Vol.2022-EIP-95 No.20
2022/2/18

GDPR における行動規範と監視組織に関するガイドラインの分析 1

森京子†

概要：2019 年 6 月 4 日、欧州データ保護会議（EDPB）は"Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679"を採択した。これは、GDPR における行動規範と監視組織に関するガイドラインである。本ガイドラインは主に、GDPR 第 40 条及び第 41 条の適用に関する実務上の運用指針及び解釈上の支援を提供することを目的としている。本ガイドラインによると、行動規範には主に次の 3 つの利点があるとされる。第 1 に、特定の産業分野を代表する業界団体等が、当該分野で行われるデータ処理の特性等を考慮した行動規範を作成できる点、第 2 に、監督機関が特定の分野のデータ処理活動をより良く理解し洞察することに繋がる点、第 3 に、データ処理におけるデータ主体からの信頼を得るためのツールになりうる点、である。行動規範のこのような制度趣旨は、我が国の認定個人情報保護団体制度の制度趣旨と共通する。しかし、この 2 つの制度は現在、十分に活用されているとはいえない。日 EU 間は 2019 年の十分性相互認定で、民間事業者においては相互の円滑な個人データ移転を図る枠組みが構築されており、この枠組みを維持するためにも、日 EU 間の制度比較を行うことには意義がある。本稿においては、ガイドライン全体を概観し、第 1 章、第 2 章及び第 3 章の分析を行った。

キーワード：行動規範,プライバシー, 個人情報保護, 認定個人情報保護団体制度

Analysis of the Guidelines on Codes of Conduct and Monitoring Bodies under Regulation Ⅰ

KYOKO MORI†

Abstract: On June 4, 2019, the European Data Protection Board (EDPB) adopted "Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679." This is a set of guidelines on codes of conduct and monitoring bodies under the GDPR. The main aim of these Guidelines is to provide practical operational guidance and interpretive support for the application of Articles 40 and 41 of the GDPR. The Guidelines state that the Code of Conduct has the following main benefits: First, Industry associations representing a particular sector may develop a code of conduct that takes into account the characteristics of data processing in that sector, and second, supervisory authorities can gain a better understanding and insight of the data processing activities of a specific sector. Third, a code of conduct can be an effective tool for earning the trust of data subjects in data processing. This purpose of the Code of Conduct is common to the purpose of the accredited personal information protection association system in Japan. However, these two systems are not being fully utilized at present. The mutual adequacy decision between the EU and Japan in 2019 established a framework for smooth mutual transfer of personal data in the private sector, and in order to maintain this framework, we think it is worth comparing the systems between the EU and Japan. In this paper, the whole guideline is overviewed and Chapters 1, 2 and 3 are analyzed.

Keywords: Codes of conduct, Privacy, Data protection, Accredited Personal Information Protection Association System

1. はじめに

2019 年 6 月 4 日、欧州データ保護会議（EDPB）は" Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679"[1]を採択した。このガイドラインの目的は、GDPR における行動規範と監視組織に関して、第 40 条及び第 41 条の適用に関する実務上の運用指針及び解釈上の支援を提供することである。

本ガイドラインでは、行動規範には主に次の 3 つの利点が挙げられる。第 1 に、特定の産業分野を代表する業界団体等が、当該分野で行われるデータ処理の特殊性や、中小零細企業の特定のニーズを考慮した行動規範を作成することができる点、第 2 に、監督機関が特定の職業、産業、その他の部門のデータ処理活動をよりよく理解し洞察することを可能にする点、第 3 に、データ処理におけるデータ主体からの信頼を得るためのツールになりうる点、である。

我が国の制度で行動規範制度に類似するものとしては、認定個人情報保護団体制度（関連条文として個人情報保護法第 47 条 - 58 条）がある。いわゆる 3 年ごと見直しに係る有識者ヒアリング［2］では、「認定個人情報保護団体について、保有個人データに関する請求権をめぐる苦情・紛争処理や、通知・同意の具体的な方法や保存期間の設定等についてより適切な役割を果たしうるよう、体制強化のための施策を検討すべき」であるという指摘がされている。

認定個人情報保護団体制度には、主に次の 3 つの期待がされている。第 1 に、「各分野ごとに取り扱う個人情報の性質、利用方法、取扱いの実態等に即した、より高い水準の自主的な取組」[3]、第 2 に、「認定個人情報保護団体が、対

† (株)KDDI 総合研究所
KDDI Research, Inc.

象事業者の運用実態や課題等の情報を収集し、それを個人情報保護委員会と共有するといった役割」[3]、第 3 に、「個人情報の適正な取扱いを確保している業界であることについて、国民から一定の信頼を得る」[4]効果、である。

このように行動規範制度と認定個人情報保護団体制度は、共通の制度趣旨を掲げている。しかし、この 2 つの制度は現在、十分に活用されているとはいえない。令和元年度個人情報保護委員会委託調査「個人情報の適切な取扱いに関する実態調査」[4]によると、個人情報保護法の対象事業者約 4,000 社のうち認定個人情報保護団体を知らない事業者は 17%で、加入している割合も 15%に留まっている。また、EDPB の登録簿[5]を見ると、2022 年現在、加盟国内で承認された行動規範は 3 件と、限定的である。

そこで筆者は、制度が十分に活用され、制度趣旨が実現される方法を検討すべく、行動規範制度と認定個人情報保護団体制度とを比較して我が国の個人情報保護法制への示唆を得るために重要な要素を抽出することを目的として、本ガイドラインを分析した。

日 EU 間は 2019 年の十分性相互認定で、民間事業者においては相互の円滑な個人データ移転を図る枠組みが構築されており、この枠組みを維持するためにも、日 EU 間の制度比較を行うことには意義があると考える。

本稿においては、ガイドライン全体を概観し、第 1 章、第 2 章及び第 3 章の分析を行った。

2. ガイドラインの背景・目的・位置付け

本ガイドラインの背景、目的、及び適用範囲について概観する。

2.1 背景

本ガイドラインの背景については、以下のように説明されている。

GDPR は、2018 年 5 月 25 日に施行された。GDPR の主な目的の 1 つは、EU 全体で一貫したレベルのデータ保護を提供し、域内市場における個人データの自由な移動を妨げるデータ保護レベルのばらつきを防止することである。また、GDPR には説明責任の原則（第 5 条）が導入されており、データ管理者は GDPR 第 5 条に規定された基本原則について責任を負い、基本原則の遵守を証明しなければならないものとされている。行動規範に関する GDPR 第 40 条及び第 41 条の規定は、実務的で、潜在的に費用対効果の高い、有意義な方法を示しており、データ保護に関する権利を満たすためのより高いレベルでの一貫した保護を実現する。行動規範は、GDPR の遵守を証明するメカニズムとして機能しうる（第 24 条(3)、28 条(5)、32 条(3)）。特に、加盟国間に存在する可能性のある、データ保護法の適用におけるばらつきの解消に役立てることができる（前文 77、81、98、99、148、168、第 24 条、28 条、35 条、40 条、41 条、46 条、57 条、64 条、70 条）。これは、行動規範が複数の加盟国における取扱活動に関連している場合に特に該当する。行動規範はまた、特定の部門に共通するデータ取扱活動について検討する機会や、GDPR の要件及び当該分野のニーズを満たし、オーダーメイドで実務的なデータ保護ルールに合意する機会も提供する。行動規範は、必ずしも特定の部門に限定して作成する必要はない。例えば、同じ特性とニーズを持った共通の取扱活動を行う場合は、行動規範を分野横断的に適用することができる。行動規範が複数の部門に適用される場合、当該行動規範に複数の監視組織が任命されることがある。しかしこの場合、行動規範は当該監視組織の役割の範囲を完全に明確にしなければならず、そのためには、どの監視組織がどの分野で第 41 条に基づく役割を果たすかを特定し、どの監視組織がどの監視メカニズムを利用できるかを特定しなければならない。

加盟国、監督機関、EDPB、欧州委員会は、GDPR の適切な適用に貢献する行動規範の作成を奨励する義務があり（第 40 条(1)）、本ガイドラインは行動規範の作成、改正、追補を行う「行動規範所有者（code owners）」を支援し、促進するものとする。

2.2 目的

本ガイドラインの目的は、以下のように説明されている。

- GDPR 第 40 条及び第 41 条の適用に関する実務上の運用指針及び解釈上の支援を提供すること。
- 行動規範の提出、承認、公表に関わる手続やルールを、国内及び EU レベルで明確にすること。
- 行動規範の詳細な見直しや評価を行う前に、所轄監督機関が求める最低限の基準を定めること（第 40 条(5)、第 55 条(1)、及び前文 122 を参照。）。
- 行動規範が GDPR の適正かつ効果的な適用を提供し貢献しているか（第 40 条(1)及び前文 98）を評価する際に考慮すべき要素を定めること。
- 行動規範の遵守状況を効果的に監視するための要件を定めること。

また本ガイドラインは、すべての所轄監督機関、EDPB、欧州委員会が一貫した方法で行動規範を評価し、評価手続に関わる手続を効率化するための明確なフレームワークとして機能しなければならない。また、このフレームワークは、行動規範の承認を求める行動規範所有者が手続に十分に精通し、承認に必要な正式な要件と適切な基準値を理解できるようにしなければならない。

2.3 位置付け

GDPR 第 40 条(3)に基づく第三国または国際機関への個人データ移転ツールとしての行動規範（第 46 条(2)(e)を参照。）に関する運用指針[6]は、EDPB が発行する別のガイドラインで検討されるものとする。また、GDPR 及び本ガイドラインに先立って、各国のデータ監督機関又は第 29 条作業部会によって承認された行動規範はすべて、GDPR の

要件に沿って見直しと再評価を行い、第 40 条及並びに第 41 条の要件及び本ガイドラインに概説されている手続に従った承認をするために、再提出をする必要がある。

3. 用語の定義

用語の定義として、以下の 7 つが言及されている。

- **認定（Accreditation）**：とは、提案された監視組織が、行動規範の遵守状況の監視を実施するための GDPR 第 41 条に規定された要件を満たしていることの確認をいう。この確認は、承認のために行動規範が提出された監督機関によって行われる。監視組織の認定は特定の行動規範にのみ適用される。ただし、認定要件を満たす場合は、複数の行動規範について監視組織の認定を受けることができる。
- **行動規範所有者（Code Owner's）**:とは、行動規範を作成して提出する団体又はその他の組織を指す。様々な類型の管理者又は処理者を代表する団体及びその他の組織が行動規範所有者になることができる（40 条(2)）。また、行動規範で要求され、国内法に沿った、適切な法的地位を有するものとする。行動規範所有者の例としては、業界団体や学術団体等が考えられる（本ガイドライン 5.2 を参照。）。
- **所轄監督機関（CompSA）**：とは、GDPR 第 55 条に基づいて職務権限を有する監督機関を指す。
- **監視組織（Monitoring body）**：とは、GDPR 第 41 条に従って規範の遵守を確認し保証するための監視機能を実行する一つまたは複数の組織/委員会（行動規範所有者の内部または外部）を指す。
- **関係監督機関（Concerned SAs）**:GDPR 第 4 条(22)と同じ意味を持つものとする。
- **国内行動規範（National code）**:1 つの加盟国における取扱活動を対象とする行動規範をいう。
- **国際行動規範（Transnational code）**：2 つ以上の加盟国における取扱活動を対象とする行動規範をいう。

4. 行動規範

行動規範とは何かということについて、本ガイドラインでは次のように説明されている。

行動規範は、説明責任を果たすための任意ツールであり、管理者及び処理者の類型ごとに具体的なデータ保護ルールを定めたものである。行動規範は、分野別の最も適切で合法かつ倫理的な行動を詳細に説明する、使いやすく効果的な、説明責任を果たすためのツールである。データ保護の観点から見ると、行動規範は GDPR に準拠したデータ処理活動を設計・実装する管理者及び処理者のためのルールブックとして機能しうる。また、EU 法及び国内法に定められたデータ保護の原則に、業務上の意味を与える。ある部門を代表する業界団体又は組織は、当該部門が効率的かつ費用対効果の高い方法で GDPR を遵守するための行動規範を作成することができる。

4.1 行動規範が扱う事項

GDPR 第 40 条(2)に含まれる非網羅的なリストで定められているように、行動規範は特に以下のような事項を扱うことができる。

- 公正かつ透明性のある取扱い（第 40 条(2)(a)）
- 具体的な場面において管理者が求める正当な利益（第 40 条(2)(b)）
- 個人データの収集（第 40 条(2)(c)）
- 個人データの仮名化（第 40 条(2)(d)）
- 個人に対して提供される情報及び個人の権利の行使（第 40 条(2)(e)(f)）
- 子どもに対して提供される情報及び子どもの保護（親権者の同意を取得するためのメカニズムを含む）（第 40 条(2)(g)）
- データ保護バイデザイン及びバイデフォルト並びに安全管理措置を含む、技術的措置及び組織的措置（第 40 条(2)(h)）（第 24 条、25 条、及び 32 条参照。）
- 侵害通知（第 40 条(2)(i)）
- EU 域外へのデータ移転（第 40 条(2)(j)）
- 紛争解決手続（第 40 条(2)(k)）

4.2 データ保護指令との比較

GDPR は、データ保護指令（95/46/EC）の廃止に伴い、行動規範、満たすべき要件、承認取得に関与する手続、及び承認後の登録、公表、並びに周知について、より具体的かつ詳細な条項を定めている（GDPR 第 40 条(2)‐(11)を参照）。これらの条項は、本ガイドラインと併せて、行動規範所有者が当該取扱部門のデータ保護基準やルールを積極的に制定することを奨励する一助になる（GDPR 前文 98 及び第 40 条(1)を参照）。

4.3 留意点

行動規範は、データ保護影響評価（DPIA）や認証など、GDPR が提供するデータ保護における説明責任を果たすためのツール一式の中から利用できるいくつかの任意ツールの一つであることに注意が重要である。行動規範と認証は任意のツールであるのに対し、DPIA は特定の状況において義務付けられている。

また、行動規範の遵守自体は、GDPR の遵守や、GDPR の下で定められた制裁や責任から管理者／処理者が免責されることを保証するものではない。

5. ガイドラインの構成

本ガイドラインは、以下のような章立てで構成されている。

5.1 章立て

1. はじめに
1.1. 本ガイドラインの適用範囲
2. 定義
3. 行動規範とは何か
4. 行動規範の利点は何か
5. 行動規範案の事前審査基準
5.1. 行動規範案の説明文書及び補足資料
5.2. 代表者
5.3. 対象とする処理
5.4. 対象とする地域
5.5. 所轄監督機関への提出
5.6. 監視のメカニズム
5.7. 監視組織
5.8. 関連する利害関係者との協議内容
5.9. 国内法令
5.10. 言語
5.11. チェックリスト
6. 行動規範の承認基準
6.1. 特定のニーズに対応
6.2. GDPR の効果的な適用を促進
6.3. GDPR の適用を明示
6.4. 十分な保護措置の提供
6.5. 効果的な監視を可能にするメカニズムを提供
7. 提出、事前審査、承認（国内行動規範）
7.1. 提出
7.2. 行動規範の認容
7.3. 承認
8. 提出、事前審査、承認（国際行動規範）
8.1. 提出
8.2. 行動規範の事前審査
8.3. 監督機関間の協力
8.4. 拒否
8.5. EDPB への提出に向けた準備
8.6. EDPB
8.7. 承認
9. 行動規範所有者と所轄監督機関とのエンゲージメント
10. 欧州委員会の役割
11. 行動規範の監視
12. 監視組織の認定要件
12.1. 独立性
12.2. 利益相反
12.3. 専門性
12.4. 手続及び組織構造の規定
12.5. 苦情処理の透明性
12.6. 監視組織と所轄監督機関との連絡
12.7. 見直しのメカニズム
12.8. 法的地位
13. 承認後の行動規範
14. 監視組織の取消し
15. 公的部門における行動規範
附属文書 1 - 国内行動規範と国際行動規範の区別
附属文書 2 - 所轄監督機関の選択
附属文書 3 - 提出用チェックリスト
附属文書 4 - 国際行動規範フローチャート

5.2 各章の構成と概要

第 1 章では、本ガイドラインの背景、目的、及び適用範囲について述べられている。第 2 章では、本ガイドラインにおける用語の定義が示されている。第 3 章では、行動規範とは何かについて説明されている。第 4 章では、行動規範の利点が説明されている。第 5 章では、行動規範の詳細な評価や見直しを行う前に、所轄監督機関が要求する最低限の基準が定められており、行動規範案の効率的な評価を促進することが目的とされている。第 6 章では、第 5 章で定めた基準による事前審査を経た行動規範案を、所轄監督機関が詳細に評価する手続が具体的に解説されている。第 7 章と第 8 章では、行動規範所有者が行動規範案を所轄監督機関に提出した後の手続について、国内行動規範（1 加盟国における取扱活動を対象とする行動規範）と、国際行動規範（複数加盟国における取扱活動を対象とする行動規範）とを区別して説明されている。第 9 章では、行動規範所有者と所轄監督機関とが連絡を取る内容や方法について注意すべき点を述べている。第 10 章では欧州委員会の役割が説明されている。第 11 章では、行動規範の監視について、第 12 章では監視組織の認定要件について、第 41 条に沿って解説されている。第 13 章では、承認後の行動規範について補足事項を説明している。第 14 章では、監視組織の取消しが解説され、第 15 章では、公的部門における適用除外が説明されている。第 41 条(6)では、承認された行動規範の監視は、公的機関や団体が実施するデータ処理には適用されないと定められているが、既存の監査要件を行動規範の監視を含むように適合させることで、行動規範を監視するための効果的なメカニズムの実装を達成できると述べている。

6. まとめと今後

本稿で扱った第 1 章、第 2 章、及び第 3 章について概観すると、特に次の 3 点が重要である。

まず、行動規範は、産業分野を代表する業界団体又は組織が、GDPR に準拠したデータ処理活動を設計・実装する管理者及び処理者のために、各産業分野とって最も適切で合法かつ倫理的な行動を詳細に説明する、自主的なルールブックであるという点である。我が国の認定個人情報保護団体制度に関するガイドライン［3］でも、「法に規定する個人情報取扱事業者等の義務は、あらゆる分野を対象とする法の性格上、必要最小限度の規律である」ことが課題と

してあげられており、行動規範制度の役割は大きいと考える。また、このような行動規範制度の制度趣旨が広く認識されることが、この制度が十分に活用されるために重要だと考える。

次に、本ガイドラインの重要な点として、行動規範制度の背景が 2 点示されていることが挙げられる。第 1 に、GDPR は加盟国間のデータ保護レベルのばらつきを防ぎ、EU 域内における自由な個人データの移動の実現を主な目的の一つとしている点である。行動規範制度はこのようなばらつきを解消することが期待されている。第 2 に、GDPR は説明責任の原則（第 5 条）を導入しており、行動規範はそのための任意ツールとされている点である。このような行動規範制度の背景と我が国の認定個人情報保護団体制度の背景における相違点・共通点を踏まえて、我が国の個人情報保護法制への示唆を検討したい。

最後に、本ガイドラインを参照する上で注意すべき点として、第三国または国際機関への個人データ移転ツールとしての行動規範（第 40 条(3)、第 46 条(2)(e)を参照。）に関しては、別のガイドライン[6]が発行されている点が挙げられる。個人データの第三国への移転を想定した行動規範を作成する場合は、本ガイドラインだけではなく、他のガイドラインも参照することとされている点を踏まえて、行動規範制度と認定個人情報保護団体制度との比較を行う必要がある。

上記の点は、本ガイドラインを分析し、行動規範制度と認定個人情報保護団体制度との比較検討を行う上で前提となる、重要な要素であると考える。本ガイドラインはこの他にも様々な内容が解説されているため、数回に分けて分析する予定である。引き続き第 4 章以降の分析を行い、制度比較において重要な要素を抽出していきたい。

参考文献

[1] The European Data Protection Board, “Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679” 〈https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf〉 (参照 2022-01-17).
[2] 宍戸常寿「個人情報保護法のいわゆる 3 年ごと見直しに関する意見」（個人情報保護委員会,2019）. 〈https://www.ppc.go.jp/files/pdf/0521_shiryou2-3.pdf〉(参照 2022-01-17) .
[3] 個人情報保護委員会（2021）「個人情報の保護に関する法律についてのガイドライン（認定個人情報保護団体編）」1-2 頁.
[4] 個人情報保護委員会「認定個人情報保護団体制度の概要」〈https://www.ppc.go.jp/personalinfo/nintei/summary/#effect〉(参照 2022-01-27) .
[5] 株式会社フューチャー・コミュニケーションズ「個人情報の適切な取扱いに関する実態調査（令和元年度）報告書」（個人情報保護委員会,2020）24 頁.
[6] EDPB, “Register for Codes of Conduct, amendments and extensions”, 〈https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en〉(参照 2022-01-17) .
[7] The European Data Protection Board, “Guidelines 04/2021 on codes of conduct as tools for transfers” 〈https://edpb.europa.eu/system/files/2021-07/edpb_guidelinescodesconducttransfers_publicconsultation_en.pdf〉(参照 2022-01-17) .