－ネットワーク管理・調査等の活動と「通信の秘密」－[1]

宇都宮大学講師・弁護士　高橋郁夫
清和大学助教授　吉田一雄

第１章　問題の所在

第１　ネットワーク管理活動や調査活動と「通信の秘密」との関係

１　序

ネットワーク管理、障害検知ならびに対策の検知から、ネットワークに関する種々の情報の収集がなされているのは、いうまでもない。また、それらの事実をもとにネットワークの管理に携わる者たちは、種々の活動をネットワークのなかで行っている。具体的なネットワークにおける種々の活動としては、（１）プロバイダ・大学等におけるインターネットにおけるパケットの収集[2]・分析行為（２）収集分析情報等の共有行為（３）大学等の研究機関におけるいわゆるハニーポット等などを用いた分析行為などをあげることができる。また、（４）として、いわゆる迷惑メールの送信についての分析・廃棄行為などをもこの活動に含めて考えることができよう。

具体的に、それらの行為が、どのような情報をどのような手法を用いて取得・分析・利用しているかということを最初に検討することとする。そして、それらの行為が、「通信の秘密」との関係[3]で、どのように位置づけられるのか、また、その議論がどこまでされているのかという点を後に検討するための準備行為とすることとする。

２　プロバイダ・大学等におけるインターネットにおけるパケットの収集・分析行為

ネットワーク関係者が、ネットワークの通信に関する情報を知得する行為を「ネットワーク観測」ということができる。この代表的な活動として、「サイバーフォース」における観測活動をあげることができる。「サイバーフォ―ス」は、その中で、「検知ネットワークシステム」とは、「全国の警察機関に多数あるインターネットとの接続点に設置された侵入検知装置 IDS を 24 時間オンラインで監視するサイバーフォースの中心となるシステム」である 。警察は、ここから収集された情報を分析することによって、インターネット上で発

---

[1] 本研究をなすにあたっては、小山覚氏（ＮＴＴコミュニケーション株式会社）、甲田博正氏（同）両名からのきわめて多大な教示を得た。ここに感謝の意を記したい。

[2] 情報処理推進機構「高トラフィック観測・分析法に関する技術調査」（http://www.ipa.go.jp/security/fy15/reports/traffic_mon/documents/traffic_mon.pdf）は、かかる収集・分析についての技術的な検討である。

[3] したがって、本稿においては、ネットワーク通信における「通信の秘密」を取り扱うものとなる。信書の秘密等の問題等については直接の考察対象とはしない。

生している様々な攻撃手法などをいち早く発見し、関係各機関への情報提供等に役立てている。また、上記のサイバーフォース以外にも、ＩＰＡの「TALOT」「TALOT2」、JPCERT/CCの定点観測システム「ISDAS」、Telecom-ISAC Japan の観測システムなどがある。

これらのネットワーク観測等の活動は、対外接続装置、高速基幹ルータ、高速スイッチ／ルータなどにおいて、インターフェース、プロトコル、IP／MAC アドレスごとのパケット送受信情報を分析し、また、いわゆるフロー送受信情報を分析したりする。

また、インターネット・サービスプロバイダーにおいては、ネットワークの安定運用のために、トラフィック変動などについてのモニターなどをおこなっている。

そして、これらの活動は、実際にインターネット上の障害が大きくなることの防止にきわめて役立ってきているということができる。その大きな具体例としては、2003 年 8 月に起きたMS-Blaster事件などをあげることができる。このMS-Blaster事件の際には、Blasterの存在を Telecom-ISAC Japan がいち早く認識し、すぐに内閣官房情報セキュリティ対策推進室の緊急対応支援チームとの連絡体制を構築し、関連した省庁間においても協力をなして対応がなされた。各プロバイダも、ネットワークへの影響を技術的に分析し、情報通信事業者へは注意を促すとともに、即座に対策を決定して実施し、被害の拡大を防止することかできたものといえるであろう。また、世界中の 20 台のホストコンピュータからプログラムをダウンロードし、第三者の指令で何らかの動作を行う、約 1.8M バイトもある「Sobig-F」という巨大ワームに対しても、狙われている 20 台のホストコンピュータを解明し、日本のインターネット・サービスプロバイダーも含めた関係者の協力の下で、その 20 台のホストコンピュータを閉鎖して感染を未然に防ぐことができたという事実があった[4]。

３　収集分析情報等の共有行為

また、２のような個別の情報収集行為は、プロバイダなどの間での情報の共有行為を伴って、ネットワークにとって有効な対応策になっていくものであるということができる。

「ワームの挙動を分析して予兆情報を収集するためには、ネットワーク上のトラフィックの異常を常に観測するシステムと国内に複数の分析機関があって、お互いに協力し合うことが必要」といわれ、種々の組織が、そのような情報の分析と共有を行うようになってきている。実際に上記の MS-Blaster 事件や「Sobig-F」事件においても情報の共有がなされたところである。

また、独立行政法人情報通信研究機構（NiCT）では、ISP を中心としてネットワーク上にセキュリティ情報を収集する機器を配備した広域モニタシステムを構築して、ログ情報をセンターで一元管理して分析するセンター構想を進めている。また、Telecom-ISAC と連携してデータの分析をリアルタイムに処理し、分析結果に基いて自動的に対策を実行する

---

[4] KDDI　技術開発本部　情報セキュリティ技術部　部長　中尾　康二氏インタビュー「ネット上のリスクは深刻に、水面下で攻防戦が展開」
（http://nikkeibp.jp/wcs/leaf/CID/onair/jp/comp/363526）

研究にも取り組んでいる。

米国においても同様の観点から、FIDnet 構想、情報システム保護国家計画（National Plan for Information Systems Protection）NCSRS 構想、EWAN 構想などがあり、実際に情報共有の理念が重要であることが強調されている(詳細は、付録 B・2・第 4・3 参照) 。もっとも、実際の共同活動の成果としては、なかなか目に見える成果は上がっていないともいわれているところである。

４　大学等の研究機関におけるいわゆるハニーポット等などを用いた分析行為

ハニーポットとは、「攻撃と侵入を観察するために、脆弱性が、存在している環境からなりたつ（A honeypot consists in an environment where vulnerabilities have been deliberately introduced in order to observe attacks and intrusions.）[5]」と定義される。このような仕組みで、いわば、攻撃者を観察するため、攻撃の阻止、攻撃の検知、攻撃への対処という方法でネットワークを守ろうとするものである。また、このハニーポットの利用は、研究目的にもきわめて有効であるということがいわれている。すなわちセキュリティ専門家は、攻撃側に関する情報やかれらの行動パターンやプロファイルに対して、十分な知識を有していないために、むしろ防御の方法とかに十分な能力を発揮しかなかったのではないかと考えられているのである。そこで、このハニーポットを利用した行為によって、攻撃傾向の分析、新種のツールや手法の特定、攻撃者とそのコミュニティの特定、早期警戒および予測の実施、攻撃者の動機の理解などさまざまな目的に利用することができ、ひいては、情報セキュリティの研究のために貴重な情報を提供することができるであろう。

この点での注目すべきプロジェクトは、ハニーネットプロジェクトである。これは、メーリングリストでの会議を中心として、参加メンバーの各自が、セキュリティに対して上記のような関心からボランティア的に参加するプロジェクトである。その活動成果は、http://www.honeynet.org/index.html でのオンライン刊行物や書籍でもって発表されている。

我が国においては、JPCERT/CC と、Telecom-ISAC Japan が、協力して実施したボットネット実態把握プロジェクトがある[6]。これは、上記 2 団体と ISP とアンチウイルスソフト・ベンダー、マネジメントセキュリティサービスベンダとが協力して、ボットネットの実態を把握しようというプロジェクトであり、そこで、ハニーポットが、利用されている。

そこの調査の結果によれば、収集した検体の８０%が、ボットであり、ハニーポットから DNS に対して、A for A と呼ばれるクエリーが連続して送信されている状況が観測された。また、ボットは、IRC サーバからの通信に応じて、攻撃先などに対して通信をなすよ

---

[5] Honeypot-based Forensics F. Pouget, M. Dacier （http://www.honeynet.org/papers/individual/AusCERT_fullpaper_BIS.pdf)。「無許可で、あるいは、不正に使用されることに価値がある情報システムリソース」とされている。

[6]「国内ユーザーの 40 人に 1 人がボットに感染」――Telecom-ISAC などが調査 (http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20050727/165402/)

うな仕組みが備わっているが、IRC チャンネルを利用して、ダウンロードが頻繁に行われ、IRC チャンネルが変更されたり、ボットネットの構成が変更されたり、スパム送信用のリダイレクトポートが変更されたり、機能が追加されたり、目的に応じたポットネットのチューニングがされたり、などの通信が行われているものと推測されるという観測結果が得られた。

また、大学においても、システムの実装のための技術面からの研究の報告[7]や実際に囮サーバをネットに接続して得たパケットを分析した研究[8]がある。

５ 迷惑メールをめぐるネットワークの管理行為について

一方的に送信される広告宣伝メールを「迷惑メール」というが、そのような迷惑メールは、不快であるばかりでなく、架空請求や児童買春の契機になっていること、携帯電話等で受け取った場合は受信を望んでいないにもかかわらず課金されてしまうこと、電気通信事業者の設備に障害を与えたり、事業に支障をきたしたりすることなどに問題がある。法的には、「特定電子メールの送信の適正化等に関する法律」が制定され、また、平成１７年５月には、「特定電子メールの送信の適正化等に関する法律の一部を改正する法律案」（改正特定電子メール法）が、成立している。ここでは、（１） 特定電子メールの範囲の拡大（２） 架空アドレスあてのメール送信を禁止する範囲の拡大及び罰則の見直し（３） 送信者情報を偽った電子メール送信の禁止及び直罰規定の整備（４） 電気通信事業者による電気通信役務の提供拒否事由の拡大（５） 指定法人による指導・助言等の業務の登録機関による実施への移行などを定めた改正がなされている。また、「迷惑メールへの対応の在り方に関する研究会　最終報告書（案）」[9]においては、法的な対応等に加えて技術的な対応が提唱されている。そ

これらの迷惑メール対策において、電気通信事業者による自主規制（役務の提供の拒否、追放支援プロジェクト、送信者情報の交換）、技術的解決策（送信ドメイン認証技術、新たな技術的解決策、フィルタリングなど）、利用者支援などが検討されている。そして、このような迷惑メールの技術的対策との関係でも、通信の秘密の問題との関連性が指摘されているのである。

第２　ネットワーク管理・調査活動と「通信の秘密」

上記でみたネットワークにおける管理・調査等の活動は、憲法や法律の規定する「通信の秘密」との関係でどのように位置づけられるのか。最初に「通信の秘密」についての一般的な解釈についてこれを眺めることとする。

---

[7] 西尾　裕平「ハニーポットの構築およびデータ分析　Building the Honey-pot system and analyzing the Honey-pot's log」（http://ka-lab.ac/archivements/2002.BT.nishio/paper.pdf）、

[8] 片岡真紀、石下由美子、萬谷暢崇、大橋史治「囮サーバで送受信されたパケット系列を統計分析することによるワーム見地システムの提案」情報処理学会研究報告 2005-CSEC－30（情報処理学会、2005）

[9] http://www.soumu.go.jp/s-news/2005/050617_3.html#f

日本国憲法は、第２１条２項において、「通信の秘密は、これを侵してはならない」と定めている。この規定において、「通信」とは、「郵便・電信・電話などによって意思や情報を伝達することをいう」という[10]と定義されている。そして、その「通信の秘密」の保護する範囲については、「保障の対象となる『すべての形式の通信』は、通信の内容にとどまらないこと当然である。差出人・発信人・受取人・受信人の氏名・住所はもとより、通信配達の日時や、郵便物ないし電信・電話の差し出し個数ないしするなど通信にかかわるすべての事実に及ぶ」とされている。また、一般的な解釈においては、関連する制定法として、電気通信事業法４条・有線電気通信法の定めをあげ、これらは、２１条２項の確認としての意味をもつものとしている。そして、特に通信の秘密と表現の自由との関係の意義付けでは、比較法的にみて、諸外国においては、「通信の秘密」を表現の自由と切り離して規定する例が多いとして、我が国における位置づけを特異なものとするかの如く分析する立場が多数[11]である。

上述の一般的な解釈を前提とするとき、既に紹介した個々のネットワーク管理・調査等の活動が、どのように法的意味づけがなされるかという点について、解釈論的な指針が十分に提供されているかという点については、否定せざるをえないであろう。そして、その懸念は、現在のネットワーク社会化における世界的な議論という観点から検討するとき、より一層、強くなる。わが国において、情報セキュリティを守る関係者の活動について「通信の秘密」の限界とで検討する際に、「通信の秘密」の議論が十分につくされていないところがあるのではないかというのが本稿の基本的な問題意識である。本稿においては、現在の「通信の秘密」をめぐる議論を洗い出し、その議論をもとに、上記ネットワーク管理・調査活動と「通信の秘密」との関係を考察するものとしたい。

---

[10]鈴木秀美「通信の秘密」「憲法の争点（第３版）」所収（有斐閣、1999）。なお、同様のものとして芦部信喜「憲法学Ⅲ　人権各論（１）［増補版］（有斐閣、2000）544 頁。阪本昌成「憲法理論Ⅲ」（成文堂、1995）376 頁、佐藤幸治編著、大学講義双書「憲法Ⅱ」（成文堂）２１９頁は、「遠隔地に存在する特定の発信者と特定または不特定受信者が、特定のチャネルを利用してなすコミュニケーション行為をいう」と定義する。

[11] 鈴木秀美(前出)によれば、「比較法的に眺めてみると、日本国憲法のように表現の自由と通信の秘密が同じ条文で規定されることは異例であり、ドイツ基本法１０条のように、表現の自由および住居の不可侵とは別個の条文として通信の秘密が規定されるか、国際人権規約Ｂ規約１７条のように、私生活や住居の不可侵とならんで通信の秘密が規定されることが多い」とされる。

第２章　従来の判決例・学説等における「通信の秘密」

第１　憲法上の「通信の秘密」をめぐる議論

１　憲法上の「通信」の意義

一般に「通信」の意味について、広義の「通信」（特定人から特定人にあてた意思の表示をいうとする立場）と狭義の「通信」（隔地者間の意思伝達を指すとする立場）があるものとされている。これについて、憲法上の「通信」について、狭義の「通信」すなわち遠隔地にいる発信者・受信者間の意思伝達に限られるのかという問題である。狭義の「通信」に関すると論じる場合には、「通信の秘密」が、媒体を通じて隔地者へと伝わる場合に特定して、かかる媒体での伝達という特性に着目して規定したものだとされることになる。また、この「通信」についていえば、明治憲法の「信書の秘密」（２６条）との解釈の連続性という問題も含まれることになる。

一般に「通信」の意味について、隔地のものに限られるかという点が判決例において論じられたということはないものと思われる。もっとも「表現の自由」という観点からするとき、という事例において抽象論として「郵便法の右の諸規定は、通信の秘密を侵してはならないという憲法二一条の要求に基いて設けられており、憲法は思想の自由や、言論、出版等の表現の自由を保障するとともに、その一環として通信の秘密を保護し、もつて私生活の自由を保障しようとしているのである。」と論じているもの[12]がある。

学説的には、広義の「通信」（特定人から特定人にあてた意思の表示をいうとする立場）と解し、個人間の会話も保護の対象であるとするものとして、奥平康弘・川添利幸・丸山健編「テキストブック憲法」127 頁「個人間の会話も通信の一態様として、その秘密が守られなければならない」（有斐閣、1977）があげられる[13]。

これに対して、狭義の「通信」（隔地者間の意思伝達を指すとする立場）を明言するものとしては、水木惣太郎「憲法講義　上巻」387 頁「通信とは隔地者間の意思伝達であり、間接的表現の１形態である」（有信堂、1956）や阪本昌成「憲法理論Ⅲ」376 頁「遠隔地に存在する特定の発信者と特定または不特定受信者が、特定のチャネルを利用してなすコミュニケーション行為をいう」（成文堂、1995）（この見解からは、「この規定は、情報伝達に関する空間的障害を除去しようとする特性に着目した、表現の下位概念である」

---

[12]大阪高判昭和 41 年 2 月 26 日（判タ 191 号 155 頁）、なお、この判決の詳細については、後述する。

[13] また、定義において広義に従うが、個人間の会話を包含しているのか、明らかではない記述としては、渡邊宗太郎「日本国憲法」103 頁（有斐閣、1948）（但し、手段としては、封書端書以外に電信電話をあげるのみである）、野中俊彦・浦部法穂「憲法の解釈Ⅱ」116 頁（三省堂、1990）、小島和司・大石眞「憲法概観（第６版）」121 頁（「通信」とは個人の内的な意思伝達を可能にするあらゆる方法をいうとする）（有斐閣、2001）などがあげられる。

と説明される[14]こともある。）がある。この立場を前提として会話当事者間の保護に関して、田上穣治「憲法要説」136 頁は「日常の会話の盗聴は、通信の秘密の保障に含まれないから、私生活に対する干渉として警察権の限界を超えない範囲では、違法ではなく、いわんや、特別な令状を要しない」（白桃書房、1958）としている。

また、明治憲法の「信書の秘密」（２６条）との解釈の連続性という問題について、一般の教科書においては、「明治憲法の「信書ノ秘密」とあったのと同じく、手紙・ハガキ・電話・電報そのほかすべての方法による通信の秘密を意味する」とする[15]ものが一般である。

２　通信内容とトラフィック・データの種別

米国においては、法執行機関との関係において法執行機関が求める情報が、「基本加入者、セッションおよび請求情報」か、「他の取引およびアカウント記録」か、「アクセスされた通信」か、「検索されていない通信」かという観点から、法執行機関に必要とされる法的手続きについて詳細に検討されている。一方、サイバー犯罪条約においては、「トラフィックデータ（通信記録）」[16]（なお、以下、トラフィック・データという）、「加入者情報」[17]についても定義がなされている。

---

[14]阪本昌成、佐藤幸治編著「大学講義双書　憲法Ⅱ　基本的的人権」219 頁（成文堂、1988）

[15] 宮澤俊義・芦部信喜「全訂日本国憲法」250 頁（日本評論社、1978）。美濃部達吉・宮澤俊義増補「新憲法逐条解説」81 頁（日本評論新社、1957）は、「旧憲法には、「信書」とあったのを「通信」と改め、電信・電話を包含する趣旨を示している」という。また、佐藤幸治、芦部信喜編「憲法Ⅱ　人権（１）」640 頁（有斐閣、1978）は、「明治憲法２６条の定める「信書ノ秘密」について通説は最広義に解していたのであって、日本国憲法はそのことを文字の上で明らかにしたといえる」とする。また、佐藤幸治は、同書において「日本国憲法による通信の秘密の無条件的保障の意義は、かかる歴史的背景において評価されなければならない。」という。

[16]一般にトラフィック・データ(「通信記録」と訳されている)については、「通信記録とは、「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」と定義されている(サイバー犯罪条約 1 条)(なお、翻訳は、http://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4a.pdf による。以下同じ)。

なお、通信記録というが、記録されていないデータであっても、通信に関するデータは、トラフィック・データとされるので、通信記録という訳語は、誤解をまねきやすい。特にリアルタイムでのモニタリングが問題となるネットワークにおいて、「記録」という用語は、使用をさけるべきと思われる。本文では、上記訳文による以外のときは、トラフィック・データとしている。

[17] 「サービス・プロバイダーによって保有されるサービス加入者に関連する情報のうち、通信記録及び通信内容以外のコンピュータ・データその他の情報であって、それにより次のことが立証されるものをいう。　ａ　使用された通信サービスの種類、そのために使用された技術的設備及びサービスの期間　ｂ　加入者の特定、郵便上の又は地理的な住所、電話番号その他のアクセスのための番号並びに請求及び支払に関する情報であって、サービス契約又は取決めに基づいて利用可能なもの　ｃ　通信機器の設置場所に関するその他の情報であって、サービス契約又は取決めに基づいて利用可能なもの。」

しかしながら、我が国においては、この峻別という考え方は、一般的なものではない。具体的にいうと、「保証の範囲は、通信のすべての構成要素におよび、通信の内容のみならず、通信の存在それじたいに関する事柄－差出人（発信人）・受取人（受信人）の氏名・住所、差出（通話・発信）個数、通信の日時、電話等の発信場所、など－についてもその秘密が保証されなければならない」と説かれるのが一般である。

論者は、この立場の行政上の解釈根拠として内閣法制局意見昭和 38 年 12 月８日（「電話の発信場所は、発信者がこれらを秘匿にしたいと欲する場合がありうるから、右の２項（現行の電気通信事業法第４条２項）にいう『他人の秘密』に該当するものと解すべきであろう」をあげる。また、大阪高判・昭和 41 年 2 月 26 日（判タ 191 号 155 頁）が、その解釈の根拠として紹介される[18]。

通信の構成要素すべてが通信の秘密として保護されていると解する立場は、学説ではよりはっきりしている。そのようなものを代表する見解として佐藤功・ポケット注釈全書「憲法（上）」（新版）382 頁の「通信の秘密の内容が信書等の内容たる通信文であることはいうまでもないが、なおその発送元や宛先をも含む。けだしこれらの事実からその内容が探知されることが可能であり、またそれらによって思想表現の自由が抑圧されるこが考えられるからである」、「表現の自由の一環としてとらえる場合には、秘密の範囲は手紙などの内容に限られるが、これに反して通信の秘密の根拠をプライバシーの保護に置く場合には、手紙などの内容に限らず宛名（受信人）・差出人（発信人）の氏名・差出個数・年月日なども発信人・受信人が秘密に欲する場合がある以上、『通信の秘密』の内容をなし、郵便法９

---

18 この事件は、郵便局の事務員として郵便物の集配の事務に従事していた公務員が、電報電話局より郵便局に差し出されていた「電話架設のご案内」と表面に印刷してある郵便物について、その名宛人の住所、氏名、電話番号を紙片に書き写し、第三者らに交付した事件について、「信書の秘密」および公務員法上の１００条１項の「職務上知ることのできた秘密」を漏らしたものであるかどうかが、議論された事案である。そして、この事案について裁判所は、「そもそも郵便物の委託者は郵便官署を信頼してその秘密を託するものであり、開封の信書や葉書であつても委託者が秘密にすることを欲する場合のあること、そして少なくとも委託者はその郵便物の内容を積極的に他人に公開する意思のないこと、郵便物の発送元や宛先といえども、それが知られることによつて思想表現の自由が抑圧される虞のあることを考えると同法上の信書には封緘した書状のほか開封の書状、葉書も含まれ、秘密には、これらの信書の内容のほか、その発信人や宛先の住所、氏名等も含まれると解すべきである。」としているのである。
この事案は、事実としては、積極的に知得している点に特徴がある。すなわち、その公務員について配達中にたまたま電話架設案内の本件書状をみて、その宛先等を知つたというのではなく、郵便局において、電報電話局から一括して差し出された電話架設案内の書状を発見するや、これを局外に持ち出して、その宛先の住所、氏名のほか、書状の中に記載されている電話番号を封筒の隙間から覗き見して書き取ったという行為なのである。したがって、自己の適法な業務活動のなかで得た事実を、任意でそれを提出することが、「通信の秘密」を侵害するかという点について裁判所の判断ではないということは注目する必要がある。また、電信に関する書類の提出については、刑事訴訟法第１００条、１２５条、２１８条および２２０条の規定に基づく請求の場合に限り、これに応ずることという趣旨の内部規定がある。

条にいう『信書の秘密』として、郵便業務に従事する者の『郵便物に関して知り得た・・・秘密』（郵便法９条２項）に含まれると解することなる（前掲大阪高判も同旨）。すなわち通信の事実（誰が誰に通信したかの事実）そのものもプライバシーに属し、秘密として保護されるのである（この意味では宛名・差出人の氏名も通信の内容をなすといってもよい）。」（有斐閣、1985）をあげることができる[19]。

もっとも、サイバー刑事法研究会報告書「欧州評議会サイバー犯罪条約と我が国の対応について」[20]によれば、サイバー犯罪条約に対する対応を考えるさいに、トラフィック・データか否かということが、法的な扱いに相違をきたす可能性があるのではないかということがいわれている。

３　通信の秘密の時間的な守備範囲（いつからが「通信の秘密」として保護されるのか、また、通信の秘密はいつまで保護されるのか ）

わが国において、例えば、「信書」の秘密が、「通信の秘密」として、保護されるとして、(ア)その保護が、「信書」の形態をとったときから発生し、また、信書の形態であれば、受信人において受け取られ、開封されたあとも「通信の秘密」として保護されるという立場と(イ)「通信の秘密」は、送信者・受信者以外の第三者にその信書が託されているときのみの保護であるので、信書であっても、第三者の取り扱いになっていなければ、通信の秘密

---

[19]憲法制定後、まもない段階においても柳澤義男・「日本国憲法逐条講義」80 頁「それは、単にその内容ばかりでなく、何人から何人に向けて、いかなる通信がなされたかといふやうなことを、他人に知らすこともできない、といふ意味である」（福地書房、1947）、大石義雄「憲法」174 頁「独り、意思の表示の内容を知ることだけではなく、何人がなした通信であるとか、又何人に対してなす通信であるかなどを知ろうとすることも、通信の秘密の侵害である」（勁草書房、1950）、水木惣太郎「憲法講義　上巻」387 頁「又表書、宛名、時日その他の事柄も、通信の内容と関連することがあり、且つ公開の意思を有しないのであるから、その秘密は保護されるべきである。このことは他の通信の秘密についてもいうことができる」（有信堂、1956）と指摘されている。その後も、奥平康弘・川添利幸・丸山健「テキストブック憲法」127 頁「通信の内容だけではなく、その発信人・受信人の住所・氏名、発信・受信地、発信・受信時間などもプライバシーに属することであるから、その秘密が保障されなければならない」（有斐閣、1977）とされ、また、現時点においても芦部信喜「憲法学Ⅲ　人権各論（１）［増補版］」544 頁「通信の秘密の保障の主要な目的が私生活の秘密（自由）にあるとすれば、保障の対象となる「すべての形式の通信」は、通信の内容にとどまらないこと当然である。差出人・発信人・受取人・受信人の氏名・住所はもとより、通信・配達の日時や、郵便物ないし電信・電話の差出個数ないし使用回数など、通信にかかわるすべての事実に及ぶ」（有斐閣、2000）とされている。

この点について、佐藤幸治は、「『差出人がその住所や名前を秘密にしようとすれば、架空の住所や仮名を用いることができるのであり、そういうことをしないで住所、氏名が書いてある郵便物は、住所氏名を秘密にする意志がないものと推定してもおおきな誤りではあるまい』とする見解もあるが、憲法の『通信の秘密』を上述のように解し、かつ法律は可能な限り憲法的価値を充填して解釈されるべきであるとすれば、支持できない見解といわなければならない」（前述 642 頁）とする。

http://www.meti.go.jp/kohosys/press/0002626/1/020418cyber.pdf

[20] http://www.meti.go.jp/kohosys/press/0002626/1/020418cyber.pdf

この点については同報告書 42 頁、45 頁、57 頁。

の保護は及ばないし、いったん受領され、開封されたあとは、通信の秘密の保護はおよばないという立場がある[21]。

このように論点を抽出した場合に、これらの点について、明確に意識している書物は少ないといえる。

前者の立場を明確に意識して論じるものとしては、大石義雄[22]「憲法」174 頁「この通信には、意思の表示者がいまだ相手方に送られないでいるものも、すでに相手方が受け取ってみてしまったものも、すべて含まれる。したがって、例えば、受け取った人がすでに開封して内容をしった後の手紙でも、国家が勝手にその内容を知ろうとしたりすることは通信の秘密の侵害である」（勁草書房、1950）がある。この立場からは、刑事訴訟法１００条の規定は、この憲法上の保障に対する例外とされることになる。また、電子メール等の場合についていえば、「電気通信事業者の取り扱い中に係る」通信の秘密保護は、電気通信事業者が提供するコンピュータ・サービスも事業者の取り扱い中にかかるものであるから、コンピュータに貯蔵・保管された情報にも及ぶと解する立場ということになろう。

後者の立場を前提としているものと考えられるものとして、田上譲治・「日本国憲法原論」130 頁「通信の内容を公権力によって調査しまたは発表することは、発信人または名宛人の占有するものについては予め捜索・差押え等を必要とするから、これによって人権が保障される（憲法２９条・３５条)。したがって通信の秘密が特別に保障されるのは、通信官署の取扱いにかかる通信の場合である」（青林書院新社、1980）がある[23]。電子メール等の場

---

21 この論点も、米国法における電子メールに対する捜索・押収が、読まれた電子メールと読まれる前の電子メールとで、その保護の必要性について、レベルが異なるのではないか、という問題に対応するものである。従来の議論においては、通信の秘密の保護は、特別に、通信官署の取り扱いにかかる場合のみ（それ以外については、憲法３５条によって保護される）に適用されるのか、それとも、発送前のものも発送後のもの、名宛人が受け取った後のものも通信の秘密として保護されるのかという問題がある。名宛人が読んだ後に、その名宛人が、通信について明らかにすることを求められたときにどのように考えるのかということになろう。また、この論点は、通信の秘密に関する規定と憲法３５条との関係は、どのようなものかという問題点をも、指摘することになる。この点については、憲法３５条の妥当領域が、有体物に限られるという立場と郵便物と同様に通信にも憲法３５条が適用されると解される立場とがある。
前述の司法省マニュアルの観点からすれば、電気通信事業者のもとに蓄積された通信について、通信が受信人のもとに到達してしまった後なおも通信の秘密として保護されるのかという問題である。この点については、電気的記録が１８０日をすぎるかどうかという観点も米国では制定法として加味されている。

22 大石義雄「日本國憲法逐條講義」109 頁「発送前のものも、発送後のもの、すなわち宛名人が受け取った後のものでも、すべて侵されてはならない通信の秘密である」（有信堂、1953）ともいう。

23 同趣旨の記述として、佐藤功「日本国憲法」（全訂第５版）226 頁「ただし、刑事手続上は、通信の秘密の保障は、逓信官署に託された通信について、これに私人の所持する文書と同様の保護を与えようとするものであるから、犯罪捜査の目的のためには、私人の所持品についてと同じく、憲法３５条の定める手続よれば、差押え、押収することができる。」とする（学陽書房、1996)。また、阪本昌成・大学講義双書「憲法Ⅱ　基本的人権」221 頁

合について、受信人が読んだ後の場合について、貯蔵・保管された情報は通信が修了した後コンピュータに保管されたもので通信そのものではなく、通信サービィスの提供業務とはいえないので、「電気通信事業者の取り扱い中に係る」通信の秘密保護は及ばないと解することになろう。この立場から安富潔「刑事手続とコンピュータ犯罪」201 頁は「貯蔵・保管された情報は、通信の結果たる情報である。したがって、事業者が提供する通信システムと結合したコンピュータに貯蔵・保管された情報の秘密を『電気通信事業者の取り扱い中に係る』通信の秘密保護に違反する侵害と見ることはできないように考える。」としている（慶應義塾大学出版会、1992）。また、井上正仁「捜査手段としての通信・会話の傍受」125 頁は、電子メールについて「受信者が読んだ上、保存ファイルに移されたものについては、受信者が受け取った郵便物を貸し金庫に預けたのに似たようなところもあるため、そもそも、『通信』としての特別の保護がなお及ぶものといえるか、疑問とする余地がある。それが及ばないとすれば、受信人の手元にある郵便物を対象にするのと基本的に異ならないから、通常の捜索・差押や検証の手続きによることが可能で、またそれで足りる、といえよう。」としており（有斐閣、1997）、かかる後者の立場を前提にするものと思われる。

4　プロバイダに対する憲法規定の適用の可能性

ネットワーク社会における通信の秘密を検討するにあたっては、憲法上の通信の秘密規定が、郵便局など政府の組織と考えられる組織についてのみ妥当するという見解と民間の通信事業者にも及ぶという見解との双方の見解が存在する。ネットワーク社会において、いわゆるプロバイダが占める役割はきわめて大きいものがあるがその位置づけが憲法上の通信の秘密との関係でどうなるかというのも興味深いところである。

この点について興味深いのは、「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」の報告書[24]である。この報告書においては、「一般的には、発信者の氏名、住所等の発信者情報についても『通信の秘密』に含まれるとされているため、この問題を検討する上では、まず、『通信の秘密』を保護した現行の法規定との関係を整理する必要がある。」とした上で、憲法上の「通信の秘密」との関係について、「基本的には、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考えられている。電気通信自由化以前については、電電公社、国際電信電話株式会社には憲法の規定が適用されていたとも考えられるが、電気通信が自由化された現在では、電気通信分野における競争の進展状況、インターネットの登場等の電気通信の多様化の進展状況にかんがみれば、憲法上の『通信の秘密』は私人である電気通信事業者等へは直接的な適用はなく、電気通信事業法等で保護されているものと考えられる。」とされている（同報告書・第４章・２（１））。

は、「通信の自由」という概念を導入した上で、「憲法２１条にいう通信の自由とは、国民にとってもっとも有効な通信手段を確保するために、通信のうち一定種を一種のコモン・キャリア（中略）として法定し、その業務従事者を国民が利用する際の各種の自由を意味するものと解すべきである」（成文堂、1988）とする。

[24] http://www.soumu.go.jp/joho_tsusin/pressrelease/japanese/tsusin/990201j501_01.html

学説的にも、阪本昌成「憲法理論Ⅲ」143 頁は、旧公衆電気通信法の規定の位置づけについての議論をあげて、通説的な立場は、「現在[25]でも、電気通信事業法上の規定につき、同様に解されているようである」とし、それに対して、「国家の監督に服する私人の行為であればステイト・アクションとなるわけではなく（略）、ＫＤＤの示す『独占・公益性』は私企業としての特徴を指すだけであり、市民が利用を強制されていると、比喩以上のものではないからである」として、「この点は、２１条２項後段が、一定種の情報伝達媒体をコミュニケイション・コモン・キャリアとして法定するよう要求したことの帰結である」（成文堂、1995）としている。また、現在の状況を念頭にして、松井茂記「インターネットの憲法学」295 頁は、「通信事業の持つ公共的性格を考慮すると、これに憲法の通信の秘密保護規定を直接適用する考え方には、一理あるが、現在のように電気通信分野が民営化された状況では、やはり電気通信事業者を政府の一部と考えることは困難であり、憲法の通信の秘密規定はそのままでは適用されないと考えるべきであろう。それゆえ電気通信事業者であるプロバイダーが送信者情報を開示することは憲法違反とはいえない」としている（岩波書店、2002）。

第２　制定法における「通信の秘密」をめぐる若干の考察

１　電気通信事業法・有線電気通信法の規定

「電気通信事業法」は、その第４条で、（秘密の保護）として、第１項では、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」と定め、また、第２項では、「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。」と定めている。また、第 104 条においては、「電気通信事業者の取扱中に係る通信（第九十条第二項に規定する通信を含む。）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。」として刑事罰が定められている。そして「電気通信事業に従事する者が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する」とされているところである。

電気通信事業法４条は、憲法２１条２項の規定を受けて、電気通信事業者の取扱いにかかる通信の秘密を規定したものであるとされる。電気通信法制研究会「逐条解説　電気通信事業法」（以下、「逐条解説電気通信事業法」という）[26]によると、「通信の秘密を保護する趣旨は個人の私生活の自由を保護し個人生活の安寧を保証する（プライバシーの保護）とともに、通信が人間の社会生活にとって必要不可欠なコミュニケーションの手段であることから、憲法第２１条２項の規定を受けて思想表現の自由の保障を実効あらしめることにある。そして自由闊達な通信がなされることを保証するための規定である」とされている。そして、電気通信事業者の取扱中にかかる通信については、いったん通信当事者の手から離れ、事業者に託されたものであるから、通信当事者が秘密を保護するための自衛措

[25] 1995 年当時をいう
[26] 電気通信法制研究会「逐条解説　電気通信事業法」（第一法規、1987）

置を講ずる余地がなく、また、秘密が侵害される危険にさらされやすいことにかんがみ、電気通信事業に対する利用者の信頼を保護するため、その秘密を侵すことを禁止しているのであるとされている。

また、有線による電気通信についても、有線電気通信法９条において（有線電気通信の秘密の保護）「有線電気通信（電気通信事業法第４条第１項又は第 164 条第２項の通信たるものを除く。）の秘密は、侵してはならない。」とされ、同１４条１項が、「第９条の規定に違反して有線電気通信の秘密を侵した者は、２年以下の懲役又は 50 万円以下の罰金に処する。」とされている。

２　「通信の秘密」の概念と「他人の秘密」

「逐条解説電気通信事業法」によれば、ここでいう、「通信の秘密」の範囲は、通信内容にとどまらず、通信当事者の住所、氏名、発信場所と通信の構成要素や通信回数との通信の存在の自立なども含むものであると解されている。これらの事実は、通信の構成要素であるとされるが、これらは、「それによって通信の内容を探知される可能性があるし、また、通信の存在の事実を通じて個人の私生活の秘密（プライバシー）が探知される可能性がある」からである。このように、通信の秘密には、通信の内容たる事実に係るものと通信の外形的な事実に係るものとがあるが、ここでは両者を保護するものである、とされている。

また、電気通信事業法においては「知り得た他人の秘密」の第三者への漏洩・窃用も禁止されている（同条２項）。ここでいう「知り得た他人の秘密」は、「通信の内容、通信の構成要素、通信の存在の事実等『通信の秘密』のほか、通信当事者の人相、言葉の訛りやプッシュホンに記憶された相手番号等直接の通信の構成要素とはいえないが、それを推知させうるものを含む」と解釈されている（「逐条解説電気通信事業法」25 頁）。

もっとも、「通信の内容」の保護たる「通信の秘密」について、通信の内容についての保護とそれ以外の「知り得た他人の秘密」の保護に外延的情報の保護を含むという解釈も成り立ち得えるのではないかということも考えられる。しかしながら、具体的な検討をなしている見解[27]は、見当たらない。

---

[27] 現行郵便法の立案当局者は、差出人・受取人の氏名・住所等は、１項の「信書の秘密」ではなくて、２項の「他人の秘密」に該当すると解していたように見受けられるとされている（佐藤幸治、芦部編「憲法Ⅱ　人権（１）」642 頁）。そして、昭和 28 年 1 月 30 日内閣法制局意見は「郵便物の差出人又は受取人の居所、氏名及び差出個数等は、もとより通信の意味内容をなすものではないけれども、通信そのものの構成要素であり、実質的に見ても、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こともあり得るのであるから、これらの事項が通常郵便法第９条による『他人の秘密』に包含されることについては大なる疑問はないといってよかろう。」という。また、昭和 38 年 12 月 9 日内閣法制局意見は、その理由のところで、公衆電気通信法第５条１項を引くと共に第５条２項に触れ、その上で、第２項についての「他人の秘密」侵害の該当性を認定しており、むしろ第１条への該当性を否定しているようにもとれると読めるところである（後述・第２章・第１・４（ア）参照）。これらの見解をとるとき、むしろ、通信の内容の保護のみが郵便法や公衆電気通信法の第１項の「通信の秘密」の射程であるというのが、これらの見解

3 憲法の規定と制定法上の規定との関係

これは、米国における第４修正と制定法の関係をみたときに、明らかになることである(後述)。わが国でも、憲法２１条２項の規定と郵便法や電気通信事業法などの制定法について、憲法の規定における通信の秘密と内容自体が、異なっているのかという問題である。これは、例えば、サイバー犯罪条約などに対応して、対象となる情報の格付けに対応して法的規制を考えるときに、憲法違反の問題が発生するのではないかという議論にも対応するところである。従来の議論からすると、制定法は、一般に憲法上の「通信の秘密」の規定を確認する趣旨の規定であるとすることが多いが、そのような解釈の妥当性について考えてみるべきではないのかという問題になってくるのである。

しかしながら、憲法の規定と制定法の規定との守備範囲が異なるのではないかという見解は、なかなか存在しない。通常の見解を引くとき、佐藤功・ポケット註釈全書「憲法」159 頁は、「『通信の秘密』にはいわゆる『逓信の秘密』（ワイマール憲法１１７・ボン憲法１０参照）も含まれる。すなわち信書・電信・電話の従業員が職務上知り得た秘密を漏らすことも禁止される。郵便法９条２項が、郵便従業員は郵便物に関して知り得た秘密を守らなければならないとしていること（同法５４条のように、還付不能の信書を開披することは業務上当然ゆるされた行為であるが、そこで知り得た秘密を漏らしてはならない）は従って憲法上の要求に基くと解する」（有斐閣、1955）とし、野中俊彦＋浦部法穂「解釈シリーズ　憲法の解釈Ⅱ　人権」（三省堂・1990）117 頁は、通信の秘密が積極的知得行為の禁止と漏洩行為の禁止の二つの意味があり、「これらのことは、制定法上も、郵便法・電気通信事業法において規定されている」としている。また、芦部信喜・「憲法学Ⅲ　人権各論（１）［増補版］」546 頁には、「通信の秘密保障を具体化した現行法規」（有斐閣、2000）という記述があるし、阪本昌成「憲法理論Ⅲ」143 頁にも、「通信業務提供者に漏洩・窃用を禁止する法令上の条規は、２１条２項後段の確認としての意味をもつ」（成文堂、1995）（但し、これは、後述の論点についての記述）という記述がある。

4 保障の内容とその限界について

そして、「通信の秘密」の内容として、一般には「通信」の「秘密」にかかる事実を「通信当事者以外の第３者が積極的意思をもって知得してはならず」「第３者にとどまっている秘密をそのものが漏洩（他人が知りうる状態にしておくこと）することおよび窃用（本人の意思に反して事故または他人の利益のために用いること）してはならない」の２つに分けてとらえられることになる。

これらの内容についての一般的な解釈問題については、本研究の範囲ではないが、以下の論点は、ネットワーク観測行為を考えるときにも示唆に富むものがある。そのような論点としては、（ア）電気通信事業者において、片側当事者の同意がある場合において、電話の発信場所を探索し、これを他人に知得させる行為の許容性（イ）事業者みずからが、

の当然の前提ではないのかと考えられるところである。

通信の片側当事者として通信の外延情報、内容を知得することの許容性（ウ）電気通信事業者が、通信の外延情報を記録することの許容性、通信の外延情報・内容の利用の許容性（エ）捜査関係事項照会に対して回答の許容性やその他の情報の開示の許容性などがあげられる。これらについて、何らかの立場から、「通信の秘密」との関係について、現時点においてなんらかの記述がなされているものとしては、以下のことがあげられる。

（ア）逆探知問題

電気通信事業者において、片側当事者の同意がある場合において、電話の発信場所を探索し、これを他人に知得させる行為が違法になるのかというのが、いわゆる逆探知の問題である。これについては、昭和38年12月9日内閣法制局意見は、「電話を利用して刑法２２２条に規定する脅迫の罪を現に侵している者がある場合に、被害者の要請によって（略）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になるか」という質問に対して「公衆電気通信法第５条は、第１項において、『公社・・の取扱い中にかかる通信の秘密は、侵してはならない。』と規定するとともに、第２項において、『公衆電気通信業務に従事するものは、在職中公社・・・の取扱い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。この職を退いた後においても同様とする。』と規定している。電話の発信場所は、発信者がこれを秘匿したいと欲する場合がありうるから、右の第２項にいう『他人の秘密』に該当するものと解すべきであろう。」「被害者の要請があるときは、公社の職員が当該電話の発信場所を探索し、これを捜査官憲に通報することは、許されるものと解すべきである。その理由を要約していえば、右の探索および通報は、脅迫の罪の現行犯人の逮捕に協力するために行われるものだからである。」としている。また、学説でも阪本昌成「電気通信事業者は、電気通信が犯罪に利用されたことを理由に、電話の発信場所を探索し、これを他人に知得させるとすれば、通信の秘密を侵害することになる（探索行為は、電通法３条違反であり、他人に知らせる行為は『電気通信事業者の取扱中にかかる通信の秘密は、侵してはならない』と定める４条１項違反となる）」「憲法理論Ⅲ」（成文堂､1995）と明言するところである。

（イ）「取扱中にかかる」の限界

また、「取扱中にかかる」という用語は、抽象的には、「電気通信事業者が管理・支配している通信」ということを意味する。では、逆に通信を行う各端末が、行う端末における通信に関する情報の取得が、この関係でどのように扱われるかという問題がある。この点については、上記の昭和38年12月9日内閣法制局意見は、「捜査官憲が、電話による通信の一方の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遺話を録音することは、公衆電気通信法第五条第一項に違反しないか」という質問に対して「電話による通話の一方の当事者甲がその利用する電話の端末の設備において聴取しうる他方の当事者乙の通話の内容は、甲の支配の下に置かれた事項であつて、法第五条第一項にいう『公社……の取扱中に係る通信の秘密』の範囲外にある事項である。したが

つて、甲が、その利用する電話の端末の設備において、乙の通話の内容をみずから録音することはもちろん、第三者に録音させることもまた、法第五条第一項の規定に違反することにはならないものと思われる。」という回答をしている。

(ウ)正当業務行為について

「電気通信事業における個人情報保護に関するガイドライン」[28]によれば、通信履歴を「記録することも通信の秘密の侵害に該当し得るが、課金、料金請求、苦情対応、自己の管理するシステムの安全性の確保その他の業務の遂行上必要な場合には正当業務行為として少なくとも違法性が阻却されると考えられる。」とされている。また、上記ガイドライン解説の(3)においては、発信者を探知するための通信履歴の解析は、目的外利用であるばかりでなく通信の秘密の侵害となると解されること、違法・有害情報掲載時に、その発信者に警告を行わないと自己のサービス提供に支障を生じる場合（自己のサービスドメインからの通信がアクセス制限される場合等）に、自己が保有する通信履歴などから発信者を探知することは、正当業務行為として行うことができることが触れられている。同じく、解説の(4)においては、通信履歴は、裁判官の発付した令状に従う場合等、違法性阻却事由がある場合を除き、外部提供は行わないこととされていること、大量の無差別のダイレクト・メールが送りつけられ、自社のネットワークやサービスが脅威にさらされており、自己又は他人の権利を防衛するため必要やむを得ないと認められる場合には、発信元の電気通信事業者に通信履歴（発信者のＩＰアドレス及びタイム・スタンプ等）を提供することは許されると考えられることなどが触れられている。

（エ）捜査関係事項照会に対して

この点については、「電気通信事業分野におけるプライバシー情報に関する懇談会」中間報告書および上記「電気通信事業における個人情報保護に関するガイドライン」において検討がなされている。このガイドラインの第２３条によれば、電気通信事業者は、通信履歴については、「課金、料金請求、苦情対応、不正利用の防止その他の業務の遂行上必要な場合に限り、記録することができる」（第１項）とされ、第２項においては、「電気通信事業者は、利用者の同意がある場合、裁判官の発付した令状に従う場合、正当防衛又は緊急避難に該当する場合その他の違法性阻却事由がある場合を除いては、通信履歴を他人に提供しないものとする。」とされている。ここにいう、通信履歴とは、「利用者が電気通信を利用した日時、当該通信の相手方その他の利用者の通信に係る情報であって通信内容以外のもの」をいうとされている。また、通信履歴は、通信の構成要素であり、電気通信事業法第４条第１項の通信の秘密として保護されるとされている。この部分は、逆に捜査関係事項照会に対して、開示してはならないことを明らかにしたものとされる。

学説的にも、捜査関係事項照会に対して、「郵便官署や電気通信事業者が通信に関する事

---

[28] http://www.soumu.go.jp/joho_tsusin/d_syohi/privacy_studygroup_interimreport_chap2_sec2.html#1

項を報告することは許されないと解すべきである」とされる[29]。

(オ)その余の開示について

電気通信事業法等との関係については、いわゆる発信者情報開示の問題において、プロバイダ責任制限法の制定以前において「電気通信事業法第４条及び有線電気通信法第９条において、電気通信事業者等に対し「通信の秘密」保護の義務が課されているところであるが、発信者情報の保護がほかの法益と抵触する場合にも絶対的に保護されるべきとは考えられない。他人の権利利益を侵害する通信については保護されない場合があると考えられ、こうした場合は、電気通信事業者等が発信者情報を開示しても、社会的相当行為として刑法第３５条により違法性が阻却され、「通信の秘密」保護義務違反による刑罰に問われないと考えられる。」という報告がなされていたところである（前出、「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」第４章・２（２））。

そして、「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－逐条解説－」において、「発信者情報は、発信者のプライバシー及び匿名表現の自由、場合によっては通信の秘密として保護されるべき情報であるから、正当な理由もないのに発信者の意に反して情報の開示がなされることがあってはならないことは当然である。」という記述がなされている。

第３　ネットワーク管理・調査活動と「通信の秘密」の現在の解釈

１　「通信の秘密」侵害行為とネットワーク管理・調査活動の具体的当てはめ

電気通信事業者においてネットワーク管理をなす場合においては、電気通信事業法上で問題になるのは、（１）「通信の秘密」に対する積極的知得行為の禁止・第三者への漏洩・窃用（２）「知り得た他人の秘密」の第三者への漏洩・窃用ということになる。

２　ネットワーク管理・調査活動における通信の消極的了知行為の限界

ネットワークにおいて、電気通信を発信人から受信人に届けるにあたって、そのために、しらなければならない通信の外形的事項を知ることは、これは当然のことである。むしろ、発信人から、この情報をもとに届けるように受託されるのであり、この受託業務に際して委託される事項とその業務の履行にあたって発生する情報については、電気通信事業者は、消極的に了知するのである。「電気通信事業に従事する者は、その業務の取扱い上、通信の内容、通信当事者、通信年月日、通信の発信地および受信地など通信の秘密を容易に知りうる地位にあることはから、その業務の取扱い上、必要な限度において、通信の秘密を知ることは、第１項の規定に違反しない」（「逐条解説　電気通信事業法」）ということは、これをいっていることになる。が、「それを第三者に漏洩したり、窃用したりすることは第１項の規定にも違反することになる。」

では、この業務の取扱い上、必要な限度において知ることになる行為（消極的了知行為）

---

[29] 樋口・佐藤・中村・浦部編（浦部著）「注解法律学全集２　憲法Ⅱ」（青林書院、1997）85 頁、86 頁

の限界はどこかという問題があるものと思われる。その限界の一つとして、一般の電話の場合であれば、発信者の逆探知に該当する状況すなわち、ネットワークへの攻撃をなしているパケットの発信元を突き止める行為を例にとって考察することができよう。電話の場合であれば、「一方の通信当事者の承諾では違法性は阻却されない場合がある」とされている（前述）。そうだとすれば、そのような通信の相手方の探知というのが、もはや、「業務の取扱い上、必要な限度」を越えているものとてして、積極的了知行為として認識されるのではないか、ということがいえる。そうだとしたときに、そのような行為を正当化する根拠というものは何であるのかということになる。ネットワーク管理の観点から、むしろ、電気通信事業者みずからが、相手を探知せざるをえないのではないか（電話の逆探知においては、受信者からの依頼での探知という問題であるのと依頼者が異なることになる）という問題があり、その意味で、電話における正当化を根拠として援用できないのではないかという疑問が発生するのである。

消極的了知行為であるとされれば、業務としての正当性が、直接的に問題にはならずに許容されることになり、これが消極的了知行為とされるかどうかは、一つの問題であろうと思われる。

ある意味で、従来の解釈においては、この消極的了知行為と、積極的な了知行為の限界というのは、明らかではなかったところであり、現代社会において、議論がなされるべき論点ということがいえるものと思われる。

３　積極的了知行為と正当業務行為

電気通信事業者みずからは、単なる通信の仲介者にすぎない場合[30]に、その管理の必要上、通信についての種々の情報を取得するというのが、どのような位置づけがなされるのかという問題がある。

パケット送受信情報を分析し、また、対外接続装置、高速基幹ルータの場所において、装置を通知するすべてのフロー送受信情報を分析することなどは、ある意味で、通信を届けるという観点からすれば、直接的に必要な行為とはいえないであろうから、積極的に了知する行為ということができるであろう。しかしながら、このような行為が、ネットワーク管理のために必要なものであることは論をまたないであろう。従って、その意味で、正当行為として違法性が阻却されることになるものと思われる。

しかしながら、その場合、どのようなネットワーク管理行為が、正当業務行為として許容されるのかということが明確であるとはいいがたいものと思われる。管理のために通信の内容まで常に了知しうるのかというと、それが許されないということは一般的に承認されるのであろう。しかしながら、具体的にどのような場合が許容されるのかという点についての議論は一向になされていないということができよう。

---

30 パケット通信については、すべて自己宛の通信であるとして、かかる点を種々の行為の正当化の根拠にする立場もあるものと思われるが、かかる見解は、極端にすぎるとおもわれる。

４　通信に関する情報の利用の問題

「通信の秘密」に関する情報については、電気通信事業者であっても、窃用は禁止されることになる。「窃用」とは、自己又は他人の利益のために用いることをいうことになるが、ネットワーク管理において、その管理のためにする利用行為がどこまでならば、窃用行為といわれないのかという点については、限界が不明確であるものといわれなければならない。

具体的には、情報の取得による攻撃分析、自らの対応、関係者へのはたらきかけ、学問的研究、その発表など、通信に関する情報の取得からする利用の問題については、いろいろな側面が考えられるが、どのようなところまでであれば、窃用行為といわれないのかという点については、その限界は、まったくもって不明瞭であるということができるであろう。

５　通信に関する情報の第三者への開示の問題

第三者への開示もの問題についても、電気通信事業者間における情報共有という問題からは、その限界がはっきりしないという問題がある。

また、ネットワーク犯罪が判明し、電気通信事業者のみの力で、真相を究明しがたいとき、通信事業者において、法執行機関の助力を得て真相の究明をすることができるのかという問題もあるのである。

第３章　比較法や日本国憲法草案の示唆するもの

第１　序

第２章までで、従来におけるわが国での議論が、ネットワークにおける管理等の活動についての限界等についての指針を提示するのに十分ではなかったことが明らかになったものと思われる。では、どのようにして、かかる管理等の活動の限界についての法的な指針を提供すべきかという問題がある。

本章においては、若干、視点を変えて、比較法的な視点や憲法制定時における通信の秘密の議論を洗い出してみて、かかる上述の問題についてのヒントをえることができないかということを検討してみることとする。

第２　比較法的見地からする「通信の秘密」の論点

１　米国法やサイバー犯罪条約からみた「通信の秘密」の憲法上の論点

ネットワーク調査・管理活動と「通信の秘密」めぐる議論において、現時点における「通信の秘密」の議論が十分な考察の根拠を提供してこなかったことは、前章までの検討で明らかになったものと思われる。さらにこの点を明らかにするために、米国における議論とわが国における議論を比較することは有意義である。付録２「IPv6 時代の通信の秘密に関する調査～ネットワーク観測の法的問題に対する米国連邦法の示唆～」や米国司法省「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）に記載されているとおり、米国では、わが国でなされている通信の秘密をめぐる解釈は、一般に第４修正（不合理な捜索および押収に対する人民の権利）と制定法の問題として、議論されている。そして、米国においては、特に制定法については、「自発的開示」か「強制的開示」かといういわば法執行機関と情報とのかかわりという観点と「通信に関する情報の格付け」という観点から議論がなされている。また、米国においては、憲法の第４修正の射程と制定法の射程との関係については、「送信の過程にある無形の電気信号を政府が「捜索」することも、第 4 修正上、問題となり得る。Berger v. New York, 388 U.S. 41, 58-60 (1967) (有線通信の傍受について、第 4 修正を適用) 参照。 しかしながら、連邦議会が Berger 判決で指摘された第 4 修正の問題に対し「犯罪防止および街路の安全性に関する包括法」の「タイトルⅢ」（Title Ⅲ of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title Ⅲ"), 18 U.S.C. §§2510-2522）を制定することで対応したことにより、そのような場合における第 4 修正の保護の外延は不明確なまま（hazy）となった。」とされており[31]、米国においても、制定法と憲法のそれぞれの限界については、はっきりしないところが残っているとされているのである。

---

[31] 米国・「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」（http://www.cybercrime.gov/searching.html）「Ⅰ令状によらないコンピュータの捜索・押収　3. プライバシの合理的な期待と第三者の保有」参照　なお、訳は、サイバー犯罪刑事手続調査委員会「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（社会安全研究財団、2004）における司法省マニュアルの翻訳による。

また、「通信に関する情報の格付け」という観点は、サイバー犯罪条約においても、議論の対象となっている。サイバー犯罪条約については、第１条ｄ項において、「「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。 」と定義がされている。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」が定められるなど、トラフィック・データと通信内容との二つの種別によって法的な規制が異なるのではないかということが示唆されているのである。

２　憲法の制定過程からの検討の意義について

また、特に米国法との比較の観点は、上記のサイバー犯罪条約の議論に対して米国の法制の影響がきわめて大きいものと考えられる時に、重要なものと考えられる。その観点からするとき、日本国憲法の成立については、米国の法律家が多大なる功績を残したことは明らかになっているが、日本国憲法の解釈論が、米国におけるかかる法理ときわめて隔絶された法理を展開しているというのは、興味深いところがある。わが国においては、「通信の秘密」についての憲法上の規定があることを前提に、米国の解釈論との相違が強調されることがあるが、はたして、日本国憲法の成立の際に、そのようなことが意識されたのかどうかということも検証することは意味があることに思える。

幸い、日本国憲法の草案の作成経過をめぐる議論については、種々の記録が明らかになり、しかも、容易にアクセスしうる状況になっている。しかしながら、この「通信の秘密」の規定が憲法の条文になった経緯についての分析もなされていない。本稿においては、日本国憲法の成立当時の歴史的な文書にあたり、しかも、それらの文書に影響を与えた文書などに接することにより、上記の「通信の秘密」についての論点についての議論状況を整理することによって、わが国における通信の秘密に関連する法整備に際しての基礎的な調査をすることも必要であろうとも思われる。

第３　ＧＨＱ案の起草過程の調査

１　ＧＨＱ案について[32]

昭和２６年 2 月 1 日、憲法問題調査委員会の試案が毎日新聞にスクープされ、「あまりに保守的、現状維持的なものに過ぎない」との批判を受け、このスクープをきっかけに、GHQ は、みずから憲法草案の起草し、それをもとに日本側に憲法を制定されるのが望ましいと考えるにいたった。2 月 3 日、マッカーサーは、憲法改正の必須要件（マッカーサー三原則）をホイットニーに示し、翌 4 日、民政局（GS）内に作業班が設置され、GHQ 草案（マッカーサー草案）の起草作業が開始された。2 月 13 日、外務大臣官邸において、ホイットニ

[32] 高柳賢三・大友一郎・田中英夫編著「日本国憲法制定の過程　Ⅱ　解説」２３頁以下（有斐閣、1972）

ーから松本国務大臣、吉田茂外務大臣らに対し、さきに提出された要綱を拒否することが伝えられ、その場で、GHQ 草案が手渡された。このＧＨＱ草案の作成の過程は、「日本国憲法を生んだ密室の９日間」[33]とも呼ばれているが、最初に各小委員会が、第１次案を作成し、次いで運営委員会と小委員会が合同委員会を開いて、それを基に第２案を作成するというやり方でおこなわれた[34]。この一連の動きは、極東委員会が日本の憲法問題について非常な関心を持っていることを感じたＧＨＱは、極東委員会の影響力を極力押さえ込むという関心からも、できるだけ早急に憲法を成立させることを望んだことによるものである。そして、毎日新聞がスクープした日本国憲法草案について、到底評価しうるものではないと判断したＧＨＱは、修正するのに時間をかけて日本政府と交渉するようもＧＨＱにおいて憲法のモデル案を作成し提供した方が効果的で早道と考えたのである[35]

ＧＨＱ案のうち、「通信の秘密」に対応する部分は、人権小委員会によって起草がなされている。この人権委員会は、医者であり、人類学者でもある社会学者のピーター・ロウスト中佐が責任者であり、ハリー・エマーソン・ワイルズ博士（経済学者で、慶応義塾大学でも教鞭をとった経験がある)、ベアテ・シロタ氏の３名で構成されていた[36]。

ここで、起草委員会での案のうち、いわゆるハッシー文書に残されている英文[37]は、

“Freedom of speech and press are guaranteed including the right to criticize any public official, agency or practice, or to urge the enactment, amendment or repeal of any law. No censorship shall be maintained, nor shall be secrecy of any means of communication be violated, ~~except in cases of criminal investigations.~~

［ This freedom shall not be interpreted to permit slander, black-mail, libel, the deliberate spreading of falsehoods or malicious rumors, nor the deliberate excitation of hatred against any law-abiding group, nor the wanton incitement of disturbance or violence. All persons shall be held accountable for the consequences of their words or actions.］

なっている。

この部分を日本語訳すると以下のようになる。

言論と出版の自由は、保証される。これは、公務員、公の機関、公の慣行を批判し、い

---

[33] 鈴木昭典「日本国憲法を生んだ密室の９日間」（創元社、1995）

[34] 竹前栄治・岡部史信「憲法制定史・第１巻」（小学館、2000）179 頁

[35]日本国憲法制定の過程　Ⅱ　解説」３０頁、ベアテ・シロタ・ゴードン「１９４５年のクリスマス」（柏書房、１９９５）131 頁など

[36]「日本国憲法制定の過程　Ⅰ」111 頁

[37] この英文については、国立国会図書館ギャラリー（http://www.ndl.go.jp/constitution/index.html）の１０５頁のものを紹介している。ハッシー文書のうち、英文・訳文ともに添削されている部分をできるかぎり再現している。なお、後述、「1945 年のクリスマス」１６９頁にも当該草案の訳文がある。

かなる法律の施行、改正、廃止を提唱する権利を包含する。~~（刑事的手続きの場合を除いて、）~~検閲は、なされてはならないし、通信の秘密は、侵されない。

［この自由は、名誉棄損、脅迫、侮辱、虚偽や悪意のある噂を周到に広めること、善良な団体に対する憎悪を周到に刺激すること、業務妨害や暴力をいわれなく煽動することを許容するものと解されてはならない。

すべての人は、発言と行動に対して責任をもたなければならない］[38]

とされている。

ここで、注目すべきは、ハッシー文書で削除されている部分をも含めて考えた時に、「通信の秘密」規定は、まぎれもなく、表現の自由という権利の一つの内容として認識されていたということである。削除された後段のいう「この自由」というのは、明らかに「通信の秘密」をも含んでいるということができる。

では、「通信の秘密」という文言のなかに表現の自由という権利のひとつの要素としてどのような意味が含まれていたのかということになる。これを確定するために、最初に、ＧＨＱ草案の背景と草案の確定までの経緯をフォローすることにする。

この草案の確定までの経緯については、わが国において、国立国会図書館ギャラリー「日本国憲法の誕生」をはじめとして、豊富な資料を得ることができる。これらの公開資料をもとにわが国において、ＧＨＱ草案の“secrecy of any means of communication”という文言が、どのような経緯・歴史的経緯によって記されたか、また、記された後、日本国憲法として制定されることになるまでの当該条項の変遷を調査することにする。

２　ＧＨＱ草案の作成にいたるまで

ＧＨＱ草案は、上記のように９日間というきわめて短い作業機関のなかで作成されるにいたったが、しかしながら、それ以前にも、ＧＨＱ内部で、日本国憲法の内容について一定の検討がなされていた。

（１）ラウエル報告書

昭和２０年１２月６日付けのマイロ E．ラウエル（Rowell, Milo E）陸軍中佐「日本の憲法についての準備的研究と提案のレポート」は、GHQ 民政局法規課長であったラウエルが、作成した報告書であって、きわめて興味深いものである。この報告書は、占領作戦によって、軍国主義者が政府の指揮を取得することを許容した権力の濫用が明らかになっているとして、報告書作成当時において、ラウエル中佐のなした事情聴取をもとに、日本にとって望ましいとされる提案事項が報告されている。そこでは、個人としての市民の人権が欠如していたことも権力の濫用の一つであるとされ、その報告書の付属文書Ａにおいては、「権利章典」が附されている。この権利章典の内容は、「日本国憲法制定の過程　Ｉ」6 頁以下に英文とその翻訳の双方が記載されているので[39]詳細は、省略するが、通信の秘密など

---

[38] なお、改正された条文については、「日本国憲法制定の過程　Ｉ」221 頁

[39]日本国憲法・検証１９４５－２０００　資料と論点　第４巻「基本的人権」にも記載されている。

に関連する事項としては、以下の記載がある。
「権利章典」は、１「事実」、２「説明（argument）」をもとにしていて提案事項（Recommendations）が記載されている。さらに、その提案事項は、「憲法改正案には、次の諸権利を保障する権利章典がふくまれていなければならないものとすること」という条項と、「推奨される（encouraged）が、必ずしも、必要とされる（required）ものではない」という条項の二つにわけられている。この前者の必要的記載事項のうち、いわば精神的自由権に関するものはとしては、
（１）宗教的崇拝の自由
（２）思想、言論、出版および集会の自由
（３）不正に対する救済を求めて部局もしくは官吏に対して請願する権利
（４）コミュニケーションに対して侵害が禁止されること（Inviolability of Communications）
などを含んでいる。
一方、後者の任意的記載事項とでもいうべきものとしては、
（１）プライバシーの権利。制定法に特段の定めがないかぎり、特に警官（peace officer）による傍受（eavesdropping）と私宅の頻繁な調査（inspection）に対して適用されるべきものである。
という記載がある。
ここでは、いわゆるコミュニケーションに対する保護が、コミュニケーションに対する侵害禁止とプライバシーの権利という二つの観点から分析されている点は、興味深いものといえるであろう。

（２）ラウエル「私的グループによる憲法改正草案に対する所見」

昭和２０年の秋から、憲法改正問題について、各種の提案が政府内部だけではなく正当、民間団体、個人の間でも活発に議論され、憲法改正についての提案や具体的な草案が相次いで発表された。そのなかで、ＧＨＱが、検討の対象としたものの一つは、高野岩三郎、室伏孝信、森戸辰男、鈴木安蔵らがメンバーとなって構成された憲法研究会が、同年１２月２６日に公表した「憲法改正案要綱」である。この要綱は、ＧＨＱにおいて翻訳されて、その翻訳をもとに、ラウエルは、昭和２１年１月１１日には、その要綱に対するみずからの分析（「私的グループによる憲法改正草案に対する所見」）をホイットニー准将に送付している。しかしながら、憲法研究会案が、通信の秘密等に対応する条項を欠いていたこともあって、このラウエル所見からは、特段通信の秘密に関する記載は見受けることができない。

３　ＧＨＱ草案の作成から、日本国政府への交付にいたるまで

（１）起草作業

昭和２６年２月４日、このＧＨＱの草案の作成作業が開始された点は、前述した。この作業は、全体を統括する運営委員会と前述の小委員会によってなされた。前述の人権委員

会の３名については、非法律家のみによって構成されていたということもあり、また、理想をできるだけ憲法に書き込もうとしていたこともあり、法律家によって構成されていた運営委員会との意見の食い違いを生ずることが多く、運営委員会は、小委員会の提案した条文をかなりの程度削除・整理をした。

前記の言論・出版の自由条項は、「市民権（Civil Rights）」の章のなかに準備されている。この「市民権（Civil Rights）」の章は、「Ⅰ　総則（GENERAL）」「Ⅱ　自由権（FREEDOM）」「Ⅲ　具体的な権利と機会（Specific Rights and Opportunities）」　「司法上の人権」とから成り立っている。そして、各節ごとに条文に分かれて、全部で４８条になっている。また、ハッシー文書からは、タイプや条文の記載の仕方も直接の担当になった３名ごとに異なっていることがわかる。現に、「司法上の人権」の部分は、節の名称や条文の番号も記載されておらず、また、「逮捕」「捜索差押」「拷問（Torture；Bail）」、「裁判」、「法規不遡及」「証言」「犯罪人引渡」などの小見出しが附されているなど、特徴がある。

本稿で問題にしている言論・出版の自由条項については、第２章・第１．１で述べたとおりである。

なお、厳密には、ハッシー文書において、当該条文については、１０５頁（２４－Ｇ－６－２）、１３２頁（２４－Ｇ－７－２）、１３５頁（２４－Ｇ－８－２）、１３８頁（２４－Ｇ－９－２）の４つの文案がある。これらの４案については、後者のほうが新しい案であると思われるが、その内容については、speech の前に assembly の用語が、加えられている以外は、ほとんど違いがない。この言論・出版の自由条項を含む自由権は、

１１条（人身の自由）
１２条（思想および良心の自由）
１３条（宗教の自由）
１４条（言論と出版の自由）
１５条（集会の自由）
１６条（移動、居所選択、職業選択の自由）
１７条（学問的教授、研究、調査の自由）

などによって構成されていた。

言論・出版の自由の条項は、ピーター・ロウスト中佐によって起草されたものと考えられる。ベアテ・シロタ・ゴードン氏は、「1945 年のクリスマス」で、本条文をロウスト中佐の筆になるものとしている（169 頁）。

（２）運営委員会での議論

これらの草稿をもとに、2 月８日、９日にかけて運営委員会において、草案についての議論がなされた。この経緯は、エラマン文書で、調査することができる。しかしながら、「言論と出版の自由」に関する議論のなかで、「secrecy of communication」の意味について特段取り上げて、議論されることはなかった。

このエラマン文書によれば、2 月 8 日には、この表現・言論の自由に関する規定について

の議論をもがなされたが、ケーディス大佐が、名誉毀損の禁止条項は、言論の自由の深刻な限界となるとして、異議を述べた[40]。彼によれば、政府の制作や活動に対しての批判が、名誉毀損であると名称づけられることによって、効果的に言論を抑圧されることになるのである。そして、名誉毀損であることの立証責任は、個人にあって政府にあるのではない。第１修正は、刑事名誉毀損法が議会を通過するのを防ぐ為に制定されたとのことである。この検討の結果、条文は削除されることになって、シンプルに、集会、言論、出版およびその他の表現の形態を保障するものとして、書き直されることになった。

翌 2 月 9 日の第 2 回会議において、この言論・出版の自由に関する条項については、特に議論がなされることはなかった。もっとも、言論・出版以外の形態による下品または下級な表現への制限が可能になるのではないかという議論がなされた。

これらの作業を経て全 92 条からなる委員会報告書がまとめられた。この協議にもとづいて作成された”Original drafts of committee reports”においては、言論・出版の自由の条項に関して

“ Freedom of assembly, speech, and press (and all other forms of expressions が追加)are guaranteed, ~~including the right to criticize any public official, agency or practice, or to urge the enactment, amendment or repeal of any law.~~ No censorship shall be maintained, nor shall the secrecy of any means of communication be violated. ~~All forms of expression other than speech and press shall be accorded the same essential freedom, but legal measures for the suppression of indecent or degrading literature, plays moving pictures, radio broadcasts, and exhibitions shall be permissible for the protection of youth and the maintenance of high public standards.~~”

とされている。

結局、上述の通り、簡潔にすべての表現の自由を記載するというケーディス大佐の意見にしたがって、政府等を批判する権利という部分と公共の基準を保護するための法的手段を認めていた部分が削除されている。結局、上記の運営委員会でもなんら検討がなされなかったことを反映して、secrecy of communication の部分については、当初のロウスト氏の原稿から、なんらの変更もされていない。

（3）日本国政府への交付

上記の憲法草案の作成作業は、作業開始の 1 週間後の 2 月 10 日に一応完了し、マッカーサー元帥の手元に内容を説明するメモとともに届けられた。マッカーサー元帥は、人権条項に対する改正禁止条項を削除し、それ以外を承認したのであった。その後も 2 月 12 日まで、運営委員会で調整が続けられた。

昭和 26 年 2 月 13 日、午前 10 時頃、ホイットニー准将、ケーディス大佐が吉田外相、松本大臣のもとを訪問して、GHQ 草案を日本側に交付した。この交付した際のやりとり等は、

---

[40] エラマン文書 15 頁、「日本国憲法制定の過程　Ⅰ」203 頁、同Ⅱ164 頁

日本国憲法成立史[41]をはじめとする書籍に詳細な記述がある。

4 日本国政府による対応と日本国「憲法改正草案要綱」について

（1）GHQ案の交付から 3 月 2 日案の提出まで

手渡された草案に対して、日本政府は、2 月 22 日の閣議において、GHQ 草案に沿う憲法改正の方針を決め、法制局の入江俊郎次長と佐藤達夫第一部長が中心となって日本政府案の作成に着手し、3 月 4 日午前、GHQ に赴いて提出した。

このGHQ案の通信の秘密条項は、その翻訳の段階で、日本国憲法草案（2 月 15 日）においては、「第二十条　集会、言論及定期刊行物並ニ其ノ他一切ノ表現形式ノ自由ヲ保障ス検閲ハ之ヲ禁シ通信手段ノ秘密ハ之ヲ犯ス可カラス」とされた。この時点で、「通信手段の秘密」として、「手段」に注目がなされている点が興味深いものである。これは、おそらく、英文の”any means of “ の means を手段として解釈したものと思われる。

その後、日本国政府は、GHQ 草案は一体をなすものであり、字句の変更等は可能だが、その基本原則についての変更を認めないとの GHQ の返事を得たこともあり、GHQ 草案に従って日本案の作成に着手することとなった。すなわち、日本国政府は、2 月 26 日の閣議で GHQ 草案に基づいて日本政府側の案を起草し、3 月 11 日を期限として GHQ に提出することを決定した。この日本政府案の起草の任にあたったのが、佐藤達夫(法制局第 1 部長、当時)であった。

佐藤達夫部長は、2 月 28 日に初稿を完成した。この初稿は、佐藤の起草した人権部分を、合わせたものであるが、この初稿においては、

「第 12 条 国民ハ、安寧秩序ヲ妨ゲザル限ニ於テ言論、著作、出版、集会(多衆運動)及結社ノ自由ヲ有ス。
(検閲ハ映画ソノ他法律ノ特ニ指定スルモノニカカル場合ノホカコレヲ行ウコトヲ得ズ)」
「第 13 条 国民ハ信書ソノ他ノ通信ノ秘密ヲ侵サルルコトナシ。公共ノ安寧秩序ヲ保持スル為必要ナル処分ハ法律ノ定ムルトコロニ拠ル」
と「通信の秘密」の条項が、表現の自由の条項とは別個に定められている。これは、大日本国憲法における「信書の秘密」を継受する条文であることを意識したものと思われる。

その後、松本烝治国務大臣、入江俊郎法制局次長などとの議論の末、第 2 稿が作成された。この第 2 稿においても通信の秘密に関する条文は、表現の自由とはまた別個の条文として規定され、「国民ハ」という書き出しの部分が、「凡テノ国民ハ」と改まっているのみである。この第 2 稿については、条文の上に GHQ 草案の条文との対象がなされており、日本案が、明確に「通信の秘密」を表現の自由と分離して定めている点については、興味深いところである。

このような作業の間、GHQ は、早急に日本案を提出するように促した。そのため、日本国政府は、急いで案文を整理し、3 月 4 日午前、松本烝治国務大臣と佐藤達夫部長は、説明

---

[41] 佐藤達夫著・佐藤功補訂「日本国憲法成立史」第 3 巻(有斐閣、1994)

書とともに GHQ に提出している(3 月 2 日案)。この 3 月 2 日案は、上記第 2 稿と同様のものである。

なお、この際に、「説明書」も提出されているが、この説明書には、上記「通信の秘密」の条項についての解説はなんらなされていない。

（2）ケーディス大佐の意見と 3 月 5 日案・「憲法改正草案要綱」

日本国政府が提出した 3 月 2 日案は、直ちに GHQ とともに翻訳・分析がなされた。しかしながら、英訳が進むにつれて、GHQ 側は、GHQ 草案と日本案の相違点に気づき、松本とケーディス大佐との間で激しい口論となった。この協議の過程については、「3 月 4・5 両日司令部ニ於ケル顛末」という佐藤達夫部長の克明な記録によって明らかになる。

しかしながら、人権を規定する第 3 章の規定は、日本案と、GHQ 草案は、すっかり違っている、これを審議しても意味はないということになって、第 14 条以下の部分については、GHQ 草案を根拠に議論することになったのである。その結果、言論・出版の自由に関する条文において「通信の秘密」が規定されるという状況が復活した。具体的には、「検閲ハ之ヲ禁シ通信手段ノ秘密ハコレヲ侵ス可カラス」という文言で規定されたのである。なお、この言論・出版の自由の関する条項については、結局、結社の自由が、集会とまとめて規定するほうが適当だということで、「集会、結社、言論及定期刊行物並ニ其の他一切ノ表現形式ノ自由」を保障するということになった経緯があった。

これらの審議の結果が、閣議用として印刷にまわされ、3 月 5 日案という形で、明らかになった。文言としては、「第十九条　集会、結社、言論及定期刊行物並ニ其ノ他一切ノ表現形式ノ自由ヲ保障ス検閲ハ之ヲ禁シ通信手段ノ秘密ハ之ヲ侵ス可カラス」とされている[42]。

この 3 月 5 日案は、GHQ の了解を得て、字句の整理をしたうえで、要綱の形で発表されることとなり、3 月 6 日午後 5 時、「憲法改正草案要綱」は、勅語や内閣総理大臣の談話などとともに内閣から発表された。ここでは、文言の訂正がなされ、「第十九　集会、結社及言論、出版其ノ他一切ノ表現ノ自由ハ之ヲ保障シ検閲ハ之ヲ禁ジ通信ノ秘密ハ之ヲ侵スベカラザルコト」とされている。ここでは、いままで「通信手段」として「手段」の文字が附されていたのにもかかわらず、最終的に削除された点が注目される。なお、この手段という文字が削除された経緯については、文献上、見つけることはできなかった。

（3）日本国憲法制定まで

日本政府は、翌 3 月 6 日、「憲法改正草案要綱」として発表し、ひらがな口語体での条文化が進められ、4 月 17 日、「憲法改正草案」として公表された。

[42] http://www.ndl.go.jp/constitution/shiryo/03/091/091tx.html

第４　起草の背景の調査

１ 詳細調査の必要性

上記の公開資料による調査から

(1) “ secrecy of any means of communication ”の条文は、ロウスト中佐が起草し、資料上からは、その内容について、議論がなされた経緯は、存在しない。

(2)ケーディス大佐は、かかる“ secrecy of any means of communication ”においても、米国の修正 1 条ないしそれと関連する法理を具現化した条文であると認識していた

(3)日本側が、「通信の秘密」の条項を言論・出版の自由とわけて提案した経緯があったが、結局その案については、採用されることはなかった。

(4)“ secrecy of any means of communication ”の文言は、「通信手段」の秘密と翻訳されていたが、その条文は、最終的には、「手段」の文言が削除されるにいたった。なお、削除された経緯は不明である。

ということがいえる。

そうすると、この“ secrecy of any means of communication ”の条文についてどのように考えるかということについては、さらに起草を直接担当したロウスト中佐の手元の資料等の検索をなすことができれば、有意義な情報が得られるものと思われる。そこで、まず、その調査をなす前に、人権章委員会のメンバーから、ロウスト中佐の起草についての何らかの情報を得ることができないかという問題がある。

２ 起草関係者の個人的資料に対する調査

次の手法としては、起草関係者が起草するにあたって参照した資料、関係者の法律的なバックグラウンドなどから、その当時の真意というものを推測するということが調査手法として考えられる。かかる手法にもとづいて調査した結果は、以下のとおりである。

（１）ベアテ・シロタ女史に対するインタビュー

調査チームは、上記の調査の手がかりとして、ベアテ・シロタ女史に対するインタビューを行った。付録１のとおりの内容を記し、ファクシミリで送付し、電話でインタビューを試みた。しかしながら、ベアテ・シロタ女史は、通信の秘密に関する条項について、聞かれるのは、初めてであるということで、具体的に誰が起草したか、またどのような資料に基づいて起草されたかということについては、知識はないということであった。

（２） ロウスト氏の資料についての調査

ロウスト氏(Pieter K Roest)のバックグラウンドについて詳細な資料を入手することはできなかった。入手しえた資料[43]から経歴をまとめると次のようになる。

ピーター・K・ロウスト陸軍中佐は、1898 年サンフランシスコ生まれ。オランダのライデン大学の医学部を卒業後、シカゴ大学で人類学と社会学の博士号を取得、南カリフォル

---

[43] 『日本国憲法を生んだ密室の九日間』52 頁、『1945 年のクリスマス』38、168、191 頁などで、”Typhoon in Tokyo” (MacMillan Co., New York)、『東京旋風』（時事通信社、1954）

ニア大学の大学院で国際関係論、法律学、経済学を修めた。陸軍に任官前は、インドのマドラスの小さな大学で講師を務め、この間カースト制度の研究を行ない、オーストラリア民族主義の研究、ジャワ島における人種間通婚の調査などを行ない、トレド大学（オハイオ州）・リード大学（オレゴン州）の社会科学部長、農務省の市場調査専門官などをつとめている。１９４２年に少佐に任官され、バージニア大学の軍政学校、エール大学の民事要員訓練所を卒業、GHQ には１９４５年秋に赴任している。

また、同じ民政局で人権条項の起草を行なったワイルズ博士は、著書『東京旋風』の中で日本占領の憤懣をぶちまけている。実は、この共同通信社の『東京旋風』は、英文オリジナル"Typhoon in Tokyo" (MacMillan Co., New York) から約 3 割を圧縮して翻訳されたものであるが、英文オリジナルおよび日本語訳のいずれにしても、ロウスト中佐を指している箇所をはっきりと特定することはできなかった。それどころか、民政局でこれほど間近に重大な仕事を勤めたにもかかわらず、ロウスト中佐の名前を見つけることすらできなかったことからは、かなり複雑な感情があることを推測させる。ベアテ・シロタ・ゴードン氏の『1945 年のクリスマス』191 頁にも、同様の指摘がある。

ロウスト中佐の経歴についての乏しい情報以外に、憲法草案起草時のエピソードから特徴を垣間見ることができる。たとえば、ベアテ・シロタ・ゴードン氏は、同書 168 頁で、基本的人権の総則の草案をめぐって、「すべて自然人は・・・」という表現を用いたことを、民族とか国とかによって束縛されない、コスモポリタンのロウスト中佐の考え方として賞賛し、「人種、信条、性別、カースト・・・」のくだりに、女性への気配りも、インドでカースト問題を研究した中佐の心配りに帰して、ロウスト中佐のインドをはじめアジアでの研究対象を前提にするようである。しかしここで、単純にコスモポリタンと評するだけでは不十分な、バックグラウンドを実は中佐は持っているのである。

信教の自由について、草案では、聖職者はいかなる種類の政治活動にも従事してはならないことを定めていた。これに対して、ケーディス大佐は、聖職者の政治活動を禁止することは、言論・出版の自由を否定することを意味するもので、憲法というのは、制限の章典ではなく、権利の章典であるべきであり、この特段の禁止規定は、憲法の中に置かれるべきではないと指摘した。この点について、草案の担当者であったロウスト中佐の考え方は、霊的な権威が政治的目的のために濫用されるのを防止することを目的とすべきという「全く違ったところに発想の起点があった」のである（「1945 年のクリスマス」、179 頁）。

ベロテ・シロタ・ゴードン氏の指摘は同僚として正しかったかもしれないが、ロウスト中佐には精神的自由や、宗教、または霊性というものには、また別の思いがあったと思われる。それは、中佐が、1933 年 9 月から 1937 年 8 月まではほぼ毎号、その後、日本進駐前の 1943 年まで断続的に寄稿していた雑誌[44]が非常に特徴的なものであることを根拠とす

[44] An Index to The American Theosophist 1933 - 1996, Wheaton
http://www.austheos.org.au/indices/AMERTH.HTM
時期的な附合と、最後の寄稿となったテーマが Discipleship in Wartime [extract

ることができる。

その雑誌は、American Theosophist といい、Theoshophy は日本語では「神智学」と訳される。神智学とは「通常の人間的な認識能力を超えた神秘的・直観的霊知によって、神を体験・認識しようとする神秘説。グノーシス主義・新プラトン派などの神秘主義にうかがえる。」（大辞林）とされるが、神智学が言及する対象は非常に広大であり、導入的な説明が非常に困難であって、一部オカルト的なものを対象とすることもある点が外部のイメージをゆがめているかもしれない。ロウスト中佐の経歴の中で社会学と人類学の博士号取得とあり、また一方、民族学者という記述があるのは、通常の大学で神智学という講座は設けられていないので、そのような学問分野を通じての神智学研究であったか、また逆に、そのような学問分野に神智学的アプローチを導入したものかのいずれかであろうと推測される。ベジタリアンというのもあるいは宗教的理由ではなかろうか。

ロウスト中佐の寄稿の中には、後に憲法起草にかかわるようなテーマとして、次のようなものが見える。

「流行論」On Popularity

評釈「生きる宗教：個人生活と社会再構築に宗教を生かすためのマニュアル」'Living Religion: A Manual for Putting Religion into Action in Personal Life and in Social Reconstruction' by Hornell Hart

「神智学と幸福」Theosophy and Happiness

評釈「現代人の人生観」'A Life View for Moderns'

「戦時における修行」Discipleship in Wartime [extract Theosophy in Australia 1942-43]

したがって、一般的に断ずることは危険であるが、政治権力はもちろん、特定の宗教・宗派の信仰を超えて、物事を偏見なしに理解しようとする神智学的視点というものを考慮すれば、平等や、自由を非常に広範に擁護しようとするロウスト中佐の考え方の淵源が垣間見られ、また制定過程での発言の真意も腑に落ちるように思われる。

占領後の足取りはよく分からないが、1968 年出版の『アフガニスタン：人、社会、文化』[45]に共著者として名前があり、また、出版年不明の単著『セイロン憲法制度』[46]の 2 冊があ

Theosophy in Australia 1942-43]であること、また、Pieter K Roest というフルネームの綴りに特徴があり、本人に間違いないと思われるが、本人の同一性を確認するまでに至っていないし、記事自体を入手することができなかった点については、留意いただきたい。

[45] Afghanistan : its people, its society, its culture / Donald N. Wilber 出版・頒布事項 New Haven : HRAF Press , c1962.形態事項 xii, 320p. : front. (map), illus., chronological tables, tabs. ; 21 cm 書誌構造リンク Survey of world cultures <BB06013374> 11//a 注記"In collaboration with Elizabeth E. Bacon, Charles A.Ferguson,Peter G.Franck, Aloys A.Michel [and] Pieter K.Roest"

[46] The constitutional system of Ceylon (Unknown Binding) by Pieter K Roest

るらしく、先の雑誌の 1968 年 8 月号に死亡記事がある。[47]

（３） それ以外の関係者の資料について

なお、調査チームは、それ以外の関係者特に、ケーディス大佐のバックグラウンド・資料其の他についての調査をなした。

ケーディス大佐の経歴に関して、収集した資料をまとめると次のとおりになる。

民政局次長のチャールズ・L・ケーディス大佐は、ルーツはスペイン系のユダヤ人。両親は、フランスのアルザス地方の出身で、アメリカ東部に移住している。１９０６年、ニューヨーク州ニューバーグ生まれ。コーネル大学とハーバード大学のロー・スクールを卒業。学生時代フランクリン・ルーズベルトのニューディール政策に影響され、以来進歩的な思想の持ち主である「ニューディーラー」を自負している。１９３０年から３３年まで、ニューヨークのホーキンス・デラフィールド・ロングフェロー法律事務所に所属弁護士として勤める。１９３３年から３７年までルーズベルト政権のイッキーズ内務長官の補佐官となり連邦公共事業局の副法律顧問、１９３７年から４２年まで財務省の副法律顧問、同じ年の四月から陸軍中尉として軍務につく。歩兵学校、指揮参謀学校を卒業したのち、陸軍省民事部に配属される。その後第七軍に所属、第一空挺隊の参謀第五部の副官となり、ノルマンディ上陸作戦、アルプス作戦、ラインランド作戦に参加している。４５年日本降伏直後、マッカーサーに続いて厚木に上陸、占領開始期の実務を処理。同年 GHQ 民政局次長に就任、日本専門家と軍人の担当官をリードし、新憲法草案(マッカーサー草案)の総責任者を務めた。また、公職追放、内務省解体、地方自治に加えて、警察制度民主化を進め、G2(情報)のウィロビー少将と対立した。その後、占領政策の"逆コース"(民主化からの逆行)で行き詰まり、４８年帰米、４９年辞職。以後、ニューヨークで弁護士活動を続けたが、マッカーサーの愛顧はあつく、マッカーサー家の財産の管財人も務めた。８０年弁護士を引退。９３年来日し TV に出演。９６年没。

３　起草当時の学説、制定法などの調査

調査チームの調査結果によってもなかなか、明確な起草者の意図を抽出することができなかったといえる。そこで、米国における第１修正とコミュニケーションとの関係についての考察をなし、また、1945 年前後の段階での関連する議論をフォローすることは有意義であろうと思われる。ロウスト中佐やケーディス大佐に成り代わって、その条項の解説文を書くとすれば、その当時において、どのようなことが議論されており、また、どのような法的状況をもとに当該起草をなしたといえるのかということが問題になるのである。

（２）表現についてのプライバシーの権利

「プライバシーの権利」について、米国の憲法のある教科書[48]は、

「プライバシーの権利」は、種々の意味を有している。不法行為のコモンローによれば、その権利は、個人の私的な生活について情報を開示されない自由のみならず、私的に所

[47] y1968 v56 i8 August p198 - obituary - Pieter K Roest – anon

[48] Nowak & Rotunda “ Constitutional Law” fourth edition(West 1991)

有している地域への侵入をされない自由を射程としていた。そのフレーズは、また、憲法的な分析から種々の意味を有している。もっとも古い憲法典の権利は、政府の捜索差押に関する第４修正によって保護されるものである。 第１修正は、言論や集会にさいしてのプライバシーの権利をいくぶんか保護するものとして考えられてきた。裁判所は、他人のプライバシーを侵害する言論に対して訴訟が提起されうるかどうかを決定する際にプライバシーの不法行為上の権利に直面してきた。

と述べている。そして、私たちは、この記述で非常によく参考にされているウォーレンとブランダイスの考察を参考にするとき、きわめて示唆に富む表現を見つけることができる。それは、「コモンローは、各個人に対して、通常、自己の思想や感情をどの範囲で他人に表示すべきかを決定する権利を保障している。われわれの統治制度のもとでは、彼は自己の思想や感情の表明を強制されることは絶対にない（ただし、証人台に立った場合は別である)。そしてまた、たとえもし彼が、思想や感情を表明しようとする場合でも、彼は、一般に、それらに対してどの限度のパブリシティを与えるべきかを決定する権利を留保している。この権利の存在は、表明に用いられた特定の方法の間によって左右されるものではない。それが言葉によって表明されたか、あるいは記号によったか、絵画によったか、彫刻に、音楽に、いずれであるにしても、それは問題ではない。 この権利の存在はまた、思想や感情の性質や価値に左右されるものでもなければ、その表明の方法がすぐれているかどうかによって左右されるものでもない。たまたま書いた手紙や、日記の書き込みにも、またもっとも価値のある詩やエッセイにも、できそこないや下手くそな絵にもそして、傑作にも、同一の保護が与えられる」[49]というものである。ここで、「個人は彼の所有に属するものを公にすべきかどうかを決定する権利をもっている」という権利というものを認識したとして、その権利を考えた時に、その権利は、「表現についてのプライバシーの権利」といわれることになろう。要は、表現者（意思伝達をなしたもの）は、その表現を公表するか否かを決定する権利を有するということである。

法理論としては、「個人的な書面や、その他知性または感情の産物を保護するこの原則は、プライヴァシーの権利」であるが、その原則が、「個人の容姿、言葉、行為、また個人的高裁関係（過程における、またはその他の）などをも保護する」ように拡大されるときに現在、議論されているプライバシーの権利の内容（私的な事項を公開することを禁じること）になるものと考えられる。

（３）米国の各州におけるプライバシーの立法化

米国の２０世紀前半において、「プライバシー権」が、存在していると認識されていたということは一つ認識しておく必要があろう。1903 年には、広告もしくは営利の目的のため、その人の同意なくしてある人の似顔、物語もしくは出来事の公表を禁止するニューヨーク州法が制定されている。また、1931 年には、州法が不存在でも、プライバシーの権利は、

[49] ブランダイス＝ウォーレン、外間　寛訳「プライヴァシーの権利」（戒能通孝、伊藤正己編「プライヴァシー研究」所収）（日本評論社、1962）９頁

合衆国憲法ならびにカリフォルニア州憲法によって保障されている「幸福追及の権利」の一部であることが確認されている[50]。

（４）米国における郵便や通信への捜索・押収をめぐる制定法の状況

また、「通信の秘密」の条項の背景となった状況を調査するという観点からは、起草当時において、米国において郵便に対する捜索や逆探知装置の利用・通信傍受がどのように位置づけられていたかという点も有意義な情報になる。

郵便物に対する捜索については、郵便物に対する第４修正条項は、その郵便の内容に対する不合理な捜索・押収を禁止するにすぎない。郵便物のアドレスおよび返送用のアドレスは、「メールカバー」とされ、よりゆるやかな規制が準備されている[51]。

後者の通信の傍受の点については、以下のような事実を指摘することができよう。

(ア)米国において、通信傍受は、当時からも第４修正条項の問題として議論されていた。

(イ)当時、米国の各州は、州法で、通信傍受を禁止するか規制する州がかなりの数、存在していた。

(ウ)オルムステッド事件において、弁護士と依頼者間の通話について、その通話が第三者に漏洩されてしまった以上は、その特権は、行使しうるものではないとされ、しかも、その際に、通信傍受をもちいて取得された通話は、証拠として排除されることはないとされていた[52]。

(エ)1934 年連邦通信法 605 条によって、通信の傍受およびそれの窃用が禁止された。同条は、「送話者の承認を受けていないものは何人も、いかなる通話をも途中で奪ってはならない。また、このような通話中に奪われた通話の存在、内容、実態、目的、影響または意味をほかに洩らしまたは公開してはならない。また、このような通話中に奪われた通話を受けた者は、その通話またはその通話の中に含まれている情報を自己の利益または権限なき、第三者の利益のために用いてはならない。」と定めている。

(オ)1942 年の Goldman 事件において、会話傍受(eavesdrop)が、第 4 修正条項違反にな

---

[50] 戒能通孝「プライヴシァシー権とその保障」（戒能通孝、伊藤正己編「プライヴァシー研究」所収）（日本評論社、1962）88 頁、久保田きぬ子「プライバシーの権利」日本国憲法体系第 7 巻　基本的人権（１）所収（有斐閣、1965）151 頁、156 頁

[51] http://www.mttlr.org/volten/pikowsky.pdf
特にその１５頁以下。現行法のもとでは、39 C.F.R. § 233.3 (2003)において規定がなされており、郵政検査官（Chief Postal Inspector）もしくは、その指定するものは、以下の状況においてメールカバー命令をなすことができるとされ、その状況として、
「(2) 法執行機関から、書面による要望がなされ、その書面において、そのメールカバーが、以下について必要であることを明らかにしているとする合理的な根拠がある場合
(i) 国家安全を保護するため
(ii) 逃亡者の居場所をつきとめるため
(iii) 犯罪しくは、その陰謀の情報を取得するため
(iv) 刑法違反による没収の財産、収益もしくは資産の特定を容易にするため」

[52] 井上正仁・前出・６頁

らないと判断された[53]。

(カ)ペンレジスター[54]の利用については、その後の判決であるが、United States v. New York Telephone Co., 434 U.S. 159, 165–68 (1977) において、ペンレジスターは、電話会議の内容を取得するものではなく、制定法によって定義されているように通信を「傍受」するものではなく、さらに、制定史からすると連邦通信傍受法（当時）[55]は、ペンレジスターの使用を制限する意図がなかったことを物語っているとして、ペンレジスターの使用は、連邦通信傍受法（当時）によって規制されるものではないという判断がなされている。また、Smith v. Maryland, 442 U.S. 735 (1979).において、最高裁判所は、ペンレジスターの使用は、第３者に移転してしまったものに合理的なプライバシーの期待を主張できないことから第４修正の捜索の目的にはあてはまらないという判断がなされている。もっとも、その後、電気通信プライバシー法により、電子的監視の場面における使用は、原則として禁止されている[56]。

４　ヨーロッパの当時の憲法状況について

起草過程で実際に参考にされた国の憲法はどれであったかについて、ベアテ・シロタ・ゴードンが参考にした国として挙げられているのは（『日本国憲法を生んだ密室の九日間』p.205)、ワイマール憲法、スカンジナビア（おそらくフィンランド）憲法、アメリカ合衆国憲法、およびソビエト社会主義共和国連邦憲法（1936 年制定）であったが、これらのうち後二者には、通信の秘密（または信書の秘密）の条項はない。また、人権宣言、国連憲章も同書には挙げられているが、通信の秘密を規定する条項は含まれていない。

日本国憲法起草時点までの欧州各国憲法につき、制定年順に見ることにする。

確認のため、明治憲法（1889 年制定）は、26 条「日本臣民は法律に定めたる場合を除く外信書の秘密を侵さるることなし」として信書の秘密のみ規定していた。

ギリシア憲法（1911 年制定）は、20 条「信書の秘密は、絶対に侵されない。」（和訳各国憲法集（衆議院法制局、参議院法制局、国会図書館調査立法考査局、内閣法制局）として、同じく信書の秘密のみ規定する。

ルクセンブルグ大公国憲法（1868 年制定、1919 年改正）は、28 条(1)「信書の秘密は不可侵である。郵便官署に委ねられた信書の秘密の侵害については、法律によって責任ある官憲を定める。」(2)「電信の秘密に対する保障は、法律によりこれを定める。」[57]とし

---

[53]井上正仁・前出・８頁

[54] 新保史生「プライバシーの権利の生成と展開」236 頁（成文堂、2000)、Pikowsky（注 51）17 頁など。

[55] 当時は、「犯罪防止および街路の安全性に関する包括法」の「タイトルⅢ」（Title Ⅲ of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title Ⅲ"), 18 U.S.C. §§ 2510-2522）を指す。

[56] この点については、（注 31）の米国・司法省マニュアル、第４章・C参照のこと

[57] s.28(1) The secrecy of correspondence is inviolable. The law determines the agents responsible for the violation of the secrecy of correspondence entrusted to the postal services.

て、信書の秘密と、電信の秘密とを区別した。

ワイマール憲法（1919 年制定）117 条は、「信書の秘密は、郵便、電信および電話の通信と同様に不可侵である。例外は、共和国法によってのみ認められる。」[58]（和訳：筆者）と規定し、信書の秘密と通信の秘密を併記する。

これに対して、フィンランド憲法（1919 年制定）12 条は、「郵便、電信又は電話による通信の秘密は、侵されない。ただし、法律で定める場合は、この限りでない。」[59]（和訳各国憲法集(続)（衆議院法制局、参議院法制局、国会図書館調査立法考査局、内閣法制局）と規定して、信書の秘密に言及しない文言である（ただし、現行の 1999 年改正においては、「信書及び電話の秘密並びにその他の機密通信は、これを侵してはならない。」[60]となっている。）

ポーランド共和国憲法(1921 年制定)106 条「すべての者は、信書、電話通信、郵便、有線およびその他の通信の秘密に権利を有するものとする。この権利に対する制限は、司法裁判所の命令に基づく場合にのみ許されるものとする。」（和訳：筆者）[61]と一括して列挙し、規定した。(参考までにその後の経過をたどると、1947 年権利宣言では、基本的人権の列挙のうち、8 項「郵便およびその他の手段の通信の秘密」（和訳：筆者）[62]と簡略化され、さらに 1952 年憲法改正では、87 条(2)「家庭の不可侵と信書の秘密は法によって保護されるものとする。家庭は法により特定され、かつ裁判所の終局判決の効果による場合にのみ捜査可能である。」(和訳：筆者)[63]として信書の捜査が制限され、1997 年改正現行では、49 条「通信の自由および秘密は、これを保障する。これに対する制限は、法律により定められた場合に、かつ定められた方法でのみ課すことができる。」(和訳：筆

---

(2) The law determines the guarantee to be afforded to the secrecy of telegrams.

[58] s.117 The secrecy of correspondence, as well as the secrecy of postal, telegraphic and telephonic communications is inviolable. Exceptions may be admitted by federal law only.

[59] 英文による条文は入手できなかった。

[60] s.10(2) The secrecy of correspondence, telephony and other confidential communications is inviolable.

[61] s. 106 Everyone shall have the right to privacy of correspondence, telephone communications, mail, cables and other communications. Any restriction of this right shall be allowed only under an order of a court of law.

[62] DECLARATION OF RIGHTS AND LIBERTIES
Approved by the Constituent Diet on February 22, 1947
THE CONSTITUENT DIET, representing the sovereign authority of the Polish people solemnly declares that in the exercise of its constitutional and legislative power and in the exercise of its supervision over the activities of the Government, as well as in its determination of the basic policies of the nation, it will continue to uphold such fundamental civil rights and liberties as:
(8) Secrecy of the mails and other means of communication;

[63] s.87(2) The inviolability of the home and the privacy of correspondence shall be protected by law. The home may be searched only in cases specified by law, and only by virtue of a final judgment of a court.

者)[64]と包括的な規定になっている。）

ここまで辿ってきたように、1945 年段階では、信書の秘密の規定との関係では、(1)通信の秘密をこれとは分けて規定する例、(2)併記する例、および(3)通信も郵便と電気通信とを列挙する例が混在していたといえる。

信書の秘密と検閲とをどのように考えるか。また、郵便の秘密を規定しながら「信書の秘密」の文言がなくなった場合に、内容以外の通信情報に関して、公権力による検閲は成立するのか否か。または、通信の秘密と表現の自由との関係はどうか。

表現の自由に関して、早くもオーストリア共和国憲法(1849 年制定)皇帝勅許 5 条「すべての者は、その意見を印刷または絵画で自由に表現する自由を有する。出版は検閲の制限に服しない。出版の濫用に対しては、抑制法が制定される。」(和訳：筆者)[65]として、検閲の禁止を規定する例が見られる。オーストリア共和国基本法（1955 年）は、10 条「信書の秘密は侵すことができず、信書の押収は、勾留又は家宅捜索の場合を除いて、戦時又は法律の定める手続に従い、裁判官の発する令状によらなければ、これを行うことはできない。」10a 条「電気通信の秘密は不可侵である。前項に対する制限は、法律の定める手続に従い、裁判官の発する令状によらなければ、これを行うことはできない。」[66]として、これによれば、検閲の禁止と、信書あるいは通信の秘密とは別立てであるように見える。

起草の際に参照したかという問題とは別になるが、信書の秘密と通信の秘密の規定の仕方についての傾向を見る意味で、1945 年の日本国憲法起草以降あまり経っていない時期までの欧州各国憲法の規定を参考までに見ることにする。

イタリア共和国憲法（1947 年制定）15 条(1)「信書及びその他一切の通信の自由及び秘密は、不可侵である。」(2)「その制限は、法律に定められた保障を伴い、司法官憲の理由を付した令状によってのみ行うことができる。」

スイス連邦憲法（1874 年制定、1948 年改正）36 条(4)「郵便および電報の秘密はこれを保障する。」

ドイツ連邦共和国基本法(1949 年制定)10 条(1)「信書の秘密並びに郵便及び電気通信の秘密は、不可侵である。」

---

64 s.49 The freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute.

65 s.5 Everyone has the right freely to express his opinion by word or writing, in print or by pictoral representation. The press cannot be subjected to censorship. Against the abuse of the press a repressive law will be enacted.

66 s.10 The privacy of letters may not be infringed and the seizure of letters may, except in case of a legal detention or domiciliary visit, take place only in times of war or by reason of a judicial warrant in conformity with existent laws.

s.10a Telecommunication secrecy may not be infringed. Exceptions to the provisions of the foregoing paragraph are admissible only by reason of a judicial warrant in conformity with existent laws.

したがって、1950 年までに憲法上規定された、各国の傾向を見ると、信書の秘密と通信の秘密を併記する例が多く、また、通信も郵便と電気通信その他とを併記する例が多く、通信の秘密に一本化する立法例は、一般的ではなかったということができる。

このことから、ロウスト中佐がヨーロッパ諸国の憲法を参照してこれを導入したという根拠はかなり希薄であると結論することができるだろうと考えられる。

第５　従来の解釈上の問題点の整理

１　比較法のなかでの位置づけについて

以上の起草の過程および起草の背景についての調査を経て、憲法上の「通信の秘密」規定に関するもともとの起草者の意図が、どのようなものであったかということを位置づけるとする場合にどのようなことがいえるであろうか。なんらかの比較法的な根拠があったものとした場合、以下の３つの方向性の可能性があるものと考えられる。

（１）ヨーロッパにおける憲法条項導入説

ＧＨＱ草案における“secrecy of communication”条項は、ピーター・ロウスト氏が、当時のヨーロッパ諸国における通信の秘密についての条項を採用したとする立場である。この立場については、上記で検討したとおりである。

（２）米国における連邦通信法６０５条等における議論を導入したと解する説

ＧＨＱ草案における“secrecy of communication”条項は、連邦通信法６０５条における通信傍受の禁止の議論（また、各州においても存在していた）における個人のプライバシー権を、憲法上の人権として認識して、表現の自由のなかで位置づけたという立場である。

（３）米国における「表現におけるプライバシー権」を導入したと解する説

ＧＨＱ草案における“secrecy of communication”条項は、ウォーレン＝ブランダイスで指摘されているいわば、「表現におけるプライバシー権」を憲法上の人権として認識してこれを記載したものと解する立場である。この場合、日本国憲法の草案の規定を眺める時に、むしろ、「言論と出版の自由は、保証される。これは、公務員、機関、運用を批判し、いかなる法律の施行、改正、廃止を強行する権利を包含する。~~（刑事的手続きの場合を除いて、）~~検閲は、なされてはならないし、意思伝達の機密性は、侵されない。」とそもそも訳されるべきであったのではないか、明治憲法以来の「信書の秘密」とは、異なった観点から、表現の自由の一環としての表現におけるプライバシー権の規定が提案されたと解すべきではなかったのかということもいえよう。

２　若干の検討

上述のような調査の結果として、わが国の憲法の「通信の秘密」の規定が、そもそもどのような意味をもったものとして制定されたかという点については、明確に位置づけることはできなかった。調査者らとしては、憲法における「通信の秘密」の規定が、意思伝達の当事者間における機密性という観点から、第三者の積極的な了知行為の禁止と意思受領

者の無権限での公表を禁止する趣旨があったのではないか、そして、現在の解釈が、憲法の起草者の意思という観点とは、かなたかけはなれたものになっているのではないかと考えてはいる[67]。しかしながら、その確証もえられたものではない。もっともすくなくても、憲法制定時の資料からは、通信の構成要素すべての保護に対して憲法上の保護が及ぶという考え方を支持する、積極的な根拠は、なんら、みつからなかったということはいえるであろう。そのような結果を前提に、現代の社会状況のもとでの「通信の秘密」をめぐる論点を考えることは一つの前進ということになるのではなかろうか。

[67] このような観点からする時、第２章で検討された各論点について、（１）憲法のいう「通信」は、隔地者間での連絡に限らない（２）通信の秘密の保障は、通信の内容にしか及ばない（３）意思伝達後も、意思伝達としてなされた内容であり、発意者が、公表を禁じた内容については、発意者は、内容を探索されることはなく、また、公表を強制されることはない（４）但し、その発意者の公表を禁じたという期待が保護されるかどうかは、社会的にその期待が合理的といえるかどうかにかかる、ということがいえるものと思われる。
　これらの各内容を詳細に検討するのは、次の機会ということになる。

第４章　検討とネットワーク管理・調査活動と「通信の秘密」への提言

第１　検討および今後の検討課題

１　検討結果について

ネットワーク管理・調査活動と「通信の秘密」の解釈について、現行の解釈においては、議論されていないことがきわめて多いこと、そして、ネットワーク管理・調査活動の実効性有る実現のためには、「通信の秘密」の解釈を現代社会の要請に応じて見直していかなければならないことは、明らかになったものと思われる。また、そもそも、「通信の秘密」の位置づけの根拠とされていた憲法の規定についても、その制定の過程を見た時に、そのような問題点に対して十分な回答を提起できるような経過で制定されたものではないこと、むしろ、いままでの「通信の秘密」の解釈が、もともとの起草者などの意識を反映していない蓋然性がきわめて高いことなども明らかになったところである。

２　残された検討課題

本稿は、ネットワーク管理・調査活動の実効性有る実現のためにそれらの活動を法的に位置づけるという問題意識のもとに、それらの解決の指針となるべき「通信の秘密」について、基本的に憲法の「通信の秘密」の解釈の観点から、調査をしたものである。しかしながら、「通信の秘密」と制定法との関係については、第２章の個別解釈の問題でみたとおり、昭和３０年代までは、通信の内容についての秘密を「通信の秘密」とし、それ以外の通信の構成要素およびその他の通信関連を「他人の秘密」と使い分けていた形跡が認められる。その後、いかなる理由によるのか、通信の構成要素のすべてが、「通信の秘密」によって保護され、そして、それは憲法の保護と保護される範囲が同一であるというように展開していったものと認められる。この経過については、今回の調査では、いまだ明らかにされなかった。なおも検討すべき課題ともいえるであろう。

３　提言にむけて

若干の課題が残されているとしても、ネットワーク管理・調査活動における「通信の秘密」のかかわりという問題点について、具体的な提言をなさなければならないし、また、その提言は、早急になされなければならないことは、明らかであろうと思われる。その場合には、比較法的な視点をも念頭に置き、ネットワークの安全性の確保とネットワークにおける通信利用者のプロイバシに対する合理的な期待との合理的な調和という観点から考察するものが望ましいものと考えられる。かかる立場から、提言をまとめると以下のようななるものとおもわれる。

第２　提言および具体的な検討が必要とされる内容

１　提言とのその意義

提言

「パケット通信における通信の秘密についての限界についての検討をなすとともに、プロバイダ等におけるネットワーク管理・調査等活動における適切な手順と適法性の限界について、総合的な検討をなし、その許容性・判断の視点・考え方とともにその活動の基準・

手続を明らかにする適切な方法が検討されるべきである」

このような場合、根拠規定がないとプロバイダ等においても、実際のネットワーク管理業務において、そのような活動ができないということも考えられ、特に、そのような管理活動における行為規範たる規定を設けて、活動時の判断の適法性を保持するという必要性があるため、特に以下の点について議論がなされなくてはならない。

（１） 通信の秘密についての限界

「通信の秘密」については、その「表現の自由」との関係、規定されている趣旨、客観的制限、時間的制限などについて、議論が不十分ではないかということは、明らかであろうと思われる。特に、外延情報といわれる部分についても、そもそもの「通信の秘密」という概念が及んでいるのかどうか、どのような条分上の根拠で、どのような法的な保護が及んでおり、その保護の限界はなんなのかという問題があるのである。その上に、パケット通信という手段のもとでは、その通信の外延情報は、通信関係者にとって傍受しうるものであり、また、その情報が、ネットワークの管理上、必要な情報であったりする。そのような通信手段への適用をも念頭に「通信の秘密」という概念を構成する場合において、「通信の秘密」という概念が、変容をとげるべきではないのかという点が議論されなくてはならない。

（２） 適切な手順と適法性の限界

ネットワーク管理・調査等活動と称されるネットワークにおける活動が、法的に許容されるべきものであることはいうまでもないことである。しかしながら、その一方で、通信の秘密の名のもとに保護されている通信の当事者のプライバシーに対する合理的な期待の保護との衝突ということも十分にありうる。したがって、かかる活動についてその限界を明らかにすることとは重要なことであろうと思われる。また、その活動の手順なども議論され、明らかになることも必要であろう。

（３）総合的な検討

本稿で検討したようネットワーク管理・調査等活動の位置づけというのは、法的な観点からは、ほとんどなされていないのと同様である。また、技術的にも、どのような行為をなしているかということについての全体的な考察という点からは、なおも不明確なところがあるということができるであろう。ここで、具体的な技術的な作業とその法的な位置づけを技術者、プロバイダ、法律家等の専門的な見地からなす共同作業が必要なものと考えられるところであり、まさに総合的な検討が必要なものと思慮されるところである。

（４）適切な方法

サービス・プロバイダーの一定の活動について明らかにするとして、どのような方法によって明らかにするかという点については、種々の手法が考えられるであろう。

一つは、例えば、「電気通信事業における個人情報保護に関するガイドライン」（平成１６年８月３１日総務省告示第６９５号）のように、告示という手段によって、プロバイダ

等のネットワークに関する観測・調査等の活動について、一定の基準を明らかにすることが可能性として考えられるであろう。

また、告示という手法によらなくても関係団体におけるガイドラインによって、その手順と限界を明らかにするということも可能なものと考えられる。現に、「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（案）」が、発表[68]されており、「自殺予告事案に対するプロバイダ等の適切かつ迅速な対応を促進することを目的として、①通信の秘密を第三者に開示する行為について、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、②自殺予告事案において、プロバイダ等が警察に対して発信者情報を開示することが緊急避難の要件を満たすか否かを検討する際の視点や考え方を示すとともに、③具体的な自殺予告事案における緊急避難の要件判断の基準及び発信者情報開示の手続を整理する」方向性が提案されている。ネットワークセキュリティ維持のためのプロバイダ等の活動は、従来の正当業務行為という判断の枠内に該当するのではないかと考えられるから、かかる関心から、「具体的なガイドライン」をまとめる方向での努力という手段も有効なものとして考えることができる。

2　検討されるべき内容

（1）　ネットワーク管理・調査活動における通信の消極的了知行為について

ネットワーク管理者等において、自己のネットワークに到達もしくは通過する通信について、そのトラフィック・データを了知することは、当然の行為である。ネットワーク管理の観点から、トラフィック・データの記録をなすことができることはいうまでもない。そして、その記録から、ネットワークの秩序に対する脅威をおよぼすと判断された場合には、コンテンツに対しても、それを積極的に了知する行為を認識することができるものとなる。消極的な了知行為は、正当化する基礎的情報を収集する根拠として位置づけられよう。

その消極的な了知行為によって得られる情報については、当然に電気通信事業者において、他人の秘密として、守秘義務が課せられるものの、了知自体は、法的な問題が生じないことは、明らかであるが、逆に、上記の秩序違反を分析するためには、通信の伝達に必要な情報以外の情報についても、記録する必要が生じてくる。そのような記録が、この消極的了知行為の範疇にはいるべきものであるのかどうか、いいかえれば、その消極的了知行為の概念の限界が、議論されるべきことになる。

（2）　ネットワーク管理・調査活動における通信の積極的了知行為について

（a ）積極的了知行為の概念

ネットワーク管理者等において、通信秩序に脅威をおよぼすと判断された場合には、自己のネットワークに到達もしくは通過する通信の情報を越えて、その発信者の外延情報をつきとめようとする場合がある。場合によっては、その内容についてまで調べない（ウイ

[68] http://www.telesa.or.jp/consortium/guideline_suicide_draft050825.pdf

ルスなどでパターンファイル該当などをみる場合）と、その通信の脅威の程度が判断されないこともあろう。それらの行為は、積極的了知行為ということになる。これらの行為が、通信秩序維持の観点から許容されるのではないかということについて議論がなされることが必要であろうと思われる。

（b ）積極的了知行為と正当化

では、上述のような積極的了知行為に該当する行為が、法的にどのように位置づけられるかという点について考えてみる。

ここで、米国法におけるプロバイダの通信についての了知行為が正当化される場合についてなどを参考とするとき[69]、トラフィック・データであるのか内容まで含むのかという点をも軸として以下のような点について、考慮すべきということができるものと思われる。

トラフィック・データに関していえば、(1) 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目的の有無（2）プロバイダの保護、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目的の有無（3）のユーザの同意の有無などで、正当な了知行為と判断することができるであろう。

また、通信内容まで含む場合に関していえば、 (1)通信の当事者または一方の通信当事者の事前の同意の有無 (2)プロバイダのサービスの遂行もしくは、権利や財産を保護する目的の有無などで、その内容についての了知の正当性が判断されるものと思われる。

これらの要素を判断要素とすることの是非や限界などが議論されるべきである。

（３） プロバイダにおける通信の一般的利用・秩序維持行為・第三者提供行為

（ａ）遮断・ルーティングの変更などの正当性について

了知した事実にもとづけば、一定の通信が、安全・安心なネットワーク運営という見地からみて、これを遮断するのが社会通念上適切だと判断されるような場合があったとして、それの遮断等をすることが許されるかどうかという問題がある[70]。この点については、迷惑メールに関する法律（改正１１条）の規定も参考になる。また、電気通信事業法におけ

---

[69] 詳細は、「付録 2 ネットワーク観測の法的問題に対する米国連邦法の示唆」参照

[70] この点で参考になるのが、郵便法における正規違反郵便物に関する取扱の法的制度である。現行郵便法は、郵政省は、郵便物引き受けの際、郵便物の内容たるものの種類・性質につき差出人に申告を求め（同法４０条１項）、郵便物が申告と異なり本法または本法に基づく省令に違反して差し出された疑いなるときは、差出人に開示を求めることができる（同法４０条２項）。また、取扱中にかかわる郵便物が本法または省令に違反して差し出された疑いなるときは、差出人または受取人に開示を求め（同法４１条１項）開示を拒否された時、または開示を求めることができない時は郵便物を開披できる（同条２項）と規定している。郵便物の場合には、内容物によっては、郵便の配達等の業務の円滑な遂行に支障を生じうる場合があるのでそれに対応する規定ということになる。

る提供義務（電気通信事業法１２１条）の規定の解釈[71]も関係することになる[72]。

また、ネットワーク秩序の維持のために、いわゆるルーティングを変更する場合もある。具体的には、特定のサイトに対する DOS 攻撃がなされている場合などに、そのパケットをネットワーク上で廃棄している。

これらの遮断・ルーティングの変更などが、一定のネットワーク管理行為として許容されるものと考えられるが、その許容される場合やその個々の手順などについての議論が望まれるものと思われる。

（ｂ）第三者への任意での提供行為について

（ア）プロバイダ等相互間での情報共有行為について

この場合、どの程度までの具体的な情報提供行為が認められるべきか、また、望ましいのか、技術的・法的な検討が必要になるものと思われる。

（イ） 一般のネットワーク管理者間での情報共有行為について

また、上述の情報共有行為は、プロバイダ相互間に限るものではない。大学や一般企業のネットワーク管理者間に対しても情報共有がなされる必要があるかもしれない。また、重要インフラ指定事業者等においては、情報共有の必要性が高いかもしれない。このような場合の法的な意義などについても検討がなされる必要があるであろう。

また、リアルタイムでの対応のための情報共有という観点以外にも、将来の対応を検討するためにそのような情報共有が必要とされることもあるであろう。

（ウ）学術的な観点からの情報共有

学術的な観点からの分析・情報共有・発表なども必要とされるものと考えられる。これらの場合の限界というもの考えなければならないものである。

（ｃ）法的な照会権限のある者からの照会についての手法の再検討

（ア） 法執行機関に対する開示について

ISP が、ネットワークに対する攻撃を関知した場合に、場合によっては、法執行機関と協力して、攻撃犯人の追求などに助力をし、また、その保有する情報を提供する必要が生じることと思われる。現実としては、警察当局からの要請があり、令状をまって、ISP がそれ

---

[71] 電気通信事業法 121 条１項は「提供義務」として「認定電気通信事業者は、正当な理由がなければ、認定電気通信事業に係る電気通信役務の提供を拒んではならない。」としている。この提供義務については、役務の提供の申し込みを受けた場合の承諾義務と役務の継続提供義務の双方を含むものと解されている。そして、「正当な理由」とは、「天災、地変、事故等により、電気通信設備に故障を生じ役務提供が不能の場合、役務を契約約款に違反する条件で受けようとする者または料金滞納者に対する場合、その申し込みを承諾することにより他の利用者に著しい不便をもたらす場合、正常な企業努力にもかかわらず、需要に対して速やかに応ずることができない場合等である。」とされている（逐条解説電気通信事業法９９頁）。この正当な理由のうち、他の利用者に著しい不便をもたらす場合とネットワークの安全性確保との関係についての考察が必要になるものと思われる。

[72] その一方で、郵便法における第１４条（郵便禁制品）、第１５条（郵便約款による差出の禁止）、第４２条（危険物の処置）との比較の問題もある。

に協力するというのが、実態であると思われるが、米国の制度を参照するかぎり、場合によっては、むしろ、ISP が、法執行機関に対して、そのイニシアチブで、協力を求める場合も十分に考えられ、そのような場合について、「通信の秘密」との関係で、適正な業務執行と判断されるのはどのような場合か、というのを明らかにしておく必要があるものと考えられる。また、有線電気通信法１３条の２においてさだめられているいわゆる「機械的不完了呼発信罪」において、プロバイダは、法執行当局に対して、協力することもありうるのであり、そのような場合についての基準も必要になろう。

また、逆に法執行機関からの照会については、令状によって初めて通信の外延的情報を明らかにすることとされているが、約款などにおいて捜査関係事項照会書に対して開示し得る場合を定めることを可能とすべきではないかということなどについても総合的な検討などが必要とも思われる。

（イ）行政権によるネットワークの安全等確保のための外延的情報に関する開示制度の妥当性について

通信の秘密のうち、外延情報についての位置づけが、本稿検討のとおりであり、本来の通信の秘密の保護の範疇から別個のものと認識される可能性があるのであれば、迷惑メール対応や情報セキュリティ対応のために、通信の内容にかかわらない外延情報を行政権が、しかるべき手法によって、取得しうるという制度の構築も可能なことになる。現に、迷惑メール対策についても、むしろ、そのような制度が必要ではないかという意見が明らかにされている[73]。

この考え方については、「行政機関に対し電子メールの送信者の契約者情報を開示することは、通信の秘密を保護する観点から原則として認められませんが、今回の法改正で特に送信者を特定することが困難な送信者情報を偽った広告宣伝メールの送信に直罰を導入することで、警察等の捜査機関による捜査が行われることになり、裁判所の発行する令状により契約者情報を開示することが可能となります。」とされているが、捜査機関による捜査が、実効性あるものとなるかどうか、という点については、疑問なしとしない。通信の秘密とネットワークの安全・安心な管理という観点からは、そのような制度の構築の可能性というのも念頭において議論をすることが可能かもしれないところである。

---

[73] 「措置命令等の行政処分について(p.8)」についてのパブリックコメントでは、「行政処分の執行の上で，契約者等の氏名・住所を総務省が調査できない問題が指摘されています。違法迷惑メールの送信者に関する情報を総務省の求めに応じて開示することが可能な枠組みを設けることができれば，事業者として適切かつ確固たる法執行に協力できるものと考えます。」（日本インターネットプロバイダー協会）とか、「措置命令等の行政処分について，ISP 事業者が契約者情報等を総務省に提供できるようなスキームを考えるべきです.」とされているところである（EditNet 株式会社）。

付録１　ベアテ・シロタ女史に対する質問事項（原文・英語）

ベアテ・シロタ　様
（ファクシミリにて）
（番号省略）

2005 年 6 月 10 日

シロタ様

（省略）

私は、宇都宮大学講師で、憲法の「通信の秘密」の条項の調査に従事しています。私と吉田一雄清和大学助教授は、憲法草案の観点から、当該条項を分析しようとしています。

今日においては、通常の解釈論者は、憲法２１条の規定は、言論と表現の自由の一環として定められており、世界できわめて珍しいものであるとしています。私達は、ウォーレンとブランダイスの有名な「プライバシーの権利」の論文が、通信の秘密の条項に影響を与えたのではないかと考えています。もし、そうだとすれば、「通信の秘密」は、表現の自由のプライバシーの側面として解釈されるべきであり、細かい点についての解釈を変更しなければなりません。

それそえに私達は、以下の点について調査したいと思っています。
(1)私達は、表現の自由の条項が Pieter K.Roest 博士によって起草されたと計測しています。これは正しいでしょうか。
(2)当該条項の起草に際して参照された文献について知っていることはありますか。
(3) 「日本の憲法についての準備的研究と提案のレポート」においプライバシーの権利の導入が示唆されていましたが、委員会において、その導入について議論はなされましたか。
(4)表現の自由の条項の導入に関連してなにかご存じのことはありますか。

高橋郁夫（サイン）
[資料]（省略）

付録２・ネットワーク観測の法的問題に対する米国連邦法の示唆

弁護士高橋郁夫

［問題点の所在］

ネットワーク管理、障害検知ならびに対策の検知から、ネットワーク観測がなされる。ここで、「ネットワーク観測」とは、ネットワーク関係者が、ネットワークの通信に関する情報を知得する行為74をいう。このような観測行為が、利用者との関係で、法律上、なんからの問題を惹起しないのか、また、観測結果の利用など具体的な運用行為について、どのような行為が法的に許容し得るのかという点について考察することが必要となる。このような問題意識を基にするとき、観測行為およびその結果の利用行為の法的位置づけについて、具体的な制定法上の規定をおいている米国連邦法の規定を参考にすべく、その基礎的な資料を提供すべき必要がある。

特に米国における観測行為についての許容性の法的な根拠をも調査し、我が国の参考にするのが、本稿の目的である。

［考察］

第１　米国における通信の機密性の位置づけ

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。

---

74 ここでは、便宜上、取得するデータが、コンテンツに関連するものであると、しないものであるとを限定しないで論じることとする。

２　「電子的記憶」と「電子的監視」

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、ある意味で不明確ということになる。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。なぜならば、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。従って、この通信途上のデータについては、制定法による規定が優先することになり、憲法問題は、発生しないものと認識されることになる。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。特に米国法のもとでは、18U.S.C.§2510(17)において「電子的記憶」として「電気送信に付随する有線または電気による通信の一時的、中間的な蔵置」または、択一的に「そのような通信のバックアップ保護の目的のための電気通信サービスによるそのような通信の蔵置」と定義されており、この概念が、中間的な地点での保存データに対する法的保護を考えるのに際して、きわめて重要な意義をもってくることになる。

第２　「電子的な記憶」に関する法的な保護

「電子的な記憶」に関連して、プロバイダに保存された通信データと「プライバシーの合理的期待」に関する法的な論点は、「自発的開示」か「強制的開示」かといういわば法執行機関と情報とのかかわりという観点と「通信に関する情報の格付け」という観点から議論がなされる。しかも、この「通信に関する情報の格付け」については、①それ自体「基本加入者、セッションおよび請求情報」か、「他の取引およびアカウント記録」か、②「アクセスされた通信」か、「検索されていない通信」かという観点から論じられている。この点についての要領のよいまとめは、以下のとおり[75]である。

	自発的開示の許容性		開示を強制するメカニズム	
	公共のプロバイダ	非公共のプロバイダ	公共のプロバイダ	非公共のプロバイダ
基本加入者、セッションおよび請求情報	§2702(c)の例外の適用のない限り、政府に対しては、不可［§2702(a)(3)］	可［§2702(a)(3)］	提出命令、2703(d) 裁判所命令、捜索令状	提出命令、2703(d) 裁判所命令、捜索令状

[75] （注 31）米国司法省マニュアルの「III 電気通信プライバシー法　F　クイック・リファレンスガイド」による。

			[§ 2703(c)(2)]	[§ 2703(c)(2)]
他の取引およびアカウント記録	§ 2702(c)の例外の適用のない限り、政府に対しては、不可 ［§ 2702(a)(3)］	可 [§ 2702(a)(3)]	2703(d) 裁判所命令、捜索令状 [§ 2703(c)(1)]	2703(d) 裁判所命令、捜索令状 [§ 2703(c)(1)]
プロバイダに残るアクセスされた通信（明けられた電子メールおよびボイスメール）および他の記録されたファイル	§ 2702(b)の例外の適用のない限り、不可 ［§ 2702(a)(3)］	可 [§ 2702(a)(2)]	通知ありの提出命令、2703(d) 裁判所命令、捜索令状 [§ 2703(b)]	提出命令、ＥＣＰＡの適用なし [§ 2711(2)]
電子メールおよびボイスメールを含む検索されていない通信（電気的記録 180 日間を超える）	§ 2702(b)の例外の適用のない限り、政府に対しては、不可 ［§ 2702(a)(3)］	可 [§ 2702(a)(2)]	通知ありの提出命令、2703(d) 裁判所命令、捜索令状 [§ 2703(a,b)]	通知ありの提出命令、2703(d) 裁判所命令、捜索令状 [§ 2703(a,b)]
電子メールおよびボイスメールを含む検索されていない通信（電気的記録 180 日間以下）	§ 2702(b)の例外の適用のない限り、政府に対しては、不可 ［§ 2702(a)(3)］	可 [§ 2702(a)(2)]	捜索令状 [§ 2703(a)]	捜索令状 [§ 2703(a)]

ここで、「公共の」プロバイダというのは、「公衆の利用が可能である」プロバイダという意味であり、特定の企業においてその従業員のみが利用できるようなものは、「公共の」プロバイダではないと判断されることになる。ここでは、①私的なプロバイダであれば、その情報を法執行機関に対して提供することが可能であること、②公共のプロバイダであっても、例外の場合（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、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、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、チャイルドポルノに関する法律で開示を委任している場合、受取人の同意をもってな

される場合など」）については、法執行機関に対する開示が認められること③プロバイダに対して開示を強制する場合でも、いわゆるトラフィッグデータ等に関する部分では簡易な手続きで開示が認められること、などの特徴を把握しておくことは有意義であろう。

第３　「電子的監視」に関する米国法の一般的な議論

１　電子的監視と法律の定め

電子的監視とは、リアルタイムで通信に関する情報を覚知する行為をいう。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。

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)）。大雑把にいえば、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。

一方、「タイトルⅢ」は、一定の例外を除いては、基本的には、通信への参加当事者でない第三者（政府などの）が、プライベートな通話を「電気、または機械その他の装置」を使用して傍受することは禁止している（18U.S.C.§2511（1））。この禁止の範囲がかなり広いことである。そして、一方で、これに対する例外も種々の場合に認められている。

２　プロバイダの電子的監視についての一般的規律

法執行機関やネットワークプロバイダが、ネットワーク観測をなしうるか、また、なしうるとして、それはどのような情報であるかという論点について検討する。

（１）トラフィック・データに関して

まず、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、観測をなしうることになる。政府機関が、みずからプロバイダとして、そのような観測をなしうるかという点については、さらに別章で検討する。

（２）通信内容まで含む場合

一方、プロバイダが、リアルタイムで通信に関する情報を、通信内容までを含んで覚知しうるかという点については、タイトルⅢに定める各種の例外の規定がきわめて参考になる。このようなプロバイダのリアルタイムでの観測行為に関連するタイトルⅢ例外としては、①「同意」例外、§2511（2）(c) －（d)、②「プロバイダ」例外、§2511（2）(a)（i)、③「コンピュータ侵入者」例外、§2511（2）(i) があげられる。これらの例外を説明すると

（ア）「同意」例外について

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。これについては、ネットワークでの運用に関しては、黙示の同意原則に基づき、適切に”バナーされ”ているコンピュータネットワークをモニタリングすることは許されるということが重要なこととなる。また、だれが通信の「当事者」かということが問題になる。いわば、通信の最終目的者が、通信の当事者であることは間違いがないとしても、その通信の途上でいわば「踏み台」にすぎない場所での通信の傍受は、その「当事者」が通信を傍受していることになるのかどうかということである。米国においては、いくつかの裁判所[76]は、ユーザが、所有者のシステムに通信を行うとき、コンピュータシステムの所有者が「通信の当事者」という文言にあたるといえると判示している。

しかしながら、この「当事者」という文言の解釈については、困難が伴うものと考えられる。「『通信の当事者』である『人』を（もちろんハッカー自身を除いて、）見つけることは—（完全に形而上学でなければ）困難な仕事といえよう。これらの困難のために、捜査官と検察官は「通信の当事者」同意例外によるときには慎重でなければならない。(d）項で論じるコンピュータ侵入者例外が、通信のモニタリングに対するより確実な基礎を提供する。」とされる[77]ところでもある。

（イ）「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

---

[76] United States v. Mullins, 992 F.2d 1472,1478（9thCir.1993）（コンピュータシステムの所有者が、通信の当事者であるので、§2511（2）(d）の同意例外によりコンピュータシステム不正使用のモニタリングが許されると述べている)、United States v. Seidlitz,589 F.2d 152,158（4thCir.1978）（傍論において、会社従業員が、権限のないユーザが、ハイジャック管理者アカウントを使用し、システムへ侵入しているのを傍受したとき、攻撃されているコンピュータシステムを賃貸して、メンテナンスする会社が「どの点から見ても通信への当事者」であったと結論を下す）を参照。

[77] 司法省マニュアル「IV 通信ネットワークにおける電子的監視・D 通信傍受法、(「タイトルⅢ」）18U.S.C.§§2510-22・3.「タイトルⅢ」の例外・b」通信当事者の同意 18U.S.C.§2511（2）(c) -(d)」参照

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点に注意が必要である。そのために、「捜査官と検察官は、プロバイダ例外の下におけるプロバイダによって行われるモニタリングの結果を受け入れることについては、慎重なアプローチを取るべきである。」とされ、むしろ、法執行機関は、このような場合は、コンピュータ侵入者例外に依拠すべきであるとされるのである。また、米国においては、航空宇宙局、郵便および軍隊などの連邦政府機関には、大規模なコンピュータネットワークとかなりの法執行機関の配置（民間機関に一般査察局があり、および軍事における刑事上の調査サービスの場合における査察局）がなされており、その場合には、この例外規定が容易に適用される危険性があるが、裁判所は、民間のネットワークの場合になされる法執行の関心とプロバイダの関心との峻別に基づいた厳格な適用をすると考えるべきであり、むしろ、法執行機関においては、この例外の安易な利用については、注意すべきであるとされているところである。

（ウ）「コンピュータ侵入者」例外

18U.S.C.§2511（2）（i）は、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[78]。

これは、法執行機関が、コンピュータに対する侵入があるとわかった場合に、その侵入者の行為を突き止めるのに際して、リアルタイムで傍受をなしうる権限はどこから発生するのかということを定めた規定である。

第４　米国における具体的な「ネットワーク観測」行動をめぐる根拠と正当性

[78]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。PATRIOT Act §§217,224,115 Stat.272,290-91,295（2001）参照。

の議論

１　問題の所在

米国におけるネットワーク観測についての抽象的な法的議論は上述のものだとして、我が国での「検知ネットワークシステム」の活動などに代表されるネットワーク観測システムに該当するようなシステムが、米国において実際にネットワークの安全性を維持するために活動していないかどうか、また、活動している場合に、その正当性について法的な議論は存在しないのかという点が問題になる。

２　「ネットワーク観測」行為の一般的な正当性

（１）正当性の判断枠組み

「ネットワーク観測行為」を想定した場合に、その観測行為によって得られる情報が　、「ルーティング、アドレスまたは信号情報」に限られる場合であるかどうかということになる。限られるのであれば、その主体が、電気・有線通信サービスのプロバイダである場合には、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の目的であれば、許容されることになる（前述のペンレジスター／逆探知装置の設置に関する 18U.S.C.§ 3121（b）参照)。もっとも、侵入を試みているとか、実際にどこからどのような侵入を試みたかという点については、上述の情報にかぎられない場合もあるものと思われ、その際については、前述のいわゆるタイトルⅢ例外の問題になる。

いわゆるコンテンツの要素を含む情報の観測を考える場合には、観測の主体ごとに観測行為の正当化根拠を考えることになる。主体が法執行機関ということになれば、「同意」例外または「コンピュータ侵入者例外」によって正当化されるか、特別の正当化根拠によらなければ、自ら観測行為をなすことはできないことになる。一方、主体がプロバイダであったとしても、それが、政府機関であり法執行機関が配置されている場合については、それについて、プロバイダ例外によって、プロバイダに基づいてなされる観測が許容されるとしても、法執行の関心によって観測がなされる場合には、かかる正当化が適用されないことに注意すべきことになる。

次に、プロバイダが取得した情報について、それを自発的に開示することの法的な許容性という問題があることになる。「公共の」プロバイダについては、法の定めがない場合には、自発的な開示が許容されないことになる。一方、かかる公共ではないプロバイダについては、自発的な開示が許容されることになる。

（２）特別の正当化根拠

もっとも、ネットワークに関する観測行為の根拠という点についていえば、タイトルⅢの規定意外に、（１）The Foreign Intelligence Surveillance Act of 1978 と（２）外国における諜報活動の法理の二つの根拠から、政府機関が観測行為をなしうる点に留意が必要になる。（１）は、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を

許容するものである。（２）は、政府の行為として外国との通信を傍受するに際しては、何らの制定法による制限はないということである。

３　FIDNET 構想と 911 以降の「ネットワーク観測」体制

具体的な政府の「ネットワーク観測」構想という点についていえば、そのような構想を正面から提案している FIDNet 構想を分析し、それから、その後の議論の進展を見ていくのがきわめて参考になる。

（１）FIDNet 構想[79]

これは、1999 年 6 月に、 General Services Administration が、政府機関に対するサイバー攻撃に対して、単一の分析および対応センターを構築するための案を提案したものである。 この FIDNet 構想は、個別の機関が単独でそれぞれ対応するというよりも、民間機関が、共同でサイバー攻撃に対して、対応し、セキュリテヤィ事案に対応するというものである。FIDNet 構想事務局は、GSA の連邦コンピュータインシデント対応部隊におかれ、民間の侵入検知システムからの報告をリアルタイムで分析し、政府への攻撃がないかどうかを判断しうるようにと考えられたものである。そして、この FIDNet 分析センターは、犯罪に該当する攻撃かどうかを判断し、情報は、FBI に転送されるというものであった。

この提案は、検討中の案が漏洩したものであるが、特にオンライン人権団体などからプロイバシを侵害するものであるとの激しい議論が巻き起こった。この構想の検討の際に、連邦検事補であった Ronald　Lee 氏が CIAO の Jeffrey　Hunker に対してこの構想の適法性について検討した旨を手紙で送ったことがある。この手紙によれば、①政府機関は、それぞれ、サービスプロバイダであり、自分のネットワークをモニターする事ができるとしても、GSA が、すべての連邦政府の「サービスプロバイダ」と言えるわけではない、②一方当事者の同意の法理によって適法なものとなるとしても、政府関係サイトへのビジタに対して、モニタリングに服することがあるという警告がかならずあるとは限らないことが指摘されている[80]。

（２）情報システム保護国家計画（National Plan for Information Systems Protection[81]）

そして、上記の FIDNet 構想は、形を替えて、結局、「情報システム保護国家計画（National Plan for Information Systems Protection）」（Version 1.0 An Invitation to a Dialogue）にまとめられている。この国家的構想は、ＰＤＤ63 でもふれられているように「合衆国の資産である重要機能に対する妨害、操作を最短に、めったにない、管理可能な、

---

[79] 批判的な分析として「Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry 」by Michael J. O'Neil*James X. Dempsey**February 10, 2000
（http://www.cdt.org/security/fidnet/oneildempseymemo.html ）

[80] “ Memo from Ronald D. Lee ”（http://www.epic.org/security/cip/lee_memo.html）および前出・（注 79）脚注 21

[81] http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf

独立した、最小限度のものにすること」をゴールとするものである。そのために、「準備と予防」「探知と対応」「強固な基礎を築くこと」という目標とする。そして、その目標のために
「準備と予防」のためのプログラムとして
①「重要インフラ資産の特定・相互関連性の分散および脆弱性の認識」
「探知と対応」の目標のためのプログラムとして
②攻撃および無権限による侵入の探知
③堅固な諜報および法執行能力を発展し、重要情報システムを法にしたがって防衛すること
④適時に攻撃の警告および情報を共有すること
⑤対応、再構築、回復のための能力を構成すること
「強固な基礎を築くこと」のプログラムとして
⑥プログラム①ないし⑤の調査発展を支援すること
⑦情報セキュリティ専門家を多数訓練し雇用すること
⑧国民にサイバーセキュリティ改善の意識を高めること
⑨プログラム①ないし⑧を支援する立法および予算を採用すること
⑩構想のすべてのステップおよびコンポーネントにおいて、市民の権利、プライバシの権利および保有するデータ保護の権利を十分に確保すること
が、採用されている。

この構想では、ネットワーク観測行為は、上記の「②攻撃および無権限による侵入の探知」のプログラムの中で論じられている。このプログラムは、高度なファイアウォール、侵入検知モニター、異常行動検出装置、企業規模の経営システムと悪意あるコード・スキャナーなどの設置により、センシティブなコンピュータシステムに対して多層をなす保護を準備するものとされる。そして、連邦のシステムを保護するために、コンピューター・セキュリティ作戦センター(最初は、国防総省、次に連邦侵入検知ネットワーク[FIDNet]が他の連邦の機関と連携)は、これらの検出デバイスから警告を受け取り、コンピュータ・エマージェンシー・レスポンス・チーム(CERTs)や他の組織とともに、攻撃を分析して、そしてサイトが攻撃をやっつけるのを手伝うとされている。

さらに、細かくみると「侵入検知モニターと防御的探知システムの設置」と「侵入検知モニターのネットワークシステムの構築」の二つの面が提唱されている。「侵入検知モニターと防御的探知システムの設置」においては、ファイアウォールの双方への侵入検知システムの設置をすること、権限者に対するアクセスおよび行動ルールと異常行動特定のためのスキャンプログラムを設置すること、企業規模のマネジメントシステムの制定によりシステムの特定をなしえ、決定をなしうるようにすること、アクセスおよび行動ルールを実現し、セキュリティパッチを適用しうるようにすること、悪意あるプログラムに対する分析技術を高めることなどが提唱されている。また、「侵入検知モニターのネットワークシス

テムの構築」においては、民間機関における防御的探知システムの連携の重要性が強調されている。

この種の探知システムは、政府ネットワークの重要なノードにおいて、自動的もしくは、人間の管理によるモニタリングシステムによってなされている。そして、米国においては、このような関連したシステムは、三種のコンポーネントからなりたっており、FIDNet は、その一つとして位置づけられるという。その三つとは

（ア）国防総省連合タスクフォース－コンピュータネットワークディフェンス（JTF-CND）

これは、2000 年時点で既に構築されており、重要な防衛ネットワークをモニタリングしており、侵入・攻撃後の再構築を援助している。

（イ）連邦侵入検知ネットワーク

これは、国防総省のシステムを参考にしたもので、GSA によって実装され、運営されるものである。実際の侵入等が発見された場合には、FedCIRC が、NIPC と連携して対応することになる。

（ウ）国家安全インシデント対応センター（NSIRC）

これは、JTF-CND、FIDNet、NIPC に対して、攻撃侵入の隔離、封じ込め、解決のための専門的援助をなす組織である。

なお、この国家構想においては、前述のような人権団体からの批判を意識したものか、プライバシの権利等についての配慮がなされている。まず、FIDNet は、民間のモニタリング情報の連携という面は消え、民間システムや非連邦システムのトラフィックをモニターするものではないこと、FBI や他の法執行機関によって運営されるものではないことなどが強調されている。そして、司法省の調査によれば、電気通信プライバシー法の規定に反するものではないとされており、また、他の連邦機関をも含めた法的調査がなされている[82]ということであった。

（3）NCSRS 構想

その後、2003 年２月に発表された「The National Strategy to Secure Cyberspace.」では、 上述のシステムは、「国家サイバースペースセキュリティ対応システム（A National Cyberspace Security Response System、以下ＮＣＳＲＳという）」の一つの局面へと発展している。このＮＣＳＲＳは、国土安全保障省（Department of Homeland Security、以下、DHS という）が、分析と警告に際して、調整役を務める民間・保政府の構想であり、国家的な重要性をもったインシデントのマネジメント、政府システム・民間インフラの継続的運営、組織間の情報の共有などを目的とするものである。

これは、「分析」「警告」「インシデント・マネジメント」「対応／回復」の各局面からなり、政府・非政府の各組織の協力的なネットワークを目指そうと言うものである。

---

[82] この法的調査が発表されたのかは、不明である。

これらの各段階における要素をあげると以下のようになる。
「分析」は、DHS 分析センターが、中心となって、戦略グループ、戦術グループ、脆弱性評価などの要素が入ることになる。「警告」は、DHS インシデント作戦センターが中心となって、サイバー警告および情報ネットワーク、ISAC などの要素が入ることになる。「インシデント・マネジメント」は、DHS インシデント・マネジメント体制が中心となり、連邦の調整、民間、州および地域の調整がこの要素となる。「対応／回復」は、国家対応緊急計画が中心となり、連邦のプラン、民間プランの調整などがこの要素となる。
この中で、上述のような「ネットワーク観測」は、「分析」の観点の内の個別の侵入の分析に関わる論点、すなわち、「戦術分析」として、また、「警告」における「サイバースペースの健康についての情報共有」「サイバー警告・情報ネットワークの拡充」の論点として意識されることになる。この報告書からは、あまり明らかではないが、情報共有・分析センター（ＩＳＡＣ）[83]と、DHS の連絡窓口、そして、これらのネットワークである Cyber Warning and Information Network（CWIN）との連携が強調されているところである。

（4）EWAN 構想など

2003 年 10 月には、Global Early Warning Information System(GEWIS)プログラムが開始された[84]。これは、DHS によって、運営されているもので、 インターネットのトラフィックフロー、レイテンシ、活動などを測定するものである。このプログラムの目的は、内容よりもネットワークのパフォーマンスにあるという。

2003 年 12 月には、国家サイバーセキュリティサミットがカリフォルニア州サンタクララで開催され、これらの構想のなかで重要な位置を閉める民間と政府との重要インフラをより安全にするために、National Cyber Security Partnership という団体[85]が設立された。このパートナーシップのなかに設置された 5 つのタスクフォースの 1 つとして早期警告タスクフォースがある。このタスクフォーシスは、2004 年 3 月 18 日に、報告書[86]を提出し、早期警告連絡ネットワークを提唱している。この報告書の内容が今後どのように米国政府の方向性に影響をあたえていくのか注目されるものといえよう。
また、実際の US-CERT Operations Center においての活動が報告[87]されており、24 時間

---

83 PDD63 によって 1998 年に設立された特定のセクター（水道、交通、エネルギー、IT など）の脆弱性、脅威、侵害などについての情報共有および分析センターをいう。
84 なお、2003 年 1 月 31 日ワシントンポストによれば、NCS によって、2001 年の 911 以降すぐに開始されたと報道されている
(http://www.securityfocus.com/printable/news/2205)。
85 http://www.cyberpartnership.org/
86 http://www.cyberpartnership.org/init-early.html。なお、この報告書においては、ネットワーク観測に関係する団体等の一覧が記載されている。

87 Lawrence C. Hale “DHS/National Cyber Security Division －Meeting the Cyber Security Threat ” （http://www.richtech.com/events/Hale.ppt）

年中無休のベースでの活動がなされているとのことである。

4 米国における「ネットワーク観測」行為の法律問題の議論について

上述のような実際の動きを見た時に、正面から、「ネットワーク観測行為」の適法性が議論されたのは、FIDNet 構想のときのみであるということができるかもしれない。しかも、その後は、情報システム保護国家計画の時点において、法執行機関への連絡という側面が弱まっていること、また、民間機関内での観測という側面が弱まっていることなどから、表立った適法性の議論は、今では行われていないようにも思われる。特に、ＮＣＳＲＳ構想以降については、民間と政府の協力による早期情報共有という観点が強化されており、政府機関による情報収集という観点が後退している点からすれば、そのような米国の状況も十分に理解できることになる。

米国法の解釈としては、米国の「ネットワーク観測行為」のうち、政府機関内のものは、政府機関内においてのネットワーク管理のためのトラフィックに対する観測であり、かつ、それ自体がプロバイダ関心からなされるという観点から、十分に正当化される(また、同意を根拠としうる可能性があることは前述した)ということになろう。民間のプロバイダについては、制定法のタイトルⅢ例外から十分に説明が尽くし、また、安全性侵害があると信じる相当の理由のある場合の政府機関への提供も合理的なものとして説明がつこう。もっとも、かかる考察は、大雑把なものといわざるをえず、情報システム保護国家計画でふれられている法的な面での調査書の発表の有無が現時点で不明なのが悔やまれるところである。