Vol.2019-EIP-83 No.12
2019/2/15

個人データ取扱いの適法化根拠に関する制度比較

小向太郎[†1]

EU 一般データ保護規則（GDPR）第 6 条は，個人データの取扱いが適法となるための要件を示している．この条項は，95 年個人保護指令の第 7 条を引き継いだものであり，EU の個人情報保護制度の根幹ともいえる．これに対して，わが国の個人情報保護制度では，本人の意思を反映しうる場面が，主として第三者提供と利用目的変更の場合等に限定されている．本報告では，GDPR における適法化根拠を日本の制度と比較し，今後の課題について検討する．

The Comparative Study on Data Protection for Location Data

TARO KOMUKAI[†1]

The Article 6 of the EU General Data Protection Rule (GDPR) provides the requirements for the lawful processing of personal data. This clause has inherited Article 7 of the Data Protection Directive of 1995 and can be said to be one of the most important provision in the EU's data protection. On the other hand, in Japan's personal information protection system, the will of data subjects are respected mainly in the case of third party provision and change of purpose of use. This paper focuses on the difference in requirement for lawful processing of personal data between the EU and Japan.

1. わが国における適法化根拠

1.1 個人情報保護制度の枠組み

個人情報保護制度は，一般にプライバシー保護に資するために整備されるものと考えられているが，具体的にどのような権利を保護するものであるかは，国や地域によって位置づけが異なる．わが国の憲法において，プライバシーが基本的人権のひとつとして保障されるということにはあまり争いがない．しかし，その具体的内容については見解が一致しておらず，例えば，どのような個人情報保護がそこから求められるのかは，明らかではない[1].

これに対して，EU では，個人データの保護が基本的人権であると位置づけられている．欧州連合基本権憲章[2]では，第 7 条の「私生活および家庭生活の尊重を受ける権利」に加えて，第 8 条「個人データの保護」がうたわれている．そして，「関係者の承諾か、その他の法定の適法な根拠に基づいて、限定された目的のために、公正に取扱われなければならない。何人も、自分に関して収集された情報に対してアクセスする権利および情報を訂正する権利を有する（第 2 項）」，「独立の機関による監督を受けなければならない（第 3 項）」と具体化されており，こうした保護を受ける権利が基本的人権であることが明確化されている．なお，米国では，個人情報の保護が基本的人権であるという考えは少なくとも主流ではなく，個人情報保護制度は，政策的に国民の保護を図るためのものと理解されていると考えてよいであろう．

しかし，いずれの立場であっても，情報化の進展によって，個人情報が思わぬ使われ方をされてしまう懸念に対応が必要であるという認識は，共有されている．個人情報保護制度は，こうした懸念に対処するために，個人に関する情報の扱いに対してルールを定め，本人の意思に反する利用を抑制し，弊害や危険の大きな行為類型を制限するために整備されてきたものである．

そして，個人情報が取扱われる過程は，「情報の取得→情報の保有→情報の発信」のように整理することができる．従来，情報の取得や利用を法律によって制限することは比較的少なかったが，コンピュータ技術とインターネットの普及によって，情報の保有や取得についてもルールを設ける傾向が強まっており，個人情報保護に関しては，一般に取得，保有，提供の全般についてルールが定められている[1].

そこで，取得，保有，提供のそれぞれについて，個人情報保護制度がどのような場合に適法な取扱いと認めるのかが問題となる．例えば，EU 一般データ保護規則（GDPR）[4]は，第 6 条が個

人データの取扱いが適法となるための要件を示しており，これらは，取得，保有，提供のすべての段階について，個人データの管理者等に要求される．これに対して，わが国の個人情報保護制度では，個人情報の取扱全般と，第三者提供および利用目的変更の場合で，個人情報取扱事業者に要求される適法化根拠が大きく異なる．

本報告では，個人データ取扱いの適法化根拠について，EU と日本の制度を比較し，その違いから示唆される課題について考察する．

1.2 IoT，ビッグデータの影響

コンピュータ処理能力の向上と，データ収集可能な情報の増大を背景に，大量のデータが分析・利用されるようになっている．その一方で，こうした技術においては，利用者等があまり意識することなく情報を収集されていることも多い．個人情報が自動的に収集されることに起因する懸念としては，次のような問題が指摘されている．

① 自分の情報がどのように使われるのか把握できない
② 情報利用を拒否することが難しい場面がある
③ 人に知られたくない情報が思いがけず使われてしまう

つまり，個人情報保護制度が目的としている，本人の意思に反する利用の抑制や弊害や危険の大きな利用類型の制限を，制度的に担保することが難しくなっているということである[3].

1.3 個人情報保護法における適法化要件

わが国の個人情報保護法において，個人情報取扱事業者が個人情報を取扱うにあたっては，利用できる目的をできる限り特定し（第 15 条），公表等することと（第 18 条）その目的の範囲で利用すること（第 16 条）が求められる．そして，個人情報を収集した事業者が，その事業者内で利用する場合には，特に本人の同意等は求められていない．

これは，「個人情報の有用性を過度に減殺しないために，利用方法，利用目的自体を規制するのではなく，利用目的の通知または公表を契機とする本人等からの苦情等を通じて，個人情報の適正な利用を確保することを基本方針」としたためであるとされる[5]．不適正な取得や（第 17 条第 1 項），他の法令に抵触する利用は許されないが，利用目的の範囲についての制約は少なく，情報の収集と収集した事業者の内部利用に関して自由度が高い制度である．

しかし，事後的に当初の目的と「相当の関連性を有すると合理的に認められる範囲を超えて（第 15 条第 2 項）」利用目的を変更するのであれば本人の同意が必要となる（第 16 条第 2 項）．また，個人データの第三者提供にも，原則として本人の事前同意が必要である．ただし，法令に基づく場合や緊急性等がある場合（第 23 条第 1 項），オプトアウト（第 23 条第 2 項），委託先への提供（第 23 条第 4 項第 1 号），事業承継（第 23 条第 4 項第 2 号），共同利用（第 23 条第 4 項第 3 号）には，本人の同意がなくとも，第三者提供が例外として許容される．

2. GDPR における適法化要件

2.1 適法化根拠

GDPR において個人データの取扱いが適法とされるのは，次のいずれかを満たす場合に限られる．

(a) データ主体が、一つ又は複数の特定の目的のための自己の個人データの取扱いに関し、同意を与えた場合。
(b) データ主体が契約当事者となっている契約の履行のために取扱いが必要となる場合、又は、契約締結の前に、データ主体の要求に際して手段を講ずるために取扱いが必要となる場合。
(c) 管理者が服する法的義務を遵守するために取扱いが必要となる場合。
(d) データ主体又は他の自然人の生命に関する利益を保護するために取扱いが必要となる場合。
(e) 公共の利益において、又は、管理者に与えられた公的な権限の行使において行われる職務の遂行のために取扱いが必要となる場合。
(f) 管理者によって、又は、第三者によって求められる正当な利益の目的のために取扱いが必要となる場合。ただし、その利益よりも、個人データの保護を求めるデータ主体の利益並びに基本的な権利及び自由のほうが優先する場合、特に、そのデータ主体が子どもである場合を除く。[6]

適法化根拠は，個人データの取扱いに先立ち，情報とその利用目的ごとに決定しておく必要がある．そして，適法化根拠にどれを選ぶかによっ

†1 日本大学
Nihon University

て，データ主体がどのようなコントロールを行使できるかが変わってくる．

まず，どのような根拠で適法化した場合であっても，「アクセスの権利」，「訂正および消去の権利」，「取扱いの制限の権利」などの権利が，データ主体に認められる．そして例えば，データ主体の同意を根拠とした場合（第(a)項）は，データ主体はいつでも何の負担もなく同意を撤回することができる．また，公共の利益・公的権限の遂行（第(e)項）や正当な利益（第(f)項）が根拠となっている場合には，異議申し立てをすることができる．

2.2 同意の条件

GDPR は，「同意の条件」を厳格に定めている（第 7 条）．個人データが同意を根拠として扱われる場合には，管理者が証明責任を負うこと（第 1 項），書面で示される利用規約によって同意内容が示される場合には他の事項と区別しデータ主体が理解しやすい態様で同意を要請すること（第 2 項），データ主体が同意をいつでも撤回できること（第 3 項），同意の任意性を判断する際に契約履行に同意を条件づけているか否かを十分考慮すること（第 4 項）が求められる．さらに，管理者は本人に対して，情報収集の事実や本人が管理者にアクセスするために必要な情報等を，知らせることが義務付けられている（第 13 条）．

特に，有効な同意であると認められるためには，①自由な同意，②特定された同意，③事前説明を受けた同意，④不明瞭ではない表示による同意，⑤明らかに肯定的な行為による同意，でなければならない（前文第(32)項）．

2.3 正当な利益

適法化根拠のなかで，いわば一般規定にあたるものが「正当な利益の目的のために取扱いが必要となる場合（第(f)項）」である．他の要件に当たらないが処理の必要性が高い場合に認められる．

この規定は，規定自体が曖昧であるとともに，解釈上の裁量（いわゆるバランシングテスト）を条文に含んでいる．つまり，管理者または第三者の正当な利益と，データ主体の保護の必要性を比べて，前者が後者を上回るときにだけ，正当化事由として認められる．これを適法化根拠とする場合には，管理者は，取扱に先立って「正当な利益」が何かという情報を本人に知らせることが求められ（第 13 条第 1 項(d)号，第 14 条第 2 項(b)号），「正当な利益」があることについて立証責任を負う．曖昧さを含んでいるからといって，「正当な利益」を安易に根拠にすることはできない．

基本的に，データ主体と管理者との間に妥当で適切な関係がある場合に認められる．例えば，「管理者からサービスの提供を受けている場合」のような状況が想定されている．（前文第(48)項）．

データ主体がその取扱いを合理的に予測できない場合には，データ主体の利益及び基本的権利が優越するため，「正当な利益」は認められない．また，公的機関の職務遂行に「正当な利益」は適用されない．公的機関に対しては立法機関が法的根拠を与えるのであって，勝手に「正当な利益」を主張することは許されない．不正行為の防止の目的のために厳密に必要性のある個人データの取扱いやダイレクトマーケティングのための個人データの取扱いも，「正当な利益」のために行われるものとみなされうるとされているが（前文第(47)項），データ主体が合理的に期待する範囲に限られるものと考えられる．

3. 適法化根拠の課題

3.1 適法化根拠の比較

GDPR においては，およそ個人データの取扱を行うのであれば，個人データの取得，保有，提供のすべての段階で，適法化根拠（データ主体の同意その他の正当化事由）が要求される．その意味では厳格であるが，「正当な利益」という一般規定が置かれているため，個人データ取扱いの必要性に応じて，個別かつ柔軟に判断される余地を残している．

これに対して，わが国の個人情報保護制度では，個人情報の取扱いに際して，利用目的の特定・公表とその範囲での利用を行っていれば，本人の同意その他の正当化事由は求められていない．本人同意等の厳格な適法化根拠が求められるのは，第三者提供と利用目的変更の場合だけに限定されており，本人が知らないあいだに情報が収集されても，法律上は問題とされない可能性が高い．しかし，本人の同意なく第三者提供が許されるための要件は，GDPR と比べて厳格であるとも評価できる．

3.2 適法化根拠と監督機関

前述の通り，わが国の個人情報保護制度において，個人データの内部利用に本人の同意その他の正当化事由が求められていないのは，個人情報の利用を過度に制限しないようにするためであったとされる．もし，内部利用も含めて個人情報の取扱い全般に，原則として本人の同意を求めることに

なると，個人情報利用のハードルが上がりすぎるということであろう．

EU の制度において，このような弊害を避けるために設けられているのが，「正当な利益」という適法化根拠である．この適法化根拠は，他の適法化根拠が妥当しないが正当な利用と認められる場合に，個人データの取扱いを適法と認めるための，落ち穂拾い的な規定である．そしてこの規定は，規制機関のある程度の裁量を前提としている．EU 諸国においてこれが機能しているのは，独立専門の監督機関がこうした判断を行っていたことによる．

我が国で，2015 年の個人情報保護法改正以前に取られていた主務大臣制のもとでは，解釈上の裁量の大きい行政規制を導入するのが難しい面がある．このような体制のもとでは裁量に関する統一的な判断を維持することが難しく，法の安定性を損なう危険があるからである．しかし，すでにわが国にも独立の監督機関として個人情報保護委員会が設置されており，専門性の高い監督機関としてこうした判断を行うことが期待できるようになっている[1]．

3.3 情報セキュリティのための情報共有

情報セキュリティ対策の必要性が高まるにつれて，対応組織間での連携や情報共有がより重要になっている．インシデント対応に関して取得した情報は，直接のインシデント対応が終了したあとも有効に活用できるものがある．どのような情報が漏洩した可能性が高いのか，攻撃者としてどのような者が想定されるかといった情報を，情報セキュリティ対策や犯罪被害防止に役立てることも重要である．そして，こうした情報にも，個人データが含まれる可能性がある．

そこで，このような情報の共有が，個人情報保護制度上許容されるのかどうかが問題となる．わが国の個人情報保護法では，個人データの第三者提供には本人の同意が必要である．そして，インシデント対応は，本人の同意がなくても第三者提供が許されるその他の例外事由（例えば，「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とき（第 23 条第 1 項第 2 号」）には，該当しないことも多いと考えられる．

一方，EU の GDPR では，適正なインシデント対応のための情報共有は，情報セキュリティを確保する目的で必要かつ相当な範囲で行われる場合には，正当な利益とみなされる．例えば，コンピュータ緊急対応チーム（CERT），コンピュータセキュリティインシデント対応チーム（CSIRT），電気通信事業者，セキュリティ提供事業者等は，サイバー脅威に対応するために，正当な利益を根拠に個人データを利用することができるとされている．具体的な利用目的としては，電子通信ネットワークへの無権限アクセスやマルウェア配布の防止、DoS 攻撃やコンピュータ・電子通信システムの破壊行為の阻止などが想定されている（前文第(49)項）．もちろん，個人情報の取扱を始める際に，このような利用を行うことを本人に伝えることが必要であり，本人から異議申し立てがなされる可能性はある．しかし，このような個人データの利用が明確に適法であることが示されていることの意味は大きい．

今後，このような情報セキュリティのための情報共有はより重要になると考えられる．また，情報利用の多様化にともない，個別の事情を考慮しつつ利用の可否を決めることが望ましい場面は増加するものと考えられる．わが国の個人情報制度においても，第三者提供と利用目的変更の場合だけに厳格な適法化根拠を求める制度設計を今後も維持すべきかどうかについて，個人情報保護制度の本来の目的を踏まえて検討すべきであろう．

謝辞

本研究は，電気通信普及財団の研究助成による研究費を得て実施した．

参考文献

[1] 小向太郎，『情報法入門（第 4 版）デジタル・ネットワークの法律』NTT 出版(2018) 1893-218 頁.
[2] CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (2000/C 364/01), the European Union Charter of Fundamental Rights, as signed and proclaimed by the Presidents of the European Parliament, the Council and the Commission at the European Council meeting in Nice on 7 December 2000.
[3] 小向太郎「データ集積の急増と個人情報の利用目的規制」電気学会論文誌 C 電子・情報・システム部門誌第 137 巻 6 号（2017 年 6 月）790-795 頁.
[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[5] 宇賀克也『個人情報保護法の逐条解説』（有斐閣，第 5 版，2016）138 頁）.
[6] 個人情報保護委員会「一般データ保護規則　仮日本語訳」https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/.