論説

通信の秘密侵害罪に関する管見

石井徹哉

第一節　はじめに

電気通信事業法四条は、その一項で、「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、同法一七九条で、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刑罰を科している。電気通信事業法は、その名が示すように、電気通信事業に関して、その公共性に鑑みて種々の規制をなすものであり、この法律は、行政法上の諸規制の根拠として意味を持っている。そのため、従来、その罰則に関してあまり議論されてこなかった。しかしながら、行政規制に関わる領域では、通信の秘密侵害罪を背景として事業者に対する種々の規制がなされている現状がある。この場合、裁判所による公権的な解釈ではなく、行政当局または事業者

側の自主的なかつ自制的な解釈によって電気通信事業者およびその関係者の行動が制約されることになる。

「今日、インターネットは、社会の隅々まで普及し、現代社会の営みに不可欠な手段となっている。いまや、個人の日常生活も企業その他の団体の業務も、インターネットを抜きにしてはほとんど成り立たないとすらいってよい」[1]。しかも、インターネットにおいては、電話回線と異なり、電気通信事業者自身がつねに通信内容を含め通信の秘密を積極的に侵害する状況が迫られている。そのほかにも、電気通信事業法の諸規制が電話を代表とする伝統的な通信回線を前提に立法されたものの、現在のインターネットにおける通信の特性と齟齬をきたしているところが多々みられる。通信の技術的な特性をみても、インターネット通信は、パケットという形で通信内容といわゆる通信の外形部分が一体化されているのであって、電話のように通信内容と受信人・発信人情報といった通信の外形部分が比較的容易に区分しうる通信と同一に考えることは、困難ではないかと考えられる。また、インターネット通信では、事業者自身による通信の秘密の知得の必要性が強く認められる。

本稿は、通信の秘密侵害罪の成立要件および阻却事由に関するいくつかの問題を検討することによって、刑法的な視点から通信の秘密の問題を明らかにし、インターネット通信における現行法上の問題を示すとともに、インターネットを基盤とする社会における将来的な展望への手がかりを導くことを試みるものである[2]。

なお、通信の秘密侵害罪は、電気通信事業法におけるものだけではなく、電気通信の手段の違いから、有線電気通信法九条、一四条および電波法五九条、一〇九条においても同様に禁止規定と刑罰法規が設けられている。もっとも、両法では、各々有線通信、無線通信によるものに限定されるだけでなく、電気通信事業法における通信の秘密が除外されている（有線電気通信法九条、電波法五九条一項参照）。さらに、電波法一〇九条では、無線通信の特性上、知得行為は、処罰されず、漏洩および窃用行為のみが処罰されている。通信の秘密侵害罪とする場

合、本来は、これらすべての罰則を射程にすべきであるが、本稿では、電気通信事業者に係る問題を中心に検討することから、電気通信事業法における通信の秘密侵害罪に限定して論じることとする。

第二節　通信の秘密侵害罪の客体

一　通信の秘密侵害罪の保護法益は、一般社会通念において、通信当事者のプライバシーとして語られることが多い。しかし、ある意味で通信の秘密を侵害する信書開封罪（刑法一三三条）の法定刑が一年以下の懲役又は二〇万円以下の罰金であり、また、業務上取り扱う個人の秘密の侵害である秘密漏示罪（一三四条）の法定刑が六月以下の懲役又は一〇万円以下の罰金であるのに対して、本罪の法定刑は、二年以下の懲役又は一〇〇万円以下の罰金であり、電気通信事業従事者に対する加重刑が三年以下の懲役又は二〇〇万円以下の罰金であることからすると、個人のプライバシーだけを保護法益として説明することは困難である。

本罪の趣旨に関しては、電気通信事業法の前身である公衆電気通信法においても、現在の電気通信事業法においても、憲法二一条二項の「検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。」と規定し、通信の秘密を保護していることから、これを受けて、通信の秘密を確保し、その実効性を担保するために、罰則を置いているものと解されている[3]。公衆電気通信法時代は、通信事業が、公企業としての、日本電信電話公社（旧日本電信電話公社法二条、五条）および国際電信電話株式会社（旧国際電信電話株式会社法）に限定されて認められていた。このような背景においては、公衆電気通信法一一二条の通信の秘密侵害罪について、憲法二一条二項を具体化するものとして理解することは、妥当であったといえる。しかし、電気通信事業が広く民間事業者

に解放されている現状にあっては、通信事業の公共性ゆえに、せいぜい憲法二一条二項の法意に照らして通信の秘密を保護したものと解されるのであって、国家による侵害を問題とする憲法二一条二項における通信の秘密と電気通信事業法における通信の秘密が同一の意義、同一の内容のものであると解する必然性に乏しい。それゆえ、通信当事者のプライバシーの保護を越えて、思想、表現の自由の保障を狙いとする[4]ということが直接の保護対象となっているとは解する必要はない[5]。本罪を憲法二一条二項を受けてのものと解するのであれば、本罪の保護法益は、通信当事者のプライバシーではなく、思想または表現の自由の保障を担保するのに必要な範囲での通信の秘密であると解するのが妥当であろう[6]。しかしながら、そのような制約をここで認める[7]のは、妥当ではない。

それでも、通信の秘密侵害罪は、通信が社会生活にとって必要不可欠なコミュニケーションの手段であることから、それを保護することによって個人の私生活の自由および安寧を保障することを基礎としていることは、否定し得ないが、それよりも、通信の秘密の保護は、コミュニケーション内容が当事者の知らないところで知得されないという通信当事者の期待[8]がその中核を形成していると解するのが適切である。このように解することによって、通信当事者が個人だけでなく、企業等の法人または団体を主体としうることをも説明できることになる。さらに、そのような通信当事者の期待を保護するために、電気通信業務の適正かつ合理的な運用およびこれに対する社会的信頼をも、通信の秘密侵害罪が保護している[9]と解すべきである。それは、通信が第三者に知得される状況が認められる場合、通信手段を安心して使用できなくなり、社会基盤としての通信が機能しなくなり、利用者の社会経済活動に著しい支障が生じてしまうからである。電気通信事業法一条が、電気通信事業の公共性を謳うのは、このような趣旨を含意している[10]。

二　前記の趣旨、保護法益の理解を前提に、通信の秘密侵害罪が客体を「電気通信事業者の取扱中に係る通

信」に限定しているのは、通信が当事者の手を離れ電気通信事業者に委ねられてしまうと、通信当事者が秘密を保護するための自衛措置を講ずることができないこと、秘密が侵害されやすい危険にさらされやすいことから、電気通信事業に対する利用者の信頼を保護する必要があるからである。[11] したがって、「電気通信事業者の取扱中」とは、発信者が通信を発した時点から受信者がその通信を受ける時点までの間をいい、電気通信事業者の管理支配下にある状態のものを意味する。[12] また、「係る」となっていることから、情報伝達が終了した後も、その情報は、保護の対象となり、例えば、通信終了後にもなお電気通信事業者が保管している通信内容等も保護の対象となる。そのため、知得行為等の侵害行為が電気通信事業者の管理下でおこなわれていれば、本罪の客体となりうる。[13]

したがって、通信を前提とせず探知が可能な情報は、たとえ電気通信事業者のもとで管理されていても、そのような情報は、個々の通信とは無関係に蓄積されてものであり、個人の情報として保護する必要性が認められるものの、電気通信事業者の管理下にある通信として知得されていないため、本罪の客体から除外される。[14] なぜならば、このような情報が知得されたとしても電気通信事業の通信の媒介に関する適正な運用およびそれに対する信頼を害することがないからである。

例えば、携帯電話は、電源が入っていると通話時以外にも微弱の電波を発しているため、この電波を最寄りの基地局アンテナで受信すれば、携帯電話のおおよその所在位置を探知することができる。このように探知された位置情報は、通話という個々の通信が確立する以前に、個別の通信と無関係に探知された情報であるから、本罪の客体とはなり得ない。[15] 他方で、同じ位置情報であっても、現在通話中のものであれば、個々の通話の発信場所を示すことになるから、電気通信事業者の取扱中に係る通信に該当し、これを知得した場合、本罪の構成要件に

該当することになる。[16] また、携帯端末のＧＰＳアンテナによる位置情報を当該端末に対して要求し、端末から位置情報を受け取ることは、機械的とはいえ、受発信による情報のやりとりがあることから、通信の秘密を侵すものと解せざるをえない。[17]

三　さらに、街中において無線アクセスポイントから発せられているＳＳＩＤおよび当該アクセスポイントのＭＡＣアドレス[18]を知得した場合、たとえ当該アクセスポイントが電気通信事業者の設置したものであったとしても、[19] これらの情報は、本罪の対象となる通信とはいえず、その行為の目的如何を問わず通信の秘密侵害罪を構成しない。これは、「電気通信事業者の取扱中に係る」ものではないということだけではなく、「通信の秘密」も肯定できないことによる。

まず、無線アクセスポイントは、その存在を示すパケット（ビーコンパケット）を定期的に送出し、一定範囲内にある無線アクセスポイントおよび無線ＬＡＮアダプタを備えた端末は、原則として自由にビーコン・パケットを受信することができる。ビーコンパケットは、ＳＳＩＤ、ＭＡＣアドレスの他、暗号設定、無線チャンネルおよびプロトコルに関する情報を含んでいる。そのため、ＳＳＩＤおよびＭＡＣアドレスは、端末等の間に個々の通信が確立される前に、不特定多数に対して送出され、受信可能範囲内にある携帯無線端末等が自由にこれを受信できるという性質を有する。それゆえ、個々の通信とは無関係に得られる情報であって、これを知得し、保管したとしても、「電気通信事業者の取扱中に係る」通信の秘密を侵したとはいえない。[20]

次に、無線アクセスポイントは、個別の通信が確立する前から不特定多数に対して、上記のように、ＳＳＩＤ、ＭＡＣアドレス等の情報を送出しているのであり、規格に適合している限り、その送出された情報を随意の端末によって受信することができるのであるから、ＳＳＩＤ、ＭＡＣアドレス等ビーコンパケットが送出する情報は、

通信の「秘密」に該当しない。すなわち、「秘密」とは、一般に知られていない事実であって、他人に知られていないことにつき本人が相当の利益を有すると認められる事実をいうが[21]、ＳＳＩＤ、ＭＡＣアドレス等ビーコンパケットが送出する情報は、通信規格に適合する端末によって誰もが自由に知得しうる情報である上、かつ、送出する側からみても、これら情報を公に送出し、告知することによってアクセスポイントとしての機能が果たされるものであるから、客観的にみても主観的にみてもその秘匿を法的保護に値するものとみることはできない。

第三節　通信の秘密侵害罪に関する違法阻却事由

一　電気通信事業者といえども、その取扱中に係る通信の秘密を侵害した場合、通信の秘密侵害罪の構成要件に該当する。電気通信事業法四条二項が、電気通信事業者について他人の秘密の侵害の禁止していることから、事業者が通信当事者となる場合に、本罪の構成要件に該当しないのではないかとの疑念が浮かぶ。しかし、同法一七九条は、四条違反に対して刑罰を科すという立法形式をとっておらず、改めて構成要件の内容を罰条として明示した上で刑罰を科している。したがって、電気通信事業者がその通信の秘密が自己の秘密か他人の秘密かにかかわらずこれを侵害した場合、本罪の構成要件に該当することは否定し得ない[22]。もっとも、同法四条二項が電気通信事業に従事する者について、通信に関して知り得た他人の秘密を守るべきことを規定しているのは、その業務の性質上、通信の秘密を容易に知りうる立場にあるものの、その業務を適切かつ円滑に遂行するのに必要な限度において通信の秘密を知得することがあるからである。この条項の趣旨からすると、電気通信事業者が通信の秘密を侵害する場合について、一定の範囲で正当行為（刑法三五条）として犯罪の違法性が阻却されることが

当然に予定されているといえる。[23]

正当行為による正当化に関して、通説[24]は、行為の目的、手段の相当性、法益侵害の比較、あるいは政策的な配慮などを総合考慮し、社会通念上許容し得る場合、あるいは法秩序全体の見地から許容し得る場合に違法性を阻却すると解している。判例も、行為の目的、手段・方法等の行為態様を考慮し、法秩序全体の見地から当該行為の違法性を判断しているとされている[25]。ただ、その実質的な価値判断としては、利益衡量が内在しており、優越的な利益の原則が妥当しているものと考えられる[26]。

以上の二つのことから、電気通信事業者が通信を配信するに際して自動的、機械的またはこれらに準じた態様において実施する措置は、自動的または機械的であるがゆえに通信の秘密を侵害する虞が少なく、かつ、電気通信役務の円滑、適切な実施、通信の公平な取扱という電気通信役務の公共性を促すものであって、そのため電気通信事業に対する信頼を害するものではない。したがって、正当業務行為として正当化されることになる。同様に、通信事業者が通信を取り扱う際に、輻輳状態が生じ、通信の配信が困難または不可能になっている場合に、輻輳の原因を探索し、これを突き止める行為は、たとえ個別の通信の秘密を侵害するにいたったとしても、違法性が阻却される。この場合、現に通信の秘密が侵されてはいるが、輻輳の原因を追及しない限り、円滑かつ適正な通信状態の復仇が望めないのであって、通信当事者の私的領域に踏み込むことはあっても、通信の安定性の確保を図るという点で通信事業の公共性に適合するものであり、通信状態の復仇こそが通信事業に対する信頼を確保することにつながるからである。また、このように、通信事業役務について正当化が認められるところに、通信の秘密侵害罪の保護法益の重点が電気通信役務の適正性およびこれに対する信頼にあるといえる。

二　前述のような通信業務に直接関わり、かつ、電気通信業務の適正性、安定性等に資する場合は、通信の秘

密侵害罪の違法阻却を肯定できる場面が多い。しかし、電気通信業務を直接に関係しないところで、通信の秘密を侵害する場合、刑法三五条による違法阻却を認めることは困難である。その端的な例が、児童ポルノ掲載サイトのブロッキング行為である。その技術的仕組み[27]の詳細は割愛するが、利用者がプロバイダを通じて児童ポルノサイトへとアクセスしようとする場合、アクセス先を監視し、リストに基づいてホスト名、ＩＰアドレス、ＵＲＬを検知して、アクセスを遮断するものである。この場合、利用者のアクセス先の監視・遮断によって通信の知得および窃用行為が存在し、通信の秘密侵害罪の構成要件に該当する。ブロッキング行為は、電気通信事業に随伴するものではなく、むしろ電気通信事業の遂行とはなんら関係しない別個の利益を保全するためになされるものであり、刑法三五条による違法阻却は、困難である[28]。

そのため、児童ポルノブロッキングに関するガイドラインは、緊急避難（刑法三七条）をその法的根拠として通信の秘密侵害罪の違法性が阻却されるものとしている[29]。すなわち、児童ポルノがウエブにアップロードされている状態は、児童ポルノの拡散により被写体となった児童の権利侵害を拡大する危険性があることから、現在の危難が存在するとし、ブロッキング以外に児童ポルノの拡散を阻止する手段が存在しない場合に、補充性の要件が充足されるとする。また、法益権衡については、被写体児童の性的虐待状況の拡散という権利侵害と通信の秘密[30]を比較した場合、前者の害が上回ることから、この要件も充足するとする。補充性の要件に関しては、児童ポルノ流通を防止するより侵害性の少ない手段（例えば、発信者側による削除、警察による検挙）が存在しないこととされている[31]。この限りにおいては、Take down. Or Block. の原則が維持されていることになる。

児童ポルノのブロッキングに関する通信の秘密侵害罪の正当化の説明として、または、理論的根拠として、緊急避難を用いることは、それ自体妥当であるかのように思われる。しかし、刑法理論として検討する場合、なお

疑念の余地がある。もっとも問題であると思われるのは、緊急避難を根拠とする行為をガイドラインによって規定しているところにある。ブロッキングを実施することは、各プロバイダの自主的な取組みとされているものの、ガイドライン[32]により実施方策を策定し、これに準拠して実施することは、実質的に児童ポルノのブロッキングの行動準則を規定していることに等しい。もともと緊急避難は、その法的性格について責任阻却事由とする見解もあるように、正当な利益の拮抗状態における利害調整の機能を果たすものであり、裁判時における事後的な評価によってなされるものである[33]。もっともこのような考え方に対しては、異論もあり、違法阻却事由も行為規範の内容をなすとの消極的構成要件論も主張されている[34]。この点に関して、理論的な一致点を見ないまま、特定の立場を前提にすることは、ガイドラインとしての性格上望ましくない。

また、ブロッキングを行動準則としてガイドラインに規定することは、実質的には、ブロッキングを行為規範化することになってしまう。このことは、児童ポルノの存在を認識しながら、ブロッキングの措置を講じない場合、不作為による児童ポルノの罪の正犯または共犯が成立する可能性を生ぜしめることになる[35]。電気通信事業法における通信の秘密は、たんに個人の私的領域の保護を目指すにとどまらず、通信事業者にいわば「土管」としての役割を徹底させ、不用意に特定の行動をさせないことで、電気通信事業の適切な運用、通信の安定性等の公共性に資することをも目的にしているものであり、緊急避難状況があるとしてもガイドラインによる行動準則化は、法の目的にあまりに反するように解される。ブロッキングは、リストを元にしてアクセスの可否を判断するものであって、個別の避難措置ではなく、継続的な運用であることからしても、前述の疑念は、一層高まることになる[36]。

より根本的な疑問は、実質的にみて、Take down. Or block. の原則が妥当しているのかというところにある。

緊急避難が認められるには、補充性の要件が充足されなければならない。警察による検挙やサイト管理者による削除が実施されないことがこの要件充足の前提になる。問題は、削除要請がそれほど機能し得ないものなのかというところにある。ドイツでは、児童ポルノのブロッキングに関する立法をしたものの、削除が功を奏したため、結局、当該法律を撤回することになった[37]。立法後も、ブロッキングを実施する前に削除の実効性を検証したところ、連邦刑事局および各州の警察当局による海外のプロバイダに対する削除要請が適切に実施されたため、「ブロッキングに代えての削除（Loschen statt Sperren）」との方針を連邦政府がとることとし、コミュニケーションネットにおける児童ポルノ対策に際するブロック規制の消滅のための法律[38]が成立し、児童ポルノに対して徹底した削除によって対抗することとなっている。ドイツにおいて有効に実施されていることがわが国ではいまだ困難なままとなっているのかがまず問題とされるべきである。児童ポルノの拡散行為を含めネットワークにおける児童の保護は、法制度だけでなく、官民共働における適切な役割分担があってこそ効果を発揮するものである。国内外の児童ポルノの削除または遮断の有効な実施のあり方をまず検討することが必要である。

また、国内サーバにおいてなお児童ポルノの拡散に対して削除またはサーバの遮断等が有効に機能しないのは、プロバイダまたはサイト管理者の削除または遮断の懈怠に対して刑事責任の成否が曖昧なところにあるのかもしれない[39]。EUないしはドイツにおいては、コンテンツプロバイダおよびホスティングプロバイダに対して一定の責任を問うことが可能とされている[40]。いずれにしても、プロバイダの自主的取り組みによって、児童ポルノがサイトに上がっている場合には、積極的に削除しうる仕組みができあがっていると、ブロッキングは、不要となり得るということには、留意しておくべきであろう。さらに、たびたび取りざたされる児童ポルノ規制に関する法改正では、禁止対象の拡大にのみ議論が偏在している[41]が、児童の性的虐待・性的搾取を防止し、児童に対する権

利侵害を阻止するには、どのような手法がもっとも効果的であるかという抜本的な議論が必要であって、刑事規制は、有効に阻止し得なかった（施策、政策の失敗）場合のあくまで補助的な手段でしかないことを再度想起しなければならない[42]。なお、削除または遮断に際し、通信の秘密の侵害が障碍となっているのであれば、まずその点を精査すべきである。

第四節　犯罪捜査に関する民間事業者との共働

一　ネットワークにおける犯罪行為に対し効果的かつ迅速に証拠を確保するためには、捜査機関による証拠収集だけではなく、一定の範囲において民間事業者との共働が必要となる場合がある。これは、ネットワーク犯罪にのみ必要となるものでないことは、刑訴法一九七条において、捜査事項照会に関する規定が置かれていることからも示される。それに加え、サイバー犯罪条約批准のための国内法整備にともなう刑訴法改正によって導入されたのが、通信記録の保全要請（刑訴法一九七条三項ないし五項）である。これは、差押えまたは記録命令付差押えをするため必要があるときは、電気通信を行うための設備を他人の通信の用に供する事業を営む者等に対し、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、三十日を超えない期間を定めて、これを消去しないよう、書面で求めるという措置である。これは、通信記録が短期間に自動的に削除されうる虞がある[43]ことから、将来差押え等の対象となるものを削除されない措置をとり、将来実施されうる証拠収集に支障がないようにするものである。捜査機関が通信記録等に直接アクセスすることはないため、任意捜査の手法のひとつとして刑訴法一九七条に規定されている。

二　しかしながら、最近のインターネットにおける技術的な動向からすると、保全要請をプロバイダ等が実施しようとすることで――実際にそのような状況が捜査に必要上生じうるのかどうかは明らかではないものの――通信の秘密侵害罪が成立してしまう懸念が認められる。考えうる例のひとつは、携帯電話等から携帯電話の回線を通じてインターネットにアクセスしている場合に、当該携帯電話端末に係るインターネットのアクセス記録を保全する場合である。携帯電話事業者によるであろうが、携帯電話回線を通じてインターネットにアクセスする場合、複数の端末がすべて同じＩＰアドレスを共用し、事業者内部のルーティングによって個別の端末へインターネット通信を配分している場合がある。この場合、具体的な携帯端末に係るインターネットのアクセス記録の保全要請を捜査機関が要請しても、事業者の側で当該端末の通信履歴等を保全するには、共用しているＩＰアドレスに係る通信履歴を精査し、指定された端末の通信履歴とそれ以外のものを峻別する作業が必要となる。この作業では、場合により、指定された通信履歴以外の多数の者の通信履歴を知得することが不可欠であって、いわば犯罪とまったく無関係な者の通信の秘密が侵害されることになる。

もう一つの例は、ホスティングサービスを提供している場合、比較的廉価にサービス提供するために、一台のハードウエアを用意し、そのシステム上に複数のバーチャルなシステムを複数さらに稼働させ、そのバーチャルなシステムをひとつのサーバとしてホスティングに供することがなされているものである。この場合、個別のバーチャルなサーバシステムおよびそこにふられているＩＰアドレスに関する通信履歴は、サーバ契約者に対する保全要請により可能であろう。しかし、バーチャルサーバの一つに対する攻撃状況に関する通信履歴の保全をしようとする場合、あるいは、そのような攻撃に備えて通信履歴を保全しようとする場合、共用されているひとつのハードウエアとしてのネットワークカードにバーチャルサーバの複数のＩＰアドレスがアサインされている

ことから、ハードウエアを提供する事業者において、すべてのパケットをキャプチャし、利用者ごとに振り分けることが必要になりうる。[44] 通信記録の適切な保全には、保全要請如何に関わらず、つねにすべてのパケットを精査して分別することが必要となり得るが、これは、捜査の必要といったなんらの正当化の契機も認められないため、通信の秘密侵害罪の成立を否定することは困難であろう。

三　保全要請の局面に限定されず、インターネットサービスにおいてクラウド化の進展が指摘される今日、ネットワーク犯罪の被害者の側においても、捜査機関に対する協力をする場合においても、民間事業者が証拠の確保・保全に向けた措置を実施する場合、通信の秘密を侵害することが不可避となる場合が一層増えていくことが予想される。こうした場合、通信の秘密侵害罪に該当するという判断をもって事業者が被害者または捜査機関との共働を拒む事態になれば、証拠保全が不十分であることから証拠収集に困難をきたしてしまうことになるであろう。

問題は、保全要請にとどまるものではなく、インターネット上における犯罪行為の証拠の保全・確保、犯罪予防のための攻撃方法の調査等にあたって民間事業者またはサイトを管理している通常の市民に協力、自主的な取組みが重要となる場合[45]がある。これらの協力等は、つねに通信の秘密侵害罪を犯すリスクを内包することになると、ネットワーク犯罪への十分な対応が困難になる虞がある。これまでのわが国の対応をみると、この領域においては、何かの問題があると、立法措置を検討するのではなく、業界団体等の自主的な取組みとの名の下にガイドラインを策定する等して対応したきたにすぎない。このようなガイドライン策定による対応は、いわば弥縫策でしかない。そればかりか、責任所在が曖昧化され、本来なされるべき実質的な利益衡量がなされるのかどうかにも、疑問が残らざるを得ないのである。

翻って考えてみると、電気通信事業法は、事業主体の変化に応じて適宜改正されてきたものの、通信それ自体の形態、性質等の変化に応じて改正はされてきたわけではない。電信電話に代表される従来型の通信においては、特に事業者が主体となって通信の秘密を保護することが肝要であり、いわば通信事業者の管理・支配する通信経路を保護すれば目的を達しうるというところに特徴がある。この場合、通信の日時、場所等の通信の外形部分の保護が同時に通信内容の保護へと結びつくことにもなる。通信記録の探知は、ただちに通信当事者のプライバシーを暴く可能性を秘めている。これに対して、インターネット通信において、パケットにおけるヘッダ情報、通信履歴、通信記録にかかるヘッダ情報は、通信内容の保護の点からみて保護する必要性が乏しいように解せられる。通信記録に係るデータを探知・知得しても、それにかかる通信内容、通信当事者が直ちに明らかになるわけではない。また、暗号化されていない通信では、通信経路全般にわたって通信内容ですら知得される可能性が高い状態にある(46)。このような実態に、現行の電気通信事業法による通信の秘密の保護は、適切なものといえるか再検討を要する。

立法的な展望としては、現行のまま通信の秘密侵害罪を残すのであれば、インターネット通信に特化した領域でもう少し柔軟な対応が可能な法的枠組みを策定し、違法阻却の余地を広げることが必要ではなかろうか。現行法のままではあまりに違法阻却の余地が狭すぎるように解せられる。あるいは、通信の秘密侵害罪のあり方を再度検討し、通信媒体によって精緻に区分けして構成要件を記述する方法もありえよう(47)。

（1） 井上正仁「電話逆探知の適法性」内藤謙先生古稀祝賀『刑事法学の現代的状況』（一九九四年）四八五頁参照。

（2） 第九回デジタル・フォレンジック・コミュニティ2012 in Tokyoにおける講演「サイバー犯罪条約批准後の法的課題」（二

○一二年）および情報セキュリティ大学院大学共同研究「インターネットと通信の秘密」第五回研究会における講演「通信の秘密侵害罪の現状と課題」（二〇一三年）の一部ならびにそれぞれの講演における質疑応答が本稿の基礎となっている。

（3）伊藤榮樹・小野慶二・荘子邦雄編『注釈特別刑法第六巻交通法・通信法編Ⅱ』（一九八二年）三四六頁〔河上和雄〕、多賀谷一照ほか著『電気通信事業法逐条解説』（二〇〇八年）三六頁。

（4）河上・前掲注三・三四六頁。

（5）なお、大阪高判昭和四一年二月二六日高刑集一九巻一号五八頁は、公衆電気通信法一一二条に関して、表現の自由の保障を問題とするが、各々の法律の背景が異なる以上、電気通信事業法にまで同様の理解が妥当すべきであるとはいえない。

（6）橋本公亘『憲法』（改訂版・一九七六年）三八六頁。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（二〇〇六年）四四頁以下、高橋郁夫ほか「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（二〇〇九年）一頁以下参照。

（7）もっとも憲法二一条二項の規定を受けて思想・表現の自由の保障を実行ならしめるということを主張する場合、通信の秘密の保護は、憲法上の保障対象であることを強調し、一切の例外を認めず、通信内容にとどまらず、通信に関わるあらゆる情報を保護すべきだという反対方向の論理へと帰結されることが、一般的である。佐藤幸治『日本国憲法論』（二〇一一年）三二〇頁以下参照。

（8）期待権といってもよいが、広い意味においては、プライバシーであろう。それは、個人の人格権に基づくものであろう。

（9）河上・前掲注三・三四六頁参照。

（10）多賀谷・前掲注三・一八頁以下参照。

（11）多賀谷・前掲注三・三七頁。

（12）多賀谷・前掲注三・三五頁。

（13）最決平成一六年四月一九日刑集五八巻四号二八一頁は、電気通信事業者が現に取り扱っていた際に盗聴録音された通信内容の一部をそのまま再生して他に漏らす行為についても、旧電気通信事業法一〇四条一項に該当するとしている。

（14）池田弥生「携帯電話の位置検索のための令状請求」判タ一〇九七号（二〇〇二年）二七頁。東京地判平成一四年四月三〇

日（平成一一年（刑わ）第三二五五号）http://www.courts.go.jp/search/jhsp0030?hanreiid=5834&hanreiKbn=04は、「『加入者データ読出・結果出力画面』のデータは、特定の携帯電話（電話番号）につき、通話中か否かの通話中情報や位置情報や設定されている留守番電話サービス用暗証番号などを記録している。このうちの、例えば当該携帯電話（電話番号）につき設定されている留守番電話サービス用暗証番号については、個々の通信とは無関係なものとして保管されている情報であり、『通信の秘密』には当たらない。」と判示している。

（15）池田・前掲注一四・二七頁。

（16）前掲東京地判平成一四年四月三〇日参照。

（17）通信の構成要素（通信の日時、場所、通信当事者の氏名、住所・居所、電話番号等の識別符号、通信回数など）は、それにより通信内容が探知される虞があり、かつ、それらの情報が特定の通信が存在するという個人の私的生活の領域を明らかにする可能性があることから、「通信の秘密」は、通信内容にとどまらず、通信の意味内容が推知される情報すべてを包含する（多賀谷・前掲注三・三八頁）。したがって、通信の発信場所としての位置情報は、これに該当することになる。

（18）ＳＳＩＤとは、Service Set Identifierのことで、無線ＬＡＮにおけるアクセスポイントの識別子のことをいう。またＭＡＣアドレスとは、Media Access Control addressのことで、ネットワーク端末、アクセスポイント等のハードウエアの識別子のことをいう。

（19）個人が設置したものである場合は、電気通信事業者の管理に係るものではない。

（20）グーグル社のストリートビューカーによる無線ＬＡＮを経由した情報収集に関して、電気通信事業法四条に規定する「通信の秘密」が侵害するものとして、総務省による行政指導がなされた（http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000056.html）。しかし、それは、無線ＬＡＮを経由した通信の一部を誤って収集したことに対するものであって、その指導内容として、「現在サービスに供されているサーバー上に保管されている電気通信事業者が提供する無線ＬＡＮを経由した通信に係る記録（通信確立前のものを除く。）の削除」および「通信確立後の通信に係る情報の収集・記録等事案の再発防止及び今後の法令遵守の方策の策定」とされていることから、通信確立前の情報については、問題ないものと判断していることが推測される。

(21)　多賀谷・前掲注三・三八頁。

(22)　昭和三八年一二月九日の内閣法制局見解（昭和三八年一二月九日内閣法制局一発第四二号・郵政大臣官房電気通信管理官宛内閣法制局第一部長回答を典拠として、他人の秘密と自己の秘密の区別を通信の秘密侵害罪の成否にとって重要視する考えもありうる。この内閣法制局見解の問題点および逆探知の法律構成については、井上・前掲注一・四八六頁以下参照。

(23)　この点で、同法四条は、行政規制としての意味が特に重要となる。

(24)　大塚仁ほか編『大コンメンタール刑法第二巻〔第三五条～第四四条〕』（第二版・一九八九年）二四三頁以下〔古田佑紀〕。

(25)　川端博ほか編『裁判例コンメンタール刑法第一巻〔§1～§72〕』（二〇〇六年）二一三頁以下〔佐久間修〕。

(26)　石井徹哉「いわゆる『デュアル・ユース・ツール』の刑事的規制について（下）」千葉大学法学論集二七巻二号（二〇一二年）五三頁以下。

(27)　http://blocking.good-net.jp/relation/参照。

(28)　詳細は、森亮二「ブロッキングに関する法律問題」ジュリスト一四一一号（二〇一〇年）七頁以下、九頁以下参照。

(29)　安心ネットづくり促進協議会「児童ポルノ対策作業部会法的問題検討サブワーキング報告書」（二〇一一年）、森・前掲注二八・一〇頁以下。

(30)　私見によれば、害の衡量には、通信の秘密だけでなく、電気通信事業の適正な運営およびそれに対する信頼も附加されるべきであるが、それを加えたとしてもなお児童ポルノの拡散による権利侵害が上回るものと解される。このことは、児童ポルノ公然陳列罪の法定刑（五年以下の懲役若しくは五〇〇万円以下の罰金または併科）と通信の秘密侵害罪の法定刑の比較によっても明らかである。

(31)　森・前掲注二八・一一頁。

(32)　例えば、安心ネットづくり促進協議会「ＤＮＳブロッキングによる児童ポルノ対策ガイドライン」（第二版・二〇一二年）。

(33)　このような立場をとりつつ、行為規範違反を構成要件該当性の実質と理解することがいわゆる厳格責任説に結びつく。福田平『違法性の錯誤』（一九六〇年）二一八頁以下。

(34)　例えば、葛原力三「消極的構成要件要素の理論」中義勝先生古稀祝賀『刑法理論の探求』（一九九二年）六七頁以下、とり

わけ七五頁以下、井田良『講義刑法学・総論』（二〇〇八年）三五〇頁以下。

(35) あくまでガイドラインであるから、そのような作為義務は生じないとするのは、安直すぎる。

(36) だからといって、ブロッキングを立法によって可能とすることは、必ずしも適切であることにはならない。国家が情報流通の阻止に積極的に介入することは、憲法二一条一項の表現の自由に対する直接的な侵害となる上、通信においてこれをなすことは、まさに検閲の禁止、通信の秘密の保護という憲法二一条二項に直接抵触することとなる（森・前掲注二八・一二頁）。児童ポルノが個人の人格権を完全に否定するものであるという深刻な権利侵害との共通認識がある社会においては、公共の福祉の観点からこのような介入もなお許容されるかもしれない（失効したとはいえ、ドイツでは、ブロッキングが法律により実施可能なものとされたのが証左である）。しかし、わが国では、児童ポルノの問題性に対する社会一般の認識が甘く、積極的な介入を是認することは困難であろう。

(37) http://www.bundesregierung.de/nn_1272/Content/DE/Artikel/2011/04/2011-04-13-loeschen-statt-sperren.html

(38) Gesetz zur Aufhebung von Sperregelungen bei der Bekampfung von Kinderpornographie in Kommunikationsnetzen, BGBl I 2011, 2958.

(39) 学説を見るならば、個々の論者により様々なニュアンスの相違がある。渡邊卓也『電脳空間における刑事的規則』（二〇〇六年）八四頁以下参照。

(40) 詳細は、石井徹哉「アクセスプロバイダの刑事責任(1)」千葉大学法学論集二〇巻四号（二〇〇六年）三三頁以下参照。Eric Hilgendorf, Strafrechtliche Anforderungen an den Jugendmedienschutz im Internet. Unter besondere Beru cksichtigung der strafrechtlichen Verantwortlichkeit von Zugangs-Providern, in: Nikolaus Bosch/Stefan Leibe (Hrsg.), Jugendmedienschutz im Informationszeitalter, 2012, S. 105ff., 1111ff. もともとプロバイダの免責に関するものであるが、責任を問いうる場合が例外的に示されている。なお、ヒルゲンドルフは、アクセスプロバイダについてすら、児童ポルノを遮断しなかったことについて不作為犯の成立を肯定すべきであるとする。

(41) 条例では、すでに先行した刑事規制が存在する。例えば、奈良県の子どもを犯罪被害から守る条例（平成一七年奈良県条例第九号）は、一三歳未満の子どもを被写体とするポルノを規制し、その単純所持を処罰している（同条例二条、一三条、

一五条）。しかし、一三歳未満の者のポルノの規制強化に反対するものではないが、本条例は、現行の児児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律（以下「児童ポルノ法」）があえて規制対象から除外した行為を処罰するものであり、憲法九四条に違反する疑いが極めて強い。また、条例の目的（一条）からみても、同条例のいう子どもポルノを刑事規制する合理的関連性が認められない。これらの点で、きわめて感情的なまたはポピュリスティックな規定であるといえよう。附言すると、児童ポルノの単純所持を児童ポルノ法により規制すべきとの強硬な意見が主張され、その際に、諸外国ではすでに単純所持が規制されているとの理由が述べられることが多い（例えば、日本ユニセフ協会「子どもポルノと日本の現状」http://www.unicefor.jp/special/0705/slide/slide.html）。しかし、正確な比較法研究をすればすぐわかることであるが、単純所持を規制するとしても、日本における児童ポルノの定義に該当するような広範囲のものについてすべて単純所持を規制しているわけではない（一〇年以上前の比較法研究ではあるが、vgl. Ulrich Sieber, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet, 1999, S. 69ff. また、最近のドイツにおける規制については、例えば、Jasmin Palm, Kinder-und Jugendpornographie im Internet, 2012, S. 89ff.）。このようなきわめて単純化された犯罪化の主張にこそ注意しなければならない。

（42）　京都府の京都府児童ポルノの規制等に関する条例（平成二三年京都府条例第三二号）は、児童ポルノ法にいう児童ポルノの単純所持、保管および取得を禁止している（同条例二条二項、七条一項）が、その違反に対して刑罰を科すのではなく、所持に対して知事による廃棄命令の措置をとらせ（八条）、その命令違反に対して刑罰を科す（一三条二項）仕組を導入にしている。なお、取得行為については、直罰規定がある（一三条一項）が、規制対象となる児童ポルノの範囲が児童ポルノ法二条三項一号および二号のものに限定されているところに特色がある。いわゆる三号ポルノを除外する点で注目すべきであるが、無対価の取得行為を処罰するだけの実質的な根拠があるのかという点には、なお疑問が残る。立法措置によるとしても、三号ポルノの規制のあり方を工夫しない限り、実質的な処罰根拠に裏付けられた刑事規制は、困難であるし、刑事規制以外の手法による効果的な規制もなしえないだろう。

（43）　電気通信事業法四条に関連して、総務省による個人情報電気通信事業における個人情報保護に関するガイドライン（平成一六年総務省告示第六九五号。最終改正平成二一年総務省告示第五四三号）二三条によると、通信履歴は、保存期間が経過

したときは速やかに消去する必要があり、その期間は、サービスの種類や課金方法、通信履歴の種類ごとに限定的に設定すべきものとされ、さらに、保存期間を設定していないときは、記録目的を達成後速やかに消去する必要があるとされている。

(44) 小山覚「『情報処理の高度化等に対処するための刑法等の一部を改正する法律』の実務的課題」第八回デジタル・フォレンジック・コミュニティin Tokyo 2011（二〇一一年）。

(45) ハニーポットを設置して、有害なパケットを解析しようとすることも、通信の秘密侵害罪に該当しうる。

(46) だからといって保護に値しないというわけではない。しかし、電気通信事業法の通信の秘密侵害罪は、信書開封罪に対当する通信の秘密を保護しようという形式にみえるが、インターネット通信は、比喩的いえば「はがき」による通信の秘密（はがきの内容に秘密性が肯定されるかどうかは一応留保しておく。だが、信書的な扱いになるには、通信の暗号化が必要である。）を保護しようというものであり、実態と法制度の乖離が激しい。

(47) これに関連して、インターネットの領域では、通信履歴の知得による統計処理、マッピング処理、ＤＰＩによる利活用の可能性が提案されているが、いずれも通信の秘密侵害罪による違法性を阻却しないことから、実施できない。通信当事者の同意を得ようにも、一方当事者の同意しか得られないのでは、違法阻却の検討にとって明らかに不十分であるし、通信業務と無関係な領域での正当化は、通信当事者の同意があっても困難なように思われる。現行法上可能なのは、通信を前提としないところで蓄積された情報の利用のみであろう。

※ 本稿は、財団法人電気通信普及財団の研究助成による研究成果の一部である。