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　第八五巻　第六号（二〇一三・二）

【論　説】

サイバー犯罪の研究（三）

――通信傍受に関する比較法的検討――

夏井高人

目　次

一　はじめに

一般に、通信傍受とは、他人間の通信に対する無権限の介入行為（通信内容への無権限アクセス及び通信内容の無権限取得）を意味する。(1)その反対解釈として、一般に、通信傍受の対象が「他人間の通信」である以上、通信当事者の一方または双方が通信内容にアクセスしまたはこれを取得する行為は通信傍受とはならないと解されている。(2)同様に、第三者が通信当事者の一方または双方の同意を得てその通信当事者の通信内容にアクセスしまたはこれを取得する行為も通信傍受とはならないと解されている。(3)そのような一般的な理解を前提に、日本国の電気通信事業法等における「通信の秘密」に対する侵害罪が構成されている。(4)

通信の秘密に関するこのような理解は、歴史的・技術的制約に起因する部分があると思われる。一般に、コンピュー

タが普及しインターネット（ＴＣＰ／ＩＰ）を用いた電気通信が一般化する以前の時代においては電気通信に用いることのできる技術的手段が限られていた。そして、電気的な通信手段が開発され一般に利用されるようになった後においても、通信装置内に通信内容が何らかの媒体に固定的なものとして記録されることは基本的になかった。(5) それゆえ、通信内容の無権限取得は、例えば電話盗聴のように、他人間の通信内容に対するリアルタイムの物理的な傍受が基本であり、その記録媒体は傍受者の脳（記憶）及びその記憶の再現であるメモ等であった。その後、テープレコーダその他の記録装置が開発されるようになってからは機械的な自動録音が可能となったが、それでもリアルタイムの通信傍受を基本として通信傍受が理解されてきたという事実は否定しようがない。(6)

しかし、伝統的な「通信の秘密」に関する理解をひとまず措いて、現実にある事実を直視してみると、非公開のデータに対する侵害行為という社会現象は、理論的にも現実にも、一般的に理解されている「他人間の通信」よりも広い範囲で発生し得るものであるということを理解することができる。

例えば、スパイウェア（Spyware）と呼ばれる無権限データ取得を主たる目的とするソフトウェアは、通信当事者の一方（被害者）のコンピュータやスマートフォンなどの内部に記録されているデータ（利用者の個人情報、電話番号、電子メールアドレス、通信履歴等）やこれらの装置によって自動的に生成されるデータ（ＧＰＳ位置情報等）を他方の通信当事者（加害者）が無権限で密かに取得するという特徴をもっている。(7) スパイウェアによって無権限取得されるデータは、電気通信によって加害者に送信されるが、この場合、その加害者が通信当事者になっているため、「他人間の通信」に対する干渉は存在しないことになる。(8)

また、例えば、マーケティング会社等の第三者に対して電子メール通信履歴を自動送信し、その通信履歴から自動的にプロファイリングされた情報をもとに自動的に商業宣伝広告が付加されることについて、送信者が同意している

電子メール送受信サービスでは、通信当事者の一方（送信者）が同意した上で電子メール送受信情報等の第三者に対する自動転送が実行されている以上、個々の電子メールの送受信それ自体としては「他人間の通信」に該当するとしても、当該第三者は（通信当事者ではなくても）当該電子メールの送受信に適法にアクセスすることができると解するのが一般的である。(9)

要するに、これらのような場合には、通信当事者の一方の同意に基づく行為として違法性阻却事由があり、「通信の秘密」に対する侵害行為は成立しないと解するのが一般的であり、(10)そのような理解を示す裁判例もある。(11)

しかし、このような事例において、伝統的な理解に基づく「通信の秘密」の侵害はないとしても、そのような電子メールを受信する側の通信当事者が同意をしていないことは明らかであるので、当該電子メールを受信する側の通信当事者にとっては「電子メールの送受信が秘密通信の一種である」との信頼を損なう結果を招きかねないことは否定できない。そのため、事案にもよるかもしれないが、「電子メールは当事者限りの秘密のものである」との信頼を侵害する行為として、その違法性を検討すべき余地はあり得ると考える。(12)

ところで、ここに一例として示したスパイウェア等のように、伝統的な意味での通信の秘密に対する侵害とはならないような行為を含め、およそ、秘密のデータ及びその送受信に対する無権限アクセス及びその内容の無権限取得を一つのカテゴリーとして認識・理解することは可能である。ただ、アクセス制御のあるシステムに対する無権限アクセス行為は、不正アクセス行為として処罰可能であるのに対し、機密のデータに対する無権限アクセス行為に関する日本国の法制は必ずしも十分なものとは言えない。

そのような意味での機密データに対する無権限アクセス行為及び機密データの無権限取得行為には非常に多種多様なものが含まれ得る。(13)そのような行為の中でも、錯誤に陥った被害者を道具とする間接正犯的な行為によって機密デー

タを取得する犯罪類型としてのフィッシング（Phishing）については、既に別稿において検討したところである。[14] また、このようなタイプの問題については、プライバシー保護という観点からも各方面から検討が重ねられてきた。[15]

以上のように、機密データに対する無権限アクセス及び機密データの無権限取得に関しては論ずべき点がかなり多数ある。しかしながら、本論文は、あくまでもサイバー犯罪の研究の一部であり、その文脈を離れて検討・考察が散漫となることを防止する必要がある。そこで、本論文では、主として他人間の秘密通信に対する干渉行為としての通信傍受行為に絞って、日本国の法令による処罰及び海外の関連法令による処罰について論ずる。

なお、日本国の通信傍受法（平成一一年法律第一三七号）に基づく通信傍受[16]及びこれに類する監視[17]は、平時における「法令に基づく行為」として違法性阻却となる（刑法三五条）。日本国に限らず、犯罪捜査の目的で裁判所の発する令状に基づく通信傍受は、一般に、違法性阻却となると解されている。また、戦時における軍事目的での通信傍受[18]は、とりわけ違法性阻却との関係において、平時における法的課題の検討とは異なる要素を多く含む。それゆえ、これらの通信傍受に関しては、本論文における検討対象としない。

また、本論文は、特に明記しない限り、二〇一二年一一月二日現在の時点で有効な法令を前提としている。

二　通信傍受に適用可能な日本国の法令

1　法制の全体構造

通信傍受行為について、全体の流れを一般的に観察してみると、①通信傍受に用いるソフトウェアや機器類の準備・

作成、②通信傍受行為の実行及び③通信傍受した情報内容の取得・保存・利用の三つに分けて考えることができる。

これらの行為は、実質的に重なる部分がある。例えば、通信傍受に用いるソフトウェアや機器類を単に準備・作成するだけでなく、それらを利用する行為は、通信傍受行為の実行行為ともなる。また、通信傍受行為を実行すると傍受される通信の内容を直ちに取得することができる場合（録音機やデータ記録装置等を用いて自動記録する場合を含む。）には、通信傍受行為の実行と通信内容の取得・保存行為とが同時に生ずることになる。そして、傍受された通信内容が他の通信傍受のために利用可能な場合には、傍受した通信内容の利用が直ちに新たな通信傍受の準備行為ともなる。

これらの行為は、連続して循環的に実行されることもあるが、個別に独立した行為として実行されることもある。しかし、論理的には相互に関係する行為となり得ることを正確に理解した上で、もし複数の犯罪が成立する場合にはその罪数関係を考えなければならない。同様に、共犯関係についても、正犯の行為の罪数を正確に理解した上で正しく考察しなければならない（図1）。

通信傍受に関して適用可能な日本国の刑罰法令（罰則のある行政法規等を含む。）の中で最も重要なものは、言うまでもなく電気通信事業法（昭和五九年法律第八六号）、有線電気通信法（昭和二八年法律第九六号）及び電波法（昭和二五年法律第一三一号）の三つの法令である（以下、これら三つの法令を総称する場合には「通信関連法」という。(19)）。

通信関連法は、主として、通信傍受行為それ自体を「通信の秘密を侵す罪」として処罰対象とするものである。しかし、通信傍受によって取得した情報内容を第三者に提供する行為（漏示）や自己または権限を有しない第三者のために利用する行為（窃用）は、通信傍受によって取得した通信内容を利用する行為に該当する。

他方で、通信傍受のためにコンピュータソフトウェアが作成・取得・提供・供用される場合には、不正指令電磁的記録に関する罪（刑法一六八条の二、同条の三）が成立し得る。この罪は、主として、通信傍受に用いるソフトウェ

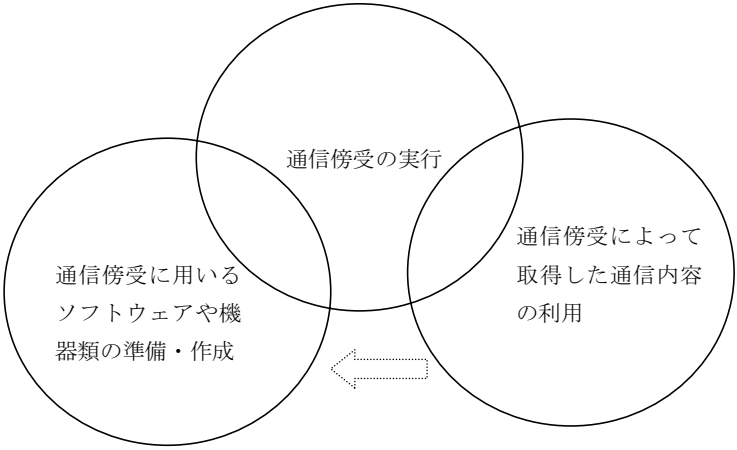

図１：通信傍受と関連する行為の相互関係

ア の準備・作成に該当する。しかし、そのようなソフトウェアを実行する行為は、通信傍受行為それ自体ともなり得る。また、通信傍受によって取得した情報内容が不正指令電磁的記録を含む場合には、通信傍受により取得した内容の利用行為が不正指令電磁的記録の取得・保管行為をも構成することがあり得る。不正アクセス罪や支払用カード電磁的記録に関する罪等についても同様に考えることができる。

以下、このような理解を前提にして検討を進める。(20)

2　通信関連法

通信関連法は、日本国における通信行政の基本となる法令であると同時に、これらの法令に規定する罰則こそが通信の秘密と関連するサイバー犯罪に対応する上で最も重要な処罰条項ともなっている。

ところで、通信関連法は、物的・技術的な通信手段という点では同一の部類に属する情報通信に関するものである。しかし、電気通信は有線通信及び無線通信の別を問わず（電気通信事業法二条一号）、かつ、電気通信事業者（同法二条五号）(21)が取扱う通信に関しては専ら電気通信事業法が適用されることになる。その結果、有線電気通信法及び電波法は、電気通信事業者以外の者が取扱う通信について適用されることになる。そして、有線電気通信法及び電波法のうち、有線電気通信法は有線電気通信（有線電気通信法二条一項）に、電波法は無線通信（電波法二条一号）にそれぞれ適用されることになる。その適用関係を図示すると、表1のとおりとなる。(22)

従来、このような法適用上の区分は、ほとんど紛れのない明瞭なものとして一般に理解されてきた。それゆえ、罰則の適用についても疑義が生ずることは比較的稀であったと思われる。

表1：通信関連法の適用関係

電気通信事業者による通信		電気通信事業者以外の者による通信
電気通信事業法		
有線通信	有線電気通信法	
無線通信	電波法	

しかし、クラウドコンピューティング（Cloud Computing）や仮想コンピューティング（Virtual Computing）の登場によって、法適用上の明瞭性に変化が生じて、あたかも雲がかかったかのような状況となりつつある。[23] このような状況の変化を踏まえた法適用関係については、別稿で論ずることとし、ここでは、応用問題を検討する際の大前提となる普通の通信形態を前提に、通信傍受について適用可能な罰則について述べる。

(1) 通信の秘密の意義

通信関連法における罰則は、「通信の秘密」を保護法益としている。[24]

通信の秘密の概念は、言うまでもなく、日本国憲法二一条二項に由来するものである。国営の通信事業のみが認められている国家においては、まさに国による検閲や通信傍受が最大の法的課題となるため、それらに関する憲法上の人権保障が重要となる。日本国においても、第二次世界大戦終了前の時代はもちろんのこと、日本電信電話株式会社等に関する法律（ＮＴＴ法・昭和五九年法律第八五号）等に基づいて通信事業が広く一般に認められるようになる以前、主として電信電話公社によって通信事業が独占されていた時代においても基本的には同じであったと考えることができる。[25]

しかし、ＮＴＴ法等に基づく電信電話公社の分割・民営化[26]の後、通信事業が民間企業によっても広く一般に遂行さ

れるようになった結果、国と国民との間を規律する法的概念の一つである基本的人権の一種としてのみ「通信の秘密」をとらえるのでは理論的に無理が生ずるようになったと考えられる。

今日、私人としての通信会社と私人としての当該通信会社による通信役務利用者との間またはいずれも私人である通信当事者間における「通信の秘密」に関しては、憲法論の立場からは人権保障の私人間効力の問題として理解するのが通例である。[27] この点について、最高裁は、一貫して直接的な効力を認めず、公序良俗の一部を構成するものとして間接的な効力を有するとの判断を示している。[28]

このような憲法学上の議論はある。しかし、非公開通信に関してその内容が秘密のものとされるべきであり、かつ、特別の正当化事由（違法性阻却事由）がない限り、その秘密とされている通信内容等を第三者が取得する行為（不特定多数の者に公開するような場合を含む。）が通信の秘密に対する侵害となるという理解を否定する者は基本的に存在しないと考えて良い。その意味で、「通信の秘密」は、民法七〇九条に規定する法的に保護されるべき利益の一つとして理解することができる。また、そうであるがゆえに、通信関連法における罰則との関係でも保護法益としての実質を有していると理解すべきである。そして、そのような意味での法的利益（「通信の秘密」という表現で示される法的利益の実質的内容）は、一般に、プライバシーの利益の一部を構成すると理解されている。[29]

ただ、仔細に検討すると、「通信の秘密」の具体的内容または構成要素及びその保護の程度については、若干の議論がないわけではない。例えば、サイバー犯罪条約の一四条以下に規定する刑事手続条項において、通信記録（traffic data）と通信内容（content data）との間に刑事事件捜査上の取扱いの差を設けているのもそのことに起因している。少なくとも、サイバー犯罪条約の起草者の理解としては、特定の通信の発信地、中継地及び到達地といった通信記録を捜査官が取得する行為は、通信内容を取得する場合よりも人権侵害の程度が低いとされている。[30] このことから、一

般に、通信の秘密の具体的対象として、通信の本体（通信当事者及び通信内容）[31]と通信記録（ＩＰアドレス等の技術的要素）とは等しく通信の秘密に含まれるものではあるけれども、その法的保護の程度に差異が生ずることがあると理解されるに至っている。

なお、通信の秘密は、音声による会話の傍受の場合だけではなく、コンピュータやネットワークシステムを介したデータ通信の場合においても当然に保護の対象となる。[32]

いずれにしても、通信関連法における「通信の秘密」の本質は、情報通信におけるプライバシーの利益と同内容のものであると解して何ら差支えがない。そして、現実に発生する通信傍受行為の多くは、通信関連法に規定する通信の秘密を侵す罪（通信の秘密侵害罪）に該当するものとして処罰されることになる。

(2) 侵害の態様

一般に、通信の秘密に対する侵害行為は、知得、漏示及び窃用の三つの行為類型に分類し得るものと解されている。[33]ただし、正確には、通信関連法中の全ての罰則において、知得罪、漏示罪または窃用罪という犯罪が個別に規定されているわけではない。この点について、後述の電波法五九条は、傍受、漏示及び窃用の三つのタイプの行為を、無線通信の秘密を侵す行為として規定しており、これらの行為は同法一〇九条（漏示及び窃用）及び同法一〇九条の二（暗号通信の傍受）により処罰される。しかし、電気通信事業法及び有線電気通信法ではそのような行為類型を示す条項は存在しない。電気通信事業法及び有線電気通信法の解釈・運用において知得、漏示及び窃用の概念が用いられるのは、あくまでも講学上の概念として用いられているのであって、法令中にそのような構成要件が規定されているのではない。電気通信事業法及び有線電気通信法の定める罰則を適用する場合には、いずれも「通信の秘密を侵す罪」となる。

(a) 知得

「知得」とは、積極的に傍受する行為を指すと解されている。[34] この傍受とは、権限なく通信内容にアクセスし、その内容を取得することを意味する。なお、電波法違反の場合には、暗号通信を解読する行為のみが傍受行為に該当する（電波法一〇九条の二）。

一般に、電波法違反の場合を除き、知得（通信傍受）の方法には限定がない。電気通信の場合であってその通信内容を人間が直接に認識・理解することができない場合には、何らかの記録装置や記録媒体に通信内容を記録した時点で知得罪としては既遂に達し、[35] その時点で行為者が通信内容を認識・理解することを要しない。[36]

ただし、非常に強固な暗号手法によって暗号化された機密通信等のように、通常利用可能な手段によっては通信内容を解読して認識・理解することができない場合には、当該暗号について復号する権限を有する者にとっては復号可能という意味で不能犯には該当しないが、知得行為の未遂に該当するものと解する。

一定の分量の通信内容を知得した場合の罪数については、事案により、併合罪となる場合[37]と包括一罪[38]となる場合とがあり得ると思われる。ただし、通信内容を知得するためにある程度の時間を要する場合であっても、当該通信内容が社会通念上一個のものとして認識されている場合[39]には、単純一罪として処理すべきである。

(b) 漏示

「漏示」とは、（知得による場合と知得以外による場合とを含め）何らかの原因により取得した他人の通信内容を第三者が知り得る状態にすることを意味すると解されている。[40] ただし、通信内容が秘密であることを要するから、当該通信内容が客観的に秘密性を有しないものである場合には漏示罪は成立し得ない。[41] また、その通信内容が既に広く知られている場合には、当該通信の秘密性が失われていることから、「漏示」に該当しない場合があり得る。[42]

知得した者が当該知得した通信内容等を第三者に漏示した場合の罪数については、別個の行為として併合罪になることがあると思われるが、知得と漏示とが同時になされている場合には、事案により、観念的競合または包括一罪として処理すべきであろうと思われる。漏示する者自身が当該通信内容を知得することを要しないのは当然のことであり、誰かが知得した通信内容を記録した媒体を入手し、その内容を第三者に提供すれば漏示が成立することになる。(43)

(c) **窃用**

「窃用」とは、本人の意思に反して自己または第三者の利益のために用いることを意味すると解されている。(44)また、一般に、「窃用」は、積極的に取得する行為を意味し、偶然の結果として情報を取得してしまった場合(45)を含まないと解されている。(46)

罪数については、知得と漏示の場合に準じて考えれば良いであろう。知得、漏示及び窃用がそれぞれ別個の行為として全て実行された場合も同様である。事案により、全ての行為を包括一罪として処理すべき場合もあり得る。

(4) 電気通信事業法上の罰則

電気通信事業法四条一項は「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない」と規定し、同条二項は「電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする」と規定している。(47)

いずれも通信の秘密を保護すべき義務を定めるものであるが、同条一項は、通常は他人間の通信内容を知ることができない者が、無権限で他人間の通信内容にアクセスまたはこれを取得するなどの行為により、通信の秘密を侵害する行為類型を前提としている。これに対し、同条二項は、電気通信事業に従事する者（使用者、管理者、従業員など）が、電気通信事業上の業務を遂行する上で知ることがあり得る他人の通信内容について、それを第三者に漏示または

窃用してはならないことを規定するものであり、一般的には、特別の地位に基づく守秘義務を定めるものとして理解されている。

他方、同法三条は、「電気通信事業者の取扱中に係る通信は、検閲してはならない」と規定している(48)。「検閲」とは、国その他の公権力主体が私人間の通信内容を知得することにより通信の秘密を侵害する行為を指すと解される(49)。このように解する場合、通信の秘密を侵害する加害者が国その他の公権力主体である場合に、いわば身分犯的に成立する違法行為が検閲であると理解することが可能である(50)。

以上を総合すると、通信傍受の禁止を定める条項は、同法三条（加害者が国その他の公権力主体である場合）及び同法四条一項（加害者が国その他の公権力主体ではない場合）であることになる。

そして、電気通信事業者の取扱中に係る通信の秘密を侵す行為については(51)、罰則の適用があり、二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（同法一七九条一項）。また、電気通信事業者の取扱中に係る通信の秘密を侵す行為を実行する者が電気通信事業に従事する者である場合には三年以下の懲役または二〇〇万円以下の罰金に処せられる（同条二項）。これらの行為の未遂行為も処罰される（同条三項）(52)。

同法三条に規定する検閲の禁止に違反する行為については、直接の罰則がない。しかし、既述のとおり、同法三条の検閲を同法四条一項の行為の身分犯的な行為であると解するとすれば、国その他の公権力主体が検閲をする場合であっても通信の秘密を侵していることには何ら変わりがないので、同法一七九条一項（通信の秘密侵す罪）の罰則が適用されるものと解される。ところが、国その他の公権力主体は、電気通信事業に従事する者ではないので、同法一七九条二項の過重処罰規定の適用がない。これは、かなり奇妙なことである。しかし、罰則の欠缺の一種だと理解するしかない(53)。

(5) 有線電気通信法上の罰則

有線電気通信法九条は、有線電気通信の秘密は、侵してはならないと規定している。電気通信事業者が取扱う通信に関する電気通信事業法四条一項に規定する通信の秘密の場合は除外されている（有線電気通信法九条括弧書き）。これは、既述のとおり、有線電気通信事業法が電気通信事業者の取扱う通信以外の有線通信にのみ適用されるからである。同様に、有線電気通信事業法の適用対象が電気通信事業者ではない関係から、有線電気通信において電気通信事業法四条二項に該当するような場合はあり得ないこととなる。

そして、同法九条に規定する有線電気通信における通信の秘密を侵す行為に対しては罰則の適用があり、二年以下の懲役または五〇万円以下の罰金に処せられる（同法一四条一項）。また、有線電気通信の業務に従事する者が有線電気通信における通信の秘密を侵す行為をしたときは、三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（同条二項）。これらの罪の未遂行為も処罰される（同法一五条）。[54]

今日の社会においては、営利企業であるインターネットサービスプロバイダ（ＩＳＰｓ）が提供する通信接続サービスを利用してインターネット通信をすることが普通になっているため、通常の情報通信に関しては電気通信事業法が適用されることになる。その結果、有線電気通信法が適用される場面は少ないのではないかと誤解する者があるかもしれない。しかし、例えば、大学の施設内だけに限定された情報ネットワークシステム（ＬＡＮ）などのように、電気通信事業者が全く関与しない有線電気通信はかなり多数存在する。そのような通信網の中にはコンピュータシステムのための情報ネットワークシステムだけではなく、ＰＨＳ携帯電話を用いた構内無線ネットワークのうち有線通信で構成されている部分のようなものも含まれる。[55] その意味で、有線電気通信法の重要性は現時点でも失われていないどころか、むしろ非常に大きな重要性を維持していると考えることができる。

ところが、近時の情報ネットワークシステムの中には、特定の施設内だけに限定されたＬＡＮのように見えるけれども、実際の物理構造としては外部の電気通信事業者が提供する情報通信サービスを借りて運用されているものがある。[56] そのような場合には、専ら電気通信事業法のみが適用されると考えるべき場合が多いと思われるが、事案により、部分的に電気通信事業者が全く関与していない構成部分が存在し得ることから、法の適用関係を考える際には、当該情報ネットワークシステムの物理構造について正確な事実認識をもつことが非常に重要である。同様の場合において、法律論としては、電気通信事業法及び有線電気通信法が競合して適用され得る場合があるのではないかと考えられるし、また、電波法も競合して適用され得る場合もあり得るのではないかと考えられる。この点は、具体的な事案によって異なるので、詳論を避ける。

(6) 電波法上の罰則

無線通信における通信の秘密に関する基本法規は電波法である。[57]

電波法五九条は、特定の相手方に対して行われる無線通信を傍受してその存在もしくは内容を漏らしまたはこれを窃用してはならないと規定している。[58] ただし、電気通信事業法四条一項の通信の秘密に該当するものは除外されている。これは、有線電気通信法との関係で述べたところと同じ理由に基づくものである。

罰則については、電波法は、漏示と窃用について罰則を設けているほか、傍受のうち暗号通信の解読行為のみを処罰対象としている。これは、一般に、暗号化されていない無線通信については、それを受信してその通信内容を知ることが可能であることによるものとされている。[59]

まず、電波法一〇九条一項は、無線局の取扱中に係る無線通信の秘密を漏らし[60]または窃用[61]した者は、一年以下の懲役又は五〇万円以下の罰金に処すると規定し、また、同条二項は、無線通信の業務に従事する者[62]がその業務に関し知

り得た前項の秘密を漏らしまたは窃用したときは、二年以下の懲役または一〇〇万円以下の罰金に処すると規定している。これらの罰則の趣旨等については、電気通信事業者が取扱う電気通信以外の無線通信である点を除いては、電気通信事業法上の罰則について述べたところと同じである。

他方、同法一〇九条の二第一項は、「暗号通信を傍受した者又は暗号通信を媒介する者であって当該暗号通信を受信したもの」が、当該暗号通信の秘密を漏らし、または窃用する目的で、その内容を復元したときは、一年以下の懲役または五〇万円以下の罰金に処すると規定し、また、同条二項は、無線通信の業務に従事する者が、同条一項項の罪を犯したとき（その業務に関し暗号通信を傍受しまたは受信した場合に限る。）は、二年以下の懲役又は一〇〇万円以下の罰金に処すると規定している。未遂行為も処罰される（同条の二第四項）。

これらの条項に規定する「暗号通信」の意義について、同条三項は、「通信の当事者（当該通信を媒介する者であって、その内容を復元する権限を有するものを含む。）以外の者がその内容を復元できないようにするための措置が行われた無線通信をいう」と定義している[63]。したがって、暗号通信に対する傍受罪が成立するためには、当該通信が単に暗号化された通信であるというだけでは足りず、通信当事者または権限を有する通信媒介者のみが復号可能な状態で暗号化された通信であることを要し、そのような通信についてのみ[64]、同法一〇九条の二第一項、二項及び三項の罪が成立し得ることになる。

ところで、電波法に規定する罰則が適用される無線通信の当事者は、私人だけに限定されるものではなく、通信当事者の一方または双方が国またはその機関である場合でも電波法所定の罰則が適用される。それゆえ、警察無線による通信を傍受し、その内容を漏示した場合には、同法一〇九条一項の漏示罪が成立することになる[65]。

3　刑法（不正指令電磁的記録）

従来、電話の通話内容の傍受に関しては物理的な機械装置である盗聴装置・タッピング装置及び関連機器類（傍受した通話内容の送受信装置等）が主要な手段であった。

しかし、今日、電話通話がアナログ通話からデジタル通話（ＩＰ電話など）へ移行したことから、従来型の電話盗聴手段に加え、デジタル電話機や回線上にある各種機器類のファームウェア内に無権限でインストールされ実行されるスパイウェアなどのコンピュータソフトウェアもまた決して無視することのできない危険な存在となっている。企業や家庭で用いられるＰＣやスマートフォンなどでは、通信傍受した内容が直ちに加害者の手元に自動送信されてしまうようにし、かつ、通信傍受の痕跡を残さないように通信傍受実行のために使用したデータや通信傍受の履歴データ等の自動消去を実行するようなソフトウェア（アプリ）を作成・実行することが非常に容易にできてしまう。そのため、このような問題の深刻さは従来型の電話機やＰＣにおける通信傍受の場合よりも著しいと言える場合がある。

加えて、装置内の基本ソフトウェア（ＯＳ）だけではなく、より物理層に近いところにある電子チップ内のファームウェアにも感染し得るトロイの木馬（Trojan horse）などのマルウェア（malicious software）を用い、ＰＣやスマートフォンの機能を完全に奪うというタイプの攻撃が世界各地の相当広い範囲で生じている(66)。このような攻撃が実行された場合、通信傍受用の特別のソフトウェアがなくても、ＰＣやスマートフォンを常時監視し、かつ、ＰＣやスマートフォンに装備されている通信ソフト等を無権限で使用して、そのＰＣやスマートフォン上で実行される通信内容を自動転送することができる（すなわち、当該装置の管理・支配を完全に奪い、無権限でリモート操作することができる(67)）。

以上のようなスパイウェアやトロイの木馬などの通信傍受用のソフトウェアは、一般に、刑法上の不正指令電磁的記録の一種であると理解することができる。そして、そのようなソフトウェアがインストールされていること、あるいは、PCやスマートフォンの支配が他人によって奪われてしまっていることを知らずに当該機器類を操作する利用者は、実質的にみて、間接正犯の道具として当該不正指令電磁的記録の供用行為を実行する行為をしているとみるべき場合がある。このことは通信傍受についても同じであり、通信の一方当事者としての利用者（A）と間接正犯の道具としての利用者（A′）が物理的な存在として同一人に重なって存在しているということがあり得る。このような場合、間接正犯の道具としての利用者（A′）が、他人である通信の一方当事者としての利用者（A）及び第三者（B）との間の通信を傍受しているという関係の成立を認めることができるとすれば、他人間の通信に対する干渉としての通信傍受の成立を認めることが可能であろう。(68)

なお、スパイウェアは、それを用いることにより、他人間の通信内容だけではなく、通信可能な機器類に含まれているデータや情報であれば何でも無権限取得することが可能である。それゆえ、厳密には通信傍受には該当しないデータに対する無権限アクセスや無権限入手を発生させている場合もある。(69)

ここでは、厳密な意味での通信傍受の機能を有するものだけではなく、主として通信傍受以外の機能を有するものも含め、適用可能な法令について検討する。

(1) 不正指令電磁的記録の該当性

不正指令電磁的記録（刑法一六八条の二第一項）は、不正指令電磁的記録の意義について、「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」（同項一号）または「前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録」（同項

二号）に該当する電磁的記録その他の記録を意味すると定義している。

この定義については、別稿[70]で詳論したとおりであるが、通常、同条の二第一項一号の電磁的記録は機械語命令によるコンピュータプログラムなどを指し、同条の二第一項二号の電磁的記録はそのソースコード[71]を指し、また、「その他の記録」はそのプリントアウトなどを指すものと解されている。しかし、例えば、ＸＭＬやＨＴＭＬのようなマークアップ言語で書かれた文書は、人間が直接に読むことのできるテキストであると同時に、コンピュータ上で直ちに実行可能なコンピュータプログラムでもある。一般に、人間が読解可能なプログラムをソフトウェアが解釈して実行するインタプリタによって実行されるコンピュータプログラムは、このような特徴を有する。また、二次元バーコードの形式で紙の上に印刷して記録されたコンピュータプログラムなどのように、読み取り装置で読み取れば直ちに実行可能なコンピュータプログラムもある。このような場合には、立法者が想定しているような明確な区分は理論的にも物理的にもできないので、同条の二第一項に規定する複数の電磁的記録またはその他の記録に同時に該当するものとして理解すべきである[72]。

通信傍受の用に供する目的で作成されるスパイウェアその他のコンピュータソフトウェアが[73]「不正指令電磁的記録」に該当することは異論がないものと考える[74]。これを刑法が規定する要件に即して分析的に考えてみると、一般に、通信傍受の用に供する目的で作成されるスパイウェアその他のコンピュータソフトウェアに関して、「通信傍受の目的」は、一般に「正当な理由」がない場合に該当し[75]、かつ、通信傍受用のソフトウェアは「人の[76]電子計算機における実行の用に供する目的」で作成されるのが通例である[77]。そして、本人が知らない間にスパイウェア[78]その他のコンピュータソフトウェアが密かに仕掛けられ通信傍受が実行される場合には、原則として、「人が電子計算機[79]を使用するに際して」、「その意図に反する動作[80]をさせるべき」指令を与えたことになると解される。

したがって、通信傍受の用に供する目的で作成されるスパイウェアその他のコンピュータソフトウェアの実行モジュールは、原則として、刑法一六八条の二第一項一号の不正指令電磁的記録に該当し、そのソースコードは同項二号の電磁的記録に該当し、また、そのプリントアウトは同項一号の指令を記録した「その他の記録」[81]に該当すると解される。

例外として、ソースコードのままで実行可能なものについては、前述のとおり、同条の二第一項及び第二項の電磁的記録に該当し、そのプリントアウトは同項一号の指令を記録した「その他の記録」に該当すると解する。

(2) 処罰可能な行為

不正指令電磁的記録を作成した者は、不正指令電磁的記録作成罪として三年以下の懲役または五〇万円以下の罰金に処せられる（刑法一六八条の二第一項）。その未遂行為も処罰される（同条の二第三項）。通信傍受の用に供する目的で作成されるスパイウェアその他のコンピュータソフトウェアの実行モジュールが不正指令電磁的記録に該当する場合、それを作成する行為は、通信傍受行為の準備的行為に該当することがあるものとして理解することができる。

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した者は、不正指令電磁的記録供用罪として三年以下の懲役または五〇万円以下の罰金に処せられる（刑法一六八条の二第二項）。その未遂行為も処罰される（同条の二第三項）。通信傍受の用に供する目的で作成されるスパイウェアその他のコンピュータソフトウェアの実行モジュールが不正指令電磁的記録に該当する場合、それを供用する行為は、通信傍受行為そのものとなる。

正当な理由がないのに、不正指令電磁的記録を取得した者は、不正指令電磁的記録取得罪として二年以下の懲役また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）。通信傍受の用に供する目的で作成されるスパイウェアその他のコンピュータソフトウェアの実行モジュールが不正指令電磁的記録に該当する場合、それを取得する

行為は、通信傍受行為の準備的行為に該当する場合があるものとして理解することができる。

そして、正当な理由がないのに、不正指令電磁的記録を保管した者は、不正指令電磁的記録保管罪として二年以下の懲役また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）。通信傍受の用に供する目的で作成されるスパイウェアその他のコンピュータソフトウェアの実行モジュールが不正指令電磁的記録に該当する場合、それを保管する行為は、通信傍受行為の準備的行為に該当する場合があるものとして理解することができる。

なお、他罪との罪数関係とりわけ通信関連法上の罰則との罪数関係については、後述するとおりである。

4　個人情報保護法

通信傍受行為によって取得される情報内容に個人に関する情報が含まれることがあることは言うまでもない。そのようにして取得される個人に関する情報のうち、特定の個人を特定するための情報（個人識別情報）については、形式的には、個人情報保護法（平成一五年法律五七号）の適用があり得る。

そのような個人情報による処罰の可能性の有無についても別稿[82]で詳論したとおりであるが、原則として、通信傍受によって無権限で他人の個人情報が取得されたとしても、そのような個人情報の取得者に対して、同法に基づいて直接に処罰することはできない。

しかしながら、個人情報取扱事業者（同法二条三項）が、その業務を遂行する上で、他人間の通信に対する通信傍受を実行する場合、同法一七条に規定する「個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない」との義務の違反が問題とされ得る。通信傍受行為は、一般に、「偽りその他不正の手段」に該当し得る

と解されるからである。

そして、個人情報取扱事業者に同法一七条の義務に違反する行為があり、そのような違反行為に対して主務大臣から勧告・指示等（個人情報保護法三四条一項）がなされた場合において、個人情報取扱事業者がその勧告・指示等を遵守しないときは、主務大臣によって是正命令等（同条二項、三項）がなされ得る。そして、その是正命令等を当該個人情報取扱事業者が遵守しない場合には、当該個人情報取扱事業者に違反行為があったものとして、罰則の適用があり得る（同法五六条）。

また、主務大臣は、個人情報取扱事業者に対し、個人情報の取扱いに関し報告をさせることができるが（同法三二条）、当該個人情報取扱事業者が、主務大臣に対して報告をせず、または虚偽の報告をした場合には罰則の適用がある（同法五七条）。

このように、個人情報保護法における罰則及びその適用は、かなり微温的なものであるので、通信傍受行為に対する刑事制裁の手段としては基本的に機能しないと考えて良い。

なお、当然のことながら、個人情報取扱事業者に該当しない者[83]の場合には、主務大臣が存在しないし、主務大臣による行政監督もあり得ないので、個人情報保護法に規定する罰則の適用も決してない。

5　不正競争防止法

通信傍受の対象となる情報内容に営業秘密（不正競争防止法二条六項）が含まれている場合、不正競争防止法に規定する不正競争行為の該当性有無が問題となる。

営業秘密は、秘密のものとして管理されていることを要するから（同法二条六項）、営業秘密に属する可能性のある情報が通信内容となっている通信であっても、その通信内容が容易に解読可能なものである場合には、秘密のものとして管理されているとは認められないことがあり得る[84]。しかし、通信手段それ自体について特定のパスワード等がなければ送受信できないような暗号化措置が講じられている場合や、通信内容であるデータが暗号化されており、権限を有する者以外の者にとっては解読不可能または非常に困難なものである場合、その通信内容となっている情報について、営業秘密に該当するものがあり得ることを否定すべき理由はない[85]。

また、一般に、通信傍受による営業秘密の取得行為は、何らかの正当化理由または違法性阻却事由が存在しない限り、通信の秘密を侵す行為であるという意味で不正の手段による取得行為であると解することができるから、不正競争防止法に規定する営業秘密の不正取得行為（同法二条一項四号）に該当し得る。

罰則の適用については、若干注意すべき部分がある。罰則である同法二一条一項一号は、詐欺等行為と管理侵害行為とに分けてその犯罪構成要件を規定している。そして、前者の詐欺等行為とは「人を欺き、人に暴行を加え、又は人を脅迫する行為」を意味し、管理侵害行為とは「不正アクセス行為その他の保有者の管理を害する行為[86]」を意味する。通信傍受行為は、それ自体としては人に向けられた欺罔行為ではなく、それによって欺罔された者が錯誤に陥ることを狙う行為ではないので、詐欺等行為には該当しない。しかし、通信手段または通信内容が暗号化されており、当該営業秘密の保有者（またはその者から権限を与えられた者）だけが当該通信にアクセスしてその内容を取得することができる場合には、「保有者の管理を害する行為」として管理侵害行為に該当し得る。

管理侵害行為により営業秘密を取得した者は、一〇年以下の懲役また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）[87]。また、管理侵害行為により取得した営業秘密を、不正の利益を得る目的またはその保有者に損害

を加える目的で使用した者、管理侵害行為により取得した営業秘密を、不正の利益を得る目的またはその保有者に損害を加える目的で開示した者は、同様に、一〇年以下の懲役または一〇〇〇万円以下の罰金に処せられる（同法二一条一項二号）。これらの罪は親告罪である（同条三項）。国外犯も処罰され（同条四項）、両罰規定がある（同条二二条）。[88]

このような不正競争取締法に違反する犯罪行為を通信傍受との関係でその対応関係を考えてみると（図1）、営業秘密の取得行為は通信傍受行為そのものであり、取得した営業秘密の使用行為及び開示行為は傍受した通信内容の利用に該当することになる。

なお、不正競争防止法は、権限なく取得した営業秘密の開示行為等についても罰則を設けている。開示行為に関する罰則と通信関連法上の罰則との罪数関係（特に、①営業秘密の使用罪と窃用に該当する通信の秘密侵害罪及び②営業秘密の開示罪と漏示に該当する通信の秘密侵害罪との罪数関係）については、後述のところに準じて応用して考えれば足りると思われる。

6　通信関連法違反の罪と他の罪との罪数関係

通信傍受行為により取得される情報内容に限定はない。その中には、クレジットカード情報やデビットカード情報のような支払用カード電磁的記録の情報に該当するものや、特定電子計算機にアクセスするための識別符号に該当するものなどが含まれていることがあり得る。これらの場合、通信関連法に定める通信の秘密侵害罪と同時に成立する他の罪との罪数関係が問題となり得る。[89]

ただし、現実の刑事公判においては、検察官が特定の罪に限定して公訴事実を構成し起訴するのが普通であること

から、潜在的には他の罪との罪数の問題が発生することがあり得る事案であっても、問題が表面化しないことが圧倒的に多いことに留意すべきである（ある罪が包括一罪となるために、いわゆる「かすがい現象」によって全体として一罪となってしまうような場合を含む。）。

ここでは、支払用カード電磁的記録に関する罪、不正アクセス禁止法違反の罪、不正指令電磁的記録に関する罪との間の罪数関係に限定して述べるが、それ以外の犯罪との間の罪数関係についても応用して考えることが可能である。

(1)　支払用カード電磁的記録に関する罪との関係

知得する通信内容が支払用カード電磁的記録の情報に該当し、かつ、支払用カード電磁的記録不正作出の目的で取得する場合には、同電磁的記録の情報取得罪が成立する（刑法一六三条の四第一項）。この罪と通信の秘密を侵す罪[90]との罪数関係は観念的競合の関係にたつと解される。

漏示する通信内容が支払用カード電磁的記録の情報に該当し、かつ、支払用カード電磁的記録不正作出の目的で情を知ってその情報を第三者に提供する行為については、同電磁的記録の情報提供罪が成立し（刑法一六三条の四第一項）、この罪と通信の秘密を侵す罪[91]との罪数関係は観念的競合の関係にたつと解される。

窃用する通信内容が支払用カード電磁的記録の情報に該当し、かつ、人の財産上の事務処理を誤らせる目的で支払用カード電磁的記録を作成する行為については同電磁的記録の不正作出罪が成立し（刑法一六三条の二第一項）、この罪と通信の秘密を侵す罪[92]との罪数関係は観念的競合の関係にたつと解される。その供用罪（刑法一六三条の二第二項）についても同じである。支払用カードの不正作出行為とその供用行為とを同一人が実行した場合には、それらの行為だけをみると牽連犯が成立するように見えるが、窃用行為は包括して一個の通信の秘密侵害罪を構成するとみることが可能な場合があり、そのような場合には、いわゆる「かすがい現象」の一種として、全体として一罪として扱い、最

も重い法定刑の罪が成立すると理解すべきであろう。[93] この点は、他罪との罪数関係についても同様に考えることができる。

窃用する通信内容が支払用カード電磁的記録の情報に該当し、かつ、支払用カード電磁的記録不正作出の目的で保管する行為については（窃用行為の一部が保管行為をも構成する場合）、同電磁的記録の保管罪が成立し（刑法一六三条の四第二項）、この罪と通信の秘密を侵す罪との罪数関係は観念的競合の関係にたつと解される。

(2) 不正アクセス禁止法違反の罪との関係

不正アクセス禁止法に定める罪についても同様に考えることができる。[94]

知得する通信内容が特定電子計算機のアクセスのために用いる識別符号に該当し、かつ、不正アクセス行為の用に供する目的で取得する場合には、他人の識別符号の不正取得罪が成立する（不正アクセス禁止法四条、一二条一号）。この罪と通信の秘密を侵す罪との罪数関係は観念的競合の関係にたつと解される。

漏示する情報内容が特定電子計算機のアクセスのために用いる識別符号に該当し、かつ、正当な理由がないのに第三者に提供する場合には、不正アクセス行為を助長する行為の罪が成立し（不正アクセス禁止法五条、一二条二号）、この罪と通信の秘密を侵す罪との罪数関係は観念的競合の関係にたつと解される。

窃用する情報内容が特定電子計算機のアクセスのために用いる識別符号に該当し、かつ、それを用いて不正アクセス行為をする場合には、不正アクセス罪が成立し（不正アクセス禁止法三条、一一条）、この罪と通信の秘密を侵す罪との罪数関係は観念的競合の関係にたつと解される。

なお、不正アクセス行為を手段として他人の通信の秘密を侵害したという事例については、不正アクセス罪と通信の秘密侵害罪との関係は、牽連犯（科刑上一罪）ではなく、併合罪の関係にたつと解される。[95]

(3) 不正指令電磁的記録に関する罪との関係

他方、知得する通信内容が不正指令電磁的記録に該当する場合については、そもそも通信の秘密が成立するかどうか（通信の秘密として法的保護の対象となり得るか）が問題となり得る。しかし、盗品や禁制品などの違法物品を窃取した場合でも、占有という法益の保護には変わりがないとして窃盗罪が成立することを認めるのが通説・判例であるので[96]、それと同様に考えると、通信の内容が不正指令電磁的記録に該当する場合であっても通信の秘密侵害罪が成立し得るということになる[97]。

そのように解することができる場合、知得する通信内容が不正指令電磁的記録であり、かつ、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それを取得した場合には、不正指令電磁的記録取得罪が成立し（刑法一六八条の三）、この罪と通信の秘密を侵す罪との罪数関係は観念的競合の関係にたつと解される。

同様に、漏示する通信内容が不正指令電磁的記録であり、かつ、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それを取得した場合には、不正指令電磁的記録提供罪が成立し（刑法一六八条の二第一項）、この罪と通信の秘密を侵す罪との罪数関係は観念的競合の関係にたつと解される。また、窃用する通信内容が不正指令電磁的記録であり、かつ、正当な理由がないのにそれを実行の用に供した場合には、不正指令電磁的記録供用罪が成立し（刑法一六八条の二第二項）、この罪と通信の秘密を侵す罪との罪数関係は観念的競合の関係にたつと解される。

三　海外の主要法令

通信の秘密と関連する海外の法制調査は、これまでも幾つかの成果が存在するが[98]、世界各国の法制を網羅したもの

は存在しない。また、電子的な通信技術やサービスの発展と共に新たなタイプの法的課題が生ずることが多々あり、それに対応するため、各国の通信関連法令が比較的頻繁に改正されている現状においては、そのような世界の立法動向を完全にフォローすることは基本的に不可能事に属する[99]。そのため、各国における通信傍受禁止関連法制を正確に比較検討することもかなり難しい状況にある。

本論文では、今後の研究のための一助とすべく、通信傍受及び通信の秘密の保護と関連して比較的参照されることが多い法令として、米国連邦刑法中にある通信傍受禁止及び罰則に関する条項（USC 18 §2511）[100]の罰則部分、そして、比較的最近、やや大規模に法改正された立法例として、オーストラリアの電気通信法（Telecommunications Act）[101]中にある通信傍受禁止情報及び罰則の部分の二つを訳出し、若干の検討を加えたいと思う。

1　アメリカ合衆国（連邦）

米国においては、連邦法及び各州の州法において、プライバシー保護のための多様な法令が制定されており、その中には違反行為に対する罰則のある法令もある。プライバシー保護の態様は多岐にわたる。その中で、通信傍受の禁止により通信の秘密を保護するというかたちでのプライバシー保護のための基本となる連邦法は、合衆国法律集第一八款の中にある第二五一一条（有線通信、会話または電気通信の傍受及び開示の禁止）である[102]。

日本国の通信関連法における知得、漏示及び窃用に対応する米国連邦法上の条項は、順に、二五一一条(1)項の(a)（傍受）、(c)（開示）及び(d)（使用）である。同条(1)項(b)（器具の使用）は、傍受のための準備行為を意味する。同条(1)項(e)は、犯罪捜査の目的で適法に傍受された通信内容の開示に関する規定である。そして、これらの禁止の違反行為に

対する罰則は同条⑷項であり、また、民事罰は同条⑸項である。

米国連邦法における罰則の法定刑は最も重い自由刑で五年以下の拘禁刑なので、日本国の通信関連法上の罰則に規定する法定刑よりもかなり重くなっているということができる。

以下、米国連邦刑法二五一一条中、同条⑵項及び⑶項の訳出を割愛し、同条⑴項⑷、項及び⑸項の訳出を試みる。(103)

第二五一一条　有線通信、会話または電気通信の傍受及び開示の禁止

⑴　本章中(104)において別段の定めがない限り、以下の者は⑷、項に規定するところにより処罰され、または⑸、項に規定するところにより提訴される。

(a)　意図的に、有線通信、会話もしくは電気通信を傍受する者、傍受を試みる者、または、その傍受をする第三者もしくはその傍受を試みる第三者を幇助する者：

(b)　次のいずれかの場合において、意図的に、会話を傍受するための電気器具、機械器具その他の器具を使用する者、その使用を試みる者、または、その使用をする第三者もしくはその使用を試みる第三者を幇助する者：

(i)　有線通信において使用される電線、ケーブルその他これに類する回線接続手段に当該器具を装着する場合、もしくは、当該器具を介して信号を送信する場合：または、

(ii)　当該器具が電波による通信を送信する場合、もしくは、当該器具が電波による通信の送信を妨害する場合：または、

(iii)　当該器具もしくはその部品が州際取引もしくは国際取引において郵便によって送信もしくは輸送されたものであることを、当該の者が知っている場合もしくは知るべき理由がある場合：または、

(iv) 当該使用もしくは使用の試みが、(A)企業その他の商人について、その州際取引もしくは国際取引に対し悪影響を与える作用を発生させる場合、もしくは、(B)その州際取引もしくは国際取引に対し悪影響を与える作用に関する情報を取得させるものである場合もしくはそのような情報の取得行為である場合：または、

(v) 当該の者が、コロンビア特別区、プエルトリコ領または合衆国の領土もしくは保護領において行為する者である場合：または、

(c) 当該情報が本項の違反となる有線通信、会話もしくは電気通信の傍受により取得されたものであることを知りつつ、もしくは、そのことを知るべき理由がありながら、意図的に、有線通信、会話もしくは電気通信の内容を第三者に開示した者もしくはその開示を試みた者：または、

(d) 当該情報が本項の違反となる有線通信、会話もしくは電気通信の傍受により取得されたものであることを知りつつ、もしくは、そのことを知るべき理由がありながら、意図的に、有線通信、会話もしくは電気通信の内容を第三者に使用した者もしくはその使用を試みた者：または、

(e)[105]

(i) 本章の二五一一条(2)項(a)(ii)、二五一一条(2)項(b)及び(c)、二五一一条(2)項(e)並びに二五一六条及び二五一八条による権限に基づく方法によって傍受された有線通信、会話もしくは電気通信を、意図的に、第三者に対して開示する者もしくはその開示を試みる者が、

(ii) 犯罪捜査と関連する通信傍受によって取得された情報だということを知りつつ、もしくは、そのことを知るべき理由がありながら、

(iii) 犯罪捜査と関連して当該情報を取得しもしくは受信し、かつ、

(iv)　正当な権限に基づく犯罪捜査を不正に阻止し、阻害しまたは妨害する目的を有する場合。

(2)及び(3)（省略）

(4)　(a)　本項(b)に規定する場合または(5)項に規定する場合を除き、本条(1)に違反する者は、本款に基づき罰金もしくは五年以下の拘禁刑に処し、または、これらを併科する。

(b)　暗号化もしくはスクランブル化されていない衛星通信の傍受を構成する行為もしくはそのような傍受と関連する行為であって、本項の違反行為以外の行為である場合、当該通信が次のいずれかに該当するときは、直接・間接に商業的利益または個人所得の獲得を目的とするものでない限り、本項の違反行為とはならない。(106)

(i)　一般公衆に対する再送の目的で放送局に向けてなされる通信：または、

(ii)　公衆に対して開かれている設備に向けて再送するものとされている音楽副搬送波としてなされる通信。ただし、データ通信もしくは電話通話を除く。

(5)

(a)(107)

(i)　当該通信が以下のいずれかに該当する場合、そのような行為を実行する者は、適法に管轄権を有する裁判所において、連邦政府によって民事訴訟を提起される。

(A)　スクランブル化もしくは暗号化されていない民間の衛星ビデオ通信であり、かつ、本章の違反となる行為がその通信の私的視聴であり、かつ、当該行為が不法行為もしくは違法行為ではない場合もしくは当該行為が直接・間接に商業的な利益もしくは個人的な商業的利益の獲得を目的として実行されるものでは

ない場合：または、

(B) 連邦通信委員会の規則第七四Dに基づき割り当てる電波で送信される無線通信であって、その通信がスクランブル化もしくは暗号化されておらず、かつ、当該行為が不法行為もしくは違法行為ではない場合もしくは当該行為が直接・間接に商業的な利益もしくは個人的な商業的利益の獲得を目的として実行されるものではない場合。

(ii) 本項に基づく訴訟においては、

(A) 本章の違反行為が当該の者にとって初回となる(4)項(a)の違反行為であり、かつ、当該の者が本款二五二〇条に基づく民事訴訟において敗訴した者ではないときは、連邦政府は、適切な差止命令による救済を求めなければならない。また、

(B) 本章の違反行為が当該の者にとって再犯以上となる(4)項(a)の違反行為となる場合、または、当該の者が二五二〇条に基づく過去の民事訴訟において敗訴した者ではないときは、当該の者は、五〇〇ドルの民事制裁金の支払義務に服する。

(b) 裁判所は、(ii)(A)に基づいて発する差止命令を執行するために裁判所に認められている権限の範囲内で法的手段を用いることができ、かつ、その命令の違反行為毎に五〇〇ドル以上の民事罰を科さなければならない。

［原文］

§2511. Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who-

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when-

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception

of a wire, oral, or electronic communication in violation of this subsection;

(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

(e)

(i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter,

(ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation,

(iii) having obtained or received the information in connection with a criminal investigation, and

(iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)-(3) [omitted]

(4)

(a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite

transmission that is not encrypted or scrambled and that is transmitted-

(i) to a broadcasting station for purposes of retransmission to the general public; or

(ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)

(a)

(i) If the communication is-

(A) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

(B) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain,

then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

(ii) In an action under this subsection-

(A) if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

(B) if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory 500 civil fine.

(b) The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than 500 for each violation of such an injunction.

2 オーストラリア

オーストラリアの電気通信法（Telecommunications Act）は、二〇〇九年に改正された。この法律には、通信傍受の禁止条項及び罰則が含まれているが、これに加え、犯罪捜査の目的で通信傍受が実行される場合の適法要件等に関する条項も含まれている。すなわち、日本国の法令で言えば、通信関連法及び通信傍受法（平成一一年法律一三七号）を一個の法律として合体したような構造をもった法律である。

最近、スマートフォンなどのモバイル機器等にスパイウェアを密かにインストールし、当該モバイル機器等の利用者の私生活や行動履歴等のデータを取得する行為について、同法に違反する通信傍受行為に該当するとのオーストラ

リア政府（国務長官）の見解が示されたとの報道がなされた。(108) 条文を読めば理解できるとおり、通信傍受の禁止に関する条文は極めて簡素であり、スパイウェアによる個人データ等の取得行為について、同国の電気通信法が定める通信傍受行為に該当するとの法解釈は成立可能である。日本国の通信関連法に定める通信の秘密侵害罪に関する罰則がスパイウェアにも適用可能かどうかを検討する上で参考になるのではないかと考える。

一般に、通信傍受に該当する行為であっても、適法な犯罪捜査の目的などの違法性阻却事由が存在する場合、当該通信傍受は違法行為とならない。しかし、どのような場合に違法性阻却が認められるかについては、議論の余地がある。オーストラリアの電気通信法は、そのような意味で非常に参考になるものと思われる。ただし、本論文では、一般的な禁止に関する条項（同法七条）及びその違反行為に対する罰則（同法一〇五条）の部分のみを訳出することにする。

なお、同法七条で禁止している行為は傍受行為（知得行為）及びその幇助行為である。また、罰則に定める法定刑は、正式裁判による場合には二年以下の拘禁刑であり、略式裁判の場合には六月以下の拘禁刑であるので、日本国の通信関連法に規定する法定刑とほぼ同等のものとして理解することができる。

第七条　通信は傍受できない

(1)　いかなる者も、通信システムを介してなされる通信について、次の行為をしてはならない。

(a)　傍受：

(b)　第三者が傍受することの承認、黙認もしくは許容：または、

(c)　自己または第三者が傍受をすることができるようにする行為もしくは事柄。

(2)ないし(10)（省略）

一〇五条　七条または六三条の違反行為

(1)　七条(1)項または六三条に違反する者は、当該条項の違反行為として有罪である。

(2)　七条(1)項または六三条の違反行為は、本条に基づき、正式裁判として起訴することができ、二年以下の拘禁刑の宣告によって処罰される。

(3)　七条(1)項または六三条の違反行為が正式裁判として起訴することができる場合であっても、簡易裁判の管轄権を有する裁判所は、次の要件を満たす場合に限り、当該違反行為について審理し判決をすることができる：

(a)　訴訟手続が司法長官または検事総長の名で遂行され：

(b)　被告人と検察官との間で合意があり：かつ、

(c)　当該違反行為について、その裁判所が審理及び判決を遂行することが適切であると裁判所が判断する場合。

(4)　七条(1)項または六三条の違反行為のある者に対して(3)項の規定に従い簡易裁判の管轄権を有する裁判所が判決を宣告する場合、その裁判所が科すことのできる刑は、六月以下の拘禁刑である。

［原文］

7 Telecommunications not to be intercepted

(1) A person shall not:

(a) intercept;

(b) authorize, suffer or permit another person to intercept; or

(c) do any act or thing that will enable him or her or another person to intercept;

a communication passing over a telecommunications system.

(2)-(10) [omitted]

105 Contravention of section 7 or 63

(1) A person who contravenes subsection 7(1) or section 63 is guilty of an offence against that subsection or section.

(2) An offence against subsection 7(1) or section 63 is an indictable offence and, subject to this section, is punishable on conviction by imprisonment for a period not exceeding 2 years.

(3) Notwithstanding that an offence against subsection 7(1) or section 63 is an indictable offence, a court of summary jurisdiction may hear and determine proceedings in respect of such an offence if, and only if:

(a) the proceedings are brought in the name of the Attorney-General or the Director of Public Prosecutions;

(b) the defendant and the prosecutor consent; and

(c) the court is satisfied that it is proper for the court to hear and determine proceedings in respect of the offence.

(4) Where, in accordance with subsection (3), a court of summary jurisdiction convicts a person of an offence against subsection 7(1) or section 63, the penalty that the court may impose is imprisonment for a period not exceeding 6 months.

四　まとめ

以上で本論文における検討を終える。

本論文は、科学技術論文ではないので、スパイウェアなどのように主として通信傍受や個人データの隠れた収集のために用いられるコンピュータソフトウェアの技術面に関する詳細な論述は省略した。しかし、現実に大量に存在し、日々ＰＣやスマートフォン等から膨大な量の機密情報を抜き取り続けているスパイウェアの脅威は十分に認識・理解されるべきものであるし、そのためには技術面における事実の理解を欠かすことができない。

今後、サイバー犯罪に関する研究を更に先に進め、より深く研究すると同時に、あるべきサイバー立法論を提示するための考察とその準備を重ねるとともに、その研究結果を論文として公表したいと考える。(109)

注

（1）　サイバー犯罪条約三条は、コンピュータ・データの違法傍受について、「コンピュータ・システムへの若しくはそこからの又はその内部におけるコンピュータ・データの非公開送信（コンピュータ・データを伝送するコンピュータ・システムからの電磁的放射を含む。）の傍受が、技術的手段によって権限なしに故意に行われること」と規定している。

（2）　多賀谷一照・岡崎俊一・岡崎　毅・豊島基暢・藤野　克編著『電気通信事業法逐条解説』（財団法人電気通信振興会、二〇〇八）三八頁

（3）　例えば、東京地裁平成二年七月二六日判決・判例時報一三五八号一五一頁は、「対話者の一方が相手方の同意を得ないでした会話の録音は、それにより録音に同意しなかった対話者の人格権がある程度侵害されるおそれを生じさせることは否定できないが、いわゆる盗聴の場合とは異なり、対話者は相手方に対する関係では自己の会話を聞かれることを認めており、会話の秘密性を放棄しその会話内容を相手方の支配下に委ねたものと見得るのであるから、右会話録音の適法性については、録音の目

的、対象、手段方法、対象となる会話の内容、会話時の状況等の諸事情を総合し、その手続に著しく不当な点があるか否かを考慮してこれを決めるのが相当である」としつつ、「本件録音は、本件捜索差押の被疑事実である昭和六三年一〇月一六日A方に対する脅迫電話の事実自体ないしこれと密接に関連する他の脅迫電話の事実の捜査を目的として、右捜索差押の際に警察官と総括立会人である被告人らとの捜索差押に関する会話及びその際の雑談を録音したものである。そして、その会話の際、被告人は会話の相手が警察官であること及び本件捜索差押の被疑事実が右の脅迫電話の事件であることを認識していた。他方、警察官は、被告人の声を録音するため、被告人に対して話しかけるなどの働きかけをしているものの、その会話は捜索差押の際のものとして特に異常なものとは言えず、またCが被告人に対してした被告人の母親の話も虚偽の内容ではない。その他、警察官が被告人を挑発し、欺罔ないし偽計を用い、あるいは誘導するなど不当な手段を用いて、被告人に無理に話をするまいとしている話をさせたというような事情も認められない」との事実認定を前提に、「以上の諸事情を総合すれば、本件録音は、その手続に著しく不当な点は認められず、適法であると認めることができる」と判示している。

（4）　高橋郁夫・林紘一郎・船橋　信・吉田一雄「通信の秘密の数奇な運命（制定法）」情報ネットワーク・ローレビュー八巻（二〇〇九）一頁、高橋郁夫・吉田一雄「通信の秘密の数奇な運命（憲法）」情報ネットワーク・ローレビュー五巻（二〇〇六）四四頁

（5）　例えば、アナログ式電話の受話器を考えてみると、音声を電気信号に変えて送信し、または、受信した電気信号を音波に変換するだけの装置であり、受話器内に音声信号や電気信号等が一時的にせよ蓄積・記録されるわけではないことから容易に理解することができる。同様に、テレックスのようなデータ通信装置においても、通常は、送受信のための装置内に一時的にせよ電気信号等が蓄積・記録されるような構造にはなっていなかった。これらインターネット以前の時代における通信手段に関しては、星名定雄『情報と通信の文化史』（法政大学出版局、二〇〇六）で詳細に解説されている。なお、アナログ通信からインターネットへは直接に移行したわけではない。その点については、夏井高人『ネットワーク社会の文化と法』（日本評論社、一九九七）三五頁以下で述べたとおりである。

（6）　このことは、通信傍受だけではなく、現実社会の要素の一部を自動的に記録する仕組みの一種である防犯カメラ（モニタ）等でも同じである。撮影された映像は、ディスク等に記録され保存されるが、撮影の対象は常にリアルタイムの「事実」である必要がある。なお、警察活動の一部としての防犯カメラの運用等に関しては、田村正博『全訂警察行政法解説』（東京法令出版、二〇一一）三〇一頁以下が参考になる。

（7）　スパイウェアの定義については諸説あり、必ずしも確定的な見解があるわけではない。しかし、法学上の定義としては、既存の法

令における定義を参考にすることは可能である。そのような法令の一つとして、アメリカ合衆国カリフォルニア州の「コンピュータスパイウェア消費者保護法（California Business and Professions Code Chapter 32. Section 22947–22947.6 - Consumer Protection Against Computer Spyware Act）」が参考になる。同法は、標的マーケティング（Targeted Marketing）または標的商業宣伝広告（Targeted advertising）及びトロイの木馬を用いた攻撃などを想定し、それらによる消費者被害の防止を目的としていることから、スパイウェアの定義についても自ずと限定的なものとなっているものの、スパイウェアの例として、キーロガーと呼ばれる打鍵情報の取得用ソフトウェアやコンピュータ利用者のＷｅｂサイト閲覧履歴といった行動履歴の取得用ソフトウェアなどを明記している。なお、スパイウェアの定義に関しては、米国ＦＴＣの検討結果である Spyware Workshop - Monitoring Software on Your PC: Spyware, Adware, and Other Software, Staff Report, March 2005' Wayne R. Barnes, Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance, University of California, Davis Vol.39: 1545, 2011 が非常に参考になる。

（8）　もちろん、スパウェアの仕様によっては「他人間の通信」に対する干渉となり得る場合があり得る。例えば、ＧＰＳによる位置情報の処理が通信会社（携帯電話会社等）のクラウドサーバと端末装置との間の通信を基礎とする処理によって実行されている場合（特に端末装置がＧＰＳ情報を取得するためのセンサーの機能しか有せず、実際の位置情報処理はクラウドサーバの中で実行されている場合）、そのような位置情報処理のための通信のやりとりに対する無権限のアクセス及びその取得は、通信当事者の通信に対する第三者からの干渉となる。

（9）　データベースを駆使したプロファイリングの応用であるマーケティング技法等については、フィリップ・コトラー（恩藏直人監訳）『コトラーのマーケティング・コンセプト』（東洋経済新報社、二〇〇三）、フィリップ・コトラー（塚本一郎監訳）『コトラー ソーシャル・マーケティング』（丸善、二〇一〇）などが参考になる。しかし、そのような技法の応用については、かなり早い時期から警鐘が鳴らされてきた。例えば、Alexander Halavais, Search Engine Society, Polity, 2009, Simson Garfinkel, Database Nation: The Death of Privacy in the 21st Century, Oreilly & Associates, 2000 などがある。

（10）　ヤフー株式会社の広告表示メールサービスでは、この種の疑義が生じた。しかし、総務省（川端達夫総務相）は、二〇一二年九月一九日の閣議において、ヤフー株式会社のサービスが電気通信事業法に定める通信の秘密の侵害には該当しないとの見解を採用する旨を報告し、閣議において了承されたと報道されている。その後、総務省は、公式に、一定の要件を満たすことを条件にこの種のサービス提供を許容する旨の見解を示した（ヤフー株式会社における新広告サービスについて（総務省・平成二

四年九月二七日）。その背景には、Google などの海外大手企業が既に類似のサービスを提供しており、日本国の企業がこの種のサービスを提供できないとすれば市場を奪われるという危惧感があるとされている。しかし、その米国においても、Google など大手企業による広告付電子メールサービスに関するプライバシーポリシーの適法性について疑問視されている。例えば、カリフォルニア州では、二〇一二年一〇月、同州の州務長官（Attorney General）は、この種のサービスを実行するためのアプリが同州の法令に違反するとして、その提供企業がプライバシーポリシーを適切なものに修正しない限り違法な不正競争行為として扱う旨の見解を示した。また、EU 加盟国の中では、Google の顧客行動履歴解析サービス（Google Analytics）が個人データ保護法に反するものであるとする個人データ保護官（Data Protection Authority）の公式見解表明が相次いでいる。同様に、カナダでは、Google が Gmail で提供しているウイルス検知サービスが自動的にメール内容を読み取り、自動プロファイリングに基づいて自動選定された商業宣伝広告を付加していることがプライバシー侵害に該当するとして大規模なクラスアクションが提起されている。Google はソフトウェアが自動処理するので人間が内容を知ってプライバシー侵害を発生することはないと主張しているが、他方で Google がそのようなデータを自動収集し、ビッグデータ（Big data）として商業利用するビジネスを展開していることも周知のとおりである。そして、収集されたビッグデータ Google の主張は、全体としてみると整合性がとれていない。

これらの点については、以下のサイトで報道されている。

ヤフー、メール内容とマッチングした新広告実施へ 総務省と折衝大詰め（IT media ニュース・二〇一二年八月二七日）http://www.itmedia.co.jp/news/articles/1208/27/news035.html［二〇一二年一一月二日確認］

総務省、ヤフーの新広告は許容範囲（MSN 産経ニュース・二〇一二年九月一九日）http://sankei.jp.msn.com/economy/news/120919/biz12091914240020-n1.htm［二〇一二年一一月二日確認］

California begins crackdown on mobile app developers (Register: 31 October 2012) http://www.theregister.co.uk/2012/10/31/california_privacy_crackdown_mobile/［二〇一二年一一月二日確認］

Using Google Analytics Is Illegal, German Government Officials Claim (Washington Post: November 24, 2009) http://www.washingtonpost.com/wp-dyn/content/article/2009/11/24/AR2009112401493.html［二〇一二年一一月二日確認］

Google Analytics breaks Norwegian privacy laws, local agency said (CIO AU: August 21, 2012)

http://www.cio.com.au/article/434164/google_analytics_breaks_norwegian_privacy_laws_local_agency_［二〇一二年一一月二日確認］

Gmail and privacy: Could Canadian class action lawsuit threaten anti-spam software? (Vancouver Sun: October 5, 2012)

http://blogs.vancouversun.com/2012/10/05/gmail-and-privacy-could-canadian-class-action-lawsuit-threaten-anti-spam-software/［二〇一二年一一月二日確認］

（11） 前掲東京地裁平成二年七月二六日判決

（12） 単なる期待権の一種に留まらず、法的に保護されるべき利益として理解すべき場合はあり得る。たとえば、通信の一方当事者（A）が他方当事者（B）に対して、通信内容を第三者に漏らすことはない旨を確約している場合に、そのように機密性が保証されたと信じたBの信頼は法的にも保護されるべきである。そのような事例において、AがBの信頼を裏切り、A及びB間の通信内容を第三者に提供した場合には、少なくとも損害賠償請求を認めるべき余地があると考える。

（13） 具体的な技術的手段に関しては、Wallace Wang, Steal This Computer Book 4.0, No Starch Press, 2006、M. Sikorski & A. Honing, Practical Malware Analysis, no starch press, 2012、Eric T. Peterson（木下哲也・有限会社福龍興業訳）『Ｗｅｂ解析Ｈａｃｋｓ―オンラインビジネスで最大の効果をあげるテクニック&ツール』（オライリージャパン、二〇〇六）、洋泉社編集部編『サイバー犯罪とデジタル鑑識の最前線！』（洋泉社、二〇一一）、内田勝也・高橋正和『有害プログラムーその分類・メカニズム・対策』（共立出版、二〇〇四）などを参照されたい。

（14） 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（二〇一三）

（15） 例えば、ＧＰＳ情報に関しては、堀部政男編著『プライバシー・個人情報保護の新課題』（商事法務、二〇一〇）二三五頁以下の第七章「位置情報技術とプライバシー―ＧＰＳによる追跡がもたらす法的課題を中心として」［松前恵環］、Ｗｅｂの行動履歴追跡に関しては、同書二八七頁以下の第八章「Ｗｅｂサービスの高度化とプライバシー・個人情報保護」［小向太郎］、行動履歴データに基づく自動プロファイリングに関しては、石井夏生利「ライフログをめぐる法的諸問題の検討」情報ネットワーク・ローレビュー九巻一号一頁などがある。

（16） 夏井高人・岡村久道・掛川雅人編『Ｑ&Ａインターネットの法務と税務（平成二四年改訂版）』（新日本法規出版）八〇九頁

［指宿　信］

（17）　通信傍受以外の方法による監視については、前掲『プライバシー・個人情報保護の新課題』一九三頁以下の「監視・追跡技術と公法的側面における課題」［新保史生］が詳しい。

（18）　例えば、David E. Sanger, Confront and Conceal, Crown, 2012 の一八八頁以下では、オリンピックゲーム（Olympic Games）という軍事上の作戦名で、イランの核施設等に対し特殊なスパイウェアを用いた諜報作戦（核施設内における通信傍受等）が実行されたことが示されている。また、エシュロン（Echelon）と呼ばれる米国諜報機関により構築されていた大規模な衛星通信傍受網については、Nicky Hager, Secret Power, Craig Potton, 1996 が最も詳しい。

（19）　通信法制全体の構造については、多賀谷一照・松本恒雄編『情報ネットワークの法律実務（平成二四年改訂版）』（第一法規）三四二一頁［石谷寧希］が詳しい。

（20）　本論文で直接の検討対象とする電気通信事業法、有線電気通信法、電波法、刑法、不正競争防止法等のほか、通信の秘密侵害行為に対して適用可能な刑罰法令として、著作権法（通信傍受によって複製権侵害が発生する場合など）及び郵便法七七条、日本電信電話株式会社等に関する法律（ＮＴＴ法）一九条に規定する贈収賄罪の規定をあげることができる。

（21）　前掲『Ｑ＆Ａインターネットの法務と税務』五七二頁［木村順吾］

（22）　厳密には、どの法令も適用されない通信形態が存在する。例えば、有線通信でも電気通信でないものについては有線電気通信法が適用されないので、たとえば、カーボンナノチューブなどの中空の線路を用いた空気圧の伝送（音波の伝送の場合を含む。）純水その他の液体の伝送（水圧の変化の場合を含む。）という有線通信の場合、その方法によって仮に機密通信が可能な場合であっても（例えば、暗号化された空気圧の列の送受信など）、それは電磁的な方法による通信ではないので、そのような有線通信には有線電気通信法が適用される余地がない。水圧の変化による通信手段の場合などでも同様である。

（23）　クラウドコンピューティングと関連する法的問題一般については、岡村久道編『クラウドコンピューティングの法律』（民事法研究会、二〇一二）、ＥＮＩＳＡ（独立行政法人情報処理推進機構訳）「クラウドコンピューティング―情報セキュリティに関わる利点、リスクおよび推奨事項（Cloud Computing: Benefits, risks and recommendations for information security）」（二〇〇九年一一月）、Thomas J. Shaw, Cloud Computing for Lawyers and Executive, Autonomous Legal & Technology Publishing, 2011、Renzo Marchini, Cloud Computing - A Practical Introduction to the Legal Issues, BSI Standard, 2010、John W. Rittinghouse, James F. Ransome, Cloud Computing: Implementation, Management, and Security,

CRC Press, 2009′ Charles Oppenheim, The No-Nonsense Guide to Legal Issues in Web 2.0 and Cloud Computing, Facet Publishing, 2012 など。

（24） 前掲高橋ら「通信の秘密の数奇な運命（制定法）」は、数次にわたる法改正を経て現行の電気通信事業法が制定されるに至るまでの間に、「通信の秘密」に関する法解釈が変容したという事実を指摘している。

（25） 高橋　勝「通信の秘密の保障について1」郵政調査時報一三巻二号一頁、同「通信の秘密の保障について2完」郵政調査時報一三巻三号四七頁

（26） 根岸　哲・舟田正之・石村善治・稗貫俊文『通信・放送・情報と法』（三省堂、一九九〇）八一頁以下［舟田正之］

（27） 海野敦史「憲法上の通信の秘密不可侵の権利性とその私人間効力」社会情報学研究一四巻二号一七頁

（28） 最高裁昭和四八年一二月一二日判決・民集二七巻一一号一五三六頁、最高裁平成元年六月二〇日判決・民集四三巻六号三八五頁など。

（29） サイバー犯罪条約の解説書（Convention on Cybercrime Explanatory Report）中の第五一項には、違法傍受罪（サイバー犯罪条約三条）の目的について、「本条は、データ通信におけるプライバシー保護を目的としている。その違反行為は、人と人との間の電話による会話に対する従来型のタッピング及び録音と同様に通信におけるプライバシーの侵害を構成する。このプライバシーの権利は、欧州人権条約八条によって保護されている（This provision aims to protect the right of privacy of data communication. The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights.）」との記載がある。
http://conventions.coe.int/Treaty/en/Reports/Html/185.htm［二〇一二年一一月二日確認］

（30） 前掲サイバー犯罪条約解説書（Explanatory Report）中の一四二項及び一四三項参照。

（31） 京都地裁昭和四一年四月一五日判決・訟務月報一二巻六号八六八頁、大阪高裁昭和四二年一二月二五日判決・判例時報五一四号八二頁

（32） 札幌地裁昭和五九年三月二九日判決・判例時報一一一六号一四三頁

（33） 前掲『電気通信事業法逐条解説』三九頁、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）一二六頁

（34） 前掲『電気通信事業法逐条解説』三九頁、前掲『情報セキュリティの法律』一二七頁

（35）電話盗聴装置から発信された無線電波を盗聴場所の外部に設置した無線受信装置で受信して記録した行為について、東京地裁平成一六年一一月一七日判決（平成一五年（特わ）第七五二一号、平成一五年（特わ）第七八〇三号、平成一六年（特わ）第一六六号、平成一六年（刑わ）第一一三七号）・判例集等未搭載（武富士盗聴事件）は、被傍受者が「他人と通話した内容を盗聴録音」した行為をもって「気通信事業者の取扱中に係る通信の秘密を侵」す行為に該当すると判示している。

（36）盛岡地裁昭和六三年三月二三日判決・判例時報一二六九号一五九頁

（37）横浜地裁平成一五年一月三一日判決・刑集五八巻四号三〇〇頁、東京地裁平成一六年五月七日判決（平成一五年（刑わ）第二三一七号、平成一五年（特わ）第七二六〇号、平成一五年（特わ）第七八〇二号）・裁判所サイト、「最新判例にみる身近な犯罪（9）――中傷・盗聴にかかわる犯罪（平成一四・三・二六札幌地判、平成一四・六・一三大阪高判、平成一六・四・二二大阪高判、平成一六・五・七東京地判）」捜査研究五八巻一〇号八七頁

（38）前掲東京地裁平成一六年一一月一七日判決

（39）例えば、かなり大きなファイルサイズの電磁的記録を傍受するために、伝送中の一個のファイルを傍受し終えるまでに長時間を要した場合などを考えることができる。アクセス集中による輻輳などに起因して通信回線の状況が悪く、結果的に通信傍受を完了するまでに比較的長い時間を要した場合なども同様に考えることができる。

（40）前掲『電気通信事業法逐条解説』三九頁、前掲『情報セキュリティの法律』一二七頁

（41）東京地裁平成一四年四月三〇日判決（平成一一年（刑わ）第三二五五号）・裁判所サイトは、特定の加入電話に関する契約者の氏名、電話番号、電話の設置場所、連絡先などの情報」（基本情報照会）及び特定の加入電話に関する「電話料金の請求書の送付先や支払状況などに関する情報」（料金基本情報）に属するデータの記録行為について、特定の通話との関係での秘密性を有するものではなく、電気通信事業法に規定する罰則の適用はない旨を判示している。

（42）東京地裁平成九年一二月二二日判決・判例タイムズ一〇一一号一八六頁

（43）最高裁平成一六年四月一九日判決・刑集五八巻四号二八一頁（前掲横浜地裁平成一五年一月三一日判決の事件の上告審判決）

（44）前掲『電気通信事業法逐条解説』三九頁、前掲『情報セキュリティの法律』一二七頁

（45）他人宛の電子メールが誤って配信されてしまったような場合がその典型例である。郵便物の誤配の場合も同じである。

（46）前掲高橋ら「通信の秘密の数奇な運命（制定法）」二五頁は概念に明確性が欠けているとの趣旨の指摘をしている。

（47）前掲『電気通信事業法逐条解説』三六頁

（48）　前掲『電気通信事業法逐条解説』三四頁

（49）　一般的な理解によれば、通信内容を知得するだけではなく、知得した内容に従い、一定内容の通信や出版その他の表現行為を禁止することを含むものとして検閲の概念が理解されている。しかし、国その他の公権力機関が単に知得するだけでも国民の表現の自由に対してかなり重大な事前抑制効果があることは明らかであるので、知得行為のみでも検閲が成立すると解するのが正しい。すると、検閲と通信の秘密の侵害とで基本的に内容的な相違は存在しないこととなり、ただ、加害行為の主体が国その他の公権力主体であるかそれ以外の者であるかという点の相違しか存在しないことになる。

（50）　ＮＴＴの前身である電信電話公社は公法人であったので、法人として通信の秘密を侵害する行為は、国またはその機関の行為として理解することが可能であり、したがって、事案にもよるが、あくまでも理論的には、電信電話公社による通信の秘密侵害行為は同時に検閲行為をも構成し得たと解される。

（51）　前掲『電気通信事業法逐条解説』三七頁

（52）　東京地裁平成八年四月二三日判決（平成七年（合わ）第一一二号、平成七年（刑わ）第一〇一一号、平成七年（特わ）第一七七五号）・判例集等未搭載は、被傍受者方の「玄関脇機械倉庫内の電話配電盤である一〇対屋内端子かんの配線に盗聴用発信機を取り付け、同棟一階出入口付近植込み内に自動録音装置付受信機を設置し」、日本電信電話会社が取扱中の「通信の秘密を侵そうとしたが、右発信機の取り付け方法を誤ったため、その目的を遂げなかった」という事案について未遂罪の成立を認めている。また、前掲盛岡地裁昭和六三年三月二三日判決は、電話の保安器内に発信機を取り付け、盗聴録音できるような状態においたけれども、その発信機を「発見され、取り外されたため、盗聴録音の目的を遂げなかった」という事案について未遂罪の成立を認めている。更に、東京地裁昭和五六年七月一六日判決・刑事裁判資料二四六号一一四六頁は、傍受者が電話柱に登り、接続端子函内の加入電話の電話回線に盗聴用発信機を仕掛け直そうとして、「同端子函内にある他の電話回線に右発信機のコードを接続させたうえ」、隣家の「垣根に前記録音装置付受信機を置き、もつて、同公社の取扱中に係る通信の秘密を侵そうとしたが、右発信機のコードを接続した電話回線が」被傍受者の「加入電話の電話回線に隣接する空回線であったため、その目的を遂げなかった」という事案について未遂罪の成立を認めている。

（53）　刑法上でも、秘密を侵す罪としては、同法一三三条（信書開封罪）及び同法一三四条（秘密漏示罪）が存在するのみであり、国その他の公権力主体が国民の秘密を侵害する場合の罪を定めていない。日本国憲法二一条二項前段が「検閲は、これをしてはならない」と定めていることからすると、日本国の憲法は、国その他の公権力主体が検閲をすることがあり得るということ

を当然想定していることになる。ところが、国その他の公権力主体についてその検閲の禁止に違反する行為があった場合の罰則が存在しないことになる。これまた極めて奇妙なことではあるが、罰則の欠缺の一種だと理解することになろう。なお、公務員が実行する検閲については、事案により、刑法一九三条に規定する公務員職権濫用罪が成立することがあり得る（ただし、全てのタイプの検閲行為がカバーされているわけではない。）。しかし、同条に規定する法定刑は二年以下の懲役または禁固であるから、私人である電気通信事業者が電気通信事業法一七九条二項の罪を実行した場合と懲役刑の上限が同じである。すなわち、法定刑の比較からすると、公務員による検閲行為については、私人による通信の秘密侵害行為と同じ程度にしか処罰されないという点で、立法上の問題が全くないとはいえない。

（54）　東京高裁平成九年六月二六日判決・訟務月報四四巻五号六六〇頁は、日本共産党幹部に対する警察による盗聴事件について、被傍受者方の電話回線に隣接するアパートの電話回線を接続して通話内容を傍受する行為は有線電気通信法所定の通信の秘密の侵害行為に該当すると判示している。

（55）　構内無線ネットワークの場合、実際には、有線通信と無線通信との混合物であることが圧倒的に多い。そのため、法令の適用に関しても、有線電気通信法と電波法とが競合して適用され得る場合がある。しかし、適用すべき条項との関係で、どのような物理的対象または物理現象に対して法令が適用されるのかを丁寧に観察すると、一般論としては適用可能な法令が競合しているようにみえる場合であっても、実際には一つの法律しか適用されない場合もあり得る。このタイプの問題を解決するためには、正確な事実認識と技術的知識を十分に獲得することが求められる。

（56）　ハイブリッド型のクラウドコンピューティングサービスを利用する場合を含む。

（57）　今泉至明『二〇〇五年改訂版電波法要説』（財団法人電気通信振興会、二〇〇五）二三〇頁以下

（58）　前掲『電波法要説』二三二頁

（59）　前掲『電波法要説』二三一頁

（60）　無線通信の内容が秘密である場合にのみ罰則の適用がある。無線通信の内容が秘密のものであることについて証拠による証明がない場合について、大阪地裁岸和田支部昭和五二年六月三日判決・刑集三四巻六号四八三頁は、「単に無線通信の存在やその内容を漏らすのみでは罰則の適用はないものである」とした上で、傍受した通信内容が秘密であるかどうかは証拠上明らかでないとして、この公訴事実に関する部分について無罪の判決をした。

（61）　電波法所定の「漏示」の意義について、東京高裁昭和五二年九月一四日判決・刑裁月報九巻九・一〇号六〇五頁は、「無線通

信が誰から誰宛に行なわれたかという事実、またはその行なわれた通信の意味内容を他人に漏らし、また他人が知りうる状態に置くことを指すものと解するのが相当である」と判示している。なお、同判決は、「受信した無線通信をスピーカーを通して二人以上の者が同時に聴取した場合、必ずしもその全員が共同して無線通信を傍受したと認めなければならないものではなく、当該無線機を購入または所持し、これにより無線通信を聴取するに至った目的、経緯、購入または所持した無線機の使用管理の状況等から共同傍受者の範囲を確定すべきであって、共同傍受者と認められない者は共同傍受者と同時に無線内容を聴取した場合であっても、共同傍受者が受信した無線通信の内容を聞かされる第三者の立場にあり、したがって通信の秘密を漏らす相手方となるものといわなければならない」とも判示している。

（62）　電波法所定の「窃用」の意義について、最高裁昭和五五年一一月二九日判決・刑集三四巻六号四八〇頁は「無線局の取扱中に係る無線通信の秘密を発信者又は受信者の意思に反して利用することをいう」と判示している（前掲大阪地裁岸和田支部昭和五二年六月三日判決の上告審判決）。

（63）　前掲『電波法要説』二三二頁

（64）　ペアキー方式の公開鍵暗号を応用した電子署名の付された通信は、暗号化された通信の一種である。しかし、公開鍵を利用可能な者であれば誰でも復号することができ、その意味では公開鍵を利用可能な者は常に潜在的な通信当事者たり得ると換言することもできる。そのような公開鍵による電子署名の付された暗号通信が無線通信によって実行された場合について、電波法一〇九条の二が適用されることはないと解する。なお、電子署名の詳細については、夏井高人『電子署名法―電子文書の認証と運用のしくみ』（リックテレコム、二〇〇一）を参照されたい。

（65）　東京地裁平成一四年六月一三日判決（平成一四年（特わ）第三〇〇〇号）・判例集等未搭載、東京地裁平成一四年三月二〇日判決（平成一四年（刑わ）二六三一号、平成一二年（特わ）五六六号）・判例集等未搭載

（66）　フィッシング（Phishing）を成功させるため、特定の企業や官庁等のＩＰアドレスの信頼性を電子的に証明するための認証局にハッキング（不正アクセス）した上で、認証局の電子証明のために用いられる各種データの無権限書き換えを実行するような攻撃が現実に存在すること（オランダのＣＡである DigiNotar に対する攻撃事例など）については、前掲「サイバー犯罪の研究（二）―フィッシング（Phishing）に関する比較法的検討」の中で触れたとおりである。すなわち、現在のインターネットでは、「誰も信用できない」という状況がいつ発生しても全く不思議ではないという非常に危険な事態に直面しているという事実を認識・理解しなければならない。そのような状況から逃れる方法はある。それは、事柄の本質やその重要性の程度に応

じ、場合によってはＩＴ機器類や電気通信を信用せず、これらを利用しない（逆から言えば、攻撃されても損失が発生しようがない場合だけＩＴ機器類や電気通信等を利用する）ということに尽きる。

（67）　ＰＣやスマートフォン等の支配が完全に奪われ無権限でリモート操作されてしまう可能性があるということ及びその実例に関しては、次のような報道がある。

Trendnet security cam flaw exposes video feeds on net (BBC: 7 February 2012)
http://www.bbc.co.uk/news/technology-16919664［二〇一二年一一月二日確認］

Banking Malware Monitors Victims by Hijacking Webcams and Microphones, Researchers Say (PC World: May 23, 2012)
http://www.pcworld.com/businesscenter/article/255979/banking_malware_monitors_victims_by_hijacking［二〇一二年一一月二日確認］

（68）　フィッシング（Phishing）の場合においても、同様に、被害者を道具とする間接正犯として理解することが可能な場合がある。この点に関しては、前掲「サイバー犯罪の研究（二）―フィッシング（Phishing）に関する比較法的検討」で論じたとおりである。

（69）　他の誰とも通信していないスタンドアロンの状態にあり、スイッチオフになっているスマートフォンをリモート操作によって自動的に起動させた上で、当該スマートフォンの内部にある小型ディスクやメモリチップ等の中に記録されているデータを検出・取得し、加害者のところへと自動伝送してしまうようなタイプのマルウェアが多数存在する。また、スマートフォン等のカメラ機能を自動起動させ、当該スマートフォン利用者の居室や仕事場等の様子を盗撮し、その映像・画像・音声等のデータをリモート操作で自動伝送するタイプのマルウェアも多数ある。このようなマルウェアの感染率は、一般に想定されているところよりもかなり高いと推定する研究者が少なくないし、現にそのような実例がある。

（70）　前掲「サイバー犯罪の研究（二）―フィッシング（Phishing）に関する比較法的検討」

（71）　ソースコードは、コンパイラを用いてコンパイルすることにより、機械語命令で構成される実行モジュールへと変換することができる。インタプリタで実行されるコンピュータプログラムはインタプリタによって逐次的に解釈され機械語命令として実行されるので、コンパイルによる一括して機械語命令に変換するような処理を要しない。現実には、純粋な機械語命令だけで構成されるアプリケーションだけではなく、インタプリタによって実行されるソースコードと機械語命令とが混在したよう

な形式で存在するアプリケーションが多数存在する。また、通常、コンピュータプログラムの実行の際に用いられる設定ファイル、パラメータのリスト、正規ライセンスを認証するための各種データなどは、単純なテキストデータとして存在しているが、それらのデータなしにはコンピュータプログラムを実行することが不可能な場合には、これらのデータがコンピュータプログラムの一部を構成していると理解することも可能である。

（72）　法令の適用関係では、単に「刑法一六八条の二第一項一号及び同項二項の不正指令電磁的記録に該当する」または「刑法一六八条の二第一項の不正指令電磁的記録に該当する」等とすれば足りる。

（73）　ここでは、通信傍受の機能を全く有しないコンピュータソフトウェアを「通信傍受の用に供する目的で作成されるスパイウェアその他のコンピュータソフトウェア」から除外して考えている。他方、例えば、Stuxnet や Flame またはこれらから派生した各種マルウェアのように、通信傍受の機能を含め、スパイウェアとしてのほぼ全ての機能を有するものは「通信傍受の用に供する目的で作成されるスパイウェアその他のコンピュータソフトウェア」に含めて考えている。要するに、客観的にそのような機能を有するか否かが重要である。

（74）　西田典之『刑法各論（第六版）』（弘文堂、二〇一二）三八九頁以下は、主として「コンピュータウイルス」を念頭に置いた記述となっている。しかし、同書三九〇頁にはコンピュータウイルスに感染し発症すると生ずる結果の一例として「外部への送信等による情報侵害」をあげている。「外部への送信等による情報侵害」は、まさにスパイウェア及びトロイの木馬の基本機能の一つであるので、同書では、スパイウェアをコンピュータウイルスの一種であると認識・理解していることになる。

（75）　例外として、当該ソフトウェアを実行するスマートフォン等の利用者が、当該ソフトウェアの機能を十分に認識・理解した上で、事前に同意している場合などには、正当な理由がある。なお、前掲カリフォルニア州のコンピュータスパイウェア消費者保護法では、①権限を有する者による機器類やソフトウェアのリモートメンテナンスの場合、②権限を有するベンダによってブラウザその他のアプリケーションのバージョンアップがなされる場合、③情報セキュリティの確保のためになされる場合、④権限のある者によるシステムやアプリケーションのリモート診断の場合、⑤裁判所の発する令状に基づく犯罪捜査その他の法執行のために必要がある場合などには「正当な理由」があるとの趣旨の規定を設けている。一般に、これらの行為が実行される場合、それが正当な理由に基づくとしても、当該コンピュータシステムの利用者にとっては想定外または想定できない（当該利用者の意図に反する）動作が実行されることになるのが普通である。

（76）　「人」には自己（加害者本人）を含まないから、自己以外の他人のことを意味する。

(77) 例外として、他の者が管理・支配するコンピュータシステムやネットワークシステムとは通信回線等によって接続されていない隔絶された閉鎖的な環境内において、製品開発や学術研究等の目的で、その目的を達するために合理的に必要な範囲内に限定して、通信傍受機能のあるソフトウェアを作成したような場合には、「人の電子計算機における実行の用に供する目的」がない。

(78) 本人が当該ソフトウェアの存在を認識していても、虚偽内容の説明その他の欺く行為により、本人に誤解や錯誤を生じさせている場合には、本人が知らない間になされたのと同価値の状況にあると評価することが可能である。この点について、前掲カリフォルニア州のコンピュータスパイウェア消費者保護法では、欺罔するための手段を用いて、①消去または機能停止していないのに消去または機能停止になったと錯覚させる場合、②利用者が消去または機能停止させようとしてもそうならないのにいつでも消去または機能停止させることができると錯覚させる場合、③虚偽内容の情報を提供することによって誤解させ、消去または機能停止を断念させる場合などをその例としてあげている。

(79) スマートフォンは、「多機能携帯電話」と訳されることがあるが、その実質は、無線による通信機能を有する小型のコンピュータシステムであって、電話機ではないので、PCと同様に「電子計算機」に該当する。いわゆるタブレット型PC、電子ブック閲覧用端末装置、オンラインゲーム操作用端末装置等についても、基本的には同じである。

(80) スパイウェアは、利用者本人が認識している以外の機能を実行するものであるから、利用者本人がそのような機能の実行を望んでいない場合には「意図に反する」ことになる。例外として、当該ソフトウェアを実行するスマートフォン等の利用者が、当該ソフトウェアの機能を十分に認識・理解した上で、①事前に同意している場合、または、②推定的同意が合理的に認定可能な場合には、「意図に反する」動作ではない。

(81) 前掲西田『刑法各論』三九一頁

(82) 前掲「サイバー犯罪の研究（二）―フィッシング（Phishing）に関する比較法的検討」

(83) 専ら犯罪行為の遂行を目的として存在する犯罪組織や違法な団体等の場合を含む。犯罪行為や違法行為を適正に実施するための行政監督などというものは、日本国の法秩序の下においてはあり得ないものだからである。仮にそのような主務大臣が存在し得るとすれば、例えば、広域暴力団を行政監督する主務大臣は、組織犯罪が適正に実施されるように行政監督すべき権限をすることになる（すなわち、広域暴力団の総親分であることになる）が、そのようなことは日本国の国家秩序の下では決して許されることではない。なお、個人情報取扱事業者の該当性有無に関しては、前掲『プライバシー・個人情報保護の新課題』九三頁以下の第三章「個人情報の窃取・漏えいと刑事罰」［石井夏生利］が参考になる。

（84） 競馬の騎手が誰であるかについての情報を電話盗聴により取得したという事案に関する判決として、Francome v Mirror Group Newspapers Limited [1984] 2 All ER 408 がある。

（85） このように解する場合、電波法に規定する暗号化された無線通信と同様、営業蜜の取得行為の理解に関しても、暗号を解読する行為をもって暗号通信の傍受行為でありかつ営業秘密の不正取得行為である（解読の時点で既遂に達する）と解することが可能である。

（86） 条文それ自体から明らかなとおり、不正アクセス行為に限定されることなく、権限を有する者でなければ許容されない行為であり、かつ、営業秘密保有者の管理権の侵害を構成する行為を広く含むものと解される。

（87） 経済産業省「営業秘密管理指針（平成二三年一二月一日改訂）」二三頁は、「不正の利益を得る目的」とは、「公序良俗又は信義則に反する形で不当な利益を図る目的のことをいい、自ら不正の利益を得る目的（自己図利目的）のみならず、第三者に不正の利益を得させる目的（第三者図利目的）も含まれる」としている。

（88） 前掲「営業秘密管理指針」二三頁は、「保有者に損害を加える目的」とは、「営業秘密の保有者に対し、財産上の損害、信用の失墜その他の有形無形の不当な損害を加える目的のことをいい、現実に損害が生じることは要しない」としている。

（89） 関連する複数の犯罪が成立する場合の罪数に関しては、前掲「サイバー犯罪の研究（二）―フィッシング（Phishing）に関する比較法的検討」の中でも若干の検討を加えた。

（90） 電波法においては傍受罪（一〇九条の二）。以下同じ。

（91） 電波法においては漏示罪（一〇九条）。以下同じ。

（92） 電波法の場合には窃用罪（一〇九条）。以下同じ。

（93） 前掲西田『刑法各論』三五二頁は、支払用カード電磁的記録に関する罪の罪数について同旨の見解を示している。

（94） 例えば、A及びB間で特定電子計算機のアクセスのために用いる識別符号を電子メール送信等の電気通信の方法でやりとりしているという事実を加害者（X）が知っており、Xが不正アクセスを実行するために、A及びB間の通信を傍受し、その識別符号を取得するというような事例を考えることができる。なお、XがA及びB間の通信内容を事前には知らなかったが、A及びB間の通信に対する通信傍受により知得した内容をXが認識・理解した後には、取得した通信内容の中に識別符号に該当するものが含まれていることを知り、それをXが保管・提供したというような場合には、応用問題として考えることが可能である。

（95） 不正アクセス行為を手段として私電磁的記録不正作出の行為が行われた場合について、最高裁平成一九年八月八日判決・刑

集六一巻五号五七六頁は、併合罪になると判示している。

(96) 最高裁昭和二四年二月一五日判決・刑集三巻二号一七五頁、最高裁昭和五五年二月二九日判決・刑集三四巻二号五六頁、前掲西田『刑法各論』一四一頁、山口　厚『刑法各論（第二版）』（有斐閣、二〇一〇）一八五頁など。

(97) 例えば、通信傍受の対象となる者（A及びB）が不正アクセス行為その他のサイバー犯罪を実行しようとしている者であり、かつ、電子メール等を用いて犯罪実行用のソフトウェアやデータのやりとりをしているという事実を加害者（X）が知っており、A及びB間でやりとりされているソフトウェアやデータを通信傍受の手段により取得すれば自らも別の不正アクセス行為その他のサイバー犯罪行為を容易に実行することができると考え、その目的で、Xが、A及びB間の通信を傍受し、その通信内容を知得するといった事例を考えることができる。なお、XがA及びB間の通信内容を事前には知らなかったが、A及びB間の通信に対する通信傍受により知得した内容をXが認識・理解した後には、取得した通信内容の中に不正指令電磁的記録に該当するものが含まれていることを知り、それを自らが使用する目的でXが保管・提供・供用したというような場合には、応用問題として考えることが可能である。

(98) 経済産業省「セキュリティホールに関する法律の諸外国調査報告書」（二〇〇三）、土屋恵司「米国における二〇〇二年国土安全保障法の制定」外国の立法二二二号一頁、植月献二「EUの情報通信規制改革―急速な通信環境変化への対応―」外国の立法二四六号四二頁、一般財団法人日本ITU協会「欧州情報通信政策動向調査報告書（二〇一一年一一月二四日）」、岡本秀之・一戸信哉・坂部　望「ASEANの通信法制―シンガポールにおけるサイバースペース関係法の調査研究―（RITE98-J0）」、米丸恒治「ドイツ流サイバースペース規制―情報・通信サービス大綱法の検討」立命館法学二五五号一〇二九頁などがある。海外法令の翻訳としては、大谷健太朗編・監訳「英国通信法―Communications Act 2003 の解説と翻訳―（RITE03-J10）」などがある。

(99) 日本国の国内法に限定した場合でも、通信関連法令（政令、条例、規則、通達等を含む。）の全てに精通した研究者の数は極めて少なく、しかも関連する全ての法的課題に対して適切に対応できる能力を有する研究者は皆無に等しい。

(100) §2511. Interception and disclosure of wire, oral, or electronic communications prohibited
http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap119-sec2511.pdf［二〇一二年一一月二日確認］

(101) Telecommunications (Interception and Access) Act 1979

http://www.1800caught.com.au/pdf/Telecommunications%20_Interceptionand_Access%20_%20Act%201979.pdf［二〇一二年一一月二日確認］

（102） 米国においても、例えば、スパイウェアに適用可能な法令に関する研究等が非常に盛んであり、毎年のようにスパイウェアを規制対象とする連邦法案が提案され続けてきた。しかし、自動プロファイリングによる電子マーケティングを推進しようとする勢力のほうが優勢であり、スパイウェア規制法の立法は成功していない。そこで、現行法の適用についての検討も重ねられているのであるが、なかなかうまくいかない部分がある。なお、この分野において最も詳細な検討結果だと思われるのは、Daniel B. Garrie, Alan F. Blakley, Matthew J. Armstrong, Legal Status of Spyware, 59 Fed. Comm. L.J. 161, January 2007 である。

（103） 原則として直訳としたが、日本語としては理解し難い部分については補って意訳した。なお、用語の意味については、18 U.S.C. § 2510 で定義されているので、同条に規定されている定義に従い、最も適切と思われる日本語を訳語として選定した。

（104） ［訳注］ 第二五一一条は、第一八款第一一九条に含まれている。

（105） ［訳注］ 適法な犯罪捜査を妨害するため、犯罪捜査のために適法に実行された通信傍受により得られた傍受内容である情報を開示する行為を禁ずる趣旨の規定である。

（106） ［訳注］ 衛星テレビ放送の受信及び音楽放送の受信については、その通信が暗号化またはスクランブル化されていない場合、営利の目的で受信する者のみを処罰するという趣旨の規定である。

（107） ［訳注］ 営利の目的のない衛星ビデオ通信及び連邦通信委員会が定める周波数帯の範囲内にある無線通信の受信については、その通信が暗号化またはスクランブル化されていない場合、連邦政府が原告となって民事制裁金の支払を求める民事訴訟を提起することになるという趣旨のことである。日本国では、近似する法的な制裁として、行政罰の一種である過料の制裁がこれに相当する。米国法では、行政官庁によって行政罰が実行されるのではなく、米国政府が原告となり違反者が被告となる民事訴訟において、民事罰としての制裁金の支払いが強制されるという点で、日本国の行政上の制裁制度とは異なった法制度を採用していることになる。また、日本国では、電波法に基づいて所管官庁である総務省が無線通信に用いる電波の周波数帯について、その割り当てをする。

（108） 次のような報道がある。ただし、本論文執筆時点（二〇一二年一一月二日）において、オーストラリア連邦政府国務長官（Attorney General）の公式サイト上で、この点に関する公式見解が示されているわけではない。

Beware apps that hide your cheatin' heart (Stuff NZ: 23 October, 2012) http://www.stuff.co.nz/technology/digital-living/7852724/Beware-apps-that-hide-your-cheatin-heart［二〇一二年一一月二日確認］

（109）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。