# サイバー犯罪の研究（四）-電子計算機詐欺に関する比較法的検討-

法律論叢　第八六巻　第一号（二〇一三・七）

【論　説】

# サイバー犯罪の研究（四）

## ――電子計算機詐欺に関する比較法的検討――

夏井高人

目　次

## 一　はじめに

日本国の刑法二四六条の二（電子計算機使用詐欺罪）は、刑法第三七章（詐欺及び恐喝の罪）の中にある刑法二四六条（詐欺罪）の特別罪として規定されている。

言うまでもなく、詐欺罪は、被害者を欺罔して錯誤に陥らせ、その錯誤に起因する瑕疵ある意思に基づいて財物の交付や財産上の利益の提供などを行わせることによって財物の占有や財産的利益を得るという行為類型に属する罪であって、定型的に、被害者自身を加害者の実行行為の道具とする間接正犯型犯罪の典型例の一つとして理解することができる。

ところが、電子計算機詐欺罪は、その構成要件要素として「被害者の欺罔」を一切含まない（被害者の欺罔が含まれる場合には、通常の詐欺罪が成立し得るということになる。）。それゆえ、電子計算機詐欺罪は、詐欺という犯罪類型とはかなり異なる類型に属する犯罪である。(1)

にもかかわらず、法律上の位置づけとしては詐欺罪の一種として法定されていることから、理論上の混乱が発生する。結論から言えば、これは、単なる立法の誤りに過ぎない。立法担当者（当時）が事態の本質を正確に理解していな

かったか、または政治的要因等により妥協したことがその最大の原因であると推定される。

本稿では、法理論上何も問題がないと一般に考えられている電子計算機詐欺罪について、法理論上の正しい位置づけを試みるとともに、これまで多数蓄積されてきた電子計算機使用詐欺罪と関連する裁判例中の主要なものを概観し、併せて関連する海外の法令を紹介し、若干の検討結果を提供することを目的とする。

## 二　立法の経過

刑法二四六条の二（電子計算機使用詐欺罪）は、昭和六二年（一九八七年）の刑法一部改正により、刑法二四六条（詐欺罪）の特別罪として、昭和六二年法律第五二号に基づき追加して新設された。(2)

窃盗罪ではなく詐欺罪の特殊類型の一つとして刑法二四六条の二が設けられた理論的根拠に関する立法者の見解は、「本罪は、詐欺罪の類型として構成されている。これは、本罪が、電子計算機がいわば人に代わって事務処理を行っている場面において、これに虚偽の情報若しくは不正の指令を与えて不実の電磁的記録を作出し、又は虚偽の電磁的記録を人の事務処理の用に供することにより、財産上不法の利益を得る行為をとらえようとするものであり、人を欺罔して財産上不法の利益を得る詐欺罪に近いものと考えられたからである」というものである。(3)

ところで、刑法二三五条（窃盗罪）は、財物の窃取行為（占有の奪取）のみを構成要件行為としているところ、財産的利益を奪取する行為を窃盗の一種として観念することは可能である。そして、もしそのような見解を採用するとすれば、現行の刑法二三四条の二の罪を刑法二三五条二項の罪（電子計算機利益窃盗罪）として構成することも理論的には可能であったと思われるが、立法者は「利益窃盗」一般を処罰することに対する批判的対応を避ける目的で、そ

のような理論的可能性をあえて回避し、国会において紛議が生ずる可能性を消滅させた疑いがある。[4] 現時点のように「物品」ではなく「役務」を中心とする情報財取引が普通になっている時代においては「利益窃盗罪」の新設それ自体について何ら異議が生ずる可能性はなく、ただその処罰範囲をどのように限定するかについてのみ争点となりそうであるが、現実にはそうではなかった。当時の時代状況からすれば、ある種の限界（時代的制約または政治的・政策的配慮をせざるを得ないような社会状況）のようなものが存在していたと理解するしかないと考えられる。

他方、昭和六二年刑法一部改正当時、英米の立法動向としても「コンピュータ詐欺罪（Computer Fraud）」が存在しており、ここで「詐欺罪（Fraud）」という用語が用いられていたし、現在でも用いられていることも原因の一つになっている可能性がある。[5] しかしながら、英米法における「Fraud」の概念は日本国法における「詐欺」の概念に限定しない用例があることに留意すべきであった。しかし、昭和六二年の刑法一部改正前には、日本国において、コンピュータ犯罪や情報犯罪あるいはこれに類する犯罪類型を専攻する研究者がほぼ皆無に近い状態であったことから、歴史的な事実として、残念ながら、英米の関連立法や判例法等について必要かつ十分な検討・吟味がなされたとは認め難い。その結果として、現行の刑法二四六条の二は、あくまでも詐欺罪の特別罪として解釈されることになった。

## 三　電子計算機使用詐欺罪の理論的位置づけ

既述のとおり、刑法二四六条の二（電子計算機使用詐欺罪）は同法二四六条（詐欺罪）の特殊類型として刑法典中に明確に位置づけられている。

しかし、例えば全ての立法過誤の場合にそうであるように、形式的な法条の位置づけや形式とは無関係に、その本

質から当該条項の法的性質や法的属性等を検討し、正しい論理関係を前提として合理的に法解釈をすべきことは当然のことなので、以下、その前提で検討を進める。(6)

## 1 欺罔行為

一般に、「詐欺」の概念は、読んで字の如く、人（他人）を騙す行為（欺罔行為）を必須の本質的要素としている。騙す対象が人でない場合、欺罔により錯誤に陥る可能性があり得ないので、一般社会概念としての詐欺に含まれることはない。

電子計算機使用詐欺罪では、欺罔されるべき人が（構成要件要素としては）存在せず、間接正犯の道具として加害者によって操作される道具としての人も存在しない。同罪では、加害者は、無権限で電子計算機を直接に操作しているだけであり、その無権限操作の結果として直接的に財産上不法の利益を得ることになる。要するに、同罪の実行行為中には欺罔行為に基づく被害者の錯誤、その錯誤に基づく被害者の処分行為なるものが一切現れない。つまり、電子計算機使用詐欺罪においては、「詐欺罪」という名称が付されておりながら、一般に詐欺罪の本質的部分であると理解されている構成要件要素が全く存在しないという点に顕著な特徴がある。

また、電子計算機は、欺罔されることも錯誤に陥ることもない。もし電子計算機内での計算処理において人の錯誤に類する状態に陥ると、その電子計算機が暴走し正常に処理をすることができなくなってしまう結果、電子計算機使用詐欺罪は、常に不能犯であるか未遂に終わることになると言わざるを得ない。(7)

本質的に、電子計算機は、電子計算機使用詐欺罪が成立するような場合であっても、入力された指令やデータ等を

そのまま正しいものとして処理するのであり、そこには被害者に対する欺罔行為も被害者の錯誤もない。その場合において電子計算機に入力された指令やデータは、単に「権限のない」入力であったというだけのことに過ぎない。(8)

以上のことから二つの理論的帰結が導き出され得る。

一方は、電子計算機使用詐欺罪は、電子計算機という装置の無権限使用の一種であるということである。

他方は、例えばパブリッククラウドのようなネットワーク型仮想電子計算機システム等ではとりわけ、装置の無権限使用というよりは情報の無権限使用の一種として純化して考えるべき余地があるということである。

そして、今後の電子技術の進化を想定すると、更に派生的な課題が存在していることに気づくことができる。(9)

以下、分けて論ずる。

## 2　窃盗罪の特別類型としての法解釈

電子計算機使用詐欺罪は、本来であれば刑法二三五条二項または同法二三五条の二として立法されるべき法的性格を有するものであった。

このことは、パチンコ球遊機を例にとって考えてみると明らかである。例えば、パチンコ球遊機に対し永久磁石等を用いてパチンコ玉を誘導し、パチンコ玉（財物）の出玉を多くするようにしてこれを取得した場合、窃盗罪（刑法二三五条）が成立することについて異論はないものと思われる。(10)この場合、被害者に対する欺罔行為が存在し得ず、機械装置を無権限で操作して財物の占有を取得する行為になるからである。そして、全く同様の行為を実行し、パチンコ玉ではなく景品交換可能な電磁的記録（景品交換ポイントなど）を得たという事案を想定してみると、その場合に

は、財物の占有を取得する行為は存在しないが、財産上の利益を得る行為は存在し、電子計算機使用詐欺罪が成立し得る。[11] つまり、この二つの種類の犯罪は、結果として財物の奪取が成立するか利得が成立するかの相違しか存在せず、いずれも欺罔行為を要素としない無権限による機械装置の操作であるという点で全く同じ犯罪類型に属するということを理解することができるのである。

この関係を模式的に示すと表1のようになる。[12]

表1　犯罪としての位置づけ

| | 財物の奪取 | 利得 |
|---|---|---|
| 欺罔行為あり | 刑法二四六条一項 | 刑法二四六条二項 |
| 欺罔行為なし | 刑法二三五条 | 刑法二四六条の二 |

現行法は、詐欺罪の特別類型という位置づけになっているが、これは、立法上の過誤の一種として理解すべきであり、立法上の体裁・形式にとらわれず、犯罪としての本質に基づく法理論上の位置づけを与えるべきである。

### 3　機器の無権限使用としての構成

既述のとおり、例えば、パチンコ球遊機の事例を想定してみれば理解可能なとおり、何らかの財物を出力する自動機械を不正に操作して財物を取得する行為は、犯罪としては窃盗罪であるが、犯罪論的には自動機械の無権限使用と

いう類型に属する行為であることになる。同様に、電子装置によって作動する自動機械を不正に操作して利得を得る行為は、犯罪としては電子計算機使用詐欺罪を構成し得るが、犯罪論的には同じく自動機械の無権限使用という類型に属する行為である。

そのことから、これらの行為は、「電子装置を組み込んだ機械装置の無権限使用」という行為類型としてひとくくりにして理解することが可能となる。

現行の刑法は、このような犯罪類型が社会に登場するよりもはるかに以前に構築された犯罪論のカテゴリーに基づいて構築されていることから、現代社会における実際と刑法上の犯罪類型の構成との間に齟齬が存在していると理解することも可能である。

今後の立法論としては、既に別稿[13]において提唱してきたとおり、「権限」という概念を中心に犯罪類型の組み換え作業がなされるべきである[14]。

## 4　無権限情報操作行為としての構成

既述の「機器の無権限使用」という考え方を更に進め、電子計算装置が組み込まれた機器類に対して無権限使用という行為が実行されたという事案を想定した場合、外形的な社会的事実としては、明らかに機器という物体の無権限使用であることになる。

しかしながら、その本質である構成要件要素を考察してみると、要するに、機器の動作を支配している電子計算機を無権限で支配する行為であるということに尽きるのであり、それは、無権限情報操作行為として認識・理解するこ

とができる。

一般に「ハッキング（クラッキング）不可能なコンピュータシステムは存在しない」と言われるとおり、およそ電子装置には必ず何らかの脆弱性要素が存在するから、当該行為の日本国法における不正アクセス罪の成否については一応措くとして、「無権限で操作される可能性（無権限で支配される可能性）を完全に排除することのできる電子装置は存在しない」という言い方をしても決して誇張とはならない。それゆえ、無線通信可能なＰＣやデジタルカメラのような比較的小さな機器類だけではなく、旅客機や自動車のような大きな物体であっても、あるいは、交通管制システムなどのような大掛かりな施設・機器類であっても、その支配を奪い、遠隔で操作することが（少なくとも机上の理論としては）可能である。

このような発想は、いまだ萌芽的なものであるかもしれない。しかし、電子装置が社会のありとあらゆる部面で普及・応用されている現代社会の状況を踏まえると、これまでとは異なる抽象モデルとして、「無権限情報操作行為」を観念することには意味があると考える。

そして、そのような新たなモデルを前提とすると、電子計算機を組み込んだ機械装置を無権限で使用する行為は、無権限情報操作行為としても観念可能であることになるから、そのような機械に対して実行される窃盗行為や電子計算機使用詐欺行為は、いずれも無権限情報操作行為の一種であると理解することが可能となるのである。

## 5　近未来の課題

ＳＦ（空想科学小説）ではなく現実の問題として、人工知能の仕組みを組み込み比較的高度な判断作業を実行可能

なロボット等の自動機械が開発され続けており、その中の幾つかは既に社会の中に入り込んでいる。掃除用のロボットのように誰から見てもロボットの一種であると認識可能なものだけではなく、例えば、自動車の自動操縦装置や各種制御装置のように自動車という機械装置の内部に組み込まれており、外見上では電子計算機の一種のように見えないものも含めると、通常予想されている以上にこの種の高度なロボットが社会内に普及し続けているという現実を認識・理解することができよう。

そして、おそらく比較的近未来の社会においては、人間の生体脳の機能を代替可能な電子装置または有機計算組織（バイオコンピュータの一種）が開発され、脳の代わりに人間の頭蓋骨の中に埋め込まれ、人間の思考作用と似たような思考作業を実行するけれども、本質的には完全なロボットであるかサイボーグであるような特殊な存在が社会の中で機能し始めることになるだろうと予測することができる。論理的な組み合わせとしては、生体脳と電子計算機の両方を協調させて機能させるような共存型の状況を考えることも可能であり、そのようなアンドロイドまたはサイボーグ的な存在は比較的現実味のあるものと言うことができると思われる。現時点で、既に感覚器という生体組織の多くが電子的な機械装置と置き換え可能な状態となっている（換言すると、臓器と機械装置との境界が既に消失してしまっている。）。

さて、このような高度に電子機器が発達し、人間の生体内に組み込まれて利用されるような状況が更に進み、もし人間の生態脳の部分を完全に電子計算機に置き換えたような存在が成立したと仮定すると、そのような存在に対しては、電子計算機に対する欺罔行為や電子計算機の錯誤はあり得ないことなので、詐欺罪が成立することはない。仮に外見上では完全な人間に対する詐欺行為が実行されているように見える場合であっても、それが人間ではなくロボット（電子装置を組み込んだ機械装置の一種）である限り、人間に対する欺罔行為と欺罔された人間の錯誤を必須の構

成要件要素とする詐欺罪ではなく、純然たる機械装置に対して実行される窃盗罪または電子計算機使用詐欺罪だけが成立可能という事態が生ずることになる。(15)

ロボットの高度化は普通の人々が通常予測しているよりもはるかに速く現実に進行しているので、このような事態の発生は、机上の空論ではなく、現実味のある想定の一部となりつつあるということができる。

しかしながら、刑法だけではなく、法哲学一般において、自由な意思をもつとされる人間以外の存在が行為の主体または客体となるような状態を前提とした研究は未だほとんどなされていないように思われる。それゆえ、そのような事態に適用可能な刑法理論もまた不在の状態が続いている。

## 四　電子計算機使用詐欺罪と関連する裁判例

電子計算機使用詐欺行為が現実にどれくらい存在するかについては必ずしも明らかではない。認知された事件数については警察庁によって毎年統計結果が公表されている。(16)しかしながら、暗数を含めると、通常推測されている以上の数の電子計算機使用詐欺事犯が存在する可能性がある。

そして、電子計算機使用詐欺罪により有罪とされた事件の判決のうち、公刊されているものはかなり少ない。

本論文では、電子計算機使用詐欺罪により有罪とされた判決中の主要なものについて概観し、その中の何件かについて若干の考察を加えることとする。

## 1　金融機関のオンラインシステムの事例

### 東京地裁八王子支部平成二年四月二三日判決・判例時報一三五一号一五八頁(17)

（事案）

青梅信用金庫において内国為替業務等の事務処理を担当していた被告人Xが、被告人Yと共謀の上で、被告人Xにおいて、昭和六二年一二月一四日から昭和六三年一一月一〇日までの間前後五回にわたり、いずれも青梅信用金庫事務集中部において、同金庫オンラインシステムの端末機を操作して、同金庫本部電算部に設置され同金庫の預金残高管理、受入れ、払戻し、為替電文の発・受信等の事務処理に使用されている電子計算機に対し、実際には振込依頼を受けた事実がないのにもかかわらず、「被告人Yが株式会社三菱銀行六本木支店ほか一行に設けていた普通預金口座に振込があった」旨の虚偽内容の情報を与え、全国銀行データ通信センター東京センターに設置されている電子計算機等に接続されている記憶装置の磁気ディスクに記憶された普通預金口座の預金残高の金額について、財産権の得喪・変更に係る不実の電磁的記録を作り、よって、財産上不法の利益を得たというものである。

（争点）

外形的事実については、電子計算機使用詐欺罪の実行行為があったと認めるほかはないと思われるが、本件では、青梅信用金庫の従業員ではない被告人Yについて、電子計算機使用詐欺罪の故意の成立が争点となった。被告人Yの弁護人の主張は、「同被告人には信用金庫の電子計算機処理システムに関する初歩的知識もなく、本件各犯行の謀議をな

し得るに必要な基本的知識を欠いていたとして、同被告人に本件各犯行の共同正犯が成立することにつき疑問を提起している。そして、被告人Xの弁護人は、被告人らの本件各犯行は、単一の意思の下に反覆継続してなされた同種の犯行であって、全体が包括的一罪を構成するものであり、平成元年三月三日以降になされた本件各追起訴は、いずれも本起訴と二重起訴の関係となり、その公訴を棄却すべきであり、また、被告人Xは、被告人Yから暴行脅迫を受けてやむなく本件各犯行を実行するに至ったものであり、被告人Xには適法行為の期待可能性が存在しないから、同被告人は無罪である」と主張した。

（裁判所の判断）

裁判所は、「被告人Yの共同正犯の成否については、関係各証拠によれば、同被告人は、振込先の預金口座を自ら開設しており、オンラインシステムの具体的操作方法や仕組みについての正確な知識まではなかったにせよ、被告人Xが信用金庫のオンラインシステムの不正操作をして本件各振込をするという認識は有していたことが認められ、本件の背任罪はもとより電子計算機使用詐欺罪についても、その構成要件的事実の認識としては十分であって、被告人Yには本件各犯行の共同正犯として欠けるところはないというべきである」と判示した。

（若干の検討）

共謀関係の成立に必要な故意の具体的内容と実行犯について電子計算機使用詐欺罪が成立するために求められる故意の具体的内容とがその精粗において異なることがあり得ることになる。弁護人の主張は、まさにその点を突いたものと言うことができる。

一般に、共謀関係が成立するためには、実行犯の行為の詳細についてまで認識・認容することが求められておらず、概括的にせよ実行行為の概要とその結果について認識・認容があれば足りると解されていることから、その故意の内

容において精粗の差が出てしまうことは必然であり避けることができないのではないかと思われる。仮に実行犯と同程度に詳細・具体的な内容についての認識・認容が求められるとすれば、およそ共犯者間に共謀関係が認められる余地がほとんどなくなってしまうであろうと考える。

## 名古屋地裁平成九年一月一〇日判決・判例時報一六二七号一五八頁

（事案）

被告人両名は、C及びDと共謀の上、株式会社東海銀行が行っている東海パソコンサービス（アンサー利用型）の都度指定方式による振込サービスを利用して、財産上不法の利益を得ようと企て、

第一　平成六年一二月九日午後五時三二分ごろ、千葉市花見川区所在の事務所において、電話回線に接続したパーソナルコンピューターを操作し、NTTデータ通信の提供する銀行アンサーシステムを介して、愛知県西春日井郡所在の東海銀行師勝ビルに設置されて同行の預金、為替等の業務のオンライン事務処理に使用されている電子計算機に対し、実際には振込送金の事実がないのに、一億四〇〇〇万円の払込送金があったとする虚偽の情報を与え、同月一二日午前九時ごろ、全国信用金庫データ通信システムの電子計算機等を介して、東京都港区所在のNTT品川ツインズビルデータ棟の信金東京共同事務センター事業組合に設置されている信用金庫第三次オンラインシステムの電子計算機に接続されている記憶装置の磁気ディスクに記録された普通預金口座の預金残高を一億四〇〇〇万円増加させて、財産権の得喪、変更にかかる不実の電磁的記録を作り、よって、一億四〇〇〇万円相当の財産上不法の利益を得た。

第二　平成六年一二月一二日、横浜市港北区所在のホテル客室において、いずれも同所に設置して電話回線に接続

したパーソナルコンピューターを操作し、株式会社東海銀行アンサーシステムを介して、株式会社東海銀行の預金、為替等の業務のオンライン事務処理に使用されている電子計算機に対し、実際には振込送金の事実がないのに、①同日午後五時一九分ごろ、普通預金口座に四億円の振込送金があったとする虚偽の情報を、②同日午後五時三四分ごろ、普通預金口座に九〇〇〇万円の振込送金があったとする虚偽の情報を、③同日午後五時四五分ごろ、普通預金口座に一〇億円の振替送金があったとする虚偽の情報を、それぞれ与え、翌同月一三日午前九時ごろ、株式会社第一勧業銀行東京事務センターに設置されている中継電子計算機等を介して、基礎勘定系システムバックエンド系電子計算機に接続された記憶装置の磁気ディスクに記録されているE名義の普通預金口座の預金残高を一四億九〇〇〇万円増加させて、財産権の得喪、変更にかかる不実の電磁的記録を作り、よって、Eに一四億九〇〇〇万円相当の財産上不法の利益を得させた。

## 2　電話通話料金の課金システムの回避の事例

**東京地裁平成七年二月一三日判決・判例時報一五二九号一五八頁**

（事案）

被告人は、「ブルーボックス」と称するコンピュータソフトを使用して作出した不正信号を用い、ＫＤＤ、ＩＯＤＣ対地国及び着信国のいずれの電気通信事業者の電話料金課金システムでも自らが課金を行うべき通話と認識しないようにすることができることを奇貨として、その通話料金の支払を免れようと企て、平成五年一一月二九日から平成六

年三月四日までの間、前後四四回にわたり、東京都大田区所在の自己の使用する電話回線から、ＫＤＤの電話交換システムに対し、真実はＩＯＤＣサービスを利用する意思がないのに、ＩＯＤＣサービスを使用する旨の番号を送出して、不正の指令を与え、ＫＤＤの電話交換システムをして、ＩＯＤＣサービス利用の申込みがなされたものと認識させて、自己の電話回線とＩＯＤＣ対地国の電話交換システムとを接続させ、更に、自己の電話回線から、「ブルーボックス」を使用して作出した不正信号を、ＩＯＤＣ対地国の電話交換システムに送り出すなどして、ＫＤＤの電話交換システムをして、ＩＯＤＣサービス利用による回線使用が継続しているものと誤認させてＩＯＤＣ対地国を中継国として着信国の着信人との間で国際通話を行い、そのころ、ＫＤＤの電話料金課金システムに対して、その国際通話がＩＯＤＣサービス利用の通話である旨の虚偽の通話情報を伝送させ、これに基づき電話料金課金システムにその旨の不実のファイルを作出させてその国際通話の通話料金相当額の支払を免れ、そのような行為によって、その国際通話に相当する合計三七万三八〇六円の財産上不法の利益を得た。

（若干の考察）

「ブルーボックス」は、電話通話料金等の課金を免れるために用いられるソフトウェアであるが、同種の課金回避用のソフトウェアはかなり多数の種類のものが存在しているのではないかと推定される。

課金を回避したという結果だけに着目する限り、電子計算機使用詐欺罪の成否が主として問題となるが、「ブルーボックス」などの課金回避用ソフトウェアの製造や利用行為などが不正指令電磁的記録（刑法一六八条の二）に該当するか否かが今後は問題とされ得ると考えられる。

## 3　いわゆるキセル乗車の事例

### 東京地方裁判所平成二四年六月二五日判決・判例タイムズ一三八四号三六三頁

（事案）

被告人は、平成二二年五月二七日、東日本旅客鉄道株式会社鶯谷駅から一三〇円区間有効の片道乗車券を使用して、東京都台東区所在の鶯谷駅に入場し、同駅で山手線外回り普通列車に乗車し、同区所在の上野駅で東北本線宇都宮行き快速列車に乗り換え、栃木県宇都宮市所在の宇都宮駅に到着した際、同日午前八時二一分頃、同駅改札口に設置してある旅客の乗車事実等により出場の可否を決する事務処理に使用する電子計算機である自動改札機に対し、自己がその乗車について岡本駅で入場したと処理される虚偽の電磁的記録である雀宮駅から岡本駅までを有効区間とする普通回数乗車券を投入し、同自動改札機を開扉させることにより同改札口を通過して出場し、よって、鶯谷駅から宇都宮駅までの旅客運賃との差額一五三〇円相当の財産上不法の利益を得た。(18)

（争点）

弁護人は、「電子計算機使用詐欺罪の構成要件にいう「虚偽」とは、電磁的記録それ自体が不正に作出されたり、改変された場合に限られるべきであって、乗車券や回数券に不正な作出、改変はなく、また、本件は、電子計算機の事務処理システムの欠陥・瑕疵に由来するものであり、このような欠陥・瑕疵について被告人らを処罰することにより補完するのは許されない」と主張した。

（裁判所の判断）

裁判所は、電子計算機使用詐欺罪における構成要件中の「虚偽」の意義について、「不正な作出、改変に限る必要性は認められない」と判示した上で、「むしろ、電磁的記録は、記録それ自体の情報に加え、これを用いるシステムが前提とする一定の意味付け等を踏まえて事務処理の用に供されているものであり、このような前提となる事柄の真実性も当該事務処理システムの円滑かつ適正な運用のために必要なものといえる。本件は、ＪＲ東日本を利用するほとんどの旅客が乗車券等の券面及び電磁的記録に従った乗車を遵守しており、ＪＲ東日本も旅客のこのような乗車を信頼し、また、これを基礎にして自動改札機及び自動精算機の事務処理システムを構築している中にあって、被告人らがその信頼を逆手に取り、これを悪用した行為と評価すべきものである。弁護人が述べるように、自動改札機や自動精算機の事務処理システムの欠陥・瑕疵に由来するものとは到底いえない。仮に、このようなシステムの前提となる事柄についても、それが電磁的記録化される必要があり、かつ、その不正な作出、改変がない限りは本罪が成立しないとすれば、それは、迅速かつ効率的な事務処理のために電子計算機による事務処理システムを導入する企業等にとって、当該システムの構築及びその維持に多大な負担を生じさせ得るものであることは明らかであり、妥当性を欠いた見解というべきである。したがって、このような前提を偽ることも当該電磁的記録自体の誤りと実質的に同等に評価することが妥当であり、自動改札機及び自動精算機の事務処理システムにおける事務処理の目的に照らし」、電子計算機使用詐欺罪の構成要件中の「虚偽」に当たるというべきであるとの判断を示した。

## 4　オンラインサイト用電子マネーの事例

### 最高裁平成一八年二月一四日決定・刑集六〇巻二号一六五頁

（裁判所の判断）

原判決及びその是認する第一審判決の認定によれば、被告人は、窃取したクレジットカードの番号等を冒用し、いわゆる出会い系サイトの携帯電話によるメール情報受送信サービスを利用する際の決済手段として使用されるいわゆる電子マネーを不正に取得しようと企て、五回にわたり、携帯電話機を使用して、インターネットを介し、クレジットカード決済代行業者が電子マネー販売等の事務処理に使用する電子計算機に、本件クレジットカードの名義人氏名、番号及び有効期限を入力送信して同カードで代金を支払う方法による電子マネーの購入を申し込み、上記電子計算機に接続されているハードディスクに、名義人が同カードにより販売価格合計一一万三〇〇〇円相当の電子マネーを購入したとする電磁的記録を作り、同額相当の電子マネーの利用権を取得したものである。

以上の事実関係の下では、被告人は、本件クレジットカードの名義人による電子マネーの購入の申込みがないにもかかわらず、本件電子計算機に同カードに係る番号等を入力送信して名義人本人が電子マネーの購入を申し込んだとする虚偽の情報を与え、名義人本人がこれを購入したとする財産権の得喪に係る不実の電磁的記録を作り、電子マネーの利用権を取得して財産上不法の利益を得たものというべきであるから、被告人につき、電子計算機使用詐欺罪の成立を認めた原判断は正当である。

## 五　海外の主要法令

日本国刑法に規定する電子計算機使用詐欺罪に相当する犯罪及び刑罰を定める法令は、かなり多数ある。

とりわけ、サイバー犯罪条約の締約国は、サイバー犯罪条約八条に規定する「コンピュータに関連する詐欺締約国は、自己又は他人のために権限なしに経済的利益を得るという詐欺的な又は不正な意図をもって、権限なしに故意に」、「コンピュータデータの入力、改ざん、削除又は隠ぺい」または「コンピュータシステムの機能に対する妨害」に該当する行為が実行され、「他人に対し財産上の損害が加えられることを自国の国内法上の犯罪とするため、必要な立法その他の措置を」とるべき義務を負っている。(19) そのことから、同条約の締約国は、財産権侵害の結果となるような電子計算機の無権限使用を禁止し処罰する法令を制定すべき国際法上の義務を負っていることになる。日本国の場合、同条約八条の要件を満たす刑罰法令として刑法二四六条の二（電子計算機使用詐欺罪）の規定が存在していることになる。

このサイバー犯罪条約八条の規定について留意すべき点は、詐欺罪の一種として刑罰法令を定めるべきことを命じていないということである。詐欺的な財産権の違法取得を実行するために無権限で電子計算機にアクセスし使用することを禁止すべきとしているだけであり、各締約国における実際の立法は、窃盗罪の特殊類型とすることもできるし詐欺罪の特殊類型とすることもできる。日本国では後者を選択したことになるが、そのような選択に理論上の問題があることは既に述べたとおりである。

海外の関連法令の中で、サイバー犯罪条約八条の起草にも影響を与えたのではないかと推定されるのは合衆国連邦刑法一〇三〇条である。この一〇三〇条の条項は、これまでも邦訳が存在するが、ブッシュ政権当時に改正され、更

に二〇一二年に最終改正された現行の条項については完全な邦訳が存在しないようであり、少なくとも一般に利用可能な形では公刊されていない。

そこで、完璧な邦訳となっている保証はないが、訳出を試みる。

## 合衆国連邦法律集一八款一〇三〇条　コンピュータと関係する詐欺及び関連行為

(a)　以下の者は、本条(c)に規定するところに従い処罰される。

(1)　認識して、無権限でもしくは権限を超過してコンピュータにアクセスする者、及び大統領執行命令もしくは制定法に基づき、国防もしくは外交上の理由により合衆国連邦政府が無権限の開示から保護すべきものと定めた情報または一九五四年原子力法一一条y項に規定する禁止データを、そのような行為[20]によって取得する情報が合衆国に対する侵害行為のために用いられ得ると信ずべき根拠を有しながら、そのような行為によって取得する者、または、外国を利するために、意欲して、そのような情報を、受領する権限のない者に対し、送信、配布もしくは伝送する者、または、送信、配布もしくは伝送されるようにする者、または、送信、配布もしくは伝送を試みる者、または、送信、配布もしくは伝送されるようにすることを試みる者、または、意欲して、そのような情報を保存する者、及びそのような情報を受領する権限を有する合衆国の官吏もしくは従業者に対するそのような情報の配布を妨げる者：

(2)　意図的に、無権限でもしくは権限を超過してコンピュータにアクセスし、それによって以下のいずれかの情報を取得する者：

(A)　金融機関の信用情報記録に含まれる情報、合衆国法律集一五款一六〇二条(n)に規定するカード発行者の情報

または公正信用報告法（合衆国法律集一五款一六八一条）に規定するような消費者に関する情報であって消費者情報の報告をする官署のファイルに含まれている情報[21]：

(B)　合衆国の部局からの情報[22]：または

(C)　保護されたコンピュータからの情報[23]：

(3)　意図的に、合衆国の部局の非公開コンピュータにアクセスする権限なく、専ら合衆国連邦政府が利用するために設置されている部局のコンピュータ、専ら合衆国連邦政府によって利用されているもしくは合衆国連邦政府が利用するために設置されているのではないコンピュータの場合には、合衆国連邦政府によって利用されているもしくは合衆国連邦政府が利用するために設置されており、そのような行為[24]が合衆国連邦政府による利用もしくは合衆国政府のための利用に悪影響を生じさせる場合には、そのコンピュータにアクセスする者[25]：

(4)　認識して、かつ、詐欺の目的で、無権限でもしくは権限を超過して保護されたコンピュータにアクセスし、かつ、そのような行為によって、意図的な詐欺を更に実行し、何らかの利益を取得する者[26]、ただし、詐欺の対象及びそれによって取得したものが単にコンピュータの利用のみであり、かつ、その利用により得る利益が過去一年間で五〇〇〇ドル以下である場合を除く[27]：

(5)

(A)　認識して、プログラム、情報、コードまたは命令の伝送を生じさせ[28]、そのような行為の結果として、権限なく、保護されたコンピュータに対し意図的に損害を発生させる者[29]：

(B)　意図的に、権限なく、保護されたコンピュータにアクセスし、そのような行為の結果として、不注意で損害[30]

を発生させる者：または

(C) 意図的に、権限なく、保護されたコンピュータにアクセスし、そのような行為の結果として、損害及び損失を発生させる者。(31)

(6) 以下に該当する場合において、認識して、無権限でアクセスされるコンピュータで用いられるパスワードその他これに類する情報について（第一〇二九条で定義する）送信を偽る者(32)：

(A) その送信が州際取引もしくは国際取引に悪影響を及ぼす場合：または

(B) 当該コンピュータが合衆国政府により利用され、もしくは、合衆国政府のために利用されるコンピュータである場合。

(7) 他人から金銭その他の有価物を奪う意図で、州際取引もしくは国際取引において、次のもののいずれかを含む通信を伝送する者。

(A) 保護されたコンピュータに損害を発生させる脅威：

(B) 無権限でもしくは権限を超過して、保護されたコンピュータから情報を取得する脅威、または、無権限でもしくは権限を超過して、保護されたコンピュータから取得する情報の完全性を損なう脅威：または、

(C) 保護されたコンピュータに発生する損害が強要行為をもたらし得る場合において、その損害との関係で金銭その他の有価物の要求。(33)

(b) 本条(a)項に基づく犯罪の実行を企てる者及びその犯罪の実行を試みる者は、本条(c)に規定するところに基づき処罰される。

(c) 本条(a)項または(b)項に基づく違反行為に対する処罰は、以下のとおりである。

(1)

(A)　本条(a)項(1)に基づく違反行為の事案であって、本条に基づく他の違反行為による拘禁刑の後に実行されたものではない場合もしくはその違反行為の試みを本副号に基づき処罰し得る場合においては、本款に基づく罰金刑もしくは一〇年以下の拘禁刑またはその併科：及び

(B)　本条(a)項(1)に基づく違反行為の事案であって、本条に基づく他の違反行為による拘禁刑の後に実行されたものである場合もしくはその違反行為の試みを本副号に基づき処罰し得る場合[34]においては、本款に基づく罰金刑もしくは二〇年以下の拘禁刑またはその併科。

(2)

(A)　(B)に規定する場合を除き、本条(a)項(2)、(a)項(3)もしくは(a)項(6)の違反行為の事案であって、かつ、本条に基づく他の違反行為による拘禁刑の後に実行されたものではない場合もしくはその違反行為の試みを本副号に基づき処罰し得る場合においては、本款に基づく罰金刑もしくは一年以下の拘禁刑またはその併科：

(B)　(a)項(2)に基づく違反行為の事案もしくはその違反行為の試みを本副号に基づき処罰し得る事案において、以下の場合には、本款に基づく罰金刑もしくは五年以下の拘禁刑またはその併科。

(i)　当該違反行為が、商業的利益もしくは私的な金銭獲得を目的として実行された場合：

(ii)　当該違反行為が、合衆国もしくは州の憲法及び法律に抵触する犯罪行為もしくは違法な行為の遂行中に実行された場合：または、

(iii)　取得された情報の価値が五〇〇〇ドルを超過する場合。

(C)　本条(a)項(2)、(a)項(3)もしくは(a)項(6)の違反行為の事案であって、本条に基づく他の違反行為による拘禁刑の

後に実行されたものである場合もしくはその違反行為の試みを本副号に基づき処罰し得る場合[35]においては、本款に基づく罰金刑もしくは一〇年以下の拘禁刑またはその併科。

(3)

(A) 本条(a)項(4)もしくは(a)項(7)の違反行為の事案であって、本条に基づく他の違反行為による拘禁刑の後に実行されたものではない場合もしくはその違反行為の試みを本副号に基づき処罰し得る場合においては、本款に基づく罰金刑もしくは五年以下の拘禁刑またはその併科：及び

(B) 本条(a)項(4)もしくは(a)項(7)の違反行為の事案であって、本条に基づく他の違反行為による拘禁刑の後に実行されたものである場合もしくはその違反行為の試みを本副号に基づき処罰し得る場合[36]においては、本款に基づく罰金刑もしくは一〇年以下の拘禁刑またはその併科。

(4)

(A) (E)及び(F)に規定する場合を除き、次の事案においては、本款に基づく罰金刑もしくは五年以下の拘禁刑またはその併科とする。

(i) 本条(a)項(5)(B)の違反行為の事案であって、本条に基づく他の違反行為による拘禁刑の後に実行されたものでない場合において、以下の危険を発生させた場合（または、違法行為の試みのときには、もしその試みが成功したとすれば危険が発生しただろうという場合）

(I) 過去一年間において一人以上の者について（合衆国によって遂行される捜査、起訴その他の手続との関係では、一台以上の保護されるコンピュータに対する侵害との関係で）、少なくとも合計五〇〇〇ドル以上の損失の発生：

(Ⅱ)　一人以上の者に対する診療、診断、治療もしくは介護の阻害もしくは妨害（または潜在的な阻害もしくは妨害）：

(Ⅲ)　個人に対する物理的な侵害：

(Ⅳ)　公衆の健康及び安全に対する脅威：

(Ⅴ)　司法、国防もしくは国家の安全に関する業務遂行において合衆国政府によってもしくはそのために用いられるコンピュータを侵害する損害：または、

(Ⅵ)　過去一年間において一〇台以上の保護されるコンピュータを侵害する損害。

(ii)　本副号に基づき処罰し得る違反行為の試み。

(B)　(E)及び(F)に規定する場合を除き、次の事案においては、本款に基づく罰金刑もしくは一〇年以下の拘禁刑またはその併科とする。

(i)　本条(a)項(5)(A)の違反行為の事案であって、本条に基づく他の違反行為による拘禁刑の後に実行されたものでない場合において、(A)(i)の(I)ないし(Ⅵ)に規定する危険を発生させた場合（または、違法行為の試みのときには、もしその試みが成功したとすれば危険が発生しただろうという場合）：及び

(ii)　本副号に基づき処罰し得る違反行為の試み。

(C)　(E)及び(F)に規定する場合を除き、次の事案においては、本款に基づく罰金刑もしくは二〇年以下の拘禁刑またはその併科とする。

(i)　本条(a)項(5)の(A)もしくは(B)の違反行為の事案であって、本条に基づく他の違反行為による拘禁刑の後に実行されたものである場合：及び(37)

(ii) 本副号に基づき処罰し得る違反行為の試み。

(D) 次の事案においては、本款に基づく罰金刑もしくは一〇年以下の拘禁刑またはその併科とする。

(i) 本条(a)項(5)(C)の違反行為の事案であって、本条に基づく他の違反行為による拘禁刑の後に実行されたものである場合：及び

(ii) 本副号に基づき処罰し得る違反行為の試み。

(E) 加害者が、(a)項(5)(A)の違反行為の実行により、重大な身体的侵害を発生させようと試みた場合または認識してもしくは不注意でそのような重大な身体的傷害を発生させた場合[38]、本款に基づく罰金刑もしくは二〇年以下の拘禁刑またはその併科とする。

(F) 加害者が、認識してもしくは不注意で(a)項(5)(A)の違反行為の実行により死亡を発生させ、またはそれを発生させようと試みた場合[39]、本款に基づく罰金刑、有期拘禁刑もしくは終身拘禁刑またはその併科とする。

(G) 以下の場合については、本款に基づく罰金刑もしくは一年以下の拘禁刑またはその併科とする。

(i) (a)(5)に規定するその他の違法行為：または

(ii) 本副号に基づき処罰し得る違反行為の試み。

(d)

(1) 捜査権限を有する他の政府機関に加え、合衆国シークレットサービスは、本条に基づき犯罪行為を捜査するための権限を有する。この合衆国シークレットサービスの権限は、財務長官と司法長官との間で締結されるべき合意に基づいて発効する。

(2) 連邦捜査局は、諜報活動、外国の対敵情報活動、国防もしくは国際関係上の理由により無権限開示から保護さ

れている情報、禁止データ（この用語は一九五四年原子力法一一条ｙ項で定義されている。）を含む場合などについて、本款三〇五六条(a)項に基づく合衆国シークレットサービスの義務[40]を侵害する行為の場合を除き、(a)項(1)に規定する違反行為を捜査する第一次的な権限を有する。

(3)　この権限は、財務長官及び司法長官間の合意に従って執行される。

(e)　本条において用いるときは、

(1)　「コンピュータ」という用語は、論理機能、演算機能もしくは記憶機能を実行する電子装置、電磁的装置、光学装置、電子化学的装置[41]またはその他の高速データ処理装置を意味し、かつ、当該装置と直接に関連するデータ記憶設備もしくは通信設備、または、当該装置と共に運用されるデータ記憶設備もしくは通信設備を含むが、自動タイプライタ、タイプセッタ、携帯用電卓もしくはこれらと類似する装置を含まない。

(2)　「保護されるコンピュータ」という用語は、

(A)　金融機関若しくは合衆国政府の専用コンピュータ、または、そのような専用コンピュータでない場合には、金融機関若しくは合衆国政府により利用されるコンピュータ、もしくは、それらのために利用されるコンピュータであって、かつ、当該行為が、金融機関もしくは合衆国政府による利用もしくはこれらのための利用に対する阻害行為となるものを意味し…または、

(B)　州際取引もしくは海外取引または通信において利用されるコンピュータを意味し、合衆国外に所在するものでも州際取引もしくは海外取引または合衆国の通信に影響を及ぼすような方法で利用されるものを含む。

(3)　「州」という用語は、コロンビア特別区、プエルトリコその他の保護領、準州及び属領を含む。

(4)　「金融機関」という用語は、

(A) 連邦預金保険公社によって保険された預金を持つ機関；
(B) 連邦準備銀行を含め、連邦準備もしくはその構成員；
(C) 全米信用組合管理局によって保険された口座を持つ信用組合；
(D) 連邦住宅融資銀行システムの構成員及び住宅融資銀行；
(E) 一九七一年農場信用法に基づく農業信用システムの機関；
(F) 一九三四年有価証券取引法第一五条に基づき米国証券取引委員会に登録した取引業者；
(G) 有価証券投資者保護法人；
(H) 一九七八年国際銀行業法第一条(b)項(1)もしくは(3)に規定するような外国銀行の支店もしくは代理店；並びに、
(I) 連邦準備銀行法第二五条または第二五条(a)項に基づいて運営されている組織；

を意味する。

(5) 「信用情報記録」という用語は、顧客と金融機関との関係を維持するために金融機関が保有する記録から引き出される情報を意味する。

(6) 「権限超過アクセス」という用語は、アクセスする者が取得もしくは改変の権限を有していないのに、コンピュータにアクセスし、かつ、当該コンピュータ内にある情報の取得もしくは改変のためにそのアクセスを用いることを意味する。

(7) 「合衆国の部局」という用語は、政府の立法部門若しくは司法部門または第五款第一〇一条に列挙された執行部門の中の一つを意味する。

(8) 「損害」という用語は、データ、プログラム、システムもしくは情報の完全性または可用性に対する何らかの

侵害行為を意味する。

(9)　「政府の組織」という用語は、合衆国の政府、合衆国の州もしくは州政府、外国及び外国の州、地方自治体、市町村その他の統治組織を意味する。

(10)　「拘禁刑」という用語は、コンピュータに対する無権限アクセスもしくは権限超過アクセスを要素とし、一年以上の服役によって処罰可能な犯罪について定める州の法律に基づく拘禁を含む。

(11)　「損失」という用語は、被害者に生じた合理的な金銭的負担を意味し、侵害行為に対する対応費用、損害を評価する行為の費用、データ、システムもしくは情報を侵害行為以前の状態に復するための修復費用、収入の喪失、被害による費用、または、役務提供の阻害により生じたものその他の副次的な損害を含む。

(12)　「者」という用語は、個人、団体、会社、教育機関、金融機関、政府機関、司法機関その他の組織を含む。

(f)　本条は、合衆国、州もしくは州政府の法執行機関または合衆国情報局の適法な捜査活動、防衛活動ないし諜報活動を禁止するものではない。

(g)　本条の違反行為により損害もしくは損失を被った者は、その加害者に対し、損害賠償請求、暫定的差止請求またはその他の衡平法上の救済を求めるため、民事訴訟を提起することができる。(c)項(4)(A)(i)の(I)、(II)、(III)、(IV)または(V)に規定する事項中のどれか一つが行為の中に含まれている場合にのみ、本条の違反を原因とする民事訴訟を提起することができる。(c)項(4)(A)(i)(I)に規定する行為のみを含む侵害行為に対する損害賠償請求は、経済的損失に限られる。侵害行為であると主張された行為の日または損害を発見した日から二年を経過したときは、本条に基づく訴訟を提起することはできない。コンピュータハードウェア、コンピュータソフトウェアまたはファームウェアの設計もしくは製造に対する侵害行為については、本条に基づく訴訟を提起することができない。

(h) 司法長官及び財務長官は、本条制定後の最初の三年間は、(a)項(5)に基づく捜査と起訴について、連邦議会に対する年次報告をしなければならない。

(i)

(1) 裁判所は、本条の違反行為により起訴された者または本条に違反する企てにより起訴された者に対して判決を宣告するに際し、他の刑に付加するものとして、かつ、州法の条項とはかかわりなく、そのような者に対し、以下のものを合衆国が没収することを命じなければならない。

(A) 当該違反行為を遂行するため、もしくは、その遂行を容易にするために用いられ、または、そのように用いる準備をした財産上の利益；及び

(B) 当該違反行為を組成しもしくは当該違反行為から得られた財産（動産もしくは不動産）、当該違反行為の結果として、直接もしくは間接にその者が得た利益。

(2) 本項に基づく財産の没収刑、その捜索及び押収並びにこれらと関連する司法手続は、本条(d)項に規定する場合を除き、一九七〇年総合薬物濫用防止並びに規制法（21 U.S.C. 853）四一三条の規定に従って実施されなければならない。

(j) (i)項においては、次の物品に対して合衆国が没収する権限を有し、当該物品について優越的な権利は存在しない：(42)

(1) 本条の違反行為を遂行するため、もしくは、その遂行を容易にするために用いられ、または、そのように用いる準備をした財産。

(2) 本条の違反行為もしくはその企てを組成しまたはそれから得られた財産もしくは不動産。

［原文］

18 USC § 1030 - Fraud and related activity in connection with computers

(a)Whoever—

(1)having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2)intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A)information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B)information from any department or agency of the United States; or

(C)information from any protected computer;

(3)intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4)knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

(A)knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B)intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C)intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(6)knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A)such trafficking affects interstate or foreign commerce; or

(B)such computer is used by or for the Government of the United States;

(7)with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A)threat to cause damage to a protected computer;

(B)threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C)demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b)Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c)The punishment for an offense under subsection (a) or (b) of this section is—

(1)

(A)a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B)a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under

subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A)except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B)a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

(i)the offense was committed for purposes of commercial advantage or private financial gain;

(ii)the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii)the value of the information obtained exceeds $5,000; and

(C)a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A)a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under

subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B)a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)

(A)except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—

(i)an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

(I)loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(II)the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III)physical injury to any person;

(IV)a threat to public health or safety;

(V)damage affecting a computer used by or for an entity of the United States Government in furtherance of

the administration of justice, national defense, or national security; or

(VI)damage affecting 10 or more protected computers during any 1-year period; or

(ii)an attempt to commit an offense punishable under this subparagraph;

(B)except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i)an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii)an attempt to commit an offense punishable under this subparagraph;

(C)except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of—

(i)an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or

(ii)an attempt to commit an offense punishable under this subparagraph;

(D)a fine under this title, imprisonment for not more than 10 years, or both, in the case of—

(i)an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or

(ii)an attempt to commit an offense punishable under this subparagraph;

(E)if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F)if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G)a fine under this title, imprisonment for not more than 1 year, or both, for—

(i)any other offense under subsection (a)(5); or

(ii)an attempt to commit an offense punishable under this subparagraph.

(d)

(1)The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2)The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3)Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e)As used in this section—

(1)the term “computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2)the term “protected computer” means a computer—

(A)exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B)which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3)the term “State” includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4)the term “financial institution” means—

(A)an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B)the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C)a credit union with accounts insured by the National Credit Union Administration;

(D)a member of the Federal home loan bank system and any home loan bank;

(E)any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F)a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G)the Securities Investor Protection Corporation;

(H)a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I)an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5)the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6)the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7)the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8)the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9)the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10)the term “conviction” shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11)the term “loss” means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12)the term “person” means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f)This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g)Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h)The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3

years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(i)

(1)The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

(A)such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B)any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2)The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j)For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1)Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2)Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this

section, or a conspiracy to violate this section.

## 六　まとめ

以上で本論文における電子計算機使用詐欺罪に関する検討を終える。電子計算機使用詐欺罪は、条文上の位置づけとは無関係に、その本質として財産上の利益の窃取行為に該当するものであり、いわば二項窃盗として認識・理解すべきものである。

他方、本論文ではあえて詳しく触れなかったが、電子計算機使用詐欺罪を構成する行為と全く同じ行為が、法解釈論上では横領罪や背任罪を構成することが十分にあり得る。この点に関しては、刑法総論の領域に属する法解釈論上の非常に厄介な問題を精密に分析・検討した上でないと正確な立論をすることができないため、更に考察を深めてから別稿において私見を明らかにしたい。(43)

電子計算機使用詐欺罪を含め、サイバー犯罪中の財産犯に属する犯罪行為に関する現行刑法上の処罰条項は、基本的には昭和六二年刑法一部改正により追加的に立法されたものである。これは、インターネットが社会に広く普及する以前の時代状況を前提としたものだと言わざるを得ない。すなわち、あくまでも財物の奪取を基本形とする財産犯の体系を前提とするものである。それゆえ、利得型犯罪は、メインの犯罪類型としては認識されていない。しかしながら、インターネットと電子商取引の普及の結果、時代は大きく変化した。物品だけではなく役務もまた重要な財産権の一部とされ、とりわけ「情報財」の価値が高まっている。そのような現在の状況を踏まえると、財産犯としての電子計算機を用いた財産的利益の無権限取得行為について、そのような類型に属するサイバー犯罪全体にわたり、法

理論の再構築が求められていると考える。

電子計算機を用いた財産権の不正取得と関連するサイバー犯罪について、引き続き調査・検討を重ね、その検討結果を論文のかたちで公にしたいと考える。(44)

注

（1）　日本国の刑法二四六条の二が制定されるに際し非常に大きな影響を与えたと思われる当時のドイツにおける学説・判例については、ウルリッヒ・ズィーバー（西田典之・山口　厚訳）『コンピュータ犯罪と刑法Ⅰ』（成文堂、一九八六）二〇四～二三七頁参照。

（2）　夏井高人『裁判実務とコンピューター法と技術の調和をめざして』（日本評論社、一九九三）八一頁以下、米澤慶治編『刑法等一部改正法の解説』（立花書房、一九八八）一一二頁以下、的場純男・河村　博『コンピュータ犯罪Q&A』（三協法規、一九八八）一三八頁以下、日本弁護士連合会刑法改正対策委員会編『コンピュータ犯罪と現代刑法』（三省堂、一九九〇）一四九頁以下参照。なお、コンピュータ犯罪について他にも非常に著名な書籍・文献が存在するが、その内容に剽窃またはこれに類する行為があった疑いがあるため、本論文では引用しない。

（3）　前掲『刑法等一部改正法の解説』一一六頁

（4）　前掲『コンピュータ犯罪と現代刑法』一五三頁

（5）　昭和六二年刑法一部改正当時の英米における立法動向に対する認識を理解するためには、辛島　睦「アメリカにおけるコンピュータ犯罪立法」法とコンピュータ一号五三頁（一九八三）が参考になる。また、電子計算機を用いた違法な財産的利益の取得行為について詐欺罪が成立するか否かが争点となった英米の裁判例に対する当時の認識については、宮野　彬「アメリカとカナダにおけるコンピュータ犯罪」法とコンピュータ一号八三頁が参考になる。

（6）　理論的には横領罪や背任罪に該当するような行為またはこれに類する行為についても理論的な整理が必要となるが、この点については別稿において改めて論ずることとし、本論文では触れないことにする。なお、この点に関する従来の議論としては、前掲『コンピュータ犯罪と現代刑法』一五三頁以下が最も詳しく論じている。

（7）　刑法二四六条の二に定める条文の文言どおりに電子計算機に対して「不正な指令」を与えると、エラーとして処理しない結果に終わるか、または、当該電子計算機が暴走するかどちらかであるので、犯罪としては既遂に達することがあり得ないとい

う意味で必ず不能犯となる。そのため、電子計算機使用詐欺罪における「不正な指令」とは、「権限なく何らかの指令を与える行為」と法解釈する以外にないと解される。

（8） このように「権限」を機軸として考察することは、従来の刑法各論におけるアプローチとは全く異なるかもしれないが、理論的にも実務的にも極めて有用である。この点については、夏井高人「アメリカ合衆国におけるコンピュータ犯罪立法動向―無権限アクセスを中心とする比較法的検討と日本法への示唆」判例タイムズ一〇〇八号一〇六頁でも若干の考察結果を示した。

（9） リアルタイムの状況分析については、筆者（夏井）が運営している下記のブログサイトに日々アップロードされる記事を参照されたい。

サイバー法ブログ

http://cyberlaw.cocolog-nifty.com/

（10） 前掲『刑法等一部改正法の解説』一一六頁。裁判例としては、最高裁昭和三一年八月二二日決定・刑集一〇巻八号一二六〇頁、東京高裁昭和三一年一月三〇日判決・東京高等裁判所（刑事）判決時報七巻一号二四頁、名古屋高裁昭和二八年一〇月一四日判決・高等裁判所刑事判例集六巻一一号一五二五頁、浦和地裁昭和二八年八月二一日判決・判例時報八号一九頁などがある。

（11） 事案は少し異なるが、変造されたプリペイドカードをパチンコ球遊機に挿入し、その球遊機を使用可能にすれば、その時点で本来であればプリペイドカードへの入金の負担という財産上不法の利益を得ることになるという点をとらえ、電子計算機使用詐欺罪の成立を認めた事例として、長野地裁諏訪支部平成八年七月五日判決・判例時報一五九五号一五四頁がある。通常、プリペイドカードを挿入すると、カード度数を電子計算機が計算処理した上で、その度数に対応する数量のパチンコ玉を自動供給する仕組みになっているが、このパチンコ玉の供給がなされた時点で既遂になるという見解を採用すると、利得罪である電子計算機使用詐欺罪ではなく財物の奪取罪である窃盗罪が成立するということになるはずである。このことからも、この両者の罪は本質的に同じ犯罪類型に属するものだということを理解することができる。

（12） 夏井高人監修『ＩＴビジネス法入門』（ＴＡＣ出版、二〇一〇）二〇五～二〇八頁

（13） 前掲夏井高人「アメリカ合衆国におけるコンピュータ犯罪立法動向」を参照されたい。

（14） 「権限」という構成要件要素を機軸として犯罪類型をまとめなおすと、様々な違法性阻却事由をより合理的に整理して認識・理解することができるという利点もある。この点については、本論文では示唆にとどめ詳論を避ける。

（15） 正確には、自律型ロボットに対して窃盗罪や電子計算機使用詐欺罪のような行為が実行されたとしても、その自律型ロボッ

トの所有者が存在せず、人間と同様に自律的に社会内で生活しているとすれば、（ロボットにも私権の共有能力すなわち権利能力を肯定するのでない限り）「法益侵害がない」という奇妙な事態が生じ得ることになる。なぜなら、当該ロボットに権利能力が認められない場合、ロボットから何かを奪っても無主物先占が成立し得ることになり、その場合には、法益侵害があり得ないという論理的帰結を承認せざるを得ないからである（当該ロボットについて人間である所有者が存在している場合には、その所有者としての人間が法益侵害を受ける被害者になることは当然の前提である。）。

（16）『平成二四年中のサイバー犯罪の検挙及び相談状況等について』（警察庁、平成二五年三月二八日）一頁によれば、電子計算機使用詐欺罪による検挙数は、平成二〇年二二〇件、平成二一年一六九件、平成二二年九一件、平成二三年七九件及び平成二四年九五件とされている。

（17）判例研究として、佐々木史郎編『犯罪経済刑法体系第三巻刑法』（日本評論社、二〇一〇）三五五頁［薄金孝太郎］がある。

（18）頁数の関係で犯罪事実の一部のみを示す。実際には同様の手口による多数回にわたるキセル乗車行為について電子計算機使用詐欺罪により起訴され、有罪となった。

（19）外務省訳に基づく。

（20）［訳注］故意による無権限アクセス行為または権限超過アクセスのことを指す。

（21）［訳注］日本国の類似情報としては、貸金業法に基づく指定信用情報機関が保有する与信情報等が相当する。

（22）［訳注］合衆国政府の部局のコンピュータシステムに無権限アクセス等をすることによって取得することのできる情報という意味である。

（23）［訳注］合衆国政府の部局のコンピュータシステム内にある情報については(B)で既に規定されていることから、(C)はそれ以外のコンピュータシステムすなわち民間部門にあるコンピュータシステムについて規定していることになる。「保護されたコンピュータ」は(e)(2)で定義されている。

（24）［訳注］無権限アクセス行為のことを指す。

（25）［訳注］合衆国連邦政府専用コンピュータに対する無権限アクセスは原則として有罪となるが、合衆国連邦政府専用コンピュータではないけれども合衆国連邦政府が利用しているコンピュータに対する無権限アクセスの場合には、合衆国連邦政府による利用に悪影響を生じさせる場合にのみ有罪となるという趣旨である。民間のパブリッククラウドコンピューティングサービスを合衆国政府及び民間企業等が共同利用しているような場合（合衆国連邦政府による業務委託先のコンピュータシステムがパ

ブリッククラウドコンピュータであり、合衆国連邦政府専用のシステムとして利用されているのではなく、他の民間企業も同じパブリッククラウドコンピュータシステムからサービス提供を受けているような場合を含む。）、後者の非専用コンピュータに対する無権限アクセスが問題となり得る。

(26) ［訳注］United States v. Czubinski, United States Court of Appeals for the First Circuit, 1997, 106 F.3d 1069.

(27) ［訳注］コンピュータシステムを無権限利用したというだけでも利用代金や電気料金の支払を免れることができるから、無権限利用されたことによる損失を計算することが可能である。

(28) ［訳注］攻撃用パケットの送信による DoS 攻撃（DDoS 攻撃）については、夏井高人「サイバー犯罪の研究（一）—DoS 攻撃（DDoS 攻撃）に関する比較法的検討—」法律論叢八五巻一号一九七頁以下を、スパイウェアに関しては「サイバー犯罪の研究（三）—通信傍受に関する比較法的検討—」法律論叢八五巻六号三六三頁以下をそれぞれ参照されたい。

(29) ［訳注］損害という結果の発生を犯罪成立要件としているので、結果犯である。ただし、結果が発生しない場合でも、別途、未遂罪として処罰される。

(30) ［訳注］「reckless」は多義的な概念であり、各国の法制によってその意味内容が微妙に異なることがある。一般的には、「無謀に」と訳されることが多いが、高柳賢三・末延三次編『英米法辞典』（有斐閣、一九五二）四〇一頁は「不注意」という訳語をあてている。米国刑事法においては、この「reckless」という概念は、「意図的（intentionally）」に結果を発生させた場合を含まない。そして、「reckless」により結果を発生させた場合、意図的に損害を発生させた場合よりも罪責が軽い。一般的には、損害という結果発生について予見または予見可能性があったのに敢えて行動し、結果を発生させた場合を指すものとして解することができる。したがって、厳密には、「reckless」として実行される犯罪行為には、日本国の故意概念上における「未必的故意」が認められる場合と「過失」による場合とを含み得ることになると思われる。

(31) ［訳注］(C)の場合、無過失でも結果を発生させた場合を処罰対象としている。法定刑は、(A)の意図的に発生させた場合が最も重く、(B)の「reckless」の場合には少し軽く、そして、(C)の場合が最も軽い。これらの法定刑の軽重は、損害発生という結果に対する主観的意図（意欲）の軽重に対応している。この点については、Orin S. Kerr, Computer Crime Law, Thomson West, 2006, p.85 が参考になる。

(32) ［訳注］合衆国法律集一八款一〇二九条(e)項(5)は、「送信（trafficc）」について、「第三者に対する伝送その他の処理をするこ

と、または、伝送その他の処理をする意図で管理を取得することを意味する」と定義している。

(33) ［訳注］いわゆる Ransomware（Ransom malware）による恐喝行為のような場合を想定するものと考えられる。

(34) ［訳注］(B)は、(A)により処罰される違反行為及びその未遂行為の行為者について、この法律違反により処罰された前科がある場合の同種前科累犯加重処罰条項である。

(35) ［訳注］(C)は、(A)または(B)により処罰される違反行為及びその未遂行為の行為者について、この法律違反により処罰された前科がある場合の同種前科累犯加重処罰条項である。

(36) ［訳注］(B)は、(A)により処罰される違反行為及びその未遂行為の行為者について、この法律違反により処罰された前科がある場合の同種前科累犯加重処罰条項である。

(37) ［訳注］(4)の(A)または(B)により処罰される違反行為及びその未遂行為の行為者について、この法律違反により処罰された前科がある場合の同種前科累犯加重処罰条項である。

(38) ［訳注］①航空機を墜落させたり建築物に衝突させたりし、それによって当該航空機の乗員や旅客等を傷害する目的で、連邦政府の航空管制システムに無権限アクセスするような行為、あるいは、②原子力発電所の制御システムを暴走させ、当該原子力発電所を爆発させることによって、当該発電所の作業員や近隣住民等を傷害する目的で、当該原子力発電所のコンピュータシステムに無権限アクセスする行為などのテロ行為を想定しているものと解される。

(39) ［訳注］(A)と同様のテロ行為などを想定しているものと解される。(A)は被害者の死亡に至らずに傷害の程度にとどまった場合に適用され、(B)は殺人または傷害致死の場合に適用される。(B)は(A)の加重処罰条項という形式をとっている。日本国法では、傷害致死罪または殺人罪が適用されることになり、併合罪として不正アクセス罪等が成立することになろう。なお、金融システムを混乱させ、投資家や銀行経営者等を破産させた上で、破産による精神的ショックから自殺することを期待して、当該金融システムに無権限アクセスや DDoS 攻撃を実行したような事案を想定した場合、破産者が常に自殺するとは限らないので、加害者に殺人の目的はあっても因果関係の立証上の問題があり、故意による犯罪として(B)が適用され得るかどうかについて疑問がある。このような事案における殺人罪の成否については、日本国法の適用の場合でも同様の疑問がある。

(40) ［訳注］合衆国法律集第一八款三〇五六条(a)項は、合衆国シークレットサービスが守るべき義務のある者（対象者）を列挙している。その中には、合衆国の大統領、副大統領、前大統領及びこれらの者の家族などが含まれている。

(41) ［訳注］現在主流の電子計算機の大部分は無機質の要素によって構成されている。しかし、バイオコンピュータに典型的に

見られるように、有機質を構成要素とするものも存在する。今後は、無機と有機の共働が更に進むであろう。「電子化学的」な場合とは、そのようなものにも適用可能と思われる。

（42）［訳注］連邦による没収に対して、その没収対象物件の所有者が所有権を主張することができないという趣旨と解される。

（43）この論点と関連する裁判事例として、東京高裁平成五年六月二九判決・高等裁判所刑事判例集四六巻二号一八九頁及びその原審判決である東京地裁平成四年一〇月三〇日判決・判例時報一四四〇号一五八頁がある。原審は、主意的訴因である電子計算機使用詐欺罪の成立を否定し、予備的訴因である背任罪の成立を認めて有罪とする旨の判決をしたのに対し、控訴審は、原審判決を破棄した上で電子計算機使用詐欺罪の成立を認めて有罪とする旨の判決をした。

（44）本論文は、文部科学省私立大学戦略的研究基盤形成支援事業（平成二三年～平成二七年度）による研究成果の一部である。