◇ 判例研究 ◇

刑事判例研究34

不正に入手した暗号資産NEMの秘密鍵で署名した上でNEMの移転行為に係るトランザクション情報をNEMのネットワークに送信した行為が刑法246条の2にいう「虚偽の情報」を与えたものとされた事例

（最判令和6年7月16日刑集78巻3号113頁）

刑事判例研究会
日原拓哉*

1．はじめに[1)]

2018年に暗号資産交換所a社に対しサイバー攻撃が行われ、同社が保有する暗号資産NEMのほぼ全部である約580億円相当が外部に移転される事態が生じた[2)]（具体的には、氏名不詳者である外部の攻撃者が、a社従業員の端末にマルウェアを感染させ外部ネットワークから当該従業員の端末経由でa社のネットワークに不正にアクセスし、遠隔操作ツールにより当社のNEMのサーバ上で通信傍受を行いNEMの秘密鍵を窃取したうえで、窃取したNEMの秘密鍵を使用して外部の不審通信先にNEMを不正送金したものであると推定されている）[3)]。氏名

＊　ひはら・たくや　大阪大学社会技術共創研究センター特任助教（常勤）

1）　なお、本稿執筆時点で確認できる最高裁判決の評釈として、橋爪隆「判批」有斐閣オンライン（記事ID：L2408005）https://yuhikaku.com/articles/-/19659、最終アクセス2024年11月20日、前田雅英「判批」《WLJ判例コラム 特報》第324号（2024WLJCC018）（https://www.westlawjapan.com/column-law/2024/240730/、最終アクセス2025年3月7日）、小池信太郎「判批」法学教室531号（2024年）115頁、永井善之「判批」新・判例解説Watch（文献番号z18817009-00-072132545）、品田智史「判批」令和6年度重要判例解説122-123頁。また、本章につき、那須翔「電子計算機使用詐欺罪における『虚偽の情報』の解釈・適用」Law & Practice No.17（2023年）227頁以下参照。

2）　日本経済新聞「コインチェックの仮想通貨不正流出、過去最大580億円」（https://www.nikkei.com/article/DGXMZO26231090X20C18A1MM8000/ 最終アクセス2025年3月22日）

3）　コインチェック社ホームページ「暗号資産NEMの不正送金に関する質問」　↗

不詳者である攻撃者はダークウェブ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。ここで攻撃者は暗号資産交換所での価格より安価なレートで交換を行った[4]。その後警視庁は、攻撃者について電子計算機使用詐欺罪（刑法246条の２）、交換に応じた者について犯罪収益等収受罪（令和４年改正前の組織犯罪処罰法11条）の疑いで捜査し、攻撃者の摘発には至らなかったものの[5]、その交換者31人を摘発した。本件はそのうちの１名が犯罪収益等収受罪で起訴された事件であるが、他の被告人に関する事件も含めて、その前提となる「犯罪収益」にかかる犯罪、すなわち氏名不詳者（攻撃者）によるNEMの移転行為が電子計算機使用詐欺罪（刑法246条の２）に該当するかが争点となった。

なお、本稿では犯罪収益移転罪に係る本件被告人の事件について取り扱うが、他の被告人の事件の判決文にも一部触れている。本件被告人の事件および他の被告人（「関連事件１」・「関連事件２」とする）における審級関係は図表のとおりである[6]。

	第一審	控訴審	上告審
本件	東京地判令和４年３月23日 刑集78巻３号261頁	東京高判令和４年10月25日 刑集78巻３号270頁	最三小判令和６年７月16日 刑集78巻３号113頁
関連事件１[7]	東京地判令和３年３月24日 LEX-DB: 25590382	東京高判令和４年６月23日 高刑速（令４）号188頁	最三小決令和６年10月７日 裁時1849号１頁
関連事件２	東京地判令和３年７月８日 LEX-DB: 25590771	東京高判令和４年３月22日 高刑速（令４）号118頁	

↘（https://coincheck.com/ja/info/faq_NEM、最終アクセス2025年３月22日）。

4) 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を入手できることになる。那須・前掲（注１）227頁。

5) 朝日新聞「NEM流出、不正交換容疑で31人を立件　主犯者は不明」（https://www.asahi.com/articles/ASP1Q3TWBP1QUTIL00B.html最終アクセス2025年３月22日）。

6) 関連事件２についてはLEX-DBによると上告中である。

7) 関連事件１では、電子計算機使用詐欺罪の成否に加えて、暗号資産の没収・追徴の可否についても検討されている。特に関連事件１の上告審決定は、暗号資産を介した電子計算機使用詐欺罪による「犯罪収益」に対する実務に影響を与えられるものと解されるが、この論点については本稿で検討する射程から外れるため省略する。

２．事案の概要

暗号資産 NEM の取引は次のようになされる[8]。すなわち、NEM の取引（送受信）を行うためには、NEM アドレス[9]を要するところ、この取引を行おうとする場合は NEM の取引日時、取引数量、送受信アドレスなどの取引に必要な情報を含むトランザクション[10]を送信元の NEM アドレスに紐づけられている秘密鍵[11]で署名することで暗号化して、NEM のネットワークに送る。NEM のネットワークは、複数の NIS[12]ノード（サーバ）で構成されているが、上記トランザクションを受けるとそのうちのいずれか１つの NIS ノードによってその送信元の NEM アドレスに紐づけられている公開鍵[13]で復号して、トランザクションに含まれる情報の整合性（秘密鍵によってなされた署名か）を機械的に確認して承認する。なお、この承認に当たっては、送信者が真の権限保有者か否かの確認はできない仕様になっている。NIS ノードはこの承認したトランザクションを、同様に承認した他

8） 以下の説明および専門用語に関しては、NEM Technical Reference Ver.1.2.1, Feb. 23, 2018（https://docs.NEM.io/pages/Whitepapers/NEM_techRef.pdf）も参照のこと。

9） N で始まる英数字で構成される40桁の文字列である（例：NBZMQO7ZPBYNBDUR2F75MCKA2S3DHDCIFG775N3D）。

10） 取引履歴等のデータのことである。NEM においては、移転されるモザイクの種類、数量、移転元・移転先アドレス、ネットワーク手数料の情報の総体を指す。トランザクションを通じて移転元アドレスの残高が減少し、移転先アドレスの残高が増加するとともに、移転元アドレスの秘密鍵による署名が付与される。

11） 公開鍵暗号による電子署名の仕組みで電子署名を行うために必要な情報のことである。

12） NEM Infrastructure Server の略称。NEM のノード用ソフトウェアを指し、ブロックチェーン管理等を行う。また、ノードとは P2P（peer-to-peer）システムにおいてシステムのネットワークを構成するサーバのことで、NEM においては、アドレスと公開鍵を持ち、ノード同士はインターネットにより通信を行われ、世界中に分散したノードでシステムが構成される。

13） アルゴリズムに従い秘密鍵から生成された情報で、秘密鍵と一対一に対応する。情報の受信者が署名を検証するために用いられる情報である。なお、この情報は他のユーザーから識別することができる。

の複数のトランザクションとともにブロックとして生成し、これをブロックチェーン[14]に組み込む。そして、他の NIS ノードと同期・連携して、NEM のネットワーク全体（全 NIS ノード）が最初のブロックから最新のブロックまで一連のブロックチェーンの情報を共有する。NEM のブロックは約 1 分ごとに生成されるが、これが順次積み重なりブロックチェーンに組み込まれ、共有されることで、書換えが事実上困難になり、取引が確定する、というものである。

a 株式会社は、暗号資産（仮想通貨）交換業等を営む会社であり、同社が扱う暗号資産には NEM（その通貨単位は XEM であり、総発行量は89億9999万9999XEM）があった。氏名不詳者は、a 社の NEM の秘密鍵を不正に入手した上、パソコン等を使用し、電気通信回線を通じて、上記秘密鍵を用いて、a 社の意に反し、平成30年 1 月26日午前 0 時 2 分頃から同日午前 8 時26分頃までの間、11回にわたり、a 社の管理する NEM アドレスから氏名不詳者らの管理する NEM アドレスに NEM 合計 5 億2630万10 XEM（日本円換算額547億1918万7322円相当）を送信、移転させた（以下、これを「本件移転行為」といい、氏名不詳者が本件移転行為によって得た NEM を「流出 NEM」という。）。その氏名不詳者は、その後流出 NEM を、ダークウェブ上に開設した交換所において格安のレートで交換していた。被告人は、その情を知りながら、平成30年 2 月21日午後11時11分頃から同年 3 月22日午前 3 時13分

14）「ブロック」とは複数のトランザクションをまとめた情報のことであり、ブロックを生成したノードにおける署名が付与され、さらにブロックチェーンにおける直前のブロックを示す情報も含まれる。「ブロックチェーン」とは、情報通信ネットワーク上にある端末同士を直接接続し、暗号技術を用いて、改ざんするにはそれより新しいデータ全てを改ざんする必要がある仕組みでデータを一本の鎖のように繋げ、正確なデータの維持を図るシステムを指す。暗号資産においては、暗号資産のある時点からある時点までのブロックの連鎖を指す。有効かつ検証可能なトランザクションのみから構成されるブロックチェーンのみが有効である。なお、NEM においては分散型台帳システムという、P2P ネットワークの参加者がブロックチェーンデータを個々の端末間でやり取りすることでそれぞれの端末で保持される形式をとっている。松嶋隆弘・渡邊涼介『改正資金決済法対応　仮想通貨はこう変わる‼　暗号資産の法律・税務・会計』（ぎょうせい、2019年）68頁も参照。

頃までの間106回にわたり、当時の自宅でパソコンを使用し、電気通信回線を介して、上記交換所で、自身が保有するビットコイン等と交換することで、流出 NEM の一部である NEM 合計約2362万6094XEM（日本円換算額７億7342万5246円相当）を受信、取得した。

被告人弁護人は、本件行為の電子計算機使用詐欺該当性について、NEM ブロックチェーンは、公開鍵と秘密鍵の一致のみをもってトランザクションの正当性を承認・共有するものであり、送信者の権限や属性は事務処理システムの目的の範囲内ではないから、氏名不詳者による本件移転行為は、ブロックチェーンに「虚偽の情報」を与えたことにはならない、として無罪を主張した[15)]。

第一審判決（東京地判令和４年３月23日刑集78巻３号261頁）は、被告人を有罪（懲役２年（執行猶予５年）、金1960万3566円の追徴）とし、以下のように述べた。

すなわち、「NEM は財産的価値であるから、NEM を保有しその取引をしようとする者は、自らが保有する NEM を適正に管理し、第三者に不法・不当に奪われることがないようにすることにとりわけ強い関心を有しているはずであ」り、「現に、NEM の取引においては、単に、トランザクションを NEM のネットワークに送るのではなく、秘密鍵で署名することで暗号化するというプロセスを経ている」。「ここで、ブロックチェーンの技術に精通している証人 D の供述によれば、秘密鍵とは、『本人だけが知っている、他人に知られてはいけない鍵』であるというのであり、『秘密鍵』と

15) その他、〔１〕氏名不詳者が A 社の NEM の秘密鍵を不正に入手した行為は不正アクセス行為の禁止等に関する法律違反の罪又は不正指令電磁的記録供用罪（刑法168条の２第２項）に該当するところ、仮想通貨においては、秘密鍵の占有者が仮想通貨の所有者であり、秘密鍵入手後に仮想通貨の財産的価値を具体化するために別途の行為を要しないから、氏名不詳者による本件移転行為は、氏名不詳者による秘密鍵の不正入手行為の不可罰的事後行為である、〔２〕NEM において不実の電磁的記録の作出を行うのは個々の NIS ノードではなく、全ての NIS ノードの集合体であり、これは「電子情報処理組織」であって「電子計算機」に該当しない、と主張しているが、電子計算機使用詐欺罪の構成要件的行為の評価について論点をしぼるため、この点については省略する。

いう言葉の通常の意味からも、D 証人が述べるところは支持できる。そうすると、秘密鍵を知っているのは、本来的には、NEM の保有者と委託等に基づいてその者から適法に知らされた者に限られる。そして、NEM は財産的価値であり、秘密鍵を他人に知られれば、その他人が秘密鍵を悪用して自らが保有する NEM を移転させることが可能になるのであるから、NEM の保有者らは、秘密鍵を厳重に管理するはずであり、かつ、そう期待される」。「この点に関し、確かに、NEM の取引過程中の、NIS ノードにおけるトランザクションの承認においては、NEM の送信者が真の権限保有者か否かの確認はできない仕様となっている。しかし、そうであるからといって、直ちに、NEM のネットワークが、秘密鍵を知る者であれば、NEM の保有者でなくても、その者の保有する NEM を送信することを容認しているとはいえない」。「NEM の取引において、わざわざ秘密鍵による暗号化のプロセスを設けていることに鑑みれば、NEM のネットワークにおいては、秘密鍵が NEM の保有者らにより厳重に管理されているであろうことを期待し、それを前提に、管理コストを省くなどして NEM の取引に参加する者の利便を図るため、NIS ノードにおけるトランザクションの承認においては、トランザクションに含まれる情報の整合性の機械的確認にとどめているとみるのが相当である。すなわち、秘密鍵による暗号化のプロセスを含む NEM のネットワークにおいては、『秘密鍵を持つ者が真の権限保有者であること』の確認を、NEM の保有者の側に委ねているだけで、これを放棄しているとかこの点に無関心であるとは解されない」。「以上によれば、NEM を送信する者の権限の有無の確認は、NIS ノードがこれを確認する仕様になっていないことを考慮しても、なお NEM のネットワーク（全 NIS ノード）の事務処理の範囲内にあるといえる」。「したがって、本件で、氏名不詳者は、不正に入手した A 社の NEM の秘密鍵を用いることで、NEM のネットワーク（全 NIS ノード）に対し、本件移転行為に係るトランザクションを送信しているのが真の権限保有者の a 社であるとの『虚偽の情報』を与えたといえる」として電子計算機使用詐欺に該当するとし

た。

控訴審判決（東京高判令和４年10月25日 刑集78巻３号270頁）では控訴棄却とし、虚偽情報該当性に関して以下のように述べた。

すなわち、原判決の言うように「確かに、NIS ノードにおけるトランザクションの承認においては送信者が NEM の正規の権限保有者か否かの確認はできない仕様となっている。しかし、NEM の取引が金融取引である以上、所論がいう規約等の存在の有無にかかわらず、正規の秘密鍵保有者による取引であることが当然の前提とされているのであって、原判決が指摘するとおり、NEM のネットワークにおいては秘密鍵が NEM の保有者らにより厳重に管理されていることを前提として、トランザクションに含まれる情報の整合性を機械的に確認するにとどめているのであって、正規の秘密鍵保有者でない者による取引は本来的に想定されていないとみることができる。そもそも、電子計算機使用詐欺罪における『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（東京高等裁判所平成５年６月29日判決・高等裁判所刑事判例集46巻２号189頁参照）ところ、氏名不詳者は、真実は、a 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 を移転する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送信したのであるから、氏名不詳者が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、正規の秘密鍵保有者による取引に係る事務処理を行うという目的に照らし、これが『虚偽の情報』に当たることは明らかである。したがって、正規の秘密鍵保有者でない氏名不詳者による本件移転行為は電子計算機に虚偽の情報を与えたものと認められる」として電子計算機使用詐欺性を肯定した。これに対して被告人弁護人は上告した。

3．判　　旨

最高裁判所第三小法廷は、上告趣意のうち判例違反をいう点は事案を異にする判例を引用するものであって本件に適切でなく、その余は憲法違反をいう点を含め実質は単なる法令違反・事実誤認の主張であって刑事訴訟法405条の上告理由に当たらないとしつつ、職権で以下のように判示した。

「NEM のネットワークに参加している者は、自らの管理する NEM アドレスに紐づけられている秘密鍵で署名しなければ、トランザクションが NIS ノードに承認されることも、ブロックチェーンに組み込まれることもなく、NEM の取引を行うことができないのであるから、秘密鍵で署名した上でトランザクション情報を NEM のネットワークに送信することは、正規に秘密鍵を保有する者による NEM の取引であることの確認のために求められるものといえる。このような事情の下では、氏名不詳者が、不正に入手した a 社の NEM の秘密鍵で署名した上で本件移転行為に係るトランザクション情報を NEM のネットワークに送信した行為は、正規に秘密鍵を保有する a 社が NEM の取引をするものであるとの『虚偽の情報』を NEM のネットワークを構成する NIS ノードに与えたものというべきである」。

なお、本判決には以下のような今崎幸彦裁判官、林道晴裁判官（今崎裁判官補足意見同調）の補足意見が示されている。

「NEM 等の暗号資産は、資金決済に関する法律上、不特定の者に対して決済手段として使用でき、かつ不特定の者との間で売買、交換を行うことができるような財産的価値であって、電子情報処理組織を用いて移転することができるものと定義されている。本件当時においても、ブロックチェーンや公開鍵暗号等の技術を用いた数多くの暗号資産が発行されており、秘密鍵による排他的支配可能性を前提に、資産等としての利用が急速に拡大し、幅広く取引の対象とされそのための市場が形成されていたということができる」。「こうした NEM 等の暗号資産が社会経済において果たしてい

る役割や重要性等に照らし、資金決済に関する法律等は、暗号資産のネットワークに参加している暗号資産交換業者に対し、暗号資産交換業者を介して取引を行う利用者保護のための規制を設け、また、本件後ではあるが、金融商品取引法は、令和元年法律第28号による改正により、暗号資産の不公正取引を規制し、暗号資産のネットワークに参加している者らの権利のより直接的な保護を図っている。正規の秘密鍵保有者でない者が不正に入手した秘密鍵で署名した上で、当該秘密鍵が紐づいているアドレスから他のアドレスに NEM 等の暗号資産を移転させた場合、正規の秘密鍵保有者が暗号資産を移転させた者に対し、少なくとも不当利得や不法行為等を理由とした民事上の請求を行うことができることについても大方の異論のないところであろう」。「刑事の分野においても、正規の秘密鍵保有者の NEM に対する権利を害する行為は、構成要件に該当する限り処罰の対象となり得る」。

「NEM が不特定多数のネットワーク参加者を得て取引の対象とされているのは、NEM のシステムによる取引における静的、動的安全の確保に対し、社会の信頼があるからにほかならない。『虚偽の情報』該当性は、こうした NEM の利用実態、ひいては NEM 等の暗号資産が社会経済において果たしている役割や重要性等の観点からの考察抜きに判断することはできないのであって、システム単体としての仕組みや働き等からロジカルに演繹されるものではない。本件において、正規の秘密鍵保有者でない氏名不詳者は、不正に入手した A 社の秘密鍵で署名した上で、当該秘密鍵が紐づいている A 社の管理する NEM アドレスから氏名不詳者らの管理する NEM アドレスに NEM を移転させる旨の本件移転行為に係るトランザクション情報を NEM のネットワークに送信した。確かに、NEM のシステムは、トランザクション情報に署名した者が正規の秘密鍵保有者であるか否かを判別する仕組みを持たない。しかし、上述のような NEM のシステムに対する社会の信頼は、正規の秘密鍵保有者が秘密鍵の管理を通じて NEM を排他的に支配することができることによって確保される。正規の秘密鍵保有

者以外の者が不正な方法で秘密鍵を入手し、これで署名することは、正規の秘密鍵保有者の NEM に対する排他的支配を害し、NEM のシステムに対する社会の信頼を損なう。こうした観点も踏まえれば、不正に入手した秘密鍵で署名した上で本件移転行為に係るトランザクション情報を NEM のネットワークに送信した行為は、正規の秘密鍵保有者であるという意味での主体を偽ったトランザクション情報を NEM のネットワークを構成する NIS ノードに与えた行為と評することができるのであり、電子計算機に『虚偽の情報』を与える行為にほかならない」。

4．検　　討

本件最高裁判決は、犯罪収益収受罪（改正前組織的犯罪処罰法11条）の前提犯罪としての電子計算機使用詐欺罪（刑法246条の２）の成否に関するものである。そのため、直接は電子計算機使用詐欺罪に関する判例とはいえないものの、その傍論において示されている部分に電子計算機使用詐欺罪の要件解釈――とりわけ「虚偽性」の解釈――に大きく関連しうる事項が含まれている。そのため、以下、刑法246条の２の構成要件要素である、「虚偽の情報を与え（る）」と「財産権の得喪若しくは変更に係る虚偽の電磁的記録」に共通する「虚偽性」の意義について立法者解説、これに関連する最高裁判例及び下級審判例と最高裁判所調査官解説を素材としながら、本判決の位置づけを検討する。

⑴　刑法246条の２における「虚偽の情報」要件の解釈

本罪が創設された1987年当時の「虚偽の情報」の立案担当者の説明では「『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」である[16]とする。そして本罪

16）　米澤慶治編『刑法等一部改正法の解説』（立花書房、1988年）117頁〔的場純男〕。

の類型のうち、「虚偽の情報を与えて財産権の得喪、変更に係る不実電磁的記録を作る」例として、銀行のオンラインシステムにおいて行員が窓口端末機を用いて虚偽の入金データを入力する行為、汎用端末機を用いて元帳ファイル上の預金残高を書き換える行為、他人のキャッシュカードを自動振込機等で不正に使用してほしいままに他人の暗証番号及び振込データを入力し仕向銀行のコンピュータセンターあるいは全銀センターを介して被仕向銀行のコンピュータセンターの電子計算機に振込電文を発出する行為が挙げられている[17]。また、「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す」る行為の例としては、財産権の得喪・変更に係る備付型の元帳ファイル等について内容虚偽の電磁的記録を正規のものと差し替える行為や、残度数を虚偽のものに改変したテレホンカードを公衆電話機の差し込み口に挿入するような行為が挙げられている[18]。ただし、拾得、窃取に係るプリペイドカードを使用して財産上の利益を得た場合、それだけでは虚偽の電磁的記録を人の事務務処理に供したとはいえないし、虚偽の情報または不正の指令を与えたものともいえないという[19]。

本罪創設後の裁判例においても上述の例に近い、預金残高記録の改変により財産上の利益を取得した事例[20]が挙げられ、そこには本罪の解釈におけるリーディングケースとして著名な東京高判平成５年６月29日高刑集46巻２号189頁も含まれるだろう。

この判決は、信用金庫の支店長であった被告人が、自己のＢに対する債務返済に充てるため、振込入金の事実がないのに部下職員に同支店設置のオンラインシステムの端末機を操作させ、同支店からＢの普通預金口座に金4600万円の振込入金をさせ、さらに自己に支払義務のある小切手を決済

17） 米澤編・前掲（注16）122頁〔的場〕。
18） 米澤編・前掲（注16）123-124頁〔的場〕。
19） 米澤編・前掲（注16）125頁〔的場〕。
20） 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、岐阜地判平成24年４月12日LEX-DB: 25481190。

するのに必要な資金を調達するために、入金の事実がないのに部下職員に前記オンラインシステムの端末機を操作させ、自己が同支店に設けていた自己名義の当座預金口座に金2800万円を入金させた事案であることを前提に、「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、金融実務における入金、振込入金（送金）に即すと、「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ものと解するのが相当である」とし、「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」ことから「虚偽の情報」に該当する旨を認めている。

その後、最高裁が本罪の「虚偽の情報」の解釈に言及したのは最決平成18年２月14日刑集60巻２号165頁（以下、「平成18年決定」という。）であった。もっとも、本決定文では構成要件のあてはめは明確に行われておらず、被告人が「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、５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」行為が、「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」というのみである。ここでは、本決定における調査官解説[21]が意義を有するものと考えられる。次節ではその調査官解説で示された見解も含めて、「虚偽性」の判断枠組をめぐる学説について考察する。

⑵ 「虚偽」性の判断枠組

本罪の構成要件要素の一つである「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」[22]に関しては多様な見解が存在する。

まず、何を基準にして虚偽性を判断するか[23]については以下のものが挙げられる。

すなわち、⑴「財産権の得喪若しくは変更に係る電磁的記録」の内容に対応する財産状態の変動についてそれをおこなうか否かを本来決定するべき立場にある者の意思あるいはその変動の効果が帰属する立場にある者の

21） 藤井敏明「判解」最判解刑事編平成18年度63頁以下。

22） 西田典之「電子計算機使用詐欺罪についての覚書――債務免脱型の不法利得を中心として――」「植村立郎判事退官記念論文集」編集委員会編『植村立郎判事退官記念論文集現代刑事法の諸問題』（立花書房、2011年）161頁、『条解刑法（第４版補訂版）』（弘文堂、2023年）800頁、大塚仁ら編『大コンメンタール刑法（第３版）第13巻』（青林書院、2018年）181頁（鶴田六郎）、大谷實『刑法講義各論（新版第５版）』（成文堂、2021年）297頁、浅田和茂『刑法各論（第２版）』（成文堂、2024年）260頁。なお、単に「内容が真実に反する情報」の記載に留めるものとして、山口厚『刑法各論（第３版）』（有斐閣、2024年）281頁、松宮孝明『刑法各論講義（第６版）』（成文堂、2024年）284頁（ただし、現金の受入のない振込入金情報という例示がある）。

23） 以下の分類は西田典之・山口厚・佐伯仁志編『注釈刑法 第４巻 各論⑶ §§ 235～264』（有斐閣、2021年）326頁以下（西田典之＝今井猛嘉）による。

利益を基準にして判断する見解[24]、(2)コンピュータ・システムを用いて利益を提供する主体の意思に反する点を基準にして判断する見解[25]、(3)「電子計算機において処理されることとなる情報をその管理者（自然人）が知ったならばその先の手続を進めないであろう情報」が「虚偽」の情報だとする見解[26]、(4)詐欺罪とパラレルに考慮して「取引上重要な事実」について偽ったものとする見解[27]、(5)財産移転に向けられて入力された情報の持つ意味とそれに対応する現実の法律関係に齟齬がある場合に虚偽性が基礎付けられるとの見解[28]である。(1)および(2)の見解は詐欺利得罪（刑法246条２項）と被害者の関係の関係を重視するところに、(3)の見解はコンピュータ・システムの設置・運営者の利害も視野に入れるところに、(4)の見解は被害者の意思ではなく詐欺利得罪の欺罔行為の解釈を踏まえる理解に、そして(5)の見解は電子計算機使用詐欺罪と詐欺利得罪の相違をその立場の違いから理解することにそれぞれ重点が置かれる。

これら見解に対しては、コンピュータによる事務処理においては迅速に大量の事務処理が可能になる反面、あくまでも入力された情報についてしかその正誤を判断できないという限界が存在し、社会通念や文脈を読み取

24） 拾得あるいは窃取したプリペイドカードの無断利用も処罰可能にする理論構成である。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頁参照。なお、この点につき虚偽性を認めることは不当であることを前提に、被害者の意思のうち財産犯としての保護に値する範囲の錯誤に限定するという詐欺罪における議論に即して、これを修正して、例えば店舗から窃取したものを当該店舗で使用するような場合を除いて、電子計算機使用詐欺罪を否定すべきという修正した形で支持するものとして和田俊憲「キセル乗車」法学教室392号（2013年）100頁。

25） 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（2013年）８頁。

26） 高嶋智光「判批」研修778号（2013年）13頁。

27） 林幹人「電子計算機使用詐欺罪の新動向」NBL No.837（2006年）32-33頁、同旨、渡邊卓也『ネットワーク犯罪と刑法理論』（成文堂、2018年）183頁（同「電子計算機使用詐欺罪における『虚偽』性の判断」高橋則夫・松原芳博・松澤伸編『野村稔先生古稀祝賀論文集』（成文堂、2015年）377頁。

28） 渡邊・前掲（注27）183頁、内田幸隆「電子マネーと財産犯――インターネットにおける事例を中心に――」刑事法ジャーナル15号（2009年）21頁。

る力はコンピュータには備わっていないと思われるために[29]、電子計算機使用詐欺罪の被害者として考慮されるのは、財産的被害を受けた者およびコンピュータ・システムの設置運営主体であり、被害者の意思は当該コンピュータ・システムの趣旨・目的を踏まえて客観的に判断せざるを得ないことに留意しなければならない[30]。

次に、ある事実が情報あるいは電磁的記録に該当することを前提に、いかなる情報が「虚偽の情報」あるいは「虚偽の電磁的記録」なのかについて、処罰範囲の明確化のためには「虚偽」の意味を画する必要があるところ、文献によればおおむね以下のように分類される[31]。すなわち、(1)当該電磁的記録が不正作出あるいは偽変造されたものに虚偽性を限定する説（最狭義説）、(2)当該電磁的記録が人の事務処理の用に供される際に読み取られる情報と事実とを比較し両者の間に不一致がある場合に虚偽性を限定する説（狭義説）、(3)当該電磁的記録が人の事務処理の用に供される際に読み取られる情報と事実の間の形式的不一致のみならず、当該電磁的記録の内容を実質的・合理的に解釈し、真実と異なる情報が含まれていれば虚偽性を充足するものとする説（広義説）である。これらについて、(1)最狭義説に対しては、情報あるいは電磁的記録を構成するデータ（数字）について特定の趣旨実現のために設定されたコンピュータ・システムとの関係で当該数字の集合に一定の意味が付与される場合に限定され、コンピュータの設置・運営の趣旨の考慮なくして電磁的記録の虚偽性を導けないという批判

29） 和田俊憲「キセル乗車」法学教室392号（2013年）100頁参照。「人は錯誤に陥るが、あらゆる事情を判断の基礎に置くことができる。機械は錯誤に陥らないが、判断の基礎となる情報はプログラミングされた範囲に限定されている。機械に処理を委ねミスのない大量の処理を可能にする代償として、判断対象となる事情を限定しているのである」。なお、機械学習を行う AI による判断の場合には判断の根拠となる事情が当初のプログラムから乖離する可能性はあるものの、ここでは検討の対象としない。

30） 西田・山口・佐伯（仁）・前掲書（注23）328頁（西田＝今井）。

31） 小林隼人「判批」警察公論67巻９号（2012年）93頁、高嶋・前掲（注27）18頁、西田・山口・佐伯（仁）・前掲書（注23）328頁（西田＝今井）。

がある[32]。さらに(2)狭義説については、結局のところ当該電子計算機を利用するコンピュータ・システムの特性は理解しなければならず広義説と内実は変わらないのではないか[33]と、その(3)広義説については、特定のコンピュータ・システムにおいて電磁的記録につき予定されている事務処理目的の認定が重要となるところ、これを無制限に拡張解釈すると虚偽性の判断が恣意的になる懸念がある[34]と批判される。

このような学説の対立を踏まえて修正された整理が近年見られるようになっている。まず、平成18年決定調査官解説の判断枠組を精緻化する理解が挙げられる。その平成18年決定調査官解説[35]では、「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、構成要素に過ぎないということになろう。なぜなら、そのような意味での「情報」こそが、財産上不法の利益をもたらす情報として社会的に意味のあるものであり、また、電子計算機をして財産権の得喪に係る電磁的記録を作成させるものだからである。したがって、真実性が問われる情報は、上告趣意にあるようなクレジットカード番号等そのものではなく、『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』ということであると考えられる」。「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。……しかし、一般にクレジット

32） 西田・山口・佐伯（仁）・前掲書（注23）328頁（西田＝今井）。
33） 西田・山口・佐伯（仁）・前掲書（注23）329頁（西田＝今井）、渡邊・前掲（注27）182頁脚注92、および冨川雅満「キセル乗車と電子計算機使用詐欺罪」松原芳博『続・刑法の判例（第３版）』（成文堂、2022年）177頁。
34） 西田・山口・佐伯（仁）・前掲書（注23）329頁（西田＝今井）。
35） 藤井・前掲（注21）69頁以下。

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、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」（太字・傍線筆者）と評価する。

すなわち「虚偽の情報」を判断する枠組[36]として、「当該コンピュータ・システムにおいて予定されている事務処理の目的」に照らした真実性判断について、当該入力行為により実現しようとする財産的な取引を全体として「情報」ととらえることが整合的であるとし、入力された個別的なデータではなく電子計算機を利用して実現しようとした取引そのものを情報として把握すべきという。これを定式化すると、① 電子計算機内に実際に含まれる情報を確認し（情報の確定）、② その情報がどのように理解されるかを評価して（情報内容の評価）、③ これら①および②を通じて明らかにされた「情報」内容が現実と一致しているかを判断する（情報内容と現実との照

36） 藤井・前掲（注21）71頁脚注11。

合）ということになる[37]。

ただし平成18年決定調査官解説においては、以下の２つの事例において留保が付けられていることにも注意しなければならない。まず、**① 他人がクレジットカードの名義人本人の了解を得た上でオンライン取引を行った場合**は最決平成16年２月９日刑集58巻２号89頁を参照しつつ、電子計算機に与えられた情報には申込みの主体に係るものがあるとすれば電子計算機使用詐欺罪の成立が考えられるとする一方で、電子計算機を使用するオンライン取引の場合において、「クレジットカードの名義人本人が当該取引を申し込んだ」とする情報と「クレジットカードの名義人本人の了解を得て当該取引を申し込んだ」という実態との違いに処罰に値するだけの虚偽性が認められるかが問題であり、「名義人本人が」ということを「名義人本人の意思に基づき」と同視できるとすれば「虚偽」性はないと考えられる、あるいは人を相手に行うなりすましと異なって名義人本人の手足として入力したという評価もありうる旨が示されている[38]。次に、**② クレジットカードの名義人本人が真実は決済する意思がないのにオンライン取引を行った場合**について、内心の支払意思までは電子計算機による事務処理で検証されることは予定されていないので入力行為とはまったく別個の事情であり「虚偽の情報」を与えたとは言えない一方、クレジットカードを利用した自動決済システムであっても名義人がクレジットカード所定の決済を実施することは前提だから、決済を申込んだ時点で引き落とし期限までに代金を決済する旨の意思の表明も含まれるから「虚偽の情報」を与えたともいえるという両面的な評価を示している[39]。ここでは、上記①②の事例の評価は「情報」としてどの範囲の事情を取り込むかにより結論が決まってくる、という[40]。

37） 冨川・前掲（注33）177頁参照。
38） 藤井・前掲（注21）73頁脚注12。
39） 藤井・前掲（注21）73-74頁脚注13。
40） 藤井・前掲（注21）74頁脚注13。

その「情報」としてどの範囲の事情をどの程度取り込むのかについては、詐欺罪とのアナロジーで電子計算機使用詐欺罪を理解する見解がある[41]。これは、行為者の電磁的記録（データ）の入力が、当該データの処理目的を参照しつつどのような意味を持つのか（＝「行為の意味付け」[42]）を考察するものであり、詐欺罪（刑法246条）の解釈を参考に「重要事項」に関する情報に限定しつつ、電子計算機使用詐欺罪における取引構造に特化して、① 重要事項性をどう位置づけるか、そして② 何を重要事項と評価すべきかに段階分けを行うものである[43]。

この両者に共通する重要事項性の判断に関し、最決平成26年３月28日刑集68巻３号646頁および最判平成26年３月28日刑集68巻３号582頁で「挙動による欺罔」を認めてきたことに着目する。上記最高裁判決・決定の調査官解説では、欺罔行為の意義について、言語によって積極的に事実を偽る場合だけでなく、その挙動の社会的意味の解釈によって事実を偽ったことみなされる場合（積極的な欺罔行為はないが一定の動作によって事実を偽る場合）が含まれると解しつつ[44]、その行為が「欺く行為といえるか（挙動による欺罔行為性）」と「欺いた内容・対象が財産的処分行為の判断の基礎となる重要な事項か（欺罔行為の内容・対象）」の両面から検討されることになり、並列的関係にある以上はその双方から欺罔行為概念を限定することはできるし、両要件の該当性判断においても、これらを基礎づける事実関係に重なる部分は考えられる[45]といいうるところ、この詐欺罪における欺罔行為の解釈枠組を電子計算機使用詐欺罪にも応用し、挙動による欺罔における「社会的意味の解釈」の決定と行為者のデータの入力の意味は当該データの処

41） 那須・前掲（注１）208頁。
42） 藤井・前掲（注21）74頁注13における「『情報』としてどの範囲の事柄を取り込むか」の判断枠組と同旨である。
43） 那須・前掲（注１）210頁。
44） 野原俊郎「判解」最判解刑事平成26年度138頁。
45） 野原俊郎「判解」最判解刑事平成26年度173頁。

理の目的を参照した決定を同視して把握する[46]。

次に、対人取引と自動取引の構造の違いをみる。対人取引においては、行為者においては実行の着手が認められる可能性は否定できないものの、相手方がその取引に応じるか否かの意思決定を欺罔行為時点ではしてはいないし、まだその取引に応じるか否かの余地が残される。一方で自動取引においては、意思決定は虚偽の入力に先立つ情報システムの設計時点で既に行われており、条件に合わない取引は応じることはできないので、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行為に電子計算機使用詐欺罪の当罰性を見出すものとみる[47]。そして、情報システムにおいて前提とされている事項に「重要事項」を見出す[48]。ここでの「情報システムにおいて前提とされている」の判断について、肯定に傾く事情としては、虚偽の判定ではなく、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るような情報システム側でチェックされている事項やデータ入力に対する情報システム外の制約[49]を、否定に傾く事情として、法令・規約による制約または物理的制約のないものやデータ入力に対する情報システム外の制約がないことを挙げている[50]。上記のように「虚偽」性を理解すれば、平成18年決定調査官解説のあてはめ[51]にも整合的であるという[52]。

この解釈によると、諸外国あるいは条約における犯罪としての「コンピュータ詐欺」の要件にある、「無権限の［unbefugt］」（ドイツ刑法263条 a）、

46） 那須・前掲（注 1 ）211頁。
47） 那須・前掲（注 1 ）212頁以下。
48） 那須・前掲（注 1 ）213-214頁。
49） 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）による制約または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が例示されている（那須・前掲（注 1 ）214頁）。
50） 那須・前掲（注 1 ）214頁。
51） 藤井・前掲（注21）70頁。
52） 那須・前掲（注 1 ）214頁。

「権限なく［without authorization］」（アメリカ合衆国法典第18編1030条(a)(4)）あるいは「権限なく」（サイバー犯罪条約（ブダペスト条約）８条）の構成要件要素が日本刑法246条の２と比較して存在しないことを鑑みれば、日本刑法でいう電子計算機使用詐欺罪については法令・規約による制約がないとみて、なお「無権限者による」行為は、必ずしも「虚偽」ということはできないといえるだろう。

⑶ 近時における電子計算機使用詐欺罪の運用について

サイバー犯罪の一類型として位置づけられる電子計算機使用詐欺罪に関し、令和５年度におけるコンピュータ・電磁的記録対象犯罪の検挙総数1,000件のうち電子計算機使用詐欺罪の検挙件数は950件であることや不正アクセス禁止法違反の罪の検挙件数が521件であること、および令和元年度より325件、511件（令和２年）、692件（令和３年）、918件（令和４年）と検挙件数についても増加の一途をたどっていることに鑑みれば[53]、電子計算機使用詐欺罪は看過することのできないサイバー犯罪とみることもできるだろう。しかし、その「虚偽性」要件の基準がやや不明確であることは前述のとおりであり、適切な処罰範囲の限界づけを図る必要もある。そこで、電子計算機使用詐欺罪の成否が争われた裁判例およびそこで示された判断枠組について概観する。

① 回数券や定期券を利用したキセル乗車事例

JR 東日本上野駅あるいは鶯谷駅から宇都宮駅の経路においていずれかの発駅の初乗運賃乗車切符で入場し着駅で雀宮駅－岡本駅（いずれも宇都宮駅の隣駅）の回数券で出場したキセル乗車（往路）と、宇都宮駅から赤羽駅あるいは渋谷駅の経路において発駅の宇都宮駅ではその初乗運賃乗車切符で入場しいずれかの着駅では往路で使用した入場記録のみが記録された切符

53） 法務省法務総合研究所編『令和６年度版 犯罪白書』（2024年12月）210頁参照。

を乗越精算機で精算した精算券で出場して、本来の乗車運賃より安価な金額で上記区間を乗車した事案に関する東京高判平成24年10月30日高刑速（平24）号146頁ではおおむね、往路について、宇都宮駅で自動改札機に投入した入場記録のない回数券は、「岡本駅乗車」の情報を入力したものとしてシステム上理解されるし、そのようなシステムは鉄道会社においても予定されていたものであり、現実は鶯谷駅または上野駅であったために「虚偽」性は充足され[54]、復路について乗車券上の情報は「鶯谷駅入場」または「上野駅入場」であり、自動改札機のシステム上もそのように評価されるところ、現実は「宇都宮駅入場」であったために「虚偽」性は充足される[55]として、結論としては往路・復路ともに電子計算機使用詐欺罪の成立を認めた。

その一方で、近鉄名古屋駅から近鉄松阪駅の経路において発駅の初乗運賃乗車切符で近鉄名古屋駅に入場し着駅で近鉄高田本山駅－近鉄松阪駅あるいはJR東海多気駅－JR東海松阪駅間の定期券によりJR東海・近鉄の

54） 那須・前掲（注１）233頁は、「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……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る。

55） 和田・前掲（注29）101頁は、有人改札の場合と比較しつつ「復路の乗車券については、もし実際は宇都宮駅で入場したという事実を知ったとしたら、出場させなかったといえ、往路と同様その意思は財産的保護に値する」。「仮に有人の精算窓口であったとしたらどうかを考えると、渋谷駅と同じく都区内の上野駅からの乗車券であるにもかかわらず、発券・入場時刻から著しく長い時間が経過しているから、少なくとも直ちには精算・出場させずに事情を聞くと考えられる。そうすると．自動精算機が精算券を発行し、直ちに出場することを認めたのは、機械化に由来することであるといえるから、出場させないという意思は、結局保護に値しない」と本罪の成立を否定する。この点については、大都市近郊区間にかかる運賃計算の特例を設けていること（JR東日本についてはJR東日本ホームページ（https://www.jreast.co.jp/kippu/1103.html、最終アクセス2025年３月14日）も鑑みれば、入場時間から出場時間までに長時間が経過していることは少なくとも事務処理目的の内容に考慮されるべき事情には入らないものと考えるべきだろう。

共同使用駅で、入場記録を判定するシステムが導入されていない松阪駅で出場した事例において、第一審である名古屋地判令和２年３月19日判時2529号117頁では、本件定期券を松阪駅[56]改札で出場する際に「入場駅情報」は読み取らないシステムである以上は、「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」はいないとして電子計算機使用詐欺罪該当性を否定したものの、控訴審である名古屋高判令和２年11月５日高刑速（令２）号522頁では「虚偽の電磁的記録」が供されていなくても、すなわち本来読み取る予定のない入場記録が自動改札機に接続された電子計算機に供されていなくても、自動改札機一般の事務処理目的として、その行為がシステム設置者の許容しないところであり、自動改札システムの目的が有効適切な乗車か否かを判断することにあるとして、電子計算機使用詐欺罪の成立を認めた[57]。

これら事例を概観すると、特に後者の事例ではもはや「財産権の得喪・変更判断に影響しない情報」を供してなくても電子計算機使用詐欺罪を認めたと評価できるだろう[58]。もちろんキセル乗車行為は社会的な非難を受ける行為であるし、鉄道会社もこれを許容するとは思われないが、法定刑の重い電子計算機使用詐欺罪ではなく、鉄道営業法違反の罪を適用すべき事例であったと思われる。

② ETC カードの第三者使用事例

被告人 A、B、C（A と生計を同一にする C の弟）の３名が C の会員名義で

56） 近鉄・JR 東海のホームが連続しており、北口は近鉄管理、南口は JR 東海管理であった。

57） この事件の問題の所在に関し、松宮孝明『誤振込みと財産犯』（成文堂、2023年）240頁以下参照。

58） もちろん、近鉄名古屋駅から松阪駅の乗車に関して150円切符を利用し正規の運賃との差額790円を免れたことについて鉄道営業法29条１号類型の「有効ノ乗車券ナクシテ乗車シタルトキ」に該当し処罰対象となるし（法定刑は２万円以下の罰金）、さらに同法18条において「有効ノ乗車券ヲ所持セス」乗車した場合は不正に免れた運賃の最大３倍の割増運賃を払わせることも可能である（鉄道運輸規定19条参照）。詳しくは松宮・前掲書（注57）238頁も参照。

のクレジットカードに付帯する ETC カードを挿入した ETC 車載器を搭載した普通乗用自動車で C が乗車せずに B が運転し A が同乗して阪神高速道路15号大阪堺線湊町出入口から流入し阪神高速道路13号東大阪線東大阪（東行）近畿道北出口ランプ[59]から流出（2022年11月 8 日）、阪神高速道路15号大阪堺線湊町出入口から流入し阪神高速道路11号池田線豊中南（北行）名神出口ランプ[60]から流出（2022年12月 2 日）するに際し、ETC による割引後の通行料金と通常の通行料金との差額たる財産上不法の利益を得たとして起訴された事案について、大阪高判令和 6 年12月20日 LEX-DB:25621915（原審：大阪地判令和 6 年 5 月 8 日 LEX-DB: 25599425）[61]は以下のように判示した。

「クレジットカードに付帯した ETC カードを使用した場合、既存のクレジットカードによる決済システムを通じての通行料金徴収がなされる以上、通行料金の発生から徴収までの局面において、ETC システムとクレジットカードの決済システムとが整合するよう理解することが相当」であり、平成18年決定を参照しつつ「クレジットカード決済を使用するオンライン取引では、消費者の利便性等の観点から本人確認がなされない場合であっても、名義人以外の者によるクレジットカード情報の入力送信は電子計算機使用詐欺の虚偽の情報の提供に当たると解され」、「ETC システムでも、高速道路の混雑防止、利便性の向上、管理費削減等のため、使用の都度の名義人の本人確認を求めていないとはいえ、上記クレジットカード決済における状況からすると、ETC カード名義人以外の者による ETC レーン通行時の当該 ETC カード情報等の送信は、虚偽の情報の提供に当たるとするのが合理的である」という。

しかし、引用されている平成18年決定の調査官解説によれば、「名義人本

59） 東大阪荒本出入口のことである。

60） 名神豊中 IC のことである。

61） 本判決の評釈として、松宮孝明「判批」新・判例解説 Watch（2025年 3 月）文献番号 z18817009-00-072152569。原審の評釈として松宮孝明「判批」新・判例解説 Watch（2024年10月）文献番号 z18817009-00-072062459、橋本広大「判批」法学セミナー839号（2024年）128頁。

人が」ということを「名義人本人の意思に基づき」と同視できるとすれば「虚偽」性はないと考えられる、あるいは人を相手に行うなりすましと異なって名義人本人の手足として入力したという評価もありうるともあり、さらに本件においては平成18年決定の事例とは異なり、クレジットカードに付帯する ETC カードをその名義人の権限なく冒用したものでもなければ、実際に通行料金をその自らの信用で割引を受け支払うのは名義人の C である。ETC システムと接続された電子計算機の情報システムが予定するものにおいて、確かに法令・規約による制約（ここではクレジットカード会員利用規約であろう。）はあるものの、実際に ETC を利用して高速道路を通行する者と ETC カードに付帯するクレジットカードの名義人との同一性の確認まで行っているわけではないため、データ入力に対する情報システム外の制約はないといえるので、「虚偽」の情報であるかについて、すなわち電子計算機使用詐欺罪を適用すべき行為であるかについてはさらなる検討の余地があるだろう。

この点、上述した前掲・大阪高判令和６年12月20日以降の類似事件において[62]、大阪地判令和７年１月14日 LEX-DB: 25621843ではカード会員と運転者が生計を同一にする事実婚状態の夫婦であり同乗者もいた事例では、「基本的に被告人 B 及び被告人 D が同居の事実婚の夫婦として同一生計の範囲内で営む消費生活の一部とみることができる……事情の下でされた被告人 D の被告人 B に対する本件 ETC カードの貸与は、そのような関係性のない第三者に対する貸与や、カード名義人が別途発行を受けたカードを包括的な許諾の下に渡した切りにする態様の貸与とは性質が異な」り、「ETC カード使用の際には本人確認のための措置がクレジットカード使用の場合とは異なり厳格にはされていない状況の下で、G 社等が本件各行為のような生計を一にする同居の事実婚の夫婦間での１枚の ETC カードの貸し借りによって使用することまで、不正通行に当たるとして許容してい

62） 松宮・前掲（注61）２頁。

ない旨の周知を十分にしていなかった」として被告人３名の電子計算機使用詐欺罪の成立を否定したものが挙げられる。その射程は、ETC カードの第三者使用を承諾した家族ではあるが同居しておらず生計も同一にしていない事例（大阪地判令和６年10月11日 LEX-DB: 25621914）や、ETC カードの利用を控えるように告げたり離婚後は返還したりように求めたがこれに応じなかったことから承諾のないまま ETC カードが元の配偶者に無断で利用された事例[63]（大阪地判令和７年１月29日 LEX-DB: 25621896）には及ばない旨が判示される。

もちろん、通行料金の潜脱と言う意味では、ETC の有無にかかわらず道路整備特別措置法に基づいて料金を徴収できる道路（道路整備特別措置法24条３項）において、当該道路を通行する緊急車両以外の自動車その他の車両の運転者が、会社または有料道路管理者が定めた通行料金を免脱するなどした場合には30万円以下の罰金に処せられるので（道路整備特別措置法59条）、この罪の成立が認められうることは付言しておく。

③ 誤振込金ネットバンキング送金事例

被告人が誤振込された金4630万円を被告人名義のネットバンキング口座に送金にした行為が、そのネットバンキングの電子計算機に「虚偽の情報」を与えて、オンラインカジノサービスを利用しうる地位という「財産上の不法の利益」を得たとして有罪判決（懲役３年、執行猶予５年）を下した山口地判令和５年２月28日裁判所ウェブサイト・LEX-DB25620093の控訴審[64]である広島高判令和６年６月11日裁判所ウェブサイト・LEX-DB25620093については、その前提となる誤振込に係る預金債権が適法に成立するかが

63） ETC カード利用者およびその運転手は有罪、ETC カード名義人は無罪となっている。

64） 本高裁判決の評釈として、品田智史「判批」新・判例解説 Watch No.211（2024年９月27日掲載）文献番号 z18817009-00-072112506、松原芳博「判評」季刊刑事弁護・無罪判例要旨120号180頁、小池信太郎「判批」刑事法ジャーナル83号（2025年）115頁。さらに、照沼亮介「誤振込にかかる金銭とその法的保護のあり方」法曹時報76巻12号（2024年）２頁も参照。なお、本件は上告中である。

争点となっている。この点、振込依頼人、仕向銀行・被仕向銀行すべてが受取人より早く誤振込の事実を知っていた場合においても、誤振込時における受取人（被告人）の被仕向銀行への告知義務は生じるかについては銀行実務に沿った事務処理を円滑に遂行する必要から、被告人以外が誤振込の事実を知っていたとしても信義則上・社会生活上の条理から「告知義務」はなお否定されないとした。

本判決において示される「当該システムにおいて予定されている事務処理の目的」[65]は、「被告人が情報を入力した電子計算機は、利用者が銀行職員等と対面することなく即時に支払委託や振込依頼を行う手続を支えるものであって、そのような手続を安全円滑に機能させるためには、その利用者は権利行使に当たり告知義務が必要であるなどといった何らかの制限を有していない者であることが当然の前提として求められている」と理解されている。この点について、被告人（受取人）においては振込金組戻承諾書に署名押印する必要があるが、それは「（誤振込の事実の）告知（する）義務」の内容とは必ずしも一致しない[66]と批判されうるし、なによりも、手続の安全円滑な機能を図るためには「告知義務」など利用に制限のある預金債権者であることが当然である理由が明確ではない。それに加えて、その前提となる告知義務の成立根拠に信義則や（社会生活上の）条理を援用すると如何様にも解釈できることになってしまい、処罰範囲を無制約に拡張しうる可能性を有する。そのような意味では、「虚偽性」判断について、それが規範的判断にならざるを得ないことを前提にしても、一般条項や法源としての解釈が分かれるものを援用することは慎重になるべきである。もちろん、本件において振込人が被告人に対して民事上の不当利得返還請求権（民法703条）があることは付言しておく。

65） 品田・前掲（注64）４頁。
66） 松宮・前掲（注61）119頁。

⑷ 暗号資産 NEM と「当該システムにおいて予定されている事務処理の目的」

前節までの電子計算機使用詐欺罪の構成要件要素である「虚偽性」判断において、電子計算機の特徴あるいはその電子計算機およびこれを構成するシステムの社会的意義を広く解釈する傾向が読み取れるように思われる。

さて、本件 NEM に関する特徴は以下のとおりである。すなわち、P2P 技術を用いた分散型管理である以上は NEM に対する単独の管理者を観念できないこと、NEM は NEM 財団による開発ではあるが流通する NEM（XEM）の完全な統制は不可能であること、秘密鍵保有者が当該 NEM にかかる権利を有するのであり、「正規の」保有者なる概念は想定されていないということである。さらに、被告人の公訴事実に記載される当時の事情として[67]、暗号資産交換業者は平成29年 4 月 1 日施行日時点ですでに登録制（資金決済法63条の 2）だったが、未登録業者においては 6 か月の移行措置が認められていたこと[68]、現在ではセキュリティ強化のためにアカウント分散、秘密鍵のオフライン管理（コールドウォレット[69]）、トランザクション実行時に複数の秘密鍵を要求する（マルチシグ）などの措置が行われているところ NEM 流出事件当時はいずれも行われていなかった[70] こと、平成30年当時は暗号資産取引業者には取引業者自身のものと利用者のものを分別管理する義務はあったものの[71]（資金決済法63条の11第 1 項［当時］[72]、仮想通貨交換業者内閣府令20条［当時］）、保有額の 5 %を超える暗号資産のコールドウォ

67） 那須・前掲（注 1 ）229頁。

68） 資金決済法附則 8 条参照。

69） その対概念は「ホットウォレット」と呼び、一般に外部のネットワークと常時接続しているウォレットをいう。ホットウォレットで管理する場合には、サイバー攻撃を受け、秘密鍵を知られ、交換業者が管理するアドレスから攻撃者が管理するアドレスに受託暗号資産を移転させるなどの流出リスクが高いとされる（高橋康文編著、堀天子・森毅 著『新・逐条解説 資金決済法（第 2 版）』（金融財政事情研究会、2023年）426頁脚注 3 。

70） 那須・前掲（注 1 ）229頁。

71） 本条の施行日は平成29年 4 月 1 日である。

72） 現行法では資金決済法63条の11第 2 項前段部分に該当する。

レット管理など[73]、利用者の暗号資産を利用者の保護に欠けるおそれが少ない方法で管理する義務[74]（資金決済法63条の11第２項後段、暗号資産交換業者内閣府令27条）は求められていなかった[75]こと、暗号資産の相場操縦（金融商品取引法185条の24）など金融商品取引法上の規律や、暗号資産取引業者が犯罪収益移転防止法上の特定事業者（２条２項32号）と定められたのは令和２年改正（令和２年４月１日施行）であったことが挙げられる。

本件最高裁判決補足意見は、以上の事情を酌んでいたかは定かではないが、「正規の秘密鍵保有者」というものを前提にした暗号資産 NEM の「社会の信頼」の確保が「虚偽の情報」の判断に一定寄与しているものと考えられる。確かに、システム単体としての仕組みや働き等からロジカルに演繹されるものではないという意味では首肯できるものであるが、その判断要素として「社会経済において果たしている役割や重要性等の観点からの考察」が入り込むとなると、クレジットカード冒用事例における第三者利用禁止条項のような明文の約款がない場合、システム設計者の想定していない内容があったとしても容易に「虚偽」を認定することが可能となって

73） 令和２年暗号資産交換業者内閣府令改正により導入され、令和２年５月１日に施行された。

74） 本条の義務違反に対しては、資金決済法108条５号による罰則（２年以下の拘禁刑もしくは300万円以下の罰金）、115条１号による両罰規定（３億円以下の罰金）が科せられうる。また、必要に応じて内閣総理大臣は立入検査等処分（資金決済法63条の15）や業務改善命令処分（資金決済法63条の16）を発令することが可能であり、これに従わない場合には暗号資産交換業者登録の全部または一部停止処分を命じることができ（資金決済法63条の17）、公告される（資金決済法63条の19）。もちろん暗号資産交換業者に対しては、不法行為に基づく損害賠償責任（民法709条）あるいは利用者との契約不履行に基づく損害賠償責任（民法415条）も考慮される。

上記規定のうち、資金決済法において平成30年当時にあったものは、分別管理義務違反の罪（資金決済法108条２号［当時］）、その両罰規定、内閣総理大臣による立入検査等処分・業務改善命令処分およびこれに従わない場合の業務一部停止または全部停止処分および公告処分（条文番号はすべて同じ）である。

75） その他暗号資産交換業者の利用者は、当該暗号資産交換業者に対して有する暗号資産の移転を目的とする債権に関して先取特権を有する（資金決済法63条の19の２）。このようにして暗号資産交換業者の利用者のリスクをカバーしている。なお、この条文は平成30年当時には存在していなかった。

しまう。ゆえに、虚偽性判断の過程における情報内容の評価ないし法令・規則による制約の中に「社会の信頼」という不明確な概念を持ち込むことは法的安定性・予測可能性に欠けるものとなるだろう。

また、判決理由において繰り返し使用されている「正規の秘密鍵保有者」という表現についても疑問が残るものである。暗号資産（ビットコイン）の設計を示したSatoshi Nakamoto論文[76]では、「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」[77]、とし、そして中央集権的な管理主体によらず取引当事者間で一義的かつ終局的に取引の安全を確保しつつ所有権的支配の移転を可能なものとする[78]が、このデジタル署名の機能性に必要な秘密鍵の秘密保持に関しては言及されていない[79]。この秘密鍵の厳重な管理が暗号資産の取引利用者には求められるところ[80]、あらゆる銘柄の暗号資産に対して当該財産の取引システムにおいて秘密鍵を管理する正規の権限者以外の者が秘密鍵を不正に入手して取引を行うことは想定されていないとするのは早計であろう。なぜなら、当該システムに秘密鍵の保有者の本人性を求めているか否かは別の問題であり、そのような本人性を確認しないシステムであるならば虚偽性判断に大きく影響を与える事情となりうるからである。

また、暗号資産の法的性質については民事判例において争われていたものでもある。東京地判平成27年 8 月 5 日 LEX-DB:25541521では破産にかかる取戻権の判断の前提として、暗号資産ビットコインが所有権の対象はならない旨を判示し、東京地判平成30年 1 月31日金判1539号 8 頁では、「ビッ

76） Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at https://bitcoin.org/bitcoin.pdf（最終アクセス2025年 3 月22日）。

77） Nakamoto, *ibid.* 邦訳は那須・前掲（注 1 ）228頁による。

78） 和田俊憲「仮想通貨・暗号資産と刑法――ビットコインおよびコインチェック事件を題材に」穴沢大輔・佐藤陽子・城下裕二・角田真理子・松原和彦編『消費社会のこれからと法 長井長信先生古稀記念』（信山社，2024年）104頁。

79） 那須・前掲（注 1 ）229頁。

80） 和田・前掲（注78）124頁、那須・前掲（注 1 ）229頁も参照。

トコイン（電磁的記録）を有する者の権利の法的性質については、必ずしも明らかではないが、少なくともビットコインを仮想通貨として認める場合においては、通貨類似の取扱いをすることを求める債権（破産法103条２項１号イの「金銭の支払を目的としない債権」）としての側面を有するものと解され、同債権……は、ビットコイン（電磁的記録）が電子情報処理組織を用いて移転したときは、その性質上、一緒に移転するものと解される」[81] と判示する。また最三小決令和６年10月７日裁時1849号１頁（関連事件１）の原審控訴審である東京高判令和４年６月23日高刑速（令４）号188頁では、「暗号資産である NEM 及び BTC は、通貨である日本銀行券や貨幣とは異なり、日本国内での強制通用力がなく、その移転を目的とする債権は、組織犯罪処罰法13条１項［当時］にいう没収可能な金銭債権には当たらない」とし、仮に暗号資産を没収可能な金銭債権であるとする検察官の解釈を採用した場合、「暗号資産が交換機能を有するのは、あくまでも予め暗号資産を資金決済の手段としで承認した特定の者との間でのみに限られ」ることを前提に、「どの程度まで当該暗号資産が決済手段として社会に受け入れられれば交換機能があり没収可能な金銭債権になるのかを評価すべきこととなるが、その判断は困難であって、金銭債権と非金銭債権との境界、ひいては没収の可否の判断が曖昧で不安定なものとなりかねない」と示していることに

81） 判文中の「仮想通貨」は現行資金決済法上の「暗号資産」と同旨である。なお、当時の「仮想通貨」の定義は資金決済法２条５項［当時］によると、

「一　物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨並びに通貨建資産を除く。次号において同じ。）であって、電子情報処理組織を用いて移転することができるもの、二　不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの」であった。ちなみに現行資金決済法２条14項の「暗号資産」については、１号の「財産的価値」の定義が「電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨、通貨建資産並びに電子決済手段（通貨建資産に該当するものを除く。）を除く」に改正されている。

も留意すべきである[82)]。

上記判決に加えて、事件当時（平成30年 2 月から 3 月）の状況に照らすと、暗号資産（仮想通貨）にかかるセキュリティの態様や法的規律、あるいは暗号資産の法的地位の解釈についての黎明期といえるものであるから、暗号資産の利用者保護の規律が確立される以前の当時の事情を斟酌すべきではないだろうか。また、仮に「正規の秘密鍵保有者」という概念を用いるならば、暗号資産取引所 C の利用者である A がひき逃げ事故により意識不明となってしまい、入院を要する状態となった。A の子である X は、A の入院費に関しては A を被保険者とする任意保険により捻出することはできたが、まだ当該事故の加害者が特定できておらず、A にかかる逸失利益の補填ができていない。また生活費を専ら A の収入から捻出していた。そこで X は、A は暗号資産甲を100単位分 C 取引所に保有していたことを思い出し、A 保有の秘密鍵を用いて当該暗号資産甲100単位をすべて日本円に換価し、生活費の弁済に充てることにした、という事例において、X は「正規の」秘密鍵保有者ではない（あるいはアカウントに「正規」にログインしていない）にもかかわらずトランザクションを行っていることとなるがこの事例の X を電子計算機使用詐欺罪で処罰されるべきか、という問題も残る。

いずれにしても「当該システムにおいて予定されている事務処理の目的」は個別具体的な規範的判断にならざるを得ないところ、本件のようにシステムの技術的特性やそれに対応する立法は行為当時と確定時点で大幅に変化がみられるものであるから、処罰範囲の精緻化・限定化を図るために行

82） ちなみにドイツ刑法では無体物の没収も可能であるため（ドイツ刑法73条 1 項参照）特別法を必要とせずに暗号資産それ自体を没収の対象とすることもできる。例えば BGH 27.07.2017 - 1 StR 412/16では暗号資産についての検討は回避しつつ、Bitcoin を没収対象たりうるとしたことは注目に値する。ただし、暗号資産のままで没収するのかあるいはそれに紐づく支払請求権の差押で実現するのかなど執行可能性に関する議論が残っている。以上の詳細につき、内海朋子「ドイツにおける暗号資産をめぐる議論」只木誠・佐伯仁志・北川佳世子編『甲斐克則先生古稀祝賀論文集［上巻］――刑事法学の新たな挑戦』（成文堂, 2024年）352-353頁参照。

為当時の規律についても積極的に考慮されるべきであるように思う。あるいは暗号資産の銘柄にもよるが、暗号資産にかかる秘密鍵不正取得によってトランザクションをする行為の処罰または制裁についてはその定義も含めて立法による対応が必要なのかもしれない[83)]。

なお本件における攻撃者の行為について、a 社従業員の端末にマルウェアを感染させ外部ネットワークから当該従業員の端末経由で a 社のネットワークに不正にアクセスをした行為については、不正指令電磁的記録供与罪（刑法168条の２）ないし不正アクセス禁止法違反の罪（不正アクセス禁止法３条，11条）の罪が成立しうることは否定しない[84)]。

5．結

電子計算機使用詐欺罪の成立要件として争いのある「虚偽の情報」あるいは「虚偽の電磁的記録」の解釈をめぐっては争いのあったところ、最高裁平成18年決定において「虚偽」性に言及して以来、裁判例においては、虚偽性の判断をめぐって処罰範囲を拡大しうるような規範的判断がなされる傾向にあることが見て取れる。

本判決はそのような中でおよそ「判例」（刑事訴訟法405条）にあたらない補足意見部分ではあるものの、「虚偽」性の判断に言及した点は重要であり、その枠組において重要な示唆がなされている。本判決は、電子計算機使用詐欺罪の構成要件の一部である、「虚偽の情報」と「虚偽の電磁的記録」における「虚偽」性判断において、暗号資産の秘密鍵に対して、設計・管理

83） 和田・前掲（注78）125頁。なお、暗号資産法制に関してはさらなる見直しが行われるとの報道がある（日本経済新聞「仮想通貨、有価証券に準ずる開示規制に 金融庁検討」（2025年２月10日））。

84） 両者の罪の法定刑はいずれも「死刑又は無期若しくは長期四年以上の懲役若しくは禁錮の刑が定められている罪」（組織的犯罪処罰法２条２項１号イ）ではないため、同罪に由来する収益は「犯罪収益」（２条２項）には該当せず、犯罪収益等収受罪（11条）や没収（13条）・追徴（16条）の対象とはならないことに留意されたい。

者あるいは開発者の情報システムにおいて前提とされているもの、あるいは情報内容の評価の過程において、暗号資産 NEM の「社会経済において果たしている役割や重要性等」や「社会的信頼」の要素が示されるが、少なくとも行為当時の状況で判断すべきである。さらに、「社会の信頼」あるいは「社会経済において果たしている役割や重要性等」を考慮要素に入れると、およそ当該システムの設計監理者の予定しない動作に対しても、それを乗り越えて処罰することが可能となる。すなわち、松阪駅キセル乗車事例高裁判決のような入場駅情報を読み取らない形式のシステムであったとしても、「自動改札機一般の“社会経済において果たしている役割や重要性等”」を考慮して処罰することは可能となるし、利用許諾をした自己のクレジットカードをその者に利用させた場合であっても、「クレジットカードにおける“社会経済において果たしている役割や重要性等[85)]”」のもとにおいて虚偽性を認定することも可能である。このような解釈基準は処罰範囲の拡張あるいは不明確化を招く強い懸念を残すものではないだろうか。

85） この場合は「与信」あるいは「信用スコア」のことになるであろうか。なお、「信用スコア」については本年11月下旬より個人による請求で開示することが可能となる（日本経済新聞「自分の信用情報、閲覧可能に　クレジット機関が数値開示」https://www.nikkei.com/article/DGXZQOUB187QG0Y4A710C2000000/．最終アクセス2025年 3 月22日）。