〈日本知財学会誌〉Vol. 16 No. 3― 2020 : 23-31

通信の秘密とサイトブロッキング（序説）

大日方信春（熊本大学法学部 教授）

Relation between Secrecy of Communication and Site Blocking

Nobuharu Obinata
Professor of Kumamoto University Faculty of Law

【要旨】「海賊版サイト」対策としてブロッキングの是非が議論されている．ただこの議論の前提にある憲法上の「通信の秘密」(21 条 2 項後段）の意義は，これまで必ずしも明らかにされてはいない．本論文では同法原則は，憲法 21 条 1 項が保障する表現の自由に内包される「通信の自由」のためのものであると述べている．そこから秘密の対象とされる「通信内容」と「通信データ」では保障程度が違うこと，通信の秘密は通信の自由の前提となる通信制度が適切に設定・運営されるためのものであることを導いている．

このような通信の秘密の理解をもとに電気通信事業法の関係条文の検討を経て，本論文の後半では「海賊版サイト」ブロッキングの憲法適合性について検討している．そこでは，「海賊版の自由」は観念できないこと，ISP による機械的なアクセス検知は「通信内容」の推知にはあたらないこと等を理由に，ブロッキングが必ずしも憲法に反するものではないと結論している．

【キーワード】 通信の秘密　　サイトブロッキング　　通信の自由

【Abstract】 This essay's aims are two. For one thing it shows clearly the meaning of "secrecy of communication". This constitutional principle has not showed sufficiently.

The other aim is examining the constitutionality of site blocking. In conclusion, this essay shows that site blocking is not always contrary to the Constitutional Law.

【Keywords】 Secrecy of Communication　　Site Blocking　　Freedom of Communication

はじめに

「海賊版サイト」に対するブロッキングをインターネット・サーヴィス・プロバイダ（以下「ISP」）が行なうことは憲法上の「通信の秘密」(21 条 2 項後段）を侵害するのか[1]．通信の秘密の意義は，この問題を解く鍵となると思われるけれども，同法原則に関する憲法学の分析はこれまで必ずしも十分なものではなかったと思われる[2]．本論文の第一の課題は，憲法上の通信の秘密の意義について明らかにすることである．

つづいて，ISP によるサイトブロッキングは憲法に反するのか．憲法学者内においてはサイトブロッキング違憲論が有力である[3]．本論文の第二の課題は，ISP による同行為の憲法適合性を検討することにある．

但し，本論文はインターネットの技術的側面を解さない者の不確かな記述を伴うものであると思われる．また，紙幅の都合もあり，憲法論としても十分な議論が展開されているわけではない．標題にある「(序説)」はその弁解である．

1．概念の整理

議論の前提として，本節では，本論文のキーワー

ISSN 1349-421X © 2020 IPAJ All rights reserved.

ドについて概説しておきたい. 本来ならば, キーワードはもっと多く，より深く考察する必要もあろう. ただ，本論文は標題に関する研究序説であるので, 重要ワードの簡単な分析に止めたい.

1.1. 「通信の自由」と「通信の秘密」

1.1.1. 通信の自由

表現とは，記号を用いて知覚・感情・思考などの「心の動き」を表出することである．ここにいう記号とは，言語，文字，絵画，音楽，身振り，手振り，表情などの「他者に反応性向を与えるもの」のことである[4].

憲法 21 条 1 項は，一切の「表現の自由」を保障している．そこには「集会」,「結社」,「言論」,「出版」という一定の表現類型が掲げられているけれども，これらは表現のうち，歴史的にみて最も伝統的で利用容易であった類型を掲げたものと理解すればよいであろう．同条項は, 類型に拘わらず, 表現（記号を用いて心の動きを他者に伝達し反応性向を得る行為）につき国家から干渉されないことを保障している.

ところで，通信とは，特定の発信者と受信者との間で，特定のコミュニケーション・チャンネルを通して，上の表現をなすことである[5]．したがって，通信とは表現の下位類型の一つであるので，通信は憲法 21 条 1 項にいう「その他一切の表現」に該当することになる．通信の自由とは「その他一切の表現の自由」の一内容であり，それは通信につき国家から干渉されないことをいう.

憲法上の通信の自由の意義は，通信の発受・搬送過程における国家による通信の妨害や差別的取扱いを禁止することにある．また，この行為規範を国家を含めた通信業務従事者との関係で規定したのが郵便法および電気通信事業法であろう.

1.1.2. 通信の秘密

憲法 21 条 2 項後段は「通信の秘密は，これを侵してはならない」と規定する．本規定は，同項前段の検閲禁止規定との類比でいえば，21 条 1 項の表現の自由を保障するにあたり，とくに濫用されがちな側面を明示的に掲げたものと理解すればよいであろう．21 条 1 項で保障された通信の自由の保障が確保されるためには，上の通信妨害や差別的取扱いが禁止されるだけでは足りず, 通信の許諾なき知得・利用（窃用）・開示（漏洩）をも禁止する必要があるというのである.

憲法上の通信の秘密の意義は，国家に対し，通信の秘密の侵害を禁止することにある．と同時に，国家を含めた通信業務従事者に通信の秘密を侵害させない法制度の設営を国家に要請したことにある．このことを規定したのもまた，郵便法および電気通信事業法であろう.

1.1.3. 「通信の自由」と「通信の秘密」の関係

上で述べたことを踏まえてここで両法原理の関係を整理しておく.「通信の自由」とは，通信の妨害や差別的取扱いを禁止する法原理である.「通信の秘密」とは「通信の自由」を保障する上で特に濫用されがちな通信の自由侵害行為をピックアップして禁止しようとした法原理である.

1.2. 「通信内容」と「通信データ」

通信の構成要素を大きく類型化すると通信の内容と通信の存在それ自体を示すデータに分けることができる．本稿では前者には「通信内容」, 後者には「通信データ」という呼称を与えている.

1.2.1. 通信内容と通信の秘密

日本国憲法の制定過程に着目したある研究は，改正草案にある「secrecy of any means of communication」の意味を注視することで，憲法 21 条 2 項にいう「通信の秘密」は通信の「内容」について保障されるものであるとの見解を表明している[6]．これにはいくつかの疑問が投げかけられているけれども[7]，通信の秘密が「通信内容」に与えられることを揺るがすものではない.

1.2.2. 通信データと通信の秘密

通信の「秘密」が，通信の内容のみならず「通信データ」まで，具体的には通信の発受者の氏名，通信の日時・回数，受取者の氏名・住所等まで対象とするものであるのかについて，従来の裁判例・学説は，説明に苦慮してきたように思われる[8].

たとえば，ある下級審は，郵便集配人が開封の書状にあった名宛人の住所・氏名・電話番号を他人に漏らしたことの違法性が争われた事例において，郵

便物の委託者の郵便官憲への信頼を根拠に「通信データ」の秘密該当性を肯定したことがある[9]．発信者の主観は「通信データ」がなぜ秘密に当たるのかを論証するものとはならないであろう．

また，憲法学説は「通信の秘密」の根拠をプライヴァシーの保護に求めるものが有力である．ある論者は「憲法学における通説的理解」を整理して「通信の秘密の対象を（略）広く理解することは，憲法21条2項後段の趣旨をプライバシーの保護に求める場合には素直な結論であ〔る〕」としている[10]．ただ，本論文は「通信の秘密」の論拠はプライヴァシー保護ではないと考えている．このことは後述している（2.2.2）．

「通信データ」も秘密の対象となることについて，実務上は「これらの事項〔通信の存在自体を示すデータ〕を知られることによって通信の意味内容が推知される」可能性が指摘されている．しかし，この理解は，単なる萎縮効果を秘密該当性の理由としている点で説得力に欠けている[11]と同時に，「推知」とは人間がある事柄から物事を推し量って知ることであろうから，インターネットにおける海賊版ブロッキング過程にある「人の知覚によらない知得」（機械的知得）からは得られない作用であろう．このことについても後述している．

1.2.3. 小　括

「通信データ」まで通信の秘密の対象であるか否かの検討は置くとして，ここでは，少なくとも「通信内容」と「通信データ」とは通信の秘密に関する規範定立にあたり区別して取り扱われるべきものであることを指摘したい．通信の秘密の保障も絶対的なものではないことを前提に，制約理由となる対抗利益との関係で，後者の保障程度は前者のそれより低いといえるであろう[12]．

1.3. 通信事業従事者

1.3.1. コモン・キャリア

通信事業者は，従来「コモン・キャリア（common carrier）」として捉えられてきた．コモン・キャリアとは「指定料金が支払われた以上，乗客や貨物の運送を拒絶できないことを法令によって義務づけられている業者[13]」のことをいう．このような理解の下，通信事業者は，①伝送行為における自由を否定されたあと，②個々の通信を詮索しない義務を負わされた（「情報不接触の原則」）．これらのことと表裏一体として，③伝送した通信内容に対する法的責任を負わない，とされてきている．このように「コモン・キャリア」概念は，通信事業従事者に法令上禁止される行為を導き出す法規範としての地位が与えられている．

ところが，この「コモン・キャリア」の概念は，法令上明確なものではない．とくに，インターネット接続事業者がこれに該当するという実定法上の規定[14]があるアメリカに対して，同規定がないわが国の場合には，注意を要するところであろう．「コモン・キャリア」とされる通信事業者として例示されるのが，郵便・電話の時代のものに一般的に止まっている現状が，この問題が未解決であることを例証していると思われる．

1.3.2. 情報不接触の原則の論拠と例外

ある論者は「『コモンキャリア』が一定の通信事業者を意味することは明かであるが，この概念の規範的な内実や射程については共通理解が存するのであろうか」との疑問を呈し，それにも拘わらず「法律上の役務提供義務の有無がコモンキャリアへの該当性を介して憲法規範の適用範囲を実質的に左右〔していることは〕」「解釈論上の合理性を欠く」と評価している（傍点は原文）[15]．どうやら「コモン・キャリア」であるか否かではなく（コモン・キャリアなら「情報不接触の原則」に拘束されるのではなく），通信制度の適切な運営という視点から通信事業従事者の法的義務を演繹する筋での検討が生産的なようである（2.2.2の末文および4.2.3の末文も参照）．

2. 憲法上の「通信の秘密」の論拠

なぜ「通信の秘密」を保障すべきなのか．本節では「通信の秘密」の論拠に関する学説の整理と評価を行なう．

2.1. プライヴァシーの権利との関係

2.1.1. 通説的見解

「通信の秘密」の論拠について，それが表現の自由の条文に含まれていることから，通説的見解は「表現の自由の保障の一つとしての意味を有する」としつつも「私生活・プライバシーの保護としての意味」を主たる目的としていると理解している[16].

これは21条2項後段をヨーロッパ型の「通信の秘密」の流れを汲むものとする理解にも適するようである[17].

2.1.2. 有力な見解

これに対して，通信の秘密を表現の自由と関連させるならばその保障範囲が狭くなると考えて，通信の秘密を表現の自由から切断して理解する見解がある．いわく「通信の秘密の意義を，表現の自由を保障するためにある，と解した場合には，その範囲は，表現の自由を確保するために実質的に保護するに値する秘密であるかどうか，によって決まるから，通信自体を秘密とみなした場合より，その範囲は，狭く解されることになる．（略）他方，通信の秘密の根拠を，プライバシーの保護にある，と解した場合には，そこで保護されるのは，通信の存在それ自体であり，通信の形式・内容が，実質的な秘密にあたるかどうかまで判断する必要がないことになる」[18].

有力説は「通信の秘密はプライヴァシーの核心部分の一つであ〔る〕」としている[19].

2.2. 本稿の見解

2.2.1. プライヴァシーを論拠とする見解への批判

通説的見解も有力説も，通信の秘密をプライヴァシーとの関係で基礎づけようとする点では共通している．ただ，こうした見解は，次のような批判があり得るであろう．

①プライヴァシーという概念を「私生活上の自由」と結びつけて理解するなら，問題の情報の非公知性・要秘匿性が問われざるを得ないのではないか．たとえば，不特定多数者に送信したダイレクト・メールは，通信の秘密が保障されるのであろうか[20].

②電気通信の当事者は，今日において，法人の場合も多い．いわゆる人格権を論拠とするプライヴァシーを，法人との関係でも成立する法益と捉えることができるのか.

③「通信データ」を保護することがなぜ「プライヴァシー」を保護することになるのか不明確である．「プライヴァシー」が憲法上の保護法益であることを認めたとしても，なお「通信データ」が対立利益と関わりなく「秘密」に該当することの論証はなされていない[21].

④プライヴァシーの権利を情報化社会の中における「自己情報コントロール権」と考えても，それが個人情報の不当な取扱いおよびそれに起因する不利益を防止するもの[22]であるなら，その恐れのない「通信データ」の無許諾利用を禁止する規範は同権利の保護からは導出できないのではないか．また，発受信者にとって他者の情報まで「自己情報」といえるか.

このように通信の秘密の意義をプライヴァシーとの関係で説明しても「通信内容」と区別された「通信データ」まで「秘密」の対象であることを論証できていないと思われる.

2.2.2. 通信の秘密は表現の自由の問題領域にある

通信の秘密は，日本国憲法上では表現の自由を保障した21条上に規定されている．したがって，まず通信の秘密の論拠を表現の自由と区別して専らプライヴァシーとの関係で理解しようとする見解は不当であろう.

つぎに「通信の秘密」をプライヴァシーと関係する法益と理解したとしても，その保護対象が「通信内容」を超えて「通信データ」にまで及ぶことの論拠とはならないであろう．通信の秘密の保障範囲を拡大するためにそれをプライヴァシーと関係させて理解することも無意味である.

本論文は通信の秘密は通信の自由の一内容であり，通信の自由は表現の自由の一内容であることから，したがって「通信の秘密」は表現の自由を保障するためのものと捉えている[23]．端的にこのように理解することが日本国憲法の条文構造にも適うであろう.

では，なぜ通信業務従事者は「通信内容」を超えて「通信データ」まで秘密の対象とすべきなのであろうか．それは，表現の自由には表現の名宛人の外に誰にも知られずに表現する自由まで含まれている

からである．但し，この自由も絶対的な保障を受けるものではない．通信事業者に，少なくとも「通信データ」についてどのような取扱いが求められるのかについては，法制度上の調整が必要であると解される．そのさい，通信事業従事者が「コモン・キャリア」であるとされていることに，インターネット時代においては，不用意に依存すべきではない．コモン・キャリアは，わが国では通信事業者に課された義務の淵源となる法概念ではないことはすでに述べた（1.3.2）．

3. 憲法と電気通信事業法の関連条文の意義

憲法上の表現の自由に内包される「通信の自由」を保障するための法原則である「通信の秘密」は，通信に関する業法において具体的に規定されている．インターネットを舞台にした通信の秘密の意義を検討するにあたり，本節では，憲法と電気通信事業法（以下「電通事業法」ということもある）の関連条文に関する理解の整理を行なう．

3.1. 検　閲

3.1.1. 憲法 21 条 2 項前段にいう「検閲」

判例は，憲法 21 条 2 項前段で禁止されている検閲について，つぎの定義を与えたことから確認しよう．すなわち「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一般的に，発表前にその内容を審査した上，不適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」[24]．

この定義により憲法上検閲ではないとされたことは何か．それは，大要，つぎのようになる．①検査対象が思想内容ではないもの，②網羅的ではなく付随的になされるもの（関税徴収手続に付随してなされた税関検査），③特定的・個別的審査（具体的犯罪に関する押収・没収），④発表禁止の効果をもたないもの，これらは判例の検閲の定義によると憲法上の検閲ではない．

この定義を厳密に捉えるなら，ブロッキングするサイトを行政機関が判断することも，憲法上の検閲には該当しないであろう．なぜなら，①サイト運営者の表現の自由が観念できるとしても，その判断は，表現形式（form of expression）の同一性を判断するもので思想内容等によるものではないこと，②閲覧希望者の知る権利を観念できるとしても，ブロッキングは事前抑制的効果が強いとはいえ，なお「発表の禁止を目的」「発表前に」と判例が拘った事前規制そのものではないこと（そもそも正規版は公開されている），これらが理由となる[25]．

よくサイトブロッキングは「検閲に該当する」といわれることがある．そこでいう「検閲」とは憲法上の検閲のことではなかろう．

3.1.2. 電気通信事業法 3 条にいう「検閲」

電気通信事業法 3 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．ここにいう「検閲」の意味について，逐条解説には「国その他の公の機関が強権的にある表現又はそれを通じて表現される思想の内容を調べることをいう」とある[26]．この理解によっても，海賊版サイトが送信している「公然性を有する通信」の表現形式を判断するものは電通事業法 3 条上の「検閲」でもないことになるであろう．強権性に欠けている．

また，上の規定の名宛人は国家である．したがって，ISP によるブロッキングがこの法律に反する行為であるとはいえないと思われる．ISP は国家機関ではない．

3.2. 電気通信事業法 4 条の 1 項と 2 項

3.2.1. 総　説

憲法 21 条 2 項後段は，前述しているように（1.1.2 末文），国家に対し通信の秘密の侵害を禁止すると同時に，通信業務従事者に通信の秘密を侵害させない法制度の設営を国家に求めている．この要請をうけて，電通事業法に設けられた規定は，その規定ぶりから，同法 4 条 2 項であると解される．

では，電気通信事業法 4 条 1 項の意義は何か．それは端的に電気通信事業従事者以外の者に対して，電気通信事業者の支配下にある通信について，その知得・窃用・漏洩を禁止していると理解すればよかろう．通信の秘密の保護を高めようとした法政策で

ある．電通事業法 179 条 1 項は，4 条 1 項に反する行為に罰則を科している．

3.2.2. 「通信の秘密」(4 条 1 項) と「他人の秘密」(4 条 2 項)

通説・実務上「通信の秘密」の対象は「通信内容」および「通信データ」とされている．これとの関連で「他人の秘密」の対象は，「通信の秘密」の対象を超えて，通信当事者の人相，言葉の訛り等をも含むものであるというのが実務的理解である[27]．

インターネット時代の通信において，この違いを維持する意味は薄いであろう．それでも，通信業務に従事しない者には「通信の秘密」を超える「他人の秘密」の保護義務は課されていないことは（4 条 1 項の構成要件には含まれていない），罪刑法定主義との関係では重要であろう．

3.2.3. 「侵してはならない」(4 条 1 項) と「守らなければならない」(4 条 2 項)

電気通信事業法 4 条 1 項は，電気通信事業者以外の者に対して通信の秘密を「侵してはならない」と規定している．これは端的に通信事業者の支配下にある通信の知得・窃用・漏洩を禁止した規定と理解すればよいことは前述した（3.2.1）．

これに対して，同条 2 項は電気通信事業者に他人の秘密を「守らなければならない」と規定している．この「侵してはならない」と「守らなければならない」の意味の違いは，同事業者に長らくある通信に対する「不干渉（hands-off）」の規範意識の下，注視されてこなかったという[28]．

ところが，この「不干渉の原則」は，電気通信事業においては，一部，インターネット・サーヴィスの安定的提供のための正当業務行為として，また，一部「媒介者の責務」を理由として，崩されてきている．前者の例としては「迷惑メール防止法」(平 14 法 26）が，後者の例としては「プロバイダ責任制限法」(平 13 法 137）による発信者情報の開示等があげられる．

たしかに，電通事業法 4 条 1 項が通信事業従事者以外を対象として課した通信の秘密非侵害（「侵してはならない」）の法規範は，その端的な規定ぶりと相俟って，一般的な行為禁止規範であると理解できる．これに対して，事業者に課された「他人の秘密」を「守らなければならない」という法規範は，国民に安心かつ円滑な電気通信事業を提供する国家の憲法 21 条上の責務を満たす通信制度の設定運営との関係で（4 条 2 項がこの要請をうけたものであることについては上述 3.2.1），法上の実質化があり得ることを前提とした規定なのではなかろうか．この点について，著者の研究はさらに深められる必要があろう．

3.3. 電気通信事業法 6 条

3.3.1. 不干渉原則の直接の規定

電気通信事業法 6 条は「不干渉の原則」が直接規定されていると理解できる．電気通信従事者をコモン・キャリアたらしめているのも，この規定の効果であろう[29]．それは，脅迫的内容の電報を配達しない民法（709 条）上および条理上の義務を，NTT について否定した裁判例の基盤にある法原則といえるであろう[30]．

3.3.2. 通信の自由の具体化

従来の学説は，通信業務の提供拒否を「通信の秘密」条項の規範内容から導き出そうとしてきたように思われる．それは牽強付会というものであろう．通信業務従事者に対する通信の取扱い拒否，不当な遅延行為，通信文の隠匿，放棄等の禁止は，通信の自由の規範内容であると理解すべきであろう[31]．

4. 海賊版ブロッキングとの関係で

ここまでの前捌きをうけて，本論文は漸く「海賊版ブロッキング」の憲法適合性を判定する段にきた．

4.1. 問題設定

4.1.1. 例　　題

20XX 年，海賊版サイトによる著作権侵害の防止を求めて，権利者がプロバイダを被告として，海賊版サイトの差止訴訟を提起したとしよう．差止めの方法は DNS ブロッキング[32] を想定する．DNS（Domain Name System）とはインターネット上でドメイン名と IP アドレスの対応関係を管理するシステムのことである．

4.1.2. 問題の所在

紙幅の都合もあり，本論文では，つぎの点に焦点

を合わせようと思う．

①海賊版ブロッキングは，サイト運営者および閲覧希望者の表現の自由（通信の自由）を侵害するか，②海賊版ブロッキングは，通信の秘密を侵害するか，③プロバイダの責任を問うことは可能か，④現行法下で可能か．

以下，順に解答を与えていく．

4.2. 本論文の解答

4.2.1. 送信者および発信者の表現の自由を侵害するか．

まず，海賊版サイト運営者の「海賊版の自由」という権益が成立するとは思えない．他者加害に及ぶ同行為は，表現の自由との関係ではその内在的制約と考えればよく，著作権法上の公衆送信権を侵害する（著作 23 条）．

つぎに，閲覧希望者の「海賊版を見る権利」という権益も成立しないと思われる．同権利をあえて一般権益として捉えるなら「知る権利」に内包されると思われるけれども，同権利はその発祥から第一義的には政府情報に対する権利として成立しているものと解するべきであり，私人運営のサイトについては，同サイトが閲覧可能であることの反射的利益と捉えればよいであろう．したがって，閲覧希望者のこの権利は，すぐ上で否定したサイト運営者の表現の自由に還元すればよいと思われる．

4.2.2. 海賊版ブロッキングは，通信の秘密を侵害するか．

サイトブロッキングは，インターネット利用者の通信一般を検知し特定の通信を遮断するという措置である[33]．したがって，海賊版サイトの閲覧と関わりない通信も含めて「通信の秘密」を侵害するのではないか，との疑問がある．

しかし，この点に関しては，まず，この検知は「通信の秘密」が第一義に保護している「通信内容」に関わるものではない．また，DNS ブロッキングに必要な「通信データ」まで秘密の対象であったとしても，それを機械的に検知することまで「通信の秘密」で保護されているのであろうか．機械的検知まで「通信の秘密」を侵害するという理解が一般に流布されているが，その根拠が明らかにされたことはないと思われる．データにより内容が推知されることを防止するためというなら，前述しているように（1.2.2 末文），人の手の介在しない検知で誰が何を推知できるのであろう．

4.2.3. プロバイダの責任を問うことは可能か．

この問題について，本論文は，プロバイダ責任制限法を補助線として考察しようと思う．

プロバイダ責任制限法 3 条 1 項は，プロバイダが送信防止措置を実施しないことで，他者の権利について生じた損害に対する不作為責任を免じられる場合について規定している（同条 2 項は，送信防止措置の実施に関し，当該情報の発信者に生じた損害に対する作為責任が免じられる場合が規定されているが，ここでは措く）．ところで，プロバイダに課されている「情報不接触の原則」あるいは「不干渉の原則」が仮に絶対的なものであるなら，そもそも上の 3 条 1 項のような規定は不要であると考えられるのではなかろうか．なぜなら，伝送している通信について事業者の責任を想起すること自体ができないのだから．

この点について，問題含みの「公然性を有する通信」に対するプロバイダによる送信防止措置の実施について，プロバイダ責任制限法の制定前から法律上許容される余地があるものとして一般的な理解があるという[34]．また，下級審の裁判例においても，プロバイダの「条理上の作為義務」を説いたものがある[35]．但し，実際にどこまでの防止措置が法律上許容されるのか，条理上の責任が生じる要件および根拠については，明確ではなかった．プロバイダ責任制限法は，憲法上の通信の自由の要請を受けた通信制度が国民の信頼の下に運営されることを目的として，プロバイダによる送信防止措置と同者に課された秘密保護要請との法上のバランスを示したものであると理解できる．その議論は，プロバイダが「コモン・キャリア」であるか否からスタートしていない．憲法上の要請を受けた通信制度が適切に運営されるためにはいかなるルールが必要であるのか．同法の視点には教条主義が見られない．

たしかに，海賊版ブロッキングは，ISP に「公然性を有する通信」に対する送信防止措置を求めるものではない．しかし，海賊版が権利者をはじめコン

テンツ産業全体に与える損害が実証されている現在[36]，インターネット通信業務従事者のこのことに対する「条理上の責任」は皆無とはいえまい．この点，外国に目を転じると「プラットフォームの責任（媒介者の責任）論」，「no fault remedy 論」等が説かれているという．ISP の「条理上の責任」論は，上述の機械的検知と通信の秘密の関係（4.2.2）とともに，これから憲法学および情報法学が従来の教条的な議論（コモン・キャリア論，秘密侵害論）から離れて，インターネット時代に相応しい議論を展開するための導きの糸となるのではなかろうか．

4.2.4. 海賊版ブロッキングは現行法上可能か．

管見の限り，電気通信事業法，プロバイダ責任制限法および著作権法に，権利侵害者ではなく ISP を名宛人とした海賊版に対する差止を求める明確な根拠規定はなさそうである．ただ「カラオケ法理」や間接侵害と構成することにより著作権法上の差止請求（112 条 1 項）の相手方性を肯定することはできるのかもしれない．

近時，通信制度自体の信頼に「通信の秘密」およびその前提となる「通信の自由」を保護する意義を見出す見解がある[37]．海賊版ブロッキングの実施には，国家にこうした行為規範を課した憲法の精神を反映させた法律の制定が望ましいとはいえるであろう．

5. おわりに

冒頭のエクスキューズを思い起こしていただきたい．著者の能力および紙幅上の制約により，論文の二つの課題（憲法上の「通信の秘密」の意義，「海賊版ブロッキング」の憲法適合性判定）に十分な検討を与えることはできていない．憲法学の時流・大勢に逆らうには心許ない内容ではあるが，各所に波紋が広がれば水面に投げられた石の本懐を遂げたと思う．

注

1 この問題に関するコンパクトな解説として，参照，関真也「サイトブロッキングと『通信の秘密』の関係」(https://business.layers.jp/articles/371)（2020 年 1 月 21 日最終閲覧）．

2 参照，宍戸常寿「通信の秘密に関する覚書」高橋和之先生古稀記念『現代立憲主義の諸相 下』487, 491 頁（有斐閣, 2013 年），曽我部真裕「通信の秘密の憲法解釈論」Nextcom 16 号 14, 14 頁（2013 年）．

なお, サイバースペースにおける言論を念頭に「通信」と「表現」を区別する 21 条の分析枠組を批判的に検討したものに，君塚正臣「日本国憲法二一条の『表現』と『通信』の間に―放送・通信技術の進歩と憲法の人権保障の行方―」関西大学法学論集 51 巻 6 号 1 頁（2002 年）がある．

3 参照，情報通信法制研究タスクフォース「著作権侵害サイトブロッキング要請に関する緊急提言」(平成 30 年 4 月 11 日)〔研究主幹として曽我部真裕，構成員に宍戸常寿〕，木下昌彦「著作権侵害サイトのブロッキングをめぐる憲法上の問題について」内閣府知的財産戦略本部検証・評価・企画委員会（平成 30 年 2 月 16 日）資料 4．

4 参照，阪本昌成『憲法理論Ⅲ』4～12 頁（成文堂，1995 年），同『憲法2 基本権クラシック〔第 4 版〕』146 頁（有信堂高文社，2011 年），同『プライヴァシー権論』231～232 頁（日本評論社，1986 年）〔以下「プライヴァシー権論」〕．

なお，表現は，思想・信条の表出にとどまらない．それは「説明のつかない感情の表出」であってもいい（参照，Cohen v. California, 403 U.S. 15〔1971〕におけるハーラン法廷意見）．また，事実に関する知覚の表出（報道）も一定の主義・主張をもってなされるゆえに表現となろう（参照，博多駅テレビフィルム提出命令事件に関する最大決昭 44・11・26 刑集 23 巻 11 号 1490 頁）．

5 特定のコミュニケーション・チャンネルとは郵便および電気通信のことである．したがって，通信とは，郵便または電気通信役務による特定者間の情報の授受のことである．

6 参照，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 5 号 44, 47～55, 68 頁(2006 年)．

7 参照，宍戸・前掲論文（註 2）494～496 頁．

8 東京地判平 14・4・30（判例集未登載，LEX/DB28075652）は「通信の秘密」の対象に「通信データ」も含まれることを肯定している．

9 参照，大阪高判昭 41・2・26 高刑集 19 巻 1 号 58 頁．

10 参照，宍戸・前掲論文（註 2）496 頁〔漢数字を算用数字に改めている〕．そこで整理の対象とされている「通説的理解」は，芦部信喜『憲法学Ⅲ 増補版』540 頁以下（有斐閣，2000 年），芦部信喜編『憲法Ⅱ 人権（一）』635 頁以下（有斐閣，1978 年）〔佐藤幸治執筆〕，鈴木秀美「通信の秘密」大石眞＝石川健治編『憲法の争点』136 頁以下（有斐閣，2008 年）である．

11 参照，阪本・プライヴァシー権論 236 頁．

12 それは情報の価値に基づくものではない．「通信内容」の暗号化は容易である反面，「通信データ」にあたる宛先やヘッダー情報のそれには限界があると思われる．宛先に届かないかもしれないので．

13 阪本・プライヴァシー権論 234 頁．

14 *See* 47 U.S.C. § 153 (11), (51) (2016).

15 海野敦史『通信の自由と通信の秘密』122，128 頁（尚学社，2018 年）．

16 参照，野中俊彦ほか『憲法Ⅰ〔第 5 版〕』397 頁（有斐閣，2012 年）〔中村睦男執筆〕．

17 宍戸・前掲論文（註 2）はボン基本法 10 条 1 項を例示してこの点を指摘している．

18 平松毅「通信の秘密」芦部信喜編『憲法判例百選Ⅰ』66, 67 頁（有斐閣，1980 年）．

19 参照, 長谷部恭男『憲法〔第 7 版〕』234 頁（新世社, 2018 年）．

20 参照，阪本・プライヴァシー権論 237 頁．

21 阪本・同書同頁は「プライヴァシーであれば，なぜ，自動的に『秘密』とみなされるのか, その演繹過程が抜けている」としている〔強調は原文〕．

22 個人情報が適切に扱われるなら，その収集・利用に情報主体の同意が必須であるとまでもはいえまい．参照，曽我部真裕「自己情報コントロール権は基本権か？」憲法研究 3 号 71 頁以下（2018 年）．

23 参照，阪本・プライヴァシー権論 240～241 頁．そこでは「郵便によって伝達する過程は，口頭による伝達する権利と同じく，言論の自由の一部である」としたアメリカ連邦最高裁の判例（Blount v. Rizzi, 400 U.S. 410, 416〔1971〕）の参照も促

されている．

24　税関検査事件に関する最大判昭 59・12・12 民集 38 巻 12 号 1308 頁．

25　著者は，海賊版表現の自由という法益は観念し得ないと考えている．なぜなら，それはもっぱら「保護されない表現」とせざるを得ないと考えているからである．その意味で，憲法上の特権または免責を想定し得る名誉毀損表現およびプライヴァシー侵害表現（公職候補者，権威者に対する言論保護等）や虚偽表現（真実発見等）とは異なると思われる（括弧が不法行為言論に憲法上の特権または免責を与える理由である．海賊版にはこれが観念し得ない）．本文は，それでもなお，サイト運営者の海賊版送信の自由，サイト閲覧者の海賊版受信の自由が成立するとした場合のものである．

26　参照，多賀谷一照監修＝電気通信事業法研究会編著『電気通信事業法逐条解説〔改訂版〕』34 頁（情報通信振興会，2019 年）．

27　同書 38 頁．

28　参照，林紘一郎＝田川義博「サイバー攻撃の被害者である民間企業の対抗手段はどこまで可能か：日米比較を軸に」情報セキュリティ総合科学 10 号 1，52〜53 頁（2018 年）．

29　参照，林紘一郎＝田川義博「サイバー攻撃対策としてのログの知得・利用と『通信の秘密』」情報セキュリティ総合科学 11 号 1，7 頁（2019 年）．

30　参照，大阪地判平 16・7・7 判時 1882 号 87 頁．

31　参照，阪本・プライヴァシー権論 234〜235 頁．

32　DNS ブロッキングの仕組については，参照，Michael Schlesinger＝遠山友寛「日本国におけるオンラインでの著作権侵害への対処 ── サイト・ブロッキングの導入に向けて ──」コピライト 677 号 26，32〜34 頁（2017 年），伊藤真＝前田哲男「サイトブロッキングと通信の秘密」コピライト 690 号 28，29〜32 頁（2018 年）．

33　インターネット利用者がアクセス先について検知されないことの期待については，児童ポルノ遮断措置の実施によりすでに失われている．

34　民法 720 条の規定に基づく正当防衛等として不法行為責任は免責されるという議論があったことについて，参照，海野・前掲書（註 15）167 頁．

35　参照，ニフティサーブ（現代思想フォーラム）事件に関する東京地判平 9・5・26 判時 1610 号 22 頁，同控訴審（東京高判平 13・9・5 判時 1786 号 80 頁），東京都立大学事件に関する東京地判平 11・9・24 判時 1707 号 139 頁．

36　参照，Photonic System Solutions (PSS)「日本におけるインターネット上の海賊版サイト及びアプリの定量化と分析」(2019 年 9 月）（未公刊）．

37　参照，渡辺康行ほか『憲法 I 基本権』216，256 頁（日本評論社，2016 年）〔宍戸常寿執筆〕．曽我部・前掲論文（注 2）．