コネクティッドカーと越境データ問題

板倉陽一郎

理化学研究所革新知能統合研究センター（AIP）客員主管研究員

弁護士・ひかり総合法律事務所

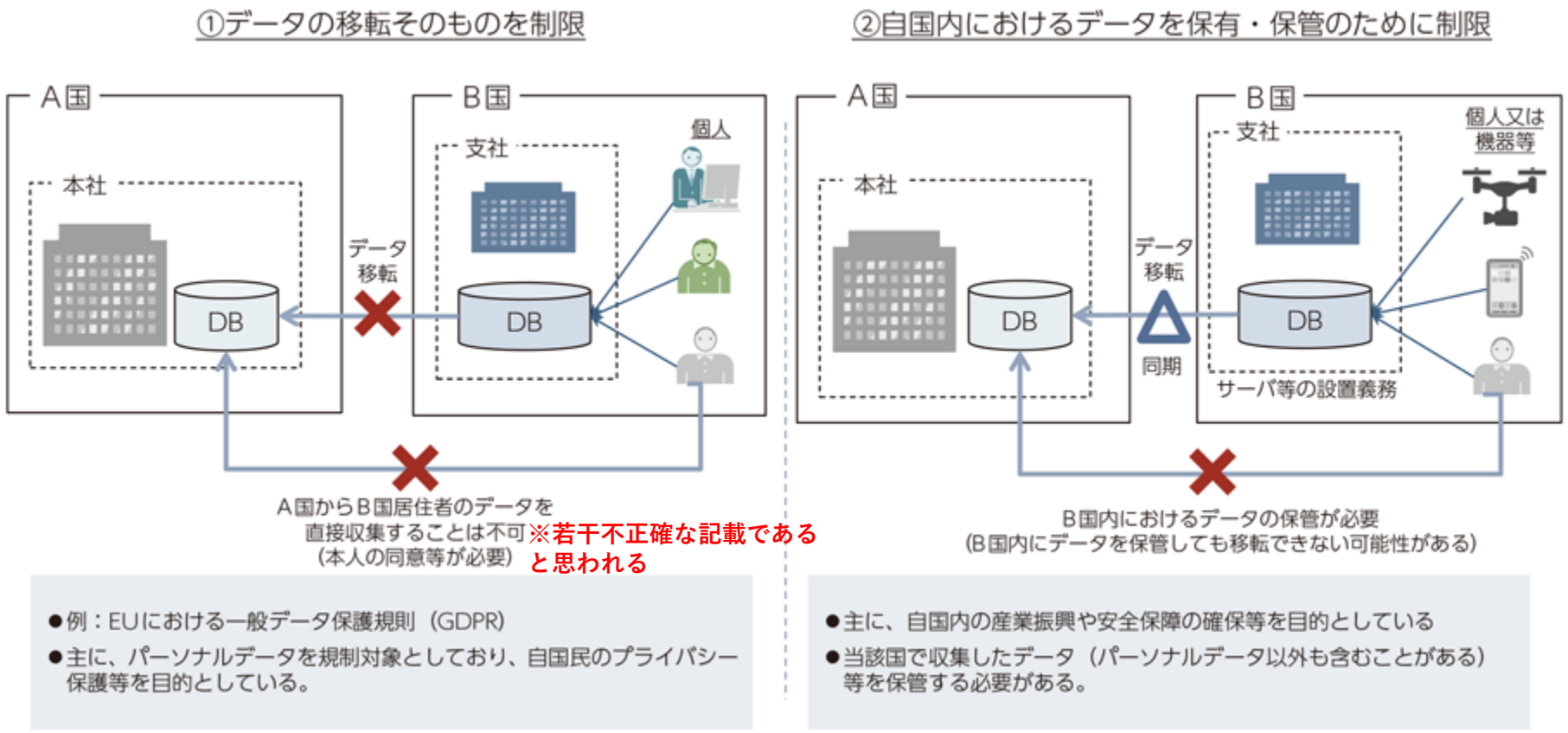
アジェンダ

- 1.　越境データ問題の類型
- 2.　欧州十分性決定に関する対話の現状
- 3.　コネクティッドカーにおけるあてはめ

自己紹介

- 2002年慶應義塾大学総合政策学部卒，2004年京都大学大学院情報学研究科社会情報学専攻修士課程修了，2007年慶應義塾大学法務研究科（法科大学院）修了。2008年弁護士（ひかり総合法律事務所）。2016年4月よりパートナー弁護士。
- 2010年4月より2012年12月まで消費者庁に出向（消費者制度課個人情報保護推進室（現・個人情報保護委員会事務局）政策企画専門官）。2017年4月より国立研究開発法人理化学研究所革新知能統合研究センター社会における人工知能研究グループ客員主管研究員。
- 総務省・AIネットワーク社会推進会議環境整備分科会及び影響評価分科会構成員，IoT推進コンソーシアム・データ流通促進WG及びカメラ画像利活用SWG委員等。

1.　越境データ問題の類型



※若干不正確な記載であると思われる

総務省平成29年度版情報通信白書より

越境データ移転制限

- ①データの移転そのものを制限（[個人データの]越境データ移転制限）
  - 欧州：国境を超えることを（中心に）制限（”Any transfer of personal data which are undergoing processing or are intended for processing after **transfer to a third country** or to an international organization…”（GDPR44条））
    - 英国：”A controller may not transfer personal data to a third country or to an international organization…”（新法案73条）
  - 日本：外国にある第三者への提供の制限（個人情報保護法24条）
  - NZ：個別の移転の制限が可能（” The Commissioner **may prohibit** a transfer of personal information from New Zealand to another State if…”（NZ1993年プライバシー法114B条第1項）
- （少なくとも欧州は）人権保障が目的
- 規律は一律ではない
  - 欧州は「越境の移転」を制限し，日本は「外国にある『第三者』への提供」を制限する。具体的な差異は同一法人間移転に生じる。
  - 十分性認定を得ている国でも一律の制限ではないことがある。

データローカリゼーション規制

- ②自国内におけるデータを保有・保管のために制限（データローカリゼーション規制）
  - ロシア：（2014年7月21日付連邦法第242-FZ号「情報・電子通信ネットワークにおける個人情報の処理手続きの適正化に関するロシア連邦法の改正について」）により，「**ロシア国内の事業者（外資系企業の現法、支店および駐在員事務所を含む）および海外の事業者であっても、ロシア国内向けのウェブサイトを通じて個人情報を収集する者（オペレーター）は、ロシア国民の個人情報をロシア国内で保存、管理しなければならない**。また、オペレーターは、個人情報（ロシア国民のものであるか否かを問わない）を処理するサーバーの場所を含む通知を通信・情報技術・マスコミ監督庁（Roskomnadzor）に提出しなければならない場合もある」（JETROウェブサイト「外資に関する規制」より）
  - 中国：**重要情報インフラストラクチャーの運営者が中華人民共和国の国内での運営において収集、発生させた個人情報及び重要データは、国内で保存しなければならない**（中国サイバーセキュリティ法37条（JETRO：大地法律事務所仮訳）
- 安全保障が目的であり，政治的な規制
  - 政治的な動きが見られる

G7香川・高松情報通信大臣会合と伊勢志摩首脳宣言

経済産業省

➢ 大臣会合の議論

経済産業省資料より

平成28年（2016年）

４月２９～３０日の大臣会合では、並行して開催されたマルチステークホルダー会合の結果も踏まえ、最終的に成果文書として、憲章、共同宣言が採択されるとともに、G7各国の具体的な取組を集めた強調行動集が策定された。

➢ 大臣会合における成果文書のポイント

- **情報の自由な流通の確保について合意**
  情報の自由な流通の原則についてG7として合意するとともに、新興国等によるデータ現地保存要求義務や、ソースコードの開示・移転要求についてG7として反対の姿勢を明確化。
- **サイバーセキュリティの推進について合意**
  サイバーセキュリティの脅威に対し、その重要性についてG7として認識を共有するとともに、国際協力、脅威分析の取組み、人材育成の強化について合意。

➢ Ｇ７伊勢志摩首脳宣言「サイバーに関するＧ７の行動と原則」

- 我々は、**情報の自由な流通がグローバルな経済及び開発を促進する基本原則**であり、デジタル経済の全ての活動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確保するものであることを再確認する。
- 我々は、引き続き、インターネットのグローバルな性質を維持し，**国境を越える情報の流通を促進**し、また、インターネット利用者が自らの選択したオンラインの情報、知識及びサービスにアクセスすることを可能とするＩＣＴ政策を引き続き支持する。我々は、適法な公共政策の目的を考慮し、**不当なデータ・ローカライゼーション要求に反対**する。

WORLD TRADE ORGANIZATION

S/C/W/374

26 September 2017

(17-5101) Page: 1/2

Council for Trade in Services Original: English

COMMUNICATION FROM THE UNITED STATES

MEASURES ADOPTED AND UNDER DEVELOPMENT BY CHINA RELATING TO ITS CYBERSECURITY LAW

The following communication, dated 25 September 2017, from the delegation of the United States is being circulated to the Members of the Council for Trade in Services.

---

1. The United States requested the inclusion of this topic on the agenda for the Council for Trade in Services in order to express its concerns with certain measures China has adopted, and related implementing measures under development, that could significantly impair cross-border transfers of information. This is one key aspect of U.S. concerns regarding China's Cybersecurity Law and related measures. If these measures enter into full force in their current form, they could have a significant adverse effect on trade in services, including services supplied through a commercial presence and on a cross-border basis. We are bringing this matter before this Council because the potential effects extend across all service sectors and have bearing on the rights of other Members.

2. The measures of concern include: The Cybersecurity Law, adopted in November 2016 and taking effect June 2017; and various implementing measures connected with the Cybersecurity Law and China's National Security Law (adopted in July 2015), including the "Measures on the Security Assessment of Cross-Border Transfer of Personal Information and Important Data" and the "Draft National Standard – Information Security Technology – Guidelines for Data Cross-border Transfer Security Assessment."

3. China's measures would disrupt, deter, and in many cases, prohibit cross-border transfers of information that are routine in the ordinary course of business. More specifically:

a. The measures would apply to "network operators," which could encompass any foreign service supplier that has a website or uses the Internet to communicate with customers, suppliers, or affiliates. Such a broad definition means that the measures could have a negative impact on a wide range foreign companies.

b. The measures, which pertain to "important data"[1] and "personal information," would severely restrict cross-border transfers unless a broad set of burdensome conditions are met. These conditions would restrict even routine transfers of information, fundamental to any modern business. They include: (a) that the network operator (or in certain cases, a governmental authority) has performed a "security assessment;" (b) that the purpose of the transfer meets standards of legitimacy, necessity, and justification; and (c) that purported risks, including to national security, social and public interests, and lawful interests of individuals, are mitigated. As one aspect of our concerns, a need to demonstrate the necessity of transfers is very troubling, since it impinges on commercial

[1] Important data is defined as "data closely related to national security, economic development and societal and public interests." The Draft Guidelines provide broad descriptions of data that can fall within this definition and lists 27 sectors, including "Communications" and "Electronics and Information," as well as "Steel" and "Food and Drugs." There is also a 28th "Miscellaneous" category that includes inter alia any sector "closely linked with national security and social public interests." This definition is so broad that it could apply to any and all data.

choices and longstanding business arrangements supported by robust trade rules, and many common transactions would not appear to meet the criteria set out.

c. With respect to "personal information," in addition to the conditions already described, a "network operator" would appear to be required to obtain consent from each individual before any cross-border transfer can take place. This is an extraordinarily burdensome requirement that could disrupt business operations without contributing to privacy protections. Many less burdensome options exist to achieve privacy objectives, including compliance with international cross-border privacy frameworks, such as the APEC Cross-Border Privacy Rules System endorsed by China; contractual agreements between network operators and third party recipients; and third-party accreditation.

d. In some circumstances, the outcome of the security assessment would result in an outright prohibition on cross-border data transfers. These circumstances are so broadly and vaguely defined – including when transfers would pose a risk to "national security," "economic development," and "social public interests," and when such transfer may be detrimental to public and national interests – that they could cover a nearly unlimited range of transactions.

e. The measures would impose local data storage requirements on operators in "critical information infrastructure sectors," which the Cybersecurity Law defines in broad and vague terms. Cross-border transfers of data by these operators would be subject to review by China's competent regulatory authorities. Such requirements would inevitably impede cross-border information flows and disrupt normal business operations.

4. Thus, the measures would impose special scrutiny, particular procedures, or bans on the cross-border transfer of expansive and loosely-defined categories of data. The result would be to discourage cross-border data transfers and to promote domestic processing and storage. The impact of the measures would fall disproportionately on foreign service suppliers operating in China, as these suppliers must routinely transfer data back to headquarters and other affiliates. Companies located outside of China supplying services on a cross-border basis would be severely affected, as they must depend on access to data from their customers in China.

5. In this regard, we note that China has undertaken market access and national treatment commitments under the General Agreement on Trade in Services for many services that would be affected by these measures. In addition, China's cross-border commitments apply to a broad range of sectors – from accounting to financial data processing to travel services. None of these cross-border services is feasible without accessing data from China, much of which would appear to fall within the scope of the restricted or banned categories.

6. The United States has been communicating these concerns directly to high level officials and relevant authorities in China. We are bringing the matter to this forum in order to raise awareness among other Members of the nature of the pending measures and their potential impact on trade. We request that China refrain from issuing or implementing final measures until such concerns are addressed. We will keep the Council informed of any further developments on this matter.

TPPにおけるデータローカリゼーション規制

第 14.1 条	定義 「個人情報」とは、特定されたまたは特定し得る自然人に関する情報（データを含む。）をいう。
第 14.11 条	情報の電子的手段による国境を越える移転 1. 締約国は、各締約国が情報の電子的手段による移転に関する自国の規制上の要件を課することができることを認める。 2. 各締約国は、対象者の事業の実施のために行われる場合には、情報（個人情報を含む。）の電子的手段による国境を越える移転を許可する。 3. この条のいかなる規定も、締約国が公共政策の正当な目的を達成するために 2 の規定に適合しない措置を採用し、又は維持することを妨げるものではない。ただし、当該措置が、(a)及び(b)の要件を満たすことを条件とする。 (a)恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと。 (b)目的の達成のために必要である以上に情報の移転に制限を課するものではないこと。
第 14.13 条	コンピュータ関連設備の設置 1. 締約国は、各締約国がコンピュータ関連設備の利用に関する自国の法令上の要件（通信の安全及び秘密を確保することを追及する旨の要件を含む。）を課することができることを認める。 2. いずれの締約国も、自国の領域において事業を遂行するための条件として、対象者に対し、当該領域においてコンピュータ関連設備を利用し、又は設置することを要求してはならない。 3. この条のいかなる規定も、締約国が公共政策の正当な目的を達成するために 2 の規定に適合しない措置を採用し、又は維持することを妨げるものではない。ただし、当該措置が、次の要件を満たすことを条件とする。 (a) 恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと。 (b) 目的の達成のために必要である以上にコンピュータ関連設備の利用又は設置に制限を課するものではないこと。

経済産業省「平成27年度我が国経済社会の情報化・サービス化に係る基盤整備事業越境データフローに係る制度等の調査研究報告書」（デロイトトーマツリスクサービス委託）より

2. 欧州十分性決定に関する対話の現状

各EU加盟国から第三国への個人データの移転

➢ 欧州から第三国への個人データの移転については、EUデータ保護指令の規定により、原則として次のいずれか手続が必要。

① 十分な保護措置を講じている国として認定を受ける（いわゆる「十分性認定」）（注１）。
② 多国籍企業内でのデータ流通を認める拘束的企業準則（BCR）を申請し、監督機関の許可を得る。
③ 標準契約条項（SCC）を締結する。
④ 本人の同意を得る。

（注１）十分性認定された11の国と地域は以下のとおり。なお、カッコ書きは十分性認定時期を示す。
スイス（2000年７月）、カナダ（民間部門のみ。2001年12月）、アルゼンチン（2003年６月）、
ガーンジー島（2003年11月）、マン島（2004年４月）、ジャージー島（2008年５月）、フェロー諸島（2010年３月）、
アンドラ（2010年10月）、イスラエル（2011年１月）、ウルグアイ（2012年８月）、
ニュージーランド（2012年12月）。
なお、イスラエル、ウルグアイ及びニュージーランドは申請から取得まで３年以上かかった模様。

（注２）日本は十分性認定を受けていないため、各EU加盟国から日本へ個人データを移転する際には、
上記②又は③が必要となる。日本は②を行っている企業はまだないが、③は存在。

➢ 2016年4月14日に欧州議会において、 EUレベルで適用されるデータ保護の統一ルールとして、EUデータ保護指令に代わって、EU一般データ保護規則（General Data Protection Regulation：GDPR）が採択され、2018年５月25日より適用される予定。各加盟国内で実施のための国内措置が必要となる「指令」から、加盟国に直接適用される「規則」に格上げされたことにより、EU域内のデータ保護ルールの一元化が図られることになる。

個人情報保護委員会資料より

日本から外国の第三者への個人データの移転

○改正個人情報保護法第24条の内容

- 以下のいずれかによって、国内と同様に外国の第三者への個人データの提供が可能

①外国にある第三者が個人情報保護委員会が認めた国に所在する場合

②外国にある第三者が個人情報保護委員会の規則で定める基準に適合する体制を整備している場合

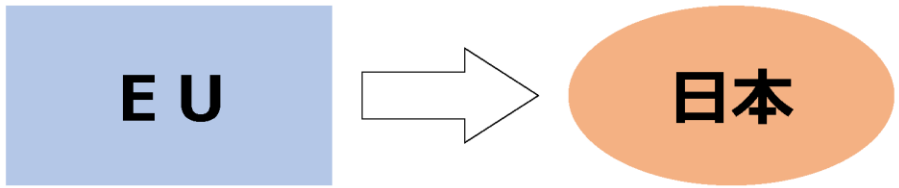
③外国にある第三者へ提供することについて本人の同意がある場合

3

個人情報保護委員会資料より

日本・EU間における個人データの越境スキーム

一般データ保護規則



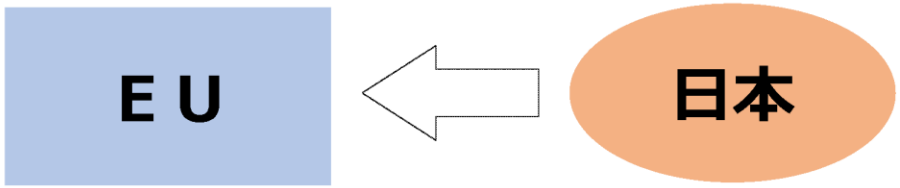
- **十分性決定**
  十分な保護水準に関して***欧州委員会***が国や地域を***評価し決定***するもの。

- **拘束的企業準則**
  企業グループ内の内部行動規範でEUの***監督機関が承認***するもの。

- **標準データ保護条項**
  欧州委員会が***採択***するもの。

- **本人同意**
  十分性の決定等がないことによるリスクについての情報が提供された後、明示的に同意。

個人情報保護法



- **国指定**
  外国にある第三者が個人情報保護委員会が認めた国に所在する場合。

- **体制整備**
  外国にある第三者が個人情報保護委員会の規則で定める基準に適合する体制を整備している場合。

- **本人同意**
  外国にある第三者へ提供することについて本人の同意がある場合。

個人情報保護委員会資料より

個人情報保護委員会熊澤委員と欧州委員会ヨウロバー委員との協力対話及び熊澤春陽個人情報保護委員会委員、ベラ・ヨウロバー欧州委員会委員（司法・消費者・男女平等担当）による共同プレス・ステートメント（平成29年（2017）年7 月3 日）

- 「日EU 間の相互の円滑な個人データ移転を図る枠組みとは、相互に、双方の個人情報保護制度の保護水準が十分であることを認める相互認証であり、来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」
  - 協力対話の結論は，欧州委員会からの十分性決定と，日本から欧州に対する同等性認定であることが明言された

- 共同プレスステートメント
- 「…両者は、双方のプライバシー法制度の最近の改正によって、双方の二つの制度は、より一層類似したものになったことを認めた．これは、特に**双方が十分な保護レベルを同時に見出すことを通して、相互の円滑なデータ流通をより一層促進する新しい機会を提供する**ものである．」
- 「以上を踏まえ、両者は、**双方の制度間の類似性が強化されたことを基礎として、関連する相違点への対処等により、2018 年の早い時期に、この目標を達成するための努力を強化する**ことを決意した．」
  - 「双方が十分な保護レベルを同時に見出す」ことが明示された他，「2018 年の早い時期」との時期が示された．欧州委員会からの十分性決定については平成29（2017）年中に検討するとの意向が示されていたが，少し後ろ倒しになり，平成30（2018 年）の「早い時期」という目標が示されたもの

「日EU 間の相互の円滑な個人データ移転について」（平成29 年7 月4 日個人情報保護委員会決定）

- 「この会談を踏まえ、**個人情報保護委員会としては、今後、欧州委員会の日本に対する十分性認定に係る作業の進捗に併せて、来年前半を目標に個人情報保護法第 24 条に基づく EU加盟国の指定を行う可能性を視野に、本年6 月16 日に個人情報保護委員会において決定した「個人情報保護法第24条に係る委員会規則の方向性について」に基づき、今後委員会規則の改正手続を進めていく**こととする．」
- 「また、EU加盟国については、EU の個人情報保護制度のみならず、その制度の遵守態勢、執行態勢並びに相互の理解、連携及び協力の可能性等について確認していく必要があることから、引き続き、情報収集・調査を行うとともに EU 加盟国の各データ保護機関等との対話を引き続き精力的に行っていくこととする．」

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS
“Commission Work Programme 2018 An agenda for a more united, stronger and more democratic Europe”（2017 年10 月24 日）

- “The Commission will finalise its guidance on the way forward on data retention. **In early 2018, the Commission also aims to adopt a decision on data adequacy for Japan** to ensure the free flow of personal data between the EU and Japan as an integral part of our strengthened economic partnership.”

- 日本のみを挙げて，「2018 年初頭」には十分性決定を行う予定であることが述べられた.
- 平成29（2017）年1 月10 日のコミュニケーションでは日本及び韓国とされていたところ，日本のみとなっている

個人情報保護委員会熊澤委員と欧州委員会ヨウロバー委員との会談及び熊澤春陽個人情報保護委員会委員、ベラ・ヨウロバー欧州委員会委員（司法・消費者・男女平等担当）による共同プレス・ステートメント（平成29（2017）年12 月14 日）

- 「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するとともに、今後、その詳細について作業すること、また、**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**」
- 「**相互に十分性を見出すことを、2018 年のできるだけ早い時期に達成するための作業を加速させる**ことを目指して、2017 年 12 月 14 日に東京で建設的な会談を行った．」
- 「両者は、この目的の重要性を、特に最近の日 EU 経済連携協定（EPA）の交渉妥結の観点から再確認した．個人データの自由な流通を確保することにより、十分性を同時に見出すことは、基本的なプライバシーの権利の保護を強化しながら、日 EU・EPA の便益を補完し拡大することができる．これは日 EU 間の戦略的なパートナーシップにも貢献する．」
- 「両者は、過去数か月の大きな進展を評価するとともに、双方の制度間の関連する相違点を埋めるための解決策を探った．両者は、次の段階へ進み、解決策の詳細について作業すること、また、議論のペースを加速させることに合意した．」
- 「これを念頭に置きつつ、次回のハイレベル会談については、議論を完結させることを目指し、2018 年初めにブリュッセルで開催することとする．」

- 平成30（2018）年第1 四半期という目標は，平成30 年5月25 日にGDPR が全面適用されることからは適切な設定
- 現在，十分性決定の手続はEU データ保護指令下で進めていると考えられるが，データ保護指令にもGDPR にも，十分性決定を求めるための請求や，その受理等，手続の詳細については規定がないため，決定にまで至らなければそもそもGDPR への経過規定にも該当することができない（決定に至った場合にはGDPR45 条9 項によりGDPR 上も有効な決定として扱われる）.
- 日本としても，欧州委員会としても，平成30 年5 月25 日は絶対的な期限


駐日欧州連合代表部
「いいね！」済み · 2月6日 ·
日・EU間の #個人情報移転 をめぐる保護措置の十分性認定に関して双方の専門家が都内で協議し、進展が見られた #EUinJapan
いいね！ コメントする シェアする
59
トップコメント
シェア22件
コメント3件
小倉 昌樹 (^^♪
いいね！ · 返信 · 1週間前
他2件のコメントを表示
コメントする...
知り合いかも
すべて見る
棚橋哲夫
共通の友達1人
友達になる

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に関するガイドラインの方向性について

平成 30 年２月９日
個人情報保護委員会

１．背景

個人情報保護委員会は、国境を越えた個人データの流通が増大する中、その円滑な移転を確保するための環境整備に取り組んでいるところである。その中で、日 EU 間の個人データの移転については、相互の円滑な移転を図る枠組みの構築を視野に、欧州委員会との間で累次の対話を重ねてきている。

平成 29 年 12 月 14 日には、当委員会委員と欧州委員会委員との間で会談を行い、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するとともに、今後、その詳細について作業すること、また、平成 30 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したところである。

この解決策として、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に関するガイドラインを策定することとし、次のような考え方を軸に検討を進めることとする。

２．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に関するガイドラインの方向性

※「➢」はガイドラインの方向性（案）

① 要配慮個人情報の範囲

EU ではセンシティブデータとして扱われる「性生活」・「性的指向」・「労働組合」に関する情報が、日本では要配慮個人情報に該当しない。

➢ EU から移転された個人データについて、「性生活」・「性的指向」・「労働組合」に関する情報に関しては要配慮個人情報と同様の取扱いを行うこととする。

② 保有個人データの範囲

EU では保有期間にかかわらず全ての個人情報について開示・訂正・利用停止等の請求権が認められるが、日本では６か月以内に消去することとなる個人データについては開示等の請求権が認められない（請求権が認められる保有個人データではない）。

➢ EU から移転された個人データについて、６か月以内に消去することとなる個人データについても保有個人データとして扱うこととする。

③ 利用目的の特定

EU 側は、EU では第三者から提供を受けた個人情報の利用目的は、取得時に特定された利用目的の範囲に制限されるのに対し、我が国の個人情報保護法にこれを直接規定する条項がないことから明確化を求めている。

➢ EU から移転された個人データについて、確認記録義務を通じて確認した利用目的の範囲内で利用目的を特定し、その範囲内で当該個人データを利用することとする。

④ 日本から外国への個人データの再移転

EU 側は、日本から EU 以外の外国への個人データの再移転について、保護レベルが確保されるよう明確化を求めている。

➢ EU から移転された個人データについて、本人同意に基づき再移転する場合は、本人が同意するために必要な移転先の状況についての情報を提供し、提供先の体制整備をもって再移転する場合は、契約等により、個人情報保護法と同水準の保護措置を実施することとする。

⑤ 匿名加工情報

EU では、加工方法に関する情報が残存している場合、安全に分離保管されていても再識別の可能性があるとして匿名化とはみなされない。

➢ EU から移転された個人データについて、個人情報保護法上の匿名加工情報として扱おうとする場合は、加工方法に関する情報を削除し、再識別を不可能なものとすることとする。

３．「EU」の定義

今回の日 EU 間の相互の個人データ移転の枠組みにおいて、欧州委員会からは、「EU」の範囲について、欧州経済領域協定に基づきアイスランド、リヒテンシュタイン及びノルウェーを含むこととしたい旨申越しがあることから、本ガイドラインの対象となる「EU」として当該定義を採用することとしたい。

なお、個人情報保護法第 24 条に基づき、当委員会が指定する外国の対象も同様に勘案することとする。

十分性決定後に予想される事態

- 日本の十分性決定は平成30 年第1 四半期までになされるように思われ，その場合，現在，標準契約約款（SCC）の締結やデータ保護指令上の同意に費やしている事業者のコストは消滅することから，我が国にとっては望ましい事態.
- 標準契約約款は基本的に変更の余地がなく，記載するだけだとはいえ，国によっては届出義務がある場合もあるし，どの範囲で締結するかなどの検討にはリーガルコストが避け得ない．越境移転を同意によって処理しようとする場合も同様である．十分性決定によって，日本への移転に特別な方策が必要なくなるということは基本的に好ましいことである.

①十分性決定の範囲が民間法に限られること

- これまでの公表文書では公的機関の法律である行政機関個人情報保護法や独立行政法人等個人情報保護法を所管する総務省が一切の姿を見せていないし，個人情報保護委員会が所管するマイナンバー法（番号利用法）についても，何らかの意見が交わされた様子がない
- PNR（航空機搭乗者情報）の税関や入管への提供については別途の十分性決定が必要になる．これは，米国やカナダ，オーストラリアと同様の状況になるということ

②「相互」の認証はどの範囲か

- 欧州委員会そのものを法24 条に基づいて同等性認定したとしても，日EU 間のデータ移転は十分ではなく，欧州連合の加盟各国を個別に同等性認定する必要がある
  - 同等性認定国を定めるための，法24 条に基づく個人情報保護法施行規則の改正については「「個人情報の保護に関する法律施行規則の一部を改正する規則（案）」に関する意見募集について」として意見公募手続に掛けられ，平成30 年1 月5 日に募集を終了している．）．

- しかし，欧州連合加盟国のすべてがフランスやドイツのような厳格な監督・執行体制を備えられているわけではなく，GDPR が適用されるからといって安易にすべて同等性認定してよいのかについては検討の余地がある．
- 日本の十分性決定を得るため，「相互」に30 か国を認定しなければならないとすれば，それは公平なのか，日本の個人情報の本人の権利利益の観点から適切なのかが検討されなければならない．

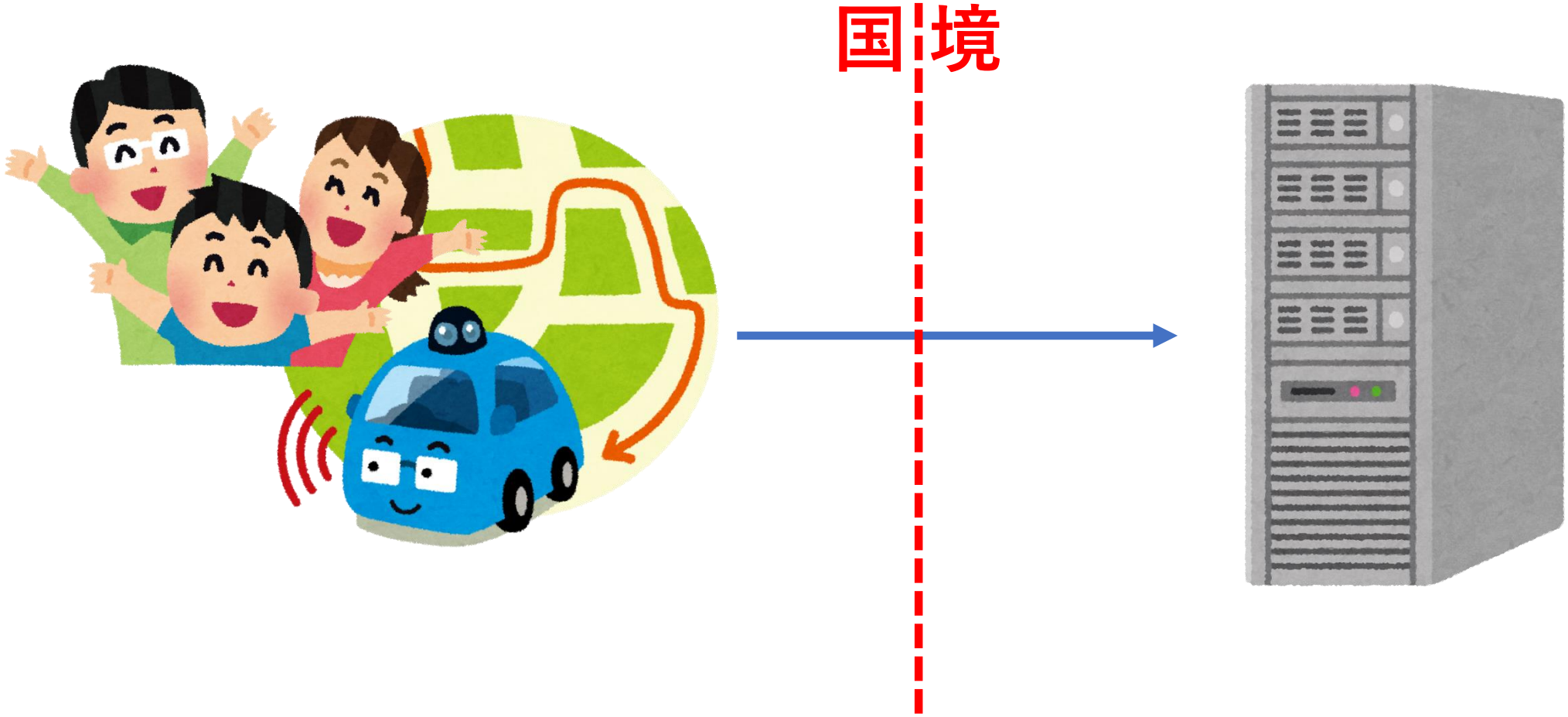
③訴訟で無効となる可能性

- 欧米セーフハーバーへの十分性決定が無効となった欧州司法裁判所のMaximillian Schrems v Data Protection Commissioner(Case C-362/14)（2015年10 月5 日）
  - 欧州委員会と米国商務省は同判例を前提に「プライバシー・シールド」を構築するための再交渉を強いられた.
  - 指令及び欧州基本権憲章の観点から欧州のデータ保護制度と”essentially equivalent”（実質的に同等）であることを求めており,「法令改正を行わない形での解決策」で妥結しようとしている日本が,この要件を突破できるのかが注目される
  - 遠からず問題視されることが予想されるのであれば，今から欧州司法裁判所での紛争を念頭に置いて準備する必要がある

3. コネクティッドカーにおけるあてはめ

- 日本の事業者において越境データ移転が問題になるのは
  - ①外国でコネクティッドカー関連サービスを提供するが，サーバを日本又は第三国に置き，直接当該サーバでデータが収集される場合
  - ②外国でコネクティッドカー関連サービスを提供し，サーバを当該外国に置くが，更に日本又は第三国のサーバに移転される場合
  - …が，メインであると思われる
- 最も問題になりやすいと思われるGDPR対応についてのケーススタディ（ただし，各国のGDPR実施法等は考慮に入れない）

①外国でコネクティッドカー関連サービスを提供するが，サーバを日本又は第三国に置き，直接当該サーバでデータが収集される場合

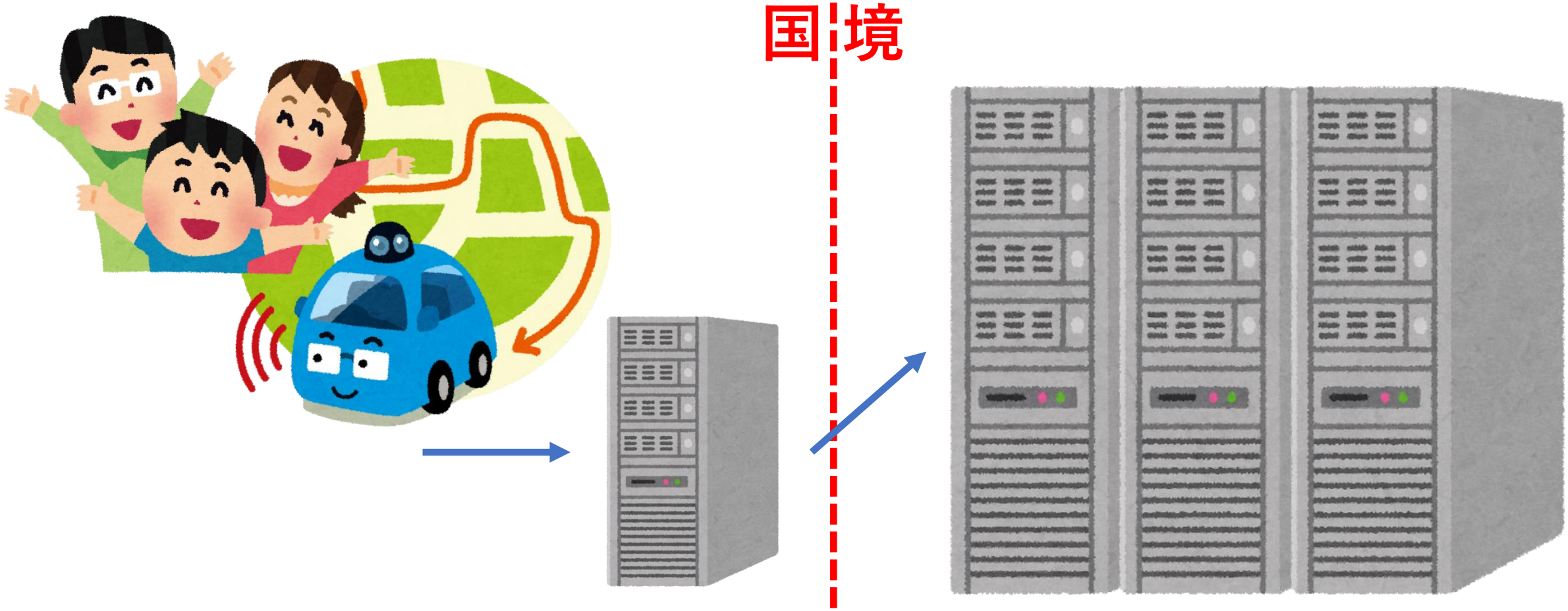


越境データ移転部分の分析

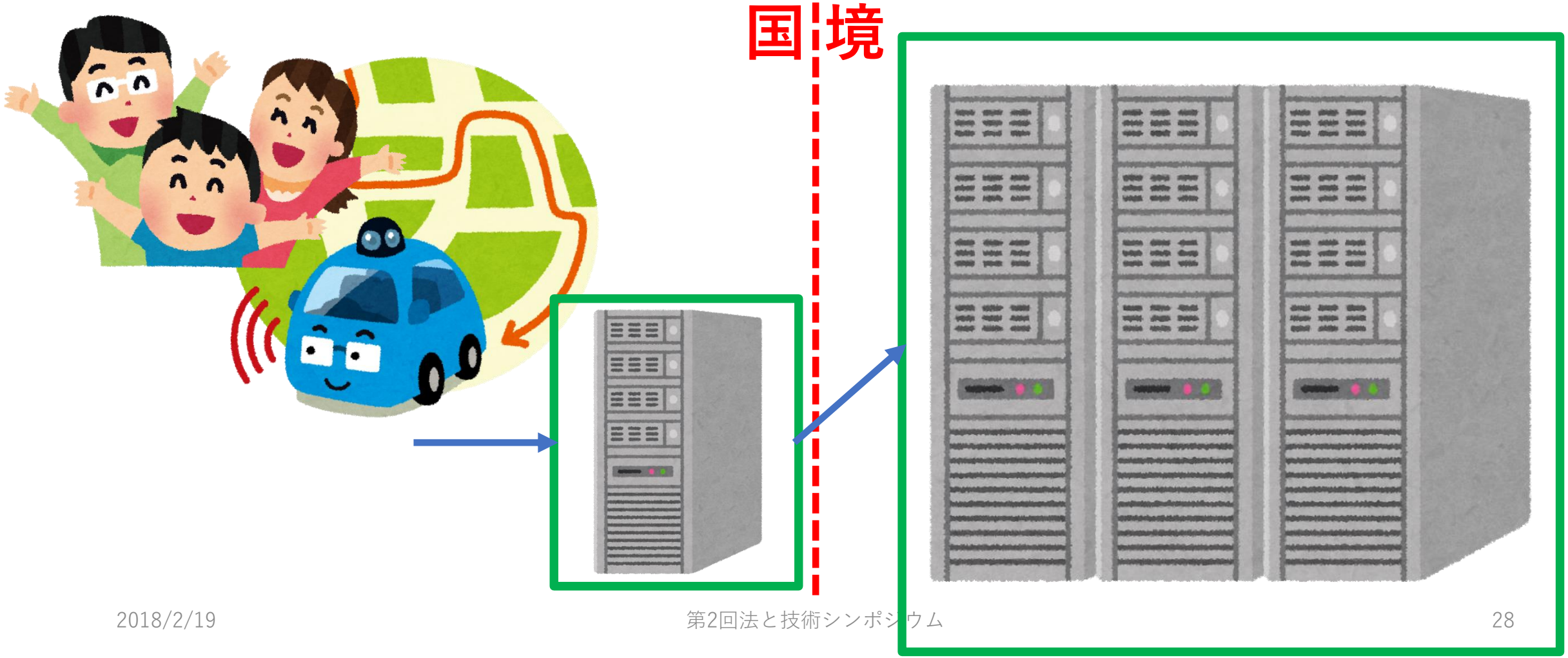
- ユーザから直接的に個人データを取得する場合は越境データ移転の問題ではない（cf.スマートフォンのアプリケーションをワールドワイドなストアで公表する場合とパラレルに考えて良いと思われる）

- 個人データの取扱いが欧州で行われているとしてGDPRが適用される可能性及び，代理人設置義務違反の問題になる可能性はある
  - Rechtbank Den Haag（オランダ：ハーグ地方裁判所）ECLI:NL:RBDHA:2016:14088はWhatsAPPに関してオランダにおける代理人設置義務及びこれに反したことによる課徴金を肯定
- 個人データの取扱いに関する域外適用はほぼ肯定される（GDPR3条2項）

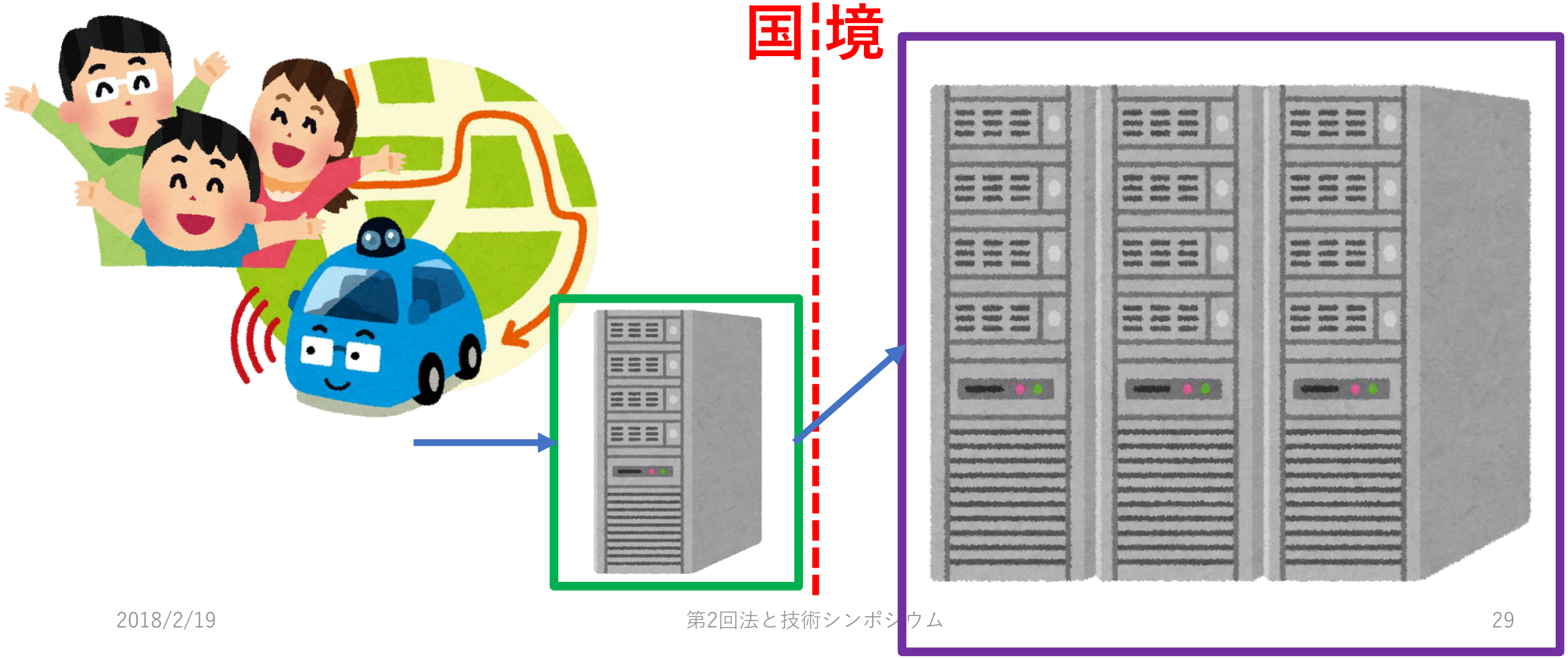
②外国でコネクティッドカー関連サービスを提供し，サーバを当該外国に置くが，更に日本又は第三国のサーバに移転される場合



②外国でコネクティッドカー関連サービスを提供し，サーバを当該外国に置くが，更に日本又は第三国のサーバに移転される場合（法人が同じ場合）



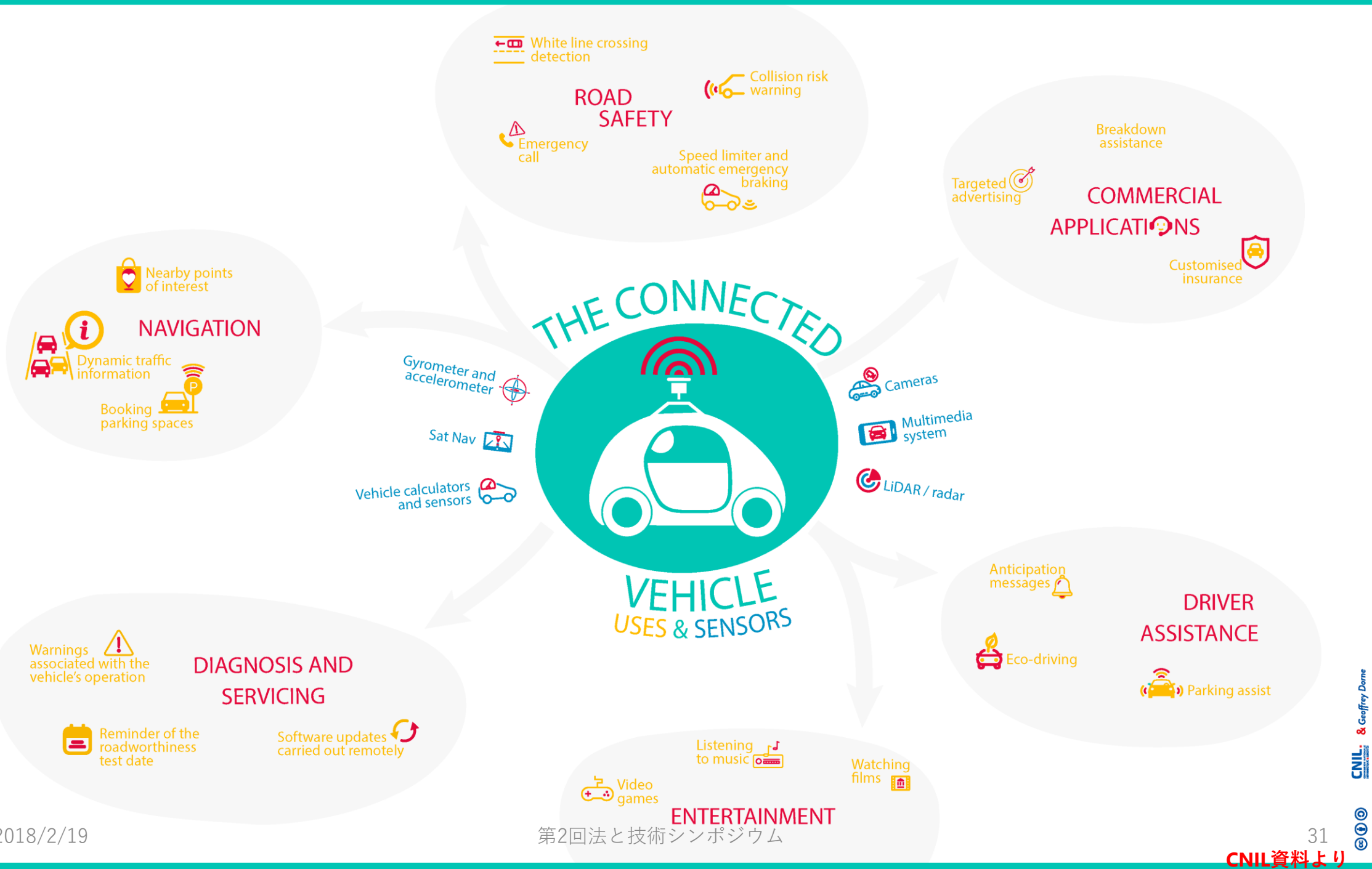
②外国でコネクティッドカー関連サービスを提供し，サーバを当該外国に置くが，更に日本又は第三国のサーバに移転される場合（法人が異なる場合）



越境データ移転部分の分析

- 個人データを取得したデータ管理者が移転する場合は越境データ移転の問題（越境移転先が管理者か処理者かはサービスによる）
- 移転の根拠
  - 同意
  - 契約の履行
  - 標準契約約款（同一法人間で用いられるかは疑問，準拠法は「データ輸出国」）
  - 拘束的企業準則（楽天が取得，IIJ，富士通が申請）
  - 十分性決定

- GDPRの直接適用や域外適用の問題は全く別


White line crossing detection
Collision risk warning
ROAD SAFETY
Emergency call
Speed limiter and automatic emergency braking
Breakdown assistance
Targeted advertising
COMMERCIAL APPLICATIONS
Customised insurance
Nearby points of interest
NAVIGATION
Dynamic traffic information
Booking parking spaces
THE CONNECTED VEHICLE
USES & SENSORS
Gyrometer and accelerometer
Sat Nav
Vehicle calculators and sensors
Cameras
Multimedia system
LiDAR / radar
Anticipation messages
DRIVER ASSISTANCE
Eco-driving
Parking assist
Warnings associated with the vehicle's operation
DIAGNOSIS AND SERVICING
Reminder of the roadworthiness test date
Software updates carried out remotely
Listening to music
Watching films
Video games
ENTERTAINMENT

CNIL資料より