プライバシーに関する国際標準化動向及び EDPB ガイドライン

目次

1. ISO/IEC JTC 1/SC 27 WG5 におけるプライバシー関連の国際標準化動向

ISO/IEC JTC 1/SC 27 WG5（アイデンティティ管理とプライバシー技術）では、アイデンティティ管理、プライバシー、バイオメトリクスの標準化を行っている。2019 年度の主な活動は、以下の通りである。

1.1. アイデンティティ管理　ISO/IEC 29115 について

エンティティ（実体）に関する属性の集合（アイデンティティ）と、そのアクセス権限情報のライフサイクル管理を行うことをアイデンティティ管理という。

2013 年 4 月に発行されたユーザー認証についてのフレームワーク規格である ISO/IEC 29115 （Entity authentication assurance framework）について、アイデンティティ管理全般についての規格である ISO/IEC 24760（A framework for identity management）との整合性を確保したり、多要素認証等の技術動向に合わせたりする改訂作業が進められている。

1.2. プライバシー ISO/IEC 27701 について

2019 年 8 月、ISO/IEC 27701「セキュリティ技術－プライバシー情報マネジメントのための ISO/IEC 27701 及び ISO/IEC 27002 への拡張－要求事項及び指針（Extension to ISO/IEC 27701 and ISO/IEC 27002 for privacy information management）」を発行した。これは、情報セキュリティマネジメントシステム（ISMS）要求事項であり、ISMS 認証基準である ISO/IEC 27001 と、情報セキュリティ管理策の実践のための規範である ISO/IEC 27002 のセキュリティ対策を PII（個人識別可能情報）の保護へと拡張した PIMS（Privacy Information Management System）の規格である。

ISO/IEC 27701 の構成は、図表 1 の通りである。

図表 1　ISO/IEC 27701 規格の構成

1 適用範囲
2 引用規格
3 用語、定義及び略語
4 一般
5 ISO/IEC 27001 に関連する PIMS 固有の要求事項
6 ISO/IEC 27002 に関連する PIMS 固有の手引
7 PII 管理者のための ISO/IEC 27002 の追加の手引
8 PII 処理者のための ISO/IEC 27002 の追加の手引
附属書 A（規定）PIMS 固有の管理目的及び管理策（PII 管理者）
附属書 B（規定）PIMS 固有の管理目的及び管理策（PII 処理者）
附属書 C（参考）ISO/IEC 29100 への対応付け
附属書 D（参考）一般データ保護規則（GDPR）への対応付け
附属書 E（参考）ISO/IEC 27018 及び ISO/IEC 29151 への対応付け
附属書 F（参考）ISO/IEC 27701 を ISO/IEC 27001 及び ISO/IEC 27002 に適用する方法

ISO/IEC 27001 に対して ISO/IEC 27701 が追加の要求事項を規定しているのは、「4. Context of the organization（組織の状況）」と、「6. Planning（計画）」についてであるが、ISO/IEC 27002 に対しては「17. Information security aspects of business continuity management（事業継続マネジメントにおける情報セキュリティの側面）」を除く「5. Information security policies（情報セキュリティのための方針群）」から「18. Compliance（順守）」まですべての箇条に追加の手引が規定されている。

図表 2　ISO/IEC 27002 に関連する PIMS 固有の手引

ISO/IEC 27002 の箇条	27701 の細分箇条
5　情報セキュリティのための方針群	6.2　追加の手引あり
6　情報セキュリティのための組織	6.3　追加の手引あり
7　人的資源のセキュリティ	6.4　追加の手引あり
8　資産の管理	6.5　追加の手引あり
9　アクセス制御	6.6　追加の手引あり
10　暗号	6.7　追加の手引あり
11　物理的及び環境的セキュリティ	6.8　追加の手引あり
12　運用のセキュリティ	6.9　追加の手引あり
13　通信のセキュリティ	6.10　追加の手引あり
14　システムの取得，開発及び保守	6.11　追加の手引あり
15　供給者関係	6.12　追加の手引あり
16　情報セキュリティインシデント管理	6.13　追加の手引あり
17　事業継続マネジメントにおける情報セキュリティの側面	6.14　PIMS 固有の手引なし
18　順守	6.15　追加の手引あり

ISO/IEC 27701 の箇条 7 は PII 管理者のための、箇条 8 は PII 処理者のための ISO/IEC 27002 の追加の手引となっており、「収集及び処理の条件」「PII 主体に対する義務」「プライバシー・バイ・デザイン及びプライバシー・バイ・デフォルト」「PII の共有、移転及び開示」に関する管理策と実施の手引を定めている。

ISO/IEC 27701 は、「5.2.1　組織及びその状況の理解」で「組織は、自らの役割を、PII 管理者（共同 PII 管理者を含む）及び／又は PII 処理者として決定しなければならない。」、「7.2.4 同意の取得及び記録の実施の手引」で、「同意は、PII 主体の自由意思により、明示的であることが望ましい」と規定していることや、図 3 に示すように GDPR 対応表が附属書 D として付いていることからも、GDPR に対応しなければならない企業にとっては参考になる規格であると思われる。

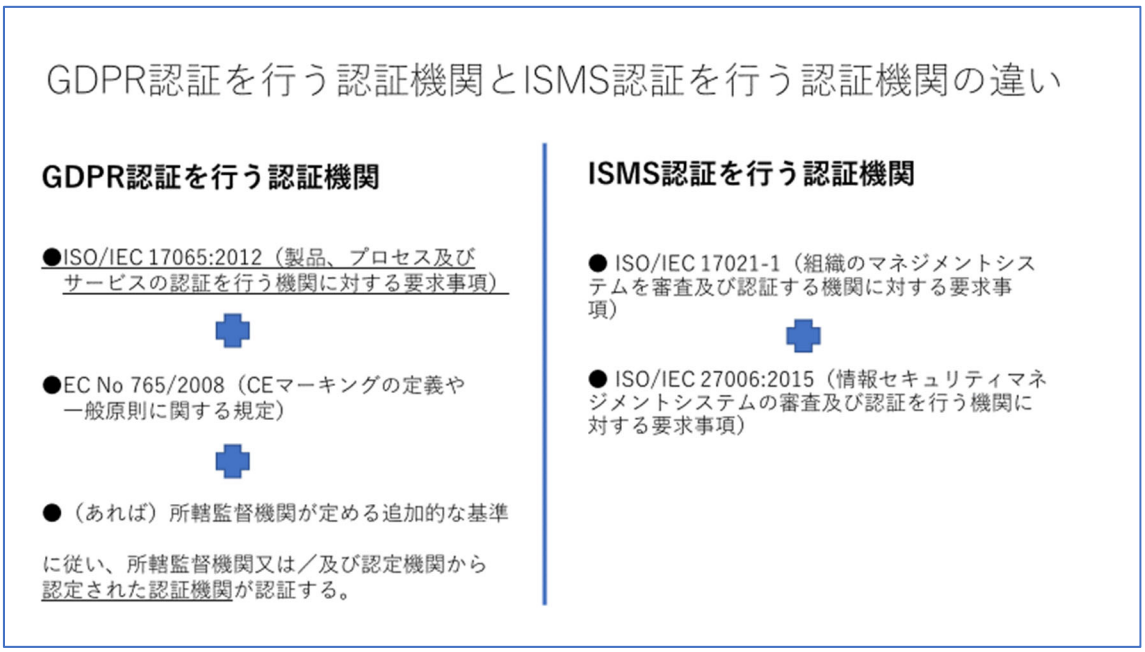
図表 3　ISO/IEC 27701 附属書 D GDPR の条文と ISO/IEC 27701 の箇条の対応表

Subclause of this document	GDPR article
5.2.1	(24)(3), (25)(3), (28)(5), (28)(6), (28)(10), (32)(3), (40)(1), (40)(2)(a), (40)(2)(b), (40)(2)(c), (40)(2)(d), (40)(2)(e), (40)(2)(f), (40)(2)(g), (40)(2)(h), (40)(2)(i), (40)(2)(j), (40)(2)(k), (40)(3), (40)(4), (40)(5), (40)(6), (40)(7), (40)(8), (40)(9), (40)(10), (40)(11), (41)(1), (41)(2)(a), (41)(2)(b), (41)(2)(c), (41)(2)(d), (41)(3), (41)(4), (41)(5), (41)(6), (42)(1), (42)(2), (42)(3), (42)(4), (42)(5), (42)(6), (42)(7), (42)(8)
5.2.2	(31), (35)(9), (36)(1), (36)(2), (36)(3)(a), (36)(3)(b), (36)(3)(c), (36)(3)(d), (36)(3)(e), (36)(3)(f), (36)(5)
5.2.3	(32)(2)
5.2.4	(32)(2)
5.4.1.2	(32)(1)(b), (32)(2)
5.4.1.3	(32)(1)(b), (32)(2)
6.2.1.1	(24)(2)
6.3.1.1	(27)(1), (27)(2)(a), (27)(2)(b), (27)(3), (27)(4), (27)(5), (37)(1)(a), (37)(1)(b), (37)(1)(c), (37)(2), (37)(3), (37)(4), (37)(5), (37)(6), (37)(7), (38)(1), (38)(2), (38)(3), (38)(4), (38)(5), (38)(6), (39)(1)(a), (39)(1)(b), (39)(1)(c), (39)(1)(d), (39)(1)(e), (39)(2)
6.3.2.1	(5)(1)(f)

しかし、現時点で「ISO/IEC 27701 は、GDPR 認証規格である。」ということはできない。なぜなら、GDPR 第 43 条(1)(b)によると、GDPR 認証は、ISO/IEC 17065 という「製品、プロセス及びサービスの認証を行う機関に対する要求事項」を満たす認証機関が行うとしている[1]。他方、ISO/IEC 27701 は ISO/IEC 27001, ISO/IEC 27002 の拡張であるマネジメントシステム規格である。ISMS 認証を行う認証機関はマネジメントシステムの審査及び認証を行う機関に対する要求事項である ISO/IEC 17021、さらに情報セキュリティマネジメントシステムの審査及び認証を行う認証機関に対する要求事項である ISO/IEC 27006 を満たさなければならない。

[1] https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf

図表 4　GDPR 認証を行う機関と ISMS 認証を行う認証機関の違い



英国認証機関認定審議会（UKAS）[2]においても、

"Please note that accredited certification for the GDPR must be based on accreditation to ISO 17065 using a certification scheme approved by the Information Commissioners Office (see GDPR, Art 42 and 43). Accredited certification of a management system for ISO 27701 under ISO 17021-1 would not meet these criteria."[3]

「GDPR の認定認証は、情報コミッショナーオフィスによって承認された認証制度を使用した ISO 17065 への認定に基づく必要があることに注意してください（GDPR、第 42 条及び第 43 条参照)。 ISO 17021-1 に基づく ISO 27701 のマネジメントシステムの認定認証は、この基準に適合しないであろう」

としており、27701 認証は GDPR 認証ではないという立場を今のところとっている。

しかし、ISO/IEC 27001 に基づき ISO/IEC 27701 に準拠することは、GDPR が組織に求める個人データの組織上・技術上の保護が可能になるとされている。フランスの CNIL も ISO/IEC 27701 は GDPR も考慮に入れた国際規格であるとしてその重要性についてリリースする[4]など高い関心が寄せられている。

---

[2] https://www.ukas.com/

[3] https://www.ukas.com/news/call-for-expressions-of-interest-iso-27701-2019-security-techniques/

[4] https://www.cnil.fr/en/iso-27701-international-standard-addressing-personal-data-protection

1.3.　プライバシー　ISO/IEC 29184 について

2014 年 10 月に経済産業省が公表した「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」（以下、経産ガイドライン）をベースに日本が国際規格案を提案した ISO/IEC 29184 （Information technology – Online privacy notices and consent：情報技術－オンラインのプライバシーに関する通知と同意）が 2020 年 6 月に発行された。

経産ガイドラインは、日本企業がグローバルな競争環境においても消費者との信頼関係を基礎にしてパーソナルデータを利活用したサービスが提供できるよう、諸外国における消費者の意思確認手続の実施状況や検討状況も調査して作成されており、EU や韓国などを含む 10 か国、地域、組織の通知と同意・選択に係る取り組みにも考慮し、ISO/IEC 29100 (Privacy framework）の 11 のプライバシー原則のうちの 2 つの原則（第 1 原則: 同意と選択、第 7 原則: 公開、透明性及び通知）を踏まえた指針となっている。

図表 5　ISO/IEC 29100 の 11 のプライバシー原則

1　Consent and choice（同意及び選択）
2　Purpose legitimacy and specification （目的の正当性及び明確化）
3　Collection limitation （収集制限）
4　Data minimization（データの最小化）
5　Use, retention and disclosure limitation（利用、保持及び開示の制限）
6　Accuracy and quality（正確性及び品質）
7　Openness, transparency and notice（公開性、透明性、及び通知）
8　Individual participation and access（個人参加及びアクセス）
9　Accountability（アカウンタビリティ）
10　Information security（情報セキュリティ）
11　Privacy compliance（プライバシーコンプライアンス）

ISO/IEC 29184 は、PII 主体に対して、どのような PII を取得しどのように処理するのかわかりやすい情報を具体的に提供した上で同意を取得するという経産ガイドラインと目的を一にしており、上記の ISO/IEC 29100 の 2 原則の指針であることに変わりはないが、ISO/IEC 29115 (Entity Authentication Assurance) 及び ISO/IEC 40500 (W3C Web Content Accessibility Guidelines (WCAG) 2.0）も考慮したものとなっており、視覚的にハンディを抱えた方によるウェブサイトへのアクセシビリティ等への配慮、海外へのデータ越境移転、同意取得のタイミングについての箇条といった、経産ガイドラインにはない規定も盛り込まれている。

1.4. バイオメトリクス

バイオメトリック認証をリモート環境でも使用可能にするためのデータ構造を定義するISO/IEC 24761（Authentication context for biometrics）の改訂が進められ、2019 年 10 月に IS として発行された。2011 年に発行された ISO/IEC 24745（Biometric information protection）は、その後の新技術を反映するための改訂が進み CD 段階にあり、モバイル機器上でのバイオメトリクスを使った認証に対するセキュリティ要件を定める ISO/IEC 27553（Security requirements for authentication using biometrics on mobile devices）は、WD 段階にあり、スマートフォンへのバイオメトリクスの適用が進みつつある中、関心を集めている。

ISO/IEC JTC1/SC27 WG5 のプライバシー関連規格と審議案件は図表 6 の通りである。

図表 6　ISO/IEC JTC1/SC27 WG5 のプライバシー関連規格

プライバシー関連で発行されている規格（発行順）

29100　Privacy framework
29191　Requirements for partially anonymous, partially unlinkable authentication
29101　Privacy architecture framework
27018　Code of practice for PII protection in public clouds acting as PII processors
29190　Privacy capability assessment model
29134　Privacy impact assessment
29151　Code of practice for personally identifiable information protection
20889　Privacy enhancing data de-identification techniques
27701　Extension to 27001 and 27002 for privacy information management
27550　Privacy engineering for system life cycle processes
29184　Guidelines for online privacy notice and consent

プライバシー関連で開発中の規格（発行までのステージの高いもの順）

20547　Big data reference architecture – Part 4: Security and privacy fabric
27551　Requirements for attribute-based unlinkable entity authentication
27570　Privacy guidelines in smart cities
27555　PII deletion concept in organizations
27556　User-centric framework for PII handling based on privacy preferences

2. 2019 年に出された EDPB ガイドラインの概要

各 EU 加盟国の監督当局の代表者及び欧州データ保護監視官局からなる欧州データ保護会議（European Data protection Board：EDPB）は、2019 年に下記のガイドラインを公表している。

2.1. Guidelines 1/2019 on Codes of Conduct and monitoring Bodies under Regulation 2016/679

Guidelines 1/2019 on Codes of Conduct and monitoring Bodies under Regulation 2016/679(規則 2016/679 に基づく行動規範及び監視機関に関するガイドライン)は、GDPR 第 40 条「行動規範」及び第 41 条「承認された行動規範の監視」を適用する際の実用的な指針である。

行動規範とは、認証同様、管理者及び処理者が自身の処理活動に適用される GDPR の義務を遵守していることを証明するツールとなるものであるが、行動規範と認証には、主に図表 4-7 のような違いがある。

図表 7　行動規範と認証の違い

	Codes of conduct 行動規範	Certification 認証
発行	管理者又は処理者を代表する組織又は団体が作成する	認証機関または所轄監督機関が作成する
承認	データ処理活動に関連して、協会または代表機関によって起草、修正、または拡張された行動規範のうち、1 つの加盟国のみに影響を与えるものは、承認を得るために当該所轄監督機関に提出しなければならない。複数の加盟国で活動を処理する場合、EDPB の意見が必要である。	承認は、所管監督機関または EDPB によって承認された基準に基づいて行われる。基準が EDPB によって承認された場合、欧州データ保護シールと呼ばれる共通の認証が得られる場合がある。
有効期限	制限なし	有効期間は最長 3 年であり、更新の必要があり、認証の要件を満たさなくなった場合には認証機関または所管監督機関により取消される場合がある。

本ガイドラインは、行動規範の利点とは、特定の部門及びその処理活動のニュアンスを踏まえた GDPR の適切な適用を実用的かつ公明性が高く、翻って費用対効果の高い方法で実

現するものであると説明しており、行動規範に盛り込む内容として、

・構成及び透明性のある処理
・特定の文脈で管理者が追求する正当な利益
・個人データの収集；個人データの仮名化
・個人に提供される情報及び個人の権利の行使
・こどもに提供される情報及び子どもの保護（親の同意を得るための仕組みを含む）
・データ保護バイデザイン及びバイデフォルトを含む技術的及び組織的な措置
・違反通知
・EU 域外へのデータ移転
・紛争解決手続き

を挙げている。

2.2. Guidelines 2/2019 on the processing on personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects

Guidelines 2/2019 on the processing on personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects（データ主体に対するオンラインサービスの提供に関連する GDPR 第 6 条(1)(b)に基づく個人データの処理に関するガイドライン）は、有料であるかどうかに関わりなく、オンラインサービス契約に関して個人データを処理する際に GDPR 第 6 条(1)(b)を適用するためのガイドラインである。

GDPR 第 6 条「取扱いの適法性」は、「１．取扱いは、以下の少なくとも一つが適用される場合においてのみその範囲内で適法である」とし、(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。」としている。

本ガイドラインでは、「契約の履行のために取扱いが必要」とは、単に契約の条件によって許可されているもの、または契約の条件に書かれているものではなく、「EU 法において独立した意味を持ち、データ保護法の目的を反映しなければならず、プライバシーの基本的権利及び個人データの保護並びに特に公平性の原則の要件を考慮することを含む」としている。

ポイントは、本当にその個人データがなければオンライン契約サービスが履行できないことが客観的に認められることで、例えばデータ主体がオンライン小売業者から商品を購入した場合、配送先として自宅住所を選択した場合には自宅住所の入力は契約履行に必要だが、自宅以外のピックアップポイントを選んだ場合には、GDPR 第 6 条(1)(b)を正当な根拠として自宅住所の入力を求めることはできない、と例示している。

Example 1　A data subject buys items from an online retailer. The data subject wants to pay by credit card and for the products to be delivered to their home address. In order to fulfil the contract, the retailer must process the data subject's credit card information and billing address for payment purposes and the data subject's home address for delivery. Thus, Article 6(1)(b) is applicable as a legal basis for these processing activities.

However, if the customer has opted for shipment to a pick-up point, the processing of the data subject's home address is no longer necessary for the performance of the purchase contract. Any processing of the data subject's address in this context will require a different legal basis than Article 6(1)(b).

例 1 データ主体がオンライン小売業者から商品を購入する。データ主体は、クレジットカードで支払い、自宅住所への配送を希望する。契約を履行するために、小売業者は、データ主体のクレジットカード情報及び請求先、及び配送のために住所情報を処理しなければならない。したがって、GDPR 第 6 条(1)(b)は、これらの処理活動の法的根拠として適用される。しかしながら、顧客がピックアップポイントへの配送を選択した場合、データ主体の自宅住所の処理は、購入契約の履行のために必要ではない。この文脈におけるデータ主体の住所の処理は、第 6 条(1)(b)とは異なる法的根拠を必要とする。

2.3. Guidelines 3/2019 on processing of personal data through video devices – version adopted after public consultation

Guidelines 3/2019 on processing of personal data through video devices – version adopted after public consultation（ビデオ機器を通じた個人データの処理に関するガイドライン）は、ビデオ機器を通じた個人データの処理に関する GDPR の適用方法に関するガイドラインである。

近年の監視カメラの高性能化や普及率の増加、年齢や人種によって認証の性能に差が生じるといった危険性があることも挙げ、防犯目的であれば、私有地を柵で囲む、落書きされにくい壁面素材を使うといったプライバシーへの侵襲性が低い物理的手段の採用も推奨しつつ、

- GDPR が適用されない「私的利用の例外」に該当する録画行為
- 管理者や第三者の正当な利益との比較考量
- ビデオ映像の第三者への開示
- バイオメトリクスデータなど特別な種類のデータの処理
- データ主体の権利（アクセス権、消去権、異議申立ての権利）
- 監視カメラ設置を警告する際の表示内容の具体例
- データ保護バイデザイン、バイデフォルトによるデータ保護の必要性

などについて具体例を交えて記述されている。

> Example: Political options could for example be deduced from images showing identifiable data subjects taking part in an event, engaging in a strike, etc. This would fall under Article 9.
> 例：ある種のイベントに参加したり、ストライキに参加するなど、特定可能なデータ主体を映す画像から政治的意見を導き出すことができる。 これは GDPR 第 9 条に該当するであろう。

2.4. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default

Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (GDPR 第 25 条データ保護バイデザイン及びバイデフォルトに関するガイドライン)は、管理者が個人データの処理を企画・設計する際に考慮しなければならない要素について書かれている。

GDPR 第 25 条は、「1. 技術水準、実装費用、取扱いの性質、範囲、過程及び目的並びに取扱いによって引き起こされる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、管理者は、本規則の要件に適合するものとし、かつ、データ主体の権利を保護するため、取扱いの方法を決定する時点及び取扱いそれ自体の時点の両時点において、データの最小化のようなデータ保護の基本原則を効果的な態様で実装し、その取扱いの中に必要な保護措置を統合するために設計された、仮名化のような、適切な技術的措置及び組織的措置を実装する。」としているが、「適切であること」とは、「有効性」に密接に関連しており、リスクや苦情の低減（定量的)、専門家による評価（定性的）を指標とする重要業績指標（KPI）などを使って有効性を検証することが重要であるとしている。そして技術的又は組織的措置を選択するうえで重要なことは、必ずしも高度な技術的ソリューションの使用を優先することではなく、「最新技術、実装コスト、処理の性質、範囲、文脈及び目的、取扱いによって引き起こされる自然人の権利及び自由に対する様々な蓋然性と深刻さのリスク」を総合的に判断することが必要であるとしている。

そして、取扱い活動の性質、範囲、文脈はデータ処理の過程で変化するため、個人データを保護するために選択した手段の有効性は定期的に見直すことが重要としている。

Example 2: A public transportation company wishes to gather statistical information based on travellers' routes. This is useful for the purposes of making proper choices on changes in public transport schedules and proper routings of the trains. The passengers must pass their ticket through a reader every time they enter or exit a means of transport. Having carried out a risk assessment related to the rights and freedoms of passengers' regarding the collection of passengers' travel routes, the controller establishes that it is possible to identify the passengers based on the ticket identifier. Therefore, since it is not necessary for the purpose of optimizing the public transport schedules and routings of the trains, the controller does not store the ticket identifier. Once the trip is over, the controller only stores the individual travel routes so as to not be able to identify trips connected to a single ticket, but only retains information about separate travel routes.

例 2:　公共交通会社は、乗客の経路に基づいて統計情報を収集したいと考えている。これは、公共交通スケジュールの変更及び列車の適切な経路選択のために有用である。乗客は、輸送手段に出入りするたびに、チケットをリーダーに通さなければならない。管理者は、移動経路の収集に関する乗客の権利及び自由に関するリスクアセスメントを実施した結果、チケット識別子に基づいて乗客を識別することができることがわかった。したがって、列車の公共交通スケジュールや経路を最適化するためには不要であるため、管理者はチケット識別子を保存しない。一旦交通移動が終了すると、管理者は、一つのチケットに結びついた移動を特定することはできず、別個の旅行経路に関する情報のみを保持するように、個々の旅行経路のみを保存する。

In cases where there can be a risk of identifying a person solely by their travel route (this might be the case in remote areas) the controller implements measures to aggregate the travel route, such as cutting the beginning and the end of the route.

移動経路のみで人を特定するリスクがある場合（地方の場合など）、管理者は、経路の出発地と目的地を削除するなど、移動経路を集約するための手段を実装する。

2.5. Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) – version for public consultation

Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1) – version for public consultation（GDPR に基づく検索エンジン事例における忘れられる権利の基準に関するガイドライン）は、2014 年 5 月の欧州司法裁判所（CJEU）の判決以降、データ主体から検索結果の非表示化要求、検索エンジンプロバイダによるリンク削除拒否に関する苦情の数が増加しているため、GDPR 第 17 条(1)に基づき、データ主体が検索エンジンプロバイダに検索結果の非表示化を求める際の根拠にでき

るもの、GDPR 第 17 条(3)により、検索結果の非表示化の要請を検索エンジン事業者が拒否できる場合について記述している。

GDPR 第 17 条(1)は、以下の場合にはデータ主体は自身に関する個人データを消去させる権利があり、データ管理者は消去する義務を負うという一般原則を示している。

- 個人データは、収集又はその他の処理の目的に関連してもはや不要である（第 17 条(1)(a)）。
- データ主体が処理の根拠となる同意を撤回した（第 17 条(1)(b)）。
- データ主体が、GDPR 第 21 条(1),(2)によって処理に異議を申立てた（第 17 条(1)(c)）。
- 個人データが違法に処理された（第 17 条(1)(d)）。
- 管理者が順守すべき EU 又は加盟国の法的義務によってデータを抹消しなければならない（第 17 条(1)(e)）。
- 個人データが、未成年者に対する情報社会サービスの提供に関連して収集されている（第 17 条(1)(f)）。

本ガイドラインは第 17 条(1)(f)について以下のように説明している。
「GDPR は ISS を定義しておらず、EU の既存の法の定義を参照している。2000 年 6 月 8 日の欧州議会及び理事会指令 2000/31/CE の前文 18[5]は「情報社会サービスの直接的な提供」の概念を広範かつ曖昧に定義しているため、解釈がやや難しい。主に、これらのサービスは「オンラインで行われる広範な経済活動に及ぶ」とされているが、「オンライン契約を生み出すサービス」に限定されず、経済活動である限り、オンライン情報や商業通信を提供するサービス、データのサーチ、アクセス、検索を可能にするツールを提供するサービスなど、それらを受け取る者から報酬を受けないサービスにも及ぶ」と規定されていることから、検索エンジンプロバイダの活動が ISS の直接的な提供に当てはまる可能性が高いようである。（中略）GDPR 第 17 条(1)(f)の適用も元々の管理者による個人データの収集の文脈に依存することを考慮に入れて、子どもに関するコンテンツを非表示化しなければならない。」としている。

[5] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32000L0031

3. ePrivacy 規則案の概要

2002 年に発効した e プライバシー指令に置き換わるものとして欧州委員会から 2017 年 1 月 10 日に公表された ePrivacy 規則案は、数度の改正を重ねているが、2020 年 5 月現在、まだ可決されていない。

e プライバシー指令は、テレコムサービスや ISP 等の電気通信事業者が対象であったが、ePrivacy 規則案では、これらの事業者に加えて

① OTT (Over The Top)サービスといわれる、メッセンジャー、クラウドメール、VoIP 等のサービスを行う事業者

② EU 域内に存在するエンドユーザーの端末の情報を扱う場合に適用されることから② Web サービスやスマートフォン・アプリケーション等を提供する事業者の大半も対象となる。

2020 年 2 月に欧州連合理事会議長国が公表した最新の規則案[6]のポイントは、事業者が「正当な利益」のために(1)電子通信メタデータを処理する (2)エンドユーザーの端末にクッキー又は類似の技術を設定する際には、特に以下のような条件を満たすこととしている。

- データ保護影響評価を行うこと、そして適宜、関連所管当局と協議すること
- 適切なセキュリティ対策を講じること
- データ処理活動についてエンドユーザーに情報提供すること
- データ処理に対する異議申し立て権をエンドユーザーに与えること
- メタデータ、あるいはクッキー又は類似の技術によって収集した情報を匿名化していない場合には第三者と共有してはならない。

しかしながら、エンドユーザーのプロファイリングや性質・特性を判断するためにクッキーや同様の技術によってメタデータや情報を収集することがエンドユーザーの利益に勝る「正当な利益」とみなされる可能性は低く、エンドユーザーが子どもである場合や、収集される情報が機微情報である場合には特に難しいという意見もあり[7]、現在の ePrivacy 規則案にも依然議論の余地がありそうである。

---

[6] https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2020/02/CONSIL_ST_5979_2020_INIT_EN_TXT.pdf

[7] https://www.huntonprivacyblog.com/2020/02/27/eu-council-presidency-releases-proposed-amendments-to-draft-eprivacy-regulation/