資料８－６

「通信の秘密」の比較法的研究・序説[1]

弁護士　高橋郁夫[2]

第１　ISP の活動と通信の秘密

１　通信の秘密の「数奇な運命」

わが国における「通信の秘密」の解釈の拡大が、現代社会において、インターネット時代の重要な情報通信の担い手である ISP の活動との関係において緊張感を有しているのではないかということができる。かかる点に関連して憲法の制定時の起草者の意図や制定法における解釈の変遷については、高橋郁夫・吉田一雄著「ネットワーク管理・調査等の活動と『通信の秘密』」[3]・「通信の秘密の数奇な運命（憲法）」（情報ネットワーク法学会誌第５巻（2006 年５月））・林紘一郎・舟橋信・高橋郁夫・吉田一雄著「通信の秘密の数奇な運命（制定法）」によって明らかになったものである。

では、現代社会において、世界各国の ISP の活動は、どのような法的位置づけのもとでなされているのか。そこでの活動と社会とのかかわりを、我が国において通信の秘密に該当する事実についての取得・利用・開示[4]について、どのような規制がなされているのかという観点から見つめなおすことは、改めて、我が国における通信に関する種々の秘密とすべき事項に対する法的位置づけを見直すのにきわめて有効な意味をもつであろう。

２　通信の秘密の射程範囲

通信の秘密が、ＩＳＰのネットワーク活動に及ぼす影響については、きわめて大きなものがあるといえる。それを具体的に述べると以下のとおりになる。

（１）通信に関連するデータの記録[5]

---

1 **なお、本調査のうち米国法に関係する部分については、基本的に 2002 年段階のものである。その後の法律の発展、解釈の発展、特にネットワークの中立性をめぐる議論などについては、フォローが十分ではない。**

2 株式会社ＩＴリサーチ・アート代表取締役

3 オンラインによる発表であるが　http://www.jaipa.or.jp/info/2005/iw2005/IW05.pdf。
なお、この報告をもとにインターネットウイーク 2005 でシンポジウムが開催されおり、その報告は、http://internet.watch.impress.co.jp/cda/event/2005/12/12/10198.html。

4 電気通信事業法の「通信の秘密」保護との関係で、問題になる行為の３つの側面ということもいえる。「通信の秘密」を侵すとは、「積極的取得」「窃用」「漏えい」の行為をなした場合であり、それらの行為に対応する側面ということになる。

5 このデータの記録については、一般に匿名性といわれている問題のうちの追跡可能性の問題である。追跡可能性は、ある・なしの問題ではなく、行為者を特定するためにかかる経済的なコストであると定義することができるであろう。その意味で、株式会社三菱総研「サイバー空間における権利利益の保護・救済のための基盤に係る調査研究」（概要版）のよう

発信者情報開示問題・法執行機関に対する情報提供問題（記録）

（２）トラフィックによる問題

帯域制限問題・セキュリティ関心からのネットワーク管理活動（取得・利用・開示）・法執行機関に対する情報提供問題（リアルタイム）

（３）通信の内容に関係する問題

有害情報についての伝達制限問題・違法情報についての伝達制限問題

がある。

第２　通信の構成要素とデータの種別

１　通信のデータの種別

電気通信に関する種々のデータとしては、一般に、通信内容のデータ、ルータやサーバの通信ログ、サーバ上のログ、データ領域のメール、課金データ、料金明細書、トラフィック分析書…などが、通信に関する種々の情報ということになる。そこでは、個々の通信を構成する要素であるものと、それ以外の事実およびそれらの記録がある。個々の通信を構成するかという観点からみるとき「通信の構成要素」「それ以外の通信の要素」「プライバシーの観点から保護すべきデータ」などにわけることができよう。

ここで、通信の構成要素のうち、通信の内容とそれ以外にわけるときに、通信の内容以外をなんと呼称するのかというのが意外と問題である。サイバー犯罪条約においては、トラフィックデータという用語が使われている[6]が、我が国では、トラフィックデータというときに、実は、トラフィック分析書において把握される抽象的なトラフィックについてのデータを示す用語として使われている。また、我が国におけるトラフィックデータの訳語とされる「通信履歴」という用語は、データの内容か否かという視点に（過去のデータの）記録という視点を混在させるものであって、きわめて誤解をまねきやすい[7]ものである。

に、一定の制度があるかどうかという問題の立て方によって分析するのは、賢明とはいえないであろう。問題は、被害者なり法執行機関がどの程度の労力・金銭（コスト）を使って、発信者を特定しうるかということであり、実務の運用まで踏み込まないと正確な分析はできない。

6 サイバー犯罪条約１条ｄ項は、『トラフィック・データ』とは、コンピュータ・システムという手段による通信に関するコンピュータ・データであって、通信の連鎖の一部を構成するコンピュータ・システムによって作り出され、かつ、その通信の発信元、あて先、経路、時刻、日付、大きさ、持続時間又はその背後にあるサービスの種類を示すものをいう。」と定義している。そして、この定義に関連して第２０条においては、「トラフィック・データのリアルタイム収集」が定められ、これに比較して、第２１条においては、「通信内容の傍受」が定められている。

7 誤訳であるといってよいであろう。リアルタイムで、トラフィックデータを分析する、もしくは共有するという論点についての考察を怠りがちになるのは、このような訳の影響があるかもしれない。また、プロバイダへの通信ログについての保全命令は、過去のトラフックデータであるから許容されるのであって、その命令は、将来にわたるものではないということについての考慮を欠きがちになる（法制審議会においてかかる規定が途中で修正された経緯を参照のこと）のは、トラフィックデータについても過去のデータか・リアルタイムでの分析かかという視点が重要であるという認識がないことをものがたっており、

英国における 2000 年捜査権限規制法 （Regulation of Investigatory Powers Act 2000 ）（RIPA という）のこの第２章（Chapter２）は、このような通信の内容とそれ以外についての分類を明言している。そこで、「通信データ（communications data)」というのは、通信に関する内容以外のデータをいうが、具体的には、

トラフィックデータ

サービス利用データ

加入者データ

の３種類からなりたっている(第 21 条(4)項)。以下、通信内容以外について通信データということがある。

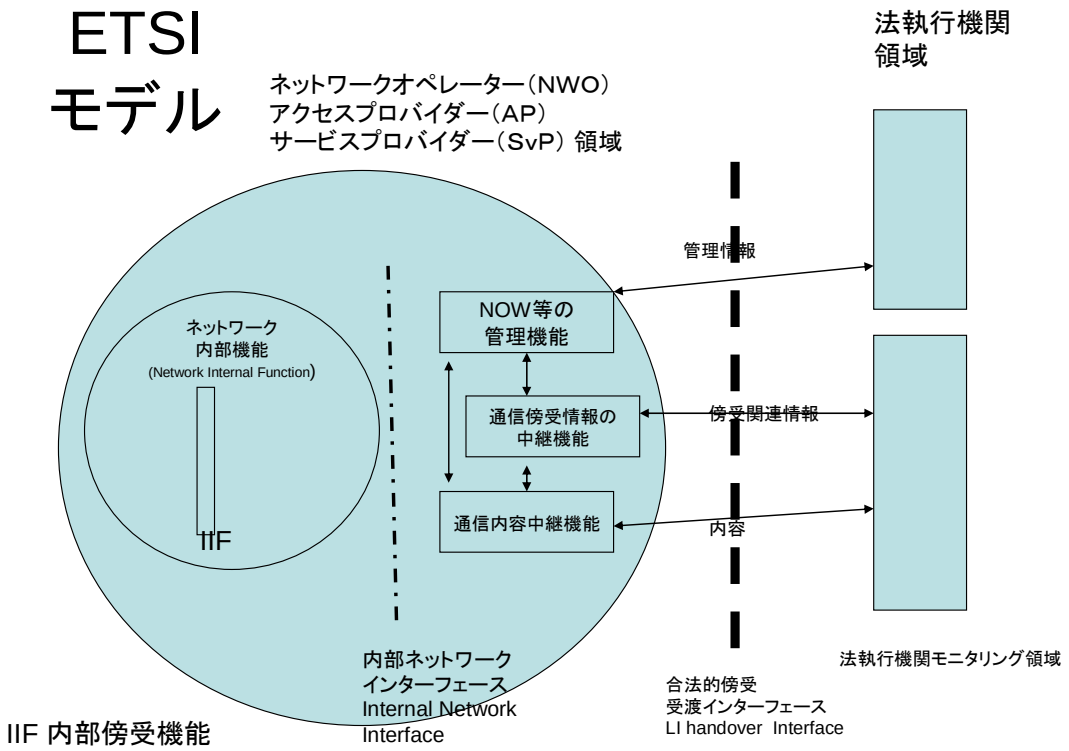
２　データの種別とデータ交換の議論

上述のデータの種別は、「合法的傍受におけるデータ交換の標準化の議論」などをみるときにきわめて参考になる。刑罰法規に違反する行為が存在している場合において、法執行機関が、かかる違法行為に関して、証拠を収集し、法執行を裁判所に求めるというのは、社会正義の維持のために絶対的に必要なことである。そして、そのために通信の傍受というのは、きわめて有効な手段として認識されている。我が国においても、「犯罪捜査のための通信傍受に関する法律」が制定されているところである。また、後述するようにプロバイダ等からの任意での法執行機関への情報提供ということも議論の念頭におかれるようになっている。

現在、インターネットの通信について、通信データおよび内容を問わず、それぞれの各国の法執行の要請により合法的に通信傍受をなし、そのデータを、法律の認めるところによりお互いに交換すべき技術的基準が定められてきている。このような傍受行為を「合法的傍受（Lawful Intercept)」とよんでいる。具体的な基準としては、ETSI モデル[8]や RFC3924 をあげることができる。例えば、ETSI モデルを例におってみたときに、このモデルは、３つのポートの構成をとっている点が特徴を有する。管理情報（administrative information (HI1)）、傍受関連情報（ intercept related information (HI2)）、通信内容（ the content of communication (HI3)）の三つにわけて、それぞれ関係者間のデータや情報の受け渡しのプロトコルを統一することになる。これを図示すると以下のようになる。

かかる誤訳と同一の根拠からでているものであろう。

[8] http://www.etsi.org/WebSite/homepage.aspx
合法的傍受の委員会のポータルは、http://portal.etsi.org/li/Summary.asp
具体的には、ES 201 671 Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic (revised version).



ES 201 671 18頁の図

管理情報（administrative information (HI1)）というのは、法執行機関とネットワークオペレーター（NWO)、アクセスプロバイダー（AP)、サービスプロバイダー（SvP）との間で交換される情報であって、合法的傍受を行うために必要とされる情報ということになる。具体的には、ターゲット識別符号、合法的傍受識別符号、傍受の開始および終了時期などについての情報を意味することになる。

傍受関連情報（ intercept related information －IRI ともいわれる(HI2)）は、ターゲットとなる通信サービスの識別情報に関連する情報またはデータである。電気通信サービスを確立したり、進行をコントロールしたりためのシグナル情報、タイムスタンプ、可能であれば、付随的情報、所在地情報などをも含むものである。

通信内容（ the content of communication (HI3)）は、まさにその通信の内容ということになる。

このモデルは、いうまでもないが、それぞれのポートに対して内国法の対応が異なることも前提としており、かかるそれぞれの情報について、各国がどのような法的対応をとっているかという点について注目すべきことは、このようなモデルに基づく円滑な情報共有という観点からして、きわめて重要におもえる[9]のである。我が国において、通信の構成要素がすべて「通信の秘密」であるとされていることによって、このような世界的に、通信の構成要素等についての区別を前提として、種々の枠組みを構成するのに、ハーモナイゼ

[9] 我が国にとってきわめて重要な作業と思われ、今後の重要な課題である。

ーションをとりにくいということがあってはならないことに留意する必要があろう。

第３　米国における通信の秘密の位置づけ

１　プライバシーの合理的な期待と法律の全体構造

最初に、米国における「通信の秘密」の保護は、それが、通信の関係者の「プライバシーの合理的な期待」を侵害するかどうか（もしくは、侵害した場合に、何らかの例外として許容されかどうか）という文脈で議論されることになる。これは、合衆国憲法第 4 修正に関して、「令状によらなくても、捜索は、それが被処分者のプライバシーの『合理的な』期待ないし『正当な』期待に反するものでない限り、合憲である。」（Katz v. United States, 389 U.S. 347, 362 (1967)）という定理としてかたられることになる。もっとも、これが、インターネットを利用した通信との関係で議論される場合には、二つの側面があることに注意がなされなければならない。すなわち、インターネットは、その構造上、通信に関するデータが、種々のサイト間を伝達され、それが、蓄積され、それが読み出されて、通信の目的人に到達するというものであるから、蓄積されたデータというものであっても、「プライバシーの合理的な期待」の対象になるという特徴を有しているのである。通常の音声通信においては、その伝達途中の通信に対するリアルタイムの受信を意味する「電子的監視」からの保護のみを考えていれば良かったのに対して、蓄積されたデータに対する保護をも考えなければならないということになる。この観点は、通信の目的地か、その中間的な地点かという点についての意識を基本的な概念として必要とすることになる。

なお、電気通信おけるプライバシーという観点からするとき、国内通信に関係する上記法体系にくわえて、国家安全を理由とする傍受の体系も存在することになる。

また、我が国において通信の秘密が影響している問題のうち、通信の内容が直接に絡む問題については、むしろ、米国では、通信の中立性の問題で議論されている。

２　米国における ISP の法律問題[10]の検討枠組み

この点における分析の視点は、以下のようになる。なお、本稿においては、いわゆるＩＳＰに対する法的規制にかぎって考察する。米国法でいう公共の電気通信サービスとされるプロバイダに対する規制に限定しての論述ということになる。

---

10 この点については、Mark Eckenwiler「Online Criminal Investigations: The USA Patriot Act,ECPA, and Beyond」「ISPs and Federal Privacy Law:Everything You Need to Know About the Electronic Communications Privacy Act (ECPA)」www.nanog.org/mtg-0010/ppt/justice.ppt がある。

	リアルタイム			記録
	取得	利用	開示	
コンテンツ	プロイバイダ例外	ネットワーク中立性(帯域制限)	任意開示 (民間)？ (LE)同意例外・コンピュータ侵入者例外	(民間)不許可・例外あり (LE)原則不許可
			法執行 (LE) タイトル 3(通信傍受)、FISA 法	(LE) 捜索令状・告知付提出命令
通信データ	積極的了知も許容	不明	(民間)不明 (LE)ペンレジスター・逆探知命令	(民事)提出命令 (LE)提出命令・d 命令

(1)リアルタイムか過去の記録か-「電子的記録」と「電子的監視」[11]

第４修正が、「プライバシーの合理的な期待」を保護するといっても、通信に関するデータに、第４修正がどのように関与するかという点は、ある意味で不明確であるとされる。これは、通信当事者は、ネットワークプロバイダに対し送信された情報には「合理的なプライバシーの期待」を保有することができないからである。情報を送信した者は、銀行記録やダイアルされた電話番号と同様に、情報の一部を開示することになり、また、第三者のもとで保管されている情報については、コントロールを第三者に対して放棄することになるので第 4 修正の保護を失うことになるからである。逆に、通信途上のデータでも、いったんは、保存されるから、蓄積されたデータにたいする保護の要請とリアルタイムで監視する電子的監視からの保護の要請という二つの観点があることが明らかになる。

リアルタイムで通信に関する情報を覚知する行為は、電子的監視といわれる。米国法のもとでは、これについては、覚知する情報の対象によって、二つのアプローチがある。通信の外形的事実に関する情報と経路情報を含むヘッダの部分については、ペンレジスター・逆探知法、18U.S.C.§§3121-27 がこれを規制し、メッセージの通信内容については、「タイトルⅢ」の厳格な規定に服することになる。

---

11 米国司法省（Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice）「犯罪捜査におけるコンピュータ捜索・差押および電子的証拠の獲得(Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations)」（以下、司法省マニュアルという）（http://www.cybercrime.gov/s&smanual2002.htm）もきわめて参考になる。なお、本稿における翻訳は、「アメリカにおけるハイテク犯罪に対する捜査手段の法的側面」報告書における「犯罪捜査におけるコンピュータ捜索・差押および電子的証拠の獲得」(以下、司法省マニュアルという)（訳・サイバー犯罪刑事手続調査委員会）（社会安全研究財団、2004）による。

(2)内容か通信データ部分か

以下のような米国法においては、通信の内容なのかそれ以外なのかという点が重要である。リアルタイムの取得にせよ、記録についてのアクセス・開示の問題にせよ、法的には、それぞれ、この種別に応じて対応が準備されている。

３　通信の内容について

プロバイダが、通信当事者間の通信の内容を了知して、それにもとづいて一定の対応をなすということが法的にどのように位置づけられているかという問題になる。プロバイダといえども、基本的には、その通信内容に対して、これを特別に取得するというものではないということになる。ましてや、政府等が積極的に取得するということはありえないことになる。

3.1.通信内容のリアルタイムでの取得・利用・開示と法的規制

（１）　「プロバイダ」例外について

18U.S.C.§2511（2）(a)(i)によると、いわゆるプロバイダの業務に従事しているオペレーター、役員、従業員、または捜査官は、必要な通常の過程において、そのサービスの遂行もしくは、権利や財産を保護するために通信を傍受し、開示し、または使用することができるとされている。ただし、そのプロバイダが、「公衆に対する」プロバイダである場合は、機械的に行われる品質管理チェックをする場合を除いて、サービスの監視や無作為のモニタリングを行ってはならないとされている。この規定によって、損害、窃盗、またはプライバシーの侵害から、システムを保護するためにプロバイダはシステムの不正使用をモニタリングすることが許されるとされ、例えば、システム管理者は、一層の損害を防ぐために、ネットワークにおいてハッカーを追跡することができるとされるのである。

しかしながら、この規定は、プロバイダ自身の権利や財産を保護するために通信を傍受して、法執行機関に開示することができるにすぎず、法執行機関が、法執行目的でシステム管理者にモニタリングを指示したり、または頼んだりすることはできない。

（２）ネットワーク中立性について

上記プロバイダ例外によれば、プロバイダが取得した内容について権利や財産を保護するため使用・開示できることになる。もっとも、その場合、どのようなことも可能なのかという論点がでてくる。米国においては、この論点は、むしろ、ネットワーク中立性の議論として議論されている。我が国でも問題になっているＰ２Ｐの帯域制限の問題である。

アメリカにおいては、著作権侵害のトラフィックに対して何らかの対応ができないかどうかという問題は、ネットワーク中立性（Net Neutrality）の問題の名のもとに議論されている。これは、おそらくトラフィックを第三者に託した以上、その内容については、了知されることが前提であるという理論的な位置づけが影響しているものと思われる。

ネットワーク中立性というのは、通信事業者は、すべてのコンテンツを平等に取扱い、えり好みしてはならないという原則をいう。2006 年ころから、この問題が議論されたが、特に、2007 年秋にアメリカ大手のプロバイダであるコムキャストが、BitTorrent のトラフィッ

クを制限しているのではないかというのが議論になり、ＦＣＣが公聴会を開催している。また、公益保護団体が、ＦＣＣ（連邦通信委員会）に対してコムキャストが、P2P トラフィックを遮断することを恒久的に禁じ、同社に 19 万 5000 ドルの罰金を科すよう求めている 。

（３）内容データの第三者への開示

プロバイダが上記プロバイダ例外によって取得した通信の内容を利用するとき、それを第三者に開示するという場合がどのような場合としてあるのか、それが具体的にどのように許容しうるのかという点については、いまだ研究が進んでいないところである。

（４）内容データのリアルタイムでの法執行機関との連携

通信の内容についてリアルタイムで法執行機関が強制的に取得するという手法は、タイトル３による傍受令状という形になる。また、 ”The Foreign Intelligence Surveillance Act of 1978”によれば，米国に根拠を置く外国人や市民が外国のテロリストのメンバーであるか外国のエージェントであると信じる相当な理由がある場合には，その通信を傍受することが可能である。また，2001 年パトリオット法において，かかる行為を前提とした条文（225 条など）が定められている[12][13]。

なお、この場合のプロバイダと法執行機関の協力については、ＣＡＬＥＡ法の規定がある。

また、プロバイダが任意に法執行機関に対して協力を求めることができる場合がある。これが、前出のプロバイダ例外もそうであるが「同意」例外および「コンピュータ侵入者」例外の規定ということになる。同意例外については 18U.S.C.§2511（2）(c)、(d) によると、通信の当事者または一方の通信当事者が事前の同意を与えた場合においては、電気通信を傍受することができる（違法行為を目的とする場合の除く）とされている。もっとも、インターネットで、通信を了知しうるので、捜査当局や ISP が同意をしているから、内容をいつもみられるという意味には用いられていない点は、重要である。コンピュータ侵入者例外は、18U.S.C.§2511（2）(i) に定められているが、4 つの要件が満たされる場合（①コンピュータの所有者またはオペレーターが侵入者の通信の傍受を許可すること②通信傍受者が捜査に合法的に従事すること③コンピュータ侵入者の通信の内容が捜査に関連すると思料する合理的理由があること④侵入者の通信以外を傍受しないこと）に、コンピュータ攻撃の被害者が、法執行機関にコンピュータ侵入者の有線または電子通信を傍受する許可を与えている。法執行機関は、そのような場合に保護されたコンピュータ「に対して、を通

[12] 特に，2005 年末にブッシュ大統領が，裁判所の令状なしに上記通信傍受をしていた件について，議会への報告を欠いていたことを認めたため，この点をめぐって議論が沸き起こった。

[13] ブッシュ大統領の令状なし盗聴事件のあと、 議会で大統領の通信傍受命令をなしうる権限を広げる法案が審議されたが、2007 年 1 月にブッシュ大統領は、令状をとって通信傍受を行うという声明をだしている。その後、本法は、改正されており、Protect America Act of 2007 が制定された。が、期限付き条項であり、2008 年 2 月 17 日に失効している。

して、あるいは、から」コンピュータ侵入者の通信を傍受することができるのである[14]。

3.2. 内容の電子的記憶についての法執行機関等への開示

通信データがプロバイダに記録される場合にその通信の内容に関するものについて、第三者への開示等の問題が発生することになる。

（１）内容のデータの第三者への開示

通信内容について、当然に秘密を前提として通信がなされている場合には、これを民間の第三者に開示する場合については、原則として禁止されるということになる。

しかしながら、(ア）開示が「当該サービスの提供あるいは当該サービスのプロバイダの諸権利または財産の保護に必然的に付随する場合」18U.S.C. §2702(b)(5)

（イ）プロバイダが「人に対し死または重大な身体的傷害の直接の危険をともなう緊急状況が遅滞なく情報を開示することを必要としていると合理的に信じる」場合、

（ウ）開示が通信の意図された受取人に対してなされる場合、意図された受取人もしくは送信者の同意をもってなされた転送アドレスに対してなされる場合（18 U.S.C. § 2702(b)(1)－(4)）

においては、許容されることになっている。

（２）法執行機関への内容の任意の開示

法執行機関に対して任意の開示が許されるのは、上記の（ア）（イ）（ウ）の場合にくわえて、(エ)「コンテンツが…サービスプロバイダによって意識せずに入手され……、犯罪の遂行に随伴しているようにみえる場合、……法執行官」対して開示がなされる場合、18U.S.C.§ 2702(b)(6)(A)、（オ）Child Protection and Sexual Predator Punishment Act of 1998, 42U.S.C.§13032 は開示を委任している場合 18U.S.C.§ 2702(b)(6)(B)である。

（３）法執行機関の強制的取得

法執行機関がＩＳＰの通信内容の記録について強制的に取得する手法として開封された内容か否かで保護の程度が変わってくる。「180 日間以上電気通信システムにおける電子的記憶に存在している有線または電気通信の内容」(18 U.S.C.§2703(a))については、§2703(b)(1)(B)および§2705 の告知条項にしたがう場合の提出命令により政府は取得が可能になる。一方、「180 日間以下の期間、電気通信システムにおいて電子的記憶にある電気通信のコンテンツ」18 U.S.C.§2703(a)については、捜索令状が必要になる。

４　通信データについての問題

4.1. 通信データのリアルタイム取得・利用・開示

（１）通信データのリアルタイム取得について

ＩＳＰが、通信データをリアルタイムで取得するとして、それは、すくなくても、通信を届けるという限りにおいては、当然のことであり、法的な問題を惹起するものではない。

---

[14]議会が延長しないかぎり、コンピュータ侵入者例外は、2001 年パトリオット法の一部として 2005 年 12 月 31 日に終了するとされていた、PATRIOT Act §§217, 224, 115 Stat. 272, 290-91, 295（2001）参照。現在では、延長された。

しかしながら、通信の伝達のレベルを越えて、一定の場合に上記消極的な了知を越えて、いわば積極的了知というレベルになると法的に許容されるのかという議論がでてくることになる。

この点で、ペンレジスター・逆探知法は、電気・有線通信サービスのプロバイダに自己のネットワークで裁判所命令なしでペンレジスター・逆探知装置を使用する権限を与えている。18U.S.C.§3121（b）は、プロバイダが、裁判所命令なしでペンレジスター・逆探知装置を使用しうるとして（1）有線・電気通信サービスの操作・維持及びテスト、またはプロバイダの権利又は財産の保護、並びにサービス乱用・不正使用からユーザを保護する場合（2）プロバイダや有線通信の終了にサービスを提供した別のプロバイダを保護するため、またはサービスの提供を受けているユーザを詐欺的、不正、乱用サービスから守るために、有線・電気通信が開始され又は終了したという事実を記録するため、または（3）そのサービスのユーザの同意を得ている場合をあげている。従って、そのペンレジスターおよび逆探知装置の定義によって明らかにされているように、「ルーティング、アドレスまたは信号情報」であって、通信内容を含まない情報については、プロバイダが、ペンレジスター・逆探知装置によって、これを積極的に知得しうることになる。ISP としては、自己もしくは別のプロバイダが何らかの攻撃がなされたという認識をなした場合、ユーザの保護の観点から必要な場合には、通信経路の記録および逆探知をすることができる。なお、リアルタイムでこのような情報を法執行機関に伝えるということが可能かどうかという点については不明である。

（２）通信データのリアルタイムでの利用について

上記ペンレジスター・逆探知装置によってえられた情報をも含めて、プロバイダが、取得した通信データをどのように利用することができるかは不明確である。報道によると、プロバイダが、攻撃に対して種々の方法をとっており、その際に、そのようなデータが相当程度利用されていることが伺われる[15]が、今後の研究課題であるということになる。

（３）通信データの第三者への開示について

民間への開示に関しては、特に規制は、存在しないようである[16]。

法執行機関に対する任意の開示は、禁止される。このような場合は、ペンレジスター・逆探知法は、「得られそうな情報が進行中の犯罪捜査に関連している」限り、検事がペンレジスター及び／又は逆探知装置の設置を許可する命令を求めて裁判所に申し立てることを認めている（18U.S.C.§3122（b）（2））のであり、法執行機関は、そのような手法をとることになろう。もっとも、内容については、プロバイダ例外・コンピュータ侵入者例外が認

---

15 Ryan Singel “ISP Seen Breaking Internet Protocol to Fight Zombie Computers -- Updated” (http://blog.wired.com/27bstroke6/2007/07/isp-seen-breaki.html)によると、Cox Communications が、DNS を書き換えることによりマルウエアを書き換えるパケットを送付したとのことであり、そのような行為が許容されるのかということが NANOG の ML で議論されたとのことである。

16 この点については、司法省マニュアル（翻訳）注２１、123 ページ

められるので、かかる例外により任意の提供がなされるかぎりで、通信データも取得することができるといえよう。そのような場合、法執行機関がかかる例外の解釈として積極的な取得が許されるかどうかについては、不明である。

なお、ペンレジスター・逆探知命令によって許容された場合、ペンレジスターは架けた相手の情報（モニタリングされた電話からダイアルされた番号など)、逆探知装置記録は架かってきた相手の情報（発信者番号情報などの）を記録する。

4.2. 通信データの提供

民間への提供か、また、政府(法執行機関)に対しては、加入者情報か、個別の通信に関するデータかが、問題となる。また、任意に開示するかどうかという点でも規制が異なっている。

（１）民間に対する提供

民間に対しては、いわゆる発信者情報開示の問題ということになる。基本的には、提出命令による。提出命令のための手続きは、簡易なものということがいえるであろう。我が国と比較した場合に、提出命令を受けたプロバイダは、そのまま開示するのが一般ということになる。但し、発信者本人への通知がなされるようになってきたということである。また、著作権侵害については、別個の規定がある。これらの点の詳細は、森亮二「米国におけるプロバイダ責任制限法」(「インターネット上の誹謗中傷と責任」所収）（商事法務、2005）に譲る。

（２）法執行機関への任意の開示の問題

プロパイダが法執行機関に非コンテンツの顧客記録を任意に開示することが許容される場合については、以下の場合があげられている。

１）開示が「当該サービスの提供あるいは当該サービスのプロバイダの諸権利または財産の保護に必然的に付随する場合」§2702(c)(3)

2）プロバイダが「人に対し死または重大な身体的傷害の直接の危険をともなう緊急状況が」開示を正当化すると「合理的に信じる」場合、§2702(c)(4)

３）開示が意図された受取人の同意をもってなされるかまたは裁判所命令もしくは法律上の手続きにしたがってなされる場合§2702(c)(1)-(2)

（３）法執行機関に対する強制的な開示の問題

強制的に開示させる手法については加入者情報については提出命令の規定が適用されることになり、パトリオット法がこの対象などを明確にさだめたことになる。この点については、具体的には、18U.S.C.§2703(c)(2)に列挙された加入者基本情報の開示を政府は強制することができる。具体的には、(A)氏名、(B)住所、(C)近距離および長距離電話の接続記録もしくはセッション回数および経過時間の記録、(D)サービスの期間（開始の日付を含む）および利用したサービスの種類、(E)電話番号もしくは機器番号あるいはその他の加入者番号もしくは一時的に割り振られたネットワークアドレスを含む識別符号ならびに(F)当該サービスのための支払手段および支払元（クレジットカード番号や銀行口座の番号な

らどれも含む）（18U.S.C.§2703(c)（2））。である。

これに対して、通信データのうち、上記以外のものについては、令状もしくは§2703（d）の裁判所命令（以下(d)命令）ということになる。）「当該サービスの加入者またはその顧客に関係する」すべての「記録またはその他の情報（（電気通信サービスとリモートコンピューティング・サービスの提供者により保持されている）通信の内容を含まない）」については、この「d」命令による請求ということになる。この命令の取得のためには、「詳細な事実（articulable facts）」を明らかにしなければならないが、政府機関は、有線または電気通信の内容または記録もしくはその他求める情報が継続中の犯罪捜査にとって重要でありかつ本質的であると信じる合理的な理由が存在することを示す具体的で詳細な事実を申立（なければならない）。この基準は、そのような申述を満足させる具体的かつ詳細な事実を有していることをたんに保証すればたりるということを法執行機関に認めるものではない。むしろ、政府は、命令の申請において裁判所にそのような事実を実際に申し述べなければならない[17]。

第４　英国

１　英国におけるプロバイダの活動に関する法規制

ISP をめぐる法律問題と「通信の秘密」に関する分析の枠組みとして

（１）通信に関連するデータの記録

発信者情報開示問題・法執行機関に対する情報提供問題（記録）

（２）トラフィックによる問題

帯域制限問題・セキュリティ関心からのネットワーク管理活動（取得・利用・開示）・法執行機関に対する情報提供問題（リアルタイム）

（３）通信の内容に関係する問題

有害情報についての伝達制限問題・違法情報についての伝達制限問題

の各論点ごとに分析するという点は前述したところである。

英国において、通信に関するデータの取扱について参考になる規定のうちでもっとも重要なものの一つは 2000 年捜査権限規制法[18]（Regulation of Investigatory Powers Act 2000 ）

---

[17] §2703（d）に対する 1994 年の修正に付随している下院報告は、以下の分析を含んでいた。

本条は、オンラインのトランザクション記録を保護するため、中程度の基準を設定している。提出命令より高いが、相当な理由による令状ほどは高くない基準である。

トランザクション・データにアクセスするための基準を引き上げた目的は、法執行機関による「証拠あさり」から守ることである。この中程度の基準のもとでは、法執行機関の事実の提示に基づいて、裁判所は、当該記録が継続中の犯罪捜査に関連しかつ本質的であると信じる具体的かつ詳細な根拠が存在することを認定しなければならない。

[18] 今井猛嘉「イギリスにおけるコンピュータ犯罪の動向と対策の研究―電子商取引時代に要請される国際的な対策に関する検討―」

(RIPA).である。また、反テロ法（Anti-Terrorism, Crime and Security Act 2001）によって定められる通信データの保全規定（第 11 編）や電気通信規定（Telecommunications (Data Protection and Privacy) Regulations 1999）の定めなども有意義であろうと思われる。

２　英国法における通信の秘密性保護の枠組み

（１）枠組み概要

	リアルタイム			記録
	取得	利用	開示	
コンテンツ (RIPA1 章傍受の規定)	RIPA3 条(3)	不明	任意開示 (民間)？ (LE)不明	(民間) 不明 (LE)原則不許可
			法執行 (LE)不明	(LE)不明
通信データ (RIPA2 章)	当然	不明	(民間)不明 (LE)RIPA21 条	(民事)命令 (LE)RIPA22 条

英国における上記問題についての基本的な枠組みを表にするとき上述のようになる。通信に対する取得・利用についての基本的な枠組みは、Regulation of Investigatory Powers Act (RIPA)[19]が、その枠組みを設定しているので、まずは、RIPA から検討することとする。

（２）RIPA 法の制定趣旨

RIPA は、犯罪（テロリズムを含む）の予防のための監視および情報収集のための方策を定めるための法律ということがいえ、その内容として「通信の傍受」「通信に関連するデータの取得および開示」「監視の実行」「秘密人的諜報資源（covert human intelligence sources）の利用」「暗号もしくはパスワードによって保護された電子データへのアクセス」「コミッショナーの氏名およびこれらの問題の監督機関の設立」を定めている。

この中で、通信に直接関係するものは、「通信の傍受」「通信に関連するデータの取得および開示」の定めであり、また、「暗号もしくはパスワードによって保護された電子データへのアクセス」も、暗号通信に対する法執行機関のアクセスという観点からは興味深いものである。従来は、これらについての英国のもともとの定めは、"Interception of Communications in the United Kingdom" (CM 4368) published on 22 June 199 であり、それらの規定を現代化したものということもいえる。

（２）　内容の「傍受」と通信データの「取得・開示」

RIPA の法目的は、犯罪（テロリズムを含む）の予防のための監視および情報収集のための方策の定めであるが、通信に関する傍受等の定めは、通信傍受、通信データの取得に関

[19] http://security.homeoffice.gov.uk/ripa/about-ripa/

する一般法の定めとしての性格をも有することになる。まず、その前提として、RIPA は、通信に冠する第三者の関わりを「通信の内容」に関するものと通信の内容以外の「通信データ（Communication Data）にわけて、規制している。通信の内容に関する行為は、「傍受（Interception)」として、非常に厳しい規制のもとにおかれている。一方、通信データに関する取得行為については、権限のある場合、もしくは要件にしたがった場合適法であることが明らかにされている。

RIPA　第１編（Part１）は、「通信（Communications)」であり、その編は、

第１章　傍受（Interception）

　違法および無権限傍受（Unlawful and authorised interception）

　傍受令状（Interception warrants）

　傍受能力およびコスト（Interception capability and costs）

　傍受結果の使用制限（Restrictions on use of intercepted material etc）.

第２章　通信データの取得および開示（Acquisition and disclosure of communications data）

　からなりたっている。

第２章にいう「通信データ」というのは、通信に関する内容以外のデータをいうが、具体的には、「トラフィックデータ」「サービス利用データ」「加入者データ」の３種類からなりたっている。

この第２章を構成する条文は、

21 条. 通信データの適法な取得および開示（ Lawful acquisition and disclosure of communications data.）

22 条. 通信データの取得および開示（Obtaining and disclosing communications data.

23 条. 権限および通知の様式および告知（Form and duration of authorisations and notices.）

24 条. 費用支払制度の整備（Arrangements for payments.）

25 条. ２章の解釈（ Interpretation of Chapter II.）

の５条からなりたっている。

３　通信内容の傍受についての規制

（１）「傍受」の概念

　第１章の中核をなす概念は、「傍受」である。第２条（２）に、傍受の定義がある。

　この法の目的のために、本条の以下の規定のもと、

　そして、トラフィックデータの取得に際して、内容が取得されるとしても、それは、傍受にはならないとされている（２条（５))。

（２）送信中の概念

　電子メールのように受信されるために、受信任のサーバにデータが保存されるシステムがある。送信中の受信等を傍受というのであれば、そのような「電子的記憶」にある通信について傍受規定の適用があるかどうかという問題がでてくる。この点については、RIPA 法は、定義を拡張して、読まれる前のデータについて、これを「通信中」であるとした（２

条（７））。もっとも、いつの段階で、この定義の範疇から離れるのかについては、判例に委ねる趣旨のようである。

（３）適法な傍受

適法な傍受についての定めがあり、(a)　電気通信サービスを提供するものにより、もしくは、そのために、(b) そのサービスの規定、運営に関連し、もしくは、そのサービスの利用に関連する法制の執行に関連してなされるときは、権限あるものとなる（３条（３））。また、係るサービスプロバイダについては、刑事免責が存在する（１条（６））。

この点についての具体的な規定は、The Telecommunications (Lawful Business Practice) Regulations[20]ということになる。この規定においては、システムの運営を確保するための通信のモニタリングが適法な傍受であると明確にされている。

また、第三者に聞かせるために送信中に記録すること自体が傍受にあたるのではないかという議論がなされているが、インターネットにおいて第三者に対する開示目的のための記録の法的意義についてなどの議論はなされていないようである。

（４）著作権侵害情報等とのかかわり

英国においてとくに近時議論がされているのは、ＥＵにおける知的財産権行使指令（Directive 2004/48/EC on the enforcement of intellectual property rights）[21]と知的財産権侵害情報との関係である。この指令の７条において、裁判所は、証拠の保全のために中間的差止命令をだすことができ、それは、ISP に対する命令も可能とされている。このような影響のもと[22]、フランスでは、３ストライクと俗にいわれるが、著作権侵害についての２回の警告を受けても、改善がない場合に、アカウントが停止されるという法案が準備されている[23]。また、英国においても、このモデルは、注目をあびている[24]。

４　通信データについての取得および開示の問題

（１）当然なしうる行為

英国においては、通信サービスプロバイダが、トラフィックデータを取得し、それを、

---

20 http://www.opsi.gov.uk/si/si2000/20002699.htm

21 指令本文については、
http://eur-lex.europa.eu/pri/en/oj/dat/2004/l_195/l_19520040602en00160025.pdf
なお、要領よく説明するものとして Will James1, Joel Smith, and Herbert “The IP enforcement directive Is further legislation really necessary to level the playing field? A UK perspective” Computer Law & Security Report vol.20 no.5 2004 がある。

22各国で、ＩＳＰに対して、著作権侵害の通信を遮断することを義務づける判決や、そのような趣旨を含む法律が議論されてきている。具体的には、ベルギーの裁判所は、ＩＳＰに対して著作権の侵害を防止するための技術的手段をとるべきであると判断している[22]。また、デンマークでも同様の判決がだされている[22]。

23「フランス―P2P でダウンロードするユーザーをインターネットから締め出す」
（http://jp.techcrunch.com/archives/if-you-p2p-download-in-france-no-internet-for-you/）

24「英国政府、「違法ダウンロード３回でネット追放」立法を準備中」
（http://jp.techcrunch.com/archives/uk-proposes-three-strikes-and-your-out-illegal-downloading-law/）

みずからのモニタリングと負荷の均衡をたもつために使用し、また、カスタマーサポートサービスのために利用することは、当然と考えられている。このトラフィックデータを利用して、どのようなことをなしうるのかという点については、調査することができなかった。

（２）リアルタイムでの開示の問題

この問題については、不明である。

（３）通信データの記録の問題

民事における発信者情報の開示については、英国においてもきわめて困難な作業であるということがいわれている。Norwich Pharmacal 命令によってなされるが、この命令においては、名誉毀損等の侵害情報を提供しているもののみではなく、その情報の拡大をしているものの電子メール保有者の身元を開示することもなされるといわれる。もっとも、名誉毀損等については、英国法においては、プロバイダ等がみずから公表者と認識されることによって責任が認められる場合がきわめて多い点については、注意する必要がある。

通信データの開示を法執行機関が社会安全の見地から求めることができるかどうかという点についていえば、通信データについては、英国では、きわめて広く認められている。警察，諜報機関，税務当局，その他命令によって特定された機関内部の公務員であって，法律で指定された身分を有する者が所定の手続きと基準にのっとって請求した場合にこれを取得することができるのである。

３　その他の法律

RIPA 以外に注目すべき法律として、反テロ法（Anti-Terrorism, Crime and Security Act 2001）によって定められる通信データの保全規定（第 11 編）や電気通信規定（Telecommunications (Data Protection and Privacy) Regulations 1999）の定めがあることは前述した。

Anti-Terrorism, Crime and Security Act 2001 の１１編においては、通信データの保全についての実務ガイドラインを発行することなどが定められている。

また、電気通信規定（Telecommunications (Data Protection and Privacy) Regulations 1999）は、トラフィックデータのうち、個人データについての保全についての定めをなしている。

これらの規定によってプロバイダの行為規範が定められているが、かかる内容等は、今後の調査課題である。

第５　提言

以上の概観から、以下の提言をなすことができる。

提言

電気通信事業者等のなす活動に関して、我が国で「通信の秘密」が関係する
（ア）通信に関連するデータの記録
発信者情報開示問題・法執行機関に対する情報提供問題（記録）　なお、保全義務
（イ）トラフィックによる問題
帯域制限問題・セキュリティ関心からのネットワーク管理活動（取得・利用・開示）・法執行機関に対する情報提供問題（リアルタイム）
（ウ）通信の内容に関係する問題
有害情報についての伝達制限問題・違法情報についての伝達制限問題
という問題について、世界各国の法的規制および実務について、詳細な研究をなして、それをもとに、我が国の現状と比較することによって、我が国の今後のネットワーク通信に関する法的規制および関係者の行為規範のあり方を早急に検討すべきである。

（１）電気通信事業者等

「通信の秘密」の問題が関係するのは、いわゆる電気通信事業者のみではない。発信者情報開示制度などについては、掲示板管理者なども問題となってくる。検討するのに際しては、そのような問題にまで視点をひろげることがシステムとしての総合的なバランスを検討する際の資料という観点からも望ましいものとなろう。

（２）法的規制および実務

「通信の秘密」が関連する事項は、きわめて実務的な内容であり、また、各国の法執行とのバランス・ＩＳＰ等の活動の実際などが関連してくる内容である。そのために、単に各国の法制度で、条文がこのようにあるという内容のみでは、なんら検討の意味がないものといえる。その意味で、実務の運用とそのためのガイドライン・行為規範等にまで踏み込んだ分析が必要となる。

（３）詳細な研究

我が国では、いわば、「通信の秘密」が、タブーとなっていて、十分な研究がなされていないところである。しかも、それは、昭和４０年代までに比較して、さらに昭和後半などからは、ほとんど研究の対象とされておらず、比較法的な研究というのにいたっては、ほとんど、存在しないものに近い。しかしながら、本稿でみたように、我が国において「通信の秘密」の解釈が拡大化した影響もあって、我が国で「通信の秘密」が関係する問題について各国の問題を比較することは、主要な各国におけるネットワークと社会のあり方を比較することはそのものになるといっても過言ではないであろう。その意味で、詳細な研究をする意義はきわめて高いものということができよう。

（４）法的規制および関係者の行為規範

我が国においては、上記論点については、種々のガイドライン等が公表されてきており、

実務の努力のなかで、妥当な結論と行為規範が求められてきた。それらを比較法的な視点をもとに、再度見直し、さらにガイドラインで対応が不可能なところについては、法改正などにより、対応していくことが必要であろう。特に、国際協調などの視点が必要になるリアルタイムデータや記録の法執行機関への提供などの点については、かかる点からの見直しが必要になる可能性がたかいものといえることになろう。