サイバー犯罪の研究（八）-電子的な横領及び類似行為に関する事例検討-

法律論叢第88巻第2・3合併号（2015.12）

【論　説】

サイバー犯罪の研究（八）

――電子的な横領及び類似行為に関する事例検討――

夏　井　高　人

目　次

1　はじめに
2　電子的な横領と背任
　2．1　理論的な検討
　　2．1．1　電子的なトークンとその侵害行為
　　2．1．2　財産罪としての基本類型
　　2．1．3　横領罪と背任罪
　　2．1．4　利益横領行為の理解
　2．2　裁判例
　　2．2．1　電子計算機使用詐欺罪における「虚偽の情報」の意義
　　2．2．2　電子計算機使用詐欺罪と背任罪との関係
　　2．2．3　電子計算機使用詐欺罪と背任罪が混在する事例
3　電子装置を用いた料金徴収業務の阻害
　3．1　理論的な検討
　3．2　裁判例
　　3．2．1　電子計算機使用詐欺罪
　　3．2．2　電磁的記録不正作出・同供用罪
　3．3　罪数
4　加害目的での背任罪と電子計算機損壊等業務妨害罪の罪数
　4．1　理論的な検討
　4．2　裁判例
　4．3　罪数
5　まとめ

1 はじめに

コンピュータシステム（電子計算機）を用いた財産権の管理や処理が普及して既に久しい。とりわけ、電子的な決済の普及が著しい(1)。物的なものと電子的なものとを含め、財物や債権等の財産権の管理は、基本的にコンピュータシステムを用いて実行されるのがむしろ普通である。

一般に、財産権に対する侵害行為の中で、物体（財物）(2)である財産権に対する他人の占有や管理を奪うことを基本的な内容とする犯罪類型に属する行為は、窃盗罪（刑法235条）、詐欺罪（同法246条）を構成することが多く、そのような犯罪行為は刑法によって規律・処罰され得る(3)。これに対し、自己の占有・管理下にある他人の財産権を違法に領得する行為については、刑法上では、横領罪（同法252条～255条）または背任罪（同法247条）に該当する。以上については、学説上も判例上も特に異論はないと考えられる(4)。

---

(1) 電子決済一般に関しては、Martin Peitz, Joel Waldfogel (eds.), The Oxford Dictionary of the Digital Economy, Oxford University Press, 2012, pp. 108–135、松本恒雄・齋藤雅弘・町村泰貴編『電子商取引法』（勁草書房、2013）117～154頁[杉浦宣彦]が参考になる。なお、電子的な契約に伴う様々な法的問題に関する公的なガイドラインとしては、経済産業省『電子商取引及び情報財取引等に関する準則』がある。情報財の基本概念については、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頁で述べた。

(2) 大塚仁・河上和雄・佐藤文哉・古田佑紀編『大コンメンタール刑法（第2版）第12巻』（青林書院、2000）169～189頁、団藤重光編『注釈刑法(6)各則(4)』（有斐閣、1966）2～10頁、山口厚『刑法各論[第2版]』（有斐閣、2010）169～171頁、西田典之『刑法各論（第6版）』（弘文堂、2012）135～142頁、前田雅英『刑法各論講義（第5版）』（東京大学出版会、2011）224～238頁、藤木英雄『刑法各論』（有斐閣、1972）30～31頁など。

(3) 窃盗罪、詐欺罪及び電子計算機使用詐欺罪の本質と罪数関係については、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61～109頁、同「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―」同誌87巻1号163～206頁で既に論じた。また、恐喝財と詐欺罪との関係については、同「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―」同誌86巻6号181～243頁（特に224～230頁）で既に論じた。

(4) 横領罪と背任罪の罪質及び相互関係に関しては、刑法学説上・理論上の議論はあった（大塚仁・河上和雄・佐藤文哉・古田佑紀編『大コンメンタール刑法（第2版）第13巻』（青林書院、2000）219～239頁、前田雅英編『条解刑法（第3版）』（弘文堂、2013）781～791頁、前掲『注釈刑法(6)各則(4)』324～337頁、前掲山口厚『刑法各論[第2版]』305～310頁、318～320頁、前掲西田典之『刑法各論（第6版）』237～243頁、253～255頁、264～268頁、前掲前田雅英『刑法各論講義（第5版）』379～387頁、390～393頁、406～411頁、前掲藤木英雄『刑法各論』56～61頁）。しかし、本論文は、この点に

しかし、加害行為の対象となる財産権が純粋な電磁的記録または電子的な状態の場合、そのような財産権は世俗的な観念や常識的な通念の上では「物体」(5)の範疇に入らないと考えられているため(6)、「占有」や「所持」という概念が成立せず、強いて言えば「管理」という概念が成立し得るのみである。そのことから、まま解

関する刑法理論や学説史の研究を主たる目的とするものではないので、深入りすることを避ける。

横領罪と背任罪との関係に関して判示した裁判例としては、「信用組合の支店長等が、支店の預金成績の向上を装うため、勧誘に応じた一部預金者に対し、正規の利息の外に多額の金員を自己の業務上保管する組合の金員中から預金謝礼金名下に勝手に支出交付し、同謝礼金を補填するため、正規に融資を受ける資格のない者に対し、前同様組合の金員を貸付名下に高利をもって勝手に支出交付したときは、それが自己の計算においてなされたものである限り、いずれも業務上横領罪を構成する」との判断を示し、「被告人等の所為が背任罪を構成することあるは格別、横領罪を構成することはあり得ない」との上告人の主張を排斥した最高裁昭和33年10月10日判決・刑集12巻14号3246頁がある（判例評釈として、佐々木史郎編『判例経済刑法体系第3巻』（日本評論社、2000）73～79頁[恒光徹]、井上正治「横領か背任か」ジュリスト臨時増刊『刑法判例百選』234～235頁、井上祐司「横領と背任の区別について」企業法研究11号221～253頁がある。）。

また、県知事の許可を条件として農地を売渡して代金を受領した者（被告人）が、ほしいままに該農地につき県知事の許可前に第三者のために抵当権を設定しその登記を経たとの事案について、傍論中で「被告人の所論担保権設定行為は背任罪を構成するとした原判決の判断は正当である」と判示した最高裁昭和38年7月9日決定・刑集17巻6号608頁がある（判例評釈として、藤木英雄「背任罪における「他人の事務」―売渡予約済農地の転売と背任罪―」別冊ジュリスト83『刑法判例百選Ⅱ各論（第2版）』124～125頁がある。）。

前者の事案では財産権である金員を貸付・交付するという処分行為が存在するのに対し、後者の事例では財産権である不動産（土地）の物的な処分行為は存在せず、その交換価値を減ずる行為（第三者のための抵当権設定行為）がなされたのに過ぎないという事案上の相違点がある。

(5) 民法上の「物」の概念については、夏井高人「艸―財産権としての植物(2)」法律論叢87巻6号129～172頁で触れた。情報それ自体に対する侵害行為に対する犯罪としての法的評価については、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―」同誌85巻6号363～420頁で述べた。

(6) 地球上に生起する全ての現象は、物理学上では等しくエネルギーの変動という物理現象の一種である。しかし、一般に、物体と物体でないものとは異なる物理現象のように観念されている。人間の認識能力がすべからく非常に優秀な数学者のレベルに達しているわけではないので、やむを得ないことだと考える。それゆえ、法学の領域に属する本論文においては、そのような量子力学的なレベルでの認識については一応措き、通常の法律家にとって認識・理解することが可能なレベルを前提として、物体という物理現象とそれ以外の物理現象とを分けて論ずることとする。ただし、近未来において、本来の意味での量子コンピュータが実現すると、常識的なレベルで認識・理解すれば足りる時代が終わってしまう可能性が高いことには留意すべきであろう。

釈論上疑義が生じ得る(7)。また、ある財産権に対する侵害行為が横領罪または背任罪に該当し刑法上の財産罪としての法的評価を受けると同時に、派生的に他の法益侵害も惹起し得るために他の法令に基づく犯罪も同時に成立し得る場合については、従来、あまり検討されてこなかったように考えられる。

本論文では、種々あり得る他の保護法益侵害中で特に業務遂行の安全という法益に着目し、業務妨害類型に属する違法行為(8)について若干の考察を試みる(9)。そ

(7) 物体である財産権の管理手段としてコンピュータシステム（電子計算機）が用いられている場合であっても、管理対象となる財産権が物体（財物）であって、純粋な電磁的記録または電子的な状態ではないときは、通常の横領罪（刑法252条1項）等の成否が論じられることになる。この場合、電磁的記録の不正作出行為等は電子的なものとなるが、それは手段的なものであるに過ぎず、電子計算機による管理の対象はあくまでも物体（財物）である。したがって、電子計算機を用いて財物の管理がなされていても、その財物が物体であり、不法領得の意思をもってその財物の占有（所持）を自らの支配下に置く行為は、奪取罪である横領罪を構成し得るものではあるけれども、電子計算機使用詐欺罪（同法246条の2）を構成するものではない。

この点について判示した裁判例として、最高裁平成21年3月26日決定・刑集63巻3号291頁がある。この決定の判例評釈として、松田俊哉「他人所有の建物を同人のために預かり保管していた者が、金銭的利益を得ようとして、同建物の電磁的記録である登記記録に不実の抵当権設定仮登記を了したことにつき、電磁的公正証書原本不実記録罪及び同供用罪とともに、横領罪が成立するとされた事例」法曹時報63巻1号253～275頁、同「時の判例　他人所有の建物を同人のために預かり保管していた者が、金銭的利益を得ようとして、同建物の電磁的記録である登記記録に不実の抵当権設定仮登記を了したことにつき、電磁的公正証書原本不実記録罪及び同供用罪とともに、横領罪が成立するとされた事例」ジュリスト1394号99～100頁、赤松亨太「新判例解説（第367回）他人所有の建物を同人のために預かり保管していた者が、金銭的利益を得ようとして、同建物の電磁的記録である登記記録に不実の抵当権設定仮登記を了したことにつき、電磁的証書原本不実記録罪及び同供用罪とともに、横領罪が成立するとされた事例」研修737号21～30頁がある。

(8) サイバー犯罪の領域において電子計算機を用いた各種業務運用システムに対する攻撃手段としてしばしば用いられ、適用法令としても業務妨害類型に属する罪（刑法233条、234条、234条の2）を考えることができるDoS攻撃（DDoS攻撃）に関しては、夏井高人「サイバー犯罪の研究（一）」法律論叢85巻1号197～232頁で論じた。また、直接的には被害者を偽サイトに誘導して機密情報を入手することを目的として実行されるものではあるけれども、そのような行為の実行により同時に業務妨害の結果を惹起し得ることが多いフィッシング攻撃については、同「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―」同誌85巻4・5号179～236頁で論じた。

(9) 客観的にはそのような事実関係が存在する場合であっても、現実の刑事訴訟実務においては、確実に有罪とすることのできる事実（訴因）に絞って公訴の提起が行われるため、有罪判決の事例は極めて稀であり、しかも、仮にそのような事案の裁判例が存在する場合であっても、判例集等によって公刊されないことが普通だと思われる。そのため、過

して、物体ではない電子的な対象について実行される横領的行為や背任的行為が刑法上ではどのように評価されるべきかについて、理論的な検討と裁判事例の検討を踏まえて論じた上で(10)、他の処罰法令が適用可能な事案類型を示唆し、その場合の罪数関係について論ずる(11)。

2　電子的な横領と背任

ここでは、自己の管理する電子計算機を用いて積極的に利得を得る利得横領行為について、理論面での検討を加えた上で、関連する裁判例について考察を行う。

積極的な利得ではなく、本来なされるべき課金を阻害して課金を免れる行為については、後述の「電子装置を用いた料金徴収業務の阻害」で検討する。また、積極的な利得行為や課金を阻害する行為ではなく、損害を発生させる目的による背信的行為については、後述の「加害目的での背任罪と電子計算機損壊等業務妨害罪の罪数」で検討する。

2．1　理論的な検討

2．1．1　電子的なトークンとその侵害行為

古来、通貨ではない様々な物体が経済価値交換のための汎用のシンボル（トークン）として用いられてきた(12)。トークンで交換される経済的価値の中には物品と

去の裁判例を判例データベース等で渉猟するだけの研究手法を採っている場合には、そもそも問題の本質的部分に想到することができない。このことは、ビッグデータによる解析の場合でも全く同じである。すなわち、ビッグデータによる情報解析という手法には、その効用に関する本質的な限界が存在する。

(10) 従来の学説を踏まえた検討結果としては、内田幸隆「電子マネーと犯罪」法とコンピュータ27号83～95頁、同「背任罪と横領罪との関係」早稲田法学会誌52巻49～65頁がある。

(11) 本論文は、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―」103頁の「まとめ」において「別稿において私見を明かにしたい」と述べたままこれまで論説というかたちでは明らかにしてこなかった私見を示すものでもある。

(12) 「トークン（token）」の本来的意味及び歴史上（考古学上）の用例については、佐伯胖『コンピュータと教育』（岩波新書、1986）90～92頁が参考になる。人類の経済取引活動の歴史におけるコインの利用に関しては、Keith Roberts, The Origins of Business, Money, and Markets, Columbia Business School Publishing, 2011, pp. 9–27が参考になる。

役務の両方が含まれ得る(13)。現代の社会においては、経済的価値の電子的な交換のために様々な電子的なトークンが用いられている。そのような電子的なトークンは、電子マネーと呼ばれることもある(14)。

電子的なトークンは、それのみで単独で機能する電磁的記録の形態をとる場合もあるし、また、単なる鍵としての機能しか有せず、それのみで単独で機能することはなく、何らかの認証システムを経て処理過程（プロセス）として電子的なトークンとしての機能を果たす場合もある。

電子的なトークンは、USBメモリやICチップのような物理媒体に記録されて存在していることがあるし、携帯電話やスマートフォン等の小型の装置・機器類の内部にある記憶装置に記録されて存在していることもある(15)。このような場合、当

(13) 現代社会においては、ゲームセンター、各種遊技施設、交通機関等で用いられる貨幣類似の「コイン」もトークンの一種とされ、トークンと呼ばれることがある。例えば、シドニー（オーストラリア）のモノレールを利用するためには、現金で「トークン」というコインのようなもの（代用貨幣）を購入しなければならない。東京の新宿御苑を利用し散策するためには、現金でカード類似のトークン（入場券）を購入しなければならない。このようなトークンは、ICカード等を用いた電子的処理によって実装されることもある。電子的なトークンは、それ自体としては物体ではない。しかし、それらいずれの場合においても、交通機関や施設等の利用料金に相当する現金を支払ったことを証明するための手段となっているという共通点を有している。また、プログラム言語の世界では、ソースコードを構成するための最小単位である記号や符号のことを「トークン」と呼ぶことがある。この場合における「トークン」は、「シンボル（象徴・符号）」と全く同義となる。

(14) 電子マネーに関する裁判例として、最高裁平成18年2月14日決定・刑集60巻2号165頁がある。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―」79頁で既に検討した。この決定の判例評釈として、藤井敏明「時の判例　窃取したクレジットカードの名義人氏名等を冒用してこれらをクレジットカード決済代行業者の使用する電子計算機に入力送信して電子マネーの利用権を取得した行為が電子計算機使用詐欺罪に当たるとされた事例」ジュリスト1334号232～234頁、鈴木左斗志「電子計算機使用詐欺罪（刑法246条の2）の成立要件をめぐって―最高裁平成18年2月14日決定（刑集60巻2号165頁）は何を判示したのか?」研修797号3～20頁、岡田好史「窃取したクレジットカードのカード番号などの情報の入力・送信により電子マネーを購入した行為と電子計算機使用詐欺罪」専修ロージャーナル3巻107～116頁、井上宏「判例研究 窃取したクレジットカードの情報をクレジットカード決済代行業者の使用する電子計算機に送信して電子マネーを購入した行為が、電子計算機使用詐欺罪に当たるとされた事例」研修698号25～38頁、鈴木左斗志「電子マネーの取得（電子計算機使用詐欺）」別冊ジュリスト190号『刑法判例百選Ⅱ各論（第6版）』116～117頁がある。

(15) いわゆる「お財布ケータイ」の類では、スマートフォンの中には鍵となる符号だけが記録されており、与信残高や預金残高の認証は、電気通信回線を介して接続されているクレジットカード会社や銀行等の金融機関のホストコンピュータ内で処理されることが一般的である。

該トークンは、独立した電磁的記録（データまたはファイル）として存在していることが比較的多い。そして、このような場合、物体（財物）としてのUSBメモリ等について、強盗罪（刑法236条）、恐喝罪（同法249条）、窃盗罪（同法235条）、詐欺罪（同法246条）、横領罪（同法252条）、業務上横領罪（同法253条）、遺失物横領罪（同法254条）等の財物奪取罪が成立し得ることは当然のことである。

問題は、記憶媒体である記憶装置を内蔵している装置等の占有移転はなく、当該記憶装置に記録された電磁的記録のみが無権限で他所に移転され、または、利用された場合である。このような場合、記録を保存するためのUSBメモリ等は物体として存在しているけれども、その物体としての占有（所持）に対する侵害行為はなく(16)、その電磁的記録の使用価値または交換価値のみが侵害されることがあり得ることになる。この後者の場合において、純粋な電磁的記録に対する侵害行為が成立し得る。そして、当該小型の装置が電子計算機の一種であると認識可能な場合であって(17)、かつ、何らかの指令や情報を当該装置に入力しなければ当該装置内の記憶装置に記録されている電磁的記録の内容を覚知し、その複製を入手できないようにされている場合（暗号化されている場合等を含む。）、その装置に対して「不正の指令」や「虚偽の情報」を入力し、その装置内に記録されている電磁的記録の内容を覚知し、その複製を入手する行為は、当該電磁的記録の複製物の入手によって直ちに何らかの経済的価値を獲得し、「利得」することが可能な態様・機能・性能を有するものである限り、電子計算機使用詐欺罪（刑法246条の2）に該当するこ

(16) 強いて言えば、当該装置に対する無権限の使用行為は存在していると言い得る。しかし、当該装置の本来の用法に従った使用ではない場合にはそもそも「使用」と言えるかどうか疑問がある。また、例えば、通勤電車内でスマートフォンやパッド型PCを使用すると周囲にいる他の乗客から画面表示内容を覗かれる危険性が極めて高いが、このような場合、画面表示内容を覗かれる可能性を予測可能なのにそのような状態をつくり出していることになるので、権利者の事実上の承諾がある場合に該当すると認めることができるのが普通ではないかと考えられる。満員電車内で携帯電話を用い大声で通話している場合も同じで、通話内容が周囲にいる他の乗客の耳に入ることを当然承知してそのような通話をしていると認めるべき場合が普通であると思われる。これらの場合においては、画面表示内容や通話内容等につき秘匿性が喪失しているということができる。

(17) USBメモリ等の小型記憶装置であっても、その機能や性能の観点からすると、電子計算機の一種だと言える場合がある。現代においては、昆虫サイズの自律型ロボットが既に実現しているので、USBメモリ型の自律型のロボットも実現可能な段階に至っている。自立型のロボットではなくても、非常に小さなサイズの電子装置が現実に無数に製造されている。そのような装置の中には電子計算機の一種と考える以外にないものが多数ある。

とがあり得ることになる(18)。

ところで、一般に、USBメモリのような小型の装置は、無線で他の装置からアクセスするか、または、それを挿入または接続したPCのキーボードを用いて当該装置を操作するのが普通である。この場合において、特に指令や符号を入力する必要がなく、通常の電子計算機に接続すれば直ちに、その装置に記録されている電磁的記録の内容を覚知し、その複製を入手することができる場合（電磁的記録が暗号化されていない場合等）、電子計算機使用詐欺罪（刑法246条の2）の構成要件行為である「不正な指令」や「虚偽の情報」の入力が全く存在しないので、電子計算機使用詐欺罪の成立はあり得ない。

また、電磁的記録の暗号化等がなされている場合を含め、小型の装置から発せられる微弱な電磁的放射（エミッション）を外部の電波傍受装置等を用いて探知し、それによって当該電磁的放射をしている装置や機器類に記録されている電磁的記録やそこで処理されている電磁的記録の内容を覚知し、その複製を入手する行為(19)は、いかなる意味においても電子計算機使用詐欺罪を構成しない。この場合においては、当該小型の装置を電子計算機と認めることのできるとしても、その装置に対する「不正の指令」または「虚偽の情報」の入力が何ら行われないからである(20)。

このように、微弱な電磁的放射の傍受という手段で電磁的記録の内容を覚知し、その複製を入手する行為について電子計算機使用詐欺罪が成立しない場合において、他の犯罪が成立し得るかどうかについて検討してみると、強いて言えば、もし当該電磁的記録が著作権法によって保護される著作物に該当するのであれば、著作権法違反の罪（無許諾の複製）が成立し得る程度ではないかと思われる(21)。この

(18) USBメモリ等の小型装置について、その性能・機能の別を問わず電子計算機としては一切認めないという見解に立脚する場合には、そもそも電子計算機使用詐欺罪が成立する余地が最初から全くないことになる。

(19) このような攻撃は、一般に、「テンペスト攻撃（transient electromagnetic pulse surveillance technology attack）」と呼ばれている。

(20) この場合、比喩的に言えば、本人は立派な服を着用していると思っているけれども他人から見れば素っ裸の状態にあるのと同然だと言える。裸体を自ら外部に晒しているので、無理に服を脱がせる必要がない、というよりも、何も着用していない。

(21) 逆から言えば、保護の必要のあるデータの中に創作性があり著作物と言えるようなオリジナルのデータを意図的に混入しておけば、万が一にもその無許諾複製行為が発生した場合には、当該オリジナルのデータも一緒に複製されることになるので、その点をとら

関連で、不正競争防止法違反の罪の成否についても付言しておくと、USB メモリ等の小型の記憶装置内に記録されている電磁的記録の内容が「営業秘密」（不正競争防止法２条６号）に該当する場合であっても、当該小型の装置から微弱な電磁的放射（エミッション）が存在している状態を放置しているときは、当該小型の装置内部に記録されている電磁的記録の内容である情報について、これが秘密として適正に保護されているとは認め難い(22)。すなわち、このような場合には、不正競争防止法違反の罪の成立を認めることができない(23)。

他方、独立して機能する電磁的記録としての電子的なトークンではなく、記憶装置内には単なる鍵のみが記録として存在しており、その鍵を用い電気通信回線を経た決済処理や認証処理がなされるというプロセス（電子的な処理過程）によって全体として経済的価値の交換を実現するための電子的なトークンの機能を果たしていることもある(24)。このような場合には、独立した電磁的記録としての電子的な

え、トラップ的に著作権法違反の罪（被疑事実）により告訴することによって刑事的事後対応という意味での防御をすることは可能だとも言い得る。

(22) 微弱な電磁的放射（エミッション）は、普通の PC やスマートフォン等の CPU、ディスプレイ装置、キーボード、ルータ、接続ケーブル等からも放出されることがある。このように、電子計算機という装置を構成するほぼ全ての部品や付属装置等から微弱な電磁的放射（エミッション）があり得る。そして、そのような微弱な電磁的放射（エミッション）を狙って、当該装置に直接にアクセスすることなく、その外部にある傍受装置を用いてデータを写し取り、そのデータを奪うことが可能となる。なお、LTE による通信が可能で、かつ、周囲にある通信可能ポートを自動検出してローカルな無線通信網を自動構築してしまうような設定になっている機器類では、むしろ積極的に電磁的放射（エミッション）を発生させていると評価することが可能な場合さえあり得る。

(23) テンペスト攻撃や同様の類型に属する各種攻撃手法が存在することは周知のとおりであるので、そのようなタイプの攻撃にも対応できるような適切な防御を尽くしていない場合、当該情報が秘密として適正に保護されているとは認めることができない。なお、営業秘密の保護に関しては、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 頁でも論じた。

(24) クラウドコンピューティングまたは仮想コンピューティングの技術を応用したシステムでは、基本的に、端末側には単なる鍵に相当する符号や識別符号のみが存在し、経済的な価値の交換に該当する電子的処理は全てクラウドコンピュータ（ホストコンピュータ）の側でなされるのが普通である。また、通信回線で相互に接続された非常に多数のコンピュータ装置の協調によって電子的処理が実行されると何らかの経済的な価値の交換に該当する電子的処理が実行されたことになるようなシステムの場合には、そのような処理を実行するための全体としてのプロセスが重要であり、個々のデータやファイルのみでは何らの機能も有しないことがある。そのようなシステム上の仕様が採用・実装されている場合においては、個々の電磁的記録の複製物は、それだけでは何も機能しないので、その複製行為を実行しても、それだけではその経済的価値を奪うことができないか、または、

トークンは存在せず、プロセスが電子的なトークンとして社会的に機能しているのである(25)。

そして、プロセスが電子的なトークンとしての機能を果している場合には、そのプロセスの処理に必要な鍵として機能する電磁的記録が存在するとしても、その鍵となる電磁的記録のみでは電子的なトークンとして機能しない(26)。

非常に難しい。なお、クラウドコンピューティングと関連する法律問題については、岡村久道編『クラウドコンピューティングの法律』（民事法研究会、2012）、Christopher Millard, Cloud Computing Law, Oxford University Press, 2013が参考になる。

(25) 仮想通貨の一種とされるBitcoinは、分散型・協調型の相互認証システムのような技術的仕様を有する経済価値交換システムの一種だとされているが、その技術の詳細についてはいまだに謎の部分が多い。仮想通貨ではなく普通の電子ファイルの分散共有の例は、ファイル共有システムWinnyなどにも見られるものである。そして、電子的なトークンについて、ファイル共有システムと類似するような分散処理機能を有するものを想定することは可能である。このような仕様を有するシステムの場合、電子的なトークンは独立した電磁的記録（データまたはファイル）として存在しているのではなく、当該システムを構成する複数の電子計算機による分散・協調的な処理結果として仮想的にその存在が表現されるだけである。そして、その実質は、何らかの電子的な処理（プロセス）を意味するのみであって、独立した電磁的記録を1台の電子計算機で処理する場合とは基本的に異なる仕組みとなっている。なお、Winnyと関連する刑事裁判事例については、園田寿『情報社会と刑法』（成文堂、2011）42～61頁、亀井源太郎「Winny事件最高裁決定と「中立的行為」論」法學研究87巻3号1～32頁、藤本孝之「ファイル共有ソフトの開発提供と著作権侵害罪の幇助犯の成否—Winny事件」知的財産法政策学研究26巻167～219頁が参考になる。仮想通貨を含め電子的な仮想財（virtual goods）に関しては、Mattias Berberich, Virtuelles Eigentum, Mohr Siebeck, 2010が参考になる。

(26) クレジットカードを用いて電子的かつ即時的な決済（与信と事後的な支払処理）がなされる場合、当該クレジットカードの中に与信残高等のデータが記録されているわけではなく、当該クレジットカードは鍵（識別子）としての機能しか有していない。オンライン処理の場合、クレジットカード発行会社は、クレジットカードによって示される符号に基づいてクレジットカード契約の利用者であるか否か及びその与信残高を確認し、認証処理をするが、そのような処理は端末側で実行されるのではなく、電気通信回線を経由して接続されているホストコンピュータの側でのみ実行される。また、電子的なプリペイドカードを用いた事前課金認証の場合には、電子的なプリペイドカード情報それ自体が一定の金額について前払いが完了している事実を証明する機能を有する場合があり得る。この場合には、紙の金券（バウチャー）と基本的には何も変わらないものだと理解することができる。しかし、電子的なプリペイドカード情報が単なる鍵としての機能しか有せず、オンラインで認証・決済処理がなされて初めてその前払いの事実の証明が実行される場合もある。このような相違が存在することに留意しなければならない。なお、クレジットカード、プリペイドカード、デビットカード（キャッシュカード）のような板状の支払手段の磁気ストライプ部分やICチップ内に記録され、カード読取装置によって認証処理を実行するため電磁的記録については、別途、支払用カード電磁的記録に関する罪（刑法163条の2～163条の5）の成否を検討しなければならない。支払用

このような場合において、電子的な鍵としての電磁的記録それ自体については、前述のUSBメモリ等の小型の装置内部にある記憶装置に記録された電磁的記録と同様に考えることができる。しかし、その鍵となっている電磁的記録を用いてなされる電子的なトークンとして機能するための計算処理は、それ自体としては、刑法上の電磁的記録（刑法7条の2）には該当せず、電子計算機による電磁的記録の「処理」に該当する。電子計算機による計算処理の対象である電磁的記録と電子計算機による計算処理それ自体とは明確に分けて認識・理解しなければならない(27)。そして、このような電子計算機を用いた動的な電子的処理それ自体に関しては、刑法に定める電磁的記録に関する罪が成立する余地はない(28)。

以上のように、①電子的なトークンが独立した電磁的記録として存在している場合と②電子的な処理というプロセスとして生じている場合のいずれにおいても、それが経済的価値を交換するための電子的なトークンとして社会的な機能を果たしているものであるときは、電子計算機に対する無権限による指令または情報の入力により当該電子的なトークンを用いた経済的価値の交換処理が実行され(29)、それによって直ちに利得が発生する限り、電子計算機使用詐欺罪（刑法246条の2）が成立する場合があり得る。

2．1．2　財産罪としての基本類型

ある加害行為が外形的に同一であるためにいかなる犯罪類型に属するかを外形

カード電磁的記録に関する罪に関しては、前掲「サイバー犯罪の研究（三）―通信傍受に関する比較法的検討」、夏井高人「支払用カード罪新設のための刑法一部改正とその問題点」判例タイムズ1061号59～64頁で述べた。

(27) 高度の分散協調による並列処理を基礎とするグリッドコンピューティング、データ駆動型のコンピュータシステム、生体脳におけるニューラルネットワークを模した人工知能型のアーキテクチャ等では、また別の考慮を要する。しかし、議論が煩瑣になることを避けるため、本論文においては、現代の企業活動等において普通に利用されている電子計算機の基本的な仕組みを前提として検討・考察を進めることにする。

(28) 電子的な処理が無権限で実行された場合、当該処理を実行するコンピュータシステムとの関係で電子計算機使用詐欺罪が成立し得ることは別問題である。これは、真正な電磁的記録を無権限で使用して財産上の利益を違法に得る場合に該当する。

(29) 電子計算機使用詐欺罪の成否に関しては、同罪の構成要件要素である「不正な指令」をどのように解するかによって結論が異なることになる。私見は、「不正な指令」の解釈につき、「適正な指令」を無権限で使用する行為（権限を超過して使用する場合を含む。）を意味すると解する。このことは「虚偽の情報」でも同じであり、情報それ自体が虚偽である場合には犯罪の目的を達することができない。この点については、更に後述する。

的行為だけでは識別不可能な場合であっても、社会的・規範的な意味において自己が管理していない他人の財産権（財物・利益）に対する侵害として認められるべきときは、犯罪学上の行為類型としては盗犯類型の犯罪に属することになる。

この場合において、対象物が物体としての財物であるときは、窃盗罪（刑法235条）、詐欺罪（同法246条1項）等の罪が成立する。これに対し、侵害の対象が財物ではない財産上の利益である場合には、詐欺利得罪（同法246条2項）、電子計算機使用詐欺罪（同法246条の2）、背任罪（同法247条）等の罪が成立し得る。

また、社会的・規範的な意味において自己が管理する他人の財産権（財物・利益）に対する侵害行為として認められるべき場合がある。この場合、犯罪学上の行為類型としては盗犯類型の犯罪に属するが、自己が支配・管理していない他人の財産権に対する侵害行為とは態様を異にする。そして、侵害行為の対象が物体としての財物である場合には、横領罪（同法252条1項）、業務上横領罪（同法253条）、遺失物横領罪（同法254条）が成立する。これに対し、侵害行為の対象が財物ではない財産上の利益である場合には、背任罪（同法247条）または電子計算機使用詐欺罪（同法246条の2）が成立し得る(30)。

ここで、侵害行為の対象が財物である場合には、横領罪（同法252条1項）と背任罪（同法247条）との罪数関係が問題となる。また、侵害行為の対象が財物ではない財産上の利益である場合には、背任罪（同法247条）と電子計算機使用詐欺罪（同法246条の2）との罪数関係が問題となる。そして、これらの全体としては、横領罪、背任罪及び電子計算機使用詐欺罪の間における罪数関係が問題となり得る。

(30) 窃盗罪（刑法235条）と電子計算機使用詐欺罪（同法246条の2）との関係について電子計算機使用詐欺罪が利益窃盗行為を処罰するという犯罪類型に属することは、既に前掲「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。横領罪と電子計算機使用詐欺との関係についても同じ関係が認められる。すなわち、犯罪学的にみて横領類型に属する行為として自己の管理する他人の利益の違法な入手が実行された場合、現行の横領罪では利益横領が認められていないので背任罪が成立し得るにとどまるように見えるが、もしそれが電子計算機による電子的な処理による場合には、電子計算機使用詐欺罪が成立し得る。その結果、そのような行為類型に関する限り、電子計算機使用詐欺罪は、利益横領罪としての本質をも兼有することとなり得る。

電子計算機を用いた利益窃盗と利益横領との識別点は、当該電子計算機の管理権の態様の相違による。当該電子計算機の管理権が他人に属する場合には利益窃盗としての電子計算機使用詐欺罪が成立するのに対し、当該電子計算機の管理権が自己に属する場合には利益横領としての電子計算機使用詐欺罪が成立し得ることとなる。この管理権の相違は、行為者の主観と離れた客観的な評価として認識することが可能である。

例えば、自己が管理・運用している電子計算機によって処理される他人の財産権（財産上の利益）に属する電磁的記録について、ある時点以降、不法領得の意思をもって管理していたという事案(31)を考えてみると、このような事案においては、不法領得の意思が発生した時点以降には、背任行為、利益横領行為(32)または電子計算機使用詐欺行為のいずれもが成立可能と思われる。

ところが、このような事案では、電子計算機の適法な利用と違法な利用との境界線を外形的・客観的な事実に直接に求めることはできない。その識別基準は、主観的な構成要件要素である不法領得の意思の有無によって識別されることになる(33)。

例えば、不法領得の意思が発生する時点よりも前の時点では自己が管理する他人の電磁的記録について適法な権限に基づき何らかの処理をしていた者が、外形的には全く同じ処理を継続しておりながら、不法領得の意思が発生した時点以降については、無権限で当該処理を実行していたことになる(34)。

---

(31) この例では、加害者に不法領得の意思が発生した前後において外形的な物的事実としては何の変化も存在せず、ただ不法領得の意思の有無のみが異なっている。

(32) 財産上の利益に対する横領行為は、現行刑法上では、横領罪（刑法252条1項）を構成しない。現行刑法上の横領罪は、財物に対する侵害行為のみを犯罪としてとらえ、財産上の利益に対する侵害行為を含まない。本論文では、犯罪の類型ではなく犯罪学的な意味における行為類型を示すものとして「利益横領行為」と表現することにする。そのような意味での利益横領行為が現行法上で犯罪として処罰可能かどうかについては、後に詳述するとおりである。なお、財産上の利益を現金と交換・換価して、財物としての現金を取得すれば、その時点で横領罪（同法252条1項）が成立し得ることは言うまでもない。本論文における主たる検討対象は、財産上の利益を取得した時点で何らかの犯罪が成立し得るか否かにある。

(33) この不法領得の意思は、主観的要素なので、その存在の証明に困難を生ずる場合があり得る。しかし、それは刑事訴訟上の証明の難易の問題であって、構成要件該当性充足の有無それ自体とは関係がない。実務上では、不法領得の意思が存在しなければ成立しないような後発的な事実（間接事実）の存在することを客観的な証拠によって証明することにより、遅くともその時点以前の時点においては不法領得の意思が発生していたという事実を証明することになるが、これは、あくまでも証明論の問題である。そのような事実の例としては、例えば、横領した金員を単に運搬しているというだけでは不法領得の意思に基づいて運搬しているのか、適法な業務の遂行として運搬しているのかを識別することが困難な場合がある。しかし、その運搬した金員を競馬場や歓楽街等で私的に浪費した事実を証明することができる場合には、明らかに、当該金員について不法領得の意思が存在したという事実を推認することができる。このように、証明の対象となる事実そのものと証明の難易の問題とは、明確に分けて論じなければならない。

(34) 当該処理が不法領得の目的で実行されることを許容するような権限が授与されることはあり得ない。

この場合において、電子計算機使用詐欺罪（同法246条の2）の構成要件要素である「不正な指令」または「虚偽の情報」の入力という実行行為に関して、権限の有無で識別すべきものとする立場（私見）では、外形的には全く同一の指令または情報の入力であっても、不法領得の意思が発生した後の時点では無権限による入力となるので、電子計算機使用詐欺罪が成立し得ることとなる(35)。この場合において、電子計算機使用詐欺罪の故意の内容としては、人間に対して実行される犯罪ではないので、「他人を欺罔すること」を全く含まない。不法領得の意思で利得を実現する目的でなされる入力行為についての認識・認容があれば、故意の内容を充足していることになる(36)。

このことは、同様に、背任罪との関係においても言うことができる(37)。

2．1．3　横領罪と背任罪

一般に、横領罪と背任罪との間の罪数関係について、犯罪行為の外形的行為（作為・不作為）は、それ自体としては同一なので、形式論理のみによるとすれば、観念的競合の場合に該当すると考えられないわけではない。しかし、通説・判例は、この場合に関して、横領罪のみが成立し背任罪は成立しないものと解している（法条競合説）(38)。電子計算機使用詐欺罪と背任罪との関係についても、通説・判例

(35) 本文中の説明においては、理解しやすいように、作為による場合のみを示した。しかし、理論的には不作為による場合があり得る。例えば、本人からの依頼により電磁的記録の移転・修正・削除等が求められているにも関わらずそれを実行しないことによって自己の利益（利得）を増加させることができ、その反面として本人の経済的利益が減少するような場合には、不作為による電子計算機使用詐欺の成立を認め得る。換言すると、利益横領行為タイプの電子計算機使用詐欺罪では、積極的に新たな指令や情報の入力がなされなくても、不作為により利益横領行為を実現することのできる場合があり得ることになる。

(36) 電子計算機を手段として用いて他人の判断形成に介入し錯誤を生じさせて欺罔する場合、当該電子計算機を手段として用いることの認識・認容に加え、そのような手段によって被害者である他人を欺罔することについての認識・認容も要するという点で異なっている。このような事例としては、被害者である他人を欺罔して詐欺サイトに誘導し、加害者（または、いわゆる「受け子」のような現金回収の依頼を受けた者）が現金として引き落としてこれを取得することのできる口座に現金の送金をさせるような事例を考えることができる。このような被害者である他人を欺罔して実行される行為は、そのための手段として電子計算機が用いられていても、電子計算機使用詐欺罪（刑法246条の2）ではなく普通の詐欺罪（同法246条）を構成する犯罪行為の一種である。

(37) 背任罪の成否と関連する裁判事例に関しては、前掲『判例経済刑法体系第3巻』115～201頁が参考になる。

(38) 前掲『大コンメンタール刑法（第2版）第13巻』219～223頁、前掲前田雅英編『条解刑法（第3版）』789～791頁など。

は、電子計算機使用詐欺罪のみが成立し背任罪は成立しないものと解している（法条競合説）(39)。

ただし、法条競合にあると解する場合でも、法条競合関係の態様中の特別法・一般法の関係、補充関係または択一関係のいずれの場合に該当すると解するべきかについては、学説上必ずしも一致しているわけではなく、論者の価値判断によって異なる(40)。この点について、補充関係説では、背任罪は、補充的な犯罪類型であり、他の犯罪が成立しない場合に成立し得るという関係にあると考えることになる(41)。これは、横領行為や詐欺行為と同様に「他人からの信頼を裏切る背信的行為」という社会的要素が必ず含まれており、最広義では背任的行為（breach of trust）の範疇にある犯罪類型(42)に属するという考え方を基礎とするものだと推

(39) 前掲『大コンメンタール刑法（第2版）第13巻』242頁、前掲前田雅英編『条解刑法（第3版）』781頁など。

(40) 前掲前田雅英編『条解刑法（第3版）』187頁は、法条競合関係の中でも択一関係にあると解している。ただし、「択一関係」との概念は、それ自体として実質的な意味内容をもつものではない。実質的には補充関係にあると解するのが妥当と思われる。その補充関係との理解を是とするか否かは、論者の価値判断による。

(41) 藤木英雄『経済取引と犯罪—詐欺、横領、背任を中心として—』（有斐閣、1965）77頁

(42) 一般に、日本国の刑法における「背任罪」は「breach of trust」と英訳されることが多い。しかし、米法における「breach of trust」の概念は、日本国の刑法における背任行為の概念よりもかなり広い。例えば、米国連邦法律集18款1033条（18 U. S. Code §1033）は、「保険業務に従事し、その者の行為が州際取引と関係する者よって実行される犯罪またはそのような者と関連する犯罪（Crimes by or affecting persons engaged in the business of insurance whose activities affect interstate commerce）」との標題の下に、同条(a)項において、「(1) Whoever is engaged in the business of insurance whose activities affect interstate commerce and knowingly, with the intent to deceive, makes any false material statement or report or willfully and materially overvalues any land, property or security - (A) in connection with any financial reports or documents presented to any insurance regulatory official or agency or an agent or examiner appointed by such official or agency to examine the affairs of such person, and (B) for the purpose of influencing the actions of such official or agency or such an appointed agent or examiner, shall be punished as provided in paragraph (2)（州際取引と関連する保険業務に従事する者が、故意に、欺瞞的な意図で、虚偽の説明若しくは文書作成をし、または、意図的かつ実質的に、土地、財産もしくは担保の価値を過大評価した場合において、(A)当該の者の資産を評価するために保険業監督官庁またそのような官庁が指定する官庁もしくは評価機関に対して提出される資産報告書もしくは資産文書との関連で、かつ、(B)そのような官庁または指定された官庁もしくは評価機関の活動に悪影響を及ぼす目的で実行されたときは、(2)項の規定に従って処罰される）」と規定している。他にも類似の連邦法及び州法が多数存在する。

定される(43)。

一般に、取引活動はそれに関与する者相互の信頼を基礎としていることから、単なる債務不履行の場合を含め、取引活動と関連する違法行為は基本的に全て背信的行為だということができる。日本国の民事法学では、刑法の背任罪との混同を避けるため「背信行為」もしくは「背信的行為」またはこれに類する語を用いることが多い(44)。

2．1．4　利益横領行為の理解

財産上の利益を奪う犯罪類型（利得罪類型の犯罪行為）については、更に別の角度からの考察を必要とする。すなわち、利益横領行為は、財物に対する行為ではなく財産上の利益に対する行為なので、横領罪（刑法252条1項）、業務上横領罪（同法253条）が成立しない。利益横領行為については、そもそも横領罪（同法252条1項）が成立しないので、成立しない犯罪行為については他の犯罪との間での罪数関係を問題とすべき余地がない。

ところが、多種多様な利益横領行為の中では、電子計算機使用詐欺罪の該当性が肯定されるべき場合があり得る。例えば、適法な業務の遂行として、他人の財産権を管理するために自己が管理する電子計算機上の処理を行っている者が、不法領得

(43) ドイツ刑法（StGB）266条は、背任罪（Untreue）について規定している。同条1項は、「Wer die ihm durch Gesetz, behördlichen Auftrag oder Rechtsgeschäft eingeräumte Befugnis, über fremdes Vermögen zu verfügen oder einen anderen zu verpflichten, mißbraucht oder die ihm kraft Gesetzes, behördlichen Auftrags, Rechtsgeschäfts oder eines Treueverhältnisses obliegende Pflicht, fremde Vermögensinteressen wahrzunehmen, verletzt und dadurch dem, dessen Vermögensinteressen er zu betreuen hat, Nachteil zufügt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.」と規定し、同条2条は「§ 243 Abs. 2 und die §§ 247, 248a und 263 Abs. 3 gelten entsprechend.」と規定している。なお、ドイツ刑法における背任罪に関しては、樋口亮介「ドイツ財産犯講義ノート」東京大学法科大学院ローレビュー8巻144～224頁（特に205～211頁）が参考になる。ドイツ法を日本国の刑法典に継受する前後の状況については、内田幸隆「背任罪の系譜、およびその本質」早稲田法学会誌52巻49～65頁」早稲田法学会誌51巻103～152頁が参考になる。

(44) 経済刑法という観点から背信的行為に対する処罰を考察するものとして、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、2008）がある。組織の内部者による背信的行為としてのサイバー犯罪に対する技術的対応に関しては、Dawn Cappelli, Andrew Moore, Randall Trzeciak, The CERT Guide to Insider Threats, Addison Wesley, 2012が参考になる。

の意思で、当該電子計算機を用いて利得する行為などがその例だと言える(45)。

そして、利益横領行為が電子計算機使用詐欺罪に該当すると同時に背任罪にも該当し得るような場合には、横領と背任の場合と同様、罪数関係が問題となる。電子計算機使用詐欺罪と背任罪との関係については、通説・判例に従い、電子計算機使用詐欺罪だけが成立し、背任罪が成立しないと解することになろう（法条競合説）(46)。

以上を前提にして考えてみると、経済的交換価値を有する電子トークンである電磁的記録またはその処理を横領する行為は、他人の財物に対する侵害行為（奪取罪）ではなく他人の財産的利益に対する侵害行為（利得罪）に該当するので、①電子計算機使用詐欺罪に該当し得る場合があること、そして、②電子計算機使用詐欺罪と背任罪の両者が成立可能であるような事案については、通説・判例に従い、電子計算機使用詐欺罪（刑法246条の2）のみが成立し、背任罪（同法247条）の成立は否定されること、以上のとおりの擬律となる。

財物に対する奪取罪としての側面だけに着目すると、窃盗罪（刑法235条）、詐欺罪（同法246条）、横領罪（同法252条1項）及び背任罪（同法247条）は、相互に異なる態様・類型に属する犯罪行為として分類可能である。しかし、汎用の計算装置である電子計算機を用いて利得する行為は、現実の行為態様としては全部同一の電子計算機を用いた電磁的記録の処理に統合されてしまう。その結果、人間に対する欺罔行為を必須の構成要件要素とする詐欺利得罪を除き、電子計算機に対して何らかの入力をすれば実行可能なものである限り、窃盗類型に属するはずの利益窃盗行為、横領類型に属するはずの利益横領行為及び背任類型に属するはずの背任利得行為は、電子計算機使用詐欺罪で対処することが可能となる。換言すると、これらの利得行為は、全て同一の類型に属するものとして理解することができる。これらの関係をまとめると、図1のようになる。

(45) この場合の故意については、前述のとおりである。
(46) 前掲西田典之『刑法各論（第6版）』255頁

	財物の奪取	電子的な利得
詐欺類型	刑法246条1項	刑法246条2項
窃盗類型	刑法235条	刑法246条の2
横領類型	刑法252条1項、253条	刑法246条の2
背任類型	なし	刑法246条の2

図1　犯罪としての位置づけ

念のために重ねて述べておくと、背任利得行為は、本来であれば背任罪（同法247条）として処罰可能な行為であるはずであるが、電子計算機による処理によって利得する行為に関する限り、外形的行為及び故意の内容としては電子計算機使用詐欺罪（同法246条の2）と一致する。そして、罪数論上、電子計算機詐欺罪と背任罪とが成立する場合には法条競合の関係にたち、電子計算機使用詐欺罪のみが成立する。その結果として、電子計算機を用いた利得に該当する部分は、背任罪の行為態様中から控除されてしまうことになる。

結局、利得罪として背任罪が成立し得るのは、電子計算機使用詐欺罪が成立しない場合に限定されることとなる。逆に、電子計算機使用詐欺罪が成立せず背任罪のみが成立するような事案を考えることは難しい。非常に特殊で例外的な事案を除き、原則として、背任罪の成否を論ずべき余地はないという結論になるであろう(47)。

以上の検討結果から理解できるとおり、電子計算機使用詐欺罪（刑法246条の2）は、経済的価値と交換する目的で利用される電子的なトークンの処理の場合を含め、不法領得の意思に基づき「不正な指令」または「虚偽の情報」を電子計算機に入力し、それによって当該電子計算機内に真実の事実関係を正確に反映しない内

(47) 最高裁昭和24年6月29日判決刑集3巻7号1135頁は、第三者のために領得する場合も横領罪における不法領得の意思に含まれると判示している。背任罪（刑法247条）は「自己若しくは第三者の利益を図り」と規定していることと形式的に対比すると第三者のために領得する場合には横領罪が成立しないかのようにも考えられ得るが、この最高裁判決の判断により、そのような形式的な識別はしないということで判例理論が確定しているということができる。従って、現実には、経済的交換価値を有する電磁的記録等についての利益横領タイプの違法行為について、背任罪だけが成立し電子計算機使用詐欺罪が成立しない事例を想定することが困難である。もっとも、私見とは異なるが、作為により不正の指令または虚偽の情報を入力した場合のみ電子計算機使用詐欺罪が成立し不作為の場合を含まないと解する立場をとると、不作為事犯の中に背任罪のみが成立し電子計算機使用詐欺罪は成立しないといった事例を机上の想定としては考えられないわけではない。

容の電磁的記録を作出することによって実行される行為である限り、犯罪学上の犯罪行為類型とは無関係に、電子計算機を無権限で操作して違法に財産上の利益を得る行為一般に適用可能なものである。

そのような観点からすると、この犯罪を詐欺罪の一種として規定する現行刑法の考え方は、基本的なところで再検討を要するということもできる。立法当時には電子計算機による処理が一般国民にそれほど普及しておらず、立法担当者が考察を深めるための前提事実の認識や予測に不十分なものがあったとしてもやむを得ない面がある。しかしながら、現時点においては、刑法理論（学説）や刑事裁判実務において、社会における経済取引の実態に即した理論構成や事実認定がなされるべきことは無論のこと、立法者においても刑法典の根本的な見直しを検討すべきであるということができる。

2．2　裁判例

2．2．1　電子計算機使用詐欺罪における「虚偽の情報」の意義

電子計算機使用詐欺罪と背任罪との理論的な関係が争点となり、第1審（東京地裁平成4年10月30日判決・判例時報1440号158頁(48)）の判断と控訴審（東京高裁平成5年6月29日判決・高等裁判所刑事判例集46巻2号189頁(49)）の判断との間で相違が生じた刑事裁判事例がある(50)。

(48) 判例評釈として、山中敬一「信用金庫支店長の指示によるオンラインシステム利用振込入金と電子計算機使用詐欺罪に成否」法学セミナー463号48頁、渡部惇「刑事判例研究（252）電子計算機使用詐欺罪の成立が否定され、特別背任罪の成立が肯定された事例」警察学論集46巻2号151～160頁、岩橋義明「信用金庫支店長によるオンラインシステムを利用した入金処理と電子計算機使用詐欺罪の成否」研修534号23～30頁がある。

(49) 判例評釈として、西田典之「電子計算機使用詐欺罪の成立が認められた事例」判例評論433号252～255頁、上嶌一高「電子計算機使用詐欺罪の成否—信用金庫支店長のオンラインシステム利用事件第二審判決」ジュリスト1036号105～107頁、林陽一「オンライン端末機操作による架空振込と電子計算機使用詐欺罪の成立」旬刊金融法務事情1428号76頁、荒川雅行「コンピュータ詐欺」別冊ジュリスト167号『刑法判例百選Ⅱ各論（第5版）』106～107頁、園田寿「コンピュータ詐欺(1)」別冊ジュリスト190号『刑法判例百選Ⅱ各論（第6版）』112～113頁、神例康博「コンピュータ詐欺(1)」別冊ジュリスト221号『刑法判例百選Ⅱ各論（第7版）』116～117頁、齊藤彰子「神田信金事件」別冊NBL 78『サイバー法判例解説』148～149頁がある。

(50) 銀行の従業員による電子計算機を用いた利得犯罪は、サイバー犯罪の中でも最も古典的な部類に属する。この点については、ドン・B・パーカー（羽田三郎訳）『コンピュータ犯罪』（秀潤社、1977）90～99頁、213～221頁が参考になる。

この事件の事案の概要は、神田信用金庫関町支店の支店長（被告人）が、勤務先の神田信用金庫とは関係がない副業等により負った個人的な債務の処理のため(51)、情を知らない部下職員を使用して自己名義の口座等に実体のない振込記録の入力をさせ、これによって、同信用金庫のオンラインシステムの記憶装置にその旨の入金があったことを示す不実の内容の電磁的記録を作出し、その記憶装置に記録された金額に相当する額の財産上の利益を得たというものである(52)。

第1審では、電子計算機使用詐欺罪（刑法246条の2）の訴因のみで公訴事実が構成されており、同罪のみの起訴となってきた。ところが、第1審裁判所から検察官に対する命令により、同法253条の業務上横領罪（第1次的予備的訴因）及び第1審公判当時の商法486条1項所定の特別背任罪（第2次的予備的訴因）の予備的訴因追加がなされた。そして、第1審裁判所は、この事件について、被告人を特別背任罪に該当するものとして事実認定し、懲役3年に処する旨の判決をした（第1審判決）。

この第1審判決に対して、控訴があった。

控訴審・東京高裁は、電子計算機使用詐欺罪の成立要件の解釈について詳細に判示した上で、原判決を破毀し、被告人の行為について、起訴当初の訴因である電子計算機使用詐欺罪が成立すると認定し、改めて懲役3年の刑とする旨を宣告した（控訴審判決）。

論点は多岐に及ぶけれども、その中で電子計算機使用詐欺罪における「虚偽の情報」の意義について、控訴審判決は、次のように判示している（当事者名等は一部仮名）。

しかしながら、刑法246条の2の「虚偽ノ情報」とは、電子計算機を使用す

(51) 控訴審判決は、「被告人は、昭和32年3月神田信用金庫に入り、平成2年5月同金庫関町支店長に就任した者であるが、昭和61年ころから生活が乱れ始め、本来の職務の傍ら、スナックの経営資金を知人に融通したり、知人と共同して株式投資や映画製作等に手を出し次々と失敗したりして、個人的な負債が雪だるま式に増加し、平成2年末ころにはそれが保証債務を含め約30億円にも達し、連日数千万円の返済資金を必要とするほどの窮状に陥り、やり繰りを続けていたが、ついに行き詰まって」本件各犯行に及んだと事実認定している。

(52) 電子計算機使用詐欺罪の既遂時期については、前掲「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―」で述べた。

る当該事務処理システムにおいて予定されている事務処理の目的に照らし、その内容が真実に反する情報をいうものであり、本件のような金融実務における入金、振込入金（送金）に即していえば、入金等に関する「虚偽ノ情報」とは、入金等の入力処理の原因となる経済的・資金的実体を伴わないか、あるいはそれに符合しない情報をいうものと解するのが相当である。右の不良貸付の事例の場合においては、電子計算機に入力された入金情報は、民事法上有効な貸付という経済的・資金的実体を伴い、これに符合しているので、虚偽の情報とはいえず、電子計算機使用詐欺罪は成立しないが（右のような実体を作出した行為につき背任罪の成否が問題になる。）、本件においては、前記2のとおり、被告人は自己の個人的債務の支払に窮し、その支払のため、勝手に、支店備付けの電信振込依頼書用紙等に受取人、金額等所要事項を記載しあるいは部下に命じて記載させ、支店係員をして振込入金等の電子計算機処理をさせたものであって、被告人が係員に指示して電子計算機に入力させた振込入金等に関する情報は、いずれも現実にこれに見合う現金の受入れ等がなく、全く経済的・資金的実体を伴わないものであることが明らかであるから、「虚偽ノ情報」に当たり電子計算機使用詐欺罪が成立する。

原判決は、①本件の入金等は、神田信用金庫の関町支店長である被告人が、同支店の業務として、部下職員に命じてなしたものであること、②支店長には入金、送金をしたり、自らのために資金手当を講ずる包括的な権限があること、③本件の各入金等は、支店長である被告人が業務として部下職員らに指示してなしたもので、神田信用金庫はその結果について民事上責任を負わざるをえないことなどを理由に、本件において被告人が入力させた入金等に関する情報は、虚偽、架空ではなく、経済的・資金的実体を伴うものであるとみるのが相当である（そのような経済的・資金的実体を作り出した点が背任罪を構成する。）、と解しているようにも見受けられる。

しかし、①については、被告人の本件各行為は、被告人が勤務先の神田信用金庫とは関係がない副業等により負った個人的な債務の処理のために勝手に部下職員を使用してなした不正行為であって、同金庫関町支店長としての業務上の行為というよりは、個人すなわち同金庫の一般顧客と同等の立場における行為に、自己の支店長としての地位を悪用したものとみるのが相当と思われ

る。②については、支店長はその支店の保有する資金の管理者であり、また、オンラインシステムの端末機やこれを操作する職員を管理・監督する者ではあっても、無制限な入金等の権限を有するわけではなく、現金等の受入れの事実がないのに、特定の口座に入金したり、振込入金したりする権限が全くないことは明らかである（右のような行為をする権限は、同金庫内の何人にも存しない。）。また、被告人の本件各行為は、実質的には同信用金庫の被告人等に対する合計7,400万円相当の信用供与ともみられるが、そのような手続は全くとられていないし、支店長に対する信用供与についていえば、そのような信用供与はその支店限りではなしえないものである。③については、本件各入金等につき、神田信用金庫が事後的に、F銀行築地支店に対して本件振込入金の無効を主張してその清算を求めたり（公訴事実第1の関係）、小切手の決済の無効を主張したりする（同第2の関係）ことができないのは、そのとおりであるが、それは、入金等が支店長により業務としてなされたためではなく、電子計算機のオンラインシステムによる為替取引等には多数の金融機関が関係し、多くの取引が相互に関連しつつ累積的になされるので、入力情報の事後的な無効処理を認めることは、取引の安全と迅速を損うことが甚だしく、その入力の取扱い金融機関の責めに帰すべき事由による事故はその金融機関の責任とし無効処理等は認められないように取り決められている結果にすぎないのである（当審証人Aの供述、信用金庫内国為替取扱規則第1編第2章13「責任の範囲」等参照）。したがって、結果として金融機関がその無効を主張することができないことになるからといって、本件のような不正の入金等に関する入力情報が虚偽ではないことになるわけではない。①ないし③の点はいずれも失当であり、その他原判決の説示や答弁にかんがみ検討しても、本件において被告人が電子計算機に入力した入金等に関する情報に経済的・資金的実体が伴っていると解すべき理由は見当たらない。

この控訴審判決に示された「虚偽の情報」に関する解釈論について、刑法学説上、特に異論はないように思われる。

私見によれば、第1審判決が述べているように、内容が虚偽の情報を入力しても電子計算機使用詐欺罪を遂行することができず、同罪を遂行するためには適正な内

容の情報を入力しなければならないことは当然のことであるが(53)、電子計算機使用詐欺罪所定の「虚偽の情報」を入力する行為とは、当該電子計算機によって処理可能な適正な内容の情報を権限なく入力することを示す趣旨の規定だと解すべきなので、結論において、私見は、控訴審判決の判断と同じになる。そして、この事案については、私見によっても電子計算機使用詐欺罪の既遂罪が成立すると解する。

なお、権限に基づいて適法に「虚偽の情報」を入力する場合の実例としては、電子計算機システムの安全性を評価したり、当該電子計算機の処理性能を評価したりする目的、その他広い意味での情報セキュリティ等の目的で、当該電子計算機の管理・運用にかかる適法な業務遂行の一部として、意図的にダミーデータを入力・記録して当該電子計算機に処理させるような例をあげることができる。このようなダミーデータの入力について、事業所の従業員にダミーデータの入力・処理に関する情報が提供され周知されていることもあるが、あえてその情報を秘匿し、情を知

(53) 前掲最高裁平成18年2月14日決定は、「被告人は、本件クレジットカードの名義人による電子マネーの購入の申込みがないにもかかわらず、本件電子計算機に同カードに係る番号等を入力送信して名義人本人が電子マネーの購入を申し込んだとする虚偽の情報を与え、名義人本人がこれを購入したとする財産権の得喪に係る不実の電磁的記録を作り、電子マネーの利用権を取得して財産上不法の利益を得たものというべきであるから、被告人につき、電子計算機使用詐欺罪の成立を認めた原判断は正当である」と判示しているけれども、ここで「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」との部分は、当該情報の物的属性に関する客観的評価を示すものではなく、当該情報を使用する行為に対する社会的評価としての「真実とは異なる」との意味に解するしかなく、それは、当該情報の入力を代行すること等の権限を本人から適法に授与されていない場合（無権限代行の場合）に該当すると解すべきなので、結局、電子計算機使用詐欺罪における「虚偽の情報」とは、無権限で「適正な情報」を入力する行為を意味すると解するほかはない（権限を超過して使用する場合を含む。）。すなわち、これら「不正な指令」や「虚偽の情報」に関して従来の裁判例にみられる解釈は、当該情報や符号の有する物理的属性に対する客観的な評価を示しているのではなく、当該情報や符号を使用する者の権限の有無に関する規範的・社会的な評価結果を意味していると理解するのが妥当である。

指令や情報は、それ自体としては、常に適正に処理することが可能なものなければならない。そうでなければ、当該電子計算機上において当該指令や情報を正常に処理させて犯罪行為を遂行することができない。このことについては、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—」104頁の注7でも指摘したとおりである。私見のような権限の有無を判断基準とする解釈論を実際に応用する例は、前掲「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—」の中で示した。なお、関連する論説として、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3～16頁がある。

らない従業員（部下）にダミーデータ（虚偽内容の情報）を入力させ、処理させることもある(54)。とりわけ、危機管理及びその擬似的対応を目的とする訓練や評価、システム監査等の場合には、このようなダミーデータ（虚偽内容の情報）の入力という手法が用いられることがある(55)。このような評価や監査に際しては、模擬攻撃（attack test）や負荷試験（stress test）と呼ばれるような操作が実行される場合もあるが、これらは、いずれも試験の対象となっているシステムの保有者・運用者から依頼を受けて実施されるもの、システムの保有者・運用者の承諾を受けて実施されるもの、または、法令に基づいて実施されるものであり、違法性阻却事由が存在するので適法行為となる(56)。

---

(54) このような適法行為としてダミーデータ（虚偽内容の情報）の入力がなされるような事例においては、構成要件該当性のレベルで「不法領得の意思」が存在しないとの理由で犯罪不成立となると考えることもできるし、また、違法性のレベルで、正当業務行為に該当し違法性阻却となるとの理由で犯罪不成立となると考えることもできるが、いずれの論拠によるとしても、電子計算機使用詐欺罪は不成立（無罪）となる。そのいずれの論拠によるべきかについて、その論理的な先後関係または優劣関係を決定付けることのできる確定的な（法解釈学上または法哲学上の）判断基準は存在しない。

(55) 日本国の「情報セキュリティ管理基準」は、JIS X 5080（ISO/IEC 17799）に基づいて策定されている。その実施の細目を定める「実施基準ガイドライン」では、「監査手続の実施（監査証拠の入手と評価）」として、「監査証拠は、関連書類の閲覧及び査閲、担当者へのヒアリング、現場への往査及び視察、システムテストへの立会、テストデータによる検証及び跡付け、脆弱性スキャン、システム侵入テストなどの方法を通じて入手される。しかし、情報セキュリティ監査人が入手した資料等がそのまま監査証拠となるわけではない。情報セキュリティ監査人は、当該資料等の入手源泉及び入手時の状況等を勘案して、監査証拠として採用するか否か、それが有する信用性及び証明力の程度を慎重に判断し、その結果等を明らかにしなければならない」と定めている。なお、この関連では、経済産業省「事業継続計画策定ガイドライン」（2005年8月）も参考になる。

(56) システムの保有者・運用者から事前の承諾を得ておらず、かつ、法令に基づくものでもないのに模擬データ等を送信して脆弱性要素を探索する行為については、とかく議論がある。このような脆弱性要素探索行為がインターネット全体の安全性を向上するために資するところが多いことは言うまでもない。しかし、当事者だけが知っており合理的な期間内に補修すれば足りる脆弱性要素を公表することに起因してサイバー犯罪実行の危険を増大させているとの批判もあり、とりわけ、脆弱性要素の存在が知られているけれどもその脆弱性要素を解消するための適切な手段が講じられていない状態にある「ゼロデイ脆弱性（zero-day vulnerability）」または「ゼロデイバグ（zero-day bug）」については、そのような批判がなされることがある。近時、米国連邦議会においては、ゼロデイ脆弱性に関する情報を公表することが国防上の観点からすると危険を招くことになるとの懸念から、脆弱性情報の自由な流通を禁止しようとする動きがある。なお、「脆弱性（vulnerability）」の意義について、情報セキュリティ企業Symantecは、同社のWebサイト上において、「脆弱性とは、コンピュータまたはネットワーク全体のセキュリティに

なお、控訴審判決は、第1審が認定した特別背任罪と電子計算機使用詐欺罪との関係については、特に判示することなく、「以上によると、本件各公訴事実については、いずれも主位的訴因である電子計算機使用詐欺罪の成立を認めるのが正当であるから、原判決はこれを認めなかった点において、法令の解釈・適用を誤ったものというべきであり、右誤りが判決に影響を及ぼすことは明らかである」としているのみである。

これは、「電子計算機使用詐欺罪が成立する場合には背任罪及び特別背任罪が成立する余地はない」との解釈を当然の前提とするものであり、この点に関する前述の通説・判例の見解を踏まえたものであると理解することができる。

2．2．2　電子計算機使用詐欺罪と背任罪との関係

電子計算機使用詐欺罪が成立する場合には背任罪が成立しないとの点について判示した裁判例としては、東京地裁八王子支部平成2年4月23日判決・判例時報1351号158頁がある(57)。

2．2．3　電子計算機使用詐欺罪と背任罪が混在する事例

電子計算機を用いた犯罪が継続して多数回にわたる場合、個々の行為については電子計算機使用詐欺罪に該当するものもあれば背任罪に該当するものもあるといった状況が発生することがあり得る。犯罪が発覚するまでの年月が長ければ長いほどその傾向が強い。このような事例に属する事案の裁判例として、東京地裁平成17年9月13日判決（公式判例集等未登載・東京地裁平成17年（刑わ）第1334号電子計算機使用詐欺、背任被告事件）がある。

この事件の概要は、スポーツクラブの運営等をしている勤務先会社の経理課職員をしていた被告人が、約1年2か月間に、多数回にわたって、銀行とオンラインで結ばれたファームバンキングシステムを悪用し、勤務先会社に設置されている同システムの端末装置を不正操作し、合計2億7000万円を超える巨額を被告人が開設した銀行預金口座に振込送金させたほか、被害会社の預金通帳、社判、代表者印を

弱点を作り出すコンピュータソフトウェアの欠陥や仕様上の問題点です。また、脆弱性は不適切なコンピュータやセキュリティの設定によって作られる可能性があります。脅威は脆弱性の弱点を利用して、コンピュータや個人データに潜在的な損害を与えます」と定義している（2015年9月23日確認）。

(57) 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―」72頁で既に検討した。

悪用し、不正に作出した預金払戻請求書や振込送金依頼書類を銀行の窓口係員に提出するなどして、合計3700万円余りを被告人が開設した銀行預金口座に振込送金させたというものである(58)。裁判所が認定した犯罪事実は、次のとおりである(当事者名等は一部仮名)。

被告人は、スポーツクラブの運営等を目的とする株式会社B経理財務本部経理課に勤務していたものであるが、

第1　同経理課に設置されたオンラインバンキングシステムの端末機を操作して同社が株式会社C銀行甲支店に開設した株式会社B名義の普通預金口座から自己が開設した銀行預金口座に虚偽の振込送金をして財産上不法の利益を得ようと企て、別紙1犯罪事実一覧表(1)記載のとおり、平成12年3月23日

(58) この判決は、被告人の犯行の動機等について「被告人は、風俗店（いわゆるソープランド）で遊興した際、接客に当たった女性従業員（いわゆるソープ嬢）を気に入ってしまい、以後、同女の求めに応じ多額の料金を風俗店に支払って同女を指名し店外デートをするようになり、被告人自身のそれまで蓄えが底を突くと、消費者金融から借入れをして風俗店への支払料金を調達していたが、それも借入限度額に達してしまい、本件各犯行により資金調達をするようになり、1日48万円もの多額の料金をほぼ連日上記風俗店に支払って、同女を指名してデートを重ねたほか、同女の要求により高級ブランド品を買い与えたり、同女とホストクラブに行くなどしていたものである。そして、被告人は、結局のところ、ホストクラブにおける遊興に耽っていた同女にだまされて会社のお金を同女に貢がされたものと思われ、その意味で哀れさを感じないわけではないが、同女のうそは通常の注意力をもってすれば容易に見抜けるものと考えられ、被告人の思慮不足は甚だしく、また、被告人は、犯行によって取得したお金は同女を救うためだけに使用し、自分のためには使用していない旨を供述するが、被告人は、要するに、自分が好きになった女性のために会社の金を不正取得したものであって、本件は身勝手で利欲的な犯行であると評価せざるを得ない。それから、その犯行態様は、経理課職員としての知識を悪用し、被害会社の会計監査体制の甘さを巧みにつき、振込先口座として正規の取引先と紛らわしい名称の口座を開設して行われ、犯行後は、提出すべき書類を隠匿したり、架空の会計処理をして発覚を防ぐなどしており、極めて巧妙な計画的犯行である上、1年2か月もの期間内に多数回にわたって繰り返された常習的な犯行である。それに、本件被害額は、合計3億1338万7070円もの巨額に達するところ、そのほとんどは上記風俗店への支払に費消したほか、同店従業員女性と行ったホストクラブで費消し、また、同女が被告人から受けた利益は、ホストクラブでの遊興によりほぼ使い果たされ、被告人から買い与えられた高級ブランド品も換価によってほとんど現存しない状況にあり、現実的な被害弁償は極めて困難であって、本件によって被害会社の受けた経済的損害は莫大である上、経理課職員である被告人が本件のような犯行を行ったことにより、被害会社の信用も傷付けられたものと考えられ、被害感情も当然厳しいものがあり、本件被害は重大であるというほかない」と判示している。

ころから平成13年5月28日ころまでの間、前後47回にわたり、東京都墨田区所在の株式会社B経理財務本部経理課において、同課に設置されたオンラインバンキングシステムの端末機を操作して、東京都多摩市内に設置された株式会社C銀行の預金残高管理・受入れ・払戻し等の事務処理に使用される電子計算機に対し、上記株式会社B名義の普通預金口座から被告人が開設した株式会社D銀行乙支店のE代表A名義の普通預金口座ほか3口座に振込があったとする虚偽の情報を与え、東京都千代田区所在のFに設置されている電子計算機等を介して、東京都多摩市内ほか3か所に設置された株式会社D銀行ほか3行の電子計算機に接続されている磁気ディスクに記録された前記E代表A名義の普通預金口座ほか3口座の預金残額を合計2億7635万9930円増加させて財産権の得喪、変更に係る不実の電磁的記録を作り、よって、合計2億7635万9930円相当の財産上不法の利益を得た。

第2　前記株式会社B名義の普通預金口座の預金を同社の正当な債務の支払に充てるための事務処理を行うなどの業務に従事していたところ、同社の従業員としては同社のため誠実にその職務を遂行すべき任務を有していたのに、自己の利益を図る目的で、その任務に背き、別紙2犯罪事実一覧表(2)記載のとおり、平成13年3月30日ころから同年5月25日ころまでの間、前後6回にわたり、東京都中央区株式会社C銀行甲支店ほか1か所において、情を知らない各支店窓口係員に、同口座から株式会社D銀行乙支店に開設した被告人管理に係るE代表A名義の普通預金口座ほか2口座に預金合計3702万7140円を振込入金させ、もって株式会社Bに同額の財産上の損害を与えた。

同裁判所は、以上のとおりの犯罪事実を認定した上で、①犯罪事実1については多数の犯罪行為中の一部について包括一罪とした上で電子計算機使用詐欺罪（刑法246条の2）の成立を認め、また、②犯罪事実2については多数の犯罪事実中の一部について包括一罪とした上で背任罪（同法247条）の成立を認め、被告人を懲役5年の刑とする旨を宣告した。

一般に、電子計算機使用詐欺罪が成立する場合には背任罪が成立しないことは既述のとおりであるが、この事案では多数回に及ぶ犯罪行為があり、それらの中で電子計算機使用詐欺罪に該当するものはそのように事実認定し、その残余を背任罪と

して扱ったものと考えられるから(59)、理論的には、通説・判例に基づくものだと評価することができる。

なお、判決に至るまでの間に多数の訴因について追起訴があったようであり、その間に、個々の訴因相互間において罪数論上の問題が生じたようであるが、この点について、同判決は、「平成17年5月19日付け追起訴状記載の公訴事実の一部は、

(59) 民法上の不当利得についても同様の考え方があり、また、国権についても行政権に関する控除説がある。すなわち、民事上の不当利得の法的性質に関しては、諸説あるけれども、他の請求権が成立しない場合に成立する補充的な請求権だとの見解がある。このような考え方は、要件事実論的には必ずしも正しくない。利得が正当な法的根拠を有するということを基礎づける事実に関しては被告が主張・立証すべきであるという見解に立脚すると、被告が請求の認諾をする場合だけではなく、請求原因事実の全てについて自白をした上で何らの抗弁も提出しないような場合には、いかなる事案についても不当利得返還請求が認容されるはずだからである。実体法上の論理関係だけではなく訴訟における動的な攻撃防御方法という観点から民法の条文を考察すると、このことはむしろ当然のことのように思われる。すると、不当利得返還請求権は、他の請求権との関係において補充的なものではなく、民事訴訟を理解する上での最も基本的なものであるとの認識に至ることができるであろう。なお、知的財産法の領域における損害論については、金子敏哉「特許権侵害による損害の2つの主な捉え方—売上減少による逸失利益と実施料相当額の関係」・『中山信弘先生古稀記念論文集　はばたき—21世紀の知的財産法』（弘文堂、2015）440～455頁所収が参考になる。

他方、国権についての控除説では、行政権は、国権の作用中から司法権及び立法権を控除した残余が全て行政権であることになる。このような考え方は、モンテスキューの時代に遡ることができる。すなわち、国権の作用を立法権と執行権の2種に分けた上で、執行権の中でも司法権を特殊なものとして控除し、その残余をもって行政権とする考え方である。そして、この控除説は、国権の作用をその機能に着目して分類し理解するという観点に限定すれば、現在でも完全に妥当する考え方だと言えるだろう。問題は、控除した残余であるはずの行政権が国権の大部分を占めているということに尽きる。立法権や司法権が発動される場面は、国権の作用の中でも極めて限定されたものであり、国の常務に属するものとは言い難い。現実には、国権の作用中の圧倒的な大部分が行政権に属していると言わざるを得ない。そのことをどのように考えるべきかについては、基本的には法解釈論ではなく政治学の領域に属することかもしれない。

しかし、単に既存の思考方法で説明することができるからそれで足りるとすることだけでは、サイバー空間に新たに生起する様々な課題についてどのような姿勢または視点をもつべきかという観点からは、いささか心もとないと言わざるを得ない。本論文を含め、これまで「サイバー犯罪の研究」として連載により考察結果を公表してきたところを踏まえると、刑事法についても同様のことを考える必要があるということを認識することができる。無論、現行法を前提とする通説・判例の立場では、横領罪や詐欺罪が成立する場合には背任罪が成立しないという関係にあるという理解が定着している。しかし、今後の立法論としては、もっと別の観点から信頼を裏切る罪という犯罪類型を想定することが可能だからである。

同年3月28日付け起訴状記載の公訴事実の一部と公訴事実を同一にするものであり、本来、訴因変更の手続がなされるべきであったことになるが、このような場合、訴因変更手続を経ることなく包括1罪の認定をすることが可能であり、また、追起訴につき二重起訴として公訴棄却判決をする必要もないものと解する（最高裁判所昭和31年12月26日判決（刑集10巻12号1746頁）、昭和35年11月15日決定（刑集14巻13号1677頁）等参照）」と判示している。

3　電子装置を用いた料金徴収業務の阻害

3．1　理論的な検討

一般に、有償の役務提供と無償の役務提供とがあり、有償の役務提供については当該役務を提供する事業者と利用者との間での契約締結が必要であって、かつ、適法な契約者であるか否かを識別するために電子的な装置・機器類が当該事業者から提供（貸与）され、これを使用しなければ有償の役務の提供を受けることができないように技術的な制限（保護）が加えられている場合、当該技術的な制限（保護）を無権限で解除または回避する行為は、全体としてみれば、当該有償役務提供者の適正な料金徴収業務に対する阻害行為（業務妨害行為）として認識することができる(60)。

(60) この種の行為は、著作権法によって保護される著作物であるコンテンツについて、暗号化等の技術的措置が講じられている場合において、そのような暗号化されたコンテンツに対して無権限で技術的措置を解除してアクセスする行為と同じ論理構造をもった事案類型だと言える。著作権法の領域では、知的財産権の一種である著作権の保護という観点のみから論じられることが多い。しかし、事業者等による当該コンテンツの提供行為は、広い意味での役務提供行為の一種として認識することが可能であり、このような見地からすると、著作物の管理情報や保護措置を回避する行為は、直接的には著作権法違反行為に該当するけれども、社会的には広い意味での役務提供に伴う課金の阻害行為すなわち業務妨害行為として観念することが可能である。逆から言えば、著作権の侵害の有無を論ずるときは、このような意味での適正な業務遂行の阻害という結果を伴わない場合には実質的な意味での法益侵害がない、または、可罰的違法性がないと解すべき場合があり得ることになる。

形式的には構成要件該当性が認められ得る全ての場合について処罰を是とすべきか否かについては、法解釈論というよりはむしろ非常に難しい政策判断が伴う。また、この

法的に保護されるべき業務が電子計算機によって処理されるものであり、かつ、実行行為が電子的な処理と関連するものである場合、通常の業務妨害罪（刑法233条、234条）ではなく、電子計算機損壊等業務妨害罪（同法234条の2第1項）が適用される(61)。未遂罪も処罰されることから（同法234条の2第2項）、電子計算機使用詐欺罪は、抽象的危険犯ではなく具体的危険犯として解釈しなければならない(62)。

ところで、電子計算機を使用して課金処理等が実行されている場合において、当該課金処理のための電子計算機に不正の指令または虚偽の情報を入力して積極的に利得するようなタイプの事案では、前述の電子計算機使用詐欺罪が成立することは当然のことである。

また、電子計算機を使用して課金処理等が実行されている場合において、当該課金処理のための電子計算機に不正の指令または虚偽の情報を入力して電子計算機による業務遂行が正常に実行されないようにした場合、それによって課金を免れる

種の議論の本質が解釈論というよりは政策論であり、経済的利害や社会的地位と関連する対立関係がそのまま政策論的立場における対立構造に反映されることになる。それゆえ、この種の問題における見解の対立が解消させることは極めて困難または不可能である。なお、著作権法違反行為の処罰に関しては、金子敏哉「著作権侵害と刑事罰―現状と課題」法とコンピュータ31号99～114頁が参考になる。

(61) 電子計算機損壊等業務妨害罪（刑法234条の2）と業務妨害罪（同法233条、234条）との罪数関係について、前掲『大コンメンタール刑法（第2版）第12巻』157～158頁は、原則として、電子計算機損壊等業務妨害罪（刑法234条の2）のみが成立する（吸収関係）と解している。ただし、電子計算機損壊等業務妨害罪の構成要件に該当し得る行為が実行された場合でも、加害者の故意としては当該電子計算機によって処理される業務ではない別の業務を妨害するものであり、当該電子計算機に対する加害行為はそのための手段的なものに過ぎず、結果として、当該電子計算機によって処理される業務には何らの支障も発生せず、当該電子計算機とは関係のない業務について妨害の結果が生じた場合などには、電子計算機損壊等業務妨害罪は成立せず、業務妨害罪（同法233条）または威力妨害罪（同法234条）と解すべき場合があると考えられる（逆の吸収関係）。近い将来、量子コンピュータが実用化し一般に普及すると、このような場合が増える可能性がある。

(62) この点については、前掲「サイバー犯罪の研究（一）―DoS攻撃（DDoS攻撃）に関する比較法的研究―」210頁で述べた。電子計算機損壊等業務妨害罪（刑法234条の2第1項）が抽象的危険犯であるとすれば、未遂罪（同法234条の2第2項）が成立する余地が全くないということになる。そして、業務妨害罪（同法233条）の罪質と電子計算機損壊等業務妨害罪の罪質とが同一であると解する場合には、電子計算機損壊等業務妨害罪を抽象的危険犯として解してはならない以上、業務妨害罪もまた抽象的危険犯として解釈してはならないという論理的帰結になる。もっとも、この両罪について罪質を異にする犯罪であると解する場合には別異に解することができないわけではない（私見は反対）。

行為については、場合を分けて考える必要がある。まず、役務提供契約その他の契約関係に基づき、当該役務の提供の対価について課金処理が実行されるような場合には、本来弁済すべき債務の弁済を免れるという意味での利得があることになるから、単純に電子計算機使用詐欺罪の適用を考えることになる。これに対し、何らの契約関係もない者が同様の行為を実行し、課金されずに役務提供を受けるような事例では、契約関係が存在しない以上、契約上の債務の弁済を免れるという意味での利得はない。このような場合には、不法行為（民法709条）に基づく損害賠償債務または不当利得（同法703条）が発生する。これら損害賠償債務や不当利得も債務の一種ではあるけれども、これらの債務は、当該電子計算機の処理を伴う業務遂行によって発生するものではなく、また、業務遂行に支障のあった電子計算機の処理が復旧しても当該損害賠償債務または不当利得は消滅せずに存続し、訴訟によって請求し得る状態に何ら変動をもたらさない(63)。このことを重視すると、観念的には、不法行為に基づく損害賠償債務の履行や不当利得の返還を免れることはできないという意味で、電子計算機使用詐欺罪における利得はないとの結論に達し得る。しかし、一般的は、民事上の債権・債務関係の本質論とはかなり矛盾する論理となり得るという解釈論上の問題はひとまず措いて、本来であれば契約を締結しなければ提供を受けることのできない役務の提供を無権限で受けた結果として通常の利用料金相当額の支払を免れていることが世俗的な意味において利得に該当するものと解するのが通例である(64)。

以上のことから、電子計算機に不正の指令または虚偽の情報を入力して役務利用の対価の支払を免れる行為は利得となり、結論として、この場合でも電子計算機使用詐欺罪が成立し得ることになる。

この場合において、債務の法的性質とは無関係に、適正な課金処理を実行することができなかったという事実だけで、業務妨害の結果を生じさせた場合に該当し得

(63) 巧妙な手口により加害行為の証跡を全て消し去ったというような事案では、実際問題として、加害者を特定し、その特定された加害者を被告として損害賠償請求等の訴訟を提起することが非常に困難または不可能となる。しかし、そのような場合であっても、客観的には、損害賠償請求権等は実体上の権利として存在しており、ただその行使・実現に厳しい障害が存在しているのに過ぎない。換言すると、不法行為に基づく損害賠償債務や不当利得の支払を事実上免れることにより利得することは民法解釈論上では不可能事に属する。

(64) 前掲『大コンメンタール刑法（第2版）第13巻』166～167頁参照。

ることは当然のことだと思われる。その結果、不正の指令または虚偽の情報を入力するという同一の行為によって電子計算機使用詐欺の結果と電子計算機損壊等業務妨害の結果の両者が発生した場合、その罪数関係が問題となり得る。

なお、利益横領類型や背任類型の事案と比較してみると、加害者が当該電子計算機で処理される電磁的記録等について何らかの支配や管理権等を有する場合（通常は、役務提供契約における役務提供者の側にある場合）には、利益横領類型や背任類型に属するものとしての電子計算機使用詐欺罪が成立することになる。これに対し、加害者が当該電子計算機で処理される電磁的記録について何らの支配も管理権も有しない場合（通常は、当該役務提供契約における役務利用者の側にある場合）には、窃盗類型に属するものとしての電子計算機使用詐欺罪が成立することになる。前者の場合には信頼を裏切る犯罪としての側面が顕著になるが、後者の場合には顕著であるとは言えない(65)。

3．2　裁判例

3．2．1　電子計算機使用詐欺罪

高速道路の通行料金は車種や重量等によって区分され、異なる課金がなされるように定められている。例えば、「普通貨物自動車」では、「単体で4車軸以上で車両制限令限度超」に該当する車両は「特大車」に区分され、「単体で4車軸で車両制限令限度以下」に該当する車両は「大型車」に区分され、「3車軸以下」に該当する車両は「中型車」に区分されるものとされている（2015年9月現在）。

この区分の該当性識別は、人間の担当者による目視によって実行されることもあるが、基本的には各種センサによって自動的に識別・区分される。とりわけ、ETCレーンから高速道路に進入する車両については100％自動識別による。そして、車軸の数の計測は、従来、路盤センサ(66)と呼ばれる装置を設置してある場所を車両

(65) 社会における一般的な倫理規範としての「悪いことをしない」との道徳命令に反する行為を実行したという意味で「社会に対する信頼を裏切った」という程度のことであろうと思われる。ただし、契約関係にある当事者の場合には、債務を履行すべき義務は法律上の義務となるので、その義務を履行するものと信頼する期待はより強く保護されるべきものである。その意味で、契約当事者間の信頼関係を裏切る行為という側面を有するものとなり得るが、契約の態様によりその度合いは異なる。

(66) 安本浩二・日浦禎・山村辰男「ETC車両検知器」富士時報75巻2号30～32頁

が通過する際に接地している車輪の数の計測から自動的に割り出されていた。そのことから、運転席から車軸の昇降を操作することができ、3車軸の状態でも4車軸の状態でも走行可能な貨物自動車については、路盤センサを通過する際には車軸を上昇させてその場所を走行・通過させることにより、実際よりも少ない車軸数の車両であるかのように路盤センサに感知させ、実際とは異なる車軸数を自動計測させる方法により、本来の通行料金区分よりも安い料金区分で自動決済処理をさせることが可能な状態になっていた(67)。

このような車軸数自動計測センサの特性に着目し、車軸数を実際よりも少なく計測させて安い通行料金区分に該当する車両として課金させた事案の判決として、横浜地裁平成27年6月9日判決・裁判所サイト(68)がある。同判決は、犯罪事実を次のように認定している。

> 被告人は、一般貨物自動車運送事業等を営むA株式会社に運転手として勤務していた者であるが、B株式会社等が管理運営する高速道路料金所と通行車両の車載器との間の無線通信等による自動的な通行料金の算出・徴収等の事務処理に使用される電子計算機等で構成されるETCシステムを利用するに際し、同システムにおいて、高速道路流入時の接地車軸数によって料金車種区分が認識され、流出時に当該区分及び通行区間によって料金が決定されることを利用して、けん引車と被けん引車の接地車軸数の合計が4車軸であり料金車種区分上の特大車（以下「特大車」という。）である連結車両で高速道路を通行

(67) 遅くとも高速道路入口に設置されているETCのゲートを通過した時点で、車両運転者と高速道路管理者との間に当該高速道路の利用契約が締結されたと考えることができるから、抽象的には、当該車両運転者について利用料金支払債務が発生していると解することができる。ただ、高速道路利用契約に基づく課金が従量制になっており、入口ゲートを通過した直後の時点では料金計算をして確定金額を課金することができないため、高速道路を通行した後に出口のETCゲートを通過した際に走行距離等を自動計算し、課金すべき利用料金を確定させる仕組みとなっているのに過ぎない。したがって、高速道路を利用する車両運転車は、その高速道路利用に伴う料金債務については契約上の債務者の立場にあることになる。それゆえ、当該運転者は、高速道路の管理者との間では、何の関係もない第三者ではなく、契約当事者として信義誠実の原則（民法1条2項）に基づき債務を履行すべき責務を負っているということはでき、その意味で、課金を阻止する行為は背信的な行為であるということができる。

(68) http://www. courts. go. jp/app/files/hanrei_jp/203/085203_hanrei. pdf［2015年9月22日確認］

するに当たり、これらの車軸のうち1車軸を一時的に上昇させることにより、同システムに、同車両の接地車軸数の合計が3車軸であり料金車種区分上の大型車（以下「大型車」という。）である旨の虚偽の情報を与えて高速道路の通行料金の一部の支払を免れようと企て、別紙一覧表（省略）のとおり、平成22年5月19日及び平成23年11月21日の前後2回にわたり、同表流入日時欄記載の各日時頃、神奈川県内所在のB株式会社高速自動車国道C自動車道（以下「D高速道路」という。）E料金所において、同料金所直前まで接地車軸数が4車軸の状態で走行してきた同表車両欄記載の各連結車両の車軸自動昇降装置をそれぞれ操作して一時的に同車両の後前軸を上昇させた3車軸の状態で同料金所ETCレーンに進入し、同状態で同レーンに設置された車軸数計測器の上を通過して、真実は、同表記載の各車両がいずれも特大車であるのに、これらがいずれも大型車であると計測させ、同計測器に接続されたETCシステムの利用による通行料金の算出等の事務処理に使用される電子計算機にその旨虚偽の情報を与えるとともに、当該計測結果を同電子計算機から送信させて同車両に搭載された車載器に挿入されたETCカードにその旨の情報をそれぞれ保有させた上、同料金所ETCレーン通過後、各車両の後前軸が自動的に降下した状態で高速道路を通行し、同表流出日時欄記載の各日時頃、同表流出料金所欄記載の神奈川県内所在のD高速道路F料金所ほか1か所において、同車載器から各流出料金所設置の前同様の各電子計算機に、真実は、同表記載の各車両がいずれも特大車として高速道路を通行したのに、これらがいずれも大型車であるとの虚偽の情報をそれぞれ送信し、同表精算日欄記載の各日頃、神奈川県内所在の株式会社GH電算室内に設置されたETCシステムの利用による通行料金の徴収等の事務処理に使用される電子計算機に前記虚偽の情報を与えて同車両の通行料金が同表支払料金欄記載の各金額である旨の財産権の得喪、変更に係る不実の電磁的記録を作り、よって、前記A株式会社に同表特大車料金欄記載の各金額との差額の合計額である1085円相当の財産上の不法の利益を得させたものである。

同裁判所は、認定した犯罪事実を踏まえ、情状を考慮した上で、被告人の行為が電子計算機使用詐欺罪に該当すると判断して、被告人を懲役1年6月（執行猶予3

年）の刑とする旨を宣告した。

この判決では、車軸を上昇させた状態で路盤センサを通過し、自動的に少ない車軸数を計測させた行為をもって「虚偽の情報」を入力したものと判断している。これを一般化すると、予め用意した「虚偽の情報」を積極的に入力する場合だけではなく、センサの脆弱性をついて、現実の状態とは異なるように計測させ、その計測結果を電子計算機に自動送信させるような場合も「虚偽の情報」を入力したことになるとの判断を示したことになる。

現代社会においては、様々なセンサが街中に設置されている。その中には、身体の一部を直接に接触させなくても自動的に認識処理をするものが多々あり、電波（人間の脳波、身体の脈動により発生する微弱な電波を含む。）、画像、音声、振動、大気中の化学成分等のセンサでは、基本的に多少離れた場所からでも正確な計測が可能となってきている。

そのようなセンサが、例えば、銀行のATM等に設置されており、正当な預金者であるか否かを自動判別するような場合には、この判決が判示しているように「虚偽の情報」の入力の範囲を拡大しても、それ自体としてはさしたる弊害はなく、むしろ、権限のない者の「なりすまし」による電子計算機使用詐欺行為を適切に処罰するために有用な考え方となるかもしれない。

しかしながら、「虚偽の情報」に関するこのような解釈をそのままのかたちで全く無限定に電子計算機損壊等業務妨害罪（刑法246条の2）の解釈に適用した場合、極論すると、かなり深刻な社会問題が発生する可能性がある。例えば、ファッションのためにカラーコンタクトを使用して街に出たり、男性が女装して歩行したりする行為が、市街における混雑状況を監視する交通管制システムや店舗内での顧客誘導システム等に用いられる電子計算機に「虚偽の情報」を入力したとして評価され、少なくとも机上の論理としては、当該業務の正常な運用を妨げるものとして電子計算機損壊等業務妨害罪の構成要件該当性が肯定されてしまう危険性がある。

このような「虚偽の情報」に関する理論上の危険性を回避するためには、そもそも構成要件該当性のレベルで詳密な検討を要することは言うまでもないが、例えば、①社会的に許容された行為として違法性阻却を考える、あるいは、②個人の基本的人権の一種である自由権の行使の範囲内にある行動については常に権限による

行為（正当行為）として違法性阻却を考えるほうが妥当ではないかと考える(69)。

なお、ETCの事例と類似する論点を含むものとして電子改札の脆弱性を悪用したいわゆるキセル乗車の事例がある。そのような類型に属する事件の裁判例として、東京地方裁判所平成24年6月25日判決・判例タイムズ1384号363頁がある(70)。

3．2．2　電磁的記録不正作出・同供用罪

衛星放送の利用者が有料番組を視聴するために必要となるB-CASカードの電磁的記録を無権限で書き換え、有料番組を視聴する契約をしていない者でも有料番組を受信・視聴できるようにしたという事案に関する裁判例として、京都地裁の有罪判決に対する控訴審の判決である大阪高裁平成26年5月22日判決・裁判所サイト(71)がある。第1審である京都地裁判決の判決文は公開されていないが、控訴審・大阪高裁の判決の中に事件の概要が要約されて判示されていることから、第1審・京都地裁で認定された事実を知ることができる(72)。

---

(69) 後者の考え方は、「不正な指令」または「虚偽の情報」の入力について、権限の有無によって識別すべきであるとする私見では必然的なものとなる。

(70) 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―」77頁で既に検討した。この判決の判例評釈として、青木陽介「自動改札機を利用したキセル乗車の場合の電子計算機使用詐欺罪の成否」上智法學論集58巻3・4号53～77頁、武藤雅光「最新・判例解説（第15回）連続しない乗車券等を使用して自動改札機から駅内に入出場する方法による、いわゆるキセル乗車の事案について、電子計算機使用詐欺罪の成立を認めた事例」捜査研究62巻6号13～23頁がある。

(71) http://www. courts. go. jp/app/files/hanrei_jp/527/084527_hanrei. pdf [2015年9月22日確認]

(72) 当時の報道資料等によれば、この事件は、当初、不正競争防止法違反の罪の容疑で捜査が開始されたもののようである。なお、控訴審における弁護人の「著作権法120条の2も、本件犯行後に改正された不正競争防止法2条10号、11号も、ユーザーが技術的制限手段の回避装置ないしプログラムを使用すること自体は、刑事罰の対象とされていないところ、このような他の法律の趣旨からみて、刑法においてユーザーによる技術的制限手段の回避行為まで処罰することは、罪刑法定主義に違反する」との主張について、控訴審判決は、「しかし、著作権法は著作権等の保護、不正競争防止法は事業者間の公正な競争をそれぞれ主たる保護法益とするのに対し、刑法161条の2は電磁的記録の果たす社会的に重要な機能に鑑みて電磁的記録に対する公共的信用を保護法益とするものであるなど、これらの法律は、犯罪構成要件の定め方のみならず、その立法趣旨や保護法益をも異にするものであるから、被告人の行為を一種の視聴制限回避行為や技術的制限手段回避行為として捉えるとしても、著作権法及び不正競争防止法がこれらの行為を刑事処罰の対象とはしていないからといって、これらと犯罪構成要件、立法趣旨や保護法益を異にする本罪の成立範囲が限定される、あるいはB-CASカードの改変とその使用につい

控訴審判決によれば、B-CASカードとは次のようなものであると認定されている。

(1) B-CASカードは、B-CAS社等が開発したICカードであって、これにより、「暗号化した番組の映像・音声等の信号を用い、限定された者が受信機で暗号を復号し、映像・音声等を受信して視聴すること」が可能となる。
(2) B-CASカードのメモリ部分には、衛星放送事業者（有料衛星放送の事業者及び一般社団法人デジタル放送推進協会（以下「Dpa」という。）の双方を含む。以下同旨）が放送する衛星放送の視聴可能期間等の情報が記録されており、衛星放送の映像・音声等の信号は、スクランブルがかけられて暗号化されている。
(3) B-CASカードの所有権はB-CAS社に帰属し、B-CASカードの利用者は同社との貸与契約に基づきB-CASカードを利用するにすぎず、利用者がB-CASカードを改変等することは禁じられている。
(4) 上記システムを前提として、衛星放送事業者らは、各々が使用を許諾されたB-CASカードの領域を書き換える権限を有しており、その権限に基づいて、各事業者と契約した相手方のB-CASカードに電波を送り、視聴可能期間等のデータを書き換えることで、同事業者に係る衛星放送を視聴可能な状態にさせるほか、その後の契約関係の変動に対応した書換えを行い、同衛星放送を視聴できない状態にさせるなどしている。

て本罪を適用することが罪刑法定主義に反するとは解されない」と判示している。なお、B-CASカードのデータ改ざん事案が不正競争防止法違反の罪に該当し得るという点を論じたものとして、菅野直「実例捜査セミナー Since 1988 改ざんB-CASカードの譲渡による不正競争防止法違反事件について」捜査研究63巻5号24～32頁がある。この論説の31～32頁によると、4名の被疑者中の1名について略式請求がなされ、他の3名については不正競争防止法違反の罪により「被告人3名は、不正の利益を得る目的で、法定の除外事由がないのに、共謀の上、株式会社ビーエス・コンディショナルアクセスシステムズが契約者以外の者に有料衛星放送を視聴させないために営業上用いている技術的制限手段の効果を妨げることにより同放送の視聴を可能とする機能を有する装置である改ざんされたB-CASカードを、東京都内の甲方ほか4か所に宛てて発送し、前記甲方ほか4か所において、甲ほか4名に前記B-CASカードを受領させて譲渡し、もって不正競争を行ったものである」との公訴事実により公判請求がなされた結果、全ての被告人について有罪判決で確定したとのことである。

(5) 有料衛星放送の事業者においては、B-CASカードにより衛星放送の視聴の可否を管理し、自社の衛星放送が視聴可能な状態に設定した相手方から視聴料を徴収して収益を上げている。
(6) Dpaにおいては、B-CASカードにより地デジ難視対策衛星放送の視聴の可否を管理し、同放送の視聴者数を必要最小限に止めるという指針を実現し、その状況を総務省に報告するなどしている。

以上のように判示した上で、控訴審である大阪高裁は、私電磁的記録不正作出罪（刑法161条の2第1項）及び同供用罪（同条の2第3項）の成立を認め、更に詳細な理由を述べて、次のように判示している（当事者名等は一部仮名）(73)。

B-CASカードに記録された電磁的記録は、刑法161条の2第1項、3項所定の人の事務処理の用に供する権利、義務に関する電磁的記録に該当し、被告人がこれを改変する行為は、同条1項所定の、人の事務処理を誤らせる目的で人の事務処理の用に供する権利、義務に関する電磁的記録を不正に作ったこと（不正作出）に該当するほか、被告人が改変した上記電磁的記録を記録したB-CASカードをテレビに接続された衛星放送受信可能なチューナー内蔵レコーダーに挿入する行為は、同条3項所定の、人の事務処理を誤らせる目的で不正に作られた権利、義務に関する電磁的記録を人の事務処理の用に供したこと（供用）に該当すると認められる。

すなわち、関係証拠によると、B-CASカードは、日本国内において、地上デジタル放送やBSデジタル放送及びCSデジタル放送を受信するためにテレビ等のデジタル放送受信機に挿入して使用するICカードであり、株式会社甲及び乙株式会社が共同で開発しそれぞれ製造して、B-CAS社に使用許諾を与え

(73) 本件の加害者（被告人）は、衛星放送番組配信会社等との間で何らの契約関係もないので、契約上の義務または責務としての信頼関係を考えることができない。その限りにおいては、強いて言えば、一般的な倫理義務としての「悪をなさない」との義務を負っているということが言える程度である。ただ、正規に契約を締結していないとしても、事実上、有償の番組の配信を受け視聴している以上、正規に契約を締結して利用料金を支払うべき倫理上の義務があると考えることは不可能ではなく、その限度で背信的な行為だと評価することは全く不可能なことではない。しかし、このように考えるべきかどうかについては、論者の世界観による。

ることにより、CAS 方式と称する限定受信方式を用いた CAS 放送の受信機において一般視聴者により使用されていること、B-CAS 社から CAS 放送実施の許諾を受けた衛星放送事業者は、衛星放送を通じて顧客等宛てに契約情報を送信して、各顧客等の使用する B-CAS カードにあらかじめ書き込まれている事業者ごとの視聴契約情報を書き換えることによって、同カードを所持しその使用権限を有する当該顧客等が当該事業者の衛星放送を受信することを可能にするものであること、そして、被告人が原判示の各 B-CAS カードに記録された電磁的記録を原判示のとおり書き換えたことにより、当該 B-CAS カードが地デジ専用か地デジ・BSCS 汎用かに関わりなく、それまでは受信不能であった WOWOW、スカパー及びスターチャンネルという各有料衛星放送並びに地デジ難視対策衛星放送について、全て 2038 年 4 月 22 日まで受信が可能となり、また、被告人が上記書換え後の上記の各 B-CAS カードをテレビに接続された衛星放送受信可能な各チューナー内蔵レコーダーに挿入したことによって、上記有料衛星放送の各事業者及び Dpa との間に視聴契約を締結することなく、上記各衛星放送を受信して視聴することが可能となったことが認められる。

そうすると、B-CAS カードに記録された電磁的記録は、衛星放送事業者から送信される事業者ごとの視聴契約情報に基づき、当該カードを所持しその使用権限を有する一般視聴者の衛星放送受信権限について、衛星放送ごとに受信権限の有無及びその期限を記録することによって、受信権限のある者による受信を可能にし、受信権限のない者による受信は不能にするものであるから、視聴契約に基づく受信権限の有無により個別の受信機による当該衛星放送受信の可否、ひいてはその視聴の可否を管理するという、衛星放送事業者の財産上又は社会的責務上の事務処理の用に供する電磁的記録であるとともに、衛星放送事業者との視聴契約に基づく受信権限に関する電磁的記録であるともいうことができる。

そして、被告人が本件各 B-CAS カードに記録された電磁的記録を改変した行為は、被告人が、受信権限のない衛星放送を受信して視聴するため、上記電磁的記録を、あたかも被告人に当該受信権限があるかのように当該衛星放送事業者の許諾を得ることなく書き換えるものであるから、同事業者の上記事務処理を誤らせる目的で、同事業者の上記事務処理の用に供している、同事業者と

の視聴契約に基づく受信権限に関する電磁的記録の不正作出に当たるということができる。

さらに、被告人が、改変した上記電磁的記録を記録した各B-CASカードを、テレビに接続された衛星放送受信可能なチューナー内蔵レコーダーに挿入した行為は、被告人が衛星放送事業者との視聴契約に基づく受信権限のない衛星放送を受信して視聴するため、あたかも被告人に当該受信権限があるかのように当該衛星放送事業者の許諾を得ることなく、書き換えられた同事業者との視聴契約に基づく受信権限に関する電磁的記録を、同事業者の上記事務処理の用に供したこと（供用）に当たるといえるのである。

以上のように判断を示した。

一般に、B-CASカード内の記憶装置に記録される課金のための基本データが私電磁的記録に該当するとの点については、人間にとって意味のある契約書等の文書に相当する電磁的記録のみを刑法161条の2第1項所定の電磁的記録と理解するか、電子計算機による課金処理のために用いられる符号であれば、当該符号がそれ自体としては人間にとって何の意味をも有するものではない場合や単なる識別符号に過ぎない場合であっても、全て同項所定の電磁的記録に該当すると解するかによって結論を異にすると考えられる。

この点について考える際には、前述のとおり、電子的なトークンには2つの態様が存在しており、現在のクラウド環境等においては、当該符号がそれ自体としてトークンになっているわけではなく単なる鍵に過ぎず、それが認証システムによって処理される場合の処理過程全体（プロセス）が社会的にはトークンとして機能する場合があるということを想起すべきである。立法者は、無論、プロセス全体を電子的なトークンとしてとらえるような考え方をもっていなかった(74)。

(74) 立法当時においては、そもそも技術開発がかなり未熟な段階にあったため、立法担当者として独立した電磁的記録ではなくプロセスが前提として電子的トークンの機能を実現するような場合について具体的な認識をもつことが難しかったと想像される。当時の立法担当者が執筆者となっている解説書等の中には、独立した電磁的記録それ自体ではなくプロセス全体をとらえて刑法161条の2の該当性を判断するという発想が窺えない（米澤慶治編『刑法一部改正法の解説』（立花書房、1988）79～82頁、的場純男・河村博『Q&Aコンピュータ犯罪』（三協法規、1988）64～96頁、米沢慶治「刑法等の一部改正法の論点（刑事法ノート123）」判例タイムズ640号56～64頁参照。なお、当時の日弁連の見

このような前提で、B-CASカード内に記録されている電磁的記録について検討してみると、要するに、この課金認証システムでは、B-CASカード内に記録されている電磁的記録である「利用者の識別子」及び「視聴可能期間」を示すデータを参照し、電磁的記録の処理結果として、当該B-CASカードを用いて衛星放送を受信している者が適法に利用契約を締結した者として識別可能であり、かつ、契約によって定められる視聴可能期間内にあるものとして計算処理されるものであれば、自動的に視聴可能として判別・処理されるというものなので、認証プロセスとしては何らかの電気通信回線(75)を経てネットワーク経由でなされているものと推定

解については、日本弁護士連合会刑法改正対策委員会編『コンピュータ犯罪と現代刑法』（三省堂、1990）103～119頁、西田典之「コンピュータの不正操作と財産犯」ジュリスト885号16～20頁が参考になる。）。したがって、厳格な意味での立法者意思説に立脚すると、同法161条の2は、個別の電磁的記録がそれ自体として「権利、義務に関する電磁的記録」または「事実証明に関する電磁的記録」となっている場合だけを想定していたと理解するのが正しい。しかし、現代社会は、既に仮想コンピュータが広く普及しているような社会環境にある時代に入っているという事実を正確に理解しなければならない。実際には仮想に過ぎないものを実在するものと誤認し、それが実在するものだという前提で法の解釈・適用等の判断をしてはならない。

(75) この利用者情報を送受信するための仕組み及び電気通信回線の詳細情報が利用者に提供されていない場合、それはいわゆる「バックドア」または「スパイ装置」の一種として違法なものとなり得るのであり、極論すれば、B-CASを用いた衛星放送というビジネスモデルそれ自体が全体として違法行為であることとなり得る。このことは、衛星放送のみならず、ケーブルテレビやインターネットテレビ等でも同様に妥当する。

仮に関連法令等によって秘密裡に利用者の個人情報を収集することを認めることができることとされている場合であっても、当該秘密裡に個人情報を収集できるものとする条項の立法根拠が他国からの侵略やテロ行為等の差し迫った危険に対応するための例外的で非恒常的措置であるような場合を除き、当該根拠法令とされる条項は憲法違反として無効であるので、結局、当該秘密裡に利用者の個人情報を収集することについての正当化事由が存在しないことになる。このような場合について考える上では、個人情報保護法16条3項を参照すべきである。なお、利用契約は「報道」それ自体とは無関係なので、同法50条1項1号の場合には該当しない。衛星通信会社が報道番組を一切提供せず、娯楽番組のみを放映するような場合を想定してみると、このことが明らかである。

これらの点を踏まえた上で、視聴者の行動等をリモートでモニタリング可能な仕様のB-CASまたはこれと類似する装置を用いたビジネスモデルを違法行為とならないようにするためには、①利用者情報を送受信するための仕組み及び使用される電気通信回線に関する情報、②送受信される情報の項目等の重要事項を利用者に対して事前に明確に示す必要がある。これらの事項が消費者契約法4条の重要事項に該当する場合には、消費者である契約当事者は、当該契約を取り消すことができるのにとどまり、当該消費者契約それ自体が当然に無効となるわけではないが、ビジネスモデル全体の適法性評価の問題としては、取消原因を常に包含している契約に基づくビジネスは違法行為であると言

されるとはいえ、B-CASカード内の記憶装置に記録されている電磁的記録は、それ自体が独立して電子的なトークンとして機能し得るものと考えることができる。その意味では、この事案における電磁的記録は、立法者が想定した範囲内にあるものだと考えることができる。

なお、B-CASカードと類似の装置を用いた課金処理阻害の事例として、「ブルーボックス」と呼ばれる装置を用いて電話使用料金の課金を免れたという事例がある。この事件については、東京地裁平成7年2月13日判決・判例時報1529号158頁がある(76)。

3．3　罪数

以上の事例は、社会的には役務提供事業者の課金業務を阻害する行為という類型に属する。これを刑法上の業務妨害罪（刑法233条、234条）としてとらえるべきかどうかについては、更に詳細な検討を経なければならない部分が多々あるけれども(77)、仮に同罪が成立し得るとした場合、電子計算機使用詐欺罪（同法246条の2）、私電磁的記録不正作出罪（同法161条の2第1項）、同供用罪（同条の2第3項）との間の罪数関係が問題となる。

一般に、電子計算機使用詐欺罪と業務妨害罪との関係は、観念的競合（同法54

わざるを得ない。なお、個人情報保護法17条及び16条所定の個人情報取扱事業者の義務の意義についても十分に考慮に入れられなければならない。これらの情報の提示を受けた者が利用契約を締結して利用者となった場合には、契約内容に事前の同意があったものとして適法行為となる。

ちなみに、この事件の被告人らは、契約当事者ではなく第三者の立場にあるので、消費者契約法の適用はない。また、仮に当該ビジネスモデルが違法性を有するものであったとしても、例えば、被告人らに対する損害賠償請求訴訟において、その違法性を主張することのできる正当な利益を有しないと解する。

(76) 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—」75頁で既に検討した。判例評釈として、奥村正雄「パソコンの不正信号送信による国際通話料金不払いと電子計算機使用詐欺罪の成否」同志社法学53巻3号377～392頁、後藤啓二「ブルーボックス事件」別冊NBL79『サイバー法判例解説』210～211頁、井上宜裕「コンピュータ詐欺(2)」別冊ジュリスト190『刑法判例百選Ⅱ各論（第6版）』114～115頁、永井善之「コンピュータ詐欺(2)」別冊ジュリスト221号『刑法判例百選Ⅱ各論（第7版）』118～119頁がある。

(77) 松原英世「パチンコ遊技機にとりつけられた電子計算機部分が刑法234条の2の電子計算機損壊等業務妨害罪にいう「電子計算機」に当たらないとされた事例」法と政治53巻2号482～468頁が参考になる。

条1項前段[78]）の関係にたつものと解する[79]。電子計算機使用詐欺罪と業務妨害罪とでは保護法益及び罪質[80]を異にすると解すべきであり、とりわけ、電子計算機使用詐欺罪では加害者の利得が構成要件要素となっているのに対して業務妨害罪では加害者の利得を必要としないので、これらの罪が法条競合の関係にたつと解すべき余地はない[81]。

他方、電磁的記録不正作出罪と同供用罪との関係に関しては、牽連犯（同法54条1項後段）の関係にあると解することについて異論はないと思われる。問題は、同供用罪と業務妨害罪との関係になるが、不正作出された電磁的記録が共用されれば直ちに業務妨害の具体的危険が発生すると考えられるから、供用行為と業務妨害行為とは同一の行為であると考えることができ、これらは、観念的競合（同法54条1項前段）の関係にあると考えられる。

背任罪（同法247条）及び電子計算機損壊等業務妨害罪（同法234条の2）との関係でも同様に考えることができる。

4　加害目的での背任罪と電子計算機損壊等業務妨害罪の罪数

4. 1　理論的な検討

背任罪（刑法247条）には2つの類型の犯罪が含まれている。一方は「自己若しくは第三者の利益」を図って実行されるものであり、他方は「本人に損害を加える目的」で実行されるものである。前者は、利益横領行為及び横領罪（同法252条、253条）と共通点の多い利欲犯であると言える。それゆえに、罪数論としては数々

(78) 前掲前田雅英編『条解刑法（第3版）』204～205頁には「前段」、「後段」との語の慣用例についての説明がある。

(79) 従来、この点が争点となった裁判事例が少なくとも公刊された裁判例の中には見当たらないのは、起訴時において、検察官が業務妨害罪にも該当するとは考えず、かつ、裁判所もそのような理論的可能性に考えを及ぼすことがなかったからではないかと想像される。

(80) 前掲『大コンメンタール刑法（第2版）第12巻』219～239頁、前掲前田雅英編『条解刑法（第3版）』690～691頁、団藤重光編『注釈刑法(5)各則(3)[改訂版]』（有斐閣、1968）398～399頁など。

(81) ただし、どの事実をとらえて訴因（公訴事実）を構成するかについては、検察官の起訴裁量に任されている。

の難問を生じさせてきた。しかし、後者は、加害目的の行為であり、加害者に利得が発生しないという点で、経済的利益に対する破壊罪という側面が強い(82)。つまり、正確には、背任罪には罪質の異なる2種類の犯罪が含まれていることになる。

経済的価値と交換可能な電子的なトークンに対する破壊行為が実行された場合、その行為それ自体としては私電磁的記録損壊罪（刑法259条）を構成し得るものであるが、背任罪との関係では、加害者に利得がない以上、加害目的での背任罪が成立し得ると考える。

4．2　裁判例

加害目的による背任罪の成立を認めた事例として、東京地裁昭和60年3月6日判決・判例時報1147号162頁がある(83)。

この判決によると、この事件の背景事情は次のとおりのようなものであった（当事者名等は一部仮名）。

> 株式会社綜合コンピューター（以下「株式会社綜コン」ともいう。）は、昭和56年4月コンピューター及びその附属部品の販売、ソフトウェアの開発、販売等を営業目的として設立された会社であり、設立当初からカシオ計算機株式会社の販売代理店（ディーラー）として同社製のオフィスコンピューターに、自社が開発した読売新聞販売店購読者管理システムのオブジェクトプログラム（以下「本件プログラム」という。）を入力したうえ、これを関東一都六県の読売新聞販売店約1800店を対象にして、各店に導入させることを主たる営業内容としていた。又、昭和58年4月ころからは富士通株式会社の販売代

(82) 破壊罪の大多数は、何らかの物的対象を破壊する行為を含む。このことは、保護法益の相違とは無関係のことで、例えば、殺人罪（刑法199条）や傷害罪（同法204条）では身体という物体の破壊、放火罪（同法108条～110条）では建造物等の物体の破壊、毀棄罪（同法258条～261条）では様々な物体の破壊（完全性の喪失）が基本的な構成要件要素となっている。ところが、加害目的での背任罪では物体の破壊が構成要件要素になっているのではなく、被害者の経済的利益が破壊の対象となっている点が明らかに異なる。

(83) 林幹人『判例刑法』（東京大学出版会、2011）373～378頁に解説がある。判例評釈として、佐久間修「コンピューター・プログラムの無断入力と背任罪の成否」産大法学19巻3号29～41頁がある。関連する論説として、半野潔「情報の刑法的保護」文社会論叢.社会科学篇18号119～143頁がある。

理店にもなって、同年８月ころから同社製の「ファコム」に入力できるオブジェクトプログラムの開発にとりかかつていた。

（中略）

本件プログラムは同社にとって極めて重要な営業上の財産であり、かつ企業秘密でもあり、仮に本件プログラムが他社に漏れ、無断で使用されることになれば、同社は本件プログラムを入力したオフィスコンピューターを他社より優位に販売することができず、会社の存立自体を危うくする可能性があるので、同社では、Ａ社長及びＢ専務が、毎日の朝礼、月１、２回の全体会議の際に、全社員に対し、本件プログラムの重要性、企業秘密性を強調して認識の徹底を図り、対外的にも、例えばコンピューターのリース契約の中途解約のときやレベルアップで解約される等の場合、当該コンピューターに入力されていた本件オブジェクトプログラムを消除したり、読売新聞販売店経営者の納金会で使用したデモ用のオブジェクトプログラムは使用後消除する等して、内容を他に漏らさない方策をとり、入力されている本件プログラムについては複製が不可能な技術的措置をとるなどして秘密の保持に努めていた。

（中略）

昭和58年８月ころ、株式会社綜コンでは、社員間で給与等待遇面に関し不満があり、同年９月被告人Ｍはこのことをカシオ計算機株式会社システム機器営業部東京システム営業所の営業担当Ｙに打ち明けた。同人は、被告人Ｍに対しカシオのディーラーとしての新会社設立を勧め、ソフトについては株式会社綜コンのソフトを使い、フロッピー方式からディスクベース方式に変えて行うこと等を示唆した。他方で右Ｙは、同年12月初旬ころＳに対しても同様の説得をし、同人は、新会社設立を決意した。被告人Ｍ及びＳは同年一二月中旬ころＹを通じて面談し、両名は共同で新会社を設立することを合意し、Ｓがユーザーを獲得し、被告人Ｍは株式会社綜コンの社員を引き抜くことのほか、新会社の扱うオフィスコンピューターに株式会社綜コンが開発した本件オブジェクトプログラムを使うことなどを決めた。その後被告人Ｍは、株式会社綜コンの社員らに新会社に加わることを勧めたが、結局被告人Ｋのみがこれに応じた。

Ｓは、昭和59年１月18日読売新聞橋本西部専売所のＺからオフィスコン

ピューターエリア3Dの注文を獲得し、これをまずS方に搬入することにした。そして、被告人M、S及びYは搬入されるエリア3Dには、被告人Kが本件プログラムを記録したフロッピーシートを保管しているので、同人にそのフロッピーシートを持参させ、これを使用して、本件プログラムを入力させることを決め、同月25日被告人Mは被告人Kに対し、同人の保管にかかるフロッピーシートを使ってS方に搬入されるエリア3Dに本件プログラムをセット入力するよう依頼し、被告人Kはこれを了解した。

以上のような経過を経て、被告人らは勤務先会社から無権限で持ち出したフロッピーディスクに記録されていた本件プログラムを別のコンピュータに記録して、勤務先会社の営業秘密である本件プログラムを違法に持ち出すこととなった。裁判所が認定した犯罪事実は、次のとおりである。

被告人両名及びSは、共謀の上、被告人Kの前記任務に背き、自己らの利益を図る目的で、昭和59年1月26日ころ、東京都所在のS方において、右S及び被告人Mが同社と無関係に読売新聞販売店であるZに賃借（リース）させ、同人方に設置予定であつたオフィスコンピューターエリア3D型1台に、被告人Kにおいて、前記フロッピーシート5枚分の前記オブジェクトプログラムを入力し、もつて株式会社綜合コンピューターに対し、右オブジェクトプログラム入力代金相当額（株式会社綜コンが昭和58年8月31日から同年12月24日までの間に本件プログラムを入力して販売したエリア3D6台のソフト料合計を基準に平均値を算出すると約170万余円となる。）の財産上の損害を加えたものである。

要するに、勤務先会社の待遇等に不満をもっていた従業員らが、勤務先会社の営業秘密であるコンピュータプログラムを無断で持ち出し、これを主力商品として、勤務先会社と競合関係にある新会社を設立・独立しようとしたという事案ということになる。従業員が独立して競合関係にある新会社を設立する場合には少なからずあり得ることであり、この事件が発生した当時には、競業避止義務等について盛んに議論がなされた。しかし、当時、現行の不正競争防止法が定めるような強力な

罰則は存在しなかった。

裁判所の認定した事実によれば、被告人らは、本件プログラムの持ち出し行為によって直接的な利益は得ていないようであるので、被害者である勤務先会社に対して本件プログラムの販売代金相当額の損失を発生させたというだけのことになるのだが、犯罪事実の欄では「自己らの利益を図る目的で」と事実認定されている。やや不鮮明な印象を与えるかもしれない。しかし、裁判所は、被告人らが独立して新会社を設立し、元の勤務先会社と競合する事業により利益を得ようとしていたという点をとらえて利得目的の行為と判断したものだと理解することができる。

したがって、この事件の事案は、利得目的の背任罪の事案であり、加害目的の背任罪の事案ではない。しかし、仮に被告人らが自己または第三者の利得を目的とすることなく、単に不満の解消として勤務先会社を困らせる目的（加害の目的）で本件プログラムを記録したフロッピーディスクを持ち出し、そのプログラムの保管のためにオフィスコンピュータの記憶装置に記録しておいたという事例を想定してみると、それでもなお背任罪の成立を免れることはできないと考えられる。

この事件は、1980年代における日本国内のIT産業の状況を知らないと理解できない部分がかなり多い(84)。当時は、顧客管理アプリ程度でのソフトウェアでも相当高額の利益を得る事業を遂行することができ、そのようなごく単純なプログラムでも営業秘密として大事に扱われていたということを知ることができる。このことはまた、現時点では極めて貴重な営業秘密や知的財産として扱われているものであっても、10年以上たつとごく普通のものになってしまっている可能性が高いことを示唆している。一般に、法改正により著作権や特許権の保護期間が次第に長くなる傾向にあるけれども、本当にそれで良いのかどうか再検討すべき余地があるのではないかと思う。

(84) 現在の標準的なスマートフォンは、この事件でプログラムを記録したオフィスコンピュータ（電子計算機）の何万倍もの処理能力と記憶能力をもっている。問題となった顧客管理プログラムにしても、現在では無料のアプリとして類似品がいくらでもある。ごく普通のPCとMicrosoft Excelのような汎用ビジネスソフトを用いれば、この事件で問題となったプログラムで処理するよりもはるかに効果的・合理的・迅速に事務処理をすることができると考えられる。それゆえ、現代の若い世代にとっては、この事件がどうして刑事事件にまで発展したのか理解しにくい部分があるかもしれない。

4．3　罪数

上記の東京地裁昭和60年3月6日判決の事例は利得目的の背任罪の事例であるが、仮にこれが加害目的の背任罪の事例であったとしても、やはり有罪となったと考えられる。そこで、加害目的の背任罪の罪質及び罪数論上の留意点ついて、簡単に述べる。

一般に、加害目的での背任罪が実行され既遂に達すると、本人（被害者）の経済的利益が滅失または減少することになるのであるが、この被害者の経済的利益の破壊という側面に着目すると、加害目的での背任罪の本質は、横領罪よりもむしろ信用毀損罪や業務妨害罪（同法233条）と非常に密接な関連を有するということを理解することができる。

このことを考慮に入れれば、業務妨害罪（信用毀損罪）と加害目的での背任罪との罪数関係は、法条競合の関係にたつと考えるべきであり、それゆえに、業務妨害罪（信用毀損罪）が成立しない場合にのみ、補充的に加害目的での背任罪が成立すると解するのが正しいと考える。

なお、加害目的の背任行為の場合、利得罪としての性質を有しないので、それが電子的に実行された場合でも電子計算機使用詐欺罪（同法246条の2）を構成しない。

5　まとめ

電子計算機使用詐欺罪が利益窃盗罪としての犯罪学的な本質を有することは既に述べてきたとおりであるが、本論文における検討結果として、電子計算機使用詐欺罪が利益窃盗類型に属する違法行為のみならず、利益横領類型に属する違法行為や背任類型に属する違法行為等に対してもまた、相当広い範囲で適用可能な処罰法令として存在し現実に社会で機能しているということを明らかにすることができたと考える。

このことは、電子計算機使用詐欺罪というものが、従来考えられてきたようなコンピュータ犯罪（電子計算機犯罪）の一種といったやや限定された法的位置づけよ

り以上のものであるということを示唆していると言うことができる。すなわち、電子計算機使用詐欺罪は、電子的な情報財について、その財産権的側面を刑事法の見地から法的に保護するための共通の法的プラットフォームの一種であり得るということを示唆しているのである。このように考えてくると、電子計算機使用詐欺罪の立法上の位置づけが適切でないということにもなる。

同様のことは、電子計算機損壊等業務妨害罪についても認めることができる。

加えて、刑法以外の法令、例えば、不正競争防止法等の関連法令との関係についても更に検討を深める必要がある。そして、時代の変化と技術革新に伴い生起する新たな法的課題にも適切に対応していく必要がある。

今後、サイバー法の領域においても、関連する法学領域と密接な関連を保持しながら、総合的な研究が尽くされることを期待したい。そのような研究はまた、様々な知的財産権を侵害する犯罪行為と刑法犯である犯罪行為との間の法解釈論上の論理関係を考察する上でも極めて重要であると考える(85)。

以上で本論文における検討を終える(86)。

---

(85) 前掲藤木英雄『刑法各論』30～31頁には、同書が刊行された1970年代における所感として、「今日の課題としては、経済生活が複雑化し、有体物に化体した利益よりは、無形的な利益に重点が移るにつれ、無形の財産、とりわけ工業所有権として保護されるに至っていないノウハウ、ソフトウェアすなわちコンピュータのプログラム、あるいは生産システム、その他の企業の経営に関する各種の情報（とくに企業秘密）等公開を条件に独占権を認める工業所有権としての保護を求めず非公開にしておくものについて刑法上の保護を与える必要があるかどうかが問題となっている」と述べられている。ここで述べられていることは、その後、その全てについて、不正競争防止法や著作権法等の改正による権利保護と罰則強化等によって実現されるに至った。また、中山信弘氏や北川善太郎氏の尽力により、この分野における研究が格段に深まり、研究者の層も厚みを増すこととなった。しかし、知的財産権の刑事的保護に関してはまだまだ研究が尽くされていない部分が数多くあると考える。

他方で、これまでの日本国の法制では、基本的に産業育成法が優位であり、私人の単なる自由を強化するという方向での法政策論は極めて貧弱または皆無である。強いて言えば、消費者保護法の関連では比較的活発な動きはあるけれども、冷静に考察してみると、消費者保護法は産業法または経済法の一種であり、産業政策の一環であり得る。そうではなく、私人の単なる自由や私生活における静穏を確保し強化するという方向での公共政策論的または法政策論的な研究がこれからの法学研究の主流となるべきであろう。この分野は、ほとんど開拓されておらず、荒野のままの状態に等しい。

(86) 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。