「心地よい DPI（Deep Packet Inspection）」と「程よい通信の秘密」

林紘一郎[1]・田川義博[2]

概 要

「通信の秘密」を守ることは,電気通信事業を他の事業から区別する産業倫理であり,「言論の自由」の守り手として不可欠の要素でもある.しかし,その運用過程で生まれた,「通信の秘密」と「他人の秘密」を同一視する原理主義的な解釈は,インターネットの時代には再検討を要する.他方で,技術的に可能なものは必ず実現されるべきだという「技術優先主義」も,また原理主義的に過ぎ,かつ日米の規制環境の違いから「公正な競争」が行なわれない恐れが強い.本稿はこのような問題意識から,DPI という技術を素材とした両者の望ましい関係を,史実の分析やケース・スタディによって再検討するものである.

結論は,「技術絶対主義」を緩和した「心地よい DPI」の可能性を探る一方で,「厳格な通信の秘密」に代わる「程よい通信の秘密」を模索することである.これは,あまりに常識的だが,常識を実現するための具体策として,① オプト・インかオプト・アウトかといった二者択一ではない選択肢の提示,② 「通信内容」と「他人の秘密」の峻別と,新しい時代にふさわしいサンクション制度の見直し,③ 電気通信事業者ではない ISP の認知,④ 違法性阻却説から構成要件該当性否認説へ,といった新しい考え方も併せて提案したい[3].

1 問題意識

「通信の秘密」を守ることは,電気通信事業を他の事業（とりわけ類似の産業）から区別する産業倫理であり,「言論の自由」の守り手として社会の信頼を得るために,不可欠の要素である.俗に「メディア産業」と呼ばれる諸産業は,参入や撤退などの「Conduit（経済的）規制」と,送信内容に関わる「Content（社会的）規制」の二つの要素で区分され[4],「P = Publishing 型」（規制は一切ない）,「B = Broadcasting 型」（Conduit 規制も Content 規制もあり）,「C = Common Carrier 型」（Conduit 規制のみあり）に 3 分される（林 [2005a]）.

---

1 情報セキュリティ大学院大学教授

2 情報セキュリティ大学院大学セキュアシステム研究所客員研究員

3 これら 4 点の提案は,過去に例のない新規性を持つものである.また,高橋・林・舟橋・吉田 [2008] における林の立場からは,かなり逸脱するものでもある.

4 ここで「規制」があるとは,民法や刑法などの一般法の規定を超えて,業法で定められた産業に固有の規律があることを意味する.

ここで C 型の理念は,「媒介する通信内容に触れてはならない」ということであり[5].それはそれで意味のある産業倫理である.しかし「通信の秘密」の概念が運用される過程で,「原理主義」とでも呼ぶべき硬直的解釈をもたらしている危険がある.憲法にも定められた概念であり,また検閲が当たり前であった戦前の苦い経験に照らして,厳格な解釈に意味があったことも事実であろう.しかし時代は急速に変わりつつある.郵便の時代から維持されてきた同概念が,回線交換型ならともかくパケット通信型のインターネットに,そのまま適用できるとは限らない.

他方で,アメリカ合衆国(以下,アメリカという)系の IT 企業の間で散見される,「技術的に可能なものは必ず実現されるべきだ」という「技術優先主義」も,また原理主義的に過ぎる.インターネットが可能にすることは前例のないことがほとんどだから,「やってみなければ分からない」というのも事実であろう.しかし,新技術に伴う弊害を除去する努力を惜しまないことは,技術を開発する努力と同程度に評価されてしかるべきであろう.

この点に関する最近の話題の中心は,DPI (Deep Packet Inspection)という技術である.本稿は,DPI を素材としてた両者の望ましい関係を,史実の分析やケース・スタディによって再検討しようとする試みである.結論は,DPI 絶対主義を緩和した「心地よい DPI」の可能性を探る一方で,「硬直的な通信の秘密」に代わる「程よい通信の秘密」を模索することである.共著者がこのような問題意識を持つに至った経緯は,以下の 3 つの側面がないまぜになった,実体験に基づくものである.

1.1 「通信の秘密」のあまりに硬直的な解釈

共著者の 2 人は,旧電電公社に入社し,民営化後の NTT とその関連会社等も含めて,30 年余の通信ビジネスの経験を持つ者である.そのため,「通信の秘密」が,電気通信事業者の社会的使命としても産業倫理としても,如何に大切であるかを骨身に沁みて感じている.1985 年の通信の自由化後に参入した事業者の中に,こうした意識が欠如したり希薄な例が見られると,憤りさえ感じてしまう[6].

しかし私たちは研究者としての経験も積んできたから,わが国の「通信の秘密」の運用実態が他国に比べて必要以上に厳格ではないか,と疑ってもいる.例えば,共著者が経験した事例に,以下のようなものがあった.まだ電報が重要な地位を占めていた時代のことである.電信電話取扱者コンクールという催しで,みすぼらしい服装で疲れきった様子の女性[7]から「お母さん,お世話になりました.先に参ります.」という趣旨の電文の送信を依頼された窓口担当者が,どう行動すべきかというテストがあった.正解は「黙って受け付けよ.通信の内容に踏み込むことは許されない」とされたが,違和感を禁じ得なかった[8].

---

5 これは「コモン・キャリア」と呼ばれる諸産業,例えば宅配ビジネスにも通ずる産業倫理である(林 [1984][1989]参照).後述の DPI と宅配業務との比較は,このような認識から出ている.

6 捜査令状によるサーバの押収が問題になった最初のケースであるベッコアメ事件(1996 年 1 月)において,サーバを丸ごと押収していく警察を阻止するでもなく傍観していた事業者が,その典型的な例である.

7 プロの女優に依頼しており,迫真の演技であった.

8 このような厳格な解釈が浸透したのは,後述の吉展ちゃん事件とほぼ同じ頃,現実に起きた事件の影響もあったかと思われる.電話交換手が強姦被害者の 110 番通報を傍受し,同僚の交換手に漏らし,その同僚が美容院で話

この設例が投げかけたものは,「通信の秘密を守ることは常に,他の諸価値を守ること以上に大切なことなのだろうか」という問いかけと言ってもよい[9].特に林は,高橋弁護士等との共同研究において,憲法と電気通信事業法における「通信の秘密」の規定が辿った「数奇な運命」を知って以来,この疑問が頭から去らない(高橋・吉田[2006],高橋・林・舟橋・吉田 [2008]).

硬直的運用の典型は,例外を設けることに対して禁止的に厳しいことであり,代表例は,インテリジェンス(知性や理解力といった一般用語ではなく,諜報の意)活動のための通信傍受を認めないことである.インテリジェンスの手段としての通信傍受はSIGINT(SIGnal INTelligence)と呼ばれ,私たちのように「情報セキュリティ」を研究対象にしている者からすれば国際常識に属するが,わが国では法的に認められていない.

インテリジェンスの世界の傍受は,犯罪捜査のための傍受(「司法傍受」)と異なり,実施主体が行政庁であり(「行政傍受」),一般的な司法手続きとは別建てになるのが普通である.そこでは,どのような手続きなら濫用を防止し,国民の基本的人権を守ることができるかが問題となる[10].何らかの形で裁判所が関与することが望ましいが,司法傍受と同じ令状主義を適用したのでは,機密性と迅速性を求める行政の要請に応えられない.その両者のバランスを取る必要がある.

しかしこのような議論は,平和主義を盲信する人が多い我が国では,タブーに近い.そこで本稿ではこの論議には直接触れず,「行政傍受」に関する論議は他の専門家に任せたい[11].言い換えれば,本稿で取り扱う対象は,DPI のような技術と通信の秘密の関係という,いわば「日常的な通信の秘密」に限ることにしたい.

日常生活においても「通信の秘密」は大切だが,犯罪捜査のための緊急措置としての通信傍受は,1963 年の吉展ちゃん事件を契機として,一般に認められるようになった[12].しかし,それはあくまでも緊急時の例外処理であり,傍受の要件をパターン化して法的に認知することには抵抗が強かったが[13],国際的な組織犯罪が注目されるようになり,国際捜査協力が必須になると,わが国だけが独自路線を貫くことはできなくなる.こうした潮流に押されて,わが国でもやっと 2002 年に「通信傍受法」が制定された(制定に至る経緯につては,井上 [1997] 参照).

したため,広い範囲に知られることとなった.傍受者は依願退職,同僚は懲戒解雇となったため後者が提訴したが,一・二審とも棄却(福知山電報電話局事件.大阪高判 1967 年 12 月 25 日,判例時報 514 号 82 ページ,判例タイムズ 218 号 226 ページ).

9 その後しばらくして,「通信の従事者もまた人間であり,問題の設定自体があまりに非人間的」ということになり,他の設問に変えられた.

10 アメリカでは,FISA(Foreign Intelligence Surveillance Act)による別途の令状や,大統領令による傍受が許されている.後者については,9・11 以降のテロ対策とはいえ,国民の基本的人権を侵害する恐れが強いとの批判が絶えない.

11 わが国にはこの種の専門家が不足しているが,例えば土屋 [2009] は優れた分析である.

12 吉展ちゃん(誘拐殺人)事件とは,1963 年 3 月 31 日に東京都台東区入谷(現在の松が谷)で起きた,男児誘拐殺人事件である.犯人からの身代金を要求する電話が入り,家族が吉展ちゃんの安否を確認するよう求め電話を引き延ばした結果,犯人からの電話の録音に成功したが,当時は犯人の架電してきた番号の逆探知が法的に許容されないとされ,また技術的にも困難であったために,犯人の所在までは突き止めることができなかった(高橋・林・舟橋・吉田 [2009]).

13 傍受の実務においては,通信設備を保有する事業者の協力が不可欠であるが,NTT 等の事業者は腰が引けていた.事業者の労働組合は,更に非協力的であった.

その運用実績は年間 20～30 件ほどの令状発行しかなく,法の実効性の点では問題が多いが[14],曲がりなりにも,通信の秘密に対する例外処理のパターン化の先駆けとして,「犯罪捜査のための通信傍受」が法制化された意義は大きい.一部の国家がテロを黙認したり,陰で支援したりしている現状では,犯罪捜査とテロ対策が交錯している部分もある.平和国家日本としては,実力不相応のインテリジェンスを論ずるよりも,地道な犯罪捜査の面から,国際貢献をしていくのが近道かもしれない.

1.2 憲法的保護と事業法による保護の二重構造

「通信の秘密」は,日本国憲法にも定められた基本的人権の 1 つである(憲法 21 条 2 項後段).この条文の名宛人(法律が想定する受取人)は,憲法という法律の性格上[15],一義的には国家ないしそれに準ずる公共機関である.したがって傍受の問題は,(司法傍受にせよ行政傍受にせよ)国家とそれに準ずる機関が傍受を実施しようとし,「通信の秘密」を上回る「傍受の必要性」があると主張した際に,どう捌いたら良いかが主たる論点である.

しかし「他人の通信の媒介」を業とする者,すなわち電気通信事業法(以下,単に「事業法」)第 2 章の適用を受ける「電気通信事業者」(以下単に「事業者」)が通信の秘密を守らないと,国家が守らないと同様か,それ以上の権利の侵害につながりかねない[16].そこで,業法としての「事業法」には,改めて「通信の秘密」を守る義務が規定されており(4 条),その違反には刑事罰が科される(179 条)[17].加えて憲法の要請を受けて,「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)という規定は,電気通信事業者に限らず「何人も侵してはならない」義務だとされている.現に 179 条には,事業者以外の者に対する罰則が想定されている[18].

ところで従来の電話中心のシステムは,独占的事業者が提供していたから,「事業者」でない一般の個人が「通信の秘密」を侵すことは,故意に傍受を試みるのでなければ,ほぼあり得ないことであった[19].ところが,通信ネットワークの中心がインターネットに移り,電話に代表される旧来のメディアを凌駕していくにつれて,新たなタイプの事業者や,事業者か単なるネットワークの利用者かが判然としないサービス提供者

---

14 通信傍受法により,毎年の令状の発行件数等を国会に報告することになっており,それによれば直近の 2010 年中の実績は 27 件である.これは「行政傍受」が年間 2,000 件以上もあるアメリカと比べれば,1%程度にすぎない.http://www.mhlw.go.jp/stf/houdou/2r98520000021ql1.html
(2012 年8月 20 日アクセス.なお以下のウエブ引用は,すべて同日にアクセスしたもの).

15 実は,憲法で「通信の秘密」を保護している国は,ごく例外的である.ただし,憲法に定めがないことが,直ちに「保護のレベルが低い」ことにつながる訳ではない.

16 これは市場を自由化した後の「後付け」の説明であり,電気通信事業はアメリカ以外の先進国では国営で実施されてきたので,民営化以前は憲法の私人間効力を論ずるまでもなかった.

17 これはいわば通説的説明であるが,憲法が途中まで「secrecy of any means of communication」という表現で検討されていたことを知れば,現在のあまりに「メディアとしての通信」に偏り,非電磁的な会話などへの適用を排除する法制と解釈は,本来の秘密保持の考えに合致していたのだろうかという疑問が生ずる(高橋・吉田[2006]).

18 もっとも「通信の秘密」ではない「他人の秘密」にも,この罰則が及ぶか否かについては,後述のように「罪刑法定主義」の観点から疑念がある.

19 無線の場合は,偶然傍受することがあり得る.法もそのことを心得ているから,有線の場合は「傍受」しただけで違法となるが(有線電気通信法 9 条),無線の場合には「傍受し漏えい」しなければ犯罪とならない(電波法 109 条).

が登場している[20].そこで,このような新種のサービス提供者に関しても,従来の通信の秘密の概念をそのまま適用できるか否かが問題になりつつある.

この点については,日米の間に規制環境の大きな違いがあるため,注意が必要である.アメリカでは,連邦政府の規制権限が連邦憲法に明記されたものに限定されると考えられているため,1934 年通信法(とその改正法)に基づいて連邦通信委員会(FCC)に規制権限があるのは,従来の電話サービスを中心とした「基本サービス」(basic service)のうち州をまたがる通信についてのみであり,「高度サービス」(enhanced service)については規制権限がない.つまり「自由市場」と考えられてきた(林 [1989]).この考え方は,1934 年法の抜本改正法である 1996 年法においても,「電気通信サービス(telecommunications service)」と「情報サービス(information service)」の差として維持されている(郵政省郵政研究所 [1997]).

アメリカでは大手通信事業者も,ケーブル事業者とともに ISP 事業を営んでいる.彼らの主たる業務は「電気通信サービス」に属し規制対象になっているが,同時に提供するインターネット・サービスについては,クリントン政権以降,産業育成の観点から「情報サービス」であるとして「非規制」(unregulation)政策が継続されている(林 [2002]).従って,「通信の秘密」がことさら問題になることはない.

これに対してわが国では,「官」に対する漠然とした信頼感と依頼心があって,アメリカ的な権限の明確化がないままに,規制が正当化される雰囲気がある.電気通信の自由化(1985 年)当初は,「第一種電気通信事業者」「第二種電気通信事業者」という二分法が採用されていた.NTT などインフラ部分を持つ事業者が「一種」で,いわゆる VAN (Value Added Service) 提供者が「二種」である.それ以外に,「通信事業者ではない情報処理業者」が存在し得た.規制を避けたいという志向の強いアメリカの事業者であったなら,より規制が緩やかな「情報処理事業者」としてのビジネス展開を選んだであろう.私たちも,そのように想定し慫慂してもいたが(林 [1984]),予想は完全に裏切られた.

加えて,いわゆる NTT 分割論議の余波を受けて,NTT 東西会社が自ら ISP 事業を営むことが嫌われたため,NTT グループでは,NTT コミュニケーションズを含めて,ISP 事業は分離子会社によって提供されている.しかし「通信の秘密」の規定は,これらの子会社にも適用されるというのが世間一般の理解である.

1.3 インターネット以降の問題

この点に関しては実際に不都合が生じていて,事業者も政策当局も人知れず悩んでいると思われる[21].不都合の典型的事例が,広義の DPI(その定義は次節で試みる)によるフィルタリング(スパムや児童ポルノ),帯域制御,ログの保全,行動ターゲティング広告などの是非である.加えて前述のとおり,アメリカの ISP(Internet Service Provider)は,通信事業者とされていないから「通信の秘密」を気にしない

[20] 2003 年の「事業法」の全面改正まで「第2種電気通信事業者」という範疇があった者が,その後 ISP に業容転換したため,わが国ではほとんどの ISP が「事業者」となっている.

[21] 私たちは林・田川 [1994] において,ユニバーサル・サービスという 100 年余の歴史を持つ概念が,インターネット時代にも適用可能か,可能だとすればどのような修正が必要か,を論じたことがある(林・田川 [1995]).本稿は,同様のアプローチで「通信の秘密」を再考することとも言える.

で事業を行なっているが,わが国ではほとんどの ISP が「事業者」であり,それに硬直的運用が輪をかけて,事業活動が萎縮しているのではと懸念される[22].

このうちフィルタリングは歴史的にも古く,今日ではスパム・メール対策として日常化した感もある.通信の受信者が,自らフィルタリング・ソフトを使っているなら問題ない.しかし ISP に依頼しているのだとすれば,そして ISP が「事業者」であるとすれば,「通信の秘密に抵触しないか」という疑問が生ずるが,ISP は加入者の依頼を受けてフィルタリングしているのだから,(違法性がない)正当な行為だという立論は成り立つ.さらには後述 4.2 の迷惑メール対策法のように,法によって正当業務行為の範囲を明確化するのは,それなりに有効である.

問題は,フィルタリングの正当化根拠が,そのまま他の DPI にも適用できるか否かである.これはかなり微妙で,ケース・バイ・ケースで考えざるを得ないと思われる.しかし,それでは事業者は DPI 技術を利用していないのだろうか? それを信ずる人は誰もいまい.今や世界をリードするアメリカ系の IT 企業は,皆行動ターゲティング広告に近い DPI を堂々と実施している[23].一方,日本の企業は皆「お行儀が良い」から,これらを「秘めやかに」実施するか,実施を抑制しているのではないかと推測される.このような状態が継続するのは,望ましいことではない.その理由は主として次の 2 点である.

第1は,公正な競争基盤(Level Playing Field)が成り立たないことである.仮に,アメリカ系企業が自由に DPI を実施し,日本の企業が自粛したとすれば,ただでさえ競争力に劣る日本の企業は,将来とも追いつけないほどのハンディを負うかもしれない[24].といって,日本の企業に自由にやりなさいと推奨することもできない.私たちのようなビジネス経験をもつ者からすれば,通信の秘密は他の法益が優先するとして簡単に放棄して良いような,価値が低いものではないし,昨今の日本企業は著しく行政の意向を慮る(逆に言えばアニマル・スピリットに欠ける)傾向があるからである.

第2の理由は,合法・違法の判断がつかないような事案を市場の決定に委ねることの弊害である.法(ないしはそれに代わる,ガイドラインなどのソフトロー)が欠けていると,事態は両極端に振れる傾向がある.ある場合には,「法がないことは,やっても良い」こととされ,他の場合には「法がないことは,すべて禁止」と受け取られることもある(アメリカは前者に,日本は後者に傾きがちなことは,過去の経験から明らかであろう).どちらのケースも望ましい状態から逸脱していることは言うまでもない.

そこで「このようなアンバランスをどう調和させたら良いか」が本稿の課題である.つまり「好き勝手に DPI をやって良い」や,「通信の秘密に例外なし」といった両極端を否定して,「心地よい DPI」と「程よい通信の秘密」という,需要側と供給側の利益や,

---

22 市場経済に慣れている読者からは信じてもらえないだろうが,わが国の ISP は,規制がない自由市場を選ぶのではなく,自ら進んで規制がある「第2種電気通信事業者」の認可(または登録)を求めたのである.前掲の注 18.を併せて参照のこと.

23 Google や Amazon 等のリーダー企業が,「プライバシー・ポリシー」の中で,「事業売却の際には個人データも含めて売却の対象にする」旨の宣言をしているのは,DPI を実施していることの「一応の証拠」(prima facie evidence) となろう.

24 共著者の 1 人である林は,ヤフーがグーグルの検索エンジンを使うことが独禁法上の問題となった際,グーグルのアニマル・スピリットを支持する論議を展開したが,その最大の論拠は「市場を萎縮させない」ことであった(林[2010])

公益と私益のバランスを取る方法を,模索しようとするものである.

その際に検討すべき諸点は,以下のようなものかと思われる.

- ISP は実態上 DPI をある程度利用していると思われるが,法的には認知されていない.DPI にも ① ヘッダ情報だけを見る,② ペイロードの部分も見る,の 2 種類があるが,まず前者は誰でも自由とすべきか?
- 他方,「事業者」は ① は許されるが,② は認められないこととすべきか?
- そもそも,ISP は「事業者」か?(わが国では,規制当局からも,ユーザからも,事業者自身の認識でも,「事業者」であることを,暗黙の前提にしている?)
- このような検討を勧めることは,わが国では「危険な発想」と思われているが,闇に隠すよりも「明るみに出して制限を課す」方がより安全と観念すべきではないか?
- また産業政策の面からは,どのような施策により ISP の営業の自由と発展を促すことができるか?

2 DPI の何が問題か?

DPI に関する問題は,なかなか分かりにくい.インターネットが一般的にブラック・ボックス化して分かりにくいことに加えて,DPI が他の技術と「あわせ技」で使われるものであり[25],加えて一部では「白日の下に晒されず,密かに行なわれている」ことが,分かりにくさを助長しているかと思われる.そこで本節では,本論に入る前に必要な範囲で解説を試みる.

2.1 DPI の定義

残念なことに,肝心の DPI という語は広狭さまざまな意味で用いられているので,ここでは大元 [2010] に依拠しながら,必要最低限の要件を押えておこう[26].

インターネットで使われているパケット交換方式とは,情報をパケット(小包)という単位に区切ってバケツリレー式に転送し,最終目的地に届ける方式である.その際,パケットのヘッダには,発信アドレスと着信アドレスが格納されていて,ルータがこれを読むことによって転送先が判断される.併せて,どのような規格のパケットなら次に転送してよいかの判断も,同じくヘッダにあるプロトコルの表記を読んで行なわれる.

商用化直後のインターネットには,FTP,Telnet,SMTP,NEWS 等々,様々なプロトコルのパケットが流れていた.ネットワーク管理者は,このうち自分たちが利用するプロトコルのみ許可し他を排除することで,外部からの不正侵入を防いでいた.その際 ACL (Access List Control) と呼ばれるパケット・フィルタリング技術が一般的であった.これは,通信の IP アドレスとプロトコル種別を判読し,通過して良い通信と拒否

---

25 この点を要領よく解説したものとして,佐藤慶浩氏のブログがある.
http://yoshihiro.cocolog-nifty.com/postit/2010/06/post-bfef.html

26 本文で引用した記述は,DPI に好意的なものかと思われる.やや批判的な解説としては,以下のものがある.「《deep packet inspection》インターネットの利用者とサーバの間でやりとりされるデータ(正確にはパケットの制御情報)を第三者が検査する技術.ファイル交換ソフトなどの過度な利用により,ネット渋滞を未然に防ぐために用いられる.利用者の趣向や行動を把握した上で配信する行動ターゲティング広告への利用の是非が議論されているほか,情報漏洩や盗聴の危険性の指摘もある.」(http://dictionary.goo.ne.jp/leaf/jn2/243627/m0u/)

する通信を判断する技術である.つまりヘッダ情報だけで,判定可能であった.

しかしインターネットの普及が進むと,アプリケーション毎に異なるプロトコルを利用していたのでは不便なので,次第に HTTP 上で実行されるようになった.ファイル交換もメールを読むのも含めて,「いつしか『HTTP is TCP』と言っていい程,様々なアプリケーションが HTTP で処理されるように」(大元 [2010])なった.

「HTTP」を許可しておけば,掲示板への書き込みも,メールの送信もでき便利である反面,攻撃者も HTTP でサーバへの不正侵入までできる.こうなると,プロトコルの種別で「通過」「拒否」を判断していた ACL では役に立たなくなってきたので,代わりに登場したのが「メッセージ内容」で判断するための高度な検査技術,すなわち「DPI」というわけである.

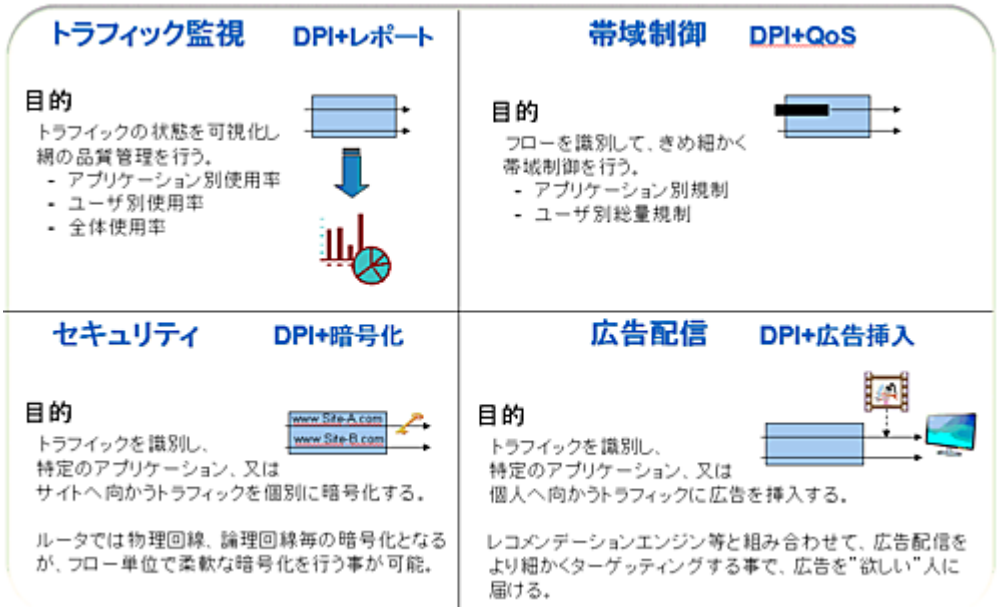
そこで,改めて DPI(Deep Packet Inspection)とは何かといえば,Inspection(検査)が示す通りパケット検査技術の一つである. パケット・フィルター(ACL)は通常 Layer3 と Layer 4 を対象としていたが,DPI では payload(通信の内容そのもの)まで見ることによって,更に上位層の情報,例えば URL やメッセージに含まれる内容や,パケットの振る舞いまで検査することが可能になった.

これによって HTTP を利用して侵入しようとするウィルスの検出などや,企業における情報漏洩対策が可能になったのである.DPI を利用したセキュリティ対策として,最も一般的なのは,Firewall と IPS(Intrusion Protection System),URL フィルタリングの組み合わせである.これは,アダルトサイトへの URL が含まれた通信や,SQL サーバや WEB サーバ等を攻撃する URL が含まれた通信等を検出するのに役立つ[27].

しかし今日では,その用途は,少なくとも次の 4 つに拡張されている,と大元 [2010] は主張している(図表 1. 参照).本稿で検討しようとするには,右側の帯域制御と広告配信が主であるが,DPI には他の用途もあること,他の用途には後述するプライバシーの懸念がさほど強くないこと,にも配慮していただきたい.

[27] こうした技法を,UTM(Unified Threat Management)と呼んでいる.

図表 1. DPI の 4 つの応用分野



(出典)大元 [2010].なお上記以外にも,ログの保全といった付帯的機能がある.

右側の 2 つのうち帯域制御については次節で細部に触れるので,ここでは世間一般に広まっている誤解の1つである「DPI とターゲティング広告は一体」という認識について,事実かどうかを見ておこう.図表 2. は,行動ターゲティング広告に必要な情報や行動のうち,DPI で実現できるのはどの部分か,を示したものである.○は DPI で実現可能,△は暗号化された情報でなければ可能,×は他の手段でしか実現できないことを示している.

図表 2. 行動ターゲティング広告に必要な情報と DPI の可能性

行動ターゲティング広告に必要な情報や行動	DPI による実現可能性	実現に必要な前提条件とその他の技術
どんなサイトを閲覧し	○	URL や Cookie で判別可能であること
何を買ったか	△	通信が暗号化されていないこと
どんな言葉で検索したか	△	通信が暗号化されていないこと
利用者の趣味・嗜好の分析	×	レコメンデーションという別の機能であり,別のソフトで実現される
広告を配信する	○	技術的には可能だが,広告枠を持っていなければ配信できない.広告枠を買うか,持っているところと提携するなどの前提が必要

(出典)大元 [2010] を一部修正

図表 2. から読み取れることは,DPI 技術はなかなか優秀だが,それも万能ではないこと,とりわけ「利用者の趣味・嗜好を分析する」のは DPI 本来の機能ではなく,他の手段に依存せざるを得ないことである.また DPI という技術がいかに優秀であっても,技術以外の前提が満たされていなければ,活用できないことである.これらは「言うまでもない」ことのようでいて,意外に見落とされている視点かと思われる.

2.2 DPI とプライバシー」とネット上の懸念

前項で述べたとおり DPI をフィルタリングに応用すれば,ヘッダのみを参照する場合には素通りしてしまうような,ウイルス,スパイウェア,ワーム等がネットワーク内に侵入するのを防ぐことができる.これは,セキュリティの確保が特に重要とされるネットワーク接続環境では,非常に有効に働く.

しかも,素通りさせたパケットの情報については記録として残さないこととすれば,通信の秘密は保証される.これを宅配便での荷物のやり取りに喩えると,宅配便の配送センターで X 線を使って違法な物品が運ばれていないか検査する作業と考えれば良い.誰の荷物であるかは特定せずに,危険な物品が運ばれていないかどうかだけを監視する分には,プライバシー保護の観点からみても特に問題はない.

しかし宅配便の配送センターには,紛失や苦情処理に対応するため,発送元と配送先,受け取り日時等の記録は残すのが一般的であろう.そこで犯罪が絡んだ場合には,宅配業者はその情報を開示する事もあり得る(もちろん正規の手続きを踏んだ上でのことだが).同じようにサーバのログを参照すれば,IP アドレスとアクセス日時が特定できるので,掲示板で不適切な書き込みをしたような場合に,自宅からプロバイダを介してインターネットにアクセスしているような場合には,個人の特定は比較的容易にできる.

ここまでは,DPI が無くても可能なことだが,DPI 技術を応用して他のソフトと組み合わせれば,個人の趣味や行動パターンなどを踏まえた,カスタマイズした広告が可能になる.しかし,この「行動ターゲティング広告」については,「何だか気持ちが悪い」という人が多いと思われる.先の例によれば,宅配便の配送センターで個人別のリストを作り,送られた荷物の中身を確認して履歴を残し,それを参照することによって個人の嗜好を判断して,ダイレクトメールを送りつけるようなものだからである.

以上の懸念が,ネット上の議論としてどのように展開しているかをしばらく眺めてみたが,プライバシーへの懸念が圧倒的であること以外に,特に気をつけるべき点は見当たらなかった[28].わが国のプライバシーに関する議論では,「プライバシーの保護」と「個人データの保護」が相互に互換性のあるものとされている.すなわち「前者の侵害は後者の侵害」であり,「後者の侵害はまた前者の侵害」という短絡した見方が

28 大元 [2010] によれば,「総務省が DPI を容認した」かに読める朝日新聞の記事(朝日新聞 [2010].2010 念 5 月 30 日)が出た直後におけるネット上の意見は,「個人の行動記録が丸裸にされる」「国が盗聴を認めた」「検閲国家日本の誕生」「日本の中国化が始まる」「通信の秘密は無視か?」「どうして個人情報を収集しなければならないのか理解できない」「インターネットの自由が奪われる」「どう考えても人権侵害」といった感情的否定論ばかりで,「肯定的な意見は見つかりませんでした(少なくとも私には)」という.

多いが,それはネット上でも変わりがなかった.

言うまでもないが,両者は概念も手法も異なるものである.仮に百歩譲って,「個人情報保護とプライバシー保護は,厳密には異なるものであるが,ここでは,個人情報保護をプライバシー保護のための手段と捉える」(牧田 [2010])ことまでは認めるにしても[29],それが有効な手段であることは誰も証明できていない.場合によっては「有害無益」な手段であるかも知れない(林 [2012]).

2.3 二者択一に対する不安

上記の分析から,① DPI に関する懸念の大部分はプライバシーに関わるものであること,② プライバシーへの懸念の一般例に漏れず,具体的な懸念というより「漠とした不安」であること,が明らかになったのではないかと考える.そして,さらにその深層心理においては,③ 個人データの取り扱いのうち「目的外利用」(個人情報保護法 16 条)や「第三者提供」(同 23 条)の承諾を与えるに際して,「承諾する」か「承諾しない」の二者択一しかないことが,大きなウエイトを占めているように思われる.

そこで,デフォルト設定になりつつある「オプト・アウトとオプト・イン」について改めて考えてみよう.オプト・アウトとは,個人情報の取扱いなどに事前の同意等は必要とせず,問題があれば「事後的に退出できる」自由さえあれば良し,とする考え方である.これに対峙されるオプト・インとは,予め利用条件を定め同意を得ておかなければならない,とする仕組みである.

現在インターネット関連サービスにおいては,この 2 つの選択肢しかないとされ,世界が分断されている気味がある.アニマル・スピリットにあふれたアングロ・サクソンの世界では,「まずやってみよう」が合言葉だから,オプト・アウトでビジネスを果敢に展開している(前節では,このような態度を「技術優先主義」と呼んだ).これに対して,何事につけても「横並び」を意識し,「お上の顔色を伺う」ことに慣れたわが国企業は,オプト・インでなければ心配だと考えて,新しいビジネス展開を逡巡しがちである.

こうした分断は,望ましいことではない.オプト・アウトの放任主義が進めば,「何でもあり」の猪突猛進企業に分があることになるが,それではプライバシーの侵害が後戻りできない事態に至ることも懸念される.他方でオプト・インを金科玉条とすれば,新技術を活かせないまま「宝の持ち腐れ」に陥るかもしれない(前節ではこのような態度を,「通信の秘密・原理主義」と呼んだ).

2.4 諸外国におけるオプト・インとオプト・アウト[30]

アメリカでは,CAN-SPM 法 (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003) によってオプト・アウト方式(携帯電話ではオプト・イン)が採用されている.ただし,わが国の特定電子メール法に比べ,悪質な迷惑メール送信手段を規制するための禁止事項が多く規定されている.な

---

[29] Swire & Litan [1998] も,論を進めるための便宜上のこととはいえ,EU の「データ保護指令」を意識的に European Privacy Directive と読み替えている.

[30] 本項の記述は,主として総務省 [2007] による.

お,CAN-SPAM 法の所管は FTC(連邦取引委員会)であるが,携帯電話向けの規制は FCC が担当している.

EU では,プライバシー・電子通信指令(2002/58/EC)によってオプト・イン方式が採用されている.また,オーストラリアでもオプト・インが採用されているなど,アメリカ以外ではオプト・イン方式が一般的方式になりつつある.

3 通信の秘密の伝統的解釈と問題点

「通信の秘密」の概念は,電気通信に固有のものではなく,郵便が通信の主体であった時代にまで遡る古いものであり,それゆえ「経路依存性」(path-dependency)に満ちている.本節では,そうした歴史を概観しておこう.なお以下の記述は,主として高橋・林・舟橋・吉田 [2008] に依っているが,私たちが意見を異にする部分は修正している(修正した場合は,その旨注意を喚起している).

3.1 郵便法という先例

郵便という事業は,ほぼ全ての国で国営事業として行なわれてきた.従って当初は,国の機関の内部通達ですべてが律せられていたが,やがて利用者である国民との間の一種の契約的なものとして,取り扱い条件の明確化がなされるようになった.1900 年に,それまでの郵便規則・郵便条例・小包郵便法などが統合されて制定された「旧郵便法」(明治 33 年法律 54 号)は,郵便業務の太宗を法制化した第 1 号である.

しかし,この法律もなお「お上の仕事を定型化したもの」であり,利用者との間の権利義務関係を明確化したものとは程遠かった.「信書の秘密侵害の罪」の条文(44 条)はあるが,そもそも「検閲はするな」とか「信書の秘密を守れ」という条文はない[31].また「公安を妨害し」または「風紀を紊乱するものと認めるときは」適用を除外されていた[32]ことに,その特徴が良く現れている[33].したがって,本来の意味での「秘密の保持」の歴史を辿るためには,新憲法下における法制から出発するのが妥当かと思われる.

わが国の法体系は第 2 次世界大戦における敗戦後,それまでの「お上優先」のものから,「個人の平等」に基づく近代的なものへと 180 度の転換を遂げた.お上が約款等に基づいて提供してきたサービス条件についても,「法治主義」の観点から権利義務関係をできるだけ法律で定めることが求められた.「新郵便法」(昭和 22 年法律 165 号)は,このような趣旨で制定されたが,その条文の中で次のように「信書の秘

31 44 条は,以下のような構成になっており(奥村 [1938]),現在の通信関連諸法の原型とも考えられる.① 郵便官署の取扱中に係る信書の秘密を侵したる者は 1 年以下の懲役又は 2 百円以下の罰金に処す,② 郵便事務に従事する者前項の行為を為したるときは 2 年以下の懲役又は 5 百円以下の罰金に処す,③ 本条の罪は告訴を待て之を論ず.(原文は漢字カナまじり文.以下同じ)

32 戦前の憲法(大日本帝国憲法)26 条も,「日本臣民は法律の定めたる場合を除く外信書の秘密を侵さるることなし」という建てつけであった.

33 電信法 5 条においても「電信又は電話に依る通信にして公安を妨害し又は風俗を紊乱するものと認むべきときは地方電気通信局に於て之を停止することを得」となっていた.

密」を守ることが,留保条件なしで明記された.

> 郵便法 8 条(検閲の禁止)
> 郵便物の検閲は,これをしてはならない.
> 同 9 条(秘密の確保)
> 1 郵政省の取扱中に係る信書の秘密は,これを侵してはならない.
> 2 郵便の業務に従事する者は,在職中郵便物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.
> 同 80 条(信書の秘密を侵す罪)
> 1 郵政省の取扱中に係る信書の秘密を侵した者は,これを 1 年以下の懲役又は 2 万 円以下の罰金に処する.
> 2 郵便の業務に従事する者が前項の行為をしたときは,これを 2 年以下の懲役又は 5 万円以下の罰金に処する.

これらの規定は,今日まで続く「通信の秘密保持」の原型となるもので,その意義は大きい.加えて,その国会審議の過程で 9 条 1 項と 2 項の違いに関する論議が交わされていたことは,本稿にとって重要な意味がある.すなわち 2 項の解説として,発信人・受信人の氏名等の問題をあげているところから,「信書の内容以外のことを 2 項で保護している」という解釈をとっていたことが推測される[34].

3.2 上田市公安調査官郵便物調査事件

新郵便法において「信書の秘密」と「他人の秘密」が同一であるか否かが論議になった事例として,上田市公安調査官郵便物調査事件がある[35].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である.当該行為が,郵便法との関係でどのように考えられるのかという点が,国会で大きな問題になった.

政府委員の答弁の混乱が明確になったのは,1954 年 5 月 21 日の参議院郵政委員会の審議である.政党の機関紙が信書に含まれるのか,宛て名の書いていない封書は信書に当たるのかという議論に続いて,「上書き」(差出人と宛先)は信書の秘密の概念に入るかという質問があった.これに対して,井本政府委員は「郵便法第 9 条第 2 項のほうの郵便の秘密という事項に当ると私は思います」と回答した.

しかし改めて,郵政当局の見解を聞きたいという質問に対して,渡辺委員は「我々は郵政省といたしましては,そういう今お尋ねの件は信書の一部分を構成するものであるとかように考えます」と回答したことで,政府内部の解釈論の不統一が明確に

---

34 「第 1 項は郵便の業務に従事する者並びにそれ以外の者すべてにつきまして一般的に規定し,第 2 項は郵便の業務に従事する者だけ,在職中郵便物に関して知り得た他人の秘密,たとえば何某からだれそれあてにどれくらいの量の郵便がいつ送られているといったようなことも,郵便物に関して知り得た他人の秘密ということになるものと考えております」という説明がなされている(衆議院逓信委員会 1947 年 11 月 11 日).

35 前述の通りわが国では,インテリジェンスに対する特別なルールが定められていないので,公安調査官の活動も「秘密保持」の原則に従わなくてはならない.

なった[36].さらに,罰則の適用との関係についても議論がなされ(同年 5 月 21 日の衆議院法務委員会),「郵便法第 9 条 2 項には罰則がございません」という回答がなされ,「郵便物の秘密を教えてくれという行為が,ただちに 80 条の 1 項の犯罪になるかどうか」は,問題があるとされた[37].

3.3 公衆電気通信法における規定と解釈

電話サービスも,誕生当初は国営で提供される国が多く,わが国も例外ではなかった.しかし,サービスの提供そのものは「公権力の行使」というよりは現業業務であるため,一般の官庁からは独立した事業体に移管する方向にあった.わが国では,国内サービスは電電公社に,国際サービスは国際電信電話㈱に委ねることとなり,そのサービスの基本を定める法律として,公衆電気通信法(昭和 28 年法律 97 号.以下「公衆法」)が制定された. 同法にも「秘密の保持」の規定が設けられたが、その規定ぶりは上記の郵便法の模写と言っても良いものであった。.

公衆電気通信法 4 条(検閲の禁止)
公社又は会社の取扱中に係る通信は,これを検閲してはならない.
同 5 条(秘密の確保)
1 公社又は会社の取扱中に係る通信の秘密は,侵してはならない.
2 公衆電気通信業務に従事する者は,在職中公社又は会社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.
同 112 条
1 公社又は会社の取扱中に係る通信の秘密を侵した者は,1年以下の懲役又は 5 万円以下の罰金に処する.
2 公衆電気通信業務に従事する者が前項の行為をしたときは,2年以下の懲役又は 10 万円以下の罰金に処する.

公衆法については,その制定に携わった当事者による逐条解説がある(金光・吉田 [1953]).その「通信の秘密」に関する解説は,「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は場合により単に通信の存在の事実をも意味し,また『侵す』とは秘密を他に漏らし(他人が知り得る状態に置くこと)または窃用すること(本人の意思に反して自己の利益の為に用いること)は勿

36 それより前の 1954 年年 4 月 3 日の衆議院郵政委員会で,齋藤政府委員は「本件のような郵便物の発受人の住所氏名等を漏らしますことは,もちろん郵便法の第 9 条第 1 項にいう信書の秘密を侵すということにはならないと存じますが, 第 2 項における郵便物に関して知り得た他人の秘密を提供するということに該当いたします」と回答している.その後,郵便法9条の秘密を守るべきという趣旨からいって,宛て名書き等も信書の秘密ではないかという質問に対して,いったん混乱した政府委員が信書の秘密であると答弁したが,「通信物の意味の内容といったようなことだけでなくして,それ以外の発信人,受取人とかいったようなことまで,やはり 2 項の方で広く業務上の秘密として守っておるわけでありまして,これに違反することはできないわけであります」と2項の「他人の秘密」として守られるという回答をしている.

37 さらに,「警察官が郵便集配人に頼んで秘密を漏らしてもらったというものが,ただちに集配人と共犯になるかどうかという点については多少の疑問がある」とされた.

論,単に積極的に知得することをも含むのである」と述べている.

また「秘密を守らなければならない」という文言は,公衆電気通信業務に従事する者においては,積極的知得行為が禁止されていないことを明確にしている趣旨であるとされる.

また,ここでの特徴は,5 条における「通信の秘密」と「他人の秘密」と峻別しないことを主旨としていること,またその考え方が 112 条にも適用され「一般には電報の本文または通話の内容を知り又は他人に漏らすことは秘密の侵害となることは勿論,さらに通信の有無および通信の当事者を知り又は他人に漏らすことも亦秘密の侵害である」とされていることである[38].

3.4 吉展ちゃん事件と内閣法制局意見

以上に述べたように,新郵便法や公衆法の制定後しばらくの間は,「狭義の通信の秘密」と「他人の秘密」の関係は必ずしも明確なものではなかった.この両者が「一体不離」という理解が公的な解釈になっていったのは,1.1 でも紹介した 1963 年の吉展ちゃん事件を契機としており,決定的な影響を与えたのが,事件の後に出された内閣法制局意見 (1963 年 12 月 9 日付.以下,「法制局意見」)である.これは,いわゆる逆探知に関して日本電信電話公社(以下,公社)が郵政大臣官房電気通信監理官を通じて行なった照会に対する,内閣法制局からの回答の形を取っている[39].

照会事項は,次の 2 点である.

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?

これに対する法制局見解は,「いずれも消極に解する」,つまり「両者とも違反しない」

という回答であった.

ここで注目すべきは,回答そのものよりも,① において逆探知行為は,「公衆法 5 条 2 項に違反するか」という質問がなされていることである.すなわち質問者側の理解としては,5 条 1 項の問題ではなく,明確に「2 項」の問題であると意識されている.従って,このやり取りは,先の国会答弁にもあったように,郵便法における「1 項を通信内容に関する規定,2 項を通信内容を除く上書き等に関する規定」とする立場を,公衆法に応用したものと解するのが素直であるように思える(これを便宜上,「峻別説」と呼ぶ).

一方で,5 条1項と 2 項は,ともに「通信の秘密」を保護するものであって,1 項は,業

---

38 ただし前述のとおり,この時代の電気通信サービスは電電公社と国際電電の独占であり,解説者の 2 人とも旧電気通信省から電電公社に引き続き勤務した者であるから,解説は主として電電公社社員向けに書かれたものではないか,と思われる.

39 公社側の実務責任者であった林節男氏(当時総裁室文書課法規係長) に対するヒアリング結果によると,郵便法の解釈等との関連性などはまったく念頭に置かなかったとのことである.また,意見作成にあたってなされた議論は,「内閣法制局の田中参事官とわれわれ電電公社の者だけで,郵政省の人がおられたという記憶がない」とのことであった.当時の電気通信監理官室はごく小さな所帯であったから,この点は十分に納得できる.

務に携わらない一般人についての定め,2 項は,業務に携わるものについての定めであるという解釈も可能であり,5 条の解釈よりも 112 条の解釈にとっては捨てがたい(これを「同一説」と呼ぶ).なぜなら,通信内容とそれ以外の「他人の秘密」を峻別する立場に立てば,一般人が他人の秘密のみを侵害した場合に,これを処罰できるか否かという大きな疑念が生ずるからである[40].

しかし「峻別説」は一顧だにされることなく,法制局意見は「同一説」に立つとする見方に収斂していった.これは,当時の法制局内で,「通信の秘密は個々の通信内容を保護するというよりも,通信の秘密性そのものを保護する規定である」という理解が広まっていたからだ,とする説もある[41].しかし私たちは,公社時代に企業倫理としての「通信の秘密」を教え込まれた経験から,「通信内容の秘密であれ,他人の秘密であれ,どちらも区別せず守ることが,世間の期待に応えることである」という倫理感が,「同一説」を導いたのではないかと考える.

すなわち法制局意見は,(少なくても公社の人間にとっては)以前から有力な解釈の立場であった,「通信の構成要素に関する情報すべてについて,一般人に対しては『通信の秘密』という文言で,従事者に対しては『他人の秘密』という文言で,同一のものを保護している」というスタンスから,逆探知の適法性について議論を整理したものと理解されていたのである.

また当時の電話交換のシステムでは,通信内容と受信者電話番号などの情報が区別されずに,同じ回線を通じて(あるいは交換手を介して)伝送されていたという事情も,判断に影響を与えたかもしれない.いずれにせよ公社は,法制局意見を受けた翌春早々に,「電文 1100 号」という社内通達を発し,「同一説」はより鮮明になった[42].

3.5 電気通信事業法への移行

公社制度は 30 年強続いたが,公社と会社による独占的サービス提供体制では対応できないほど技術が進歩しサービスも多様化してきたことから,全事業分野への複数事業者の参入と公社の民営化が検討されるようになった.そして他の 2 公社の民営化と共に,電気通信事業制度の抜本的な変革が試みられることなり,1984 年に電気通信事業法および日本電信電話株式会社法が制定された(施行は翌 1985 年.なお国際電信電話㈱は,遅れて 1998 年に,特殊会社から一般の株式会社となった).

しかし電気通信事業法の通信の秘密に関連する条文は,公衆法をそのまま踏襲

---

40 私たちは「罪刑法定主義」の観点から,その場合には処罰する根拠がないと考えるが,この点は後に再説する.なお小向 [2011] も,やや遠慮がちながら,可罰性に疑問を呈している.

41 高橋・林・舟橋・吉田 [2009] はそのような見方を取る.「この当時,すでに,内閣法制局において,通信についての『秘密』は,むしろ,『秘密性』とでもいうべきものであって,秘密にすべき性質をもっている,したがって,通信の構成要素から特定のものを通信の秘密として,それ以外の構成要素と峻別することはできないという認識を有していたのではないかという事実も明らかになった.」

42 電文 1100 号は,法制局意見をベースにしているのは当然であるが,それまでの 11 通の諸通達を廃止し,全体を包括的に分かりやすく解説し直した,一種の「新マニュアル」の感がある.例えば,先の設例に近いケースを次のように解説している.「問 12. 家出人から自宅に自殺予告の電話がかかり,その家族等から発信番号の調査依頼があった場合,(措置)遺書がある場合等自殺の恐れが強いと認められる場合は,通達(番号等略)により,応じて差し支えない.」

し,公社の民営化にともなって用語が変更になっているものの,実質的な変更はなされなかった.また前述したように,通信の秘密と電気通信事業従事者の罰則加重規定についての議論がなされていたが,この部分についても具体的な対応はなされなかった.もっとも,通信の秘密保持のための具体的な規定として,同法 35 条(業務の停止等の報告),36 条・37 条など(業務の改善命令)などの規定が設けられている.

また事業法は,競争の進展とネットワークの相互接続の一般化等に伴い,2003 年に大幅に改正された(平成 15 年法律 125 号))が,その際にも通信の秘密に関する部分は,そのまま引き継がれている(多賀谷・岡崎 [2005]).

3.6 「他人の秘密」侵害行為の可罰性

以上の分析から,「通信の秘密・原理主義」を生んだかもしれない要素の 1 つとして,「通信の秘密」と「他人の秘密」を同一視するか否かという論点があったという事実が判明した.この点が最も先鋭な対立をもたらすのは,「他人の秘密」侵害行為の可罰性論議である.図表 3. のようなマトリクスを作ってみれば,本文の説明がより良く理解できよう.

図表3. 他人の秘密の可罰性検討

保護対象 / 罰則	「通信の秘密」(4 条 1 項)	「通信に関して知り得た他人の秘密」(4 条 2 項)
通信の秘密の侵害一般(179 条 1 項)	Ⓐ 何人も侵害者になり得る	Ⓑ (この欄の解釈について 2 説あり)
電気通信事業の従事者による同上の侵害(179 条 2 項)	Ⓒ 電気通信事業の従事者のみが侵害の主体になり得る(身分犯)	Ⓓ 電気通信事業の従事者のみが侵害の主体になり得る(身分犯)

つまり,「同一説」に立てば上表の Ⓐ は Ⓑ と,Ⓒ は Ⓓ と同じことになるから,そもそも表を作る意味がない.ところが「峻別説」に立てば,上表の Ⓑ と Ⓓ には,次の 2 つの解釈があり得ることになる[43].

① 「通信の秘密」を侵せば,何人も侵害責任(刑事)を問われるが,事業に従事する者以外の者が「他人の秘密」を侵しても,それに対応する罰則規定がないから,可罰性がない.

② 「通信の秘密を侵す」とは,狭義の「通信の秘密」だけでなく「他人の秘密」を侵すことをも包摂した概念であるから,「他人の秘密」の侵害者も,「通信の秘密」を侵した者と同様,可罰性がある.

文言に忠実で,「罪刑法定主義」にも忠実であろうとすれば,私たちには ① 説しかあり得ないように見える.しかし,電電公社の職員には「職業倫理としての通信の秘密」が沁み込んでいたから,目が曇ったのであろう.① を唱えるものはほとんどなく,

[43] なお両説以外にも,「通信の秘密」と「他人の秘密」は,同じものを視点を変えて呼んだに過ぎない(電気通信事業の従事者から見れば「通信の秘密」で,一般人から見れば「他人の秘密」),という説(同義説)があり得るが,ここでは煩瑣になるので「同一説」に含めて考える.

社内常識は② に収斂していった.当時の社内有権解釈を代表的するものとして,電気通信関係法コンメンタール編集委員会(編) [1973] は,次のように述べている.

「通信の内容はもちろん,通信の当事者(発信人,受信人)の居所,氏名,発信地,受信地,通信回数,通信年月日など(中略)通信そのものの構成要素であり,これらの事項を知られることによって通信の意味内容が推知されるような事項はすべて含まれる」[44].

3.7 発信電話番号表示サービスの経験

通信の秘密と他の保護法益との均衡が問題なったのは,今回が初めてではない.早くも固定電話中心の時代の 1997 年に,発信者番号表示の是非をめぐって議論が交わされ,社会的コンセンサスが形成された経緯がある[45].

電話のシステムは開発当初から「発信者優位」の仕組みであった.受信者側には,ベルが鳴ることで「電話がかかってきた」ことは分かるものの,「誰からかかってきたのか」は知る方法がなかった.この欠陥を悪用した,いわゆる迷惑電話が問題になったのは,電話の普及が一巡しデジタル化が進んで通話と信号処理を別々に行なうことが可能となった,1980 年代後半以降のことであった[46].今日の迷惑メールの電話版,といった方が若者には分かりやすいかもしれない.

「迷惑電話から逃れたい」という切実な要望に応えようとするサービスは,発信電話番号を応答前に着信側に通知し,電話機などのディスプレイに表示するサービスである[47].しかし心配されたのは,「通信の秘密」との関連であった.それまでのシステムでは,受信者が発信者を知る手段がなかったから,「発信者電話番号を受信者との関係において,通信の秘密に含まれるとする見解が生まれるようになった」(多賀谷 [1997])からである.「通信の秘密・原理主義」の匂いがするが,当時の感覚では「それが当然」という雰囲気もあった.

そこで懸念を最小にするために,以下のような配慮がなされた.

① 郵政省においては,サービス開始に先立って「発信者情報通知サービスにおける発信者個人情報の保護に関するガイドライン」を策定し,事業者に遵守を促した.

② また同サービスの認可に当たって,「発信電話番号非通知機能」の提供を受けている回線でも,発信の都度解除できるようにすること」等を求めた.

このような経験が,DPI に応用できるだろうか.共通点は,2 点ある.まず第1は,「情報の仲介者である電気通信事業者の扱いが問題になっている」ことである.その意味では,後述する「情報プライバシー」としての議論がなされている点で,DPI との共

---

44 電気通信法制研究会 [1987]は,:事業法4条2項の「通信の秘密」について,「通信の秘密(通信内容+通信の構成要素)+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を含む」と理解しており,3 つの要素を含むと考えているかに見える.

45 以下の記述は,堀部(編著)[1998] に多くを依存している.

46 NTT は,発信電話番号表示サービス(サービス名はナンバー・ディスプレイ)導入の背景として,① 迷惑電話対策として利用者や行政から要望がある,② 海外での相次ぐサービス開始,③ 電話網のデジタル化等の技術・設備面での進展,の 3 点を挙げていた(堀部 [1997]).

47 同時に提供されたサービスに,発信電話番号アナウンス・サービスなどもあったが,ここでは省略する.

通点がある.第 2 点は,何らかの技術を用いて,人手が介在しない形での解決策が模索されていることである.これは,Lessig [1999] が指摘した,「code あるいは architecture による解決」に期待していることになる[48].

しかし,発信者情報開示と DPI の事例では,決定的な差も存在する.それは前者では,通信事業者が行なうのは情報開示のシステムの提供だけで,通信の内容はもとより,通信の有無や宛先といった「他人の秘密」に当たりそうな部分についても,一切タッチしていないのに対して,DPI では事業者(通信事業者であれ,ISP であれ)が自ら通信内容を利用しようとしている点である.

その意味では,本項の説明は参考程度にすぎず,DPI と通信の秘密の関係については,次節以下のインターネット時代のケースを中心に,原点に帰って議論しなければならない.

3.8 通信手段の変化

なお今後の議論に資するためには,通信手段の変化にも着目しておくべきだろう.図表 4. は,主たる通信手段の変化を,郵便－＞電報－＞電話(手動式交換)－＞電話(自動式回線交換)－＞インターネット(パケット交換)と図式化した場合に,「通信の秘密」と「他人の秘密」が峻別され得るものか否か,を検討したものである.意外なことに,郵便の時代に峻別可能であった両者が,自動化等で一旦不可能になり,インターネットという最新のシステムで再び峻別可能になった様子が読み取れる.

図表 4.「通信の秘密」と「他人の秘密」の峻別可能性

主たる通信手段	郵便	電報	電話(手動交換)	電話(自動式回線交換)	インターネット(パケット交換)
「通信の秘密」の例	手紙や封書において伝えたい内容	電文そのもの	通信内容	同左	同左
「他人の秘密」の例	発信人・あて先・筆跡など	発信人・あて先など	①当事者の発着信番号・発信時刻など ②当事者の性別・発音の訛りなど	①が主で,②は意図的に傍受した場合のみ	発着信アドレス
両者の峻別の可能性	封書の場合,両者は峻別可能	両者は同時に扱われるし,秘匿の程度に差はない	両者は同時に知得される	事業者が介在する頻度は低いが,傍受すれば同時に知得さ	アドレス部分の情報だけを読み取ることは可能

48 レッシグによれば,社会制御の方法は,① norm,② market,③ law,④ code あるいは architecture,の 4 つがあるが,インターネットの時代には ④ による制御が優勢になるという.この事例は,その典型的な例と言えよう.

				れる	
フロー情報とストック情報	フロー情報のみ	フロー情報のみ	フロー情報のみ	フロー情報のみ	ストック情報も考慮の要あり

なお,図表 4. のインターネットの欄については,3 つの点に留意していただきたい.1 つは,それ以前の通信手段が記録性を持たなかったのに対して,インターネットは記録する(ログを取ったり,ミラー・サイトを作る)ことが容易なことである.従って,従来のメディアでは,そこに流れる情報の秘密性だけが問題であったのに対して,インターネットではストック情報の秘密性も問題になり得ることである.

2つ目として,インターネットでは秘匿性の高い1対1のeメールがある一方で,「公然性を有する通信」とも呼ばれる 1 対 N 型または N 対 N 型で,通信の秘密を厳守する必要性に乏しい「通信」が数多く存在することにも,留意が必要であろう.この限りでは,「通信の秘密」厳守の重要性は,従来に比べれば相対的に減少すると思われる.

しかし他方で,Twitter に不用意な書き込みをしたら,他の書き込み等から「書き込みをした本人(発信者)」が特定され,「さらし」という激しいバッシングに会うことが多発している.書き込み内容(通信内容)自体は公開されているので,秘匿性はないものと考えられるが,発信者の特定はプライバシー侵害に当たることもあり得るように思われる.したがって,このケースで守るべきは,「通信内容」ではなく,むしろ「発信者に関する情報などの通信の構成要素」(他人の秘密)であろう.

第3点として,海外の動向にも留意する必要があろう.グローバル化によって世界が狭くなれば,犯罪もまたグローバル化していく.その際,国際協力が不可欠とすれば,犯罪の構成要件や手続き法などをグローバルに合わせておく必要も生ずるからである.この点で「海外法制などをみると,通信内容と通信データ部分についての保護をわけて論じることもよくなされている」との指摘(高橋 [2008])にも留意する必要があろう.

4 インターネットと 通信の秘密に関連する主な事例

発信電話番号表示サービスの実現後も,インターネット利用の拡大に伴い次々と発生する個別の事案に対応すべく,「通信の秘密」に関する法解釈の面での工夫がなされてきた.そこで,先例としてこれらの事例を紹介し,学ぶべき点は何か,違いがあるとすれば何かを考察しよう.なおその前に,法学に馴染みが薄い読者のために,ある行為が違法な行為(犯罪)だとされる手順を説明し,本節の理解を容易にしておこう.

犯罪は個人の権利や社会の秩序等を乱す行為であり許されないが,それに対して刑罰を科すこともまた,形式的には個人の権利を侵害することになる.しかも人間の判断には,間違いが付きものである.そこで近代国家においては,犯罪の類型(犯罪単位では「構成要件」という)と,それに対応する刑罰の種類や軽重等を,予め法律で定めておかねばならないこととされ(罪刑法定主義,憲法 31 条,39 条),その解

釈も謙抑的になされなければならない.

ある行為が犯罪に当たるか否かは,まず法律で定められた「構成要件」に当たるかどうか(構成要件該当性)で判断される.構成要件は犯罪を類型化したものであるから,これに当たるとすれば,まずは違法性ありと推定される.しかし,違法な行為が直ちに犯罪になるわけではない.というのも,後述する外科医の手術のように,見かけ上構成要件(傷害罪)に該当するようでも,怪我や疾病を治すためという「正当な業務」として行なうものがあるからである.形式的には「違法」に見えるものであっても,その違法性が「阻却」される(違法性阻却という)例として,正当行為(刑法 35 条)・正当防衛(同 36 条)・緊急避難(同 37 条)がある[49].

こうした一般原則を適用すれば,ISP がある行為を行なった場合に,まず(外形的)構成要件的に,電気通信事業法 4 条の通信の秘密の侵害行為と判断されるかどうかが問題となる.仮に侵害行為と判断された場合でも,利用者の(個別かつ明確な)同意を得ている場合や,同意を得ていなくとも違法性阻却事由があれば,適法行為とされる.

違法性阻却事由の一つである正当業務行為(刑法 35 条)としては,従来から「事業の維持・継続に必要な行為で,たとえば,課金・料金請求のために通信当事者の通信履歴を利用する行為や ISP がルータにおいて通信のヘッダ情報を知得して経路を制御する行為等」が認められていた.この他,「ネットワークの安定的運用等のために必要な措置については,目的の正当性,行為の必要性,手段の相当性を慎重に検討した上,正当業務行為と解されている」(日本インターネットプロバイダー協会ほか [2007]).

正当業務行為以外の違法性阻却事由として,正当防衛や緊急避難に該当するケースがある.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.

なお,ある情報が違法性を帯びている場合に,当該情報を遮断することが「通信の秘密」を侵害することにならないか,という視点で典型的なケースと思われるのは,児童ポルノ情報である.児童ポルノは,① 製造時に児童への性的虐待を伴う,② 被害児童に対する脅迫の道具となり得る,③ 一旦流通すれば回収が困難,④ 児童を性欲の対象と捉える風潮を助長することから,世界的に厳しい取締りが期待され[50],わが国でも 2009 年に「児童買春・児童ポルノ禁止法」が制定されている[51].

そこでこれを取り締まる側からすれば,なるべく多くの人からの通報を得て,それが違法なものであるかを迅速に判断し,違法性ありとされた場合には直ちに ISP にア

---

49 最後に,こうした行為を行なった者に,責任能力があったかどうかが検討される.一般的な成人の行為には責任能力があるが,心神喪失または心神耗弱(刑法 39 条)の場合は罰せられなかったり,刑が軽減される.また,14 歳未満の者の行為は罰せられない(同 41 条).

50 警察庁「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).なお本文は,国際常識を文章化したものであるが,国内の児童ポルノに対する見方は,児童虐待の視点で捉えるよりも「ポルノの一種」と,やや軽く見ている傾向がある.

51 正式名法は,「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」(平成 11 年法律 52 号)である.

クセスを遮断してもらいたいところである.その際,一旦ネット上に流出してしまえば回収できないのだから,裁判所の判決を求めるだけの時間的余裕はない.したがって,結果として削除要請が過剰になり勝ちなのも,役目上止むを得ない面がある.

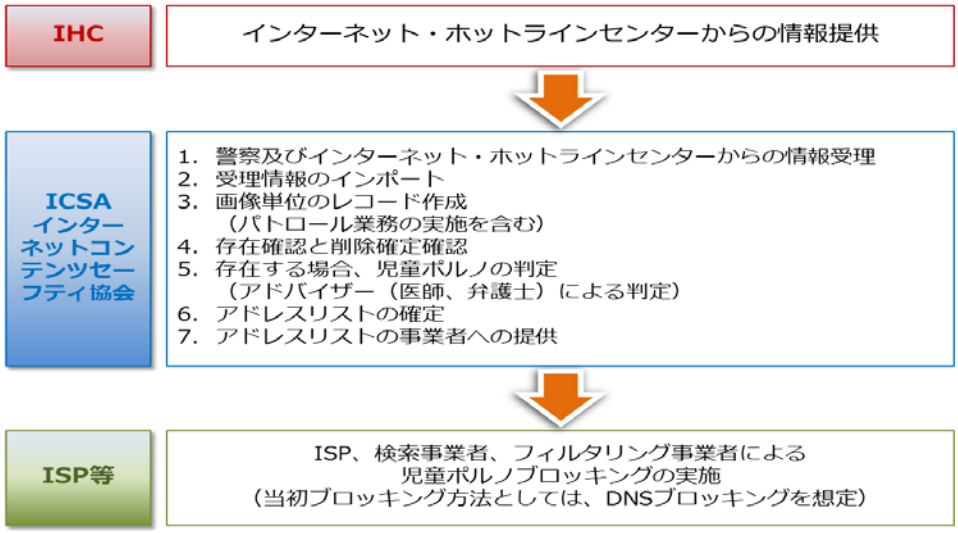
他方,削除要請を受ける ISP の側からすれば,違法なコンテンツをいつまでも放置しておくのは本意ではないが,さりとて自分だけの判断で削除をするには知識が乏しいし,なによりも「通信の秘密」を侵すことはできない.となると,削除が過少になる傾向は否定できないが,それも「職務に忠実なため」という側面がある.

このように取り締まる側の要請と,ISP 側の期待等を総合勘案して設立されたのが,インターネットコンテンツセーフティ協会(Internet Content Safety Association = ICSA)である.ICSA は児童ポルノ掲載アドレスリスト作成管理団体として,児童ポルノ画像が掲載されたサイトに係るアドレスリストの作成・管理を行なうなど,インターネットを通じた違法コンテンツの流通を防止するために,民間事業者等が講じる各種取組みを支援することになっている[52].

疑わしいサイトの通報からアクセス遮断までの流れは図表 5.の通りであり,児童ポルノの禁止という一方の法益と,通信の秘密保持という他方の法益を両立させる仕組みとして,良く考えられているのではないかと思われる.なぜなら,以下の 3 つの条件を確保することで,チェック・アンド・バランス(法的には適法手続き=due process of law)が保たれているからである.① 情報提供機関と判定機関が別,② 判定機関と実施機関も別,③ これ以外にモニター機関としての児童ポルノ流通防止対策専門委員会がある[53].

次節以降のケース・スタディにおいても,この事例を参照しつつお読みいただければ幸いである.

図表 5. 児童ポルノにおける情報提供からアクセス遮断への流れ



(

52 http://www.netsafety.or.jp/about/001.html

53 共著者の 1 人林が,現在委員長を勤めさせていただいている.

出典)インターネットコンテンツセーフティ協会.なお本図以外に,このプロセス全体をモニターする専門委員会がある.

4.1 プロバイダ責任制限法における情報の送信防止措置と発信者情報開示

インターネット利用における通信の秘密に関して,最初に問題となったのは,2001年に施行されたプロバイダ責任制限法[54]に係る問題である[55].

インターネットでは,従来の1対1で内容の秘匿を要する通信以外に,本法2条1項で規定されている「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,放送を除く送信)」のように秘匿性がない通信の増加が顕著である.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,他の人の目にふれることになるため,被害を受けたと主張する人が法的な救済を求める場合がある.

この場合に,被害を受けたと主張する人は,情報発信が匿名でなされることが多いため,当事者間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.このため,被害の回復を求めるために,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ISP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[56].

ところが,ISP は基本的に conduit 事業者であり,「通信の秘密を厳守し content にノータッチ」が求められる立場にある.加えて,ISP 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会うことになる.

conduit 事業者であるISPにcontentへの関与を認め,またこの関与に伴って発生する可能性のあ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,ISP 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,ISPの情報の削除や発信者情報開示行為が,ISPの正当業務行為であることが認められた.

またこの法律に関しては,プロバイダ責任制限法ガイドライン等検討協議会が策定した「名誉毀損・プライバシー関係ガイドライン」(初版 2002 年,プロバイダ責任制限法ガイドライン等検討協議会 [2004]),「発信者情報開示関係ガイドライン」(初版2007年,プロバイダ責任制限法ガイドライン等検討協議会 [2007])などいくつかのガイドラインがある[57].

---

54 正式には「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」

55 本項で述べるプロバイダとISPと同義であるが,法律の名称が「プロバイダ責任制限法」と略称されているので,それに従う.

56 発信者情報の開示は,当事者間の紛争の解決の前提になるものであるが,訴訟を提起する際にも「住所・氏名」によって相手を特定しなければならないから,不可欠なものである(民事訴訟法 133 条).

57 ガイドラインは,判例や行政機関による法令の適用関係に関する解釈を求めたものではない.しかしながら,ガイドラインに従った行為は,形式的には通信の秘密を侵害する態様で行なわれた場合でも,(正当業務行為として)違法性が阻却されるとの判断がなされることが期待される(日本インターネットプロバイダー協会ほか [2007].ただ

4.2 迷惑メール対策としてのポート 25 ブロッキング

電子メールが広く利用されるようになるにつれて,迷惑メールやスパムメールと呼ばれる電子メールが増大して,トラフィック全体の中で大きな割合を占め,社会的にもその対策が求められるようになった.

このため 2002 年に「特定電子メールの送信の適正化等に関する法律」が制定・施行され,法的な対応がなされるようになった.また迷惑メール対策を強化するために,2005 年と 2008 年に同法が改正され,禁止範囲の拡大,オプト・アウトからオプト・インへの変更,法の実効性の強化や国際連携の強化が図られている(総務省[2007]).

いわゆる迷惑メールは,同法では特定電子メール(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なうための手段として送信する電子メール」と定義されているように,広告・宣伝目的のメールの送信を規制しようとするものである.この目的に資するよう,同時に特定商取引法が改定され,取引態様の面から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 ISP は,OP 25 B(Outbound Port25 Blocking)や IP 25 B(Inbound Port25 Blocking)といった,送信者のパケットチェックを行なっている.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.

同法 11 条では,電子メールサービスを提供する電気通信事業者(ISP)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」ことを明文で規定しているからである.このように迷惑メールの場合には,明文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おり,法的な解釈が分かりやすくなっている[58].

ただし,オプト・アウトからオプト・インへの法改正の根拠付けについては,若干の疑問なしとしない.というのも,「アンケート調査の結果,フィルタリングを望む声が 80%程度あった」ことを根拠にしているが,個人の選択の自由を奪う決定としては,根拠薄弱と思われるからである.もっとも 2.3 で述べたように「二者択一しかない」という思い込みが,そうさせたのかもしれない.

4.3 インターネット上の「自殺予告」

インターネット上を流通する情報は多種・多様で,中には違法・有害情報も含まれている.発信者の法的責任が生ずる違法情報としては,著作権侵害・名誉毀損などの権利侵害情報や,児童ポルノや麻薬売買の広告などのその他の違法情報がある.また,発信者に直ちに法的責任が生ずるとまでは言えないが,社会全体から見れば

し表現を一部修正).

58 なお迷惑メールに関しては,総務省が 2011 年にガイドラインを策定している.

有害情報とされるものには,人の尊厳を害する画像や自殺を誘因する書き込みなど公序良俗に反する情報や,青少年に有害な情報がある.

中でも,自殺予告を含む自殺関連ウェブ・サイト等で知り合い集団自殺を決行した件数と死者数が,2004 年の年間の 19 件 55 人から,2005 年 6 月末までの半年間で 25 件 70 人に達した.社会的にも大きな問題となり,人命保護の観点から緊急に対応する必要があるとして,電気通信業界 4 団体は 2005 年 10 月に「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」を策定した(電気通信事業者協会ほか [2005]).通信の秘密に関する自主規制のガイドラインとしては,初期のものといえる.

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 番通報を行な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 ISP 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.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る.

このガイドラインでは,自殺予告案件に対する ISP 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.

なお,ISP などが発信者情報を開示したことにより,本人に損害が生じた場合の民事上の損害賠償責任については,正当防衛(民法 720 条 1 項),緊急避難(同条 2 項)に当たる場合のほか,緊急事務管理(同法 698 条)の要件を満たす場合にも,開示行為の違法性が阻却されて損害賠償責任を負わないとされている(電気通信事業者協会ほか [2005])

4.4 ぷららネットワーク社による Winny の接続遮断

インターネットと通信の秘密に直接関係する事例として,ぷららネットワーク社が 2006 年 3 月に,ファイル交換ソフト Winny による通信の完全規制(遮断)を行なう旨を発表したケースがある.

同社の対応の背景としては,① ウイルスに感染したパソコンから Winny を介した意図せぬ個人情報や機密情報の流失が多発して,これを防止することが大きな社会問題になっていた,② Winny などの特定のアプリケーションのトラヒックが,全体の中で大きな割合を占めるようになり,他の利用者の利用に悪影響を与える恐れが高くなっていた,③ 同社は以前から平均トラヒックを大幅に超える利用者に対しては,他の会員の迷惑にならないレベルまで,アプリケーションを含めてトラヒック制御を行なうことを会員規約に定めていた,等の事情があった.このような状況において,同社は利用者が安心して利用できるネットワーク環境を提供することが,通信事業

者の責務であると考え,Winny による通信を完全に規制するとの発表を行なった(ぷららネットワーク [2006]).

この方針発表に対して総務省は,同社に説明を求め検討を行なった結果,Winny による通信の完全規制は,通信の秘密の侵害に抵触する可能性が高いとの見解を示した.このため,同社は Winny 通信を遮断するサービスを希望者に対してだけ提供することを決定した.また,デフォルトで Winny フィルターを提供するが,利用者自身が解除することも可能にしている.この事例では,Winny 通信を遮断するサービスは,外形的に通信の秘密を侵害しており,違法性阻却事由も明確にあるとは言えないとの判断に基づいて,利用者の同意を得ることで通信の秘密侵害であることを避けたという経過になっている.

前述したように,日本企業は法的にグレーの領域の問題について,リスクを回避する(自主規制する)傾向が強いが,ぷららネットワーク社の事例は例外的であった.グレー領域の問題にチャレンジしたことが,結果として,4.6 で取上げる 2008 年の「帯域制御の運用基準に関するガイドライン」の策定を促したともいえ,チャレンジの重要性を示している.

4.5 大量通信等への対処策

インターネットの普及とともに,動画データなど大容量の通信も可能になった.これは利用者の利便の向上をもたらす半面,電気通信事業者の設備に過大な負荷を与え,円滑なサービス提供の脅威ともなり得る.この対策を講ずるためには,通信内容を識別した上で何らかのネットワーク制御が必要であり,通信の秘密の問題をクリアする必要がある.このため,2007 年 5 月に通信事業者 4 団体は「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」を関係者に配布し,2011 年 3 月の改定を機に公表した(日本インターネットプロバイダー協会ほか [2007]).

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,ISP の設備に対して攻撃が行なわれるケースもあるので,この場合には ISP 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の OP25B・IP25B や帯域制御がある.加えて,これらの対処策に,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.

4.6 帯域制御問題

前項の大量通信等のガイドラインに含まれている問題ではあるが,サイバー攻撃などとは異なり,インターネット・トラヒックの高い割合での増加が恒常的に続いていることに,どう対応するかという問題がある.利用者間の利用の公正性の観点から,電気通信事業者 4 団体が 2008 年に「帯域制御の運用基準に関するガイドラン」を策定している(日本インターネットプロバイダー協会ほか [2008]).

ここでは,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,(外形的)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,ISP 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[59].

まず利用者の個別かつ明確な同意があれば,当該利用者に関する限りは,通信の秘密の侵害とはならない.これを普通契約約款に含めておけば,形式的には通信の秘密の問題を回避することができる.しかしシュリンク・ラップ契約やクリック・ラップ契約に疑義が提起されているように[60],これだけで回避できるとするのは問題であろう.

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 ISP 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 ISP 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な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(手段の相当性)が必要であり,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.

4.7 DPI 技術を活用した行動ターゲティング広告

個人生活の履歴であるライフログを活用したビジネスとして,過去の閲覧履歴等に応じた広告を配信する,行動ターゲティング広告が注目されている.この問題を検

59 帯域制御の実施主体としては,ISP のほか,MVNO を含む移動通信事業者,固定通信事業者等が想定されている.日本インターネットプロバイダー協会ほか [2007] 参照.

60 シュリンク・ラップ契約(Shrink-wrap contract)とは,主に市販のパッケージ・プログラムの外箱内に封入されている使用許諾条項に,包装を開封すると当該条項に同意したものとみなされる旨の記載があるため,包装の開封と同時に成立するとされる契約の俗称.クリック・ラップ契約は,それのオンライン版で,クリックすると同時に契約が成立するとされるもの.

討したものとして,2010 年 5 月に総務省から「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」が公表された(総務省 [2010]).

ここでは行動ターゲティング広告を,「蓄積されたインターネット上の行動履歴から利用者の興味・嗜好を分析して利用者をクラスターに分類し,クラスターごとに広告を出し分けるサービスを指す」ものとしている.また「DPI 技術を活用した行動ターゲティング広告は,ISP が,ネットワークを通過するパケットを解析して利用者の興味・嗜好を分析し,これにマッチした広告を利用者に配信するものである」としている[61].

上記の説明からも分かるように,DPI 技術は(外形的に)構成要件的には,通信の秘密を侵害する行為である.したがって,前項の帯域制御のように違法性阻却事由の検討が済んでいる利用法と,今後の検討が必要になる利用法があり,行動ターゲティング広告は後者に属する問題であり,同研究会で検討が行なわれたのもそのためであった.

同提言では,違法性阻却事由が認められる事例を上げたうえで,「事例の根底にある基本的な考え方は,利用者である国民全体にとっての電気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を正当業務行為として認めるもの」であり,「DPI 技術を利用した行動ターゲティング広告について正当業務行為とみることは困難である」としている.したがって,通信当事者の個別かつ明確な同意が必要であるとしている.

また,ライフログ活用サービス全体に関しては,プライバシー侵害や利用者の不安感があり得るので,利用者に一定の配意をして,円滑なサービスに資する対策を行なうための「配慮原則」を提言している[62].

4.8　各種ガイドライン等に見る「通信の秘密」概念の混乱

本節で紹介してきた各種ガイドライン等は,いずれも「通信の秘密」に関連する要素を含んでおり,そのうち 3 件は「通信の秘密」に直接言及してもいる.ところが,これらにおいて同概念が統一されていないばかりか,「同一説か峻別説か」についてさえ,混乱しているのではないかと思われる.図表 6. は,各種ガイドライン等における該当の記述を抜き出したものであるが,混乱の度合いが読み取れるであろう.

図表 6.　各種ガイドライン等に見る「通信の秘密」の概念

ガイドライン等	該当の記述	同一説か峻別説か
「電気通信事業者における大量通信等へ	事業法第4条の通信の秘密の範囲については,個別の通信に係る通信内容のほか,個別の通信の構成要素,存否の事実,個数等も含まれるも	不明だが,同一説かと推定される.なぜなら,「通信の秘密＝通

61 「DPI 技術とはネットワークを通過するパケットのヘッダ情報やペイロード情報を解析し,通信の特徴や振舞いを分析する技術を指している.従来,DPI 技術は,帯域制御のための要素技術として利用されてきたが,現在,ファイアウオールでは防ぎきれないインターネット上の脅威に対する防衛手段のための要素技術として,より洗練された行動ターゲティング広告のための要素技術として,先進的な利用が検討されており,今後の展開が期待される技術」とされている.

62 そこに含まれるのは,以下の 6 項目である.①広報,普及・啓発活動の推進,②透明性の確保,③利用者関与の機会の確保,④適正な手段による取得の確保,⑤適切な安全管理の確保,⑥苦情・質問への対応体制の確保.

の対処と通信の秘密に関するガイドライン」(日本インターネットプロバイダ協会ほか[2007])	のとされている.個別の通信の構成要素の範囲については,通信当事者,通信日時,通信量,ヘッダ情報等広範な情報が含まれるものと考えられるため,本ガイドラインにおいて検討する際にも,個別の通信に附随する情報については,通信の秘密の構成要素に当たりうることを前提として検討することが適当である.	信内容＋通信の構成要素」としているが,他人の秘密について言及していないことから,少なくとも峻別説ではないと思われるからである.
帯域制御の運用基準に関するガイドライン(日本インターネットプロバイダ協会ほか[2008])	「通信の秘密」の範囲は,個別の通信に係る通信内容のほか,個別の通信に係る通信当事者の氏名,発信場所,通信日時,通信量やヘッダ情報等の構成要素,通信の存否の事実,通信の個数なども含む広範なものである.また,「通信の秘密」を「侵害する行為」には,通信当事者以外の者が,「通信の秘密」に該当する事項を積極的意思をもって知得しようとすること及び通信当事者の意思に反して当該事項を自己又は他人の利益のために利用することも含まれる. したがって,ISP 等が,例えば,特定の P2P ファイル交換ソフトに特有のパケットのパターンを検知して制御する場合のように,自己のネットワークを通過するパケットのヘッダやペイロード情報をチェックすること,特定のアプリケーションに係るパケットを検知すること,その結果を踏まえ当該パケットの流通を制御することは,それぞれの行為が「通信の秘密」の侵害行為に該当することになる. また,ISP 等が,ユーザのトラヒック量を検知して,特定のヘビーユーザについてはそのパケットの流通を制御することも,個別の通信に係る通信量を把握すること,当該把握に基づき制御を行うことになるため,それぞれの行為が「通信の秘密」の侵害行為に該当することになる.	不明だが,同一説かと推定される.なぜなら,「通信の秘密＝通信内容＋通信の構成要素」としているが,他人の秘密について言及していないことから,少なくとも峻別説ではないと思われるからである.
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(総務省[2010])	①DPI 技術を活用した行動ターゲティング広告については,ISP によってネットワークを通過するパケットの解析が行われるものであるため,4.で検討した個人情報保護法やプライバシー保護の関係に加えて,通信の秘密の保護との関係で検討が必要となる.以下では,通信の秘密の保護との関係を整理するが,同技術を活用した行動ターゲティング広告の実施に当たっては,個人情報保護法及びプライバシーへの配慮も併せて必要であることは言うまでもない. ②「通信の秘密」は,通信内容はもちろんのこと,通信の日時,場所,通信当事者の氏名,住所・居	①行動ターゲティング広告の法的問題としては,通信の秘密と個人情報保護・プライバシーの両方の配慮が必要であることを明記.次節で述べる「ストック情報」を想定した記述であると考えられる. ②次節で指摘するように,通信の秘密と個

	所,電話番号などの当事者の識別符号,通信回数等,これらの事項を知られることによって通信の意味内容が推知されるような事項全て(通信の構成要素)を含むものである.電気通信事業に従事する者に対しては,通信の秘密のほか,契約の際に入手した契約者の個人情報等,個々の通信の構成要素とはいえないが,それを推知する可能性のあるものに対しても,守秘義務を課している.(注70 ただし,罰則は通信の秘密を侵害した場合に限られる.(電気通信事業法 179条))	人情報保護・プライバシー問題を混同している可能性がある.また注 70 の記述は,他人の秘密を包含しているかに見えるが,用語として「他人の秘密」に触れていない.

5 プライバシーあるいは秘密の一種としての「通信の秘密」とインターネットによる変化

前節の検討結果を踏まえて,そもそも「通信の秘密」を守るのは何のためなのか,そしてその要請はインターネットの時代に変化しているかどうか,を考えてみよう.

5.1 プライバシーとしての「通信の秘密」

「通信の秘密」の保持は,プライバシー保護の一側面である[63].しかし,共同体意識が強く,近代市民革命を経ていないわが国では,プライバシーの概念が未確立で,混乱さえ招いている.しかも,個人情報保護制度の導入が,それに輪をかけた傾向があり,感情が先走って学術的な議論が成り立ちにくい.そこで,本論に入る前に,まずプライバシーの定義と,その中における通信の秘密の位置づけについて,大まかな理解を得ておこう.なお,前者については必然的にアメリカの事例に依拠せざるを得ないが,ここでは細部に立ち入ることができないので,詳細は別稿(林 [2012])を参照されたい.

図表7. は,私たちなりに,アメリカでプライバシーがどう捉えられているかを一覧にしたものである.現在のアメリカの一般的な理解は,プロッサー[64]4 分類 を超えた点があり,6 つの支分権(図表 7. の「区分」欄の ① から ⑥)と考えるか,4 つのカテゴリー(同「備考」欄の,憲法的,空間的,情報的,財産権的)と考えるかしかなかろう[65][66].

---

63 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」と述べている.憲法的議論としては「通信の秘密は言論の自由を担保する手段」との位置づけも可能と考えるが,今日では少数派かもしれない.なお憲法には関連する規定として,「幸福追求権」(憲法 13 条),「検閲の禁止」(21 条 2 項前段),「適正手続き」(31 条)「令状主義」(35 条)があり,通信傍受という例外措置を考える際に問題となるが,ここでは深入りしない(井上 [1997] 参照).

64 Prosser の 4 分類とは,以下のものをいう.① 他人の干渉を受けないはずの私的な空間に侵入されること(intrusion),② 他人に知られたくない事実を公表されること(public disclosure of private facts),③ ある事実が公表されて他人の目に誤った印象を与えること(false light),④ 氏名や肖像などが他人によってその利益のために利用されること(appropriation)(この解釈は,林 [2005a]による).

65 ⓪と表記した「自己決定権」としてのプライバシーは日本人には馴染みが薄いが,アメリカでは服装やライフスタイルはもちろん,趣味や性的嗜好なども含んだものと考えられている.とりわけ女性における人工妊娠中絶の選択は,対立点が少ない大統領選挙の終盤では必ず浮上し,賛否が分かれる.

著作財産権における支分権を統一概念で捉えることが難しいように,これらは「諸権利の束」(bundle of rights)であり,当該個人の権利であるという以上の共通項を見出すのは,ほとんど不可能である(Post [2003]).

図表7. 現代アメリカにおけるプライバシーの分類

区分(支分権?)	定義	類似の概念	人格権か財産権か	備考
①自己決定権	性的志向や,(女性の場合)子供を生むか生まないかを,自分が決定する権利		人格権(基本的人権の一種)	「憲法的プライバシー」とも呼ばれる
②不法侵入	他人の干渉を受けないはずの私的な空間に侵入されること		人格権	プロッサーの 4 分類の 1 種.「空間的プライバシー」
③私事の公開	他人に知られたくない事実を公開されること(未公表著作物を公表されないことを含む)	④ 名誉毀損とは別という立場もあるが,実際上は競合する場面が多いと思われる	人格権	同上.次項と合わせて,「情報プライバシー」
④誤解を招く公表	ある事実が公開されて,他人に誤った印象を与えること	同上	人格権	同上
⑤不正利用	他人の名前や類似性を無断で利用し収益を上げること	コモン・ロー上の著作権(大陸法系では,公表権)	人格権寄り	同上.これも情報プライバシーと言えるか?
⑥パブリシティの権利	有名人が,自分の氏名や肖像・似顔絵などを,商品化して売り出す権利	わが国では「競走馬のパブリシティ」が争われた.	財産権	⑤と混同される場合もあるが,純財産権的

5.2 秘密の一種としての「通信の秘密」

一方,「通信の秘密」の保持は,「秘密保護」の一類型でもある[67].秘密の保護対象

---

66 情報的プライバシーなどの概念は,村上 [2010] による.

67 わが国では,現行憲法が平和主義を掲げて以来,「秘密は無い方が良い」といった漠然たる感情が支配し,包括的な「秘密保護法制」を十分検討してこなかった嫌いがある.尖閣諸島での中国船衝突事件(2010 年 9 月 7 日)の映像流出が問題になったため,やっと秘密保全法が上程されたが,それすらも店晒しになっている.

は,国家・企業・個人といったように,その保有者(秘密は情報の一種であるため「占有」できないので,有体物のように「所有」という状態を観念しにくい)で分類されるのが通例であるが,その中に「保有者にかかわらず流通過程にある秘密の保持」という類型を追加すべきであろう(林 [2005b]).これを表示すると,図表 8. のようになる.この「流通過程にある秘密の保持」の類型こそ,「通信の秘密」の要請に他ならない[68].

図表 8. 秘密の漏洩に対する刑事罰

秘密の保有主体( )内は秘密の名称	秘密の流通過程	実定法の具体例	懲役刑の量刑
国家		特別防衛秘密 防衛秘密 国家公務員の守秘義務	10 年以下の懲役 5 年以下の懲役 1 年以下の懲役
	(電気)通信	通信の秘密(事業従事者の場合) 無線通信における暗号復元	有線＝3 年以下の懲役,無線＝2 年以下の懲役 1 年以下の懲役
企業(営業秘密)		不正競争防止法	10 年以下の懲役
個人(個人情報)		個人情報保護法	行政罰＊であり,かつ直接罰はない

＊ 他に行政罰として,多数の例がある.

(出典)林 [2005b] の記述を表にまとめたもの.

図表 8. にも見られる現在の秘密保護法制の問題点は,① 刑法に秘密保護の一般的規定がないこと(刑法 13 章にはわずか 3 条しかなく,133 条(信書開封)は「通信の秘密」の一種を守り,134 条(秘密漏示)は特定の職業従事者の守秘義務を定め,135 条(親告罪)は,その手続きを定めたものに過ぎない),② したがって多くを個々の法律,特に行政法規に委ねていること,③ 刑の軽重がバランスを欠いているのではないかとの疑いがあること(特に,公務員の守秘義務意違反が軽すぎること),といった諸点であろう(林 [2005b]).

以上を総合すると,通信の秘密は,図表 7.では ③ のパターンとして情報プライバシーのカテゴリーに属し,図表 8. における「流通過程の秘密の保持」であることは,日本的理解では異論がなかろう.しかしアメリカでは,コモン・ロー(判例を中心とした法体系)という特徴もあって,図表 7.に関しては ② の発展系として形成されてきた(林 [2005a]).すなわち当初は,物理的侵入を伴う通信の秘密の侵害だけが違法とされており,次第に「プライバシーの期待空間」という形で,物理的侵入を伴わない侵害も違法とされるようになった(この転換点に立つ歴史的判決として,カッツ事件判

68 情報という無形財を保護する手段として知的財産型と秘密型があるが,「情報法」という名をを冠する書物でも,このような「情報法の客体論」は十分に展開されていない(林 [2011b]).

決がある[69].

また近代的なプライバシー侵害の代表例である「私的事実の公表」(図表 7.の③)については,憲法修正 1 条(言論の自由を定めた条項)があるため,常に「私的利益と公的利益との均衡」が要請され,名誉毀損(同 ④)との境界が曖昧になっている.その結果,とりわけ言論機関の報道内容については,「公益性あり」との推定が働いているのではないかと思われるほどである[70].

このような歴史的経緯は,現在でもアメリカにおける法解釈に影響を与え続けており,わが国ほど「通信の秘密」に神経質ではないようである.より具体的なアメリカの特徴は,以下のような諸点である.① わが国と違って憲法には該当条文がない.② 連邦通信法[71] 705 条が,通信事業者だけでなく「何人も」侵してはならない事項を定めているが,この規定そのものが,冒頭で「合衆国法典 18 巻 119 章(通信の傍受)の場合を除き」と留保条件付である.③ これ以外にも,FISA[72]や愛国者法[73]など,特別法による適用除外が数多くある.④ 上記 ②の違反行為の罰則は,当然定められている(連邦通信法,501 条,502 条)が,705 条には「通信内容」と「その他の秘密」を区分するような表現はない.

5.3 インターネット利用に係る事例の特徴点

これまで述べてきたインターネットにおける通信の秘密に関する 7 つの事例から,特徴として以下のような諸点を挙げることができる.

1) 蛮人の行為を防ぐ行為が,通信の秘密からみて正当業務行為などに該当するので,違法性阻却事由があるとされたのが,プロバイダ責任制限法,迷惑メール,自殺予告,大量通信等,帯域制御の 5 事例である.また,ぷららの Winny の遮断行為は利用者の同意を取ることで適法行為とされた.現時点では,DPI 技術を利用する行動ターゲティング広告は,正当業務行為とは認められないため,利用者の個別・明確な同意を取る必要があるとされている.
2) 広義の通信の秘密には,通信内容(狭義の「通信の秘密」)と通信の構成要素とされる事項(「他人の秘密」)があるが,プロバイダ責任制限法における ISP による権利侵害情報と思われる情報の削除,迷惑メールの送信防止措置(電気通信役務の提供拒否)は通信内容そのものに関する措置である.一方,同法における発信者情報開示,自殺予告等の発信者情報の開示,大量通信等や帯域制御に関しては,主として通信の構成要素(すなわち「他人の秘密」)に対する措置である.
3) また,違法性阻却事由としては,まず通信設備に支障を与え,円滑な電気通信

---

69 Katz v. United States, 389 US 347 (1967)

70 言論機関の報道が,名誉毀損であると主張する者は,報道に「現実の悪意」(actual malice)があることを立証する責任があるとして,挙証責任の転換を図っている最高裁の判決があることは,このような推測を可能にしている.New York Times v. Sullivan, 376 U.S. 254 (1964) 参照.

71 Communications Act of 1934 as Amended by Telecommunications Act of 1996

72 Foreign Intelligence Surveillance Act, Public Law 110-261(2008 年修正)

73 いわゆる USA PATRIOT Act

役務の提供を確保するためとされるのが,迷惑メール,大量通信等,帯域制御の事例である.加えて帯域制御に関しては,利用者間の公平性が理由のひとつに挙げられ,通信設備の可用性確保に着目している.

4) 一方プロバイダ責任制限法では,発信者(表現者)の表現の自由を守りつつ,権利を侵害されたと主張する人の権利を守る場合に,書き込みの削除や発信者情報開示ができるとしている.また自殺予告のガイドラインでは発信者の生命に関して「現在の危難」,「補充性」,「法益の権衡」という緊急避難(刑法 37 条 1 項)の要件を満す場合に,発信者情報の開示ができるとしている.これらの事例では,通信当事者の権利なり生命の危険に対処することが理由となっている.

5) ISP の違法性阻却事由が認められた事例では,通信の流通過程で ISP が行なう行為(フロー情報)に関する事例が迷惑メール,大量通信等,帯域制御の事例であり,通信が行なわれてネット上に存在する通信の結果としての情報(ストック情報)に関するものが,プロバイダ責任制限法と自殺予告の事例である.

6) ガイドラインについては,迷惑メール(特定電子メール)のガイドランを行政機関(総務省)が策定している以外は,業界団体が策定している.ただし,業界団体がガイドラインを策定している場合でも,総務省がオブザーバーなどとして関与しており,実際の違いはそれほどないのかもしれない.このように,事業者あるいは業界団体の自主規制(self-regulation)に加え,規制当局がその策定・運用に一定の関与しており,生貝[2011]のいう共同規制の色彩が強いようである[74].

5.4 インターネット利用における「通信の秘密」の変化と対策

以上のケース・スタディを元に,インターネット利用における通信の秘密に関して,時代の変化に即応するにはどうすべきか,を考えてみたい.

1) フローからストック情報へ

従来の通信手段の代表格である電話は,1 対 1 の即時型通信である.その特徴は,第1に当事者間の通信であること,第 2 に即時型で記録が残らない場合が多いことである .つまりフローとしての当事者間情報が「通信の秘密」の保護対象であるため,主としてプライバシー保護の観点から,「電気通信事業者の取扱中に係る」(事業法 4 条 1 項)通信を保護するのが,合目的的であったと考えられる .

一方インターネットにおける通信のうち,ホームページや SNS・ブログなどのソーシャルメディアでは,内容に秘匿性のない「公然性を有する通信」 がトラヒックの大宗を占めている.公衆に対してなされた言説なのだから秘匿性はなく,「通信の秘密」が適用される場面はなさそうに見える.

ところが 3.8で述べたように,Twitter での書き込みが他の情報と照合されて発信者が特定され,バッシングを受け「さらし」に会うケースも生じている.つまり「インターネットは忘れない」(矢野 [2007])という特質がデメリットとなって,フロ

74 共同規制というのは,主に EU の情報政策分野を中心に世界各国に広がりつつある,企業や業界団体の行なう自主規制に対して,政府が枠組み設定や監視・罰則権限の保持等を行なうことによって,柔軟な自主規制のメリットを活かしつつも,適切な政府関与をすることで確実に目的を達成していこうという政策手法.生貝 [2011] 参照.

一情報ではなくストック情報から,思わぬ被害も生ずるということである .

2) 個人の特定可能性と通信の秘密

上述の例は,発信がなされた結果,ネット上に大量の情報が検索可能な形で蓄積されていることから生ずる(これは公然性を有する通信の帰結でもある).このことは,上述の「電気通信事業者の取扱中に係る」の解釈にも関わる問題である.すなわち,通信回線を流れている通信内容だけが問題なのか,終了後の通信内容にもこの「取扱中」の規定が及ぶのかとの問題である[75].

その代表例として先に Twitter の例をあげたが,そこでの論点は,どこかで聞いた覚えがないだろうか? そう,個人情報保護法における「個人情報」とは,「生存する個人に関する情報であって,当該情報に含まれる氏名,生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ,それにより特定の個人を識別することができることとなるものを含む.)」(同法2条1項)であった.Twitter の書き込み情報が上記に該当すれば,それが匿名や変名のものであっても,法的には「個人情報」ということになる[76].

ここにインターネットという前例のないシステムの,特異性と危険が隠されている.この論点は,プライバシー保護の手段として個人データを保護することが所期の目的を達成しているか否か,という論点と交錯する点が多い.

3) 「通信の秘密」と「他人の秘密」の峻別と適切な解釈

以上の検討結果から,現代においては,フロー情報に関する「通信の秘密」も大切だが,ストック情報に関する「他人の秘密」を守る意味が,相対的に高まっていることが判明した.そこで,一時背後に退けられていた峻別説,すなわち「通信の秘密」と「他人の秘密」を峻別する考え方を,もう一度検討してみる必要がありそうである[77].

つまり,両者を峻別した上で,「通信の秘密」にはそれ相応の,「他人の秘密」には別途それにふさわしい保護のあり方を考えよ,ということである.この点を曖昧にしておくと,従来の「同一説」の延長線上で考えるか,明確な意思表示なく「なし崩し的に」逸脱した解釈を導くか,というジレンマに陥ることになりかねない.

現に所管する総務省において,研究会の報告書の中とはいえ,「通信の秘密」について「通信内容」に加えて「通信の日時,場所,通信当事者の氏名,住所・居所,電話番号などの当事者の識別符号,通信回数等,これらの事項を知られることによって通信の意味内容が推知されるような事項全て(通信の構成要素)

---

75 「通信の秘密」保護の始期と終期については,高橋・吉田 [2006] 参照.

76 もっとも同法は行政法であり,規制の対象としての「個人情報取扱事業者」に該当するか否かについては,別途の判断が必要になる(同法 2 条 3 項など).

77 3.8 では通信内容と通信データ部分についての保護を論ずる必要について述べたが,通信データ部分に該当する通信の構成要素としてどのような事項を入れたらよいかについては,この内容をその性格に応じて細分化したうえで,通信の秘密の対象とすべき構成要素と対象外とすべき構成要素に分けることも,インターネット利用の規律の国際的ハーモナイゼーションを考慮すれば,今後の課題になるであろう.例えば,サイバー犯罪条約では,traffic data という用語が,またイギリスの 2000 年捜査権限規制法(Regulation of Investigatory Powers Act 2000=RIPA)では,第 2 章 21 条で communications data という用語で通信データ部分をトラヒックデータ,サービス利用データおよび利用者情報の三つに分けている.

を含むものである」という考えが示されている(総務省 [2010]).この考え方は,同一説の延長だとも考えられるが,通信の秘密を拡大解釈したとの疑いも持たれる.

同報告書は上記箇所に続いて「通信の秘密のほか,契約の際に入手した契約者の個人情報等,個々の通信の構成要素とはいえないが,それを推知する可能性のあるものに対しても,守秘義務を課している」と述べた上で,その注において「ただし,罰則は通信の秘密を侵した場合に限られる(電気通信事業法 179 条)」と述べている.ここでは,通信の秘密の延長線上にあるものと,それとは保護法益や保護対象を異にする個人情報が,混同されている恐れが強い.

また注の記述については,既述のとおり「可罰性あり」とする説と,「なし」とする説が対立していたはずだが,総務省は新たな解釈を打ち出したのだろうか?罪刑法定主義の観点から「可罰性なし」を主張する共著者も,「結果オーライ」と喜んでいる訳にはいかない.法的な考察は,結果よりもそこに至る過程の方が,大切だからである.

4) 発信者情報の扱い

総務省 [2010] に賛同できないとすれば,秘匿性のない通信内容に関する通信の構成要素はどう考えれば良いだろうか.通信の構成要素のすべてを,通信の秘密に包摂していこうとする考えには疑問があるが,発信者情報だけは別かもしれない.仮に秘匿性のない通信内容の場合であっても,発信者情報には表現の自由を守る観点から,保護が及ぶべきとの考えもある[78].

また,プロバイダ責任制限法 4 条には発信者情報開示に関する規定があることは,発信者情報に重きが置かれていることの証左である.そういえば,電話時代に通信の秘密が問題になったのは,3.7 で紹介した発信者番号表示サービスであった.

6 4つの提言

以上の検討を踏まえて私たちは,結論として「技術絶対主義」を緩和した「心地よい DPI」の可能性を探る一方で,「硬直的な通信の秘密」に代わる「程よい通信の秘密」を模索することを提案したい.これは,あまりに常識的だが,常識を実現するための具体策として,① オプト・インかオプト・アウトかといった二者択一ではない選択肢の提示,② 「通信内容」と「他人の秘密」の峻別と,事業に従事する者以外の者の「他人の秘密」侵害に対するサンクションの見直し,③ 電気通信事業者ではない ISP の認知,④ 違法性阻却説から構成要件該当性否認説へ,といった新しい考え方も併せて提案したい.

78 松井 [2010] は,「匿名で表現することも表現の自由に含まれると解すべき」としている.

6.1 提言1＝DPI に関する「心地よさ」の保証:二者択一でない選択肢の提示

世間では依然として,個人情報の漏洩事故が後を絶たない.漏洩された本人は,良い気持ちがしないのはもちろんだが,しかし実害がどの程度かと問われれば,漏洩した側もされた側も,明確な尺度を持ち合わせていない.個人情報の漏洩とプライバシーの侵害との因果関係は,それほど漠としたものであるし,プライバシーの侵害そのものも,客観的尺度で測りにくい[79].満員電車で知らぬ人と体がくっつくのは避けたいが,恋人とならぴったりくっついていたい」.

また仮に,個人情報の漏洩がプライバシー侵害につながるとして,どこまで事前に抑制すべきか(あるいは,できるか)は,さらに難問である.厳しい規制をすれば「過剰反応」が起きて,小学校のクラスの連絡電話網が消滅する,災害時要支援者の一覧表が共有されない,といった事態を招く[80].それでは何もしないでいれば良いかというと,企業の場合は顧客の信用を得ることができないから,ビジネスに支障が出る.しかし過剰も過少も,「個人情報の保護がプライバシー侵害を阻止し得る」と考えている点では,同じ「思い込み」に囚われているのかもしれない.

しかも,個人の考え方は多様化している.「プライバシーを売る」というと非難すべき行為と受け止められるかもしれないが,ショッピング・サイトなどで有利な特典が得られるとなれば,人々は喜んで個人情報を「売り渡す」[81].若い世代は,他人と知り合いになれるというだけで,唯々諾々とプライバシー関連情報を公開している.芸能人は,自分の結婚・離婚や,冠婚葬祭を売りに出す場合もある.これらは,すべて歓迎すべきこととは言えないが,逆にすべて禁止すべきことども言えない.

つまりプライバシー関連情報の扱いで困った点は,① 事後になれば,「あれは良い.これはダメ」というパターンをある程度判断できるが,事前に決めておくのは難しい,② それでもなお事前に決めるのが良いとすれば,かなりの組み合わせの選択肢を用意しておかねばならない,という 2 点に集約されよう.

そこで両極端を排して,中庸を得た解決策を探る時期が来たのではないかと考えるが,その際には著作権の事例が参考になる.というのも,著作権は「情報」という無形の財貨に対して,何らの手続きを要せず排他権を付与する(無方式主義)という仕組みであるため,プライバシーを含めた「情報」の法的位置づけを考える際の,先行事例となり得るからである(プライバシー権を初めて世に問うた Warren & Brandeis [1890] も,未公表著作物の取り扱いを思考実験の事例にしている.林 [2012][2005a] 参照).

加えて私たちには,クリエイティブ・コモンズの世界的展開に関して,いささかの経

79 アメリカの憲法学者である Robert C. Post も,以下のように述べている.Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings. (Post [2001]).

80 いわゆる「過剰反応」の実例については,以下を参照.
http://www.caa.go.jp/seikatsu/kojin/chousa07.html

81 情報処理振興機構(IPA)の調査によれば,人々は世間で言われるほどプライバシーを気にしておらず,ある程度のメリットがあれば,安易に個人データを提供している.http://www.ipa.go.jp/about/press/20100813.html

験もある[82].クリエイティブ・コモンズとは,レッシグなどの呼びかけに呼応した社会運動で,著作権者による All Rights Reserved を認めるでもなく,利用者による No Rights Reserved = All Public Domain を認めるでもなく,その中間である Some Rights Reserved を認めようとするものだからである(クリエイティブ・コモンズ・ジャパン(編)[2005]).

このような中庸を担保する方法として,先のレッシグの分類によれば,① norm,② market,③ law,④ code あるいは architecture,の 4 つがあり得るが,現実のビジネスが「権利強化一本やり」と「すべてパブリック・ドメイン」という形で分断されていることは,① と ② が機能していないことを意味する.とすると,残された手段は ③ か ④ ということになる.

③ による方法には,ハード・ローの改正によるものと,業界基準などのソフト・ローによるものがある.しかし上述の分断を前提にすれば,ソフト・ローしかあり得ないと思われる.サービス提供者が独自か,業界が結束して普通契約約款を定め,その中で選択肢を用意する方法である.④ のコードまたはアーキテクチャーによる方法とは,それを技術的に支えるソフトウエアを準備することであり,実行上は両者の組み合わせが望ましい.

クリエイティブ・コモンズの実際では,図表 9. のようなマークで利用者が利用条件を容易に識別できるようにした上で,これを支える普通契約約款(deed)と,html ベースのソフトウエアを用意している.すなわち図表の両端にある,© (権利 100%)と PD(Public Domain)の間に,以下の 6 つの組み合わせを許容しようとするものである.

図表 9. クリエイティブ・コモンズの許諾条件

しかも,この組み合わせの元になる権利表示は,図表 10. のわずか 4 つの記号である.それぞれは前述のごとく,マークと約款とソフトウエアで構成されており,図表 10. のような意味を持つものと説明されている(「表示」などの日本語訳が分かりにくいので,私たちの責任で,英語の表記も付加した).

図表 10. クリエイティブ・コモンズにおける権利表示

BY マーク(attribution)

表示

作品のクレジットを表示すること

NC マーク(non-commercial use)

非営利

営利目的での利用をしないこと

82 共著者の 1 人である林は,クリエイティブ・コモンズ(CC)がまだ「カウンター・コピライト」と称していた 1999 年に「デジタル創作権」(ⓓマーク)を提唱したので,ある意味ではクリエイティブ・コモンズのライバルでもあったが,彼らの趣旨に賛同して契約約款の日本語化を世界に先駆けて実施する手伝いもしたので,この間の経緯は熟知している(林 [1999a] [1999b],クリエイティブ・コモンズ・ジャパン(編)[2005] 参照).

ND マーク(no derivatives)
改変禁止
元の作品を改変しないこと

SA マーク(share alike)
継承
元の作品と同じ組み合わせの CC ライセンスで公開すること

利用可能な組み合わせを,パブリック・ドメイン(PD)寄りのもの,すなわち右寄りから説明すると,次のようになる[83].いささか細部に入りすぎる懸念はあるが,プライバシーについて同様の仕組みが可能かどうかを議論するため,お許し願いたい[84].なぜなら,これは(権利の仲介者ではなく)権利者自身が著作物の流通過程をコントロールしようとする権利表示システム(Digital Rights Expression= DRE)であり,「自己情報コントロール権」を主張する向きがあるプイラバシーの権利表明にも,役立つはずだからである[85].

1) 著者の氏名等を表示し,自由に(営利目的を含む,以下同じ)利用する旨の宣言(BY マーク)
2) 著者の氏名等を表示し,改変結果をすべての人が利用できるようにするので,自由に利用する旨の宣言(BY マーク+SA マーク)
3) 著者の氏名等を表示し,改変しない条件で利用する旨の宣言(BY マーク+ND マーク)
4) 著者の氏名等を表示し,非営利目的で,自由に利用(改変したり配布したり)する旨の宣言(BY マーク+NC マーク)
5) 著者の氏名等を表示し,非営利目的で,改変結果をすべての人が利用できるようにするので,自由に利用する旨の宣言(BY マーク+NC マーク+SA マーク)
6) 著者の氏名等を表示し,非営利目的で,改変しない条件で利用する旨の宣言(BY マーク+NC マーク+ND マーク)

プライバシーの扱いは,著作権の支分権の扱い以上に困難が予想される.現に既存の P3P(Platform for Privacy Preference)などは,必ずしも期待通りの成果を上げていない[86].著作権の DRE で成功したレッシグも,P3P への期待は過大だったのかもしれない.しかし,プライバシーの権利表示に成功すれば得られるメリットはさらに大きい.そろそろ皆が,その努力をする時期に来たのではないかと思われる.

その具体例として,次の 2 つを分けて考えると,案外進展があるかもしれない.それは,

---

83 詳しくは,以下のクリエイティブ・コモンズのサイトを参照されたい.
http://creativecommons.jp/licenses/

84 6 つの組み合わせを仔細に見れば,氏名表示(BY マーク)は,すべてに共通であることに気づかれるであろう.実は発足当初のクリエイティブ・コモンズの案では,これは 1 つのオプションであったが,その後必須とされるようになった.林の㋑マークは,氏名表示権を中心に構成されていたので,この点では両者の接近がなされたことに,ある種の感慨を覚える.

85 共著者は「自己情報コントロール権」そのものには否定的であるが,「個人データを property 的に扱う」ことには意義があると考える.ただし,その見返りに「人格権」は放棄せざるを得ないことに,日本の法学者は気づいていない(林 [2012]).

86 http://www.w3.org/P3P/

① 個人データを氏名と結びつけたまま使う＝BY マークに同じ.これは「通信の秘密」型,
② 個人データを匿名化して使う＝cc やマークと反対の Non-Attribution という権利宣言を考える＝「他人の秘密」型,という区分である.前者を NC マークを中心に,後者をシェア・アライク・マークを中心に構成し直すことができれば,クリエイティブ・コモンズのアイディアを個人データに拡張できることになる.これは先に述べた,「発信者情報を別扱いする」という発想に通ずるものである.

6.2 提言 2＝通信の秘密の硬直的解釈から「程よい」解釈へ:「通信内容」と「他人の秘密」の峻別と,新しい時代にふさわしいサンクション制度の見直し

次に,「通信の秘密・原理主義」でもなく,「通信の秘密無視」でもない,「程よい」通信の秘密とは,どの程度と考えれば良いのだろうか.読者の中にはスパム対策として,Baysian Filter を入れている方もおられるだろう[87].それによって,一旦 [spam] に分類されたメールを,後刻見直して「やはりスパムだ」としたり,一部は「正常なメールだ」と判断して「着信メール」のフォルダーに入れ直したりしているのではないだろうか.後者の確率は当初ある程度高いが,手動による再分類をソフトウエアが学習するにつれて,比率は下がってくる.やがて,ほとんど人手を要さないでスパムの分類ができるので,いらいら感が大幅に緩和された経験をお持ちだろう.

このやり方は,受信者が受信者自身のメールを分類しているので,通信の秘密の問題は生じない.ところが,同じことを ISP の頼むとすると,どうだろうか？ もちろん,メールを受信する人と ISP との間で契約を交わしているだろうから,原則的には ISP は受託者であり,委託者である受信者の意を汲んでいる限り違法性はないとも言える.しかし例えば,スパムに該当すると判断されたメールを全部,ISP が削除してしまい,受信者にも知らせないような契約だったらどうだろうか？

現にグーグルが提供する Gmail の仕組みは,それに近いように思われる.「スパムが一切来ないので嬉しい」という利用者もいるかもしれない.しかし,「スパムでないものをスパムと判定してしまう」リスク,すなわち false positive の誤りは避けようがないから,本来伝達すべきメールが伝達されない危険を内包していることになる[88].つまり,一定の確率で「通信の提供そのもの」を拒否していることに等しく,4.4 で述べたぷららネットワークスの事例と同様,「通信の秘密」以上に問題ではないかと思われる[89].この点に関する限り,「通信の秘密」の主旨や,その元になっている「検閲の禁止」の

87 ベイジアン・フィルタ (Bayesian Filter) とは,単純ベイズ分類器を応用し,対象となるデータを解析・学習し分類する為のフィルタ.学習量が増えるとフィルタの分類精度が上昇するという特徴をもつ.個々の判定を間違えた場合には,ユーザが正しい内容に判定し直すことで再学習を行なう.
http://ja.wikipedia.org/wiki/

88 誤った判定には 2 つのタイプがある.スパムフィルタの例では「本当はスパムではないのにスパムと判定された(大切なメールがスパムフォルダに行ってしまった)」という場合と,「本当はスパムなのにスパムではないメールと判定された(スパムが受信箱に入ってきた)」という2つの場合である.英語では前者を false positive,後者を false negative と呼ぶ.

89 NTT ぷららのサービスでは,スパムと認定されたメールも,一定期間は見ることができるようになっており,期間経過後自動的に削除される.

主旨を徹底する必要があろう.

他方,「通信の秘密」を余りに厳密に解釈することは,折角の新技術の実用化を阻害する恐れが強い.3.7 で述べた発信者番号表示制度は,検討当初はプライバシー上の問題を指摘する声が多かった.しかし実際に導入してみると,喜んで利用する人が多く,携帯電話においてはデフォルト設定にさえなっている.これを文化的にみれば,発信者番号表示制度以前の電話は,「ベルが鳴ったら必ず出ましょう」という「発信者優位・受信者無視」の仕組みであったが,この制度以降は「発信者と受信者の権利のバランスを取る」仕組みに変質した,と評価することができる.

技術の進歩は,通常既存の秩序と相容れない場合が多い.そこで,予見される懸念が多い場合,技術開発にストップをかけるべきか否かが問題になる.しかし既に述べたように,ことがプライバシーに関わる場合,事前に侵害の態様を類型化することが難しく,最終的には裁判所の判断を仰がねばならないケースが多いことに留意する必要がある.これを言い直せば,「まずやってみて,問題があれば事後的に対応する」ということにならざるを得ない面が強い,ということである.

そこで具体的に「程よい」通信の秘密を実現するためには,以下の 4 点が必要ではないかと考える.

- 「検閲の禁止」は,スパム・メールを利用者の承諾なく消去することにも及ぶことを明確にする(迷惑メール対策法に明記する).
- 「通信の秘密」は,通信内容にのみ及ぶものであることを明確にし,それに付随する情報は「他人の秘密」として峻別する(電気通信事業法の改正).
- 「他人の秘密」の侵害が,電気通信事業従事者以外の者によってなされた場合には,加罰性がないことを明確にする(電気通信事業法の改正).
- 刑事罰を科さない代わりに,民事的な救済手段をソフト・ローとして整備する.具体的には,次項のコミットメント責任をモデルに,業界単位等でコミットの内容を標準化し,それに違背した場合には相応の損害賠償責任を負うことを明確にする(法改正は要さない)
- 逆に,電気通信事業者以外の者によって「電気通信役務」(電気通信事業法 2 条三号)と同等のサービスが提供されていることを前提に,「通信の秘密」は何人も侵してはならないものであることを明確にする(電気通信事業法の改正).

これらを法文としてどのように構成するかは,立法技術に未熟な私たちに十分な素養がないので,専門家に委ねたい.ここでは誤解を避けるために,上記の考えに従えば前述の図表 4. は,次の図表 11.のように読み替えられることだけに触れておきたい.

図表 11.「通信の秘密」と「他人の秘密」の可罰性(改正提案)

保護対象 / 罰則	「通信の秘密」(4 条 1 項)	「通信に関して知り得た他人の秘密」(4 条 2 項)
あらゆる侵害(改正 179 条 1 項)	Ⓐ 何人も侵害者になり得る	Ⓑ (加罰性なし)
電気通信事業の従事者による同上の侵害(改正 179 条 2 項)	Ⓒ 電気通信事業の従事者のみが侵害の主体になり得る(身分犯)	Ⓓ 電気通信事業の従事者のみが侵害の主体になり得る(身分犯)

なおここで,私たちの案が 4.8 や 4.9 で述べた「これからは通信の秘密も大切だが,他人の秘密を守る意味が高まってくる」という指摘と矛盾するのではないか,という批判に答えておこう.一見すると,「他人の秘密」の侵害が電気通信事業従事者以外の者によってなされた場合には,可罰性がないことを明確にするという案は,責任を軽減しているかのように思われる恐れがあるからである.

確かに一般的には,民事責任よりも刑事責任の方が,責任の追及が厳しいような印象がある.しかし,たとえ個人に対する場面ではそれが妥当するとしても,法人にそのまま当てはまるとは限らない.現行の法体系は「個人責任があって,初めて法人の責任が論じられる」という建前を取っていて,法人が刑事責任を問われるのは,「両罰規定」がある場合に限られる90.つまり見かけとは違って,法人の刑事罰はごくレア・ケースなのである.

加えて,情報を扱うに際しての刑事責任を法定することが如何に難しいかは,「情報窃盗」の例を見れば明らかである.有体物が「窃盗」から保護される(刑法 235 条ほか)のに対して,いわゆる「情報を盗む」という行為が罰せられるのは,図表 8.にもあるとおり「営業秘密」など特定の場合に限られる(林 [2011]).さらに,「秘密」として保護したい情報が,現在の刑法で保護される仕組みにもなっていない(前述のとおり刑法 13 章の「秘密を侵す罪」は,秘密一般を保護するものではない).

このようなことから,個人情報を漏洩した者に,刑事罰を直接科すべきだとする意見(いわゆる「直罰方式」)はあるものの,実現可能性は低いし,また実現すべきではなかろう.そのためには,刑法 13 章全体の見直しが必要だからである.とすると,刑事罰に傾斜するのではなく,民事的な対応がどこまで可能かを見定める方が現実的となる.共著者の態は,そのような意味で理解していただきたい.

6.3 提言 3=「事業者」の自己宣言(非宣言)というコミットメントによる電気通信事業者ではない ISP の認知

上記のような案を実施する場合,「電気通信事業者」と「非電気通信事業者」を区別するメルクマールが,従来以上に重要になってくる.従来なら,これは法定事項であり,電気通信事業法に明記すべきことという考えが主流になりそうである.しかし同法の歴史をみれば,当初「第1種電気通信事業者」と「第2種電気通信事業者」に区分していたものを,1997 年の改正で「規制緩和」の観点から廃止した経緯がある.

当初両者を峻別していたのは,旧電電公社のように巨大な設備投資をして事業を展開する場合と,回線等を第 1 種事業者から借りてコンピュータ等を接続するだけで身軽に事業を展開する場合では,ビジネス・モデルに優位の差があると考えられたことであった(林 [1984],[2005a]).そこで,前者は許可制で,後者は登録制か届出制で規制されることになった(電気通信法制研究会 [1997]).

しかし,コンピュータから生まれたサーバやルータが,電気通信設備としての交換機に取って代わるようになり,また通信の分野でも光ファイバやデジタル無線技術の進展によって,設備のダウンサイジングが可能になった.これによって価格と性能の

90 法人の業務に関して,法人の代表者や従業員(法令上は従業者)が法の定める違反行為をした場合に,その従業者等と事業主体である法人の両方を処罰する旨定めた規定.

比率が大幅に改善するようになったため,「第 1 種」と「第 2 種」の差はほとんど無くなってきた.しかも規制緩和の考え方が浸透してきたので,全体として規制色を弱める必要が生じた.そこで,2003 年に電気通信事業法が抜本的に改正され,第1種と第 2 種の区分は廃止されたのである(多賀谷・岡崎 [2005]).

日本企業はこのような流れを熟知しているし,しかも「お上」に従順であったから,ISP に属する多くの企業は当初から第 2 種の登録等をして,自ら「電気通信事業者」であることを誇りにしてきた[91].この時,「当社は他人の通信を媒介するのではなく,情報サービスを提供する会社である」と位置づければ,第 2 種の登録等を要せず,自由市場で営業することができたし,私たちがそのような道を慫慂していたことは既に述べた(林 [1984]).

このような事態は,コンピュータと通信がほぼ一体化したインターネットの時代には,より現実味を帯びてきた.なぜなら,ここでは第1種と第 2 種の区分が曖昧になるだけでなく,事業者と利用者の区分も曖昧になるからである(林・湯川・田川 [2006]).この機を捉えたアメリカの企業は,前述のとおり「情報サービス」が非規制であることを所与として,「電気通信事業者でない ISP」として事業展開するのみならず,同じ発想でわが国に進出している.

そのため大部分が電気通信事業者であるわが国の ISP と,電気通信事業者とは名乗っていないアメリカ系の事業者との間で,「不平等競争」(level playing field がない競争)が起こっている.しかも Google 等のアメリカ系の事業者は,日本法人を設立しているものの権限は限られており,事業展開の基礎となるサーバ等はアメリカ本国においているため,総務省の権限外で事業展開していることになる.いわば「治外法権」を享受しているようなものである.

このような事態を放置できないと考えたのか,最近に至ってわが国のヤフーが「インタレストマッチ広告」という新サービスを始めると宣言して,話題を呼んでいる.これは,「メールの中身を機械的に解析し,関心の高い広告を配信するもの」(週刊ダイヤモンド編集部 [2012])だというから,まさに本稿で議論してきたものに他ならない.ヤフー自身も,「一部に行動ターゲティング技術を利用している」ことは認めている[92].ただし,前述した宅配便における違法託送品の検査のように,送り主や配送先に係りなくメッセージ内のキーワードだけを摘出・照合する技術であるという.

このような事態に,どう対処すれば良いだろうか.従来の流れに沿って考えれば,法改正によって対処することは,規制緩和の方向に反するかもしれず,良い方法とは言えまい.しかし根拠がないまま,総務省が行政指導できるような時代ではない.そこで参考になるのが,プライバシー・ポリシーに関するアメリカの「自己宣言方式」である.

アメリカのプライバシー保護に関する第三者評価認証制度である TRUSTe は,事業者がプライバシー・ステイトメントやポリシーをウェブ・サイト上に「表示」することで,消費者との間で一定の「コミット」をするよう制度上要請されている.つまり,わが国のプライバシー・マーク制度とは異なり,自己宣言を基調とする制度設計となってい

91 中には,第 2 種の中でもより規制が厳しい「特別第2種」の資格を得ようとして,要件(国際サービスの提供か,全国的など大規模な事業展開)のクリアに努力した企業も散見された.

92 http://listing.yahoo.co.jp/service/int/index.html

る[93].

そして,消費者に対して表示と異なる欺瞞的な行為をした場合は,FTC(連邦取引委員会)の調査権の発動を招く.民間の第三者評価認証制度が,事業者取得コストの負担を軽減しながら,法律との補完関係によって一定程度の消費者保護の実効性を確保できるという,好例として参考になろう(林・鈴木 [2008]).

そこで私たちは,法人責任を前提にして「コミットメント責任」という仮説を提示して,今後の議論を促している(林・田川・浅井 [2011]).コミットメントという用語はゲーム理論等において広く使われているが ,ここでの語感に最も近いと思われる定義は,主として行動経済学の分野で使われている「コミットするというのは,自分が将来にとる行動を表明し,それを確実に実行することを約束すること」(梶井[2002])であろう.

これらを踏まえ,以下の定義に該当するものを,を,「コミットメント責任」と呼ぶことにしている (林・田川・浅井 [2011])[94].

> 事業者が,情報管理の取扱いに関する約束事を消費者に対して表示し,または社会に対して宣言したにもかかわらず,それに違反することによって生じる責任(法的責任を中心としながらも,より広い概念としての責任.免責を含む)(林・鈴木[2008]).

コミットメント方式を,本稿の問題に適用すれば,以下のような仕組みを導入することを意味している.つまりISP 全社に,「電気通信事業者」であり続けようとするならば,「他人の秘密を含めた通信の秘密を,ミッションとして遵守する」旨のコミットメントを義務付ける.具体的には「通信の秘密保護ポリシー」の策定と,その公開(ウエブ上のホーム・ページにポータルを設ける)を義務付けるのである.

これに応じた社は,電気通信事業者として登録等が済んでいれば,そのまま現在の地位を認められるが,未済の場合は登録等を停止条件として,新たにその地位が認められる.他方これに応じない社,すなわちコミットしない社は,「自社は電気通信事業者ではない」ことを宣言したものとして,「非電気通信事業者」と認定される.

前述のとおり私たちの改正案では,「通信の秘密」と「他人の秘密」は峻別され,前者は国民であれば(あるいは,日本に活動の拠点を置く法人であれば),誰もが守らなければならない.しかし後者は,電気通信事業者にのみ課せられた責務であるので,コミットした者のみが,その適用を受け,他の者は刑事責任を免れる(しかし民事責任については,別にコミットすることを求められる).これを,法律を用いて分類するのではなく,自己宣言に基づいて分類しようとするのが,私たちの案である.

---

93 翻って,日本における運用の実際は,「プライバシー・ポリシー」に横並びに近い決まり文句を並べ,それに反するビジネスをしている企業があったとしても,対策は限られている.主務大臣はどのような関与が可能だろうか.公正取引委員会が,景品表示法等によって介入できるだろうか.日本情報経済社会推進協会(JIPDEC)が,認証を与えたプライバシー・マークを表示しながら,主旨に反する活動をしているとして,法律によることなく契約上関与できるだろうか.このあたりが不明確であるとしたら,「プライバシー・ポリシー」を表示することを推奨する現在の個人情報保護法制は,いったいどこまで考えて,何をねらいとしているのか,はなはだ疑問となってくる.事業者は誰とも「コミット」することなく,単なる形式的な表示をしているにすぎないからである(林・鈴木[2008]).

94 これは,経済学(市場主義),経営学(自律主義),法学(法治主義)の三分類との比較でいえば,自律主義を基本にしながらも,最低限法定される限界をわきまえて(法治主義),また市場における信頼の形成と維持に配慮しつつ(市場主義),企業があらかじめスポーツ大会における「選手宣誓」のような形で約束事を公開し,それに縛られる,という仕組みだと考えればよい.

このような方式は,サービス毎に適用することもできる.例えば,前述のヤフーの新サービスについて,ヤフーが自社のサイトでサービス内容を明示し,メッセージのどの部分を活かしているのか,無視しているのか,あるいは匿名科しているのか等を,コミットするのである.

6.4 提言④=違法性阻却説から構成要件該当性否認説へ

前 4.節で検討した事例はいずれも,「形式的には通信の秘密の侵害に当たるが,法に基づく(あるいは他の法益を実現するために不可欠な)正当な行為であるから違法性が阻却される」という論理構成を取っていた.

これは今までの法解釈では,主流の考えと言ってもよい.例えば,電気通信法制研究会(編著) [1987] においては,電気通信事業者の通常の知得行為が,違法性阻却事由となる構成が用いられている.すなわち「知得」とは「積極的に,通信の秘密を知ろうという意思のもとでなされる行為であって,偶然に通信の秘密を知ることはこれに当たらない」と述べるとともに,「電気通信事業者が業務上の必要から行う知得行為」について,「正当行為」(刑法 35 条)として違法性が阻却されると論じている.ここにおいて,「違法性阻却事由としての構成が示されていると評価することができる」(高橋・林・舟橋・吉田 [2008]).

これは,「外科医が行なう手術は,(形式的には傷害罪になり得るが)原則として違法性がない」という一般化した例で表わすことができる.しかし,外科医のケースは誰にでも理解できるのに対して,通信の秘密のケースはそれほど単純ではない.外科手術が違法でないことはすぐに分かるが,DPI が違法でないかどうかは,事実関係を細かく聴いてみなければ分からない,ということである.

これは繰り返し述べてきた,「プライバシーの事前規制は難しい」という事実を裏返した表現とも言えるが,法的な不確実性が残されていることは,ビジネス上は大きな問題である.特にわが国企業は,「石橋を叩いて渡る」「リスク回避的に行動するのが出世の秘訣」といった文化を持っているから,不確実性を極端に嫌う傾向がある.

その意味では,私たちが提案している「電気通信事業者でない者が,他人の秘密を侵しても可罰性がない」という方式は,ビジネスに役に立つものと思われる.この案では,違法性が阻却されるのではなく,その手前で構成要件に該当しない(そもそも犯罪類型に当たらない)ことが明確だからである[95].

仮に,秘匿性を要さない「公然性を有する通信」に関しては,「通信の秘密」の対象外(ただし,通信内容はともかく発信者情報には原則秘匿性がある)とすれば,ISP の多くの業務(1 対 1 の e メールのような依然として通信の秘密厳守の業務や発信者情報の秘匿を除く)は,通信の秘密の対象外になるので,違法性阻却事由を問題にするまでもなく,構成要件該当性がなくなる.もしそうなれば,ISP は自己の業務として,パケットの検知,利用が可能になり,1.2(ISP 業務は情報サービスで非規制)や 1.3(日米の競争条件の不均衡など)に述べた心配はなくなり,産業的にイコールフッティングが実現される.

---

95 その典型例はインテリジェンスのための通信の傍受であり,本稿では検討の対象から外した点に戻ることにならざるを得まい.

しかし上記のように,ISP の業務の多くで「通信の秘密」に関して構成要件該当性がなくなるということは,必ずしもISPが自由にパケットの検知や利用を行なって良いということを意味しない.行動ターゲティング広告を事例として考えてみよう.

まず,クッキーベースのターゲティング広告でも,4.8 で紹介した総務省の第二次提言では,事業者が利用者から取得し得る情報を個人識別性から評価して,それ単独では個人情報に該当しないとしている.しかし,ウェブ上の行動履歴や位置情報は,「個人の内面に係るような秘匿性の高い情報と考えられる」としており,これらの情報が「大量に蓄積され」,「転々流通するうちに個人識別性を獲得する」恐れがあるとしている.このため,プライバシー侵害のリスクを軽減するために,「行動履歴や位置情報等の取扱いについての透明性を高めることや,利用停止や取得停止等の利用者関与の手段を提供するなど,相応の配慮が求められる」とされる.

DPI 技術を利用した行動ターゲティング広告は,クラスタリング技術を利用して個人が特定されないようなシステムにしているとされているが,個人をより特定した方がよりカスタマイズされた広告配信が可能になるため,個人が特定されプライバシーが侵害される恐れもそれだけ大きいといえる.

この点については,通信の秘密の観点からではなく,プライバシーや個人情報保護の観点からの取り組みが必要であろう.この取り組みが他のインターネッ利用の事例と同じく十分になされるとすれば,通信の秘密の保護法益である,プライバシー保護が実現できることが期待できる.また,一方で,前述したように,国際的なイコールフッティングが実現できるという,ウイン・ウインの関係が実現できるのではないだろうか.

6.5　C 型規制から C´型規制へ

本節で述べてきたことは,共著者の 1 人である林が 2005 年ごろから思い描いてきた「C 型規制から C´型規制へ」というトレンドの実現でもある.1 節の冒頭でも述べたとおり,

俗に「メディア産業」と呼ばれる諸産業は,参入や撤退などの「Conduit(経済的)規制」と,送信内容に関わる「Content(社会的)規制」の二つの要素で区分され,「P = Publishing 型」「B = Broadcasting 型」「C = Common Carrier 型」に 3 分される(林 [2005a]).

しかし,インターネットの登場に伴って,従来の「P 型」「B 型」「C 型」のいずれにも属さないタイプのビジネスが登場してきた.これをどのような形で規制すべきか,あるいは「非規制政策」を維持すべきかが論点であった.その際,林が作図したのは,図表 12. のような位置づけであった.

図表 12. メディア産業と規制のあり方

Content（社会的）規制 / Conduit（経済的）規制	あり	なし
あり	B = Broadcasting 型	C = Common Carrier 型
なし	I= Internet 型？	P = Publishing 型

ここで I = Internet 型?と question mark を付けていたのは,この類型があり得ることは理解しつつも,それが望ましいことか,必然的なことかについて,当時は自信がなかったからであった.特にインターネットの「非規制政策」を考察してきた経験から,「すべてを市場原理に任せる」ことが魅惑的に思えたため,何らかの規制が入ることに躊躇があったことは否定できない(林 [2002]).

しかし,プロバイダ責任制限法の制定と,その実態をみることにより,また上述の「コミットメント責任」のように,市場原理を生かしつつ最低限の規制を加える方法があることを知った今となっては,I 型という規制方式があり得ることを明確にするのがベターと考えるようになった.本節の 4 つの提案を,そのような文脈で理解していただけると幸いである.

7 残された論点

予定の紙幅を大幅に超えてしまったので,最後に 1 点だけ気にかかっている点に触れておきたい.それは,わが国における Watch Dog の機能不全である.権力は腐敗しやすいものなので,これを常時監視している者が必要である.本来なら,マスメディアがその任に当たるべきところだが,日本のマスメディアの信頼が地に落ちていることは,(当事者以外は)誰でも知っている(もっとも痛烈,かつ同業者として核心を突いた見方として,ファクラー [2012] 参照).

そこで,これに代わる民間の機関に期待が集まるが,その点でもわが国の現状は寂しい限りである.アメリカでは,ACLU(American Civil Liberties Union)のように信頼できる人権団体や,EFF(Electronic Frontier Foundation)のようにインターネットに特化したアクティビストの団体があって,常時不正の摘発体制を取っている(彼らのサイトに行けば,おびただしい件数の裁判を抱えていること,それだけ活発に権利擁護に動いていることを示している).残念ながらわが国には,これに匹敵する組織がない[96].

私たちの提案のように「程よい通信の秘密」を認めることは,一定の範囲で従来の厳格な解釈を緩めることに他ならないが,それが「歯止めなし」になることは,共著者の本来の目的ではない.健全なカウンターパワーの出現と発展に,期待するところ大である.

[96] ACLU に対応するわが国の組織として JCLU があり,それなりの実績があるが,インターネットの関する限り彼我の差は大きい(自由人権協会(編) [2007]).

参考文献

[1] 朝日新聞 [2010]「『ネット全履歴もとに広告』総務省容認 課題は流出対策」2010 年 5 月 30 日朝刊
[2] 生貝直人[2011]『情報社会と共同規制』 勁草書房
[3] 井上正仁 [1997]『捜査手段としての通信・会話の傍受』有斐閣
[4] 大元隆志 [2010]「DPI は悪なのか? 『ネット全履歴をもとに広告 総務省容認 課題は流通対策』について思うこと」
[5] http://blogs.itmedia.co.jp/assioma/2010/06/dpi.html
[6] 奥村喜和男 [1938]『郵便法論』克明堂書店
[7] 梶井厚志[2002]『戦略的思考の技術―ゲーム理論を実践する』中公新書
[8] 金光昭・吉田修三 [1953]『公衆電気通信法解説』日信出版
[9] クリエイティブ・コモンズ・ジャパン(編)[2005]『クリエイティブ・コモンズ』NTT 出版
[10] 小向太郎 [2011]『情報法入門(第 2 版)』NTT 出版
[11] 自由人権協会 [2007]『市民的自由の広がり:JCLU 人権と 60 年』新評論
[12] 週刊ダイヤモンド編集部 [2012]「新サービスが開けた通信の秘密というパンドラの箱」『DIAMOND online』2012 年 7 月 12 日号(第 685 回)
[13] http://diamond.jp/articles/print/21403
[14] 総務省 [2007]「迷惑メールへの対応の在り方に関する研究会 中間とりまとめ」
[15] http://www.nic.ad.jp/ja/materials/iw/2007/proceedings/C4/iw2007-C4-02-03-03.pdf
[16] 総務省 [2010]「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」http://www.soumu.go.jp/menu_news/s-news/02kiban08_02000041.html
[17] 総務省 [2011]「特定電子メールの送信等に関するガイドライン」
[18] http://www.soumu.go.jp/main_content/000127185.pdf
[19] 高橋郁夫 [2008]「『通信の秘密』の比較法的研究・序説」(総務省「次世代の情報セキュリティ政策に関する委員会」の第 8 回配布資料)
[20] http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/next_generation/080523_2.html
[21] 高橋郁夫・吉田一雄 [2006]「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』第 5 巻,情報ネットワーク法学会
[22] 高橋郁夫・林紘一郎・舟橋信・吉田一雄 [2009]「通信の秘密の数奇な運命(事業法)」『情報ネットワーク・ローレビュー』第8巻,情報ネットワーク法学会
[23] 欠番
[24] 田川義博 [2004]「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.22 No.2
[25] 多賀谷一照・岡崎俊一 [2005]『改正電気通信事業法逐条解説』電気通信協会
[26] 土屋大洋 [2009]「デジタル通信傍受とプライバシー:米国おける FISA(外国インテリジェンス監視法)を事例に」『情報通信学会誌』27 巻 2 号

[27] 電気通信事業者協会・テレコムサービス協会・日本インターネットプロバイダー協会・日本ケーブルテレビ連盟 [2005]「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」 http://www.telesa.or.jp/consortium/suicide/pdf/guideline_suicide_051005.pdf
[28] 電気通信法制研究会(編著) [1987]『逐条解説 電気通信事業法』第一法規出版
[29] 日本インターネットプロバイダー協会・電気通信事業者協会・テレコムサービス協会・日本ケーブルテレビ連盟・テレコムアイザック推進会議 [2007]「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」
[30] http://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf
[31] 日本インターネットプロバイダー協会・電気通信事業者協会・テレコムサービス協会・日本ケーブルテレビ連盟『帯域制御のガイドライン』(2008 年)
[32] 日本インターネットプロバイダー協会・電気通信事業者協会・テレコムサービス協会・日本ケーブルテレビ連盟『帯域制御のガイドライン』(2008 年)
[33] 長谷部恭男 [2008]『憲法(第 4 版)』新世社
[34] 林紘一郎 [1984]『インフォミュにケーションの時代』中公新書
[35] 林紘一郎 [1989]『ネットワーキングの経済学』NTT 出版
[36] 林紘一郎 [1999a]「ディジタル創作権の構想・序説ーーー著作権をアンバンドルし,限りなく債権化する」『メディア・コミュニケーション』No.49
[37] 林紘一郎 [1999b]「ⓓマークの提唱ーーー著作権に代る『ディジタル創作権』の構想」『Glocom Review』 Vol.4.No.4
[38] 林紘一郎 [2002]「インターネットの非規制政策」林紘一郎・池田信夫(編著)『ブロードバンド時代の制度設計』東洋経済新報社,所収
[39] 林紘一郎 [2005a]『情報メディア法』東大出版会
[40] 林紘一郎 [2005b]「「秘密」の法的保護と管理義務:情報セキュリティ法を考える第一歩として」『富士通総研研究レポート』富士通総研経済研究所 No.243
[41] 林紘一郎 [2010]「グーグル・ヤフー提携を考えるⓉ『技術』と法の調和 問われる」『日本経済新聞』「経済教室」欄,2010 年 11 月 17 日
[42] 林紘一郎 [2011a]「第 7 章法学的アプローチ」日本セキュリティマネジメント学会監修・松浦幹太編著『セキュリティマネジメント学』共立出版
[43] 林紘一郎 [2011b]「情報法の客体論:「情報法の基礎理論」への第一歩」『情報通信学会誌』 Vol. 29, No. 3
[44] 林紘一郎 [2012]「privacy と property の微妙なバランス:Post 論文を切り口にして Warren & Brandeis 論文を読み直す」『情報通信学会誌』(査読中)
[45] 林紘一郎・鈴木正朝 [2008]「情報漏洩リスクと責任―個人情報を例としてー」『法社会学』69 号
[46] 林紘一郎・田川義博 [1995]『ユニバーサル・サービス』中公新書
[47] 林紘一郎・田川義博・浅井達雄 [2011]『セキュリティ経営:ポスト 3. 11 の復元力(レジリエンス)』勁草書房
[48] 林紘一郎・湯川抗・田川義博 [2006]『進化するネットワーキング:情報経済の理論と展開』NTT 出版
[49] ファクラー,マーティン [2012]『本当のことを伝えない日本の新聞』双葉新書

[50] ぷららネットワーク [2006] 報道発表「ぷららバックボーンにおけるWinnyの通信規制について」
[51] http://www.plala.or.jp/access/living/releases/nr06_mar/0060316_2.html
[52] プロバイダ責任制限法ガイドライン等検討協議会 [2004]『プロバイダ責任制限法:名誉毀損・プライバシー関係ガイドライン』
[53] http://www.telesa.or.jp/consortium/provider/pdf/provider_mguideline_20110921_1.pdf
[54] プロバイダ責任制限法ガイドライン等検討協議会 [2007]『プロバイダ責任制限法:発信者情報開示関係ガイドライン』
[55] http://www.telesa.or.jp/consortium/provider/pdf/provider_hguideline_20110921_1.pdf
[56] 堀部政男(編著)[1998]『発信者番号表示とプライバシー』NTT 出版
[57] 牧田潤一朗 [2010]「アメリカのプライバシー保護法制の日本への示唆」『Law & Practice』No.4
[58] 松井茂紀 [2010]「インターネット上の表現行為と表現の自由」高橋和之・松井茂紀・鈴木秀美(編)『インターネットと法(第 4 版)』有斐閣
[59] 村上康二郎 [2009]『個人情報保護の基礎理論に関する研究:情報プライバシー権の日米比較』情報セキュリティ大学院大学博士請求論文
[60] 矢野直明 [2007]『サイバーリテラシー概論:IT 社会を同生きるか』知泉書館
[61] 郵政省郵政研究所 [1997]『1996 年米国電気通信法の解説』商事法務研究会
[62] Post, Robert C. [2001] 'Three Concepts of Privacy,' "Georgetown Law Journal," Vol.89, No.2087
[63] Swire, Peter P. and Robert E. Litan [1998] "None of Your Business" Brookings Institution