# ドイツのデータセキュリティ法制

## ——個人データ保護法制の技術的側面——

藤原静雄

## 一 はじめに

周知のように、一九八〇年九月二三日のOECD理事会プライバシー保護勧告の八原則[1]は、わが国のデータ保護法制にも大きな影響を与えたものであるが、その第五は「安全保護の原則（Security Safeguards Principle）」であり、「データは、その紛失又は不当なアクセス・破壊・変更・開示の危険に対し、合理的な安全保障措置により保護されなければならない」とするものである。この原則について堀部政男教授は、「今日ではセキュリティとプライバシー保護の区別はかなりよく理解されていると思われるが、セキュリティが確保されていれば、プライバシーは保護されるという言い方がよくなされることがある。しかし、セキュリティとプライバシー保護が重なり合う面は主としてこの部分であることに注意する必要がある[2]」と述べられている。セキュリティの側面のみを捉えてプライバシー保護という人権の根幹に関わる問題を論じることに対する警告を発せられたものといえるであろう。ただ、一方で、OECDが一二年後の一九九二年一一月二六日、情報システムの安全のためのガイドライン[3]を新たに策定したことに示されるように、セキュリティの問題が情報技術の進展とともにますます重要性を帯びてきていることも事実である。実際、OECDのガイドラインは、必ずしも個人データ保護と関連させられているわけではないが、個人データ保護の問題にも大きな影響を与えるものである。個人データ保護にとっ

てセキュリティ措置のもつ意味が違ってきたといってもよいであろう。

ところが、わが国の現状には、先の堀部教授の警告以前の問題、すなわち、プライバシー意識とも関係するのであろうが、セキュリティ問題の存在は理解されていても、そのための対策は行われていないに等しいという問題があると思われる。暗号・認証技術の展開[4]にみられるように、セキュリティ技術は飛躍的な発展を示しているが、その実務、とくに行政実務での運用との間に著しい乖離があると言い替えることもできよう。

このような問題意識の下に、以下では、議論の整理のために、個人データ保護とデータセキュリティ（Datensicherheit）の問題の関係[5]について一言触れた後、データセキュリティの問題に関するドイツの議論の現況を紹介してみたい。ヨーロッパで最も厳格な個人データ保護法制[6]を有するといってよい国で、データセキュリティの問題がいかなる法制を前提として、どのような形で論じられているかを整理しておくことは、今日の状況に合わなくなった点も含めて、わが国の議論の参考になるのではないかと考えるからである。

## 二　データ保護とデータセキュリティ

(1)　連邦データ保護法によれば、データ保護の目的は、個人を、各人のデータが扱われる際に、その人格権が侵害されることから守ることである（一条一項）。これに対して、データセキュリティは、学説上、「個人データの不法・不当な扱いを防ぎ、そしてデータの完全性・利用可能性を保持し、データの処理のために導入されている設備を守る、すべての組織上及び技術上の（法的でない）規制及び措置の総体である[7]」と、あるいは「ハードウエアー及びソフトウエアーの破壊または破損、並びにデータの濫用を防ぐための、技術上及び組織上のすべての措置の総体[8]」と定義されている。

以上の定義に関連して、次の三点を指摘しておく必要があろう。第一に、データ保護とデータセキュリティは相互に重なり合う関係にある（例えば、データセキュリティが十全でなければ、データ保護も全うされず、個人の人格権は保護できない）。しかし、収集制限、利用制限といった原則は、データセキュリティとは直接の関係のないものである。第二に、データ保護が個人の人格権

を保護するものであるとすれば、データセキュリティはデータ処理を保護するものといってよい。したがって、そこでは、データ、プログラム、処理システムを、日常的な処理ミスから災害に至るまで保護することが目的となる。第三に、データセキュリティの目的は、連邦データ保護法九条の目的より広い。それゆえ、データ保護法の対象とならないデータやもっぱら企業や行政の利益のためになされるセキュリティ措置は、独自の法的価値を有するものと位置付けられる必要がある。(9)

(2) データセキュリティとデータ保護の交錯

① 現実の問題として、情報技術の進展によりデータセキュリティとデータ保護の問題は切り離せないものとなっている。両者に関わる問題として、例えば、連邦データ保護監察官は、(10) チップカード、携帯可能なパーソナルコンピュータ、電子文書交換（ＥＤＩ）、コンピュータネットワーク、システム管理者に関わる問題などを挙げている。システム管理者を誰が管理するかという問題（後述四―4―(2)参照）を含めて興味深い論点ばかりであるが、以下では、日常性という観点から、チップカードを巡る問題を通じて、データセキュリティとデータ保護が交錯する場面をみておくこととしたい。

② 技術的にみれば、磁気カードからＩＣカードに至るまで、チップカードに登載可能な情報量は着実に増えている。使用される領域は、ドイツの場合、電話、移動電話、医療、銀行、有料テレビの順に多いが、量的拡大は爆発的なものであることわが国におけると同様である。これらのカードについてもセキュリティ対策の柱は、個人識別番号（パスワード、PIN, Personal Identification Number）、認証（Authentisierung, 主として発信者の同一性確認）、権限の付与（Autorisierung, 誰がカードのアプリケーションを起動させることを許されるか、例えば、患者の医療カードに登録された医師）である。これらのセキュリティ措置の確実性は、暗号・認証技術の進歩により急速に高まっているものの、データ保護との関係で次のような問題があるとされる。

第一は、本人確認すなわち暗証番号に関してである。理論的には番号の桁数が増えれば増えるほど、安全性は高まるわけであるが、多くのカードの多くの番号を通常の利用者は記憶できない。高齢者等の場合は尚更である。番号が増えればメモを必要とするか簡単な番号が使用さ

れるだけということにもなりかねないというディレンマである。この問題は、指紋あるいは網膜の血管パターンという生物学的標識で解決されうるであろうが、一般的に用いる場合には新たなデータ保護法上の問題を生じるおそれがある。第二は、開示（Offenbarung）の問題である。クレディットやチェック、さらにはそれらを含んだ多機能カードの場合には、現在の世界の主流であるシステム（端末で一度カード上の全てのアプリケーションを読んでから、必要なアプリケーションが存在するか否かを確認する）では、カード所有者の情報が当人の知らない間に蓄積ないしコピーされるおそれがある。第三は、カード利用者のデータが、銀行、保険等のいわば私的データバンクの中に沈みこんでしまい、コントロール不可能になるという問題がある。

チップカードについて、一般的には、右のような問題があるが、具体例を健康情報カードについてみておくこととしたい。

③　ドイツでは、一九九三年に健康保険カード[11]が法的に導入されてから、健康あるいは保健情報カードに関わる議論、すなわち健康情報の処理と患者のデータの保護に関わる議論が増えている[12]。この点について、後述のような基本問題が未解決であり、関係者の間にネットワークを通じての利用に関しては議論が尽くされていないという認識が存在するにもかかわらず、現実には、カードそのものは実務で既に導入されているという事実が存するようである。

未解決の基本問題としては、第一に、コンピュータネットワークの運営者及び従事者に刑法上の守秘義務（二〇三条一項）が及ばないことである。第二は、いかなる条件で健康情報へのアクセスを認めるかである（例えば、本人に行為能力がなく、補助者が健康問題について情報を与えられておらず、アクセスコードも知らないという条件で認めるか等）。第三は、チップカード上に体系的に健康情報を載せることに意義があるとして、患者は、すべての医師・医療関係者に、すべての情報を開示しなければならないのかということである。第四に、データセキュリティを保ちつつ当事者に自己情報開示を認める工夫ができるかということである。

これらの中にはセキュリティ技術で解決可能な問題もあるし、立法者が新たな枠組みを提供しなければならな

い問題もあるようである。けれども、ドイツでは、実務の一人歩きをチェックする機関として、連邦及び州のデータ保護監察官が一定の役割を果たしており[13]、医療関係者[14]を含む専門家が、技術面、経済面、倫理面からの議論を行っているという点も指摘しておく。

## 三　データセキュリティの体系と手続

ドイツの個人データ保護の領域でこれまでに論じられている、データセキュリティ法制の体系と手続を整理しておくと、以下のようになる[15]。

### 1　データ処理の際の危険

#### (1)　危険の類型

データセキュリティーの観点から見た、個人データが流通する際の危険は、次の三つのカテゴリーに分類できるとされる。すなわち、①災害：火災、浸水、落雷、磁気の影響、停電など、②過誤：操作ミス、データ送信の際の過失によるデータの改竄、ハードの欠陥、素材の疲労、ソフトウエアーの欠陥など、③濫用：データ処理システムの権限なき利用、データの窃視（Ausspähen）、無権限のデータ入手、画像の横取り、回線の盗用、情報の遮断、ハードウエア・ソフトウエアーの操作、コミュニケーションの遮断などである。

#### (2)　危険の原因

わが国でも同様であるといってよいが、ドイツでは、大規模な損害はいわゆるハッカーによってではなく、自己の職場のデータセキュリティシステムをかいくぐって犯罪を行う従業員・公務員、そして経験の浅いあるいは不注意な利用者によってもたらされるといわれている。コンピュータを扱う従業員・公務員の犯罪が増えているが、同時に、ウイルス、害虫、トロイの木馬といった名で呼ばれる、外部の第三者に起因するが注意すれば防げる被害が多いということである。

### 2　データセキュリティの基本構想

個人データ保護に対する危険性は、自動的データ処理、マニュアルによるデータ処理、そして書類態様のデータ処理で、それぞれ異なる。勿論、自動的データ処理の場合がもっとも危険性が高いことはいうまでもないが、マニュアル処理にセキュリティ措置が不要なわけではないことが忘れられてはならないであろう。

データセキュリティのシステムは、常に具体的な状況に適したものであるべきであるが、システム設計の際に

は、次のような定式に従って行うべきであるとされる。すなわち、①危険及び保護すべきデータの分析（データの態様及び危険度、処理の目的と意義）、②要求の分析、③具体的な危険の調査、④可能な措置の調査、⑤措置の評価、⑥利用価値の分析、⑦選択、調整、実行、⑧監視、である。

3　具体的措置

個人データ保護法制の一環としてのデータセキュリティは個人データ保護、それを通じた人格権の保護に資することを目的とするものである。したがって、データセキュリティの目的は、次の四つの領域を包括するといわれる。すなわち、個人データの、①信頼性（Vertraulichkeit）、②完全性（Integrität）、③利用可能性（Verfügbarkeit）、④監督可能性（Kontrollierbarkeit）である。

(1)　信頼性

信頼性の維持は、データ保護において決定的な重要性をもつ。権限を与えられた利用者だけが、その権限の枠内で個人データに触れる可能性をもつことが許される。信頼性は、蓄積されたデータにもネットワークでやりとりされるデータにも関係する。この場合、信頼性を実現するためには、①建築上の措置による身体的な出入りのコントロール、②利用者の認証及び本人確認、③データの暗号化といった措置を施すことが必要であるといわれている。

(2)　完全性

データ処理システムの完全性については、蓄積されたデータ、プログラム、ハードウエアーが無傷であることなどが挙げられる。あるシステムの変更は、権限ある利用者によってのみ行うことが許される。回線に触れることについても同様である。完全性というのは、蓄積されたデータと伝達されるデータとを問わず、意図的なあるいは意図的でない変更を防ぐことを意味している。したがって、データの完全性を維持するための措置とは、システムの権限なき操作を避けるためのすべての措置ということになる。例えば、①暗証番号、②電子署名、③安全なシステムによるプログラムの隔離（例えば、特別に安全なサーバーの導入）、④コンピュータ、デスク、回線への接近のコントロール、⑤コンピュータ、プログラム、利用者及びデータの真正を担保するすべての他の措置などが挙げられている。

(3)　利用可能性

利用可能性というのは、認められた利用者が必要に応じて、情報及び他の情報源にアクセスできるということを意味する。これは情報の紛失及び消失に対するセキュリティも含む。具体的には、①建築上の措置、②権限なき消去からの保護、③誤りの認識又は誤りの訂正のための措置、④システムあるいはシステム構成要素に余裕をもたせるような措置が挙げられている。

(4)　監督可能性

監督可能性とは、データ処理システムの適切さを審査するための手段を創り出すことを意味する。組織上及び技術上の措置によって実現されるものである。これは記録化と適正さの技術的確保の問題といってよい。

## 四　データセキュリティ法制

### 1　連邦データ保護法九条

(1)　まず、議論の対象となる連邦データ保護法九条の訳文[16]を掲げておくこととする。

連邦データ保護法九条：自ら若しくは委託で個人データを処理する公的及び非公的機関は、この法律の規定の実施、とくにこの法律の附則に掲げられた必要項目を保障するために必要な技術的かつ組織的な措置を講じなければならない。措置が必要とされるのは、もっぱら、その費用が達成される保護目的と相応の比例関係にある場合である。

(2)　九条は、旧法（一九七七年連邦データ保護法）の六条を、ほぼそのまま受け継いだものである。ただ、旧法においては、「連邦政府は、連邦参議院の同意を得て、法規命令により、技術及び組織の各々の状況に応じ、附則に掲げる要求を補正する権限を有する」という規定があったが、これは一度も利用されなかったという事実、そして技術の発展は、附則の変更ではなく新たな具体的措置を必要とするという認識から削除されている。

(3)　わが国の法制との関係では、次の二点に触れておきたい。第一点は、九条は、データセキュリティのための措置を、公的部門と私的部門とを問わず、自動的処理とマニュアルによるデータファイルの処理とを問わず義務づけ、さらに公的部門では書類の処理に応じたセキュリティの保障を要求しているということである。したがって、民間部門においても、九条違反は秩序罰によって

担保されているのである（三八条五項一文、四四条一項七号）。第二点は、九条二文にいう、セキュリティ措置の必要性と比例原則についてである。これに関して、実務では、連邦及び州のデータ保護受託官によって展開されてきたモデルが妥当している。すなわち、個人データを、そのsensitive性の程度により五段階に分けて比例原則違反か否かを衡量している。例えば、誰もがアクセスできるデータ（レベルA）、濫用が当事者の社会的地位に影響を及ぼすデータ（レベルC）、濫用が直接に当事者の健康、生命あるいは自由に影響を与えうるデータ（レベルE）では、それぞれデータセキュリティに必要な技術的・組織的措置を講じるためにかかる費用と、データ保護の目的との比例関係の判断は異なることになる。(17)

2　連邦データ保護法九条一項の附則

(1)　連邦データ保護法は、個人データを自動的に処理する場合、とくにコンピュータ処理の場合について九条に附則を置いている。附則では、以下の一〇の原則が、施すべき措置として挙げられている。(18)以下に、条文の邦訳を掲げコメントを付しておくが、コメントは現時点での技術を前提に原則を読んだものである。

①　立入りの管理：個人データが処理されるデータ処理施設への無権限者の立ち入りを禁止すること。

【コメント】　建物、コンピュータ等「物」へのアクセスの管理であるが、これについては、施設への身体的なアクセスと理解されていること、施設が分散している場合には難しく（各自のパーソナルコンピュータを想起せよ）、集中的施設ではサーバーなどを通じて行い易い。

②　データ媒体の統制：データ媒体が、無権限で解読、複写、変更、除去される可能性を防ぐこと。

【コメント】　デスクレスのワークステイションの導入や退出時のコントロールが基本とされているが、例えば、デスクの持ち出し、持ち運びの最少化のような日常的な措置が重要とされる。(19)

③　記憶装置の管理：記憶装置への無権限の入力ならびに蓄積された個人データの無権限の読み取り、変更または消去を防ぐこと。

【コメント】　ここでの有効な措置が、身分確認や認証システムを前提とした、暗号鍵の制度である。

④　利用者管理：データ処理システムがデータ伝送装置（例えば、端末装置の接続）を通じて、無権限の者に

より利用される可能性の排除。

【コメント】　ここでも、身分確認や認証システムの存在が前提となるが、利用者管理のためには、アクセスをアクセス地点ごとに審査・妨害できる設備が必要ということになる。

⑤　アクセスの管理：データ処理システムの利用権限を有する者のみが、独占的に、そのアクセス権限の下にあるデータにアクセスできるということを保障すること。

⑥　提供の管理：個人データがデータ伝送装置によっていかなる機関に提供される可能性があるのかにつき審査及び検証できるということの保障。

【コメント】　提供可能性の制限が不可能であれば、すべての提供を記録しなければならないが、実際は、データの類型ごとにプログラムを変えて、データ類型ごとに提供できる範囲を変えることは可能である。

⑦　入力の管理：いかなる個人データが、いかなるときに、いかなる者によってデータ処理システムに入力されたかを事後に審査及び検証できるということの保障。

⑧　委任の管理：委任に基づいて処理される個人データが、委任者の指示に適合する場合にのみ処理されうることの保障。

【コメント】　契約の履行の確認がポイントであるが、抜き打ちの検査等によらない限りその確認は困難である。(20)

⑨　移送の管理：個人データの伝送ならびにデータ記載物の移送に際して、データが無権限で解読、複写、変更、消去される可能性の排除。

【コメント】　ここでももっとも有効的な手段がデータの暗号化である。勿論、移送の記録管理が行われることを前提としている。

⑩　組織管理：官庁若しくは企業の組織を、データ保護の特別の要求に応じられるように構成すること。

【コメント】　データセキュリティの大半は、技術的な措置よりも行政あるいは企業内部の組織的な措置により達成されるという。そして、執られるべき措置は、組織の態様、組織の任務、組織の構成に左右されることになる。いかなるデータを（外交・防衛データ、治安関係データ、企業秘密、個人データなど）、いかなる組織が扱うかにより具体的措置は異なることになる。一般的な具体的措置としては、休暇や入院に関わる関連規定の整備、周辺装置（ファックスやプリンター）へのアクセス管理、セ

ンシティヴなデータを扱うときの監視体制などが挙げられている。

(2)　一九九〇年法の附則は、一九七七年法のそれを若干修正しているものの、基本的枠組みは変わっていない。すなわち、これらの要請は、行政や企業が日常的に行うべきことから、かなり高度のセキュリティを要する組織でなければ対処できないと思われるものまでを射程に入れた一般的なものであるということができる。

この附則は、具体策をデータ処理機関に委ねており、問題の多様性と技術の発展に対する柔軟性を有する規定の仕方であるともいえよう。しかしながら、次のような実務からの批判があることも指摘しておきたい。第一に、右の要請は実務における補助としては不十分であるという批判[21]である。一個のセキュリティ計画を策定するためには、危険の分析評価が不可欠であるが、附則の要請はそのための指針としては具体性を欠くということであろう。実際、ドイツでは、分析・評価からセキュリティ施策を組み立てるという作業は、一九八〇年代に民間部門におけるデータ保護管理実務において展開してきている。第二は、より根本的な批判であって、一九七七年法の附則のカタログ自体が、既に当時、急速な社会のコンピュータ化を前に暫定的なものとしての性格しか持ち得ないと評価されていたのに、一九九〇年法でもその内容に変化がみられないことに対するものである。すなわち連邦政府は、職場におけるパーソナルコンピュータの日常的な利用、大規模なデータバンク・情報システムの進展、コンピュータの処理速度の飛躍的向上に伴うデータの利用可能性の拡大、光デスク、CD-ROMなどの新たなデータ媒体の登場、世界的なネットワークの出現、いわゆるウイルスやハッカーによるシステム侵害といった事実を認識していたが、データセキュリティの問題はデータ保護（情報の自己決定権という人格権の保護）にとり、周辺的なあるいは副次的な効果しかもたないであろうと評価していたという批判である。一九九〇年法施行後の展開はこの批判を裏付けているとも言えるが、技術はもはや一般原則では対処できない地点にまできたという認識が立法者にあったという見方もあるように思われる。

3　シュレスヴィヒ＝ホルシュタイン州の試み[22]

(1)　シュレスヴィヒ＝ホルシュタイン州は、一九九二年データ保護法[23]の改正に合わせ、連邦に先駆けて、個人

データ保護法の領域において、コンピュータ社会に適合したデータセキュリティシステムを構想したといわれる。それは、公的部門に限られたものであるが、具体的には、データ処理施設に次のような措置の義務づけないし確立を要求するものである。①特別のセンシティヴなデータの処理の際のセキュリティ分析、②決定面と処理面の分離、③パーソナルコンピュータ利用に際してのセキュリティのためのソフトウエア使用の義務づけ、④システムプログラムの変更の記録、⑤行政庁の外部に出されるデータの暗号化、⑥資料作成についての最小限の要請の定義、⑦記録資料の保存期間の確定、がそれである。これは、州のデータ保護監察官の強い要請の賜であるとされている。

(2) これらの要請は、一九九四年九月一三日施行（経過規定がある）のデータ保護命令に広く取り入れられるところとなった。

データ保護命令は六つの基本原則あるいは構想から成り立っている。第一は、すべての行政庁に対する統一的な規制の創設である。これまでは様々な形式で行われていたデータ処理のための規制が、命令という法形式で、州、自治体、州の監督に服するすべての公的機関に一律に適用されることになるわけである。第二は、最少の要求の確立である。これは、自動化された行政の過程・執行に対する最低限の要請を明らかにしようというものである。第三は、データ処理の専門家によって達成された水準に合わせるという目標設定である。従前は、行政庁は、大多数のデータ処理施設が行っている以外のことを行う必要はなかったということである。第四は、費用負担者（納税者）に対するセキュリティ責任の強化である。第五は、データ処理施設と手続利用者の責任の分離である。自動化された手続の発展と運営は利用者（各専門部署）に対するサービスとみなされるが、それは本来の行政手続（例えば、行政行為の発布）からは独立したものである。したがって、組織内で、少なくとも両者の責任の範囲を論理的に詰めておくことが必要というわけである。第六は、形式に係る規定を置かずに、目標基準の定義を置くことである。つまり、行政課題・過程の多種多様性に鑑みれば、できることは、特定の許可手続規定を置くことではなく、専門家である第三者による検証のみであるという認識に立つ構想である。

(3)　データ保護令では、右の構想が具体的に明定されているわけであるが、ここでは、そのうちの幾つかのものを見ておくこととしたい。

①　規定どおり（ordnungsgemäß）の定義　自動的手続による行政庁の個人データ処理が「規定どおり」であるといえるためには、データ処理が現行法に合致している、セキュリティ構想が存在する、プログラム及び手続が文書で示されている、テストが済んでいるという諸条件を充たしていなければならない。

②　追跡可能な記録の作成義務　自動化された手続の記録は、少なくとも、その時々の事務、使用したプログラムの記載を含む手続の経過、プログラムと手続のテストの記述を含んでいなければならない。

③　記録の保存期間の確定　機械処理の結果が完全に紙の形で存在する手続にあっては、記録資料は、当該プログラムによってデータにアクセスがなされる限り保存されなければならない。もっぱら自動化されたデータファイル内でデータを作成する手続にあっては、記録の保存義務は、データの消去（又は出力）まで存在する。データを他の機関に提供する手続にあっては、保存期間は少なくとも六年間となる（提供データが可読な形で存在している場合を除く）。

④　危険分析　特別の服務上のあるいは職業上の秘密に該当する、あるいは特別に保護に値する個人データが、自動的に処理される場合には、危険分析においてセキュリティ措置とともに、当該セキュリティ措置を通して、いかなる理由によりいかなる危険が除去されるかが記述されなければならない。

⑤　データファイルの暗号化の義務　持ち運び可能なコンピュータの場合には、盗難などに備えて、データファイルを暗号化しなければならない。

4　パーソナルコンピュータとデータセキュリティ

(1)　連邦データ保護法九条、同条附則に示されているデータセキュリティ措置は、コンピュータの大きさを区別しているわけではない。したがって、パーソナルコンピュータにも当然適用されることになる。けれども、シュレスヴィヒ＝ホルシュタイン州の例を引くまでもなく、連邦データ保護法の要請がパーソナルコンピュータについては修正されなければならないことを疑うものはいないであろう。(24)

要するに、パーソナルコンピュータの場合には、使用者及び関係者を権限なきアクセスから保護するという観点（職場の誰でもが触れる、デスクのコピーも容易になる、同一機種・同一システム・ソフトを使用している場合にはさらに簡単になる）からも、またデータ処理権限を有するものが不法な使用をするという観点（独立の作業形態、相互監視の不能）からも、データセキュリティは困難になるのである。これをセキュリティの目的との関連でいえば、パーソナルコンピュータの導入は、監督可能性の問題を大きく変えていることになる。パーソナルコンピュータの場合には、組織と個人の間に機能的な分離を認めることは困難だからである。利用者のみがシステムの利用権を有しているといってよいからである。さらに、ウイルスが簡単に伝染するという問題もある。そして、パーソナルコンピュータの軽量化・小型化つまりノートブック型等の携帯型機種の登場が、この問題をさらに複雑なものとしているというわけである。

連邦データ保護法九条の附則の実施について、パーソナルコンピュータを前提としたデータセキュリティ措置としては、パスワードの工夫にはじまり、個人所有のコンピュータの仕事場への持ち込みの禁止、センシティヴなデータのシステム管理者による処理など多くの提案がなされている。しかしながら、これらの実施は必ずしも徹底していないようである。

(2) ネットワークの運営の場合には、データ交換のために、基幹施設の利用がすべての人に開かれているという原則から生じる問題がある。ネットワークの参加者は、どのルートで自己のデータが流れるか、どこで中間的に蓄積されるかコントロールすることはもはや不可能であるといってよい。それゆえ、データ保護立法によって保護されているデータがネットワークを通じて提供される場合には、信頼できるシステムの運営がなされなければならないのである。その具体策として、暗号鍵の利用が論じられているのである。同時に、パーソナルコンピュータによるネットワークの利用に際しては、データ処理の対象となる当事者の個人データとともに、ネットワークの利用者の個人データも保護されなければならないという問題も忘れられてはならないであろう。

ところで、システムの実際の運用において最も重要な役割を果たすのは、システム管理者である。そこで、シ

ステム管理者をどう管理するかという問題もデータセキュリティを語る場合には論じておく必要がある。システム管理者は、当該システム上の全てのデータファイル及びプログラムに無制限にアクセスできる可能性があるし、そうでなければ迅速にその職務を全うすることができないであろう。そうであるとすると、その権限の濫用の可能性も考慮にいれたセキュリティ措置を講ずるべきであるということになる。ネットワークの大小を問わず、「信頼する」のが唯一の対策であるという状況は改められなければならない。例えば、連邦データ保護監察官は、システム管理者の権限を複数人に分配し、管理者自身はアクセスできないあるいは単独ではアクセスできない記録をとるシステム・ソフトウエアの使用を勧めている[25]。その必要性の判断については、既に触れたところ（三―3―(1)）が当てはまる。

5　連邦情報技術安全庁

本稿で度々言及している技術的要求に関連して、ドイツでは、一九九一年に、情報技術における安全性のための連邦局（Bundesamt für Sicherheit in der Informationstechnik（BSI）、以下「情報技術庁」と略す）が、連邦上級官庁として設置され、連邦内務省の下に置かれている（設置法一条）[26]。この法律にいう情報技術とは、情報の処理または伝達のためのすべての技術上の手段をいい（同法二条一項）、情報技術におけるセキュリティとは、情報の利用可能性、無傷性、信頼性に関わる一定のセキュリティの水準を、①情報技術上のシステムあるいはシステムの構成要素の内部において、そして、②情報技術上のシステムあるいは構成要素の利用に際して、セキュリティ措置を通じて維持することをいう（同条二項）。その所掌事務は、情報技術を適用する際の危険分析、セキュリティ措置の開発（三条一項一号）、セキュリティの審査・評価のためのメルクマール・手続・道具の開発（同項二号）、システムのセキュリティの審査及び評価、並びにセキュリティ認定書の発行（同項三号）、連邦又は連邦の委託による企業が公的に秘密の保持を要する情報（暗号事項）の処理又は伝達のために使用するシステムの許可、及び公開鍵の作成（同項四号）、情報技術セキュリティに権限を有する連邦の官庁の支援、とくに連邦データ保護監察官の支援の優先（同項五号）、情報技術セキュリティに反する行為を防止する等、一定

の条件の下に書面で要請があった場合に限定された警察、検察、憲法擁護庁などの支援（同項六号）、セキュリティ相談（同項七号）である。三号にいうセキュリティ認定書（Sicherheitszertifikat）は、一定の条件の下に、情報技術システムの作成者や運営者に付与されるものである（同法四条）[27]。

また、情報技術庁は、一九九二年には、情報技術セキュリティのためのハンドブックを編集し、一九九四年には主としてパーソナルコンピュータを念頭においたハンドブックを編集している。内務省は、後者に収められている措置を編集して一般的勧告とする予定であるという[28]。

## 五　おわりに

個人データ保護との関係におけるデータセキュリティの問題について、わが国でも暗号・認証技術を前提とした議論は少なくない[29]。しかしながら、暗号・認証技術を語る以前に尽くすべき議論すなわち日常的なデータセキュリティの原則、とくに組織的なセキュリティ措置は、徹底されていないのが実情であるように思われる。暗号鍵が権限ある利用者対策としては万能ではなく、またデータの消去に対しても効果的でない以上[30]、公的部門・私的部門を問わず、マニュアル処理、自動的処理別の、そして対象データの性質に応じた、さらにパーソナルコンピュータの小型化を前提とした基本的セキュリティ措置が施されているか、今一度検証する必要があるのではなかろうか。とくに公的部門について言えば、わが国の場合にも、特殊なデータを扱わない通常の行政組織であっても、例えば、電子計算組織管理運営規程、小型電子計算組織管理運営規程が定められていることが多く、それらの規程はデータ保護管理者・データ保護責任者を置くことを定めるとともに、データセキュリティに関する条項（「必要な装置を講じなければならない」とする規程が多い）を一応含んでいる。さらには、データ保護管理者からのデータ保護責任者に対する通知という形で、パソコン・ワープロ等小型電子計算組織に係るデータ保護についての定めをもつ自治体もある（ここでは、ある程度具体的なセキュリティ対策が書き込まれることもある）。けれども、右の規程は概略的なものであることが多く、相互信頼に基づく管理体制の下で、フロッピーディスクの管理等にはじまるセキュリティの具体的装置が定

められ、実施されているかという問題があるように思われる。

（1）八原則については多くの文献があるが、さしあたり、総務庁行政管理監修『新訂版　逐条解説　個人情報保護法』（一九九一、第一法規）三五九頁以下参照。ちなみに、安全保護原則は、わが国の個人情報保護法（行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律）にも五条一項に努力義務規定として存在する。

（2）堀部政男『自治体情報法』（一九九四、学陽書房）二五三頁。

（3）OECDは、①責任原則（主としてセキュリティに関わる者の責任の明確化）、②認識原則（情報システムに対する認識を高める）、③倫理原則、④観点多様化原則（技術、行政、組織、法制などの総合的検討等）、⑤比例原則（安全性のレベルと情報システムの重要性・危害の程度等との均衡）、⑥統合原則（一貫したシステムの構築）、⑦適時原則、⑧再評価原則（周期的な見直し）、⑨民主主義原則の九つの原則を立てている。本稿のドイツの議論と重なる部分も多いことを指摘しておく。

（4）例えば、松井充「暗号・認証技術」電子情報通信学会誌、Vol. 79 (1996) No. 2, pp 107-114, 電子情報とネットワーク利用に関する調査研究会編『高度情報通信社会　日本の岐路』（一九九六、第一法規）一三四頁以下参照。

（5）したがって、本稿では個人データ保護を超えた企業秘密などのデータセキュリティの問題は扱っていない。

（6）ドイツの個人データ保護法制については、堀部政男編『情報公開・個人情報保護』（一九九四、有斐閣）二八七頁以下（藤原静雄執筆）参照。

（7）Similis u. a., BDSG-Kommentar § 9 Rdn. 3, 1995.

（8）H. Auernhammer, Bundesdatenschutzgesetz, 1993, Einf. Rdn. 5.

（9）このような観点から、データセキュリティ法制の設計を試みる論考として、多賀谷一照「情報セキュリティ」岩波講座・現代の法一〇巻『情報と法』二一三頁以下がある。

（10）BfD-Tätigkeitsbericht 1993-1994, S. 404 ff. 本稿の記述は一九九五年に提出された資料に基づくものである。最近二年間の活動報告書はまだ公にされていない。したがって技術面の記述は補正の必要があるかもしれないことを、予めお断りしておく。

（11）Ebenda, S. 218 ff.

（12）Ebenda, S. 258 ff.

（13）例えば、一九九四年三月九・一〇日に、連邦と州のデータ保護監察官の合同があり、そこで保健制度におけるチップカードの使用について議論している。

（14）医療関係者による研究として、わが国では、愛媛県西条市の「西条市保健医療福祉情報システム」に係る実験が著名である。

（15）体系と手続に関しては、Tinnefeld/Ehemann, Ein-

führung in das Datenschutzrecht, 1992, S. 249 ff. を主として参考にした。

(16) 連邦データ保護法の改正法の翻訳として、野村武司「改正ドイツ連邦データ保護法」山梨学院大学社会科学研究一二号一二三頁以下、旧法の翻訳として、藤原静雄「西ドイツ連邦データ保護法」國學院法学二七巻一号五一頁以下を挙げておく。

(17) Simitis u. a., a. a. O. (Fn. 7), Rdn. 30. わが国の行政実務で、センシティブなデータについての処理を行う場合にも、同じことが妥当すべきであろう。

(18) 以下の記述は、Simitis u. a., a. a. O. (Fn. 7), Auernhammer, a. a. O. (Fn. 8), Tinnefeld/Ehmann, a. a. O. (Fn. 14) によるが、コメントはわが国の実務も踏まえてのものである。

(19) したがって、わが国の自治体間でみられたという、オンライン結合が禁止されているためにデスクを持ち運びして職務共助が必要な行政庁に出向くという実務は、ドイツ人の目からは驚くべきことということになる。

(20) わが国の場合にも、例えば、委託された業者がデータを確実に破棄していることは、職員がそれを現認する以外に確認する方法はない。

(21) Datenschutz-Berater, 1995 Nr. 4, S. 1 ff.

(22) Ebenda, S. 3 ff.

(23) 一九九一年一〇月三〇日に改正され、一九九二年一月一日より施行されている。

(24) P. Volle, 8 9 BDSG als irrealer Maßstab für PC, CR 1992, S. 500 ff.

(25) BfD-Tätigkeitsbericht, a. a. O. (Fn. 10), S. 425. わが国の場合にも、管理者のアクセスを制限するシステムを採用している自治体（例えば、神奈川県保健福祉情報システムなど）もある。また、民間部門の場合には、例えば、組織内のランが閲覧されていないかという別の問題も考えられる。

(26) Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz-BSIG) vom 17. Dezember. 1990, BGBl. I 1990, S. 2834.

(27) わが国でも、例えば通産省の「情報処理サービス業電子計算機システム安全対策実施事業所認定規程」（告示）などが存在するが、他の領域と同じく縦割りである。

(28) BfD-Tätigkeitsbericht, a. a. O. (Fn. 10), S. 429.

(29) 例えば、前掲註（4）・電子情報通信学会誌の特集を見よ。

(30) P. Volle, a. a. O. (Fn. 24), S. 504. なお、暗号鍵については、フランスやサウジアラビアのように、国家のコントロールの下におくのかという問題と、国際的な標準化をどう考えるかということが、ドイツでも議論されている。Vgl. Datenschutz-Berater, 1996 Nr. 1, S. 1 ff.

（國學院大学教授）