Vol.2023-EIP-99 No.14
2023/2/17

行動規範のモニタリングに関する一考察
～GDPR における行動規範とモニタリング組織に関するガイドラインの分析３～

森京子[†1]

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"[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モニタリング組織に関して、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、行動規範の承認プロセスにおける一貫性を確保することである。

GDPR における行動規範制度は、GDPR の適正な適用に貢献する行動規範という自主ルールの作成を、欧州委員会等が奨励する制度である。行動規範は、所轄監督機関が承認を行う（GDPR 第 40 条(5)）。一方、行動規範の遵守状況に対するモニタリングは、所轄監督機関による認定を受けた組織（Monitoring Body）に委任される。本ガイドラインを分析すると、所轄監督機関等の承認が得られるのであれば、行動規範のモニタリング方法には様々な手段があり得ることが示されている。

本稿では、行動規範のモニタリングに関する解釈を示している本ガイドライン第 11 章、第 12 章、及び第 14 章を概観する。さらに、各加盟国におけるモニタリング組織の認定要件及び欧州における議論を紹介する。これらを踏まえて、GDPR の行動規範制度におけるモニタリング方法を、特定の場面における適正な個人データの取扱いを検討するという観点で分析する。

キーワード：行動規範，プライバシー，個人情報保護，共同規制

A Consideration of Monitoring Codes of Conduct
Analysis of the Guidelines on Codes of Conduct and Monitoring Bodies under Regulation Ⅲ

KYOKO MORI[†1]

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.

Codes of Conduct system under the GDPR is a system whereby the European Commission and others encourage the creation of voluntary rules called codes of conduct that contribute to the proper application of the GDPR. The code of conduct is approved by the competent supervisory authority (Article 40(5) of the GDPR). On the other hand, monitoring of compliance with the Code of Conduct is delegated to a body accredited by the competent supervisory authority (Monitoring Body). An analysis of the Guidelines indicates that there are various possible methods for monitoring codes of conduct, provided that they are approved by the competent supervisory authority, etc.

In this paper reviews Chapters 11, 12, and 14 of these Guidelines, which provide an interpretation of the monitoring of codes of conduct. Furthermore, the requirements for accreditation of monitoring organizations in each member state and the discussions in Europe will be presented. Based on these, the monitoring methods in the GDPR's Codes of Conduct system will be analyzed from the perspective of examining the proper handling of personal data in specific situations.

Keywords: Codes of conduct, Privacy, Data protection, Co-regulation,

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モニタリング組織に関して、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、行動規範の承認プロセスにおける一貫性を確保することである。

GDPR における行動規範制度は、GDPR の適正な適用に貢献する行動規範という自主ルールの作成を、欧州委員会等が奨励する制度である。行動規範は、所轄監督機関が承認を行う（GDPR 第 40 条(5)）。一方、行動規範の遵守状況に対するモニタリングは、所轄監督機関による認定を受けた組織（Monitoring Body）に委任される。そして、GDPR 第 40 条(4)では、「行動規範を適用している管理者又は処理者によるその行動規範の条項遵守を強制的にモニタリングできるようにする仕組みを含めなければならない」と規定さ

†1 (株)KDDI 総合研究所
KDDI Research, Inc.
一橋大学大学院法学研究科ビジネスロー専攻修士課程に在学中である。

れている。さらに、本ガイドライン第 11 章では、「モニタリングの手続きは、当該行動規範が適用対象としているデータ処理によって生じるリスク、寄せられた苦情や特定のインシデント、及び行動規範を遵守する管理者及び処理者の数等の要素を考慮するのであれば、様々な方法で設計できる」と示されている。このように、所轄監督機関等の承認が得られるのであれば、行動規範のモニタリング方法には様々な手段があり得る。

実際に承認された行動規範には、オンライン広告や製薬分野のもの等がある。クラウド分野においては、適用範囲を処理者に限定した 2 つの行動規範が、2021 年 5 月に同時に EDPB の承認意見を得た[2]。

我が国のクラウドサービスにおける個人情報保護法上の論点には、クラウドサービスの利用はどのような場合に個人データの「提供」に該当するかというものがある。この点について個人情報の保護に関する法律についてのガイドライン」 に関するＱ＆Ａ7-53 では、「クラウドサービスを提供する事業者において個人データを取り扱うこととなっているのかどうか」が判断基準とされている。この判断基準については、「処理契約に定めるべき事項を法律レベルでより明確に規定し、クラウド事業者に遵守を義務付ける、といった手法」[3]が提案されている。このような、分野ごとの課題に対する具体的な手法を、事業者側がまとめ、民間組織がモニタリングを行う制度が GDPR における行動規範制度である。クラウド分野の行動規範において、どのようなモニタリング手法が提案されているか、モニタリング組織はどのように認定されるかを検討することは、この問題に対して一定の示唆を与えうる。この他の分野においても、特定の場面における適正な個人データの取扱いを検討する上で、GDPR にモニタリング組織の認定基準や、各行動規範のモニタリング方法は参考になりうる。

本稿では、行動規範のモニタリングに関する解釈を示している本ガイドライン第 11 章、第 12 章、及び第 14 章を概観する。さらに、各加盟国におけるモニタリング組織の認定要件及び欧州における議論を紹介する。これらを踏まえて、GDPR の行動規範制度におけるモニタリング方法を、特定の場面における適正な個人データの取扱いを検討するという観点で分析する。

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。また、本稿における用語の定義は、ガイドラインに準じており、詳細は第 1 章から第 3 章の分析[4]で記載している。

2. 行動規範のモニタリング組織

本ガイドライン第 11 章では、モニタリング組織を所轄監督機関が認定するプロセスを概説している。要点は以下の 5 つである。

- 行動規範が承認されるためには、行動規範の中で、モニタリング組織を特定し、当該モニタリング組織が行動規範をモニタリングする能力があることを所轄監督機関が認定しなければならない。
- GDPR 第 63 条に基づき、所轄監督機関によるモニタリング組織の認定は、所轄監督機関が欧州委員会に対して認定要件案を提出し、承認を得た要件に基づいて行われる。
- 行動規範所有者は、所轄監督機関によるモニタリング組織の認定を受けるために、提案したモニタリング組織が、GDPR 第 41 条(2)に定められた要件を満たしていることを説明・実証する必要がある。
- GDPR 第 41 条は、モニタリング組織の要件に柔軟性を持たせているが、本ガイドライン第 12 章で 8 つの要件として概説している第 41 条(2)の認定要件を満たさなければならない。

本ガイドライン第 12 章では、GDPR 第 41 条(2)をもとに、以下の 8 つの認定要件を概説している。

2.1 独立性

本ガイドライン第 12 章で概説される 8 つの認定要件のうち、一つ目は独立性である。ガイドラインでの説明のうち、要点は以下の 4 点である。

- 行動規範所有者は、行動規範が適用される業界に対して公平にモニタリングを行うことができるよう、モニタリング組織が当該業界から適切に独立していることを証明しなければならない。
- モニタリング組織は、行動規範所有者である業界団体等の内部組織でも外部組織でもよく、状況に応じて適切に提案することができる。
- 内部組織をモニタリング組織として提案する場合、行動規範所有者は、公平性・独立性を保つためのリスク管理方法を説明することになるだろう。例えば、行動規範所有者（業界団体等）から、スタッフ及び経営陣並びにアカウンタビリティ及び機能を分離しなければならない。これらを達成する方法としては、行動規範所有者（業界団体等）とモニタリング組織の報告管理体制を分ける等が挙げられる。
- モニタリング組織は、データ保護責任者（DPO）と同様に、指示を受けずに独立して行動することができ、任務遂行の結果として生じうる、あらゆる種類の制裁又は干渉から保護されなければならない。
- モニタリング組織は、行動規範の起草に参加した外部の弁護士やその他の当事者に関して、独立性又は利益相反のリスクを十分に特定し、当該リスクを軽減するための適切な保護措置を示し、当該メカニズムの適切性を証明しなければならない。
- 特にモニタリング組織が行動規範所有者（業界団体等）の内部にある場合、予算やその他の資源管理が完全に自律していることも、独立性を示す一つの要素である。

2.2 利益相反の不存在

本ガイドライン第 12 章で概説される 8 つの認定要件のうち 2 つ目は利益相反性である。行動規範所有者は、モニタリング組織の任務遂行が、利益相反に繋がらないことを証明しなければならない。

2.3 専門性

本ガイドライン第 12 章で概説されている 8 つの認定要件の 3 つ目として、行動規範所有者は、モニタリング組織がその役割を効果的に遂行するために必要なレベルの専門知識を有していることを証明しなければならない。要点は以下の 2 点である。

- データ保護法及び特定の業界や処理活動に関する、モニタリング組織の知識・経験を説明する書類を提出しなければならない。
- モニタリング組織のスタッフは、適切な業務経験があり、訓練を受けている必要がある。

2.4 手続きとガバナンス構造の確立

本ガイドライン第 12 章で概説されている 8 つの認定要件の 4 つ目は、適切なガバナンス構造と手続きの確立である。これは、管理者及び処理者が行動規範を遵守する資格があるかを評価し、その遵守をモニタリングし、行動規範の運用方法について見直しを行うといった対応をモニタリング組織が適切に行うために必要な認定要件である。要点は以下の 3 つである。

- 行動規範の遵守を積極的かつ効果的にモニタリングするための手続きとガバナンス構造として、以下の方法が挙げられる。
  - 無作為又は抜打ちの監査
  - 年次検査
  - 定期的な報告
  - アンケート
  - 定期報告結果や監査報告書の公表
- モニタリングの手続きは、当該行動規範が適用対象としているデータ処理によって生じるリスク、寄せられた苦情や特定のインシデント、及び行動規範を遵守する管理者及び処理者の数等の要素を考慮するのであれば、様々な方法で設計できる。
- 行動規範所有者は、モニタリング組織が適切な方法で任務を遂行するために十分な資源と人員を有していることを証明しなければならない。行動規範を遵守する管理者又は処理者の数及び規模、並びに関連するデータ処理の複雑さ及びリスクの程度に応じたものでなければならない。

2.5 苦情処理の透明性

本ガイドライン第 12 章で概説されている 8 つの認定要件の 5 つ目は、苦情処理の透明性である。要点は以下の 4 つである。

- モニタリング組織は、公平で透明性のある方法で苦情処理を行うことができる効果的な手続きとガバナンスを確立しなければならない。そのためには、一般に公開された苦情処理プロセス、苦情を処理するための十分なリソース、モニタリング組織が行う決定の一般公開を保証すること、が必要である。具体的な方法としては、苦情受付から解決までのプロセスを、行動規範を説明するガイダンスなどに記載するといった方法で、一般に公開することが挙げられる。
- 管理者又は処理者が行動規範の条項に反する行為を行った場合に、行動規範の停止又は除外権限をモニタリング組織に与える等の方法により、行動規範の遵守を確保するための効果的な手続きを確立させなければならない。
- 行動規範の条項に違反した場合、モニタリング組織は直ちに適切な措置を講じる義務がある。これらの措置は、特に重大な違反があった場合、モニタリング組織によって公表されることがある。
- モニタリング組織は必要に応じて、行動規範を遵守する管理者又は処理者、行動規範所有者、所轄監督機関、及び全ての関係監督機関に、講じた措置及びその正当性について、過度の遅延なく通知することができなければならない。さらに、国境を越えた行動規範（Trancenational code）である場合には、管理者又は処理者の主監督機関（GDPR 第 56 条）が特定できる場合には、主監督機関にも通知しなければならない。

2.6 所轄監督機関との連絡

本ガイドライン第 12 章で概説されている 8 つの認定要件の 6 つ目として、所轄監督機関との連絡について以下の 2 点が求められる。

- モニタリング組織は、行動規範に関してモニタリング組織が実施した対応を、所轄監督機関や他の監督機関に効果的に連絡できなければならない。例えば、行動規範に違反した場合の措置に関する決定、定期的な報告書の提供、又は監査結果等の提供などが挙げられる。
- 所轄監督機関の通知や合意なしに、行動規範を遵守する管理者又は処理者が一方的にモニタリング組織を承認・撤回・停止できる行動規範は、GDPR 第 41 条(5)に違反する。

2.7 行動規範の見直し

本ガイドライン第 12 章で概説されている 8 つの認定要件の 7 つ目として、行動規範を見直す仕組みが必要である。

- 法律の適用や解釈に変更があった場合や、当該行動規範が適用対象とするデータ処理又は行動規範の内容に影響を与える可能性のある新たな技術開発があった場合に、それらに対応するための見直しを行う仕組みを設ける必要がある。

2.8 適法な地位

本ガイドライン第 12 章で概説されている 8 つの認定要

件の 8 つ目として、モニタリング組織は、適法な地位を有していなければならない。

- モニタリング組織及び関連するガバナンス構造において、モニタリング組織が第 41 条第 4 項に基づく役割を遂行するために適切な地位を有し、GDPR の第 83 条第 4 項（c）に基づく罰金を課すことができることを、行動規範所有者が証明できる方法で策定する必要がある。

3. モニタリング組織の取消し

第 14 章ではモニタリング組織の認定取消しを説明している。モニタリング組織が GDPR を遵守していない場合、所轄監督機関は、第 41 条(5)に基づき、モニタリング組織の認定を取消す権限を有する。要点は以下の 2 つである。

- 行動規範所有者は、モニタリング組織の認定が取り消される場合を想定して、行動規範案を作成する必要がある。
- 当該行動規範において認定を受けたモニタリング組織が一つしかない場合、行動規範を遵守する管理者又は処理者の評判や事業利益に悪影響を及ぼし、データ主体やその他の利害関係者からの信頼を低下させる可能性がある。
- 状況が許す限り、認定の取消しは、所轄監督機関がモニタリング組織に対して、適切な改善を行う機会を与えたり、応急的な対応を行ったりした後にのみ行われるべきである。
- モニタリング組織を取消す決定は、全ての関係監督機関及び欧州委員会に通知されなければならない（GDPR 第 40 条(11)）。

4. 各加盟国における認定要件の例

本稿第 3 章で説明したとおり、GDPR 第 41 条は、モニタリング組織の認定要件に柔軟性を持たせており、所轄監督機関によるモニタリング組織の認定は、所轄監督機関が欧州委員会に対して認定要件案を提出し、承認を得た要件に基づいて行われる。

各加盟国が欧州委員会の承認を得た認定要件は、基本的に本ガイドラインの内容に沿っているが、加盟国独自の要件を追加している場合もある。

例えばフランスの認定要件では、本ガイドライン第 11 章において 3 つ目の認定要件として示されている「専門性」要件について、「専門性が一人の個人に集中していない」[5]ことを追加している。また、ベルギーの認定要件では、本ガイドラインで 5 つ目の認定要件として示されている「苦情処理の透明性」について、「苦情の解決が遅延した場合に、その理由を苦情の受領後 3 か月以内に苦情申立者に通知するものとする」[6]という内容を追加している。

5. 欧州における議論

欧州においては、「個人データを処理する組織の数とその処理能力が増加」[7]する中で、「監督当局が管轄内のあらゆるデータ処理業務をモニタリングし、必要な場合には法律を執行するには、リソースが不足している」[7]と指摘されている。

また、クラウド分野の業界団体が作成した 2 つの行動規範を比較した論文では、行動規範の「モニタリングとエンフォースメントが実際にどのように行われるかは、行動規範の将来の成功を左右する」[8]とも指摘されている。

6. まとめと今後の課題

本稿では、行動規範のモニタリングに関する解釈を示している本ガイドライン第 11 章、第 12 章、及び第 14 章の分析を行い、各加盟国におけるモニタリング組織の認定要件及び欧州における議論を紹介した。

GDPR 第 40 条(4)では、行動規範には、「行動規範を適用している管理者又は処理者によるその行動規範の条項遵守を強制的に監視できるようにする仕組みを含めなければならない。」と規定されている。そして、本ガイドライン第 11 章では、モニタリング組織認定要件の 4 つ目である「適切なガバナンス構造と手続き」の項目において、「モニタリングの手続きは、当該行動規範が適用対象としているデータ処理によって生じるリスク、寄せられた苦情や特定のインシデント、及び行動規範を遵守する管理者及び処理者の数等の要素を考慮するのであれば、様々な方法で設計できる」と示されている。

このように、所轄監督機関等の承認が得られるのであれば、行動規範のモニタリング方法には様々な手段があり得る。さらに、本稿第 3 章で説明したように、所轄監督機関が行うモニタリング組織の認定は、各加盟国によって異なる。例えばフランスとベルギーを比較しても、本ガイドライン以外の要件を独自に追加している。

欧州においては、個人データの処理が増大する中で、監督当局のみでモニタリングを行うにはリソースが不足していることが指摘されている。また、モニタリングが実際にどのように行われるかが、GDPR の行動規範制度の中で重要な点であると言われている。

今後も個人データ処理の増大が予想される中でモニタリングのためのリソースが限られるという課題に対して、GDPR の行動規範制度のように民間組織に一定程度委ねる方法は、我が国の議論においても参考になり得る。また、特定の場面における個人データの適正な取扱いを、行動規範制度や実際の行動規範を参考に検討することで、我が国に一定の示唆を与えうる。

今後の課題としては、実際に承認手続きが完了した行動

規範を対象として、モニタリングが実際にどのように行われているかについて追加の調査を行う。

引用参考文献

[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] The European Data Protection Board, “Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the “EU Data Protection Code of Conduct for Cloud Service Providers” submitted by Scope Europe”〈https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf〉(参照 2023-1-22).

[3] 岡田淳ほか，個人情報保護をめぐる実務対応の最前線 第 3 回 個人データの第三者提供と共同利用をめぐる論点(1),」NBL1208 号 p.48，p.50（2021）.

[4] 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.

[5] Autorité de protection des donneés, Décision relative aux critères d’accréditation des organismes de supervision chargés de contrôler le respect des codes de conduite,24 septembre 2020〈https://www.autoriteprotectiondonnees.be/publications/decision-nr.-01-2020-of-24-09-2020.pdf〉（参照 2023-1-22）.

[6] CNIL，Deliberation no. 2020-050 of 30 April 2020 on the adoption of the requirements for accreditation of monitoring bodies in charge of the monitoring of compliance with a code of conduct，〈https://edpb.europa.eu/system/files/2021-03/requirements-for-accreditation-of-monitoring-bodies.pdf〉(参照 2023-1-22).

[7] Irene Kamara，Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardization 'mandate', European Journal of Law and Technology, Vol 8, No 1, 2017.〈https://www.ejlt.org/index.php/ejlt/article/view/545/723〉(参照 2023-1-23).

[8] Carl Vander Maelen，GDPR codes of conduct and their (extra)territorial features: a tale of two systems，International Data Privacy Law, Volume 12, Issue 4, November 2022, p.313,〈https://academic.oup.com/idpl/article-abstract/12/4/297/6808916?utm_source=advanceaccess〉(参照 2023-1-22).