

(判例評釈)

不正アクセス罪と他罪との罪数関係

岡 田 好 史

(不正アクセス行為の禁止等に関する法律違反、電子計算機使用詐欺、私電磁的記録不正作出、同供用、有印私文書偽造、同行使、詐欺、窃盗被告事件、平成15・8・21東京地裁刑6部判決、平成15年(刑わ)第980号・第1795号・第1988号、公刊物未登載[TKC文献番号:28095229])

キーワード

【事実の概要】

被告人は、①不正に入手したXの識別符合とA社発行のX名義のクレジットカード番号等の情報を使用し、インターネットを介して同社のオンラインシステムに不正にアクセスして虚偽の情報を与えた上、インターネット上の商品の通信販売において、前記カード番号を入力するなどして、購入名下に商品を騙し取ろうと企て、クレジットカード会社のサーバ・コンピュータに不正にアクセスしてXが住所を変更した旨の虚偽の情報を記憶・蔵置させ、当該会員になりすましてインターネット通信販売により商品を注文、受領して窃取し、あるいは騙取し、②不正に入手したYの金融機関口座番号や識別符合等を利用して、銀行のサーバ・コンピュータに不正にアクセスし、Yが住所を変更した旨の虚偽の情報を記憶・蔵置させた上、Yを装って必要書類を偽造・行使してキャッシュカード等の再発行を請求、これを受領し、騙取するとともに、同銀行のサーバ・コンピュータに不正にアクセスしてYが定期預金を解約した旨の虚偽の情報、および新たな暗証番号を設定した旨等の虚偽の情報を記憶・蔵置させた上、キャッシュカードおよび暗証番号を使用して現金自動預払機から現金を引き出して窃取し、さらに③不正に入手したZほか1名を利用権者として付された識別符合である電話取引用暗証番号およびオンライン用暗証番号を入力して、銀行のサーバ・コンピュータに不正アクセスを行い、預金者が、被告人があらかじめ開設しておいた架空名義の預金口座に対し送金する手続を行った旨の、あるいはいったん他の預金者の口座に送金する手続を行った旨の虚偽の情報を記憶・蔵置させた上でZが前記架空名義口座に送金する手続を行った旨の不実の電磁的記録を作り、財産上不法の利益を得たというものである。

1

【判旨】

東京地裁は、「周到な計画に基づき、金融機関等のインターネット取引における本人認証手続を巧みにかいくぐり、さらに、自己の犯行を隠蔽し、警察の追及を免れるべく幾重もの防護措置を施した巧妙極まるものである。……加えて、本件犯行の基本的手口は模倣性が高

いものであることも無視できない。」として被告人を懲役4年に処した。その際に、法令の適用に当たって下記のような判断を示した。

①の不正アクセス、私電磁的記録不正作出、同供用と窃盗、詐欺との間には、それぞれ順次手段結果の関係があるので、刑法54条1項後段、10条により結局以上を1罪として刑および犯情の最も重い窃盗罪の刑で処断する。

②の不正アクセス、私電磁的記録不正作出、同供用との間には、順次手段結果の関係があるので、刑および犯情の最も重い不正作出私電磁的記録供用罪の刑で処断する。偽造有印私文書の一括行使は1個の行為が数個の罪名に触れる場合であり、有印私文書の各偽造とその各行使と詐欺との間にはそれぞれ順次手段結果の関係があるので、刑法54条1項前段、後段、10条により結局以上を1罪として最も重い詐欺罪の刑（ただし短期は、偽造私文書行使罪の刑のそれによる）で処断する。不正アクセス、私電磁的記録不正作出、同供用、窃盗との間には順次手段結果の関係があるので、刑法54条1項後段、10条により1罪として最も重い窃盗罪の刑で処断する。

③の不正アクセスと電子計算機使用詐欺との間には、それぞれ手段結果の関係があるので、刑法54条1項後段、10条により結局以上を1罪として刑および犯情の最も重い電子計算機使用詐欺罪の刑で処断するとする。

以上は、刑法45条前段の併合罪であるから、47条本文、10条により、最も重い詐欺罪の刑に法定の加重をする。

【評釈】

1 本件は、被告人が、いわゆるまんが喫茶等に設置されているインターネットに接続可能なパーソナル・コンピュータに、キーロガーというソフトウェアを仕掛けて入手した他人の識別符号等を利用して、クレジットカード会社のサーバ・コンピュータに不正アクセスし、会員が住所を変更した旨の虚偽の情報を記憶・蔵置させ、当該会員になりすましてインターネット通信販売により商品を注文、受領して窃取するなどした事案である。不正に入手した他人の金融機関の口座番号等の個人情報を利用し、周到な計画に基づき、金融機関等のインターネット取引における本人認証手続を巧みにかいくぐり、さらに、自己の犯行を隠蔽し、警察の追及を免れるべく幾重もの防護措置を施した悪質かつ巧妙極まるものとして世間の耳目を集めた⁽¹⁾ 事例である。

2 (1) 不正アクセスをめぐる問題が刑事立法の次元にまで発展した背景には、コンピュータと通信技術の急速な発展にともなうコンピュータ犯罪の複雑化と国際化という事情がある。社会のコンピュータ化が進み、コンピュータに対する人の意識も変わってきたことで、もはや個々人の内面的倫理観だけに頼る時代ではなくなってきた。とくに、1990年代後半のインターネットの爆発的広がりにより、コンピュータ・ネットワークが経済社会インフラとなるにしたがい、それに対する事故や犯罪への対処が重要な課題となっていた。

2 不正アクセス事件が注目を集めるにしたがい、不正アクセスの犯罪化を望む声も高まり、また、国際司法共助の点からも立法化すべきであると主張されるようになったため、1999（平成10）年に「不正アクセス行為等の禁止に関する法律」（以下、不正アクセス禁止法と略す）は成立し、2000（平成11）年2月13日に施行された。

(2) 不正アクセス禁止法は、電気通信回線に接続され、かつアクセス制御機能が設けられているコンピュータに対する侵入行為を不正アクセスと定義し（3条1項）、不正アクセス行為を行った者を処罰するとしている（8条）。法定刑は、1年以下の懲役または50万円以

下の罰金である。ただし、「電気通信回線に接続している電子計算機」の「当該電気通信回線を通じて行う」行為に限定されている。同法は、不正アクセス罪の類型として、①識別符号盗用型不正アクセス（3条2項1号）、②セキュリティ・ホール攻撃型不正アクセス（3条2項2号、3号）という二つのものをあげている。識別符号盗用型不正アクセスは、他人の有する識別符号（ID・パスワード）を無断入力することにより、アクセス制御機能により制限されている特定電子計算機の特定利用をしようする状態にさせることを禁止したものである。

（3）不正アクセス禁止法が保護しようとしているのは、「アクセス制御機能に対する社会的信頼」という社会的法益である。ハッキングは、クラッキングの前段階行為ともいえる行為であり、ソーシャル・エンジニアリング⁽²⁾によるパスワード窃取の例のように、識別符号盗用型不正アクセスの場合には、技術的手段だけでは防ぎ得ないこともあるため、処罰することについて一定の合理性が認められる。では、ハッキング行為自体に当罰性が認められるのであろうか。コンピュータおよびコンピュータ・ネットワークの社会経済的重要性が増大しつつある今日においては、システム自体に法的保護を与えることは必要であろうし、不正アクセス行為を住居侵入罪との対比で捉えることは可能であろう⁽³⁾。したがって、不正アクセス自体に当罰性は認められることになろう。住居侵入罪では物理的な侵害が要件となっているが、コンピュータの場合には、アクセス制御システムを突破することがこれに相当しよう。

（4）不正アクセス禁止法が初めて適用されたのは、他人の識別符号を使って無断でインターネット接続プロバイダのサービスを利用していたというケースに対してのものであった⁽⁴⁾。本件の場合も被告人は、X、Y、Zという他人の識別符号を無断で使用して、サーバ・コンピュータにアクセスしており、典型的な識別符号盗用型不正アクセスの事案であるといっていよい。2006年度上半期における不正アクセス罪の検挙件数は、264件と前年同期の約1.3倍に増加し、上半期だけで2005年1年間の検挙件数とほぼ同じ数に上っている⁽⁵⁾。そのすべてが識別符号盗用型不正アクセス事案であり、本件のように利用権者のパスワードの設定・管理の甘さにつけ込んだものが大半を占める。また、識別符号を知り得る立場にあった元従業員、知人等によるものが次いで多いが、いずれにせよ特に高度な技術を有していない者でも行えるものである。しかし、ソーシャルエンジニアリングを利用したり、フィッシングにより識別符号を入手する事案があがるなどコンピュータ技術を悪用したり利用権者を誤信させたりするものも発生している。

不正アクセス禁止法違反に係る被疑者についてみると、面識のない他人によるものが最も多く（29事件（243件））、次いで元交際相手や元従業員等の顔見知りの方によるもの（12事件（20件））、ネットワーク上のみの知り合いによるもの（2事件（2件））となっている。不正アクセス行為の後に利用されたサービスとしては、インターネット・オークションが最も多く（18事件（213件））、次いでオンラインゲーム（10事件（11件））、ホームページ公開サービス（5事件（5件））、インターネットバンキング（4事件（21件））の順となっている。不正アクセス行為の動機としては、本件同様、不正に金を得るため（21事件（230件））が最も多く、次いで元交際相手、元勤務先等に対する嫌がらせや仕返しのため（10事件（10件））、好奇心を満たすため（7事件（19件））、オンラインゲームで不正操作を行うため（3事件（3件））の順となっている。

3（1）本件においては、被告人が、電気通信回線を介して、A社が設置・管理するアクセス制御機能を有する特定電子計算機に、Xを利用権者として付された識別符号を入力して不正アクセスをし、Xが住所等を変更する手続を行った事実がないのに、変更等の手続を行った旨

の虚偽の情報を送信し、上記電子計算機の記憶装置に同情報を記憶・蔵置させ、事実証明に関する電磁的記録を不正に作出し、同社の事務処理の用に供している。このように、不正アクセス行為の後に別な犯罪がなされた場合に、その罪数処理をいかに解するかということが問題となる。本件において不正アクセス罪との関係で問題となったのは、大別すると①不正アクセスと私電磁的記録不正作出・同供用、②不正アクセスと私電磁的記録不正作出・同供用・詐欺、③不正アクセスと私電磁的記録不正作出・同供用・窃盗、④不正アクセスと電子計算機使用詐欺の4点である。この点につき、東京地裁はいずれの場合も牽連犯と判断した。

本判決の結論の如く不正アクセス行為によって特定電子計算機の特定利用をしようの状態になったことを利用して、当該電子計算機を操作し、様々なコンピュータ犯罪・ネットワーク犯罪が行われた場合に、その関係を単純に住居侵入罪と他罪との関係と同様に捉えて牽連犯とすることは、妥当なのであろうか。

(2) 数個の犯罪が行われ、それぞれについて犯罪が成立する場合において、一般的に一方が他方の手段となるような関係にある場合を牽連犯(刑法54条1項後段)という。牽連犯における牽連性には、主観的牽連性と客観的牽連性がありうるが、従来判例は、牽連犯について客観的牽連性のみが要件であるとする客観説に立ち、「犯罪の手段とは、或犯罪の性質上其手段として普通に用いられる行為をいうのであり、又犯罪の結果とは或犯罪より生ずる当然の結果を指すと解すべきものであるから、牽連犯たるには或犯罪と、手段若しくは結果たる犯罪との間に密接な因果関係のある場合でなければならない。従って犯人が現実に犯した二罪がたまたま手段結果の関係にあるだけでは牽連犯とはいいい得ない」⁽⁶⁾とし、通説もこの立場を支持している⁽⁷⁾。

牽連犯が科刑上一罪とされるのは、社会的事実の一体性が認められることにある。観念的競合と異なり、牽連犯の場合は一体性の程度は弱く、その程度はさまざまである。そのため、牽連犯の成立を認めるためには、社会通念上典型的に一体と評価できるような場合に限られる。その一体の程度の判断基準として、他人の住居の庭先に侵入して住居内を密かにのぞき見た場合における住居侵入罪と軽犯罪法1条23号の罪が牽連犯に当たるとした最判昭和57年3月16日⁽⁸⁾は、「数罪間に罪質上通例その一方が他方の手段又は結果となる関係があり、しかも具体的に犯人がかかる関係においてその数罪を実行した場合には、右罪数関係は牽連犯として」科刑上一罪として扱われると判示している。これは、客観的牽連性の判断に当たっては、単に抽象的な牽連性があるだけでは足りず、具体的牽連性があることを必要とする趣旨であると解される。

抽象的牽連性が認められる類型としては、構成要件自体が手段・目的または原因結果の関係を予定している場合や、罪質上、当該犯罪だけでは究極の犯罪目的が実現せず、それを手段として他の犯罪に発展することが予定されている場合などがある。

(3) 不正アクセス行為の後に電子計算機損壊等業務妨害罪(刑法234条の2)、電子計算機使用詐欺罪(刑法246条の2)等の犯罪が行なわれた場合に、不正アクセス罪とそれらの罪とは、牽連犯の関係にあるように見える⁽⁹⁾。

たとえば、電子メール・サーバに蓄積された他人の電子メールを知得するために、当該他人の識別符号を利用してサーバに不正アクセスを行ったとすれば、他人の住居の庭先に侵入して住居内を密かにのぞき見た場合と同様に考えることが可能であると思われるため、不正アクセス行為と電気通信事業者法における電気通信事業者の取扱中に係る通信の秘密を侵す行為の関係は、罪質上前者が後者の手段と考えられ、社会通念上典型的に一体と評価しうることから、両者の関係は、牽連犯と解しうるであろう。

しかし、コンピュータ・ネットワークを悪用し不正アクセス以外の犯罪をなすために不正アクセス行為をした場合に、不正アクセス罪と他罪の罪数関係が常に牽連犯となると考えることには疑問がある。

不正アクセス禁止法が、不正アクセス行為自体を処罰の対象としているのは、不正アクセス行為の横行によりアクセス制御機能に対する社会的信頼が失われた場合には、犯罪の抑止力一般が低下し、犯罪が行われやすい環境が生ずることとなるという点に着目したからである⁽¹⁰⁾。わが国の不正アクセス禁止法は、個々の不正アクセス行為が他の犯罪と結びつくおそれがあるかどうかを問題としておらず、具体的権利侵害ないしは侵害の危険から個々の利用権者の利益を保護しようとするものではないことに留意する必要がある。

不正アクセス禁止法は、「電気通信回線を通じて行われる電子計算機に係る犯罪の防止」を目的の一つとしている。しかし、不正アクセス行為を犯罪化しているのは、先述したとおり、「アクセス制御機能に対する社会的信頼」を確保するためである。不正アクセス行為をした者がすべてクラッキング行為を行うわけではないことから、アクセス制御機能に対する社会的信頼の侵害という、その行為自体の危険性を考慮したものである。それゆえ、不正アクセス行為の後に電子計算機損壊等業務妨害罪、電子計算機使用詐欺罪等の犯罪が行なわれた場合には、不正アクセス行為をそれらの犯罪に対する単なる手段であるとは評価できず、不正アクセス罪と他罪の評価は牽連犯とはならず、併合罪となると考えられる⁽¹¹⁾。

もっとも、一個の行為が不正アクセス罪と他罪を構成する場合があります。たとえば、ネット・バンキングにおいて送金を行う際に、送金を行うための識別符合と送金の指示内容が手元のパソコンから一つの操作で同時に銀行のサーバ（特定電子計算機）に入力され、当該他人の口座から他の口座に架空送金を行った場合には、他人の識別符合を盗用して入力するという行為は一個であるが、当該行為は、不正アクセス罪と電子計算機使用詐欺罪の構成要件に該当することになる。このような場合には、両罪の関係は観念的競合となろう。

したがって、本判決における不正アクセス禁止法に関する罪数判断は、法の解釈を誤ったものというべきである。

また、不正アクセス罪は、アクセス制御機能を単位として、これを付加したアクセス管理者ごとに判断されるべき⁽¹²⁾であって、不正アクセス1回ごとに1罪が成立するとすべきではないと考える。不正アクセス禁止法第3条2項各号に共通で「当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするもの」という除外理由がおかれていることから、各号の類型に法定刑上の差異が設けられていないことから、いずれの不正アクセス行為も法益を侵害する程度は同じであり、アクセス管理権を前提としていることは明らかであろう。

4 不正アクセス禁止法の解釈に際しては、罪数判断をめぐって統一が見られないように思われる。このような事態は、本件判決のように不正アクセス行為を住居侵入罪に擬制していることから起きているものと思われる。不正アクセス罪は、前述のとおりそれ自体当罰性が認められるのであるから、必ずしも罪質上、当該犯罪だけでは究極の犯罪目的が実現せず、それを手段として他の犯罪に発展することが予定されているとは言い切れない。牽連犯は、抽象的牽連性のみで成立するわけではない。したがって、不正アクセス罪と他罪との間で抽象的牽連性が認められる事例があるとしても、他罪の構成要件との関係でどれだけ具体的牽連性が認められるかにより牽連犯を構成すべきであろう。不正アクセス行為がネットワーク上の不正「侵入」行為を処罰するものであるが、住居侵入罪と不正アクセス罪では、立法趣

旨や保護法益が異なることを念頭に置くべきである。解釈に際しての混乱を避けるためにも、今後の判例の蓄積、法の運用実態の分析が求められよう。

※ 文献挙示の方法は、法律編集者懇話会「法律文献等の出典表示方法」の方式に準じている。

- (1) キーロガーで口座情報を不正入手、金を詐取した男逮捕〈<http://www.itmedia.co.jp/news/articles/0411/04/news098.html>〉。(2006年12月22日確認)
- (2) 「人をだまして、狙ったシステムのセキュリティを危険にさらすパスワードその他の情報を暴露させること」(福崎俊博訳『ハッカーズ大辞典(改訂新版)』アスキー(2002年)520頁)。1980年代にハッカーたちは、技術的でない手段によって情報を得るための戦略を説明するためにこの言葉を使い始めたという(Ira Winkler, Corporate Espionage p.94(1997)(稲垣伸子訳『現代産業スパイ事情』日経BP社(1998年)127頁)。
- (3) 園田寿「不正アクセス」法学教室228号(1999年)45頁、園田寿・牧野二郎・露木康浩・前田雅英「《座談会》ハイテク犯罪の現在」現代刑事法8号(1999年)18頁、「検証不正アクセス対策法」ハッカージャパン4号(1999年)148頁。
- (4) 千葉地判平成12年7月12日判例集未登載。岡村久道・近藤剛史『インターネットの法律実務[新版]』新日本法規(2001年)396頁参照。
- (5) 「平成18年上半年の不正アクセス行為の発生状況等について」〈<http://www.npa.go.jp/cyber/statics/h18/pdf32.pdf>〉。(2006年12月22日確認)
- (6) 最判昭和24年7月12日刑集3巻8号1237頁。
- (7) 植松正『刑法概論I総論[再訂版]』勁草書房(1974年)436頁、団藤重光『刑法綱要総論[第3版]』創文社(1990年)362頁、佐久間修『刑法講義総論』成分堂(1997年)、堀内捷三『刑法総論[第2版]』有斐閣(2004年)318頁、大塚仁『刑法概説総論[第3版増補版]』有斐閣(2005年)483頁、前田雅英『刑法総論講義[第4版]』東京大学出版会(2006年)506頁等。
- (8) 刑集36巻3号260頁。
 評釈としては、龍岡資晃「住居侵入罪と軽犯罪法1条23号の罪との罪数関係」ジュリスト769号(1982年)102頁以下、香川達夫「住居侵入罪と軽犯罪法1条23号の罪との罪数関係」判例評論284号(判例時報1049号)(1982年)226頁以下、伴義聖「住居侵入罪と軽犯罪法1条23号の罪とは牽連犯の関係にあるとされた事例」研修412号(1982年)47頁以下、宇津呂英雄「住居侵入罪と軽犯罪法1条23号の罪とは牽連犯か」警察学論集36巻11号(1983年)148頁以下、龍岡資晃「住居侵入罪と軽犯罪法1条23号の罪との罪数関係」法曹時報37巻9号(1985年)314頁以下、山室恵「住居侵入罪と軽犯罪法1条23号の罪との罪数関係」警察研究58巻11号(1987年)37頁以下等がある。
- (9) 前田雅英編集代表『条解刑法』弘文堂(2002年)643頁は、不正アクセス行為を手段として電子計算機損壊等業務妨害罪が犯された場合、両罪は牽連犯となると指摘している。
- (10) 不正アクセス対策法制研究会編著『逐条 不正アクセス行為の禁止等に関する法律[補訂]』立花書房(2001年)25頁。
- (11) 前掲・逐条150頁。
- (12) 前掲・逐条147頁、岡村・前掲注(4)342頁。

(受理 平成19年1月15日)