連邦刑事庁（ＢＫＡ）・ラスター捜査・オンライン捜索（２）

――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――

植　松　健　一

第三章　ＢＫＡ法改定の境界値②――ＩＴ基本権・私生活形成の核心領域・裁判官留保

本章では、いわゆる「オンライン捜索」（Online-Durchsuchung）[1][2]に関する連邦憲法裁判所判決（BVerfGE 120, 274）について、ＢＫＡ法改定問題を意識しながら考察を加えていく。

1　背景

（1）端緒　法政策的論題としての「オンライン捜索」は、連邦内務省が二〇〇六年一〇月一〇日に「国内治安強化プログラム」（Programm zur Stärkung der Inneren Sicherheit：ＰＳＩＳ）を公表し、その関連経費一億三二〇〇万ユーロが同年一一月九日に連邦議会予算委員会で承認されたことを一つの契機とする。ショイブレ連邦内相は、「可能性としての犯罪準備が予め事前に認識され、妨げられる。これにより住民の安心感も強化される」という認識の下、ＢＫＡ、連邦警察（ＢＰ）、連邦憲法擁護庁（ＢＶｆＳ）、及び連邦情報技術保安庁の下に「即戦力型及び出動・捜査支援型のツール（die operative und die einsatz- und ermittlungsunterstützende Instrumentar）を構築することで、依然存続する脅威状況に効果的且つ毅然と対峙する」ことを、このプログラムの目標と説明した[3]。ＰＳＩＳでは、「こうした目標のためのひとつの重要な礎石」として「訴追に関係する内容について遠隔地にあるパソコンを捜査できる技術的な能力」が挙げられていたことから（措置2―1）[4]、野党等からは、これは「オンライン捜索」導入を示唆したもので、「諸官庁が公式に『ハッカー』として活動することを予定しているのは明白」[5]といった批判を招くことになる。

（2）概念と手法　「ハッカーとしての警察」[6]といった批判者たちの警鐘もあって「オンライン捜索」という言葉は人口に膾炙されるようになったが、その全体像は技術的可能性の観点も含めて未知・不明確な点が多く、その定義も諸説存在する状況である。この点について若干の整理をしておきたい。

①「情報技術システム」（informationstechnisches System）――連邦憲法裁は、この捜索の対象となる「情報技術システム」（以下、本稿では引用文中も含めて「ＩＴシステム」と略記する）として机上型パーソナル・コンピュータの他、住居や自動車内に設置された電子通信機器、ラップトップ、携帯情報端末（PDA）、さらに携帯電話や電子手

帳等の中で一定水準のデータ収集・保存機能を備えた機器を想定している（vgl. BVerfGE 120, 274 [311, 314]）[7]。

②「オンライン捜索」――連邦最高裁判所（ＢＧＨ）の決定では、「被疑者が利用するパーソナル・コンピュータ／ラップトップの捜査、とりわけハードディスク、メインメモリに記録されたデータの捜査、並びにこれらの押収」及び「コンピュータの記録メディアに保存されたデータをコピーし、捜査官庁による点検（Durchsicht）の目的でダビングするための当該措置の秘密の実行」並びに「この目的のためにプログラミングされたコンピュータ・プログラムをインストールさせるよう被疑者に手渡すこと」、を「いわゆるオンライン捜索」と呼んでいる（BGHSt 51, 211）。他方、連邦憲法裁の判決では、より限定的且つ明快に「技術的侵入手段を用いたＩＴシステムへの秘密の接続（Zugriff）」と定義されている（BVerfGE 120, 274 [277]）。さらに、学説では「オンライン捜索」と一般に呼ばれる措置のうち、ＩＴシステムへの秘密接続により一回のみ又は限定時点でデータをコピーする「オンライン点検」（Online-Durchsicht）と、システムを継続的に監視する「オンライン監視」（Online-Überwachung）との区別が意識されているようである[8]。後者の概念は、「源泉型電子通信監視」（Quellen-Telekommunikationsüberwachung）[9]と呼ばれる暗号化された電子通信に対する監視を目的とするＩＴシステムへの侵入を抱含しうる。後で見るように連邦憲法裁も「オンライン捜索」を基本法一三条二項の意味における「捜索」とはみなしておらず、「捜索」という用語自体が不適切だという指摘[10]ももっともである。しかし、本稿ではさしあたり、「ＩＴシステムへの秘密の接続」という連邦憲法裁の定義を前提に稿を進めることにする[11]。

③捜索に用いられる技術――捜査対象となるＩＴシステムへの侵入は、ネット上から侵入する方法と、対象パソコン等にソウトウェアを秘密裡にインストールする方法との二つが考えられるが、このためのコンピュータ・プログラムとして„Remote Forensic Software“（ＲＦＳ）が利用される。「トロイの木馬」（Trojanisches Pferd）又は「連邦の木

馬」（Bundes-Trojaner）[12]の通称で知られるこのプログラムは、自己増殖性はないものの、一般のEメールやアプリケーション・ディスクを装いユーザーのITシステムに侵入し、アンチ・ウイルスソフトを無効化し、当該システムで作成・利用された電子文書やEメール、各種パスワード、クレジットカード番号等の記録、キーボードの入力信号の記録（キーロガーの利用）、あるいはパソコン電話通信の記録などを行い、これを捜査機関のパソコンに伝達する。さらに、捜査対象パソコンに登録されたメールアドレスから別のパソコンへの侵入も可能とされる[13]。

（3）NRW州憲法擁護法　PSISに示されていた方向に呼応するようにNRW州は〇六年一二月二〇日に州憲法擁護法（VSG）を改定し、刑事訴追領域ではなく公安的情報収集の領域（すなわち州憲法擁護局［Verfassungsschutzbehörde］の調査権限）でのオンライン捜索を可能とした。NRW州議会の第一読会から本会議採決まで約三ヵ月のスピードで成立したその五条二項は以下のような規定となっていた。

> 憲法擁護局は、諜報手段としての情報徴取に関する第七条の基準の下で、以下の各号に掲げる措置を講ずることができる。
> …
> ⑪　インターネットの秘密の観察（Beobacht）その他の解析、とくにインターネット上のコミュニケーション装置（Kommunikationseinrichtung）への秘密の関与若しくは当該装置への捜査のような措置、又は技術的手段を用いたITシステムへの秘密の接続。これらの措置が、信書・郵便・電信電話への侵害を示している又は態様及び重大さの点でこれに類する場合には、当該侵害は基本法一〇条に関する法律[14]の要件の下でのみ許される。

法案審議の際の提出理由書では、インターネットを利用した過激派（Extremist）の犯行準備やサイバー攻撃の増大に対応しうる「実効的な情報収集」の必要性が指摘され、五条二項一一号は、公開されたサイトの観察のみならず、

チャット・ルームやネット・オークションへの関与、ドメイン所有者の確認、秘密サイトの発見、「保存されたコンピューター・データへの接続」等を可能にする規定という位置づけがなされていた（NRW LTDrucks 14/2211, S. 17. また、提出理由書からは情報自己決定権の侵害に配慮した規範特定性の要請充足のための法改定であると法案提出者が考えていた点も確認できる）。

（4）連邦最高裁判所（BGH）の違法判断とそのインパクト　このような内務省や州治安官庁の動きに水を差したのは、まずは連邦最高裁である。先に引用した意味での「オンライン捜索」に関する連邦最高検察庁の二件の令状請求に対して連邦最高裁U・ヘベーンシュトライト捜査判事は、〇六年一一月二五日及び二八日、情報自己決定権の重大な侵害である当該捜査には法律上の授権が必要であるという理由から、同年二月の事案で令状を出した前任捜査判事の判断（3 BGs 31/06）を覆すかたちで、検察の請求を斥けた（1 BGs 184/06; 1 BGs 186/06）[15]。これに対する連邦検事総長の異議に対しても、〇七年一月三一日の連邦最高裁判所刑事第三部決定は「秘密のオンライン捜索」を刑事訴訟法の根拠の無い不適法な措置と判断して当該異議を却下している。連邦最高裁は、令状請求書で挙げられていた通信監視（刑事訴訟法一〇〇ａ条）や住居監視（同一〇〇ｃ条）、あるいは技術捜査の一般権限（同一〇〇ｆ条一項二文）がいずれも「秘密のオンライン捜索」の法的根拠とはならず、情報自己決定権を侵害する措置に対して必要な法律の留保や規範明確性・規範特定性の原則を充たしていないと解したのである（BGHSt 51, 211）。連邦最高裁の違法判断に対して内務省サイドは「オンライン捜索」を当面実施しないとする一方、それでも捜査手法として不可欠という姿勢は崩さず、基本法改定による合法化も視野に入れた早急な法整備の必要性を表明した[16]。同時に、連邦議会での追求やメディア取材の過程で、ＢＶｆＳやＢＫＡが従来から秘密のオンライン侵入を実施していた実態が明らかになった[17]。ＢＶｆＳの場合、〇五年にシリー連邦内相（当時）の職務命令に基づき「オンライン捜索」が実施さ

れた事実が確認されているが、これは明確な授権規定に基づかず、ＢＶｆＳ法八条二項が定める議会への報告も怠った問題のある措置といえる。

（5）ＢＫＡ法改定問題　このような状況に本稿第一章で言及したＢＫＡ法改定問題が絡んでくる。内務省は、一方では犯罪捜査に「オンライン捜索」を用いるための刑事訴訟法の改定を、他方では「国際テロリズム」の危険防除の枠内でのＢＫＡ法への「オンライン捜索」権限の挿入を期待していた[18]。しかし、この「オンライン捜索」の是非をめぐり連立政権内部の国内治安政策上の不協和音が表面化する。連邦最高裁決定後、ＳＰＤ左派出身の連邦司法大臣Ｂ・ツュプリースが、「オンライン捜索」の立法化への難色を公然と示すようになったからである。彼女は〇七年二月一三日の欧州一〇カ国警察会議（開催地ベルリン）の演説の中で現職閣僚でありながら連邦内務省が推進する「オンライン捜索」を「国家的ハッキング」と呼び強く非難した。「新たな秘密の監視権限が実際に必要なのか心底丁寧に考えてみるべきだというのが私の思うところです。予防的領域でも抑止的領域でも全く同様のことが言えます。わが国の警察が高く評価されている要因には、公開性の光を厭う必要がないという点もあるのです。いわゆる『オンライン捜索』によって、軽率にこの評価を危険に晒すべきではありません[19]」、と。こうした連立政権内の意見対立を別にしても、刑事捜査に「オンライン捜索」を用いた場合、スパイウェアその他の手段による侵入が原因でＩＴシステムは何らかの改変を被る可能性があり[20]、また捜査機関が侵入に成功するようなパソコンはすでに他の第三者によるハッキングやウィルスの侵入を許している可能性もそれだけ高いことを意味しており、そのようなパソコンから徴取したデータが刑事事件の公判での証拠として採用されうるのかという根本的な疑問も指摘されていた[21]。しかし、司法省の消極姿勢とは対照的に、内務省はＢＫＡ法改定作業を進め、七月一一日に公表した同法改定の内務省原案（ショイブレ原案）の中に、ＮＲＷ州憲法擁護法五条二項を範にしたと見られている[22]授権規定を盛り込んだ。しかし、ＮＲ

W州憲法擁護法五条二項それ自体が連邦憲法裁判所の憲法異議手続に付されていた。憲法異議を提訴したのは、一件はフリーライターのB・ヴィンセマンと左翼党（DIE LINKE）州支部運動員（原告Ⅰ。代理人は人権擁護団体Humanistische Unionの常任幹事を務める弁護士のF・ロッガーン）、もう一件はFDPの元連邦議会議員で元連邦内務大臣も務めた弁護士のR・バウムら（原告Ⅱ）である（州政府側の代理人は、パッソー大学法学部公法・安全法・インターネット法講座教授D・ヘックマン）。この二つの原告団は一定の成果を勝ち取った「大盗聴」違憲確認訴訟原告団の流れをそれぞれ汲んでおり、前者が左翼党系、後者がFDP系という点では市民提訴のかたちをとった「大連立」政権の国内治安政策に対する政治的抵抗とみることもできよう。ツュプリース連邦法相はBKAへの「オンライン捜索」権限付与の是非はこの憲法異議に対する連邦憲法裁の判断を待って判断されるべきだと主張しており[23]、このような文脈で当該憲法異議は判決前から世論の関心を集めていたのである[24]。

2　判決要旨

NRW州憲法擁護法五条二項一一号、同三項、五a条一項、七条二項、及び八条四項二文を対象とするこの憲法異議に対して連邦憲法裁判所第一法廷は、二〇〇七年一〇月一〇日の口頭弁論を経て[25]、〇八年二月二七日に判決を言渡した。その内容は、五条二項一一号の訴え部分について、同規定が基本法一条一項と結びついた二条一項及び一九条一項二文に反し違憲無効とするものであった（自余の請求部分については訴え自体が不適法として却下、又は請求に理由はないとして棄却している）。多くの争点を含む本件の全体像を見渡すために、まず、その判決主旨（Leitsäze）を訳出しておこう。

① 一般的人格権は、ＩＴシステムの秘密性と完全性の保障に対する基本権（Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme）を含む。

② ＩＴシステムのネットワークを監視し、その記憶媒体を解読することを可能にする当該ＩＴシステムへの秘密の侵入が憲法上許されるのは、極めて重要な法益（ein überragend wichtiges Rechtsgut）に対する具体的な危険についての事実上の手がかりが存在する場合に限られる。極めて重要な法益とは、人の身体、生命及び自由、又はその脅威が国家の存立や基盤若しくは人間の生存の基盤に関わるような公共の利益のことをいう。危険が極めて近い将来において発生するという十分な蓋然性がいまだ確認できない場合でも、特定の事実が、個別具体的な事案において特定された人物が脅かしている、極めて重要な法益に対する危険を示している限りにおいて、措置は正当化されうる。

③ ＩＴシステムに対する秘密の侵入は、原則として裁判官の令状の留保の下で、講ずることができる。このような侵害を授権する法律は、私生活形成の核心領域を保護するための予防策を設けねばならない。

④ 授権が、コンピューター・ネット上の継続的な電子通信の内容や状態を把握し、あるいはそれに関連するデータを解析する手段たる国家的措置に限定されている場合には、侵害は基本法一〇条一項に照らして評価されねばならない。

⑤ 国家が右目的のため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に関する情報を入手する場合に、基本法一〇条一項への侵害が生じるのは、国家機関がコミュニケーション当事者から閲覧の承諾を得ていないときに限られる。

⑥ 国家が一般的にアクセスできるインターネットの中でコミュニケーションの内容を徴取したり、一般的にアクセスできるコミュニケーション過程に関与する場合には、原則として国家は基本権を侵害するものではない。

以下、判決理由となるＣ部分（BVerfGE 120, 274 [302 ff.]）の流れを辿っていきたい（小見出しは筆者による。小見出し後の括弧内数字は連邦憲法裁判所判例集の該当頁を示す）。

（1）「ＩＴシステムの秘密性と完全性の保障に対する基本権」の意義（302―306）

判決は、まず、ＮＲＷ州憲

法擁護法五条一一号一文二段第二肢（以下、本節及び3節おいては本件授権規定と略記）が、「ＩＴシステムの秘密性と完全性の保障に対する基本権」という特別の形状（Ausprägung）をとった一般的人格権を害する（verletzen）と認定する。そして判決は、この基本権コンセプトの意義と内容を明らかにするために、「ＩＴシステムがいたるところに偏在し、その利用が多数の市民の生活の営みにとって中心的な意義を持つに至った」現代の技術の進歩が個人の人格と発展可能性に極めて有益である一方、しかし同時に、簡単にデータを作成、加工、保存できるパソコンのネットワーク化によりもたらされる個人データ流出などの事故が人格への新たな脅威となっている状況を丹念に描いている。曰く、パソコンが仕事でもプライベートでも多様な用途に活用され、メインメモリや記憶媒体に個人的・社会的な対人関係やネットの利用状況に関する大量の情報が含まれる今日、これらのデータが第三者により徴取・解析された場合、そこからネット利用者の人格の逆推知が可能になる。とくにネットに接続されたシステムの場合、他人によるシステム上のデータの覗き見や不当な操作を目的とする接続を通じて、その危険性はさらに高まる。暗号化などの防衛策も、ひとたびシステムが侵入を受ければ効果を失うことがある。このように「個人は、妨げられることのない人格発展の見地から正当化される、この種のシステムの完全性と秘密性への期待を国家が尊重することに頼らざるをえない」ため、「基本権上の高い保護」が要請される。

（2）「ＩＴシステムの秘密性と完全性の保障に対する基本権」の保障範囲（303，306－315）　このことを踏まえ判決は、「ＩＴシステムの秘密性と完全性の保障に対する基本権」は、「情報自己決定権のような一般的人格権の別の具体化、及び基本法一〇条や一三条の自由権保障が、保護を与えないもしくは十分には与えない場合に、これらの権利に付け加わる」ものと位置づけた上で、これら各基本権が「ＩＴの発達により生じた保護の必要性を十分に考慮したものではない」ことを個々に論証してゆく。

すなわち、まず、①電子通信の秘密の保障（基本法一〇条一項）は、「通信回線を利用した個人受信者への情報の非身体的な伝達を保護するもの」であり、ＩＴシステムの利用それ自体の監視や、システムの保存媒体捜索のための接続から個人を保護するものではない。また、データ解析を行う他の官庁への提供を目的とする電子通信への接続も、継続的な電子通信ではないから、一〇条一項侵害とはならない。しかし、電子通信監視目的でのＩＴシステムへの進入（源泉型電子通信監視）の場合、通信利用と無関係の保存情報や特定のサービスの請求回数のような付随的なデータまでも含めたシステム全体が覗き見られ、さらに被侵入ＩＴシステムが世帯内の諸機器と連動していれば個々人の住居内での行動までが把握されてしまう危険性が伴うため、その脅威は通常の電子通信監視の比ではない（源泉型電子通信監視に限定されたシステム接続ならば基本法一〇一項が「唯一の基本権上の基準」となるが、口頭弁論の証言によれば、仮に監視実施機関が意図しなくとも措置目的とは無関係の情報の取得が現在の技術の下では回避できないという）。

また、②住居の不可侵性の保護（基本法一三条一項）もＩＴシステム侵入に対する保護とはならない。人間の尊厳及び人格発展の観点から「私生活が発展する空間的領域」を保護法益とする基本法一三条一項は、接続形態に規定されない総合的な保護を付与するものではない。「侵入が当事者のコンピュータのネットワークへの接続を利用したものである限り、住居の境界により付与される空間的な私的領域は侵されていない」（携帯型ＩＴシステムに対する捜査の場合、捜査機関はシステムの位置を特定できない場合すら少くない）。

最後に、③情報自己決定権は「個人が自己の人格発展のためにＩＴシステムの利用に頼らざるをえず、且つ、その際には個人データをシステムに委ね、又は、そもそも当該ネットワークを通じてのみ不可避的に個人データを産出していることから生じる人格への脅威を十分に想定してはいない。このようなシステムに接続した第三者は潜在的には

極度に巨大で表現力を持ったデータの束を、さらなるデータ徴取やデータ加工に頼ることもなく手に入れることができる。このような接続は当事者の人格にとっての重大性の点で情報自己決定権が保護する個々のデータ徴取をはるかに超えている」。

次に判決は、「ＩＴシステムの秘密性と完全性の保障に対する基本権」の保護範囲と権利の性格を描き出す。それによれば、不正な侵入によって「個人の生活形成の本質的部分を覗き見ること」や「人格の鮮明な像を獲得すること」が可能になるほどの規模と多様性をパソコンやＩＴ上のネットワークが含む場合には、システム機器の形態（机上型かモバイルか）や使用目的（私的利用か事業用か）に関わらず、この基本権が適用され、その対象はパソコンのみならず、右のことを可能にする程度のデータ徴取・保存機能を備えていれば携帯電話や電子辞書も含まれるとされる。この権利が保護するのは、「まず、その保護範囲に含まれるＩＴシステムによって作成、改変、保存されるデータが信用のおけるものであり続けるという利用者の利益」である。また、「保護されたＩＴシステムの完全性が、当該システムの作業、機能、保存内容が第三者の手で利用されうるようなシステム接続により、傷つけられる場合」にはこの権利の侵害が推定される。とくにこの権利は「システム上にあるデータが完全に又は本質的な部分について覗き見ることができる秘密の接続」（そこには、メインメモリ内のデータや一時的又は継続的にシステムの記憶媒体に保存されたデータに加えて、措置対象者のデータ処理諸過程（Datenverarbeitungsvorgänge）に関するデータ徴取をねらいとする場合も含まれる）から個人を保護する。又、この基本権の保護は「ＩＴシステムへの接続が容易か、それとも著しいコストをもって可能かという点に左右されず存在するのである。ただし、基本権上承認されうる秘密性の期待・完全性への期待が存在するのは、当事者がＩＴシステムを自分のものとして（als eigenes）利用し、それゆえ状況によって当事者が単独で又は利用権限のある他人と一緒にＩＴシステムを自己決定によって利用できるという点を出発

点におくことが許される場合に限られる。自己所有のＩＴシステムの利用が他者の処分権能（Verfügungsgewalt）の中にあるＩＴシステムを経由してなされる限りで、利用者の保護はそこにも及ぶ」。

（３）規範特定性・規範明確性（315―318）　判決は、右権利が無制約ではなく、その侵害も「憲法に適合した法律上の根拠」があれば、「予防的目的のためにも、刑事訴追のためにも正当化されうる」ことを前提に、本件授権規定の憲法適合性の検討に入る。まず、判決は、措置の要件を単に「基本法一〇条に関する法律の要件の下で」と定めるだけの本件授権規定が、不特定・不明確な法概念によって公権力行使の予見可能性と当該権力行使に対する司法判断可能性が脅かされてはならないとする規範明確性・規範特定性の要請と合致しないと断ずる。その際、判決は、いかなる措置が基本権侵害となるかという複雑な見極めと評価を必要とする問題は第一次的・優先的に立法者の任務であるという点を強調した上で、それゆえにこそ、措置に関わる基本権の構成要件を指摘するだけで当該基本権侵害に対する予防策を法律により具体化するという立法者に課された任務を免れるような立法技術は、テクノロジーの発展に対応した新種の捜査措置を規律する本件授権規定のような場合においては、特定性の要請を充たすことにならないと説く。しかも、本件授権規定は「態様及び重大さ」において基本法一〇条の侵害に類する措置も予定しているが、いかなる措置がそれに該当するかの具体的な基準が全く明記されていない点で問題があるというのである。

（４）合理性・必要性（319―321）　次に判決は本件授権規定の合理性・必要性を審査し、それらの判断に際する立法者の大幅な評価余地を前提に、各要請は充たされていると判断する。まず、合理性の点では、「テロ」等の危険との対峙は憲法上の極めて重要な法益である国家の安全と国民の生命・身体・自由の安全に資するものであるところ、極右や「テロリスト」による電子化・デジタル化された通信手段を利用した犯罪の準備・実行の可能性の増大が憲法擁護局の実効的な任務遂行を妨げている現状では、ＩＴシステムへの秘密の接続は脅威状況の解明の可能性を拡大す

る点で、目的に対して合理的であるとする。その際、判決は、スパイウェアを用いた秘密の接続がアンチウィルス・ソフトによりブロックされてしまうといった技術面での難点や徴取された情報の公判上の証拠価値の難点が文献や本件口頭弁論の証言において指摘されている点を踏まえつつも、接続が常に失敗するわけではなく、技術面での問題は将来的な改善が予測されるとし、又、証拠採用の困難さは徴取される情報の価値自体を貶めるものではなく、まして、危険前段階の予防的な憲法擁護局の調査活動に必要な情報は刑事手続の証拠とは性格が異なるとして、これらの批判を退けている。さらに、判決は、当該システム上のデータを徴取する手段として、ＩＴシステムへの秘密の接続と同程度に効果的で、しかし当事者の負担がより軽いものは他に存在しないと立法者が推定したことも許される判断であるとし、必要性の原則にも違反しないと認定した。

（5）狭義の比例原則（321―327）　しかしながら、判決は本件授権規定が狭義の比例原則の要請を充たしていないと判断する。そのために、まず判決は本件授権規定の基本権侵害の高強度性を論証する。すなわち、ＩＴシステムの下でデータ保存された文書、画像、音声には個人の人間関係や生活の営みに関するセンシティブな個人情報が含まれ、しかもそれは規模と多様性で従来の情報源を上回るため、このデータ・ストックに国家が接続すれば、「全体的眺望の中で高度なデータが交際やコミュニケーションのプロフィールの像から当事者の人格まで広範に帰納推論を可能にする明白なリスクと結びつ」き、さらに当該データに措置対象者の第三者とのコミュニケーションに関する情報が含まれている場合には、措置は第三者の情報も把握できる点で著しい面的網羅性（Streubreite）を持ち、市民の遠隔通信への参加の可能性を制約する。とくに、本件授権規定が認める秘密の接続によるシステムの長期的監視と継続的な情報徴取の場合には、①措置対象者の人格にとって重要なセンシティブ情報やシステム接続のためのパスワード等の情報の獲得を可能にする、②措置対象者が自ら設定しているＩＴ上の防御手段を毀損する、②接続が秘密に行わ

れるため当事者が事前又は事後に裁判上の救済を求める可能性を奪う、③秘密の接続はコンピュータの完全性を脅かすと同時に当事者さらには第三者の法益を脅かすため侵害が格段に強いものになる、とされる。このような侵害が適切性（Angemessenheit）の観点から許容される条件として具体的に提示されたのは、①極めて重大な法益に対する具体的危険の存在、②裁判官留保、③私生活形成の核心領域の保護、の三点である。そして、以下のような考察から、本件授権規定がこれらの憲法上の要請を充たしていないと判断されたのである。

①具体的な危険（327－331）――判決は、まず、極めて強い基本権侵害においては侵害のきっかけ（Eingriffsanlass）がぞんざいに規律されている場合には、それだけで比例性に反すると述べ、①立法者が「一方に基本権侵害の態様と強度と、他方に侵害を授権した構成要件要素との間の均衡を維持しなければなら」ないが、②「脅かされている法益侵害が極めて重要なものである場合ですら、十分な発動の蓋然性の要請は放棄されうるものではない」という立場を示す。そして、本件授権規定のような侵害が適切性を充たすのは、授権規定が「当該侵害を極めて重大な法益に対する具体的な危険の事実上の手がかりの存在に依存させている場合に限られる」とする。その際、「極めて重大な法益」とは、「まず、人の身体、生命、自由」及び「その脅威が国家の基盤や存立又は人間の生存の基盤に関わるような公共の利益」と定義され、後者には「例えば、生存に関わる公的な配慮施設（existenzsichernde öffentliche Versorgungeinrichtung）の本質的部分の機能力（Funktionsfähigkeit）なども含まれる」とされる。その上で、判決は、当該法益にとっての「具体的な危険の事実上の手がかりが存在」している旨が授権規定に明記される必要を指摘する。すなわち、秘密の接続には、推定や一般的経験則のみでは十分ではなく、「個別の事案、危険が損害に転ずる時間的近さ、及び危険惹起者（Verursacher）たる個人との関連」という三基準で特定されるところの「具体的危険の発生」に予測が関連付けられねばならない」というのである。「これは、国家の介入がなければ見通せる時点において規範の

保護法益に対する損害が特定の人物により惹起されるという十分な蓋然性が個別事案において存在する事実状態のことである」。しかしながら、「危険が確実に近い将来において発生するという十分な蓋然性がいまだ確認しえない場合」でも、「特定の事実が個別具体的な事案において脅かされている極めて重大な法益に対する危険を証明する限りにおいて」ＩＴシステムへの接続は、正当化されると判決はいう。ただし、ここでの事実は、「一方では、少なくともその方法において具体化され時間的に見通せる出来事に対する推論を許し、且つ他方において、その本人特定性について少なくとも、監視措置が当人を目標として講じられ、且つそれに限定されうる程度には明確なものであるような特定の人物が関与しているという推論を許すもの」が要求されている。したがって、授権規定の定める「保護法益にとっての個別事例ではまだ見通せない具体的な危険の前段階にまで事実上の侵害のきっかけがさらに広く拡大されているような場合」には基本権侵害の重大さが考慮されておらず、憲法上許容しえないと判示する。そして判決は、措置の実施機関の違いは侵害を被る措置当事者にとって関係のないことである以上、この憲法上の要請を警察にも公安機関にも等しく妥当すると解する。この点、本件授権規定における州憲法擁護局による諜報的措置の発動条件は、「当該方法によって憲法敵対的企てに関する情報が獲得されうるという推定に関する事実上の手がかりにすぎず」、「侵害に対する構成要件の見地からも、保護されるべき法益の重大さの見地からも、十分な実質的侵害境界値ではない」とされる。

②裁判官留保（令状留保）（331－335）――次に判決は、本件侵害正当化の第二の条件として、「当事者の利益を手続法上守るための適切な法律上の予防策」の存在、具体的には、「独立且つ中立的機関による事前的コントロール」である裁判官令状の留保を挙げる。このようなコントロールは、授権規定の定める侵害要件の遵守の有無を審査対象とするため、法が規律していない侵害境界値を補う機能は果たせないとしても、しかし、「当事者自身が措置の秘密

性のために自己の利益を事前に維持することが不可能な場合において、秘密の捜査措置に関する決定が当事者の利益を十分に考慮して下されることを保障しうる」というのである。判決も、一般論として事前コントロールをいかなる機関がいかなる手続で行うかの判断は立法者に裁量であるとしながらも、本件のような特に強い基本権侵害を伴う措置については裁量は収縮し、原則として裁判官の令状が要請され、しかも、「裁判官が予定されている措置の適法性を十分に審査し、理由を文書で付記することが条件」だとする。もとより、「切迫した危険」（Gefahr im Verzug）のような緊急の場合に裁判所以外の機関にコントロールを付託することは例外的に許されうるが、その際にも、①当該機関が裁判所と同様の独立性と中立性が確保されている、又は中立的な機関による終局的な審査が留保されていること、②理由付記などの要請が遵守されていること、が必要である。しかるに、G10法三条一項一文は同法の定める犯罪を何人かが計画、着手、実行している「疑いに対する事実上の手がかり」だけで監視措置を認めており、又、G10法一〇条は州憲法擁護局の申立てに基づき所轄の州最高官庁が監視措置の事前命令を発することを認めており、裁判官留保又はこれと同等のコントロール制度を規定しておらず（NRW州G10法三条六項が規定する州G10委員会による事前コントロールも、本件授権規定では挙げられていない）、州最高官庁は裁判所と同等の独立・中立性を有していない以上、同法の引証だけでは憲法上の要請としての事前コントロールを保障するには十分ではない。

③私生活形成の核心領域の保護（335―339）――第三に判決は、公共の重大な利益保護が目的の立法であろうとも絶対的に保護されなければならない私生活形成の核心領域への侵害を回避するための十分な予防策が本件授権規定には欠けていると指摘する。すなわち、ITシステムは日記的な記録や私的な録画・録音など「高度に個人的な内容のデータ」の作成・保存にも利用されているため、これへの秘密の接続、記録媒体の点検、インターネット通信監視等が核心領域に属する個人データを徴取する危険性は高く、しかも措置の秘密性のために措置対象者が異議申立を行う

機会がないことを指摘し、このような危険を遮断する適切な手続的予防策が法律により規律されていること、また、その際に核心領域保護が「二段階の保護コンセプトの枠内で保障されている」ことを求める。すなわち、第一段階の保護は、核心領域に関わるデータがＩＴ技術上・捜査技術上可能な限り徴取されないことを法律で明記することである。とくに「個別具体的な事案において特定のデータ徴取が私生活の核心領域に関わることを示す具体的な手がかりが存在する場合には、原則として当該徴取は行われてはならない」（ただし監視妨害の目的で核心領域に属する内容と犯罪等に関わる内容が意図的にコミュニケーション中に混在されていることを示す「具体的な手がかり」が存在する場合はこの例外とされる）。しかし、データが核心領域に関わるか否かは徴取措置実施前の段階では明らかでない場合が多いため、第二段階の保護として、核心領域に関わるデータが徴取された場合でも、核心領域侵犯の強度と措置対象者の人格発展への影響を最小限にとどめるための適切な手続規定が必要になる。この点で極めて重要なのが、「措置対象者の利益を十分に考慮した適切な手続」を踏まえた被徴取データの事後点検（Durchsicht）の存在であり、この過程で核心領域に関わるデータの徴取が判明した場合には速やかに（unverzüglich）抹消され、その提供や利用が行われない旨が規律されていなければならないとされる。ところが、引証されているＧ10法はこのような核心領域保護規定を置いていないため、本件授権規定における核心領域保護規定の不在という瑕疵を治癒するものではないと判断されたのである。

（6）インターネット解析（Internetaufklärung）その他（340－350）　以上の理由から本件授権規定におけるＩＴシステムへの秘密接続の部分（第二肢）は無効とされた。さらに判決は同規定のインターネットの秘密の見張・解析に関する授権部分（第一肢）も基本法一〇条一項等に違反し無効とした。しかし同時に判決は、一般論として官庁が一般的にアクセス可能な手段による個人関連情報の取得は禁止されていないことを前提に、覆面捜査官型の詐術を

用いたネット上のコンタクトのような「コミュニケーション相手の完全性とモティベーションに対する保護に値する信用」を利用した捜査でなければ情報自己決定権の侵害に当たらず、まして純粋なインターネット解析措置は、「コミュニケーション相手の本人確認性と正直さへの信用は保護に値せず」、いかなる基本権侵害も生じないという傍論的な説示を加えている（Ⅱ［340―346］）。さらに判決は、五条二項一一号は全体として無効のため五条三項及び一七条に関する審査の必要はないとし（Ⅲ［346］）、最後に金融機関を通じての預金状況や取引状況に関する情報徴取を授権した五a条については情報自己決定権の許される侵害として合憲判断を下しているが（Ⅳ［346―350］）、ここではその論旨は省略する。

3　検討

「ここ十年でこれほど学問上・政治上の注目を集めたものは見当たらない」[26]とも評される本判決には多様な論点が含まれており、その全体像の把握と本格的な考察のためには別稿が必要であろう。本判決が認知したＩＴ基本権（判決の言葉では「ＩＴシステムの秘密性と完全性の保障に対する基本権」[27]）と、通信の秘密、住居不可侵、自己決定権という既存の基本権との連関を検討するだけでも、それぞれの基本権にまつわる豊富な議論蓄積を踏まえねばならず、その他にもＩＴ基本権の客観法的性格に関わる問題や、そこから派生する私法上の保護の要請の点など広い奥行を持つ論点が控えているからである。ここでは、本判決に対する評釈等を参考にした論点整理と、それらに対する本稿なりの若干の考察を行うにとどめ、次章につなげたい。

（1）「新しい基本権」の導出

本判決が世論や学説の耳目を引いたのは、なによりもＩＴ基本権という新しい基本権コンセプトが語られた点である。

①概念――この基本権は「ＩＴシステム」、「秘密性」、「完全性」という三つの要素から成り立っている。判決が念頭におく「ＩＴシステム」については先に説明した。「秘密性」と「完全性」の意味についてはＴ・ベッケンフェルデの判例評釈が参考になる[28]。それによればVertraulichkeitとして事実上判決が念頭に置いているのは、「国家による（秘密の）覗きや監視からのシステムにより作成され、当該システムの『中に』保存されているデータ状態の保護に対する信用（Vertrauen）」のことだという。この信用こそが、「個人の本人関連データを一回又は繰り返しアクセスできる動態的な全体に纏め上げ、したがって不正な接続の下で当事者を彼の個人的な生活の営みの点で丸裸にすることができるＩＴシステムの媒介能力」を左右するからである。他方、「完全性」とは第三者による覗き見、監視、操作からのシステムの無傷性（Unversehrheit）が含意されており、したがって実際に個人データを覗き見られたかどうかに関わらずシステムの無傷性を損なう侵入――それはシステムの信用を傷つけ（kompromittieren）、システムに何らかの障害をもたらし、第三者による不正操作の原因にもなる――それ自体が、基本権侵害と見なされることになるという。

「完全性の保障」というコンセプトには、このような危険からの保護が含意されているわけであるが[29]、個人のパソコンの秘密性とは独立に、右のような意味における完全性の保護が当該基本権の内容とされている点は注目に値しよう。「ＩＴシステムの秘密性と完全性の保障」というコンセプトを一般的人格権から導き出すという発想は本件異議申立人の中にすら明確なかたちで形成されておらず[30]、まさしく連邦憲法裁のオリジナルな産物であるが、情報通信や住居内での会話が公権力によって把握されることがもたらす「信用」失墜の危険性は従来から文献の中で語られてきたところであり[31]、それを独自の基本権の保護範囲として設定し直したものと見ることもできる。

②基本法一三条との関係――しかし、基本法に明示されていない基本権を解釈によって導出する以上、他の基本権

との関係が問題とならざるをえない。実際、本判決以前、すなわち連邦最高裁決定後に盛んになった「オンライン捜索」の憲法的限界に関する論議の中心舞台は基本法一三条の住居の不可侵性の保障であった。有力な見解は、個人のパソコンに保存されたデータを一三条の保護範囲の問題と捉えた上で、刑事訴追目的での「オンライン捜索」については、基本法改定による明示がない限り許されないと説くものであった(32)。家宅侵入を伴わない「オンライン捜索」は同条三項を根拠とする刑事訴追目的の聴覚的監視とは解し難く、同条四項を根拠とする「住居の監視のための技術的手段」の使用は危険防除目的で認められる措置だからである（ＮＲＷ憲法擁護法に基づく公安情報収集のための「オンライン捜索」も同じことが言える(33)）。先に触れたように基本法改定を視野に入れた立法論が政治的に登場していたのもこのためであるが、連邦議会の三分の二の賛成を必要とする基本法改定の現実性を考えれば「法政策上の死(34)」に他ならない。仮に、「オンライン捜索」を同条三項又は四項で根拠付けるか、あるいは同条二項の「捜索」（これも物理的な住居への立入りを意味するため本来は無理がある）で説明をつけるとしても、この場合には、裁判官留保や「切迫した危険」（Gefahr im Verzug）の存在といった基本法上の厳格な要件に加えて、「核心領域」の絶対的保護という判例上確立された原則の遵守が立法上求められることになる。しかし、この一三条保護範囲肯定説には批判も少なくなかった。その理由としては、①ラップトップや携帯電話は通常住居外で利用されることが多い、②一三条の保護法益は住居という空間的バリアにおける秘密の行動であるがコンピュータ上の作業にはそのような性格が欠けている、③住居の不可侵性は静穏を目的とするものであり、ＩＴシステムによる他者とのコミュニケートとは目的が真逆である、などの点が挙げられている(35)。否定説の多くは、「オンライン捜索」を情報自己決定権侵害の問題と捉える(36)。一三条保護範囲肯定説からすれば、一三条よりも基本法明文上の制約の少ない自己決定権に舞台を移すことは「オンライン捜索」の安易な正当化を招くものと映るが、後者の説においても「単なる情報自己決定権の―しかし重大な―

侵害」[37]と受けとめ、私生活形成の核心領域の絶対的保護を要請したり、侵害に比例する厳しい境界値を設定すれば両者の対立は相対化されるはずであり[38]、本判決はそのような方向を選択したといえる。連邦憲法裁は、「一方で完全な侵害禁止を打ち立てはしなかったものの、他方では侵害の正当化に伴う要請を強固なものと把握しようとすることで、『オンライン捜索』をめぐる政治的な論議に現行憲法解釈論上の（de constituione lata）調停的な出口を示したのである」[39]。それゆえ、保護範囲否定説の側からは本判決の一三条解釈は好意的に受けとめられたが、他方、一三条保護範囲肯定説からは、捜索対象者にとってＩＴ機器が住居内にあるか外にあるかの区別は関係のないことであるし、保護範囲の限定は監視技術の高度化の前に一三条の意義を低減させかねないという批判が出ることになる[40]。いずれにせよ、現状の技術ではネットを通じた侵入ソフトのインストールの成功の確率はなお高くなく、並行して秘密の住居立入りによりパスワード情報を取得したり、直接にパソコンに侵入ソフトをインストールする状況が予想され、運用上「オンライン捜索」における基本法一三条の出番はけして少なくはないと見られていることも指摘しておこう[41]。

③基本法一〇条との関係――本判決では、基本法一〇条の通信の秘密の保障についても、通信切断後の情報徴取を基本権一〇条の保護範囲から外したが、これはパソコンや携帯電話に保存されたＥメール、パソコン通信、携帯メール等の通信記録の捜索を目的とする当該機器の押収に関して二〇〇六年に第二法廷が下したハイデルベルグ決定（BverfGE 115，166［187－190］）の判断を踏襲したものであり[42]、その限りでは新規なものではない。ただし、この決定の示した法理自体への批判も少なくなく、一〇条の射程限定には議論の余地がある。とはいえ本判決では、一三条とは対照的に、一〇条とＩＴ基本権の部分的な競合関係が認められており、とくに源泉型電子通信監視が通話以外のＩＴシステム内の情報も同時に徴取することでシステムの完全性を害する場合には、ＩＴ基本権による保護が及ぶと解されている[43]。

④情報自己決定権との関係――さらに、一般的人格権から連邦憲法裁の解釈により導き出された権利という点でＩＴ基本権と出所を同じくする情報自己決定権との関係において、本判決はより多くの批判に晒されている。遡ってみるに、国勢調査判決以来、連邦憲法裁は情報自己決定権の射程拡大に努めてきた。前記の第二法廷のハイデルベルグ決定は、通信切断時の携帯電話の保存情報等について基本法一〇条の保護範囲から外す一方で、これらを情報自己決定権の保護範囲の問題として処理した（BVerfGE 115, 166［187－190］）。第一法廷自身も本件のわずか一年前の口座調査決定（BVerfGE 118, 168［183 f.］）では、国勢調査判決に依拠しながら情報自己決定権の拡大解釈を試みている。本稿第二章ラスター捜査でも、措置の面的広範性を自己決定権侵害認定の決め手としたのであった（BVerfGE 115, 320．本稿第二章参照）。こうした経緯からすれば、本件授権規定も、これまでの判例と同様に情報自己決定権の問題としてカバーできるではないかという疑問が出るのは当然であろう。したがって本判決における新たな基本権の創出は、情報自己決定権の射程を狭めることでその基本権保障の能力を削いだ点で、「単に余計というだけでなく、基本権ドグマーティクに間違った途を示すもの」と厳しく批判する評釈もある。秘密の接続が個々の個人データの取得では言い尽くせない侵害だというのであれば、なおのこと情報自己決定権の保護範囲として構成すべきであり、「そこから情報自己決定に対する次に来る大規模攻撃の備えとなるような比例性審査のための基準を発達させる方が適切であったはずである」というのである。[44] とくに本判決が情報自己決定権をもっぱら個人データの保護を対象としたものと限定的に把握した点は、国勢調査判決における情報自己決定権への理解との不整合が指摘されている。人格の生活形成の本質的部分の閲覧を可能にするパソコンへの侵入行為を、従来の判例が情報自己決定権の名で保護してきたデータの獲得・変更と同種のものと把握することがなぜに不可能なのかを本判決は明確には説明していないというのである。[45] 確かに本判決では、ＩＴ基本権の保護範囲から外れるとされた一般に公開されたインターネット上の情

報解析や、金融機関からの取引情報の提供等については、自己情報決定権の保護範囲にすら含めないか、又は保護範囲に該当するとした上で簡単に侵害を正当化しており（後述（7）参照）、批判的評者のこのような危惧も理由のないことではない。[46]

他方、このような批判に対して、判決擁護の論陣を張るのがW・ホフマン―リームと、判決当時、ホフマン―リーム付の連邦憲法裁調査官であったM・ベッカーである。[47] ベッカーは、IT基本権を有害・不必要とする評釈を、情報自己決定権の力への過大評価だと批判する。ホフマン―リームやベッカーからすれば、そもそもスタート点としての国勢調査判決自体が情報自己決定権の意味を正確に把握できていない。すなわち、国勢調査判決は、この権利を自由権としてのみ捉え、国家機関による個人情報の徴取、保存、利用、提供を当該権利の侵害と推定した。しかしながら、行政手続のほとんどは特定個人の何らかの情報と何らかの関わりを持つ以上、この判決のアプローチでは、公権力の情報収集活動等の内で人格にとり重大なものと些細なものの区別無しに法律の留保を求めるという不都合を招き、比例性衡量の基準も不明確なものになってしまう。これらの点から国勢調査判決のアプローチを批判する論者たち（その代表論者こそホフマン―リームである）[48]は、個人関連データないしは情報の社会的環境への依存性を強調し、情報自己決定権の本質を当該データ・情報への国家の関わりをプロセス化・透明化する一方、当事者に個人のコミュニケーション過程への自己決定的参加権を付与することで人格の保護と発展に資するという点に見出してきた。こうした社会連関説に与しながらベッカーは、情報自己決定権の機能的側面の二重性に着眼する。彼によれば、この権利の第一のそして主要な機能は、データや情報への国家の関わりを法で規律させ、もって当事者に十分な認識可能性と影響可能性を保障するという、客観法的要請である。もう一つは、「真性の」侵害防禦権としての情報自己決定権の側面である。この場合、情報自己決定権は、データや情報が特定の文脈において利用されることから生じる人格への脅威に

対して脅威発生時点で（punktuell）対応しはするが、しかし、それ自体保護に値するプライベートな退避圏までの射程は持たない。このように自己決定権の射程を限定した場合、その隙間を埋めるＩＴ基本権という新たなコンセプトがどうしても必要になってくる。[49] なぜなら後者の権利は、発生時点的脅威状態だけではなく、プライベート領域全般を保護するものだからである。かくして、個人のＩＴシステムは、個別具体的な事例において個人のセンシティブなデータが徴取されるか否かとは無関係に、国家による覗き見から保護されるのである。また、情報自己決定権を可能な限り包括的なかたちで国家及び私人による情報取扱いの一般条項にとどめておくべきと考えるベッカーは、ＩＴ基本権との役割分担による自己決定権のドグマーティク上の負担軽減を期待している。[50] また、Ｔ・ベッケンフェルデは、「オンライン捜索」が情報自己決定権侵害とされた従来の措置よりもはるかに高い侵害境界値（極めて重大な法益に対する具体的な危険、裁判官留保、私生活形成の核心領域）を必要とするため、比例原則の統一性の維持という法技術上の観点からもＩＴ基本権という新カテゴリーの創設も正当化されうると説明している。[51]

右に見てきたようなＩＴ基本権不要・有害論と必要論との対立は、単に保護範囲の役割分担の問題というだけではなく、すぐ後でも触れる基本権の客観法的側面の問題や解釈方法論としての保護範囲の限定の問題等とも連関する根の深い対抗軸が背後に控えていることがわかる。電子通信回線やインターネットを通じた公権力による個人情報徴取に対する情報自己決定権の「機能不全」は夙に指摘されており、[52] その再検討が主張される流れの中で本判決がどのような位置づけを占めるかは興味深い点であるが、ここでは問題の所在が明らかになればさしあたり十分である。

（２）「新しい基本権」の意義―客観法・保護義務論・脱個人化　連邦憲法裁が激しい批判を覚悟の上で新たな基本権を案出した説明として、この基本権の性格を主観的権利ではなく客観的法と捉えているからだという見方がある。[53] 基本権の二重機能という発想はドイツ憲法学にとっては特段に目新しいものではないが、[54] システム保障としての

ＩＴ基本権においては、その客観法的性格がより顕著となる。この客観法的側面から私人による法益侵害に対しての国家の保護義務も導かれることになり[55]、この方面での議論は今後より活発になると思われる[56]。本稿ではこの点をさらに展開することはできないが、本判決が基本権論に与える（であろう）インパクトの大きさを理解するために、Ｏ・レプジウスの分析を見ておきたい[57]。レプジウスは判決の基本権解釈を激しく批判する論者の一人ではあるが、判決を、現代治安法制の脱個人化（Entindividualisierung）傾向の下での基本権の主観的防禦機能の機能不全に対処するための、やはり脱個人化された基本権保障のアプローチとして「機能上の」観点からひとまず了解する[58]。レプジウスは、しかし規範特定性・規範明確性違反で処理できる本件とは異なり、より緻密な構成要件を持つ洗練された立法に対してこのような客観法的システム保障中心のアプローチでは対峙できないのではないかと予測する。さらにレプジウスは、この判決を「保護範囲」（Schutzbereich）思考から「保障内容」（Gewährleistungsgehalt）思考への転換という基本権解釈方法の「新傾向」の文脈に位置づける[59]。これまでの連邦憲法裁は伝統的な「保護範囲」に立脚して、その保護範囲の拡大により個人の防禦権としての基本権を保障してきた。しかし近時の連邦憲法裁（とりわけ第一法廷）は、保障範囲という概念の下、より社会的・機能的連関性をもった客観法的思考の中で保護範囲を確定しようとする姿勢を見せはじめている（BVerfGE 105, 252［グリコール決定］; BVerfGE 105, 279［オショー決定］[60]）。もとより、こうした「新傾向」については強い批判もあり[61]、レプジウスもそうした批判論に与する。「一方では基本権保護の主観的な中心化に固執しながら、他方では予防国家における自由喪失の異論の余地のない客観的次元を、客観的憲法上の限界をもって――しかし主観的権利の客観法的な濃縮をもってではなく――考慮に入れること[62]」がレプジウスの示す次善の戦略である。このようなレプジウス説に対しては、ＩＴシステムの完全性は措置により当該システムの秘密性が損なわれる限りで保障されると捉え、あくまで主観的な人格関連性との連関の中でシステム保障を語っていた本判決の「読み

替え」違いだとホフマン＝リームやベッカーが強く反論しているとおり[63]、自己の議論枠組みにやや引き付け過ぎの感はある。とはいえＩＴ基本権（及び連邦憲法裁の基本権ドグマーティク）の今後の展開を見据えた一つの読み方[64]としては鋭い洞察を含んでおり、少なくとも本判決はそのような読み方を可能にする「開かれたテキスト」であるともいえよう。

（3）規範特定性・規範明確性　評釈の中で本判決の規範特定性・規範明確性判断への言及がわずかなのは、措置の強度な基本権侵害を認定したにもかかわらず、合理性・必要性を簡単に認め、だがしかし規範特定性・規範明確性違反の観点から違憲性を導き出すという直線的でない論証の流れは、近時の連邦憲法裁の判断傾向の特徴として特に目新しいものではないからであろう[65]。西原博史は、このような実質的基準から形式的基準への「退却」による審査の実質化という意義を指摘した上で、しかし「立法技術的に洗練された法文によって予防的に何が何のために統制されるべきかが明らかになれば、それで裁判所による違憲審査が行き詰る」おそれを指摘している[66]（次章で扱う改定ＢＫＡ法は、まさにそのような「洗練された法文」である）。他方、連邦憲法裁の規範特定性・規範明確性に関する認定基準それ自体が不明確・不特定ではないかという疑念も出されており[67]、一見明快なその法理にも弱点があることがわかる。

（4）私生活形成の的核心領域　本件授権規定が比例性違反と認定された大きな理由は、絶対的に保護されるべき「私生活形成の核心領域」侵害回避のための対処が立法上講じられていないという点にあった。いわゆる「領域理論」における核心領域の絶対性という発想は、連邦憲法裁の判例上、判断枠組みとしては曲折を経ながらも基本線として維持されており[68]、とりわけ大盗聴判決では住居監視の際の核心領域保護の必要性の強調が刑事訴訟法の関連法規の違憲性認定に大きな役割を果たした（BVerfGE 109, 275. 税関刑事局判決［BVerfGE 110, 33］やニーダーザク

センン通信監視判決［BVerfGE 113, 348］もこの流れを踏襲する[69]。しかしながら、大盗聴判決の核心領域論に対しては、何が高度に個人的な会話で何が共同社会の利益に関わる会話かは外部からは認識できない以上、私人の住居内部の事柄は常に絶対的に保護されなければならないはずだとする二裁判官の反対意見が付されたことも念頭に置いておく必要があろう［Abweichnde Meinung der Richterinnen Jaeger/Hohmann-Dennhardt, BVerfGE 109, 275［382―384］][70]。しかも、本判決の核心領域論は、大盗聴判決多数意見のそれよりもさらに後退している可能性がある。大盗聴判決では、何が核心領域に属するかの詳しい検討がなされ、そこでは、「高度に個人的な信頼のおける人物」、「秘密の空間的状況」が核心領域侵犯認定の手がかりとされており、前者の例として措置当事者の家族、親しい友人、さらに宗教者や弁護士など証言拒否権を持つ地位にあるもの（刑訴法五三条）が挙げられていた（BVerfGE 109, 275［320―323］）。本判決は、このような大盗聴判決の基準の参照指示も付すことなく、何が核心領域かという困難な判断を実務に委ねてしまった感があるが[71]、本判決が「高度に個人的内容を持つデータ」を核心領域の内容の一つと解している以上、「オンライン捜索」の一三条侵害性の否定は大盗聴判決の緩和が認められる理由にはならないはずである。その点は別にしても、大盗聴判決反対意見の指摘のとおり、措置時点で核心領域に属する会話や情報か否かが外部からは判定できない以上、二段階保障コンセプトは、その二段階目、すなわち措置が核心領域を侵犯した場合の消去義務の保障に大きな負荷をかけるかたちで成立していることがわかる。したがって、判決の示した私生活形成の核心領域保護の二段階保障コンセプトは、立法者への要請としての意義は大きいとしても、運用レベルでは「絶対的な保護」という言葉の与える印象ほどには実効的ではないものなのかもしれない[72]。

（5）「具体的危険」の再定位？　本判決は、「オンライン捜索」のような重大な基本権侵害の境界値を「極めて重要性な法益に対する具体的危険の事実上の手がかりが存在する場合」に設定し、それが危険防除であろうと公安的

情報収集であろうと変るところがないと説示した点が注目される。[73] したがって基本線としては本稿前章で取り上げたラスター捜査決定の流れを踏襲し、かつこれを諜報・公安的情報収集の場面でも確認したと本判決を評することができる。この点では、ＢＮＤの通信監視について、基本権侵害の条件は警察法や刑事訴訟法のそれとはおのずと異なると説示した一九九九年の戦略的通信監視判決（**BVerfGE 100, 313 [383]**）との整合性が気になるが、本判決では、一般論として憲法擁護局の諜報・公安的情報収集に具体的疑いの契機を必ずしも必要としないとした上で、[74] 本件授権規定の基本権侵害の強度との比例上、「高められた要請」が当てはまるという構成をとっている（**BVerfGE 120, 274 [330 f.]**）。先にＩＴシステムへの秘密の侵害は従来の通信監視の比ではないと説示した箇所がここで生きてくる。しかしながら、本判決は具体的危険のメルクマールとして①「個別具体事案」、②「危険が損害に転ずる時間的近さ」、③「危険惹起者たる特定人物との関連」の三点をいったん挙げながら、本件のような「予防的な目標設定の領域」で要請されるのは「具体的危険」の存在そのものではなく、特定の事実に支えられた「事実上の手がかり」であり、「危険が直近の将来に（**in näherer Zukunft**）発生する十分な蓋然性」は必要としなかった点で、ラスター捜査決定が打ち出した境界値を緩和する方向を示している。[75] この点、連邦憲法裁がその説示とは実際には異なり、警察の「予防的抑止」と情報機関による諜報活動との機能的性格の違いにやはり配慮したため後者の活動余地をより広く残したと考えるべきか、[76] それとも、本件措置が「極めて重大な法益」の保護を目的とするため反比例公式ないしは「**je-desto**公式」[77] の判断枠組みに照らしてラスター捜査決定における「現在の危険」の内実が緩和されたと見るべきか、本判決の説明のみでは明確ではない。そもそも、ラスター捜査決定以上の「高度なタブー」の設定とも評される[78]「極めて重大な法益」という概念自体が実はさほど明確ではない。「人の健康、生命、自由」が重大な法益であることは否定できないとしても、「人間の存立の基盤」として「生存に関わる公的な配慮施設の本質的部分の機能力」も含まれる

とされており（BVerfGE 128, 274 [328]）、そこでは公共交通や電気・水道供給等が念頭に浮かぶところであるが、単なる器物損壊や威力業務妨害として処理しうる（処理すべき）事案にまで概念が拡大されるおそれを内包した定義であることも注意が必要であろう。[79] 他に、基本法一三条や刑事訴訟法上の「切迫した危険」との概念整序の必要性も指摘されている点も付言しておきたい。[80]

（6）裁判官留保　オンライン捜索を一三条の保護範囲から排除した連邦憲法裁であるが、裁判官留保については一三条並の厳しい条件をオンライン捜索に設定した。このような判断は、前述のレプジウスが指摘するように、客観法的・手続法的なアプローチによる基本権保障にとって重要な意味を持つ。[81] もっとも、電話盗聴や電子通信監視の際の裁判官令状が制度趣旨で期待されているような機能を発揮していない現状もいくつかの実証研究が明らかにしているところであるし、[82] 本判決自身も判決中で住居捜索に関する先例（BVerfGE 103, 142 [152]）を掲げて裁判官留保の運用上の批判の存在を認めてはいる（BVerfGE 128, 274 [332]）。また、本判決の基準に従ってオンライン捜索に裁判官の令状を要件とした場合、現行の裁判官の人員数では対応不可能という現場裁判官からの声もある。[83] こうした実務の現状を踏まえれば、裁判官留保の法令上の明記は基本権保護の条件整備として重要ではあるが、その限界も存在することは――この点はＢＫＡ法改定論議にも当てはまることが――留意が必要であろう。

（7）「オンライン・パトロール」（Online-Streife）と金融取引状況調査の合憲性　本判決の傍論は、「オンライン・パトロール」と呼ばれる捜査官庁・情報収集官庁によるインターネット解析等について、まずＩＴ基本権の保護範囲外であることを確認した上で、基本法一〇条一項の保護に入る通信接続時は別として、又、覆面捜査官類似の手法を用いた場合を別として、情報自己決定権の侵害性も原則として否定している。一方でＩＴシステム内の個人情報とシステムへの信頼性に極めて敏感な姿勢を示した判決が、他方で一般にアクセスできるメーリング・リストやチャッ

ト等における継続的コミュニケーションを、当該コミュニケーション上の人格の本人特定性の不在を理由に保護に値しないと一蹴した点は――評釈での支持もあるとはいえ[84]――違和感の残るところではある[85]。公開されているＨＰや個人ブログ等の単なる閲覧からの情報獲得なら格別、例えばメーリング・リストやチャット・ルームで一般のアクセス者を装い情報を獲得するような場合、当該行為がインターネット上のコミュニケーションの信用性を毀損し、また利用者に（連邦憲法裁が夙に警戒してきたところの）「動揺効果」をもたらすという視点がより強く示される必要があったのではなかろうか。この点は、前出のベッカーも、メーリング・リストのような「古典型」意見交換のみを想定した本判決の認識の不十分さを認め、より参加者の本人特定性が高いFacebookのようなネットワークについては基本権侵害性がより高くなると指摘している[86]。

他方、州憲法擁護法五ａ条に基づく金融取引情報の取得についても――技術的・コスト的な理由から州憲法擁護庁レベルでは実際には実施のハードルの高い「オンライン捜索」の授権ではなく、実は〇六年の法改定の主眼は国内の「テロ」ネットワークの資金流通把握を目的とした、この五ａ条であったと見てもよいのであるが（vgl. LTDrucks 14/2211, S. 15 ff.）――情報自己決定権の侵害と認定した上で、合理性・必要性、規範特定性・規範明確性、狭義の比例原則のいずれも充たすとし、これを憲法上正当化される侵害と認定している。しかし、ここでもインターネットを通じた決済や信用保証の基盤となる銀行口座の「秘密性と完全性」こそＩＴ基本権コンセプトが保障すべきことなのではないのかという疑問が呈されている[87]。いずれにせよ、このような手法で徴取された情報の保存、評価、変更、譲渡については情報自己決定権の保護範囲となるはずである。

4　簡単な小括

これまでの考察から、連邦憲法裁が打ち出したＩＴ基本権の内容と「オンライン捜索」に設定された侵害境界値の構造及びそれらに伴う解釈上・運用上の問題点が確認できた。ＩＴ基本権というコンセプトに対しては、否定的な見方も含めて今後も議論が続くであろう。本稿で指摘したような当該基本権の客観法的性格といったレベルの問題はもとより、より細かい解釈上の課題も残されている[88]。ホフマン＝リーム自身が認めるように[89]連邦憲法裁も本判決ではＩＴ基本権というコンセプトを精密に描き切っておらず、他の基本権解釈の成果を借りつつの試行錯誤段階である（すでに指摘たように、「秘密性と完全性」という発想自体、自己情報決定権、通信の秘密、住居の不可侵という既存の基本権の内実から生まれてきたものであり[90]、又、「オンライン捜索」の侵害境界値［極めて高度な法益に対する具体的危険の事実上の手がかり、核心領域保護、裁判官留保］は、その保護対象外とされたはずの基本法一三条の文法に則って多くが語られている。一〇条との部分的競合も承認されている）。とはいえ、新たな基本権を手がかりにＩＴ化された現代社会が直面する課題に連邦憲法裁が対処しようとした意欲自体は正当に評価されてよいし、新たな基本権コンセプトがひとたび判例上打ち出された以上、この基本権が抱える難点は今後の判例の積み重ねの中で充填又は軌道修正していくのが――こうした精製過程の結果、もともとＩＴシステムという対国家防禦権的な場面としては（少なくとも現在のところ）かなり限定されたものを想定したこの基本権の役割は「名目以上、権利未満[91]」にとどまり、むしろＩＴ保護立法の法整備や私法上の権利救済の場面にその活路を見出すことになる可能性もありうるが――妥当な線といえよう。

これに対して、比例性審査の点では、ラスター捜査決定等の場合と同様、授権規定の合理性・必要性が簡単に承認されており、ＩＴシステムへの秘密の接続という措置を極めて重大な基本権侵害と認定した点との対象が際立ち、合

理性・必要性審査の存在意義自体が問われかねない状況を再認識させるものとなった。また、狭義の比例性検討の中で確認された法治国家的基準、すなわち「極めて高度な法益に対する具体的危険の事実上の手がかり」の存在、核心領域保護、裁判官留保についても、それらが公権力による予防的監視措置に対する大きな歯止めであることは否定しえないにせよ、本章で検討したように、大盗聴判決やラスター判決の基準からの看過できない後退を示している点は正確に見ておく必要がある。

なお、この判決に続いて同年三月一一日に連邦憲法裁第一法廷は、EU指令に基づく電話通信記録保存（BVerfGE 121, 1）と、州警察法における自動車ナンバー標識の自働照合措置（BVerfGE 120, 378）の合憲性についてそれぞれ重要な判断を下しており、本稿第一章で触れた国内治安政策に対する連邦憲法裁判所の姿勢をさらに浮き立たせることになった。しかし、航空安全法判決やラスター捜査決定では憲法政策上の評価が二分されていたのと比較すると、数多い解釈論上・理論上の批判にも関わらず、本判決の結論に対する評価はメディアでも学説でも概ね肯定的であった。これは、問題となった規定が結局は規範特定性・規範明確性で処理できる杜撰な立法として判決以前から違憲の指摘がなされていたことや[92]、包括的な監視国家を連想させる「オンライン捜索」という未知の措置に対する世論一般の警戒感が強かったこと等[93]が要因であろう。ともかく、この判決により、連邦憲法裁は法案提出前のBKA改定法に境界値を示したのであり、このことに対して政治がどのように応答したかについては、章を改めて見ていくことにする。

（続く）

註

（1）「オンライン捜索」については、まず刑事訴訟法の領域で二〇〇〇年前後から法的検討がはじめられていた。z. B. Wolfgang Bär, Durchsuchungen im EDV-Bereich(Ⅰ), (Ⅱ), CR 1995, S. 158 ff., 227 ff.; ders., Polizeilicher Zugriff auf Kriminelle Mailboxen, CR 1995, S.489 ff.; ders., Handbuch zur EDV-Beweissicherung im Strafverfahren, Stuttgart u. a. 2007, Rn. 311－321, 456－475; Mark Alexander Zöller, Verdachtslose Recherchen und Ermittlungen im Internet, GA 2000, S. 563 ff.; Michael Germann, Gefahrenabwehr und Strafverfolgung im Internet, Berlin 2000, insb. S. 282－285, 540－550; Thomas Böckenförde, Die Ermittlung im Netz, Tübingen 2003, S. 209. ff. insb. 219－225; Manfred Hofmann, Die Online-Durchsuchung, NStZ 2005, S. 121 ff. 連邦最高裁決定が出た二〇〇七年には、この年だけでも膨大な文献が出ているが、憲法論又は技術的な観点から特に重要なものとして、Johannes Rux, Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, JZ 2007, S. 285 ff; Ulf Buermeyer, Die „Online-Durchsuchung“. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, S. 154; ders., Die „Online-Durchsuchung“. Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugrffs auf Computersysteme, HRRS 2007, S. 328 ff.; Peter Schanz, Verfassungsrechtliche Problem von „Online-Durchsuchungen“, KritV 2007, S. 310 ff. 他に、Matthias Jahn/Hans Kudlich, Die strafprozessuale Zulässigkeit der Online-Durchsuchung, JR 2007, S. 57 ff.; Martin Kemper, Anforderungen und Inhalt der Online-Durchsuchung bei der Verfolgung von Straftaten, ZüR 2007, S. 105 ff.; Brian Valerius, Ermittlungmaßnahmen in Internet, JR 2007, S. 275 ff.; Charles von Denkowski, „Online-Durchsuchung“, Kriminalistik 2007, S. 177 ff. Ernst Hunsicker, „Online-Durchsuchung“, Kriminalistik 2007, S. 187 ff.; Kai Cornelius, Anmerkung, JZ 2007 S. 798 ff.; Martin Kutscha, Verdeckte „Online-Durchsuchung“ und Univerletzlichkeit der Wohnung, NJW 2007, S. 1169 ff.; Marco Gercke, Heimliche Online-Durchsuchung, CR 2007, S. 245 ff.; Gerrit Horning, Ermächtigungsgrundlage für die „Online-Durchsuchung“?, DuD 2007, S. 575 ff.; Hartmut Pohl, Zur Technik der heimlichen Online-Durchsuchung, DuD 2007, S. 684 ff.; Markus Hansen/Andreas Pfitzmann/Alexander Roßnagel, Online-Durchsuchung, DRiZ 2007, S. 225, 227 ff.; Dirk Fox, Realisierung, Grenzen und Risiken der „Online-Durchsuchung“, DuD 2007, S. 827 ff.

（2）二〇〇八年の連邦憲法裁判決後の膨大な文献の中から、まずは、Fredrik Roggan (Hersg.), Online-Durchsuchungen, Berlin 2008; Thomas Böckenförde, Auf dem Weg zur elektronischen Privatsphäre, JZ 2008, S. 925 ff.; Matthias Bäcker, Die Vertraulichkeit der Internetkommunikation, in: Hartmut Rensen/Stefan Berink (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts, Berlin 2009, S. 99 ff. 等が参照されるべきである。また、Stefan Holzner, Die Online-Durchsuchung, Kenzingen 2009も、諸論点が手際よく整理されており、諸外国の立法動向も含めた問題の把握に便利である。他に判決の評釈類として、Michael Sachs/Thomas Krings, Das neue „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, JuS 2008, S. 481 ff.; Thomas B. Petri, Das Urteil des Bundesverfassungsgerichts zur „Online-Durchsuchung“, DuD 2008, S. 443 ff.; Martin Kutscha, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, S. 1042 ff.; Gerrit Hornung, Ein neues Grundrecht, CR 2008, S. 299 ff.; Rainer Erd, Bundesverfassungsgericht veraus Politik, KJ 2008, S. 198 ff.; Gabriele Britz, Vertraulichkeit und Integrität Informationstechnicher System, DÖV S. 411 ff.; Uwe Volkmann, Anmerkung zum Urteil des BVerfG vom 27.2.2008, DVBl 2008, S. 590 ff.; Burkhard Hirsch, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, NJOZ 2008, S. 1907 ff.; Wolfgang Hoffmann-Riem, Der grundrehtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, S. 1009 ff.; Hartmut Brenneisen u. a., Reaktion auf neuartige Informationseingriffe, Die Polizei 2008, S. 245 ff.; Alexander Roßnagel/Christoph Schnabel, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, S. 3534 ff.; Hans Peter Bull, Meilensteine auf dem Weg des Rechtsstaates, JBÖS 2008/2009, S. 317 ff.; Christoph Gusy, Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, DuD 2009, S. 1 ff.; Michael Klopfer/Florian Schärdel, Grundrechte für die Informationszugangsfreiheit?, JZ 2009, S. 453 ff.; Michael Heise, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, RuP 2009, S. 94 ff.;Dieter Hömig, 》Neues《 Grundrecht, neue Fragen?, JURA 2009, S. 207 ff.

（3）vgl. Pressemitteilung des Bundesministerium des Innern vom 10.11.2006.

（4）PSIS, S. 18. 同プログラムには他に、ドイツ鉄道（DB）の保有する民間警備力との協働、鉄道施設や空港でのビ

デオ監視の強化等も盛り込まれている。

（5） z. B. Pressemitteilung der Fraktion DIE LINKE von 25.10.2006.

（6） z. B. Christian Rath, Die Polizei als Hacker, taz. von 11.12.2006.

（7） vgl.auch Holzner, a. a. O.（Anm. 2）, S. 4.

（8） Petri, a. a. O.（Anm. 2）, S. 443.「オンライン捜索」という用語の不正確さの指摘は、すでにauch Buermeyer, a. a. O.（Anm. 2）, Technischer Hintergrund, S. 154. さらに、T・ベッケンフェルデは、措置の移行段階に順じて、「オンライン侵入」、「オンライン点検」、「オンライン監視」、「オンライン保全」の四概念を区別する（Bäckenförde, a. a. O.［Anm. 2］, S. 929 f.）

（9） 源泉型電子通信監視とは、「暗号化前の送信情報や受信者による暗号平文化後の受信情報を捕捉する監視過程」のことを言う（Hoffmann-Riem, a. a. O.［Anm. 2］, S. 1021）。暗号化又はデジタル化された通信（例えば„Skype“を利用したインターネット通話）では伝達過程での通話捕捉が困難なことから、このような監視手法の必要性が唱えられている（vgl. Buermeyer, a. a. O.［Anm. 1］, Technischer hintergrund, S. 160）。

（10） Bäckenförde, a. a. O.（Anm. 2）, S. 929 f.

（11） 〇八年一月に改定された刑事訴訟法一一〇条三項に基づく電子記録媒体の点検は、秘密性を欠くため、ここでいう「オンライン捜索」の授権規定ではない（vgl. Stephan Schlegel, „Online-Durchsuchung light“, HRRS 2008, S. 26）。

（12） 「トロイの木馬」は、ウィルス・プログラム群「メールウェア」（Malware）の一つである。より多機能性を持つプログラム群「バックドア」（Backdoor）を用いれば、捜査官庁のパソコンからのカメラやマイクロフォンの遠隔操作を通じて捜査対象のパソコンが設置された場所の監視までも可能なため（vgl. Buermeyer, a. a. O.［Anm. 1］, Technischer Hintergrund, S. 155－157）、「オンライン捜索」の批判者は「バックドア」による包括的監視の危険性を指摘するが、さしあたり現実の法政策論議の対象ではない（vgl. Schantz, a. a. O.［Anm. 1］, S. 311）。„Bundes-Trojaner“は、ドイツ語協会選定「二〇〇七年の言葉」第八位に入った（http://www.gfds.de/index.php?id=210）。

（13） vgl. Gercke, a. a. O.（Anm. 1）, 246－248.「オンライン捜索」に関する技術上の基本知識と問題点について、より詳しくは、vgl. z. B. Buermeyer, a. a. O.（Anm. 1）, Technischer Hintergrund, S. 154 ff; Fox, a. a. O.（Anm. 1）,

S. 827 ff.; Markus Hansen/Andreas Pfizmann, Techniken der Online-Durchsuchung, in: Roggan, a. a. O. (Anm. 2), S. 131 ff.; Holzner, a. a. O. (Anm. 2), S. 10－17.

(14) 一〇条二項が予定する法律の根拠による制限の具体化として制定された、「信書、郵便及び電信電話の秘密の制限に関する法律」の略称。通常はさらにG10法と略記される。

(15) この各決定について、vgl. Kundlich, a. a. O. (Anm. 1), S. 57.

(16) vgl. Gercke, a. a. O. (Anm. 1), S. 246. auch Peter Schaar, Das Ende der Privatsphäre, München 2007, S. 122 f. ショイブレ自身は、最高裁の判断は国内治安法制のあり方を世論、議会、政府に委ねたという点で「驚くほどのことではなく」、「民主主義の理論上はポジティブなもの」と述べている（Wolfgang Schäuble, Aktuelle Sicherheitspolitik im Lichte des Verfassungsrechts, ZRP 2007, S. 210)。「オンライン捜索」の必要性を強調する一方、具体的危険の要件を求める比較的バランスのとれた推進論として、Denkowski, a. a. O. (Anm. 1), S. 180 f.

(17) vgl. Hirsch, a. a. O. (Anm. 2), S. 1908. この点は、本件憲法異議の口頭弁論の場でBKA長官J・ツィールケとBVfS長官H・フロムが自ら証言している（BVerfGE 120, 274 [276])。

(18) vgl. auch Hunsicker, a. a. O. (Anm. 1), S. 186.

(19) Rede der Bundesministerin der Justiz, Brigtte Zypries MdB beim 10. Europäischen Polizeikongress am 13. Febuar 2007 in Berlin. 演説の全文は連邦司法省のウェッブサイト（http://www.bmj.de）にアップされている。連立政権内でのツェプリースの抵抗について、vgl. auch Der Spiegel vom 28.7.2008, S. 32 ff. しかしこの記事は、彼女がシュレーダー政権下の内務政務次官として「テロ」対策法制定に関わった事実の指摘も忘れていない。

(20) vgl. z. B. Fox, a. a. O. (Anm. 1), S 833 f.

(21) Hansen/Pfitzmann/Roßnagel, a. a. O. (Anm. 1), S. 228.

(22) vgl. Erd, a. a. O. (Anm. 2), S. 120－123.

(23) vgl. FAZ. NET vom 27.7.2007. vgl. auch. FAZ. NET vom 29.7.2007.

(24) FAZ. NET vom 11.10.2007も、この憲法異議をショイブレ案をめぐる前哨戦と位置づける。

(25) この模様について、vgl. FAZ. NET vom 11.10.2007.

(26) Horning, a. a. O. (Anm. 2), S. 299 f.

(27) 本稿で考察した当該基本権の性格を鑑みると、「IT基本権」(IT-Grundrecht) 又は「コンピュータ基本権」(Computer-Grundrecht) という略称が適切かという逡巡は残るが、さしあたり本稿では、以下引用文中以外「IT基本権」と略記する。

(28) Böckenförde, a. a. O. (Anm. 2), S. 928.

(29) vgl. auch Backer, a. a. O. (Anm. 1), S. 125; Hoffman-Riem, a. a. O. (Anm. 1), S. 12; Hornung, a. a. O. (Anm. 1), S. 303. また、M・ハンゼン＝A・フィッツマンは、「情報が完全、正確及びアクチャルなものであること、又はそのような状態でないと明確に認識しうること」を「完全性」と呼んでいる (Hansen/Pfizmann, a. a. O. [Anm. 13], S. 132)。本稿では、このような概念定義をめぐる議論を参考に、„Vertraulichkeit und Integrität“に「秘密性と完全性」という訳語をさしあたり充てている。なお、かかる意味での「完全性」は、システム内のデータ保護の付随的効果としてもたらされるものであり、独自の保護法益とするのは不適切であると批判する訴訟もある (Eifelt, a. a. O. [Anm. 2], S. 522)。

(30) 申立人Ⅰの異議申立理由書は人権擁護団体Humanistische UnionのHP (http://www.humanistische-union.de)、申立人Ⅱの異議申立理由書はO・バウムのHP (http://www.gerhart-baum.de) にそれぞれアップされている。もっとも、ツュブリース連邦法相が判決直前に「デジタル化された生活領域用に裁断された具体的な基本権」の必要性を語っているなど (FAZ vom 31.1.2008)、こうした基本権登場の土壌は存在したと思われる。

(31) とくに基本法一〇条一項の通信の秘密 [Fernmeldegeheimnis] について、通信内容や通信状態のVertraulichkeitが語られ (z. B. BVerfGE 107, 229 [313]; 115, 166 [183])、公権力による通信監視とその記録が「コミュニケーション交換の率直性や電子通信設備の非侵入性 (Unzugänglichkeit) の保護への信用を著しく脅かす」(BverfGE 107, 299 [320]. 傍点は筆者) ことが認識されてきた。一三条一項についても、住居の「秘密性」や「完全性」が文献の中で語られてきた (z. B. Schanz, a. a. O. [Anm. 1], S. 317; Gercke, a. a. O. [Anm. 1], S. 250)。Britz, a. a. O. (Anm. 2), S. 412の見方も本稿の分析を裏づけている。また、その意味では、Schanz, a. a. O. (Anm. 1), S. 315 f. の指摘 (とくに、「市民が自己のパソコンに保存されたデータを自分だけが利用で来、かつ秘密性があるという点を

根拠をもって信用できる」という一文など）も本判決の問題認識を先取りしている。

(32) Schantz, a. a. O. (Anm. 1), S. 313－321; Hornung, a. a. O. (Anm. 1), S. 577 f.; Rux, a. a. O. (Anm. 1), S. 292－295; Valerius, a. a. O. (Anm. 1), S. 279 f.; Bär, a. a. O. (Anm. 1), Handbuch zur EDV-Beweissicherung, Rn. 467. U・ブエルマイアーは、一〇条一項の保護範囲となる源泉型電子通信監視を除いた住居内にあるITシステムへの侵入を一三条一項の保護範囲とした上で、同条四項の場合に、かつ私生活形成の核心領域の保護の下でのみ認める（Buermeyer, a. a. O. [Anm. 1], Verfassungsrechtliche Grenzen, S. 332－337)。

(33) 一九九八年の基本法一三条改定の際に当初案に存在した憲法擁護機関に関する特別規定を削除した立法者意思を根拠に、情報機関による住居監視をそもそも違憲と解する見解として、Manfred Baldus, Präventive Wohnraumüberwachungen durch Verfassungsschutzbehörden der Länder, NZwZ 2003, S. 1292 f.

(34) Oliver Lepsius, Das Computer-Grundrecht, in: Roggan, a. a. O. [Anm. 2], S. 23. さらに、P・シャンツは、「オンライン捜索」導入のための一三条改定が基本法改定の限界内にとどまりうるか疑問を呈する（Schantz, a. a. O. [Anm. 1], S. 321)。

(35) z. B. Böckenförde, a. a. O. (Anm. 1), S. 323 f.; ders., a. a. O. (Anm. 2), S. 926.; Kutscha, a. a. O. (Anm. 1), S. 1170 f.; Gercke, a. a. O. (Anm. 1), S. 250. 個人は不正侵入のリスク覚悟でオンラインに自己のパソコンに接続した時点で自覚的に基本権保護を放棄したとみなし、侵害強度を低く捉える説もある（Hofmann, a. a. O. [Anm.1], S. 124)。

(36) NRW憲法擁護法改定の州議会の審議でも、この点が争点となった（vgl. Kutscha, a. a. O. [Anm. 1], S. 1169. vgl auch Rux, a. a. O. [Anm. 1], S. 292. Fn. 45)。

(37) Zypries, a. a. O.

(38) z. B. Kutscha, a. a. O. (Anm. 1), S. 1170 f.

(39) Britz, a. a. O. (Anm. 1), S. 42.

(40) Hornung, a. a. O. (Anm. 2), S. 301.

(41) vgl. Lepsius, a. a. O. (Anm. 33), S. 26.

(42) z. B. Schantz, a. a. O. (Anm. 1), S. 322 f.; Buemeyer, a. a. O. (Anm. 1), Verfassungsrechtliche Grenzen, S. 330.

(43) Hoffmann-Riem, a. a. O. (Anm. 2), S. 1021 f. Bäcker, a. a. O. (Anm. 2), S. 130－132は，判決の示したIT基本権と基本法一〇条との競合を一部の判例評釈は見落としている，と批判する。

(44) Britz, a. a. O. (Anm. 2), S. 414. auch Bull, a. a. O. (Anm. 2), S. 324.

(45) Lepsius, a. a. O. (Anm. 33), S. 30. auch Britz, a. a. O. (Anm. 2), S. 413 f.; Horning, a. a. O. (Anm. 2), S. 301 f.; Bull, a. a. O. (Anm. 2), S. 319 f.; Sachs/Krings, a. a. O. (Anm. 2), S. 483; Eifert, a. a. O. (Anm. 2), S. 522; Volkmann, a. a. O. (Anm. 2), S. 591 f.

(46) もっとも，本判決から一二日後の三月一一日の判決（BVerfGE 120, 378）では，連邦憲法裁第一法廷は情報自己決定権を手がかりに，自動車ナンバー標識の自動認識装置による情報徴取・照合措置を授権したヘッセンとシュレスビッヒ＝ホルシュタインの州警察法の規定を違憲と判断しており，連邦憲法裁が自己決定権の射程限定の方向に舵を切ったとは直ちには言えない。近時の判例動向は，vgl. Walter Frenz, Informationelle Selbstbestimmung im Spiegel des Bverf G, DVBl 2009, S. 333 ff.

(47) Hoffmann-Riem, a. a. O. (Anm. 2), S. 1009 ff.; Bäcker, a. a. O. (Anm. 2), S. 99 ff.

(48) Wolfgang Hoffmann-Riem, Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 1998, S. 520 f. 情報自己決定権論の到達点を確認するには，ホフマン＝リーム以上に社会依存的性格や客観法的側面を重視するM・アルベルスの近時の業績（Marion Albers, Informationelle Selbstbestimmung, Baden-Baden 2005; ders., Umgang mit personenbezogenen Informationen und Daten,in: Wolofgang Hoffmann-Riem/Eberhard Schmidt-Aßmann/Andreas Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band 2, München 2008）が参照されるべきである。

(49) IT基本権と情報自己決定権との関係を特別法と一般法の関係という意味での「補充性」の関係で捉える一部の評釈の理解（z. B. Petri, a. a. O. [Anm. 2], S. 444）に対して，ホフマン＝リームはIT基本権と情報自己決定権の並立という捉え方を鮮明にしている（Hoffmann-Riem, a. a. O. [Anm. 2], S. 1019）。補充性を語りうるとすれば，通信の秘密との関係の方である（vgl. Bäcker, a. a. O. [Anm. 2], S. 131）。

(50) Bäcker, a. a. O. (Anm. 2), S. 124.

(51) Böckenförde, a. a. O. (Anm. 2), S. 928.

(52) Karl-Heinz Ladeur, Das Recht auf informationelle Selbstbestimmung, DÖV 2009, S. 45 ff.

(53) Lepsius, a. a. O. (Anm. 34), S. 41.

(54) 枚挙に暇がないが、vgl. z. B. Hans Dieter Jarass, Grundrechte als Wertentscheidungen bzw. objektivrechtliche Prinzipien in der Rechtssprechung des Bundesverfassungsgerichts, AöR 1985, S. 363 ff. 全九巻予定で現在順次刊行中のD・メルテン＝H―J・パピーア編『基本権要綱』では、R・ヴァールが、比較法的観点からドイツ圏の客観法的志向を浮き立たせる整理を行っている（Rainer Wahl, Die objektiv-rechtliche Dimension der Grundrechte im internationalen Vergleich, in: Detlef Merten/Hans-Jürgen Papier (Hrsg.), Handbuch der Grundrechte in Deutschland und Europa, Bd. 1, Heidelberg 2004, S. 745 ff.

(55) Petri, a. a. O. (Anm. 2), S. 446 f.; Sachs/Krings, a. a. O. (Anm. 2), S. 486.

(56) 私法上の影響への言及は、Gusy, a. a. O. (Anm. 2), S. 39; Roßnagel/Schnabel, a. a. O. (Anm. 2), S. 3534 ff. Klopfer/Schärdel, a. a. O. (Anm. 2), S. 453 ff. は、同盟90／緑の党提出のデータ保護法案を中心に判決のデータ保護法制への影響を検討する。vgl. auch, Renate Künast, „Meine Daten Gehören mir“, ZRP 2008, S. 201 ff.

(57) Lepsius, a. a. O. (Anm. 34), S. 48－54.

(58) Lepsius, a. a. O. (Anm. 34), S. 49. そこでは、現代治安法制がもたらす現象として、①措置対象者が実態把握できないことによる裁判的救済の困難を補うコントロール手段（議会の統制委員会や裁判官留保等）の必要性、②従来の措置と違い市民の行動変更を目標としない、むしろ市民が行動を変えないことが意味を持つ監視措置、③潜在的に監視されているという感情がもたらす社会全体規模の動揺効果、④監視技術の進歩に伴う人格プロフィールの把握を可能にするデータの統合化効果（summierender Effekt）が指摘されている（ebenda, S. 49－51)。レプジウスの所論について詳しくは、vgl. Oliver Lepsius, Freiheit, Sicherheit und Terror, Leviathan 2004, S. 64 ff., insb. S. 82 f. 講演録として、オリバー・レプジウス（河村憲明訳）「自由・安全・テロリズム」警察学論集五八巻六号（二〇〇五年）一二四頁以下とくに三二―三八頁。リスク配慮行政一般についても、vgl. ders., Riskosteuerung durch Verwaltungsrecht,

VVDStL 63, 2004, S. 283－290.

(59) Lepsius, a. a. O. (Anm. 34), S. 42－47. この方向を唱導する論者こそ他ならぬホフマン－リームである。vgl. z. B. Wolfgang Hoffmann-Riem, Enge oder Weite Gewährleistungsgehalte der Grundrechte?, in: Michael Bäuerle (Hrsg.), Haben wir wirklich Recht?, Baden-Baden 2004, S. 53 ff. insb. 63. 関連して vgl. Enrst-Wolfgang Böckenförde, Schutzbereich, Eingriff, verfassungsimmanente Schranken, Der Staat 2003, S. 165 ff. 議論状況の概観は vgl. Uwe Vollkmann, Veränderungen der Grundrechtsdogmatik, JZ 2005, S. 261 ff. すでに日本でも 小貫幸浩「基本権が『保障するもの』は何か・続」高岡法学一六巻一・二号（二〇〇五年）一頁以下 丸山敦祐「情報提供活動の合憲性判断とその論証構造」阪大法学五五巻五号（二〇〇六年）一一二頁以下 における紹介・検討がある。

(60) グレゴール決定については 丸山敦裕「市場競争に影響ある情報の国による公表」ドイツ憲法判例研究会編『ドイツの憲法判例Ⅲ』（信山社・二〇〇九年）所収二九二頁以下 オショー決定については 西原博史「政府の情報提供活動における〈警告〉と信教の自由の保障」同書所収一一七頁以下 参照。

(61) 「新傾向」を明確に批判した論考として Wolfgang Kahl, Vom weiten Schutzbereich zum engen Gewährleistungsgehalt, Der Staat 2004, S. 167 ff. このカールの批判に対するホフマン－リームの反論は Wolfgang Hoffmann-Riem, Grundrechtsanwendung unter Rationaltätsanspruch, Der Staat 2004, S. 203 ff. 小貫・前掲註（59）の紹介が詳しい。

(62) Lepsius, a. a. O. (Anm. 34), S. 54.

(63) Hoffmann-Riem, a. a. O. (Anm. 2), S. 1064, Fn. 62; Bäcker, a. a. O. (Anm. 2), S. 125 f., Fn. 114, S. 128. auch Böckenförde, a. a. O. (Anm. 2), S. 928, Fn. 39, Hömig, a. a. O. (Anm. 2), S. 209 f. その是非はともかく「保護範囲から保障内容へ」という「新傾向」が主に信教の自由や職業の自由の判例に即して議論されてきたことからすれば 本判決に「新傾向」の特徴を見出すためには 詳しい説明が求められよう。

(64) auch Ladeur, a. a. O. (Anm. 52), S. 54 f.

(65) 連邦憲法裁の規範特定性・規範明確性の法理の概観は vgl. Roberto Bartone, Gedanken zu den Grundsätzen der Normenklarheit und der Normenbestimmtheit als Ausprägungen des Rechtsstaatsprinzips, in: Rensen/Berink, a. a. O. (Anm. 2), S. 305 ff. さらに規範真実性（Normenwahrheit）という「第三の」概念への近時の関心について vgl. z. B.

Stephan Meyer, Die Verfassungswidrigkeit symbolischer und ungeeigneter Gesetze, Der Staat 2009, S. 278 ff.; Klaus-Dieter Drüen, Normenwahrheit als Verfassungspflicht?, ZG 2009, S. 60 ff.

(66) 西原博史「リスク社会・予防原則・比例原則」ジュリスト一三五六号（二〇〇八年）八〇―八一頁。小山剛「自由・テロ・安全」大沢秀介・小山剛編著『市民生活の自由と安全』（成文堂・二〇〇六年）所収三三六頁も参照。

(67) Hans-Heinrich Trute, Grenzen des Präventionsorientierten Polizeirechts in der Rechtsprechung des Bundesverfassungsgerichts, Die Verwaltung 2009, S. 88－93.

(68) この点につき、さしあたり、根森健「人格権の保護と『領域理論』の現在」時岡弘先生古稀『人権と憲法裁判』（成文堂・一九九二年）七五頁以下、同「日記類似の個人的な手記の刑事手続での利用と一般的人格権」ドイツ憲法判例研究会編『ドイツの憲法判例Ⅱ（第二版）』（信山社・二〇〇六年）二五頁以下、参照。

(69) そこでは、「知覚や感情のような内心の出来事、並びに、高度に個人的な性質を持つ考えたこと、見たこと、及び体験したことが、とりわけ国家的機関の監視の下にあるという不安無しに、表現される可能性」が核心領域に含まれるとされている（BVerfGE 109, 275 [313]）。憲法改定の限界論にまで射程の及ぶ大盗聴判決の検討は、基本法や刑事訴訟法のコンメンタール内での言及も含めて膨大であるが、まずは、vgl. Fredrik Roggan (Hrsg.), Lauschen im Rechtsstaat, Berlin 2004. 他に、vgl. z. B. Erhar Denninger, Verfassungsrechtliche Grenzen des Lauschens, S. 101 ff.; Christoph Gusy, Lauschangriff und Grundgesetz, JuS 2004, S. 457 ff. 邦語文献として、平松毅「住居に対する高性能盗聴による盗聴」ドイツ憲法判例研究会・前掲書註（60）三二〇頁以下、小山・前掲註（66）二〇五頁以下、等がある。

(70) 大盗聴判決の核心領域論への批判として、vgl. z. B. Manfred Baldus, Der Kernbereich privater Lebensgestaltung, JZ 2009, S. 218 ff.; Ralf Poscher, Menschenwürde und Kernbereichsschutz, JZ 2009, S. 272 f.

(71) この点も含め本判決の核心領域論に対する詳しい批判は、Maximilian Warntjen, Der Kernbereichsschutz nach dem Online-Durchsuchungsurteil, in: Roggan, a. a. O. (Anm. 2), S. 57 ff.

(72) 本判決の二段階コンセプトは、「絶対的な保護」を要請しながら、この保護が守られないことを「不可避」と見る大盗聴判決の矛盾をより鮮明なものにした（vgl. Warntjen, a. a. O. [Anm. 71], S. 61－63; Poscher, a. a. O. [Anm. 70], S. 272 f.）。R・ポシャーは、絶対的保護の対象を住居内の出来事に限定し、外部の会話や覆面捜査官や捜査協

力者を利用した情報収集措置を範囲外に置いてきた連邦憲法裁の核心領域論を「空間的思考」と位置づけ、そのことがもたらす基本権保護の空洞化を批判する。人間の尊厳や人格発展に重大な関わりを持つ親密な会話は常に住居の中でのみなされるわけではない（時にはその外でこそなされる）からである。したがって彼は立法論として、警察法において核心領域の保護を一般条項として設けることを推奨する（ebenda, S. 269 ff. vgl.auch Christian Stark, Das neue Recht polizeilicher Datenerhebung und -verarbeitung in Niedersachsen, NdsVBl 2009, S. 145 ff. insb. 148）。近時の学説では核心領域論批判が勢いを得ているが、一部の批判論の背後には連邦憲法裁の「人間の尊厳」（基本法一条一項）の援用の仕方への批判、より具体的には航空安全法判決法理の見直し論や拷問禁止原則の緩和論と連動しているため（vgl. Poscher, ebenda, S. 274）、その全体的な評価は解釈論上のそれとは別の目配せも必要と思われる。拷問禁止原則のゆらぎについては、玉蟲由樹「人間の尊厳と拷問の禁止」上智法学論集五二巻一・二号（二〇〇八年）二二五頁以下、も参照。

（73） Hornung, a. a. O.（Anm. 2）, S. 304.

（74） このくだり（BVerfGE 120, 274［330］）では、「新たな警察法（学）」を提唱するM・メストルの二〇〇七年の論文とU・フォルクマンによるラスター捜査決定への批判的評釈の参照を請う余裕を連邦憲法裁は見せている。

（75） この点の批判として、z. B. Kutscha, a. a. O.（Anm. 2）, S 1043 f. M・メストルは、BKA改定法に関する連邦議会内務委員会専門家公聴会の場で、連邦憲法裁はオンライン捜索に具体的危険は必要としないと認めたのだと、一般的な判例理解とは異なる見解を示しているが（BT-Drucks. 16/9588, S. 21 f.）、判決には危険概念に関する用語使用の若干の混乱もみられ（vgl. Britz, a. a. O.［Anm. 1］, S. 415）、このような読み方を可能にする余地を含んでいる。しかしT・ベッケンフェルデは、いずれにせよ本判決の示した「新たな危険概念」の下でも刑事訴追や警察の予防的抑止としてのオンライン捜索は可能でも、憲法擁護局が諜報活動のために用いるのは困難であり（判決は、「危険前段階で活動する官庁仕様にした侵害のきっかけのための法律上の基準を、基本権への脅威の重大さと強度を例えば警察法における伝統的な危険概念が果たしてきたのと同程度に考慮に入れるようなかたちで産み出すことなど成功するはずがないとしても」、憲法上の要請が緩和されることはないと述べている[BVerfGE 120, 274［331］]、メストルが主張する国家の危険前段階的活動に対する危険概念の再構成をもたらすほどの修正ではないと見る（Bäckenförde, a. a. O.［Anm.

2], S. 931)。

(76) vgl. Roggan, Präventive Online-Durchsuchungen, in: Roggan, a. a. O. (Anm. 2), S. 103－105.

(77) この訳語の使い分けの合意については、本稿第二章4（2）参照。

(78) Bäckenförde, a. a. O. (Anm. 2), S. 931.

(79) この点を鋭く指摘したものとして、Lepsius, a. a. O. (Anm. 34), S. 39 f.

(80) Britz, a. a. O. (Anm. 2), S. 415. 重大な法益への損害発生十分な蓋然性が条件とされる（vgl. z. B. Gilbert Gornign, Art. 13, in: Starck/Mangolt/Klein [Hrsg.], Kommentar zum Grundgesetz, Bd. 1, 5. Aufl., München 2005, Rn. 71）「切迫した危険」は加重された危険概念の類型に入るが、C・グズィの警察法教科書では、「切迫した危険」を官庁間の権限移譲に用いられる概念とし、本来の管轄機関による防除が不可能又は直ちには不可能と思われる場合に危険が「切迫」していると説明されている（Christoph Gusy, Polizei- und Ordnungsrecht, Tübingen 2009, Rn. 129)。両概念の事実上の差は少ないとする見解もある（Hornung, a. a. O. [Anm. 2], S. 304)。

(81) 裁判官留保制度の法治国家的意義と法状況については、vgl. Tjark Erich Aschmann, Der Richtervorbehalt im deutschen Polizeirecht, Würzberg 1999.

(82) z. B. Chrisiane Kürpe-Gescher, Die Überwachung der Telekommunikation nach den §§100a,100b StOP in Rechtspraxis, Berlin 2005; Otto Backes/Christoph Gusy, Wer kontrolliert die Telefonüberwachung?, Frankfurt. a. M. u. a. 2003. この点は、Georg Hermes, Art. 13, in: Horst Dreier, Grundgesetz Kommentar, Bd. 1, 2. Aufl., Tübingen 2004, Rn. 31でも指摘されている。もっとも、そこで指摘されている令状運用の実態は日本の刑事手続の実態を知る者にとっては特段驚くべきことではない。

(83) ドイツ裁判官連盟（DRB）議長C・フランクの見解はheise onlineの配信記事（http://www.heise.de/newsticker/Richter-halten-Kontrolle-von-heimlichen-Online-Durchsuchungen-fuer-illusorisch--/meldung/104238）を参照。

(84) Böckenförde, a. a. O. (Anm. 2), S. 935; Sachs/Krings, a. a. O. (Anm. 2), S. 482.

(85) vgl. Eifert, a. a. O. (Anm. 2), S. 522; Hornung, a. a. O. (Anm. 2), S. 305.

(86) Bäcker, a. a. O. (Anm. 2), S. 133－135. M・アイフェルトは、チャット等での公権力の覆面的アクセスを意見

表明の自由（基本法五条一項）に対する国家の中立性の問題としても捉えている（Eifert, a. a. O. [Anm. 2], S. 522）。

(87) Kutscha, a. a. O. (Anm. 2), S. 1043.

(88) 例えば、ある評者たちは、判決が「秘密性への利益」と「秘密性の期待」を互換的に用いることに起因する保護に値する利益の輪郭の不明確さを指摘する（Sachs/Krings, a. a. O. [Anm. 2], S. 484）。今後の事案の中で、こうした点も詰められる必要がある。

(89) Hoffmann-Riem, a. a. O. (Anm. 2), S. 1019.

(90) 註（80）で紹介したホーヌング説のように「切迫した危険」と「具体的危険」の内実はそれほど変らないと解すればなおさらである。一二条の基本権保護装置とIT基本権のそれとの近似性の指摘は、Britz, a. a. O. (Anm. 2), S. 415. 一二条保護範囲否定説のM・ベッカーも、住居という「壁」の秘密性（親密性）とITシステムというバーチャルな空間内の利用者のそれとをパラレルで捉えられている（Bäcker, a. a. O. [Anm. 2], S. 119）。

(91) Gusy, a. a. O. (Anm. 2), S. 38 f.

(92) z. B. Rux, a. a. O. (Anm. 1), S. 291－295. 本件憲法異議の口頭弁論ではH―J・パピーア裁判長が厳しい口調で州政府代理人説明を求めた模様がメディアでも報じられており（FAZ. NET Vom 11.10.2007）、レプジウスは、違憲判決は予想できたと述べている（Lepsius, a. a. O. [Anm. 36], S. 21）。

(93) SZ紙での司法問題に関する鋭い論説で鳴らし、シュレーダー前連邦首相をして「連邦憲法裁判所第三法廷」と言わせしめたH・プラントルの近著は、こう説明する。数々の治安立法制定の際に見られたそれをはるかに凌ぐ「オンライン捜索」への抵抗感は、「官憲国家アレルギーというよりは、法治国家的センシビリティの再覚醒の問題である。PCは電話よりも、もしかしたら寝室よりも、はるかに国家とは関わりのないプライバシーの真髄と見なされている。ことが個人のパソコンの話となれば、それ以外の場面で悪名に近いものになっていたデータ保護というものに対するセンシビリティが目を醒ますのだ」と（Heribert Prantl, Der Terrorist als Gesetzgeber, München 2008, S. 112 f.）。

付記

本稿は、島大法学五二巻三・四号掲載分にて言及したとおり、筆者のビーレフェルト大学（ドイツ連邦共和国）での在外研修期間中（二〇〇八年一〇月～二〇〇九年九月）に構想・執筆されたものであるが、本号掲載分の校正作業は帰国後となり、この段階で本稿が取り上げたドイツの動向を扱う日本の最新文献にも接することができた。本稿が紹介する立法・判例動向の少なからぬ部分は、これらの文献の中で、すでに（且つ本稿よりも精緻なかたちで）紹介され、もはや周知の事実となっている事柄も多いと思われる。にもかかわらず、本稿には、問題意識、考察方法、分析結果の点で、これら先行業績と異なる独自の意義がなおも存在すると思われるため、叙述における重複箇所の存在を承知で、本稿を公表するものである。以下、これら先行業績を掲げさせていただくことで、執筆者各氏のご寛恕を請いたいと思う。

まず、本稿第一章で触れた基本法七三条一項九a号挿入とその問題点については、上代庸平「テロ対策権限の垂直的配分」大沢秀介・小山剛『自由と安全』（尚学社・二〇〇九年七月）所収二三八頁以下、において詳しく紹介されている。

第二章で扱った連邦憲法裁判所ラスター捜査決定については、徳本広孝「網目スクリーン捜査の法的統制」渥美東洋『犯罪予防の法理』（成文堂・二〇〇八年一二月）所収二九一頁以下、島田茂「ドイツ警察法における犯罪予防の目的と危険概念の関係」甲南法学四九巻三・四号（二〇〇九年三月）一頁以下、宮地基「安全と自由をめぐる一視角」法政論集二三〇号（二〇〇九年六月）三三五頁以下、がそれぞれ本格的な考察を行なっている。

第三章（本号掲載分）の「オンライン捜索」判決については、石村修「ドイツ―オンライン判決」大沢・小山編前掲書所収二六一頁以下、島田茂「予防的警察措置の法的統制と比例原則の適用」甲南法学五〇巻一号（二〇〇九年九月）七二頁以下（とりわけ、この島田論文は多くの重要な指摘を含んでいると思われる）、がある。

なお、〇八年のＢＫＡ法改定問題についても、島田・同右や上代論文で触れられている。この問題を扱う本稿第四章（島大法学五二巻三号掲載予定分）では、これらからの示唆を本文中に反映させたい。