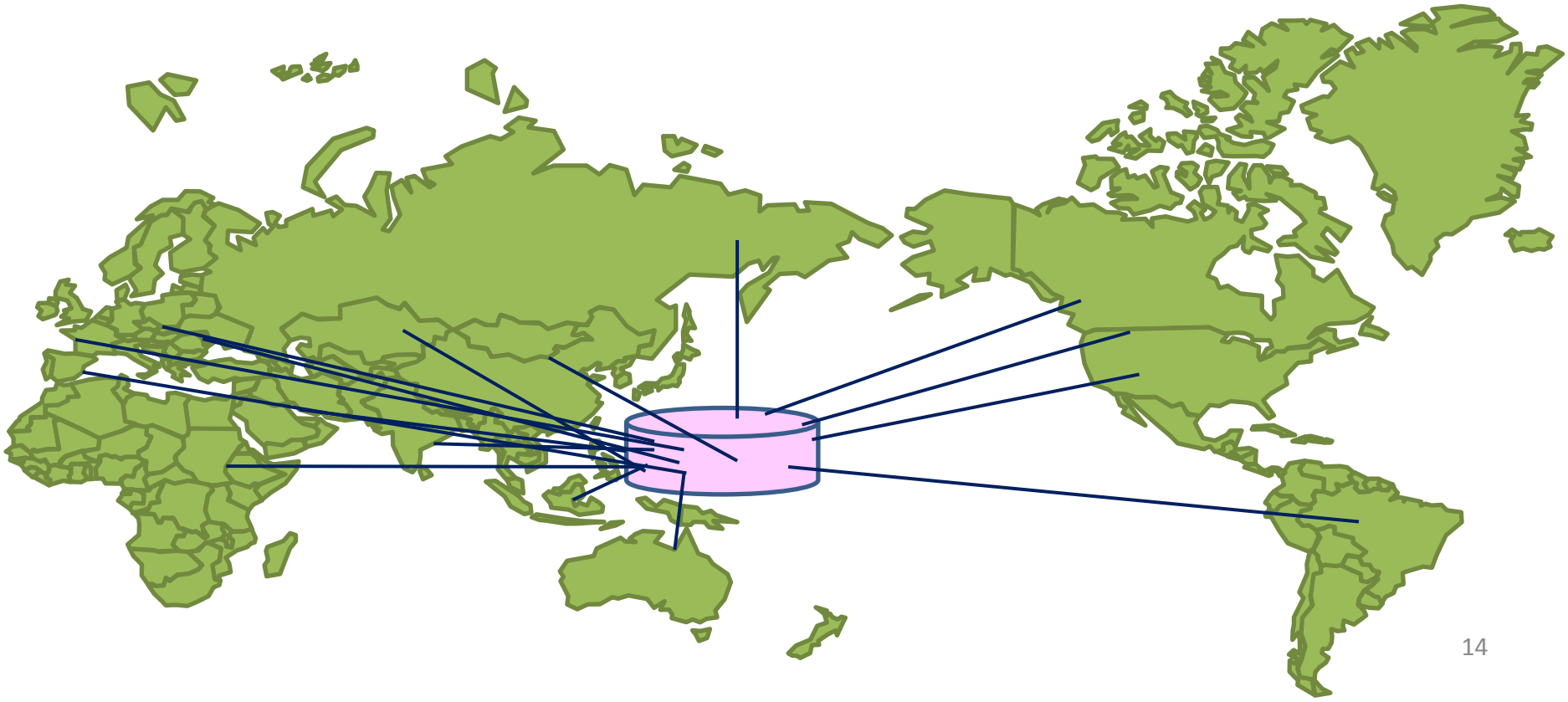
新たな動き：規則化

- 進捗：
  - 2012年　委員会　法案
  - 2014年　欧州議会　第1読会　採択
  - 現在、閣僚委員会で検討中
  - 早くて2015年制定？

2.2　域外からのサービス

想定するケース

- データや実質の機能提供も一元管理
- サービス提供者も1社（又は「グループ」として、不明確）



2.2 域外からのサービス

EU指令（に基づく各国法）は適用されるか？

- 指令第4条第1項(a)

  その国内における、「コントローラ」の施設（establishment）の活動において、（個人情報が）「取扱」われていれば、その国の法律が適用される。

  同じ「コントローラ」が、複数の国で施設があれば、それぞれの国の法律による義務に従う。

素朴な疑問

域外からのサービスでは、「施設」はないのでは？

2.2 域外からのサービス

EU指令（に基づく各国法）は適用されるか？

- 指令第4条第1項(c)

  コントローラがEU域内に設立されない場合は、加盟国にある設備（Equipment）（自動であるか否かを問わず）を個人情報取扱のために利用する場合は、その設備が単なる域内を通過する伝送目的であるときを除き、その加盟国の法律が適用される。

PC/ブラウザや、ネット家電を利用したクラウドビジネスは、設備（equipment）を利用している、と解釈されるのか？

加盟国equipmentの利用とは

「適用法に関する意見」
（2010年12月16日　第29条ワーキンｸﾞﾊﾟｰﾃｨｰ）

- 機器を「個人情報取扱のために利用している」というためには、「コントローラの何らかの活動」と「コントローラの個人情報を取扱う明確な意思」が必要（＊1）で、具体的判断はケースバイケース

＊1　WP56（2002年5月30日の29条WPの意見）

- 域外のサイトへのアクセスすべてを対象にするつもりではなく、「機器が個人情報の取扱のためにコントローラにより自由に使える場合」を対象とする
- 「コントローラが、機器がどのように動くかを決めることによって、データの内容と取扱い方法に関する決定をしていれば、自由に使える、と言える」
- この「自由に使える権限」は、機器の所有権とは別物である

2.2 域外からのサービス

EU法は適用されるか　第4条第1項（c）の適用は？

加盟国equipmentの利用とは

「適用法に関する意見」（続き）

- 「ユーザーのPCを使って個人情報が収集される場合に、例えばクッキーやジャバスクリプトバナーに関して、第4条第1項(c)号により、EU個人情報保護法が域外のサービスプロバイダに適用される可能性を29条WPは認識している」

→　あえて、単なるPCやWebブラウザではなく、クッキーやジャバスクリプトがPCに入れられていることに言及しているのは、単なるPCやブラウザでは、この「コントローラの意思と行為」の要件を欠くからと思われる。

→　例えば、視聴履歴を取得する機能を持ったネットワークTVや、スマホからの位置情報取得は、機器を「個人情報取扱のために利用している」といえ、機器が存在する国の個人情報保護法が適用されることになるだろう。
（視聴履歴が個人情報とすれば）

時代と技術の変化に対応しつつも、抑制的な、バランスの取れた解釈

2.2 域外からのサービス

第4条第1項(c)号に該当すると

- EU指令に定める実質的な義務
  - 利用目的の決定、合法的利用、コントローラの開示等。それほど困難ではない
- 対象の加盟国内に設置された代表を指名
  - 多くの加盟国では代表はDPAへの登録も義務
- コントローラ、代表は、手続き上の義務も
  - 取扱の登録、等

- 「機器」のあるすべての加盟国（28か国?!）
- 言語対応、手続きに詳しい弁護士の利用、費用、時間、官僚主義への対応・・・・

規則案
（2014年3月欧州議会の第一読会通過案）

第3条第2項

この規則は、以下の場合、域内に施設がないコントローラまたはプロセッサによる域内の情報主体の個人情報の取扱に適用する;

- 域内の情報主体に対し、有償か否かを問わず、商品やサービスを提供する場
- 域内の情報主体をモニターする場合

第25条

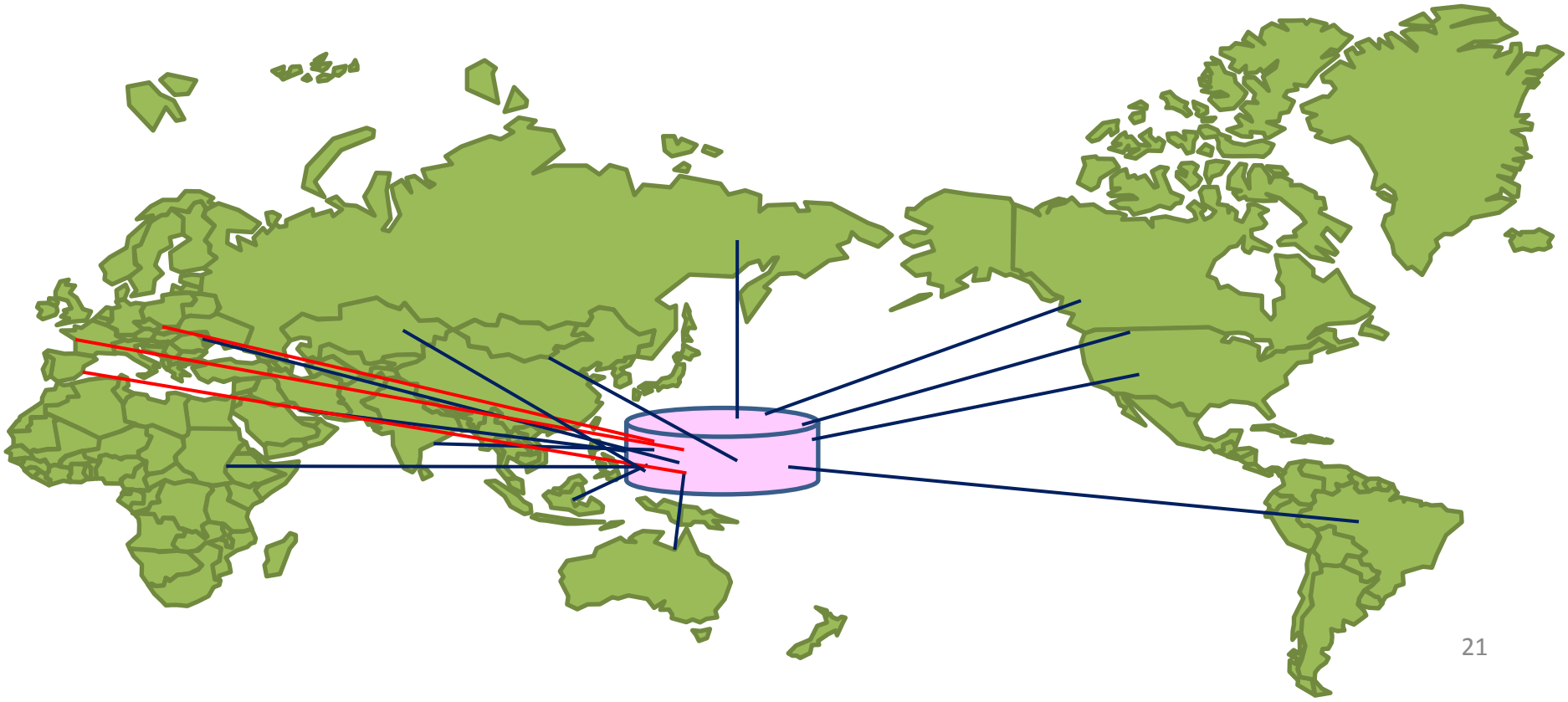
1. 第3条第2項の場合、コントローラは、EU内に代表を指名しなければならない。

3. 代表は、提供又はモニターしているうちの1加盟国に置けばよい。

2.3　域内からのサービス

想定するケース

- 域内拠点を関与させたサービス
  　各域内拠点が個人情報の収集者（コントローラ）
- データや実質の機能提供はグローバル一元管理



2.3 域内からのサービス
2.3.1

域外移転制限

第25条第1項
加盟国は、処理されている、又は後に処理される予定の個人データの第三国への移動は、当該第三国が適切なレベルの保護を提供している場合に限られることを規定するものとする

免除規定

第26条第1項

加盟国は、・・・以下の条件に基づいて行うことができることを規定するものとする。

(a) 移転の提案に対する本人の明確な同意

(b) 本人とコントローラとの契約の履行か、本人の要請に対する契約前の手段の実施に必要

(c) 本人の利益のためのコントローラと第三者間の契約の履行に必要

(d)～(f)略

第2項

加盟国は、コントローラが契約等により十分な保護を立証した場合は、許可することができる。

第1項による移転に消極的

1998年 WP意見書

第1項に基づく移転は、輸入者側に義務がないため、適用に消極的で、非常に限定的な場合しか適用されない。

本人同意は、十分な保護がない国に移転される具体的なリスクを説明された後、明確で明示的な同意が必要、とし、対面の場合ぐらいなら認められる

2012年 WP クラウドコンピューティングに関する意見書

1998年の意見書は、第1項の例外は繰り返しがなく大量でも構造的でもない場合のみに適用されることを意味しており、クラウドコンピューティングに適用することはほとんど不可能

第2項による移転

加盟国による判断だが、実質EU委員会のコントロールに

独自の判断は、その後も複雑

→　実務上、「標準契約」を活用するが、「一言一句変更できない」

第26条第3項

　第2項により許可する場合、加盟国はEU委員会と他の加盟国に伝え、反対があれば、撤回等の措置を取らねばならない。

第4項　EU委員会が、第2項における判断で、十分な保護を提供すると判断すべき標準契約を定めた場合は、それに従わねばならない。（移転を認めなければならない。）

標準契約と再委託可能性

1. Controller to Controller契約
   - 輸入者もContoller
   - 2001年 SET-I
     2004年 SET-II （民間提案から制定）
2. Controller to Processor契約
   - 輸入者は委託先
   - 2002年制定 →2010年改訂、2002年版廃止
     ポイント：再委託先にも権利行使可を条件として再委託可能と明記

Controller to Controllerでの委託は？

- 条文上は、委託を想定
  - SETーI 別紙 セキュリティ確保

    委託者を含み、輸入者の許可のもとで行動するどんな者も、輸入者の許可がなければ取扱ってはいけない

  - SET-II

    II.輸入者の義務
    (b) 輸入者は、委託先を含み、輸入者が個人情報にアクセスることを許可したすべての第三者が、個人情報の機密性とセキュリティを尊重し維持するための手続きを定めること。委託先を含み輸入者の許可のもとで行動するどんな者も、輸入者からの指示にのみ基づき個人情報を取扱う義務を負う‥

Controller to Controllerでの委託は？

標準契約実施状況のワーキングドキュメント（2006年 EU委員会）

- データコントローラに対する調査で出た改善すべき点

  「標準契約使用の”logistics”に関するものだった。加盟国やDPAが下記項目に柔軟なアプローチを取ることによって、制約と受け止められている事項は解消すると思われる」

  - マスター契約の使用
  - 輸入者からの更なる移転に関する明確化の必要性
  - 不当な遅延の回避の必要性
- 委員会コメント
  - 2002年版 C-P 一般的なのに全く言及なく、要再検討
  - 2001年 C-C

    「実務上はしばしば発生しているのに、標準契約上輸入者であるコントローラが外注するためのクリアな規定がない」「標準契約がコントローラからの委託もカバーしている可能性を検討し、関係条文を入れることを望む」
  - 2004年のSET-IIについては、言及なし

クラウドサービスでの輸出者は？

- 日本の本社も主体的にサービスを提供するが欧州の関係会社も主体的に利用する：C-C契約
- 各加盟国の関係会社が主体的に利用するなら、それぞれがコントローラ ＝ それぞれと契約！
- 第26条第2項「加盟国の許可」（標準契約により、許可義務があるだけ）
  →一部の国では、手続きが簡略化されているが、まだ、半数以上が契約のDPAへの登録義務

  言語対応、手続きに詳しい弁護士の利用、費用、時間、官僚主義への対応・・・・

コントローラの特定

2010年　適用法に関する意見書

- 適用法の特定はコントローラとその施設を特定すること。
このリンクの帰結として、コントローラの責任を確認。
- 「施設」とは、法人である必要はなく、その脈絡で個人情報を取扱う活動(activities in the context of which personal data are processed)を効果的、現実的に行使しているかが決め手。
- 一連のオペレーションに複数国にまたがる複数のプロセスが関与していても、それが一つの目的のためであれば、適用法は一つ。だからデータの所在ではなく、”context of activities”＝活動の脈絡が決定的要素となる

コントローラの特定

2010年 適用法に関する意見書 事例5

域外企業：インターネットサービス業者（コントローラ）

- ほとんどの加盟国に事務所あるが、個人情報の取扱に係る事案は、アイルランドオフィスのみ取り扱う。
  加盟国の事務所は、一般的な宣伝活動。
  アイルランドのみが個人情報が効果的に取扱われる活動
- ハンガリーにデータセンター：技術的メンテナンスにのみ関与

- アイルランドオフィスの活動がEU個人情報保護法の適用
- 他の加盟国の取扱にも、アイルランド法が適用される
- 安全管理については、ハンガリー法
  （指令第17条第3項：加盟国は妥当な技術的組織的対策を義務つける）＝地元のプロセッサに対し、調査等の権限

コントローラの特定

2013年 ドイツ 行政控訴裁判所 判決

- シュレスビッヒホルスタイン州 DPA が Facebookを、匿名での登録を認めないのは、個人情報保護法違反として訴追
- Facebookが控訴 （手続き上かも？？）
- 判決：Facebookの運営はFacebook Ireland Ltdで行われ、Facebook Germany GmbHはドイツのユーザーアカウントに影響を与えずマーケティングと宣伝のみを行っているため、指令第4条第1項（a）号の判断に関係するのは、Facebook Ireland Ltdであり、ドイツのユーザーアカウントについてもアイルランドの個人情報保護法が適用される

Cf

消費者団体が消費者団体が、プライバシーポリシーの複数の条文がドイツの不正競争防止法、民法、個人情報保護法等に違反しているとして、ベルリン地裁に差し止めを求めた訴訟 3件
→すべて原告が勝訴。裁判所もドイツの個人情報保護法に照らして判断。

コントローラの特定

2014年 欧州裁判所 決定 （スペインDPAからの付託）

＝Googleへの削除要求事件 （忘れられる権利で有名）

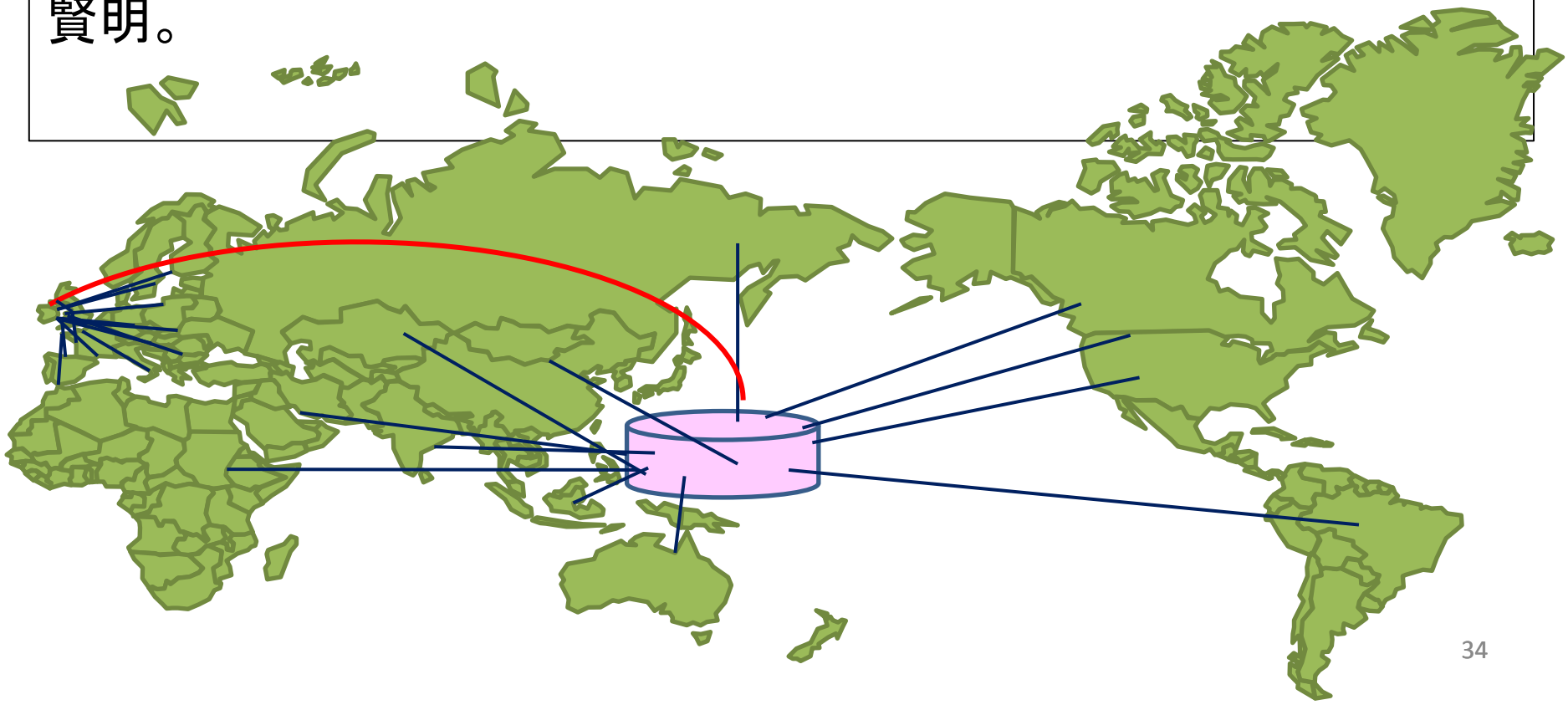
- スペインの子会社の活動は、スペイン個人情報保護法適用のトリガーとなる
- スペインの子会社は、個人情報は取扱わず、宣伝とマーケティングだけを行うが、、検索サービスという事業は広告なくては成り立たないので、スペインの子会社の活動は「その脈絡で個人情報を取扱う活動」である

- 欧州に検索サービス自体にかかわる施設がない中で、何とかGoogleに法を及ぼしたい、という動機が働いてもおかしくないケース
- 内容的にも事実を積み重ねて理屈を組み立てた感があり、もしも欧州内にGoogleの運営を行っている会社があった場合、同様の解釈となるか疑問。
- むしろ、世界のWebサーバからデータを収集するロボットを指令第4条第1項（c）号の”equipment”として解釈とした方が今後の混乱が防げたのではないか。

実務上の効率化

各加盟国の関係会社をコントローラにするよりも、

1社をコントローラとして、各国で必要な作業があるなら、委託先と位置付けるスキームでビジネスを組み立てる方が、手続き的にも賢明。



2.4　最後に　規則化への期待

- one stop shoppingと統一的対応
  - 各国「人権」保護とのせめぎあいはあるものの・・・
  - 本来のEUの目的：統合により米国に並ぶ勢力に
  - ビジネスからの要請
- 手続き重視から実質重視へ

- 相互承認スキームの発展によるビジネスへの負担軽減