米国等における個人情報保護と利活用に関する近況

中沢 潔
JETRO/IPA New York

1　サマリー

欧州連合（EU）では、2018 年 5 月 25 日に GDPR（The General Data Protection Regulation）が施行される。
PwC Japan の調査によれば、2017 年 7 月時点で、GDPR への対応について、①準備の具体化を完了、②準備の具体化を開始、③アセスメントを完了、④アセスメントを開始、⑤準備に未着手である企業の割合は、　米国：①22%、②26%、③21%、④27%、⑤　4%　英国：①　8%、②32%、③21%、④34%、⑤　5%　日本：①　2%、②17%、③22%、④48%、⑤12% となっている。
2018 年 2 月現時点で、GDPR は施行前であり、準拠ガイドラインもすべて発表されていない状況であり、各社は現時点で考えられる実務的な対応を行っているのが実際であろうが、GDPR への対応が不十分なままでは、巨額の制裁金というリスクを抱えたまま、GDPR の施行を迎えることになる。

また、いわゆる「GAFA」について、米国の消費者は、「社会の不可欠な要素になっている」という点について 55%が同意した一方で、「個人データの保護を強化したい」と考えている回答者も 43%にのぼった。「社会生活をシンプルにした」と 37%の回答者が評価しているが、「社会への影響力が強くなりすぎている」とした回答者も 31%であり、「信用できるやり方で入手した消費者とユーザーのデータを適切に扱っている」とした回答者は 23%であった。
EU では、Google、Facebook、Amazon といったインターネット・テクノロジー企業に対する税制の改革検討を進めている。2017 年 9 月に発表された、欧州委員会の徴税のあり方を再考するレポート"A Fair and Efficient Tax System in the European Union for the Digital Single Market"[1]では、従来の企業への課税が 23.2%であるのに対して、国際展開するデジタル企業への課税は 10.1%にとどまっていると指摘している。

加えて、データの越境を禁止する法律（”data residency law”）を制定する動きが、EU や中国だけではなく、世界中に広がりつつある。米国通商代表部（Office of the United States Trade Representative 、USTR）の 2017 年度報告書” 2017 National Trade Estimate Report on FOREIGN TRADE BARRIERS”[2]では、2015 年、2016 年の中国政府が米国等の広範な ICT 製品・サービスを国産に置き換えようとする動きに対し、懸念を示している。そして、2015 年の中国の国家セキュリティ法は情報安全保障を目的として謳っているが、経済産業政策上の意図が含まれており、2015 年 12 月のカウンターテロリズム法と 2016 年 11 月のサイバーセキュリティ法は ICT 製品・サービスの中国国内への輸入に対する貿易制限となっていると指摘している。

[1] https://ec.europa.eu/taxation_customs/sites/taxation/files/1_en_act_part1_v10_en.pdf
[2] https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf

今後は、個人情報に限らず、金融・税金関連情報、通信情報、政府及び公共機関の情報等について、各国は自国内での保存を求める動きを取っている。米国も、金融・税金関連情報、政府及び公共機関の情報については、データの自国内の保存を求めている。いずれにせよ、中国などの事例にも見られるように、個人データの域内管理は世界的なトレンドとなりつつある。こうした各国の法令へのコンプライアンスを遵守していく上でも、まず GDPR への対応が重要になってくる。GDPR の施行が、情報の域内管理の世界的標準につながる可能性もある。

2　欧米の個人情報保護法制動向

（1） 米国の個人情報保護法制

米国の個人情報保護法制については、2015 年 9 月号[3]の 4 章で「米国の個人情報保護に関する法律」として詳しく紹介したので、ここではその概要、アップデート及び米国連邦取引委員会（Federal Trade Commission、FTC）について述べる。

・概要

米国連邦政府では 1974 年の情報公開法（Freedom of Information Act）成立以来、個人情報保護を包括的な法律で扱うのではなく、電子メールやインターネットなどの情報技術の進歩とテロリズムなどの時代の要請に対応する形で、医療や金融などセクター毎に個別の法律を立法化してきた。また、オバマ政権下では、2013 年 12 月にスノーデン事件が発生し、個人情報保護についての見直しを迫られることになり、新たな法案が提案されることになった（各法案の現在の状況を図表 1 に示す）。また、州政府では、連邦法に基づき具体的な内容を定めた、各州の実情に対応する州法を制定し、個人情報保護に取り組んできた。

図表 **1**：**2015** 年 **4** 月号で紹介した米国の個人情報保護に関する法案の現在のステータス

法案名	内容	2018 年 2 月現在のステータス
Personal Data Notification Act（個人情報の通知と保護法）	新たな個人情報保護連邦基準	2017 年 9 月 18 日、James “Jim” Langevin 下院議員（ロードアイランド州選出、民主党）から、″H.R. 3806：Personal Data Notification and Protection Act of 2017″として提出[4]。
Consumer Privacy Bill of Rights（消費者プライバシー権利章典）	ユーザーへの自身のデータをコントロールする権利の付与	2017 年 11 月 14 日、Patrick Leahy 上院議員（バーモント州選出、民主党）から、″S. 2124: Consumer Privacy Protection Act of 2017″として提出[5]。
Student Data Privacy Act（学生データ保護法）	教育現場から得た学生データを利益目的に使用することの禁止	2017 年 4 月 6 日、Edward “Ed” Markey 上院議員（マサチューセッツ州選出、民主党）から、″S. 877: Protecting Student Privacy Act of 2017″として提出[6]。
Cybersecurity Information Sharing Act（サイバー・セキュリティ情報共有法）	サイバー攻撃による個人情報保護	2017 年 11 月 7 日、Kamala Harris 上院議員（カリフォルニア州選出、民主党）から、″S. 2083: Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act of 2017″として提出[7]。

出典：各種資料を元に作成

・アップデート

2015 年 9 月以降での米国の個人情報保護法制に関する変化としては、インターネット・サービス・プロバイダー（ISP）に関する動きがある。2017 年 4 月 3 日、トランプ大統領は、ISP に顧客のオンラインプライバシー保護を求める規則の廃止に署名した。この規則は、ISP が顧客の位置情報、経済情報、健康情報、子供の情報、Web ブラウジング履歴を広告やマーケティングのために利用する前に、顧客の同意を得ることを必要とするというものであり、顧客のプライバシー保護に関して ISP は Google や Facebook といったインターネット企業よりも厳しく規制されることになっていた。この規則は、オバマ政権の最終日に米連邦通信委員会（Federal Communications Commission、FCC）によって承認され、2016 年 10 月に成立し 2017 年 12 月 4 日に施行の予定だったが、2017 年 3 月 28 日に下院で撤廃された [8][9][10]。

[3] https://www.ipa.go.jp/files/000048013.pdf
[4] https://www.govtrack.us/congress/bills/115/hr3806
[5] https://www.govtrack.us/congress/bills/115/s2124
[6] https://www.govtrack.us/congress/bills/115/s877
[7] https://www.govtrack.us/congress/bills/115/s2083

この規則廃止への対応として、およそ半数の州が対策を講じている。現在、顧客が情報の開示を認めない限り、ISP は顧客に関する特定の個人情報を守らなければならないと定めているのはネバダ州とミネソタ州の 2 州である。両州とも個人特定情報の開示を禁じているが、ミネソタ州では ISP に対して、顧客のネットサーフィン行動と訪問 Web サイトについての情報開示前に許可を取ることも義務づけている。2017 年にネバダ州では、カリフォルニア州やデラウェア州と同様に、ネバダ州住民の個人特定情報を収集する Web サイト・オペレーター業者とオンライン・サービス業者に対して、その情報の利用方法について通知することを求める州法を制定している [11]。

・**FTC** について

米国の個人情報保護法制に関して重要な役割を果たしているのが、FTC[12] である。FTC の役目は、消費者を独占的、詐欺的、不公正な商取引から保護し、消費者の十分な情報に基づく選択と市場競争への理解を促すことで、過度の法制度によるビジネスへの負担をなくすことである [13]。FTC は連邦政府の独立行政委員会であり、FTC の委員長及び委員は、上院の承認を経て、大統領が任命する [14]。プライバシー保護に関しては、不公正や詐欺などの行為を監視・監督する立場にあり、最近では IoT 時代にあわせた Fair Information Practice Principles[15] を含むガイドラインを策定している [16][17][18]。

（2）EU の個人情報保護法制（GDPR：General Data Protection Rule）

・**GDPR** 概要

欧州連合（EU）では、2018 年 5 月 25 日に GDPR（The General Data Protection Regulation）[19] が施行される。GDPR は、個人情報の保護と管理に関する従来の EU データ保護指令（Directive 95/46/EC）[20] を置

き換えるものとして、2016 年 4 月 14 日に欧州議会で制定された。これまでは、EU データ保護指令に基づき各国がデータ保護に関する法律を制定していたため、国毎に差異が生じていたが、GDPR は EU 加盟国すべて[21]に適用される包括法である。

[8] https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rulesidUSKBN1752PR
[9] http://money.cnn.com/2017/04/03/technology/internet-privacy-law-trump/index.html
[10] https://arstechnica.com/tech-policy/2017/04/trumps-signature-makes-it-official-isp-privacy-rules-are-dead/
[11] http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-legislation-related-to-internetservice-providers.aspx
[12] https://www.ftc.gov/
[13] https://www.ftc.gov/about-ftc
[14] http://www.jftc.go.jp/kokusai/worldcom/kakkoku/abc/allabc/u/america.html
[15] FTC Fair Information Practice Principles（FIPPs）とは、FTC の公正情報行動原則。『公正情報行動とは、1970 年代に FTC が、その概念を提案したものである。FIPPs に関しては、国土安全保障省が 2008 年に、同省における基本的プライバシー方針とその運用原則として、「1974 年プライバシー法（P.L.93-579）に基づく FIPPs」を 定めた（Dec.29, 2008, Memorandum Number: 2008-01）。その内容は、①透明性、②個人の参加、③目的の限定、④必要最低限の情報、⑤利用制限、⑥情報の品質及び完全性、⑦セキュリティ、⑧説明責任及び監査の 8 項目である。』井樋三枝子、「外国の立法：立法情報・翻訳・解説. (月刊版. 252-1)」、国立国会図書館、2012 年 7 月 http://dl.ndl.go.jp/view/download/digidepo_3507782_po_02520106.pdf?contentNo=1
[16] https://japan-dmc.org/?p=6992
[17] https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-bestpractices
[18] https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-bestpractices
[19] https://www.eugdpr.org/
[20] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[21] 実質的には、欧州経済領域（European Economic Area、EEA、EU28 ヶ国に加え、アイスランド、リヒテンシュタイン、ノルウェイ。英国を含まない）が対象となる。Brexit 後の英国動向については不確定。https://www.eugdpr.org/gdpr-faqs.html

GDPR では、プライバシーを基本的人権としており、個人に自身の個人データに関する取り扱いの自由と権利を認めている。ここでの個人データ対象は、EU 内の居住に関わらず、EU 内所在の個人データが対象となっている。また、個人データの利害関係者として、データ管理者を中心に、データ処理者、データ受領者、第三者、データ保護責任者、監督機関、欧州データ保護役員会といった利害関係者の役割が定義されている。そして、EU 内での個人データの処理や、EU 外への移転にかかる要件が定義されている。

GDPR では、各対象の範囲に注意が必要である。EU 内所在の個人データが対象となるため、EU 内に拠点を持たない企業・組織も GDPR の対象になる。個人データと定義されて GDPR の対象となっている情報には、個人と直接紐付かない IP アドレス、クッキーID、RFID タグも含まれている。EU 内の個人のデータを処理するデータ処理者も GDPR の対象となる。個人データのうち、特別なカテゴリーの個人データ[3]については、

[3] 人種や民族的出自、政治的見解、宗教的・哲学的信条、労働組合加入状況、遺伝子情報、生体認証データ、健康データ、性生活や性的指向データ

取り扱いが原則禁止されている。また、不可逆的にデータ主体の識別を防止できない限りは、匿名化データとして GDPR の対象外にはならない。データ主体識別につながる個人データを仮名処理した仮名化データは、元データを追加すれば個人を特定できるため、個人データとして GDPR の対象に含まれる。また、暗号化された個人データも、暗号鍵が廃棄されない限り、個人データとして GDPR の対象に含まれる。

GDPR では、個人データの取り扱いについても、各種要件が取り決められている。個人データの取り扱いに当たっては、まず個人に詳細事項を通知・説明し、積極的な同意取得を得ることを必須条件としており、個人データはこの同意を得た範囲でのみ取り扱える。その上で、個人は同意しても、いつでも同意撤回が可能である。そして、個人データを取り扱う企業・組織には、個人データの安全な管理保護が求められ、大組織ではデータ処理のログ保管が義務づけられている。そして、個人データに漏洩が発生した場合、72 時間以内に監督機関に通知しなければならない。

また、GDPR では、EU 内の個人データを第三国や国際機関へ移すデータ移転は原則禁止されている。このデータ移転には、EU 内で管理されているデータに EU 外からアクセスすることや、EU 外の第三国のサーバーを介した EU 内でのデータのやり取りも含まれている。データ移転を行うには、GDPR に例外として定められた個人データの EU 外への移転要件のいずれかを満たさなければならない。GDPR では移転要件として、実務的には、移転先のデータ保護の十分性認定、明確な同意の取得、適切な保護措置（標準契約条項（SCC）、あるいは拘束的企業準則（BCR））の取得の 3 つの方法が想定されている。

移転先のデータ保護の十分性認定は、EU が十分な水準の個人データ保護が行われていると認定した国に与えられる。現時点では、日本も米国も認定を得ていない。現在、データ保護の十分性認定を受けているのは、アンドラ、アルゼンチン、カナダ（民間組織のみ）、フェロー諸島、イギリス王室属領ガーンジーとジャージー、イスラエル、マン島、ニュージーランド、スイス、ウルグアイだけである。なお、EU と米国は、2016 年にプライバシー・シールド（EU-US Privacy Shield）[4]の合意に達しており、ここで定められたデータ保護基準を満たしているという米国商務省の認定を受けた米国企業は GDPR 施行後も EU 内データの移転が可能である。また、2017 年 7 月 6 日、ブリュッセルで行われた第 24 回日 EU 定期首脳協議では、安倍晋三内閣総理大臣とジャン＝クロード・ユンカー欧州委員会委員長（H. E. Mr. Jean-Claude JUNCKER、President of the European Commission）から、データの保護と活用に関する共同宣言が発表され、ここでは 2018 年の早い時期までに相互のデータ移転を可能とするために努力することが述べられている[5]。

GDPR 違反に対する制裁としては、違反した規定の内容により、1000 万ユーロあるいは前会計年度全世界売上高の 2%のうち多い額、あるいは、2000 万ユーロあるいは前会計年度全世界売上高の 4%のうち多い額、このいずれかを最大とする金額が罰金として課せられる。

・海外企業が **GDPR** に対して求められる対応海外企業が GDPR に対して求められる対応について、JETRO では、『「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）（2016 年 11 月）』[6]

[4] https://www.privacyshield.gov/welcome
[5] http://www.mofa.go.jp/mofaj/files/000270697.pdf
[6] https://www.jetro.go.jp/world/reports/2016/01/dcfcebc8265a8943.html

と『「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（実践編）（2017 年 8 月）』[7]を作成し、公開している。入門編冒頭では、以下のように欧州外
企業が GDPR に対して求められる具体的な対応が概観されている。

『GDPR は、EU を含む欧州経済領域（EEA）域内で取得した「氏名」や「メールアドレス」「クレジットカード番号」などの個人データを EEA 域外に移転することを原則禁止している。ここでいう「個人」とは、EEA 域内の所在者全般を指し、現地進出の日系企業に勤務する現地採用従業員や、日本から派遣されている駐在員も含まれるため、注意が必要だ。行政罰規定があり、違反行為に対しては、高額の制裁金が課されるリスクもある。

GDPR の適用対象には、営利活動に従事する企業のみならず、公的機関・地方自治体・非営利法人なども含まれる（外交・防衛・警察などについて例外あり）。すなわち、EEA 域内に現地法人・支店・駐在員事務所を置くすべての企業・団体・機関が、GDPR への対応を検討することが求められている。また、中小・零細企業も対象であり、EEA 域内に現地法人・支店・駐在員事務所を置かない事業者であっても、インターネット取引などで EEA 所在者の顧客情報を取得・移転する場合、適用対象となり得る。また、こうした事業者には EU における代理人の選任義務が課せられるケースがあり、その場合の義務違反にも高額の制裁金が課されるリスクがあるので要注意だ。
このため、EEA と個人データをやり取りする日本のほとんどの企業や機関・団体が適用対象となり、適用が開始される 2018 年 5 月 25 日までに適切な準備を進めることが必要だ。他方、GDPR の内容は、法解釈を伴う専門的なものであるため、EEA でビジネスを行う企業の間でも正確に理解されていない側面もある。特に、EEA にビジネスを展開しようとする中小企業には、大きな負担となることが想定される。』

入門編では、GDPR の概要を説明した後、実務事項の基礎的な解説を「Q&A 基礎編」、インターネット取引や名刺などの社外関係における個人情報の取り扱いを「Q&A 応用編（社外関係）」、人事情報などの社内関係における個人情報の取り扱いを「Q&A 応用編（社内関係）」として Q&A 形式で具体的に解説している。また、実践編でも Q&A 形式で、標準契約条項（Standard Contractual Clauses：SCC）[8]と拘束的企業準則

[7] https://www.jetro.go.jp/world/reports/2017/01/76b450c94650862a.html
[8] 『SCC とは、現行の「EU データ保護指令」に基づき EEA 加盟国で立法された各国個人情報保護法の適用対象となる個人データを、十分なレベルの個人データの保護が確保されているとみなされない EEA 外の国へと移転する際に、当該個人データに十分な保護を提供するための法的手段である。
別の角度から説明すれば、SCC とは、欧州委員会によって決定されたデータ移転の契約書の雛形であり、EEA 内のデータ輸出者と EEA 外のデータ輸入者の二当事者間で、当該雛型を使ってデータ移転契約を締結することで適切な保護措置を提供し、適法なデータ移転を可能とするものである。』『「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（実践編）（2017 年 8 月）』pp.3

（Binding Corporate Rules：BCR）[9]による対応、データ保護責任者（Data Protection Officer：DPO）[10]の選任などのコンプライアンス対応における問題が取りあげられている。

・GDPR 準拠に向けた課題

GDPR 準拠に向けては、複雑な同意取得、利害関係者との連携といった課題がある。

GDPR では、「個人データの処理の適法性の根拠としての同意」および「個人データの EEA 域外への移転を適法化するための同意」の 2 種類の同意がある。後者は、前者の要件をすべて満たした上で、さらに「十分性決定および適切な保護措置がないことによって、当該移転によってデータ主体に対して生じ得るリスクについて情報提供を受けた後、データ主体がその提案された移転に明示的に同意」することが必要である。

「個人データの処理の適法性の根拠としての同意」を取得するには、次表の条件が満たされていることをチェックしなければならない。

図表 **2**：データ主体の同意の条件

	同意の条件（GDPR 第 7 条）
1	処理が同意に基づく場合、管理者は、個人データ主体が自己の個人データの処理に対して同意しているということを証明できるようにしなければならない。
2	個人データ主体の同意が他の案件にも関係する書面において与えられている場合、その同意の要求は、明瞭かつ平易な文言を用い、理解しやすくかつ容易にアクセスし得る形で、その他の案件と明らかに区別できる方法によって明示されなければならない。
3	データ主体は、同意を与える以前に以下の事項が通知されていなければならない。同意の撤回は、その付与と同程度に容易なものでなければならない。 ・データ主体は、いつでも同意を撤回する権利があること。 ・同意の撤回は、撤回前の同意に基づく処理の適法性に影響を与えない。
4	同意が自由意思によりなされているかについて判断する際、サービス約款を含む契約の履行が、当該契約の履行に必要のない個人データの処理に対する同意を条件としているか否かについて、最大限の考慮が払われなければならない。

[9]『BCR とは、「事業者グループまたは共同経済活動に従事する事業者グループ内で、1 ヵ国または複数の EU 域外の第 3 国の管理者または処理者に向けて個人データ移転または一連の個人データ移転のため、EU 加盟国の領域上にある管理者または処理者によって遵守される個人データ保護方針」をいう（第 4 条 20 号）。BCR は、GDPR の対象である個人データが、十分なレベルの保護が確保されているとみなされない EEA 外の国に EEA 内から移転される場合に、当該個人データに対して適切な保護を提供する法的手段である。』『「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（実践編）（2017 年 8 月）』pp.6

[10]『BCR を実施するために DPO を選任することは義務ではない。管理者および処理者は、次のいずれかの要件を満たす場合には DPO の選任義務がある（第 37 条 1 項、4 項）。

(1) 処理が公的機関または団体によって行われる場合（但し、司法権に基づく裁判所の行為を除く）

(2) 管理者または処理者の中心的業務が、その性質、適用範囲および/または目的によって、大規模にデータ主体の定期的かつ系統的な監視を必要とする作業である場合

出典:「EU 一般データ保護規則(GDPR)」に関わる実務ハンドブック(入門編) 表 9 pp.23

また、データ主体から個人データを収集する場合、管理者は、データ主体に以下の情報を提供しなければならない。

- 管理者と(該当する場合には)代理人および/またはデータ保護責任者(DPO)の身元および連絡先詳細
- 処理の目的および法的根拠
- 処理の法的根拠としての管理者または第三者が追求する正当な利益
- 個人データの受取人または受取人の種類
- 管理者の EEA 域外の第三国または国際組織への個人データの移転の意思、および十分性決定の有無、または(該当する場合には)適切な保護措置への言及や当該コピーの入手方法、または入手先
- 個人データの保管期間、期間の決定ができない場合には決定の基準

(3) 管理者または処理者の中心的業務が、第 9 条で言及された特別カテゴリーの個人データまたは第 10 条で定める有罪判決および犯罪に関する個人データを大規模に処理する場合
(4) EU または加盟国の法律(例:ドイツ)で DPO の選任が義務付けられている場合
・2017 年 7 月 5 日、GDPR 施行のための新ドイツ連邦データ保護法が成立した。
・データ保護責任者の選任に関して、法案は現在のドイツデータ保護法の規定を維持しており、個人データの自動的処理に関して少なくとも 10 名の従業員を雇用する企業は、DPO を選任する義務を負う。GDPR では、例外的な場合においてのみ、企業に選任義務が課されている。
・管理者および処理者は、GDPR 第 35 条に基づくデータ保護影響評価が必要な処理を行う場合、DPO を選任しなければならない。これは個人データが商業上のデータ移転またはマーケティングもしくは市場調査の目的で行われる場合にも当てはまる。』『「EU 一般データ保護規則(GDPR)」に関わる実務ハンドブック(実践編)(2017 年 8 月)』 pp.20

- 監督機関に苦情を申し立てる権利を含めた、データ主体の権利
- 同意をいつでも撤回することができる権利
- プロファイリング(自然人の個人的な側面を評価するため、または、自然人の職務業績や経済状態、健康状態、個人的な嗜好、関心、信頼性、行動、所在、移動などを分析したり、評価したりするために個人データを利用する、あらゆる形式の個人データの自動的な処理)および処理に利用するロジックに関する有意な情報や、データ主体に対する処理の意義や想定上の結果を含む、自動化判断(automated decision-making)の有無
- 個人データの提供が、法律上または契約上の義務、または契約を締結するのに必要な要件であるか否か、およびデータ主体に個人データの提供の義務があるか否か、ならびに、当該データ提供の不履行により起こり得る結果

次に、「「個人データの EEA 域外への移転を適法化するための同意」の要件としては、明示的な同意があったといえるためには、個人データを EEA 域外へ移転させることを説明した上で、この移転に対し同意するかどうかを「はい」または「いいえ」で回答させることが典型的な形となる。これについては、チェック欄を設けて、

「このチェック欄にチェックを入れた場合には、当該個人データの日本への移転について明示的に同意したものとみなします」としてチェックをさせるといった形が考えられる[11]。ただし、チェック欄にデフォルトでチェックが入っていた場合は、自由意志で同意が行われたとはみなされず、同意は無効となる。

以上の通り、GDPR 準拠の同意取得には、複雑な手続きが必要となる。また、同意の証明については、第 29 条作業部会（Article 29 Working Party）[12]からガイドラインの公表が予定されている。

次に、利害関係者との連携であるが、GDPR では、個人データの利害関係者として、データ管理者、データ処理者、データ受領者、第三者、データ保護責任者、監督機関、欧州データ保護役員会の役割が定義されている。

- データ管理者（Controller）
  - GDPR が定義する個人データの取扱いの目的や手段を決定する、単独または共同の自然人や組織であり、個人データ処理要件を遵守する責任者。
- データ処理者（Processor）
  - データ管理者に代わり個人データを処理する自然人や組織であり、データ管理者が兼務することもある。兼務していない場合には、データ管理者がデータ処理者による個人データ処理に責任を負う。
- データ受領者（Recipient）
  - 個人データが開示される先の自然人や組織であり、個人データを収集・取得する主体とは異なる。
- 第三者（Third Party）
  - データ主体、データ管理者、データ処理者、データ管理者かデータ処理者の下でデータ処理権限をもつ者、以外の自然人、法人、組織、機関。
- データ保護責任者（Data Protection Officer: DPO）
  - 条件に該当する場合に任命され、GDPR で定められている要件をデータ管理者とデータ処理者に対して通知・勧告し、データ管理者およびデータ処理者の管理・処理業務を監視する。データ管理者とデータ処理者から独立し、監督機関との連携も行う。
- 監督機関（Supervisory Authority）
  - GDPR にもとづく個人データの保護を監視する EU 各国に設置された独立公的機関で、不服申し立てや違反時の通知を受け付ける。
- 欧州データ保護役員会（European Data Protection Board）
  - 欧州データ保護監督機関（既存の EU データ保護指令 Directive 95/46/EC により設置されたデータ保護監督を行う独立機関）の代表で構成され、EU 内役員会として、GDPR の履行を監督する監督機関の代表。

GDPR のもっとも重要な義務の一つは、個人データ漏洩時 72 時間以内に監督機関へ通知することである。72 時間という短時間で通知を行うためには、これら利害関係者と連携する体制を十分に整えておく必要が

[11] 以上は、「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編） Q17 pp.23 から引用。

[12] 第 29 条作業部会は、EU データ保護指令第 29 条に基づき 1996 年に設置されたアドバイザリー機関であり、EU 加盟国の専門家代表で構成されている。
http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

ある。この通知義務に違反した場合も、高額の制裁を課される可能性がある。

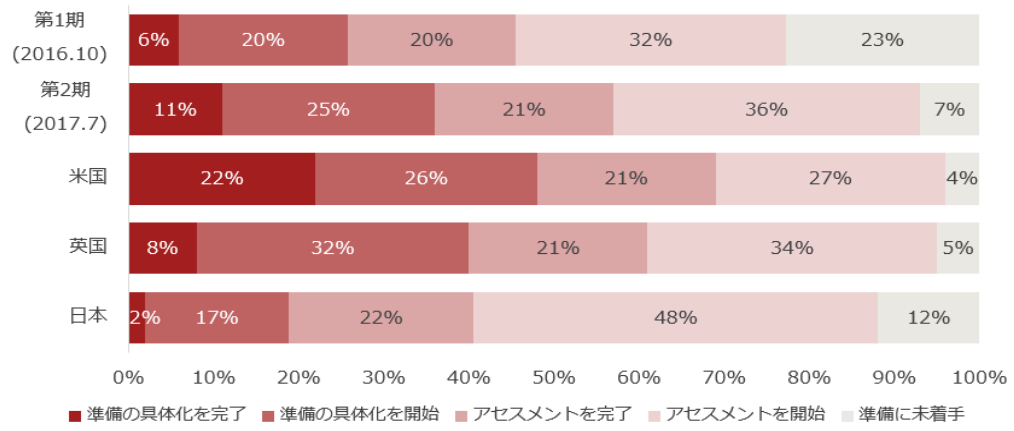
・米国企業の **GDPR** への対応状況
MediaPro の調査によれば、米国企業の 54%が GDPR への対応を最優先事項だとしているにもかかわらず、米国企業勤務の回答者の 59%が GDPR について初めて聞いたと回答した。業種別に見ると、GDPR について初めて聞いたと回答したのは、金融業界で 52%、テクノロジー業界で 42%、ヘルスケア業界で 53%、サービス業界で 56%、小売業界で 65%、教育業界で 78%、公務員で 70%、その他で 69%であった。調査の結果、GDPR に向けてプライバシーと個人情報の取り扱いについて教育を行い、企業の文化と意識を変革する必要があることが明らかになった[13]。

ネットワーク・セキュリティ装置ベンダー、ウォッチガード・テクノロジーが行い、2017 年 9 月に発表した世界 1,600 組織以上が参加したグローバル・サーベイでは「37%もの回答者が GDPR への遵守義務があるのかどうかさえ知らず、4 分の 1 以上（28%）が、遵守義務がないとの認識」であった[14]。

2017 年 6 月に PwC Global が実施した GDPR への対応状況調査では、GDPR コンプライアンス準備の進捗状況について、「準備の具体化を完了した」とする米国企業が 22%であるのに対して、日本企業は 2%にとどまっている。また、『GDPR 対応に対する投資額を比較すると、アセスメントが完了したとする企業のうち、62%の企業が 100 万ドル（約 1 億 1200 万円）以上、26%が 500 万ドル(約 5 億 6000 万円) 以上の投資を見込んでおり、運用具体化が完了したと回答した企業のうち、88%の企業が 100 万ドル以上を、59%の企
業が 500 万ドル以上の投資を予定している。』[15]。

図表 **3**：**GDPR** コンプライアンス準備の進行状況

[13] https://www.helpnetsecurity.com/2018/01/10/usa-employees-unaware-gdpr/
[14] https://www.watchguard.co.jp/press-release/170915.html
[15] https://www.pwc.com/jp/ja/knowledge/thoughtleadership/gdpr.html



出 典 ：PwC Japan[16]

しかし、GDPR 対応タスクフォースを内部で結成している組織は米国で 47%、英国で 39%に過ぎず、GDPR のギャップ分析を行うために第三者を雇っているのは 3 分の 1 であり、コンプライアンス遵守支援のために第三者のコンサルタントを雇っているのはおよそ 3 分の 1 に過ぎない。このことは、多くの企業は万全の準備が出来ていないということを示唆している。GDPR への対応は膨大な作業であり、専従のリソース抜きに対応することは困難だからである。大規模な個人のモニタリングに関わる企業にとって GDPR コンプライアンスの上で決定的に重要であるにもかかわらず、DPO やプライバシー担当者を雇っているのは、英国で 29%、米国有力企業の 18%に過ぎない[17][18]。

・企業の **GDPR** への対応事例現時点で GDPR は施行前であり、準拠ガイドラインもすべて発表されていない状況であり、各社は現時点
で考えられる実務的な対応を行っているのが実際である。

GDPR に対応するためには、ウェブやスマートフォン App のユーザーエクスペリエンス設計レベルで、具体的な対応に落とし込む必要がある。例えば、同意取得をサービスの条件提示の条件にしてはならない。また、ユーザーの同意を得るに当たって、オプトイン（事前承諾）となるチェック済みのチェックボックスを提示しても、ユーザーの自由意志に基づく同意を得たとは見做されない。そして、個人データの利用法に応じて、同意取得についても必要十分なレベルの同意をケース毎に得る必要がある。同意に基づき個人データを利用する自社及び他社も明記しなければならない。さらに、同意の撤回についても、同意と同様に容易なものとしなければならない。ユーザーエクスペリエンス設計に当たっては、こうした点を考慮して行う必要がある[37]。

[16] https://www.pwc.com/jp/ja/knowledge/thoughtleadership/gdpr.html
[17] http://www.computerweekly.com/news/450432510/Top-UK-and-US-firms-still-overestimating-GDPR-readiness
[18] https://www.econsultancy.com/blog/69253-gdpr-10-examples-of-best-practice-ux-for-obtaining-marketing-consent

また、GDPR への対応は、社内の大規模なプロジェクトとなるため、実施にあたり計画的に行う必要がある。準備段階では、主な社内利害関係者への根回し、GDPR 対応チーム結成、社内関連部門の特定と確認、第三者によるデータ処理範囲の特定と確認、個人データを保管する中央サーバーの設置、データ保護ポリシーとプライバシー通知の改定と配布、社内外の個人データ取扱者に対する研修といった活動を行わなければならない。対応活動では、社外へのプライバシー通知の周知と管理、法的手続きのメカニズムの検証と記録、データ主体からの権利要求の処理と記録、第 3 国へのデータ移転の検証と記録、個人データ漏洩時の報告と管理といった課題に対応する必要がある。施行後の維持運営に当たっては、データ保護ポリシー理解のエビデンス、個人データ処理登録の適正な実施の確認、業務変更による影響評価の実施、第三者の個人データ処理のコンプライアンス確認、個人データ取り扱いの有効性実証といった活動を行っていくことが求められる[19]。

クラウドサービスを提供する各社では、自社が提供するサービスの GDPR 対応と共に、顧客のクラウドサービス利用に際して、これら各社はデータ処理者となり、データ管理者である顧客に代わり個人データを処理することになる。Google[20]、Amazon[21]など各社では、クラウドサービスを利用する顧客に対しても、GDPR 対応の周知に努めている。Google では、Gmail から Google Docs に至るまでの様々な同社のサービスにおいて、ユーザーがどのデータを共有するかを選択できるようにした。GDPR では、データを処理する前にユーザーの同意を得ることが必要になるため、同意合意書を書き直し、データの処理も容易になるような方式に改め、多くの製品の手直しを行った。Amazon ではクラウド・ストレージのデータ暗号化を強化し、データ処理の方法に関するユーザーとの同意取得を単純化すると共に、ユーザーがデータを保存する地域を、ヨーロッパあるいはその他の地域から選択できるようにした。こうした有力企業のオンラインでのプライバシーやデータ処理の取り扱い方の動向は、その他の多くの企業が参考にするとみられる[22]。
Facebook のターゲット広告[23]では、広告クライアントに広告ターゲット選択肢として、98 点の個人情報（下記）を挙げている。この中には、何らかの推論を利用している項目もあるとみられる[24]。だが、英 Financial Times が各社の GDPR 対応進捗状況を確認するために、GDPR だけでなく英国 UK 1998 Data Protection Act でも認められているデータ主体によるデータ開示要求を行ったところ、Facebook と Amazon からは回答が得られなかったことを、2018 年 2 月 8 日の記事で明らかにしている[25]。また、欧州でももっとも厳格な消費者保護制度を持つとされるドイツで、連邦消費者センター連盟（VZBZ）が Facebook のデフォルトのプライバシー設定とデータ利用はドイツの消費者保護法に違反するとして訴えた裁判で、2018 年 2 月、ベルリン地方裁判所は訴えを認め、Facebook は敗訴している[26]。2017 年 9 月には、スペインの個人情報保護庁

[19] https://www.infosecurityeurope.com/__novadocuments/355669?v=636289786574700000
[20] https://www.google.com/cloud/security/gdpr/
[21] https://aws.amazon.com/jp/compliance/gdpr-center/
[22] https://www.nytimes.com/2018/01/28/technology/europe-data-privacy-rules.html
[23] https://www.facebook.com/ads/about/?entry_product=ad_preferences
[24] https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-totarget-ads-to-you/?utm_term=.57c83e5866e8
[25] https://www.ft.com/content/5c1987d2-05d2-11e8-9650-9c0ad2d7c5b5
[26] https://www.theguardian.com/technology/2018/feb/12/facebook-personal-data-privacy-settings-ruled-illegalgerman-court

(Agencia Española de Protección de Datos、AEPD)が、Facebook 社のデータ保護法違反に対して、120 万ユーロの罰金を課している[27]。GDPR の Facebook への影響を懸念する声も、株式市場では出始めている[28]。

しかし、Facebook でも、Facebook および Instagram、Oculus、WhatsApp を含む関連企業における個人情報の取り扱いはすべて、GDPR 基準に準拠する予定であるとしている[29]。Facebook では、GDPR への対応について、会社設立以来最大のプロジェクトとして取り組んでいる[30]。2018 年 1 月 29 日には、同社のプライバシー原則を初めて公開し、新たなプライバシー設定「グローバル・セキュリティ・センター」の導入準備を進めていることも明らかにしている [5031]。Facebook の新たな「グローバル・セキュリティ・センター」は、これまで Facebook 内の各所に分散されていた為にユーザー自身による管理が困難だった、ユーザーの投稿公開範囲及びデータ共有を認める広告の種類について、一つのページにまとめ、ユーザーが自身で管理できるようにしたものである。また、Facebook は 2017 年 11 月には、人工知能を利用してユーザーの自傷行為をモニタリングするプログラムを公開したが[32]、メンタルヘルスなどの健康上の敏感なデータにアクセスする同意を得なければならないために、欧州では公開しない。ユーザーの写真が投稿されたことを追跡する顔認識技術[33]も欧州では利用しない[34]。

（参考）**Facebook** ターゲット広告で広告主に提示されるターゲット選択肢[35]
1.場所、2.年齢、3.世代、4.性別、5.言語、6.学歴、7.専攻分野、8.学校、9.人種、10.収入と純資産、11.住宅所有とタイプ、12.住宅価格、13.住宅サイズ、14.敷地面積、15.家を建築した年、16.世帯構成、17. 30 日以内に記念日を迎えるユーザー、18.家族や故郷から離れているユーザー、19.記念日を迎える友人を持ち、新たに結婚あるいは婚約をしたか、最近転居をしたか、または誕生日が近づいているユーザー、20.遠距離恋愛にあるユーザー、21.新たな恋愛関係にあるユーザー、22.新たな仕事についたユーザー、23.新たに婚約したユーザー、24.新たに結婚したユーザー、25.最近転居したユーザー、26.すぐに誕生日を迎えるユーザー、27.親、28.新たに子供を持つ親、29.「タイプ」（教育熱心、トレンディーなど）別の母親、30.政治に係る可能性のあるユーザー、31.保守派とリベラル派、32.交際状況、33.雇用主、34.業種、35.役職、36.オフィスタイプ、37.関心、38.オートバイを所有しているユーザー、39.車を購入しようとしているユーザー（そして、どのような種類/ブランドの車か、どのくらいのうちにか）、40.最近自動車部品やアクセサリーを購入したユーザー、41.自動車部品やサービスが必要と思われるユーザー、42.運転する自動車のスタイルとブランド、43.車の購入年、44.車の年数、45.ユーザーが次の車にどれくらい支払う可能性があるか、46.ユーザーが次の車を購入

[27] http://www.telegraph.co.uk/technology/2017/09/11/facebook-hit-12m-fine-spain-breaking-privacy-laws/
[28] http://www.businessinsider.com/wall-street-worrying-about-effect-of-gdpr-on-facebook-2018-2
[29] https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliancewith-the-gdpr
[30] http://www.kenpoushinsa.sangiin.go.jp/kenpou/houkokusyo/houkoku/03_26_01.html
[50] https://japan.cnet.com/article/35113897/
[31] https://www.facebook.com/about/basics/privacy-principles
[32] http://www.itmedia.co.jp/mobile/articles/1611/01/news049.html
[33] http://jp.techcrunch.com/2017/12/20/2017-12-19-facebook-facial-recognition-photos/
[34] https://www.nytimes.com/2018/01/28/technology/europe-data-privacy-rules.html
[35] https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-totarget-ads-to-you/?utm_term=.57c83e5866e8

する可能性が高い場所、47.勤務会社の従業員数、48.中小企業を所有するユーザー、49. 経営幹部や役員であるユーザー、50.慈善活動に寄付したユーザー（種類別）、51.OS、52.キャンバスゲームをプレイするユーザー、53.ゲーム機を所有するユーザー、54.Facebook イベントを作成したユーザー、 55. Facebook Payments を使用したユーザー、56. Facebook Payments で平均より多くの額を費やしたユーザー、57. Facebook ページを管理するユーザー、58.最近 Facebook に写真をアップロードしたユーザー、59.使用インターネットブラウザ、60.使用電子メールサービス、61.新たな技術を受け入れるのが早いか、遅いか、62.駐在員（国別）、63.信用組合、国営銀行、地域銀行に勤務するユーザー、64.投資家（投資タイプ別）、65.信用限度額、66.クレジットカードの有効なユーザー、67.クレジットカードの種類、68.デビットカードを持っているユーザー、69.クレジットカードで残高を持っているユーザー、70.ラジオを聴くユーザー、71.テレビ番組の嗜好、72.モバイルデバイス・ユーザー（使用するブランド別）、73.インターネット接続タイプ、74. 最近スマートフォンやタブレットを購入したユーザー、75.スマートフォンやタブレットからインターネットにアクセスするユーザー、76.クーポンを使用するユーザー、77.ユーザー世帯が購入した衣類のタイプ、78.ユーザー世帯が買物を多くする時期、79.ビール、ワイン、またはスピリッツを大量に購入するユーザー、80.食料品購入ユーザー（及びその種類）、81.美容品購入ユーザー、82.アレルギー薬、咳/風邪薬、鎮痛薬、および店頭薬を購入するユーザー、83.家庭用品に支出するユーザー、84.子供やペット向け製品を購入するユーザー（ペットの種類）、85.世帯として平均以上の支出をするユーザー、86.オンラインあるいはオフラインで買い物をする傾向のあるユーザー、87.ユーザーが利用するレストランの種類、88.ユーザーが買物をする店舗の種類、89.オンライン自動車保険、高等教育または住宅ローン、およびプリペイドデビットカード/衛星テレビを提供する企業からのオファーを「受け入れやすい」ユーザー、90.ユーザーが家にいる時間の長さ、 91.すぐに転居する可能性のあるユーザー、92.オリンピック、フットボール、クリケット、ラマダンに興味のあるユーザー、93.仕事や娯楽のために頻繁に旅行するユーザー、94.通勤するユーザー、95.ユーザーが取る休暇のタイプ、96.最近旅行から帰ったユーザー、97.最近旅行アプリを使用したユーザー、98.タイムシェアを利用しているユーザー

（3） 日米欧の個人情報保護に対する定義・考え方の違い

EU の GDPR は日本や米国の個人情報保護・プライバシー関連法と比べて、定義や考え方に大きな違いがある。GDPR は、プライバシーを基本的人権と捉えた個人情報保護に関する包括法である。日本では、プライバシーの権利は憲法上も明文化されておらず、各種判例によってプライバシーを保護している[36]。日本の個人情報保護は、2003 年 5 月 23 日に成立した「個人情報の保護に関する法律（平成 15 年法律第 57 号）」が包括法として基になっている。米国では、憲法上もプライバシーを基本的人権とする法律はないため包括法もなく、必要に応じて業界ごとに対応する法律を設けている。

日米欧の個人データ保護に関する法律には、次表のような定義や考え方の違いがある。国境を越えたインターネットの発展やグローバル化が進む中で、GDPR の施行は EU 内にとどまらず、EU とビジネスを行う全ての国に大きなインパクトを及ぼすものである。

[36] http://www.kenpoushinsa.sangiin.go.jp/kenpou/houkokusyo/houkoku/03_26_01.html

図表 **4**:日米欧の個人情報保護・プライバシー関連法

	日本	米国	**EU**
法律	個人情報保護法:包括法	分野毎の各法律(2015 年 9 月号参照)	General Data Protection Rule (GDPR):包括法
施行時期	2005 年 4 月 1 日(全面施行)	各法律による	2018 年 5 月 25 日
個人データ(情報)の定義	生存する個人に関する情報であって、特定の個人を識別することができるもの(他の情報と容易に照合でき、それにより特定の個人を識別することができるもの含む)又は個人識別符号が含まれるもの	各法律によって異なる	個人データを、直接的または間接的に識別あるいは識別可能な EU 内に所在する自然人に関する情報
個人データ(情報)の対象	携帯電話番号、端末 ID、クレジットカード番号、会員 ID、IP アドレス、クッキーID、位置情報などは単体では対象外(ただし、複数情報を組み合わせて特定の個人を識別し得る場合は、これらも個人情報に含まれる)	各法律によって異なる	携帯電話番号、端末 ID、クレジットカード番号、メールアドレス、会員 ID、IP アドレス、クッキーID、位置情報も対象
データ主体の権利	開示、訂正等、利用停止等及び第三者提供の停止を請求する権利など	COPPA 、HIPPA 、FCRA では定義されているが、その他の法律では定義なし	同意撤回の権利、異議申立ての権利、通知を受ける権利、データの訂正・消去を求める権利など
データ主体への同意	目的外利用、要配慮個人情報の取得時、第三者提供時に同意を規定	基本的にはデータ主体への同意を求めているが、内容は各法律で規定	厳格な規定あり
データ漏洩時の監督機関への通知	個人情報保護委員会等に速やかに報告するように努める義務	ほとんどの州が制定している州法で規定	データ漏洩発覚から 72 時間以内の監督機関への通知義務
違反時の制裁	個人情報保護委員会の命令に違反した場合や報告徴収・立入検査に協力しなかった場合等に、罰則を規定。なお、個人情報データベース等不正提供罪に該当する行為については直罰規定があり、罰則として 1 年以下の懲役あるいは 50 万円以下の罰金を規定	各分野の法律や州法に従う。個別の規定がない場合は、訴訟による賠償請求。あるいは、FTC の法執行	1000 万ユーロあるいは前会計年度全世界売上高の 2%のうち多い額、あるいは、2000 万ユーロあるいは前会計年度全世界売上高の 4%のうち多い額、このいずれかを最大とする金額の罰金

域外移転及び域外適用	域外移転としては、個人データを外国にある第三者に提供する場合が対象。域外適用としては、外国にある個人情報取扱事業者のうち、日本の居住者等国内にある者に対して物品やサービスの提供を行い、これに関連してその者を本人とする個人情報を取得した者が、外国においてその個人情報又は当該個人情報を	州法も含め、個人情報の海外移転を禁じる法律は見当たらない [57]	域外移転としては、個人データの第三国又は国際機関への移転が対象。域外適用としては、EU 内に拠点のない管理者又は取扱者による取扱いのうち、EU 在住のデータ主体に対する商品・サービスの提供に関する取扱い又は EU 域内で行われるデータ主体の行動の監視に関する取扱いは対象
	用いた匿名加工情報を取り扱う場合は対象		

[57] 2004 年、オハイオ州では、州の調達契約において、書面での同意無しには個人データを海外に移転してはならないとする法案が提案されたが、実現しなかった。同様の法案は、ミズーリ州などでも提案されている。2011 年に、ニューヨーク州議会では、事前の同意なしに消費者の個人情報を国外に転送することを禁止する法案が提案された。これは国外でのデータ保存は消費者のデータ漏洩等を危惧する形を取っていたが、地元企業の優遇を意図したものであった。
https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

出典：各種資料を元に作成

3　米国の個人情報の利活用動向

（1）各種情報機器から得られる個人情報の取り扱い（スマートフォン、スマートスピーカー、コネクテッドカー等）

・スマートフォンスマートフォン App（アプリ）はライブラリーを提供しているサード・パーティーに依存しているので、ユーザーが個別の App と同意を行っても、サード・パーティーは各 App の同意範囲以上の個人情報をユーザーとの直接の同意なしに得ている可能性がある。スマートフォン App の 70%以上は、パーソナルデータを、Google Analytics、Facebook Graph API、Crashlytics[37]といったトラッキングを行うサード・パーティーにレポートしている。例えば、地図情報 App を使うのに、現在の位置情報を使わなければ不便であるし、これ自体は問題ない。しかし、多くの App では、ユーザーの行動を解析し、ソーシャルメディアと結びつけて、広告を表示するサード・パーティーのライブラリーを利用している。こうした多くのライブラリーはセンシティブなデータを収集している。こうしたライブラリーの開発者はユーザーのプロファイルを詳細に把握することができる。ユーザーが別々の App を利用していても、その App 両方が同じライブラリーを使用していれば、ライブラリーを提供しているサード・パーティーは両方の情報を組み合わせることが出来る。例えば、ユーザーは、それぞれの App に対して別々に個人情報の利用を許可していても、地図 App とメッセージ App からの情報を組み合わせれば、サード・パーティーはどこで誰と会おうとしているかということまで把握することができる。
App 側では、どのようなライブラリーを使っているかについてまでユーザーに対して知らせることはないので、ユーザー側では自分の情報がどのように把握されているのかを知ることはない。App がどのようなサイトに情報を送信しているのかを調べる App を開発し、1600 名以上が利用している 5000 以上の App について調

[37] https://try.crashlytics.com/

査したところ、広告目的でユーザーをトラッキングしている 598 のインターネット・サイトが明らかになった。ここには、Facebook、Google、Yahoo、Verizon Wireless などが含まれている。調査では、70%以上の App が少なくとも 1 つのトラッキング・サイトに接続し、15%は 5 つ以上のトラッキング・サイトに接続していた。電話番号やデバイス固有の 15 桁の IMEI 番号[38]といったデバイス識別子を利用しているトラッキング・サイトは、4 分の 1 に上った。App トラッキング・サイトは、スマートフォンだけではなく他のデバイスでの利用も結びつけて、クロス・デバイスでユーザーのオンライン上のパーソナリティーを把握していた。こうしたトラッキング・サイトは独立企業であるとは限らない。例えば、Google の親会社、Alphabet の傘下には、Google Analytics、DoubleClick、AdMob といったトラッキング・サイトがあり、調査した App の 48%以上からデータを収集していた。こうして収集されたトラッキング・サイトのデータの 60%以上は、米国、英国、フランス、シンガポール、中国、韓国に存在するサーバーに送られる。これらの国では、監視技術が運用されており、厳格な個人情報保護法が機能しているとは限らない。ドイツ、スイス、スペインのような厳格な個人情報保護法のある国に住んでいても、こうしたサーバー所在地の政府機関によってデータにアクセスされる可能性が潜在的にある[39][40]。

・スマートスピーカー

2018 年の CES（Consumer Electronics Show）では、音声認識を利用した様々な「スマート・ホーム」機器が発表された。Amazon Alexa や Google Assistant、Apple 社の Siri といった先行各社のスマートスピーカーだけではなく、テレビ[41]、サーモスタット、照明スイッチ[42]、冷蔵庫[43]、シャワー[44]から便器[45]に至るまで、Amazon や Google の音声認識を利用した音声認識機能を持つ様々な商品が発表されている。現在、Google Assistant は、Android デバイスだけでなく iPhone まで含めて、全世界の 4 億台のデバイスで利用可能であり、1500 以上の「スマート・ホーム」デバイスで利用されている。Amazon の Alexa も、2017 年のホリデーシーズンだけでも世界中で数千万台が販売されたとしている。こうした機器では、周囲の雑音や他の家族の声といった周囲の環境への対応、コンテクストを理解する能力などの課題も指摘されている。しかし、同時にプライバシー面からの不安も指摘されている。検索キーワードのマーケティング利用だけではなく、これらのデバイスが本当に起動していないときでも音声を録音・利用していないのかという点である。これらのデバイスは、「OK、Google」、「Hey, Siri」、「Alexa」といった起動ワードで話しかけると瞬時に起動する。これらのデバイスは、直前の数秒の音声を常に録音あるいは認識しており、起動ワードを認識すると動作を開始する。これについては、本当に起動ワードを認識しているだけなのか、プライバシーを侵害されないのかという懸念が潜在的にある[46][47]。ある商品について会話した翌日にその商品をウェブ広告で目にすることになっても、それが前日の会話からスマートスピーカーが得た情報によるものなのか、単なる偶然なの

[38] https://www.gsma.com/services/mobile-equipment-identity/about-imei/
[39] https://www.scientificamerican.com/article/7-in-10-smartphone-apps-share-your-data-with-third-party-services/
[40] https://arxiv.org/pdf/1609.07190.pdf
[41] https://www.cnet.com/news/ces-2018-press-day-news/
[42] https://www.cnet.com/news/idevices-put-alexa-into-a-light-switch-at-ces-2018/
[43] https://www.cnet.com/news/heres-whats-next-for-samsung-family-hub-smart-fridge-ces-2018/
[44] https://www.engadget.com/2018/01/07/moen-alexa-siri-shower-start/
[45] https://www.theguardian.com/technology/2018/jan/12/ces-2018-voice-controlled-showers-robots-smart-toilets-ai
[46] https://www.scientificamerican.com/article/alexa-what-are-you-doing-with-my-familys-personal-info/
[47] https://www.pcworld.idg.com.au/article/632878/my-smart-speaker-always-listening/

かは分からない。こうしたプライバシーに対する不安から、アメリカ人の 27%はボイス・アシスタント機能を使わな
いという調査結果もある[48]。

・コネクテッドカー
コネクテッドカーでは、ワイヤレス・ネットワークを通じて、運転の安全性確保のための情報を取得し、周囲の環境からコネクテッドカーが取得した大量の画像データなどをクラウドに送信することで、様々な情報の利活用が期待されている。コネクテッドカーもネットワークに接続する情報機器であり、実際に走行中のコネクテッドカーをハッキングして乗っ取れ得ることが、既に実証されている[49]。コネクテッドカーが扱う情報にはユーザーの位置情報などの個人情報も当然含まれることになり、個人データの取り扱いが問題となる。

実際、すでに Tesla 社の最新車には、定期的なワイアレス・アップデートで安全機能とナビゲーション機能が追加され、交通状況がリアルタイムで更新される地図とナビゲーションが装備されている[50]。Tesla 社では、利用規約の中でプライバシー・ポリシーについて説明しており、「当社の製品とサービスの利用に関し、主に（1）お客様またはお客様のデバイスからの情報およびお客様またはお客様のデバイスに関する情報、（2）お客様のテスラ車両からの情報および同車両に関する情報、（3）お客様のテスラエネルギー製品からの情報および同製品に関する情報、の 3 種類の情報を収集」することを説明している[51]。

GDPR の下で、コネクテッドカーからのデータをどう扱うべきかについてルールを明確に定めるには、まだ時間がしばらくかかるとみられている。しかし、現状でも、レンタカーの情報エンターテイメントシステムに Bluetooth を通じてスマートフォンを接続すれば、車のシステムにユーザーの個人情報が残るため、この情報をレンタカーの返却前に自分で消去しなければ、レンタカー業者が一々消去してくれているとは限らないため、個人情報がここから流出する危険性がある[52][53]。

（2）Google、Apple、Facebook、Amazon（”GAFA”）による個人情報寡占

Google、Apple、Facebook、Amazon をまとめて GAFA と呼ばれることがあるが、これは元々フランスで生まれた呼称である。その背景としては、この米国 4 社による圧倒的な情報支配に対する欧州の警戒と反発がある[54]。

図表 **5**：**GAFA** 各社の売上高と時価（**2018** 年 **2** 月現在）

	Google(Alphabet)	Amazon	Facebook	Apple
設立	1998 年 9 月 7 日	1994 年 7 月 5 日	2004 年 2 月 4 日	1976 年 4 月 1 日

[48] https://www.forbes.com/sites/blakemorgan/2018/02/05/are-digital-assistants-always-listening/#7e302edb4eeb
[49] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[50] https://www.tesla.com/jp/modelx
[51] https://www.tesla.com/jp/about/legal?redirect=no
[52] https://privacyinternational.org/report/987/connected-cars-what-happens-our-data-rental-cars
[53] https://www.theregister.co.uk/2018/02/14/connected_vehicles_data_and_privacy/
[54] https://qz.com/303947/us-cultural-imperialism-has-a-new-name-gafa/

本社	カリフォルニア州マウンテンビュー	ワシントン州シアトル	カリフォルニア州メンロパーク	カリフォルニア州クパチーノ
2017 年度売上高	1109 億ドル	1778 億ドル	406 億ドル	2292 億ドル
時価総額	7610 億ドル	7058 億ドル	5117 億ドル	8770 億ドル

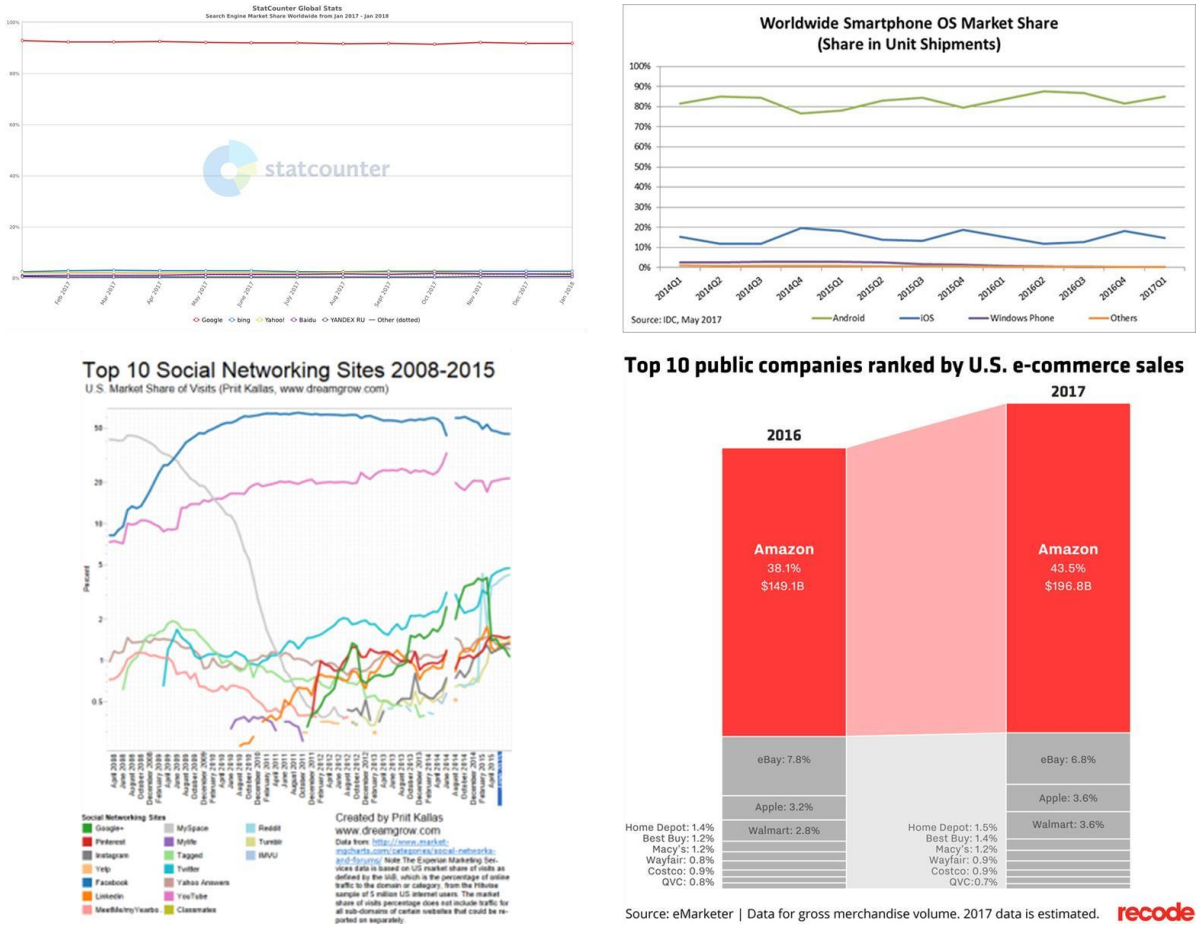
出典:各種資料を元に作成

上図の GAFA 各社の売上高に近い GDP を 2016 年度時点で持つ国としては、GAFA それぞれに対して、クウェート(1109 億ドル)、ニュージーランド(1850 億ドル)、リトアニア(427 億ドル)、フィンランド(2385 億ドル)といった国の名前が挙がる。一私企業とはいえ、GAFA 各社は中小国に匹敵するレベルの経済規模をもっていることになる[55]。

ユーザー数で見ると、Google の全ユーザーは 22 億人(2015 年[56]、Android のユーザーは 20 億人(2017 年)[57])、Amazon のアクティブ・ユーザー・アカウントは 3 億 400 万人[58]、Facebook のアクティブ・ユーザーは 22 億人[59]、Apple のユーザーは 5 億 8800 万人[60]と言われる。これらの企業は、必ずしもユーザー数を公開している訳ではなく、推計も含まれる。

[55] http://databank.worldbank.org/data/download/GDP.pdf
[56] https://www.forbes.com/sites/stevedenning/2015/04/23/has-google-really-died/#1b264bee466c
[57] https://techcrunch.com/2017/05/17/google-has-2-billion-users-on-android-500m-on-google-photos/
[58] https://www.statista.com/statistics/237810/number-of-active-amazon-customer-accounts-worldwide/
[59] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
[60] http://www.businessinsider.com/credit-suisse-estimates-588-million-apple-users-2016-4

図表 **6**:**GAFA** の市場シェア:サーチエンジン世界市場シェア(左上)、スマートフォン **OS** 世界市場シ ェア(右上)、**SNS** サイト訪問者数全米シェア(左下)、全米 **e** コマース市場シェア(右下)



出典:statcounter(左上)[61]、IDC(右上)[62]、Dreamgrow(左下)[63]、recode(右下)[64]

サーチエンジンの市場シェアは、Google が 90%以上を握っており、Bing、Yahoo!、Baidu を圧倒している(上図左上)[65]。スマートフォン OS のシェアは、Google の Android が 85%前後、Apple の iOS が 15%程

[61] http://gs.statcounter.com/search-engine-market-share
[62] https://www.idc.com/promo/smartphone-market-share/os
[63] https://www.dreamgrow.com/top-10-social-networking-sites-by-market-share-of-visits-august-2015/
[64] https://www.recode.net/2017/10/24/16534100/amazon-market-share-ebay-walmart-apple-ecommerce-sales-2017
[65] http://gs.statcounter.com/search-engine-market-share

度で推移しており、2 社で市場の 99%以上を握っている（上図右上）[66]。2015 年 8 月時点の全米 SNS サイト訪問者数シェアは、Facebook が 45.6%、Google の YouTube が 21. 6%、他のサイトは 5%以下であり、Facebook が他を引き離している（左下）[67]。2017 年の全米 e コマース市場では、Amazon のシェアは 43.5%であり、売上げは 1968 億ドルに達し、2 位以下の eBay6.8%、Apple3. 6%、Walmart3.6%を大きく引き離している（右下）[68]。

GAFA は、主力の製品・サービスにおいて圧倒的なシェアを占めており、こうした寡占状態ではネットワークの外部性が働き、製品・サービスの利便性はますます向上することになる。こうした状態では、多少の不便や強制的な個人データの提供を強いられても、利用し続けることの便益の方が大きいため、ユーザーは GAFA の製品・サービスを利用し続けざるをえないことになる[69]。

2017 年 3 月に米国の消費者に対して「Google、Apple、Facebook、Amazon といった国際的なインターネット企業について、以下の質問に同意するか」という質問をしたところ、「社会の不可欠な要素になっている」という点について 55%が同意した一方で、「個人データの保護を強化したい」と考えている回答者も 43%にのぼった。「社会生活をシンプルにした」と 37%の回答者が評価しているが、「社会への影響力が強くなりすぎている」とした回答者も 31%であり、「信用できるやり方で入手した消費者とユーザーのデータを適切に扱っている」とした回答者は 23%であった[70]。

EU では、Google、Facebook、Amazon といったインターネット・テクノロジー企業に対する税制の改革検討を進めている。欧州委員会では、現在の税制は前世紀に決められたものであり、現在のテクノロジーに照らしてオンライン経済活動の実情に合わないものになっているとして、徴税のあり方を再考するレポート"A Fair and Efficient Tax System in the European Union for the Digital Single Market"[71]を、2017 年 9 月 21 日に発表している。そこでは、従来の企業への課税が 23.2%であるのに対して、国際展開するデジタル企業への課税は 10.1%にとどまっていると指摘されている[72]。

2016 年の米国大統領選挙に関するロシアの投稿に利用されたとして名前の挙がった 2 社、Google と Facebook の 2017 年のロビー費用は、Google が 1800 万ドル、Facebook は 1150 万ドルであったが、Google、Facebook に加えて、Twitter のユーザーは、SNS を通じてロシアからの操作による広告、フェイクニュース、詐欺的な投稿を多く目にすることになったという疑いがもたれている。2017 年 10 月には、幹部が議会に召喚され、2018 年の中間選挙では内容のスクリーニング技術を改善する旨を誓っている。Amazon もまた、その規模に対する懸念、政府調達、配送ドローンといった案件に対するロビー活動に 1300 万ドル

[66] https://www.idc.com/promo/smartphone-market-share/os
[67] https://www.dreamgrow.com/top-10-social-networking-sites-by-market-share-of-visits-august-2015/
[68] https://www.recode.net/2017/10/24/16534100/amazon-market-share-ebay-walmart-apple-ecommerce-sales-2017
[69] https://www.economist.com/news/leaders/21735021-dominance-google-facebook-and-amazon-bad-consumersand-competition-how-tame
[70] https://www.statista.com/statistics/702587/perception-of-international-tech-and-internet-companies-in-us/
[71] https://ec.europa.eu/taxation_customs/sites/taxation/files/1_en_act_part1_v10_en.pdf
[72] https://www.theguardian.com/business/2017/sep/21/tech-firms-tax-eu-turnover-google-amazon-apple

を費やしている。移民規制と海外売上げを巡る税制度はテック大企業全般の課題であり、Apple もまた 700 万ドルをロビー活動に費やしている[73]。

GAFA の影響はテクノロジーの範疇にとどまらず、今や社会、政治、経済、文化のなかでも論じられている。

（3） 中国などの個人データ越境禁止に対する米国の反応

中国の代表的なインターネット企業、バイドゥ（百度、Baidu）社[74]、アリババ（阿里巴巴、Alibaba）[75]、テンセント（騰訊、Tencent）社[76]、ジンドン（京東、JD.com）社[77]の 4 社は、”BATJ”と総称される。現在、企業価値が 10 億ドルを超えるアジアのユニコーン企業は 60 以上あるが、そのうち 41%はこの BATJ の支援を受けている。また、中国国内のユニコーン企業のうち、この 4 社の支援を受けている割合は 46%になる。この 4 社のアジアにおける存在感は、ますます高くなっている[78]。

なかでも、Alibaba 社はデータ活用を武器に事業を拡大しており、2017 年の年間収益は 45～49%の成長を見込んでいるほどである。同社は、e コマース、映画配信、金融サービス、ロジスティックスなどのサービスを手がけ、ここから得られたユーザーの支出、位置情報、視聴履歴などのデータを、e コマース出品者のターゲット・マーケティングに利用しており、その大きな効果から中国のデジタル広告支出における最大のシェアを握っている。そして、その情報をサプライチェーンの効率化にまで活用している。7 億 3000 万人の中国のインターネット・ユーザーが生み出す e コマースとオンライン広告の市場は、2016 年で 9300 億ドルに上った。BATJ の 4 社は、ユーザーのデータを巡り、激しい競争を繰り広げている。しかし、中国の新たなサイバー・セキュリティ法の下では、政府はこうした個人データのほとんどすべてにアクセスできることになる[79]。

中国のサイバーセキュリティ法は、2017 年 6 月 1 日に施行された。この法律では、特定のデータを中国国内に保管することを「ネットワーク・オペレーター」に対して求めており、中国当局に「ネットワーク・オペレーター」に対して抜き打ち検査を行う権限を与えている。中国政府は、この法律は中国のサイバーセキュリティを世界レベルにすることを目指した法律であるとしている。外国企業の間では、この法律における用語の定義の曖昧さ[80]やガイドラインの未整備から不安が広がっており、18 ヶ月の段階的導入期間の間、様子を見る動きが取られている。

[73] https://www.bloomberg.com/news/articles/2018-01-24/google-outspends-tech-rivals-on-washington-lobbying-in2017
[74] http://ir.baidu.com/phoenix.zhtml?c=188488&p=irol-irhome
[75] https://www.alibaba.com/
[76] https://www.tencent.com/en-us/index.html
[77] http://corporate.jd.com/
[78] https://www.cbinsights.com/research/asian-unicorns-baidu-alibaba-tencent-jd-investors/
[79] https://www.ft.com/content/cca7f5ea-5567-11e7-80b6-9bfa4c1f83d2
[80] https://www.huntonprivacyblog.com/2017/06/09/china-releases-draft-guidelines-cross-border-data-transferspursuant-cybersecurity-law/

このサイバーセキュリティ法は、2016 年 11 月の全国人民代表会議で決議された。この法律も、2010 年の中国政府白書における「中国領土内において、インターネットは中国の主権下にある」という主張からの流れにある。中国政府は 2015 年 7 月以来、インターネットのコントロールと個人データへのアクセスに関する一連の法律と法案を導入してきた。

また同法は、「ネットワーク・オペレーター」と「重要分野」の事業に対して適用される。サイバーセキュリティ法では、「ネットワーク・オペレーター」とは、ネットワークの所有者、管理者、プロバイダーと定義されており、「ネットワーク」とは、情報を収集・保存・送信・交換・処理するコンピューターとその関連機器からなるあらゆるシステムと定義されている。つまり、電子メールやデータを扱うほとんどすべてのビジネスが対象になる。
「重要分野」の対象となるのは、通信、情報サービス、エネルギー、運輸、水道、金融サービス、公共サービス、電子政府サービスである。法律事務所 Baker McKenzie は、これら分野のサプライヤーやパートナーも、この法律の適用対象になる可能性があると指摘している[81]。そして、「ネットワーク・オペレーター」は、中国の犯罪や安全保障にかかわる問題に協力する義務があり、当局の求めに応じて、すべてのデータへのアクセスと「技術協力」（具体的な内容は定められていない）を提供しなければならない。また、「重要分野」の「ネットワーク・オペレーター」は、収集・生成したデータを中国本土内に保管しなければならない。中国市民に関するビジネス情報とデータは、中国国内のサーバーに保管しなければならず、許可なしに国外に持ち出すことはできない。

そのためこの法律は、外国企業の懸念材料となっている。抜き打ち検査と認証に際して、ソースコードや暗号などの重要情報について当局から提出を求められる可能性があり、地元競合企業への流出や中国政府により利用の可能性がある。また、定義と条文が曖昧であるため、中国国内の競合企業が抜き打ち検査を当局に要請するといったことに利用される可能性もある。データの中国国内保管に対応するためには、政府の抜き打ち検査の対象となるサーバーに投資するか、中国のファーウェイ社、テンセント社、アリババ社といったローカル・サーバー・プロバイダーに新たに費用を支払わなければならない。これらの企業は、第 12 次 5 カ年計画（2011～2015 年）の一環として、近年国内データセンターに巨額の投資を行ってきた[82]。

こうしたデータの越境を禁止する法律（”data residency law”）を制定する動きは、EU や中国だけではなく、世界中に広がりつつある。米国通商代表部（Office of the United States Trade Representative 、USTR）の 2017 年度報告書” 2017 National Trade Estimate Report on FOREIGN TRADE BARRIERS”[83]では、デジタル貿易障壁を「データの越境、デジタル製品、インターネットによるサービス、その他の技術要求に対する制限や差別的な活動」と定義している。この中で、2015 年、2016 年の中国政府が米国等の広範な ICT 製品・サービスを国産に置き換えようとする動きに対し、米国は懸念を示している。そして、2015 年の中国の国家セキュリティ法は情報安全保障を目的として謳っているが、経済産業政策上の意図が含まれており、2015 年 12 月のカウンターテロリズム法と 2016 年 11 月のサイバーセキュリティ法は ICT 製品・サービスの中国国内への輸入に対する貿易制限となっていると指摘している。この問題は、2015 年 9 月の習近平総書記の訪米時にも、当時のオバマ大統領との間で話し合われ情報技術分野における一連の原則が合意

[81] https://www.bakermckenzie.com/en/insight/publications/2017/04/china-releases-draft-rules/
[82] https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/
[83] https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf

された[84]。

こうした法律は、自国内のサービス・プロバイダーを優遇する保護主義につながるだけでなく、自国内にデータセンターを設立することを促し、直接投資を促進することになる。しかし、これはクラウド・コンピューティングの効率的なアーキテクチャー設計、言論の自由や国際貿易には障害となる。こうしたデータの越境を禁止する法律の制定は、民間部門と政府部門について、それぞれトレンドとなりつつある。民間部門で集められた個人データの越境を禁止する法律は、2015 年にロシアで制定されたのが最初である。同様の法律はカザフスタンでも施行されており、ブラジルも議論を進めている。また、政府のデータの越境を禁止する法律は、中国、インドネシア、カナダ、ナイジェリアで制定されている[85]。

McKinsey Institute のレポートによれば、国境を越えるデータの流通によって、2014 年には 2.8 兆ドルの GDP が生み出された[86]。しかし、データの越境を禁止する法律が各国に広がれば、経済発展の妨げとなりかねない。個人情報を自国内のサーバーに保存しなければならないというロシア当局の規制を受けて、LinkedIn はロシアでのビジネスを放棄した。また、オーストラリアはすべての医療データを自国内で保存することを求めているが、例えば、人工知能を活用したサービスを病院に提供しようとしても、サービス・プロバイダーは各国に施設を設置しなければいけないことになり、採算が見合わないとなれば、先端サービスから取り残されるようなことにもなりかねない。実際、LinkedIn は、ロシアでの法律が変わらない限り、比較的小さなロシア市場に参入する意思を持っていない[87]。欧州国際政治経済研究所（European Centre for International Political Economy、ECIPE）の 2014 年のレポート[88]によれば、こうしたデータの越境を禁止する法律が GDP に与える影響は、ブラジルで－0.2%、中国－1.1%、EU－0.4%、インド－0.1%、インドネシア－0.5%、韓国－0.4%、ベトナム－1.7%になると試算されている。

4　今後の展望、日本への示唆

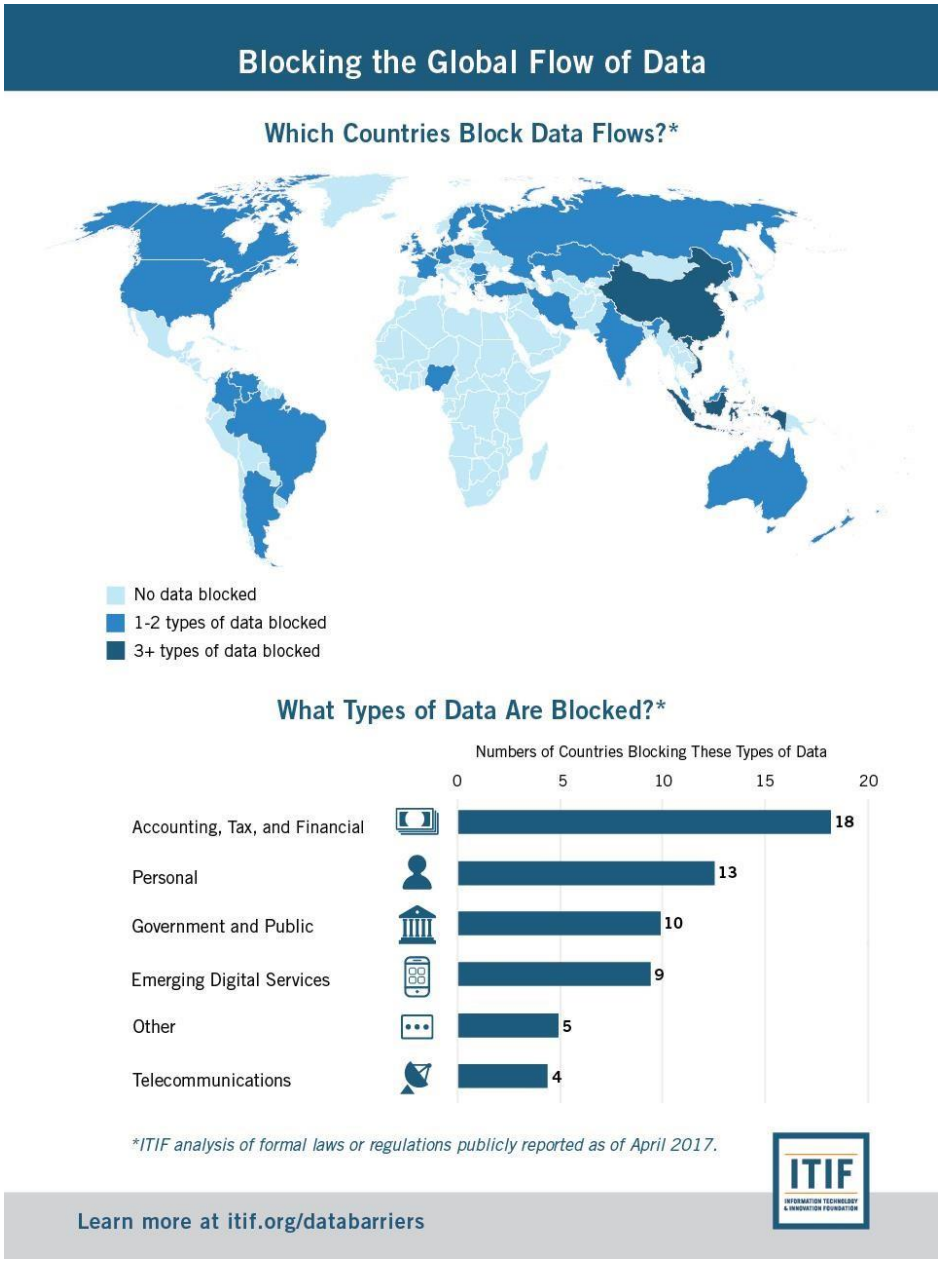
2018 年 2 月現時点で、GDPR は施行前であり、準拠ガイドラインもすべて発表されていない状況であり、各社は現時点で考えられる実務的な対応を行っているのが実際であろうが、GDPR への対応が不十分なままでは、巨額の制裁金というリスクを抱えたまま、GDPR の施行を迎えることになる。

また、今回は個人情報を中心に取りあげたが、金融・税金関連情報、通信情報、政府及び公共機関の情報等について、各国は自国内での保存を求める動きを取っている（図表 7）。米国も、金融・税金関連情報、政府及び公共機関の情報については、データの自国内の保存を求めている[89]。いずれにせよ、中国などの事例にも見られるように、個人データの域内管理は世界的なトレンドとなりつつある。こうした各国の法令へのコンプ

[84] https://ustr.gov/sites/default/files/files/reports/2017/NTE/2017%20NTE.pdf (p.80)
[85] https://www.bna.com/data-residency-laws-n57982086177/
[86] https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx
[87] https://www.usatoday.com/story/money/2017/08/12/more-u-s-companies-push-back-foreign-must-store-data-hererule/558702001/
[88] http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf
[89] https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

ライアンスを遵守していく上でも、まず GDPR への対応が重要になってくる。GDPR の施行が、情報の域内管理の世界的標準となっていく可能性もある。

図表 7：世界のデータ越境禁止の動向



出典：Information Technology& Innovation Foundation[90]

[90] https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

※ 本レポートは、注記した参考資料等を利用して作成しているものであり、本レポートの内容に関しては、その有用性、正確性、知的財産権の不侵害等の一切について、執筆者及び執筆者が所属する組織が如何なる保証をするものでもありません。また、本レポートの読者が、本レポート内の情報の利用によって損害を被った場合も、執筆者及び執筆者が所属する組織が如何なる責任を負うものでもありません。