能動的サイバー防御法案に対する意見書

～国民監視と先制攻撃の危険な問題点を解明する～

自由法曹団

１　何をしようとする法案か

(1)　提出された法案は

本年２月７日、政府は、能動的サイバー防御法案を国会に提出した。「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（サイバー対処能力強化法）と「同法律の施行にともなう関係法律の整備等に関する法律」案（同整備法）という２法案である。

本法案は、第一に、サイバー攻撃事案を基幹インフラ事業者に報告させることにしており、これを罰則をもって強制する。第二に、被害防止のために平時から基幹インフラ業者をはじめ、国民の送受信する通信情報を取得してサイバー空間を監視し、把握する制度を設けている。第三に、サイバー攻撃のおそれのある場合には、攻撃者を検知して攻撃元のサーバー等へ侵入して事前に無害化する措置をとれるようにする攻撃的な対応を可能とする制度が導入される。

同法案は、政府がサイバー空間を広く把握し、国外のコンピュータシステムにも介入して「無害化」の名のもとに攻勢的な活動を認める内容となっていることから、「サイバー先制攻撃法」というにふさわしい危険な法案である。

(2)　サイバー攻撃と犯罪防止

法案は、「国家及び国民の安全を害し、又は国民生活もしくは経済活動に多大な影響を及ぼすおそれのある国等の重要な電気計算機のサイバーセキュリテイを確保する重大性が増大している」としたうえ、不正なサイバー攻撃による「被害の防止を図る」ことを目的として提出されたと説明されている（法案提出の「理由」）。

確かに、ロシアによるウクライナへの侵略戦争においては、サイバー攻撃により予め破壊工作を準備し、武力攻撃と組み合わせた「ハイブリッド戦」が行われたともいわれている。また、民間飛行機の運行や銀行取り引きが機能麻痺する事態が発生するなど、経済や情報、国民生活に不可欠な基幹インフラのシステムの機能を混乱･停止させるサイバー攻撃も行われている。

しかし、そもそもサイバー攻撃は、相手方のシステムに不正にアクセスして、混乱させたり機能を停止させたりする犯罪行為であり、それを防止する犯罪対策として検討される必要がある。実際、不正アクセス行為禁止法（１９９９年）、さらには刑法改正（２０１１年）により、不正にアクセスしてデータを書き換えたり、取得したりする行為などについて犯罪として処罰する規定がつくられてきた。そして、犯罪捜査のために、リモートアクセスやサーバーへの捜索・差押などの手続きも進められるようになっていった。そして、２０１３年には、サイバーセキュリテイ基本法が制定され、事業者・教育研究機関、行政機関における対策が進められ、戦略本部が設置されるに至っている。

国境を越えるサイバー攻撃に対してはサイバー犯罪から社会を保護するための国際協力を確認したサイバー犯罪条約が２０１２年に発効し、その強化が図られるとともに、２０２４年１２月には、国連サイバー犯罪条約が国連総会で採択されるなど、国際間での協力、対策の強化が進められている。

このようにサイバー攻撃に対しては犯罪捜査の範囲内で必要な立法等の措置がとられている。

(3)　人権と平和を危うくする法案

本法案は、上記のような従来の犯罪捜査の範囲を超えて、インターネット通信を国の支配、監視下におくとともに、国外のコンピュータ等に対してもプログラムを停止・削除等して相手国の軍事・経済への攻撃、先制攻撃にも及ぶ措置を認めるものである。憲法で保障している通信の秘密を侵し、憲法の平和主義に反するおそれ

がある。

自由法曹団は、本法案によって実施されようとしている政府の措置等に関して、それぞれ問題点と危険性を指摘するとともに、法案のねらいを明らかにするために、本意見書を作成した。

平和と人権を危うくする本法案は、速やかに撤回するべきである。仮に撤回されないとしても、本意見書で指摘した問題点やねらいを多くの国民に知ってもらうとともに、国会審議において問題点を明らかにして廃案にするべきである。

２　罰則で報告を強制

(1) 罰則により基幹インフラ事業者に対する報告を強制

法案は、基幹インフラ事業者に対して、①特定重要電子計算機（サイバーセキュリティが害された場合に、特定重要設備の機能が停止し、又は低下するおそれがある一定の電子計算機）を導入したときは、その製品名等を事業所管大臣へ届出ること（４条）②不正アクセス行為等により特定重要電子計算機のサイバーセキュリティが害されたこと又はその原因となり得る一定の事象を認知したときは、その旨及び一定の事項を事業所管大臣及び内閣総理大臣に報告することを義務付けている（５条）。情報提供の対象となる事業者は、基幹インフラ事業者とされる鉄道、航空、郵送、金融、電気、ガス、水道、放送など５３社２１３事業所である。

基幹インフラ事業者がインシデント報告等を行わず、是正命令を受けても対応しない場合２００万円以下の罰金（８３条）、基幹インフラ事業者がインシデント報告等に関連し、資料提出等を求められても対応しない場合３０万円以下の罰金が定められている。

なお、内閣総理大臣は、サイバー攻撃による被害の防止のため、重要電子計算機を使用する者など（あらかじめ同意を得た者に限る）を構成員とする協議会を設置し、構成員に守秘義務を伴う被害防止に資する情報を共有及び必要な資料提出などを求めることができる（４５条）。

(2)　政府による情報提供の強制

政府は、サイバー法案は、官民の連携を強化して、サイバー攻撃から国民生活を守るための法律であると謳っている。しかし、その内容は、経済安保法で定められた基幹インフラ事業者に対して、罰則のもとで、情報提供を行わせる内容となっており、官民の「協力」ではなく、政府による情報提供の「強制」である。経済活動に対して権力が介入する余地をいっそう広げることとなる。

３　通信情報の取得と選別

(1)　政府による通信情報の取得

ア　同意によらない通信情報の取得

政府は、不正行為に用いられるとの疑いがあるときは、送受信者の同意なくして、次の通信について通信情報を把握できる。

①　外外通信（１７条）～ＩＰアドレスなどから判断して国外設備を送信元及び送信先とする電気通信に該当する電気通信であって、国内設備を用いて媒介されるもの

②　特定外内通信（１１条、３２条）～ＩＰアドレスなどから判断して国外設備を送信元とし、国内設備に送信される電気通信

③　特定内外通信（３３条）～ＩＰアドレスなどから判断して国外設備から国内設備に送信される電気通信

内閣総理大臣は、これらを分析して国外の攻撃インフラ等の実体把握のため必要があると認める場合には、サイバー通信情報管理委員会の承認を受け、通信情報を取得することができる（１７条、３２条、３３条）。

イ　同意に基づく通信情報の取得

内閣総理大臣は、基幹インフラ事業者その他の電気通信役務の利用者との協定に基づき、当該利用者が送受信する通信情報の提供を受けることができる（12 条、15 条）。

(2)　取得情報の消去を確認する制度は無い

内閣総理大臣は、取得した通信情報について、人による知得を伴わない自動的な方法により、対象とすべき通信のうち①機械的情報であって②調査すべきサイバー攻撃と関係があると認めるに足りる状況があるものを、承認を受ける際に定めた基準に基づき選別した後、それ以外のものを直ちに消去する措置を講ずる（22 条、35 条）。ここで機械的情報というのは、送信元又は送信先である電気通信設備を識別するＩＰアドレス、通信日時その他の通信履歴にかかる情報、電気通信設備に指令を与える情報等とされている。しかし、消去する措置が実際に講じられたかを確認する制度は無い。

(3)関係行政機関の長への協力強制

内閣総理大臣は、自動選別又は選別後の通信情報の分析をするために必要があると認めるときは、防衛大臣その他の関係行政機関の長に対し、必要な協力を要請でき、要請を受けた関係行政機関の長は、その掌握事務に支障を生じない限度において、協力を行うものとする（２７条）。

「その掌握事務に支障を生じない限度」との限定はついているが、「その掌握事務に支障を生じない限度」とは、曖昧不明確であり、実際には、協力を断ることができる場合は想定できず、「協力」ではなく、「強制」である。

(4)　サイバー通信情報監理委員会

法案は、通信情報の利用の適正確保のため、サイバー通信情報監理委員会を置くこととし（４６条）、同委員会は、内閣総理大臣による同意によらない国外関係通信の取得に際しての遅滞のない審査・承認、通信情報の取扱いに対する継続的な検査、無害化措置に際しての審査・承認などの事務を行い、通信情報を保有する機関に対する勧告等の権限を付与する（６３条～６８条）

(5) 通信を広く監視し通信の秘密を侵す危険

同意のない情報取得については、国外に関わる通信に限定されているが、国外と接続された電気通信設備を通じて情報を取得することになる。基幹インフラ事業者その他の電気通信役務の利用者との協定（同意）を前提とする情報取得についても、個別の情報取得に関する同意を得るわけではなく、一度同意すれば、網羅的・継続的に情報を取得することが可能となる。

日本国内においての通信であっても、一度、国外のサーバーを経由したり、国外の通信事業者を利用する場合には、同意なく、情報を取得することも可能となる。受信発信した当の本人すら知らないまま、政府によって通信情報が取得される事態も起こりうるのである。

このような通信情報の取得は、日本国憲法が保障する通信の秘密を侵害するものである。同様に情報を取得する制度である盗聴法（通信傍受法）においてでさえ、犯罪が発生した場合に、裁判所が発布する令状が必要となるが、法案は、情報取得について裁判所の審査は一切必要ない。サイバー通信情報監理委員会が置かれ、独立機関であるとされているが、委員長及び委員４人の合計５人の組織であり、通信の秘密の侵害を防ぐ審査能力を有する機関といえるかについては強い疑いがある。

そもそも、政府は、メールアドレス、ＩＰ情報、送信先などの「機械的情報」を取得して、これを把握できることとされているが、それ自体、通信の秘密を侵害することとなる。のみならず、それ以外の情報、例えば、「〇〇月××日に雨が降りました。」などのコミュニケーション情報については、削除するシステムになっていると説明しているけれども、本当に、コミュニケーション情報を削除しているかどうかを検証するシステムとはなっていない。

このように、法案は、日本国憲法が保障する通信の秘密を侵害し、日本を監視国家とする危険な内容である。

４　アクセス・無害化と先制攻撃の危険

(1)　警察と自衛隊による無害化措置の概要

関連法案のうち、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（以下、「整備法」という）２条では、警察官職務執行法に新たに第６条の２を加え、まず、警察庁長官からサイバー危害防止措置執行官として指名された警察官が（同条１項）、サイバー攻撃に用いられる電気通信等を認めた場合で、そのまま放置すれば重大な危害が発生するおそれがあるため緊急の必要があるときに、①攻撃関係サーバ等の管理者等への措置の命令や、②攻撃関係サーバ等への措置（インストールされている攻撃のためのプログラムの停止・削除など）を自ら実施できるとされている（同条２項）。国外の攻撃関係サーバ等への措置に際しては、外務大臣との事前協議が必要とされ（同条３項）、措置に際しての手続は、独立機関の承認の上（同条４項）、警察庁長官等の指揮によるとされているが（同条１１項）、承認を得るいとまがないと認める特段の事由がある場合は、事後通知でよいとされている（同条４項ただし書き）。

また、整備法では、自衛隊法第８１条の３、第９１条の３、第９５条の４も新設等により改正し、内閣総理大臣が、①一定の重要な電子計算機に対するサイバー攻撃であり、②外国政府を背景とする主体による高度な攻撃と認められるものが行われ、③自衛隊が対処する特別の必要があるときに、通信防護措置を命じた上で（第８１条の３第１項）、新たな行動類型として、自衛隊の部隊等が警察と共同で措置を実施するとされている（同条３項）。また、自衛隊及び日本に所在する米軍が使用する電子計算機をサイバー攻撃から職務上警護する自衛官も、緊急の必要があるときに無害化措置を実施できるとされ（第９５条の４第１項）、措置を実施する場面・措置の内容は、警察と同様とされている（第９１条の３・改正警職法の準用）。

これらについては、内閣官房（新組織）が、国家安全保障局（ＮＳＳ）とも連携しつつ、その司令塔機能を発揮し、警察と防衛省・自衛隊は、措置の実施主体として、内閣官房の調整の下で　緊密に連携するとされている。米軍に対する攻撃につ

いても、自衛隊が無害化措置を実施できることは、集団的自衛権の行使にもつながる問題となる。

(2)　主権侵害のおそれ

このような「アクセス・無害化」は、外国の主権侵害となるおそれがある。また、「無害化」というが、要は日本側からの先制的サイバー攻撃を容認するものであって、いずれかの国による武力行使を誘引するリスクがあり、憲法９条との関係で問題がある。

まず、今回の「アクセス・無害化」を国外にあるサーバ等に対して行う場合、主権侵害に該当するとしても、「緊急状態」等の国際法上の法理を援用するなどして、国際法上許容される範囲内で実施するとされている。

そのとおりであれば、原則主権侵害に該当し、違法性阻却事由を日本側が立証しなければならないという構成であるということになるが、これでは、相手国からは主権侵害と評価されかねない。このような手法について、具体的な境界も引けないまま、前のめりで導入しようとしていることに問題がある。

(3)　戦争の開始につながるおそれ

国家安全保障戦略では、武力攻撃事態に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害拡大を防止するために能動的サイバー防御を導入するものとされており、今回の法案は、そのためのものとされる。しかし、外国から受けるサイバー攻撃も、それを防止する無害化措置も、以下のとおり、戦争の開始につながるおそれがある。

ア　これまでの政府答弁

政府は、「サイバー攻撃のみであっても、例えば、物理的手段による攻撃と同様の極めて深刻な被害が発生し、これが相手方により組織的、計画的に行われている

場合には武力攻撃に当たり得ると考えられ・・・サイバー攻撃による武力攻撃が発生した場合には、憲法上、自衛のための必要最小限度の範囲での武力の行使が許される」としている（安倍内閣総理大臣・令和元年５月１６日衆・本会議）。

そして、「どのようなサイバー攻撃であれば、それだけをもって武力攻撃に当たるかというのは、これは、その時点のさまざまな情勢、相手方の明示された意図、攻撃の手段、態様などを踏まえて個別的に判断せざるを得ないと思いますが、例えばアメリカは、国防省の資料によれば、武力の行使とみなされているものの中に、原子力発電所のメルトダウンを引き起こすもの、人口密集地域の上流のダムを開放し決壊をもたらすもの、航空管制システムの不具合をもたらして航空機の墜落につながるものなどが含まれると言っております。・・・自衛隊による、相手方によるサイバー空間の利用を妨げることは、相手方による武力攻撃が発生しているということが前提であって、これは現行法に基づいて実施することが可能であります。他方、何ら武力攻撃が発生していないにもかかわらず武力を行使する、いわゆる先制攻撃は、国際法上も許されていないというふうに考えているところでございます。ただ、このサイバー攻撃が、いかなる時点で武力攻撃があったか、サイバー攻撃の着手がいかなる時点であったかということについては、これはもうさまざまな情勢を判断して個別具体的に判断しなければならない。（河野防衛大臣・令和２年４月７日衆・安保委）」としている。

イ　エスカレートし、戦争につながるおそれ

政府答弁によっても、武力行使との境界があいまいであり、外国から受けるサイバー攻撃も、それを防止する無害化措置も、ともに武力行使とシームレスにある議論だとすれば、いずれかの側のとらえ方によっては、武力攻撃があったとして、自衛権の行使＝戦争の開始につながるおそれがある。

この点、今回の無害化措置がとられる場合に、当初から、日本側が武力攻撃に相当する措置をとることは想定しがたい。しかし、このように無害化措置であったと

しても、相手側から、自衛隊からサイバー攻撃による先制攻撃があったとみなされ、物理的な反撃を受けるというリスクは否定できない。一方、当初は、日本側が無害化措置をとり、特にこれが先制的であった場合に、相手側から、報復があり、さらに日本側で対処をしているうちにエスカレートし、いずれかの時点で、武力攻撃があったとされる危険性は高いと言わざるを得ない。

法案提出に先立つ、サイバー安全保障分野での対応能力の向上に向けた有識者会議の提言では、「平時と有事の境がなく、事象の原因究明が困難な中で急激なエスカレートが想定されるサイバー攻撃の特性から、武力攻撃事態に至らない段階から我が国を全方位でシームレスに守るための制度とすべき。」としている（提言１１頁）。平時と有事の境なく急激なエスカレートが想定されるのがサイバー攻撃の特性であると断じているのであり、このような見解をもとにすれば、上記で述べたエスカレートする危険性は、極めて現実的なものである。

こうしたリスクは、政府側の事前・事後の承認、ないしは、人選に政府側の意向が及ぶことが想定される「独立」機関の承認では、排除できない。

ウ　軍事一体化で進められる無害化措置の危険

無害化措置の手法について、その内容は、現時点においてなんら具体化されていない。

そもそも、能動的サイバー防御というもの自体、幅のある概念であるが、どのような無害化措置が武力攻撃と区別されるのか。また、本法案では、どのような無害化措置を想定しているのか。さらに、想定されている無害化措置は、サイバーセキュリティの手法として、どのような範囲をカバーできるのか。政府が例として挙げる被害事例への対応として、その他のシステム防御の手法より有効であるのか。それらのメリットが上記リスクを上回るのか、といった疑問がある。

これらが不明である一方で、もともとは、能動的サイバー防御は、日米防衛協力のための指針（２０１５．４．２７）でも、例えば、「平時から緊急事態までのい

かなる状況においてもサイバーセキュリティのための実効的な協力を確実に行うため、共同演習を実施すること」とされており、このような経過の中では、本法案は、自衛隊と米軍との一体化のためのものというべきである（なお、平成３１年４月２５日参議院外交防衛委員会では、サイバー攻撃が、一定の場合には日米安全保障条約５条にいう武力攻撃にあたりうることが確認されている。）。現に、本法案では、在日米軍が使用する電子計算機も、対象となっている。

すなわち、本法案により、集団的自衛権の行使や敵基地攻撃に踏み出す過程で、サイバー攻撃を無害化する対応に及ぶことになる危険があることを指摘せざるを得ない。

エ　まとめ

こうした点につき、議論のないまま、このような「アクセス・無害化」を認める法案を成立させることは許されない。

５　法案提出の経緯と危険性

(1)　安全保障＝軍事としての対応

２０１３年に閣議決定された国家安全保障戦略及び防衛大綱では、サイバー空間における対応について、自衛隊の効率的な活動を妨げる行為を防止するため、統合的な常続監視・対処能力を強化するとともに、専門的な知識・技術を持つ人材や最新の機材を継続的に強化・確保することが明記された。

加えて、２０１８年に定められた防衛計画の大綱では、有事において、我が国への攻撃に際して当該攻撃に用いられる相手方によるサイバー空間の利用を妨げる能力等、サイバー防衛能力の抜本的強化を図ることが明記された。

このように、サイバー攻撃に対する対策は、安全保障の問題として、軍事的にも重要な課題と位置付けられ、自衛隊での対応が進められているものである。

(2)　経済安保　－基幹インフラに対する攻撃と情報保全強化

サイバーセキュリテイ基本法は、２０１６年に同法の改正により、独立法人等も監視･監査の対象とされ、秘密保護規定が設けられ、２０１８年には、行政･重要インフラ、関連事業者等によるサイバーセキュリテイ協議会を設置し、秘密保護や情報提供義務を課する同法の改正が行われたた。

政府は、このような動きを安全保障の問題として位置づけ、２０２２年、サイバー攻撃等から防御するための基幹インフラ整備を進める経済安保法を通常国会で成立させた。そのうえ、２０２３年には、重要経済基盤に関して保護されるべき情報の保全とセキュリティクリアランス制度を導入する経済秘密保護法を成立させ、サイバー攻撃に対する強靭化を進めた。個人のプライバシーや表現の自由を侵害するおそれのある制度が導入されるに至ったのである。

本法案においては、経済安保法においてサイバー攻撃に対して強靭化が必要とされる鉄道、航空、郵送、金融、電気、ガス、水道、放送など基幹インフラ事業者（１５業種）について、インシデントに関する報告を強制され、通信情報を提供する協定を強制される問題がある。しかも、経済安保秘密保護法により、本法案で扱われる通信情報が重要経済安保情報とされて、刑罰による秘密保護とセキュリティクリアランス制度が適用されて、監視強化やプライバシー侵害等がなされるおそれがある。

(3)　日米軍事強化と一体として進められてきた法案づくり

２０２２年１２月に、軍事予算を激増させて軍備を強化し、敵基地攻撃能力を保有する安保３文書が閣議決定され、そのなかで強靭化をはかる対応に加えて、「能動的サイバー防御」を進めることが明記された。

３文書のうちの国家安全保障戦略では、脆弱性等を随時是正するための仕組みを構築する一方で、「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に

排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する」とされたのである。

そのために、同文書では、能動的サイバー防御として、情報収集・分析能力を強化し、①「重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める」こと、②「国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める」こと。③「国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃について、可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする」こと、そしてそのための新たな組織の設置や法制度の整備が提起されたのである。ここでは、まさに本法案の骨格が提示されている。

２０２４年に入って、有識者会議（サイバー安全保障分野での対応能力の向上に向けた有識者会議）で議論され、１２月にまとめられた同会議の提言を受け、政府は、今通常国会において、能動的サイバー防御に関連する法案を提出する準備を進めてきたのである。

このような動きは、すでに、２０１５年４月の日米政府が合意した新ガイドラインにおいて提起されている。そこでは自衛隊及び米軍の利用する重要インフラ及びサービスに対するものを含めて、日本に対するサイバー事案が発生した場合の対応、とりわけ、日本が武力攻撃を受けている場合に発生するものを含め、日米両政府は緊密に協議し、適切な協力行動をとり対処することが確認されている。２０２２年１月の日米安全保障協議委員会（２＋２）でも、強固なネットワーク防衛及びあらゆる種類のサイバー脅威への共同対処が日米同盟にとって必須であることが確認され、２０２４年７月の２＋２では脅威に対処する防御的サイバー作戦における緊密な協力を促進するとされている。

このように、今回のサイバー防御に関する法案の提出は、日米共同での戦争を進

めるうえで必要不可欠な制度づくりとして位置づけられており、日米同盟強化と一体となって進められていることは明白である。

(4)　まとめ

以上の経緯からも明らかなように、法案提出に至る経過と軍事拡大、日米同盟の強化を進める動きは一体のものであり、戦争する国づくりの重要な仕組みを作ろうとする狙いがあることは明らかではないだろうか。

平和と人権を危うくする本法案は、速やかに撤回するべきである。仮に撤回されないとしても、国会審議において問題点を明らかにして廃案にするべきである。

以上

****

２０２５年3月１２日

編集　自由法曹団・改憲阻止対策本部
発行　自由法曹団
〒112-0014 東京都文京区関口 1-8-6
メゾン文京関口Ⅱ202 号
Tel 03-5227-8255 Fax 03-5227-8257
URL http://www.jlaf.jp/

****