〔論　説〕

電子計算機使用詐欺罪における「虚偽の情報」の解釈・適用

那　須　翔

Ⅰ　はじめに

電子計算機使用詐欺罪（以下「電算機詐欺罪」という）は、1987 年、窃盗罪と詐欺罪の処罰の間隙を埋めるべく新設された。当時、銀行のオンラインシステムに架空の振込みを入力して自己の口座残高を増やす行為、他人のキャッシュカードを ATM に挿入して自己の口座に振込みをする行為、偽造したプリペイドカードを利用してサービスの提供を受ける行為などが想定されていた。その後、最高裁は、盗品であるクレジットカードをオンラインで使用して電子マネーを購入した行為に本罪を適用した。決定文は簡潔であったが、調査官解説が「虚偽の情報」を規範的に判断すべきことを示した。その後の下級審は、調査官解説が示した手法を応用し、様々な行為に本罪の成立を認めてきた。このような傾向に対し、学説からは、処罰拡大への懸念が示されてきた[1)]。

このような中で、近時、電算機詐欺罪に関する 2 つの裁判例が現れた。一つは、サイバー攻撃により暗号資産 NEM に係る秘密鍵を入手し、それを利用して当該 NEM を外部に移転した行為に本罪の成立を認めた判決である[2)]（以下「令和 4 年東京高判」という）。もう一つは、いわゆる誤振込に係る預金を（決済代行サービスを通じて）オンラインカジノで費消した行為に本罪の成立を認めた判決である[3)]（以下「令和 5 年山口地判」という）。しかし、私見によれば、両判決は、少なくとも理由付けにおいて不当である。

本稿では、電算機詐欺罪の「虚偽の情報」要件について、立案担当者見解と判例を分析した上で（Ⅱ）、詐欺罪に関する議論を参照しつつ、対人取引（人が介在

---

1) このような懸念が生じた一因は、立案担当者が「〔本罪〕の適用場面を明らかにする上で中核的な意味」を込めていた「財産権の得喪、変更に係る電磁的記録」という概念（米澤慶治編『刑法等一部改正法の解説』117 頁〔的場純男〕（立花書房、1988））が、コンピュータ化、ネットワーク化の進展によりその機能を果たさなくなったことにあると考えられる。なお、立案段階では、「処罰範囲のいたずらな拡大を防止するとともに、適用場面を明らかにする」というより踏み込んだ説明がされていた（「法制審議会刑事法部会 46 回速記録」56 頁、「骨子（事務当局私案）についての刑事法部会における事務当局説明要旨」6 頁 117 頁。これらの資料は法務省刑事局に対する行政文書開示請求によって入手可能である）。

2) 東京高判令和 4 年 6 月 23 日公刊物未登載。被告人本人が判決文を公開している。<https://twitter.com/cc_prosecuted/status/1553319993210802176>（2023 年 6 月 30 日最終アクセス）。

3) 山口地判令和 5 年 2 月 28 日裁判所 Web サイト。

する取引）と自動取引（そうでない取引）の異同も意識した限定付けを提案し（Ⅲ）、その上で、令和 5 年山口地判及び令和 4 年東京高判を含む、これまで問題とされてきた事例について検討する（Ⅳ）。これらの検討の概要は、Ⅴに示す。

II　立案担当者見解・平成 5 年東京高判・平成 18 年最決

1　「虚偽の情報」の定義

立案担当者によれば、「『虚偽ノ情報』とは、当該システムにおいて予定されている事務処理の目的に照らし、その内容が真実に反する情報、『不正ノ指令』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い、『与ヘ』とは、これらの情報または指令を人の事務処理に使用する電子計算機に入力することをいう」[4]。平成 5 年の高刑集搭載の東京高裁判決[5]（以下「平成 5 年東京高判」という）は、これを踏襲している。

最高裁は、平成 18 年の決定[6]（以下「平成 18 年最決」という）において「虚偽の情報」に関する判断を示した。同決定は、事例判断であり、明示的に解釈を示したものではないが、担当調査官は立案担当者解説及び平成 5 年東京高判を引用しており[7]、最高裁も立案担当者見解を前提としていると思われる。

なお、これに対して、「虚偽の情報」とは、財産状態の変動について決定すべき立場にある者の意思に反するような情報をいうとする説もある[8]。立案担当者が情報システムの設計・運用者の意思に着目するものであるのに対して、財産的利益の帰属主体の意思に着目するものといえるが[9]、「虚偽の情報」は情報システムに入力されるものであり[10]、本罪の適用が問題となる場面では、財産的利益の帰属主体は当該財産的利益を当該情報システム（の設計・運用者）に委ねていると

---

4)　米澤編・前掲注 1）121 頁〔的場〕。
5)　東京高判平成 5 年 6 月 29 日高刑集 46 巻 2 号 189 頁。
6)　最決平成 18 年 2 月 14 日刑集 60 巻 2 号 165 頁。
7)　藤井敏明「判解」最判解刑事篇平成 18 年度 56 頁（2009）。
8)　鈴木左斗志「電子計算機使用詐欺罪（刑法 246 条の 2）の諸問題」学習院大学法学会雑誌 37 巻 1 号 210 頁（2001）、和田俊憲「キセル乗車」法教 392 号 100 頁（2013）。
9)　橋爪隆「銀行預金に関連する財産犯について」法教 440 号 97 頁注 3（2016）。
10)　橋爪隆「電子計算機使用詐欺罪における『虚偽』性の判断について」研修 786 号 8 頁（2013）参照。

いえるから、情報システムの設計・運用者の意思に着目することでよいと思われる。

２　平成 5 年東京高判と平成 18 年最決

次に、平成 5 年東京高判、平成 18 年最決とその調査官解説を確認する。

（1）平成 5 年東京高判

平成 5 年東京高判は、信用金庫の支店長が、自らの債務を免れるため、振込み等の事実がないのに、担当者に命じて債権者の口座・自己の口座に振込み等があったとする入力をさせた事案に関わる。前記入力をさせた行為が「虚偽の情報」を与えたかが問題となり、判決は、以下のとおりこれを認めた。

「刑法 246 条の 2 の『虚偽ノ情報』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『虚偽ノ情報』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…不良貸付の事例の場合においては、電子計算機に入力された入金情報は、民事法上有効な貸付という経済的・資金的実体を伴い、これに符合しているので、虚偽の情報とはいえず、電子計算機使用詐欺罪は成立しないが（右のような実体を作出した行為につき背任罪の成否が問題になる。）、本件においては、…被告人は自己の個人的債務の支払に窮し、その支払のため、勝手に、支店備付けの電信振込依頼書用紙等に受取人、金額等所要事項を記載しあるいは部下に命じて記載させ、支店係員をして振込入金等の電子計算機処理をさせたものであって、被告人が係員に指示して電子計算機に入力させた振込入金等に関する情報は、いずれも現実にこれに見合う現金の受入れ等がなく、全く経済的・資金的実体を伴わないものであることが明らかであるから、『虚偽ノ情報』に当た」る。

（2）平成 18 年最決

平成 18 年最決は、路上で仮眠中の男性からクレジットカードを窃取した者が、名義人名、カード番号及び有効期限を冒用し、これらをクレジットカード決済代行業者（出会い系サイトの利用代金の支払いに使用していた）の使用する電子計算機に入力送信し、電子マネーの利用権を取得した事案に関わる。前記入力送信行

為が、「虚偽の情報」を与えたものかが問題となり、決定は、以下のとおりこれを認めた（なお、上告趣意は、名義人等の情報それ自体は実在のものである旨主張していた）。

「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〔名義人氏名、番号及び有効期限〕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」。

(3) 平成 18 年最決調査官解説

平成 18 年最決は、上記のとおり簡潔なものであったが、担当調査官は、次のように述べている[11]。

「被告人が電子計算機に与えた『情報』は、『本件クレジットカードによる決済で一定額分の電子マネーの購入を申し込む』ということであり、クレジットカードの名義人氏名、番号、有効期限等は、上記『情報』の構成要素にすぎない」。

「次に、上記与えられた『情報』の内容に申込みの主体に係るもの（クレジットカードの名義人本人によるものであること）が含まれるかどうかが問題になる。…本件システムでは、クレジットカード面上の情報を入力するだけで決済ができ、それ以上に申込人がカードの名義人本人であることを示す情報（主体認証情報）の入力が求められていない。そのことから、本件システムではクレジットカードの名義人本人以外の者が電子マネーを購入することを容認していると考える余地もあり、そうだとすれば、被告人が与えた情報にも、システムで要求されていない申込みの主体に関する情報は含まれていない、とすることもできそうだからである。／しかし、一般にクレジットカード会社の約款では、会員がクレジットカードを他人に譲渡、貸与等することは禁止されており、オンラインによる取引においても、例外は認められていない。クレジットカードによる決済を行うオンライン取引は、クレジットカード会社と提携して行われるものであり、特別の事情がないかぎり、このようなクレジットカードの仕組みを踏まえたものと考えられる。そして、クレジットカードの所持人と名義人は原則として同一であり、

11)　藤井・前掲注 7）69〜71 頁。

カード面上に表示されるクレジットカード番号や有効期限等の情報を正しく入力することは当該カードを所持する名義人本人でなければ通常はできないものであり、本件システムは、このような事情を前提にしていると考えることができる。そうすると、取引の際にカード面上の情報以外に主体認証情報の入力を求めていないとしても、そのことから当該システムが名義人以外によるクレジットカードの使用を容認する趣旨とすることはできないと考えられる」。

「結局、本件システムはクレジットカードの名義人本人以外の者が利用することを予定しておらず、被告人による行為は、電子計算機に対して『クレジットカードの名義人本人が同カードによる決済で一定額分の電子マネーの購入を申し込んだ』とする情報を与えたものということができる」。

３　調査官解説の分析とそれまでの議論の再定位

平成 18 年最決の調査官解説では、「虚偽の情報」を与えたかどうかが、行為者がどのような「情報…を与え」たのかを規範的に確定した上で（「行為の意味付け」と呼ぶことにする）、それが「虚偽」であるのかを判断するという 2 ステップの判断枠組みが採用されている[12]（なお、実際には、まず本件で「虚偽の情報」が与えられているとしたらそれはどのような情報かを考え、次に、行為者が本当にそのような情報を与えたと評価できるのか（そのような解釈は可能なのか）を考えることになるものと思われる）。数字、文字列などのデータとその意味内容を区別して考えるとき[13]、本条にいう「情報」は、明らかに意味内容としてのそれである（意味内容であって初めてその真偽が観念できる）。そして、電算機詐欺罪の成立が問題になるような場面では、行為者が何らかのデータを入力するが、それがどのような意味を持つかは、当該データの処理の目的を参照することによってのみ確定することができる。この意味で、規範的な「行為の意味付け」を行うこと自体は妥当だと思われる。

このような「行為の意味付け」は、立案担当者解説には明示されていなかった。もっとも、立案担当者も、例えば、「無人店舗でサービスが提供された場合において、〔窃取した〕カードの正当な所持人たる預金者の口座から引き落とし

12)　藤井・前掲注 7）71 頁注 11。

13)　データと情報の区別につき、西貝吉晃「情報刑法―序説」太田勝造編著『AI 時代の法学入門―学際的アプローチ』250 頁（弘文堂、2020）。

た金額[14]を入金資金とする不実の記録…を作出することによって、販売店に対する代金支払を免れる点について、不実の記録に基づいて不法利得した」と評価することは想定していた[15]。平成 18 年最決が行った「行為の意味付け」は、そのように評価できる理由を言語化したものといえる。

一方、平成 5 年東京高判は、立案担当者が想定した事例の一つに関わるところ、「行為の意味付け」よりは、「経済的・資金的実体」に符合しているかという真偽の判定に重点を置いた判断を示している。もっとも、平成 18 年最決の調査官解説を踏まえたとき、次のように、前者に重点を置いて再構成することも可能であると思われる[16]。すなわち、信用金庫のオンラインシステムの取扱い上、入金等の操作は、その原因となる経済的・資金的実体に符合することが前提とされている。そのため、入金等の情報を入力する場合、その原因となる経済的・資金的実体に符合するものである旨の「情報…を与え」るものとの解釈がなされる。そして、当該事案では、入力された入金等は、その原因となる経済的・資金的実体に符合しないものであったから、前記情報は虚偽である、と。ここでは、平成 18 年最決が当てはめの中で行った「行為の意味付け」が、「虚偽の情報」の解釈においていわば先取りして行われたといえるが、信用金庫のオンラインシステムという、当該事案で問題となった情報システムの性質や仕組みが前提とされていることに留意すべきである。

Ⅲ　「虚偽の情報」の解釈・適用方法に関する試論

1　問題と基本的な方向性－重要事項性

問題は、平成 18 年最決の担当調査官が「残された問題」として認めるとおり、「『情報』としてどの範囲の事柄を取り込むか」であり[17]、本稿の表現によれば、どのような場合に「行為の意味付け」を行うことができるかである。

---

14)　銀行 POS システムという、現在のデビットカードに相当する（ただしキャッシュカードを利用する）取引が想定されている（米澤編・前掲注（1）126 頁〔的場〕）。

15)　米澤編・前掲注 1）126 頁〔的場〕。

16)　藤井・前掲注 7）71 頁注 11、渡邊卓也「電子計算機使用詐欺罪における『虚偽』性の判断」野村稔先生古稀祝賀 367～368 頁（2015）。

17)　藤井・前掲注 7）72～73 頁、73～74 頁注 13。

これについて、詐欺罪の解釈を参考に、重要事項に関する情報に限定する解釈が提案されている[18]。方向性としては妥当だと考えられるが、それによって直ちに前記の問題が解決するわけではない[19]。また、私見によれば、そもそも詐欺罪と電算機詐欺罪では、取引の構造（特に意思決定の内容や位置付け）が異なり、そのことを考慮したとき、詐欺罪の解釈を電算機詐欺罪にそのまま反映することは適切ではない[20]。そこで、次節以下では、①重要事項性をどこに位置付けるべきか（結論として、「行為の意味付け」の基準として位置付けるべきである）を検討した上で、②何を重要事項と評価すべきか（結論として、情報システムにおいて前提とされている事項とすべきである）を検討する。

２　重要事項性をどこに位置付けるか

詐欺罪においては、「人を欺〔く〕」の解釈として、「重要な事項」を偽ったことが要求される[21]。何らかの虚偽告知（＝偽ること）がされた場合に、それが重要事項に関するものであったかがテストされるのである。もっとも、詐欺罪においては、重要事項性は、別の場面でも作用することがある。すなわち、挙動による欺罔[22]の場面である。以下に詳述する。

暴力団関係者によるゴルフ場利用に関する平成 26 年 3 月 28 日の 2 つの判例[23]（以下この節においてそれぞれ「宮崎事件」「長野事件」という）の担当調査官（両事件で共通である）は、挙動による欺罔を、「その挙動の社会的意味の解釈によって事実を偽ったとみなされる場合」と説明し[24]、それは「取引における重要な内容であるため、当事者間でそれが存在することが当然であると意識しており、いわ

---

18) 研究者によるものとして、渡邊・前掲注 16）376 頁、和田・前掲注 8）100 頁、岡部天俊「判批」北大法学論集 69 巻 4 号 204 頁（2018）。法務省刑事局関係者によるものとして、鶴田六郎「判批」研修 532 号 20 頁（1992）（「本システムにとっては本質的な事項」）、井上宏「判批」研修 698 号 31 頁（2006）（ただし重要事項という語は用いない）。

19) 詐欺罪に関して佐伯仁志「詐欺罪（1）」法教 372 号 108 頁（2011）。

20) 橋爪・前掲注 10）4 頁、7 頁、渡邊・前掲注 16）361 頁、井上・前掲注 18）37 頁注 5。

21) 最決平成 22 年 7 月 29 日刑集 64 巻 5 号 829 頁。

22) 例えば、最決平成 19 年 7 月 17 日刑集 61 巻 5 号 521 頁（前田巌「判解」最判解刑事篇平成 19 年度 320 頁（2011）が明示する）、最決平成 22 年 7 月 29 日前掲注 21）（増田啓祐「判解」最判解刑事篇平成 22 年度 186 頁（2013）が明示する）、最決平成 26 年 3 月 28 日刑集 68 巻 3 号 646 頁（野原俊郎「判解」最判解刑事篇平成 26 年度 166 頁（2017）が明示する）。

23) 最判平成 26 年 3 月 28 日・前掲注 22）（宮崎事件）、最判平成 26 年 3 月 28 日刑集 68 巻 3 号 646 頁（長野事件）。

24) 野原俊郎「判解」最判解刑事篇平成 26 年度 138 頁（2017）。

ば『言葉にする必要がない』状況」において認められるとする[25]。ここでは、重要事項性が挙動による欺罔を認めるべきかどうかの基準とされている。

さらに、宮崎事件判決・長野事件決定は、関係する事情を検討した上、一方で**挙動による欺罔**を認めず無罪とし（宮崎事件）、他方で**挙動による欺罔**と**重要事項性**の双方を認めて有罪としている（長野事件）。これについて、調査官は、**挙動による欺罔**を認めるべきかどうかと**重要事項性**とでは「判断を基礎付ける事実関係に重なる部分があることが多い」ことを指摘している[26]。

電算機詐欺罪においてはどうか。同罪においては、先に述べたとおり、行為者が行ったデータ入力の意味は、当該データの処理の目的を参照して決せられる。この作業（本稿が「行為の意味付け」と呼んでいるもの）は、挙動による欺罔における「社会的意味の解釈」と同等である[27]。そうすると、詐欺罪において、挙動による欺罔を認めるかどうか（ある事項を補う「社会的意味の解釈」を認めるかどうか）の基準として重要事項性を位置付けることができるのと同様に、電算機詐欺罪においても、「行為の意味付け」を認めるかどうかの基準として重要事項性を位置付けることができると考えられる。

なお、電算機詐欺罪においては、重要事項性は、専ら「行為の意味付け」を認めるかどうかの基準として位置付ければ足り、例えば「当該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、重要な事項について、その内容が真実に反する情報」などと解釈し直す必要はないと考えられる。すなわち、挙動による欺罔の事案では、ある者が偽った事項が重要事項であるかどうかは、その者が何を偽ったかを明らかにしないことには判断できないため[28]、重要事項性の判断は、実質的に挙動による欺罔を認めるかどうかの判断に吸収されると考えられるところ、電算機詐欺罪においては、当該データの処理の目的を参照した「行為の意味付け」が常に行われる（だからこそ「当該システムにおいて予定されている事務処

25)　野原・前掲注 24）147 頁。
26)　野原・前掲注 24）173 頁。
27)　橋爪・前掲注 10）6 頁も、平成 16 年最決の事案を挙動による欺罔のアナロジーで説明する。
28)　野原・前掲注 24）173 頁は論理的な先後関係はないとするが（176 頁注 11）も参照）、論理的にはそうであっても、重要事項性の判断を先行させる場合、少なくとも不自然な判断とならざるを得ないように思われる。なお、最決平成 22 年 7 月 29 日・前掲注 21）は、挙動による欺罔を認めたものであるが、重要事項性を中心とする判示を行っており、野原の解説はそれとの整合性を意識したものである可能性がある。

理の目的」の参照が、特殊な場面での判断方法ではなく、虚偽性一般の判断方法として位置付けられていると考えられる[29]）、言い換えれば、いわば全事例が挙動による欺罔に相当するため、別に重要事項性を要求する必要はないと考えられる。

３　どのような場合に「行為の意味付け」を行うべきか―自動取引の構造に即して

では、どのような場合に重要事項性が認められるか。以下、自動取引の構造（特に意思決定の内容や位置付け）を対人取引と対比しつつ検討した上で、それに適合的な解釈を提案する。

まず、**詐欺罪**は、個別の取引に係る意思決定を、虚偽告知によって歪めることを規制するものである。では、どのような虚偽告知を対象とするのが合理的か。**対人取引**においては、虚偽告知時点では、意思決定は未だ行われておらず、取引者が多様な情報に反応する（＝そのような情報を基礎として意思決定をする）可能性が残されている。そのため、多様な情報についての虚偽告知を対象とするほかない。もっとも、それでは財産犯としての詐欺罪によって規制すべきとはいえないような事項についての虚偽告知も同罪の対象に含まれてしまう。そこで、重要事項性という要件の下で、当該取引者の意思決定を歪める（つまり意思決定の内容を異ならしめる）可能性があり、かつ、財産犯としての詐欺罪を発動する価値のあるような虚偽告知をスクリーニングするのである。

これに対して、**自動取引**においては、意思決定は、虚偽入力に先立つ情報システムの設計（パッケージ化されたシステムの導入の決定を含む）の時点で既に行われている。自動取引に使用される情報システムの設計に係る意思決定は、直接的には情報システムの機能、業務フロー等を決定するものであるが、同時に、取引一般を対象として、どのような条件が満たされたときに取引を行うかを決定するものでもある（これと対比すれば、対人取引においては、当該取引を行うかどうかについて意

29）藤井・前掲注 7）72 頁注 11 は、「何をもって電子計算機に与えられた『情報』ととらえるかによって、『虚偽』かどうかは自ずから決まってくる場合もあ」るとするが、平成 5 年東京高判・前掲注 5）のように、一見「情報」の内容が自明であり、「虚偽」かどうかが主たる問題となると思われた事例ですら、本文のように再構成できることからすれば、全てのケースは藤井の言うような場合に当たると言ってよいのではないか。なお、詐欺罪においても、挙動による欺罔の事例とそうでない（作為による詐欺の）事例の区別は相対的であり、あらゆる言動は多かれ少なかれそれが行われた状況を考慮して解釈されるが、それが顕著な場合に「挙動による欺罔を認めた」とのラベリングが行われるのだと思われる。

思決定がなされる）。もちろん自動取引においても個別の取引についての決定は行われるが、それは情報システムによる機械的・非意思的な決定であって、情報システムの設計時の意思決定の実現過程にすぎない。では、虚偽入力はなぜ規制されるのか。意思決定は既に行われているから、それを歪めるということはありえない。そうではなく、情報システムの設計時に行われた意思決定に反する態様で情報システムを操作し、情報システムの設計時の意思決定に反するような個別の取引に係る（機械的）決定を行わせるものだからと考えられる。詐欺罪に関して述べたところと対比すれば、**電算機詐欺罪**は、情報システムの設計時の意思に反する態様で情報システムを操作し、情報システムの設計時に行われた意思決定の実現過程に介入することを規制するものなのである（なお、電算機詐欺罪はしばしば詐欺罪の「補充類型」であることが強調されるが、体系的には盗取罪であり、利益窃盗を部分的に処罰するものであること[30]に留意すべきである）。

このような電算機詐欺罪における取引のメカニズム（特に意思決定の内容や位置付け）や、そこから導かれる虚偽入力を規制すべき理由に照らしたとき、電算機詐欺罪によって規制すべき虚偽入力を、詐欺罪における虚偽告知のように、ひとまず多様な情報についての虚偽入力とした上で、意思決定への影響や要保護性によって絞り込むことによって定義することは適切ではない。ではどうすべきか。自動取引においては、情報システムの設計に際して、多様な情報に反応する可能性が放棄され[31]、情報システムにおいて前提とされた事項に反応する（言い換えれば、そのような情報を基礎として機械的決定をする）可能性のみが留保されているといえる[32]。そうすると、電算機詐欺罪においては、情報システムにおいて前提

---

30)　山口厚『刑法各論』274 頁（有斐閣、第 2 版、2010）参照。

31)　情報システムの設計に係る意思決定には、（対人取引ではなく）自動取引によるとの意思決定も含まれるから、このような可能性は、単にもはや残されていないというにとどまらず、意思的に放棄されているのである。これに対して、何らかのチェックをしないことについて、顧客の利便性を考慮したのであって、放棄したのではないとの反論が考えられる（後掲の JR 東日本不正乗車事件における控訴審判決、近鉄不正乗車事件における控訴審判決参照）。しかし、顧客の利便性を考慮するのは、それが取引機会増加等の観点から合理的だからであるはずであり、放棄の動機に過ぎない。

32)　和田・前掲注 4）100 頁参照。なお、和田は、①重要事項性を基本的にはシステム管理者に置き換えて判断するが、②機械化したために判断対象外に置かれた事情は重要事項と評価しないとしているように見える。しかし、①のアナロジーが常に可能なわけではなく（例えばブロックチェーン上で行われる暗号資産の取引）、今後そのようなシステムはますます増えると思われる。

とされている事項が重要事項であり（このことは、自動取引においては意思決定が既になされている以上、重要事項性は、意思決定の産物である情報システムにおける当該事項の扱いから読み取るべきである[33]、とも言い換え可能である）、そのような事項であって初めて当該事項を補う「行為の意味付け」が許されると解するべきである[34]。そして、情報システムでチェックされている事項[35]はもちろん、それ以外の事項でも、データ入力に対する情報システム外の制約[36]、例えば法令による制約、規約（情報システムを操作する者に適用される社内規程、利用規約等）による制約、物理的制約を考慮して、その事項（の真実性）を前提として情報システムが構築されているような事項は、情報システムにおいて前提とされていると評価すべきである一方、そのような制約が存在しない事項や、そのような制約を考慮したとはいえない事項については、当該前提が存在しない場合に取引を行わないという可能性は放棄されたと言うべきであり、情報システムにおいて前提とされているとは評価すべきではない[37]。

以上の解釈は、平成 18 年最決が、情報システムがどのような事情を前提としていたかを問題としていたこと[38]と整合するほか、立案担当者が本罪を情報システムのセキュリティを補うものとして位置付けていたこと[39]と整合する。

---

33) 渡邊・前掲注 16）372 頁。渡邊は「何らかの者の具体的な『意思』を基準とすべきとの考え方自体に、充分な根拠があるとは思われない」（同）とするが、「本罪の成否が争われている『システムにおいて』予定されている客観的な制度趣旨に照らして、虚偽性を判断すべき」（同）、「虚偽性を判断するのは、あくまで人間」（374 頁）ともしており、後者の「客観的な制度趣旨」が何者かの意思決定の産物であることまで否定する趣旨ではないと思われる。

34) 「行為の意味付け」を行うべきか否かの基準をこのように定式化したとき、実は、重要事項という中間概念は不要となるともいえる。

35) チェックされているといっても、単に当該事項に係るデータが一定の条件を満たすかの判定がなされているといった意味であり、虚偽を発見できることまで意味するものではない。対人取引において、人は必ずしも虚偽を発見できず、そうだからこそ詐欺罪が必要とされるが、自動取引における情報システムも同じである（渡邊・前掲注 16）373〜374 頁を参照）。

36) この制約は、当該情報システムやそこに入力されるデータの取扱いに関するものでなければならず、単に当該入力によって債務不履行が可能になるとか、不当利得が生じるというだけでは足りないと考えるべきである。「虚偽の情報…を与えて」は、不法利得があったことを前提に、その手段をスクリーニングする要件であるから、不法利得があったことはその基準として機能しない。

37) 橋爪・前掲注 10）12 頁、渡邊・前掲注 16）372 頁、376 頁、和田俊憲「判批」法教 480 号 117 頁（2020）、井上・前掲注 18）31 頁、高嶋智光「判批」研修 778 号 21 頁（2013）。

38) 藤井・前掲注 7）70 頁（「本件システムは、このような事情を前提にしている」）。挙動による欺罔に関する野原・前掲注 24）147 頁の表現（「当事者間でそれが存在することが当然であると意識しており」）も同旨である。

39) 米澤編・前掲注 1）13 頁〔古田佑紀＝多谷千香子〕。

なお、以上の解釈は、「虚偽」という法文の文言とはいくらかの距離がある。アメリカ法（合衆国法典 18 章 1030 条(a)(4)）、ドイツ法（刑法 263 条 a 第 1 項）、サイバー犯罪条約（同条約 8 条）では、「コンピュータ詐欺」に相当するタイトルが使用されつつも、条文の文言としては「認可なしに」「権限なしに」といった表現が取られている。認可や権限の割当ては情報システムの設計者（・運用者）が行うものであるから、「虚偽」を以上のように解釈する場合、それはこれらの立法例における「認可なしに」「権限なしに」とほとんど同じ意味になると思われる。

Ⅳ　事例の検討[40]

Ⅲに述べた判断枠組みの下で、判例等に現れた事例の処理を検討する。先に事例と結論をまとめると、次のとおりである。

分野	事例の特徴	判例・文献	判例・文献の結論	本稿の結論
クレジットカード	他人名義・承諾なし	平成 18 年最決	○	○
	他人名義・承諾あり	平成 18 年最決調査官	—	○
	自己名義・支払意思なし	平成 18 年最決調査官	—	×
銀行	オンラインシステム不正操作	平成 5 年東京高判	○	○
	ATM・ネットバンキング―他人名義・承諾なし	裁判例（注 53）	○	○
	ATM・ネットバンキング―自己名義・誤振込み	令和 5 年山口地判	○	×
プリペイドカード	偽造プリペイドカード（ダイヤル Q2 事件）	裁判例（注 59）	○	○
	窃取・拾得プリペイドカード	立案担当者	×	×
	KDD 国際電話不正利用事件	裁判例（注 62）	○	○

40)　裁判例を概観するものとして、大塚仁ほか編『大コンメンタール刑法第 13 巻』184～187 頁（青林書院、第 3 版、2018）〔和田雅樹〕。

サービス不正利用	JR 東日本不正乗車事件	裁判例（注 65）	往路〇、復路〇	往路×、復路〇
	近鉄不正乗車事件	裁判例（注 66）	〇	×
	NEXCO 東日本不正利用事件	裁判例（注 70）	〇	〇
暗号資産	暗号資産移転	令和 4 年東京高判	〇	〇

1　クレジットカード関係[41)]

（1）他人名義・承諾なし事例

盗取・拾得した他人名義のクレジットカードを使用し、何らかのサービス（典型的にはオンラインサービスだが、これに限られない）を利用したり、サービスの利用に必要なポイントを購入したりする事例である。平成 18 年最決の類型であり[42)]、本罪の成立が認められてきている。

この類型では、クレジットカードについての物理的な制約・規約による制約から、クレジットカード番号、有効期限、セキュリティコードを入力できるのは名義人のみであり、したがって、それらを入力した者がクレジットカードの名義人であることがシステムにおいて前提とされている。

（2）他人名義・承諾あり事例

他人名義のクレジットカードを、当該他人の承諾の下使用し、何らかのサービスを利用したり、サービスの利用に必要なポイントを購入したりする事例である。平成 18 年最決の担当調査官が「残された問題」とする類型の一つである[43)]。

承諾の下に他人のクレジットカードを使用する事例の処理は、詐欺罪においても議論があるが[44)]、少なくとも自動取引においては、加盟店の黙認[45)]があり得

41)　クレジットカード取引の概観として小塚荘一郎＝森田果『支払決済法』180 頁以下（商事法務、第 3 版、2018）、宮居雅宣『決済サービスとキャッシュレス社会の本質』1 頁以下（きんざい、2020）。

42)　最決平成 18 年最決・前掲注 6）のほか、東京高判平成 31 年 2 月 8 日高刑速令和元年 110 頁（積極）。

43)　藤井・前掲注 7）73 頁、同注 12。「残された問題」とするものの一つである。

44)　多和田隆史「判解」最判解刑事篇平成 16 年度　82〜83 頁、86 頁注 11、12、13（2007）。なお、多和田が認めるとおり、このようなケースが実際に起訴されることは稀であると思われる。

45)　多和田・前掲注 44）82 頁。なお、同 86 頁注 11 は、「配偶者の場合は、クレジットカードの名義人とは性が異なることが一見して明らかな場合が多いから、加盟店は名義人本人でな

ない以上、平成 18 年最決と同様の「行為の意味付け」を認め、本罪の成立を認めてよいと思われる[46]。ただし、調査官が指摘するとおり、名義人の手足として評価できる場合は別であり[47]、そうでないとしても、実質的違法性阻却の余地があると考えられる[48]。

（3）自己名義・支払意思なし事例

自己名義のクレジットカードを使用し、決済資金の調達の見込みがないことを知りながら、何らかのサービスを利用したり、サービスの利用に必要なポイントを購入したりする事例である。平成 18 年最決の担当調査官が「残された問題」とする事例のもう一つである[49]。

決済資金の調達の見込みがないことを知りながらクレジットカードを使用する事例の処理は、詐欺罪においても議論があるが[50]、それについていずれの見解に立つとしても、少なくとも電算機詐欺罪は成立しないのではないかと思われる。すなわち、仮に対人取引において加盟店に支払意思（厳密には、決済資金の調達の見込みがないことの認識だと思われる）の確認の必要性が認められるとしても[51]、自動取引においてそれは不可能である。他人名義事例では、物理的な制約・規約による制約から、実質的に本人確認がされたと考えることが可能であったが、支払意思についてはそのような制約は存在せず、支払意思があることが前提とされているとはいえない。したがって、クレジットカード番号等を入力することに、支払能力を有する旨の情報を与えたとの「行為の意味付け」をすることはできず、本罪は成立しないと解するべきである。

いことを認識した上で、使用を許することになる場合が多い」とするが、加盟店の多くは名義の確認を行っていないと思われる。

46) このように解した場合、家事従事者等がクレジットカード取引から排除されてしまうが、クレジットカード取引が信用供与の面を有する以上、やむを得ない。そのような人々を排除することによる機会損失がそれによって回避できるリスクを上回ると考えるイシュアは、家事従事者等を対象としたサービスを提供するであろうし、そのようなサービスは「家族カード」などとして現に提供されている。

47) 藤井・前掲注 7）73 頁注 12。

48) 多和田・前掲注 44）83 頁。

49) 藤井・前掲注 7）73 頁、同注 13。「残された問題」とするものの一つ。

50) 山口・前掲注 30）264 頁以下。

51) ただし、加盟店は貸倒れリスク・審査コストを免れる対価として手数料を支払っていることからすれば、このような確認義務を課すことには合理性がなく、実際に一般的なアクワイアラの加盟店規約においてもそのような義務を課している例は見当たらない以上、専ら詐欺罪に問うためだけに信義則上の義務を措定することは、適切ではないと思われる。

なお、このことは、結論の妥当性の観点からも支持可能だと思われる。すなわち、クレジットカードのイシュアは利用限度額の範囲内で包括的に貸し倒れリスクを取り、その対価として加盟店から手数料を得ているのだから、そのリスクの現実化は、単なる債務不履行と変わるところがないと思われる。

2　銀行関係

（1）オンラインシステム不正操作事例[52]

銀行のオンラインシステムにおいて、自己の管理する口座への振込みの事実がないのに、それがあったとする操作をする（より端的に言えば、自己の口座残高を水増しする）事例である。平成 5 年東京高判の類型であり、本罪の成立が認められている。

この類型では、振込みの操作に係る物理的制約（端末に接触する必要性から、操作できる人間は限られる）、社内規程等による制約から、システムにおいて、振込みに係る操作はその原因となる経済的・資金的実体に符合してなされることが前提とされていたといえる。そこで、II に述べたとおり、振込みに係る操作に、その原因となる経済的・資金的実体に符合するものであるとの「行為の意味付け」がなされ、それは虚偽であるから、本罪が成立する。

（2）ATM・ネットバンキング―他人名義・承諾なし事例

盗取等に係る他人名義のキャッシュカードを使用し、ATM を利用して当該他人名義の口座から自己の管理する口座への振り込みを行う事例である。裁判例において本罪の成立が認められており[53]、いわゆる還付金詐欺もこの類型として処理されている[54]。

平成 18 年最決と同様、キャッシュカード・暗証番号についての物理的な制約・規約による制約から、キャッシュカードを挿入し暗証番号を入力できるのは名義人のみであり、それらを挿入・入力した者がクレジットカードの名義人である

---

52)　平成 5 年東京高判・前掲注 5）のほか、大阪地判昭和 63 年 10 月 7 日判時 1295 号 151 頁、東京地八王子支判平成 2 年 4 月 23 日判時 1351 号 158 頁、名古屋地判平成 9 年 1 月 10 日判時 1627 号 158 頁（いずれも積極）。

53)　東京高判平成 31 年 3 月 15 日裁判所 Web サイト（LEX/DB 25570207）。

54)　例えば大阪高判平成 28 年 7 月 13 日高刑速平成 28 年 195 頁。処分行為なしとして電算機詐欺罪の間接正犯として処理されているようである。間接正犯がありうることは、立案担当者も認めていた（米澤編・前掲注 1）123、137 頁〔的場〕）。

ことが前提とされているといえる。そこで、それらの挿入・入力に、自らが名義人である旨の情報を与えたとの「行為の意味付け」がなされ、それは虚偽であるから、本罪が成立する。

なお、ATM ではなくネットバンキングサービスを使用する場合も、パスワード（やワンタイムパスワード）についての物理的な制約・規約による制約から、同様に処理できると思われる。

(3) ATM・ネットバンキング―自己名義・誤振込み事例

自己の口座に誤振込みがされた（かつ当初残高等から誤振込みに係る部分が区別可能である）場合に、ATM やネットバンキングを利用して自己の管理する他の口座にその金額を振り込んだり、デビットカードを利用して、その金額をもって何らかのサービスを利用したり、サービスの利用に必要なポイントを購入したりするための支払いをしたりする事例である。令和 5 年山口地判の類型であり、同判決は本罪の成立を認めた。

この類型では、対人取引における誤振込みに関する判例[55]（以下この節において「平成 15 年最決」という）を電算機詐欺罪にも応用できるかが問題となるが、不作為による欺罔は、告知義務が履行されていれば被欺罔者が財物を交付しなかったであろうといえることが前提であり（III に述べたとおり、対人取引では多様な情報に反応する可能性が残されており、それゆえに告知義務が認められる）、自動取引においてはそのような可能性は放棄されているのであるから、告知義務が認められない（なお、これを敷衍すれば、およそ不作為による欺罔のアナロジーで「不作為による虚偽の情報の付与」を認めることはできないとも考えられる）。したがって、誤振込に係る金額ではない旨の情報を与えたとの「行為の意味付け」をすることはできず、本罪は成立しないと考えられる。

これに対し、令和 5 年山口地判は、「誤って受取人口座に振り込まれた金銭についてどのように処理をするのが相当かを早期に検討」するためには「受取人口座に誤って振り込まれた金銭について、その原因行為の有無等につき受取人がどのように認識しているのかをなるべく早期に被仕向銀行が知る必要がある」との告知義務を認めているが、その根拠が明らかではない（この告知義務は平成 15 年最決が認めた告知義務とは別物である）。また、告知義務が認められることは「被仕

55)　最決平成 15 年 3 月 12 日刑集 57 巻 3 号 322 頁。

向銀行の窓口で取引する場合であろうと、インターネットを通じて電子計算機に情報を入力して取引する場合であろうと変わりはない」とするが、その根拠も明らかではない。

令和 5 年山口地判以前にも、例えば橋爪隆は、本罪の成立を認めるべきことを説いていた[56]。しかし、この見解は、電算機詐欺罪における「行為の意味付け」が、（不作為による欺罔ではなく）挙動による欺罔における社会的意味の解釈に相当する作業であることを看過しているように思われる。橋爪自身も、平成 15 年最決が、挙動による欺罔ではなく不作為による欺罔を問題にしたこと自体は正当だったとする一方[57]、平成 18 年最決を挙動による欺罔のアナロジーで説明しているところ[58]、III に述べたとおり、電算機詐欺罪は後者に相当する。

3　プリペイドカード関係

（1）偽造プリペイドカード事例（ダイヤル Q2 事件）

ダイヤル Q2 は、NTT が提供していた情報料回収サービスである。情報提供者は NTT と契約し、代金の回収を委託し、ダイヤル Q2 用の番号の割当てを受ける。利用者は、ダイヤル Q2 用の番号に電話をかけ、一定のコンテンツ（投資顧問、性的コンテンツ等）を聞く。情報料は、固定電話等からの利用の場合、NTT が後日発信元の番号の契約者に通話料金とともに請求し、公衆電話からの利用の場合、テレホンカード（磁気式のプリペイドカードであり、最大 5000 円相当であった）の残高から回収した。被告人らは、使用済みテレホンカードの残高を改ざんし、それを使用して公衆電話から自己のダイヤル Q2 用の番号に電話をかけ、NTT に変造に係る残高相当額を振り込ませようとした（未遂）。平成 4 年の岡山地裁は、この事案について電算機詐欺未遂罪の成立を認めた[59]。

この事例では、法令（支払用カード電磁的記録に関する罪、同罪新設前は私電磁的記録に関する罪）による制約から、テレホンカードは偽造のものではないことが前提とされているといえる。そのため、テレホンカードの挿入には、それが偽造のも

---

56) 橋爪隆「誤振込みと電子計算機使用詐欺罪」法教 504 号 1 頁（2022）、橋爪隆「銀行預金に関連する財産犯について」法教 440 号 108 頁（2016）。

57) 橋爪・前掲注 56）106 頁。

58) 注 27）参照。

59) 岡山地判平成 4 年 8 月 4 日公刊物未登載（鶴田・前掲注 18）13 頁に詳しい）。パッキーカード事件（長野地諏訪支判平成 8 年 7 月 5 日判時 1595 号 154 頁）も同様に処理できる。

のではない旨の情報を与えたとの「行為の意味付け」がなされ、それは虚偽であるから、本罪の成立を認めることができると考えられる。

（2）窃取・拾得プリペイドカード事例

窃取または習得したプリペイドカードを使用し、何らかのサービスを利用するといった事例である。立案担当者は、この類型について、前記の偽造プリペイドカード事例と区別して、本罪が成立しないとしていた[60]。

プリペイドカードは、例えばクレジットカードと異なり、まさにプリペイド（前払式）であるがゆえに、（サービス提供の対価として）プリペイドカードを受け入れる事業者は、そのプリペイドカードがどのようにして入手されたかに関心を払う必要がない。そのため、プリペイドカードを受け入れるシステムにおいて、プリペイドカードが適法に入手されたものであることが前提とされているとはいえない[61]。したがって、カードの挿入には、それが窃取・拾得に係るカードでない旨の情報を与えた旨の情報を与えたとの「行為の意味付け」をすることはできず、本罪は成立しないと考えられる。

これに対して、当該カードが偽造されたという属性と、窃取または拾得されたという属性は、情報システムによりチェックされないという点で共通の処理がなされており、電算機詐欺罪との関係でも同様に扱うべきではないかとの疑問が生じうる。しかし、当該カードが偽造されたものでないかがチェックされないのは、法令による制約を前提としているためであるのに対し、窃取または拾得されたものでないかがチェックされないのは、対価回収の仕組み上カードが窃取・拾得に係るものであるかどうかに情報システムの設計者が関心を有しないためであって、法令（例えば窃盗罪、占有離脱物横領罪など）による制約を前提としているためではないという点で、両者は区別できると思われる。

4　サービス不正利用関係

（1）KDD 国際電話不正利用事件

KDD の国際電話サービスの利用代金を免れた事例である。手順は、(a) KDD の交換システムに IODC サービス（着払いとなる接続方式）の利用を意味する番号

60)　米澤編・前掲注 1）125 頁〔的場〕。

61)　鶴田・前掲注 18）20 頁。前掲岡山地判平成 4 年 8 月 4 日も、偽造プリペイドカードにつき本罪の成立を認めるにあたって、代金回収との関連性を指摘する（鶴田・前掲注 18）20 頁）。

を入力する、(b) IODC サービスに対応した国（スペイン）の交換システムに接続する、(c) スペインの交換システムに接続キャンセルの信号（本来 KDD から送信される）を送信／着信国（ドイツ）への自動電話（IODC とは別の接続方式で、発払いとなる）を送信する、(d) スペインの交換システムから KDD の交換システムに送信されるキャンセルを確認する信号が中断されるとともに、ドイツの着信者に接続されるというものである（簡略化した）。この結果、KDD では着払いと認識され、スペインでは自国は単なる経由国と認識され、ドイツでは発払いと認識されるため、いずれの電話会社からも請求がなされないこととなる。平成 7 年の東京地裁は、この事案について、本罪の成立を認めた[62]。

この事例では、着払いか発払いかは端的にシステムによりチェックされているから、その真実性が前提とされているといえる。そのため、被告人の行為（(a)と(c)を併せて評価すべきだと思われる[63]）は、着払いとなるべき通話である旨の情報を与えたとの「行為の意味付け」なされる。実際には、IODC サービスによる接続がキャンセルされている以上、発払いとなるべき通話であるから、前記情報は虚偽であり、本罪が成立する。

（2）JR 東日本不正乗車事件[64]

JR 東日本上野駅―宇都宮駅間（往路）、宇都宮駅―渋谷駅間（復路）におけるキセル乗車の事例である（簡略化した）。被告人は、**往路**では、上野駅から 130 円区間の乗車券で入場し、雀宮駅―岡本駅間（上野駅から見て、各駅は雀宮駅―宇都宮駅―岡本駅の順で並んでいる）の回数券で出場した。出場時、回数券には入場記録が

---

62) 東京地判平成 7 年 2 月 13 日判時 1529 号 158 頁。事案は小川新二「判批」警察公論 50 巻 11 号 124 頁以下（1995）に詳しい。

63) 小川・前掲注 62）124 頁、芝原邦爾「判批」別ジュリ 167 号（刑法判例百選 II 第 5 版）109 頁（2003）。判決は(a)のみで構成するが（「〔IODC〕サービスを利用するためでなく、単に、本件電話回線を IODC 対地国の電話交換システムに接続させることのみを目的とする」点で虚偽）、内心を問題とすることはクレジットカード・支払意思なし事例と同様の問題を生じさせる。

64) 本件及び後掲の近鉄に係る事件は、いわゆる供用型として処理されたが、「不実の電磁的記録」の不実性は「虚偽の情報」の虚偽性と同様に判断される。なお、「財産権の得喪、変更に係る電磁的記録には、オンライン化された銀行の元帳ファイルのような備付型のものと、プリペイドカードのような携帯型のものとがあり、これに応じて不正行為の態様も異なることから」作出型と供用型が区別されたが（米澤編・前掲注 1）117 頁〔的場〕）、この区別は必然的なものではないし（渡邊・前掲注 16）365 頁）、今後モバイルデバイスを利用した支払いが普及することに伴って、相対的に改ざんが容易な「携帯型」の利用はなくなっていくと思われる。

なかったが、当該区間の回数券は、岡本駅が自動改札未設置駅であったため、入場記録がなくても自動改札から出場できるようになっていた。**復路**では、宇都宮駅から 190 円区間の乗車券で入場し、渋谷駅では、前記 130 円区間の乗車券と、乗車料金との差額 60 円を精算機に投入し、精算券を発行させ、この精算券を使用して出場した。前記 130 円区間の乗車券は、入場から長時間が経過していたため、自動改札から出場することはできないようになっていたが、精算機ではそのような制限がされていなかった。平成 24 年の東京高裁は、この事案について、往路・復路のいずれについても本罪の成立を認めた[65]。

この事案では、**往路**については、回数券の入場記録（そもそも記録されていなかった）は宇都宮駅のシステム（改札機）によりチェックされていない。システム外の制約を考慮しても、岡本駅（を含む当該区間の自動改札未設置駅。以下同じ）から入場した者でなければ雀宮駅―岡本駅間の回数券を所持・使用し得なくするような制約は存在していないから、当該区間の回数券を投入する者は岡本駅から入場したことが前提とされているとはいえない。したがって、当該区間の回数券を投入することに、岡本駅から入場した旨の情報を与えたとの「行為の意味付け」をすることはできず、本罪は成立しないと考えられる。

復路については、130 円区間の乗車券の入場記録が渋谷駅のシステム（精算機）によりチェックされているから、乗車券を投入した者は入場記録どおりの駅から乗車したことが前提とされているといえる。そのため、上野駅の入場記録が記録された乗車券（この点が往路及び近鉄の事例と異なる）を投入する行為には、上野駅から入場した旨の情報を与えたとの「行為の意味付け」がなされる。被告人は実際には宇都宮駅から入場していたから、前記情報は虚偽であり、本罪が成立すると考えられる。

これに対し、判決は、**往路**について、①「下車駅である宇都宮駅においては、回数券の有効区間内に自動改札機未設置駅がある場合、同駅から乗車した旅客の利便性を考慮し、入場情報がなくても出場を許している」が、これは、②「下車の際に自動改札機に投入された回数券の磁気部分に入場情報のエンコードがないことが有効区間内にある自動改札機未設置駅における入場情報に代わるものとして扱」っているためであり、③「この自動改札システムの目的、機能に照

65)　東京高判平成 24 年 10 月 30 日高刑速平成 24 年 146 頁。

らせば、入場情報のない別表記載の回数券を宇都宮駅の自動改札機に投入する行為は、同自動改札機に対し、当該回数券を投入した旅客がその有効区間内にある自動改札機未設置駅（岡本駅）から入場したとの入場情報を読み取らせるという意味を有して」いるとし、「虚偽の情報」を与えたことを認めた。③のような「行為の意味付け」を行うことができるかどうかが問題であるが、本稿の立場によれば、①の取扱い自体は②のような事情によるものだとしても、②がシステム外の制約によって確保されているとはいえない以上、②がシステムにおいて前提とされているとはいえず（いわば①の取扱いを承認した者の意思において前提とされていたにすぎない）、③のような「行為の意味付け」を行うことはできないと考えられる。

一方、**復路**については、判決は、「下車駅の自動精算機の事務処理システムは、投入された乗車券にエンコードされた入場情報により乗車した駅を確認し、下車駅との間の乗車区間を把握した上、精算の要否を判定、演算するものであり、かつ、その入場情報は精算を行う駅における出場に対応する乗車に係る入場情報であることが当然の前提となっている」ところ、「被告人…が…渋谷駅で自動精算機に投入した乗車券には、…上野駅における入場情報がエンコードされており、それは被告人…の出場に対応する乗車に係る実際の入場駅である宇都宮駅とは異なる点で虚偽のものである」とし、「虚偽の情報」を与えたことを認めた。ここでもそのような「行為の意味付け」を行うことができるかどうかが問題であるが、判決がいう「当然の前提」は、システムにおいても前提とされているといえるから、判決の結論は正当だと考えられる。

（3）近鉄不正乗車事件

近鉄名古屋駅―松阪駅間におけるキセル乗車の事例である。150 円区間の乗車券で入場し、近鉄高田本山駅―松阪駅間の磁気定期券または JR 東海多気駅―松阪駅間（松阪駅は近鉄と JR 東海の共同使用駅である）の磁気定期券で出場した。磁気定期券には入場記録がないが、当該両区間の磁気定期券は、周囲に無人駅が多かったため、入場記録がなくても自動改札から出場できるようになっていた。令和 2 年の名古屋地裁は本罪の成立を認めなかったが、同年の名古屋高裁は原判決を破棄し、本罪の成立を認めた[66]。

---

[66] 名古屋地判令和 2 年 3 月 19 日判時 2529 号 117 頁、名古屋高判令和 2 年 11 月 5 日高刑速令和 2 年 522 頁。

しかし、JR 東日本事件の**往路**と同様に、入場記録がシステムによりチェックされておらず、定期券の有効区間内の駅から入場した者でなければ当該定期券を所持・使用しえなくするような制約は存在していないから、当該定期券を使用して出場する者は当該区間内の駅から入場したことが前提とされているとはいえない。したがって、当該定期券を使用して出場することに、当該区間内の駅から入場した旨の情報を与えたとの「行為の意味付け」をすることはできず、本罪は成立しないと考えられる。

紙幅の関係上具体的に紹介することができないが、一審判決は、情報システムによりチェックされているかどうかのみを検討して「行為の意味付け」を否定したものであり、この点で不十分であるが[67]、控訴審判決は、情報システムにおいて何が前提とされているかを検討することなく（控訴審判決の表現によれば、「本件自動改札機の事務処理の現状」を無視して）結論を導いており、結果として情報システムにおいて前提とされていない事項について「行為の意味付け」を行っており、この点で過剰であると思われる。控訴審判決は、「本件自動改札機が入場情報を判定対象としていないからといって旅客がどのような乗車をしたかの判断を〔近鉄〕が放棄したものでない」旨述べるが、そのように言える理由があるといえるかどうかが問題であり、結論として、（積極的に望んでではないにせよ）そのような判断を行う機会を放棄していたと言わざるを得ない[68]。控訴審判決のこの記述は、平成 18 年最決の調査官解説の「名義人以外によるクレジットカードの使用を容認する趣旨とすることはできない」[69]との表現の影響を受けている可能性があるが、平成 18 年最決の事案では、カードに係る物理的制約・規約による制約を前提として情報システムが構築されていたという違いがあることに留意すべきである。

---

67)　一審判決は、事務処理の目的と情報システムの機能を混同していると思われる。両者は「事務処理の目的を実現するために情報システムの機能が定義される」という関係にある。情報システムの機能は基本的に事務処理の目的に適合するように定義されるのが通常であるのに対し、情報システムは事務処理の手段の一つにすぎず、それのみで事務処理の目的を実現できるようにはなっていない（さらに言えば、他の要素、言い換えれば情報システム外の制約と組み合わせてもなお事務処理の目的を完全には実現できるようになっていない）のがむしろ通常である。

68)　注 31）参照。

69)　藤井・前掲注 7）70 頁。

（4）NEXCO 東日本不正利用事件

高速道路の利用料金を一部免れた事例である。ETC を利用する料金所のシステムにおいては、高速道路流入時の接地車軸数によって車種区分が認識され、料金が決定されている。また、近時のトレーラーには、積載量が小さい場合に、自動で一部の車輪を持ち上げ、当該車輪を使わないこととする機能が備わっているものがある（リフトアクスル）。被告人の使用していた車両のリフトアクスルは、「下降」「自動」の 2 つのモードを持ち、「自動」にセットした場合、一度車軸が上昇し、その後積載量に応じて下降するようになっていた。被告人は、高速道路の流入料金所直前で「自動」にセットすることにより、車軸の一つを一時的に上昇させ、「特大車」（4 車軸）に該当する車両を「大型車」（3 車軸）と認識させ、通行料金の一部を免れた。平成 27 年の横浜地裁は、本罪の成立を認めた[70]。

この事例では、車軸数に関する法令（道路法 47 条 1 項に基づく車両制限令 3 条 1 項 2 号ロ～ニ）の制約から[71]、3 車軸で流入した車両は、法令上 3 車軸で走行可能な状態である（したがって一定以下の積載量である）ことがシステムにおいて前提とされているといえる。そのため、3 車軸の車両で流入することには、当該車両が 3 車軸で走行可能な状態である旨の情報を与えたとの「行為の意味付け」がなされ、それは虚偽であるから[72]、本罪が成立すると考えられる。

---

70) 横浜地判平成 27 年 6 月 9 日裁判所 Web サイト（LEX/DB 25447348）。事案は岩田聡「リフトアクスルトレーラと ETC システムを悪用した高速道路不正通行事件の解」月刊交通 2016 年 4 月号 44 頁以下（2016）に詳しい。

71) なお、車軸数に依拠した定義は、「東日本高速道路株式会社供用約款」2 条が参照する「料金の額及びその徴収期間」（道路整備特別措置法 23 条の規制を受け、同法 25 条 1 項により公告される）において採用されている。例えば積載量が基準であり、その代理変数として車軸数が測定の対象となっているわけではない。
「東日本高速道路株式会社供用約款」
<https://www.e-nexco.co.jp/company/law_ordinance/covnants/east_stipulation.html>（2023 年 6 月 30 日最終アクセス）
「料金の額及びその徴収期間」
<https://www.e-nexco.co.jp/assets/pdf/company/law_ordinance/120420business_license/fee.pdf>（2023 年 6 月 30 日最終アクセス）

72) 判決はどのような「情報」が与えられ、それがどのような点で真実に反するのかを明示しないが、通行中「積荷に変動はなかった」ことや、「上記流入料金所を通過した時点において、その後の各通行区間を後前軸が上昇した 3 車軸の状態で通行することができないものであった」ことに言及している。

５　暗号資産移転事例

（1）概要

暗号資産の秘密鍵をサイバー攻撃や暴行・脅迫などにより入手し、これを利用して当該暗号資産を他のアドレスに移転する事例である。令和 4 年東京高判の類型である[73]。

2018 年、暗号資産交換所 Coincheck に対しサイバー攻撃が行われ、Coincheck が保有する暗号資産 NEM のほぼ全部、約 580 億円相当が外部に移転される事態が生じた（Coincheck 事件）[74]。攻撃者はインターネット[75]上に交換所を開設し、入手した NEM を他の暗号資産に交換した（攻撃者はディスカウントしたレートで交換を行った。これにより、攻撃者はロンダリングができ、交換に応じた者は安価に NEM を入手できる）。警視庁は、攻撃者について電算機詐欺罪、交換に応じた者について犯罪収益等収受罪（組織犯罪処罰法 11 条）の疑いで捜査し、攻撃者の摘発には至らなかった[76]一方、交換者 31 人を摘発した[77]。そのうちの一人に関するのが本件であり、被告人が「収受」したものが「犯罪収益」であるといえるかの前提として、攻撃者の行為が電算機詐欺罪に該当するかが問題となった。判決は、結論として電算機詐欺罪に該当することを認めた。

---

73)　暴行の事例として、名古屋高判令和元年 5 月 23 日裁判所 Web サイト（LEX/DB 25570279）がある。ただし、暗号資産交換所を利用していた個人から、交換所における ID・パスワードが書かれたノートを奪取した事例であり、秘密鍵を奪取した事例ではない。

74)　「コインチェックの仮想通貨不正流出、過去最大 580 億円―日本経済新聞」<https://www.nikkei.com/article/DGXMZO26231090X20C18A1MM8000/>（2023 年 6 月 30 日最終アクセス）

75)　交換所はダークウェブ上に開設された。ダークウェブとは、インターネットの一部であるが、通常のブラウザからはアクセスできない領域である（もっとも、アクセスに必要なツールは一般に入手可能である）。

76)　国連安保理専門家パネルは、2019 年 3 月の報告書（S/2019/171）において、ロシアのセキュリティ会社の分析に依拠し、北朝鮮の組織的犯行としたが（para 117, Annex 39）、同年 8 月の報告書（S/2019/691）においては、該当する記述を削除した。

77)　「流出の仮想通貨 NEM、不正交換疑い 31 人摘発　188 億円分: 日本経済新聞」<https://www.nikkei.com/article/DGXZQODG21EFZ0R20C21A1000000/>（2023 年 6 月 30 日最終アクセス）

（2）暗号資産の仕組み

暗号資産の設計を最初に示したのは、Satoshi Nakamoto の 2008 年の論文[78]である。同論文は、①デジタル署名を用いて、②銀行などの信頼できる第三者を必要とせず、③二重払いを防ぐ仕組みを提案するものである[79]。

デジタル署名とは、メッセージの送信者の本人性及びその内容の真正性（改ざんがなされていないこと）を確認するための[80]、公開鍵暗号方式[81]を応用した技術的な仕組みである。具体的には、①メッセージの送信者はメッセージをハッシュ関数にかけてダイジェストを生成する[82]、②送信者はダイジェストと秘密鍵（署名生成鍵[83]）からデジタル署名を生成する、③送信者はメッセージ・電子証明書（秘密鍵とペアとなる公開鍵が含まれている）、デジタル署名を合わせて送信する、④受信者は受領したデジタル署名を公開鍵（署名検証鍵[84]）により検証し、本人性を確認する、⑤受信者は受領したメッセージをハッシュ関数にかけてダイジェストを

78) Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at https://bitcoin.org/bitcoin.pdf（2023 年 6 月 30 日最終アクセス）

79) Nakamoto・前傾注 78）。Abstract に簡潔にまとめられている。

80) 逆に言えば、デジタル署名によっては、メッセージの改ざんや窃取（盗み見）を防止したり、窃取がなされていないかを確認したり、改ざんされた場合にどの箇所がどのように改ざんされたかを確認することはできない。

81) 公開鍵暗号方式は、暗号化方式の一種であり、共通鍵暗号方式（秘密鍵暗号方式とおも呼ばれる）と対比される。公開鍵暗号方式を使用したメッセージのやり取りは、①メッセージの受信者が、秘密鍵（一定の長さのランダムな文字列である。）をもとに公開鍵（同前）を生成し、送信者に公開鍵を送信し、②送信者が、受領した公開鍵を使ってメッセージを暗号化し、受信者にその暗号化されたメッセージを送信し、③受信者が秘密鍵を使用して暗号化されたメッセージを復号する、という流れで行われる。暗号化と復号を別の（しかし対応関係にある）鍵で行うことに特徴があり、暗号化に使用する鍵が流出しても問題が生じないため（そのため公開鍵と呼ばれる）、鍵のやり取りの安全性が保証されない環境でも安全にメッセージのやり取りができる。

82) ハッシュ関数は、任意の長さの文字列（キーと呼ばれる）を一定の長さの文字列（ハッシュ値と呼ばれる）に変換する関数である。ハッシュ値は人間でも扱いやすいような短い長さに設定されるため、ダイジェストと呼ばれることがある。ハッシュ値からキーを推測することはできないが、同じキーを入力すれば同じハッシュ値が得られ、異なるキーを入力すれば（全く）異なるハッシュ値が得られるため、データが改ざんされていないかの検証に使用される。

83) 秘密鍵と署名生成鍵は同じ性質のものであるが、暗号化（復号）に使用する場合には秘密鍵、デジタル署名（署名の生成）に使用する場合には署名生成鍵と呼ばれることがある。

84) 公開鍵と署名検証鍵は同じ性質のものであるが、暗号化に使用する場合には公開鍵、デジタル署名（署名の検証）に使用する場合には署名検証鍵と呼ばれることがある。

生成し、これとデジタル署名を照合し、真正性を確認する、ということが行われる[85]。

デジタル署名が機能するためには、秘密鍵が秘密に保たれていることが必要であるが、これについて、Satoshi 論文は何ら手当てを加えていない[86]。Satoshi 論文が提案するのは、信頼できる第三者がいない状況下でデジタル署名の検証結果を合意するためのアルゴリズムにすぎず、デジタル署名の信頼性は前提とされている。NEM においては、Satoshi 論文が提案したものとは異なるアルゴリズムが採用されているが、やはりデジタル署名の信頼性（秘密鍵の漏洩等が生じていないこと）は前提とされている。

そうすると、秘密鍵の秘密保持は、一般的な（≒暗号資産に特殊ではない）手段によって行うほかない。その例として、現在では、アカウントの分散（特定の秘密鍵の漏洩等の影響範囲が小さくなる）、秘密鍵のオフライン管理[87]（ネットワーク経由の攻撃に強くなる）、送金等のトランザクションの実行に複数の秘密鍵を要求すること[88]（1 つの秘密鍵の漏えい等の影響が小さくなる）などが行われているが、Coincheck 事件ではいずれも行われていなかった[89]。

（3）秘密鍵を知る者と別に「保有者」を観念できるか

上記の暗号資産の仕組みからすると、暗号資産に係る情報システムにおいては、「秘密鍵を知る者＝暗号資産の保有者」として扱われているといえる。ここ

---

85)　以上につき、齋藤孝道『マスタリング TCP/IP 情報セキュリティ編』99 頁（オーム社、第 2 版、2022）。Web 上でアクセス可能かつ平易な説明として、「電子署名の仕組み｜一般財団法人　日本情報経済社会推進協会」<https://www.jipdec.or.jp/project/research/why-e-signature/PKI-crypto-mechanism.html>（2023 年 6 月 30 日最終アクセス）

86)　例えば山澤昌夫ほか「暗号資産（ビットコイン）・ブロックチェーンの高信頼化へ向けての MELT-UP 活動（II）―運用と倫理―」コンピュータセキュリティシンポジウム 2018 論文集 870 頁（2018）、岩下直行「暗号資産への脅威と対策―ビットコインの社会への展開による変質―」デジタルプラクティス 10 巻 3 号 441 頁（2019）、島岡政基ほか「暗号資産交換所のカストディリスクと鍵管理」情報処理学会論文誌ジャーナル 9 号 1364 頁（2020）。

87)　コールドウォレットと呼ばれる。

88)　マルチシグと呼ばれる。

89)　現在、暗号資産交換業者は登録制となり、顧客の暗号資産と自己の暗号資産の分別管理、保有額の 5%を超える暗号資産のコールドウォレット管理が義務付けられているが（資金決済法 63 条の 2、63 条の 11 第 2 項、交換業府令 27 条）、登録制は事件当時完全には施行されておらず（平成 28 年法改正により導入後、経過規定により未登録業者の業務継続が許されていた）、コールドウォレットは義務化されていなかった（令和 2 年交換業府令改正により導入）。

から、秘密鍵を知る者と別に暗号資産の「保有者」を観念できるかという疑問が生じる（観念できなければ、「保有者以外の者」が秘密鍵を入力するという事態は生じえないから、秘密鍵を入力することが「虚偽の情報」を与えたと評価されることはありえないことになる）。しかし、そもそも仮想通貨・暗号資産は通貨・資産として設計されている以上、支配可能（他者を排除可能）である必要があり、デジタル署名はそのための手段として採用されている。そうすると、一応、秘密鍵を知る者と別に暗号資産の「保有者」を観念することはできると考えられる。

（4）秘密鍵は「保有者」でなければ入力できないことが前提とされているか

以上を前提に、秘密鍵の入力に自らが保有者である旨の情報を与えたとの「行為の意味付け」をすることができるかを検討すると、次のとおりである。

確かに、暗号資産に係る情報システムそれ自体は、デジタル署名の信頼性をチェックする仕組みを持たない。しかし、デジタル署名は、トランザクションを入力した者が暗号資産の「保有者」であることを確認するための手段として用いられており、暗号資産の仕組みが全体として暗号資産の「保有者」に秘密鍵を秘密に保つ（ための物理的、技術的制約を設ける）インセンティブを付与していることを考慮すれば、暗号資産に係る情報システムは、秘密鍵は「保有者」でなければ入力できないことを前提としているといえる。したがって、秘密鍵の入力に自らが保有者である旨の情報を与えたとの「行為の意味付け」をすることができる。

（5）判決について

紙幅の関係上具体的に紹介することができないが、令和 4 年東京高判は、「金融実務等における『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ような情報をいうと解される」という平成 5 年東京高判の規範の下で、「氏名不詳者は、コインチェック社が管理する NEM アドレスから氏名不詳者らが管理する NEM アドレスに暗号資産 NEM が移転するなどという取引は何ら行われていないにもかかわらず、それがあったとする情報を入力送信したのであるから、氏名不詳者が同社の電子計算機に与えた情報には経済的・資金的実体が欠けており、これが『虚偽の情報』に当たることは明らかである」とした。しかし、II に述べたとおり、平成 5 年東京高判の前記の規範は、信用金庫のオンラインシステムという当該事案で問題となった情報システムに即した「行為の意味付け」を、「虚偽の情報」の解釈において先取りして行ったものであり、本件に適切ではなかったと思われる。

V　おわりに

本稿の前半（I～III）では、まず、平成 18 年最決の担当調査官が示した「『情報』としてどの範囲の事柄を取り込むか」という問題に対し、平成 18 年最決が示した「情報」を実質的に解釈するアプローチを前提としつつ、重要事項性によってそのような実質的解釈の限界を画するという学説・実務家によって既に示されていたアプローチを（挙動による欺罔との類似性に着目して）支持し、その上で、対人取引と自動取引のメカニズム（特に意思決定の内容や位置付け[90]）の違いに着目して、情報システムにおいて前提とされている事項を重要事項と評価すべきであること、情報システムにおいて前提とされているといえるためには、当該事項が情報システムにおいてチェックされているか、当該事項について情報システムが当該情報システム外の制約を前提として構築されていることが必要であることを示した。

その上で、本稿の後半（IV）では、前半で示した立場から、判例等に現れた事例はどのように処理されるべきであるかを検討した。特に令和 5 年山口地判については、平成 15 年最決を電算機詐欺罪に応用することはできず、このことは、詐欺罪と電算機詐欺罪がそれぞれ対象とする対人取引と自動取引の違いに由来するものであることを示した。

一方、自動取引においては多様な情報に反応する可能性が放棄されているという、本稿が前提とする評価には議論がありうる。また、本稿の提案によっても、どのような場合に情報システムが当該情報システム外の制約を「前提」としているといえるか等の問題は残ると考えられ、これらは本稿の限界である。批判を仰ぐことができれば幸いである。

---

90)　ここで示した電算機詐欺罪の性質論、すなわち、詐欺罪が意思決定を虚偽告知に歪めるものであるのに対し、電算機詐欺罪は既に行われた意思決定の実現過程に介入するものであることは、電算機詐欺罪の議論全般において意識されるべき事柄と考える。