Discussion Purpose Only

海外の個人情報保護制度の動向について

2019.2.25

株式会社みずほ銀行

証券部 調査チーム

海外の個人情報保護制度をご説明する背景

- 情報流通のグローバル化が進展し、国際データ流通圏も展望した国際連携が求められていく中、個人情報保護法等の国内の法令整備が行われていく可能性がある。※1

- 「実効的な本人関与（コントローラビリティ）」がキーファクターとなる情報銀行※2においては、本邦の個人情報保護法等の国内法令の遵守に止まらず、GDPR等の海外法制度を念頭においた、ビジネスモデル・制度設計が望まれる。

- GDPR ※3は、EU域内に拠点のない管理者等がEU域内のデータ主体（個人）の個人データを取扱う場合にも適用されるため、例えば、観光関連の情報銀行を営む際に、取扱う情報の中に、EU域内の外国人旅行者のデータが含まれると、GDPRの域外適用が問題となりうる。

※1. 第75回高度情報通信ネットワーク社会推進戦略本部第6回官民データ活用推進戦略会議合同会議（平成30年12月19日開催）総理発言
「（略）個人情報や重要産業データを適切に保護しつつ、我が国主導で、自由で開かれた国際データ流通圏を世界に広げていくための国際連携を進めてください。また、その前提として、関係大臣において、個人情報保護法を始め必要な国内の法令整備と、体制強化に直ちに着手してください。」
※2.「情報信託機能の認定に係る指針ver1.0」（P.7）より
※3. 欧州連合（EU）で施行されている一般データ保護規則（General Data Protection Regulation）

1-1: 欧州GDPR ～施行経緯～

- データ保護指令（1995年～）
  - ✓「世界各国の個人情報保護法制のモデルとして参照」されてきたデータ保護指令に基づき、EU加盟国が、それぞれ国内法を整備し、個人データの保護を図ってきた。
  - ✓ EU加盟国は同指令に含まれる内容をミニマム・ルールとし、各国で国内法を整備。

  ⇒ データ保護指令の課題
    - 規制の跛行性による対応コストの発生
    - EU域内消費者のプライバシー保護強化の重要性が増加

- EU域内の統一的な新たなルール「EU一般データ保護規則（GDPR）」を制定。
  - ✓ 2012年1月：欧州委員会が原案を提案し、欧州議会・欧州理事会での審議開始
  - ✓ 2016年4月：GDPR採択
  - ✓ 2018年5月：GDPR施行
  - ✓ 2018年7月：欧州経済領域※で採択

※ 欧州経済領域（Europian Economic Area、EEA）。EU加盟国28カ国並びにノルウェー、アイルランド及びリヒテンシュタインを加えた31カ国から成る。GDPRはEEA合同委員会の採択を経て（2018年7月）、EU加盟国だけでなくノルウェー、アイルランド及びリヒテンシュタインにおいて各国内法を通じて適用されている。

1-2: 欧州GDPR　～消費者保護の強化～

- GDPR施行により、個人の権利強化、適用範囲の拡大、罰則の強化がなされた。

	GDPR	データ保護指令
1. 個人の権利（例）	※下記の権利への対応は原則無償（第12条第5項等※）	
同意の撤回権	• 個人は自己の同意をいつでも撤回する権利を有し、撤回は同意を与えるのと同じように容易なもので無ければならない（第7条第3項）	• 条文明記なし
消去権	• 個人は個人データにかかる同意の撤回等の一定の要件下で、管理者等に対して不当に遅滞することなく当該個人データを消去させる権利を有する（第17条）	• 個人はデータが不完全または不正確で、取扱が指令の規定に違反している場合の消去権を有する（第12条(b)号）
データ ポータビリティ権	• 個人は、例えば同意等に基づき取扱われかつその取り扱が自動化された手段で行われる場合の要件下で、①構造化され一般的に使用され機械可読な形式で自らの個人情報を受け取ること、そして②技術的に可能な場合には、別の企業等に対して直接その個人情報を提供することを求めることができる（第20条）	• 条文明記なし
2. 域外適用	• EU域外からEU域内のデータ主体に向けてサービスを提供したり、その行動の監視をしたりする場合に適用される（第3条第2項）	• EU域内の拠点が無くともEU域内に設置された機器を使用して個人データの処理を行う場合に適用される（第4条第1項）
3. 個人データの 域外移転	• 十分性認定、BCR、SDPC、特定の状況における例外、等により認められている（第44条～第50条）	• 十分性認定、BCR / SCC、の規定あり（第25条、第26条）
4. 罰則	• 最大で2,000万ユーロか全世界連結売上高4%のいずれか高い金額（第83条）	• 各国の国内法による

※ 同意の撤回への無償対応は、GDPR同意に関するガイドラインに記載されている。

1-3: 欧州GDPR　～情報銀行の認定指針等との比較～

- 消費者のコントローラビリティ確保の趣旨を踏まえ、認定指針ver1.0※1、及びガイドブックver1.0※2は、GDPRに近い考え方で制度設計されている。

	GDPR	認定指針ver1.0 (★)※1 ガイドブックver1.0 (▲)※2
同意の撤回権	• 個人は個人データ取扱にかかる同意をいつでも撤回する権利を有し、撤回は同意を与えるのと同じように容易なもので無ければならない（第7条3項） • 手数料：原則無償	• 情報銀行は個人の請求に基づき利用・第三者提供を停止(★) • 個人は、個人情報を同意の範囲内で管理又は利用（第三者提供を含む）する業務の委任について、情報銀行が別途定める手続に従い、いつでもその全部又は一部を撤回（個人情報の取扱い停止、個人情報の訂正又は削除を含む。）することができる。ただし、当該撤回は既に行われた委任業務には及ばず、将来向かって効力を有し、当該撤回が情報銀行に到達以降、情報銀行は直ちに個人の当該撤回にかかる本委任業務を停止する。(▲) • 情報銀行は、本人から委任業務の撤回があった場合、提供先第三者にその旨を通知し、当該第三者は、当該通知を受けたのち直ちに撤回により求められる措置を行う。(▲) • 手数料：記載なし
消去権	• 個人は個人データ取扱にかかる同意の撤回等の一定の要件下で、管理者等に対して不当に遅滞することなく当該個人データを消去させる権利を有する（第17条） • 手数料：原則無償	• 情報銀行は、簡易迅速で負担のないユーザーインターフェイスにより、消去の請求を可能とする仕組みを提供する(▲) • 情報銀行は、本人がその特定の状況で適切及び可能であれば、個人データの正確性及び完全性に異議申立てができ、個人データを削除等することができるようにし、情報提供先に対して削除等を連絡する(▲) • 情報銀行は、過度な遅延又はコストを伴わず、単純、迅速かつ効率的な方法で本人がこれらの権利を行使することができる手順を確立する(▲) • 手数料：「過度な（略）コストを伴わず」と記載
データポータビリティ権	• 個人は、個人データ取扱にかかる同意等に基づき取扱われかつその取扱が自動化された手段で行われる場合の要件下で、①構造化され一般的に使用され機械可読な形式で自らの個人情報を受け取ること、そして②技術的に可能な場合には、別の企業等に対して直接その個人情報を提供することを求めることができる（第20条） • 手数料：原則無償	• 簡易迅速で負担のないユーザーインターフェイスにより、開示の請求を可能とする仕組みを提供する (★・▲) • 他の事業者へのデータの移行などいわゆるデータポータビリティ機能を提供する場合には、その旨を明示する(★・▲) • 手数料：記載なし

※1. 認定指針ver1.0：「情報信託機能の認定に係る指針ver1.0」（平成30年6月）に記載されている「情報信託機能の認定基準」より。情報信託機能の認定スキームの在り方に関する検討会が公表
※2. ガイドブックver1.0：『「情報銀行」認定申請ガイドブックver1.0』（平成30年12月）および付属のモデル契約約款より。一般社団法人日本IT団体連盟 情報銀行推進委員会が公表

1-4: 欧州GDPR　～域外適用（第3条第2項）～

- GDPRは、以下の(a)又は(b)に関連する、「EU 域内に拠点のない管理者等」による「EU域内のデータ主体の個人データの処理」についても適用される（GDPR第3条第2項）。
  (a) EU 域内のデータ主体に対する商品又はサービスの提供
  (b) EU 域内で行われるデータ主体の行動の監視

⇒例えば、本邦情報銀行が、EUに居住する個人の個人データを“直接”取扱う場合は、GDPRの域外適用を受ける可能性がある点に、留意が必要

GDPR第3条（地理的適用範囲）

- 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
  1. 本規則は、その取扱いがEU 域内で行われるものであるか否かを問わず、EU 域内の管理者又は処理者の拠点の活動の過程における個人データの取扱いに適用される。
- 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
  (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
  (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
  2. 取扱活動が以下と関連する場合、本規則は、EU 域内に拠点のない管理者又は処理者によるEU 域内のデータ主体の個人データの取扱いに適用される：
  (a)データ主体の支払いが要求されるか否かを問わず、EU 域内のデータ主体に対する物品又はサービスの提供。又は
  (b)データ主体の行動がEU 域内で行われるものである限り、その行動の監視。
- 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.
  3. 本規則は、EU 域内に拠点のない管理者によるものであっても、国際公法の効力により加盟国の国内法の適用のある場所において行われる個人データの取扱いに適用される。

（出所）個人情報保護委員会の仮日本語訳より

1-5: 欧州GDPR ～個人データの域外移転（第44条～第50条）～

- 個人データの移転先がEU域外の第三国等となる移転は、十分性認定（GDPR第45条）等（下図参照）が充足される場合においてのみ、適法に行われる。
  但し、GDPRの域外適用への留意が必要である。

  ⇒本邦情報銀行が、EU域内の情報提供元（例えば現地の旅行会社）から個人データを取得する場合

  ⇒従前はBCR承認取得、SCCを含む契約締結、例外事由により対応していたが、2019年1月23日に日本も十分性認定を受けたことで、補完的ルール※1の遵守での対応も可能となった。

欧州委員会による十分性認定（GDPR第45条第1項）
- 第三国等が十分なデータ保護の水準を確保していると欧州委員会が決定した場合

～認定国～

アンドラ、アルゼンチン、カナダ、フェロー諸島、ガーンジー、イスラエル、マン島、ジャージー、ニュージーランド、スイス、ウルグアイ、米国※2、**日本（2019年1月23日）**
（個人情報保護委員会HP※3より、2019年1月24日時点）

※日本においては、補完的ルールを遵守する必要あり。

充足 / 未充足

適切な保護措置（GDPR第46条第1項）
- 管理者等は、その管理者等が適切な保護措置を提供しており、かつ、データ主体の権利及び効果的な司法救済が利用可能なことを条件としている場合

～適切な保護措置の例～
- BCR（拘束的企業準則、Binding Corporate Rules）（GDPR第47条1項）：監督機関によるBCRの承認を受ける。
  BCRとは、企業グループの中又は共同事業を営んでいる事業者グループの中で、第三国等内の管理者等に対して個人データの移転をするために、加盟国の領土に設けられた管理者等によって遵守される個人データ保護方針である（GDPR第4条第20項）。
- SDPC（標準データ保護条項、Standard Data Protection Closes）（GDPR第46条第2項(c)(d)）：個人データの移転元と移転先の間で、欧州委員会等が採択・承認したプライバシー保護に関する十分な保護措置等を内容とする適切な条項（SDPC）を含む契約締結する。

充足 / 未充足

適法

充足

特定の状況における例外（GDPR第49条第1項）
- 当項に規定する条件（第1項(a)~(g)、第1項後段）中のいずれかを満たしている場合

～例外事由の例～
- データ主体の明示的な同意がある場合（第1項(a)）
- データ主体と管理者との間の契約の締結・履行のため移転が必要な場合（第1項(b)）
- 管理者及びそれ以外の法人又は自然人との間で、データ主体の利益のための契約締結・履行のため、移転が必要な場合（第1項(c)）

※1. 個人情報保護委員会が定める「個人情報の保護に関する法律に係る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に関する補完的ルール」。十分性認定を根拠とする個人データの域外移転の場合には、補完的ルールの遵守が必要となる。
※2. 米国はプライバシー・シールドの枠組みに限定されている。当該枠組みにおいて米国企業は、一定のルール遵守の宣言、米国商務省への登録、定期的な遵守状況の検証を受けることで、適法に域外移転を行うことが可能となる（別冊NBL#162より）
※3. 個人情報保護委員会HP：https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/

2-1: 海外の個人情報保護規制　～米国～

- 米国では、連邦法や各州法において多数の異なる法規制が存在し、法規制のアプローチも業種・データの種類により異なり（下表：連邦法の例）、包括的な個人情報保護の法律は存在しない。
- 昨年6月にカリフォルニア州で成立した消費者プライバシー法（州法）は、消費者の権利を認め、また域外適用の可能性もある。また、連邦法によるプライバシー規制を求める流れもある。※1

連邦法	概要	名宛人／対象情報
Children's Online Privacy Act of 1998	インターネット及び児童のプライバシーに関する連邦法	13歳未満の児童向けウェブサイト等から個人情報を取得している運営者／オンライン上で収集された児童に関する個人情報
Gamm-Leach-Bliley-Act of 1999	財務データ及び金融機関に関する連邦法	銀行、証券会社、保険会社、金融仲介業者等の金融機関／金融機関が入手する情報で、公的に入手できない個人情報等
Health Insurance Portability and Accountability Act of 1996	医療情報及び記録に関する連邦法	医療保険提供者、医療サービス提供者等／個人の身体的若しくは精神的な健康に関する状況、医療提供実績等
The Federal Trade Commission Act	競争法	特定の分野の個人情報を規制するものではなく、米国消費者を不公正又は欺瞞的な取引慣行から保護する一環として、個人データを保護する合理的な手段を講じなかった企業に対して適用

<u>カリフォルニア州消費者プライバシー法（CaCPA）（2018年6月成立、2020年1月施行予定）</u>

✓ 消費者の権利（例）：
- 開示請求権（第1798.110条）、第三者提供の停止請求権（オプトアウトの権利）（第1798.120条(a)）、消去権（第1798.105条(a)）（但し、契約履行のために必要な場合等は削除する必要はない（第1798.105条(d)））

✓ 域外適用：
- 対象事業者：「カリフォルニア州で事業を行っている」者であり、以下a,b,cのいずれかを満たす者（第1798.140条(c)）・等※2
  「a. 年間売上高が25百万ドル超」、「b. 合計5万件/年以上の個人情報を商業目的で購買し、受領し、売却しまたは共有している」、「c. 年間売上高の50%以上を個人情報の売却から得ている」
- 消費者：カリフォルニア州の住民（第1798.140条(g)）

✓ 個人データの域外移転：　条文への明記なし

※1. 「政府が欧州連合（EU）の一般データ保護規則（GDPR）が規定する個人情報保護策の一部の採用を検討する中、アップルやフェイスブックなどIT大手は連邦レベルでのプライバシー保護法制の必要性を認めている」（2019/1/8日本経済新聞）。「米アップルのティム・クック最高経営責任者（CEO）は16日付の米タイムに寄稿し、「個人データを扱う企業は米政府が規制すべきだ」と主張した。（略）個人データを扱う企業を（略）米連邦取引委員会（FTC）の規制下に置く案を示した」（2019/1/18日本経済新聞）

※2. CaCPAの適用を受ける事業者を支配し、又はその事業者から支配され、及び、その事業者と共通のブランドを有している事業者に対してもCaCPAが適用され得る。

2-2: 海外の個人情報保護規制　～中国～

- 2016年3月：第13次5カ年計画※を公布
  - ✓ データ資源の安全保護強化、インターネット空間の科学的管理、重要情報システム安全の全面保障を志向
- 2017年6月：中华人民共和国网络安全法（ネットワーク安全法）施行
  - ✓ サイバーセキュリティ分野の基本法
  - ✓ 2018年5月：「個人情報安全規範」施行
    - – ネットワーク安全法における個人情報保護規定の具体的な内容
  - ✓ 下位規範やガイドラインは一部を除いて、大半が意見募集稿

ネットワーク安全法及び関連する法令等（意見募集稿も多く、各種規定について今後の動向に留意が必要）

✓ 消費者の権利（例）：
- 不法取得・使用された場合の削除権（ネットワーク安全法第43条）
- 開示（個人情報のコピーの）請求権、削除請求権、アカウント抹消請求権、同意撤回権（個人情報安全規範第5.6条）

✓ 域外適用：
- 中国国内におけるネットワークの構築、運営等を通じて個人情報を取得することとなる場合（ネットワーク安全法第37条）
- 「中国国内における運用」とは、中国国内に登録していないネットワーク運営者であっても、中国国内で業務を展開、または中国国内に商品・サービスを提供する場合（データ越境移転安全評価指針第3.2条：意見募集稿）

✓ 個人データの域外移転：
- 重要情報インフラの運営者の個人情報の国内保存義務、及び域外移転規制（ネットワーク安全法第37条）
- ネットワーク運営者の個人情報の国内保存義務及び域外移転の場合の手続等を規定（個人情報と重要データ越境移転安全評価弁法第2条：意見募集稿）

※ 第13次5カ年計画：2016-2020年の5カ年についての計画（2016年3月公布）。中華人民共和国では1953年以来、基本的に5年ごとに経済・社会の発展プランを5カ年計画として策定し、これに基づき政策が策定・実施されている。

免責事項