Vol.2022-EIP-96 No.15
2022/6/10

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 2

森京子[†1][†2]

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。筆者は、行動規範制度と認定個人情報保護団体制度が十分に活用され、両制度の趣旨が実現される方法を検討すべく、制度比較を行うための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ている。本稿においては、第 4 章から第 8 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 Ⅱ

KYOKO MORI[†1][†2]

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 author analyzes these Guidelines with the aim of extracting important elements for comparing the systems in order to examine how the code of conduct system and the accredited personal information protection association system can be fully utilized and the purpose of both systems can be realized. In this paper, Chapters 4 through 10 were 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。本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。

筆者は、GDPR における行動規範制度と我が国の個人情報の保護に関する法律（以下「個人情報保護法」という。）における認定個人情報保護団体制度が十分に活用され、両制度の趣旨が実現される方法を検討すべく、制度比較を行うための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ている。また、日 EU 間は 2019 年の十分性相互認定で構築された、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ている。

本稿においては、本ガイドラインにおける用語の定義等の整理、全体の概説、第 1 章から第 3 章の分析を踏まえ[2]、第 4 章から第 10 章の分析を行う。

なお、次章以降、矢羽根の箇条書きで記載した部分は、筆者が本ガイドラインを抜粋して翻訳したものである。

2. ガイドラインの利点

行動規範の利点について、本ガイドライン第 4 章では主に次の点[1]が説明されている。

- 各分野で行われるデータ処理の特殊性を考慮した、管理者及び処理者のための行動規範を作成することができる。
- GDPR の適正かつ効果的な適用に貢献するものであれば、行動規範は全ての処理部門で利用でき、当該部門に適した、限定的又は広範な範囲で起草することが可能であり、管理者及び処理者の類型の代表者としての基準を満たしていれば、実務上は、分野を横断する内容を含むことができる。
- 行動規範は、一定程度の共同規制を提供することができる。
- 特定の処理活動に関するより細やかな運用指針が提供されることにより、管理者及び処理者がデータ保護監督機関にかけることがある依存度を低下させることができる。
- 行動規範は、管理者及び処理者が各自の分野におけるベストプラクティスルールを策定及び合意するための、一定程度の自律性と制御性を提供することができ、

†1 (株)KDDI 総合研究所
KDDI Research, Inc.

†2 一橋大学大学院法学研究科ビジネスロー専攻修士課程
Hitotsubashi University

特定の分野における処理業務のベストプラクティスの処理業務を集約する機会にもなる。

- データ処理手順における重要な問題に対処し、より良いデータ保護における法令遵守を達成するための、企業にとって信頼できる重要なリソースになり得る。
- 共通の処理活動に関して特定の部門が直面している問題に対する実務上の解決策を提供することで、信頼と法的安定性を提供することができる。
- 行動規範は、データ主体から信用と信頼を得るための効果的なツールになり得る。
- 行動規範は、第三国へのデータ移転の分野でも重要かつ有用なメカニズムになる可能性がある。GDPR は、第三国に対する個人データの移転における、適切な保護措置を提供する要件を満たすために、第三国の管理者又は処理者が、行動規範の遵守に同意することを認めている。（GDPR 第 40 条(2)(j)及び第 40 条(3)）
- 第三国に対する個人データの移転における適切な保護措置を提供する行動規範は、GDPR が提供する保護レベルを国際社会でより広く促進・普及させるとともに、第三国への移転における法令遵守を持続可能にする。
- 欧州経済領域外でのデータ処理に対するデータ主体の信頼と信用をさらに発展・促進させるメカニズムとしても機能する。
- 行動規範は、処理者及び管理者にとって、効果的に説明責任を果たすツールとして機能し得る（GDPR 前文 77、第 24 条(3)、及び 第 28 条(5)）。
- 行動規範の遵守は、データ処理の安全性（第 32 条(3)）等の特殊事情を評価する際、DPIA（第 35 条(8)）においてデータ処理の影響を評価する際、又は制裁金を課す（第 83 条(2) (j)）際に、監督機関が考慮する要素にもなる。なお、EDPB で採択された、GDPR における制裁金の適用及び設定に関するガイドライン［3］の行動規範への適用に留意が必要である。

さらに、第 4 章では、実際に行動規範制度の活用が見込まれる事例を示しながら、行動規範の利点について次の点[1]を説明している。

- より費用対効果の高い方法でデータ保護における法令遵守を実現できるメカニズムを提供することで、中小零細企業にとって、特に重要で有益なツールとなる可能性がある（GDPR 第 40 条(1)を参照。）。例えば健康に関する類似の研究活動に携わる零細企業は、広範なデータ保護分析を独自に行うのではなく、それぞれの関連団体を通じて集まり、健康データの収集と処理に関する行動規範を共同で策定することができる。
- 特定の職業、産業、その他の分野のデータ処理活動に対する理解と洞察を深めることができるため、監督機関にとっても有益である。例えば、特定の非営利分野における処理に関する取決めが、公正かつ透明性があることを確保するための一連のルールについて、承認を求めることができる。あるいは、個人データ収集の適法な根拠から個人データ侵害の通知まで、特定の非営利分野における処理活動の全てを網羅するために、GDPR に基づく様々な規定を組み合わせて適正に適用する行動規範を作成することを選択できる。
- 一般市民の懸念や、業界内部で認識されている懸念から生じる様々な問題に対処することができる。例えば、研究目的で健康データを処理する場合、機微性の高い健康情報の処理に適用されるルールの遵守を促進するために採用すべき適切な措置に関する懸念は、詳細な行動規範の存在によって緩和される可能性がある。このような行動規範は、公正で透明性のある方法で次の事項を概説することができる。
  - データ主体に提供される情報に関して適用されるべき関連する保護措置。
  - 第三者から収集されたデータに関して適用されるべき適切な保護措置。
  - データの連絡又は配布。
  - データの最小化原則の尊重を確保するために実装されるべき基準。
  - 具体的な安全管理措置。
  - 適切にデータを保有する計画。
  - データ主体の権利行使の結果としてデータを管理するメカニズム（GDPR 第 32 条及び第 89 条）

3. 行動規範案の事前審査基準

本ガイドライン第 5 章では、所轄監督機関が第 40 条(5)に基づく行動規範の詳細な評価や見直しを行う前に満たすべき条件について説明している。これらの条件は、全ての行動規範案を効率的に評価することを目的としており、以下の基準が適用される。なお第 5 章は、全ての行動規範（国内行動規範（National code）及び国際行動規範（Transnational code））、並びに改正又は追補された行動規範にも適用される。

3.1 説明文書及び補足資料

行動規範案を提出する際は、説明文書及び必要に応じて補足資料を添付しなければならない。説明文書では、「行動規範の目的、適用範囲、及び GDPR の効果的な適用をどのように促進するか」について、明確かつ簡潔な説明を記載しなければならない。添付する補足資料の例としては、「行動規範案策定に向けた協議の概要、メンバー（行動規範の適用を受ける者）に関する情報、行動規範の必要性を証明する調査」[1]などが挙げられる。

3.2 代表者

事前審査基準のうち、代表者の基準について、本ガイドラインでは以下のとおり説明されている。

行動規範は、第 40 条(2)に従い、管理者又は処理者の類型を代表する団体又はその他の組織等（行動規範所有者（Code Owner's））から提出されなければならない。行動規範所有者の例としては、「業界団体、代表者団体、部門別組織、学術団体、利益団体等」[1]が挙げられる。行動規範所有者は、「メンバーのニーズを理解し、行動規範の適用を予定する処理活動又は分野を明確に定義する能力があることを、所轄監督機関に対して証明しなければならない。」[1]

代表者であることの判断基準は、当該部門の定義やパラメータにもよるが、特に以下の要素から導き出すことが可能である。

- 当該分野に関連する管理者と処理者のうち、行動規範の潜在的なメンバーの数又は割合。
- 当該行動規範の分野及び処理活動に関する代表組織の経験。

3.3 適用する処理の範囲及び地理的適用範囲

行動規範案には、行動規範案を適用する処理の範囲（「個人データの処理業務（又は処理の特徴）、及び管理者及び処理者の類型を明確かつ正確に決定する範囲」）及び地理的適用範囲を明確に定義しなければならない。地理的適用範囲を明確にするため、国内行動規範であるか、国際行動規範であるかを明記しなければならない。また、国際行動規範として提出する場合は、関係監督機関のリストを添付しなければならない。

3.4 関連する利害関係者との協議内容

事前審査基準のうち、関連する利害関係者との協議内容に関する基準については、本ガイドライン第 5 章で次のように説明されている。

「行動規範所有者は、行動規範案を提出する際に、関連する利害関係者と適切なレベルの協議が行われたことを確認し、証明する必要がある。」[1]その際、「行動規範の潜在的なメンバーに適用される可能性がある他の行動規範に関する情報や、当該行動規範が他の行動規範をどのように補完するかを必要に応じて示すものとする。」[1]

また、「有用性がないとして、関連する特定の利害関係者との協議が行われなかった場合は、行動規範所有者がこの点を説明しなければならない。」[1]

3.5 その他の事前審査基準

上記 3 つの事前審査基準のほか、本ガイドライン第 5 章では以下の点[1]が挙げられている。

- 行動規範所有者は、行動規範案の見直しのために選択した監督官庁が、第 55 条に基づく職務権限があることを確認しなければならない。
- 行動規範案は、当該行動規範を適用している管理者又は処理者による当該行動規範の条項遵守を監視できるメカニズムを提案しなければならない（第 40 条(4)）。
- 民間及び非公共機関又は組織の処理活動を含む行動規範案は、監視組織を特定し、その組織が第 41 条に基づきその職務を遂行することを可能にするメカニズムを規定しなければならない。公共部門が関与する行動規範も、行動規範を監視するための適切なメカニズムを規定しなければならない。
- 行動規範所有者は、行動規範案が関連する国内法令を遵守していることの確認を行わなければならない。
- 行動規範所有者は、行動規範を提出した所轄監督機関の言語要件に従うべきであり、国際行動規範の場合は、所轄監督機関の言語及び英語で提出しなければならない [4]。

4. 行動規範案の承認基準

第 6 章では、第 5 章で示され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。行動規範所有者が、当該行動規範案が次のようなものであることを証明できなければならない事項について、第 6 章では以下の点[1]を挙げている。

- 特定の部門又は処理活動で生じる特定のニーズを満たす。
- GDPR の適用を容易にする。
- GDPR の適用を具体化する。
- 十分な安全管理措置を提供する。
- 行動規範の遵守を監視するための効果的なメカニズムを提供する。

また、本ガイドライン第 6 章では、上記 5 つの承認基準ごとに具体的な事例を示して解説されており、その内容を概観する。

4.1 特定のニーズを満たす行動規範の例

行動規範の所有者は、行動規範を制定する必要性を証明することが求められる。そのため、行動規範は特定の部門又は処理活動で生じるデータ保護における課題に対処するものでなければならない。本ガイドライン第 6 章で示されている特定のニーズを満たす行動規範の例は以下の 2 点である[1]。

- 消費者の信用リスクを検出する情報システムの分野では、収集されたデータが適切かつ正確であり、信用を保護するという特定の正当な目的のみに使用されることを保証する、十分な保護措置及びメカニズムを提供する行動規範を策定する必要性が識別されること。
- 健康に関する研究分野では、GDPR における明示的な同意とそれに伴う説明責任の要件を適切に満たすた

めの基準を設定することで、同意の取得方法に一貫性を持たせるための行動規範を策定する必要性が識別されること。

4.2 GDPR の適用を容易にする方法の例

GDPR 前文 98 にあるように、行動規範の承認を得るためには、行動規範所有者が、当該行動規範が GDPR の効果的な適用を促進することを証明できなければならない。GDPR の効果的な適用を促進する方法の例は以下の 3 点[1]である。

- 当該分野特有の定義を一覧にして提供することや、当該分野に特に関連する問題に適切に焦点を当てること。
- 当該分野特有の専門用語を使用して、分野における GDPR の要件の実装を詳細に説明すること。
- ダイレクトマーケティングにおける個人データの使用等、特定分野の処理活動に関連する見込みの高いリスクを十分に考慮し、当該特定分野のリスクに照らして適用される管理者又は処理者に関連する義務を適切に調整すること。

4.3 GDPR の適用を具体化する方法の例

行動規範は、「全てのメンバーに対して現実的かつ達成可能な基準を設定する必要があり、十分な付加価値を提供するために必要とされる質及び内的整合性が必要」[1]である。なおこの基準は、1998 年 9 月 10 日に採択された「行動規範に関する今後の作業：行動規範作業部会による検討のための手順に関する作業文書 [5]で初めて採用された。本ガイドライン第 6 章では、GDPR の適用を具体化する方法例が以下 5 点[1]挙げられている。

- 行動規範が単に GDPR を再記述するものではないこと。
- 業界独自の専門用語を使用し、具体的な事例や 「ベストプラクティス」の例を提供すること。
- 過度に法律的であることを避けること。
- 承認された行動規範を普及させ、その存在と内容を個人に知らせる計画を概説すること。
- 特定の部門や処理活動に対して欧州委員会が発表又は承認した関連する意見及び立場を適正に考慮すること。

GDPR の適用を具体化する行動規範の例として、さらに次の点[1]が述べられている。

- 処理活動に関する規定を含む行動規範は、適用を予定している加盟国において、当該処理活動の適切な法的根拠の特定を容易にする可能性もある。

4.4 十分な保護措置を提供する例

十分な保護措置を提供する行動規範の例は、本ガイドライン第 6 章で以下の 2 点[1]が示されている。

- 子供や健康に関するデータの大規模な処理、プロファイリング、体系的な監視など、「高リスク」の処理活動において、適切な保護レベルを実現するために、管理者又は処理者に対するより厳しい要求が行動規範に含まれることが予想される。さらに、行動規範所有者は、そのような高リスク領域の処理を含む行動規範を裏付けるために、前文 99 に基づき、より広範な協議を実施することが有益となる場合がある。
- 子供のデータや健康データの処理などの「高リスク」分野における行動規範には、当該個人データの機微性を考慮した、より強固で厳格な安全管理措置を含むことが期待される。

4.5 効果的な監視を可能にするメカニズムの提供例

効果的な監視を可能にするメカニズムには、「定期的な監査と報告義務、明確で透明性のある苦情処理と紛争解決手続き、当該行動規範に違反した場合の具体的な制裁及び救済措置、並びに当該違反を報告するための方針」[1]が含まれる。

4.6 参考とすべき文書

また、本ガイドライン第 6 章では、行動規範の付加価値及び当該価値が効果的であることの判断について、第 29 条作業部会文書「業界の自主規制を判断する：どのような場合に第三国のデータ保護水準に有意義な貢献ができるか。」[6] を考慮することが推奨されている。

5. 申請、事前審査、承認（国内行動規範）

本ガイドライン第 7 章及び第 8 章では、行動規範案の所轄監督機関提出後の手続について、国内行動規範と、国際行動規範とを区別して説明している。なお、承認済みの行動規範を改正又は追補する場合についても、第 7 章及び第 8 章が適用される。国内行動規範における手続きを概説する第 7 章の要旨は以下のとおりである。

申請時においては、行動規範所有者が、当該申請が行動規範案の正式なものであることを所轄監督機関に対して明確に示すことが重要である。

事前審査段階においては、事前審査基準を満たさないとする決定がされた場合、「行動規範案の規定に関する実質的又は中核的な問題ではなく、一般的又は手続き的な予備的要件に基づく可能性が高い」[1]。この場合、手続きは終了し、行動規範所有者が再申請を希望する際は、改めて正式な手続きを行うこととなる。

承認段階においては、「国内法で特定の期限が定められていない限り、所轄監督機関は妥当な期間内に意見案を作成すべき」[1]である。所轄監督機関は、「意見書により、行動規範所有者に対して有益なフィードバックを提供することができる。」[1]所轄監督機関が不承認決定を下した場合、行動規範所有者が行動規範案の再申請を希望する際は、改

めて正式な手続きを行う必要がある。所轄監督機関が行動規範案を承認した場合、所轄監督機関は行動規範を登録し、ウェブサイト等を通じて公表する必要がある（第40条(6)）。また、GDPR 第 40 条(11)は、EDPB に対し、承認された全ての行動規範を一般に公開するよう求めている。

6. 申請、事前審査、承認（国際行動規範）

国際行動規範における手続きを概説する第 8 章の要旨は以下のとおりである。

基本的には、国内行動規範に関する第 7 章の記述と同様であり、申請段階については主に次の 3 点[1]で異なる。

- 所轄監督機関は、行動規範所有者に対し、文書の受理を通知し、行動規範案を上記の事前審査基準に照らして見直した後、内容に対する詳細な評価を実施する（本ガイドライン附属文書 3 を参照。）。
- 所轄監督機関は、行動規範の提出を他の全ての監督機関に直ちに通知し、確認及び参照が容易になるような特記すべき内容を提供する。これに対し、全ての監督機関は、GDPR 第 4 条 22 項(a)(b)に基づく関係監督機関であるか否かを返答しなければならない。
- 管理者又は処理者が当該監督機関の加盟国内に拠点を有するため、又は当該監督機関の加盟国に居住するデータ主体が、当該処理によって重大な影響を受けるか、又はその可能性が高いために、個人データの処理に関係する監督機関が行動規範案の共同評価者となることが想定されている。

また、事前審査段階以降の手続きでは、次の点[1]で第 7 章の記述と異なる。

- 行動規範案が上記の事前審査基準を満たす場合…行動規範の承認に向けた評価に関して、以下に示す略式の協力手順が開始される。
- 所轄監督機関は、関係監督機関を特定する通知を発行し、行動規範案の実質的な評価を支援する共同評価機関を任意で最大 2 つまで要請するものとする。原則として、14 カ国以上の加盟国が行動規範に関係している場合、所轄監督機関は 2 つの共同評価機関に相談する。この基準の下では、個別の案件ごとに 1 つ又は 2 つの共同評価機関を置くことが可能である。
- 共同評価機関の役割は、所轄監督機関による行動規範案の評価を支援することであり、共同評価機関確定後 30 日以内に、行動規範の内容に関する意見を提供しなければならない。これらの意見は、所轄監督機関が承認のための評価を行う際に考慮される。その上で、GDPR 第 40 条(7)に従い、所轄監督機関は、決定案を EDPB に提出すべきかについて最終的な判断を下さなければならない（第 63 条及び第 64 条を参照。）。
- 当該協力手続きは、所轄監督機関が行動規範案の承認を目指している場合にのみ発生し得る（第 40 条(7)及び第 64 条(1)を参照。）。
- 所轄監督機関が行動規範案の EDPB への送付を行わない決定を下した場合、所轄監督機関は、全ての関係監督機関に対し、行動規範の承認を拒否する旨及び理由を通知しなければならない。
- 所轄監督機関が行動規範案の承認を目指す場合、EDPB に提出する前に、所轄監督機関は当該承認案を全ての関係監督機関に回覧する。全ての関係監督機関は 30 日以内に回答し、関係監督機関からの回答がない場合は、行動規範は次の段階に進む。
- GDPR 第 40 条(7)に基づき、EDPB への送付を決定した場合、所轄監督機関は当該決定を、一貫性メカニズムの手続きに従い、全ての監督機関に連絡する。
- 所轄監督機関は、手続規定及び GDPR 第 40 条(7)に基づき、本件を EDPB に送付する。
- EDPB は、GDPR 第 64 条に基づき、GDPR 第 40 条(7)に規定された事項に係る意見を発行するものとする（第 70 条 (1)(x)を参照。）。なお、国際行動規範の承認に関する評価を実施し、決定を連絡する際には、EDPB 手続規定と GDPR 第 64 条の規定が EDPB 及び所轄監督機関に適用される。
- EDPB の意見は、GDPR 第 64 条(5)に基づき所轄監督機関伝えられ、第 40 条(5)に基づき、当該決定案を維持又は改正するかを所轄監督機関が判断する。GDPR 第 64 条(8)に従って所轄監督機関が EDPB の意見に従わない場合の手続きに留意されたい（第 64 条(7)を参照）。
- EDPB の意見は、GDPR 第 40 条(8)に基づき欧州委員会に提出することもできる。
- EDPB は、第 40 条(11)に基づき、承認されたすべての国際行動規範を整理列挙し、公衆がそれを利用できるようにするものとする。

7. 所轄監督機関と行動規範所有者との連携

本ガイドライン第 9 章では、所轄監督機関と行動規範所有者との連絡方法について、主に以下の 4 点[1]が説明されている。

- 正式な提出後における所轄監督機関と行動規範所有者間の連絡は、主として明確化を目的とするものであり、原則として、行動規範所有者は行動規範案の特定の条項について更なる協議を求めるべきではない。行動規範所有者は、行動規範案を提出する前に、必要に応じて監督機関と連携を図ることが期待される。
- 行動規範所有者は、行動規範案に関する問い合わせに回答することができ、妥当な期間内での回答が求められる。行動規範所有者は、所轄監督機関に対し、単一又は専用の窓口を設けることが推奨される。

- 行動規範案について決定を行う前に、情報を追加で必要とするかどうかは、所轄監督機関の裁量に委ねられ、また、当事者間の連絡方法についても所轄監督機関の裁量に委ねられる。
- 所轄監督機関は、国際行動規範の承認手続き全体を通じて、主要な連絡窓口としての業務を継続して行う。

8. 欧州委員会の役割

欧州委員会の役割について、本ガイドライン第 10 章は次の 2 点[1]を説明している。

- 欧州委員会は、実装法令によって、承認された国際行動規範が EU 域内において一般的な有効性を持つと決定することができ、その場合、適切な周知を確保するものとする（第 40 条(9)(10)）。
- 当該決定は、GDPR の適用対象となっていない管理者又は処理者が、有効性を持った行動規範に関して拘束力があり執行可能な約束を形成することも許容することになる（第 40 条（3）を参照。）。これにより、適切な保護措置が実施され、データ主体の権利と効果的な法的救済が確保されることを根拠として、第三国又は国際機関へのデータ移転が可能となる（第 46 条 1 項及び第 46 条 2 項（e）も参照。）。

9. まとめと今後

本稿で扱った第 4 章から第 10 章を概観すると、特に次の点が重要である。

本ガイドライン第 4 章では、まず、行動規範制度の利点について、①各分野で行われるデータ処理の特殊性を考慮した、管理者及び処理者のための行動規範を作成することができる、②特定の職業、産業、その他の分野のデータ処理活動に対する理解と洞察を深めることができるため、監督機関にとっても有益である、③データ主体からの信頼を得るための効果的なツールになり得る、と説明されている。この点、我が国の個人情報保護法における認定個人情報保護団体制度は、「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）」[7]において、①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、②認定個人情報保護団体が、対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、という制度趣旨が説明されており、少なくとも上記 3 点において共通の制度趣旨を有する制度であるといえる。

次に、行動規範は、必ずしも特定の分野に限定して作成する必要はなく、代表者としての基準を満たしていれば、実務上は、分野を横断する内容を含むことができる[1]と説明されている。この点、認定個人情報保護団体制度では、令和 2 年に、企業の特定分野（部門）を対象とする団体を認定できるよう改正が行われた（個人情報保護法第 47 条第 2 項及び第 3 項）。改正前は、対象事業者の全ての分野（部門）を対象として、その業務を行うこととされていたが、「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）」[7]では、次の 2 つの実態を踏まえた改正であると説明されている。「①個人情報取扱事業者等における業務実態の多様化や IT 技術の進展に伴い、民間団体が特定分野における個人データの取扱いに関するルールを運用していくことや、積極的に対象事業者に対して指導等を行っていくことの重要性が増してきた」[7]こと、及び「②個人情報取扱事業者等にとっても、事業展開が多様化・多角化される中で、当該個人情報取扱事業者等の業務の範囲に適合した認定個人情報保護団体を選択することが容易でなくなってきている」[7]ことである。

また、当該改正において想定されている事例として、「特定分野（部門）の事業が業種横断的に行われている場合に、当該特定分野の個人情報等の取扱いを対象とする法人」[7]が示されているが、上記の事例を想定した改正は、行動規範制度との類似性を高めるものといえるかについて、十分制相互認定の枠組みを維持するために日欧の制度の整合性を検討する観点から、調査が必要だと考える。

第 3 に、本ガイドラインでは、健康データを用いた研究活動に携わる企業などを挙げ、行動規範制度の活用が見込こまれる事例を示している。我が国の認定個人情報保護制度の活用を検討する上で、このような海外の知見が役立つ可能性がある。また、当局が活用事例を積極的に示していくことが、制度趣旨が十分に実現されるために重要ではないかと考える。

4 点目として、行動規範は、一定程度の共同規制を提供することができると説明されているが、共同規制として捉える議論は、我が国でも認定個人情報保護団体制度に対して進められている[8][9][10]。

5 点目として、本ガイドライン第 5 章以降では、行動規範案の所轄監督機関への提出から承認までの手続きが説明されているが、監督機関による行動規範の承認（GDPR 第 40 条(5)）、EDPB による意見陳述（第 40 条(7)）、欧州委員会の関与（第 40 条(9)）が規定されているように、自主ルール[11]である行動規範に対して「政府の側が公式な承認を行う」[12]形で関与する制度となっている。この点、我が国の認定個人情報保護団体制度では、個人情報保護委員会は、個人情報保護指針の変更その他の必要な措置をとるべき旨を命ずることができ（個人情報保護法第 57 条）、自主ルールの適正性について関与が可能である。こうした関与の方法は、生貝（2011）が整理した「自主規制に対する公的統制の手段」[12]における「適正性の確保」[12]に位置づけられると考える。また、本ガイドライン第 5 章で、行動

規範案の事前審査基準に挙げられているように、「行動規範所有者は、行動規範案を提出する際に、関連する利害関係者と適切なレベルの協議が行われたことを確認し、証明する必要がある。」[1]この点において認定個人情報保護団体制度は、認定個人情報保護指針を作成する際、消費者の意見を代表する者その他の関係者の意見を聴くことが、認定個人情報保護団体の努力義務とされている。自主規制に対する両制度の当該手法は、「一般市民や消費者団体等の意見申立・参加経路を設けるよう要請する」[12]ものであるといえ、「適正性の確保」[12]に位置づけられると考える。両制度の適正性が確保されることは、両制度の「データ主体からの信頼を得るための効果的なツール」[1]及び「国民から一定の信頼を得る」[7]という制度趣旨の実現にも貢献するといえる。

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。引き続き第 11 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] 森京子「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」『研究報告電子化知的財産・社会基盤（EIP）2022-EIP-95』（情報処理学会,2021）
[3] Article 29 Data Protection Working Party, “Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253”
〈https://ec.europa.eu/newsroom/article29/redirection/document/80836〉(参照 2022-05-03) .
[4] EDPB, “EUROPEAN DATA PROTECTION BOARD RULES OF PROCEDURE Version 8”,
〈https://edpb.europa.eu/system/files/2022-04/edpb_rules_of_procedure_version_8_adopted_20220406_en.pdf〉(参照 2022-05-03) .
[5] EUROPEAN COMMISSION,” Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct, DG XV D/5004/98, WP 13” , adopted on 10 September 1998 .
[6] EUROPEAN COMMISSION, “Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?, DG XV D/5057/97 final, WP 7”
〈https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp7_en.pdf〉（参照 2022-05-03）.
[7] 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）」
[8] 生貝直人 「個人情報保護に関わる共同規制の国際動向」『 令和 3 年 3 月 16 日「認定個人情報保護団体シンポジウム開催」（結果概要）』（個人情報保護委員会,2021）
[9] 小林慎太郎「『匿名加工情報』 によるビッグデータビジネス活性化への期待と課題 マルチステークホルダー・プロセスによるルール作り」『知的資産創造』36 頁（NRI,2015）
[10] 総務省 2013 ）「パーソナルデータの利用・流通に関する研究会（第 6 回）議事要旨」2 頁,3 頁
[11] 小向太郎＝石井夏生利『概説 GDPR―世界を揺るがす個人情報保護制度』45 頁（NTT 出版,2019）
[12] 生貝直人『情報社会と共同規制 インターネット政策の国際比較制度研究』47 頁、48 頁（勁草書房,2011）