令和 8 年 11 月 13 日

警察官職務執行法改正案

立憲民主・無所属
参議院議員　石垣のりこ

立憲民主党の石垣のりこです。

会派を代表してただいま議題となりました「警察官職務執行法改正案」について質問します。

本法案は、匿名・流動型犯罪グループ、いわゆるトクリュウによる強盗や特殊詐欺等の被害を防止するため、被害が差し迫った者に対する保護措置を整備するとともに、重大犯罪に使用されたスマートフォン等の端末に遠隔で接続し情報を取得する「被害防止電子計算機調査」を可能にするものと説明されています。

トクリュウによる犯罪が深刻な社会問題となっており、その被害を未然に防止するための対策が必要であることは言うまでもありません。

しかし、目的が正当であれば、どのような手段も許される訳ではありません。新たな調査手段を導入するのであれば、その実効性だけでなく、人々のプライバシーや通信の秘密を侵害することがないのか、また、社会全体のサイバーセキュリティに新たな危険を生じさせることがないのか、慎重に検証する必要があります。

特に、今回議論されている「遠隔解析」という手法は、端末に外部から接続し、内部の情報を取得するための技術的な措置を伴うものです。しかし、その仕組みや、使用するプログラムの機能について政府は「犯人側から対抗措置を講じられ、被害防止措置に支障が生じるおそれがあることから、お答えすることは差し控えさせていただきます」との答弁を繰り返すばかりです。

また、この半年の間には、AI を悪用したと思われるサイバー攻撃が相次ぎ、中には自律型 AI エージェントによる攻撃を受けた可能性を指摘する企業もあります。

防衛省防衛研究所も、十月三十日発行の NIDS コメンタリーにおいて、AI によってサイバー攻撃の規模と速度が大きく変化していることを指摘しています。

このように、サイバー攻撃を取り巻く環境が大きく変化している中で、今回導入しようとする「遠隔解析」の安全性についても、従来とは異なる観点から検証する必要があります。

以上を踏まえて、国家公安委員会委員長及び関係大臣に、質問します。

1.　今回の警察官職務執行法の改正は、現行法の下では不正アクセス行為の禁止等に関する法律その他の法令に抵触する可能性のある他人の電子計算機への接続や情報取得、いわゆる、不正アクセスを、一定の要件の下で警察官が適法に実施できるようにするための法的根拠を設けるものだと理解しています。

つまり、今回導入する「遠隔解析」には、法改正がなされていない現段階では違法となる行為も含まれるのか、国家公安委員長、明確にお答えください。

2. 衆議院での審議で、政府は、今回の「遠隔解析」について、対象端末に接続し、その時点で端末内に存在する情報を一度だけ取得するものであり、通信の内容を継続的に監視するものではないと説明しています。つまり、「遠隔解析」を実施した時点で、調査に必要な情報が端末内に残っているとは限らないということです。

政府は、どのような根拠に基づき、「遠隔解析」を実施する時点で必要な情報が端末内に存在すると判断するのか、「遠隔解析」を実施したが、必要な情報が存在しないという空振りも多く発生すると考えますが国家公安委員長の見解を伺います。

3. 今回の制度では、「遠隔解析」の対象を「重大犯罪に使用されたと認める合理的な理由のある端末」としています。しかし、対象となる端末は犯罪に使用された端末だと答弁すればするほど、犯罪グループ側が対抗措置を取りやすくなってしまうのではないでしょうか。

具体的には、犯罪に使用した端末の使い回しをやめて、事件ごとに端末を変更したり、全く犯罪と関係ない第三者に譲渡したり、実際の犯行計画や指示は別の端末でやり取りし、警察が解析する可能性のある端末には偽の情報を残すなどの対抗措置を取ることが容易に想像できます。

国家公安委員長に伺います。政府は、こうした犯罪グループ側の対抗措置をどの程度想定しているのでしょうか。また、そうした対抗措置を講じられた場合にも「遠隔解析」の実効性を確保できると考える根拠を明らかにしてください。

4. 今回の「遠隔解析」によって、トクリュウの実行役や指示役だけではなく、その背後にいる首謀者、いわゆるラスボスの特定及び検挙、犯罪組織網の実態解明につながると考えていますか。たとえ、端末から取得できる情報によって、犯罪の実行役や末端の指示役を特定できたとしても、資金の流れを支配し、犯罪全体を指揮する首謀者にはたどり着けないのではないでしょうか。今回の制度によって、どのような犯罪者の検挙や被害防止が可能になると見込んでいるのか、国家公安委員長、具体的にお示しください。

5. 警察庁に事前に確認したところ、令和３年以降の過去５年と本年令和８年に、暴力団員及び匿名・流動型犯罪グループのメンバーに捜査情報その他の職務上知り得た情報を提供するなどして、懲戒処分を受けた警察職員は十二人にものぼるとのことでした。これは事実でしょうか。国家公安委員長に伺います。

6. 今回の改正によって創設される被害防止電子計算機調査官が取得する情報は犯罪組織にとって極めて価値の高いものです。犯罪組織が調査官に対して、調査官本人やその家族

への危害をほのめかして脅迫したり、多額の金銭で買収したり、ハニートラップで籠絡したりする可能性も想定しなければなりません。こうした犯罪集団に対して、調査官個人の倫理観や守秘義務の自覚に委ねるだけで、通信の秘密を守ることができると考えているのか。国家公安委員長に政府の認識を伺います。

7.　今回の「遠隔解析」は、特定の人物を対象とするのではなく、過去に犯罪に使用された端末を対象とするものです。したがって、犯罪に使用された時点と「遠隔解析」を実施する時点で、端末の使用者が変わっている可能性があります。犯罪とは無関係な第三者が使用している端末に接続し、その通信内容や個人情報を取得することも起こり得ると考えますが、通信の秘密やプライバシー侵害との関係を考慮してもなお、許容される調査だと考えているのか政府の見解をお示し下さい。国家公安委員長にお伺いします。

8.　本法案第九条第六項では、裁判官の許可に係る対象電磁的記録に該当しない情報を取り扱った場合、これを他の者に提供してはならず、調査を終えた後に消去することとしています。この場合、該当しない情報は消去することになりますが、調査官が見たことには変わりなく、記録は消せても記憶は消すことができません。

令状によって取得が認められていない情報を調査官が閲覧すること自体が、プライバシーや通信の秘密を侵害することになると考えますが、憲法第二十一条第二項の検閲の禁止や通信の秘密との関係も含め、国家公安委員長、政府の見解をお示し下さい。

9.　サイバー攻撃を取り巻く環境は、AI の進歩によって大きく変化しています。先月あたりから情報漏洩のニュースを耳にしない日はなく、先月公表された国内のサイバー攻撃の数は、過去最多の 233 件に達したとの報道がありました。

特に大きな変化として、AI が攻撃の一連の工程を自動化し、人間が個々の操作を行わなくても攻撃を進めることが可能になっていることについて、政府はどのように認識しているのかサイバー安全保障担当大臣、明確にお答え下さい。

10.　AI を利用した攻撃では、人間が想定していた範囲や権限を超えて AI エージェントが行動した事例も報告されています。今回の「遠隔解析」に使用するプログラムについても、自動的に侵入方法を選択したり、情報を収集したりする機能を備える可能性があるのではないでしょうか。使用するプログラムが、調査官の指示や認識を超えて想定外の動作を行う可能性について、どのような検証を行っているのか国家公安委員長、明らかにしてください。

11.　仮に「遠隔解析」によって侵入した端末が他の端末と通信している場合、その通信相手の端末にも侵入し、情報を取得することが技術的には可能と考えますが政府の認識はいかがですか。例えば、対象端末の通信履歴や連絡先等から通信相手を特定し、その端末

にも侵入を試みるような機能を調査官が使用するプログラムが備えている場合、当初の調査対象とは異なる端末にまで調査が拡大することはありますか。また、調査官が意図していないにもかかわらず、プログラムの自動処理によって別の端末への侵入や情報収集が始まる可能性はないと断言できるでしょうか。国家公安委員長にお伺いします。

12.　トクリュウは、犯罪によって得た収益を資金源として、国内外の高度な技術者を高額な報酬で雇用したり、サイバー犯罪を専門とする集団から技術やプログラムを調達することも可能であると考えます。一方、警察の技術者は、公務員としての給与体系や予算、調達手続などの制約を受けることもあり、警察側の技術力が常に犯罪グループ側を上回るとは限らず、場合によっては犯罪グループ側がより高度な技術力を有することも考えられます。

このような犯罪グループが、警察による接続を検知して通信手段を変更したり、警察のプログラムを解析して逆に悪用したりする可能性について、どのような検証を行っているのか。また、犯罪グループ側の技術力が警察を上回った場合、どのような対応を取るのか、国家公安委員長、お答えください。

13.　政府は、昨今の AI を悪用したサイバー攻撃の高度化・大規模化を踏まえ、十一月五日に、国家サイバー統括室から事業者等に対し、脆弱性の継続的な把握と速やかな修正・解消を求める要請を出すなど、社会全体でサイバー攻撃への対策を強化しています。

一方、警察が被害防止目的とはいえ、脆弱性を利用し、その修正を遅らせるような「遠隔解析」という手法を認めるのであれば、政府全体のサイバーセキュリティ政策と矛盾するのではありませんか。

脆弱性を利用して対策を進める間に、その脆弱性がハッカー集団に利用されて別の被害が発生するなどの事態が生じないとは言い切れません。犯罪防止上の必要性と国民全体のサイバーセキュリティの確保をどのように両立させるのか、政府全体として一貫した方針を明確にしてください。国家公安委員長にお伺いします。

14.　警察が被害防止目的で利用した脆弱性について、調査終了後に端末の製造事業者等に通知し、修正を促す仕組みはあるのでしょうか。

遠隔解析に際して、既存の脆弱性を利用するだけでなく、端末に侵入するために新たな脆弱性を作り出したり、既存の脆弱性を拡大させたりする可能性はないのですか。

警察が端末に侵入するために利用した脆弱性や、送り込んだプログラムがトクリュウ自体や第三者によって解析され、悪用される可能性も否定できません。

また、当該端末が第三者によるサイバー攻撃の踏み台として利用される危険もあります。

つまりは、警察の「遠隔解析」が、結果として犯罪グループに新たなサイバー攻撃の手段を提供することになり得るのです。このような懸念について、どのような安全対策を講じるのか具体的に明らかにしてください。国家公安委員長にお伺いします。

15.　今回の改正によって導入される「遠隔解析」と同様の手法を、今後、公安調査庁や国家情報局などのインテリジェンス機関が、治安維持や安全保障を目的とする予防的な情報収集活動に導入することを、政府として検討しているのではないかと懸念する声が届いています。治安維持や安全保障を目的とした予防的な情報収集に広げることはないと断言できますか。内閣官房長官にお伺いします。

16.　また、今後、重大犯罪に関与したと認められる端末に限らず、犯罪予防のため、犯罪に関与する疑いのある者の端末に接続して情報を取得するなど対象を拡大することはないのか、検討しているか否かも含めて、国家公安委員長の明確な答弁を求めます。

繰り返しますが、トクリュウによる犯罪被害を防止することの重要性はいうまでもありません。しかし、これまで述べてきた通り、今回の警職法改正案は、プライバシーの侵害や通信の秘密を脅かすことへの懸念だけではなく、犯罪グループに偽情報をつかまされて調査や捜査を混乱させるおそれや、調査に脆弱性を利用することで、かえって新たなサイバー攻撃の危険を生み出し、社会を危機に陥れる可能性すらあります。

自律型AIの進歩によってサイバー攻撃の脅威が急速に高まる中、社会全体で脆弱性の発見と修復に力を注いでいるにもかかわらず、警察がその脆弱性を利用することによって、国民全体に取り返しのつかない不利益を及ぼすことにならないのか、極めて大きな懸念があります。

犯罪を防止するための制度が、かえって犯罪を助長し、国民を危険にさらすことになっては本末転倒です。政府には、制度の実効性と安全性を改めて厳しく検証することを求め、質問を終わります。