◇資　料◇

# データ保護の新たな構想

## ――インターネットの挑戦――

アレクサンダー・ロスナゲル*
米丸恒治（訳）

### 一　古くからの目標――新たな道

最近、インターネットの幅広い利用によって、データ保護が新たな挑戦の前に立たされていることがはっきりしてきている。第一に、インターネットによって、毎日の行動、考え方および選好についての多くの市民の個人関連データが、ドラスティックに収集される可能性が増大している。第二に、インターネットによって、何人も情報およびデータ処理の可能性を世界的に入手しうるものとなっている。集積されたデータの全部を瞬時に地球のいたるところに移動させあるいは呼び出すことができる。インターネットでは、国境のコントロールがない。データ処理は、ひとつのデータ処理装置の中で行われるのではなく、ネットの中で、多数の関係者によって行われる。誰が、どこで、どの個人関連データを処理し、処理させるのかは、もはや一国民国家によってはコントロールすることはできない。なるほど、データ処理者が、ドイツにその所在を有するときは、ドイツ連邦共和国のデータ保護法が適用される。[1] しかしインターネットを通じて外国から行動しているデータ処理者に対しては、ドイツのデータ保護法は、無力である。[2]

こうした新たな挑戦は、これまでのデータ保護法を古びたもののように思わせる。ドイツ連邦共和国の憲法である基本法は、なるほどあらゆる市民に対して情報の自己決定を求める基本権を保障している。[3] 原則として、市民は、自己に関するデータが他人によって収集、利用されてよいかどうか、どのデータをそうされてもよいかについて決定することができるものでなければならない。しかし、連邦データ保護法によって保障されることができるこの自己決定権は、ますます少なくなってきている。

しかしまさにこの目的のために、この法律は、一九七八年に施行された。これは、個人関連データを処理することの原則禁止を定めている。例外は、関係者が同意し、または法令がそれを許容しているときにのみ存在する。データの利用は、同意の中で、または法令の中で列挙された目的に拘束される。関係者は、告知、訂正、停止または削除を求める権利を有する。データ処理者は、国家の行政庁により監督されるものとされている。この古くからのデータ保護法は、ひとつの責任あるデータ処理機関がひとつの中央データ処理装置で処理しまたはかかる機関に伝達される個人関連データのファイルに即して作り上げられている。このデータ保護の構想は、七〇年代において、中央の国家的な大型計算機のパラダイムによって開発されてきたのである。今日においてもなおこの形式で処理される限りでは、それもなお利用可能なものであり続ける。しかし個人関連データが、世界的なデータ・ネットの中で、多数の関係者により、中央の統括的な監督の可能性なしに処理される限りで、この構想は時代遅れのものとなり、そして新たな構想により補完または代替されるべきなのである。

### 二　答としてのテレサービスデータ保護法

立法者は、インターネットによる新たな挑戦をうけとめて、テレサービスデータ保護法（ＴＤＤＳＧ）の形式で答を出した。[4] この法律は、一九九七年八月一日に施行された。[5] これは、インターネット上のサービスに適用される特別領域の法律である。

ＴＤＤＳＧは、一方で、データ保護の実証された諸原則を新たな技術的発展に適合させようとし、他方では、はじめて、自己によるデータ保護（Selbstdatenschutz）およびシステム的なデータ保護（Systemdatenschutz）という新たな手がかりを実施にうつそうとする。次のようなこれまでに実証された諸原則は、インターネット上のサービスにも妥当する。

・許可留保：同意または法令に基づいてのみのデータ利用（ＴＤＤＳＧ三条一項）。新しい点は、ＴＤＤＳＧ三条七項により電子的にも同意を与えることができるという点である。[6]

・目的拘束：許容された目的のためだけのデータ利用。新しい点は、例えば、利用データ（利用に関するデータ）は、利

用の後ただちに消去しなければならないというＴＤＤＳＧ四条二項の命令、およびＴＤＤＳＧ四条四項の、個人関連のプロファイルを作成することの禁止である。

・透明性：データ利用についての関係者への教示および保存されたデータの閲覧権。新しい点は、たとえば、ＴＤＤＳＧ七条で保障された、サービスプロバイダのもとにおいて無償で、オンラインで、保存されたデータの閲覧をする権利である。(7)

## 三　新たなデータ保護の構想

しかし、技術の発展とその世界的な利用によって、補完的に新たなデータ保護の構想を必要とする二つの挑戦がつきつけられている。

第一に、新たな構想は、ダイナミックな技術発展が―それはおそらくもっと根本的かつ急速なものとなろうが―さらに続くということを考慮しなければならない。したがって個別の専門的な問題にばらばらな答を出しては、十分ではない。むしろ構造的な解決が必要である。必要なのは、継続的に変化する挑戦に対して繰返し新たな答を出すことのできる、学習能力のあるシステムを構築することである。したがって、データ保護は、



技術の中に組み込まれなければならない。

第二に、新たなデータ保護の構想は、国民国家の規律力が、そしてまたヨーロッパ連合の規律力も、グローバルなデータ・ネットワークに対しては限界があるということを受け入れなければならない。人格の保護のための中央の国家的な基準と、独立の国家的な機関によるその統制は、今後ともさらに不可欠であり続けるが、しかし将来的な課題に対してはますます適合しなくなる。したがって、関係者は、自らを保護することのできる状態におかれなければならない。

この挑戦に基づいて、三つの新たなデータ保護の構想が追求されるべきである。

### 三・一　技術によるデータ保護

技術は、データ保護の敵対者としてだけではなく、その補助者としても見なされるべきである。(8) データ保護が、国家の立法者の影響が及ぶ範囲から離れれば離れるほど、データ保護は、ますます世界的に有効にならなければならない。このことは、有効な世界法秩序がないために、データ保護が技術の中に組み込まれたときにのみ可能である。この方法は、二つのメリットをもつ。データ保護技術が、―データ保護法と異なり―世界的に有効であり、技術企業が、―立法者と異なり―極めて迅速に学習するシステムそのものであることである。

この二つのメリットは、データ保護技術に関して市場を発展させることに成功したときに、利用し得る。(9) データ保護技術が販売されるときは、それは、データ保護に対する新たな技術的挑戦と同様にダイナミックに発展するであろう。この点に関する好例は、暗号ソフトウェアおよびセキュリティーサービスに関する急速に発展する市場である。法的な要求事項は、技術的な解決を刺激し、それに市場を創造する。なぜなら、少なくとも法律の適用領域においては、個人関連データを利用するすべての者がデータ保護技術を必要とするからである。さらに、国家は、かかる発展を支えるために、適合的な大綱条件を設定し、対応する研究を促進することができる。

技術的なデータ保護は、純粋に法的なデータ保護よりもずっと効果的でもある。技術的に妨害されまたは阻止されることのできることは、もはや禁止する必要はない。行動規律には違反することができるが、技術システムの技術的な限界には違反することはできない。データ保護技術は、統制と罰則の機能を行うことができるのであり、刑罰を不要のものとすることができる。





ＴＤＤＳＧ三条ないし六条は、はじめて、サービスプロバイダによる技術構成に目標を定めている。法律は、否定的な技術結果を緩和することに限定されているのではなく、技術の構成に対して影響を与えるのである。(10)

### 三・二　自己によるデータ保護（Selbstdatenschutz）を通じた情報自己決定

しかし技術への要求事項もまた、それぞれの国家の中でのみ作用することができる。自己によるデータ保護を可能とする規律は、さらに大きく作用する。(11) 関係者には、その情報の自己決定を自ら保護するための自らの手段が与えられているべきである。自己によるデータ保護は、デジタル署名、匿名および仮名の行動、暗号、ステガノグラフィー（訳注1）およびその他多くの技術的補助手段によって向上され得るのである。(12) この端緒は、二つのメリットを約束する。(13)

関係者は、それ自体、自らの利益から同様に継続的に学習しかつ極めて迅速に反応するシステムである。それゆえ、関係者に対してそのつど重要にみえる自己による保護をいつでも実現し得るような状況におくことは、―それが可能と思われるところでは―広く普く被う基準により関係者を強制的に喜ばせるよ

りも、より意味があるのである。さらにその他、この端緒も世界的に作用する。つまり、自己による保護技術は、原則として、グローバルなネットワークにおけるあらゆる接点において適用することができる。

三・二・一　P3Pの例

自己決定は、データ処理についての透明性を前提とする。ここでは、WWWコンソーシアムの「Platform for Privacy Preferences Projekt (P3P)」のデータ保護規格が助けとなりえよう。[14] P3Pは、データ保護行動の定式化された機械的に可読な叙述を可能とする。プロバイダは、その「ポリシー」を定式化し、そのweb上での問い合わせに対し、まず最初の「レスポンス」でその「ポリシー」を参照させる。P3Pユーザー・コンポーネントを用いて、ユーザーは、そのユーザー指定条件（ユーザー・プレファレンス）を定式化し、これを手元に保存して、ダウンロードしたプロバイダの「ポリシー」と比較する。その結果に応じて、ユーザー・コンポーネントは、さらなる行動―すなわちウェブサイトをさらに利用するか、ウェブサイトを去るか―を自動的にまたはユーザーの手元でのユーザーとのやりとりの後で、はじめる。ユーザは、P3Pユーザー・コンポーネントの補助によって、そのデータ保護についての要求事項を満足するサービスのみを求めるように配慮することができる。P3Pの利用は、テレサービスのデータ保護親和性の評価（レイティング）の中にある。形式的な叙述は、自動的な（または少なくとも半自動的な）評価を可能とする。それによって、テレサービスは、全面的に評価され尽くすことができる。さらにさまざまなテレサービス間の比較がより通観しやすいものになる。[15] データ信託者としてユーザのためのデータ保護サービスを提供する新たに現れた企業である「インフォメディアリス（'Infomediaries'）」は、それゆえP3Pを最も集中的に利用するのであろう。[16]

三・二・二　仮名の例

仮名行動の構想には、自己によるデータ保護のための特別の意味がある。[17] それゆえこの点に若干詳細に立ち入るべきである。匿名データの処理は、なるほどデータ保護法上の「データ節約」という目標を最大限に実施に移すものではある。しかし匿名性は常に望ましくまたは意味があるというわけではない。[18] 人物との関連がなくなれば、容易に個人的な行動の責任が失われ得る。さらに、多くの生活状況の中で、たとえば契約当事者として、官職の担当者または権限の担当者として、人物を特定することができることが必要である。

データ節約と同様に人物の特定可能性をも可能にするために、仮名行動の構想が顧みられることができる。[19] というのは、それが、原則（不特定性）と例外（特定可能性）を区別することによって、不可欠な、関係者の同一性確認と、匿名でありたいというその願望との目標の衝突を、回避することができるからである。「仮名」という言葉は、ギリシャ語（pseudonymos、「いつわってそう呼ばれる」）に由来し、一般的な理解では、「作り出された名前」、「見せかけられた名前」または「偽名」を意味する。[20] BDSG（連邦データ保護法）案三条六a項の草案は、「仮名化」を「関係者の特定を排除しまたは本質的に困難にすることを目的として氏名およびその他の特定徴表をある符号で代替すること」と定義している。関係者は、さまざまな状況の中で、仮名（符号）のもとに行動することによって、それを知るあらゆる者について、彼に繋がっておりかつその意思に反して収集、処理および伝達されることのできるデータの痕跡を残すことを防ぐことができる。個人関連データについて個人を特定する部分を事後的に仮名で置き換えるときは、これと同様の効果を目指すことができる。だが仮名は、ある特定の人物に属させられたものであるから、この人物は、―匿名データの利用とは異なり―帰属規則（Zuordnungsregel）を通じて特定されることができるのである。仮名行動者に対しては、それがたとえば契約義務を履行しなかったり、その権限を踰越したようなときは、責任を負わせる可能性があるのである。

正しい取り扱いがされれば、仮名は、重要なその他の利益、つまり研究、計画、統計、マーケティングまたは広報活動のような利益がデータ保護に対して過去においてしばしばもたらしたりもたらされたりした、望ましくない衝突状況を回避するための重要な手段であることがわかる。[21] この点は、特に電子商取引についていえる。従来、電子商取引では、データ保護の問題がごまかされてきた。その結果、事業者は、手元に個人関連データを収集し、しかもその取引に直接必要とする以上に多くの情報を集めてきたし、一方、顧客は、必ずしも取引に必要でないデータについては、システム上すべての点についてごまかしているのである。商店のデータ収集は、「駅前通」に住み、夢のような電子メールアドレスや電話番号を持ち、一〇人の子供がいる九〇歳の「ドナルド・ダック」などといったところからわき出すのである。商店は、あふれんばかりの不要なデータを保有している。顧客は、事業者を信用せず、その正しいデー

タをもってまさに迂回するのである。仮名が使われれば、顧客に対して、正しい付加的な表示をさせるようにできるであろうし、かつ事業者は、個人関連ではないものの、しかしその他の点では真の顧客プロファイルをつくりあげることを可能としうるであろう。

仮名の付与によって、個人関連データは、次のように変えられるべきである。つまり、仮名が、そのそれぞれの帰属規則を知ることなしには、時間、費用および労働力の不当に大きな負担を伴ってしか特定のまたは特定可能な自然人に帰属させられることができず、しかし例外的な場合については、帰属規則を用いて人物の特定が可能であるように変えられるべきなのである。[24] 仮名化のデータ保護親和的な効果というのは、そのつどの帰属機能を利用することのできないデータ利用者に対して、得られる。それゆえ、そのデータ利用者に対しては、符号の帰属と氏名の主体の特定性は、ただちには可能ではないのである。それに対して、帰属規則を知る者にとっては、帰属させることは容易であり、そのデータは彼にとっては人物に関連させることが可能なのである。第三者に帰属規則がないときは、個人関連可能データとの区別という点では、匿名データと何らの違いもない。[25]



ここでは、帰属規則の保有者によって仮名を区別することが法的には意味がありうる。基本的に、仮名の三つの種類を区別することができる。

仮名が、もっぱら関係者自身によって与えられ、特定データとともに同時に利用されまたは保存されるものではないとき、個人関連は、関係者自らによってのみ見いだされ得る。[26] たとえば、インターネット上のサービスを受ける前に有していなければならない、自由に選択されたユーザＩＤが、ユーザー自身によって付与された仮名である。データを処理する事業者にとっては、もっぱらかかる仮名と結びつけられているデータは、基本的になんら個人関連性は示していない。この場合においては、仮名の特定を放棄することは、ユーザのみの手中に握られていることになる。

仮名が、帰属規則のみを有している、信頼に値する第三者によって与えられることもありうる。[27] この組織形式は、署名法が前提としている。欲する者は何人も、署名法七条一項により、仮名として、その固有の氏名と異なる名で認証をさせることができる。[28] 付加的に、証明証または属性証明証の中で、署名法七条二項および三項により、代表、職業許可、職位、ならびにその他の権限を確認させることができ、そしてそれにより、その



個人の特定性を暴露しなければならないということなしに、法的取引において資格ある者として登場することができる。[29] この選択肢においては、関係者のみならず、第三者も仮名の特定を知っている。もちろん、典型的には、帰属規則の保有者と潜在的なデータ利用者の組織的な分離がある。そこで、たとえば関係者は、その仮名による証明証をある認証機関から得て、そしてそれをインターネット上での購入の際に、基本的に帰属規則へのアクセス権を有しないさまざまな事業者に対して用いるのである。

第三の可能性は、もともとのデータ利用者が仮名を与えかつ帰属規則を有している場合である。このとき仮名は、このもともとのデータ利用者に対しては保護はしないが、しかしその他すべての第三者に対しては保護をする。たとえば、インターネットモールの経営者が、バーチャルな訪問者にその住所および氏名の届出の際に、「ウィンド・ショッピング」のための仮名を割り当て、それを用いて、訪問者が個別のインターネットショップで買物ができる。ネットショップは、その製品に関心を持っている者の同一性にはあずかり知らない。モールの経営者は、購入者の同一性については知っており、それに対してその住所あてに請求書および商品を送付することができる。第二の選択肢における同様に、関係者は、もはやひとりで仮名の同一性を保持することはできない。むしろ関係者は、この秘密を、独自に暴露することのできる他人と共有する。第二の選択肢と違って、帰属規則を知る者は、自らのデータ利用の利益を有しており、仮名にもかかわらずデータを個人関連的に用いることができる。動的に与えられるＩＰナンバーは、このさらに別の例である。アクセスプロバイダには、ユーザの個人関連データがなるほど知られているが、ユーザは、選択された事業者のサーバに対してはプロバイダのＩＰアドレス範囲の範囲内ではあるが一時的に仮名として機能する変動するＩＰアドレスのもとで行動する。第三者にとっては、ＩＰアドレスを通じての個人関連性は、確立されることはできないのである。個人関連は、帰属規則を手にしているアクセスプロバイダと協働したときにのみ、確立することができる。

ＴＤＤＳＧ四条一項は、三つのすべての選択肢を可能にしている。それは、あらゆるサービスプロバイダに対して、技術的に可能でかつ期待可能である限りで、ユーザにテレサービスの請求およびその支払を匿名でまたは仮名の下で可能とすることを求めている。このことは、まず第一に、第三の選択肢を指示する。だが、サービスプロバイダは、仮名を自ら与えかつ管理

する必要はなく、認証機関の仮名の証明証または自ら生成した仮名を受け入れることもできよう。

この規定とともに、同時に、マルチメディアサービスのプロバイダに、このデータ保護親和的な方法を利用するための刺激が与えられているべきである。仮名化によって、データは、その個人関連性を実務上は増加させる。プロバイダには、それによってデータ保護法律の適用範囲から除外されるチャンスが開かれている。[31] 個人関連が実務上排除されるにもかかわらず、プロバイダ義務が継続的に適用されるなどということがあれば、規定の趣旨および目的と相いれないことになる。[32] 逆に、まさにデータ保護要求が妥当しないことは、匿名または仮名のデータの利用によって個人関連データの節約の目標を実施に移すという刺激をあたえるのである。かかるデータのみを利用している者は、以下のような諸要求事項を免除される。つまり、

・BDSG四条一項、TDDSG三条一項から生じるデータ処理の一般的な禁止に服さない。特別な許可要件にも拘束されず、データ利用の同意も得なくてもよい。
・仮名のデータについては、目的拘束が妥当しない。特に、データ伝達についての特別の制限は遵守しなくてもよい。
・データ収集の前に、TDDSG三条五項によりユーザに教示



を行わなくてもよい。
・特殊な、または必要性の原則から生じる消去義務に服さない。
・BDSG三五条から生じる修正、停止および消去の義務には関わらない。
・TDDSG四条四項によるプロファイル形成の原則的な禁止に服さず、TDDSG四条二項三号および四号による秘密保持と分離されたデータ処理の要求事項に従わなくてもよい。
・データの技術的・組織的なセキュリティー確保のための義務は関わらない。
・最終的に、BDSG三二条による私的なデータ処理者について定められた届出義務も消滅する。
・データ保護監督の措置は、個人に関連させ得るデータではないという確信を監督行政庁が得られるまで、実施されるにすぎない。

ただ、仮名の利用に際しては、一定のデータ保護リスクが残っている。長い間同じ仮名が使われているときは、この仮名についての情報が名寄せされる（連結される）可能性がある。そうするとデータ収集され、ある仮名のもとでの包括的なプロファイルまで生じることがありうる。仮名が暴露されれば、関連人物のこれらすべてのデータが一挙に帰属させ得るものとなる。別のリスクが、これまで帰属規則を知らなかった者にも知られるという点にある。このことは、たとえば、無意識のうちに、帰属規則を知る者が、受領者に仮名の暴露を可能とするような知識を気づかないうちに放棄してしまうことによって起こり得る。上述した偶然的な暴露の危険と並んで、仮名にとっては、とりわけ意図的な、任意の暴露は、決定的な役割をはたしている。[33]

匿名行動に対する仮名利用の利点は、紛争事例における仮名の、必要に応じた暴露の可能性にも、あるいはまさにその点にこそある。このことは、第一に―たとえば、クレームの場合に―仮名使用者の利益のためにありうる。しかしまた仮名で行動する者と協力するその他のパートナーも、仮名の暴露への正当な利益をもち得る。そこで、給付の交換が同時に行われず、一方当事者が先に給付を行うような法的取引に際して、その先に給付を行う当事者は、匿名で行動する者に対して給付を行うことを期待することはできない。むしろ、彼は、不履行または不完全履行の場合において契約当事者に責任を負わせ、かつありうる保証請求権を実現する可能性を持たなければならない。この場合において、紛争の場合にきちっとした暴露手続によって



仮名の暴露が保障されているときは、仮名の補助を用いて、自己決定されたデータ保護を確保することができ、事前に給付する者の利益を考慮することができる。契約当事者が、支払請求権の履行にのみ関心があるときは、その利益は、仮名についての保証金によって満足されることができ、その支払がなされれば暴露を無用にする。[34]

暴露によって、ある仮名について保存されているすべてのデータは、個人関連データになる。そのときは、この時点から、データ保護法の規律が適用されるが、しかし個人関連データの収集、処理および利用のためにデータ保護法が求めている多くの保護措置は、もはやその時点では事後的に取り戻そうとしても意味がない。

事後的な暴露の結果は、データ利用者にとっても、とりわけ関係者にとってもきわめて不満足なものである。[35] 情報自己決定のために十分な保護を保障するためには、暴露のリスクに対する配慮と個人関連データではないがかかるデータになりうるデータについてその効果を提供するデータ保護法上の規定が不可欠である。[36] したがって、次の点についての配慮規定が不可欠である。

・関係者の情報。彼が、仮名性を除去されるのを避けるために、

どの措置を行うことができるかまたは避けなければならないかについて知らなければならない。事後的に、少なくとも、関係者が仮名データの利用についての情報を得ることができることが必要である。[37]

・仮名の特性のセキュリティ確保。第一に仮名の人物関連の蓋然性を減らし、かつ第二に、暴露の潜在的な損害を減少させるための配慮措置が不可欠である。

しかしこれまで、ドイツ法においては、私人のための暴露手続規定が欠けている。署名法一二条二項は、公安行政庁および秘密情報機関のための暴露請求権のみを定めている。懸案のＴＤＤＳＧの改正の中で、暴露請求権および適切な暴露手続が定められれば、仮名による行動の構想は、新らしくかつ成果を約束する、自己によるデータ保護の道具となるのではなかろうか。

### 三・三　システム的データ保護によるデータ節約

サービスプロバイダに対して、ＴＤＤＳＧは、その三条四項で、新たなデータ保護目標として、データ回避またはデータ節約を求めている。最良のデータ保護は、まったく個人データが生じないときに確保されるという認識から出発している。その場合、個人データが収集および処理されることのできるそのシステム構造の構成によって、個人データの収集および利用が回避され、ユーザの自己決定が確保されるべきなのである。[40]

システム的データ保護は、サービスプロバイダに、それがサービス提供に際しできるだけ個人データを少なく生じさせるように切り替えることができるかどうか、データ処理構造を審査することを求めている。[41]そこで、時間課金による給付の提供によれば、内容を記録保存しないですむし、定額制料金にすれば、接続時間を記録しないですむ。電子的に発注されるが物理的に配送される製品の場合は、販売者は購入者の名称および宛先を、仲介する発送サービス事業者は、製品および価格を知らなければならないというデータ分配的なシステム組織が残っていることもありうるであろう。システム的データ保護に決定的なのは、インターネットにおける支払手続の選択であろう。給付と反対給付が安全に同時に交換される場合は、技術的にはこの交換をデパートや市場におけると同様に匿名で行うことができる。このことは、たとえば、「Secure Transaction Standard (SET)」[42]によるクレジットカードでの支払の場合に達成することができるが、そのバージョンでは、三つの鍵のペアを用いて購入者が販売者に対して仮名でのみ立ち現れることができる。自己によるデータ保護を可能とするために、ＴＤＤＳＧ四条一項は、あらゆるサービスプロバイダに対して、技術的に可能でありかつ期待可能である限りで、ユーザに、テレサービスの要求およびその支払を匿名でまたは仮名を用いて可能とすることを求めている。[43]

システム的データ保護は、ドイツの機関に対してのみ実行され得る。世界中のサービスプロバイダに対しては、データ保護に適合的な解決策が競争上のメリットをもたらすときにのみ、模範として見習うべきものとして作用するのである。しかしシステム的データ保護は、データ保護技術に組み込まれ、そしてこれらを通じて世界的に提供されることができるのである。

## 四　実施の問題および解決の端緒

ＴＤＤＳＧは、立法者にとっては一つの実験であった。それゆえ、立法者は、二年後に評価を実施することを決定した。評価は、昨年の夏に実施され、二つの重要な結果をもたらした。[44]第一の結果は、ＴＤＤＳＧは、基本的にうまくいっていると実証されているという確認であった。しかし、第二の結果は、関係している経済の一部において、特に中小企業においては、まだ十分にその要請が認識されていないかまたは注意を払われていないという確認であった。また、これら中小企業に対しては、技術的な可能性についても十分に教示がなされていなかった。[45]

この執行の欠陥は、説得的な法（persuasives Recht）の根本的な問題である。[46]過剰規制という非難を避けるために、ＴＤＤＳＧでは刑罰規定を放棄した。[47]このことは、国家、市民および企業のパートナー的な関係の枠内では意味があるかもしれないが、補完的な措置を必要としている。私は、執行の欠陥を緩和するための二つの端緒を考えている。

### 四・一　刺激：データ保護監査（Datenschutzaudit）

第一に、企業の行動論理に強力に沿うメカニズムが用いられなければならない。かかるメカニズムを提供するのが、データ保護監査である。つまり、そのデータ保護の努力を宣伝することのできる確保された可能性によって、サービスプロバイダは、任意に、継続的なデータ保護の向上に資するところのデータ保護マネージメントシステムを定立するようにしむけられるべきである。[48]企業は、データ保護措置についての外部からの審査の後に、データ保護監査マークをその宣伝に用いることができる。[49]

継続的な改善という目標は、データ保護監査が、学習システムとして理解されるときにのみ達成されることができる。[50]定期的な間隔で、データ処理機関は、その目標設定の実施を審査し、

目標設定を修正改善していく。これまでのデータ保護措置の実施にともなう積極および消極の経験は、修正改善の中で取り入れられるが、反省的な形式で次の改善段階を決定するのである。このような学習プロセスの構造化がなされれば、データ保護の中に、新たな促進的要素が付け加えられよう。個別の解決策を際だたせるのが重要なのではなく、継続的に極めて迅速に変化する世界の中で繰返し繰返し新たな挑戦に対する解決策を見いだすマネージメントシステムの能力が重要なのである。

データ保護監査についての大綱法の法案は、連邦政府の委託を受けて、一九九九年夏に作成された。[51] 連邦政府は、この提案に基づいて、データ保護監査法を制定することを意図している。[52]

### 四・二　模範：DASITの例

第二に、法律の有効性は、啓蒙および納得のための包括的な付随的措置によって促進されなければならない。TDDSGの積極的な効果は、その内容、特にそれを実現に移すその可能性を十分に宣伝してはじめて期待されるべきものである。TDDSGが、シンボル的な法として示されるのみならず、パイロット的解決策および実演的解決策に向けてより多くの努力がなされなければならない。



かかるパイロット的解決策および実演的解決策は、インターネットにおける電子的購入および支払については、「テレサービスにおけるデータ保護（DASIT）」研究プロジェクトで作り上げられるものである。このプロジェクトは、DGバンク、ドイツ組合銀行株式会社、GMD情報技術研究センター有限会社およびカッセル大学の憲法適合的技術構成プロジェクトグループによって九八年一〇月から二〇〇一年三月まで実施される。これは、連邦経済技術省によって財源負担される。プロジェクトにおいては、「電子商店街（Electronic Mall）」の組織的な例および「電子財布（Electronic Wallets）」の技術的な例によりながら、どのようにTDDSGの要請が実務の中で実施に移されることができるのかが示される。電子商店街については、商品の提供からその発送および支払までのどこで個人データが節約可能であるかが研究される。電子財布については、SETの基準を用いて、匿名でおよび仮名を使ってどのように購入および支払が可能かが示される。さらにこの電子財布はまた、ユーザが、そのデータ保護権を実現することを支えるであろう。電子財布では、P3P基準によるデータ保護志向的なクライアントとサーバの通信の可能性が実現される。さらにこの電子財布は、電子的に同意をし、同意を撤回し、オンラインで自ら個人について記録保存されたデータを閲覧しそしてオンラインでデータの訂正、停止または消去の請求を行う可能性を提供する。これらの諸解決策は、夏からフィールド実験で試験が行われることとなっている。[53]

## 五　展　望

私には、ドイツ連邦共和国は、インターネットにおける将来志向的なデータ保護を実現するための正しい途上にいるように思われると、そのように、私は述べてきたことを全体としてまとめることができる。その実証の後には、TDDSGの新たなデータ保護の構想は、次の段階で一般的なデータ保護のために連邦データ保護法の中に取り入れられるであろう。データ回避およびデータ節約、システム的データ保護、匿名性および仮名性についての諸原則は、全データ保護法に対して包括的にあてはまる原理として妥当するのである。しかし実際によいデータ保護を確保するためには、よい法律のみでは十分ではない。それを十分に実施に移すことにかかっているのである。

（1）　たとえば、Engels/Einterbäumer, Kommunikation und Recht 1998, 197 f. を見よ。

（2）　たとえば、Roßnagel, Zeitschrift für Rechtspolitik 1997, 26 ff.; Garstka, Deutsches Verwaltungsblatt 1998, 987f.; Hoffmann-Riem, Datenschutz und Datensicherheit 1998, 686 を見よ。

（3）　BVerfGE, 65, 1 (42 ff.).

（4）　TDDSGは、著者の主宰する憲法適合的技術構成プロジェクト・グループ（provet）の「オンライン・マルチメディアサービスにおけるデータ保護」についての鑑定書（一九九六年）によって、準備されたものである。<http://www.iid.de/iukdg> und <http://www.provet.org/bib/mmge> を見よ。

（5）　〔連邦と州との〕立法権限の分配に基づいて、インターネット上のサービスは、テレサービスとメディアサービスとに区別された。テレサービスに関するデータ保護は、連邦がTDDSGで規定し、メディアサービスに関するデータ保護は、州が、マルチメディア州際条約で規定した。この点について詳細には、Roßnagel, in: ders. (Hrsg.), Recht der Multimedia-Dienste, Einführung, Rn. 13 ff. を見よ。それらの規定は、連邦と州との申し合せに基づき、ほとんど文言が同じであるから、以下では、簡略化のためTDDSGのみにふれる。

（6）　この点、Bundesregierung, BT-Drs. 14/1191, 13 も見よ。

（7）　この点について詳細には、Schaar, in: Roßnagel (Fn. 5), Kommentierung zu § 7 TDDSG を見よ。

（8）　たとえば、Information and Privacy Commissioner/Registratiekamer, Privacy-Enhancing Technologies: The Path to Anonymity, 1995 を見よ。

（9）　Büllesbach, Recht der Datenverarbeitung 1995, 1; Büllesbach,

Recht der Datenverarbeitung 1997, 239 を見よ。

(10) Lanfermann, Recht der Datenverarbeitung 1998, 4 ; Bizer, in Roßnagel (Fn. 5), § 3 TDDSG, Rn. 15 ff. ; Schaar, in Roßnagel (Fn 5), § 4 TDDSG, Rn. 43 ff. を見よ。

(11) 自己によるデータ保護については、たとえば、Roßnagel/Wedde/Hammer/Pordesch, Digitalisierung der Grundrechte ?, 1990, S. 220, 240 ff., 297 ff. ; provet (Fn 4) ; Trute, Juristenzeitung 1998, 829 ; Hoffmann-Riem, in : Bäumler (Hrsg.), Der neue Datenschutz, 1998, 21 f. ; Schrader, ebda., 206 ff. ; ders., DuD 1998, 128 ; Engel-Flechsig, in : Lehmann (Hrsg.), Rechtsgeschäfte im Netz-Electronic Commerce, 1999, 19 ff. ; Roßnagel, Datenschutz und Datensicherheit 1999, 255f. を見よ。

〔訳注1〕 ステガノグラフィー（Steganography）とは、「情報非可視化技術」、「電子迷彩技術」のことで、他人にみられたくない情報を別のデータの中に埋め込み、秘密データそのものを見えなくしてしまう技術である。

(12) これらの技術については、たとえば、Zwischenbericht der Enquete-Kommission “Zukunft der Medien in Wirtschaft und Gesellschaft” zu “Sicherheit und Schutz im Netz”, BT-Drs. 13/11002, 94f. ; Konferenz der Datenschutzbeauftragten, Datenschutzfreundliche Technologien, ‹http://www.datenschutz-berlin. de/ to/datenfr.htm› を見よ。

(13) この点については、Roßnagel, Datenschutz und Datensicherheit 1999, 255 ff. を見よ。

(14) The Platform for Privacy Preferences 1.0 (P3P 1.0) Specification ; W3C Working Draft, 2.11.1999. Previous Version : Platform for Privacy Preferences (P3P) Specification, W3C Working Draft 26.8.1999 ; s. auch P3P Guiding Principles, W3C Note 21.7.1998, ‹http://www.w3.org/p3p›.

(15) この点について、詳細には、Grimm/Roßnagel, in : Kubicek/Braczyk/Klumpp/Roßnagel (Hrsg.), Golbal @Home, Jahrbuch für Telekommunikation und Gesellschaft 2000, 293 ff. を見よ。

(16) たとえば、www.digitalme.com ; www.enonimous.com ; www.privaseek. com ; www.privacybank.com ; Hagel III/Singer, Net Worth. The Emerging Role of the Infomediary in the Race for Costumer Information, 1999 を見よ。

(17) 匿名または仮名の要請については、たとえば、Registratiekamer/ Information & Privacy Commissioner, Privacy-enhancing Technologies : The path to Anonymity, 1995 ; Rat für Forschung, Technologie und Innovation, Informationsgesellschaft-Chancen, Innovationen und Herausforderungen, 1995, 2. 5 Empfehlung 23, ‹http://www.technologierat.de/vdi/frames/report95.htm› ; Art. 29-Datenschutzarbeitsgruppe, Budapest-Berlin Memorandum on Data Protection and Privacy on the Internet, ‹http://www.datenschutz-berlin.de/doc/eu/gruppe29/bbmem_de.htm› ; Enquete-Kommission “Zukunft der Medien in Wirtschaft und Gesellschaft” (Fn. 12), 94 f ; Simitis in : Festschrift für Kübler, 1997, 285 ff. を見よ。

(18) 匿名のテストについては、Caronni, Datenschutz und Datensicherheit 1998, 623 ff. を見よ。

(19) この点については、Roßnagel in : Festschrift für Podlech, 1994, S. 245f. ; provet/GMD, Die Simulationsstudie Rechtspflege, 1994, 210 ff. ; BT-Drs. 13/7385, 23 ; Roßnagel, in : ders. (Fn. 5), Einführung, Rn. 61f. ; Bizer, in : Roßnagel (Fußn. 5), § 3 TDDSG, Rn. 175 ff. を見よ。

(20) 匿名性のデータ保護法上の意味については、Simitis (Fn. 17), 309 を、匿名技術については、Borking, Datenschutz und Datensicherheit 1996, 654. ; Arbeitskreis Technik der Konferenz der Datenschutzbeauftragte, Datenschutz und Datensicherheit 1997, 709 ff. ; Federrath/Pfitzmann, Datenschutz und Datensicherheit 1998, 628 ff. ; Demuth/Rieke, Datenschutz und Datensicherheit 1998, 623 ff. ; Roessler, Datenschutz und Datensicherheit 1998, 619 ff. を見よ。

(21) Brockhaus-Die Enzyklopädie, 20. Aufl. 1996 ; Bizer/Bleumer, Datenschutz und Datensicherheit 1997, 46.

(22) TDDSG四条一項は、仮名を用いた利用については、定義をしていない。法律上の定義の必要性については、Bundesregierung, BT-Drs. 14/1191, 15 を見よ。

(23) Begründung zu § 10 Abs. 6 und § 22 Landesdatenschutzgesetz Schleswig-Holstein, LT-Drs. 14/1738, 55f., 67f. を見よ。

(24) シュレスヴィヒ・ホルシュタイン州データ保護法一三条五項、アラスデンブルク州データ保護法一三条二項一号と同様である。AK Technik (Fn. 20) (Datenschutz und Datensicherheit 1997, 711) および「データ保護監査・マルチメディア（“Datenschutz-Audit Multimedia”）」(Datenschutz und Datensicherheit 1999, 290) の定式も見よ。

(25) そのようにいうものとして、Begründung zu § 22 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein, LT-Drs. 14/1738, 66f.

(26) AK Technik (Fn. 20), Datenschutz und Datensicherheit 1997, 711 は、自ら生成した仮名について述べている。

(27) かかる可能性については、AK Technik (Fn. 20), Datenschutz und Datensicherheit 1997, 711 もそれによるいわゆるレファレンス仮名について予定している。この点については、IDDSGについての政府提案理由、BT-Drs. 13/7385, 23 も見よ。この種の仮名は、いわゆる場所的および組織的に仮名化されたデータから区分されて信頼性ある機関において保存されるものとされているレファレンスリストを通じてのみ人物との関連を確立することができる。

(28) この点については、Roßnagel, in : ders. (Fn. 5), § 7 SigG, Rn. 34f. を見よ。

(29) 適格性を与える証明証〔適格証明証〕を伴う仮名については、Roßnagel, in : ders. (Fn. 5), § 7 SigG, Rn. 62f. ; provet/GMD (Fn. 19), 213 ff. ; Pordesch, in : Roßnagel/Haux/Herzog (Hrsg.), Mobile und sichere Kommunikation im Gesundheitswesen, 1999, 156 ff. を見よ。

(30) Schaar/Schulz, in : Roßnagel (Fn. 7), § 4 TDDSG, Rn. 49.

(31) Begründung zu § 4 TDDSG, BT-Drs. 13/7385, 23 を見よ。

Engel-Flechsig, Recht der Datenverarbeitung 1997, 65; ders. (Fn. 11), 21; Schulz/Schaar, in: Roßnagel (Fn. 5). § 4 TDDSG, Rn. 45; Bäumler, Datenschutz und Datensicherheit 1999, 260 も見よ。

(32) Gola/Schomerus, Kommentar zum BDSG, § 3 Anm. 14. 2; § 40 Anm 2. 3; Simitis, in: Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum BDSG, § 40 Rn. 60. Für eine rechtliche Gleichstellung auch der Landesbeauftragte für Datenschutz Schleswig-Holstein, LT-Drs. 14/1738, 40; Bizer, in: Roßnagel (Fn. 5), § 3 TDDSG, Rn. 69, 168.

(33) この点について詳細は、Roßnagel/Scholz, Multimedia und Recht 2000, Heft 7,（近刊）を見よ。

(34) Pfitzmann/Waidner/Pfitzmann, Datenschutz und Datensicherheit 1990, 305 ff.; Pfitzmann, Datenschutz und Datensicherheit 1999, 406 を見よ。

(35) この点について、より正確には、Roßnagel/Scholz, Multimedia und Recht 2000, Heft 7,（近刊）を見よ。

(36) この点については、たとえば、Bizer, Forschungsfreiheit und informationelle Selbstbestimmung, 1992, 153 ff.; BVerfGE 65, 1 (49); BVerfG, Neue Juristische Wochenschrift 1987, 2805 (2806) を見よ。

(37) 予防的透明性は、既にTDDSGの七条によって事後的な透明性が命じられるTDDSG四条一項二段に既に含まれている。

(38) TDDSG四条四項一段は、仮名の利用の下で作成された利用プロファイルについて、かかるセキュリティ原則を既に定めている。

(39) この点については、既にRoßnagel, Datenschutz und Datensicherheit 1997, 75 ff. を見よ。

(40) システム的データ保護について、基本的には、Podlech, in: Festschrift für Grüner, 1982, 451 ff. を見よ。Roßnagel (Fn. 19), 236 ff.; ders., Zeitschrift für Rechtspolitik 1997, 29; ders., Datenschutz und Datensicherheit 1999, 256; Engel-Flechsig, Datenschutz und Datensicherheit 1997, 13 f.; Büllesbach/Garstka, in: Müller/Pfitzmann (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik, Band I, 1997, 383 ff.; Hoffmann-Riem, Archiv des öffentlichen Rechts 1998, 535; Kloepfer, 62. Deutscher Juristentag 1998, D, 98f.; Garstka, Deutsches Verwaltungsblatt 1998, 988; Trute, Juristenzeitung 1998, 827f. も見よ。技術構成によるデータ保護については、たとえば、Bäumler, Datenschutz und Datensicherheit 1997, 448 ff.; ders., Recht der Datenverarbeitung 1999, 7; Bizer, in: Bäumler (Hrsg.), Datenschutzgesetze der dritten Generation, 1999, 28 ff. を見よ。

(41) Bundesregierung, BT-Drs. 14/1191, 13. Bizer, in: Roßnagel (Fn. 5), § 3 TDDSG, Rn. 131 ff. も見よ。

(42) この点については、SET, Secure Electronic Transaction Specification, V. 1.0, 31.5.1997, ‹http://www.setco.org/› を見よ。

(43) この概念については、Schaar/Schulz, in: Roßnagel (Fn. 5), § 3 TDDSG, Rn. 44 ff. を見よ。

(44) 評価については、Schulz, in: Kubicek et al. (Hrsg.), Multimedia @Verwaltung. Jahrbuch Telekommunikation und Gesellschaft 1999, 202; Roßnagel, Datenschutz und Datensicherheit 1999, 253; Bäumler, Datenschutz und Datensicherheit 1999, 258; Büllesbach, Datenschutz und Datensicherheit 1999, 263 も見よ。

(45) Bundesregierung, BT-Drs. 14/1191, 14 ff.; Bäumler, Datenschutz und Datensicherheit 1999, 262, Wolters, Datenschutz und Datensicherheit 1999, 277, 280; Bundesbeauftragter für den Datenschutz, 17. Tätigkeitsbericht, 1999, 146; Tettenborn, Multimedia und Recht 1999, 519. Roßnagel, Datenschutz und Datensicherheit 1999, 257; Büllesbach, Datenschutz und Datensicherheit 1999, 265; Grimm/Löhndorf/Scholz, Datenschutz und Datensicherheit 1999, 273.

(46) この点については、Roßnagel, Neue Zeitschrift für Verwaltungsrecht 2000, 266 ff. を見よ。

(47) この点は、計画されているTDDSG改正の中で、行われることとなっている。そこでは、九条において週料規定が定められている。Bundesregierung, BT-Drs. 14/1191, 16.

(48) データ保護法の遵守は、自明のことであって、何ら顕彰には値しない。

(49) この点については、Roßnagel, Datenschutzaudit-Konzeption, Durchführung, gesetzliche Regelung, 2000 を見よ。

(50) この点に、日本における一PDECおよびCBAのプライバシー・マーク制度との決定的な違いがある。

(51) この点についての鑑定書は、Roßnagel (Fn. 49) に所収されている。

(52) Bundesregierung, BT-Drs. 14/1191, S. 14 und Bundesregierung, Aktionsprogramm "Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts, BT-Drs. 14/1776=BR-Drs. 551/99, abrufbar unter ‹http://www.bmwi.de›. Kap. 3. 4; Tettenborn, Multimedia und Recht 1999, 520.

(53) この点については、Grimm/Löhndorf/Scholz, Datenschutz und Datensicherheit 1999, 272; Grimm/Löhndorf/Roßnagel, E-Commerce meets E-Privacy, in: Bäumler (Hrsg.), Datenschutz im Electronic Commerce, 2000（近刊）を見よ。

＊　ロスナゲル教授（法学博士）は、カッセル大学の公法講座の教授であり、特に技術法および環境保護法を重点研究領域としている。
本稿は、DGバンク（フランクフルト）、GMD情報技術研究センター（ダルムシュタット）およびカッセル大学憲法適合的技術構成プロジェクトグループ（provet）により実施され、連邦経済技術省により助成されている「テレサービスにおけるデータ保護（Datenschutz in Teledinesten; DASIT）」という研究プロジェクトから得られた成果である。本稿は、著者が、二〇〇〇年四月一八日に京都の立命館大学で行った講演を基礎にしている。

## 〔訳者解説〕

米丸　恒治

本講演は、ドイツのカッセル大学において、憲法適合的技術構成プロジェクト（provet）を主宰し、サイバースペースにおける個人データ保護などの分野で活発な研究活動を行い、政府の立法作業の準備作業にも関係しておられるアレクサンダー・ロスナゲル教授が、立命館大学において行われたものである。本講演は、教授も関係されたドイツのテレサービスデータ保護法で取られている構想にふれながら、グローバルなネットワークにおいて送受信される個人データの保護のために、どのような法的対応が必要なのかについて述べられたものであり、現在進められているわが国における個人データ保護の法制化論議においても有意義なものである。以下、訳者として、簡単に本講演の背景と、若干の補足説明をしておきたい。

### 一　EU個人データ保護指令とドイツ

EUでは九五年に制定された「個人データ処理に係る個人の保護およびかかるデータの自由な移動に関する一九九五年一〇月二四日の欧州議会および理事会の指令九五／四六／EC」（略称でデータ保護指令[1]）の国内措置が、現在行われようとしている。本来の予定からすれば、国内措置は、九八年に終了していなくてはならないはずだったが、多くの国で国内措置が遅れ、現在それに向けた作業が進められている。このEU指令に先立つ歴史や内容に影響を与えた考え方について、ここでは詳しく触れることはできないが、ドイツのデータ保護法制は大きな影響を与えたもののひとつである。

そのドイツにおいても、EU指令の国内措置は遅れており、本稿執筆時点において、連邦データ保護法[2]の改正法案[3]は、ようやく閣議決定を経てやっと連邦議会または連邦参議院に提出されようとする段階である。このようにドイツでは、EU指令の国内措置が遅れてきたが、こうした構成国の国内措置の遅れに対して、EC委員会は、フランス、ルクセンブルク、オランダ、ドイツおよびアイルランドの諸構成国をEC裁判所に提訴する措置をとっている（二〇〇〇年一月）。

現状では、EU指令の進んだ部分をドイツが後追いするところと、一方で、インターネット上のコミュニケーションについては、後述のように一歩進んだ部分もあるが、いずれにせよこのEU指令で確立しているデータ保護についての原則が、国際的には大きな意味を持ってきつつある。

### 二　情報・通信サービス大綱法とテレサービスデータ保護法

一方、ドイツでは、講演の中に登場する情報・通信サービス大綱法（IuKDG）の中で、「テレサービスにおけるデータ保護に関する法律（テレサービスデータ保護法、TDDSG）」を定め、サイバースペースにおいて提供される情報・通信サービスであるテレサービスについてのデータ保護の法制度を整備した[4]。情報・通信サービス大綱法は、ドイツが、サイバースペースにおける基盤整備の一環として、テレサービスなるサービス範囲を確定し、そこにおける責任の明確化を図るとともに、デジタル署名、データ保護などの法整備をおこなったものである。ドイツにおける総合的なサイバースペース法としての意味を持つ法制として、国際的にも注目されてきたものである。

ドイツでは、サイバースペースにおけるデータ保護の関連では、サイバースペース外の一般社会でも適用される一般法である連邦データ保護法、電気通信サービスに適用される電気通信サービス企業データ保護令、テレサービスに適用されるTDDSGの、それぞれの適用がなされている。講演の中では、主としてこのTDDSGの紹介がなされた。

講演では、TDDSGの構想として、国家による法的な制裁をともなう従来の連邦データ保護法の法規制の限界を補う新たな構想として、技術によるデータ保護、自己によるデータ保護、システム的データ保護の三つの構想が紹介されている。いずれも、従来の法規制の中にはみられなかったか、または十分意識されていなかった構想をデータ保護の体系に組み込むものとして、注目される。なおこうした新たな構想は、従来から、連邦データ保護法が官民を通じたデータ保護規制を行ってきた上に、その限界を補うものとして構想されているものであることが看過されてはならない。本講演で強調されている新構想は、法的規制とあいまって、総合的な個人データ保護の体系を目指すものなのであって、法的規制のない、技術的対応および自主規制を偏重するものではないのである。この点は、わが国におけるデータ保護法制の構築にあたっても留意されるべき点のひとつであろう。

### 三　若干の補足説明

講演の中心は、サイバースペースにおいてデータ保護を確保しようとする際の新たな構想と、その実施に際して個人データ保護の実効性を確保するための手段としてのデータ保護監査（Datenschutzaudit）およびプロジェクト実験を通じたモデルの開発および普及である。それぞれの点については、講演を参照していただくこととして、若干の点について、補足をしておこう。

①技術の重視

講演では、国家権力による法規制の限界を補うものとして、技術によるデータ保護の重要性が強調されている。特に、個人データ保護親和的な技術が開発され、それがネットワーク関連の商品に組み込まれて国際的に普及することにより、国家権力の限界を補うことができることへの注目は、重要である。

②個人による自己防衛

国家による法規制を補い、まさに個人情報についての自己コントロールを行うための「自己によるデータ保護」は、個人情報が国家権力の規制の及ばないグローバルなネットワークで送受信されている中で、再確認されなければならない基本原則であろう。講演では、そのためのいくつかの手段が紹介されている。

③仮名による自己防衛

自己によるデータ保護の手段のひとつとして、講演では、仮名（pseudonym）の利用が紹介されている。わが国では、匿名（anonym）と仮名（pseudonym）の意義がほとんど区別されないまま、いずれも自らの氏名を隠し、責任の所在を不明にするためのものとしての理解がされがちである。しかし講演の中で詳しく述べられているように、仮名は、個人情報を秘匿して自己防衛しつつも、その責任を追求すべき場面では、仮名の本人の所在をつきとめ、責任を追求し得ることができる制度として、重要視されていることに注意が必要である。仮名の本人特定のためのしくみが確保されていて、その利用が推奨されていることが重要なのである。

ＴＤＤＳＧの中では、仮名によるサービスの利用を認めなければならないものとして、明示的に、仮名の利用が保障されていることは講演でもふれられている。

仮名の利用による個人データ保護の構想は、ドイツのみならず、国際的にも認知されつつある。九九年一二月一三日のＥＵ電子署名指令[5]は、電子署名の認証を担当する認証機関（指令上は、認証サービスプロバイダ）、認証機関の認定を担当する認定機関、およびそれらの監督行政機関が、それぞれＥＵ個人データ保護指令の内容を遵守することを求めるとともに（八条一項）、仮名での認証および電子署名、すなわち証明証の中に仮名を用いて認証を受け、その証明証を用いて電子署名を利用することを確保することを求めている。仮名での証明証を用いて、仮名で署名しても、本人の確認は認証機関により確保されるために、法的紛争に際しては、認証機関を通じて、本人確認がなされる結果、問題は生じないしくみがとられることになる。

ここでは、講演で紹介された仮名の利用は、無責任な状況をもたらすのではないこと、またその構想が単なる理論的産物でなく、実務上も、国際的に広がりつつあることを補足しておきたい。

（1）Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281 (23/11/1995), p. 31. 本指令については、既にわが国でもいくつかの訳が公開されている。堀部政男研究室訳・新聞研究五七八号一七頁以下（一九九九年）、庄司克宏訳・横国七巻二号一四三頁以下（一九九九年）、郵政省電気通信局電気通信事業部データ通信課訳・多賀谷一照・松本恒雄編集代表『情報ネットワークの法律実務』（第一法規、一九九九年）七一二三頁以下、オンラインでは、〈URL http://www.isc.meiji.ac.jp/~sumwel_h/doc/intnl/Direct-1995-EU.htm〉などがある。この指令については、堀部「プライバシー保護の国際的調和論」新法一〇三巻一一・一二号二九頁以下（一九九七年）、同「EU個人保護指令と日本」ジュリスト『情報公開・個人情報保護』三五八頁以下、藤原静雄「個人データの保護」『岩波講座　現代の法　一〇　情報と法』（岩浪書店、一九九七年）一八七頁以下、井奈波朋子「EC指令とプライバシー」多賀谷・松本編集代表・前掲四三八九頁以下、David Bainbridge, EC Data Protection Directive, 1996; Ulrich Dammann/Spiros Simitis, EG-Datenschutzrichtlinie-Kommentar, 1997; Eugen Ehmann/Marcus Helfrich, EG Datenschutzrichtlinie-Kurzkommentar, 1999 など参照。

なお、ＥＵでは、本指令とは別に、電気通信セクターに適用される指令が制定されている。電気通信部門における個人データ処理およびプライバシー保護に関する指令（Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (December 15, 1997), O.J. L24 (30/01/1998), p. 1）である。現在、この指令の改正案が提案されているが、これは、パケット通信、インターネットなどの新たな通信方式も含めて、通信技術中立的なデータ保護法制を確立するためのものである。Vorschlag für eine Richtlinie des Europäischen Parlament und des Rates über die Verarbeitung personenbezogener Daten und Schutz der Privatsphäre in der elektronischen Kommunikation, KOM (2000) 385, v. 12. Juli 2000 参照。

（2）連邦データ保護法については、藤原静雄「西ドイツ『連邦データ保護法』政府草案について（一、二）」国学院二四巻四号一七頁、二五巻一号一頁以下（一九八七年）、同法の邦訳として、同「西ドイツ連邦データ保護法」国学院二七巻一号五一頁以下（一九八九年）参照。また、同法の適用される民間部門のデータ保護については、山下義昭「ドイツにおける民間部門の個人情報保護について」石村善治古稀記念『法と情報』（信山社、一九九七年）三九三頁以下、村上裕章「ドイツにおける民間個人情報の立法的保護」田村善之編『情報・秩序・ネットワーク』（北海道大学図書刊行会、一九

九九年）一一七頁以下参照。

（3）本稿執筆時点では、二〇〇〇年六月一四日に閣議決定が終了した法案を参照した。同法案は、〈URL http://www.dud.de/dud/files/bdsg(9000.zip (retr. 30.6.2000)〉で公開されている。

法案では、講演でも紹介されているような、仮名化の定義（三条六a号）、TDDSGで導入されたデータ回避・データ節約原則の規定（三a条）、データ保護監査（九a条）が法定されているほか、EU指令にあわせて、第三国への移転の制限規定（四b条）なども盛り込まれている。この法改正については、別途紹介の機会を持ちたいと考えている。

（4）情報・通信サービス大綱法、テレサービスデータ保護法については、拙稿「ドイツ流サイバースペース規制―情報・通信サービス大綱法の検討」立命二五五号一四一頁以下（一九九八年）参照。テレサービスデータ保護法の試訳は、同一八二頁以下参照。

テレサービスを支える、いわば下位の基盤的サービスである電気通信サービス部門のデータ保護については、電気通信および郵便制度の規制に関する法律一〇条一項に基づく、電気通信サービスを供給する企業のためのデータ保護に関する命令、略称電気通信サービス企業データ保護令（Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen; Telekommunikationsdienstunternehmen-Datenschutzverordnung, v. 12.7.1996, BGBl I S. 982; TDSV）が規制をしている。

（5）電子署名のための共同体の枠組に関する一九九九年一二月一三日の欧州議会および欧州連合理事会の指令 1999/93/EC (Directive 1999/93/EC of the European Parliament and of the council of 13 December 1999 on a Community framework for electronic signatures, O. J. L13 (19. 1. 2000), p. 12) については、訳者による試訳、「EU電子署名指令」立命二六八号二七六頁以下（二〇〇〇年）を参照。なお、拙訳の中で、まさに本文で述べた仮名の利用についての箇所で「仮名」と訳すべき箇所が「匿名」となっている（考慮事項(25)項、八条三項、付属書Ⅰ(c)、付属書Ⅳ(f)の四箇所）。重要な訳語についてのミスであり、この場でお詫びして、訂正させていただきたい。