講　演

# コンピューター犯罪と一九八六年の西ドイツ刑法改正

クラウス・ティーデマン
丹羽正夫
城下裕二　訳

経済犯罪と、ある社会の経済的・社会的状態との間の因果連関は、多くの要因から成っておりますが、こうした因果連関のなかで、技術の絶え間ない進歩は新たな種類の要因となっております。たとえば、モータリゼーションと道路交通量の増大は、刑法および刑事司法を新たな問題に直面させました。それとまったく同じように、機械装置の経済や行

政への導入と普及は、一般に合理化や進歩をもたらすと同時に、新たな種類の犯罪行為を犯す機会や手段をも生み出しているのであります。

本講演では、コンピューター犯罪の例を手がかりにして、こうした問題領域を犯罪学的および刑法的観点から概説したいと存じます。コンピューター犯罪は、それが国際的な現象であるという点だけをとってみても、比較(法)研究の対象として魅力的なものといえます。そしてこのコンピューター犯罪という国際的現象は、――その発現形式には様々な相違がみられるにもかかわらず、――本質的には各々の経済システムのあり方から独立したものであり、傾向としてはコンピューターが使用されているところではどこでもみられるのです。(1) コンピューター犯罪が比較法的観点からとくにアクチュアルなテーマになっているもうひとつの理由は、なかんずくそれが過去一〇年間に、様々な国際機関（とりわけOECDやヨーロッパ審議会(Europarat)）の広範囲にわたる活動を生み、多数の国において立法上の改正措置にもつながったということであります。――コンピューターに関連する経済犯罪対策のために刑法を改正する法律案は、過去数年間になかんずくデンマーク、スウェーデン、アメリカ合衆国、イギリス、オーストラリア、カナダ、日本および西ドイツで可決されました。そして(日本でさらに立法上の考慮が重ねられているほか)、これと同様の改正案が、とくにフィンランド、フランス、ノルウェー、ポルトガル、オーストリア、スコットランド、スイス、そしてまた南アメリカでも議論されております。もし我々が――犯罪学的および刑法的観点からは、従来等閑視されてきたのではありますが――電子的データ処理(EDV)の分野における私的領域（「プライバシー」）の法的保護をも含めて考えるとしますと、(2) さらに広い範囲で議論がなされていることになります。すなわち、この問題を含めて考えますならば、かなり多くの法領域において、経済や行政におけるコンピューターの使用の増大により、新たな(刑)法的規制や(刑)法改正についての

検討がなされているといえるのです。

以下、本講演ではまずコンピューター犯罪の概念および現象形式、原因、発生頻度および暗域(Dunkelfeld)、被害の規模および行為者の範囲を第I部で論じ、続いて第II部では、これらに関連する法的諸問題を、新しく改正された西ドイツ刑法におけるその解決をも含めて論じたいと存じます。そして最後に、ドイツにおける改正立法の全体的評価を、先述のOECDやヨーロッパ審議会による提案にも照らしつつ、第III部で行なうことにいたします。

## I　コンピューター犯罪の概念と現象形式

OECDの定義するところによれば、コンピューター犯罪という概念で言い表わされるのは、自動的データ処理システムないしデータ通信システムに関連してなされる、法規に違反し、倫理的に非難すべき又は許容されないすべての行為態様であります。(3)

この定義はまず第一に、コンピューターを用いたデータの収集・貯蔵・連結および転送により、市民のプライバシーを脅かす諸事例に及ぶものであります。もっとも、この点に関するかぎりでは、コンピューターに貯蔵されたデータの利用による重大な人格権侵害の事例は、西ドイツではごくわずかしか知られておりません。それにもかかわらず、西ドイツの立法者は一九七七年一月二七日の連邦データ保護法(Bundesdatenschutzgesetz vom 27. 1. 1977)により、この――きわめてあいまいに――データ保護と称される対象(Materie)を、諸外国の例にならって法律上包括的に規定し、これを(まったく不明確な)処罰規定によって補強したのでした。(4)西ドイツと同様に日本もプライバシーの保護に関す

るOECDのガイドラインに署名いたしましたが、日本でも現在このような法律の立法化が進められております。

他方、コンピューター犯罪におきましては、一九八六年五月一五日の第二次経済犯罪対策法（2. Gesetz zur Bekämpfung der Wirtschaftskriminalität＝2. WiKG）によって、一九八六年八月一日の同法施行以来西ドイツではとくにとり上げられるようになった、自動的データ処理を利用した財産侵害の問題が重要であります。この問題領域については、日本でも今年の六月に刑法的規制がなされるに至りましたが、以下の論述はこの第二の問題領域に限定して行ないたいと存じます。そのさい、証拠の収集や外国との司法共助といった手続的問題はとくに取り上げません。なぜなら、こうした点に関するかぎり、ヨーロッパでは法的問題はごくわずかしか生じていないからであります。

コンピューター犯罪の問題をめぐる西ドイツの議論のはじめには、そもそもそのような犯罪が存在するのかという問題がありました[5]。今日では、なかんずくズィーバー（Sieber）が一九七四年以降フライブルク大学の犯罪学・経済刑法研究所で行なった調査に基づき、コンピューター犯罪というものの存在を証明するものとして、西ドイツや諸外国における多数の刑事訴訟を挙げることができます。ズィーバーは一九八〇年までに全部で五〇の事例を記録化いたしました[6]。それ以来西ドイツでは、数百のソフトウェアの窃取（Software-Diebstahl）の事例および多数のキャッシュ・ディスペンサーの不正利用（Bankomaten-Mißbrauch）が知られるに至っております。日本の警察による調査も国際的レベルでとくに注目されたものですが、その最近のデータによりますと、年間約一、〇〇〇件のコンピューター犯罪が記録されています。この日本の警察による調査もまた、コンピューター犯罪という新しい形の不正行為の実態を、説得力ある仕方で証明しているのであります。

コンピューター犯罪とその発生件数の問題が特別の意義を有するのは、単に、決済過程(Abrechnungsvorgang)の自動化が進んでいることだけがその理由なのではありません。むしろ重要なのは、コンピューターの製作者のみならず、とくにコンピューターの利用者が、セキュリティの面を長い間きわめてないがしろにしてきたということなのです。[7] それゆえ、過去数年間におけるコンピューター犯罪の発生件数は、相当な量にのぼるものであったと推測せざるをえないのであります。とりわけ――ただし、もっぱらというわけでは決してありませんが――銀行経営においては、コンピューター犯罪の応用範囲が無数に生じております。そして、銀行経営の分野におけるコンピューター犯罪の危険は、書類の不要な支払勘定システムを導入しようという経営プランが実現されれば、さらに大きなものとなるでしょう。現在、決済施設の外国への移転や集中がすでに実施されておりますが、このこともまた、刑事訴追を実際上のみならず、法的にも困難なものにするのであります。データ処理の分野における暗数については、大まかな評価を下すことさえ実際上は不可能であると思われます。我々が知りえた西ドイツにおける刑事事件では、コンピューター犯罪の発覚は、ほとんどが単なる偶然によるものであったのです。また、一般に、発覚した事件に限っていえば、告発がなされないことがしばしばあります。なぜかと申しますと、(とくに銀行がそうですが)事件に関係した企業は、このような犯罪が明るみに出ることによる信用の低下を恐れるからなのです。またこれに加えて、行為者が自由刑に処せられてしまうと、行為者が事件後も仕事を続けてかなりの収入を得る場合よりも、発生した損害の賠償が困難になってしまうため、告発はあまりなされていないのであります。

これまでに知られているさまざまな事例のなかでは、五つの特殊な犯罪群がとくに目立ったものであります。[8] 以下、この五つの類型につき順次説明いたしますが、ここでは一般的な経済犯罪(たとえば貸借対照表にからむ犯罪や、税法

事犯、保険金詐欺など）を犯すさいのコンピューターの使用は、とくに考慮しないことにいたします。

1　コンピューター犯罪に関する犯罪学的議論の中心になっているのは、不正操作（Manipulation）であり、これはデータの入力段階のみならず、データの処理段階にも、そしてまた出力段階にも関連しうるものであります。入力の不正操作はインプット不正操作（Input-Manipulation）とも呼ばれ、また出力の不正操作はアウトプット不正操作（Output-Manipulation）とも呼ばれます。そして、データ処理段階での改ざん（Fälschung）は、プログラム不正操作やコンソール不正操作の形で行なわれるのです。これらに対して、データ処理施設の機械的部分をなす、いわゆるハードウェアの不正操作は、実際上さほど重要なものではありません。

インプット不正操作の例としては、西ドイツではじめて訴訟で争われたコンピューター犯罪の事案を挙げることができます。[9] 本件の被告人は、バイエルン労働官署で児童手当係の事務担当者として働いておりました。他の担当者のイニシャルを偽造して、被告人は五千マルクから一万マルクの児童手当追加支払金を、不法に自己のいくつかの口座ならびに家族の口座に振り込んだのでした。被告人はおよそ十カ月間にわたってこのような不正操作を二九回行ない、それによって被告人と、被告人同様に手当を受け取っていた八〇歳を越える彼の祖父母は、二五万マルク以上の児童手当を受領したのであります。被告人は一九七三年に、背任の連続犯、文書偽造の連続犯および職務上の不実記載により、三年の自由刑に処せられました。不正操作の発覚は偶然によるものでした。すなわち、被告人が口座を持っていた銀行の取締役が、被告人の上司も同席していた飲食店の常連席で、子供がたくさんいることによって金持ちになれる旨を冗談半分にほのめかした（ことが事件発覚のきっかけとなったのです。被告人の上司が発言の趣旨をたずねたところ、取締役

は、銀行の顧客の一人が高額の児童手当の支払いを受けていることを示したのでした。被告人の上司はこれを不審に思い、翌日すべてのリストを再検査したところ、被告人が不正操作をしていた事実が浮かび上がったのであります[訳注(1)]。

プログラム不正操作の例としては、南ドイツのある事件を挙げることができます。[10] 本件の被告人は、ドイツのある大きな株式会社でプログラマーとして働いておりました。彼は特別に作成したプログラムを用いて、同社のデータ記憶装置に架空の人物の給与データを入れ、この架空の人物の給与が振り込まれる口座として自分の口座を指定したのです。この給与の不正操作は、こうした簡単な方法によるだけでも多くの会社でうまくやりとげることができたのですが、しかしながら、事件のあった会社では発覚してしまう可能性がありました。それと申しますのも、同社ではコンピューターによって、綿密に検査・評価された給与支払票、照合簿（Kontrolliste）、経理一覧表および貸借対照表が作成されていたからであります。そこで被告人は、給与支払票等に関する不正操作の発覚を妨げるために給与支払プログラムを変更し、架空の同僚に対する支払いについては給与支払票がプリントアウトされぬようにするとともに、その支払いがコンピューターによって作成された照合簿にも表われぬようにしたのです。さらに被告人は、同社の経理一覧表と貸借対照表を作成するプログラムをも不正操作いたしました。それによって彼はついに、着服した金額が税務署に納付すべき給与所得税からは差し引かれ、それゆえ同社の経理一覧表および貸借対照表において不足額として目につかないようにするのに成功したのです。やはり偶然によって不正操作が発覚するまでに、被告人は約一九万三千マルクを不正に得たのであります。彼は詐欺の連続犯および背任の連続犯により、二年の自由刑に処せられました[訳注(2)]。

多方面に影響を及ぼしたヘルシュタット銀行（Herstatt-Bank）の倒産に関連してなされたコンソール不正操作は、お

そらく最もセンセーショナルなものであったと言ってよいでしょう。[11] ヘルシュタット銀行では、かなりの範囲にわたって、外国為替取引が銀行のコンピューターに入力されなかったり、あるいは遅れて入力されたりしたのです。そのさい、確認書やパンチテープへの記録は、いわゆる中断キーを押すことによって妨げられました。これによって損失は隠蔽され、取引の総量と、いわゆるネットポジション(Nettoposition)は外見上低く保たれたのです。こうした方法によって、ヘルシュタット銀行では数十億ドルにのぼる金額が記録されないか、あるいは正しく記録されなかったのであります。[訳注(3)]

近年ますますその使用が増大しておりますデータ遠隔処理システムは、上述のような不正操作のテクニックの、きわめて興味ぶかい、そしてまた前途に多くの可能性をはらんだヴァリアンテを生みだしております。すなわち、コンピューターが公の電話回線ないし専用回線を経由してデータ遠隔処理システムと接続されている場合には、行為者は被害をこうむった企業にみずから侵入する必要はなく、自分の端末機を用いて不正操作を自宅から行なうことができるのです。これに関する事例といたしましては、あるアメリカの学生による不正操作を挙げることができます。この学生はすでに七〇年代に、自宅から公の電話回線を経由して Pacific Telephone Corporation のセントラルコンピューターにアクセスし、総額約百万ドルにのぼる商品を無償で交付させることに成功したのであります。[12・訳注(4)]

以上述べましたような諸事例にもとづくだけですでに、コンピューター犯罪のさまざまな特徴が明らかになってまいります。すなわち、まず第一に――古典的な財産罪におけるのとは異なり――コンピューター犯罪では行為とその結果が通常離ればなれであり、このことが犯行の発覚を著しく困難にするのであります。さらに、コンピューター犯罪の継続的効果(Dauerwirkung)ということがこれに付け加わります。つまり、所為がもし第一回目に成功したといたしま

すと、それはしばしば――とくにプログラム不正操作や、いわゆる固定データ(Stammdaten)[訳注(5)]の不正操作の場合――、偶然ないし的確な検査により発覚するまで継続的なものとなるのです。そしてこの場合、事後的に個別の検査を行なってもほとんど意味がありません。なぜかと申しますと、コンピューターにより処理された作業過程は莫大な数になりますから、こうした個別的検査はきわめて大きな労力を要するものになるでありましょうし、そうなると結局、コンピューターにより達成された効率化を台なしにしてしまうからであります。

たった今述べましたことから、コンピューター犯罪により発生した被害がきわめて大きなものになる傾向が明らかとなってまいります。

以下で述べますような、その他の事例群におきましても、被害の規模や犯行の態様といったことから、新たな様相が浮かび上がってくるのであります。

2　データ処理の領域における産業スパイ（コンピュータースパイ）を容易にしているのは、データがきわめて狭いスペースに貯蔵されており、ただちに他のデータ収録材に移すことができるという事実であります。ここで無権限のデータ利用の中心になっておりますのは、いかなる分野・領域におきましても――ソフトウェアの窃取とも呼ばれる――コンピュータープログラムの無権限利用です。――コンピュータープログラムは、その作成にしばしば多大な作業コストを必要といたしますし、営業上の重要なノウハウを含んでいることもまれではありません。そのほかに重要なものとしては、なかんずく研究データ、顧客データ集積庫(Kundendateien)および貸借対照表が挙げられます。次に、ソフトウェアの窃取の事例として、いわゆる現金徴収プログラム事件を御紹介いたしますが、本件は、コンピュータープログラム

に著作権の保護が及ぶかという、かつて激しく争われていた問題につき連邦通常裁判所が判断を示したもので、それゆえにきわめて重要な事案であります。(13)

本件の被告人Tは、ある現金徴収会社のフリーのスタッフとして、同社の従業員と共に複雑なプログラムシステムを開発したことがありました。このプログラムシステムには、同社が何年もかけて作成した重要なデータ集積庫も、その一部として組み入れられたのであります。プログラム作成上の必要から、Tは同社の電算機センターへの自由な立入りを、週末に特別に許されたことが何回かありました。一九七九年の暮れに同社はたまたま、すなわち、新任の電算機センター長が行なったチェックによって、Tが一九七九年一〇月一三日に、同社のプログラムの最も重要な部分とデータ集積庫を、持参した磁気ディスクにコピーしたことを突きとめたのであります。これに基づいて開始された調査の結果、Tがその間に自分のデータ処理サービス会社を設立し、同社のものとかなりの範囲にわたって同一のプログラムシステムを、いくつかのライバル企業に提供していたことが判明いたしました。それとともに、当該プログラムシステムが他の二つの電算機センターですでに使用されていることを示す事実も明らかとなったのであります。

コンピュータースパイの新たな可能性は、西ドイツ国内の企業による産業スパイ行為ばかりではなく、諸外国による政治的スパイ行為にも利用されます。一例を挙げますと、西ドイツで一九七〇年代になされた、ある刑事訴訟においては、西ドイツ当局がとくに東ドイツによるコンピュータースパイの可能性を、かなり早い時期から認識していたことが明らかとなりました。この情報によりますと、すでに一九六四年に東ベルリンで「長期計画」が練り上げられていたということであります。そしてその内容は、後に情報部員になろうとする者にまずデータ処理の基礎教育を受けさせ、し

かる後に、西ドイツのデータ処理産業においてさらに訓練を継続する任務を与える、というものだったのです。[訳注(6)]

3　被害の規模という点からも、また犯行態様の点からも注目すべきものとしては、さらに、データ処理の領域におけるサボタージュの事例があります。これらサボタージュの事例も、コンピュータースパイの事例と同様に、データがきわめて狭いスペースに高密度に圧縮されていることにより容易となるのです。プログラムやデータの破壊は、たとえば火を放ったり、磁石や特別に作成された「消去プログラム」を用いたりして行なわれますが、プログラムやデータがすべて破壊されてしまうと、企業活動全体の継続が危うくなりかねません。サボタージュの行為者としては、外国の諜報機関、政治的狂信者、そして企業への恨みから復讐心に燃えている社員といったものが考えられます。

コンピューターサボタージュの例としては、西ドイツのGinsheim-Gustavsburgにあります MAN-Werkという会社の電算機センターで一九八三年に起こった、「革命分子」によるセンセーショナルな爆弾テロの事案を挙げることができます。本件爆弾テロは、「軍備増強」と軍需産業に対する抗議の表明として行なわれたものでありました。[14] テロリストによる同じようなテロ行為としては、なかんずくベトナム反戦運動と関連したアメリカ合衆国の事案が知られておりますし、後にはイタリア、フランスおよび日本の事案も知られるに至っております。

コンピューターサボタージュが、ハードウェアの物理的な破壊によってではなく、データの消去ないし変更によりなされる場合はどうでしょうか。こうした形のサボタージュについては、いわゆる「ウィルスプログラム（Viruspro-gramm）」によりひきおこされる危険が、西ドイツではとくに関心を集めております。この「ウィルスプログラム」は、プログラマーや第三者によってひそかに潜り込ませられるわけですが、ここで重要なのは、ウィルスに「感染した」コ

ンピュータープログラムを使用した場合に複製されるプログラム部分であります。ウィルスプログラムはこうして複製されることにより、コンピューターにストックされている他のプログラムやデータのなかに侵入していきます。そして――それがデータ処理システム全体に蔓延した後には――たとえばあらかじめセットされた時点に、全般的なデータの消去や、その他のサボタージュ行為をひきおこすことがありうるのです。産業や行政は、今日ではデータ処理施設に高度に依存しておりますから、こうした形のコンピューターサボタージュは、現代の産業社会を脅かすものとなるのであります。

4　これに対して、データ処理施設の無権限利用、すなわち、いわゆるマシンタイムの窃取（Zeitdiebstahl）は、それほど危険なものではありません。マシンタイムの窃取において被害者の財産的損害が問題となるのは、なかんずく他人の「客先番号（Account-Nummer）」を用いて計算を行なった場合であります。

マシンタイムの窃取の例としては、ドイツのある州の刑事局（Landeskriminalamt）により捜査手続が進められた事件を挙げておきましょう。本件では、ある州職員が、自分のデータ処理サービス会社を設立し、プログラム名とジョブ（Job）[訳注(7)]名を偽って、州のコンピューターにより臨時の計算業務を無断で行なった、として咎められたのであります。[15]

5　いわゆる「ハッキング（Hacking）」も、マシンタイムの窃取の特殊な事例群とみなすことができます。「ハッキング」という概念で言い表わされるのは、ふつう他人のデータ処理システムへの侵入でありまして、より詳しく申しますと、私腹を肥やす目的や、スパイ目的、あるいは損害を与える目的でなされるのではなく、単なる遊び心（Spieltrieb）から――たいていの場合「コンピューター狂いの」少年たちによって――なされるものをいいます。[16]

こうした少年たちの動機になっているのは、他人に自慢したいという個人的欲求なのですが、データ保護を改善しようという動機からハッキングがなされることもまれではありません。一九八四年にハンブルクで起こった、ドイツのビデオテックスシステム[訳注(8)]に関連する事件を例として、それを示すことができます。この事件は次のような内容のものでした。すなわち、ドイツ連邦郵便の代表者が、データ保護専門家会議の席上、ハンブルクのあるコンピュータークラブの会員たちがビデオテックスシステムの弱点につき述べたことを「ナンセンスだ」と評したため、同クラブの会員たちは一九八四年一一月一七日に、ハンブルクのある貯蓄銀行(Sparkasse)所有の、有料でビデオテックスシステムにより提供される画像情報(Btx-Seite)を入手してみせたのであります。会員たちの述べたところによれば、彼らはパスワードをシステムの欠陥により知ったのでした。彼らはこの画像情報を——九マルク九七の値段で——コンピュータープログラムごとに一三時間にわたって公衆に提供いたしました。こうした方法で彼らは、その後同クラブの会員が、一九八四年一一月一九日にハンブルク・データ保護評議委員室において事件を報道機関に知らせるまでの間に、約一三万四千マルクを同クラブの料金口座へ入金させることに成功したのです。

こうした少年層の「ハッカー」たちの動機は、しばしば無害なものなのではありますが、そうは申しましても、他人のデータ処理システムへの無権限の侵入は、次のような理由ひとつをとってみても無害なものとはとうてい言えません。すなわちその理由とは、他人のデータ処理システムへの無権限の侵入は、データを誤って消去してしまうことや、システムの封鎖につながることもまれではないということです。さらにまた看過されてはならないのは、ハッキングの成功が、不正操作やスパイ行為を実行しようという気を少年たちに起こさせることであります。

一例を挙げますならば、一九八二―八三年にベルリンで係属した、ある事件の捜査手続では、ドイツ連邦郵便がビデオテックスシステムの実地試験を一九八二―八三年に行なった間に、次のような不正利用が――一部は一六歳の生徒によって――上首尾に行なわれたことが明らかとなりました。すなわち、①自己の支出を減らす意図ないし他のビデオテックスシステム加入者（以下、加入者と略称――訳者注）に損害を与える意図をもって、他人所有の、有料でビデオテックスシステムにより提供される画像情報（以下、画像情報と略称――訳者注）を、犯行と無関係な加入者の勘定で手に入れる。②自己の料金口座への入金額をふやす意図をもって、自己所有の有料の画像情報を、他の加入者になりすまして自分で呼び出し、その料金を他の加入者に支払わせる。③画像情報を呼び出している加入者のデータをひそかに記憶装置に入れる目的で、いわゆる「データ落とし（Datenfallen）」を取りつける。④他の加入者による情報提供を妨害し、またその内容を変更する。⑤他人のデータの消去。⑥他人のパスワードの変更。その結果として、正当な権限を有するパスワード所有者は、もはや自分のシステムを使用できなくなりますが、犯人は手に入れたパスワードを用いて、他人の費用で作業を継続しうることとなるでありましょう。⑦送信者コードおよびタイトルコード（Absender- und Kopfzeilen angaben）を偽って、ビデオテックスシステムに侮辱的ないし脅迫的な情報を流す、等々といったことが行なわれたのであります。本件刑事手続は――一部は行為者の行為には可罰性が欠けるとの名目により、一部は行為者の証明が欠けるために、また一部は責任の軽微性を理由として――打ち切られたのでした。

（以上、丹羽訳）

## II　刑法上の対応

これまで述べてきましたコンピューター犯罪の概念は、新しい方法による犯罪行為が、そこで用いられる行為手段を基準にして犯罪学の見地から類型化されることを示しております。多くの場合コンピューター犯罪は、振替金、業務上の秘密、ノウ・ハウ、その他の情報といった、実体のない行為客体に関わります。従って、西ドイツのみならず多くの他の国々における従来の構成要件が、この新しい方法による犯罪をほんの部分的に、しかもごく稀にしか把えようとしていないことは、何ら驚くにあたらないのです。

もちろん西ドイツにおいては、処罰の間隙を埋めるために、現行の処罰規定を拡大解釈するという――基本法一〇三条二項によって広く禁止された――方法は採用されませんでした(17)。その代わりに立法者は、一九八六年五月一五日に公布された第二次経済犯罪対策法によって、特にコンピューター不正操作、コンピュータースパイ、コンピューターサボタージュ及びデータに対する無権限のアクセスに関する新たな処罰規定を導入しました。以下におきましては、これらの犯罪グループについて、まず――新法を本質的に理解するために――古典的な処罰規定の適用範囲と処罰の間隙を示し、次に各々の場合において、第二次経済犯罪対策法によって創設された構成要件について説明致します。

### 1　コンピューター犯罪対策における最も重大な処罰の間隙は、従来の法によってコンピューター不正操作を刑法上捕捉しようとする場合に生じます。例えば、いわゆる振替金は、フランス法やスイス法とは異なり、通説的なドイツの法観念によれば窃盗罪や横領罪の構成要件（刑法二四二条・二四六条）上の問題とはなりません。従って、ある金額につき、故意にかつ不法に銀行口座への振替、貸方通知ないしは銀行口座からの預金引出を行っても、窃盗罪や横領罪の

構成要件に該当しません。行為者は、貸方に記入された金額が支払われることによってその所有者になるため、現行法の所有権保護の構成要件は通常使えなくなってしまうのです。例外は、例えばキャッシュディスペンサーを不正使用するような特別な事例においてのみ考えられます。もっともこのキャッシュディスペンサーの不正使用といった特別な事例を、窃盗罪や横領罪、あるいは詐欺罪として処理することについては、ドイツの判例や学説において――日本と異って――多くの異論があり、今後連邦通常裁判所はデュッセルドルフ高等裁判所の提出決定（Vorlagebeschluß）に基づいてこの点を明らかにしなければなりません[18]。さらに、このような特別な事例以外でも、コンピューター犯罪に関する刑法上の諸問題は財産犯罪や偽造犯罪に集中しております。

ドイツ刑法によれば（広く諸外国においても）、詐欺罪の構成要件（刑法二六七条）は、人を欺罔して錯誤に陥れることを前提としております（これに対してフランス刑法は「欺罔手段」による行為で足りるとしていますので、その限りではコンピューター犯罪の場合もさほど問題はありません）。従って「コンピューターの錯誤」といったものは、ドイツ刑法上は考えられません。確かに、個々の事例において、事務処理者や決定権限者、検査官の介入から生じた数々の不正操作は、結局は錯誤のメルクマールを人の錯誤に限定することによって、詐欺罪の構成要件で捉えることができるでしょう。しかし、このような帰結は個々の事例の偶然性に依拠しているのであって、刑法二六三条によっても対処し得ない事例が少なからず存在する、ということを決して無視することはできないのです[19]。

また――ロマン法圏に属する諸法には伝統的に知られていなかった――背任罪の構成要件（刑法二六六条）も、二六三条によって生じた処罰の間隙を部分的にしか埋めることはできません。この構成要件は、企業外の人々と同様、パ

ンチャー、プログラマー、オペレーターを除外します。なぜならば、ドイツの判例上要求されてきた、活動の自由、一定の独立性、及び個人の責任といった要件が、彼らには欠けているからです。コンピューターのプログラミングは確かに高度の専門的知識を必要としますが、データ処理の結果に関しては、たいてい、裁量による判断を行う余地のない正確な指示を仰がなければなりません。従って二六六条は、通常はインプット・データを作成し検索する事務処理者にのみ適用可能となります。「補助事務処理者（Hilfssachbearbeiter）」について下級審判例は、一定の裁量の余地が存在する場合に、背任罪の構成要件該当性を肯定する傾向にあります。(20)

文書偽造罪（刑法二六七条）について西ドイツ刑法は、「物体化された、証拠となる事実の表示（verkörperte und beweiserhebliche Erklärung）」としての文書が、人の観念を表わしたものであることを必要としております。我々がこの要求に疑問を提起するといたしましても、コンピューターのデータとプログラムは、いずれにせよ文書とは言えません。なぜならば、電磁的に貯蔵されたデータは、可視的ではないからです。そのうえ、データからはしばしば作成者を知ることができず、また、企業内のプログラムや照合簿の場合は、文書の定義が要求しているような法律上の取引や証明制度のためのものではないこともあるからです。(21)

通説によって文書概念と人の観念の表示とが結びつけられていたために、技術的記録物の偽造という特別構成要件（刑法二六八条）が一九六九年に刑法典へ導入されました。しかし、従来の通説によれば、プログラム不正操作の場合に行為者によって変更されたコンピュータープログラムは、技術的記録物ですらありません。またインプット不正操作の場合にも、行為者は刑法二六八条三項が予定しているように「記録の過程に妨害的に干渉することによって記録の結果に」

影響を与えたことにはなりません。従って、技術的記録物という構成要件には、コンピューター不正操作の領域においては、結局きわめて狭い適用範囲しか妥当しないことになります。(22)

第二次経済犯罪対策法は、コンピューター不正操作の対策について、財産保護のみならず、偽造犯罪の領域においても処罰の間隙を埋めることになりました。まず詐欺罪の構成要件において生ずる財産保護の間隙は、コンピューター詐欺罪の構成要件（刑法二六三条a）によって除去されました。この構成要件の文言は、一般的な詐欺罪の構成要件の文言に厳密に則っており、欺罔行為と錯誤の惹起（die Täuschungshandlung und die Irrtumserregung）、及び――記述されていない――財産処分（die Vermögensverfügung）のメルクマールは、コンピューター使用の際に具体的な人の思考や行為の代わりとなるメルクマールによって置き換えられています。すなわち二六三条aによれば、「自己若しくは第三者に不法な財産上の利益を得させる目的で、プログラムの不実の作成、不実のデータ若しくは不完全なデータの使用、データの無権限使用又はその他データ処理過程の結果に影響を及ぼして他人の財産に損害を与えた者」は五年以下の自由刑又は罰金に処せられます。この構成要件の適用範囲は、データ処理過程の結果が、直接、財産上の損害を惹起した場合に限られるのです。つまり、財産上重要なデータ処理過程のみが含まれることになります。また構成要件に掲げられた手段を用いることによって、技術上必然的に「虚偽の」結果へと至るよう決定づけられたデータ処理過程は、二六三条の詐欺罪の構成要件における錯誤に基づく思考・決定過程に相当し、他方この「虚偽の」結果は二六三条における財産処分に相当します。立法者はこのような方法で、不都合な、予期し得ない範囲にまで処罰が広がることを回避しようとしたのです。

二六三条aの個々の場合の行為は、行為者が、コンピューターの技術的補助手段によって行われる財産処分に「影響

を及ぼす」ことです。これによって一方では、行為者は自らの行為により直接、財産処分を行う必要のないことが明らかになります。このことは、財産処分の内容が第一に（その後の）コンピューターの処理結果に依存しており、単に行為者の直接的なインプットによるのではない場合に見られます。またインプット段階では直接的に何ら関与せず、インプット段階のために虚偽のデータを提供するだけでも本罪の行為者となり得るのです。他方、影響を及ぼすことというメルクマールは、それがプログラム作成に対するものであっても、また、データ処理過程に対するものであっても、行為者が不正操作を行ったデータが処理過程で受理され、処理過程を共同決定しなければならないということを要件としています。さらに構成要件は、「それ――すなわち影響を及ぼすこと――によって」他人の財産に損害を与えることを必要としております。従って、行為者によって影響を受けたデータ処理過程の結果は、財産上の損害を与えることについての原因となっていなければなりません。

二六三条aの行為手段について述べますと、構成要件はまず「不実の、若しくは不完全のデータの使用によって」データ処理過程の結果に影響を及ぼすことを規定しています。このような行為態様によって、インプット不正操作の大部分が捉えられます。構成要件が、明文上さらに「プログラムの不実の作成」に言及しているのは、発見するのが困難で特に危険なプログラム不正操作が構成要件に該当することを明らかにしようとしているにすぎません。と申しますのは、プログラムは単に特別な種類のデータに過ぎませんから、プログラム不正操作はそれ自体既にインプット不正操作に含まれているためです。次に構成要件は、「データの無権限使用」という行為によっても実現され得ます。この、やっと補足的に挿入された行為態様は――一瞥しただけではわかりませんが――（私ティーデマンの[23]提案に従って）紛失あるいは窃取されたキャッシュカードが、無権限の第三者や、権限はあっても保証額を越えて使用しようとするカード所有者によって濫用される場合を特に捉えようとするものです。――もっともこの契約違反の当罰性については争われてお

り、体系上はむしろ背任罪に位置づけられる事例ですが。最後に、「その他データ処理過程への無権限の作用によって」財産上の損害を生ぜしめる行為も可罰的となります。この行為態様は、コンソール不正操作やハードウエア不正操作、及びプロムグラムの時間的経過に影響を及ぼす場合と、データ処理に対する作業指示に作用する場合とをカヴァーしています。

主観的構成要件として二三六条aは、一般的な詐欺罪の構成要件と同様、故意及び不法領得の意思を必要としています。

偽造犯罪の領域における処罰の間隙は、刑法二六七条の文書偽造罪の構成要件に厳密に則った証拠となるデータの偽造罪（刑法二六九条）という新しい構成要件によって埋められます。二六九条によれば、「法律上の取引において人を欺罔するため、証拠となるデータを、それを知覚する際に真正でない文書若しくは変造の文書が存在するように貯蔵し若しくは変更し、又は右のように貯蔵され若しくは変更されたデータを行使した者」は五年以下の自由刑又は罰金に処せられます。二六九条は行為客体として、従来の手書きによる書類作成の際に文書とみなされていたデータを含んでいます。例えば、連邦中央登録簿（Bundeszentralregister）、営業中央登録簿（Gewerbezentralregister）、戸籍簿、捜査データ貯蔵庫におけるデータといった、行政データバンクからのデータや、あるいは、土地登記簿を電子的データ処理へ変換する場合の土地登記簿記載事項、さらには顧客、給与振込口座、銀行口座について電子的に貯蔵された固定データのような個人の経済活動に関するデータがこれにあたります。

二六九条の行為は、既に貯蔵されているデータの変更だけでなく、「法律上の取引において人を欺罔するため」に新しいデータを記憶装置にインプットする場合も含んでいます。さらに同条の構成要件は、そのようなデータの行使をも処

罰します。しかし――その限りでは立法者は二六七条の構成要件に厳密に則ろうとしているのですが――データの貯蔵ないし変更は、「それを知覚する際に真正でない文書若しくは変造の文書が存在するように」行われることが要件とされています。従って、この新しい処罰規定の下でも、文書の一部を作成したり変更したりすることによる、単なるいわゆる不可罰な虚偽文書の作成（schriftliche Lüge）が示すような行為態様は明らかに捉えられておりません。そのために二六九条によって保護される範囲は二六七条によるそれよりも広くはならないのです。すなわち重要なのは、データが貯蔵もしくは変更され、それが表示ないし再生されて知覚できるようになってはじめて、二六七条の意味での文書偽造が生ずることです。[24] このように二六七条と仮定的に対比していくならば、必然的に、二六九条の新しい構成要件に、法律上の取引を処理する際に法的に重要な事実の証拠データとしての使用が予定されているデータだけを含めることができるようになるのです。「証拠となる（beweiserheblich）」という文言は、このような構成要件上の必要性を簡潔に表わしております。

「法律上の取引において欺罔するため」という二六九条の主観的構成要件要素は、二六七条のそれに一致します。しかしこのメルクマールは、新設された二七〇条の法律上の定義[訳注(9)]によって、あらゆる文書・データ偽造の構成要件について統一的に、行為者が「法律上の取引におけるデータ処理への不実の影響」を与える意図で行った場合にまで拡張されています。明文で拡張することが必要なのは、「法律上の取引において欺罔するため」というメルクマールが、人間だけに対するものなのが否かが不明確だからです。このようにデータ処理へ影響を与えるという方法によって証拠やデータを偽造する場合の法律上の定義は、証拠やデータの真正に関する検査が人間によって行われない限り、実際上の意味をもちます（例えば銀行振替取引におけるデータ収録材の交換や、法律上の取引における全自動システムの利用などの場合です）。

以上述べましたところから、第二次経済犯罪対策法の新設によって、刑法によるコンピューター不正操作の捕捉が、財産刑法のみならず、文書犯罪の領域においても保証されたということが確認されました。

2　「ソフトウェアの窃取」及び「コンピュータースパイ」の法的評価については、刑法上のみならず、民事法上も興味ある問題が提起されます。この問題は、特に著作権(刑)法及び競争(刑)法に関連するものです。単なるコピーの作成は、ドイツ刑法によれば、いわゆる価値説(Sachwerttheorie)からも窃盗罪や横領罪の意味における領得(Zueignung)とはなりません――プログラムとデータに関して問題となる財物性(Sacheigenschaft)は全く別に致しますが。従って、第二次経済犯罪対策法の制定以前には、特別刑法上の構成要件のみがこれらの行為と関わっていたのです。

西ドイツにおけるコンピュータープログラムの権利保護をめぐる論争の中心には――日本と同様に――、長い間コンピュータープログラムの著作権保護に関する問題が存続してきました。西ドイツの立法者は、著作権法(Urheberrechtsgesetz=UrhG)二条一項一号で保護される著作物のカタログに、一九八五年の追加条項において「データ処理システムのためのプログラム」という文言を挿入することによって、この論争を決着させました。連邦通常裁判所も、先に述べました現金徴収プログラム事件において――旧法に基いて――コンピュータープログラムの著作権保護適格を原則的に肯定しましたが、その際、著作権法二条二項によってすべての著作物に求められている「個人的、精神的な創造物」という要件に対し高度の要求を行いました。著作権保護適格を有するコンピュータープログラムの原本性に、かような高度の要求を行うことは、実際上コンピュータープログラムを著作権保護の対象として扱うことを非常に困難にします。将来的には、判例上広くコンピュータープログラムに著作権法を適用することが望まれます。なぜならば、著

作権法は、現行法上コンピューターソフトウェアに対して要求されている「絶対的」な権利保護を保証し得ますし、ソフトウェアのバイヤー（Aufkäufer）による「善意取得」を防ぐこともできるからです。

故意による行為者及びソフトウェアのバイヤーに対しては、営業・企業秘密の漏洩に対する競争法上の処罰規定（不正競争防止法〔Gesetz gegen den unlauteren Wettbewerb＝UWG〕一七・一八・二〇条）も存在します。この構成要件は、秘密にされるコンピュータープログラムだけでなく、その他のデータ処理システムにおいて貯蔵された秘密のデータ、例えば住所データ、貸借対照表、研究データなども含みます。第二次経済犯罪対策法が施行されるまでは、営業・企業秘密が、勤務者・労働者・営業実習生によって雇用契約の有効期間中に漏洩されたり、営業秘密が法律上あるいは倫理上許されない方法で知り得た個人によって無権限に利用されたり、他人に打ち明けられたりすることがさらに要件とされていました。第二次経済犯罪対策法は、不正競争防止法一七条二項を追加して刑罰による保護を拡大し、行為としては、行為者が「営業・企業秘密を（a）技術的手段の使用、（b）秘密が印されている複写の製作、（c）秘密が印される物件の奪取、によって無権限に入手若しくは確保する場合」としました。この新規定によって、産業スパイの場合、捜査当局にとってはより早い段階での刑法上の介入が可能となったのです。

西ドイツ刑法典以外の法律では、一九八七年になって初めて導入された、コンピューターチップ及びトポグラフィーの保護に関する規定もあります。この新法は、一九八四年のアメリカ合衆国半導体チップ保護法（US-Semiconducter Chip Protection Act）とは異って罰則規定を設けており――その限りでは日本の一九八五年法[訳注(10)]と同様ですが――、ただその罰則は、日本の法律におけるほど広範囲にわたってはおりません。

西ドイツ刑法典の領域では、二〇二条aによって、コンピューターに貯蔵されたデータの窃取及びスパイ行為の保護が付加されました。この新しい処罰規定はデータ探知罪と呼ばれ、ドイツ連邦議会の法務委員会によって、第二次経済犯罪対策法に導入されました。これによれば、「自己のために予定されてなく且つ権限のない探知に対して特別に保護されているデータを、権限がないのに、自ら入手し、又は他人に入手させた者」は三年以下の自由刑又は罰金に処されます。従ってこの規定についてはプログラム窃取を含めた情報の窃取が問題となります。この規定によって保護されるデータに関し二〇二条a二項は「電子若しくは電磁によって、又はその他直接的に知覚できない方法で貯蔵され、若しくは伝達されるもの」と定義しています。この場合データが、二〇三条の個人の秘密侵害罪にいう秘密を示すものである必要はありません。しかし刑法上保護の対象となるのは――不正競争防止法一七条におけるように――プログラム入手という特定の形式に限られます。プログラムコピーに対する全般的な保護というものは存在せず、西側の諸国においても――フランスで無駄な試みがなされてからは――将来的に予定されておりません。

二〇二条a一項の構成要件上用いられている「入手（Verschaffen）」の概念は、理由書によりますと、ドイツの立法者が多くの他国の法と違って不処罰にしようとした、いわゆるハッキングによる他のデータバンクへの単なる侵入よりは進んだ段階を意味します。しかし、「ハッキング」は（「ハッカー」のスクリーン上に現われた）データを可視的にすることを伴いますので、新規定の主要な適用範囲は、この犯罪形式の範囲内では、データがコード化されない限りで存在します。[25] このような帰結は――特に国際的な観点からは――全く望ましいものと思われます。解釈にあたっては、物体化されていない対象（情報）を「入手」するとはどういうことかをすべて解明する必要があります。すなわち（二〇二条の信書の秘密侵害罪のような）単なる知識の獲得や「処分権（Verfügungsgewalt）」の取得――情報についてこ

れらの場合が一体どのように解されるべきかが明らかにされなければならないのです。従来ドイツ刑法においては、入手という概念は国家機密探知罪(九六条)に関して知られてきました。そこでは、入手とは一般に、知識の獲得(Erlangung von Kenntnis)と解されています。(26)

3　データ処理の領域においてなされたサボタージュ行為は、第二次経済犯罪対策法の施行前に、既に器物損壊罪(刑法三〇三条)によって捉えられていました。と申しますのは、判例及び通説は、この構成要件を、器物本体を人が損壊するということ以上に、器物の機能性を損なうことにまで拡張していたからです。従って特に有力な見解によれば、電磁帯に記録された事項の消去も、器物自体が本来の用法を維持したままで、そこに与えられた情報が破壊されるだけであるにもかかわらず、器物の損壊とみなされるのです。(27)

第二次経済犯罪対策法は――日本の新しい改正と同様――、疑義を避けるたるにデータ破壊の可罰性について明文で示しました。新設されたデータ変更罪の構成要件(三〇三条a)によれば、「データ(二〇二項a二項)を違法に消去し、隠蔽し、使用不能にし、若しくは変更した者」は二年以下の自由刑又は罰金に処せられます。

三〇三条aの行為客体は、二〇二条a二項の法律上の定義における、すべての「直接的に知覚できない」データです(この点については、以下に述べるところを参照)。三〇三条の器物損壊に相当する、データの「消去」行為とは、回復不可能なまでに全く識別できなくすることです。これに対してデータの「隠蔽」は、権利者のアクセス権を奪って、使用不可能にすることを言います。その限りで、三〇三条aの適用範囲は三〇三条のそれよりも広くなることになります。「使用不能」とは、データの使用能力が損われた結果、通常の使い方ができなくなり、目的を達せられなくなることを

指します。さらにデータの「変更」は、連邦データ保護法二条一項三号にいう内容の改ざん(inhaltliches Umgestalten)、すなわちデータの情報内容と表示価値の改変といった機能妨害を意味します。

伝統的な器物損壊罪（三〇三条）、及び新設されたデータ変更罪（三〇三条a）の法定刑では、サボタージュが電子的データ処理の領域にもたらしうる損害に応じたものとはならないため、第二次経済犯罪対策法の立法者はさらに、コンピューター妨害罪（三〇三条b）という加重類型を導入しました。三〇三条bによれば、「他人の経営体、他人の企業若しくは官庁にとって本質的に重要であるデータ処理を、一、三〇三条a一項の行為を行うこと、又は、二、データ処理施設若しくはデータ収録材を破壊し、損壊し、使用不能にし、除去し、若しくは変更すること、によって妨害した者」は、五年以下の自由刑又は罰金に処せられます。構成要件は、データ処理が「本質的に重要」でなければならないということによって限定されています。従って、特に大企業の計算センターないしは施設において貯蔵されており、企業あるいは官庁の機能の中心となる情報を含むデータ（及びその処理）への侵害がこの規定では予定されているのです。電子タイプライターの不正操作のように従属的な意味しか持たないサボタージュ行為は、もとより構成要件に該当致しません。しかし一方で、三一六条bの公共の経営妨害罪において要件とされているような、経営が妨害されるという結果は必要ではありません。

三〇三条bの一項一号が三〇三条aの加重類型となる一方で、三〇三条bの一項二号はコンピューターハードウェア及びデータ収録材のサボタージュ行為に関連致します。二号で言及されている「破壊」及び「損壊」の概念は、三〇三条のそれに相当するものです。二号の客体は、権限を有する者の自由な処理・利用範囲から遠ざけられたときに「除去」

されます。また客体は、その被利用能力が通常の使用に耐えないほど強度に損われた場合に「使用不能」となり、従来とは異なる状態を惹起された場合に「変更」されることになります。

なお三〇三条cによれば、三〇三条a及び三〇三条bにおいて、刑事訴追のための公益が存しない場合には、行為は告訴がなければ訴追されないことになっております。

4　先に述べました「マシンタイムの窃取」すなわちコンピューター施設の無権限使用の犯罪グループについて、ドイツの立法者は――従来の日本の立法者と同様に――新規定を設けることを顧慮してまいりませんでした。従って、データ処理施設の濫用は、今日でも、ドイツ刑法上の所有権ないし財産犯罪の構成要件には該当致しません。すなわち使用窃盗（刑法二四八条b）は、現行法によれば特定の行為客体（自動車及び自転車）に関してのみ可罰的となります。また、電力盗用の特別構成要件（二四八条c）にもデータ処理施設の濫用は該当しません。なぜならば、当該事例において「電力を正規に引き込むため」に予定されたものでない導線が用いられることはないからです。また行為者の一定の活動の自由と被害者の財産上の損害を必要とする背任罪の構成要件（二六六条）も、特別な状況下で適用できるに過ぎません。実際上特に問題となるのは、データ処理施設の（わずかな）電力消費量や、（わずかな）消耗度ではなく、施設の濫用から生じた、行為者の多大な利得（Bereicherung）なのです。ですからむしろこの行為は、二四八条bや二六五条aが規定しているような、給付詐欺ないしは使用窃盗に関わってきます。以上のことから考えますとマシンタイムの窃取は、ドイツ立法者が拒否してきた、新しい処罰規定の創設によってのみ、捉えることが可能であると思われます。スカンジナビア諸国は、使用窃盗の一般構成要件の拡張を一部で決定しましたが（デンマーク、スウェーデン）、これは問題なくデータ処理におけるマシンタイムの窃取を含むものです。もちろん、例えばデンマークで、どの範囲の無権限

使用が可罰的となるかは明らかではありません。マシンタイムの窃取を犯罪化する問題に関して、国際的な一致が達成されるということは、恐らくあり得ないでしょう。[28]

（以上、城下訳）

## III　OECDおよびヨーロッパ審議会の国際的活動

序論ですでに確認いたしましたように、コンピューター犯罪は、日本や西ドイツばかりではなく、他の多くの諸国におきましても法改正や法改正の動きを生じさせました。コンピューター犯罪に対処するための改正案の統一化は、きわめて重要な課題であります。なぜなら、コンピューター犯罪はデータ遠隔処理システムを用いて外国から行なうことができますから、もし当該外国に処罰規定がないといたしますと、「コンピューター犯罪のオアシス」（コンピューター犯罪天国）ともいうべき状況が生じてしまいかねないからなのです。それゆえ、構成要件の内容を諸国間で調和のとれたものにすることは、一方ではそれぞれの国の国境を越えたデータ通信を安全なものにするのに役立ちますし、また他方では自由かつ平等な競争の確保にも資するのであります。このような理由から、パリにあります経済協力開発機構（OECD）は、各国の様々な法改正の動きを相互に調和のとれたものにすべく、すでに早い時期から努力してきたのでした。こうした調整にあたってきたOECDのICCP-Komitee[訳注(1)]は、ズィーバーによる比較法的研究を基礎にして、次に述べますような行為を処罰するよう各加盟国に勧告いたしました。

(a)　違法な財産移転を達成する意図をもって、故意に、コンピューターのデータおよび（または）コンピュータープログラムを、入力、変更、消去および（もしくは）隠蔽（Unterdrückung）すること

(b) 改ざんをなす意図をもって、故意に、コンピューターのデータおよび（または）コンピュータープログラムを、入力、変更、消去、および（もしくは）隠蔽すること

(c) コンピューターまたはデータ通信システムの機能を妨げる意図をもって、故意に、コンピューターのデータもしくはコンピュータープログラムを、入力、変更、消去および（もしくは）隠蔽することまたはその他のコンピューターシステムの妨害を故意に行なうこと

(d) プログラムを商業上利用する意図をもって、コンピュータープログラムの独占権（ausschließliches Recht）を故意に侵害すること

(e) コンピューターシステムおよび（または）（複数の）データ通信システムへの干渉もしくはその傍受が、故意に、権限を有する者の許可なくして行なわれ、かつ、セキュリティのため講じられた措置を侵してまたは不正な（unlauter）もしくは損害を与える意図をもってなされたものである場合のそれらの行為

これらの提案は、現在ヨーロッパ審議会内の委員会によって、さらに細部の検討が行なわれております。今日、国際的なデータ通信網がすでに存在し、拡大していることを考えますと、それぞれの国がデータ通信の分野でまったくひとり歩きすることは無意味になりましたし、またそれは大きな訴訟上の困難を生じさせることでありましょう。こうしたことにかんがみますならば、国際機構のこのような作業により、情報法の分野における法の統一化がさらに進むことが望ましいのであります。(29)

西ドイツについて申しますならば、先述のOECDの勧告は、――ハッキング（上述e）の可罰性に疑問が残ることを別にすれば――第二次経済犯罪対策法の制定により、完全に実現されました。これら多くの刑法的保護の面での改善とならんで、将来もさらに根本的に考えてみなければならないのは、刑法が有体物という古典的な行為の客体とそれに見合った行為に、かなりの程度まで準拠しているということであります。情報や、その他の非物質的な法益は、従来、個別的な形でしか保護されてきませんでした。すなわち、発明として、技術上および商業上のノウハウとして、貸借対照表項目（Bilanzposten）として、あるいは個人のパーソナリティーに関連するコンピューター処理されたデータとして、等々の形でしか保護されてこなかったのであります。ハフト（Haft）[30]は、この点に関して、窃盗罪、横領罪、詐欺罪の構成要件を一律に拡張し、それらを上述のような情報や、さらにはすべての非有体物にまで及ぼそうという重大な提案を行なっております。しかもハフトは、こうした構成要件の拡張を単に解釈によって行なおうとしているのです。しかしながらわたくしは、ハフトの考えとは反対に、そのように構成要件を一律に拡張することは不可能であり、また賢明ではないと考えております。むしろ長い目で見た場合にぜひとも必要なのは、新たな、かつ今日の経済にとって死活にかかわる法的対象でありますところの、コンピューターの内外に存する「情報」というものの法的性格を、民事法的および刑法的に確定することなのです。[31]そしてそのさいには、――刑法的保護が必要とされるほどの――情報の特別な要保護性は、情報がコンピューターに貯蔵されているというだけで認められるのかどうかということも、決定されねばならないでありましょう。

（以上、丹羽訳）

## 原注

(1) Überblick bei *Sieber*, The International Handbook on Computer Crime, 1986, und zuvor *Tiedemann*, in : Council of Europe (Herausgeber), Criminological Aspects of Economic Crime, 1978, S. 224 ff.

(2) Dazu bereits *Tiedemann/Sasse*, Delinquenzprophylaxe, Kreditsicherung und Datenschutz in der Wirtschaft, 1973 ; neue internationale Literaturübersicht bei *Manna*, in der italienischen Zeitschrift L' Indice Penale 1986, 711 ff.

(3) *Sieber* a. a. O. (Fußnote 1) S. 2 ; *Tiedemann* , Wirtschaftsstrafrecht und Wirtschaftskriminalität Bd. II, 1976, S. 149.

(4) Dazu näher *Höft*, Straf- und Ordnungswidrigkeitenrecht im Bundesdatenschutzgesetz, 1986 ; *Schünemann*,ZStW Bd. 90 (1978) S. 11 (23 ff.) ; *Tiedemann*, bei *Berz*, ZStW Bd. 90 (1978) S. 210 (213).

(5) Vgl. *Lampe*, GA (Goltdammers Archiv für Strafrecht) 1975, 1 ff.

(6) *Sieber*, Computerkriminalität und Strafrecht, 2. Auflage 1980, S. XXI f.

(7) Vgl. *Sieber*, Betriebs-Berater (Zeitschrift) 1982, 1433 ff. ; *Tiedemann*, Wertpapier-Mitteilungen (Zeitschrift) 1983, Teil IV S. 1326 (ff.).

(8) Zu dieser Aufteilung bereits *Tiedemann* a. a. O. (oben Fußnote 3) S. 150 ff.

(9) Vgl. *Sieber*, Computerkriminalität (oben Fußnote 6) S. 47 ff. ; *Tiedemann*, Wirtschaftsstrafrecht (oben Fußnote 3) S. 151 f.

(10) Vgl. *Sieber* a. a. O. (oben Fußnote 6) S. 58 f.

(11) *Tiedemann* a. a. O. (oben Fußnote 3) S. 150.

(12) *Tiedemann*, WM a. a. O. (oben Fußnote 7) S. 1327.

(13) Dazu näher *Sieber*, Betriebsberater (BB) 1983, 977 ff.

(14) Badische Zeitung vom 22. 9. 1983 S. 2.

(15) *Tiedemann*, WM a. a. O. (oben Fußnote 7) S. 1328.

(16) Zusammenfassend—auch zu dem im Text folgenden Fall—*Sieber*, International Handbook (oben Fußnote 1) S. 19.

(17) So aber der Vorschlag von *Haft*, NStZ (Zeitschrift "Neue Zeitschrift für Strafrecht") 1987, 6 ff.

(18) Dazu zuletzt *Schmitt*, Jura (Zeitschrift) 1987, 640 ff.

(19) Vgl. *Lackner*, in : Leipziger Kommentar zum Strafgesetzbuch, 10. Aufl. § 263 Rdn. 86 ; *Tiedemann*, Juristen Zeitung (JZ) 1986, 865 (869).

(20) *Sieber*, Computerkriminalität (oben Fußnote 6) S. 247 ff,

(21) *Tiedemann* a. a. O. (oben Fußnote 19) S. 869 f.

(22) *Sieber* a. a. O. (oben Fußnote 6) S. 297 ff. ; *Tröndle*, in : Leipziger Kommentar § 268 Rdn. 8 a.

(23) a. a. O. (oben Fußnote 7) S. 1331.

(24) *Tiedemann* a. a. O. (oben Fußnote 19) S. 870.

(25) *Tiedemann* a. a. O. (oben Fußnote 19) S. 868.

(26) *Schönke/Schröder/Stree*, Strafgesetzbuch, 22. Auflage 1985, 96 Rdn. 4 ; auch *Trüger*, in : Leipziger Kommentar § 96 Rdn. 3.

(27) *Tiedemann*, Wirtschaftsstrafrecht (oben Fußnote 3) S. 154 f. ; *Wolff*, in : Leipziger Kommentar § 303 Rdn. 6 mit

weiteren Nachweisen.

(28) *Lenckner*, Computerkriminalität und Vermögensdelikte, 1981, S. 21 ; aber auch *Sieber*, International Handbook (oben Fußnote 1) S. 84 f.

(29) Zutreffend *Müller/Wabnitz*, Wirtschaftskriminalität, 2. Auflage 1986, S. 211 f.

(30) *Haft* a. a. O. (oben Fußnote 17).

(31) Vgl. bereits *Tiedemann*, in : von Caemmerer-Festschrift, 1978, S. 643 ff.

## 訳注

(1) 本件につき、ウルリッヒ・ズィーバー（西田典之・山口厚訳）『コンピューター犯罪と刑法Ⅰ』（成文堂、昭和六一年）四八―五〇頁（「児童手当事件」）参照。末尾の〔 〕内の記述は、同書五〇頁による。

(2) 本件につき、ズィーバー・前掲注(1)五九―六〇頁（「プログラム不正操作事件」）参照。

(3) 本件につき、ズィーバー・前掲注(1)六二―六五頁（「銀行残高事件」）参照。

(4) 本件につき、ズィーバー・前掲注(1)五二―五四頁（「電話注文事件」）参照。

(5) いわゆる固定データおよび可変データの意義、両者の区別につき、ズィーバー・前掲注(1)七三頁、七六頁、八〇頁参照。

(6) 本件につき、ズィーバー・前掲注(1)一一五―一一六頁（「スパイ潜入事件」）参照。

(7) ジョブ（Job）とは、計算機によって実施される仕事の単位であり、複数のプログラムの実行によって構成される「ひとまとまりの仕事」のことをいう。詳しくは、各種のコンピューター用語辞典等を参照されたい。

(8) ビデオテックスシステム（Video-tex-system）とは、電話線と家庭用テレビを組み合わせた情報サービスネットワークであり、大容量のファイル装置に各種の画像情報を蓄積したセンターに対して、家庭やオフィス内のテレビ受像器から公衆電

話回線を通じてアクセスし、利用者の必要とする情報を取り出すものである。ドイツではBildschirmtext（＝Btx）と称され、また日本ではキャプテンシステムと呼ばれるものがこれにあたる。（以上につき、八木暁・勅使河原可海編著『現代人のコンピュータ　コンピュータネットワーク』（朝倉書店、昭和五八年）一八八頁以下等を参照。）

（9）二七〇条は「法律上の取引におけるデータ処理への不実の影響は、法律上の取引における欺罔と同じとする」と定めている。

（10）「半導体集積回路の回路配置に関する法律」（いわゆる〝半導体チップ法〟）を指す。

（11）ICCP＝Information, Computer and Communications Policy

〔訳者あとがき〕

本稿は、西ドイツ・フライブルク大学教授で、同大学犯罪学・経済刑法研究所所長のクラウス・ティーデマン（Klaus Tiedemann）博士が、一九八七年九月二五日に本学部の刑事法研究会特別例会において行った講演〝Computerkriminalität und deutsche Strafrechtsänderung von 1986〟の原稿を訳出したものである。

ティーデマン教授は、一九三八年四月一日、ウェストファーレンのウンナに生まれ、テュービンゲン大学でカール・ペータース教授の助手を勤めた後、一九六八年に同大私講師、同年冬学期にギーセン大学正教授となり、一九七五年からフライブルク大学教授として、刑法（特に経済刑法）、刑事訴訟法、犯罪学の各分野にわたって多くの研究を発表されている。最近の著作としては、Die Auslegung des Strafprozeßrechts, in : Festgabe für Karl Peters, 1984, S. 131ff ; Die Bekämpfung der Wirtschaftskriminalität durch den Gesetzgeber. Ein Überblick aus Anlaß des Inkrafttretens des 2. WiKG am 1. 8. 1986, in : JZ 1986, S. 865ff ; Das Parteienfinazierungsgesetz als strafrechtliche lex mitior, in

: NJW 1986, S. 2475ff ; Gründungs- und Sanierungsschwindel durch verschleierte Sacheinlagen, in : Festschrift für Karl Lackner, 1987, S. 737ff ; Die Parteispenden —— Entscheidung des BGH, in : NJW 1987, S. 1247ff. などがある。ティーデマン教授の経歴及び著作について、詳しくは宮澤浩一編『西ドイツ刑法学・学者編』（一九七六年）六四二—六四六頁、宮澤浩一・井田良「西ドイツ刑法学の現状（追録Ⅷ）」法学研究（慶応義塾大学）五九巻八号（一九八六年）一一一頁などを参照されたい。

ティーデマン教授は、一九八七年九月に日本学術振興会の招聘で初来日され、約一か月にわたって全国の大学において様々なテーマの講演をされた。本稿と同一テーマの講演は、岡山大学及び広島大学においても行われた由である。

なお、本稿第Ⅱ部における西ドイツの新しい処罰規定の訳出に際しては、神山敏雄「西独における第二次経済犯罪対策法の制定」法律時報五八巻一一号（一九八六年）五三頁以下を参考にした。

訳出に際しては原文にできるだけ忠実な訳を心がけたが、場合によっては多少意訳した部分もある。その他の訳出上の凡例は、次の通りである。

1 訳文中、（ ）の部分は原文で括弧が使用されている箇所、ないしは原語を併記した箇所である。

2 原文でアンダーラインを付されている語句には、訳文では傍点を付した。

3 原文の引用記号 〃 〃 は、「 」に変えて訳出した。

4 原文の固有名詞（地名、会社名、組織ないし機関名など）は、著名なものを除き、カタカナで表記せず原文のままとした。

5 原文中の略語DV（＝Datenverarbeitung）は原則として「データ処理」と訳したが、前後の文脈によっては「コン

ピューター」と訳した場合もある。