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と刑法246条の２の「虚偽の情報」

（最三小判令和６年７月16日刑集78巻３号113頁）

横　山　裕　一

第１　はじめに

本件は、国内ではトップクラスの額となった暗号資産[(1)]の不正流出に端を発した事件である。暗号資産交換業者がハッキングを受け、顧客の暗号資産NEMの暗号鍵が盗み出されてNEMも流出したとの事案である。本件で取り上げる判例は、ハッキングをして暗号鍵とNEMを直接盗みだした者が被告人ではなく、流出したNEMをそれと知って譲り受けた者が被告人となっている点に注意が必要である。

本件の事件発生から判決までの一連の論理を追うためには、暗号資産（ここではNEM）に関する情報も不可欠であるから、本判決を検討する際に若干の補足を加えることとする。

なお、本稿の本文及び注釈部分に引かれた下線はすべて筆者による。

第２　事案の概要（末尾の図表を参照）

１　被告人は、ダークウェブ上で、氏名不詳のXから暗号資産であるNEMを譲り受けた。被告人がXから譲り受けたNEMは、Xが、A社の保有するNEMの秘密鍵を不正に入手してこの秘密鍵を用い、A社の管理するNEMアドレスからXらの管理するNEMアドレスに移転させたNEMの一部であった（A社からXらの管理するアドレスへ移転させたNEMを「本件NEM」、本件NEMの移転行為を「本件移転行為」という。）。被告人がXから譲り受けたNEMは、本件NEMの一部であった。

２　Xの行った本件移転行為が、刑法246条の２にあたるとし、被告人は、情を知って犯罪行為により得た財産を収受したとして、組織的な犯罪の処罰及び犯罪収益の規制等に関する法律第２条２項１号イ及び同法11条により起訴されたものである。

すなわち、組織的犯罪処罰法第２条柱書は「この法律において「犯罪収益」とは、次に掲げる財産をいう。」とし、同条１項柱書は「財産上の不正な利益を得る目的で犯した次に掲げる罪の犯罪行為（日本国外でした行為であって、当該行為が日本国内において行われたとしたならばこれらの罪に当たり、かつ、当該行為地の法令により罪に当たるものを含む。）により生じ、若しくは当該犯罪行為により得た財産又は当該犯罪行為の報酬として得た財産」とした上で、「イ　死刑又は無期若しくは長期四年以

(1)　従前は仮想通貨と呼ばれることもあったが、令和２年５月１日に施行された資金決済法の改正に基づいて、法律上の呼称は暗号資産で統一されることとなった。

上の懲役若しくは禁錮の刑が定められている罪（ロに掲げる罪及び国際的な協力の下に規制薬物に係る不正行為を助長する行為等の防止を図るための麻薬及び向精神薬取締法等の特例等に関する法律（平成三年法律第九十四号。以下「麻薬特例法」という。）第二条第二項各号に掲げる罪を除く。）」、「ロ　別表第一（第三号を除く。）又は別表第二に掲げる罪」と規定しており、本件では、当時10年以下の懲役刑とされていた電子計算機使用詐欺罪（刑法246条の２）がXに認められるのであれば、被告人には共犯ではなく固有の犯罪として組織的犯罪処罰法違反が成立する。そのため、被告人は、Xのした本件移転行為は刑法246条の２の規定する「虚偽の事実…を与えて」には該当せず、そのため、被告人には組織犯罪処罰法違反は成立しないと主張して争った。

なお、A社が保有していたNEMの暗号鍵が盗み出されたことについて、不正アクセス行為の禁止等に関する法律違反の成立は間違いないものの、その法定刑は最長でも３年以下の懲役刑（現在は拘禁刑）であり、上述のとおり組織的犯罪処罰法の定める懲役４年以上の法定刑という点をクリアできないため、電子計算機器使用詐欺罪で立件するほかなかったと思われる。

３　第１審（東京地判令和４年３月23日）及び控訴審（東京高判令和４年10月25日）はともに、本件移転行為が刑法246条の２の「虚偽の情報」を与える行為に該当するとして、有罪判決を下し、これに対して被告人が上告をしたのが本件である。

なお、弁護側は、秘密鍵の不正取得が不正アクセス防止法違反に該当するため不可罰的事後行為であるとの主張や電子計算機に該当しないとの主張などもあわせて行っているが、本稿では「虚偽の情報」該当性に絞って検討をする。

第３　判決の内容(2)（以下「本判決」という。）

「１　原判決が是認する第１審判決の認定及び記録によれば、被告人が収受した暗号資産（仮想通貨）であるNEMは、氏名不詳者が、不正に入手したA株式会社（以下「A社」という。）のNEMの秘密鍵を用いて、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アドレスに移転させたNEM（以下「本件NEM」という。）の一部であったと認められる（以下、本件NEMの移転行為を「本件移転行為」という。）。そして、NEMの取引においては、取引日時、取引数量、送受信アドレス等の取引に必要な情報（以下「トランザクション情報」という。）を、送信元のNEMアドレスに紐づけられている秘密鍵で署名した上でNEMのネットワークに送信すると、NEMのネットワークを構成するいずれか一つのNISノード（サーバ）が、送信元のNEMアドレスに紐づけられている公開鍵で、署名が秘密鍵によってなされたものであるかを検証し、トランザクション情報の整合性を機械的に確認して、トランザクションを承認し、こうして承認されたトランザクションが、他の承認されたトランザクションとともにまとめて一つのブロックとして生成され、これが順次積み重なりブロックチェーンに組み込まれ、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NEMのネットワーク全体が共有することで、書換えが事実上困難になり、取引が確定するというのである。

(2)　本決定の解説・講評として、品田智史「暗号資産の移転と電子計算機器使用詐欺罪における「虚偽の情報」の意義」ジュリスト増刊1610号122頁、橋爪隆「暗号資産の移転と電子計算機使用詐欺罪の成否」有斐閣有斐閣Online ロージャーナル2024.８.14号、小池信太郎「不正に入手した秘密鍵による暗号資産の移転と電子計算機使用詐欺罪」法学教室531号115頁、山本高子「不正に入手した秘密鍵を使用して暗号資産を送信することが，電子計算機使用詐欺罪の「虚偽の情報」を与えたといえるか」法学セミナー841号122頁、永井善之「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」新・判例解説Watch36号165頁などがある。

２　所論は、氏名不詳者が不正に入手した秘密鍵を用いて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、刑法246条の２にいう「虚偽の情報」を与えたことにならず、本件移転行為は電子計算機使用詐欺罪に該当しないから、本件NEMは、組織的な犯罪の処罰及び犯罪収益の規制等に関する法律（以下「組織的犯罪処罰法」という。）２条２項１号にいう「犯罪行為により得た財産」に当たらず、被告人には、令和４年法律第97号による改正前の組織的犯罪処罰法11条違反の罪（以下「犯罪収益等収受罪」という。）は成立しないと主張する。

３　しかしながら、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。したがって、本件移転行為が電子計算機使用詐欺罪に該当し、本件NEMが組織的犯罪処罰法２条２項１号にいう「犯罪行為により得た財産」に当たるとして、その一部を収受した被告人について、犯罪収益等収受罪の成立を認めた第１審判決を是認した原判断は正当である。

よって、刑訴法414条、396条により、裁判官全員一致の意見で、主文のとおり判決する。」

なお、今崎幸彦裁判官の補足意見(3)が付されており、林道晴裁判官がこれに同調している。

第４　本判決の検討

１　NEMに関する基本的な仕組み

本判決が本件移転行為について「虚偽の情報」に該当することを肯定した理由を検討するにあたって、まずは前提となるNEMの基本的な仕組みについて確認をする。

NEM（なお、通貨単位としてはXEMを用いる。）は、分散型台帳を用いて価値移転を行うブロックチェーンにより構成される暗号資産で、2015年に誕生したものである。台帳はアカウント残高方式で管理され、発行主体を欠く点に特徴がある。ネット

(3)　「私は、法廷意見に賛同するものであるが、上告趣意が、NEMのシステムは、主体情報を認証しないのであるから、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、「虚偽の情報」を与えたことにならないなどと主張していることに関連し、私なりの理解を補足しておきたい。

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。

ワークの実体はNIS（NEM Infrastructure Server）と呼ばれるノード群（NISノード）で、各ノードが台帳の複製を保持し、取引の検証、伝播及びAPI提供を担う。送金は、送金元が宛先アドレス・金額・手数料・任意メッセージ等を含むトランザクションを作成し、秘密鍵で電子署名することから始まる。この署名によりデータの完全性と本人性が形式上担保されることになり、署名済み取引はP2PでNISノードへブロードキャストされ、各ノードが署名の正当性、残高充足、二重支払いの有無、手数料水準や形式適合性を検証し、問題なければ未承認キューであるメモリプールに保持され順にノード群へと伝播されていく。ノードは合意規則に従ってブロックを受理し、台帳が更新され、送金元残高は金額と手数料分減少し、受取人残高は金額分増加する。承認されたブロックが積み上がるほど巻き戻しは現実的に困難となるため、一定数の承認到達をもって事実上の取引の確定と扱われる。

また、他の暗号資産とNEMが特徴的に異なるのは、NEMが暗号資産として立ち上げを開始した際に発行上限枚数をすべて発行しており、以後に新たなNEMが発行されることはないという点である。

以上がNEMの極めて基本的な仕組みとなるが、従来電子計算機使用詐欺罪が適用されてきた事案と大きく異なるのは、NEMは発行主体ないし管理主体を欠く点にあるといえる。NEMは、NEMネットワーク立ち上げ時に発行上限枚数がすべて発行されたことは前述のとおりであるが、この時点でNEMはその秘密鍵を保有する者しか処分を行えない状態となっており、NEMの開発技術者の手を離れてしまっている(4)。また、管理主体の点についていえば、電子計算機使用詐欺罪において「虚偽の情報」を与える対象となるのは電子計算機であるが、NISノードとして稼働している各コンピューターはあくまで当該コンピューターが電気的に稼働していることを管理するのみで、NEMネットワークを管理しているわけではない(5)。このようなNEM及び暗号資産の特徴を踏まえ、氏名不詳Xには電子計算機使用詐欺罪は成立しないとして弁護側が争ったのが本件である。

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。」（下線は筆者による。）

(4)　もちろん、NEMの技術開発者が秘密鍵を取得していないことはありえないが、それはあくまで他の一般的なNEMネットワーク参加者と同様の状態であって、それ以外に何らかの特別な権限が付与されているわけではない。

(5)　ここに述べたNEMの特徴等については、NEMの開発者が作成したとされる技術資料（ホワイトペーパー）を参照。配布場所の一例として、https://nemproject.github.io/nem-docs/pages/Whitepapers/NEM_techRef.pdf。（2025年９月19日閲覧）

２　本判決が「虚偽の情報」にあたると判断したプロセスと「虚偽の情報」に関する前提問題

本判決は、前半部分において事案の骨子及びNEMの仕組みについて概要を述べた上で、「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。」とし、このような事情を前提に、不正に入手した秘密鍵を使用して署名したトランザクション情報の送信は「虚偽の情報」をNISノードにあたえたものであると判示した。すなわち、正規に秘密鍵を保有するものでなければ、署名済みのトランザクション情報を作成することもNISノードに送信することもまた許されないという準則を前提としている。

「虚偽の情報」とは、電子計算機を使用す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であるとされ[(6)]、単に入力された情報が真実に反しているかではなく、当該電子計算機による事務処理の目的に照らし、その内容が真実に反するかを実質的に判断することになる[(7)]。すなわち、単に客観的事実に合致しない情報に限定されるものではなく、電子計算機に与えられた情報と情報を与えた者の法的地位や背景事情なども考量し、情報入力行為によって実現される財産的な処分行為を全体として捉えて、「虚偽の情報」に該当するか否かの実質的判断がされることになろう[(8)]。また、現代の情報技術からすれば、客観的事実に合致しない情報であればシステム的なチェックで処理時に弾くことができるように設計・構築されていることが通常であるから、「虚偽の情報」に該当するか否かが争われる事件の場合には、まさに前述の実質的判断の過程が最も重要となる。本事案でいえば、仮に実際にA社がXのウォレットにNEMの送金を実行するとした場合にNISノードに送信する情報と、本事案においてXがNISノードに送信した情報とはその内容が完全に同一となるはずである。その点では、客観的事実との不一致を理由に「虚偽の情報」に該当するという結論を導き出すことは当然できない。そして、XがNISノードにトランザクション情報を送信した後者の行為のみ「虚偽の情報…を与え」たとされるのは、実質的な判断をすると、後者のみが事務処理の目的に照らしてその内容が真実に反した情報に該当するということになろう。この点について検討する前に、電子計算機使用詐欺罪の代表的な判例についても簡単に紹介をする。

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るなどした行為につき、その入力した情報が「虚偽ノ情報」にあたるとした事案（東京高判平成５年６月29日高刑集46巻２号189頁）では、「本件のような金融実務における

(6)　東京高判平成５年６月29日高集46巻２号189頁。
(7)　大塚仁他『大コンメンタール刑法』第13巻（第３版、青林書院、2018年）181頁。
(8)　後述する最判平成18年２月14日刑集60巻２号165頁についての解説である判タ1207号142頁は、当該判例について「要するに、刑法246条の２にいう「情報」とは、電子計算機に文字通り入力されたクレジットカードの名義人の氏名等のみをいうのではなく、その入力により実現される財産権の得喪に関する処分の内容やその主体等を含むという趣旨に解される。」「クレジットカード会社の約款では、インターネットを介した取引においても、名義人以外の者によるカードの使用は認めておらず…名義人以外によるカードの使用を容認した趣旨ではないと考えられる。」としており、クレジットカード会社の約款の内容が「虚偽の情報」該当性の判断において考量されることに言及している。

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ものと解するのが相当である。」とし、いわば送金を実行するための法的地位や経済的実態を有していたかという社会的事実（特に被告人の事情）を問題としている。また、被告人が、窃取したクレジットカードの番号等を冒用し、インターネットを介してクレジットカード決済代行業者の電子計算機に本件クレジットカードの名義人氏名等を入力送信して電子マネーの購入を申し込んだとの事案（最決平成18年２月14日刑集60巻２号165頁）でも、「カード名義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」たとしており、カード会社の約款により通常禁止されているカード名義人ではない者によるクレジットカードの使用という事情を重視していると思われる。(9)

これらの判例によれば、犯人によって入力された外観上の情報自体は客観的事実に合致しているとしても、電子計算機に入力された情報を処理して財産的処分行為を行う者において、その情報の利用態様を明確に禁止し又は利用態様の実態を知っていれば当然に財産処分行為を完了させなかったであろう場合に、「虚偽の情報」に該当するとの判断がなされているいえるだろう。そして、電子計算機使用詐欺罪を規定する刑法246条の２の冒頭に「前条に規定するもののほか」とあるように同罪が体系上246条の詐欺罪の補充規定であること(10)を前提に考えた場合、電子計算機使用詐欺罪における「虚偽の情報」と詐欺罪の欺罔行為に共通する部分があるのではないかとも考えられる。すなわち、暴力団関係者の利用を拒絶しているゴルフ場において暴力団関係者であることを申告せずに利用申込みをした行為について、最判平成26年３月28日刑集68巻３号582頁の事案では欺罔行為には当たらないとし、同日刑集68巻３号646頁の事案では欺罔行為に当たるとされた。類似の２つの事案において両者の結論を左右したのは、特にゴルフ場施設が暴力団員でないことの確認を厳格にしていたか否かにあるとされている。(11)(12)これまで述べてきた「虚偽の情報」該当性判断には実質的判断が求められること、本段落で述べた財産的処分行為を行う者において、その情報の利用態様を明確に禁止し又は利用態様の実態を知っていれば当然に財産処分行為を完了させなかったであろう場合に、「虚偽の情報」に該当することとも平仄が合う。

3　本判決の内容について

本判決について従前の判例の傾向を踏まえて改めて検討をすると、「虚偽の情報」に該当するか否かは、NEMネットワークにおいてNISノードに送信された情報をどのように取り扱うべきかの準則から検討をすべきこととなる。前記クレジットカード冒用事例に則して考えれば、クレジットカード会社の

(9)　前掲注(8)参照。カード名義人以外者のカード使用を禁止しているということは、クレジットカード上に記載された情報を入力してカードを使用する行為は、使用者がカード名義人本人であるとの情報を入力しているのと同義であるとも説明できる。藤井敏明「判解」最判解刑事編平成18年度63頁も、「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」と説明している。

(10)　前掲注(7)・大塚179頁。

(11)　法律時報87巻４号121頁（2015年）は、被告人のゴルフ場施設利用申込み行為が欺罔行為に当たらないとした事案について、周辺のゴルフ場において、本件各ゴルフ場と同様に暴力団関係者の施設利用を拒絶する旨の立て看板等を設置し暴力団排除活動を推進しながらも、実際には暴力団関係者の施設利用を許可又は黙認する例が複数あり、ゴルフ場の利用客は当然に暴力団関係者でないといえる状況になかったことが重視されたと指摘する。

(12)　法律時報87巻４号123頁（2015年）は、ゴルフ場施設利用申込み行為が欺罔行為に該当するとした事案について、入会契約に際して、暴力団関係者等を同伴・紹介しない旨の誓約をしている点を重視し、前者の事案とは異なり、入会時の当該誓約を前提とする個別の施設利用申込みは、その同伴者が暴力団員ではないことを保証する意思をも黙示的に表示しているものと認められると指摘している。

約款に相当するNEMの準則・約款等があればその内容から検討することになろう。ところが、NEMの公式ドキュメントには、主に技術的な資料とポリシーが掲げられているのみで、いわゆる規約にあたるものは存在しない[13][14]。いわば、「虚偽の情報」と疑われる情報を入力された側の事情で考量できるものがないことになる。そのため、「虚偽の情報」に該当するか否かは別のアプローチにより判断基準を立てなければならないことになる。本判決の特徴は、この点にあると考えられる。

改めて法廷意見である判決理由をみると、「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。」とするが、必ずしも自明の理屈ではない。秘密鍵による暗号化を必要としない暗号資産は暗号資産たり得ず、ブロックチェーン技術を用いた暗号資産の特性上、秘密鍵によらなければトランザクションができないという仕組みを組み込むことは技術上の必然に過ぎない。取引管理をする中央集権的なシステムが存在しない以上は、正しい秘密鍵さえ所持していれば当該NEMを如何様にも処分することができるというだけであって、その点だけを見れば「虚偽の情報」ではなく真実の情報とも評価できる。「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」という判例の文言も、暗号資産の仕組み上正しい秘密鍵で署名しなければ取引が承認されないという技術的な説明を改めてしているだけであって、そのような技術の存在が、なぜ法解釈として正規に秘密鍵を保有していることと繋がるのか説明がなされていない。たとえば、『鍵穴と鍵が一致しなければ解錠できないから、解錠行為は、正規に鍵を保有していることの確認のために求められるもの』との説明に一定の理解が得られるのは、解錠に用いられる鍵が極めて重要な物であり、おいそれと他人に預けるような性質のものではないこと、他人に解錠された場合に中の貴重品が奪われるなどの重大な被害が生じうることが説明不要なレベルでの経験則となっているからであろう。ところが、本事案はブロックチェーン技術と「虚偽の情報」という先鋭且つ新しい議論の場面であり、どのような経験則が働くのかは必ずしも自明ではない。弁護人も、クレジットカード冒用事例（及びその調査官解説）を挙げて、同事案における約款に相当する準則がないため、トランザクション情報の送信は、正規に秘密鍵を保有するものがであるとの情報までを含めて送信したことにはならない旨主張している。そのため、NEMの技術的な仕組みと結論との間には、より詳細な説明が求められる場面であると思われる。

この点については、今崎幸彦裁判官が補足意見で

(13)　技術資料を含むNEMに関する情報の公開サイトの一例として、https://nemproject.github.io/nem-docs/pages/。（2025年９月19日閲覧）

(14)　なお、弁護人は、上告趣意書の第４において同様の主張をしている。「その理由は、平成18年裁決の決定書からは明らかではないが、同決定の調査官解説によれば、「一般にクレジットカード会社の約款では、会員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、お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」という約款の存在を重要な理由としていた。もし、一般にクレジットカードの利用を会員本人に限る約款が存在しないような場合には、クレジットカードの利用をするために「カードの名義人氏名、番号、有効期限」のみを送信したことをもって、「名義人本人が申し込んだとする虚偽の情報」を送信したとは言えないと解される。」（原文ママ）

理由を述べている。すなわち、資金決済法が暗号資産交換業者に対して利用者保護のための規制を設け、（本件後ではあるものの）金融商品取引法が暗号資産の不公正取引を規制していることを挙げた上で、「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。」とし、単に技術的な側面からのみアプローチするのではなく、また、利用者間の事情[15]からのアプローチでもなく、社会におけるNEMの役割や機能からのアプローチという方法で「虚偽の情報」該当性を導き出している。そして、「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。」として、NEMシステムに対する社会の信頼は、トランザクション情報への署名が正規に秘密鍵を保有している者によって行われていることによって支えられているとの趣旨を示している。有体物ではないもののNEMに財産的価値があることそれ自体は社会的に認められているといえるため、NEMの正当な権利者が、これを第三者に領得された場合は領得者に刑事的な非難がなされて然るべきという考え方は正当であろう。しかしながら、ここでも「NEMシステムに対する社会の信頼」が果たしてブロックチェーン技術を前提とする場合にも妥当するのかという疑問はなお残る。すなわち、これが電子マネーやポイントの決済システムに対する信頼というのであれば、その背後に当該システムを構築した企業等に対する信頼や責任追及の余地が存在するのに対して、NEMシステムに代表されるブロックチェーン技術においては中央集権的なシステムは存在せず、技術的なルールに従って淡々と処理されるのみであり、そこに人の意思が介在する余地はない。このような仕組みは、NEMネットワークに参加する者のうち多数の者が認識しているだろうし、ブロックチェーン技術（NEMシステム）に対して、正規の秘密鍵保有者以外のトランザクション情報の送信及び処理がなされないシステムであることまでは期待していないのではなかろうか。裏を返せば、NEMネットワーク参加者が信頼しているのは、正しい秘密鍵さえ持っていれば確実にNEMの移転ができる（持っていなければ移転は絶対に不可能）という確かな技術的裏付けなのではないのかということである。補足意見が、このような事情も踏まえた上でNEMのシステムに対する社会の信頼を論じているかは判然としない。あくまで補足意見のレベルでの表現ではあるが、将来同種同様の事案が発生した際には、法廷意見として議論が深掘りされることを望む。

仮に本件が「虚偽の情報」に当たらないとした場合、財産的価値のあるNEMをその権利者たるAの意に反して自己に移転させたXの行為に、民事上の責任追及は別として、刑法上いかなる犯罪が成立するだろうか。このような観点からも、すでに個人においても保有が浸透している暗号資産について、

（15）　もっとも、前述のクレジットカード冒用事例のような被告人と決済代行会社といった双方当事者を観念することはそもそも著しく困難又は不可能である。NEMネットワーク自体は管理者が存在しておらず、被告人が送信したトランザクション情報を受け取り管理する法人ないし自然人を観念できないからである。

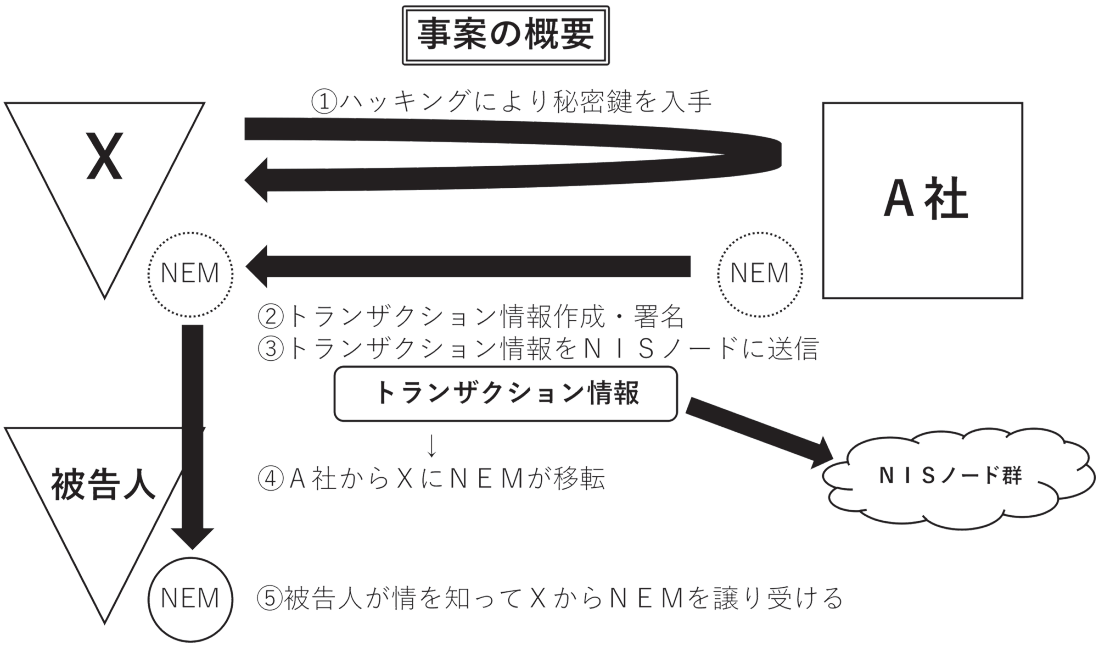
刑事上の保護を及ぼそうとする本判決及び今崎裁判官の補足意見は、結論の妥当性という点では極めて正当であるといえるため、「虚偽の情報」に該当する理由についての議論は今後も引き続き進めていかなければならないと考える。

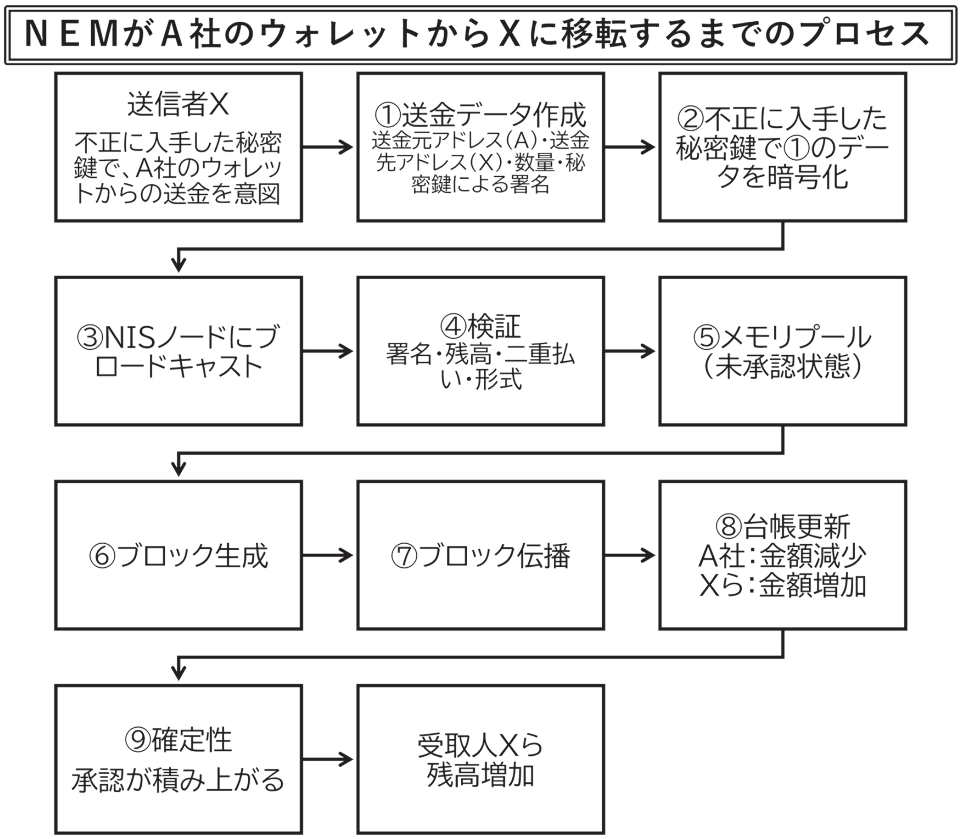
なお、暗号資産を取引所（暗号資産交換業者）で管理している場合、秘密鍵も取引所において管理されることが通常であるため、不正に入手した他人のログイン情報を用いて取引所にログインして自己又は第三者に暗号資産を移転する操作を行った場合には、平成18年決定と同様の理由で電子計算機使用詐欺罪が成立することになろう。最決令和元年９月９日LEX文献番号25564294は、被告人が、金品等を奪った上で被害者を殺害し、奪ったノートに記載されていたログイン情報を使用して暗号資産交換業者のサーバーコンピュータにログインして、被害者の口座内のビットコインを被告人の口座に送信する旨の情報を与えたことが「虚偽の情報」にあたるとして、被告人に電子計算機使用詐欺罪を成立させた事案である。

第５　今後の検討課題

これまでみてきたとおり、不正に入手した秘密鍵を使用してトランザクション情報に署名をした上で、NEMを移転させるために当該トランザクション情報をNISノードに送信した行為は、NISノードに対して「虚偽の情報」を与えたことになるというのが本判決の結論であるものの、その理由付けに関してはなお深掘りをする余地が残されているように思われる。多くの暗号資産が類似の仕組みを利用していることから、今後同様の事件が起こった場合、暗号資産の仕組みが同様であれば、裁判所の判断もまた同様となるはずであるため、新たな判例の登場を待ちつつも本判決に対する検討を更に進めたい。今後、仕組みの異なる暗号資産が問題となった場合や、NFTのように同じくブロックチェーン技術を利用しているが異なる目的でシステムが構築されている技術についても適用されるのかなど、類似のテクノロジーの事案における取扱いについても、同様に検討を進める次第である。

以上





本判決は、①②を前提に、③の行為により「虚偽の情報」を与えたとする。