

個人情報保護法の3年ごと見直しに向けて

2019年3月27日
経団連情報通信委員会

本日の発表内容

1. わが国として目指すべき方向
2. 新たな仕組みに関する意見
3. 既存制度に関する意見
4. 国際的なデータの円滑な流通に関する意見

1. わが国として目指すべき方向

1. 目指すべき方向 Society 5.0 for SDGs

- ✓ わが国が目指すべきは、経済成長と社会課題解決の両立を図る、人間中心の社会である、「Society 5.0」。
- ✓ 「Society 5.0」実現のためには、デジタルテクノロジーとデータの活用が必要不可欠。
- ✓ 「Society 5.0」はSDGsの達成にも貢献。



2. 新たな仕組みに関する意見

(1) データポータビリティ

- ✓ データポータビリティについて検討する際には、消費者ニーズや事業者のメリット・実務負担、産業政策等の幅広い観点を十分に考慮し、わが国として最適な仕組みを議論すべき。

(2) 課徴金の導入

- ✓ 個人情報保護法への課徴金の導入については、慎重な検討が必要。

- 企業の個人データの活用を萎縮させる懸念。
- 個人情報取扱事業者は個人情報保護法を遵守(法第42条に基づく命令が発出された事例はなし)。

(3) 端末情報の取扱いに関する規律

✓ 事業活動の実態や消費者の利便も十分に踏まえ、クッキーなどの端末情報の取扱いについて新たな規律を設けることについては、慎重な検討が必要。

- 端末情報単体では特定の個人を識別せず、個人の権利利益の侵害と無関係。
- 端末情報を他の情報と照合することにより容易に特定の個人を識別できることとなった段階で、事業者は個人情報保護法に基づき適切な取り扱いを実施。

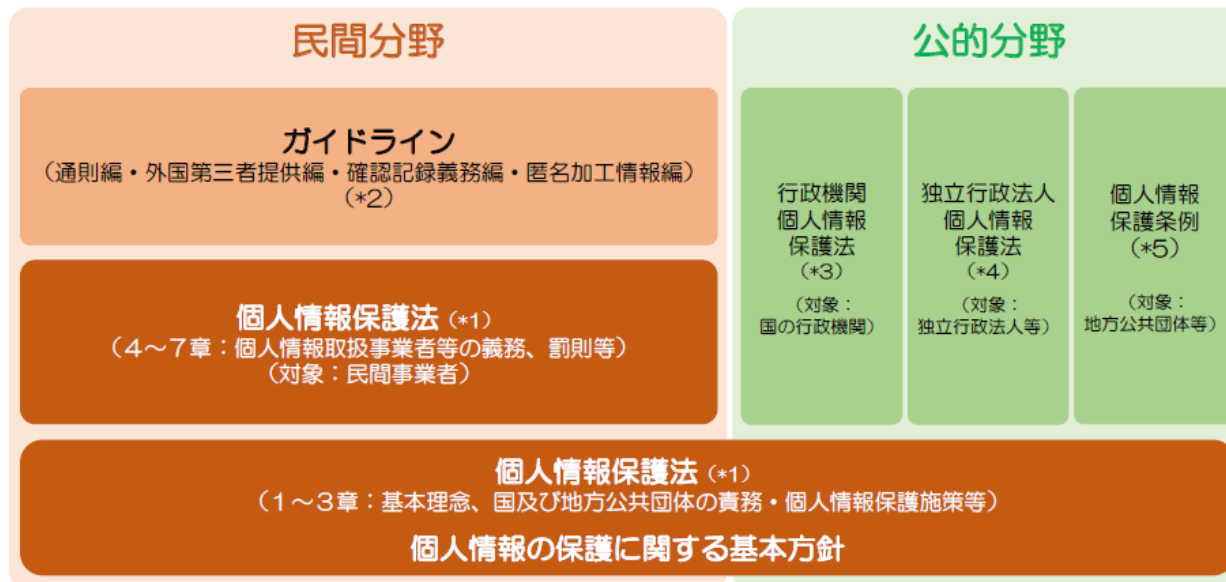
3. 現行制度に関する意見

2. 現行制度に関する意見 ①

(1) 公的部門での個人情報取り扱い

- ✓ 国の行政機関や国立大学法人等が個人情報保護法に定める義務・罰則等の適用対象でなく、わが国における個人情報の取扱いルールの一統化を阻害。
- ✓ 個人情報保護委員会が民間部門のみならず、公的部門における個人情報の適正な取り扱いの確保を図ることとすべき。

個人情報保護に関する法律・ガイドラインの体系イメージ



- (*1) 個人情報の保護に関する法律
- (*2) 金融関連分野・医療関連分野・情報通信関連分野等においては、別途のガイドライン等がある。
- (*3) 行政機関の保有する個人情報の保護に関する法律
- (*4) 独立行政法人等の保有する個人情報の保護に関する法律
- (*5) 個人情報保護条例の中には、公的分野における個人情報の取扱いに関する各種規定に加えて、事業者の一般的責務等に関する規定や、地方公共団体の施策への協力に関する規定等を設けているものもある。

(2) ガイドライン等の改善

- ✓ 実務の実態を踏まえ、ガイドライン等の充実や見直しを行うべき。(※1)(※2)

(3) 国内外事業者への公平・公正な法の適用・執行

- ✓ 海外事業者による規律に従った適切な個人情報の取り扱いを確保するため、外国政府機関との執行協力を着実に実施することが必要。

4. 国際的なデータの円滑な流通に関する意見

(1) データの自由な越境流通の確保

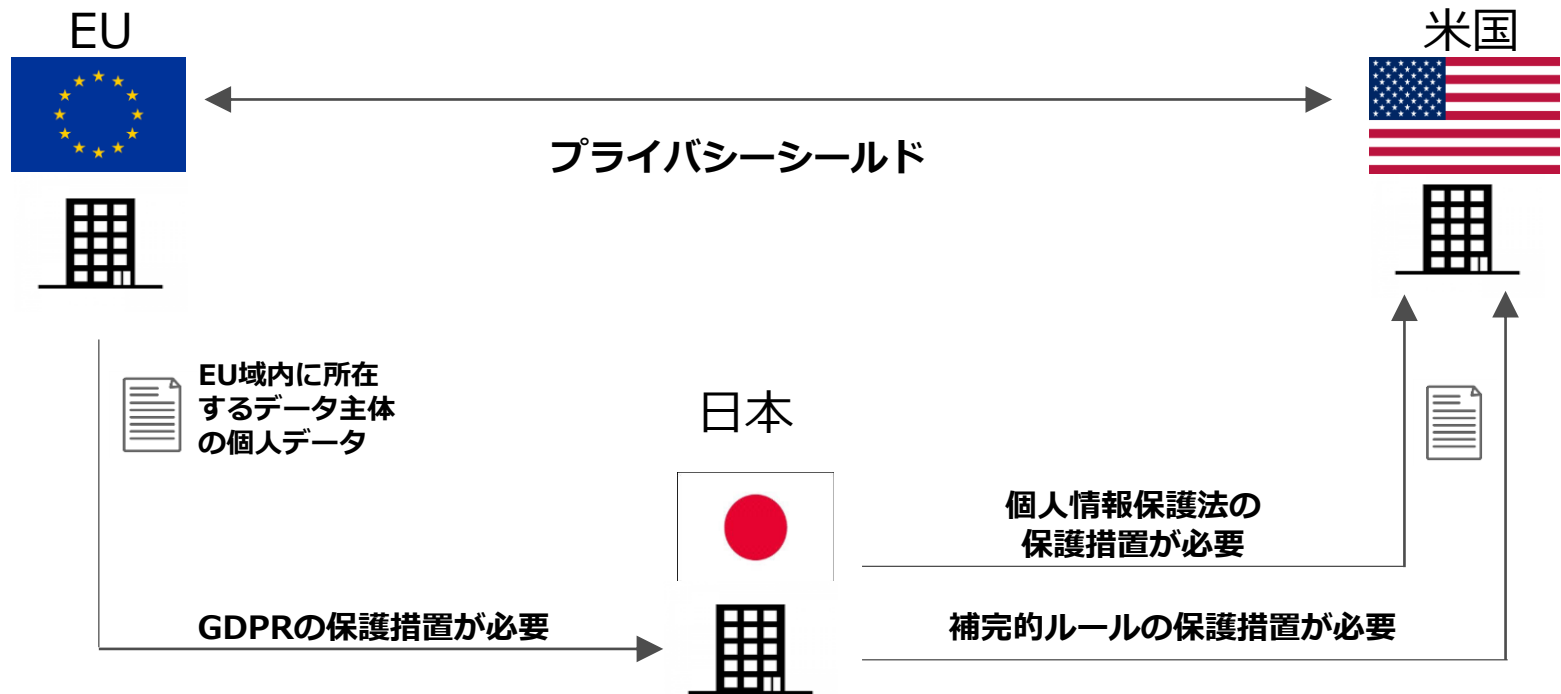
- ✓ Society 5.0実現のため、国境を越えて情報が自由に流通する環境の確保が大前提。
- ✓ データの自由な流通に向けて国際的に調和のとれた制度の構築を主導すべき。その一方で、国家機密や安全保障に係る情報、営業秘密など越境移転が望ましくないデータについては、WTO・GATSの規律を前提に、TPPの規律を参考として、必要な例外が認められるべき。
- ✓ 各国のデータローカライゼーション規制の緩和・撤廃を働きかけるべき。

(2) 越境移転についてのルールの整理

① EUからの個人データの越境「再」移転の規制への対応

- ✓ 日本の事業者が、EUからの個人データを米国の事業者にも再移転する場合、再移転先の事業者が米国・EU間のプライバシーシールドに基づく認証を受けていれば、「補完的ルール」を不適用とする仕組みを検討すべき。

- GDPRは、EU発のデータの越境移転のみならず、越境「再」移転も規制対象。
- EU発のデータを日本に移し、そこから、EUとの間で個人データを流通させる枠組みを有する米国に移転する場合も、日本の事業者は、個人情報保護法と「補完的ルール」をとともに遵守することが必要。



② 外国の第三者への個人データの提供

✓ 外国の第三者への個人データの提供が認められる適法性要件の追加を検討すべき。

- 外国の第三者へ個人データを提供する場合（法第24条）、次の①～③までのいずれかに該当すれば、事前に本人同意を取ることは不要。
 - ①その第三者が法第24条に基づき指定される国に所在する場合（※3）
 - ②第三者が「個人情報保護委員会規則で定める基準に適合する体制」を整備している場合（※4）
 - ③法第23条第1項で認められる場合（※5）
- しかし、①については、現状「EU」のみ。②については、基準に適合する体制を整備しているかどうかの確認が困難であるケースが存在。③については、法令に基づく場合等に限定。

Appendix

(※1) ガイドラインの充実が必要な事項 (例) 【スライド5】

① 匿名加工情報(法第2条第9項)

- 「特定の個人を識別することができないように」を解説した「あらゆる手法によって特定することができないよう技術的側面からすべての可能性を排除することを求めているのではなく、少なくとも一般人及び一般的な事業者の能力、手法等を基準として…通常の方法により特定できないような状態にすること」(「個人情報保護法ガイドライン(匿名加工情報編)」2-1)。

② 利用目的の変更(法第15条第2項、法第18条第3項)

- 本人への通知または公表によって個人情報の利用目的を変更することができる「本人が通常予期し得る限度と客観的に認められる範囲」(「個人情報保護法ガイドライン(通則編)」3-1-2)。

③ 第三者提供の制限の原則(法第23条第1項)

- 本人の同意無しに個人データを第三者に提供できる「人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難である時」を例示した「個人情報保護法ガイドライン(通則編)3-4-1」。

④ 保有個人データの開示(法第28条)

- 保有個人データの開示を請求された際に、開示しないこととできる「業務の適正な実施に著しい支障を及ぼす場合」(法第28条第2項2号)を例示した「個人情報保護法ガイドライン(通則編)3-5-2」。

(※2) ガイドラインの見直しを要する事項 (例) 【スライド5】

➤ 漏えい等が発生した場合の報告

- 個人情報保護委員会の告示では、漏えいした個人データに高度な暗号化が施されている場合などには個人情報保護委員会等への報告を不要としている(平成29年個人情報保護委員会告示第1号3-(2))のに対し、金融分野では、暗号化処理がなされていても報告が必要(金融機関における個人情報保護に関するQ&A問IV-4(答)④)。
- 安全管理技術の進展等を踏まえ、金融分野においても、個人情報保護委員会の告示と同様の例外措置を認めるべき。

(※3) 法第24条に基づき指定される国【スライド8】

- 個人の権利利益を保護するうえで我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるもの。

(※4) 個人情報保護委員会規則で定める基準に適合する体制を整備している場合【スライド8】

- 「個人情報の保護に関する法律についてのガイドライン(外国にある第三者への提供編)3-1」には、①適切な措置を講ずることを約した契約、確認書、覚書等の締結、②CBPR認証の取得が、事例として掲げられている。
- しかし、①については、基準に適合する体制を整備しているかの確認が困難なケースがあり、②については、APEC/CBPRの参加国数や事業者数が少ないという現実を踏まえる必要がある。

(※5) 法第23条第1項で認められる場合【スライド8】

- ① 法令に基づいて個人データを提供する場合（第1号関係）
- ② 人の生命、身体又は財産といった具体的な権利利益が侵害されるおそれがあり、これを保護するために個人データの提供が必要であり、かつ、本人の同意を得ることが困難である場合（第2号関係）
- ③ 公衆衛生の向上又は心身の発展途上にある児童の健全な育成のために特に必要な場合であり、かつ、本人の同意を得ることが困難である場合（第3号関係）
- ④ 国の機関等が法令の定める事務を実施する上で、民間企業等の協力を得る必要がある場合であって、協力する民間企業等が当該国の機関等に個人データを提供することについて、本人の同意を得ることが当該事務の遂行に支障を及ぼすおそれがある場合（第4号関係）