# 第６章ドイツにおける有害プログラムの刑事的規制

## 第1節　ドイツにおけるネットワーク刑法

### コンピュータ・ウィルスとの関係においてー

１　ドイツのネットワーク刑法をコンピュータ・ウィルスによる侵襲という視点からみた場合、問題となる条文は、刑法典上の 202 条 a、303 条 a、303 条 b が問題の中心となるが、さらに不正競争防止法(UWG)17 条ならびに連邦情報保護法(BDSG)43 条、48 条もその射程にはいってくることとなる。まず、これをネットワーク刑法の保護法益である情報のインテグリティという観点から整理してみる。

情報のインテグリティ(Integrty of data)を情報の正確性という点でみるなら、情報それ自体の正確性の確保すなわち情報の損壊ないし変更に対するインテグリティと情報へのアクセスに対するインテグリティという二つの側面でみることができる。前者の情報の損壊に対するインテグリティを問題にするのが、ドイツ刑法 303 条 a および 303 条 b である。これに対して、情報へのアクセスに対するインテグリティを問題にとするのが、刑法 202 条 a であり、さらに情報内容に応じて、不正競争防止法 17 条が営業上の秘密について、連邦情報保護法 43 条が個人情報についてその保護を図っている[1]。

２　ドイツ刑法 202 条 a[2]は、データの探知、すなわち媒体に記録された情報および伝送中の情報への無権限のアクセスを処罰するものであり、いわゆる「ハッキング」行為[3]を捕捉する。

---

[1]もちろんこれらの法律はネットワーク上の侵害行為にのみ限定して適用されるものではなく、当該構成要件に該当する以上、ネットワークを用いない場合であっても処罰されうる。さらに、刑法 202 条 a、303 条 a および 303 条 b は、1987 年の第二次経済犯罪対策法によって導入されたものであり、そのときにコンピュータ詐欺罪などの規定も立法されたが、ここでは問題領域外にあるため、言及しない

[2] 202 条 a　データの探知(Aussphaen)

(1)　権限がないのに(unbefugt)、自己のために予定されておらずかつ無権限(unberechtigt)のアクセスに対して特別に保護されているデータを、取得しまたは他人に得させた者(sich oder einem anderen verschaffen)は、３年以下の自由刑または罰金に処する。

(2)　１項の意味におけるデータは、電子的、磁気的またはその他直接認知しえない形態で貯蔵されまたは伝送されるものに限られる。

その意味では、情報セキュリティの重要な部分を保護するものといえる[4]。ただし、刑法上の保護法益という点では、形式的秘密を保護するものであり、このかぎりでは、わが国の信書開披罪に類比するものとして位置づけることができる。基本的な構成要件は、データの無権限のアクセスであり、データの管理者が保護しようとしているデータに対して権限なくアクセスした場合、データ探知罪が成立する。

これに対して、情報の実質的秘密の保護はその情報の内容、すなわち何に関する情報であるかによってさらに別の構成要件に該当することとなる。不正競争防止法 17 条は企業秘密についてその保護を図るものであり、連邦情報保護法 43 条[5]は個人情報を保護するものである。いずれも、ネットワーク上のデータに限定されず、権限なく企業秘密あるいは個人情報を入手する行為を処罰するものである。もっとも、これらの犯罪はネットワーク上の行為あるいは電磁的記録に関するかぎりいずれも 202 条 a を前提とし、各々観念的競合の関係にたつ。また、202 条 a はデータの内容如何をとわず保護するものである。したがって、以下の考察ではもっぱら刑法 202 条 a を取り扱うものとする。

3　データの損壊、すなわちデータの正確性それ自体を問題とするのが刑法 303 条 a[6]ある。すなわち、データの無権限の変更・毀損をその構成要件とする。さらに、刑法 303 条 b は、たんなるデータの損壊だけでなく、情報処理過程に対する利益をも保護する。その意味では、コンピュータによる情報処理の一般的な安全性を保護するものといえる。この点で、303 条 b[7]

---

[3] ただし、サーバへのたんなる侵入行為、無権限のコンピュータの使用は処罰の対象とはならない。この点においてわが国の不正アクセス防止法よりは処罰の限定がなされている上、その規制目的も明確である。

[4] 情報セキュリティをどのようなものとするかについては、異論もあろうが、(1)デバイスに記録されたデータの正確性、(2)伝送中のデータの正確性、(3)伝送されたデータの受領の正確性が最低限保証される必要があろう。202 条 a はこのうち(1)(2)の両方を保護するものとして重要である。

[5] 連邦情報保護法 43 条は次のとおりである。
(1)　権限なく、この法律で保護されている公開されていない個人に関係するデータを
1. 貯蔵、変更もしくは伝送し、
2. 自動化された方式によって呼び出せるように準備をし、または
3. データ補完装置（補完場所）から呼び出しもしくは自己または第三者のために入手した者は、１年以下の自由刑または罰金刑に処する。
(2)　この法律で保護されている公開されていない個人に関係するデータの伝送を不正な指示によって領得し、
1. 16 条４項１文、28 条４項１文に反して、また 29 条３項、39 条１項１文または 40 条１項との関連において伝送されているデータを第３者に譲渡することによって他の目的のために利用し、または
2. 30 条１項２文に反して 30 条１項１文において特徴づけられているメルクマールまたは 40 条３項３文に反して 40 条３項２文おいて特徴づけられているメルクマールを集めた者も同様に処罰する。
(3)　行為者が有償または自己もしくは第三者の利益をはかりあるいは第三者に損害を与える目的で行為した場合は、２年以下の自由刑または罰金刑に処する。
(4)　略（親告罪の規定）
連邦情報保護法の 16 条の規定は、非公的な立場の者へのデータの伝送が許容される場合を列挙しているもの、28 条以下は具体的な目的に応じてデータの蓄積に関してガイドラインをしめすもの。

[6]
303 条 a　データ変更
(1)　データ（第 202 条 a 第 2）違法に消去し、隠蔽し、使用不能にし、または変更した者は、２年以下の自由刑または罰金に処する。
(2)　本条の未遂は罰する。

[7] 303 条 b　コンピュータサボタージュ（コンピュータ妨害）
(1)　他人の経営体、他人の企業または官庁にとって本質的に重要であるデータ処理を次に掲げる行為によって妨害した者は、５年以下の自由刑または罰金に処する。
１　第 303 条 a 第１項の行為をおこなうこと
２　データ処理施設またはデータ貯蔵媒体を破壊し、毀損し、使用不能にし、除去しまたは変更すること
(2)　本罪の未遂は罰する。

は個人的法益をこえた利益を保護するものといえる。ただし、303 条 b は、データの変更・毀損による行われる情報処理の阻害のみならず、コンピュータ等情報処理のためのハードウェアの毀損によるものも処罰をしているが、ウィルスとの関連においては、1号による 303 条 a の行為によるものにその考察を限定してよいであろう。わが国との比較において重要なことは、ドイツでは、わが国における業務妨害罪と同様の処罰規定を有していないてため、情報処理を阻害する業務妨害のみが処罰されることになる点である。

さらに、これらの罪はいずれも未遂を処罰する点がウィルスの投与の可罰性を考える上で重要となる。すなわち、ドイツ刑法 22 条は「その行為についての表象にしたがって、構成要件の実現を直接に開始した」場合を未遂と定義している。それゆえ、以下の論述に見られるような有害なプログラムを被害者のシステムに送付ないし投与した場合、303 条 a ないし b の罪の未遂犯の成立を認めることができるであろう。

| 加害行為の態様 | 問題となる有害なコード | 罰条 | 侵害されるセキュリティの内容 |
|---|---|---|---|
| データの毀損 | ウィルス<br>ワーム | 303条a<br>303条b<br><br>（303条）<br>（317条） | データの正確性の侵害<br>データの改変・破壊に対するインテグリティ |
| システムの毀損 | | | |
| システムへの侵入 | Back Orifice | 202条a | データ・アクセスに対するインテグリティ |
| 無権限アクセス | トロイの木馬 | UWG17条<br>BDSG43条 | |

# 第2節　有害プラグラムによる攻撃と犯罪の成否

## 第1項 有害プログラムによる情報のインテグリティの侵害

1　ネットワークに関わる有害なプログラムによる利益侵害も情報のインテグリティの侵害である。したがって、ウィルスによる攻撃対象も前節において述べたインテグリティの点によ

る二つの類型に対応する。無権限のデータアクセスとしてのコンピュータ・スパイとデータ破壊としてのコンピュータ・サボタージュがそれである。

2　コンピュータ・スパイに利用されるプログラムとして考えられるものは、いわゆる「トロイの木馬」タイプ[8]のプログラムや Back Oriffice に代表されるようなリモート・アクセスのプログラムである。典型的なウィルスでこのような機能をするものもあるが、ドイツではまだ問題になっていないようである[9]

コンピュータ・サボタージュとして問題となる有害プログラムによる攻撃において、その行為の客体となりうるのは、コンピュータのハードウェアとソフトウェアの両方である。すなわち、あるプログラムがシステムの基本的なソフトをはじめとするプログラムファイルを破壊ないし削除することによって、303 条 a ないし b の成立が問題なるだけでなく、通常の器物損壊罪の成否すらも問題とされる。このようなプログラムの典型的なものは、ハードディスクを初期化したり、特定のファイルを削除する機能を有するウィルスであろう。さらには http によるアクセスに際して、ActiveX などを組み込むことで同様の機能を果たさせることも可能であり、その場合にも問題となる。また、アメリカにおけるインターネットワーム事件[10]にみられるように、ワームもデータないし情報処理の適正性を侵害することがありうる。

3　以下では、上述のふたつの視点をもとに、有害プログラムの機能に着目し、刑法上の問題点を検討することとする。

# 第3節　コンピュータ・スパイ

## 第1項　トロイの木馬の事例

コンピュータ・スパイに利用される典型的なコードは「トロイの木馬」と呼ばれるものである。これは、プログラムのなかに、データの消去、変更または送出をおこなう下位のコードが組み込まれているものである。ドイツにおいて問題となったのは T-online Power Tools 事件[11]

---

[8] トロイの木馬をプログラムの保持者が予期しえない動作を示すタイプのものを指称する定義もあるが、ネットワークで問題とされる場合には、個人のパソコン等から ID やパスワードを盗み取るタイプのものさすのが通例である上、ドイツにおける議論ではトロイの木馬は後者のタイプのものであること前提に議論されている。

[9] U. Sieber, Teil 19 Strafrecht und Strafproze ｧ recht, in:T. Hoeren/ U. Sieber (Hrsg.), Handbuch Multimedia-Recht, 1999, Rdn. 44 は日本におけるニフティ・サーブ（当時）で広まったパスワード探知のウィルスを例にあげている。

[10] このワームプログラムは、ネットを通じて他人のコンピュータに侵入するために、標準化されたハッキングツールを使用する。それによって、数日で約 6000 のコンピュータを麻痺させたものである。この事件の行為者は、ワームプログラムがどのくらい早くインターネットに広まっていくのかテストしようとしただけなのに、少数の位を書き間違ったためにプログラムがコントロールできずに広まることになったと、反論した。この主張にみられるように、ウィルスの拡散に対する処罰に関しては、故意の証明の問題が生じる。

[11] この事件の内容は、以下のとおりである。
「少年ハッカー、T-online をクラック

と呼ばれるものである。1997 年の末に起きたこの事件では、二人の少年が、表向きはネットへのアクセスを最適化する T-online Power Tools をインターネットにアップロードし、一般にダウンロードできるようにしたのであるが、このソフトは、インストールによって、T-online へのアクセスに関するデータをユーザの知らないうちにこの二人の少年たちに伝送するというものであった。もちろん T-online へのアクセスするためのユーザ ID とパスが伝送されるのは、利用者のハードディスクにそれらが記録されているばあいだけであったが、それでも、この事件は当時まで世間では完全であると考えられていたドイツのオンラインサービスへのアクセスに脆弱性があること示すものとして注目された。

## 第2項 トロイの木馬に関わる刑法的問題

１　では、一般的にトロイの木馬を配布することはどのような刑法的問題が生じるであろうか。この点については、次のような例をもとに考察してみることとする。

AはBにメールをつかって「トロイの木馬」を送った。これは（Bに気づかれずに）そのパスワードをAに伝送するものである。このパスワードをつかって、Aは、のちにBのコンピュータに侵入し、関心のあるデータをコピーした。

２　まず問題となるのは、コンピュータへの侵入の点である。すなわち、トロイの木馬をＢのコンピュータへ組み込むことはどのように解すべきかが問題とされる。もっとも、Ｂのコンピュータへたんに侵入しただけでは不可罰のままである。それでも、保護されたデータのコピーをおこなった時点でそれは可罰的なものとなりうる。

Ａはデータをコピーすることによって自己の支配に移し、202 条 a１項の意味でデータを「入手した」ものである。しかも、それらのデータは権限者の意思によるとＡのために予定されているとはいえないものである。202 条 a の適用の可否の点でもっとも問題となるのは、それらのデータについて特別のアクセスの保護が存在していたかどうかということである。Ｂはたしかにそのデータをパスワードによって保護していたが、それでも、その障害はＡにとってたいした困難もなく克服できたのである。202 条 a にいう「保護」が客観的に一定程度のセキュリティ措置を施すことを要求するのであれば、この場合、202 条 a は成立しえない。しかしながら、202 条 a は個人の形式的秘密を保護するものであるから、その成立にとっては、権限者の保護意思を明確に示すいかなるアクセス保護も十分であるとの前提に立つと解するのが妥当で

---

二人の 16 歳の少年が、あきれるほど簡単な方法で、数百人の T-online の顧客のアクセスデータを入手した。 このいたずらは、ホームバンキング、E-コマースおよびいわゆる「使用料」に関して争いのある事例における判例に関する帰結をもたらしたといえるであろう。

クラックした ID とパスワードをつかって、二人のハッカーは、これらの顧客に費用を負担させることで、ドイツ最大のオンラインサービスににについて課金され、電話料金で差し引かれるすべての機能を利用できるようになった。同様の方法で、彼らは、ホームバンキングの口座へのアクセスも手に入れることができた。

T-Online の業務執行役員である Eric Danke は、「きわめて真剣に受け止めるべき事件」であり、これはすべてのセキュリティ構想を熟慮し、発展させることになるだろう。短期的には、T-Online はこの具体的な攻撃に抵抗できるデコーダ・アップデイトを提供するであろう、と語った。

ふたりの少年は、その行為によって、何らかの損害を惹き起こそうとしたのではなく、T-Online の基本的なセキュリティの欠如とデコーダ・プログラムのセキュリティの不十分さをおおやけにしようというものであった。ふたりは、"T-Online Power Tools"という有名なサポートプログラムの著者であり、このソフトを「トロイの木馬」としてアクセスデータを極秘に伝送するために利用した。彼らは、優れたプログラミング知識を利用していないにもかかわらず、アクセスデータの単純な暗号化を短期間にハックすることができたのである。ハック後３ヶ月して、彼らはその行為を中止し、その大胆な行為をわれわれに対して打ち明けた。」

あるとされる。したがって、このような事例についても、202 条 a の可罰性を肯定できることになるとされる。

３　つぎに、パスワードの入手について、パスワードを転送したことそれ自体が 202 条 a１項に該当するかが問題となる。第一に、システムに貯蔵されたパスワードは 202 条 a２項の意味での「データ」とみることができる。また、パスワードの性質上、それが第三者のために予定されたものとは当然いえない。問題となるのは、パスワードがそれ自体権限のないアクセスに対してとくに保護されていたのかということである。この場合、パスワードそれ自体による保護は問題にならない。というのは、その種のアクセス制限は他のデータを権限のないアクセスから保護するものだからである。そこで、パスワードが通常基礎としている秘密保持は、202 条 a１項の意味での保護と考えることができる。というのは、パスワードの秘密保持は客観的な作用を有しているからである。アクセスの可能性は、パスワードによって、ソフトウエア技術上の保護によるのと同様に、信頼できる形で阻止されている。したがって、202 条 a の成立を肯定することができよう。

４　最後に、「トロイの木馬」を送付・機能させたことについて、トロイの木馬をうまく隠して配置したことが 303 条 a の構成要件に該当しないかが問題となる。まず、データの抑圧・使用不可能にするとのメルクマールについてみてみる。Ａはたしかにトロイの木馬を転送することによってＢのハードディスクの一部を占拠した。それでも、その点について、データを「抑圧する」ということも「使用できなくする」ということも認めることはできないとされる。つぎに、データの変更というメルクマールについてであるが、Ｂの固有のデータの存在する領域を別のデータを挿入することによってデータを変更したと認めることが可能であるとされる。なぜなら、303 条 a は権限者のそのデータの完全な使用可能性という利益を利益を保護するものだからである。しかしながら、トロイの木馬の配置によってＢの固有のデータの使用可能性が制限されたかというと、トロイの木馬の無権限の転送はそのような使用可能性の制限はともなわず、したがって、トロイの木馬の無権限の転送は 303 条 a の構成要件に該当せず、303 条の可罰性も排除される。なお、202 条 a は未遂を処罰しないため、データの無権限のアクセスの意図をもってトロイの木馬の送付しても、それだけでは不可罰の未遂である[12]。

## 第3項 Back Oriffice の投入とその使用

Back Oriffice による他人のコンピュータのリモート操作は、まず、データのアクセスの点について、原則としてトロイの木馬の場合と同様に解することができ、無権限に保護されたデータにアクセスした場合にかぎり、202 条 a が成立しうる。したがって、無権限にリモートコントロールするにとどまるかぎりは不可罰である。このことは、その他のリモートコントロールプログラムについても同様に解することができる。しかしながら、たんなる無権限のリモートコントロールをこえて、他人のコンピュータにあるデータを変更ないし消去した場合には、303 条 a が成立することになり、さらに、そのことが情報処理を阻害したときは 303 条 b に該当することとなる。

---

[12] 以上の点については Hilgendorf, Grundfälle zum Computerstrafrecht, JuS 1997, 130ff.

# 第4節 コンピュータ・サボタージュ

## 第1項 コンピュータ・ウィルス、ワーム

1　コンピュータ・ウィルスは特定の宿主に寄生することで、増殖する点に特徴があるが、そのコードの機能形態は多様である。ドイツのネットワーク刑法においてウィルスを投入したことが処罰されるためには、ウィルスの機能が刑法 303 条以下に規定される構成要件的結果を惹起する必要がある。そのかぎりで、ウィルスのタイプがいわゆるブートセクタ・ウィルスであるか、マク・ロウィルスであるかあるいはコンパニオン・ウィルスであるかといった宿主の種類と犯罪の成否は無関係である。これに対して、ワームは独立のプログラムがコンピュータシステムに侵入することで攻撃をおこなうものであるが、ウィルスと同様、その効果としてどのような結果を惹起したのかが問われる。

2　刑法 303 条は、他人の「物」を損壊しなければならない。有体物に対する物理的損壊が問題となる。しかし、この場合、有体物それ自体の物的な破壊だけをとらえるのではなく、その正規の使用を不可能にする場合をも含めるならば、ウィルスなどがコンピュータのハードディスクを初期化した点について、客観的に刑法 303 条の通常の器物損壊罪の構成要件に該当することとなる。したがって、このことによって業務、企業ないし官庁にとって本質的に重要な情報処理を阻害すれば、303 条 b１項２号により、コンピュータサボタージュの構成要件に該当することになる。このような機能を果たさなくとも、有害なコードによって、データの消去、変更がおこなわれ、あるいは使用できない状態にされた場合には、303 条 a のデータ変更の構成要件に該当し、このことによって業務、企業ないし官庁にとって本質的に重要な情報処理を阻害したときは、303 条 b１項２号によるコンピュータサボタージュの罪が成立することになる。それゆえ、ウィルスの拡散について処罰を考慮するばあいには、ハードディスクの初期化のように明確なデータの損壊の場合は別として、ウィルスの機能が 303 条 a の構成要件的結果を惹起するのものかが重要である。

3　ドイツにおいて、ウィルスによるコンピュータサボタージュが問題となった事件は、クリスマスツリー事件といわれるものである。これは、クリスマスグリーティングのメールにクリスマスツリーをディスプレイに表示させるプログラムを添付したものであるが、このプログラムに組み込まれたコードが、ディスプレイへのデータの表示と同時に、自己のプログラムを複製して同一のクリスマスグリーティングのメールをメールクライアントプログラムのアドレスデータにアクセスし、アドレスに記載されている全員に送付するというものであった。そのため、感染したデータを受け取った者がプログラムを起動するたびに雪だるま式に感染データの配布メールを送出する結果となり、そのことがネットワークへの過大な負荷をかけたことによってシステムダウンへといたったのである。このプログラムの作者は告訴されたものの、「『クリスマスツリーワーム』では、きわめて限定的な範囲でのみ実験しようとしただけであり、ワームを解き放って損害が発生することなど考えていなかった」と主張した。そのために、器物損壊、データの改変およびコンピュータサボタージュを理由とする有罪判決は、ネットワークの損害に関して故意が証明されないとして、不可能であるとされた。 故意の点については問題がないとの意見も存する（後述第 2 項参照）。

この事例は、メリッサ型のマクロウィルスと同様のものである点は重要である。すなわち、メリッサ型ウィルスの投与・配布は、その故意の点に問題がなければ、同様にドイツ刑法 303 条 b による可罰的となるということである。

4　このような故意の点に問題ない場合、303 条以下の規定は未遂を処罰するため、刑法 22 条の未遂の一般原則にしたがい「直接的な開始」が認められるときは、未遂犯の成立を考えることができる。たとえば、コンピュータウィルスをあるコンピュータに投入したが、しかしまだその攻撃客体となるデータへの作用がない場合には 303 条 a の未遂犯が成立する[13]。

## 第2項 ウィルスの拡散における故意の問題

ウィルスなどデータの改変をもたらすコードを投入する行為を処罰するためには、故意が必要である。しかしながが、ドイツ刑法 15 条にいう故意は、いわゆる未必の故意で十分である。したがって、303 条以下の犯罪の成立にとっても未必の故意で足りることとなる。この点、ドイツの判例および通説は、未必の故意について、結果を是認しつつ甘受したということが客観的指標にしたがって認められれば故意を肯定することができるとしている。すなわち、その判断にとって、結果の明白性、危険性だけでなく、危険回避のための予防措置への関与という点が重要な基準となる。そこで、可罰的な結果の発生を相当程度の蓋然性をもって予見したが、それにも関らず、それを回避することをおこなわなかった者は、たとえその結果を実際には「望んでいなくとも」、故意を以って行為している。これに対して、一定の予防措置を講じて、「すべてうまくいくにちがいない」と考えたことから、結果をほんのわずかの蓋然性しかないと考えた者は、通常、認識ある過失により行為しているのである。そのため、これをクリスマスツリーワーム事件にあてはめた場合、行為者は、そのような損害のそれほど遠くない可能性を認識しているが、しかし、結局どうでもよいと考え、そのため自分の実験の現実化を受け入れていた場合には、その種の未必の故意を肯定することは可能であったとする意見もある[14]。

## 第3項 メール攻撃によるコンピュータサボタージュ

1　昨年問題となったメリッサ、さらにはドイツにおけるクリスマスツリー事件が示すように、ネットワークにおけるメール機能を利用した攻撃が生じている。多量のメールの送付行為も、情報処理を阻害することがある場合には 303 条 b の成否を検討する必要がある。

AはEメールをつかってBに無限メールを送付し、重要な報告（いくつかの匿名の通信を含め複数の取引のもう込み）がBに届くことを妨げた。そのことによって、Aが予見したように、Bは著しい財産的損失を被った。

2　この事例をもとに、スパムなどのメール送付に関わる解釈論的問題を明らかにしてみる。この事例で二つの客体を考えることが可能である。第一はBのメールボックスにあるデータである。このデータについては 303 条 a１項のデータの変更といえるかが問題となる。Bのメールボックスへ無限メールを転送する行為は、受取り手のデータを無限メールによって変更しておらず、そのメールボックスのデータの記憶スペースを満杯にしただけしかない。したがって、データの改変それ自体は問題とすることができない。そのため、303 条 b１項２号の成否を考慮するにあたっては、Bのメールボックスを使用できなくしたといえるかが重要となる。この点、303 条 b１項２号にいう「使用できなくする」とは、当該ハードウエアが正規の方法で使用できないほど重大な程度の使用可能性の侵害をいい、その使用可能性の侵害が相当程度

---

[13] Vgl. auch Schönke/Schröder/Stree, 303a Rdn. 7.
[14] U. Sieber. a.a.O., Rn. 47ff.

継続的なものであり、それゆえただちに除去できないものでなければならない。それゆえ、Aの無限メールをBは容易にハードディスクから削除することができ、それによってメールボックスの機能を回復することが可能であるため、メールボックスおよびメールボックスの内容についてAは不可罰であるとせざるをえない。この結論については法政策的には問題のある帰結であると評価する者もいるが、妥当であるとの見方が強い。

3　第二に、Bに第三者によって送付されたデータについて 303 条 a の成否が問題となる。すなわち、Aの無限メールがそのデータのBへの到達を妨げていることが「隠匿した」といえないかということである。この場合、データの隠匿とは継続的あるいは一時的なものであっても、権限ある者のアクセスからデータを奪うことをいう。そこで、Aは到着した電子メールをBのアクセスから奪ったのではなく、たんにBのアクセス可能性をそもそも生じることを妨げているすぎず、直接的にはこの定義に該当しないといえる。しかしながら、274 条1項1号に関する RG の判例によると、郵便配達人が誤って間違った住所へ配達した手紙へのアクセスを妨げた場合にも、「隠匿した」といえ、行為者が抑制した手紙について自己の処分権限を保持していたことも決定的な相違を基礎づけるものではないとする。この判例を本事例にあてはめるならば、データを権限者のアクセスから奪った場合だけでなく、権限者に存すべきデータがそのアクセス領域に到達することを妨げた場合にも、データを隠匿したといえると解することができよう。

4　では、当該電子メールが権限者のアクセスから奪われていたといえるであろうか。前提として、問題のデータについて誰が権限者であるといえるかを明らかにする必要がある。303 条 a の客体となるデータの権限者は、Skripturakt[15]によってデータを生み出した者であるとするのが通説である。この理解からすれば、電子メールの送信者が権限者であると解されることになる。これに対して、名宛人への送信によってデータの権限を委譲したとの考え方もありうるが、データの権限がデータの責任をも包含するということを考えると、データの権限の委譲は、原則として、名宛人による事実上の支配可能性の引受けがあってはじめて認められるべきである。

こうして、電子メールの送信者がアクセスを奪われていたといえるであろうか。通常、電子メールのコピーが送信者の手元に残っているのであり、送達不可能な電子メールは送信者の元に戻ってくる。とすれば、電子メールの送信者は、そのデータのアクセスの可能性をBのメールボックスに無限メールが占拠したことによって失われてはいないものといえる。この点で、権限者のアクセスは制限されていないし、それどころか.保護されているといえ、したがって、303 条 a 1 項の成立は排除される。

5　なお、この事例では、274 条1項2号による証拠上重要なデータの隠匿も問題となる。274 条1項2号の保護法益はデータの証拠権限、証拠上の重要性である。すなわち、法取引における証拠を一定のデータによって提出権利がその中心的位置を占める。問題となるデータの範囲は、274 条1項2号の文言によると、202 条 a2項の意味におけるデータすべてであるが、本条項の位置づけおよび保護法益に鑑みると、法取引において証拠としての適性があり、特定されていて、かつ名義人を認識させるものであり、そのためそれが視覚的に認知可能であるならば文書が存在するであろうような思想の表明が問題となる。そこで、匿名の送信の場合は名義人の認識可能性を欠くのでこれに該当しないが、取引に関するメールはこれに該当するといえる。そのほかに、主観的構成要件要素として他人に損失を加える目的が必要とされるが、これが肯定されれば、未必の故意の問題はあるものの、本罪の成立を肯定することができる[16]。

---

[15] Welb, IuR 1988, 443ff.

[16] ドイツ刑法 26 条ないし 27 条における共犯の従属性の規定は共犯行為独自の可罰性を限定する。

6　以上はいわゆるスパムあるいはメールボムによる攻撃についての検討であるが、ウィルス等によって同様の効果が生じる場合についても、同一の法解釈がなされるものといえる。

## 第4項 コンピュータ・ウィルスのネットワークへの配布行為の可罰性

1　以上の検討は、行為者自身がウィルスを投与する場合だけを問題としてきた。しかしながら、ウィルスの作者またはウィルスを保有している者がネットワーク上のウエッブページあるいはニュースグループなどを通じて配布した場合についてはどのようになるであろうか。

2　有害プログラムを保有している者が 202 条 a または 303 条 a ないし 303 条 b を実現する意図を有する者にその手段として利用するためのウィルス等の有害プログラムを配布した場合に、それらの罪の幇助犯が成立することに争いはない。ウィルスを配布してそれらの罪の実行を教唆した場合についても、教唆犯が成立することになる。

3　問題は、たんに一般的にネットワーク上のサーバにウィルス等の有害プログラムをアップロードした場合である[17]。単純のアップロードにとどまっているかぎりは何らの罪責も生じないであろう。しかしながら、第三者が有害プログラムのアップロードをどこかで知り、アップロードされたウィルス等を取得し、これを 202 条 a または 303 条 a ないし 303 条 b を実現すべく被害者のコンピュータに投与し、これらの罪が実現された場合にはどのようになるであろうか。

たとえば、アップロードした者がたんにデータをアップしただけでなく、html ファイルにウィルスであることを明記し、ウィルスの投与・他人のシステムの破壊を煽動した文言を付している場合、当該データを取得した者が実行にでたときに、概括的な故意による教唆犯の成立を認めることは可能である。しかしながら、有害プログラムのデータだけをアップロードしている場合、または、ウィルス等であること示しただけである場合については、かならずしも教唆犯の成立を認めることは困難である。この場合、教唆の成立に必要な故意の実行行為の特定が欠如しているからである。同様の理由により幇助犯の成立を認めることも困難であろう。誰かがダウンロードして配布するであろうという意図であったとしても、それだけを根拠に処罰するのは妥当ではない。 さらに、たとえ共犯としての行為形態を認めえたとしても、共犯の従属性があるため、配布行為を単独で処罰することはできない。ドイツにおいては、上述のコンピュータ刑法の構成要件に該当しないウィルス等有害なプログラムの配布行為を処罰するという刑法的保護の前提領域への可罰性の拡大については、否定的である[18]。

# 第5節 有害なコードに対する将来的な展望

現在のところ、ドイツにおいては、コンピュータウィルスをはじめとする有害なコードに対する新たな特別のストラテジーは存在しないとされる。現行の 303 条 a および 303 条 b で完全

---

[17] もちろん、TLG５条によりサーバを管理する企業がこれを排除する義務が生じうる可能性はある。
[18] この点はジーバー教授に対する口頭ならびに私信による質問によるものである。

に十分である考えられており、この点で争いは存在しない。そのかぎりで、抽象的危険犯の形態での「前提領域」の保護が必要であるとの議論すら存在しない。これは、刑法を法治国原理への適合させることためには、具体的な法益侵害性が必要であるとの認識が一般化していることが基本的な理由であろう。わが国に比べてより未遂犯の成立時期を早い段階で認め、かつ不能犯を可罰的とする法制にあり、そのような状況で未遂以前の段階である「前提領域」へその保護を拡大することは、刑法の謙抑性を害するものと考えられるからである。さらに、1987 年の第二次経済犯罪対策法の導入に際しては、この「前提領域」の保護についての一般的な議論がすでに十分検討され、現行の刑法の形態で十分であるとの認識が一般的に形成されているといえる。 もっともこのような考えの背景には、303 条 a ないし b が未遂犯を処罰しているため、たんにウィルスを配布・投与しただけでも処罰可能となるからである。この点、器物損壊罪および業務妨害罪について未遂処罰規程を持たないわが国の法制と比較する際に注意することが必要である。

さらに、わが国は、一般的な業務妨害罪の処罰に加え、電子計算機業務妨害罪が存在している。通常の業務妨害罪の構成要件については、争いがあるものの、判例にしたがい、その罪質を危険犯と理解するならば、ドイツにおいて未遂として処罰されているもの、あるいはウィルス等の有害なコードの配布行為それ自体も、わが国の現行法において捕捉することは可能となろう。このように、考えるならば、ドイツとの比較において、その処罰に相違があるのは、データ探知がわが国では不可罰であるという点である。不正アクセス禁止法は、認証の回避による無権限のサーバーへのアクセスを処罰するものであり、データ一般に対する無権限のアクセスからの法的保護は存在していない。情報処理の中核がデータにあると考えられる以上、その法的な保護を規定することがわが国の今後の課題となろう。

(担当 神奈川大学講師 石井徹哉)