第１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 10 日（月）午後３時 00 分から午後５時 00 分まで

２　開催場所

日比谷国際ビルコンファレンススクエア８Ｄ

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
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

４　議事概要

(1)　警察庁官房長挨拶

森元官房長から開会の挨拶があった。

(2)　構成員紹介

事務局から構成員の紹介が行われた。

(3)　座長選出

川出委員が座長に選出された。

(4)　警察庁説明

中山捜査支援分析管理官から匿名・流動型犯罪グループによる犯罪被害対策に係る現状及び課題並びに御議論いただきたいポイントについて説明があった。

(5)　自由討議

匿名・流動型犯罪グループへの技術的措置の必要性、当該技術的措置を実施するための制度及び当該技術的措置の導入に当たっての実効性・適正性担保につい

て議論することとされたところ、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。

なお、当日欠席された金子委員からは、書面により意見が提出された。

ア　匿名・流動型犯罪グループへの技術的措置の必要性について

○　匿名性の高いＳＮＳアプリ、そして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、その高度化と悪用への対策は、長年にわたり大きな課題となってきた。

技術革新が早く、その悪用による被害の拡大に対して、法制度による対応が遅れる構造的な課題が存在しており、警察法第２条において個人の生命、身体及び財産の保護という責務を任じられている警察が適切な対応を図らなければ、国民の不安から、利用の全面的な制限や、全利用者の通信の大規模監視などの逆に極端な規制を導入すべきという主張も出てくることとなり、そうなれば、実効的な取組とそのための社会的合意形成も困難になるおそれがある。

事務局より説明のあった匿名・流動型犯罪グループによる犯罪被害の深刻さとそれに対する対策の必要に鑑みれば、明確かつ具体的な立法事実が存在し、国民の生命・身体・財産という法益への具体的な危険を防ぐために必要な限度での実効的な技術的措置を整備する対策の必要性が高いのではないか。

○　昨今の犯罪発生状況、被害の状況等から考えると、このような犯罪による被害の発生を防止するために必要となる情報を取得するための技術的措置の制度化は必要。

○　匿名・流動型犯罪では、強盗の実行役として起訴され、その後の人生を棒に振ってしまうほどの重い処罰が課される例が大きく報じられているにもかかわらず、「目の前の高額報酬」に目がくらみ、強盗等の重大犯罪に関与する者が後を絶たない。

これらは、刑罰規定の持つ一般予防効果や特別予防効果が十分に機能していないということ。

匿名・流動型犯罪については、インセンティブとしても、犯行への関与ツールとしても、「通信手段」が鍵となっている構造があるため、それを踏まえた対応をすべき必要性が高い。

○　匿名・流動型犯罪グループ対策として、新たに技術的措置を導入する必要はある。例えばサイバー犯罪捜査の現場において課題となっているのは、犯罪者の行為に適当な対抗措置をとることができない点にある。

匿名・流動型犯罪グループによる犯罪が、財産に対してのみならず、人の生命・身体に対しても行われることに鑑み、警察としても相応の「武器」となる技術的措置を備える必要がある。

また、匿名・流動型犯罪グループによる犯罪は、国境なく行われるものであるところ、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諸外国のものと比べて狭いものになっているのが現状。技術的措置を導入することにより、そうした現状が改善されることを期待する。

○　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。

○　匿名・流動型犯罪グループのように散在型の犯罪者について物理的に追いかけることは容易ではなく、警察のリソースにも限りがあることから、必要な法制度を正面から設計し、実効的な被害防止を図ることが望ましい。

○　現行の刑事手続においては、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用アプリケーションによるやり取り等の内容を明らかにすることは非常に困難。そのため、現行の法制度のままでは、警察がいくら努力したとしても、匿名・流動型犯罪グループによる犯行を食い止めることはできない。

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ていること、また、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ことに鑑みれば、匿名・流動型犯罪グループに対する新たな技術的措置を早急に導入し、さらなる被害の発生を未然に防止することが強く求められている。

○　一般国民として、匿名・流動型犯罪グループ対策が隙のないものとすることを期待しており、新たに技術的措置を導入する必要はあると考えるが、プライバシーの侵害は可能な限り少なくなるようにしてほしい。

「実行犯を検挙しても上位の指示役を特定できない」という事態が現行法制度の限界であれば、また、新たな措置で技術的に解決できるのであれば、早急に実現し、また、被害防止のみならず、指示役の検挙にもつなげてほしい。さらに、闇バイトに応募した若者が重い罪に問われるような事態を未然に防いでほしいが、罪を犯していない段階の者も対象にするには、目的の部分で工夫が必要かもしれない。

○　被害者の受ける財産的打撃、精神的な打撃等は計り知れない。従前の刑事手続だけでなく、そういった悲惨な被害者を生まないための対策が急務。

新たな技術的措置の導入により、犯罪被害を阻止することだけでなく、犯罪に加担している自覚がない末端の者の犯行を未然に防ぐことにつながるのではないか。

イ　当該技術的措置を実施するための制度について

○　事業者が取り扱う通信に関する諸制度と比較して、個人の所有する端末に

おけるプライバシーに関する議論は憲法上も未成熟な分野。

電気通信事業法及び個人情報保護法により、事業者による通信ないし情報・データの取扱いに対しては公法的規律があり、またその規律によって利用者の通信の秘密ないし個人のプライバシーの保護を図る一方、公権力による事業者からの情報取得、いわゆるガバメントアクセスについても、憲法及びその趣旨を具体化する法律による規律が存在するところ。これに関しては、日 EU 個人データ越境移転に関する相互十分性認証や、OECD ガバメントアクセス宣言においても、日本は、法的根拠、比例性、透明性の確保等のグローバルスタンダードにコミットしてきたところ。

他方、端末に関するプライバシーについては、かつて電気通信事業法改正をめぐる検討に際して「通信関連プライバシー」としての保護を検討することが提唱されたことがあるものの、その場合には端末識別符号等が念頭に置かれていたところ。差し当たり、今回の対策において求められる、端末側において保存ないし閲覧される匿名性の高いＳＮＳアプリの通信内容については、電気通信事業法はともかく憲法上の通信の秘密の保護が及ぶとともに、「私的領域」であるパーソナルな端末であること、またその分量が多く他の通信等とも関連することから、プライバシーの保護が及ぶものとして考えるべきでないか。

その一方で、通信の秘密やプライバシーを適正手続の原則の下で必要な限度で制限して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、それぞれこの原則を具体化する形で定め、法的な規律の下で実施することを認めているところ。さらには、検証による通信傍受や装着型ＧＰＳ捜査に関する最高裁判例等において、憲法上の比較考量に関する確立された議論枠組みが存在するところ。

これらの従来の法制及び議論枠組みを踏まえて、通信傍受のように流れる音声やデータを捕捉するという継続的な措置か保存されたデータへの措置か、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していくというアプローチが合理的であると理解。

また、個人の権利利益の観点からは、取得する情報の個別性、また防止されるべき被害の重大性や切迫性等の情報取得を正当化し得る公益の内容及び措置により実現される程度の比例性も問題となり得るのではないか。

○　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、能動的サイバー対処能力強化法（以下「ＡＣＤ法」という。）の検討に当たって、こうした原則に加えて、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つつ丁寧な検討を行うべきであり、抽象的な議論のみで「許容される」あるいは「許容されない」との結論を得ることは適切ではなく、実体的な規律とそれを遵守するための組織・手続的な仕組み作りが必要であり、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とされたところ。

今回の検討に当たっても、こうした整理を参考としつつ、技術的措置により犯人使用端末内の情報を取得するという調査の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、そして調査を必要不可欠な手段とするところの被害防止のため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確保が求められるのではないか。

○　制度化に当たっては、情報取得のための技術的措置に加えて、収集した情報により被害が切迫している状況が明らかとなった場合には、そのような被害の発生や拡大を防止するために必要となる措置についても検討する必要があるのではないか。具体的には、情報取得の措置に加えて、取得した情報を用いて行う措置という、２つの措置の制度化が必要ではないか。

これらは行政措置として法律で定められるべきであると思うが、その際には、当然のことながら、憲法の理念に合致する制度、また、既存の法体系に適合するような制度とする必要がある。権限行使において濫用等の問題が起こらないよう、その規定振り、要件や手続の定め方については、慎重に検討しておくことが不可欠となると考える。

○　今回導入す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。この点、制度化に当たっては、様々な例が参考となると思われるが、有力な参照候補として、ＡＣＤ法が挙げられるのではないか。

○　内外・外内通信の取得に関する措置はＡＣＤ法に規定されており、これが、今回における情報取得の措置に相当するもの。その上で、深刻なサイバー攻撃の未然防止を実現するためには、具体的な手法・措置の実施が必要になるが、そのための措置が、アクセス・無害化措置として警察官の職務について規定する警察官職務執行法の６条の２において規定されているという関係にある。

このように整理ができるとすれば、情報取得の措置の１つの参考例はＡＣＤ法の規定ぶりとなるのではないか。

○　匿名・流動型犯罪グループに対処する場合には、「犯罪があると思料するとき」に行われる捜査、すなわち刑事司法上の手続として、新たな技術的措置を位置付けることも考えられ、それ自体にも、更なる犯行の抑止という意味での犯罪被害・犯罪加害の防止としての意義もある。

しかしながら、捜査は、証拠の収集と被疑者の特定とを中心に展開されていくものである一方、匿名・流動型犯罪グループ対策の構造的問題を踏まえた対処をする場合は、犯罪が成立する「直前」の段階・場面において、新たな技術的措置を講じ、より直接的かつ積極的に犯罪被害を防止すべき場合が多々あることが考えられる。そうであれば、警察法２条が規定し、それを受

けた警察官職務執行法１条にいう「犯罪の予防」、すなわち犯罪の未然防止等を目的とした行政的措置として、警察官職務執行法に位置付けることが望ましいと考えられる。

○　匿名・流動型犯罪グループは「警察等の目を盗んで」虎視眈々と機会を伺い犯罪を行うものである。そのため、より積極的な抑止のための介入をすべき状況が生じた場合に、犯罪の未然防止等を目的とした行政的措置として位置付けられる新たな技術的措置を実効的に行うことのできる権限とするためには、

・　対象者に察知されることなく密行的に行使できる権限であること。
・　犯行ツールとして使われるスマートフォン等の電子計算機端末の物理的な所在が不明であっても、電磁的記録の取得を可能とする権限であること。
・　犯罪被害が切迫する者に対する被害を防止するための情報の取得が認められること。

が必要となると考えられる。

○　新しい技術的措置を講ずる範囲等が確定していれば、解析技術に関してそれを公にする必要はないと考えられる。それは、犯罪捜査という文脈であるが従来から行われている捜索や、あるいは行政的な犯則調査における調査において、その対象範囲が確定していれば、捜索や調査等を実践するための手法を公にすることは必ずしも求められておらず、それは、捜索等の実効性を確保するためのものと解することができる。そうであれば、新しい技術的措置での解析技術に関して、それを公にすることは必ずしも求められず、むしろ秘匿性を重視すべきである。

○　現行の捜査で、被疑者の所持するスマートフォンやパソコン等の端末を差し押えた場合は、当該端末に記録された情報については、全体に関して解析を行った上で、犯罪の立証に用いるほか、将来の犯罪対策に資する警察活動にもつなげている。それは、犯罪捜査が、個々人に対する１回限りの活動ではなく、次々に発生する事件の解明を通じ、犯罪の抑止や、潜在的な被害者の被害防止等の正当な法益を保護するためであると考えられる。

それも踏まえた上で、新しい技術的措置を、仮に端末内の情報に対する継続性を有しない警察の権限として整理するとすれば、刑事訴訟法における差押えに関する要件・手続を一つの目安として、許容要件を構成することが考えられる。

○　従来の、通信傍受法や情報流通プラットフォーム対処法においては、事業者を巻き込む制度を構築することで対処してきたところ。しかし、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は、事業者を巻き込む制度設計は機能しにくい。

○　今回新たに導入すべきと考える技術的措置は、被害防止だけでなく、捜査においても有用となると思われる。他方、技術的にはメールのやり取り等を継続的に把握することも可能であるため、措置の継続性の有無に係る法的な

線引きと技術的な線引きを明らかにして議論していく必要性についても留意する必要がある。

○　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。

○　今回導入すべきと考える技術的措置については、警察が「遠隔」から犯行グループの端末にアクセスし、犯罪に悪用されているアプリケーションの通信内容等を迅速に把握・「解析」する措置であるため、仮の名称として「遠隔解析」という呼び方をするが、この「遠隔解析」の制度設計に当たっては、行政手続に位置付ける方向性と、刑事手続に位置付ける方向性の２つがあり得る。

もとより、刑事手続上の措置は、犯罪の予防と峻別されるようなものではなく、むしろ、警察実務においては、特定の犯罪の訴追・処罰に向けて刑事手続上の措置を取ることが、同時に、新たな犯罪の予防にも資するという場面が多く存在し、例えば、警察が電車内のスリの常習者を逮捕することが、新たなスリ被害の防止にも資するという事例等を挙げることができる。このように考えれば、今回導入すべきと考える「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、一概に否定されるべきではない。

しかしながら、警察がいくら「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、新たな実行犯を補充して犯行が継続されてしまうという匿名・流動型犯罪グループの犯行の構造に照らせば、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と考えられる。また、匿名・流動型犯罪グループの犯行を未然に防止する観点からは、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べき場面が多いと予想される。

これらの事情に鑑みると、今回新たに導入すべきと考える「遠隔解析」を、犯罪の予防や阻止を正面から目的に据えた行政手続上の措置として位置付けることに十分な合理性が認められる。

○　特定の制度を構築する上で設けるべき要件・手続は、警察がリアルタイムで継続的に情報を取得するか否かによって大きく異なる。具体的には、既に保存されているデータを一回的に取得するだけの郵便物の差押え・電磁的記録提供命令・検証の実施要件・手続と比べて、リアルタイムで流れてくる音声やデータを継続的に捕捉しようとする通信傍受の実施要件・手続は、相当に厳格なものとなっている。

○　今回新たに導入すべきと考える「遠隔解析」は行政手続上の措置として位置付けるべきであると考えているが、そのような法的位置付けにするとしても、当該措置によって継続的にデータを取得しようとするのであれば、やはり刑事手続上の通信傍受と同様に厳格な要件や手続を設ける必要があり、その結果、「遠隔解析」の実施件数も少なくなってしまうと予想される。

今回の有識者会議に求められているのは、匿名・流動型犯罪グループの犯行による未曾有の被害額及び人身被害の深刻さを前にして、それらの犯行に対抗するための実効的かつ機動的な措置を導入することであると認識しており、そのような観点からは、情報の継続的な取得を伴う措置の導入については将来的な課題としつつ、まずは、早急に行うべき緊急の立法措置として、犯行グループの端末に保存されているデータを一回的に取得するだけの非継続的な措置に限定して、「遠隔解析」の立法化を目指すことが合理的と考える。

○　現行の刑事手続において、警察は、裁判官の発付した令状に基づき、被疑者の所持するスマートフォンやパソコン等を被疑事実に関連する証拠物として差し押さえ、その端末内に保存されている情報を解析して、捜査活動に活用しているが、今回新たに導入すべきと考える「遠隔解析」は、対象となる端末を特定した上で、裁判官の事前の許可に基づき、当該端末内に保存されている情報を一回的に取得・解析する措置とするなら、オンラインにより遠隔で実施する点を除けば、現行の刑事手続で行われているスマートフォンやパソコン等の物理的な差押え及びその後のデータ解析と何ら異なるものではない。それゆえ、「遠隔解析」によって取得す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一つの目安になるのではないか。

ウ　当該技術的措置の導入に当たっての実効性・適正性担保について

○　今回の技術的措置は、行政手続による情報取得である場合でも、通信の秘密及びプライバシーの制約であり、またその程度も重大であることから、少なくとも裁判官による事前の司法審査が必要ではないか。

同時に、従来の差押えなどが事後の訴訟でのコントロールの存在を前提としていたところ、今回の対策が犯人グループの存在を契機としつつ、その後の被害を防止することに主眼があることからすれば、情報取得時の裁判官による事前審査だけでは、通信の秘密及びプライバシーの制約を正当化し、かつその範囲を相当なものにとどめるための統制として十分とはいえないのではないか。

具体的な対処としては、まず、一般的・抽象的な警察の責務規定にとどまらず、犯人グループによる通信内容を解明して、重大な犯罪の被害防止につなげるという警察活動に即した具体的な法的な根拠と位置付けを与えるべ

きではないか。また、被害防止の活動に従事する警察官と、そのために必要不可欠な調査のための措置を行う警察官又は所属の役割とをひとまず明確に分離した上で、調査の要件、調査により得られた情報の管理、被害防止の活動に従事する警察官への情報提供の範囲と手続等について明確な実体的規律を定めるべきではないか。

さらに、この実体的規律について、オペレーションの迅速性・実効性を確保しつつ、裁判官の事前審査を含めた適切な手続的統制を組み込むとともに、調査のための措置を行う警察官又は所属の専門性や組織的統制等に配意した制度設計を目指すべきではないか。

○　適正性の担保のためには、措置について、措置の権限の濫用等が生じないように、事前事後の手続の整備、手続の公正性と透明性とを確保することに留意すべきではないか。特に、情報取得の措置については、憲法上保障された通信の秘密に十分に配慮し、過剰な情報取得とならないよう、留意する必要がある。また、制度全体として、法執行において問題が生じないよう、制度的な担保が用意されていることも重要であり、具体的には、第三者機関による関与や、第三者機関への報告等の仕組みが考えられる。

また、高い専門性を有する警察官に措置を行わせるなど人材配置により、手続の適正性を担保することも考えられるのではないか。

○　実効性の担保とは、権限が適切に行使されその目的に沿った効果を発揮することを意味するものと思われるが、そのためには、制度自体が明確であり、実施現場における運用に際し疑問等が生じない、「使える」制度設計であることも重要。

○　新たに導入すべきと考える技術的措置に関しては、対象者のプライバシーの利益に対して著しい制約を加えるものであり、また、物理的な差押えと同程度の強制処分と捉えられるものであるといえる。そのため、仮に行政調査権限として位置付けるとしても、一定の行政手続については令状主義の要請が及ぶとする、最高裁判例の示す憲法第 31 条及び第 35 条の法意を考慮する必要がある。それゆえ、事前の司法審査制度を設けるとともに、適正手続保障の観点に十分に配意する必要がある。

○　今回新たに導入すべきと考える「遠隔解析」は、行政手続上の措置として位置付けるべきであるところ、憲法第 31 条や第 35 条が第一義的に想定しているのは刑事手続であって行政手続ではないが、「遠隔解析」は、刑事訴訟法上の捜査機関でもある警察が実施する行政警察活動上の措置であって、刑事手続とも密接な関連性を有しており、また、措置の内容も、対象者の意思に反して端末にアクセスし、同端末に保存されているデータを強制的に取得・解析するものとなることに鑑みれば、今回新たに導入すべきと考える「遠隔解析」には、憲法第 31 条及び第 35 条の保障が及ぶと解すべき。

○　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に課されている要件との均衡に照らし、警察が「遠隔解析」を実施する場合には、その対

象となる端末を何らかの方法で特定することが必要になる。ただし、対象となる端末が特定できるのであれば、具体的な特定方法は、電話番号であるとＩＰアドレスであるとを問わない。

また、憲法第 35 条の令状主義の要請や刑事手続上の既存の強制処分に課されている手続との均衡に照らし、「遠隔解析」を実施するための実体的要件や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司法審査を受けることも必要であると考える。先ほど申し上げた、対象端末を特定する要請と合わせれば、警察は、対象となる端末を合理的な根拠に基づいて特定し、それを裁判官に明示した上で、事前の令状審査を受けることになる。

その上で、「遠隔解析」を実施するための実体的要件としては、重大犯罪の予防を目的とする行政警察活動上の措置であることに鑑みて、第１に、重大犯罪による被害が発生するおそれ、第２に、被害発生を防止する緊急の必要性、第３に、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等を要求することが考えられる。

○　今回の「遠隔解析」は、その性質上、対象者に対して裁判官の令状を事前に呈示し処分内容を告知することはできない。そこで、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ことが必要である。

ただし、対象者の所在が不明であるなど通知をすることが困難な場合には例外的に通知を不要とし、対象者に通知することによって警察による犯罪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可能にすべきであると考える。

○　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、詳細な制度の内容は、しっかりと情報保全を図るべき。他方で、適正性担保も留意する必要がある。

○　今回新たに導入すべきと考える技術的措置は、対象者が認知できない密行的に実施する措置であり、事後救済を図るためにも、事後的担保手続が必要である。また、警察が適正に措置を実施したことを担保する観点からも、事後的担保手続は必要不可欠。

○　プライバシーの塊であるスマホを覗き見することは、原則的には許されないが、凶悪犯罪防止のためであれば、国民感情としても受け入れ可能。

目的、犯罪類型、対象者、取得するデータを限定し、当該犯罪と無関係のデータ、特に対象者以外の者のプライバシーに関わるデータを速やかに消去するといった明確なルールを定め、運用を徹底すべき。

加えて、消去の履歴も残し、ルールが適正に運用されていたことを第三者が事後的に監査し、結果を公表する仕組みも必要。検討から施行後を含む各段階で透明性を確保することで、国民の理解と受容性が向上する。

○　匿名・流動型犯罪グループが関与していると見られる犯罪の被害は、甚大なものである。国民を被害から守るためにも、一刻も早く実効的な対策を講

じるべき。

他方、その適正性担保については、司法手続であっても行政手続であっても、裁判官の令状あるいは第三者委員会の承認を得る手続をとることで担保できるものと考える。

エ　その他の御意見について

○　学校等での教育として、「実行行為を行ったら想像を超える刑罰を受ける」ことになり、一生を棒に振ることになるので、絶対やめるよう教える、実行行為に誘われても、指示者等の手口（実行行為者の住所・連絡先・家族構成・家族の氏名・年齢・勤務先などを聞いて来る）を事前に教え、これを聞かれたら途中でも止めるよう教えることが重要ではないか。

○　警察においては従前より、インターネットホットラインセンターにおいて犯罪実行者募集情報を削除するなど対策を講じているにもかかわらず、匿名・流動型犯罪グループによる犯罪は減少せず、今回検討しているような措置を導入せざるを得ない点も明らかにするべき。

○　以下の３点について整理してほしい。

・　対象が海外にいる場合の国際法的整理

・　偶然、クラウドサーバにアクセスするＩＤ・ＰＷを把握した場合のあり得べき措置

・　対象端末内に盗撮画像や児童ポルノ画像等他の犯罪への関与を示すものがあった場合のあり得べき措置

○　要件等については、継続性の有無等具体的な措置内容に応じて変わることから、今回の議論を踏まえて、事務局から具体的措置のイメージを示してほしい。

また、議論の参考資料として、川崎民商事件をはじめとする関連判例やＡＣＤ法に関する資料を整理してほしい。

○　議論の前提として「秘匿性」と「匿名性」の定義について、明確にしてほしい。

以　上