サイバーセキュリティ対策と通信の秘密

海　野　敦　史

Interrelations between Measures to Ensure Cybersecurity and Secrecy of Communications in Japanese Law

Atsushi UMINO

Abstract

It has been suggested that secrecy of communications stipulated in the Constitution of Japan and some legal acts hinder measures to ensure cybersecurity. This paper challenges this view and postulates that the legal interests of secrecy of communications include ensuring the security of communications networks. However, there are indeed few, and mostly scattered articles that stipulate secrecy of communications in Japanese law. It appears that they are based on the notion that "secrecy" is tantamount to privacy or what we would like to hide. On this basis, they are interpreted as if they were intended for the prohibition of actively knowing, leaking or utilizing information that is secret in communications. As a result, Japanese legal acts do not stipulate concrete measures that may be needed to ensure cybersecurity or the security of networks, although a basic act on cybersecurity enacted in recent years requires public authorities to take necessary legal measures for cybersecurity. If the Constitution of Japan allows a certain level of measures to ensure cybersecurity, even though they might accompany legal acts that actively grasp the secrecy of information, they should be articulated in relevant laws such as the telecommunications business act. Therefore, we need to determine and articulate under law to what extent these measures are allowed while balancing this with protecting privacy in communications.

Key Words

secrecy of communications, Constitution of Japan, cybersecurity, telecommunications business act, cyber attacks

目　　次

1 序　論

近年，デジタル社会の進展，5Gや人工知能（AI）等の新興技術の発展，新型コロナウィルス感染症の拡大に伴う通信用ネットワーク（以下，単に「ネットワーク」という）への依存度の高まり，サイバー攻撃をはじめとするサイバー空間における脅威の悪質化・巧妙化等の複合的な要素を背景に，サイバー空間全体の安全性・信頼性ないしサイバーセキュリティ[1]の確保の必要性が著しく増している．このような状況を受け，近時の我が国では，サイバーセキュリティ基本法（平成26年法律104号）に基づくサイバーセキュリティ戦略が改定され，「誰一人取り残さない」サイバーセキュリティの確保の方向性が打ち出されたところであるが[2]，国際的な評価は必ずしも高いとは言えないようである．例えば，2021年6月，英国の政策研究機関である国際戦略研究所は，サイバーセキュリティの確保の水準に関して日本を3段階のうち最も低いグループに位置づけ，通信の秘密という憲法上の制約があることが主因となって攻撃的なサイバー機能が未発達となっているという旨を説いている[3]．通信の秘密がサイバーセキュリティを適切に確保するために必要となる対策（以下，「サイバーセキュリティ対策」という）を講じるうえでの妨げとなるという旨は，しばしば国内でも指摘されている[4]．

もとより，通信の秘密とは，日本国憲法（以下，「憲法」という）21条2項後段において規定され，電気通信事業法（昭和59年法律86号）4条をはじめとする関係の法律で具体化されているものである．憲法上の通信の秘密の保護の前提には，国民各人の「通信の自由」[5]があると解されている[6]．通信の秘密は，通信の自由を保護する砦となる基本権であるにもかかわらず，なぜサイバーセキュリティ対策を講じるうえでの障壁として位置づけられることになるのだろうか．サイバーセキュリティ対策が適切に講じられることは，憲法の予定する「通信」を国民が利用するうえでの必要条件となるのであって，通信の秘密に関する規定がこれを阻むというのは論理的な矛盾ではないだろうか．仮に当該規定が所要のサイバーセキュリティ対策を妨げることとなっているのであれば，それは通信の秘密の解釈やそれを具体化する立法に不備があるということを示しているのではないか．

もっとも，サイバーセキュリティ対策の重要性が今日ほどに増す以前から，一定の行政目的の実現に資するために通信の秘密を構成する情報へのアクセス等を事実上許容する立法上の措置が講じられていたことは，指摘されていた．かつて筆者は，これを「立法を通じた正当チェック行為の増加」[7]と称したが，例えば，青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律（平成20年法律79号）21条の規定や，風俗営業等の規制及び業務の適正化等に関する法律（昭和23年法律122号）31条の8第5項の規定等を通じて，「通信管理主体[8]が自らの支配・管理するネットワークの内部の流通情報をチェック（内容把握）する行為」（正当チェック行為）が立法により実質的に許容されてきた[9]．これらにかんがみると，ネットワークの環境整備上不可欠となると認められる範囲内で通信の秘密を構成する情報へのアクセス等が行われることは，通信の秘密との関係においても既にある程度正当化されてきたとも言える．それゆえ，サイバーセキュリティ対策の一環としてかかるアクセス等が行われたとしても，必ずしも当然に通信の秘密条項に抵触するものとはならないはずである．しかしながら，通信の秘密の趣旨がネットワーク上を流通する情報（以下，「流通情報」という）に不用意にアクセスしないことを含意するのであれば，なぜ前述のような「正当チェック行為」が法律上許容され得るのかということが明らかにされなければならない．

以上を踏まえ，本稿は，基本的なサイバーセキュリティ対策との関係における通信の秘密の意義を解釈論的に追究するとともに，その立法論的課題を明らかにすることを目的とする．なお，文中の意見にわたる部分はもっぱら筆者の私見であり，その所属組織の見解とは一切無関係である．

2　法律上の通信の秘密に関する従前の解釈

法律上の通信の秘密に関する規定は，いずれも憲法21条2項後段の規定を受けて定められたものとされているが[10]，複数の個別法に散在しており，その規律の内容も必ずしも一義的ではない．具体的には，電気通信事業法4条・179条，有線電気通信法（昭和28年法律96号）9条・14条，電波法（昭和25年法律131号）59条・109条・109条の2，郵便法（昭和22年法律165号）8条・80条，民間事業者による信書の送達に関する法律（平成14年法律99号．以下，「信書便法」という）5条・44条等の規定において，通信の秘密に関する規律がある．これらのうち，サイバーセキュリティ対策との関係において特に重要となると考えられるのが，電気通信事業の基幹法である電気通信事業法4条の規定である．そこで，まずは当該規定の内容に対する一般的な理解について，整理する．

電気通信事業法4条1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」と定める．ここでいう「侵す」とは，通信当事者以外の者が「積極的意思をもって知得しようとすること，さらにそれを漏洩，窃用すること」を指すものと解されている[11]．これらの中で，積極的な知得の禁止については，電波法59条の規定と大きく異なり，相対的に厳格な運用が行われている．すなわち，電波法59条では，無線通信の存在又は内容を漏えい・窃用[12]することは禁止されているものの，「電波を傍受してその存在や内容を知るだけ」[13]の行為は禁止対象となっていないのに対し[14]，電気通信事業法4条1項では，通信の秘密を知ろうとする意思の下で行われる知得行為自体が禁止対象と解されている．

これらの通信の秘密の侵害については，通信当事者の有効な同意がある場合には該当しないとされているほか，一定の違法性阻却事由がある場合にも（通信当事者の同意がなくとも）許容されるものと解されている[15]．ここでいう違法性阻却事由とは，①法令行為に該当する場合，②正当業務行為に該当する場合，③正当防衛又は緊急避難に該当する場合，であるとされる．そして，前記②の正当業務行為とは，(ア)目的の正当性，(イ)行為の必要性，(ウ)手段の相当性の各要件を充足する行為であるという．また，前記③の正当防衛とは，急迫不正の侵害を受けたときに，自己又は他人の権利を防衛するためやむを得ずした行為であり，緊急避難とは，(a)現在の危難の存在，(b)法益の権衡，(c)行為の補充性を充足する行為であるとされる[16]．

このように，電気通信事業法上の通信の秘密については，「積極的な知得，漏えい及び窃用」といった行為の類型が「侵害」に該当するものとされ，法令行為・正当業務行為や正当防衛又は緊急避難に該当する場合にはその違法性が阻却されるという刑事法上の理論的な枠組みに根ざした解釈が行われている．その背景には，通信の秘密の侵害罪が罰則として規定されているという事情（電気通信事業法179条1項参照）もある．それゆえ，例えば電気通信事業者がサイバーセキュリティ対策のために個々の通信に関する情報に積極的にアクセスし，その内容を検知することは，基本的に「侵害」に該当することとなり，正当業務行為等への該当性の検証に関するステップを別途踏むことにより，初めてその正当化の道が開かれるということになっている．

しかしながら，前述のとおり，電気通信事業法上の通信の秘密は，憲法上の通信の秘密を踏まえ，これを具体化するために定められたものとされている．そうであれば，電気通信事業法上の通信の秘密の「侵害」の可能性とその判断についても，憲法上の通信の秘密の「侵害」がどのように認定されているのかということを踏まえて行われるべきであり[17]，それを勘案しないまま，刑事法の理論的な枠組みを安易に援用することは，正鵠を射たアプローチとは言いがたい．換言すれば，憲法上の通信の秘密の「侵害」が認められる射程を勘案しつつ，電気通信事業法上の通信の秘密の「侵害」の範囲が過度に広範に及ぶものとならな

いような解釈論が求められるところであり，それに応じた当該射程の立法による具体化も必要となり得る．

3　憲法上の通信の秘密の趣旨を踏まえた法律上の通信の秘密

前節の考察を踏まえ，まず，憲法上の通信の秘密の「侵害」について考えることとする．有力な学説は，個々の通信の内容や存在等に関して，公権力及び通信業務従事者による積極的な知得や漏えい等の行為がこの「侵害」に該当するという旨を説いている[18]．もっとも，通信業務従事者を侵害の主体とする考え方には否定的な見解も提示されているが[19]，「侵害」に該当する主な行為の類型を積極的な知得や漏えい等を中心に捉える点においてはほぼ共通項を有すると言える．

そのうえで，通説は，通信の秘密不可侵は絶対的に保障されるものではないと解しており[20]，憲法 13 条の定める「公共の福祉」に基づく制約に服することを承認している．しかも，近年では，通信の秘密条項における（通信の自由を保護するための）客観法的要請として，ネットワーク上における最低限の安全性・信頼性ないしセキュリティの確保等の命題が内在しているという旨も指摘されている[21]．

これらにかんがみると，電気通信事業法上の通信の秘密についても，「公共の福祉」の確保の必要性やネットワーク上の安全性の確保等の客観法的要請を充足する観点から，公権力や電気通信事業者（通信管理主体）による一定の行為が（たとえ「積極的な知得，漏えい及び窃用」の類型に属するものであっても）許容されるという解釈論上の道筋をたどることが合理的であるように思われる．近年の判例も，電気通信の利用者においては，電気通信事業法上の「通信の秘密が保護されているという信頼の下に通信を行っており，この信頼は社会的に保護の必要性の高いもの」であるとしつつ，送信者に関する情報の秘匿に対して「客観的にみて保護に値するような利益」を有しているという旨を説いているが[22]，かかる「信頼」についても，ネットワーク上における最低限の安全性・信頼性ないしセキュリティ等の確保を前提として成り立つものであると考えられる[23]．

他方，「積極的な知得，漏えい及び窃用」といった行為の類型が「侵害」と解されてきた背景には，通信の秘密をプライバシーないし秘匿性とほぼ同視する思想があると考えられる[24]．個々の通信に関する情報の有するプライバシーや秘匿性が破られる潜在性を秘めているからこそ，これらの行為の類型が原則として禁止されるというわけである．確かに，かかるプライバシーないし秘匿性の保護は，憲法 21 条 2 項後段の規定が予定する「通信」の利用環境において，極めて重要な要素の一つであろう．しかし，憲法上制度的に確保されることが予定された「通信」の利用環境は，必ずしもそれにとどまるものではない．すなわち，憲法は，国民各人が安全に安心して支障なく通信役務を利用できるようになることを予定しており，そのためには，個々の通信におけるプライバシーの保護（及び通信手段を用いた表現の自由の保障）だけでなく，ネットワーク上のセキュリティの確保，基本的な通信役務の適切な提供等の総合的かつ多面的な要素が必要となると考えられる[25]．そして，それらのさまざまな要素が適切な通信制度の設営を通じて充足されることを前提としつつ，憲法は「通信」を明示的に規定したものと解することが合理的である[26]．

そうであれば，通信の秘密の保護とは，もっぱら個々の通信に関する情報が有するプライバシーないし秘匿性を保護するために公権力や通信管理主体による積極的な知得，漏えい及び窃用といった行為を制限するだけでなく，状況によっては，当該行為を必要と認められる範囲で実施したうえでもサイバーセキュリティ対策が適切に講じられることをも含意するものと言える．かつて筆者も主張したとおり，「いくら『秘密』が公権力により保障されても，『通信』ないしネットワークそのものがセキュリティ上の理由により破壊的な損傷を受けるなどの事態に陥れば，そもそも『秘密の保護された通信』が実現し得ず，いわば『本来

転倒』となり得る」[27]からである．換言すれば，情報が流通するネットワーク空間の安全性ないしセキュリティの確保は，各人が通信におけるプライバシー等を害されない状態を維持するための前提となる．

同時に，電気通信事業者は，私人として，経済的自由権（憲法22条1項，同29条1項参照）を享有している．それゆえ，自らが支配・管理するネットワーク自体に関して，財産権（特に，所有権）[28]を有するとともに，当該ネットワークを用いて利用者に提供する通信役務の取扱いに関して，営業の自由[29]を有することとなる．このとき，通信役務を円滑に提供する前提として，支配・管理下のネットワーク上の流通情報を一定の範囲で確認したり，基本的なセキュリティの確保を図るために必要となる措置を講じたりすることは，電気通信事業者によるネットワーク設備の管理・運用に対する経済的自由権（筆者はこれを「通信管理権」[30]と称している）の行使の一環として許容される余地が残されているはずである[31]．それにもかかわらず，かかる「通信管理権」を看過したまま，電気通信事業者による流通情報の「積極的な知得，漏えい及び窃用」といった行為の類型がただちに「侵害」に該当すると解するのは，論理的な飛躍があると言わざるを得ない．すなわち，少なくとも憲法の次元においては，「積極的な知得，漏えい及び窃用」といった行為が絶対的に禁止されるのではなく，基本的なセキュリティの確保を図る観点からの通信管理権の行使との適切なバランスの中で当該行為が制約を受けることとなるのであって，そのバランスは一次的には立法により確保されることが予定されているものと考えられる．だからこそ，憲法の明文においては，流通情報へのアクセスが原則的に禁止されているわけではなく，「侵してはならない」という規範的な判断を伴う規定となっているとも言える[32]．

したがって，憲法上，ネットワーク上の基本的なセキュリティの確保をも含意した「通信の秘密」の保護が適切に図られるための必要条件として，一定の通信制度（通信に関する法規範の集合体）が立法を通じて設営されることが予定されていると解される[33]．このような通信制度の適切な設営は，公権力に対する憲法上の要請（義務）であるとも言える．それゆえ，法律上の通信の秘密についても，単に憲法上の通信の秘密を確認するものにとどまらず，かかる要請を受けて定められたものとして捉えることが合理的である．電気通信事業法4条1項が通信の秘密の「侵害」の主体を通信管理主体としての電気通信事業者だけでなく一般私人にも拡大していること[34]は，単なる立法政策というよりも，憲法上の要請を踏まえ，国民各人が安全に安心して支障なく通信役務を利用できるようになるための通信制度の設営の「工夫」の結果にほかならない．

以上を踏まえると，電気通信事業者等が基本的なサイバーセキュリティ対策を目的として利用者の通信の秘密となる情報を最小限の範囲で検知する行為（以下，「基本的セキュリティ対策行為」という）については，正当業務行為等の要件を充足するとの観点から「違法性が阻却」されるものではなく，「公共の福祉」の確保の必要性やネットワーク上の安全性の確保等の客観法的要請の充足に資する観点に基づき実施することが求められるもの（そもそも「侵害」に該当しないもの）と位置づけられる[35]．そして，基本的セキュリティ対策行為の適切な実施の余地を制度的に設けることは，「公共の福祉」の確保の責務を負う公権力（特に立法権）に対する要請として捉えることが可能である[36]．その場合，基本的セキュリティ対策行為の具体的な範囲はどこまでかということが問題となり得るが，少なくとも，現に一定規模のサイバー攻撃等を受けた場合にネットワークや流通情報の安全性を確保するうえで不可欠となる相当な手段により講じられる最低限の措置については，当該範囲に収まり得るものと考えられる[37]．したがって，かかる範囲内において，通信の秘密を構成する情報に関する積極的な知得や窃用等の行為が行われたとしても，それは「侵害」に該当する行為ではないと捉えることが妥当であろう．

もっとも，このような解釈に対しては，従前の法律解釈論を前提に，通信の秘密を構成する情報の積極的な知得，漏えい等の行為のうち，基本的セキュリティ対策行為として法令行為や正当業務行為等に該当するものについて，（憲法上も）その実施が正当化され得ると解せば足りるのではないかという反論もあろう[38]．かかる反論の背景には，これらの正当化は憲法上の要請に基づくものではなく，あくまで立法政策によるものであるという思想が見え隠れする[39]．しかし，仮にそのように捉える場合，法律の想定する法令行為や正当業務行為等が常に十分な基本的セキュリティ対策行為を許容するという保証はなく，「通信」に関する不十分な立法又は立法不作為に「対抗」できなくなるおそれが生じ得る[40]．同時に，正当業務行為等への該当性に関する個別の判断が実質的に行政裁量に委ねられる結果，許容される基本的セキュリティ対策行為の範囲が過度に狭く解され，その結果として通信の秘密が当該行為の実施を妨げるという冒頭に提起した問題が現実のものとなる可能性もある．したがって，基本的セキュリティ対策行為の実施については，単に立法政策上かろうじて許容されているものと解するのではなく，通信制度の適切な設営の一環を占める憲法上の要請そのものであると捉えることが合理的である．

4　サイバーセキュリティ基本法及びデジタル社会形成基本法との関係

電気通信事業法が通信の秘密を構成する情報の「積極的な知得，漏えい及び窃用」を相当厳格に禁止するものと解されてきたことに象徴されるように，法律上の通信の秘密は，おおむね，通信の秘密を構成する情報への能動的なアクセスを禁止する消極的な規律として位置づけられてきた．しかも，前述のとおり，法律上の通信の秘密に関する規定は各個別法に分散しており，それらにおいては，サイバーセキュリティの確保の必要性から当該情報の検知等がどこまで許容されるかといった積極的な規律については特段示されていない．これらのことが，通信の秘密が障壁となって基本的セキュリティ対策行為の実施が妨げられていると捉えられる原因となってきたように思われる．

もっとも，我が国の立法は，サイバーセキュリティ対策を求める規律をまったく欠いているわけではなく，近年かかる規律が整備されつつある．例えば，サイバーセキュリティ基本法は，「サイバーセキュリティに関する施策を総合的かつ効果的に推進し，もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに，国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること」を目的としつつ（同法1条），「サイバーセキュリティに関する総合的な施策を策定し，及び実施する責務」を国に課している（同法4条）．そのうえで，政府に対し，サイバーセキュリティに関する施策を実施するため必要となる「法制上の措置」等の実施を義務づけている（同法11条）．

また，デジタル社会形成基本法（令和3年法律35号）も，「信頼性のある情報の自由かつ安全な流通の確保」を図ることを目的に掲げつつ（同法1条），「デジタル社会の形成に関する施策を策定し，及び実施する責務」を国に課している（同法13条）．同時に，政府に対し，デジタル社会の形成に関する施策を実施するため必要となる「法制上の措置」等の実施を義務づけている（同法17条）．そのうえで，当該施策の策定に当たり，「サイバーセキュリティ（中略）の確保，情報通信技術を用いた犯罪の防止，情報通信技術を用いた本人確認の信頼性の確保，情報の改変の防止，高度情報通信ネットワークの災害対策，個人情報の保護その他の国民が安心して高度情報通信ネットワークの利用及び情報通信技術を用いた情報の活用を行うことができるようにするために必要な措置」が講じられることを求めている（同法33条）．

このようなサイバーセキュリティ基本法及びデジタル社会形成基本法の趣旨を踏まえると，法律上の通信の秘密に関しては，「積極的な知得，漏えい及び窃用」の原則的な禁止に対する要請がサイバーセキュリティに関する施策の実施に対する

要請との関係において絶対的に優位に立つわけではなく，両者の要請の適切なバランスが確保されることが，法律上も明示的に予定されつつあるものと考えられる．その前提として，基本的セキュリティ対策行為の実施とその許容について，これが憲法上の要請として位置づけられるものと理解されているか否かはともかく，少なくともその重要性が認識され始めているという事情を指摘することができるように思われる．そうであれば，個別法で個々に当該バランスのあり方を規律するのではなく，包括的な立法において，憲法上の要請を踏まえた「法律上の通信の秘密の保護のあり方」を明確に示すことが求められよう．それゆえ，前述の「分散型」の通信の秘密に関する規定を横断的に束ねつつ，単に「秘密」となる情報の積極的知得，漏えい及び窃用を原則として禁止するにとどまらず，それらが許容され得る場合も示したうえでの，新規の横串的な「通信の秘密の具体化法」が（前述の「法制上の措置」の一環として）必要となるように思われる[41]．

それでは，かかる「通信の秘密の具体化法」はどのような内容となるべきものであろうか．この点について，次節において検討する．

5 「通信の秘密の具体化法」に向けた立法論

「通信の秘密の具体化法」においては，個々の通信に関する情報の秘匿性を保護するための措置（「積極的な知得，漏えい及び窃用」の原則的な禁止）と，ネットワーク上における最低限の安全性・信頼性ないしセキュリティの確保を図るための措置とのバランスのあり方を示すことが必要である．このような観点から，以下の各点が立法において明示されるべきであろう．

第一に，電気通信事業法４条１項や有線電気通信法９条は，「秘密」について「侵してはならない」と定めているが，「侵す」こととなる具体的な行為の類型が明示される必要がある．この点については，従前の解釈が示してきたとおり，原則として「積極的な知得，漏えい及び窃用」がその主な類型になり得ること自体に大きな異論は乏しいと思われるが，前述のとおり，電気通信事業法と電波法とで「積極的な知得」の扱いが異なっている点については議論の余地があろう．少なくとも，「電気通信事業者の取扱中に係る通信」に関しては，有線通信か無線通信かにかかわらず，電気通信事業法４条１項が優先的に適用される旨が示されている（有線電気通信法９条，電波法59条参照）ことから，当該通信において「積極的な知得」が「侵害」となり得るという点には共通了解が形成されてきたものと考えられる．

そのうえで，「公共の福祉」の確保を目的として相当な手段により必要最小限の範囲で行われる行為については，それが「積極的な知得，漏えい及び窃用」の類型に属するものであっても，「侵す」場合には該当しないという旨が示されることが求められるように思われる．すなわち，当該行為については，「侵す」行為に該当するにもかかわらずその違法性が阻却されるというのではなく，そもそも「侵す」行為に該当しないという旨が明確にされるべきである．また，流通情報を知得する意図をもってそれを部分的・断片的に垣間見る覗き見等の「積極的な知得」未満の情報へのアクセス行為についても，「積極的な知得」に準ずる前段階の行為として，「侵す」類型に該当し得ると考えられるところ[42]，かかる観点からの立法論的検討も求められよう．

第二に，既に言及したように，基本的セキュリティ対策行為が憲法上のみならず法律上も求められるのであれば，立法において，（公権力や電気通信事業者等が実施する）当該行為を許容又は義務化するための措置が必要となり得る．ところが，電気通信事業を規律する電気通信事業法は，通信の秘密との関係において，かかる措置に関する一般的な規定を設けていない[43]．この点については，有線電気通信法や電波法についても同様である．

他方，郵便法はかかる措置を（部分的に）明示している．すなわち，郵便法は「信書の秘密」や「郵便物に関して知り得た他人の秘密」を保護する一方（郵便法８条），劇物等の郵便禁制品（郵

便物として差し出すことが禁止されているもの）を限定的に規定し（同法 12 条）[44]，当該禁制品を含め郵便法等に違反して差し出された疑いのある郵便物について，差出人が中身の開示を拒否した場合における日本郵便株式会社による郵便物の強制的な開披を許容している（同法 32 条 2 項）．郵便物の強制的な開披は，通信の秘密となる情報を積極的に知得するものであるから，当該秘密の侵害に該当し得る行為であるが，これが郵便のネットワークの保護を指向した郵便禁制品等の概念を手がかりとして，大手を振って行われ得ることとなっているのである．このような規律は，憲法が求める「公共の福祉」の確保の必要性やネットワーク上の安全性の確保等の客観法的要請を充足する観点に基づき，「秘密」となる情報や内容物を積極的に探知し得る場合を具体化したものと捉え得る．

一方，電気通信事業法等は「郵便禁制品相当の情報」について包括的な定めを設けておらず[45]，例えばマルウェア等を検知するための電気通信事業者による通信の秘密を構成する情報へのアクセスも一般的・明示的には許容していない．しかし，近年のサイバー攻撃等の増大や高度化の状況にかんがみると，郵便のネットワークと同様に，電気通信のネットワークにおいても，電気通信役務の安定的かつ円滑な提供を確保する観点から，「流通禁制情報」とでも称すべき，発信されること自体が抑止されることが求められる情報の類型が認められる．その典型が，マルウェア等のネットワークに重大な物理的・機能的障害をもたらし得ると認められる情報又はコード（以下，「ネットワーク加害情報」という）であると考えられる．それゆえ，電気通信事業法においても，憲法上の通信の秘密の保護を具体化する観点から，電気通信の利用者において発信することが禁止されるネットワーク加害情報を具体的に特定することが必要であると考えられる．同時に，ネットワーク加害情報の発信源の特定やその流通経路からの排除等を目的とするものである場合には，通信の秘密を構成する情報の電気通信事業者による必要最小限度の探知については，電気通信事業法上の通信の秘密の保護の必要性や，不正アクセス行為の禁止等に関する法律（平成 11 年法律 128 号）3 条に基づく不正アクセス行為の禁止等にかかわらず，基本的セキュリティ対策行為として正当に行われ得るという旨も明示されることが求められよう．当該探知については，その違法性が阻却されるものではなく，そもそも「侵害」に該当しない行為として位置づけられるべきである．

第三に，第二の点に関連して，電気通信の利用者に対する透明性を確保する観点から，（実施することが許容される）基本的セキュリティ対策行為の内容が立法上具体化されることが望ましいと考えられる．現在，総務省の「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」の「第三次とりまとめ」において，「マルウェアに感染し得る脆弱性を有する端末の利用者に対する注意喚起」等が，また同研究会の「第四次とりまとめ」において，「ISP が，自らのネットワーク内のルータ等の電気通信設備を通過するユーザの通信トラフィックに係るデータのうち，フロー情報を収集・蓄積し，そのフロー情報を分析して，未知の C&C サーバの検知を行うこと」が，それぞれ一定の条件の下に許容される旨が示されているところ[46]，このような具体的な行為の類型が法律の次元で規定される必要があろう．

第四に，通信の秘密の侵害となり得る行為が通信当事者の同意により許容され得る場合における当該同意のあり方が具体的に示される必要があると考えられる．この点に関しては，現在，総務省の「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 29 年総務省告示 152 号）及び「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 29 年総務省告示第 152 号．最終改正平成 29 年総務省告示第 297 号）の解説」において，個人情報の保護の文脈における具体的な同意の取得のあり方が定められるとともに，その詳細について，「同意取得の在り方に関する参照文書」が策定・公表されている[47]．そこでは，通信の秘密を構成する情報の取得に関して，「通信当

事者の個別具体的かつ明確な同意」が必要であるとされている[48]．また，総務省によれば，「有効な同意があるとは，原則として，通信の秘密を侵すことに対する認識，認容がある場合」を指すものとされ，「通常は契約約款等に基づいた事前の包括同意のみしかない場合を含まない」という[49]．このような詳細事項のうち基幹的な部分については，規律の透明性や当事者の予見可能性を確保する観点も踏まえ，法令のレベルでの規定が求められるように思われる．

6　結　　論

法律上の通信の秘密に関する規定は，「秘密」の概念がプライバシーないし秘匿性とほぼ同視されがちであったことを背景として，流通情報の「積極的な知得，漏えい及び窃用」といった行為を原則として禁止する規律と捉えられてきた．そのため，当該行為は基本的に通信の秘密の「侵害」に該当するものとされ，その行為を正当化するためには，法令行為や正当業務行為等の「違法性阻却事由」が必要となると解されてきた．しかし，法律上の通信の秘密に関する規定が憲法上の通信の秘密を受けて定められたことにかんがみれば，憲法上の通信の秘密の保護法益を精緻に問うことなくして，当該規定の解釈論は成り立ち得ないはずである．

憲法上の通信の秘密については，かつては通信におけるプライバシーや表現の自由を保障するものと解する考え方が通説的であったが，今日ではそれらに加え，ネットワークそれ自体や通信役務の提供に関する最低限の安全性ないしセキュリティの確保等の客観法的要請を伴うものと捉える考え方が有力になりつつある．しかも，憲法上の通信の秘密が「公共の福祉」の確保の必要性から制約されるということは，かねてより通説となっており，当該必要性は前述の「違法性阻却事由」とは異なる枠組みの下で捉えられてきたところである．

このような通信の秘密の構造にかんがみれば，相当な手段を用いて行われる基本的セキュリティ対策行為についても，憲法上の通信の秘密条項が内包する客観法的要請に基づき，それが適切に実施される限り，各人の「通信の自由」を確保するうえで求められる行為であると捉えることが合理的である．すなわち，かかる基本的セキュリティ対策行為は，通信の秘密の「侵害」に該当するけれども違法性が阻却されるというわけではなく，そもそも「侵害」に該当しない行為であって，むしろ憲法上適切な実施が要請され得る行為であると言える．それゆえ，通信の秘密に関する規定がサイバーセキュリティ対策の実施を妨げているとする冒頭で言及した所論は，不適切な解釈論に基づいているものと言わざるを得ない．

しかし，かかる解釈論が浸透しがちであることにも一定の理由がある．それは，憲法上の通信の秘密を受けてそれを具体化するはずの法律上の通信の秘密に関する規定が，諸法に散在していて総合的・統一的に定められていないだけでなく，基本的セキュリティ対策行為が許容される具体的な範囲等についてはほぼ「沈黙」しているということである．そのため，流通情報の「積極的な知得，漏えい及び窃用」の原則的な禁止という一側面ばかりに光が当たり，当該禁止と基本的セキュリティ対策行為の許容とのバランスをどのように確保するのかといった重要な論点に対し，立法が明確な手がかりを与えていないこととなっている．

もっとも，近年においては，サイバーセキュリティ基本法やデジタル社会形成基本法の制定を中心に，サイバーセキュリティ対策の重要性に焦点を当てた規律の芽も出始めているが，それらと通信の秘密に関する規定との相互関係については，議論が不十分となっているように見受けられる．また，伝統的な郵便法には「郵便禁制品」の概念が定められており，それを含む郵便物は強制的な開披等の対象となり得るのに対し，電気通信の領域の基幹法となる電気通信事業法にはネットワーク加害情報を特定した「流通禁制情報」のような概念は特段規定されていない．

このような状況を改善するうえで，立法論上「通信の秘密に関する具体化法」が必要となるように

思われる．特に，サイバーセキュリティ対策の必要性も見据えた「流通禁制情報」に関する規律や許容される基本的セキュリティ対策行為の内容の明確化を含め，前述のバランスの確保のあり方とそのために必要となる具体的な規律が法律の次元で包括的に定められることが求められよう．

注

1）サイバーセキュリティの定義について，サイバーセキュリティ基本法（平成 26 年法律 104 号）2 条参照．

2）「サイバーセキュリティ戦略」（令和 3 年 9 月 27 日：閣議決定）10 頁参照．

3）（The International Institute for Strategic Studies 2021: 82）

4）例えば，井上宗典「対サイバー攻撃 国際連携カギ」（2021 年 7 月 28 日読売新聞 13 頁）．

5）その趣旨について，（海野 2018: 29–32）参照．

6）（佐藤 2020: 356），（芦部 2000: 541），（阪本 1995: 141）参照．

7）（海野 2015: 33）．

8）その意義について，（海野 2018: 7）参照．

9）かかる立法の具体例について，（海野 2015: 30–31）参照．

10）（電気通信事業法研究会編 2019: 35），（郵便法令研究会編 1982: 43）参照．

11）（高嶋 2015: 777）参照．併せて，（電気通信事業法研究会編 2019: 36），（総務省 2014: 15–16）参照．

12）窃用とは，正当な理由なく発信者又は着信者の意思に反して利用することを指すものと解されている．平成 16 年 4 月 13 日第 159 回国会衆議院総務委員会議事録第 13 号 17 頁（有冨寛一郎政府参考人発言）参照．

13）傍受とは，積極的な意思をもって，自己に宛てられていない無線通信を受信することを指すものと理解されている．（園部・植村 1984: 286），（今泉 2020: 292）．

14）（高嶋 2015: 779）参照．傍受のみでは電波法 59 条違反にはならないという解釈は，同法 109 条 1 項から裏づけられるものと解されている．

15）（電気通信事業法研究会編 2019: 37）参照．

16）（総務省 2014: 16–17），（総務省 2018: 10–11），（総務省 2021b: 8）参照．

17）憲法学説においても，電気通信事業法 4 条等の解釈・適用に当たっては，「憲法 21 条の趣旨を十分に考慮すべきである」と指摘されている．（長谷部 2018: 234）参照．

18）（芦部 2000: 545），（佐藤 2020: 356）参照．

19）（曽我部 2013: 20）参照．この点について，筆者は，憲法上の通信の秘密の「侵害」の主体は，公権力のほか，一定の通信設備を用いて他人間の通信に関与する通信管理主体（その大半は私人）も含まれると解している．その理由について，（海野 2018: 11–12）参照．ただし，具体的に「侵害」に該当する行為の内容に関して，公権力と通信管理主体との間には規範的な差異があり，通信管理主体の中で情報の伝送・交換を直接行う「伝送系通信管理主体」とそれ以外の「非伝送系通信管理主体」との間にも一定の懸隔があると考えられる．その詳細について，（海野 2018: 39–44）参照．

20）（芦部 2000: 546），（佐藤 2020: 357），（高橋 2020: 269）参照．

21）（海野 2018: 31）参照．

22）最決令和 3 年 3 月 18 日民集 75 巻 3 号 822 頁参照．

23）そもそも通信の秘密は，通信当事者としての国民各人が通信の利用に際して公権力や通信管理主体に対して有する一定の「信頼」に基づいて発現するものと考えられる．通信の秘密の侵害についても，基本的にかかる「信頼」に背反すると認められる行為の実施により成立するものと言えよう．この点の詳細について，（海野 2015: 130–133）参照．このとき，ネットワーク上における最低限の安全性・信頼性ないしセキュリティが維持されることは，当該「信頼」が確保されるうえでの必要条件となろう．

24）通信の秘密をプライバシーの核心部分の一つと捉える学説として，（長谷部 2018: 234）参照．

25）（海野 2015: 41），（海野 2018: 4）参照．

26）（海野 2015: 44–49），（海野 2018: 29–32）参照．

27）（海野 2015: 41）．

28）財産権は法律により内容形成される権利ではあるが（憲法 29 条 2 項参照），その核心部分において，各人が所有する「物的手段の使用・収益・処分に対する権利」を保障するものと解される．その詳細について，（海野 2010b: 163–173），（海野 2015: 339–343）参照．

29）営業の自由の意義とそれに関する管見について，（海野 2010b: 192–206）参照．

30）（海野 2015: 18, 347–348），（海野 2018: 8）参照．

31）しかし，学説上，この「通信管理権」については，ほとんど議論されるに至っていない．電気通信事

業者が自らの通信設備とその運営に対して経済的自由権を有しないとするのであれば格別，当該自由権を（他の私人の場合と同様に）肯定する限り，「積極的な知得，漏えい及び窃用」といった行為を憲法の次元で正当化する可能性を秘めた「通信管理権」が認められる具体的な射程について，解釈論的に究明することが求められると言えよう．この点に関する管見について，（海野 2015: 343–367）参照．

32）「侵す」行為は，ある行為の類型に該当すればただちに認められるというものではなく，一定の規範的な評価（原初的な状態からのマイナス方向への変化の発生）を伴って認定されるものであると考えられる．この点について，（海野 2015: 294–297）参照．それゆえ，当該評価において，憲法上の複数の保護法益のバランスに配意することが必要となる．また，「侵してはならない」ことを公権力が確保するためには，一定の作為（制度的措置）が必要となる．（海野 2021: 194）参照．

33）（高橋 2020: 268），（海野 2015: 47），（海野 2018: 32）参照．

34）電気通信事業法 4 条 1 項は，同条 2 項との対比において，「侵してはならない」という禁止規範が及ぶ主体の対象に一般私人を含めていると解される．また，電気通信事業法 179 条 1 項は，同条 2 項との対比において，「電気通信事業者の取扱中に係る通信の秘密を侵した者」に一般私人を含めていると解される．併せて，（電気通信事業法研究会編 2019: 36）参照．

35）筆者は 2010 年に公表した論文において，「国が，通信業務従事者を通じて，通信システムの保護を目的としつつ IP アドレスから送信者を特定し，場合によっては当該送信者に対して送受信を停止する等の措置」を例示しつつ，かかる行為が通信制度の安定的運営の確保のために不可欠と認められる範囲で行われることは，「一般には通信の秘密侵害に該当するものの正当行為として違法性ないし違憲性が阻却されるものと理解されているが，管見は，そもそも通信の秘密不可侵に内在する通信制度の安定的運営という価値秩序を保護するために必要なものであって，秘密侵害に該当しない（違法性が阻却されるのではなく，もとより違法ではない）と解する」と説き，このような点を主張し続けている．（海野 2010a: 30–31）参照．併せて，（海野 2015: 32–33）参照．

36）ただし，ここでいう基本的セキュリティ対策行為は，通信（ネットワーク）の安全性等を確保するために不可欠となると認められる基幹的なセキュリティ対策を指すのであって，例えばサイバー攻撃の実施者に対してサイバー攻撃をもって「反撃」し，そのシステムを停止させるなどの攻撃的な手法を採ることの許容までをも求めるものではない．なお，かかる攻撃的な手法については，その実施者の帰属先次第では「武力攻撃」に該当する可能性もあり，国家の自衛権の問題ともなり得るため（国際連合憲章［昭和 31 年条約 26 号］51 条参照），当該手法の可否を判断するに当たり，自衛権の射程に関する解釈論が別途必要となり得る．

37）昨今では，IoT（Internet of Things）のセキュリティ対策の一環としての「サイバー攻撃に対する電気通信事業者の積極的な対策の実現」が必要であり，「電気通信事業者が自らトラフィックの流れ（フロー情報）を把握・分析して攻撃元の C&C サーバ（マルウェアに感染した端末に対して指令を与えるサーバ）を検知し，検知した C&C サーバに関する情報を電気通信事業者間で共有し，サイバー攻撃の予兆を捉えて早期に対処できるようにする」ことが求められると指摘されている（（総務省 2021a: 13–15）参照）．「端末機器側の対応だけでは，端末の踏み台への悪用に適切に対応することが難しくなっていく」中で，「トラフィックが通過するネットワーク側でより機動的な対処を行う環境整備が必要」となっている現状（（総務省 2021a: 11, 14）参照）に照らせば，このような措置は基本的セキュリティ対策行為の射程に入り得るものと考えられる．

38）（宍戸 2013: 522）参照．

39）（曽我部 2013: 19）参照．

40）（海野 2015: 58–59），（海野 2018: 27）参照．

41）筆者は 2012 年に公表した論文において，「立法論としては，秘密の侵害に該当する場合とそれ以外の場合との区別を規範的に方向づける基本原理を示しつつ，通信の秘密及びそれを包含する憲法適合的な通信制度の設営を保障（制度的保障）するための基本法が必要となる」と説いたが，かかる基本原理はいまだ立法化されるに至っていない．（海野 2012: 10）参照．

42）（海野 2015: 306）参照．

43）もっとも，電気通信事業法 116 条の 2 の規定は，電気通信事業者がいわゆる DDoS 攻撃等の「送信型対電気通信設備サイバー攻撃」への対処を共同して行うための認定送信型対電気通信設備サイバ

ー攻撃対処協会について定めている．

44）郵便禁制品の設定には，①郵便の業務を支障なく行うための自衛的な必要性，②社会の秩序を維持するための公共的な必要性，の双方の意味合いがあるとされる．（郵便法令研究会編 1982: 67）参照．なお，信書便法 48 条の規定も，信書便物に関して郵便禁制品相当のものを差し出す行為について罰則の対象とするとともに，それが差し出された場合における没収について定めている．

45）ただし，有線電気通信法 13 条 1 項は，「有線電気通信設備の機能に障害を与えて有線電気通信を妨害した者」に対する罰則を設けており，電波法 108 条の 2 第 1 項は，「無線設備の機能に障害を与えて無線通信を妨害した者」に対する罰則を設けている．また，電気通信事業法 180 条 1 項は，「みだりに電気通信事業者の事業用電気通信設備を操作して電気通信役務の提供を妨害した者」に対する罰則を設けている．

46）（総務省 2018: 23–25），（総務省 2021b: 9–12）参照．

47）総務省報道資料（令和 3 年 2 月 25 日）参照：https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000111.html（2022 年 1 月 3 日最終閲覧）．

48）（総務省 2017: 31）参照．

49）（総務省 2018: 10）参照．

【参考文献】

［邦文文献］

芦部信喜（2000）『憲法学Ⅲ 人権各論（1）〔増補版〕』有斐閣．

今泉至明（2020）『電波法要説 改訂第 11 版』情報通信振興会．

海野敦史（2010a）「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』14（2）：17–35．

海野敦史（2010b）「財産権及び営業の自由の『多層的構造』」『経営と経済』90（1/2）：153–256．

海野敦史（2012）「憲法上の通信の秘密に対する『侵害』の射程」『公益事業研究』64（1）：1–13．

海野敦史（2015）『「通信の秘密不可侵」の法理―ネットワーク社会における法解釈と実践』勁草書房．

海野敦史（2018）『通信の自由と通信の秘密―ネットワーク社会における再構成』尚学社．

海野敦史（2021）『情報収集解析社会と基本権』尚学社．

阪本昌成（1995）『憲法理論Ⅲ』成文堂．

佐藤幸治（2020）『日本国憲法論［第 2 版］』成文堂．

宍戸常寿（2013）「通信の秘密に関する覚書」長谷部恭男・安西文雄・宍戸常寿・林知更編『高橋和之先生古稀記念 現代立憲主義の諸相 下』有斐閣，pp.487–523．

総務省（2014）「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第一次とりまとめ」（平成 26 年 4 月）．

総務省（2017）「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 29 年総務省告示第 152 号．最終改正平成 29 年総務省告示第 297 号）の解説」（平成 29 年 9 月〔令和 3 年 2 月更新〕）．

総務省（2018）「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第三次とりまとめ」（平成 30 年 9 月）．

総務省［サイバーセキュリティタスクフォース］（2021a）「ICT サイバーセキュリティ総合対策 2021」（令和 3 年 7 月）．

総務省（2021b）「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第四次とりまとめ」（令和 3 年 11 月）．

曽我部真裕（2013）「通信の秘密の憲法解釈論」『Nextcom』16: 14–23．

園部敏・植村栄治（1984）『法律学全集 15–Ⅰ　交通法・通信法〔新版〕』有斐閣．

高嶋幹夫（2015）『実務 電気通信事業法』NTT 出版．

高橋和之（2020）『立憲主義と日本国憲法 第 5 版』有斐閣．

電気通信事業法研究会編（2019）『電気通信事業法逐条解説 改訂版』情報通信振興会．

長谷部恭男（2018）『憲法 第 7 版』新世社．

郵便法令研究会編（1982）『郵便法概説』通信事業教育振興会．

［英文文献］

The International Institute for Strategic Studies（2021 ）. *Cyber Capabilities and National Power: A Net Assessment,* https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power（2022 年 1 月 3 日最終閲覧）．