サイバー犯罪の研究（六）-違法な電子メールに関する比較法的検討-

法律論叢　第八六巻　第六号（二〇一四・三）

【論　説】

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――

夏井高人

目　次

一　はじめに

一般に、サイバー犯罪の範疇に含まれる犯罪行為は、①固有のサイバー犯罪及び②電子的手段を利用した犯罪の二つの類型に分けて考えることができる。前者は、電子計算機や電気通信等の電子的手段を必須の構成要件要素として成立する犯罪であり、それなしには犯罪が成立しないという意味で固有のサイバー犯罪である。後者は、非電子的な手段によっても犯罪を実行することができるが、電子的な手段によることも可能であり、かつ、電子的な手段特有の問題を含むものという意味でサイバー犯罪の一種である。サイバー犯罪条約(1)もこのような犯罪類型としての区別を基礎概念として構成されている。

ところで、電子メールは、現代の社会生活において欠かすことのできない重要かつ有用な通信手段の一種であることから、その発信者及び受信者の情報やデータが確実に伝達・処理されないと、情報通信の安全性や信頼性に対して深刻な悪影響を及ぼすこととなり得る。このことから、電子メールの送受信データの確実性・信頼性を保護法益とし[2]、送受信データを偽る行為を規律する法令として、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・以下「特定電子メール適正化法」という。）が制定されている。そして、同法中の罰則に定める犯罪行為は、電子的手段の一種である電子メールの送受信情報を必須の構成要件要素としているという意味で、①固有のサイバー犯罪の範疇に属するものと理解することができる。

他方、電子メールは、単に通信文を伝送するための電子的な手段であるというだけではなく、添付ファイル（attached file）等の機能によりコンピュータプログラムやデータ等を記録した電子ファイルを伝送するための運搬手段としての社会的機能も有している[3]。

そのことから、電子メールは、例えば、マルウェア（malware）などの不正指令電磁的記録（刑法一六八条の三）、わいせつ電磁的記録（同法一七五条）、他人の著作権等の知的財産権や情報財としての権利を侵害する内容を含む電磁的記録、脅迫（刑法二二二条）、名誉毀損（同法二三〇条）、恐喝（同法二四九条）、詐欺（同法二四六条）等の犯罪を実行するための文言を内容とする電磁的記録、他人のアクセス管理のための識別符号（不正アクセス禁止法五条）や支払用カード電磁的記録の情報（刑法一六三条の四）その他の犯罪を組成する文章、情報またはデータの電子的な運搬・伝送のために用いられることがある。そして、電子メールの添付ファイルとして送信された不正指令電磁的記録を用いて業務妨害行為[4]、電子計算機使用詐欺行為[5]、テロ行為を含む破壊行為[6]、通信傍受行為等[7]が実行されることもある。これらは、電子的な手段の一種である電子メールを一般犯罪の遂行のために用いるという意味で、②電子的手段

を利用した犯罪の範疇に属するものと理解することができる。ただ、これらの場合、電子メールは、単なる運搬手段の一種に過ぎず、それ自体として違法な存在であるということはできないという点に留意すべきである。(8)

これに対し、理論的には②電子的手段を利用した犯罪の範疇に属するものであっても、そのような行為が独立罪として処罰の対象となる場合には、①固有のサイバー犯罪として評価すべき性質を有する場合もある。例えば、ストーカー行為は、非電子的な手段を用いて実行されることも可能である。現実に、物理的なつきまとい行為の事例が多数存在するので、電子メールを用いてストーカー行為を実行し得るとしても、類型的には、②電子的手段を利用した犯罪の範疇に属するものと理解するのが正しい。しかし、ストーカー行為等の規制等に関する法律（平成一二年法律第八一号・以下「ストーカー行為規制法」という。）二条一項五号は「電子メールを送信」する行為を独立の構成要件要素として規定しているので、(9)その意味で①固有のサイバー犯罪の一種としての性質も有していると解することが可能である。(10)

このように、電子メールを用いたサイバー犯罪には異なる態様・性質のものが含まれる。更に、犯罪行為の予備行為や準備的行為まで含めると、現行法によって処罰可能な大多数の種類の犯罪について②電子的手段を利用した犯罪が成立し得ることになる。しかしながら、その全てについて論ずることは不可能である。

そこで、本論文では、主として①電子メールという電子的手段を犯罪成立のための必須の構成要件要素としている犯罪（固有のサイバー犯罪としての電子メール犯罪）及び②電子メールを構成要件要素となっているわけではないが現に実行される機会があると思われるものを中心に、何らかの意味で違法性を有する電子メール(11)を論じ、この分野における法律実務及び理論研究に資することを目的とする。

二　発信者情報の詐称

1　問題の所在

一般に、電子メールは、特定の送信者から特定の受信者[12]に対して送信される電子的な通信手段の一種である。

送信者データ（受信者の電子メールアドレスまたはIPアドレス）が実在する正確なものである場合、仮に受信者のデータ（受信者の電子メールアドレスまたはIPアドレス）に誤りやエラー等があったとしても、当該電子メールの送信が不成功（不達）に終わるだけであるので、その結果は送信者だけが負担することになる[13]。また、当該電子メールが何らかの犯罪と関連を有するものである場合、その送信者データが実在し正確なものである限り、捜査機関は、当該電子メールの送信処理に用いられた電子メールサーバなどに残されている通信履歴データを辿って当該電子メールの送信者を割り出すことが可能となる。

他方、仮に送信者データに誤りやエラー等がある場合、当該送信者が利用している電子メールサーバでの電子メール送信処理の過程でエラーが生じ、送信失敗で終わるのが普通である[14]。しかしながら、送信者が、DNSサーバに不正アクセスしてこれを無権限操作するなど何らかの技術的手段等を用い、送信者が利用している電子メールサーバ上では問題なく送信処理が実行されるけれども、当該電子メールの不達の場合の送信者への不達通知処理の際や受信者からの返信の際に、真の送信者に対して不達通知や返信メールの送信がなされないように意図的に何らかの細工を施した場合（以下「送信者データの詐称」という。）には様々な問題が発生する。この場合、送信者データを詐称して電子

メールを発信した送信者は、自らは何らの損失を被ることがない状態を確保し、真の送信者を容易に追跡できないようにした上で、匿名の状態で様々な犯罪行為その他の違法行為を実行できてしまうことになる。

更に、送信者のデータ及び受信者のデータのいずれもが実在しない虚偽のものであった場合、何らかの技術的手段を用いて虚偽の送信者データのままで電子メールの送信ができてしまうと、当該電子メールの宛先となっている受信者データが不実のものであることから当該電子メールは不達となるが、それに伴って自動的になされる不達通知処理は、送信者データが不実のものであることから処理完了とならない。この場合、電子メールサーバ及び電子メール伝送ソフトウェアの仕様次第では、いつまでたっても当該電子メールの不達処理が完了せず、様々な不都合が生ずる原因となり得るという問題がある。更に送信者データが詐称され、かつ、実在する第三者の送信者データに書き換えられている場合、不達通知は当該第三者のメールボックスへと大量に送信されることになるので、当該第三者には全く非がないのに、深刻な被害を受けてしまうことがあり得る。(15)

以上のような問題が現実的に最も顕在化したのは、いわゆるスパムメール（SPAM メール）と呼ばれる商業宣伝広告用電子メールの大量送信行為についてであった。(16) そのため、送信者データの詐称を禁止する世界各国の立法は、スパムメール対策のものとして形成されてきたし、日本国の法制もその例外ではない。(17) しかしながら、電子メールの送信者データを詐称する行為は、本来のスパムメールのように商業宣伝広告用電子メールの場合だけではなく、スパムメールを装ったフィッシングの目的、詐欺の目的またはマルウェア感染の目的など他のサイバー攻撃を実行する目的で送信される電子メールにおいてもしばしばみられる。そのようなサイバー攻撃では、主として、加害者を容易に特定できないようにするため、送信者データの詐称が行われる。(18)

これらのことから、電子メールにおける送信者データの詐称という行為は、スパムメールの文脈に限定して理解す

べきものではなく、より広く一般化してとらえるべきである。電子メールは、その汎用性のゆえに、様々なタイプのサイバー犯罪を実行するための電子的手段[19]の一つとなり得ること、そして、電子メールを用いて遂行される多種多様な犯罪行為の加害者を容易に特定できないようにするための手口の一つとして送信者データの詐称が実行されることを正確に認識・理解する必要がある。

2 法制

(1) 日本法

特定電子メール適正化法二条二号は、「特定電子メール」について「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。）[20]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」と定義している。

そして、同法四条は、「送信者は、特定電子メールの送信に当たっては」、法定の除外事由がない限り、当該送信者の氏名又は名称（当該電子メールの送信につき送信委託者がいる場合は、当該送信者又は当該送信委託者のうち当該送信に責任を有する者の氏名又は名称）（同条一号）、特定電子メールの送信をしないように求める旨の通知（一定の事項に係る特定電子メールの送信をしないように求める場合にあっては、その旨）（同法三条三項本文）[21]を受けるための「電子メールアドレス又は電気通信設備を識別するための文字、番号、記号その他の符号であって総務省令・内閣

府令で定めるもの」[22]（同法四条二号）及び「その他総務省令・内閣府令で定める事項」[23]（同条三号）が、当該電子メールの「受信をする者が使用する通信端末機器の映像面に」正しく表示されるようにしなければならないと定めている。[24]

加えて、同法五条は、「送信者は、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であって」、「当該電子メールの送信に用いた電子メールアドレス」及び「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」（送信者情報）を「偽って特定電子メールの送信をしてはならない」と規定し、また、同法六条は、「送信者は、自己又は他人の営業のために多数の電子メールの送信をする目的で、架空電子メールアドレスをそのあて先とする電子メールの送信をしてはならない」[25]と規定している。

これらが送信者データの詐称の禁止条項である。直接的には、同法四条は送信者情報が正確に表示されるようにすべきことを求め、同法五条は虚偽の送信者情報の送信を禁止し、そして、同法六条は架空の送信者情報の送信を禁止していることになる。

同法四条の違反行為に関して、同法七条は、「総務大臣及び内閣総理大臣（架空電子メールアドレスをそのあて先とする電子メールの送信に係る場合にあっては、総務大臣）は、送信者が一時に多数の者に対してする特定電子メールの送信その他の電子メールの送信につき、第三条若しくは第四条の規定を遵守していないと認める場合又は送信者情報を偽った電子メール若しくは架空電子メールアドレスをそのあて先とする電子メールの送信をしたと認める場合において、電子メールの送受信上の支障を防止するため必要があると認めるときは」、当該送信者に対し、「電子メールの送信の方法の改善に関し必要な措置をとるべきことを命ずることができる」と規定している。同条の措置命令に違反した者については罰則の適用があり、一年以下の懲役または一〇〇万円以下の罰金に処せられる（同法三四条二号）。

同法五条に規定する送信者情報を偽る電子メールを発した送信者は、一年以下の懲役または一〇〇万円以下の罰金

に処せられる（同法三四条一号）。法人の代表者、代理人、使用人その他の従業者が、その法人又は人の業務に関して虚偽の送信者情報を発した場合には、当該法人も処罰される（同法三七条）。

このようにして、特定電子メール適正化法は、電子メールの送信者情報を偽る行為を禁止し、その違反行為を処罰するものとしている。したがって、送信者情報を偽る特定電子メール等は、固有のサイバー犯罪の一種という意味で違法な電子メールであるということができる。(26)

しかし、送信者情報を偽る行為等の禁止は特定電子メールに限定される。特定電子メールの送信者は、「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」に限定される（同法二条二号）。したがって、非営利の団体（国際的なテロ組織や犯罪組織等）(27)や営利を営まない個人が送信者となっている場合、そのような者が送信者として実行した送信者データの詐称行為については特定電子メール適正化法の罰則が適用されないという重大かつ致命的な立法上の欠陥がある。この点については別稿において既に詳論したとおりである。(28)

(2) アメリカ合衆国法

アメリカ合衆国連邦法中で日本国の特定電子メール適正化法における送信者データの詐称に対する処罰と類似する条項を有する法令は、合衆国連邦法律集一八款一〇三七条（18 USC §1037）である。(29)この法律も全ての電子メールについて送信者データの詐称を処罰する趣旨のものではなく、商業宣伝広告メールについて送信者データの詐称を含め送信者の同一性を偽る行為を処罰するものである。その仮訳を試みる。

合衆国連邦法律集一八款一〇三七条　電子メールと関係する詐欺及び関連行為

(a) 一般―州際取引または国際取引において、(30)認識して、次のいずれかを実行した者またはそれを企てた者は、(b)項

の規定により処罰される。

(1)　権限なく、意図して、保護されたコンピュータからもしくはそのようなコンピュータを介して、複数の商業電子メールメッセージを伝送するようにすべく、保護されたコンピュータにアクセスする者、

(2)　当該メッセージの発信地に関して受信者もしくはインターネットアクセスサービスを騙しもしくは誤解させる意図で、複数の商業電子メールメッセージを中継または伝送するために、保護されたコンピュータを使用する者、

(3)　複数の商業電子メールメッセージ中のヘッダ情報を実質的に偽る者、または、そのようなメッセージを意図的に伝送させる者、

(4)　五以上の電子メールアカウントもしくはオンラインユーザアカウントまたは二以上のドメイン名について、真の登録者の同一性を実質的に偽る情報を用いて登録する者[31]、または、意図的に、そのような虚偽のアカウントもしくはドメイン名の組み合わせを用いて複数の電子メールメッセージを伝送させようとする者、または、

(5)　五以上のIPアドレスの登録者に関して、自己が登録者またはその適法な承継人であると虚偽の表示をする者、または、意図的に、そのようなIPアドレスから複数の商業電子メールメッセージを伝送させようとする者。

(b)　罰則―(a)項に規定する犯罪に対する処罰は次のとおりである。

(1)　次の場合には、本款に規定する罰金刑、五年以下の拘禁刑、または、その併科とする。

(A)　合衆国連邦法もしくは州法に規定する重罪の遂行として違反行為が実行された場合：または、

(B)　被告人が、複数の商業電子メールメッセージの伝送を含む行為もしくはコンピュータに対する無権限アクセスの罪により、本条もしくは一〇三〇条[32]または州法に基づき拘禁刑の宣告を受けたことがある場合[33]：

(2)　次の場合には、本款に規定する罰金刑、三年以下の拘禁刑、または、その併科とする。

(A) 当該違反行為が(a)(1)に規定する違反行為となる場合：

(B) 当該違反行為が(a)(4)に規定する違反行為となる場合であり、かつ、二〇以上の虚偽の電子メールアカウントもしくはユーザアカウントの登録または一〇以上の虚偽のドメイン名登録を含む場合：

(C) 当該違反行為の遂行により伝送された電子メールメッセージの分量が過去二四時間以内に二五〇〇を超過する場合、過去三〇日間に二万五〇〇〇を超過する場合、または、過去一年間に二五万を超過する場合：

(D) 当該違反行為により、一名以上の者に対し、過去一年間に合計五〇〇〇ドル以上の損失を発生させた場合：

(E) 当該違反行為の結果として、当該違反行為を実行した者が過去一年間に合計五〇〇〇ドル以上の額の利益を得た場合：

(F) 当該違反行為が、被告人が組織者もしくは首謀者となって他の三名以上の者と共謀して実行された場合：

(3) それ以外の場合には、本款に規定する罰金刑、一年以下の拘禁刑、または、その併科とする。

(c) 没収

(1) 一般―本条に規定する違反行為を実行した者に対して刑を宣告する裁判所は、次の物件について、合衆国連邦のために被告人から没収することを命じなければならない。

(A) 当該違反行為によって得た全利益を構成しまたはそのようなものとして追跡可能な全ての財産、不動産もしくは動産：及び

(B) 当該違反行為を実行するためもしくはその実行を容易にするために用いられまたは用いようとした装置、ソフトウェアその他の技術。

(2) 手続―規制品法（21 U.S.C. 853）四一三条に規定する手続中で同条(d)項以外の手続、連邦刑事訴訟規則三二・

二に規定する手続は、本条に基づく刑事没収手続の全ての段階において適用する。

(d) 定義―本条においては：

(1) 損失―「損失」という用語は、本款一〇三〇条(e)項に規定する用語としての意味を有する。

(2) 実質的―(a)項(3)及び(4)においては、当該メッセージの受信者、受信者の代わりに当該メッセージを処理するインターネットアクセスサービス、[34] 本条違反があると主張する者の能力を損ない、または、当該電子メールメッセージを発信した者を特定し、突き止めもしくは応答し、違反容疑事実を捜査する法執行機関[35]の能力を損なう結果となるようにヘッダ情報または登録情報が改変されもしくは隠蔽された場合、そのヘッダ情報または登録情報は、実質的に虚偽のものである。

(3) 複数―「複数」という用語は、過去二四時間に一〇〇通以上の電子メールメッセージ、過去三〇日間に一〇〇〇通以上の電子メールメッセージ、または、過去一年間に一万通以上の電子メールメッセージであることを意味する。

(4) 他の用語―他の用語については、二〇〇三年 CAN-SPAM 法三条に規定する用語としての意味を有する。

［原文］

18 USC § 1037 - Fraud and related activity in connection with electronic mail

(a) In General–Whoever, in or affecting interstate or foreign commerce, knowingly–

(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,

(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent

to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,

(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,

(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or

(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses,

or conspires to do so, shall be punished as provided in subsection (b).

(b) Penalties.– The punishment for an offense under subsection (a) is–

(1) a fine under this title, imprisonment for not more than 5 years, or both, if–

(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

(2) a fine under this title, imprisonment for not more than 3 years, or both, if–

(A) the offense is an offense under subsection (a)(1);

(B) the offense is an offense under subsection (a)(4) and involved 20 or more falsified electronic mail or online user account registrations, or 10 or more falsified domain name registrations;

(C) the volume of electronic mail messages transmitted in furtherance of the offense exceeded 2,500 during any 24-hour period, 25, 000 during any 30-day period, or 250,000 during any 1-year period;

(D) the offense caused loss to one or more persons aggregating $5,000 or more in value during any 1-year period;

(E) as a result of the offense any individual committing the offense obtained anything of value aggregating $5,000 or more during any 1-year period; or

(F) the offense was undertaken by the defendant in concert with three or more other persons with respect to whom the defendant occupied a position of organizer or leader; and

(3) a fine under this title or imprisonment for not more than 1 year, or both, in any other case.

(c) Forfeiture.–

(1) In general.– The court, in imposing sentence on a person who is convicted of an offense under this section, shall order that the defendant forfeit to the United States–

(A) any property, real or personal, constituting or traceable to gross proceeds obtained from such offense; and

(B) any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offense.

(2) Procedures.– The procedures set forth in section 413 of the Controlled Substances Act (21 U.S.C. 853), other than subsection (d) of that section, and in Rule 32.2 of the Federal Rules of Criminal Procedure, shall apply to all

stages of a criminal forfeiture proceeding under this section.

(d) Definitions.– In this section:

(1) Loss.– The term "loss" has the meaning given that term in section 1030 (e) of this title.

(2) Materially.– For purposes of paragraphs (3) and (4) of subsection (a), header information or registration information is materially falsified if it is altered or concealed in a manner that would impair the ability of a recipient of the message, an Internet access service processing the message on behalf of a recipient, a person alleging a violation of this section, or a law enforcement agency to identify, locate, or respond to a person who initiated the electronic mail message or to investigate the alleged violation.

(3) Multiple.– The term "multiple" means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period.

(4) Other terms.– Any other term has the meaning given that term by section 3 of the CAN-SPAM Act of 2003.

3　事例

特定電子メール適正化法七条に基づく総務省及び消費者庁の措置命令事例[36]並びに同法違反の罪による有罪判決の事例としては、次のようなものがある。なお、二〇一三年一一月末日現在、公式判例集等に収録された刑事裁判事例は見当たらない。

これらの事例の内容を検討してみると、いわゆる「出会い系サイト」またはこれに類するサイトへの勧誘のための電子メール送信の事例がほとんどであることを理解することができる。(37)

(1) 法三条及び四条違反行為に対する措置命令

株式会社エレクトリックオペレーションは、①少なくとも平成二一年六月から同年一一月までの間、出会い系サイト「ショコラ」、「セレブガーデン」、「アドコミュ」、「レインボー」、「ラブデスティニー」、「ガーデン」及び「セックスアンドザマネー」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ずに電子メールを送信し、また、同意を得た旨の記録を保存しておらず、法第三条第一項及び第二項の規定に違反する行為を行い、また、②「レインボー」の広告又は宣伝を行う電子メールにおいて、送信者の氏名又は名称を正しく表示しておらず、法第四条の規定に違反する行為を行っていたとして、同社に対し、平成二一年一二月四日付けで措置命令がなされた。

個人事業者であるSは、①少なくとも平成二一年一〇月から平成二二年二月までの間、出会い系サイト「星の砂」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ずに電子メールを送信し、また、少なくとも平成二一年一〇月から平成二二年一月までの間、同意を得た旨の記録を保存しておらず、法第三条第一項及び第二項の規定に違反する行為を行い、また、②広告又は宣伝を行う電子メールにおいて、少なくとも平成二一年一〇月から平成二二年二月までの間、送信者の氏名又は名称を正しく表示しておらず、法第四条の規定に違反する行為を行っていたとして、個人事業者Sに対し、平成二二年三月五日付けで措置命令がなされた。

株式会社アンビションは、①少なくとも平成二二年二月一七日から平成二二年八月四日までの間、自己が運営する出会い系サイト「Pure Life」及び他者の運営するサイトの広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行い、また、②広告又は宣伝を行う電子メールにおいて、少なくとも平成二二年二月から平成二二年七月までの間、送信者の氏名又は名称を正しく表示しておらず、法第四条の規定に違反する行為を行っていたとして、同社に対し、平成二二年八月一〇日付けで措置命令がなされた。

株式会社ノブロは、①少なくとも平成二二年九月一日から平成二三年四月一七日までの間、自己の運営するウェブサイト「カジュアル」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行い、また、②広告又は宣伝を行う電子メールにおいて、少なくとも平成二二年九月一日から平成二三年四月一七日までの間、送信者の名称を表示しておらず、法第四条の規定に違反する行為を行っていたとして、同社に対し、平成二三年五月九日付けで措置命令がなされた。

個人事業者であるKは、①少なくとも平成二二年一二月四日から平成二三年五月一九日までの間、自己の運営するウェブサイト「セレクト」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行い、②また、広告又は宣伝を行う電子メールにおいて、少なくとも平成二二年一二月四日から平成二三年五月一九日までの間、送信者の氏名又は名称及び受信拒否の通知ができる旨を表示しておらず、法第四条の規定に違反する行為を行っていたとして、個人事業者Kに対し、平成二三年六月一日付け

で措置命令がなされた。

株式会社 Breeze は、①少なくとも平成二二年一一月二五日から平成二三年五月一九日までの間、自己の運営するウェブサイト「マジカルラブ」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行い、また、②広告又は宣伝を行う電子メールにおいて、少なくとも平成二二年一一月二五日から平成二三年五月一九日までの間、受信拒否の通知ができる旨を表示しておらず、法第四条の規定に違反する行為を行っていたとして、同社に対し、平成二三年六月一三日付けで措置命令がなされた。

株式会社 FINE は、①少なくとも平成二二年九月一二日から平成二三年五月一五日までの間、自己の運営するウェブサイト「For you premium」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行い、また、②広告又は宣伝を行う電子メールにおいて、少なくとも平成二二年九月一二日から平成二三年五月一五日までの間、受信拒否の通知ができる旨を表示しておらず、法第四条の規定に違反する行為を行っていたとして、同社に対し、平成二三年六月一三日付けで措置命令がなされた。

合同会社ウインラックは、①少なくとも平成二三年三月二日から平成二三年一〇月二七日までの間、自己の運営するウェブサイト「ミラクル」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行い、また、②広告又は宣伝を行う電子メールにおいて、少なくとも平成二三年三月二日から平成二三年一〇月二七日までの間、送信者の名称及び受信拒否の通知ができる旨を表示してお

らず、法第四条の規定に違反する行為を行っていたとして、同社に対し、平成二三年一二月二日付けで措置命令がなされた。

株式会社アイエイコミュニケーションズは、①少なくとも平成二四年二月九日から平成二四年五月二四日までの間、ウェブサイト「ファーストクラス」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行い、また、②広告又は宣伝を行う電子メールにおいて、少なくとも平成二四年二月九日から平成二四年五月二四日までの間、送信者の名称及び受信拒否の通知ができる旨を表示しておらず、法第四条の規定に違反する行為を行っていたとして、同社に対し、平成二四年七月四日付けで措置命令がなされた。

有限会社ナビーレは、①少なくとも平成二四年三月一九日から平成二五年一月二三日までの間、ウェブサイト「FLASH」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行い、また、②広告又は宣伝を行う電子メールにおいて、少なくとも平成二四年三月一九日から平成二五年一月二三日までの間、送信者の名称を表示しておらず、法第四条の規定に違反する行為を行っていたとして、同社に対し、平成二五年三月一九日付けで措置命令がなされた。

(2) 法三条違反行為に対する措置命令

株式会社スパイラルネットは、少なくとも平成二一年九月一七日から平成二二年三月一日までの間、出会い系サイト「Vogue～ヴォーグ～」及び「椿～TSUBAKI～」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行っていたとして、同社に対し、平成二二年四月七日付けで措置命令がなされた。

株式会社広告研究所は、少なくとも平成二一年一〇月一日から平成二二年二月二八日までの間、出会い系サイト「カラット～Carat～」及び「ロメオ～Romeo～」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行っていたとして、同社に対し、平成二二年四月一五日付けで措置命令がなされた。

株式会社シックスエストレラは、少なくとも平成二二年一二月二一日から平成二三年四月一七日までの間、自己の運営するウェブサイト「マイストーリー」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行っていたとして、同社に対し、平成二三年四月二七日付けで措置命令がなされた。

株式会社ライズ（旧社名：株式会社SEO）は、少なくとも平成二三年一〇月一六日から平成二四年三月二九日ま

での間、ウェブサイト「天使の階段」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行っていたとして、同社に対し、平成二四年五月九日付けで措置命令がなされた。

株式会社福田は、少なくとも平成二四年一〇月一〇日から平成二五年二月二六日までの間、ウェブサイト「Quiero」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行っていたとして、同社に対し、平成二五年三月二七日付けで措置命令がなされた。

株式会社アレグレは、少なくとも平成二四年一一月二六日から平成二五年八月三一日までの間、ウェブサイト「Tomorrow」及び「EDEN」の広告又は宣伝を行う電子メールを送信するに当たり、受信者の同意を得ておらず、法第三条第一項の規定に違反する行為を行っていたとして、同社に対し、平成二五年九月二〇日付けで措置命令がなされた。

(3) 有罪判決

京都地方裁判所平成二三年四月二八日判決（公式判例集等未登載）[38]

（犯罪事実の概要）

サイト運営会社ユニバーサルフリークスは、平成二二年一〇月ころ、出会い系サイトの広告又は宣伝を行う電子

メールを送信するに当たり、架空の電子メールアドレスを用い、中国やフィリピンのサーバ経由で送信するなどして、特定電子メールの送信者情報を偽った。

（量刑）

被告人（元代表者）　懲役一〇月（執行猶予三年）
被告人（元役員二名）　各懲役八月（執行猶予三年）
被告人（運営会社）　罰金七〇〇万円

三　SPAMメール

1　スパムメール問題の現状

商業宣伝広告目的で大量に発信される電子メールの問題は、数年前までのように大いに騒がれていた状況よりは幾分か鎮静化したかのように見える。その背景には、既述の特定電子メール適正化法に基づく総務省及び消費者庁の措置命令によるところが大きいと思われる。それと同時に、総務省等によりガイドライン[39]が策定され、スパムメールに対する法的規制について周知徹底されたことが効果をあげたということも考えられる。

他方では、スパムメールを自動的に判別し、受信者の手元に届く前に自動的に消去したりゴミ箱のフォルダに格納したりしてしまうような電子的な仕組み（スパムフィルタ）が進歩したことも大きく影響していると推定される。関連各社が提供するセキュリティソフトやセキュリティサービス等を使用することにより、個々の電子メールクライア

ントアプリケーションレベルでも、Web メールやクラウドベースでの電子メールサービスの場合におけるサーバレベルでも、スパムメールの自動フィルタリングが実装・運用されるようになった。

その結果、「大半の消費者がそのような電子メールの受信を望んでいない」という事実が誰の目にも明らかになってしまったのではないかと思う。このことは、ごく一部の特殊な業務を遂行する事業者等の場合を除き、商業宣伝広告のために電子メールを発信しようという事業者側のインセンティブを大幅に減殺したものと推定される。(40)

また、別の角度から検討してみると、現在の電子的なマーケティング技術の主流は、いわゆるビッグデータ等に代表されるような巨大なデータベースを駆使した電子的解析技術に基づき、消費者の行動履歴等を自動解析し、より標的を絞り効果的なピンポイントの商業宣伝広告を実現する手法へと移行している。そのため、「電子メールを無差別かつ大量に送信する」という古典的な手法がかなり陳腐なものとなってしまったと考えることもできる。換言すると、より効果が乏しいと考えられる商業宣伝広告手段（スパムメール）からより効果が高いと考えられる商業宣伝広告手段（ターゲット広告）への移行・切り替えが急速に進んでいると評価することが可能である。

現時点においても商業宣伝広告のようにみえる電子メールが大量に送信されてくることは事実である。しかし、そのような電子メールの実質を検討してみると、本来の商業宣伝広告のための電子メールが相対的に減少している一方、商業宣伝広告目的の電子メールのような外見を装いフィッシングや詐欺など別の犯罪の目的を遂行するために送信されてくる偽装電子メールが相対的に増加していることを理解することができる。そして、フィッシング等の目的による偽装電子メールは、従来想定されていたスパムメールとは異なる犯罪性を有する。

ここでは、本来の商業宣伝広告目的での電子メールについて適用される日本国の現行法規の骨格部分である特定電子メール適正化法（既述の送信者情報を偽る行為等の禁止等に関する部分を除く。）及び特定商品取引に関する法律

（以下「特定商取引法」という。）について概観する。(41)

2　法制

(1)　日本法

(a)　特定電子メール適正化法

特定電子メール適正化法三条は、特定電子メールの送信について、次のように規定し、原則として禁止としている。(42)

1　送信者は、次に掲げる者以外の者に対し、特定電子メールの送信をしてはならない。

一　あらかじめ、特定電子メールの送信をするように求める旨又は送信をすることに同意する旨を送信者又は送信委託者（電子メールの送信を委託した者（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。）をいう。以下同じ。）に対し通知した者

二　前号に掲げるもののほか、総務省令・内閣府令で定めるところにより自己の電子メールアドレスを送信者又は送信委託者に対し通知した者

三　前二号に掲げるもののほか、当該特定電子メールを手段とする広告又は宣伝に係る営業を営む者と取引関係にある者

四　前三号に掲げるもののほか、総務省令・内閣府令で定めるところにより自己の電子メールアドレスを公表

している団体又は個人（個人にあっては、営業を営む者に限る。）

2　前項第一号の通知を受けた者は、総務省令・内閣府令で定めるところにより特定電子メールの送信をするように求めがあったこと又は送信をすることに同意があったことを証する記録を保存しなければならない。

3　送信者は、第一項各号に掲げる者から総務省令・内閣府令で定めるところにより特定電子メールの送信をしないように求める旨（一定の事項に係る特定電子メールの送信をしないように求める場合にあっては、その旨）の通知を受けたとき（送信委託者がその通知を受けたときを含む。）は、その通知に示された意思に反して、特定電子メールの送信をしてはならない。ただし、電子メールの受信をする者の意思に基づき広告又は宣伝以外の行為を主たる目的として送信される電子メールにおいて広告又は宣伝が付随的に行われる場合その他のこれに類する場合として総務省令・内閣府令で定める場合は、この限りでない。

要するに、商業宣伝広告目的での電子メールが、原則として、包括的に禁止されている（同条一項、三項）。同条一項は、事前に送信を求める通知がないのに送信する行為を禁止し、同条三項は、受信拒否の通知があったのに送信する行為を禁止する趣旨の規定である。一項の例外として同項各号に規定されている事項のうち、一号、二号及び四号所定の場合とは、概ね次のように解される。

まず、送信者または送信委託者に対して、事前に、特定電子メールの送信をするように通知した場合（一号）。この場合における「送信委託者」は営利目的で委託業務を遂行する団体及び個人に限定されるので、営利目的を有しない団体または個人が送信委託者である場合には、適法に送信を求める通知がなされたとは認められない。

次に、書面により自己の電子メールアドレスを送信者または送信受託者に通知した場合（二号）。この通知が書面に

よるべきことは、特定電子メールの送信の適正化等に関する法律施行規則二条一項一号に規定されており、例外がある（同規則六条所定の場合など）。なお、特定電子メール適正化法三条三項の規定に基づき「拒否」の通知を電子メールによって行った場合に、書面により自己の電子メールアドレスを通知したと理解（曲解）されることを防ぐため、同規則二条二項は、送信拒否の電子メールによる通知は特定電子メール適正化法三条一項二号所定の「通知」に該当しない旨を明定している。

そして、自己の電子メールアドレスを公表している団体又は営業を行う個人の場合（四号）。この自己の電子メールアドレスの「公表」について、同規則三条は、「自己の電子メールアドレスをインターネットを利用して公衆が閲覧することができる状態に置く方法とする。ただし、自己の電子メールアドレスと併せて特定電子メールの送信をしないように求める旨の文言をインターネットを利用して公衆が閲覧することができる状態に置いたときは、この限りではない」と規定している。したがって、例えば、インターネット上で巡回ロボットプログラム等を用いて自動的に電子メールアドレスを収集した場合、当該自動収集が「特定電子メールの送信をしないように求める旨の文言」を無視して電子メールを収集するような仕様になっている場合には、同規則三条ただし書により、特定電子メール適正化法三条一項四号所定の公表された電子メールアドレスに該当しないことになるので、その電子メールアドレスに対する特定電子メールの送信対する送信行為は、同条一項に違反する行為となる。

他方、特定電子メール適正化法四条は、同法三条による送信の禁止とりわけ同条三項所定の受信拒否通知の実効性を確保するため、特定電子メールの送信者の表示義務を定めている。

特定電子メール適正化法三条または四条の違反行為があり、かつ、「電子メールの送受信上の支障を防止するため必要があると認めるときは」、「総務大臣及び内閣総理大臣（架空電子メールアドレスをそのあて先とする電子メールの

送信に係る場合にあっては、総務大臣）は」、当該電子メールの送信者等に対し、電子メールの送信の方法の改善に関し必要な措置をとるべきことを命ずることができる（同法七条）。この措置命令に反する行為については、罰則の適用があり、一年以下の懲役または一〇〇万円以下の罰金に処される（同法三四条二号）。法人の代表者、代理人、使用人その他の従業者が、その法人又は人の業務に関して措置命令に反する行為をした場合には、当該法人も処罰される（同法三七条）。

また、総務大臣または内閣総理大臣は、同法の施行に必要な限度において、「特定電子メール等の送信者若しくは送信委託者に対し、これらの送信に関し必要な報告をさせ、又はその職員に、これらの送信者若しくは送信委託者の事業所に立ち入り、帳簿、書類その他の物件を検査させること」（同法二八条一項）ができる。加えて、総務大臣は、同法の施行に必要な限度において、「電気通信事業者その他の者であって、電子メールアドレス又は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（特定電子メール等の受信をする者が使用する通信端末機器の映像面に表示されたもの又は特定電子メール等の送受信のために用いられたもののうち送信者に関するものに限る。）を使用する権利を付与したものから、当該権利を付与された者の氏名又は名称、住所その他の当該権利を付与された者を特定するために必要な情報の提供を求めること」（同法二九条）ができる。

なお、総務大臣は、特定電子メール適正化法に相当する外国の法令を執行する外国の当局（外国執行当局）[43]に対し、その職務の遂行に資すると認める情報の提供を行うことができ（同法三〇条一項）、また、外国執行当局からの要請があったときは、政治犯罪に対する捜査の場合[44]、日本国では犯罪とならない行為に対する捜査である場合などを除き、同法三〇条一項の規定により提供した情報を「当該要請に係る外国の刑事事件の捜査等に使用することについて同意をすること」ができる（同法三〇条三項）。これらの場合には、当該情報提供行為は、国家公務員としての守秘義務違反

行為とならない。ただし、総務大臣が同法三〇条三項の同意をする場合には、法務大臣及び外務大臣から確認を受けなければならない（同法三〇条四項）。

(b) 特定商取引に関する法律

特定電子メール適正化法は、特定電子メールを送信する送信者の業種・業態とは無関係に、特定電子メールの送信者全てについて適用される。これに対し、特定商取引法は、同法によって規律される特殊な業種・業態の者についてのみ適用されるものである点が異なっている。ところが、これら二つの法令に含まれている法規制には重複している部分があるように見えるので、相互の関係がわかりにくいという面があることは否定できない。しかしながら、特定電子メール適正化法は、営利目的の事業者が送信する電子メール全般について適用されるのに対し、特定商取引法は、通信販売、連鎖販売取引及び業務提供誘引取引が有する問題を軽減し消費者保護の目的を実現するために適用されることから、法の制度趣旨が異なっており、それゆえに、外見上類似する複数の法令が存在しているような状態になっていると理解すべきであろう。(45)

特定商取引法において電子メール関連の規制があるのは、主として、①通信販売電子メール広告をする販売業者または役務提供事業者（同法一二条の三）、②これらの者から電子メール広告の委託を受けた通信販売電子メール広告受託事業者（同法一二条の四）、③連鎖販売取引をする事業者等（同法三六条の三）、④これらの者から電子メール広告の委託を受けた通信販売電子メール広告受託事業者（同法三六条の三）、⑤業務提供誘引販売をする事業者（同法五四条の三）及び⑥これらの者から電子メール広告の委託を受けた通信販売電子メール広告受託事業者（同法五四条の四）である。これら以外の事業者に対しては特定商取引法の適用がないが、特定電子メール適正化法の適用はあることに留意しなければならない。

特定商取引法は、従来は、商業宣伝広告目的の電子メールについて受信しない旨の通知を受けた場合には送信してはならないとの規律になっていた（いわゆるオプトアウト方式）。しかし、この方法では実効性がないとの批判があったことなどから、平成二〇年の一部改正により、事前に同意を得ている場合などを除き、原則として、商業宣伝広告目的での電子メール送信ができないものとされるに至った（いわゆるオプトイン方式）[46]。承諾をしていない者に対する電子メール広告に関する禁止条項は、次のとおりである（各条文中の本論文における考察と直接の関連を有しない部分は省略）。

①　通信販売関係

第一二条の三（承諾をしていない者に対する電子メール広告の提供の禁止等）

販売業者又は役務提供事業者は、次に掲げる場合を除き、通信販売をする場合の商品若しくは指定権利の販売条件又は役務の提供条件について、その相手方となる者の承諾を得ないで電子メール広告（当該広告に係る通信文その他の情報を電磁的方法（電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法であって主務省令で定めるものをいう。以下同じ。）により送信し、これを当該広告の相手方の使用に係る電子計算機の映像面に表示されるようにする方法により行う広告をいう。以下同じ。）をしてはならない。

一　相手方となる者の請求に基づき、通信販売をする場合の商品若しくは指定権利の販売条件又は役務の提供条件に係る電子メール広告（以下この節において「通信販売電子メール広告」という。）をするとき。

二　当該販売業者の販売する商品若しくは指定権利若しくは当該役務提供事業者の提供する役務につき売買契約若しくは役務提供契約の申込みをした者又はこれらにつき売買契約若しくは役務提供契約を締結した者に対し、

主務省令で定める方法により当該申込み若しくは当該契約の内容又は当該契約の履行に関する事項を通知する場合において、主務省令で定めるところにより通信販売電子メール広告をするとき。

三　前二号に掲げるもののほか、通常通信販売電子メール広告の提供を受ける者の利益を損なうおそれがないと認められる場合として主務省令で定める場合において、通信販売電子メール広告をするとき。

2　前項に規定する承諾を得、又は同項第一号に規定する請求を受けた販売業者又は役務提供事業者は、当該通信販売電子メール広告の相手方から通信販売電子メール広告の提供を受けない旨の意思の表示を受けたときは、当該相手方に対し、通信販売電子メール広告をしてはならない。ただし、当該表示を受けた後に再び通信販売電子メール広告をすることにつき当該相手方から請求を受け、又は当該相手方の承諾を得た場合には、この限りでない。

3　（省略）

4　販売業者又は役務提供事業者は、通信販売電子メール広告をするときは、第一項第二号又は第三号に掲げる場合を除き、当該通信販売電子メール広告に、第一一条各号に掲げる事項のほか、主務省令で定めるところにより、その相手方が通信販売電子メール広告の提供を受けない旨の意思を表示するために必要な事項として主務省令で定めるもの[47]を表示しなければならない。

5　前二項の規定は、販売業者又は役務提供事業者が他の者に次に掲げる業務のすべてにつき一括して委託しているときは、その委託に係る通信販売電子メール広告については、適用しない。

一　通信販売電子メール広告をすることにつきその相手方の承諾を得、又はその相手方から請求を受ける業務

二　第三項に規定する記録を作成し、及び保存する業務

三　前項に規定する通信販売電子メール広告の提供を受けない旨の意思を表示するために必要な事項を表示する業務

第一二条の四

販売業者又は役務提供事業者から前条第五項各号に掲げる業務のすべてにつき一括して委託を受けた者（以下この節並びに第六六条第四項及び第六項において「通信販売電子メール広告受託事業者」という。）は、次に掲げる場合を除き、当該業務を委託した販売業者又は役務提供事業者（以下この節において「通信販売電子メール広告委託者」という。）が通信販売をする場合の商品若しくは指定権利の販売条件又は役務の提供条件について、その相手方となる者の承諾を得ないで通信販売電子メール広告をしてはならない。

一　相手方となる者の請求に基づき、通信販売電子メール広告委託者に係る通信販売電子メール広告をするとき。

二　前号に掲げるもののほか、通常通信販売電子メール広告委託者に係る通信販売電子メール広告の提供を受ける者の利益を損なうおそれがないと認められる場合として主務省令で定める場合において、通信販売電子メール広告委託者に係る通信販売電子メール広告をするとき。

2　前条第二項から第四項までの規定は、通信販売電子メール広告受託事業者による通信販売電子メール広告委託者に係る通信販売電子メール広告について準用する。この場合において、同条第三項及び第四項中「第一項第二号又は第三号」とあるのは、「次条第一項第二号」と読み替えるものとする。

②　連鎖販売関係(48)

第三六条の三（承諾をしていない者に対する電子メール広告の提供の禁止等）

統括者、勧誘者又は一般連鎖販売業者は、次に掲げる場合を除き、その統括者の統括する一連の連鎖販売業に係る連鎖販売取引について、その相手方となる者の承諾を得ないで電子メール広告をしてはならない。

一　相手方となる者の請求に基づき、その統括者の統括する一連の連鎖販売業に係る連鎖販売取引に係る電子メール広告（以下この章において「連鎖販売取引電子メール広告」という。）をするとき。

二　前号に掲げるもののほか、通常連鎖販売取引電子メール広告の提供を受ける者の利益を損なうおそれがないと認められる場合として主務省令で定める場合において、連鎖販売取引電子メール広告をするとき。

2　前項に規定する承諾を得、又は同項第一号に規定する請求を受けた統括者、勧誘者又は一般連鎖販売業者は、当該連鎖販売取引電子メール広告の相手方から連鎖販売取引電子メール広告の提供を受けない旨の意思の表示を受けたときは、当該相手方に対し、連鎖販売取引電子メール広告をしてはならない。ただし、当該表示を受けた後に再び連鎖販売取引電子メール広告をすることにつき当該相手方から請求を受け、又は当該相手方の承諾を得た場合には、この限りでない。

3　（省略）

4　統括者、勧誘者又は一般連鎖販売業者は、連鎖販売取引電子メール広告をするときは、第一項第二号に掲げる場合を除き、当該連鎖販売取引電子メール広告に、第三十五条各号に掲げる事項のほか、主務省令で定めるところにより、その相手方が連鎖販売取引電子メール広告の提供を受けない旨の意思を表示するために必要な事項として主務省令で定めるもの[49]を表示しなければならない。

5　（省略）

第三六条の四

統括者、勧誘者又は一般連鎖販売業者から前条第五項各号に掲げる業務のすべてにつき一括して委託を受けた者

（以下この章並びに第六六条第四項及び第六項において「連鎖販売取引電子メール広告受託事業者」という。）は、次に掲げる場合を除き、当該業務を委託した統括者、勧誘者又は一般連鎖販売業者（以下この条において「連鎖販売取引電子メール広告委託者」という。）が行うその統括者の統括する一連の連鎖販売業に係る連鎖販売取引について、その相手方となる者の承諾を得ないで連鎖販売取引電子メール広告をしてはならない。

一　相手方となる者の請求に基づき、連鎖販売取引電子メール広告委託者に係る連鎖販売取引電子メール広告をするとき。

二　前号に掲げるもののほか、通常連鎖販売取引電子メール広告委託者に係る連鎖販売取引電子メール広告の提供を受ける者の利益を損なうおそれがないと認められる場合として主務省令で定める場合において、連鎖販売取引電子メール広告委託者に係る連鎖販売取引電子メール広告をするとき。

2　前条第二項から第四項までの規定は、連鎖販売取引電子メール広告受託事業者による連鎖販売取引電子メール広告委託者に係る連鎖販売取引電子メール広告について準用する。この場合において、同条第三項及び第四項中「第一項第二号」とあるのは、「次条第一項第二号」と読み替えるものとする。

③　業務提供誘引販売関係(50)

第五四条の三（承諾をしていない者に対する電子メール広告の提供の禁止等）

業務提供誘引販売業を行う者は、次に掲げる場合を除き、その業務提供誘引販売業に係る業務提供誘引販売取引について、その相手方となる者の承諾を得ないで電子メール広告をしてはならない。

一　相手方となる者の請求に基づき、その業務提供誘引販売業に係る業務提供誘引販売取引に係る電子メール広

告（以下この章において「業務提供誘引販売取引電子メール広告」という。）をするとき。

二　前号に掲げるもののほか、通常業務提供誘引販売取引電子メール広告の提供を受ける者の利益を損なうおそれがないと認められる場合として主務省令で定める場合において、業務提供誘引販売取引電子メール広告をするとき。

2　前項に規定する承諾を得、又は同項第一号に規定する請求を受けた業務提供誘引販売業を行う者は、当該業務提供誘引販売取引電子メール広告の相手方から業務提供誘引販売取引電子メール広告の提供を受けない旨の意思の表示を受けたときは、当該相手方に対し、業務提供誘引販売取引電子メール広告をしてはならない。ただし、当該表示を受けた後に再び業務提供誘引販売取引電子メール広告をすることにつき当該相手方から請求を受け、又は当該相手方の承諾を得た場合には、この限りでない。

3　（省略）

4　業務提供誘引販売業を行う者は、業務提供誘引販売取引電子メール広告をするときは、第一項第二号に掲げる場合を除き、当該業務提供誘引販売取引電子メール広告に、第五三条各号に掲げる事項のほか、主務省令で定めるところにより、その相手方が業務提供誘引販売取引電子メール広告の提供を受けない旨の意思を表示するために必要な事項として主務省令で定めるもの[51]を表示しなければならない。

5　（省略）

第五四条の四

業務提供誘引販売業を行う者から前条第五項各号に掲げる業務のすべてにつき一括して委託を受けた者（以下こ

の章並びに第六六条第四項及び第六項において「業務提供誘引販売取引電子メール広告受託事業者」という。）は、次に掲げる場合を除き、当該業務を委託した業務提供誘引販売業を行う者（以下この条において「業務提供誘引販売取引電子メール広告委託者」という。）が行うその業務提供誘引販売業に係る業務提供誘引販売取引について、その相手方となる者の承諾を得ないで業務提供誘引販売取引電子メール広告をしてはならない。

一　相手方となる者の請求に基づき、業務提供誘引販売取引電子メール広告委託者に係る業務提供誘引販売取引電子メール広告をするとき。

二　前号に掲げるもののほか、通常業務提供誘引販売取引電子メール広告委託者に係る業務提供誘引販売取引電子メール広告の提供を受ける者の利益を損なうおそれがないと認められる場合として主務省令で定める場合において、業務提供誘引販売取引電子メール広告委託者に係る業務提供誘引販売取引電子メール広告をするとき。

2　前条第二項から第四項までの規定は、業務提供誘引販売取引電子メール広告受託事業者による業務提供誘引販売取引電子メール広告委託者に係る業務提供誘引販売取引電子メール広告について準用する。この場合において、同条第三項及び第四項中「第一項第二号」とあるのは、「次条第一項第二号」と読み替えるものとする。

④　罰則適用の相互関係

これらの禁止に違反する行為等に対する罰則は、同法七二条一項四号に規定されており、違反者は一〇〇万円以下の罰金に処される。また、同条一項四号の罪を犯した者が、その提供した電子メール広告中において、その受信者が送信者に対して受信拒絶の通知をするために必要な事項を表示しなかったときは、同法七二条二項により、一年以下の懲役または二〇〇万円以下の罰金に処される（事案により、懲役刑及び罰金刑を併科）。加えて、同条一項

四号の罪を犯した者が、著しく事実に相違する表示をし、若しくは実際のものよりも著しく優良であり、若しくは有利であると人を誤認させるような表示をしたときは、同法七二条二項により、同様に処罰される。これらの罰則の適用関係を整理すると、表1のとおりとなる。

表1　罰則の適用関係

	承諾のない者に対する電子メール送信	受信者から受信拒否通知を受けた後の電子メール送信	不当表示
通信販売電子メール広告をする販売業者又は役務提供事業者	一二条の三第一項	一二条の三第二項	一二条
通信販売電子メール広告受託事業者	一二条の四第一項	一二条の四第二項（一二条の三第二項を準用）	
連鎖販売取引を行う者等	三六条の三第一項	三六条の三第二項	三六条
連鎖販売取引電子メール広告受託事業者	三六条の四第一項	三六条の四第二項（三六条の三第二項を準用）	
業務提供誘引販売業を行う者	五四条の三第一項	五四条の三第二項	五四条
業務提供誘引販売取引電子メール広告受託事業者	五四条の四第一項	五四条の四第二項（五四条の三第二項を準用）	

(c) 罪数

特定電子メール適正化法に規定する罰則は、送信者情報を偽る行為（同法五条）に対するもの（同法三四条一号）及び措置命令（同法七条）に反する行為に対するものである（同法三四条二号）。

まず、送信者情報を偽る行為（同法五条）については、特定商取引法所定の罰則が適用される行為中に重なる部分がないので、他に特定商取引法違反行為が成立する場合でも、送信者情報を偽る罪は別個の行為であり、両罪の関係は併合罪（刑法四五条）となる。

他方、措置命令違反行為（特定電子メール適正化法七条違反行為）については、行政庁による是正措置の確保を主眼とするものであり、もし措置命令が適正に遵守された場合には特定電子メールの送信行為それ自体について違法があっても処罰されることはない。これに対し、特定商取引法に規定する罰則は、同法所定の事業者による電子メール送信行為の適法性確保を主眼とするものであって、行政庁による命令等に従って是正措置が講じられた場合であっても当該事業者の行為について違法性が失われるわけではなく、当該事業者の違法な送信行為等について処罰可能であるという状態に何ら変更はない。それゆえ、これらの罪は併合罪の関係にたつと解される。例えば、特定商取引法違反行為となるような承諾のない者に対する電子メール送信行為について特定電子メール適正化法七条所定の措置命令がなされたにもかかわらず送信者がその命令に従わなかった場合には、承諾のない者に対する電子メール送信の罪（特定商取引法違反の罪）と措置命令違反行為の罪（特定電子メール適正化法違反の罪）がいずれも成立し、両罪は、併合罪の関係にたつ。

(2) アメリカ合衆国法

アメリカ合衆国連邦法中で日本国の特定電子メール適正化法における同意を得ない商業宣伝広告目的電子メールの送信行為に対する処罰と類似する条項を有する法令は、既述の合衆国連邦法律集一八款一〇三七条（18 USC §1037）である。

同条のほか、関連する法例として、合衆国連邦法律集一五款七七〇四条（15 USC §7704）がある。同条(d)では、性的な事柄を含む商業宣伝広告目的電子メールの送信行為において、所定の方式[52]を遵守しないときは、五年以下の拘禁刑によって処罰するものとしている。その条文の原文のみ示し、仮訳は省略する。

［原文］

15 USC § 7704 - Other protections for users of commercial electronic mail

(d) Requirement to place warning labels on commercial electronic mail containing sexually oriented material

(1) In general

No person may initiate in or affecting interstate commerce the transmission, to a protected computer, of any commercial electronic mail message that includes sexually oriented material and–

(A) fail to include in subject heading for the electronic mail message the marks or notices prescribed by the Commission under this subsection; or

(B) fail to provide that the matter in the message that is initially viewable to the recipient, when the message is opened by any recipient and absent any further actions by the recipient, includes only–

(i) to the extent required or authorized pursuant to paragraph (2), any such marks or notices;

(ii) the information required to be included in the message pursuant to subsection (a)(5); and

(iii) instructions on how to access, or a mechanism to access, the sexually oriented material.

(2) Prior affirmative consent

Paragraph (1) does not apply to the transmission of an electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

(3) Prescription of marks and notices

Not later than 120 days after December 16, 2003, the Commission in consultation with the Attorney General shall prescribe clearly identifiable marks or notices to be included in or associated with commercial electronic mail that contains sexually oriented material, in order to inform the recipient of that fact and to facilitate filtering of such electronic mail. The Commission shall publish in the Federal Register and provide notice to the public of the marks or notices prescribed under this paragraph.

(4) Definition

In this subsection, the term "sexually oriented material" means any material that depicts sexually explicit conduct (as that term is defined in section 2256 of title 18), unless the depiction constitutes a small and insignificant part of the whole, the remainder of which is not primarily devoted to sexual matters.

(5) Penalty

Whoever knowingly violates paragraph (1) shall be fined under title 18, or imprisoned not more than 5 years, or both.

(3) EU法

EUの電子通信プライバシー保護指令（Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector）一三条は、商業宣伝広告目的の電子メールに関する禁止条項を含むものとなっている。EUの加盟各国は、同条の規定に基づき、必要な立法措置を構ずるべきものとされている。以下、仮訳を試みる。

電子通信プライバシー保護指令第一三条　求められていない通信(53)

1　ダイレクトマーケティング目的で、人間が関与しない自動着信システム（自動着信装置）(54)、ファクシミリ装置（ファックス）または電子メールを用いることは、事前の承諾を与えた申込者との関係においてのみ認められる。

2　第一項の規定にかかわらず、自然人または法人が、指令95/46/ECに従い、製品または役務の販売との関係でその顧客に対して電子メール送信をするための電子的な連絡先情報を取得している場合には、当該自然人または法人は、自己の類似製品または類似役務のダイレクトマーケティングのために顧客の連絡先情報を用いることができる。ただし、当該情報が収集される際において、または（当初はその情報の使用を拒絶していなかった場合には）個々のメッセージ送信の際において、当該顧客に対し、無料かつ容易な手段で当該連絡先情報の使用に対する異議を述べる機会が明白かつ適正に与えられている場合に限る。

3　加盟国は、第一項及び第二項に規定する場合を除き、関係する加入者(55)の同意のない場合及び求められていない通信の受信を望まない加入者と関連する場合のいずれにおいても、ダイレクトマーケティング目的の求められていない通信が許されないようにすることを無償で確保するための適切な措置を講じなければならない。これらの措置の選択

は、自国の立法によって定められる。

4　いかなる場合においても、その通信を行う送信者の同一性を偽装または隠蔽しながら、または、受信者がそのような通信の停止を求める送信をすることのできる正確なアドレスを欠く状態で、ダイレクトマーケティング目的の電子メールを送信する行為は、禁止されなければならない。

5　第一項及び第三項は、加入者が自然人である場合に適用される。加盟国は、共同体法及び適用可能な自国の立法の枠組みの中で、求められていない通信に関して自然人以外の加入者の正当な利益が十分に保護されるようにすることもまた確保しなければならない。

［原文］

Article 13 Unsolicited communications

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

2. Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

3. Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation.

4. In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

5. Paragraphs 1 and 3 shall apply to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected.

3　事例

商業宣伝広告目的による電子メール大量送信行為それ自体について有罪として処罰した裁判事例は、二〇一三年一一月末日現在で検索可能なものとしては、公式判例集等中に見当たらない。ただ、携帯電話のいわゆる「ワン切り」やスパムメールの大量送信等によって顧客を勧誘し、予めわいせつな音声等を記録していたサーバにアクセスさせ、そのわいせつな音声等を公然と陳列したとの犯罪事実につき有罪とした裁判事例（平成二三年法律第七四号による刑法一七五条改正前の事案）は存在する。

東京地裁平成一四年一〇月一八日判決（同地裁平成一四年（刑わ）一四九二号わいせつ物陳列被告事件・公式判例集等未登載）

（犯行に至る経緯）

被告人らは、共謀の上、東京都新宿区（以下略）所在の被告人X方に、性交時における男女の会話やその際の感情などを露骨な声音で表現したわいせつな音声を記憶させた、録音再生機と電話回線の連動した装置（コミュニケーションサーバ）を設置した上、同サーバから多数の携帯電話に電話をかけて瞬時に接続を切り、同サーバの電話番号をその携帯電話に着信記録として残すという方法（いわゆるワン切り）や、メール配信サーバから多数の携帯電話に対して上記コミュニケーションサーバの電話番号等を表示したメールを送信するという方法により、同サーバの電話番号等を広く宣伝し、顧客の注意を惹いて同サーバへのアクセスを勧誘した。

（犯罪事実）

被告人X、Y及びZは、共謀の上、平成一四年二月上旬ころから同年三月一日ころまでの間、同サーバに電話をかけてきたAら不特定多数の者に対し、同サーバに記憶させた上記わいせつな音声を再生して聴取させ、もって、わいせつ物を公然と陳列した。

（量刑）

被告人X及びY　懲役一年（執行猶予三年）

被告人Z　懲役一〇月（執行猶予三年）

四　マルウェア感染

1　問題点

一般に、電子的な手段の一種である電子メールを一般犯罪の遂行のために用いる場合、電子的手段を利用した犯罪の範疇に属するものと理解することができること、そのような意味でのサイバー犯罪には多種多様なものがあり得ることは既述のとおりである。そうした電子メールを利用した犯罪行為の中で、電子メールの本文がテキストとしてのみ存在している場合には、その意味内容を示すことが犯罪行為の一部分を構成する場合が多いと思われる。

ところが、HTML メールを含め、電子メールの本文に様々なプログラムやスクリプト等を組み込むことができ、当該電子メールをメールクライアントソフトウェアやブラウザ等で表示させたとたんに、当該電子メールに組み込まれたプログラムやスクリプトを自動実行したり、あるいはリンク先のサイトを自動表示させると共にそのサイトに設定してあるプログラムを自動実行させたりすることによって、当該電子メールをいわばトリガー（引き金）として、様々な犯罪行為を実行するように仕組むことは技術的に可能であるし、現にそのような事例が多数存在する。(56)

そのような電子メールをトリガーとして別の犯罪行為を実行するものの中で、今日その深刻さを増しているのは、フィッシング攻撃及びマルウェア感染であることは言うまでもない。(57) このようなサイバー犯罪は今後も更に手口が巧妙になり、被害が増大する可能性があるが、その中でも Ransom 攻撃と呼ばれる恐喝類似のサイバー犯罪による被害が増加しており、世界各国の警察当局も警戒を強めている。そこで、本論文では、Ransom 攻撃について特に述べる

ことにする。

2 Ransom 攻撃

(1) 攻撃の態様

Ransom 攻撃は、マルウェアを用いてパソコンやスマートフォン等の利用者からその制御を奪い、いわばパソコン等を乗っ取った上で、警察や著作権管理団体等を偽装した電子メール表示やサイト表示をさせ、罰金を支払わなければ当該パソコン等を破壊すると脅し、要求された金員を支払わなければ当該パソコン等のディスク記録内容を物理的に破壊したり使用不能状態にしたりするようなタイプの攻撃、または、マルウェアを用いてパソコン等の制御を奪い、その利用者が当該パソコン等を制御できない状態にした上で、当該利用者に対し、正常な状態に戻してほしければ金員を支払うべき旨を要求するタイプの攻撃などのことを意味する。[58][59] いわば利用者のパソコン等を人質にとり、解放金を要求する行為という攻撃態様から、「身代金要求攻撃」と呼ばれることもある。ただし、類似の行為または応用的な行為が多種類存在していることから、明確に定義をすることが難しいようなタイプの事例もある。[60]

Ransom 攻撃に用いられるマルウェアは、一般に、「ランサムウェア（Ransomware）」または「身代金要求型不正プログラム」と呼ばれている。[61] ランサムウェアの感染経路は多種多様であるが、電子メールに添付されたファイルから感染する場合や、電子メールから誘導されるサイト上で感染する場合などが比較的多いとされている。これらの場合、電子メールはマルウェア感染のための手段として位置づけることが可能であるが、Ransom 攻撃全体の流れの中でみると、攻撃を実効的に遂行するための利用者による制御を奪う行為の実行着手に相当すると評価することが可能であ

ろう。

そして、Ransom 攻撃による被害という側面から考察してみると、パソコン等を使用不能状態にされることは、機器類の物理的な毀損または機能的な毀損として財産権侵害になることは言うまでもない。しかし、それ以上に、現代社会において不可欠な情報財を記録した機器類を使用不能状態にされることにより、社会・経済上極めて重大な損失を発生させ得るものである。例えば、もし使用不能にされるパソコン等の記録媒体上に企業の営業秘密や特許発明技術その他の重要な情報財が記録されていた場合、その情報財が使用・実施不能状態にされてしまうことになることから、当該企業の生死を分けるような出来事が生ずる危険性さえある。他方、Ransom 攻撃の攻撃者からの要求に応じて被害者が金員を支払った場合、その支払額分だけの経済的損失が発生することは当然のことである。そして、そのような金員の支払は、恐喝または恐喝類似行為による犯罪者及び犯罪組織の資金源を増大させるという意味で、社会の安全にとって重大な脅威となる。

(2) 刑罰法令の適用

Ransom 攻撃には様々な態様のものが存在するし、攻撃者の意図（故意）の内容次第で成立する犯罪が異なるのも当然のことである。以下、典型的と思われるタイプのものを想定した上で、犯罪実行の段階を追って日本国の刑罰法令に基づく処罰可能性の有無を検討する。なお、以下の論述は、行為者に「正当事由」が何ら存在しない場合を前提としている。

(a) ランサムウェアの製造行為

まず、本論文においては、ランサムウェアの例として、原則として、被害者（個人または企業）が利用しているコ

ンピュータシステム内にあるハードディスクを無権限で暗号化してしまい、復号キーがないと当該ハードディスクを使用できない状態にしてしまうようなタイプのコンピュータプログラム（電磁的記録）を前提とする。このようなタイプのランサムウェアが不正指令電磁的記録（刑法一六八条の二第一項）に該当することについては異論がないと思われる。

ランサムウェアが不正指令電磁的記録に該当する場合、故意に[62]、その作成行為及び提供行為を実行した者は、三年以下の懲役または五〇万円以下の罰金に処される（同法一六八条の二第一項）。作成または提供を試みたものの、その作成または提供に失敗した場合には、未遂処罰条項がないので（同法一六八条の二第三項参照）、罪とならない。

なお、自己が作成するのではなく、故意に、第三者が作成したランサムウェアを取得した者またはこれを保管[63]した者は、二年以下の懲役または三〇万円以下の罰金に処される（同法一六八条の三）。未遂処罰規定はない。

(b) ランサムウェアの伝送行為

故意に、①ランサムウェアを電子メールに添付して送信し、その電子メールの受信者のシステムに当該ランサムウェアを感染させる行為、②特定のサーバにアクセスすべきことを内容とする電子メールを送信し、その電子メールの受信者を当該サーバにアクセスさせ、そのサーバからのダウンロードや当該サイトのブラウザ閲覧等により当該受信者に当該ランサムウェアを感染させる行為は、いずれも不正指令電磁的記録を実行の用に供する行為を構成するものと解される。この不正指令電磁的記録の供用行為を実行した者は、三年以下の懲役または五〇万円以下の罰金に処される（同法一六八条の二第二項）。その未遂行為も処罰される（同法一六八条の二第三項）。

なお、実行の着手時期について、①の場合は、遅くともランサムウェアを添付した電子メールの送信の時点で実行の着手があったと解することができる。これに対し、②の場合には、特定のサーバからランサムウェアを感染させる

ことができるようにした時点または当該サイトへアクセスすべきことを内容とする電子メールを送信した時点のいずれか早い時点で実行の着手があったと解することができる。そして、既遂時機については、当該ランサムウェアを電子メール受信者に感染させた時点である。被害者のシステムにランサムウェアを感染させれば足り、現実にランサムウェアとしての機能を実現していなくても、加害者がいつでも当該ランサムウェアを起動させ実行させることが可能になっていれば、供用行為としては既遂に達すると解される(64)。

加えて、②の場合において、当該サイトへアクセスすべき旨の記載内容が強要罪（同法二二三条）に該当する場合、当該電子メールの送信行為は不正指令電磁的記録供用罪の実行行為の一部であるので、事実行為としては同一の行為であり、強要罪との関係では、観念的競合（同法五四条一項）の関係にたつと解される。

(c)　ランサムウェアの感染により制御を奪う行為

感染したランサムウェアの実行により電子メール受信者のコンピュータシステムが使用不能状態になった場合、人の業務に使用する電子計算機である限り(65)、電子計算機損壊等業務妨害罪（同法二三四条の二第一項）が成立し得る。ただし、その既遂時機については、未遂罪処罰条項（同法二三四条の二第二項）(66)との関係で解釈が分かれ得るものの(67)、通説によれば、妨害の結果が現実に発生しなくともその危険が生じた時点で既遂に達するとしている(68)。

不正指令電磁的記録供用罪との罪数関係については、電子計算機損壊等業務妨害罪の既遂時機に関する解釈とのかねあいもあるが、刑法解釈学上のどの見解に立脚した場合でも遅くともランサムウェア感染の時点で電子計算機損壊等業務妨害罪の実行の着手があったと解すべきことについては異論がないであろうから、そのような理解を前提にすると、両罪は観念的競合（同法五四条一項）の関係にたつと解される(69)。

他方、当該コンピュータシステムが人の業務に使用するものとは認められない場合、当該コンピュータシステムが

動産として器物に該当する限り、ランサムウェアによって物理的に破壊する行為は、器物損壊罪に該当し得ると解する[70]。器物損壊罪が成立する場合、損壊行為を実行した者は、三年以下の懲役または三〇万円以下の罰金に処せられる（同法二六一条）。

器物損壊罪と不正指令電磁的記録供用罪との罪数関係については、電子計算機損壊等業務妨害罪の場合と同じである。

(d) 解放金名目に金員を要求する行為

ランサムウェアによってコンピュータシステムが使用不能状態にある場合に、金員を支払わなければ引き続き使用不能状態が継続するまたは当該コンピュータシステムが物理的に破壊されると脅し、金員の支払いを求める行為が恐喝罪（同法二四九条）に該当することについては異論がないと思われる。

恐喝罪が成立する場合、金員を喝取した者は、一〇年以下の懲役に処される（事案により、同法二四九条一項または二項）。未遂行為も処罰される（同法二五〇条）。

恐喝目的でランサムウェアを感染させるための電子メールを送信するというタイプの事例では、一般に、当該電子メール送信の時点で恐喝行為についても実行の着手があったと解するべきであろう[71]。被害者が要求に応じて金員を支払った時点（同条一項）または送金処理をした時点（同条二項）で既遂となる。

問題は、ランサムウェアの仕様にもよるが、①真実は暗号化されておらず正常に使用可能であるか、または、真実は簡単に暗号を解除でき使用可能状態に戻すことができるのに、そうではないと被害者が錯誤・誤信している状態を利用した場合、②真実は当該コンピュータシステムが既に物理的に破壊されており復旧しようがない状態にあるのに、金員を支払えば復旧のための復号キーを入手できると被害者が錯誤・誤信している状態を利用した場合、あるいは、③加害者には複合キーを提供するつもりが全くないのに、被害者が金員を支払えば交付するものと錯誤・誤信している

状態を利用した場合である。これらの場合については、事案にもよるが、詐欺罪と恐喝罪の観念的競合となるか、または、恐喝罪のみが成立するかが検討課題となる。(72) 通常は、恐喝罪のみが成立するものと解する。(73) ただし、③の場合において、加害者が当該ランサムウェアとは全く無関係な者であり、たまたま被害者がマルウェア感染により狼狽している状態にあることを知って、ランサムウェアを感染させた者のように装い、修復を約束して金員を要求したというような事案では、詐欺罪のみが成立する場合があり得ると考える。

なお、不正指令電磁的記録供用罪と恐喝罪との罪数については、金員要求行為を開始した時点で恐喝行為の実行の着手があったと認めるべき事案では、事実行為は二個になるが、牽連犯（同法五四条一項）ではなく併合罪（同法四五条）となると解すべきであろう。(74) 他方、不正指令電磁的記録供用の時点で恐喝行為の実行の着手があったと認めるべき事案では、事実行為は一個になり、観念的競合（同法五四条一項）となると解される。

五　まとめ

以上で本論文における検討を終える。

電子メールは、その汎用性のゆえに大きな社会的有用性を有していると同時に、犯罪者にとっても極めて便利な犯罪実行手段となり得るものである。本論文では、サイバー犯罪という観点から、主として電子メールそれ自体が犯罪構成要件の一部となっている場合及びそれに準ずるような場合に主眼をおいて法的課題に関する考察を行った。

しかしながら、現実に存在している犯罪事例では、電子メールを他の犯罪を遂行するための手段として用いるという態様のものが極めて多い。例えば、わいせつ画像や児童ポルノの伝送、詐欺、恐喝、ネットいじめのための違法な

内容の文章の伝送手段として電子メールを用いる例、多種多様なマルウェアを感染させるための添付ファイルの伝送手段として電子メールを用いる例等がその代表例であると言えるだろう。無論、これらも広い意味でのサイバー犯罪の一部を構成するものである。しかし、本論文においてその全部を詳述することは不可能である。本論文では、いわゆるスパムメール対策及び近時深刻な被害を発生させつつある Ransom 攻撃についての検討結果を示した。

電子メールを利用したサイバー犯罪の中で Ransom 攻撃以外の類型に属する犯罪行為に関しては、フィッシング攻撃[75]やスパイウェア[76]との関連で既に別稿において論じた部分を除き、他日を期したい。[77]

注

（1） Convention on Cybercrime (CETS No.185)
http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185［二〇一三年一一月一六日確認］

（2） 電子メールの送受信のために用いられる技術的データは、物理的な郵便物でいえば宛名や差出人の情報と同じ社会的機能を有するものであり、電子メールの送受信にとって不可欠の構成要素である。送受信データが電子メールサーバ等に通信履歴として記録される場合、そのような履歴データはトラフィックデータ（traffic data）と呼ばれることがあり、サイバー犯罪条約においてもこのような用例が見られる。トラフィックデータは、通信文本体（content data）とは区別され、捜査機関によってそれらが捜索・押収される場合、そのような捜査活動に伴うプライバシー侵害の程度・内容が異なることから、サイバー犯罪条約中の刑事訴訟手続に関する条項でも異なる取り扱いが規定されている。また、電子メールサーバ等に通信履歴として記録されるものと記録されないものとを含め、メタデータ（meta data）と呼ばれることもある。電子メールの通信文（本文）を本体として観念した場合、本体としての通信文データとの関係において隠された技術的データという意味で「メタ」という相対関係があることになるので、この名がある。元 CIA 職員により情報リークがなされた結果、米国諜報機関による電子メール等の通信傍受及びデータ収集が大きな議論を呼んでいることは周知のとおりである。ただし、米国諜報機関の説明によれば、傍受・収集された通信データの大半は、テロリスト容疑者の電子メールアドレスや IP アドレス等が送受信先となっている通信に対する傍受などのように特に集中的に通信傍受がなされた事例を除き、そのような意味でのメタデータであったとされている。詳細は不明である。

（3）　通信文（本文）を一文字も含まず、添付ファイルのみが付された電子メールを想定してみると、電子メール通信という技術が、いわばファイル伝送のためのコンテナとしての役割だけを果たしているということを理解することができる。

（4）　夏井高人「サイバー犯罪の研究（一）―DoS 攻撃（DDoS 攻撃）に関する比較法的研究」法律論叢八五巻一号一九七頁

（5）　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」法律論叢八六巻一号六一頁

（6）　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」法律論叢八六巻二・三合併号八五頁

（7）　夏井高人「サイバー犯罪の研究（二）―フィッシング（Phishing）に関する比較法的検討」法律論叢八五巻四・五号一七九頁、同「サイバー犯罪の研究（三）―通信傍受に関する比較法的検討」法律論叢八五巻六号三六三頁

（8）　このことは、例えば、宅配便によって麻薬を運搬したという事例を想定してみると容易に理解することができる。このような場合、その宅配便による搬送のために用いられたパッケージそれ自体としては違法なものではなく、価値中立的なものであって、単に具体的な事案において犯罪の用に供されたというだけのことであるので、犯罪組成物件（刑法一九条一項一号）ではなく、犯罪供用物件（同条一項二号）として没収の対象となり得るというのに過ぎない。このことは、物体の場合だけではなく、電子的な仕組みである電子メールを利用して何らかの犯罪が実行された場合でも同じである。

（9）　警察庁生活安全局長「ストーカー行為等の規制等に関する法律の一部を改正する法律の施行について（通達）」（平成二五年七月三日警察庁丙生企発第七六号）

（10）　解釈論としては、ストーカー行為規制法二条一項一号所定の「つきまとい」行為の一類型として認識することも可能であるので、仮に同法二条一項四号に「電子メール」の送信行為が規定されていなかったとしても、つきまとい行為等の一種として扱うことが可能であると解される。このような理解を前提とする場合、同法二条一項四号の規定は、注意的に構成要件要素を明確にするための条項であると解釈することになり、結果的に、電子メールによるつきまとい行為は、①固有のサイバー犯罪ではなく②電子的手段を利用した犯罪の範疇に属するということになる。なお、ストーカー行為等の規制等に関する法律の一部を改正する法律（平成二五年法律第七三号）によるストーカー行為規制法一部改正前の事案であるが、東京高等裁判所平成一四年一二月一七日判決・判例時報一八三一号一五五頁は、私用パソコンから電子メール送信をしたという事案について、ストーカー行為規制法二条一項一号所定のつきまとい行為に該当するとの判断を示している。

（11）　ここでいう「違法性を有する」とは、電子メールが犯罪構成要件要素となっている場合は無論のこと、構成要件要素となっ

ていない場合でも犯罪を実行するための主要な手段として電子メールが犯罪の用に供された場合を広く含む趣旨である。電磁的記録としての電子メールそれ自体が没収の対象となった刑事裁判事例については詳らかではないが、理論的には没収の対象となり得るという意味で、犯罪の実行の用に供された電子メールは違法な存在である。

（12） CC メール及び BCC メールでは特定多数の受信者に対して同時に同一内容の電子メールが送信されるが、これらの送信方法では複数の電子メールが電子的に同時送信処理されるというだけのことであり、基本的には特定の送信者から特定の受信者に対する通信であることに何ら変わりはない。

（13） 正確には、架空の受信者宛に大量の電子メールを同時送信すると、その電子メールを処理する電子メールサーバに一定の負荷をかけることになるが、現在のコンピュータシステムや通信回線の能力からすると、DoS 攻撃をしかけた場合と同程度の支障が発生することはまずないと考えてよい。むしろ、当該電子メールの不達の通知がほぼ同時に集中して送信者のシステムに配達されることになることから、送信者データが実在する正確なものであり、かつ、送信者のコンピュータシステムや通信回線の能力が十分でない場合には、送信者に何らかの支障が生ずることはあり得る。この場合、送信者データ（電子メールアドレスまたは IP アドレス）が第三者による詐称ではなく、送信者自身の正確なものであるとすれば、不達通知の集中受信によって何らかの損失が発生したとしても、それは送信者自身の自業自得ともいうべきことである（民事損害賠償責任の問題としては、仮に不達通知システムの設計・運用等に何らかの過失があり、その過失行為と送信者の損失との間に相当因果関係が認められる場合であっても、送信者の損害額全額について過失相殺すべきものであろう。）。

（14） 通常は、送信者が利用している電子メールクライアントアプリケーションと電子メールサーバ間の通信が正常に確立されないため、電子メールの送信処理が実行されないで終わることが多いと思われる。

（15） そのような結果を意図的に狙ったサイバー攻撃があり得る。例えば、電子メールではなくパケットレベルのことではあるが、応用的なサイバー攻撃の手法の一つとして、DNS リフレクション攻撃または DNS アンプ攻撃（DNS Amplification Attack）というものがある。これらの攻撃手法は、全体としてみると、DDoS 攻撃の手口の一部を構成していることが多い。警察庁は、「DNS の再帰的な問い合わせを悪用した DDoS 攻撃手法の検証について」（平成一八年七月一一日）、「DNS リフレクション攻撃に対する注意喚起について」（平成二五年四月一一日）及び「中国を発信元とする再帰問い合わせ可能な DNS サーバの探索行為の増加について」（平成二五年九月一一日）を発し、日本国においても現実に DNS リフレクション攻撃が実行される危険性について注意喚起をした。DNS リフレクション攻撃によりコンピュータシステムの運用に支障が発生したときまたはその危

険性が発生したときは、電子計算機損壊等業務妨害罪の成否が検討されることになる。

（16）　EC-Council, Computer Forensics: Investigating Network Intrusions and Cyber Crime, Cengage Learning, 2010, Chapter 7

（17）　岡村久道・近藤剛史『インターネットの法律実務［新版］』（新日本法規、二〇〇一）五二三～五三二頁、宗田貴行『迷惑メール規制法概説』（レクシスネクシス・ジャパン、二〇〇六）九～七二頁、岡村久道ほか「パネルディスカッション：電子メール法制をめぐる諸問題」情報ネットワーク・ローレビュー二巻七九～一三九頁、平野 晋「迷惑メールに関する米国法との比較法的考察」法とコンピュータ二一号二五頁、大磯 一「法令解説：迷惑メール対策 直罰規定の導入等、特定電子メール法による取締りの強化–特定電子メールの送信の適正化等に関する法律の一部を改正する法律」時の法令一七四四号六頁

（18）　いわゆる「なりすまし」や未成年者の詐術によりネット上で契約が締結された場合の民事上の法律効果等については、経済産業省「電子商取引及び情報財取引等に関する準則（平成二五年九月）」i 四一～六一頁。

（19）　加害者の追跡を困難にするための手法が送信者データの詐称のみに限定されるものでないことは言うまでもない。様々な手口が存在する。詐称された場合を含め、真の送信者を追跡し割り出すための手法については、Sherri Davidoff & Jonathan Ham, Network Forensics: Tracking Hackers through Cyberspace, Prentice Hall, 2012, pp. 23–157 が参考になる。

（20）　電気通信事業法二条二号は、「電気通信設備」について「電気通信を行うための機械、器具、線路その他の電気的設備をいう」と定義している。また、同法二条一号は、「電気通信」について「有線、無線その他の電磁的方式により、符号、音響又は影像を送り、伝え、又は受けることをいう」と定義している。特定電子メール適正化法二条二号は、「電気通信設備」の定義として電気通信事業法二条二号における定義を借用する形式で立法されているだけであるので、特定電子メール適正化法に規定する特定電子メールが電気通信事業者によって媒介される電子メールに限定されるという趣旨ではない。電気通信事業者によって媒介されるものであると否とを問わず、日本国内にある電気通信設備から送信される電子メール及び日本国内にある電気通信設備に対して送信される電子メールは、全て特定電子メールに該当し得る。例えば、電気通信事業者を介さないで特定の施設内の設備や移動式の車両等から企業や個人の電気通信設備に対して直接に電磁的方式を用いて電子メールが送信されるような場合にも特定電子メールに該当することがあり得る。

（21）　ただし、「契約の申込みをした者又は契約を締結した者に対し当該契約の申込み、内容又は履行に関する事項を通知するために送信される電子メールにおいて広告又は宣伝が付随的に行われる場合」、「電子メールの受信をする者に対し広告又は宣伝が

行われることを条件として提供される電子メール通信役務を用いて電子メールが送信される場合であって、その電子メールにおいて当該電子メール通信役務の提供をする者により広告又は宣伝が付随的に行われる場合」及び「前二号に掲げる場合のほか、広告又は宣伝以外の行為を主たる目的として送信される電子メール（電子メールの受信をする者の意思に反することなく送信されるものに限る。）において広告又は宣伝が付随的に行われる場合」（同規則六条）については、同法三条三項ただし書に規定する受信拒否者に対する例外的な場合として適用除外となる。これらの条項は、かなりゆるやかに解釈することが可能である。そのため、電子メールの受信拒否に関する限り、特定電子メール適正化法は、いわゆる「ザル法」として消費者保護のために十分に機能しない可能性がある。

（22）　特定電子メールの送信の適正化等に関する法律施行規則（平成一四年総務省令第六六号）七条は、①不特定の者によって受信されることを目的とする電気通信の送信（公衆によって直接受信されることを目的とする電気通信の送信を除く。）の用に供される電気通信設備（特定電気通信設備）のうち受信拒否の通知を受けるための用に供する部分（当該通知をするために必要な情報の明確かつ平易な表現による提供その他の方法により特定電子メールの受信をする者が当該通知を容易に行うことを可能とするために必要な電磁的記録を保存したものを含むものに限る。以下この条において「通知受領部分」という。）をインターネットにおいて識別するための文字、番号、記号その他の符号または②前号に規定する符号に対応させた文字、番号、記号その他の符号であって、特定電子メールの受信をする者が当該符号を用いてその使用する通信端末機器により通知受領部分に接続できるものと規定している。

（23）　特定電子メールの送信の適正化等に関する法律施行規則九条は、原則として、①特定電子メールの送信をしないように求める旨の通知を、法第四条第二号に掲げる電子メールアドレスをそのあて先とする電子メールの送信をすることにより、または、同規則八条に定める文字、番号、記号その他の符号を用いることにより行うことができる旨、②当該送信者（当該電子メールの送信につき送信委託者がいる場合は、当該送信者又は当該送信委託者のうち当該送信に責任を有する者）の住所及び③特定電子メールの送信についての苦情、問合せ等を受け付けることのできる電話番号、電子メールアドレス又は特定電気通信設備のうち苦情、問合せ等の受付の用に供する部分をインターネットにおいて識別するための文字、番号、記号その他の符号若しくはそれに対応させた文字、番号、記号その他の符号であって特定電子メールの受信をする者が当該符号を用いてその使用する通信端末機器により当該部分に接続できるものを表示すべきものと規定している。

（24）　従来、電子メールは文字などの符号を送信するための電子的な手段として構築・利用されてきた。そのため、電子メールは

二次元的なものであるとの固定観念が定着しており、そのために電子メール関連立法の全てが二次元的な画面表示を前提とするものとなっている。しかし、現在、三次元プリンタ（3D printer）技術の発達により、通信は二次元的な要素で構成されるものだけではなく三次元的な要素を含むものへと変容を遂げつつあるのであり、その結果として、受信内容が画面表示ではなく何らかのかたちでの空間での状態形成といったような現象を含むものとなりつつある。また、量子コンピュータによる通信の場合には、従来の電子メールとは異なる方式による電磁的通信が実行されることになるかもしれない。これらのような場合を含め、急速な社会環境の変化に対応した適切な立法論的検討が進められなければならないと考える。

（25）　特定電子メール適正化法二条四号は、「架空電子メールアドレス」について、「多数の電子メールアドレスを自動的に作成する機能を有するプログラム（電子計算機に対する指令であって、一の結果を得ることができるように組み合わされたものをいう。）を用いて作成したものであること」及び「現に電子メールアドレスとして利用する者がないものであること」の両方の要件を充足する電子メールであると定義している。前者の要件が存在するため、コンピュータプログラムによって自動生成されたものではなく手作業で作成された虚偽の電子メールアドレスは、たとえそれが巨大な人海戦術により多数作成されたものであっても「架空電子メールアドレス」ではないことになる。この点については議論があり得る。また、後者の「現に電子メールアドレスとして利用する者がないものであること」については、偶然の出来事として現に電子メールアドレスとして利用する者が存在したとしても、電子メールアドレスを生成する者がその事実の有無を確認する意思を有せず、偶然の一致がある場合に意識的に現実に存在する電子メールアドレスを排除しなかった場合には、後者の要件を充足するものと解する。そのように解するのでなければ、特定電子メール適正化法六条に規定する禁止が空文化することが明らかである。なお、プライバシー保護等の目的により、プロキシサーバその他の匿名化のための電子的な仕組みを用いて電子的に自動変換された電子メールアドレスは、特定単数の電子メールアドレスであり、かつ、実在する電子メールアドレスであるので、特定電子メール適正化法所定の「架空電子メールアドレス」に該当しないことは言うまでもない。

（26）　特定電子メール適正化法一一条は、送信者情報を偽る電子メールに対して電気通信事業者が技術的な対応策を講ずる場合の適法性の根拠として、「電気通信事業者は、送信者情報を偽った電子メールの送信がされた場合において自己の電子メール通信役務の円滑な提供に支障を生じ、又はその利用者における電子メールの送受信上の支障を生ずるおそれがあると認められるとき、一時に多数の架空電子メールアドレスをそのあて先とする電子メールの送信がされた場合において自己の電子メール通信役務の円滑な提供に支障を生ずるおそれがあると認められるとき、その他電子メールの送受信上の支障を防止するため電子メー

ル通信役務の提供を拒むことについて正当な理由があると認められる場合には、当該支障を防止するために必要な範囲内において、当該支障を生じさせるおそれのある電子メールの送信をする者に対し、電子メール通信役務の提供を拒むことができる」と規定している。すなわち、この場合には、電気通信事業者による役務提供拒否行為について違法性阻却事由が存在することになる。なお、携帯電話の特定接続サービス契約に基づき大量の架空アドレス宛電子メール送信の送信回数に相当する損害の賠償を命じた事例として、東京地裁平成一五年三月二五日・判例時報一八三一号一三二頁があり、また、符号等をランダムにあてはめて生成された大量の架空電子メールアドレス宛の電子メール送信の差止め仮処分を認めた事例として、横浜地裁平成一三年一〇月二九日決定・判例時報一七六五号一八頁がある。

（27） 一般に、犯罪組織は、犯罪行為によって経済的な利益を得ている。経済学的には、利益または収益として計上されるべきものであるし、反復継続してそのような行為を営む組織は営利的な組織であるということが可能であるかもしれない。しかし、法的には、そのような利益または収益は非合法なものとして没収されまたは被害者へ還付されるべきものである。それゆえ、特定電子メール適正化法の解釈に当たっては、このような犯罪組織を営利団体であると解することができない。

（28） 前掲夏井「サイバー犯罪の研究（二）」一九〇～一九一頁

（29） なお、15 USC §7703 も参照されたい。

（30） ［訳注］州内の犯罪行為については、連邦刑法ではなく、各州の刑法が適用される。連邦の刑法は、州をまたがる取引及び国際取引と関連する犯罪行為について適用される。

（31） ［訳注］虚偽内容の申請書類を提出して別人になりすましたアカウントやドメイン名を取得する場合だけではなく、アカウントやドメイン名を登録するサーバに無権限アクセスし、無権限で虚偽内容のデータを登録してアカウントやドメイン名を取得する行為を含む趣旨と理解することができる。

（32） ［訳注］合衆国連邦刑法一〇三〇条の仮訳は、前掲夏井「サイバー犯罪の研究（四）」八一頁以下にある。

（33） ［訳注］合衆国連邦刑法または州刑法によりコンピュータ犯罪を実行した者として拘禁刑に処罰されたことのある再犯者を重く罰する趣旨の規定である。日本国の現行刑罰法令中には、このような例はない。

（34） ［訳注］電子メールサービスの提供者のことを意味する。クラウドコンピューティングサービスを基盤とする Web メールサービス提供者の場合や SNS におけるメッセージ交換サービス提供者等も含まれるものと解される。

（35） ［訳注］警察のことを意味する。

（36）本論文中で紹介する措置命令事例は、網羅的ではない。なお、一般財団法人日本データ通信協会迷惑メール相談センターのサイト内にある「総務省における行政処分実施状況」では、過去の措置命令事例を一覧表示して、その情報を提供している。

総務省における行政処分 実施状況

http://www.dekyo.or.jp/soudan/activities/mic.html［二〇一三年一一月一六日確認］

（37）いわゆる「出会い系サイト」には固有の社会的問題または法的問題が存在する。参考になる裁判事例としては、東京高裁平成二三年六月一四日判決・東京高裁（刑事）判決時報六二巻五二頁、大阪高裁平成一六年九月二四日判決・家裁月報五七巻七号四五頁、福岡高裁平成二〇年二月八日決定・家裁月報六〇巻八号六六頁、新潟地裁長岡支部平成一四年一二月二六日判決・刑集六〇巻五号四三〇頁、東京地裁平成一七年一二月一六日判決・判例時報一九三二号一〇三頁、福岡高裁平成一七年九月一四日判決・判例タイムズ一二二三号一八八頁などがある。それとは別に、「出会い系サイト」を装い、実際には女性ではないのに女性を装った男性等のサクラを用い、利用料金名目に金員を詐取することを目的として運営されているサイトも存在している。この点については、岡村久道編『インターネットの法律実務―理論と実務』（新日本法規出版、二〇一三）三七八頁［川村哲二］を参照されたい。

（38）この判決は、二〇一一年四月二九日付け毎日新聞京都版に掲載された報道記事によりその存在を知ることができる。ただし、判決文（原文）を入手することができないので、認定事実等の内容に関する正確性は保障できない。京都地方裁判所及び京都地方検察庁に対する問い合わせ結果によると、この事件の確定判決は存在し、その原本を同検察庁で保管しているが、判決原本を公開することはできず、今後も公開する予定はないとのことであった。なお、他の報道記事等によれば、この事件で問題となったサイト運営会社ユニバーサルフリークスは、事件後、解散したようである。

（39）総務省総合通信基盤局消費者行政課・消費者庁取引対策課「特定電子メールの送信等に関するガイドライン」（平成二三年八月）

http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/pdf/m_mail_081114_1.pdf［二〇一三年一一月一六日確認］

（40）いわゆるCRM（Customer Relationship Management）の場合を含め、商業宣伝広告のための電子メール送信によって売り上げを大幅に増加させることができるというビジネスモデルそれ自体が単なる幻想の一種であった可能性がある。しかしながら、この点に関する社会学的な調査はほとんどなされていないというのが実情である。

（41）拒否しても繰り返し送信されてくる電子メールについては、商業宣伝広告目的であると否とを問わず、いわゆる迷惑メール

の一種であり、悪質なものについてストーカー行為の一種として処罰対象とされることになった。この点については、前掲警察庁生活安全局長「ストーカー行為等の規制等に関する法律の一部を改正する法律の施行について（通達）」三～四頁で解説されているとおりである。なお、この通達では、「①その全部若しくは一部においてSMTPが用いられる通信方式を用いるもの、又は②携帯して使用する通信端末機器に、電話番号を送受信のために用いて通信文その他の情報を伝達する通信方式を用いるものをいうと解される。①にはパソコン・携帯電話端末によるEメールのほか、Yahoo!メールやGmailといったウェブメールサービスを利用したものが含まれ、②にはSMS（携帯電話同士で短い文字メッセージを電話番号宛てに送信できるサービスをいう。）が含まれるものと解されるが、例えば、Facebookやmixi等におけるメッセージ機能等のうち上記①又は②に該当しないものであれば、含まれないものと解される」との法解釈が示されている。

（42）　特定電子メール適正化法三条に規定する送信の禁止は、送信者情報を偽ることなく正当に商業宣伝広告目的の電子メールを送信する場合に適用される。

（43）　特定電子メール適正化法と同じ立法目的を有する法令の執行担当官庁だけに限定されるので、例えば、外国の諜報機関や軍等のように国防目的で存在している国家機関に対する情報提供の場合を含まないと解される。

（44）　国際的なテロリストとして殺人行為等の犯罪捜査の目的となっている場合、その行為が「政治犯罪」に含まれるものと解するべきかどうかについては慎重な考慮が必要となる場合があり得る。

（45）　もっとも、立法技術の問題としては、関連する省庁の共同所管として、統合された電子メール法を立法することは可能であるし、そのほうが一般国民にとってわかりやすいことは言うまでもない。

（46）　消費者庁取引物価対策課・経済産業省商務情報政策局消費経済政策課『平成二一年版　特定商取引に関する法律の解説』（商事法務、二〇一〇）一一三頁、齋藤雅弘・池本誠司・石戸谷豊『特定商取引法ハンドブック［第四版］』（日本評論社、二〇一〇）二九二頁

（47）　特定商取引に関する法律施行規則一一条の六は、「電子メールアドレス（相手方が通信販売電子メール広告の提供を受けない旨の意思を表示することができるものに限る。）」または「電子情報処理組織において識別するための文字、記号その他の符号若しくはこれらの結合（電子計算機に入力されることによって当該電子計算機の映像面に表示される手続きに従うことにより、相手方が通信販売電子メール広告の提供を受けない旨の意思を表示することができるものに限る。）又はこれに準ずるもの」を「当該通信販売電子メール広告の本文に容易に認識できるように表示しなければならない」と規定している。

（48）　連鎖販売契約は、初期においてはマルチ商法やねずみ講として社会問題化し、その後、日本アムウェイをめぐり名誉毀損事件等が提起された。連載販売契約においても電子メールを用いた商業宣伝広告がなされることがある。これらの点については、前掲『特定商取引法ハンドブック［第四版］』四四八頁以下（特に四七〇頁以下）を参照されたい。

（49）　特定商取引に関する法律施行規則二七条の四は、「電子メールアドレス（相手方が連鎖販売取引電子メール広告の提供を受けない旨の意思を表示することができるものに限る。）」または「電子情報処理組織において識別するための文字、記号その他の符号若しくはこれらの結合（電子計算機に入力されることによって当該電子計算機の映像面に表示される手続きに従うことにより、相手方が連鎖販売電子メール広告の提供を受けない旨の意思を表示することができるものに限る。）又はこれに準ずるもの」を当該連鎖販売取引電子メール広告の本文に容易に認識できるように表示しなければならないと規定している。

（50）　業務提供誘引販売取引は、内職商法やモニター商法として社会問題となっている。様々な態様のものがあり、中には完全な詐欺行為に該当するものもあるが、詐欺行為に該当しないものでも消費者保護の観点からすると深刻な問題のある事例が珍しくない。業務提供誘引販売取引においても商業宣伝広告電子メールが用いられることがしばしばある。これらの点については、前掲『特定商取引法ハンドブック［第四版］』五五四頁以下（特に六二七頁以下）を参照されたい。

（51）　特定商取引に関する法律施行規則四二条の四は、「電子メールアドレス（相手方が業務提供誘引販売取引電子メール広告の提供を受けない旨の意思を表示することができるものに限る。）」または「電子情報処理組織において識別するための文字、記号その他の符号若しくはこれらの結合（電子計算機に入力されることによって当該電子計算機の映像面に表示される手続きに従うことにより、相手方が業務提供誘引販売取引電子メール広告の提供を受けない旨の意思を表示することができるものに限る。）又はこれに準ずるもの」を「当該業務提供誘引販売取引電子メール広告の本文に容易に認識できるように表示しなければならない」と規定している。

（52）　「Advertisement」を省略した表現である「ADV」との符号を電子メールの表題部に付すべきものとされている（15 USC §7710）。

（53）　「unsolicited」という表現は、いわゆる迷惑メール一般について見られる英語表現であるが、とりわけ商業宣伝広告目的で一方的に送りつけられてくる電子メールについて「unsolicited email message」等として用いられることが多い。受信者が送信を求めていないのに、求められていない送信者から送信されてくるという意味合いである。

（54）　［訳注］電話交換手の手作業による接続ではなく電話交換機等によって自動的に接続される電話システムのことを意味する。

（55）［訳注］「subscriber」は、電話の場合には電話サービス契約加入者となる。電子メール受信者の場合には当該電子メールサービスの利用者ということになるが、ここでは便宜「加入者」と訳することにした。指令それ自体が電話サービス契約加入者に限定するものでないことは文脈上明らかである。

（56）問題のない電子メールにマルウェア感染させる手法としては、クラウドベースのメールサービスではクラウドサーバに不正アクセスした上で、マルウェア感染させるような不正指令電磁的記録を当該サーバ内に組み込み、そのサーバを介して送受信される電子メールにマルウェアを感染させる手法、あるいは、スマートフォン上で機能するメールクライアントアプリとしてマルウェア感染用に製造された不正指令電磁的記録を流通させ、当該アプリによって処理される電子メールにマルウェアを感染させる手法などもある。同様に、電子メールの本文を作成するための文書作成アプリケーション（Microsoft Word や Adobe Acrobat 等）の汚染という手口もある。そして、そのような場合には、マルウェアを感染させられた電子メールが更に他所に感染を拡大させることともなり得る。これらのような手法が用いられても、単純に電子メールがマルウェア感染しているだけの場合にはセキュリティソフトやウイルス検知ソフト等によって感染の検知・検出をすることが可能である。しかしながら、利用者が使用しているパソコンやスマートフォンにインストールされているオペレーティングシステム（Android、iOS、Windows 等）の根幹部分を汚染し支配を奪ってしまうようなマルウェアの場合、セキュリティソフト等による検知・検出を無効にされてしまうことがあることに留意すべきである。

（57）脚注（7）参照

（58）使用不能状態にする手法としては、無権限でディスク全体を暗号化してしまう方法がある。この場合、金員支払の要求に応じれば暗号化され使用不能状態にされたディスク等を復号して使用可能状態に復旧させるための復号キーを渡すとの通知を受けるといったかたちで Ransom 攻撃が実行される。ただし、要求された金員を支払っても復号キーが送付されることがない場合が多く、その点では恐喝と詐欺が複合したような犯罪類型である場合がある。

（59）トレンドマイクロ社が二〇一三年一〇月三日及び同月二三日に広報した攻撃実例として、次のような記事がある。

「QUERVAR」、「RANSOM」および「ZACCESS」が連携する攻撃を確認
http://blog.trendmicro.co.jp/archives/6066［二〇一三年一一月二九日確認］
ランサムウェア「CryptoLocker」、オンライン銀行詐欺ツール「ZBOT」を経てコンピュータに侵入
http://blog.trendmicro.co.jp/archives/8017［二〇一三年一一月二九日確認］

（60）　犯罪行為として理解する際には、当該攻撃の主要な構成要素を分析的に検討すると同時に、行為全体としての流れに着目してその行為の目的及び犯罪的結果を総合的に評価する必要がある。これらの考察によって、複数の異なる犯罪の複合として理解すべきか、それとも、全体として一個の恐喝行為または詐欺行為等を構成するものと理解すべきかを判断すべきである。

（61）　「CryptoLocker」と名づけられたプログラムが有名であり、世界各地で多数の甚大な被害を発生させている。なお、実際には、他の複数のマルウェアなどの電子的攻撃手段が組み合わされた複合的な攻撃として実行されるのが一般的であるので、単体のランサムウェアだけが問題となることは比較的少ない。

（62）　プログラムの設計を誤った場合、または、バグなどの不具合を発見できなかった場合などのように、故意なく、ランサムウェアと同様の機能を営むソフトウェアを作成しても不正指令電磁的記録の作成罪及び提供罪は成立しない。この場合、民事上の損害賠償責任（債務不履行または不法行為）が問題となり得るのみである。この点については、前田雅英・松本時夫・池田　修・渡邉一弘・大谷直人・河村　博編『条解刑法［第三版］』（弘文堂、二〇一三）四七〇頁、西田典之『刑法各論［第六版］』（弘文堂、二〇一二）三九二頁参照。

（63）　Webメールサービスやクラウド型メールサービスの場合を含め、電子メールサーバ内のメールボックスにランサムウェアを添付した電子メールが記録されたまま受信者によってダウンロードされていない状態のときは、形式的には当該電子メールサーバの管理者の保管状態にあるのと同じことになるが、故意が認められない限り、当該管理者やサービス提供者について不正指令電磁的記録保管罪は成立しない。ただし、管理者であるエンジニア等の従業者が、ランサムウェアが添付されている電子メールであることを検知して認識した上で、それを私的に取得する目的で、無権限でその電子メールの複製物を取得したときは、故意による取得罪が成立すると解される。ただし、プロバイダが認識しつつも不作為で放置した場合に、故意を認定すべきかどうかについては慎重な検討を要するが、当該業者として合理的な期間内に合理的な対応をとらなかった場合などには、問題となり得る。

（64）　前掲前田『条解刑法［第三版］』四六八頁

（65）　電子計算機損壊等業務妨害罪が成立しない場合でも、器物損壊罪（刑法二六一条）の成否は問題となり得る。ランサムウェアがハードディスクを暗号化するだけの機能を有する場合、復号キーさえあれば直ちに復旧させて使用可能状態とすることができるから、器物を損壊したと解するのは困難ではないかと思われる（使用不能とされた結果として業務妨害罪が成立し得ることは別である。）。これは、金庫の鍵を隠して開錠できなくしてしまった場合、当該金庫を損壊したとは言い難いということ

からも理解できる。現行刑法は、私人が所有・占有する動産等の利用を阻害する行為については明確に定めていないと解するのが正しい。立法的検討を要する。ただ、ランサムウェアがハードディスク上のデータを消去し復旧不可能な状態にする機能を有する場合にはまた別の考慮を要する。この点については、東京地裁平成二三年七月二〇日判決（同地裁平成二二年（刑わ）二一五〇号・平成二二年（刑わ）二六五一号・公式判例集等未搭載）が参考になる。この判決は、コンピュータウイルスによってハードディスクを使用不能にし、その効用を損なわせた行為をもって器物損壊罪の成立を認めている。判例評釈として、園田寿「判例批評「イカタコ事件」（東京地判平成23．7．20公刊物未登載）について―器物損壊罪における「損壊」の概念」甲南法務研究八巻一〇三頁がある。

（66）　前掲前田『条解刑法［第三版］』七〇六頁

（67）　前掲夏井「サイバー犯罪の研究（一）」二一〇頁

（68）　前掲前田『条解刑法［第三版］』七〇四頁。なお、前掲西田『刑法各論［第六版］』一三二頁は「外形的混乱」が生じた時点であるとしている。

（69）　前掲前田『条解刑法［第三版］』四七二頁

（70）　脚注（65）参照

（71）　不正指令電磁的記録供用の故意しか有していなかった者が、マルウェア感染により被害者が心理的に動揺していることを知り、その後に、被害者の動揺に乗じて金員を喝取しようとの故意を有するに至ったという事案では、恐喝罪の実行着手時期は後の時点となる。

（72）　山口 厚『刑法各論［第二版］』（有斐閣、二〇一〇）二八七頁

（73）　最高裁昭和二四年二月八日判決・刑集三巻二号八三頁

（74）　最高裁平成一九年八月八日決定・刑集六一巻五号五七六頁

（75）　前掲夏井「サイバー犯罪の研究（二）」一八八頁

（76）　前掲夏井「サイバー犯罪の研究（三）」三八〇頁

（77）　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。