総務省 情報通信政策レビュー 第9号 2014年11月
Information and Communications Policy Review No.9 November, 2014

特別寄稿

インターネットにおける基本権保障のあり方

西土　彰一郎[1]

要　旨

日本において電気通信事業者は、法律上、「通信の秘密の保護」と「差別的取扱の禁止」により、通信の伝達のみに関わっていれば足りると考えられてきた。この「基本設計」は、インターネットにおける通信の秘密のあり方をも規定している。しかし近年、「安全・安心なインターネット」の提供を重視する立場から、以上の「基本設計」をインターネットにまで及ぼすことに対して、厳しい批判が加えられている。それによると、インターネットの安全性を実現するうえで重要な役割を担っているインターネット媒介者が通信データを活用できるようにするため、通信の秘密の保護領域を限定すべきであるという。しかし、たとえば最近のドイツの基本権理論を踏まえるならば、むしろ従来の日本の「基本設計」こそが憲法上要請されているものと結論づけることができる。

キーワード：通信データ、インターネット媒介者、通信の秘密、情報自己決定権、デジタル基本権

１．はじめに

近年、日本の電気通信法制はインターネットをめぐる諸問題に十分対応できていないのではないかと、しばしば批判されている[2]。他方で、従来の通信の秘密の解釈を反省することにより、こうした批判に応答を試みる憲法学説も現れている[3]。

本稿は、こうした議論を参考にしたうえで、日本の電気通信法制のモデルを、通信の秘密を含むインターネットの自由の観点から再評価することを目的としている。その際、イ

---

[1] 成城大学法学部教授

[2] 高橋郁夫＝吉田一雄「『通信の秘密』の数奇な運命（憲法）」『情報ネットワーク・ローレビュー』5巻44頁以下（2006年）、高橋郁夫＝林紘一郎＝船橋信＝吉田一雄「通信の秘密の数奇な運命（制定法）」『情報ネットワーク・ローレビュー』8巻1頁以下（2009年）、林紘一郎＝田川義博「『心地よいDPI（Deep Packet Inspection）』と『程よい通信の秘密』」『情報セキュリティ総合科学』4号3頁以下（2012年11月）、情報セキュリティ大学院大学「インターネットと通信の秘密」研究会報告書「インターネット時代の『通信の秘密』再考」（2013年6月、〈http://lab.iisec.ac.jp/~hayashi/610REPORTIII.pdf〉）、田川義博「インターネット利用における『通信の秘密』」『情報セキュリティ総合科学』5号1頁以下（2013年11月）、高橋郁夫「インターネット媒介者の役割と『通信の秘密』」『Nextcom』16号（2013年）4頁以下。

[3] 宍戸常寿「通信の秘密に関する覚書」長谷部恭男＝安西文雄＝宍戸常寿＝林知更（編）『現代立憲主義の諸相―高橋和之先生古稀記念』（有斐閣、2013年）489頁以下、曽我部真裕「通信の秘密の憲法解釈論」『Nextcom』16号（2013年）14頁以下。

ンターネットにおける基本権保障のあり方をめぐる最近のドイツの議論を参照しつつ、それを日本法へと照射することにより、日本の電気通信法制モデルの意義を析出したいと思う。

問題の所在を明らかにするため、まずは、ごく簡単に日本の電気通信法制を見ておく。

２．日本の電気通信法制のモデル

２．１．上位概念としての検閲の禁止

電気通信事業法は、電気通信事業者に対して通信検閲の禁止（3 条）と通信の秘密の保護（4 条）を課している。規範の名宛人等で違いはありうるものの、通信検閲の禁止と通信の秘密の保護は、憲法 21 条 2 項に由来するものとして理解されてきた。

憲法上の通信の秘密の保護法益をめぐっては、そもそも争いがある。現在では、プライバシー権のみを挙げる、あるいは表現の自由とプライバシー権の二つを挙げつつ後者に力点を置く学説が多い[4]。また、通信の秘密の保護の対象は、通信内容のみならず、通信当事者の住所、氏名、発受日時・場所、通信回数などの外形的事項（以下、通信データと記す）をも含むと考えられている。通信の秘密の保護の核心は通信内容であるものの、通信データから通信内容が推知されうる場合がある以上、通信データも保護の対象とすべきであるからであるという[5]。ただし、この見解は、「プライバシー固有情報」と「プライバシー外延情報」を分けて把握する「自己情報コントロール権」説を踏まえているように思える[6]。プライバシー権の理解によっては、通信データをも独立に保護すべきことになろう[7]。いずれにせよ、事業法上、電気通信事業者は、通信当事者の通信内容と通信データを積極的に取得、窃用、漏洩することが禁止されることになる。

事業法上禁止される検閲に関しては、最高裁判所による憲法 21 条 2 項の検閲概念の定義[8]を参考にしつつ、①通信事業者の取扱中に係る通信の内容またはそれを通じて表現される思想の内容を調査し、②場合によっては、不適当と認めるものの発信を禁止すること、と規定される[9]。このうち、①を捉えて、検閲を通信の秘密の侵害とほぼ同義であるとの指摘

---

4 学説の整理として、参照、岡崎俊一「通信の秘密の保護とその課題」多賀谷一照＝松本恒雄編『情報ネットワークの法律実務（二）』（第一法規、2004 年）3303 頁以下、鈴木秀美「通信の秘密」大石眞＝石川健治（編）『憲法の争点』（有斐閣、2008 年）136 頁、宍戸・前掲注（3）500 頁以下、曽我部・前掲注（3）15 頁以下など。

5 たとえば、郵政省「電気通信サービスにおける情報流通ルールに関する研究会報告書」（1997 年 12 月、〈http://www.soumu.go.jp/main_sosiki/joho_tsusin/pressrelease/japanese/denki/980105j601.html〉）3 章 4 節を参照。

6 参照、佐藤幸治『日本国憲法論』（成文堂、2011 年）181 頁以下。

7 参照、高橋和之「インターネット上の名誉毀損と表現の自由」高橋和之＝松井茂記＝鈴木秀美（編）『インターネットと法〔第 4 版〕』（有斐閣、2010 年）83 頁。通信データを独立に保護すべきである論拠を提供するプライバシー権の理解として、棟居快行教授の「自己イメージのコントロール権」説がある。棟居快行『人権論の新構成』（信山社、1992 年）173 頁以下。さらに参照、棟居快行「通信の秘密」『法学教室』212 号（1998 年）45 頁。

8 最高裁昭和 59 年 12 月 12 日大法廷判決民集 38 巻 12 号 1308 頁。

9 郵政省・前掲注（5）3 章 3 節（2）を参照。なお、佐藤・前掲注（6）322 頁によれば、憲法 21 条 2 項の検閲とは異なり、通信の検閲は、発表前（事前）の禁止に限定されず、発

もある[10]。ただし、通信内容の推知可能性、あるいは通信データの有する独自の意義の観点からは、通信データの調査も禁止されるべきことになろう。他方、②は、電気通信事業法６条で定めている電気通信役務の提供の差別的取扱の禁止につながるように考えられる。以上の理解からすれば、事業法上の検閲の禁止は、①通信の秘密と②差別的取扱の禁止を包摂する上位概念として整理できる。

上位概念としての検閲の禁止は、電気通信事業の規律体系における中核として位置づけられてきた。したがって、インターネットをめぐる法的枠組みにおいても、検閲の禁止と通信の秘密がいわば基礎的な役割を果たしている。そこから、「憲法学が想定していなかった意図せざる『基本設計』」としての「インターネットの自由」という考え方が定着するようになったとの指摘もある。それによれば、「憲法上の通信の秘密は、電気通信事業法におけるそれを通じて、インターネット上の表現行為の匿名性を相当程度保障し、違法有害情報対策について政府による直接的な法執行ではなく電気通信事業者の自主的な取組みによるものとする方向を導くとともに、事業者による通信に係る情報の利活用には正当業務行為該当性か利用者の有効な同意を要求するという形で、インターネット利用者の自由・利益を確保する機能を果たしてきた」[11]という。また、別の指摘によれば、電気通信事業法は、通信の秘密の保護に加え、電気通信役務の提供の差別的取扱の禁止を定めることにより、「電気通信事業者は通信の伝達のみに関わっていれば足りる、そして、通信それ自体について差別的な取り扱いをしてはならないというモデルを構築」しており、このモデルがインターネット媒介者にも適用されてきた[12]。

２．２．日本モデルに対する批判

しかし、こうした日本の「基本設計」あるいは「モデル」は、最近、安全・安心なインターネットの提供というインターネット媒介者の役割を真正面から肯定する立場から、厳しい批判にさらされている。こうしたインターネット媒介者の役割の具体例と法律との関わりについては、すでに詳細な分析がなされている[13]。ごく一例を挙げておくならば、「大量通信等への対処策」、「帯域制御問題」、「DPI 技術を利用した広告」などである。

「大量通信等」とは、一般社団法人日本インターネットプロバイダー協会ほかの「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」によれば、DDos 攻撃（＝ネットワーク上の関係のない複数のコンピュータに攻撃プログラムを仕込んでおき、それらの分散している複数のコンピュータから一斉に特定のサーバーを標的とした攻撃[14]）等のサイバー攻撃、マルウエアの感染拡大、迷惑メールの大量送信および壊れた

表後（事後）の積極的な知得をも含むとされている。

[10] 郵政省・前掲注（5）3 章 3 節（2）を参照。

[11] 宍戸・前掲注（3）519 頁。

[12] 高橋・前掲注（2）6 頁。

[13] 小向太郎『情報法入門〔第 2 版〕』（NTT 出版、2011 年）71 頁以下、林＝田川・前掲注（2）22 頁以下、情報セキュリティ大学院大学「インターネットと通信の秘密」研究会報告書・前掲注（2）7 頁以下、田川・前掲注（2）19 頁以下、高橋・前掲注（2）7 頁以下、宍戸・前掲注（3）506 頁以下など。

[14] 高橋・前掲注（2）8 頁。

パケット等の通信をいう。大量通信は電気通信事業者の設備に過大な負荷を与えるため、何らかのネットワーク制御が要請されるが、そのためにはヘッダ情報等の探知が必要となり、通信の秘密の侵害となる。こうした通信の秘密の侵害は、正当防衛、緊急避難、正当業務行為の解釈により許容されるにすぎない。

「帯域制御」とは、たとえばP2Pファイル交換ソフトの利用はネットワーク帯域の多くを占有し、ネットワークの混雑や他の利用者の利用を阻害してしまうため、利用者間の利用の公正を図る観点から、特定アプリケーションのパケットを探知して、その流通を制御することを意味する。したがって、帯域制御も通信の秘密の侵害となる。一般社団法人日本インターネットプロバイダー協会ほかの「帯域制御の運用基準に関するガイドライン」によれば、利用者の個別かつ明確な同意があれば、この利用者に関する限り、通信の秘密の侵害は存在しない。また、帯域制御が通信事業者の正当業務行為として許容される可能性もあるという。

パケット検査技術の一つであるDPI（Deep Packet Inspection）技術を活用した行動ターゲティング広告は、総務省の「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会　第二次提言」によれば、通信の秘密を侵害する。なぜなら、通信事業者がネットワークを通過するパケットを解析して利用者の興味・嗜好を分析し、これにマッチした広告を両者に配信するものであるからである。そのうえで同提言は、正当業務行為として認められるのは、利用者である国民全体にとっての電気通信役務の円滑な提供の観点から正当・必要な措置であるところ、DPI技術を利用した広告はこれに該当しないという。この種の広告を行うためには、通信当事者の個別かつ明確な同意が必要であるとしている。

日本の「基本設計」あるいは「モデル」に批判的な立場からすると、以上のように、インターネット媒介者は安心・安全なインターネットの健全な利用のために、きわめて多様で重要な役割を果たしているにもかかわらず、そのための行為が違法であるという前提から出発するために、インターネット媒介者に萎縮効果が発生する恐れがある。その原因は、通信の秘密の肥大化にあるのであり、少なくとも通信データについては通信の秘密の保護領域から外すべきであるという。

確かに、以上の批判的な指摘を待つまでもなく、通信の秘密といえども絶対的な保障ではない。その制約は、萎縮効果防止の観点から、正当業務行為や緊急避難の構成によるのではなく、法律によるべきである[15]。しかし、その制約の範囲と密度については、インターネット媒介者の積極的役割に対する社会の要請に照らして判断するのではなく、まずは「インターネットの自由」の意義を反省するなかで検討すべきであろう。日本の「憲法学が想定していなかった意図せざる『基本設計』」としての「インターネットの自由」を法理論により正当化し、そうして上位概念としての通信検閲の禁止を再定位する可能性はないのであろうか。こうした問題意識から、以下では、ドイツの議論を検討することにより、いわば日本モデルの可能性を探究してみたいと思う。ドイツでは、連邦憲法裁判所が「デジタル基本権」という新しい基本権を提示したことにより、インターネットにおける基本権のあり方をめぐる議論が盛んに行われているからである。

15 曽我部・前掲注（3）20頁。

３．ドイツにおける「インターネット基本権」

３．１．通信の秘密

インターネット上のコミュニケーションの自由（機密性）は、第一に「通信の秘密」により保護される。ドイツでは、基本法 10 条が、遠隔通信の秘密の不可侵を保障している。まずは、基本法 10 条の趣旨、保護の対象・射程について見ておく。

３．１．１．通信の秘密の趣旨と保護の射程

ドイツ連邦憲法裁判所の判例、そして支配的な学説によると、基本法 10 条の趣旨は私的な生活の営みの保障にある。信書・郵便・通信は、他者による媒介に依存し、第三者のアクセスを可能とするために、国家の追跡という特別な危険が生ずる。基本法 10 条は、特別な追跡制限を設けることにより、この危険に対処しているのである。基本法 10 条は「人格の発展のためのメディアを、原則として国家が侵入してはならない保護ゾーンとして評価することにより、人格を保護している。個別事例において、コミュニケーション内容が特別に保護に値するように見えるかどうかは、基本権保護にとって重要ではない。この限りで、基本法 10 条は、形式的な接続点を有しているのであり、そこからその保護領域が展開されうる」[16]。

以上の説明から、基本法 10 条の保護の対象・射程について、以下の四つの結論が導き出される。第一に、基本法 10 条の名宛人は公権力である。第二に、保護ゾーンという形式的な性格上、基本法 10 条は、通信内容はもちろん、通信データをも保護する。通信データは、コミュニケーション行為態度に対する相当な逆推論を可能にすることからも、そのように根拠づけられる[17]。第三に、基本法 10 条は、メディアに固有の危険に対処するものであって、コミュニケーションの相手方に対する信頼を保護しない。第四に、第三者による容易なアクセス可能性に対処する観点から、通信内容・データがコミュニケーションプロセスの終了後、コミュニケーション参加者の支配領域の中で保存されている場合には、基本法 10 条の保護の対象外となる。

裁判所によると、基本権は発展に開かれているため、基本法 10 条も、電気通信の機密性を、媒介のための技術に関係なく保護している[18]。したがってインターネット上のコミュニケーションも基本法 10 条の保護の対象となる。では、インターネット上のコミュニケーションにおいて以上のような通信の秘密の保護の射程は、いかなる様相を呈するのであろうか。

３．１．２．インターネットと通信の秘密

（１）ブロッキング、変動 IP アドレスを例にして

まず、以上の第一と第二の結論に関連して、学説上、「国家機関自ら、コミュニケーショ

---

16 *Matthias Bäcker,* Die Vertraulichkeit der Internetkommunikation, in: *H.Rensen/S.Brink* (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts, 2009, S. 103.

17 BVerfGE 67, 157, 172. ただし、本稿注（31）をも参照。

18 BVerfGE 115, 166, 182. なお参照、西土彰一郎「接続データの保護―ドイツ憲法判例研究（161）」『自治研究』90 巻 9 号（2014 年）119 頁以下。

ン関連性を有するデータをそもそも収集していない、また他のデータとの共同作用において初めて、テレコミュニケーションプロセスの内容・状況の追跡もしくは逆推論を可能にするようなデータのみを収集する場合、基本法 10 条の保護領域の限界に到達する」[19]と指摘されている。この点で問題となるのが、ブロッキングと変動 IP アドレスの本人確認である。

ある学説によると、利用者による特定のコンテンツへのアクセスを阻止するように通信事業者を義務づけるブロッキングは、通信の秘密を侵害しない。通信事業者は、ブロッキングを実施するにあたり、その顧客のトラフィックデータやコンテンツデータを処理しなければならないものの、これらのデータは、官庁に引き渡されないからである[20]。

同じことが、変動 IP アドレスの本人確認についても当てはまるという。この本人確認は、変動 IP アドレスに対応する接続データの閲覧を要する。ただし、国家の任務を遂行するうえで必要となる変動 IP アドレスの本人確認のため、立法者が通信事業者に対して以上のデータにアクセスし、その解析の結果得られた変動 IP アドレス保有者情報を関係機関に提供するように義務づけたとしても、そこに通信の秘密の侵害は存在しない。なぜなら、国家の関心はこの接続データにないため、通常、かかるデータは関係機関に通知されないからである[21]。

もっとも判例は次のように指摘して、以上のような義務づけは通信の秘密を侵害するとした。「通信事業者は、変動 IP アドレスの本人確認のためには、中間段階において、顧客の相応の接続データを閲覧しなければならない、すなわち、具体的な通信プロセスにアクセスしなければならない。（中略）役務提供者により個別に保存されている以上のような電気通信の接続は、通信の秘密に含まれる。立法者が通信事業者に対して、かかるデータにアクセスし、国家の任務遂行のために活用するよう義務づけている限り、基本法 10 条 1 項に対する侵害が存在する」[22]。この趣旨からすると、上記のブロッキング措置の義務づけも基本法 10 条 1 項の侵害と評価されることになろう[23]。

（2）メディアに固有の危険の対処

次に、第三の結論に関係して、連邦憲法裁判所は、少なくとも一人のコミュニケーション参加者が承認しているのであれば、国家が技術上予定された方法により通信内容あるいは通信データを認識したとしても、通信の秘密の侵害はないという[24]。基本法 10 条はコミュニケーションの相手方に対する人的信頼を保護していない、つまり、人的信頼の不確実性は口頭の手段による特定人相互のコミュニケーションでも生ずる危険であって、支配不能なコミュニケーション手段に固有のものではないからである。具体的には以下のように

---

19 *M. Bäcker* (Fn. 16), S.110.
20 *M. Bäcker* (Fn. 16), S.110.
21 *M. Bäcker* (Fn. 16), S.111ff.
22 BVerfGE 130, 151, 181. Vgl. nur *Hermes*, in: *Dreier*, Grundgesetz, 3.Aufl.［2013］,Art.10 Rn.42.
23 Vgl. BVerfGE 125, 260, 310. Vgl. auch *Alexandra Heliosch*, Verfassungsrechtliche Anforderungen an Sperrmaßnahmen von Kinderpornographischen Inhalten im Internet, 2012, S.218.
24 BVerfGE 120, 274, 340f.

なる[25]。

第一に、通信の秘密の侵害がない場合として、国家が、通信内容あるいは通信データを認識するために技術上予定された方法にしたがうことにより、コミュニケーション参加者はこの認識を承認しているものと見なすことができるときが挙げられる。たとえば、国家機関が、アクセス遮断がなされていない World Wide Web 上のウェブサイトを呼び出す、誰にでも開かれているメーリングリストに登録するような場合である。

また、あるコミュニケーション参加者が国家機関に対して意図的に、特定の人々にのみ開放されているコミュニケーションプロセスへのアクセスを開く場合、さらに、国家機関が届出に際してその属性と動機について虚偽の申告をすることにより、閉じられたコミュニケーションサービスへのアクセスを詐欺により手に入れる場合にも、通信の秘密の侵害はない。後者に関して、基本法 10 条は進行中の遠隔コミュニケーションを国家から保護しているのであって、国家との意図しない遠隔コミュニケーションからの保護を与えていないからである。

第二に、通信の秘密の侵害がある場合として、国家が技術上予定された方法により、しかしコミュニケーション参加者の意思に反して通信内容あるいは通信データを認識するときと、技術上予定されていない方法でこの種のデータを認識するときとがある。前者の例として、安全措置が施されたコミュニケーション内容にアクセスするために、キーロギングにより突き止められたパスワードを投入すること、また、捜査職員が家宅捜索の枠内で、スイッチが入れられた関係者の PC を、その E メールを呼び出すために用いるように、国家機関が高権的強制によりアクセスを可能にした場合である。後者の例として、端末電話傍受などが挙げられる。

（3）時間的限界

最後に、第四の時間的限界について、判例は次の二つの理由を挙げている。第一に、基本法 10 条は、コミュニケーションメディアの技術的特性に固有の危険に対処することを規範目的としている。この危険とは、前述の通り、第三者による容易なアクセス可能性であり、情報伝送が終了したときにはこの危険性は存在しない。第二に、通信内容と通信データがいったんコミュニケーション参加者の支配領域のなかで保存されると、それらはもはや利用者が自ら作成したデータから区別されえなくなる[26]。

確かに、この見解に対しては、学説上、関係者の自己保護の可能性を過剰評価しているとの批判がある[27]。実際に、その後の判例では、利用者が自分で秘密裡のデータ追跡からの保護措置を講ずることができる「範囲内では」、基本法 10 条の保護が考慮されないと述べる裁判例もある[28]。しかしこうした批判も、結論としては、前述の第二の理由に着目して、コミュニケーション固有のリスクではなく一般的な情報技術上のリスクが存在していることを根拠に、通信の秘密の時間的制限それ自体には賛同している[29]。

---

[25] 以下につき、*M. Bäcker*（Fn. 16), S.106ff.
[26] BVerfGE 115, 166, 181ff.
[27] *M. Bäcker*（Fn. 16), S. 115f.
[28] BVerfGE 120, 274, 307f.
[29] *M. Bäcker*（Fn. 16), S.116.

ただし、ウェブメールのように、通信内容と通信データが「ネットワークのなかの」コミュニケーション媒介者の許で保存されているのであれば、通信の当事者は引き続きコミュニケーションに固有のアクセス・リスクにさらされている。この場合には、基本法 10 条の保護が及ぶ。インターネット・コミュニケーションに関しては、「支配」の意味をめぐる詳細な検討が必要となることを示している[30]。

３．２．情報自己決定権

もっとも、基本法 10 条による保障を受けないとしても、インターネット・コミュニケーションの機密性は、基本法 1 条 1 項と関係する同 2 条 1 項のいわゆる情報自己決定権により保障されうる[31]。この情報自己決定権は、1983 年の連邦憲法裁判所の国勢調査判決により初めて言及されたものであり、特定のコミュニケーション手段にも、特定のコミュニケーション内容にも限定されていない。

３．２．１．情報自己決定権の定義と規範目的

国勢調査判決は、情報自己決定権を、個人に対して自分の個人データの引渡と利用について原則として自分で決める権限の保障として定義した[32]。その規範目的は、個人データが無制約に収集、保存、利用、提供されることから個人を保護すること、すなわち、国家あるいは私人のデータ・情報権力を規律することにある。この点を、国勢調査判決を参考にした最近の学説の整理にしたがい分節化すると、次のようになる。

第一に、個人は、他者が自分についてどのような認識を有しているのか、ある程度評価できる場合にのみ、成功の見込みをもって他者に対して自己を表出（描出）できるという（外的）自己表出の権利の保障のため[33]、第二に、私的生活の営みの基本権保護を、その危険化の段階にまで前倒しすることにより、実効的に保護するため、第三に、生き生きとした個人の行為を間接的に保護するため（萎縮効果論）、である[34]。したがって、情報自己決

---

30 BVerfGE 124, 43, 54. *M. Bäcker* (Fn. 16), S.116f. 以上につき、西土・前掲注（18）123 頁以下。

31 このことは、情報自己決定権と通信の秘密は一般法と特別法の関係に立ち、規範目的それ自体は同じであることを意味している。したがって、情報自己決定権の理解によっては、コミュニケーション行為態度に対する相当な逆推論を可能にすることを理由として通信データの保護を導き出す連邦憲法裁判所の判例とは異なり、本稿の脚注（7）を付した本文で指摘したように、通信データを独立に保護すべきことになる。こうした情報自己決定権の理解を示すものとして、本稿の脚注（41）を参照。

なお、情報自己決定権と通信の秘密の保障の程度の違いにつき、後者の侵害に対する引用命令（基本法 19 条 1 項 2 文）が挙げられる。*Hermes* (Fn. 22), 3. Aufl., Art.10 Rn.16, 46, 68.

32 BVerfGE 65, 1,43（平松毅「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、2003 年）60 頁以下）.

33 近年では、内的自己描出権の具体化として情報自己決定権を捉え直す見解も提示されている。本稿脚注（41）を参照。最近の研究として、参照、高橋和広「ドイツ連邦憲法裁判所による情報自己決定権論の展開」『六甲台論集』59 巻 2 号（2013 年）57 頁以下。

34 *Matthias Bäcker,* Das IT-Grundrecht: Funktion, Schutzgehalt, Auswirkungen auf staatliche Ermittlungen, in: *R. Uerpmann-Wittzack* (Hrsg.), Das neue

定権は、各基本権保障を実効化するための道具的権利として位置づけられうる[35]。

３．２．２．法的構成と保護の対象

以上の規範目的を踏まえて、情報自己決定権は、前述の定義のように防御権（処分権）的に構成される。それと並び、個人データ・情報処理をプロセスとして構造化し、透明性を維持し、関係者に対してこのプロセスに影響を及ぼす可能性を与えるよう国家に要請する客観法としても構成されうる。

（防御権としての）情報自己決定権の保護の対象たる個人関連データに関しては、通信の文脈でいうと、通信内容のみならず通信データをも含む。蓄積される通信データの量と意味内容は、コミュニケーション当事者の明確な像を成立せしめるからである[36]。

３．２．３．処分権的構成に対する批判

ただし、情報自己決定権の客観法的構成については学説上、大方の賛成が得られてはいるものの、処分権としての構成に対しては最近厳しい批判にさらされている。

かつて、連邦憲法裁判所判事であったホフマン＝リーム教授のもとで助手を務めたベッカー教授は、情報自己決定権を処分権として捉えるならば、個人関連データ・情報のあらゆる収集、保存、処理、利用あるいは伝達が、法律により規律されなければならない基本権侵害となってしまうと批判している。個人関連情報は社会的現象であることが、情報自己決定権の保護領域の段階ですでに考慮されなければならないと指摘する[37]。

現在、ドイツ連邦憲法裁判所の判事を務めているブリッツ教授は、個人の処分権に直接依拠する情報自己決定権の構想は、不可能なこと（情報処分権）を保障しているのか、あるいは、情報とデータの関係を意識しない限り、規範的に不必要なこと（データ処分権）を保障することになると述べている。彼女は、まず、データを「記憶媒体で記録されている記号、そして情報の基礎として機能しうる記号」として、情報を「特定の社会的文脈において、観察、通知、あるいはデータから形成され、そうして利用されるような意味要素」として定義する。そして、自由の毀損は、ある者がその人格および行為に対する他者の特定の期待を予期することにより、その際には特に、その人格について他者が情報に条件づけられて抱く特定の考えに依拠している不利益的決定を予期することにより生ずると指摘する。そのうえで、一方で情報は、個人関連データについての他者による意味構築という、予期された、あるいは現実に生じた社会現象であるため、個人関連データに依拠している情報についての処分権は存在しえないという。他方で、個人関連「データ」に対する処分権については、情報との関係を考慮に入れるのであれば、意義が認められると述べる。データ処分権の承認は、情報の成立と利用を規律するための法的道具であり、こうして間接

Computergrundrecht, 2009, S. 3f.; *Gabriele Britz*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: *W. Hoffmann-Riem*(Hrsg.), Offene Rechtswissenschaft, 2010, S.569ff.

[35] *G.Britz*（Fn. 34), S.573f.

[36] *M. Bäcker*（Fn.34), S.4ff.

[37] *M. Bäcker*（Fn.34), S.6f.

的に実体的な自己決定を促進するという[38]。ここでの情報自己決定権とは、各社会的文脈における「データ→情報」転換メカニズムの保護を目的とするものであり、社会的文脈ごとに細分化した各基本権保障を実効化する道具的権利であるということになろう。

３．２．４．防御権の再構成

以上のように情報の成立と利用を規律するための法的道具として情報自己決定権を読みなおすブリッツ教授は、さらに分析を進めて、「データあるいは情報が特定の不利益をはらんでいる文脈において利用されることから生ずる人格の危険に対処」するのが情報自己決定権の防御権的側面であると再構成する。すなわち、連邦憲法裁判所は、情報自己決定権を、構想上、危険にさらされている他の自由の保護に向けており、情報自己決定それ自体のために保護しているわけではないと指摘したうえで、防御権的保護は、特定の情報措置に対してのみ与えられており、それに対応して、保護領域は精緻化されうると主張するのである[39]。では、ここでいう特定の情報措置とはいかなるものであろうか。

ブリッツ教授によれば、a）それに基づいて関係者にとって不正な不利益を及ぼす具体的な決定がなされる情報措置、b）萎縮効果を及ぼす情報措置、c）特別な危険状況をもたらす情報措置を挙げている。c）については、さらに、①一方で現実の利用文脈の抽象的な予見可能性と、他方でそれと結び付けられた不利益の程度の組み合わせから、重大な危険状況が生じうるようなデータと情報の収集、②内容上、最初から不利益利用の特別に高いリスクを内包しているデータと情報の収集、③秘密裡のデータ・情報収集、④ある個人についての広範囲に及ぶ情報を獲得するために、統計上の想定を利用し、それと具体的な個人関連データを結合させる場合、⑤巨大なデータ・情報群の設定、⑥機密性に対する正当な期待が毀損されるとき、の六類型に整理している[40]。

３．２．５．インターネット・コミュニケーションと情報自己決定権

以上のような再構成については、「人格の危険」等、一般論としてさらなる検討を要するように思われる[41]。しかし、ここではインターネット・コミュニケーションの機密性の保護

---

[38] *G. Britz* (Fn. 34), S.566ff.
[39] *G. Britz* (Fn. 34), S.568.
[40] *G. Britz* (Fn. 34), S.578ff.
[41] この点について、ごく簡単に指摘しておきたい。
かつてルーマンは『制度としての基本権』（今井弘道＝大野達司訳、木鐸社、1989年）のなかで、基本権保障の意義を社会の機能的分出化に対応させて位置づけなおすよう主張した。基本権は各社会的文脈で規定される「役割」を保障するものであり、この保障は各社会的文脈のカップリングの禁止を要請することになる。この要請は、本稿の主題に即して捉えなおすならば、各社会的文脈に固有の「データ→情報」転換メカニズムを保障するものといえよう。
以上を前提にして、「人格の危険」の問題を意識しつつ、情報自己決定権の規範目的の一つであった自己描出権を見てみると、それは、ブリッツ教授が指摘するように、外的自己描出権と内的自己描出権に区別することができる。前者は、個人が各社会的文脈で引き受けている「役割」と矛盾する情報が生じないように、自己関連データを任意に秘密、公開・開示することにより、自らをあらゆる不利益から保護する自由である。ただし、ブリッツ

の観点から若干指摘しておくにとどめる。

前述のように、情報自己決定権は、通信の秘密の保護から漏れるインターネット・コミュニケーションの機密性の保障の受け皿として機能する。しかし、情報自己決定権の保護領域の精緻化に向けたブリッツ教授の努力が示しているように、防御権としてのそれは、特定の個別の情報措置に点描的に対処できるにすぎない。個人関連情報が社会的現象であること、「人格の危険」がもはや十分に実効的に回避されえない時点においてようやく、データ・情報処理プロセスの結果に直面することがないようにすること、この二点をすでに

教授によると、そこでいう不利益は、法的に重要なもののみが問題となる。そして、情報により条件づけられて脅威となっている不利益の重大性にとって重要であるのは、法的に保護されている外的発展の自由の諸側面が毀損されているかどうかであるという。したがって、外的自己描出権は、社会的文脈の分出に対応している各基本権保障に吸収されることになる。

これに対して、内的自己描出権は、「役割」保障に吸収されない側面を有している。この権利について、ブリッツ教授は次のように指摘している。少々長いが、引用してみる。「一般的人格権の中心的機能は、人格発展のプロセスを、相互行為による人格構築という条件下で、自己のものとして、それゆえに『自由なもの』として確保し、そうして人格の自律的な発展のための根本条件を保障することにある。情報自己決定権は、（中略）個人が人格を独自に十分に構築するために必要である、自己の人格に対する本人、そして他者の期待から離れて内的に反省する可能性の条件を創り出すことに寄与しうる。このような内的な開放性は、個人が他者による実際の、そして想定上のアイデンティティ期待に拘束されていると見て、距離を置いて自己を確証し自己を新たに方向づけるプロセスに立ち入らないことにより、とりわけ危険にさらされる。個人が、特定の、場合によってはとりわけ強力な情報を抑えることに成功するならば、このことは、他者による他律的な像を防ぎ、他者による認識を個人の自己表現へと向けさせることができることに寄与する。自己の人格についての他者による像に対する作用を認識して初めて、自律を確保する自己確証プロセスが遣り甲斐のあるように思われる。」

この点について私見を交えて敷衍させると、内的自己描出権とは多様な社会的文脈での行為を自分なりに整合化する内的反省としての自己描出を保障するものであるといえよう。この反省を受けて、既存の「役割」と真正面から衝突することを避けつつも、それとはやや乖離する行為を遂行することにより、個人は社会構造に対する異議申し立てを行うことができ、それこそが「自由」の意味である。しかし、こうした個人による各社会的文脈の自己表出のデータを集めると、「内的反省」プロセスが透視されてしまう。これに対抗するのが、情報自己決定権なのである。それは、スティグマ化からの自由としての平等権と同じ構造を有している。情報自己決定権と内的自己表出権を区別するならば、前者は後者のための道具的権利ということになろう。Vgl. *Gabriele Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, S. 52ff.　もっとも以上のような見方は、本稿の脚注（7）で指摘したように、すでに日本において棟居教授により「自己イメージのコントロール権」として主張されている。

なお、以上の整理にしたがうならば、本文で触れられている個別の情報措置に関して、a）は外的自己描出権としての情報自己決定権が、b）と c）は内的自己描出権としての情報自己決定権がそれぞれ対処すべきことになる。また b）は内的自己描出権としての情報自己決定権の主観権的側面が、c）は同権利の客観法的側面が対応することになろう。

保護領域のレベルで考慮しなければならない以上[42]、対処すべき個別の情報措置を特定化して、情報自己決定権の防御権的内容を明確化することは理解できる。しかし、以上二点の問題意識を突き詰めるならば、国家・私人のデータ・情報処理の構造化、透明性の確保、この枠組みでの関係者の利益の保護というプロセス化を求めるものとして、つまり客観法として情報自己決定権を第一に把握すべきことになろう[43]。

ただし、この客観法的構成に関しても、インターネット・コミュニケーションの文脈では修正を要するとの指摘もある。情報自己決定権を「データ→情報」転換メカニズムの保護を目的とするのであれば、インターネットにおけるこの転換メカニズムの特性を把握しておくべきである。コンピュータ・ネットワークとしてのインターネットでは、二元的にコード化されたデータが機械的に処理されて情報へと転換されるため、個人（人間）に関連づけられたデータ保護というよりもソフトウェアなど技術に関連づけられたデータ保護として構想される必要がある[44]。そうであるならば、情報自己決定権の保護目的を出発点としつつも、その個人関連性にこだわるべきではなく、「インターネットというネットワークの技術的機能条件の保障」として再構成しなければならないという[45]。

こうした再構成にとり重要な示唆を与えているのが、2008 年の連邦憲法裁判所の判決（BVerfGE 120, 274）により示された新しい基本権としての「情報技術システムの機密性および完全性の保障に対する権利」、すなわちデジタル基本権である。

３．３．デジタル基本権[46]

３．３．１．ドイツ連邦憲法裁判所 2008 年 2 月 27 日判決

この事件では、過激派およびテロリスト集団によるインターネット・コミュニケーションの内容を突き止め、犯罪の計画・実行を発見・阻止する目的で、「オンライン捜索」（情報技術システムの安全性の間隙を利用した、または偵察プログラムのインストールにより行う技術的侵入で、情報技術システムの利用の監視、記憶メディアの捜索、さらにはターゲットであるシステムの遠隔操作を可能とする措置）などを州憲法保護庁に授権していたノルトライン・ヴェストファーレン州憲法保護法の規定の合憲性が問題になった。裁判所は、かかる規定は「デジタル基本権」を毀損し、無効であるとの判断を下した。裁判所があえてデジタル基本権を打ち出したのは、基本法上の通信の秘密、情報自己決定権だけでは、インターネット・コミュニケーションに関し、十分な保護が期待できないからである。

それによると、情報技術システムの利用は、多くの市民の人格の発展にとり不可欠とな

---

[42] *M. Bäcker* (Fn.34), S.6f.
[43] *M. Bäcker* (Fn.34), S.4f.
[44] *Thomas Vesting*, Das Internet und die Notwendigkeit der Transformation des Datenschutzes, in：*K.-H.-Ladeur* (Hrsg.), Innovationsoffene Regulierung des Internet, 2003, S. 179.
[45] *Thomas Vesting*, Die innere Seite des Gesetzes, in：*I. Augsberg* (Hrsg.), Ungewissheit als Chance, 2009, S. 55f.
[46]以下の叙述は、西土彰一郎「デジタル基本権の位相」〔鈴木秀美編『憲法の規範力　第４巻』（信山社、2014 年公刊予定）所収〕の第 2 章と重なるところが多い。ご寛恕を乞う。

っている。しかし、いったん「トロイの木馬」のようなスパイプログラムが情報技術システムにおいて記憶されている多数のデータに侵入すると、市民の行為やコミュニケーションの輪郭が露見してしまう。情報技術システムがはらんでいるこうした危険性に対処するうえで、通信内容・データの「記憶」を保護の対象としてはいない通信の秘密は無力である。また、情報自己決定権も、個別のデータ収集から当事者を保護するにとどまり、国家による情報技術システム全体への侵入から保護しない。オンライン捜索は個別のデータ収集を超えている。それは、システムの利用を監視し、記憶メディアを捜索し、またはターゲットとなるシステムを遠隔操作することを可能にするからである[47]。

デジタル基本権は、以上のような保護の欠缺を埋める目的で生み出された。それは、「情報技術システムの機密性に対する権利」と「情報技術システムの完全性の保障に対する権利」の二つに分けることができる。

前者を保護する必要性について、裁判所は次のように指摘する。複雑な情報技術システムは、個人関連データの創出、処理および蓄積と深く関係している多様な利用可能性を提供する。この個人関連データは膨大な量であり、しかもセンシティブな性質を有するものを含んでいる。このような広範囲にわたるデータ蓄積への国家のアクセスは、収集データを鳥瞰することにより、行為およびコミュニケーションの特徴にまでいたる関係者の人格を帰納的に推論することを可能にしてしまう。関係者の人格を嗅ぎつけることから保護するためには、情報技術システムへの国家の不当なアクセスから保護されなければならず、この点に「情報技術システムの機密性に対する権利」の意味がある[48]。

電算機上の損害とデータ蓄積の操作からの保護を意図する後者は、本判決において「インターネットに固有の性格、オンライン捜索の技術的条件・作用が取り上げられ、反省された」ため、導出された[49]。裁判所によれば、第一に、情報技術システムは利用者により蓄積された情報を有しているのみならず、データ処理との関連で自らデータを創り出す。このデータは、利用者の利用行為についての情報を提供し、この情報の存在について彼は認識できない。それゆえに利用者は、不正な侵入から情報技術システムを守ることができない[50]。第二に、情報技術システムの高い複雑性の程度により、少なくとも平均的な利用者は自己のデータへの不正侵入を確認または阻止することができない。データの暗号化にしても、第三者が情報技術システム全体への侵入に成功したら、それは無力化する[51]。

きわめて多様な個人データを含んでいる、そしてこのデータへの侵入により捜査人が当事者の人格および生活形態の像を完全に描くことができる、このようなシステムへの侵害が意図されている場合に、「情報技術システムの機密性および完全性の保障に対する権利」が用いられる[52]。このデジタル基本権の保護領域は、私的に利用される情報技術システムお

---

47 BVerfGE 120, 274, 307ff.
48 BVerfGE 120, 274, 322ff.
49 *Martin Eifert*, Informationelle Selbstbestimmung im Internet, NVwZ 2008, 522.
50 BVerfGE 120, 274, 305.
51 BVerfGE 120, 274, 306.
52 BVerfGE 120, 274, 314.; *Laura Köpp/Seraphine Kowalzik/Britta Recktenwald*, BVerfG v. 27.2.2008, RUB RR 2/2009, S. 39. https://zrsweb.zrs.rub.de/rubrr/dok/RUBRR-O003-2009W-Koepp_Kowalzik_Recktenwald.pdf

よび営利上利用されるそれを含む。この情報技術システムという概念は広く理解され、携帯電話や電子カレンダーも含む。機器が多数の個人関連データを記憶しうるかどうかのみが重要である。しかし、機密性・完全性に対する当事者の期待が基本権上保護に値するのは、彼が情報技術システムを自己の利用に供し、場合によっては彼自身や他の利用資格者のみが情報技術システムを処理していると前提にできるときのみである[53]。

３．３．２．学説の批判

（１）情報自己決定権との関係について

以上で見てきたように、連邦憲法裁判所は、通信の秘密と情報自己決定権では、インターネットに固有の危険に十分に対処できないことを根拠に、基本法１条１項と関係する同２条１項の一般的人格権からデジタル基本権を導き出すとの理路を採用している。確かに、通信の秘密についてはそのようにいえるかもしれない[54]。しかし、果たして情報自己決定権によって対処できないのか疑問を挟む余地があり、この観点からの批判が存在する。

ブリッツ教授は、次のように批判している。連邦憲法裁判所は、詳細な根拠づけを経ずに、情報自己決定権は個別のデータ収集からのみ保護するものと想定する一方で、デジタル基本権は、基本権享有主体の情報技術システムに対する国家の侵入からも保護するという。しかし、情報自己決定権を個別のデータ収集に限定する理由は存在しない。情報自己決定権は比較的「無害な」基本権侵害にのみ対抗できて、重大な基本権侵害からの保護を与えないという構造は、不可解だからである。確かに、情報自己決定権の保護領域を「下限」に即して確定することには、困難が伴う。しかし、大量のセンシティブな個人データが収集される場合には、情報自己決定権の侵害として容易に評価されうる。自由の強い侵害に対しては、それに対応して強い正当化要求により対処すればよいのであり、ドグマーティク上、このことは情報自己決定権の枠組みで比例原則により実現されうる。裁判所は、情報自己決定権の保護領域を軽率に切り詰めて、あえて保護の隙間をつくったにすぎない[55]。

---

[53] BVerfGE 120, 274, 315.; *L. Köpp/S. Kowalzik/B. Recktenwald* (FN 52), S.39.

[54] *Gabriele Britz*, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, 413. 他方で、*Oliver Lepsius*, Das Computer-Grundrecht: Herleitung-Funktion-Überzeugungskraft, in: *F. Roggan* (Hrsg.), Online-Durchsuchungen, 2008, S.23ff.は、本判決における基本法10条1項の保護領域の画定に対しても批判的な分析を試みている。

[55] *G. Britz* (FN 54), 413. Vgl. *M. Eifert* (FN 49), 521f.; *O.Lepsius* (FN 54),S.28ff.; レプジウス教授によれば、本判決により示唆された情報自己決定権の保護の欠缺は、情報技術システムにより自ら生み出されるデータ群という脱個人化の論拠がなければ、理解されえないという。そのうえで、レプジウス教授自身は、ブリッツ教授と同様、情報自己決定権は個別のデータ収集からのみ保護するとの想定には理論的根拠がないこと、現に「現代のデータ処理の条件下」での個人の保護が意図されているという国勢調査判決の基本定式と結び付くことにより、連邦憲法裁判所第一法廷は本判決の１年前に情報自己決定権の広い解釈を前提にして、情報自己決定権は個別のデータ収集のみならず、大量のデータにより脅かされる個人像の把握からも保護するものと示唆していること（Vgl.BVerfGE 118, 168, 183f.）、そして、第二法廷の判決のなかにも、送信プロセスの終了後にコミュニケーション当事者の支配領域に記憶された接続データは情報自己決定権の保護領域に含まれると判断した判例もあること（Vgl. BVerGE 115, 166, 181ff.）などを指

アイフェルト教授もブリッツ教授と同様の指摘をしつつ、さらに「情報技術システムの完全性の保障に対する権利」について以下のように批判する。「機密性保護についての基本権は、裁判所の説示に沿うならば、すでに導出された、この場面でまさに十分に保護を及ぼす情報自己決定権と同様に、説得的に一般的人格権から導出されうる一方、このことは、完全性の保護については困難である。後者では、人格との関連性は、間接的で道具的であるのにすぎない。裁判所は、それゆえに説得的にも、個人関連データへのアクセスを高度に可能にするようなシステムに、保護を限定している。しかし、まさにこの背景に立てば、固有の保護の必要性は疑問となる。システムの完全性が危険にさらされるのは、システムの毀損により、そのなかで蓄積されているデータへのアクセスが可能となるからにほかならない。すなわち、独立して対処される必要はない。むしろ、データ保護にあたり、常に同時に十分に対処されるような付随的危険である」[56]。

（2）客観法としてのデジタル基本権について

アイフェルト教授の指摘は、「情報技術システムの完全性の保障」は、技術に向けられた非人格的基本権として展開する恐れがあるとの批判につながる[57]。この点を深く分析しつつ批判しているのが、レプジウス教授である。

彼によれば、連邦憲法裁判所は、デジタル基本権導出の根拠の力点を個人化可能な行為または個人に帰属されうるデータにではなく、むしろ技術的システムの用意それ自体に置いている。つまり、「保護に値するのは、個々人のデータの流れを事実上作り出すことではなく、ネット化したコミュニケーションの機会であり、客観的なシステム保護が意図されている。かくして基本権により保護されている領域は、個人の行為ではなく、一定の発展可能性の技術的利用可能性と結び付いている」。「情報技術システムの完全性の保障に対する権利」は行為ではなくシステムを、作為ではなく期待を保護している[58]。

（3）反論

以上のような批判に対して、デジタル基本権を支持する立場からの応答も存在している。

連邦憲法裁判所判事として本判決に主導的な役割を果たしたとされるホフマン＝リーム教授は、デジタル基本権と情報自己決定権との関係について、デジタル基本権の保護領域を厳密に画定する思考の背後には、基本権ドグマーティクの明晰化という問題意識があることを強調している[59]。また、ベッカー教授は次のように指摘している。デジタル基本権は、

摘している。

[56] *M. Eifert* (FN 49), 522.

[57] *M. Eifert* (FN 49), 522.

[58] *O.Lepsius* (FN 54), S.33.

[59] *Wolfgang Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter Informationstechnischer Systeme, JZ 2008, 1019. ホフマン＝リーム教授は、情報自己決定権とデジタル基本権の各保護領域を次のように線引きしている。情報技術システムの侵入を伴わないデータ収集（とさらなるデータ処理）、それに対応する権限創出に対しては、引き続き情報自己決定権が問題となる一方、データ収集の実施のために、複雑な情報技術システムが侵入、覗き見、場合によっては操作される場合には、デジタル基本権の保護次元が妥当する。情報技術システムの機密と完全性の基本権保

特定の生活領域を私的生活圏というゾーンとして包括的に保護するものであり、基本法10条と同じ構造を有している。人格の発展にとっての必要性（その裏面としての危険）が特殊な私的生活圏により記述されうる限り、人格の保護に対する基本権のさらなる彫琢をこの私的生活圏という接続点に即して展開することが好ましい。この彫琢は、保護領域のレベルにおいて、特別に保護の必要性のあるコミュニケーションの一断面を記述し、非特定的な情報自己決定権よりも比例原則を精緻に嚮導できる[60]。

以上の反論は、「情報技術システムの機密性および完全性の保障に対する権利」は情報自己決定権に収斂しうるし、そうさせても何ら差し支えはないと指摘するブリッツ教授およびアイフェルト教授と、情報自己決定権の実効化の必要性をめぐり評価を異にしているにすぎないともいえよう[61]。

他方で、連邦憲法裁判所はデジタル基本権を客観法として把握しているとの批判に対して、ホフマン＝リーム教授は次のように反論する。情報技術システムは即自的にではなく、むしろその完全性が個人との関連性を有している限りにおいてのみ、基本権により保護される。したがって、デジタル基本権は技術に向けられた非人格的基本権として構成されてはいない。この点を、アイフェルト教授とレプジウス教授は看過しているという[62]。

（4）二つのデジタル基本権

このように、ホフマン＝リーム教授は、連邦憲法裁判所のいう「情報技術システムの完全性の保障に対する権利」をあくまで主観的権利として主張している。

確かに、前述の通り、デジタル基本権の規範目的は情報自己決定権と同じであると想定されている。また、本判決のいうデジタル基本権が主観的側面を有していることも否定できない。しかし、デジタル基本権の保護領域と人格の発展の関連性は、レプジウス教授によれば、主観的権利としての地位の確立のために機能しているのではなく、客観的なシステム保護を主観的メルクマールにより画定するものにすぎない。主観的利益と期待（権利ではない！）は、客観的に要請される保護を輪郭づけるにすぎないのである[63]。連邦憲法裁判所のいう「情報技術システムの完全性の保障に対する権利」は、情報自己決定権の行使の条件である情報技術システムの機能性に対する「信頼」を取り出して、それ自体を保護

護は、侵入（場合によっては操作）それ自体に関係するのみならず、侵入の結果（によってのみ）到達されるデータおよび情報の収集・使用にまで拡大される。それに対応して高められた人格保護のハードルは、侵入によりアクセス可能となった人格に関連するデータの取扱にまで拡大する。

60 *M. Bäcker* (Fn. 16) S.123f.

61 ただし、情報自己決定権の実効的保障のために「保障領域」（Gewährleistungsbereich）思考を採用するホフマン＝リーム教授の見解は、彼自身が承認するように、客観法的思考一般へと展開する潜在力を有している。

62 *W. Hoffmann-Riem* (FN 60), 1012.

63 *O.Lepsius* (FN 54), S.35. さらにレプジウスは、裁判所がデジタル基本権を基本法1条1項と関係する同2条1項により根拠づけて、一般的人格権として論証していることに関しても、本来主観的防御権である一般的人格権を客観法的類型にまで拡大していると批判する。*O.Lepsius* , ebd., S.36.

の対象としている。ここでいう「信頼」は、「社会的期待」を意味しており[64]、それを保護するということは、「個人の自由の展開に影響を及ぼす主観的に望ましい状態の保障」である[65]。「情報技術システムの完全性の保障に対する権利」は、レプジウス教授が指摘していたように、「個人」の「行為」ではなく、社会的期待を根拠にして情報技術システムの利用可能性という「客観的」な所与の「事実状態」を保障する[66]。この点で、「情報技術システムの完全性の保障に対する権利」は主観的側面を有してはいるものの、やはり基本権の客観法的次元を前提にしていると判断すべきであろう。そして、このことはむしろ積極的に評価されうる。なぜなら、それにより、前述したように「インターネットというネットワークの技術的機能条件の保障」としてデジタル基本権を位置づけることが可能となるからである[67]。そこでいわれている技術的機能条件とは、「発信元から送信先へのデジタル・データパケットの送信プロセスの技術的な成功条件」を意味しており、デジタル基本権は、「特定の技術的機能条件により保障されるデータの流れの非操作性を保障」するものである[68]。

以上の考察からすると、裁判所のいう「情報技術システムの機密性に対する権利」は情報自己決定権の実効化として位置づけられる一方、「情報技術システムの完全性の保障に対する権利」は客観法的性格を有する独自の権利（＝デジタル基本権）として主張できよう。

４．「インターネット基本権」の整理

インターネット・コミュニケーションの文脈で今まで分析してきた通信の秘密、情報自己決定権、デジタル基本権の射程を簡単に整理すると、以下のようになる。

① 通信の秘密は、メディアに固有の危険に対処するものである。そして、進行中のデータ・情報の通信のみを保護の対象とする。メディア技術上予定されない方法で、または当事者全員の承認なく、国家が通信内容・データを認識する場合、通信の秘密の侵害が認められる。

② 情報自己決定権は、一般的人格権としての性格上、メディアに固有の危険に焦点をあてるものではない。国家が、少なくとも一人のコミュニケーション参加者の承認を得て、技術上予定された方法でインターネット・コミュニケーションの内容あるいは状況を認識する場合、通信の秘密の侵害はないものの、情報自己決定権の適用は問題となりうる。

③ デジタル基本権は、情報技術システムに固有の危険に対処する。その保護は、システムにおいて記憶・処理されるデータにまで及ぶ。

なお、2008 年のドイツ連邦憲法裁判所の判決によれば、国家がシステムの利用者の承認なく、しかし技術上予定された方法でデータを収集する場合、デジタル基本権に対する侵害はなく、当該措置は通信の秘密に即して評価されなければならないという。なぜなら、このような場合、データを処理・記憶するシステムの利用者は、自分のシステムを以上の

---

64 *Vagias Karavas*, Grundrechtsschutz im Web 2.0: Ein Beitrag zur Verankerung des Grundrechtsschutzes in einer Epistemologie hybrider Assoziationes zwischen Mensch und Computer, in:*C. Bieber/M.Eifert/T.Groß/J.Lamla* (Hrsg.), Soziale Netze in der digitalen Welt, 2009, S.317.

65 *O.Lepsius* (FN 54), S.34f.

66 *O.Lepsius* (FN 54), S.34.

67 この点についての法理論上の論拠については、西土・前掲注（46）第 3 章を参照。

68 *Vagias Karavas*, Digitale Grundrechte, 2007, S. 156f.

アクセスに対して意識的に開放したといえるため、こうしたアクセスが生じないことを当てにすることはできないからである[69]。ただしこれに対しては、学説上、次のような批判がある。「このようにして線引きされた基本権は、予測可能な技術的発展を十分に考慮できない。技術上そのために予定された方法における『ネットワークのなかの』データへのアクセスが、デジタル基本権への侵害でないのであれば、著しい保護の隙間が生ずる。この隙間を――その保護目的からすれば適してはいない――基本法 10 条が埋めなければならなくなる」[70]。この立場からすると、技術上予定されない方法、またはシステムの利用者の承認なくデータを認識、捜査する場合に、デジタル基本権の侵害が存在することになる。

５．おわりに――日本モデルへの示唆――

以上、インターネットにおける基本権のあり方をめぐるドイツでの議論を見てきた。通信の秘密の趣旨と保護の射程はさておき、「デジタル基本権」の議論は、インターネットの自由と日本の「基本設計」を評価するうえで、貴重な示唆を与えている。

前述のように、「デジタル基本権」は、①「情報技術システムの機密性に対する権利」と②「情報技術システムの完全性の保障に対する権利」からなる。①は、情報自己決定権の実効化として位置づけられる。そして、学説上、情報自己決定権の規範目的の一つとして内的自己描出権が挙げられており、内的自己描出権は、日本の「自己情報コントロール権」説にいう「周辺情報」を「固有情報」とは独立に、そして対等に保護する[71]。この見解に立脚すると、①は、通信データの効率的な取得・窃用・漏洩を禁止するという法命題をも含むことになる。他方で②は、一定の技術的機能条件により保護されるデータの流れの非操作性を命ずる法命題としての内容を有している。このように整理するならば、①は日本の電気通信事業法上の「通信の秘密」、②は「差別的取扱の禁止」に対応しており、①と②を包摂する上位概念としての「デジタル基本権」とは（日本でも客観法的側面が強調されてきた）「検閲の禁止」を意味しているといえよう。

確かに、電気通信事業法の法的枠組みは、「憲法学が想定していなかった意図せざる『基本設計』」であるといえる。しかし、「デジタル基本権」はこうした日本モデルをむしろ要請しているのであり、安心・安全なインターネットの利用に対するインターネット媒介者の役割を重視して通信データを通信の秘密の保護領域から外すことには、慎重でなければならない。インターネット媒介者の役割は、「ネットワークの自由というメタ・イデオロギー」[72]により規定されていると理解すべきであろう。

すでに 1990 年代に日本でも多賀谷一照教授が、通信の秘密の概念の再構築にあたり考慮すべき基本的原則として、基本的通信セキュリティの確保（＝システムとしての通信の秘密総体、通信が安全かつ確実になされることの利用者への保障）、狭義の通信の秘密の保護（＝人と人との間の私的な 1 対 1 の通話の実質を持つもののみ「通信の秘密」の保護を及ぼすこと）、そして個人情報・プライバシーといったほかの法益による通信内容の保護とい

69 BVerfGE 120, 274, 344.
70 *M. Bäcker* (Fn. 16), S.129.
71 本稿脚注（31）と（41）を参照。
72 *V. Karavas* (Fn. 68), S.179.

う三つを挙げていた[73]。こうした視座は、本稿で検討した「デジタル基本権」、「通信の秘密」、「情報自己決定権」の関係（＝「インターネット基本権」）をめぐる基本的な発想と重なり合う点が多いように思われる。

参考文献

[01] *Alexandra Heliosch*, Verfassungsrechtliche Anforderungen an Sperrmaßnahmen von Kinderpornographischen Inhalten im Internet, 2012, Universitätsverlag Göttingen, Germany

[02] *Gabriele Britz*, Freie Entfaltung durch Selbstdarstellung, 2007, Mohr Siebeck, Germany

[03] *Gabriele Britz*, Vertraulichkeit und Integrität informationstechnischer Systeme, Die Öffentliche Verwaltung (DÖV), pp. 411-415, 2008 Heft 10, Kohlhammer,Germany

[04] *Gabriele Britz*, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: *W. Hoffmann-Riem* (Hrsg.), Offene Rechtswissenschaft, 2010 , Mohr Siebeck, Germany

[05] *Georg Hermes*, Artikel 10 Brief-,Post-und Fernmeldegeheimnis, in: *H. Dreier*, Grundgesetz-Kommentar, 3.Aufl., pp.1150-1204, 2013, Mohr Siebeck Germany

[06] *Laura Köpp/Seraphine Kowalzik/Britta Recktenwald*, BVerfG v. 27.2.2008 - 1 BvR 370/07 u. 1 BvR 595/07 (Online-Durchsuchung), Rechtsprechungs-Report der Ruhr-Universität Bochum (RUB RR), pp.36-46, 2009 Heft 2, Ruhr-Universität Bochum https://zrsweb.zrs.rub.de/rubrr/dok/RUBRR-O003-2009W-Koepp_Kowalzik_Recktenwald.pdf （2014/8/26 確認）

[07] *Martin Eifert*, Informationelle Selbstbestimmung im Internet, Neue Zeitschrift für Verwaltungsrecht (NVwZ), pp.521-523, 2008 Heft 5, Beck, Germany

[08] *Matthias Bäcker,* Die Vertraulichkeit der Internetkommunikation, in: *H.Rensen/S.Brink* (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts, pp. 99-136, 2009, De Gruyter Recht, Germany

[09] *Matthias Bäcker,* Das IT-Grundrecht: Funktion, Schutzgehalt, Auswirkungen auf staatliche Ermittlungen, in: *R. Uerpmann-Wittzack* (Hrsg.), Das neue Computergrundrecht, pp.1-30, 2009, Lit Verlag, Germany

[10] *Oliver Lepsius*, Das Computer-Grundrecht: Herleitung-Funktion-Überzeugungskraft, in: *F. Roggan* (Hrsg.), Online-Durchsuchungen, pp.21-56, 2008, Berliner Wissenschafts-Verlag, Germany

[73] 多賀谷一照『行政とマルチメディアの法理論』（弘文堂、1995 年）197 頁以下。さらに参照、宍戸・前掲注（3）521 頁以下、田川・前掲注（2）32 頁以下。

[11] *Thomas Vesting*, Das Internet und die Notwendigkeit der Transformation des Datenschutzes, in： *K.-H.-Ladeur* (Hrsg.), Innovationsoffene Regulierung des Internet, pp. 155-190, 2003, Nomos, Germany
[12] *Thomas Vesting*, Die innere Seite des Gesetzes, in： *I. Augsberg* (Hrsg.), Ungewissheit als Chance, pp.39-59, 2009, Mohr Siebeck , Germany
[13] *Vagias Karavas*, Digitale Grundrechte, 2007, Nomos, Germany
[14] *Vagias Karavas*, Grundrechtsschutz im Web 2.0: Ein Beitrag zur Verankerung des Grundrechtsschutzes in einer Epistemologie hybrider Assoziationes zwischen Mensch und Computer, in:*C. Bieber/M.Eifert/T.Groß/J.Lamla*(Hrsg.), Soziale Netze in der digitalen Welt, pp. 301-325, 2009, Campus-Verlag, Germany
[15] *Wolfgang Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter Informationstechnischer Systeme, Juristen Zeitung (JZ), pp.1009-1022, 2008 Heft 21, Mohr Siebeck, Germany
[16] 岡崎俊一「通信の秘密の保護とその課題」、多賀谷一照＝松本恒雄編『情報ネットワークの法律実務（二)』、pp.3303-3319、第一法規、2004 年
[17] 小向太郎『情報法入門〔第 2 版〕』、NTT 出版、2011 年
[18] 佐藤幸治『日本国憲法論』、成文堂、2011 年
[19] 宍戸常寿「通信の秘密に関する覚書」長谷部恭男＝安西文雄＝宍戸常寿＝林知更（編）『現代立憲主義の諸相―高橋和之先生古稀記念』、pp. 487-523、有斐閣、2013 年
[20] 情報セキュリティ大学院大学「インターネットと通信の秘密」研究会報告書「インターネット時代の『通信の秘密』再考」（2013 年 6 月）
http://lab.iisec.ac.jp/~hayashi/610REPORTIII.pdf （2014/8/26 確認）
[21] 鈴木秀美「通信の秘密」大石眞＝石川健治（編）『憲法の争点』、pp.136-137、有斐閣、2008 年
[22] 曽我部真裕「通信の秘密の憲法解釈論」、『Nextcom』、16 号、pp.14-23、KDDI 総研、2013 年
[23] 高橋郁夫「インターネット媒介者の役割と『通信の秘密』」、『Nextcom』、16 号、pp.4-13、KDDI 総研、2013 年
[24] 高橋郁夫＝吉田一雄「『通信の秘密』の数奇な運命（憲法)」、『情報ネットワーク・ローレビュー』、5 巻、pp.44-70、商事法務、2006 年
[25] 高橋郁夫＝林紘一郎＝船橋信＝吉田一雄「通信の秘密の数奇な運命（制定法)」、『情報ネットワーク・ローレビュー』、8 巻、pp.1-26、商事法務、2009 年
[26] 高橋和広「ドイツ連邦憲法裁判所による情報自己決定権論の展開」、『六甲台論集』、59 巻 2 号、pp.57-116、神戸大学大学院法学研究科、2013 年
[27] 高橋和之「インターネット上の名誉毀損と表現の自由」、高橋和之＝松井茂記＝鈴木秀美（編）『インターネットと法〔第 4 版〕』、pp.53-86、有斐閣、2010 年
[28] 多賀谷一照『行政とマルチメディアの法理論』、弘文堂、1995 年
[29] 田川義博「インターネット利用における『通信の秘密』」、『情報セキュリティ総合科学』、5 号、pp. 1-35、情報セキュリティ大学院大学、2013 年
[30] ニクラス・ルーマン『制度としての基本権』、今井弘道＝大野達司訳、木鐸社、1989

年
[31] 西土彰一郎「接続データの保護―ドイツ憲法判例研究（161）」、『自治研究』、90 巻 9 号、pp143-151、第一法規、2014 年
[32] 西土彰一郎「デジタル基本権の位相」、鈴木秀美編『憲法の規範力　第 4 巻』、信山社、2014 年公刊予定
[33] 林紘一郎＝田川義博「『心地よい DPI（Deep Packet Inspection）』と『程よい通信の秘密』」、『情報セキュリティ総合科学』、4 号、pp. 3-52、情報セキュリティ大学院大学、2012 年
[34] 平松毅「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〕』、pp. 60-66、信山社、2003 年
[35] 棟居快行『人権論の新構成』、信山社、1992 年
[36] 棟居快行「通信の秘密」、『法学教室』、212 号、pp.44-47、有斐閣、1998 年
[37] 郵政省『電気通信サービスにおける情報流通ルールに関する研究会報告書』、1997 年 12 月
http://www.soumu.go.jp/main_sosiki/joho_tsusin/pressrelease/japanese/denki/980105j601.html （2014/8/26 確認）