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　第八五巻　第四・五合併号（二〇一三・一）

【論　説】

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――

夏　井　高　人

目　次

一 はじめに

詐欺行為の本質は、被害者の錯誤に乗じて何らかの価値あるものを被害者自身に提供させるところにある。すなわち、被害者自身を道具とする間接正犯のような犯罪としての基本的構造をもっている。

一般に、他人を欺罔して財産を奪い取る詐欺行為は、おそらく人類の文明社会の発生と共に誕生したものであり、相当古い時代からあるものと推定される。詐欺の標的とされたのは基本的には物体としての財物であった。そのため、伝統的な刑罰法令においては、物体の詐取を基本的な形態とする犯罪類型が想定されてきたし、明治時代に制定された日本国の刑法における詐欺罪（刑法二四六条一項）の構成もそのようなものとなっている。より正確には、詐欺罪のみならず、世界の刑法における財産犯の体系は、物体としての財産の保護を主体として構築され維持されてきた。

その後、人類社会の経済取引が盛んになり、物体ではない債権それ自体が財産権としての重要性を増すにつれ、例えば、欺罔行為によって金銭債務の支払を免れる行為や金銭債権を移転させる行為のように「財産上の利益」を得る

行為もまた詐欺行為の一種であると認識されるようになった。日本国の刑法においても、財産上の利益が保護法益の一つとして規定されている（刑法二四六条一項）。

更に人類社会が発展すると共に、物体の提供だけではなく役務の提供もまた社会的に大きな財産価値を有するに至った。そのため、役務について財物と同様に刑法上の保護が与えられてしかるべきであるにもかかわらず、世界の刑法思想の大勢がそのような役務の重要性を承認するという歴史的段階にはまだ至っていないことが明らかである。例えば、電気窃盗（刑法二四五条）は、理論的には電気供給役務に対する侵害罪として構成することも可能であるはずなのに、実際には財物奪取罪の一種（法定の類推）として刑法中に規定されている。

まして、財物でも財産的利益でも役務でもない純然たる「情報」を刑法によって保護することの重要性については、その本質をとらえた理解が普及しているとは言い難い状況にある。(1)

もちろん、電子通信技術が一般に普及する以前の時点においても「情報」を奪う行為は存在した。しかし、従来は、「情報を奪う行為」とは言っても標的とする情報を記録した物理媒体を奪うことが犯罪の主体となっていたと考えてよい。(2)このことは、日本の裁判例でも同様である。

他方で、「情報」は、財産権としての経済的価値が重要となる場面が多々ある。しかし、そのような経済財としての「情報財（information goods）」(3)という側面のみならず、例えば個人識別性や国家機密性といったような（経済財としての観点とは異なる）別の次元での価値（交換価値以外の価値）を有する場合がある。そのため、「情報を奪う行為」の保護法益もまた、財産権に限定されることなく、多種多様なものとなり得る。それゆえ、「情報を奪う行為」を単に財産犯の一種としてのみとらえることは、この種の違法行為の法的本質を見誤ることにもなり得るし、その結果として、適切でない立法的対応を導くこととともなりかねない。

本論文では、以上のような問題意識に基づき、様々なサイバー犯罪[4]の中でも現代社会において非常に大きな経済的損失を発生させる原因行為の一つであるいわゆるフィッシング（phishing）を素材としつつ、被害者の錯誤に乗じて「情報」を奪う行為一般について、比較法的検討を行う[5]。

そして、これらの検討を踏まえながら、「情報を奪う行為」と関連する保護法益が多様であるという認識を前提に、現行の日本国法令に基づく刑事罰の適用可能性について論じ、もって法律実務に資することを目的とする。

なお、検討対象とした日本国法令は、原則として、二〇一二年一〇月一日の時点で施行され有効となっている法令に限られる。

二　フィッシング（Phishing）

一般に、フィッシング（phishing）とは、①ソフトウェアの脆弱性等を悪用し、返信アドレスを偽装した電子メールを送信する行為や偽装されたハイパーリンクを真正なものと信じさせる行為等によって被害者を錯誤に陥らせ、②錯誤に陥った被害者を偽装されたサイト上に誘導した上で、③そのサイトを真正なものと誤信した被害者にＩＤ、パスワード、銀行アカウント、クレジットカード番号、その他の識別符号などを入力させることにより、④入力された符号を無権限で取得する行為を意味する[6]。

社会的病理現象としてのフィッシングの危険性については、二〇〇五年ころから強く認識されるようになった[7]。その最近の傾向について、フィッシング対策協議会は、「二〇〇九年の後半から、我が国におけるフィッシングの報告件数が増加している。二〇一一年度のフィッシング対策協議会に対するフィッシング情報の報告件数は対前年度で約二

三％増（二〇〇九年度二八三件から、二〇一〇年度四〇六件、二〇一一年度四九八件）、フィッシングサイトの件数は、対前年度で約一三％増（二〇〇九年度二六〇件から、二〇一〇年度五一六件、二〇一一年度五八二件）である。これは、二〇〇九年度の傾向が継続しており、フィッシングサイトのテイクダウンを回避するなど、フィッシング手法の高度化や、関与する犯罪者の増加を反映しているものと考えられる」との認識を示している。(8)

さて、フィッシングには、①スパムメールのようなやり方で多数（特定多数または不特定多数）の者に同一内容の電子メールを送信し、たまたま錯誤に陥ったメール受信者等を偽装したサイトに誘導する場合及び②特定の者（個人、組織、団体）を標的として誘導するためのメールを送信し、その特定の者だけを偽装したサイトに誘導する場合がある。(9)後者の場合を特に標的型フィッシング（targeted phishing）、標的型メール攻撃、(10)ＡＰＴ攻撃（Advanced Persistent Threats）(11)またはスピアフィッシング（spear phishing）等と呼ぶ場合がある。(12)フィッシングは、電子メールなどの文字によって実行されるのが通例であるが、音声によることもあり得ることである。音声によるフィッシングは、voice phishing の省略形としてヴィッシング（Vishing）と呼ばれている。(13)日本国で「振り込め詐欺」と呼ばれる詐欺類型もその一種として理解することができる。

ＡＰＴ攻撃またはスピアフィッシングの実例としては、例えば、ＲＳＡの SecurID に対するサイバー攻撃の際に実行されたＲＳＡ従業員に対するスピアフィッシングの例(14)や三菱重工が保有する防衛機密事情を狙ったサイバー攻撃の際に実行された同社従業員に対するＡＰＴ攻撃の例(15)などがある。(16)ＡＰＴ攻撃では、現実に存在する個人・組織・団体等から送信された信頼できるもののように偽装した電子メール等を用い、巧みに偽装サイトへ誘導したり、機密情報等を含む電子メールを返信させたりする手口が用いられることがしばしばある。(17)

「フィッシング（phishing）」という語の語源については、諸説ある。fishing のスラングの一種だという説(18)が有力だ

が、ほかに①phreaking と fishing との合成語とする説[19]、②sophisticated と fishing との合成語とする説[20]及び③password harvesting fishing の短縮形であるとの説[21]などがあり、確実な説はない。しかし、どれが真の語源であるにしろ、フィッシング（phishing）という攻撃手法が存在することそれ自体については異論がない[22]。

フィッシングの手法を用いた情報の無権限取得行為は、一般に、「フィッシング詐欺（phishing SCAM または phishing fraud）」と呼ばれている。しかし、フィッシングによって取得されるのは情報であって財物または財産上の利益ではないので、日本国刑法が規定する財産罪としての「詐欺」とは異なる意味で「詐欺」の語が用いられていることに留意しなければならない。また、「phishing fraud」の場合の「fraud」とは、米国連邦及び各州の犯罪法における個人識別情報の無権限取得（ID theft）のことを意味し、日本国刑法に規定する詐欺罪（刑法二四六条）のことではないので、注意を要する。混乱を避けるため、「phishing」の日本語訳としては、単に「フィッシング」を用いるのが妥当と思われる[23]。

三　保護法益の相違に基づく適用可能な刑罰法令の検討

日本国において、フィッシング行為を一般的に処罰対象とする法令は存在しない。しかし、フィッシングのような被害者を錯誤に陥らせ、その錯誤に基づいて被害者から特定の種類に属する情報を提供させる行為を処罰対象行為とする法令が幾つか存在する。それら個別の刑罰法令における保護法益に着目しつつ、フィッシング行為に対して適用可能な現行法令を概観すると、次のとおりとなる。

1 ネットワークシステムの安全性・信頼性の確保

(1) アクセス制御機能

フィッシングによって無権限で取得される情報の中には、特定電子計算機にアクセスするために用いられる識別符号としてのＩＤやパスワード等に該当するものがある。識別符号は、アクセス管理者によって設定されるものである。そして、不正アクセス禁止法の保護法益は、特定電子計算機のアクセス制御機能に対する社会的信頼の確保にあると解するのが通説である。(24)

従来、他人の識別符号を無権限で提供する行為については、不正アクセス行為を助長する行為（平成二四年三月三一日法律第一二号による改正前の不正アクセス禁止法四条）となるほか、無権限で識別符号を用いてアクセスする行為は不正アクセス行為（同法三条）として処罰可能であったものの、無権限で他人の識別符号を取得・保管する行為については罰則が存在しなかった。しかし、前記三菱重工へのサイバー攻撃（二〇一一年九月）や衆議院及び参議院に対するサイバー攻撃（二〇一一年八月～一〇月）などにより識別符号が奪われるという事件が発生したことから、識別符号の無権限取得行為についても処罰できるようにすべきであるとの社会的要請が高まったとされている。(25)

このような社会情勢の変化を受け、平成二四年三月三一日法律第一二号により不正アクセス禁止法の一部改正がなされ、フィッシングを構成する各行為のうち、①（詐欺罪における欺罔行為に相当する）他人の識別符号の要求行為、②（詐欺罪における詐取行為に相当する）他人の識別符号の取得行為、③（詐欺罪では不可罰的事後行為である）他人の識別符号の提供行為及び④（同じく詐欺罪では不可罰的事後行為であるか、事案により刑法二五六条二項の罪に

相当する）他人の識別符号の保管行為が処罰されるべき行為として明定されるに至った[26]。

なお、⑤他人の識別符号の行使行為については、特に行使罪が新設されたわけではないが、他人の識別符号を不正アクセスの目的で行使すれば、当然のことながら、不正アクセス行為（同法三条）が成立することになる。

(a)　他人の識別符号の要求行為

同一部改正によって、フィッシングの実行行為（詐欺罪における欺罔行為に相当する行為）を「要求する行為」として処罰する条項が新設されることとなった（同改正後の不正アクセス禁止法七条）。

一部改正後の七条は、「当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電気通信回線に接続して行う自動公衆送信（公衆によって直接受信されることを目的として公衆からの求めに応じ自動的に送信を行うことをいい、放送又は有線放送に該当するものを除く。）を利用して公衆が閲覧することができる状態に置く行為」（同条一号）及び「当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電子メール（特定電子メールの送信の適正化等に関する法律（平成一四年法律第二六号）第二条第一号に規定する電子メールをいう。）により当該利用権者に送信する行為」（同条二号）について、「アクセス制御機能を特定電子計算機に付加したアクセス管理者になりすまし、その他当該アクセス管理者であると誤認させて」実行してはならない旨を規定している。同法七条違反の行為は、一年以下の懲役または五〇万円以下の罰金に処せられる（同法一二条四号）。

(b)　他人の識別符号の取得行為

同一部改正によって、フィッシングによる取得の場合を含め、不正アクセス行為を実行する目的によるものである

限り、無権限で識別符号を取得する行為（詐欺罪における詐取行為に相当する行為）の全てを「取得する行為」として処罰する条項が新設されることとなった（同改正後の不正アクセス禁止法四条）。

一部改正後の同法四条は、「何人も、不正アクセス行為（第二条第四項第一号に該当するものに限る。第六条及び第一二条第二号において同じ。）の用に供する目的で、アクセス制御機能に係る他人の識別符号を取得してはならない」と規定し、同条に違反してアクセス制御機能に係る他人の識別符号を取得した者は、一年以下の懲役または五〇万円以下の罰金に処せられる（同法一二条一号）。

(c) 他人の識別符号の保管行為

同一部改正によって、フィッシングによる取得の場合を含め、不正アクセスの目的で不正に取得された識別符号を保管する行為（詐欺罪においては不可罰的事後行為）についても処罰条項が新設された（同法六条）。

一部改正後の同法六条は、「不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管してはならない」と規定し、同条違反の行為は、同法四条及び七条と同様に罰せられる（同法一二条三号）。

(d) 他人の識別符号の提供行為

同一部改正によって、同改正前の同法四条を一部改正し、フィッシングにより取得した識別情報である場合を含め、業務その他正当な理由による場合を除き、他人の識別符号を提供する行為（詐欺罪においては不可罰的事後行為）について処罰する条項が設けられた（同改正後の同法五条）。

一部改正後の同法五条は、「何人も、業務その他正当な理由による場合を除いては、アクセス制御機能に係る他人の識別符号を、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない」と規定し、同条違反の行為は、同法四条、六条及び七条と同様に罰せられる（同法一二条二号）。

(e) **罪数**

同法七条の「要求」行為、同法四条の「取得」行為、同法五条の「提供」行為及び同法六条の「保管」行為相互の罪数関係については必ずしも明確ではない。[27]

取得または保管した識別符号を行使する行為は、不正アクセス行為そのものを構成するが（同法三条）、不正アクセス行為と要求行為・取得行為・保管行為との間の罪数関係もまた明確ではない。[28]

なお、不正アクセス行為の後、不正アクセスした特定電子計算機内に記録されていた他人の識別符号を取得する行為は、新たな取得行為を構成する。この場合における不正アクセス罪と取得罪との関係は、併合罪（刑法四五条）となる。[29]

(2) ブラウザ等のアプリケーション

フィッシングの実行のための手口は電子メールの偽装だけに限らない。ヴィッシング（Vishing）[30]のように音声を用いた詐欺行為は別として、ブラウザにマルウェア（Malware）[31]を感染させ、真正なサイトのようにみせかけて偽サイト（フィッシングサイト）へと誘導する手口もある。加えて、ブラウザにマルウェア感染をさせるわけではないが、ブラウザの表示上で偽サイトを真正なものとみせかける手口として、ＤＮＳサーバに対するＤＮＳ偽装攻撃（DNS Spoofing）やＤＮＳキャッシュポイゾニング攻撃（DNS cache poisoning）などがある。[32]このような攻撃が実行され、当該ＤＮＳサーバの記録が無権限で書き換えられたような場合には、事案により、電磁的記録不正作出罪（刑法一六八条の二）、私電磁的記録毀棄罪（刑法二五九条）、電子計算機損壊等業務妨害罪（刑法二三四条の二）、不正アクセス罪（不正アクセス禁止法三条）等が成立し得る。ＤＮＳサーバの運用者は、いわば間接正犯の道具としてフィッシング実行のために利用された被害者という立場にたつことになる。[33]

また、Facebook[34]、LinkedIn[35]、Google+[36]のようなソーシャルメディア（ＳＮＳ）を感染経路としてスマートフォンの

アプリ等にマルウェアを感染させる手口などもある。

このような利用者を錯誤に陥らせてフィッシングサイトへと誘導するマルウェアは、「人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録」すなわち不正指令電磁的記録（刑法一六八条の二[37]）に該当すると理解することが可能である。

そして、「正当な理由がないのに、人の電子計算機における実行の用に供する目的で」不正指令電磁的記録を①作成する行為もしくは②提供する行為（同条の二第一項一号）、または、③「正当な理由がないのに」不正指令電磁的記録を実行の用に供する行為（同条の二第二項）を実行した者は、三年以下の懲役又は五〇万円以下の罰金に処せられる。未遂罪も処罰される（同条の二第三項）。

また、「正当な理由がないのに、人の電子計算機における実行の用に供する目的で」不正指令電磁的記録を④取得する行為もしくは⑤保管する行為を実行した者は、二年以下の懲役又は三〇万円以下の罰金に処せられる（刑法一六八条の二第三項）。

(3) 電子メール通信

偽装サイト（フィッシングサイト）への誘導のために電子メールの返信アドレスを偽装する手口が用いられることがある。

例えば、XXXというＩＰアドレスから送信されてきた電子メールのように見えるが、実は真のＩＰアドレスYYYを隠蔽してXXXであるかのよう見せかけるための偽装であり、その電子メールに返信をすると表示されている電子メールアドレスのＩＰアドレス（XXX）とは別のＩＰアドレス（YYY）へと電子メールが返信されてしまうような仕掛けになっている場合がある。このような場合において、返信された電子メールの本文に機密事項等が含まれていると、その機密事項等を含む情報が、ＩＰアドレスYYYを支配している者（加害者）に届けられることになり、そのよ

うな送信者（被害者）を道具とする間接正犯的な行為によって無権限で加害者に取得されてしまうことになる。

他方、電子メールの本文中において真正なサイトへのＵＲＬリンク（WWW）が設定されているが、実は真のサイトのＵＲＬ（ZZZ）を隠蔽してWWWであるかのように見せかけるための偽装であり、そのWWWと表示されているリンクをクリックするとZZZへと接続されてしまうような仕掛けになっている場合もある。この手口は、主として、マルウェアに感染させるための仕掛けがしてあるサイトへの誘導のために用いられることが多いが、フィッシングサイトへの誘導のために用いられることもある。

これらのようなＩＰアドレスやＵＲＬの偽装行為の中で、「電子メールの送受信のために用いられる情報のうち送信者に関するもの」の偽装行為については、特定電子メールの送信の適正化等に関する法律（平成一四年四月一七日法律第二六号・以下「特定電子メール適正化法」という。）に定める禁止条項及び罰則が適用され得る。

すなわち、特定電子メール適正化法五条は、①「当該電子メールの送信に用いた電子メールアドレス」または②「当該電子メールの送信に用いた電気通信設備を識別するための文字、番号、記号その他の符号」を偽って特定電子メールを送信する行為を禁止している。そして、同条に違反する行為を実行した者は、一年以下の懲役又は一〇〇万円以下の罰金に処せられる（特定電子メール適正化法三四条一号）。

ただ、「特定電子メール」とは、「電子メールの送信（国内にある電気通信設備（電気通信事業法第二条第二号に規定する電気通信設備をいう。以下同じ。）からの送信又は国内にある電気通信設備への送信に限る。以下同じ。）をする者（営利を目的とする団体及び営業を営む場合における個人に限る。以下「送信者」という。）が自己又は他人の営業につき広告又は宣伝を行うための手段として送信をする電子メールをいう」と定義されていることから（同法二条二号）、商業宣伝広告を目的としない電子メールは「特定電子メール」に含まれないことになる。そして、通常、フィッ

シングのために送信される電子メールは、商業宣伝広告を目的とするものではなく、何らかの犯罪行為または反社会的行為の実行を目的とするものであることから、原則として、「特定電子メール」には含まれないということにならざるを得ない。同法の適用があるのは、商業宣伝広告を目的とする電子メールでありながら、同時にフィッシングのための手段として送信される電子メールであるような場合のみである。

なお、内容的に虚偽を含む記述（符号）が含まれる電子メールであっても、当該記述が「電子メールの送受信のために用いられる情報のうち送信者に関するもの」に該当しない場合には、同法の適用はない。事案により、電磁的記録不正作成罪（刑法一六一条の二）が成立し得るのみである。

このほか、電子メールアドレス等の偽装をするプログラムやスクリプト等が電子メール内に組み込まれた状態で送信される場合には、そのプログラムやスクリプト等が前述の不正指令電磁的記録（刑法一六八条の二）に該当し得る場合があることは言うまでもない。

(4) 偽装されたサイトに対する信頼の保護

フィッシングサイト[38]によって偽装された真正のサイト（以下「被偽装サイト」という。）の商業的利益を保護法益ととらえることが可能な場合がある。フィッシングを成功させるために真正なサイトとそっくりの偽サイト（フィッシングサイト）が構築されるような場合がその典型例である。

例えば、フィッシングの目的でクレジットカード会社ＶＩＳＡの偽サイト（フィッシングサイト）が構築されたという事例を考えてみると、その偽サイトではＶＩＳＡの真正な商標等が欺罔行為の手段として使用されているはずであることから、ＶＩＳＡの有する商標権の侵害が発生し得ることになる。

他方、偽サイト（フィッシングサイト）上で表示されるコンテンツの中には真正なサイトから無許諾でコピーされ

たものが用いられることがあり、その場合には、その無許諾でコピーされ使用された部分について著作権法違反（同一性保持権、複製権、公衆送信権の侵害）が発生し得ることになる。

更に、偽サイト（フィッシングサイト）が存在することによって利用者間に混乱が生じ、真正なＶＩＳＡサイトの業務に支障を生じさせた場合には、未必的なものであるにせよ業務妨害の結果発生について故意の成立を認め得る限り、刑法上の業務妨害罪が成立し得ることになる。

これらの場合は、いずれも、偽装される企業等の法人、個人、その他の組織・団体が存在しており、かつ、それらの組織や個人が商法上の商人であると理解することが可能な場合などに適用可能である。ただし、非営利法人等に関しては、別の考察が必要となる。

以下、偽装サイト（フィッシングサイト）によって偽装された真正なサイトを被害者とする場合について述べる。

(a)　商標法違反の罪

商標法は、商標権または専用使用権の侵害の場合（商標法七八条）及び虚偽表示を行った場合（同法七四条）について、罰則を定めている（同法八〇条）。

商業サイトを偽装したＷｅｂサイトを用いたフィッシングにおいては、事案により、そのいずれかに該当する事例が少なくないものと思われる。

まず、同法七八条は、「商標権又は専用使用権を侵害した者（第三七条又は第六七条の規定により商標権又は専用使用権を侵害する行為とみなされる行為を行った者を除く。）は、一〇年以下の懲役若しくは一〇〇〇万円以下の罰金に処し、又はこれを併科する」と規定している。

また、同法七四条は、「登録商標以外の商標の使用をする場合において、その商標に商標登録表示又はこれと紛らわ

しい表示を付する行為」を禁止し（同条一号）、この禁止に違反する者は、三年以下の懲役又は三〇〇万円以下の罰金に処せされる（同法八〇条）。

(b) 著作権法違反の罪

真正なＷｅｂサイト上の真正なコンテンツを無許諾で複製し、真正なサイトとそっくりな偽装サイトを構築するためにそのサイト上で用いた場合において、当該コンテンツが著作物であるときは、当該コンテンツの複製権侵害または公衆送信権侵害が問題となり得る。また、著作物であるコンテンツを無許諾で改変した場合には、当該コンテンツの同一性保持権の侵害が問題となり得る。

これらいずれの場合についても、著作権法違反として、著作権法に定める罰則が適用可能である（著作権法一一九条）。

この点に関する裁判例としては、フィッシングの目的でヤフー株式会社（Yahoo Japan）のホームページを偽装した偽サイトを構築した行為が著作権侵害に該当するとして有罪となった事例がある（東京地判平成一七年九月一七日・判例集等未搭載）。この事件において、被告人は、著作権法違反の罪及び不正アクセス禁止法違反の罪の二つの公訴事実により起訴されていたのであるが、東京地裁は、いずれも有罪と認め、被告人に対し、懲役一年一〇月（執行猶予四年）の刑を言い渡した。東京地裁が認定した著作権法違反の事実は「ヤフー株式会社が開設したホームページを利用するために必要な他人のログインＩＤ及びログインパスワードを入手するため、被告人が管理する公衆の用に供されている電気通信回線に接続している自動公衆送信装置である大阪市中央区〈省略〉株式会社Ｃ所在のサーバコンピュータ上に、ヤフー株式会社が著作権を有する著作物であるホームページのログイン画面を複製しようと企て、法定の除外事由がなく、かつ、著作権者の許諾を受けないで、公衆からの求めに応じて自動的に公衆に直接受信させる目的で、平成一七年二月一八日ころ、前記株式会社Ｃにおいて、前記サーバコンピュータの記録媒体に、前記ログイン

画面を複製して記録し、そのころから同月二四日ころまでの間、前記複製に係るログイン画面を送信可能化し、もって前記著作権者の著作権を侵害」したというものである（公訴事実第一・当事者名等は一部仮名）。なお、被告人は、公訴事実第一の行為により構築した偽サイト（フィッシングサイト）を使って他人のＩＤ及びログインパスワードを取得した上で、取得したＩＤ及びログインパスワードを用い、真正なYahoo Japanホームページにアクセスした。そのアクセス行為については、不正アクセス行為（不正アクセス禁止法三条）に該当するものとして有罪とされた（同判決中の公訴事実第二）。

(c)　業務妨害罪

一般に、フィッシングは、真正なサイトに対する直接の攻撃行為を構成しない。したがって、フィッシングが実行されても、偽装サイト（フィッシングサイト）によって偽装された真正なサイトに対する電子計算機損壊等業務妨害罪（刑法二三四条の二）を構成するものではないし、同様に、威力業務妨害罪（刑法二三四条）を構成するものでもない。

しかしながら、フィッシングのための偽装サイトを構築・運用する行為は、「偽計」の一態様であると考えることができるから、偽計業務妨害罪（刑法二三三条）の成立を認め得る場合があり得ると考えられる(39)。ただし、この場合の故意としては、ほぼ常に未必的な故意にとどまると考えられる。なぜなら、フィッシング実行者の意図としてはフィッシングにより欺罔された者から何らかの情報を取得することが主たる目的なのであって、その結果として副次的または派生的に真正なサイトについて業務妨害の結果が発生したとしても、そのような結果の発生は当該犯罪の主たる目的ではあり得ないからである。

なお、通説によれば、既遂となる時期は、現実に業務妨害の結果が発生した時点ではなく、業務妨害の結果発生の具体的な危険が生じた時点である(40)。

2 情報の安全性・信頼性の確保

(1) プライバシーに属する情報

フィッシングは、社会的な見地からすれば、特定の人の通信内容の秘密を無権限で取得する行為に該当する場合があり、その意味で、電気通信事業法、有線電気通信法及び電波法に定める通信の秘密に対する侵害の罪が成立し得るのではないかと考えられることがある。

しかしながら、現行の電気通信事業法、有線電気通信法及び電波法における「通信の秘密」は、他人の間でなされる通信の秘密を指すものであり、通信当事者間の通信を指すものではない。そして、フィッシングでは、通信の受信者がフィッシングの実行者となっている。換言すると、フィッシングの実行者が通信の一方当事者となっている点に特徴がある。

そのため、フィッシングにおいては、「他人間の通信」という意味での「通信の秘密」に対する侵害は、いずれも成立しないことになる。(41)

「通信の秘密」に関するこのような理解は、一般人の素朴な感情とは相当に乖離しているかもしれない。しかし、現行法における通信の秘密の保護及び侵害行為に対する罰則がそのような構成になっている以上、やむを得ないものである。これらの法令における「通信の秘密」の保護は、他人間の通信に通信当事者以外の第三者が干渉することを禁止するものであるのにとどまる。(42)

なお、フィッシングによって通信の秘密に対する侵害がなされないとしても、フィッシングにより無権限で取得される情報内容がプライバシーの利益を含んでいる場合には、別途、プライバシー侵害として民事上の不法行為（民法

七〇九条）に基づく損害賠償責任が成立し得ることがある。

また、フィッシングにより無権限で取得された情報内容が第三者に開示されることによって、名誉毀損が成立することもあり得る。名誉毀損が成立する場合、民事上は不法行為に基づく損害賠償請求が可能であると同時に、刑法上も名誉毀損罪として処罰対象行為となり得る（刑法二三〇条）。

なお、個人情報保護法中にも罰則は存在するが、主務大臣の勧告・指示等（個人情報保護法三四条一項）を個人情報取扱事業者が遵守しない場合に主務大臣によってなされる是正命令等（同条二項、三項）について、当該個人情報取扱事業者に違反行為があった場合に適用されるものである（同法五六条）。すなわち、個人情報の取扱に関する行政監督法規の一種である個人情報保護法に基づく「主務大臣の行政監督権の実効性確保」が保護法益となっているのであり、個人情報に関して当該個人情報の本人が何らかの法的利益を有するものという前提でその私的な法的利益を保護法益として罰則が設けられているわけではない。

以上のことから、フィッシングによって個人の私生活に関する情報が無権限で取得されてしまったとしても、刑事罰の適用がない場合のほうが多いということになる。現行の刑罰法令の体系においては、私人の私生活上の利益（法益）が比較的軽視されてきたし現在でもそうであるという歴史的事実を反映するものにほかならない(43)。

(2) 電子的な支払手段に関する情報

フィッシングにより無権限で取得される情報の中にはクレジットカードなどの支払手段と関連を有するものが多々含まれている。国際的な犯罪組織の中には、様々なサイトに対する不正アクセスやフィッシングによって取得した他人のクレジットカード情報を、クレジットカードの偽造のために情報を求めている犯罪者や犯罪者集団に売り渡すといった例がかなり多数ある(44)。

一般に、クレジットカードは、提示と番号の確認等だけで決済手段として用いられることがあるけれども、クレジットカードの真正性を確認するために電子認証処理を経てからクレジットカード決済が実行処理される場合が普通となっている。

クレジットカードとは別に、ネットワークシステムで処理される電子決済は多岐にわたっており、純粋な電子バウチャー等として利用可能な電子的決済手段がかなり広範に利用されるようになってきている。そこでは、物体としてのプラスチックカード上の磁気ストライプ部分やプラスチックカード内に埋め込まれたＩＣチップ内に記録された情報が機械装置によって処理されるのではなく、番号や符号等で示される決済情報がそのままで用いられる。[45] そのような電子バウチャーや電子プリペイドサービスの例としては、例えば、米国の Groupon や日本の WebMoney 等[46]によって提供されているネット決済サービスなどをあげることができる。

そして、ネット上でのクレジットカード決済の場合でも、実質的にはカード番号等の符号の電子的なやりとりだけで決済が完了してしまうことが多い。例えば、Amazon のサイト上でクレジットカード決済により書籍を予約・購入する場合などがその例である。また、PayPal のように、会員としてのＩＤ情報（アカウント情報）がクレジットカードやデビットカード（銀行カード）による電子決済と連動している場合もある。[47]

これら電子的な支払手段の中で、支払用カードに用いられる電磁的記録との関係では、その電磁的記録の内容である情報をフィッシングにより取得する行為や第三者に移転する行為等が問題となり得る。これらの行為については、刑法に定める支払用カード電磁的記録不正作出等の罪[48]または割賦販売法違反の罪が成立することがある。

これに対し、電子決済に用いられる情報であっても支払用カードに用いられるものでないものについては、事案にもよるが、フィッシングによる情報の無権限取得行為の中でもかなり限定された行為についてのみ、通常の電磁的記録不正作出罪（刑法一六三条の二）の成立があり得るのにとどまる。

(a) 支払用カード電磁的記録に関する罪

フィッシングとの関係で特に重要なのは、支払用カード電磁的記録不正作出準備罪（刑法一六三条の四）である。この罪は、他人の「財産上の事務処理を誤らせる目的」で実行されることを要件としている。そのため、クレジットカードの偽造等を目的とするのではなく、純粋にクレジットカード情報の無権限取得だけを目的とするフィッシングの場合には、刑法一六三条の四所定の罪が成立しないことにも留意すべきである（ただし、このような場合においても、後述の割賦販売法違反の罪が成立することがあり得る。）。

刑法一六三条の四第一項は、他人の財産上の事務処理を誤らせる目的でなされる支払用カード電磁的記録を取得する行為を処罰対象行為としている。例えば、支払用カード電磁的記録の不正作出（刑法一六三条の三第一項）を実行するためにフィッシングにより無権限で他人のクレジットカード情報を取得する行為は、まさにこの取得行為に該当することになる。この取得行為を実行した者は、三年以下の懲役又は五〇万円以下の罰金に処せられる（同法一六三条の四第一項）。未遂犯も処罰される（刑法一六三条の五）。

また、無権限で取得された支払用カード電磁的記録の情報を保管する行為は、刑法一六三条の四第二項に該当し、同条の四第一項と同じ刑に処せられる。例えば、フィッシングサイトで取得された他人のクレジットカード情報を他のサーバに伝送してその中に記録・蓄積したり、その他の電子記録媒体上に記録したりするような行為は、この支払用カード電磁的記録の情報の保管行為に該当する場合があり得る(49)。

そして、刑法一六三条の四に規定する取得行為の目的で「器械又は原料を準備」する行為については、刑法一六三条の四第三項の罪が成立する。ここでいう「器械又は原料」には物体としての器具や機械装置等だけではなく電子的なものも含まれるとするのが通説である。したがって、例えば、支払用カード電磁的記録の情報を無権限で取得し、取

得した他人の支払用カード電磁的記録の情報を用いて不正指令電磁的記録を作出する目的で、フィッシングサイトを構築し運用する行為は、この「器械又は原料を準備」に該当することがあり得る。

なお、刑法一六三条の二に定める「支払用のカード」には、取引が実行されるのと同時または取引がなされた後に決済がなされるクレジットカードやデビットカード（キャッシュカード）だけではなく、取引がなされる前に決済が実行される電子的なプリペイドカードも含まれるというのが通説である。(50)

ただし、物体としてのカードが存在し得るものであり、かつ、そのカードの作出のために用いられる情報でなければならないため、カードに記録されることがあり得ない純粋に電子的な決済手段（電子的なバウチャーや電子プリペイドサービスなど）は、ここでいう「支払用のカード」から除外されることになる。(51)

(b) 割賦販売法違反の罪

支払用カード電磁的記録不正作出等に関する刑法上の処罰条項は、あくまでも物体である支払用カードに用いられる電磁的記録の不正作出等に用いる目的で実行された行為のみに適用される。そのため、例えば、Ｗｅｂサイト上にあるネットショップ等で直接にクレジットカード情報を入力して行使することを目的とする場合のように、支払用カードの電磁的記録不正作出を目的とするのではない場合には、これらの処罰条項を適用することができない。

そこで、割賦販売法の一部改正により、他人を欺いてクレジットカード情報を取得する行為について罰則が設けられることになった（割賦販売法四二条の二第二項）。

同法同条の二第二項が定める犯罪行為は、①「正当な理由がないのに、有償で、クレジットカード番号等を提供」する行為、②「正当な理由がないのに、有償で、クレジットカード番号等」の提供を受ける行為及び③「正当な理由がないのに、有償で提供する目的で、クレジットカード番号等を保管」する行為である。この提供を受ける行為の中に

はフィッシングによる場合も含まれる。

なお、割賦販売法における「クレジットカード番号等」とは「クレジットカード等購入あっせん業者が、その業務上利用者に付与する第二条第三項第一号の番号、記号その他の符号をいう」と定義されている（割賦販売法三五条の一六第一項）。したがって、クレジットカードとして用いられるもの以外の電子的決済手段（電子バウチャー、電子プリペイドサービス等）で用いられる符号等の情報は含まれないことに留意すべきである。

(c) 罪数

フィッシングにより取得されたクレジットカード情報が電子決済手段として用いられるだけではなく、特定のサイトにアクセスするためのアカウント情報としても機能している場合、その情報は、刑法に規定する支払用カード電磁的記録であると同時に不正アクセス禁止法に定める識別符号でもあり得ることになる。

既述のとおり、支払用カード電磁的記録作出準備罪が成立するためには、支払用カード電磁的記録不正作出行為の用に供する目的という主観的構成要件を充足していることを要し、また、不正アクセス禁止法上の他人の識別符号の取得罪及び保管罪が成立するためには「不正アクセスの目的」という主観的要件の充足を要する（同法の提供罪については、「業務上その他正当な理由」がないことが要件となる。）。

ところが、ある識別符号が特定電子計算機にアクセスするための識別符号であると同時に当該特定電子計算機内において処理される電子決済（事務処理）を機能させるための符号でもある場合であって、かつ、アクセス用のカードとクレジットカードを兼ねているような支払用カードを作成した上で、それを用いて不正アクセスを実行しようとする者は、これら二種類の目的（主観的構成要件要素）を両方とも具備していると認められる場合があり得ることになる。[52] このような事例は、クレジットカードだけではなく各種電子決済手段において現実に生じ得るものであると考えられる。例え

ば、電子決済機能付の学生証カードであって、当該学生が所属する大学のコンピュータシステムにログオンする際に、電子決済に用いるのと同じカード番号等の情報を識別符合として用いることができるものなどを想定することができる。

さて、そのように支払用カード電磁的記録であると同時に識別符号でもある場合、罪数上の問題が生ずることがあり得る。例えば、そのような情報の取得行為、保管行為及び提供行為について、刑法上の支払用カード電磁的記録不正作出準備（刑法一六三条の四第一項、二項）と不正アクセス法上の他人の識別符号の取得罪（不正アクセス禁止法四条）、保管罪（同法六条）及び提供罪（同法五条）とがそれぞれ同時に成立する可能性がある。(53)

このような場合の罪数については、同一の行為で複数の罪名に触れる場合として観念的競合（刑法五四条一項）の関係にたつと理解するのが妥当と思われる。

フィッシングによって割賦販売法違反の罪が成立する場合についても、それぞれの犯罪固有の構成要件が充足される限り、同様に考えることができる。すなわち、同一の行為について、それぞれの罪の主観的構成要件要素及び客観的構成要件要素が共に充足される場合には、その行為が触れる複数の罪の間の関係は、観念的競合（刑法五四条一項）の関係にたつものと解する。

(3) 企業秘密に属する情報

フィッシングにより無権限で取得される情報が不正競争防止法に定める営業秘密に該当する場合を想像することは非常に困難ではないかと思われる。

例えば、企業の特定のサーバ等へアクセスするためのＩＤやパスワード等について「営業秘密に属する」と考える経営者は決して少なくないだろうと推測される。しかし、フィッシングを実行可能な偽装Ｗｅｂサイト（フィッシングサイト）で用いられるようなＩＤ（アカウント情報）やパスワード情報が営業秘密に属するという場合を想像する

ことは難しいし、もしあるとしても極めて例外的な事例に属するのではないかと思われる。

ただ、非常に特殊なフィッシングの場合には、営業秘密の侵害行為として理解できる場合がないわけではない。例えば、偽サイト上で偽の入力フォームのようなものが構築されており、それが真正な入力フォームであると錯誤した従業員等が営業秘密に属する情報を入力・記入してしまうといった事例を想定することは可能である。

そのような例外的な場合には、不正競争防止法違反行為として罰則の適用を検討する余地がないわけではない（不正競争防止法二一条一項一号及び二号）。

なお、前述のスピアフィッシングやＡＰＴ攻撃などによって無権限で取得したアカウント情報を悪用し、当該アカウント情報を用いてアクセスできるサイトに不正アクセスを実行した上で、そのサイト内にある営業秘密を無権限で取得するような行為は全く別の類型の犯罪行為に属する。そのような行為が「不正の利益を得る目的で、又はその保有者に損害を加える目的」で実行され、その行為が「その他保有者の管理を害する行為」に該当する場合には、別途、不正競争防止法違反の罪が成立し、一〇年以下の懲役若しくは一〇〇〇万円以下の罰金に処せられる（同法二一条一項一号）。同項一号の「その他保有者の管理を害する行為」とは、他人の営業秘密を不正取得するために保有者の営業秘密の管理を外部から害する行為のうち、財物の窃取、施設への侵入及び不正アクセス行為を除いたものを意味し、その立法趣旨としては、「今後の情報通信技術等の急速な進歩によって可能となるハイテクを用いた悪質な手口にも適切に対応できるよう、限定列挙ではない形で規定したものである」とされている(54)。

(4)　著作権のある情報

一般に、フィッシングによって無権限で取得される情報は比較的単純な符号の組み合わせのみで構成されている場合が多い。そのため、そのような符号の組み合わせに創作性を認めることは難しく、それが著作物（著作権法二条一

項一号）となることもほとんどないと考えられる。

しかしながら、例外的として、例えば、フィッシングによって無権限で取得される情報が創作性のある画像によって構成される場合またはそのような画像要素を構成部分とする符号列等の場合には、その符号列等は著作物の一種となり得る。

そして、一般に、通常電子的な送信行為の本質は、量子コンピュータ[55]による物質伝送的な処理とは異なり、送信先において送信元にあるコンテンツの複製（写像）を生成する処理であることになるから、常にコンテンツの複製処理を伴うことになる。

したがって、フィッシングによって無権限で取得されるコンテンツが著作物であるときは、当該コンテンツの複製権侵害が問題となり得る。そして、複製権侵害となる行為については、著作権法違反として著作権法に定める罰則が適用可能である（著作権法一一九条）。

3　若干の検討

以上の検討は、フィッシング行為として認識可能な社会的病理現象について、「ネットワークシステムの安全性・信頼性の確保」という情報を処理する仕組みを保護法益としてとらえる観点と「情報の安全性・信頼性の確保」というネットワークシステムで処理される対象を保護法益としてとらえる観点とを対比させるという手法に基づくものであった。換言すると、「対象の処理」と「処理の対象」という異なる視点から対比させて、フィッシング行為に対して現行の刑事法制が十分に対応しているかどうかを明らかにするための試みの一つでもある。

ところで、刑事法の体系と係る伝統的な法理論の立場を重視して考察し直してみるとすれば、刑法の体系がとって

いるように、国家法益、社会法益及び個人法益という三つのカテゴリに分けるとどういうことになるかという考察も、思考の整理上、不可欠であると思われる。[56] そこで、そのような視点から若干の検討を試みる。

まず、最も形式的な基準から分類してみると、次のようになるだろう。[57]

Ⅰ　**国家法益**

なし

Ⅱ　**社会法益**

アクセス制御機能（不正アクセス禁止法）
アプリケーション（刑法・不正指令電磁的記録罪）
電子メール（特定電子メール適正化法）
支払手段（刑法・支払用カード電磁的記録罪、割賦販売法）
企業秘密（不正競争防止法）
通信の秘密（電気通信事業法等）

Ⅲ　**個人法益**

業務の遂行（刑法・業務妨害罪）
商標権（商標法）
著作権（著作権法）

この形式的基準に基づく分類は、それ自体としては正しいと考えるが、いかにも違和感を禁じ得ないものである。その原因について考えてみると、①電子技術や通信技術が横断的・手段的なものであり、縦割りの法益分類に馴染まないものであることを無視しており、かつ、②実質的な被害または被害者を全く考慮に入れていないからであると思われる。国家、企業その他の組織、個人の別を問わず、電子技術は誰によっても利用可能なものであることから、その利用に伴う社会的病理現象の一つとしてのフィッシング等の被害もまた、国家、企業その他の組織及び個人の別を問わず、全ての利用者に生じ得ることになる。すなわち、この種のサイバー犯罪に関する限り、伝統的な意味での法益分類（国家法益、社会法益及び個人法益）は、ほとんど意味がないだけではなく、逆に、国家政策遂行上、企業経営上及び私生活の維持上、かなり有害な影響を及ぼすことがあり得るのではないかと考えられる。

そこで、試みに、上記の各法令等によって、どのような法主体が、直接的なものと間接的なものとを含め何らかの法的利益としての利害関係を有しているか否かについて検討してみると、表1のようになるだろう（もちろん、見解の相違により、異なる分類をすべしとの意見もあり得る。）。

この表1から理解できることは、情報技術と関連して生ずるサイバー犯罪は、やはり横断的なものであること、それに対し、知的財産権に関連する法益保護は主として企業の利益にかかわるものであることである。

未来の刑法典がどのようなかたちのものになるのかについては誰も予言することはできない。しかし、①情報社会の進展に伴い、現にフィッシングのようなサイバー犯罪が発生していること、そして、②サイバー犯罪は、国、組織及び個人の別とは関係なく、誰にとっても法益侵害の可能性があるという意味で、どのような立場の者にとっても重要な利害関係のある社会事象であることを正しく認識・理解することが重要である。

本論文における直接の検討対象であるフィッシングを含め、サイバー犯罪の刑事法制度全体とのかかわりに関する

正しい認識・理解を踏まえ、適正な法制度を構築・運用しなければならない。

	国			国民	
	立法	司法	行政	企業	非企業
アクセス制御機能（不正アクセス禁止法）	◎	◎	◎	◎	○
アプリケーション（刑法・不正指令電磁的記録罪）	◎	◎	◎	◎	○
電子メール（特定電子メール適正化法）	△	△	△	○	○
支払手段（刑法・支払用カード電磁的記録罪、割賦販売法）	△	△	△	◎	○
通信の秘密（電気通信事業法等）	○	○	○	○	○
企業秘密（不正競争防止法）	×	×	×	◎	×
業務の遂行（刑法・業務妨害罪）	◎	◎	◎	◎	×
商標権（商標法）	×	×	×	◎	×
著作権（著作権法）	△	△	△	○	△

表1　情報の保護に関する利害関係

（◎＝利害関係濃厚、○＝利害関係あり、△＝利害関係希薄、×＝利害関係なし）

四　海外の立法例

フィッシング行為に対して適用可能な日本国における刑事法制度の検討を踏まえ、法制度上の対比（比較法的検討）を通じて問題点の所在を明らかにするため、海外の立法例についても触れることにする。

海外の立法例をみると、「フィッシング（phishing）」を処罰対象とする立法例はほとんどない。しかし、フィッシング行為の本質部分は、他人を欺罔して錯誤に陥らせ、その錯誤に乗じて、無権限で、他人の個人識別情報等を取得するということにある。法文中において明確に「フィッシング（phishing）」という語を用いていなくても、実質的な意味でフィッシング行為を処罰する目的で制定された刑罰法令は存在する。

例えば、英米法系の国々では、個人識別情報の無権限取得を意味する「identification theft」[58]という語を用い、フィッシング行為とほぼ同じ実質を有する行為を処罰している。

本論文では、フィッシングを含むサイバー犯罪の学術研究及び日本国における今後の立法論及び法政策の形成において比較的高い学術的価値及び実務的価値を含むものと思われるドイツ、米国及びカナダの立法例を紹介することにする。

1　ドイツ

ドイツ刑法中の犯罪の中で本論文のテーマであるフィッシングとの関係で重要な条項は、二〇二条ａ（通信傍受罪）、二〇二条ｂ（データ傍受罪）及び二〇二条ｃ（通信傍受及びデータ傍受の準備罪）の三つである。ドイツ刑法の条文

は、ドイツ連邦法務省のサイト上[59]において、独文及び英文の二種類の形式で公開されている。[60]

以下、ドイツ刑法二〇二条a（通信傍受罪）、二〇二条b（データ傍受罪）及び二〇二条c（通信傍受及びデータ傍受の準備罪）の私訳（直訳）である。

第二〇二条a　通信傍受罪

(1)　自己に属するものではなく、かつ、無権限アクセスに対して特別な保護のされているデータを、自己又は第三者のために無権限で取得した者は、三年以下の自由刑又は罰金に処する。

(2)　第一項のデータは、電気的、磁気的その他直接に知覚できない方式で記録又は送信されるもののみを意味する。

［原文］

§ 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

第二〇二条b　データ傍受罪

非公開のデータ伝送[61]もしくはデータ処理装置からの電磁放射[62]から、技術的手段を用いて、自己に属しない特定のデータ（第二〇二条a第二項）を自己又は第三者のために違法[63]に傍受した者は、他の条項に基づきより重い刑に処せられる場合を除き、二年以下の自由刑又は罰金に処する。

［原文］

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2.) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

第二〇二条ｃ 通信傍受及びデータ傍受の準備罪

⑴ 第二〇二条aもしくは第二〇二条bの犯罪行為を実行する目的で、次のものを製造し、自己又は第三者のために取得し、譲渡し、第三者に提供し、頒布その他の方法で利用可能にした者は、一年以下の自由刑又は罰金に処する。

1. データ（第二〇二条a第二項）にアクセスすることができるようにするためのパスワードその他のセキュリティコード、又は
2. その行為を実行するためのコンピュータプログラム

(2)　第一四九条二項及び三項を準用する。

［原文］

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

2　米国

米国では、個人識別情報の無権限取得行為（ID Theft）を処罰する連邦法としてアメリカ合衆国連邦法律集一八款一〇二八条（18 USC §1028）[64]が制定されているほか、合衆国連邦を構成するほぼ全ての州において何らかの形でこの種の行為を処罰する州法（州の犯罪法または刑法）が制定されるに至っている[65]。これらの法令を適用して処罰した事例は既に多数存在しており、その中でも社会的に注目を集めた事件については、連邦警察（ＦＢＩ）のサイトなどで事件の概要等の事実が公表されている[66]。

一般に、米国の刑事法及び犯罪学においては、「ID Theft」とは社会保険番号の無権限取得行為のみではなく、他の種類の番号や記号情報等を含め、「他人の識別情報」を広く含むものとして理解されており、多種多様な個人識別情報を保護の対象として「ID Theft」の概念が形成されてきた。フィッシングとの関係において特に重要なのは、連邦法一〇二八条(c)項(3)である。

以下、連邦法一〇二八条の抄訳（直訳）である。(67)

第一〇二八条　個人識別文書及び個人識別情報と関連する詐欺及びこれに類する行為

(a) 本条(c)項に示す場合において、以下の犯罪行為を実行した者は、本条(b)項の規定に従い処罰される。

(1) 認識して、(68)適法な権限なく、個人識別文書または偽造の個人識別文書を作成した者：

(2) 認識して、当該文書が盗まれたものであること、もしくは当該文書が偽造の個人識別文書であることを認識して、個人識別文書もしくは偽造の個人識別文書を送付した者：

(3) 認識して、違法に使用する目的もしくは違法に送付する目的で、五通以上の個人識別文書（所持者が使用するために当該文書が適法に発行されたものである場合を除く。）を所持した者：

(4) 認識して、合衆国を欺くために当該文書を使用する目的で、個人識別文書（所持者が使用するために当該文書が適法に発行されたものである場合を除く。）もしくは偽造の個人識別文書を所持した者：

(5) 認識して、当該文書作成器具を偽造の個人識別文書の作成もしくは偽造のために用いられる他の文書作成器具の作成に用いる目的で、文書作成器具を作成、送付または所持した者：

(6) 認識して、当該個人識別文書が盗まれたものもしくは当該個人識別文書が適法な権限なく作成されたもの

であることを知りつつ、合衆国の個人識別文書である個人識別文書または合衆国の個人識別文書のように見える個人識別文書を所持した者：または、

(7)　認識して、連邦法上の犯罪を構成する違法行為または適用可能な州法もしくは自治体法令に基づき重罪を構成する違法行為を実行、幇助もしくは教唆する目的で、適法な権限なく、他人の個人識別手段を移転もしくは使用した者。

(b)　本条(a)項の犯罪行為に対する処罰は次のとおりである。

(1)　(3)及び(4)に規定する場合を除き、犯罪行為が以下のとおりである場合には、本款に規定する罰金もしくは一五年以下の拘禁刑またはこれら刑の併科とする。

(A)　以下のものであるもしくは以下のものように見える個人識別文書もしくは偽造の個人識別文書の作成または送付の場合：

(i)　合衆国によって発行された個人識別文書もしくは合衆国の権限に基づき発行された個人識別文書：または、

(ii)　出生証明書、運転免許証もしくは個人識別カード：

(B)　五通を超える個人識別文書もしくは偽造の個人識別文書の作成または送付の場合：

(C)　前項(5)の犯罪行為の場合：または、

(D)　前項(7)の犯罪行為の場合であって、一以上の個人識別手段の送付もしくは使用がなされた場合であり、かつ、その犯罪行為の結果として、犯罪行為を遂行した者が過去一年間に合計一〇〇〇ドル以上相当の何かを得た場合。

(2) (3)及び(4)に規定する場合を除き、犯罪行為が以下のとおりである場合には、本款に規定する罰金もしくは三年以下の拘禁刑またはこれら刑の併科とする。

(A) 個人識別手段、個人識別情報もしくは偽造の個人識別情報の上記以外の所持、送付または使用：または、

(B) 前項(3)もしくは(7)の犯罪行為：

(3) 犯罪行為が以下のとおりに実行された場合には、本款に規定する罰金もしくは二〇年以下の拘禁刑またはこれら刑の併科とする。

(A) （九二九条(a)項(2)に規定する）麻薬密輸犯罪を容易にするため：

(B) （九二四条(c)項(3)に規定する）暴力犯罪との関連で：または、

(C) 本条に基づく前科による拘禁刑が終了した後に。

(4) （本款の二三三一条(1)に定義する）国際的テロリズムの犯罪行為を容易にするために犯罪行為が実行された場合には、本款に規定する罰金もしくは二五年以下の拘禁刑またはこれら刑の併科とする。

(5) (a)項のどの犯罪行為の場合についても、犯罪行為に使用された個人財産もしくは使用するつもりであった個人財産を、合衆国が没収する。並びに、

(6) これら以外の場合については、本款に規定する罰金もしくは一年以下の拘禁刑またはこれら刑の併科とする。

(c) 本条(a)項に規定する場合とは、次のような場合のことである。

(1) 個人識別文書もしくは偽造の個人識別文書が合衆国の権限に基づいて発行されたもの、もしくはその権限に基づいて発行されたもののように見える場合、または、個人識別文書もしくは偽造の個人識別文書の作成のために設計され、もしくはそれに適する文書作成器具：

(2)　当該違法行為が本条(a)項(4)の犯罪行為である場合：または、

(3)　次のいずれかの場合：

(A)　電子的な方法による文書の送付を含め、本条によって禁止される作成、送付もしくは使用が州際取引もしくは国際取引においてなされ、またはこれらの取引に悪影響を及ぼす場合：または、

(B)　個人識別手段、個人識別文書、偽造の個人識別文書もしくは文書作成器具が、本条によって禁止される作成、送付もしくは使用の際にメールにより送信される場合。

(d)　本条においては、

(1)　「文書作成器具」という用語は、個人識別文書、偽造の個人識別文書その他の文書作成器具を作成するために特に構成され、もしくはそのために主に使用される器具、印章、雛形、コンピュータファイル、コンピュータディスク、電子機器類、またはコンピュータハードウェアもしくはソフトウェアを意味する。

(2)　「個人識別文書」という用語は、特定の個人に関する情報を確認する際、個人識別をするために用いられまたは個人識別のためのものとして一般に承認されている文書形態の一つであって、合衆国連邦政府、州、州政府の部局、外国政府、外国政府の部局、国際機関または準国際機関によって、またはその権限に基づいて作成または発行される文書を意味する。

(3)　「偽造の個人識別情報」という用語は、個人識別をするために用いられまたは個人識別のためのものとして一般に承認されている文書形態の一つであって、次のものを意味する。

(A)　政府機関の権限に基づいて発行されるものではないものであり：かつ、

(B)　合衆国連邦政府、州、州政府の部局、外国政府、外国政府の部局、国際機関または準国際機関によって、

［原文］

またはその権限に基づいて発行されたように見えるもの。

(4)「個人識別手段」という用語は、特定の個人を識別するために、単独でまたは他の情報と一緒に用いられる名前もしくは番号を意味し、以下のものを含む。

(A) 名前、社会保険番号、生年月日、州または政府が公式に発行した運転免許証もしくは識別番号、外国人登録番号、政府のパスポート番号、労働者番号もしくは納税者番号：

(B) 指紋、声紋、網膜もしくは虹彩の画像、その他の唯一無二な身体的特徴といった固有の生体データ：

(C) 唯一無二の電子的な識別番号、アドレスもしくはルーティング・コード：または、

(D) （一〇二九条(e)項に規定する）通信識別情報もしくはアクセス装置。

(5)「個人識別カード」という用語とは、個人識別のみを目的として州政府または地方自治体政府が発行する個人識別文書を意味する：

(6)「作成」という用語は、改変、証明または組み立てを含む：

(7)「送付」という用語は、個人識別文書、偽造の個人識別文書または文書作成器具を選択すること及び個人識別文書、偽造の個人識別文書または文書作成器具を第三者が利用可能なオンライン上の場所に置くこともしくはそのように指図することを含む：並びに、

(8)「州」という用語は、合衆国の全ての州、コロンビア特別区、プエルトリコ、合衆国のその他の保護領、領地及び領土を意味する。

Sec. 1028. - Fraud and related activity in connection with identification documents and information

(a) Whoever, in a circumstance described in subsection (c) of this section -

(1) knowingly and without lawful authority produces an identification document or a false identification document;

(2) knowingly transfers an identification document or a false identification document knowing that such document was stolen or produced without lawful authority;

(3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor) or false identification documents;

(4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor) or a false identification document, with the intent such document be used to defraud the United States;

(5) knowingly produces, transfers, or possesses a document-making implement with the intent such document-making implement will be used in the production of a false identification document or another document-making implement which will be so used;

(6) knowingly possesses an identification document that is or appears to be an identification document of the United States which is stolen or produced without lawful authority knowing that such document was stolen or produced without such authority; or

(7) knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that

constitutes a felony under any applicable State or local law;

shall be punished as provided in subsection (b) of this section.

(b) The punishment for an offense under subsection (a) of this section is -

(1) except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than 15 years, or both, if the offense is -

(A) the production or transfer of an identification document or false identification document that is or appears to be -

(i) an identification document issued by or under the authority of the United States; or

(ii) a birth certificate, or a driver's license or personal identification card;

(B) the production or transfer of more than five identification documents or false identification documents;

(C) an offense under paragraph (5) of such subsection; or

(D) an offense under paragraph (7) of such subsection that involves the transfer or use of 1 or more means of identification if, as a result of the offense, any individual committing the offense obtains anything of value aggregating $1,000 or more during any 1-year period;

(2) except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than three years, or both, if the offense is -

(A) any other production, transfer, or use of a means of identification, an identification document, or a false identification document; or

(B) an offense under paragraph (3) or (7) of such subsection;

(3) a fine under this title or imprisonment for not more than 20 years, or both, if the offense is committed -

(A) to facilitate a drug trafficking crime (as defined in section 929(a)(2));

(B) in connection with a crime of violence (as defined in section 924(c)(3)); or

(C) after a prior conviction under this section becomes final;

(4) a fine under this title or imprisonment for not more than 25 years, or both, if the offense is committed to facilitate an act of international terrorism (as defined in section 2331(1) of this title);

(5) in the case of any offense under subsection (a), forfeiture to the United States of any personal property used or intended to be used to commit the offense; and

(6) a fine under this title or imprisonment for not more than one year, or both, in any other case.

(c) The circumstance referred to in subsection (a) of this section is that -

(1) the identification document or false identification document is or appears to be issued by or under the authority of the United States or the document-making implement is designed or suited for making such an identification document or false identification document;

(2) the offense is an offense under subsection (a)(4) of this section; or

(3) either -

(A) the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means; or

(B) the means of identification, identification document, false identification document, or document-making implement is transported in the mail in the course of the production, transfer, possession, or use prohibited by this section.

(d) In this section -

(1) the term "document-making implement" means any implement, impression, template, computer file, computer disc, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement;

(2) the term "identification document" means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals;

(3) the term "false identification document" means a document of a type intended or commonly accepted for the purposes of identification of individuals that -

(A) is not issued by or under the authority of a governmental entity; and

(B) appears to be issued by or under the authority of the United States Government, a State, a political subdivision of a State, a foreign government, a political subdivision of a foreign government, or an international governmental or quasi-governmental organization;

(4) the term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any -

(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device (as defined in section 1029(e));

(5) the term "personal identification card" means an identification document issued by a State or local government solely for the purpose of identification;

(6) the term "produce" includes alter, authenticate, or assemble;

(7) the term "transfer" includes selecting an identification document, false identification document, or document-making implement and placing or directing the placement of such identification document, false identification document, or document-making implement on an online location where it is available to others; and

(8) the term "State" includes any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession, or territory of the United States.

3 カナダ

カナダの犯罪法二八章（Criminal Code Chapter 28）は、ＩＤ窃盗及びＩＤ詐欺（Identity Theft and Identity Fraud）[69]を犯罪として規定している。ここでいう「窃盗」及び「詐欺」も財物の窃取や詐取を意味するのではなく、あくまでも個人識別情報の無権限取得のことを意味する。同条は、特に明記しているわけではないが、当然に電子的な手段による個人識別情報の無権限取得の場合を含むものと解釈されるので、フィッシングについても適用があると解される。[70]

以下、カナダ犯罪法二八章の抄訳（直訳）である。

四〇二条一　「識別情報」の定義

四〇二条二及び四〇三条においては、「識別情報」とは、個人を識別するため、もしくは個人を識別しようとするために単独でもしくは他の情報と組み合わせて一般に使用される情報形態の一つとしての情報（生体情報及び生理情報を含む。）であって、指紋、声紋、網膜画像、虹彩画像、ＤＮＡ型、名前、住所、生年月日、手書きの署名、電子署名、利用者名、クレジットカード番号、デビットカード番号、金融機関アカウント番号、社会保険番号、健康保険番号、運転免許証番号またはパスワードを含む。

［原文］

402.1 Definition of “identity information”

For the purposes of sections 402.2 and 403, “identity information” means any information - including biological or physiological information - of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, driver’s licence number or password.

四〇二条二　ＩＤ窃盗

(1)　当該犯罪行為の構成要素の一部として詐欺、欺瞞もしくは虚偽を含む正式裁判で起訴可能な犯罪行為を実行するために当該情報を使用する目的があるという合理的な推定を生じさせ得る状況において、認識して、他人の識別情報を取得または所持する者は、犯罪行為を実行する者である。(71)

(2)　当該犯罪行為の構成要素の一部として詐欺、欺瞞もしくは虚偽を含む正式裁判で起訴可能な犯罪行為を実行するために当該情報が使用されるものかどうかに関して認識しつつ、もしくはそのことに関して留意せずに、他人の識別情報を送付し、使用可能にし、配布し、販売し、もしくは販売目的で提示する者、または、これらの行為をする目的で他人の識別情報を自己の管理下に入れる者は、犯罪行為を実行する者である。(72)

(3)　［省略］

(4)　本条(1)または(2)の犯罪行為の容疑で起訴される被告人は、当該犯罪行為が実行された場所であるとされている場所、被告人が発見された場所もしくは被告人が勾留されている場所で当該犯罪行為に係る公判を遂行する管轄

権を有する裁判所によって、公判を受け及び処罰される。しかしながら、当該犯罪行為が州外で実行されたものであるとの申立てがある場合には、当該州の州務長官の事前の承諾を得ないで当該犯罪に係る刑事訴訟手続をその州内において開始することができない。(73)

(5) 本条(1)または(2)の犯罪行為を実行する者は、

(a) 正式裁判で起訴可能な犯罪行為として有罪であり、五年以下の期間内で拘禁刑に処せられ、または、

(b) 略式裁判に基づき処罰可能な犯罪行為として有罪である。

［原文］

402.2 Identity theft

(1) Everyone commits an offence who knowingly obtains or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.

(2) Everyone commits an offence who transmits, makes available, distributes, sells or offers for sale another person's identity information, or has it in their possession for any of those purposes, knowing that or being reckless as to whether the information will be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.

(3) [omitted]

(4) An accused who is charged with an offence under subsection (1) or (2) may be tried and punished by any court

having jurisdiction to try that offence in the place where the offence is alleged to have been committed or in the place where the accused is found, is arrested or is in custody. However, no proceeding in respect of the offence shall be commenced in a province without the consent of the Attorney General of that province if the offence is alleged to have been committed outside that province.

(5) Everyone who commits an offence under subsection (1) or (2)

(a) is guilty of an indictable offence and liable to imprisonment for a term of not more than five years; or

(b) is guilty of an offence punishable on summary conviction.

五　まとめ

以上で本論文における検討を終える。

本論文ではフィッシングを素材として日本国の法制及び海外の代表的な関連法制について比較法的な検討を加え、若干の私見を述べた。

本論文において直接の検討対象となっているのはフィッシングである。フィッシングの手口（電子的または非電子的な技法）は日々変化しており、より巧妙な手口がどんどん考案されている。また、技術的手段に関しては、各種の電子的なツールがインターネット上の闇サイトなどを介して流通している現状からすると、かなり厄介な時代になったものだとの感を禁ずることができない。

フィッシングに限らず、サイバー犯罪に対して直接的な防御となり得るのは情報セキュリティのマネジメント及び

技法である。法は、あくまでも事後的な処罰や損害賠償等を準備し、あるいはそれを強制することによって、加害者（犯人）を社会から隔離すると同時に特別予防的な効果（再犯の防止等）を期待し、また、将来の加害者に対して一般予防的な抑止効果を期待するというかたちで社会に働きかけることしかできない。

しかし、それでもなお、法というものが国家によって強制可能な非常に強力な統制手段の一つであることは明らかである。そのような統制手段によって保護されるべき法益主体が存在するのに法による保護が欠けている場合には立法によって補わなければならないし、また、統制の過剰の弊害がある場合にはその運用を再検討しなければならない。

本論文では、ごく少数の立法例について簡単な比較検討しか加えることができなかったが、今後、この分野において、様々な立場の研究者や実務家らの手によって、より良い研究成果が生み出されることを期待したい。(74)

注

（1） サイバー犯罪に関する条約（平成二四年条約第七号）は、その起草当時においてはサイバー犯罪に関する最新の内容を盛り込むものとされていた。しかし、同条約においても、純粋な「情報」の無権限取得または違法取得に関する条項は存在しない。そのため、EUの関連委員会等において見直し作業が進められている。

（2） 天正一〇年（一五八二年）、織田信長は、明智光秀の謀反によって本能寺においてその生涯を終えた。その後、明智光秀は、期待できる戦国大名らに対し、加勢を依頼する内容の密書を送った。ところが、明智光秀の密書を届けるため各地に派遣された者の中で毛利氏に密書を届けるべしとの命を受けた者は、毛利側の武将清水宗治が守る備中高松城の攻城戦のため陣を構えていた羽柴秀吉（後の豊臣秀吉）の陣場に迷い込み、明智光秀から毛利氏に宛てた密書を羽柴側に奪われることとなってしまった。羽柴秀吉は、その密書によって信長死去の事実をいち早く知ることとなり、その結果、他の競争相手（織田信長の後継候補となる戦国武将）よりも早く京に向けて駆け戻ることができ、明智光秀を倒すことができたとされている。豊臣秀吉の「中国大返し」と通称されるこれらの出来事が史実であるのか後世の作り話であるのかは必ずしも判然とせず、諸説ある。また、それが史実であったか否かを現代において確定することは非常に難しい。しかし、仮にそれが史実であったとした場合、羽柴秀吉にとって重要だったのは「信長死去」という事実に関する「情報」そのものであったのにもかかわらず、その情報を

取得するためには「密書」という「物体」を奪取する行為が不可欠だったということに着目すべきである。このことは、一般に、「情報」を得るためには、その情報を記録した物体を取得することが重要であったということを意味している。同様に、ある「情報」を得るために特定の者を拘束し、拷問を加えて自白させるという場合においても、その情報を記憶している物理的存在としての「人間」を確保することが必須となる。例えば、豊臣秀吉の「中国大返し」の場合、仮に羽柴側の陣に迷い込んだ者が密書を携行しておらず、口伝する役割を担っていたというのが史実であったと仮定した場合、拷問、脅迫、誘惑または説得などによって自白させることが必要であったと考えられる。このような場合においても、物体である密書から情報を得るプロセスと基本的には同様である。異なる要素としては、情報を記録している記録媒体が紙などの物体であるか人間の生体脳であるかの相違しかない。そして、人間の生体脳は物体の一種である。なお、正確には、自白の強要の場合には、自白者自身が脳内に記録された情報を解読し音声信号に変換して伝達する処理を行うことになる。しかし、その場合でも、伝達された音声信号を受信して情報内容を解釈・理解するのは拷問を加えて自白させた者である。これは、生体脳以外の物体に記録された情報の場合であっても、暗号化された文書の解読の場合になされるプロセスと非常に良く似ている。

（3）　「情報財」を定義することは必ずしも容易なことではない。本論文中では、通常の経済取引の対象としての「財」となり得る経済財をもって「情報財」であると定義することにする。これは、暫定的な定義であり、法的概念を含めたものとしての「情報財」としては、より正確かつ詳細な検討を要する。例えば、経済産業省「電子商取引及び情報財取引等に関する準則」においては、電気通信回線を介した「電子的な役務提供」または「電子的なコンテンツ提供」などを指すものとして「情報財」の概念が用いられている。これらの点については、更に調査・研究を深めた上で、別稿によって改めて論じたいと考える。

（4）　サイバー犯罪の概要については、夏井高人監修『ＩＴビジネス法入門』（Ｔａｃ出版、二〇一〇）一六八頁以下及び夏井高人「サイバー犯罪の研究（一）―DoS 攻撃（DDoS 攻撃）に関する比較法的検討―」法律論叢八五巻一号一九七頁以下で述べたとおりである。

（5）　フィッシングと密接な関係を有する通信傍受に適用される日本国法に関しては、別稿（「サイバー犯罪の研究㈢」法律論叢八五巻六号）で詳しく述べる。

（6）　フィッシング対策協議会は、フィッシング（phishing）について、「実在する組織を偽装した電子メールによって、ユーザネーム、パスワード、アカウントＩＤ、ＡＴＭの暗証番号、クレジットカード番号といった個人情報を、金融機関等の信頼できる団体に成り済まして打ち明けるように誘い込むこと」と定義している（フィッシング対策協議会『フィッシング対策ガイド

ライン二〇一一年度版』一頁）。

http://www.antiphishing.jp/report/pdf/antiphishing_ guide.pdf［二〇一二年一〇月一九日確認］

（7） 荒金陽助・間形文彦・柴田賢介・塩野入理・金井　敦「フィッシング詐欺の状況と対策に関する考察」情報処理学会研究報告 2006–EIP–31(5) 三三頁（二〇〇六）、荒金陽助・塩野入理・金井　敦「フィッシング詐欺によるブランドへの影響に関する考察」情報処理学会研究報告 2007–EIP–36(2) 五頁（二〇〇七）、柴田賢介・神谷　造・佐野和利・荒金陽助・塩野入理「迷惑メールにおける誘導手法に関する一考察」情報処理学会研究報告 2007–CSEC–38(47) 三二六頁（二〇〇七）、荒金陽助・柴田賢介・佐野和利・塩野入理・金井　敦「携帯電話に対するフィッシング詐欺の可能性と対策について（携帯端末、モバイルアプリケーション、モバイルコンピューティング）」情報処理学会研究報告 2007–MBL–41(14) 六七頁（二〇〇七）など

（8） フィッシング対策協議会ガイドライン策定ワーキンググループ『フィッシングレポート 2012―新たな脅威の動向とそれに向けた対策と課題―』（二〇一二年六月）一頁

（9） Targeted Phishing, Cisco White Paper, 2012

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10154/ironport_ targeted_ phishing.pdf［二〇一二年一〇月二〇日確認］

（10） 内閣官房情報セキュリティセンター（ＮＩＳＣ）『わが国の重要インフラ防護への取組み』（二〇一二年二月二三日）

http://www.ipa.go.jp/security/event/2012/cip_ sympo/documents/lecture01.pdf［二〇一二年一〇月一九日確認］

（11） 独立行政法人情報処理推進機構（ＩＰＡ）は、ＡＰＴ攻撃について、「ソフトウェアの脆弱性を悪用し、複数の既存攻撃を組合せ、ソーシャルエンジニアリングにより特定企業や個人をねらい、対応が難しく執拗なサイバー攻撃」と定義している。ＩＰＡテクニカルウォッチ『新しいタイプの攻撃』に関するレポート ～Stuxnet（スタックスネット）等の新しいサイバー攻撃手法の出現～

http://www.ipa.go.jp/about/technicalwatch/20101217.html［二〇一二年一〇月一九日確認］

（12） 「targeted phishing」と呼ぶ例もある。例えば，M. Sikorski & A. Honing, Practical Malware Analysis, no starch press, p.299 など。

（13） Report on Phishing - A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States-, Binational Working Group on Cross-Border Mass Marketing Fraud, October

2006, p.10

(14) Uri Rivner, Anatomy of an Attack
http://blogs.rsa.com/rivner/anatomy-of-an-attack/［二〇一一年一〇月一九日確認］
Avivah Litan, RSA SecurID attack details unveiled - lessons learned
http://blogs.gartner.com/avivah-litan/2011/04/01/rsa-securid-attack-details-unveiled-they-should-have-known-better/［二〇一一年一〇月一九日確認］

(15) Japan, US Defense Industries Among Targeted Entities in Latest Attack
http://blog.trendmicro.com/trendlabs-security-intelligence/japan-us-defense-industries-among-targeted-entities-in-latest-attack/［二〇一一年一〇月一九日確認］

(16) 最新情報は、フィッシング対策協議会のＷｅｂサイト（http://www.antiphishing.jp/）上で提供されている。

(17) 警察庁「サイバーインテリジェンスをめぐる情勢」焦点二八〇号（二〇一一年三月）三頁

(18) 岡村久道『情報セキュリティの法律（改訂版）』（商事法務、二〇一一）一五三頁

(19) Fraud Watch International, What is Phishing?
http://www.fraudwatchinternational.com/phishing-fraud/phishing-home/［二〇一一年一〇月一九日確認］
Mano Paul, Phishing: Electronic Social Engineering
http://www.certmag.com/read.php?in=3594［二〇一一年一〇月一九日確認］

(20) Ken Dunham, Phishing Isn't So Sophisticated: Scary!
http://www.infosectoday.com/Articles/Phishing.pdf［二〇一一年一〇月一九日確認］

(21) Phishing (Password Harvesting Fishing)
http://unaclibre.org/unac/index2.php?option=com_ content&do_ pdf=1&id=4127［二〇一一年一〇月一九日確認］

(22) 「Social phishing」と呼ぶ例もあるが、実質的意味は変わらない。例えば、R.F. Smallwood, Safeguarding Critical e-Document, Wiley, 2012, p.61 など。

(23) 前掲『フィッシング対策ガイドライン』二頁以下では安易に「フィッシング詐欺」という用語を用いている部分があるが、正確ではないし誤解を招く危険性があるので、用語例については専門の法律家の意見を聴いて検討した上で、早急に改訂すべきだ

と考える。

（24） 不正アクセス対策法制研究会編著『逐条不正アクセス行為の禁止等に関する法律（補訂第二版）』（立花書房、二〇〇八）二〇頁以下、前掲岡村『情報セキュリティの法律（改訂版）』一三一頁以下など

（25） 警察庁『不正アクセス禁止法改正の概要』中の「不正アクセス禁止法の改正について」の項

（26） このように本体となる行為（不正アクセス行為）のみならず、関連する周辺行為を網羅的に処罰対象とする立法様式は、後述する支払用カード電磁的記録不正作出等の罪における立法様式と類似するものである。

（27） 同法四条の「取得」行為にはフィッシングによる取得の場合を含むものの、フィッシング以外の手段による場合も広く処罰対象行為としていること、それに対し、同法七条は典型的なフィッシングの場合を想定した条項であることを重視すると、同法七条の要求罪と同法四条の取得罪との関係は手段・結果の関係にあり牽連犯（刑法五四条一項）の関係にたつのではなく、別罪として併合罪（刑法四五条）の関係になるとも考えられる。この罪数問題と比較的似た関係にある不正指令電磁的記録準備罪の取得、保管及び提供の罪数関係について、通説は牽連犯説を採用しているから（脚注（53）参照）、これと同様に理解するとすれば、牽連犯の関係にたつと解することになろう。

（28） 現実に生じている識別符号等の行使（不正アクセスの実行）の例の中には取得者自身が行使する場合もあるけれども、大量に取得した者が闇市場においてそれを売りさばいて金銭的利益をあげ、闇市場でその識別符号を入手した者がそれを行使（不正アクセスを実行）するという例が非常に多い。このようなインターネットの暗黒面（無権限で取得された識別情報等の闇市場における流通実態）を重視するとすれば、牽連犯（刑法五四条一項）ではなく併合罪（刑法四五条）の関係になるとも考えられる。ここでも不正指令電磁的記録準備罪の取得、保管及び提供の罪数に関して通説は牽連犯説を採用していること（脚注（53）参照）を重視するとすれば、牽連犯の関係にたつと解することになろう。

（29） 最判平成一九年八月八日・刑集六一巻五号五七六頁は、不正アクセス罪と私電磁的記録不正作出罪との罪数関係について、「犯罪の通常の形態として手段又は結果の関係にあるものとは認められず、牽連犯の関係にはないと解するのが相当であるから、本件につき両者を併合罪の関係にあるものとして処断した原判断は相当である」と判示している。

（30） 前掲注（13）

（31） Robert M. Slade, Software Forensics - Collecting Evidence from the Scene of a Digital Crime-, McGraw-Hill, 2004, pp.91–112

（32）　ＤＮＳサーバ内の記録及びその真正性の電子証明書を発行するＣＡのサイト内の記録が無権限で書き換えられた場合、ブラウザの安全性がいかに高く、ＩＰアドレスの真正性を確認する認証機能が充実している場合であって、そもそも真正なＩＰアドレスであることの電子証明書が偽装されてしまっていることから、偽サイトへと誘導されてしまうことがあり得る。現実に発生した事件としては、二〇一一年九月、オランダのＣＡである DigiNotar が攻撃を受けて業務遂行不可能となり破産した後、同年一一月、同国におけるＣＡ業務を引き継いだはずのＫＰＮが同様に攻撃を受けたという事件がある。このような場合には、インターネット上の電子認証の全てを信頼することができない状態に陥ることがあり得る。

‘Hacked server’ claims another certificate authority casualty, ZDNet, November 6, 2011 http://www.zdnet.com/blog/london/-8216hacked-server-claims-another-certificate-authority-casualty/596［二〇一二年一〇月一九日確認］

DigiNotar Hacked Out Of Business, dark READING, Sep 20, 2011 http://www.darkreading.com/authentication/167901072/security/attacks-breaches/231601790/diginotar-hacked-out-of-business.html［二〇一二年一〇月一九日確認］

（33）　フィッシング実行者に利用されることになった原因について、ＤＮＳサーバの運用者に過失が認められる場合、当該ＤＮＳサーバの運用者がフィッシングの直接の被害者に対して不法行為（民法七〇九条）に基づく損害賠償責任を負うことがあり得ることは別問題である。

（34）　http://www.facebook.com/［二〇一二年一〇月一九日確認］

（35）　http://www.linkedin.com/［二〇一二年一〇月一九日確認］

（36）　https://plus.google.com/［二〇一二年一〇月一九日確認］

（37）　立法者は、刑法一六八条の二第一項一号の「電磁的記録」は機械語コードを意味し、同項二号の「記録」はそのソースコードを意味するものと理解していたものと推定される。例えば、西田典之『刑法各論（第六版）』（弘文堂、二〇一二）三九一頁にはそのような理解が示されているし、前田雅英『刑法各論講義（第五版）』（東京大学出版会、二〇一一）五五七頁も同旨である。しかし、今日、Java のようなソースコードベースで機能するコンピュータプログラムが普通に存在する。また、ＸＭＬなどのマークアップ言語で書かれた文書は、テキストでありながらコンピュータプログラムとしても機能する。各種スクリプト言語で書かれたテキストでも同様のものがあり、要するに、ソースコードでありながら実行プログラムでもあるものが多数存在す

る。このような事実を考慮に入れると、包括して同条の二第一項一号及び二号の電磁的記録に該当すると理解すべき電磁的記録が存在することに留意すべきである。なお、同書三八一頁には、電磁的記録不正作出罪（刑法一六八条の二）に規定する電磁的記録の意義について、「プログラムは、コンピュータに対するコマンドの組み合わせにすぎないから、本条にいう電磁的記録にはあたらない」としているが、前提としている事実認識がかなり古い時代のコンピュータプログラムの印象に支配されているものと思われ、正確性を欠いている。正しくは、コンピュータプログラムの中にはコマンドのみならず様々なテキストが含まれており、そうでなければコンピュータプログラムとして機能しない（古いプログラム言語 FORTRAN で書かれた最も単純な数値計算プログラムでさえ、コマンドのみではコンピュータプログラムとして全く機能しない。アセンブラプログラムの場合でさえそうであり、引数なしには何も機能しない。）。

（38）前掲『フィッシング対策ガイドライン』一頁

（39）悪ふざけで偽サイトを構築した場合には、軽犯罪法一条三二号の「他人の業務に対して悪戯などでこれを妨害した者」に該当し得ることがある。フィッシングは、情報の無権限取得を目的とする行為であって、悪ふざけを目的とする行為ではないので、フィッシングについて軽犯罪法違反の罪が成立する事例は想定し難い。

（40）電子計算機損壊等業務妨害罪が一部改正され、未遂罪も処罰されることとなった（刑法二三四条の二第二項）。このこととの関係で、業務妨害罪の罪質に関する議論が大きな影響を受けていることになることは、前掲夏井「サイバー犯罪の研究（一）」二一〇頁で触れた。

（41）フィッシング行為やスパイウェアの実行行為などのように、被害者自身を道具とする間接正犯的な行為であり、かつ、被害者以外には加害者しか通信当事者が存在しないという類型の出来事について、そもそも「通信の秘密」に関する伝統的理解をそのまま適用してよいかどうかについては真剣に再検討すべき余地がある。このような場合、被害者は加害者の道具として機能していることから、実質的には、①単純に被害者の機密領域に侵入しているのであり、かつ、②その侵入の手段として通信技術を悪用しているだけであると認識することが可能である。ここでいう機密領域の保有主体が企業である場合には、その機密領域内に存在する情報は営業秘密であり得る。しかし、その機密領域の保有主体が個人（非企業）である場合には、単なる私的領域への侵入が存在するだけということになるだろう。このように通信技術を悪用し、被害者自身を道具として操作する方法によりその被害者の機密領域にある情報を取得する行為は、「適正な通信に対する干渉」という伝統的な意味での通信の秘密に対する侵害行為とは本質的に異なる「通信の濫用による干渉」という新たな通信の秘密侵害類型の存在を認識可能とする

ものである。ただし、現行の電気通信事業法等の通信関連法令に定める罰則の適用という場面では、慎重な対応が求められる。なぜならば、現行の通信関連法令は、伝統的な意味での「通信の秘密」のみを前提にして構築されているのであり、罰則もまた同じであることから、そのような基本構造の相違を無視し、現行の罰則の規定のままで法解釈の変更のみに基づいて罰則を適用することは、罪刑法定主義の観点から問題なしとしないからである。基本的には立法的対応が必要となるものと思われる。

（42）　前掲夏井『ＩＴビジネス法入門』二四〇～二四六頁、前掲岡村『情報セキュリティの法律（改訂版）』一一五頁～一一九頁。

（43）　日本の刑法とドイツの刑法を比較してみると、日本の刑法では、第一三章（秘密を侵す罪）の中に信書開封罪（刑法一三三条）及び秘密開示罪（同一三四条）の二つの罪が規定されているのにとどまるのに対し、ドイツ刑法では、第一五章（個人の生活領域及び秘密領域の侵害）の中に盗聴罪（ドイツ刑法二〇一条）、盗撮罪（同二〇一条ａ）、信書開封罪（同二〇二条）、通信傍受罪（同二〇二条ａ）、データ傍受罪（同二〇二条ｂ）、通信傍受及びデータ傍受の準備罪（同二〇二条ｃ）、個人の秘密開示罪（同二〇三条）、企業秘密侵害罪（同二〇四条）及び通信の秘密侵害罪（同二〇六条）が規定されていることを理解することができる。ドイツの立法例と比較してみると、日本では私人の法的利益（特に私生活上の秘密）が相対的に軽視されているという事実を明確に認識することができる。この点については、更に後述する。

（44）　例えば、Shaheed Bilal という者（被告人）が、二〇〇八年以降約二年間にわたり、ネット上で購入した他人のクレジットカード情報を用い、家族ぐるみで、iPhone や iPad 等の Apple 製品（総額一〇〇万ドル以上相当）を購入し、あるいは盗んだ物品をネット上で売りさばいていたという事件があった。その後、被告人は、共犯者である家族らと共に逮捕・起訴され、拘禁刑四年六月～九年の不定期刑に処する旨の判決を受けた（判決当時二九歳）。この事件は、Apple iScam 事件として知られており、被告人は家族犯罪グループのリーダーだったとされている。

Leader of Apple iScam gets up to 9 years in prison, REUTERS, June 22, 2012 http://in.reuters.com/article/2012/06/21/apple-crimering-idINL1E8HLB9T20120621［二〇一二年一〇月一九日確認］

（45）　グルーポンジャパン（http://www.groupon.jp/）は、電子的なクーポン券の発行を業務としている。

（46）　WebMoney（http://www.webmoney.jp/）は、電子的なプリペイドカードの発行及び決済を業務としている。

（47）　二〇一一年、誰かによって無権限取得された PayPal のアカウントがネット上の闇サイトにおいて低額で売りさばかれていると報じられた。

Buy hacked PayPal accounts for 50c, SC Magazine, Oct 6, 2011

http://www.scmagazine.com.au/News/275877, buy-hacked-paypal-accounts-for-50c.aspx［二〇一二年一〇月一九日確認］

（48） 刑法の支払用カード電磁的記録不正作出等の罪（刑法一六三条の二～一六三条の五）は、支払用カードに用いられる電磁的記録の内容である情報の取得・移転・保管等のいわば幇助行為の類型に属する行為を独立罪として定めるものである。これは、既述の不正アクセス禁止法一部改正により設けられた他人の識別符号の要求行為、取得行為、保管行為及び提供行為といった犯罪類型の構成に影響を与えたものと考えられ、その意味で非常に重要であると思われる。

（49） 日本国の裁判所の刑事裁判例中でフィッシングにより支払用カード電磁的記録を取得または保管した事例は見当たらない。従来は、スキマーと呼ばれるクレジットカード情報傍受専用装置（スキミング装置）等を用いた犯行が主流であったためと推測される。そのような事例として、東京高判平成一六年六月一七日・東京高等裁判所（刑事）判決時報五五巻一～一二号四八頁がある。なお、同判決は、保管罪の罪数について、「支払用カード電磁的記録情報保管罪は、支払用カード電磁的記録不正作出罪の準備行為を罰する性質の罪であるところ、本件のように、一個のスキマーに複数の電磁的情報が保管されている場合には、電磁的情報の一件ごとに本罪が成立するのではなく、保管されている電磁的情報全部について、包括して一個の本罪が成立すると解すべきである」と判示している。

（50） 前掲西田『刑法各論（第六版）』三四四～三四五頁

（51） 前掲西田『刑法各論（第六版）』三四七頁は、「カードとは分離された状態で電磁的記録（たとえば、磁気情報部分）のみを不正に作出したが、いまだカードに貼付されていないような場合には、不正作出の未遂（一六五条の五）または準備（一六三条の四）にとどまる」としている。

（52） 正確には、二つの異なる種類に属する主観的意図（目的）が同時に並存している場合である。このような主観的目的が現実に並存する場合、実際の人間の意識内容としては常に明確に「並存」として認識または意識されているとは限らない。しかし、証拠によってそのような状態にあったと推認することが可能である限り、並存していたという事実を認定することは可能である。

（53） 前掲西田『刑法各論（第六版）』三五二頁は、刑法一六三条の四の不正作出準備罪に含まれる取得罪、保管罪及び提供罪の罪数について、牽連犯となるとしている。また、前掲前田『刑法各論講義（第五版）』五一一頁は、「取得と保管、取得と提供、保管と提供はそれぞれ牽連犯の関係に立つ」としている。

（54） 経済産業省知的財産政策室編著『逐条解説不正競争防止法（平成二一年改正版）』（有斐閣、二〇一〇）一七九頁

（55） 西野哲朗「量子コンピュータ」情報処理三六巻四号三三七頁、Simon J. Devitt, William J. Munro & Kae Nemoto, High

performance quantum computing, Progress in informatics : PI 8, pp.49–55 など。

（56）　実際には明確に分けられるものではない。例えば、国家法益は国際的な法人格主体としての「国」の直接の法的利益または国家主権から直接に由来する法的利益を保護法益とするものであることにほぼ異論はないであろう。しかし、民主主義という政治理念を前提とする限り、国民の利益を全く度外視して国家の利益を考えることは許されない。すなわち、国家の存立それ自体を直接に保護法益としている内乱罪（刑法七七条）ひとつとってみても、国民が一人も存在しない状態での日本国というものを観念することは無意味であり、また、国家の存立は国民の生存を物的に確保することを目的としていることからすると、国家の構成員である国民の生存という私的利益を保護法益としているとも理解することが可能なのである。国家が国民によって構成されているという観念のない時代（とりわけ第二次世界大戦の終戦前の時代）には純粋に観念的な存在としての「国」を観念し、そのような意味での「国」の法益を理論的に承認することは可能であったかもしれない。しかしながら、現代の状況は全く異なる。本論文では、そのような認識を前提としつつも、とりあえず伝統的な刑事法学上の法益分類に基づいた検討を試み、今後のより良き立法論の構築に向けた論点の提供をしようと思う。

（57）　一般に、秘密を侵す罪（刑法一三章）は、社会法益に関する犯罪類型に含まれると解されている。それゆえ、そのような伝統的な分類の下においては、通信の秘密及び企業秘密もまた社会法益に含まれるとせざるを得ない。支払用カード電磁的記録についても、文書偽造の罪（刑法一七章）が社会法益に関する犯罪類型に含まれていると解されていることから、同様に扱うことになる。

（58）　「identification theft」は、「ＩＤ窃盗」と和訳されるのが通例である。しかし、「phishing fraud」を「フィッシング詐欺」と訳するのが適切でないのと同様、財物ではない純然たる情報の無権限取得行為について「窃盗」という訳語をあてることも適切ではないと考えられる。もっとも、将来、仮に財産的法益と非財産的法益の両方を平等に認識・理解するような法思想が普及する時代が来るとすれば、非財産的法益の無権限取得の場合においても「詐欺」や「窃盗」の語を用いても何ら差し支えがないような状況になるかもしれない。なお、これらの点については、夏井高人「アメリカ合衆国におけるコンピュータ犯罪立法動向―無権限アクセスを中心とする比較法的検討と日本法への示唆」判例タイムズ一〇〇八号一〇六頁でも若干の考察結果を示した。

（59）　Bundesministerium der Justiz: Strafgesetzbuch
http://www.gesetze-im-internet.de/stgb/index.html［二〇一二年一〇月二〇日確認］

（60） この英文は、公式英訳であろうと推測されるところ、ドイツ刑法二〇二条b及び同法二〇二条c中にある「Abfangen von Daten」というドイツ語の語句が英文では「Phishing」となっていることに留意すべきである。すなわち、ドイツ刑法二〇二条b及び同法二〇二条cは、フィッシング行為に対する処罰条項である。ただし、本論文においては、二〇二条b及び二〇二条cがEUのサイバー犯罪条約（Convention on Cybercrimes）と関連するものであるとの立法経過に鑑み、「データ傍受」という訳語をあてることにした。

（61） ［訳注］暗号化された通信などを指すものと解される。

（62） ［訳注］電子計算機における無線通信及び装置からの電磁波放射の二つを含むものと解される。

（63） ［訳注］Thomas Fischer, Strafgesetzbuch und Nebengesetze 59. Auflage, C. H. Beck, 2012 中の二〇〇条bの解説（一三三四頁）によれば、「unbefvgt」とは、一般的な「違法」という意味で用いられている。

（64） CHAPTER 47 - FRAUD AND FALSE STATEMENTS (sections 1001–1040)
http://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI-chap47.pdf［二〇一一年一〇月二〇日確認］

（65） What Are Identity Theft and Identity Fraud?
Department of Justice
http://www.justice.gov/criminal/fraud/websites/idtheft.html［二〇一一年一〇月二〇日確認］

（66） Romanian national pleads guilty to possessing unauthorized credit cards numbers, identity theft
United States Department of Justice, United States Attorney's Office, District of Minnesota, October 7, 2008
http://www.justice.gov/criminal/cybercrime/press-releases/2008/popaPlea.pdf［二〇一一年一〇月二〇日確認］
SoCal Manager of International Computer Hacking Ring Sentenced to Five Years in Federal Prison for Defrauding Banks
U.S. Attorney's Office, May 14, 2012
http://www.fbi.gov/losangeles/press-releases/2012/socal-manager-of-international-computer-hacking-ring-sentenced-to-five-years-in-federal-prison-for-defrauding-banks［二〇一一年一〇月二〇日確認］

(67) 諸般の事情により 18 USC §1028 の(e)項以下の条文（原文）を割愛し、(a)項～(d)項までについてのみ翻訳を試みた。

(68) ［訳注］「knowingly」は、日本国刑法における「故意に」とほぼ同義と解されるが、直訳であるので「認識して」と訳した。ただし、その認識すべき具体的内容は、(a)項(1)～(7)に規定する個々の犯罪行為類型によって異なる。なお、関連する裁判例として、Flores-Figueroa v. United States, 556 U.S. 646 (2009)、United States v. Cabrera, 208 F.3d 309 (2000) 等がある。

(69) 脚注（57）参照

(70) 四〇二条一、四〇二条二(1)、(2)、(3)及び(5)を訳出し、同条二(4)の和訳を割愛した。

(71) ［訳注］要するに、詐欺罪で有罪となる行為のために使用する目的があったと推定されてもやむを得ない状況下において、他人の識別情報を所持する行為は犯罪行為として処罰されるという趣旨の条項である。

(72) ［訳注］要するに、詐欺罪で有罪となる行為のために使用する目的があると知りつつ、①他人の識別情報を提供・販売するなどの行為、または、②他人の識別情報を提供・販売するために保管する行為は犯罪行為として処罰されるという趣旨の条項である。

(73) ［訳注］前段は裁判所の管轄権を定める条項である。被疑事実である犯罪実行地や被告人の勾留場所にある裁判所が管轄権を有する。後段は、カナダが複数の州で構成される連邦国家であることから、管轄権のない州においては州務長官（州の司法長官）の事前の同意なく公判を開始することを禁止する趣旨の条項である。

(74) 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（平成二三年～平成二七年度）による研究成果の一部である。