N-023

デジタル時代におけるプライバシーに係るルール整備の提案
Proposal for establishing rules related to privacy in the digital age

上條 英夫†
Hideo Kamijo

1. はじめに

デジタル技術を活用した新たな利用分野では、ビジネスモデルの変革や技術革新等が著しいことから、民間主導で自主ルールが策定、運用されることが望ましいとされる。しかしながら、現行の法規制の枠内で民間の自主的な取り組みに任せるだけでは、利用者のプライバシー確保は難しい。たとえば、第三者サイト経由で個人に関連するデータが収集されても、利用者は第三者サイトのアクセス時にはそのことを認識できない点や、プロファイリング実施についてプライバシーポリシーに記載されていても、プロファイリング自体を拒否したり、異議を唱えたりする方法は分からない点など、利用者が自分に関連するデータの扱いを理解し、コントロールすることが難しい現状がある。また、個人に関連する情報の取扱いは情報の非対称性が大きく、特にプロファイリングのように、個人の内面操作に利用されうるといった、現代社会が重視する基本的な価値に与える影響の大きさや、個人に関連する情報の取得・利用の状況を外部から把握することの困難さ等を考えると、一層のルール整備が必要と考えられることを拙稿（参考文献[1]）にて考察した。本稿では一層のルール整備の方向性として「ガバナンスとマルチステークホルダーによる実施基準に基づく規制」を提案する。

2. ルール整備の方向性の考察

ルール整備の方向性について、ルールの形成・執行の観点により類型化したルールの特徴、およびプライバシーないし個人データ保護分野の先駆的規制とされる欧州一般データ保護規則（GDPR）における規制のあり方を参考に考察を行う。

2.1 ルールの類型化とその特徴

ルールには形成と執行という異なった局面があり、下表のとおりルールの形成と執行を国が担うケースと国以外が担うケースによって 4 つのカテゴリーに分類できる。それぞれの特徴をデジタル時代のプライバシーのルール整備、特にルールの実効性確保の観点から検討する。

ルール形成／執行	国家が執行しない	国家が執行する
国家以外が形成する	カテゴリー1 社会規範、業界団体による自主規制等	カテゴリー3 会計基準、商慣習法等
国家が形成する	カテゴリー2 労働法上の努力義務規定等	カテゴリー4 ハードロー

表　ルール形成・執行の類型
（参考文献[2] 5 頁を元に筆者加工）

●カテゴリー１
国家がルールの形成、執行に関与しないものであり、人々に自発的に守られている社会規範や業界団体等による自主規制などが該当する。本稿に関係する業界団体等による自主規制については、規制が及ぶ範囲が特定の自主規制グループに限られ、自主規制グループに参加する企業等の数が増え、参入・退出の頻度が多くなるほど、また、参加企業等の均質性が乏しいほど、規制の実効性確保が難しくなるとされる。また、複雑な商品・サービス内容で高度な内部情報が規制遵守の確認のために必要となるような、情報の非対称性が大きいケースも規制グループ内の監視コストが多大になり規制を維持しにくいといった特徴がある。デジタル関連のプライバシー分野は、こうした特徴がすべて当てはまり、自主規制には向かないと考えられる。

●カテゴリー２
国家がルールを形成するが、ルールの執行は行わないものであり、労働法上の努力義務規定等が該当する。当カテゴリーは努力義務であり、実効性のあるルール整備を検討する本稿のスコープ対象外である。

●カテゴリー３
ルール形成は国家以外が行うが、ルールの執行は国家が行うもので、法が国家以外による規範作成を前提とするものである。従うべき基準を法律で示した上で、基準の具体的な内容そのものは社会的に適切な水準を関係者（マルチステークホルダー）で定め、違反時には国家による法の執行が予定されているという方法である。たとえば会計基準では、会社法、金融商品取引法、法人税法いずれも「一般に公正妥当と認められる基準（慣行）」に従うとされているが、この基準（慣行）自体は法令で定められていない。この基準は民間団体内の「企業会計基準委員会」により設定され、金融庁長官が個別に承認することとなっている。このような方法は、従うべき適切な基準を法令で定めることが容易ではないデジタル関連のプライバシー分野のルール形成においても有効な手法であると考えられる。

●カテゴリー４
国家が法令としてルールの形成および執行を行うものである。行政機関や民間団体等によるガイドラインや基準等により、法令が補完されるケースも含まれる。一般的にはルールの実効性確保の観点では最も有効であると考えられる。特に、企業と法執行者の間の情報の非対称性が大きい場合、法による懲罰的なペナルティの用意はルールの実効性確保に向けた企業に対するインセンティブとして有効とされる。一方、デジタル関連におけるプライバシーのような技術進歩が著しい分野で、法で明確なルールを定めることは課題となる。

† 情報セキュリティ大学院大学　Institute of Information Security

2.2 GDPR における規制のあり方

GDPR は上記カテゴリー４に属する。ここでは情報の非対称性、および明確なルール化が難しい点を GDPR がどのように克服しようとしているかを考察する。

2.2.1 情報の非対称性への対応

GDPR は情報の非対称性を克服するため、以下のような制度上の仕組みを用意していると考えられる。

法令違反に対する懲罰的なペナルティとして、最大で、2,000 万ユーロまたは前会計年度の世界全体における売上総額の 4%までのいずれか高い方という高額な制裁金を科している（第 83 条）。これは情報の非対称性がある中で、抑止力として機能すると考えられる。

また、独立の監督機関の設置を加盟国に義務付けている（第 51 条）。監督機関は完全な独立性が求められ（第 52 条）、情報提供命令、データ保護監査方式による調査実施、職務上で必要な全個人データ・情報へのアクセスなど広範な調査権限が付与されている（第 58 条）。また、事前協議手続に基づく管理者への助言、越境データ移転に関する承認などの承認・助言の権限なども付与されている。監督機関がこれらの権限を行使することにより情報の非対称性が緩和されると考えられる。

GDPR は法令違反の際のデータ主体に対する救済措置として、データ主体が自己に関する個人データの取扱いが GDPR 違反と判断する場合、監督機関に異議を申し立てる権利（第 77 条）、自己の権利が侵害されたと判断する場合、管理者又は処理者を相手方とする効果的な司法救済を得る権利（第 79 条）、違反行為の結果として財産的な損害又は非財産的な損害を被った場合、管理者又は処理者からその被った損害の賠償を受ける権利（第 82 条）など、様々な権利をデータ主体に認めている。これらは直接的にはデータ主体の権利保護規定であるが、ルール執行における情報の非対称性を緩和する一定の効果も期待できるであろう。

2.2.2 明確なルール化が難しいことへの対応

GDPR では、ルール明確化のため、法令解釈・運用に関する指針として、EU の公的機関（欧州データ保護会議）が採択・承認した「同意に関するガイドライン」「自動処理による個人に関する決定およびプロファイリングに関するガイドライン」など各種ガイドラインが示されている。しかしながら、ガイドラインは条文の解釈・説明において、たとえば「やむをえない正当な根拠と考えられる事項のいかなる説明も提供しない」「何が基準になるかを正確に決めるのは難しい」と記載するなど、基準が明示されず判然としない部分が存在する。こうした明確なルール化の難しさを克服するため、GDPR は、GDPR の遵守を保証しそのことを説明できるようにするための技術的および組織的な措置を管理者に求めていると考えられる。すなわち GDPR は、管理者に処理の性質、範囲、状況、目的、自然人の権利及び自由に対する様々な蓋然性と深刻度のリスクを考慮に入れた上での GDPR の遵守とその説明責任を負わせ（第 24 条）、そのための技術的・組織的な措置として、データ保護バイデザインおよびデータ保護バイデフォルトによる対応の実装（第 25 条）、データ保護影響評価の実施（第 35 条）、データ保護責任者の設置（第 37 条～第 39 条）などのガバナンス体制構築を求めていると考えられる。また、このようなガバナンス体制が構築され機能していた場合には、法令違反時の制裁金が考慮されることを規定している。

3. ルール整備の方向性　－ガバナンスとマルチステークホルダーによる実施基準に基づく規制－

デジタル時代におけるプライバシーに係るルール整備に当たっては、明確なルール化が難しく、情報の非対称性が大きい中でルールに実効性を持たせるための工夫が必要である。これについては、GDPR における規制の働かせ方、特に、高額な制裁金と、法が要求する技術的・組織的措置を構築・機能化していた場合には制裁金の減免を規定化することにより、技術的・組織的措置の実効性ある実施を促す GDPR のガバナンスベースの手法はルール整備の方向性として参考になる。また、技術的・組織的措置の適切な水準については、「2.1 ルールの類型化とその特徴」のカテゴリー３の方式、すなわち「法が国家以外による規範作成を前提」に、マルチステークホルダーにより具体的基準等を定める考え方が有効と考えられる。

デジタル時代におけるプライバシーに係るルール整備は、上記を統合した「ガバナンスとマルチステークホルダーによる実施基準に基づく規制」によることが有効と考えられる。すなわち、総論的な部分のルール形成とルール執行は法によるガバナンスベースの規制として国が行い、実施すべき具体的な措置の水準等についてはマルチステークホルダーが実施基準を作成するというものである。具体的には以下のイメージである。

・法によるガバナンスベースの規制とし、法に概要（利用者の権利、求める技術的・組織的な措置、違反時の罰則（ガバナンス構築・機能化のインセンティブとなる重さ）とガバナンス構築・機能化による減免、詳細は「技術的・組織的な措置の実施基準」によること等）を規定する。

・「技術的・組織的な措置の実施基準」は、社会的に適切な水準を定めるために、マルチステークホルダーが関与する組織で策定し、技術進歩に応じて短いサイクルで改定を実施する。

4. おわりに

本稿ではデジタル時代におけるプライバシー分野の一層のルール整備の方向性として「ガバナンスとマルチステークホルダーによる実施基準に基づく規制」を提案したが、具体的なルールの中身には踏み込んでいない。デジタル化の進展が個人のプライバシー、ひいては現代社会が重視する基本的な価値に与える影響の大きさ等を踏まえた具体的なルール整備を早急に進める必要があろう。

参考文献

[1] 上條英夫「デジタル時代におけるプロファイリングの課題と規制の方向性」(情報処理学会 第 83 回全国大会講演論文集、2021)
[2] 編集代表 中山信弘、藤田友敬編「ソフトローの基礎理論」(有斐閣、2008).
[3] 生貝直人「情報社会と共同規制」(勁草書房、2011)
[4] 小向太郎＋石井夏生利「概説 GDPR」（NTT 出版、2019）
[5] 山本龍彦 「『完全自動意思決定』のガバナンス ―行為統制型規律からガバナンス統制型規律へ？」 (総務省 学術雑誌『情報通信政策研究』 第３巻第１号、2019)