論　説

政府による間接的情報収集，特に第三者を通じた情報収集に関する米国法理
――第三者理論（Third Party Doctrine）と電子的監視をめぐって――

中山代志子

はじめに

米国連邦裁判所は，政府による情報収集において，情報主が，意図して対象情報を第三者へ移転することによって，当該情報に対するプライバシーの合理的期待を失うという理論を採ってきたといわれる(1)。この理論が，third party doctrine（以下，「第三者理論」という）である(2)。

米国政府が従来から様々なツールを用いて情報収集活動を展開してきたことはよく知られた事実であろう。とりわけ昨今のデジタル技術の発達を背景としてe-surveillance（電子的監視）実務の拡大は著しい。第三者理論は，従来から学説上の批判が根強かったが，昨今，とりわけ電子的監視との関係で，その妥当性が問われている。

他方，日本においては，同様の理論は存在しない。むしろ，日本のプラ

（1） Orin S. Kerr, *The Case For Third-Party Doctrine*, 107 MICH. L. REV. 561, 563-564 (2009).

（2） *Id.* at 561. 原文は，「the controversial rule that information loses Fourth Amendment protection when it is knowingly revealed to a third party」。

イバシーの理論からすれば，情報が第三者へ移転するとともに元の情報主の権利が及ばなくなるという考え方は奇異に感じられるかもしれない。しかし，日本においても，第三者へ情報が移転すると，当該第三者の任意の協力によって，やすやすと政府による情報収集がなされている可能性がある(3)。その状況は，第三者理論を肯定する米国と同様，あるいはそれ以上に，政府優位の可能性がある。にもかかわらず，第三者理論あるいはこれと類似の議論が不在であるということは，ルールも法整備もなされずに，第三者を経由して政府により情報が収集されていることを意味する。その意味で，米国における第三者理論をめぐる議論ならびに第三者理論を背景とする法制度の問題点を理解することには意義がある。

また，第三者を介する場合でなくても，政府が，情報主本人に内密に情報収集する場合には，第三者を経由する情報収集と共通する問題がある。すなわち，内偵による情報収集や尾行，空からの撮影，その他の「内密の情報収集」には，第三者を経由する情報収集と同様，情報主が異議を唱える機会がなく，集積された情報の利用態様についても知る術がないという共通の問題がある。第三者理論をめぐる議論を批判的に考察することにより，情報主本人に内密に行われる情報収集に共通する問題を解決する視点が得られる可能性がある。

本稿の目的は，このような問題関心に基づき，第三者理論をとるといわれる米国連邦裁判例，これをもとに発展した電子監視に関する米国連邦法制度，ならびに同理論を支持する主張とこれに対する批判を検討し，同理論の現状と課題を理解することにある。第 1 章でまず米国の連邦憲法修正 4 条および第三者理論をめぐる米国法特有の法理論について概観し，第 2 章で 第 1 章で述べた理論の具体化としての電子的監視の法制度を概観する。そして，第 3 章において同理論を支持する論者の根拠とそれに対する反論を検討し，最後に同理論の今後と日本への示唆について考察する。

（3） 田村正博『全訂警察行政法解説』295-296頁（東京法令出版，2011年）参照。

第１章　米国憲法修正４条の役割と「第三者からの情報収集」

米国では，政府の情報収集の必要性と私人のプライバシーの調整において，憲法修正４条が大きな役割を果たしている。本章では，次章で考察する電子的監視法制の基盤として，米国憲法修正４条が果たしてきた役割，中でも第三者に情報が移転した際の考え方を中心に概観し，背後にあるプライバシー観について考察する。

１　米国憲法修正４条の役割

本項では，第三者を通じた情報収集について考察するために前提となる，米国憲法修正４条に関する基本的な判例の流れを確認する。

（１）　米国憲法修正４条の規定内容

米国憲法修正４条は，日本国憲法35条と異なり，必ずしも令状に特化した規定ではない。その第一文は，searches および seizures が reasonable であることを求めているにすぎない(4)。この柔軟性ゆえに，同条は，政府による情報収集活動と私人のプライバシー領域の調整原理として，刑事・行政手続のいずれかを問わず利用されてきた(5)。当然，修正４条は，政府による電子的監視活動と調査対象者私人の自由との間の調整を図る基本条

（４）　緑大輔「無令状捜索押収と適法性判断（１）―憲法35条による権利保障―」修道法学28巻１号146頁（2005年）も，日本国憲法35条と米国憲法修正４条の文言の相違と作用の相違について指摘する。

（５）　修正４条の規律が刑事手続のみではなく行政手続にも適用されることを確立した判例は，Camara v. Municipal Court of the City and County of San Francisco, 387 U.S. 523（1967）ならびに See v. City of Seattle, 387 U.S. 541（1967）であり，その後，行政調査にも修正４条は適用されるという判例法は確立している。判例の流れをまとめたものとして，山本未来「児童虐待防止法９条の３に基づく児童虐待強制立入調査と令状主義―合衆国憲法修正４条の行政調査への適用を手がかりに―」愛知大法学部法経論集183号１頁（2009年）参照。

項としても利用される(6)。

修正 4 条の条文は，極めて単純だが多義的といわれる(7)。この条項が第一文の reasonableness と連動するのか，全く別個と解するべきなのか，についても議論がある(8)。reasonableness は，理論上は令状要件とは別個独立の要件であると考える余地もあり，そのように述べる論者がある(9)一方で，判例においては，令状なく行われた search(es)(10) は，unreasonable との強い推定が働き，逆に令状に基づく search(es) は，reasonable であるとの推定が働くという令状との強い関係を基本としつつ，多くの例外を認めてきた(11)。

第三者を通じた情報収集に関しては，当該情報収集が，search(es) に該当するか否か，が主たる争点として議論されてきた。以下では，search (es) 該当性について判断した主要判例を概観する。

（6） *See* James G. Carr, The Law Of Electronic Surveillance 2-8. 1, 2-9, 2-22, 2-23 (1991) [hereinafter Electronic Surveillance].

（7） Joshua Dressler & Alan C. Michaels, Understanding Criminal Procedure Volume 1: Investigation (Sixth Edition) 49 (2013) [hereinafter Criminal Procedure]. 該当する訳文は，ジョシュア・ドレスラーほか著（指宿信監訳）『アメリカ捜査法』（レクシスネクシス・ジャパン，2014年）71頁。なお同書では「assumption of the risk」を「リスク想定」法理と訳している（111頁等）。assume は「想定する」ことでもあるが，第三者への情報移転によって開示のリスクを負うという文脈からすると，責任や負担を負うという趣旨であると考えるので，この文脈における「assumption of risk」には，「引き受け」「受け入れ」などの語を選択した。

（8） Criminal Procedure, *supra* note 7, at 51-52.

（9） Akhil Reed Amar, *Fourth Amendment First Principles*, 107 Harv. L. Rev. 757, 761-762 (1994).

（10） 米国憲法修正 4 条においていかなる行為が「search（es）」であるかという問題は，まさに同条による保護の範囲を確定する論点であり一義的でない。他方で日本における「捜索」が何を意味するかという問題も，憲法および刑事訴訟法の解釈として議論のあるところである。そこで，以下では米国憲法修正 4 条にいう search（es）を特に意味する場合は，原文のまま引用することとする。なお，単数複数は，文脈により変わりうるので，search（es）と称する。

（11） Criminal Procedure, *supra* note 7, at 162-164.

（2） 修正4条の判断基準に関する主要判例

憲法起草者の考えでは，私有財産とりわけ住居に対する物理的な侵襲あるいは侵入（intrusion，trespass）が不合理に行われないこと，が主要な関心事であった(12)。初期の判例においても，物理的侵襲に対する規律が，関心の中心であった。1928年の Olmstead v. United States（「Olmstead 判決」）(13) においても，物理的侵襲のない単なる電話傍受を，修正4条が適用される search（es）でないとした。また，1942年，Goldman v. United States（「Goldman 事件」）(14) が，壁に取り付けた bugging 装置（電子的盗聴装置）による会話（電話する声）の傍受について，物理的侵襲を伴わないため修正4条に反しないとした。

Olmstead-Goldman 判決により，しばらくの間，修正4条は，物理的侵襲を伴わない盗聴を規律できないでいたが，大きな転換点となったのが，Katz v. United States（「Katz 判決」）(15) であった。連邦最高裁は，物理的侵襲を伴わない，電話ボックスの外側への装置設置であっても修正4条の対象たる search（es）であるとし，電子的通信の監視が修正4条の規制のもとに置かれることとなった。とりわけ，ハーラン判事の同意意見に現れた，「修正4条は場所ではなく人を保護するものであり，プライバシーの合理的期待を保護するものである」との文言が一つの基準となり，以後，プライバシーへの侵襲に対して一般的に修正4条の規律が機能しうると解されることとなる。

（12） Criminal Procedure, *supra* note 7, at 52-54.

（13） 277 U.S. 438（1928）. 禁酒法の時代に組織的に酒類を違法に取引していた被告人らの事務所や住所をつなぐ電話線に傍受線を挿入して会話を傍受し立件した。判決は，修正4条は住居等への立入を保護するが，「住居外にある電話線およびそれにのって送られる通話」は保護の範囲外であるとした。同判決においてブランダイス判事は盗聴を発信者のプライバシー侵害であるとしたが，少数意見にとどまった。山中俊夫「「オルムステッド対合衆国」事件：アメリカ刑事法判例訳選 1」同志社法學 17巻（3）139-153頁，146頁（1965年）。

（14） 316 U.S. 129（1942）.

（15） 389 U.S. 347（1967）.

この基準は，（情報収集対象者に）①主観的にプライバシーの期待があること，とともに②社会通念上，保護に値するプライバシーへの期待があること，という 2 つの要素から成る(16)。多くの場合，主観的な期待が，客観的にも保護に値するプライバシーへの期待といえるか，という点が争点となる(17)。

ところで，Katz 判決は，自らの意思によりアクセス可能な状態に置かれた情報についてはプライバシーの期待がないことを説いたことによっても，後の判例にしばしば引用される。その意味で，第三者理論の基礎を築くことにもなった(18)。

その後，第三者理論の内容をはっきりと示したとされているのが，United States v. Miller(19)（以下「Miller 判決」という）と Smith v. Maryland(20)（以下「Smith 判決」という）である。

Miller 判決では，密造酒製造について起訴された被告人が，捜査当局が文書提出命令に基づき銀行から入手した銀行取引記録の証拠排除を申立てた(21)。最高裁は，高裁判決を覆してその申立てを却下した。その理由として，「口座保有者は，本人の情報を第三者に開示することにより，当該情報が当該第三者から政府に提供されるリスクを受け入れた」とし(22)，

(16)　Criminal Procedure, *supra* note 7, at 79.

(17)　*Id*. at 79 [3].

(18)　たとえば Miller 判決（425 U.S. 435, at 442）は，Katz 判決が「自らの意思で公にした情報は修正 4 条の保護を受けない」と述べた点を指摘し，当該情報がプライバシーの正当な期待を認めうるものか否かを検討する。

(19)　425 U.S. 435 (1976).

(20)　442 U.S. 735 (1979).

(21)　違法品搬送に使用されたトラック，ラジオ装置，金属板等の購入に関する金融取引記録として，Miller 名義の預金口座，小切手，貸付その他一切の銀行記録が入手された。被告人は，地方裁判所の職員が白紙で発行し地方検事が完成した subpoena（文書提出命令）に瑕疵があることなども主張したが，最高裁判所は本文記載の理由により，対象文書が修正 4 条の保護を受けないとの理由で証拠排除不要と判断し，文書提出命令の瑕疵については判断しなかった。

(22)　判決は，後述の United States v. White, 401 U.S. 745, 751–752 (1971) を引用する。

それは「当該情報が，限定された目的にのみ利用され，信頼は裏切られないという前提のもとで提供された場合でも同様である」と述べた(23)。

Smith 判決の事案は，強盗被害者の女性が，犯人とされる男から脅迫電話を受け，目撃情報等から被告人が怪しいという状況の中で，捜査当局は令状を取得せず電話会社の協力のもとに pen-register（通話先探知機）を設置し，被告人の家からの通話記録を調べたところ，被害女性に対する架電を確認し，その他の資料と併せて被告人の家屋の捜索令状を取得する資料とした，という事件である。法廷意見は，自宅から架電したという点で私的な性格は認められるとしても，犯人とされる男は，架電先番号情報を自発的に電話会社に提供しており，電話会社から正当な理由で政府に提供されるリスクを引き受けている，したがってプライバシーの合理的期待を主張できない，とした(24)。

2　間接的情報収集に関する判例法理

次に，第三者からの情報収集ではないが，直接本人に接触することなく間接的・遠隔的に情報を収集する手段に関する判例を概観し，その法理を整理する。

---

(23)　425 U.S. 435, at 443.　被告人は，銀行秘密保持法（Bank Secrecy Act）による守秘義務により，subpoena（文書提出命令）が，口座保有者の私的な文書を捜索し差押えるのと同様の機能を果たしている，と主張したが，受け入れられなかった。なお，ブレナン判事とマーシャル判事の反対意見がある。ブレナン判事は銀行が被告人に知らせず当局に協力したことを重視して高裁判決を支持し，マーシャル判事は，銀行秘密法が令状なく顧客の情報を保存することを義務付けていること自体が顧客の修正 4 条の権利を侵害して違憲であり，違憲な法に基づき保存された文書に依拠することはできない，とした。

(24)　判決は Miller 判決をも引用している（at 744）。本判決に対してはスチュワート判事とマーシャル判事の反対意見が付されている。スチュワート判事は，電話番号は通話内容と同様に憲法上の保護の下にある，とした。マーシャル判事は，電話の重要性に鑑みると，その監視は十分に侵害的であるとした。

（1） 間接的な監視活動に関する主要な判例法理

(a) オープンフィールド

修正 4 条が保護を与えるのは「家屋」とその周辺にある宅地までであり，その外側にはプライバシーの合理的期待がなく，同所での捜索は，search(es) ではないとされる理論がある。これをオープンフィールドの法理といい，Oliver v. United States(25) により確認された。また，United States v. Dunn(26) によれば，①家に対するその土地の近接性，②柵に囲まれているか，③土地の用途，④観察を阻止するために講じられた手段により判定される(27)。

発展型として空からの監視がある。最高裁は，California v. Ciraolo(28) において，人間の知覚能力を増幅せずに行う飛行機での監視について，公的航路に飛行機が通ることは日常茶飯事であるから，上空の飛行機から裏庭の麻薬栽培を目撃した行為を search(es) でないとした。また，Dow Chermical Co. v. United States(29) では，環境基準違反の監視のための上空からの工場撮影について，内側を透視したり会話を聴いたわけではないから search(es) ではない，とした。さらに Florida v. Riley(30) は，立入禁止の温室に対する，低空でのヘリコプターによる監視を search(es) ではないとした。

---

(25) 466 U.S. 170 (1984).

(26) 480 U.S. 294 (1987).

(27) Criminal Procedure, *supra* note 7, at 86.

(28) 476 U.S. 207 (1986).

(29) 476 U.S. 227 (1986). 曽和俊文・アメリカ法1988巻 1 号156頁（1988年）参照。

(30) 488 U.S. 445 (1989). 上空から監視されたモービルハウスと温室には周囲に鉄線が張られ，「立入禁止」の標識が掲げてあったが，法廷意見は，誰もがヘリコプターで400フィートの高度から温室を観察できたこと，敷地内の私的な事柄（intimate details）を観察したわけではないこと，騒音・粉塵等により温室の使用が妨げられなかったことなどを挙げて，Riley には合理的なプライバシーの期待がないとした。

(b)　スパイ，協力者

第三者経由の情報収集の一類型といってもよいのがスパイ，あるいは協力者（偽装友人）による情報収集である。Katz 判決以前の判決として Hoffa v. United States（「Hoffa 判決」）(31)，Katz 判決以後の判決として，United States v. White（「White 判決」）(32) がある。

Hoffa 判決では，話をした相手が自分を裏切るリスクは人間社会の本来的な条件であり，話をした以上，そのようなリスクを引き受けている，とされた。White 判決では，情報提供者との会話を電子機器により盗聴したことが問題とされたが，電子的録音機器等で会話を捜査員に送信していたとしても，Hoffa 事件と同様であるとした。ハーラン判事とダグラス判事は，これに対して反対意見を唱えており，マーシャル判事が反対意見に同調している。反対意見は，第三者による監視がプライバシーの利益に及ぼす影響を重視し，情報機器を利用した電子的監視の問題性を強調し，単なる協力者の利用にとどまらず情報機器を利用する場合には，令状による抑制が必要だとしている(33)。

(c)　尾行，ゴミ漁り

家の宅地外に廃棄したゴミについて，連邦最高裁は，California v. Greenwood(34) において，Smith 判決を引用して，ゴミが警察や公衆により開封されないという主観的期待があるものの，自発的に他人のアクセス可能な状態においたことから，プライバシーの合理的な期待がなくなる，とした(35)。

(31)　385 U.S. 293, 414 [4] (1967). 捜査対象者は，ホテルのスイートルームで政府への情報提供者であることを知らずに会話した。

(32)　401 U.S. 745 (1971).

(33)　401 U.S. 745, 756, 771-772.

(34)　486 U.S. 35 (1988).

(35)　Criminal Procedure, *supra* note 7, at 92 は，反対意見を支持し，ごみを漁られるかもしれないという単なる可能性をもって憲法上のプライバシーの合理的期

また，尾行については，United States v. Knotts(36)（以下「Knotts 判決」）が，路上でビーパーの助けを借りて容疑者を尾行した行為につき，Smith 判決などを引用し，公道を走行する車は，自分の位置情報を他人に晒しているのであり，公的場所から目視で入手できる情報を入手しても，search (es) に当たらないとし，ビーパーによる監視であっても同様であるとした(37)（ビーパー使用に関する問題点については次項参照）。

(d)　コンピュータ上の情報

一般に，コンピュータの中に格納されているファイルのプライバシーには，容器の中の貨物と同様に，情報主のプライバシーの合理的期待が及んでいると解されている(38)が，自ら晒した情報についてはプライバシーの合理的期待を失う。下級審であるが，例えばエイジェントが肩越しにスクリーン上のパスワードを覗き見た場合(39)や，システム管理者が監視していることを承知で利用しているコンピュータ上の情報(40)や，公的に共有

待を失うのであれば，強盗の可能性があるからといって家の中のプライバシー期待を否定するのだろうか，と疑問を呈している。

(36)　460 U.S. 276 (1983). 麻薬製造に使う薬品を購入する会社の承諾を得て，怪しい容器にビーパーを設置し，容器の移動を追跡した。

(37)　460 U.S. 276, at 282–283.

(38)　Office of Legal Education Executive Office for United States Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* [hereinafter *DOJ Manual*] at 3–4, http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf;（文字化けする場合は，Department of Justice, Computer Crime & Intellectual Property Section のサイト http://www.justice.gov/criminal/cybercrime/ から入り，Documents and Reports から選択，文字コードを Unicode（UTF-8）に変換する。）. 同資料は米司法省が，連邦検事の研修および実務のために作成したもので，Orin S. Kerr が主著者であった2001年版を改訂したものである（同資料「前書き」）。司法省の立場を代弁するものではない，との断りはあるものの，一定の立場のための資料であることを念頭に置かなければならない。とはいえ，電子的に記録された情報の政府による収集に関する網羅的な情報源として有用である。本稿では，とりわけ電子的記録に関する情報収集における米政府の立場を理解するために，適宜引用する。

(39)　United States v. David, 756 F. Supp. 1385, at 1390 (D. Nev. 1991).

された図書館のコンピュータに保存された文書(41)や，盗難や詐欺に遭って第三者に渡ったコンピュータの内容物(42)については，プライバシーの合理的期待は認められないとする判決がある(43)。

（2） 特殊技術の利用

技術の進歩によって，今まで不可能だった情報収集が可能となる。間接的な情報収集手法を活用するにあたっても，技術の進歩によって，プライバシーの合理的期待に変化を認めるべきか否か。この問題については，電話ボックスの外側への装置設置に関する Katz 判決の前から，「公衆に一般に利用可能な」技術であるか否かによって結論を異にする可能性が示唆されてきた(44)。

Smith 判決では，電話会社が電話番号を記録する pen-register（通話先探知機）を設置・使用することを search(es) ではないとし，前述 Knotts 判決では，化学薬品のドラム缶へのビーパーの設置利用を search(es) ではないとした。しかし，United States v. Karo（「Karo 判決」）(45)では，公的

---

(40)　United States v. Gorshkov, 2001 WL 1024026.

(41)　Wilson v. Moreau, 440 F. Supp. 2d 81, 104 (F.R.I. 2006).

(42)　United Sates v. Caymen, 404 F. 3d 1196, 1200 (9th Cir. 2005); United States v. Lyons, 992 F. 2d 1029, 1031-32 (10th Cir. 1993).

(43)　See *DOJ Manual*, *supra* note 38 at 5-6.

(44)　Criminal Procedure, *supra* note 7, 94-95. United States v. Lee, 274 U.S. 559 (1927) において，懐中電灯や探照灯の使用は search(es) に当たらないとし，On Lee v. United States, 343 U.S. 747 (1952) では，適法な眺望点からの目撃は，拡大用機器を利用しても search(es) でないと述べた。また，前述の Dow Chemical Co. v. United States, 476 U.S. 227 (1986) では，航空機からの写真撮影について，精密ではあるが「地図製作に普通に使われる」簡便な市販カメラを使用した監視を search(es) でないとした。

(45)　468 U.S. 705 (1984). 結論として証拠排除を認めた高裁判決を覆したが，その理由は，ビーパー利用に関係なく収集された証拠が家宅捜索令状発付に十分であったからだった。本件では，所有者の同意のもとにビーパーを装着した容器を追跡して隠れ家を特定し，令状をもって家宅捜索した。傍論であるが，ビーパーの装着は search ないし seizure には当たらないが，家の中に容器が搬入さ

場所ではなく家の中の薬品容器の移動を監視するために利用されたビーパーは，修正 4 条に服するとの立場が示された。

また，Kyllo v. United States（「Kyllo 判決」）(46) は，熱画像探知機の利用について，search（es）に該当するとした。多数意見は，家の中という領域の保護を優先し，外部への熱発散の感知のみであっても，プライバシーに対する侵襲とみなした。

家の中と外でのプライバシーの期待に対する姿勢の違いが，やや変化したと見られるのが，United States v. Jones(47)（以下「Jones 判決」）である。FBI が，麻薬密売の嫌疑ある被告人（Jones）らの車両に GPS 装置を取り付けて追跡調査を行い，それにより入手した隠れ家の情報をもとに家宅捜索令状を得て証拠を収集したという事件である。FBI は，GPS 装置による監視について，10日以内に監視活動を行うことを認める令状を得ていた。しかし捜査官は，令状発付の11日後に，令状により指定された地域外に停車中の車両（Jones の妻名義であるが Jones が使用していた）に装置を装着し，その後28日間にわたり監視したことから，令状なく GPS 追跡調査を行うことの合憲性が問題となった(48)。

同判決法廷意見は，車両は修正 4 条の対象たる「effect（物）」に相違な

れ，ビーパーが家屋内の情報収集に利用された点は修正 4 条の違反であると指摘された。

(46)　533 U.S. 27 (2001). 家の中でマリファナ栽培のために放熱していることを，壁の外に設置した熱探知機によって確認し，その情報をもとに家宅捜索の令状を取得した。裁判所は，通常一般人が入手できない機器を利用して，本来私的な家の中の様子を探ることは search（es）であり，令状がなければ不合理と推定される，とした。

(47)　132 S. Ct. 945 (2012).

(48)　地方裁判所は，公道上の移動情報についてはプライバシーの合理的期待は存在しないとして Knotts 判決等を引用し，証拠排除の申立てを一部しか認めなかった（451 F. Supp. 2d 71, 88 (2006)）。共犯者 Maynard とともに上訴したところ，高裁判決は，令状なく GPS 装置を装着する証拠収集は修正 4 条に抵触するとした（U.S. v. Maynard, 615 F. 3d 544 (C.A.D.C. 2010)）。本最高裁判決は，政府の申立によりサーシオレイライを認めた判断である。

く，これにGPS装置を取り付けその動きを監視することはsearchである，とし，18世紀のEntick v. Carrington(49)を引用して「政府が，私人の財物を，情報収集のために物理的に占有した」ことを重視した。そして，Katz判決において示された，「プライバシーの合理的期待」基準は，コモンローに由来するtrespass基準に付加されたものであり(50)，それだけを適用しなければならないという排他的なものではなく，本件のように，外界に自ら晒した情報の視覚的な収集について修正4条のsearchではないという結論と整合的に解釈するべき場合には，ビーパーの装着による財産への侵襲というtrespassに着目するべきである（将来的に，trespassに関係なく，監視活動を修正4条違反とする必要を生じる場合があるかもしれないことを示唆しつつ，本件においてそのような問いに答える必要はない），という(51)。

このように，法廷意見は伝統的なtrespass理論に依拠しているが，従前の理屈では「公に晒されている」情報の取得に過ぎない類型である，公道上での車両の移動状況の監視について，修正4条のsearch(es)に当たるとしたことは，やはり注目すべきであろう(52)。本判決についてはさらに後述するが，モザイク理論(53)を容認し，修正4条の適用範囲を広げた，

---

(49)　95 Eng. Rep. 807 (C. P. 1765).

(50)　132 S. Ct. 945, 953.

(51)　132 S. Ct. 945, 953–954. 判決はまた，政府の主張に応える形で，Knotts判決，Karo判決との関係について述べている。すなわち，Knotts事件は，Katzの「プライバシーの合理的期待」基準に関する判示をしているところ，ビーパーは被告人が保有する以前に，容器のその当時の所有者の同意のもとに装着され，被告人も装着を争わず，裁判所も修正4条について判断しなかったので，trespass理論には触れる必要もなく，それゆえ触れていないだけであるとした。また，Karo事件についても，ビーパー装着においてtrespassは生じていなかったケースであることを指摘している。

(52)　本判決の同意意見はスカリア判事が執筆しているが，ソトマイヤー判事，アリート判事の同意意見があり，両判事はtrespass理論に依拠する法廷意見に批判的見解を披瀝している。ギンズバーク，ブライヤー，ケイガン判事がアリート意見に同調した。

との見方もある(54)ように，プライバシー侵害の捉え方について，変化の兆しを示している。

もっとも，訓練された麻薬捜査犬による探索に関する2013年の判決において(55)，最高裁は，家の敷地への犬の侵入を捉えて令状を取得するべきであるとしており，ここでも物理的侵入（trespass）ならびに家の中のプライバシーの期待を重視する傾向は維持されている。

（3） まとめ

これらの判決からは，間接的な監視活動の合憲性が，憲法修正 4 条の search(es) 該当性として議論されてきたこと，連邦最高裁は，家の中に存在する情報については手厚い保護を認める一方，プライバシーの主体が自ら第三者からアクセス可能な状態に置いた情報について，客観的に保護すべきプライバシーの期待を否定する傾向があること，技術の進化に関しては，通常人も利用可能な技術か否かを判断基準とすることがわかった。そして最近，修正 4 条の保護範囲について，Katz 判決が示したプライバシーの合理的期待という判断基準と，伝統的な trespass 理論に基づく基準との関係を整理し，将来，trespass 理論を介することなく監視によるプライバシー侵害そのものに焦点を当てる可能性を示唆する判決が現れた（Jones 判決）。

次に，第三者からの情報収集に特化して，連邦裁判所の理論を概観する。

（53） もともと情報公開請求事件において，個人の特定が直ちにできない情報であっても，その組合せによって個人情報が特定できる場合には，個人情報として開示を拒否すべきという理論として定着している。

（54） Christopher Slobogin, *Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 Duke J. Const. L. & Pub. Pl'y 1, 3–4 (2012).

（55） See Florida v. Jardines, 133 S. Ct. 1409 (2013).

3　電子的監視に関連する第三者からの情報収集に関する理論の展開

前項では間接的情報収集手段に関する判例法理を概観し，整理した。本項では，間接的情報収集のなかでも，第三者からの情報収集に焦点を絞り，電子的監視に関連する事例にも着目して，判例理論を検討する。

（1）　プライバシーへの期待の消滅時点

電子的に保存された情報についても，政府の search（es）の対象者の「プライバシーの合理的期待は，その情報へのコントロールを失い，第三者へ渡したとき，失われる可能性がある」というのが DOJ Manual の見解である(56)。壊れたコンピュータを修理に出す，とか，情報そのものをだれかに送信する場合，第三者に保管を依頼するなどの場合に，その情報へのコントロールを失うことになるとされる(57)。

しかし例えば，A が B という配送者を利用して C に何かを送ることを想定した場合に，情報が B のもとにあるときには，その内容は一般的に修正 4 条の保護下にあり，政府がその内容を検査するためには令状を要する，と説明される(58)。

一方，下級審判決であるが United States v. Young（「Young 事件」）(59) で

（56）　*DOJ Manual*, *supra* note 38 at 8.

（57）　*Id.*

（58）　*DOJ Manual*, *supra* note 38 6–7。同書で引用する United States v. Villarreal, 963 F. 2d 770, 774（5th Cir. 1992）では，リン酸のドラムを輸送中の運送人が，内容が軽く，音もしないことから不審に思い，関税吏を呼んだところ，官吏が，開封しマリファナが出てきたという件で，運送業者に預けた者には内容物に対するプライバシーの期待があるとして，修正 4 条違反とされ証拠排除された。

（59）　*DOJ Manual*, *supra* note 38 at 6 note 2; 350 F3d 1302, 1308–09（11th Cir. 2003）は，被疑者が虚偽の申告によりガソリンの税金を免れ，多額の現金を Fedex を利用して送金しようとしたところを，Fedex の協力を得て無令状で嫌疑ある荷物を X 線透視し，現金を発見したという事件であった。Fedex は，明示的に現金の送付を禁止しており，業者の一存で荷物を開封して調査することがある旨告知していたという事情のもとで，裁判所は，荷送人は，荷物のプライバ

は，宅配業者が明示的に開披可能性を告知していたことにより，原情報主のプライバシーの期待が消滅したという判断が示された。興味深いのは，Young 事件判決において，宅配業者が顧客に告知していた内容は，「現金封入禁止」という条項と，違反がないかどうかを確認するための業者による開披の可能性であったのに対し，調査は，税務当局と入国管理局による，税法違反事件の証拠集めと麻薬取引疑惑の裏付け資料集めであった。すなわち，荷物の内容物についてプライバシーを有している者が，もしも宅配業者の告知によって開披に同意し，あるいは告知された限りにおいてプライバシーを放棄したと構成するならば，告知内容とある程度一致した開披目的でなければならないはずであるが，そうではなく，およそ開披に同意したと擬制した上で，あらゆる目的において，かつ，宅配業者だけでなく当局が調査目的で開披することも可能となるのである。客観的なプライバシー期待とは，このように，プライバシー保有者の主観から切り離されている。

プライバシーの期待は，ひとたび対象物が，想定された送付先へ到着したとき，消滅する(60)。情報が，想定された送付先である第三者に到達した後，当該第三者が任意に政府に開示する際には，情報主のプライバシーの期待は保護されない。

このルールは，情報が電子的に送付される場合でも同様に妥当する(61)。

シーへの期待を失ったとして，無令状の調査を合憲と判断した。

(60)　下級審判決だが United States v. King, 55 F. 3d 1193, 1196 (6th Cir. 1995)。同事件では，詐欺事件の主犯 King が共犯である妻に宛てた書簡を，別の共犯（妻から捨てるよう依頼されて入手した者）が自ら FBI に提供した。この場合には，かかる書簡の証拠能力は否定されず，King が自ら宛てた書簡の「受取人（妻）による受け取りとともに，King の当該書簡に対するプライバシーへの期待は終了する」ため，King には修正 4 条違反を主張する適格がない，とした。

(61)　下級審だが United States v. Horowitz, 806 F. 2d 1222 (4th Cir. 1986). 被告は価格情報を競業者に対してメールで送信したが，裁判所は，その送信により，情報への支配権を移転したとみなした。

インターネット・サービス・プロバイダー（以下「ISP」という）が保有するアカウント情報に関して，後述の Stored Communications Act により令状よりも軽い手続きでの入手が可能とされているのも，メールの送受信者記録や，ISP に提供されたウェブサイト・アドレスのインターネットプロトコルを取得するために pen-register を利用することについて修正 4 条の保護範囲外であるとされることも，ISP の顧客は，プロバイダーの事業情報として保有されたアカウント情報に対してプライバシーの合理的期待を有しないことと整合する(62)。

（2） 保管中の物へのプライバシー期待

第三者理論には例外がある。それは，当該物に対する支配を失っていない場合（暫時預かってもらったような場合）であり，この場合には，当該物及び内容に対するプライバシーの期待は保護される(63)。送り主が保有するプライバシーへの期待は，第三者に保有されている物への支配権が縮小するとともに消滅する。例えば，ロッカーに保管していたコンピュータに対する支配権は，ロッカーの料金を未払いにした結果，コンピュータへのアクセス権が消滅し，あるいはホテルの部屋のプライバシーへの期待は，ホテルの賃借期間経過とともに失われる(64)。

（3） 私人による捜索

当局の指示でその代理として行うのでない限り，私人による捜索には，

---

(62)　*DOJ Manual*, *supra* note 38 at 9; United States v. Perrine, 518 F. 3d 1196, 1204 (10th Cir. 2008).

(63)　下級審だが United States v. James, 353 F. 3d 606, 614 (8th Cir. 2003); United States v. Most, 876 F. 2d 191, 197-98 (D.C. Cir. 1989); United States v. Barry, 853 F. 2d 1479, 1481-83 (8th Cir. 1988); United States v. Presler, 610 F. 2d 1206, 1213-14 (4th Cir. 1979).

(64)　下級審だが United States v. Poulsen, 41 F. 3d 1330 (9th Cir. 1994); United States v. Allen, 106 F. 3d 695, 699 (6th Cir. 1997).

修正 4 条は適用されないとされる(65)。私人が偶々見つけた犯罪の証拠を警察当局に差し出した場合には，私人による発見には修正 4 条の適用はない(66)。私人が政府から依頼を受けて行うのではなく，自発的に行うという点が重要である。限界事例として，下級審判決であるが，ハッカーが児童ポルノを発見し警察に届け出た事件において，このこと自体は修正 4 条の問題にはならないが，警察が匿名ハッカーに対してハッキングを訴追しないことを保証し，さらなる情報提供を依頼し，その 1 年後に，同ハッカーがさらなる児童ポルノの証拠物件を提供したケースにおいて，裁判所は，当初の情報提供が，警察との代理関係に先行していたことから，いまだハッカーが警察の代理として動いていたとまではいえない，としたが，「政府の活動は許容限度ぎりぎりだった」とした(67)。

（4） 同意による捜索との関係

仮に当該調査が search（es）に該当するとしても，相手方の真意による有効な同意があれば，令状を取得せず捜索しても，また相当な理由がなくても，unreasonable とはいえない(68)。

共同で権限を持つ場合などに，第三者の同意を有効な同意といえるか，という議論がなされており，一定の条件のもとに共有者，共同権限保有者らの同意による開示が認められている(69)。United States v. Matlock(70) がリスクの引き受け基準を示しているとされる(71)。

---

(65)　Criminal Procedure, *supra* note 7, at 57; United States v. Jacobsen, 466 U.S. 109, 113 (1984). しかし，私人として行う捜索の範囲を超えてはならない。

(66)　*Id.*

(67)　United States v. Jarrett, 338 F 3d 339 (4th Cir. 2003).

(68)　Criminal Procedure, *supra* note 7, at 247; *DOJ Manual*, *supra* note 38 at 15; Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

(69)　Criminal Procedure, *supra* note 7, at 255–256, *DOJ Manual*, *supra* note 38 at 19–27.

(70)　415 U.S. 164 (1974).

(71)　Criminal Procedure, *supra* note 7. もっとも，同 257–259 によれば，その後，

これは第三者経由の情報収集に限らず，一般的な令状主義の例外であるが，第三者理論の根拠の一つとしても，第三者によりさらに開示されるリスクを引き受けた，あるいは同意した，とみなされるという理屈がある(72)。情報を政府に提供する第三者と，情報の原保有者との間に，一種の共同権限者の関係を想定すれば，同意捜索の議論は，第三者理論にも応用可能と思われる。

（5） 内容物に対するプライバシー期待と外容情報の区別

プライバシーの期待は，物が梱包され第三者に保有されているような場合に，その内容物に対しては一般的に存在し，第三者理論の及ばない領域であるとされる(73)。逆に，梱包の外側情報（例えば宛名）については，プライバシーの期待が低下するとの考え方がある。

Berger v. New York(74) で，無線通信の電子的盗聴が修正 4 条の対象とされたのも，後述の，電信・電話の通信傍受に関して令状を得て行う厳格な手続きを定めた Title III of Omnibus Crime Control and Safe Streets Act of 1968（通称「Title III」）(75) が制定されたのも，通信の「内容」が梱包内容物と同視されているからである。

第三者理論を確立した先例として挙げられる Smith 判決において，問題となったのは，脅迫犯が発信している電話の通話先番号のみという，外容情報(76) であった。同じく第三者理論を示した例として挙げられる Miller

---

Georgia v. Randolph, 547 U.S. 103（2006）を経て，基準は流動的な状況とみられる。

(72)　もっとも，後述するように，そもそも情報主の同意を擬制することが適切かについては，議論がある。

(73)　下級審であるが United States v. Villarreal, 963 F. 2d 770, 774（5th Cir. 1992）

(74)　388 U.S. 41（1967）. 賄賂の謀議が盗聴された。

(75)　18 U.S.C. §§2510-22.

(76)　以下で用いる「内容情報，外容情報」の語については，山本龍彦「アメリカにおける対テロ戦略と情報プライバシー」大沢秀介ほか編『自由と安―各国の理論と実務』（2009年）140頁，145頁にある content information と envelope

判決でも，問題となった情報が，銀行の口座情報であり，銀行が事務情報として保有管理している情報であったことが重視された。

4　背景にあるプライバシー観

上記の第三者理論は，米国のプライバシー観と密接な関係がある。そこで，本項では，米国における「プライバシー」概念の捉え方が日本と異なることが指摘されていることについて述べる。

阪本昌成(77)は，私事の公表による「プライバシー」の侵害と表現の自由の衝突という視点から，日本のプライバシー法制を米国と比較して分析している。同氏の分析によれば，米国は，言論の自由な流通を是とし，パターナリスティックな「プライバシー」保護を拒否する。日本の判例は，人間の尊厳という価値観によって，主観的な「隠しておきたい」という選考を権利化し，容易に表現の自由を縮小させ，準則・基準のない「全面的な個別衡量論につかりきっている」(78)。米国におけるプライバシーの利益保護は，主観的な期待の保護に偏ることなく，他の憲法的価値との調和の中で，経済学的な比較衡量の対象となる客観的な価値として考察される，とされる(79)。

逆に，こうした米国の情報プライバシー論は，ヨーロッパに比べて「遅れている」と評されることもある(80)。

山本龍彦は，米国のプライバシー論が「遅れている」様子を以下のように指摘している。まず Smith 判決に示される米国の情報プライバシー論の特徴として，①コミュニケーションの内容と外容情報の峻別論を挙げ

---

information の訳語を利用した。

(77)　阪本昌成「プライバシーの権利と表現の自由（１）」立教法学76号（2009年）34頁以下。

(78)　阪本昌成「プライバシーの権利と表現の自由（２・完）」立教法学77号（2009年）141頁 , 155頁。

(79)　前掲注77）54-58頁参照。

(80)　山本・前掲注76）141-142頁。

る。また，②自発的に第三者に譲渡するとプライバシーの期待を失うというSmith判決の論理（本稿でいう「第三者理論」）は，情報の管理・取り扱いに関する関心の低さの顕れであると指摘する(81)。そして，このような特徴は，インターネット時代になっても，変わらず出現していると指摘する(82)。

こうした「遅延」の背景として，同氏は，①ナチスの経験を経ていない，②プライバシーを，ある者の隠された世界に対する侵犯と捉える考え方が残っているというSoloveの指摘を援用している(83)。

5　小括

以上のとおり，第三者を通じた政府による情報収集に関する米国連邦裁判所における判例法理は，以下のようなものである。

情報収集の必要性と情報主の権利の調整は，修正4条のsearch(es)に該当するか否かの判断において議論され，プライバシーの期待が保護されているときには，search(es)に該当し，原則として令状を要することとされる（令状を要するとは，犯罪等の情報収集目的となる事象の嫌疑があるという「相当の理由」(probable cause)があることについて裁判所の審査を経て令状を取得することが前提となる)。ここでいうプライバシーの期待とは，主観的な期待とともに客観的な要保護性をいい，要保護性は規範的判断であって，情報主個人の主観からは切り離された利益として，情報主のプライバシー保護の社会的必要性の観点から判断されている。

---

(81)　前掲145頁。同所で引用されているFrancesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. Rev. 609 610-611 (2007)によれば，米国でテロ対策目的で行われているNSA（国家安全保障局）によるデータの収集を，欧州の諜報機関が行う場合には，収集に関して厳しい要件を課されるだけでなく，5年を超えて情報を保存してはならないという（Council Directive 2006/24 arts. 3, 6, 2006 O.J. (L 105) 54 (EC).)。

(82)　前掲147-149頁。

(83)　前掲151頁。

そして，⑴情報が外容情報か内容情報かによりプライバシーの期待の程度が異なり，保護の態様もこれに応じて異なる。外容情報は，情報主が自ら誰からもアクセス可能な状態に置いていることから保護を要しないとみなされるが，内容情報は，家の中のプライバシーと同様の憲法修正 4 条による保護を受ける。

⑵情報主が，自らの意思で，情報の支配権を第三者へ移転することによって，客観的なプライバシーの期待の保護可能性が消滅する。すなわち，当該第三者から情報を収集する際に，政府は修正 4 条に基づく保障を前提とする厳格な要件（相当の理由および令状発付）を遵守する必要がない。

⑶情報が第三者の手元にある場合に，第三者の同意のみによって情報に対するプライバシーの期待は消滅しないが，共同の権限ある第三者の同意であれば，情報主の同意と同視され，相当の理由も，令状も不要となる。

このような判例の状況のうち，同意による情報収集に関して，あくまでも情報の原保有者あるいは情報主を起点として同意権限を考察している点は肯首できるものの，その情報主が，自ら第三者に情報を移転したことを条件として，一気にプライバシーへの期待が消滅するとみなすことには，違和感を感じざるを得ない。Smith 判決にせよ Miller 判決にせよ，特定人に対する相当の嫌疑がすでに存在しており，かつ情報収集方法の物理的侵襲の程度は低かったことを考えると，第三者理論として一般化することなく解決することも可能だったと思われる。外容情報と内容情報の峻別による相違についても，プライバシーへの主観的期待とのずれがあまりにも大きい。

そこで次章では，このような法理論を反映した実際の法制度を検討し，上記の特徴ならびに問題点の，法制度における出現状況を考察する。

第 2 章　電子的監視の法制度

米国では，以上に述べた修正 4 条をめぐる解釈ないし理論を背景にし

て，電子的監視に関する法制度が精緻に整備されている。本章では，第三者理論と関係の深い，電子的監視に関する法制を概観し，同理論との関係における問題点を指摘する。

1　多様な電子的監視活動の類型

電子的監視（electronic surveillance）の方法には様々なものがある。様々な電子監視の手法・用語をまとめると，以下のようになる(84)。

（ⅰ） wiretapping（電信電話傍受）：電信電話通信内容を通信の途中で傍受すること。

（ⅱ） eavesdropping（傍受）：会話等を秘密裏に記録すること。Wiretapping が通信機器ごしの通信内容に関する盗聴であるのに対し，こちらは直接の会話の盗聴である。

（ⅲ） bugging（電子的盗聴）：発言者の近くに機器を設置してその会話を録音したり盗聴したりする方法。

（ⅳ） consent surveillance（一方当事者の同意による監視）：会話の一方当事者が相手に知られないように録音したり，他者に聴かせる方法。

（ⅴ） pen register（通話先探知）：電話線に装置を取り付け，特定の電話から発信された先の番号を読み取ることによって送信先情報を取得する装置(85)。

（ⅵ） trap and trace devices（逆探知）：特定電話が受信した通信の，発信元番号を逆探知する装置(86)。インターネットのヘッダーは to/from 両方の情報を含むので，ヘッダーを読み取る機器は pen/trap device と呼ばれる(87)。

これらのうち，最初の 4 つは内容の傍受にかかるものであるのに対し，後ろの 2 つの目的は，後述のように外容情報の取得にあることから，プラ

(84)　なお，訳語は筆者によるもので，定訳ではない。
(85)　18 U.S.C. §3127 (3).
(86)　18 U.S.C. §3127 (4).
(87)　*DOJ Manual*, *supra* note 38 at 154.

イバシー保護の程度が軽くなっている。

2　法制度の歴史的経緯

盗聴機器の発達とともに米国では古くから盗聴による捜査が自由に行われてきた。前述の Olmstead 判決により盗聴装置による捜査実務が承認されたが，同判決法廷意見は，盗聴による捜査を規律する法制度の創設を示唆しており(88)，これを受けて Federal Communications Act of 1934（1934年連邦通信法）(89) が制定される。当時の同法605条は，「何人も，発信者の同意なくして，いかなる通信も傍受できず，傍受した通信の存在，内容，趣旨，目的，効果または意図を，何人に対しても漏示または公開してはならない」(90) と定めた。

その後，Nardone v. United States（「ナードン事件判決」）(91) を通じて，①連邦通信法605条のいう「何人」とは私人のみではなく，通信傍受の禁止は，連邦捜査機関の傍受にも及んでいる，②違反によって得られた傍受内容は証拠排除されることが示された(92)(93)。こうした連邦通信法605条に対

(88)　277 U.S. 438, 468.

(89)　47 U.S.C. 151-609 (1982).

(90)　Nardone 判決（302 U.S. 379 (1937) at 380-381）に引用されている当時の原文「no person who, as an employe, has to do with the sending or receiving of any interstate communication by wire shall divulge or publish it or its substance to anyone other than the addressee or his authorized representative or to authorized fellow employes, save in response to a subpoena issued by a court of competent jurisdiction or on demand of other lawful authority; and no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect or meaning of such intercepted communication to any person.」による。

(91)　302 U.S. 379 (1937). 同事件で裁判所は，no person あるいは any person とは政府を含むと解し，また傍受した通話内容を証言することも「漏示」に当たるとした。

(92)　Nardone v. United States, 308 U.S. 338 (1939) のいわゆる第二ナードン事件判決では，違法証拠そのものでなく，違法な盗聴により得られた派生証拠の証拠能力を排除した。

する例外として，①通話者の一方の同意があれば傍受可能とされ，しばしば司法取引の結果得られる同意によって傍受がなされた(94)ほか，②電話会社による情報提供(95)，③国家安全保障のための盗聴（裁判所は，大統領が憲法上有する「国家の安全を保持する義務」を果たし「外交権限」を行使する場合は605条の適用を避けた）(96)があった。

その後，前述の Goldman 判決が，電話機に送信される前の会話内容を，連邦通信法605条の対象外であるとした(97)が，連邦通信法による盗聴規制は，司法当局が重大犯罪を捜査するための支障になるばかりで，違反も横行し，実効的な盗聴規制になっていないとの批判が大きく，政府による電子的監視を，適切な規律のもとに適法に可能とするための立法が求められていた。こうした世論ならびに Katz 判決を受けて制定されたのが，Title III(98)である。Title III は，連邦捜査当局が令状を得て国内の有線・口頭・電子的通信の傍受を行うことができる権限を付与し，手続を定めている。同法に基づく傍受は，後述のように，具体的犯罪の嫌疑を示す相当の理由に基づき，必要最小限の方法・期間により，しかも被疑者への通知を要件として行う必要がある(99)。

---

(93)　経緯につき，井上正仁『捜査手段としての通信・会話の傍受』（有斐閣，1997年）7－8頁，岡本篤尚『《9.11》の衝撃とアメリカの「対テロ戦争」法制』（法律文化社，2009年）167頁参照。

(94)　Electronic Surveillance, *supra* note 6 at 1-12によれば，同意の任意性が否定されることはほぼなかったという。

(95)　Electronic Surveillance, *supra* note 6 at 1-13.　電話会社が，税務当局の呼出状，大陪審の subpoena（文書提出命令），FBI エージェントからの要求に従うことはできた。

(96)　Electronic Surveillance, *supra* note 6 at 1-14; United States v. Coplon, 185 F. 2d 629 (2d Cir, 1950) では違法とされたが United States v. Butenko, 494 F. 2d 593, 602 (3d Cir.), cert. denied, 419 U.S. 881 (1974).

(97)　605条が保護しているのは，電信送信されたメッセージそのものであって，内容の秘匿性ではなく，会話内容が隣室で傍受されても，電話機から電話機への送信を傍受したものではないから同条の保護するものではない，という。

(98)　18 U.S.C. §§2510-22 (2014).

(99)　18 U.S.C. §2518.

その後，Title III は Electronic Communications Privacy Act of 1986（ECPA）によって改正され，さらに2001年愛国者法によりテロ対策のための無令状傍受権限が拡大された(100)。

3　犯罪捜査に関する監視

現在，電子的手段による監視法制は，一方では通信・会話等のコミュニケーションをその時点で（同時に）傍受する手法に対する規制を定める法制，他方で電磁的に記録されたデータ情報を取得する手法に対する規制を定める法制に大きく分かれている。そして，そのいずれについても，内容情報の取得と外容情報の取得方法に明確な相違がある。内容情報と外容情報とでは，プライバシーの利益の重要度に差があるとの考えが一般的にあり，同法の起草者はかかる考えに依拠したものと考えられる(101)。具体的には，以下の様に複雑である。

（1）　電磁的に保存された情報

まず，電磁的に保存された情報の取得については，18 U.S.C. §§2701-2721（Stored Communications Act と称されることもある。以下，「SCA」という。）に定められている。サービス業者が，公衆に利用可能なサービス(102)を提供している場合には，私的サービスよりも厳しい規制となっている(103)。

---

(100)　石井夏生利「ACLU v. NSA　令状なき通信傍受に対する差止の可否：セキュリティ対プライバシー」『総務省情報通信政策研究所・海外情報通信判例研究会報告書（第一集）』（2010年）（http://www.soumu.go.jp/main_content/000050881.pdf , 2015年 1 月 3 日最終閲覧）91頁。

(101)　*DOJ Manual*, *supra* note 38 at 115-116.

(102)　*DOJ Manual*, *supra* note 38 at 119. 2711条(2)によれば，誰でも料金を支払い所定の手続を遵守すれば加入して利用可能なサービスをいう。

(103)　*DOJ Manual*, *supra* note 38 at 115-116. 同書によれば，立法者は，公衆に利用可能なサービスは，プライバシーの利益保護の重要性がより高いと考えた。もっとも，何が「公衆」か，は一つの論点である。

（a）　文書提出行政命令（administrative subpoena）による取得

同法において，外容情報は，（１）利用者の基本情報（氏名，住所，電話番号，利用サービスの種類と期間，ID 情報，支払方法等）と（２）その他の外容情報（加入者に関する，通信内容以外の記録その他の情報）とに区分されており，（１）基本情報については subpoena により取得することができる（18 U.S.C. §2703（c）（2））(104)。

（２）のその他の外容情報とは，通信内容以外の外容情報すべてを含み，ログやアカウント使用記録などが含まれ，2703条(c)(1)が適用される(105)。

「提出命令」に加えて利用者に対し事前または事後の通知を行う場合には，基本情報等の文書提出命令により取得可能な情報に加え，180日を超えて保存されている電子的コミュニケーションの内容情報，利用者・顧客のために保存された遠隔コンピュータ・サービス・プロバイダー（以下「RSP」という）の保有する電子通信の内容を取得できる(106)。

（b）　2703条(d)項裁判所命令

次に Section 2703（d）に基づく裁判所の命令を得ることにより，内容情報以外のすべての外容情報を取得することができる(107)。この命令を取得す

---

(104)　*DOJ Manual*, *supra* note 38 at 121. 2703条(c)(2)項によれば，（事前の裁判所の審査のない）administrative subpoena により基本情報を取得できる。なお，subpoena は通常，「召喚状」と訳されるが，ここでの subpoena は文書の提出を命ずるもので，人の召喚は伴わないので，原語のまま，あるいは文書提出命令と表記する。

(105)　同項によると，電子的通信サービスまたは RSP から外容情報を得るためには（A）犯罪捜査のための令状，（B）2703条(d)項による裁判所命令，（C）加入者または契約者の同意，（D）当該業者が行っているネット販売に関連して加入者・契約者の詐欺捜査に関する正式な要求書の提出のほか，（E）(2)項に従い基本情報を取得できる。

(106)　*DOJ Manual*, *supra* note 38 at 129-130. 事前通知により弊害（例えば生命身体の危険，証拠隠滅，証人候補の萎縮など捜査の重大な障害または裁判の遅延原因）があると監督官が証明する場合には，取得後90日以内に通知することによって通知要件を充足できる（18 U.S.C.§2705（a）(1)(B), 18 U.S.C. §2705（a）(2)）。

るためには，捜索令状のような「相当の理由」を必要としないが，subpoena よりも厳しい要件（対象通信における内容が進行中の犯罪捜査に関連し重要であること示す合理的な根拠があることを「specific and articulable facts」（具体的かつ明瞭な事実）を示すことにより示す必要がある(108)。

2703条（d）による裁判所命令に加えて事前または事後の利用者への通知を行う場合には，180日を超えて保存されている内容情報，RSP が加入者または契約者に代わって保有している電子的通信の内容情報をも取得可能となる(109)。

（c）　令状（warrant）

さらに，刑事手続法に定める手続に従って捜索令状（warrant）を取得すれば，Section 2703（d）の命令に通知を行うことにより取得できる情報に加え，内容情報（180日以下の短期間保存されているもの）も取得可能となる（18 U.S.C. §2703（a））。言い換えると，捜索令状によって捜査官は当該アカウントに関するあらゆる情報を取得することができる(110)。同令状の執行は，通常，プロバイダーに対して令状記載の資料を作成提出させることによって行われる(111)。

（d）　私人による情報収集

以上の法制は，仮にプロバイダー等の情報保管者が情報提供を拒否した場合にも情報提供を強制することができる制度であるのに対し，プロバイダーが自発的に情報を提供する場合には，2702条に基づき，以下のような規律が定められている。

---

(107)　*DOJ Manual*, *supra* note 38 at 129–130. 18 U.S.C. §2703（d）.

(108)　*DOJ Manual*, *supra* note 38 at 130–131.

(109)　*DOJ Manual*, *supra* note 38 at 132–133. 事前の通知による弊害が大きい場合には，裁判所による事後通知の許可を得て，事後通知とすることもできる。

(110)　*DOJ Manual*, *supra* note 38 at 133.

(111)　*DOJ Manual*, *supra* note 38 at 134, 18 U.S.C. §2703（g）.

まず，プロバイダーの提供するサービスが公衆に利用可能なものではない場合には，プロバイダーによるメール内容の開示はSCAにより禁止されない(112)。

これに対しプロバイダーのサービスが公衆に利用可能なものである場合には，当該プロバイダーは，SCAにより，いかなる第三者に対しても，内容情報を開示してはならず，その他の情報は，政府機関に対しては，例外に該当しない限り，開示してはならない(113)。例外的に，公共安全上の必要性が契約者のプライバシーの利益を凌駕するあるいはプライバシーに重大な脅威とならない一定の場合に開示が許容される(114)。

（2） リアルタイム（同時）監視

電子的な同時（リアルタイムの）監視についても外容情報と内容情報の峻別が見られる。外容情報についてはPen/Trap法（Pen Registers and Trap and Trace Devices chapter of Title 18; 18 U.S.C. §§2510-2522）3121-3127）(115)により，内容情報についてはTitle III（Wiretap Act, 18 U.S.C.§§2510-2522）により規制されている(116)。

---

(112)　*DOJ Manual*, *supra* note 38 at 135, 18 U.S.C. §2702（a）.

(113)　*DOJ Manual*, *supra* note 38 at 136. 18 U.S.C. §§2702（a）(3), (c)(6). 政府機関以外に対して外容情報を提供することは自由である。「例外」は外容情報に関しては2702条(c)項に定められており，2703条により許される場合，加入者・契約者の適法な同意がある場合，サービス提供に伴い必要な場合もしくは事業者の財産や権利を保護するために必要な場合，人の死亡もしくは重大な傷害を避けるために緊急に必要な場合（政府機関に対する開示），等が挙がっている。

(114)　*DOJ Manual*, *supra* note 38 at 136-137. 例外的に内容情報の第三者・政府への提供が可能となるのは，2702条(b)項によれば，（1）プロバイダーの財産を守る為必要な場合，（2）偶然に犯罪に関連する情報を見つけた際に捜査機関に対し提供する場合，（3）人の身体生命への危険が迫っている場合に遅滞なく政府機関に提供する場合，などがある。

(115)　当初ECPAの一部として成立した。

(116)　*DOJ Manual*, *supra* note 38 at 151.

（a） Pen/Trap 法（18 U.S.C. §§ 3121-3127）に基づく裁判所命令による取得

外容情報（addressing information. 架電先番号，メールのアドレスやルート情報などのヘッダー情報）については，Pen/Trap 法が，裁判所命令によって取得することを認めている。

捜査機関は，進行中の犯罪捜査に「関連する（relevant）」可能性があることを示して申請し，裁判所は，事実の真実性について独立の審査を行うことなく，申請に理由ありと判断すれば，pen/trap 機器を一定期間(117) 設置することを許す命令を発する。

Pen/Trap 法は，プロバイダーが自ら所有するネットワークに対し，サービス・保守等の必要に基づきあるいはユーザーの同意により傍受機器を設置する場合は裁判所の命令を要しないと定める(118)。

携帯基地局情報（通話の始点・終点において接続した基地局を知ることにより携帯電話で通話した者の居所を知ることができる）は，Pen/Trap 法による命令(119) に加えて前述の18 U.S.C. §2703（d）の裁判所命令を同時に得て取得する(120)。

（b） Title III（18 U.S.C. §§2510-2522）

内容情報については，Title III の厳格な手順に従う必要がある。すなわち，同法は，会話，電信電話ならびに電気通信の傍受，傍受情報の利用，開示を原則禁止しており(121)，その例外として，以下の場合にはこれらが

(117)　18 U.S.C. §3123（c）によれば原則60日間，さらに60日延長可能。
(118)　*DOJ Manual*, *supra* note 38 at at 158. 18 U.S.C. §3121（b）.
(119)　18 U.S.C. §3121（a）により必要。
(120)　*DOJ Manual*, *supra* note 38 at 160. Communications Assistance for Law Enforcement Act of 1994（CALEA）により，政府は Pen/Trap 法のみに依拠することができないため（47 U.S.C. §1002（a）参照）.
(121)　*DOJ Manual*, *supra* note 38 at 162, 167. 18 U.S.C. §2511（1）. 違反に対しては罰則がある。

可能とされる(122)。

（ⅰ） 2518条の裁判所命令による場合（Title III Order といわれる）。傍受によって，2516条に列挙された重罪の証拠を発見できるとの相当の理由（probable cause）が認められなければ発付されない(123)。また，通常の捜査が失敗しもしくは成功しないことが合理的に明らかであり，犯罪の証拠を提供しないコミュニケーションの傍受可能性を極小化する方法でなされる必要がある(124)。

（ⅱ） 通信通話の一当事者による同意がある場合（同意に基づく傍受は，もっとも頻繁に利用される方法である(125)。同意は明示黙示を問わない。）。（2511条(2)(c)-(d)）

（ⅲ） プロバイダーがその財産を保全するために行う傍受（プロバイダーが，財産や権利の保全のため捜査機関に通信情報を提供することはできるが，捜査機関から，システム管理者に対して監視を指示もしくは依頼することはできない）(126)（2511条(2)(a)(i)）。「以後のネット利用は監視されている」旨のバナー表示による同意，あるいはユーザー契約中で監視への同意を擬制することも有効である(127)。

（ⅳ） 不正アクセスの被害者が不正アクセスを監視するために行う傍受。（2511条(2)(i)）

（ⅴ） 通常の業務遂行としてなされる傍受。（2510条(5)(a)）

（ⅵ） 偶然入手した犯罪情報を自発的に提供する場合（2511条(3)(b)(iv)）

（ⅶ） 公にアクセス可能な通信は誰でも傍受可能（公開掲示板，公的チャットルームの会話など）（2511条(2)(h)(i)）

4　国家安全保障のための監視

他方，国家安全保障に関する大統領の情報収集権限とこれに対する規制の

(122)　*DOJ Manual*, *supra* note 38 at 167.
(123)　18 U.S.C. §2516, 2518 (3)(a)-(b).
(124)　18 U.S.C. §2518 (1)(c), (5).
(125)　*DOJ Manual*, *supra* note 38 at 168.
(126)　*DOJ Manual*, *supra* note 38 at 174.
(127)　*DOJ Manual*, *supra* note 38 at 170-172.

あり方については，上記の法制度とは別に Foreign Intelligence Surveillance Act（FISA）(128) が定める。

（1） 安全保障と大統領の情報収集権限

1972年，United States v. United States District Court(129) で，連邦最高裁は，国内の過激派に対する無令状監視が，当時の Title III の §2511(3) にあった「本章の規定は，武力その他の不法な方法により政府を転覆させる試みあるいは政府の存続もしくは構造に対する明白かつ現実の危険に対する，大統領の憲法上の権限を制限するものではない」との文言により正当化されるか否かについて，Title III は国家安全保障上の監視については，定めていない，とし，憲法修正 4 条を直接適用し，事前の令状審査なく監視を行うことは，許されないと判断した。これを受けて制定された FISA は，事前の裁判所の審査という要請と，安全保障上の秘密保持の要請とを同時に充たし，国家安全保障上の監視を憲法上可能とするための法制度である。特徴的な制度として，秘密法廷である Foreign Intelligence Surveillance Court（FISC）による事前審査がある(130)。

2001年の9.11テロを受けて制定された愛国者法（通称 PATRIOT Act）(131) は，Title III だけでなく FISA も改正した。同改正により，政府権限は飛躍的に拡大し，司法チェックが緩くなった（次に述べる Wall も解消され，むしろ情報共有が促進された）(132) が，スノーデン事件を契機に，外容情報

---

(128)　Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, §101, 92 Stat. 1783, 50 U.S.C. ch 36.

(129)　407 U.S. 297, 92S. Ct. 2125, 32 L. Ed. 2d 752 (1972).

(130)　http://www.fisc.uscourts.gov および http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.htmls 参照。

(131)　Pub. L. No. 107-56, 115 Stat. 272. 同法概要および逐条解説ならびに関連法につき，中川かおりほか「米国愛国者法（反テロ法）（上）（下）」外国の立法214号 1 頁（2002年），215号 1 頁（2003年）参照。

(132)　Sections 218 and 504 of the USA PATRIOT Act が特に問題視されている。218条は FISA は外国諜報を「主要な」目的とする場合のみでなく「重要な」目的

（メールの内容ではなく，送信者・タイトル・送信・受診日時などの関係する情報で，「メタデータ」といわれる情報）の収集に対しても規制しようとする揺り戻しが起こり，網羅的な収集などを制限する立法がなされた（後述USA FREEDOME Act of 2015）。

（2） Wallとその意義

FISAのもとで，犯罪捜査情報と安全保障のための諜報の取扱機関の間にWallが存在した。これは，犯罪捜査が主目的の場合は，FISAの緩和された手続きを利用して証拠収集することはできず，ECPAのルールに従わなければならない，というルールである(133)。

PATRIOT Act施行前はFISAによる監視または物理的捜索の申請においてはExecutive Branchの責任ある地位の官名により，その目的が「犯罪捜査」ではなく「海外諜報」であると証する書面を付して申請することとされており，判例により，それは「主要な目的」が諜報にあることを要件とするものと解されていた(134)。この「主要な目的」の認定において裁判所が政府内の調整活動を勘案していたことから，この要件は，諜報活動と犯罪捜査執行の政府内調整を妨げてきたとの理解がある(135)。1995年には，司法省（DOJ）は，法執行機関（捜査機関）と諜報機関の情報共有を峻別する手続ルールを策定した。ルールは，ある程度の情報共有を許容する趣旨だったが，実際には情報共有を避ける実務が広がった。

PATRIOT Actはこの仕切りを取り除き，「主要な目的」の要件を削除し

とする場合に利用可能とし，504条は，諜報に携わる職員が法執行機関と協議し，協力して捜査等に当たることを許容する。FBIはこの規定につき，1995年以降の過剰な「壁」意識を減少させ，適切な情報共有を促すものと述べている。http://www.fbi.gov/news/testimony/usa-patriot-act-amendments-to-foreign-intelligence-surveillance-act-authorities（last visited January 4, 2015）「E. The "Wall"」の部分参照。

(133) Daniel J. Solove, Nothing To Hide at 74 (2011).

(134) *Id*. at 76.

(135) *Supra* note 132). FBI資料参照。

た（同法218条によれば，「重要な」監視または捜索の目的が諜報であれば，FISA による監視が可能となる）。これには批判もある(136)。

（3） 最近の動き― USA FREEDOM Act of 2015

スノーデン事件により暴露された国家安全保障局（NSA）による包括的な架電情報収集は，2015年 6 月，USA FREEDOM Act of 2015の制定によって，一定の制限に服することとなった(137)。

問題状況としては，政府による諜報活動を適切に規律するために議会が制定した FISA の縛りが徐々に機能不全に陥り，9.11事件を契機に，さらに緩和されることにより，最終的に，テロと無関係の一般米国民の架電情報の無差別包括的収集（FISC の許可のもとに，米国大手電話会社が，ほぼすべての米国民の架電情報を，即時かつ秘密裏に NSA へ転送していた）が正当化されるに至ったことから，内容にわたらない情報であっても，プライバシーへの侵害性は高く，修正 4 条による保護を必要とする状況が出現しているのではないかとの懸念が広がってきたことがある(138)。政府は Smith 判決を挙げて，架電情報のメタデータ（架電日時，継続時間，架電先などの内容にわたらない情報）については，プライバシーの合理的期待がないという理屈を，根拠の一つとしていた。また，このような政府見解を肯定する地裁判決も出ていた(139)。

---

(136) Solove, *supra* note 133).

(137) 正式名称は，Uniting And Strengthening America By Fulfilling Rights And Ensuring Effective Discipline Over Monitoring Act Of 2015, PL114-23 [HR2048]. 発効は2015年 6 月 2 日から180日以内。

(138) *See* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harv J. L. & Pub. Pol'y 757 (2014),

(139) ACLU v. Clapper, 959 F. Supp. 2d 724; 2013 U.S. Dist. LEXIS 18086. しかし *Id.* at 867-868 は，包括的情報収集と Smith 判決の事案が異なる点を正しく指摘する。すなわち，Smith 判決の事案では，令状こそ取得しなかったが，すでに具体的な容疑事実が特定され，取得情報が容疑情報に密接に関わるものに限定される可能性が高かった事案だった。

このような状況に対してプライバシー保護の立場から，数回にわたり法案が議会に提出された。結局，国防上の施策の承認(140)と併せる形で上下両院の賛成を得て，USA FREEDOM Act of 2015が制定された。同法により，検索キーワードを特定してFISCの許可を得るように義務づけられたことにより，政府が包括的無差別にあらゆる架電情報を収集することはできなくなったほか，FISCの決定のうち重要な部分を公開するなどの改革がなされることとなった(141)。

3　第三者理論との関係―その功罪

（1）　評価すべき点

米国の電子的監視法制は，連邦最高裁が示したプライバシーについての考え方を基礎として，warrantを要する場合，裁判所命令またはsubpoenaと情報主への通知を要する場合，subpoenaのみによる場合，というように，保護の態様を段階的にして，プライバシー保護の必要性と政府による情報収集の必要性に応じて比例的に調整しようとする試みであるといえる。煩雑な面もあるが，明示的な規範を構築して実務上広範に存在する情報収集手法を統制しようとしている点は評価されるべきであろう。

特に，日本との比較において特筆すべき点としては，（1）第三者からの情報収集の際に，軽減された手続が許される条件として，情報主への通知・同意を要件としている点，（2）もっとも重厚な手続である令状による取得であっても，情報主への通知が，事後にはなされるのが原則であること，（3）国防上の監視について，犯罪捜査上の監視とは異なる法制度が構築されている点である。

---

(140)　FISCの監督のもと，國際テロリストが米国内に入国した後も72時間は米国外人に対する監視を継続できるようにすること，などの国防上の権限強化がなされた。

(141)　米国議会司法委員会サイト参照（http://judiciary.house.gov/index.cfm/usa-freedom-act, last visited on June 26, 2015）.

（2） 問題点

上記のような長所はあるものの，問題点も指摘できる。特に第三者理論に由来する問題点を指摘すると，以下のとおりである。

まず，外容情報・内容情報の区別によって，遵守すべき手続や実体法上の嫌疑の大きさ（相当の理由＞合理的嫌疑＞関連性）が段階的に異なるような仕組みが構築されている。外容情報には第三者理論が適切に当てはまるが，内容情報には第三者理論が適用されないという第三者理論に付随する考え方によるものである。しかし，現代の電子化社会において，電子的記録の外容情報（メールの送信先，時間，タイトル等）を個人別に集積するならば，個人に関する豊富なプライバシー情報のファイルができ上がることは容易に想像されるところである。このような集積を目的とする外容情報の収集を，それが外容情報を対象とするというだけの理由でプライバシーの期待を否定することは，いかにも不適切である。

次に，電子的監視に関する法制度の緻密な制度設計が，現実と齟齬をきたしていると思われる部分も見受けられる。たとえば前述のように，連邦法は，通信終了後180日間のみ，相当の理由に基づく令状を取得することを求めている。すなわちプロバイダーが180日を超えて当該情報を保有しているときには，subpoena による軽減された要件により取得できるのだが，この背景には，第三者であるプロバイダーに保有された情報に対するプライバシーの期待は，リアルタイムに授受されている情報に比べ，低い，という位置付けがあると思われる。しかし，電子的通信の場における保存された情報は，リアルタイムの情報以上に価値を持つ場合がある。リアルタイムの傍受は，人の行動の継続的集中的監視につながるという意味でプライバシーへの影響が大きいことは疑いないが，電子的に保存された情報について，プライバシーへの影響の低いものと類型化しているところに，電子的情報の有用性に対する誤った評価がある。このような類型化の前提として，自ら進んで第三者に保管させている者のプライバシーへの期待は低減する，という第三者理論の基本思想が存在すると疑われる。

また，第三者理論によれば，第三者が開封した内容情報は，情報主のプライバシーとの関係において憲法修正 4 条の保護から外れるため，第三者からこれを取得する際に，政府は修正 4 条に基づく厳格な実体および手続要件（相当な理由および令状）を必要としない。この結論は，開封されたメールの内容は，所定の到達先に到達した情報のプライバシー保護が消滅するものとして無令状で収集できるという政府の立場の根拠となるが，そうすると，むしろ開封しないスパムが保護されることになってしまうなど，デジタル化社会に十分対応できていない(142)。

これらの問題点に関連して，第三者理論に対して批判的な学説の言い分を，次章において検討する。

第 3 章　第三者理論 に関する学説の議論

1　擁護論と反対論

以上のような連邦法制ならびに連邦裁判所の判断の底流に，第三者理論があるとの認識は，従来から学界において共有されており(143)，関連する議論も活発になされてきた。本章では，そのうちでも第三者理論擁護論を展開する Kerr 氏との対立を明確にする最近の見解を紹介し，第三者理論の今後の行方について考察する。

（1）　Orin S. Kerr による第三者理論擁護論

第三者理論は，連邦裁判所によって採用されてきたが，学説は常にこれに対して批判的であった(144)。正面から第三者理論を擁護する論者は Orin S. Kerr のみという状況であるが，その主張は明快である(145)。同氏の主張

(142)　後掲注152）Nojeim の指摘。

(143)　Wayne R. Lafave, Search And Seizure: A Treatise On The Fourth Amendment (4th ed.), § 2.7 (c), 747 (2004).

(144)　Kerr, *supra* note 1, at 563 note 5).

は，おおむね 2 つの柱から成る。

一つは，旧来の捜査と現代の捜査の間で，技術が進展したことによる差異をできるだけなくそうというものである。かつて通信手段がまったくなかった時代に，人は歩いて会って通信していたが，公道を歩いて誰と会ったかという情報は，尾行や追跡等によって収集されてきた。通信手段が電子的になった今でも，だれに，いつ通信したかという情報は，内容情報とは性質が異なり，基本的にオープンであると考えるべきであるという。

もう一つは，様々な要素を考慮してプライバシーの合理的な期待の有無を判断するのは，基準が曖昧で予測可能性が低すぎるという主張である。第三者への開示の時点で，公道に出たのと同視するという理屈は明確であり，事前の予測可能性を増すという。

最初の論拠である技術的中立性の議論は，技術進歩が犯罪者側にも捜査側にも有利・不利なく中立的に機能するように，従来認められていた情報収集と同程度の情報収集を，そのまま認めようという発想である(146)。Kerr は，もともと認められていた情報収集手法に対し，新規技術が警察の能力の向上に資するのに応じて，これに均衡するように，修正 4 条による政府の権限への制約を増す必要はあるが，逆に新規技術が犯罪者の能力向上にも役立つ場合には，新技術の出現によって警察の能力が著しく減退することのないよう，被疑者側のプライバシーの期待を消滅させるべきであり，実際に判例はそのように調整を行っているとの見解を示している(147)。

---

(145)　*See*, Kerr, *supra* note 1.

(146)　Kerr, *supra* note 1, at 579–580.

(147)　*See* Orin Kerr, *Equilibrium-Adjustment Theory*, 125 Harv. L. Rev. 476, 501 (2011).

（2） 反対論

(a)　反対論の大要

反対論には，大別して，プライバシーの捉え方そのものに対する変化を考慮するべきだというものと，一律にプライバシーの期待を消滅させることが不合理だとするものがある。後者は，よりきめ細かい，事情に応じた対応を求める。多くの論者は両方の主張を総合して反論しているが，以下では二つの方向性に整理して反対論を検討する。

(b)　プライバシーに関する合理性に対する批判を強調する見解

第三者理論が導びくプライバシーに関する結論に，合理性がない，という批判である。この見解にも，（ⅰ）現代における技術の進化に対応できていない，という批判と，（ⅱ）第三者理論が前提とするプライバシーの捉え方そのものへの疑問を呈する見解がある。

前者の見解として，Nojeim は，1970年代と現代では，通信手段と技術がまったく異なると指摘する(148)。曰く，第三者理論の本質は，「窃盗容疑者の手紙が，容疑者の友人の机の上にあった場合に，警察は，友人に対して手紙の提出命令を発するか，当該友人の同意を得て手紙の提出を受けうるか，それとも容疑者の所有物として扱い，捜索令状を取得しなければならないか」ということだ，とした上で，「第三者への開示」に際しての「consent」の概念が，時代に合わなくなってきている，とする。すなわち，インターネット時代の通信において，第三者を介さない通信はありえず，第三者が経営する倉庫に物理的に格納していると修正４条の保護を受け，電子的にオンラインでプロバイダーに保管させるとプロバイダーに対する提出命令のみで取得されるというのは不合理である，という。また，

(148)　Orin Kerr and Greg Nojeim, *The Data Question: Should the Third-Party Doctrine Be Revisited?*, ABA Journal (Aug. 1, 2012), http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/ (last visited on June 28, 2015).

Nojeim は，Smith 判決は，電話の発信情報を，さしたる情報ではないと考えたかもしれないが，より情報量の多いデータは，形式上「内容」と言えなくても，修正 4 条の対象と考えるべきであると主張する(149)。

後者の論者として Slobogin と Solove が挙げられる。

Slobogin(150) は，「第三者に譲渡した段階でプライバシーへの期待がなくなる」という一律の効果は，実際の人々のプライバシー意識と整合しないと述べる。同氏の行った調査(151) によれば，情報の性質と収集の態様により，人々のプライバシー侵害性に関する感じ方が異なるという。そして，こうした感じ方の違いに応じ，手続（令状，提出命令のいずれを要するか，いずれも要しないか，相当の理由を要するか，合理的な疑いレベルでよいか，関連していればよいか）が変化すべきだと主張する(152)。

Solove は，より直接的批判を行っている(153)。すなわち，Solove は，第三者理論によって，コンピュータ事業者が保有するあらゆる情報が簡単に政府により収集されうる状態は，犯罪者以外の一般人のプライバシーに対する脅威であると危惧する。同氏はまた，プライバシーを分類し，その侵

(149)　かかる批判への直接の回答ではないが，Kerr は，Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) において，修正 4 条における search の判断にモザイク理論をとり込む（諸般の事情を勘案して全体としてみて search(es) に該当するかどうかを判断する）ならば，曖昧さゆえ収拾がつかなくなると主張しており，筆者の見解では，「情報量が多い」か否か，といった曖昧な基準によることには反対であろうと推測する。

(150)　CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151-164 (2007).

(151)　Christopher Slobogin & Josephe E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at Understandings Recognized and Permitted by Society*, 42 DUKE L.J. 727 (1993); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS L.J. 213, 275-78 (2002). 様々な場所と態様による調査を，人々がどのように受け止めるかについて調べたもので，山本龍彦が前掲書で一部を紹介している。

(152)　SLOBGIN *supra* note 150, at 180-196.

(153)　SOLOVE, *supra* note 133, at 102-110.

害の程度は，情報の種類・性質により変わるのではなく，侵害態様によって異なるのだとし，一切の情報の性質の違いを捨象する。

同氏は，外容情報（envelope 情報）であっても，履歴を詳細に収集分析されることによって個人の行動，嗜好，友人関係，思想が浮かび上がってくるものだと指摘する。そして，修正 4 条の保護のあり方を，情報の性質に応じて変更するのではなく，むしろ政府のプライバシーへのアクセス態様に着目することを提唱する。Solove は，情報主のプライバシーに対し政府がかかわりを持つ行動類型を，①情報収集，②情報分析，③情報開示・伝達，④侵襲の 4 つのパターンに分けて観察し，それぞれの場面に応じた保護のあり方を探ることを提唱する(154)。

(c)　一律の扱いに対する疑問を強調する見解

第三者理論に対して，筆者が違和感を感じる主たる要因は，第三者への情報移転によって一律にプライバシーへの期待を消滅させることにある。米国でも一律の取扱いに対する批判がなされている。

Epstein は，修正 4 条を，よりきめ細かい，柔軟な対処のできるルールにするべきだと主張する(155)。Epstein は，第三者理論の適用場面か否かという判断基準ではなく，いかなるレベルのプライバシー保護を与えるべきかを個別に判断しようとする。

Epstein はまず，第三者理論の論拠の一つとして，第三者へ送付することによってその後開示されるリスクを引き受けた，あるいは同意した，という主張があるが，そうした自律的判断をベースにした議論が当てはまらない場合がある(156) ほか，知っていることと引き受けることは異なり，同意の擬制を拡大することは濫用につながること(157)，通知して警告すれば

(154)　Daniel Solove, Undesatanding Privacy 103-106 (2008).

(155)　Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 Berkley Tech. T.J. 1199 (2009).

(156)　*Id*. at 1203. 同意できない状態の中で手術をしなければならない時など。

よいというものではない(158)ことなどを指摘し，こうした「擬制」のルールは，当人が擬制されないよう契約によりルールから逃れる途を用意していない点で，自律的判断に基礎づけられたものではないとする(159)。

Orin Kerr は Epstein の議論に対し，結論はあまり Kerr の考えと異ならないと反論する(160)。Kerr の指摘するとおり，Epstein は，「相当の理由」に基づく令状という硬直的な枠組みではなく，reasonable suspicion による一定の調査権行使を可能とするべきと主張し(161)，柔軟な修正 4 条の枠組みを提唱する。そして，警察は，ほかの一般私人ができることは（令状なく）できる，とする(162)結果，reasonable suspicion がある限り，令状なく一定の怪しい人物を（一般人が不法行為にならずに行うことができる態様で）観察することもできるとして Terry 判決(163)を支持する(164)。また，内容にわたらない情報に関する事案として Smith 判決を肯定する(165)。

Henderson は，ケースバイケースの判断によってさまざまな要素を考慮に入れ，技術の進化や社会通念の変化にも合わせて，柔軟に「プライバシーの合理的期待」を探究するべきであり，一刀両断の明確性を求めるべきではないと主張する(166)。そして，9 つの考慮すべき要素と，4 つの考慮

(157)　*Id*. at 1204. 危険な業務に就く場合でも，怪我の危険をすべて引き受けたとはいえないとする。

(158)　*Id*. at 1205.

(159)　*Id*. at 1206.

(160)　Orin S. Kerr, *Deffending the Third-Party Doctnine: A Response to Epstein and Murphy*, 24 Berkeley Tech. L.J. 1229, 1230-1232 (2009).

(161)　Epstein, *supra* note 155, at 1211, 1225. Epstein は，国家安全保障上の調査は「相当の理由」がなくても reasonable suspicion によって可能とするべきとし，第三者のもとに保管された文書等の収集を肯定する。

(162)　*Id*. at 1215.

(163)　Terry v. Ohio, 392 U.S. 1 (1968).

(164)　Epstein, *supra* note 155, at 1223.

(165)　*Id*. at 1217.

(166)　Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepp. L. Rev. 975 (2007).

しなくてよい要素を正しく衡量すれば，裁判基準として十分成り立つと提案する。

同氏は以下のような9個の考慮要素を提唱する(167)。

（ⅰ）（第三者への）開示の目的

Henderson は，第三者に対して当該情報を開示することが，社会で生きていくために不可欠であるとすれば，政府が当該第三者から情報を入手することは制約される方向に働くべきとする。

（ⅱ） 情報の性質が個人的なものであるか

ありふれて個人的でない情報は，政府がアクセスしてもよい―例えば銀行に保有されている住所氏名情報はアクセスしてよいが，詳しい取引記録はそうではない，という。また，個人的な性質のレベルに応じて政府のアクセスへの制限が比例するべきであるとする。個人的情報は，通常「自主的に」第三者に提供されたものではないからである，という。

（ⅲ） 情報の量

政府が保有する情報の量が多くなればなるほど，収集された情報の完全性ゆえに，その性質は，より個人的なものとなる。また，仮に個々に収集される情報が些末なもの（氏名，住所等）であっても，データベースとして集積された大量情報があれば，他の情報とマッチングしたり分析することにより，侵害的な利用を可能とするからである。

（ⅳ） 情報主の期待（社会通念）

職場の PC には通常プライバシーは期待できないというのが社会通念であるように，情報主の予期する範囲が考慮されるべきである。また，何が社会通念かについて，裁判所は立証を尽くさせるべきであり，Slobogin が行ったような実態調査（前述注151）に即した研究成果を取り入れ，現在の実務を見直すべきである。

（ⅴ） 第三者の認識

第三者が，当該情報を秘密であると認識しているならば，政府の入手を制約する要素となる。第三者が情報主に対して負う秘密保持義務に配慮するという趣旨。当局から要求されているというだけで，情報が秘密でないと（第

(167) *Id.*

三者が）考えると推定するべきではなく，秘密保持の約定があれば，尊重されるべきであるとする。

（vi）　積極的に秘密を保証する法律の存在

司法当局が具体的に禁止されている行為を行ったのであれば，そうした情報収集は「reasonable」とはいえない。

（vii）　政府の必要性(168)

政府が情報を必要とする必要度の高さと，プライバシーへの影響の程度との間で調整点をみつけるべきである。必要性の立証責任は政府にある。必要な情報の性質，範囲，関連性については，政府に自由裁量が認められるわけではない。

（viii）　個人の記憶

政府が求める情報が，記録そのものではなく，第三者である個人が記憶していることを陳述することである場合は，政府のアクセスを認める方向に働くべきとする。

（ix）　変化する社会通念と技術

新しい社会通念や技術に対応し，これらを新たな考慮要素とするべきとする。

考慮すべきでない要素

（x）　情報の記録形態

原情報の記録形態が第三者のもとで変更されても，修正 4 条の保障は影響を受けない。

（xi）　第三者の「よき市民」としての動機

第三者が協力的に情報を提供したとしても，考慮要素としない。

（xii）　政府の収集方法

政府の情報収集手法により制約は変わるべきではない。第三者を召喚して陳述させても，令状をとって情報収集しても，同じくらい権利への影響がある。

（xiii）　司法当局の行為によって生じた予見

司法当局自ら全国民に予告することによってプライバシーの期待を消滅さ

(168)　*Id*. at1008.

せることは認めるべきではない。司法当局自らの行為によって私人の「期待」が左右されてはならない。

このように見てくると，Henderson の見解は極めてバランスのよい落ち着きのよいものに感じられる(169)。同氏の議論には，日本の行政法における裁量論において持ち出される「考慮要素・考慮すべきでない要素」の評価によって行政権力とプライバシーを調整しようというロジックとの類似性を見出すことができる。個別論点の判断についてはやや異論もありうるが，日本への示唆という点で参考になる。

（3） 小括

総じて Kerr の第三者理論擁護論は明快であり，実務的指針としては有用であろう。Kerr の指摘するとおり，何が「合理的」なのか，の判断枠組みとして，各要素の総合判断だけでは，結局バラバラの判断となってしまう恐れがある。本人が自らの意思で第三者に引き渡したという状況があれば，そのことによって，本人の支配権の程度が類型的に減少していると考えることは一定の合理性があり，様々な考慮要素を均等に考慮するという手法に比べ予測可能性は高い。

しかし，現代の技術を前提とした情報の収集・集積・利用の態様を考えるとき，それがプライバシーに影響する態様は，Smith 判決や Miller 判決の時代とは全く異なる。前章で見た現行法の問題点は，上記の技術の進化に対応できていないという批判と相通じている。Slobogin や Solove のいうプライバシー保護の必要性との齟齬も，結局は，現在想定されている第三者理論が，デジタル時代におけるプライバシーの保護のあるべき態様に対応できていないことから生じているのである。

---

(169) なお，Henderson は，Solove と Slobogin の主張にも概ね賛成するが，Solove が，情報内容の性質による相違を捨象して収集態様に着目している点に，Slobogin が，内容情報と外容情報の峻別を維持する点に対し，それぞれ反対している。See *Id.* at 1019.

Kerr は，プライバシーの合理的期待の有無を「総合的に」考察すると（いわゆるモザイク理論）の取り入れにも反対する。その背景には，裁判所が「総合判断」によって法創造を行うことへの警戒があるようだ。Kerr は，むしろ，ステップごとの明快な判定を行い，それが不適切な解を導くならば国会が制定する法律によって明示的に処置すべきであるとする(170)。

しかしながら，単体での情報がプライバシー保護の必要がないように見える場合でも，集積されることによって，例えば人の行動パターンや交友関係，思想傾向などが見て取れることは否定しがたい。そのような情報を把握されること自体が，プライバシーへの許容し難い侵襲であるとの見解(171)は，特にデジタル化され，あたかもすべての人が一定程度，プライバシーを放棄しているような時代にあって，却って重要度が増している(172)。すなわち，現代のデジタル社会においては，プライバシーの終焉ともいえるほどに，公に自己情報が流出している。しかし，だからこそ，自由にこれを集積されることによって，深刻なプライバシー侵害が生じる可能性を生じているともいえるのである。この問題について連邦最高裁が認識を示したのが前出 Jones 判決であり，その判決意見（特に同意意見）は，今後の第三者理論に対する大きな示唆を含んでいる。

2　Jones 判決とその後

2011年 Jones 判決において，法廷意見は，プライバシー侵害の態様に応じて search（es）への該当基準を 2 種に分け，（1）Olmstead 型の物理的侵襲基準と（2）Katz 型のプライバシーの期待基準があるとし，同事件は前者で解決するケースであるとした。これに対しては，Katz 判決は物理的侵襲基準を否定したはずだ，などの批判がなされている(173)。

---

(170)　*See* Kerr, *supra* note 149.

(171)　Solove, *supra* note 153.

(172)　Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 Miss. L.J. 1309, 1338 (2012).

しかし同判決の同意意見，特にソトマイヤー判事の意見は，修正 4 条は物理的侵襲に依らずにプライバシーを保障するものと捉え，政府に監視されること自体から生じる萎縮効果を問題視するとともに，第三者理論がデジタル時代に合わなくなっており，見直す必要があると明確に指摘した。ソトマイヤー意見に依拠して，NSA による FISA に基づく網羅的情報収集（収集された情報は電話のメタデータすなわち外容情報である）を修正 4 条違反としたニューヨーク連邦地方裁判所判決も現れた(174)。そして，限定的ながら法改正につながったことは既述のとおりである。

さらに，Riley v. California(175) は，適法な逮捕に際して押収した携帯電話内の電子的情報にアクセスするためには，緊急の場合として正当化されるとき以外は，新たな令状を必要とすると判示した(176)。つまり，デジタルデータの保存先は，それが例えば第三者である ISP であっても，ブリーフケース内の情報と同様に，修正 4 条のプライバシーの期待が存続するものと判断される可能性があることを示唆した。この判決を受けて，従来か

---

(173)　George M. Dery III, Ryan Evano, *The Court Loses Its Way With The Global Positioning System: United States v. Jones Retreats To The "Classic Trespassory Search"*, 19 MICH. J. RACE & L. 113, 139–140 (2013).

(174)　Klayman v. Obama, F. Supp. 2d, 2013 U.S. Dist. LEXIS 176925, 2013 WL 6571596 at 14–17 (D.D.C. Dec. 16, 2013). 控訴中。もっとも，同じニューヨーク連邦地裁で同じ月に下された別の判決（前述の ACLU v. Clapper, 959 F. Supp. 2d 724; 2013 U.S. Dist. LEXIS 18086）では，電話先情報にはプライバシーの合理的期待がないとした Smith 判決に従うべきであるとして，同じデータ収集を修正 4 条に反しないとした。

(175)　134 S. Ct. 2473 (2014). 同判決に関する論稿として，柳川重規「逮捕に伴う捜索・押収の法理と携帯電話内データの捜索――合衆国最高裁 Riley 判決の検討」法学新報121巻11・12号527頁参照。

(176)　法廷意見（ロバーツ判事）は，携帯電話が，その高い保存機能ゆえに質的・量的にプライバシーへの影響が甚大であることを重視し，例えば，逮捕に伴い偶々見つけた 1－2 枚の写真を押収することが正当化されるからといって，携帯電話に保存された数千枚の写真の押収は正当化できないなどと述べている。これに対しアリート判事は，一部反対意見において，立法府に委ねるべきことがらであるとした。

らの第三者理論が変容し，デジタル化されたデータに関する適用範囲については，より制限的な結論もありうると指摘する論者もある(177)。

まとめ

（1） 第三者理論の現状と今後

第三者理論は，修正 4 条におけるプライバシーの合理的期待保護の理論と背中合わせの議論であり，規範的なプライバシー保護の限界を設定する理論として，今も連邦最高裁によって明確に認識されている。電子的監視の精緻な法制は，第三者理論を前提としており，今後も第三者理論の考え方そのものは存続するであろう。

その上で，プライバシー情報がサイバースペースにおいて氾濫し，プライバシーの喪失とともにプライバシーへ侵害の日常的脅威に直面している現代人のプライバシー事情との調整の鍵は何であろうか。筆者は，それは，プライバシー情報の単位の捉え方を変更することにあると考える。同様の考え方はモザイク理論としてすでに提案されている。今後の第三者理論は，モザイク理論によって一定の緩和ないし変容を遂げていくと予想される。

（2） 日本への示唆

日本には，第三者への情報移転をプライバシー期待の減少契機として明示的に認識する議論はない。しかし筆者は，日本においても，実際には第三者理論が実務に浸透していると考えている(178)。この点は今後検証した

(177) Laurie Buchan Serafino, *"I Know My Rights, You Go'n Need A Warrant For That:" The Fourth Amendment, Riley's Impact, And Warrantless Searches Of Third-Party Clouds*, 19 Berkeley J. Crim. L. 154 (2014) at 159-161 は，第三者理論がクラウドコンピューティングサービスには及ぼされるべきでないと主張し，その主張の中で，前述の Riley v. California を引用している。同主張はしかし，第三者理論そのものを全否定する趣旨ではないと思われる。

いと考えるが，この仮説がもしも正しいとするならば，まずは実際に採用されている，日本における第三者理論を，明示的に認識するべきである。そして，米国においても，第三者理論の行き詰まりが露呈している現在，第三者への情報移転によるプライバシーの期待の減少を，認めるべきか，認めるとすれば，どのような条件が整ったときに，どの程度認め得るかを，明確に議論の対象とするべきである。その際に米国の議論を参照することができるだろう。例えば，米国法制が前提とする様々な考え方を，前提条件として考慮しなければなるまい。例えば（１）情報提供に対する同意は情報保有主体のみでは決定づけられない，（２）第三者経由の情報収集における情報主への通知の位置付け（情報主への通知により手続要件を緩和する仕組み），（３）令状，subpoena，相当の理由，合理的な嫌疑といった，手続上，実体上の要件を，プライバシー保護の必要性に応じて比例的に配置しようとする個別立法の考え方などは参照すべきであろう。

以上

（謝辞）　本論稿は，JSPS 科研費研究活動スタート支援（26885093）の助成を受けた研究の一部である。

（追記）　本稿脱稿後，富井幸雄「安全保障上の電子的監視――権力分立と合衆国憲法修正第四条の交錯」法学新報122巻３・４号75頁に接した。本稿でも一部触れた安全保障目的の電子的監視について，権力分立，とりわけプライバシー保護における司法の役割という視点から詳細な検討がなされている。本稿で述べた第三者理論は，第三者法理として紹介されている。同稿には，修正四条が諜報には厳格に適用されていないとの指摘がある。この点に

(178)　各省庁が公表している「個人情報の保護に関する法律についてのガイドライン」を見る限り，警察の任意の求めに応じて保有する個人情報を提供する場合には，本人の同意を得ることにより国の期間の事務遂行に支障を及ぼすおそれがあるときの典型例として挙げられている（法16条３項４号関係）。警察の捜査に対する加入者・契約者の情報提供に令状を条件としているのは，通信事業者に対する総務省のガイドラインだけである（2015年５月１日，各省ウェブサイトにて確認）。

関連して，修正四条の行政調査への適用状況について，次稿で研究することとしたい。