

ドイツにおけるテロ防止のための情報収集 —テロ対策データベースと通信履歴の保存を中心に—

国立国会図書館 調査及び立法考査局
海外立法情報課 渡辺 富久子

【目次】

はじめに

I テロ防止のための情報収集

- 1 テロ防止のための情報収集と個人情報保護との関係
- 2 テロ防止のための情報収集を目的とした立法措置

II テロ対策データベース

- 1 テロ対策データベース法（2006年12月31日施行）
- 2 連邦憲法裁判所判決（2013年4月24日）と法改正（2015年1月1日施行）

III 通信履歴の保存義務

- 1 通信事業者への通信履歴保存義務の導入（通信法及び刑事訴訟法の改正：2008年1月1日施行）
- 2 連邦憲法裁判所判決（2010年3月2日）
- 3 通信事業者への通信履歴保存義務の再導入（通信法及び刑事訴訟法の改正：2015年12月18日施行）

おわりに

翻訳：テロ対策データベース法

通信法（抄）

刑事訴訟法（抄）

はじめに

2001年9月11日のアメリカ同時多発テロ事件は、国際的なイスラム過激派組織による無差別大量殺戮テロという新たな次元のものであり、以降、ドイツにおいても、テロ対策のために多くの立法措置がとられてきた⁽¹⁾。ドイツにおけるテロ対策立法は、団体規制、警察や情報機関の権限強化、テロに係る犯罪の構成要件の拡大、マネーロンダリング規制等の個別の領域について、関係法律の改正という形で継続的に行われている。これらの立法措置は、末尾の表1「2001年9月11日のアメリカ同時多発テロ事件以降のドイツの主なテロ対策立法」に掲げるとおりである。

本稿は、これらのうち、警察や情報機関の情報収集の権限強化に関する立法措置（表1の施行日に網掛けがしてあるもの）を対象とする。ドイツにおいては、警察や情報機関の

(1) ドイツでは、極左過激組織のドイツ赤軍（Rote Armee Fraktion: RAF）による政府や民間の要人テロが社会的な問題となっていた1970年代から、テロ対策立法が行われていた。例えば、刑法典にテロ組織結成の罪（第129a条）を導入した1976年の法律 Gesetz zur Änderung des Strafgesetzbuches, der Strafprozeßordnung, des Gerichtsverfassungsgesetzes, der Bundesrechtsanwaltsordnung und des Strafvollzugsgesetzes vom 18. August 1976 (BGBl. I S. 2181) や、同罪の構成要件を拡大した1986年の法律 Gesetz zur Bekämpfung des Terrorismus vom 19. Dezember 1986 (BGBl. I S. 2566) 等がある。詳細は、渡邊斉志「IV テロ対策 3. ドイツ」『主要国における緊急事態への対処—総合調査報告書—』（調査資料2003-1）、国立国会図書館調査及び立法考査局、2003、pp.98-100 <http://dl.ndl.go.jp/view/download/digidepo_999552_po_20030107.pdf?contentNo=7&alternativeNo=> を参照。以下、インターネット情報は、2016年5月31日現在のものである。

権限強化を積極的に法制化しようとする連邦議会と、国家の監視体制の行き過ぎを抑制しようとする連邦憲法裁判所との間で、安全（Sicherheit）と自由（Freiheit）の均衡が模索されている⁽²⁾。

以下では、第Ⅰ章でテロ防止のための情報収集の権限強化の概要を紹介する。次に、テロ防止のための情報収集手段の例として、第Ⅱ章でテロ対策データベースについて、第Ⅲ章で通信事業者に対して課される通信履歴の保存義務について、関連する法律及び判決の概要を紹介する。また、テロ対策データベース法並びに通信法及び刑事訴訟法における通信履歴の保存義務に関連する規定を訳出する。

I テロ防止のための情報収集

1 テロ防止のための情報収集と個人情報保護との関係

テロを未然に防止するためには、疑わしい人物に関する情報を事前に広く収集することが不可欠である。そのため、2001年以降のテロ対策立法においては、テロを未然に防止するための情報収集に力点が置かれ、警察や情報機関に対して個人情報収集の権限が様々に与えられることになった。⁽³⁾

テロ対策立法においては、特に、個人情報保護の原則との兼ね合いが問題となる。ドイツにおいて、個人情報保護は、個人の人格の自由な発展のための権利として非常に重視されている。ただし、公共の利益が優先される場合には、個人情報保護も制約を受ける。公共の利益と個人情報保護の利益の比較衡量は立法者の任務であり、立法の際には、規範の明確性の原則（Bestimmtheitsgrundsatz）⁽⁴⁾、必要性の原則、比例原則（Verhältnismäßigkeitsgrundsatz）⁽⁵⁾等が考慮されなければならない⁽⁶⁾。

ドイツにおいては、近年、国家による監視活動と市民の自由との比較衡量の結果、社会が安全でなければ市民は自由に行動することもできないとして、テロ対策が強化されている⁽⁷⁾。そして、市民のプライバシーの侵害につながる様々な情報収集が法制化されることになったのである。

2 テロ防止のための情報収集を目的とした立法措置

テロ防止のための情報収集の権限を有するのは、警察官庁及び情報機関である。犯罪の捜査及び危険防止（Gefahrenabwehr）⁽⁸⁾は、第一義的には州の任務であり、州警察及び州刑

(2) ドイツにおいては、安全は個人の自由の基礎であり、国家は、市民の自由の制約が必要かつ適切な範囲となるようにして、安全対策を行うと考えられている。Josef Isensee, „§ 71 Gemeinwohl im Verfassungsstaat“, Josef Isensee und Paul Kirchhof, *Handbuch des Staatsrechts*, Band IV, Dritte, völlig neubearbeitete und erweiterte Auflage, Heidelberg: C.F. Müller, 2006, S. 41.

(3) Günter Krings, „Terrorismusbekämpfung im Spannungsfeld zwischen Sicherheit und Freiheit“, *Zeitschrift für Rechtspolitik*, 6/2015, 4. September 2015, S. 167ff.

(4) 規範の明確性の原則とは、個人情報保護の制限の要件と範囲を、市民が認識することができるように明らかに定めなければならないという原則をいう。平松毅「7 自己情報決定権と国勢調査—国勢調査法一部違憲判決—」ドイツ憲法判例研究会編『ドイツの憲法判例 第2版』信山社出版, 2003, pp.61-62.

(5) 比例原則とは、公権力が個人の権利を侵害する場合に要求される原則で、手段が目的達成のために適切か、目的達成のための最小限度の手段か、権利の侵害が目的達成の利益に比して不当でないかを考慮するものである。Carl Creifelds, *Rechtswörterbuch*, 20. Neu bearbeitete Auflage, München: Beck, 2011, S. 1289.

(6) 詳細は、平松毅「個人情報保護—ドイツにおける個人情報保護概念の形成—」『公法研究』53号, 1991.10, pp.72-84を参照。

(7) Krings, *op.cit.* (3).

事庁が担当する。連邦の警察官庁としては、連邦警察（Bundespolizei）及び連邦刑事庁（Bundeskriminalamt）が連邦内務省の下に設置されている。連邦警察は、国境警備や鉄道交通警察、航空交通警察等を所掌し、連邦刑事庁は、刑事警察事項における連邦と州の協力、組織犯罪の捜査及び刑事警察の領域における国際協力等を所掌している⁽⁹⁾。情報機関には、連邦憲法擁護庁（Bundesamt für Verfassungsschutz）及び州の憲法擁護官庁、軍事防諜局（Amt für den Militärischen Abschirmdienst）並びに連邦情報局（Bundesnachrichtendienst）がある⁽¹⁰⁾。ドイツにおいては、国内治安は警察の任務、対外的な防衛は連邦軍の任務とされており、連邦軍は、国内のテロ対策を行わない⁽¹¹⁾。

これら官庁によるテロ防止のための情報収集を目的とした立法措置として、代表的なものに次のものがある。

- ①情報機関に対して、民間の通信事業者や金融機関、航空会社から国際テロ防止のために必要な個人情報収集する権限を与えた第2次テロ対策法の制定⁽¹²⁾（2002年1月1日施行）
- ②警察と情報機関が共同で運用するテロ対策データベースの根拠法であるテロ対策データベース法の制定⁽¹³⁾（2006年12月31日施行）（第Ⅱ章で詳述）
- ③連邦刑事庁に対して、国際テロ防止のために、秘密捜査官⁽¹⁴⁾の投入、住居内の録音・録画、ラスタースearch⁽¹⁵⁾、オンライン検索⁽¹⁶⁾、通信傍受等の権限を与えた連邦刑事庁法の改正⁽¹⁷⁾（2009年1月1日施行）
- ④通信事業者に対して通信履歴保存義務を課すための通信法及び刑事訴訟法の改正⁽¹⁸⁾

(8) 危険防止とは、主に犯罪の防止であり、刑事訴追ではない。Wolf-Rüdiger Schenke, *Sicherheitsrecht des Bundes*, München: Beck, 2014, S. 7.

(9) 山口和人「ドイツの国際テロリズム対策法制の新たな展開―「オンライン検索」を取り入れた連邦刑事庁法の改正―」『外国の立法』No.247, 2011.3, p.55 <http://dl.ndl.go.jp/view/download/digidepo_3050612_po_02470003.pdf?contentNo=1&alternativeNo=>を参照。

(10) 連邦憲法擁護庁は、連邦内務省の下部組織であり、自由で民主主義的な憲法秩序に反する組織（極右、極左及びテロ組織）を監視する。州の憲法擁護官庁は、同様の任務を担う各州の官庁である。軍事防諜局は、連邦軍の一部局で、軍隊内の防諜活動を行う。連邦情報局は、連邦首相府に属し、安全保障上重要な外国情報を収集する。渡邊斉志「ドイツにおける議会による情報機関の統制」『外国の立法』No.230, 2006.11, p.124 <http://dl.ndl.go.jp/view/download/digidepo_1000336_po_023005.pdf?contentNo=1&alternativeNo=>を参照。

(11) 松浦一夫「ドイツ連邦軍の対テロ活動と議会統制―対テロリズム安全保障と「議会の軍隊」をめぐる憲法問題―」『比較憲法学研究』21号, 2009, pp.70-72. 詳細は、松浦一夫「9・11米国テロ事件以後のドイツ政府の対応と政策課題」『防衛法研究』26号, 2002, pp.47-83を参照。

(12) Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361). 詳細は、渡邊斉志「【短信：ドイツ】テロ対策のための立法動向」『外国の立法』No.212, 2002.5, pp.105-114; 渡辺富久子「【ドイツ】テロ対策法の期限延長」『外国の立法』No.250-2, 2012.2, pp.14-15 <http://dl.ndl.go.jp/view/download/digidepo_3383247_po_02500207.pdf?contentNo=1&alternativeNo=>を参照。

(13) テロ対策データベース法は、表1の連邦及び州の警察及び情報機関の共同データベースを設置する法律（2006年12月31日施行）により制定された。Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz) vom 22. Dezember 2006 (BGBl. I S. 3409). また、2012年には、テロ対策データベースと同じ仕組みの極右対策データベース（Rechtsextremismusdatei）も、連邦刑事庁に設置されている。Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Rechtsextremismus-Datei-Gesetz) vom 20. August 2012 (BGBl. I S. 1798).

(14) 秘密捜査官とは、身分を隠して捜査する警察官である（連邦刑事庁法第20g条）。

(15) ラスタースearchとは、諸機関に保存された個人データを集め、電子的に照合して特定のメルクマールに該当する人物を抽出する捜査手法である。山口 前掲注(9), p.60を参照。

(16) オンライン検索とは、犯罪を犯す疑いが一定の事実により正当化される者について、当事者に知られないように、特別なソフトウェアを用いて外部からコンピューターにアクセスし、データを収集する行為である。同上, pp.60-61を参照。

(17) 連邦刑事庁法の改正は、表1の国際テロリズム対策法（2009年1月1日施行）による。Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008 (BGBl. I S. 3083). 同上, p.60を参照。

(2008年1月1日施行)(第Ⅲ章で詳述)がある。

①については、情報機関が警察と類似した調査権限を持つようになり、これが警察と情報機関の分離の原則(Trennungsgebot)(第Ⅱ章で述べる。)に反すること、また、情報機関の調査は裁判所の統制を受けないこと⁽¹⁹⁾、③については、連邦刑事庁に対して、いまだ犯罪が生じていない段階でプライバシーを侵害する措置を可能としたこと⁽²⁰⁾、また、従来、州警察が「危険防止」の一環として行ってきたテロ防止の任務を連邦刑事庁も所掌するようになった上、連邦刑事庁が情報機関に類似してきたこと等が問題として指摘されている⁽²¹⁾。

社会の安全に重きを置き、テロ対策を強化するこれらの立法に対して、連邦憲法裁判所は、市民の自由を重視する方向の判決を下してきた⁽²²⁾。主要な判決を、末尾の表2「テロ対策立法に関する連邦憲法裁判所の主要な判決」に掲げた。これらの判決において、連邦憲法裁判所は、テロ防止のための諸制度の枠組み自体を合憲としつつ、それらの実施の詳細を定める規定については基本権への十分な配慮を求め、一部については違憲と判断してきた。判決においては、特に、①通信の秘密や住居の不可侵といった基本権の侵害が許容される場合の要件は、比例原則及び明確性の原則によらなければならないこと、②私的生活の中核領域(Kernbereich privater Lebensgestaltung)⁽²³⁾を厳格に保護しなければならないこと、③基本権を侵害する措置は、裁判所の命令や記録の義務、当事者への通知等の手続を必要とすることが強調されてきた⁽²⁴⁾。

以下では、テロ対策データベースと通信履歴の保存義務に関する法律の規定を、当該規定について連邦憲法裁判所が下した判決の具体例とともに紹介する。

Ⅱ テロ対策データベース

1 テロ対策データベース法(2006年12月31日施行)

テロ対策データベース法は、2007年から連邦刑事庁において運用されているテロ対策データベース(Antiterrordatei)の根拠法である。同法は、国際テロの脅威を受け、警察と情報機関との情報交換を促進するために制定され、2006年12月31日に施行された。

同法の制定時の概要を以下に紹介する。テロ対策データベースに参加するのは、連邦刑事庁、連邦警察、州刑事庁、連邦及び州の憲法擁護官庁、軍事防諜局、連邦情報局並びに税関刑事庁(Zollkriminalamt)⁽²⁵⁾(以上に挙げた官庁を合わせ、以下「参加官庁」という。)である(テロ対策データベース法第1条。以下、この章において単に条番号を掲げる場合

(18) Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EC vom 21. Dezember 2007 (BGBl. I S. 3198).

(19) Hans-Jürgen Lange, *Wörterbuch zur Inneren Sicherheit*, Wiesbaden: VS Verlag für Sozialwissenschaften, 2006, S. 339. 情報機関の活動は、連邦議会の統制を受ける。

(20) 山口 前掲注(9), pp.54-55.

(21) Rainer Griesbaum und Frank Wallenta, „Strafverfolgung zur Verhinderung terroristischer Anschläge – Eine Bestandsaufnahme“, *Neue Zeitschrift für Strafrecht*, 33(7), 15. Juli 2013, S. 373.

(22) Markus Möstl, „Das Bundesverfassungsgericht und das Polizeirecht; Eine Zwischenbilanz aus Anlass des Urteils zur Vorratsdatenspeicherung“, *Deutsches Verwaltungsblatt*, 125(13), 1. Juli 2010, S. 808.

(23) 連邦憲法裁判所の判決によれば、私的領域の中核領域に含まれる感情表現や愛情表現等は保護の対象となるが、処罰可能な具体的行為に関する会話は保護対象ではない。Lutz Meyer-Goßner und Bertram Schmitt, *Strafprozessordnung: Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen*, München: Beck, 2015, S. 390.

(24) Möstl, *op.cit.*(22); Hans-Jürgen Papier, „Rechtsstaat im Risiko“, *Deutsches Verwaltungsblatt*, 125(13), 1. Juli 2010, S. 801ff. を参照。

(25) 税関刑事庁は、麻薬密輸等の犯罪の捜査権限を有する。

には、テロ対策データベース法の条項を指す。)。参加官庁は、①テロ組織及びその支援集団の加入者及び支援者、②政治的目的の暴力行為を実施、支援、準備又は賞賛する者、③テロ組織の加入者若しくは支援者又は政治的目的の暴力行為を実施、支援、準備若しくは賞賛する者との接触者（Kontaktperson）について、以下のデータをテロ対策データベースに登録する義務を負う（第2条及び第3条）。

①基礎データ（氏名、旧姓、他の名前、仮名、異なる表記による氏名、性別、生年月日、出生地、出生国、現国籍及び旧国籍、現住所及び旧住所、身体的な特徴、言語、方言、写真、身分証明書に関する事項）

②拡張基礎データ（通信端末機の番号等、電子メールアドレス、銀行口座、登録車両、家族状況、民族、宗教、爆薬や銃器の製造や取扱いに関する知識等）

テロ対策データベースには、その他、これらの人物と関係があり、国際テロを解明する手がかりを得ることができると推測される団体や関係のある物（Sachen）等が登録される。

参加官庁は、国際テロ対策のために必要な場合には、特定の人物を検索して、その基礎データにアクセスすることができる。データを入力した官庁が承認した場合には、さらに、その拡張基礎データにアクセスすることができる（第5条）。また、参加官庁は、国際テロ対策のために必要な場合には、アクセスしたデータを利用することができる⁽²⁶⁾（第6条）。テロ対策データベースには、2013年6月時点で、約15,000人が登録されている⁽²⁷⁾。

この法律において特に問題になったのは、警察と情報機関の分離の原則である。ドイツにおいては、ナチス時代に両者の機能を併せ持っていた秘密国家警察ゲシュタポ⁽²⁸⁾への反省から、戦後、連合軍の意向を受けてこの原則が堅持されてきた⁽²⁹⁾。警察と情報機関は組織的に分離され、情報機関は、逮捕や捜索、押収、鑑識等の、警察が権限を有する任務を行うことはできない⁽³⁰⁾。しかし、テロ対策データベースにより、公開捜査を行う警察が、情報機関が秘密裏に得たデータを手に入れることも可能となるため、警察と情報機関の分離の原則の違反ではないかと指摘されていた⁽³¹⁾。

2 連邦憲法裁判所判決（2013年4月24日）と法改正（2015年1月1日施行）

連邦憲法裁判所は、2013年4月24日、テロ対策データベース法に関して判決を下した（1 BvR 1215/07）⁽³²⁾。判決では、国際テロ対策の公益は非常に大きいと、警察と情報機関の

(26) ここでいう「利用」とは、テロ対策データベースのデータと当該官庁が有するデータとの照合及び国際テロ対策のための既知情報の伝達の要請である。

(27) „Die Antiterrordatei“. 連邦内務省ウェブサイト <http://www.bmi.bund.de/DE/Themen/Sicherheit/Terrorismusbehaempfung/Antiterrordatei/antiterrordatei_node.html> を参照。2007年8月から2011年7月までのテロ対策データベースの運用実績は、Deutscher Bundestag, *Drucksache* 17/12665 (neu) を参照。2010年8月から2011年7月までの検索件数は、約67,000件であり、各州の刑事庁の検索が約54%、連邦刑事庁が約27%等となっている。

(28) ゲシュタポ (Geheime Staatspolizei: Gestapo) は、1933年から1945年まで存続した政治犯取締りのための政治警察である。1936年に刑事警察と統合、1939年にナチ党の親衛隊SSと統合し、ナチ党との結びつきの強い国家機関であった。その主な任務は、ナチ党が敵対者とみなした人々（ユダヤ人、ロマ民族、共産主義者等）の取締りであり、ナチ党独裁体制の維持に資した。ゲシュタポの活動は、数多くの市民の密告に基づいていたとされる。Martin H. W. Möllers, *Wörterbuch der Polizei*, München: Beck, 2001, S. 645; イアン・カーショー（石田勇治訳）『ヒトラー権力の本質』白水社, 2009, pp.105-115. (原書名: Ian Kershaw, *Hitler*, 1991)

(29) Lange, *op.cit.*(19), S. 338.

(30) Volkmar Götz, „§ 85 Innere Sicherheit“, Isensee und Kirchhof, *op.cit.*(2), S. 693f.

(31) Lange, *op.cit.*(19), S. 339.

(32) 本判決の要旨は、ドイツ憲法判例研究会「ドイツ憲法判例研究 (158) 対テロデータファイル法による情報機関・警察の情報共有と情報自己決定権 [ドイツ連邦憲法裁判所第一法定 2013.4.24 判決]」『自治研究』90(6), 2014.6, pp.119-127 を参照。

情報交換は正当化されるとし、テロ対策データベース法の基本的枠組み自体は合憲とされた。しかし、警察と情報機関の情報交換は、情報自己決定権⁽³³⁾の重大な侵害でもあり、緊急の例外的な場合にのみ許容されるものであるとした。その上で、判決は、ドイツ連邦共和国基本法（憲法に相当する。以下「基本法」という。）の規定に抵触する個別の規定について、2014年末までの改正を立法者に命じた。特に、登録するデータの範囲及びデータベースの利用条件を、より限定的とすることが求められた。

2014年に、判決の要請に従ってテロ対策データベース法は改正され、2015年1月1日に施行された⁽³⁴⁾。主要な改正点として、①それまで、テロ組織の加入者及び支援者等との接触者も基礎データとして登録していたため検索可能であったが、接触者をテロ組織の加入者及び支援者等に紐づく拡張基礎データの一項目とし、直接検索できないようにしたこと（第2条旧第3号の削除）、②それと知らずにテロ組織の支援集団を支援する者を登録対象から除外したこと（第2条第1号）、③政治的目的の暴力行為を賞賛する者を登録対象から除外したこと、④拡張基礎データの一項目（例えば「宗教」や「民族」）から検索した場合に、ヒットした全ての人物の基礎データを閲覧することができないようにし、当該情報の管理に責任を有する官庁と文書番号のみを閲覧することができるようにしたこと（第5条）等がある。

Ⅲ 通信履歴の保存義務

テロ防止を目的として通信事業者に対する通信履歴保存義務が最初に導入されたのは、2008年である⁽³⁵⁾。これは、EUデータ保存指令（2006/24/EG）⁽³⁶⁾の実施のために、刑事訴訟法及び通信法を改正したものであった（2008年1月1日施行）⁽³⁷⁾。しかし、このときに導入された通信法及び刑事訴訟法の関連規定は、2010年の連邦憲法裁判所の違憲判決により無効となり、EUのデータ保存指令自体も、2014年の欧州司法裁判所の違法との判断により無効となった。それにもかかわらず、通信履歴の保存はテロ防止のために不可欠であるとして、通信事業者に対する通信履歴保存義務は、2015年に再導入された⁽³⁸⁾。以下、ドイツの規定を中心に、その内容及び経緯の概要を紹介する。

(33) 連邦憲法裁判所は、1983年の国勢調査判決において、デジタル化の進展した今日、個人情報無制限な収集、保存、利用及び伝達からの保護の必要性を説き、一般的人格権（基本法第2条）から、自己の個人データの引渡し及び利用について原則として自分で決定する権利（情報自己決定権）を導出した。Creifelds, *op.cit.* (5), S. 623; 高橋和広「情報自己決定権論に関する一理論的考察」『六甲台論集 法学政治学篇』, 60(2), 2014.3, pp.105-165.

(34) Gesetz zur Änderung des Antiterrordateigesetzes und anderer Gesetze vom 18. Dezember 2014 (BGBl. I S. 2318). テロ対策データベース法は、2006年の制定当初は、2017年末までの時限立法であったが、2014年の改正により恒久的な法律となった。

(35) 実際には、1990年代半ばから通信事業者に対して通信履歴の保存を義務付ける法律を制定しようという試みが継続して行われていた。しかし、違憲の疑念があるためいずれも失敗していた。国内において通信履歴の保存義務の法制化を可能にするために、ドイツは、EU指令の制定に向け働きかけを行った。詳細は、Antonie Moser-Knierim, *Vorratsdatenspeicherung: Zwischen Überwachungsstaat und Terrorabwehr*, Berlin: Springer Vieweg, 2014, S.150ff. を参照。

(36) Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (OJ L 105, 13.4.2006, pp. 54-63).

(37) 前掲注(18)

(38) Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218).

1 通信事業者への通信履歴保存義務の導入（通信法及び刑事訴訟法の改正：2008年1月1日施行）

EUデータ保存指令は、重大な犯罪の捜査、確認及び訴追のために、一般国民の通信データ（通信日時、通信開始時の場所、利用者識別番号等）を6～24月の間保存することを民間の通信事業者に対して課すための法整備を加盟国に義務付けるものであった⁽³⁹⁾。その際、通信履歴保存義務は、2007年9月15日まで（インターネットの通信履歴については2009年3月15日まで）に、これを導入するための規定を設けなければならぬとされた。

ドイツにおける最初の通信履歴保存義務の導入は、この指令を実施するものであった。通信履歴の保存期間及び保存されるデータの範囲に関する規定は、連邦議会議員の決議⁽⁴⁰⁾に基づき、EU指令の要請を最低限満たすものにとどまった。通信履歴の保存義務に関する規定として、通信法に第113a条（データの保存義務）及び第113b条（保存したデータの利用）が、刑事訴訟法に第100g条（通信データの入手）が新たに定められた。

通信履歴とは、主に、固定電話、携帯電話、電子メール及びインターネットを利用した際に把握される端末機の識別番号（電話番号、アカウント番号又はIPアドレス）及び通信が行われた日時である。携帯電話の場合には、通信開始時の場所も保存される。通信の内容は、保存してはならない。保存期間は、6月とされた（通信法第113a条）。通信事業者は、保存した通信履歴を、刑事訴追（重大な犯罪又は通信を用いた犯罪の場合）、危険防止又は情報機関の任務の遂行のために、所管の機関に伝達することができる（通信法第113b条）。いずれの場合も、その通信履歴当事者への通知を行わないで、通信履歴を伝達することが可能である。

2 連邦憲法裁判所判決（2010年3月2日）

このような通信履歴の保存は、テロ等の犯罪の疑いのない一般市民の通信履歴までもが国家の監視対象になるとして、市民や法曹界から問題視されていた。通信履歴の保存は通信の秘密や情報自己決定権に反すること、保存された通信履歴を組み合わせると個人の性格や行動のプロフィールを再構成することが可能となること等の理由から、法律が施行されて間もない2008年2月には、多くの市民が連邦憲法裁判所に憲法異議（Verfassungsbeschwerde）を申し立てていた⁽⁴¹⁾。

2010年3月2日、連邦憲法裁判所は、通信履歴の保存は、テロ防止のために適切かつ必要な手段であり、合憲とした。しかし、これを実施するための規定である通信法第113a条及び第113b条について、データ利用の制限及びデータ保全⁽⁴²⁾に関する規定がないこと等から、基本法第10条第1項（信書及び通信の秘密）に抵触し、無効と判示した。また、保存された通信履歴を検察が刑事訴追のために入手することができる旨を定める刑事訴訟

(39) 今岡直子「イギリスにおけるデータ保全及び調査権限法の制定—EUデータ保全指令の無効裁定を踏まえて—」『外国の立法』No.264, 2015.6, pp.6-7 <http://dl.ndl.go.jp/view/download/digidepo_9381676_po_02640002.pdf?contentNo=1&alternativeNo=>を参照。

(40) Deutscher Bundestag, Drucksache 16/545. 2006年2月7日、当時の連立与党のキリスト教民主・社会同盟（CDU/CSU）と社会民主党（SPD）は、欧州理事会においてEUデータ保存指令案に賛成するよう、連邦政府に対して要請する決議（Antrag）を提出し、当該動議は同年2月16日に連邦議会において採択された。

(41) 連邦憲法裁判所の当該判決に関するプレスリリース „Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß“, Pressemitteilung, Nr.11/2010, 2010.3.2. <<http://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2010/bvg10-011.html>>を参照。憲法異議（基本法第93条第1項第4a号）とは、公権力によって自己の基本権を侵害された者が、その救済を求めて、連邦憲法裁判所に申し立てることができるものである。

(42) データ保全とは、保存した通信履歴を権限のない閲覧や使用から保護することである。

法第 100g 条第 1 項第 1 文の一部も、対象の犯罪が十分に限定的でないとして、無効とされた。また、保存された通信履歴の利用は、裁判所による命令及び当事者への通知を要件としなければならないとした。

判決（1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08⁽⁴³⁾）によれば、国家が通信履歴にアクセスする要件及び通信履歴保存の様態は、法治国家の原則と合致し、市民の基本権に配慮したものでなければならない。この連邦憲法裁判所判決を受け、ドイツにおいては、前述のとおり、通信事業者による通信履歴の保存義務はなくなった。

さらに、欧州司法裁判所が、2014 年 4 月 8 日、EU データ保存指令を無効と判断した（C-293/12, C-594/12）。同裁判所によれば、データ保存指令は、重大な犯罪の訴追という公益を目的としており、その限りにおいて通信履歴の保存期間を法律で定めることの必要性を認めている⁽⁴⁴⁾。しかし、同指令の規定は比例原則⁽⁴⁵⁾に鑑みて基本権を侵害しているとした。欧州司法裁判所は、通信履歴の保存は必要最低限としなければならないとし、全ての者の全ての通信手段の通信データ全部を保存するような通信履歴の保存、何ら犯罪の疑いがない者の通信履歴の保存、重大な危険防止との関連がない者の通信履歴の保存は、EU 基本権憲章第 7 条（プライバシーの権利）及び第 8 条（個人情報の保護）に違反するとした。この欧州司法裁判所の判決は、ドイツの連邦憲法裁判所判決よりも厳しく基本権の保護を要求している⁽⁴⁶⁾。

3 通信事業者への通信履歴保存義務の再導入（通信法及び刑事訴訟法の改正：2015 年 12 月 18 日施行）

連邦刑事庁は、2010 年 3 月 2 日の連邦憲法裁判所の判決の結果、通信事業者による通信履歴の保存義務がなくなったことを受けて、その影響を調査した⁽⁴⁷⁾。この調査において、連邦刑事庁は、通信事業者に対して通信履歴提供の要請を行った件数、その結果入手できた件数を把握した。調査の対象とした期間は、2010 年 3 月 2 日から 2011 年 4 月 26 日までであった。この期間中、連邦刑事庁は、通信事業者に対して 5,082 件の通信接続についてのデータの入手を要請した。このうち、4,292 件（約 84%）について、データを入手することができなかった⁽⁴⁸⁾。なお、この期間に入手することができた通信履歴は、通信事業者の通信履歴保存義務に基づくものではなく、通信事業者が料金精算等の事務のために保存していた通信履歴であった⁽⁴⁹⁾。各通信事業者における業務目的のための通信履歴の保存期間はそれぞれ異なり、保存期間が数日と非常に短い場合もある。そのため、通信履歴

(43) 本判決の翻訳は、Karl-Friedrich Lenz 訳「翻訳 通信履歴保存に関するドイツ連邦憲法裁判所 2010 年 3 月判決」『青山法学論集』52(1), 2010, pp.201-317 を参照。

(44) Holger Münch, „Praktische Nutzung der „Vorratsdatenspeicherung““, *Zeitschrift für Rechtspolitik*, 48(5), 24. Juli 2015, S. 132.

(45) 前掲注 (5) を参照。

(46) Anna Mrozek, Die Vorratsdatenspeicherung im Zahnradwerk des europäischen Mehrebenensystems, *Die Öffentliche Verwaltung*, 69(3), Februar 2016, S. 90.

(47) Bundeskriminalamt, *Abschlussbericht: Stand der statistischen Datenerhebung im BKA zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu „Mindestspeicherfristen“*. <https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Mindestspeicherfrist/studie.pdf?__blob=publicationFile> を参照。

(48) 入手することができなかった 4,292 件のうち、刑事訴追を目的とするものは 4,256 件、危険防止を目的とするものは 36 件であった。前者 4,256 件の通信履歴提供の要請のきっかけとなった犯罪は、コンピューター犯罪 1,898 件（約 45%）、児童ポルノの頒布、入手及び所持又は性犯罪 1,639 件（約 39%）であった。ibid. S. 16.

(49) 通信事業者は、料金精算や追加的な通信網の整備等の業務目的のために通信履歴を保存することができ（通信法第 96 条）、検察は、この規定により保存された通信データを刑事訴追のために入手することができる（刑事訴訟法第 100g 条第 1 項）。

の保存義務がなくなったことにより、効果的な刑事訴追に影響が及ぶことが確認された。このような調査結果に鑑みても、通信履歴の一定期間の保存の義務付けが、捜査当局により望まれていた⁽⁵⁰⁾。

2015年6月、連立与党のキリスト教民主・社会同盟(CDU/CSU)と社会民主党(SPD)は、通信履歴の保存義務を再導入する法律案⁽⁵¹⁾を連邦議会に提出した。法案は、2015年中に連邦議会及び連邦参議院を通過し、制定された法律は2015年12月18日に施行された。

新たな法律も、通信法と刑事訴訟法を改正する法律であった。通信法には、第113a条([通信データ保存の]義務を負う者及び補償)、第113b条(通信データの保存義務)、第113c条(データの利用)、第113d条(データ保全の保証)、第113e条(記録)、第113f条(要件一覧)及び第113g条(安全対策指針)が、刑事訴訟法には、第100g条(通信データの入手)、第101a条(裁判所の決定、データの表示及び分析並びに通信データの入手の際の[当事者への]通知義務)及び第101b条(通信データの入手に関する統計)が定められた。

新しい制度は、連邦憲法裁判所の判決を踏まえ、前の制度よりも基本権に配慮したものとなっている。以下に、改正の概要を紹介する。

①通信履歴の保存

保存の対象となる通信は、固定電話、携帯電話、インターネット電話及びインターネットであり、対象として、インターネット電話が追加され、電子メールが除外された⁽⁵²⁾。通信履歴の保存期間は10週間であるが、携帯電話及びインターネットの通信開始時の場所に関する情報のみ4週間である。通信の内容は、従前同様保存してはならない(通信法第113b条)。

②データ利用の制限

刑事訴追のために通信履歴の検察庁への伝達が許容される重大な犯罪が、法律に列举して定められた(刑事訴訟法第100g条第2項)。危険防止のための通信履歴の警察への伝達は、人の身体、生命若しくは自由又は連邦若しくは州の存立にとって具体的な危険があることが要件とされた。さらに、通信事業者が検察、警察及び情報機関の求めに応じて顧客の契約データ及び個人データを提供する際に、提供するデータをIPアドレスを用いて特定及び分析することができるが、通信事業者は、そのために、保存した通信履歴を利用することができることとされた(通信法第113c条第1項)。

また、精神的な問題に関する相談を受け付ける教会施設又は社会生活上の問題に関する相談を受け付ける官庁において職業上の守秘義務を負う職員との通信は、その履歴が保存されないことになった(通信法第113b条第6項)。また、弁護士、医師、連邦及び州議会議員等の刑事事件において証言を拒否することができる者については、通信履歴は保存されるが、警察や検察は、刑事訴追のためにそのデータを入手することができないとされた(刑事訴訟法第100g条第4項)。

③裁判所による命令

刑事訴追のために通信履歴を入手する際には裁判所による命令を要すること(刑事訴訟法第101a条第1項)、また、この際当事者に通知しなければならず、やむを得ず当事者への通知を行わない場合には裁判所による命令を要すること(同第6項)が定められた。

(50) Münch, *op.cit.*(44); S. 130.; Deutscher Bundestag, *Drucksache* 18/5088, S. 1.

(51) Deutscher Bundestag, *ibid.*

(52) 基本権の侵害の強度を減じる目的で、保存するデータの量を少なくするために、電子メールが除外された。
ibid., S. 2.

④データ保全

データの保全は、暗号化技術、通常の任務のためのデータの保存場所とは異なる場所における通信履歴の保存及びアクセス権の限定等（通信法第 113d 条）並びに通信履歴へのアクセスの記録（同第 113e 条）により保証される。データ保全のための技術指針は、連邦ネットワーク庁⁽⁵³⁾が連邦データ保護受託者⁽⁵⁴⁾の了解を得て策定する（同 113f 条）。

今回の改正について、電子メールが保存義務の対象から除外された点、職業上の守秘義務が考慮された点は改善点と言えるが、何ら犯罪の疑いがない者及び重大な危険防止との関連がない者の通信履歴が保存される点で、いまだ欧州司法裁判所の求める基準には達していない、という評価がある⁽⁵⁵⁾。EUにおいても、欧州司法裁判所の判決を踏まえたデータ保存指令を再制定しようとする動きがある⁽⁵⁶⁾。また、今回の改正法が施行されて間もなく、連邦憲法裁判所に対して憲法異議が申し立てられていることもあり⁽⁵⁷⁾、法律が再改正される可能性が高い。

おわりに

ドイツにおいては、ナチス時代のゲシュタポや東ドイツのシュタージ⁽⁵⁸⁾の経験もあり、テロ対策として個人情報の収集を立法化し、国家による監視体制を強化することは、法治国家にとっての危機と捉える見方も強く、連邦憲法裁判所は、数次の判決により、このような立法傾向に歯止めをかけようとしている。

2016 年 4 月 20 日には、連邦刑事庁に対し国際テロ防止のための調査権限を与えた 2009 年の連邦刑事庁法改正について、連邦憲法裁判所の判決があった（1 BvR 966/09, 1 BvR 1140/09）。判決は、連邦刑事庁に与えられたテロ調査権限は基本法に抵触しないとしながらも、住居内の録音・録画やオンライン検索といった措置の要件が厳格でないとして、2018 年 6 月末までの該当規定の改正を立法者に求めた。⁽⁵⁹⁾

他方、連邦政府は、2016 年 6 月 1 日、外国の情報機関との共同のデータベースの設置、密航業者対策のための連邦警察の秘密捜査官の投入、通信事業者による前払式携帯電話の顧客の本人確認等を内容とするテロ対策のための法律案を決定した⁽⁶⁰⁾。連邦議会は、こ

(53) 連邦ネットワーク庁（Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn）は、電力、ガス、通信、郵便、鉄道の分野のネットワークの規制官庁である。

(54) 連邦データ保護受託者（Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit）は、連邦政府の提案を受けて、連邦議会により選任され、行政官庁の監督を受けず、連邦議会による統制を受ける。連邦データ保護受託者は、連邦の行政官庁の他、通信事業者におけるデータ保護を検査する。„Aufgaben“. 連邦データ保護受託者ウェブサイト <http://www.bfdi.bund.de/DE/BfDI/Artikel_BFDI/AufgabenBFDI.html;jsessionid=7C5547B72764F80DB6154ED84838E43D.1_cid344> を参照。

(55) Andreas Nachbaur, „Vorratsdatenspeicherung „light“: Rechtswidrig und allenfalls bedingt von Nutzen“, *Zeitschrift für Rechtspolitik*, 48(7), 16. Oktober 2015, S. 216.

(56) „Vorratsdatenspeicherung: Neue Ansätze für EU-Richtlinie“. digitalcourage Website <<https://digitalcourage.de/blog/2015/vorratsdatenspeicherung-neue-ansaeetze-fuer-eu-richtlinie>> を参照。

(57) „Erste Verfassungsbeschwerde gegen neue Vorratsdatenspeicherung“, 2015.12.19. heise online <<http://www.heise.de/newsticker/meldung/Erste-Verfassungsbeschwerde-gegen-neue-Vorratsdatenspeicherung-3049697.html>> を参照。

(58) シュタージ（国家保安省）は東ドイツの情報機関で、捜査・逮捕等の執行権限も有しており、東ドイツ社会に網の目のような監視網を張りめぐらしていた。加藤雅彦ほか編『事典現代のドイツ』大修館書店、1998, pp.214-215 を参照。

(59) 詳細は、渡辺富久子【ドイツ】連邦刑事庁のテロ調査権限に関する連邦憲法裁判判決『外国の立法』No.268-1, 2016.7, pp.10-11 <http://dl.ndl.go.jp/view/download/digidepo_10133184_po_02680105.pdf?contentNo=1> を参照。

の法案を6月24日に可決し、法律は7月30日に施行された⁽⁶¹⁾。

ドイツにおいては、近年流入した大量難民の中にテロリストが紛れていた事実が発覚したことなどもあり⁽⁶²⁾、今後も、テロ防止のための立法が続くことが予想される。しかし、一連の立法措置により、警察や情報機関等の諸機関の区別が曖昧となっており⁽⁶³⁾、これが国家や民主主義の意味を変容させつつあることも指摘されている⁽⁶⁴⁾。社会の安全確保は立法者の重要な責務であるが、基本権に十分配慮して情報収集の要件を定めることが要請されており、今後の立法動向も注目される。

(わたなべ ふくこ)

(60) „Prepaid-Karten künftig nur noch mit Ausweis“, *Süddeutsche Zeitung*, 2. Juni 2016, S.1. Entwurf eines Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus (Deutscher Bundestag, *Drucksache* 18/8702). 通信事業者は、検察、警察及び情報機関の求めに応じて、契約者の個人データの提供を義務付けられている（通信法第111条～第113条）。前払式携帯電話の契約者の個人データをも把握することにより、通信事業者の契約者情報のデータが増え、テロ対策に資するとされている。

(61) Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus vom 26. Juli 2016 (BGBl. I S. 1818).

(62) 2016年6月2日、警察当局は、デュッセルドルフにおいて自爆テロを計画していたシリア人3名を逮捕した。連邦刑事庁は、ドイツに流入した難民のうちテロ容疑で49件の調査を行っている。また、連邦刑事庁は、テロ組織の加入者又は支援者の疑いがあるとして380件の情報提供を受けている。„BKA: Viele Hinweise auf Terroristen unter Flüchtlingen“, *Frankfurter Allgemeine Zeitung*, 4. Juni 2016, S. 1; „Große islamische Szene in Nordrhein-Westfalen“, *Frankfurter Rundschau*, 3. Juni 2016, S. 4.

(63) 植松健一「連邦刑事庁(BKA)・ラスター捜査・オンライン捜索(1)―憲法学的観点からみたドイツにおける「テロ対策」の現段階―」『島大法学』52(3/4), 2009.3, pp.6-7を参照。

(64) Lange, *op.cit.*(19), S. 133f.

表 1 2011 年 9 月 11 日のアメリカ同時多発テロ事件以降のドイツの主なテロ対策立法

施行日		法律名
		(原語)
		法律の概要
2001 年	12 月 8 日	第 1 次テロ対策法 (注 1)
		Erstes Gesetz zur Änderung des Vereinsgesetzes vom 4. Dezember 2001 (BGBl. I S. 3319)
		宗教的な性格を有する結社は、結社法の規制対象外であったが、同法を改正し、テロ組織とみなされる結社の禁止が可能となった。
2002 年	1 月 1 日	テロ対策資金に関する法律
		Gesetz zur Finanzierung der Terrorbekämpfung vom 10. Dezember 2001 (BGBl. I S. 3436)
		連邦軍、連邦国境警備隊、連邦刑事庁等のテロ対策資金を捻出するために、たばこ税法及び保険税法を改正し、たばこ税率及び保険税率が引き上げられた。
	1 月 1 日	第 2 次テロ対策法 (注 1)
		Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361)
		情報機関に対して、国際テロが発生するおそれがある場合に、航空会社、金融機関、通信事業者から個人情報入手する権限を与えた。2007 年 1 月 10 日までの時限立法であった。
	8 月 15 日	マネーロンダリング対策法 (注 2)
		Geldwäschebekämpfungsgesetz vom 8. August 2002 (BGBl. I S. 3105)
		EU のマネーロンダリング指令 2001/97/EC が国内法化された。
	8 月 23 日	第 34 次刑法典改正 (注 1)
		34. Strafrechtsänderungsgesetz - § 129b StGB vom 22. August 2002 (BGBl. I S. 3390)
		刑法典に第 129b 条を新設し、国内の犯罪組織及びテロ組織に適用される第 129 条及び第 129a 条が外国の組織にも適用されるようになった。
2003 年	11 月 6 日	銀行法の改正
		Zweites Gesetz zur Änderung des Zollverwaltungsgesetzes und anderer Gesetze vom 31. Oktober 2003 (BGBl. I S. 2146)
		テロ組織の資産凍結が定められた。
	12 月 28 日	EU のテロ対策のための枠組決定 2002/475/JI を国内法化する法律 (注 3)
		Gesetz zur Umsetzung des Rahmenbeschlusses des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung und zur Änderung anderer Gesetze vom 22. Dezember 2003 (BGBl. I S. 2836)
		刑法典第 129a 条を改正し、テロ組織首謀者等に対する最高刑の上限が引き上げられた。
2004 年	5 月 1 日	連邦住民保護・防災支援庁設置法
		Gesetz über die Errichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe vom 27. April 2004 (BGBl. I S. 630)
		国家的危機に際して関係機関の調整及び住民保護の計画を行う連邦住民保護・防災支援庁が設置された。
	7 月 29 日	交通手段確保法
		Verkehrsleistungsgesetz vom 23. Juli 2004 (BGBl. I S. 1865)
		大規模なテロや自然災害等に際して交通手段を確保するための法律が制定された。
2005 年	1 月 15 日	航空安全法 (注 4)
		Luftsicherheitsgesetz vom 11. Januar 2005 (BGBl. I S. 78)
		航空機のハイジャック事件に対処するための法律が制定された。
2006 年	12 月 31 日	連邦及び州の警察及び情報機関の共同データベースを設置する法律
		Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder vom 22. Dezember 2006 (BGBl. I S. 3409)
		連邦及び州の警察及び情報機関が共同で運営するテロ対策データベースが設置された。

2007 年	1 月 11 日	テロ対策法補充法
		Terrorismusbekämpfungsergänzungsgesetz vom 5. Januar 2007 (BGBl. I S. 2)
		第 2 次テロ対策法の期限が 5 年間延長された（～2012 年 1 月 10 日）。
	6 月 15 日	税関捜査業務法改正法
		Gesetz zur Änderung des Zollfahndungsdienstgesetzes und anderer Gesetze vom 12. Juni 2007 (BGBl. I S. 1037)
		税関捜査業務法が改正され、税関が犯罪防止のために行う通信傍受等の際の私的生活の中核領域の保護が定められた。
2008 年	1 月 1 日	通信傍受等の要件を新たに定め、EU のデータ保全指令 2006/24/EC を国内法化する法律
		Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EC vom 21. Dezember 2007 (BGBl. I S. 3198)
		刑事訴追における通信傍受等の際の私的生活の中核領域の保護（刑事訴訟法の改正）、通信事業者の通信履歴の保存義務（通信法の改正）が定められた。
	8 月 21 日	マネーロンダリング対策補充法
		Geldwäschebekämpfungsergänzungsgesetz vom 13. August 2008 (BGBl. I S. 1690)
		EU のマネーロンダリング指令 2005/60/EC 及びその実施指令 2006/70/EC が国内法化された。
2009 年	1 月 1 日	国際テロリズム対策法（注 5）
		Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008 (BGBl. I S. 3083)
		連邦刑事庁の任務に、国際テロリズムの危険防止が追加された。
	6 月 18 日	第 2 世代シェンゲン情報システム法（注 6）
		Gesetz zum Schengener Informationssystem der zweiten Generation vom 6. Juni 2009 (BGBl. I S. 1226)
		EU の第 2 世代シェンゲン情報システムの設置、運用及び利用に関する決定 2007/533/JI が国内法化された。
	8 月 4 日	国家を危うくする重大な暴力行為の予備の訴追に関する法律
		Gesetz zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten vom 30. Juli 2009 (BGBl. I S. 2437)
		刑法典に第 89a 条等が追加され、国家を危うくする重大な暴力行為の予備が刑罰の対象となった。
	8 月 5 日	欧州警察機関（ユーロポール）法等改正法（注 7）
		Gesetz zur Änderung des Europol-Gesetzes, des Europol-Auslegungsgesetzes und des Gesetzes zu dem Protokoll vom 27. November 2003 zur Änderung des Europol-Übereinkommens und zur Änderung des Europol-Gesetzes vom 31. Juli 2009 (BGBl. I S. 2504)
		EU のユーロポールの設置に関する決定 2009/371/JI が国内法化された。
2012 年	1 月 10 日	EU 決定 2008/615/JI を国内法化する法律
		Gesetz zur Umsetzung des Beschlusses des Rates 2008/615/JI vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität vom 31. Juli 2009 (BGBl. I S. 2507)
		EU のテロ及び複数国間の犯罪対策のための複数国間の協力の深化に関する決定 2008/615/JI が国内法化された。
	8 月 31 日	連邦憲法擁護庁法改正法
		Gesetz zur Änderung des Bundesverfassungsschutzgesetzes vom 7. Dezember 2011 (BGBl. I S. 2576)
		第 2 次テロ対策法の期限が 4 年間延長された（～2016 年 1 月 10 日）。
2012 年	8 月 31 日	極右対策データベース法
		Rechtsextremismus-Datei-Gesetz vom 20. August 2012 (BGBl. I S. 1798)
		警察と情報機関が共同で運用する極右対策データベースが設置された。

2013 年	6 月 1 日	ビザ警告データベースを設置し、滞在法を改正する法律
		Gesetz zur Errichtung einer Visa-Warndatei und zur Änderung des Aufenthaltsgesetzes vom 22. Dezember 2011 (BGBl. I S. 3037)
		滞在法に第 72a 条が新設され、ビザ申請者のデータとテロ対策データベースのデータの照合について定められた。
	9 月 1 日	ビザ情報システムアクセス法
		VIS-Zugangsgesetz vom 6. Mai 2009 (BGBl. I S. 1034)
		EU のテロ及び他の重罪の防止、発見及び捜査を目的とした加盟国の特定官庁及び欧州警察機関（ユーロポール）のビザ情報システムへのアクセス権に関する決定 2008/633/JI が国内法化された。
2015 年	1 月 1 日	テロ対策データベース法等を改正する法律
		Gesetz zur Änderung des Antiterrordateigesetzes und anderer Gesetze vom 18. Dezember 2014 (BGBl. I S. 2318)
		連邦憲法裁判所の判決（1 BvR 1215/07）を受け、法改正が行われた。
	6 月 20 日	国家を危うくする重大な暴力行為の予備の訴追に関する規定を改正する法律
		Gesetz zur Änderung der Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten vom 12. Juni 2015 (BGBl. I S. 926)
		テロ戦闘員の渡航及びテロ資金供与を防止するために、刑法典が改正された。
	6 月 30 日	身分証明書法等改正法
		Gesetz zur Änderung des Personalausweisgesetzes zur Einführung eines Ersatz-Personalausweises und zur Änderung des Passgesetzes vom 20. Juni 2015 (BGBl. I S. 970)
		身分証明書法が改正され、テロ戦闘員の中東への渡航を阻止するために身分証明書の剥奪が可能となった。
	11 月 21 日	憲法擁護機関の協力を改善する法律
		Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 (BGBl. I S. 1938)
		連邦憲法擁護法が改正され、極右対策及びテロ対策の強化として、連邦及び州の憲法擁護官庁（注 8）の協力が改善された。
	12 月 10 日	第 2 次テロ対策法の規定の期限の延長に関する法律
		Gesetz zur Verlängerung der Befristung von Vorschriften nach den Terrorismusbekämpfungsgesetzen vom 3. Dezember 2015 (BGBl. I S. 2161)
		第 2 次テロ対策法の期限が 5 年間延長された（～2021 年 1 月 10 日）。
	12 月 18 日	通信データの保存義務及び保存期限を導入する法律
		Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218)
		通信法等が改正され、通信事業者の通信記録の保存義務が再導入された。
2016 年	7 月 30 日	国際テロ対策のための情報交換を改善する法律
		Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus vom 26. Juli 2016 (BGBl. I S. 1818)
		連邦憲法擁護庁法等が改正され、連邦憲法擁護庁は、国際テロ対策を目的として、外国の情報機関と共同のデータベースを設置することができるようになった。

* 施行日に網掛けがしてある法律は、警察や情報機関の情報収集の権限強化に関するものである。

（注 1）渡邊斉志「【短信：ドイツ】テロ対策のための立法動向」『外国の立法』No.212, 2002.5, pp.105-114 を参照。

第 1 次テロ対策法は、アメリカ同時多発テロ事件が起こる以前から予定されていたものである。

（注 2）戸田典子「【短信：ドイツ】マナーロンダリング対策立法」『外国の立法』No.212, 2002.5, pp.115-119 を参照。

（注 3）渡邊斉志「【短信：ドイツ】テロリスト犯罪規定を改正するための法律案—EU 法の国内法化—」『外国の立法』No.218, 2003.11, pp.150-156 を参照。<http://dl.ndl.go.jp/view/download/digidepo_1000480_po_021809.pdf?contentNo=1&alternativeNo=>>

（注 4）渡邊斉志「ドイツにおけるテロ対策への軍の関与—航空安全法の制定—」『外国の立法』No.223, 2005.2, pp.38-50 を参照。<http://dl.ndl.go.jp/view/download/digidepo_1000422_po_022302.pdf?contentNo=1&alternativeNo=>>

（注 5）山口和人「ドイツの国際テロリズム対策法制の新たな展開—「オンライン捜査」を取り入れた連邦刑事庁法の改正—」『外国の立法』No.247, 2011.3, pp.54-82 を参照。<http://dl.ndl.go.jp/view/download/digidepo_3050612_po_02470003.pdf?contentNo=1&alternativeNo=>>

（注 6）シェンゲン情報システムは、シェンゲン協定締約国と第三国との国境管理のためのシステムで、第三国の国籍を有する者や犯罪容疑者が登録される。第 2 世代シェンゲン情報システム（2013 年 4 月 9 日に運用開始）

においてはテロ対策が強化され、生体データも登録される。須田祐子・前田幸男「シェンゲン情報システム（SIS）の現状と課題―「国境のないヨーロッパ」の国境管理とITシステム―」『境界研究』No.3, 2012, pp.1-13 を参照。

(注7) 欧州警察機関（ユーロポール）は、国際犯罪に関するインテリジェンス情報センターであり、加盟国間の情報交換を支援する。ジェームス・シンブソン「EU としてのインテリジェンス「合同状況センター」「EU 衛星センター」「欧州軍参謀部情報班」「ユーロポール」」『ワールド・インテリジェンス』No.7, 2007.7, p.88 を参照。

(注8) 連邦憲法擁護庁及び州の憲法擁護官庁は、自由で民主主義的な憲法秩序に反する組織（極右、極左及びテロ組織）を監視する情報機関である。

(出典) Deutscher Bundestag, Wissenschaftliche Dienste, *Terrorismus: Definitionen, Rechtsgrundlagen und Maßnahmen zur Terrorismusbekämpfung*, 2009, S. 6ff 等に基づき、筆者作成。

表2 テロ対策立法に関する連邦憲法裁判所の主要な判決

判決日	判決名（判決引用又は事件番号）
	判決の概要
2004.3.3	住居盗聴（Großer Lauschangriff）判決（BVerfGE 109, 279）
	被疑者の住居における盗聴を定めた基本法第13条第3項から第6項までの規定を合憲とした。しかし、これを実施する刑事訴訟法第100c条等の規定は、盗聴の要件が明確でなく、人間の尊厳を定める基本法第1条等に抵触するため、違憲とした。特に、私的生活の中核領域の保護は絶対であり、犯した犯罪行為に関する会話の録音の場合でも、人間の尊厳の不可侵性を確保する規定を定めなければならない。（注1）
2005.7.27	危険防止のための通信傍受（Telefonüberwachung）判決（BVerfGE 113, 348）
	ニーダーザクセン州警察法の危険防止のための通信傍受に関する規定について、通信の秘密の侵害の要件が明確に特定されていないとして、違憲とした。（注2）
2006.4.4	ラスター捜査（Rasterfahndung）（注3）判決（BVerfGE 115, 320）
	ノルトライン・ヴェストファーレン州警察法の危険防止のためのラスター捜査に関する規定について、安全確保という国家の目的に鑑みてラスター捜査自体は違憲ではないが、ラスター捜査は情報自己決定権を強く侵害するため、その実施は具体的な危険が存在することを要件としなければならないとして、当該規定を違憲とした。（注4）
2008.2.27	オンライン検索（Online-Durchsuchung）判決（BVerfGE 120, 274）
	ノルトライン・ヴェストファーレン州憲法擁護法のオンライン検索に関する規定について、オンライン検索は、著しく重要な法益（身体、生命、自由又は国家の存立等）に対する具体的な危険が存在することについて事実による根拠が存在する場合にのみ、憲法上許されると判示した。（注5）
2010.3.2	通信履歴保存（Vorratsdatenspeicherung）判決（BVerfGE 125, 260）
	刑事訴訟法及び通信法の通信履歴保存義務に関する規定について、通信履歴の保存自体は合憲であるが、当該規定においてはデータ利用の制限、裁判所の命令、当事者の権利保護及びデータ保全が定められていないため違憲とした。（注6）
2013.4.24	テロ対策データベース（Antiterrordatei）判決（BVerfGE 133, 277）
	テロ対策データベース法について、国際テロ対策の公益は非常に大きいと、警察と情報機関の相互の情報交換は正当化されるとし、法律の基本的枠組み自体は合憲としたが、データの範囲及び利用条件をより制限しなければならないとし、個別の規定を違憲とした。（注7）
2016.4.20	連邦刑事庁の国際テロ防止のための調査権限判決（1 BvR 966/09, 1 BvR 1140/09）
	連邦刑事庁法の国際テロ防止のための調査権限に関する規定について、国際テロ防止のために調査権限を連邦刑事庁に与えたことは許容されるが、比例性の原則を超えて基本権を侵害する監視措置、他の官庁へのデータ伝達、外国へのデータ伝達等の規定は違憲であるとした。（注8）

（注1）平松毅「53 住居に対する高性能盗聴器による盗聴—「大盗聴（Großer Lauschangriff）判決—」ドイツ憲法判例研究会編『ドイツの憲法判例 III』信山社出版，2008，pp.320-326 を参照。

（注2）西原博史「43 予防的通信監視と通信の秘密・比例原則—ニーダーザクセン警察法違憲判決—」同上，pp.254-259 を参照。

（注3）ラスター捜査とは、諸機関に保存された個人データを集め、電子的に照合して特定のメルクマールに該当する人物を抽出する捜査手法である。

（注4）植松健一「連邦刑事庁（BKA）・ラスター捜査・オンライン検索（1）—憲法学的観点からみたドイツにおける「テロ対策」の現段階—」『島大法学』52(3/4)，2009.3，pp.8-24 を参照。

（注5）山口和人「ドイツの国際テロリズム対策法制の新たな展開—「オンライン検索」を取り入れた連邦刑事庁法の改正—」『外国の立法』No.247，2011.3，p.61 <http://dl.ndl.go.jp/view/download/digidepo_3050612_po_02470003.pdf?contentNo=1&alternativeNo=> を参照。

（注6）Karl-Friedrich Lenz 訳「翻訳 通信履歴保存に関するドイツ連邦憲法裁判所 2010 年 3 月判決」『青山法学論集』No.52(1)，2010，pp.201-317 を参照。

（注7）ドイツ憲法判例研究会「ドイツ憲法判例研究（158）対テロデータファイル法による情報機関・警察の情報共有と情報自己決定権 [ドイツ連邦憲法裁判所第一法廷 2013.4.24 判決]」『自治研究』90(6)，2014.6，pp.119-127 を参照。

（注8）渡辺富久子「【ドイツ】連邦刑事庁のテロ調査権限に関する連邦憲法裁判決」『外国の立法』No.268-1，2016.7，pp.10-11 <http://dl.ndl.go.jp/view/download/digidepo_10133184_po_02680105.pdf?contentNo=1> を参照。

テロ対策データベース法

Antiterrordateigesetz

国立国会図書館 調査及び立法考査局
海外立法情報課 渡辺 富久子訳

第1条 テロ対策データベース

- (1) 連邦刑事庁 [Bundeskriminalamt]、連邦警察法第58条第1項に基づく法規命令⁽¹⁾に定める連邦警察官庁、州刑事庁、連邦及び州の憲法擁護官庁、軍事防諜局 [Militärischer Abschirmdienst]、連邦情報局 [Bundesnachrichtendienst] 並びに税関刑事庁 [Zollkriminalamt] (参加官庁⁽²⁾) は、ドイツ連邦共和国に関わりを有する国際テロの解明又は対策のために法律で定められた各々の任務の遂行を目的として、連邦刑事庁において、標準化⁽³⁾された中央のテロ対策データベース (テロ対策データベース) を共同で運用する。
- (2) 連邦内務省は、次の各号に掲げる要件を全て満たす場合には、法規命令により⁽⁴⁾、他の警察執行官庁に、テロ対策データベースの参加官庁として参加の権限を与えることができ、州の官庁を参加させる場合には当該官庁を所管する州の要請に基づくものとする。
1. 当該官庁が、個別事件に限らず、ドイツ連邦共和国に関わりを有する国際テロの対策の任務を特別に有すること。
 2. 第1項に規定する任務の遂行のためにテロ対策データベースへのアクセスが必要であり、かつ、データが登録されている者の保護すべき利益及び参加官庁の安全の利益を考慮して、[当該官庁の参加が] 適切であること。

第2条 テロ対策データベースの内容及びデータ登録義務

参加官庁は、当該官庁に効力を有する法規に基づき警察又は情報機関として有する情報 (既知の情報) により、既に収集したデータが次の各号に掲げる事項に関連することが明らかである事実上の根拠がある場合であって、かつ、ドイツ連邦共和国に関わりを有する国際テロの解明又は対策のために当該データが必要である場合には、当該データを、第3条第1項の規定によりテロ対策データベースに登録する義務を負う。

1. 以下の者

- a) 刑法典第129a条⁽⁵⁾に規定するテロ組織で国際的な関わりを有するもの又は刑法典

* この翻訳は、2014年12月18日に最終改正されたテロ対策データベース法の条文 Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz) vom 22. Dezember 2006 (BGBl. I S. 3409), das zuletzt durch Artikel 1 des Gesetzes vom 18. Dezember 2014 (BGBl. I S. 2318; 2016 I 48) geändert worden ist <<https://www.gesetze-im-internet.de/bundesrecht/atdg/gesamt.pdf>>. を訳出したものである。以下、インターネット情報は、2016年5月31日現在のものである。訳文中[]内の語句は、原綴も含め、訳者が補ったものである。

- (1) 連邦警察官庁の管轄に関する法規命令。Verordnung über die Zuständigkeit der Bundespolizeibehörden vom 22. Februar 2008 (BGBl. I S. 250).
- (2) ここに挙げた連邦刑事庁から税関刑事庁までの全ての官庁を指す。
- (3) 標準化とは、複数のコンピューターでデータを共有したり、複数のコンピューターをネットワークで接続したりするための規格を作成すること。これにより、異なるメーカーのコンピューター間での情報共有が容易になる。秀和システム第一出版編集部編『最新標準パソコン用語事典 2013-2014年版』秀和システム、2013、pp.572-573.
- (4) この規定に基づき、テロ対策データベースへの参加の権限を有する警察執行官庁を追加して指定する法規命令が制定されている。Verordnung über die Benennung weiterer zur Teilnahme an der Antiterrordatei berechtigter Polizeivollzugsbehörden vom 11. März 2015 (BGBl. I S. 302).

第 129b 条第 1 項第 1 文⁽⁶⁾の規定により第 129a 条が適用されるテロ組織でドイツ連邦共和国に関わりを有するものに加入する者又はそのような組織を支援する者

- b) a) に規定する組織を支援する集団に加入する者
- c) b) に規定する集団がテロを支援する活動を行っていることを知りながら、当該集団を支援する者
- 2. 政治的若しくは宗教的な利益を国際的に貫徹するための手段として違法な暴力を行使する者又はそのような暴力行使を支援し、準備し、若しくはその活動、特にこのような暴力行使の主唱により、故意に暴力行使を引き起こす者
- 3. 事実上の根拠に基づいて、第 1 号又は第 2 号に規定する者と関連があり、国際テロの解明又は対策のための情報を得ることができると推定される場合において、当該情報を得ることがドイツ連邦共和国に関わりを有する国際テロの解明又は対策のために必要であるとき、以下の事項
 - a) 組織、集団、財団又は企業 [の名称、所在地等]
 - b) 物 [Sachen]、銀行口座、住所、通信接続識別番号 [Telekommunikationsanschluss]⁽⁷⁾、通信端末機、ウェブサイト又は電子メールアドレス

第 1 文の規定は、参加官庁が、当該官庁に適用される法規に基づいて電子的な加工を施すことが許されるデータに限り適用する。

第 3 条 登録義務が課されるデータ

- (1) テロ対策データベースには、[調査により] 判明している限りにおいて、次の各号に掲げるデータを登録する。
 - 1. 第 2 条第 1 文第 1 号及び第 2 号に規定する者に係る以下の事項
 - a) 氏名、旧姓、他の名前、仮名、異なる表記による氏名、性別、生年月日、出生地、出生国、現国籍及び旧国籍、現住所及び旧住所、身体的な特徴、言語、方言、写真並びに第 2 条の該当規定及び他の法律の規定に違反しない限りにおいて、かつ、本人確認のために必要な限りにおいて身分証明書に関する事項（基礎データ）
 - b) 以下の他のデータ（拡張基礎データ）
 - aa) 本人の通信端末機又は他人の通信端末機の通信接続識別番号及び [本人が] 所有する通信端末機又は利用した [他者の] 通信端末機
 - bb) 電子メールアドレス
 - cc) 銀行口座
 - dd) 貸金庫
 - ee) [本人が] 登録する乗り物又は利用した [他者の] 乗り物
 - ff) 家族状況
 - gg) 民族 [Volkszugehörigkeit]
 - hh) 個別事件において国際テロの解明又は対策のために必要な限り、宗教
 - ii) 参加官庁が特定の事実に基づき有する既知情報により刑法典第 129a 条第 1 項及び第 2 項に規定するテロ犯罪の予備及び実行に資する [と判断する] 特別な能力、

(5) Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322). 刑法典第 129a 条は、ドイツ国内におけるテロ組織の結成に対する罰則を定める。

(6) 刑法典第 129b 条は、外国のテロ組織に、第 129a 条が適用される旨を定める。

(7) 通信接続識別番号とは、通信施設へのアクセスに必要な一意の電話番号やアドレスで、通信役務の利用を可能とするものをいう（通信監視令第 2 条第 10 号）。

特に爆薬又は銃器の製造又は取扱いに関する特別な知識及び技能

jj) 修了した学校教育、職業教育及び職業に関する事項

kk) 安全性審査法⁽⁸⁾第1条第5項にいう生活上重要な施設、交通施設若しくは交通機関、供給施設⁽⁹⁾若しくは供給機関、公共交通機関若しくは官庁における現在の又は過去の職務

ll) 危険性、特に銃器の所持又は暴力志向性

mm) 自動車運転免許及び飛行機操縦免許

nn) 第2条第1文第1号及び第2号に規定する者が会合する場所又は地域であつて、当該の者が赴いたところ

oo) 第2条第1文第1号 a) 又は第2号に規定する者との接触者

pp) 第2条第1文第1号 a) 又は b) に規定する具体的な組織又は集団の名称

qq) 既知情報の登録の根拠となった最近の出来事があつた日付

rr) 参加官庁のデータベースに既に登録されているデータについて、実際の根拠に基づく概要的な注記、補記及び評価で、当該基礎データ及び拡張基礎データに関わるもの。ただし、個別事件において義務的裁量⁽¹⁰⁾により必要な場合、かつ、国際テロの解明又は対策のために不可欠な場合に限る。

ss) [当該の者が] 自ら運営するウェブサイト又は第2条第1文第1号若しくは第2号に規定する活動のために主として利用するウェブサイト

2. 第2条第1文第3号に規定する組織、集団、財団、企業、物、銀行口座、住所、通信接続識別番号、通信端末機、ウェブサイト又は電子メールアドレスの同定に資する事項。ただし、これらに関する追加的な個人情報是不含まない。

3. 第1号及び第2号に規定する各データにつき、既知情報を有する官庁、文書番号又は他の事務番号及び機密等級

(2) 第1項第1号 b), oo) に規定する接触者とは、第2条第1文第1号 a) 又は第2号に規定する者と一時的又は偶然でなく接触があり、かつ、当該の接触者から国際テロの解明又は対策のための追加的な情報を得ることを期待することができるという実際の根拠がある者をいう。接触者については、第1項第1号 b), oo) に規定する拡張基礎データとして、その同定及び連絡のために、氏名、旧姓、他の名前、仮名、異なる表記による氏名、性別、生年月日、出生国、現国籍、現住所、写真、本人の通信端末機又は他人の通信端末機の通信接続識別番号、電子メールアドレス及び職場連絡先に限り登録することができる。

(3) 登録義務が課されるデータに、他の法規に基づく表示をしなければならない場合には、当該表示は、テロ対策データベースにおける登録の際にも保持しなければならない。

(4) 連邦刑事庁は、第1項第1号 b), gg), hh), ii), kk) 及び nn) の規定により登録しなければならないデータのための基準及び範疇を行政規則において定める。この行政規則は、[改正の都度、] 最新の文言で連邦官報 [Bundesanzeiger] において公示しなければならない

(8) Sicherheitsüberprüfungsgesetz vom 20. April 1994 (BGBl. I S. 867). 安全性審査法は、連邦の情報機関及び公的機関並びに民間の生活上及び防衛上重要な施設において機密情報を取り扱う職員的身元審査の要件及び手続を定める法律である。

(9) 供給施設とは、電力、水、ガス等を供給する施設をいう。

(10) 義務的裁量とは羈束裁量のことであり、具体的な行政行為をする場合に、適法であるかどうかについての客観的基準により行われる行政庁の裁量をいう。法令用語研究会編集執筆『有斐閣法律用語辞典 第3版』有斐閣、2006、p.1257を参照。

ない。連邦刑事庁は、第1項の規定により登録しなければならない他のデータの基準を当該行政規則において定めることができる。

第4条 登録の制限及び匿名化

- (1) 当事者の特別な秘密の利益又は特に保護すべき利益のために例外的に必要な場合には、参加官庁は、第3条第1項第1号b)に規定する拡張基礎データの全部若しくは一部の登録を行わないことができ（登録の制限）、又は第2条に規定する者、組織、集団、財団、企業、物、銀行口座、住所、通信接続識別番号、通信端末機、ウェブサイト若しくは電子メールアドレスに係るデータの全てを、他の参加官庁が照会した場合にデータの登録が分からないような方法で若しくは当該登録したデータにアクセスができないような方法で入力することができる（登録の匿名化）。登録の制限及び匿名化については、官庁の長又は当該の長により特別に委託された上級官吏が決定する。
- (2) 照会を受けたデータが匿名化されている場合には、データを入力した官庁は、全ての照会データの電子的な伝達を受け、照会した官庁と遅滞なく連絡を取り、第7条の規定により既知情報の伝達が可能か否かを明らかにしなければならない。データを入力した官庁は、個別事件の事情に基づき秘密の利益が上回る場合に限り、[照会した官庁と]連絡を取らない。第2文に規定する決定の理由は、文書に記録しなければならない。伝達された照会データ及び第3文に規定する文書は、遅くとも、匿名化されたデータを削除しなければならないときまでに、削除又は廃棄しなければならない。
- (3) 次の各号に掲げる措置又はこれらに相当する州法の規定に基づく措置により得られた個人データは、匿名化して登録しなければならない。
 1. 刑事訴訟法第100a条又は連邦刑事庁法第20l条に規定する措置⁽¹¹⁾
 2. 刑事訴訟法第100c条又は連邦刑事庁法第20h条に規定する措置⁽¹²⁾
 3. 刑事訴訟法第99条に規定する措置⁽¹³⁾
 4. 連邦刑事庁法第20k条に規定する措置⁽¹⁴⁾
 5. 連邦刑事庁法第16条に規定する住居内の措置⁽¹⁵⁾
 6. 基本法第10条関係法第1条第1項に規定する制限⁽¹⁶⁾
 7. 連邦憲法擁護法第9条第2項に規定する措置⁽¹⁷⁾
 8. 税関捜査業務法第22a条又は第32a条に規定する措置⁽¹⁸⁾

(11) Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319); Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl. I S. 1650). 刑事訴訟法第100a条及び連邦刑事庁法第20l条は、通信傍受を定めている。

(12) 刑事訴訟法第100c条は住居の内部における録音を、連邦刑事庁法第20h条は住居の内部又は外部における録音・録画を定めている。

(13) 刑事訴訟法第99条は、郵便物の押収を定めている。

(14) 連邦刑事庁法第20k条は、オンライン検索を定めている。オンライン検索とは、犯罪を犯す疑いが一定の事実により推定される者について、当事者に知られないように、特別なソフトウェアを用いて外部からコンピューターにアクセスし、データを収集する行為である。

(15) 連邦刑事庁法第16条は、連邦刑事庁の秘密捜査官は、刑事訴追において、身体、生命又は自由に対する危険を防止するために必要不可欠な場合には、捜査対象者の住居において秘密裏に録音・録画をしてもよい旨を定めている。

(16) 基本法第10条関係法第1条は、連邦及び州の情報機関による通信の秘密の制限を定めている。

(17) Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970). 連邦憲法擁護法第9条は、住居内の録音及び録画の措置による基本権の制限を定めている。

(18) Zollfahndungsdienstgesetz vom 16. August 2002 (BGBl. I S. 3202). 税関捜査業務法第22a条及び第32a条は、捜査官は、身体、生命又は自由に対する危険を防止するために必要不可欠な場合には、捜査又は調査対象者の住居において秘密裏に録音・録画をしてもよい旨を定めている。

9. 税関捜査業務法第 23a 条に規定する措置⁽¹⁹⁾

第 2 条第 1 文第 1 号及び第 2 号に規定する者又は第 2 条第 1 文第 3 号に規定する事項について〔本項〕第 1 文に規定するデータと他のデータの両方を登録しなければならない場合には、第 1 文に規定するデータのみ匿名化しなければならない。又は、入力する官庁は、第 1 文に規定するデータの登録を行わないことができる（登録の制限）。

第 5 条 データへのアクセス

(1) 参加官庁は、任務の遂行に必要な場合又は国際テロの解明若しくは対策のために必要な場合には、テロ対策データベースに登録されたデータを電子的な手続で利用することができる。照会した官庁は、検索結果が得られた場合には、次の各号に掲げるデータにアクセスすることができる。

1. a) 人物を照会した場合には、その基礎データ
- b) 第 2 条第 1 文第 3 号に規定する組織、集団、財団、企業、物、銀行口座、住所、通信接続識別番号、通信端末機、ウェブサイト又は電子メールアドレスを照会した場合には、登録されたデータ
2. 第 3 条第 1 項第 3 号に規定するデータ

照会した官庁は、〔氏名による〕検索結果が得られた場合において、データを入力した官庁が〔照会した官庁の〕要請に基づき承認したときには、当該の者について登録された拡張基礎データにアクセスすることができる。これに関する〔データを入力した官庁の〕決定は、その時々効力を有するデータ伝達に関する規定に従う。照会する官庁が第 3 条第 1 項第 1 号 a) に規定する氏名ではなく、拡張基礎データの項目で検索する場合において、検索結果が得られたときには、第 3 条第 1 項第 3 号に規定するデータのみアクセスすることができる。氏名で検索したにもかかわらず、複数のデータが得られた場合には、第 5 文⁽²⁰⁾の規定を準用する。

(2) 照会した官庁は、人の身体、生命、健康若しくは自由又は著しい価値を有する物であって、公益のために維持が必要であるものに対して現存する危険の防止のために特定の事実に基づいて不可欠である場合、かつ、〔照会した官庁の〕要請に基づくデータの伝達を〔データを入力した官庁が〕適時に行うことができない場合において（緊急の場合）、検索結果が得られたときには、直接拡張基礎データにアクセスすることができる。緊急の場合であるか否かについては、官庁の長又は当該の長により特別に委託された上級官吏が決定する。決定及びその理由は、文書に記録しなければならない。当該データへのアクセスについては、第 3 文に規定する決定についても記した上、記録しなければならない。データを入力した官庁には、遅滞なく、事後の同意を求めなければならない。〔データを入力した官庁が〕事後の同意を拒否した場合には、当該データを利用することはできない。照会した官庁は、当該データを遅滞なく削除するか、又は第 11 条第 3 項の規定により遮断〔Sperren〕⁽²¹⁾しなければならない。データが第三者に伝達されていた場合には、データの利用は許されない旨を、遅滞なく、当該第三者に対して通知しなければならない。

(3) 参加官庁においては、授権された職員のみがテロ対策データベースにアクセスする

(19) 税関捜査業務法第 23a 条は、通信の秘密の制限を定めている。

(20) 1 つ前の文を指す。

(21) 遮断とは、データの追加的な加工又は利用を制限する措置である（連邦データ保護法第 3 条第 4 項第 4 号）。

ことができる。

- (4) 「データの」照会に際しては、その目的及び緊急性を必ず申告しなければならず、目的及び緊急性は記録され、分かるように表示されなければならない。

第6条 データの利用

- (1) 「データを」照会した官庁は、検索結果が検索対象の人物又は第2条第1文第3号に規定する事項に該当するか否かの検証の目的⁽²²⁾、国際テロの解明又は対策の任務の遂行のための既知情報の伝達の要請の目的及び第6a条に規定する目的に限り、アクセスしたデータを利用することができる。国際テロの解明又は対策の任務の遂行以外の目的でデータを利用することは、次の各号に掲げる要件を全て満たす場合に限り許容される。
1. 特に重大な犯罪の訴追又は人の身体、生命、健康若しくは自由に対する危険の防止のために必要であること。
 2. データを入力した官庁が利用に同意したこと。
- (2) 緊急の場合には、「データを」照会した官庁は、国際テロに関連して第5条第2項第1文に規定する現存する危険の防止のために不可欠である場合に限り、アクセスしたデータを利用することができる。
- (3) 第1項第2文又は第2項の規定によりデータを利用する場合には、当該データにその旨を表示しなければならない。当該データを伝達した場合には、伝達を受けた官庁も、当該表示を保持しなければならない。これは、第3条第3項に規定する表示にも適用する。
- (4) 連邦刑事庁又は州刑事庁が連邦検事総長の要請に基づいて又はその委任を受けてテロ対策データベースを利用する場合には、連邦刑事庁又は当該州刑事庁は、刑事訴追の目的のために、連邦検事総長に対してアクセスしたデータを伝達する。連邦検事総長は、第1項第1文に規定する要請のために当該データを利用することができる。その際、刑事訴訟法第487条第3項⁽²³⁾の規定を準用する。

第6a条 プロジェクトに関連したデータの拡張利用

- (1) 連邦の参加官庁は、刑法典第129a条、第129b条及び第211条⁽²⁴⁾に規定する国際テロの犯罪が行われ、これにより人の身体、生命又は自由に対する危険が生じるであろう旨の推定が特定の事実に基づき証明される国際テロの企てに関する情報の収集及び分析の目的に合致する場合であって、個別事件に関するプロジェクトにおいて個別事件の一層の関連を解明するために必要であるときには、法律に定める任務の遂行のために、第4条の規定により匿名化されたデータを除き、第3条の規定によりデータベースに登録されたデータを拡張利用することができる⁽²⁵⁾。
- (2) 連邦の参加官庁は、通常より重い刑罰を科される国際テロの犯罪〔*qualifizierte Straftaten*〕の訴追のための個別事件に関するプロジェクトにおいて個別事件の一層の関連を解明するために必要である場合には、法律に定める任務の遂行のために、第4条の規定により匿名化されたデータを除き、第3条の規定によりデータベースに登録されたデータを拡張利用することができる。通常より重い刑罰を科される国際テロの犯罪とは、刑法典第89a条、第89b条、第91条、第102条、第129a条、第129b条、第211条又は第

(22) テロ対策データベースと、当該官庁が有するデータのデータの照合のこと。

(23) 刑事訴訟法第487条第3項は、データ伝達に際して責任を有する官庁を定めている。

(24) 刑法典第129a条はテロ組織の結成について、第129b条は外国における犯罪組織及びテロ組織について、第211条は謀殺について罰則を定めている。

(25) 「プロジェクト」及び「拡張利用」の定義については、それぞれ第6a条第4項及び第5項で定めている。

212 条⁽²⁶⁾に規定する構成要件を満たす国際テロの行為をいう。

- (3) 連邦の参加官庁は、通常より重い刑罰を科される国際テロの犯罪の防止のための個別事件に関するプロジェクトにおいて個別事件の更に広い関連を解明するために必要である場合には、かつ、そのような犯罪が行われるであろう旨の推定が特定の事実に基づき正当化される場合には、法律に定める任務の遂行のために、第 4 条の規定により匿名化されたデータを除き、第 3 条の規定によりデータベースに登録されたデータを拡張利用することができる。第 2 項第 2 文の規定を準用する。
- (4) プロジェクトとは、客観的に対象を限定した一定期間の任務であって、危険若しくは差し迫った損害、当該事情の関係者又は当該任務の目的若しくは影響に鑑みて特別な意義を有するものをいう。
- (5) [データの] 拡張利用とは、人、人の集団、金融機関及び物の関連付け、重要でない情報及び既知情報の削除、詳細な既知情報の追加並びに登録されたデータの統計的評価をいう。連邦の参加官庁は、このために、次の各号に掲げる手段をも用いてデータベースを検索し、人間関係並びに人、人の集団、金融機関及び物の関連を記述し、並びに検索基準を評価することができる。
1. 音声データ又は不完全なデータ
 2. 複数のデータ項目を使用した検索
 3. 人、金融機関、組織及び物の関連付け
 4. 検索対象期間の限定
- (6) プロジェクトのための [データの] 拡張利用において [テロ対策データベースへの] アクセス権を有するのは、[この法律の] 適用領域において直接当該任務を委任された者に限定されなければならない。プロジェクトのためのデータの拡張利用には、2 年以内の期限を付さなければならない。プロジェクトのための [データの] 拡張利用の要件が継続して存在し、かつ、プロジェクトにおいて得られた情報からプロジェクトの継続の必要性が生じた場合には、期限は、2 回まで、各々 1 年を限度として延長することができる。
- (7) プロジェクトのためのデータの利用は、申請に基づき、指示ことができる。申請は、官庁の長又はその代理人が書面により行わなければならない、理由を記載しなければならない。申請には、指示に必要な事項を全て記載しなければならない。指示は、申請を行う官庁の専門的監督 [Fachaufsicht]⁽²⁷⁾を行う連邦の最上級官庁が行う。指示は、書面による。指示書には、指示の理由、プロジェクトのためのデータの拡張利用に必要なデータの種類であって第 3 条に規定するもの、プロジェクトのためのデータの拡張利用の範囲及び期間を記さなければならない。プロジェクトのためのデータの拡張利用の範囲は、プロジェクトの目的達成に必要な程度に限定されなければならない。指示書には、理由を記載しなければならない。当該指示の理由においては、第 1 項から第 3 項までに定める要件、特に、事件の一層の解明のためにプロジェクトのためのデータの拡張利用が必

(26) 刑法典第 89a 条は国家を危うくする重大な暴力行為の予備について、第 89b 条は国家を危うくする重大な暴力行為を為すためにテロ組織と関係を持つことについて、第 91 条は国家を危うくする重大な暴力行為を為すための指導について、第 102 条は外国の機関及び代表者に対する攻撃について、第 212 条は故意による殺人について罰則を定めている。

(27) 専門的監督とは、上級官庁が下級官庁に対して行う監督で、任務の遂行が適法で目的に合っているか否かを検査する。Walter Krebs, „§ 108 Verwaltungsorganisation“, Josef Isensee und Paul Kirchhof, *Handbuch des Staatsrechts*, Band V, Dritte, völlig neubearbeitete und erweiterte Auflage, Heidelberg: C.F. Müller, 2007, S. 488.

要であることを明らかにしなければならない。指示を行う官庁は、データ保護法に基づく統制 [Kontrolle] を目的として、申請書及び指示書を2年間、ただし、[2年間以上にわたった場合には、] 少なくともプロジェクトのためのデータの拡張利用の期間、保存する。

- (8) 第7項の規定により指示された[データの]拡張利用は、基本法第10条審査会（基本法第10条関係法第15条第1項から第4項までに定める。）⁽²⁸⁾の同意がある場合に限る、実施することができる。差し迫った危険がある場合には、第7項第4文の規定により指示を行う官庁は、当該審査会の同意がなくても、[データの拡張利用の]実施を指示することができる。委員会が許容しない指示又は不必要と認める指示は、第7項第4文に規定する所管官庁により、遅滞なく取り消されなければならない。この場合には、データの拡張利用により得られたデータ及び既知情報を利用することは絶対に許されず、当該データは、遅滞なく削除しなければならない。
- (9) 第6項第3文の規定による期限の延長には、第7項及び第8項の規定を準用する。
- (10) プロジェクトの実施に際してのデータ保護法上の責任は、指示を行った官庁が負う。プロジェクトにおいて得られた既知情報の伝達は、一般的なデータ伝達の規則に従う。第6条第4項第1文の規定は、第1項に規定するプロジェクトにおいて得られた既知情報に準用する。
- (11) 第1条第1項の規定により参加の権利を有する州の官庁は、第1項から第10項までの規定に準じる州法の規定に基づいて、第1項から第3項までに規定する目的のために、第4条の規定により匿名化されたデータを除き、第3条の規定によりデータベースに登録されたデータを拡張利用することができる。第1文の規定は、第1条第2項に規定する法規命令によりデータベースへの参加の権利を有する州の官庁にも適用する。

第7条 既知情報の伝達

第6条第1項第1文に規定する要請に基づく参加官庁間の既知情報の伝達は、その時々々に効力を有するデータ伝達の規則に従う。

第8条 データ保護法上の責任

- (1) テロ対策データベースに登録したデータについて、特にデータ収集の合法性、データ入力可否並びにデータの正確性及び最新性についてのデータ保護法上の責任は、データを入力した官庁が負う。データを入力した官庁は、表示しなければならない。[データの]照会の可否の責任は、データを照会する官庁が負う。
- (2) データを入力した官庁のみが、当該データを変更し、訂正し、遮断し又は削除することができる。
- (3) 一の官庁が、他の官庁が入力したデータが正確でないと推定する根拠を有する場合には、当該官庁は、データを入力した官庁に早急にこれを通知し、データを入力した官庁は、当該通知を遅滞なく検証し、必要な場合には、当該データを遅滞なく訂正する。

第9条 記録並びに技術的及び組織的な措置

- (1) 連邦刑事庁は、全てのアクセスについて、データ保護の統制を目的として、日時、検索されたデータの確認を可能とする事項、アクセスに責任を負う官庁及び第5条第4

(28) 基本法第10条審査会は、連邦議会に設置された審査会で、通信の秘密の基本権を制限する情報機関の措置の全体を統制する。通信傍受等の監視措置には、同審査会の同意が必要である。渡邊斉志「ドイツ「信書、郵便及び電信電話の秘密の制限のための法律」の改訂」『外国の立法』No.217, 2003.8, pp.115-133. <http://dl.ndl.go.jp/view/download/digidepo_1000495_po_21703.pdf?contentNo=1&alternativeNo=>を参照。

項に規定するアクセスの目的を記録しなければならない。記録は、それを知ることがデータ保護の統制、データ保全、データ加工装置の適法な運用の確保又は機密事項の場合において知ったことの証明に必要な場合に限り、使用することができる。専ら第1文に規定する目的のために保存した記録は、2年後に削除しなければならない。

- (2) 連邦刑事庁は、連邦データ保護法第9条⁽²⁹⁾の規定により必要な技術的及び組織的な措置を講じなければならない。
- (3) 連邦刑事庁は、2017年8月1日を初回として3年ごとに、テロ対策データベースのデータ概要及び利用について連邦議会に報告する。当該報告書は、連邦議会への送付と同時に、連邦刑事庁のウェブサイトにおいて公表しなければならない。

第10条 データ保護法に基づく統制及び当事者に対する通知

- (1) 連邦データ保護受託者は、連邦データ保護法第24条第1項の規定により、データ保護の実施の統制の義務を負う。州の官庁がテロ対策データベースに入力したデータについては、第8条第1項の規定により当該州が責任を負う限りにおいて、州のデータ保護受託者が州におけるデータ保護の統制の実施と併せて、その統制を行うことができる。この場合、連邦データ保護受託者は州のデータ保護受託者と協力する。
- (2) 第1項に規定する機関は、その所管の範囲において、少なくとも2年ごとにデータ保護の実施を統制する義務を負う。
- (3) 連邦刑事庁は、第8条第1項第1文の規定によりデータ保護法上の責任を負い、[当事者に対する]通知の是非を当該官庁に適用される法規に基づいて審査する官庁と協議して、匿名化されずに登録されたデータについて、連邦データ保護法第19条⁽³⁰⁾の規定に基づき、[当事者に対する]通知を行う。匿名化されて登録されたデータについての[当事者に対する]通知は、データを入力した官庁に適用される法規に基づいて行う。

第11条 データの訂正、削除及び遮断

- (1) 不正確なデータは、訂正しなければならない。
- (2) 個人データは、その登録が許容されない場合又はそれを知ることが国際テロの解明又は対策のためにもはや必要でない場合には、削除しなければならない。当該データは、遅くとも、参加官庁に適用される法規に基づいて当該データに帰属する既知情報を削除しなければならないときまでには、削除しなければならない。
- (3) 削除すると当事者の保護すべき利益を侵害すると推定する根拠がある場合には、削除に代えて、遮断を行う。遮断されたデータは、削除を行わない理由に基づく限り、これにアクセスし、又は利用することができる。また、遮断されたデータは、特に価値の高い法益の保護に不可欠な場合で、かつ、そうしなければ事情の解明の見込みがないであろう場合若しくは事情の解明が著しく困難となるであろう場合又は当事者が同意した場合にも、これにアクセスし、又は利用することができる。
- (4) データを入力した官庁は、当該データに適用される期限の際、及び、個々のデータの処理の際、個人データを訂正又は削除しなければならないか否かを検証する。

第12条 [データベースの] 設置命令

連邦刑事庁は、共同データベースのために、[データベースの]設置命令において、

(29) 連邦データ保護法第9条は、データを収集、加工及び利用する機関は、データ保護のために技術的及び組織的な措置を講じなければならない旨を定めている。

(30) 連邦データ保護法第19条は、当事者に対する通知について定めている。

参加官庁と協議して次の各号に掲げる事項を定める。

1. 把握しているドイツ連邦共和国に関わる国際テロの範囲
2. 第1条第2項の規定により他に参加する警察執行官庁
3. 第3条第1項の規定により登録しなければならないデータ
4. 登録義務が課されるデータの入力
5. 参加官庁においてアクセス権を有する部署
6. 任務の目的及び緊急性の区分
7. 記録

設置命令は、連邦内務省、連邦首相府、連邦防衛省、連邦財務省及び州の参加官庁を所管する州の最上級官庁の同意を必要とする。設置命令の制定に際しては、事前に連邦データ保護受託者の意見を聴取しなければならない。

第13条 基本権の制限

信書、郵便及び電信電話の秘密の基本権（基本法第10条）並びに住居の不可侵の基本権（基本法第13条）は、この法律の基準に従って制限される。

（わたなべ ふくこ）

通信法（抄）

Telekommunikationsgesetz

国立国会図書館 調査及び立法考査局
海外立法情報課 渡辺 富久子訳

第 113a 条 [通信データ保存の] 義務を負う者及び補償

- (1) 第 113b 条から第 113g 条までに規定する通信データの保存、利用及び保全について義務を負うのは、最終利用者のために公の通信役務を提供する通信事業者 [Erbringer öffentlich zugänglicher Telekommunikationsdienste] とする。第 113b 条から第 113g 条までの規定により保存されるデータの全てを自ら生成又は加工しない通信事業者⁽¹⁾は、次の各号に掲げる義務を負う。
1. 役務提供の際に自らが生成又は加工しないデータが第 113b 条第 1 項の規定により保存されることを確保すること。
 2. 連邦ネットワーク庁⁽²⁾の要求に基づき、データを保存する者を遅滞なく通知すること。
- (2) 第 113b 条及び第 113d 条から第 113g 条までの規定の実施により [通信データ保存の] 義務を負う者に生じる必要な費用に対しては、過度の負担⁽³⁾の防止又は補償に必要であると認められる限りにおいて、適切な補償金が支払われなければならない。補償金額は、実際に生じた費用に基づく。補償の申請については、連邦ネットワーク庁が決定する。

第 113b 条 通信データの保存義務

- (1) 第 113a 条第 1 項に掲げる者は、次の各号に掲げる国内のデータを、当該各号に定める期間保存する義務を負う。
1. 第 2 項及び第 3 項に規定するデータ 10 週間
 2. 第 4 項に規定する通信の場所に関するデータ 4 週間
- (2) 通信事業者は、次の各号に掲げるデータを保存する。
1. 転送の場合も含め、送信側及び受信側の電話番号又は他の識別番号
 2. 通信の開始及び終了の日時及び標準時間帯⁽⁴⁾
 3. 電話サービスにおいて様々なサービスが利用可能である場合には、利用したサービス
 4. 携帯電話の場合には、さらに次の事項
 - a) 送信側及び受信側の国際移動体加入者識別番号⁽⁵⁾
 - b) 送信側及び受信側の国際移動体装置識別番号⁽⁶⁾

* この翻訳は、Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 17 des Gesetzes vom 19. Februar 2016 (BGBl. I S. 254) geändert worden ist <https://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf> から、Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I S. 2218) により定められた通信履歴の保存義務に関連する規定を訳出したものである。インターネット情報は、2016 年 5 月 31 日現在のものである。訳文中 [] 内の語句は、原綴も含め、訳者が補ったものである。

- (1) 通信サービスの提供を行うが、自身の通信施設を有さず、他の事業者の通信施設を使用するものをいう。
Deutscher Bundestag, Drucksache 16/5846, S. 69.
- (2) 連邦ネットワーク庁 (Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn) は、電力、ガス、通信、郵便、鉄道の分野のネットワークの規制官庁である。
- (3) 通信データの保存のために、通信事業者に不当なほどの費用がかかった場合のこと。
- (4) 標準時間帯とは、同じ標準時を使う地域全体をいう。
- (5) 国際移動体加入者識別番号とは、携帯の利用者に割り振られた固有の番号をいう。
- (6) 国際移動体装置識別番号とは、端末の ID をいう。

c) 前払式のサービスの場合には、最初のサービス利用の日時及び標準時間帯

5. インターネット電話の場合には、送信側及び受信側の IP アドレス及び割り当てられた利用者識別番号

次の各号に掲げる事項には、第 1 文の規定を準用する。

1. ショートメッセージ、マルチメディアメッセージ又は類似のメッセージの送信。この場合には、第 1 文第 2 号の規定は、「メッセージの送信及び受信の日時」と読み替える。
 2. 受信のなかった送信又はネットワーク管理者の介入があったために成功しなかった送信で、通信事業者が第 1 文に規定する通信データを第 96 条第 1 項第 2 文⁽⁷⁾に規定する目的のために保存又は記録したもの
- (3) インターネット通信事業者は、次の各号に掲げるデータを保存する。
1. インターネット利用のために利用者に割り当てられた IP アドレス
 2. インターネット利用が行われる一義的な接続識別番号及び割り当てられた利用者識別番号
 3. 割り当てられた IP アドレスの下でのインターネット利用の開始及び終了の日時及び標準時間帯
- (4) 携帯電話の利用の場合には、接続の送信側及び受信側において通信の開始時に利用したセル⁽⁸⁾の名称を保存しなければならない。インターネット通信事業者は、移動端末の利用の場合に、インターネット接続の開始時に利用したセルの名称を保存しなければならない。これらに加えて、当該セルの無線アンテナの地理的位置及び主ビーム方向⁽⁹⁾が分かるデータを保存しなければならない。
- (5) 通信の内容、閲覧したインターネットサイトに関するデータ及び電子メールサービスのデータは、この規定に基づいて保存してはならない。
- (6) 第 99 条第 2 項に規定する通信のデータ⁽¹⁰⁾は、この規定により保存してはならない。これは、第 99 条第 2 項に掲げる機関からの電話による通信に準用する。第 99 条第 2 項第 2 文から第 7 文までの規定を準用する。
- (7) データは、権限を有する機関から情報提供の要請があった場合に、遅滞なく提供することができるようにして保存しなければならない。
- (8) 第 113a 条第 1 項の規定により〔データの保存の〕義務を負う者は、遅滞なく、遅くとも第 1 項に規定するデータ保存の期限の経過後 1 週間以内に、第 1 項の規定により保存したデータを消去して復元不可能とするか、又は復元不可能な消去の措置を講じなければならない。

第 113c 条 データの利用

(1) 第 113b 条の規定により保存したデータは、次の各号に掲げる目的のために利用することができる。

1. 特に重大な犯罪の訴追のために第 113b 条に規定するデータの入手を刑事訴追官庁⁽¹¹⁾に対して許容する法律の規定に基づいて刑事訴追官庁がデータの伝達を要求した

(7) 第 96 条は、業務目的のための通信データの保存を定めている。

(8) セルとは、移動通信システムの無線基地局から電波が届いて通信ができる範囲「ゾーン」の小規模なものをいう。日経コミュニケーション編『通信ネットワーク事典 2003-2004 年版』日経 BP 社、2003、p.778。

(9) 主ビーム方向とは、セルのアンテナから放出される電波の最大放射方向をいう。竹田義行監修『ワイヤレス・ブロードバンド時代の電波 / 周波数教科書』インプレスネットビジネスカンパニー、2005、pp.92-96。

(10) 精神的な問題に関する相談又は社会生活上の問題に関する相談のための教会施設又は官庁との通信。

(11) 刑事訴追官庁は、検察庁である。

場合に、当該刑事訴追官庁に対する伝達

2. 人の身体、生命若しくは自由又は連邦若しくは州の存立にとっての具体的な危険の防止のために第 113b 条に規定するデータの入手を州の危険防止官庁⁽¹²⁾に対して許容する法律の規定に基づいて州の危険防止官庁がデータの伝達を要求した場合に、当該州の危険防止官庁に対する伝達

3. 第 113 条第 1 項第 3 文に規定する情報提供⁽¹³⁾のための通信事業者による利用

(2) 第 113a 条第 1 項の規定により [データの保存の] 義務を負う者は、第 113b 条の規定により保存したデータを第 1 項に掲げる目的以外の目的で利用することはできない。

(3) データの伝達は、第 110 条第 2 項に規定する法規命令⁽¹⁴⁾及び第 110 条第 3 項に規定する技術指針⁽¹⁵⁾の基準に従って行う。データは、当該データが第 113b 条の規定により保存されたものであることが分かるように表示しなければならない。データが他の機関に伝達された場合には、当該機関は、当該表示を保持しなければならない。

第 113d 条 データ保全の保証

第 113a 条第 1 項の規定により [データの保存の] 義務を負う者は、技術的及び組織的な措置により、かつ、最新の技術水準に応じて、第 113b 条第 1 項の規定により保存したデータが権限なく閲覧及び利用されないことを保証しなければならない。措置は、特に次の各号に掲げるものを含む。

1. 特に安全な暗号化技術の使用
2. 通常の任務のための保存場所とは別の場所における保存
3. インターネットから切り離されたデータ加工装置に対してインターネットからのアクセスがなされないように高度の保護措置を講じた保存
4. [データの保存の] 義務を負う者により特に権限を与えられた者に限ったデータ加工装置へのアクセス権
5. データへのアクセスに際して、[データの保存の] 義務を負う者により権限を与えられた者が 2 人以上関与すること。

第 113e 条 記録

(1) 第 113a 条第 1 項の規定により [データの保存の] 義務を負う者は、データ保護の統制を目的として、第 113b 条第 1 項の規定により保存したデータへのあらゆるアクセス、特に閲覧、複写、変更、削除及び遮断の記録を確実なものにしなければならない。特に、次の各号に掲げる事項を記録しなければならない。

1. アクセスの日時
2. データにアクセスした者
3. アクセスの目的及び方法

(2) データ保護の統制以外の目的で記録データを利用することはできない。

(12) 危険防止官庁は、警察である。

(13) 通信事業者は、検察、警察及び情報機関の要求に基づいた情報提供（契約データ及び契約者の個人データ）のために、提供するデータを動的 IP アドレスを用いて特定することができ、自動的に分析することができる（第 113 条第 1 項第 3 文）。

(14) 通信傍受の措置の技術的及び組織的な実施に関する法規命令。Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation vom 3. November 2005 (BGBl. I S. 3136)。

(15) 通信傍受のために法律上規定する措置を実施するための技術指針。Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften. Ausgabe 6.3. (Vfg. 18/2016), BNetzA Abl. Nr.6 vom 6. April 2016, S.716。

- (3) 第 113a 条第 1 項の規定により [データの保存の] 義務を負う者は、1 年後に記録データを削除することを保証しなければならない。

第 113f 条 要件一覧

- (1) 第 113b 条から第 113e 条までに規定する義務の実施に際しては、特に高水準のデータ保護及びデータの質を保証しなければならない。連邦ネットワーク庁が連邦情報技術安全庁⁽¹⁶⁾及び連邦データ保護受託者の了解を得て策定する技術指針及び他の措置一覧に含まれる全ての要件を満たした場合に、当該水準に達しているものとみなす。
- (2) 連邦ネットワーク庁は、第 1 項第 2 文に規定する一覧に含まれる要件が遵守されているか否かを継続して検証し、その際、最新の技術水準及び専門家の意見を考慮する。連邦ネットワーク庁は、一覧の変更の必要性を認めた場合には、連邦情報技術安全庁及び連邦データ保護受託者の了解を得て一覧を変更しなければならない。
- (3) 第 109 条⁽¹⁷⁾第 6 項第 2 文及び第 3 文の規定を準用する。第 109 条第 7 項の規定は、「第 109 条第 1 項から第 3 項までに規定する要件」を「[第 109 条] 第 1 項第 1 文、第 113b 条第 7 項及び第 8 項、第 113d 条並びに第 113e 条第 1 項及び第 3 項に規定する要件」と読み替えて適用する。

第 113g 条 安全対策指針

第 113a 条第 1 項の規定により [データの保存の] 義務を負う者は、第 109 条第 4 項⁽¹⁸⁾に規定する安全対策指針において、次の各号に掲げる事項を追加して記載する。

1. 第 113b 条から第 113e 条までに規定する義務の遂行のために運営するシステム
2. 当該システムから生じ得る危険
3. 当該危険の防止のため及び第 113b 条から第 113e 条までに規定する義務の遂行のために策定し又は計画した技術指針又は他の措置

第 113a 条第 1 項の規定により [データの保存の] 義務を負う者は、第 113b 条に規定する [データの] 保存の開始後遅滞なく及び安全対策指針の変更の際に遅滞なく、安全対策指針を連邦ネットワーク庁に提出しなければならない。第 113a 条第 1 項の規定により [データの保存の] 義務を負う者は、安全対策指針に変更がない場合には、2 年ごとに、連邦ネットワーク庁に対して変更のない旨を文書で報告しなければならない。

（わたなべ ふくこ）

(16) 連邦情報技術安全庁（Bundesamt für Sicherheit in der Informationstechnik）は、連邦内務省の下部機関であり、国家レベルの情報セキュリティを所管する。

(17) 第 109 条は、通信の秘密及び利用者の個人情報の保護のために、通信事業者が講じなければならない技術的保護措置について定めている。第 6 項第 2 文は、安全対策指針の策定の際に関係者が参加すること、第 3 文は、安全対策指針が連邦ネットワーク庁により公表されることを定めている。第 7 項は、連邦ネットワーク庁は、通信事業者に対して第三者機関による検査を命じることができることを定めている。

(18) 第 109 条第 4 項は、通信事業者の策定する安全対策指針には、運用する通信システム及び提供する通信サービス等が記載されることを定めている。

刑事訴訟法（抄）

Strafprozeßordnung

国立国会図書館 調査及び立法考査局
海外立法情報課 渡辺 富久子訳

第 100g 条 通信データの入手

(1) 特定の事実に基づき、正犯又は共犯として次の各号に掲げる犯罪を犯した疑いがある者については、事実関係の解明に必要で、かつ、事案の重要性に鑑みて適切な限りにおいて、通信データ（通信法第 96 条第 1 項）⁽¹⁾を入手することができる。

1. 個別事件に鑑みて重要な意味を持つ犯罪、特に第 100a 条第 2 項⁽²⁾に掲げる犯罪又は未遂が可罰的である場合には未遂罪若しくは犯罪として処罰される予備罪

2. 通信を用いた犯罪

第 1 文第 2 号の場合には、他の方法では事実関係の解明の見込みがないであろう場合に限り、当該措置を行うことができる。この項の規定による通信の場所に関するデータの入手は、事後に発生した通信データ又はリアルタイムの通信データについて、第 1 文第 1 号の場合に限り、かつ、事実関係の解明又は被疑者の居場所の特定に必要な限りにおいて、行うことができる。

(2) 特定の事実に基づき、正犯又は共犯として第 2 文に掲げる特に重大な犯罪を犯した疑いがある者又は未遂が可罰的である場合には未遂罪を犯した疑いがある者について、行為が個別事件において特に重大である場合には、事実関係の解明に必要な限りにおいて又は他の方法では被疑者の居場所の特定が著しく困難となり若しくは見込みがない限りにおいて、かつ、事案の重要性に鑑みて適切な限りにおいて、通信法第 113b 条の規定により保存した通信データを入手することができる。第 1 文に規定する特に重大な犯罪は、次の各号に掲げるものとする。

1. 刑法典⁽³⁾に規定する犯罪

a) 第 80 条、第 81 条、第 82 条及び第 89a 条に規定する平和に対する反逆 [Friedensverrat]⁽⁴⁾、内乱 [Hochverrat]⁽⁵⁾ 及び民主主義的法治国家を危うくする行為⁽⁶⁾

* この翻訳は、Strafprozeßordnung（刑事訴訟法）in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 1 des Gesetzes vom 21. Dezember 2015 (BGBl. I S. 2525) geändert worden ist <<https://www.gesetze-im-internet.de/bundesrecht/stpo/gesamt.pdf>> から、Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten（通信データの保存義務及び保存期限を定めるための法律）vom 10. Dezember 2015 (BGBl. I S. 2218) により定められた通信履歴の保存義務に関連する規定を訳出したものである。以下、インターネット情報は、2016 年 5 月 31 日現在のものである。訳文中 [] 内の語句は、原綴も含め、訳者が補ったものである。また、翻訳に際しては、『ドイツ刑事訴訟法典』（法務資料第 460 号）法務省大臣官房司法法制部司法法制課，2001；『ドイツ刑法典』（法務資料第 461 号）法務省大臣官房司法法制部司法法制課，2007 を参考にした。

(1) 通信事業者が業務目的で保存する電話番号や通信の日時等のデータ。

(2) 第 100a 条第 2 項は、その捜査のために通信傍受を行うことができる犯罪（平和に対する反逆、殺人、性犯罪等）を列挙している。

(3) Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1988 (BGBl. I S. 3322)。

(4) 刑法典第 80 条に規定する平和に対する反逆は、侵略戦争の予備である。

(5) 刑法典第 81 条に規定する内乱は、ドイツ連邦共和国の存立の侵害又は憲法秩序の変革（連邦に対する内乱）である。第 82 条に規定する内乱は、1 州の領域の他州への併合若しくは州からの分離又は憲法秩序の変革（州に対する内乱）である。

(6) 刑法典第 89a 条に規定する民主主義的法治国家を危うくする行為とは、国家を危うくする重大な暴力行為の予備である。

並びに第 97b 条とも関連する第 94 条、第 95 条第 3 項及び第 96 条第 1 項並びに第 97a 条、第 98 条第 1 項第 2 文、第 99 条第 2 項、第 100 条及び第 100a 条第 4 項に規定する国家反逆 [Landesverrat]⁽⁷⁾ 及び対外的安全を危うくする行為⁽⁸⁾ の犯罪

- b) 第 125a 条に規定する犯情の特に重い騒乱 [Landfriedensbruch]、第 129 条第 4 項後半と関連する同条第 1 項に規定する犯罪組織の結成並びに第 129b 条第 1 項とも関連する第 129a 条第 1 項、第 2 項、第 4 項及び第 5 項第 1 文に規定するテロ組織の結成
- c) 第 176a 条、第 176b 条、第 177 条第 2 項第 2 文第 2 号及び第 179 条第 5 項第 2 号の場合における性的自己決定権⁽⁹⁾ に対する犯罪⁽¹⁰⁾
- d) 第 184b 条第 2 項及び第 184c 条第 2 項の場合における児童及び青少年ポルノの頒布、入手及び所持
- e) 第 211 条及び第 212 条に規定する謀殺 [Mord] 及び故意による殺人 [Totschlag]
- f) 第 234 条、第 234a 条第 1 項及び第 2 項、第 239a 条並びに第 239b 条の場合における人身の自由に対する犯罪⁽¹¹⁾ 並びに第 232 条第 3 項、第 4 項又は第 5 項及び第 233 条第 3 項に規定する性的搾取及び労働力搾取のための人身取引で重罪であるもの
- g) 第 244a 条第 1 項に規定する犯情の重い集団窃盗、第 250 条第 1 項又は第 2 項に規定する犯情の重い強盗、第 251 条に規定する人の死亡を伴う強盗、第 255 条に規定する強盗の刑で罰せられる恐喝、第 253 条第 4 項第 2 文に掲げる要件⁽¹²⁾ がある場合における同条に規定する恐喝、第 260a 条第 1 項に規定する集団による業としての盗品等蔵匿並びに第 261 条第 4 項第 2 文に掲げる要件⁽¹³⁾ がある場合における同条に規定する資金洗浄及び不法に入手した財産の隠匿
- h) 第 306 条から第 306c 条まで、第 307 条第 1 項から第 3 項まで、第 308 条第 1 項から第 3 項まで、第 309 条第 1 項から第 4 項まで、第 310 条第 1 項、第 313 条、第 314 条、第 315 条第 3 項、第 315b 条第 3 項、第 316a 条及び第 316c 条の場合における公共危険罪⁽¹⁴⁾

2. 滞在法⁽¹⁵⁾ に規定する犯罪

- a) 第 96 条第 2 項に規定する外国人の密入国

(7) 刑法典第 94 条は国家機密の漏洩について、第 95 条第 3 項は重大な国家機密の公表について、第 96 条第 1 項は国家機密漏洩のための国家機密の入手について、第 97a 条は国家機密とはならない秘密の漏洩について、第 98 条第 1 項第 2 文は外国のための重大なスパイ活動について、第 99 条第 2 項は外国の情報機関のための重大なスパイ活動について罰則を定めている。

(8) 刑法典第 100 条はドイツ連邦共和国に戦争を招来する目的で外国の政府等と関係を結ぶことについて、第 100a 条第 4 項は国家反逆のための重大な物の偽造及び情報の捏造について罰則を定めている。

(9) 性的自己決定権とは、誰といかなる性行為を行うかについて、公権力から干渉されることなく、自ら決定することのできる権利である。中里見博「「セックスワーク」・性的自己決定権・人格権」憲法理論研究会編『憲法学の最先端（憲法理論叢書 17）』敬文堂，2009，p.22。

(10) 刑法典第 176a 条は特に犯情の重い児童に対する性的虐待について、第 176b 条は人の死亡を伴う児童に対する性的虐待について、第 177 条は性行為の強要及び強姦について、第 179 条は反抗不能な者に対する性的虐待について罰則を定めている。

(11) 刑法典第 234 条は人身強取について、第 234a 条は拉致について、第 239a 条は恐喝による人身強取について、第 239b 条は人質について罰則を定めている。

(12) 第 253 条第 4 項第 2 文は、犯情の特に重い恐喝の要件として、行為者が業として行為を行ったこと及び恐喝を継続的に行うために結成された集団の構成員として行為を行ったことを挙げている。

(13) 第 261 条第 4 項第 2 文は、犯情の特に重い資金洗浄の要件として、行為者が業として行為を行ったこと及び資金洗浄を継続的に行うために結成された集団の構成員として行為を行ったことを挙げている。

- b) 第 97 条に規定する人の死亡を伴う密入国及び業としての密入国及び集団による密入国
- 3. 対外経済法⁽¹⁶⁾に規定する犯罪
第 17 条第 1 項から第 3 項まで並びに第 18 条第 7 項及び第 8 項に規定する犯罪
- 4. 麻薬法⁽¹⁷⁾に規定する犯罪
 - a) 第 29 条第 3 項第 2 文第 1 号に掲げる要件がある場合における同条第 1 項第 1 文第 1 号、第 5 号、第 6 号、第 10 号、第 11 号又は第 13 号及び第 3 項に規定する特に重大な犯罪
 - b) 第 29a 条、第 30 条第 1 項第 1 号、第 2 号及び第 4 号並びに第 30a 条に規定する犯罪
- 5. 麻薬前駆物質管理法⁽¹⁸⁾に規定する犯罪
第 19 条第 3 項第 2 文に掲げる要件がある場合に同条第 1 項に規定する犯罪
- 6. 武器管理法⁽¹⁹⁾に規定する犯罪
 - a) 第 21 条とも関連する第 19 条第 2 項又は第 20 条第 1 項に規定する犯罪
 - b) 第 22a 条第 2 項と関連する同条第 1 項に規定する特に重大な犯罪
- 7. 国際刑法典⁽²⁰⁾に規定する犯罪
 - a) 第 6 条に規定する民族謀殺
 - b) 第 7 条に規定する人道に対する犯罪
 - c) 第 8 条から第 12 条までに規定する戦争犯罪
- 8. 銃器法⁽²¹⁾に規定する犯罪
 - a) 第 51 条第 2 項と関連する同条第 1 項に規定する特に重大な犯罪
 - b) 第 52 条第 5 項と関連する同条第 1 項第 1 号に規定する特に重大な犯罪
- (3) 1 のセル [Funkzelle]⁽²²⁾において発生した全ての通信データは、次の各号に掲げる要件を全て満たす場合に限り、入手することができる(セル通信データ照会[Funkzellenabfrage])。
 - 1. 第 1 項第 1 文第 1 号の要件が満たされていること。
 - 2. データの入手が事案の重要性に鑑みて適切であること。

(14) 刑法典第 306 条は放火について、第 306a 条は犯情の重い放火について、第 306b 条は犯情の特に重い放火について、第 306c 条は人の死亡を伴う放火について、第 307 条は核エネルギーにより爆発を引き起こすことについて、第 308 条は爆薬により爆発を引き起こすことについて、第 309 条は電離放射線の濫用について、第 310 条は爆発犯罪又は放射線犯罪の予備について、第 313 条は出水を引き起こすことについて、第 314 条は公共に対する危険な毒害物質について、第 315 条は鉄道交通、船舶交通、航空交通に対する危険な侵害について、第 315b 条は道路交通に対する危険な侵害について、第 316a 条は運転者に対する強盗による攻撃について、第 316c 条は航空交通及び海上交通に対する攻撃について罰則を定めている。

(15) Aufenthaltsgesetz in der Fassung der Bekanntmachung vom 25. Februar 2008 (BGBl. I S. 162). 滞在法は、外国人の出入国管理及び滞在について定める法律である。滞在法の解説及び 2007 年時点の全訳は、戸田典子「ドイツの滞在法―「外国人法」から EU「移民法」へ―」『外国の立法』No.234, 2007.12, pp.4-112. <http://dl.ndl.go.jp/view/download/digidepo_1000294_po_023401.pdf?contentNo=1&alternativeNo=>を参照。

(16) Außenwirtschaftsgesetz vom 6. Juni 2013 (BGBl. I S. 1482). 対外経済法は、外国との物品、役務、資本等の取引について定める法律である。

(17) Betäubungsmittelgesetz in der Fassung der Bekanntmachung vom 1. März 1994 (BGBl. I S. 358). 麻薬法第 29 条第 3 項は、特に重大な麻薬犯罪を定めている。

(18) Grundstoffüberwachungsgesetz vom 11. März 2008 (BGBl. I S. 306). 麻薬前駆物質とは、麻薬の製造に使用される化学物質である。麻薬前駆物質管理法第 19 条第 3 項は、特に重大な犯罪を定めている。

(19) Gesetz über die Kontrolle von Kriegswaffen in der Fassung der Bekanntmachung vom 22. November 1990 (BGBl. I S. 2506).

(20) Völkerstrafgesetzbuch vom 26. Juni 2002 (BGBl. I S. 2254).

(21) Waffengesetz vom 11. Oktober 2002 (BGBl. I S. 3970, 4592; 2003 I S. 1957).

(22) セルは、1 つの携帯電話の基地局から電波が届く範囲である。

3. 事実関係の解明又は他の方法による被疑者の居場所の特定の見込みがないこと又は著しく困難であること。

通信法第 113b 条の規定により保存した通信データは、第 2 項に規定する要件を満たす場合に限り、セル通信データ照会として照会することができる。

- (4) 第 53 条第 1 項第 1 文第 1 号から第 5 号までに掲げる者⁽²³⁾について、第 3 項第 2 文とも関連する第 2 項に規定する通信データを入手することによりこれらの者に対して〔職業上の秘密について刑事事件において〕証言の拒否が許される情報を得ることになると予想される場合には、当該通信データの入手を行ってはならない。それにもかかわらず得た情報は、利用してはならない。この入手に関する記録は、遅滞なく消去しなければならない。当該情報を得た事実及び記録の消去の事実は、文書に記録しなければならない。捜査が、第 53 条第 1 項第 1 文第 1 号から第 5 号までに掲げる者でない者を対象とするが、この者に対して証言の拒否が許される情報を得ることになると予想される場合にも、第 2 文から第 4 文までの規定を準用する。第 160a 条第 3 項及び第 4 項の規定を準用する。
- (5) 公共のための通信事業者以外から通信データを入手する場合には、通信データの入手は、通信の終了後に、一般的な規定に基づいて行う⁽²⁴⁾。

第 100h 条～第 101 条（略）

第 101a 条 裁判所の決定 [Entscheidung]、データの表示及び分析並びに通信データの入手の際の〔当事者への〕通知義務

- (1) 第 100g 条の規定により通信データを入手する際には、次の各号に掲げる基準に従って、第 100a 条第 3 項及び第 100b 条第 1 項から第 4 項⁽²⁵⁾までの規定を準用する。
1. 第 100b 条第 2 項第 2 文に規定する決定主文において、伝達すべきデータ及びデータを伝達すべき期間を明瞭に記す。
 2. 第 100b 条第 3 項第 1 文の規定により情報提供の義務を負う者⁽²⁶⁾は、伝達したデータのうち、どのデータが通信法第 113b 条の規定により保存されたかをも通知しなければならない。

第 100g 条第 3 項第 2 文とも関連する同条第 2 項の場合においては、第 1 文にかかわらず、第 100b 条第 1 項第 2 文及び第 3 文⁽²⁷⁾の規定は適用しない。第 100g 条第 3 項に規定するセル通信データ照会に際しては、第 100b 条第 2 項第 2 文第 2 号⁽²⁸⁾の規定にかかわらず、通信の場所及び時間を狭く限定し、十分に特定すれば足りる。

- (2) 第 100g 条の規定による措置が命ぜられる場合又は延長される場合には、個別事件の命令の理由欄において、入手するデータの範囲及び当該データが収集されるべき期間

(23) 第 53 条は、聖職者、弁護士、医師、連邦及び州議会議員等は、刑事事件において証人として証言を拒否することができる旨を定めている。

(24) 一般的な規定とは、例えば刑事訴訟法第 94 条（押収）であり、通信データの入手は、電磁記録媒体や紙媒体の通信記録の押収により行われる。Deutscher Bundestag, Drucksache 18/5088, S. 33.

(25) 第 100a 条第 3 項は通信傍受の対象者を、第 100b 条は通信傍受のための裁判所による命令を定めている。

(26) 通信事業者を指す。

(27) 第 100b 条第 1 項第 2 文及び第 3 文の規定は、遅滞のおそれがある場合には、裁判所による命令でなく、検察庁の命令により通信傍受を行うことができる旨を定めている。

(28) 第 100b 条第 2 項第 2 文第 2 号は、裁判官が行う通信傍受の命令において、電話番号等の通信の識別番号を掲げなければならない旨を定めている。

をも考慮して、措置の必要性及び適切性の概要を記さなければならない。

- (3) 第 100g 条の規定により入手した個人データは、その旨を表示し、遅滞なく評価しなければならない。表示の際には、当該個人データが通信法第 113b 条の規定により保存されたデータであるか否かを明瞭に記さなければならない。当該個人データが他の機関に伝達された場合には、当該機関は、当該表示を保持しなければならない。個人データの消去については、第 101 条第 8 項⁽²⁹⁾の規定を準用する。
- (4) 第 100g 条第 3 項第 2 文とも関連する同条第 2 項の規定により入手した利用可能な個人データは、当該通信の当事者の同意なく、次の各号に掲げる目的に限り、かつ、次の各号に掲げる基準に従って、利用することができる。
1. 第 100g 条第 3 項第 2 文とも関連する同条第 2 項の規定により措置を命ずることができる犯罪の解明又はそのような犯罪の被疑者の居場所の特定のための刑事手続でなければならない。
 2. 人の身体、生命若しくは自由又は連邦若しくは州の存立にとっての具体的な危険の防止を目的とした伝達（通信法第 113c 条第 1 項第 2 号）でなければならない。
- データを「他の機関に」伝達する機関は、当該伝達及びその目的を文書により記録しなければならない。第 1 文第 2 号に規定するデータが、危険防止のために講じられた措置の裁判前又は裁判における検証のためにもはや必要でなくなった場合には、危険防止を所管する機関⁽³⁰⁾は、当該データに関する記録を遅滞なく消去しなければならない。消去については、文書により記録しなければならない。[措置の] 裁判前又は裁判における検証のために「データの」消去を見合わせている場合には、当該データはこの目的に限り利用することができる。他の目的のための利用は許されない。
- (5) 通信法第 113b 条の規定により保存された利用可能な個人データが、警察法において定められた措置により得られた場合には、第 100g 条第 3 項第 2 文とも関連する同条第 2 項の規定による措置を命ずることができる犯罪の解明又はそのような犯罪の被疑者の居場所を特定する目的に限り、当該通信の当事者の同意なく、刑事手続において利用することができる。
- (6) 当該通信の当事者には、第 100g 条の規定により通信データを入手した旨を通知しなければならない。第 101 条第 4 項第 2 文から第 5 文まで及び第 5 項から第 7 項まで⁽³¹⁾の規定は、次の各号に掲げる基準に従って準用する。
1. 第 101 条第 4 項第 3 文の規定により通知を行わない場合⁽³²⁾には、管轄の裁判所による命令を必要とする。
 2. 第 101 条第 6 項第 1 文⁽³³⁾の規定にかかわらず、同条第 5 項第 1 文の規定により通知を見合わせる場合⁽³⁴⁾には、常に管轄の裁判所による命令を必要とし、また、初回の通知の見合わせには 12 月以内の期限を付さなければならない。

(29) 第 101 条第 8 項は、通信傍受等の秘密の捜査において得られた個人情報で、不要なものは、遅滞なく消去しなければならない、消去の事実を記録しなければならない旨を定めている。

(30) 危険防止（Gefahrenabwehr）とは、主に犯罪の防止であり、危険防止を所管する機関は警察である。

(31) 第 101 条第 4 項から第 7 項までの規定は、秘密裏の捜査に際しての当事者への通知、通知を行わない場合、通知を行わないことに関する裁判所の決定等を定めている。

(32) 通知を行わない場合における通信の当事者の利益が、通知の利益を上回る場合。

(33) 第 101 条第 6 項第 1 文は、通知の見合わせの更新には、その都度裁判所の同意を必要とする旨を定めている。

(34) 人の生命、身体及び自由又は相当な価額の財産に危険がある場合。

第 101b 条 通信データの入手に関する統計

第 100g 条に規定する措置については、第 100b 条第 5 項⁽³⁵⁾の規定に準じて毎年統計を作成しなければならない、当該統計には、次の各号に掲げる項目を設けるものとする。

1. 第 100g 条第 1 項、第 2 項及び第 3 項に規定する措置の各々について、次の件数
 - a) 当該措置が実施された手続の件数
 - b) 当該措置の最初の命令の件数⁽³⁶⁾
 - c) 当該措置の延長の命令の件数
2. 固定電話、携帯電話及びインターネットの各々について、通信データの入手の命令の時から経過した週数ごとに、次の件数
 - a) 第 100g 条第 1 項に規定する〔措置の〕命令の件数
 - b) 第 100g 条第 2 項に規定する〔措置の〕命令の件数
 - c) 第 100g 条第 3 項に規定する〔措置の〕命令の件数
 - d) 照会したデータの一部を入手できなかったため、その一部について成果のなかった命令の件数
 - e) データを全く入手できなかったため、成果のなかった命令の件数

（わたなべ ふくこ）

(35) 第 100b 条第 5 項は、州及び連邦刑事総長は、連邦刑事局に対して、通信傍受の措置について毎年報告する旨を定めている。

(36) 延長の命令を含まない。