［論文］

# GDPRに見る日本における個人情報取り扱いとその政策課題

小　林　　和　馬

## 1．イントロダクション

本稿は個人情報の取り扱いに関する国際標準として注目されている一般保護規則（GDPR）の制度とその動向についてサーベイを行い、日本における個人情報保護の現状やその政策の課題について考察を行った。

近年におけるDXや自動化の進展に伴い、行政や民間企業におけるインターネットを通じた取引や手続きへの需要が急速に高まり、住所や氏名といった個人情報のような重要な情報もインターネットで頻繁に取り扱われるようになった。しかし、インターネットでの取引や手続きは国を跨いだ国際間の情報処理となり可能性が高くなった。その際に俗にハッカーやクラッカーと呼ばれる悪意を持ったインターネット利用者に通信を傍受され、個人情報等の重要情報が流失し、経済的損失や場合によっては信用を喪失する事態となっている。

そうした事態に世界に先駆けて個人情報についてのルール化・法制化し、2018年5月28日、デジタル社会に則した強化の要請に即した形で施行したのが欧州（EU）31カ国による一般保護規則（GDPR）であり、これが世界のデータ管理やデータ利用の国際標準として、存在感を高めている。

## 2．GDPRに至るまでの歴史的経緯とその特徴

GDPRに至るまでの歴史は1978年の情報処理と自由に何する国家委員会（CNIL）による「データ保護法」に始まり、保護すべき情報を明確化し、データの利活用が示された。ここから1980年OECD理事会による「プライバシー保護と個人データの国際流通についての勧告」に基づきOECD8原則として「収集制限の原則」、「データ内容の原則」、「目的明確化の原則」、「利用制限の原則」、「安全保護の原則」、「公開の原則」、「個人参加の原則」、そして「責任の原則」の8項目が定められた。その後、1995年にはデータ保護指令によりEU加盟国にデータ保護の国内法を定めるよう要請していた。GDPRはこうした経緯を踏まえ発展させる形で、1995年のEU指令を廃止し、EU加盟国すべてに適用される法規としてより強力な体制を構築した。

## 3．GDPRの特徴と課題

GDPRにおいては、第5条1項にて6つの基本原則を定め、個人データの保護を前文において「基本的な権利の一つ」とした欧州連合基本憲章の派生法であるとした；①適法性、公正性及び透明性、②目的の限定、③データの最小化、④正確性、⑤記録保存の制限、さらに⑥完全性及び機密性の6つとなっている。

これら基本原則に基づき、データ主体の自由及び権利を保護する目的の下で、

・データ主体の権利
・管理者の義務
・制裁

これらの仕組みを規定として設け、制裁も規定することとなったことが実効性を踏まえても注目すべき点となっている。こうした仕組みと特徴により、問題となるのは本稿では3点挙げ、その問題点を指摘したい。

第一に基本原則③とした「データの最小化」の問題である。この問題は、個人データが十分かつ関連性があり、必要なものに限定されなければならないとされている原則である。この問題はデータの「域外移転」を伴うGDPRの域外適用に付いての問題に発展し、GDPR第44条では「現に取扱われている又は第三国又は国際機関への移転の後に取扱いを意図した個人データ移転は、その第三国又は国際機関から別の第三国又は国際機関への個人データの転送に関するものを含め、本規則の他の条項に従い、本章に定める要件が管理者及び処理者によって遵守される場合においてのみ、行われる。本章の全ての条項は、本規則によって保証される自然人保護のレベルが低下しないことを確保するために適用される」と一般原則が示されている。各国の国内法の規定との整合性に違いが生じることが本稿で後述の日本の例でも明らかであり、ターゲティング広告のような行動追跡を伴う複数の国をまたいでのデータの取り扱いは問題となる可能性がある。

GDPRでは第3条2項において、「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」とされ、指摘したターゲティングによる行動追跡については、「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

動の監視は行われる」と規定されているが、「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」とも規定され、国際的な罪やサービスの提供に際してはGDPR に則した対応をその対象地域で一貫して行う必要がある。

データの最小化の観点から考えると、現在 AI などとも活用しながら発展が期待されているターゲティング広告などの行動追跡型の情報の取得と収集はこの基本原則との間で本質的に二律背反あるいは矛盾を起こす可能性があると考えている。

第二に EU による規定と罰則と「十分性認定」による各国国内法との間で差異が生じ、ニュアンスの問題も含めて存在や認識のズレを生んでいる問題がある。

2022年１月現在、十分性認定を受けた第三国はアルゼンチン共和国、アンドラ公国、イスラエル国、ウルグアイ東方共和国、英国、英国王室属領ガーンジー、英国王室属領ジャージー、英国王室属領マン島、カナダ、韓国、スイス連邦、デンマーク王国自治領フェロー諸島、日本国、ニュージーランドの14カ国となっている。

十分性認定については、EU 域外への移転について、GDPR45条では「第三国又は一領土又は第三国内の複数の特定セクター又は国際機関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、第三国又は国際機関への個人データの移転を行うことができる。その移転は、いかなる個別の許可も要しない。（個人情報保護委員会仮訳を著者修正）」としており、この決定を十分性認定としている。この十分性認定について、日本は GDPR 第45条に基づく十分性認定の発行を2019年１月23日に行っている。

十分性認定の問題は、一度認定を受けてしまうと、データの域外移転に関する手続きや許可が必要なくなる点にある。これにより、データ保護について SCC（標準契約条項）、現在では SDPC（標準データ保護条項）という域外移転の合意書、あるいは GDPR 第47条１項と２項において定められている企業グループに従事する者が遵守すべき個人データ保護の方針（BCR）も必要なくなる。

この十分性認定の問題が GDPR における最も大きな問題であり、この存在には31カ国もの大規模な EU という地域で規定された内容とはいえ、EU 内の国内法でも違世界規模での取り組みとしてはあくまで関係する各国への対応となる上、どのような指針でデータを保護・管理するのかが明示されることはない。各国国内法が保護に対して一定の水準を満たしているとはいえ、差異が特に制裁をする際に混乱や訴訟の温床になりかねない。

さらなる問題点として、十分性認定国におけるデータ主体から得るはずの同意が、日本を含めた先進国や EU 関係国の十分性認定により、同意を得ずにデータ移転可能となる実質的な「抜け道」となる可能性がある。これは実務的な混乱を避ける目的ではないかと考えられるが、形骸化の恐れもある。実際、インターネットを通じて EU 域内のデータ主体に対して材やサービスの提供といったビジネスを行うこともある。すると、SCC や BCR がないため GDPR に基づいたデータ主体の同意がなく、想定したデータ主体が主体的にデータをコントロールするといった思想や GDPR が第１条１項や前文42項にある同意を証明できるようにしなければならない規定がありますが、長文にわたる難解な法律用語を並べた同意文章に同意するよう求められても、実際それが同意内容を理解し同意したことになるのかについては疑問が残り、実務上の問題ともいえる。このようにして仕組みや規定が実質機能しなくなる可能性も考えられる。

加えて、日本の法制度や企業においての対応を考える場合、前述の GDPR に至る歴史的議論の経緯を踏まえ、GDPR 前文１項にあるような基本的人権であることの前提を踏まえる必要があることは次の日本における個人情報保護法との差異の議論から明らかとなる。

## ４．日本の個人情報保護法との相違点

EU の GDPR と日本の個人情報保護法との違いは、やはり多岐にわたり違いが見られる。

第一の違いは GDPR における「個人データ」と個人情報保護法の「個人情報」の違いにある。概ね個人の識別についての認識やそのための手段などには違いがない。

しかし、大きく違いが現れるのがオンライン識別子についてである。オンライン識別子は位置情報や IP アドレスやクッキーといったインターネット利用に際して個人を識別することができる可能性があるデータを個人データとして扱っている一方、個人情報保護法ではオンラ

イン識別子は個人情報に当たらないと考えられている。

GDPRでは個人を識別できる可能性があれば対象となるので、クッキーや電力使用量など、一見個人を識別するのは困難と思われる情報などであっても、現在では前述のターゲット広告などで個人の行動を追跡することで間接的に個人の識別に資する可能性があることを想定している。現在ではスマートフォン上のアプリで、開発やサポートを目的としているものもあるが、マーケティングなどにも活用可能な操作履歴や課金状況などを含む利用履歴を入手している。

したがって、現在の日本の状況はGDPRに対し十分性認定を受けているものの、十分対応したものであるのか疑問が残り、GDPRと同等の認識・対応とするべきであると考える。

第二に、本人の同意であるデータ主体の同意について違いが見受けられる。GDPRでは同意の要件については任意性、特定性、説明をうけた（informed）、明確性の４つの点から同意が形成されることが示されているが、日本の個人情報保護法にはそうした同意の要件はない。さらに、手続きとして立証を求めるGDPRに対して個人情報保護法では「適切な方法」としか規定されていない。これでは日本の規定が手続きを通じて何を求めているのかが明確ではない。「保護できればどのような手続きでもよい」というのは一見柔軟な対応や規定のようにも見えるが、手続きを通じてどのような目的を果たすのかが示されていないのは問題であると考える。

同意についての重大な問題はGDPRには存在する「同意を撤回する権利」が存在しない点にある。一度同意はしたが状況や管理者の変更によって個人情報の管理の継続を望まない場合は、インターネットを使い変化の早いデジタル社会を考えれば、容易に想像できる。にもかかわらず、日本の個人情報保護法はこの「同意を撤回する権利」を認めていない。つまり、一度同意してしまったら、二度と個人情報の提供や管理への同意を、不正による取り消しがない限り、撤回することができないことになる。こうした仕組みにしておくのは、やはりGDPRのような基本的人権を通じてデータ保護があるといった、法律の前提が日本の個人情報保護法にはないことが原因であると考える。この点もまた十分性認定の観点からもGDPRを踏まえた同意についての認識や仕組みにするべきであると考える。

このことが、次に挙げる「適法な取り扱い」の認識の違いにもつながっていく。GDPRと個人情報保護法は共通して適法性を求めているものの、その対象は異なっている。

GDPRは個人データの取り扱い全般に対しての適法性を求めている。それに対して、日本の個人情報保護法上の適法な取り扱いは第17条において個人情報の取得についてのみにしかその適法性を問うていない。前述の同意についての認識や仕組みの違いが適法性の違いに派生していると考えられる。この点はデータ保護が基本的人権を基礎にしているという根幹に関わる問題のため、問題は重大で制度論として議論ももちろん必要ではあるが、どのような社会にするのか政策的議論を深める必要があると考える。

## 5．国際的な個人情報保護と日本の対応における課題

匿名データを利活用する基盤の構築が個々の企業で求められており、対応に苦慮する一方、日本における個人情報保護法では一度同意を取り付ければ、データ主体からの撤回の申し出ができないため、実質データのコントロールはデータ主体による監視や管理が機能せず、管理者が行うことになる。

この点を考慮すると、個人情報流出に際しての損害をどのように評価し、補償するのか問題となる。損害の評価や補償には基準がなく、任意で数百円程度の謝罪金で済ますケースがそれ以前から多発しており、まったく損害と補償のバランスが取れておらず[1]モラルハザードの温床となる可能性があり、日本企業が国際的な非難を呼ぶ可能性がある。

1）本稿記載指摘のような事例は2014年に起こったベネッセコーポレーションの顧客情報流出事件において、金額500円の“おわび”の例がある。直近の個人情報の大規模漏洩については、2022年６月29日にCD・レコードの販売などを手がけるディスクユニオンが運営するオンラインショップ「diskunion.net」ならびに「audiounion.jp」において、大規模な顧客データの漏えいがあった。漏洩した個人情報は氏名、住所、電話・FAX番号、メールアドレス、ログインパスワード、さらに会員番号で最大70万1000件が流出した可能性があるとした。（NHK　2022年６月29日　https://www3.nhk.or.jp/news/html/20220629/k10013694311000.html）

## 6．結論

本稿では個人データの保護を目的としたGDPRについて成立の経緯と特徴、さらに問題点を指摘した。さらに、日本において個人情報を保護する目的の個人情報保護法について、GDPRとの十分性認定を得ているとするものの、法律としてその成立過程や成り立ちが異なるため、大きな相違点があり、本稿において指摘した。問題点が基本的人権に関わるものもあり、本質的議論が必要になることから、法律論や制度論として議論するのではなく、政策論としてインターネットを通じたデジタル社会がメタバースとしてその世界を拡張しようとする現代にあってどのような社会を構築するべきか、議論の必要性があることを本稿議論により強く再認識した。

**〈参考文献〉**


EU (2016) “DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL”, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN.

EU (2016) “REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL”, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

EU (2018) “REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL”, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552577087456&uri=CELEX:32018R1725.

打川和男（2021）『個人情報保護法の基本と実務対策がよ～くわかる本』

小向太郎、石井夏生利（2020）『概説GDPR　世界を揺るがす個人情報保護制度』、NTT出版。

福本洋一（2021）『「個人データ」ビジネス利用の極意』、商事法務。

牧野総合法律事務所弁護士法人･合同会社LEGAL EDGE（2019）『最新GDPRの仕組みと対策がよ～くわかる本』、秀和システム。

渡邉雅之（2019）『GDPR　EU一般データ保護規則　法的リスク対策と個人情報・匿名加工情報取扱規程』、日本法令。

個人情報保護委員会（2017）『データポータビリティの権利に関するガイドライン』、https://www.ppc.go.jp/files/pdf/dataportability_guideline.pdf。

個人情報保護委員会（2021）『管理者及び処理者の概念に関するガイドライン』、https://www.ppc.go.jp/files/pdf/kanrisha_syorisha_gainen_guideline_v2.0.pdf。

個人情報保護委員会（2016）『データ保護オフィサー（DPO）に関するガイドライン』、https://www.ppc.go.jp/files/pdf/dpo_guideline.pdf。

個人情報保護委員会（2016）『管理者又は処理者の主監督機関を特定するためのガイドライン』、https://www.ppc.go.jp/files/pdf/kanrisya_guideline.pdf。

個人情報保護委員会（2017）『データ保護影響評価（DPIA）及び取扱いが2016/679規則の適用上、「高いリスクをもたらすことが予想される」か否かの判断に関するガイドライン』、https://www.ppc.go.jp/files/pdf/dpia_guideline.pdf。

個人情報保護委員会（2017）『規則における制裁金の適用及び設定に関するガイドライン』、https://www.ppc.go.jp/files/pdf/seisaikin_guideline.pdf。

個人情報保護委員会（2017）『自動化された個人に対する意思決定とプロファイリングに関するガイドライン』、https://www.ppc.go.jp/files/pdf/profiling_guideline.pdf。

個人情報保護委員会（2017）『透明性に関するガイドライン』、https://www.ppc.go.jp/files/pdf/toumeisei_guideline.pdf。

個人情報保護委員会（2018）『規則に基づく個人データ侵害通知に関するガイドライン』、https://www.ppc.go.jp/files/pdf/tsuuchi_guideline.pdf。

個人情報保護委員会（2018）『規則第49条の例外に関するガイドライン』、https://www.ppc.go.jp/files/pdf/article49reigai_guideline.pdf。

個人情報保護委員会（2020）『同意に関するガイドライン』、https://www.ppc.go.jp/files/pdf/doui_guideline_v1.1_koushin.pdf。

個人情報保護委員会（2020）『GDPRの地理的適用範囲（第3条）に関するガイドライン』、https://www.ppc.go.jp/files/pdf/chiritekitekiyouhanni_guideline2.1.pdf。

個人情報保護委員会（2020）『新型コロナウイルス感染症

の発生下における科学的研究を目的とした健康に係るデータの取扱いに関するガイドライン03/2020』、https://www.ppc.go.jp/files/pdf/covid19kenkoudata_guideline_v 1 _1.pdf。
個人情報保護委員会（2020）『ビデオ装置を介した個人データの取扱いに関するガイドライン』、https://www.ppc.go.jp/files/pdf/video_souchi_guideline_v2.0.pdf。
個人情報保護委員会(2020)『一般データ保護規則(GDPR)の前文』、https://www.ppc.go.jp/files/pdf/gdpr-preface-ja.pdf。
個人情報保護委員会(2020)『一般データ保護規則(GDPR)の条文』、https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf。