戦争と一体の先制的サイバー攻撃法を廃止しよう！
通信の秘密、表現の自由を守ろう！

2025 年６月５日

共謀罪 NO ！実行委員会
「秘密保護法」廃止へ！実行委員会

ネット監視・先制サイバー攻撃法案（いわゆる能動的サイバー防御法案）が 5 月１６日、参議院本会議で採決され、成立しました。私たちは戦争と一体の同法案の採決を満腔の怒りをこめて弾劾するものです。同法案に反対したのは共産党、れいわ新選組、沖縄の風でした。この事実の中に石破政権による日本の戦争する国への転換の攻撃が進むなかで、恐るべき勢いで政党の翼賛化が進んでいることをみてとることができます。

私たちは戦争と一体の同法を絶対に認めることはできません。同法の廃止を求めてたたかい続けていくとともに、その施行過程を厳しくチェックしていくことを宣言します。

警職法「改正」で警察・自衛隊が侵入・無害化？！

ネット監視・先制サイバー攻撃法（以下同法と略）の大きな問題は、サイバー空間における警察、自衛隊の先制攻撃が、自衛隊法の「改正」ではなく警察官職務執行法（以下、警職法と略）の「改正」を軸に行なわれることになったことです。これは実に重大な問題です。

侵入・無害化は、他国のネットワークに侵入し、攻撃の元とされるサイバーの機能を無効化するものであり、他国の主権を侵害するものです。そもそも警職法は国内を対象としたものであり、外国を対象としたものではありせん。能動的サイバー防御の名のもとに警察権の及ばない外国の地域に、権限を及ぼそうとする同法の「改正」を認めることはできません。

そもそもいわゆる能動的サイバー防御問題は、一昨年の安保三文書で先制的敵基地攻撃能力の保有と一体のものとして示されたものです。この点からも明らかなようにそれは自衛隊の課題としてだされたのです。ところが、法案は警察権の行使の問題として警職法の「改正」として打ち出してきたのです。それは、自衛隊法「改悪」で自衛隊が先制的なサイバー攻撃をできるとしたならば、先制的敵基地攻撃と一体のものとして批判がでることを恐れ、それを避けるための苦肉の策でした。そこで先制的サイバー攻撃を警察権の行使として、警職法の「改正」で対応するというペテンにでたのです。そもそも警察庁は能動的サイバー防御に関する有識者検討会では、この問題について警職法「改正」で対応するのは次元が違うのではないかとさえいっていました。ところが、警察、自衛隊の侵入・無害化は警職法の「改正」でおこなうこととされたのです。

そして、防衛省・自衛隊は警察を前面にたてながら能動的サイバー防御の目的である攻撃元とされる他国のサイバーに内閣総理大臣の命令で侵入・無害化できる通信防護措置の権限を自衛隊法８１条３を新設することで手に入れたのです。それだけではなく治安出動時、防衛出動時などの４つの類型において、「改正」された警職法を準用することで侵入・無害化ができるようになりました。

全市民監視型システムの導入に踏み込む

政府は能動的サイバー防御の名のもとについに全市民監視型システムの導入に踏みきりました。

全市民監視型システムの導入は、政府・警察庁にとって１９９９年の盗聴法制定以来の

念願でした。その野望が表面化したのが２００１年のメール盗聴装置の導入でした。警察庁は、それまでメール盗聴は、裁判所の令状にもとづくメールを通信事業者からフロッピーで渡してもらえばよいとしていましたが、その説明を覆し、警察庁のメール盗聴装置を通信事業者のメールサーバに接続し、そこにすべてのメールを通し、裁判所の令状にもとづくメールのみをピックアップするとしたのです。しかし、警察庁はその装置のプログラム、仕様などを明らかにしませんでした。これでは裁判所の令状と無関係なメールが盗聴されてもわかりません。警察庁は、通信事業者の批判と世論の反発で同装置をつかうことはできず、結果としてすべてのメール盗聴装置を廃棄せざるをえませんでした。

政府は同法で２００１年のメール盗聴装置などとは比較にならない大規模な形で事業者、市民などの通信を監視するシステムを導入することができるようになります。それは外外通信、外内通信、内外通信、内内通信などのすべての通信を対象とすることができるからです。最初は、世論の批判を恐れ、監視する通信の範囲を制限することにするでしょうが、それは政府にとって大した問題ではありません。全市民監視システムが導入されれば、対象通信の範囲を拡大していけばよいだけのことだからです。

国会で自動選別装置の検証を！

政府は、通信の秘密が侵害されるのではないかという危惧、批判に対して、「自動選別装置は通信の内容は対象としない」、「ＩＰアドアレスのなどの機械的情報だけしか取得しない」としていますが、同法に賛成した政党もふくめ政府の説明に信頼をおいているわけではありません。それは、この間、政府が公文書の偽造、破棄などの数々の悪行をおこなってきたからです。

国会は、市民の通信の秘密が侵害されないように、本当に政府の言うように自動選別装置が機械的情報だけを取得し、そのほかの情報は消去されるのか、不正が行われる余地はないのかなどチェックする専門機関をつくり、同装置の検証をすべきです。

この点についていえば、２０１９年の盗聴法改悪をめぐる議論がおこなわれていたなかで、立会人制度をなくし、警察で直接盗聴するというシステムの導入に当たって、警察庁が自らの提案の妥当性についての検証をデロイト・トーマツ・コンサルティング株式会社に依頼していたことは重要です。警察庁としては、盗聴法改悪のために警察に対する不信を払しょくするためのやむを得ない検証の依頼だったのでしょう。本来ならば、政府が同法の自動選別装置の信用性について検証するための措置をとるべきだったのです。そうした措置がとられていない以上、国会がこの自動選別装置について市民の通信の秘密を守れるのか検証すべきです。

通信事業者への圧力を許さない

この先制的サイバー攻撃は通信事業者の全面的な協力なしに成立しません。なぜなら世界にはりめぐらせた通信事業者の通信網をとおして通信がおこなわれているからです。報道によれば、政府と通信事業者の協定について、通信事業者のなかには「民間から情報を吸い取るだけではないか」などの声がでており、慎重な態度をるところもあるといわれています。それは政府と変な協定を結べば、その事業者から利用者が離れ、通信の秘密を守る事業者のところにいってしまうかもしれないからです。能動的サイバー防御態勢は、すべての通信事業者の参加を必要とします。そのため政府から通信事業者に対して協定の締結をもとめる圧力が強まることは疑いありません。私たちは通信事業者の自主性を尊重するよう政府に強く求めるとともに、通信事業者には政府と協定の内容の公表を強く求めていきます。