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提言

令和８年９月
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

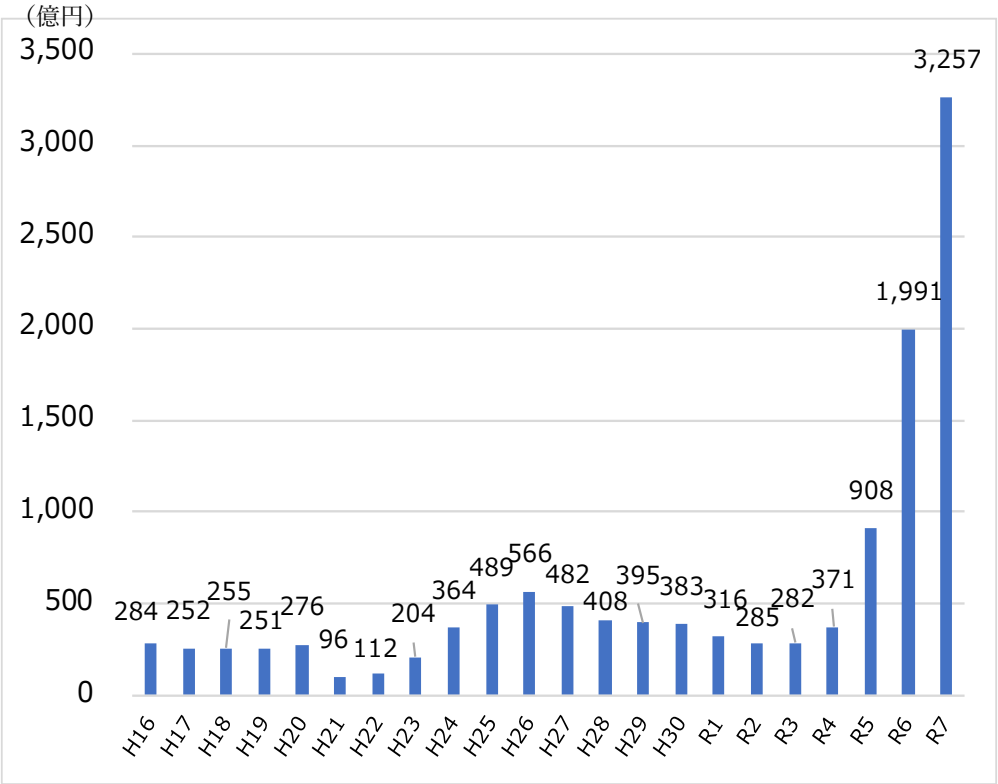
第１　匿名・流動型犯罪グループによる犯罪の発生状況等

１　特殊詐欺の被害状況

特殊詐欺の被害額は、この数年で爆発的に増加している。令和７年中は約 3,257 億円に達し、過去最悪を更新することとなったが、令和８年上半期は前年同期を更に上回る約 1,816 億円となっており、これは１日当たり約 10 億円の被害が発生している計算になる。また、個別の事案を見ると、９回にわたり総額約 12 億円がだまし取られるなど、長期間の巧妙な欺罔により、継続的に巨額の金銭が詐取される事例も発生している。

こうした特殊詐欺の多くに、匿名・流動型犯罪グループが関与しているとみられる。

【図１】特殊詐欺の被害状況



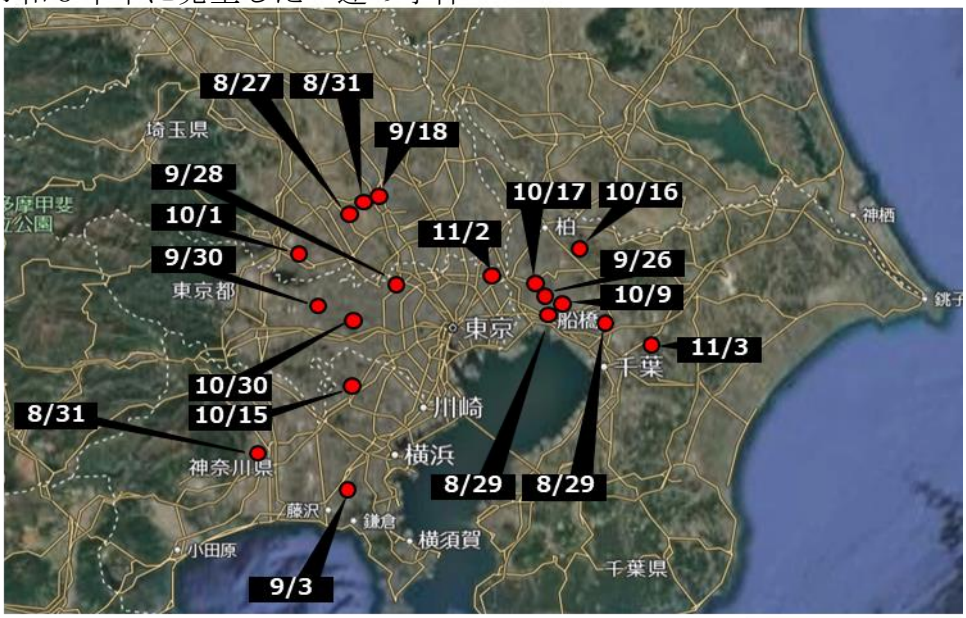
２　強盗等の被害状況

匿名・流動型犯罪グループは、凶悪な事件も多数引き起こしている。

令和６年には、南関東１都３県において、「闇バイト」を実行役とする 18 件の強盗事件が２か月以上にわたって連続発生しており、このうち１件で被害者が殺害され、12 件で被害者が負傷している（令和８年２月までに 55 名（延べ 85 名）が検挙されている。）。

また、令和８年５月には、栃木県内で、高校生等を実行役とする強盗殺人事件が発生した。この事件では、実行役は現場指示役の指示に従い被害者を殺害したほか、現場指示役と上位指示役は高い秘匿性を有する通信用アプリケーション（以下「通信アプリ」という。）を使用していたことが判明している。

【図２】　令和６年中に発生した一連の事件



※都道府県警察において検挙広報を実施したもの

Google マップ 地図データ ©2024に加筆

３　匿名・流動型犯罪グループによる犯罪の被害防止に向けた取組

(1)　実態解明及び取締りのための取組

警察では、匿名・流動型犯罪グループの組織構造、内部統制の方法、資金の流れ等を解明し、その撲滅を図るため、

○　広域的な捜査連携や仮装身分捜査（令和７年１月に導入）による取締り

○　匿名・流動型犯罪グループ情報分析室（令和７年 10 月に警察庁に設置）における全国の情報の集約・分析

○　匿流ターゲット取締りチーム（略称「Ｔ３」。全国警察から捜査員を派遣し、令和７年 10 月に警視庁に設置。令和８年４月に体制増強）による取締り

○　外国の捜査機関との連携等の国際捜査力の強化（令和８年６月からタイにリエゾンを派遣）

等に取り組んでいる。

(2)　広報啓発をはじめとした被害防止のための取組

警察では、自治体、自治会、関係団体・事業者等と連携し、

○　特殊詐欺の犯行に悪用されることが多い国際電話の利用休止を呼び掛ける活動（「みんなで止めよう!!国際電話詐欺 #みんとめ」）の推進

○　特殊詐欺の被害防止に資する警察庁推奨アプリ（令和７年 12 月に推奨制度を導入）の普及促進

○　金融機関と連携した被害拡大防止の推進

等に取り組んでいる。

(3)　犯罪インフラ対策のための取組

匿名・流動型犯罪グループにとって犯罪インフラが使いにくいものとなるよう、

○　犯罪収益の移転の阻止と被害者への返還を効果的に行うための「架空名義口座」に係る制度の整備（令和８年６月に立法措置済み）

○　「送金犯罪」（令和８年７月に罰則を導入）の取締り
○　不正に取得された携帯電話について携帯電話不正利用防止法に基づく役務提供拒否を促すための携帯音声通信事業者への情報提供
○　データ通信専用 SIM の契約締結時に本人確認を義務付ける制度の整備（令和８年５月に立法措置済み）

等に取り組んでいる。

４　匿名・流動型犯罪グループによる犯罪の被害防止に係る課題

前記３のとおり、警察等が匿名・流動型犯罪グループによる犯罪への対策を強化・推進しているにもかかわらず、期待される効果が十分に得られているとは言いがたい状況となっている。これには、以下の２つの原因があると考えられる。

(1)　匿名・流動型犯罪グループへの捜査の困難性

匿名・流動型犯罪グループの捜査は長期化する傾向にあり、具体的には以下のような例がある。

○　犯行グループの実行役は、「架け場」としてホテルを利用しており、頻繁に犯行拠点を移転させていた。また、警察の尾行への警戒心が極めて高かった。このため、ひとたび移転先を把握しても、直ちに行方をくらますということが繰り返され、詐欺事件の発生から「架け場」におけるかけ子の検挙までに約７か月を要することとなった。その間、当該犯行グループの標的とされた人々に対し、被害防止のための措置をとることができなかった
○　犯行グループの実行役は、「架け場」として車両を利用し、移動しながら犯行を行っていた。このため、実行役の特定や居所の把握が難しく、詐欺事件の発生から「架け場」におけるかけ子の検挙までに約５か月を要することとなった。その間、当該犯行グループの標的とされた人々に対し、被害防止のための措置をとることができなかった。

また、匿名・流動型犯罪グループの被疑者のうち、「捨て駒」である実行犯を検挙しても、上位の指示役や次の標的を速やかに特定することは困難であり、新たな実行役が補充されて犯行が継続されることとなる。

このため、刑事手続により、これらの犯罪を一つ一つ立件して対処するだけでは、同種犯行の反復・拡散に迅速に歯止めをかけることができない状況にある。

(2)　秘匿性の高い通信アプリの悪用等

特殊詐欺の被害者に連絡が行われていた拠点において、当該連絡用のスマートフォンとして 84 台が差し押さえられた例や、投資詐欺事件に係る実行犯のリクルーターであった者が、１名で 12 台のスマートフォンを所持していた例があるなど、匿名・流動型犯罪グループがスマートフォンやタブレット等の犯行ツールを活用して犯罪を敢行している実態が把握されている。

また、上記のような犯行拠点で差し押さえたスマートフォンやタブレットに、標的となる人物の詳細な情報（氏名、住所、電話番号、生年月日、性別、家族構成、学歴、所得、保有銀行口座、使用するスマートフォンのメーカー、やり取りした際の状況（通信アプリを使えるか、文字入力によるやり取りができるか等））が掲載された「闇名

簿」が、エクセルファイル、画像ファイル等として記録されていた例があり、こうした情報が犯人間で通信アプリを介して共有されている実態が把握されている。

現行制度の下で、警察が犯行グループの通信内容等を解明するためには、主に

① 通信事業者の協力の下、その保管・管理する通信ログ等の情報を取得する手法

② 通信経路上の通信を捕捉する手法

③ 犯行グループのスマートフォン等を押収し、その保存データを解析する手法

が考えられる。

しかし、匿名・流動型犯罪グループ等は、エンド・トゥー・エンド暗号化技術が用いられた通信アプリを使用することが常である。その場合、送信者の端末で暗号化された情報が受信者の端末で復号されることから、通信経路の途中段階（通信事業者のサーバや通信経路）の情報は常に解読不能な暗号文の状態となっている。このため、仮に、通信を媒介する通信事業者の協力を得て前記①又は②の手法をとったとしても、その内容を復号・解明することは技術的に不可能であり、こうした情報を警察が被害防止に活用することができない状況となっている。また、前記③の手法については、そもそも押収に至るまでに相当長期間の捜査を要するとともに、仮に押収できたとしても、被疑者が画面ロックの解除に応じないことや、自動的に情報が消去されていくことが多いことから、情報を迅速な被害防止に活用できる可能性は低い。

５　被害防止に必要な情報を入手することにより警察が果たし得る責務

犯人が通信アプリを利用して行う犯人間の相互連絡や被害者への連絡には、これから敢行しようとしている犯罪の標的となる人物に関する情報等、切迫する犯罪被害に関する情報が含まれており、それが犯人の端末に記録されていると考えられる。

警察がこうした情報を把握することができれば、犯人を直ちに特定・検挙できない場合であっても、切迫した犯罪被害を防止する責務を果たすことが可能となると考えられる。

具体的には、入手した情報に基づき、

○ 標的となっている人物の所在の特定

○ 犯罪の切迫性の見極め

○ 実行され得る犯罪の罪種、実行犯の人数、手口・凶器等に応じた態勢の整備

等を行った上で、適切な警察活動（重点的な警備・警ら、防犯指導等）を通じて犯罪被害の未然防止を図ることとなる。

６　小括

匿名・流動型犯罪グループが実行する特殊詐欺や強盗等の被害は極めて憂慮すべきものであり、警察等が取組を強化しているが、匿名・流動型犯罪グループの捜査をめぐっては、前記４(1)のような課題があり、直ちにその組織全体を検挙し、刑罰法令の適用により継続する犯行を止めることは、極めて困難と言わざるを得ないことから、十分な被害抑止効果が得られていない状況にある。

他方で、犯人間でのやり取り等に含まれている情報の中には、前記４(2)のとおり、犯罪の標的となる人物の特定等に資する情報が含まれており、こうした情報が入手でき

れば、警察による効果的な被害防止措置が期待できるものの、従来の手法では当該情報を警察が入手することは難しい。

こうした状況を踏まえれば、匿名・流動型犯罪グループによる犯罪の被害を防止するためには、犯行グループの端末から犯罪に悪用される通信アプリ等の通信内容等を迅速に把握し、犯罪の被害が切迫する者に対して警察が直接的かつ積極的に被害防止措置を講じる制度を導入することが急務である。

第２　新たな制度の具体的な方向性

１　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の必要性

近年、匿名・流動型犯罪グループによる特殊詐欺の被害額は顕著に増加しており、令和７年中の被害額は過去最多となったほか、人身犯罪である強盗事件も連続的に発生し、国民の尊い生命が奪われる事態にまで至っているなど、匿名・流動型犯罪グループによる犯罪の被害は正に異常事態と呼ぶべき深刻な状況となっている。

匿名・流動型犯罪グループは、実行犯の募集、犯行の指示等を、通信内容について高い秘匿性を有する通信アプリを使用し、かつ、非対面で匿名によりこれを行うことが一般的である。こうした特徴を有する犯罪者達を物理的に追いかけることは容易ではなく、そのために費やせる警察のリソースにも限りがある。また、「捨て駒」である実行犯を検挙したとしても、上位の指示役や次の犯行の標的を速やかに特定することは困難であり、その間に新たな実行役が補充されて犯行が継続することになる。こうした厳しい実態を踏まえると、匿名・流動型犯罪グループに対しては、刑罰規定の持つべき予防効果が十分に機能していない状況になっていると言わざるを得ない。

また、パーソナルな端末であり移動しながら動画等も発信できるなど豊富な情報がやり取りされるスマートフォンは、個人の生活や経済・社会の発展に貢献してきた反面、その悪用への対策は、長年にわたり大きな課題となってきた。特に、秘匿性の高い通信アプリについては、匿名・流動型犯罪グループが犯行に悪用し、警察による捜査・対策をより困難にしている。

具体的には、現行の刑事手続においては、捜査機関が、通信端末を押収する以外の方法で通信内容等を把握するための手段として、通信事業者に命じて事業者が保管・管理する情報を提供させる電磁的記録提供命令と、通信経路上の通信内容をリアルタイムで捕捉する通信傍受という２つの捜査手法が認められているが、これらの捜査手法では、強固な暗号措置が講じられた通信アプリによって犯行グループがやり取りした犯罪関連通信の内容を解明することは極めて困難である。

また、現行制度上、切迫する犯罪に対して、その被害防止のために警察が必要な情報を速やかに取得するための手段は、刑事手続上の手段よりもさらに限られている。

こうした現状に鑑みれば、匿名・流動型犯罪グループに対する新たな技術的措置として、犯行グループの端末から犯罪に悪用される通信アプリの通信内容等を迅速に把握し、被害防止に活用する手法（以下「遠隔解析」という。）を早急に導入することが必要である。被害者の受ける財産的打撃、精神的な打撃等は計り知れず、こうした悲惨な被害者を生まないための対策が急務である。また、当該措置の導入により、重大な犯罪に加担している自覚が薄い末端の者による犯行を未然に防ぎ、それが同時に、「闇バイト」に安易に応募した若者が重い罪に問われるような事態を防ぐことにもつながることが期待される。

諸外国においては、遠隔解析に類似した制度が既に構築されている。我が国での遠隔解析の導入の検討に当たっては、こうした他国の制度[1]も参考となる。なお、匿名・流動型犯罪グループによる犯罪は、国境を越えて行われることも多いことから、技術的措置を導入することにより、諸外国の当局との協力の現場において、我が国が実施可能な措置の選択肢が広がることも期待される。

2　遠隔解析に係る制度の在り方

遠隔解析により個人の端末から取得することとなる、秘匿性の高い通信アプリの通信内容については、憲法上の通信の秘密に関わるものであるとともに、プライバシーの保護が及ぶものとして考えるべきである。

その上で、適正手続の下で、必要な限度で通信の秘密やプライバシーを制約する捜査を行うことは憲法上も認められており、現行の刑事訴訟法も、こうした捜査の具体的な手続を規定することにより、人権の保護と公益の実現の調和を図っている。また、我が国では憲法上の比較衡量に関する確立された議論枠組みが既に存在しており、これらを踏まえた制度設計を指向するべきである（後記５に詳述）。

情報の取得が正当化されるためには、措置により実現される公益の内容と程度が、人権の制約の度合いを上回っているという意味での比例性も必要である。予防的観点から行政措置として犯罪被害の発生そのものを防止するためには、メタ情報だけでなく通信の中身を確認することとなるため、措置の対象者の特定や取得・管理する情報の範囲の決定は丁寧に行い、適正性が担保されるようにする必要がある。

犯人が使用する端末から被害防止に資する情報を取得するという目的を達成するために必要かつ合理的な実体的規律、通信の秘密に係る情報が適正に取得・管理されるための手続的規律、そして調査結果を活用して行われる被害防止のための警察活動全体の適正を確保するためのガバナンスの仕組みが求められる。

遠隔解析の制度化に当たっては、技術的措置に関する規定に加えて、収集した情報等により被害が切迫している者が判明した場合に、その被害の発生や拡大を防止するための措置に関する規定も、併せて整備する必要がある。

3　被害の発生や拡大を防止するための措置

「事案の真相を明らかにし、刑罰法令を適正且つ迅速に適用実現すること」を目的とする刑事手続により、犯罪を一つ一つ立件して対処するだけでは、匿名・流動型犯罪グループによる同種犯行の反復・拡散に歯止めをかけることはできない。このため、現在、犯罪の検挙のみならず、政府を挙げた広報啓発等により被害防止の取組も推進しているが、それでもなお被害が拡大していく厳しい現状を踏まえれば、一定の重大な犯罪については、より直接的かつ積極的な手法により被害を阻止する必要がある。

---

[1] 第２回有識者検討会において、事務局から英国（調査権限法）、ドイツ（刑事訴訟法、バイエルン州警察法）について紹介がなされた。

警察は、警察法第２条により、個人の生命、身体及び財産の保護に任じることとされている。この責務を具現化する形で、犯罪による被害が切迫する者等を警察が特定した場合には、直ちに当該被害を防止するための措置をとることを法律に明記し、警察による一層迅速な対処を促進するべきである。

４　遠隔解析の概要

現行制度上の手段では、犯罪による被害が切迫する者を特定するための情報をはじめとする被害防止に必要な情報を迅速かつ十分に取得することは困難である。こうした現状を踏まえれば、国民の権利利益の侵害を最小限にするよう配意しつつ、当該必要な情報を取得する技術的措置として、遠隔解析を行う権限を設けるべきである。

遠隔解析の制度設計に当たっては、従来の法制及び議論枠組みを踏まえて、生成されるデータを継続的に取得していく措置か保存されたデータを取得する１回の措置か、また、行政手続か刑事手続かという観点に着目して、制度設計における要件や手続を整理することが合理的である。

遠隔解析を刑事手続上の捜査手法として位置付けるアプローチも考え得るが、特定の犯罪の訴追・処罰を目的とする刑事手続上の措置によっては十分な犯罪予防効果が得られないおそれがあること、予備や未遂も含め犯罪としては未だ成立していない段階においても警察が介入するべき場面が多いと予想されること等の事情が認められることに鑑みると、遠隔解析を、犯罪の予防や阻止を目的とする行政手続上の措置として位置付けることには十分な合理性が認められる。

その上で、端末内の情報を継続性なく取得する権限として整理するとすれば、刑事訴訟法に基づく差押えの要件・手続を一つの目安として、遠隔解析の要件・手続を構成することが考えられる。

また、遠隔解析については、現行制度が直面している課題を踏まえ、

○　犯行グループに察知されることなく密行的に実施できるものであること

○　犯行ツールとして使用されるスマートフォン等の端末の所在場所が不明であっても、当該端末が特定されていれば、当該端末に記録された情報の取得を可能とするものであること

○　犯罪による被害が切迫する者を特定する情報その他の被害防止に必要な情報の取得を可能とするものであること

が必要である。加えて、遠隔解析によって取得するべき情報の範囲については、刑事訴訟法に基づいてスマートフォンやパソコン等の端末を物理的に差し押さえることにより得られる情報の範囲が目安になると考えられる。

遠隔解析は、一定の重大な犯罪による被害が切迫した際に、当該被害を防止する目的で行使する行政調査権限として新設することが考えられる。当該権限については、警察官が犯罪の予防を含む職権職務を遂行するために必要な手段を定めることを目的とする警察官職務執行法の中に規定することが考えられる。

遠隔解析の具体的な手法を検討するに際しては、端末同士が直接鍵交換をして暗号通信を行うようなインターネットの世界において、従来の事業者を巻き込む制度設計は機能しにくいことに留意するべきである。また、技術的な措置は、様々な可能性がある一方、対策も容易であることから、制度の詳細な内容については十分に情報保全を図るべきである。

5　遠隔解析の具体的制度

①　遠隔解析の要件

遠隔解析は、被害防止に必要な情報が、対象となる端末（電子計算機）のどこにどのような形式で記録されているのかが分からないという状況において、犯人への事前通知は行わずに、権限を行使する時点で当該電子計算機に記録されている電磁的記録のみを抽出して可視化し、その中から被害防止に必要な情報を選別して取得するものとして、関係する国内外の制度を参考に、その実施要件を定めるべきである。

なお、遠隔解析は、上述のとおり「権限を行使する時点で当該電子計算機に記録されている電磁的記録のみ」を対象とする措置であることから、生成されるデータを継続的に取得するものではない。

A　犯罪被害が発生するおそれ

遠隔解析の要件は、刑事訴訟法に基づく差押えの要件を目安とするべきであり、犯罪被害の発生見込みにつき、より厳格な基準（例えば、通信傍受における「十分な理由」）までは求める必要性は認められない[2]。

他方、遠隔解析は、犯行グループによる犯罪被害の発生・拡大の具体的なおそれが認められる場合に限って実施することが望ましく、例えば、一定の重大な犯罪の発生が現に確認された場合で同種の犯罪被害が懸念されるとき等に厳格に限定することが考えられる。

なお、匿名・流動型犯罪グループのような特徴を有する犯罪者達による犯罪の被害を防止するための実効性のある要件とする必要があることから、「数人の共謀によると認められる犯罪の被害」を対象としつつも、犯罪者間の継続的な結合等を前提とした要件は設けるべきではないと考えられる。

B　対象とする電子計算機の使用者

---

[2] 刑事手続上の要件として「十分な理由」が規定されている例としては、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があり、一般用語としての「十分」が与える印象に比べて、相当高い嫌疑が必要であることを意味する要件とされている。

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」と規定され、必要となる嫌疑は相対的に低くなっており、差押えの要件は「罪を犯したと思料される」と規定され、必要となる嫌疑は「相当な理由」よりも更に低くなっている。

このことからも、遠隔解析の要件について、「十分な理由」まで必要とするのは均衡を失すると解される。

遠隔解析は、切迫する被害を防止するための必要な措置であるものの、犯罪とは無関係の者が使用する電子計算機に対しても遠隔解析を実施されるのではないかとの懸念は確実に払拭するべきである。その観点から、遠隔解析の対象となる電子計算機は、被害が発生するおそれがある重大犯罪の犯人が使用すると合理的に認められるものに限定するべきである。

C　対象とする電子計算機

遠隔解析は、切迫する被害を防止するための措置であり、後述のように、犯罪による被害が切迫する者を特定する情報や切迫する犯罪の実行に関する情報などを取得するものである。

そのような情報は、指示役から実行犯への指示などの犯人同士の連絡や犯人から被害者への連絡に用いられた電子計算機に保存されている蓋然性が高いと考えられることから、遠隔解析の対象は、こうした電子計算機であることが合理的に認められるものに限定するべきである。

D　対象とする電磁的記録

遠隔解析の目的は、匿名・流動型犯罪グループ等による重大な犯罪の被害が切迫する者を調査・特定した上で、当該者への注意喚起、警察の対処態勢の整備等を迅速に行い、被害を的確に防止できるようにすることである。

このため、遠隔解析により取得するべき電磁的記録としては、犯罪による被害が切迫する者を特定する情報（氏名、住所が分かる情報、自宅写真等）のほか、犯罪が行われる日時、襲撃に加わる実行役の人数、準備している凶器等の切迫する重大な犯罪に関する情報が想定される。

また、実際の運用においては、刑事訴訟法に基づいて電磁的記録を取得する処分を実施する際に得られる情報の範囲も参考にするべきである。

E　緊急性

遠隔解析は、差し迫った人身・財産等への危険を回避するなど、必要な場合に限定して権限を行使することが望ましいことから、重大な犯罪による被害の発生・拡大が差し迫っており、警察官による職務執行を緊急に行う必要があることを要件として設けるべきである。

F　補充性

遠隔解析は、電子計算機の使用者に事前に通知することなくそこに記録された電磁的記録を確認するものであり、プライバシーの権利等を制約するものである。この調査権限が真に必要な場合に限り行使されるようにするための要件を定めることが望ましいことから、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ことを要件として設けるべきである。

②　遠隔解析の事前手続

遠隔解析は、憲法第 31 条及び第 35 条の要請を踏まえれば、遠隔解析ができる場合に該当すると認める理由のほか、対象となる電子計算機、取得する電磁的記録の範囲等について、裁判官による事前の審査（許可状の発付）を受けることとするべきである。また、事前の司法による審査（許可状取得手続）においては、憲法第 35 条の特定性の要請や刑事手続上の既存の強制処分の要件との均衡に照らし、遠隔解析の対象となる電子計算機を電話番号、ＩＰアドレスなどの何らかの方法で特定するとともに、取得する電磁的記録の範囲を当該対象となる電子計算機に記録されていると合理的に認められる前記５①Ｄのような電磁的記録として特定することが要求される。

③　必要な処分

遠隔解析に当たっては、対象となる電子計算機内のデータを確認し、取得対象となる情報を探し、選別するという過程を経ることが想定される。この過程においては、技術上の特性から、対象の電子計算機内のデータを、遠隔解析を行う警察官の電子計算機に送信した上で、その内容を確認することが必要となることも考えられる。

現在の刑事訴訟法の規律を踏まえれば、取得対象情報を探して選別するという目的に必要な限度で、対象の電子計算機内のデータを一時的に警察官の電子計算機に送信し、これを知得することを許容する制度とすることが妥当であり、刑事訴訟法と同様の「必要な処分」に相当する行為を法定するべきである。

６　憲法との関係

①　憲法第 13 条及び第 21 条第２項との関係

個人が所有する電子計算機におけるプライバシーに関する議論は憲法上も比較的未成熟な分野であるが、遠隔解析の対象となる電子計算機に保存されている秘匿性の高い通信アプリの通信内容は、憲法上の通信の秘密に関わるものであるとともに、プライバシーの保護が及ぶものとして考えるべきである。

その上で、適正手続の下で、必要な限度で通信の秘密やプライバシーを制限しながら捜査を行うことは憲法上も認められており、現行の刑事訴訟法も、住居の捜索や郵便物の差押え、検証、通信傍受等、捜査の具体的な手続を規定することにより、人権の保護と公益の実現の調和を図っている。また、検証による電話傍受や装着型ＧＰＳ捜査に関する最高裁判例[3][4]等において、憲法上の比較衡量に関する確立された議論枠組みが存在している。

従来の法制及び議論枠組みを踏まえて、通信傍受のように次々と生じる音声や生成されるデータを捕捉し続ける継続的な措置か、保存されたデータを一の機会に取得する非継続的な措置か、また、行政手続か刑事手続かという観点に着目して、制度設計における要件や手続を整理していくことが合理的である。

遠隔解析については、裁判官に取得を許可された電磁的記録以外の電磁的記録を取り扱った場合には、これを速やかに消去しなければならず、かつ、他者に提供してはならない旨の規定を置く（後記７②Ｂ）とともに、遠隔解析を実施する警察官に対す

---

[3] 最決平成 11 年 12 月 16 日刑集 53 巻９号 1327 頁

[4] 最大判平成 29 年３月 15 日刑集 71 巻３号 13 頁

る組織的統制を図る（後記７②Ａ・Ｄ）ことによって、公共の福祉に資する重要な目的のために必要な範囲内に限り行うものといえることから、憲法 13 条の法意に反するものではないと考えられる。

また、通信の秘密は、憲法上の権利であるが、法律により公共の福祉のために必要かつ合理的な制限を受けることも認められる。

行政手続による通信の秘密の制限については、抽象的な議論のみで「許容される」又は「許容されない」との結論を得ることは適切ではなく、具体的な制度設計の各場面において通信の秘密との関係を考慮し、実体的な規律とそれを遵守するための組織上・手続上の仕組みを作ることが必要であり、加えて、明確で詳細なルールとなるよう考慮することが適当である。

遠隔解析については、保存されたデータを一の機会に取得する非継続的な措置として、切迫する重大な犯罪被害を防止する目的の範囲内で情報を取得するための必要かつ合理的な実体的規律が設けられること（前記５①）、通信の秘密に関わる情報が適正に取得・管理されるための手続的規律が設けられること（後記７②Ｂ～Ｄ）、遠隔解析と被害防止措置という一連の警察活動の全体の適正を確保するためのガバナンスの仕組みが担保されること（後記７②Ａ・Ｄ）を前提にすれば、通信の秘密やプライバシーへの制約が生じたとしても、その制約の程度はやむを得ない限度にとどまると考えられる。

②　憲法第 31 条及び第 35 条との関係

遠隔解析については、法律で定められた手続が適正でなければならないことをも意味すると解されている憲法第 31 条や、捜索及び押収について厳格な令状主義の原則を定め、一定の行政手続にもその要請が及ぶと解されている憲法第 35 条との関係が論点となる。

遠隔解析による情報の取得の目的は、被疑者の特定・検挙ではなく、犯罪による被害が切迫する者に対して被害防止の措置を講じることである。遠隔解析により取得できる情報は当該目的のために必要なものに限られることや、不要な情報の消去義務が設けられること（後記７②Ｂに詳述）を前提とすれば、遠隔解析が、刑事責任追及のための資料の収集に直接結びつく作用を一般的に有するものとは認められない。

しかし、この調査権限に基づく電磁的記録の取得は、プライバシーの権利の侵害を伴うものであり、かつ、その実質において電子計算機の物理的な差押えと同程度の強制処分と認められることから、一定の行政手続については令状主義の要請も及ぶと解される憲法第 35 条の法意を考慮する必要があり、事前の司法による審査を設けるべきである。

遠隔解析については、前記５②のような司法による審査を設けることを前提とすれば、それにより、憲法第 31 条及び第 35 条の要請を満たすと考えられる。

7　遠隔解析の導入に当たっての実効性・適正性担保措置

①　実効性の担保

遠隔解析が真に被害防止に資する制度となるよう、以下の点に留意する必要がある。

○　厳格な要件、適正な手続を導入することを前提としながら、実効性のある対策を導入する必要がある。
○　技術は日々進化することを踏まえ、その変化に柔軟に対応できる制度とする必要がある。
○　犯人らに容易に対抗措置をとられないよう、技術的措置の詳細については徹底した情報保全を図る必要がある。

②　適正性の担保

前記５①及び②のとおり、遠隔解析の制度を設けるためには、重大犯罪による被害発生の高度な蓋然性、緊急性・補充性、犯人の端末への限定等の厳格な要件を設定した上で、事前の司法による審査を受けることとするべきであり、加えて、適正性担保のために以下の措置も講ずるべきである。また、運用上も、情報保全を図りつつ、遠隔解析の導入によって、逆に国民の安全が脅かされることのないよう配意するべきである。なお、憲法上の要請を満たした制度であっても、その趣旨を満たした適正な執行が重要なのはいうまでもない。

A　遠隔解析を行う者の厳格化

被害防止の活動に従事する警察官と、遠隔解析を行う警察官との役割を分離した上で、遠隔解析を適正に行うために必要な知識及び能力を有すると認められる警察官を警察庁長官が指名し、遠隔解析の実施権限は当該指名された警察官にのみ認めることとするなど、当該権限の適正な行使を制度的に担保するべきである。

B　取得が認められた情報に該当しない情報の消去

遠隔解析により取得する情報の範囲を、目的に照らして必要な範囲内に限る観点から、技術上やむを得ず、取得が認められた情報に該当しない情報を取り扱うこととなった場合においては、その全てを消去することとするべきである。

また、こうして消去するべき情報が、遠隔解析を行う警察官以外の警察官に提供されることのないようにすることなどを制度的に担保するべきである。

C　遠隔解析の対象となった電子計算機の使用者への通知

遠隔解析においては、措置に際して許可状の提示を行い得ないので、その措置がなされたかどうかを相手方が認知することが困難であることが想定される。このため、相手方の権利の保護に必要な事項を遅滞なく相手方に知らしめることで、万が一違法な処分が行われたような場合に、救済の道を開いておくことが望ましい。

他方で、通知によって犯行グループに対策を講じられてしまう事態や通知するべき対象者を特定できない事態も想定される。このため、通知については、犯罪被害の防止に支障がある場合及び通知先となるべき使用者に関する情報が不明である場合を除いて行うこととしつつ、当該使用者に関する情報が明らかである場合には、当該支障がなくなった後、速やかに行うこととするべきである。

D　公安委員会による事後監督

遠隔解析が濫用され、警察による不当な干渉・監視が行われるのではないかとの不安を国民が抱くことによって、警察による適正な職務執行に悪影響が生じることのないようにするべきである。

現行の警察制度においては、警察官職務執行法に基づく避難措置の実施結果の報告を受けたり、警察の不適切事案に対する監察機能を果たしたりする管理機関として、国家公安委員会及び都道府県公安委員会（以下「公安委員会」という。）が存在している。

これを踏まえ、遠隔解析を行った警察官は、所属の公安委員会にこれを悉皆的に報告し、その確認を求めることとするべきである。また、適正性を確保するため必要があれば、公安委員会が具体的な措置をとることができることとし、透明性の確保に努めつつ、事後監督を行う公安委員会の機能がしっかりと果たされるよう運用するべきである。

８　遠隔解析により得られた情報の活用の在り方

一般に、法律で規定される権限は、それぞれの規定が設けられた趣旨・目的に従って行使されなければならず、他の目的のために行使されてはならない。

このため、遠隔解析も、犯罪被害の防止という目的を逸脱し、犯罪捜査を目的として権限を行使することは許されず、かつ、制度上もそれを担保するべきである。

他方で、行政調査により収集・取得された資料の刑事手続での利用に関しては、税務調査に関する最高裁判例[5]において、行政調査で得られた資料を端緒として刑事手続に移行することや当該資料を刑事手続の証拠として利用することも許容されることが示されている。このような判例を踏まえれば、重大犯罪による被害の防止という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した情報については、刑事訴訟法等に基づく必要な手続を経ることにより、刑事手続で利用することも許容されると解される。特に、現行法上、必ずしも司法による審査を経ない他の行政調査によって取得された情報であっても刑事手続で用いることが許容されているという状況に鑑みれば、厳格な要件・手続を設け、司法による審査を受けて適正に取得された遠隔解析による情報について刑事手続での利用を禁止する理由はないと考えられる。なお、情報の活用に当たっては、当該情報が対象の電子計算機から確かに取得したものであることが事後的に確認可能であることも重要である。

[5] 最判昭和 51 年 7 月 9 日集刑 201 号 137 頁及び最決平成 16 年 1 月 20 日刑集 58 巻 1 号 26 頁

第３　遠隔解析の制度、運用等に関するその他の意見[6]

１　遠隔解析の法的性格

○　今回導入するべき技術的措置の特徴は「調査対象者において、自らが調査対象となっていることが伝わっていない状態で行われる情報の取得であること」であり、これは、従来行政法の領域で議論してきた「行政調査」とは大きく異なる。

○　行政手続と憲法第 31 条及び第 35 条との関係についての最高裁判決[7]では、全ての行政手続にその要請が及ぶとは解されていないが、更に重要な点として、行政手続は、刑事手続とその性質においておのずから差異があり、また、行政目的に応じて多種多様であるとされている点が挙げられる。

また、この判決に付されている意見も重要であり、この意見では、「行政庁の処分は、刑事上の処分と異なり、その目的、種類及び内容が多種多様であるから、不利益処分の場合でも、個別的な法令について、具体的にどのような事前手続が適正であるかを、裁判所が一義的に判断することは困難というべきであり、この点は、立法当局の合理的な立法政策上の判断にゆだねるほかはない」とされている。行政手続であることをもって刑事手続よりも軽い要件でよいというわけではなく、この遠隔解析に関して行われているように、行政手続ごとに要件を個別に考えなければならないものである。

なお、今般導入を検討している遠隔解析については、事前に司法による審査を受けることとして憲法第 35 条の令状主義の要請を確実に満たす方向での制度構築が検討されているということを確認したい。

○　匿名・流動型犯罪グループによる犯罪は、財産犯であろうと身体犯であろうと、発生してから対処するのでは遅く、予防的観点から、行政措置としてその発生そのものを防止する必要がある。したがって、端末の情報を確認するとしても、メタ情報だけでなく、通信の中身を確認する必要があるが、中身を確認する以上、措置の対象者の特定は丁寧に行い、外部から見て公平性が担保されるようにする必要があるのではないか。

○　遠隔解析が事前の司法による審査を経る手続である以上、法制化の際には、裁判所による事前の審査を適正に行い得る、客観的な事実関係に基づき蓋然性の判断ができるよう要件を的確に規定することが必要ではないか。

２　遠隔解析の運用上の参考となり得る刑事訴訟法の実務・判例等

○　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１回限りの執行しか認められないが、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。これを踏まえれば、遠隔解析を実施した際、近い将来に必要な情報が当該端末に記録される蓋

---

[6] 本項は、検討会における各委員の意見を基に、第２の「新たな制度の具体的な方向性」の考え方の背景となる議論、制度運用上の留意点、議論の過程等について整理・記載したものであり、必ずしも委員の総意としての意見を示すものではない。

[7] 最大判平成４年７月１日民集 46 巻５号 437 頁〔成田新法事件〕

然性が高いことが判明した場合には、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・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、長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。最高裁判例[8]において、捜索・差押え中に届けられた物品についても捜索・差押えに係る許可状の効果は及ぶとされていることから、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の実施中に新たに記録された情報を取得することは、許容されると考えられる。もっとも、遠隔解析の目的達成のために必要な限度を超えて、過度に長時間にわたり対象の電子計算機に対する接続を行い続けるような運用は許されないことは当然である。

○　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・可読性のない電磁的記録媒体（例えば、USB メモリ）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」をすることも可能である。

こうした刑事訴訟法の規律及び憲法第 35 条の下で警察に認められている権限の範囲を踏まえれば、今回新たに導入する遠隔解析に基づく情報の取得においても、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送信させ、これらを知得することは許容されると考えられる。

○　選別を行った結果として、取得するべき対象に含まれないと判断された情報については、刑事訴訟法の現在の運用との対比においても、警察がこれを保有し続けることは許されず、確実に消去することが必要である。

○　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。そのため、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、当初の捜索差押令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ことに鑑みれば、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、直ちに証拠保全をすることは許されないと考えられる。

○　遠隔解析を実施するための要件として、重大な犯罪による被害の発生・拡大が差し迫っており、警察官による職務執行を緊急に行う必要があるという趣旨で「緊急性」を設ける場合であっても、当該緊急性については、刑事訴訟法上の「緊急性」、すなわち「その時点で当該処分を行わないと目的を達成できない」という要件とは、必ずしも一致するものではない。なお、これは「緊急性」という言葉の多義性を指摘する趣旨に留まり、遠隔解析に対する事前の司法による審査を緩和するべきであるという趣旨の意見ではないことを確認したい。

---

[8] 最決平成 19 年２月８日刑集 61 巻１号１頁

３　ＧＰＳ判決との関係

○　遠隔解析を実施した場合には、いわゆるＧＰＳ判決[9]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るべきと考える。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、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。

○　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などと整理して、立法措置を求めた。今回の遠隔解析は、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法定すること等を前提とすれば、当該最高裁判決との関係で問題が残るものではない。

４　遠隔解析の技術的手法

○　通信事業者であっても、端末間での強固な暗号措置が講じられていれば、メッセージの閲覧等を行うことは技術的には事実上不可能である。

○　遠隔解析の実施手法については、端末の脆弱性を突いたり、端末の利用者を欺罔する手段を用いざるを得ない場面等があり、警察がこうした手法を用いることは認められるべきだと思う。他方、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である。

○　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。

５　事後監督・透明性の確保

○　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。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も執行に関わる制度であるため、サイバー通信情報監理委員会が事後的にチェックを行うこととされたと思われるが、今回の遠隔解析は、純粋に、警察行政（警察行政法の執行）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」によるチェックとすることが適当ではないか。その際、不適切な遠隔解析が実施された場合には、公安委員会による適切な是正措置が実施されるべきである。

○　個人情報を取り扱う部分に関する事後的なチェックの主体は、例えば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。また、遠隔解析の実施に伴う個人情報の取扱いに関しては、個人情報保護法にも則った適切な運用が確保されるよう個人情報保護委員会との連携が必要になるだろう。遠隔解析の適正性を確保するために重層

[9] 前掲注４

的なチェック機能が作用しているということが、国民に認知されることにより、国民からの信頼を得られる制度となるのではないか。

○　公安委員会が監督をすることについて、組織の中立性や監督能力等に関する懸念を示す意見もあるが、公安委員会制度は、戦後の日本の警察行政の根幹となるものである。警察による法執行のガバナンスとして、都道府県警察については都道府県公安委員会に、警察庁については国家公安委員会に、それぞれの役割を果たしてもらうことは非常に重要と考える。遠隔解析の事後監督については、技術的・専門的知見が必要となるが、その点については、別の組織に委ねるとしなくても、現行の公安委員会制度の枠組みにおいても工夫をすれば十分に対応できるのではないか。

いずれにしても、事後監督に係る「透明性の確保」は極めて重要であり、それには様々な方法がある。法律にどこまで書くのか、どのような運用とするかは、法制度の均衡も踏まえて調整されていくことになるであろう。

○　警察による遠隔解析に関する事後監督を行う組織として、公安委員会が適当なのかという意見もあり得るだろう。監督の実効性を高めるため、専門的知見を有する外部の者による補助等の可能性についても検討するべきではないか。

○　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、同委員会の設立経緯等を踏まえると必ずしも現実的ではなく、公安委員会において従来の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。

○　事後的なチェックについては、必要な監督・監察の体制を整えるとともに、事後的に振り返れるような形式で実施内容等を公表することにより、透明性を確保することが重要である。それにより、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。

○　刑事手続上の捜査手法に対する透明性確保の規律を見てみると、リアルタイムで流れてくる音声を継続的に捕捉する通信傍受については実施状況の公表が法定されているのに対し、既に保存されている電子メールの内容や通信履歴を相手方に提供させて取得する電磁的記録提供命令については、そのような公表制度は法定されていない。実施状況の公表について法定するか否かは、これまでも検討の視点となってきた「継続的に情報取得を行うか否か」によって区別されているものと思われる。

今回は、刑事手続ではなく行政手続上の措置として遠隔解析を導入する方針であるため、一概に論じることはできないが、今回の遠隔解析を継続性のない一回的な措置として創設するのであれば、実施状況の公表について法定することまではしないという方針も選択肢ではないか。

なお、これは公表制度をあえて法定することまではしないという趣旨にとどまり、実務上は、透明性を確保する観点から、遠隔解析措置の実施状況を何らかの形で公にすることは必要であると考える。

○　透明性確保のための一つの手法として遠隔解析措置の実施状況の公表を行う場合においても、公表を通じて、犯人が自分の事件で遠隔解析措置が行われたという事実を推察し、対策をとることができるようになれば、実効性の観点で大きな問題が生じる。遠隔解析措置の実施状況を何らかの形で公にするとしても、個別事案との紐付けがなされないように、情報の粒度や公表のタイミング等について慎重に検討する必要がある。

○　真のデータ主体に処分があったことが知らされない形で処分が行われることは、現行制度にも事業者を相手方とする電磁的記録提供命令といった例がある。遠隔解析は、このような真のデータ主体に処分があったことが知らされない形で行われる処分の別類型を新たに定めるものであるといえるが、遠隔解析は、被処分者と真のデータ主体のいずれとの関係でも処分の存在が知らされないため、より密行性が高いという側面がある。この点、既存の電磁的記録提供命令で求められている事前の司法による審査に加えて、データ主体に対する事後通知、公安委員会による事後監督、そして透明性への配慮がなされるべきことが骨子案に明記されており、より重い適正性担保措置が設けられているといえる。

６　遠隔解析の対象端末が国外に所在する場合の考え方

○　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に影響が生じ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を、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。

○　匿名・流動型犯罪グループによる犯行が海外で行われることも想定されるところ、今回導入を検討している遠隔解析については、端末が海外に所在する場合においても対象となり得る制度設計を考えていくべき。

組織犯罪への対応では、関係国が危機感を共有し、緊密な連携を図ることが標準となっている状況を踏まえると、相手国との協力関係の下に権限を執行していくという運用が通常想定される。具体の運用としても、国際法に照らし、その国の主権を侵害することがないよう相手国の同意を得て遠隔解析を実施することが基本となるのではないか。

○　越境リモートアクセスに関する最高裁決定[10]は、サイバー犯罪に関する条約の定める特定の状況下における越境リモートアクセスの許容性を判示しつつ、それ以外の状況下で同様の手続をとった場合における許容性については今後の国際法の議論に委ねているものと考えられる。この最高裁決定では、差押え対象となる端末と被処分者が国内に所在しその端末から接続する海外所在のサーバへのリモートアクセスの許容性が論じられたのに対し、遠隔解析では、処分の対象となる端末や被処分者が海外に所在し得るといった相違があり、その場合の許容性については、正に今後の国際法の議論に委ねられた領域と言えるだろう。

なお、この最高裁決定においては、サイバー犯罪に関する条約において許容された方法によらない手続について、違法かどうかの判断を明示的には行わず、少なくとも重大な違法を構成するものではないとして証拠能力を認める判断を行っている。この点も、遠隔解析の制度を運用するに当たって一つの参考となるのではないか。

７　制度の在り方に関する将来的な検討

[10] 最決令和３年２月１日刑集 75 巻２号 123 頁

○　遠隔解析の対象を犯人の使用端末に限定する点については、遠隔解析制度の導入の目的に照らして十分な合理性が認められるものであるが、今後の技術の進展等により、犯人が使用すると合理的に認められる端末のみを対象としていたのでは、被害の発生・拡大を十分に防止できないという新たな立法事実が生じた場合や、将来、刑事訴訟法上の捜査手法として遠隔解析と同様の措置を創設しようとする場合には、被疑者以外の第三者が使用する端末を対象とすることの当否や、対象とする場合の実施要件の在り方について、改めて議論する必要があるのではないか。

○　遠隔解析については、今後の犯罪情勢や技術動向等を踏まえ、適切な運用の在り方について検討を行うことが望ましいのではないか。

○　仮に今回の措置を警察官職務執行法に定める場合、一定期間の経過後に措置の規定を見直す仕組みとすべきかどうかについては、警察官職務執行法の法制上の位置付けを考慮する必要がある。警察官職務執行法は、全国の警察官の職務執行について定めるいわば職務執行の根幹たる法律、基本法のようなもので、軽々に見直しをするような法律ではない。新しい措置を同法に導入する場合には、頻繁かつ拙速な見直しは避けるよう慎重を期するべきであり、濃密な検討と議論を重ね、熟考の上、制度化すべきである。

○　遠隔解析を的確に実施するためには、必要な知識及び能力を有する警察官が不可欠である。法令と通信技術に精通し、かつ、犯人の端末から被害防止措置に必要な情報を過不足なく抽出できる高度な人材の確保・育成も、重視されるべきである。

○　前記第２の１のとおり、遠隔解析の導入により、重大な犯罪に加担している自覚が薄い末端の者による犯行を未然に防ぐことにもつながることが期待されるが、警察庁が力を入れている教育面の啓発活動についても、今回の立法措置により、更に広く効果を持つことが期待される。

参考資料１　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　構成員名簿

【有識者委員】

座長　川出　敏裕　東京大学大学院法学政治学研究科教授

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

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

（敬称略、委員は五十音順）

【警察庁出席者】

森元　良幸　官房長

土屋　暁胤　総括審議官

中村　彰宏　長官官房企画課長

中山　卓映　刑事局捜査支援分析管理官

参考資料２　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　開催状況

【第１回】　令和８年８月 10 日（月）

○　自由討議（技術的措置に係る各種論点について議論）

【第２回】　令和８年８月 26 日（水）

○　自由討議（海外制度や前回議論を踏まえた各委員の意見を踏まえた制度イメージについて議論）

【第３回】　令和８年９月２日（水）

○　提言骨子取りまとめ
○　自由討議（遠隔解析の導入に向けたその他の論点について議論）

【第４回】　令和８年９月９日（水）

○　自由討議（提言の取りまとめに向けた議論）

【第５回】　令和８年９月 24 日（木）

○　提言取りまとめ