# インターネット利用における「通信の秘密」

田川義博[1]

伝統的な「通信の秘密」は,電気通信事業者が預かった他人の通信を,ノータッチで受信者に伝えることを意味していた.この伝統的な「通信の秘密」の概念が,インターネット利用の普及・拡大によって大きく変質している.本稿はこの変質により,どのような法的な課題が生じているかを考察して,今後の「通信の秘密」のあり方を考えるヒントを得ることを目的にしている.

まず第 1 章において「通信の秘密」の概念・法体系について概説したうえで,第 2 章において,従来の伝統的な「通信の秘密」の理解を,電気通信事業法 4 条を手掛かりに分析する.これらの「通信の秘密」の理解を基礎にして,第 3 章ではインターネット利用の状況変化と,この変化に対応して進められている政策・法制度の特徴的事項を分析するとともに,「通信の秘密」の変質の特徴点を分析する.ついで第 4 章では,「通信の秘密」に関する電気通信事業者の役割の変化を述べたうえで,さらに第 5 章において「通信の秘密」の遵守主体の問題,「通信の秘密」の保護法益,公然性を有する通信などの問題についての法的考察を行う.そして最後に第 6 章において,これからの「通信の秘密」のあり方についての若干の考察を行う.[2]

## 1.「通信の秘密」の概念と法体系

### 1.1 電気通信事業法における「通信の秘密」と用語の定義

「通信の秘密」はすべての人が遵守すべき法的義務であるが,歴史的には電気通信事業者が遵守すべき法的義務として論じられてきた.郵便における「信書の秘密」も「通信の秘密」の一部ではあるが,本稿では主として電気通信における「通信の秘密」の問題を扱い,必要に応じて「信書の秘密」の問題にも言及することとしたい.

まず,「電気通信」,「電気通信役務」,「電気通信事業」などの用語について,意味を確認しておきたい.これらの用語は電気通信事業法第２条において,以下のように定義されている.(下線は筆者付加)

[1]セキュアシステム研究所客員研究員

[2] 本稿の執筆については, 林紘一郎・田川義博「『心地よい DPI(Deep Packet Inspection)』と『程よい通信の秘密』」,情報セキュリティ大学院大学紀要,2012 年,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 Rethinking 'Secrecy of Communications' in the Internet Age」,2013 年,に多くを依拠している部分がある.また,林紘一郎氏に懇切なコメントをいただいた.謝意を表したい.

・電気通信　有線,無線その他の電磁的方法により,符号,音響又は影像を送り,伝え,又は受けることをいう.(1 号)
・電気通信設備　電気通信を行うための機械,器具,線路その他の電気通信設備をいう.(2 号)
・電気通信役務　電気通信設備を用いて他人の通信を媒介し,その他電気通信設備を他人の通信の用に供することをいう.(3 号)
・電気通信事業　電気通信役務を他人の需要に応ずるために提供する事業(中略)をいう.(4 号)
・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をいう.(5 号)

この規定を受けて,第 4 条に以下の規定が置かれている.(下線は筆者付加)

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.
2　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.

この 4 条違反の罰則として,179 条に以下の規定が置かれている.(下線は筆者付加)

電気通信事業者の取扱中に係る通信(164 条 2 項に規定する通信を含む.)の秘密を侵した者は,2 年以下の懲役又は 100 万円以下の罰金に処する.
2 電気通信事業に従事する者が前項の行為をしたときは,3 年以下の懲役又は 200 万円以下の罰金に処する.
3 前 2 項の未遂罪は,罰する.

## 1.2 「通信の秘密」とは

上記の 2 条の各定義から分かることは,「電気通信事業者」は,「電気通信役務」を,「他人の需要に応ずるために提供する事業」を営む者である.また電気通信役務とは,他人の通信を預かって運ぶために,「電気通信設備を用いて他人の通信を媒介し,その他電気通信設備を他人の通信の用に供すること」である.

また「通信の秘密」に関しては,「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(4 条 1 項)」と規定されており,197 条 2 項で電気通信事業の従事者の「通信の秘密」侵害行為に対する罰則が加重されている.

この問題を通信当事者からみるとどうなるであろうか.歴史的にみると,「通信の秘密」は公権力による検閲から信書を保護するための「信書の秘密」として近代憲法に登場した.[3]
離れた場所の間で通信を行う場合には,通信を運ぶことを第 3 者に依頼せざるを得ない.こ

[3] 出典:鈴木秀美 “通信の秘密”136 頁,大石眞・石川健治編「憲法の争点」Jurist 増刊,2008 年 12 月 15 日号

の場合に,通信を運んでいる第 3 者または公権力が,途中で通信内容等を見ることがあるとすれば,通信当事者は安心して通信することができない.

判例でも地裁レベルの判決ではあるが,東西 NTT が脅迫的内容の電報の受付・配達を差し止める条理上の作為義務を負うか否かが争われた事件において,「電気通信事業者は,利用者間で通信が行われるに際し,あくまでも物理的な通信伝達の媒体ないし手段として,発信者から発信された通信内容をそのまま受信者に伝達することが,その提供する役務の内容として予定されて」いるとして,差し止めは「公共的電気通信事業者としての職務の性質からして許されない違法行為」であるとして(大阪地判平成 16.7.7 判時 1882 号 87 頁),[4] 電気通信事業者が通信内容に関与することが明確に否定されている.

以上のことから考えると,電気通信事業者は他人から預かった通信を運ぶことがその役割であるので,運ばれる「他人の通信」にノータッチが求められる.これが電気通信事業者に課された,伝統的な「通信の秘密」の意義である.

1.1 の冒頭で述べたように,歴史的にみて,「通信の秘密」は通信事業者が遵守すべき法的義務である.また通信事業者以外の一般人が通信の伝達過程に介入することは技術的にも困難であったこともあって,「通信の秘密」は通信事業者の法的義務として長年議論されてきた.[5]

## 1.3 現行の「通信の秘密」の法体系

まず憲法 21 条 2 項後段において,「通信の秘密は,これを侵してはならない」との規定がある(なお 1 項で集会・結社・表現の自由および 2 項前段で検閲の禁止が規定されている).この憲法 21 条 2 項後段の規定に関する考察については,「5.『通信の秘密』の法的問題の考察」において述べる.

法律レベルでは,1.1 で述べた電気通信事業法の規定の他に,有線電気通信法,電波法に(通信の)秘密の保護の規定がある.

まず有線電気通信法では,9 条で「有線電気通信の秘密は侵してはならない.」となっているが,規律対象の通信としては,電気通信事業法 4 条 1 項又は 164 条 2 項の通信は除かれている.

9 条違反の罰則を規定している 14 条では,1 項において 2 年以下の懲役又は 50 万円以下の罰金の規定があるが,2 項において有線電気通信の業務に従事する者が前項の行為をしたときには,3 年以下の懲役又は 100 万円以下の罰金と,刑罰が加重されている.

また,電波法では,59 条で「何人も法律に別段の定めがある場合を除くほか,特定の相手方に対して行われる無線通信(中略)を傍受してその存在もしくは内容を漏らし,又はこれを窃用してはならない.」ことが規定されている.規律対象の無線通信としては,有線電気通信法の規定と同様に,電気通信事業法 4 条 1 項又は 164 条 2 項の通信は除かれている.

罰則を規定している 109 条 1 項では,「無線局の取扱中に係る無線通信の秘密を洩らし,又は窃用した者」の罰則が定められているが,「無線通信の業務に従事する者がその業務に関し知り得た前項の秘密を洩らし,または窃用したとき」には,電気通信事業法および有

[4] 宍戸常寿 “通信の秘密について”20～21 頁参照.http:www.win-cls.sakura.ne.jp/pdf/35/02.pdf

[5] もっとも,アナログの携帯電話では,事業者以外の一般人が無線電波を傍受すると,会話が聞くことができることが話題になったことがあったが,デジタル化によってこの話題も沈静化した.

線電気通信法の規定と同様に,刑罰が加重されている.また,109 条の 2 の暗号通信に関する規定においても,無線業務従事者に対する刑罰加重が規定されている.

このように,「通信の秘密」の規定がある上記の三つの法律を比較すると,以下の特徴点がある.

1) 有線電気通信法,電波法とも,電気通信事業法 4 条 1 項又は 164 条 2 項の通信は,その規律対象外となっている.

2)電気通信事業法では通信の秘密,有線電気通信法では有線電気通信の秘密,電波法では無線通信の秘密の侵害行為が禁止されており,その禁止される対象者は,すべての人である.しかしながら,当該業務の従事者が侵害行為を行った場合には,刑罰がいずれの法律でも加重されている.

3)規律対象となっている通信の範囲について,電気通信事業法では「電気通信事業者の取扱中に係る通信」が,電波法では「無線局の取扱中に係る無線通信の秘密」であるのに対して,有線電気通信法ではこの「取扱中に係る」との規定はない.

4)原則として,通信の秘密の「知得,漏示,窃用」の行為が全て禁止されているが,無線通信については技術的性格上「善意の知得」があり得ることから,知得行為自体は可罰性がないとされている(後に詳説する).

5)電気通信事業法では,1.1 にあるように 4 条 1 項の「通信の秘密」の侵害行為禁止規定に加えて,同条 2 項では,電気通信事業の従事者に対する「他人の秘密」の遵守規定があることが,有線電気通信法および電波法とは異なる点である.

## 1.4 「通信の秘密」の保障の限界

### 1.4.1 「通信の秘密」の保護に対する例外を規定する法律

上記のように,「通信の秘密」の保護は憲法や法律で規定されているが,現行法上の制限としては,たとえば,刑事訴訟法では郵便物の押収(100 条・222 条),破産法では破産者宛の郵便物や電報の破産管財人による開封(190 条[現行 82 条]),関税法では郵便物の差押え(122 条),監獄法[現行は,刑事収容施設及び被収容者等の処遇に関する法律]では在監者[受刑者等]の信書の発受等につき検閲[検査]その他の制限(46 条―50 条)[現行 127 条など]を定めている.[6]

これらの「通信の秘密」の保護を制約する規定のうち,刑事訴訟法 100 条において差押が認められる要件が,一般の差押の対象である「証拠物又は没収すべき物と思料するもの」(同 99 条)と比べて,その要件を緩和している点でその合憲性には強い疑問がある,との指摘がある.[7]

また,1999 年に制定された通信傍受法(「犯罪捜査のための通信傍受に関する法律」)では,検察官または司法警察員は,法定犯罪(薬物,銃器および集団密航に関する犯罪,組織的な殺人犯罪の 4 類型)に限り,犯罪に関する通信実行の嫌疑があり,他の方法では犯人の特定,犯行の状況・内容の把握が困難な場合,裁判官の発する傍受令状により通信の傍受ができるようになった.[8]これも「通信の秘密」の保護を制約する法律である.

---

[6] 出典:芦部信喜,高橋和之補訂「憲法 第 5 版」214 頁,岩波書店,2011 年

[7] 出典:佐藤幸治「日本国憲法」322～323 頁,成文堂,2011 年

[8]出典:鈴木・前掲注 3,137 頁

1.4.2 「通信の秘密」の保障の限界に関する学説

「通信の秘密」の保障を制約できる根拠は何であろうか.

佐藤[2011]は,「憲法による『通信の秘密』の保障は無条件であるが,一定の内在的制約を受けることについては異論をみない」とする.[9]

渋谷[2013]も内在的制約を肯定しているが,「審査基準の観点からすると,通信の秘密を侵害する制度は,厳格審査に付され,その立法目的が真にやむをえない(compelling)ものであって,その立法目的達成手段が,その目的にとって必要不可欠のものであり,その手段の権利制約の程度が必要最小限のものでなければならない.」とする.[10] この渋谷説は,違憲立法審査権における二重の基準論[11]を踏まえたものであると考えられる.

鈴木は,「通信の秘密も公共の福祉によって制限される」とする.[12]「通信の秘密」が公共の福祉によって制約できるかについては,人権と憲法上の権利を区分したうえで,長谷部[2008]のいう「切り札としての権利」については,公共の福祉を理由にした制約は許されないとの論からの検討も必要であるように考えられる.[13]

この他,インターネット利用に関して,プロバイダなどによる「通信の秘密」を外形的に侵害する行為が,正当行為として認められる法律やガイドラインがいくつも制定されている(インターネット利用に関する考察は,4 章で取上げる).

以上の「通信の秘密」に関する基礎的な法制度をふまえて,インターネット時代にふさわしい「通信の秘密」の問題について考えていきたい.まず,「通信の秘密」は従来どのように解釈されてきたかについて論ずる.

# 2. 従来の「通信の秘密」の法解釈

本章では,電気通信事業法 4 条の規定に関する従来の法解釈について論ずることにしたい.(条文については,1.1 を参照)

## 2.1 「通信の秘密」の保障内容

2.1.1 憲法における保障内容

憲法 21 条 2 項後段の「通信の秘密は侵してはならない」との規定の保障内容として,佐藤[2011]は,①公権力による積極的知得行為の禁止,②通信業務従事者による職務上知り得た通信に関する情報の漏えい行為の禁止に加えて,③通信業務従事者による不当・差

[9]出典:佐藤・前掲注 7,322~324 頁

[10]出典:渋谷秀樹「憲法 第 2 版」415 頁,有斐閣,2013 年

[11]二重の基準論については,長谷部恭男「憲法 第 4 版」107～120 頁,新世社,2008 年参照

[12]出典:鈴木・前掲注 3,136 頁

[13]人権と憲法上の権利の区分については,辻村みよ子「人権と憲法上の権利」64~65 頁,大石眞・石川健治編「憲法の争点」Jurist 増刊,2008 年 12 月 15 日号参照.切り札としての権利については,長谷部・前掲注 11,116～120 頁参照.また,高橋和之「人権論の論証構造―「人権の正当化」論と「人権制限の正当化」論(Ⅰ) ジュリスト No.1421, 2011.4.15 も参照

別的な取扱いの禁止をあげている.[14] なお,鈴木[2008]は,「通信の秘密」の保障内容が①と②であることに学説に異論はないとしている.[15]

また,「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.」との電気通信事業法 3 条の規定は,憲法 21 条 2 項の検閲の禁止とは異なり,事前審査に限定されない.さらに,通信業務従事者に通信に関する情報提供を求めるのが禁止されるのは,いわゆる「通信の検閲の禁止」の帰結であるとする.[16]

したがって,通信事業従事者が,②にあるように職務上知り得た通信に関する情報を,公権力に対して提供することは,禁止されることになる.

佐藤[2008]は,この法制は事業者をコモンキャリアと捉え,憲法の趣旨から要請されるあるべき姿を法律により明示的に定めたものとしている.[17]

### 2.1.2 法律レベルにおける保障内容

「通信の秘密」の保障内容としては,通信の当事者以外の第3者が「通信の秘密」を他に漏らし(他人が知りうる状態におくこと),または窃用する(本人の意思に反して自己または第三者の利益のために利用すること)ほか,「通信の秘密を知ろうとする意志をもって,積極的に知ることも含まれる」[18]とされているが,ほぼ憲法の保障内容と同様であると考えられる.

なお,「通信の秘密」の侵害行為は,有線と無線においてその構成要件を異にする.有線通信の場合には,知得,漏えい,窃用が禁止行為であるが,無線通信の場合には電波法 59 条において,「通信を傍受してその存在若しくは内容を漏らし,又はこれを窃用すること」となっており,単なる知得(傍受)は秘密侵害になっていないのは,無線は空中に広く伝播するので,知得する意思がなくとも知りうることがあるためであるとされる.[19]

## 2.2 「通信の秘密」の範囲[20]

### 2.2.1 憲法における解釈

「通信の秘密」の範囲に関しては,例えば芦部[2011]は「通信内容はもとより,その差出人(発信人)または受取人(受信人)の氏名・居所および通信の日時や個数など,通信に関するすべての事項に及ぶ」[21]としている.

また,佐藤[2011]は,「コミュニケーションの内容のみならず,コミュニケーションの存在自体に関する事柄(例えば,信書であれば,信書の差出人・受取人の氏名・住所,信書の差出個数・年月日など)を包含する」[22],としている.

---

[14]出典:佐藤・前掲注 7,321～322 頁

[15]出典:鈴木・前掲注 3,136 頁

[16]出典:佐藤・前掲注 7,322 頁

[17]出典:佐藤・前掲注 7,322 頁

[18]出典:電気通信関係法コンメンタール編集委員会編「電気通信関係法詳解＜下巻＞40 頁,一二三書房,1973 年

[19]出典:前掲注 18,40 頁

[20]2.2～2.4 の記述については,注 2 の文献に多く依拠している.

[21]出典:芦部信喜・前掲注 6,213 頁

[22]出典:佐藤・前掲注 7,321 頁

両説とも,「通信の秘密」の範囲としては,通信内容に加えて,通信当事者等の情報などの通信の構成要素を含むとしていることは共通している.

2.2.2 電気通信事業法における解釈

4 条では前述したように,1 項で「通信の秘密」,2 項で「他人の秘密」を規定している.通説では,1 項の「通信の秘密」の対象範囲は,通信内容だけではなく,通信当事者,通信日時,通信量,ヘッダー情報や通信の存否自体もその保護対象であるとされている.（以後、通信内容以外の「通信の秘密」の対象となるこれらの事項を「通信の構成要素」と呼ぶ.）この解釈は,憲法の「通信の秘密」の範囲と同じであり,憲法の解釈をそのまま電気通信事業法に持ち込んだものと考えられる.

このように,「通信の秘密」として通信内容と通信の構成要素の両方を,1 項の「通信の秘密」とする解釈を「同一説」,「通信の秘密」の保護対象は通信内容だけであり,通信の構成要素は2項に規定されている「他人の秘密」であるとする解釈を「峻別説」として,2.4 においてその歴史的な推移を考察する.

## 2.3 「電気通信事業者の取扱中に係る」の意義

後述の吉展ちゃん事件における内閣法制局の回答に関して,片桐[1986]は「事業者の取扱中に係る通信」について,以下のように述べている.

「発信者が通信を発した時点から受信者がその通信を受ける時点までの間における通信をいい,通信が受信者に伝達されて受信者の支配下にあるものは含まないとされているが,本法制局意見は,一方当事者甲の利用する電話の端末の設備において聴取し得る他方当事者乙の通話の内容は甲の支配下に置かれたものであるから,同項にいう『取扱中に係る通信の秘密』に当たらないとしている.したがって,司法警察職員等が通話の内容を録音するためには,通話の内容を支配する甲の同意があれば足りることとなり,乙が現行犯人である等の要件を要しない.」[23]

また判例では,一旦「通信」のプロセスを経た以上,通話内容が録音されたテープを他者から入手し（つまり,自らは探知行為をなさないで,物理的なテープを入手したに過ぎなくても）「電気通信事業者の取り扱い中に係る」通信であるとの特性は失われない,と判示した最高裁決定がある.すなわち,最二小決2004 年4 月19 日（刑集58 巻4号281ページ）は,上告趣意は刑訴法405 条の上告理由に当たらないとしつつ,職権で次のように判示している（下級審も,同じ意見）.

「被告人の上記行為は,たとえ自らは盗聴録音に関与していないとしても,電気通信事業者が現に取扱っていた際に盗聴録音された通話内容の一部をそのまま再生して他に漏らすものであるから,（一部略）『電気通信事業者の取り扱い中に係る通信（中略）の秘密を侵した』ことに当たると解するのが相当である.」

ただし,「通信」というプロセスと無関係な情報は,「通信の秘密」に入らないとする考えも

[23]出典：片桐裕「70 電話の逆探知,通話の録音等」551 頁,前田正道編「法制意見百選」,有斐閣,1986 年

通説であると思われる.後述の同一説の立場をとる東京地判が,次のように述べている.

「例えば電話番号については,通信履歴（カッコ内略）におけるそれのように,個々の通信を取り扱った電気通信事業者のもとで,当該個々の通信に関係するものであることがわかる形で保管されている場合には,『通信の秘密』として保護されるが,電話番号情報（カッコ内略）におけるそれのように,個々の通信とは無関係に蓄積されたものである場合には,たとい電気通信事業者のもとで管理されていたとしても,また,個人情報として保護する実際上の必要性の高いものであっても,『通信の秘密』の保護の対象外である.けだし,それは『「通信の」秘密』に当たらないからである.」（東京地判2004年4月30日,裁判所HP）

## 2.4 電気通信事業法における「通信の秘密」と「他人の秘密」の区分

### 2.4.1 電気通信事業の従事者に対する刑罰加重

前述したように,4 条 1 項はすべての人が「通信の秘密」を遵守することを求めており,2 項は電気通信事業の従事者に対してのみ「他人の秘密」の遵守を求めている.

また,179 条においては,1 項で「電気通信事業者の取扱中に係る通信（中略）の秘密を侵した者」に対して,2 年以下の懲役又は 100 万円以下の罰金に処することを規定し,2 項で「電気通信事業に従事する者が」1 項の行為をしたときは,刑罰を加重している.

### 2.4.2 郵便法における「通信の秘密」と「他人の秘密」

現行憲法が施行された 1947 年に,旧郵便法に代わり施行された郵便法 9 条において,1 項で「郵政省の取扱中に係る信書の秘密」を保護し,2 項で郵便の業務に従事する者に対する「郵便物に関して知り得た他人の秘密」を保護する,という区分が設けられた.
この郵便法における「通信の秘密」および「他人の秘密」の意義については,以下のように説かれている.[24]

「信書の秘密とは,信書の内容はもちろんであるが,さらに信書に関する一切の事項が含まれるのである.したがって,その差出人,受取人の住所又は居所及び氏名も含まれることになる.」（1 項）
「郵便物に関して知り得た他人の秘密とは,通信文などの内容,その他郵便物の発受人の住所,氏名,差出個数,取扱年月日,その他通信そのものの構成要素を成す一切の事項をいうものであるが,これらの事項を知ることによって,通信の意味内容が推察されることも考えられるので,これらの事項もまた他人の秘密に属するものとされるのである.」（2 項）

この解説では,「信書の秘密」として信書の内容に加えて,信書に関する一切の事項が含まれるとしている.また「他人の秘密」は,「通信文などの内容,その他通信そのものの構成要素を成す一切の事項をいう」とされており,2 項の「他人の秘密」には,1 項の「信書の秘密」が含まれるという解説になっている.

憲法では「通信の秘密」の遵守が規定されているのに対して,郵便法 8 条 1 項では「通信の秘密」の一部である「信書の秘密」に加えて,2 項では郵便業務に従事する者に対して

[24]出典：郵務局業務課内郵便法例研究会編「郵便法概説」44～45 頁,（財）通信事業教育振興会,1982 年

は「信書の秘密」を含む「他人の秘密」の遵守を求めている.

これに対して,刑罰の適用対象行為は,「他人の秘密」全体ではなく,「信書の秘密」の侵害行為だけとなっており,遵守義務内容の規定(8条2項)と罰則適用行為の範囲(80条2項)が異なっており,若干分かりにくい規定になっている.(この解釈を複合説と呼ぶ.)

また,この郵便法の「通信の秘密」と「他人の秘密」の区分の法解釈に関して,筆者が行った個別の照会に対して,以下の回答をいただいた.[25]

> 郵政公社設立までの郵便法では信書以外に小包役務の規定があり(現在は削除),現行法でも第三種郵便や第四種郵便には明らかに信書ではないものが含まれている.
> したがって,少なくとも郵便法上では,「信書の秘密」と「郵便物に関して知り得た他人の秘密」の範囲は明確な差がある.

この解釈では,信書＝通信であるのに対して,郵便業務従事者が遵守すべき「他人の秘密」には信書ではないものが含まれているので,両者には明確な差異があることになる.

上記の複合説に対して,「他人の秘密」には,「信書の秘密」を含まないと解釈すれば,「他人の秘密」に関しては,罰則が適用されないので,遵守義務内容と罰則適用の関係を直接結び付けることができ,分かりやすい規定になると考えられる.(この解釈を「分離説」と呼ぶ.)

いずれの説を採った場合であっても,「信書の秘密」以外の「他人の秘密」に関しては,刑罰の適用がないことを明確にすることが,罪刑法定主義の観点から重要であると考える.

郵便法制定時期が公衆電気通信法の制定時期より早いこと,および主務官庁が同一であったことから考えると,公衆電気通信法における「通信の秘密」と「他人の秘密」の区分は,郵便法の規定を取り入れ,その規定が現行の電気通信事業法にもそのまま引き継がれているものと推測される.

### 2.4.3 同一説

電気通信事業法4条1項に規定する「通信の秘密」の対象範囲に関して,前述したように,通信内容および通信の構成要素の両方が,「通信の秘密」であるとの解釈が同一説である.

1985 年の通信自由化に適合的な法律として,電気通信事業法が制定された.「通信の秘密」の規定については,電気通信の独占時代の法律である公衆電気通信法 5 条にあった「公社または会社の取扱中」との文言が,電気通信事業法 4 条では「電気通信事業者の取扱中」に変更されただけで,他の文言は変更されずそのまま公衆電気通信法の文言が取り入れられた.

公衆電気通信法が制定された1953年に,同法の制定に携わった当事者による逐条解説書では,以下のように明らかに同一説にたって述べられている.[26]

> 「而して『通信の秘密』とは通信の内容は勿論,誰から誰への通信であるかという事実また

[25]総務省郵便課長である岡崎毅氏から個人的な見解として,懇切な回答をいただいた.謝意を表したい.

[26]出典:金光昭・吉田修三「公衆電気通信法解説」,日信出版,1953 年

は場合により単に通信の存在の事実をも意味し（後略）」

また「通信の秘密」に関する判例は多くはないが,同一説にたっている.

1)「ここに『通信の秘密』とは単に通話内容だけでなく誰と誰が通話したかという事実をも指し,またこれを『侵す』ということは通信の内容を他人に漏らすだけでなく,必要もないのに他人の通話を聞くことも含まれるものと解すべきである」（大阪高判1967年12月25日.判時514号82ページ）.
2)「電気通信事業法104条（現在の179条）にいう『通信の秘密』には,通話の内容のほか,通信当事者の住所・氏名・電話番号,発受信場所,通信の日時・時間・回数なども含まれると解すべきである.」（東京地判2004年4月30日,裁判所HP）.

現在の「通信の秘密」に関連しては,電気通信事業者団体が策定したガイドラインや総務省研究会での報告書では,「通信の秘密」に関しては同一説にたった解説・記述がなされており,実務上も同一説によって運用が行われている.

2.4.4 峻別説

現状の通説は同一説ではあるが,歴史的には,同一説による「通信の秘密」の法解釈とは異なり,「通信の秘密」の対象範囲は,通信内容だけで,通信の構成要素等は「他人の秘密」である（峻別説）と伺わせる事例がある.

1)事例 1：上田市公安調査官郵便物調査事件

1953年12月と翌年3月に,長野県上田市で公安調査庁に勤務する者が,郵便集配人に対して特定の機関紙（朝鮮関係の非公然の機関紙類）の発行部数や,特定の人間への郵便の存否などを問いただしたという事件が発生し,国会でこの事件に関する郵便法の法解釈について質疑が行われた.

1954 年 4 月 3 日の衆議院郵政委員会では,政府委員からは若干の答弁の混乱はあったものの,郵便物の発受人の住所氏名等を漏らすことは,郵便法 9 条 1 項の「信書の秘密」侵害に該当せず,2 項の郵便の秘密によって守られる,との答弁がなされている.

この答弁は,9 条 1 項「信書の秘密」が通信内容だけであって,郵便物の発受人の住所氏名等は「信書の秘密」に該当しないとも受け取られる答弁である.

また,同年 5 月 21 日の参議院郵政委員会では,政党の機関誌が信書に該当するか,宛名の書いていない封書は信書に該当するかとの質問があった.この質問に対して,郵便法 9 条 2 項の侵害行為であるとの答弁と,1 項の侵害行為であるとの答弁がなされ,政府内部の解釈論の不統一がみられた.

この事例をみると,当時は信書の秘密と他人の秘密の区分が,自明のものとして定着していなかった様子が伺える.

2)事例 2：吉展ちゃん事件に関する郵政省からの照会に対する内閣法制局の回答

1963 年に発生した幼児誘拐身代金要求事件である吉展ちゃん事件では,電話の逆探知（脅迫行為を行った者の発信場所を探索する行為）,および捜査当局が脅迫を受けている当事者の同意を得て脅迫電話を録音することが,当時の公衆電気通信法 5 条に違反す

るかどうかに関して,当時の電電公社が郵政省経由で内閣法制局に以下の照会を行った.

①電話を利用して脅迫の罪を現に侵している者がある場合に,公社の職員が発信場所を探索し捜査官憲に通報することは,公衆法 5 条 2 項に違反するか.
②捜査官憲が,通話の一方の当事者の同意を得て他方の当事者の通話を録音することは,公衆法 5 条 1 項に違反するか.

これに対する内閣法制局の回答は「いずれも消極に解する」,すなわち①および②の行為は,公衆電気通信法 5 条に違反しないというものであった.

この照会,回答のやりとりにおいて注目すべきなのは,照会側の電電公社が,①において電話の逆探知（脅迫行為を行った者の発信場所を探索する行為）が 5 条 2 項,すなわち 1 項の「通信の秘密」違反ではなく,2 項の「他人の秘密」に違反するか,との峻別説を伺わせる立場で照会したことである.

ただし,この内閣法制局の回答が電話の発信場所の探索は 2 項の「他人の秘密」に該当するとの判断であるとしつつも,片桐[1986]は,憲法 21 条 2 項後段には通信内容だけではなく,通信の構成要素等も含まれ,他の事案でも内閣法制局は郵便法 9 条の他人の秘密についても同様に解していると述べている.さらに郵便法 9 条と同様の規定である公衆電気通信法 5 条および電気通信事業法 4 条も,これと異なった解釈をする特段の理由に乏しいとの見解を示しており,同一説をとっている.[27]

この「通信に関して知り得た他人の秘密」に関して,以下のような解釈をとっている文献もある.[28]

1)他人の秘密の範囲については,従来の通信内容,通信の構成要素,通信の存在の事実等「通信の秘密」のほか,通信当事者の人相,言葉の訛りやプッシュホンに記憶された相手番号等直接の通信の構成要素とはいえないが,それを推知させうるものも含む.

電気通信事業という他人の通信を扱う公共性の高い事業に従事する以上,より幅広い義務を課して,「通信の秘密」の保護に万全を期したものである.

2)電気通信事業の従事者に対する罰則の適用については,1 項の「通信の秘密を侵した」場合に刑罰加重される.通信の秘密の構成要素以外の他人の秘密を守らないことについては罰則の適用はなく,民事上・服務上の責任を問われるにとどまる.

この解釈では,他人の秘密の範囲は,「通信の秘密」を含むものの,刑罰の適用については,1 項の「通信の秘密」の範囲を超える事項に関する違反行為については,刑罰の適用はないことを明確にしている.

また長谷部[2012]は,「同法 4 条 2 項の規定する『通信に関して知り得た他人の秘密』は,『通信の秘密』そのものより範囲が広く,具体的な通信の受信,発信の場所や受信者,発信者の氏名などを含むものと考えられる.」[29]と述べており,峻別説によっていることを伺わせる.

---

[27]出典：片桐・前掲注 23,548～549 頁

[28]出典：電気通信法制研究会「逐条解説　電気通信事業法」25 頁および 267～268 頁,第一法規出版会,1987 年

[29]出典：長谷部恭男「通信法」67 頁,宇賀克也・長谷部恭男編「情報法」,有斐閣,2012 年

### 2.4.5 「他人の秘密」の範囲

電気通信事業法 4 条 2 項において電気通信事業の従事者に課せられた「他人の秘密」の遵守義務の範囲についての通説は,「通信の秘密」は通信内容＋通信の構成要素である（同一説）としたうえで,「他人の秘密」＝「通信の秘密」＋ α とするものである（複合説）.

上記の 1987 年の逐条解説は,「他人の秘密」を「通信の秘密」に該当する事項とそれ以外のものに分けて,「通信の秘密」侵害には罰則適用,それ以外の「他人の秘密」には罰則不適用とする解釈である.

歴史的にみて「通信の秘密」は,公権力による通信への介入を禁止するとともに,通信を運ぶ事業者に預かっている通信へのノータッチを求め,「通信の秘密」の保障を行おうとすることが,その意義であった.2.1.1 で述べたように佐藤は「事業者をコモンキャリアと捉え,憲法の趣旨から要請されるあるべき姿を法律により定めたもの」としている.

電気通信事業法 4 条 1 項で,「電気通信事業者の取扱中に係る通信の秘密」の保障を定め,2 項で電気通信事業の従事者に「他人の秘密」の遵守を求めている.これは,電気通信事業の従事者が業務遂行上,一般人よりも広い範囲の利用者ないし利用情報を得ることのできる立場にあるので,この業務上得られる情報を「通信の秘密」よりも広い範囲の「他人の秘密」という法概念を創出して,保障したと考えられる.

一方,「通信の秘密」侵害に対する従事者の刑罰を加重しているが,「通信の秘密」の範囲を超える「他人の秘密」に関しては,刑罰は不適用で,違反行為に対しては民事法,行政法による対応に委ねている.これは,他の事業における同様の行為との均衡を考えて,業務情報の積極的知得,漏えい,窃用という行為は,民事法,行政法によって対処することにしているものと考えられる.

このことを考慮して,「他人の秘密」に「通信の秘密」を含める複合説と,「他人の秘密」は「通信の秘密」を含まず,それ以外業務遂行上得られた利用者ないし利用情報であると考える分離説とを比較すると,1 項は従事者を含む全ての人に対する規定であると解釈したうえで, 侵害行為と,侵害行為に対する罰則適用との対応関係が明確になるので,従事者に関しては,「通信の秘密」侵害には刑罰（加重）適用,「他人の秘密」侵害には刑罰不適用とする分離説が,より適切な解釈ではないかと考える.

### 2.4.6 分離説にたった「他人の秘密」

郵便業務には信書（通信）以外の部分がかなりあるので,郵便法においては「信書の秘密」以外の「他人の秘密」には,いくつかの事項が含まれていると考えられる.

これに対して電気通信事業法は,通信だけを対象にした法律である.同一説を取った場合には,「通信の秘密」に該当しない「他人の秘密」に該当する事項は,郵便法の場合とは異なり,極めて限定的であると考えられる.

しかしながら,限定的とはいえ,「通信の秘密」に該当する違反行為には罰則が適用され,それに該当しない「他人の秘密」には,罰則の適用はないとの解釈を採った場合には,「通信の秘密」と「他人の秘密」を区分する意義はある.もっとも,範囲が極めて限定的なのに,「他人の秘密」という規定を設けたことについては,その必要性に若干の疑問が残る.

この問題については,インターネット時代にふさわしい「通信の秘密」法制のあり方の考察の項で再度取上げる.

以上の「通信の秘密」と「他人の秘密」に関する解釈を比較したのが,図表 1 である.

**図表 1 「通信の秘密」と「他人の秘密」の説の比較**

| | 通信の秘密<br>同一説 | 通信の秘密<br>峻別説 | 他人の秘密<br>複合説 | 他人の秘密<br>分離説<br>(峻別説) |
|---|---|---|---|---|
| 通信内容 | ○ | ○ | ○ | × |
| 通信の構成要素等 | ○ | × | ○ | ○ |

注 1:「通信の構成要素」というのは,通信内容には含まれない通信当事者に関する情報,通信の日時,通信の受発信の場所および通信の存在の存否などを指す.(芦部注 21,佐藤注 22,長谷部注 29 参照).

注 2:○は該当,×は非該当.

注 3:同一説:「通信の秘密」には通信内容と通信の構成要素の両方が含まれるとの説

峻別説:「通信の秘密」は通信内容,「他人の秘密」は通信の構成要素等とする説

複合説:「他人の秘密」には通信内容,通信の構成要素等が含まれるとの説

分離説(峻別説):「他人の秘密」には,通信の構成要素等のみが含まれるとの説

## 3 インターネット利用が「通信の秘密」など法制度に与える影響

インターネットの普及・拡大とともに,社会経済活動でも個人生活でもインターネットへの依存度が大きくなっている.このためインターネット利用の良否・巧拙が,産業の国際競争力や生活の質の向上に大きな影響を与える.

本章では,万人がインターネットを利用することで生み出される機会の面と,蛮人がインターネットを利用することで生み出される脅威の面の両方から,インターネット利用の特徴を探り,その変化に対応する法制度整備の状況を概観する.次いで,「通信の秘密」に対する影響を探る.

### 3.1 インターネット利用が生み出す機会[30]

まず新しいサービス・アプリケーションが次々と開発され,市場に投入されたことが挙げられる.1993 年の World Wide Web に始まり,Google などの検索システムおよび検索連動型広告, Facebook などの SNS(ソーシャルネットワーキングサービス)をはじめとして,動画・音楽配信サービス,電子書籍,ソーシャルゲーム,ネット無料通話,米国でのピンタレストやインスタグラムなどの情報共有サービスなど多彩なサービス・アプリケーションが,数多く活発に利用されている.

[30]3.1~3.4 の記述は,以下の文献に多く依拠している.田川義博「インターネット利用におけるガバナンスのあり方:自由・創造と秩序・安全のはざまのなかで」,上智大学「コミュニケーション研究」第 43 号,2013 年 http://repository.cc.sophia.ac.jp/dspace/bitstream/123456789/34915/1/200000016987_00013 2000_27.pdf

2008 年の米国大統領選挙では,ソーシャルメディアが活発に利用され,日本でも 2013 年夏の参議院選挙から解禁された.また 2011 年の北アフリカのチュニジア,エジプト,リビアの政変では,ソーシャルメディアが大きな役割を果たしたといわれている.

さらに,スマホ,タブレット,スマート TV のような多彩な端末機器が市場に投入され,この端末機器とサービス・アプリケーションの相乗効果により市場が大きく成長している.

## 3.2 インターネット利用が生み出すポジティブ・インパクト

企業などの組織内や企業を超えたレベルで,インターネット上で自由な情報流通が行われることで,新たな知的創造が進み,インターネットが「集合知」を生み出す契機になっている.例えば,Linux による OSS（Open Source Software）開発の事例が有名である.

また,インターネット利用が市民のエンパワーメントときずなの強化に役立っている事例もみられる.たとえば東日本大震災では,多くの企業や NPO・ボランティアが,多くの被災者・被災地支援のサイトを短時間で立ち上げた.これらの活動によって支援の輪が大きく広がった.

さらにインターネット利用の活発化によって,インターネット・ビジネスが急拡大して,米国の Google,Apple,Amazon,Facebook などの企業や,日本では楽天,Yahoo ジャパン,DeNA などの企業が急成長しており,より重要な産業になっている.この万人利用の面では,事業者側と利用者側の間で win-win の関係となっているといえる.

## 3.3 インターネット利用が生み出す脅威

情報発信のハードルが技術的にもコスト的にも大きく下がったことで,万人の利用が可能になった反面で,万人のなかに潜む蛮人のインターネット利用で,以下のような好ましくない事象が多発している.

1)情報セキュリティ・インシデント（事例）が多発している.最近では標的型サイバー攻撃によって,企業の営業秘密,個人情報や国家の機密情報の漏えいが大きな社会問題になっている.

2)違法・有害,権利侵害情報が大量に流通している.これには,名誉毀損,プライバシー侵害,著作権侵害,詐欺的情報などがある.

3)信憑性の薄い情報が大量に流通している.たとえば,流言・デマ,やらせ情報などがある.この流言・デマの拡大では,悪意のある蛮人だけではなく,善意の人々の書込み等が結果として,流言・デマを広めてしまうケースもある.

4)コミュニケーション・トラブル等が多発している.たとえば,Twitter などへの不用意な書込みに端を発する炎上・さらしや,即レス症候群のようなネット利用疲れなどがある.

5)蛮人の行為ではないが,思わぬ事象・トラブルが発生することがある.たとえば,Google サジェスト機能によって,ある人が犯罪に関係しているとの表示がなされたことによって,その人が仕事を失い,また,再就職に支障が出た.このため,Google にサジェスト機能の表示差止を求める仮処分を東京地裁に提起し認められたものの,Google はこの差止命令に従っていない.また,2013 年 4 月の東京地裁の判決で,名誉毀損を認め米国 Google 本社に対して表示差し止めと 30 万円の賠償を命じたが,Google 側は控訴している.[31]

[31]出典：http://www.nikkei.com/article/DGXNASDG14024_U3A610C1CC0000/

## 3.4 脅威の発生要因

3.3 で述べたような事象発生には,以下のような要因があると考えられる.

1)社会経済活動におけるネットワーク利用の拡大・深化によって,個人情報・機密情報を含む膨大な情報が電子化されて,ネットワーク上に存在するようになっている.この情報の窃取を狙って,標的型サイバー攻撃と呼ばれる意図的な攻撃がなされている.また,このような外部からの意図的な攻撃に加えて,内部者の意図的もしくは過失による情報漏えいも数多くみられる.

2)スマホなどの新しい利用者機器を狙った不正アプリが顕著に増加している.

3)情報セキュリティ意識・スキルレベルが低い利用者が多数存在して,対策が不十分な場合が多い.(永遠のビギナー)

4)企業等でも不正利用に関する監視・対策が不十分なケースが多い.また新しい攻撃手法が登場して攻撃に利用されるため,情報セキュリティ対策が後追いになるケースも多い.

5)自分の個人情報漏えいやプライバシー侵害に警戒心をもつ利用者がいる一方で,便利で楽しいサービスを利用する際に,事業者のプライバシー・ポリシーを理解しないままに,事業者の求めに応じて個人情報を自ら進んで提供する利用者も多く存在している.

6)ネットワークでは,匿名による情報発信なら個人が特定されないと思いこむ,または,ごく身近な人々に伝えるような意識で情報発信を行うなど,ネットワークの特性を理解していない利用者が多数存在している.

7)Twitter などでは,情報が短時間に急激に拡散する.

8)法律に無知または無関心なため,違法・有害情報や権利侵害情報を発信する利用者が多数存在している.加えて,違法だと知っていても,あまり意識することなく(著作権侵害コンテンツのダウンロードなど)違法行為を行う人々も多数存在している.

9)ネットワーク利用の利便性を追求して,膨大な情報を扱うための新しいサービス・アプリが開発・導入されているが,グーグル・サジェスト機能のように,人手を介さないで自動処理の場合でも,思わぬ被害をもたらすこともある.

## 3.5 インターネット利用の普及・拡大に対応した政策・法制度整備

上記の 3.1 から 3.4 におけるインターネット利用の機会と脅威に対応するために,政策・法制度整備が進められており,多くの新規立法または法改正が行われている.

この対応は 4 つの分野で行われている.

### 3.5.1 通信・放送関係事業者に関する政策・法制度整備

例:電気通信事業法,放送法等.

この分野の政策・法制度は,事業構造なり規制に影響を与える分野である.デジタル革命で conduit(インフラ設備)と content の組み合わせが原理的に自由になり,ブロードバンド化で現実化した.産業構造的には,サイロ型から(多層)レイヤー型へ転換して,マスメディアコンテンツがインターネットでも流通するようになった(3.6.2 参照).この産業構造の転換に対応するために,通信・放送総合的法体系の検討を経て,放送法等改正が行われ,2011 年に施行された.

「通信の秘密」との関連では,1.2 で述べたように伝統的に「通信の秘密」は通信事業者

を対象にしているが,同じようなサービスが電気通信役務として提供されるだけでなく,アプリケーションとしても提供が可能であるため,事業者レベルでの「通信の秘密」の適用が,どこまで及ぶのかが不明確になっている.(この問題は,5.1 で取上げる)

3.5.2 インターネット利用の拡大・普及を促進する政策・法制度整備

例:電子署名・電子認証法(「電子署名および認証業務に関する法律」)(2001 年),

e 文書法(「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律:通則法,民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律:整備法」),IT 書面一括法(「書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律」).

3.1~3.2 で述べたように,この分野の政策・法制度は,多彩で便利なサービスの提供を,さらに促進しようとするものであり,インターネット利用が有する巨大な潜在的可能性を解き放つための政策・法制度である.

ブロードバンドインフラ整備を促進する政策や,電波開放政策など政策的な促進策も講じられている.

「通信の秘密」の関連では,ライフログを含むビッグデータの活用によって,新たな産業を興す課題などがある.安倍内閣の成長戦略でも「世界最高水準の IT 社会の実現」の具体策として,「IT 利活用裾野拡大のための規制・制度改革,公共データの民間開放などを実施します.」と謳われている.

3.5.3 インターネット利用による弊害を規制する政策・法制度整備

例:不正アクセス禁止法,個人情報保護法,プロバイダ責任制限法(「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」),迷惑メール防止法(「特定電子メールの送信の適正化等に関する法律」),不正競争防止法,1987年および2001年の刑法改正.

3.3～3.4で述べたように,この分野の政策・法制度は,インターネット利用における多くの脅威に対処しようとするものである.「通信の秘密」の関連では,情報セキュリティの強化策および違法有害情報の流通・蓄積への対処策等が課題である.

3.3～3.4 における課題の基礎にあるのは,国家・企業の機密情報を含む膨大な情報がインターネット上で流通し,蓄積されていることである.また,社会経済政府活動や個人生活がインターネットに大きく依存しているために,情報セキュリティでいう機密性,完全性,可用性が損なわれることで大きな悪影響が生ずるだけに,的確・迅速な対応が求められている.

3.5.4 インターネット・ビジネスに関する法律

例:独占禁止法,特許法,商標法,著作権法,消費者法

インターネット・ビジネスはネットワークの外部性(ネットワーク効果)が働くために,反競争的行為を行わなくとも「ひとり勝ち」現象がみられることがある.「ひとり勝ちを放任することがイノベーションを促進すると同時に,逆にそれが経路依存性となってイノベーションを阻害する」[32]ことも考えられる.ネットワーク効果を上回る技術革新があれば,特定企業の独占・

[32]出典:林紘一郎・湯川抗・田川義博「進化するネットワーキング,第 2 章 一人勝ちとネットワークの外部性」

寡占状態は解消されるが,競争政策上どのような政策を取るべきかがしばしば論議されている.

また「通信の秘密」の関連では,消費者のプライバシーや個人情報保護の問題とも関連して,議論されている.

### 3.5.5 通信と情報処理

インターネット利用では,通信と情報処理が融合して,一体となってサービスが提供されている.歴史的には,通信は規制されており,米国では 1982 年の AT&T 分割まで regulated monopoly と呼ばれる独占下の規制が続いていた.

一方,コンピュータによる情報処理サービスは規制されたことがなく,自由なビジネスとして発展してきた.ところが,通信と情報処理が融合してくると,規制されている通信と非規制の情報処理をどのように切り分けるかが大きな規制上の問題となった.

この問題に対処するために,FCC（連邦通信委員会）はコンピュータ調査を行い,1971 年,1979 年,1980 年と 3 次に及ぶ決定を行って,規制分野と非規制分野を切り分けた.現在の連邦通信法では,電気通信サービスと情報サービスの区分となっている.同様の問題に 3 回も決定が行われたということは,それだけこの切り分けが困難な問題であることも意味している.

このなかにあって,インターネットに関しては非規制政策が取られており,FCC をはじめとして,米国政府は,以前からインターネットの自由を支持する見解を表明している.[33]

2012 年 12 月に開催された,国際電気通信規則(ITR)の改正を議論するための ITU(国際電気通信連合)の会議では,セキュリティを理由にして,インターネット上の表現に政府が介入できるようにするとの提案があった.この提案に対して,日米欧などの政府代表が強く反対して,この提案は撤回された.

しかしながら,最終段階で「インターネットの安全」の確保に関する条項が入れられた.この改正条項を含む最終規則改正案は,賛成 89 カ国で成立したものの,この条項に反対した日米欧など 55 カ国は署名を拒否するという異例の事態となった.[34] 情報セキュリティを巡る規制論議として注目される.

米国のインターネット企業に対しては,「通信の秘密」の問題を含み,多くの批判がなされているが,上記の米国における通信と情報処理の区分およびインターネット政策の歴史を考えると, 原則自由・例外規制の発想で,自由なビジネスを展開していることは,理解できる面がある.

## 3.6 インターネット利用の普及拡大による「通信の秘密」の変質

3.1～3.4 において述べたように,インターネット利用の普及拡大が大きな機会を生み出

---

94 頁,NTT 出版,2006 年

[33]インターネットは一度も規制されたことがないので,deregulation ではなく,unregulation という新語によって,インターネット規制の政策論を展開している文献として,以下の文献を参照.

Oxman, Jason,“The FCC and the Unregulation of the Internet”, OPP Working Paper No.31, Office of Plans and Policy, FCC, 1999 年

[34]出典：田川・前掲注 30,27 頁

すと同時に,一方で大きな脅威をも生み出している.これらの機会と脅威に対する対処策として,3.5 において述べたような政策・法制度整備が行われている.

インターネット利用の普及・拡大よって生出される機会と脅威とそれに対応する政策・法制度のなかに,「通信の秘密」に関する対応策が含まれている.「通信の秘密」に与えるインパクトとしては,以下の事項があげられる.

3.6.1 「通信の秘密」保護に関する電気通信事業者の役割の変化

1.1 で述べたように,他人の通信を預かって運ぶ電気通信事業者は,伝統的な役割として預かった他人の通信にはノータッチであることが求められていた.

しかし,インターネット利用の普及・拡大に伴う弊害に対処するために,他人の通信(コンテンツ)に関与が求められるようになっており,電気通信事業者の伝統的な「通信の秘密」との関わり方が変質している.

3.6.2 インターネット・サービス提供事業者と「通信の秘密」の関わりの不明確化

3.5.1 で述べたように,従来の conduit(設備)と content を垂直統合型(サイロ型)から(水平)レイヤー型へと産業構造が変化している.従来の電気通信事業者の担う conduit とその設備を利用して流通する情報・コンテンツの 2 層構造ではなく,conduit,プラットフォーム,端末,アプリケーションという多層レイヤー構造になっている.このなかで,さまざまなプレーヤーが一面競争,他面提携してサービスが提供されている.

このため,伝統的に「通信の秘密」の遵守が求められる電気通信事業者と,それ以外のインターネットビジネス・サービスの提供者の間で,「通信の秘密」の適用範囲が不明確になっている.この状況のなかで,「通信の秘密」の遵守義務のある電気通信事業者にだけに,「通信の秘密」の厳格な運用がなされた場合には,企業間競争において公正競争(equal footing)が損なわれるのではないか,との懸念も生じている.

3.6.3 インターネット利用の機会を拡大する政策・法制度と「通信の秘密」

3.5.2 および 3.5.4 で述べたように,ライフログを含むビッグデータの活用による新たな市場の成長が期待されているが,インターネット利用者にとっての「通信の秘密」およびプライバシー・個人情報保護の権利を調整する必要がある.

3.6.4 インターネット利用における脅威に対処する政策・法制度と「通信の秘密」

3.3で述べたように,情報セキュリティおよび違法有害情報への対処策等が課題である.

まず情報セキュリティに関しては,インターネット上で流通・蓄積している膨大な機密情報・個人情報の窃取等を狙ったサイバー攻撃が激化している.とりわけ,特定の政府機関・企業を標的とした長期にわたる執拗で高度な標的型攻撃によって,機密情報が窃取され流出する事例が多数報告されている.これには,国家安全保障や原子力に関する情報も含まれている.

また,電力,通信,金融,交通などの重要インフラの制御系システムに対するサイバー攻撃も報告されており,インターネットと接続されていないシステムの情報セキュリティ対策の重要性も指摘される状況になっている.

さらに,インターネット上には大量の違法有害情報が流通・蓄積していて,権利侵害の防止も課題になっている. これらの対策を講ずるために,情報発信者の「通信の秘密」の権利

を制約する必要があるが,どのような制約なら良いのかについて,対策によって守るべき法益との調整を図る必要がある.

3.6.5「公然性を有する通信」における「通信の秘密」

通信はもともと秘匿性があるので,「通信の秘密」の保障が重要であるが,インターネット上ではむしろ多くの人にアクセスしてもらいたいとの意図をもった,秘匿性を有しない通信が増加している.これが「公然性を有する通信」と呼ばれるもので,「通信の秘密」の観点からも通信と表現の境界,通信過程と蓄積の区分の問題として論議されている.

これらの問題については,3.6.1の問題を第4章で,他の問題を第5章で考察する.

# 4 「通信の秘密」保護に関する電気通信事業者の役割の変化

1.2 で述べたように,通信事業者の伝統的な「通信の秘密」に関する役割は,自分が預って運ぶ「他人の通信」の内容にノータッチでいることである.すなわち,conduit を担う電気通信事業者は,自分が運ぶ他人の通信(content)にノータッチであるという,conduit と content の相互独立性が長年維持されてきた.

この長年の電気通信事業者の「通信の秘密」に関する役割が,インターネット利用において大きく変質している.この変質の原因は 3 章で述べたインターネット利用の普及・拡大に対応するためであるが,伝統的に運ばれる他人の通信にノータッチが強く求められてきた電気通信事業者にとって,「通信の秘密」の変質にどう対応すれば良いかが大きな問題になっている.

一方 4.2 でみるように,「通信の秘密」に関する個別の解釈により,個別案件の解決が図られており,それはそれで一応の成果をあげているものの,事業者や利用者にとって十分に予見可能性のある一般原則が解釈として確立しているわけではない.

## 4.1 プロバイダ等による「通信の秘密」の侵害行為を適法と認める根拠

電気通信事業者が他人の通信にノータッチであるべきという原則を離れ,他人の通信に関与できるとする根拠については,現在は刑法理論に依拠している.

「刑法第 2 編　罪」において,どのような行為を行ったら罪となるかが定められている.これが,構成要素該当性といわれるものである.

一方第 2 編で定める構成要件に該当した場合であっても,第 1 篇第 7 章「犯罪の不成立及び刑の減免」の規定によって,正当な事由があって違法性がない(違法性阻却),または責任を問うことができない(責任阻却)の場合には,犯罪が成立せず刑罰は課されない.

違法性阻却事由に基づいて,刑罰が課されないのは,以下の行為である.

・正当行為(35 条)　法令または正当な業務による行為は,罰しない.
・正当防衛(36 条)　急迫不正の侵害に対して,自己または他人の権利を防衛するために,やむを得ずにした行為は,罰しない.
・緊急避難(37 条)　自己又は他人の生命,身体又は財産に対する現在の危機を避けるため,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.ただし,その程度を超えた行為は,情状により,その刑を軽減し,又は免除することができる.

2　前項の規定は,業務上特別の義務がある者には,適用しない.

この規定は,「通信の秘密」侵害の構成要件に該当する行為に関しても適用される.

35 条の正当行為に該当するとされるのは,「通信の秘密」の侵害行為（知得,漏えい,窃用：2.1「通信の秘密」の保障内容の項参照）によって失われる「通信の秘密」の保護法益よりも,他により大きな法益があって,それを保護する場合である.したがって,「通信の秘密」の保護法益と他の保護法益を比較衡量することによって,違法性阻却に該当するかどうかが判断されることになる.また,刑法における保護法益の類型としては,個人的法益,社会的法益,国家的法益がある.

上記の違法性阻却事由に加えて,「知得・窃用・漏洩にみえる行為であっても,通信当事者の同意がある場合には,通信の秘密侵害には当たらない.」[35]

この同意は,通信の秘密という重大な事項についての同意であるから,その意味を正確に理解したうえの真意に基づいた同意でなければ,有効な同意とはいえず,通信当事者の同意は,「個別」かつ「明確」な同意である必要がある,との指摘がある.[36]また一方当事者のみの同意で足りるのか,双方当事者の同意が必要なのかの議論も必要である.

## 4.2 プロバイダ等電気通信事業者等が通信内容（コンテンツ）に関与できることを定めた法律とガイドライン[37]

以下のような法律や、電気通信事業者団体が策定・運用するガイドラインが整備されたことによって,4.1 の基本的な判断枠組みに基づいて,インターネット利用において,電気通信事業者であるプロバイダや他の事業者が「通信の秘密」の構成要件に該当する行為を行っても適法とされるようになっている.

### 4.2.1 プロバイダ責任制限法

3.5.3 で述べたプロバイダ責任制限法では,同法 2 条 1 項に規定される「特定電気通信（不特定の者によって受信されることを目的とする電気通信のうち放送を除く通信）」の規定に該当する情報の発信者が,名誉毀損・プライバシー侵害など権利侵害と思われる情報を発信すると,不特定に人々に受信される.これによって社会的評価の低下などの被害を受けたと主張する人が,法的な救済を求めることがある.

この場合,情報発信が匿名でなされることが多いため,当事者間や訴訟で問題を解決しようとしても,相手方を特定することが困難である.そこで,特定電気通信役務提供者（法2条3項：特定電気通信設備を用いて他人の通信を媒介し,その他特定電気通信設備を他人の用に供する者をいう）であるプロバイダに,情報の削除（送信防止措置）や発信者情報の開示を求めることになる.

ところが,プロバイダは一般に電気通信事業者であるので,「通信の秘密」を厳守しコンテ

---

[35]出典：宍戸・前掲注 4,20 頁

[36]出典：総務省「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会：第二次提言」56 頁,2010 年 5 月

[37]4.2 の記述は,注 2 の文献に多く依拠している.

ンツにノータッチが求められる立場にある.加えて,プロバイダが被害を受けたと主張する人の要求に応じようとすると,発信者の権利を侵害していると発信者から反撃される可能性もあり,いわば両者の間で板挟みに遭うことになる.

この板挟み状態を解消するために,プロバイダにコンテンツへの一定の関与を認め,またこの関与に伴い発生する法的責任を軽減することで被害者救済を図るとともに,プロバイダの法的ジレンマを軽減しようとするのが,プロバイダ責任制限法である.この法律の施行によって,情報の削除や発信者情報開示行為が,プロバイダの正当業務行為であることが認められている.

### 4.2.2 迷惑メール防止法

迷惑メールは,同法で特定電子メール(2条)として,「電子メールを送信する者が,自己または他人の営業につき広告又は宣伝を行うための手段として送信する電子メール」と定義されている.同法は,この特定電子メールの送信を規制することによって,迷惑メールを受取る個人を守るとともに,過剰な負荷などにより通信設備に支障が主ずることを防止しようとするものである.この目的に資するよう,特定商取引法が改定され,取引態様の面からも迷惑メールを規制している.

特定電子メールの送信を規制するためにプロバイダは,OP25(Outbound Port25 Blocking)やIP25B(Inbound Port25 Blocking)といった,送信者のパケット検査を行っている.この行為は外形的(構成要件的)には電気通信事業法4条の「通信の秘密」の侵害ではあるが,受信者の同意を得ている,または同意を得なくとも違法性阻却事由があるため,適法行為であるとされている.

すなわち同法11条に,「電子メールサービスを提供する電気通信事業者(プロバイダ)が,電子メール通信役務の円滑な提供に支障になることを防止するために必要な範囲内において,支障を生じさせるおそれのある電子メールを送信する者に対し,電子メール通信役務の提供を拒むことができる」の規定をおくことで,迷惑メールの送信をブロックすることが適法行為であることを明確にしている.

### 4.2.3 プロバイダ等の関与を規定する各種ガイドライン

インターネット利用に関して,さまざまな好ましくない事案が発生したため,この個別課題を解決するために,プロバイダ等が通信等に関与することに関してのガイドラインが,電気通信事業者団体によって,策定・運用されている.

#### 1)「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 年策定)[38]

自殺予告の対策は,電子掲示板への書き込みを発見した人や,自殺予告を内容とする電子メールを受信した人が,110番通報を行うことが契機となることが多い.通報を受けた警察が自殺防止のために,書き込みをした人や電子メールの送信者を特定するための情報（発信者情報）を入手することが必要になる場合がある.

このような場合には,警察は電子掲示板の管理人やプロバイダに対して,任意で発信者情報の開示を求めることになる.発信者情報は,電気通信事業法4条の「通信の秘密」に該当するため,原則として開示は許されないと解されている.しかも自殺予告に関しては,情報発信者の同意を得ることは通常困難であるため,開示が緊急避難の要件を満たす場合には,発信者情報の開示に関して違法性が阻却されることになって

[38] http://www.kantei.go.jp/jp/singi/it2/others/gaido.pdf

いる.

このガイドラインでは,自殺予告案件に対するプロバイダなどの適切かつ迅速な対応を促進するために,緊急避難の要件を満たす場合には裁判官の発付する令状がなくても開示が許されることを明確にした上で,緊急避難の要件に関する視点・考え方を示すとともに,判断基準や手続きを定めている.

2)「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」[39] (2007 年策定,2011 年第 2 版)

このガイドラインでは,DoS攻撃やDDoS攻撃等のサイバー攻撃,マルウエアの感染拡大,迷惑メールの大量送信および壊れたパケット等を「大量通信等」としている.この大量通信に対して,通信設備を守り円滑なサービスを提供するためには,これらの大量通信等に係る通信を遮断することが必要になる.大量通信等に係る通信を他の通信と識別するためには,通信の構成要素であるヘッダー情報の検知等が必要になるため,(外形的)構成要件的に通信の秘密の侵害行為になると考えられている.したがって,その対応措置が適法行為であると言えるのかどうかが問題となる.

大量通信等では,プロバイダの設備に対して攻撃が行われるケースもあるので,この場合にはプロバイダ自身が通信当事者となるため,通信の秘密の侵害の問題とはなり得ない.その他の場合には,正当業務行為や正当防衛・緊急避難に該当するかが問題になる.大量通信等によるネットワークに対する攻撃への対処策としては,たとえば迷惑メール対策としてOP25B・IP25Bの活用や帯域制御があるが,目的の正当性,行為の必要性,手段の相当性があることが必要である.

また,通信設備に対する攻撃では,設備を防衛することや緊急対応策を講ずる必要性があることから,他の事例とは異なり,正当業務行為以外の違法性阻却事由である正当防衛や緊急避難に該当するケースがあると考えられる.

ただし,正当防衛が成立するためには,急迫不正の侵害が存在していること,また,緊急避難が成立するためには,現在の危難の存在,危機を避けるためにやむを得ずにした行為であること(補充制),避難行為から生じた害が避けようとした害の程度を超えないこと(法益の均衡)が必要である.

3)「帯域制御の運用基準に関するガイドライン」[40](2008 年策定,2010 年・2012 年改定)

ブロードバンドの普及が進展しているなかで,特定少数の利用者がP2Pファイル交換ソフトを利用することで,ネットワーク帯域を多く占有し,ネットワークの混雑や他の利用者の利用を阻害することが問題にされた.

その対策としての帯域制御では,特定アプリケーションのパケットを検知して,当該パケットの流通を制御するので,構成要件的には「通信の秘密」を侵害している.そこで,他の事例と同様に,この行為の適法性の検討が必要になり,プロバイダなどが実施する帯域制御が認められる合理的範囲を定めたのが,このガイドラインである.

また違法性阻却事由がある場合には,当事者の同意がなくとも帯域制御することが許されることになる.帯域制御がプロバイダの正当業務として認められるためには,帯域制御の目的がプロバイダ等の業務内容からみて正当性があること,その目的を達成するために帯域制御を行う必要性があること.加えて帯域制御の方法が妥当なものであることが必要であ

39 http://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf

40 http://www.jaipa.or.jp/other/bandwidth/1203_guidelines.pdf

り,同ガイドラインではその原則をふまえて,具体的な措置の適法性を検討している.

図表2は,上記に述べた各法律・ガイドラインの比較表である.

**図表2 各法律・ガイドラインの比較表[41]**
（プロバイダ等がパケット検査を認められている例）

| 法律・ガイドライン | 対象行為 | 関与の根拠 | 法益 | 検査対象のパケットの種類 |
|---|---|---|---|---|
| A:プロバイダ責任制限法 | 送信防止措置（アクセスブロック）<br>発信者情報開示 | 正当業務行為（法令） | 個人的 | ペイロード<br>IPヘッダー |
| B:迷惑メール防止法 | 送信ブロック | 受信者の同意<br>正当業務行為（法令） | 個人的<br>社会的 | TCPヘッダー |
| C:自殺予告ガイドライン | 警察への発信者情報の開示 | 緊急避難 | 個人的 | IPヘッダー |
| D:大量通信等への対処のガイドライン | 大量通信等の識別のためのパケット情報の取得 | 正当業務行為<br>正当防衛<br>緊急避難 | 社会的 | ヘッダー,ペイロード両方の場合がある |
| E:帯域制御の運用基準のガイドライン | 特定のアプリケーションのパケットを検知,流通を制御 | 正当業務行為 | 社会的 | TCPヘッダー<br>ペイロード |

注1：ペイロード：データ本体（通信内容）,ヘッダー：データの先頭に付加される,データ自身に関する情報で,IPヘッダーやTCPヘッダー等に分かれる.
注2：AおよびCの発信者情報は,通信傍受ではなく,掲示板やブログなどの書込み記録として,サーバに蓄積されている通信内容と送信元のIPアドレスを検査している.
注3：EにおけるP2Pファイル交換ソフトについては,アプリケーションのプロトコルが区々なので,ヘッダーとペイロードの両方の場合がある.

## 4.3 現状の対処の仕組みに関する問題点

インターネット利用に関して,「通信の秘密」の問題に対処している現状は,以上の通りである.すなわち,個別課題について個別に対処策を検討して,新たな法律を制定するか,又は主として電気通信事業者団体がガイドラインを策定・運用することで対処してきた.

プロバイダ等の電気通信事業者は,電気通信事業法で「通信の秘密」の遵守が規定されている一方で,外形的には「通信の秘密」侵害行為を行うことが, 個別課題毎に求められている.

しかしながら,現時点では明確な一般的判断ルールはないため,新たなサービスを始めようとするときなどに,「通信の秘密」に関して、どのような対処策が求められるのかの判断に苦しむ場合が生じている.

一方で,「通信の秘密」の適用を受けない企業が似たようなサービスを行っても,「通信の秘密」に関する制約を受けないのではないかとも考えられ,分かりにくい状況が続いている.

[41] 検査対象のパケットの種類に関しては,JPNIC（一般社団法人 日本ネットワークインフォーメーションセンター）の前村昌紀氏に解説いただいた.謝意を表したい.

2013年6月に報告書をまとめた総務省「パーソナルデータの利用・流通に関する研究会」では,プライバシー保護などに配慮した個人情報の利用や活用に関して,「マルチステークホルダープロセス」が掲げられているが,日本においては実際の当事者である事業者の政策形成プロセスへの取組みが現時点では,必ずしも強くないような印象を受ける.

このような状況にあって2013年9月に,グーグル,ヤフー,eBay,フェイスブック,アマゾン・ジャパン,グリー,DeNAの7社によって「アジアインターネット日本連盟（AICJ）」の設立が発表された.今後の活動としては,インターネット業界,とりわけ上位レイヤーに携わる事業者の声を集約し,日本におけるインターネット政策についての提言・理解促進活動・調査研究等を行うことを掲げており,今後このような動きがどう展開されるのかが注目される.

# 5 「通信の秘密」の法的問題の考察

インターネット利用に関しては,3章で述べたように問題状況が大きく変化したために,従来の「通信の秘密」の理解は大きく変質せざるを得ない状況にある.

「通信の秘密」に関する現実的な変化に,それに関する法的な検討は追いついているのだろうか.「通信の秘密」を取り巻く通信状況が大きく変化したものの,「電気通信事業・郵便事業の民営化以前の状態を念頭に置いて,通信の秘密に関する憲法学説が組み立てられている」[42]との指摘もある.

とはいうものの,「通信の秘密」に関する憲法解釈については,新たな問題状況にふさわしい研究も行われている.本稿において詳細な検討を行う余裕はないが,検討すべきいくつかの課題について,若干の考察を行いたい.

## 5.1 「通信の秘密」の適用事業者[43]

3.6.2 で述べたように,インターネット・サービス提供事業者と「通信の秘密」の関わりが不明確になっている.さしむき,以下の非対称が存在していることについて述べる.

### 5.1.1 電気通信事業者と電気通信事業者ではない事業者との間の非対称

電気通信事業法 4 条 1 項では,「電気通信事業の取扱中に係る通信の秘密は,侵してはならない.」と一般的に規定されており,電気通信事業の従事者の「通信の秘密」の侵害行為に対しては,刑罰加重になっている.（179 条 2 項）

また,同法 164 条に該当する電気通信事業は,同法の適用除外になっているものの,同法 3 条及び 4 条の規定は適用されることになっている.

電気通信事業参入マニュアル[追補版][2005]では,各種情報のオンライン提供,WEB サイトのオンライン検索,オンライン計算処理,電子メールマガジンの配信,電子掲示板など,現在インターネットで多く利用されているサービスは,登録,届出が不要とされている.[44] これ

---

[42]出典：宍戸・前掲 4,16 頁

[43]5.1 の記述は,注 2 の文献に多く依拠している.

[44]出典：総務省電気通信事業部データ通信課「電気通信事業参入マニュアル[追補版]－届出等の要否に関する考え方及び事例」,2005 年.なおこの参入マニュアルは,電気通信ネットワークを利用した多様なサービスを提供しようとする場合に,電気通信事業法で定められている「登録」や「届出」の要否に関する判断基準と事例を示そうとするものである.しかしながら,条文との対応関係が明確に記載されていないし,本

は,164 条 1 項 3 号の「電気通信設備を用いて他人の通信を媒介する電気通信役務以外の電気通信役務を電気通信設備を設置することなく提供する電気通信事業」に該当するためと考えられる.

さらに,インターネット上で Web サイトを開設して自らの情報を発信することや,ネット通販・ネットバンキングサービスを提供することは,電気通信役務には当たるが,それは自己の需要に応ずるためのものだから電気通信事業に当たらず,これらのサービスを行うだけの者は電気通信事業者としての規律は受けない.[45]

なぜなら,電気通信事業とは,2 条 4 号の定義によって,「他人の需要に応ずる」ためのものだから,自己の需要に応ずるためのものは,電気通信事業に該当しないためである.若干分かりにくいが,4 条適用事業者および 164 条適用事業者には「通信の秘密」の規定が適用されるが,自己の需要に応ずるサービスは電気通信事業に該当せず,164 条の適用を受けないので,「通信の秘密」の適用はないものと考えられる.

実際のインターネット上のサービスでは,①上記の 4 条に該当する電気通信事業,②164 条に該当する電気通信事業,および③非電気通信事業の 3 つの類型の事業者が,連携または競合してサービス提供なりビジネスが行われている.このため,利用者からは誰が「通信の秘密」の適用事業者なのかが,分かりにくくなっている.

インターネット・サービスでは,利用者の利用傾向を分析して新しいサービス開発に生かしたり,利用者に合った広告を配信したりするために,利用者の通信情報を分析して,より競争優位にたとうとすべく,事業者相互での競争が行われている.このために,「通信の秘密」の適用事業者とそうではない事業者の間の競争においては,公正競争上の非対称性が生じている可能性がある.

今後,インターネット上で高度で多彩なサービスが提供されることが予想(期待)されるが,この非対称性の問題をどう扱っていったら良いかについての検討が必要であると考える.

### 5.1.2 日米間等における規制制度の非対称性

米国憲法には,「通信の秘密」を直接規定する条文はなく,修正(補正)4 条が「通信の秘密」に該当する条文であるとされている.しかしながら,修正(補正)4 条は「プライバシーの期待」への侵入を禁止するだけで,「通信の秘密」を一般的に保護するものではない.

もっとも個別法では,わが国と同程度に「通信の秘密」を保護する規定があるが,外国諜報活動などに適用される例外を定めた法律も多く,総じて「通信の秘密」にわが国ほどの感度を持って対応しているかどうかは疑わしい.また 3.5.5 で述べたように,米国では伝統的に,コンピュータ・サービス業は電気通信事業ではなく,非規制の自由市場であるとされてきた経緯がある.

そこで,米国出自のグーグルなどの企業は,こうした米国的発想で事業展開しており,また彼らの主たる設備が米国など日本国外に設置されていることから,日本法の適用は受けないものとしている.

わが国の国民にサービスを提供する以上,日本法が提供されると考えるのは常識的であるが,電気通信事業法 4 条の「通信の秘密」の規定は国外適用されない.このため外国の事

---

稿のテーマである「通信の秘密」についての記述はなされていない.

[45]出典:宍戸・前掲注 4,18 頁.前掲注 44,15~16 頁「事例 2 非電気通信事業」参照

業者が国外で行う事業については,電気通信事業法の効力が及ばない.併せて刑罰の適用については,刑法 8 条が適用されるので,電気通信事業法の罰則の国外適用はない.

インターネット上でのサービスの提供や利用は,グローバルな広がりをもって行われているにも関わらず,そのサービスや競争に関する法制度が異なるために,日米等の企業間の競争条件が equal footing になっていないとの指摘が多くなされている.また animal spirit の違いもあるとの指摘も考慮すると,日米間等の企業間の競争条件の違いはさらに大きくなる.

## 5.2 憲法における「通信の秘密」

### 5.2.1 「表現の自由」と「プライバシー保護」

「通信の秘密」の保護法益として鈴木[2008]は,「表現の自由」と「プライバシー保護」の両方としつつも,プライバシー保護に重点を置く学説が多いとしている.[46]

例えば,佐藤[2011]は,「通信の秘密」の保障は,人間のコミュニケーション過程の保護に関わるので,「表現の自由」と密接な関わりがあるが,「表現の自由」が不特定または多数者に向けられるものであるのに対して,「通信の秘密」は個人間の私的接触を可能にする内的コミュニケーションであるので,「私生活の秘密（自由）」ないし「プライバシーの権利」の保護の一環であるとしている.[47]

また「コミュニケーションの私秘性を確保することでプライバシーを守るとともに,通信手段を用いた表現の自由をも保障する性格を有する.」との指摘もある.[48]

他方,「通信の秘密」の保障を「通信の自由」の一環ととらえて「表現の自由」との関連を重視する学説[49]がある一方で,長谷部[2008]は「通信の秘密はプライヴァシーの核心部分の一つであり,憲法はこれをとくにとりあげて明文で保障したもの」[50]としている.

もっとも,このどちらの法益を保護するのかの解釈論に関しては,「当のプライバシーと表現の自由の境界自体が,ほかならぬインターネットによって流動化しつつある」ので,どちらの解釈を採っても,同じような保護範囲であるとの説明は可能であるとする説もある.[51]

### 5.2.2 「通信の秘密」の秘密遵守の名宛人

「通信の秘密」の規定は誰に向けた規定であろうか.「通信の秘密」が国家権力の通信過程への介入を禁止する趣旨であることは,憲法が国家権力の行使に対する制約であるという立憲主義の立場から異論はないであろう.[52]

また,1.2 で述べたように「通信の秘密」が公権力および通信当事者以外の通信を運ぶ

---

[46]出典:鈴木・前掲注 3,136 頁

[47]出典:佐藤・前掲注 7,321 頁

[48]出典:長谷部恭男・中島徹・赤坂正浩・阪口正二郎・本秀紀編「ケースブック憲法[第 4 版]」263 頁,弘文堂,2013 年

[49]出典:阪本昌成「憲法理論Ⅲ」139 頁,成文堂,1995 年

[50]出典:長谷部・前掲注 11,230 頁

[51]出典:宍戸・前掲注 4,26 頁

[52]例えば,愛敬は立憲主義の観点からの憲法理論に関する研究を以下の文献で行っている.愛敬浩二「立憲主義の復活と憲法理論」,日本評論社,2012 年

者の検閲の禁止から信書を保護する「信書の秘密」に由来することを考えても,公権力に対する規定であることは理解できるであろう.

### 5.2.3 私人間効力論

「ケースブック憲法」[2011]では,「平等者相互間における人権の保障は基本的には『私的自治』に委ねられ,争いが生じた場合には必要な最小限のルールは法律によって定められることになっていた.」しかし,私人間が平等という前提が崩れてきた状況で,「法律が不存在あるいは不十分な場合に,裁判所が何らかの形で憲法を適用し人権侵害を救済する理論を形成できないかが模索されるようになってきた.」[53]この問題が私人間効力の問題であるが,同書では 5 つの説をあげている.

このうち,現在では,私的自治の原則とのバランスをとりうるように,法律の一般条項（民法 90 条,709 条が中心）を媒介にして間接適用を考えるべきとする「間接適用説」が有力説であるとされている.例えば,佐藤[2011]は,「間接効力説が妥当であるとする立場が通説化した」[54]とする.

5.2.2 で述べたように,憲法は公権力に対する制約であって,私的自治が原則である私人間の法律関係には,適用されないというのが基本的な解釈である.もしこの立場を堅持するとすれば,私人間の権利侵害を救済・調整する法律が十分に整備されていない場合には,私人間の権利侵害は救済できないことになる.この古典的理解超えて,巨大な企業などの社会的権力を規制するための憲法解釈が,私人間効力論である.

私人間効力論は,企業などの強大な社会的権力が私人間での権利侵害を行った場合に,憲法を通じて規制しようとするものである.ところが「通信の秘密」については,電気通信事業法など法律によって「通信の秘密」の保護を規定しており,憲法にまで立ち返って私人間効力を問題にする余地はないように考えられる.

ところが,4 で述べたように「他人の通信」にノータッチの原則が,インターネット利用では崩れているうえに,5.1 で述べたように「通信の秘密」の適用に関して2つの非対称性がみられ,インターネット利用者からみると,自分の「通信の秘密」が守られているのかどうかについて分かりにくい状況になっている.

むろん,「通信の秘密」に関する権利侵害行為の案件に関して,プライバシー侵害などの理由で,裁判所に損害賠償なり,差し止め命令を求めることも考えられる.「通信の秘密」の保護法益が,プライバシー保護であるとの学説が有力であることを考えると,この領域については,「通信の秘密」,プライバシーの保護領域は重なり合っていることから当然のことと考えられる.

このように「通信の秘密」の保護に関して法律が不十分な場合に,憲法を適用することによって,「通信の秘密」侵害行為を規制する余地もあるように考えられるが,現在の問題状況はさらに大きく変化している.この問題は 6.3 で取上げる.

## 5.3 公然性を有する通信[55]

---

[53]高橋和之編「ケースブック憲法」57～58 頁,有斐閣,2011 年参照

[54]出典：佐藤・前掲注 7,165 頁

[55]5.4 の記述は,注 2 の文献に多く依拠している.

インターネットにおいては通信内容の秘匿性がない「公然性を有する通信」[56]が増加しているが,この公然性を有する通信を「通信の秘密」の観点からどう考えるべきであろうか.

この問題について,「インターネット上の情報伝達であっても,例えば電子メールのように,秘匿性の下で発信者が特定の受信者に対して情報を伝達する構造のものについては,古典的な通信の秘密が及ぶ.」としながらも,「掲示板・ブログ・SNS などを用いた情報発信は,『いわゆる公然性を有した通信』に当たるため,憲法 21 条 2 項の『通信』ではなく,同項 1 項の『表現』に該当すると考えられる」とする説がある.[57]

しかしながら,「公然性を有する通信」といっても,通信の流通過程ではどの通信が通信内容の秘匿性のない通信なのかは分からない.またソーシャルメディアの多くが秘匿性のない通信であるとしても,LINEなどでは公開相手をごく限定的にしている場合があり,必ずしもすべての通信内容に秘匿性がないとはいえない.したがって,通信がなされている流通過程においては,「通信の秘密」は原則として守られるべきと考える.

一方,発信行為が終了してインターネット上に蓄積され,多くの人がアクセスし,通信内容を見ることができるようになった場合には,これはむしろ,通信としてではなく,表現として捉えるべきものとなる.この場合には,表現の自由が原則として適用されることになるが,他の法益,例えば名誉毀損やプライバシー侵害があれば,その表現行為が制約されることになる.

また,匿名による発信行為も表現の自由として認められると考えられるが,仮に匿名であってもインターネット上の他の情報と突合することによって発信者が特定されて,「炎上」や「さらし」という現象を引き起こすことがある.

この問題に対しては,表現と通信の区分を考えれば,「通信の秘密」の法理を適用するのではなく,表現行為を規制する法理,例えば名誉毀損やプライバシー侵害の法理で対処することが適切ではないかと考える.[58]

つまり,「公然性を有する通信」であっても,通信流通過程は「通信の秘密」で保護し,通信終了後にインターネット上で公開された通信内容については,表現として保護もしくは規制されるという考え方である.

したがって,4.1.1で述べたプロバイダ責任制限法においては,匿名でなされた情報発信によって権利侵害されたと考える人が,通信内容である発信情報の削除を求めるのは,「表現の自由」の問題であり,通信の構成要素である発信者情報の開示を求めることは,「通信の秘密」の問題となる.

## 5.4 憲法の「通信の秘密」と法律レベルにおける「通信の秘密」

### 5.4.1 憲法の「通信の秘密」

立憲主義から考えて,憲法の「通信の秘密」に関する規定は,公権力による「通信の秘密」の侵害行為を禁止することが目的である.この観点から,憲法の通説である「通信の秘密」の範囲を,通信内容だけではなく,通信の構成要素などを含めて,広くとることは維持すべきと考える.

---

[56]「公然性を有する通信」という用語は,1996年の郵政省の研究会報告書で,通信と放送の「中間領域的サービス」を意味する用語として,初めて使われた用語で,当初は通信と放送の区分があいまい化したことを意味していた.出典：田川義博「通信・放送産業の地殻的変動と産業融合の進展」,情報通信学会誌 Vol.22No1,2004年5月,21頁

[57]出典：大石眞・大沢秀介[2012]「判例憲法」113～114 頁,有斐閣,2012 年

[58]松井茂記・高橋和之・鈴木秀美編「インターネットと法　第4版」,有斐閣,2010年,49頁では,匿名で表現することも表現の自由に含まれる,としている.

2001 年 9 月 11 日の同時多発テロ事件発生以来,米国では人々の権利が安全を理由にして制限される事例がみられるようになった.愛敬[2012]は,この正当化根拠として,社会安全が確保されてこそ自由の享受が可能になる」との「安全の中の自由論」という法理があると述べている.[59] また 9. 11 以降,脅威の内容と程度に応じて,事前・先制・予防的な対応を行う傾向が強まったとも述べている.齋藤[2005]は,治安としてのセキュリティの台頭と生命/生活のセキュリティの後退を自由の問題として論じている.[60]

西原[2008]は,立憲主義の観点から公権力が人々の権利を制限するためには,以下の命題を満たしていることが必要とする.[61]国家が権力的手段を投入するには,

命題 1:正当化根拠が必要

命題 2:法律上の根拠が必要(形式的法治国家の命題)

命題 3:基本権保障の利益を上回る実質的な正当化根拠が必要(実質的法治国家の命題)

この命題 3 には,①(手段の規制目的に対する)適合性,②(手段は目的達成に必要最小限に限定される)必要性,③(手段は制約される基本権に優越する価値を有する規制目的の達成に資するものに限定される)狭義の比例性,の要素がある.西原は,法律の合憲性コントロールの仕組みのなかで,最も大きな役割を果たすのは命題 3②の比例原則であると述べている.(もっとも、現在はむしろ命題②の役割が大きくなっているとも述べている.)

この権力制限の枠組みが,9.11 以降の安全(テロ防止)を重視するなかで揺らいでいる.愛敬は,米国憲法理論では,「自由と安全のトレードオフ」の議論,すなわち,安全の向上のためには,自由の切り詰めが合理的との議論が大勢となっていると述べつつも,この議論は自由を削減すると安全が自然に高まることを(暗黙の)前提にしているので,テロ対策の現実的な効果を合理的にチェックすることを怠りがちになる,とも述べている.[62]

この現実的な効果を考えるという問題は,刑法における厳罰化傾向にも共通している.厳罰化傾向には,処罰の早期化(抽象的危険も罰する,これは予防的な要素を併せて有している),刑罰の重罰化などが含まれる.[63]しかしながら,いくら厳罰化傾向を推し進めたとしても,犯罪がなくなるわけではなく,さらに厳罰化傾向が際限なく進む恐れがある.

一方,奈良[2007]は,日本人のリスク観の特徴として,リスクに敏感でゼロリスクを求める傾向や安全より安心を重視する傾向を挙げている.[64]

処罰の早期化や安心を求める傾向が強まれば,西原が指摘する公権力が人々の権利を制約する正当化の原則が崩れる恐れがある.この意味で,9.11 以降の「安全の中の自由論」は,公権力と人々の人権との関係を変化させる可能性が大きいと考える.

情報セキュリティ分野でも,図表 3 でみるように国家安全保障が大きな課題となってきている.すでに米国では,2011 年 7 月に国防総省はサイバー空間を陸海空,宇宙についで第

---

[59]出典:愛敬・前掲注 52,203 頁.

[60]齋藤純一「自由」「第 3 章　自由と安全」99～108 頁,岩波書店, 2005 年参照

[61]西原博史 “リスク社会・予防原則・比例原則“,Jurist No.1356,2008.5.1-15,75～81 頁参照

[62]愛敬・前掲注 51,226～235 頁参照

[63]島田聡一郎「リスク社会と刑法」9~35 頁,長谷部恭男等編「リスク学入門 3　法律からみたリスク」,岩波書店参照

[64]出典:奈良由美子編「生活とリスク」197～210 頁,財団法人放送大学教育振興会,2007 年

5 の作戦領域と位置づけ,重要インフラ防衛を含む米軍のサイバー防衛能力を強化する方針を打出している.[65]

国家安全保障分野におけるサイバー空間の防衛能力強化の手法としては,前述した 9.11 以降の予防的措置が含まれる可能性もあり,憲法上も大きな検討テーマになるものと考える.

### 5.4.2 法律レベルの「通信の秘密」

法律レベルでの「通信の秘密」の規定における規制対象は,主として民間事業者である.

「3 インターネット利用が『通信の秘密』など法制度に与える影響」および「『4 通信の秘密』保護に関する電気通信事業者の役割の変化」において述べたように,インターネット利用に関する「通信の秘密」は,電話時代の「通信の秘密」とは大きく変質している.

この問題は,憲法レベルで公権力に対して,厳格に「通信の秘密」保護の遵守を求める観点とは異なり,インターネット利用で期待されている,機会を生かし,脅威を減少させるツメル取組みの法益と「通信の秘密」の保護法益との比較衡量によって,「通信の秘密」の保護範囲を決めていく検討が必要である.

法益の比較衡量に関しては,一方で「通信の秘密」の保護法益がある.他方 3.5 及び 4.2 で述べたインターネット利用に関連する法やガイドラインの保護法益がある. 4.1 で述べたように,プロバイダ等による「通信の秘密」の侵害行為を適法と認める根拠として,刑法理論があり,社会的法益および個人的法益の観点から,違法性阻却理論に基づく検討が行われた結果,現在の法やガイドラインが制定・運用されている.

また,情報セキュリティ分野では,情報セキュリティの意味合い,攻撃者・攻撃意図・攻撃対象などが,図表 3 のように変化していて,ますます状況は広範化,深刻化している.

**図表 3 情報セキュリティ分野における変化**

| | 2001~2003 年 | 2004~2008 年 | 2009~2012 年 |
|---|---|---|---|
| セキュリティの意味合い | サーバーや PC の保護 | 企業・組織の社会的責任 | **リスク(危機)管理・国家安全保障** |
| 攻撃目的 | いたずら | いたずら,金銭 | 同左＋抗議,諜報 |
| 法律 | 不正アクセス禁止法(00),電子署名法(01) | 個人情報保護法全面施行(05),e-文書法(05),日本版 SOX 法(08) | 不正競争防止法改正(10),刑法改正(ウイルス作成罪)(11),不正アクセス禁止法改正(12) |

出典:「2013 年 10 大脅威」IPA,2013 年 3 月 を一部修正

情報セキュリティの対処策における「通信の秘密」は,攻撃者の「通信の秘密」の保障であるので,攻撃行為が違法な場合には「通信の秘密」の保障は及ばない.

インターネット上を流通する膨大な通信(情報)のうち,違法な意図を有する通信(情報)を抽出するためには,検査の効率化、検査コストの低減化をすることがが,実務上の大きな

[65]出典:林紘一郎・田川義博・淺井達雄「セキュリティ経営」39 ページ,勁草書房,2011 年

課題である.またウイルス検知など情報セキュリティ対策では,DPI(Deep Packet Inspection)技術の導入も必要になるが、上記および費用負担の課題をクリアする必要がある。

このような視点も加えて,「通信の秘密」の保護法益を守ることと,インターネット利用の機会と脅威の保護法益を比較衡量して,望ましい法的秩序を形成することが,今後の大きな検討課題である.

「電気通信事業法において憲法と同じ通信の秘密が保護されており,しかもそれが非常に広くかつ強力は保護であると理解されている結果,一般的な個人情報・プライバシー保護を遥かに超える義務が電気通信事業者に課せられている」[66]との指摘がある.

4．3 で述べたように,一方で「通信の秘密」の遵守を求められ,他方で「通信の秘密」の侵害行為を求められている電気通信事業者のジレンマが,現状の仕組みに関する問題点である.上記の指摘の観点からも,このジレンマを少しでも減少させる取組みが求められていると考える.

## 6 おわりに:これからの「通信の秘密」

これからの「通信の秘密」のあり方を考えるうえでの論点として,いくつかの事項について述べておきたい.

### 6.1 「通信の秘密」の範囲

この問題については,以下の宍戸の指摘[67]を取上げたい.

1）情報法の専門家からは,通信の秘密の保護範囲は通信の内容に限られるべきであり,どのサイトにアクセスしたとか,誰が誰と通信を行っているかといった通信の存在それ自体に関する事項は,憲法・電気通信事業法上の通信の秘密の範囲外と考えるべきではないか,という疑問が提起されている.

2)憲法上の通信の秘密の範囲を広く理解することが現在のインターネット環境との関係で適切かどうかという問題提起として受け止めるならば,その指摘には耳を傾けるべきものが多分に含まれているようにも思われる.

この指摘は,「通信の秘密」の範囲として,2.4 で述べた「通信の秘密」と「他人の秘密」の区分に関わる指摘である.[68]

EU 電子プライバシー指令（2002 年）[69]では,2 条で「traffic data」と「communication」

---

[66]出典:宍戸・前掲,24 頁

[67]出典:宍戸・前掲注 4,25 ページ

[68]宍戸のいう「情報の専門家からの疑問の提起」に関しては,以下の文献を参照
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 巻,2006 年,44 頁以下.高橋郁夫・林紘一郎・船橋信・吉田一雄「通信の秘密の数奇な運命（制定法）」情報ネットワーク・ローレビュー 8 巻,2009 年,1 頁以下.

[69] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Of 12 July 2002

を分けたうえで,5 条で「Confidentiality of the communications」を規定し,6 条で traffic data の取り扱いについての規定を置いている.communication は通信内容に,また traffic data は通信の構成要素に該当する用語であると考えられる.

英国の捜査当局の通信の取得を規律する Regulation of Investigatory Powers Act 2000 においても,第 2 章 21 条で communications data と traffic data が区別されており,それぞれ定義が与えられている.これも「通信の秘密」と事業者が業務上得られる「他人の秘密」の区分を伺わせる区分となっている.

このように,欧米の通信に関連する法制度では,「通信の秘密」と「他人の秘密」を区分した法制度が採られているようにも思われ,内容については今後の研究に待ちたい.[70]

## 6.2 「通信の秘密」の再構成に関する一つの提言[71]

「憲法上の通信の秘密には,なお保護に値する核心が厳として存在する一方で,電気通信事業者に対して必要以上の拘束である『過剰』と,本来対処すべき課題に対して少なくとも直接的には機能していないという『過少』の両側面があると,考えられる.」との宍戸の指摘[72]は,本稿の考察を通しても首肯できる指摘と考えられる.

この問題状況に対する一つの提言を行ったのが,多賀谷[1995]である.

多賀谷は注 71 の文献において,「通信の秘密」は音声アナログ電話の時代とブロードバンド時代においては,その技術的基礎が異なっているので,概念を見直すべきとの提言を行っている.この提言が行われた 1995 年は,日本ではまだインターネット利用が普及・拡大する前で,かつブロードバンド環境にもなかった時期であったことから,この提言の先見性に驚かされる.

詳細の内容については注 71 の文献を参照願いたいが,おおよそ以下のような指摘がなされている.

1)音声アナログ電話時代には,形式秘としての「通信の秘密」との捉え方であり,漏えいしないようなシステムにする役割は電気通信事業者に委ねられてきた.
2)この時代には,電気通信事業者以外の者が「通信の秘密」を侵す可能性は低いが,録音装置・コンピュータによる通信データの記録などの形で,通信回線を流通している情報を,キャリア以外の者が実効支配する技術的可能性が高まったので,形式秘としての「通信の秘密」は,情報の保護システムとして不十分になる可能性がある.
3)データ通信において,「通信の秘密」は広い意味での通信セキュリティの一要素にすぎず,「通信の秘密」の保護と並んで,通信にエラーのないこと(完全性の要求),相手方に確実に送信されたことの確認,受信の確認など通信セキュリティの保全が求められる.

---

[70]情報セキュリティ大学院大学が主催する,2013 年 11 月から始まる第 2 期「通信の秘密研究会」では,欧米の「通信の秘密」の法制度に関する調査を行う予定であり,「通信の秘密」と「他人の秘密」の区分に関しても,ヒントが得られることが期待できるので,その成果を待ちたい.

[71]インターネット利用における「通信の秘密」の再構成を考えるときに,示唆に富む議論として以下の文献を参照.多賀谷一照「行政とマルチメディアの法理論」,弘文堂,1995 年,「第三部第一章 『通信の秘密』の現代的意義」190～206 頁

[72]出典:宍戸・前掲注 4,26 頁

多賀谷はこの認識にたって,「通信の秘密」の主観性・形式性が,人格権的な保護の法理に近い外形をもっているのは,音声通信の技術的特徴・制約に負うところが多いとして,「通信の秘密」の再構築に当たって考慮すべき,以下の基本的原則を提言している.

①基本的セキュリティの確保：電気通信事業者が保障すべきなのは,システムとしての通信の秘密総体,通信が安全かつ確実になされることである.

②狭義の「通信の秘密」の概念：「通信の秘密」の概念は,通信のすべてではなく,人と人との間の私的な 1 対 1 の通話の実質をもつものに限定して維持されるべき.

③他の法益による通信内容の保障：②によって,「通信の秘密」として保護されない通信も,プライバシー保護,営業秘密の保護,消費者の保護など,他の法益の観点から保護の対象になる.

④「通信の秘密」のソフト的な捉え方・暗号処理：企業等がその営業用途などの重要な通信を行う場合には,一般レベルでの「通信の秘密」では従来からセキュリティレベルとして不十分.21 世紀においては,通信内容の秘密保護・セキュリティ保護の重点は,回線のセキュリティから暗号鍵による保護に移っていることであろう.

以上のような提言は,2 章で述べた従来の「通信の秘密」の法解釈とはかけ離れている.また 3～5 章における考察ともかい離が大きいが,基本的な発想としては共通する部分があるように考えられる.

しかしながら,6.1 や 6.3 で述べる考察および「通信の秘密」を取り巻く通信状況が大きく変化しているのに,「電気通信事業・郵便事業の民営化以前の状態を念頭に置いて,通信の秘密に関する憲法学説が組み立てられている」との宍戸の指摘（注 42 参照）を考慮すれば,多賀谷のいうように,情報セキュリティやプライバシー保護の問題とも関連づけて,インターネット利用にふさわしい「通信の秘密」概念を再構築する意義は大きいと考える.[73]

## 6.3 インターネット利用において解決が迫られる新たな課題

「通信の秘密」の保障については,1.2 で述べたように憲法上の名宛人は国家であり,公権力の通信への介入から通信当事者を守ることが趣旨であった.しかしながら現実的には,通信当事者から預かった通信を運んでいる電気通信事業者が,「他人の通信」にノータッチを求めることで,通信当事者の「通信の秘密」を保護しようとするのが,電気通信事業法などの法であることは,1 において述べた.

5.2.3 における私人間効力説は,一国のなかに閉じた問題を解決するには,有効な説であると考えられるが,「通信の秘密」の事業者間での非対称性は,インターネット利用のグローバル化のなかでも生じているため,一国の憲法で解決することには困難性がある.

現在はインターネット利用に関するビジネスの主要部分は,Google のようなグローバルにビジネスを展開しているインターネット企業が担っているので,一国の法制度によって対処する有効性が問われているのである.

この難問に関して曽我部[2012]は,「国家による規制が実際上容易ではなく」,自由の規

---

[73] その後のインターネットの展開過程で、アーキテクチャーとしてセキュリティへの配慮が希薄であったことが明らかになったが、そのことをもって論者の指摘が先駆的であったことを否定することにはならないと考える。

制について「法による規制等と並んでいわゆるアーキテクチャーによる規制が多用され」,「このような規制方式には自由を脅かす固有の問題がある.」,[74]「今日,世界的なネット企業に対抗する重要な手段として,憲法ではなく,市場の働きを支える競争法が用いられているのは理由がある.」[75]と指摘している.[76]

この観点からは,グローバルに展開されるインターネット・ビジネスに関しては,一国の法制度で対抗することは困難であり,グローバルな政策・法制度のハーモナイゼーションが必要である.また,ハーモナイゼーションの対象は,「通信の秘密」,プライバシー・個人情報保護および情報セキュリティと広い分野であることが望ましいと考える.

**参考/引用文献**

愛敬浩二「立憲主義の復活と憲法理論」,日本評論社,2012 年
芦部信喜,高橋和之補訂「憲法　第 5 版」,岩波書店,2011 年
宇賀克也・長谷部恭男編「情報法」,有斐閣,2012 年
大石眞・大沢秀介「判例憲法」,有斐閣,2012 年
大石眞・石川健治編「憲法の争点」Jurist 増刊,2008 年 12 月 15 日号
片桐裕　“70　電話の逆探知,通話の録音等”前田正道編「法制意見百選」,有斐閣,1986 年
金光昭・吉田修三「公衆電気通信法解説」,日信出版,1953 年
齋藤純一「自由」,岩波書店,2005 年
阪本昌成「憲法理論Ⅲ」,成文堂,1995 年
佐藤幸治「日本国憲法」,成文堂,2011 年
宍戸常寿　“通信の秘密について”,http:www.win-cls.sakura.ne.jp/pdf/35/02.pdf
渋谷秀樹「憲法　第 2 版」,有斐閣,2013 年
島田聡一郎　“リスク社会と刑法”長谷部恭男等編「リスク学入門 3　法律からみたリスク」,岩波書店
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　Rethinking ‘Secrecy of Communications’ in the Internet Age」,2013 年
総務省「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会：第二次提言」,2010 年 5 月
総務省電気通信事業部データ通信課「電気通信事業参入マニュアル[追補版]－届出等の要否に関する考え方及び事例」,2005 年

---

[74]出典：曽我部真裕　“自由権―情報社会におけるその変容”,特集憲法入門 13 頁,法学セミナー,日本評論社,2012 年

[75]出典：曽我部・前掲注 74,14 頁

[76]本稿でもこのような問題認識に基づいて,「通信の秘密」の問題を考察するためには,3.1～3.4 で述べたようにインターネット利用の全体的な状況を把握・分析し,これに対応する政策・法制度整備に関して,インターネット・ビジネスを含む 4 つの領域の把握・分析が不可欠と考えて,3.5 において考察を行った.

曽我部真裕 “自由権—情報社会におけるその変容”,特集憲法入門,法学セミナー,日本評論社,2012 年
高橋和之 “人権論の論証構造—「人権の正当化」論と「人権制限の正当化」論(Ⅰ)”, ジュリスト No.1421 2011.4.15
高橋和之編「ケースブック憲法」,有斐閣,2011 年
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 巻,2006 年
高橋郁夫・林紘一郎・船橋信・吉田一雄 “通信の秘密の数奇な運命(制定法)”情報ネットワーク・ローレビュー8 巻,2009 年
多賀谷一照「行政とマルチメディアの法理論」,弘文堂,1995 年
田川義博 “インターネット利用におけるガバナンスのあり方—自由・創造と秩序・安全のはざまのなかで—”,上智大学「コミュニケーション研究」第 43 号,2013 年
http://repository.cc.sophia.ac.jp/dspace/bitstream/123456789/34915/1/200000016987_000132000_27.pdf
田川義博 “通信・放送産業の地殻的変動と産業融合の進展”,情報通信学会誌 Vol.22No1,2004 年 5 月
電気通信関係法コンメンタール編集委員会編「電気通信関係法詳解＜下巻＞」,一二三書房,1973 年
電気通信法制研究会「逐条解説　電気通信事業法」,第一法規出版会 1987 年
奈良由美子編「生活とリスク」,財団法人放送大学教育振興会,2007 年
長谷部恭男「憲法　第 4 版」,新世社,2008 年
長谷部恭男・中島徹・赤坂正浩・阪口正二郎・本秀紀編「ケースブック憲法[第 4 版]」,弘文堂,2013 年
林紘一郎・田川義博「『心地よい DPI(Deep Packet Inspection)』と『程よい通信の秘密』」,情報セキュリティ大学院大学紀要,2012 年
林紘一郎・田川義博・淺井達雄「セキュリティ経営」,勁草書房,2011 年
林紘一郎・湯川抗・田川義博「進化するネットワーキング」,NTT 出版,2006 年
松井茂記・高橋和之・鈴木秀美編「インターネットと法　第 4 版」,有斐閣,2010 年
郵務局業務課内郵便法例研究会編「郵便法概説」,(財)通信事業教育振興会,1982 年
DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Of 12 July 2002
Regulation of Investigatory Powers Act 2000
http://www.nikkei.com/article/DGXNASDG14024_U3A610C1CC0000/
http://www.kantei.go.jp/jp/singi/it2/others/gaido.pdf
http://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf
http://www.jaipa.or.jp/other/bandwidth/1203_guidelines.pdf
Oxman, Jason,“The FCC and the Unregulation of the Internet”, OPP Working Paper,No.31, Office of Plans and Policy, FCC, 1999 年