通信の秘密とプライバシーを脅かす遠隔アクセス権限を導入する警察官職務執行法改正案に反対し、徹底した国会審議と抜本的修正及び修正なき場合の廃案を求める声明

２０２６年１１月２日

自　由　法　曹　団
団長　黒　岩　哲　彦

政府は現在開会中の臨時国会において、匿名・流動型犯罪グループ（いわゆるトクリュウ）等の対策を理由に、警察官職務執行法（警職法）の改正案を提出した。本改正案には、犯罪の被害防止を名目として、警察が「犯人が連絡に用いた」と認めた「電子計算機」（スマートフォン、タブレット、パーソナルコンピュータ等）にネットワーク経由で遠隔からアクセスし、内部に保存された通信履歴や各種電磁的記録を複写・取得（遠隔解析）できる新たな権限（以下、「被害防止電子計算機調査」という。改正法案９条）の新設が盛り込まれている。

本法案には次に述べるように市民の基本的人権に対する過度の制約をもたらすなど極めて深刻な問題があり、現行の法文・枠組みのまま成立させることは到底容認できない。

1. 憲法が保障する「通信の秘密」「プライバシーの権利」の侵害

現代のスマートフォン、タブレット、パーソナルコンピュータは、個人の私信、位置情報、人間関係、生体情報、財産情報のほか、思想信条に関わるものから嗜好に至る多様な検索履歴などが包括的に集積された「個人のプライバシーの要衝」である。本法案は、これらスマートフォン等の端末に秘密裏かつ遠隔でアクセスし、現在進行形で生成される通信記録や位置情報、過去の通信履歴といった電磁的記録の取得・複写を認めるものであり、日本国憲法第 21 条第 2 項が保障する「通信の秘密」、および同第 13 条に基づく「プライバシーの権利」を明確に侵害する。しかも、複写・取得の対象となる情報に限定はなく、「切迫重大犯罪の実行に関する事項を示す情報」とされれば、様々な情報が際限なく複写・取得されてしまうことになり、プライバシー侵害の程度は極めて重大である。

2. 対象犯罪・発動要件の曖昧さと捜査権限の際限なき拡大

本法案では被害防止のための義務規定と結びつける形で遠隔調査権限が規定されているが、対象となる犯罪類型の絞り込みや「犯人が犯人間の相互連絡又は被害切迫者への連絡に用いたと認める合理的な理由」の判断基準が抽象的であり、運用の拡大解釈を許す余地が大きい。現に犯罪に使用された端末ではなく、「犯罪に利用される」と警察官が認めれば遠隔操作による端末の盗み見、情報取得が合法化されかねないのであり、市民のプライバシーを著しく侵す危険の高い手法である。しかも、現に犯罪に利用された端末ではない「計算機」（ここには、第三者名義の端末やサーバー等も含まれると思われる。）について「犯罪に利用されると認められる」根拠はなんなのか、どのような事情をもとにそのような判断ができるのか、法文にはなんらの基準も示されていない。

また、対象となる「重大犯罪」は「人の生命若しくは身体に危険を及ぼし、又は財産に重大な損害を及ぼすおそれのある犯罪」とされるのみで、通信傍受法のような対象犯罪の列挙がない。

本来、事案発生後の犯罪捜査を規律する刑事訴訟法ではなく、事前の危険予防を目的とする警察行政法（警職法）の中にこのような高度の強制処分に匹敵する権限規定を設けることは、要件の緩和や

司法警察活動への実質的転用（法規制の潜脱）を招く危険を強くはらんでいる。つまり、事実上、令状に基づく強制捜査を前倒しで令状もなく実行しようとするものと言える。

これは、犯罪捜査を目的とする司法警察活動でさえ認められていない活動権限を、犯罪捜査の前段階である行政警察活動の中で認めてしまうものであり、行政目的に比して明らかに過剰な手段を与えるものといえる。

3. 令状主義の潜脱による適正手続原則への抵触

法は、裁判官による許可を手続き要件としてはいるが、上記のように実体要件が不明確で、現在の令状発付の実際でも「人質司法」と批判されるような状態のもとでは、手続き要件が厳格に機能するとは考えにくい。また、裁判官の許可状の有効期間に法律上の規制はなく、長期間の調査も可能である。

電磁的記録の差押えでは令状の呈示や立会いが、通信傍受では対象犯罪の限定や事後の不服審査申立てが定められているのとは異なり、被害防止電子計算機調査は、令状の呈示も立ち会いもなく、対象者に知られないまま行われる。事後の通知も調査官の判断で先延ばしにされ得る。

また、実施に際しては、調査官はいったん網羅的に情報を取得することになる。「該当しない」情報を削除するとしても調査の終了後であり、「該当しない」かどうかの判断は調査官に任され、たとえ削除してもメモに残すことが事実上可能であって、プライバシー侵害の危険はなくならない。

このような潜入的な情報取得は、憲法第 35 条の令状主義が要求する対象の特定性や手続的正当性を実質的に形骸化させる恐れが強く憲法 31 条の適正手続原則にも抵触する危険性が高い。

4. 過去の警察による情報不正利用に照らした濫用への強い懸念

権限の行使にあたり一定の消去義務や事後通知規定が置かれているとされるものの、密行的に行われる電磁的記録の調査において、実効的な外部監視が機能するか極めて疑問である。事後の監督も、警察が事務局を担う公安委員会への報告にとどまる。過去、神奈川県警において廃棄処分すべき運転免許証の個人情報が長年にわたり公安部門へ不正に提供されていた事案をはじめ、警察組織内部における個人情報の目的外利用や情報管理の不透明さは度々指摘されてきた。厳格な第三者機関による常時監視や透明性が担保されないまま、警察に極めて強大なサイバー監視権限を付与することは、将来にわたり市民一般のプライバシーや市民運動・言論活動の監視へと濫用される現実的な危険を排除できない。

さらに、法第９条１項は、警察庁長官が警察官のうちから被害防止電子計算機調査官を指名するとしているが、これは、戦後警察の民主化の柱であった都道府県警察への分権という構造を変えてしまい権限の集中した国家警察作りを促進する危険性が強い。それとともに、大垣警察市民監視事件名古屋高裁判決（２０２４年９月１６日）が指摘したとおり、第三者機関による法的統制もなしに警察の権限の拡大を図ることの危険性も重大である。

5. 国外の端末への適用と主権侵害

本法案第９条には、対象となる端末の所在地の限定がないという問題もある。特殊詐欺は国外の拠点から国内の被害者に連絡する形態が典型であり、国外の端末への適用こそが本法案の主要な使途となりうる。しかし、他国の領域における端末に、その国の同意なく侵入して情報を取得することは主権侵害のおそれがある。「サイバー犯罪に関する条約」が国際捜査共助によらない越境アクセスを認め

るのは、公開されたデータか、開示する正当な権限を有する者の同意がある場合に限られる（条約第３２条）。日本の裁判官の許可のみで、他国領域での公権力の行使を正当化することはできない。

6. 弁護士との秘密交通権の侵害

さらに、犯罪への関与を懸念した者が弁護士に相談した場合もその情報が踏査され得る。その結果、弁護士との秘密交通権を侵害し、弁護士との相談の機会が奪われ、ひいては被疑者・被告人の防御権が侵害されたり犯行を思いとどまったりする契機を失いかねない。

7. 結論

以上、国会は、トクリュウなど治安対策の必要性のみを過大に強調することなく、本法案がはらむ憲法上の問題等について慎重かつ徹底的な審議を尽くすべきである。報道によれば拙速なスケジュールで成立させることを予定しているようであるが、慎重な審議なしに成立させることはあってはならない。

また、少なくとも要件の厳格な限定、対象犯罪の極めて厳正な絞り込み、令状審査基準の明確化、取得した情報の捜査・公判への利用の禁止、国外端末への適用の排除、国会への報告と実施状況の公表、そして独立した第三者機関による実効的な事後検証システムの確立など、市民の権利擁護に足る抜本的な修正が必要である。自由法曹団は、これら抜本的な修正を求め、本改正案の成立に断固として反対し、廃案とすることを求める。

以上