エストニアにおける個人情報保護と公的データの利用
-- データは誰のものなのか？ --

エストニアの電子政府やeヘルスに関する講演等で、よくある質問の一つとして「エストニアでは、データは誰のものなのか？」というのがある。例えば、「エストニアでは、医療データは誰のものなのか？」とか、「データの所有権は誰にあるのか？」といった質問である。

この場合、「データは所有権という考え方に馴染まないものである[1]」とした上で、「（健康情報システム等の）公的データベースは政府が法令で統制（control）している」が、その一方で「個人（患者）にはデータ主体として法令で定められた権利が認められている」と説明している。

より重要なのは、「公的データベースには法令で定められた目的があり、その目的のために利用される」ということだ。つまり、「その医療データベースは、誰のために何のためにあるのか？」が良い質問ということになる。

従って、法令で定める目的によっては、個人データであっても、本人の同意なしに公開されることがある。例えば、「医療従事者と活動資格の全国登録簿[2]」では、医師や看護師の登録番号、氏名、専門分野、勤務先などを公開している。このデータベースの目的の一つとして「国民の保護」があり、その目的を達成する上で最低限必要と考えられる個人情報を、法令に従って公開しているのだ。

しかし、上記のように厳格な解釈をしない場合、データ主体の権利を誇張する形で「データの所有者（owner）は市民自身である[3]」と説明されることもあるので注意したい。

エストニアの公的データベースの歴史

エストニアの公的データベースとデータの権利義務関係について理解するためには、その歴史を紐解く必要がある。

エストニアでは、1996年の欧州データベース指令（96/9/EC）[4]による、いわゆる「データベース権」の確立を踏まえて、1997年にデータベース法[5]が制定された。欧州データベース指令は、データベースの著作権保護について定めるもので、一般に公開されるデータベースの利用者の権利と義務なども定めている。

---

[1] 経済産業省のIoT推進コンソーシアム「データの利用権限に関する契約ガイドライン（平成29年5月 ver1.0）」では、「データは無体物であって民法上の所有権の対象ではない」と説明している。
https://www.meti.go.jp/policy/mono_info_service/connected_industries/sharing_and_utilization/20170530003-1.pdf

[2] 医療従事者とライセンスの全国登録簿 https://www.tervishoiuamet.ee/index_page_176.html

[3] I spy with my little eye…privacy! https://e-estonia.com/i-spy-with-my-little-eyeprivacy/

[4] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009

[5] Andmekogude seadus https://www.riigiteataja.ee/akt/32230

同指令を受けて制定されたエストニアのデータベース法は、データの収集や処理など、官民のデータベースの管理について共通ルールを定めるもので、データベースを次のように定義している（第2条）。

『本法の意味におけるデータベースとは、国、地方自治体、公共または民間団体によって維持される組織化されたデータのセットであり、自動化されたデータ処理を使用して維持されるか、手動で維持される。データベースは、簡単にアクセスできるように、または機械的処理ができるように組織化された形式で維持される。』

データベースの所有者については、第4条で定めており、所有者（omanik）は、個人、公人、国または地方自治体がなり得るとしている。エストニア語の「omanik」は、英語の「owner」に該当するもので、財産法上の所有権（omandioigus）ともリンクしている。

同法では、データベースの所有者が、データベースの最終責任者である「責任処理者」とされるが、これは現在の欧州一般データ保護規則（GDPR）[6]における「データコントローラー」に該当する。責任処理者によって「承認された処理者」が、責任処理者の命令に従って実際のデータベースの管理・運営を行うことになる（第5条）。この「承認された処理者」は、GDPRの「データプロセッサー」に該当する。

国および地方自治体は、この法律に規定された方法でデータベースを構築するとされ（第5条）、共和国政府および地方政府のデータベース、ならびに個人が保有する機微な個人データを含むデータベースの国家登録簿を、「国家データベース登録簿」という名称で制定するものとした（第16条）。

このように、エストニアのデジタル国家で最も重要な「データガバナンス」は、この1997年に成立したデータベース法によって確立したと言える。同法では、「データベースの所有者が誰なのか」を明らかにすることで、データベースの「責任処理者」が決まるという構成になっている。

その後、2000年に公共情報法[7]（情報公開法）と人口登録法（住民登録法）が制定されたことで、公的データベースの位置づけが、より明確になっていく。公共情報法では、公的情報について保有者（teabevaldaja）を定めており、英語では「holder」となる。他方、人口登録法では住民登録データベースを政府の財産（英語のproperty）と捉えて、国が所有者（omanik）であるとした。

情報（データを含む）は「所有」という概念に馴染まないので、「保有者」という言葉を使い、データベースについては財産権の対象となるので「所有者」を定めるという住み分けである。

GDPR（欧州一般データ保護規則）の影響

こうした考え方に変化が見え始めたのは、2008年にデータベース法が公共情報法に吸収される形で統合し、新しい公共情報法になった頃からである。2008年1月施行の改正公共情報法[8]では、情報は保有するという考え方はそのままで、データベースについては所有者（omanik）という記述が無くなり、その代わりにデータベースの管理や処理に関する記述が多くなっている。

---

[6] GDPR（General Data Protection Regulation：一般データ保護規則） 個人情報保護委員会
https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/
[7] Avaliku teabe seadus https://www.riigiteataja.ee/akt/26643
[8] https://www.riigiteataja.ee/akt/12900546

GDPRの考え方に、より近づいた形だ。しかし、2008年の人口登録法[9]では、依然として「政府がデータベースの所有者（omanik）である」としていた（第7条）。

その後、オープンデータの法的な地位の確立などを経て、最後の変化として、2018年のGDPR（EU一般データ保護規則）の適用を受けた、各法令の大幅な改正が実施されることになる。この改正により、2019年1月施行の改正人口登録法[10]からも「政府がデータベースの所有者（omanik）である」という記述が消えた。

しかし、データベースの所有者（omanik）という考え方が、エストニアの法令や電子政府から無くなったのかと言えば、そういうわけでもない。各データベースを規定する法令の中には、データベースの所有者（omanik）の規定が残っているものもあり、RIHA国家情報システムカタログ[11]では、各情報システムやデータベースの所有者（omanik）を登録項目としている。

それでは、「公的データベースの所有者（omanik）」を日本語に訳する場合は、どうすれば良いのだろうか。筆者の答えとしては、素直に「所有者」で良いと考える。ただし、「GDPRの管理者（コントローラー）」とほぼ同じ意味で使用されることが多いので、文脈によっては注記を付けると良いだろう。

例えば、エストニアの医療総合データベースである「健康情報システム[12]」について、「承認された処理者」である政府機関のTEHIK（健康福祉情報システムセンター）は、次のように説明している。

『健康情報システムのデータは、患者ポータルを通じて患者自身にも表示されます。健康情報システムは、2008 年にすでに作成されています。データベースの所有者（omanik）、つまり管理者である社会問題省は、TEHIK にデータベースの管理と開発を許可しています。』

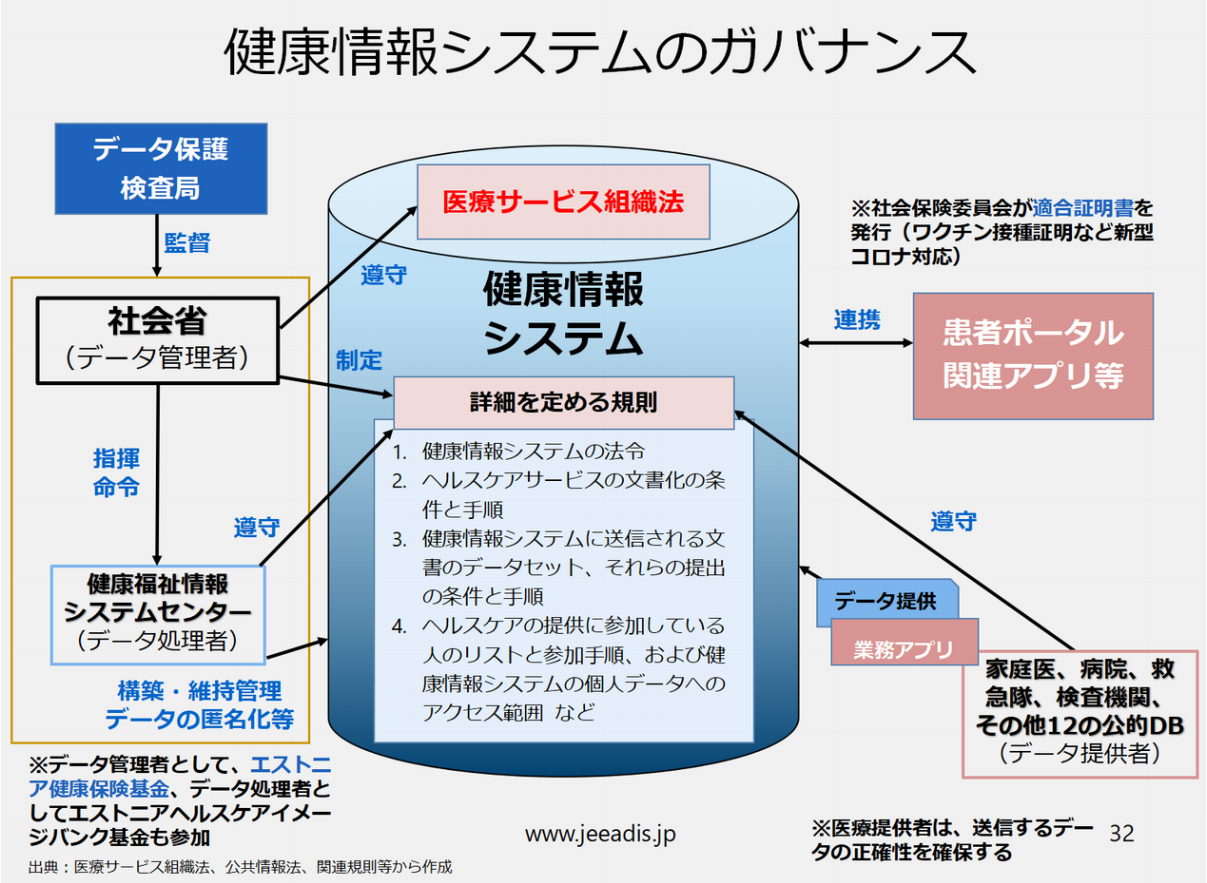
健康情報システムのガバナンスとデータ主体の権利

健康情報システムのガバナンスは、下記の図表に示す通りである。データベースの所有者でありデータコントローラーである社会（問題）省を監督するのは、データ保護検査（監督）局となっている。データベースを構築する前には、国家情報システム局による技術的なチェックも受ける。健康情報システムの患者・市民向けの公開インターフェースとして「患者ポータル」があり、データ提供者である医師や検査機関等のインターフェースとして各種業務用アプリケーションが存在する。公的データベースには、一般市民向けと職員向けのインターフェースを設置するのが通常で、インターフェースの設置責任はデータコントローラーにある。

最も重要なのは、健康情報システムのガバナンスの下で流通するデータは、法令によって標準化され実装が義務付けられていることだ。ここで言うデータ標準とは、データの形式・内容・交換・保存を含んでいる。

---

[9] https://www.riigiteataja.ee/akt/12806791
[10] https://www.riigiteataja.ee/akt/122122018013
[11] Administration system for the state information system RIHA
https://www.ria.ee/en/state-information-system/administration-system-riha.html
[12] TEHIK 健康情報システム　https://www.tehik.ee/tervise-infosusteem



図表：健康情報システムのガバナンス（2022年現在）

健康情報システムにおけるデータ主体（患者等）の権利[13]については、次のように整理している（2022年11月現在）。

1. データ主体の識別（権利の行使等で必要となる認証方法の指定）
2. データ主体が自身に関する情報および個人データを受け取る権利
3. アクションを実行し、データを送信および変更するデータ主体の権利
（個人データを提出するデータ主体の権利、データ主体が意思を表明する権利など）
4. 不正確な個人データの修正を要求するデータ主体の権利
5. 医療サービス提供者による個人データへのアクセスを拒否するデータ主体の権利
6. 第三者に個人データへのアクセスを許可するデータ主体の権利

エストニアの個人データ保護法と医療データの利用

日本の個人情報保護法にあたる、エストニアの個人データ保護法「Isikuandmete kaitse seadus[14]」（英語：Personal Data Protection Act）は、2007年に成立し2008年から施行した。現在は、GDPR（EU一般データ保護規則）の適用を受けた新しい個人データ保護法[15]（2009年1月

[13] 健康情報システムの法令 第5章 データ主体の権利 https://www.riigiteataja.ee/akt/130062018004
[14] https://www.riigiteataja.ee/akt/12802623

[15] 個人データ保護法 https://www.riigiteataja.ee/akt/104012019011

施行）となっており、用語の定義などはGDPRに従っている。そのため、エストニアの個人データ保護法を理解するためには、GDPRとセットで読み解く必要がある。

個人データ保護法の保護対象は「自然人の基本的権利と自由」で、個人情報の範囲は「識別可能な自然人に関する全てのデータ（形式は不問）」となっている。個人データの利用については、本人の同意が無い場合、別途法的な根拠が必要となる。

医療データは「特別な種類の個人データ」として、一般の個人データよりも厳格に保護されているが、医療・福祉サービスを提供する場合の利用については、もちろん本人の同意は不要である。健康情報システムに集められた医療データについては、医療サービス組織法[16]および関係法令[17]に基づいて、医療サービスの提供だけでなく「医療サービス品質の向上、患者（データ主体）の権利の保護、公衆衛生の保護と健康記録の維持、健康統計の作成と健康管理」など、幅広く利用できるようにしている（法第59条）。

科学研究や公式統計に必要な個人データの処理は、仮名化した個人データを利用することで、本人の同意を不要としている。この場合、倫理委員会[18]またはデータ保護監督官が、利用目的の検証（科学、歴史研究・公式統計の目的であるかどうか）を行う。科学研究には、政府機関（行政権力）による政策立案も含まれる

その後、個人の識別可能データを仮名（pseudonymised）形式にするが、再識別化は、追加の科学研究・公式統計で必要な場合のみ認められる。さらに、次の場合には、個人識別可能なデータを利用することもできる。これらの判断も、倫理委員会が行う。

1. 仮名化したデータでは研究等の目的を達成できない（著しく困難）
2. 個人識別可能データの処理に特に高い公益性がある
3. データ主体に追加義務が発生せず権利を不当に侵害しない

EUでは、個人データの利活用について、仮名化データの利用を推奨しており、それを受けてエストニアでも、GDPR対応の医療データ仮名化が進んでいる。その一つが、健康福祉情報システムセンターによる「Health Sense[19]」プロジェクトである。Health Senseは、データの仮名化、難読化、オープンデータ化のツールであり、関係機関に無償で配布されている。

エストニアにおける仮名化データの歴史は古く、2001年施行のゲノム法（ヒト遺伝子研究法：Human Genes Research Act）で既に規定しており、この当時は、仮名化（pseudonymised）ではなく、符号化（coded）としていた。現在のGDPR対応のゲノム法[20]（2019年施行）では、第23条で仮名化の具体的な方法を、同24条で非仮名化（再識別化）の条件等を定めている。

データは誰のものなのか？

[16] 医療サービス組織法 https://www.riigiteataja.ee/akt/110102022003
[17] 健康情報システム規則 https://www.riigiteataja.ee/akt/130062018004
[18] Research Ethics Committee of the University of Tartu https://ut.ee/en/node/113848
[19] Health Sense https://www.tehik.ee/health-sense
[20] ヒト遺伝子研究法 https://www.riigiteataja.ee/akt/113032019064

「データは誰のものなのか？」という質問に対して、法律上の解釈や説明は可能でも、一般の人々が感覚的に理解し納得できるような答えを提示することは難しい。誤解を招きやすい「自己情報コントロール権[21]」といった言葉に振り回されることなく、データ主体の権利[22]について整理し理解することが、やはり大切であろう。最後に、データ主体の権利とその制限について、日本でも参考になりそうなエストニアの事例を、いくつか挙げておこう。

個人識別コード

エストニアの個人データ保護監督局[23]は、個人識別コード（エストニアの住民を一意に識別する番号）について、次のように説明している。

『個人識別コードは、通常の個人データに属します。個人識別コードは、特定の個人を識別する必要がある場合（同名の場合）に開示します。また、個人識別コードの代わりに生年月日のみを開示することができます。[24]』

日本のマイナンバーと異なり、エストニアの個人識別コードは通常の個人データであり、（商業登記簿等の誰でも閲覧可能な公開情報の一部として）開示される場合があり、データ主体である本人は、それを拒否することができない。

犯罪歴照会サービス

法務省が提供する「犯罪歴照会サービス（Karistusregister[25]）」は、裁判記録を管理する電子訴訟ファイルサービス「E-toimik[26]」の追加機能として、2012年から運用している。このサービスを利用することで、自分または関係する未成年者や法人に関する前科データ（強制入院等を含む）を、無料で要求できる。他人のデータは承認（請求権の確認）が必要で、有料（4ユーロ）となる。自分の犯罪歴データに誰が照会したのかを、本人は確認できる。保存期間（照会可能な期間）が経過した後の犯罪歴データは、削除される前にアーカイブへ転送される。

企業や公的機関等の雇用主は、法令（児童保護法等）が定める雇用要件を確認するために、雇用しようとする者に関する犯罪歴を照会し確認する義務がある。「犯罪歴照会サービス」を利用して照会できる場合は、本人に対して犯罪歴の有無を直接確認（例：面接で「あなたは犯罪歴がありますか？」と質問する）してはいけないことになっている。

エストニアでは、学校の教師や保育園の保育士といった特定の専門職に限らず、子供と接触する機会がある職業に就く際には、過去に一定の犯罪歴が無いことが雇用条件となる。その確認義務を雇用主に負わせているため、上記のようなサービスが提供されている。

公共サービスとプロファイリング

現在の電子政府サービスのトレンドとして、「積極的サービス」や「見えないサービス」と言われるものがある。これは、申請不要の新しいサービス方式で、日本では「プッシュ型サービス」と言われるものだ。

---

[21] Q1-2保護法の目的は何ですか。https://www.soumu.go.jp/main_sosiki/gyoukan/kanri/question01.html
[22] GDPR: Rights of the data subject https://gdpr-info.eu/chapter-3/
[23] Data Protection Inspectorate https://www.aki.ee/en
[24] Küsimus-vastus https://www.aki.ee/et/eraelu-kaitse/kusimus-vastus
[25] Karistusregister https://www.rik.ee/et/karistusregister
[26] E-toimik https://etoimik.rik.ee/

エストニアの社会保険委員会が運用している「社会福祉給付ポータル（あなたの給付）[27]」も、申請不要の「見えないサービス」を提供している。社会福祉給付データベース[28]に登録されたデータや他の公的データベース（社会保障情報システムなど）のデータを利用することで、子供が生まれた家庭に対してオンライン通知を行った上で、児童手当を給付している。同様のサービスとして、育児休業手当の支給などもある。

こうした申請不要のプッシュ型サービスを実現するためには、住民とサービスのマッチングや自動処理が必要になる。エストニアの個人データ保護監督局では、これを「自動化された意思決定とプロファイリング[29]」として整理しており、プロファイル分析を含む自動化された意思決定が許可されるのは、次の3つのいずれかに該当する場合としている。

1) 顧客との契約締結や履行のため
2) 自動意思決定を法律で規定している
3) 自動意思決定とプロファイル分析に本人が同意した

自動化された意思決定とは、IT ツールを使用して人間の介入なしに人に関する意思決定が行われることを意味する。プロファイリング（プロファイル分析）とは、決定が下されていなくても、その人に関する予測を行うために、その人に関する状況を評価することを意味する。例えば、企業や組織が年齢、性別、身長などの個人の特性を評価したり、特定のカテゴリに分類したりする場合である。税務当局は、データベース内の情報に基づいて個人のプロファイル分析を行い、それに基づいて自動決定を下すことができる。

上記の児童手当の給付は、「2) 自動意思決定を法律で規定している」に該当するケースである。また、分析するデータに「特別な種類の個人データ[30]」が含まれている場合は、2または3の場合に限ってプロファイリングが可能になる。EUのガイドライン[31]に従った運用であると言えるだろう。

自動化された決定は、法的効果をもたらしたり、個人にその他の望ましくない影響を与える可能性があるため、その決定が不正確・不完全なデータに基づいて行われたことが判明した場合、自分の個人データを修正する権利を持たなければならない。電子政府サービスで自動化された意思決定やプロファイリングを行う場合は、各種手当の受給など、本人に不利益を与える可能性が少ないものから適用するのが良いだろう。

2022年11月10日
日本・エストニア EU デジタルソサエティ推進協議会 (ジェアディス)
理事　牟田 学
お問合せ https://www.jeeadis.jp/contact.html

[27] 社会福祉給付ポータル（あなたの給付）https://iseteenindus.sotsiaalkindlustusamet.ee/
[28] 社会サービスと福利厚生のデータベース https://www.riha.ee/Infos%C3%BCsteemid/Vaata/star
[29] 自動化された意思決定とプロファイリング
https://www.aki.ee/et/eraelu-kaitse/automatiseeritud-otsused-ja-profiilianaluus
[30] GDPR 第9条：人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、又は、労働組合への加入を明らかにする個人データの取扱い、並びに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、又は、自然人の性生活若しくは性的指向に関するデータ
[31] 自動化された個人に対する意思決定とプロファイリングに関するガイドライン
https://www.ppc.go.jp/files/pdf/profiling_guideline.pdf