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 6 月

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

本報告書は、2012 年 11 月から 2013 年 5 月にかけて開催された、「インターネットと通信の秘密」研究会が到達した結論部分を、取りまとめたものである。取りまとめは、情報セキュリティ大学院大学が、キヤノン・グローバル戦略研究所の協力を得て行ない、研究会には以下の各社（社名のアイウエオ順）が参加した。NEC ビッグローブ（株）、NTT コミュニケーションズ（株）、（株）KDDI 総研、ソネットエンタテインメント（株）、ヤフー（株）。

本件のお問い合わせ先：情報セキュリティ大学院大学、林紘一郎研究室。
〒221-0835　横浜市神奈川区鶴屋町 2-14-1
電話＆Fax: 045-410-0222、E メール：hayashi@iisec.ac.jp

Executive Summary

1. 本報告書は、情報セキュリティ大学院大学が主宰し、電気通信事業者やインターネット・サービス・プロバイダの有力企業に参加いただいた、「インターネットと通信の秘密研究会」（2012 年 10 月～2013 年 5 月）の成果を取りまとめたものである。
2. 参加者に共通するのは、個人の権利としての「通信の秘密」の重要性は十分に理解した上で、郵便や電話の時代に発展した論理が、インターネットの時代には見直しが迫られているという問題意識である。
3. 検討の結果、参加者は上記の問題意識を再確認し、次の 2 つの視点を中心に、何らかの見直しが必要であるとの結論に至った。① インターネット時代に「通信の秘密」の変質がみられる。（第 1 章）、② 電話時代からの伝統的な「通信の秘密」の論理は、インターネット時代では「通信の秘密」に関して、「過剰」と「空白」を生み出している。（第 2 章）。
4. その上で、見直しのための視座として以下の 3 点を中心に検討した（第 3 章）。A） 憲法論的視点、B） 事業法的視点、C） 非対称の解消。なお非対称の例として、これを細分し「通信サービスと通信サービス以外」の間のもの、「電気通信事業者と事業者以外の者」の間のもの、「日米の規制環境の差」を取上げた。
5. その結果、次の 7 つの提案をするに至った（第 4 章）。1）「通信の秘密」の理念の整理、2）3 層構造（狭義の通信の秘密、他人の秘密、プライバシー関連情報）に基づく見直し、3)「通信の秘密」に関する事業者の責務、4）クラウド・ビジネスの規律、5）コミットメント責任、6）サイバー攻撃や行動ターゲティング広告等への対応、7）「正当行為」や「通信当事者の合意」の意味についての再考。
6. しかし、インターネットという新しい強力なツールは、「通信の秘密」という部分だけに影響を及ぼすわけではなく、今やメディアの秩序全体に影響を与えつつある。第 5 章では、以下の 3 点について付言しているが、これらを見直す過程で、「通信の秘密」についても、再再考が必要になるかもしれない。a） 通信と情報処理と放送の融合、b） メディア規制に関する PBC モデル、c） インターネットの登場と I 型モデルの有効性。

目次

第１章　インターネット時代の到来と「通信の秘密」の変質

電話時代からの伝統的な「通信の秘密」に関する法規定としては、まず憲法 21 条 2 項後段（「通信の秘密は、これを侵してはならない。」）の規定があり、法律レベルでは、電気通信事業法、有線電気通信法、電波法がある。また、郵便関係では郵便法において信書の秘密が規定されており、刑法 133 条に信書開封罪が規定されている。

1990 年代前半の商用化（林 [2005]）以来インターネットの発展は著しく、今や電話や e メールはもとよりファイルの交換、動画の送信、情報の検索･共有、ソーシャル・ネットワーキングにいたるまで、電気通信の主役はインターネットになったと言ってよい。

インターネット時代になってからは、「通信の秘密」に関係の深い法律として「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」（以下、「プロバイダ責任制限法」と呼ぶ）や「特定電子メールの送信の適正化等に関する法律」（以下、「迷惑メール法」と呼ぶ）等が新たに制定された。

このようにインターネット時代の「通信の秘密」は、電話の時代の通信の秘密とはかなり変質している。第 1 章では、どのように変質しているかをみよう。

1.1 電話とインターネットの比較

電話とインターネットの属性のうち、通信の秘密と関係が深いと思われる 6 点を比較すると、図表１．のようになる。なお、ここに登場する次の 6 つの用語は、本報告書では一貫して以下の定義に従うものとする。

- 通信の秘密：電気通信事業法 4 条 1 項で規定された「通信の秘密」（「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。」）
- 他人の秘密：同法 4 条 2 項で規定された「他人の秘密」（「電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。」）
- 電気通信役務：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。（同法同条 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（同法 2 条 4 号）
- パーソナルデータ：個人に関する情報（総務省「パーソナルデータの利用・流通に関する研究会」論点整理（2013 年 4 月 8 日）に同じ。）
- 正当行為：法令または正当な業務による行為（刑法 35 条）、正当防衛（同 36 条）、緊急避難（同 37 条）、さらには通信当事者の合意に基づく行為の総称。

また、プライバシーやデータ・プライバシーは通信の秘密との関連性があるが、この問題はそれ自体が大きな問題なので、本報告書では通信の秘密に焦点を当てて検討する。

図表１．電話とインターネットの属性の比較

属性	電話	インターネット
① 事業の特徴	利用者の音声（情報）を conduit 事業者である通信事業者が運んでいる。通信事業者のサービス（役務）提供が事業の中心	アプリで多様なサービスが可能、多様な事業者による多層レイヤ化が進展。通信事業者と通信事業者以外の事業者が混在してサービスを提供している。
②公然性のある通信の可能性	なし	通信内容の秘匿性を有しない通信が大量に流通・蓄積されている。
③通信の秘密と他人の秘密の関係	共通線信号方式以前は、区分が難しかった	ヘッダとペイロードで区分可能
④発着信端末の特定	電話番号で特定は容易	発信端末は成りすまし（踏み台）やオニオン・ルータなどで特定が難しい
⑤記録性	ログは一定期間保存可能だが、通信内容はキャリアには記録されない	同左。なお、大量の通信内容（情報）がネット上（サーバ内）に蓄積されていて、この蓄積情報にアクセスするマン・マシーン型の通信が多くなされている。
⑥プライバシー侵害の可能性	故意犯でなければ侵害の可能性は低い	匿名による情報発信であっても、linkable なパーソナルデータとの突合で侵害の恐れがある

1.2 インターネット利用に関して通信の秘密が問題となった事例

通信の秘密の侵害行為に関しては、電気通信事業法 179 条 1 項で「電気通信事業者の取扱中に係る通信（第 164 条第 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」ことが、同条 2 項で「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。」と規定されている。また、有線電気通信法や電波法にも、通信の秘密侵害に対して刑罰規定があるが、いずれも電気通信事業に従事する者が通信の秘密の侵害行為をした場合には、刑罰が加重されている。

通信の秘密を侵すという行為類型（「構成要件」という）に該当する行為をする場合には違法性ありと推定されるが、通信当事者の同意を得てその侵害行為をした場合のほか、狭

義の正当行為（刑法 35 条)、正当防衛（同 36 条)、緊急避難（同 37 条）の 3 パターンに該当する行為と認められる場合には違法性が阻却され、刑罰は科されない。（さらに、刑罰を科すには有責性があることも要する。）

インターネット利用に関して、以下に述べるような事象が発生しており、これに対処するために、外形的（構成要件的）には通信の秘密の侵害行為であっても、通信当事者の同意または違法性阻却事由があるために、その行為が違法ではないと認められる事例が多くみられる（事例の詳細は、林・田川 [2012] を参照)。

＜事例 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に係る問題である。

インターネットでは、同法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、通信内容に秘匿性がない通信の増加が顕著である。こ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、不特定の人々に受信されることになって、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場合がある。

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[1]。

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。

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た[2]。

＜事例2：迷惑メール対策＞

---

[1] 発信者情報開示は、当事者間の紛争の解決の前提になるものであるが、「住所・氏名」によって相手を特定しなければ訴訟を提起できないので、裁判上も不可欠なものである（民事訴訟法 133 条）。

[2] またこの法律に関しては、「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 [2007]）、「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 [2011]）などいくつかのガイドラインがある。

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「迷惑メール法」が制定・施行され、法的な対応がなされた。また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。

迷惑メールは、同法では特定電子メール（2 条）として、「電子メールを通信する者が、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、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、OP25B（Outbound Port 25 Blocking）や IP25B（Inbound Port 25 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、正当行為であるとされている。

同法11条では、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」ことを明文で規定し、迷惑メールの送信をブロックすることが正当行為であることを明確にしている。

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。

＜事例 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、違法情報（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等）も含まれている。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、2005年には 6月末までの半年間で 25件 70人 に達したため、社会的にも大きな問題となった。このため、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による、110 番通報が契機となることが多い。通報を受けた警察は、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。

そこで警察は、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が、発信者情報は「通信の秘密」に該当するとされ、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。そこで、このガイドラインは、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。

なおプロバイダ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]）。

＜事例 4：大量通信等への対処策＞

ブロードバンドの普及で動画などの大容量通信が可能になり、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るようになった。対策を講ずるためには、通信内容を識別した上での何らかのネットワーク制御が要請され、通信の秘密の問題をクリアする必要がある。2007年5月に電気通信事業者 4 団体等は、「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、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。大量通信等に係る通信を他の通信と識別し、大量通信等に係る通信を遮断するためには、通信の構成要素であるヘッダ情報等の検知が必要で、（外形的）構成要件的に通信の秘密の侵害行為になるとされる。

したがって、その対応措置が正当行為であると言えるのかどうかが問題となるが、大量通信等がプロバイダの設備に対する攻撃である場合には、プロバイダ自身が通信当事者となるので、通信の秘密の侵害とはなり得ない。プロバイダの通信設備以外に対する攻撃でも、設備を防衛することや緊急対応策が、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、①自己又は他人の生命、身体、自由又は財産に対する現在の危難があること（現在の危難の存在）、②危難を避けるためにやむを得ずにした行為であること（補充性）、③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かったこと（法益の権衡）が必要である。

＜事例 5：帯域制御問題＞

事例 4 に含まれている問題ではあるが、インターネット・トラヒックの恒常的な増加に対応して利用者間の利用の公正性を図る観点から、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（その後2011年に改定）（日本インターネットプロバイダー協会ほか [2011]）。

ここでは、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するとされる。そこで、他の事例と同様に、この行為の正当性の検討が必要になり、プロバイダ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[3]に疑義が提起されているように、これだけで回避できるとするのは問題であろう。

また、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正当行為性を検討している。

＜事例6：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。この問題に関しては、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、プロバイダ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。

---

[3] 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。

上記の説明からも分かるように、DPI 技術は（外形的）構成要件的には、「通信の秘密」を侵害するとされる。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とされ、同研究会で検討が行われた。

同提言では、違法性阻却事由が認められる事例をあげたうえで、「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はこれに該当せず、「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、DPI 技術を行動ターゲティング広告に利用する場合には、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、円滑なサービス対策を行なうための「配慮原則」を提言している。

1.3 「通信の秘密」の変質を促す新しい動き

インターネットは汎用のネットワークであるため、上記以外の新サービスが次々と登場している。ここでは、総務省の「パーソナルデータの利用・流通に関する研究会」の論点整理で取り上げられている、代表的事例を紹介する。

事業者による新しいサービスとしては、まずセキュリティ目的での利用が考えられる。例えば送信元のサーバー所在地やドメイン名等、さらにメール添付のファイル等の分析を行うことができれば、成りすましや不正な目的でのメール利用の検知が可能となる。

またマーケティングのための通信ログの使用が考えられる。例えば電気通信事業者が、通信ログを統計的に分析してマーケティング情報として活用することは、「通信の秘密」の侵害に当たるとの懸念がある。一方、非電気通信事業者におけるサイトアクセスログは、「通信の秘密」には当たらないので、広く活用されている。

伝統的な電気通信事業者以外の、新しい事業者による新しいサービスとしては、消費者生成メディア（CGM）におけるミニメール内容確認が考えられる。例えば SNS など消費者生成メディアにおけるメッセージ機能（いわゆるミニメール）悪用に起因する犯罪を防止するため、ミニメールを監視し削除する事業者が登場している。

また金融事業者によるインターネットバンキング上でのクーポン提供が考えられる。例えばクーポンを配布したい小売業者等が、Cardlytics にクーポンの配布条件を依頼する。Cardlytics は、銀行に対して該当する顧客の抽出を依頼すると、銀行は取引データを分析して該当顧客を抽出し、対象顧客にインターネットバンキング上でクーポンを提供する。

1.4 「通信の秘密」の変質の特徴的事項

1.1 で述べたように、多様なアプリによるサービスが拡大したことに伴い、「通信の秘密」の適用を受ける事業者の範囲が分かりにくくなってきた。また、伝統的な通信概念とは異なり、通信内容の秘匿性を有しない「公然性のある通信」が増加しており、「通信の秘密」に影響を与えている（詳しくは後述する）。

さらに 1.2 の事例でみたように、インターネットで生じているネガティブな個別課題に対処するために、外形的（構成要件的）には「通信の秘密」を侵害した場合であっても、正当業務行為や緊急避難に該当するため違法性がないとされる事例が、多く見られるようになっている。この個別的対処の検討を通して、プロバイダ責任制限法や迷惑メール防止法が制定され、また事業者が自主的なガイドラインを作成するなど、一応の成果を上げている。

また、前出の 2010 年 5 月の「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」においては、「電気通信事業者による通信の秘密の侵害行為が正当業務行為となる場合については、実務上の運用事例を通じて一定の考え方が整理されてきている」として、事例をあげたうえで、「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」と述べられている。

しかしながら、法律や各ガイドラインを詳細に検討すると、この原則に沿った場合以外にも、外形的（構成要件的）な通信の秘密侵害行為も、正当行為としている場合がみられる。例えば、プロバイダ責任制限法や「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ン」においては、利用者の生命、身体、名誉などの個人的法益を守るために、通信事業者の外形的な（構成要件的な）通信の秘密侵害行為も、正当行為であるしている。

以上のことから、外形的（構成要件的）に「通信の秘密」の侵害行為が正当行為と認められるのは、通信事業の公共的性格から社会的法益を守るために認められる場合と、利用者である個人の権利を守るという個人的法益の両方の場合があると考えられる。

もとより、「通信の秘密も絶対的に保障されるものではなく、不可欠な公共の利益を実現するために適切に設定された必要最小限の制約は許される」（長谷部 [2012] p.68）。そこで、インターネット上の様々な事象について、「通信の秘密」の保護と他の法益とのバランスを図り、事業者の予見可能性を高めるためには、どのような場合が違法行為で、どのような場合が正当行為になるかに関する、明確な判断基準を設定する必要がある。

表現の自由の分野においては、たとえば、米国では違法な行為の扇動に関するブランデンブルグ基準や public officials を批判する言論が名誉毀損と認められるためには、原告側で表現者の現実の悪意（actual malice）の立証が要件とされる、などの判断基準が判例上確立している[4]。もし「通信の秘密」に関する正当行為の判断基準が明確になれば、法的な

[4] ブランデンブルグ基準とは、「暴力または犯罪を唱道する言論の規制が許されるのは、その唱道が切迫した（imminent）不法な行為を扇動しまたは生み出すことを意図したものであり、かつそのような不

予測可能性が向上するので、事業者がビジネス的なリスクを取りつつ、インターネット利用に係るネガティブインパクトに適正に対処することができるようになると期待できる。

今後、インターネット上ではサイバー攻撃など情報セキュリティ問題が深刻化することが予想され、この問題に適切に対処することがナショナルセキュリティの観点からも一層重要性を増す。またインターネットを活用することが、産業的にも、社会的にも、個人生活でもプラスの価値を生み出すと期待されている。このように、プラスを生み出す、マイナスを防ぐ両面で、インターネット利用にふさわしい「通信の秘密」に向けて、他の法益とのバランスを図るための明確な判断基準を設けることが重要な課題である。

第 2 章　伝統的な「通信の秘密」の法解釈の「過剰」と「空白」

第 1 章で述べたように、インターネット時代においては「通信の秘密」は変質しているが、その解釈は電話時代から継承したものである。そこでまず、「通信の秘密」に関する現在の法解釈を探ることにより、それが一面において「過剰」であり、他面において「空白」であることを明らかにしたい。

検討すべき課題は、第一に憲法 21 条 2 項における「通信の秘密」の範囲および憲法の直接適用問題、第二に電気通信事業法 4 条 1 項の「通信の秘密」と同条 2 項の「他人の秘密」の峻別問題、第三に同 4 条の「通信事業者の取扱中に係る通信」の範囲の問題である。

2.1 通信手段の変遷と「通信の秘密」

上記 3 点のうち、検討の中心は「通信の秘密」と「他人の秘密」の峻別問題であるが、そもそも峻別することが可能なのかという問題がある。

この点について、主たる通信手段の変遷との関係で表示したのが、図表 2 である。この表から、郵便の時代に「封書の中身と宛名書き等」として区分可能だった「通信の秘密」と「他人の秘密」が、電報と電話の時代にはシステム的にも区分困難となり、インターネットに至って、再び区分可能になっていることが分かる。

しかし、こうした変化を指摘する文献や学説は皆無と言ってよいほどで、次節以下で紹介するように、わが国の判例・行政解釈・学説はほぼ一部の例外的な解釈を除き、「通信の秘密」と「他人の秘密」は一体不可分のものと理解しているかにみえる。

法な行為を扇動または生み出しそうな場合」をいう。現実の悪意とは、「public official に対する批判は、それが偽りであると知りながら、または偽りであるか否かを無謀に無視して述べたことを、批判された側が立証しなければ、名誉毀損的な虚偽について損害賠償を求めることができない」とする法理（林 [2005] p.87 注 10）および p.101）。

図表２．主たる通信手段の変遷と「通信の秘密」と「他人の秘密」の区分可能性

主たる通信手段	郵便	電報	電話（手動交換）	電話（自動交換）	インターネット（パケット交換）
「通信の秘密」の例	手紙･封書において伝えたい内容	電文そのもの	通話内容	同左	同左
「他人の秘密」の例	発信人・宛先・筆跡など	発信人・宛先など	発信者と受信者の番号、通信当事者の性別、発音の訛りなど	同左	発信と受信のアドレス、使用するプロトコルなど
両者の区分可能性	封書の場合、両者は区分可能	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れる。ただし共通線信号方式の導入以後は区分可能	ヘッダ情報だけを読み取ることは可能

2.2　憲法 21 条 2 項と民間事業者への直接適用問題

憲法 21 条 2 項後段「通信の秘密は、これを侵してはならない。」の規定における「通信の秘密」の対象範囲に関しては、一般に「電気通信事業者の取扱中に係る通信の秘密」（電気通信事業法 4 条）と同義に解されている。また、「侵す」とは、知得、漏洩、窃用であると解されている。（詳しくは後述する。）

憲法の名宛人は、基本的には国家であるが、私人の行為への適用に関しては直接適用と間接適用の二つの解釈がある。通信事業が電電公社（と旧 KDD、以下同じ）によって行われていた時代には、どちらの説をとってもあまり差はなかったが、1985 年に電電公社が民営化され、また競争導入によって多数の通信事業者が存在するようになった現在は、民間企業である通信事業者に憲法が直接適用されるか否かが問題になる。

前出の長谷部は、「通信の秘密に関する限り、憲法が私人間にも直接適用されるという考え方と、電気通信事業法をはじめとする規制法、および私法上の一般条項を通じて憲法が間接適用されるにとどまるという考え方とがありうる。」と、両説を並行的に述べている（長谷部 [2012] p.68）。

また、「情報通信の不適正利用と苦情対応の在り方に関する研究会」（総務省 [1999]）では、憲法の基本的人権の規定は、公権力との関係で国民の権利・自由を保護するものであるとしている。また、電気通信が自由化された現在では、憲法の「通信の秘密」は私人である電気通信事業者等へは直接適用はなく、電気通信事業法で保護されていると考える、と述べられている。

2.3 電気通信事業法 4 条の「通信の秘密」と「他人の秘密」

憲法 21 条 2 項では、「通信の秘密は、これを侵してはならない。」と規定されており、事業法における「通信の秘密」と「他人の秘密」の区分はない。これは、そもそも「他人の秘密」という概念を意識していないものと思われ、有線電気通信法や電波法における通信の秘密の規定においても同様である。

なぜ事業法レベルで、「通信の秘密」と「他人の秘密」の二つの区分が設けられたかの経過については明らかではないが、後述する公衆電気通信法に先行して 1947 年に制定された郵便法 9 条でも、「信書の秘密」を保護する 1 項と郵便の業務に従事する者が郵便物に関して知り得た「他人の秘密」を漏えいすることを禁止する 2 項が、別々に規定されている。

「信書の秘密」の内容としては、信書の内容のみならず、差出人・受取人の氏名、住所又は居所等、信書に関する一切の事項を含むとされおり、「他人の秘密」の内容としては、信書の内容のみならず、差出人・受取人の氏名、住所又は居所、取扱年月日、差出個数その他通信そのものの構成要素を成す一切の事項とされており、これを保護する理由としては、これらの事項を知ることにより通信の意味内容が推知され得るためであるとしている（総務省研究会 [2007]）。

しかし、従来からの法解釈では、この二つの文言を区分しない法解釈がほとんどである。ちなみに、上記の総務省研究会[2007]の第 2 回資料 2 では、信書の秘密等と対比させて「通信の秘密」について以下のような記述がみられる。

- 通信の秘密：通信の内容のみならず、通信当事者の住所、氏名、受発信地、通信年月日等通信の構成要素や通信回数等の通信の存在の事実の有無を含む。（下線は筆者付記）
- 通信に関して知り得た他人の秘密：通信の秘密のほか、通信当事者の人相、言葉の訛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言えないが、それを推知させるもの。

ここで、「通信の秘密」が通話内容だけでなく、通信の構成要素や通信の存在に関する事項も含むとする解釈を「同一説」、通信の秘密の保護対象は通信内容であり、通信の構成要素や通信の存在に関する事項は「他人の秘密」であるとする解釈を「峻別説」と呼ぼう。行政解釈は過去から現在まで一貫して「同一説」をとっている中で、本報告書は後述するように、峻別説をとるべきことを提言したいが、結論を急ぐ前に、まず「通信の秘密」と「他人の秘密」がどう扱われてきたかに関する、過去の経過を辿ってみよう。

＜電電公社発足時の解釈＞

電電公社時代の通信の秘密については、公衆電気通信法 5 条に現在の電気通信事業法 4 条と同内容の規定があった。その制定に関わった当事者による逐条解説（『公衆電気通信法解説』）では、「通信の秘密」は以下のように説かれており、「同一説」をとっていることが分かる。なお、この 1953 年は電電公社が発足した年である。

「『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云う事実又は場合により単に通信の存在の事実をも意味し又『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）又は窃用すること（本人の意思に反して自己の利益の為に用いること）は勿論、単に積極的に知得することをも含むのである。又『秘密を守る』とは秘密を他に漏らし又は窃用しないことであって、公衆電気通信業務に従事する者にあっては単なる積極的知得が禁止されていないのは業務の遂行上内容等を知得することが必要である場合がある（例えば電報の受付、伝送等）為である。従って罰則の適用に関しては単なる積極的知得は従事者の場合は秘密の侵害にならないし、又一般人の場合にも挙証の関係で処罰の対象にならないことが多いと想像される（法第 112 条参照）。」（金光・吉田 [1953]）。

＜吉展ちゃん事件を受けた電電公社からの質問と内閣法制局の回答＞

1963 年に発生した、幼児誘拐事件である吉展ちゃん事件は、いわゆる「逆探知」が初めて行われたため、「通信の秘密」を語る上で画期的な事件となった。事件後電電公社は、逆探知等の合法性を確認するため、郵政省を経由して内閣法制局に、以下の二つの事項について照会した。

第 1 問：電話を利用して刑法 222 条に規定する脅迫の罪を現に犯している者がある場合に、被害者の要請によって、電電公社の職員が当該電話の発信場所を探索し、これを司法警察職員等の捜査官憲に通報することは、公衆電気通信法第 5 条第 2 項の規定に違反することとなるか。

第 2 問：司法警察職員等の捜査官憲が、電話による通話の一方当事者甲の同意を得て、甲の利用する電話の端末の設備において他方の当事者乙の通話を録音することは、公衆電気通信法第 5 条第 1 項の規定に違反することとなるか。

これに対して内閣法制局は、「お尋ねの問題はいずれも消極に解する」との回答を行った。この電電公社の照会内容と内閣法制局のやりとりを見る限りでは、両者とも 5条1項 と2項、すなわち「通信の秘密」と「他人の秘密」を明確に分けて論じているようにみえる。特に注目すべきは、第1問で（電話の発信場所を探索する）逆探知行為は、他人の秘密を規定している「公衆法 5条2項 に違反するか」という「峻別説」にたった照会をしていることで、この内閣法制局意見を論評した片桐は、内閣法制局意見では、電話の発信場所は「他人の秘密」に該当することについて積極に解しており、峻別説の立場をとっているとみている（片桐 [1986]）。

ところが、回答を得た側の電電公社は、「同一説」にたつ通信の秘密に関する社内通達を出した。その背景については以下の指摘がある。

「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。」（高橋ほか[2009]）。

この推測は、当時の通信手段の中心は電話（自動交換と手動交換）と電報であり、論理的には両者を区分できるものの、2.1 通信手段の変遷と「通信の秘密」で述べたように、「通信の秘密」と「他人の秘密」を区分できる可能性は低く、現実として区分する実益があまりなかった事情を反映しているのではないだろうか。

法構成上は、「通信の秘密」を守ることはすべての人を対象としており、電気通信事業法179 条 1 項において、侵害に対しては刑罰も課されている。一方、「他人の秘密」の規定は、通信事業の従事者を対象とした規定であり、同法 179 条 2 項において、通信事業の従事者は身分犯として刑罰が加重されているものの、それが「他人の秘密」を含むか否かについては、必ずしも明確ではない。

高度成長期への入り口に差し掛かっていた、当時の電話の時代には、通信事業の従事者以外の第三者が「通信事業者の取扱中に係る」通信の秘密を侵害する可能性は、実際上極めて低かった。そのため、通信の秘密の侵害に関する関心は、もっぱら通信事業者に向けられていた。したがって、「通信の秘密」より広範な「他人の秘密」を含む規定を置いて、これを通信事業者の責務とすることによって、通信全体を保護しようとしたのではないかと考えられる。

一方、独占的に通信事業を運営していた電電公社では、通信内容の秘密であれ、他人の秘密であれ、どちらも区別せずに守ることが世間の期待に応えることである、との企業倫理観があって、これが同一説を取る動機になったのではないかと推測される。

＜同一説の立場をとる判例＞

通信の秘密に関する判例は多くないが、「通信の秘密」と「他人の秘密」の関係については、これを一体不可分のものと捉える視点が明確である、代表的な判決は 2 件とも、以下のように述べている。

「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)。

「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）。

＜同一説をとっている行政解釈＞

行政解釈上は、前述したように電話の時代から一貫して「同一説」をとっており、「通信の秘密」が問題となった事例に関する、各種のガイドラインでも同様である。たとえば、電気通信事業者 4 団体が策定した「帯域制御の運用基準に関するガイドライン（2011 年改定版）」では、以下のように述べている。なお、「通信の秘密」の対象は個別の通信であると述べているのは、後出の東京地裁判決と同趣旨である。

「（電気通信事業法 4 条 1 項の）『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または他人の利益のために利用することも含まれる。（下線は筆者付加）」

同じく電気通信事業者 4 団体が策定した「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（第 2 版）」では、上記ガイドラインと同趣旨の記述の他、以下の記述がある。

「2. 機械的検索と通信の秘密

機械的に処理される仕組みであっても、電気通信事業者の取扱中に係る通信に関し、その通信の秘密に属する情報（中略）について機械的に検索を行い特定の条件に合致する通信を検知し、当該通信を通信当事者の意思に反して利用する行為は、通信の秘密の侵害（窃用）（事業法 4 条、179 条）に当たる。

ただし、通信当事者の同意があれば窃用に当たらないため、構成要件を満たさない。

また、正当として違法性阻却事由がある場合には（中略）通信の秘密侵害罪は成立しない。」（後略）（下線は筆者付加）

＜「他人の秘密」には刑罰の適用がないとする解釈例＞

電気通信の自由化と電電公社の民営化が行なわれた1985年に制定された電気通信事業法の解釈に関して、電気通信法制研究会［1987］は、以下のように述べており、峻別説と断定するわけにはいかないが、少なくとも刑罰の適用に関しては、「他人の秘密」を守らないことについて適用はないと明確に述べている。

「（電気通信事業法）第4条の第1項と第2項の関係については、第2項は電気通信事業者に従事する者について、職務上正当行為としての知得行為は違法性がないこと、守るべき範囲は、通信の構成要素以外のものであってもそれを推知させるものを含むという第1項に

対する特則を定めたものである。他方罰則の適用関係については電気通信事業に従事する者について本条第1項の『通信の秘密を侵した』場合に加重罰を科することとしている（第2項）。したがって、①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対し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。（以下略）」（pp.267~268）。

＜峻別説をとっていると思われる学説＞

学説でも多くは、同一説をとっていると思われるが、前出の長谷部［2012］は、以下のように述べており、峻別説に立っているようである。

「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。」

2.4 「事業者の取扱中に係る」の意義

前出の吉展ちゃん事件における内閣法制局の回答に関して、前出の片桐［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。」（下線は筆者付加）

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通説化しているかと思われる。前述の＜同一説の立場をとる判例＞で述べた東京地判が、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分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。」

2.5 伝統的な法解釈における過剰

第1章でみたようなインターネット時代の通信の秘密の変質を考えると、本章でみてきたように伝統的な通信の秘密の法解釈には、現在の通信の実情に合わない以下のような過剰な状況がみられる。

＜過剰（1） 憲法的価値の貫徹と過度の自己規制＞

高橋・吉田［2006］によれば、憲法制定の過程でのマッカーサー草案では、secrecy of any means of communication を保護しようとしたのに、最終案文では、文化的違いもあって「通信」の秘密だけが強調され、そのまま成文化されたという経緯があるという。

つまり、制定過程での文言は「いかなる手段のコミュニケーションの秘密」も保護する、という意味であると思われるが、その後の検討過程で、フェース・ツー・フェースの会話を含むコミュニケーションを意味する any means of に該当する文言は、原文からは削除された。その上で、コミュニケーションと通信を同義と理解して、現在の「通信の秘密」の規定になったと思われる（ただし、英文憲法として出版されている邦語文献では、現在でも any means of の語を残している）[5]。

また電気通信の自由化と NTT の民営化がなされた後は、憲法が直接適用されることは明白ではなくなったはずなのに、あまり議論されなかった。事業法においても、「検閲の禁止」と「通信の秘密」だけは、何人にも適用されると解釈されてきた。刑法典には、信書に関しては「信書開封罪」の規定があるのに、「通信の秘密侵害罪」の規定はなく、郵便と電気通信ではバランスを欠いているなど、再検討の視点は多数あるものと思われる。

その際、「通信の秘密」と「他人の秘密」という法文上で明らかに違う概念を同一視した上、「罪刑法的主義」の厳格な解釈を取らず、ともに同じ罪が科されるものとされてきた点は、特筆すべき事柄である。ただし、前出の1987年の『逐条解説 電気通信事業法』では、「他人の通信」に関しては、電気通信事業法179条の罰則の適用はないとしているが、極めて例外的である。

過度の自己規制の背景としては、事業者（特に独占的サービス提供者であった電電公社）は、憲法的価値である個人の権利と事業者の責務を同一視し、社員をそのように指導して

[5] マッカーサー草案外務省仮訳（1946 年 2 月 26 日臨時閣議で配布）も「通信手段ノ秘密ハ之ヲ侵ス可カラズ」となっている。

きたこと、他の通信事業者や新規参入者も電電公社の方針を受け入れたほか、「何事にもお上に頼る」風潮があったためではないか、と思われる。

＜過剰（2） 「通信の秘密」と「他人の秘密」の同一視＞

1953年の公衆電気通信法の制定当初から、この両者を同一視してきた。2.3 に述べたように、1953年の『公衆電気通信法解説』では、以下のように述べられている（金光・吉田[1953] に関する高橋ほか [2009] のコメント）。

1）「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。

2）「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。（同書によれば、「秘密を守る」とは、秘密を他に漏らしまたは窃用しないことであるとされている。）

3）公衆電気通信法５条の「通信の秘密」において「他人の秘密」と峻別しない趣旨が、同法112条にも応用され「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」と明言されている。

＜過剰（3） 「ネットワーク制御」という事業者の本来の業務でも「違法性阻却」を論議するという萎縮効果＞

同一説をとった場合「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になる。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のほか、通信当事者の意思に反して該当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。

したがってプロバイダ等が、例えば Winny 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。

またプロバイダ等が、ユーザーのトラヒック量を検知して、特定のヘビーユーザー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（だだし、帯域制御に関しては個別に解決が図られている）[6]。

＜過剰（4） Deep Packet Inspection （DPI）＞

DPI技術を利用した場合に、情報セキュリティ対策に有効である可能性や行動ターゲティング広告に利用することが考えられるが、パケットのヘッダやペイロードを利用することで、「通信の秘密」を侵害すると考えられて利用が進んでいない。

2.6 伝統的な法解釈における空白

電話と電報の時代に関して、2.1 では「通信の秘密」と「他人の秘密」を区分できる可能性が低く区分する実益に乏しい、また 2.3 では、電気通信事業の従事者以外の第三者が「電気通信事業者の取扱中に係る通信の秘密」を侵害する可能性は極めて低かったので、「通信の秘密」はもっぱら電気通信事業者に向けた規定と考えられていたと述べた。

1985 年の通信事業の自由化と電電公社の民営化に伴って制定された電気通信事業法においても、当時はまだ電話が中心のサービスであったため、憲法論を含めて「通信の秘密」についての見直しがなされないまま、今日に至っている。

ところが、インターネット利用が通信の大宗を占めるようになると、1.2の事例でみたように、conduit 事業者であって本来 content にノータッチが求められるコモン・キャリアが、利用者や通信役務の安定的供給を確保するために、正当行為として「通信の秘密」を外形（構成要件）的に侵害して、content に関与することを求められるようなっている。また、旧第二種電気通信事業者という概念が発展的に解消されたこともあってプロバイダという新しい業態が生まれ、その事業者の多様性が顕著である。

このように、電話・電報の時代に conduit 事業者に課せられていた「contentにノータッチ」という大原則が大きく変質している。この現実に伝統的な「通信の秘密」の法解釈が、インターネットには適合的ではないというのが、「過剰」の問題である。

一方、1.1で述べたように、インターネット・ビジネスでは、電気通信事業者中心の電話事業とは異なり、多彩なアプリ・サービスが多様な事業者によって提供されており、そのビジネス構造の特徴である多層レイヤ化が進展している。そのなかで電気通信事業者と通信事業者以外の事業者が混在して、ビジネス展開がなされている。この新しい事象に、伝統的な「通信の秘密」はうまく対応できておらず、いわば「通信の秘密」に関する空白の領域が生じている。これを「過少」と呼ぶとすれば、以下の事象がみられる。

＜空白（1） 事業者の新サービス＞

電気通信事業者は、前述のように「憲法的価値としての通信の秘密」と、「事業の産業

6 http://www.jaipa.or.jp/other/bandwidth/info_080523.html

倫理としての通信の秘密」を同一視してきたので、その保護の面が強すぎて、インターネット利用が有する潜在的な可能性に必ずしも目が向いていなかった。

「通信内容」（狭義の通信の秘密）はさておき、「他人の秘密」の部分だけを使っても、新しいサービスが可能であるのに、それも禁じられているものとして、強い自己規制を行ってきた。ましてや「通信内容」に触れる場合には、それが絶対的に禁止されるものという思い込みがある。

インターネット時代の「通信の秘密」を検討するには、インターネット利用の安心・安全のための情報セキュリティの機密性確保策と関連付けること、およびインターネットが有する潜在的可能性を現実化するために、イノベーションを引出し、多様なサービスを多く生み出していくとの視点からの検討をさらに強化する必要がある。

＜空白（2） 新事業者の登場と新事業者に対する「通信の秘密」の適用＞

「通信の秘密」と「他人の秘密」を（場合によっては「パーソナルデータ」をも）混同していることから、電気通信事業者以外の者に対する「通信の秘密」の適用について、一律で硬直した対応となりがちである。（狭義の「通信の秘密」は「何人も」守らねばならないはずだが、事業者か否かで区分する傾向がある。例えば、LINEは事業者として登録しているため「通信の秘密」の規定が適用されるが、Skype は未登録なので適用しようがない、といった風に）。

現に、外資系のインターネット事業者については、日米の規制環境の差もあって、行政指導はなされているようだが、日本法の趣旨が徹底できていない。また今後存在を高めるであろうクラウド事業者についても、同様のことが言える。

一方で、青少年インターネット環境整備法にいう「特定サーバー管理者」（同法21条）や、サイバー犯罪条約に対応して改正された刑事訴訟法における「自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者」（同法197条3項）に対する適用は、それなりに合理性はあるものの、「通信の秘密」に介入する当事者が国家権力であるだけに、濫用の危険がないよう慎重な対応が望まれる。

第３章 再検討のための視座

以上みてきたように、第1章で述べたインターネット時代における通信の秘密の変質に適切に対応するには、電話時代から続く「通信の秘密」の法解釈の再検討が必要である。この再検討の視座として、主として憲法論、主として事業法論、および3つの非対称（asymmetry） すなわち「通信サービスと通信サービス以外」の間の非対称、「電気通信事業者と事業者以外の者」の間のもの、「日米の規制環境の差」について、個別に述べる

ことにしたい。

3.1 主として憲法論

電気通信に関する「通信の秘密」は、憲法以前からある「信書の秘密」（その実は信書の検閲）を引き継いでいるため、電気通信に関する「通信の秘密」の憲法論的位置づけの議論が、十分行われてきたとはいえない。加えて現憲法が GHQ の主導で制定されたため、「通信の秘密」（その実は「コミュニケーションの秘密」）が十分に検討されたとは言えない、という経緯もある。

「通信の秘密」の法的根拠（法益）についても、プライバシーが根拠なのか、表現の自由が根拠なのか、この両方の重層性が根拠なのか、詰めた議論はないように思える。法人の通信の役割は重要であるが、例えば仮にプライバシーを根拠として場合には、法人のプライバシーという概念は成立し得るのか、というような問題もある。

また「通信の秘密」の適用範囲に関しても、1.4 で述べたように、「通信の秘密も絶対的に保障されるものではない。不可欠な公共の利益を実現するために適切に設定された必要最小限の制約は許される」ので、「通信の秘密」と「他の法益」の法益バランスをどのように取るべきなのかが重要な課題である。

これまでも 1.2 の事例でみたように、「通信の秘密」に関して解決を迫られる課題について、個別の検討が行われた結果として、法律制定やガイドラインの整備が進められてきており、一応の成果を上げている。

しかしながら、インターネット利用の将来も見据えつつ、全体を捉えた法制度整備が行なわれてきたとはいえない。このため、「通信の秘密」の判断基準について事業者からみると「予見可能性」が低く、これが前述した萎縮効果を生んでいるものと考えられる。今後の全体的な検討を通して、「過剰」と「空白」事象を解消することが望まれる。

また、インテリジェンス活動と犯罪捜査に関する「通信の秘密」の扱いも、秘密法制全体の中で位置づけを明確にすることも課題である。

3.2 主として事業法論

まず、「通信の秘密」と「他人の秘密」を混同しないことが、原点かと思われる。その根拠は、以下の３点である。

１）用語（文言）が違えば、内容が異なるのは一般的なことであり、個人の権利･義務にも関係が深い法律用語については、その点について特に慎重であらねばならないこと。

２）この分野では唯一の公式見解ともいうべき 1963 年の法制局見解が、両者を使い分けていること。

３）前述の金光・吉田［1963］以前においては、両者の関係が論議されたが、決着がついていないこと（高橋ほか［2009］）。

電電公社発足の年である 1953 年の『公衆電気通信法解説』以降の法解釈によって、今日の

いわゆる通説的解釈が出来上がったが、そこには以下の特徴がある。

1）国営で公権力の行使に準ずる事業体への規律が、民営化後も継続されている。

2）「個人の権利」としての「通信の秘密」と、事業者の責務としてのそれが同一視されてきた歴史がある。

1.1 で述べたインターネット事業の特性・可能性を踏まえ、民間企業においてもサイバー攻撃への対策を検討する上で支障になっているとのプロバイダの声や、パーソナルデータを活用した新サービス（行動ターゲティング広告など）展開への要望、国際競争における equal footing 論にも対処が必要である。

このための事業法レベルの課題としては、まず情報セキュリティ分野での機密性（confidentiality）（秘密の刑事法的保護、不正アクセス禁止、個人データ保護など）、完全性（integrity）や可用性（availability）と関連付けて検討すること、併せてインターネット利用でのイノベーション力を引出すことなどがあり、4.6 で述べるような検討がなされることが望まれる。

3.3 通信と通信以外のサービス間の非対称

「通信」と「通信以外の手段」の間に非対称が存在する。例えば、通話を録音したテープを入手し、それを町内会のメンバーに聞かせた者は罪に問われる（最二小決 2004 年 4 月 19 日、刑集 58 巻 4 号 281 頁）。一方で、（通信事業者ではない）セキュリティ会社の社員がオンラインで入手した監視カメラ情報を漏らしても、（他の罪状で罪を問われるにしても）「通信の秘密」の侵害ではない。

3.4 通信事業者と通信事業者以外の者との間の非対称

通信事業者と通信事業者以外の者との間にも、非対称が存在する。広義の「通信の秘密」のうち、「他人の秘密」の秘匿義務は通信事業者のみに課された責務である。ところが 1.1 で述べたように、インターネットでは（電気通信事業者であるかどうかに関わらず）多くの事業者が混在してサービス展開しており、ビジネス・レイヤ上も多層レイヤ化が進展している。したがって、同じようなサービスを提供しても、「通信の秘密」に関しては、異なる扱いになる可能性がある。

すなわち電気通信事業法では、2 条 3 号で電気通信役務を規定し、同 5 号でその役務を他人の需要に応ずるために提供する事業が電気通信事業であるとされ、同 5 号で電気通信事業者は、電気通信事業を営むことについて登録及び届出を要する（9 条及び第 16 条 1 項）こととされている。これは伝統的な conduit 事業者の役割は、他人の通信（メッセージ）の媒介あるいは役務の供用であるとの理解と一致している。

また 164 条 1 項では同法の適用除外になる電気通信事業の範囲が明記されている。この 3 号には「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回線設備を設置することなく提供する電気通信事業」も含まれている。しかしな

がら同条 2 項で、同法 3 条（検閲の禁止）と 4 条（秘密の保護）に関しては、1 項で同法の適用除外になっている電気通信事業で登録・届出を要しない電気通信事業にも適用することが明記されている。

したがって、①「通信の秘密」が適用される登録・届出電気通信事業者、② 事業法の適用除外になっているが「通信の秘密」は適用される電気通信事業者、③ 電気通信役務に該当する役務（サービス）を提供していないため「通信の秘密」の適用がない事業者の 3 種類の事業者が混在していて、この 3 者によって、連携または競合してインターネット・サービスなりビジネスが行われている。

ここで問題は 2 つある。第 1 は上記の ① と ② の事業者に関して、同法 4 条 1 項の「通信の秘密」を守る義務が課されることには異論がないが、「他人の秘密」に関しても刑罰加重を規定した 179 条 2 項が適用されるかどうかである。私たちは「罪刑法定主義」を貫くためにも、狭義の「通信の秘密」に関してのみ加重罰が科され、「他人の秘密」侵害には民事的・服務的責任を負うにとどまる（電気通信法制研究会［1987］と同じ）との解釈に立ちたいが、その旨を何らかの形で明確化する必要があろう。

第 2 の問題は、② と ③ の区分である。164 条の規定は「電気通信事業に従事する者」に該当するかどうかの問題である。インターネット時代には、事業者と利用者の区分さえ曖昧になっており、事業者と非事業者を明確にするにも努力が必要である。そこで勢い「自己宣言」つまりは「事業者として登録あるいは届出をしたかどうか」で、事業者か否かを判断する傾向がある。これは便法としては役に立つが、問題の本質的な解決にはならない[7]。

3.5 日米の規制制度の非対称

日米の間にも、非対称がある。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、修正（補正）4 条は「プライバシーの期待空間」への侵入を禁止するだけで（そのような手段で入手された証拠は証拠能力がない[8]）、「通信の秘密」を一般的に保護するものではない。

これに対して、日本国憲法では「通信の秘密」に関する直接の規定がある。もっとも制定過程では、「通信の秘密」の語はもともと secrecy of any means of communication であって、会話を含めたコミュニケーション全体の秘密を保護するつもりであったところ、訳語が不適切であったため、「通信」だけが突出してしまった。

また秘密の保護を規定する電気通信事業法は、国外適用はなく、米国の事業者が国外で行なう事業については、電気通信事業法の効力が及ばない（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についての国外適用はない）。

このため、「通信の秘密」に関する日米の法制度の違いがあるために、インターネット・

---

[7] LINE は事業者として登録しているが、Skype はそうではないようである。この差が、そのまま「通信の秘密」が適用されるかどうかの差になる、というのは常識的ではないだろう。

[8] Exclusionary Rule （違法収集証拠排除原則）という。

ビジネスが equal footing で行なえない、との声が出てくる理由になっている。

加えて、アメリカでは「州際通信のみが連邦の規制対象で、情報処理は非規制」である。これを所与とするアメリカ系企業は、日本で営業する場合でも、この非対称を有利に利用している。「情報処理の要素があれば、規制から逃れられる」という気持ちが滲み出ているように見受けられる。

わが国でも、一時「回線開放」が声高に叫ばれた時代には、専用線の共同使用・他人使用の範囲を画定する際に、「情報処理が伴うか否か」がメルクマールとされた時代があった。その際には、「なるべく処理があることにしたい」というインセンティブが働いたが、電気通信事業法が制定されたときは逆に、「わが社も（第二種でよいから）事業者になりたい」という気持ちが強く、こぞって（その当時の）登録に走ったように見受けられる。前述のとおり、「自己申告」にも良さはあろうが、それのみに依存して法の適用に差が出るというのでは、客観性を欠くのではないかと思われる。

なお、一時「ネットワークの中立性」が大きな問題になり、「通信事業者はコンテンツにタッチすべきでない」との主張が強かったが、サイバー攻撃の激化等により、そのような主張は背後に退いているかと思われる。むしろ、コンピュータ・サービスがクラウド化して、通信と情報処理の境界が曖昧になるにつれて、asymmetry がより深刻になっているのではないかと思われる。

第4章 改善のための 7 提案

第3章で述べた視座にたって、インターネット時代にふさわしい通信の秘密のあり方を見直すために、以下の 7 つの提案をしたい。

1)「通信の秘密」の理念の整理、2) 三層構造（狭義の通信の秘密、他人の秘密、プライバシー関連情報）に基づく見直し、3)「通信の秘密」に関する事業者の責務、 4) クラウド・ビジネスの規律、5) コミットメント責任、6) サイバー攻撃や行動ターゲティング広告等への対応、7) 正当行為や通信当事者の合意の意味についての再考。

ただし第7点については、今回は第1段階の提案として問題の存在を指摘するにとどめ、代わりに若干の付言を収めている。

4.1 理念の整理

プライバシー論議と同様かそれ以上に、「なぜ通信の秘密が大切か」についての基本理念が整理されていないので、再考すべきである。

憲法論的には、通信の秘密をプライバシー権の１つと捉えるか、言論の自由の保障方法の 1 つと捉えるのか、いずれかに割り切るべきではないのか、議論の整理を図りたい。参考までに、プライバシーの一種と捉えるか、言論の自由の保障と考えるかによって、どの

ような法解釈上の問題が生ずるかを整理すると、次表のようになる。

図表３.「プライバシー」説と「言論の自由」説の比較

比較項目	プライバシー説	言論・表現の自由説
歴史との整合	プライバシーという信書の秘密以後の概念で説明	「信書の秘密が検閲への対抗として生まれた」という史実と一致
権利の性質	公権力からの自由（消極的権利）	公権力からの自由（消極的権利）と「知る権利」など積極的権利への転回可能性
権利の主体	自然人に限られる	法人が含まれる可能性
権利の客体	「公然性のある通信」の扱いに苦慮	「公然性のある通信」は「通信の秘密」としては守られないが、「言論・表現の自由」としては守られる
合意の有効性	合意による対処の範囲が広い	合意があっても認められない場合がある
他の言説との関係	通信に媒介された言説を、他の言説から区別することの不自然性	他の言説とも共通の根拠で説明可能
その他	プライバシーの概念自体が曖昧さを残している	左記の欠点が生じない

「通信の秘密」の法益が何であるかを再考する一つの視点として、憲法的な個人の権利と、通信事業者に求められる「事業者としての責務」を分けて、それぞれに求められることを明らかにしていくような検討が望ましいのではないか。

なお、「通信の秘密」を秘密法制全体の中に位置づけることが望まれる（林・田川 [2012] pp.31～33）が、その際これまで議論が乏しかったインテリジェンス活動についても、正面から捉えて検討する必要がある。「臭い物に蓋をする」態度でいると、却って人権侵害を見落とす恐れがあるからである。

4.2 「他人の秘密」「通信の秘密」「パーソナルデータ」の三層構造

以下の三層構造で、「通信の秘密」およびそれに関連するパーソナルデータ等を再整理すべきである。なお、図表 4 で述べたのは、講学上の「理念型」であって、実務上はグレーゾーンが不可避であると思われる（ヘッダとペイロードの区分にしても、カプセル化によってペイロード内にヘッダ情報も含めて格納されるなど）。ここでは、まず基準点を定めるために、こうしたニュアンスはとりあえず無視していることをご理解いただきたい。

図表４．三層構造

情報の種類	該当する情報の例	保護方式	OSI のレイヤ
パーソナルデータ	プライバシー侵害につながり易い個人データ	原則は契約によるが、消費者保護の観点から「不当条項」など限定的な強行法規を認める	通信以外で入手する情報も含む
通信の秘密	通信の内容（ペイロード）。位置情報も通信の内容として伝送されれば該当	憲法的価値（個人の権利）を保護するために、制定法（できれば刑法）による	レイヤ 4 以上
他人の秘密	（狭義の）通信の秘密を除く、通信の付帯情報。ビーコン的位置情報	事業者の義務として、プライバシー・マークなどの第三者認証とコミットメント責任を組み合わせた制度を導入する	レイヤ 1～3

ここで、以下の理由から、「通信の秘密」と「他人の秘密」の両者を峻別すべきである。

1）法律の文言が違えば、別の概念と考えるべき（「他人の秘密」の概念は、1947 年制定の郵便法以来、一貫している）

2）ましてや、それが刑事罰と結びついているとすれば、「罪刑法定主義」の原則からも、謙抑的に解釈すべき（「他人の秘密」は不可罰だと考えるべき）

3）1963 年の法制局見解も、両者を峻別していると解すべき（片桐 [1986]）

4）事業法制定当時の解釈も、峻別説であったと読み取れるし、少なくとも刑罰の適用に関しては明確に峻別説をとっている。（電気通信法制研究会 [1987]）

ところで、 1.1 で述べたように、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」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。

1.4 で述べたように、外形的（構成要件的）に通信の秘密侵害に当たる行為が、正当行為と認められるケースとしては、通信事業の公共的性格から社会的法益を守るために認められる場合と、利用者である国民の権利いう個人的法益を守る場合という、両方の場合があることは前述した。

もっとも「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 などのように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、一般的には表現の自由が原則であるが、他の法益、例えば名誉毀損やプライバシー侵害があれば、その表現行為が規制されることになる。

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、その発信内容（表現）に関して炎上し、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。（これは 4.7 で述べるグローバル市場経済における各国の事業者間の競争環境を equal footing にすべきとの論点と関連している。）

つまり、「公然性を有する通信」であっても、通信流通過程で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。

4.3 「通信の秘密」に関する事業者の責務

4.2 で述べたように、「狭義の通信の秘密」と「他人の秘密」を峻別し、前者を「個人の権利」と、後者を「事業者の義務」とする法制がふさわしいと考える。（最三小決 1999 年 12 月 16 日、刑集 53 巻 9 号 1327 頁）

（狭義の）「通信の秘密」は、他の秘密（営業秘密や国家機密）と同様、情報主体（当該情報の帰属主体）が秘匿したい情報であるが、（他の二者と違い）その支配・管理が通信事業者に委ねられているので、通信事業者にまで情報主体の権利が及ぶこととすべきである（個人の権利）。

他方、狭義の通信の秘密以外の事項（現行法では「他人の秘密」）は、運輸関係の公益事業におけると同様、コモン・キャリアの職務遂行上不可欠の顧客に関する「業務情報」であり、今後クラウド化がさらに進展することも踏まえて、事業運営上の秘密（事業者の責務）として、契約や約款を補う強行法規として規定すべきである。

さらに、ＳＮＳなどの新しい通信手段の発達や検索技術の進歩と共に、「紐付け可能な（linkable）情報」の保護が問題になっているが、これらはパーソナルデータ保護の一般論として論ずべきである。

4.4 クラウド・ビジネスの規律

クラウドはコンピュータ・サービス業なので、事業法的規制はないが、public convenience and necessity の条件を満たし、20 世紀初頭に問題になった公益事業 （public utility） 的な規制が必要との意見もある。しかし、独占または寡占が生じたとしても、自然独占性が

あるからではなく、競争の結果生ずるに過ぎないので、事業規制は行き過ぎかと思われる。

ただしサービス内容として、１）安全に届ける（safety）、２）勝手に中身を見ない（security）の 2 点は法的な担保があってしかるべきかと思われる。最低でも、約款の不当条項の無効化（現在、債権法の改正で議論されている[9]）は必要であろう。

市場で起きる問題は、市場で解決するのが原則であり、約款や業界団体の基準のような自主的規制に任せることを基本とすべきであるが、nudge する（やさしくつつくことで気づかせる[10]）までは許されると思われるので、第三者評価認証制度とコミットメント責任の組み合わせが有効かと思われる。

なおコミットメント責任のモデルは、米国 FTC 法 5 条であるが、FTC 法においては執行が独立行政委員会に委ねられているのに対して、コミットメント責任は原則として民事責任で、裁判所で解決することを前提にしている。

いずれにしても、クラウド・ビジネスはグローバルに展開されているので、equal footing の意味からも、ガバナンスの仕組みや政策・法制度に関しては、国際的なハーモナイゼーションが必要である。

4.5 コミットメント責任

コミットメント責任という考え方は、林・鈴木［2008］に遡るもので、新たな提案とは言いがたいが、判例の中にもこれに近い発想が見られるなど、最近の展開を踏まえて今後の検討素材としたい。まず、その概念の要点だけを紹介すれば、以下のとおりである（林・田川［2012］pp.45~46）

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．これを踏まえ、以下の定義に該当するものを、「コミットメント責任」と呼ぶことにしている。

.

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。つまりプロバイダ全社に、「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

9 http://www.moj.go.jp/content/000049817.pdf

10 アメリカには、大統領の直属のポストとして the Administrator of the White House Office of Information and Regulatory Affairs という nudge 担当の職位がある。

ーム・ページにポータルを設ける）を義務付けるのである。

これに違背すれば、契約違反（債務不履行）としての責任を問われる。実は、ヤフーBBの個人情報漏洩事件に関する大阪高裁の判決は[11]、一部この考え方と符合する。というのも、原審（大阪地裁）が BB テクノロジーの情報漏洩に対する責任を認める一方で、ヤフーにはその責任はないとしたのに対して、以下の理由でヤフーにも責任を認めたからである[12]。① BB テクノロジーとヤフーとは「外形上一体のものとして」サービスを提供していた、② ヤフーはインターネット上に「情報セキュリティ宣言」を表示し、子会社等の保有する個人情報についてもセキュリティ対策を取ることを宣言していた。

コミットメント責任の考えは、① 債務不履行と考える、② 使用者責任ではなく法人自身の責任と考える、という点で上記の判決とは異なるが、「表示と責任」を結びつけた新しい視点を提供したものとして注目される。このような発想は、藤田 [1994] の先駆的研究以来進展していないが、これを契機に議論が深まることを期待したい。

なお、コミットメントは契約責任の一種と考えているので、大阪高裁判決のような判例の積み重ねで具体化していくことで十分と思われるが、典型契約の一種として民法（債権法）に追加することも考えられる。それでもなお実効性が疑われるようなら、FTC 法と同じように行政機関の行為発動の要件とすることも考えられる。

4.6 サイバー攻撃や行動ターゲティング広告等への対応

この問題に関しては、「通信の秘密」の法益と、プロバイダなどの通信事業者の役割・責務の視点から考えてみたい。

まず、「通信の秘密」の法益はいままで見たように、表現の自由の一環としての通信の自由を守るためであると同時に、その核心部分はプライバシーであるとの指摘もあるように個人の権利を守る（個人的法益）という側面がある。この場合には当事者の同意があれば、外形（構成要件）的に通信の秘密を侵害しても、正当行為と認められる。1.2 の事例 1 のプロバイダ責任制限法や事例 3 のインターネット上の「自殺予告」がこのカテゴリーに属する。

ただ現状では、どのような当事者の同意が法的に有効な同意であるかに関しての判断は、それぞれの問題に関して個別になされており、今後は、問題状況全体の中で、かつ具体的な事象を見通した検討が必要であると考えられる。

一方、「通信の秘密」には社会的法益もあり、ネットワーク社会といわれる現在では、通信役務の安定的提供が、通信事業者の重要な責務であり社会的役割である。この社会的法益の側面では、正当行為として認められるには同意は必要とされない。そこで、外形（構成要件）的に通信の秘密侵害行為であったとしても、正当行為になる場合はどういう場合

---

11 大阪高判 2007 年 6 月 21 日、2006 年（ネ）1704 号事件、判例集未登載。

12 ただし、その論拠は不法行為に基づくとしている点や、ヤフーと BB テクノロジーの社員との間に「使用者と被用者の関係が成立していた」とするなど、やや擬制に過ぎると思われる。

であり、違法行為になる場合はどのような場合であるかに関して、他の法益とのバランスを考えて、明確な判断基準を示すことが必要である。

この判断基準は、情報セキュリティなどネットワークを防衛する分野において、特に必要である。現状では、「情報セキュリティを守る活動について（中略）『通信の秘密』の議論が十分尽くされていない」、との指摘がある（高橋・吉田 [2006]）ことにも、留意すべきであろう。

またインターネットの活用を通して、利用者の便益・満足度を高めていくことが、社会的にも、経済的にも重要であり、この活用のために、外形（構成要件）的に「通信の秘密」を侵害する場合でも、どういう場合が正当行為であり、どういう場合が違法行為になるかについて、明確で具体的な判断基準を示すことが望まれる。事業者の「通信の秘密」に関する予見可能性を高めることで、事業者のイノベーションを引出し、インターネット利用の便益を増大させることになるからである[13]。

4.7「正当行為」や「通信当事者の合意」の意味についての再考

「通信の秘密」と「他人の秘密」を峻別することで、1.2 で紹介した問題事例のほとんどは氷解し、「他人の秘密」の守り方に関して事業者がどのようなコミットをするかに委ねられるものと考えられる。しかし、何分にも長期間にわたって法解釈に依存してきた分野を、自主判断とコミットメント責任に任せるのであるから、十分な移行期間を取って着実に進め「客観性」を担保することが不可欠と思われる。

その際、従来違法性阻却事由の中心概念であった狭義の「正当行為」と「通信当事者の合意」をどのように再構成するかが、大切なポイントになろう。今回の研究会では、時間の制約等のため、この部分の具体的提言に至らなかったが、次の緊急課題であることは間違いないので、早急な検討の開始が期待される。

4.8 提言に関する付言

以上のように、「通信の秘密」の法益には、個人の権利を守る個人的な法益の側面と、電気通信役務の安定的提供という通信事業者に課された社会的法益がある。加えて、インターネットの活用による社会・経済への貢献という、社会的視点も必要である。このように「個人の権利」の側面と、「通信事業者の責務」の側面を分けたうえで、「通信の秘密」と「他の法益」とのバランスを取る際の、明確な判断基準を明らかにすることが、インターネット時代の通信の秘密の変質のなかで、求められていると考える。

以上の検討を通して、以下の認識を共有することを提言したい。

1) サイバー攻撃に対処するには、パケットの分析が極めて有効であり、この方法は、平時におけるセキュリティ対策としても活用できる。

---

[13] 研究会では、さまざまなケースが出されたが、いずれも公に検討されているケースではなく、今後通信事業者の社会的役割や責務を果たすうえで、明確かつ具体的な判断基準が必要である。

2)　同様に、この技法を広告に活用すれば、「行動ターゲティング広告」と呼ばれる、新しい手段になる。

3)　このような新技術については、「通信の秘密」を絶対視するのではなく、「秘密の保護」と「新技術による活用」の両者の利益を比較考量することによって、バランスを取るといった平衡感覚が必要である。

4)　その際には、日本企業の国際競争力への配慮も必要である。

以上の提言に関して注意すべきは、グローバル市場経済においては、個人の権利を守る面と、各国企業間の競争環境での equal footing を図る面の両面で、各国間の政策・法制度のハーモナイゼーションが必要なことである。

この観点から考えると、「通信の秘密」に関する法制度は、少なくとも日米では大きく異なっており、政策・法制度のハーモナイゼーションを図るうえでは、現在総務省研究会で検討されている「パーソナルデータ」の検討状況を踏まえて、各国共通の課題である「プライバシーや個人データ」にウエイトを置くことが望ましいのではなかろうか。

情報セキュリティ分野では、的確・強力な機密性、完全性、可用性対策を通して、インターネットやクラウドにおける利用者の安心・安全を確保することが、インターネット利用の一層の活発化につながるとされている。この点は、インターネットの潜在力を顕在化する上でも重要である。また、事業者がインターネットの安定的役務提供を行えるような制度設計こそ、利用者と事業者間での win-win 関係を作り上げることができる。

国際的なハーモナイゼーションを図ることは、事業者間の equal footing を実現するものであり、インターネット時代にふさわしい「通信の秘密」の保護とインターネットの活用の姿である。このような観点から、「通信の秘密」の再考を行うことを提言したい。

第５章　インターネットの普及とビジネス・モデルの変化

第 4 章で述べた「通信の秘密」の見直しに関する 7 つの提言が具体化されることで、情報セキュリティの充実を図ることが期待できる。また、イノベーションを活発化することで、インターネットのもつ巨大な潜在的可能性を顕在化することができる。この結果、利用者は個人の権利が守られるなかで、大きな便益を得ることができるし、事業者もより安定的な通信役務の提供が可能になり、win-win の関係を構築することが期待できる。

「通信の秘密」の再考によって、以上の効果が期待できるが、情報産業ないしインターネット産業のビジネス・モデルと、産業のガバナンスのあり方についても、より広範な変化が生じているので、最後に産業融合とそれに対応した規制の変化について述べることにしたい。

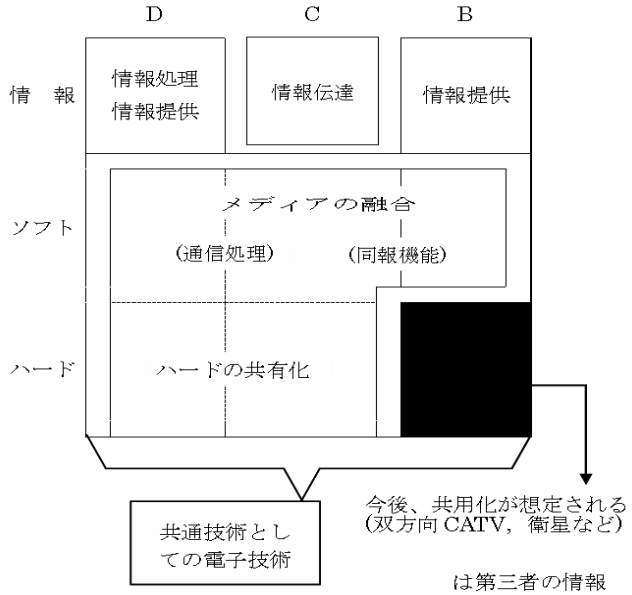
5.1 通信と情報処理、通信と放送の融合

「融合」という言葉はもはや新鮮さが薄れたかの感があるが、事象としての通信と放送の融合やその法制が話題になることが多い。しかし歴史的には、通信とコンピュータによる情報処理の融合が先行し、通信と放送の融合はインターネットが実用化されて以降のことである。この三種の産業分野、つまり通信・情報処理・放送の融合について、約 30 年前の 1984 年に展望したのが以下の図表５．である。

通信と情報処理の融合事象は、米国で始まった。規制制度からみると、通信は連邦通信法でコモン・キャリア・ルールにより規制がかけられる一方で、情報処理には規制がなく、融合事象が進展すると規制の通信と非規制の情報処理の境界を決めることが、困難になってきたからである。

そこで、州際通信の規制機関である FCC（連邦通信委員会：Federal Communication Commission）は、この境界を決めるために 3 次にわたる「コンピュータ調査」を行って、裁定をくだした。現在は、規制対象となる通信サービス （telecommunications service） と非規制の情報サービス （information service） に分けられていて、インターネットにおけるプロバイダ事業は日本とは異なり、非規制になっている。

図表５．情報処理・通信・放送の融合



（出典）　林［1984］

5.2　Ｐ型・Ｂ型・Ｃ型モデルとＩ型モデルの登場

しかし、技術的に別だった産業分野が、同じ技術を使うようになったからといって、直ちに規制のあり方が同じになる訳ではない。マスメディアと通信事業の規制の違いを説明したのが、下図である。ここで、経済的規制にせよ社会的規制にせよ、「あり」というのは業法のレベルで規制が制度化されていることを意味する。例えば「わいせつ情報を送ってはならない」というには立派な社会規範であるが、それが（刑法という一般法のとどまら

ず）業法に規定されている場合のみ、下表６．で「あり」と表記される。

図表６．メディア産業の規制の類型

	社会的規制あり	社会的規制なし
経済的規制あり	B 型：Broadcasting	C 型：Common Carrier
経済的規制なし	I 型：Internet？	P 型：Press

（出典）林 [2005]

マスメディアの中でも、新聞・出版（Press 型）と放送（Broadcasting 型）では、規制の在り方が正反対である。すなわち、放送には経済的規制（参入規制、料金規制など）と社会的規制（安全規制やコンテンツ=番組規制）の両方が適用されているのに対して、新聞・出版には経済的規制も、社会的規制もかけられていない[14]。

一方、伝統的な通信事業者（Common Carrier=C型ビジネス）には、参入規制などの経済的規制がかけられており、コモン・キャリア・ルールが適用されている。コンテンツ規制のような社会的規制がかけられていないのは、伝統的な通信事業者は conduit 事業者であり、預かった顧客の通信にノータッチが求められているためである。

これに対して、プロバイダなどのインターネット事業者は、conduit 事業者から転じたものもあるが他の分野からの参入もあり、現在ではその性格が変わってきている。アメリカでは通信事業者への規制が厳しく、この分野に参入したのは大部分が情報処理を出自とする事業者であり、規制を嫌う彼らは政治的なアピールもしつつ、当初から規制を回避してきた（米国におけるこの政策を unregulation 政策と呼ぶことがある[15]）。

このような歴史的経緯から、プロバイダなどのインターネット事業者のサービスは、アメリカでは情報サービに分類されており原則的に非規制、日本では出自にもよるが主要なプロバイダが旧第二種電気通信事業者から転じていることもあって、原則的に電気通信事業法の規制対象となっていることは前述した。

しかし 1.2 の事例でみたように、歴史的な経緯はともかくプロバイダは現在、何らかの形で content に関与することが求められている。このような社会的要請に応えるには、どうしたら良いか。業法で対応すべきか、一般法に期待するのか、私たちはインターネットの成熟とともに「メディアのあり方」という新しい問いに直面している。

5.3 インターネット・モデルと規律のあり方

上記のように、従来「狭義の通信」は、「伝送内容にタッチしない業態」と考えられてきたが、その役割が変化しつつある。そのきっかけとしての「プロバイダ責任（制限）法」

14 この放送と新聞の規制の違いが合理的であるとするのが、ボリンジャーの部分的規制論である。部分的規制論については、林 [2005] 参照。

15 unregulation 政策については、林 [2002] 参照。

の制定以降は、Ⅰ型に変質しつつあると見るべきだろうか。

他方、もともと何らの規制も受けないで発展してきたインターネット・ビジネス（Ⅰ型）も、児童ポルノや違法サイトの削除などで、content 規制を受けざるを得ないと見るべきだろうか。「放送倫理」という厳しい規制を受けてきたB型ビジネスは、引き続き同様のレベルの規制を受けるべきか。それとも、Ⅰ型規制と同等のレベルの規制を上限とすべきか。

いずれにしても、従来とは違った「メディア規制」のあり方が問われており、クラウドも包摂したビッグ･ピクチャーを描くべき時期に来たのではないか、思われる。現在の法秩序は 1985 年の電気通信の自由化と電電公社の民営化に基づくものと考えられるが、その当時にはインターネットは存在したものの、今日のような圧倒的地位は獲得していなかったことに注意する必要があろう。

その後の変化は、俗に言う「ドッグ・イヤー」そのものとも言うべき激変であり、私たちは今こそ、1985 年体制に代わりインターネット産業に関する新しい規律を必要としている。

[引用文献]

片桐裕「70 電話の逆探知、通話の録音等」前田正道編［1986］『法制意見百選』有斐閣

金光昭・吉田修三[1953]『公衆電気通信法解説』日信出版

総務省［1999]「情報通信の不適正利用と苦情対応の在り方に関する研究会」報告書

総務省［2007]「郵便・信書便制度の見直しに関する調査研究会」第 2 回資料 2、http://www.soumu.go.jp/yusei/seido_minaoshi/pdf/070327_1_si2.pdf)

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」

高橋郁夫・吉田一雄［2005]「ネットワーク管理・調査等の活動と『通信の秘密』」http://www.jaipa.or.jp/info/2005/iw2005.pdf)

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

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

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

電気通信法制研究会［1987]『逐条解説 電気通信事業法』ぎょうせい

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［2011]「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（第 2 版)」http://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf

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（改定)」(2012 年)
http://www.jaipa.or.jp/other/bandwidth/guidelines.pdf
長谷部恭男[2012]「第 4 章 通信制度」宇賀克也・長谷部恭男編『情報法』有斐閣
林紘一郎［2002]「インターネットと非規制政策」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
林紘一郎［2005]『情報メディア法』東京大学出版会
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―」『法社会学』第 69 号
林紘一郎・田川義博・淺井達雄［2011］『セキュリティ経営　ポスト 3.11 の復元力』勁草書房
林紘一郎・田川義博［2012］「心地よい DPI （Deep Packet Inspection） と程よい通信の秘密」『情報セキュリティ総合科学』第 4 号
藤田寿夫［1994]『表示責任と契約法理』日本評論社