

電話番号探知捜査について : アメリカ愛国者法を契機として

著者	松代 剛枝
雑誌名	關西大學法學論集
巻号	57 6
ページ	1020-1037
発行年	2008-03-15
その他のタイトル	Pen Register and Trap-and-Trace Surveillance : What does section 216 of the USA PATRIOT Act imply?
URL	http://hdl.handle.net/10112/12229

電話番号探知捜査について

——アメリカ愛国者法を契機として——

松代剛枝

目次

- 序
- 一 愛国者法三二六条の背景——通信内容情報保護から通信経路情報保護へ——
 - 二 「限定的開披」法理の系譜（アメリカ判例）
 - 三 「自発的開披」法理の系譜（アメリカ判例）
 - 四 日本法への示唆
- 跋

序

電話の着信先・発信元——いわゆる通信経路情報——を探知するためには、順探知機器ペンレジスタ (pen register) なし逆探知機器 (trap and trace device) を用いる。前者は、特定電話からダイヤルした先の電話番号を記録する性能を備えた機器 (着信先番号記録機器) であり、後者は逆に、特定電話に対してダイヤルした源の電話番号を記録する性能

を備えた機器（発信元番号記録機器）である。アメリカ合衆国で二〇〇一年に成立した「愛国者法（USA PATRIOT Act）」は、その二一六条において、このように電話番号のみを想定していた従前の順探知・逆探知機器の法的定義・法体系を、電子メールの着信先・発信元探知の場合へと拡張した。

本稿では、通信経路情報取得という捜査手法の法的性格と、その中で電話番号探知の占める位置とを、アメリカ法を素材に検討する。⁽¹⁾ わが国における議論枠組との異同を明らかにすることで、比較法的示唆を得たい。

一 愛国者法二一六条の背景——通信内容情報保護から通信経路情報保護へ——

1

アメリカ法では、従来から、郵便の通信内容情報は憲法上の保護を受けるが、その封筒外部情報（受取人及び差出人の氏名住所、切手・消印、寸法・重量）については誰も見うることから「プライバシーの合理的期待」を有しない——第四修正の保護はない——と考えられてきた。後者に関する連邦法上唯一の規制は一九七五年制定の連邦規則であるが、それによれば、捜査官は必要性の合理的理由を示しさえすれば当該通信経路情報を取得しうる。⁽³⁾ 司法審査は不要であり、当該処分に対する不服申立手段もない。そしてかかる郵便の通信経路情報に相応するものとして、着信先電話番号についても、一九七九年に合衆国最高裁判所は、同じく第四修正の保護はないと判示した（Smith v. Maryland⁽⁴⁾）。この判断は主に、電話番号という情報が、①限定的なものであること（後述二「限定的開披」法理）と、②電話会社に対して自発的に開披されていること（後述三「自発的開披」法理）とに、由来する。他方、このような電話の通信経路情報とは異なり、電話の通信内容情報については、既に一九六七年の Katz v. United States⁽⁵⁾

が第四修正の保護対象と認めたとうえで、一九六八年の「犯罪取締・街路安全に関する総括的法律」第三編（以下「Title III」という⁽⁶⁾）が、所定犯罪類型についての厳格な要件に基づく傍受令状発付という形でその保護を明文化していた。

その後議会は、一九八六年の「電子的通信のプライバシーに関する法律 (Electronic Communications Privacy Act)」(以下 ECPA とする) において、順探知・逆探知機器の設置・使用に裁判所命令 (court order) を要求することによって、電話の通信経路情報（着信先及び発信元電話番号、通話時刻・継続時間）に制定法上の保護を与えた⁽⁷⁾。尤も、当該命令の発せられる基準は、通常の令状発付に要求される「相当な理由 (probable cause)」よりも低く、捜査官は「獲得される見込みのある情報が……進行中の犯罪捜査と関連する」ことを裁判所に対して確証すれば足りる。前記 Title III のような対象犯罪類型の制約もなく、対象者が当該捜査の被疑者である必要もない。加えて、捜査官が裁判所に対して情報取得結果の報告義務を負わない点でも、その要件は、通常の搜索差押令状の場合に比して明らかに緩やかであった。

2

電子メールの登場は、この「通信経路情報（電話番号）」法制に新たな疑義を生ぜしめた。電子メールの通信内容情報取得については、電話の通信内容情報取得に際して要求される前記 Title III が拡張的に及ぼされるべく早や一九八六年に法改正が成っていたもの⁽⁸⁾、通信経路情報取得については、順探知・逆探知機器の電話限定定義が依然として維持されていたからである⁽⁹⁾。ここにおいて、電話及び電子メールの通信内容情報は Title III によって（通常の搜索差押に比して）手厚く保護され、電話の通信経路情報（電話番号）は ECPA によって（通常の搜索差押に比して）緩やかに保護されるが、電子メールの通信経路情報は法的空白状態に陥った。かかる状況は、以後二〇〇一年の

愛国者法二一六条の制定時まで続くことになる。

この法的欠缺を埋める解釈として。もし仮に電子メールの通信経路情報が電話の通信経路情報の法体系 (ECPA) の射程にないと解釈するならば、捜査官には通信事業者 (インターネット・サービス・プロバイダ) に対する強制手段がない以上、通信事業者はその契約者との個人情報保護規約等からして、情報提供に協力しない可能性が高い。従って、捜査官としては、電子メールの通信経路情報の取得について、内容取得に係る傍受令状を得なければならぬ——あるいは情報取得しうる適法な手段は一切存在しない——ことになりかねない。かかる事態を懸念してか、司法省は、ECPA が電子メールにも適用されると解釈し、大方の実務もまたそのように運用されてきた。⁽¹⁰⁾ 但し、二〇〇〇年一月の一判例は、電話限定定義に該当する順探知機器ではないことを理由として、通信事業者に対するメールアドレス探知命令の発付を拒んでいた。⁽¹¹⁾

3

このような状況下で齎された二〇〇一年の愛国者法二一六条は、電子メールの通信経路情報に対しても、電話番号のそれと基本的に同様の保護を与える趣旨を明文化した。⁽¹²⁾ すなわちこれは、既存実務 (の大勢) を立法にて承認したものと違ってよい。尤も、同条は同時に新たな要件として、当該探知の詳細記録を保全してこれを探知命令の期間終了後三〇日以内に裁判所に提出する義務を、捜査機関に課した。⁽¹³⁾ そして、この新要件が電話番号には及んでいないことからすれば、この改正法体系は、電子メールの通信経路情報に対して、僅かながらより手厚い保護を与えたものといえる。

なお、二一六条は、愛国者法の中にありながら、当初から広く非テロ事件一般における適用を念頭に創設されてお

り、かつ、愛国者法の^{サンセット}時限措置条項の対象外となっている点も、興味深い⁽¹⁴⁾。

二 「限定的開披」法理の系譜（アメリカ判例）

1

合衆国最高裁判所は、一九七九年の前記 Smith 判決において、政府の要請を受けた電話会社が私宅からかけられた電話番号を記録するために順探知機器を設置・使用することは、修正四条にいう搜索ではないと判示した。このとき同裁判所は、順探知機器による電話番号探知を電話の通信内容情報取得とは区別して緩やかに許容する論理として、順探知機器が極めて限定的な情報（着信先電話番号）しか開披しない点に着目していた。

2

かかる「限定的開披」法理は、他の捜査手法の許容例の裡にも看取される。例えば警察犬による臭気検査が、手荷物等の内部に禁制品が存在するという情報のみを明かすことを以て許容されている如くである。⁽¹⁵⁾

この法理に対しては、しかし、電話番号が果たして保護に値しないほどに限定的情報に過ぎないか当初から素朴に疑義が存在したうえ、以下のような近時判例動向に鑑みても、いまや再検討の時期に至っているように思われる。

二〇〇一年の *Kyllo v. United States*⁽¹⁶⁾ において、合衆国最高裁判所は、熱画像機器 (thermal imager) を用いて公道から私宅を解析——屋内熱量分布（大麻栽培用照明装置の存在・使用を推認させる情報）探知——したことを、搜索にあたりと判示した。その判断根拠は、① 一般的に公衆に使用されていない機器の使用と、② 屋内の私事の開披とである。曰く、「本件のように、一般的に公衆に使用されていない機器を政府が使用して、物理的侵入なしには予

め知りえなかった屋内情報を開披するならば、その監視は「搜索」である」と。確かに熱画像機器は家からの相対的熱発散という「限定的」情報を探知するのみではあるが、本件法廷意見によれば、「家の中では……全てのもものは私事 (intimate details) である。なぜなら、この領域全体が、詮索好きなき政府の目の届く心配のない状態にあるからである」「家に対する修正四条の保護は、情報の質や量の測定と結びつけられては、こなかった」(Scalia 判事執筆)。

ここで想起されるのは、電波発信器を対象物 (禁制品容器等) に設置してその動向を監視する捜査手法において、動向を屋内まで追跡すれば搜索にあたることである。たとえ当該電波発信器によって「唯一探知した物が屋内にあるエーテル缶である」としても⁽¹⁷⁾。

3

順探知・逆探知機器は、「一般的に公衆に使用されていない機器」である。「屋内の私事」か否かについては、少なくとも私宅の固定電話からかけられた場合の発信元電話番号探知は、当該時刻に当該私宅内に人が居るという現在情報を明らかにする点で、前記 Kyllo 判決の基準に照らせば保護されるべき法益の侵害にあたりうる⁽¹⁸⁾。他方で、私宅外の固定電話 (公衆電話等) や携帯電話を発信元として探知する場合は、発信者現在地情報にこのような「屋内」保護は及ばないとも考えられる。しかし、一般に想定される公衆視から外れた態様による現在地情報取得ではある以上、これがそのまま許容されるべきか否かは、搜索差押法体系全体を睨みつつなお検討すべき課題である⁽¹⁹⁾。比べて、着信先電話番号探知については、受信者の現在地情報を包含するとは限らない——着信していても受話器が取られない場合や留守番電話応答の場合もありうる——点で、相違する (尤も、偶発的要素が大いに与っているので、本質的相違とまではいえまい)。なお、郵便や電子メールの場合は、通信経路情報の裡に人の現在地情報を、少なくとも電話の

ような直接的な意味では包含しない。

とりわけ電話番号がどの程度「限定的」情報であるのかを、あらためて検討する必要がある。

三 「自発的開披」法理の系譜（アメリカ判例）

1

合衆国最高裁判所は、一九七九年の前記 *Smith* 判決において、着信先電話番号探知を搜索ではないと判示するにあたって、もうひとつ、電話会社への「自発的開披」法理——あるいは「リスク想定」法理——を用いて「プライバシーの合理的期待」を否定した。

同裁判所によれば、第一に、そもそも人は一般に、自分がかけた番号についてプライバシーの現実的期待を持たない。電話契約者は自分の月払請求書に添付されている通話明細を受領している以上、自分のかけている番号が電話会社に伝わっていること、及び、電話会社がこの情報を記録する性能を備えていることを、了知している。従って、「十中八九 (in all probability)」、そもそも人は自分のかけた番号についてプライバシーの現実的期待を抱いてはいない、と。

そして第二に、仮に自分のかけた電話番号についてプライバシー期待を抱いている者がいたとしても、この期待は客観的に不合理であるという。人は、自分が第三者に「自発的に」引き渡す情報については、その情報の更なる伝播リスクを既に想定・負担しているのであり、プライバシーの適法な期待を有しないからである（「自発的開披」法理ないし「リスク想定」法理）。すなわち、電話契約者は、第三者（電話会社）に対して情報（着信先電話番号）を意

識的に晒すことによつて、その情報が捜査官に伝えられるリスクを既に想定・甘受している（べきである）、と。

2

かかる「自発的開披」法理の適用は、前記 Smith 判決の理解によれば、秘密録音（当事者録音及び同意録音）の場合と通底する。⁽²⁰⁾

ここで当事者録音とは、覆面捜査官等が、自身に対するかあるいは自身の面前にいる他者に対する被疑者の供述をそのまま取得する場合（純粹な「偽装友人 (False friend)」類型）であり、同意録音とは、被疑者と会話している相手方に秘聴器を携帯させて捜査官が被疑者の供述を（同時）間接的に取得する場合（「秘聴器付き偽装友人 (wired false friend)」類型）である。合衆国最高裁判所は、前記 Smith 判決に先立つ一九六七年度の Hoffa v. United States⁽²¹⁾ 及び一九七一年の United States v. White⁽²²⁾ において、これらのいずれの形態についても、自発的開披（リスク想定）法理ゆえ搜索ではないと判示していた。

この論理に則れば、屋内発着信の通話であっても場所の保護は及ばない。

3

しかし、この「自発的開披」法理が成り立つためには、その前提として、人が自分の秘密意思疎通を享受すべき者を定める際に自由に裁量権を行使しうる状況が存在しなければならない。そして、少なくとも電話番号の引渡しにあっては、引渡し先が会話相手方ではなく電話会社であること、かつ、現代社会において電話を使う場合には電話会社を通す以外に選択肢がないことからすれば、秘密録音の場合とはその前提において異なっており、「自発的開披」法理による許容はより難しい。なお、情報の引渡し先として会話相手方を含まないというこの構図は、電話番号の場

合に固有である。通信内容情報のみならず通信経路情報においても、少なくとも郵便の場合には（そして通常は電子メールの場合にも）、引き渡される情報は通信事業者と通信相手方とで基本的に同一である。

そもそも「ある者に対して情報を開披する者は、この情報が他の目的で他の人々に対して開披されうるリスクを当然に想定する」という一般的ルール定立に対しては、そのような社会における人々の意思疎通の萎縮効果への懸念ゆえ、疑義も根強い。「自発的開披」法理を拡張的に用いることには、厳に慎重さが求められる。

四 日本法への示唆

1

アメリカ法においては、当初から通信経路情報と通信内容情報とは大きく隔差づけられており、前者については憲法上の保護は及ばないと考えられてきた。このような中で一九八六年の立法（ECPA）は通信経路情報取得のうち電話番号探知を対象として初めて司法審査を要求したが、その要件はなお極めて緩やかであった。そして、このとき構築された緩やかな保護の法体系が、電話番号からこのたび愛国者法において新たに電子メールに及ぶに至っても、基本的になお維持されている。

2

翻って、わが国において。憲法二二条二項が「通信の秘密は、これを侵してはならない」と規定するところ、通信経路情報と通信内容情報とは、ともに当初からいずれもこの「通信の秘密」の保護下にあった。

郵便については、郵便法八条一項が「会社（旧文では郵政省）の取扱中に係る信書の秘密は、これを侵してはなら

ない」とし、同条二項が「郵便の業務に従事する者は、在職中郵便物に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。」とする。この解釈につき、昭和二八年の内閣法制局見解は、「郵便物の差出人又は受取人の居所、氏名及び差出個数等は、もとより通信の意味内容をなすものではないけれども、通信そのものの構成要素であり、実質的に見ても、これらの事項を知られることによって、通信の意味内容が推知されることもありうる」から、郵便法八条二項の「他人の秘密」にあたるとして、「通信の秘密」の保護を及ぼしてきた。⁽²³⁾

かかる郵便にまさに相応するものとして、電話及び電子メールについても、電気通信事業法四条一項が「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない」とし、同条二項が「電気通信事業に従事する者は、電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。」とする（前身たる公衆電気通信法五条一項・二項も各同旨）。そして、昭和三八年の内閣法制局見解は「電話の発信場所は、発信者がこれを秘匿したいと欲する場合がありますから、『公衆電気通信法五条』の第二項にいう『他人の秘密』に該当する」ので、「〔日本電信電話〕 公社の職員が電話の発信場所を探索し、これを他人に知得させることは、原則として法第五条第二項に違反」するとして、やはり「通信の秘密」の保護を及ぼしてきた。⁽²⁴⁾

但し、この三八年見解は、「電話を利用して脅迫の罪を現に犯している者がある場合において、被害者の要請があるときは、公社の職員が当該電話の発信場所を探索し、これを捜査官憲に通報することは、許されるものと解すべきである」ともいう。ここで提示された例外許容要件は、身代金要求事件等に係る「現行犯性」及び「被害者の要請（一方当事者の同意）」⁽²⁵⁾である。⁽²⁵⁾この点、その後の実務においては、「被害者、その他の者の生命・身体・財産に重大

な危害が切迫しており、他の方法ではこれを救うことが困難であると認められる」ときであって通話の一方当事者が同意している場合とも解しており、要件に若干の緩和がみられる⁽²⁶⁾。ただいづれにせよ、双方当事者不知を前提に成り立つ着信先電話番号探知の方は、通信内容情報取得（双方当事者不知）に伴う場合を除いては、⁽²⁷⁾基本的に想定されてこなかったことが窺われる。すなわち、問題は端的に電話の「逆探知」という形で提示されてきた。

かかる状況は、一九九九年の通信傍受法成立（二〇〇〇年八月一五日施行）後において、通信内容情報取得については新設の傍受令状を以て許容されうるに至っても、⁽²⁸⁾なお変わらない。

3

電話番号探知について、わが国の学説は、①「一方当事者の同意」の下に、同意録音に準じた形で「プライバシー期待の乏しさ」を挙げるか又は（実務とほぼ同じく）「現行犯性」もしくは「正当防衛」を挙げて例外許容する見解⁽²⁹⁾と、②（かかる例外許容構成を併用しつつも）検証令状を以て許容する見解⁽³⁰⁾とに、大別される。更に、一部には、③「一方当事者の同意」のみを以て許容する見解⁽³¹⁾も存在する。

思うに、第一に、電話内容情報の引渡し先は会話相手方であるが、電話番号情報の引渡し先は電話会社である。その意味で、一方当事者の同意があっても、考慮の一要素とすることは格別、同意録音の枠組をそのまま適用しうるものではない。同意録音の許容枠組に当て嵌めようとすれば、その同意は「電話会社の同意」ということになるが、これは、情報引渡し先を選択する裁量権がないという点において、そもそも同意録音許容枠組成立の前提を欠く（本稿三参照）。尤も、「一方当事者の同意」を要求することは、必然的に発信元電話番号探知への限定——着信先電話番号探知の不許容——という帰結を導く点において、大きな意味を持つ。既存令状を適用する見解を採れば、この限定は

失われることになろう。

第二に、発信元電話番号探知は、通信履歴情報取得の性格と発信者現在地情報取得の性格とを併せ持つ（なお、電話番号からの当該契約者情報の割り出しについては、通信の秘密の枠外として、捜査関係事項照会（刑訴法一九七条二項）による⁽³²⁾）。そして現在実務では、過去の通信履歴情報取得については検証あるいは（通信明細の記録用紙の）差押令状が、携帯電話の全地球測位システム^Sによる電話所持者の現在地情報取得については検証令状が要求されている⁽³³⁾。これらの実務の当否自体なお検討の余地を残すが、少なくとも発信元電話番号探知は両者の性格を併せ持つに近く、特段の捜査利便性とともにも独自の権利侵害性を有する。その意味で、限定的情報のみを開披するものとしての劣位保護の法体系は、通信経路情報なかんづく発信元電話番号の場合には、到底適合しない（本稿二参照）。

わが国において、発信元電話番号探知の根拠・法的性質については従来必ずしも詳細に論じられてきたわけではないが、「通信の秘密」の保護を及ぼしたうえでの、一方当事者同意の下での急急的例外許容という構成は、実務をも含めてある程度広く共有・承認されてきた。かかる限定指向自体は基本的に望ましいものと思われるが、実務運用に委ねられた判断基準の潜在になお問題を残す。しかし、この点への懸念ゆえにただちに既存の検証令状枠に落とし込もうとすれば、順探知許容をも視野に入れた射程拡張を招くとともに、新種の権利侵害——この点は今日ますます顕在化している——を容れた事実上の新類型令状創設であるとの批判をも生じよう。将来的には立法論検討の余地もあるが、いずれにせよ許容基準の潜在的弛緩を避けるべく、まずは法的性格の特異性を念頭においたうえでの現行許容基準の顕出・画定が先決である。

跋

アメリカにおいて、このたび愛国者法が電子メールの通信経路情報に対して齎した法規制は、従前の経緯・状況に照らせば、それ自体決して権利制約的性格を持つものではなかった。アメリカ愛国者法が、プライバシー保護法的性格を持つと屡々いわれることも、この点ではなるほど故ないわけではない。

しかしながら、このたび電子メールを取り込むことでその正当性自体は疑われることのなかった既存の法体系——とりわけ電話番号探知の固有の権利侵害性とそれに相応しからぬ^{ラフ・セーフガード}雑駁な保護措置——こそ、実は問われるべきであったように思われる。

- (一) See Recent Decision, *Installation and Use of a Pen Register Dose Not Constitute a Fourth Amendment "Search"*—*Smith v. Maryland*, 38 Md. L. REV. 767 (1979); Clifford S. Fishman, *Pen Registers and Privacy: Risks, Expectations, and the Nullification of Congressional Intent*, 29 CATH. U. L. REV. 557 (1980); John Applegate & Amy Grossman, Note, *Pen Register After Smith v. Maryland*, 15 HARV. CIV. RIGHTS-CIV. LIB. L. REV. 753 (1980); Les Brannon, Note, *Application of the Fourth Amendment to Pen Register Surveillance — No Justifiable Expectation of Privacy: Smith v. Maryland*, 33 Sw. L. J. 1283 (1980); JoAnn Guzik, *The Assumption of Risk Doctrine: Erosion of Fourth Amendment Protection Through Fictitious Consent to Search and Seizure*, 22 SANTA CLARA L. REV. 1051, 1073-78 (1982); John M. Burkoff, *When is a Search Not a "Search"?* *Fourth Amendment DoubleSpeak*, 15 U. TOL. L. REV. 515, 537-41 (1984); G. C. Smith, *We've Got Your Number*, 367 UCLA L. REV. 145 (1989); Christian David Hammel Schultz, *Unrestricted Federal Agent: "Carnivore" and the Need to Revise the Pen Register Statute*, 76 NOTRE DAME L. REV. 1215 (2001); STEPHEN J. SCHULHOFER^①, *THE ENEMY WITHIN* 39-40 (2002); Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother that isn't*, 97 NW. U. L. REV. 607 (2003); I WAYNE R. LAFAYE, *SEARCH AND SEIZURE* § 2.7 (b) (4th ed. 2004); STEPHEN J. SCHULHOFER

②, RETHINKING THE PATRIOT ACT 85-93 (2005); J. McClintick, *Web Surfing in Chilly Waters: How the PATRIOT Act's Amendments to the Pen Register Statute Burden Freedom of Inquiry*, 13 AM. U. J. GENDER SOC. POL'Y & L. 353 (2005); 1 JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE §§ 6.05, 6.09, (4th ed. 2006); 岡本篤尚「愛国者法による FISA の改正と電子的監視権限の強化」神院三五巻四号一〇七九頁(二〇〇六)；わが国の詳細な研究として、井上正仁『強制捜査と任意捜査』一九二頁(二〇〇六)、有斐閣)「同」電話逆探知の適法性』『刑事法学の現代的状況(内藤謙先生古稀祝賀論文集)』四八三頁(一九九四、有斐閣) 初出] 参照。

なお、インターネット閲覧の場合の発信元・着信先探知については、いかなるウェブサイトを閲覧したか、すなわちいかなる情報を摂取したかという情報とほぼ一体である点で、別途問題を生じうる。この情報取得は、図書館から借りた本の題名一覧やレンタルビデオ店から借りたビデオのタイトル一覧と比肩しうるほどに「内容」的かつ「私事」的でありうると思判される (e.g. SCHULHOFER^①, *supra* note 1, at 39)。しかし、この点については、形態は通信経路情報取得ではあるが、むしろ通信内容情報取得そのものとも構成しうる」と、そもそも人と人との意思疎通としての通信とは同列に扱い難いこと等に鑑み、本稿では検討の射程外とした。

- (2) *Ex parte* Jackson, 96 U. S. 727, 733 (1877); 18 U.S.C.S. § 1703.
- (3) 39 C.F.R. § 233.3. See Kerr, *supra* note 1, at 631.
- (4) 442 U.S. 735 (1979). See also *United States v. New York Tel. Co.*, 434 U.S. 159 (1977) (通話内容情報取得についての法規制(後掲註(9))が及ぼすこと判示).
- (5) 389 U.S. 347 (1967).
- (6) Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Title III, § 802, 82 Stat. 197, 212; 18 U.S.C.S. §§ 2510 *et seq.*
- (7) Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, Title III, § 301 (a), 100 Stat. 1848, 1868; 18 U.S.C.S. §§ 3121 *et seq.*
- (8) 18 U.S.C.S. §§ 2510 *et seq.*, amended by Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, Title I, § 101, 100 Stat. 1848, 1851.

- (9) 順探知機器の定義は「a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached」であり、逆探知機器の定義は「a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted」であり、(18 U.S.C.S. § 3127 (3), (4), prior to 2001 amendment)。文言上、特に前者を電話限定的とする。
- (10) U. S. Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2002), at IV-C, available at <http://www.usdoj.gov/criminal/cybercrime/s&manual2002.htm>。その数々数百件程度を参照。See also Carl S. Kaplan, *Concern over Proposed Changes in Internet Surveillance*, N. Y. TIMES, Sept. 21, 2001, at E1. See also Kerr, *supra* note 1, at 634.
- (11) *In re United States*, Cr-00-6091 (N. D. Cal. Nov. 17, 2000), unreported [cited by Kerr, *supra* note 1, at 635].
- (12) *Amended by* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 [*i.e.* USA PATRIOT Act], Pub. L. No. 107-56, Title II, § 216 (c) (2), (3), 115 Stat. 272, 290. 順探知機器の定義は「a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication」であり、逆探知機器の定義は「a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication」であり、修正された (18 U.S.C.S. § 3127 (3), (4))。前掲註(9)の旧定義と比較参照。
- (13) 18 U.S.C.S. § 3123 (a) (3). 同条は、パケット交換データ通信にのみ適用される。
- (14) 従来からテロ事件捜査の場合については、対外諜報監視法 (FISA) に許容規定が存在した。詳しくは岡本・前掲註(1)参照。なお、一般事件対象であった時限措置条項にかからない捜査手法が愛国者法中に規定された例として、他に「告知遅滞捜索 (sneak and peek search)」がある (同法二二二条)。この点につき、拙稿「いわゆる『秘密捜索』について——アメ

リカ愛国法を手がかりとして——」法時七八卷五号六七頁（二〇〇六）参照。

- (15) United States v. Place, 462 U. S. 696 (1983).
- (16) *Kyllo v. United States*, 533 U. S. 27 (2001). 熱画像機器 (thermal imager) とは「赤外線放射——殆ど全ゆる物体が放っているが裸眼では見えないもの——を探知できる」機器である。「この機器は、温もりに比例して放射を画像に変換し、……熱画像を映し出すビデオカメラの如く機能する」(at 29-30)。本件で捜査官は、被告人が大麻栽培用に屋内で強力な照明装置を使用しているとの疑いをもって、公道上の駐車車両から熱画像機器によって被告人宅を調べたところ、車庫屋根と一方壁面が当該建物の他の部分に比べて温かいとの情報を取得した。この情報は、当該住居の搜索令状獲得に際して疎明資料として使用された。
- (17) *United States v. Karo*, 468 U. S. 705 (1984).
- (18) *Kyllo* 判決と *Smith* 判決との整合的理解は、困難である。DRESSLER & MICHAELS, *supra* note 1, at 103; SCHULHOFER②, *supra* note 1, at 90; George C. Thomas III, *Time Travel, Hovcrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment*, 80 NOTRE DAME L. REV. 1451 (2005).
- (19) この点につき詳しくは、拙稿「捜査における人の写真撮影——アメリカ法を中心として——」『光藤景皎先生古稀祝賀論文集(上)』一一一頁（二〇〇一）、成文堂）参照。
- (20) なお加えて、*Smith* 判決は、*United States v. Miller*, 425 U. S. 435 (1976)——銀行顧客がビジネス上の通常の方法で銀行員に「自発的に知らせる」情報にはプライバシーの適法な期待はないと判示した事例——をも援用している。
- (21) 385 U. S. 293 (1967).
- (22) 401 U. S. 745 (1971).
- (23) 昭和二八年一月三〇日内閣法制局一発第八号・郵政大臣官房文書課長宛内閣法制局第一部長回答。仮に二項の「他人の秘密」を一項の「通信の秘密」と区別するとしても、両者ともに憲法上の「通信の秘密」には含まれると考えられる。井上・前掲註(1)二〇七頁。
- (24) 昭和三八年一二月九日内閣法制局一発第二四号・郵政大臣官房電気通信監理官宛内閣法制局第一部長回答。大阪高判昭和四一年二月二六日高刑集一九卷一号五八頁も同旨。

(25) ここでの身代金要求事件等には、強要罪、公務執行妨害、職務強要罪、威力業務妨害、恐喝罪、逮捕監禁罪、略取罪などが想定されており、単なる脅迫は含まれない(幕田英雄『捜査法解説〔第二版〕』一二九頁(二〇〇二)、東京法令)。実務においては、被害者の同意書を徴したうえ電話取扱局長宛「発信元探索協力要請書」(刑事訴訟法第二一三条により現行犯逮捕をするうえで必要につき協力方要請する」と記載)によることとされている(幕田・一二九―一三〇頁)。

(26) 幕田・前掲註(25)一二九―一三〇頁。捜査実務研究会編『実務捜査提要』二九七―二九八頁(一九八〇)、東京法令(部内資料。井上・前掲註(1)一九四頁にて引用)も併せ参照。

(27) 通信傍受法施行前において、検証令状を以て通信内容情報取得を許容した例は僅かながらある(最決平成一一年一月一六日刑集五三卷九号一三二七頁等)が、その際、通信内容自体の検証に先立って検証令状で通信経路情報を取得することは、問題とされていなかった。井上・前掲註(1)二一〇頁。なお、稗田雅洋「通信内容の傍受の可否」『新実例刑事訴訟法Ⅰ』一七頁、三四―三五頁(一九九八、青林書院)も参照。

(28) 内容情報取得と同時にを行う番号探知については、通信傍受法一六条で許容されている。この場合は、通信傍受に付随してこれに実質的に包含され新たな法益侵害というに足りないから、別個に令状を要しないと解されている。三浦守ほか『組織犯罪対策関連三法の解説』五一〇―五一二頁(二〇〇一、法曹会)。

(29) 本註の以下の諸見解はいずれも「一方当事者の同意」のある場合を前提としている。そのうえで、主に「プライバシー期待の乏しさ」に依拠して例外許容する見解として、光藤景皎『刑事訴訟法Ⅰ』一七六頁(二〇〇七、成文堂)、三井誠『刑事手続法(1)』(新版)七三頁(一九九七、有斐閣)、白取祐司「科学捜査と人権」『刑事訴訟法の争点(新版)』七八頁、八〇頁(一九九二)があり、主に「現行犯性」(加えて論者によっては「手段の非代替性」)に依拠して例外許容する見解として、山内一夫「脅迫電話の逆探知」の合憲性」判時三七六号六頁(一九六四)、土本武司『犯罪捜査(部分補訂版)』一三二―一三三頁(一九八七、弘文堂)、藤木英雄ほか『刑事訴訟法入門(第三版)』七九―八一頁(二〇〇〇、有斐閣)(土本)、石丸俊彦ほか『刑事訴訟の実務(上)』(新版)二二七九頁(二〇〇五、新日本法規)(川上拓二)、井戸田侃『刑事訴訟法要説』一一五頁(一九九三、有斐閣)、松尾浩也「鈴木茂嗣編『刑事訴訟法を学ぶ(新版)』一七三頁(一九九三、有斐閣)」「庭山英雄)、阪村幸男「盗聴」熊谷弘ほか編『捜査法大系Ⅲ』一三三九頁、二五五―二五六頁(一九七二、日本評論社)がある。更に、「正当防衛的構成」で許容するもの(田宮裕『刑事訴訟法(新版)』一二五頁(一九九六、有斐閣)(但し、五

十嵐清・田宮裕『名譽とプライバシー』二七四頁（一九六八、有斐閣）では「現行犯の場合には……一種の合理的な緊急行為として」許容、田宮『総合判例研究叢書(16)・刑事訴訟法』三二二頁（一九六五、有斐閣）では「現行犯の場合の緊急捜索・押収とまったく性質の同じ問題」として許容、「一種の防衛行為として」許容するもの（田口守一『刑事訴訟法（第四版補正版）』一〇三頁（二〇〇六、弘文堂）、「正当防衛ないし現行犯的構成によって」許容するもの（鈴木茂嗣『刑事訴訟法（改訂版）』九四頁（一九九〇、青林書院）、「正当防衛的状况・現行犯的状況によりプライバシーの合理的期待が欠ける」として許容するもの（田宮裕編『ホーンブック刑事訴訟法（改訂新版）』一〇九頁（一九九五、北樹出版）（浅田和茂）など、そのニュアンスには若干の違いがみられる。同意録音との関係についても、完全に同視するものやや隔差づけるものがあり、必ずしも一致をみない。

(30) 井上・前掲註(1)二二〇頁、辻裕教「通信・会話の傍受——検察の立場から」三井誠ほか編『新刑事手続Ⅰ』三六七頁、三七七—三七八頁（二〇〇二、悠々社）。

(31) 通信内容情報ではないことと、私人（通信事業者）による情報取得であることを挙げて、一方当事者の同意のみで足りりとする（渡辺咲子『刑事訴訟法講義（第四版）』八四頁（二〇〇七、信山社）、渥美東洋『全訂刑事訴訟法』一三三—一三四頁（二〇〇六、有斐閣））。

(32) 伊丹俊彦編『実例搜索・差押えの実際』一七七頁（一九九五、立花書房）、三浦ほか・前掲註(28)五〇九頁。

(33) 池田修・前田雅英『刑事訴訟法講義（第二版）』一五六頁（二〇〇六、東京大学出版会）。伊丹・前掲註(32)一七七頁、池田弥生「携帯電話の位置探索のための令状請求」判タ一〇九七号二七頁（二〇〇二）、指宿信「ハイテク機器を利用した追尾監視型捜査——ビデオ監視とGPSモニタリングを例に——」『鈴木茂嗣先生古稀祝賀論文集（下）』一六五頁（二〇〇七、成文堂）も参照。

(34) 立法による例外許容基準の明確化を要求するものとして、例えば松尾浩也『刑事訴訟法（上）（新版）』一二九—一三〇頁（二〇〇一、弘文堂）。

※ 本研究は、二〇〇七年度関西大学学術研究助成基金（共同研究）において、研究課題「アメリカ合衆国におけるテロ対策と市民的自由の保護との総合的研究」として研究費を受けたものの成果の一部である。