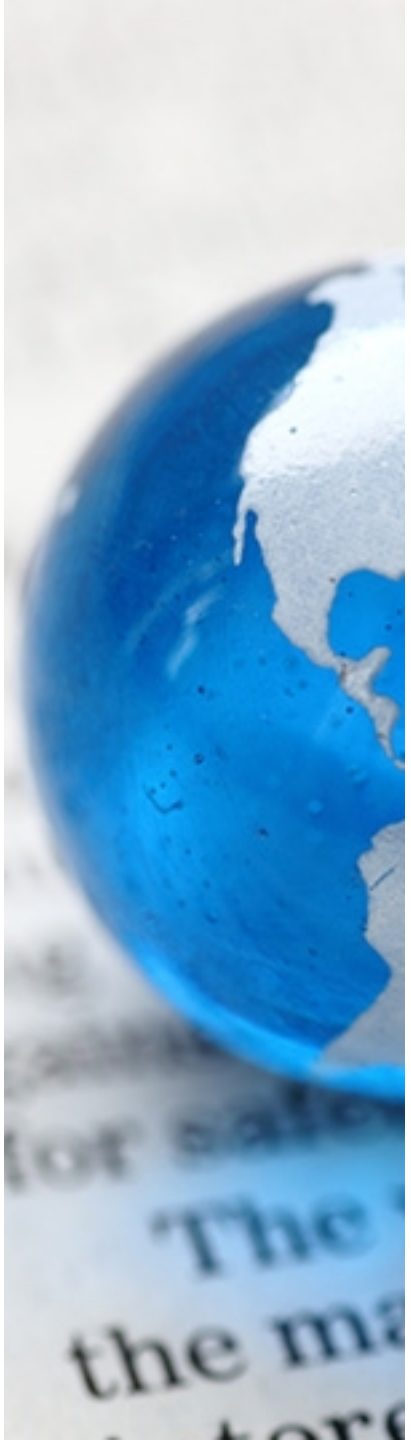
個人情報保護法改正における論点　及び
ニューノーマルにおけるパーソナルデータ活用のあり方



野村総合研究所

ICTメディア・サービス産業コンサルティング部　小林慎太郎　藤原彬人
DXコンサルティング部　南島安平
コーポレートイノベーションコンサルティング部　渡辺翔太

2020年7月2日

NRI

Share the Next Values!

本日お話させていただくこと

テーマ１：提供先で個人データとなる情報の第三者提供の制限

テーマ２：仮名加工情報

テーマ３：国際的な動向（域外適用・越境移転）

テーマ４：ニューノーマルにおけるパーソナルデータ活用のあり方

個人情報保護法の
改正項目のうち、
データ利活用と国際関係
をとりあげます

本日取り上げるテーマと個人情報保護法の改正項目との関係

1．個人の権利の在り方

- **利用停止・消去等の個人の請求権**について、不正取得等の一部の法違反の場合に加えて、**個人の権利又は正当な利益が害されるおそれがある場合にも要件を緩和**する。
- **保有個人データの開示方法**（※）について、**電磁的記録の提供を含め、本人が指示できる**ようにする。

（※）現行は、原則として、書面の交付による方法とされている。

- 個人データの授受に関する**第三者提供記録**について、**本人が開示請求できる**ようにする。
- ６ヶ月以内に消去する**短期保存データ**について、保有個人データに含めることとし、**開示、利用停止等の対象**とする。
- オプトアウト規定（※）により第三者に提供できる個人データの範囲を限定し、**①不正取得された個人データ、②オプトアウト規定により提供された個人データについても対象外**とする。

（※）本人の求めがあれば事後的に停止することを前提に、提供する個人データの項目等を公表等した上で、本人の同意なく第三者に個人データを提供できる制度。

2．事業者の守るべき責務の在り方

- 漏えい等が発生し、個人の権利利益を害するおそれがある場合（※）に、**委員会への報告及び本人への通知を義務化**する。

（※）一定数以上の個人データの漏えい、一定の類型に該当する場合に限定。

- **違法又は不当な行為を助長する**等の**不適正な方法**により個人情報を利用してはならない旨を明確化する。

3．事業者による自主的な取組を促す仕組みの在り方

- 認定団体制度について、現行制度（※）に加え、**企業の特定分野(部門)を対象とする団体を認定できるようにする。**

（※）現行の認定団体は、対象事業者のすべての分野（部門）を対象とする。

テーマ２

4．データ利活用に関する施策の在り方

- イノベーションを促進する観点から、氏名等を削除した**「仮名加工情報」を創設**し、内部分析に限定する等を条件に、**開示・利用停止請求への対応等の義務を緩和**する。
- 提供元では個人データに該当しないものの、**提供先において個人データとなることが想定される情報の第三者提供**について、**本人同意が得られていること等の確認を義務**付ける。

テーマ１

5．ペナルティの在り方

- 委員会による命令違反・委員会に対する虚偽報告等の**法定刑を引き上げる**。

（※）命令違反：6月以下の懲役又は30万円以下の罰金
→ 1年以下の懲役又は100万円以下の罰金
虚偽報告等：30万円以下の罰金 → 50万円以下の罰金

- データベース等不正提供罪、委員会による命令違反の罰金について、法人と個人の資力格差等を勘案して、**法人に対しては行為者よりも罰金刑の最高額を引き上げる**（法人重科）。

（※）個人と同額の罰金（50万円又は30万円以下の罰金） → 1億円以下の罰金

テーマ３

6．法の域外適用・越境移転の在り方

- 日本国内にある者に係る個人情報等を取り扱う外国事業者を、**罰則によって担保された報告徴収・命令の対象**とする。
- 外国にある第三者への個人データの提供時に、**移転先事業者における個人情報の取扱いに関する本人への情報提供の充実等**を求める。

※　その他、本改正に伴い、「行政手続における特定の個人を識別するための番号の利用等に関する法律」及び「医療分野の研究開発に資するための匿名加工医療情報に関する法律」においても、一括法として所要の措置（漏えい等報告、法定刑の引上げ等）を講ずる。

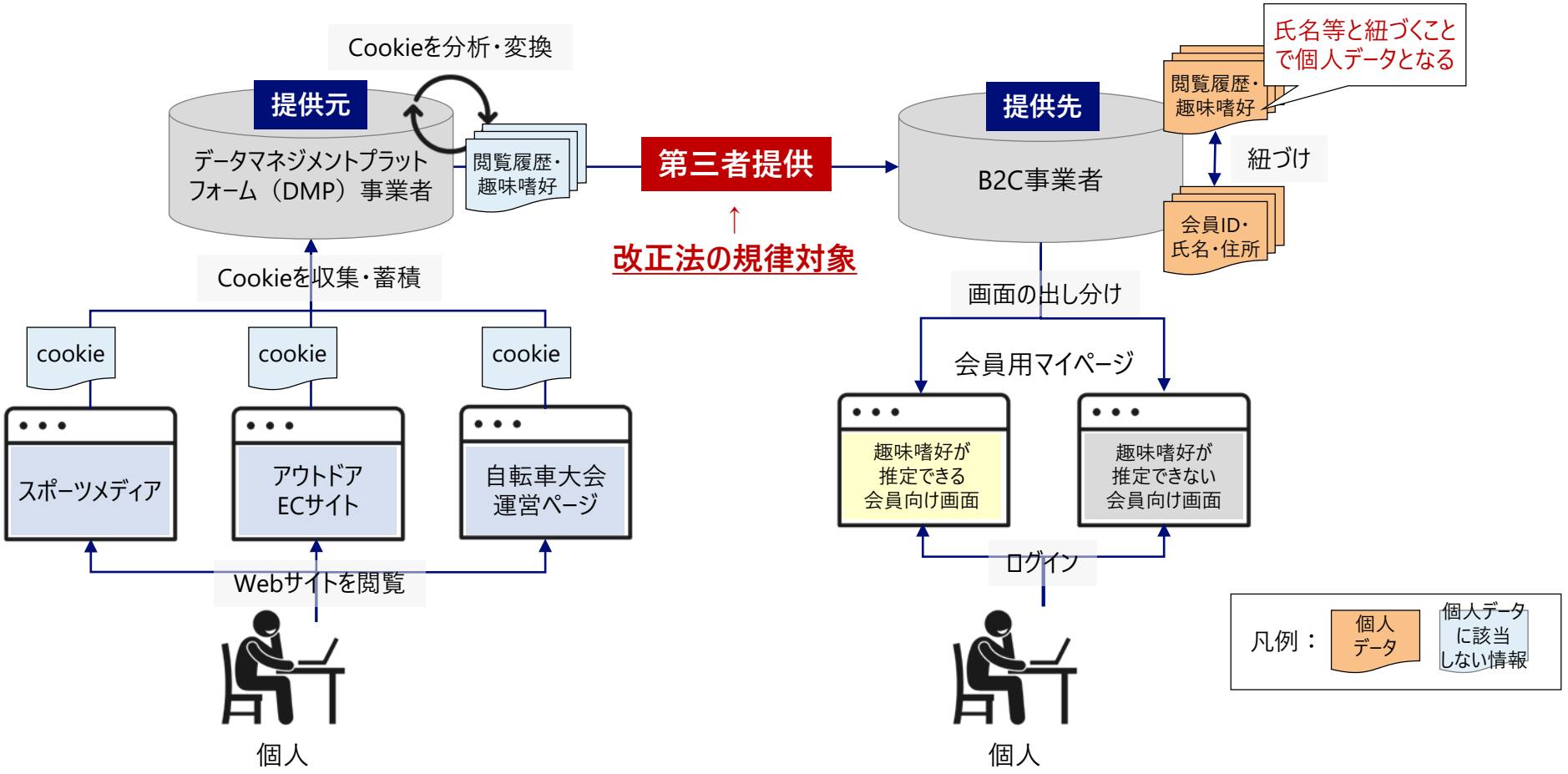
出所）個人情報保護委員会「個人情報の保護に関する法律等の一部を改正する法律案（概要）」（2020年3月10日）に加筆して作成

テーマ１：提供先において個人データとなる情報の第三者提供の制限

テーマ１：提供先において個人データとなる情報の第三者提供の制限

提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供について、本人同意が得られていること等の確認が義務付けられる。

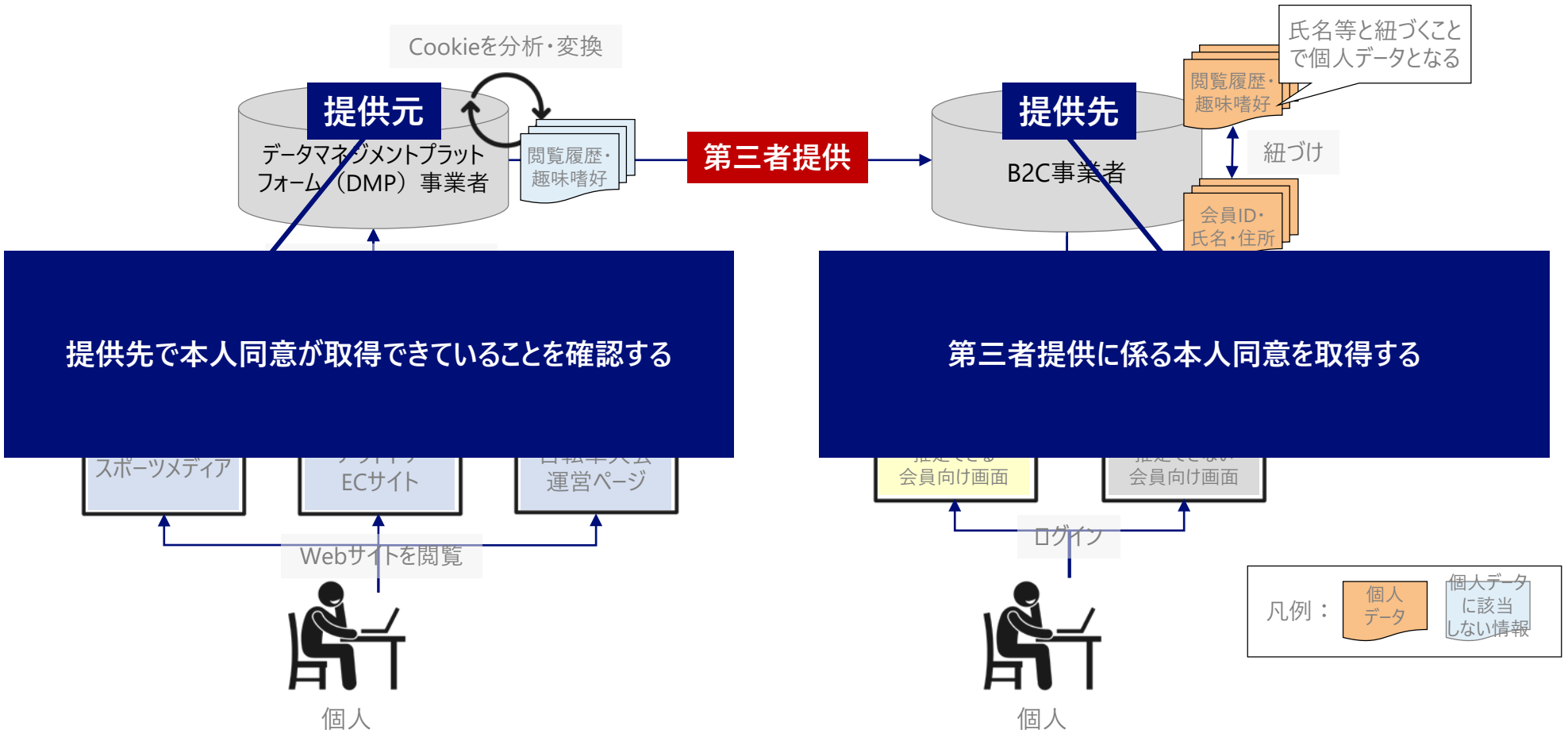
提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供の例



テーマ１：提供先において個人データとなる情報の第三者提供の制限

規律対象となる第三者提供を行う場合、提供先の事業者は本人同意の取得が義務付けられ、提供元の事業者は同意取得有無の確認が義務付けられる。

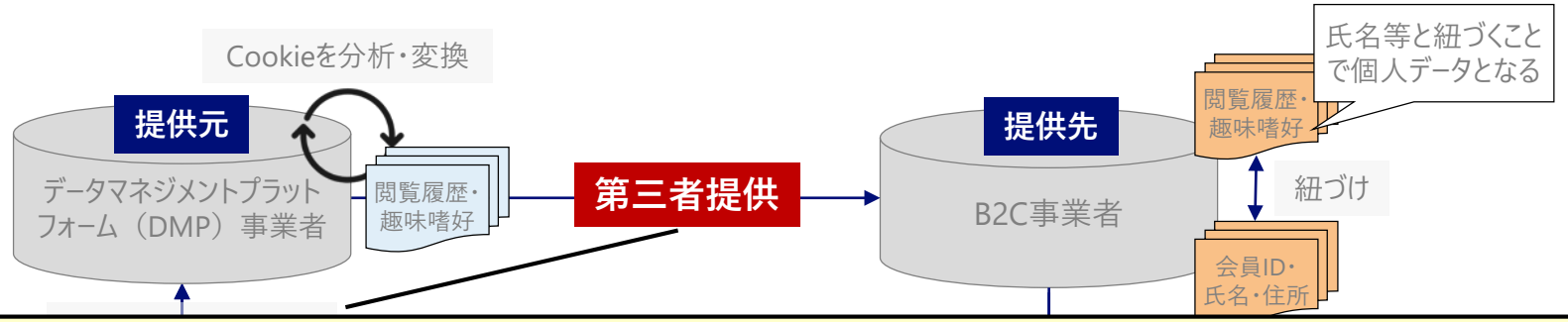
規律対象となる第三者提供を行う際に事業者に課せられる主な義務



テーマ１：提供先において個人データとなる情報の第三者提供の制限

国会答弁により、規律対象となる第三者提供の考え方や事業者による同意取得・確認の方法について具体化が図られつつある。

提供元では個人データに該当しないものの、提供先において個人データとなることが想定される情報の第三者提供の例



【提供先で個人データとなることが想定される場面】

- 提供先が個人データとして取得することを**提供元の事業者が想定している場合**
  例）事前に情報を受領した後に、他の情報と照合して個人データにするといった旨を告げられている場合

- 取引状況等の事情に客観的に照らして、個人データとして取得することが**一般人の認識を基準として想定できる場合**
  例）プラットフォーマーなどに対し情報を提供する際、提供先のプラットフォーマーが当該情報を氏名等で紐づけて利用することを想定しつつ、そのために用いる固有ＩＤ等を併せて提供する場合

※ 提供先による同意取得方法はガイドライン、提供元による同意取得有無の確認方法は委員会規則にて明らかになる予定

第201回 参議院 内閣委員会 第13号 会議録（令和２年６月４日）

テーマ１：提供先において個人データとなる情報の第三者提供の制限

利用規約の改正やWebサイトの改修など、提供元・提供先の事業者双方に相応の対応が求められることから、施行規則・ガイドラインの制定を待たず準備を進めることが肝要と考える。

規律対象となる第三者提供を行う際の義務への対応例

提供先 **（B2C事業者など）**	➢ **第三者提供を受けた個人関連情報※を個人データと紐づけた利用を行うにあたり、本人同意を取得する（利用規約の改正や同意の取り直しが生じる）** ➢ **上記本人同意を得ている個人データとそうでない個人データとを峻別し、マーケティング施策等の実施にあたり管理する（Webサイトの改修が生じる）**
提供元 **（DMP事業者など）**	➢ **データ提供の契約書面において提供先となる事業者が本人同意を取得する旨、確認する条項を挿入する**

※　個人関連情報：生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないもの
具体的には氏名と結び付いていないインターネットの閲覧履歴、位置情報、クッキー等などが含まれる

テーマ１：提供先において個人データとなる情報の第三者提供の制限

本人同意の取得を適切に行うツールとして、コンセント・マネジメント・プラットフォームの導入や、同意取得済のデータを流通させる仕組みとして「情報銀行」の利用促進が考えられる。

コンセント・マネジメント・プラットフォーム（CMP）の概要

- Webサイトやアプリ上で、閲覧・利用者のデータ取得・利用に係る同意を取得し、管理するためのツール
- 2019年に広告に関する国際的な業界団体IAB Europe　がTransparency& Consent Framework（TCF2.0）の枠組みを策定し、同枠組みに基づくツールを提供するCMPベンダーが欧米を中心に登場しつつある

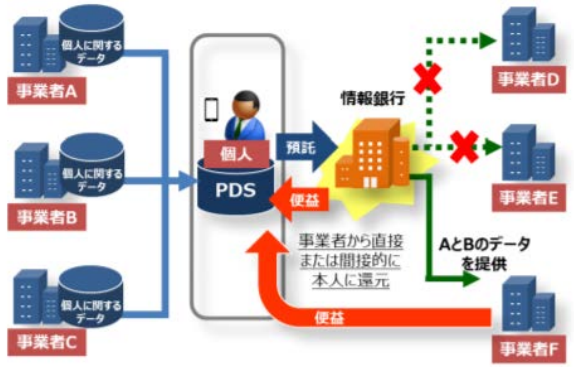
CMPの画面イメージ

利用目的や第三者提供先ごとに同意を取得することができ、適切な同意取得・管理につながる

「情報銀行」の概要

- 個人と「情報銀行」となる事業者との間で、データの活用等に関する契約を締結し、個人から預託を受けた情報を「情報銀行」は他の事業者へ提供する仕組み
- 預託対象となるデータ項目として、氏名・住所等以外にも購買履歴等の履歴情報が想定されている

「情報銀行」のイメージ



※ 本人には便益が還元されず、社会全体にのみ便益が還元される場合もある。

「情報銀行」の仕組みを利用することで、適切な情報の流通につながる

（出所）一般社団法人 日本ＩＴ団体連盟情報銀行推進委員会「「情報銀行」認定申請ガイドブック ver 1.0 」

まとめ

■ 改正法により、提供元では個人データに該当しないものの、**提供先において個人データとなることが想定される情報の第三者提供**について、**規律がかかる**ようになる。

■ 規律対象となる第三者提供を行う場合、主に以下の対応が事業者には義務付けられる。

- 提供先の事業者：**第三者提供に係る本人同意の取得**
- 提供元の事業者：提供先事業者による**同意取得有無の確認**

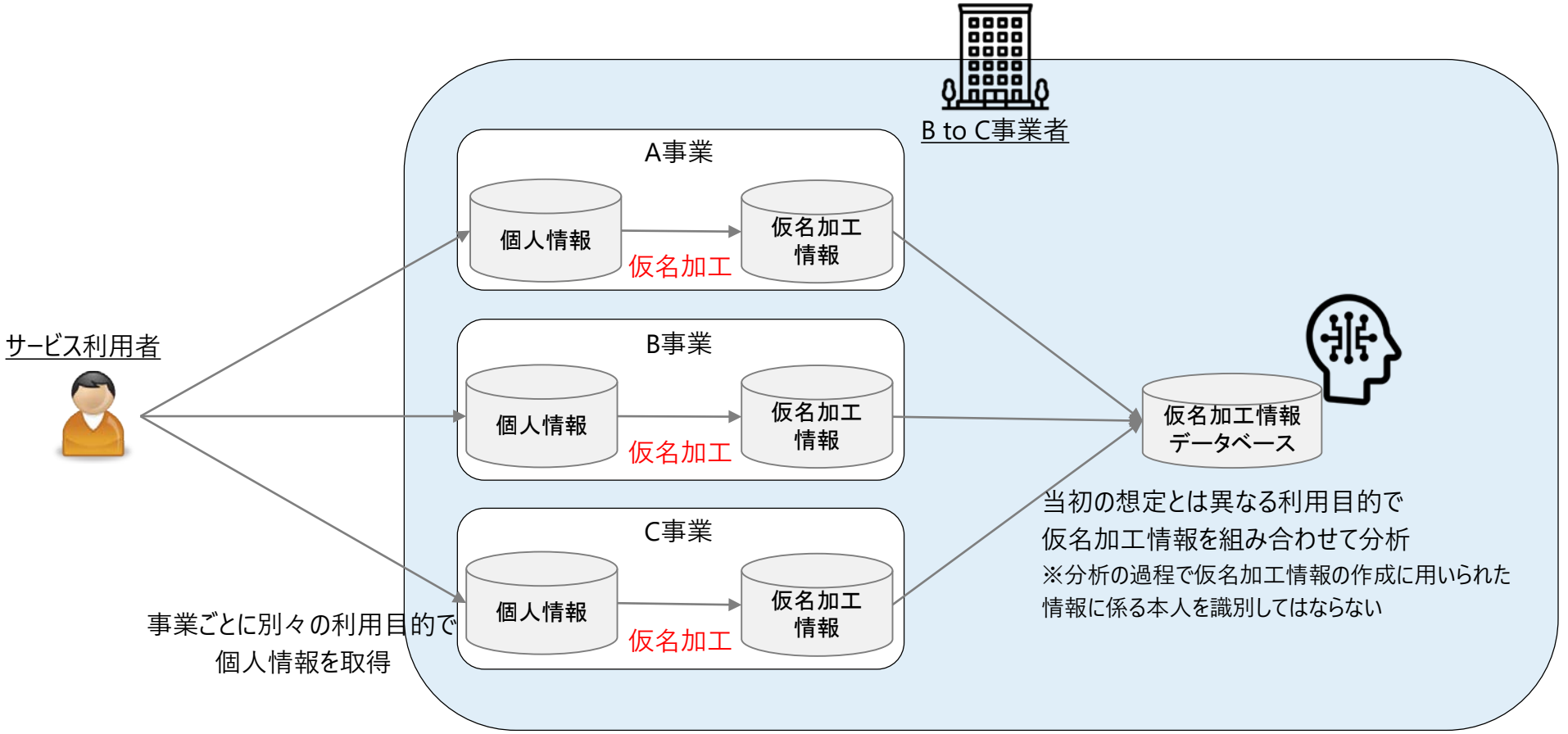
■ 義務化に対し、利用規約の改正やWebサイトの改修など、提供元・提供先の事業者双方に相応の対応が求められることから、**施行規則・ガイドラインの制定を待たず準備を進めることが肝要**と考える

■ 本人同意を取得した上で個人データを第三者に提供することの重要性が増すことから、同意取得を適切に行うツールとして、**コンセント・マネジメント・プラットフォームの導入**や、同意取得済のデータを流通させる仕組みとして**「情報銀行」の利用促進が今後進む**ことが考えられる。

テーマ２：仮名加工情報

仮名加工情報の活用イメージ

想定される活用事例：それぞれ別の利用目的で取得した個人情報を、同一事業者が新たな利用目的で組み合わせて活用するケース



（参考）個人情報保護委員会は、「仮名加工情報」の活用事例として、以下の2つを挙げている。（内閣府規制改革推進会議第7回成長戦略ワーキンググループ資料1-2より）
①当初の利用目的としては特定されていなかった新たな目的で、データセット中の特異な値が重要とされる医療・製薬分野における研究用データセットとして用いるケースや、
不正検知等の機械学習モデルの学習用データセットとして用いるケース等。
②事業者が過去に取得した個人情報を新たな形で利活用（特定の個人を識別する必要のないもの）したい場合に、
その利活用が、当初に特定した利用目的の範囲内に該当するものであるか、判断に迷うようなケース。

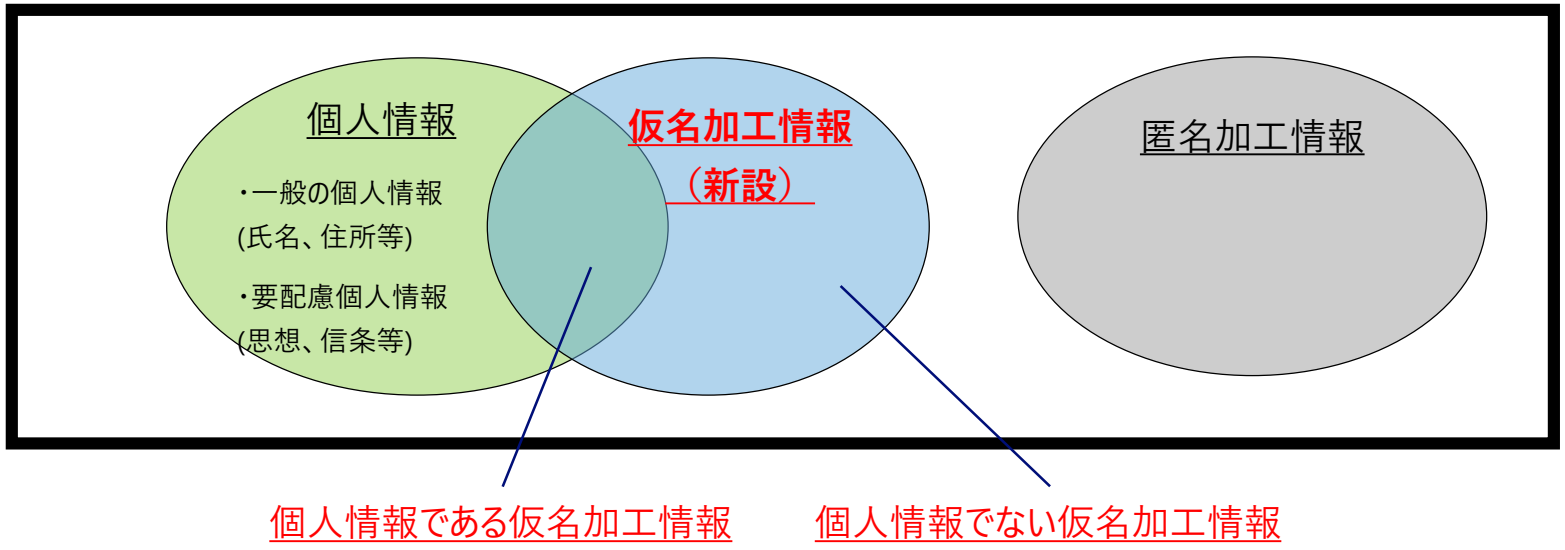
仮名加工情報

事業者内におけるイノベーション促進のため、改正法で新たに「仮名加工情報」の制度を導入。

■ 仮名加工情報とは

- 「仮名加工情報」とは、「他の情報と照合しない限り特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報」（改正法第2条の9）である。
- 「仮名加工情報」は、**個人情報と匿名加工情報の中間的規律**として位置付けられている。（「個人情報保護法　いわゆる３年ごと見直し　制度改正大綱」より）
- **加工基準や求められる安全管理措置は、個人情報保護委員会規則で定められる予定**となっている。

仮名加工情報の位置づけ



仮名加工情報

事業者の内部でデータを柔軟に活用できる「仮名加工情報」
外部とのデータ連携で活用できる「匿名加工情報」

- 現行法では、既にデータ流通を目的として創設された「匿名加工情報」制度が存在しているが、加工基準が厳しく、またデータの粒度が粗くなってしまうため、一部業界を除いて活用が進んでいない。
- 「仮名加工情報」は、内部利用に限定されるが「匿名加工情報」より緩い加工基準で作成でき、利用できる情報が多いため、**事業者内部におけるイノベーションを促進する制度**である。

仮名加工情報と匿名加工情報の活用シーンの比較

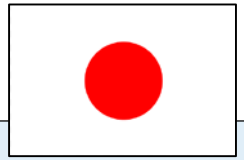
	仮名加工情報	匿名加工情報
内部/外部	• 内部利用	• 外部利用（データ連携）
活用の具体例	• 社内の複数の事業で別々の利用目的で取得した個人情報を、事業横断的に活用したい場合 • 社内で保持するデータを、AIの学習や分析に活用したい場合	• 社内の個人情報をもとに外部の研究機関と共同で分析・研究を行う際、本人から同意を取得することが困難である場合

仮名加工情報

EUの一般データ保護規則（以下GDPR）では「仮名化データ」を安全管理措置の一環として導入。日本の改正法においても、その考え方が一部参考にされている。

2018年施行のGDPRで導入

- GDPRにおける"pseudonymised data（仮名化データ）"は原則としては**安全管理措置の一環**だと考えられている。
- 仮名化を施すことで、個人データを活用しやすくなる規定がいくつか設けられている。
  - 例：個人データを取り扱う際の保護措置の1つとして仮名化が施されていると、「正当な利益」の目的のためにその取扱いが必要と判断されやすくなる可能性がある。
- EU域内では、各種機関が発行するガイドラインでユースケースや事業者が守るべき行動規範が示される等、徐々にノウハウが蓄積してきている。



今回の法改正で導入

- 今回の法改正前から、一部の事業者は**安全管理措置として**個人情報を仮名化して管理していた。
- 今回の法改正では、「仮名加工情報」の制度を導入することで、一定の安全管理措置がとられているとして、事業者内部での活用において規制が緩和されたと思われる。

仮名加工情報

「仮名加工情報」には、個人の請求権に係る義務が適用除外になる等のメリットがある。一方、第三者提供が制限される等、注意が必要。

■ 特に、「個人情報でない」仮名加工情報の第三者提供ができない点に注意が必要である。

- 本来個人データ以外は第三者提供の制限が適用されないが、**仮名加工情報になると第三者提供ができず、規制強化ではないか**という声がある。
- **仮名加工情報を作成した場合に対外的な宣言は不要である（＝事業者自ら、仮名化されたデータと仮名加工情報を区別する必要がある）と思われる**ため、仮名加工情報として取り扱う場合には第三者提供ができない点を認識したうえでメリットを享受しなければならない。（今後の委員会規則を要注視）

メリット

保持しているデータの内部での利用価値が高まる

- 当初定めた個人情報の利用目的と合理的な関連性がない利用目的であっても、利用することが可能（第15条2項）

事業者内での管理コストが下がる

- 開示、利用停止等の個人の請求権に対応する義務が緩和（第28～34条）
- 仮名加工情報を漏えい時に、当局への報告や本人への通知が不要（第22条の2）
- 取扱事業者の名称等の公表が不要（第27条）

注意が必要な点

第三者提供ができない

- 法令に基づく場合を除いて、第三者提供はできない（第35条の2の6項）

漏えい等防止のため保護措置を取る必要がある

- 安全管理措置（第20条）
- 従業者の監督（第21条）
- 委託先の監督（第22条）

（個人情報である場合）利用目的の特定や公表が必要

- 個人情報である仮名加工情報の場合、利用目的の変更が柔軟にできるようになるが、変更後も利用目的の特定と公表は引き続き必要（第15条1項、第18条）

まとめ

1. 改正法で新たに導入された「仮名加工情報」は、事業者内部でのデータ活用促進のための制度である。
   - ある事業者がそれぞれ別の利用目的で取得した個人情報を仮名加工して、新たな利用目的のために組み合わせて活用するケースが想定される。
   - 事業者内部での活用に限定した「仮名加工情報」は、データ流通を目的とした「匿名加工情報」より、加工基準は緩く設定されると思われる。
   - EUのGDPRでは「仮名化データ」が安全管理措置の一環として導入されており、それによって一部の規制を緩和する考え方が日本の改正法においても参考にされている。

2. 「仮名加工情報」の活用にあたっては、そのメリットと注意が必要な点の両面を注視する必要がある。
   - 「仮名加工情報」は、利用目的の変更が柔軟に行えたり、本人からの請求権が及ばなかったりする等、事業者にとって活用のメリットがある。
   - 一方、本来第三者提供の制限がかからない非個人情報であっても、「仮名加工情報」となることで第三者提供ができなくなるため、利用目的に鑑みて活用の是非を検討することが重要である。

テーマ３：国際的な動向（域外適用・越境移転）

テーマ３：国際的な動向（域外適用・越境移転）

データの越境移転や法の域外適用に対する規律は強化。消費者向けには同意取得における透明性向上、企業向けには海外事業者との競争条件の平等を目的としている。

■ 域外適用とは外国の事業者に対して日本法を適用すること、越境移転とは日本から国外の事業者に対する個人情報の第三者提供を指す。現行法上、越境移転は原則禁止され、①同意、②相当措置、または③十分性認定がある場合のみ許容される（以下、これらを総称して「越境移転オプション」と呼ぶ）。

越境移転における情報提供義務の拡大

（１）越境移転の同意取得に際して、下記の情報提供が義務化（第24条第2項）

- 移転先国の個人情報保護制度
- 移転先組織の個人情報保護措置、等

以上の追加的な情報提供義務については、施行日より適用され、遡及しない（附則第4条）

（２）本法上事業者が講ずべき措置に相当する措置（相当措置）に基づく移転の場合には、相当措置に関する情報提供が義務化（同条第3項）

本人がより適切に移転先の国や組織のリスクを認識して同意を与えられることとなる

域外適用における委員会の執行能力の強化

個人情報保護委員会に下記の権限が追加

- 外国に所在する事業者に対する報告徴収、立入検査、命令の権限（第75条）
- 送達規定（第58条の3）
- 公示送達（期間は6週間）（第58条の4）

域外適用が認められる電気通信事業法と同様、海外事業者とのイコールフッティングを主な目的とする。

テーマ３：国際的な動向（域外適用・越境移転）

越境移転における透明性強化は世界的に珍しい立法。日本の推進するDFFT※との関係で理解することが重要であり、産業界も透明性向上による消費者との「信頼」形成が求められる。

- 情報開示の強化はGDPR水準を超え国際的に前例がない。移転先国の政策によって個人データに関する権利が制限されたり不適切に利用されるリスクを本人に明示し、本人の関与を拡大することが立法趣旨である。
- 上記規律強化に対応する日本企業には、DFFTとの関係を意識して、**特にローカライゼーションやガバメントアクセス（GA）等に関する情報提供が求められることとなると考えられる。**
  - 現時点の提供すべき情報として、移転先国名、個人情報保護制度などが想定。制度について、事業者が移転先の環境を認識するために企業独自の取組が望まれるが、委員会も参考情報を提供予定（令和2年6月4日参議院、其田局長答弁）。

法改正の背後にある諸外国のデータ関連政策が引き起こすリスクと法改正における対応方針

諸外国のデータ関連政策とその引き起こすリスク	
データ・ローカライゼーション政策	本人による消去請求に越境移転先事業者が対応できないリスク
外国政府による無制限なガバメント・アクセス	我が国で取得され越境移転された個人データが不適切に利用されるリスク

法改正におけるリスク対応の方針

- 2019年G20会合でDFFT概念が合意された。
- 国家間では相互に信頼性を確保した自由なデータ流通を促進する必要性あり
- **個人データのフリー・フローを支える信頼を事業者と本人の間においても確保することが重要**

※DFFT（(Data Free Flow With Trust)）とは、2019年1月のダボス会議で安倍総理大臣が提唱した概念。個人データや安全保障機密等は保護されるべきであるが、非個人データは自由な越境流通を可能とする制度枠組みを指す。

出所）個人情報保護委員会「制度改正大綱」よりNRI作成

（参考）個人情報保護とGAの関係については、下記を参照。

今日、サイバー空間に対する諜報活動の重要性が増す一方、他国民を含むプライバシー侵害の懸念が生じている。また、諜報活動は秘匿性が高く、それゆえ産業スパイ的な活動等の濫用の懸念も指摘される。こうした懸念から近年、GAを理由として自国からのデータの越境移転制限が欧米等で生じているが、このような制限はデータの自由流通を阻害するため、既存の通商協定との抵触や日本の進める信頼ある自由なデータ流通（DFFT）との関係でも問題を生じ得る。

現状、EUや米国では、GAに対して一定の条件が満たされない限り個人データの国外移転を制限している。こうしたデータの越境移転制限について、GATS上はデータの移転制限には規律が及ばないがサービス提供を阻害する措置として問題となり得るほか、CPTPPでは制限そのものに規律を及ぼすが、両協定においてプライバシー保護や安全保障を理由として措置が正当化される余地があることを明らかにした。

出所）https://www.rieti.go.jp/jp/publications/dp/19j067.pdf

テーマ３：国際的な動向（域外適用・越境移転）

日本企業は、改正法の施行規則などを踏まえつつ、越境移転オプションのメリット/デメリットを比較して、いかに信頼性を担保しながら越境移転を実施するか検討するべき。

法改正を踏まえた越境移転オプションの概要と評価（メリット/デメリット）

		オプションの概要	法改正に伴うオプションの評価と対処方針
同意		• 移転先国・組織の保護水準を開示して本人同意を取得（開示範囲は現時点では不明）。	• 開示範囲拡大によって対応コストが上昇し、評価は下がる。 • 依拠を継続する場合、今後の開示範囲の明確化に注意して、関連する社内規程の改正が必要。
相当措置	独自	• 企業が日本の個人情報保護法で求められるものと同等の水準を移転先に整備。	• 開示義務が規定されたことで説明責任が拡大し、評価は下がる。 • 依拠を継続する場合、今後の開示範囲の明確化に注意して、関連する社内規程の改正が必要。
	法定	• GDPR上のBCRやSCC※、APEC・CBPRなど組織単位での個人情報保護体制を担保する枠組を活用。 （注：相当措置は正式にはCBPRのみが認定）	• テンプレートが存在するため取り組みやすく、開示対応も容易である。 • 日本法との対応関係には引き続き留意する必要がある。
十分性認定		• 個人情報保護委員会が外国の個人情報保護制度を評価して決定。現在EU・EEA加盟国のみ。 • 企業にとって直接の関与は困難。	• 企業の関与可能性が低く評価はもともと低い。 • 大量のデータを特定国に移転している場合、政府への働きかけを検討する余地はある。

※BCR：拘束的企業準則、SCC:標準契約条項

テーマ３：国際的な動向（域外適用・越境移転）

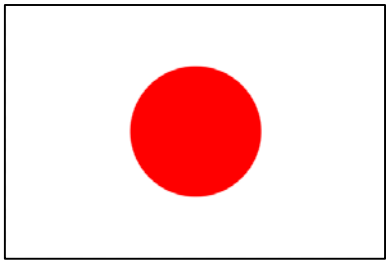
法改正と並行し、個人情報保護委員会はDFFT形成に向け、日欧米3極によるデータ自由流通圏を構築しつつあるが、日本から米国への移転には依然として同意または相当措置が必要。

米EUプライバシーシールド（PS）に基づく移転が可能

米国の現行法には越境移転規制がなく、対応不要

米国の現行法には越境移転規制がなく、対応不要

相互認証に基づく移転（EUからの移転データに対する追加的対応を除いて対応不要）



米国には日本からの十分性認定がないため対応が必要（同意、相当措置）

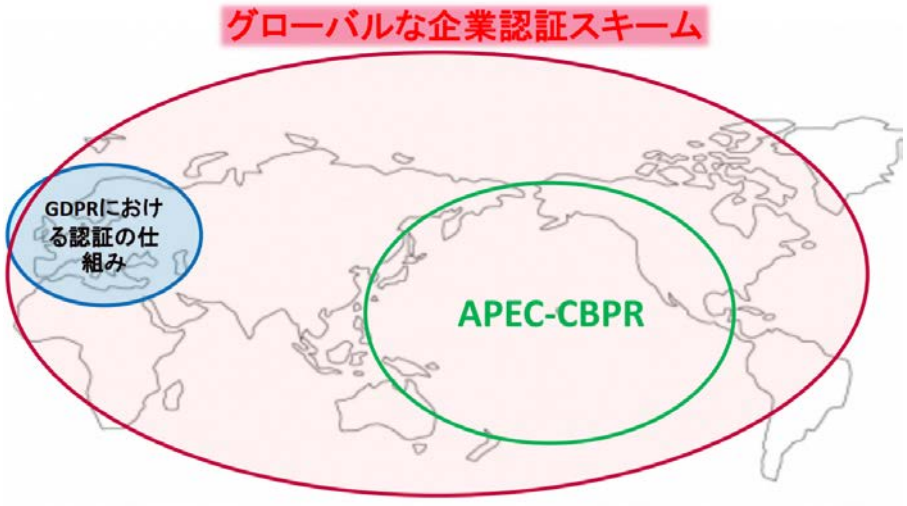
PS類似の枠組を設定？

テーマ３：国際的な動向（域外適用・越境移転）

日本企業は政府に対し、短期的には組織単位の移転スキーム拡大、中長期で相互認証を目指した個人情報保護体制の整備支援を行うよう働きかけるべき。

- 近年、GDPR等の影響もあり、日本に類似した越境移転制限を導入する新興国が拡大。日本企業の展開する新興国と日本のデータフローをどのように確保するかが、改正法を経た政策課題として生じている。
  - シンガポール、マレーシア、タイが導入済み。インドネシア、インドなどが法案を作成済。
- 日本企業にとって海外とのデータフローをいかに確保するかが重要である。短期的には組織単位の移転スキーム拡大、中長期では主要パートナー国の個人情報保護体制の確立に向けた支援が望まれる。

組織単位の移転スキーム拡大



経済的に重要なパートナー国における法整備と、特に法「運用」に向けた支援が重要

国名	法律（案）名	ステータス
シンガポール	Personal Data Protection Act	施行済
マレーシア	Personal Data Protection Act	施行済
タイ	Personal Data Protection Act	施行が1年延期され、2021年6月へ
インドネシア	Data Protection Law	2020年1月法案を国会提出
インド	Personal Data Protection Bill	2019年12月法案を国会提出

出所）個人情報保護委員会事務局「個人データに関する国際的なデータ流通の枠組みに係る進捗について」（令和2年5月15日）

まとめ

1. 法改正により、越境移転における情報提供義務が拡大し、域外適用に向けた委員会の執行権限が強化。
   - 越境移転では、同意取得や相当措置に基づく移転に際して、移転先の国や事業者に関する情報提供の範囲が拡大した。
   - 諸外国でデータローカライゼーションや無制限なGAが拡大し、本人の権利行使が阻害される、または不適切な利用がなされるといったリスクが生じているため、同意取得に際してリスクを明示し、本人関与を拡大する趣旨である。
   - 域外適用では報告徴収、立入検査、命令の権限や、送達関連の規定が整備された。これは、域外に所在する企業への執行権限を強化することで、日本企業と海外企業のイコールフッティングを実現するものである。

2. 情報提供義務の拡大に伴い、日本企業は越境移転に係るオプションを再検討する必要がある。
   - 情報提供義務の拡大にともない、同意や企業独自の相当措置といったオプションの評価が（相対的に）低下する一方で、法定の相当措置（GDPR上のBCRやSCC、APEC・CBPR）の評価が上昇。
   - 同意や企業単位の相当措置に引き続き依拠する場合、開示義務の明確化を踏まえたプライバシーポリシーの改訂等の対応が必要とされる。
   - 今後の展望として、日本企業は政府に対して、日米欧のデータ流通圏構築に向けた米国との関係構築（PS類似の枠組構築）、組織単位の移転スキーム拡大、ASEANなどの重要なパートナー国に対して相互認証を目指した個人情報保護体制の整備支援、といった取り組みを行うように働きかけていくべきである。

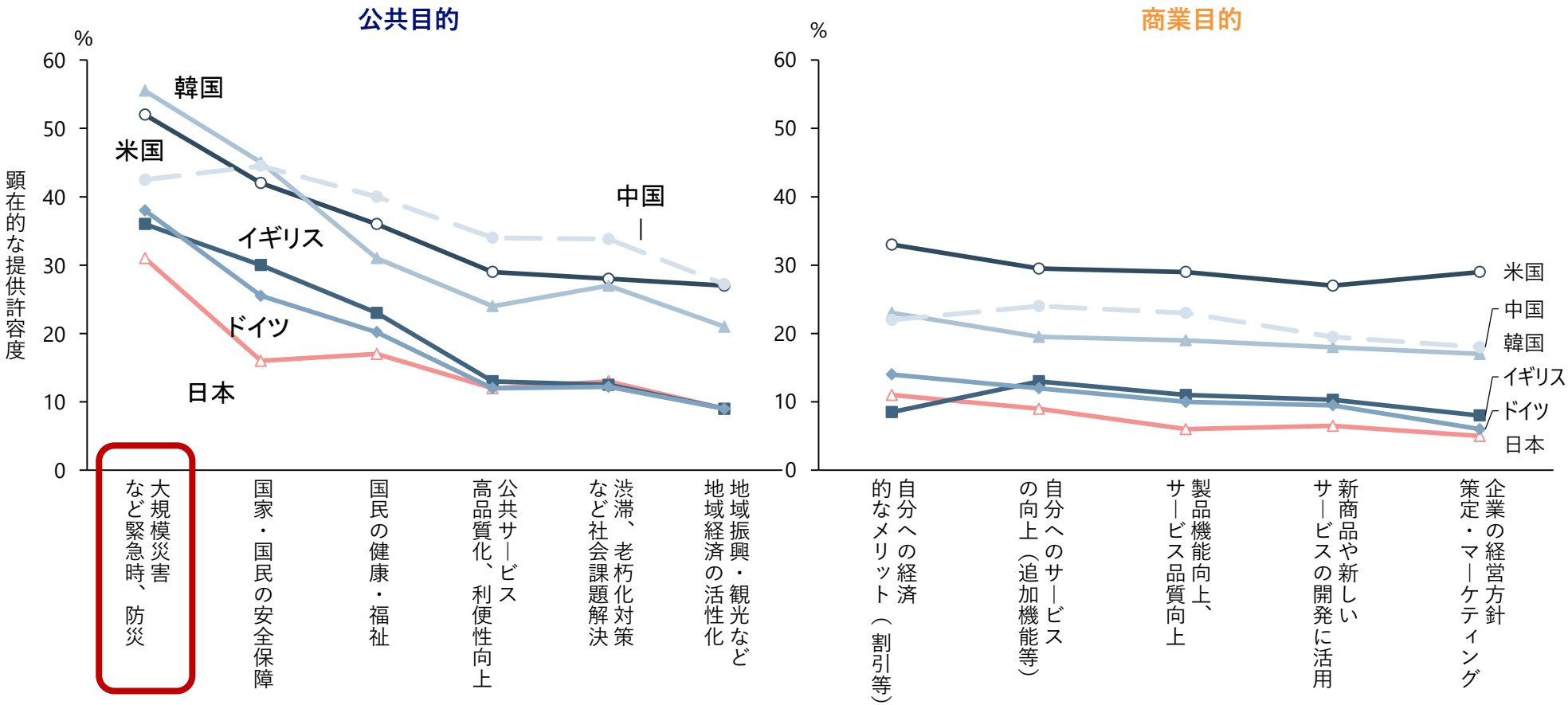
テーマ４ ：ニューノーマルにおけるパーソナルデータ活用のあり方

本節は、新型コロナウィルス対策緊急提言として公表したものを、を本メディアフォーラム用に再構成したものである。
「コロナ禍におけるパーソナルデータ活用のあり方 －「監視社会」ではない「見守り社会」の実現に向けて－」
https://www.nri.com/jp/keyword/proposal/20200610_2

テーマ４ ：ニューノーマルにおけるパーソナルデータ活用

日本人のパーソナルデータ提供に対する許容度は、諸外国と比較して、公共目的、商業目的のいずれの場合も低い。緊急時においても然り。

パーソナルデータの提供に関する許容度（利用目的別）



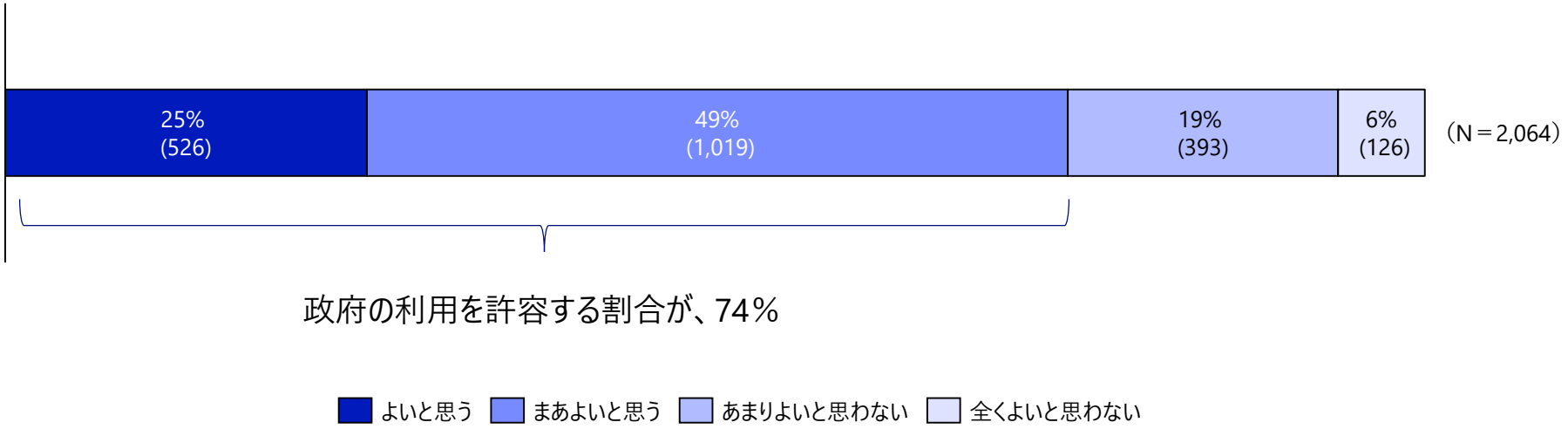
出所）総務省「パーソナルデータ提供等に係る消費者向け国際アンケート調査」（2017年）

テーマ４ ：ニューノーマルにおけるパーソナルデータ活用

一方で、コロナ禍では、データが匿名化されている場合、携帯電話の位置情報であっても、政府の利用を許容する割合は74%と高い。

■ 問：諸外国では新型コロナウイルスの感染拡大状況を把握することを目的として、通信事業者が保有している位置情報を政府が取得・活用しています。日本政府が同様の取組みを行うことはよいと思いますか。最も当てはまるものをお選びください。ただし、位置情報は、個人が特定できないように加工されてから政府が取得するものとします。

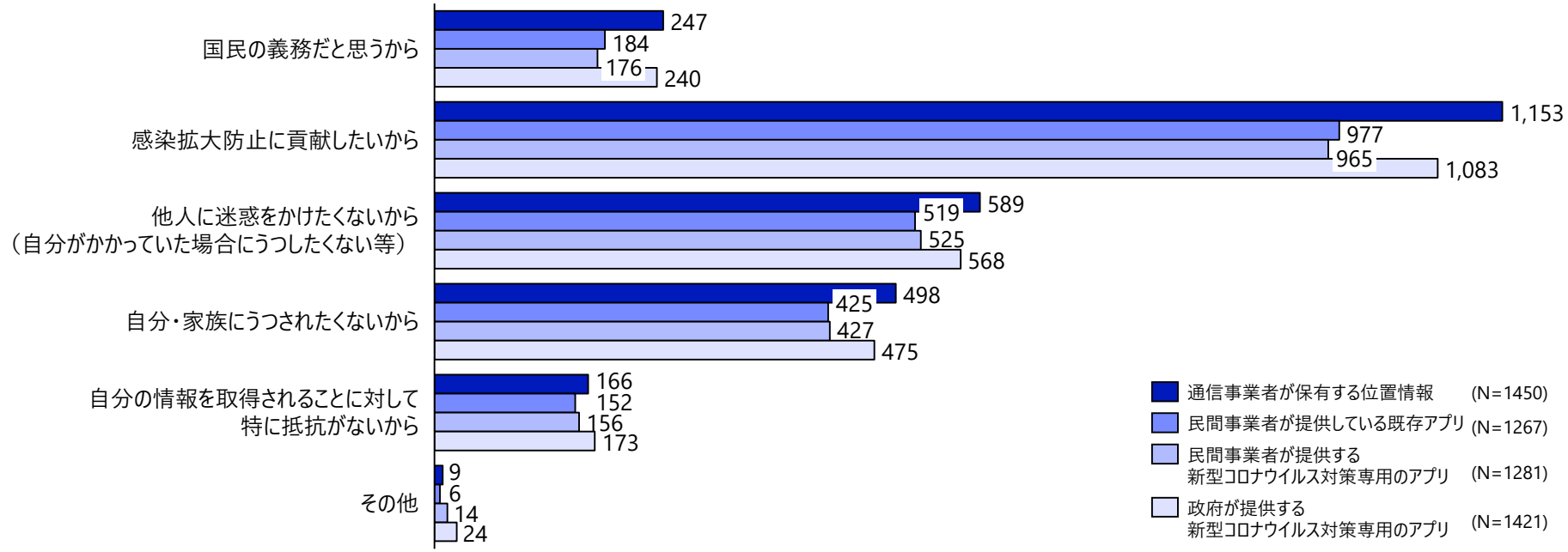
- 位置情報とは、通信を行う際に使用した携帯電話基地局の位置を示す「基地局に係る位置情報」、Wi-Fiアクセスポイントの位置を示す「Wi-Fi位置情報」、GPSで取得する「GPS位置情報」の三種類が存在します。
- 位置情報の精度は概ね数百メートル～数メートルです。



出所）NRI「新型コロナウイルス感染拡大による生活の変化に関するアンケート」（2020年4月）

政府による位置情報のデータ利用を許容する理由は、「感染拡大防止に貢献したいから」が最も高く、「他者に迷惑をかけたくない」といった他者との関係を気にする回答が多かった。

■ 問：政府が次の方法（通信事業者が保有する位置情報、民間事業者が提供している既存アプリ、民間事業者が提供する新型コロナウイルス対策専用のアプリ、政府が提供する新型コロナウイルス対策専用のアプリ）で位置情報を取得することについて、それぞれ「よいと思う」、「まあよいと思う」と感じた理由について、次の中からあてはまるものを全て選んでください。



出所）NRI「新型コロナウイルス感染拡大による生活の変化に関するアンケート」（2020年4月）

テーマ４ ：ニューノーマルにおけるパーソナルデータ活用

感染拡大対策に用いられるパーソナルデータには、厳格なプライバシー保護措置。

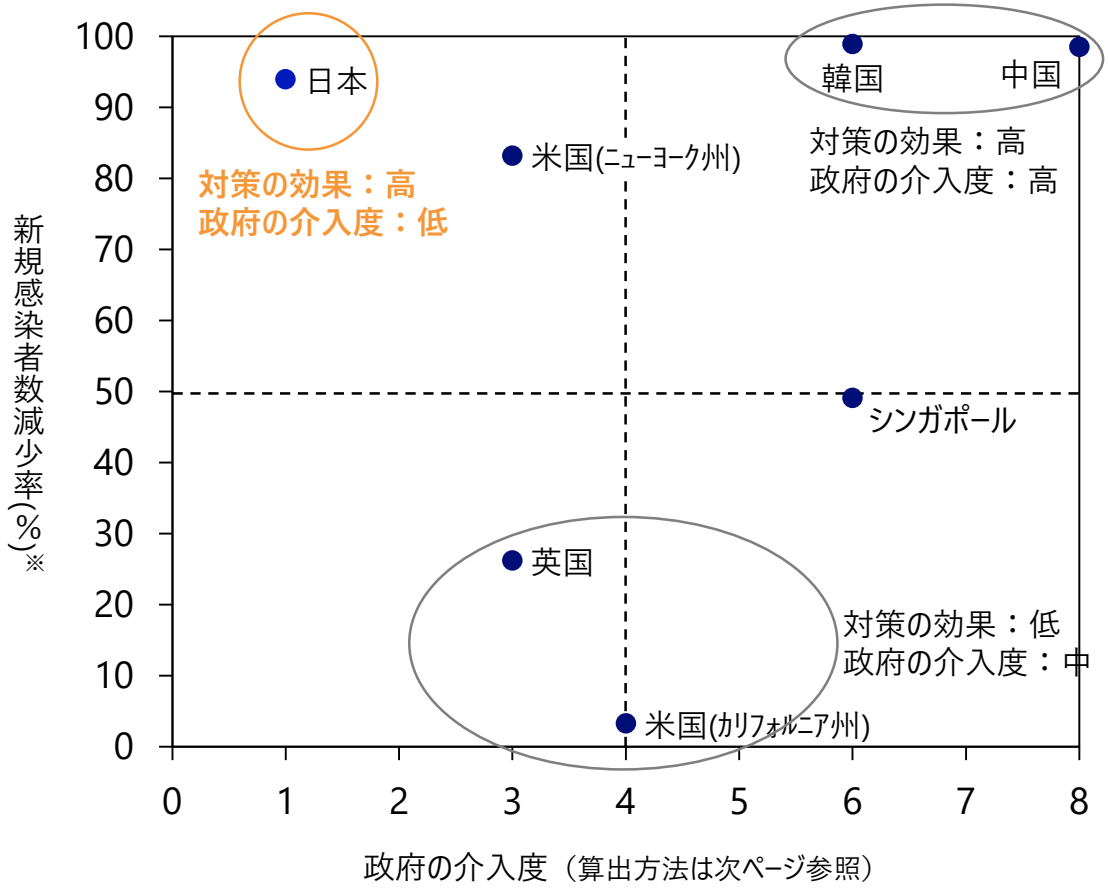
事業者・取組み		概要	取り扱うデータ	プライバシーへの配慮		
				同意取得	情報の消去	その他
位置情報を利活用した大規模統計情報の提供	Yahoo!JAPAN「新型コロナウイルス感染症対策協力プロジェクト」	• 新型コロナウイルス感染症の感染者が特徴的に行うと考えられる検索・購買行動のエリア増減率をもとに、クラスターが発生している可能性のあるエリアを推定する	• 位置情報、検索履歴、購買情報を統計化したもの • 4月20日時点で100万人超	• プロジェクトへの協力に同意、かつ、Yahoo!JAPANアプリ、Yahoo!MAPアプリ（Android版のみ）における位置情報の利用を許可したユーザのみ情報を取得する	• プロジェクト終了後、1年以内に消去する	• アドバイザリーボードの助言を受けながら実施する
	NTT docomo「モバイル空間統計」	• 属性（性・年代・居住エリア）毎のエリア内人口やエリア間を移動する人口や、属性毎の接触頻度（1時間以内に一定の範囲で何人と接触したかを根拠に、どれだけの接触があったかを計算したもの）等を推計する	• 位置情報を統計化したもの • 端末データ（7,800万台分）	• 包括的な同意を取得するとともに、オプトアウトの仕組みを提供している	• なし	• 有識者の助言を受けて作成した統計作成・提供に関するガイドラインを公表している
新型コロナウイルス感染者と接触した可能性等の通知	大阪府「コロナ追跡システム」	• ユーザが訪れた店舗やイベント等に、新型コロナウイルス感染者が同じ日に訪れていた場合、健康管理を促すメールを配信する	• 訪れた店舗・イベント情報 • 訪れた月日 • メールアドレス	• 利用時にサービス規約に同意が必要 • 本人の同意のもと、本人が発症日と陽性判明日を登録する	• 新型コロナウイルス感染症収束後にシステムから消去する	• メール内容に、接触日や接触場所の記載はないが、クラスターが発生した場合、発生場所が記載される
	神奈川「LINEコロナお知らせシステム」	• ユーザが訪れた店舗やイベント等に、新型コロナウイルス感染者が同じ時間帯に訪れていた場合、健康管理を促すLINEメッセージを配信する	• 訪れた店舗・イベント情報 • 訪れた日時 • LINEが神奈川県に対して発行したユーザ識別子	• 利用時にサービス規約に同意が必要 • 接触者への通知に本人の同意はない（保健所を通じて感染報告を受けた神奈川県が、感染者が訪れた店舗やイベント等を訪れたユーザにLINEで通知）	• 2021年3月末に終了予定	• メール内容に、接触日や接触場所の記載はない
	厚生労働省「接触確認アプリ」	• ユーザが新型コロナウイルス感染者と、ウイルス感染者との接触により感染のおそれがある期間に、感染者と概ね1m 以内の距離で継続して15 分以上の　近接状態が続いた場合、健康管理を促すアプリの通知を配信する	• アプリが端末毎に発行した識別子（日時、接触符号） • 厚労省が感染者に割り振る処理番号	• アプリのインストール時に、感染者が処理番号を登録し、自身が感染したことをアプリ上で報告する際に同意を取得する	• アプリが発行した識別子は14日で削除する • 処理番号は登録後即削除する	• プライバシー、セキュリティーの有識者がアプリの仕様検討会に参加し、運用上の留意点を公表している

出所）各種公開情報をもとにNRI作成

テーマ４ ：ニューノーマルにおけるパーソナルデータ活用

日本は、中国・韓国のように強制力を伴う私権制限をせず、かつ欧米と同等以上にプライバシー保護に配慮しながら、感染拡大を抑え込んでいる。

各国の感染拡大抑止策における「政府の介入度」と新規感染者数減少率の関係



出所）NRI

※ 新規感染者数の減少率は、ロックダウン（またはそれに類する外出自粛を促す宣言発令）期間中のピーク時の新規感染者数と、ロックダウン解除日の新規感染者数を比較して算出した。なお、ロックダウンが5月24日時点で解除されていない場合は、5月24日時点の新規感染者数と比較した。

テーマ４ ：ニューノーマルにおけるパーソナルデータ活用

政府の介入度は、外出制限の強制力の強さと、IT施策における政府による情報アクセスとデータ機微度の観点から評価。

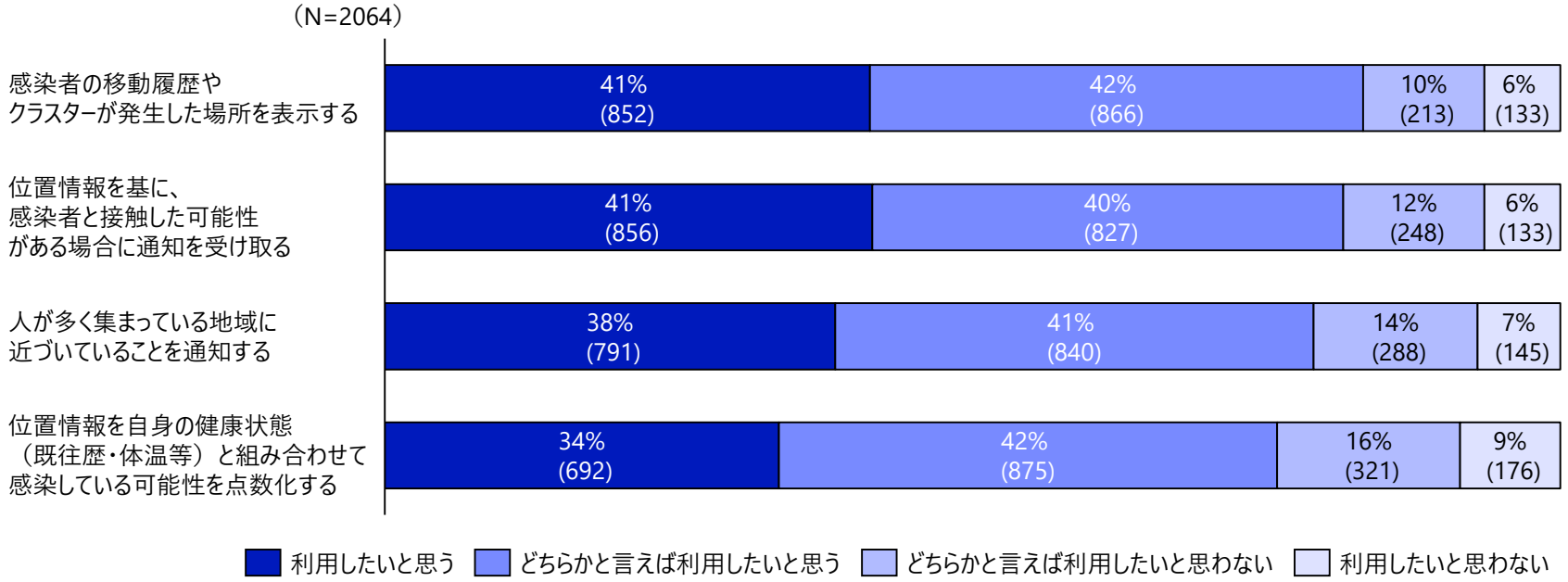
感染拡大抑止策における「政府の介入度」に係る指標

点数	外出制限の強制性		政府がアクセスできるデータのプライバシー性	
	外出の禁止/要請	罰則の強さ	接触者を特定できる情報	データの機微度
2	禁止	罰則あり （罰金＋身体的拘束）	• アプリダウンロードは強制であり、かつ政府は利用者の個人情報をアプリ経由で知ることができる	• 特定の個人が濃厚接触者であるという情報及び位置情報が取得される
1	要請どまり	罰則あり （罰金のみ）	• アプリダウンロードは任意であるが、政府は利用者の個人情報をアプリ経由で知ることができる • またはアプリダウンロードは強制であるが、政府は利用者の個人情報をアプリ経由で知り得ない	• 特定の個人が濃厚接触者であるという情報または位置情報が取得される
0	特に対応なし	罰則なし	• アプリダウンロードは任意であり、かつ政府は利用者の個人情報をアプリ経由で知り得ない	• 特定の個人が濃厚接触者であるという情報及び位置情報のいずれも取得されない

テーマ４ ：ニューノーマルにおけるパーソナルデータ活用

位置情報を活用した感染対策のための情報サービスの利用意向は総じて高い。プライバシーへの配慮とあわせて、ユーザーにとってのメリットを明確にすることが重要。

■ 問：収集した位置情報を活用したサービスとして次のようなものが考えられます。それぞれのサービスについて利用したいと思いますか。最も当てはまるものを一つお選びください。



出所）NRI「新型コロナウイルス感染拡大による生活の変化に関するアンケート」（2020年4月）

まとめ

1. 日本人のパーソナルデータ提供に対する許容度は、世界で最も低いレベル
   - コロナ禍においても、パーソナルデータの取り扱いにあたって、プライバシー保護に十分留意することが不可欠。

2. 匿名化などのプライバシー保護措置があれば、許容度は高まる
   - 携帯電話の位置情報であっても、匿名化されている場合は、74％が政府による利用を許容。
   - 理由は、「感染拡大防止に貢献したい」、「他者に迷惑をかけたくないから」、といった社会や他者との関係性への配慮。

3. 実際に、接触確認アプリをはじめ、感染拡大対策としてのパーソナルデータは、厳格なプライバシー保護措置が講じられている。
   - データ最小化（匿名処理、保存場所、保持期間）、通知・同意の取得、有識者によるレビューなど、様々な観点からプライバシーバイデザインを実践。

4. 消費者から支持され、理解が得られるデータ活用を今後も推進するべき
   - 日本は、中国・韓国のような強制力の伴う私権の制限をせずに、かつ欧米と同等以上にプライバシー保護に配慮して、感染拡大を抑え込んでいる特異な国。
   - プライバシーへの配慮をしつつ、利用者（消費者）へのメリットを明確にすることが重要。


Share the Next Values!