

[投稿: 研究論文]

# ネットワーク空間上における ブロッキングの憲法適合性

## The Constitutionality of Blocking Access to a Website in Cyberspace

海野 敦史

慶應義塾大学環境情報学部教授

Atsushi Umino

Professor, Faculty of Environment and Information Studies, Keio University

Correspondence to: yachagny@sfc.keio.ac.jp

**Abstract:** ネットワーク空間上で行われる情報へのアクセスの遮断措置としてのブロッキングは、その実施の態様次第では、憲法適合的に行われ得る。その主な理由として、第一に、対象ウェブサイト等へのアクセスが制限される以上、表現の自由に対する一定の制約となるも、表現者自身の表現物表出の自由が直接妨げられるわけではないという点が挙げられる。第二に、憲法 21 条 2 項後段が「通信」の健全な制度的利用環境の確保を予定していると解される中で、通信の秘密たる情報を「窃用」することになるとしても、ネットワーク空間上での法秩序の維持という「公共の福祉」の確保を目的として実施される限り、通信の秘密の侵害とは認められないという点である。

Blocking as a measure to block the access to information in cyberspace can be constitutional depending on how it is implemented. The main reasons for this are as follows. First, while it places certain restrictions on freedom of expression since it limits access to the target website, it does not directly impede the freedom of expression of the expresser themselves. Second, given that the second part of Article 21, Paragraph 2 of the Constitution of Japan provides for the maintenance of a sound institutional environment for the use of communications, even if it results in the “stealing” of confidential information in communications, it does not constitute a violation of the secrecy of communications as long as it is implemented for the purpose of ensuring the “public welfare,” which includes maintaining law and order in cyberspace.

**Keywords:** 憲法、ブロッキング、通信の秘密、表現の自由、通信の自由、検閲禁止の法理、通信制度

Constitution of Japan, blocking, secrecy of communications, freedom of expression, freedom of communications, prohibition of censorship, communications system

### 1. 序論

情報通信の領域では、しばしばネットワーク空間<sup>1)</sup>における「ブロッキング」の合憲性が問題となる。ここでいうブロッキングとは、利用者がウェブサイト等を閲覧しようとする場合に、インターネット経由のアクセスを提供するインターネット接続役務提供者等が、当該利用者の同意を得ることなくアクセス対象のウェブサイト等のホスト名や IP アドレスないし URL を検知し、そのアクセス (通信) を一方的に遮断する措置のことを指す。すなわち、他人の権利・利益を害する情報その他の違法なコンテンツに利用者がインターネット経由でアクセスしようとする場合に、

SNS 等を管理するプラットフォーム事業者による送信防止措置 (SNS からの情報の削除等)<sup>2)</sup>とは別に、情報の伝送ないし媒介<sup>3)</sup>に直接携わるインターネット接続役務提供者等が個々の通信の宛先を検知して物理的に特定のウェブサイト等へのアクセスを実現させないようにするための措置である。

このブロッキングについては、日本国憲法 (以下、「憲法」という) 21 条 1 項が規定する「表現の自由」や同条 2 項前段の「検閲の禁止」 (検閲禁止の法理) との関係で議論されることがあるほか、同項後段の「通信の秘密不可侵」の規範との関係がしばしば問題となる<sup>4)</sup>。もっとも、実務上、

児童ポルノサイトへのアクセスに対してブロッキングが行われる場合には、法律の次元で正当化されるものとかねてより解されてきた<sup>5)</sup>。一方、政府における検討において、いわゆる海賊版サイト<sup>6)</sup>へのアクセスに対してブロッキングが行われようとしたときには<sup>7)</sup>、当該ブロッキングの憲法適合性、特に通信の秘密の侵害の可能性をめぐって関係者の見解が割れ、その実施が見送られたという経緯がある<sup>8)</sup>。また、近年では、我が国で賭け事として利用される場合には違法となるオンラインカジノサイトへのアクセス(刑法〔明治40年法律45号〕185条参照)をめぐっても議論の俎上にあがり、政府が当該アクセスに対するブロッキングの合憲性を改めて検討する必要性に迫られている<sup>9)</sup>。その中では、「実施には慎重な検討が求められる」とされつつ、「ブロッキングが単に有効な対策であるだけでは足りず、他のより権利制限的ではない有効な対策が尽くされたかどうかを検証することが必要」と指摘されている<sup>10)</sup>。

このようなブロッキングの実施の可否をめぐる議論がたびたび行われる背景には、とりわけ通信の秘密不可侵の保護法益の核心が何かということに対する共通理解が十分に得られていないという問題があるように思われる。ブロッキングの実施に当たり特に問題となるのが、通信の秘密が侵害される可能性であることから、通信の秘密不可侵の規範があたかもブロッキング実施の「壁」になっているかのように捉えられることさえある。

もっとも、この規範に関しては、憲法のみならず法律によっても規律されているため<sup>11)</sup>、「憲法上の通信の秘密」との関係に加え、「法律上の通信の秘密」との関係が問題となる。後者は前者を受けてそれを具体化したものという考え方<sup>12)</sup>や、後者の保障の趣旨及び保護範囲は前者のそれに等しいという考え方<sup>13)</sup>も提示されているが、「法律上の通信の秘密」はその侵害の主体の射程を一般私人にまで拡大していると解されることから<sup>14)</sup>、一般私人に対する規律ではない「憲法上の通信の秘密」の単なる具体化にとどまらない要素が内包されているとも言える。しかも、「憲法上の通信の秘密」については、その論理的な前提として「通信の自由」を保護していると解されており<sup>15)</sup>、一定の(憲法適合的な)通信制度の保障という趣旨を含むと解する学説が有力になっているため<sup>16)</sup>、「法律上の通信の秘密」とは異質な保護法益を含んでいる。それゆえ、「法律上の通信の秘密」の侵害に該当しないことが、「憲法上の通信の秘密」の侵害に該当しないということを証するものとは必ずしもならないはずである。一方、「法律上の通信の秘密」の侵害については、罰則をもって禁止されていることから<sup>17)</sup>、刑事法上の正当行為(刑法35条)や緊急避難(刑法37条)等の枠組みに沿った「違法性阻却事由」が妥当し得

るものと解されている<sup>18)</sup>。しかし、法律上の「違法性阻却事由」がそのまま憲法上の「違憲性阻却事由」となるとは限らないことから、刑事法上の枠組みをただちに「憲法上の通信の秘密」の侵害の正当化事由と解し得るわけではない<sup>19)</sup>。

以上を踏まえ、本稿は、ブロッキングの憲法適合性について法的考察を加えることを目的とする。その際、議論の無用の混乱を避ける観点から、原則として憲法上の権利としての基本権の保障との関係に着目することとし、通信の秘密に関しては、「憲法上の通信の秘密」との関係を中心に考察する。また、ブロッキングの対象に関しても、これまで実務上の議論の焦点となってきた海賊版サイトやオンラインカジノサイト等(以下、「海賊版サイト等」という)へのアクセスを主に念頭におくこととする。ただし、ブロッキングをめぐるのは、「法律上の通信の秘密」との関係において議論が蓄積されている要素も少なくないため、必要に応じて当該議論にも言及し、またそれを参照することとしたい。

## 2. ブロッキングをめぐる近年の主要学説の概要とその検討

### 2.1 違憲可能性説の概要

近年の主要学説は、海賊版サイトに対するブロッキングを念頭にその憲法適合性を論じるものが多かったが、その論旨の骨格はオンラインカジノサイト等に対するブロッキングにも妥当し得るところが大きいため、それらの要点について包括的に概観する。これらのウェブサイトに対するブロッキングについて、その行為の態様としては違憲になり得るという旨を示す考え方(以下、「違憲可能性説」という)<sup>20)</sup>は、主に以下の各点を指摘する。その主張の基軸は、ブロッキングが(憲法上又は法律上の)通信の秘密の侵害に該当し得るという点にあるが、表現の自由との関係についても問題視されている。

第一に、通信の秘密の侵害は、個々の通信に関する情報の積極的な知得、漏えい又は窃用(通信当事者の意思に反して自己又は他人の利益のために利用すること)により生じるという前提の下、ブロッキングは、問題となるウェブサイトへアクセスしようとししない利用者の場合、インターネット接続役務提供者等があらゆる利用者の通信の宛先を実質的に監視することにより実施されるため<sup>21)</sup>、その情報の積極的な知得及び当該宛先へのアクセスを遮断するための窃用に当たり、通信の秘密の侵害に該当し得るとされる<sup>22)</sup>。同時に、ブロッキングに伴う利用者の通信の宛先の監視は、そのプライバシーにとって深刻な脅威となるという<sup>23)</sup>。これらに対し、学説上は、個々の通信の宛先をインターネット接続役務提供者が積極的に知得・利用する

ことは、少なくとも通信の内容に関わらない部分(パケットデータ部分)である限り、正当行為として通信の秘密の侵害に該当しないという反論も提示されている<sup>24)</sup>。また、「憲法上の通信の秘密」の侵害に関する行為類型としては、「秘密」たる情報の積極的知得や漏えいが該当すると解されてきた中で、そもそも「窃用」が想定されていない可能性があるため<sup>25)</sup>、仮にブロッキングが窃用に該当したとしても「憲法上の通信の秘密」の侵害には当たらないと解する余地が残されているという旨を示唆する学説もある<sup>26)</sup>。

第二に、「法律上の通信の秘密」の侵害の違法性については、刑事法上の緊急避難として阻却される余地もあると解されているところ<sup>27)</sup>、その成立要件である①現在の危難の存在、②やむを得ずにした行為であるという意味での補充性、③法益の権衡、のそれぞれの充足の有無が問題となるとされる。実務上正当化されている児童ポルノサイトに対するブロッキングに関しては、当該サイトがインターネット上で閲覧され得る状態におかれた段階で、関係する児童の心身の健全な発展に重大な悪影響が生じるおそれがあり、自己の意思に反して性的欲求の対象とされることに伴う人格的利益の侵害が生じ得るということに照らし、「現在の危難」等が認められると解する余地がある<sup>28)</sup>。そのため、法律の次元においては、児童ポルノサイトのブロッキングの違法性が緊急避難として阻却されるものと捉える余地があるが<sup>29)</sup>、違憲可能性説の立場からは、少なくとも海賊版サイトのブロッキングに関しては「現在の危難」を認めがたいうえに、著作権者等が講じた対策の実効性も明らかでないため補充性も認めがたく、「法益の権衡」を充足するとも言えないという旨が説かれている<sup>30)</sup>。特に、児童ポルノサイトのブロッキングでは被害の回復困難性を有する人格権の侵害等との権衡が問われるのに対し、海賊版サイトのブロッキングでは財産権としての著作権等の侵害との権衡が問われる中で、それらを同列に論じることは困難であるとされる<sup>31)</sup>。同時に、海賊版サイトであるか否かが一見して明らかではない場合など、対象外のウェブサイトまで誤って遮断してしまう「オーバーストッキング」のおそれが高いことにかんがみても、補充性を認めることは困難であるという<sup>32)</sup>。このような論理からすれば、児童ポルノサイト以外のブロッキングについては、緊急避難による正当化は困難であるということになろう。その場合、違法性は阻却されずに「法律上の通信の秘密」の侵害が認められ得ることになるが、そうであれば(当該秘密と共通の保護法益を有する)「憲法上の通信の秘密」の侵害も認められるという論理展開になりがちである。

もっとも、違法なウェブサイト又は違法行為を助長すると認められるウェブサイトに対するブロッキングをイン

ターネット接続役務提供者等に義務づける立法(以下、「ブロッキング義務づけ立法」という)が適切に行われれば、それに基づくブロッキングは、法令に基づく正当行為として違法性が阻却される可能性もある。しかし、ブロッキング義務づけ立法の目的の重要性及びその手段の必要性・合理性が立法事実に基づき精査されることとなる中で、「各種ブロッキングは違憲になることが多い」とされる<sup>33)</sup>。

第三に、公権力が特定の種類のウェブサイトを指定してインターネット接続役務提供者等にブロッキングをさせることは、公権力が私人に検閲的行為を代行させる「代理人による検閲」となり、「事前抑制の原則的禁止の法理」<sup>34)</sup>を内包する表現の自由の保障との関係でも問題となるとされる<sup>35)</sup>。とりわけ、海賊版サイトのブロッキングについては、著作権の侵害以外にも、名誉毀損をはじめとする広範な類型の表現に対して「事前抑制的手法」であるブロッキングが行われることに道を開く可能性があるため、各種のウェブサイトを用いた表現者にとっての重大な懸念材料となるという<sup>36)</sup>。

## 2.2 違憲可能性説の検討

まず、第一の点(通信の秘密たる情報の窃用の可能性)についてであるが、ブロッキングは利用者の通信の宛先を検知し、それを当該利用者の意思に反して利用するという点において、通信の秘密たる情報の「窃用」に該当し得る。これは、例えば青少年に有害な情報へのアクセスを防ぐためのフィルタリングが、当該青少年の保護者の意思に基づき正当に行われることとの大きな相違点である<sup>37)</sup>。

もっとも、ブロッキングという行為については、「憲法上の通信」の提供に関する公権力の責務の観点から再定位することも可能である。ここでまず問題となるのが、「憲法上の通信」とはどのような通信を指すかということである。もとより、コミュニケーションにはさまざまな態様がある中で、「憲法上の通信」とは、通信当事者による直接的な支配・管理の及ばない一定の通信設備(ネットワーク)を用いて通信事業者等の第三者の助力を得て行われる行為として位置づけられる。なぜなら、対面での口頭会話、伝書鳩、糸電話等による情報のやり取りのように、通信設備を特段用いずに通信当事者の独力で完結するコミュニケーションについては、当該情報を保護するうえでは、通信当事者自身がその秘匿性等に配慮した取扱いを行えば足り、公権力との関係においても、もっぱら当該情報の取扱いに関するプライバシーの問題として捉え得る(あえて「通信の秘密」を觀念する必要のないし実益が乏しい)からである<sup>38)</sup>。それゆえ、「憲法上の通信」は、実定法に基づく制度的措置を欠いた「自然状態」では成立し得ず、一定の通

信制度の設営を不可欠とし、それを前提に行われ得るコミュニケーションであると解される。したがって、憲法21条2項後段の規定は、憲法適合的な「通信」の制度的利用環境の構築(通信制度の設営)を公権力に要請していると解される。

この要請の一環として、「基本的な通信役務」の適切な提供を制度的に確保する責務、さらには当該責務に基づきインターネット接続役務提供者等の通信管理主体(発信者及び着信者以外の第三者的な立場から通信の秘密たる情報の取次に直接関わる者)<sup>39)</sup>が「基本的な通信役務」を提供しなければならないという命題が導かれ得る<sup>40)</sup>。ここでいう「基本的な通信役務」にさまざまなインターネット接続役務が軒並み該当するの否かについては議論の余地があるとしても、少なくとも各人の生活拠点等で用いられる固定系のインターネット接続に関しては、これに該当し得ると言えよう<sup>41)</sup>。それゆえ、インターネット接続役務提供者によるブロッキングについては、本来予定された通信役務の提供が適切に行われなければならないことに直結するため、(窃用ではなく)前述の責務の不履行ないし憲法上の要請に反した行為として構成する余地も残されている。

そのうえで問題となるのは、仮にブロッキングが窃用等に該当するとしても、それがただちに通信の秘密の侵害となるのかということである。違憲可能性説においては、ブロッキングないし窃用が憲法13条の予定する「公共の福祉」の確保の必要性<sup>42)</sup>に基づく正当な制約と認められる余地について、十分な検討が行われていないように思われる。違法行為を促す蓋然性の高いと認められるウェブサイトへのアクセスを遮断することは、一般的な法秩序の確保に加え、各人が安心してインターネット経由の通信を利用できるようになるという意味での「通信」の健全な制度的利用環境の構築に資する行為であり、また基本権としての「通信の自由」を確保するための土台となり得るものとも言えることから<sup>43)</sup>、「公共の福祉」を根拠とする制約の正当性が肯定される余地が大きいと考えられる。このように解すれば、ブロッキングが憲法上の要請としての「基本的な通信役務」の適切な提供に関する責務に違反するとも断じ得ないであろう。

次に、第二の点(法律上の緊急避難との関係)についてであるが、そもそも緊急避難への該当性は、「法律上の通信の秘密」の侵害に関する違法性を阻却するとしても、必ずしも「憲法上の通信の秘密」の侵害に関する違憲性を阻却するものではないと考えられる。憲法上、当該侵害とされる行為が正当な制約となり得るか否かについては、「公共の福祉」の確保の必要性に基づき決せられるべきであって、ここに法律の次元での議論を持ち出すこと自体が十分

な合理性を欠く。仮に「法律上の通信の秘密」との関係に絞って考えるとしても、少なくとも海賊版サイト等に対するブロッキングについては、緊急避難として構成することが困難であると考えられる。なぜなら、恒常的に行われ得る当該アクセスの可能性について、それがもたらし得る効果(アクセスした者における著作権法違反や賭博罪の成立等の可能性)に照らしても、「現在の危険」をただちに認めることが困難であるからである。よって、もっぱら緊急避難との関係に照らす限りにおいては、当該ブロッキングは通信の秘密に対する制約として正当化され得るものではない。これに対し、一定のブロッキング義務づけ立法が適切に行われ、それに基づく必要最小限度のブロッキングが行われる場合には、「法律上の通信の秘密」の侵害に関する違法性を阻却するだけでなく、「憲法上の通信の秘密」との関係においても「公共の福祉」の確保の必要性に基づく正当な制約と捉えられる可能性がある。この点については、後述することとしたい。

他方、第三の点(表現の自由との関係)については、仮にもっぱら行政権の判断に基づきブロッキングが恣意的・無作為的に行われるようであれば、本来はブロッキングの対象とされる必要のない正当な表現も含め、表現の自由に対する過度な萎縮効果をもたらし得るため、違憲の可能性が生じ得るであろう。このような表現者に対して事実上発生し得る萎縮効果については、それ自体を表現の自由に対する制約と捉え、その憲法適合性の論証を求めることが合理的であるという旨を説く学説も有力である<sup>44)</sup>。しかし、ブロッキング義務づけ立法において、ブロッキングの対象が開設自体違法となる一定のウェブサイト又は違法行為を助長すると認められるウェブサイトに限定されたうえで、ブロッキングが実施される条件及び手法が具体的に明確化されるなどの制度整備が行われ、それに基づく運用が適切に行われるようであれば、前述の萎縮効果の度合いも低減し、表現の自由との関係上ただちに違憲と認められるものではなくなるように思われる。もっとも、ブロッキングを表現に対する「事前抑制」と捉える考え方も含め、表現の自由との関係については、より詳細な検討が必要となるため、改めて考察を加えることとする。いずれにしても、通信の秘密の保護及び表現の自由の保障との関係の双方の観点から、ブロッキングをただちに違憲と断じることが困難であると言えよう。

## 2.3 合憲説の概要

ブロッキングは基本的に憲法適合的に実施され得るものと捉える考え方(以下、「合憲説」という)は、表現の自由及び通信の秘密の双方の基本権を保障する観点から、その

合憲性を示唆している。その概要を整理すると、以下のとおりである。

第一に、表現の自由との関係において、わいせつ表現や名誉毀損表現等が一定の制約を受けていること(刑法175条・230条参照)にかんがみれば、違法なウェブサイトの表出の自由を憲法上の権利として観念することは困難であることから、それに対するブロックングの実施はその侵害となるものではないとされる。かかる考え方によれば、表現の客体となる表現物の受領者(以下、単に「受領者」という)の権利として、違法なウェブサイトを閲覧する自由を観念することも困難であり、同様の論理が妥当するといふ<sup>45)</sup>。

第二に、通信の秘密との関係において、ブロックングが人間の知覚を経ずに情報を自動的ないし機械的に検知することを伴う行為である限り、それを当該秘密の侵害と観念することは論理必然的ではないとされる。その背景には、通信の秘密はプライバシーを保護する意味合いを有する中で、ブロックングについては、自動的・機械的に検知された情報と個人の私生活や私的事項とを関連づける行為を伴わないことから、通信の秘密の侵害には該当するものではないという思想がある<sup>46)</sup>。もっとも、かかる考え方に対しては、電気通信の大半が機械的に処理されている今日では、通信の秘密の保護を空洞化させる危険性を内包することから、採用し得ないとする有力な批判が提示されている<sup>47)</sup>。

第三に、同じく通信の秘密との関係において、インターネット接続役務提供者が通信の宛先に関する情報を用いることは当然であって、当該情報の漏えいがあるわけではなく、その窃用が認められるとしても侵害の程度は極めて軽微なものであるから、それを上回る法益が認められる限り、ブロックングのための当該情報の利用は通信の秘密を侵すことにはならないという旨の考え方が示されている<sup>48)</sup>。また、ブロックングは、自らの通信設備を用いて他人間の通信の媒介に関する役務を提供しないという不作為にすぎず、当該媒介の目的から逸脱した利用とは言えないことから、そもそも「窃用」には該当しないという考え方も提示されている<sup>49)</sup>。

第四に、インターネット接続役務提供者が自主的に違法なウェブサイトを特定し、あらかじめ当該サイトへの接続要求は遮断することを示したうえで、自動的に当該サイトへの接続を拒絶することは、個別にアクセス情報を検知するものではない限りにおいて正当化されるという考え方がある<sup>50)</sup>。この考え方は、一定の条件下でのブロックングを合憲と捉えるものであり、これによれば、「画像や映像を中心とした児童ポルノやリベンジポルノ、漫画やアニメなどの作品への海賊版行為は違法性が判断しやすいこと」

に着目しつつ、このような対象に限定してブロックングの実施を検討すべきであるとされる<sup>51)</sup>。

## 2.4 合憲説の検討

第一の点(表現の自由との関係)については、他人の権利・利益を不当に害すると認められる表現物であれば、その表出の自由は「公共の福祉」を確保する観点から制約され得ると言えるであろう<sup>52)</sup>。しかも、ブロックングは表現物そのものをネットワーク上から排除するものではないことから、表現者の表現の自由との関係においては違憲性が認められる余地が比較的小さいと言える。しかし、例えばオンラインカジノサイトのように、違法性を伴い得るものではあるけれども他人の権利・利益を害することが明らかとは言いがたい表現物については、それに対する情報受領権の行使をブロックングという手段を通じて強制的に妨げることが表現の自由の侵害に該当しないとはただちに断じ得ない。そこで、まずはこの点に関する検討が必要である。

ここで、表現の自由の保障の基軸については、表現者自身の「国家からの自由」に関する利益を保護することにあると考えられる<sup>53)</sup>。仮に表現者の(表出行為に関する)利益を差し置いて受領者の(受領行為に関する)利益を積極的に保護することに表現の自由の保障の基軸があるのだとすれば、自律的な各受領者により異なり得るはずの個々の表現物に対する評価を公権力が先取りして一定の表現規制を行うことが比較的容易に正当化され得るところ、そのような行為は民意を通じた自己統治の確保という表現の自由の保障根拠に正面から抵触することとなるからである<sup>54)</sup>。実際、判例も、「公の福祉に反しない限り、いいたいことはいわせなければならない」と説きつつ<sup>55)</sup>、表現の自由の保護法益の基軸が表現者の利益にあることを示唆している。それゆえ、ブロックングにより受領者の情報受領権が一定の範囲で制約されるとしても、ウェブサイトを通じた表現者自身の表現の自由が直接制約されるわけではないことから、その制約度合いは比較的弱いものであると言える。

そのうえで、受領の対象となる表現物自体が(他人の権利の侵害を伴わずとも)違法なものないし違法な行為を伴い得るものである場合には、その違法性を示す根拠法令の規定が違憲と認められるものではない限りは、たとえ当該受領自体に違法性がなかったとしても、それを受領する自由が全面的に保障されるものではないと考えられる<sup>56)</sup>。よって、「公共の福祉」を確保する観点から、違法な表現物にアクセスする自由が一定の制約を受けたとしても、ただちに表現の自由の侵害となるものではないと思われ、その限りにおいて、前述の合憲説の考え方は合理的である。

第二の点(情報の自動的な探知との関係)については、

単純に機械的な処理であるから通信の秘密ないしプライバシーを侵害しないとは言えないということは、前述の学説上の批判が指摘するとおりであろう。そもそも、通信の秘密不可侵の規範は、通信当事者のプライバシーを保護するのみならず、通信の自由及びその客観法的側面としての「基本的な通信役務」の適切な提供の確保や、憲法適合的な通信制度の設営等を要請するものであるから<sup>57)</sup>、仮にプライバシーの侵害に当たらないとしても、それが当然に通信の秘密の侵害に該当しないということの十分な論拠にはならない。それゆえ、通信の秘密との関係に関しては、より精緻な分析が必要となるが、この点については後述する。

第三の点(窃用との関係)については、「窃用」が「公共の福祉」の確保の必要性に基づく正当な制約と認められる余地について検討する必要があるということは、違憲可能性説の検討に際して述べたことが当てはまる。すなわち、「窃用」の度合いが軽微であるか否かを考えるよりも、「窃用」が「公共の福祉」に沿った行為であるか否かを見極めることが肝要である。なお、ブロッキングは通信の構成要素となる情報を通信当事者の意思に反して利用することにより実施されるものであるから、たとえそれが通信役務の不提供(不作為)としての要素を有するとしても、「窃用」という行為の類型に該当すること自体は否めない。

第四の点(あらかじめ特定されたウェブサイトの接続拒否の位置づけ)については、「ブロッキングが常に合憲となるわけではなく、一定の条件下で合憲となり得る」ということを示したものであり、それ自体は正鵠を射た指摘であると思われる。問題は、どのような対象に絞ってブロッキングの実施が憲法上認められ得るのかということであるが、違法性が明確な児童ポルノサイトや海賊版サイト等に必ずしも限られるものではなく、犯罪の端緒となり得るフィッシングサイト等、誰もが情報通信を安心して利用するために必要となるネットワーク空間上の秩序(法秩序を含む)を明らかに乱すおそれがあると認められるウェブサイトも含まれ得ると考えられる。

### 3. 表現の自由及び通信の自由とブロッキングとの関係

検閲禁止の法理との関係については別論として、表現の自由との関係においてブロッキングが違憲であると明確に主張する学説は見当たらないが、その観点からの検討は有益であると思われるため、更なる考察を加えることとした。特に、違憲可能性説が示唆するような、ブロッキングを表現に対する「事前抑制」と捉える考え方については、再検討が必要であると思われる。

まず、一般に、表現の自由との関係において、表現行為に先立ち公権力がそれを抑制するという意味での「事前抑

制」については、表現物の発表の機会を失わせ得ることや、表現に対して重大な萎縮効果をもたらし得ることなどから、事後規制に比べてその憲法適合性を慎重に検討すべきであると考えられている。すなわち、表現の自由の保障には、表現物の表出に対する公権力(立法権を含む)による事前抑制が原則として禁止されるという命題(事前抑制の原則的禁止の法理)が含まれると一般に解されている<sup>58)</sup>。

ここでいう「表現行為」については、表現者による表現物の表出行為のみならず、受領者による受領行為も含むと解する考え方が有力であるところ<sup>59)</sup>、かかる考え方によれば、受領前に抑制する行為も「事前抑制」に含まれ得ることとなる<sup>60)</sup>。実際、一定の表現物(ウェブサイト)に対するブロッキングが行われる可能性は、その受領行為を「事前抑制」する効果をもたらし得るものであることから、波及的に関係する表現者にも一定の萎縮効果を与え得ると考えられる。それゆえ、ブロッキングのあり方については、さしずめ慎重にその当否が見極められる必要があると言えるだろう。

しかしながら、事前抑制の対象となる「表現行為」に受領者の受領行為も含めて捉える考え方には疑問がある。なぜなら、既述のとおり表現行為の本質は表出行為にあり、表現の自由の保障において受領者の利益は副次的に保護されるにとどまるものと考えられるところ、表現者の意図する形で表現物が表出された後であれば、たとえ受領者の受領前であったとしても、表現自体は完了していると捉え得るからである。したがって、憲法21条1項に基づき原則として禁止される「事前抑制」についても、表現物の表出に関する事前抑制として捉え、受領者の受領に先立つ事前抑制については別に捉える必要があるように思われる。換言すれば、憲法上、萎縮効果の大きさも踏まえて原則として禁止されるのは、基本的には表現物の表出に対する事前抑制であって、受領者の受領に先立つ事前抑制については必ずしもこの限りではない(当該抑制の程度や効果等に応じた個別の判断が必要)と考えられる。

ここで、海賊版サイト等のブロッキングは、既に表現物が表出された後で行われる行為であるから、表現者との関係では「事前抑制」とは言いがたい。その意味において、もっぱら受領者との関係から「事前抑制」となり得る行為であると言えるが、副次的に保護される受領者の「知る自由」ないし情報受領権を制約するものととどまる。また、かかるブロッキングが受領者の権利を制約するがゆえに表現者に一定の範囲で波及的に負の効果をもたらし得るとしても、表現の核心である表出行為それ自体に重大な萎縮効果を与えるものとは認めがたい。それゆえ、ブロッキングについては、必ずしも事前抑制の原則的禁止の法理に背馳す

るものとは言えないように思われる。換言すれば、ウェブサイトの開設者である表現者による表現の機会を剥奪するものではなく、受領者によるアクセスの機会を妨げるという点では表現の自由に対する一定の制約となり得るものの、受領者の権利自体は副次的に保護されるものにとどまるということを踏まえ、「公共の福祉」の確保のために必要となる正当な制約と位置づけることが可能である。

むしろ、ブロッキングについては、表現の自由とは区別された「通信の自由」に対する制約としての側面が問題となり得る。既述のとおり、通信の自由は、憲法 21 条 2 項後段の規定が保護する通信の秘密の論理的な前提となるとされる基本権であり、主観的権利としての「通信手段を用いた表現の自由」のみならず、発信者と着信者とが情報のやり取りを行う「通信」そのもの（通信過程）の自由を保護し、その健全な制度的利用環境の確保を公権力に求める客観法的要請を伴うものとして位置づけられる<sup>61)</sup>。

このとき、表現の自由の場合と異なり、通信の自由については、発信者の権利のみならず、受領者となる着信者の権利をもほぼ同等に保護するものと考えられる。なぜなら、「表現」は表現者がメッセージを表出すれば行為としてはひとまず完了し、それが誰にも受領されないことも想定され得るのに対し<sup>62)</sup>、「通信」は発信者が発した情報を着信者が受信し、又は受信し得る状態におかれるまでは行為として完結しないからである。すなわち、「通信」は発信者及び着信者という二面的な通信当事者の存在を前提とするところ、通信の自由が保護される環境の下では、発信者による「発信（送信）の自由」が保護されるのと同様に、着信者による「着信（受信）の自由」、すなわち発信者から発せられた情報を着信しようとする行為が公権力等により不当に妨げられないことが確保されなければならない。よって、ウェブサイトの情報の受領者を実質的な「着信者」と捉える場合<sup>63)</sup>には、ブロッキングにより着信者の「着信の自由」<sup>64)</sup>が阻害される点が通信の自由の侵害とならないかということが問題となる。

この問題に関しては、表現の自由に対する制約の場合と同様に、通信の自由との緊張関係が生じる行為であっても、「公共の福祉」を確保する観点から正当に行われ得るものについては、当該自由の侵害とは認められないという命題<sup>65)</sup>が一次的な回答を与えてくれる。すなわち、一定のブロッキング義務づけ立法に基づき行われ得る海賊版サイト等のブロッキングは、たとえ着信者の権利を正面から制約する側面を有するとしても、各人が安心してインターネット経由の通信を利用できるようになる制度的利用環境の形成を指向するものと認められる限り、通信の自由の客観法的要請を充足しつつ「公共の福祉」を確保する観点か

ら行われる行為として位置づけられ得る。また、その制約の手段としても、例えば当該サイトを通じたオンライン決済の停止等、他にも当該利用環境の形成に資する手段がないわけではないが、決め手となる有効な代替手段が乏しい中では、十分にその正当性が認められ得るように思われる。

#### 4. 検閲禁止の法理とブロッキングとの関係

違憲可能性説が指摘する「代理人による検閲」となる効果も踏まえると、ブロッキングと検閲禁止の法理との関係についても若干の検討を加えることが有用であろう。この関係におけるブロッキングの憲法適合性については、そもそも「検閲」をどのように定義し、検閲禁止の法理の保護法益をどのように捉えるかということによって結論が大きく変わり得る。

判例は、検閲について、「行政権が主体となって、思想内容等の表現物を対象とし、その全部又は一部の発表の禁止を目的として、対象とされる一定の表現物につき網羅的に、発表前にその内容を審査した上、不相当と認めるものの発表を禁止することを、その特質として備えるもの」と極めて狭く定義している<sup>66)</sup>。この定義に照らす限りでは、検閲はそもそも行政権を実施主体とするもので、かつ「発表前」の審査に限られることから、インターネット接続役務提供者の行うブロッキングが「検閲」に該当する余地は乏しくなる<sup>67)</sup>。仮にこのような解釈を採る場合には、ブロッキングと検閲禁止の法理との関係は問題とならず、過剰な「私的検閲」のおそれについては、私人間の法益の権衡をどのように図るかの問題におおむね吸収されることとなろう<sup>68)</sup>。また、検閲の概念を狭く捉えつつ、検閲禁止の法理を事前抑制の原則的禁止の法理の部分概念ないし一要素と捉える立場<sup>69)</sup>からは、検閲は事前抑制の中でも特に絶対的に禁止される形態と位置づけられることとなるため、ブロッキング義務づけ立法との関係上、あえて（事前抑制の原則的禁止の法理とは別に）検閲禁止の法理を援用する意義は乏しくなろう。

しかし、判例上の「検閲」の定義が実質的に検閲禁止の法理を死文化させるほどに狭すぎること<sup>70)</sup>や、必ずしも「発表を禁止すること」に該当しないものの不当な表現物等の審査及び抑圧を伴う行為もあり得るということを踏まえると、「検閲」とは、「各人の表現ないし情報の発着信に関して、公権力が主体となって、表現物の発表前又は通信の客体となる情報の着信前の段階で、その内容を審査したうえで、不相当と認めるときに当該発表を禁止し、又は当該情報の流通を遮断すること」と定義することが妥当であるように思われる<sup>71)</sup>。これは、検閲の実施主体を公権力全体と捉えている点において、判例の定義よりも広範である。そもそも、憲法規範の一次的な名宛人は公権力

全体であり、学説上も「検閲」の主体について公権力全体と捉える考え方もかねてより提示されていること<sup>72)</sup>も考慮すれば、このような捉え方は合理的であると言える。

同時に、前述の定義は、「表現物の発表前」の発表禁止に限らず、ネットワーク空間上における「情報の着信前」の流通遮断についても「検閲」の概念に包含しているという点にその特徴がある。従前の学説では「表現(表現物)に対する検閲」に焦点が当てられ、「通信(ネットワーク空間上の情報)に対する検閲」が十分に観念されてこなかった(ないしもっぱら通信の秘密の問題に吸収されると解されてきた)感があるが<sup>73)</sup>、ネットワーク空間を流通する情報の中には「表現」の客体ないし表現物とは言えないものも含まれ得る中で<sup>74)</sup>、当該空間上で表現物たる情報とともに流通の遮断としての「検閲」が行われるリスクがあることにかんがみれば、「表現に対する検閲」と「通信に対する検閲」とを一体的に捉えることが妥当であるように思われる。すなわち、検閲禁止の法理は、表現の自由のみならず、通信の自由をも補完する役割を果たすものと言える。

このように、公権力による審査の結果として情報の流通を遮断する行為と位置づける場合<sup>75)</sup>には、ブロッキング義務づけ立法に基づき行われるブロッキングについて、これを「立法権による検閲」<sup>76)</sup>と位置づける余地が生じ得る<sup>77)</sup>。前述のとおり、ブロッキングが行われようとする段階で問題となる表現物は既にインターネット上に表出されているはずであることから、当該表現物に対するブロッキングについては、事前抑制の原則的禁止の法理からみた表現の自由の保障の問題とは別に、情報の流通の遮断を伴う「検閲」の可能性をあえて正面から問題とする実益が大きいと考えられる<sup>78)</sup>。もとより、誰もが手軽に発信・アクセス可能なインターネット経由の通信を通じて表出される情報に関しては、表出前の「事前抑制」を問題とする物理的な余地が事実上乏しく、むしろ当該情報の流通時における公権力(立法権も含む)の抑制措置(遮断措置)が問題となる。

このとき、検閲禁止の法理の射程について、かかる遮断措置の禁止という意味合いも含めて観念すれば、ブロッキング義務づけ立法に基づくブロッキングも一定の情報の流通を遮断する措置として位置づけられるため、当該法理の問題として捉えられることとなる。検閲禁止の法理を定める憲法21条2項の規定は、同時に通信の秘密不可侵を規定しており、その前提として「通信の自由」が保護されるという相互関係があることにかんがみれば、当該自由を支える「(通信を通じた)情報の自由な流通」という状態を妨げる強制的な遮断措置については、通信の自由との関係の

みならず、検閲禁止の法理の下でも原則として禁止されると解される<sup>79)</sup>。ここに、ブロッキングとの関係において、表現の自由(事前抑制の原則的禁止の法理)とは別に、検閲禁止の法理との関係を正面から問う意義ないし実益がある。

もっとも、その場合であっても、「検閲」は個別の表現物その他の情報の<sup>・</sup>具体的<sup>・</sup>な審査及びその結果に基づく流通の遮断をその本質とする行為であると解される一方、立法権の行う「立法」とは<sup>・</sup>一般的<sup>・</sup>的<sup>・</sup>な法規範の定立であると解されていること<sup>80)</sup>にかんがみると、ブロッキング義務づけ立法に基づくブロッキングを「検閲」の概念で包み込むことが困難となるようにもみえる。しかし、たとえ立法自体が一般的・抽象的な法規範の定立として位置づけられるとしても、一定のブロッキング義務づけ立法において、インターネット接続役務提供者等の通信管理主体に個々の問題情報に対するブロッキングの実施が具体的に義務づけられる場合には、(仮にブロッキングの対象となるウェブサイトが法律の委任に基づき政省令等により特定されたとしても)立法権が実施主体となって個別の表現物の具体的な審査をインターネット接続役務提供者等に命じるものと捉えることが可能である。したがって、そのようなブロッキングは、インターネット接続役務提供者等を実行部隊とした「立法権による検閲」と位置づける余地があり、その限りにおいて、検閲禁止の法理に抵触する可能性が問題となる。

このとき、仮に「立法権による検閲」が特定の表現行為の恣意的な抑圧を目的として行われる場合には、実際に違憲となる可能性が高まるが、その目的が表出行為そのものの抑圧ではなく、一定の違法性が認められる表現物の受領・流通の抑止にあり、ネットワーク空間上の法秩序の維持を企図していると認められる限りにおいては、「公共の福祉」の確保の観点から正当化されるものと解する余地が残されているように思われる<sup>81)</sup>。もっとも、仮に検閲が<sup>・</sup>絶対的<sup>・</sup>に禁止されるのであれば、ブロッキングは常に違憲ということにもなり得るが、「通信に対する検閲」としての「情報流通の遮断」については、「公共の福祉」の確保の必要性が当てはまる余地が大きいと考えられる。なぜなら、「通信」はネットワーク空間という一種の閉鎖的な領域で行われるがゆえに、その円滑な実施を図る観点から一定の秩序の形成が求められ得るところ、当該秩序を確保するための手段として、一定の範囲で「遮断」が実施されることが求められ得るからである。

そもそも、検閲禁止の法理は、各人の表現の自由及び通信の自由の補完のみならず、情報の流通過程全般に公権力がみだりに介入しないことを通じて、各種のウェブサイト

や SNS 等の「国民参加型メディア」を含むマスメディア全体が発展することをその保護法益とするものと解される<sup>82)</sup>。SNS 等を含めた新旧各種のマスメディアが個人の尊厳とともに(表現の自由に支えられた)民主主義<sup>83)</sup>を支える役割を果たしている今日において、それらのマスメディアにおける表現の自由及び通信の自由(情報の自由な流通)が恣意的な検閲により妨げられることとなれば、民主的な政治過程に重大な悪影響が及ぶのみならず、各人の自律も脅かされることとなり得る中で、検閲禁止の法理がそのような可能性の発現に一定の歯止めをかけていると考えられるからである。他方、海賊版サイト等のブロッキングは、ネットワーク空間における法秩序を維持し、当該空間で正当に運営されるウェブサイト等の発展、ひいては国民参加型マスメディアの発展とそれに支えられた民主主義の発展に資すると認められることから、検閲禁止の法理(の保護法益)に適合的に実施され得るものと言える。

以上のように解する限り、海賊版サイト等のブロッキングによる「検閲」については、たとえ立法権による実施と位置づけられるとしても、「公共の福祉」の確保に資するものとして、例外的に許容され得ると考えられる。もっとも、その実施の態様が、立法に基づかないなどの適正な手続によらない場合や、表現の自由又は通信の自由に対する過度な制約となる方法で行われるものと認められる場合には、これらの基本権の侵害(違憲)となる可能性も残されるということには留意が必要である。

## 5. 通信の秘密とブロッキングとの関係

通信の秘密との関係におけるブロッキングの合憲性については、既述の学説上の議論に照らし、アクセス情報の検知及びその利用に伴う「窃用」の扱いが最大の焦点となると考えられる。ブロッキングは、利用者の意思に反した形でその通信の宛先を検知しつつ遮断するという「窃用」を伴う態様の行為である。既述のとおり、これを「通信の自由」の客観法的要請としての「基本的な通信役務」の適切な提供への背反の問題として捉える余地もあるが、形式的に「窃用」に該当する限り、まずはその窃用が通信の秘密の侵害と言えるのか否かを検討する必要がある。そこで、そもそも通信の秘密の「侵害」とはどのような行為の類型を指すのかということについて、検討する。

既述のとおり、「憲法上の通信の秘密」の侵害については、当該秘密を構成する情報の(積極的な)知得や漏えいという行為が該当すると一般に解されてきた。当該行為の主体については、公権力に限られると解する考え方が今日では有力になりつつあるが<sup>84)</sup>、通信事業者等の通信管理主体もこれに含まれると解する学説も提示されている<sup>85)</sup>。

しかし、このような一般的な捉え方を論じるのみでは、解釈論として不十分であると思われる。その理由として第一に、通信の秘密の保護法益が十分に検討されていないということが挙げられる。伝統的な憲法学説は、通信の秘密とは、①通信当事者(発信者及び着信者)のプライバシーの保護、②通信当事者の表現の自由の補完、をその保護法益とするものと捉えてきた<sup>86)</sup>。もちろん前記①か前記②かのいずれに比重をおくかという点で必ずしも一致していなかったものの<sup>87)</sup>、これらの両側面にほぼ収斂していたと言える。

ところが、通信の秘密の論理的な前提として「通信の自由」があり、それにより国民の誰もが健全な制度的利用環境下で自由に「通信」を行うことができるようになることが保障されている中で、通信管理主体が「通信」の完結のために一定の関与を行うことが予定され、当該主体により直接的又は間接的に(公権力を經由して)「秘密」が侵害されるリスクがあるということを踏まえると、通信の秘密の保護法益は前記①及び②のみに収斂するものではないと言える。なぜなら、通信当事者は、当該リスクを承知のうえで、統治主体である公権力及び「秘密」たる情報を直接取り扱う通信管理主体がそれをみだりに知得や漏えい等しないことを信用しつつ、当該情報の伝送等を託すことになるのであって、このような所為の本質は、通信当事者となり得る我が国の国民全体が普遍的に有していると客観的に認められる「信頼」にほかならないところ、かかる「信頼」を土台とする制度的利用環境の保護が「通信」の利用に当たって憲法上予定されていると考えられるからである。すなわち、通信の秘密の保護とは、各通信当事者が公権力及び通信管理主体に対して有すると認められる「信頼」を基礎として成立する「通信」の制度的利用環境を確保することにその主軸があるものと考えられる<sup>88)</sup>。それゆえ、「憲法上の通信の秘密」の侵害の主体には、「信頼」の向かい先である公権力及び通信管理主体の双方が含まれると解される<sup>89)</sup>。かかる「信頼」の内実には、伝統的に説かれてきた通信当事者の通信過程におけるプライバシー(及び表現の自由)の保護のみならず、ネットワーク空間上のセキュリティや通信基盤それ自体の健全性の確保等の多様な要素が含まれ、これらの要素が通信の秘密の具体的な保護法益となると考えられる<sup>90)</sup>。

このような通信当事者(利用者)の「信頼」を基礎として「通信」が成立するという捉え方については、学説上かねてより主張されていたが<sup>91)</sup>、近年の判例もそれを(「法律上の通信の秘密」との関係において)示唆するに至っている<sup>92)</sup>。このような通信当事者の「信頼」に適合すると認められるか否かという視点を捨象して、特定の行為の類

型を一律かつ機械的に「侵害」に直結させる解釈は、正鵠を射たものとは言えないであろう。

一般に、海賊版サイト等の違法なウェブサイトのブロッキングを公権力が義務づけることは、ネットワーク空間における一定の法秩序及び「通信」の過程を含めた制度的利用環境の確保（ひいては「公共の福祉」の確保）を目的とすることは明らかであるため、それが行為の類型として「窃用」に該当し得るからといって、通信当事者の「信頼」に背馳するものとなるわけではない。それどころか、かかる法秩序等の確保は、憲法 21 条 2 項後段に基づき保障される「通信制度」の内実に組み込まれるべき一要素であると捉え得る。また、インターネット接続役務提供者の行為としても、それが一定のブロッキング義務づけ立法に基づく措置として行われるものである限り、通信当事者も予見し得る行為であって、その「信頼」に反するものとは認められない。したがって、当該立法に基づくブロッキングは、たとえ主観的権利としての通信の自由と緊張関係に立ち、利用者のプライバシーにも一定の影響を及ぼし得るとしても、ただちに通信の秘密の侵害に該当するものではないと解し得る。

第二に、そもそも「窃用」については、「法律上の通信の秘密」の侵害をめぐる議論は別として「憲法上の通信の秘密」の侵害の一類型とは必ずしも捉えられてこなかったという経緯がある<sup>93)</sup>。実際、既に示したとおり、憲法学説では当該侵害の形態として「窃用」を指摘するものは乏しい。その理由は明らかではないが、窃用を行ううえでは情報の知得が必要となることから、その知得という類型を指摘しておけば足りるという思想があったのではないかと推察される<sup>94)</sup>。しかし、通信の秘密たる情報を知得することと、それを本来の目的とは異なる用途に利用することとは、明らかに別種の行為であり、通信当事者の「信頼」に背馳する度合いは後者の方が高いと捉えるのが自然であろう。とりわけ、通信管理主体の行為としては、積極的知得は必ずしも通信当事者の「信頼」に反するものではないと考えられるのに対し、窃用は別段の事情が認められない限り「信頼」に反するということが推定され得る。そうであれば、一般に「窃用」は通信の秘密の侵害となる可能性が高い行為類型として位置づけられるべきであり、その侵害への該当性を解除するのが「公共の福祉」の確保の必要性と捉えることが妥当である。

このとき、ブロッキングについては、前述の理由から、行為の類型としては「窃用」に該当するけれども、「公共の福祉」の確保のために必要となる行為であって、「侵害」には該当しないと解する論理の道筋をたどることが合理的である。海賊版サイト等のブロッキングは、ネットワーク

空間における違法な行為を制止させる（ないし防止する）ために行われることが予定され得るものである。その制止を端的かつ実効的に実現するための手段として一般に認知されているのがブロッキングである<sup>95)</sup>。かかるブロッキングが立法に基づいてインターネット接続役務提供者に対する義務として行われる限り、前述のとおり法秩序及び「通信」の制度的利用環境の確保という「公共の福祉」のために行われるものと認められる。その限りにおいて、これは決して通信の秘密を侵害するものではないと言える。

もっとも、ブロッキングについても、個々の通信の秘密たる情報を不当に利用したり、故意に漏えいさせたりするなどの不適正な態様で実施される場合には、憲法 13 条から導かれ得る比例原則<sup>96)</sup>等に照らして通信の秘密等の侵害となり、憲法適合性が維持されないこととなり得る<sup>97)</sup>。よって、インターネット接続役務提供者に一定のブロッキングを義務づける立法措置が講じられ、それに基づき適正な形でそれが実施される必要がある。また、現状ではブロッキングに代替し得る有力なアクセス防止手段が存在していないが<sup>98)</sup>、将来、技術開発の進展等によりブロッキング以外のより権利制限的でない新たな手段が見いだされた場合には、ブロッキングの実施が違憲と評価されることとなる可能性もある。さらに、現時点においても、ブロッキングの技術的な回避策はあると指摘されており<sup>99)</sup>、今後その実効性が著しく低下していくおそれも否定できない。それゆえ、過度な基本権の制約とならないよう、実施の態様には常に目を光らせる必要がある<sup>100)</sup>。

## 6. 結論

海賊版サイト等に対するブロッキングは、現時点の技術の動向を前提とする限り、表現の自由及び検閲禁止の法理との関係はもとより、「憲法上の通信の秘密」やその前提となる通信の自由との関係においても、一定の立法措置に基づき憲法適合的に実施され得る。その理由として、通信の秘密不可侵の規範は、公権力及び通信管理主体に対して各人が有すると客観的に認められる「信頼」を基礎として成立する「通信」の制度的利用環境の保護を指向していると解されるところ、海賊版サイト等に対するブロッキングの実施は当該保護に資する行為であって、基本的にそれに反するものとは言えないという要素が挙げられる。むしろ、公権力においては、かかる「信頼」に応える観点から、少なくとも違法な行為を招来ないし助長すると認められる一定のウェブサイトへのアクセスについては、インターネット接続役務提供者等の通信管理主体によるブロッキングが適切に履行されるような制度的利用環境を構築することが、各人の「通信の自由」を適切に保護するうえで求めら

れ得ると言えるように思われる。もっとも、技術革新の動向等に応じて、将来的にブロッキングの有効性が大幅に低減したり、ブロッキング以外のより権利制限的でない代替手段が開発されたりした場合には、ブロッキングの実施が「信頼」に反すると認められる状況が発現することもあり得るであろう。

他方、ブロッキングは、表現者によるウェブサイトの表出の自由を直接制約するものではないことを踏まえ、表現の自由に対する侵害とは認めがたい。同時に、検閲禁止の法理との関係に関して、一定の立法措置に基づくブロッキングが「立法権による検閲」と位置づけられるとしても、基本的には、ネットワーク空間上における法秩序を確保するための「公共の福祉」の観点から例外的に許容され得るものと解される。もっとも、オーバーブロッキングを全面的に許容するなど、表現の自由及び通信の自由を過度に制約すると認められる場合には、比例原則等に照らして違憲と評価される可能性も生じ得る。

以上を総合すると、ブロッキングは、それがネットワーク空間上における法秩序及び「通信」の制度的利用環境の確保を目的として立法に基づき適切に行われる限り、基本権の保障との関係から、憲法適合的なものと捉えることが可能である。従前の議論では、ブロッキングが「窃用」を伴う行為であることからただちに通信の秘密の侵害に結びつけて捉えられるきらいもあり、それがゆえに慎重な検討が必要な行為とされてきた。確かにブロッキング義務づけ立法の実施・運用に当たっては、精緻な制度設計が必要なのは言うまでもないが、通信の秘密は決してブロッキング実施の「壁」となるものではなく、むしろブロッキング実施が「通信の自由」の客観法的要請としての「通信」の制度的利用環境の確保に資するものとなり得る。そして、通信の秘密の保護に対する要請の根底には、公権力及び通信管理主体に対する通信当事者・国民利用者の客観的な期待としての「信頼」があり、その内実はおそらくプライバシーの保護にとどまるものではないという根本的な出発点が認識されるべきであるように思われる。

## 注

- 1) 多数の者がアクセスないし利用可能な通信用ネットワーク上の空間を指す。
- 2) 特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律(平成13年法律137号)2条9号参照。
- 3) ここでいう「媒介」とは、「他人の依頼を受けて、情報(符号、音響又は影像)をその内容を変更することなく伝送・交換し、隔地者間の通信を取次ぎ、又は仲介してそれを完成させること」と捉えられている。電気通信事業法研究会編(2024)68頁参照。
- 4) 裁判例も、「ブロッキングを実施した場合には、(中略)ユーザーの全通信内容(アクセス先)の検知行為が実行され、このことが日本国憲法21条2項の通信の秘密の侵害に該当する可能

- 性がある」と説いている(東京高判令和元年10月30日2019WLJPCA10306001参照)。
- 5) 安心ネットづくり促進協議会(2010)22頁参照。併せて、児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律(平成11年法律52号)16条の3参照。
  - 6) 漫画、アニメ等のコンテンツを著作権者等の許諾を受けずに不正に掲載している違法なウェブサイトのことを指す。
  - 7) 知的財産戦略本部・犯罪対策閣僚会議(2018)参照。
  - 8) 『インターネット上の海賊版対策に関する検討会議』(座長)検討状況報告(平成30年10月30日)参照。なお、この検討会議の経緯等について、久保＝安田＝鈴木(2020)5-9頁、穴戸(2025)327-328頁参照。
  - 9) 総務省(2025)3頁参照。
  - 10) 総務省(2025)17頁参照。
  - 11) 電気通信事業法(昭和59年法律86号)4条、有線電気通信法(昭和28年法律96号)9条、郵便法(昭和22年法律165号)8条等参照。
  - 12) 電気通信事業法研究会編(2024)76頁参照。
  - 13) 穴戸(2023)156頁参照。
  - 14) 電気通信事業法4条の解釈について、電気通信事業法研究会編(2024)76-84頁、海野(2015a)135頁・149頁参照。
  - 15) 佐藤(2020)356頁、海野(2015a)42頁参照。もっとも、「通信の自由」はしばしば通信手段を用いた「表現を非公開で行う自由」(高橋(2024)277頁)と同視されがちであるが、それにとどまらない保護法益(3節言及の「着信の自由」のほか、2.2節言及の「基本的な通信役務」の適切な提供の確保等の客観法的要請)を有していると解される。その詳細について、海野(2015a)190-216頁、海野(2018)29-32頁参照。
  - 16) 高橋(2024)277頁、渡辺ほか(2023)270頁(穴戸常寿執筆)、海野(2015a)47-48頁参照。
  - 17) 電気通信事業法179条、有線電気通信法14条、郵便法80条等参照。
  - 18) 電気通信事業法研究会編(2024)79頁参照。
  - 19) 刑法の解釈から導かれる違法性阻却事由が憲法解釈論にも妥当し得ると主張するための合理的な理由が提示されていないという旨を指摘するものとして、海野(2015a)62頁参照。近年の憲法学説上も、緊急避難等の違法性阻却事由を考慮する解釈論について、「正当業務行為や緊急避難の要件を借りて利益衡量を行うもの」であって「本来は、通信内容と通信の構成要素、さらには位置情報等の通信に関連する情報それぞれにつき、どのような保護がなされるのか、基本的な規律を法律に規定すべき」と説く見解が提示されている。曾我部(2020)68頁参照。
  - 20) 違憲可能性説は、必ずしもブロッキングが違憲であると断じるものではなく、違憲になり得るという旨を示し、一定の警鐘を鳴らすものである。
  - 21) ブロッキングは「すべてのインターネット利用者の宛先を網羅的に確認することを前提とする技術」であるとされる。総務省(2025)3頁参照。
  - 22) 森(2010)9頁、成原(2018)47頁参照。
  - 23) 成原(2018)48頁参照。
  - 24) 高橋〔郁〕(2023)39頁参照。このような考え方に対しては、国民全体にとっての通信役務の円滑な提供の確保の観点からは、海賊版サイトに対するブロッキングは正当業務行為とはなり得ないとする見解も提示されている。曾我部(2020)67頁参照。
  - 25) 「憲法上の通信の秘密」の侵害の行為類型としては、積極的知得及び漏えいが挙げられることが一般的である(例えば、佐藤(2020)356頁、渋谷(2017)413-414頁、長谷部編(2017)434頁〔阪口正二郎執筆〕参照)のに対し、「法律上の通信の秘密」の侵害の行為類型については、知得・漏えい・窃用が挙げられることが多い(電気通信事業法研究会編(2024)79頁参照)。この点を指摘するものとして、曾我部(2020)63-64頁参照。
  - 26) 伊藤＝前田(2018)36頁参照。
  - 27) 知的財産戦略本部・犯罪対策閣僚会議(2018)4頁参照。同文書においては、悪質な海賊版サイトに関するブロッキングについて、たとえ憲法上の通信の秘密の侵害に当たると仮定しても、刑法上の「緊急避難」の要件を満たす場合には違法性が阻却されると説かれている。
  - 28) 東川(2024)207頁参照。
  - 29) このような運用に対しては、立法を経ずに行政解釈のみに依

- 拠して緊急避難への該当性を認めること自体に問題があるとする主張も提示されている。東川(2024) 209 頁参照。
- 30) 曾我部(2020) 68 頁、曾我部(2021) 118 頁、大島(2026) 73-74 頁参照。
- 31) 前掲東京高判令和元年 10 月 30 日参照。併せて、成原(2018) 48 頁参照。もっとも、かかる考え方に対しては、違法なウェブサイトにて著作権を侵害するコンテンツが置かれ続けることに伴う収益の流出や著作権者の創作意欲の低下等にかんがみると、人格的利益との比較において一概に法益権衡の要件を充足しないと言い切ることはできないとする反論も提示されている。東川(2024) 208 頁参照。
- 32) 森(2010) 11 頁参照。
- 33) 大島(2026) 74 頁参照。
- 34) 佐藤(2020) 285 頁参照。
- 35) 森(2010) 12 頁、成原(2018) 48 頁、東川(2024) 215 頁参照。
- 36) 成原(2018) 48 頁参照。
- 37) 法律に基づくインターネット接続役務提供者によるフィルタリングについては、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) 17 条参照。
- 38) 海野(2018) 54-57 頁参照。
- 39) ここでいう「通信管理主体」とは、他人の需要を充足するために、一定の通信設備を用いて他人間のコミュニケーションの完結に向けて関与し、それに寄与する役務を提供しつつ、その過程で通信の秘密たる情報を直接取り扱う者のことを指す。海野(2018) 7 頁参照。
- 40) 海野(2015a) 46 頁・195 頁、海野(2018) 30 頁参照。「基本的な通信役務」の適切な提供の具体的なあり方について、海野(2015) 227-245 頁参照。
- 41) 実際、電気通信事業法 7 条に基づく規律の下でも、一定の固定系インターネット接続役務が「第二号基礎的電気通信役務」として位置づけられている(電気通信事業法施行規則〔昭和 60 年郵政省令 25 号〕 14 条の 3 第 1 項参照)。
- 42) 憲法 13 条の規定が内包する客観法的要請の詳細について、海野(2021) 59 頁参照。
- 43) オンラインカジノの利用等の違法な行為への入口となるウェブサイトへのアクセスが適切に遮断される環境は、誰もが安心してネットワーク空間(通信)を利用するための制度的な条件ともなり得る。
- 44) 毛利(2020) 330 頁参照。この学説は、「個々の表現活動が民主政治全体への貴重な貢献であること、それを禁止することが萎縮効果を通じて活発で豊かな討論の縮小、民主政治の機能低下を生み出す危険があることを考慮に入れる必要がある」(同書 298-299 頁)と説きつつ、表現の自由に対する制約の憲法適合性を判断するに当たって萎縮効果への配慮が必要となるという旨を示している。
- 45) 大日方(2021) 86 頁参照。
- 46) 大日方(2021) 85 頁参照。
- 47) 宍戸(2023) 154 頁参照。
- 48) 伊藤=前田(2018) 36 頁参照。
- 49) 伊藤=前田(2018) 34-35 頁参照。これによれば、「窃用」は「他人の通信を媒介する目的以外の目的」で行われる場合にのみ問題となるとされ、問題となる「サイトがブロッキング対象かどうかの検証プロセスも、通信の媒介を実現するプロセスの 1 つ」であるとされる。
- 50) 東川(2024) 206 頁参照。
- 51) 東川(2024) 218 頁参照。
- 52) 最判平成 20 年 4 月 11 日刑集 62 巻 5 号 1217 頁参照。
- 53) 有力な学説上、「表現の自由は『国家からの自由』を核心とし、国家による妨害の排除を請求しうる権利であり、国家による積極的行為を請求しうる権利ではない」と説かれている(芦部(2023) 191 頁参照)。併せて、海野(2018) 64-65 頁・87-88 頁参照。
- 54) 毛利(2020) 306 頁参照。この学説は、「表現の自由が民主政治に不可欠だという当然のように思われる主張は、国民一人一人が表現の説得力について自律的に判断できる主体であるという前提を有している」、「表現の受け手はそれぞれ自律した個人として表現内容を評価するのであって、その人々がどのような反応を示すかは、誰にも予測できない」(同書 302 頁)と説いている。そのうえで、「表現内容が受け手にもたらす反応を政府が一方向的に認定すること自体」が問題となるとし、「表現が受け手にもたらす効果は表現制約の理由にならないという原則」(同書 308 頁)ないし「政府は表現内容が受け手にもたらす効果を勝手に見積もってそれを表現制約の理由としてはならない」(同書 304 頁)という命題が確立されるべきであると主張している。併せて、そもそも憲法 21 条 1 項が「『表現を受け取る自由』を保障しているのかどうかは、定かではない」と説く有力な学説として、高橋(2022) 134 頁参照。
- 55) 最大判昭和 27 年 8 月 6 日刑集 6 巻 8 号 974 頁参照。
- 56) そもそも、表現の自由の保障とは、表現物の「表出の自由」の保障を基軸とするものであって(注 53 参照)、個々の表現物がどのような形でどの程度その受領者に受領されるのかを保障するものではないと考えられる。海野(2021) 240 頁参照。
- 57) その具体的な内容について、海野(2015a) 44-50 頁、海野(2018) 29-32 頁参照。また、注 15 参照。
- 58) 芦部(2000) 359 頁、佐藤(2020) 285-286 頁参照。
- 59) 芦部(2000) 361 頁参照。
- 60) 一部の学説においては、表現物の「発表前受領後をも事前抑制に含めようとする試みは、表現の自由の保障を拡大しようとするもの」であると評価されている。そのうえで、「発表後であっても表現の自由の優越的地位に沿って厳格に対応していくことが重要である」と説かれている。川岸(2024) 224-225 頁参照。
- 61) 通信の自由の内実の詳細について、海野(2015a) 190-208 頁参照。
- 62) 海野(2015a) 104 頁、海野(2018) 65 頁・88 頁、海野(2021) 240 頁参照。
- 63) ウェブサイトへのアクセスは、アクセスしようとする者(閲覧者)が URL を用いて送信要求(HTTP リクエスト)を行い、それにウェブサーバーが応答(HTTP レスポンス)することにより、行われ得る。それゆえ、当該閲覧者は、厳密には HTTP リクエストの「発信者」ということになり得るが、閲覧者とウェブサイト(ウェブサーバー)との交信が行われており、情報の発信源がウェブサイト側になることにかんがみれば、実質的な情報の「着信者」と位置づけることが可能である。
- 64) 海野(2018) 30 頁参照。
- 65) 海野(2015a) 297 頁参照。
- 66) 最大判昭和 59 年 12 月 12 日民集 38 巻 12 号 1308 頁参照。
- 67) 学説上、判例のように「検閲」を極端に狭く解しすぎると、検閲への該当性が否定されつつ、それと区別された「事前抑制」が容易に認容されるという「本末転倒」な帰結が導かれるという問題点が指摘されている。川岸(2024) 224 頁参照。
- 68) SNS の管理者等がプラットフォーム上の流通情報を任意に削除等する行為を伴う「私的検閲」を「表現の自由としての検閲」と捉え、当該管理者等の基本権である「表現の自由」の行使とその私的検閲の対象となる表現物の表現者の権利との相克関係が問題となるという旨を指摘する学説として、駒村(2024) 308 頁参照。
- 69) 佐藤(2020) 286 頁参照。他方、検閲禁止の法理を事前抑制の原則的禁止の法理と一体的に捉え、検閲の概念を機能的に捉える学説も有力である(芦部(2000) 362-363 頁参照)。このような立場に立つある学説は、表現物の伝達が意図されている段階での公権力による不当な制約を防止する観点から、検閲と事前抑制とを一元的に捉えることが「表現の自由にとって保護的」とであると説いている。川岸(2024) 224 頁参照。
- 70) この点につき、例えば、奥平(1988) 97-98 頁参照。
- 71) 海野(2015a) 401 頁参照。
- 72) 芦部(2000) 362 頁、芦部(2023) 218 頁参照。
- 73) 伝統的な憲法学説においては、「通信の秘密に関する検閲とは、公権力により通信の秘密を破ることをいう」(宮沢(1974) 383 頁)と説かれている。
- 74) 海野(2018) 66 頁参照。
- 75) 海野(2015a) 381 頁・389-390 頁参照。
- 76) 海野(2015a) 390 頁参照。
- 77) 憲法学説上は、「検閲を行う主体を行政権に限定するか、裁判所も含めるか」(高橋(2024) 241 頁)が主な争点となってきたが、「検閲」の主体を公権力と捉える限り、立法権がその主体から外れると解する合理的な理由は乏しく、法律により一定の事業者等に「検閲」相当の行為を義務づける場合には、「立法権による検閲」を概念する余地があると考えられる。
- 78) 事前抑制の原則的禁止の法理と検閲禁止の法理との関係について、憲法学説は、①検閲禁止の法理は広く表現行為の事前抑制を対象とするが、例外も認められると捉える考え方、②検閲は絶対的に禁止されるが、それは一般的な事前抑制より

も狭い概念であって、検閲に該当しない事前抑制が「事前抑制の原則的禁止の法理」の問題となると捉える考え方、に大別されると指摘されている。毛利ほか(2022) 217 頁(毛利透執筆)参照。しかし、表現の自由から導かれる事前抑制の原則的禁止の法理は、表現の核心を占める表出行為の事前抑制を主に念頭におくものであって、表現物の受領行為の抑制については必ずしも直接問題とするものではないのに対し、検閲禁止の法理は、表現物その他の情報が流通する状態も視野に入れつつ、当該情報に対する公権力の審査の結果を踏まえ、その流通の遮断に結びつく行為(表出行為の遮断に限らず受領行為の遮断も含まれる)を原則として禁止するものと解しつつ、両法理を区別して捉えることが妥当であるように思われる。「検閲」の客体については、もっぱら表現物に限らず広く情報全般が含まれるのであって、表現の自由のみに引き寄せて(表出行為の事前抑制に限定する形で)検閲禁止の法理を捉える必要性が乏しいからである。

79) 海野(2015a) 381 頁参照。

80) 芦部(2023) 320 頁、長谷部編(2020) 485 頁(六戸常寿執筆)参照。

81) 「検閲」の概念を狭く捉える立場からは、検閲は絶対的に禁止されると説かれている(佐藤(2020) 286 頁参照)。そうであれば、「立法権による検閲」について、「公共の福祉」の確保に基づき例外的に許容される場合などは想定されないこととなり得る。他方、「検閲」の概念を機能的に広く捉える考え方からは、裁判所による検閲について「厳格かつ明確な要件の下で許されることもある」とされ、それが必ずしも絶対的に禁止されるわけではないという旨が説かれている(芦部(2023) 218 頁参照)。思うに、憲法 21 条 2 項前段には、憲法 36 条と異なり、「絶対に」といった文言はないため、絶対的に禁止されると解する合理的な根拠を欠く。それに加え、少なくとも憲法が保護する「通信」の領域においては、ネットワーク空間上で憲法規範に背馳する状態を招来すると認められる情報(セキュリティ上の重大な脅威となり通信の利用を著しく妨げる情報や他人の基本権に関する法益を侵害し通信の安定的な利用それ自体を著しく萎縮させ得ると認められる情報等)の流通が恒常的に行われる場合には、その流通の遮断が「検閲」ないしそれに類した行為により正当に行われ得ると考えられるため、「公共の福祉」の確保を理由とする例外を観念する余地が認められる。海野(2015a) 387 頁参照。

82) 海野(2015a) 385 頁参照。

83) 憲法 1 条・15 条 1 項・43 条 1 項等の規定に照らし、憲法は民主主義の体制を予定していると解される。

84) 毛利ほか(2022) 271 頁(毛利透執筆)、六戸(2023) 153 頁参照。

85) 佐藤(2020) 356 頁、長谷部編(2017) 434 頁(阪口正二郎執筆)、渋谷(2017) 414 頁、海野(2015a) 53-54 頁参照。

86) 芦部(2000) 541 頁参照。

87) プライバシーの保護に軸足を置く主な学説として、長谷部(2022) 237 頁参照。表現の自由の補完に軸足を置く主な学説として、阪本(1995) 140 頁参照。

88) 海野(2015a) 131-133 頁、海野(2018) 34 頁参照。ここでいう「信頼」は、各人の主観的な期待ではなく、各人が公権力や通信管理主体に対して有すると客観的に認められる期待を指す。また、法律上の通信の秘密の保護法益をめぐる解釈論として、「信頼」の確保を指摘するものとして、電気通信事業法研究会(2024) 76 頁参照。

89) その意味において、憲法 21 条 2 項後段の規定は、「通信事業者に特別の位置づけを与える」(渡辺ほか(2023) 270 頁〔六戸常寿執筆〕)のものであると言える。仮に通信事業者その他の通信管理主体が憲法 21 条 2 項後段の規定(その客観法的要請を含む)に拘束されず、もっぱら「法律上の通信の秘密」に基づく規律を受けるのだとすると、技術革新の動向等に応じて当該規律の及ばない「法律上の欠缺」が生じ得る中で、立法措置が適時適切に行われるという保証もないことから、利用者の「通信」に関する基本権が適切に保護されない状況が生じるおそれがある。同時に、通信管理主体自身において、自らのネットワーク設備に対する財産権等の行使を通じて特定の「通信」に関する情報を差別的に取り扱うなどの恣意的な行為が行われる場合には、憲法の次元において当該情報の利用者(通信当事者)が「対抗」できなくなるという問題も抱えることとなる。よって、通信管理主体も、個々の通信を取り扱う局面においては「憲法上の通信の秘密」を保護する義務を負う主体となると解される。この点について、海野

(2015a) 50-54 頁、海野(2018) 27 頁参照。

90) すなわち、通信の秘密の保護法益の核心は、ここでいう「信頼」そのものと言うよりも、「信頼」を基礎として成立する制度的利用環境にある。その意味において、「信頼」は機能的な説明概念にとどまるとも言える。なお、「信頼」という概念は、公務員の政治的表現の自由に対する制約が問題となった猿払事件判決(最大判昭和 49 年 11 月 6 日刑集 28 卷 9 号 393 頁)において「行政の中立的運営が確保され、これに対する国民の信頼が維持されることは、憲法の要請にかなう」という形で、当該制約を正当化するための論拠として用いられ、学説の批判の対象となってきた(例えば、抽象的な「国民の信頼」がそれ自体として公務員の政治的表現を制限すべき理由にはならないと説く学説として、浦部(2016) 179 頁参照)。その根底には、「信頼」という概念を通じて、表現の自由に対して許容される制約の範囲が無限定に拡大し得るという懸念があったと思われる。このような「信頼」の概念に対する批判にかんがみると、通信の秘密が保護する制度的利用環境の土台に通信当事者の「信頼」があるとする考え方に疑問が提示されるかもしれない。しかし、猿払事件判決における「信頼」が公務員の政治的表現の自由の制約事由となっており、かつ憲法上の保護法益そのものとして位置づけられているのに対し、通信の秘密における「信頼」は、「憲法上の通信」の制度的利用環境を支える基礎条件として機能するものであって、一種の説明概念であるという点で、猿払事件判決の場合とは意味合いが大きく異なる。換言すれば、猿払事件判決における「信頼」は、国民各人の心理的な信頼感をベースとしているのに対し、通信の秘密における「信頼」は、個人の心理や感情に基づくものではなく、通信の利用者が一般に有すると認められる構造的な前提条件(通信に際して公権力や通信管理主体による不当な干渉等を受けずに安心して安全に行うことができること)に対する合理的・客観的な期待をその内実とするものである。したがって、「信頼」がやや抽象的な概念であるからといって、通信の秘密との関係においてその妥当性・有用性が否定されるべきものということにはならず、またそれにより許容される制約の範囲が無限定に拡大されるということにもならないと考えられる。

91) 海野(2015a) 142-143 頁参照。

92) 最決令和 3 年 3 月 18 日民集 75 卷 3 号 822 頁参照。もっとも、判例は、「電気通信事業法 4 条 1 項が通信の秘密を保護する趣旨」について、「表現の自由の保障を実効的なものとするとともに、プライバシーを保護することにある」としつつ、「電気通信の利用者は、電気通信事業においてこのような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」と説いているのであって、通信の秘密それ自体の保護法益が「信頼」であるとまでは断じていない。

93) 既述のとおり、主要な憲法学説は、積極的知得及び漏えいを侵害の類型として挙げている(注 25 参照)。

94) もっとも、近年の憲法学説では、「通信を成立させる以外の目的で通信の秘密に属する事項の取得・利用・提供が広く通信の秘密の侵害に当たる」と説くものもある。渡辺ほか(2023) 271 頁(六戸常寿執筆)、六戸(2025) 324 頁参照。かかる立場からは、「窃用」も通信の秘密の侵害に該当し得ることとなる。なお、「通信」の制度的利用環境の確保という観点からは、当該侵害が認められる範囲を「通信を成立させる以外の目的」に限定することの妥当性については議論の余地があるように思われる。

95) 総務省(2025) 20 頁参照。

96) その詳細について、さしあたり、海野(2011) 69-76 頁参照。

97) なお、学説上は、通信の秘密に対する制約となる立法に関して、「公共の福祉に適合する重要な目的のために必要かつ合理的な範囲での制限を、目的外の取得・利用等がされないことを担保するための制度的な措置を加えた上で、立法化することは憲法上許される」と説くものもある。渡辺ほか(2023) 272 頁(六戸常寿執筆)参照。このような見解に照らせば、ブロッキング義務づけ立法について、それが「公共の福祉に適合する重要な目的のために必要かつ合理的な範囲での制限」と認められ、ブロッキングの目的外利用等を防止するための制度的措置が当該立法上盛り込まれている限り、必ずしも比例原則による審査を経ずとも、その憲法適合性が認められ得るということになろう。通信の秘密の主たる保護法益を「通信」の健全な制度的利用環境と捉える限り、衡量可能な利益

を厳密に特定しがたい場合も少なくないと考えられることから、もっぱら比例原則に依拠するよりも、問題となる制約を規定する立法(ブロッキング義務づけ立法)の内容に合理性が認められるか否かを端的に問うアプローチの方が、通信の秘密の制約のあり方の検討には親和性が高いと言えるかもしれない。

- 98) 実務上、アクセス警告方式等が提案されてきたものの(総務省(2019)7-21頁参照)、ブロッキングほどの実効性をあげるものと評価されてはいない。ブロッキング以外の「他の手段が一定程度講じられている中であってもなお、被害が減らないという実態」も指摘されている。総務省(2025)17頁参照。
- 99) 例えば、VPN(仮想的な専用線)等によりDNSサーバ(ドメイン名とIPアドレスとを紐づけ、変換する仕組みを提供するサーバ)を迂回する方法等が指摘されている。総務省(2025)20頁参照。
- 100) 諸外国では、ブロッキングの実施に関する制度的対応のあり方について、国・地域により径庭が見られる。例えば、欧州連合(EU)においては、古くは情報社会指令(Directive 2001/29/EC)8条3項に基づき、権利者において、著作権等の侵害に利用される仲介者(インターネット接続役務提供者等)に対して差止命令(ブロッキング命令も含まれ得る)を求める地位が保障され、それに基づく構成国内の法制化が適宜行われた。一方、オープンインターネット規則(REGULATION (EU) 2015/2120)3条3項においてウェブサイト等のブロッキングが原則として禁止されているが、公権力の命令を含む法令に基づく措置の場合等は例外となっている。これを踏まえ、デジタルサービス法(REGULATION (EU) 2022/2065: DSA)9条は、構成国の当局が違法コンテンツに対してブロッキングを含めた一定の行動をとるよう命じる際の手続等について規定している。したがって、インターネット接続役務提供者等の仲介サービス事業者が当局の命令に従ってブロッキングを行うことは、オープンインターネット規則の定めるブロッキング原則禁止の例外に該当し得るものと位置づけられ、一定の場合にはブロッキングが強制的に行われ得ることが予定されていると言える。EUでは基本権憲章(Charter of Fundamental Rights of the European Union: 2000/C 364/01)7条に基づき通信が尊重される権利が保障されていることも踏まえつつ、このような制度的枠組みが設けられていることに照らすと、ブロッキングも、その対象が違法な表現物であって一定の手続に基づき実施される場合には、適法(基本権の保障に適合的)となり得るという旨が示唆される。なお、米国においても、かつては連邦通信委員会(FCC)の規則(FCC 15-24: FCC 24-52)によりブロッキングの原則禁止が定められていた時期もあったが(海野(2015b)52-53頁参照)、2026年現在この内容は実質的に無効化されている(See Ohio Telecom Ass'n v. FCC (*In re* MCP No. 185), 124 F.4th 993 (6th Cir. 2025).)。もっとも、当該規則で禁止対象となっていたのは合法的なコンテンツ等の差別的なブロッキングであって、違法なコンテンツ等のブロッキングは禁止の対象外となっており、今日においても違法なウェブサイトへのアクセスの遮断を明示的に禁止する連邦法の規律は特段設けられていない。

## 参考文献

- 芦部信喜(2000)『憲法学Ⅲ 人権各論(1)』(増補版)。有斐閣。  
 芦部信喜〔高橋和之補訂〕(2023)『憲法』(第八版)。有斐閣。  
 安心ネットづくり促進協議会(2010)「法的問題検討サブワーキング報告書」。  
 伊藤真、前田哲男(2018)「サイトブロッキングと通信の秘密」『コピライト』690, 28-38頁。  
 海野敦史(2011)『行政法綱領—行政法学への憲法学的接近—』晃洋書房。  
 海野敦史(2015a)『「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(2015b)「米国における新オープンインターネット保護規則及びそれを定める命令・決定の諸相—ネットワークの中立性をめぐる議論の二次的な到達点とその要諦—」『ICT World Review』8(1), 41-73頁。  
 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。  
 浦部法穂(2016)『憲法学教室』(第3版)。日本評論社。  
 大島義則(2026)「ブロッキングの可否—通信の秘密を中心として」『ジュリスト』1619, 70-75頁。  
 奥平康弘(1988)『なぜ「表現の自由」か』東京大学出版会。  
 大日方信春(2021)「海賊版サイト・ブロッキングの憲法適合性」『法律時報』93(2), 82-87頁。  
 川岸令和(2024)『表現の自由の苦難』日本評論社。  
 久保雅一、安田和史、鈴木香織(2020)「サイトブロッキングの現在地」『日本知財学会誌』16(3), 4-13頁。  
 駒村圭吾(2024)「表現の自由としての検閲?」高橋和之、長谷部恭男編『芦部憲法学—軌跡と今日的課題』岩波書店, 289-315頁。  
 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(2023)「表現の自由(5)(表現の自由の現代的課題②—放送の自由、通信の秘密、インターネットと表現の自由)」『警察学論集』76(10), 135-178頁。  
 宍戸常寿(2025)「通信の秘密・再訪」『行政法の理論と実務 宇賀克也先生古稀記念』319-342頁。  
 渋谷秀樹(2017)『憲法』(第3版)。有斐閣。  
 総務省(2019)「インターネット上の海賊版サイトへのアクセス抑止方策に関する検討会」(令和元年8月)。  
 総務省(2025)「オンラインカジノに係るアクセス抑止の在り方に関する検討会 中間論点整理」(2025年9月)。  
 曾我部真裕(2020)「通信の秘密」『法学セミナー』786, 62-68頁。  
 曾我部真裕(2021)「2018年情報通信法制タスクフォース：著作権侵害サイトのブロッキングに対する意見表明」『情報法制レポート』1, 118-120頁。  
 高橋郁夫(2023)「欧州における著作権侵害コンテンツに対する媒介プロバイダの対応責任の動向とわが国への示唆」『Nextcom』53, 32-41頁。  
 高橋和之(2022)『人権研究1 表現の自由』有斐閣。  
 高橋和之(2024)『立憲主義と日本国憲法』(第6版)。有斐閣。  
 知的財産戦略本部・犯罪対策閣僚会議(2018)「インターネット上の海賊版サイトに対する緊急対策」(平成30年4月)。  
 電気通信事業法研究会編(2024)『電気通信事業法逐条解説』(再訂増補版)。情報通信振興会。  
 成原慧(2018)「海賊版サイトのブロッキングをめぐる法的問題」『法学教室』453, 45-52頁。  
 長谷部恭男(2022)『憲法』(第8版)。新世社。  
 長谷部恭男編(2017)『注釈日本国憲法(2) 国民の権利及び義務(1) §10～24』有斐閣。  
 長谷部恭男編(2020)『注釈日本国憲法(3) 国民の権利及び義務(2)・国会 §25～64』有斐閣。  
 東川玲(2024)『情報空間と法—表現の自由の衝突とプライバシーの新たな諸相』京都大学学術出版会。  
 宮沢俊義(1974)『憲法Ⅱ』(新版：改訂)。有斐閣。  
 毛利透(2020)『国家と自由の法理論—熟議の民主政の見地から—』岩波書店。  
 毛利透ほか(2022)『憲法Ⅱ 人権』(第3版)。有斐閣。  
 森亮二(2010)「ブロッキングに関する法律問題」『ジュリスト』1411, 7-13頁。  
 渡辺康行ほか(2023)『憲法Ⅰ 基本権』(第2版)。日本評論社。

[受付日 2025. 11. 28]

[採録日 2026. 4. 1]