

情動的措置を授権する規定の「特定性」と「二重扉」 — ドイツの議論 —

實原隆志*

はじめに

ドイツ国内での違憲審査としては、比例原則や利益衡量に基づく審査があるが、ドイツにおいて情動的な措置の合憲性が検討される際には、手段の比例性ばかりが審査されているわけではない。それゆえ、ドイツにおいて用いられている違憲審査の特徴について検討するとすれば、制約手段の比例性以外の審査も取り上げる必要があるように思われる。そこで、以下では、「特定性の要請」と『「二重扉」モデル』を、それぞれドイツにおける違憲審査の場面で登場している特徴的なものとして挙げることでドイツにおける違憲審査の枠組みの一部を紹介し、それを日本で参照した場合にどのような示唆を得られるか、そして、どのような問題が生じるかを検討する¹。

*福岡大学法学部教授

¹ 本稿は、2020年9月28日にJILIS情報法×憲法研究会・第二回研究会（オンライン開催）において、同題の下で報告した内容に、当日の質疑と報告後の状況を反映させるための修正を行って作成されたものである。

1. ドイツにおける「特定性の要請」(Bestimmtheitsgebot)

(1) 税関刑事庁決定による説明²

「特定性の要請」について連邦憲法裁判所が具体的に述べた初期のものと
して、2004年の税関刑事庁決定がある。この決定において連邦憲法裁判所は、
監視措置の授権に対する「特定性の要請」を、どのような端緒があり、どの
ような条件の下で、ある行為が監視されるリスクを伴うのかを、本人が認識
できることを求めるものであるとした。連邦憲法裁判所は、この要請は、国
家による侵害の行為の具体的な行為条件を知らない者のためのものでもある
とし、端緒を生み出したわけではなく、どちらかというと偶然に該当してし
まっている形になっている第三者にとって特定性が必要なものであり、監視措
置の条件を、基本的には後になればわかるような方法で法秩序が規定してい
ることが必要であるとした。このようにして、この決定では、授権規定に特
定性が求められることで、監視措置の端緒や条件、リスクが特定されている
必要性が措置の秘匿性を考慮して求められ、それにふさわしい法秩序である
べきことを求める要請として「特定性の要請」が説明される形になっていた。

この事件で問題となった、税関刑事庁の権限についてみると、外国貿易法
(Außenwirtschaftsgesetz)では、外国貿易法や戦争兵器規制法(Kriegswaf-
fenkontrollgesetz)での犯罪を予防するために、信書・郵便・通信に服す送
付物を開披・閲読することと、通信を監視・記録することを税関刑事庁に認
めており(39条1項)、そうすることで、信書・郵便・通信の秘密を制約す
ることを認めていた。そして、そのようにして取得された個人データは、「公
的機関」によって処理されてよいことになっていた(41条2項)。

この決定の結論として、各規定は、先述の「特定性の要請」を満たしてい
ないとして違憲とされた。そこで「特定性の要請」を満たさないとされたも

² 連邦憲法裁判所・第一法廷2004年3月3日決定(BVerfGE 110, 33)。

のとしては、「参照規定を参照する参照規定」（Verweisungskette）、個人データの受領当局が特定されていないこと、条文編集上の不正確さ、などがある。この決定をみてみると、一口に「特定性の要請」といっても、そこには様々な要請が含まれていることがわかる。また、この決定は、授権規定にはなぜ特定性が必要なのかも説明している。一つの要因として行政の統制が挙げられ、「特定性の要請」は行政の行為裁量との関係で、それを限定する機能を有しているとし、それが国家の法律適合的な行為を保証し、国家による恣意から市民の自由を保護するのだとしている³。ほかにも、「特定性の要請」には司法の統制という機能もあり、裁判所が行政を法的な基準によって統制できるようにするのに役立つのだとも述べている。ただ、「特定性の要請」の強度は侵害の種類と重大性などによって変わるとしている。

このように、「特定性の要請」の必要性とその内容について述べたこの決定では、取得した個人データを公的機関が処理することを認める規定の合憲性が問題となり、「特定性の要請」の強度は侵害の種類と重大性などとの関係で一定の可変性をもつものとして説明された。こうした説明をみる限りではあるが、連邦憲法裁判所は、「特定性の要請」を、権力分立的な要素を含む、柔軟性のある要請として解しているものと思われる。

（２）「三段階審査」のなかでの位置づけ

ドイツにおける違憲審査としてのいわゆる「三段階審査」は比例性審査も含むものであり、そこでは、授権規定の特定性が検討されるのに先立ち、保護領域該当性と、それに対する侵害（Eingriff）該当性が審査される。そうした侵害があるとされると、その侵害の正当性が検討され、その際には授権規定が存在しているか、また、その法律に特定性が備わっているかが検討される。授権規定に特定性が認められると手段の比例性の審査に移るが、法律

³ 行政の拘束の重要性は、本人は監視措置を知らないことから導かれるとしている。

に特定性が認められない場合には、手段の比例性を審査するまでもなく、当該措置などが違憲であることが確定する。この後にもみるように、「特定性の要請」の観点での審査がドイツにおいて一定程度定着しているということになると、ドイツにおける違憲審査では、比例性の審査の比重が、一般に考えられているほどには高くないということになるのかもしれない。

(3) 判例における「特定性の要請」⁴

当該措置に特化した授権規定に基づく措置は、一般的に「標準的措置(Standardsmaßnahme)」と呼ばれる。税関刑事庁決定もそうした措置を問題にしたものであるが、それ以降の判例でも、こうした、標準的措置を授権する規定のあり方が、特定性の観点で問題とされている。当該規定の特定性を審査した結果、合憲との判断が出ることも⁵、違憲との判断が出ることもあり⁶、また、争点も、利用目的の不特定性、侵害閾値の不特定性、措置が行われる範囲の不特定性など、多岐にわたっているが、いずれにしても、連邦憲法裁判所においては、授権規定の「特定性」が違憲審査における重要な争点となっている。

別の場面では、関係する個別立法はあるものの、それを当該の措置の授権根拠とできるかが「特定性」の問題として論じられることがあり、その一例として、「ヴァーチャル覆面捜査官の投入」をめぐる議論がある⁷。現実世界で身分を偽装して行う(リアル)覆面捜査官に関する規定は、ドイツにおい

⁴ 拙著『情報自己決定権と制約法理』(信山社、2019年)190頁以下。

⁵ 最近のものとして、第二次契約者データ決定において合憲とされた部分(NJW 2020, S. 2699 ff. <Rn. 205>)。

⁶ BVerfGE 150, 244 (第二次Nシステム決定); NJW 2020, S. 2235ff. (外国にいる外国人の通信の解明を問題にした決定)。また、第二次契約者データ決定において違憲とされた部分(NJW 2020, S. 2699ff. <Rn. 122ff.>)など。

⁷ この報告のうちのこの部分は、科研費・基盤研究(C)「インターネット上での公権力による情報収集とプライバシー権—その立法的統制」(2018年度～2020年度)の研究成果の一部である。

ては既に刑事訴訟法110a 条の2 項と3 項にあるが、この規定を、SNS などのプロフィールを偽装してインターネット上で情報を収集することまで認める規定として理解できるかには争いがあり、ドイツ国内の学説の一部には、そう理解すると特定性との関係で問題となるとの指摘がある⁸。ヴァーチャル覆面捜査官に関する議論状況を見ると、「当該措置自体を直接授権する規定はないが、関係しそうな措置を具体的に授権する規定はある」という場合に、それを援用できるかが検討される際にも、当該措置の授権規定としての「特定性」を問題とする余地があると考えられていることがわかる。

また、連邦憲法裁判所の判例に戻ると、2007年の部会決定では、監視カメラの使用とそれによって取得されたデータの保存を、個人データ保護法の例外規定を援用して正当化できるかが問題となった。この決定において連邦憲法裁判所は、バイエルン州データ保護法16条1 項と17条1 項は、得られた動画資料の記録を伴うビデオ監視の授権根拠としては十分に特定されていないとして、当該措置を違憲であるとした⁹。監視カメラのような、今日において一定の重要性のある手法による情動的措置の憲法上の問題が、部会で処理されるにとどまったことには意外なところもあるが、それは、監視カメラの使用について個人データ保護法の例外規定を援用するということが明らかに不合理であるために、「憲法異議には明らかに理由がある (begründet)」（連邦憲法裁判所法93c 条1 項1 文）と考えられたからであろう。この決定の特徴に話を戻すと、この事件では、当該措置と直接的に関連する規定がなく、関連性が強くない規定を授権規定と理解するとその規定が特定性を満たさなくなるので、当該措置が違憲とされたと理解できる。また、監視カメラの使用まで授権する規定として理解してしまうと、個人データ保護法による授権が過度に広汎なものになってしまうという問題もあるだろう。このような事

⁸ Saleh Ramadan Ihwas, *Strafverfolgung in Sozialen Netzwerken*, 2014, S. 170.

⁹ BVerfGK 10, 330<Rn. 45>.

例は、ドイツでは珍しい部類に属すると思われるが、「京都府学連事件」における最高裁判決のように¹⁰、技術的な手法を使った捜査の根拠として警察法2条1項を挙げる日本の議論は、情動的な措置の根拠規定として、該当する措置との関連性が強くない、既存の法律を挙げているという点で、「レーゲンスブルク型」に近いものといえよう。

以上のように、ドイツにおいては、当該措置を直接授権する規定がある場合、当該措置自体を授権しているわけではないが関連性がある程度はある規定がある場合、当該措置と関連する措置を具体的に授権する規定はない場合、のいずれにおいても「特定性の要請」が争点となっており、「特定性の要請」を満たさないとして違憲となるのが、当該規定である場合と、当該措置である場合とがある。そうした「特定性の要請」が登場する場面を二つに分けるとすれば、そのひとつは「当該『授権規定の特定性』」が問題とされる場合である。この場合には「規範の明確性 (Normenklarheit)」と類似した要請となり、その要請が満たされないとされれば、当該規定が違憲と判断される。もう一つが、「当該規定の『授権規定としての特定性』」が問題となる場合であり、授権規定として援用されている規定がこの要請を満たしていないとされれば、この場合には、その措置が違憲になる。先に挙げたなかでいえば、「標準的措置」の授権規定の場合には「授権規定の特定性」の問題となり、「ヴァーチャル覆面捜査」に関する議論や「レーゲンスブルク決定」は、「授権規定としての特定性」を問題にしたものとして整理できる。

(4) 小括：ドイツにおける「特定性の要請」

このように、ドイツ国内の違憲審査においては、税関刑事庁決定以降、「授権規定」の「特定性」を審査する傾向が強まっており、比例性の審査にとどまらない検討が行われている。「特定性」の検討には、「授権規定の特定性」

¹⁰ 最大判1969年12月24日（刑集23巻12号1625頁）。拙稿「判批」長谷部・石川・宍戸編『憲法判例百選Ⅰ〔第7版〕』（有斐閣、2019年）36頁以下。

の検討と「授権規定としての特定性」の検討があるのではないかということは、先に述べたところであるが、いずれにしても、ドイツの判例実務を追う際には、「特定性の要請」について述べている部分に注目することが必要になっている。

2. ドイツにおける「二重扉（Doppeltür）モデル」

ここまで取り上げた「特定性の要請」は、既に2004年の決定において用いられたものであり、その後の判例を通じてある程度は定着をみせていると思われる。それとは別に、もう少し新しい違憲審査の枠組みとして「『二重扉』モデル」もあるため、次に、そうした「二重扉モデル」について述べることにする。

（1）ドイツ連邦憲法裁判所の2012年の決定と2020年の決定

① 2012年決定¹¹において問題となった規定

2012年の決定では連邦通信法の規定がいくつか問題となっている。この法律の111条は、電話番号や回線所有者といった個人情報（氏名、住所など）で構成される、「契約者データ（Bestandsdaten）」を保存するよう義務づけており、112条1項ではその「契約者データ」¹²を顧客データのなかに保存するよう義務づけていた。112条1項ではさらに、連邦ネットワーク委員会がそのデータを自動的に取得できるようにしておく義務が、通信事業者に対して課せられていた。連邦ネットワーク委員会は112条2項で挙げられている機関に、取得したデータを提供してよいことになっており、それらの機関からの照会に基づいて、通信事業者が保有している契約者データを取得し、各機関に提供することになっていた。連邦ネットワーク委員会に対する照会が

¹¹ BVerfGE 130, 151<Rn. 123-125>. また、拙稿「通信サービスの利用者データを保存・提供させる手続の合憲性」自治研究90巻10号（2014年）148頁以下。

¹² 連邦通信法の定義規定は、3条に置かれている。

違法である可能性もあるが、連邦通信法の112条4項2文では、提供の窓口となる連邦ネットワーク委員会が提供の適法性を審査するのは、これについて特別な端緒が存在する場合のみであるとしており、これは、連邦ネットワーク委員会には厳格な審査義務はないということであるとされている¹³。このように、まず連邦通信法112条関係では、111条によって保存される契約者データの保存義務と、それを連邦ネットワーク委員会が自動的な方法で取得できるようにしておく義務について定められており、提供の適法性に対する連邦ネットワーク委員会の責任は、厳格な審査義務を負わないという形で制限されていた。

次に、連邦通信法の113条1項1文では、通信事業者に対して、管轄の機関からの照会に基づいてデータを「手動」で開示するよう義務づけており、この場合に開示の対象となるデータは、この法律の95条1項と111条によって収集・保存できるデータであった。これらのデータには、事業者の契約関係を内容的に形成、変更・終了させるデータも含まれており、例えば銀行振込や特別（割引）料金に関する個々の記載も含むものである。113条1項1文に基づく開示の相手先となる機関は、任務に関連する形で、抽象的に規定されるにとどまっておらず、照会を行える行政当局が限定的に列挙されているわけではなかった。113条1項1文に基づく開示においても、113条2項5文は、開示請求の適法性に対する責任は、3項で挙げられている、提供を求める側の機関が負うとしている。このように、連邦通信法の113条は、通信事業者において保存されている、利用上のデータの開示義務について規定し、開示先となる機関を抽象的に挙げるとともに、112条の場合と同様に、提供側の責任を制限する形で規定していた。

同じく113条1項のうちの、今度は2文についてみると、これは、やはり

¹³ Franz Jürgen Säcker (Hrsg.), TKG, 3. Aufl., 2013, § 112, S. 2535ff. <S. 2545> (Diethelm Kleszczewski).

各種の規定に基づく場合の開示義務を規定するものであったが、そこで開示の対象となるデータは情報端末や保存設備への無権限のアクセスから保護するために必要なデータであり、個人識別番号（PIN）や PIN ロック解除コード（PUK）、要するに、パスワードのようなコードも含むものであった。そして、この場合もデータの開示の適法性に対する責任は113条2項5文により、3項で挙げられている、データを照会する側の機関が負うことになっていた。このような形で、連邦通信法の113項1項2文は、同項1文の場合とは異なり、パスワードなどの開示義務について規定する一方、開示の適法性に対する提供側の責任は、1文の場合と同様に、制限される旨を規定していた。

以上述べた通り、2012年決定で問題となった連邦通信法の諸規定では、契約者データや通信データ、また、パスワードのようなアクセスデータの授受について定められており、いずれについても、その授受における提供側の責任は制限されていた。

② 連邦通信法112条・113条の射程範囲¹⁴

これらの規定の合憲性を審査するにあたり、連邦憲法裁判所は、データの収集と保存、利用とを区別すべきであるとした。そして、国家の任務を遂行するためのデータ授受（Austausch）の規定の場合には、さらに、開示を行う機関の側でのデータの提供と、照会を行う機関の側でのデータの取得とを区別しなければならず、それぞれの侵害が独自の法律上の根拠を要すると述べた。そこにおいて、立法者は、描写的に述べるならば、データを提供するためのドアだけでなく、照会を行うためのドアも開けなければならず、二つの法的根拠が相まって、つまり、二重扉のように作用するような、両方の法的根拠があって初めて、個人データの授受を行えるのだとしたうえで、デー

¹⁴ BVerfGE 130, 151<Rn. 123>.

タを取得するための根拠規定がないことを指摘した。当時の連邦通信法はデータの提供権限を規定するのみで、取得するための要件を規定していなかった以上、取得側の規定が合憲か違憲かという議論はできなかったこともあり、この決定は、「二重扉モデル」との関係では、データを取得するための要件が規定されていないことを指摘して終わった。

③ 連邦憲法裁判所第一法廷・2020年5月27日決定¹⁵

この決定を受け、その後、データの取得側に対する規定が整備され、2020年の決定が、それらの規定の合憲性を検討した。提供側の規定の詳細は省くが、先にも言及した、提供の適法性についての責任は、改正法においても、3項で挙げられている取得側の機関が負うことになっている（連邦通信法113条2項4文）。問題は、2012年の決定を受けて整備された提供側の授権規定も含めた、関連データの授受に関する規定の合憲性であるが、連邦憲法裁判所は、それらの規定の一部を違憲だとした。まず、提供側の規定が違憲とされた理由であるが、侵害閾値が限定されておらず、比例的でない指摘している。特に問題とされたのは、侵害を行うのに必要な、事実の端緒（Anlass）がなく「任務の遂行」のためでも回答してよいことになっていたことであり、これでは利用目的の限定という点で問題があるとした。他方で、取得側の授権規定も問題となり、これについても、様々な点が違憲とされた。指摘された問題の主なものとしては、データの取得を限定する侵害閾値が前提とされていないこと、規範上明確（normenklar）な参照規定になっていないこと、重大犯罪の場合に限定されていないこと、文書化義務の不備、などがある。2020年決定についてもいくつか述べてきたが、本稿との関係では、2020年決定が、2012年決定当時には制定されていなかった、取得側の授権規定の合憲性を検討し、その一部を違憲とすると同時に、提供側の規定の一部も違憲と

¹⁵ NJW 2020, S. 2699ff. なお、判決文が公表されたのは2020年7月17日である。

したという点が重要である。

④ 小括：ドイツ連邦憲法裁判所の2012年の決定と2020年の決定

ここまで連邦通信法とその関係法の規定の合憲性を扱った二つの決定をみてきたが、2012年決定と2020年決定を総合して考えると、連邦憲法裁判所は官民の間での個人データの授受について、提供側と取得側の双方に授権規定を求め、さらに、それらの合憲性を、授受の対象となるデータの重要性をふまえて、場合によっては厳格に審査しようとしているといえるだろう。

（2）「極右主義・ヘイトクライム撲滅法」の審議における議論

こうした「二重扉モデル」への言及は、先に挙げた2012年と2020年の決定だけでなく、2020年に入って議会に提出された「極右主義・ヘイトクライム撲滅法案」（以下、「ヘイトクライム対策法」）の審議過程においてもみられる。連邦の連立与党は、極右主義やヘイトクライムを撲滅するためには効果的な刑事訴追も必要であり¹⁶、その前提となるのは、被疑者を特定し、証拠を保全することだと考え¹⁷、SNS事業者を含むテレメディア事業者を規制対象とする改正法を提案した。この改正法案は、2020年7月3日に連邦参議院（Bundesrat）を通過した¹⁸。

次に、この改正法による授権の内容をみると、改正テレメディア法では、新15a条が、テレメディア事業者に対して契約者データと利用データ（Nutzungsdaten）の提供を授権し、新15b条がアクセスデータの提供を授権していた。そして、提供の適法性についての責任は照会側の機関が負うと

¹⁶ 2017年には「ネットワーク執行法（SNS法）」が制定され、SNS事業者は、違法なコンテンツが着実に削除されるような体制をつくるよう求められている。この法律について、拙稿「ドイツのSNS法——オーバーブロッキングの危険性について」情報法制研究4号（2018年）46頁以下、など。

¹⁷ BT-Drs. 19/17741, S. 40ff.

¹⁸ 本稿作成時点（2020年12月）では、連邦大統領の署名待ちとなっている。これに関しては後述する。

していた。そこでの規定内容は、基本的には、先述の連邦通信法の関係規定と同様であり、連邦の連立与党自身も、連邦通信法の関係規定を参考にしたとしている¹⁹。他方で、取得側の授権規定であるが、刑事訴訟法の100g条をテレメディア法の新15a条の権限の裏づけに、100j条を新15b条関係の権限の裏づけにもすることになっており、100j条の措置には、以前から裁判所の命令が必要である。これらの刑事訴訟法の規定に加えて、連邦刑事庁法10条1項2文にも、テレメディア法の新15a条1項1文に対応するデータの取得権限が規定されることになっていた。刑事訴訟法の改正規定によって、契約者データ・利用データ・アクセスデータの取得の授権が予定されており、また、連邦刑事庁法の改正案では、そのうち、アクセスデータの取得までは認められていなかったということになる。本稿において注目したいのは、連邦の連立与党が法案を提出した理由を述べているなかで、連邦憲法裁判所の「二重扉モデル」を確認していることである²⁰。連立与党は、ドイツの刑事訴訟法161条や163条といった一般条項では、連邦憲法裁判所が連邦刑事庁決定²¹で示した要請を満たすのかが問題になるため、規範上明確（normenklar）な形成等が必要であることを指摘した。このことから、2012年に連邦憲法裁判所が示した「二重扉モデル」も含めた判例の動向を、ヘイトクライム対策法を立案した連邦与党も、かなり意識していたことがわかる。ここまで2020年に連邦議會を通過した、ヘイトクライム対策法について述べてきたが、そこでの規定や連邦の連立与党の説明をみると、ヘイトクライム対策を目的にして、テレメディア事業者が保有する個人データの授受について新たに規定を追加することになり、立案者自身、連邦憲法裁判所の「二重扉モデル」等を強く意識していたということになるだろう。

¹⁹ BT-Drs. 19/17741, S. 40.

²⁰ BT-Drs. 19/17741, S. 38.

²¹ BVerfGE 141, 220.

その一方で、「連邦参議院」からは、連邦議会に対して様々な要望・指摘がなされている²²。そのうちの 하나가、連邦の立法者によって明らかに意図されている条件を、法案の15b条2項から、刑事訴訟法100j条1項2文にも受け継ぐことが必要ではないかというものである。さらに、同様の批判は連邦議会に提出された、学者の意見書においてもみられ、刑事訴訟法100j条では、テレメディア法15b条が開示義務について規定しているところよりも対象犯罪が広がっているのではないかと批判がある²³。それらの意見書のなかで、本稿の関心と関係する指摘を詳しく行っているものとして、Bäckerによるものがあり、Bäckerは、契約者データ・利用データ・アクセスデータのそれぞれについて、提供と取得に関する規定の合憲性を検討し、一部の規定を違憲だとしている²⁴。

そのような批判がありながらも、この法案は2020年の7月に議会を通過したが、本稿執筆時点において、連邦大統領は連邦政府に対して法律の改正を求め、署名を見合わせている²⁵。先述の、2020年の7月に入って公表された2020年5月付の違憲決定が、ヘイトクライム対策法の作成において依拠されていた規定を違憲としたことで、ヘイトクライム対策法にも違憲である疑いが生じたためである。同法の署名・施行に手間取っていることについて説明を求める野党からの質問に対して、連邦政府は、合憲性に懸念がある規定として、利用者データの開示規定をテレメディアサービス事業者に拡張しよう

²² BR-Drs. 87/1/20, S. 17f.

²³ Ulrich Kelber, Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, S. 7.

²⁴ Matthias Bäcker, Stellungnahme zu dem Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, S. 13ff.

²⁵ <https://www.sueddeutsche.de/politik/gesetz-hasskriminalitaet-steinmeier-bundesregierung-1.5058806> (最終アクセス日: 2020年12月15日)。また、神足祐太郎「諸外国におけるインターネット媒介者の『責任』」レファレンス839号(2020年)131頁以下<152頁>。

としている連邦刑事庁法の新10条、連邦通信法113条を参考にして予定されていたテレメディア法の新15a条、そして刑事訴訟法の新100j条を挙げている²⁶。本稿を執筆している段階では、管轄官庁から各種の専門家・団体に対して意見が求められており、同年内の制定を目指して連邦政府内で調整中であるとのことである²⁷。

ここでは、ヘイトクライム対策法による改正内容、そして、連邦政府による法案の趣旨の説明と、法案に対する批判的な見解を取り上げてきた。それらをもとにみると、通信事業者と公的機関との間での個人データの授受だけでなく、テレメディア事業者と警察・公安機関の間での個人データの授受のための法改正の議論においても、法案に対する賛成・批判の双方において、「二重扉モデル」の影響を確認でき、それは同法の可決後の混乱にも示されているように思われる²⁸。

（3）2012年決定以前の議論状況

上述の2012年と2020年の決定は、提供側の授権としての連邦通信法の関係規定を検討の対象としたものであり、2020年改正法は、テレメディア法の関係規定と、取得側への授権規定を整備するものであった。そして、ヘイトクライム対策法のうちのテレメディア法の改正案は、連邦通信法を参考にしたとされている以上、それぞれの議論において「二重扉モデル」が意識されていることは当然といえは当然である。そうすると、「二重扉モデル」は2012年の決定で問題となった制度と関連する場面でしか用いられない、新しく、しかも、射程の極めて狭いものである可能性もある。そこで、データの提供

²⁶ BT-Drs. 19/23867, S. 3f.

²⁷ https://bitkom.org/sites/default/files/2020-12/20201201_bitkom_stn_bestandsdatenauskunft.pdf（最終アクセス日：2020年12月15日）。

²⁸ 本報告のうち、この部分の記述は、公益財団法人・電気通信普及財団 2019年度研究調査助成（通常枠）「ヘイトスピーチ対策として SNS 事業者に対行政責任を課す場合の法的課題」による研究成果の一部である。

に関する一般法にあたる連邦データ保護法をみても、以前の28条2項(現24条1項1号²⁹⁾)は、第3章にあった規定であり、第3章で適用対象の一つとなっていたのが「公的ではない機関のデータ処理」である。そのなかの28条2項が、目的外での提供・利用が認められる場合を挙げ、旧28条2項2号のなかのbでは、国家・公共の安全に対する危険を防御するため、もしくは、犯行を訴追するために必要な場合が挙げられていた。この28条2項2号bについて、2012年決定よりも前になされていた説明をみると、28条2項2号のなかでも、危険防御当局・刑事訴追当局の側でのデータの照会までは、この規定だけでは授権されているわけではないことが、より強調されている³⁰。それをみる限りで述べれば、2012年決定よりも前に、データの提供に対する授権と、収集に対する授権は別々のものでなければならないという考え方自体は、既にあったといえそうである。ここでは、「二重扉モデル」の射程が極めて限定されたものである可能性を考え、「二重扉」という言葉を用いた2012年決定よりも、前の段階の連邦データ保護法の規定と、それに関する説明をみた。それをみる限り、「二重扉」との言葉が使われる前から、その内容自体は既に、個人データ保護一般の問題として、特に警察・公安当局との関係で唱えられていたといえるように思われ、データの提供と取得には別々の根拠規定が必要であり、データの「提供」を認める規定ではデータの収集・保存の授権規定にはならないということ自体は、2012年決定が初めて述べたというわけではなく、その射程も個人データ保護分野一般に及ぶものとして考えられていたものと思われる。

²⁹ 現行法の規定は、公的ではない機関に対して、データを収集した時とは別の目的での「処理 (Verarbeitung)」を認めるものとなっているが、これに基づいて「提供」が認められるとされている。BDSG 24条1項1号による授権範囲 (の限定) を「二重扉モデル」に言及することで説明しようとしているものとして、Gernot Sydow (Hrsg.), Bundesdatenschutzgesetz, 2020, S. 288 (Fn. 26) (Nikolaus Marsch)。

³⁰ Jürgen Taeger/Detlev Gabel (Hrsg.), Kommentar zum BDSG, 2010, S. 741 (Jürgen Taeger)。

(4) 小括：ドイツにおける「二重扉 (Doppeltür) モデル」

以上のように、ドイツにおける「二重扉モデル」は、2012年の決定において登場したにとどまらず、のちの関連判例や、それとは別の改正法案の審議過程においても検討の枠組みとして用いられている。また、2012年決定の以前から、個人データの「提供」を認める規定では、警察・公安当局側の「取得」の授権とはならないと考えられていたようであるため、2012年決定が「二重扉モデル」を提唱するよりも前の段階で、ドイツにおいては、個人データの提供と取得にはそれぞれ別々の授権規定が必要であるという考え方が既にあり、その射程も広いものとして捉えられていたのだと思われる³¹。それゆえ、「二重扉モデル」の内容は、ドイツにおいて有力な審査基準であり、今後も用いられる指標であり続けると考えられる。

3. 日本の議論へのあてはめ

ここまで、ドイツ国内の「特定性の要請」と「二重扉モデル」について概観してきたが、ドイツでそのような議論がされているとして、問題となるのは、それが日本の議論においてどのように位置づけられるかであろう。

(1) 「特定性の要請」³²

まず、「特定性の要請」は、刑事訴訟法197条2項の、いわゆる「捜査関係事項照会」のことを考える上で参考になるかもしれない。近年、Tポイント関係の個人情報、捜査関係事項照会の枠組みで警察に提供されていることが問題となったが³³、捜査関係事項照会について規定する刑事訴訟法197条2

³¹ 二重扉審査の下では、データの「提供」・「取得」のそれぞれの授権規定の特定性が審査されるため、「特定性の要請」と二重扉審査には密接な関連性があるといえる。

³² 関連する検討については、拙稿「捜査員による情報収集活動における国内法・日本国憲法上の問題」国際人権31号(2020年)49頁以下において、既に行っている。

³³ 共同通信・2019年1月20日発信記事。共同通信社会部取材班「丸裸にされる私生活 企業の個人情報と検察・警察」世界921号(2019年)107頁以下、三木由希子「捜査関係事項照会問

項は、情報化社会が到来するよりも、はるか以前に制定された規定である。こうした規定を基に、現代的な個人情報をも民間事業者に対して照会して提供させることが認められるのかは、検討を要するところであろう。

ここでは、Tポイントと捜査関係事項照会の関係を手がかりとしたが、ドイツでの監視カメラや「ヴァーチャル覆面捜査官」を使用した措置の授権規定の「特定性」に関する議論をみると、刑事訴訟法197条2項が警察に個人情報を提供する上での授権規定たりえない場合もあるのではないかと、また、いかなる団体にも、いかなる情報でも要求できるという規定なのであれば、刑事訴訟法197条2項は違憲なのではないか、という疑問も生じるころである。本稿において先に使った整理を使うならば、「授権規定としての特定性」という点での問題である。

また、刑事訴訟法197条1項と任意処分との関係や、刑事訴訟法241条の令状主義についても、ここまで述べたのと同様のことが当てはまるだろう。「同様のこと」というのは、要するに、これらの規定は今日用いられているような技術的な手段を用いた捜査を想定しておらず、それらを授権する規定であるとはいえないのではないかと、そして、それらを授権根拠として行われている捜査は違法・違憲なのではないかと、他方、そうした捜査を広く認める規定なのであれば、これらの規定が違憲なのではないか、ということである。つまりは、ここでも「授権規定としての特定性」を問題にする余地があるように思われる。

以上のようにして、「特定性の要請」を日本でも参照した場合、刑事訴訟法197条2項や同法197条1項の適用範囲にとどまらず、それらの「授権規定

題を考える 民間事業者の警察への情報提供にルールを」時の法令2071号（2019年）57頁以下。JILIS「捜査関係事項照会対応ガイドライン（案）」（2019年3月17日）https://jilis.org/proposal/pages/2020-03-17/sousa_guideline.pdf（最終アクセス日：2020年12月15日）3頁、7頁は、この問題を機に、捜査関係事項照会について規定する刑事訴訟法197条2項を根拠とした提供範囲の限定を試みる。

性」の議論にも行きつき、さらには、令状の要否にとどまらず、同法241条に基づいて令状を発付できるのか、つまり、令状発付の可否も問われることになるようにも思われ、これは、いずれも、「授権規定としての特定性」という観点を参考した場合に必要な議論ということになるだろう。

(2) 「二重扉モデル」

捜査関係事項照会については、「特定性の要請」との関係で先にも取り上げたが、警察からの捜査関係事項照会を受けた民間の事業者が個人情報を提供することが認められるとすれば、その根拠は、おそらく個人情報保護法23条1項1号なのであろうが、この号は「法令に基づく場合」としかしていない。その一方で、この場合の取得側への授権は、先述の刑事訴訟法197条2項である。しかし、現状の捜査関係事項照会では、提供側への「授権」も、取得側への授権も概括的にすぎるようにも思われ、こうした規定の仕方であると、照会を受けた事業者は、当該の照会とそれに基づく提供の合法性を判断する余地がほとんどないままに、保有している個人情報を相手方（警察など）から言われるがままに提供せざるを得ないことにならないかが危惧される。そこで、「二重扉モデル」を参照することで、個人情報の提供と取得の双方に対する授権規定の妥当性を個別に検討することが必要であること、特に、捜査関係事項照会においては、提供・取得側の双方に対して、授権規定が二重に概括的であることが明らかになるようにも思われる。

また、「二重扉モデル」と、マイナンバー制度を対比して考えてみると、マイナンバー法の条文上は、例えば「刑事事件の捜査」において、特定個人情報を提供できることになっており、その場合に、個人番号(マイナンバー)の提供を求めることも、特定個人情報を収集・保管することもできることになっている。それゆえ、「刑事事件の捜査」の場面が限定されなければ、犯罪捜査分野での個人番号を含む個人情報(特定個人情報)の授受に歯止めをかけられない構造になっているといえる。そして、特定個人情報の取得に特

化した、個別的な授権規定があるわけでもない。政府側からは捜査関係事項照会で個人番号を使うことが可能であるなどの説明がなされているが³⁴、いずれにしても、取得側の規制を十分に行っておかなければ、警察等が「法令に基づいている」と主張すれば、事業者側は言われるがままに個人番号を含む個人情報を提供せざるを得なくなり、それによって、個人番号を含む情報の授受に対する規律が機能しなくなることにもなりかねない。そこで、「二重扉モデル」を参照することで、現行のマイナンバー制度の課題が示されるとともに、特定個人情報のプライバシー性に応じた、取得側に対する具体的な授権規定の必要性が明らかになるように思われる。

また、先に挙げた JILIS のガイドラインは、個人情報の提供側と取得側の責任との関係でも興味深いものであり、ガイドラインの案では「捜査との関連性がない情報を漫然と開示をした事業者は、本人の権利を侵害したものととして、不法行為責任を負う可能性があることには留意が必要」であるとしたうえで、事業者は、捜査関係事項照会がなされた場合には、捜査関係事項照会書の記載内容から、適法性について確認を行わなければならないとしている。それだけの引用にとどめると、一方的に事業者側に重い責任を課そうとする提言であるかのような誤解を招きかねないところではあるが、捜査は元来秘密に行われる性質を有し、捜査機関と事業者との間には捜査状況についての大きな情報ギャップもあることを指摘したうえで、事業者における関連性の審査にあたって事業者の側で、必要な措置を講じなければならないのは、「明らかに」関連性が疑われる照会の場面に限定されており、事業者側の負担に配慮する姿勢もみせている。ただ、ドイツ流の「二重扉」的な規律にこだわるならば、原則的に取得側の責任であることを明示したり、提供側の責任は限定的なものであることを、正面から指摘したりする余地はあるという

³⁴ 福島みずほ参議院議員の質問主意書と、それに対する政府の答弁書(内閣参質189第136(2015年6月2日))。

ことになるのだろう。このガイドラインは、事業者に対する指針を示そうとするものである以上、そこまでの検討・提言を求めることには難しいところもあることは理解できるとはいえ、取得側（警察）の責任を、どこかの機会でも強調することも必要であろう。その点、「二重扉モデル」を参照することで、提供側の民間事業者の責任と、取得側の警察の責任の重さを、さらに明確に分けられるように思われ、原則的に取得側の責任であることを明らかにしておくことも考えられるだろう。

以上のことから、ドイツの「二重扉モデル」を日本国内の議論において参照することは、捜査関係事項照会やマイナンバー制度における、情報の取得側となる公的機関に対する授権の厳密さの問題を検討する契機となると思われる³⁵、また、「二重扉モデル」は、情報を取得する側により重い責任を負わせるべきであることを示すものとなりうるように思われる。

（3）検討課題

ここまでは、「特定性の要請」や「二重扉モデル」が日本でも参考になるのではないかという方向で述べてきたが、そこには課題もあるだろう。ひとつ、問題となると思われるのは、「特定性の要請」と比例原則の関係であり、「特定性の要請」は比例性の審査の一部にすぎないとみる余地もあるだろう。例えば、目的や侵害閾値が特定されていなければ、措置の適用範囲が広範になり、その結果、比例性も満たせなくなると考えることができる。ただ、「特定性の要請」には、比例性審査の一内容にすぎない要請もあれば、それにとどまらない要請もあり、その限りにおいては重要性があるといえるだろう。なかでも、「授権規定としての特定性」という要請は、十分な授権規定を根拠としない措置の違法性を問うものであり、手段の比例性とは別の観点での

³⁵ 先にも挙げた Bäcker が連邦議会に提出した意見書は、令状に基づく取得要件が緩やかであると、事業者にとって妥当する提供の許可の条件は満たされていない場合にも、個人データを提供せざるを得ないことにもなりうるとの問題を指摘している（Bäcker, Fn. 24, S. 17）。

検討を求めるものであろう。

また、「二重扉モデル」との関係では、情動的措置の憲法上の統制ということであれば、取得側に対する統制が必要であるとすれば足り、「二重」の授権が必要であるとまではする必要はないと考える余地もあるだろう。その点、連邦通信法の合憲性に関する、連邦憲法裁判所の先述の二つの決定をみてもわかるように、ドイツでは提供側に対して個人情報の提供を容認（授権）³⁶する規定が先行して整備されており、照会・取得側に対する授権の必要性は、提供側に対する「授権」規定が既にあるという状況で指摘されるようになったという経緯がある。また、日本においても、個人情報の保護との関係では、個人情報を保有・提供するに至った官民の機関に対する規律がまず求められていたように思われ、情報を取得する側の規律を考える際にも、情報を提供する側に対する規律が必要であることが前提とされていることが一般的であるように思われる。それゆえ、「二重扉モデル」のうち、取得側に対する規律の必要性を強調することも考えられるとしても、どちらの国においても提供側と取得側に対するそれぞれの規律のあり方の問題として、つまり、「二重」の授権の必要性の問題として検討することには、一定の合理性があるように思われる。

さらに、これは「特定性の要請」と「二重扉モデル」の両方に関係することであるが、それらを参照しても、アメリカの議論を基に組み立てられている議論とかみ合わないおそれもある。管見の限りではあるが、アメリカにおいては、刑事手続上の措置の法定は当該措置が合憲であるための要件とはされておらず、法定されていることの意義が指摘される場合であっても、「法定しておいた方がよい」とされるにとどまっているように思われる³⁷。その

³⁶ 情報の提供を民間の事業者に認めることを「授権」とすることの妥当性には異論の余地もあるが、本稿の文脈の限りにおいては、民間の事業者は公的な機関が使用するために個人情報を提供するのであり、「授権」という表現を用いたとしても差支えはないと思われる。

点、「特定性の要請」や「二重扉モデル」をみると、ドイツでは、具体的な法律上の根拠があることが、憲法上必要なものとされていることがわかる。そのため、日本国内の憲法学や刑事訴訟法学において、アメリカのモデルが主流なのであれば、ドイツのモデルを参照するのは難しいのかもしれない。ただ、刑事手続上の情報取得という文脈での「特定性の要請」であれば、日本国憲法においては31条に位置づけられるものとして理解できると思われ³⁷、31条が、基本的には、プロイセンを参考にして作られた明治憲法から引き継がれた規定であることを考えるならば、ドイツの議論を参照して、法定にこだわる議論を展開することは、日本国憲法の下でも必ずしも無駄ではないように思われる。

以上に基づくならば、「特定性の要請」は手段の比例性の要請には還元されない内容も含んでおり、また、「二重扉モデル」を参照して情報を提供する側と取得する側を「二重」に規律するための方策を検討することにも、個人情報保護をめぐる議論や制度の沿革をふまえれば、ある程度の意味があるといえるだろう。また、情動的措置に対する授権の必要性を憲法31条に位置づけることができるのであれば、本稿で扱った分野においてドイツの議論を参照することにも一定の意義があるといえるだろう。それゆえ、本稿で扱ったドイツ国内の議論を日本で参照する上で検討すべき事項も少なくないとしても、ドイツ国内で示されている要請やモデルを日本国内で参照することには、少なからぬ意味があるといえるように思われる。

(4) 小括：日本の議論へのあてはめ

以上のようにして、「特定性の要請」を日本でも参照する場合、特に「授権規定としての特定性」という観点が参考になるように思われる。そして、

³⁷ 拙稿「『GPS 捜査』の憲法上の問題—比較対象としてのアメリカ国内の議論—」福岡大学法学論叢63巻1号(2018年)1頁以下。

³⁸ 拙著、前掲注(4)214頁。

ドイツの「二重扉モデル」を日本国内で参照することで、情報の取得側の規律が検討課題であることが明らかになるだろう。本稿で扱った議論を日本で参照する上では検討課題も少なくないが、それらはいずれも日本国内でドイツの議論を参照することの意義を否定するものとはならないと考えられる。それゆえ、本稿で取り上げたようなドイツの議論は、日本の議論においてもそれなりに役に立つとはいえるだろう。

4. まとめ：情動的措置を授権する規定の「特定性」と「二重扉」

— ドイツの議論 —

以上のように、ドイツ国内の近年の判例では、授権規定の特定性を慎重に審査する傾向がみられる。そして、「二重扉モデル」が提唱される以前から現在に至るまで、個人データの提供と取得にそれぞれ別々の授権規定が必要であるという考え方は、ドイツ国内において一定程度の定着をみせている。問題は、それらの枠組みを日本において参照する価値であるが、「特定性の要請」や「二重扉モデル」を日本で参照することは、特に、情動的措置とその「授権規定」の憲法上の問題の検討を、より慎重に行う契機となりえるように思われる。

おわりに

以上が本稿での検討を通じて導かれた結論であるが、本稿において論じられなかったことも少なくない。まず、本稿で取り上げた「特定性の要請」のうち、「授権規定としての特定性の要請」は、既に日本でも検討されている争点である可能性もある。「医療関連性が『医行為』の要件だとすれば違憲の疑義が生じる」とした、いわゆる「タトゥー訴訟」の大阪高裁判決の説明は³⁹、医師法が広く解釈され、医師法が制定されたのちに広まった「タトゥー」の彫師にも適用されるとする場合に生じる問題を指摘するものであろう。本

稿で取り上げた、「授権規定としての特定性」の検討は、いわゆる「適用審査」の一部であるにとどまるかもしれない。ただ、本稿の関心とは異なる分野での事例であることもあり、両者の関係については検討できなかった。また、情報自己決定権の制約の正当化に関する日独両国の状況の違いについては、統治機構論の問題としても検討する余地がある⁴⁰。統治に関係する規定と、人権の正当化要件との関係についても、立ち入った検討が必要であるが、本稿ではそれを行うには至らなかった。日本国憲法の31条と41条の関係に関する検討も含めて、今後の検討課題としたい。さらに、本稿で挙げたような、「特定性の要請」から導かれる様々な要請が、「手続の適正」原理に収まるのかには疑問も示されており⁴¹、それについても別の機会での検討としたい。

³⁹ 大阪高判2018年11月14日（判時2399号88頁）。解説として、曾我部真裕「判批」判例時報2415号（2019年）132頁以下（判例評論）。また、同「タトゥー施術規制をめぐる憲法問題」小山剛・新井誠編『イレズミと法 大阪タトゥー裁判から考える』（尚学者、2020年）92頁以下<93頁以下>。

⁴⁰ 法律時報92巻13号（2020年）14頁（櫻井智章）。

⁴¹ 玉蟲由樹「書評 實原隆志『情報自己決定権と制約法理』（信山社、2019年）」憲理研叢書28号（2020年）247頁以下<250頁>。