「クラウド上に保管された電子的証拠に対する捜索・押収についての日米比較法的研究」に関する研究成果報告書

研究代表者　　川　島　享　祐　　立教大学法学部　准教授

１ はじめに

現代社会においては、情報通信技術の発展に伴い、個人に関係する大量の情報が、クラウドサービス等を通じて電子データの形で保存されており、その中には、犯罪に関係する証拠も含まれる。そのため、犯罪の捜査を行う捜査機関としては、このようなクラウド上に保管された電子的証拠を取得する必要性が高い。本研究は、このような捜査機関による電子的証拠の捜索・押収に対して、どのような法的規律を及ぼすべきかという問題を、アメリカ法と日本法を比較しつつ検討するものである。具体的には、本研究は、①令状主義の要請が電子的証拠に対してどのように及ぶかという問題、②電子的証拠は第三者が管理するサーバに保管されているという点が、法的規律にどのように影響するかという問題、③電子的証拠の収集に際して生じる国際法上の問題を検討した。

本報告書においては、本研究の研究成果のうち、インターネット・サービス・プロバイダ（以下「ISP」という）によるデータの予備的保存の問題に焦点を当てて報告する。この問題は、ヨーロッパにおいてはデータ・リテンションの問題として知られている。本報告書においては、国家が法律により一般的かつ包括的に、又は、捜査機関が個別事案ごとに、ISP に対して、通信履歴の保存を義務付けることに、どのような法的な（とりわけ憲法上の）問題があるかを検討する。

実はこの問題は、後述するように、筆者が本研究を実施したアメリカにおいては顕在化していない。しかし、上記①ないし③の問題のうち、②の問題を調査していくうちに、アメリカとヨーロッパ・ドイツと日本とでは、第三者たる ISP が保管しているデータを捜査機関が取得する際の法的規律がまったく異なっており、その背後に、本報告書のテーマであるデータの予備的保存の義務付けに関する EU 規模の議論があることが判明した。そして、この問題は、まさに今、我が国において電気通信事業者に対する通信履歴の保存の義務付けという形で顕在化しており[1]、各国における法的規律を紹介する価値は高いといえる。

本報告書においては、まず、ドイツ法・EU 法における ISP によるデータの予備的保存に関する議論を紹介したうえで（II.）、アメリカ法における議論状況を検討する（III.）。

２ ドイツ法・EU 法[2]

2-1 データ保存指令の制定

ヨーロッパにおいては、約 20 年にわたって、ISP に対してデータの予備的保存を義務付けることが可能かという問題が司法の場で争われてきたが、これは、2006 年に欧州連合（EU）でデータ保存指令（Date Retention Directive）[3]が採択されたことに端を発する。これは、2004 年 3 月にマドリード列車爆破テロ事件が起きたことを受けて、同月の欧州理事会（European Council）においてテロ撲滅宣言が採択され、サービス・プロバイダによる通信トラッフィックデータの保存に関するルールの制定のための措置の検討が指示されたこと

[1] 「通信履歴の保存の在り方について（要請）」（令和 7 年 9 月 16 日総情適第 48 号、総基用第 92 号）参照。

[2] *See generally,* Adam Juszczak & Elisa Sason, Recalibrating Data Retention in the EU: The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning?, 2021 eucrim 238 (2021)；Maria Tzanou, The Fundamental Right to Data Protection：Normative Value in the Context of Counter-Terrorism Surveillance (2017)；Marion Albers, Data Retention in Germany, in European constitutional Courts towards Data Retention Laws (M. Zubik et al. eds. 2021)；Jan Podkowik et al., Judicial Dialogue on Data Retention Laws: A Breakthrough for European Constitutional Courts?, 19 I•CON 1597 (2021).

[3] Directive 2006/24/EC.

を契機とする [4]。データ保存指令の目的は、電気通信事業者によって生成又は処理される一定のデータが、重大な犯罪の捜査、解明及び訴追のために利用可能となることを確保するために、そのようなデータの保存を電気通信事業者に対して義務付ける、加盟国の規定の調和（harmonise）を図るというものであった（同指令1条1項）。

データ保存指令により、加盟国は、電気通信事業者において一定のデータが保存されることを確保する措置をとる義務を負い（同指令3条）、また、保存されたデータが、個別事案において、権限ある当局のみに対して国内法に従い提供されることを確保するための措置をとる義務を負う（同指令4条）。同指令の下で保存の対象となるデータは、トラフィックデータと位置データ（traffic and location data）、及び、利用者等の同定に必要な関連データとされ、電気通信の内容に関するデータはその対象とならない（同指令5条）。また、データの保存期間は、通信の日から6か月ないし2年とされた（同指令6条）。

その後、データ保存指令に基づき、紆余曲折を経て、加盟国各国でデータ保存法が制定された。データ保存指令の有効性は、その発効後からEU司法裁判所（CJEU）において争われたが、同裁判所の当初の判例は、データ保存指令の制定権限に関する形式的なものであり、それによる基本権の制約について判断するものではなかった。そのような中、加盟国各国の憲法裁判所等が、データ保護指令を実施する国内法規定が各国憲法や欧州人権条約に適合するかを判断することとなった [5]。

2-2 ドイツ連邦憲法裁判所の違憲判断（2010年）

（１）データ保存指令の国内法化

本報告書が検討対象とするドイツにおいても、2008年にデータ保存指令が国内法化（transposition）された。これは、大きく以下の3つの内容を構成要素としていた [6]。

第1は、電気通信事業者に対して、電気通信事業によって生成された一定の個人データを、業務目的のために必要な期間を超えて保存することを義務付ける規定である。電気通信法旧96条は、電気通信事業者に対して、業務目的に必要な限度での電気通信データの保存と利用を許容する規定であるが、同法旧113条aは、これを超えて、一定の電気通信データを6か月間保存するよう義務付けるものであった。

第2は、電気通信事業者に対して、一定の要件の下で一定の当局に対してこれらのデータを提供することを義務付ける規定である。電気通信法113条bは、データ利用の目的について、犯罪の訴追、公共の安全に対する重大な脅威に対する防御、諜報活動の実施、という3つの目的を限定列挙していた。

第3は、当局がデータの送信を要請し、一定の目的のために当該データを利用することを認める規定である。本報告書が検討対象とする犯罪の訴追に関しては、刑訴法100条gが、刑事司法機関によるデータの取得に関する要件を規定している。

（２）連邦憲法裁判所による違憲判断

ドイツの連邦憲法裁判所は、2010年3月2日の判決で、このような国内法の各規定は電気通信の秘密を保障するドイツ基本法10条1項に適合しないと判断した [7]。

本判決は、まず、基本法10条1項の保護範囲に関して、電気通信の秘密は、通信内容だけでなく、通信に関する事情すなわち非内容情報にも及ぶと述べる。そのうえで、電気通信事業者に対して、電気通信データを取得し、保存し、国家機関に送信するよう求める上記国内法の規定は、それぞれ基本法10条1項に介入（Eingriff）するものであるとする [8]。そして、本判決は、そのような基本権への介入が実質的に正当化されるかを判断するために、比例原則を適用する [9]。

ここで注目に値するのは、本判決が、基本権に介入する規制手段の投入によって得られる利益と失われる

[4] European Council, Declaration on Combating Terrorism, 25 March 2004.

[5] *See* Podkowik et al., *supra* note 2, at 1600-03. 具体的には、2008年から2012年の間に、ブルガリア（2008年）、ルーマニア（2009年）、ドイツ（2010年）、キプロス（2011年）、チェコ（2011年）において、このような判断がなされた。

[6] *See* Albers, *supra* note 2, at 118-20.

[7] BVerfGE 125, 260=NJW 2010, 833.

[8] BVerfGE 125, 260=NJW 2010, 833, Rn 188-90.

[9] BVerfGE 125, 260=NJW 2010, 833, Rn 204ff.

利益の権衡が保たれていることを要求する狭義の比例性の審査において、電気通信のトラフィックデータを6か月間保管することを義務付けることによる介入の重大性を指摘する際に、データの情報価値（Aussagekraft）が広範囲にわたることを強調している点である。すなわち、まず、トラフィックデータであっても、場合によっては、データ自体から、又はそれをさらなる捜査の連結点とすることで、市民の社会的な環境や個人の活動について深い洞察が得られることがある。また、トラフィックデータは通信内容に関するデータではないが、包括的かつ自動的に分析をすることで、内密領域に関してまで十分な内容的な推認が導かれ得る。さらに、トラフィックデータは、長期間観察されると、その組み合わせから、社会的・政治的な所属や、個人的嗜好、傾向、弱点などを詳細に明らかにし得る。そして、トラフィックデータについてこのような利用を可能とする保管は、基本権への重大な介入を基礎づけると判示した[10]。

そのうえで、本判決は、電気通信法113条aのような6か月間の保管義務は、当然に憲法上禁止されるわけではないとしつつも[11]、電気通信のトラフィックデータの予備的な保存が狭義の比例性を充足するためには、とりわけ、①データセキュリティ（Datensicherheit）の基準、②データ利用の範囲と要件、及び、③データ利用の透明性を確保するための措置やそのための不服申立て手段（Rechtsschutz）及び違反に対する制裁に関して、特別な憲法上の要求に基礎づけられたものでなければならないとする[12]。そして、本判決は、結論として、本件の国内法はこれらの憲法上の要求を満たすものではなく、電気通信法113条a、113条bは、基本法10条1項に適合せず、刑訴法100条gは、電気通信法113条aに基づいて保管されるデータの引渡しを許容する限りにおいて、同条項に適合しないと結論付けた[13]。

このように本判決は、ISPに対するデータの予備的保存の義務付けは、基本法10条1項が保障する電気通信の秘密への介入になるとしつつも、一般的かつ包括的な保存を一定期間義務付けたとしても当然に比例原則には違反しないとし、しかし、保存による介入の重大性にかんがみれば、①ないし③について特別な憲法上の要求がなされるとしている。

このうち、①のデータセキュリティの確保は、データを予備的に保存することそれ自体から生じる問題に対応するものといえる。これに対して、②のデータ利用の範囲と要件、及び、③データ利用の透明性の確保は、捜査機関によるデータの取得といった、保存されたデータの利用を規律するものである。そして、データの保存とその利用の関係について、本判決は、データ利用の範囲と要件（②）に関する判示の中で、データの保存に存する介入が重大であればあるほど、データ利用の要件と範囲が狭く限定されていなければならないと述べたうえで、実際上すべての電気通信のトラフィックデータを、特定の犯罪の捜査といった理由なく系統立って保存（anlasslos systematische Speicherung）することによって獲得される集積データ（Datenbestände）を利用するためには、特に高度の要件が必要であるとする。この理由として、本判決は、このデータの分析は、私的生活に深く入り込む推認や、場合によっては詳細な人格と行動に関するプロファイルを可能にするので、このデータの援用は、電気通信の内容の傍受よりも重要でないと直ちにいうことはできないのであり、むしろ、特別に高度の公共の福祉の利益に奉仕する場合にのみ、比例性があると見なされるという点を指摘している[14]。

このように、本判決は、ISPに対するデータの予備的保存の義務付けについて、トラフィックデータという通信の内容情報ではない情報であっても、それが集積されることで、私生活や人格・行動に対する詳細が明らかになり得るということから、保存自体による介入の重大性を基礎づけている。そのうえで、本判決は、データの保存に焦点を当てつつも、その利用についても合わせて検討し、保存自体による介入の重大性から、捜査機関による取得というデータの利用に関する厳格な要請を導いているといえる。

2-3 EU司法裁判所のデータ保存指令に対する無効判断

その後、EU司法裁判所は、2014年のDigital Rights Ireland判決[15]において、データ保存指令の有効性

[10] BVerfGE 125, 260=NJW 2010, 833, Rn 211-12.

[11] BVerfGE 125, 260=NJW 2010, 833, Rn 219.

[12] BVerfGE 125, 260=NJW 2010, 833, Rn 220.

[13] BVerfGE 125, 260=NJW 2010, 833, Rn 306.

[14] BVerfGE 125, 260=NJW 2010, 833, Rn 226-27.

[15] CJEU, Judgment of 8 April 2014, Digital Rights Ireland and Others (C-293/12 and C-594/12) ECLI:EU:C:2014:238. (hereinafter Digital Rights Ireland)

そのものについて検討を加え、これを無効と判断した。

本件において、EU 司法裁判所は、EU 基本権憲章（以下「憲章」という）7 条、8 条及び 11 条に照らしてデータ保存指令の有効性を判断するよう求められた。同 7 条は、「私的並びに家族の、生活、住居及び通信を尊重される権利」を、同 8 条は「自らに関する個人データの保護に対する権利」を、同 11 条は「表現の自由の権利」を保障している [16]。もっとも、本判決が判断を示したのは前二者に関してであり [17]、本報告書でもこれらに焦点を当てる。

本判決は、まず、憲章 7 条について、データ保存指令によって電気通信事業者に対して課される、個人の私的生活や通信に関するデータの一定期間の保存義務は、それ自体が、憲章 7 条によって保障される権利への介入を構成するとする。また、権限ある国内の当局による当該データへのアクセスは、この基本権に対するさらなる介入を構成するという。加えて、憲章 8 条についても、同様に、データ保存指令は、憲章 8 条によって保障された個人データの保護に対する基本権にも介入すると述べる [18]。

もっとも、憲章 52 条 1 項は、憲章が認める権利及び自由の行使に対する制限は、比例原則に服し、「それが必要なときであって、かつ連合の認める一般的利益の目標に真に合致するとき又は他人の権利及び自由の保護の必要性に真に合致するときにのみ設けることができる」と規定する [19]。そのため、本判決は、データ保存指令による憲章上の権利への介入が、同条に照らして正当化されるかを検討している。

まず、一般的利益の目標に真に合致するかという点について、本判決は、データ保存指令の実質的な目標（material objective）は重大な犯罪の捜査、解明及び訴追のために、データを利用可能とすることであり、権限のある国内の当局がデータにアクセスできるようにそれを保存することは、一般的利益の目標を真に満たすとする [20]。もっとも、介入の比例性について、本判決は、まず、本件では、私的生活を尊重される基本権に照らした個人データの保護が果たす重要な役割、及び、データ保存指令が生じさせる当該権利に対する介入の範囲及び重大性にかんがみ、EU の立法府の裁量は減じられ、当該裁量の審査は厳格に行われるべきであるとする [21]。

そして、本判決は、比例原則の当てはめにおいて、①データ保存指令は、広範囲にわたるやり方で、すべての個人、すべての電気通信、すべてのトラフィックデータを、重大な犯罪との戦いという目標に照らして行われる区別、制限又は例外なく、対象とするものであるが、②対象となる「重大な犯罪」や、権限を有する国内の当局のデータに対するアクセス及びその事後的な利用に関する実体的・手続的要件を内容としていないなど、当局によるアクセスの客観的な基準を定立しておらず、また、③データのカテゴリや目標に応じた保存期間について区別がないと述べ、厳格に必要なものに現実に限定されることを確保する規定によって、

[16] EU 基本権憲章
第 7 条　私的生活及び家族生活の尊重
あらゆる人は、私的並びに家族の、生活、住居及び通信を尊重される権利を有する。
第 8 条　個人データの保護
①　あらゆる人は、自らに関する個人データの保護に対する権利を有する。……
第 11 条　表現及び情報の自由
①　あらゆる人は、表現の自由の権利を有する。……
翻訳に際しては、衆議院憲法調査会事務局『欧州憲法条約――解説及び翻訳』（衆憲資 56 号、平成 16 年 9）（https://www.shugiin.go.jp/internet/itdb_kenpou.nsf/html/kenpou/chosa/shukenshi056.pdf/$File/shukenshi056.pdf）を参照した。

[17] Digital Rights Ireland, *supra* note 15, para. 69-70.

[18] *Id.* para. 34-36.

[19] 第 52 条
①　この憲章が認める権利及び自由の行使に対するいかなる制限も、法により定められ、かつ当該権利と自由の本質を尊重するものでなければならない。比例原則に服しつつ、制限は、それが必要なときであって、かつ連合の認める一般的利益の目標に真に合致するとき又は他人の権利及び自由の保護の必要性に真に合致するときにのみ設けることができる。

[20] Digital Rights Ireland, *supra* note 15, para. 41-44.

[21] *Id.* para. 48.

介入が厳密に制限されているとはいえないと判示した[22]。また、④電気通信事業者によって保存されるデータの安全性（security）と保護についても、濫用のリスクや違法なアクセス・使用に対する効果的な保護を確保する十分な保護手段を規定していないとした[23]。そして、これらを踏まえ、データ保護指令は比例原則に違反し、無効であると結論付けた[24]。

これらの要素のうち、①③④は、データの保存に関して限定が不十分であることを指摘するものである一方、③は、データへのアクセスという、保存されたデータの利用に対する規制が不十分であることを指摘するものといえる。このように、本判決もドイツの連邦憲法裁判所と同様、データの保存に焦点を当てつつも、その利用に対する規制の十分性を合わせて検討しているといえる。

2-4 その後の EU 法――ドイツ法との関係を中心に

Digital Rights Ireland 判決は、データ保存指令を無効としたが、同指令を国内法化した各国の立法の有効性については検討していないため、そのような国内法に対して直接的な影響があったわけではない。EU 加盟国の中には、Digital Rights Ireland 判決を受けてそのような国内法を無効と判断するものもあり、また、限定的な改正をするものもあったが、同判決の認定と要件がどの程度国内法に影響するのかは不明確であった[25]。そのため、同判決後、このような国内法の EU 法適合性が、EU 司法裁判所で争われることになった。

（１）Tele2/Watson 判決（2016 年）

この点についての最初の EU 司法裁判所の判決が、Tele2/Watson 判決である[26]。本件においては、データ保存指令を国内法化したスウェーデンとイギリスの規定が、通信の秘密を保護する EU の ePrivacy 指令[27]の下で許容されるかが問題となった。

本判決によれば、ePrivacy 指令は、憲章 7 条及び 8 条に規定された権利の完全な尊重を確保しようとするものである。すなわち、EU の立法者は、同指令により、個人データとプライバシーの高レベルの保護が、用いられている科学技術にかかわらず、すべての電気通信サービスに関して保障され続けることを確保しようとしたとされる。そして、そのような規定の一つが、同指令 5 条 1 項の通信の秘密の保護であるという[28]。

ePrivacy 指令 5 条 1 項によれば、利用者本人以外の者は、利用者の同意なく、電気通信に関するトラフィックデータを保管することが原則として禁止され、同指令 15 条 1 項に従って合法に権限を付与された場合と場合と通信の伝達のために必要な技術的保存の場合に、例外的にこれが許容される[29]。このうち、本件において重要なのは、犯罪の捜査や訴追という目的のために、同指令 5 条が保障する通信の秘密を制限する立法措置を採用することを許容する、同指令 15 条 1 項である[30]。

[22] *Id.* para.56-65.

[23] *Id.* para.66.

[24] *Id.* para.71.

[25] Juszczak & Sason, *supra* note 2, at 240.

[26] CJEU, Judgment of 21 December 2016, Tele2 Sverige and Watson and Others (C-203/15 and C-698/15) ECLI:EU:C:2016:970. (hereinafter Tele2/Watson).

[27] Directive 2002/58.

[28] *Id.* para.82-84.

第 5 条　通信の秘密（Confidentiality of the communications）

① 加盟国は、国内法を通じて、公衆通信網及び公に利用可能な電気通信サービスを用いた通信及び関連するトラフィックデータの秘密を確保する。とりわけ、加盟国は、第 15 条 1 項に従って合法に権限を付与された場合を除き、利用者以外の者による、当該利用者の同意のない通信及び関連するトラフィックデータの聴取、記録、保管、その他の種類の傍受又は監視（listening, tapping, storage or other kinds of interception or surveillance）を禁止する。本項は、秘密性の原則を害することなく通信を伝達するために必要な技術的保管を妨げない。

[29] Tele2/Watson, *supra* note 26, para.85.

[30] 第 15 条　指令 95/46/EC の特定条項の適用

① 加盟国は、当該制限が、指令 95/46/EC〔データ保護指令〕第 13 条第 1 項において言及される、国家の安全保障（すなわち、自国の安全保障〔State security〕）、防衛、公共の安全、又は、犯罪若しくは

本判決は、同指令 15 条 1 項の解釈に関して、同条項は、加盟国に対して、通信の秘密と関連するトラフィックデータの秘密性を確保する原則的義務の射程を制限するものであるから、この規定は、厳格に解釈されなければならないと述べる。とりわけ、同指令 15 条 1 項 3 文は、通信の秘密を制限する立法措置が EU 法の一般原則に従うものであることを要求しているところ、この一般原則は憲章によって保護される一般原則と基本権を含むので、同指令 15 条 1 項の解釈に当たっては、憲章 7 条で保障されるプライバシー権、及び、憲章 8 条で保護される個人データの保護に対する権利の重要性が考慮されなければならないとする [31]。

そのうえで、本判決は、同指令 15 条 1 項や憲章 52 条 1 項等が定める比例原則を適用する。その際に、本判決は、本件における国内法が、すべての電気通信手段に関する、すべての契約者及び登録利用者のすべてのトラフィックデータと位置データの一般的かつ無差別的な保存を規定するものであり、かつ、電気通信事業者に対して、そのデータを、例外なく、体系的かつ継続的に保存する義務を課すものであることに注意が必要であると述べる [32]。そのうえで、本判決は、保存が義務付けられているデータの内容・性質と基本権に対する介入の重大性について、次のように指摘する。

まず、保存が義務付けられているデータの内容・性質について、本判決は次のように述べる。本件の国内法によって保存が義務付けられるデータは、送信元と送信先を追跡・特定し、通信の日時、期間、種類を特定し、利用者の通信装置を特定し、移動式通信装置の場所を明らかにし得る。また、このデータは、とりわけ、契約者又は登録利用者の名前と住所、架電者の電話番号、架電された電話番号、及びインターネット・サービスの IP アドレスを内容としており、契約者又は登録利用者と通信をした者や、その通信が行われた場所の特定を可能にするとともに、ある期間内に、契約者又は登録利用者が、一定の人と通信をした頻度を明らかにする。このように、本件の国内法によって保存が義務付けられるデータは、全体としてみると、日常的な習慣、永続的又は一時的な居住地、日常的その他の移動、行われる活動、それらの者らの社会的な関係、それらの者が頻繁に出入りする社会的環境といった、データが保管される者の私生活に関するとても正確な結論を導くことを可能とし、とりわけ、関係する個人のプロファイル、すなわち、プライバシー権を考慮すると、現実の通信内容と同等にセンシティブな情報を確立する手段を提供する [33]。

そして、本判決は、このような立法に伴う、憲章 7 条及び 8 条に規定された基本権に対する介入は、とても広範囲にわたるものであり（very far-reaching）、特に重大なものであると考えられなければならないとする。それは、契約者や登録利用者に通知されることなくデータが保存されるという事実は、関係人に対して、私的生活が継続的な監視の対象となっていると感じさせる可能性があるからである [34]。

その上で、本判決は、データの保存を原則とし、保存されるデータと公共の安全に対する脅威の結びつきを要求しない国内法は、厳格な必要という限界を超えていると判示した。そして、本判決は、憲章 7 条、8 条及び 11 条、並びに 52 条 1 項に照らして読んだとき、同指令 15 条 1 項は、犯罪対策を目的として、すべての電気通信手段に関して、すべての契約者及び登録された利用者のすべてのトラフィックデータと位置データを、一般的かつ無差別的に（general and indiscriminate）保存することを規定する国内法を排除することを規定するものと解釈されなければならないと結論付けた [35]。

これまで、ドイツの連邦憲法裁判所の判例や EU 司法裁判所の Digital Rights Ireland 判決は、ISP に対するデータの予備的保存の義務付けについて、データの保存に焦点を当てつつも、その利用に対する規制も

> 電気システムの無権限利用の予防、捜査、解明若しくは訴追を保護するために、民主主義社会の中で必要性、適合性、及び比例性が認められる措置を構成する場合には、本指令第 5 条、第 6 条、第 8 条第 1 項、第 2 項、第 3 項及び第 4 項、並びに第 9 項に規定される権利又は義務の射程を制限するための立法措置を採用することができる。この目的のため、加盟国は、とりわけ、本項に規定された事由に基づいて正当化される限定された期間にわたるデータの保存（retention）を規定する立法措置を採用することができる。本項で言及されるすべての措置は、欧州連合条約第 6 条及び第 2 項において言及されるものを含む、共同体法の一般原則（the general principles of Community law）に従わなければならない。

[31] Tele2/Watson, *supra* note 26, para.89, 91-93〔憲章 11 条の表現の自由についても言及しているが、ここでは省略する〕.

[32] *Id.* para.94-96.

[33] *Id.* para.98-99.

[34] *Id.* para.100.

[35] *Id.* para.104-07.

合わせて検討していた。これに対して、本判決は、専らデータの保存の問題に焦点を当て、その利用に対する規制は重視していない。

この点は、本判決の4年後に下されたQuandrature du Net判決[36]によってより明確になる。同判決は、「トラフィックデータと位置データの保存は、それ自体で、一方で、利用者以外の者が当該データを保管することを禁止する〔ePrivacy〕指令5条1項からの逸脱を構成し、他方で、憲章7条及び8条に規定された、私的生活の尊重及び個人データの保護に対する基本権への介入を構成する」のであり、「そのようなデータへのアクセスは、それについてなされる事後的な利用に関わらず、〔上記の〕基本権への別個の介入であるので、保存されたデータが事後的に利用されたか否か〔は〕無関係である」と述べている[37]。

このように、Tele2/Watson判決以降、EU司法裁判所の判例は、ISPに対するデータの予備的保存の義務付けについて、データの保存とその利用に対する規制を切り離し、前者の問題に焦点を当てるようになる[38]。

（2）SpaceNet/Telekom Deutschland判決（2022年）

このように、Tele2/Watson判決は、「犯罪対策を目的として、すべての電気通信手段に関して、すべての契約者及び登録された利用者のすべてのトラフィックデータと位置データを、一般的かつ無差別的に保存することを規定する国内法」はePrivacy指令15条1項の下で認められないと判示した。もっとも、同判決は、ISPに対してデータの予備的保存を義務付けることが一切禁止されるわけではないということも示唆していた[39]。その後、EU司法裁判所は、いかなる目的の下、いかなる範囲であればこれが正当化されるのかについて検討していくことになる。ここでは、本報告書の検討対象であるドイツ法についてこの点を検討した、2022年のSpaceNet/Telekom Deutschland判決[40]を検討しよう。

本判決は、Tele2/Watson判決と同様に、通信の秘密を保障するePrivacy指令と憲章7条、8条及び11条との関連を指摘する[41]。もっとも、本判決は、同指令15条1項は加盟国に対して通信の秘密を例外的に制限する立法措置を許容しており、その限りにおいて、同条項は、憲章7条、8条及び11条は絶対的な権利ではないと指摘する。そして、様々な利益や権利の間のバランスをとること、及び、そのようなバランスを可能にする法的枠組みを確立することが必要であるという点を強調する[42]。

そのうえで、本判決は、そのようなバランスをとるための手段である比例原則の下で、ePrivacy指令15条1項に基づいてとられる措置によって追求される公共の利益の目標には、それぞれの重要性に応じた序列（hierarchy）がある点、及び、そのような措置によって追求される目標の重要性は、それに伴う介入の重大性に比例していなければならないという点を指摘する[43]。そして、そのような措置の目標ごとに、許容される措置を検討している。

まず、①国家安全保障という目標は、同指令15条1項に掲げられたその他の目標を上回るものであり、加盟国が、真の、現在する又は予見可能な国家安全保障に対する深刻な脅威に直面している場合には、加盟国は、一定の条件の下で、一般的かつ無差別的に、トラフィックデータと位置データの保管を義務付けることができるとする[44]。

次に、②犯罪の予防、捜査、解明、訴追が目標である場合については、重大な犯罪に対する対応（combat）

[36] CJEU, Judgment of 6 October 2020, La Quadrature du Net and Others (C-511/18, C-512/18 and C-520/18) ECLI:EU:C:2020:791.

[37] *Id.* para.115-16.

[38] 以下で見るSpaceNet/Telekom Deutschland判決においても、同旨の判示がなされており（SpaceNet/Telecom Deutschland, *infra* note 40, para.60）、同判決においてはさらに進んで、データの保存と保存されたデータへの当局によるアクセスは、別個の介入を構成するから、アクセスの規制によって、一般的な保存による重大な介入を限定又は回復することはできないと指摘されている（*Id.* para.91）

[39] Tele2/Watson, *supra* note 26, para.108-11.

[40] CJEU, Judgment of 20 September 2022, SpaceNet and Telecom Deutschland (C-793/19 and C-794/19) ECLI:EU:C:2022:702. (hereinafter SpaceNet/Telecom Deutschland)

[41] *Id.* para.51-62.

[42] *Id.* para.63-65.

[43] *Id.* para.66-71.

[44] *Id.* para.72.

という目的のために、トラフィックデータと位置データの一般的かつ無差別的な保存を義務付ける国内法は、厳格な必要性という限界を超え、正当化され得ないと指摘する[45]。しかし、指令15条1項は、重大な犯罪に対する対応と公共の安全に対する重大な脅威の予防を目的とする下記の立法的措置を排除しないとする。

第1は、トラフィックデータと位置データの、対象を限定した保存（targeted retention）である。このデータの保存は、客観的で差別的でない要素に基づき、対象者のカテゴリにより、又は地理的な基準を用いて限定される[46]。

第2は、インターネットの接続元に割り当てられたIPアドレスの一般的かつ無差別的な保存である。この保存は、厳格に必要な期間に限定される[47]。本判決は、これが許容される理由として、オンラインで遂行される犯罪、とりわけ児童ポルノの取得・頒布等の犯罪については、IPアドレスが犯人特定のための唯一の方法であるという点を強調している[48]。

第3は、電気通信システムの利用者の市民識別情報（civil identity）に関するデータの一般的かつ無差別的な保存である[49]。

第4は、トラフィックデータと位置データの迅速保存（expedited retention/quick freeze）である。これは、電気通信事業者に対して、有効な司法審査を経た管轄当局の決定によって、一定期間、当該事業者が所持するトラフィックデータと位置データを迅速に保存するよう義務付けるものである[50]。

3 アメリカ法

次に、ISPに対するデータの予備的保存の義務付けに関する、アメリカ法における議論状況を検討する。まずは、連邦憲法第4修正が、ISPが保管するデータについてどのような保護を及ぼしているのかを確認したうえで（1.）、連邦の制定法である保管通信法（Stored Communications Act 〔SCA〕）の関連規定について検討する。

3-1 第4修正とISPが保管するデータ

アメリカの連邦憲法第4修正は、第1文で「不合理な捜索・押収」を禁止し（合理性条項）、第2文で、令状は、「相当な理由」に基づき発せられ、かつ、捜索場所と押収対象物を明示するものでなければならないことを定める（令状条項）[51]。この合理性条項と令状条項の関係には争いがあるが、以前の判例は、令状によらない捜索・押収は原則として不合理であり、例外的に令状がなくてもよい場合があると解しており、現在でも、令状要請（warrant requirement）の原則とその例外という形で判例法理が整理されることが多い[52]。このような第4修正の構造を踏まえ、捜査機関の行為が第4修正に違反するかを判断する際には、まず、①それが「捜索」又は「押収」に該当するかが判断され、これに該当する場合には、②それが「不合理」といえるか、すなわち、令状要請を充足し又は令状要請の例外に該当するかが判断される[53]。

第4修正の「捜索」該当性（①）について、連邦最高裁は、1967年のKatz判決[54]以降、プライバシーの

[45] *Id.* para.74.
[46] *Id.* para.75.
[47] *Id.* para.75.
[48] *Id.* para. 100.
[49] *Id.* para.75.
[50] *Id.* para.75.
[51] 第4修正
身体、住居、書類及び所有物について、不合理な捜索・押収（拘束）を受けることない人民の権利は、侵されてはならない。いかなる令状も、宣誓又は確約によって支持される相当な理由に基づき、かつ、捜索されるべき場所及び押収（拘束）されるべき人又は物を明示するものでなければ、発せられてはならない。
[52] *See* Joshua Dressler et al., Understanding Criminal Procedure Vol. 1: Investigation 175-83 (8th ed. 2021).
[53] *See id.* at 62-64.
[54] Katz v. United States, 389 U.S. 347 (1967).

合理的期待テストを用いている。これによれば、捜査機関の行為により対象者のプライバシーの合理的な期待が侵害される場合には、「捜索」が生じる[55]。プライバシーの合理的期待テストの下、第4修正は、インターネットの世界とは区別された物理世界において、閉鎖空間内部の情報についてはプライバシーの合理的期待を認め、その取得に関して保護を及ぼすのに対して，その外部の情報取得に関しては保護を与えない[56]。

また、第4修正に関しては、第三者法理（third party doctrine）と呼ばれる法理が、判例により形成されている。これによれば、ある者は、第三者に任意に引き渡した情報についてプライバシーの合理的期待を有さず、第4修正の保護を受けないとされる[57]。連邦最高裁は、これまで、銀行が保管する顧客記録や、ペンレジスターによって得られる電話利用者の電話番号について、第三者法理により第4修正の保護を否定してきている[58]。

この第三者法理によれば、ISP が保管するインターネット利用者の通信に関する情報（通信の内容情報と非内容情報）も、第4修正によって保護されないということになり得る。現に、2010年の Warshak 判決まで、この点について不明確な状況であった[59]。

しかし、第6巡回区控訴裁判所は、2010年の Warshak 判決において、通信の内容情報である電子メールを ISP から取得することは第4修正の「捜索」であり、令状が必要であると判示した[60]。これは、通信の内容情報の限度で第三者法理を否定し、第4修正の保護を及ぼすものと理解できる。同判決は連邦の巡回区控訴審レベルのものであるが、現在ではその他の法域においても、同様の見方が受け入れられつつある[61]。他方で、非内容情報の取得については、なお第三者法理が妥当し、第4修正の適用は否定される[62]。

このように、アメリカ法においては、通信の内容情報と非内容情報とが区別され、前者に対してのみ第4修正の保護が及ぼされている。この法的規律の基礎にある発想は、物理世界における第4修正の規律を、類推によりインターネットの世界にも及ぼす、というものであると見ることができる。すなわち、まず、前述のように、第4修正は、ⓐ物理世界において、閉鎖空間内部の情報取得に関して保護を及ぼすのに対して，その外部の情報取得に関しては保護を与えない。また、②物理世界において，第三者に任意に委ねられた情報は第三者法理により第4修正の保護が及ばないが，通信に関しては，例外的に第4修正の保護が及ぼされることがある。この発想により、物理世界において、封筒という閉鎖空間内部の手紙（＝通信の内容情報）の閲読は第4修正の「捜索」に該当するが、封筒の宛名（＝非内容情報）の確認は「捜索」ではない。この発想は、既に電話による通話に及ぼされており、電話の内容（＝通信の内容情報）の傍受は「捜索」だが、電話番号（＝非内容情報）の把握は「捜索」ではない[63]。インターネットの世界における通信の内容情報と非内容情報との区別も、同様の発想を類推して応用することでもたらされたものと理解することができる[64]。

これに対して、この発想との整合性が問題となるのが、2017年の Capenter 判決である[65]。同判決は、携帯電話事業者が保管する基地局位置情報の取得は第4修正の「捜索」であり、令状が必要であると判示した。これは、この情報に関して第三者法理の適用を否定したということを意味するが、物理世界において、位置情報は閉鎖空間内部の情報とはいいにくく、また、それは通信の内容情報でもない。そのため、同判決の判断の基礎にある発想は、上記の通信の内容情報と非内容情報との区別の基礎にある発想とは異質のものであ

[55] *See* Dressler et al., *supra* note 52, at 72. ただし、2012年の Jones 判決は、プライバシーの合理的期待のテストに加えて、トレスパス・テストを用いている（Jones v. United States, 565 U.S. 400 (2012)）。

[56] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1010-11 (2010).

[57] *See* Dressler et al., *supra* note 52, at 107.

[58] *See* United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

[59] *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1210-11 (2004).

[60] United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

[61] *See* Wayne R. LaFave et al., Criminal Procedure, Vol. 2, § 4.4(c) n.10 (4th ed. November 2024 Update).

[62] *See id.* § 4.4(b). なお、後述の Carpenter 判決には留意が必要である。

[63] *See id.* § 4.2, § 4.3.

[64] *See* Kerr, *supra* note 56, at 1017-31.

[65] Carpenter v. United States, 585 U.S. 296 (2018).

るように見える[66]。

3-2 保管通信法に基づく証拠の保全要請

次に、制定法である保管通信法の「証拠の保全の要請」に関する規定について検討する。同法 2703 条(f)によれば、電気通信事業者等は、「政府機関の要請に基づき、裁判所命令の発付その他の手続までの間、その所持する記録その他の証拠を保全する（reserve）ために必要なすべての措置をとるものとする」とされている。この記録は、90 日間保存され、政府機関による再度の要請に基づき、さらに 90 日間延長されるものとされている[67]。本条の保存要請に基づいて保全されたデータは、通信内容であれば令状で、非内容情報であればサピーナ又はこれに類する提出命令で取得することができる[68]。

本条に基づく保全要請に関して確立した判例は存在しないが、実務上は、捜査機関と ISP の次のような見解に基づき運用されているようである。まず、捜査機関が本条に基づく要請をする時機については、捜査機関が「裁判所命令の発付その他の手続」を積極的に求めているということまで要求されず、捜査機関は制限なく保存要請をすることができるとされる。この見解の背景には、この規定は保存要請があった場合における ISP の対応を規制するのみであり、捜査機関を規制するものではないという発想がある[69]。

また、本条で保存要請の対象となる「その所持する記録その他の証拠」が、非内容情報のみなのか、通信の内容情報をも含むのかについては、文言上は不明であるが、実務上は、通信内容を含むという運用が確立しているとされる[70]。もっとも、実務上、保存要請は、通信の内容情報を対象とする場合であっても第 4 修正の保護は及ばないという前提で運用されている。この実務運用の基礎には、通信の内容情報は第 4 修正によって保護されるので、その開示については令状が必要となるが、その保存はあくまで予備的な段階に過ぎず、プライバシーの問題は生じないので、保存要請に第 4 修正の保護は及ばない、という発想があると考えられる[71]。

さらに、保存要請に特定性の要請はなく、ISP に対して、特定のアカウントのすべての記録を保存するよう求めることも可能である。このような実務運用は、保存は予備的な段階でありプライバシーの問題を生じさせないという上記の基本発想と整合的といえる[72]。ただし、保存要請の権限は、過去に作成された記録に対してのみ及び、まだ作成されていない記録を将来記録することの要請はできないと解されている[73]。

もっとも、このように、通信の内容情報の保存も含めて、本条に基づく保存要請に第 4 修正の保護が及ばないという見方を前提とした実務運用に対しては批判もある。Orin S. Kerr は、①通信内容の保全要請は「政府の行為（state action)」であるとしたうえで、②それは第 4 修正の「押収」に該当するので、③その実施に令状は不要であるが、原則として相当な理由、場合によっては合理的な嫌疑がなければならないと主張している[74]。この見解は、保存要請が「押収」に該当する理由として、のちの捜査機関による利用のためにデータをコピーし、データに対するコントロールを獲得することは、第 4 修正の「押収」であること、また、実質論としても、保存によって、ユーザーには、データを消去することができなくなりそれに対するコントロールを失うという害悪が生じており、予備的段階であるから害悪が生じていないとはいえないという点を指摘している[75]。

ただし、この批判論の射程は、ISP が保管する通信の内容情報の保存に限定されており、非内容情報はその対象となっていない。これは、インターネットの利用者は、保管されたデータの通信内容に対して第 4 修

[66] *See* LaFave et al., *supra* note 61, § 4.4(b).

[67] 18 U.S. Code § 2703 (f).

[68] *See* Orin S. Kerr, *The Fourth Amendment Limits of Internet Content Preservation*, 65 St. Louis U. L.J. 753, 773-74 (2021).

[69] *See id.* at 762.

[70] *See id.* at 764-65.

[71] *See id.* at 766.

[72] *See id.* at 770.

[73] *See id.* at 766. この解釈の根拠は、「その所持する記録その他の証拠を保全する」条文の文言である。ただし、裁判例の中には将来の記録の保存も要請できることを示唆するものがある。

[74] Kerr, at 778-802.

[75] *Id.* at 782-85.

正の権利を有するが、原則として非内容記録にはそれを有さないからである[76]。

このようなKerrの批判論に対しては、元連邦検察官からの反論がある[77]。

4 おわりに

本報告書は、ISPに対するデータの予備的保存の義務付けという観点から、ドイツ法・EU法とアメリカ法について、比較法的検討を行った。両者の法的規制の在り方や問題へのアプローチの仕方はまったく異なっており、これには、「通信の秘密」という概念の有無のほか、プライバシーに関する理解の相違も関わっていると考えられる[78]。今後は、これらのアプローチの相違の言語化をさらに試み、我が国への応用可能性を検討していきたい。

【参考文献】

Maria Tzanou, The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance (2017)

Adam Juszczak & Elisa Sason, Recalibrating Data Retention in the EU: The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning?, 2021 eucrim 238 (2021)

Marion Albers, Data Retention in Germany, in European constitutional Courts towards Data Retention Laws (M. Zubik et al. eds. 2021)

Jan Podkowik et al., Judicial Dialogue on Data Retention Laws: A Breakthrough for European Constitutional Courts?, 19 I・CON 1597 (2021)

Werner Beulke/Sabine Swoboda, Strafprozessrecht (16 Aufl. 2025)

Joshua Dressler et al., Understanding Criminal Procedure Vol. 1: Investigation (8th ed. 2021)

Wayne R. LaFave et al., Criminal Procedure, Vol. 2 (4th ed. November 2024 Update)

Orin S. Kerr, Applying the Fourth Amendment to the Internet: A General Approach, 62 Stan. L. Rev. 1005 (2010)

Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash L. Rev. 120 (2004)

Orin S. Kerr, The Fourth Amendment Limits of Internet Content Preservation, 65 St. Louis U. L.J. 753 (2021)

Michael L. Levy, Preservation Letters and Fourth Amendment Seizures: A Response to Professor Kerr, 66 St. Louis U. L.J. 749 (2022)

James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty 113 Yale L.J. 1151 (2004)

内藤大海「ドイツにおける通信関連情報の予備的保存について」吉開多一＝小西暁和『刑事政策の新たな潮流――石川正興先生古稀祝賀論文集』(2019年)93頁

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月

[76] *Id.* at 778-79 & n.114.

[77] Michael L. Levy, *Preservation Letters and Fourth Amendment Seizures: A Response to Professor Kerr*, 66 St. Louis U. L.J. 749 (2022).

[78] *See, e.g.*, James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 1151 (2004).

Legal Restrictions on Law Enforcement Data Collection from ISPs: A Comparative Study of the United States, Germany, and Japan	2024 Visiting Scholars Symposium (UC Berkeley, School of Law)	2024 年 10 月 18 日