第２回　匿名・流動型犯罪グループによる犯罪被害対策のための技術的措置に関する有識者検討会
議事概要

１　開催日時

令和８年８月 26 日（水）午後１時 00 分から午後３時 15 分まで

２　開催方法

オンライン

３　出席者

(1)　有識者委員

上沼　紫野　ＬＭ虎ノ門南法律事務所　弁護士
上原哲太郎　立命館大学情報理工学部教授
金子　正志　金子正志法律事務所　弁護士
川出　敏裕　東京大学大学院法学政治学研究科教授
沢田登志子　一般社団法人ＥＣネットワーク理事
宍戸　常寿　東京大学大学院法学政治学研究科教授
成瀬　　剛　東京大学大学院法学政治学研究科教授
野口貴公美　一橋大学大学院法学研究科教授
星　周一郎　東京都立大学法学部教授

(2)　警察庁

森元　良幸　官房長
土屋　暁胤　総括審議官
中山　卓映　刑事局捜査支援分析管理官

４　議事概要

(1)　事務局説明

事務局から英国・ドイツの類似制度、補足的な論点整理並びに第１回検討会での御意見の整理及び当該整理に基づく制度・運用イメージについて説明があった。

(2)　自由討議

(1)の説明を踏まえた有識者委員からの主な意見（順不同）は以下のとおりであった。

ア　英国・ドイツの類似制度について

○　イギリスの調査権限法に規定されている特定機器干渉令状と、ドイツの刑事訴訟法に規定されているオンライン捜索は、いずれも、法執行機関が「遠隔」から対象者の端末にアクセスして、当該端末内の情報を「解析」する点で、本検討会が導入しようとしている遠隔解析と共通する側面を有している。

しかし、イギリスの特定機器干渉令状とドイツのオンライン捜索には、処分の継続性の有無という点で差異がある。すなわち、イギリスの特定機器干

渉令状は、調査権限法 99 条 6 項に規定されているように、対象端末内に既に保存されているデータを一回的に取得する措置であって、リアルタイムで流れてくるデータを継続的に捕捉することは認められていないが、ドイツのオンライン捜索は、刑事訴訟法 100e 条 2 項に基づいて、裁判所の命令に 1 か月以内の期間が定められ、その期間を更新することも予定されていることから分かるように、端末内に既に保存されているデータのみならず、リアルタイムで流れてくるデータを継続的に捕捉することをも許容している。

資料４の３頁の表において、ドイツのオンライン捜索の要件は、イギリスの特定機器干渉令状の要件と比較して、必要性や対象犯罪の観点で、より厳格なものとなっているが、これは、ドイツのオンライン捜索が端末からの継続的な情報取得を許容する措置であることによるものと思われる。

本検討会で導入を検討中の遠隔解析は、イギリスの特定機器干渉令状と同様に、あくまで対象端末内に既に保存されているデータを一回的に取得する処分であって、継続性を有しないので、ドイツのオンライン捜索ほど厳格な要件を設ける必要はないと考える。

○　英国とドイツの類似制度からの示唆として、検討中の遠隔解析は、刑事手続と明確に区分できる行政手続ではないといえるのではないか。遠隔解析の目的である犯罪の予防はいわゆる行政警察活動であるが、犯罪の取締りという司法警察活動と連続的に捉えることが可能である。したがって、遠隔解析を行政手続と定めた場合であっても、刑事手続と完全に切り離すべきではないのではないか。

我が国の法制においては、両者を連続的に法定することは難しいかもしれないが、要件の定め方、必要な手続等については、刑事訴訟法を参考に検討を進めるべきであろう。

○　英国とドイツの類似制度の紹介は、諸外国がどのような点に配慮して制度設計をしているのかが明らかとなり、大変参考になった。諸外国の制度をそのまま我が国の法制度にあてはめる必要はないと思うが、その考慮要素は今回の検討においても参考になると思う。

イ　補足的な論点整理について

(ｱ)　「措置の継続性」をめぐる考え方

○　同一の事象について令状の執行を繰り返して行えるかという論点について、現行の刑事訴訟法上の整理では、身体の拘束を伴う令状は、原則として一回限りの執行しか認められないが、捜索差押えについては、捜索差押え後に必要が生じた場合には、令状を再度請求し、裁判官の許可を得て、再度これを行うことができるものとされている。

これを踏まえると、遠隔解析を実施したところ、例えば「案件の詳細は明日連絡します」といったやり取りがあった場合等、近い将来に必要な情報が当該端末に記録される蓋然性が高い状況が判明し、新たな遠隔解析の実施の必要性が認められる場合には、再度裁判官の許可を得た上でその内

容を把握することも、憲法第 31 条及び第 35 条との関係で許容される。

○　法的な継続性のない処分と整理されている捜索差押え等においても、一定時間に及ぶことは目的達成のために必要な限度でのみ認められている。平成 19 年の最高裁判決において、捜索差押え中に届けられた物についても捜索差押許可状の効果は及ぶとされ、当該物を差し押さえることは認められると解されていることを踏まえれば、継続的な情報取得のための措置としないものとして検討する遠隔解析において、その実施中に新たに記録された情報を取得することは、憲法第 31 条及び第 35 条との関係で許容されると考えられる。

なお、幅広く情報を取得しようと、遠隔解析を必要以上に長時間実施することは、権限の濫用であり、許されないだろう。

(ｲ)　捜索に伴う「知得」等に関する考え方

○　刑事手続において、警察が被疑者宅の捜索・差押えを実施する場合には、被疑者宅に存在する物件が差し押さえるべき物に該当するか否かを判断するという目的に必要な限度で、書類の内容や室内の状況等の情報を知得することができ、当該物件が可視性・可読性のないＵＳＢメモリ等の電磁的記録媒体である場合には、当該記録媒体に保存されている電磁的記録を可読化し、モニターに投影するなどの必要な処分をすることもできる。ただ、捜索に必要な限度を超えて、被疑者宅にある全ての物や文書の内容等を詳細に撮影・記録することは、別途の権利侵害を構成するため、許容されない。

これが現在の刑事訴訟法の規律であり、憲法第 35 条の下で警察に認められている権限の範囲であることを踏まえれば、導入を検討中の遠隔解析に基づく情報の複写・取得においても、刑事訴訟法の必要な処分に相当する行為を法定することにより、取得対象情報を探し選別するという目的に必要な限度で、対象端末内の情報を一時的に複写し、これらを広く知得することは許容されると考えられる。他方、選別を行った結果として、取得すべき対象に含まれないと判断された情報については、警察がこれを保有し続けることは許されず、前回の会議でも御指摘があったように、確実に消去することが必要になるのではないか。

○　我が国の刑事訴訟法には、米国のプレイン・ビュー法理に相当する規定、すなわち、無令状での緊急差押えを認める規定は設けられていないため、警察が捜索差押えの現場において、令状発付の根拠となった被疑事実とは別の犯罪に関する証拠を発見した場合には、当初の捜索差押許可状とは別の法的根拠に基づいて差押えを実施する必要がある。例えば、発見した物件が規制薬物等の禁制品であれば、禁制品所持の事実に基づいて被疑者を現行犯逮捕し、当該逮捕に基づいて無令状で禁制品を差し押さえることが考えられるほか、別の犯罪を被疑事実として当該物件の差押令状を裁判所に請求し、当該令状の発付を受けて、差し押さえることも考えられる。

これが現在の刑事訴訟法の規律であることからすれば、警察が遠隔解析

を実施する過程で、対象端末内において盗撮画像や児童ポルノ画像など他の犯罪への関与を示すデータを発見したとしても、そのことだけを理由として、直ちにそのデータを保全することは許されないという結論になると思われる。

○　刑事訴訟法に規定されているリモートアクセスは、警察がパソコン等の電子計算機を物理的に差し押さえるに当たり、当該パソコンとオンラインで接続されたサーバ内に保存されているデータをダウンロードして取得するための特別な措置を法定したものである。被疑事実に関連するデータは、パソコンの中だけでなく、オンラインで接続されたクラウド等にも保存されていることが考えられるため、警察がパソコンを差し押さえる際には、クラウド等に保存されているデータも一緒に差し押さえる必要性が認められる。

しかし、警察がオンラインを通じてサーバ内に保存されているデータをダウンロードする行為は、捜索現場にあるパソコン等を物理的に差し押さえる行為とは、処分の対象を異にし、その性質も大きく異なるため、別途の裁判官の許可を明示的に得るという法律上の整理になっている。

今回導入を検討している遠隔解析においても、オンラインで接続されたクラウド等に保存されているデータを取得・解析する必要性が認められる場合は当然あると思われる。もっとも、パソコン等の物理的な差押えを前提としつつ、リモートアクセスというオンライン上の捜査権限を新たに組み込んだ刑事訴訟法と異なり、遠隔解析は元々オンラインで実施する措置として立法化されるため、当該クラウドサーバに対して改めて遠隔解析を行うというだけであれば、リモートアクセスのような別途の法律上の規定を設ける必要はなく、実務の運用で対応できるのではないか。

ただし、警察が遠隔解析により重大犯罪に用いられているクラウドサーバの存在やＩＤ・パスワード等の接続方法を把握したとしても、発付済みの許可状が当該クラウドサーバへの接続を具体的に許容するものとなっていない場合には、クラウドサーバへの遠隔解析を直ちに実施することはできない。当該クラウドサーバは、当初の遠隔解析の対象端末とは異なる処分対象であると整理されるため、別途、クラウドサーバに対する裁判官の許可状を得たうえで、遠隔解析を行う必要がある。

(ｳ)　「秘匿性」と「匿名性」

○　「秘匿性」と「匿名性」の相違については、サイバーセキュリティにおけるコンフィデンシャリティ等の文脈では重要な意味を持つかもしれないが、今般の立法措置に係る議論においては、打破されるべき対象としての「秘匿性」と「匿名性」は必ずしも法的に峻別する必要はなく、「どのような情報が必要であり、遠隔解析を用いなければ速やかに情報を取得することが困難であるのか」という措置の実施要件側から整理すればよいのではないか。

(ｴ)　対象端末が海外に所在している場合の考え方

○　現行刑事訴訟法の規定の中には、リモートアクセスのように、運用によっては当然に国外に所在するサーバ等への影響が発生し得る手続も含まれているが、その場合に我が国の執行管轄権の行使が国際法上許容されるか否かは、運用の問題として位置付けられており、法律の規定において整理するという方針は取られていない。遠隔解析を創設するに当たっても、このような立法の在り方に倣うことが適切であろう。

そのため、遠隔解析の対象端末が海外に所在している場合に国際法上どのように整理するかについては、後日、事務局から説明がなされるとのことであるが、遠隔解析の立法の在り方そのものを検討する上では、この問題はひとまず直接の影響を及ぼさないものと考えて、議論を進めて良いと思う。

○　我が国が遠隔解析を行う場合だけではなく、我が国に存在する端末が他国からの遠隔解析の対象となる可能性も考えられることを踏まえ、国際法上の執行管轄権の整理はお願いしたい。

ウ　第１回検討会での御意見の整理及び当該整理に基づく制度・運用イメージについて

(ｱ)　基本的な制度の在り方

○　遠隔解析は、継続性がないものの、スマートフォンを密行的に解析するため、要件の一つである「犯罪被害が発生するおそれ」について、実務への影響がないのであれば、「十分な理由」を要件として設けてもよいのではないか。

○　刑事訴訟法の世界において、要件について「十分な理由」と定められているのは、現場の警察官が裁判所による令状なくして身柄拘束ができる緊急逮捕等であり、かなり高い嫌疑が必要となることを意味する。他方で、令状を取得して逮捕する通常逮捕の要件は「相当な理由」であって、嫌疑は低くなり、差押えについていえば「罪を犯したと思料」と、「相当な理由」よりも更に低い嫌疑で足りる要件が定められている。このことからも、遠隔解析の要件については「犯罪被害が発生するおそれ」で足り、「十分な理由」まで必要とするのは均衡を失すると解するのが適当ではないか。

○　一国民としては、犯罪を憎むが、犯罪グループの構成員であると誤認される、又は仕立て上げられることは恐ろしい。他方、取りこぼすリスクを考えれば、「犯罪被害が発生するおそれ」について、過度に高い見込みを求めるのは適切でないことについては同意する。だからこそ、事後の適正性担保手続が重要となる。

○　基本的な制度・運用の在り方を検討するに際しては、遠隔解析という情報収集活動は被害防止のために行うものであることを踏まえ、警察法第２条を具体化する形で被害防止責務を具体化すること、「専門的知見を有する」警察官が措置を実施すること、裁判所が要件充足性を審査し、実施に際しては裁判所の許可が必要とされていることの３点が特に重要であり、不要

な情報については削除することが不可欠であると思われる。

○　遠隔解析の対象となる端末の特定については、慎重さが求められる。

また、技術的に誤った措置がとられることのないようにするため、遠隔解析の実施に当たる警察官について、専門的知見を有する者に限定する方向性については、維持していただきたい。

○　遠隔解析の実施手法については、脆弱性などを使わざるを得ない場面があると思う。被害防止措置のために国民の安全を脅かしているのかと言われないような運用を担保するべき。

○　刑事訴訟法は既に発生した、取り返しのつかない状態になった犯罪の捜査について規定するものであるため、手続に重点が置かれているものであると思う。他方で、遠隔解析はこれから発生する可能性のある犯罪による被害を未然に防止するための措置であることから、要件や手続を検討する際にはこの差異について留意する必要があるのではないか。

○　機微な情報が保存されているスマートフォン等にアクセスする遠隔解析を行うためには、当該対象端末から必要な情報を取得できる蓋然性が高いことが必要となるのではないか。また、不必要な情報を無制限に取得できないようにするためにも、対象端末の特定や不要な情報の削除は特に重要になると思う。

○　遠隔解析を継続的な処分として実施できないようにするためにも、時間制限を設けるといったことも考えられるのではないか。

○　遠隔解析を実施する者は、専門的知見を有する警察官に限定される方向性だが、遠隔解析が飽くまでも被害防止のために行われるものであるということをより明確にするためにも、当該警察官は捜査部門に所属しない者とするべきではないか。取得した情報を捜査に利用するのは妨げないが、内部での統制が曖昧になり、情報が流用されているのではないかという外部からの疑念を払拭するためにも、警察庁による組織的統制は必要になるであろう。

○　遠隔解析の実施に当たっては、裁判所に個別に許可された取得対象ではない電磁的記録を扱うことも考えられるが、その場合にはこれを消去する、遠隔解析を実施する警察官を組織的に分離して、措置に関わっていない他の警察官には当該情報は提供しない、などの規範を法定することとすれば、比例性が担保されることとなる上、その手続的・組織的な担保が図られることとなり、通信の秘密やプライバシー権の保障を定める憲法の趣旨に沿うものとなる。

具体的には、取得予定以外の電磁的記録を取り扱った場合には、速やかに消去することに加え、遠隔解析実施警察官以外への提供を禁ずる規定や、消去しなければ、取得情報を遠隔解析実施警察官以外に提供してはならない旨の規定を置くこと、また、こうした措置を実施する警察官に対しての組織的統制も図ることで、手続面も含めて憲法上の要請が満たされると考えられる。

○　今回議論されている遠隔解析では、実態に即した厳格な要件に加えて、裁判所の許可を得るという事前手続、不要な情報の削除や相手方への通知という、組織的に分離されたところでの事後手続を含む全体を通じての組織的統制等が全体として構築されるのであれば、その全体をもって、プライバシーや通信の秘密の制約も、憲法上許容された合理的な範囲であると解される。

○　要件の一つとして検討されている補充性について述べたい。現行法上、補充性を要件としている措置としては、リアルタイムで流れてくる音声等を継続的に取得する通信傍受が挙げられるが、今回導入を検討している遠隔解析は継続性のない一回的な情報取得措置のため、補充性要件は、遠隔解析の憲法上の許容性を基礎付ける上で必須の要件ではないという理解も十分にあり得るのではないか。

また、今回の遠隔解析は秘匿性の高い通信アプリを用いて犯人間でやり取りされる犯行計画等の解明を目指すものであり、前回の検討会でも度々言及されたように、秘匿性の高い通信アプリの現状に鑑みれば、警察が遠隔解析という手法を用いなければ、被害防止に必要な情報を速やかに取得することが困難であるということも、自ずと明らかであるため、ほとんどの場合に満たすこととなると考えられる補充性要件を、あえて法律上で要件化する必要があるのかという点についても、立法政策上、様々な意見があるものと考えられる。

しかし、今回の立法が、他の方法によっては解決が困難な秘匿性の高い通信アプリへの対策を目指すものであるならば、他の方法によっては速やかに被害防止のための情報を収集することが困難であるという意味での補充性を、遠隔解析の実施要件として法律上明記することが、やはり素直な方向性ではないか。

○　要件の一つとして検討されている緊急性について、この要件は、飽くまでも今回の遠隔解析が重大犯罪の予防・鎮圧を目的とする行政警察活動上の措置であることから導かれるものと理解している。そのため、仮に、将来、「遠隔解析」と同様の措置を刑事手続上の捜査手法として導入することになった場合には、改めて、緊急性を実施要件とすべきか否かについて検討することになるのではないか。

(ｲ)　適正担保のための事後手続

○　匿名・流動型犯罪グループへの対策は、法制度によるものを含め、国民にとって分かりやすいものであることが必要である。一般国民に信頼される制度とするため、不要な情報の削除、我が国に数は多くない事後監督の制度について、集中的に議論を深めてほしい。

○　憲法第 31 条の適正手続の要請に照らし、警察が遠隔解析を行った場合には、原則として、事後的に対象者に対してその旨を通知する必要があると考えている。

刑事手続において、警察が、通信事務を取り扱う者が保管又は所持する郵便物等を差し押さえた場合には、発信人や受信人は当該差押処分を認識する

ことができないため、事後的に発信人又は受信人に対してその旨を通知しなければならないとされており、遠隔解析の事後手続においても、これと同趣旨の規律を設けるべきだろう。

もっとも、当該事後通知については、それによって審理が妨げられる虞がある場合は、この限りではないとされているため、その趣旨を遠隔解析の場面に応用すれば、対象者に遠隔解析を実施した旨を通知することによって警察の被害防止措置が妨げられるおそれがある場合には、通知のタイミングを遅らせることも許容されるのではないか。

また、郵便物等には、通常、発信人や受信人の氏名や住所が記載されるため、警察が発信人又は受信人を特定して通知することが容易であるのに対し、遠隔解析の対象端末は電話番号やＩＰアドレスなどで特定されるだけであり、警察が端末の使用者やその所在を特定して通知することが困難となる場合も多いと予想される。警察に不可能な作業を強いることは適当ではないので、対象端末の使用者の所在が不明であるなど処分を通知することが困難である場合には、例外的に通知を不要とするべきではないか。

○　遠隔解析の対象となった電子計算機の使用者への通知は、原則的に必要と考える。一般的な行政手続では、通知ができない場合は公示送達で代替することも参考となる。

他方、通知の実施によって被害防止措置に支障が生じる場合等には一定期間を空けるなどしつつ、可能な限り通知を行うことを原則として、代替策を考えていくべきではないか。

○　遠隔解析を実施した対象が指示役であった場合等には、通知を行ったことにより今後の警察活動に支障が及ぶ可能性もある。こうした例外があることを前提に、通知の方法等について検討する必要がある。

○　適正手続の観点から、遠隔解析を実施した場合には、いわゆるＧＰＳ判決の趣旨から見ても、その対象者にできるだけ速やかに事後の通知を行うことが原則として必要であり、この点を法律上明文化すべきと考える。しかし、今回の措置については、通知がそもそも困難である場合や、通知により被害防止に支障が生じる場合も当然考えられ、そのような場合には、憲法第 31 条と実効性のバランスに鑑み、適正担保の観点から相当と認められる限度で条件を定めて、対象者への通知の時期を後ろへ遅らせたり、通知を要しないこととしたりする旨の例外規定も用意するべきではないか。

○　対象端末の特定を誤るなどして犯罪とは無関係の人に対して遠隔解析を実施してしまった場合や、消去するべき情報を消去しなかった場合等、手続に瑕疵があった場合に、通知がなされることとするとともに、そうした場合にどのような被害救済措置が考えられるのか整理しておく必要があるのではないか。

○　ＧＰＳ判決においては、最高裁は、捜査対象の車両等にＧＰＳ端末を取り付けて継続的に位置を把握する捜査活動を継続性のある検証と同様の性質を有する等と整理して、立法措置を求めた。今回の遠隔措置は、継続性のな

い措置として立法していくとの方針であり、ＧＰＳ判決に挙げられているような適正性担保措置の一候補に相当する事後通知を原則として法定し、例外についても法定すること等を前提とすれば、今回の遠隔解析は、当該最高裁判決との関係で問題が残るものではない。

○　遠隔解析が適正に実施されていることを担保するために、第三者機関が事後的にチェックする仕組みが必要になるのではないか。

サイバー対処能力強化法については警察以外に、防衛省や外務省といった複数機関が執行に関わる制度であるため、事後的なチェックを行う新たな機関としてサイバー通信情報監理委員会を新設したと思われるが、今回の遠隔解析は、純粋に、警察行政の世界であるから、既に存在している機関である「公安委員会」によるチェックが考えられるのではないか。

○　事後的チェック機能を高度化するために、チェック項目を公表するのは効果的であると思う。英国の調査権限法においては、調査権限監察官が監査・監督をし、その実施内容は公表されていることも参考になるのではないか。

○　遠隔解析の具体的手法については高い秘匿性が必要だが、取得した情報について、確かに犯人が持っていた対象機器から取得することができた情報である、ということを事後的に確認できることを担保していただきたい。

○　事後的なチェックについては、実施内容等を公表することで透明性を確保することにより、事後的な手続が適正に行われていることが明らかとなり、国民も安心するのではないか。

○　サイバー通信情報監理委員会に遠隔解析の事後監督まで行わせることは必ずしも現実的ではなく、公安委員会において、これまでどおり警察に対するチェック機能を発揮させるべきではないか。

○　国民は警察と公安委員会を一体的な組織として見がちである。情報隠蔽への懸念が残ると国民の信頼が得られないので、事後チェックは、警察とは独立した組織が行うことが望ましい。サイバー通信情報管理委員会が適切でないなら、例えば個人情報を取り扱う部分に関する事後的なチェック主体を個人情報保護委員会とすることも考えられるのではないか。

(ｳ)　遠隔解析により得られた情報の活用

○　取得した情報は取得の目的の範囲内で利用することが原則であるものの、遠隔解析は司法警察活動にもつながる可能性がある措置であることを踏まえ、相手方・関係者の権利保護や手続等に留意する必要はあるが、取得した情報の「可能な範囲での利用」の検討を行うべきではないか。「利用することはできない、難しい」と考えずに、「利用すること」を前提として、そのために必要な制度的手配、仕組み、利用の範囲や制限の在り方等を考えるべきである。

ただし、情報を活用する場面は、捜査の端緒として用いる場面から、既存の捜査において犯罪を立証するために用いる場面まで様々であるため、取得情報の活用については、その場面を丁寧に細分化して議論する必要があるのではないか。

○　税務調査で取得した情報が捜査の端緒として利用されていることも踏まえ、令状主義の趣旨を没却しないことを前提に、取得目的の範囲内で取得した情報を刑事手続で利用することは問題ないと思う。

○　今回の遠隔解析は行政手続上の措置として創設されるものであるため、この措置によって得られた情報の活用の在り方を考えるに当たっては、税務調査で用いられる質問検査権等の行政調査権限によって得られた資料を刑事手続で用いることが許されるかという論点に関する最高裁判例が参考になると思う。

まず、最高裁昭和 51 年７月９日判決は、税務調査中に犯則事件が探知された場合に、これが端緒となって、犯則事件としての調査に移行することは禁じられていない旨を判示しており、税務調査で得られた資料を端緒として、犯則調査ひいては刑事手続に移行することは許容されると解されている。

また、最高裁平成 16 年１月 20 日決定は、税務職員が税務調査において質問検査権を行使する際に、取得収集される証拠資料が後に犯則事件の証拠として利用されることを想定できたとしても、そのことによって直ちに、質問検査権の行使が違法になるわけではない旨を判示しており、学説では、「税務調査における質問検査によって取得収集された資料は、後に刑事事件たる犯則事件の証拠として利用することができる」ということを前提とした判断であると理解されている。

このような判例の理解を踏まえれば、重大犯罪の被害防止という行政目的を達成するために実施される遠隔解析によって取得収集した情報を、後に刑事手続で利用することも許容されるのではないか。

さらに踏み込めば、川崎民商事件の最高裁判決が述べているように、税務調査における質問検査権の行使には憲法第 35 条の保障が及ばないため、事前に裁判官の令状を取得することは求められていない。そのような行政調査手続によって得られた資料であっても、後に刑事手続の証拠として用いることは許されるというのが現在の判例法理である。

これと比較した場合、今回導入を検討している遠隔解析は、憲法第 35 条の法意を踏まえ、事前に裁判官の令状を取得した上で実施し、不要な情報があればこれを消去しなければならないこととする措置とするならば、このような厳格な手続を経て得られた情報について、刑事手続での利用を禁止する理由はないのではないか。

以　上