警察政策学会資料　第94号
平成29（2017）年 6 月

米国における行政傍受の法体系と解釈運用

警察政策学会

テロ・安保問題研究部会

米国における行政傍受の法体系と解釈運用

日本大学　危機管理学部教授　茂田　忠良

目　次

Ⅰ　本稿の目的

行政傍受（国家安全保障のためインテリジュンス機関が実施する通信傍受）[1]は、20世紀に入り無線や有線の通信技術が発達すると共に発展したが、何れの国においても、国家安全保障上の必要から秘密裡に行われ、当初は憲法や法律との整合性は殆ど意識されることなく実施されていた。

やがて、20世紀も末に近づくと、合憲性や合法性が強く意識されるようになって、米国では行政傍受と憲法修正第4条の関係が議論されるようになり、1978年には行政傍受の一部を規制する対外諜報監視法[2]が制定された。しかし、行政傍受の実態は依然として秘匿されているために、それに係わる法体系や解釈運用は必ずしも明瞭でない。

本稿では、先ず、米国において行政傍受の開始から20世紀半ばまで、その合法性がどのように意識され扱われてきたかを分析する。次に、1978年に対外諜報監視法が制定されてから現在までの、行政傍受法制の基本構造、修正第4条と行政傍受の関係、及び行政傍受情報の捜査利用、更にメタデータの取扱の問題を取り上げ、米国における行政傍受の法体系及びその解釈運用の実態と発展過程を明らかにしようとするものである。

本稿の分析で使用した主な資料は、米国の法令、最高裁判所判決、対外諜報監視裁判所の各種判決、行政傍受に関する各種政府資料（公式公表文書、情報公開要求に基づく開示文書、漏洩文書）である。

なお、本稿は『危機管理研究』創刊号に掲載した拙稿「米国における行政傍受の法理と運用」（主として本稿のⅥ、Ⅶ、Ⅷに対応）[3]に大幅に加筆したもの（特に、Ⅲ、Ⅳ、Ⅴ、Ⅸは新規に執筆）である。

---

[1] 一般に、司法傍受は犯罪捜査のため裁判所の令状を得て実施する通信傍受、行政傍受は国家安全保障のため行政機関内の手続で実施する通信傍受とされるが、本稿では、（特別裁判所の関与するものも含め）国家安全保障という行政目的のためインテリジュンス機関が実施する通信傍受を論考の対象とする。従って、論考の対象となる通信傍受は主として、対外諜報機関、就中コミント機関である国家安全保障庁及びその前身機関による米国内における通信傍受、並びに（セキュリティ・サービス機関としての）FBIによる国家安全保障のための通信傍受である。

[2] Foreign Intelligence Surveillance Act of 1978.　本稿では「対外諜報監視法」と訳し、略称として「監視法」と言う。なお、本稿ではIntelligenceの訳語として、「インテリジュンス」又は「諜報」を使用する。Informationとの混同を避けるためである。

[3] 茂田忠良「米国における行政傍受の法理と運用」『危機管理学研究』創刊号（日本大学危機管理学部危機管理学研究所、2017年3月）78－99頁。

Ⅱ　行政傍受に関係する憲法規定

行政傍受に関係する主な米国憲法規定は、第 2 章第 1 条と修正第 4 条である。修正第 4 条は当然であるが、第 2 章第 1 条との関連に注目する必要がある。先ず、その概要を確認する。

1　憲法第 2 章第 1 条～大統領の国家安全保障のための権限

大統領の行政権には、憲法上、国家安全保障のための広汎な権限が含まれると解釈されており、インテリジェンス活動はその一部と理解されている[4]。

即ち、憲法第 2 章第 1 条の規定により、大統領の就任時の宣誓文には″I will…to the best of my ability, preserve, protect and defend the Constitution of the United States." （私は、・・・全力を尽くして、合衆国憲法を保持し、保護し、擁護します。）の句が含まれるが、「合衆国憲法を保持し、保護し、擁護する」こと、即ち国家の安全保障は、大統領の任務であり権限であることを示していると解されている[5]。そして、行政府は、国家安全保障のための諜報活動は議会の制定する法律の根拠なしに行うことができると解釈して行ってきた[6]。実際、現在米国における諜報活動についての基本規程は、大統領命令第 12333 号「合衆国諜報活動」[7]である。

第 2 次世界大戦前から戦後に至るまで、米国政府は、対外インテリジェンス（諜報）のためにも、国内のセキュリティ（安全保障）対策でも行政傍受を広汎に、法律の授権なしに、且つ裁判所の令状なしに、実施してきたのである。

但し、国家安全保障のための活動についても、連邦議会の制定した法律があれば、拘束力を持つのは言うまでもない[8]。そのため、修正第 4 条との関係が意識される前においても、行政傍受が既存の法律に抵触する可能性について、行政府の中で議論され

---

[4] US White House, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 12 December 2013, 64, 69.　Accessed 29 August 2014, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[5] United States v. United States District Court, 407 U.S 297(1972) at 310. --James G McAdams III, *Foreign Intelligence Surveillance Act (FISA): An Overview,* (2007), 2.　Accessed 29 August 2014, http://www.flect.gov/training/programs/legal-division/downloads-articles-and-faqs/articles/foreign-intelligence-surveillance-act. html.

[6] Id.

[7] US EO 12333 United States Intelligence Activities, amended through 2008.

[8] 国家安全保障のための活動についても、連邦議会の制定した憲法に適合した法律があれば、拘束力を持つのは言うまでもないが、連邦議会の立法権も無制限ではない。Ⅷ３で見るように、連邦議会の立法権も、憲法第 2 章第 1 条に基づく大統領権限を侵害することはできないとされており、限界があると認識されている。

てきた。

２　連邦憲法修正第４条（不合理な捜索・拘束押収の禁止）

連邦憲法修正第４条は次のように規定する。

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.（不合理な捜索及び拘束押収から身体、家屋、書類及び所持品の安全を保障される国民の権利は、これを侵してはならない。いかなる令状も、宣誓又は誓約によって裏付けられた相当な理由があり、且つ、捜索する場所及び拘束押収する人又は物を特定したものでない限り、これを発してはならない。）

行政傍受は、当初本条との関係が意識されることはなかったが、1967 年に最高裁判所が刑事捜査における通信傍受を本条の適用対象となる捜索押収（search and seizure）であると判示したため、本条との関係が論点となってきた。

本条は、不合理な捜索・拘束押収を禁止したものであり、必ずしも裁判官の令状を必須と規定したものではない。そこで、刑事司法目的ではない国家安全保障目的の通信傍受にも、裁判官の発する令状（warrant）を必要とするのか、必要としない（いわゆる national security exemption）としても、本条の禁止する不合理な捜索押収とはならない要件は何なのか等が論点となってきた。

Ⅲ　米国コミント実施組織についての基礎知識

行政傍受に係わる法体系と解釈運用の分析の前に、前提の基礎知識として、米国において行政傍受を行ってきた主要な機関について簡単に触れておきたい。行政傍受を行う諜報機関は、主にコミント（通信諜報）機関[9]とセキュリティ・サービスである。

コミント（通信諜報）とは、有線通信や無線通信を傍受して、通信内容を解読（暗号解読）し、或いは通信状況を分析（通信状況分析）することによって、情報を得る諜報活動である。20 世紀においては、外交通信や軍通信の暗号解読や軍通信の通信状況分析による成果が注目を集めてきた。21 世紀に入ると、サイバー空間が情報空間として劇的に拡大したため、現在のコミント対象は、E メール、チャット、ファイル送信、ビデオ会議、ウェブサイト閲覧履歴その他サイバー空間で行われる活動全般に及んでいる。

歴史上注目されてきたコミント機関としては、『ブラック・チェンバー』、海軍 OP-20-G、陸軍 SIS、そして国家安全保障庁などがあり、また、セキュリティ・サービスとしては FBI がある。

１　『ブラック・チェンバー』（1919－1929 年）[10]

1917 年 4 月米国が第一次世界大戦に参戦すると、陸軍情報部はハーバート・ヤードレーを責任者として第 8 課（MI-8）を設置し、秘密通信文や外交暗号の解読に取り組んだ。同課は、理論的分析に加えて、外国公館からの暗号書の盗写や電信官の篭絡（色仕掛け）も活用して、暗号解読に成果を上げた。

この成果を受け、大戦後の 1919 年、国務省と陸軍省が資金を出して、民間機関として『ブラック・チェンバー』（責任者ヤードレー）が設立された。同機関は、各国暗号の解読に取り組んだが、特に日本の暗号解読に注力し、1920 年代の日本の外交暗号は概ね全て解読していた。また、海軍武官や陸軍武官用の暗号も一部解読していた。1920～1921 年ワシントン軍縮会議で、米国政府が暗号通信の解読によって日本代表団の手の内を全て知っていたのは有名な話である。

外交通信文は、民間通信事業者から入手していた。『ブラック・チェンバー』は 1929 年に国務長官の意向で閉鎖された。

---

[9] コミント機関は、20 世紀後半には、エリント（電子諜報）やテリント（テレメトリー信号諜報）にも業務分野を拡大して、シギント（信号諜報）機関と称されるようになるが、本稿ではコミント機関と称する。

[10] 主として次の資料による。

--ハーバート・ヤードレー『ブラック・チェンバー』（荒地出版、1999 年）

--Army Security Agency, *Japanese Codes and Ciphers 1919-1929,* August 1946.

２　海軍の OP-20-G（1922－1945）と NSG[11]

海軍は、第一次世界大戦中からコミントに取り組み始めたが、1922 年に海軍情報部内のコミント分析組織に OP-20-G という名称が与えられ、外交通信や海軍通信の解読を行った。主要対象は日本であり、1922 年と 20 年代末と 2 回に亘りニューヨークの日本総領事館に侵入して海軍武官用の暗号を盗み、更に理論的に分析するなどして、継続的に日本海軍暗号を解読してきた。その後、第 2 次世界大戦中に日本海軍 D 暗号を解読したのは有名である。なお、第二次世界大戦前にはニューヨーク日本総領事館から領事館用外交暗号を盗み出している。

海軍は、外交通信や海軍通信の傍受を、1924 年頃から自らの組織を使って始めている。1935 年にはそのための専門組織として、海軍安全保障群（Naval Security Group: NSG[12]）を創設した。

第二次世界大戦後 OP-20-G と NSG は統合され、1950 年からは全体が NSG と呼称されていたが、2010 年コミント機能は海軍第十艦隊（艦隊サイバー司令部）に移管された。

３　陸軍の SIS（1929-）、SSA(1943-)、ASA(1945-)、INSCOM（1977-）[13]

陸軍も第一次世界大戦中にはコミントに取り組んだが、終戦により取組は中断された。再開したのは、1929 年に設立された信号諜報サービス（SIS）である。日本外務省の機械式暗号の解読で有名であり、「レッド暗号」（1935 年運用開始）を 1937 年 2 月、「パープル暗号」（1939 年運用開始）は 1940 年 11 月に解読に成功している。外交通信は、自ら通信を傍受すると共に、民間通信事業者からも通信を入手していた。

組織は、大戦中の 1943 年に信号安全保障庁（SSA）に改組され、大戦後の 1945 年には陸軍安全保障庁（ASA）に改組された。更に、1977 年、陸軍の一般の諜報機関と統合されて諜報・安全保障司令部（INSCOM）に改編された。

---

[11] 主として次の資料による。
-- Thomas Johnson, *American Cryptology during the Cold War, 1945-1989, BookⅢ: Retrenchment and Reform, 1972-80* (Center for Cryptologic History, 1998)
--Frederick Parker, *Pearl Harbor Revisited: U.S. Navy Communications Intelligence 1924-1941*, 3rd ed., (Center for Cryptologic History, 2013).
--NSA, *Pearl Harbor Review,* last modified 3 May 2016, accessed 14 September 2016, https://www.nsa.gov/about/cryptologic-heritage/center-cryptologic-history/pearl-harbor-review/index.shtml

[12] Security は、「安全保障」と訳しているが、米国インテリジュンス社会では Security は、「安全保障」という意味の他に、第二次世界大戦前後から「コミント（通信諜報）とコムセック（通信保全)」を総称する名称としても使われ始め、現在ではほぼ「シギント業務全般」の別称として使われている。

[13] 主として NSA, *Pearl Harbor Review* による。

４　国家安全保障庁 National Security Agency: NSA[14]

1952 年に設置された国家的コミント機関である。当初はその存在自体が秘匿されていたが、1975 年に至り初めて存在が公認された。

米国の 17 の諜報機関の内、最大最強の諜報機関であると見られている。現在の年間予算額は 1 兆円以上、人員 3 万 5 千人である。米国は陸海空軍海兵隊にも作戦支援用のシギント組織があるが、NSA は中央安全保障サービス CSS を通じてこれら諸組織も統制している。

セカンド・パーティ、サード・パーティと呼ばれる諸国との協力関係により、世界中にその情報収集網を構築している。セカンド・パーティとは、英、加、豪、ニュージーランド 4 カ国であり、これら諸国とは第二次世界大戦における協力を基礎に UKUSA と呼ばれる密接な協力関係を結んでおり、その活動は殆ど一体化している。サード・パーティとは、その他の協力国であり、30 カ国以上に及ぶ。

国家安全保障庁はこれらの関係を利用して、世界中に通信の傍受拠点を設置しており、その総数は約 500 ヵ所[15]、主要なものだけでも 150 ヵ所[16]程度に及んでいる。現在の行政傍受（データ収集）の方法は多様であり、

- ○　米国内の民間データセンターからの収集、
- ○　国内外の通信基幹回線からの傍受、
- ○　在外公館を拠点として行う特別収集サービス（NSA と CIA の共同事業）、
- ○　外国衛星通信の傍受、
- ○　シギント衛星による大気圏外での収集

などがある。

５　連邦捜査局 FBI

世界の先進民主主義諸国は概ね、国家安全保障のため国内で諜報活動を行う機関としてセキュリティ・サービスを、治安を所管する内務省傘下に設置している。元々は警察機関が行っていた業務であるが、その専門性特殊性から、警察機関から分離して専門機関としている。英国セキュリティ・サービス、フランス対内安全保障総局（DGSI）、ドイツ憲法擁護庁（BfV）、豪安全保障諜報機構 ASIO、加安全保障諜報局 CSIS 等で

---

[14] NSA の概要については、茂田忠良『米国国家安全保障庁の実態研究』（警察政策学会、2015 年）8-23 頁、33-35 頁参照。

[15] 次の分析資料によれば、2013 年 3 月現在 NSA がシギント収集を行っている施設数は 504 ヵ所である。“SIGINT Activity Designators(SIGADs),” *Electrospaces,* updated 23 August 2016, accessed 30 August 2016, http://electrospaces.blogspot.jp/p/sigint.html

[16] シギントデータの主要な記憶装置である XKeyscore サーバーの設置場所が世界中に約 150 ヵ所ある。従って、主要な収集施設も概ね 150 ヵ所程度と推定できる。茂田『米国国家安全保障庁の実態研究』115-122 頁参照。

ある。

これに対し米国では、専門のセキュリティ・サービス機関が設置されず、法執行機関である FBI がセキュリティ・サービス機関としての機能を担ってきた。即ち、FBI は法執行機関であると同時に、インテリジェンス機関でもある。

セキュリティ・サービスの諜報活動では、ヒューミントと共にコミントである行政傍受も行っているのが通常であり、国内における行政傍受運用の主要機関でもある。

Ⅳ　20 世紀中期までの法解釈と運用[17]

20 世紀中期までのコミント機関及び FBI による行政傍受の解釈と運用について概説する。

１　米国によるコミント活動の開始

米国のコミント活動は、第 1 次世界大戦を契機に開始され、米国内では外交通信が主たる対象であった。外交通信を読むには、通信の入手と暗号解読の二つの作業が必要となる。外交通信の入手では、民間通信会社の協力が大きい役割を果たしてきた。また、1920 年代には、陸海軍の受信所による無線通信の直接傍受も開始されている。

当然の事ながら、これらのコミント活動は秘匿されていたため、一般国民の知るところはならなかった。コミント活動の従事者も、実際は憲法や法律との関係を意識せずに活動していたというのが実態である。当初はそれで全く困らなかったと言ってよい。

なお、米国は他の国と同様、外交暗号解読は、純粋に理論的分析によって行うだけでなく、外国公館に工作員を侵入させて暗号書を盗写する、女性工作員を電信官に接近させて情報を入手するなどのヒューミントも活用して行っているが[18]、これらの活動の合法性についての議論は見当たらない。当然の必要悪とされたのであろう。

２　法律との衝突

コミント活動は、先にも述べた通り、大統領の国家安全保障上の権限に基づくと考えられているため、活動それ自体には法律の根拠は要しない。また、コミント機関はその存在自体が秘匿されてきた。現代米国の代表的機関である国家安全保障庁 NSA もその存在が公表されたのは 1975 年であり、それ以前はそもそもコミント活動の合法性などを公然と議論する状況になかったのである。

---

[17] Thomas Johnson, A*merican Cryptology during the Cold War, 1945-1989, Book I: The Struggle for Centralization, 1945-1960* (Center for Cryptologic History, 1995), 64,
--Thomas Johnson, *American Cryptology during the Cold War, 1945-1989, Book Ⅱ: Centralization Wins, 1960-1972*(Center for Cryptologic History, 1995), 475,479,

[18] その実態については次の資料を参照。
--ヤードレー『ブラック・チェンバー』
--Johnson, *American Cryptology, Book I,* 162.
--Johnson, *American Cryptology, BookⅢ*, 86.
大使館など外国公館を標的とする行政傍受の手法には、他に電話傍受や大使館内へのマイク設置などがあり、これは昔も今も世界標準の活動である。しかし、第二次世界大戦の前後の時期には米国ではコミント機関の任務とはされていなかった（基本的には FBI の任務であったと推定できる）ためか、米国の国家安全保障庁 NSA 関係文書では、この種活動の合法性に関する記述は、今まで目にしていない。

しかし、秘密の活動であっても、少なくとも建前上は法律に違反できないという意識はあった。そこで、連邦議会の立法により、コミント活動が違法と解釈される可能性のある法律が制定された場合、それら法律の解釈との整合性をどう図るかという問題が生じた。次の法律である。

（１）1927 年無線法

無線法は、1912 年に制定され[19]、同法第 4 条は無線事業者に通信内容を漏洩し公表することを禁止していた。しかし、同条はその適用に行政側の裁量を認めていたので、コミント活動では余り問題とならなかった。

ところが、1927 年に無線法が全面改正され[20]、第 27 条に次の規定が置かれた。

（第 1 文）無線通信事業者は、管轄権をもつ裁判所の発出した提出命令に応じる場合、その他権限ある当局からの要求がある場合を除いて（...in response to a subpoena issued by a court of competent jurisdiction, or on demand of other lawful authority）、無線通信内容を漏洩し又は公表してはならない。

（第 2 文）無線通信発信者の承認を受けた者でなければ、無線通信を傍受して通信内容を漏洩し又は公表してはならない(no person ... shall intercept any message and divulge or publish the contents...)。

（２）1934 年通信法

1934 年通信法が制定され[21]、1927 年無線法は全面改正された。同法は有線通信を含む通信全般を規制する一般法であるが、第 605 条には無線法第 27 条の規定がほぼそのまま継承された。変更点は、保護対象を無線通信から有線通信を含む全通信に拡大したことである。なお、1934 年通信法第 605 条の規定は現在でもほぼそのまま残されている。

３　コミント担当者の法律解釈

これら二つの法律は、外交通信に対するコミント活動で二つの問題を生み出した。第１は、通信事業者の協力維持である。外交通信は通信事業者から入手するのが迅速正確で且つ安価であるが、通信事業者による外交通信の提供は法律違反ではないかという問題である。第２は、政府自らが外交通信を傍受するとしても、これが 1927 年無線法第 27 条第 2 文（及びこれを継承した 1934 年通信法第 605 条）の「・・・通信を傍受して通信内容を漏洩し又は公表してはならない」に違反しないかという問題である。そもそもコミント活動は秘匿されているため、コミント活動を公認する法律は存在しなかった。そこで、通信傍受が違法であるならば、コミント活動自体が違法では

---

[19] Radio Act of 1912.
[20] Radio Act of 1927.
[21] Communications Act of 1934.

ないかという問題である。

これに対するコミント担当者の行政解釈は、次のものであった。

第１の通信事業者の協力確保に関しては、外交電文の提供は、「権限ある当局からの要求がある場合」に該当する正当な行為であるという解釈である。コミント活動を行う権限は、最終的には大統領、及び大統領の指揮下でコミント業務に携わる各級指揮官にあり、大統領或いは各級指揮官の要求が「権限ある当局からの要求」であると解釈したのである[22]。

第 2 の「通信を傍受して通信内容を漏洩し又は公表してはならない」は、単なる傍受を禁止するものではなく、傍受し「且つ」漏洩又は公表する行為を禁止している。他方、コミント活動は、通信を傍受し暗号を解読するがその利用は政府内に限定されており「漏洩」「公表」されることはないので、違反しないと解釈したのである[23]。

但し、当時のコミント担当者がこの解釈に自信を持っていた訳ではない。フランク・ルーレットは、1930 年代から米国コミントの中心人物であり日本の外交暗号を解読した立役者であるが、彼は、国家安全保障庁のオーラルヒストリーのため聴取を受け、日米開戦前の状況に関して、「違法の虞はあったが、国益のために必要な活動であり、秘密は保たれると確信していた。また、通信事業者も愛国心から参画してくれた」旨を述べている[24]。

４　行政解釈を裏打ちする立法と大統領の動き

コミント活動の合法性に関する行政解釈を裏打ちし補強する動きが、その後なされていく。

（１）スパイ防止法[25]の 1933 年改正

1933 年に、スパイ防止法が改正され、政府職員が外国政府とその在米公館の間の通信から得られた知識を開示する行為が犯罪とされた[26]。この立法により、連邦議会が「外国政府と在米公館の間の通信から情報を得る活動」が行われており、且つ当該活動の秘密を守る必要がある判断したことが示された。婉曲な表現ではあるが、コミント活

---

[22] Johnson, *American Cryptology, Book I,* 273.

[23] *Id.*

[24] NSA-OH-1976-(1-10), Oral History Interviews, “Frank Rowlett,” 350-361, accessed 8 October 2015, https://www.nsa.gov/news-features/declassified-documents/oral-history-interviews/assets/files/nsa-OH-1976-1-10-rowlett.pdf

[25] Espionage Act of 1917.

[26] 本改正は、ハーバート・ヤードレーが 1931 年に『米国のブラック・チェンバー』を出版して、第一次世界大戦中と 1920 年代の米国のコミント活動（日本外交暗号の解読を含む）を暴露し、更に新たな出版を企図していた。そこで、かかる行為を犯罪として新たな出版を阻止するため急遽立法されたものである。

動の存在と合法性を議会が認めたと解釈できるものである。

（２）スパイ防止法の 1950 年改正

本改正は、1933 年の改正を更に徹底して、コミント情報漏洩罪とも呼べる規定を創設したものである[27]。コミント活動とコミント情報の秘密を包括的に保護する規定である（刑法第 37 章第 798 条）。これにより、コミント活動の存在が包括的に公認され、1934 年通信法第 605 条はコミント活動を制限するものではないと解釈されるようになった[28]。

（３）1952 年トルーマン大統領の秘密覚書の発出

米国は、1952 年にコミントの国家中央機関である国家安全保障庁 National Security Agency を設立した。その基となったのが、1952 年 10 月 24 日付のトルーマン大統領の秘密覚書である。同覚書は、コミント組織の任務と運営方法を明示して国家安全保障庁の設置を指示している。秘密覚書ではあるものの大統領の意思が明示され、1934 年通信法第 605 条に規定する「権限ある当局」（lawful authority）の意思が明示されたと解釈された[29]。即ち、民間通信事業者に通信の提供を要求する際の適切な根拠とされたのである。

（４）1968 年総合犯罪対策・街路安全法[30]による刑法改正

本法は総合的な犯罪対策を打ち出した法律であるが、その一環で、合衆国法典第 18 篇第 1 部に第 119 章が新設された。本章は主として法執行機関による通信傍受について規定すると共にそれ以外の通信傍受を禁止したものであるが、更に、行政傍受については同章と 1934 年通信法 605 条の制約が適用されないことを確認しているのである。

即ち、第 119 章第 2511 条第 3 項は「本章及び 1934 年通信法第 605 条の規定は、・・・合衆国の安全保障に不可欠な対外諜報情報を得るために・・・、大統領が必要と考える措置を採ることができる大統領の憲法上の権限を制限するものではない。」と規定されたのである（いわゆる national security exemption）。

国家安全保障庁のヒストリアンは、本規定によりコミント活動の正当性が完全に認められたと記述している[31]。

また、この規定振りは、国家安全保障のために行う対外諜報活動は大統領の憲法上の権限であることを前提とし、それを明示している。従って、コミントを含む対外諜

---

[27] 第二次世界大戦後の米国で「真珠湾奇襲」の責任を巡って公聴会が何度も行われ、関連して日本の暗号解読についての情報が相当開示され又は漏洩された。そこで、コミント活動の秘密を守るために本改正が行われたものである。

[28] Johnson, *American Cryptology, Book I,* 274.

[29] *Id.*

[30] Omnibus Crime Control and Safe Streets Act of 1978.

[31] Johnson, *American Cryptology, Book Ⅱ*,474.

報活動は、(議会の制定する法律の根拠を必要とせず) 大統領の命令によって遂行しうることを議会が公認したこととなる。

こうして、米国のコミント担当者は、憲法上の国家安全保障のための大統領権限がコミント活動の根拠である旨が固まったと解釈している。

５　FBI による行政傍受の運用

以上コミント機関による行政傍受について述べてきたが、セキュリティ・サービスとしての FBI でも行政傍受に取り組んでおり、それに関する文書資料には次のものがある。なお、これらの文書が適用対象とする組織が FBI のみであるのか、当時のコミント機関も含むものか、必ずしも明確ではない。但し、NSA 開示文書中に通信傍受の根拠としてこれら文書についての言及が見られないこと[32]、そして文書の内容から判断して、少なくとも（１）（２）は FBI のみを対象としてものと推定できる。

（１）1940 年 5 月 21 日ルーズベルト大統領の司法長官宛て覚書[33]

政府に対するスパイ活動や破壊活動を防止するため、司法長官に対して通信傍受を認める権限を指示し承認したもの。

（２）1946 年 7 月 17 日トルーマン大統領に対する司法長官の伺い[34]

通信傍受については、1940 年の大統領覚書に従い行ってきたが、現下の状況に鑑みて、国内の安全保障問題又は人命が危険に晒されている場合に対象を拡大することを提起したもので、トルーマン大統領は同日これに同意している。

この大統領の指示を受け、通信傍受の対象は、国家安全保障問題のみならず、組織犯罪捜査にも拡大された[35]。

（３）1965 年 6 月 30 日ジョンソン大統領の全省庁長官宛て覚書[36]

電話通信傍受が無差別に行われているとして、当事者の同意の無い通信傍受は真に国家安全保障に係わる場合に限定する、司法長官の承認無しに通信傍受を行ってはいけないなど通信傍受の限定を指示したもの。

この覚書を契機に通信傍受の使用が一時縮小したようである。しかし、指示内容から判断して、指示の時点では、令状無しの通信傍受は国家安全保障のみならず犯罪捜査も含めて広汎に行われるようになっていたことが推定できる。

---

[32] 先にも記載した 1952 年トルーマン大統領の秘密覚書については、開示された NSA 内部文書は「権限ある当局」(lawful authority) の意思として強調している。(1) や (2) の指示が NSA にも適用されるものであるならば、同様に「権限ある当局」の意志として記載されていたと考えられる。Johnson, *American Cryptology, Book I,* 274 参照。

[33] United States v. Smith, 321 F. Supp.424 （C.D. Cal. 1971）at 430-431 で引用。

[34] Id. at 431 で引用。

[35] United States v. United States District Court, 407 U.S 297(1972) footnote 10.

[36] United States v. Smith, 321 F. Supp.424 （C.D. Cal. 1971）at 431-432 で引用。

Ⅴ　通信事業者の協力状況

以上の記述から、米国では、通信傍受を認める個別の法律規定に基づかないで、大統領の憲法上の権限に基づいて行政傍受が幅広く行われていたことが推定できるが、通信事業者の協力を得て行われてきた主な行政傍受の経緯を見てみよう。

１　第１次世界大戦とその後[37]

米国が第一次世界大戦に参戦すると、陸軍は情報部に第 8 課を設置して外交電文の解読を中心にコミント活動に取り組んだ。その際、通信文は通信事業者の協力を得て入手した。この協力関係は、大戦終了後も継続したが、協力についての法律上の根拠が明確でないために、通信事業者は次第に協力を渋るようになり、1927 年無線法が制定された後は更に協力が得難くなった。それもあって、ヤードレーの『ブラック・チェンバー』が 1929 年に閉鎖されると、この協力関係は終了した。

２　第２次世界大戦とその前

1934 年通信法第 606 条は、戦時における大統領権限を規定した条項であり、必ずしも法文上明白ではないが、軍事検閲の根拠条項と解されている[38]。

大戦中は、本条による軍事検閲により、外国と米国間の通信は全て軍事検閲の対象となっており、検閲対象中、情報価値がある判断された通信は、軍情報部のコミント機関に提供されていた[39]。

また、軍事検閲の根拠とされた第 606 条(c)項の規定は、宣戦布告に至らなくても、国家緊急事態の布告があれば実施可能である。米国は独・英仏間で戦争が始まった 1939 年 9 月時点で国家緊急事態を布告しているので、民間通信会社の協力による外国在米公館の外交通信の入手は、米国の参戦前のこの時点頃には始まっていたと考えられる。

---

[37] ヤードレー『ブラック・チェンバー』参照。

[38] US Senate, *Book Ⅲ, Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, Final Report of the Select Committee to Study Operations with respect to Intelligence Activities (1976), 767.　Accessed 2 October 2016, http://www.aarclibrary.org/publib/church/reports/book3/contents.htm

[39] Britt Snider, *Recollections from the Church Committee's Investigation of NSA: Unlucky Shamrock* (CIA Center for the Study of Intelligence, 1999), last updated 27 June 2008, accessed 30 September 2016, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter99-00/art4.html

３　「シャムロック」計画

（１）「シャムロック」計画[40]

第 2 次世界大戦の終結により軍事検閲は終了したが、国際通信は情報源として有用なため、民間通信会社の任意の協力を得てその入手は継続された。この計画の暗号名が「シャムロック」である。

1945 年 8 月陸軍コミント機関は、米国の国際通信会社三社（RCA、ITT、ウェスタン・ユニオン）に協力継続を依頼したが、三社は電信提供が違法行為に当らないという司法長官の保証が得られることを条件に協力を継続した。1947 年には三社は協力継続の条件として、国防長官と司法長官に加えて大統領が、本協力が国家安全保障上必須であり、且つ本協力により訴追されることがないと保証することを要求した。そこで、同 12 月には国防長官が三社にその保証を伝えている。更に 1949 年に国防長官が交代したため新国防長官が同趣旨を三社に対して再確認している。

通信提供は、陸軍のコミント機関（1952 年以降は NSA）が、三社の国際通信の拠点であるニューヨーク、ワシントン DC、サンフランシスコ、サンアントニオの 4 か所で、国際通信の写しを入手していた。具体的な実施要領は、会社によって異なり、RCA と ITT は国際通信全体を一旦 NSA に提供して、対外諜報上必要な通信の選択は NSA の裁量に委ねていた。一方、ウェスタン・ユニオンは特定国との通信に限定し且つ同社の施設で NSA 職員が必要なものを抽出するようにしていたようである。

その結果、1973 年から 1975 年の間では、NSA では提供を受けた膨大な通信の中から毎月平均 15 万件を分析して情報成果を挙げていた。また、本計画により米国人を含む膨大な国際通信が収集されていたため、CIA からの要請に応じて、米国人反戦運動家の通信も検索抽出していた（これは「ミナレット」計画と呼ばれた）。

ところが 1970 年代に米国では諜報機関の活動が批判に晒されたため、「ミナレット」計画は 1973 年に中止、「シャムロック」計画は 1975 年 5 月に中断された。

1978 年に対外諜報監視法が制定されると、「シャムロック」計画が主目的としていた対外諜報は、同法第 105 条の電子的監視（行政傍受）として規定され、同条により対外諜報監視裁判所の命令を得て行わるようになった。

なお、NSA の法律家によれば、「シャムロック」計画についての政府の公式の立場は、憲法解釈、合衆国法典第１８篇第 119 章第 2511 条第 3 項の解釈、最高裁判決（後

---

[40] 主に次の資料による。
-- US Senate, *Book Ⅲ, Supplementary Detailed Staff Reports,* 765-766.
-- Snider, *Recollections.*
-- James Hudec, *Unlucky Shamrock: The View from the Other Side* (CIA Center for the Study of Intelligence, 2000), last updated 3 August 2011, accessed 30 September 2016, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol44no5/html/v44i5a12p.htm

述）に照らし合わせても、正当な対外諜報活動であり違法行為ではなかったというものである[41]。

（２）「ニュー・シャムロック」計画[42]

本計画は民間事業者の協力を得て行うものではないが、監視法第 105 条に関連するのでここで言及する。

「シャムロック」計画は、民間通信事業者の協力を得て国際民間通信から対外諜報情報を得るものであるが、より直接的に在米外国公館を標的にするのが「ニュー・シャムロック」計画である。1950 年代に開始された FBI と NSA の協力事業であり、在米の外国公館に盗聴器を仕掛ける行為が中心である。常時 60 から 70 の外国公館が収集対象とされてきた。

対外諜報監視法が制定されると、これも監視法第 105 条による監視裁判所の命令が必要となった。

４　「通過通信収集」（TRANSIT）

本件については、現在まで注目されておらず、開示されている資料も極めて少ないが、NSA からの漏洩情報を分析すると次の状況が推定できる[43]。

1978 年に対外諜報監視法が制定されたが、同法が規制対象としたのは、米国内の標的に対する通信傍受であり、米国外の標的に対する米国内での通信傍受は規制対象外であった。そこで、外国間通信（米国外の者が別の米国外の者と行う通信）が米国を経由する場合に、この通信を米国内で収集することは大統領権限に基づき依然として可能ということになる。

そこで、この通信の収集が「通過通信収集」（TRANSIT）として、民間通信会社の協力を得て 1980 年代から開始されている。「フェアビュー」（協力：ATT)、「ストームブリュー」（協力：当初 MCI、ベライゾンが継承）他の計画が行われており、現在でも協力は継続している。なお「フェアビュー」計画は遅くとも 1985 年には開始されている。

現在、インターネット通信に占める米国の強大な地位のため、本収集によるデータ収集は相当な量に及んでいる。

---

41 Hudec, *The View from the Other Side.*

42 Johnson, *American Cryptology, BookⅢ,* 93,106.

43 茂田忠良「米国国家安全保障庁のシギント収集プラットフォーム」『警察政策第 18 巻』（警察政策学会、2016 年）198-200 頁参照。

５　「大統領監視計画」（別名「ステラーウィンド（恒星風）」[44]

2001 年に 9/11 同時多発テロ事件が発生すると、直後から一部民間企業は積極的に協力を申し出た。そして 10 月 4 日ブッシュ大統領は、従来の情報収集では不十分であるとして、電子的監視（行政傍受）強化の緊急措置を命じる秘密覚書を発出した。これには、①通信の一方当事者がアフガニスタンにいる場合又は一方当事者がテロ容疑者である場合に、米国内との通信であっても通信内容を収集するものと、②米国内の電話通信とインターネット通信のメタデータ[45]を収集するものと、二つの収集計画が含まれていたようである。

NSA 長官は大統領覚書が発出されると、民間通信事業者 7 社以上に対して、憲法第 2 章に基づき大統領が承認し司法長官が同意したものであるとして、書簡を発出して行政傍受強化について正式に協力を要請した。

この要請に応じ、民間通信事業者は少なくとも三社が全面協力を行い、電話通信とインターネット通信の両者について、通信内容とメタデータ提供の協力を開始した。

協力は短期間の緊急措置として始まったが、長期化するに従って法的根拠について議論されるようになり、対外諜報監視法の手続に乗せることが模索された。

先ず、インターネット・メタデータ収集については、対外諜報監視法第 401 条（ペンレジスター/トラップアンドトレース（PR/TT）装置の設置）を根拠とすることとなり、2004 年 7 月から監視裁判所の命令を得て行うようになった。

そうこうする内に、2005 年 12 月にニューヨーク・タイムズ紙が、大統領の秘密命令による情報収集の存在を暴露報道し、更に 2006 年 5 月には「USA Today」紙が、ATT、ベライゾン、ベルサウス（当時）の 3 社が電話メタデータを政府に提供していると暴露する記事を掲載した[46]。そこで、電話メタデータについては、同月中に愛国者法第 215 条（監視法第 501 条）（業務記録の提出）による裁判所命令によることとして、同月から実施に移された。通信内容の収集については、2007 年 1 月から監視法第 105 条の要件の解釈を緩和して一部を同条の手続に乗せることができたが、諜報機関

---

[44] この経緯は次の資料に詳しく記載されている。NSA, Office of the Inspector General, *ST-09-0002 Working Draft*, 24 March 2009、accessed 6 November 2014, https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf
--USA, Offices of Inspectors General of the DOD, DOJ, CIA, NSA and ODNI, *Report on the President's Surveillance Program, Vol 1,* 10 July 2009, accessed 5 October 2016, https://oig.justice.gov/reports/2015/PSP-09-18-15-full.pdf

[45] メタデータについては、「Ⅸメタデータの取扱」で詳しく述べる。

[46] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *The New York Times,* 16 December 2005, accessed 7 November 2014, http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0
--Leslie Cauley, "NSA has massive database of American' phone calls," *USA TODAY,* 10 May 2006, updated 11 May 2006, accessed 7 November 2014, http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm

にとっては極めて不十分なものであった。そこで立法化の動きが加速され、2007 年米国保護法[47]により監視法第 105B 条が規定され、同条に基づく収集に移行した。更に 2008 年改正で同条を引き継いで監視法第 702 条が制定された。

こうして、これらについては対外諜報監視法中の既存の或いは新規の条項に根拠を有する収集に移行した。

[47] Protect America Act of 2007.

Ⅵ　対外諜報監視法制定と現在の行政傍受法制の基本構造

米国の行政傍受法制は、憲法第 2 章の大統領権限に基づく大統領命令の体系と、対外諜報監視法による体系との二重構造となっている。

１　対外諜報監視法の制定

（１）大統領命令

先にも述べたように、大統領の行政権には、憲法上、国家安全保障のための広汎な権限が含まれると解釈されており、対外諜報はその一部と理解されている。従って、対外諜報は、基本的に、連邦議会の制定する法律の根拠無しに、米国の内外に於いて大統領の行政命令によって行うことができる。

対外諜報に関しては大統領命令が幾つか出されてきたが、現在有効な命令が大統領命令第 12333 号「合衆国諜報活動」[48]である。本命令は、諜報活動の目的、諜報諸機関の責務、諜報活動の実施について包括的に定めた諜報活動に関する基本文書である。1981 年 12 月レーガン大統領によって制定され、累次の改正（直近の改正は 2008 年ブッシュ大統領による）を経て現在に至っている。諜報諸機関は本大統領命令に基づき対外諜報を行っている。

（２）対外諜報監視法の制定

しかしながら、米国史上では、行政府が権限を濫用したことが度々あり、特に米国がベトナム戦争を戦った 1960 年代には、FBI や CIA や陸軍諜報機関が、法律の根拠なしに反戦運動や米国人の反戦運動家に対して広汎な情報収集を行った[49]。更に、1972 年にはニクソン大統領によるウォーターゲート事件が惹き起こされた。

これに対して、1976 年上院のチャーチ委員会は、諜報諸機関の活動に関し「如何なる諜報機関も、法律の根拠なしに国内の安全保障活動（諜報活動）に従事してはならない」「対外諜報のためであっても、NSA は国内通信を傍受してはならない」等の包括的な勧告を行った[50]。

この勧告を踏まえて、1978 年対外諜報監視法が制定された。これは、本来、対外諜報目的で米国内の対象を標的として米国内で行う電子的監視（通信傍受）に制約を課したものである。規制のため、特別裁判所である対外諜報監視裁判所が設置され、米国内で特定の通信傍受を行うには原則として同裁判所（秘密審議）の命令（order）（105 条）を要することとなった。但し、本法律は、米国外での活動は規制対象外であり、国外に於ける活動（米国内から行う国外の標的に対する通信傍受を含む）は、依然と

---

[48] Executive Oder 12333, United States Intelligence Activities.
[49] US White House, *Liberty and Security in a Changing World,* 53-57.
[50] *Id.* 57-63.

して大統領の裁量に委ねられていた。

なお、本法の制定に伴い、コミント担当者が高く評価していた合衆国法典第 18 編第 119 章第 2511 条第 3 項の”national security exemption”の規定は削除された。

（３）対外諜報監視法の諸改正

その後、対外諜報監視法は度々改正され、1995 年に物理的捜索（301 条以下）、1998 年にペンレジスター/トラップアンドトレース(PR/TT)装置の設置（401 条以下）と業務記録の提出（501 条以下）の規定が加わった。更に 9/1 1 テロ事件後の 2001 年の愛国者法[51]制定、2008 年の対外諜報監視法改正（702 条以下）などにより、諜報諸機関の権限が拡大され、本法は、米国内での対外諜報活動を規制するものから、米国内で行う対外諜報（米国内から行う国外標的に対する諜報を含む）について、民間事業者に協力義務や守秘義務を課すなど強制権限規定の色彩が強くなってきている。

２　大統領命令に基づく行政傍受の体系

（１）大統領命令第 12333 号「合衆国諜報活動」

米国外で行われる行政傍受は、本命令を根拠として主として国家安全保障庁 NSA によって行われている。

具体的な収集取組としては次のものがある。①海外における通信基幹回線からの傍受、②在外公館を拠点として行う特別収集サービス（NSA と CIA の共同事業）、③外国衛星通信の傍受、④シギント衛星による大気圏外での収集である。①は、外国政府と協力して、或いは米国単独で行っており、コード名「オークスター」「インセンサー」「マスキュラー」「ランパート A」「ミスティック」「ダンシング・オアシス」等多くの計画がある[52]。

（２）通過通信収集（TRANSIT）

対外諜報監視法による規制対象は、米国内の標的に対する活動であり、米国内における収集であっても米国外の標的に対するものは規制対象外である。そこで、外国間通信（米国外の者が別の米国外の者と行う通信）がたまたま米国を経由する場合に、この通信を米国内で収集することは規制対象外となる。NSA はこれを通過通信収集（TRANSIT 権限による収集）として取り組んでいる。これによる収集データは、インターネット通信に占める米国の強大な地位のため、相当な量に及んでいる。

具体的な収集取組としては、米国内を通過する通信基幹回線からの包括的な傍受であり、「フェアビュー」「ストームブリュー」の計画があり、それぞれ大手の通信事業者である ATT とベライゾンの協力を得て行われている[53]。

---

[51] US Patriot Act of 2001.

[52] 茂田『米国国家安全保障庁の実態研究』57-65 頁、71-79 頁参照。

[53] 茂田「米国国家安全保障庁のシギント収集プラットフォーム」198-199 頁参照。

３　対外諜報監視法による行政傍受の体系

主要な監視法第 105 条と第 702 条による傍受について述べる。

（１）対外諜報監視法第 105 条

1978 年に対外諜報監視法が制定された際に規定されたものである。

規制対象は、米国内に於ける通信や施設を標的として行われる電子的監視であり、具体的には次の 4 種類の行為が対象である（101 条)。

①　米国内に所在する米国人が発・受信する有線・無線通信の内容（コンテンツ）を、当該米国人を標的として収集すること。

②　米国内に所在する人が発・受信する有線通信の内容を米国内で収集すること。

③　米国内に所在する人々だけの間で行われる無線通信の内容を収集すること。

④　有線・無線通信の収集以外で、米国内で情報収集のため監視機器を設置使用すること。（要するに、施設に侵入しての盗聴器の設置等のことである。）

電子的監視の対象は外国勢力又はその代理人（米国人を含む）であり、実施には監視対象を特定した対外諜報監視裁判所の個別の命令（order）を要する。命令を取得するには、司法長官の承認を得て監視裁判所の秘密審議を経る必要がある（104 条、105 条)。また、諜報活動の過程で、本来の監視対象でない米国人の情報を入手した場合の対処手続として、米国人のプライバシー保護のための「最少化手順」[54]を定めることとされている。

なお、米国内の通信であっても、外国勢力間のみの通信で米国人の通信が含まれる可能性がないものについては、監視裁判所の命令を要せず、司法長官の認証に基づき大統領が命令できる（102 条)。

具体的な取組としては、「ブラーニー」がある。これは傍受対象を特定しての収集であるが、ATT、ベライゾン他民間通信事業者 30 社以上の協力を得て全米 70 ヵ所以上で通信へのアクセス拠点を持っている。傍受対象となっているのは、外交施設、外国政府の代理人、テロ容疑者などである。本計画の実施では FBI と NSA が密接に協力している[55]。

（２）対外諜報監視法第 702 条

①　第 702 条の制定

2001 年に 9/11 同時多発テロ事件が発生すると、国際テロ対策を含む対外諜報のため、既存の通信傍受では不十分であるとして、ブッシュ大統領の秘密指示に基づき民間事業者の協力を得て「ステラーウィンド」計画が開始された。これは、米国外に所在する対象者を標的として通信傍受を行う際に米国内との通信も収集対象とする、或

---

[54]「最少化手順」(Minimization Procedures)とは、一旦収集したデータについて米国人に関する非公開情報の保持や情報化を最少化し、その配布を制限する手順である。50 USC Sec. 1801(h).

[55] 茂田「米国国家安全保障庁のシギント収集プラットフォーム」196-198 頁参照。

いは通信メタデータについては米国内の通信を収集対象とするものであった。

ところが、先にも述べたように、大統領指示による秘密収集計画の存在が、2005 年 12 月と 2006 年 5 月と続けてマスメディアによって、暴露報道された[56]。そのため、大きな政治問題となったが、結局収集の必要性が考慮されて、2007 年米国保護法[57]により対外諜報監視法第 105B 条が規定され、更に 2008 年の改正で同条を引き継ぎ同法第 702 条が制定された[58]。

本改正は、米国内で行う一定の包括的通信傍受について、監視裁判所による個別の命令を必要とせず、行政命令により実施する制度である。また、これに関して民間事業者に協力義務が課されることとなった。

② 第 702 条の手続

第 702 条によれば、司法長官と国家諜報長官は共同して、米国外に所在すると合理的に信じられる非米国人[59]を諜報の標的として認可(authorize)することができる。両長官がこの認可をするに当たっては、事前に、監視裁判所に、対外諜報情報の収集目的、「標的決定手順」[60]（米国人情報を極力収集しないようにするため）と「最少化手順」[61]（米国人情報の保持配布を極力限定するため）を提出し、監視裁判所の承認を得なければならない。その上で、両長官は通信事業者に対して協力命令（direct）を発することができ、事業者が協力しない場合には、監視裁判所に要請して協力の強制命令(order to compel)の発布を受けることができる。他方、事業者は、両長官の協力命令に従った場合には、その協力に関して民事刑事の責任を問われることがない。

③ 具体的な収集取組

具体的な収集取組としては、「プリズム計画」と通信基幹回線からの収集がある。

「プリズム計画」とは、通信事業者のデータセンターから、米国外にいると合理的に信じられる者を対象として、対象者に関する通信データを提供させる包括的な計画である。G メールやホットメールなどウェブメールやチャットのリアルタイムでの傍受も可能である。米国内のデータセンターには世界中の情報が集中しており、対外諜

---

[56] Risen and Lichtblau, “Bush Lets U.S. Spy on Callers Without Courts,” *The New York Times*。
--Leslie Cauley, “NSA has massive database of American’ phone calls,” *USA TODAY*.

[57] Protect America Act of 2007.

[58] 第 702 条は、当初は有効期間 1 年間の時限立法で、1 年経過毎に有効期間が延長されてきたが、2012 年 12 月には有効期間が 5 年間（2017 年末まで）延長されている。

[59] 非米国人とは、米国人（即ち、米国民又は米国永住権保有者）でない者と定義されている。50 USC Sec.1801(i).

[60] 「標的決定手順」(Targeting Procedures)とは、米国外に所在すると合理的に信じられる者のみを標的とし、且つ、通信当事者が全て米国内に所在すると知られている場合は収集を行わないようにするために、諜報機関が実施すべき手順である。50 USC Sec. 1881a(d).

[61]「最少化手順」(Minimization Procedures)とは、一旦収集したデータについて米国人に関する非公開情報の保持や情報化を最少化し、その配布を制限する手順である。50 USC Sec. 1881a(e).

報情報の収集には極めて有効なプログラムである。政府機関としては、主として FBI、NSA、CIA が関与している。民間事業者としては、現在マイクロソフト、グーグル、フェイスブックなど事業者 9 社が参加している[62]。

また、米国内の通信基幹回線からの収集では、収集標的は米国外にいると合理的に信じられる者であるが、その者と米国内との通信が含まれる。収集に際しては、収集標的を特定する必要はなく、米国人を直接的な標的としない限り、通信データの包括的取得が可能である。通信データは民間事業者の協力を得て包括的に収集しており、コード名「フェアビュー」や「ストームブリュー」計画などにより、膨大なデータを収集している[63]。

④　米国人のプライバシー保護の実際

「標的決定手順」「最少化手順」は、米国人に関する情報収集と情報化を極力限定して、米国人のプライバシーを保護するために規定されているが、この保護は必ずしも厚いものではない。

ここで注意すべき点は、第 1 に、これらの「手順」では、当然のことながら米国外にいる非米国人の保護は全く考慮されていないことである。第 2 に、これらの手順によっても米国人が当事者となる通信の収集、即ち付随的収集（incidental collection）は排除されないことである。監視法第 702 条は、「米国内にいる者を意図的に標的にしてはならない」「米国外にいる米国人を意図的に標的としてはならない」「送受信者の全てが米国内にいると知られている通信を意図的に取得してはならない」等[64]としているのみであり、米国外の非米国人を標的として情報収集を行った結果、これに付随して米国人や米国内にいる者が当事者となる通信を収集することが想定されている。実際、2006 年上院での（第 702 条の前身規定である第 105B 条の）法案審議において、当時の CIA 長官マイケル・ヘイデン（9.11 時の NSA 長官）は、国外のテロリストと米国内との通信の傍受が最も重要であると証言している[65]。

そして、この付随的収集は相当な量に及んでいる。その理由は、そもそも「フェアビュー」や「ストームブリュー」計画では、当初から米国外と米国内の間の通信が収集対象とされており、また「プリズム」計画でも、例えば収集対象を IP アドレスで特定した場合、この IP アドレスは監視対象者以外に数百人が使っている可能性もある。或いは、監視対象者がオンラインのチャットルーム入った場合には、そのチャットル

---

62 「プリズム計画」の詳細については、茂田『米国国家安全保障庁の実態研究』42-51 参照。
63 茂田「米国国家安全保障庁のシギント収集プラットフォーム」198-199 頁参照。
64 50 USC Sec. 1881a(b).
65 General Michael Hayden, Testimony to the Judiciary Committee of the US Senate (FISA for the 21st Century), 26 July 2006, accessed 10 April 2017, https://fas.org/irp/congress/2006_hr/072606hayden.html

ームの全ての通信を取得するとされる[66]。結果として、多くの米国人の通信を収集してしまうのである。

そこで、問題は、特に「最少化手順」の実態である。監視裁判所が承認した 2015 年版の「最少化手順」を見てみよう[67]。

NSA の「最少化手順」[68]を見ると、先ず、付随的に収集された通信の一方当事者が米国人であっても外国通信であれば、即ち、通信当事者の少なくとも一人が外国にいる場合には、①犯罪の証拠となる情報が含まれている場合、②価値ある対外諜報情報が含まれる場合、③米国人を匿名化した場合[69・70]には、情報配布が可能である。また、

---

[66] Barton Gellman, Julie Tate and Ashkan Soltani, "In NSA-intercepted data, those not targeted far outnumber the foreigners who are," *The Washington Post*, 5 July 2014, accessed 26 September 2016, https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html

[67] 監視裁判所は、2015 年 11 月 6 日、「標的決定手順」と「最少化手順」を承認する決定を下しているが、これらの「手順」は情報開示されている。同決定が承認したのは、同年 7 月に提出された「標的決定手順」（NSA と FBI 用）と「最少化手順」（NSA、FBI、CIA、国家テロ対策センター（NCTC）用）である。US, Foreign Intelligence Surveillance Court, Memorandum Opinion and Order, 6 November 2015, accessed 23 May 2016, https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf

[68] 2015 NSA Section 702 Minimization Procedures, https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf

[69] 米国外の非米国人を標的として情報収集を行った際に、これに付随して米国人が当事者である通信或は米国人について言及した通信を入手した場合の、米国人情報の取扱方法を諜報関係者から取材した報道があるので紹介する。Adam Entous and Danny Yadron, "U.S. Spy Net on Israel Snares Congress," *The Wall Street Journal*, 29 December 2015, accessed 4 January 2016, https://cryptome.org/2015/12/nsa-spies-israel-congress.htm

この報道によれば、米国人関連通信の取扱については冷戦時代からの慣行があり、個人名や企業名・組織名が分からないように、「某米国人」或は「某米国組織」として記載して情報化する。但し、政府高官は、情報内容を理解するため必要な時は、個人名や企業名を聞くことができる。

その後、連邦議会議員については規制が強化され、1990 年代初めから、政府高官の要求によって連邦議会議員の名前を知らせた場合には、議会の情報特別委員会に通知することとなった。更に、2011 年の NSA の内部指示では、外国標的と議会議員間の直接通信は入手した場合は原則として破棄することとされた。但し、これについても例外規定があり、NSA 長官が「重要な外国諜報」(significant foreign intelligence)を含むと認めた場合は破棄しなくても良いこととされている。従って、NSA 長官が認めた場合には、某米国人と外国人○○との通信ということで議員本人に知らせることなく情報化が可能である（その際、連邦議会議員であることは通信内容から明らかとなることが多いと考えられる）。更に、連邦議会議員と外国人、例えば外国大使との会話や通信を、その外国大使が本国外務省に報告した通信については、収集に制限はなく、情報化に際して米国人名を記載しなければよいということになる。

[70] ホワイトハウスにおける匿名化した米国人の人定情報取扱について、次の報道がある。

元国家安全保障担当の高官によれば、（国家安全保障担当補佐官などの）高官には個人担当のインテリジェンス・ブリーファーが付き、高官が関心のある情報報告を毎朝提供してくれる。その際、情報報告では米国人は匿名化されているが、国家安全保障或いは対外政策上特に重要な情

FBI と CIA には「最少化」していないデータ提供が可能である。更に、純然たる米国内通信（通信当事者が全て米国内にいる場合）ですら、次の４類型に当てはまり NSA 長官が特に認めた場合には、情報の保管配布が可能である。即ち、①重要な（significant）対外諜報情報が含まれている場合、②犯罪の証拠となる情報が含まれている場合、③暗号など技術情報が含まれている場合、④人命や財産に重大な危害をもたらす差し迫った脅威情報が含まれる場合[71]。

また、FBI の「最少化手順」[72]を見ると、対外諜報目的に止まらず、一般犯罪捜査目的でのデータの検索抽出、そして証拠としての使用を認めている。

第 702 条により収集されたデータにどれだけ米国人の情報が含まれているか、その中の米国人の情報がどれだけ利用されているか、全体像は不明である。但し、米政府の開示資料[73]にその一端を伺わせるものがある。それによれば、第 702 条による収集データで構築したデータベースにおいて、2015 年中の諜報機関(NSA、CIA、FBI 及び NCTC)による米国人対象（標的）のデータ検索件数は、通信内容については 4672 件（主として NSA と CIA。FBI を含まない）、メタデータについては 2 万 3800 件（主として NSA。CIA と FBI を含まない[74]）であった。これだけでも相当な件数であるが、

報で人定を知る必要があると考えれば、それをブリーファーを通じて要求できる。ブリーファーは報告元の諜報庁に要求を伝え、当該庁が人定開示の可否を決定する。これは、人定情報の政治利用を避けるためである。

--Karen DeYoung, "White House decries media 'lack of interest' in reports of Obama officials spying," *The Washington Post*, 3 April 2017, accessed 7 April 2017, https://www.washingtonpost.com/world/national-security/white-house-decries-media-lack-of-interest-in-reports-of-obama-officials-spying/2017/04/03/bd8650fe-18b6-11e7-bcc2-/7d1a0973e7b2_story.html?utm_term=.4d39152fc156.

--Aaron Blake, "Susan Rice isn't a 'smoking gun,' but she does have explaining to do," *The Washington Post,* 5 April 2017, accessed 6 April 2017, https://www.washingtonpost.com/news/the-fix/wp/2017/04/04/susan-rice-isnt-a-smoking-gun-but-she-does-have-some-explaining-to-do/?utm_term=.add01f20d92e

また、国家安全保障会議の元インテリジェンス担当高官（Stephen Slick）によれば、人定開示の要求は、日常的にある訳ではないが、と言って非常に珍しいことでもないという。

--Maggie Haberman and Matthew Roenberg, "Trump, Citing No Evidence, Suggests Susan Rice Committed Crime," *The New York Times,* 5 April 2017, accessed 6 April 2017, https://www.nytimes.com/2017/04/05/us/politics/trump-interview-susan-rice.html?_r=0

[71] 2015 NSA Section 702 Minimization Procedures, Sections 5, 6 参照。

[72] 2015 FBI Section 702 Minimization Procedures, https://www.dni.gov/files/documents/2015FBIMinimization_Procedures.pdf

[73] DNI, *Statistical Transparency Report Regarding Use of National Security Authorities,* 30 April 2016, accessed 6 May 2016, https://www.dni.gov/files/icotr/ODNI%20CY15%20Statistical%20Transparency%20Report.pdf

本資料と脚注 118 の資料を併せて検討すると、2015 年時点で第 702 条による収集データに対して検索できる諜報機関は、NSA、CIA、FBI、NCTC の４機関である。

[74] 開示資料には、FBI 及び他 1 機関が除かれていると記載されており、他 1 機関は CIA と推定

これらにはFBIによる検索件数は含まれていない。

FBIのデータベースでは、第702条による収集データと第105条による収集データは統合して保管されており、このデータベースで米国人について検索すると、（通信内容検索にしろ、メタデータ検索にしろ）自動的に全データを対象として検索を行うため、第702条による収集データについての検索件数を示すことはできないとされる[75]。FBIは対外諜報情報を得る目的と共に犯罪の証拠を得る目的でもデータ検索をすることが可能であり、実際、犯罪捜査目的でデータを検索するのが通常業務となっているのであるから、FBIによる検索件数は膨大な数に及ぶと推定できる[76]。「裏口からの捜索」（backdoor searches）と批判される所以である。

されている。Jenna McLaughlin, "NSA and CIA Double Their Warrantless Searches on Americans in Two Years," *The Intercept,* 4 May 2016, accessed 6 May 2016, https://theintercept.com/2016/05/03/nsa-and-cia-double-their-warrantless-searches-on-americans-in-two-years/

次の書簡によれば、CIAのシステムは、米国人に対するメタデータ検索件数を記録するようにできていない。ODNI, A letter to Senator Ron Wyden, 27 June 2014, accessed 6 January 2016, https://www.wyden.senate.gov/download/?id=184d62f9-4f43-42d2-9841-144ba796c3d3&download=1

[75] ODNI, A letter to Senator Ron Wyden, 27 June 2014.

本書簡によれば、2013年時点で第702条による収集データに対して検索できる諜報機関は、NSA、CIA、FBIの3機関である。

[76] Id.

Ⅶ　連邦憲法修正第４条と行政傍受

行政傍受は、当初修正第４条との関係が意識されることはなかったが、1967年カッツ事件で最高裁判所が刑事捜査における通信傍受を本条の適用対象となる捜索押収（search and seizure）に当ると判示したため、本条との関係が論点となってきた。

論点となったのは、コミント収集活動が本条の適用対象となる捜索押収（search and seizure）に当たるのか否か。当たるとして、国家安全保障のための通信傍受は裁判官の発する令状(warrant)を必要としない(national security exemption)のか。必要としない要件は何なのか等である。

最高裁判所や対外諜報監視裁判所の判決、決定を分析すると、対外諜報目的の通信傍受については、修正第４条の令状を必要とせず、全ての事情を斟酌して通信傍受の仕組が合理的か否かで合憲性を判断しようとする立場であり、その際、国家安全保障という最高に重要な利益と（米国人の）個人のプライバシーを保護する措置を比較衡量するとしている。

それでは、行政傍受に関連する主要な判例を見ていこう。

１　1967年カッツ対米国（Katz v. United States）最高裁判決[77]：通信傍受は修正第４条の捜索押収に当るとした事例

最高裁は、本判決において、初めて犯罪捜査のための通信傍受を修正第４条の適用対象として取り上げ、同条の捜索押収に当ることを明示した。

本件は、被告人チャールズ・カッツが公衆電話を通信手段として違法賭博を行っていたところ、FBIが公衆電話ボックスに録音機材を設置し通話を記録して、犯罪の証拠としたものである。これに対して被告人は、修正第４条に違反するとして、証拠の排除を求めて上告した。最高裁は、修正第４条は個人のプライバシーを保護するもので個人の通話も保護されるべきである、閉ざされた電話ボックス内での通話を記録することは捜索押収に当る、無令状での通話傍受は憲法が禁止する「不合理な捜索押収」であると判示した。

本判決により、通信傍受は修正第４条の捜索押収に当り、刑事事件ついては裁判所の令状が必要であるという憲法解釈が確定した。

そのため、既述したように、1968年に総合犯罪対策・街路安全法が制定されて、合衆国法典第18篇第119章において、法執行機関による通信傍受の要件や手続きが規定されたのである。

但し、本判決はその脚注において、国家安全保障に関する通信傍受について裁判官

---

[77] 389 U.S. 347.

による令状が必要か否かの問題は本事件では提起されていないとわざわざ記述し、国家安全保障に関する通信傍受には本判決が適用されないことを明示していた[78]。

２　1972 年米国対米国地区裁判所(United States v. United States District Court)、通称ケイス（Keith）事件・最高裁判決[79]：国内の安全保障目的の通信傍受でも、修正第 4 条の令状（warrant）が必要とした事例

カッツ事件で、犯罪捜査のための通信傍受には裁判所の令状が必要なことが明示されたが、それでは、国家安全保障のための通信傍受（行政傍受）にも令状が必要なのであろうか。実際、行政府は、長らく裁判所の令状を得ないで行政傍受を行ってきたのである。

これについて最高裁が初めて判断をしたのが本判決である。政府側は国家安全保障に関する通信傍受には修正第 4 条は適用されないと主張したが、最高裁は、外国勢力に係わる場合は別として、純粋に国内のみに係わる状況では、安全保障を理由とする無令状の通信傍受は修正第 4 条に違反すると判示した。

本件は、白人左派過激組織「ホワイト・パンサー党」の幹部ローレンス・プラモンドンらがミシガン州アンアーバー市の CIA 事務所前で爆弾を爆発させたなどとして起訴された事案である。被告人の弁護人は、この訴訟においてプラモンドンについて（令状なしに行われた違法な）通信傍受の記録を提出するよう要求した。これに対して FBI は、通信傍受は政府機構を攻撃し転覆しようとする国内組織の企てから国家を防護するためになされたものであり、国家安全保障のためであるので、その実施に令状は必要なく適法であるとして傍受記録の提出を拒否した。地区裁判所のケイス判事は、純然たる国内問題での行政傍受に関しては、国家安全保障を理由にした令状除外は認められないとして、傍受記録の開示を命令した。

FBI は、控訴裁判所に異議を申し立てが却下されたため、最高裁判所に異議を申し立てたが、最高裁でも却下された。このため、FBI は傍受記録を開示することは出来ないとして、起訴を取り下げた。

最高裁判決の要旨は、次の通りである。

---

[78] Id. at 358 footnote 23.　先に見たように、行政府は、憲法上の大統領権限についての行政解釈に基づき、裁判官の令状無しに国家安全保障のための通信傍受を、第二次世界大戦時から当時に至るまで実施していた。本判決は、かかる通信傍受に対して適用されないことを明示することにより、現実に行われていた無令状の行政傍受を黙認する実質的効果を有していたと言える。また、後に見るように、1970 年代においても、対外諜報のための無令状の通信傍受を容認する連邦控訴裁判所の判決は続出している。

[79] 407 U.S. 297.　本判決の意義については、次の論文が詳しい。 Trevor W. Morrison, "The Story of United States v. United States District Court (Keith): The Surveillance Power," *Columbia Public Law & Legal Theory Working Papers., 2008,* (Paper 08155). http://lsr.nellco.org/columbia_pllt/08155

最高裁は、先ず、大統領は憲法第 2 章第 1 条により、「合衆国憲法を保持し、保護し、擁護する」任務を課されており、この任務には（国家安全保障の一部である）違法な政府転覆から政府を保護する権限が暗示(implicit)されている[80]として、大統領の国内の安全保障に関する任務に憲法上の基礎を認める。その上で、一方で、政府は国内の安全保障の任務があるが、他方、不合理な監視により個人のプライバシーと表現の自由が侵害される危険があり、二つの基本的価値を比較衡量する必要があるとする[81]。そして、国内の安全保障のための監視を裁判所の関与なしに行政府に一任することは、政治的反対者の監視に濫用される危険性など問題があるとして、修正第 4 条の裁判官による事前審査、即ち、令状の対象外とはできないと結論づけている[82]。

但し、最高裁は、国内の安全保障に関連する令状制度は、犯罪捜査の制度と同一である必要はないとして、特別の手続の創設まで示唆している[83]。

更に、最高裁は、外国勢力に対する国内外での監視については、本判決の対象外であることを繰り返して強調した上で[84]、判決文の脚注で令状に拠らない監視の合憲性の可能性に言及している[85]。

ところで、最高裁判決を執筆したパウエル判事は、最高裁判事に就任前、外国勢力に対する監視については、大統領は裁判官による令状に拠らずに通信傍受が実施できるという意見を再三表明していた。且つ、外国勢力と国内勢力はしばしば相互に関係しているので、外国勢力と国内勢力の区別は意味がないとも表明していた[86]。従って、純粋に国内勢力に関して出された本最高裁判決の適用範囲は実は限定されていると見られている。

事実、本判決以降も対外諜報活動を理由とする無令状の行政傍受は継続されており、連邦の控訴裁判所ではこれを認める判決が続出しているのである[87]。

本判決後、政府は、無令状の行政傍受は、対外諜報目的に限定して行うようになった。

---

[80] 407 U.S. 297 at 310.
[81] Id. at 314-315.
[82] Id. at 320-321.
[83] Id. at 322-324.
[84] Id. at 308, 321-322.
[85] Id. at 322 footnote 20.
[86] Morrison, "The Surveillance Power," 13-15, 28.
[87] Morrison, "The Surveillance Power," 29 によれば、無令状の行政傍受を認める以下の決定が出ている。
--United States v. Brown, 484 F.2d 418 (5th Cir. 1973), cert. denied, 415 U.S. 960 (1974).
--United States v. Butenko, 494 F.2d 593 (3d Cir.) (en banc), cert. denied sub nom. Ivanov v. United States, 419 U.S. 881 (1974).
--United States v. Buck, 548 F.2d 871 (9th Cir.), cert. denied, 434 U.S. 890 (1977).

３　2002 年匿名事件決定（対外諜報監視控訴裁判所[88]、2002 年 11 月 18 日）[89]：　監視法第 105 条による監視（通信傍受）について、修正第 4 条の令状要件を満たしていない可能性はあるが、合憲であるとした事例

本事件は、対外諜報監視法第 105 条による通信傍受（行政傍受）の捜査利用（後述）に関する事案である。意見陳述人が、第 105 条の裁判所命令は修正第 4 条の令状の要件を満たしていないことを前提にして、刑事訴追を主目的とする監視（通信傍受）は修正第 4 条の令状に基づかない限り違憲であると主張した[90]のに対して、第 105 条の合憲性を判断したものである。

先ず、修正第 4 条の令状の要件について、最高裁判決は一般犯罪捜査において、①司法による事前審査、②「相当の理由」、③捜索押収する場所と物の特定の三つの要件を定めているとする[91]。そこで、司法傍受における手続と比較して、第 105 条による裁判所の命令の手続を見ると、①の司法による事前審査は満たしている。②「相当の理由」については、司法傍受では特定の犯罪が行われていると信じるに足りる相当な理由が必要であるが、本手続では、外国勢力又はその代理人であると信じるに足りる相当な理由で良く、（憲法が人権を保障する）米国人が関与する場合には外国勢力の代理人の定義は犯罪と関連付けられているが、刑事法令違反行為に関与する可能性がある程度でよいとされている[92]。③の押収物の特定では、司法傍受では特定の犯罪に関連する特定の通信であるが、本手続では、対外諜報情報の類型を示せばよいとされている[93]。

これらの検討に加え、控訴裁判所は、通信傍受の必要性の要件、傍受期間の設定、「最少化手順」、関係者への通告の有無など、本手続の特徴を司法傍受との対比で検討する[94]。

以上を踏まえ、本手続は、特に②「相当の理由」と③特定性で、司法傍受と異なるところがあり、修正第 4 条の令状の要件を満たさない可能性がある[95]。しかし、そうであっても憲法的に認められる可能性があるとする。

その上で、控訴裁判所は、大統領は対外諜報情報を入手するために無令状の捜索を

---

88 Foreign Intelligence Surveillance Court of Review.　本稿では「対外諜報監視控訴裁判所」と訳し、略称として「控訴裁判所」を使用する。
89 In Re: Sealed Case, 310 F.3d 717 (F.I.S.C. 2002), http://news.findlaw.com/hdocs/docs/terrorism/fisa111802opn.pdf
90 Id. at 38.
91 Id. at 39.
92 Id. at 40-42.
93 Id. at 42-44.
94 Id. at 44-46.
95 Id. at 46-47.

行う固有の権限を持っていることは連邦裁判所の累次の判決[96]で認められており、裁判所の義務はその憲法上の権限の境界を定めることであるとする。そして、監視法は憲法上の大統領権限を侵害(encroach)することはできず、問題は、監視法が、古典的な令状制度に近く憲法的に合理的な捜索押収と言い得る仕組を提供することによって、憲法上の大統領権限を正しく敷衍(amplify)しているかどうかであるとする[97]。

そして、一般犯罪捜査と対外諜報犯罪の特徴を比べると、一般刑事法の主目的は、行為者処罰と一般予防の二つであるが、対外諜報犯罪に関する政府の関心は圧倒的に目前の犯罪行為の阻止である。刑事司法手続は外国勢力による悪意ある取組に対抗する総合的な取組の一部であり、処罰は副次的な目的に過ぎない[98]。外国勢力によるテロやスパイ行為の脅威から国を守る監視法の制度は、一般犯罪対策とは異なるものであるとする[99]。

結論として、監視法第 105 条の手続は、修正第 4 条の令状の要件を満たさないとしても、それに近いものがあり、本手続による監視（通信傍受）は合理的であり、従って憲法修正第 4 条に適合すると述べている[100]。

本判決の解釈として、監視法第 105 条の裁判所命令は修正第 4 条の令状要件を満たしていると判断したとする説[101]もあるが、むしろ、令状要件を満たしていないことを暗黙の前提とした上で合憲性を認めたものと評価すべきであろう。その理由は上述の判決要旨に現れているが、特に次の 3 点が指摘できる。第 1 に、行政傍受の実務では、本条に基づき在米の多くの外国公館に対して恒常的に行政傍受（監視）が行われている[102]が、そのための裁判所命令が「相当の理由」と押収物の特定の両面で修正第 4 条の令状要件を満たしているとは到底考えられないこと。第 2 に、米国人を監視対象とする場合は、間接的に犯罪と関係付けられているが、一般の司法傍受と比べて本条の手続要件は相当緩やかなものになっていること。第 3 に、判決理由の全体構成が、司法傍受の手続要件と対比してその違いを指摘した上で、対外諜報情報の特殊性を強調して、本条による捜索押収は合理的であると結論付けていることである。

---

96 本決定は、無令状での文書の捜索押収が問題となった次の判決を例示する。U.S. v. Truong, 629 F.2d 908 (1980) at 914.

97 Id. at 48-49.

98 Id. at 52-53.

99 Id. at 55.

100 Id. at 56.

101 Steve Vladeck, “More on Clapper and the Foreign Intelligence Surveillance Exception,” *LAWFARE*, 23 May 2012, accessed 2 September 2016, https://www.lawfareblog.com/more-clapper-and-foreign-intelligence-surveillance-exception

102 茂田「米国国家安全保障庁のシギント収集プラットフォーム」196-198 頁及び茂田『米国国家安全保障庁の実態研究』91-92 頁参照。

4　2008年ヤフーに対する協力命令に関する決定（対外諜報監視控訴裁判所、2008年8月22日）[103]：監視法第702条の監視（通信傍受）について、修正第4条の令状条項は適用されないとした事例

本件は、「プリズム」という行政傍受の秘密計画に関するものである。

2007年に改正追加された対外諜報監視法第105B条（現702条）に基づいて、司法長官と国家諜報長官が共同で監視（行政傍受）を認可して同年11月に民間通信事業者ヤフーに対して協力命令を発し、更に、監視裁判所が事業者に協力の強制命令を発したところ、ヤフーが修正第4条に違反する無令状の捜索押収であるとして控訴裁判所に異議を申し立てたものである。

裁判当時は、裁判関係事項は殆ど公表されなかったが、控訴裁判所の意見だけが機密部分を削除して2009年1月に開示された。2014年9月に至り、より多くの訴訟関係文書が開示されたが、理論的部分は2009年の開示決定に尽くされているので、これを基に控訴裁判所の論旨をみると次の通りである。

裁判所は、先ず、本件は、国家安全保障上の利益と、修正第4条が保障する米国人のプラバシーの利益の比較衡量を必要とする問題であるとする[104]。

その上で、本件の監視（行政傍受）については、修正第4条の令状は必要ないとしている。その理由は、第1に、最高裁判所は、従来から、令状や「相当の理由」を要求することが実際的ではなく『特別の必要』がある場合には、令状を不要としてきた。例として、警察官が職務質問の際に自己の安全を守るために対象者の服の外から武器の有無を調べる行為（pat-frisk）などを列挙する[105]。第2に、本件で問題となっている、国家安全保障目的で、国外にいると合理的に信じられる外国勢力及びその代理人を対象として行う監視は、通常の法執行の問題とは異なり、政府の利益が特に強烈(particularly intense)である[106]。第3に、外国勢力の監視では迅速性、秘密性、秘匿性が極めて重要であり、令状を要求することは、政府が緊急性のある情報を収集する能力を阻害し、国家安全保障という肝腰な利益を害する可能性がある[107]。これらの理由から、監視が、国家安全保障を目的として対外諜報を得るために行われ、国外にいると合理的に信じられる外国勢力及び代理人を対象としている場合には、修正第4条の令状の要求は対外諜報には適用されないと考えると結論付けている。

但し、令状を要件としないことは、政府に完全な裁量権を与えるものではない。修

---

[103] In Re: Directives to Yahoo! Inc. Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004(Foreign Intel. Surv. Ct. Rev. 2008), https://fas.org/irp/agency/doj/fisa/fiscr082208.pdf

[104] Id. at 3.

[105] Id. at 13.

[106] Id. at 13-14.

[107] Id. at 17.

正第 4 条は不合理な捜索押収を禁止しており、監視が合理的である必要がある。合理的であるか否かは、全ての事情を斟酌して判断する必要があるが、守られるべき政府の利益と比較して個人のプライバシーの利益を守るため十分な措置が採られているか、比較衡量する必要がある。そして、政府の利益がより重大であれば憲法的に許容される個人のプライバシーの侵害はより大きくなるとした上で、問題となっている政府の利益は国家安全保障上の利益であり「最高に重要なもの」（of the highest order of magnitude）である。この重要な利益に鑑みてプライバシー保護が合理的か否かを判断する必要があるとする[108]。

その上で、本件通信傍受の運用全般を検討して、「標的決定手順」「最少化手順」や、大統領命令第 12333 号 2-5 の規定の準用（米国人を対象とする時は、同人が外国勢力の代理人であると信じる相当な理由があることを司法長官が認定すること）など、プラバシーの保護措置を列挙する[109]。

結論として、政府は、国民の安全という国家にとって最重要な利益を守る責務を負っている。そして、政府が不当な侵害から個人を守り付随的なプライバシーへの侵入を最少化する各種の保護措置を制度化している以上、裁判所は国家安全保障を保護しようとする政府の努力を妨害すべきではないと結んでいる[110]。

本命令は、対外諜報目的の監視（通信傍受）について令状要件の除外（いわゆる foreign intelligence exception）を認めたものであるが、対外諜報について無条件に令状要件を除外したものではない。法第 105B 条で定めた枠組内で外国にいる者を標的として行なう対外諜報に令状要件の除外を認めたものである。そのため、一見、除外範囲は狭いようにも見える。しかし、次の理由から実際上の除外範囲は広いと言える。

第 1 に、プリズム計画で取得される通信のデータは全て、米国内のデータセンターから取得されるのであり、全て米国内での捜索押収である。米国内での捜索押収に令状要件を除外しているのである。

第２に、外国にいる者を標的にした監視であれば、標的とした外国にいる者と米国内の米国人との通信も取得できるのである。そして、米国内の米国人同士のインターネット通信であっても、それを「cc」で外国にいる者に送信すれば、その通信も取得できるのである。

第３に、第 105B 条では、外国にいる米国人を標的とする米国内からの収集でも、修正第４条の令状を必要とせず、司法長官の決定があれば可能としている点である。（なお、2008 年改正の対外諜報監視法第 703 条では、この事例については裁判所の命令が必要となった。）

---

[108] Id. at 17-19.
[109] Id. at 21-25.
[110] Id. at 28-29.

なお、本決定と先に見た 2002 年匿名事件決定を合わせて解釈すると、対外諜報監視裁判所の論理に従えば、対外諜報監視法は、行政府が対外諜報のために国内で監視（通信傍受）する権限を創設したものではなく、大統領が元来持っている憲法上の権限を敷衍したものである。従って、仮に対外諜報監視法が何らかの理由で廃止されることがあった場合、大統領は対外諜報のための監視（通信傍受）が出来なくなるのではなく、依然として憲法に基づく大統領権限として監視を行う余地があることとなる。その場合は、国家安全保障上の利益と憲法修正第 4 条が保障する米国人のプライバシーの利益を均衡させる合理的な行政的仕組を作ることが課題であるが、具体的な仕組が合理的であるか否かの判断は、その際の国家安全保障を取り巻く環境にも影響を受けることになろう。

５　まとめ：　本章で述べたところを、簡単に表記すると次の通りである。

行政傍受に関する法制の基本構造

＜一般的権限＞米国内外
憲法第 2 章第 1 条に基づく国家安全保障上の大統領権限
大統領命令第 12333 号「合衆国諜報活動」

＜米国内において＞
憲法修正第 4 条（不合理な捜索・拘束押収の禁止）の適用。
1967 年カッツ判決（最高裁）～通信傍受は「捜索押収」に該当。

○　純粋に国内の安全保障に係わる通信傍受
1972 年ケイス判決（最高裁）～修正第 4 条の裁判官の令状が必要。

⇒現在に至るまで、令状制度は未整備。

○　対外諜報に係わる通信傍受
対外諜報監視控訴裁判所：2002 年匿名事件決定
2008 年ヤフーに対する協力命令に関する決定
～修正第 4 条の規定する裁判官の令状は不要。但し、
修正第 4 条が禁止する不合理な捜索押収であってはならない。

⇒「対外諜報監視法」の適用
同法は「合理的な捜索押収」を定式化したもの。即ち、憲法上の大統領権限を、国家安全保障上の利益とプライバシーの保護の二つの基本的価値の均衡を図りながら、敷衍したもの。
いわば、権限確認規定であって、権限創設規定ではない。

Ⅷ　行政傍受情報の捜査利用

対外諜報目的の行政傍受では、修正第 4 条に規定する令状なしに多量の情報が収集されており、これには米国人情報も含まれる。そこで、これら情報の犯罪捜査利用はどのように捉えられているのかを、次に見てみよう。

1　行政傍受情報の捜査利用

先ず、行政傍受情報の捜査利用は、実態としては幅広く行われていると推定できる。国家諜報長官室の公式文書[111]には、米国インテリジェンス社会の主たる顧客として、（大統領や閣僚などの）政策決定者、軍隊、法執行機関の三者が挙げられている。法執行機関が顧客として挙げられる理由は、テロ対策や薬物対策が主体と考えられるが、他の一般治安対策での支援も含まれていると考えるべきであろう。

非米国人との関係では、行政傍受情報の捜査利用は何ら問題はないと考えられている。国家安全保障法第 105A 条では、連邦政府の法執行機関の要請を受けて、米国の諜報機関は、国外の非米国人を対象として法執行目的での情報収集ができるとまで規定されている[112]。

問題となるのは、憲法修正第 4 条との関係であり、米国人に関する行政傍受情報の捜査利用が認められるかである。司法傍受よりも緩い要件で実施された行政傍受による取得情報を刑事司法手続で使用するのは、修正第 4 条による人権保障を潜脱することにならないのであろうか。この点については、米国政府の立場は問題がないというものである。例えば、2014 年 3 月司法省職員（attorney）は「一旦適法に収集され既に政府保有となった情報については、その情報内容を検索するのは憲法修正第 4 条で規制される捜索には当たらない」と説明している[113]。

この論理では、適法に政府保有になった情報については、憲法修正第 4 条の規制は問題にならないのであるから、必要に応じて幅広く利用できることとなる。そして、この考え方に従い捜査利用に関する法令が定められ、現実に一般犯罪捜査を含め幅広く利用されていると見られる。

---

111 US, ODNI, “National Intelligence Program,” January 2016, accessed 14 January 2016, https://fas.org/irp/budget/nip-fy2016-fs.pdf

112 National Security Act of 1947, amended through August 2007, Sec. 105A.
但し、国防総省関連の諜報機関で、法執行目的の支援ができるのは、国家安全保障庁 NSA, 国家偵察局 NRO，国家地理空間諜報庁 NGA、国防諜報庁 DIA の 4 機関に限定され、陸海空軍海兵隊それぞれの諜報組織は除外されている。

113 Spencer Ackerman, “NSA searched data troves for 198 ‘identifiers’ of Americans’ information,” *The Guardian,* 30 June 2014, accessed 16 September 2016, http://www.theguardian.com/world/2014/jun/30/nsa-data-troves-identifiers-information

行政傍受情報の捜査利用に関する法令も、行政傍受の法体系に応じて二つの体系がある。大統領命令第 12333 号に基づくものと、対外諜報監視法に基づくものである。それぞれについて見てみよう。

（１）大統領命令第 12333 号「合衆国諜報活動」の体系

大統領命令第 12333 号「合衆国諜報活動」は、第 2 部「諜報活動の実施：３情報の収集」で、米国人に関する情報の収集と配布を規制する手順を定めるべき旨を規定しているが、(i) 号では、付随的に得られた情報であって、連邦、州、地方或いは外国の法令に違反するかも知れない活動に関する情報は、その収集保持配布を認める旨を定めている[114]。

これを受けて各諜報機関は、関連する諸規程を定めている[115]。その中の代表例として国家安全保障庁 NSA の規程 Procedures Governing NSA/CSS Activities That Affect U.S. Persons[116]を見ると、犯罪の証拠である通信或いは情報は法執行目的の配布であれば、米国人の人定を含めて許される旨規定されている[117]。

（２）対外諜報監視法の体系

対外諜報監視法第 101 条(h)は、「最少化手順」を定義している。「最少化手順」は元来、米国人に関する非公開情報の保持と配布を最少化して、米国人のプライバシーを保護するための手順である。ところが 101 条（h）(3)は、犯罪の証拠であって法執行目的での保持と配布を認めるべき情報について、同手順でその保持と配布の手順を定める旨を規定している。

現在、監視法第 702 条による電子的監視で要求される「最少化手順」が一部黒塗りながら公表されている[118]。そこで先ず、国家安全保障庁 NSA の「最少化手順」を見る

---

114 EO 12333 United States Intelligence Activities, Part 2 Conduct of Intelligence Activities, 2-3 Collection of Information.

115 この諸規程の多くは、2016 年 7 月に情報公開された。”Statues of Attorney General Approved U.S. Person Procedures Under E.O. 12333,” *CRYPTOME*, 14 July 2016, accessed 22 July 2016, ttps://cryptome.org/2016/07/EO12333-AG-Guidelines-for-PCLOB-July-2016.pdf を参照。

116 NSA/CSS Policy 1-23, “Procedures Governing NSA/CSS Activities That Affect U.S. Persons,” 11 March 2004, revised through 29 May 2009, https://www.dni.gov/files/documents/1118/CLEANED022.%20NSA%20Core%20Intelligence%20Oversight%20Training.pdf

117 前註記載文書中の”ANNEX: Classified Annex to Department of Defense Procedures Under Executive Order 12333, Sec. 4 Procedures, A4(l) を参照。

118 ODNI, “Release of 2015 Section 702 Minimization Procedures,” *IC on the Record*, 11 August 2016, accessed 16 September 2016, https://icontherecord.tumblr.com/post/148797010498/release-of-2015-section-702-minimization. ここでは、次の 4 つの「最少化手順」が、一部黒塗りながら開示されている。

--2015 NSA Section 702 Minimization Procedures

--2015 FBI Section 702 Minimization Procedures

と、犯罪の証拠が含まれると合理的に信じられる通信については、国内通信（全通信当事者が米国内にいる通信）でも米国人が当事者となる外国通信でもその保持と配布を認めている[119]。更に、FBI に対しては、収集した情報を「最少化」せずに生データを提供することを認めている[120]。

次に、FBI の「最少化手順」を見ると、収集データを対外諜報目的と同時に法執行目的でも使用することが全体を通じて明確に打ち出されている。FBI では、連邦犯罪の防止と連邦犯罪からの保護のため、収集データを検索することが通常業務となっていることが明瞭である[121]。また、FBI は法執行目的のために生データを含む情報を、検察官や他の連邦、州、地方の法執行機関に提供できることが明確に規定されている[122]。

これら「最少化手順」は、監視裁判所決定（2015 年 11 月）[123]によって適正なものであると承認されている。決定に際しては、意見陳述人が、FBI「最少化手順」は、対外諜報目的と共に一般犯罪捜査目的でデータを検索抽出し証拠として使用できこととしているのは、憲法修正第 4 条違反であると主張したのに対し、監視裁判所は、データを FBI が一般犯罪捜査に使用できるとしても、第 702 条と「標的決定手順」「最少化手順」等の全体の制度枠組は、対外諜報目的のため適正に構築されているので、修正第 4 条に違反しないと認定している[124]。

また、2016 年 12 月第 9 巡回控訴裁判所は、対外諜報監視法第 702 条による情報が捜査の端緒となった爆弾テロ未遂事件について、「第 702 条に由来する」（derived from Sec.702 surveillance）証拠の価値を認める判決を出している[125]。

--2015 CIA Section 702 Minimization Procedures
--2015 NCTC Section 702 Minimization Procedures

[119] NSA Procedures の Section 5(2), Section 6(a)(3), (b)(8)参照。

[120] NSA Procedures の Section 6(c)(2)参照。

[121] FBI Procedures の III D footnote 3 を特に参照。

[122] FBI Procedures の III F, ＶB 参照。

[123] Foreign Intelligence Surveillance Court, Memorandum Opinion and Order, 6 November 2015, accessed 23 May 2016, https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf

[124] Id. at 26-36, 39-44.　なお、本決定は 702 条 g 項（2）（ｖ）は、データ収集の目的に関して、対外諜報情報の取得を重要目的（a significant purpose）と規定し、主要目的（a primary purpose）と規定してないことを指摘して、収集データの利用を対外諜報目的に限定する必要はない旨述べている。

[125] United States v. Mohamed Osman Mohamud, No 14-30217, 2016 (9th Cir. 5 December 2016), http://caselaw.findlaw.com/us-9th-circuit/1756495.html
--US DOJ, *Convicted Bomb Plotter Sentenced to 30 Years,* 1 October 2014, accessed 12 December 2016, https://www.justice.gov/nsd/pr/convicted-bomb-plotter-sentenced-30-years.
--Jenna McLaughlin, "Americans Have Hewer Privacy Rights When Emailing People Overseas, Court Rules," *The Intercept,* 8 December 2016, accessed 9 December 2016, https://theintercept.com/2016/12/07/americans-have-fewer-privacy-rights-when-emailing-pe

なお、2015 年初に出された国家諜報長官室の文書によれば、第 702 条によって付随的に収集された情報の法執行での使用は自主規制を行い、犯罪の証拠として法廷に提出されるのは、国家の安全保障に係わる場合と一定の重要犯罪の場合に限定するとしている[126]。

上記から、米国では、適正に行われた行政傍受によって収集された情報を刑事司法手続において利用することが認められていることは明白である。

２　捜査利用目的の行政傍受

ところで次に、刑事司法手続に使用する目的を持って実施要件の緩い行政傍受を行うことが許されるのだろうか。被疑者の人権保障という観点からは、許されるべきではないという主張がなされると考えられるが、米国では許されるのである。本件に関する裁判所の判断を見てみよう。

本件は、対外諜報監視法第 105 条による監視（通信傍受）のための「最少化手順」に関する事案である。1978 年に監視法が制定され第 105 条による監視が開始されて以来、同条による対外諜報情報を法執行に利用する手続が定められ、それに従って実施されてきた。即ち、当時有効な 1995 年 11 月制定の手順は、対外諜報監視法によって収集した情報の刑事捜査での利用は認めていたものの、検察官がその収集を指揮統制してはならないと定めていた[127]。要するに対外諜報情報を捜査で利用するのは良いが、捜査目的で対外諜報監視法の監視を行ってはならない旨定めていたのである。

ところが、2001 年に愛国者法が制定され、対外諜報監視法が改正された。そこで、司法長官は、2002 年 3 月に「最少化手順」の補則手順を定め、監視裁判所の承認を求めたのである。

本補則手順[128]は、インテリジュンス部門と捜査部門間の情報共有と協力を進めるも

---

ople-overseas-court-rules/

本件は、米国人モハメッド・モハムド（当時 19 歳）が大量殺人を目的としてポートランド市のクリスマス点灯式会場で自動車爆弾を爆発させようとした事案の控訴審判決である。同人は、FBI の囮捜査によって検挙されたのであるが、捜査の端緒の一つが監視法第 702 条に基づく情報であった。即ち、ICPO 赤手配者でテロ容疑者であるサウジアラビア人アムロ・アル・アリを標的とした第 702 条に基づく通信傍受によって、米国内に居住するモハムドとの通信が付随的に捕捉されたものである。アル・アリとの通信はモハムドの犯意と情状を評価するために重要な情報であったため、法廷に提出されたようである。

[126] ODNI, *Signals Intelligence Reform 2015 Anniversary Report*, January 2015, accessed 26 September 2016, https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

[127] Attorney General, Memorandum, “Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations,” 19 July 1995, accessed 21 September 2016, https://fas.org/irp/agency/doj/fisa/1995procs.html

[128] Attorney General, Memorandum, “Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI,” 6 March

のであり、FBI 捜査部門や司法省検察官に対して、対外諜報情報の捜査利用に止まらず、通信傍受の実施ついて助言を認めるものであった。また、司法長官は、愛国者法の成立により「対外諜報監視法は、対外諜報が重要目的（a significant purpose）である限り、主として(primarily)法執行目的でも使用できる」と主張した[129]。

そこで、この手順を認めるか否かが争点となったのである。

（１）2002 年対外諜報監視裁判所に提出された全ての事案に対する意見と命令（対外諜報監視裁判所、2002 年 5 月 17 日）[130]

監視裁判所は、司法省の「手順」提案の一部を拒否したのである。

その理由は、先ず議論は米国人にのみ関係すると限定した上で[131]、本手順は、対外諜報監視法による監視や捜索の開始・実施・継続・拡大について、刑事検察官に FBI のインテリジェンス担当者に対する助言を認めるものであり、これは犯罪捜査と訴追を進めるために本裁判所の命令を使用しようとするものであり、認められないとする[132]。

そして、裁判所は、手順を修正して、法執行官は監視法による捜索や監視に関してインテリジェンス担当者に助言をしてはならず、FBI や司法省刑事部は、法執行官が刑事訴追を進めるために同法の権限の使用を指示したり統制しないようにしなければならないと命令した[133]。

本決定そのものに対して司法省は控訴しなかったが、その後監視裁判所が本決定に基づき個別の具体的な監視事案について制限を課したため、関連して本決定について控訴裁判所が審理することとなった。

（２）2002 年匿名事件決定（対外諜報監視控訴裁判所、2002 年 11 月 18 日）[134]

控訴裁判所は先ず、原審は、監視法が、行政府内のインテリジュンス部門と捜査部門との間に障壁を作っていることを前提としているが、これは法律に根拠が無い。また、政府の監視目的が主として刑事訴追ではない場合にのみ、監視裁判所は監視（行政傍受）命令を出せると理解しているが、これも法律に根拠が無いと述べる[135]。

その上で、監視法の性格について、法律の構造[136]から見て、監視法の目的から対外

2002, accessed 21 September 2016, https://fas.org/irp/agency/doj/fisa/ag030602.html

[129] Id.

[130] In re All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F.Supp.2d 611.

[131] Id. at 614.

[132] Id. at 624.

[133] Id. at 626-627.

[134] In Re: Sealed Case, 310 F.3d 717 (F.I.S.C. 2002), http://news.findlaw.com/hdocs/docs/terrorism/fisa111802opn.pdf

[135] Id. at 5-6.

[136] 外国勢力の代理人の定義が、米国人の場合は犯罪と関係づけられていることを例示している。

諜報犯罪での訴追が排除されていると考えるのは不可能である。また、対外諜報情報に、対外諜報犯罪の証拠も含まれることは、立法過程からも明白であるとする[137]。そして、政府の最優先目的は、外国勢力（及びその代理人）によるテロやスパイ活動を阻止することであるが、刑事訴追もそのための一手段であり、監視法は、対外諜報情報を刑事訴追で使用することを全く制限していないとする[138]。

次に控訴裁判所は、2001 年愛国者法による監視法改正の趣旨を原審は過小評価しているとする。先ず、監視法第 104 条（a）(7)(B)が改正されたが、改正前は「対外諜報の収集」が監視の主たる目的（the purpose）であったが、改正により重要な目的（a significant purpose）で足りることとなったと指摘して、「監視対象が潜在的な諜報情報源であり且つ刑事訴追の潜在対象である場合に、本改正により法執行部門が監視裁判所の命令を得やすくなる」という立法当時の上院議員の議会発言を引用している[139]。

そして、外国勢力の代理人に対処する際に、政府に刑事訴追以外に何らかの現実的な対処手段が残されている限り、「対外諜報の収集」という監視の「重要な目的」を満たしているのであり、本改正により、監視裁判所が、刑事訴追とその他の対抗措置のどちらに政府が重きを置いているかを比較する必要はなくなったとする。監視の目的が、刑事訴追よりも広く、進行中の陰謀の阻止など訴追以外の潜在的対抗手段が含まれている限り、要件を満たすのであるとしている[140]。

即ち、純粋に過去のテロ事件やスパイ事件捜査であって現在に脅威を及ぼさないものであれば、現在の脅威の阻止が成り立たないので監視法による通信傍受は許されない。しかし、現在進行中の（或いは将来の）脅威がありこれを阻止する目的がある限り、監視法による通信傍受は認められ、且つ監視法による傍受情報を犯罪の証拠として使用することも自由であることとなる。そうなると、テロ調査（捜査）やスパイ調査（捜査）では、純粋な過去の事件捜査など稀であり現在の脅威への対処が基本であるから、訴追目的を保持していようとも、常に監視法による通信傍受ができることとなる。

更に捜査部門と諜報部門の関係について、控訴裁判所は、改正第 106 条(k)は、捜査部門と諜報部門の障壁を除去するために追加された条項であり、両部門の活動を調整するために両部門が協議することができる旨を規定している。協議には字義的に勧告も含むものである。そして、この調整や協議において、捜査、諜報の両部門の役割は何も規定されていないのであるから、何れの部門が指導性を発揮しようと問題ないと

---

137 In Re: Sealed Case, 310 F.3d 717 (F.I.S.C. 2002), 11-12.
138 Id. at16.
139 Id. at 29.
140 Id. at 34-35.

まで述べている[141]。

本決定は、1978年の対外諜報監視法制定以来、インテリジュンス部門と捜査部門の間に築かれてきた「壁」（Wall）を崩壊させたと評価されており[142]、テロ対策、スパイ対策を行うインテリジュンス機関（兼捜査機関）の言い分を100%認めたものである。

３　パラレル・コンストラクション（Parallel Construction）

米国では、行政傍受情報の捜査利用が広く認められていることが以上の分析から明確になったが、他方、実際の行政傍受情報の捜査利用、その具体的事例については、報道されることは少ない。

これは、行政傍受情報の捜査利用が余りなされていないことを示すのであろうか。

この点について参考になる報道がある[143]。報道は、FBIではなく、麻薬取締局DEAの捜査に関するものであるが、機微な情報源や捜査手法を秘匿する必要があるときは、捜査の真の端緒を秘匿して、被告人、或いは検察官や裁判官に示すための、「端緒」を作り出す手法である。パラレル・コンストラクションと呼ばれる。DEAには特別作戦部（Special Operations Division）という数百人規模の部署があるが、この特別作戦部からの捜査の端緒情報は、捜査書類、令状請求、検察官、公判廷、外国機関等に秘匿することとされている。同部からの端緒情報には、国家安全保障庁NSAや秘匿協力者からの情報が含まれるとされる。そこで、暴露されたパラレル・コンストラクションの実例を見ると、真の端緒情報は国家安全保障庁からのコミント情報であるにもかかわらず、捜査官はそれを隠して、検察官に対して秘密の協力者から得た情報が端緒であると述べた事例がある。

このパラレル・コンストラクションという技法は、機微な情報源を秘匿するため、DEAに限らず、FBIでも広く使われていると考えられる。そして、一般に行政傍受、特に、大規模に行われている行政傍受は、間違いなく一般には知られたくない機微な情報源であり、秘匿されているものと考えられる。

---

[141] Id. at 30-31.

[142] McAdams, *Foreign Intelligence Surveillance Act (FISA): An Overview,* 6-8.

[143] John Shiffman and Kristina Cooke, "Exclusive: U.S. directs agents to cover up program used to investigate Americans," *Reuters*, 5 August 2013, accessed 16 September 2016, http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805

Ⅸ　メタデータの取扱

最後に、一般には余り注目されていないが、実務上は極めて重要なメタデータの取扱について分析したい。

１　メタデータの定義と有用性

メタデータとは、通信内容を除く通信に付随する情報の全てと定義されている。

具体的には、携帯電話通話であれば、通話当事者の電話番号、携帯端末識別番号(IMEI)、利用者識別番号（IMSI、シムカードに記載)、回線識別符号、通話日・時刻、通話時間、テレホンカード番号、携帯端末位置データ等である。また、インターネット通信であれば、当事者のメールアドレス、IP アドレス、通信日・時刻、通信時間、更には、SNS 通信の通信内容以外のデータ、ネットワークに於ける活動履歴（訪問ウェブサイト、ログイン時刻、地図検索履歴等)、その他各種のデータが該当する。

メタデータには、通信内容そのものは含まれないものの、情報価値は極めて高い。大量のデータ分析により情報を抽出できるのである。人間関係の分析、人物分析、行動分析などができ、更に位置情報を利用して無人攻撃機による攻撃にも使われており、米国諜報社会が極めて重視している情報である[144]。

既述したように、米国国家安全保障庁は多様な方法でデータ収集（行政傍受）を行っているが、その収集データの中から、メタデータ専用のデータベースを作成して情報分析に役立てている。また、FBI を含む諜報コミュニティのためのメタデータの分析システムも存在する位である[145]。

ところで、メタデータで重要なのは、米国政府がメタデータ収集には憲法修正第４条が適用されないと考えていることである。米国政府は、2013 年 9 月に発表した白書で、電話メタデータに関して次の立場を取っている。即ち「連邦最高裁判所の諸判決によれば、電話通話者は電話番号を通信事業者に任意に提供している。そして、電話メタデータは、通信事業者が料金徴収その他の業務目的で通常保管している情報である。そして、このように通信事業者に顧客が任意に提供した情報については、これを政府機関に提供する際に、憲法修正第４条の問題は生じない。通信事業者のデータ保管場所まで、個人のプライバシーの期待権は及ばない[146]。」そして、この論理は、電話に限らず、インターネット・メタデータでも同様である。

---

144 詳細については、茂田『米国国家安全保障庁の実態研究』105-114 頁参照。

145 前掲、111 頁参照。

146 US, *Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act,* 9 August 2013, 19-21, accessed 11 November 2014, http://big.assets.huffingtonpost.com/Section215.pdf

従って、米国内でも法律に違反しない限り、メタデータの収集が可能であるということになる。

２　憲法修正第４条との関係についての裁判所の判断

通信メタデータは修正第 4 条の保護対象にならないという判断は、架電先電話番号について、1979 年の最高裁判決で初めて示された。そして、この最高裁判決の論理に従う限り、その他の通信メタデータも修正第 4 条の対象とならないこととなる。実際に、各種の通信メタデータに関して、その後各地の連邦控訴裁判所で、修正第 4 条の保護対象とならないという判決が続出している。ここでは、1979 年最高裁判決と、最新の電話位置情報に関する連邦控訴裁判所判決を見てみよう。

（１）1979 年スミス対メリーランド州（Smith v. Maryland）最高裁判決[147]：　架電先電話番号は修正第４条の保護対象には当たらないとした事例

本件は、警察の要請により電話会社が、裁判所の令状なしに会社施設内にペンレジスター（PR 架電先電話番号記録装置）を設置して、強盗容疑者が自宅から架けた架電番号を記録した事案である。被告人は、無令状の記録装置の設置は修正第 4 条に違反しているので、これによる証拠を排除するべきであると主張したが、メリーランド州の裁判所が認めなかったので、最高裁で審理することとなった。

最高裁は、修正第 4 条はプラバシーの正当な期待権を保護しているが、架電番号は電話会社に通知され、会社は業務上の必要からこれを記録して使用している。従って、架電番号が一般に秘匿されることを期待することはできない[148]。また、第三者に任意に提供された情報については、プラバシーの正当な期待権は存在しないというのが累次の最高裁判決である。1976 年のミラー事件で、銀行口座の情報のように第三者（銀行）が限定した目的で使用すると信頼して提供した場合でも、プライバシーの正当な期待権は生じないと判示しており[149]、架電番号も同様である[150]。従って、架電番号取得装置の設置と使用は、修正第 4 条の捜索に該当せず、令状を必要としないと判示した[151]のである。

（２）メタデータに関する最近の裁判例～2016 年米国対グラハム事件判決（第４巡回控訴裁判所）[152]：電話位置情報は修正第 4 条の保護対象には当たらないとした事例

本事件は、強盗で逮捕された犯人の余罪追及のために、犯人の携帯電話の位置情報

---

147 442 U.S. 735.
148 Id. at 742-743.
149 United States v. Miller, 425 U.S. 435(1976).
150 442 U.S. 735. at 743-744.
151 Id. at 735.
152 United States v. Graham, Nos 12-4658/4825, 2016 (4th Cir. 31 May 2016)

履歴[153]を取得した事案である。警察は、合衆国法典第 19 編第 1 部第 121 章の 2703 条(c)(d)項により、修正第 4 条の令状よりも緩い要件で発布される裁判官命令によって、通信事業者から位置情報履歴を取得した。被告人は、これは憲法修正第 4 条違反であるとして証拠排除を要求したものである。

第四巡回控訴裁判所は、携帯電話の位置情報は第三者（通信事業者）に任意に提供された情報であり、修正第 4 条の保護は及ばない。第三者が限定された目的でのみ使用すると信頼して提供した情報であっても同様である[154]。このような「第三者理論」(third party doctrine)は、現代の状況に合致しないかも知れないが、最高裁判所の確立した判例であり、最高裁判所の判断が変わらない限り、位置情報履歴が修正第 4 条の保護対象になることはない[155]と明言している[156]。

これらの判決を読む限り、最高裁判所が、必ずしも、通信メタデータは全て修正第 4 条の保護対象ではないと判示した訳ではないが、他方、保護対象とする判決は存在しない。現状では、通信メタデータは修正第 4 条の保護対象ではないとの政府解釈に沿って各種制度が運用されていると言えよう。

３　電話メタデータと愛国者法第 215 条（対外諜報監視法第 501 条）の問題

電話メタデータ収集では、2013 年 6 月に元 NSA 勤務員スノーデンによる告発により、FBI が愛国者法第 215 条に基づいて米国内の電話メタデータを包括的に収集していたことが暴露され、政治問題化した。そこで、本件の経緯と結末について概観して見たい。

（１）米国における電話メタデータの包括収集の開始（2001 年）[157]

9/11 同時多発テロ事件後、当時の NSA 長官マイケル・ヘイデンは、ブッシュ大統領からテロ対策のため情報収集の強化を命ぜられたが、その際、対策の一つとして通信メタデータの利用を提案した。即ち、米国関連の電話やインターネット通信のメタデータを収集して、これを分析することにより未知のテロリストを発見しようとしたの

---

[153] 本件でいう位置情報履歴とは、携帯電話で通話した際、及びテキストメッセージを送受したした際に通信を中継した最寄りの電話電波塔の位置情報の履歴である。Id. at 12.

[154] Id. at 5-6.

[155] Id. at 36-37.

[156] Id. at 21-22. 本判決は、メタデータを修正第 4 条の保護対象でないとした連邦控訴裁判所の判決を列挙しているが、その一部は次の通りである。

--United States v. Reed, 575 F. 3d 900(9th Cir. 2009)　電話の入電番号

--United States v. Bynum, 604 F. 3d 161(4th Cir. 2010)　メールアドレス、電話番号等

--United States v. Suing, 712 F. 3d 1209(8th Cir. 2013)　インターネットの IP アドレス

--United States v. Forrester, 512 F.3d 500(9th Cir. 2008) 閲覧ウェブサイトの IP アドレス

[157] この経緯については、次の資料が詳しい。NSA, Office of the Inspector General, *ST-09-0002 Working Draft*, 24 March 2009、accessed 6 November 2014, https://www.aclu.org/files/natsec/nsa/20130816/NSA%20IG%20Report.pdf

である。

必要なデータは、従来からの国外での通信傍受に加え、米国内の主要通信事業者三社の任意の協力を得て取得することとなった。

こうして、米国関係電話通話メタデータの包括収集が始まったが、この協力は極めて有効であり、2003 年時点では、三社の協力により米国関与国際通話の８１％のメタデータが取得可能であった[158]。

（２）愛国者法第 215 条によるメタデータ収集開始（2006 年）

ところが、2006 年 5 月に、電話通信会社が電話通話メタデータを極秘裏に政府に提供していることが暴露報道された。このため三社の任意の協力が得難くなり、着目されたのが愛国者法第 215 条による業務記録の提供命令である。

愛国者法は 2001 年の 9/11 同時多発テロ事件の後に対策法として急遽制定されたものであるが、同法第 215 条は、対外諜報情報入手或いはテロ対策と防諜のため、FBI 長官は、業務記録が「ある認可された調査に関連する（relevant to an authorized investigation)」と信じる合理的な根拠がある場合には、監視裁判所の命令（order）を得て当該業務記録の提出を受けることができるというものである。

この規定に基づき、FBI はテロ対策調査のため米国関連の全ての電話通話のメタデータが必要であるとして、監視裁判所の命令を得て、電話通信事業者上位三社に対して、三社が保有する電話メタデータ全てを NSA に対して提供させ、メタデータのデータベースを構築し、NSA と FBI が分析に使用していたのである。

このような膨大なデータを要求できた背景には、電話メタデータの収集は憲法修正第４条でいう押収に当らないという解釈がある。そのため、収集すべき個別のメタデータを特定することなく、業務記録の提出として包括的に収集できるという解釈が生まれたのである[159]。

（３）連邦控訴裁判所による違法判決：2015 年 ACLU 対クラッパー事件判決（第２巡回控訴裁判所）[160]

しかし、この事実が 2013 年 6 月に暴露報道されると、さすがの米国人もそのデータ

---

158 *Id.* 27.

159 *DNI Clapper Declassifies and Releases Telephone Metadata Collection Documents,* 31 July 2013, accessed 11 November 2014, http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/908-dni-clapper-declassifies-and-releases-telephone-metadata-collection-documents.参照。

なお、上記 *Metadata Collection Documents* によれば、収集対象データは、通話当事者の電話番号、携帯端末識別番号（IMEI)、利用者識別番号（IMSI)、回線識別符号、通話日・時刻、通話時間、テレホンカード番号他である。

160 ACLU v. Clapper, No 14-42 (2nd Cir. 2015), http://law.justia.com/cases/federal/appellate-courts/ca2/14-42/14-42-2015-05-07.html

量の膨大さと包括性には驚いて、プライバシーの侵害ではないかと注目を集めた[161]。

そこで、同月アメリカ市民自由連合（American Civil Liberties Union）等の人権NGO団体が、修正第4条違反である等と主張してその差止を求めて提訴した。連邦地区裁判所が訴えを却下したため、原告は控訴し、第二巡回控訴裁判所は、2015年5月7日判決を下した。

第二巡回控訴裁判所は、憲法判断は回避したものの、本件のような包括的収集は愛国者法第215条で許された範囲を超える違法収集であるとして、違法を宣言した。即ち、通信事業者に対して米国内で発受信された電話通話全ての記録を、毎日継続して且つ将来に亘って提供を求めるのは、収集している情報の量が余りにも膨大であり且つ無限定である[162]。立法趣旨は、資金洗浄や薬物取引などの犯罪対策と同様の手段をテロ対策にも認めるというものであり、本件のような包括的情報収集は立法趣旨を超えている[163]。法は「ある認可された調査に関連する」情報の提供を規定しているが、本件情報収集は、関連する調査が全く特定されておらず、テロ対策一般のためのデータベース構築が目的であるとして[164]、違法を宣言した。

但し、原告の差止要求に対しては、連邦議会で愛国者法第215条改正案が審議中であるので、その成行を斟酌する必要があるとして、差止命令を出さずに、審理を地区裁判所に差し戻した[165]。

本判決は、包括的収集を違法とした論理は極めて妥当な判決であるが、判決時期や差止を認めなかった点など、政治情勢に対する配慮が色濃く伺われるものである。

（4）愛国者法215条の改正（2015年6月）[166]

愛国者法215条は2015年5月末までの時限法であったが、2015年6月2日米国自由法が制定されて、有効期間が延長されると共に、その内容が改正された。

本改正により、監視法第501条（愛国者法215条）に通話記録（call detail records）

---

[161] 愛国者法215条による電話メタデータ収集で、実際に米国関連通話のどれだけを収集していたかは、明確ではない。下記の記事によれば、2006年当時は米国通話のほぼ100%のメタデータを収集できていたが、2013年夏の時点では30%以下に落ちており、政府はその回復に努めていたという。収集比率の低下の理由は明確ではないが、インターネット回線利用通話の増加、データ処理等収集技術の問題、スノーデン告発による担当者の多忙などが考えられるとしている。--Ellen Nakashima, "NSA is collecting less than 30 percent of U.S. call data, officials say," *The Washington Post*, 8 February 2014, accessed 10 February 2014, http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html.

[162] ACLU v. Clapper, No 14-42 (2nd Cir. 2015) at 60-64.

[163] Id. at 65.

[164] Id. at 66-68.

[165] Id. at 93-97.

[166] USA Freedom Act（Summary and Text）, accessed 3　June 2015, https://www.congress.gov/bill/113th-congress/house-bill/3361

についての項目が新設され、FBI が米国で電話メタデータを包括的に収集することは禁止された（米国自由法 103 条）。これに代えて、FBI 長官はテロ対策においては対象者を特定して、監視裁判所の命令を得て、この者と二つ先の連絡者（連絡先の更に連絡先まで）の間の電話メタデータを取得できることとされた。命令は 1 回最長 180 日間有効（延長可能）であり、この間通信事業者は命令に係る電話メタデータを毎日提供する義務を負う（米国自由法 101 条）。対象となる電話メタデータには、通話当事者の電話番号、携帯端末識別番号、利用者識別番号、通話日・時刻、通話時間、テレホンカード番号が含まれるが、携帯端末位置データは含まれない。なお、緊急時には、司法長官は裁判所の命令を得るまで 7 日間に限り業務記録の提供を要求することもできることとされた（同法 102 条）。これらの改正規定は制定 180 日後に施行された。

本改正案は、米国のインテリジュンス機関も関与して作成されものであり、米国インテリジュンス機関のデータ収集能力に大きな変更をもたらすものではないと見られる。実際、元 NSA 長官のマイケル・ヘイデンは、本改革について、2015 年 6 月公開の会合で、愛国者法 215 条による収集は小さなもの（that little 215 program）で、この改革は問題ない（Cool!）と述べている[167]・[168]。

4　インターネット・メタデータと対外諜報監視法第 402 条の問題

電話メタデータと異なり注目を集めていないが、インターネット・メタデータ収集の問題もある。米国政府は、電話メタデータと同様に、米国関連のインターネット・メタデータも収集してきたのである。

インターネット・メタデータは、当初は電話メタデータと同様に大統領の秘密指示に基づき通信事業者の任意の協力を得て行われていたが、政権内でもその正当性に疑問が呈されたため、2004 年 7 月からは対外諜報監視法 402 条（いわゆる PR/TT 命令）の規定に基づき収集していた[169]。しかし、これは 2011 年 12 月に停止された。その理

---

[167] Michael Hayden, “Former NSA Chief Michael Hayden on Edward Snowden’s leaking of classified information,” *WST Video News*, June 2015, accessed 19 June 2015, https://screen.yahoo.com/former-nsa-head-hayden-snowdens-020710743.html

[168] 「問題ない」と言える一つの要因は、対象通話のメタデータ収集率は、旧制度では諸々の要因のため 2013 年時点では 20～30％まで低下していた。これに対して、新制度では裁判所の令状が必要など手続要件は加重されているものの、対象通話は 100％収集可能となり、新制度の方が効果的となる可能性が指摘されている。
--Ellen Nakashima, “The head of the NSA just undercut Rubio’s claims last night at the debate,” *The Washington Post*, 16 December 2015, accessed 25 December 2015, https://www.washingtonpost.com/world/national-security/rubio-goes-on-attack-over-nsa-surveillance-at-gop-debate/2015/12/16/60255890-a3fc-11e5-b53d-972e2751f433_story.html

[169] Spencer Ackerman, “Fisa court order that allowed NSA surveillance is revealed for first time,” *The Guardian,* 19 November 2013, accessed 29 September 2016, https://www.theguardian.com/world/2013/nov/19/court-order-that-allowed-nsa-surveillance-i

由は、継続するだけの価値がないということである。

インターネット・メタデータ分析自体の価値は、NSA がそのための特別のデータベースを構築して取り組んでおり、疑いがない。従って、この停止は、米国関連のインターネット・メタデータ収集自体を停止したのではなく、他の方法による収集と対比して、相対的な価値が低下したため停止したということである。事実、情報公開された NSA 内部資料[170]によれば、当該データは、大統領命令 12333 号及び対外諜報監視法 702 条による収集（通信基幹回線からの収集等）によって代替されていることが伺える[171]。

---

s-revealed-for-first-time

[170] NSA, Inspector General Report, "Report on the Special Study of NSA's Purge of Pen Register and Trap and Trace Bulk Metadata," date-deleted (circa 2012), accessed 25 November 2015,
https://assets.documentcloud.org/documents/2511338/savage-nyt-foia-nsa-release-11-10-2015.pdf
--Office of DNI, "Newly Declassified Documents Regarding the Now-Discontinued NSA Bulk Electronic Communications Metadata Pursuant to Section 402 of the Foreign Intelligence Surveillance Act," 11 August 2014, accessed 6 September 2014,
http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1099-newly-declassified-documents-regarding-the-now-discontinued-nsa-bulk-electronic-communications-metadata-pursuant-to-section-401-of-the-foreign-intelligence-surveillance-act

[171] Charlie Savage, "File Says N.S.A. Found Way to Replace Email Program," *The New York Times,* 19 November 2015, accessed 24 November 2015,
http://www.nytimes.com/2015/11/20/us/politics/records-show-email-analysis-continued-after-nsa-program-ended.html?_r=1

X　まとめ

米国における行政傍受に関する法体系と解釈運用の実態について、行政傍受の出発点である20世紀前期と中期に遡って概観した上で、現状について、特に憲法第2章第1条、同修正第4条と対外諜報監視法の関係等について詳細に分析してきた。そこで、本稿を振り返って、法体系と解釈運用の特徴をまとめると、次の通りである。

1　20世紀中期までの法体系と解釈運用の特徴

20世紀中期までの行政傍受の法体系と運用の特徴を、要約すると次の通りである。

(1) 当初、行政傍受は、完全に秘匿されて行われ、一般国民の知るところとならず、出発点においては合憲性や合法性は余り意識されなかったが、やがて、民間通信事業者の協力確保の観点などから、合法性が意識されることとなった（Ⅳ1・2)。

(2) 米国内における行政傍受では、通信事業者からの任意の協力を得て行われたが、任意の協力は一時中断するなど紆余曲折を経ながらも21世紀まで継続している。主要なものは次の通り。第1次世界大戦後の「ブラック・チェンバー」、第2次世界大戦後の「シャムロック」計画（1975年まで)、1980年代からの「通過通信収集」（現在も継続中)、9.11事件以後の「ステラーウィンド」計画（2007年まで）である（Ⅲ１、Ⅴ)。

(3) 通信事業者の協力に影響を与える法制では、1927年無線法や1934年通信法が、「通信事業者は、権限ある当局からの要求がある場合を除いて、通信内容を漏洩してはならない」旨を定めている。そこで、「権限ある当局からの要求」が何であるのかの解釈について、紆余曲折があったが、国家安全保障庁については、その設立を指示した1952年10月のトルーマン大統領の秘密覚書によって、「権限ある当局」（＝大統領）の意思が明確にされたと解釈されていた（Ⅳ2・3・4)。

(4) 行政傍受を行うコミント活動については当初は全く法律上の根拠規定が存在せず、合法性や正当性は不安定であったが、スパイ防止法の1933年及び1950年改正によって、コミント情報漏洩罪とも呼べる規定が制定され、コミント活動の存在が連邦議会によって包括的に承認されたと解釈された。更に、刑法の1968年改正では、「合衆国の安全保障に不可欠な対外諜報を得るために、大統領が必要と考える措置を採ることができる大統領の憲法上の権限を制約するものではない」（いわゆるnational security exemption）と規定され、コミント活動の正当性が連邦議会による憲法解釈上も完全に認められたと解釈された（但し、本規定は1978年対外諜報監視法制定時に削除されている）（Ⅳ2・3・4)。

２　現在の法体系と解釈運用の特徴

現在、即ち、1967 年カッツ判決と 1972 年ケイス判決を受け、更に 1978 年対外諜報監視法制定後に発展形成された行政傍受の法体系と解釈運用法制の特徴を、要約すると次の通りである。

(1) 米国の行政傍受は、大統領命令第 12333 号「合衆国諜報活動」に基づく行政命令の体系と対外諜報監視法に基づく体系の二重構造となっている。

(2) 大統領は、憲法第２章第１条の規定により「合衆国憲法を保持し、保護し、擁護する」、即ち国家安全保障の任務を課されており、この任務を実施するための諜報活動は議会の制定する法律の根拠を必要とせずに国内外において行うことができる。この憲法上の権限に基づき大統領命令第 12333 号が制定され、行政傍受を含む諜報活動が実施されている（Ⅱ1、Ⅶ2・3)。

(3) 他方、通信内容は個人のプライバシーとして修正第４条の保護対象であり、通信傍受は同条の「捜索押収」に該当する（Ⅶ1)。そこで、対外諜報目的で行う行政傍受は、憲法上の大統領の固有の権限であり、その実施に当たり同条が規定する裁判官の令状（warrant）までは必要としないものの、その実施について行政府に完全な裁量権がある訳ではなく、同条が禁止する不合理な捜索押収であってはならない（Ⅶ3・4)。

そして、対外諜報目的で行う行政傍受が合理的であるか否かは、全ての事情を斟酌して判断する必要があるが、その際、国家安全保障上の利益と米国人のプライバシーの保護という二つの基本的価値を比較衡量する必要がある(Ⅶ3・4)。

(4) 対外諜報監視法は、このような国家安全保障上の利益とプライバシーの保護という二つの基本的価値の比較衡量の上に、連邦議会が憲法上の大統領権限を正しく敷衍した仕組である（Ⅶ3)。

即ち、対外諜報監視法は、米国内における行政傍受の権限を創設した法律ではなく、元来大統領が持っている憲法上の権限を定式化したものであり、仮に、同法が何らかの理由により廃止されることがあった場合でも、行政府において二つの基本的価値を均衡させる合理的な仕組を創ることができるならば、大統領命令による行政傍受が可能であるということになる(Ⅶ3・4)。

(5) 行政傍受情報の捜査利用は許される。行政傍受情報であろうとも、一旦適法に収集され既に政府保有情報となったものについては、その情報内容を検索することは修正第４条が規定する捜索には当たらないと解釈されている。そして、この解釈に従い、大統領命令第 12333 号の下位規程や対外諜報監視法に基づき定められた「最少化手順」では、行政傍受情報の法執行目的での利用配布の手順が規定されている（Ⅷ1)。

(6) 更に、捜査利用目的を持って行政傍受を行うことも許される。即ち、対外諜報監

視法では、対外諜報の収集が監視（行政傍受）の「主たる目的」である必要があったが、2001 年愛国者法による改正により、「重要な目的」で足りることとなった。そこで、監視（行政傍受）の目的が、刑事訴追よりも広く、現在進行中の陰謀の阻止など訴追以外の潜在的対抗手段が含まれている限り、要件を満たすと解釈されるに至った。即ち、国際テロ対策やスパイ対策において、純然たる過去の事件捜査でなく、現在又は将来の脅威が存在しこれを阻止する目的がある限り、捜査利用目的があったとしても、対外諜報監視法による通信傍受が許されるのである（Ⅷ2)。

(7) 通信メタデータについては、修正第 4 条の保護対象ではないとする裁判例は存在するが、保護対象であるとする裁判例は存在せず、通信メタデータは保護対象でないとする政府解釈に基づき各種制度が運用されている（Ⅸ２)。

(8) 米国内電話メタデータの包括的収集の根拠とされた愛国者法第 215 条は、2015 年 6 月に改正され、対外諜報監視裁判所の個別の命令を得て取得する方式に変更されたが、米国諜報コミュニティにとっては大事ではなく支障は生じていない（Ⅸ３)。

(9) 米国内インターネット・メタデータの収集は、2004 年から対外諜報監視法第 402 条に基づき行われていたが、2011 年に中止された。米国諜報コミュニティは代替的な収集手段を有していると考えられる（Ⅸ４)。

３　米国の行政傍受法制の展開で印象深い点。

米国の行政傍受の法体系と解釈運用の実態の分析を通じて、特に印象に残ったのは、次の三点である。

(1) 行政傍受に関する法制度は、連邦議会が制定した法律によって全てが規制されているのではなく、連邦議会に加えて、憲法に基づく国家安全保障上の大統領権限、連邦最高裁判所、対外諜報監視控訴裁判所、対外諜報監視裁判所などの相互作用の中で形成されていること。

(2) 行政傍受に関する法制度は、完成された静的なものではなく、生成発展してきたものであり、且つ現在も生成発展の途上にあること。

(3) 行政傍受に関する法制度の生成発展は、現実の国際情勢、国家安全保障の必要からも大きく影響を受けていることである。

本稿が、米国における行政傍受の法体系と解釈運用の理解に資するところがあれば、幸いである。