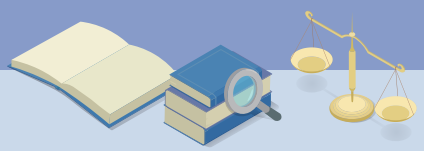
誌上法学講座

消費生活相談に関連する刑法



第4回

電子計算機使用詐欺罪

穴沢 大輔　Anazawa Daisuke　明治学院大学法学部消費情報環境法学科教授
専門は刑法、その中でも主に財産犯罪・経済犯罪を研究。『入門経済刑法』(共著、信山社、2021年)など執筆。
消費生活アドバイザー。東京都医学総合研究所人対象研究倫理審査委員会外部委員

総務省によれば、2022年の日本のインターネット利用率(個人)は84.9%となっており[*1]、国民が広く生活の中で利用していることになります(コロナ禍では、特にオンラインでの取引が活性化したのは記憶に残るところですね)。今回は、インターネットを利用した取引(以下、ネット取引)に潜む犯罪について考えてみましょう。

パソコンやスマホを用いた詐欺罪

事例1　Aは、「免税店の閉店にあたり、高級腕時計が在庫処分として格安で売り出される」という広告を見つけ、百貨店名が示されていたことから通販サイトにアクセスし、代金引換で購入した。しかし、受け取った箱を開けると、時計は高級品ではなく、さらに壊れていた[*2]。

皆さんは、Aがだまされているので詐欺のような気がするが、パソコンやスマホを用いているので、何罪になるのかよく分からない、と思われたかもしれません。ただ、本講座で示してきた思考方法によれば、これが詐欺罪に該当することは問題ないでしょう。すなわち、Aは、欺罔(ぎもう)行為により錯誤に陥らされ、代金引換で金銭を交付し、壊れた時計という本来の使用もできないものを手にしたのであって、損失もあり、詐欺罪の条文に当てはまる被害者だからです。

詐欺罪は、「人(A)」を欺いて財物を交付させる罪であり、パソコンやスマホがツールとして用いられていたとしても、人が欺かれていれば、その適用にまったく問題はないのです。したがって、偽の警告表示にだまされて、プリペイド型電子マネーで支払わされる[*3]のも基本的には同じです。

「こうした事案が詐欺罪に当たるのだとすると、その次の条文に規定されている『電子計算機使用詐欺罪』(刑法246条の2。以下、本罪)は、どのような場合に適用されるのか？」これは、ごく自然な問題意識だと思います。この条文の制定経緯を確認しておきましょう。

電子計算機使用詐欺罪の新設

1987(昭和62)年の刑法改正では電子計算機(コンピュータ)を用いた犯罪について一定の対応がなされました。コンピュータが用いられますと、大量、迅速かつ正確なデータの処理が人に代わって行われることになります。それは大変便利なことですが、それだけ犯罪の温床にもなりやすいといえます(偽造関係の改正については、次回本講座第5回で解説予定です)。

実は、この改正では、不正データの入力により不法の利益を得る行為の処罰が、従来の詐欺罪では対応できないことが指摘されたのです。もう少し、具体化してみましょう。例えば、Xが、ある金融機関のコンピュータを不正に操作して自己の預金残高を改ざんして、それを別の金融機関の口座に振り込ませたとしましょう。ここで詐欺罪による処罰ができればよいのですが、「人」が欺かれていないため、条文の文言に当てはまらず、適用ができないのです(金銭を盗ん

＊1　総務省「令和5年版情報通信白書」https://www.soumu.go.jp/johotsusintokei//whitepaper/ja/r05/html/nd24b120.html
＊2　国民生活センター 見守り新鮮情報「百貨店をかたる偽通販サイトにだまされないで」(2022年2月8日発行)
https://www.kokusen.go.jp/mimamori/pdf/shinsen415.pdf
＊3　国民生活センター 見守り新鮮情報「偽警告表示プリペイド型電子マネーで支払わせる手口に注意」(2021年3月9日発行)
https://www.kokusen.go.jp/mimamori/pdf/shinsen388.pdf

だのだから窃盗罪ではないか、と思われた人がいるかもしれません。確かに、その感覚は鋭いのですが、窃盗罪は「物」を奪うと規定されておりまして、やはり対応ができないのです)。

こうした不法な利益を得る行為が野放しになることを避けるために、本罪が新設されました。次の事例で、適用場面を確認してみましょう。

本罪が適用される事例

事例2 X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た。

少し複雑なのですが、246条の2の条文構造を確認しながら本事例を考えてみましょう。まず、「人の事務処理に使用する電子計算機」に対してなされることが必要です。ここでは、決済側のコンピュータ、すなわち、電子マネーを販売する決済代行業者のコンピュータになります。

続いて、これが重要な概念なのですが、「虚偽の情報若しくは不正な指令を与え」ることです。この点、最高裁は同様の事案で次のように述べています(最高裁平成18年2月14日決定)。「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」を与えた、と。この虚偽の情報とは、一般的に「当該電子計算機による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て、その内容が真実に反する情報」と解されています。ですので、コンピュータに入力された情報それ自体は、数値としては正しいとしましても(高裁で、弁護人は「クレジットカード上の名義人名、カード番号及び有効期限の各情報」は「正規のクレジットカードの情報そのもの」であり、虚偽とはいえないと主張していた)、「虚偽」の情報といえるのです。当たり前のように感じられたかもしれませんが。

そして、「財産権の得喪若しくは変更に係る不実の電磁的記録を作り、(中略)財産上不法の利益を得(中略)た」ことが必要です。前述の最高裁では「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11万3000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」とされ、本罪の成立が認められたのです。

このように、いわば機械をだます行為によって不実の電磁的記録が作成され、利益を得る行為が本罪の処罰対象とされるのです。

もう一例紹介しておきましょう。

事例3 Xは、高速道路のETCシステムにおいて連結車両の通行料金が流入料金所で計測された接地車軸数を基に算出されることを悪用し、流入料金所の直前で車軸自動制御装置を操作して一時的に車軸を上昇させ、自車を特大車ではなく、大型車扱いにして差額の支払いを免れた。

高速道路も以前は「人」が料金所で対応するしかありませんでした。この場合には「人」が介在していますので、不正に通行料金を免れる行為について、伝統的な詐欺罪による処罰が検討されてきました(肯定例として、福井地裁昭和56年8月31日判決)。ただ、皆さんもご存じのように、ETCシステムは「人」が介在しない料金徴収システムであり、事例と同様の事案を扱った判決では、「車両がいずれも特大車であるのに、これらがいずれも大型車であると計測させ」て虚偽の情報が与えられたうえで、「車両の通行料金が同表支払料金欄記載の各金額である旨の財産権の得喪、変更に係る不実の電磁的記録」を作ったと評価され、有罪とされています(横浜地裁平成27年6月9日判決。このほかにも、不正通行事例はあります。例えば、NEXCO東日本ウェブサイト参照[*4])。

*4 NEXCO東日本ドライバーズサイト(ドラぷら) https://www.driveplaza.com/etc/etc_guide/effort/

さらに、暗号資産の不正な移転行為についても、本罪の成立を認めた判決があります（東京地裁令和３年７月８日判決参照。「暗号資産NEMにつき、氏名不詳者が、P2株式会社の管理するNEMアドレスから氏名不詳者らが管理するNEMアドレスに送信する旨の情報を与えて暗号資産NEMを移転させた」行為に本罪を認めた）。

本罪の適用について、ある程度お分かりいただけたと思います。なお、本罪は、このような作成型のみならず供用型も処罰の対象にしています。条文上、「又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して」という部分になります。例えば、内容虚偽の交通系ICカードを用いて、電車を不正に利用する行為がこれに当たります。

フィッシングへの適用

事例４　携帯電話会社名で「不正ログインされた可能性があるので、IDとパスワードを変更してください」等のSMS（ショートメッセージサービス）が届き、携帯電話会社のID、パスワード、暗証番号等を入力したら、その後携帯電話会社から身に覚えのない決済メールが届いた＊５。

ID・パスワードなどの情報を不正に奪う行為について、その処罰がどうなるのか、本罪が適用されるのか、と聞かれることがあります。ただ、先にもみたように、本罪は不正に利益を得る行為が処罰の対象であり、ここでは、直接の金銭的被害はありません。

もっとも、こうした行為が処罰に値しないとはいえません。事例のようなID・パスワードなどを入力させる行為は「フィッシング」として、警察庁も注意喚起しています＊６。

フィッシングの処罰規定は、刑法典ではなく、特別刑法である不正アクセス行為の禁止等に関する法律（以下、不正アクセス禁止法）にあります。そこでは、他人の識別符号（ID・パスワード）を不正に取得する行為や識別符号の入力を不正に要求する行為が禁止の対象とされ（同法４条、７条）、その禁止違反に刑罰が科されます（同法12条。１年以下の拘禁刑または罰金）。

そうだとすれば、「罰せられるのはよいが、フィッシング『詐欺』とは名ばかりで、重く処罰されないのでは」という疑問が湧くかもしれません。この点は、その後になされる行為がさらに犯罪と評価され、重く処罰されることになります。つまり、取得したID・パスワードを用いて不正にログインすれば、不正アクセス禁止法違反（不正アクセス行為。同法３条、11条）となり、さらに、そのログイン状態で不正に送金をすれば、先に確認したように本罪に当たりますので処罰することが可能です。そして、そうした行為を多数人に対して行えば、それぞれ犯罪と評価されます（東京地裁平成29年４月27日判決参照。懲役８年の実刑とされた）。この意味で、不正アクセス行為はコンピュータを用いた他人の財産の侵害等に向けた、いわばネットワークの中で鍵のかかった入口を突破したことを処罰対象とするものといえましょう。

なお、「クレジットカード番号等」については、人をだましてそれを提供させる行為は割賦販売法により処罰の対象とされています（割賦販売法49条の２。不正アクセス行為によって取得する行為も処罰する）。この点につき、東京高裁令和２年３月18日判決は、与信を伴わず即時的な支払決済に用いられるデビットカードの会員番号等の情報は本条のクレジットカード情報等に当たらないとしました（それを認めた第１審判決を破棄）。

次回は、偽造や電磁的記録の不正作出について解説します。

＊５　国民生活センター「携帯電話会社をかたる偽SMSにご注意！－あなたのキャリア決済が狙われています－」（2019年９月５日公表）
https://www.kokusen.go.jp/news/data/n-20190905_1.html

＊６　警察庁ウェブサイト https://www.npa.go.jp/bureau/cyber/countermeasures/phishing.html