



## 不正アクセスと刑法

その他のタイトル	Unauthorized Access and Criminal Law
著者	園田 寿, 北岡 弘章
雑誌名	関西大学法学論集
巻	47
号	6
ページ	893-913
発行年	1998-02-25
URL	<a href="http://hdl.handle.net/10112/00024511">http://hdl.handle.net/10112/00024511</a>

# 不正アクセスと刑法

北園  
岡田  
弘  
章 寿

- 一 はじめに
- 二 事例とその検討
- 三 おわりに

## 一 はじめに

昭和六二年になされたコンピュータ関連の改正刑法についての考察は既に多数の論考がある。これまで問題になっていた事例は多くが金融機関等のオンライン関連（金融機関の内部者あるいはCD犯罪といわれる）の不正行為が主流であった。<sup>(1)</sup>したがって、法改正もかかる事例を念頭になされたものと思われる。ところが近時、新聞報道等でインターネット等による外部からの不正アクセスによる被害も見られるようになって<sup>(2)</sup>いる。そこで本稿は、近時の具体的な事例を元に、右改正刑法の射程を洗い直すことを目的とするものである。

インターネットの普及と共にネットワークにおいて電子商取引を行うことへの関心が高まっているのであるが、他方インターネットはオープンなネットワークであることからそのセキュリティ上の欠陥、すなわち、プライバシー保護が十分でないとの指摘がされている。このように、インターネット上のデータについてのセキュリティの確保に対して関心が高まっていることから不正アクセスに対して刑罰による処罰を望む声も強くなっている。また、インターネットが世界に広がるネットワークであることから、国によっては不正アクセスそのものが犯罪になるとされており、外国から日本へ捜査依頼がきても、双罰性の原則から捜査協力ができないとの指摘もなされており、<sup>(3)</sup> 捜査当局による不正アクセス取り締まりに対する対応も検討されているようである。

このように立法化が予定されているとしても、それは、現行法によつてはカバーできないことを明らかにした上で進めるべきであろう。その意味で、現在把握されている不正アクセスの事例<sup>(4)</sup>を検討した上で、現行法の解釈論上の射程を明らかにする必要がある。

(1) 関西大学の加藤敏幸教授もわが国の「コンピュータ犯罪」は、従来から金融機関等のオンライン・ネットワーク関連の犯罪が主流であり、金融機関内部犯行であるオペレータによるデータ改竄などの不正操作やCDカード偽造事件が大半であった。また近時においても、自動車登録ファイルや住民基本台帳ファイルなどの電磁的公正証書原本不実記録の犯罪が多いと言われていると指摘している。週刊「ダイヤモンド」別冊研究者へのメールインタビューより (<http://www.alpha.co.jp/chojikan/intview/katoh.html>)

(2) 不正アクセスの被害については、被害者からの報告をもとにJPCERT(コンピュータ緊急対応センター・<http://www.jp-cert.or.jp/>)のホームページで公表されているが、犯罪には暗数がつきものであり、潜在的には多数の不正アクセスが行われていると考えられる。特に、企業側の心理として不正アクセスにあっては、不名誉かつ企業の信用にも関わる事故故、不正アクセスにあっては、そのことを秘匿する傾向にあることも指摘されているところであり、不正アクセス

スの実態をわかりにくくしているとの指摘も為されている。

(3) 「兼元・ICPO総裁に聞く」一九九七年二月三一日読売新聞

(4) なお、コンピュータ犯罪を論じる際にはいわゆるコンピュータウイルスによる被害についても論じられることも多い。実際に不正アクセスよりも報告されている件数等も多く被害も広範であることから、それに対する検討も重要である(ウィルス被害についてはIPA情報処理振興事業協会のコンピュータセキュリティ対策のホームページを参照のこと <http://www.ipa.go.jp/SECURITY/index.html>)。ウィルスについては、コンピュータに感染した段階では処罰できないと解されており、発病の段階でしか処罰できないとされている(平成八年四月に警察庁情報システム安全対策研究会発表の「情報システムの安全対策に関する中間報告書」参照)。ただし、不正アクセスとウィルス被害の問題は質的に異なるものである。コンピュータウィルスの感染は、主としてコンピュータの管理者自身の行為を介在することによって感染することが多く、例えば、ウィルスの入った電子メールを開封したり、他人のウィルスに感染したソフトウエア等をコピーする際にウィルスに感染しそれをインストールする際に感染するのである。したがって、必ずしもウィルスは不正アクセスを前提としないので、検討は今後に譲りたい。

## 二 事例とその検討

1 コンピュータに関連する不正行為の類型はさまざまなのがあるが、①データの不正操作 ②コンピュータの無権限使用 ③データの不正入手、漏示 ④コンピュータの破壊に分けることが一般的であると思われるので、便宜的にかかるとの類型ごとに事案を検討することとする。<sup>(1)</sup>

(1) 的場純男「コンピュータ犯罪と刑事法上の問題点」ジュリスト八四六号七頁。

(2) いくかの事案は、goo (<http://www.goo.ne.jp/index.html>) infoseek (<http://www.infoseek.co.jp/>) といった検索エンジンを利用し検索したものである。

不正アクセスと刑法

2 ① データの不正操作

事例 一 (京都地判平成九年五月九日判時一六一三号一五七頁)

パソコン通信のサーバーの電子掲示板等に他人名義で虚偽の情報を書き込み、同情報を閲覧したのから商品代金名下に振り込み送金された金員を騙取すると共に、右詐欺事犯の発覚を免れるため、パソコン通信のホストコンピュータ上に登録された他人の住所等を無断で変更するなどした被告人に対し有罪判決が言い渡された事案。

判決によると、自らプログラムしていたハッキングソフト (GOMEMBER LIST) に記載されたニフティの会員情報をもとに会員のパスワードを解析するソフト) を利用して、他人のパスワードを探り当てたりしていたが、これを利用してニフティ会員に成り済まして売買名下金員をだまし取ろうと考えるようになり、①私書箱業者を利用して架空の住所を設定して、右住所で実在する他人名義の銀行口座開設申込書を偽造して口座を開設し、②ニフティのホストコンピュータに保存されている会員の住所情報を架空の住所に変更したうえ、③他人のパスワードを使ってニフティ内に勝手に潜り込み、ニフティが会員に提供する電子掲示板に実在する会員名義でパソコンのCPUとメモリーを売るなどと虚偽の情報を掲載し、この情報を閲覧して申し込みをしてきた被害者らに対し、さらに商品を確認して送付する、代金等は前記口座に入金して欲しいなどの電子メールを送信するなどして、被害者から右口座に振り込み送金を受けて代金名下に八六万円余を騙取した。④その後、被害者らからの追求や警察の捜査を免れるため、前記ホストコンピュータの前記住所情報を私書箱業者の住所から別の住所に変更するなどした。

①の事実につき私文書偽造同行使、②④の事実について私電磁的記録不正作出罪、③の事実につき詐欺罪の成立を認めた判例である。

本判決については、被告人が争わなかったようであり、個々の犯罪の正否に関する説明はなされていないがここで若干の検討を加えることとする。

まず、電子掲示板に虚偽の情報を掲載し架空の部品販売をすることは、多数人が関与するパソコン通信等オープンなネットワークの特徴を利用した新しい形態の犯罪である。しかし、単に手段としてパソコン通信を使っているにすぎず、人を欺いたと言える以上は、通常の詐欺罪に該当することになる。ちなみに、電子計算機使用詐欺罪について定める刑法二四六条ノ二が「前条に規定するもののほか」と規定していることから明らかなように、電子計算機使用詐欺罪は詐欺罪の補充類型であり、詐欺罪が成立する場合には、電子計算機使用詐欺罪は成立しない。

では、私電磁的記録不正作罪の点についてはどうか。

まず、人の事務処理を誤らせる目的が必要であるが、「人の事務処理を誤らせる目的」とは、一般に不正に作られた電磁的記録が用いられることにより、他人の事務処理を誤らせる目的のことを指す<sup>(1)</sup>。

右判旨ではこの点、「パソコン通信サービス『ニフティサーブ』を提供するニフティ株式会社を誤らせる目的で、<sup>(2)</sup>」としか記載されていない。本件被告人は、ニフティサーブの会員のID及びパスワードを使用して、その会員の住所及び電話番号を変更させており、ニフティ株式会社はかかる情報を元にして、会員の管理を行っているのであるから、かかるデータを変更させたことは、人の事務処理を誤らせるものといえよう。そして、「不正に」作るとは、権限なく又は権限を濫用して電磁的記録を作ることをいうとされているから、<sup>(2)</sup> 会員の住所・電話番号を架空のものに変更することは、権限がない場合に当たるとであろう。

次に、「ニフティ株式会社経営情報システム部に設置されたコンピュータの記憶装置内の『顧客データベース

「ファイル」は、「その事務処理の用に供する権利、義務または事実証明に関する電磁的記録」にあたる。「権利、義務、または事実証明に関する」の意味は、私文書偽造の場合と同義であるとされており、実社会生活に交渉を有する事項を証するに足りるものであれば足りるから、顧客管理に関する（これに基づき課金等の事務も行われる）ファイルは事実証明に関する記録である。又、電磁的記録とは「一定の記録媒体の上に情報あるいはデータが記録、保存されている状態を表す概念<sup>(4)</sup>」とされていることからコンピュータの記憶装置内の「顧客データベースファイル」はこれに該当し、したがって、私電磁的記録不正作出罪が成立するとした右判旨は妥当であろう。

なお、本件の場合には、刑法一六一条の二第三項の不正作出電磁的記録供用罪については起訴されていないようである。

罪数については、私文書偽造・同行使が牽連犯となり、それらと詐欺罪、私電磁的記録不正作出罪とが併合罪の関係となっている。

右判決では、電子計算機使用詐欺罪については、何らふれられていないが、その成否についても検討しておく。

本件行為が行われたパソコン通信は有料のサービスであり、他人名義のID、パスワードを使用した場合には、その名義人に対してアクセス時間に対応した課金が為されるシステムとなっている（これは、インターネットにプロバイダーという接続業者を介して接続する場合も同様である）。このような場合、他人のID、パスワードを利用することによって、本来支払うべき課金を免れたことを捉えて、電子計算機使用詐欺罪が成立するのではないかが問題となる。

本件事案は、従量制の課金が行われるサービスの事案であるが、立法段階では有料のデータベースに関して議論が

なされており、本質的な差異はないことから、有料データベースでの議論を中心に見ていくこととする。

この点、前記刑法改正の際の法務省刑事局立案担当者（以下「立案担当者」という）の説明によれば、「有料データベースの利用ないし有料サービスの享受という意味での財産上の利益についていえば、これは、契約者を装ってそのID番号及びパスワードを電子計算機に入力したこと自体によって得られたものであって、不実の記録に基づいて得たものとはいえない。他方、正規の利用料金の支払を免れるという意味での財産上の利益については、データベースの利用契約者においては、契約者ID番号とパスワードを使用してなされた利用については、契約者が当然料金を支払うべきものとされているため、不正利用者は、データベースとの関係で不実の記録とは無関係に不法行為による損害賠償義務を事実上免れたに過ぎないと見るべき場合が多いと思われる。また、このように考えると、他人の電話機を無断で使用するような場合と同様、データベースの課金ファイルに作出される記録は、当該ID番号の客観的な使用度数そのものを記録しているのであって、不実の記録が作出されたとはいえないと見る余地もあろう。」として電子計算機使用詐欺罪の成立を否定している。<sup>(5)</sup>

また、他の立案担当者も、有料データベースの使用について、用いられたパスワードは、本来の名義人がデータベース提供業者に料金を支払うことを条件にデータベースを利用する契約に基づいて提供された鍵のようなものであって、これを行為者が勝手に用いたとしても、パスワード自体は虚偽の電磁的記録とはいえず、それゆゑ行為者が得たといえなくもない財産上不法の利益は虚偽の電磁的記録に基づいて得られたものでないとする。<sup>(6)</sup>

これに対して西田教授は、「使用料金の決済が電子計算機によって処理されている場合、その課金ファイル上に、あたかも本来の保有者が利用したかのような記録が残るときは、債務免脱型の不法利得として、本条前段に当たるこ



となる」として本罪の成立を肯定されている。<sup>(7)(8)</sup>

それでは、かかる点についてどう解するべきであろうか。

「虚偽の情報」とは、当該システムにおいて予定されている事務処理目的に照らし、その内容が真実に反する情報といい、「不正の指令」とは、同じく事務処理の目的に照らし、与えられるべきでない指令をいうとされている。<sup>(9)</sup> かかる定義については特段の異論はないようである。まず、「虚偽の情報」といえるのかについて検討する。IDとパスワードによる認証システムにおいて予定されている事務処理目的というものを考えるならば、IDとパスワードが一致していることを確認することにある。IDと入力すべきパスワードが一致している以上、その内容が真実に反しているとはいえないであろう。では、「不正の指令」にあたらぬであろうか。「与えられるべきでない」ということからするならば、「虚偽の情報」と異なり、ある程度規模的な要素を加味して解放することが可能である。他人のIDとパスワードを入力することは、与えられるべきでない情報であると見ることが可能であろう。ただし、不正の「指令」とは、プログラムによって情報を与えたということの意味すると解するのが一般的である。<sup>(10)</sup> 確かに、このように解すると、「虚偽の情報」と「不正の指令」の区別をした意味がなくなるが、さりとてデータを入力することとプログラムによってデータを送ることがコンピュータのシステム上質的に異なるものではない以上、かかる区別を採ることは実際上困難であることから、「不正の指令」の要件を満たさずと解することも可能であると考ええる。

「不実の」とは、客観的にみて真実に反する内容であることを意味している。この点でも、実際に使用していない契約者が使用したかの様な記録が作出されるのであるから、かかる要件では構成要件該当性を否定できないと思われる。

では、「財産上不法の利益を得」たといえるであろうか。「財産上の利益を得」たとえ、財産権の得喪、変更に係る不実又は虚偽の電磁的記録に基づき事実上財産を自由に処分できる利益を得ること及び債権者の追求が事実上不可能となりかねない状態を生じさせて債務を免れることなどであると指摘されている。立案担当者の指摘するように、有料サービスの享受という意味での財産上の利益についていえば、それは不実の電磁的記録を作成して得たものではなく、電磁的記録との因果関係なしに利益を得ていることになるのである。ただし、「データベースの利用契約者においては、契約者ID番号とパスワードを使用してなされた利用については、契約者が当然料金を支払うべきものとされている」と指摘されている点については、契約者のパスワードの管理にまったく帰責性がないような場合にまで料金の支払い義務を負うとするのは疑問である。したがって、行為者が代金支払債務を免れているのではないかとの疑問もあり、この点についてはなお検討の余地があるろう。

したがって、一応、有料サービスの無権限利用によって電子計算機使用詐欺罪は成立しないと考える。

(1) 鶴田六郎・横島裕介・米澤慶治編「刑法等一部改正法の解説」(一九八八年)八五頁。なお同書は以下「米澤編解説」と略する。

(2) 「不正に」という要件に権限濫用の場合を含むのか否かについては設置主体との関係で、無権限でまたは権限を逸脱して電磁的記録を作成することとする説と権限を濫用して電磁的記録を作成する場合を含むとする説の争いがある。有形偽造と無形偽造とを区別していないことに示されるように、文言自体の意味として権限濫用の場合を含まないと解することは困難である。また、権限を逸脱した場合と濫用した場合の実際上の差は少ないものと考えられる。なお、電子計算機使用詐欺罪の事案である(東京高判平成五年六月二十九日判時一四九一号一四一頁)が、「信用金庫支店長によるオンラインシステムを利用した振込み入金処理等について、本位的訴因である電子計算機使用詐欺罪の成立を否定し商法の特別背任罪の成立を認めたと原判決が誤りである」として電子計算機使用詐欺罪の成立を認められた事例が、参考になる。

(3) 事実証明に関する文書とは、実社会生活に交渉を有する事項を証するに足りる文書(最決昭和三三・九・一六刑集一二・一三・三〇三二)であるとされている。ただし、社会生活において一定程度以上の重要性を有するものに限られると解すべきである。

(4) 刑法七条ノ二は刑法におけるコンピュータ犯罪における共通の要件として電磁的記録という要件を設けている。便宜上ここでその概要を簡単に整理することとする。

かかる定義規定新設の理由は、「コンピュータに用いられる記録には、様々な性質のものがあることから、今次改正による処罰規定の適用範囲を明らかにするため定義規定を設けることが適当と考えられ」たためとされている(的場純男・河村博米沢編解説六〇、六一頁)。

処罰範囲の限定の意味は、「記録」であって「記録物」ではなく(ハードディスクには多数のファイルがあるので)、さらに、情報や秘密と言ったものそれ自体を客体とするものではないことを明らかにした点にある。そして電磁的「記録」とされている以上は、中継されている途中、たとえば転送中のメール上のデータは、刑法上の電磁的記録に当たらないとされている(的場純男・河村博前掲米沢編解説六一頁)ただし、通信あるいは処理中のデータを操作した場合であっても、その結果として、あるべきでない電磁的記録ができあがるのであれば、その時点で、不正作罪の成立を認めうる(中森喜彦・「コンピュータと文書犯罪」刑法雑誌二八巻四号五〇二頁)ので、通信中のデータに対する行為がすべて不可罰となるわけではない。

(5) 的場純男・前掲米沢編解説一三二頁。

(6) 米澤慶治・大コンメンタール刑法(一九九一年)一〇巻一五〇頁。

(7) 西田典之「コンピュータと業務妨害・財産罪」刑法雑誌二八巻四号。

(8) 前田教授は、他人の電話回線が接続された配電盤の電話配線接続端子に自分で改造した電話機様の器具を接続させ、回線から自己の開設したダイヤルQ2番組への通話状態にしてそれを長時間継続させ、NTTから情報料名下に二〇〇万円を自己名義の銀行口座に振り込ませたという事案につき、通話記録自体は「虚偽」とはいえないので、二四六条の二の「虚偽の情報」には該当しないとし、二四六条の二にいう「不正の指令」とは、財産権に係る記録を作出・変更するようなプログラムを用いる行為を意味するから、不正の指令にもあたらないとして、電子計算機使用詐欺罪の成立を否定している。(L

esson 刑法37(一九九七年)三三四頁 岡山地判平成四年八月四日判例集未登載の判決を元にした説例の様である。

(9) 東京高判平成五年六月二十九日は、「虚偽の情報」とは、電子計算機を使用する当該事務処理システムにおいて予定されている事務処理の目的に照らし、その内容が真実に反する情報をいうものであり、本件のような金融実務における入金、振込入金(送金)に即していえば、入金等に関する「虚偽の情報」とは、入金等の入力処理の原因となる経済的・資金的実体を伴わないか、あるいはそれに符合しない情報をいうものと解するのが相当であるとされている。(判時一四九一号一四一頁・西田典之・判例評論四三三号七四頁)

(10) 山中敬一・情報ネットワーク時代の法学入門(一九八九年)一七九頁。

### 3 ② データの不正入手

#### 事例 二

七〇〇〇人分のパスワードが漏えい、セキュリティへの認識不足が原因

平成九年五月二五日、NTT PCコミュニケーションズ(本社東京)のインターネット接続サービスのユーザー約七〇〇〇人分のパスワードが漏えいした。会員のパスワードを格納したシステム開発用サーバーが不正アクセスを受けたためだ。このサーバーは不正アクセスに対する対策に不備があった。

その後の調査の結果、五月二五日の二二時三八分からの二四分間、スタッフ用のIDを使ったアクセスがあった。正規のスタッフはこの時間にアクセスしておらず、これが不正なアクセスであることが判明した。この二四分間にだれかがパスワード・ファイルを参照した記録も残っていたため、NTT PCはパスワードが漏えいした可能性はきわめて高いと判断した。

当時、NTT PCの開発部門は新しい顧客管理用ソフトを開発しており、サンプル・データとして二月一〇日時点の全会員のパスワード・ファイルを使っていたという。この開発用サーバーはインターネットに直接接続されており、「ファイアウォールなど特別なセキュリティ措置は施していなかった」(広報)ため、外部からの不正アクセスを受けたとみられる。

不正アクセスと刑法

三九(九〇三)

（関 信浩 日経コンピュータ六月三日号 <http://biztech.nikkeibp.co.jp/biztech/WCS/Internet/bj970620061.html>）

### 事例 三

NTT情報通信研究所のコンピューター通信網が外部から侵入されていた問題で、同社ヒューマンインタフェース（HI）研究所（神奈川県横浜須賀市）の通信網も今年3月侵入を受け、大量の社外秘資料が漏えいしていたことが六日、毎日新聞社の調べで明らかになった。侵入は情通研と同様、研究者用に設けていた電話回線経由で安全対策のすきを突いていた。

毎日新聞の調べでは、侵入者は情通研と同じ東北地方の二〇代の会社員。会社員の証言によると、今年三月二〇日、自作の専用のプログラムでHI研のホストコンピューターに接続する電話番号を突き止めた。さらにID（個人識別番号）とパスワード（暗証番号）とともに「guest」と入力して侵入。HI研の二つのホストコンピューターから、A4判に印刷して約三〇〇ページにわたる資料を入手した、という。

ソフトウェア関係者によると、「guest」のIDとパスワードはコンピューターを設置する際のテスト用に使われ、使用後は通常削除されるという。今回は何らかの理由で消し忘れたとみられる。

（電子データが危ない・毎日新聞jamjamサイバー編集局 <http://www3mainichi.co.jp/hensyu/rame.html>）

右の事例は、いずれもパスワード等が漏洩した事案つまり不正行為者の側から見ればデータの不正入手の事案である。電子計算機使用詐欺罪については、情報を不正入手すること自体によって得られる利益と、被害者側における情報自体の価値の減少とは必ずしも対応するものでなく、財産上の利益が被害者の不利益において犯人に移転したといえないとして成立しない、すなわち「財産上の利益」を得たとは言えないとされている。

また、電子計算機損壊等業務妨害罪については、立案担当者の説明によれば無権限使用の場合と同様に同罪は成立

しないとされる。<sup>(2)</sup>

事案二のように一定の者のみがアクセスすることが許されているシステムにおいては、通常ログファイルという、誰がいつアクセスしたのかを自動的に記録する様なシステムとなっているのが通常である（かかるファイルがなければ不正アクセスを発見することも不可能である）。そこで、ログファイルの作成を捉えて私電磁的記録不正作出罪に問うことができないであろうか。

まず、私電磁的記録不正作出罪が成立するためには、電磁的記録が単に作出されただけではなく「不正に」作出されたと言えなければならぬ。「不正に」とは、権限なく又は、権限を濫用して電磁的記録を作るということである。他人のID・パスワードを使用する権限はなく、他人のID・パスワードを利用しなければ、ログファイルを作成することもできないという意味で、「不正に」との要件を満たすと考える。この点、ログファイルは、システムの機能として自動的に作成されるファイルであって、不正アクセスをした者が意図して作成したファイルではないことから、電磁的記録を作出したといえないとの考え方もあろう。しかしながら、コンピュータを使った事務処理においてはある程度プログラムによって自動的にファイルが作成されることが予定されており、ID・パスワードの入力行為をとらえて作成したと見ることも可能であろう。また、ハッキングを意図的に行うようなものであれば、十分ログファイルが作成されることも認識しており、このような実態に鑑みれば、作出したものと見ることも十分可能である。

それでは、人の事務処理を誤らせる目的があると言えるであろうか。「人の事務処理を誤らせる目的」とは、不正に作られた電磁的記録が用いられることにより、他人の事務処理を誤らせる目的のことであって、ここに「事務処理」とは、財産上、身分上その他の人の生活関係に影響を及ぼし得ると認められる事柄の処理をいい、業務として行

3 われる事務か否か、法律的な事務か否か、財産上の事務か否かを問わないと説明されている。ログファイルは、当該コンピュータにアクセスすることができる者だけがアクセスしているかを確認する手段として不可欠のファイルであり、他人が使用したかの様なログファイルが作成されることは、ログファイルの証明機能を誤らせることになる。特に、パソコン通信のような有料サービスの場合には右ログファイルを前提に課金を行うことから、他人のIDとパスワードでアクセスしたような場合には、課金を誤らせるという意味で、人の事務処理を誤らせる目的は認められることになろう。ただし、本件では、内部の研究者向けということで、課金を前提としたシステムではないことから、人の事務処理を誤らせる目的ありといえるのか若干疑問である。特に、かかる要件が、処罰範囲を限定するために設けられたものであることからすれば、かかる場合をも含めることは、立法趣旨に反することになろう。

また、ログファイルが自動的に作成されることから、ハッキングのような態様ではなく、たまたまID・パスワードを知っていたらずら半分に無権限使用をしたような場合は、目的あるいは故意を欠く場合もあり得るであろう。

(1) 的場純男・前掲米澤編解説一三二頁。

(2) この点については、無権限使用の項目参照。

(3) 鶴田六郎Ⅱ横島裕介・前掲米澤編解説八五頁。

#### 4 ③ コンピュータの無権限使用

##### 事例 四

東京大学大型計算機センター(東京都文京区)が学内外の研究者用に登録制で運用しているコンピューターシステムが一〇年近

く不正アクセス（無権限使用）されていたことが一日、毎日新聞の調べで分かった。登録していない人物が安全対策の甘さによって侵入、盗み見た正規利用者のID（個人識別番号）とパスワード（暗証番号）を勝手に使って接続したうえ、同システム経由で首相官邸などへの侵入も試みていた。同センターは全面的な安全対策の見直しを始めた。

毎日新聞が入手した資料によると、この無登録者が初めて侵入したのは一九八〇年代末。首都圏の別の私立大学教授に八六年に発行された二つのIDとパスワードを勝手に使用、電話回線経由で不正アクセスを繰り返していた。

無登録者の証言によると、当初の侵入目的はスーパーコンピュータを使うことで、ID、パスワードともに「news」を入力したところ、侵入できたという。以後、不正専用のプログラムを使って複数の利用者のIDやパスワードを割り出し、これで最近も利用を続けているという。

（電子データが危ない・毎日新聞jamjamサイバー編集部 <http://www3mainichi.co.jp/hensyuu/frame.html>）

この事案については、当初の侵入目的はスーパーコンピュータを使うことで、ID、パスワードともに「news」を入力したということであるから、他からパスワード等を取ったのではなく、典型的な無権限使用の場合である。（それ以降の侵入については、データの不正入手の問題を含むことになる。）

このようなケースの場合、設置管理者の意思に反してコンピュータを使用されたとして、電子計算機損壊等による業務妨害罪（刑法二三四条の二）に該当しないかにつき検討する。

立案担当者の説明によれば、右のような行為は構成要件該当性が否定されると解されている。その理由は、右のような行為は、通常、「使用目的に沿うべき動作をさせず又は使用目的に反する動作をさせて」という要件に該当しないこと、一般的に、そのような行為によって、業務の遂行が外形的に妨げられるとは認められないので、「業務を妨害し」という要件にも当たらないからとされている。<sup>(1)</sup>



西田教授は、右のような行為の場合、他人のパスワードを用いている点をとらえて、「虚偽の情報若しくは不正な指令」を与えたとも評価しうるところであるし、また、電子計算機の設置者すなわち当該コンピュータシステムを管理しているものからすれば、無権限者にかかる電子計算機の利用はその意思に反する動作であって、「使用目的に沿うべき動作をさせず、または使用目的に反する動作をさせて」いるとも十分可能であるとされている<sup>(2)</sup>。

神山教授は、「不正の指令」を与えたと解釈しうる余地は十分にあるが、当該パスワードによってコンピュータを使用することが、たとえ誰によってなされようとも、設置者の客観的目的に反したとみることは通常無理であり、さらに、大型コンピュータを使用して演算や検索をする場合には、その処理能力が大きいため同時に多くの者がそれを使用でき、このような場合には無権限使用者の使用が他人の業務を妨害することは通常考えられないとされ、解釈論として、無権限使用は本条の構成要件該当性がないものとされている。

まず、同条の「使用目的」とは具体的な業務遂行の場面において実現しようとしている目的をいうと立案当局は解しているようだが、文言上はかかる限定を読みとることは困難であり、神山教授が指摘されているように「目的」をどう捉えるかにより解釈は分かれることにならう。そして、当該コンピュータシステムにパスワードが設定されている場合には（本件では設定されている）、設置者の客観的な目的に反したとみることも可能である。

さらに業務が妨害されていないとの点についても、西田教授が指摘されているとおり、マジックホン事件について偽計業務妨害罪の成立を肯定した最高裁決定（最決昭和五九年四月二七日刑集三八巻六号二五八四頁）の立場によれば、業務を妨害されているとみる事が可能である。すなわち、マジックホンの取り付けにより課金装置の作動を不能にしても、それは課金業務自体をストップさせたり外形的に混乱させる訳ではなく、当該加入入電話者に対する課金

業務における個別的な料金計算を誤らせたにすぎないと見ることが可能なのである。「業務を妨害し」の意味については、偽計・威力業務妨害罪のそれと同様であると説明されていることからするならば、「外形的に」混乱していないからといって、解釈論上業務が妨害されていないとは言えないように思われる。<sup>3)</sup>

業務妨害罪の保護法益は、人の業務の遂行の意思決定あるいはその遂行の実現としての行動の自由ととらえられている（立案担当者の説明によれば二三四条の二も保護法益は同様である）。そうすると、確かに、無権限使用されていたとしても、コンピュータシステム自体に何ら本来の動作と異なることがない以上、コンピュータシステムの運営の意思決定や実際の運営の自由をなんら「妨害」されていないのではないかと見ることがもできる。しかし他方、妨害されるのはコンピュータシステム自体ではなく、業務である以上、コンピュータシステムに何らの負荷がかからなかったとしても業務が妨害されたと言いつ得る場合があるように思われる。（コンピュータシステムに負荷がかかる等の点については「使用目的に反する動作をさせて」の解釈の問題である。）

また、仮に電子計算機損壊等業務妨害罪に該当しないと解したとしても、マジックホンの利用が、偽計業務妨害罪に該当するのであれば、少なくとも有料の電子計算機のシステムの無権限使用については、偽計業務妨害罪で処罰することが可能ではないかとの疑問が生じる。マジックホン事件においては、「課金装置の作動を不能にした行為」を捉えて業務妨害罪を肯定しており、有料の電子計算機の無権限使用も、課金プログラムの作動を不能にしている点は共通しているからである。

本件事案については、新聞記事では明らかでないが、大学のしかも内部の研究者向けであることから、課金を行っていないかたのではないかと考えられる。とするならば、不正アクセスがあるか否かを発見するのが東京大学大型計

算機センターの本来的な業務ではないという意味で、本罪には該当しないと考えられるのではないだろうか。この点、課金業務を外形的に妨害したと解しうるマジックホンの事案と異なるところである。

- (1) 横島裕介・前掲米澤編解説一〇五頁。
- (2) 西田典之「コンピュータと業務妨害・財産罪」刑法雑誌二八巻四号五一七頁。ただし、西田教授も運用上は、立案当局の説明通りに運用されるべきである旨指摘されているところである。
- (3) マジックホン事件は、昭和六二年改正前の事件であるが、改正後であれば、電子計算機使用詐欺罪で立件されていた可能性が高い。この点、国際電信電話株式会社の回線に通話料金が計算されないようパソコンで不正信号を送った上で国際通話を行ってその通話料金の支払を免れたことが、電子計算機使用詐欺罪にあたりとされた判例がある(東京地判平成七年二月一三日判時一五二九号一五八頁)。
- (4) 山口教授はマジックホン事件の決定につき、「通話料金課金業務を問題としつつも、あくまでも「課金装置の作動を不能にした行為」を捉えて業務妨害を肯定することにより、業務の外形的妨害を認めたものであ」と評されている。山口厚・判例百選Ⅱ第三版・二五一頁

#### ④ コンピュータの破壊

#### 事例 五

インターネット・サービス・サービスプロバイダーの認証サーバー、WWWサーバー等のシステムに何者かが侵入し、これらのシステム中のプログラムやデータを破壊して、インターネットへの接続、ホームページの掲示等のサービスを停止させた。

(露木康浩・コンピュータ犯罪等の現状と法制度上の課題・ジュリスト一一一七号一〇四頁より引用)

#### 事例 六 朝日放送サイトにわいせつ画像を流した男を起訴

朝日放送（本社・大阪市）が開設しているホームページの画像の一部がわいせつ画像に切り替わっていた事件で、大阪地検は二日、埼玉県富士見市のコンピューター会社員（二七）を電子計算機損壊等業務妨害、わいせつ図画公然陳列の罪で起訴した。ホームページなどの内容を改ざんする「クラッカー」が、電子計算機損壊等業務妨害罪で起訴されたのは初めて。

起訴状などによると、コンピューター会社員は、五月一八日午前六時四〇分～同一〇時二〇分の間、東京のインターネット接続業者を経由して、朝日放送のウェブサーバーに侵入。不正な指令を与え、ホームページ「ABCセンター」の天気予報データファイル九ページを改ざん。このうち、五ページをわいせつ画像と入れ替えて朝日放送の業務を妨害した。大阪府警は、朝日放送からホームページの交信記録の提出を受け、インターネット接続業者を割り出すとともに、会社員がISDN回線を利用していたことから電話番号が判明、同月二三日に逮捕した。

（毎日新聞 jamjam インターネット事件取材班 <http://www.mainichi.co.jp/hensyu/jiken/gazo/0612-3.html>）

電磁的記録とは「一定の記録媒体の上に情報あるいはデータが記録、保存されている状態を表す概念<sup>(1)</sup>」であるから、ホームページのデータは、インターネットのサービス・プロバイダーのサーバコンピュータ上のディスクアレイ（記録媒体）上に記憶されているものであって、一定の期間記憶されているものであるから、これは、電磁的記録にあたる。そして、システム中のデータの破壊をした場合には、当該事務処理の場面において与えられるべきでない指令を与え、その結果電子計算機のサービスを止めることによって使用目的に沿うべき動作をなさしめず、結果としてインターネットへの接続サービス等の業務を行えないようにしていることから、事例五が刑法二三四条の二の電子計算機損壊等業務妨害罪に該当することは明らかである。

わいせつ画像を送信した事案（事例六）については、ホームページ上のデータを削除し、かつ、わいせつ画像を送信しているが、「使用目的に沿うべき動作をなさしめず」とは、具体的な業務遂行において当該電子計算機を使用し

て実現しようとしている目的に適合するような動作をいうとされているので、ホームページ上で表現しようとしていたことを妨げている以上、かかる要件も満たすものである。そして、業務の内容は偽計威力業務妨害罪におけると同様であり、人が反復継続する意図で行う経済的社会的活動を妨害することをいい、ホームページ上にデータを表示することは経済的社会的活動であるから、データの表示を妨げたことは、業務を妨害したと言えよう。<sup>(4)</sup>

したがって、事例二についても二二四条の二に該当することとなる。<sup>(5)</sup>

(1) 的場純男・河村博・前掲米澤編解説六一頁。

(2) (3) 横島裕介Ⅱ米澤編解説一〇二頁。

(4) わいせつ画像を送信した事案については、電子計算機損壊等業務妨害罪の成立だけでなく、わいせつ図画公然陳列罪の成立も認められている。電子データとわいせつ図画公然陳列罪との問題点については、「わいせつの電子的存在について」関西大学法学論集第四七巻第四号五四一頁以下参照。http://w3scan.or.jp/sonoda/

(5) なお、本件ではデータを破壊しており電磁的記録毀棄罪も同時に成立するが、両罪は、その保護法益、罪質を異にしており、電磁的記録毀棄罪が電子計算機損壊等業務妨害罪に吸収されるというような関係にはなく、通常両罪は観念的競合の関係にある(的場純男・前掲米澤編解説一六一頁)とされている。

### 三 おわりに

以上、具体的な事例を元に昭和六二年改正による、不正アクセスの処罰の射程について検討してきたが、一般に単なる無権限使用や情報の不正入手は処罰されないとの説明がなされているところであるが、無権限使用については当該構成要件の文言上右のような行為が処罰されないということは必ずしも明確となっていないといわざるを得ない。文言の解釈によっては、十分に処罰が可能であるように思われる。現在のところ、無権限使用や情報の不正入手につ

いて処罰された例は見あたらなかったが、これも六二年改正の趣旨に沿った運用がなされているからと見ることできるのである。

無権限使用については、本稿で検討したように、現行法でも部分的に処罰できる場合があるのではないかと考えているが、例えばネットワーク上に流れているデータを不正に入手したような場合には、現行法の適用によっては処罰し得ないのであり、かかる行為を処罰するのであれば、やはり立法化することになるのであろう。

ただし、立法化に際しては、不正アクセスされる側のセキュリティシステムの問題についても考慮すべきである。仮に、セキュリティシステムが技術的に完全であって不正アクセスを許さないレベルであれば、あえて刑罰をもつてかかる行為を処罰する必要はないであろう。今回検討した事例においても、事例二、三、四、については、パスワードは設定しているものの、実際にはある程度知識のある者であれば試すようなキーワードをパスワードにしており（又は削除することを忘れていた）、かかるセキュリティの不備さえなければ十分不正アクセスを防げた事案であるといえるのである。セキュリティを施すかどうかは、コンピュータを設置する側の意識の問題であって、これを施さないコンピュータシステムをも刑罰で保護する必要があるのかはなお検討する必要があると考える。<sup>(1)</sup>

(1) セキュリティについての一般的な資料としては、郵政省の報告書「情報通信ネットワークの安全・信頼性に関する研究会」を参照されたい。 <http://www.mpa.go.jp/policyreports/japanese/group/internet/net-index.html>

#### 【追記】

本稿は、何回かの研究会において不正アクセスについて園田と北岡が議論した内容の一部であり、研究会での討論を踏まえて最終的に北岡がまとめたものである。