# サイバー犯罪に対する捜査手法について（三・完）

鈴木一義

はじめに
**第一章**　囮捜査的手法（以上、第一二二巻第七・八号掲載）
**第二章**　潜入捜査（undercover investigation）
**第一節**　サイバー空間における潜入捜査（以上、第一二三巻第一一・一二号掲載）
**第二節**　小　括
**第三章**　通信傍受などの監視手法
**第一節**　物理的監視
**第二節**　電子的監視（electronic surveillance）
**第三節**　小　括
おわりに（以上、本号）

# 第二章　潜入捜査（undercover investigation）

## 第二節　小　　括

一(1)　**第一節**で行った検討を振り返ると、潜入捜査・秘密捜査について、インターネット空間における場合と現実空間における場合とでは、潜入期間面では、前者がそれ程短期間で済む訳ではないために差は余りないであろうが、インターネット上には、行為者の意図を示すようなリアルタイムの詳細な証拠が提示されるなど、捜査官の目に触れ易い情報が多く存するといった点、また、捜査官に対する身体・生命の危険が発生するリスクが相対的に低くなるであろう点などで、現実世界における潜入捜査・秘密捜査の場合とに違いが見られよう。捜査官に対する身体・生命の危険が発生するリスクが低いであろうという点は、捜査活動に対するマネジメントのあり方の違いにも関わって来よう。更に、児童の振りをして犯罪者予備軍に対応しなければならない点で、インターネット上の潜入捜査における捜査官に課される精神的なストレスが高まる面があろう点、演じる人物像の形成の際に文書化に努めておく必要があろう点、自分が企図していたことは妄想であったという抗弁等を犯罪者に許さないようにするために、現実の世界で犯罪行為を犯す意思が明確にある人物にフォーカスして行くべきである点などでも、インターネット空間における場合と現実空間における場合とで違いが見られよう。そして、これらインターネット空間における場合の特徴に関しては、潜入捜査・秘密捜査に関するポリシーを準備することで対応を図ることが有用且つ重要と思われる。

(2)　犯行を予測して、前もって情報を把握して捜査機関の側から積極的に行動を行って行くという邀撃的・積極的

な志向の重要性についても、それに伴うコストと便益の衡量による分析、リスク評価等の重要性を含めて、インターネット空間における潜入捜査の場合と現実空間における潜入捜査の場合とで基本的なアプローチに違いはないであろうが、少なくとも、前者において得られる判断のための諸要素は、後者においても示唆を与えるであろう。そして、サイバー犯罪が国際的な拡がりを持ち、且つ、技術面でも急速に進展している点に鑑み、サイバー犯罪捜査における邀撃的・積極的なアプローチの有用性は確かなものとなっていると言えよう。

二(1)　かかる点を踏まえて、捜査機関に対するポリシーの具体的内容を検討するならば、例えば、総論で、潜入捜査・秘密捜査の目的は証拠収集、そして最終的には犯罪者を有罪にすることにあるといった形で、捜査目的を明確にした上で、潜入捜査は対象とする犯罪の重大性や対象とされる人物の前科・性格に照らして相応なものであること、犯罪が行われたか、行われていることを疑う理由もないのに、オンライン上の潜入捜査は捜索のための手段として用いられてはならないこと等を明記すべきであろう。捜査の最終目的は被疑者・被告人を有罪にすることにある以上、検察官や裁判官に正当と認められるように、潜入捜査活動は相当なものでなければならないからである。そして、潜入捜査活動の運用計画は、充分に練られたものでなければならないであろう。具体的には、捜査活動を通じて捜査官に指針を与えるべく、明確な目的を示し、また、各捜査官の個別の役割とか職務の割当てを詳細に定めることになり、更に、―通常の潜入捜査に比して相対的にウェイトの度合いは高くないにせよ―捜査官の安全にも充分な配慮を行う必要がある。加えて、運用計画は実行前に監督者による審査を受けることとすべきであろう。

(2)　次に、オンライン潜入捜査は、様々な捜査官等が同じ犯罪者に対する類似の捜査活動に関わるため、捜査官は、他の捜査官の存在を認識せぬ儘に非常に危険な情況に晒されることがあるし、当然ながら似たような捜査活動が並行

して行われると、捜査官が協力・協調する場合よりも、非効率で効果が薄くなることにもなりかねない。そこで、捜査官はかかる捜査の抵触・衝突を回避するように努めるべきであり、監督官も適切な告知をするなどして、抵触を回避させるようにすべきである旨規定しておくべきであろう。

(3) 既に触れた点と重なるが、潜入捜査の最終目的が犯罪者を有罪にすることにある以上、当該捜査活動が検察官・裁判官に正当なものと認められる必要がある。そこで、既に触れたように、捜査活動に関して充分な計画が必要であると共に、当該捜査活動が妥当なものでなければならない。かかる意味で、捜査官は潜入捜査活動を始める前に監督官の許可を得る必要がある。また、捜査官は情報提供者や被疑者の監視を行っている他の捜査官のフォローを得つつ、潜入捜査活動の裏付けを確かなものにして行くべきであり、更に当然ながら、各種法規・ガイドラインを遵守しなければならないといった点を定めておくべきであると考える。

(4) そして、かかるオンライン上の潜入捜査活動については、捜査官の長の審査を受ける必要がある。そして、捜査活動に許容出来ない部分が発生した場合には、当該捜査官と協議の上、当該捜査活動を継続すべきか否かについて監督官に速やかに報告すべきであり、監督官にも個々の捜査官の能力を評価することが求められる。その上で、規定された手続に違背した場合には、内部監査部門の審査を受けるべきことになる旨なども定めておくべきことになろう。

三 以上の議論は、主としてアメリカ合衆国などで論じられていることであるが、その内容は、相応の普遍性を有していると考えられ[144]、我が国で潜入捜査を行う場合にも共通して留意すべき内容であると思われる。この点、囮捜査について、我が国ではアメリカ合衆国ほどの規模や数に至っていないと思われる[145]点に鑑みれば、潜入捜査活動においても、その規模と数においてアメリカ合衆国ほどには至っていないと推測することは可能であろう。その意味で、アメ

リカ合衆国の議論をその儘我が国に当て嵌めることには慎重でなければならないが、潜入捜査のメリットを活かしつつ、その弊害を極力抑えて行くためには、以上で触れた内容について認識し、我が国において更に検討を加えて行く意義があると考える。

## 第三章　通信傍受などの監視手法

本章では、サイバー犯罪に対する捜査手法の内で、通信傍受など監視的手法について、主として、当該手法が頻繁に活用されているアメリカ合衆国の動向を素材に検討を加えてみたい。**第一節**では、物理的監視手法[146]、**第二節**では、通信傍受を始めとする電子的監視手法を取り上げる。[147]

### 第一節　物理的監視[148]

一(1)　捜査機関が物理的監視を行う目的は、一方で、被疑者が犯罪を犯した地点を特定したり、それ迄発見されていなかった証拠を収集することにあると共に、他方では被疑者の所在・位置を明らかにすることによって、被疑者の正当なアリバイを証明することにある。更に、例えば、被疑者が児童ポルノのダウンロードのような重大犯罪を行っている点が確認出来たならば、当該被疑者を逮捕するという点も目的となる。物理的監視の場合、一般の通常犯罪の捜査に有用であるけれども、その有用性は同様にサイバー犯罪にも当て嵌まると言える。

そして、かかる物理的監視には、単一の監視であっても、場合によっては数週間といった時間、設備やマンパワー

をかける必要があるため、本来であれば、サイバー犯罪の予防・検挙のためには、コンピュータを操作している被疑者を監視しているのが一番良いのであろう。尤も、現実にそれを実行することは極めて困難であり、時間をかけたからと言って監視活動が奏功するとは限らず、技術やタイミング・運といった要素が結果を左右する。ただ、被疑者の住居・仕事・交友関係・従前の行動などを認識した上で、監視活動について計画を立てて行った方が、時間の浪費を防ぎ、捜査が奏功する可能性を高めるということは言えよう。

(2) 物理的監視には、公然とした監視と隠密裏の監視がある。前者において、犯罪証拠の収集が目的にあることは当然であるが、被疑者に自分が追跡されている点を自覚させることで犯罪行為を抑止しようとの狙いもある。後者は、被疑者の行動に干渉しない儘に、当該行動を監視して情報や証拠を収集することを目的としている。

二(1) 物理的監視の例として、まず、移動手段による監視が最も多用されているものの一つであろう。例えば、自動車による追跡・監視がそれであり、サイバー犯罪捜査として大変な労力が払われることになるが、特に、サイバー犯罪を犯した者がコンピュータの側にいる場合には、有用且つ必要な捜査活動と言えよう。単一の車で追跡すると対象者に見つかり易くなるため、囮の車を使って複数の車で監視するなど、監視のプランを詳細に詰めることが重要な作業となる。そして、かかる追跡手法によって、被疑者が誰と交信していたのか、何をしていたのか、どこを移動していたのか、どの経路を選択したのか等の情報が分かり、このような被疑者の行動から交友関係が特定出来たり、別の情報源が判明したり、捜索令状請求の計画が立てられるようになるなど、サイバー犯罪―それに必ずしも限定される訳ではないが―の捜査に寄与しよう。尤も、自動車による場合、例えば、道路が非常に混雑している時には、追跡する複数相互の車両に充分な注意を払えないため、先頭車両を頻繁に変える訳には行かなくなるし、他方、田舎の場合、

追跡するチームの車両の数が多くなると目立ってしまうという憾みがあるなど、自動車による追跡は周囲の環境に影響を受ける面がある。また、被疑者が喫茶店など建物等に入った場合には、監視する捜査官も自分の足で追跡しなければならなくなるなど被疑者の行動にも左右される面もあろう。

(2) かかる追跡の過程で、被疑者の車両の所有者を合衆国自動車局等に照会することも有用であるとされる。特に、被疑者が運転している自動車の所有者が被疑者の場合は、被疑者特定に重要な意味を持つことになろう。

また、追跡過程で、例えば、被疑者がインターネットカフェのコンピュータに触れた場合などに、当該指紋を取得することも被疑者特定の手法となろう。更に、公共のゴミ置き場に、被疑者が犯罪で用いた物を捨てることもあるが、被疑者を追跡監視しつつ、被疑者が捨てた物を取得すると、犯罪に関わるメールなどが含まれていることもあって、捜査上有用なこともある。

三(1) 次に、自動車による追跡では、捜査官が対象者を肉眼で捕捉しにくい場合には、航空機（小型無人機・ヘリコプター・固定翼の航空機など、種類は様々である）による追跡が有用な監視手段となる。航空機による監視の場合、その高度のため、地上の対象者からは監視されていることが実際上確認出来ず、また、自動車による追跡監視に比して広範囲を容易に捕捉することが可能となる。

(2) 航空機による監視に際しては、ヴィデオカメラ等による記録を行うことも可能であり、赤外線カメラによって昼夜を問わず監視が出来るという利点もある[149]。但し、今後、無人機が安価で利用可能になれば事態は変わって来得るが、航空機を一時間飛ばすのには相当の費用を要するので、当該捜査が非常に重要な案件でないとコスト的に見合わないため、航空機による監視が発動される事例は多くないとは言えよう。また、監視対象となる被疑者が建物の中な

どに入った場合は、空からの監視は困難となるため、自動車による追跡監視や捜査官自身による追跡と組み合わせ、無線機器などで連絡を取り合いつつ、相互に連携して行くことも必要となって来よう。

四(1)　上記で触れたように、航空機による監視と併用されていたカメラによる監視は、合衆国運輸省によって、高速道路、犯罪発生率や交通量が多い地域、交通の流れが一望出来る交差点地域に対象を瞬時に撮影するカメラを設置する形でも実現されている。また、赤信号でも通過する交通法規違反の車両を撮影するカメラも設置されており、多くの場合、これらには回転して撮影する機能や対象物の細部を拡大して撮影する機能等も付加されている。そして、多様なヴィデオとカメラを組み合わせるアプローチは被疑者の監視にとって効率的であり、数週間といった長期間に亘って対象を記録することが出来るヴィデオカメラも存在し、被疑者が取調べの際に、自分がそこにいた乃至いなかったと主張した場所に防犯カメラがあれば、被疑者の主張の真偽が明らかになることもあるから、被疑者のアリバイの裏付けを取るためにも活用することが可能となる。

(2)　これに加えて、民間企業・民間機関においても、業務のセキュリティを担保するため、政府機関が設置する以上に多くの防犯カメラが、デパート・ガソリンスタンド・銀行・喫茶店など様々な場所に設置されており[150]、官民の防犯カメラを組み合わせると、―対象者のプライヴァシー保護を目的とした制約の必要性という点は看過することは出来ないが―公共空間・私的空間の内で非常に大きな領域を捕捉することが出来る。例えば、喫茶店などで被疑者が使用しているコンピュータのモニター画面を確認することが可能な場合もあろう。

(3)　他方、にもかかわらず、官民の防犯カメラを組み合わせても、全ての場所を捕捉出来る訳ではないため、監視の必要性に照らした、特定の目的のための、地域を特定したカメラを捜査官が設置する必要も生じる。かかる特定目

的で設置されるカメラは、特定の被疑者の行動の特定に役立つし、また秘密裏に設置するカメラの方が情況の必要性に応じて電柱その他様々な場所に設置されることになるので、―ここでも被疑者に対するプライヴァシーの問題は重大な課題として残るものの―柔軟な捜査活動を可能にしよう。

(4) 加えて、被疑者の家や車両に秘かに音声受信装置やヴィデオを設置する必要がある場合もある。これに関しては、裁判所による令状承認に加えて、対象者の家屋に秘かに侵入するなどの高度な技能が必要とされよう。

**五** 更に、家屋等のセキュリティのための装置として、ＲＦＩＤチップ（電波で情報を読み取る超小型無線チップ）によって特定の場所へのアクセスに対する承認がプログラムされているカードなどがあるが、被疑者が当該カードを使えば、使用した日時・使用者等が記録されることになるので、当該使用事実が分かれば、結果として被疑者を特定することも可能となる。また、生体認証装置も、使用者の指紋その他の身体的特徴に依拠し、署名とか音声認識といった使用者の行動に照らして、当該個人を特定して行くことになる。そこで、これらの手段によって、被疑者を特定することが出来たり、その行動履歴が明らかになることもある。

## 第二節　電子的監視（electronic surveillance）

電子的監視とは、広くは、捜査機関が電子的乃至機械的装置を用いて、人々の私的活動に関する情報を収集することなどと定義される。[151] 電子的監視には様々な方法があり、例えば、電話線から通話内容を傍受するワイヤタッピング（wiretapping）と傍受装置を設置した上で室外に聞こえて来る会話内容を当該装置により傍受するバッギング（bugging）などがそれに含まれ、オンライン監視は、この内、ワイヤタッピングに類似するとも指摘される。[152] そこで、本節では、

まず従前の通信傍受・電子的監視の発展について振り返り（**第一款**）、次いでその後新たに出現したオンライン監視について検討を加えることとしたい（**第二款**）。そして、その上で、**第三款**では、電子的監視手段の具体例について概観を行う。

### 第一款　従前の通信傍受と対象範囲の拡大

一　従前より、傍受機器による監視は、小型で発見されにくく、遠隔地から秘かに傍受可能であるから、潜入捜査等に比して発動に際して安全であり、設置も容易で費用が抑えられ、また、長期に亘って大量の記録を収集出来るなど強力で効果的な捜査手段として、特に組織犯罪と戦うための武器として、捜査機関はこの採用を支持していた。犯罪者側も傍受機器を用いる以上、捜査機関がこれを使用することは公正上の面からも問題がないと考えていたのである。一九世紀半ばに電信、同世紀後半に電話が発明された後、通信の当事者以外の者が通信回線を介して行われる通信を無断で傍受するという例が既に問題とされていた。この点、かかる捜査機関による傍受の妥当性については、大要、①その危険性に鑑み、許容しない、②一般には認めないが、国家の安全を守ることを目的としてのみ許容する、③国家安全のための捜査に加えて組織犯罪その他重大犯罪捜査のために、充分な安全弁を設けて狭く限定した法があれば許容するという三つの立場に分かれていたが、最終的に立法においては③の立場が採用された。即ち、一九二八年のオルムステッド事件[153]、一九四二年のゴールドマン事件[154]は、捜索・差押に物理的侵入を伴う不法侵害を要件としていたため、有体物への物理的侵入を伴わない電話傍受は捜索・差押に該当せず、従って、令状なき通信傍受は連邦憲法修正第四条の保護を受けられなかった。しかし、この間、連邦及び州の各種の法執行機関が違法な傍受を行っているこ

とが指摘されており、一九六一年のシルバーマン事件で連邦最高裁は有体物要件を変更し[155]、一九六七年のカッツ事件[156]において、連邦最高裁は、触れることが出来ない会話を政府が傍受する行為はプライヴァシーに対する侵害であり、合衆国憲法修正第四条の捜索・差押を構成するとして同条違反を認めて、不法侵害要件・物理的侵害要件を廃した。そして、かかるカッツ事件やバーガー事件連邦最高裁判示[157]を承けて、連邦議会は、従前の法を明確化すべく、一九六八年総合的犯罪防止及び街路の安全に関する法律を制定した（同法の第三編が「ワイヤタッピング及び電子的監視」であり、Title Ⅲと称される[158]）。Title Ⅲは、触れることが出来ない会話について規律し、有体物よりも複雑となり易い面を除去することを企図して、有線及び口頭での通信（内容、存在、会話の意味・趣旨等々）に関するプライヴァシー保護を定め、狭い限定された例外的場合を除いて[159]、連邦・州の捜査官による、電話傍受・電子的監視、傍受内容の第三者への開示、法廷での証拠としての使用を原則として禁止する[160]。

二　当初の通信傍受は、専ら電話による会話内容の傍受であったが、それ自体、首魁の追及などの過程で活用するなど、現在でもサイバー犯罪対策に寄与する。ただ、現在の捜査技術の進歩は口頭会話などの傍受に止まらず、その捕捉する対象物は広範囲に及んでいる[161]。即ち、Title Ⅲは、一九八六年電子通信プライヴァシー法（the Electronic Communications Privacy Act of 1986 ; ECPA）[162]によって「電子的通信」（electronic communications）を保護対象に追加すると改正された[163]。また、愛国者法（単一の法律でなく、連邦法を数百に亘って修正・改正している）によって、傍受のための犯罪リストに、化学兵器に関する犯罪や、テロに関する規定、重罪に該当するコンピュータ詐欺・コンピュータ濫用等が追加されており、且つ、インターネットサービスプロバイダなど、保護されたコンピュータの所有者または管理者から権限を得た者が、不正アクセスをする者の監視が出来るようにするための改正も行われている。更に、愛国者

法は、Title Ⅲのみならず、ＥＣＰＡ[164]、また、ＦＩＳＡ等を改正し、電子的監視権限等を拡大している[165][166]。

三　これらの結果、傍受・電子的監視は、携帯電話を含む電話の傍受に止まらず、傍受のためのソフトウェアを用いること等によって、リアルタイムでテクストメッセージやｅ-メールによるコミュニケーション、インターネット上のチャット等を捕捉するに至っている[167]。プライヴァシーの合理的期待への配慮とのバランスは必要であるものの、傍受・電子的監視は、リアルタイムで被疑者の発した言葉を捕捉するなど、証拠収集において非常に効果的な手段となっていると言えよう。

## 第二款　オンライン監視の有用性とリスク

一　インターネット上の電子的監視であるオンライン監視という手段は、インターネット上のデータ及びその流通や、ブロードバンド通信等の監視などをその内容とし、例えば、捜査機関が、サービスプロバイダに対して携帯電話の加入者の位置情報を提出させるように、裁判所命令を申請する等といった形で行うことが考えられよう。このオンライン監視は、捜査機関にとっては少ないリスクで、安価で信頼出来る遥かに多量の情報を入手出来るという意味で、**第一款**で検討した伝統的な通信傍受よりも、有用で効果的な捜査手段と言えよう。即ち、オンライン監視の方が、電子ネットワークの多くの地点でデータに狙いを付けることが出来るため、対象者の電話に傍受装置をセットアップするなどの手段によって従前の電話によるネットワークを傍受するよりも、文書・画像・映像・音声ファイルなど多量の情報を取得する可能性が高く、また、ソフトウェア（スパイウェアとして知られるソフトウェアは、対象者のオンライン上の行動を継続的に監視し、当該行動に関する情報を秘密裏に収集する）をインストール等しておくなどの手段で対象者のコ

ンピュータに遠方からアクセスしたり、遠方からコンピュータのデータを読み取ることも出来、従前の傍受のように、対象者の住居等に侵入する必要も必ずしもなく、日進月歩の技術発達によりコスト面でも低く済むのである。[168] 他方、これらの利点の裏返しとなるが、オンライン監視は、これによって対象者の生活の全体像を捕捉出来るようになるため、インターネットが通信の主要な形態となっており、You Tube・Twitter・Facebook 等において人々が交友関係を形成している今日において、プライヴァシーの侵害に対しては大きな脅威を与える存在であると言える。[169]

二　従前の傍受の場合、既に触れたように、ワイヤタッピングとバッギング等があり、それらの手段中重複する内容のものもあったが、オンライン監視手段は―相対的にはワイヤタッピングに近いとは言えようが―それよりも多元的と言える。例えば、電話内容の傍受においては両当事者の通話の存在が前提となるが、オンライン監視の場合、e-メールなどではそのような前提はなく、サーバに蓄積されれば済むなど、幾つかの異なった段階や異なった場所に対象が多元的に存在する。

三　いずれにせよ、度重なる法改正においても、オンライン監視の法体系は非常に混沌としていると論じられるところであり、連邦裁判例においても、e-メールや携帯電話等が多用されているにもかかわらず、電子的通信の傍受に対する合衆国憲法修正第四条の要件についてのガイドラインに関して示すことは殆どなく、また、オンライン監視に対する憲法面での異議の提起にも消極的であるとされている。[170] そして、法体系等がクリアな場合であっても、オンライン情報に関するプライヴァシーの保護は低いと評せられている。[171]

## 第三款　電子的監視手段の例

一　本款では、物理的監視との区分が明確でない場合もあるが、電子的監視手段の例を瞥見してみたい。[172]

二(1)　ペン・レジスターや、電子的刺激等を受信して、電子通信が送信される装置に生じる番号を特定する形で、電話の発信源を特定する捕捉・探知装置（Trap and Trace devices）[173]は、電話からの受発信情報やインターネット通信を記録する電子的装置である。ペン・レジスターは発信番号を記録し、捕捉・探知装置は受信番号を記録する。[174]捕捉される情報には、ダイヤルされた電話番号、通話の長さ、e-メールメッセージの発信者・受信者の特定情報等が含まれる（内容迄は捕捉されない）。携帯電話の通話日時・通話期間等は、被疑者の位置情報を示すものとなり得、また、他人でなくて被疑者自身が電話を所有していたという事実を確認出来ることもある。

(2)　また、携帯電話番号が分からなかったり、被疑者が頻繁に携帯電話を変える場合、被疑者の特定が難しくなるが、Triggerfishという携帯電話中継塔（無線基地局）に類似する装置を用いて携帯電話を傍受することで、携帯電話番号・シリアル番号・位置等が明らかになる。Triggerfishは、ペン・レジスターや捕捉・探知装置のための携帯情報を取得することを助けるし、ワイヤタッピングにも寄与する。

(3)　次に、家屋の固定電話に関する情報は、被疑者が家にいたことを示し、被疑者が家にいなかったという主張を論駁する資料になり得る。

(4)　そして、連邦・州毎に歩道上の他人のゴミを収集することの適法性は分かれるが[175]、仮に適法とした場合、当該ゴミの中に被疑者の位置を示す証拠が見出される場合もある。例えば、喫茶店のような無線ネットワークにアクセス出来る場所でのレシート等がそれであり、当該喫茶店の住所や日時等が記録されていれば、或いはまた、捨てられた

レシートから購入物を割り出すことが出来れば、捜査に有用な重要証拠として事件解決の鍵となり得る。

三(1)　携帯電話が受発信をするためには、中継塔（無線基地局）と交信している必要があり[176]、携帯電話のプロバイダーは接続しているログを作成・管理する。そして、中継塔の記録を入手出来れば、ＧＰＳ付きの携帯電話のように、捜査機関は、一定期間、電話の動きを追跡することが可能となる。中継塔から得る位置情報の正確さは、地域・地形・建物・天候・日時等のファクターに左右される[177]。

(2)　そして、中継塔による分析は、物理的監視活動とも連携する。中継塔による分析からは、携帯電話の場所は分かるものの、被疑者が当該携帯電話を持っているか否かは確認出来ない（例えば、被疑者が携帯電話を第三者と共有している場合もあるし、不注意で他人の車両に置き忘れてしまうことなどもある）。それゆえ、他の監視手法等と連携することで、被疑者の所在についての情報を検証することが可能となり、また必要となるのである。

四(1)　例えば、被疑者がレンタルする車にＧＰＳをインストールするとか、生産段階で新しい車両にＧＰＳをインストールするといった形で、被疑者の車にＧＰＳをインストールすることが仮に可能であるならば、当該車両を見失う恐れもなく、継続的に、また遠距離からでも監視が可能となり、情報データの蓄積も出来るようになる。そして、被疑者の有する特定された携帯電話について中継塔による分析を行うことで、手間を省き、被疑者の動静を追跡することが更に出来るようになる。

(2)　高速道路使用料などの自動回収装置によって、被疑者車両の位置情報・運行日時等が明らかになる。また、被疑者の位置の履歴を判断する手段としては、被疑者の運転記録をチェックする方法がある。

五　被疑者の行動を詳細に見ると、被疑者がしばしば訪れる場所は重要な資料となる。そして、当該ジムとかホテル

等において被疑者がメンバーズカードを用いると、当該履歴情報の価値も高くなる。例えば、クレジットカードによって、被疑者の過去の履歴場所が明らかになるし、監視カメラと併用すると、被疑者の履歴は非常に明確となり、被疑者のアリバイの検証にも有効となる。また、被疑者のクレジットカードによる購入をリアルタイムで監視することが出来れば、犯罪の進行情況が明らかになる。更に、例えば、既知のサイバー犯罪者がオープンな無線接続を用いる場所を定期的に訪れているとしたら、それは犯罪のために再び無線接続を用いる際の手掛かりとなろう。

六(1)　インターネットが生活の必須の部分を担うようになって来ると、個人情報もオンラインから広く取得出来るようになり、インターネットを介しての被疑者の監視が容易になると共に効果的となる。潜入捜査の場合と同様となろうが[178]、オンライン上では現在の被疑者の行動や位置が分かるため、オンライン上で被疑者の情報を得ることが重要になる。例えば、ＳＮＳでは、イベント通知などがなされているから、被疑者がそのイベントに参加するということであれば、そのイベントをターゲットに被疑者の監視を行えば良いということとなり、被疑者からは監視されているということも分かりにくくなり、監視の成功率が高まるということになる。

(2)　また、これも潜入捜査の場合と共通しようが、ブログのコメント等を精査すると、犯行の詳細や動機等が読み取れることもあり、加えて写真等も掲載されていて、被疑者やその所在地の特定も可能となるなど、重要な証拠となり得る。そして、オンライン捜索によりＩＰアドレスを入手し、物理的監視による成果等で検証を行えば、サイバー犯罪者の身元を割り出すことも可能となるのである。

七　以上素描したところからも分かるように、電子的監視手段には物理的監視手段との線引きが明確に出来ない場合も多く、電子的監視にウェイトを置いている度合いが相対的に強いに過ぎない場合もある。かかる意味でも、電子的

監視手段・物理的監視手段いずれかに囚われることなく、両方の手法を組み合わせつつ、対象を捕捉して行くというアプローチが有用と言え、現に実践されているものと思われる。

## 第三節　小　括

一　アメリカ合衆国では、組織犯罪者などへの恐れと全体主義社会に向かう恐れという相反するような感情が従前から同居していた。そのため、電子的監視は捜査官にとっては有用な捜査手段であったけれども、プライヴァシー保護を重視する立場からは、隠れて継続的に情報を収集出来る（且つ犯罪活動と関係ない情報を無差別に収集可能である）等といった、既に触れたような電子的監視の特質から、個人情報・通話情報を露見させるなど、従前の捜査手段に比して遥かに個人のプライヴァシーを侵害し、全体主義を招来しかねない等と、懐疑的な目で見られて来た。無論、捜査官も法律に違反する監視には反対しているし、プライヴァシー保護を重視する側も公共の安全を保護するために捜査の必要性に配慮する意味は認めていようから[179]、捜査の必要性とプライヴァシー保護との衡量によって規律を図って行く必要性については認識は共有されていたと言えよう。そして、その衡量の所産として、裁判官が積極的に関与することで、法執行の濫用の危険性からの保護を図るとか、他に捜査手段がない場合に電子的監視の発動が許されるといった要件設定を行う等の方向が考えられた。

この点、オンライン監視を許容するＥＣＰＡについて、政府の解釈は緩やかであり、また、現在生じている通信内容の傍受に対する司法的チェックは機能するものの、それ以外の司法的チェックは限定的であって、Title Ⅲが想定していた本来の通信傍受に比べて、オンライン監視についてはプライヴァシー保護は充分に達成されていないとの評

価もあろうが、これについても裁判所による規律と議会による法改正によってバランスある対応を図って行くことが本則であるように思われる。

二　ただ、翻って考えれば、オンライン監視や電子的監視の規律だけに目を奪われる訳には行かないと考える。第一節で鳥瞰したように、監視手法には物理的な監視もあり、その侵襲性なども電子的監視に比して必ずしも劣るものではない。例えば、物理的監視の例である防犯（ヴィデオ）カメラは、従前のワイヤタッピング（既に触れたように、電子的監視手段の代表例とされている）に比して、対象者の会話のみならず行動全体を明らかにし、且つ継続的に一定期間情報を収集する訳であるから、対象者のプライヴァシー保護の観点からは、防犯カメラの方がワイヤタッピングよりも制約が必要であるとも言えるであろう。無論、既に触れたように、物理的監視と電子的監視の区分も相対的なものに止まり、両手法が併用される場合もあり得るから、物理的監視・電子的監視・オンライン監視の比較に過度に重点を置くことにも大きな意味はないであろうが、逆に言えば、物理的監視の諸手法においても、裁判所による対応と議会による法改正によってバランスある対応を図って行く必要性は些かも減じられることはないということになろう。

三　この点、嘗て、我が国においても、盗聴（通話等傍受）は、対象が特定しにくく、性質上どうしても地引網的性質を有し、その対象の中に正当に保護されるべき未確認の会話が混入せざるを得ず、また、写真撮影の場合と違って、緊急事態でのみ必要とされる訳ではなく、且つ従前の強制処分が予定する枠を超えた広く深いプライヴァシー侵犯の余地を含んでいるだけに、既存の令状の形式に拘泥しない厳格な規制が必要であるから、第一に、それが許容されるためには国民的討議を経た上での立法府による決断を要し、第二に、既存の強制処分には見られない、特に厳しい令

状発付のための要件・手続が予め法定されている必要があるとの見解が有力に主張された[180]。しかし、従前の傍受に見られる①侵襲性、②継続性、③無差別性[181]、④秘密性といった特徴は、監視カメラや、更にオンライン監視・傍受にも同様乃至より以上に当て嵌まると言えよう。例えば、従前の傍受は当事者間の会話を明るみにするけれども、監視カメラ等は対象者の行動そのものを明らかにするし、継続性という意味でも、監視カメラ等は一定期間全体の情報を収集するという意味で、従前の傍受に比べて勝るとも劣る所は少ないであろう。そして、無差別性という点では、監視カメラ等においては、対象者に罪を負わせることとなるような情報のみならず、罪を負わせることとは関係ない情報や、違法行為を行ったと疑う相当な理由がない者の情報をも捕捉することになりかねない。更に、秘密性という点でも、監視カメラ等は今や技術的にも秘密に設置することが可能となっている。傍受・監視カメラ等・オンライン監視に共通するこれらの特徴に鑑みれば、伝統的な傍受に限定することなく、監視手段全体を視野に入れてこれを規律することで、対象者の救済・プライヴァシーの保護を図っていく方向での法的枠組みを重視すべきであり、オンライン監視の規律もかかる観点から検討を深めて行くべきであると考える[182]。

## おわりに

一　以上、サイバー犯罪における囮捜査的手法（第一章）、潜入捜査（第二章）、通信傍受を始めとした監視手法（第三章）について検討して来たが、サイバー空間が捜査の主たる対象領域であるからと言って、現実空間におけるそれら捜査と、基本的に大きな差異はないと言えよう。サイバー犯罪においては、確かにソーシャルメディアが多用され、携帯

電話もそれらにアクセスすべく、犯罪組織等に活用されているものの、それらに対する捜査手法が、通常犯罪に対する手法と大きく異なって来るとは思われない。特に、コンピュータ等を操作している被疑者を物理的乃至電子的に監視しようとする場合には、正に現実空間にいる被疑者をターゲットにしている以上、差異の度合いは一層小さくなるものと考える。

二(1)　ただ、サイバー空間においては、捜査官に対する身体・生命の危険が発生するリスクが現実空間におけるそれよりも低いであろうこと、一方で、現実空間における働き掛けと異なり仮想空間における働き掛けを演じなければならないため、その分、捜査官がメンタル上受けるストレスは高くなり得るであろうこと、物理的に存在することを必ずしも必要とせず、犯罪者は世界中を移動出来、その意味でグローバルな問題を孕み易いこと[183]など、サイバー空間における捜査の特殊性という点は存在する。尤も、この特殊性を踏まえつつ、我が国に対する示唆という観点からは、サイバー空間における米英の捜査手法は、現実空間における捜査手法・サイバー空間における捜査手法双方に対して有益な知見を提供してくれるものと思われる。まず、囮捜査的手法について見るならば、アメリカ合衆国等におけるインターネット上の囮捜査における違法・適法を分ける判断ファクターは、インターネット上のみならず通常空間においても、我が国の裁判例における判断ファクターをより精緻なものにして行くために参照する意義があろうし、私人による囮捜査に関しては、その儘の形かは格別、将来的に我が国においても類似の事例は生じ得るから、そこにおいて展開されている議論は、サイバー空間・現実空間を問わず、我が国にも影響を及ぼすと考えるのが自然であろう[184]。また、サイバー犯罪対応においては、官民の連携が必要とされており[185]、民間分野の活躍する余地が増えるであろうから、囮捜査的手法の領域における、民間の働き掛けと捜査機関の働き掛けとの線引きやジャーナリストに対する

規律等に関する知見は、一定の示唆を与えるものと思われる。

(2) 次に、潜入捜査についても、サイバー空間において得られる、潜入捜査発動のためのコスト・便益の判断過程は、現実空間においても示唆を与えるであろう[186]。特に、我が国においては、潜入捜査自体についての知見が充分に蓄積されているとは言いにくいと思われるため、現実空間・サイバー空間を問わず、アメリカ合衆国などで議論されている上記判断過程・判断要素を参照する意義はあると思われる。また、アメリカ合衆国等においては、オンライン潜入捜査に関して捜査官を規律するポリシーが策定されているが、これも我が国が潜入捜査を行う場合、サイバー空間・現実空間を問わず、示唆するところは大きいと思われる。

(3) 更に、監視的手法については、そもそも、コンピュータ等を操作している被疑者を物理的乃至電子的に監視しようとする場合には、現実空間にいる被疑者をターゲットにしている以上、サイバー空間・現実空間とで差異の度合いが小さい点は、上記で述べた通りである。加えて、従前の傍受に見られる①侵襲性、②継続性、③無差別性、④秘密性といった特徴は、現実空間における監視カメラ等にも当て嵌まり、更にオンライン監視・傍受にも同様乃至より以上に該当すると言えるであろう点も既に見た通りである。ここからは、傍受・監視カメラ等・オンライン監視に共通する特徴に鑑みて、監視手段全体を視野に入れてこれを規律することで、対象者の救済・プライヴァシーの保護を図って行く方向での法的枠組みが求められており、その意味で、現実空間とサイバー空間における、この領域での捜査の規律における重なり合いの度合いがより強まっていると言えよう。

三(1) 以上のように、比較法的知見という点に関しては、我が国では、囮捜査的手法・潜入捜査・監視的手法の多くが、アメリカ合衆国などに比べて多用されているとは言えないため[187]、サイバー空間におけるそれら手法に関する知見

は、サイバー空間・現実空間いずれに対しても、重要な示唆を我が国に与えるものと思われる。

(2) 他方、現実空間における捜査とサイバー空間における捜査との関係という点を考えるならば、既に触れたように、両者に根本的な違いが多く見られるとは思えず、両者は表裏一体の関係と捉えることにも合理性があるように感じられるが、翻って、サイバー空間における物理的監視手段（これは現実空間における物理的監視手段とオーヴァラップするところが大きいと思われる）と電子的監視手段、更にオンライン監視手段とで、捜査に対する規律の面で重なり合うべきところが大きいと考えられる点に鑑みても、サイバー空間における規律と、現実空間における規律を相互にフィードバックさせながら、サイバー空間・現実空間の違いに過度に囚われることなく、捜査の必要性とプライヴァシーなど人権の保護のバランスに配慮した規律の枠組みを構築して行く必要性が大きいように思われる。(188)

**四** 特に、サイバー空間においては、犯行を予側して、前もって情報を把握しつつ、捜査機関の側から積極的・邀撃的（proactive）な働き掛けを行って行く必要性も高いであろう。しかし、邀撃的捜査の必要性は、例えば、振り込め詐欺事犯のように、現実空間においても高まっている。サイバー空間における囮捜査的手法・潜入捜査・通信傍受などの監視手法に現れる邀撃的性質は、現実空間におけるそれら手法に見られる邀撃的性質の高まりを予感させるものであるとも言えよう。

(144) イギリスにおいても、インターネット上の秘密捜査官の配置に関して、秘密捜査官の効果的且つ効率的な活用のためには、オンライン上の秘密捜査活動に際して、主任捜査官や上官の承認を事前に得た行為に焦点を当てるべきであるとか、秘密捜査官がオンライン上の行動を監視したり、これに参加したりする場合には事前の許可を得ておくことが必要である、あらゆる秘密活動はその儘の形で文書化しておき、電子フォーマットで保管しておくべきである、秘密捜査官は判例法や法律を遵

守すべきである、コンピュータに基づく電磁的証拠に関する監査記録等の作成・保管等が必要であるが、かかる過程を独立した第三者が検証出来るようにしておくべきであるといった点が謳われている（See e. g. Barrie Sheldon, Paul Wright, *Policing and Technology*, 2010, Learning Matters Ltd. 62-3）。個々の指摘は内容的に新奇なものでないという点も理由になろうが、イギリスでもアメリカ合衆国と同様の問題意識が持たれている点には留意すべきであろう。

(145) **第一章第二節第三款**参照。但し、平成二八年三月三日、札幌地方裁判所において、犯意誘発型の囮捜査が認定された（毎日新聞平成二八年三月四日朝刊など参照）点に照らして、違法な囮捜査が想定以上に存在しているのではないかという可能性にも留意する必要があろう。

(146) 物理的監視手法の例として、See e. g. Brett S havers, *Placing the Suspect Behind the Keyboard*, supra at. 57–.

(147) 物理的監視の例である追跡の過程で、無線傍受等を行うこともあるため、物理的監視と電子的監視が峻別出来る訳ではない。インターネットでの電子監視が監視カメラシステム等と独立に存在すると断じることは難しく、管制手段の集合の一部と捉えるべきとするものとして、例えば、Michael McGuire, "Online surveillance and personal liberty", *Handbook of Internet Crime*, edited by Yvonne Jewkes and Majid Yar, supra at. 492.

(148) 本監視手法は、我が国の追跡型捜査手法において用いられる諸手法と相当程度重なって来ると思われる。追跡型捜査手法について、鈴木一義「無人機（unmanned aerial vehicle）の研究（三）」『法学新報』第一二一巻第五・六号（平成二六年）第三章第三節など参照。

(149) 例えば、無人機が赤外線カメラ等を搭載していることについては、鈴木一義「無人機（unmanned aerial vehicle）の研究（一）」『法学新報』第一二〇巻第三・四号（平成二五年）第一章、井上孝司『ドローンの世紀』（平成二七年　中央公論新社）七八頁以下、白鳥敬『無人兵器』（平成二八年　河出書房新社）二四頁、三三頁など。

(150) See e. g. Darryl K. Brown, *Free Market Criminal Justice*, 2016, Oxford University Press, New York, 178.

(151) See e. g, Susan Freiwald, "ONLINE SURVEILLANCE : REMEMBERING THE LESSONS OF THE WIRETAP ACT", 56 Ala. L. Rev. 9–, 15 (2004–2005).

(152) See e. g, Susan Freiwald, "ONLINE SURVEILLANCE : REMEMBERING THE LESSONS OF THE WIRETAP ACT", supra at 21.

(153) Olmstead v. United States, 277U. S. 438(1928).

(154) Goldman v. United States, 316U. S. 129(1942).

(155) Silverman v. United States, 365U. S. 505(1961). 隣家との境界壁内に差し込まれた釘状の細長い傍受マイクが壁の話者（被疑者）側にごく僅かに侵入していた場合に捜索とされ、これにより、合衆国憲法修正第四条に関する有体物・財産権侵入概念は瓦解しつつあったとされる。

(156) Katz v. United States, 389U. S. 347(1967).

(157) Berger v. New York, 388U. S. 41(1967). 連邦最高裁は、物理的侵入を伴う事案であったにもかかわらず、会話も合衆国憲法修正第四条の保護の範囲内にあり、それを捕捉するために電子的機器を用いることは捜索に該当すると解して、修正第四条の適用を根拠付けた。そして、連邦最高裁は、相当な理由がある場合にのみ監視を認める裁判所命令を要求し、場所や対象物の特定、傍受が必要以上に亘らないこと等を示唆し、適切な司法監督について強調した。更に、バーガー判決は州法の欠点について判示しており、これが議会が総合的犯罪防止及び街路の安全に関する法律第三編を制定することに寄与した。

(158) 裁判例・立法の経緯については、CharlesDoyle, *Privacy : An Overview of the Electronic Communications Privacy Act*, 2012, Congressional Research Service[–] ; Christopher R. Brennan, "Katz Cradle : Holding On to Fourth Amendment Parity in an Age of Evolving Electronic Communication" William & Mary Law Review 53 (5) 1797–1800–（2012）, 井上正仁『捜査手段としての通信・会話の傍受』（平成九年　有斐閣）六頁以下、二七頁以下、石井夏生利『個人情報保護法の現在と未来』（平成二六年　勁草書房）「第五章　米国の国家安全と監視強化」、鈴木一義「無人機（unmanned aerial vehicle）の研究（二）」『法学新報』第一二一巻第一・二号（平成二六年）第二章第一節、ジョシュア・ドレスラー&アラン・C・ミカエル［指宿信　監訳］『アメリカ捜査法』（平成二六年　レクシスネクシス・ジャパン）九六頁以下などを参照。

(159) Berger 判決を承けて、正当理由を要求した。また、傍受の最小化、企図する情報が取得されたら傍受はすぐに止める、事後的にで良いが対象者に通知する等について規律した（多くの傍受は対象者に知られることなく進められるが、事後の通知によって秘密性とのバランスを図る）。従前の捜索と比べると電子的監視の規律はずっと厳しいもので、電子的監視は他の捜査手段が不可能な場合の最後の手段とされた。

(160) 猶、Title Ⅲが通常の刑事犯罪における通信傍受等を対象とするのに対して、ウォーターゲート事件を承けて一九七八年に

成立したＦＩＳＡ（外国諜報監視法）は外国諜報情報の監視等を規律する。See e. g., Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein and Peter Swire, *The NSA Report*, 2013, Princeton University Press, New Jersey, 20–, 82–.

(161) 主として、石井夏生利・前掲書『個人情報保護法の現在と未来』二五九頁以下参照。

(162) ＥＣＰＡは、電話のワイヤタッピング、ペン・レジスターから今日の台頭する諸技術迄、全ての電子的通信を政府が監視する際の立法の枠組みを提示するものであると言われる。そして、ＥＣＰＡは三つの部分から成る。即ち、①通話のみの傍受を保護していたTitle Ⅲのアップデート・改正、②蓄積されている通信に関する法律（the Stored Communications Act）、③ペン・レジスターや捕捉・探知装置の設置・使用を規律する条項である。

(163) ファクシミリやコンピュータ通信等を捕捉する。ＥＣＰＡ制定時においては、電子的通信は揺籃期であり、ワールド・ワイド・ウェブは未発達であったし、インターネットも一般には使用されることは少なく、ｅ－メールを使う人も少数に限られていた（ＥＣＰＡ制定時は、Title Ⅲ制定時に比べ、科学技術の進展に伴うプライヴァシー侵害等に関する社会の関心も弱かった）。そこで、電子的通信の進展のために、議会は、電信や口頭会話に加えて、電子的通信を定めた。そして、その後、ＥＣＰＡは、一九九四年の法執行のための通信援助法（the Communications Assistance for Law Enforcement Act [CALEA]）により改正され、法執行機関がデジタルネットワークを継続的に傍受する能力を通信サービスプロバイダが確保するように規定し、また、二〇〇一年九月一一日同時多発テロを契機に制定された愛国者法（the USA PATRIOT ACT）は法執行機関員に新しい道具を提供した。尤も、これら改正によってＥＣＰＡの基準・枠組みに大きな変更はなされておらず、オンライン監視についてはＥＣＰＡのアップデートは不充分で、解釈論の余地が大きいとも評されている。Susan Freiwald, "ONLINE SURVEILLANCE: REMEMBERING THE LESSONS OF THE WIRETAP ACT", supra at 41–2, 53–, 74–.

(164) ＥＣＰＡは、捜査官が取得しようとする、対象者の電子的コミュニケーションの情報の量・態様に応じて、令状その他必要書類のレヴェルを分けている。例えば、氏名・住所・期間といった加入者の基本的情報については強制令状（subpoena）、業務・取引情報は裁判所命令（court order）、ｅ–メールメッセージの内容については捜索令状（search warrant）が必要となる。捜索令状が一番高度の要件を必要とし、裁判所命令がそれに次ぐ。そして、裁判所命令があれば強制令状によって得ることが可能な情報をも得ることが出来るというように、上位の令状等は下位の令状等に取って替わることが出来るという

形での上下関係があるとされる。See e. g., Robert Moore, *CYBERCRIME*, 2nd ed., supra at 181–. See also, Susan Freiwald, "ONLINE SURVEILLANCE : REMEMBERING THE LESSONS OF THE WIRETAP ACT", supra at 46–［ＥＣＰＡは、傍受の対象情報を、まず、①現に行われている通信内容、②通信・通話の内容そのものでない付随的情報（電話番号・電子アドレス情報、電話が継続したか否か、期間等）に分けるが、①②の境界は曖昧であり、例えば、ペン・レジスターは対象者の電話番号を単に取得するものとして、②に該当するとする。また、ＥＣＰＡは、リアルタイムの電子情報が保管されている情報か否かで、保護の程度に差を付けるとする。次に、ＥＣＰＡは、③保存・蓄積されている内容情報の取得と、④保存・蓄積されている付随的情報を区分し、③については、一八〇日以内の保存内容を合衆国憲法修正第四条で保護し、長期的に保存される内容情報の方が保護の程度が低いと捉える（そして、④については長期的保存についての裁判所命令か令状があれば、捜査機関による取得を可能とする）。更に、⑤ワールド・ワイド・ウェブを使う時に生じる情報をウェブ・トラフィック・データと位置付ける］.

(165) 尤も、既に触れた点と重なるが、愛国者法は、テロに対する捜査の取扱に大きな変化を与え、アメリカ合衆国の市民の自由（オンライン上のプライヴァシー保護の低減を含む）に影響を与えたものの（二〇〇一年九月一一日テロ発生以降のアメリカ合衆国における監視活動強化の流れについては、例えば、ジュリア・アングウィン［三浦和子　訳］『ドラグネット監視社会』［平成二七年　祥伝社（原著　二〇一四年）三六頁以下など参照］）、電子的監視・オンライン監視について、その法的枠組み等に劇的な変化を与えるものではないと評される。Susan Freiwald, "ONLINE SURVEILLANCE : REMEMBERING THE LESSONS OF THE WIRETAP ACT", supra at 67–; Orin S. Kerr, "Internet Surveillance Law after the USA PATRIOT ACT : The Big Brother that isn't" 97 Northwestern University L. R. 607, 608, 673 (2003).

(166) そして、二〇一五年には、二〇一五年サイバーセキュリティ法（the Cybersecurity Act of 2015）が制定された。本法の評価は未だ必ずしも明確でないが、従前よりも、ネットワークのオペレーターに監視等についての広い権限を与える可能性があると評されている。See e. g. Orin Kerr, "How does the Cybersecurity Act of 2015 change the Internet surveillance laws?", the Washington Post, December 24, 2015.

(167) e–メールが傍受の対象として優れているとは一概に言えず、暗号化されると傍受しにくいので、インターネット上でリアルタイムで音声上のコミュニケーションを行うスカイプ等の方が傍受対象として優れていると評されることもある（尤も、

スカイプも暗号化されれば傍受は難しくなろうが）。See e. g., Michael McGuire, “Online surveillance and personal liberty”, supra at 502.

(168) 特に、携帯電話などモバイルにおけるインターネット技術の進展は電子的監視・オンライン監視を容易にすることが多いであろう。ただ、一方で、個々の通信の内容を追跡等するには時間などを要するため、効果的な監視が困難になる面もあるであろう。

(169) ECPAにおいては、一九八六年以降重要な定義の改正はなされておらず、ワールド・ワイド・ウェブやインターネットを捕捉出来ていない。また、どの活動にどの法規を適用するかについても殆ど実施不可能となって来ており、新たなオンライン監視活動の中には法規制を免れるものも出て来ていると言えよう。See e. g., Susan Freiwald, “ONLINE SURVEILLANCE : REMEMBERING THE LESSONS OF THE WIRETAP ACT”, supra at 42–, 52– ; Christopher R. Brennan, “Katz Cradle : Holding On to Fourth Amendment Parity in an Age of Evolving Electronic Communication”, supra at 1810.

(170) その原因としては、ECPAに排除法則による救済が規定されていないこと等が指摘されている。Susan Freiwald, “CELL PHONE LOCATION DATA AND THE FOURTH AMENDMENT : A QUESTION OF LAW, NOT FACT” 70 Md. L. Rev. 681, 681–2(2011).

(171) Susan Freiwald, “ONLINE SURVEILLANCE : REMEMBERING THE LESSONS OF THE WIRETAP ACT”, supra at 52.

(172) 電子的監視の最も知られた例はワイヤタッピングであるとするものとして、See e. g., Brett Shavers, *Placing the Suspect Behind the Keyboard*, supra at 70. 電子的監視手段の例として、Id., at 70–, ジョシュア・ドレスラー＆アラン・C・ミカエル［指宿信　監訳］・前掲書『アメリカ捜査法』一二三頁以下、渥美東洋編『米国刑事判例の動向　Ⅳ』（平成二四年　中央大学出版部）二八五頁以下など参照。

(173) これらは、ECPAにおいても規律されており、また、愛国者法で適用範囲がｅ－メール等に関する情報の送り手・受け手にも拡大されている。

(174) ペン・レジスタートという名称で、ペン・レジスターと捕捉・探知装置の両方を包含することもある。

(175) 連邦最高裁は、当該事案においては修正第四条に違背しないとした。California v. Greenwood, 486U. S. 35(1988). 鈴木一義・

前掲「無人機（unmanned aerial vehicle）の研究（二）」五六頁以下など参照。州法に関する裁判例として、ジョシュア・ドレスラー&アラン・C・ミカエル［指宿信　監訳］・前掲書『アメリカ捜査法』一四五―六頁など。

(176) 携帯電話端末と中継塔、無線ネットワーク制御装置との遣り取りについては、例えば、中嶋信生・有田武美『携帯電話はなぜつながるのか』（平成一九年　日経BP社）第二章・第三章など。

(177) 携帯電話の中継塔を使って位置を割り出す手法では障害物によって支障が生じることがあるので、Wi-Fiネットワークによって携帯電話の位置を推定する手法も採られるようになった。ジュリア・アングウィン［三浦和子　訳］・前掲書『ドラグネット　監視社会』二一四頁以下など。また、基地局を偽装する装置（スティングレイ）を巡る近時の情況について、指宿信「偽装携帯基地局を用いた通信傍受」『法学セミナー』二〇一五年一一月号一頁以下。

(178) **第二章第一節五**など参照。

(179) 個人の自由と安全との関係については、大石眞『権利保障の諸相』（平成二六年　三省堂）二九頁以下、四四頁など。

(180) 田宮裕『刑事訴訟法［新版］』（平成八年　有斐閣）一二二―三頁。田宮裕編著『刑事訴訟法Ⅰ』（昭和五〇年　有斐閣）一四七―八頁〔田宮〕をも参照。

(181) 過去の通信の捕捉よりも、将来の通信を捕捉しようとする方が、無差別性は強まろう。See e. g. Orin S. Kerr, "Internet Surveillance Law after the USA PATRIOT ACT : The Big Brother that isn't", supra at 616-.

(182) オンライン監視についても、プライヴァシー侵襲において防犯カメラと類似する部分が見出せるから、プライヴァシーを保護する枠組みを、インターネットの領域においても拡張して行くような視点が必要とされよう。

(183) 例えば、インターネットのユーザーは一国のみに止まるものではないため、インターネットに対する法規の適用も一国のみに限定されるものではなく、越境的になっていると言えよう。See e. g. Orin S. Kerr, "The Fourth Amendment and the Global Internet" 67Stanford L. R. 285, 287- (2015).

(184) **第一章第二節第三款**など参照。

(185) **第一章第一節一**など参照。

(186) **第二章第二節**など参照。

(187) 尤も、監視カメラ等については、我が国でも多くの地域で活用されているとは言えよう。鈴木一義・前掲「無人機（unmanned

aerial vehicle）の研究（三）」第三章第二節四など参照。

（188）　はじめに　でも触れたように、サイバー犯罪以外の一般的な事案における捜査手法の課題は、この辺りにも現れて来るように考えられる。

（日本比較法研究所嘱託研究員）