サイバー犯罪の研究（七）-オンライン詐欺に関する事例検討-

法律論叢第87巻第1号（2014.8）

【論　説】

サイバー犯罪の研究（七）

――オンライン詐欺に関する事例検討――

夏　井　高　人

目　次

一　はじめに

サイバー犯罪に限らず、被害者を欺罔し、いわば被害者自身を間接正犯の道具として財物や財産上の利益を違法に取得する詐欺行為（刑法246条1項、2項）は、比較的ありふれた犯罪類型の一つに属する。

被害者に対する欺罔行為、その欺罔行為に基づく被害者の錯誤（判断誤り）、その錯誤に基づく被害者による財物の交付または財産上の利益の提供を必須の犯罪構成要件要素とする。このことから、財物や財産上の利益以外の情報または情報

財(1)の取得を目的とする詐欺的行為（フィッシングやSCAMなど）と区別され、また、欺罔されることも錯誤に陥ることもない電子計算機に対する財産上の利益取得行為である電子計算機使用詐欺罪（同法246条の2）及び同様に欺罔されることも錯誤に陥ることもない機械装置や電子計算機に対する財物取得行為である窃盗罪（同法235条）と区別される(2)。

このような構成要件要素を充足する限り、詐欺行為の手段としての欺罔行為に限定はない。インターネットを含め、電子的な通信手段を用いた欺罔行為は、現時点では比較的ありふれたものとなっている(3)。このような電子的な通信手段を用いた欺罔行為は、インターネットが普及する以前のパソコン通信時代から存在した。

本論文では、サイバー犯罪の研究（一）～（六）で論じてきたところを踏まえ、情報通信技術を犯罪の手段として用いる詐欺行為について、日本の裁判事例を素材にして、類型論的な考察を試みる。なお、本論文で検討対象にする事例は網羅的なものではない。

二　公衆通信サービスと関連する事例

1　パソコン通信の事例

日本国において、インターネット普及以前に主流となっていた情報通信サービスは、ニフティサーブ（現在のニフティ株式会社が運営する@nifty）、PC-VAN（現在のビッグローブ株式会社が運営するBIGLOBE）、mixiといったパソコン通信だった。この種の通信サービスでは、現在のFacebook等のソーシャルメディア

(1) 情報財の概念定義については、夏井高人「情報財—法概念としての意義」明治大学社会科学研究所紀要52巻2号213～241頁で詳論した。

(2) 詐欺及び詐欺類似犯罪との区別等については、夏井高人「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86巻1号61～110頁で詳論した。

(3) 警察庁によって認知された検挙人員については毎年その統計結果が公表されている。例えば、警察庁「平成25年中のサイバー犯罪の検挙状況等について」（平成26年3月27日）によれば、平成25年中に検挙されたサイバー犯罪事例総数8113件中で詐欺罪に該当するものは956件であり、全体の中に占める割合は約11.8パーセントとなっている。また、電子計算機使用詐欺罪の件数は388件となっており、詐欺罪と電子計算機使用詐欺罪の件数の合計1344件は全体の約16.6パーセントを占めている。

（またはSNS）において提供されるサービスと同様に、一定の限られた利用者間での電子メール送受信、オンラインチャット、電子掲示板（BBS）等のサービスが提供されていた。

これらパソコン通信で提供される各種サービスの中で、電子メールを用いるものとオンラインチャットを用いるものは、原則として特定個人間の通信を用いるものであるが、このような通信手段は、欺罔のための手段として用いられているのみであり、財物の交付（財産上の利益の移転）は別の送金手段（口座振込、宅配便による送付等）を利用する点で、通常の郵便書簡や電話等を欺罔行為の手段として用いた詐欺行為と基本的には何ら変わるものではないと考えることができる。この点では、携帯電話等を用いて欺罔し、口座振込や宅配便による現金の送付を受けることにより既遂に達する「振り込め詐欺」と呼ばれるタイプの詐欺事犯等でも同じである。

これに対し、パソコン通信で提供される各種サービスの中で、電子掲示板を欺罔行為の手段として用いた詐欺行為は、原則として不特定多数人間の通信を用いるものであり、通常の郵便書簡や電話等を欺罔行為の手段として用いる詐欺行為とは若干異なる性質を有する。後者のようなタイプの犯罪類型は、インターネットが普及した後に盛んとなったネットオークションを欺罔行為の手段として用いた詐欺行為と類似する点がある。ただし、パソコン通信が主流であった時代においては、財物の交付（財産上の利益の移転）は別の送金手段（口座振込、宅配便による送付等）を利用するのが通例で、それゆえに通常の詐欺罪（刑法246条）が成立するのが一般的であったのに対し、インターネットが普及した後の時代のネットオークション詐欺では、競り落としとほぼ同時に電子的な決済が自動的に実行され、財産上不法の利益の取得が同時に実行されるのが一般的であることから、刑法246条2項の詐欺罪が成立するのが普通である点が異なっている(4)。

(4) 通常は、人間の被害者が欺罔され、その欺罔により錯誤に陥った被害者による競り落とし行為とネット上での電子決済を実行することによって成立する犯罪類型であることから、詐欺罪（刑法246条2項）が成立する。しかしながら、比較的近い将来、人間ではないロボット（物理装置としてのロボットの場合とネット上のコンピュータソフトウェアとしてのロボットの場合との両者を含む。）がネットオークションの利用者として登場することが考えられる。この場合、競り落とし行為とネット上での電子決済は当該ロボットに記録されたコンピュータプログラムにより自動実行され、かつ、これが欺罔され錯誤に陥ることはないので、詐欺罪は成立しない。このロボットの事例において、民

パソコン通信サービスを用いて実行された詐欺事例は、実際には多数存在したと推定される。しかし、公刊された判例集等で検索可能な事例としては、ニフティサーブの電子掲示板サービスを欺罔行為の手段として用いた事例（京都地裁平成9年5月9日判決・判例時報1613号157頁）が1件あるのみである(5)。

同判決では、パソコン通信サービス・ニフティサーブで提供される電子掲示板サービスを欺罔行為の一部として利用して詐欺を実行したという事案について、被告人を有罪として懲役2年・保護観察付執行猶予3年（求刑・懲役2年）の刑が宣告された。

同判決における「罪となるべき事実」は、次のとおりである（関係者名等は一部仮名、住所等は一部省略）。

（罪となるべき事実）

被告人は

事上では、ロボットの保有者について、不法行為（民法709条）に基づく損害賠償請求権が成立し得ることは明らかであるが、それは、ロボットによる取引行為の適正さに対する侵害行為として理解されるべきものであり、ロボットに対する欺罔行為なるものを肯定する根拠となるものではない。このような事案については、刑法上の解釈論としては、電子計算機使用詐欺罪を考えることが可能である。ただし、加害者において、被害者が生きた人間であるのか機械装置またはソフトウェアとしてのロボットであるかを判別する方法が存在しないので、故意論としては非常に難しい問題が伏在している。現時点での仮の結論としては、生きた人間であれば詐欺罪としての故意とロボットであれば電子計算機使用詐欺罪としての故意とが混在した包括的な故意があると認定する以外にないのではないかと考えるが、事案によっては故意を阻却すべき場合があり得る。このようなタイプの検討課題は、実は既に現実に存在している。例えば、現在の証券取引の大半はソフトウェア対ソフトウェアというかたちで相互に自動実行されている。その一方が詐欺的な電子取引を実行している場合、包括的な故意としてどのようなものを考えるべきかにより、事案のとらえ方に相違が生ずるであろう。要は、現実社会において、生きた人間が実際に活動している領域が次第に減少してきており、とりわけ高速処理を要する分野ではほとんど全部の処理が生きた人間の介在なしに電子的な自動処理によってまかなわれているという現実を直視して法理論を再構築しようとするかしないかという法解釈学上の態度決定のいかんにかかっていると認めるべきである。このような問題に関して、興味ある示唆を含むものとして、Ugo Pagallo, The Law of Robots – Crimes, Contracts and Torts, Springer, 2013及びMichel Dion, Financial Crimes and Existential Philosophy, Springer, 2014が参考になる。

(5) 判例評釈として、島岡まな「パソコン通信を利用した詐欺罪およびホストコンピュータ上に登録されたデータ変更に私電磁的記録不正作出罪が認められた事例」判例時報1667号223頁（判例評論483号61頁）、原島　肇「ニフティサーブ電子掲示板詐欺事件」別冊NBL79号サイバー法判例解説102頁がある。

第1　平成8年1月23日ころ、埼玉県富士見市所在のA方において、行使の目的をもって、ほしいままに、かねてから入手していたあさひ銀行の普通預金（兼総合口座）申込書（入金票）のおなまえ欄に「B」と署名するとともに、おところ欄に「東京都渋谷区（略）」、生年月日欄に「47、5、17」、お勤め欄に「フリーター」、口座開設ご希望店欄に「渋谷」などと記入し、もって、B名義の右申込書1通を偽造した上、同月24日ころ、これを真正に成立したもののように装って、埼玉県浦和市所在の同銀行ポストサービス係に郵送し、そのころ、情を知らない同係係員をして、右申込書を東京都渋谷区渋谷2丁目20番11号所在の同銀行渋谷支店に送付させ、同年2月1日ころ、同支店に到着させて行使し、

第2　平成8年2月下旬ころから3月初旬ころまでの間、前記A方において、行使の目的をもって、ほしいままに、かねてから入手していた第一勧業銀行の普通預金新約申込書用紙のおなまえ欄に「C」と署名するとともに、生年月日欄に「47、4、2」、おところ欄に「渋谷区（略）」、お勤め先欄に「フリーランサー」、口座開設希望店欄に「渋谷」などと記入し、もって、C名義の普通預金新約申込書1通を偽造した上、そのころ、これを真正に成立したもののように装って、千葉県印西市所在の第一勧業銀行マイバンクセンターS係に郵送し、情を知らない同係係員をして、右申込書を東京都渋谷区宇田川町23番2号所在の同銀行渋谷支店に送付させ、同年3月14日ころ、同支店に到達させて行使し、

第3　売買代金名下に金銭を詐取しようと企て、平成8年4月13日ころ、真実は、パソコン部品を売り渡す意思がないのにこれがあるかのように装い、パソコン通信サービス「ニフティサーブ」（以下単に「ニフティ」という。）の電子掲示板に、右ニフティ会員のCであるかの如く装って、C名義で、「今回もパーツうります。ペンチアムCPUとSIMMをまとめ買いすると1個が破格のお値段でかえるのです。購入方法は、どのパーツも、手付け金¥10000を先にしはらい、残りのお金は品物到着時に郵便やさんに払います。」などと虚偽の情報を書き込んだ上、別紙一覧表一記載のとおり、同日ころから同月17日ころまでの間に、右掲示板を閲覧して問い合せをしたDほか2名に対し、売買代金あるいは手付け金を支払えば、注文にかかるパソコン部品を郵送する旨の虚偽の内容の電子メールを送信し、同人らをしてその旨誤信させ、よって、同月15日から同月17日までの間に、前後3回にわたり、前記第一勧業銀行渋谷支店のC名義の普通預金口座に合計74万4390円の振込入金を受け、もって、人を欺いて金銭を交付させ、

第4　パソコン通信サービス「ニフティサーブ」を提供するニフティ株式会社の事務処理を誤らせる目的で、ほしいままに

1　平成8年3月27日ころ、前記A方において、被告人所有のパーソナルコンピューター（以下、単に「パソコン」という。）を操作し、東京都大田区所在の富士通株式会社情報処理システムラボラトリ内のコンピューターに、電話回線を通じて、前記ニフティ会員のCの住所が「埼玉県入間市（略）」から「東京都渋谷区（略）」に、電話

番号が「0429（略）」から「03（略）」にそれぞれ変更された旨の虚偽の情報を送信し、情を知らない右ニフティ株式会社メンバーサービス部係員をして、その旨の情報を、東京都品川区《番地略》所在の大森ベルポートA館ニフティ株式会社経営情報システム部内に設置されたコンピューターの記憶装置内の「顧客データベースファイル」に記憶させ、もって、事実証明に関する電磁的記録を不正に作出し、

2　平成8年4月18日ころ、前記A方において、被告人所有のパソコンを操作し、前記富士通株式会社情報処理システムラボラトリ内のコンピューターに、電話回線を通じて、前記Cの住所が「東京都渋谷区（略）」から「愛知県名古屋市（略）」に、電話番号が「03（略）」から「052（略）」にそれぞれ変更された旨の虚偽の情報を発信し、情を知らない右ニフティ株式会社メンバーサービス部係員をして、その旨の情報を、前記ニフティ株式会社経営情報システム部内に設置されたコンピューターの記憶装置内の「顧客データベースファイル」に記憶させ、もって、事実証明に関する電磁的記録を不正に作出し、

第5　売買代金名下に金銭を詐取しようと企て、平成8年4月13日ころ、真実は、パソコン部品を売り渡す意思がないのにこれがあるかのように装い、前記ニフティの電子掲示板に、右ニフティ会員のCであるかの如く装って、C名義で、「今回もパーツうります。ペンチアムCPUとSIMMをまとめ買いすると一個が破格のお値段でかえるのです。購入方法は、どのパーツも、手付け金¥10000を先にしはらい、残りのお金は品物到着時に郵便やさんに払います。」などと虚偽の情報を書き込んだ上、別紙一覧表二記載のとおり、同日ころから同月15日ころまでの間に、右掲示板を閲覧して問い合せをしたEほか2名に対し、手付け金を支払えば、注文にかかるパソコン部品を郵送する旨の虚偽の内容の電子メールを送信するなどし、同人らをしてその旨誤信させ、よって、同月15日から同月17日ころまでの間に、前後3回にわたり、前記第一勧業銀行渋谷支店のC名義の普通預金口座に合計12万円の振込入金を受け、もって、人を欺いて金銭を交付させたものである。

事案の流れを簡単に整理すると、被告人は、①詐取する代金名目の金銭の振込送金先口座として、予め第一勧業銀行にC名義の預金口座を開設しておき（有印私文書偽造、同行使罪）、②実在するCになりすまし、ニフティサーブの電子掲示板サービスを用いて虚偽のパソコン部品販売を掲示し、その掲示板の内容によって欺罔された被害者らから代金等の振込送金を受けて金員を詐取し（詐欺罪）、③詐欺事犯の発覚を免れるため、実在するCのニフティサーブの会員登録情報（住所・電話番号）を無権限で修正した上で（電磁的記録不正作出罪）、更に、④実在するCになりすまし、ニフティサーブの電子掲示板サービスを用いて虚偽のパソコン部

品販売を掲示し、その掲示板の内容によって欺罔された被害者らから代金等の振込送金を受けて金員を詐取し、そして、⑤警察の捜査を免れるため、実在するCのニフティサーブの会員登録情報（住所・電話番号）を無権限で再度修正した（電磁的記録不正作出罪）という事案である。要するに、詐欺行為のための欺罔行為の手段としての電子掲示板への虚偽の販売情報の書き込み行為[6]は2度行われたことになる[7]。なお、Cのニフティサーブ・アカウントを被告人が無権限で取得し、これを無権限で使用してニフティサーブのシステムにアクセスした点は、現時点では不正アクセス行為として処罰対象となり得るが、本件発生時点では不正アクセス行為の禁止等に関する法律（平成11年8月13日法律第128号・最終改正平成25年

(6) 民法上では、電子掲示板上での購入者の勧誘のための書き込みは、契約の申込みの誘引に該当し、契約の申込の意思表示ではない場合が多い。本件事案においても、ニフティサーブの電子掲示板上の書き込み表示を読んだ被害者らが電子メールにより加害者と連絡をとった上で売買契約を締結している。このことから、厳密には、被害者と加害者間での電子メールのやりとりは、途中までが契約交渉過程に該当し、最終的な妥結の電子メール送受信により売買契約が締結されたと理解するのが正しい。ただし、刑事実務上においてこのような解析的・分析的な考察がなされたり、それを踏まえた公訴の提起がなされたりすることはほぼ皆無であり、一般的には、契約の申込の誘引の段階で詐欺行為の実行の着手があったものとされている。本件事案に即して換言すると、詐欺の故意に基づいて電子掲示板への契約の申込の誘引である書き込みが実行されれば、詐欺罪の構成要件の一部である欺罔行為が実行されたことになると解するのが通例である。これらの点について、民法上の詐欺と刑法上の詐欺罪との相違を明確に意識し、その点を分析する内容の研究成果はないのではないかと思われる。なお、電子商取引としての契約の成立時期に関しては、経済産業省「電子商取引に関する準則（平成25年9月）」中にある「I-1 オンライン契約の申込みと承諾」が参考になる。また、強行法規違反であるがゆえに無効となる法律行為との関連で不当利得を論ずるものとして、伊藤　進「私法規律の構造（二）—強行法規の効力・その効力構造（下）」法律論叢86巻6号69～128頁がある。

(7) 民事上では、詐欺による意思表示は取消すことのできるものであり、取消しがなされるまでは有効である（民法96条1項）。本件に即して言うと、ニフティサーブの電子掲示板の書き込みを信じて送金した被害者が取消しの意思表示をしなければ、民法上では詐欺とならないので、刑法上も詐欺罪は成立しない。しかし、詐欺による意思表示は、同時に、要素に錯誤のある意思表示でもあり、かつ、欺罔された表意者には通常は重大な過失があるとは考えられないから、その意思表示は錯誤により無効となる（民法95条）。それゆえ、欺罔された被害者が詐欺罪により告訴する場合には、加害者に対して意思表示の取消しをしなくても当該意思表示は無効となる。すると、実際には、民法に規定する詐欺取消の条項が機能する場面はほとんどないということが可能である。現実の警察実務においても、詐欺取消がなされたか否かを問わず、告訴があれば詐欺被疑事件として立件し捜査を開始するのが通例である。なお、詐欺取消や錯誤により無効となった意思表示に基づいて提供された金員は不当利得となり、その返還請求をなし得る（民法703条）。

5月31日）が制定されていなかったため、無罪となる。

同判決は、量刑の事情として、次のように判示している。

（量刑の理由）

本件各犯行は、被告人がいわゆるパソコン通信の大手サーバーである「ニフティサーブ」の電子掲示板等に他人名義で虚偽の情報を書き込むなどし、偽造の申込書を用いて開設した他人名義の口座に右情報を閲覧した者からパソコン部品代金名下に振込送金を受けてこれを騙取し、さらに、右詐欺事犯の発覚を免れるため、パソコン通信のホストコンピューター上に登録された他人の住所等を無断で変更するなどしたという事案である。

すなわち、被告人は、パソコン通信のネットを通じて「F」なる人物から他人名義の架空口座の作り方（郵送による銀行口座開設の申込みを行う方法を使うと銀行からの身分証明書の確認を免れることができる。私書箱を開設して住所とすれば他人名義で容易に架空口座が開設できるということ）やニフティ会員の入会時の情報（クレジットカード情報、ID及び仮パスワード）を教えてもらったり、自らプログラムしていたハッキングソフト（GOMENBER.LSTに記載されたニフティの会員情報をもとに会員のパスワードを解析するソフト）を利用して、他人のパスワードを探り当てたりしていたが、これらを利用してニフティ会員になりすまして売買名下に金員を騙し取ろうと考えるようになり、①私書箱業者を利用して架空の住所を設定して、右住所で実在する他人名義の銀行口座開設申込書を偽造して口座を開設し（本件第1、第2の事実）、②ニフティのホストコンピューターに保存されている会員の住所情報を右架空の住所に変更したうえ（判示第4の1の事実）、③他人のパスワードを使ってニフティ内に勝手に潜り込み、ニフティが会員に提供する電子掲示板に実在する会員名義でパソコンのCPUとメモリーを売るなどと嘘の情報を掲載し、この情報を閲覧して申込みをしてきた被害者らに対し、さらに商品を確実に送付する、代金等は前記口座に入金して欲しいなどの電子メールを送信するなどして、被害者から右口座に振込送金を受けて代金名下に86万円余を騙取した（判示第3及び第5の各事実）。④その後、被害者らからの追及や警察の捜査を免れるため、前記ホストコンピューターの前記住所情報を私書箱業者の住所から別の住所に変更するなどした（判示第4の2）というのである。

このように、本件各犯行は、パソコンやパソコン通信に精通した被告人が中学生の頃から培ってきたコンピュータープログラミングの知識や、パソコン通信を通じて得た犯罪紛いのいわゆる裏情報をもとに、パソコン通信あるいはインターネット上の情報を容易に信用して売買が行われている現状、サーバー側のホストコンピューターから非公開の会員情報が入手可能な状態であること、会員自身により設定されたパスワード自体も氏名や生年月日等から容易に推測可能なものが多いこと、銀行の口座開設についてもその身分確認を擦り抜ける方法があること等、パソコン通信ないしこれに付

随するシステムの弱点に付け込んで、コンピューター上に勝手に偽りの情報を書込むなどし、結局不特定多数の被害者から多額の金員をだまし取ったという非常に狡猾かつ計画的犯行で、犯行態様は非常に悪質である。

また、本件各犯行は、判示の手口により、パソコン通信上で他人の名前をかたって虚偽の情報を流布し不特定多数人から詐欺したという点において、情報ネットワークの発展やパソコンの益々の普及に伴い今後増加が予測される犯行形態であるうえ、IDとパスワードの一致のみで個人を識別するというパソコン通信の匿名性を利用し、前記の弱点を利用して周到な準備をし、犯人の特定を非常に困難にしたという点において、捜査が困難で模倣性が高い犯行形態といわなければならず、一般予防の見地からも重い処罰が必要な犯罪である。

以上のような事情に加え、被告人は本件詐欺も併せ同じ手口で少なくとも700万円近く手に入れていることなどまさに営業犯的犯行といわざるをえないこと等を併せ考慮すると、本件各犯行についての被告人の刑事責任は重いというべきである。

被告人は、中学生のころからコンピュータープログラミングを、大学生のころからパソコン通信を始めるようになり、パソコン雑誌等でのアルバイト等を通じて、前記のように、パソコンに精通するようになったものであるが、本件各犯行当時は、犯行発覚の端緒となった会社の同僚以外には親しい友人もなく、パソコン通信上で名前も性別もわからない犯罪紛いの行為を行っている者らとの交流を中心に生活してきたものであって、今後の交遊関係によっては再犯可能性は否定できない。また、現状では被告人の近親者もパソコンを用いた際の被告人の行動を十分監督できない状態にあるといわなければならない。

しかしながら、他方、本件各詐欺の被害については被害弁償がなされており、余罪分についても被害者の特定できるものについて一部被害弁償がなされ、被告人は今後も弁償に尽くして行く旨誓っており、被害者の多くから嘆願書が提出されていること、被告人は、本件により相当期間身柄を拘束され、これを契機に自らの犯行の重大性に気づいて真摯に反省し、今後は被告人は今後現実を人間との精神的交流を大切にすると共に、この種の犯罪の予防の為に自らの知識や経験を使っていく旨述べていること、被告人は本件発覚により勤務先を懲戒解雇され社会的な制裁を受けていること、被告人は、保釈後再就職先で真面目に働き、両親に立て替えてもらった被害弁償金の返還に努めていること、被告人にはこれまで前科前歴が全くないこと、被告人の父親も本件を機に被告人との交流を取り戻し十分監督する旨誓っていることなどを総合考慮すると、現時点では被告人の再犯の可能性は低く、社会内で更生する意欲も十分あると認められる。

以上の各事情を総合考慮すると、被告人には、その刑事責任を明確にしたうえで、保護観察に付し、今回に限り、刑の執行だけは猶予するのが相当であると判断する。

この量刑の理由によれば、本判決においては、被告人が「中学生のころからコン

ピュータープログラミングを、大学生のころからパソコン通信を始めるようになり、パソコン雑誌等でのアルバイト等を通じて、前記のように、パソコンに精通するように」なり、そのようにして「中学生の頃から培ってきたコンピュータープログラミングの知識や、パソコン通信を通じて得た犯罪紛いのいわゆる裏情報をもとに」本件犯行を実行したものであって、情報通信に関する専門知識を悪用して実行された犯罪行為である点、そして、「被告人は本件詐欺も併せ同じ手口で少なくとも700万円近く手に入れていることなどまさに営業犯的犯行といわざるをえない」として、犯罪目的が常習性のある営利目的のものである点が重視されていると言える。

このように量刑の理由で示されている被告人にとって不利な事情だけをとらえるとすれば、本件事案の被告人は、世界規模でボットネットなどを駆使し情報財を奪いまくるネット犯罪者グループと何ら変わりがない者だということになりそうである。しかし、本件の被告人がそのような電子犯罪者グループと関係のある人間だとの証拠はないし、量刑の理由でもそのようには示唆されていない。量刑の理由を読む限り、本件事案は、組織犯罪とは異なる孤立した単発の模倣犯的な犯罪だったと評価するのが妥当である。

このニフティサーブ上の電子掲示板サービスを欺罔行為の手段として利用した犯罪と同種の手口による犯罪行為としては、他に、いわゆる投資詐欺（出資法違反の罪となる場合などを含む。）や霊感商法などの事案も存在する。また、盗品（盗品ではないが強行法違反となるような態様で違法に取得された物品である場合を含む。）、粗悪品、不良品、模倣品、違法複製品等を正規のものとして販売する事案もある。これらの犯罪類型の中には、本来であれば、単純に詐欺罪で処断可能なものがかなり多数含まれていると考えられるが、一般的には特別法違反の罪として軽く処罰されるか行政処分程度で処理されているものがあり、その意味では、特別法の存在が本来あるべき刑事司法の適正な運営を阻害する要因となっていると推定すべき部分がある。この点については、従来ほとんど研究がなされていない(8)。

(8) この分野に関して現時点で最も詳しい文献は、佐々木史朗編『経済刑法体系第3巻　刑法』（日本評論社、2000）だと思われるが、同書においても本論文で指摘したような問題意識は明確ではない。神山敏雄・斉藤豊治・浅田和茂・松宮孝明『新経済刑法入門』（成文堂、2011）16頁では刑法の詐欺罪と特別刑法との役割分担に関する論述はあるが、問題意識が明確ではない。なお、詐欺罪における欺罔行為それ自体については、足立友子「詐欺罪における欺罔行為について（一）：詐欺罪の保護法益と欺罔概念の再構成」名古

今後、真剣に検討がなされてしかるべきである。

なお、本件以降にも同種事案について有罪とされた事例が存在するが、前述のとおり、公刊されている判例集等には収録・公開されていない。量刑事情としても本件判決が先例として十分であるとの理解があるように思われるが、電子技術も社会情勢も大きく変化してきており、同種事案について量刑事情として何を重視すべきかについても再検討の余地があるため、無思慮な先例墨守だけは避けるべきである。

2　インターネットの事例

インターネット上で生起する詐欺事犯には多種多様なものがあり、単に古典的な詐欺がインターネットを媒介物として実行されているといったものから、高度に自動処理されるシステムの中でソフトウェアを駆使して自動実行されるものまである。後者の中には詐欺罪（刑法246条）ではなく電子計算機使用詐欺罪（刑法246条の2）が成立するものが多いと考えられるが、財物でも財産上の利益でもない情報または情報財の取得を目的とする犯罪行為の場合には別の解釈論を検討しなければならないことがある(9)。本論文では、従来から比較的よく議論されてきており、刑事裁判事例もあるネットオークション詐欺とワンクリック詐欺に限定して論ずることにする。

(1)　ネットオークション詐欺

ネットオークションは、インターネット上で実行されるオークション類似の電子商取引の一種であり、オークション出品者が応札された金額を了承すると落札の処理が実行される(10)。正常なネットオークションにおいて、落札が決定されると、

屋大學法政論集208号97～144頁、同「詐欺罪における欺罔行為について（二）：詐欺罪の保護法益と欺罔概念の再構成」名古屋大學法政論集211号137～181頁、同「詐欺罪における欺罔行為について（三）：詐欺罪の保護法益と欺罔概念の再構成」名古屋大學法政論集212号349～379頁、同「詐欺罪における欺罔行為について（四）：詐欺罪の保護法益と欺罔概念の再構成」名古屋大學法政論集214号329～363頁、同「詐欺罪における欺罔行為について（五・完）：詐欺罪の保護法益と欺罔概念の再構成」名古屋大學法政論集215号391～423頁がある。

(9) 夏井高人「サイバー犯罪の研究（二）―フィッシング（Phishing）に関する比較法的検討―」法律論叢85巻4・5号179～236頁、同「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85巻6号363～420頁で詳論したとおりである。

(10) 基本形は古物営業の一種と考えられているが、実際には、オークションサイトのシステムを店舗として利用した通常の売買契約であることが多い。オークションサイトを店舗

目的物が宅配便により落札者に対して送付され、代金引換または口座振込などにより決済される。代金引換の場合、民事上は留置権と同様の担保権的機能が自動的に生ずるので、目的物に特に不具合や不当表示等がない限り問題が生ずることは少ない。しかし、落札代金の支払が先履行となっており、口座振込や電子的な自動決済(11)等によって落札代金の支払がなされたのに、目的物が送られてこないことがある。このような場合においては、故意の存在が認められる限り、通常の詐欺罪（口座振込の場合には刑法246条1項の詐欺罪、自動決済の場合には同法246条2項の詐欺罪）が成立し得る。逆に、落札代金が後払いになっている場合において、目的物が送付されたのに、代金の支払いがなされないことがある。このような場合においては、故意の存在が認められる限り、やはり通常の詐欺罪（刑法246条1項）が成立し得る。

しかしながら、ネットオークションの出品者と落札者が同一人であり、オークションシステムを悪用して不実の送金処理を実行させるようなタイプの犯罪類型では、欺罔される人間が存在しない。欺罔に相当する行為は、電子計算機であるオークションシステムに対する不正な操作行為だけである。したがって、このような行為については、詐欺罪（同法246条）ではなく、電子計算機使用詐欺罪（同法246条の2）が成立し得る。

公刊されている判例集等には、ネットオークション関連事犯として2件の裁判例が収録されている。一方は、有罪の事例であり（東京地裁平成15年12月11日判決・平成15年（刑わ）3300号、平成15年（刑わ）3889号、平成15年（刑わ）

として利用する利点としては、定額で価格が固定されることがなく、購入希望者が多ければ競争が生じ、販売者希望額よりもずっと高額で最終的な売買契約の締約（競り落とし）が決定されることがあり、そのような場合には、店舗として利用する販売者にとって有利な状況が発生することになる。このような経済現象は、定価販売だけの世界では想定し難いものかもしれない。しかし、本来的に、売買代金は浮動的なものであり、需要と供給の関係によって値上がりも値下がりもするのが当然であるので、そのような本来の売買契約のプロセスをネット上で実現するための機能をネットオークションシステムが有していると理解することも可能である。

(11) クレジットカードによる自動決済が一般的だが、最近では各種電子マネーによる決済も普及してきている。電子マネーの中にはプリペイド型のものが多く、この場合、予め購入した電子マネー単位が被害額の上限となる。その額は、一般に比較的低額である。しかし、クレジットカードと同様の与信型の電子マネーの場合には、与信額の上限が被害額の上限となることから、相当高額の被害が生ずることがあり得る。

4125号・公式判例集等未登載）、他方は、無罪の事例（神戸地裁平成19年4月23日判決・裁判所サイト(12)）である。

東京地裁判決（有罪判決）の事案は、被告人（当時40歳の男性会社員）が、①漫画喫茶に設置されていたパソコンから不正アクセスすることによってオークションサイト利用者の登録データを改変し、被告人以外の登録利用者になりすますことができるようにした上で（不正アクセス禁止法違反の罪、電磁的記録不正作出罪、同供用罪）、②ネットオークションの出品に対して、他の登録利用者になりすました被告人が応札して落札者となり、③落札代金については、オークションサイト上の立替払いシステムを悪用し、なりすまされた登録利用者が立替払い機能を利用したかのように不実の電子決済に基づく送金処理をさせ、④その送金処理によって被告人の口座に落札代金額相当の送金処理をさせて財産上不正の利益を得た（②～④について電子計算機使用詐欺罪）というものである。

同事件の判決では、被告人に対し、懲役2年10月の刑が宣告された。

同判決において認定された罪となるべき事実は、次のとおりである（関係者名等は一部仮名、住所等は一部省略）。

（罪となるべき事実）

被告人は、ヤフー株式会社（以下「ヤフー」という。）が設置して管理するコンピュータに不正アクセスした上、その運営するオークションの会員が、電子メールアドレスを変更し、自己の出品した商品を落札し、その落札代金立替払サービスの利用を指定し、その代金相当額の送金を依頼した旨の虚偽の情報を送信し、さらに、金融機関が設置して管理するコンピュータにも自動的に送信させ、自己の預金残高が増加した旨の虚偽の情報を各コンピュータに記憶蔵置させて、財産上不法の利益を得ようと企て、

第1　法定の除外事由がないのに、

1　別表1—1の「不正アクセス一覧表」記載のとおり、平成15年3月25日午前7時22分ころから同年4月2日午前6時43分ころまでの間、前後10回にわたり、札幌市中央区（略）所在の甲ビルのB店内において、同所に設置のコンピュータから、電気通信回線を介して、ヤフーが東京都千代田区（略）所在の乙ビルに設置して管理するアクセス制御機能を有する特定電子計算機である認証サーバに、ヤフーの会員であるDを利用権者として付された識別符号であるログインID（略）及びログインパスワード（略）をそれぞれ入力して上記特定電子計算機を作動させ、上記アクセス

(12) http://www.courts.go.jp/hanrei/pdf/20070618133219.pdf［2014年4月12日確認］

制御機能により制限されている特定利用をし得る状態にさせ、

2　別表1—2の「不正アクセス一覧表」記載のとおり、同年3月31日午後3時45分ころから同年5月1日午前10時16分ころまでの間、前後37回にわたり、前記B店内において、同所に設置のコンピュータから、電気通信回線を介して、ヤフーがアクセス制御機能を有する特定電子計算機である前記認証サーバに、Eほか7名を利用権者として付された識別符号であるログインID及びログインパスワードをそれぞれ入力して上記特定電子計算機を作動させ、上記アクセス制御機能により制限されている特定利用をし得る状態にさせ、もって、不正アクセス行為をした。

第2　ヤフーの事務処理を誤らせる目的で、権限なく、

1　別表2—1の「電子メールアドレス変更状況」記載のとおり、同年3月28日午後2時50分ころから同年4月2日午前6時44分ころまでの間、前後3回にわたり、前記B店内において、前記第1の1記載の方法により、ヤフーが前記乙ビル内に設置して管理する電子計算機であるUDBサーバに対し、実際は、前記Dが電子メールアドレスを変更した事実がないのに、同人が電子メールアドレスを変更する手続をとった旨の虚偽の情報を送信し、上記電子計算機に接続された記憶装置に上記情報を記憶蔵置させ、

2　別表2—2の「電子メールアドレス変更一覧表」記載のとおり、同年4月7日午後10時40分ころから同年5月1日午前10時17分ころまでの間、前後16回にわたり、前記B店内において、前記第1の2記載の方法により、ヤフーが設置して管理する前記UDBサーバに対し、実際は、前記Eほか6名が電子メールアドレスを変更した事実がないのに、同人らが電子メールアドレスを変更する手続をとった旨の虚偽の情報を送信し、上記電子計算機に接続された記憶装置に上記情報を記憶蔵置させ、

もって、事実証明に関する電磁的記録を不正に作出し、ヤフーの事務処理の用に供した。

第3　ヤフーの事務処理を誤らせる目的で、権限なく、

1　同年3月28日午後3時24分ころ、前記B店内において、前記第1の1記載の方法により、ヤフーが前記乙ビル内に設置して管理する電子計算機であるオークションサーバに対し、実際は、前記Dが、ヤフーオークションで被告人がF名義で登録したIDを使用して出品したノート型パソコン1台を落札した事実がないのに、上記Dが同商品に対して入札を行い、24万7500円で落札した旨の虚偽の情報を送信し、上記電子計算機に接続された記憶装置に上記情報を記憶蔵置させ、

2　別表3—1の「ヤフーオークション一覧表」記載のとおり、同年4月2日午前11時21分ころから同月27日午前1時39分ころまでの間、前後7回にわたり、前記B店内において、前記第1の2記載の方法により、ヤフーが設置して管理する前記オークションサーバに対し、実際は、前記Eほか5名が、ヤフーオークションで被告人がF名義で登録したIDを使用して出品した商品を落札した事実がないのに、上

記Eらが同商品に対して入札を行い、合計63万4600円で落札した旨の虚偽の情報を送信し、上記電子計算機に接続された記憶装置に上記情報を記憶蔵置させ、

3　別表3—2の「ヤフーオークション一覧表」記載のとおり、同年3月31日午後3時57分ころから同年4月21日午前10時41分ころまでの間、前後9回にわたり、前記B店内において、前記第1の2記載の方法により、ヤフーが設置して管理する前記オークションサーバに対し、実際は、前記Eほか6名が、ヤフーオークションで被告人がF名義で登録したIDを使用して出品した商品を落札した事実がないのに、上記Eらが同商品に対して入札を行い、合計109万3500円で落札した旨の虚偽の情報を送信し、上記電子計算機に接続された記憶装置に上記情報を記憶蔵置させ、

もって、事実証明に関する電磁的記録を不正に作出し、ヤフーの事務処理の用に供した。

第4　ヤフー及び金融機関の事務処理を誤らせる目的で、権限なく、前記Bにおいて、

1　同年3月29日午前11時22分ころ、前記第1の1記載の方法により、ヤフーが設置して管理する前記オークションサーバに対し、実際は、前記Dが、前記第3の1記載のヤフーオークションで商品を落札した事実がないのに、ヤフーの子会社である株式会社Gが提供する落札代金立替払サービス「ヤフーペイメント」の利用を指定した上、被告人が管理する株式会社H銀行インターネット支店のF名義の普通預金口座に落札代金の一部である7万7500円の送金を依頼した旨の虚偽の情報を送信し、前記オークションサーバから自動的に上記Dが会員契約をしているIクレジットサービス株式会社に同人名義のIカードの与信照会を行わせ、同カードの利用承認後、上記オークションサーバに接続された記憶装置に記憶蔵置させ、もって、事実証明に関する電磁的記録を不正に作出し、ヤフーの事務処理の用に供し、さらに、同月31日、上記オークションサーバから上記情報を、ヤフーが振込業務等を委託しているH銀行が千葉県印西市（略）所在のJ株式会社内に設置して管理する為替システムのコンピュータに自動的に送信させ、同年4月1日午前5時55分ころ、G名義の普通預金口座から前記F名義の普通預金口座に7万7500円が送金されて同人名義の預金残高が同額増額した旨の虚偽の情報を、同電子計算機に接続された記憶装置に記憶蔵置させ、もって、権利、義務に関する電磁的記録を不正に作出して、H銀行の事務処理の用に供するとともに、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、7万7500円相当の財産上不法の利益を得た。

2　別表4—1の「ヤフーペイメント及び口座入金一覧表」記載のとおり、同年4月3日午前10時31分ころから同月27日午前2時22分ころまでの間、前後7回にわたり、前記第1の2記載の方法により、ヤフーが設置して管理する前記オークションサーバに対し、実際は、前記Eほか5名が、前記第3の2記載のヤフーオークションで商品を落札した事実がないのに、Gが提供する前記ヤフーペイメントの利用を指定した上、被告人が管理する前記F名義の普通預金口座に落札代金の全部又は一

部である合計63万100円の送金を依頼した旨の虚偽の情報を送信し、上記オークションサーバから自動的に上記Eらが会員契約をしている信販会社に同人ら名義のクレジットカードの与信照会を行わせ、同カードの利用承認後、上記オークションサーバに接続された記憶装置に記憶蔵置させ、もって、事実証明に関する電磁的記録を不正に作出して、ヤフーの事務処理の用に供し、さらに、上記オークションサーバから上記情報を、H銀行が設置して管理する電子計算機である前記為替システムのコンピュータに自動的に送信させ、同月4日から同月30日までの間、前後5回にわたり、G名義の普通預金口座から前記F名義の普通預金口座に合計63万100円が送金されて、その預金残高が同額増額した旨の虚偽の情報を、同電子計算機に接続された記憶装置に記憶蔵置させ、もって、権利、義務に関する電磁的記録を不正に作出して、H銀行の事務処理の用に供するとともに、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、合計63万100円相当の財産上不法の利益を得た。

3　別表4—2の「ヤフーペイメント及び口座入金一覧表」記載のとおり、同年3月31日午後10時1分ころから同年4月21日午前11時53分ころまでの間、前後9回にわたり、前記第1の2記載の方法により、ヤフーが設置して管理する前記オークションサーバに対し、実際は、前記Eほか6名が、前記第3の3記載のヤフーオークションで商品を落札した事実がないのに、Gが提供する前記ヤフーペイメントの利用を指定した上、被告人が管理する前記F名義の普通預金口座に落札代金の全部又は一部である合計78万3500円の送金を依頼した旨の虚偽の情報を送信し、上記オークションサーバから自動的に上記Eらが会員契約をしている信販会社に同人ら名義のクレジットカードの与信照会を行わせ、同カードの利用承認後、上記オークションサーバに接続された記憶装置に記憶蔵置させ、もって、事実証明に関する電磁的記録を不正に作出して、ヤフーの事務処理の用に供し、さらに、上記オークションサーバから上記情報を、K銀行株式会社が東京都千代田区（略）所在の丙ビル26階に設置して管理する電子計算機であるK銀行ホストコンピュータに、H銀行が管理する前記為替システムのコンピュータ等を介して、自動的に送信させ、同月2日から同月22日までの間、前後5回にわたり、G名義の普通預金口座から前記F名義の普通預金口座に合計78万3500円が送金されて、その預金残高が同額増額した旨の虚偽の情報を、同電子計算機に接続された記憶装置に記憶蔵置させ、もって、権利、義務に関する電磁的記録を不正に作出して、Kの事務処理の用に供するとともに、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、合計78万3500円相当の財産上不法の利益を得た。

他方、神戸地裁判決（無罪事件）における公訴事実の概要は、次のとおりである。

（公訴事実の概要）

被告人は、ヤフー株式会社がインターネット上で主催するヤフーオークションを利用して、電化製品の販売をしていたところ、同オークションを利用して、電化製品の販売名下にインターネット利用者から金員を詐取しようと企て、平成16年11月17日から同年12月23日までの間、多数回にわたり、販売に供する商品を発送する確実なめどがないのに、これを秘し、パソコンを使用して、ヤフー株式会社が管理するサーバに、商品名、開始価格、数量、発送期日等の競売による売却情報を送信、掲示して購入者を募り、掲示を閲覧して競売に参加し落札した者に電子メールで連絡するなどし、落札金額と送料を被告人が指定した郵便貯金口座あるいは銀行預金口座に振り込めば、約1か月ないし2か月後に落札商品を受け取れるものと誤信させ、よって、同年11月19日から同年12月27日までの間、各落札者らをして、被告人が管理する前記預貯金口座に合計600万4140円を入金させ、もって、それぞれ、人を欺いて財物を交付させたものである。

要するに、代金を支払えば商品を発送するように装い、その代金を詐取したという古典的な類型に属する事案だと言える。

ところが、本件の公判では詐欺の故意の存在について争われ、弁護人は、「本件は商取引上の債務不履行であって、被告人に詐欺の故意はなく、欺罔行為が存在しないから無罪である」と主張した。審理の結果、神戸地裁は無罪の判決をした。判決理由中にはその検討結果が縷々述べられており、結論部分では「以上のとおり、被告人は、平成16年7月ころ以降ヤフーオークション取引が赤字になっていること自体は認識しつつ、同年11月中旬以降、オークションへの出品数を増加させて、それまでに出品した落札者に対する仕入資金を得ようとしたものとは認められるものの、当時の自己の財政状況に関し、おおまかにせよその客観的な赤字額を認識していたものとは認められない。そうすると、その当時、被告人が、赤字の補填についてデザイン関係等による収益で賄うことができると思っており、ヤフーオークション以外のそれらの収益で補填して、オークションに出品した商品を仕入れて落札者に対して発送することができると考えていたとの可能性が相当程度残るものといわざるを得ず、落札者に対して掲示したとおりに商品を発送することができないかもしれないことを認識しながら、それでもかまわないと思ってあえて出品したものと認めるには未だ合理的疑いが残るというべきである」と述べられている。

一般に、詐欺の故意の立証責任は全て検察官にあり、本件において検察官がその

立証に成功しなかった以上、無罪の判決となるのは当然のことだと考える。ただし、検察官が本当にその立証に成功しなかったのかという点については評価が分かれるものと思われ、社会的にも少なからぬ批判の残る事件となった。

この神戸地裁の無罪判決における判断の当否はさておき、あくまでも一般論としては、継続的にオークションサイトを利用して出品形式で物品販売業を営み、それによって比較的大きな額となる取引をしている者については、所得税の確定申告等の際に自己の収支について正確に把握する機会が当然あるはずであり、それゆえに、当該の者の知的能力が通常人と比較して著しく劣っているなどの特段の事情がない限り、相当程度明確に赤字見込みを想定することが可能な状態にあると推論するのが常識に適った事実認定（経験則）である(13)。ただ、裁判官が経理・会計や税務処理に関する知識・経験を全く有しない場合、そのことを正しく認識・理解できるかどうかは全く別問題である。その意味で、本件は、現行の裁判制度が本来的にもつ機能上の限界を示す事例の一つとして理解することも可能であろう。

(2) ワンクリック詐欺

俗にワンクリック詐欺と呼ばれる詐欺類型は、アダルトサイト等を偽装したウェブサイト等において、サイト内の閲覧ページに入るための入室ボタンや画像等に仕掛けがあり、それをクリックすると有料サイトである旨の表示がなされ、高額の代金の支払いが求められるようになっているサイトのことを指している。しばしば、任意の支払いに応じなければ刑事告訴や民事訴訟の提起をするなどの脅迫文言が表示されたり、そのような内容の電子メールや葉書等が届いたりすることがある。

このような行為は、クリックした訪問者にはそのサイトの利用料金を支払う義務がないのにそのように誤信させ、利用料金名目で金員の支払いをさせる点をとら

(13) 収支状況を全く認識していない完全な放漫経営である場合、当然のことながら、赤字であるかどうかを判断することはできない場合があり得るが、現実には仕入れに対する支払が毎月発生するので、完全に認識できない状況というものを想定することができない。仮にそのような状況が存在したとすれば、それでもなお経営を継続することは、それ自体として、未必的・概括的な詐欺の故意を肯定する事情となり得ると考える。この点については、商法学や経営学において論じられている理想像としての経営者の資質・能力と現実に存在する経営者の資質・能力との齟齬・乖離が著しいことがあるという現実を踏まえた議論が必要ではあるが、経営能力が全くないのに企業経営に従事すること自体について社会的にどのような評価が妥当かという観点も踏まえた上で、詐欺罪における故意の事実認定には規範的評価や価値判断が含まれることがあり得るということを正確に理解することが重要である。

え、1回のクリックでそのような結果が生じるのでワンクリック詐欺と呼ばれている。確かに、詐欺類型に属するものはある。しかしながら、分析的には恐喝罪に類するものもあり、その境界線は微妙である。この点は、ランサムウェアによる恐喝または詐欺（身代金要求攻撃）と類似する部分がある(14)。事案による相違とりわけ被害者の主観的要素の立証の難易があるので、一概には断ずることができないが、証拠により立証可能な範囲内で、事案の本質を見極め、恐喝類型に属するか詐欺類型に属するかを正しく見定める必要がある。

公刊された判例集に収録された裁判事例は1件ある。奈良地裁平成18年4月12日判決・刑集61巻9号824頁がそれで、控訴及び上告があり、上告審である最高裁決定が刑集61巻9号821頁に収録されている関係から、その第1審判決として控訴審である大阪高裁判決・刑集61巻9号835頁と共に刑集に収録されている。

奈良地裁の判決では、アダルトサイト関連の広告代理業を営む有限会社の代表取締役である被告人（当時21歳の男性）に対し、共犯者である実母との共謀による詐欺罪（刑法246条1項）及び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（平成11年8月18日法律第136号）違反の罪により、懲役2年及び罰金100万円の刑が宣告された。

奈良地裁判決において認定された罪となるべき事実は、次のとおりである（関係者名等は一部仮名、住所等は一部省略）。

（罪となるべき事実）

被告人は、

第1　デジタルコンテンツの企画・制作・運営等を業とする有限会社Lの代表取締役であるが、自己の運営するインターネット上のアダルトサイト「M」にアクセスした者から有料サイト利用料金徴収名下に金員を詐取するとともに同詐取にかかる犯罪の収益の取得につき事実を仮装しようと企て、真実は、相手方に有料サイト利用の意思がなく有料サイト利用契約は成立せず、料金支払いの義務は発生しないのにこれあるように装い、

1　平成17年4月20日、東京都新宿区（略）所在の甲ビル6階新宿データセンター内に設置されたサーバーコンピューター内に記憶・蔵置された前記「M」に、岡山県美作市（略）所在の智頭急行宮本武蔵駅構内から、携帯電話を使用してアクセスした

(14) ランサムウェア（Ransomware）については、夏井高人「サイバー犯罪の研究（六）―違法な電子メールに関する比較法的検討―」法律論叢86巻6号225～230頁で詳論したとおりである。

A（当時32歳）に対し、「ご登録ありがとうございます。あなたの個体識別番号は登録させて頂き、入会手続を完了しました。支払期日を過ぎても入金確認ができない場合、規約に基づき個体識別番号をもとに延滞料金、損害金を加算して直接請求させていただきます。無視されますと、簡易裁判所から訴状と呼び出し状が自宅に届きます。」などと内容虚偽の表示をさせて前記Aにこれを閲覧了知させた上、さらに、これにより同所から同サイト上に記載された連絡先に、有料サイト利用契約締結の意思がないのに登録されたため解約する意図で電子メールを送信した同人に対し、「利用料金のお振込みが確認できてからでないと退会できません。」などと内容虚偽の電子メールを返信するなどし、同人をして有料サイト利用契約が有効に成立しており、前記「M」サイト運営者に対してサイト利用料支払いの義務があるものと誤信させ、よって、同月21日、同人をして、大阪市西区（略）所在のO信用組合本店営業部から奈良市（略）所在のP信用金庫大安寺支店に開設された被告人が管理するB名義の普通預金口座に現金2万7000円を振込入金させた上、更に同日、前記Aに対し、「規約に記載のとおり提携サイトにも登録となります。提携サイトの分をお支払い下さい。Q28,000円、R30,000円、S35,000円。合計93,000円があなたの残りの利用料金になります。」などと記載した電子メールを送信し、同人をして、前記Qなどの各有料サイト利用契約が有効に成立しており、サイト運営者に対してサイト利用料支払いの義務があるものと誤信させ、同月22日、前記O信用組合本店営業部から前記P信用金庫大安寺支店のB名義の普通預金口座に現金9万3000円を振込入金させ

2　同年5月5日、前記「M」に、静岡市葵区（略）から、携帯電話を使用してアクセスしたC（当時38歳）に対し、前同様の内容虚偽の表示をさせて前記Cにこれを閲覧了知させた上、さらに、これにより同所から同サイト上に記載された連絡先に、有料サイト利用契約締結の意思がないのに登録されたため解約する意図で電子メールを送信した同人に対し、「使ってたとか使ってない、間違ったとかは一切関係ありません。退会は入金確認後になります。」などと内容虚偽の電子メールを返信するなどし、同人をして有料サイト利用契約が有効に成立しており、前記「M」サイト運営者に対してサイト利用料支払いの義務があるものと誤信させ、よって、同月6日、同人をして、静岡県榛原郡吉田町（略）所在のT信用金庫神戸支店から前記P信用金庫大安寺支店に開設された被告人が管理するB名義の普通預金口座に現金2万7000円を振込入金させた上、更に同日、前記Cに対し、「規約に記載のとおり提携サイトにも登録となります。提携サイトの分をお支払い下さい。Q28,000円、R30,000円、S35,000円。合計93,000円があなたの残りの利用料金になります。」などと記載した電子メールを送信し、同人をして、前記Qなどの各有料サイト利用契約が有効に成立しており、サイト運営者に対してサイト利用料支払いの義務があるものと誤信させ、同月9日、前記T信用金庫神戸支店から前記P信用金庫大安寺支店のB

名義の普通預金口座に現金9万3000円を振込入金させ

3　同月10日、前記「M」に、京都市右京区（略）のD方から、携帯電話を使用してアクセスしたE（当時18歳）に対し、前同様の内容虚偽の表示をさせて前記Eにこれを閲覧了知させた上、さらに、これにより同所から同サイト上に記載された連絡先に、有料サイト利用契約締結の意思がないのに登録されたため解約する意図で電子メールを送信した同人に対し、「間違って入会などなりません。あなたの意思でこちらのサイトに入ってこられたのですよ。正常な退会処理ができないかぎり請求は止まりません。規約にも書いてありますようにM27,000円以外にQ28,000円とR30,000円、S35,000円。合計120,000円があなたの利用料金になります。3日を越えますと延滞料金が発生します。」などと内容虚偽の電子メールを返信するなどし、同人をして前記各有料サイト利用契約が有効に成立しており、サイト運営者に対してサイト利用料支払いの義務があるものと誤信させ、よって、同月12日、同人をして、大阪府堺市（略）所在の株式会社U銀行初芝支店から前記P信用金庫大安寺支店に開設された被告人が管理するB名義の普通預金口座に現金12万円を振込入金させ

4　同月13日、前記「M」に、滋賀県守山市（略）から、携帯電話を使用してアクセスしたF（当時35歳）に対し、前同様の内容虚偽の表示をさせて前記Fにこれを閲覧了知させた上、さらに、これにより同所から同サイト上に記載された連絡先に、有料サイト利用契約締結の意思がないのに登録されたため解約する意図で電子メールを送信した同人に対し、「使ってたとか使ってない、間違ったとかは一切関係有りません。解約はお振込み確認後に受付となっております。」などと内容虚偽の電子メールを返信するなどし、同人をして有料サイト利用契約が有効に成立しており、サイト運営者に対してサイト利用料支払いの義務があるものと誤信させ、よって、同月14日、同人をして、同市（略）所在の株式会社V銀行播磨田支店から前記P信用金庫大安寺支店に開設された被告人が管理するB名義の普通預金口座に現金2万7000円を振込入金させた上、更に同日、前記Fに対し、「M27,000円を登録したと同時にQ28,000円、R30,000円、S35,000円。合計120,000円があなたの利用料金になります。」などと記載した電子メールを送信し、同人をして、前記Qなどの各有料サイト利用契約が有効に成立しており、サイト運営者に対してサイト利用料支払いの義務があるものと誤信させ、同月27日、同人をして、前記株式会社V銀行播磨田支店から前記P信用金庫大安寺支店のB名義の普通預金口座に現金12万円を振込入金させ

5　同年6月3日、前記「M」に、沖縄県那覇市（略）から、携帯電話を使用してアクセスしたG（当時15歳）に対し、前同様の内容虚偽の表示をさせて前記Gにこれを閲覧了知させた上、さらに、これにより同所から同サイト上に記載された連絡先に、有料サイト利用契約締結の意思がないのに登録されたため解約する旨の電子メールを送信した同人に対し、「登録画面が表示されましたら登録完了となり、料金が発生しております。」などと内容虚偽の電子メールを返信するなどし、同人をして有料サイ

ト利用契約が有効に成立しており、前記「M」サイト運営者に対してサイト利用料支払いの義務があるものと誤信させ、よって、同月4日、同人をして、同市（略）所在の株式会社W銀行国場支店から奈良市（略）所在の株式会社X銀行奈良支店に開設された被告人が管理するH名義の普通預金口座に現金2万7000円を振込入金させ

6　同日、前記「M」に、静岡県浜松市（略）から、携帯電話を使用してアクセスしたI（当時39歳）に対し、前同様の内容虚偽の表示をさせて前記Iにこれを閲覧了知させた上、さらに、これにより同所から同サイト上に記載された連絡先に、有料サイト利用契約締結の意思がないのに登録されたため解約する意図で電子メールを送信した同人に対し、「登録画面が表示されましたら登録完了となり、料金が発生しております。解約メールを送信して解約されるわけではなく、規約にもあるよう解約はお振込み確認後に受付となっております。」などと内容虚偽の電子メールを返信するなどし、同人をして有料サイト利用契約が有効に成立しており、前記「M」サイト運営者に対してサイト利用料支払いの義務があるものと誤信させ、よって、同日、同人をして、同市（以下略）所在の株式会社Y銀行浜松支店から前記X銀行奈良支店に開設された被告人が管理するH名義の普通預金口座に現金2万7000円を振込入金させた上、更に同日、前記Iに対し、「規約に記載のとおり提携サイトにも登録となります。提携サイトの分をお支払い下さい。Q28,000円、R30,000円、S35,000円にも同時に登録されており、その利用料金93,000円が残ってる。」などと記載した電子メールを送信し、同人をして、前記Qなどの各有料サイト利用契約が有効に成立しており、サイト運営者に対してサイト利用料支払いの義務があるものと誤信させ、同日、同人をして、前記Y銀行浜松支店から前記X銀行奈良支店のH名義の普通預金口座に現金9万3000円を振込入金させ

もって人を欺いて財物を交付させるとともに、犯罪収益の取得につき事実をそれぞれ仮装し

第2　前記有限会社Lの代表取締役であるが、自己の運営するインターネット上のアダルトサイトにアクセスした者から有料サイト利用料金徴収名下に金員を詐取した犯罪収益等の取得につき事実を仮装しようと企て、別紙一覧表記載のとおり、同年2月22日ころから同年6月10日ころまでの間、552回にわたり、前記有料サイト利用料金徴収名下に欺罔された者をして奈良市（略）所在の株式会社Z銀行奈良支店に開設された甲名義の普通預金口座ほか10口座に、現金3185万8000円を振込入金させ、もって犯罪収益等の取得につき事実を仮装し

第3　Nと共謀の上、同年5月25日ころ及び同月29日ころの2回にわたり、奈良市（略）所在のJビルK号室において、乙らが株式会社X銀行奈良支店より詐取したH宛にて発行された普通預金通帳1通、キャッシュカード1枚及びワンズダイレクトカード1枚を、その情を知りながら、上記乙らから代金合計1万円で買い受け、もって、財産に対する罪に当たる行為によって領得された物を有償で譲り受けたものである。

奈良地裁判決では、金融機関の口座から他の金融機関の口座への資金移動（振込）をもって財物の交付としてとらえている。しかし、ここには財物の移転は一切存在せず、電子計算機の計算処理上での資金移動があるだけである。したがって、本件公訴事実のうち詐欺罪が成立する部分に関しては、刑法246条1項の詐欺罪ではなく同法246条2項の詐欺罪が成立すると解するのが正しい（ただし、ある口座から他の口座へと資金移動するのではなく、端末機等に現金を入金して送金処理をした場合には、端末機に現金を挿入した時点で財物である現金の処分行為があったと認めることができるから、同法246条1項の詐欺罪が成立し得る。）。また、そのように解さないと、財物の交付と財産的利益の移転との区別が不明瞭となり、電子計算機使用詐欺罪の解釈・適用との間で重大な齟齬をきたすことになりかねない。

被告人の控訴理由は、訴訟手続の法令違反、法令適用の誤り及び量刑不当であった。控訴審である大阪高裁は、法令違反及び法令適用の誤りについては被告人の主張を認めなかったものの、原審である奈良地裁判決以降の時点で生じた事情（追加的な被害弁償等）を斟酌し、原審判決を破棄して、懲役1年2月及び罰金100万円の刑を宣告した。

上告審においては、被告人の主張はいずれも認められず、上告棄却の決定となっている。その理由中では、罪数に関する「詐欺と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10条1項の犯罪収益等隠匿とが刑法54条1項前段の観念的競合の関係に立つ場合、詐欺罪の法定刑は10年以下の懲役であり、犯罪収益等隠匿罪のそれは5年以下の懲役若しくは300万円以下の罰金又はこれの併科であるから、いわゆる重点的対照主義によれば、被告人に対する処断は重い刑を定める詐欺罪の法定刑によることになり、軽い罪である犯罪収益等隠匿罪の罰金刑を併科することはできない」との上告理由について、「数罪が科刑上一罪の関係にある場合において、その最も重い罪の刑は懲役刑のみであるがその他の罪に罰金刑の任意的併科の定めがあるときには、刑法54条1項の規定の趣旨等にかんがみ、最も重い罪の懲役刑にその他の罪の罰金刑を併科することができるものと解するのが相当」であると判示されている。

本件における被告人の行為が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違反の罪に該当すると認定されたことは既述のとおりである。同法1条は、「この法律は、組織的な犯罪が平穏かつ健全な社会生活を著しく害し、及び犯罪に

よる収益がこの種の犯罪を助長するとともに、これを用いた事業活動への干渉が健全な経済活動に重大な悪影響を与えることにかんがみ、組織的に行われた殺人等の行為に対する処罰を強化し、犯罪による収益の隠匿及び収受並びにこれを用いた法人等の事業経営の支配を目的とする行為を処罰するとともに、犯罪による収益に係る没収及び追徴の特例等について定めることを目的とする」と規定し、「組織的に行われた殺人等の行為に対する処罰」、「犯罪による収益の隠匿及び収受並びにこれを用いた法人等の事業経営の支配を目的とする行為」に対する処罰及び「犯罪による収益に係る没収及び追徴の特例等について定めること」に主眼が置かれている。これらのうち、「犯罪による収益の隠匿及び収受並びにこれを用いた法人等の事業経営の支配を目的とする行為」に対する処罰は、犯罪組織とは無関係の犯罪行為についても適用され得るもので、同法2条2項1号は、「犯罪収益」について「財産上の不正な利益を得る目的で犯した別表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」と定義し、同法別表（二タ）は、「刑法第246条から第250条まで（詐欺、電子計算機使用詐欺、背任、準詐欺、恐喝、未遂罪）の罪」と規定している。そして、同法10条1項は、①犯罪収益等の取得若しくは処分につき事実を仮装する行為及び②犯罪収益等を隠匿する行為につき、5年以下の懲役若しくは300万円以下の罰金に処し、又はこれを併科するものと規定している。そのことから、犯罪組織と関係のない者及び行為であっても、詐欺罪により得た収益を仮装または隠匿する行為は、同法違反の罪として処罰され得ることになる(15)。ところが、「罪名が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違反の罪」となることから、犯罪組織と全く無関係の者であっても組織犯罪者であるとの誤解を受け、社会的に不当な差別的評価を受けるおそれがある。この点は、立法技術上の問題点として再検討すべき余地があると思われる。

(3) サクラを使った出会系サイト詐欺

インターネット上には様々なタイプの交際サイトが存在し、異性または同性の性的関係を伴い得る交際相手を求める人々の交際サイトも存在する。その中には真

(15) 関連する先例として、最高裁平成20年11月4日決定・刑集62巻10号2811頁がある。

面目な交際サイトがある一方で、犯罪的な目的で交際サイトを偽装しているところもある。偽装サイトの例としては、マルウェアを感染させるように仕組まれたサイトがあり、また、異性との交際を求める利用者を装う「サクラ(16)」と呼ばれる従業員または共犯者を用い、サイトの利用料金名目で金銭を詐取する目的で構築・運営されている詐欺サイトもある(17)。

サクラを用いた偽装出会い系サイトについても検挙事例が幾つかあるけれども、公刊されている判例集などに収録されている裁判例は乏しい(18)。

---

(16)「サクラ」の語源は不明だが、江戸時代ころに発生し、明治時代以降には露天商などが客に商品の評価を誤らせて実際の品質に見合わない高価で売るために用いる偽客（共犯者的な偽客）のことを指すと理解されている。消費者保護との関連では、近年、いわゆるステルスマーケティングと呼ばれる手口が問題視されている。これは、有名タレントなどが実際には当該商品を使用していないのに、「素敵だ」とか「効果がある」といったコメントを自己のブログに書き込み、実質的に商業宣伝広告を手伝っており、しかも、隠れて宣伝広告報酬を得ている場合などに特に問題視されてきた。これは、典型的に古典的な意味での「サクラ」の手口の一種であることがあり得る。無論、実際に購入して使用した感想をブログに記事として掲載することは表現の自由の一部に含まれ、それぞれのブログ作成者が自分の責任で意見表明することは自由なので、そのような正規のブログ記事等とサクラによるステルスマーケティング等とは明確に区別して考えなければならない。また、知人・友人・親族等の商売を支援・応援するためであることを明記したブログ記事も自由になし得ることは当然なので、これもまた明確に区別して考える必要がある。問題となるのは、実質的には単なる商業宣伝広告であることを隠して意見表明を行い、しかも、それに対して当該商品等の製造者や販売者等から相応の対価が支払われている場合だと言える。このようなステルスマーケティングの手法は、カルト系の団体・組織や新興宗教等に類する組織・団体等でも用いられることがある。他方、アダルトサイト等では、若干異なる意味で「サクラ」という用語が用いられることがある。これは、顧客勧誘のための手口の一種ではなく、まさに「なりすまし」による詐欺の手口の一種として理解すべきもので、露天商等が用いてきた「サクラ」とは類型が異なる。しかし、偽の顧客であるのにそれを秘して顧客を誘引し、販売利益を向上させるという意図・目的において共通するところがあるので、非常に広い意味では同じ類型に属するものとして認識され、「サクラ」と呼ばれてきたものだろうと推定される。

(17) この種のサイトでは、送信者情報を偽る電子メール等による勧誘が行われることがしばしばある。この点については、前掲「サイバー犯罪の研究（六）―違法な電子メールに関する比較法的検討―」181～223頁で詳論した。

(18) 民事判決としては、東京高裁平成25年6月19日判決・判例時報2206号83頁がある（上告）。同判決では、「以上によれば、被控訴人は、本件各サイトにおいて、サクラを使用して、かつサクラであることを秘して、資金援助や連絡先交換又は待合せ等、役務ないし利益の提供をする意思もないのに、それがあるように虚偽のメールを送信させて、それらが一定程度実現する可能性があると控訴人を誤信させ、控訴人に役務ないし利益の取得のため、送受信等を多数回繰り返させたり、上記資金援助等の目的達成のためには虚偽の暗号送信等の手続が必要であるとの虚偽の事実を申し向けてその旨控訴人を誤信させ、利用

やや特殊な事案ではあるが、東京地裁平成24年6月29日判決（平成24年（合わ）37号・公式判例集等未登載）がある。

東京地裁判決では、被告人3名に対し、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違反の罪により、懲役3年（被告人2名については執行猶予5年）の刑が宣告された。

この事件は、アダルトサイト等でしばしば見られる典型的な「なりすまし」型の顧客誘引手法により、真実はそうではないのに顧客の交際相手となり得る者だと誤信させ、当該サイトの利用料金等の名目で多額の金員を詐取したというものである。金額がかなり高額だということから考えると、顧客の側にも反省すべき点がないとは言えないと思われるが、それが民事上では過失相殺の原因となったり、あるいは、刑事上では詐欺罪の成立を阻害するものとなったりすることはない。まさにそのように顧客が夢中になり正常な判断ができないようにすることを狙った犯罪類型に属するものであり、顧客がそのようになることを意図して計画され実行された犯罪だからである。一般に、加害者の意図したとおりに被害者の判断形成に錯誤や瑕疵が生じた場合、それは、まさに詐欺行為から結果発生までの間の因果の流れが加害者の意図どおりに実現したということを意味するだけである。

東京地裁判決において認定されている罪となるべき事実は、次のとおりである（関係者名等は一部仮名、住所等は一部省略）。

（罪となるべき事実）

被告人3名は、それぞれ東京都千代田区（略）に事務所を置いてインターネットサイトの運営等の事業を行う株式会社Aのアルバイト従業員として、架空の男性会員になりすまして女性会員に電子メールを送信していたものであり、同社は、女性会員から現金をだまし取ることを共同の目的とする多数人の継続的結合体であって、実質的経営者であるBらの指揮命令に基づき、あらかじめ定められた任務の分担に従って一体として行動する組織により、その目的を実現する行為を反復して行っていた団体であるが、被告人3名は、男性会員と連絡先を交換するための手数料等の名目で女性会員から現金をだまし取ろうと考え、それぞれ、別表記載のとおり、共犯者欄記載の者らと共謀の上、被告人甲においては、平成23年10月4日頃から同年11月10日までの間、被告人乙においては、同年10月4日頃から同年11月10日までの間、被告人丙において

料金名下に多額の金員を支払わせた詐欺に該当するものというべきである。被控訴人は、控訴人に対する不法行為責任を免れることはできない」との判決理由が示されている。

は、同年10月11日頃から同年11月10日までの間、Cほか6名に対し、真実は、被告人らがDなどと名乗る架空の男性会員になりすまして電子メールを送信しているのに、実在の男性会員が電子メールを送信しているかのように装って、交際を求める電子メールを送信するなどした上、手数料を支払えば男性会員と連絡先を交換することができる旨のカスタマーセンターからの電子メールや、連絡先交換のために支払った手数料は後に必ず弁済する旨の架空の男性会員からの電子メールを多数回にわたり送信したり、手数料を支払えば架空の男性会員との関係で現金を受け取ることができる旨のカスタマーセンターからの電子メールを送信したりするなどして、Cらに、電子メールの交換を行っている男性会員が実在の人物であり、要求された手数料を支払えば、男性会員と連絡先を交換することができ、かつ、連絡先交換のために支払った手数料は後にその男性会員から弁済を受けることができるとか、手数料を支払えば男性会員との関係で現金を受け取ることができるなどと誤信させ、よって、Cらに、被告人甲及び被告人乙においては、いずれも同年10月6日午後2時1分から同年11月10日午後0時2分までの間、78回にわたり、被告人丙においては、同年10月12日午前10時59分から同年11月10日午後0時2分までの間、48回にわたり、東京都府中市（略）E銀行府中支店に開設された株式会社A名義の普通預金口座ほか1口座に、被告人甲及び被告人乙においては、いずれも現金合計517万8000円を、被告人丙においては、現金合計343万8000円をそれぞれ振込入金させ、もってそれぞれ団体の活動として、詐欺の罪に当たる行為を実行するための組織により人を欺いて財物を交付させたものである。

三　金融機関の送金システムと関連する事例

銀行や信用金庫などの金融機関が提供するオンライン送金サービスは、オンラインでのクレジットカード決済サービス（通常はポストペイの決済サービス）や電子マネー決済サービス（通常はプリペイドの決済サービス）等と同様、現代の社会生活上非常に便利で有益なものであり、欠かすことのできないものとなっている。しかしながら、本人確認が適切に行われず、不正アクセスや電磁的記録の改変等に対する情報セキュリティ上の措置が適切に講じられておらず、または、組織内での非違行為を阻止するための組織内統制が十分に機能していない場合、真実は資金移動がないのに電子計算機に記録されている電磁的記録上では資金移動がなされたものとして情報が改変され、そのように当該電子計算機を機能させ、現金の引き落としや口座データの増加などの犯罪的結果を発生させることが不可能ではない。現実

に、銀行等においてオンラインシステムが導入された当初には、送金金額や払戻可能金額等に制限がなく、また、銀行等の金融機関の経営陣が電子計算機を用いた自動処理それ自体に不慣れであったことから、その実務上の諸問題について明確な問題意識を持つことができず、それゆえ、システム監査が適正に実施されていなかったことなどから、マスコミを騒がせるような大事件が続出した。もし取得する対象が現金だけという状況の下であれば、それが法的には横領・背任・詐欺のいずれに該当するかについて議論の余地はあり得るにせよ、非常に高額の被害額となるような犯罪を遂行するにはそれなりの物理的困難が伴う。ところが、電磁的記録の改変や電子計算機の無権限操作だけで巨額の資金移動が可能である状況では、ごく普通の従業員によって、驚くべき高額の被害を発生させ得る犯罪が遂行されてしまうことがあり得る。そのようなタイプの事件は、属に「オンライン詐欺」と呼ばれていた。この種の事件に関する判決中の幾つかは公式判例集等にも登載されている。

以下、詐欺罪（刑法246条）が成立するとされた事例、電子計算機使用詐欺罪（同法246条の2）が成立するとされた事例、詐欺罪と電子計算機使用詐欺罪の両方が成立するとされた事例の3つの類型に分け、その識別点を意識した上で若干の考察を試みる。

1　詐欺罪の事例

オンライン詐欺の事案として最も有名な事件は、いわゆる「三和銀行オンライン詐欺事件」である。この事件については、大阪地方裁判所昭和57年7月27日判決・判例時報1059号158頁がある(19)。

この判決では、被告人両名に対し、いずれも懲役2年6月の判決が宣告された。

事案の概要は、まるで推理小説が現実化したものであるかの如きドラマ性を有するものである。そして、その事実関係については、本論文中においてその要約を示すよりも判決文中に詳細に事実認定されているところをそのまま引用するほうがむしろ本件の事案としての流れを理解しやすいと考えるので、長文になるが引用することにする。同判決中の事実認定部分（「被告人両名の身上、経歴およびその関係」及び「罪となるべき事実」）は、以下のとおりである（関係者名等は一部仮名、

(19) 判例評釈として、友松義信「三和銀行オンライン詐欺事件」別冊NBL79号サイバー法判例解説144頁がある。

住所等は一部省略）。

（被告人両名の身上、経歴およびその関係）

被告人Yは昭和45年3月、立正大学を卒業後、旅行業者である東急観光株式会社に入社し、営業あるいは外国旅行の添乗員として稼働していたが、昭和47年に結婚した妻の実家が寺院で、大阪府茨木市内で霊苑の分譲、管理を業とするA霊苑管理事務所を営んでいたことから、右経営を手伝うため、昭和49年末ころ、右東急観光株式会社を退社してこれに勤務し、その後、墓地の管理などを目的として設立されたA管理サービス株式会社の専務取締役を経て、昭和54年に右会社と同様の営業目的で妻の母親を代表取締役として設立されたA管理株式会社の取締役となり、主として渉外業務を担当するとともに、昭和50年から、友人に頼まれフィリピン、マニラ市所在の旅行案内業「エアーアンドカーゴトラベルコーポレーション（略称ACトラベル）」を引継いで経営していたもの、被告人Xは、昭和42年3月京都市内の明徳商業高校を卒業後、三和銀行に入社し、以来、大阪府茨木市永代町（略）所在の同銀行茨木支店において、電話交換手、普通預金係を経て、昭和47年からは当座預金係として稼働していたものであるが、被告人Yは、前記茨木霊苑事務所が三和銀行茨木支店に当座預金口座等を開設していたことや、同被告人自身も同支店に個人の当座及び普通預金の各口座を開設していたことから、昭和50年ころから同支店に出入りしていたところ、昭和53年に入り、被告人Yが同支店に開設していた右個人当座預金に残高不足が目立つようになったことから、当座預金係をしていた被告人Xが被告人Yに入金を催促することが多くなるとともに、被告人Yが同支店に来店して現金を被告人Xの許に持参したりすることなどが重なるうちに被告人両名は親しくなり、昭和54年4月ころには情交関係を結ぶに至った。

（罪となるべき事実）

第1、被告人Yは、前記のとおり昭和50年からマニラでACトラベルの経営をはじめたものの、同社には引継いだ際にきかされていたよりも多額の負債があったばかりか、仕事の量も当初予想した程とれないうえ、経理や従業員の管理を現地人に任せていたこともあって、ガイド料金などもおもうように入らず、赤字が続く状態となり、このため、当初は妻の実家から金を借りて赤字の穴埋めをしていたものの、昭和53年ころからは、サラ金業者や知人から借金しては同社につぎ込んだため、次第に借金の額がふくれあがり、被告人Xからも情交関係のできた直後からこれらの借金やその利息の支払に充てるため再三に亘り金員を借り受けるなどしてその場しのぎをしてきたものの、昭和56年2月末には同社のマニラにおける負債が約3,000万円のほか国内における個人負債が約6,000万円にも達し、金利等に月額約150万円の支払を余儀なくされるに至り、同年3月に入ると倒産必至の苦境に追い込まれていたものであるところ、被告人Yは、同年3月3日ころ、同府箕面市内で被告人Xと会った際、同被告人に借金の申

し込みをしたものの、これを断わられたため、同被告人に対し、永い間銀行に勤めているのだから何とか銀行から金を引き出す方法はないのか、と尋ねたところ、当時、既に三和銀行では本店のコンピューターと各支店の端末機を結び情報を集中管理するいわゆるオンラインシステムを導入しており、各支店行員において端末機を操作して他支店発行の預金通帳に入金記帳ができ、かつ、同時にコンピューターに組み込まれた当座預金口座に入金を入力しうる仕組みになっていたため、同被告人から、他の支店へ入金する金を同銀行茨木支店で代受けした形でコンピューターに入金を打ち込めば他の支店にすぐ入金されるので、その支店から金を引出す方法がある旨きかされたことから、被告人Yは、現在の窮状を抜け出すためには、自分に好意を持ち、従順であった被告人Xに頼んで右の方法で同銀行から金員を騙取するほかないと決意し、同被告人に対し、犯行後直ちに国外へ逃亡すれば逮捕されることはないので、右の方法での金員の騙取を考えて欲しい旨頼むとともに、被告人Yは、右の話の中で被告人Xから、多額の金を引き出すには普通預金より当座預金の方が不自然でないが当座預金口座は容易には作れないという話が出た際、当座預金口座は暴力団に頼めば簡単に作れる旨同被告人に話してあったことから、この際、同被告人に右の方法による犯行を決意させあるいはその翻意を防ぐため、右の犯行に暴力団が関与しているように装うこととし、その後、同月8日迄の間、電話であるいは同府高槻市内の淀川堤防や茨木市内の安威川堤防などで直接会って、同被告人に対し、再三右犯行を決意するよう懇願するとともに、逡巡する同被告人に対し、預金通帳の作成などを暴力団に頼んでしまったので、ここで中止すると落し前をとられるし、これをきちんとしないと自分も殺されるし、同被告人も銀行にいられなくなる等とその事実がないのにあたかも暴力団が関与しているかのように申し向けて決意を促し、一方、被告人Xは、この間、被告人Yから犯行を決意するよう懇願されたものの、右犯行は当日のうちに犯行自体ばかりかその犯人が自分であることまでもが発覚するものであるうえ、犯行後逮捕を免れるためには国外へ逃亡しなければならないものであったことから、当初はこれを断わっていたものの、被告人Yに対する愛情からこれを断われば同被告人から捨てられるのではないかとのおもい、また、年老いた両親との潤いのない生活や職場に対する不満、さらには、被告人Yとは別の妻子ある男性との長い交際の間に婚期を逸したことによる前途に対する失望感などから、同被告人の懇願を受け入れることによって新しい生活が開けるかもしれないとの期待と、前記の同被告人の暴力団が関与している旨の言葉から、遂に前記の方法による犯行を決意するに至り、同月8日、前記安威川堤防で被告人Yと会った際これを承諾し、ここにおいて被告人両名共謀のうえ、同月9日、同府豊中市内のホテルにおいて、騙取金額は2億円とすること、騙取は架空名義の普通預金口座を利用し、この預金通帳を偽造する方法で行うこと、右の架空名義の普通預金口座は、犯行が当日茨木支店閉店後直ちに発覚することから、限られた時間内での犯行の完了と被告人Xの国外脱出を成功させるため、預金引出が容易な右茨木支店周辺の支店および同被告人の国

外脱出の経路にあたる東京の支店に開設することとし、その通帳と印鑑とを入手しておくこと、犯行日は銀行が最も多忙でかつ多額の現金が用意されている25日とすること、犯行後被告人Xは、被告人Yの知人Bがおり、警察力の弱いマニラへ逃亡することとし、その際、出発は警察の手配のされにくい羽田空港からとすること、などの謀議をした後、同月12日、被告人両名は上京し、翌13日、鈴本、佐々木の各印鑑を購入したうえ、東京都港区新橋（略）所在の同銀行新橋支店に架空人鈴本吉男名義で、同区虎ノ門（略）所在の同銀行虎ノ門支店に架空人佐々木武男名義で、それぞれ金1,000円を預金し、次いで帰阪したうえ、大阪府吹田市元町（略）所在の同銀行吹田支店に架空人鈴本啓一名義で、同府豊中市中桜塚（略）所在の同銀行豊中支店に架空人佐々木健一名義で、それぞれ金1,000円を預金して、右各支店発行の各架空人名義の普通預金総合口座通帳各1通を入手し、その後同月24日までの間に、さらに、架空入金の額は大阪の支店は各3,000万円、東京の支店は各6,000万円とすること、架空入金後入金票およびジャーナルを処分すれば架空入金の事実が茨木支店独自では解明できず時間がかせげることからこれらを処分すること、架空入金後預金の引出は被告人Xにおいて行い、その際できるかぎり現金とするとともに、怪しまれないように多少預金を残すこと、などを取り決めたほか、被告人Xにおいて当時の自宅において、吹田支店分として鈴本啓一名義で金額2,500万円の、豊中支店分として佐々木健一名義で金額2,500万円の、新橋支店分として鈴本吉男名義で金額5,300万円の、虎ノ門支店分として佐々木武男名義の金額5,200万円の、各普通預金総合口座払戻請求書を作成するとともに、架空入金の方法は現金代受けは現金有高が閉店後早急に照合されて不正が発覚することから振替代受けにすることを決めたほか、被告人両名で被告人Xの勤務する右茨木支店から右吹田支店迄の所要時間を実際に車を走らせて預金引出に要する時間を計るなどした後、被告人Xにおいて、

1、同月25日午前10時0分ころ、右茨木支店において、行使の目的をもってほしいままに、同支店77号端末機を操作して前記吹田支店発行の鈴本啓一名義の預金通帳のお預り欄に、同日金3,000万円の振替入金があり、これを右茨木支店が代受けしたように偽りの記帳をなし、もって右吹田支店作成名義の私文書1通を偽造し、同時にコンピューターに組み込まれた鈴本啓一名義の右預金口座にその旨入力したうえ、同日午前11時25分ころ、右吹田支店に赴き、同支店係員に対し、右偽造した通帳をあたかも真正に成立したもののように装って鈴本啓一名義の金額2,500万円の普通預金払戻請求書と共に提出行使し、同係員をして払戻請求のあった金額が真正に入金されているものと誤信させ、よって、即時同所において同人から預金払戻名下に現金2,500万円の交付を受けてこれを騙取し、

2、前同日午前10時3分ころ、前記茨木支店において、行使の目的をもって、ほしいままに、前記端末機を操作して前記豊中支店発行の佐々木健一名義の預金通帳のお預り金額欄に、同日金3,000万円の振替入金がありこれを右茨木支店が代受けし

たように偽りの記帳をなし、もって右豊中支店作成名義の私文書1通を偽造し、

3、前同日午前10時7分ころ、前記茨木支店において、行使の目的をもって、ほしいままに、前記端末機を操作して前記新橋支店発行の鈴本吉男名義の預金通帳のお預り金額欄に、同日金6,000万円の振替入金がありこれを右茨木支店が代受けしたように偽りの記帳をなし、もって右新橋支店作成名義の私文書1通を偽造し、同時にコンピューターに組み込まれた鈴本吉男名義の右預金口座にその旨入力したうえ、同日午後2時54分ころ、右新橋支店に赴き、同支店係員に対し、右偽造した通帳をあたかも真正に成立したもののように装って鈴本吉男名義の金額5,300万円の普通預金払戻請求書と共に提出行使し、同係員をして払戻請求のあった金額が真正に入金されているものと誤信させ、よって即時同所において、同人から預金払戻名下に現金500万円および同銀行新橋支店長服部健吉郎振出しにかかる金額4,800万円の小切手1通の交付を受けてこれを騙取し、

4、前同日午前10時24分ころ、前記茨木支店において、行使の目的をもって、ほしいままに、前記端末機を操作して前記虎ノ門支店発行の佐々木武雄名義の預金通帳のお預り金額欄に、同日金6,000万円の振替入金があり、これを右支店が代受けしたように偽りの記帳をなし、もって右虎ノ門支店作成名義の私文書1通を偽造し、同時にコンピューターに組み込まれた佐々木武雄名義の右預金口座にその旨入力したうえ、同日午後3時20分ころ、右虎ノ門支店に赴き、同支店係員に対し、右偽造した通帳をあたかも真正に成立したもののように装って佐々木武雄名義の金額5,200万円の普通預金払戻請求書と共に提出行使し、同支店係員をして払戻請求のあった金額が真正に入金されているものと誤信させ、よって即時同所において、同人から預金払戻名下に現金2,000万円および同銀行虎ノ門支店長渡辺弘振出しにかかる金額3,200万円の小切手1通の各交付を受けてこれを騙取し、

第2、被告人YおよびCの両名は、いずれも本邦内に住所を有する居住者であるが、共謀のうえ、大蔵大臣の許可を受けず、かつ法定の除外事由がないのに、Cにおいて、同年4月5日、千葉県成田市三里塚字御料牧場（略）所在の新東京国際空港から香港行旅客機に支払手段である本邦通貨をもって表示される前記第1の3記載の同銀行新橋支店長服部健吉郎振出しにかかる金額4,800万円の小切手1通および前記第1の4記載の同銀行虎ノ門支店長渡辺弘振出しにかかる金額3,200万円の小切手1通を携帯して搭乗したうえ、香港に向け出発し、もって支払手段を輸出し、

第3、被告人YおよびDの両名は、いずれも本邦内に住所を有する居住者であるが、共謀のうえ、大蔵大臣の許可を受けず、かつ法定の除外事由がないのに、Dにおいて、同年3月28日、前記新東京国際空港から香港行旅客機に支払手段である本邦通貨2,200万円を携帯して搭乗したうえ、香港に向け出発し、もって支払手段を輸出したものである。

以上のような事案である。本件詐欺行為が実行された時点は、昭和62年の刑法の一部改正(20)による電子計算機使用詐欺罪（刑法246条の2）が新設される以前である。それゆえ、本件の事案については、もし人間が一切介在しないで電子計算機使用詐欺行為が実行されたとすれば、詐欺罪としては無罪であり、利益窃盗罪が存在しない以上、窃盗罪で対処することもできず、結局、横領罪または背任罪で対処せざるを得ない事案だったと考えられる。本件の犯行を遂行するために実行された電磁的記録の不正作出（不実の送金処理データへの無権限書き換え行為）についても同様である。犯罪事実第2及び第3の行為については、当時における外国為替及び外国貿易管理法70条9号、18条1項、外国為替管理令8条1項、2項、4項、昭和55年大蔵省告示117号、3項、4項が適用されている。現時点では、犯罪収益と関連する諸法規の適用も検討されることになるであろう。

以上のような前提で、大阪地裁判決において、詐欺罪の成立を認めたことは妥当である。当時、銀行内での送金処理についてはオンライン処理が可能となっていた。すなわち、オンラインによる送金処理の過程では人間が介在しないため、電子計算機で処理される電磁的記録の改変行為があっても、人間に対する欺罔行為が存在し得ない。すなわち、この処理過程だけに着目する限り、欺罔行為を必須の構成要件要素とする詐欺罪（刑法246条）が成立する余地はない。しかしながら、本件の被告人Xは、詐欺行為遂行の手段としての不実の送金処理によって生成された口座残高が存在することを前提に、複数の銀行窓口において、預金を払い戻すために用いる申込用紙等（私文書）を偽造し、窓口の担当銀行員に対して、これを提出して行使し、その銀行員を欺罔して現金または小切手を詐取したのであるから、この時点の行為をとらえれば、明らかに詐欺罪（刑法246条1項）が成立する。

刑法一部改正により電子計算機使用詐欺罪（同法246条の2）が新設された後である現時点では、同罪が適用可能である。もし本件と同様の事案について同罪を適用するとすれば、送金先口座に対する送金処理が完了し、口座残高を増加させる不実の電磁的記録が作成された時点で、財産上の利益を違法に獲得したことになるか

(20) 刑法改正の概要については、米澤慶治編『刑法等の一部改正法の解説』（立花書房、1988）が詳しい。なお、電子計算機使用詐欺罪の解釈・運用上の問題点については、前掲「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—」で詳論したとおりである。

ら、その時点で、電子計算機使用詐欺罪が既遂となる。その後の現金や小切手の入手行為は、電子計算機使用詐欺罪との関係では不可罰的事後行為として評価することになる。それゆえ、一般的には、私文書偽造罪と同行使罪と詐欺罪とは、全体として牽連犯となるが、本件のような事案について電子計算機使用詐欺罪が適用される場合には、①電子計算機使用詐欺罪と②私文書偽造罪及び同行使罪（この2罪の関係は牽連犯）とは、全体として牽連犯となるのではなく、①の犯罪行為と②の犯罪行為とで併合罪の関係に立つことになると解すべきである。

2 電子計算機使用詐欺罪の事例

既述のとおり、刑法一部改正により電子計算機使用詐欺罪が新設された後の時点においては、金融機関の送金処理等について人間が介在することがなく、それゆえ人間に対する欺罔行為も存在し得ない事案について、実質的には利益窃盗行為として評価可能なものとして電子計算機使用詐欺罪の適用が可能となった。

現在、いわゆるパソコンバンキングやインターネットバンキングと称されるサービスのように、家庭や事務所のPCから銀行等の金融機関のWebサイトにアクセスしログオンした上で、利用者が直接に口座データにアクセスして送金処理等をすることが可能となっている。このような仕組みをコンビニエンスストア店舗内に設置されている専用端末装置（ATM）を用いて実現する仕組みもかなり普及している。これら様々な態様のものを、一般に、ネットバンキングと呼んでいる。

ネットバンキングにおいても、例えば、ATM装置から現金の払い出しを受ける行為のような場合には、財物である現金の占有取得行為として、通常の窃盗罪の適用を考えることが可能である(21)。これに対し、送金処理だけで既遂と達するよ

(21) 誤送金等により口座残高が増加していることを知り、誤った口座残高だということを認識しつつATM等で払い戻しを受け現金を取得する行為は、窃盗罪に該当する。この例の場合、電子計算機使用詐欺罪が成立する余地はないし、人間に対する欺罔行為が存在しないので詐欺罪も成立せず、増加した残高は物体としての遺失物でもないので遺失物横領罪が成立する余地も全くない。このような事例は、机上の空論ではなく、現実に存在し得る。例えば、みずほ銀行のシステム統合の際にこのようなタイプの誤送金や混乱が生じた実例がある。関連する事例として、いわゆる振り込め詐欺の「出し子」と呼ばれる預金引き落としを担当する共犯者について、電子計算機使用詐欺罪や詐欺罪に関する共謀が認められない場合には、窃盗罪が成立するとの判断を示した名古屋高等裁判所平成24年7月5日判決・高等裁判所刑事裁判速報集平成24年207頁がある。この判決では、ATM端末装置の占有に対する侵害として論じている。しかし、この論理は、結論

うな事案では、人間が介在しておらず、人間に対する欺罔行為が存在し得ない以上、電子計算機使用詐欺罪の成否が検討されることとなろう。

さて、地方銀行でネットバンキングが開始されると、すぐに専門技能を悪用した犯罪が実行されることとなった。最も有名な事案は、東海銀行で発生した事件で、ホワイトカラー犯罪としての側面と組織犯罪としての側面の両面をもつ犯罪学上でも非常に興味深い事例の一つとなっている。その判決は、名古屋地方裁判所平成9年1月10日判決・判例時報1627号158頁(22)として公開されている。

この判決では、被告人両名について、懲役6年の刑が宣告された。

この判決において「罪となるべき事実」として事実認定された犯罪事実は、次のとおりである（関係者名等は一部仮名、住所等は一部省略）。

（罪となるべき事実）

被告人両名は、C（被告人Aの関係で分離前の相被告人）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1　平成6年12月9日午後5時32分ごろ、千葉市花見川区（略）所在の前記D経営にかかる株式会社甲野開発センター事務所において、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（略）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、株式会社乙山が東海銀行八重洲支店に開設している普通預金口座から右甲野開発センターが両総信用金庫都賀支店に開設している普通預金口座に1億4000万円の払込送金があったとする虚偽の情報を与え、同月12日午前9時ごろ、同

を左右するものではないにしても論理それ自体としては明らかに誤りであり、現金という財物に対する占有を考えるべきである。ATM端末装置は、財物である現金に対する占有を物理的に保持するための装置（手段）に過ぎない。なお、このような事例において、「出し子」が現金で払い戻すのではなく、更に他の口座へと送金（転送）するという事案を想定してみると、占有の奪取が一切ないので窃盗罪も成立しない。また、電子計算機使用詐欺罪の成立も認められない。利益窃盗罪を正面から認めた立法をしなかった立法上の過誤の一種として理解することが可能である（ただし、電子計算機使用詐欺罪制定時における日弁連の立場は、利益窃盗罪について忌避的だった。現実を無視した観念の過剰現象だと言える。この点については、前掲「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—」でも触れたとおりである。）。

(22) 判例評釈として、日高義博「電子計算機使用詐欺罪の成立を認めた事例：東海銀行オンライン詐欺事件」判例時報1661号219頁（判例評論481号57頁）、菅原胞治「東海銀行オンライン詐欺事件」別冊NBL79号サイバー法判例解説150頁がある。

電子計算機に順次接続されている社団法人東京銀行協会全国銀行データ通信センターに設置されている全国銀行通信システム電子計算機及び株式会社しんきん情報システムセンターに設置されている全国信用金庫データ通信システムの電子計算機を介して、東京都港区（略）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右甲野開発センター名義の普通預金口座の預金残高を1億4000万円増加させて、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、1億4000万円相当の財産上不法の利益を得た。

第2　平成6年12月12日、横浜市港北区（略）所在のWホテル新横浜510号室において、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、前記銀行アンサーシステムを介して、前記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、①同日午後5時19分ごろ、株式会社Xが東海銀行丸ノ内支店に開設している当座預金口座からEが株式会社第一勧業銀行新宿支店に開設している普通預金口座に4億円の振込送金があったとする虚偽の情報を、②同日午後5時34分ごろ、株式会社Yが東海銀行本店営業部に開設している普通預金口座から右E名義の普通預金口座に9000万円の振込送金があったとする虚偽の情報を、③同日午後5時45分ごろ、Z株式会社が東海銀行大阪支店に開設している当座預金口座から右E名義の普通預金口座に10億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13日午前9時ごろ、同電子計算機に順次接続されている前記全国銀行通信システムの電子計算機及び東京都渋谷区（略）所在の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を介して、同所に設置されている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右E名義の普通預金口座の預金残高を14億9000万円増加させて、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、右Eに14億9000万円相当の財産上不法の利益を得させた。

この犯罪事実に関する事実認定のみでは、この事件のもつ犯罪学上及び情報セキュリティ上の重要性を正しく認識することができない。この事件の社会現象としての本質を理解し、情報財（情報資産）を保護する情報セキュリティ上の目的に資するためには、犯行に至る経緯を踏まえて詳細な論述のある「量刑の事情」を精読しなければならない。長文になるが、その主要部分を引用する（関係者名等は一部仮名、住所等は一部省略）。

（量刑の理由）

一　前掲証拠及び被告人Aの経歴に関する同被告人の警察官調書によって認められる被告人らの経歴と本件犯行に至る経緯は、次のとおりである。

1　被告人Aは、高等学校を中退後、家業の材木商を手伝い、その後宝石商、材木商、不動産仲介業等をし、この間に詐欺罪等の犯行を重ねて服役した。そして、出所後不動産仲介を目的とする会社や石油類の小売りを目的とする会社を設立して、これらの会社を経営している。被告人Bは、防衛大学で基礎工学を専攻してコンピューターについて勉学し、同大学卒業後コンピュータープログラムの製作会社に勤務したが、2年ほどで辞めて、自らコンピュータープログラムの製作会社を設立した。しかし、この会社が倒産し、その後医療機器関係の会社やコンピューター関係の人材派遣会社等を設立したものの、いずれも倒産し、平成4年ごろから携帯電話の販売業をしていたが、重なる倒産で多額の借金を抱えていた。共犯者のCは、株式会社東海銀行の行員であったもので、同行のコンピューターの管理をしている同行師勝センターシステム部に所属し、同部システム設計第一リージョン外為グループに配属されて、オンラインの顧客取引情報を銀行内の各部にコンピューターを通じて流す作業に従事していたが、サラ金等からの借金がかさみ、その返済に窮していた。共犯者のDは、甲会系の暴力団組長で、株式会社X開発センターを経営しており、被告人Aとは不動産売買や地揚げ等の仕事を一緒にして長年の付き合いがあった。

2　本件犯行に利用された東海パソコンサービス（アンサー利用型）は、NTTデータ通信株式会社が提供している自動照会システムである銀行アンサーシステムを利用して行なわれるエレクトロニック・バンキング（電子決済システム）サービスの一つである。銀行アンサーシステムは、NTTの一般公衆回線を利用して銀行システムのダイレクトフロントコンピューターにアクセスできるシステムで、顧客は、右東海パソコンサービス（アンサー利用型）の契約をすれば、パーソナルコンピューター（パソコン）等の端末を利用して銀行のコンピューターにアクセスして、残高照会、振込、振替等のサービスを受けることができるものである。また、本件犯行に利用された都度指定方式による振込サービスは、顧客が振込の都度、振込金融機関と振込口座を指定できるもので、事前に振込口座を届け出て登録する必要のないものである。そして、この方式を利用するには、3種類の暗証番号（固定暗証番号、確認暗証番号、承認暗証番号）をパソコンに入力することになっていた。そのため、顧客以外の者でも、顧客の契約している店番、口座番号、暗証番号等のデータを入手して、この暗証番号等を解析できれば、その顧客の口座の資金を移動することができた。

3　Cは、前記のとおり借金の返済に窮していたが、平成6年4月ごろ、スポーツ新聞に掲載された融資関係の広告を見たことをきっかけにして知った金融会社の関係者らから被告人Bを紹介された。被告人Bは、右紹介者から、Cについて、コンピューター関係の部署にいる銀行員で、サラ金から借金をして困っており、その立

場を利用して金をつくることを考えている人物であると説明を受けて、Cを紹介された日に、Cらと銀行の顧客データを流して金にすることなどを話し合った。そして、その後、被告人Bは、銀行の顧客データの買手をさがし、右紹介者やその知人の暴力団関係者を通じて知った被告人Aに対して、Cについて説明して、銀行の顧客データを買う話を持ち掛けた。被告人Aは、金に困って顧客データを外部に流すような行員であれば、金を渡しておけばいずれ銀行に対して不正な工作をするのに利用できるものと考えて、同年7月11日ごろ、被告人Bの紹介でCに会い、Cに顧客リストの入ったテープの代金として500万円を渡し、被告人Bには紹介料として100万円を渡した。

4　Cが被告人Aに渡した右テープは、情報の入ってないものであったが、被告人Aは、先に被告人Bらとの雑談中に、銀行のコンピューターを上手く操作すれば不正送金ができて金が取れるとの話が出たことがあり、その後も被告人Bから同様の話が出たことから、Cを利用してコンピューターの不正操作により大金を取得することを企て、被告人Bにその意図を伝えた。こうして、被告人両名は、同年7月中旬ごろ、Cに対し、コンピューターを使って送金等のサービスを受けられるシステムの顧客データを流すように要求し、同月下旬ごろには東海銀行のパソコンサービスのパンフレットを入手し、Cにそのシステムについて説明させるなどして相談した。そして、その結果、市販のパソコンが使用できて一般電話回線から侵入することの容易なアンサー利用型の都度指定方式を悪用して、多額の資金を移動してこれを騙取することにし、被告人AがCに対し、アンサー利用型のサービスを受けている顧客の店番、口座番号、暗証番号等不正送金に必要なデータを流すように求めた。そして、被告人Aは、共犯者の前記Dを仲間に加え、同人が経営している株式会社X開発センター名義の両総信用金庫の口座を不正送金の受皿となる口座として確保し、さらに、知人を介して、Eが短時間に巨額の現金を用意できる大手都市銀行に顔が利くことを知り、右Eに対し、政治家への献金であるなどと偽って、不正に送金した預金が現金化できるように手はずを整えた。また、被告人らは、被告人Bの知人のFに依頼して、パソコンにアンサーシステムを接続する作業をしてもらい、同人から同システムにアクセスする方法を教わった。

5　一方、被告人らから前記アンサー利用型のサービスを受けている顧客に関するデータの入手を依頼されたCは、いったんは別のデータをアンサーシステムの顧客データであると偽って被告人Aに渡したが、被告人Bがこれに気付き、被告人らから追及されるに及んで、同年11月ごろ、システム部外部接続グループの所属員に対して「外為関係のシステム開発に必要だ」などと嘘を言って借り出したアンサー契約マスターに関する磁気テープのコピーからイージーリストを作成し、これを被告人Aに渡し、さらに、被告人らの求めに応じて、指定された企業の口座のスクランブル（暗号変換）処理された固定暗証番号及び確認暗証番号等が印字されたダンプリスト

やレイアウトフォーム等を被告人Aに渡し、その見方を被告人らに説明した。そして、同年12月初めごろには、同様にスクランブル処理された承認暗証番号の入ったダンプリストを追加して渡した。

6　被告人らは、前記Fに開設させた口座を使って実際に資金移動ができるか試してみるなどして、最終的に右のようにしてCから渡されたスクランブル処理された暗証番号の全てを解析することに成功し、同年12月9日及び同月12日の両日、判示のとおり、それぞれ不正送金を実行した。その際、被告人らは、犯行が発覚するのをできるだけ遅らせるために、企業の一般的な業務終了時刻である午後5時以降に犯行を実行することにして、ターゲットにした企業の全てについて、同月9日（金曜日）の午後5時以降に不正送金を実行しようとして、まず、判示第1の犯行を実行したが、次に実行を予定した企業について、資金移動のための入力を試みて失敗したため、同月12日（月曜日）の午後5時以降に判示第2の犯行を実行したものである。なお、判示第2の犯行は、現金化する前に犯行が発覚して現金化はできなかったものである。

二　本件は、このように、被告人らが、コンピューターを駆使するエレクトロニック・バンキング（電子決済システム）サービスの一つである都度指定振込サービスを悪用して、合計16億3000万円をその支配する預金口座に振込入金させて同額の財産上不法の利益を得て、このうち14億9000万円については、早期に発覚して預金口座からの引き出しに失敗したものの、1億4000万円については、預金口座から引き出して、その現実の利益を取得した電子計算機使用詐欺の事案である。

この種のサービスは、時代の要請であり、その利便性が評価されて各企業に浸透し、その利用が増加している現状において、本件犯行は、こうしたサービスに対する信用の低下を招き、金融機関や企業の関係者に多大の衝撃を与え、特に金融機関においては、都度指定方式によるサービスの安全性の再検討を迫られるなど、これが社会に与えた影響は極めて大きい。また、被害に遭った銀行に対しても、信用の低下や口座から引き出された顧客に対する賠償はもとより、善後策を含めて多大の出費を余儀なくさせたものである。

被告人らは、自己の利得や借金の返済資金を得るために、こうした犯行を極めて周到に計画して準備し、巧妙な手口で多重の防御システムを突破して敢行し、前示のような多額の資金を預金口座に入金させ、そのうち1億4000万円については、預金口座から引き出して、その現実の利益を取得したものであって、動機に特に酌量する点がない上、犯行は計画的かつ悪質であり、犯行の結果も重大である。

被告人らのうち、被告人Aについては、本件の一連の犯行を敢行するに当たって、共犯者に対して随時必要な指示を与えるとともに、資金や場所などを提供し、資金移動の受皿となる口座を確保し、目標とする企業や引出金額を最終的に決定するなど、主犯的な立場にあったものである。また、判示第1の犯行で得た1億4000万円については、警察官調書と公判供述とで受領した現金についてそごする点がみられるが、現金と

小切手を合わせてその半額近くを取得している。被告人Aは、こうした自己の取り分について、判示第2の犯行による多額の入金を信じていたことから、そのうちの多くを関係者の求めに応じて貸し付けたこと、受領した手形類が不渡りになったこと、Cや被告人Bに対して分配金（合計400万円）を渡していること、犯行のために相当の経費を使っていることなどを挙げて、差し引きすればそれほどの利得は残らなかった旨供述しているが、そのような事情があったとしても、被告人Aは、相当の取り分を自己の支配下に置いたものということができる。加えて、被告人には、過去に窃盗罪や詐欺罪などの財産犯の前科があるところ、その中には銀行員を教唆して約束手形を窃取させた事案も含まれている。

次に、被告人Bは、被告人Aに比して従たる立場にあったとはいえ、Cを被告人Aに紹介したり、振込サービスを悪用して大金を不正送金できる話を持ち出すなどして本件犯行のきっかけをつくった上、自らのコンピューターに関する豊富な知識を提供して、Cから受領した暗号等のデータを解析したり、実際にパソコンを操作するなどの重要な役割を分担したもので、その存在は本件犯行に欠くことのできないものであった。そして、被告人Bは、当初の紹介料として受け取った100万円の中から自己の分として34万円を取得したほか、判示第1の犯行の分け前として被告人Aから現金100万円を受け取っており、他に宿泊代や飲食代も提供されていたもので、判示第2の犯行による現金引き出しが成功していれば、当然更に相当の分け前に与ることができたものである。

この「量刑の事情」を読めば理解できるとおり、本件事案は、①犯罪組織である暴力団の構成員Dと犯罪歴のある被告人Aとが主導的な役割を果たしているという点で、組織犯罪としてのサイバー犯罪という側面を有し、②大学で工学に関する専門的な教育を受け、IT関連の経営の経験があって、いわば高度な知識・能力を有する技術者である被告人Bが実質的な犯罪行為実行者となっているという点で、高度な専門技能を悪用した犯罪としてのサイバー犯罪としての側面を有し、そして、③被害者である東海銀行の従業員であり、顧客データ等を保守・管理すべき立場にありながら、サラ金等からの借財がかさんで暴力団員に弱みを握られていたCが不正アクセス等のために必要な機密データを他の共犯者らに横流した結果、現実に本件犯行を遂行可能になったという意味で、いわゆるホワイトカラー犯罪としての側面及び企業の内部統制失敗例としての側面を有している。これらの要素のうち、③の顧客データ等の機密情報の闇市場での流通は近時における深刻な社会問題となっているもので、関連して各種サイバー犯罪を惹起する動因となり得るととも

に国防という観点からも由々しき問題を発生させ得るものである(23)。これらサイバー犯罪において夙に指摘されてきた諸要素が全て盛り込まれている事案として、いわば金融機関を被害者とするサイバー犯罪の基準標本的な位置づけにある事例だと評価することも可能であろう。情報セキュリティとしての情報財の保護・リスク管理の立場からは、このような複合的な要素を個別的に詳細に検討することが重要であることは言うまでもないが、それと同時に、情報セキュリティのためには、単に技術面における対応を考えるだけでは十分ではなく、人間系の課題についても綿密な検討を加え、しかるべき対応策を講じておくことが重要であると考える。ただし、その際に留意しなければならないことは、加害者となり得る者は使用者の指揮命令に服する従業員だけとは限らないということである。企業犯罪やホワイトカラー犯罪においては、例えば、粉飾決算がそうであるように、企業経営者（経営陣）が主体となり、組織的に遂行しなければ実現できない犯罪類型が存在する。サイバー犯罪の中には、そうしたものが決して少なくないという事実を直視しなければ、真の解決策・対応策を得ることはできないであろう(24)。

(23) そのような問題点については、前掲「サイバー犯罪の研究（二）—フィッシング（Phishing）に関する比較法的検討—」及び「サイバー犯罪の研究（三）—通信傍受に関する比較法的検討—」で触れたとおりであるほか、夏井高人「サイバー犯罪の研究（五）—サイバーテロ及びサイバー戦に関する比較法的検討—」法律論叢86巻2・3号85～134頁で詳論したとおりである。

(24) 現在の情報セキュリティマネジメントシステム（ISMS）は、マネジメントの主体である経営陣及び経営陣と同視することのできる管理職従業員は「悪をなさない」という前提で理論体系が構築され、監査を含めた運用がなされている。しかし、現実には、様々な企業犯罪の事例をみれば即座に理解することができるとおり、まさにその経営陣が「悪をなす」事例が決して少なくない。この点において、現在の情報セキュリティマネジメントシステム（ISMS）が全く機能しない課題が存在するという事実を承認することが大事である。現在の情報セキュリティマネジメントシステム（ISMS）によって対処可能な事柄についてはその適正な構築・運用によるべきである。しかし、現在の情報セキュリティマネジメントシステム（ISMS）が機能しようのない課題については、全く別の理論を構築し、適正に実務運用することが急務となっている。これは、根本理論の部分におけるパラダイムシフトを伴うことであるので、従来の情報セキュリティマネジメントの専門家では対応できない課題の一つでもある。比喩的に言えば、従来の発想は「神の神は存在しない」というものであったのであるが、今後は、「神の神が存在する」を想定する必要がある。

3　詐欺罪及び電子計算機使用詐欺罪の事例

詐欺罪と電子計算機使用詐欺罪の両方の罪（併合罪）を認定した事例もある（同一の行為について詐欺罪と電子計算機使用詐欺罪の両方が成立する事例という趣旨ではない。）。そのような事例の代表例として、大阪地方裁判所昭和63年10月7日判決・判例時報1295号151頁[25]をあげることができる。詐欺罪の構成要件と電子計算機使用詐欺罪の構成要件の相違を理解する上で有用だと思われる。

大阪地裁判決では、被告人両名に対し、懲役1年6月（被告人Yについては執行猶予4年）の刑が宣告された。

この判決において認定された「罪となるべき事実」は、次のとおりである（関係者名等は一部仮名、住所等は一部省略）。

（罪となるべき事実）

被告人Xは、大阪市西区九条（略）所在の株式会社第一勧業銀行九条支店に勤務し、預金・為替業務に従事していたものであって、A（昭和23年7月12日生）と親密な交際をしていた者、被告人Yは、Aの親しい友人であるが、

第1　被告人Xは、

1　別表記載のとおり、昭和62年7月27日午後2時55分ころから同年9月4日午前8時39分ころまでの間、3回にわたり、第一勧業銀行九条支店において、同銀行オンラインシステムの預金端末機を操作して、東京都渋谷区渋谷（略）所在の同銀行東京事務センターに設置され同銀行の預金の残高管理、受入れ、払戻し等の事務処理に使用される同システムの電子計算機に対し、実際には振替入金の事実がないのにもかかわらず、被告人Xの同支店普通預金口座（総合口座取引のもの）に20万円、30万円、20万円の振替入金があったとする虚偽の情報を与え、同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同口座の預金残高を4万7527円、17万1446円、4万9582円として財産権の得喪、変更に係る不実の電磁的記録を作り、よって、合計70万円相当の財産上不法の利益を得た。

2　Aと共謀のうえ、同年9月9日午後0時38分ころ、第一勧業銀行九条支店において、被告人Xが、前記預金端末機を操作して、前記電子計算機に対し、実際には振替入金の事実がないのにもかかわらず、Aが知人のBから預金を払い戻すことを認められている同人の同支店普通預金口座（総合口座取引のもの、預金残高100円）

(25) 判例評釈として、芝原邦爾「コンピュータ詐欺」別冊ジュリスト117号刑法判例百選Ⅱ各論（第3版）98頁がある。

に90万円の振替入金があったとする虚偽の情報を与え、前記磁気ディスクに記録された同口座の預金残高を90万100円として財産権の得喪、変更に係る不実の電磁的記録を作り、よって、90万円相当の財産上不法の利益を得た。

第2　被告人両名は、Aと共謀のうえ、偽造した振込依頼書を用い、第一勧業銀行九条支店から予め開設しておいた株式会社三和銀行野田支店C名義普通預金口座に振込名下に入金させて利得しようと考え、同年9月29日午後11時ころ、大阪市港区波除（略）甲マンション107号被告人X方において、A及び被告人Yが、行使の目的をもって、ほしいままに予め入手しておいた第一勧業銀行九条支店備付けの振込依頼書用紙1枚の振込先欄に「三和」銀行「野田」支店、受取人欄に「C」、金額欄に「45,000,000」等と記載するなどしたうえ、依頼人欄に「大和証券（株）西支店」と冒署し、もって、大和証券株式会社西支店作成名義の金額4500万円の振込依頼書1通を偽造し、同月30日午前11時ころ、第一勧業銀行九条支店において、被告人Xが、同支店為替担当係員に対し、右偽造に係る振込依頼書1通をあたかも真正に成立したもののように装い他の正規の振込依頼書とともに回付して行使し、同係員Dをしてその旨誤信させ、よって、同日午前11時23分ころ、同女をして同支店為替端末機を操作させて全国銀行データ通信システムを通じ同支店から同市福島区吉野（略）三和銀行野田支店C名義普通預金口座に金4500万円を振込入金させ、もって、右同額の財産上不法の利益を得たものである。

これらの認定事実のうち、第1の各行為では人間が介在しないため欺罔行為が存在せず、口座残高データが改変された時点で電子計算機使用詐欺罪が既遂となる。これに対し、第2の行為では、私文書偽造・同行使によって銀行従業員に対する欺罔行為が実行され、その欺罔による錯誤により、当該従業員が送金処理を行い、送金先口座残高を増加させるという処分行為を行った時点で詐欺罪（刑法246条2項）が既遂となっている。現実の銀行システムでは、どちらの犯罪行為の場合でも同様に電子計算機による処理に基づく口座残高の変動が生ずるわけであるが、口座残高データ（電磁的記録）を直接に無権限で改変する行為であるか、あるいは、情を知らない銀行員等を間接正犯の道具として利用するのと同様の意味で操作し、当該銀行員等の判断・動作に基づいて口座残高データ（電磁的記録）を間接的に無権限で改変する行為であるかの相違だと理解することができる。

四　まとめ

以上で、オンライン詐欺と呼ばれる犯罪行為に含まれる幾つかの犯罪類型のうち、主要なものについて、典型的な事例だと思われる判決を素材とする考察と検討を終える。「オンライン詐欺」という語それ自体は、極めて緩やかに広義に解釈されることがあり、厳密には詐欺類型に属しない犯罪行為を含むことがある。

本論文では、詐欺類型と非詐欺類型との識別点を意識した論述を基本としたが、まだ未解明の検討課題が多々ある。とりわけ、横領罪及び背任罪との関係については、従来の刑法理論に若干問題を含む部分がある。しかし、このような犯罪類型についても正確な考察を踏まえて全体構造を解明しなければ、情報財の刑事法的保護に関する検討を完了したことにはならない。更に熟慮・研究を重ねた上で、いずれその研究成果を公表したいと考える(26)。

(26) 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23年～平成27年度）による研究成果の一部である。