政府への通信情報提供システムはサイバー攻撃に対する脆弱な仕組みの導入にしかならない――改めてサイバースパイ・サイバー攻撃法案の廃案を訴える

* 新たなサイバー攻撃の格好の標的としての「バックドア」

サイバースパイ・サイバー攻撃法案[1]は現在参議院で審議中です。この声明に署名した各団体はこれまでも本法案の廃案を強く求めてきました。今一度廃案にすべき理由を述べ、本法案を提出した政府や法案に賛成した野党各党に、改めて廃案とするよう訴えます。

通信情報を政府に提供するシステムはサイバー攻撃者にこれまでにない新たな通信情報へのアクセス手段を与えることになります。

サイバー攻撃など情報通信ネットワークへの加害行為は、組織の内部と外部のインターネットなどとを繋ぐ情報通信の出入口にあたる部分を標的にします。この出入口を防御するために必要な「戸締り」をすることが通信事業者等ネットワーク管理者の役割でもあります。建物の出入口の安全を確保するために必要な「戸締り」をすることと同じです。

組織内部の情報の完璧な安全を実現するには、外部との情報の出入りを認めず組織内部の情報通信を完全に外部から隔離して密閉してしまう以外の方法はありません。しかし、この仕組みでは、組織の外部との通信は不可能になり、情報通信が果すべき本来の外部との通信機能を損なうことになります。どうしても外部との情報通信のための「出入口」が必要になります。

本法案は、警察や自衛隊等政府機関が通信情報を利用できるように、既存の「出入口」とは別の裏口――バックドアと呼びます――を通信事業者等が設けることになります。つまり、政府への通信情報の提供のために、組織の外部との出入口を、もうひとつ作る、ということになります。ネットワークへの違法な侵入者にとって、このバックドアは、これまでにはなかった新たな侵入可能な出入口になります。たとえていえば、建物の安全を確保するために、これまであった出入口以外に「警察官専用入口」のようなドアを設置するようなものです。攻撃者からすれば、攻撃可能な箇所が更に一箇所増えたことになります。

政府は、バックドアは完璧に外部からの違法な侵入を防御できるものだ、と主張するでしょう。しかし、このバックドアを通信情報が行き交い、これを管理する人たちは、このドアの鍵の開閉ができる以上、故意であれ過失であれ、このバックドアは脆弱な性質を持たざるをえないのです。しかも情報通信を網羅的に収集する技術的な可能性を与えるこうしたバックドアは、サイバー攻撃に対してより脆弱な条件を政府自らが作ることになり、法案が意図することとは真逆の対応にしかなりません。

ネットワークのセキュリティの基本は、外部との接点を必要最小限とし、システムを可能なかぎりシンプルにして、通信情報の利用を本来意図されたユーザー以外にはアクセスさせないような環境を確実に構築することにあります。今回の法案は、このセキュリティの基本そのものを大きく逸脱しています。

従って、通信事業者等は、本法案が求めるような政府との協定に応じるべきではありません。改めて通信事業者の皆さんに、通信事業者が果すべき社会的な責任に基づきて、本法案への反対の意思表示を示してほしいと思います。

* 政治活動家、人権活動家、ジャーナリストなど政府にとって不都合な人々が標的になる

本法案には様々な情報収集と分析についての文言上の歯止めが書かれています。しかし、私たちはこの文言がどのようなものであれ、政府が通信情報を網羅的に収集できる技術的な能力を持つことになる以上、網羅的な収集と監視とスパイ行為は防げないと考えます。

---

1 正式名称は「重要電子計算機に対する不正な行為による被害の防止に関する法律案」「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律案」

残念ながら、法律は技術を完全に制御できていません。スピード違反の自動車が存在するのは、技術的に法定速度以上のスピードを出せる車の製造が可能だからです。本法案の場合も同様です。法律で通信情報の収集に様々な歯止めの文言があったとしても、技術的な歯止めを設けていません。国会では通信情報の収集についても、サイバー攻撃の手法についてもプログラムなどの技術的な内容を検討していません。したがって、情報収集の仕組みが構築されれば、自動車同様技術的には違法行為が可能な状態になりうる危険性があることを強く危惧します。

この情報収集の危険性については様々なケースが想定されます。

国会に議席をもつ野党の議員たちに対する情報収集の手段に用いられる可能性があります。選挙に不利になるようなプライバシー情報や外部には出されないはずの党内の議論など、情報通信システム上のデータが政府側に筒抜けになることを覚悟する必要があります。あるいは、与党の議員であっても「身体検査」の手段として、技術的には通信情報を用いることが可能です。

ジャーナリストは、内部告発者も含めて情報源となる人たちとの接触に伴う通信情報が政府側に把握される危険性が極めて高くなります。この場合、取材先の人たちの安全も確保できなくなります。こうなれば、取材相手はより一層警戒し、取材に応じなくなる可能性があります。こうした事態は、権力犯罪を暴露することを困難にし、明らかな報道の自由の侵害ともなります。

弁護士の場合も同様です。通信情報が政府側に把握されるために、依頼者との通信の秘密は技術的に確保できなくなり、依頼者の安全を確保できなくなり、訴訟等の内部情報が漏洩する危険性が高くなります。とくに国などを相手とする権力犯罪と立ち向かう弁護士にとって、相手側の国に情報を把握されやすい状況が技術的に生み出されてしまいます。

政府の政策などに反対して活動している活動家たちにとっても、自分たちの人間関係や組織実態などをこれまで以上に詳細に、警察などによって把握される技術的な環境に晒されます。とくに、日本国内で、移民・難民など海外にルーツをもつ人たちと一緒に活動している団体や個人は、海外との通信へのより厳しい監視に晒されます。また、米軍基地に反対する運動は、日本政府を通じて反対運動に関わる通信情報を米軍などへも提供することがより容易になる環境に晒されます。

言うまでもなく、網羅的な通信情報収集のバックドアは、人々の日常的なプライバシーに関わる情報を政府が把握することにもなり、社会的な活動に関わっていなければ、監視やスパイの対象にならない、ということではありません。

* それでも法案に賛成しますか？
国会議員の皆さんに問います。本法案は、これまでになかった新たなサイバー攻撃に対する脆弱なバックドアを作ることになります。それでもなお本法案に賛成ですか。

上記に述べた本法案のバックドアに関する問題は、法案全体の問題のごく一部に過ぎません。重要でありながら全く国会の審議では議論にすらなっていないために、ここに問題提起するものです。ぜひこの問題に注目し、法案について廃案とするよう、国会議員の皆さんに訴えます。

2025 年 5 月 12 日

署名団体
JCA-NET
ATTAC 首都圏
反監視情報
ふぇみん婦人民主クラブ

(今後増える予定)