論題 Title	通信の秘密をめぐる議論の諸相
他言語論題 Title in other language	Aspects of the Debate over the Secrecy of Communications
著者 / 所属 Author(s)	神足　祐太郎（KOTARI Yutaro） / 国立国会図書館調査及び立法考査局　国土交通課
雑誌名 Journal	レファレンス（The Reference）
編集 Editor	国立国会図書館 調査及び立法考査局
発行 Publisher	国立国会図書館
通号 Number	834
刊行日 Issue Date	2020-07-20
ページ Pages	43-61
ISSN	0034-2912
本文の言語 Language	日本語（Japanese）
摘要 Abstract	日本国憲法及び電気通信事業法等の各種法律に規定される「通信の秘密」について、その内容、趣旨、通信事業者の業務との関係を整理し、これをめぐって行われてきた議論を紹介する。

通信の秘密をめぐる議論の諸相

国立国会図書館　調査及び立法考査局
国土交通課　神足　祐太郎

目　　次

キーワード：通信の秘密、ブロッキング、ネットワーク中立性、違法有害情報、電気通信事業法

要　旨

① 日本国憲法第21条第2項後段は、「通信の秘密は、これを侵してはならない」として、通信の秘密を保障し、電気通信事業法等の各種法令においても、通信の秘密は侵してはならないものとして、刑事罰が規定されている。

② 通信の秘密の保障の範囲には、通信内容の秘密にとどまらず、通信の外形的事項、構成要素（メタデータ）も含まれると考えられており、これらの知得、窃用、漏えいは通信の秘密の侵害に当たる。

③ 憲法上の通信の秘密の趣旨は、表現の自由の保障としての意味を認めつつ、プライバシー保護の趣旨を重視する見解が有力とされているが、「通信の自由」の保障の有無や法律上の通信の秘密との関係など、論点も残されている。

④ 通信の秘密は、通信事業者の業務の様々な局面に関係し、いったん、通信の秘密侵害の罪の構成要件を満たすと考えた上で、刑法上の違法性阻却事由（正当行為、正当防衛、緊急避難）に該当するかを検討するというかたちで慎重な検討が行われ、各種ガイドラインが作成されてきた。

⑤ また、近年では、通信の秘密は、違法又は有害な情報（児童ポルノ、海賊版サイト）のブロッキング、ネットワーク中立性、セキュリティなど、様々な議論の中で論点となってきたほか、国外事業者への対応のため、電気通信事業法の改正も行われた。

⑥ 諸課題への対応のため、通信内容に関する保護と通信の外形的事項に関する保護の程度を分ける等、通信の秘密の解釈の再検討を求める声がある一方、通信の秘密は日本のインターネットにおいて「意図せざる「基本設計」」としての意義を持つという指摘もある。

⑦ 国外事業者への適用や新しいビジネスモデルへの影響、事業者への負担等を考慮すると、個別の事例に応じた検討にとどまらず、通信の秘密の制約が認められる一般的な条件について、検討を深める必要がある。

はじめに

日本国憲法第21条第2項後段は、「通信の秘密は、これを侵してはならない」として通信の秘密の保障を規定している。また、「電気通信事業法」（昭和59年法律第86号）等の法律においても、通信の秘密の保護が罰則付きで規定されている。これらの規定は、郵便、電話などを念頭に置いた情報通信法制の中で、一定の役割を果たしてきたものの、活発な議論が行われる論点ではなかった(1)。

他方、近年、インターネット社会が進展し、違法又は有害な情報のウェブサイト等を通じた一般公衆に向けた発信、サイバー攻撃など従来と異なる問題が生じる中で、通信の秘密は大きな論点の一つとなっている。これらの問題の解決に当たって、インターネット・サービス・プロバイダ（ISP）等を含むインターネット媒介者(2)の役割が重要視されるようになっており、媒介者の行為と通信の秘密の関係が論点となる。

本稿では、通信の秘密の概念について、内容・趣旨、ISP等を含む通信事業者(3)の業務との関係等を整理した上で、近年の通信の秘密に関わる議論を紹介する。

Ⅰ　通信の秘密の概要

1　通信の秘密に関する規定

「通信の秘密の不可侵は、近代憲法の原則の一つ」(4)とも言われ、大日本帝国憲法（明治憲法）（第26条）においても、信書の秘密(5)の保障が規定されていた。この規定は、1831年のベルギー憲法、1850年のプロイセン憲法等の諸外国の憲法の影響を受けたものであるとされる(6)。

明治憲法において、「信書の秘密」は、独立の一条をなしていたが、日本国憲法においては、その第21条で、表現の自由の保障（第1項）、検閲の禁止（第2項前段）と並んで、通信の秘密の保障が規定されている。

法律においても、例えば、電気通信事業法第4条第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」と規定し、その実効性を確保するため(7)、同条第2項におい

＊　本稿におけるインターネット資料の最終アクセス日は令和2年6月15日である。

(1)　曽我部真裕「通信の秘密の憲法解釈論」『Nextcom』16号, 2013.Winter, p.14. 本稿では取り上げることのできなかった憲法上の通信の秘密と通信傍受等との関係を含め、近年の議論を紹介し、課題を整理したものとして、以下の論考がある。同「情報法ナビゲーション（第4回）通信の秘密」『法学セミナー』786号, 2020.7, pp.62-68.

(2)　経済協力開発機構（OECD）報告書において、インターネット媒介者（Internet Intermediaries）は、「インターネット上で、第三者間を接続し又は通信を促進する。それらは、第三者によって発信されるコンテンツ、製品及びサービスに対し、アクセスを提供し、ホストし、送信し、若しくはインデックスを行い、又は第三者に対しインターネットサービスを提供する」者と定義され、インターネット・サービス・プロバイダ（ISP）、ホスティングプロバイダ、ソーシャルネットワーキングサービス、検索エンジンなどが含まれるとされている。*The Economic and Social Role of Internet Intermediaries*, OECD, 2010.4, p.9. <https://www.oecd.org/internet/ieconomy/44949023.pdf>

(3)　なお、本稿では、「通信事業者」の語を広義の通信（郵便、電気通信等を含む。）の担い手を指す言葉として用い、電気通信事業法上の電気通信事業者を「電気通信事業者」という。

(4)　佐藤幸治「通信の秘密」芦部信喜編『憲法Ⅱ―人権（1）―』有斐閣, 1978, p.635.

(5)　なお、文言上「信書の秘密」ではあるが、通説においては、開封の書状・葉書、電信電話の秘密を包摂するよう広義に解釈されていた（佐藤　同上, p.640; 美濃部達吉『逐条憲法精義』有斐閣, 昭和2 (1927), p.381.）。

(6)　佐藤　同上, pp.637-638.

(7)　藤田潔・髙部豊彦監修, 髙嶋幹夫『実務電気通信事業法』NTT出版, 2015, p.767.

て、電気通信事業従事者に対し守秘義務を課している[8]。また、通信の秘密の侵害に対しては、罰則も設けられている（同第 179 条）[9]。これらの規定は、日本電信電話株式会社（NTT）として民営化される以前の日本電信電話公社等に対する公衆電気通信法（昭和 28 年法律第 97 号）等の規定から引き継がれたものである。

電気通信事業法のほか、電波法（昭和 25 年法律第 131 号）（第 109 条ほか）、郵便法（昭和 22 年法律第 165 号）（第 8 条ほか。「信書の秘密」の保護）等にも、これに類する規定が置かれている。こうした法律上の通信の秘密と憲法上の通信の秘密の関係については、一般には、①憲法上の規定を受け、これを拡充・確認する意味を持ち、②憲法がもっぱら公権力からの侵害に対応するものであるのに対し、法律上の規定は通信事業者・私人からの侵害を対象に含むと考えられている[10]。また、通信事業者は、憲法の規定について直接の適用を受けるわけではないとしても、電気通信事業者が日常生活に不可欠な電気通信業務を扱うといった性質上、法律の条文の解釈適用にあたって、憲法の趣旨を十分に考慮すべきであるとされる[11]（議論の詳細はⅠ章 4 を参照）。

２　通信の秘密の内容

通信の秘密の対象範囲は、通信の内容にとどまらず、通信の日時、場所、通信当事者の氏名、通信回数等の通信の構成要素（メタデータとも言われる。）を含むものであると解されている[12]。

電気通信事業法における侵害の態様としては、「知得」、「漏えい」、「窃用」が挙げられる[13]。知得とは、第三者が積極的意思を持って知ろうとすることを言い、偶然に知ることはこれに当たらない。漏えいは、知り得た通信の秘密を他者が知りうる状態にすること、窃用は当事者の意思に反して自己又は他人の利益のために用いることをいう。

３　通信の秘密の趣旨

明治憲法において、信書の秘密は独立の一条によって規定され、郵便の国家による独占を前提として、国家に対し、秘密の保持と忠実な業務遂行を要請したものとして、私生活の不可侵

⑻「電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。」（電気通信事業法第 4 条第 2 項）

⑼　電気通信事業者の取扱中の通信の秘密を侵害した者には、2 年以下の懲役又は 100 万円以下の罰金が科せられる（第 179 条第 1 項）。電気通信事業に従事する者の違反に対しては、3 年以下の懲役又は 200 万円以下の罰金である（同条第 2 項）。

⑽　小向太郎『情報法入門　第 4 版』NTT 出版, 2018, p.38; 曽我部真裕「通信の自由と秘密」曽我部真裕ほか『情報法概説　第 2 版』弘文堂, 2019, p.51. なお、公衆電気通信法時代については、独占事業体である公社・会社によるものであって、公益性・国家権力との強い関係を有することなどから、日本電信電話公社等も憲法上の規定の適用を受け、公衆電気通信法等の規定は憲法上の要請に基づくものであるという解釈も存在した（佐藤　前掲注⑷, pp.640-641.）。

⑾　長谷部恭男『憲法　第 7 版』新世社, 2018, p.234. 宍戸常寿東京大学大学院法学政治学研究科教授は、この見解を多くの憲法学者が暗黙裡に採用する立場と評している（宍戸常寿「通信の秘密に関する覚書」長谷部恭男ほか『現代立憲主義の諸相　下』有斐閣, 2013, p.502.）。

⑿　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』情報通信振興会, 2019, p.36. こうした外形的要素も、通信内容を推知させるものとされる。ただし、憲法上の通信の秘密に含まれるかは明確ではないとする指摘もある（高橋和之『立憲主義と日本国憲法　第 4 版』有斐閣, 2017, p.256.）。なお、通信の秘密の範囲をどこまでと捉えるかは、国によって異なるが、明治憲法下においては、当時のドイツ等に範を採りつつ、通信の有無や送受信者の氏名等もその範囲に含めるという解釈がなされていた（田中次郎『通信法釈義』博文館, 明治 34 (1901), pp.46, 399-400; 川村竹治『電信法要義』交通学館, 明治 33 (1900), pp.156-157.）。

⒀　侵害の態様について、以下を参照した。多賀谷監修, 電気通信事業法研究会編著　同上, pp.36-37; 曽我部　前掲注⑽, p.54. 一方、憲法上は積極的知得行為及び漏えい行為を意味するとされる（宍戸　前掲注⑾, pp.496-497.）。

の観点から理解されていた(14)。

一方、日本国憲法における通信の秘密は表現の自由と同一の条文で規定されていること(15)との関係で、その趣旨について議論がある。代表的な学説は、①プライバシー権を主眼とする考え方、②表現の自由の保障の一部をなすとする考え方、③これら両方の側面を同等に持つとする考え方に分類することができる(16)。

憲法上、一般に広く発信することを前提とする「表現」と特定者間にとどまる「通信」は区別されており(17)、通信の秘密の趣旨は後者の保護にあることから、プライバシー権の一環と見ることができるというのが①説の立場である。この立場からは、通信のメタデータはその保護の対象となることが当然視される(18)一方で、通信の秘密の趣旨を専ら表現の自由に求めた場合、通信の秘密の保護の範囲が狭小化されてしまう可能性があるとの観点で批判される(19)。例えば、発信先や回数といった通信の構成要素の秘密保護の必要性を、内容が推知されてしまうことのみに求めるとすれば、掲示板への投稿等のいわゆる「公然性を有する通信」については、保護の対象外とすることも考えられる(20)。

一方で、通信の秘密が憲法第21条に組み込まれている以上、表現の自由の一環として見るべきだという②説も有力である(21)。また、プライバシー保護の観点から通信の秘密を基礎付けようとする場合には、一般的にプライバシー保護の対象とは考えられていない法人にも通信の秘密が認められていることとの関係も問題となる(22)。

こうした議論を踏まえ、憲法上の通信の秘密の趣旨は、表現の自由の保障としての意味を認めつつ、プライバシー保護の趣旨を重視する見解が有力とされている(23)。

---

⑭ 齊藤雅俊「憲法21条の「通信の秘密」について」『東海法科大学院論集』3号, 2012.3, pp.116-119. それゆえに、「信書の秘密」の範囲は封書に限定されないとされた（美濃部　前掲注⑤, pp.380-381.）。

⑮ 表現の自由と通信の秘密を同一の条で規定するのは、比較憲法上稀であるとされる。諸外国で、通信の秘密がプライバシー保護の一環として規定されていることは、通信の秘密の趣旨をプライバシー保護と考える論拠の一つとなっている（佐藤　前掲注④, pp.635-636.）。もっとも、明治憲法が参照した当時の欧州諸国における、通信（信書）の秘密は、精神活動の自由（コミュニケーションの権利）と密接な関係を有していたと主張されている（齊藤　同上, pp.120-123.）。

⑯ 海野敦史『「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, 2015, p.38. もっとも、多くの学説においては、通信の秘密は表現の自由とプライバシーの両方に関係することを少なからず認めており、実質的な違いは大きくないと見ることもできる（同, p.74; 芦部信喜『憲法学Ⅲ―人権各論（1）―増補版』有斐閣, 2000, pp.541-543.）。なお、憲法制定経緯の調査を通じ、通信の秘密の趣旨を米国のコモンローにおける「意思伝達のプライバシー」と捉え、保障の範囲を通信内容の保護とする論文及びこれに対する批判として以下の論考がある。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, 2006, pp.67-70; 宍戸　前掲注⑪, pp.494-495, 509.

⑰ 他方、インターネットを通じた情報の流通は、通信技術を用いて不特定多数に伝達を行う（公然性を有する通信）こともあり、その性格も議論されている（後掲注⑳の記述も参照）（曽我部　前掲注⑩, pp.48-50.）。

⑱ 佐藤　前掲注④, p.641.

⑲ 専ら通信の内容だけがその対象となる（メタデータが保護されない）あるいは、萎縮効果の点から議論するにとどまらざるを得ず公権力からの保護を弱めかねない（同上, p.635; 宍戸　前掲注⑪, p.500.）

⑳ 「電気通信サービスにおける情報流通ルールに関する研究会報告書」1998.1.5. 総務省ウェブサイト <https://www.soumu.go.jp/main_sosiki/joho_tsusin/pressrelease/japanese/denki/980105j601.html>; 高橋和之「第2章　インターネット上の名誉毀損と表現の自由」松井茂記ほか編著『インターネットと法　第4版』有斐閣, 2010, p.83. ただし、プライバシー保護を主眼とする説においても、表現と通信の峻別が重視されるため、「公然性を有する通信」は憲法上の通信に当たらない又はその保護が限定されるという立場が有力である（佐藤幸治『日本国憲法論』成文堂, 2011, p.321; 宍戸常寿「第10章　表現の自由」渡辺康行ほか『憲法Ⅰ―基本権―』日本評論社, 2016, p.257.）。こうした見解に否定的なものとして以下の論考がある。松井茂記『インターネットの憲法学　新版』岩波書店, 2014, pp.382-383, 408.

㉑ 阪本昌成『憲法理論　3』成文堂, 1995, p.140.

㉒ 多賀谷監修, 電気通信事業法研究会編著　前掲注⑫, p.35.

㉓ 宍戸　前掲注⑪, p.508; 鈴木秀美「通信の秘密」大石眞・石川健治編『憲法の争点』（ジュリスト増刊）有斐閣, 2008, p.136.

４　通信の自由と憲法・法律の関係に関する議論

郵便や電話の時代から積み重ねられた議論によって、通信の秘密の保護の範囲、趣旨等の核心的な部分については一定の合意が形成されているものの、通信の自由化（民営化）、インターネットの発展や機器間通信の増加といった通信の今日的状況を踏まえると(24)、通信の秘密の「外延」にはなお論点が残されているとされる(25)。代表的な論点として、「通信の自由」の保障の有無やこれに関連した憲法上の要請（法律上の規定の関係）が挙げられる。

通信の秘密を、表現の自由の一環として見る学説の中には、表現の自由の下位分類としての「通信の自由」を通信の秘密の論理的前提（保障内容の一部）であると主張し、コモン・キャリア（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付けられている業者）を法定することを憲法が要請しているとするものもある(26)。こうした立場からは、法律上の通信の秘密や取扱いの不当な拒否の禁止等を含む通信法制のあり方を憲法上の要請として理解することができる(27)。

また、通信の秘密の趣旨をプライバシー保護と理解する立場からも、論理的前提としての通信の自由の保障が主張されるようになっている。佐藤幸治京都大学名誉教授は、通信の自由を「非公開でコミュニケーションを行う自由」として理解し、通信の自由をプライバシー権の保護の一環としての通信の秘密の前提とした上で、「通信業務提供者から公正な通信業務の提供を受けることができること」も通信の秘密の意味内容に含まれると主張している(28)。

このように憲法が「通信の自由」を保障し、一定の作為義務を課しているという見解を採る場合には、憲法上の「通信」や憲法が要請する「通信制度」の範囲の画定が求められることになる(29)。一方で、あくまでも通信の秘密は国家の不作為義務を定めたもので、各種の法律や民間事業者の義務は、憲法の趣旨や通信の性質を踏まえた立法政策によるものと位置付けるべきだとの考え方もある(30)。

Ⅱ　通信の秘密と電気通信事業者

通信の秘密は、悪意を持った情報の漏えい(31)といった特別な場面でのみ問題になるわけではなく、日常的な業務の実施との関係でも解釈が積み重ねられてきた。以下では、現在の議論の

⑵④　通信の現状を踏まえた学説の批判的検討として以下を参照。海野　前掲注⑴⑥, pp.38-41.

⑵⑤　曽我部「通信の秘密の憲法解釈論」前掲注⑴, pp.15-16; 宍戸常寿「通信の秘密について」『企業と法創造』9(3), 2013.2, p.18. <http://www.win-cls.sakura.ne.jp/pdf/35/02.pdf>

⑵⑥　阪本昌成「第四章　「通信の自由・通信の秘密」への新たな視点」『プライヴァシー権論』日本評論社, 1986, pp.229-244.

⑵⑦　同上

⑵⑧　佐藤　前掲注⑵⓪, pp.321-322. なお、佐藤名誉教授の立場の変化を指摘するものとして、曽我部「通信の秘密の憲法解釈論」前掲注⑴, p.22.

⑵⑨　宍戸　前掲注⑴⑪, pp.501, 503.

⑶⓪　曽我部「通信の秘密の憲法解釈論」前掲注⑴, p.19. その理由として、一般に日本の憲法学においては、憲法上の自由権から国家の作為義務を導くことには慎重であることが挙げられている。ほかに、憲法が立法を要請していることに否定的なものとして、以下の著作がある。松井茂記『日本国憲法　第３版』有斐閣, 2007, pp.515-516; 渋谷秀樹『憲法』有斐閣, 2007, p.373.

⑶①　公衆電気通信法時代の事例として、電話交換手が職務上知り得た通話内容を美容院で話したことで懲戒免職となった事件（「福知山電報電話局」事件）がある（藤田・髙部監修, 髙嶋　前掲注⑺, pp.778, 780; 林紘一郎「第５章　サイバーセキュリティと通信の秘密」土屋大洋監修『仮想戦争の終わり―サイバー戦争とセキュリティ―』KADOKAWA, 2014, p.185.）。

前提として、電気通信事業法上の規定と電気通信事業者を含む電気通信事業を営む者[32]の業務との関係を示す。

1　日常業務との関係

日本では、一般に、電気通信事業者における通信の秘密の取扱いに関しては、極めて慎重な検討が行われており、知得目的の正当性等を厳格に吟味し、第三者に開示する際には厳格な手続を要求する傾向がある[33]。電気通信事業者が行う業務上の行為についても、形式上通信の秘密侵害の構成要件を満たすとした上で、刑法（明治 40 年法律第 45 号）上、違法性が阻却されるか（利用者の個別の同意があるか[34]、正当行為、正当防衛、緊急避難等に当たるか）を検討するというアプローチが採られている[35]。

例えば、日本電信電話公社時代には、料金明細データの取得に対しても極めて慎重な態度が採られており、記録開始に先立ち通話先電話番号を取得することの可否や記録の詳細さを個別の利用者に選択させる方式が採られている[36]。このほかにも、例えば、通話時間帯等に基づく料金プランのための記録などにも、通信の秘密に係る検討を要したという[37]。

2　違法性阻却事由と関連ガイドライン等

通信の秘密は、様々な領域に及び得るものである。個別のサービス・対応における違法性阻却事由の要件の充足等に関する解釈については、政府有識者会議の報告書類やガイドラインに示されている。

(1) 正当行為

刑法第 35 条は、「法令又は正当な業務による行為は、罰しない」として正当行為という違法性阻却事由を規定している。正当行為は、法令に基づく行為（法令行為）と正当業務行為に分けることができる[38]。法令行為については、刑事訴訟法（昭和 23 年法律 131 号）、「犯罪捜査のための通信傍受に関する法律」（平成 11 年法律第 137 号。「通信傍受法」）に基づく押収、通信傍受などが挙げられる。後者の正当業務行為として認められる基準としては、「国民の社会・経済・文化的インフラである通信役務の特色を踏まえ、個別の契約に基づく役務提供義務の履行

---

[32] 電気通信事業法は、電気通信事業者（電気通信事業を営むことについて、第 9 条の登録を受けた者及び第 16 条第 1 項の規定による届出をした者）（同法第 2 条第 1 項第 5 号）を主たる規律の対象としており、一定の要件を満たす電気通信事業について適用を除外している（同第 164 条第 1 項）が、通信の秘密の規定は、除外の例外となっており、「電気通信事業を営む者の取扱中に係る通信」について適用される（同第 3 項）。なお、電気通信事業の分類と適用関係については以下も参照。総務省「電気通信事業参入マニュアル　追補版」（平成 17 年 8 月 18 日策定（令和元年 10 月 1 日最終改定））<https://www.soumu.go.jp/main_content/000477428.pdf>

[33] 藤田・髙部監修, 髙嶋　前掲注(7), p.778.

[34] 同意については、「真意」と評価できるものであること（「個別」かつ「明確な」同意）が必要とされる（宍戸　前掲注(11), p.513.）。もっとも、通信の秘密侵害罪は、電気通信事業の公共性等の社会的な利益も保護法益としており、同意があることで直ちに違法性が阻却されるわけではないという見方もある（石井徹哉「第 373 号コラム「通信の秘密侵害罪における正当業務行為について」」2015.8.3. デジタル・フォレンジック研究会ウェブサイト <https://digitalforensic.jp/2015/08/03/column373/>）。

[35] 「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 4 月 18 日総務省告示第 152 号）第 5 条第 4 項 <http://www.soumu.go.jp/main_content/000507466.pdf>; 多賀谷監修, 電気通信事業法研究会編著　前掲注(12), pp.36-37; 曽我部　前掲注(10), p.56.

[36] 藤田・髙部監修, 髙嶋　前掲注(7), p.783.

[37] 同上, p.785.

[38] 山口厚『刑法総論　第 3 版』有斐閣, 2016, p.111.

のみならず、いつでも誰でも自由に通信を利用できる環境を確保するという観点に立ち、利用者である国民全体にとっての通信役務の円滑な提供という見地から正当・必要と考えられる措置」がその範疇に入ると考えられている(39)。例えば、自己のネットワークの正常な運用のために、通信を制御することなどが挙げられる。その一例として、「帯域制御の運用基準に関するガイドライン」(40)（以下「帯域制御ガイドライン」という。）では、特定のソフト(41)の通信が、一定のネットワーク帯域(42)を占有し、他の利用者の利用に通信の遅延等の影響が生じている場合に、通信量が特に多いソフトに限定して、必要な限度で、使用できる回線容量や通信速度等に基準を設けネットワーク上の通信量を制御すること（帯域制御）は、正当業務行為に該当する可能性が高い等と整理している(43)。

(2) 正当防衛

刑法第 36 条第 1 項は、「急迫不正の侵害に対して、自己又は他人の権利を防衛するため、やむを得ずにした行為は、罰しない」として正当防衛という違法性阻却事由を規定している。正当防衛の要件として、①急迫不正の侵害、②自己又は他人の権利の防衛、③防衛行為（防衛の意思等）、④やむを得ずにした行為であること（防衛行為の必要性・相当性）が挙げられる(44)。次の緊急避難と異なり、正対不正の関係であるために、補充性等の要件は求められない。すなわち、緊急避難の要件とされる補充性が、やむを得ずにする行為であること（ほかに有効な手段がないこと）を求めるのに対し、正当防衛については、必要性・（反撃行為の侵害に対する）相当性から判断される(45)。ただし、防衛は侵害者に向けられたものである必要がある。正当防衛に当たると整理している例として、サイバー攻撃等について扱った「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」(46)（以下「サイバー攻撃等ガイドライン」という。）がある。例えば、サイバー攻撃等が発生した場合に、当該通信の特性を把握し、これに基づき特定の通信を遮断する行為は、通信の秘密の侵害に当たり得る(47)。しかし、事業者設備に生じる侵害を防止するためにこれを行う場合には、正当防衛（又は緊急避難）として、違法性が阻却されると考えられるという。

---

(39) 「法的問題検討サブワーキング報告書」2010.3.30, pp.8-9. 安心ネットづくり促進協議会ウェブサイト <https://www.good-net.jp/files/original/20171101221901808 3684.pdf>

(40) 帯域制御の運用基準に関するガイドライン検討協議会ほか「帯域制御の運用基準に関するガイドライン（改定）」（令和元年 12 月最終改定）<https://www.jaipa.or.jp/other/bandwidth/1912_guidelines.pdf>

(41) ガイドラインでは、P2P ファイル交換ソフトについて検討している。P2P（Peer to Peer）とは、情報等を要求する側と要求を受けて提供する側が分かれているクライアント―サーバ形式とは異なり、対等のもの同士で通信を行う仕組みをいう。匿名の利用者間で動画等のやり取りをするファイル交換ソフトによるネットワーク帯域の占有が問題となっていた。

(42) 帯域とはもともとデータ転送に用いられる周波数の幅を言うが、そこから転じて、比喩的に単位時間当たり通信量を指す言葉としても使われる。例えば、高速通信が可能な回線を、ブロードバンド（帯域幅が広い）などという。「帯域幅の概要」2014.3.5. KDDI ウェブサイト <https://www.kddi.com/yogo/%E9%80%9A%E4%BF%A1%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9/%E5%B8%AF%E5%9F%9F%E5%B9%85.html>

(43) 帯域制御の運用基準に関するガイドライン検討協議会ほか　前掲注(40), p.9.

(44) 山口　前掲注(38), pp.119-139.

(45) 同上, pp.134-139, 153.

(46) インターネットの安定的運用に関する協議会「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン　第 5 版」2018.11.30. <https://www.jaipa.or.jp/other/intuse/guideline_v5.pdf> なお、同ガイドラインは、日本インターネットプロバイダー協会等の事業者 4 団体による「インターネットの安定的運用に関する協議会」で検討し、平成 19 年に第 1 版（当初題名は「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」）が制定された。その後、総務省での検討結果等を受けつつ、改版が加えられている。

(47) 同上, p.11.

(3) 緊急避難

刑法第37条第1項は、「自己又は他人の生命、身体、自由又は財産に対する現在の危難を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない」として、緊急避難という違法性阻却事由を規定している。緊急避難に当たるためには、①現在の危難の存在、②補充性、③法益の均衡の要件を満たしている必要がある。このうち、「現在の危難」は、法益の侵害に対する差し迫った現実の危険の存在、「法益の均衡」は避難行為によって生じる害が避けようとした害を超えないことをいう(48)。緊急避難として整理している事例として挙げられるのが、インターネット上の自殺予告(49)に関するガイドライン(50)である。同ガイドラインでは、インターネット上の掲示板における自殺予告等について、警察から照会があった場合に、発信者情報を開示することにつき、緊急避難としての要件を満たす条件を整理している。

このほか、緊急避難に当たると整理された重要な例として、電気通信事業者の自主的取組としての児童ポルノサイトのブロッキングが挙げられる。これについては、Ⅲ章1で詳述する。

3　ウェブサイト等へのアクセスの仕組みと通信の秘密

次章では、特にインターネットと通信の秘密に関係した議論を紹介するため、その前提として、ウェブサイト等へのアクセスの仕組みを概観する。

(1) ウェブサイト等へのアクセスの仕組み

インターネット上の各端末には、IPアドレスといわれる番号（例：192.168.7.21）が付されており、情報の送受信はこの情報を用いて行われる。しかし、こうした番号を一つ一つ記憶することは困難であるため、一般には、ドメイン名（例：ndl.go.jp）が用いられる。ドメイン名は、IPアドレスと対応しており、その対応付けを保持・検索するシステムがDNSである(51)。ウェブサイトの閲覧ソフトに、アクセス先のURL(52)を入力すると、DNSサーバにアクセスし、これに対応するIPアドレスを得て、改めて、当該IPアドレスに向けた通信を行う。データは、パケットと呼ばれる小さな単位に分割され、送受信される。このパケット方式により、1本の回線で同時に多数の通信が可能となる。他方、1本の回線を共用するため、通信品質（速度等）は必ずしも保障されないベストエフォート型のサービスとなる(53)。

---

(48)「法的問題検討サブワーキング報告書」前掲注(39), p.14.

(49) なお、通信を通じた自殺予告をどのように扱うかは、電報の時代から問題になっていた。昭和28年、心中の前にそれを予告する電報を打っていた事件があり、電報局が通報しなかったことに対して批判が寄せられた。例えば、名古屋大学の柏木千秋教授（当時）は正当行為又は緊急避難に当たるとして、通報すべきだったとコメントしている。染谷義一「通信の秘密に関する一考察」『電気通信業務研究』45号, 1953.10, pp.56-64.

(50) 電気通信事業者協会ほか「インターネット上の自殺予告事案への対応に関するガイドライン」2005.10. <https://www.telesa.or.jp/wp-content/uploads/consortium/suicide/pdf/guideline_suicide_051005.pdf>

(51) Domain Name Systemの略。「ドメイン名ってなに？」JPRSウェブサイト <https://jprs.jp/related-info/about/address/>; 「DNSとは」日本ネットワークインフォメーションセンターウェブサイト <https://www.nic.ad.jp/ja/basics/beginners/dns.html>

(52) Uniform Resource Locatorの略。通信方式（プロトコル。例：http）、ドメイン名、ファイル名等をまとめて表す文字列のこと（例：https://www.ndl.go.jp/jp/diet/index.html）をいう。「URL（ユーアールエル）」JPRSウェブサイト <https://jprs.jp/glossary/index.php?ID=0061>

(53) 大和哲「ケータイ用語の基礎知識　第289回：ベストエフォートとは」『ケータイWatch』2006.9.12. <https://k-tai.watch.impress.co.jp/cda/article/keyword/30985.html>

⑵ ブロッキングと通信の秘密

ウェブサイト等へのアクセスとの関係で通信の秘密が問題となる典型的な例として、ブロッキングが挙げられる。ブロッキングとは、違法又は有害な情報が蔵置されているサーバにおいて情報が「削除」されない場合等に、インターネットへのアクセスを提供するISP等が、当該情報への接続を遮断することをいう(54)。ブロッキングの手法には、いくつかあるが(55)、日本では、DNSブロッキングと呼ばれる手法が限定的に採用されている。

DNSブロッキングは、ドメイン名に対するIPアドレスの応答において、偽のIPアドレスを返すことで特定のウェブサイトにアクセスさせないようにする手法である。ISP単位で管理するDNSサーバにおいて処置することが可能である(56)。他の手法と比べれば、安価に導入できる一方、あるドメイン名に対するアクセス全体を停止することになるため、過剰な遮断（オーバーブロッキング）が生じる(57)。

すなわち、DNSブロッキングは、利用者のアクセスするドメインをいったん全て機械的に確認した上で、該当サイトにアクセスする通信を選別するものであり、取得した通信データを本来の目的とは異なる目的で用いるため、通信の秘密の侵害（知得、窃用）に当たると考えられている(58)。

Ⅲ　通信の秘密をめぐる近年の議論

通信の秘密は、インターネット通信を含む、電気通信の様々な局面で関係し、これまでにも、各種の課題に応じて、その適用関係について検討が行われてきた。近年でも、いくつかの事例において、通信の秘密を主要な論点とする議論が生じた。以下では、これらを紹介することを通じて、通信の秘密の現代における評価を検討する。

⑸4 森亮二「ブロッキングに関する法律問題」『ジュリスト』1411号, 2010.11.15, pp.7-8. なお、同様に接続を防ぐ手法に「フィルタリング」がある。ブロッキングとフィルタリングの主な違いは利用者の意思の有無（フィルタリングは利用者の選択によるが、ブロッキングは強制的手段）にあると説明される（「法的問題検討サブワーキング報告書」前掲注⑶9, p.4.）。なお、諸外国では用法が異なる場合があるので留意する必要がある。

⑸5 例えば、IPアドレス単位でブロッキングする手法やURL単位でブロッキングする手法がある。前者については、あるIPアドレスを持つサーバには複数のドメイン名が共存しており、オーバーブロッキングが生じること、後者については分割されたパケットを収集して内容を確認する必要があり、機器導入にかかる費用負担が大きいことなどが指摘される。児童ポルノ流通防止協議会「ブロッキングに関する報告書」2010.3, pp.14-16. インターネット協会ウェブサイト <https://www.iajapan.org/press/pdf/siryou5-20100325.pdf>; 上原哲太郎「技術に詳しくない方でも分かる?!ブロッキングの技術的課題」（著作権侵害サイトのブロッキング要請に関する緊急提言シンポジウム　資料）2018.4.22. 情報法制研究所ウェブサイト <https://jilis.org/events/data/20180422jilis-blocking-uehara.pdf>

⑸6 他方、他のDNSサーバを利用するように利用者側で設定することで回避も可能である（立石聡明「防弾ホスティング・CDN・ブロッキング―仕組みと諸課題について―」『法とコンピュータ』37号, 2019.7, p.32.）。

⑸7 児童ポルノ流通防止協議会　前掲注⑸5, p.13.

⑸8 「法的問題検討サブワーキング報告書」前掲注⑶9, pp.4-6. なお、DNSサーバへの問合せについて、通信当事者は電気通信事業者であると見ることができることや知得・窃用が他人の通信を媒介する目的から逸脱したものと言えないことから、通信の秘密の侵害に当たらない（又は宛先情報のみが窃用されており侵害は軽微である）とする主張もある（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, 2018.10, pp.32-36.）。これに対しては、アクセス先が通信の秘密の保護対象に当たることに疑いがないのにこれを除外するのは不合理である、インターネットにおいては宛先情報は内容と直結する情報であるといった点から批判がある（一般財団法人情報法制研究所情報通信法制研究タスクフォース「著作権侵害サイトのブロッキング要請に関する緊急提言」2018.4.11, p.5. <https://jilis.org/proposal/data/2018-04-11.pdf>; 成原慧「海賊版サイトのブロッキングを巡る法的問題」『法学教室』453号, 2018.6, p.48; 小倉秀夫ほか「ブロッキングをめぐる解釈論と立法論」『法とコンピュータ』37号, 2019.7, pp.58-59.）。ほかのブロッキング手法についても、通信の秘密を侵害すると考えられている。

1　児童ポルノブロッキング

(1) 児童ポルノブロッキングの経緯

平成 11 年に「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」[59]（平成 11 年法律第 52 号。「児童ポルノ禁止法」）が制定された。児童ポルノに関する統計が取り始められた平成 12 年以降、平成 16 年ごろまで児童ポルノの検挙件数は、年間 170 件程度で推移していたが、その後、インターネットによる不特定多数への提供を中心に件数が急増していった（平成 18 年で 616 件、平成 22 年には 1,342 件に達した。）[60]。こうした状況を受けて、警察庁や一般財団法人インターネット協会、加盟企業において、対策の一つとして、児童ポルノサイトのブロッキングが検討されるようになった[61]。

警察庁の総合セキュリティ対策会議は、平成 20 年度の報告書において、ブロッキングの実施に向けた検討が必要であるとして、「児童ポルノ掲載アドレスリスト作成管理団体」[62]やブロッキングの実施に向けた検討等を行う会議体の設置等を提言した[63]。その後、「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 年法律第 79 号。「青少年ネット環境整備法」）の成立を受けて事業者を中心として設立された「安心ネットづくり促進協議会」及び一般財団法人インターネット協会が事務局となった「児童ポルノ流通防止協議会」（オブザーバーとして警察庁、総務省等）が中心となって検討が進められた。各種報告書・ガイドラインの作成・公表を経て、平成 23 年 3 月、児童ポルノ流通防止対策専門委員会[64]が、一般社団法人インターネットコンテンツセーフティ協会を「児童ポルノ掲載アドレスリスト作成管理団体」に選定し、同年 4 月から児童ポルノブロッキングが開始された[65]。

(2) ブロッキングと通信の秘密

上述のとおり、DNS ブロッキングは、通信の秘密の侵害に当たると考えられるため、違法性が阻却されるかが問題となる。結論として、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グループ）報告書において、児童ポルノブロッキングは緊急避難に当たると整理された[66]。現在の危難の要件は、「当該児童の心身とその健全な成長への重大な影響が生ずるとともに、本来性欲の対象とされるべきでない段階で自己の意思に反して性欲の対象にされた性的虐待画像が公開されることにより特に保護を要する人格的利益に対

59　平成 26 年法律第 79 号による改正で、現行の名称は「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」

60　「【児童ポルノ事件】検挙件数の推移」警察庁ウェブサイト <https://www.npa.go.jp/safetylife/syonen/no_cp/newsrelease/2017_statistics_data.pdf>;「3　ネットワーク利用犯罪への対策」警察庁『警察白書　平成 23 年』2011, p.39. <https://www.npa.go.jp/hakusyo/h23/honbun/pdf/06tokushu2.pdf>

61　「児童ポルノ事件　最多」『朝日新聞』2010.2.18, 夕刊.

62　児童ポルノ該当性の判断、リストの維持・管理等について、透明性と客観性を確保しつつ、警察等が把握した情報に基づき、児童ポルノ掲載アドレス等のリストを作成し、流通防止対策を行う事業者に提供を行うとともに、掲載されている児童ポルノに係る情報について検証を行う団体をいう。

63　総合セキュリティ対策会議「インターネット上での児童ポルノの流通に関する問題とその対策について」（平成 20 年度総合セキュリティ対策会議報告書）2009.3. 警察庁ウェブサイト <https://www.npa.go.jp/cyber/csmeeting/h20/pdf/pdf20.pdf>

64　児童ポルノ流通防止協議会から構成員が移行して、平成 22 年に発足した。

65　ブロッキングに至るまでの経緯については、以下の資料を参照した。「児童ポルノ対策の取り組みの経緯　3. 民間での検討」安心ネットづくり促進協議会ウェブサイト <https://www.good-net.jp/blocking/prehistory/prehistory_3>

66　以下の整理について次の文献を参照した。「法的問題検討サブワーキング報告書」前掲注(39), pp.8-21; 森　前掲注(54), pp.8-11.

する侵害が生じている」等として認められた。また、検挙及び削除といった手段に容易性・実効性がない場合、例えば、サーバが海外にあり管理者が不明であって削除等の実効性がない場合には、補充性の要件が認められるとした。また、法益権衡の要件については、児童ポルノによって侵害される権利侵害の深刻さから認められる可能性が高いとしつつ、児童ポルノ禁止法により定められる児童ポルノの外延が明確でない（例えば、家族写真のようなものも含まれ得る[67]）ことから、定義上の児童ポルノではなく、重大な権利侵害が生じているものに限定するべきとされた。

２　海賊版サイトブロッキング

運営管理者の特定が困難で、侵害コンテンツの削除要請も難しい大規模な海賊版サイト（「漫画村」等）が開設され、出版業界等が経済的に大きな被害を受けるなど[68]、インターネット上における漫画、アニメ、映画等コンテンツの海賊版サイトが大きな問題となっており、政府知的財産戦略本部・犯罪対策閣僚会議は、平成 30 年 4 月 13 日に「インターネット上の海賊版サイトに対する緊急対策」等を決定した[69]。この中で、民間事業者による自主的な取組として、「漫画村」等の特定の 3 サイトに限定してブロッキングを行うことが適当であるとの見解が示された[70]。ブロッキングは、上述のとおり、通信の秘密の侵害に当たるが、緊急避難の要件を満たせば、違法性が阻却されるとする[71]。また、同時にブロッキングに関する法制度整備等の検討のため、知的財産戦略本部の下に関係事業者、有識者による検討体を設置するものとされた。

これに先立つ報道では、政府が ISP に対し海賊版サイトへの遮断を要請すると報じられていたこと[72]もあり、研究者らによって構成される情報法制研究所のタスクフォースや事業者団体などが、慎重な対応を求める意見書を公表していた[73]。ここでは、後述する緊急避難要件の充足に関する疑問のほか、法治国家原理からの逸脱の観点等からも批判された[74]。すなわち、重要な権利の制約に当たる行為をプロバイダに事実上義務付けるものであり、法令による慎重な制度設計がなされるべきであるにもかかわらず、緊急性を理由に法律という形式を潜脱することの問題である。また、政府による緊急対策の公表後、3 サイトのブロッキングを行うことを

⑹ 児童ポルノ禁止法第 2 条第 3 項の定義のうち、第 3 号「衣服の全部又は一部を着けない児童の姿態であって性欲を興奮させ又は刺激するものを視覚により認識することができる方法により描写したもの」について、家族写真でも入り得るという指摘があった（「法的問題検討サブワーキング報告書」同上, p.19.）。

⑹ 金額には疑義が呈されることもあるが、漫画村で約 3000 億円の被害があったと試算されている（知的財産戦略本部・犯罪対策閣僚会議「インターネット上の海賊版サイトに対する緊急対策」2018.4, pp.1, 4. <https://www.kantei.go.jp/jp/singi/titeki2/kettei/honpen.pdf>）。

⑹ 知的財産戦略本部・犯罪対策閣僚会議「インターネット上の海賊版対策に関する進め方について」2018.4.13. <https://www.kantei.go.jp/jp/singi/titeki2/kettei/susumekata.pdf>; 同上

⑺ 知的財産戦略本部・犯罪対策閣僚会議　前掲注⑹, p.2.

⑺ 同上, pp.1-2. なお、要件を満たす場合には緊急避難となり違法性が阻却されるというだけで、具体的に 3 サイトについて、緊急避難が成立するとはされていないことも指摘されている（宍戸常寿東京大学大学院法学政治学研究科教授の発言）（「【緊急開催】著作権侵害サイトのブロッキング要請に関する緊急提言シンポジウム」2018.4.22. 情報法制研究所ウェブサイト <https://jilis.org/proposal/data/2018-04-22.pdf>）。

⑺ 「海賊版サイト：政府、遮断要請へ　著作保護に「緊急避難」」『毎日新聞』2018.4.6.

⑺ 一般財団法人情報法制研究所情報通信法制研究タスクフォース　前掲注⑸

⑺ 同上, pp.2-4. ほかに、プロバイダに対し運用面の費用・訴訟リスク等の不合理な負担が生ずるといった点も指摘された。

表明した日本電信電話（NTT）グループ(75)に対しては、消費者団体による抗議等が行われた(76)。

(1) 緊急避難としてのブロッキング

主に電気通信事業法上の通信の秘密との関係で示された政府の「緊急避難」論に対しては、以下のような点からその要件を満たしていないのではないかという指摘がなされた(77)。まず、補充性については、他の手段（削除要請、広告出稿停止、海賊版サイトに対する訴訟）が尽くされているかどうかが必ずしも明らかではない(78)。特に、海外サーバに置かれたサイトに対する訴訟が困難であるとされていたところ、米国の制度を用いて発信者情報が開示された例があったこと(79)も、他の手段が尽くされていないことをうかがわせる事情となった。また、法益権衡についても、通信の秘密と、財産権である著作権（最終的には損害賠償による補填も可能である）を比較した場合に、後者が優越すると言えるかは疑わしいとされた(80)。

(2) ブロッキングの法制化

ブロッキングを法制化する場合には、憲法上の通信の秘密との関係が問題となる(81)。知的財産戦略本部の下に設置された、インターネット上の海賊版対策に関する検討会議において、ブロッキングに関する制度整備が議論されたが、委員間で意見が激しく対立し、中間とりまとめをまとめないという異例の事態に発展した(82)。

ブロッキングの法制化を求める立場からは、①被害が甚大であること、②諸外国においてもブロッキングの法制化が行われていること、③その他の手法によって対応できないサイトが存在していること、④国外からの権利侵害に対して国内の法制度によって対応できるようにする必要があることなどが主張された(83)。一方、ブロッキングの法制化が合憲と言えるのは、①具

---

(75) 日本電信電話株式会社ほか「インターネット上の海賊版サイトに対するブロッキングの実施について」2018.4.23. <https://www.ntt.co.jp/news2018/1804/180423a.html>

(76) 主婦連合会・全国地域婦人団体連絡協議会「NTT グループ「インターネット上の海賊版サイトに対するブロッキングの実施について」に対する意見書」2018.4.25. <http://www.chifuren.gr.jp/180425opinion2.pdf>

(77) 亀井源太郎「刑事法研究者から見た海賊版サイト対策を巡る動き」『Law and Technology』87 号, 2020.4, p.72.

(78) 成原　前掲注(58), pp.47-48; 一般財団法人情報法制研究所情報通信法制研究タスクフォース　前掲注(58), pp.2-3.

(79) 運営管理者の特定が困難であるとされていた「漫画村」について、相手方氏名不詳のまま、米国で訴訟を提起し、訴訟手続の中で開示を受けた。山口貴士「意見書（ディスカバリー制度を利用した海賊版サイト運営者の特定について）」（知的財産戦略本部検証・評価・企画委員会インターネット上の海賊版対策に関する検討会議（タスクフォース）（第 9 回）資料 5-2）2018.10.15. 首相官邸ウェブサイト <https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/kaizoku/dai9/siryou5-2.pdf>;「海賊版サイト「漫画村」の運営者を特定か　法的措置へ」『BuzzFeed News』2018.10.10. <https://www.buzzfeed.com/jp/takumiharimaya/manga-mura>

(80) なお、児童ポルノブロッキングの際の議論においては、著作権侵害には妥当しないと整理されていた（「法的問題検討サブワーキング報告書」前掲注(39), pp.20-21.）。

(81) 曽我部真裕京都大学大学院教授は、憲法上の通信の秘密の侵害としては程度が高くないとしても、表現の自由（インターネットユーザーの知る権利）等の観点から慎重に検討されるべきであることを指摘している。なお、ブロッキングの法制化に当たっては、財産権の保障（憲法第 29 条第 3 項）等の他の憲法上の問題や、詳細な制度設計に係る論点があるが、本稿では触れない。曽我部真裕「オープンな場で筋の通った検討を―ブロッキングの法的な問題点―」『新聞研究』804 号, 2018.7, p.51.

(82) 「ブロッキング法制化で大激論、異例の取りまとめ断念」『日本経済新聞（日経 xTech）』2018.10.16. <https://www.nikkei.com/article/DGXMZO36529840W8A011C1000000/>

(83) 林いづみ「憲法適合的な法制度とするための具体的な検討をすみやかに進めるべき」（知的財産戦略本部検証・評価・企画委員会インターネット上の海賊版対策に関する検討会議（タスクフォース）（第 8 回）資料 2）2018.9.19. 首相官邸ウェブサイト <https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/kaizoku/dai8/siryou2.pdf>; 一般社団法人コンテンツ海外流通促進機構ほか「ブロッキングの法制化を求める意見書」（知的財産戦略本部検証・評価・企画委員会インターネット上の海賊版対策に関する検討会議（タスクフォース）（第 9 回）資料 2-1）2018.10.10. 同 <https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/kaizoku/dai9/siryou2-1.pdf>

体的・実質的な立法事実に裏付けられ、②重要な公共的利益の達成を目的として、③目的達成手段が実質的に合理的な関連性を有し、④事実上、他に実効的な手段が存在しないか著しく困難な場合に限られるという点は争いのないところであるが、ブロッキングの法制化に慎重な立場からは、①について被害実態や諸外国での導入状況に疑念があること、④について他に実効的な手段がないとは言えないことなどを理由として、合憲性に疑念が呈された(84)。また、著作権侵害に関してブロッキングを認めることによる、ほかにブロッキングが主張されている権利侵害（例えば名誉毀損）等への拡大等の影響等も論点となった(85)。

3　発信者情報の開示

インターネット上のコンテンツによって、権利を侵害された者が、当該コンテンツの発信者に対して、民事上の損害賠償請求等を行うためには、発信者を特定する必要がある。しかし、インターネット上のコンテンツについては､発信者が必ずしも明らかにされていない(匿名性)。そこで、発信者に関する情報を有するプロバイダ等に対して、情報の開示が求められることになる。一方で、匿名による表現について、発信者に関する情報は、憲法上の表現の自由や通信の秘密の保障が及ぶと考えられ(86)、許可なくこれを開示することは外形的には通信の秘密の侵害に当たる(87)。平成 13 年に成立した「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（平成 13 年法律第 137 号。「プロバイダ責任制限法」）(88)では、①権利侵害が明らかであり、②開示を受けるべき正当な理由があるという要件を満たした場合には、発信者情報（総務省令に挙げられたもの(89)）を開示することが認められている（第 4 条第 1 項)。開示請求を受けたプロバイダ等は、原則として、発信者の意見を聴く必要がある（同条第 2 項)。

しかしながら、開示の判断を誤った場合には、通信の秘密侵害罪に問われる可能性があることなどから裁判外での任意開示は例外的な場合にとどまると考えられており(90)、実際に任意に開示される事例は稀であるとされる(91)。任意に開示されない場合の裁判手続においては、時間

---

(84)　インターネット上の海賊版対策に関する検討会議・知的財産戦略本部「「インターネット上の海賊版対策に関する検討会議」中間まとめ（案）～インターネット上の海賊版サイトに対する総合対策～」（インターネット上の海賊版対策に関する検討会議（タスクフォース）（第 9 回）資料 1）2018.10, p.84. 同上 <https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/kaizoku/dai9/siryou1.pdf>; 一般財団法人情報法制研究所情報法制研究タスクフォース「著作権侵害サイト対策検討における論点整理」2018.6.3. <https://jilis.org/proposal/data/2018-06-03.pdf>

(85)　森亮二「ブロッキング法制化反対の理由」（インターネット上の海賊版対策に関する検討会議（タスクフォース）（第 7 回）資料 7）2018.9.13. <https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/kaizoku/dai7/siryou7.pdf> ここでは、人格的利益として尊重される名誉毀損と財産上の利益の侵害にとどまる海賊版サイトを比較し、後者にのみブロッキングという手段が認められることの問題も指摘されている。

(86)　総務省総合通信基盤局消費者行政第二課『プロバイダ責任制限法　改訂増補第 2 版』第一法規, 2018, p.5.

(87)　藤田・高部監修, 高嶋　前掲注(7), p.835.

(88)　なお、同法第 3 条等で損害賠償責任の制限につき規定されている情報の削除等（送信防止措置）については、公然性を有する通信に関し、通信の秘密の対象外であるという解釈（ゆえに民法上の作為義務が生じ得る）を前提としているという（斉藤邦史「プロバイダの送信防止作為義務と通信の秘密」『Nextcom』41 号, 2020.Spring, p.35.)。

(89)　「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律第四条第一項の発信者情報を定める省令」（平成 14 年総務省令第 57 号）

(90)　総務省「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律―解説―」（平成 29 年 1 月更新）p.26. <https://www.soumu.go.jp/main_content/000461787.pdf>

(91)　清水陽平「発信者情報開示に関する課題について」（第 1 回発信者情報開示の在り方に関する研究会　資料 1-3）2020.4.30. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000685612.pdf>

的・金銭的負担が大きいこと[92]などから、総務省では、「発信者情報開示の在り方に関する研究会」（座長：曽我部真裕京都大学大学院法学研究科教授）を設置し、開示対象となる情報の範囲、任意開示のあり方、裁判手続の負担等を論点[93]として、議論を行っている[94]。

4　セキュリティの確保

通信の秘密とセキュリティの確保については、主に①具体的なサイバー攻撃への対応と通信の秘密の関係、②保安・諜報活動と通信の秘密の関係の二つの観点から論じられている。

前者のサイバー攻撃への対応については、平成25年の「サイバーセキュリティ戦略」（平成25年6月10日情報セキュリティ政策会議決定）において、「情報セキュリティを目的とした通信解析の可能性等、通信の秘密等に配慮した、関連制度の柔軟な運用の在り方について検討する」とされた[95]。その後、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」で検討が行われ、上述のサイバー攻撃等ガイドラインの改版につながっている[96]。また、サイバー攻撃に関する情報共有やその情報を活用した対応においても、通信の秘密の保護が問題となり得るが、この点について、平成30年の電気通信事業法改正により、制度整備が行われている[97]。

後者の保安・諜報活動と通信の秘密については、諸外国において、テロ対策を含む国家安全保障のため、通信傍受が行われている[98]。一方で、日本では通信傍受は、犯罪捜査に限定的に

⑼② 任意で開示されない場合、裁判手続によることになる。その際、通常の例では、第一段階として、ソーシャルメディア事業者等にIPアドレス等の開示を求め（仮処分）、第二段階として、その情報をもとにISPに開示請求の訴訟を提起し、これによって発信者情報が得られれば、発信者に対して損害賠償請求を行う、といったように3段階の裁判手続が必要で、金銭的・時間的負担が大きい。特に海外プロバイダを相手取る場合には、訴状の送達手続に時間を要する。「主な検討課題（案）」（第1回発信者情報開示の在り方に関する研究会　資料1-5）2020.4.30. 同上 <https://www.soumu.go.jp/main_content/000686000.pdf> 以下も参照。神足祐太郎「権利侵害とプロバイダの責任―インターネット上の名誉毀損への対応―」『調査と情報―ISSUE BRIEF―』919号, 2016.8.25, pp.13-14. <https://dl.ndl.go.jp/view/download/digidepo_10189094_po_0919.pdf?contentNo=1>

⑼③ 「主な検討課題（案）」同上

⑼④ なお、令和2年5月下旬、インターネット上で誹謗中傷を受けた女性（プロレスラー、タレント）が亡くなったことを受けて、高市早苗総務大臣は、7月に予定される中間取りまとめで全体像を示した上で、「スピード感を持って」必要な制度改正に臨みたいとしている。研究会では、総務省令で規定される開示対象となる情報の範囲に電話番号を加える等の方向性で議論が進められている一方、開示要件の緩和には慎重な見解も見られる（「高市総務大臣閣議後記者会見の概要」2020.6.5. 総務省ウェブサイト <https://www.soumu.go.jp/menu_news/kaiken/01koho01_02000920.html>;「高市総務大臣閣議後記者会見の概要」2020.5.26. 同 <https://www.soumu.go.jp/menu_news/kaiken/01koho01_02000917.html>; 出口絢「SNSの誹謗中傷「電話番号も開示対象にすべき」に賛同多数、総務省の有識者会議」『弁護士ドットコムニュース』2020.6.4. <https://www.bengo4.com/c_23/n_11303/>）。

⑼⑤ 情報セキュリティ政策会議「サイバーセキュリティ戦略―世界を率先する強靭で活力あるサイバー空間を目指して―」2013.6.10, p.31. 内閣サイバーセキュリティセンターウェブサイト <https://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf>

⑼⑥ こうした一般的なサイバー攻撃への電気通信事業者の対応の観点のほか、武力行使としてのサイバー攻撃に自衛隊が対応する場合に通信の秘密との関係で問題が生じる可能性も指摘されている（宍戸常寿ほか「AIと社会と法　パラダイムシフトは起きるか？（NUMBER 08）サイバーセキュリティ」『論究ジュリスト』32号, 2020.冬, p.162.（湯淺墾道情報セキュリティ大学院大学教授の発言））。

⑼⑦ 第三者機関を通じて電気通信事業者間の情報共有等を行うものであり、第三者機関の認定のほか、当該機関における通信の秘密の保護等について定められた。「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」（平成30年法律第24号）立案担当者による解説として以下を参照。影井敬義ほか「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」『情報通信政策研究』2(1), 2018.12, pp.167-189. <https://www.soumu.go.jp/main_content/000567073.pdf>

⑼⑧ 米国では、2013年、政府がインターネットのメタデータ等を大規模に傍受していたことが暴露された（林　前掲注⑶①, pp.202-206.）。諸外国における通信傍受について、以下を参照。情報セキュリティ大学院大学「インターネットと通信の秘密」研究会「インターネット時代の「通信の秘密」各国比較」2014.5, pp.11-14. <http://lab.iisec.ac.jp/~hayashi/2014-7-7.pdf>

用いられるものであり、サイバーセキュリティ対策等のための傍受は行われていないが、今後、制度・組織の整備が必要であるという主張がある(99)。

5　ネットワーク中立性

ネットワーク中立性とは、インターネット上を流れる通信を平等に取り扱うという原則のことをいう。通信回線の容量に制約がある中で、(例えば金銭と引換えに) 特定の通信のみを優先する行為などが許されるかという問題である。これは、競争、イノベーションへの影響や表現の自由の観点から、2000 年代以降、米国で情報通信政策分野の一大トピックとなった(100)。他方、日本では、通信の秘密や利用の公平（電気通信事業法第 6 条）といった事業法上の規律によってそもそもこの種の問題が起こりにくかったことが指摘されており(101)、関連のガイドラインの策定に当たってもこれらの規律が参照されてきた(102)。

近年モバイル通信の重要性が高まっていることやゼロレーティング(103)等の新たな商慣行が生まれていることといった内外の環境変化から、ルールの見直しが必要であると考えられ、総務省は「ネットワーク中立性に関する研究会」を設置して検討を行った（中間報告書を平成 31 年 4 月公表(104)）。特に通信の秘密との関係で議論された事項として、「通信の最適化」(105)及び「ゼロレーティング」が挙げられる(106)。前者については、帯域制御ガイドラインが改定され、後者については新たに「ゼロレーティングサービスの提供に係る電気通信事業法の適用に関するガイドライン」(107)が作成・公表された。

改定された帯域制御ガイドラインにおいて、通信の最適化のうちペーシング、不可逆圧縮等については、各ユーザの利用できる帯域を一定の水準以下に制限する（公平制御）といったより緩やかかつ公平な方法を採り得ることを理由に、通常は手段の相当性を欠くこと、したがって、正当業務行為に当たらず、実施する場合には利用者の個別の同意が必要であると整理された(108)。

---

(99)　土屋大洋『サイバーセキュリティと国際政治』千倉書房, 2015, pp.204-205; 林　同上, pp.206-209. 米国のような広範にわたる傍受を認めるべきではないとしつつ国の安全のために必要最小限の制約を加えるためには、立法措置を含めた適切な運用ルールの制定等が求められるとするものとして以下がある。石井夏生利「国家安全と通信の秘密」『Nextcom』16 号, 2013.Winter, pp.31-32.

(100)　神足祐太郎「ネットワーク中立性をめぐる議論」『レファレンス』803 号, 2017.12, pp.82-89. <https://dl.ndl.go.jp/view/download/digidepo_11003877_po_080304.pdf?contentNo=1> を参照。

(101)　立石聡明「Network Neutrality 再燃」『ITU ジャーナル』47(5), 2017.5, p.5. <https://www.ituaj.jp/wp-content/uploads/2017/05/2017_05-01-Special-NetworkNewtrality.pdf>;「ネットワーク中立性についての議論 〜IGCJ 15 報告その 2〜」2016.10.20. JPNIC BLOG <https://blog.nic.ad.jp/2016/913/> 日本における議論については、同上, pp.93-98 を参照。

(102)　平成 18 年から平成 19 年にかけては総務省の「ネットワークの中立性に関する懇談会」において検討が行われ、結果策定されたのが前述した帯域制御ガイドラインである。

(103)　従量料金制又は上限データ通信量を定めた定額料金制の料金体系において、特定のアプリ・コンテンツの利用について使用データ通信量にカウントしないサービスのことをいう。

(104)　「ネットワーク中立性に関する研究会中間報告書」2019.4. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000613654.pdf>

(105)　回線混雑時の通信品質確保の一環として、モバイル回線経由でデータを送信する際に、データの流れる速度を調整すること（ペーシング）、画像・動画を（不可逆）圧縮・加工して送信することをいう。送受信されるデータが変更されることから、アプリケーションに不具合が生じるケースなどがあり問題化した。実積寿也ほか「シンポジウム（第 5 分科会）通信の秘密等に関する最近の議論動向」『情報ネットワーク・ローレビュー講演録編：第 15 回研究大会講演録』2016.7, pp.187-195; 谷本宏昭「個人情報保護等の現状・動向について―「通信の秘密」の保護に関する動向―」『ICT World Review』11(1), 2018.4・5, pp.41-42.

(106)　「ネットワーク中立性に関する研究会中間報告書」前掲注(104), pp.26, 31.

(107)　総務省「ゼロレーティングサービスの提供に係る電気通信事業法の適用に関するガイドライン」2020.3. <https://www.soumu.go.jp/main_content/000678277.pdf>

(108)　帯域制御の運用基準に関するガイドライン検討協議会ほか　前掲注(40), pp.13-14, 16.

ゼロレーティングについては、①サービスの利用者と非利用者の通信を区別するために情報を利用すること、②利用者の通信のうち特定のコンテンツにアクセスする通信を区別するために情報を利用すること、の二つの場面で通信の秘密が問題となる。①については、課金等のために必要かつ相当な行為であり、正当業務行為に当たると整理された(109)。他方、②については、ゼロレーティングサービスは必須のサービスとは言えず、正当業務行為に当たるとは言えないので、個別の同意が必要であるとされた(110)。

6　国外事業者への適用

電気通信事業法上、電気通信事業者としての認定は、電気通信設備の設置を基準として行われており、従来、国内に向けてサービスを提供する事業者であっても、国外に拠点を置き、かつ、国内に電気通信設備を置かない事業者については、電気通信事業法の規律が及ばないと考えられてきた(111)。この点について、かねて国内事業者と国外事業者に対する規制の公平性の観点から問題視されてきた。例えば、国内事業者が、ウェブメールにおいて、内容を解析した上で関連の広告を配信することは、通信の秘密との関係で問題視されたが、同様の手法は（日本でサービスを行っている）国外事業者において既に導入されているものであった(112)。

総務省は、平成30年から情報通信審議会、「プラットフォームサービスに関する研究会」等において、この点に関する議論を進めてきた。令和2年2月に公表されたプラットフォームサービスに関する研究会最終報告書では、「我が国の利用者の利用者情報の適切な取扱い」及び「国内外の事業者間の公平性を確保し、イコールフッティングを図る観点」から、「国内事業者か国外事業者かにかかわらず、通信の秘密の保護に係る規律が等しく及ぶようにすることが適当」であるとされた(113)。そして、執行管轄権の問題を解決するため、国外事業者に対し、国内代表者等を指定させること等が適当であると結論付けられた(114)。令和2年の第201回国会（常会）において、この点に関する改正を含む、「電気通信事業法及び日本電信電話株式会社等に関する法律の一部を改正する法律」（令和2年法律第30号）が成立した。

7　通信の秘密の評価

これまで見てきたとおり、通信の秘密は、様々な問題と関連して論点となってきた。こうした議論を背景として、通信の秘密又はその解釈・運用のあり方に関しては、肯定的・批判的な双方の立場から評価が行われている。

---

(109)　総務省　前掲注(107), p.15.

(110)　同上, pp.15-16.

(111)　第186回国会参議院総務委員会会議録第18号　平成26年5月13日　pp.8-9. なお、国外事業者への電気通信事業法の適用については通信の秘密以外の分野でも取り上げられてきた（「多様化・複雑化する電気通信事故の防止の在り方について報告書」2013.10.31, p.23. 総務省ウェブサイト <http://www.soumu.go.jp/main_content/000257952.pdf>）。後述の「電気通信事業法及び日本電信電話株式会社等に関する法律の一部を改正する法律」（令和2年法律第30号）の審議においては、属地主義に基づいて外国法人も規律の対象であるとした上で、これを前提として法執行の実効性を強化するとしている（第201回国会　衆議院総務委員会議録第14号　令和2年4月14日　p.16.）。

(112)　「ヤフー新広告　疑問の声　「秘密　侵害では」　メール読み取り　関連商品表示」『読売新聞』2012.6.25. その後、総務省は、サービス提供のための要件を示した（「ヤフー株式会社における新広告サービスについて」2012.9.27. 総務省ウェブサイト <https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000122.html>）。

(113)　「プラットフォームサービスに関する研究会最終報告書」2020.2, p.7. 同上 <https://www.soumu.go.jp/main_content/000668595.pdf>

(114)　同上, p.8. なお、このほか、刑事罰を代替する措置を検討すること、業務改善命令の発動にかかる指針を策定すること、事業者と行政の継続的対話を通じ透明性・予見可能性を向上させることなどを提言している。

伝統的な通信の秘密の解釈のあり方に対しては、日本における通信の秘密の解釈が先進諸外国に比しても厳格で(115)、通信手段の変化に伴って(116)、規制に「過剰」と「空白」が生まれること(117)、そのため、インターネット媒介者に、通信の秘密についての従来の解釈を適用した場合、例えば、違法又は有害な情報対策（Ⅲ章1～3）やセキュリティ対策（Ⅲ章4）等の局面において、期待される役割を十分に果たせないという懸念があることが指摘されている(118)。このように現行の通信の秘密の解釈によって生じる問題を指摘する立場からは、しばしば、通信の内容とメタデータを区別して論ずべき（後者の保護の程度を検討すべき）であると主張される(119)。

他方、宍戸常寿東京大学大学院法学政治学研究科教授は、通信の秘密について、いわば「意図せざる「基本設計」」としての意義を有すると評価している(120)。通信の秘密は、インターネット上の表現行為の匿名性を相当程度保障し、違法又は有害な情報の対策に関して政府による直接的な法執行ではなく自主的な取組によるものとする方向を導き、あるいは、事業者による情報の利活用に対して都度有効な同意を要求する（Ⅲ章5）といった形で、インターネット利用者の自由・利益を確保する機能を果たしているというのである。諸外国において、表現の自由や個人データの保護といった異なる権利によって保護されてきた「インターネットの自由」が日本においては「通信の秘密」によって形作られてきたと見ることもできるだろう(121)。このような立場からは、仮に、通信の秘密の対象となる情報を収集・分析する必要があるのであれば、それにふさわしい組織・手続の保障が必要であると考えられる(122)。

加えて、ガイドライン等を通じて違法性の阻却に関する解釈を積み重ねることについては、①緊急避難等の、本来は緊急の際に用いられる理論によってブロッキングのような恒常的な枠組みを説明することの問題、②必ずしも法令に依拠せずステークホルダーや有識者によって構成される研究会等の報告書などを契機とした事業者の取組によって実質的な規制が行われていることによるグローバル企業への適用の困難さ（Ⅲ章6）等といった点から批判があり、法律の規律密度を上げるべきである（法治主義の徹底）という見方もある(123)。

---

(115) 林紘一郎「情報法の観点から―検閲の禁止・通信の秘密・利用の公平など―」『Law and Technology』87号, 2020.4, p.82; 情報セキュリティ大学院大学「インターネットと通信の秘密」研究会　前掲注(98), p.i.

(116) 電話の場合には、メタデータと内容を区分することは困難であったが、インターネットにおいては可能であるといった違いが指摘されている（情報セキュリティ大学院大学「インターネットと通信の秘密」研究会「インターネット時代の「通信の秘密」再考」2013.6, p.6. <http://lab.iisec.ac.jp/~hayashi/610REPORTIII.pdf>）。

(117) 「過剰」については、通信内容とメタデータを同様の保護の対象と考えていることから、電気通信事業者としての本来的な業務においても違法性阻却を議論しなくてはならないという点で委縮効果が生じていること等、過剰な自己規制が生じているという。「空白」については、新事業者に対する規制の空白などが挙げられている（同上, pp.20-24.）。

(118) 高橋郁夫「インターネット媒介者の役割と「通信の秘密」」『Nextcom』16号, 2013.Winter, pp.4-5.

(119) 情報セキュリティ大学院大学「インターネットと通信の秘密」研究会　前掲注(116), p.25; 林　前掲注(31), pp.208-209. 曽我部教授は、通信の秘密を制約する法律の合憲性を検討するに当たり、通信内容とメタデータの保護の程度を分けて考える余地があると指摘しており、海賊版サイトブロッキングの法制化についてもそのような観点から（通信の秘密については）合憲性を緩やかに判断することができる可能性を指摘している（曽我部「通信の秘密の憲法解釈論」前掲注(1), p.20; 前掲注(81)の記述参照）。一方、メタデータは、インターネット通信において、プライバシー保護の上で重要な意味を持つ（アクセス先を示す情報によって通信の内容が高いレベルで推知される）との指摘も注目される（ダニエル・J・ソロブ（赤坂亮太ほか訳）『プライバシーなんていらない!?―情報社会における自由と安全―』勁草書房, 2017, pp.174-181.（原書名: Daniel J. Solove, *Nothing to hide*, 2011.））。

(120) 宍戸　前掲注(11), p.519.

(121) 「（耕論）サイト遮断と言うけど 赤松健さん 宍戸常寿さん 別所直哉さん」『朝日新聞』2018.9.7; 森亮二「サイトブロッキングに関する議論の問題点はどこにあったのか」『Business Lawyers』2019.2.14. <https://www.businesslawyers.jp/articles/488>

(122) 宍戸常寿「サイバー空間を守る「監視」と「負担」の議論を」『Wedge』31(1), 2019.1, p.10.

おわりに

「通信（信書）の秘密」の概念が生まれた当時のような、国家あるいはそれに準ずる主体による通信の独占は見られなくなっており、通信の秘密の保護の前提は変化している(124)。

一方で、様々な局面における情報通信の利活用が進むにつれて、通信の内容にとどまらず、メタデータや通信を行う端末と紐付けられた情報(125)の保護の重要性は増している。諸外国において、通信の秘密の保護にかかわる新たな立法が検討され(126)、あるいは、情報通信の機密性や完全性の保障にかかわる新たな基本権が生み出されている(127)ことはその証左と言える。また、情報通信の分野では、新たな独占の主体（プラットフォーム事業者）が登場し、大きな問題を提起している(128)。

こうした状況を踏まえれば、通信の秘密には、現代的意義を見出すこともできよう。その一方で、国外事業者に対してもその遵守を求め、新たなビジネスモデルを阻害しないためには、これまで個別的に解釈が示されてきた事例を含め、通信の秘密の制約が認められる条件を示す一般的な理論を構築(129)し、基準を明確化することが求められる(130)。

（こうたり　ゆうたろう）

---

(123) 曽我部「通信の秘密の憲法解釈論」前掲注(1), p.20; 同「2030年のネットワークの規律のあり方についての憲法的考察」（情報通信審議会電気通信事業政策部会電気通信事業分野における競争ルール等の包括的検証に関する特別委員会・主査ヒアリング（第4回）資料4-2）2018.11.12, p.11. 総務省ウェブサイト <https://www.soumu.go.jp/main_content/000584598.pdf>

(124) 齊藤　前掲注(14), pp.123-129.

(125) 例として、ウェブサイトから閲覧者のブラウザに対して発給されるCookie（クッキー）が挙げられる。同じサイトにアクセスした場合に、ブラウザから情報が送信され、過去にアクセスしたことがわかる。端末と結び付いた情報であって、それ自体では個人を特定できないこと等から、（他の会員情報等と突合されるなどして個人を特定できる場合を除けば）個人情報として扱われていないが、実質的には個人を追跡できる可能性がある。これを通信の秘密の保護の対象として検討する可能性が指摘されていた。秋山瑞季「個人情報保護法見直しの概要」『調査と情報―ISSUE BRIEF―』1089号, 2020.2.27, pp.3-5. <https://dl.ndl.go.jp/view/download/digidepo_11454495_po_1089.pdf?contentNo=1>;「［解説スペシャル］閲覧履歴　知らずに拡散　個人情報保護法見直し　検証」『読売新聞』2019.3.20.

(126) 島村智子「【EU】電子通信分野におけるプライバシーの保護に関する規則案」『外国の立法』271-1号, 2017.4, pp.8-9. <https://dl.ndl.go.jp/view/download/digidepo_10322292_po_02710104.pdf?contentNo=1>

(127) ドイツでは、これまでの通信の秘密、情報自己決定権に加えて、憲法裁判所の判決において「デジタル基本権」の概念が提示されている（西土彰一郎「インターネットにおける基本権保障のあり方」『情報通信政策レビュー』9号, 2014.11, pp.66-73. <https://www.soumu.go.jp/iicp/chousakenkyu/data/research/icp_review/09/09-3nishido2014.pdf>）。

(128) 曽我部真裕「自由権―情報社会におけるその変容―」『法学セミナー』57(5), 2012.5, pp.12-14.

(129) 上野達弘「ブロッキングとリーチサイトをめぐる議論状況」『法とコンピュータ』37号, 2019.7, p.15.

(130) その際には、例えば、インターネット上の匿名表現の自由について、これまで実質的な保護を与えてきた通信の秘密のほか、表現の自由により直接的に保護されると考えることもできるなど、通信の秘密、表現の自由、プライバシーの境界は揺らいでいることを踏まえ、表現の自由やプライバシー権とその制約という原理の調整として議論し、通信の秘密の内容を分解し、個別に検討することもあり得る（宍戸　前掲注(11), pp.519-522.）。